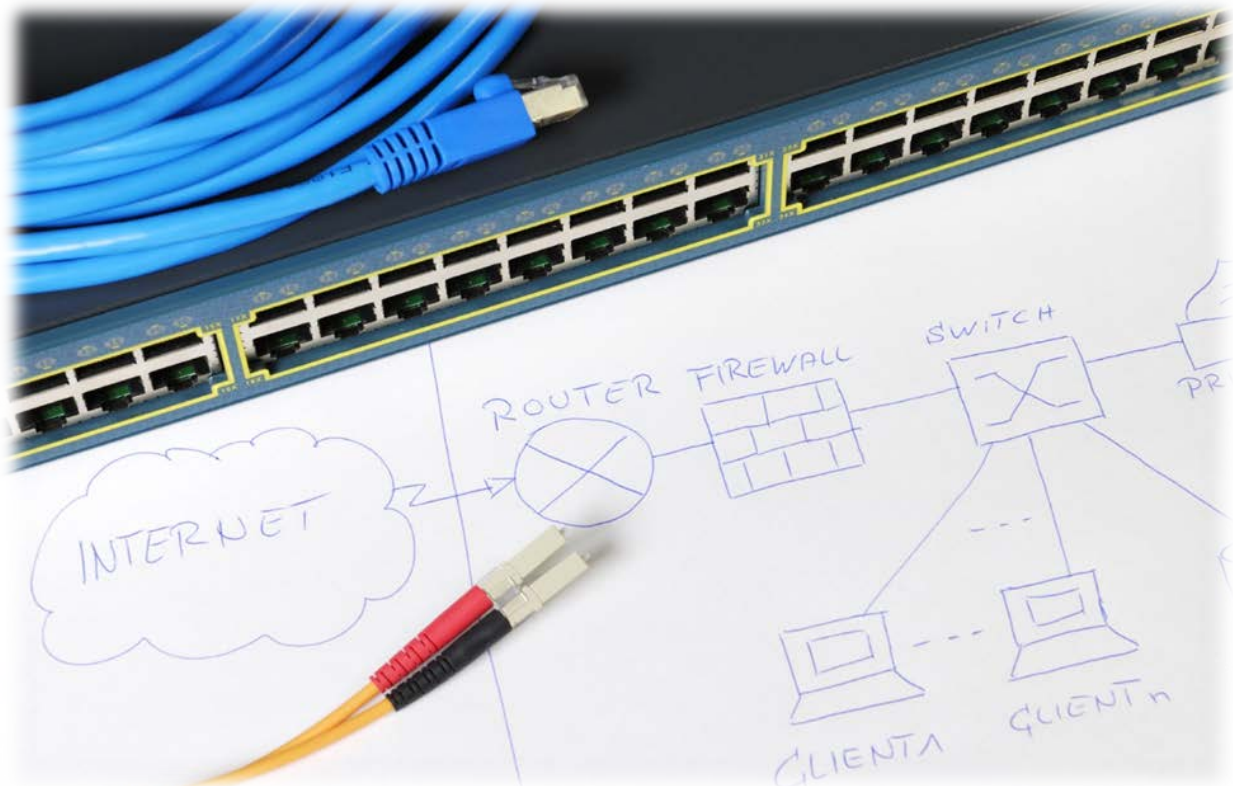


Network Design Cookbook:

Architecting Cisco Networks

Version 10.1.10 (Updated: October 30, 2015)



Michel Thomatis, CCIE #6778
RouteHub Group, LLC
www.RouteHub.net



Network Design Cookbook: Architecting Cisco Networks

by

Michel Thomatis, CCIE #6778

Copyright 2011 Michel Thomatis
All rights reserved.

ISBN-13: 978-1-257-75024-5

No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems, without permission in writing from the author. The only exception is by a reviewer, who may quote short excerpts in a review.

May 8, 2011

CCDE, CCIE, CCDP, CCIP, CCNP, CCVP, CCSP, CCDA, CCNA, CCENT, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or web site are the property of their respective owners.

ROUTEHUB GROUP END-USER LICENSE AGREEMENT

END USER LICENSE FOR ONE (1) PERSON ONLY
IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS,
DO NOT OPEN OR USE THE TRAINING MATERIALS.

IMPORTANT! BE SURE TO CAREFULLY READ AND UNDERSTAND ALL OF THE RIGHTS AND RESTRICTIONS SET FORTH IN THIS END-USER LICENSE AGREEMENT ("EULA"). YOU ARE NOT AUTHORIZED TO USE THIS NETWORK CONFIGURATION GUIDE/TRAINING UNLESS AND UNTIL YOU ACCEPT THE TERMS OF THIS EULA.

This EULA is a binding legal agreement between you and ROUTEHUB GROUP, LLC (hereinafter "Licensor") for the materials accompanying this EULA, including the accompanying computer Network Configuration Guide/Training, associated media, printed materials and any "online" or electronic documentation (hereinafter the "Network Configuration Guide/Training"). By using the Network Configuration Guide/Training, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or attempt to use the Network Configuration Guide/Training.

The Guide & Training Materials shall be used by only ONE (1) INDIVIDUAL who shall be the sole individual authorized to use the Guide & Training Materials throughout the term of this License.

1. Grant of License

The Network Configuration Guide/Training is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Network Configuration Guide/Training is licensed, not sold. This EULA grants you the following rights:

- A. You may use, access, display and run only one copy of the Network Configuration Guide/Training, on a single computer, workstation or terminal ("Computer"). The primary user of the Computer on which the Network Configuration Guide/Training is installed may make a second copy for his or her exclusive use for archival purposes only.
- B. You may store or install a copy of the Network Configuration Guide/Training on a storage device, such as a network server, used only to run the Network Configuration Guide/Training on your other Computers over an internal network. You must, however, acquire a license for each separate Computer on which the Network Configuration Guide/Training is run, displayed or utilized from the server or similar device. A license for the Network Configuration Guide/Training may not be shared or used concurrently on different Computers.
- C. Your license rights under this EULA are non-exclusive. All rights not expressly granted herein are reserved by Licensor.
- D. You may not sell, transfer or convey the Network Configuration Guide/Training to any third party without Licensor's prior express written consent.

2. Price and Payment

If you have not previously paid the license fee for the Network Configuration Guide/Training, then you must pay the license fee within the period indicated in the applicable invoice sent to you by Licensor.

3. Support Services

This EULA is a license of the Network Configuration Guide/Training only, and Licensor does not assume any obligation to provide maintenance, patches or fixes to the Network Configuration Guide/Training. Licensor further disclaims any obligation to provide support or to prepare and distribute modifications, enhancements, updates and new releases of the Network Configuration Guide/Training.

4. Replacement, Modification and/or Upgrades

Licensor may, from time to time, and for a fee, replace, modify or upgrade the Network Configuration Guide/Training. When accepted by you, any such replacement or modified Network Configuration Guide/Training code or upgrade to the Network Configuration Guide/Training will be considered part of the Network Configuration Guide/Training and subject to the terms of this EULA (unless this EULA is superseded by a further EULA accompanying such replacement or modified version of or upgrade to the Network Configuration Guide/Training).

5. Termination

You may terminate this EULA at any time by destroying all your copies of the Network Configuration Guide/Training. Your license to the Network Configuration Guide/Training automatically terminates if you fail to comply with the terms of this agreement. Upon termination, you are required to remove the Network Configuration Guide/Training from your computer and destroy any copies of the Network Configuration Guide/Training in your possession. No refund with the product will be granted.

6. Copyright

- A. All title and copyrights in and to the Network Configuration Guide/Training (including but not limited to any images, photographs, animations, video, audio, music and text incorporated into the Network Configuration Guide/Training), the accompanying printed materials, and any copies of the Network Configuration Guide/Training, are owned by Licensor or its suppliers. This EULA grants you no rights to use such content. If this Network Configuration Guide/Training contains documentation that is provided only in electronic form, you may print one copy of such electronic documentation. Except for any copies of this EULA, you may not copy the printed materials accompanying the Network Configuration Guide/Training.

B. You may not reverse engineer, de-compile, disassemble, alter, duplicate, modify, rent, lease, loan, sublicense, make copies of, create derivative works from, distribute or provide others with the Network Configuration Guide/Training in whole or part, transmit or communicate the application over a network.

7. Export Restrictions

You may not export, ship, transmit or re-export Network Configuration Guide/Training in violation of any applicable law or regulation including but not limited to Export Administration Regulations issued by the U. S. Department of Commerce.

8. Disclaimer of Warranties

LICENSOR AND ITS SUPPLIERS PROVIDE THE NETWORK CONFIGURATION GUIDE/TRAINING "AS IS" AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY (IF ANY) IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF LACK OF VIRUSES, AND OF LACK OF NEGLIGENCE OR LACK OF WORKMANLIKE EFFORT. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, OF QUIET ENJOYMENT, OR OF NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE NETWORK CONFIGURATION GUIDE/TRAINING IS WITH YOU.

9. Limitation of Damages

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE NETWORK CONFIGURATION GUIDE/TRAINING AND WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF LICENSOR OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS EXCLUSION OF DAMAGES WILL BE EFFECTIVE EVEN IF ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

10. Arbitration

Any dispute arising under this EULA will be subject to binding arbitration by a single Arbitrator with the American Arbitration Association (AAA), in accordance with its relevant industry rules, if any. The parties agree that this EULA will be governed by and construed and interpreted in accordance with the laws of the State of California. The arbitration will be held in California. The Arbitrator will have the authority to grant injunctive relief and specific performance to enforce the terms of this EULA. Judgment on any award rendered by the Arbitrator may be entered in any Court of competent jurisdiction.

11. Severability

If any term of this EULA is found to be unenforceable or contrary to law, it will be modified to the least extent necessary to make it enforceable, and the remaining portions of this Agreement will remain in full force and effect.

12. No Waiver

No waiver of any right under this EULA will be deemed effective unless contained in writing signed by a duly authorized representative of the party against whom the waiver is to be asserted, and no waiver of any past or present right arising from any breach or failure to perform will be deemed to be a waiver of any future rights arising out of this EULA.

13. Entire Agreement

This EULA constitutes the entire agreement between the parties with respect to its subject matter, and supersedes all prior agreements, proposals, negotiations, representations or communications relating to the subject matter. Both parties acknowledge that they have not been induced to enter into this EULA by any representations or promises not specifically stated herein.

Table of Contents

1	ABOUT THE AUTHOR	8
2	THE ARCHITECTURE OF NETWORK DESIGN.....	9
3	DESIGN PROCESS.....	28
4	DESIGN STEPS	30
5	REQUIREMENTS	31
6	GENERAL DESIGN	35
7	SOLUTIONS	47
	A	48
	<i>Application Delivery</i>	49
	B	58
	<i>Bring Your Own Device (BYOD)</i>	59
	C	60
	<i>Call Center</i>	61
	<i>Cloud Computing</i>	68
	<i>Collaboration</i>	70
	<i>Conferencing</i>	71
	<i>Content Security</i>	75
	D	87
	<i>Data Center</i>	88
	<i>Data Loss Prevention</i>	124
	<i>Desktop Solution</i>	125
	<i>Disaster Recovery</i>	126
	<i>DMZ & Extranet</i>	128
	E	131
	<i>Endpoint Security</i>	132
	F	133
	<i>Firewall</i>	134
	I	147
	<i>Identity Access Control</i>	148
	<i>Internet Edge</i>	157
	<i>Internet of Things (IoT)</i>	175
	<i>Intrusion Prevention</i>	176
	L	188
	<i>Local Area Network (LAN)</i>	189
	M	219
	<i>Messaging</i>	220
	N	228
	<i>Network Management</i>	229
	O	234
	<i>Optimization</i>	235
	P	242
	<i>PCI/DSS</i>	243
	<i>Physical Security</i>	245
	<i>Presence</i>	246
	<i>Proxy</i>	249
	S	255
	<i>Server Solution</i>	256
	<i>Social Networking</i>	258
	<i>Software Defined Networking (SDN)</i>	259
	<i>Storage</i>	261
	T	272
	<i>Teleworker</i>	273
	U	277
	<i>Unified Computing</i>	278
	V	291
	<i>Video</i>	292
	<i>Virtualization (Network)</i>	298
	<i>Virtualization (System)</i>	301
	<i>Voice (Unified Communications)</i>	303
	<i>VPN & Remote Access</i>	330

W		339
	<i>Web & E-Commerce</i>	340
	<i>Web 2.0</i>	343
	<i>WebEx</i>	344
	<i>Wide Area Network (WAN)</i>	345
	<i>Wireless</i>	363
8 SERVICES		382
A		383
	<i>Access Control Lists (ACL)</i>	384
B		385
	<i>BGP</i>	386
	<i>BPDU</i>	390
	<i>Bridge Assurance (BA)</i>	391
	<i>Broadcast Suppression</i>	392
C		393
	<i>CEF, IP</i>	394
D		395
	<i>DFC</i>	396
	<i>DHCP</i>	397
	<i>DHCP Snooping</i>	398
	<i>DMVPN</i>	399
	<i>DNS</i>	402
	<i>Dynamic ARP Inspection</i>	403
E		404
	<i>Easy Virtual Network (EVN)</i>	405
	<i>EIGRP</i>	407
F		410
	<i>FabricPath</i>	411
	<i>First-Hop Redundancy Protocol (FHRP)</i>	420
	<i>Flex Link</i>	421
	<i>FlexVPN</i>	422
G		423
	<i>General Best Practices</i>	424
	<i>GET VPN</i>	425
	<i>GLBP</i>	427
H		428
	<i>HSRP</i>	429
I		430
	<i>IPSec VPN</i>	431
	<i>IPv6</i>	436
	<i>In-Service Software Upgrade (ISSU)</i>	454
	<i>Intrusion Prevention</i>	455
L		456
	<i>Layer 2 Multi-Path (L2MP)</i>	457
	<i>Layer 2 VPN (L2VPN)</i>	458
	<i>Locator/ID Separation Protocol (LISP)</i>	459
	<i>Loop Guard</i>	462
M		463
	<i>MAC-in-MAC</i>	464
	<i>Medianet</i>	465
	<i>MPLS VPN</i>	466
	<i>Multicast, IP</i>	470
	<i>Multi-CE VRF (VRF-lite)</i>	477
N		479
	<i>Network Address Translation (NAT)</i>	480
	<i>NSF & SSO</i>	482
	<i>Network Management</i>	483
O		484
	<i>OSPF</i>	485
	<i>OTV</i>	489
P		491
	<i>Policy Based Routing (PBR)</i>	492
	<i>Port Channel (802.3ad)</i>	493
	<i>Port Monitor</i>	494
	<i>Port Security</i>	495

	<i>Power over Ethernet (PoE)</i>	496
Q	<i>Quality of Service</i>	497
	<i>Quality of Service</i>	498
R	<i>Root Guard</i>	515
	<i>Root Guard</i>	516
	<i>Routing, IP</i>	517
S	<i>Security Best Practices</i>	521
	<i>Security Best Practices</i>	522
	<i>SNMP</i>	524
	<i>Spanning Tree Protocol (STP)</i>	525
	<i>SSL VPN</i>	528
	<i>SLA, IP</i>	529
	<i>Source Guard, IP</i>	530
	<i>Stacking Technology</i>	531
	<i>Stateful Switchover (SSO)</i>	531
	<i>Static Routing</i>	532
	<i>Syslog</i>	533
T	<i>Trunking (802.1Q)</i>	534
	<i>Trunking (802.1Q)</i>	535
	<i>TrustSec (Cisco)</i>	536
U	<i>UDLD</i>	538
	<i>UDLD</i>	539
	<i>Uplink Fast</i>	540
V	<i>Virtual Extensible LAN (VXLAN)</i>	541
	<i>Virtual Extensible LAN (VXLAN)</i>	542
	<i>Virtual LAN (VLAN)</i>	545
	<i>VLAN Trunking Protocol (VTP)</i>	546
	<i>Virtual Port Channel (vPC)</i>	547
	<i>Virtual Switching System (VSS)</i>	554
	<i>VRF-lite</i>	557
W	<i>WCCP</i>	558
	<i>WCCP</i>	559
0 - 9	<i>802.1X</i>	560
	<i>802.1X</i>	561
9	DESIGN OPTIONS	562
10	DESIGN RESOURCES	563
	<i>SERVICE PROVIDER (ISP) LIST</i>	563
	<i>TOOLS AND URLS</i>	564
	<i>OTHER RESOURCES</i>	565
	<i>1: Router vs Firewall</i>	565
	<i>2: RFI Checklist</i>	566
	<i>3: Performance: Blocking, Non-Blocking, and PPS</i>	567
	<i>CONFIGURATION CHECKLIST</i>	569
	<i>1: Checklist for Routers</i>	569
	<i>2: Checklist for Access Switches</i>	571
	<i>3: Checklist for Core/Distribution Switches</i>	573
	<i>4: Checklist for Firewalls</i>	575

1 About the Author

Michel Thomatis, CCIE #6778, has spent the last 17 years as a network engineer/architect. As a 10-year CCIE, Michel loves the opportunity to provide training in a wide-array of network technologies. He formerly worked at Cisco, as well as in government, banking, and non-profit organizations. Currently, Michel is the owner and Chief Network Architect and Trainer at RouteHub Group, LLC.

2 The Architecture of Network Design

Information Technology and Roles

1

Information Technology

When I was on jury duty once, the judge asked me what I do for living and my response was "IT". He responded by saying what is "IT"? Though we expect everyone to know what IT is people who are not in that world just don't understand. My own family doesn't really know what IT is. If you say "work with computers" they automatically assume that you can fix their slow computer problems. IT or Information Technology is a profession with many different facets or specialties. One of them being computers or desktop administration. Like a doctor they can specialize with the heart, skin, the brain, or maybe the bones. IT is the same, just not life threatening.

Everyone starts out with Desktop administration which deals with working with computers, troubleshooting computers, installing software like Microsoft Office, and other similar tasks. The impact is low, meaning that if a computer fails it only affects that user and not all users.

From there these are other specialties an IT person can focus on:

- **Servers:** Server Administration, System Engineer
- **Networking:** Network Administration, Network Engineer, Network Architect
- **Security:** Security Administration, Security Engineer, Network Engineer
- **Database (DB):** DB Administration (DBA), DB Engineer
- **Development/Engineering:** Programming, Web
- **Telephony:** Phone Technician, Network Engineer
- **Management:** Project Management, IT Management

Server administration deals with managing servers like web servers or email servers to provide various services/solutions. The impact is higher than desktop administration because if a server fails it can affect a large group of users trying to access that server.

Networking works completely in the background where users are not aware of their existence. They provide the infrastructure and the capability that a computer can access other computers or servers on the network. This includes the Internet, but there are some components required from the server administration side like DNS and Security administration like Firewalls or Content Security. In the networking world, it is just supposed to work, however the impact level is higher than any other IT specialty because if the network fails that impacts ALL users and services.

Security administration really has two roles, Information Security (or Policy) and Operations. Information Security deals with writing up a policy of do's and don'ts users, servers, desktops, networks, phones, everything "must" comply with especially if there are mandates companies need to follow such as PCI, SOX, or HIPPA. Security Operations deals with

managing security components such as Firewalls, IPS/IDS, Content Filtering, running audits, looking at security logs, etc. Some of these Security operations are usually done by the network engineer in regards to the Firewall. So a network engineer will usually manage the network, but also manage the firewall and its configuration.

Database administration deals with managing and supporting database servers that can be integrated with other servers and/or services on the network. This is usually a field that stands alone from the rest of the pack meaning if you are working on databases, you're only working on databases. This also has a high impact that many servers may rely on for their application and data. For example, if the database is offline regardless if the server is functional, the servers will not work until the database is on-line.

Development has many different facets itself that mainly involve programming such as new applications, tools, scripts, to web pages. This is the one field that has a lot of concern in regards to job stability where much of this type of work is being outsourced to other countries.

Telephony administration deals with managing the phone system and essentially, like the network engineer, works in the background unnoticed. When you pick up a phone and place a call to someone, it just works. But this field is responsible for providing phone access for users. This field has evolved into Voice over IP (VoIP) where phones can be plugged directly into the network making moves, additions, and changes extremely easy. Since voice is going across a network most of these roles are also being pushed to the network engineer especially when Voice VLANs, 802.1Q, PoE, QoS, and Multicast are involved. Day to day operations can still be done by a phone technician.

And then there is **Management**, which can be Project managers responsible for managing projects in an organized manner. And IT Management such as IT managers, IT directors, or a CTO dealing with managing IT people and to streamline IT to align with the business model. Or what IT managers should be doing.

In most companies many IT people will wear multiple hats. So you will usually see a Server person, a Network person, and a Desktop person. A network person will work on the network, security, and voice for the company. The server person will work on the servers, database, maybe some programming (like Visual Basic), to some desktop administration. Larger businesses with a lot of network components that need to be managed those roles are usually divided out between different groups.

From the list provided I mentioned administration and engineering. What is the difference? That will depend on your company. I know a few consulting companies who call their server administrators "Network Engineers", but they do not deal with networks or know much about networking to begin with. When I was working at LLNL/DOE my official job title was a Computer Scientist, but I was responsible for the architecture, configuration, and tier 3+ support for the backbone infrastructure. My job title to others was a Senior Backbone Engineer, which reflected closely to what I actually did. So actual job titles and roles will vary greatly based on a person's definition of the title.

So back to the administration and engineering roles. Usually, Network or System administration deals with day-to-day operations and some configuration where needed. A network, security, or system engineer can deal with the administration roles, but also deal with the design aspects within that field.

Many people will also wear a design hat with their job since the workload for pure design work is minimal. And another point to discuss is that every IT person has worked in every IT role out there, but they have a primary field that they specialize in. For example, I deal with network engineering, but I have built computers, installed servers, done DCPROMOs, setup Exchange, dealt with doing security audits, Perl programming including some VB scripts. Same for other IT people who have configured a router or firewall, but they are server people. It comes down to what dedicated field you provide value and a trusted level of expertise. Again, I can install a Windows 2008 domain controller, but I don't know the big picture involved including best practices.

So IT is a growing and very popular profession with many different facets. When people ask me what I do, I tell them that I am in IT specializing with Network Engineering.

In IT nothing is by the book. Being certified (e.g. CCNA, CCIE, JJNCIE, CISSP, etc.) strays completely away from the reality of what is going on in IT. Designs are usually not by the book. I have seen many different type of networks that you will not typically see in text books or case studies.

The bottom line is this in IT everything changes. IT is not 100% perfect.

IT is not perfect mainly due to business processes, objective challenges, administer/engineer preferences and experiences. We will discuss this further.

Another reason is that business requirements and expectations may change in a short period of time. For example, I worked at a place where the IT management staff did not see the need for considering VoIP, so the network was built around that requirement. Within less than a year my manager was reading one of his IT director magazines and says "we should be using VoIP" plus the current PBX system was set to expire. This situation resulted in the company spending more money with buying new hardware to replace the new hardware we just bought less than a year ago. The main reason for this was that management didn't feel comfortable about VoIP because it was new to them and didn't know what to expect.

This type of occurrence in one form or another exist in most company network's today where IT Management is making IT decisions resulting in the IT staff left to support this unique design.

Things are not what it seems for beginners in the IT field. A person who recently passed their CCNA going into a new network get confused that what they have learned is not being executed.

The way a network is deployed is based on the preferences of the engineer, consultant, business owner, and IT management staff. We all have preferences to how a network should be deployed.

Some portion of the network may be unique to the client/company that may not be referenced in any recommendation or case study design. This would be a unique element to that design.

I don't expect all networks to be the same, but following a structure that can produce a recommended design should always be considered.

Let's break this down further into different sections since preferences is the root cause for how a network is designed and deployed. Some of these preferences have consequences that can provide challenges to one or more of the technical objectives.

This is the breakdown of what we will discuss further.

- General Preferences
- Hardware Preferences
- Unique Elements

A network design is based on the network architect and/or decision maker preferences. These are some of the preferences that the design will be based upon:

- Hardware Preference
- Configuration Interface (e.g. CLI, GUI)
- Protocols, Technologies
- Support Model

This will be discussed further under the section "Architect Roles" when we further define how these preferences affect the design.

The decision maker may not like Layer 2 and will never include that in their design. This is an example of having a Protocol/Technology Preference to not use Layer 2 services. The consequence results to a lack of extending subnets across the network to challenges for implementing VoIP ideally.

The decision maker may be a new CTO joining the company and deciding to replace all network gear to Cisco because he/she has a Hardware Preference for Cisco. That consequence would result to higher costs, training, and potentially limitations of supporting various components on the network.

The decision maker may be a consultant who will support the network that will be deployed. Therefore, they may have a preference to choose a solution and hardware that they feel comfortable to support providing great value-add to their client. That consequence could result in the network not being ideally designed and may cause issues in the future. This would be an example of building a separate voice network which connects into the LAN.

Or the decision maker may be a server administrator or person more comfortable with GUI interfaces for making configuration changes. Therefore, their preference would be to choose products that have a GUI interface. That consequence may result in limited configuration support for certain services and features like MPLS.

These are example of preferences that may alter what the network design will eventually look like. This is determined during the requirements gathering to understand the preferences involved.

Early on in my IT career, I have learned to never have discussions about politics nor religion. They can be very heated discussions and lead to no result. However, I like to add a third item to that list which is vendor hardware preferences.

Every engineer, consultant, or any IT person for that matter has a preference to what they would choose for a router, switch, server, firewall, to even a computer system. Some may have no preference, but majority already know in their minds what they would choose.

For example, my hardware preference for routers, switches, security solutions, voice solutions, and wireless is with Cisco products. I have many partners who prefer SonicWALL for a firewall solution or Juniper. I know a client that prefers Fortinet because they like the GUI interface it provides for management.

Some prefer Microsoft for servers and desktops, a client of ours in San Francisco prefers Mac-based systems for their desktops. And the list goes on.

The reason we have a definite hardware preference is because of two factors:

- Skilled Experience
- Vendor Relationship

I have been working with Cisco products for over 15 years with designing, deploying, and troubleshooting. I know them very well, so I have a lot of working experience with Cisco products. I also understand how to use Cisco (the Vendor Relationship aspect) and how not to use them. I like the support model for the Cisco TAC and how to use it. I know when to engage Cisco and when to not engage Cisco for getting new product information, getting certified, to getting a Cisco person on-site at a client location.

If IT people have a preference to one vendor they may have a dislike towards another vendor. For example, I have two clients who do not like Cisco or SonicWALL firewalls. They love Juniper firewalls. I personally question most of the configuration and monitoring aspects for Juniper and Checkpoint firewalls, so I do have my own dislike preferences. Many IT people bash Windows for being prone to many viruses and crashes, thus the release of the many MAC vs. PC commercials.

The primary reason for the dislike towards another vendor is based on two factors:

- Low/Limited Skilled Experience
- Poor/Limited Vendor Relationship

The same factors for what makes it a preference for a person.

The two clients who dislike Cisco Firewalls are not fond of CLI and have less than a year of working experience with Cisco firewalls. They don't work with Cisco firewalls a lot or have any related training. They worked with Juniper firewalls. This includes their limited experience with SonicWALL products. They never deployed them and have no production experience. They are comfortable with how to administrator the Juniper because they know what to expect. They also love Juniper support. They didn't like Cisco support because the whole SMARTnet contract process and how to open a ticket was confusing to them. In reality they only done it twice and didn't know the process.

Let's pick on me for a little bit. I prefer CLI, I can provide value-add expertise and implement many solutions via CLI faster than GUI. However, GUI for Cisco UCM and Wireless LAN Controllers is very simple for administration. My working experience with Juniper and Checkpoint firewalls is very limited and I am very comfortable with how to administrator Cisco products.

Having a dislike besides the limited experience could be related to a bad relationship with the hardware vendor. For example, I have a partner who was trying to become a Cisco partner and the process was confusing to them, which took several months. The Juniper Partnership program was easier for them and that was the moment when they preferred Juniper products over Cisco products. Therefore, they experienced a poor vendor relationship with Cisco because of the partnership ordeal. ROUTEHUB GROUP became a Cisco partner in short time because again we have experience and know how the process works.

Another reason for a dislike is when an IT person says Juniper Firewalls are faster than Cisco firewalls. I often like to inquiry more on what they did to determine that. Such as what was the Cisco product model, the Juniper product, who configured the Cisco Firewall, and who configured the Juniper Firewall. The answer most of the time is the same. They configured both firewalls, but have higher experience with one product over the other. So in this case they have strong experience with the Juniper products and little with Cisco. They did some Google searches to get the Cisco firewall working. Also they used a Cisco product that was aimed for the SMB/Medium market and the Juniper product chosen was aimed for large enterprises.

So, it wasn't a fair alignment of products based on the business size and the configuration of the Cisco firewall was questionable due to limited experience. This is fairly common when preferences and dislikes are exchanged. The bottom line is this, no product is truly poor in performance and what it provides if it is deployed correctly. And if it is deployed for the correct market segment and meets the requirements. That is the only factors that are important. I have seen SonicWALL firewalls deployed in SMB networks causing no issues. I have seen WatchGuard firewalls deployed without any impact or issues. I have personally deployed Cisco Firewalls for Small to Large Enterprise environments without any performance issues. The reason for these three cases is that they were all deployed based on true production experience and met the overall requirements.

Therefore, when you choose the hardware for a component determine the following:

- Meets the business and technical requirements
- Aligns (if applicable) with the Business size of the network & business

- Simplicity and Administration
- Experience and the Support Model
- Realistic Metric Conditions (e.g. Performance)

Let me quickly discuss what "Realistic Metric Conditions" means. Different firewall models provide metrics such as firewall throughput and VPN throughput. This also goes for switches with the forwarding rate, backplane traffic, to throughput with a line module for a chassis. The main determination is to understand the realistic metrics. For example, let's say that firewall product "A" provides 1Gbps for firewall performance and firewall product "B" provides 500Mbps for firewall performance. Most IT people will say that firewall product "A" is the better choice, especially if that is their preference. Well if your Internet connection is a T1, then your highest possible throughput through the firewall is roughly 1.5Mbps. That is far below the metrics for products "A" and "B", so both are a good choice.

This discussion can be heated as you can see, therefore, the only main point is choosing a hardware product based on the requirements, support model, and value-add expertise for deploying the product into the network.

c	Unique Elements

A unique element is a network solution that is unique to the client/company. It is not seen in any recommendation or case study design. Some unique elements can be justified by the requirements and building that solution ideally. But some unique elements can be bad and likely created to serve a specific purpose.

Many network engineers who go into an existing network environment will look at the network and will often say "who designed and configured this network?"

The irony is that every network has a unique element. And everyone has taken part of a unique element design at some point in their career.

Let me provide an example to illustrate this point. I had a client who wanted to know if we can enable about 100+ DHCP scopes on the Cisco Core switch. Well yeah, it can, but it's not recommended, and it should be configured on a dedicated DHCP server. Well this was the client's network and they made the decision of using the Core switch to act as the DHCP server with over a 100 DHCP scopes. Then they can follow-up with using a dedicated DHCP server sometime in the future. Something that is often said and quickly forgotten about until an issue comes up.

This is an example of a unique element that can occur in one form or another. So, why is this the case?

Its several things, but they are usually done for the following reasons:

- Support Band-Aid
- Cost
- Convenience and Availability
- Simplicity
- Unique Requirement

With the example I provided, it was a matter of simplicity, convenience, and availability. Because ideally a dedicated server should be taking care of those functions. But that requires a new server to be built, with likely new hardware that needs to be purchased, hence, additional cost. Next, they have to install the OS, spend time configuring it, and then enable DHCP. Next they have to rack the server, cable, power, and then test it out. It's a lot easier to enable DHCP services on the Core switch to eliminate doing any of those steps. That is how it happens and it all starts from the decision maker.

Here is another example, let's say there is a server running DHCP scopes, but it fails and is impacting the business. As a quick Band-Aid they enable DHCP services on a Cisco router and everything is running again. The services may eventually get moved back to a server, but will likely remain on the Core router for an extended period of time. Even up to a point when the next network engineer/consultant who comes in will say "who designed and configured this network? Why is DHCP enabled on a Core router with all these scopes? They should be deployed on dedicated server".

You get the point and see how the cycle works. This is considered as a preferences that may determine how a network is designed.

Components

1

Business Objectives

The biggest determination for moving ahead on a project or not approving it is based on cost. The business wants to know how much it will cost them. Therefore, understanding the budget requirements for consideration becomes very valuable during the design process. There are many ways for doing a network design and going in blind without knowing the budget could prevent possible challenges.

Simplicity and Productivity are other objectives to provide robust service with easy management and possible automation. For example, a company may want to implement Auto Attendant (AA) to eliminate the need for an administrative assistant, which can focus on other tasks to build the business. Therefore, we have an automated menu to provide information about the company, directions, and access to the phone directory. This also leads to another business objective called, Total Cost of Ownership (TCO) and Return on Investment (ROI). By implementing AA we have allowed our administrative assistant within the company to bring additional services and revenue for the company.

Other objectives deal with providing a technical advantage and new services for clients such as Unified Messaging or VLANs. Another objective is based on requirements or mandates from regulatory compliances (e.g. PCI, SOX, and HIPPA) including doing a technology refresh by replacing older hardware. The requirement objective can deal with providing best practices for the network including the technical objectives.

The following objectives are considered within our design as technical requirements:

1. **PERFORMANCE:** Performance deals with the rate and quality of traffic delivery across a network. Bandwidth and throughput are one of the components that can describe performance. QoS is another component that assigns priority to specific traffic on the network. Port buffers and queues also fall into quality of traffic delivery which is often discussed with Congestion Management and Avoidance with QoS.
2. **RELIABILITY:** Reliability deals with the redundancy and stability of the network. Faults on a network will occur in the form of hardware, software, or human related failures. Therefore, it's important to understand how long can the network be down (the SLA) before a serious impact occurs (e.g. customers leaving). The answer for most cases would be as minimal as possible, less than 1 or 4 hours. Therefore building a network with redundancy is important to consider and construct within a network design. However, higher redundancy requirements mean higher costs and complexity.
3. **SCALABILITY:** Scalability deals with the growth or increase of users, servers, and services on the network. Building a network to accommodate today's requirements is not good if we don't understand the requirements and expectations for tomorrow. This is obtained during the requirements gathering.
4. **SECURITY:** Security provides protection of confidentiality and integrity for users, servers, and services on the network. This may include mandates or regulatory compliances such as PCI, HIPPA, or SOX. Much of best practices focus around this technical objective.
5. **FLEXIBILITY:** Flexibility has a dual meaning and purpose. The first deals with understanding the potential use of network services and technologies that may be included with the design in the future. For example, maybe the design today does not include VoIP, but it may be included in another 1 or 2 years. Therefore, the design should consider those additions. The second deals with integration of existing or legacy infrastructure. This may include an older phone system or PBX with requirements to ideally work with the new design like a new Cisco Unified Communication Solution. Understanding these considerations and possible additions is also important.
6. **NETWORK MANAGEMENT:** Network Management also has a dual purpose dealing with Management and Monitoring. Monitoring deals with providing proactive fault management (e.g. monitoring when devices are UP or DOWN, traffic usage), performance management (e.g. using a protocol called NetFlow to view traffic flow conversations and top-talkers), and configuration management (e.g. backing up configuration, performing audits and defining best practices). Management deals with the IT support model of who will be supporting the designed network at a Tier 1, Tier 2, and maybe a Tier 3 level. Deploying a complex design with Tier 1 level staff may present challenges, so understanding the support model is important.

Scalability	Reliability	Performance	Security
Management	Flexibility	Hardware	Design Aspects

There are a lot of networking terms that are out there and it's confusing to know where they belong such as Routing, Switching, LAN, Wireless, Security, VPN, Unified Communication, and the list goes on. I have come up with an organized way to group these technologies and solutions. They are broken down into Network Services and Network Solutions.

A Network Solution would be one of the following:

- LAN, Data Center, WAN, Internet Edge, Remote Access, Cloud Computing

And Network Services would be one of the following:

- Routing & Switching, Security & VPN, Multicast, QoS, IPv6

What are the differences between the two? Consider the solution as a completed puzzle with multiple pieces. Some solutions may have more pieces than others. Each piece in the puzzle (our solution) is a Network Technology or service. For example, a WAN Solution will likely to consist of services like Routing, Security, and VPN. Business Owners or IT Management will tend to seek out solutions and do not need to know about the details, which are the network services. Network Engineers and Consultants will likely seek out Network services within a solution for assistance.

Locations deals with where the components on the network reside. The location can be any of the following:

- IDF
- MDF
- Data Center
- Office/Other

The IDF is a wiring closet that connects back to an MDF room or Data Center.

The MDF is a wiring closet that connects to other IDF rooms including Data Centers.

The Data Center is a dedicated room with Data Center components such as racks, cabinets, ladder racks, cooling, and more. Mainly used for server farm environments.

Office/Other locations is where a user's computer/laptop is located such as an office, cubicle, or a work space. Each location that has 1 or 2 ports that is wired back to an IDF, MDF, or maybe a Data Center location.

There can be variations for some of these rooms such as a Lab or training class. A training classroom can be a type of "Office/Other" location. Or a lab can exist in either a Data Center, IDF, or an MDF room. It's based on how the wiring is constructed.

Therefore, it's important to understand all of the computer room locations and how everything is wired. This is information gathered during the requirements phase that makes a difference in defining what the design will eventually look like.

For example, let's focus with a simple LAN design. If there was one computer room location like an MDF wiring closet, then the LAN topology could either be a LAN Collapsed Core or a LAN Core with a LAN Access layer. A LAN Collapsed Core would be a better choice.

However, let's say there is an IDF room where all Office/User/Computer locations are wired to. And the IDF is connected to an MDF room. Well we automatically know that the LAN topology for this design, at a minimum, would be a LAN Core with a LAN Access. The LAN Core would exist in the MDF and the LAN Access would exist in the IDF.

This information is important and is used during the design process when building the actual topology of the foundation solutions (e.g. LAN, WAN, Data Center, Internet Edge).

5	Business Size

This part can be confusing among IT people who can create some debate, but ultimately it's not really a big issue. The question that comes up is "what is considered as a small network, a medium network, and a large network in terms of the number of users".

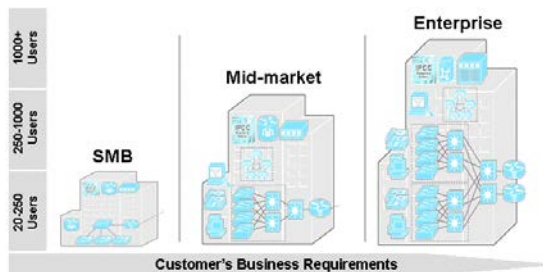
I have seen many different numbers for each business size even among Cisco engineers.

Server administrators and consultants view small, medium, and large differently also.

For example, some Microsoft Consultants say that a small network is between 1-50 users. A Medium size network is between 50-250 users. And a large network is 250+.

Well, in the networking world, up to 250 users is Small or SMB. 1000+ users is typically a large network.

The picture below reflects the business size more accurately based on user count:



Additional Business Sizes: SOHO (up to 10 nodes), Small (10 – 48 nodes)

Now business size alone doesn't mean that is it. It still comes down to the overall requirements gathered.

But first, why is knowing the business size important for a network design? It's used as a good baseline for what product models to get for a particular solution and not going overboard. It's a good reference point to start out with. For example, the Cisco ASA 5505 firewall is recommended for Small sized networks (around 20-50 users). Therefore, we can start with a Cisco ASA 5505 for Small network sized clients.

However, the requirements may require hardware that is not marketed for small networks, maybe for larger networks. For example, a Microsoft Gold Partner that has about 30 employees was looking for a new phone system. Based on the business size they would be a Small/SMB. The Cisco CallManager Express (CME) solution would easily support this client based on their business size. However, they had SIP requirements that wasn't supported on Cisco CME (at the time), so we deployed the Cisco Unified CM 5 solution (suited for larger networks) to meet their technical requirements.

We will show the process for how you can determine the best hardware for a solution in a design. It's very clever and accommodates those two points.

Design

We have been talking about IT in the real world not being perfect and may have many unique elements involved. Therefore, why introduce a process for doing a network design if those factors are the case. Simple! IEEE was established to provide a structure for technologies that vendors can follow. For example, 802.1Q is an industry standard protocol used for carrying multiple VLAN tags across a single physical interface. It allows a structure with a set of rules and concepts that different vendors like Cisco, Juniper, and Foundry can follow making it possible to extend VLANs between them.

This is where the Design Cookbook and its general purpose come into play, but for network design. The main purpose of the Design Cookbook is to provide a structured and organized system for designing a network and understanding the real world conditions involved.

In the IT world today, there are many whitepapers, books, websites that discuss best practices but it's incomplete and doesn't discuss the big picture of the network. I think every IT person agrees on the idea of implementing best practices. They want to improve what their servers or network is doing for easier administration and support. But it's difficult to understand what to follow or where to go. For example, in a Cisco SRND document many years ago, Cisco recommended that OSPF neighbor timers be tuned to 1 second for the hello timer and 3 seconds for the dead timer. That's great, but many other recommended numbers started showing up to say 2 seconds, 3 seconds, and so forth.

Or what percentage number to use for storm control on switches. For many years network engineers have ask me these questions on what is recommended.

You will often see statements in books or websites saying the following: *"These values will vary depending on your environment and traffic conditions"*.

This statement doesn't answer any questions in terms of what values should be used. What information did the author use to come up with those numbers, what was the size of the environment, what the traffic conditions are, or how many routes exist. No baseline of information were given, so there are many engineer's struggling trying to determine what to do for the best intentions for configuring their network. This creates the challenges seen in all networks today.

There is no structure or standard for engineers to create a "close-to" perfect network with best practices in mind. This idea is possible and AutoQoS is an example of that. I personally knew one of the individuals responsible for the development of this feature to simplify QoS configuration and provide best practices without the confusion of what we should do.

You input one syntax on a switch port based on what is connected (e.g. IP Phone and Desktop) and everything is preconfigured following best practices. With the release of AutoQoS I get very few questions on how to deploy QoS correctly and what is recommended.

There are other examples, but engineers like a standard of something they can follow for doing things correctly and what is recommended.

The purpose of this Design Cookbook is to provide that structure and system for designing a network aware of many real life conditions.

The design process in a nutshell consist of the following steps:

- 1) Requirements
- 2) Solutions
- 3) Services
- 4) Hardware
- 5) Design Options

First, we gather all the necessary business & technical requirements including any expectations.

From the gathered requirements we determine what solutions (Foundation Solutions and Network Solutions) are applicable for our design. These solutions can be a LAN, WAN, Remote Access, to Unified Computing.

Next we determine what services such as routing or switching will reside on top of our solutions including any best practices.

With the solutions and services in our design we determine the hardware for each component in the design.

The ultimate design may be presented as multiple options that will list the hardware components, estimated pricing, and other recommendations.

We will explain this entire design process and the resources that can be used in this Design Cookbook.

The Design Cookbook is applicable for Small, SMB, Medium, and Large size Enterprise networks. It is not applicable or ideal for the following:

- Service Provider Networks
- System Infrastructure Designs (Microsoft, Linux, Mac)
- Application Design (Database)
- Management Process
- Information Security Policy

The design process will be updated to consider these type of networks and solutions in the future, which will still follow the same general design structure.

But, the network design can be referenced for all other IT solutions in general.

The design cookbook is a work in progress because again everything in IT changes. New services, solutions, and hardware devices are always being released or updated.

The design process has been constructed to consider these aspects, so the focus of the design process is really with the structure itself.

What do we mean by "structure"? This would be the process network engineers or consultants would follow for building a recommended network using various components along the way.

New solutions, services, and hardware are constantly evolving over the years like Cloud Computing or new hardware devices like the Cisco ISR2 1900 series. These are components that are being added, updated, or removed over a period of time.

The structure never changes, the components within the process are updated to reflect current trends and conditions for "todays" or "next-generation" networks.

5

Design Options

When you go through the design process you may come out with multiple network designs that may be presented to a client or management team. They will choose the design based on their own criteria and what is important. That criteria may involve additional questions to validate what their decision will be.

The main point behind this is to not get caught up with "how" they make their decision. A high percent for that decision will be based on the overall cost and recurring costs. It makes sense, but understanding the budgetary considerations provides better insight with their expectations.

For example, I completed a network design for a client that required high 10-Gigabit Ethernet port capacity and replacing all End of Life (EoL) hardware. 80% of their hardware was EoL, so new hardware was needed to support their requirements. The design process would be focused around those requirements that is asked by the business.

Doing that the design involved the Cisco Nexus 7000, 5000, and 2000 series switches. The estimated cost was over a million. They almost panicked and wanted to discuss this further. This later resulted in the business realizing that their requirements were not realistic and that their eyes were bigger than their stomach. They didn't need high 10-Gigabit Ethernet support and could still utilize their existing hardware. So their requirements were redefined.

This is the real world of design that happens all the time and no book or certification like the CCDE (or the expensive CCA) will teach you about these scenarios. Budget is a huge component for how the design is constructed. Regardless of these redefined business and technical requirements, the network architect must present a set of design options to the table.

Here is a summary for the type of design options that can be presented:

- **Design with Hardware Consolidation:** a design where the hardware and solutions in the design can be consolidated together.
- **Design without Hardware Consolidation:** a design where the hardware is not consolidated with other components. It could have consist of existing hardware or service providers that was determined during the requirements phase.
- **Design based on Technical Objectives:** a design heavily focused around the technical objectives.
- **Design based on Preferences:** a design focused around a specific preference by the decision maker and/or architect.

These preferences can consist of the following:

- Hardware Preference
- Configuration Interface (e.g. CLI, GUI)
- Protocols and Technologies that are used
- Support Model
- Unique Elements

Providing options shows the business that multiple designs are possible. It allows them to see the differences along with any pros and cons for each option.

When a network design is being built always ask yourself or others this simple question. Who is the primary architect? That decision will make the difference if a design is not ideal, but it makes sense to the primary architect.

It's recommended that the network designer be the primary architect for a design to consider the big picture on how it is designed with best practices in mind. They can easily follow the design process outlined in this cookbook.

A network designer playing the secondary architect role may encounter design challenges and most of it is due to the preferences set by the primary architect.

Let me provide an example when primary and secondary architects are involved. Let's say you are a Microsoft Consultant, your preferences will likely be towards Microsoft solutions and products. But it also means you are designing like a system engineer and not as a network architect. The Microsoft consultant may prefer deploying SonicWALL firewalls for the Internet Edge and using Linksys Business Class switches for the LAN. This is what they have done many times for their clients and feel more comfortable with that design, deploying it, and supporting it.

However, one of the solutions that is required to be added to the design is Voice over IP (VoIP). The Microsoft consultant is not comfortable with that design, deployment, or support for such a solution. What does he/she do in this case? Like many consultants they will bring in another consultant/engineer to handle the design for the Voice solution. This would be the secondary architect providing a solution for one part of the network design.

Well here is the tricky part, when deploying a Voice Solution it's recommended that it be converged with the data network on the LAN. So, we need switches to support 802.1Q, VLAN, QoS, and PoE to power the phones. The Microsoft Consultant never dealt with those protocols on the Linksys switch before and presented a challenge for that person to support it.

The primary architect preference may either accept what is being proposed because it is recommended or to build this voice network separately. This happens to be a true story where I was the secondary architect in this engagement responsible for the design of a Voice solution. Based on the preferences and the support model, I designed a completely separate network just for the voice network that would connect into the LAN because they were using MS Exchange 2007 UM for Messaging services. This was not a recommended design, but was ideally designed separately in its own island.

These type of scenarios and architect roles will come up like this. I been on many design projects where as a secondary architect, the primary architect trusted the recommendations made and updated the design to accommodate that. But there were other cases where the primary architect had their preferences on what the design would look like and only wanted my involvement on the solution that was sought after.

These preferences may be related to a wide number of things such as:

- Hardware Preference
- Configuration Interface (e.g. CLI, GUI)
- Protocols, Technologies used
- Support Model

I worked in an environment where one client DID NOT want to implement any VLANs, STP, or anything Layer 2 on their network. This gave me a quick impression that he/she had a bad experience with L2 in the past like with a broadcast storm bringing down the entire network. And from that experience they have never used L2 services again. That is a good example of preferences that will exist for primary architects and what secondary architects need to be aware of.

Keep these in mind and always try to engage designs as the primary architect. If you are engaged as a secondary architect present a design option that would include a recommended design for all solutions for further awareness and consideration.

When you go through the design process you can present a couple of design options back to the client or IT management team. Now here is the big question they will ask. From the list of design options, which one would you recommend.

From the design options you need to choose one design that you would recommend based on your professional criteria. This will likely be based on your experience and preferences for that ultimate decision.

This selection will define what is most important to you in a network design. For example, when I do network designs I emphasis on the following areas:

- Consolidation
- Simplicity
- Flexibility

Consolidation: I believe that consolidating solutions together helps to provide simplicity and a single solution. For most of my designs I consolidate the firewall services into the Edge router allowing myself and my team to manage a single device instead of two devices (Firewall and the Edge Router).

Simplicity: Just keep it nice and simple. If the requirements call for implementing VLANs or MPLS configure the configuration needed for that solution. Configuring additional timers or additional options brings complexity and a component for troubleshooting that can be difficult to determine. Configure what is necessary, but still allow best practices to be configured where needed. Some designs or existing environments may configure tricky routing mechanisms providing a lot of complexity. When I gather the requirements and understand what is needed then the routing can be configured in a simplified manner. Don't just configure things to be complicated because you think it should be.

Flexibility: I like to deploy a design that will always consider other solutions and services that may be added in the future. Even though it was not outlined in the requirements. For example, I completed a LAN design that involved VLANs, 802.1Q, and QoS. Within 3 months a new design requirement was added for deploying IPv6. No problem, with the current hardware based on the design we easily implemented IPv6 in a recommended fashion without any impact to the original design. This is an example of providing flexibility with additional services and solutions to a design.

Therefore, you need to determine what areas you mainly focus on for proposing a recommended design among other multiple design options available. This may include specific hardware solutions like using SonicWALL for Network Security or preferences for implementing Layer 2 or Layer 3 on the LAN or Data Center network.

Either way choose a design option that you as the network engineer recommend for the client or IT management to consider.

It will be very rare that the network you design is new meaning a new building or new equipment. It will be rare, but it does happen and doing it right makes all the difference. I have been involved with many new designs for clients where I followed the same design process to construct a recommended design.

For example, we had a new client opening a new business in a new building. Great opportunity to design and deploy the network correctly. During the design process we tried to accommodate all areas of the technical objectives to avoid future challenges. This design included LAN, Internet Edge, and Voice solutions

All areas were considered and deployed in the design with the exception of reliability and the support model (network management).

The support model was on an "as-needed bases" with some type of escalation. The company didn't want to incur any cost for hiring IT employees' only consultants. They also didn't want any redundancy within the design due to costs.

The complete solution offering was offered to the client for consideration.

After two years the main voice system was experiencing problems and impacting their voice services. There was no redundancy and resulted in long hours of downtime to fix the issues. This is an example of challenges with one or more of the technical objectives focused on reliability. This is what most networks will face and it all starts from the decisions made at the beginning for which design to deploy.

This is extremely common and assessing what technical objectives are met and not met. Most technical objectives not addressed usually involve some type of reason pointing back to costs or other unique conditions.

"New" can also mean implementing a new solution like Voice into an existing network. It's important to understand from the business what existing components can be reused and if it is required or optional to be included into the design.

What about existing networks? That depends on what your engagement is with that existing network. Here are some examples:

- 1) Are we doing an assessment to provide how the network can be redesigned to a recommended design
- 2) Replacing a solution or a component in a solution
- 3) Migrating one solution to another solution
- 4) Adding additional services to the existing network and/or solutions
- 5) Downgrade a solution or network topology

So how can the design process work with existing networks? Treat the existing network as one of the requirements that is gathered. We know how it is configured, the services involved, and the solutions involved. Plus we can communicate with the client, business owners, or IT management staff on their requirements and expectations. Most of this will likely be accomplished with a site survey.

When you gather all of the requirements, go through the design process to determine what the recommended design "should" look like for the existing network. Those design options can be presented back to the client or IT management team presented in a network assessment document. I do this type of work often and in many cases responsible for executing the redesign to the recommended design proposed.

This process works whether a solution is being replaced, migrated, downgraded, or adding services like IPv6. Go through the design process with those considerations to determine what the recommended design "should" look like.

9	Other Networks

A network may consist of one or more components not necessarily seen anywhere else, but they exist due to requirements by the business.

In essence it is a network that really mirrors an existing solution, but with a unique use.

For example, one environment I have seen had a separate network that was dedicated for business partners like Bank America and Reuters. They managed their own routers and connections into those devices using a T1 or dial-in connection. This network was called a Business Partner network. This unique network connected into an Internet edge firewall separated from the internal network. That is solution that is not necessarily referenced anywhere we have seen before. So how does this fit into our design?

We look at what this "Business Partner Network" resembles from other known solutions and we determine it is really a DMZ solution which it is a network that provides services for the untrusted network connected into a firewall infrastructure. Therefore, our Business Partner network is a type of DMZ network. So it should be considered as a DMZ in our design following the same best practices, but labeled as an "OTHER" solution.

Another example is using a DSL network for users or guests to access the Internet. This is simply another type of Internet Edge Solution added to our network.

During the design process when we start selecting applicable solutions, if there is a unique solution required determine what the "OTHER" solution is based upon and use that in the design process.

A network engineer is a person who works in a company that reports to an individual in IT Management receiving a recurring paycheck from the company.

A network consultant is a person who works directly with another company that works with either the network engineer and/or IT management team. The consultant bills their time for all work effort and projects spent with the client.

What is considered billable or non-billable will vary from consultant to consultant. In general any work effort that provides "value" to the client is billable. So how does a network design fit into this model for what is billable or non-billable. If you are a network engineer they can simply build a network design following the design process.

As a consultant the approach is different and will depend on the situation. Under normal cases, a consultant is hired to do a network assessment to determine how the existing network is configured and what is recommended. This is the best case to use the design process. Remember an existing network is considered as a component in our requirements gathering for knowing what solutions exists, what services exist, and what hardware components are used. This provides great information for going through the design process and building what recommended design options are available. This is considered as a billable work effort.

However, what about cases where a client is seeking a proposal for a solution. This is where things gets tricky, because a proposal is not billable work effort, but you do want to provide some value to the proposal. Many consultants starting out don't know about this and is trying to build their business by getting clients. Basically they have no anchor, which is a big client keeping the company afloat in terms of profitability. If a smaller client leaves or if a proposal for a new project doesn't go anywhere that is ok because you have your anchor. Most smaller consulting groups don't really have that.

Therefore, many consultants starting out may provide a full design in a proposal spending long hours with no result. So, what do you do if a client is seeking a proposal for a new voice solution. Here is what you can do. For the proposal whether it is an RFP (Request for Proposal), details sent in an email, or maybe a phone call, these are considered as the business & technical requirements. If you can get more details, based on some of the requirement questions available in this cookbook, then that will provide additional information to work with.

With the requirements and determining the solutions applicable for the design, internally go through the design process to building a couple of design options. You can present either 3 or maybe just a single design option back to the client.

So what's actually being presented? With the single (or three) design option, list all the hardware and the total cost in a quote/proposal. You may have a simple write-up that may list basic pros, cons, and considerations. If you want to provide a type of graphic include a sample or example graphic in a general context. Or you can create a simple VISIO diagram for the best design option.

This is what many consulting companies with years of experience are doing. Providing the hardware for the solution a client is after and providing the total cost. If a design is needed with all the details associated with it then that would be billable work effort.

Furthermore, most cases a company who is seeking a proposal may be doing a "bid", meaning they are sending their requirements to multiple IT consulting companies then they will determine which company they will work with. This

determination is based on whatever criteria that company is using, but most of the time it is directly related to "low cost" factors.

Sometimes during a proposal or bid, a consulting group may ask the client to view what proposals they have received to either validate, improve, or to lower costs. It's important to understand that this can happen and the chances of "you" winning a bid is very low to none. That is why many consulting companies including myself do not spend long hours on a proposal write-up. But it does depend on the project and the opportunity it could create. Either way it depends on the time the consultant wants to spend.

As a consultant I rarely get engaged with bids. I focus around clients who are after consulting groups that can provide professional value to their network based on our experience and credentials.

The design process is a structured system that can be used by engineers and consultants to design a network ideally with best practices and the technical objectives in mind.

The design cookbook also provides awareness of how IT decisions fit in the real world and how a network can be designed with those components. It also provides awareness to business owners and IT management staff of the importance of designing an ideal network including the consequences if it is not done correctly.

They hold the key for what their network will become. If the network can be designed correctly then following the design process will help consider all aspects for the network. If the network cannot be designed ideally due to costs or consultant/business/management preferences then the design options should still be presented for considerations, but aware of the potential consequences.

The Engineer's Recommendation defines what you stand for and what a good network design is, based on your experience and preferences among the design options available.

You understand how networks can be designed and why they are not perfect. The bottom line is when you go into a network (new or existing) gather what requirements you can.

Whether it is from an RFP, communicating with the business, to gathering details through a site survey on the existing network.

From there you can go through the design process and the resources presented in the design cookbook.

Then present the design options to the business and/or decision makers with your recommendations.

Again these design options presented that may consist of the following:

- Design with Hardware Consolidation (Recommended Design Option)
- Design without Hardware Consolidation
- Design based on Technical Objectives
- Design based on Preferences

For each design option it may include pros, cons, and consequences.

The decision maker will make their determination based on their own internal criteria for which option to move forward on, if any.

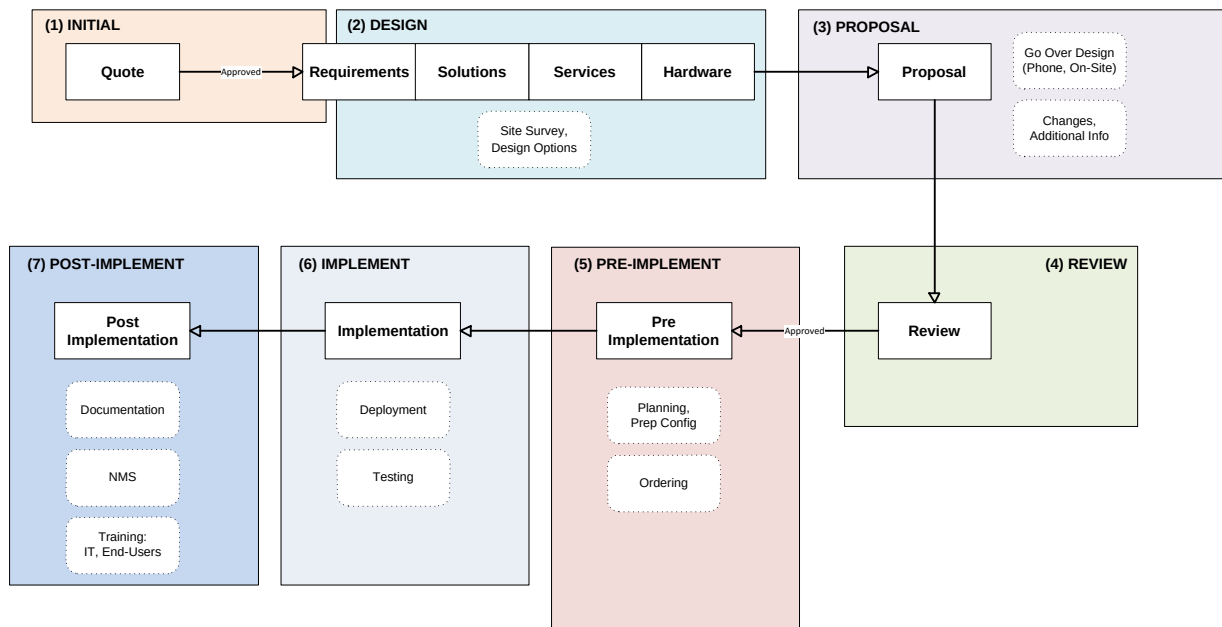
So you can see why IT is not perfect, but as engineers or consultants, we choose the clients we want to work with and who understands the importance of building an ideal design.

Many of my consulting clients believe in that. When I worked in companies in the past, that was my primary reason for leaving the organization. The IT Management staff never truly believed in a recommended design or doing things with structure. They were not comfortable with new technologies or changes. But their actions lead to higher costs and serious challenges to the technical objectives. Resulting in being reactive and spending more money at the end. The design was built based on Preferences by the decision makers, which was the IT management staff. We had to continue to provide support Band-Aids and other methods to accommodate the preferences of the decision makers.

Forming my own consulting company and officially writing the design cookbook originates from what I experienced with my past employment and various consulting environments. And to provide recommended solutions for clients who believe in those principles. This cookbook guide provides that structure for building a network design ideally and keeping what is important nice and simple along the way.

3 Design Process

When a network design starts, a process begins and a series of steps occur. This design guide is focused on the “Design Steps” shown here in this general process.



Let's discuss each of these phases shown in the design process:

1. **Initial Phase:** This is the first phase of the design process. This is where your manager or group within your company initially approaches you that they need a particular solution deployed. Or it can be a company going to a consulting group (e.g. RouteHub) for deploying a solution. In this case they want to obtain a quote to determine the cost for the consulting group to complete a network design aligning with the requirements, present a network design diagram, and the equipment that will be used. If the client does not want to pay for a network design, simply complete the network design internally (using this design guide) without the details (e.g. Subnets, Standards, Services, etc.), but only include the hardware for that design into the quote. Any details of a design would be billable work effort that should be communicated.
2. **Design Phase:** If the quote is approved then you start designing the network. This is where the design guide comes into play for building the design in a series of steps shown in the next section. In a nutshell the design phase involves gathering the requirements, building the solutions that are needed (e.g. LAN, Virtualization), the network services that will be used on the network (e.g. Routing, Switching, MPLS), and determining the hardware for each component in the design. During this process a site-survey to understand the environment may be needed. At the end multiple design options can be presented to the client/management team with a single solution being recommended by the engineer or consultant.
3. **Proposal Phase:** In the next phase, the recommended design option(s) are put together into a document and given to the client/management team. They will look over it and will usually require you, the engineer or consultant, to go over the proposed network design for better understanding or justification. This may be done by email, phone, or on-site. A presentation may be required. Changes may occur where the initial requirements could have changed due to costs and/or what they really need. Or gathering additional information for the client/management team to use for further consideration.
4. **Review Phase:** In this phase it is up to the decision makers (the client and/or management team) for how they want to proceed with the cost outlined in the proposal to other considerations. It's very common that a

proposed design is not approved due to cost. If it is approved then the design process continues to the next phase.

5. **Pre-Implementation Phase:** Once the project has been approved all of the hardware, software, and services are ordered. This could take a few days to potentially 30-40+ days if a new Service Provider is included in the design. During this phase all planning for deploying the design occurs including preparing the configuration to racking and cabling the equipment where applicable.
6. **Implementation Phase:** In this phase you start configuring (unless already configured) and deploying the solution into the production network. After deployment, testing is done to confirm access to services such as Email or Active Directory. Once everything is configured correctly save the configuration and get a backup.
7. **Post-Implementation Phase:** In the last phase various operations may occur after the network is deployed. Documentation may be put together such as Network Diagrams, troubleshooting documents, to inventory lists. You may setup and add the network components into NMS for monitoring the faults and performance if it is part of the scope. Training with the IT staff or end-users can occur at this phase depending on the solution deployed.

4 Design Steps

Step #1: Requirements

In the first step of the design process you will gather all of the general and technical requirements for the design. This will help to understand the business size, the solutions, and services that will be used. It will also determine the level of redundancy, performance, and flexibility desired by the company. **WHERE TO GO:** Go to the section *"5 Requirements"*.

Step #2: General Design

Once the requirements has been determined, you will begin with the general design which is focused on the building, the rooms, and wiring where the network equipment will exist. It will also provide standards to follow for the Data Center, Naming, IP Addressing, to VLAN schemas among others. The General Design will follow the technical objective categories to show what objective is being focused on. **WHERE TO GO:** Go to the section *"6 General Design"*.

Step #3: Solutions

In the third step, for all the solutions determined during the requirements phase (step 1) you will complete the design steps listed for each solution based on the technical objectives listed. **WHERE TO GO:** Go to the section *"7 Solutions"*.

Step #4: Services

Once the solution design and the hardware was been determined, the next step is to complete the design for all services selected from all previous steps based on the technical objectives. **WHERE TO GO:** Go to the section *"8 Services"*.

Step #5: Design Options

The final step is to construct multiple design options that can include consolidation, redundancy, different hardware, and/or topologies selecting one of those as your "recommended" option as an engineer. **WHERE TO GO:** Go to the section *"9 Design Options"*.

5 Requirements

The first step in the design process is to gather all of the requirements that will be used for the network design. These are the general requirements to understand the business requirements, expectations, and any challenges involved. The technical requirements is used to understand the technical objectives that should be considered to the type of traffic that will be used on the network. Then determining all solutions and services that will be used. Follow the steps listed below to get started:

Step 1	General Requirements

Determine the business requirements by asking the business owners (and/or engineers) some of the following general questions.

1. What are the business requirements and expectations?
2. What are the current challenges experienced today?
3. What kind of traffic and services will be used?
4. Are there any budgetary considerations?
5. Are there any existing conditions to consider? (e.g. hardware, providers)
6. What is the current support model? (how is your network supported)
7. Are there any preferences (good or bad)?
8. Who is the primary architect for the network design (if applicable)?
9. What is the business size for the network (e.g. Small, SMB, Medium, Large)
10. What is the number of remote locations? (HQ office? Branch office?)
11. What is the number of users for each location? (Note: what is the business size)
12. What is the number of computer rooms in each building?
13. What is the timeframe for completing this design and/or deployment?

After the general questions are completed additional tasks may be needed in order to build the network design by understanding what the business currently has today and how it is setup. It may include one or more of the following:

1. Gather Contact Information
2. Obtain Current Network Documentation (e.g. Network Diagram)
3. Conduct Site Survey (if applicable or approved) for the following:
 - a. Current Design Topology
 - b. Locations (e.g. MDF, IDF, Data Center)
 - c. Existing Conditions (e.g. Hardware, Providers)
 - d. Current configuration on the network
 - e. Challenges and/or Issues
 - f. Performance Measurement
 - g. Wireless: Wireless AP Coverage (if a Wireless Solution is needed)

Step 2	Technical Requirements

Once the general requirement questions have been determined it's important to discuss the critical technical objectives for the design and deployment. Most issues and challenges with a network today are due to the result of lack or no consideration for the technical objectives.

Please ask the relevant questions below to understand the technical objectives needed for the design which will also provide awareness for what should be considered.

Technical Objectives:

Questions	Technical Objective
What kind of performance and data volume is expected on the network including out to the Internet? What is the expected throughput required? What kind of traffic will be used?	Performance
Failures on a network will occur, therefore, what would be the impact to your business if a failure occurred on the network for many hours (4+)? What would be the length of downtime that could cause an impact? Note: if an outage/failure causes a business impact that is greater than the cost for providing additional redundancy (e.g. hardware, secondary service providers) then implementing redundancy (partial or full) is recommended. Determine the redundancy level desired based on the following: - Full: Higher costs (double-triple), Higher redundancy, length of downtime (<1 hour to none) - Partial: moderate costs, Low redundancy, length of potential downtime (2-4+ hours) - None: no additional costs, no redundancy. Length of potential downtime (4-8+ hours)	Reliability
What applications are more critical to be up and running over other applications?	Reliability
How many users are on the network today and how many are expected to grow in the future?	Scalability
How many servers are on the network today and are expected to be added in the future?	Scalability
What is the business size for the network design based on general requirement #9.	Scalability
Are there any specific compliances (like PCI or SOX) that your company must comply with?	Security
What solutions and services are anticipated to be added in the future?	Flexibility
Who will support the network deployed and how will escalations work?	Network Management

Traffic:

Questions
What kind of traffic and services will be used? Will there be Voice and Video traffic?
Will there be low or high amount of Internet web traffic expected? (e.g. personal web-surfing, multimedia, downloads)
Will there be low or high amount of Email traffic expected? (e.g. large attachments sent)
Will there be low or high amount of traffic used for FTP, File services, or batch-related applications?
What is the expected utilization (33%, 50%, or 100%) on the network? (Note: Most will operate around 33% or less)

Other:

Questions
Applicable to the network engineer/architect for the proposed network design: Define any preferences with technologies/services used, configuration type (CLI, GUI), hardware, technical likes & dislikes?

Once the general and technical requirements are gathered, determine what solutions will be used on the network. You will see a range of questions, the solution used, and who the question should usually be asked to. For example, if we ask the business or engineer if they need Internet Access (the first question listed under Common/Basic Solutions) then we know that an Internet Edge solution will be needed for the design. That question can be asked to either the Business (B) or the Engineer (E, default for all questions).

Many of the questions you can ask may already been gathered from the requirements and expectations, therefore, go through these questions and determine which solutions based on the questions would apply for this design. Eliminate what you feel does not apply. Next if you are working with only a business person (not technical by default) then ask the questions that are bolded below. These are the most common solutions used in majority of networks. If you are working directly with a technical/engineer person you can ask them most of the questions listed to see what additional solutions may be needed outside what from has been already chosen.

Use the questions below as a reference. You do not have to ask all of these questions, but you can definitely do so if you are not sure if all the appropriate solutions are accounted for.

Required Solutions:

These are solutions that are required for the design.

Questions	Solution Used	Type
Network focused around User endpoints (e.g. desktops, printers, access points, IP Phones): Will there be desktops, printers, and servers?	LAN	B
Network focused around Server endpoints (e.g. Servers, Storage): Is there a dedicated location where server farms will exist?	Data Center	E

Recommended Solutions:

These are recommended solutions that should be strongly considered for the design.

Questions	Solution Used	Type
Monitor faults, errors, and performance on the network proactively?	Network Management	E

Common/Basic Solutions:

These are common solutions that are used and asked for a network design.

Questions	Solution/Service Used	Type
Do you need Internet Access?	Internet Edge	B
Will there be multiple sites that will need to communicate with one another?	WAN	B
Allow individual users to access the network remotely?	VPN & Remote Access	B
Protection against untrusted users, attacks, and data loss?	Firewall	B, E
Dedicated network only accessible from the outside and to protect the inside network?	DMZ & Extranet	E
Provide voice services and features?	Voice	B
Provide voicemail and Auto Attendant capabilities?	Messaging	B
Provide network services or solutions at another site if the primary location is down?	Disaster Recovery	B
Access to network resources (internally) without using Ethernet wiring/cables?	Wireless	B
User who primarily works at home and need remote access to the network?	Teleworker	B
Provide Data Loss Prevention for the network?	Data Loss Prevention	B
Provide PCI compliancy for the network?	PCI	B

Advanced Solutions:

These are advanced solutions that are usually asked by the engineer or chosen by the network architect for an enhancement to the network or solution.

Questions	Solution Used	Type
Allow small group of users to access the network remotely without using a dedicated WAN?	VPN & Remote Access	E
Protection against untrusted/abusive websites and email (like Spam messages)?	Content Security	E
Provide large number of voice calls with multiple callers on a single call?	Conferencing	B
Provide a voice help desk service with call queues?	Call Center	B
Provide advanced security for desktop computers?	Endpoint Security	E
Provide web services and advanced features like blog or RSS feeds?	Web 2.0 System Solution	B
Provide user availability for voice calls?	Presence	B
Provide video support with voice for individual users or a conference room?	Video	B
Provide web services focused on social networking?	Social Networking System Solution	B
Provide services or applications to public/private users?	Cloud Computing System Solution	B, E
Partition multiple instances (like networks) on the same physical hardware platform on the LAN or WAN?	Network Virtualization	E
Virtualize multiple servers on a physical server?	Server Virtualization System Solution	
Scale a large number of servers, disk space, and memory resources easily in your Data Center?	Unified Computing	E
Increase deployment of servers and have 200+ servers in the data center (today & expected growth)?	Unified Computing	E
Improve application performance over the WAN?	Optimization	E
Network focused on high performance, workload, 1000s of servers, and low latency? Determine the number of servers that will be used in the HPC network? Determine the bandwidth requirements per server in the HPC network? Determine the latency and oversubscription requirements in the HPC network?	HPC	E
Network based on web servers and e-commerce capabilities?	Web & E-Commerce	B
Distribute traffic between multiple servers (or sites)?	Application Delivery	E
Network focused on storage capabilities for servers?	Storage	E
Provide faster Internet access and support for caching web sites?	Proxy	E
Provide network access based on the identity of the user (considered as advanced security)?	Identity Access Control	E
Advanced protection for application traffic against threats, attacks, and malicious behavior?	Intrusion Prevention	E
Is there a technical requirement for IPv6 services?	IPv6	E
Is there a technical requirement for Multicast services?	Multicast	E
Connecting two networks together quickly over a network (e.g. Internet) using basic tunneling services?	Network Virtualization	E

At the end of this step you should have a list of solutions and services determined that will be considered for the network design.

6 General Design

In this section you will determine the locations and wiring between rooms in the building where the solutions/services will exist. The general design will also provide best practices that should be considered for the data center itself, hardware redundancy, information security practices, and standards to follow.

Step 1	Scalability for General Design

Step 1-1	Determine all the rooms in the building

Determine the rooms in the building(s) that can be any of the following:

- **IDF:** a wiring closet that is wired (fiber or copper) back to the MDF location. IDF wiring is usually patched from the user desk locations, cubicles, or office to patch-panels in the IDF room. Some IDF rooms may be wired between each other or directly to a Data Center.
- **MDF:** a wiring closet connecting to multiple IDF rooms and may be connected into a Data Center. An MDF may have Internet and WAN circuits terminated if they are extended from the MPOE.
- **Data Center:** a dedicated room that consist of servers, racks, cabinets, server patch panels, and other data center facility components. A Data Center may be wired directly to an MDF and/or IDF closets. Internet and WAN circuits could also be terminated in the Data Center if they are extended from the MPOE.
- **Lab:** similar to a Data Center, but dedicated for testing or lab devices that may be wired back to a Data Center, MDF, and/or IDF location.
- **Classroom:** a classroom location that consist of students with multiple computer stations. Either individual ports could be wired back to a MDF, IDF, or Data Center through a patch panel. Or using a single wire (or more) leading back to a MDF, IDF, or Data Center where the classroom has a dedicated switch where all computer devices connect into.
- **Other:** any other computer or wiring room consisting of network equipment not easily placed in any of the common room locations listed above.

Recommendations: a site survey may be required to determine all of the computer rooms in a building including the wiring between those rooms. These are questions that can be asked to the business and/or technical individuals who set this up.

Step 1-2	Determine the wiring between rooms

For each computer room determined from the last step, what is the wiring used between the various rooms. Also determine what media & connectors are used with the wiring:

1. **Rooms:** First, for all computer related rooms in a building, determine how the rooms are wired between each other (rooms and/or with other buildings)? What are the estimated distances between them?
2. **Media:** Next determine if fiber or copper wiring is used between these rooms which will depend on the distance. For fiber it can be either single-mode (longer distances) or multi-mode (shorter distances, but longer than copper). If wiring between the rooms is less than 100 meters (328 feet) then Ethernet can be used (copper wiring). If the wiring between rooms/buildings is between 100 meters to 3Km or 10Km (2-6 miles) use Fiber (multi-mode). If the wiring between rooms/buildings is between 30 Km or 40 Km (20-40 miles) use Fiber (single-mode).

3. **Connectors:** based on the wiring between the rooms determine the connector type that will be used for the termination (or patch panel) into that room. If using copper wiring (Ethernet) the connector will be RJ-45. If using fiber (single-mode or multi-mode) the connector will likely be ST or LC ports. They may also be SC ports based on the fiber distribution panel that is used.

Recommendations: If Ethernet wiring is used it is recommended to use CAT 6 cabling to support 1Gbps bandwidth services.

Step 1-3

Identify all of the site locations

If there are multiple locations for the network that will involve a WAN, determine all of the locations in the WAN and their type based on the following:

- **Hub** (Main Office): the main location of the network where all sites will (or may) connect to for network resources.
- **Spoke** (Remote/Branch site): a smaller location of the network that need to connect into a main office or Data Center for network resources. If voice services are used then the remote site can communicate directly with other remote sites based on the WAN connectivity deployed. Determine the number of remote sites that exist.
- **Data Center:** a location dedicated for servers accessed by users/clients in the main and remote offices. This can also be considered as a Disaster Recovery site for the remote sites and/or main office.

Step 1-4

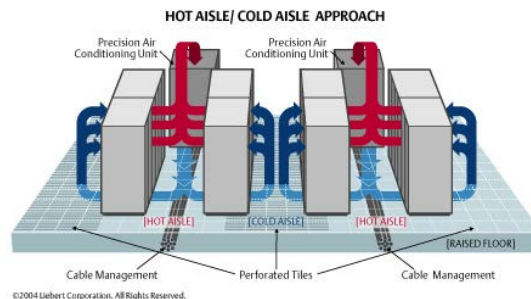
Data Center facilities

Data center facilities involves environmental (e.g. cooling, air flow, power), management (e.g. cabling, labeling), and equipment (e.g. racks, cabinets, trays) elements. These are really a design in itself, but below are best practice facility components that should be considered for any data center deployment.

- **Power:** any network equipment (e.g. routers, switches, servers) connecting into a single power circuit should never use over 75 or 78% of allocated current (amp) for that circuit as a best practice. For example, if the power circuit is a 20 amp circuit and connected is a power strip with servers, switches, and routers then the equipment's power usage should not exceed 15 amps. There are more design considerations for power listed in Step 1-6.
- **Cooling:** it is recommended to ensure proper cooling for the data center so the network equipment don't over-heat and shutdown. Some of the cooling options include: In-row cooling, overhead cooling, raised floor with underfloor cooling, and wall-mounted cooling. There are more design considerations for cooling listed in Step 1-5.
- **Racks (or Cabinet):** all equipment (routers, switches, servers, etc.) should be placed into a rack (or cabinet) that is bolted down into the floor and earthquake protected. Determine what post rack to use, most Data Center racks will be 4-post racks (42-inch deep cabinets supporting up to ~45RU) which can provide more flexibility for cable and power management.
- **Rack Mounts:** Most servers come with rack mounts that use the square hole-style vertical cabinet rails. Racks should use the square rail mounting options.
- **Cable Management:** this should be used for servers, desktops, and network connections terminated from patch panels connecting into the network switches/routers. This provides good cable management and organization in the data center.
- **Cable Tray:** this should be used between racks in the data center for clean cable management and organization.
- **Labeling:** all devices and cables should be labeled for better management and organization.
- **UPS:** critical network components (e.g. Core, Mainframe, servers, etc.) should be connected to a UPS unit in the event of a power failure. When choosing a UPS device, it's important to determine the following aspects for its selection: (1) determine the battery load it can carry and for how long. A UPS device can switch over the current load to a set of internal or external batteries if that is supported by the UPS that is used. (2) determine if

the UPS device can operate as on-line (power is filtered through the batteries all the time) or switchable (the batteries only used during a power loss).

- **Power Strips:** it's recommended to use Smart or IP enabled power strips that would connect into the network equipment. The power strips would then connect into a UPS unit. With IP enabled power strips this can allow engineers to remotely power cycle equipment when needed. Smart Power Strips have the ability to monitor the current Amps that is used for better awareness of the power usage.
- **Temperature:** must not be colder than 50 degrees Fahrenheit or hotter than 95 degrees Fahrenheit.
 - **Raise ambient temperature:** raise the room temperature in the data center.
- **Air Flow:** confirm the airflow for the hardware chosen. It can be front (intake) to back (exhaust) or right (intake) to left (exhaust), which is NEBS compliant. This is important for cooling and airflow in the Data Center which is discussed further under Hot Aisle and Cold Aisle.
 - Use **blanking panels** to maintain proper airflow for the hardware in a rack/cabinet.
 - Use **proper vent placement** and partitioning of space.
 - Standalone servers and network chassis (using vertical modules), the air flow goes front-to-back.
 - For network chassis (using horizontal modules), the air flow goes left-to-right.
- **KVM/ILO (OOB):** provide console access to server equipment if the engineer is unable to access the server directly over the network.
- **Network Hardware:** how network switches are positioned in the data center.
 - **Top-Rack Switching (every rack):** the network switches should be placed on the top of all racks in the data center (called Top-Rack Switching) where all servers in that rack connect to that top rack switch directly. This is common for larger data centers like the Facebook server farm. This is a recommended option to consider which avoids large amounts of cables being sent to one location that can have an impact with air flow and cooling. These are fixed switches that will either be 24 or 48 ports.
 - **Top-Rack Switching (every other rack):** The fixed switches can also be located in every other rack if needed which is more common for medium sized data centers.
 - **End-of-Row Switching (using a Modular Switch or Fixed switch):** Another option is to use a single modular or fixed switch located at the end of the one of the racks where all servers are cabled back to that single switch. That fixed/modular switch is then wired back to a Core or Aggregation/Distribution switch.
 - **Cisco Nexus 5000/2000 Series:** the Cisco Nexus 5000 and 2000 presents a new option that is very ideal and highly recommended. In this option fixed switches, using the Cisco Nexus 2000 series, are located in every rack (or every other rack) then wired back to a small modular switch at the beginning of the row, the Cisco Nexus 5000 series. The great thing about this option is that the fixed switches are treated as line modules in the 5000 modular switch simplifying the environment.
- **Hot Aisle / Cold Aisle:** Use Hot Aisle and Cold Aisles to achieve cooling efficiencies. Consider air flow of the equipment. What you want is cool air to flow through the intake of the equipment blowing the hot air out the exhaust and sent through the AC unit. The picture below provides a best practice on how data center air flow aisles should be designed.



Cooling within your Data Center or any server related room is strongly recommended. Otherwise some of the equipment in that room will shutdown if the temperature exceeds 95 degrees for any length of time. The ideal temperature for a server room is typically ~68 degrees. But it's also important to understand that you don't want the server room to be too cold. Otherwise, that will create a possible condensation problem when the outside air has a high level of humidity leaving moisture on the equipment.

Any electronic component will emit heat, therefore it's important to understand the amount of heat (in Watts) that each device may give off. You also need to consider other related elements that give off heat such as people. People typically give off ~100 watts of heat. Those numbers may be important if you have staff members that work inside of the Data Center or server room location for any extended period of time.

To determine the best cooling system needed for the Data Center (or server room) you need to first calculate the total wattage for all equipment in the room. Then you factor in the recommended power usage of 75%.

For example, if all of the equipment in the room is 2500 watts. That would be $2500 \times 75\%$ which would be 1,875 watts.

The AC systems will provide cooling power represented in either Tons or BTU (British Thermal Unit).

- To determine the cooling power based on Tons: $(\text{Total Wattage} \times 75\%) / 3500 = \text{Tons}$
- To determine the cooling power based on BTU it would be: $(\text{Total Wattage} \times 75\%) \times 3.41 = \text{BTU per hour}$

Back to our example, we calculated that the total wattage in our computer room was 1,875 watts. We can then calculate the cooling power based on Tons or BTU needed in that computer room.

- Cooling Power based on Tons: $1875 \text{ watts} / 3500 = \sim 0.54 \text{ tons}$
- Cooling Power based on BTU: $1875 \text{ watts} \times 3.41 = \sim 6394 \text{ BTU}$

Therefore, we can consider a power cooling system that can support those cooling requirements. There is a portable air conditioner unit by KwiKool that supports cooling power up to 2 tons or 24,000 BTU (picture below).



Those numbers fall well within our cooling power requirements and recommendations. However, it's always important to factor scalability if additional equipment will be added in the Data Center (or server room) over time.

It's important to understand the total power (in watts) that will be used for all network and computer/server equipment. As mentioned in the General Design, the equipment should be plugged into a power circuit not exceeding the total of 75% as a best practice. This includes if you are using a UPS for power backup with your critical devices. You can determine the total wattage by calculating the Wattage from all devices. You can typically get this info from the power adapter and/or documentation of the hardware you are using. You can also calculate the wattage if the voltage and Amps is provided (which you can find on the actual equipment if applicable). The formula would be: $\text{Watts} = \text{Voltage} \times \text{Amps}$

It's also important to understand what type of power circuits will be used. This will be based on the Voltage and Amps. For example, most dedicated power circuits will be 120v 20amp circuits. The total power wattage for that circuit would be 2400 watts ($120 \times 20 = 2400$). You take that calculated total and multiple it by 75% which will be 1800 watts ($2400 \times 75\% = 1800$). This means as a best practice all network/server equipment plugged into a 120v 20amp circuit should support up to 1800 watts.

Let's say we have a small data center with four servers, two small business switches, and a firewall connected to the Internet. All of these components would be plugged into a single 120v 20amp circuit. The estimated wattage for those components would be as followed:

- Server (250 watts)
- Switch (80 watts)
- Firewall (60 watts)

Doing the math that would be: $(4 \text{ servers} \times 250 \text{ watts}) + (2 \text{ switches} \times 80 \text{ watts}) + (1 \text{ firewall} \times 60 \text{ watts}) = 1220 \text{ watts}$

This would be below the recommended usage of 1800 watts for that power circuit. If the number of servers grows then a second 120v 20amp power circuit would be required.

This is how you should approach the power design for your network based on the hardware and the power circuits that will be used.

Step 2	Reliability for General Design

For any general redundancy the following best practices that can be done for any component on the network.

- **Hardware:** using redundant hardware is very common to provide hardware level redundancy. This may also include redundant line modules and Supervisor engines (CPU) depending on the model that is used.
- **Connections:** for most solutions like the LAN, Data Center, or WAN using redundant interconnections can provide fast convergence for failures including load balancing capabilities.
- **Power:** redundant power supplies, using a UPS (like APC), and connecting to different power circuits for the network equipment is critical.
- **Protocols:** the use of various network protocols like HSRP or dynamic routing protocols can provide redundancy mechanisms in its operation.
- **Software/Features:** services or features unique to the hardware model such as ISSU, which allows engineers/consultants to perform IOS upgrades without impacting the production environment.

Step 3	Security for General Design

Step 3-1	Create Security Policy

Security policies are non-technical critical components to any design to ensure that the network infrastructure is organized through documentation, maintenance, to security best practices for how the network is used. Security policies deals with security aspects with the do's and don'ts for how the network should be used and administered. This is really an extension of best practices, but more from a policy perspective that should be followed. The main reason for implementing a policy for engineers, technicians and users to follow is to lower the risks of security threats that could occur. For example, a typical Information Security (IS) policy will explain how the Internet should be used by a company which may be accompanied by a content filtering solution to enforce that policy. But with that policy in place it can avoid the issue of users going to a random website and potentially downloading something malicious that in return could infect an entire server farm resulting in an outage. Below are recommended security policies to consider with your designed network.

- **Passwords:** passwords used on the network or hosts should follow a password policy to include some of the following: A password should be complex with at least 8 characters containing special characters, numbers, and capital letters. Passwords should not be some standard word in a dictionary such as password or cat. Passwords should be changed every 60 or 90 days (maybe 30 days). And a lockout should be configured where three wrong login attempts the account is locked requiring the administrator to unlock the account.
 - **One Time Passwords (OTP):** This is also called Two-Factor Authentication. Authorizes one-time password information relayed from the access control server. OTP used to reduce brute force password attacks.
- **Physical Installation:** the critical network and server equipment should be in a secure Data Center location or locked cabinet/rack. Its recommended to implement an Electronic Access Control system for authorized access into the Data Center. Including placing security cameras to provide proactive monitoring inside and outside of the Data Center location.
- **Data Center Facilities:** its recommended to follow many of the Data Center facilities recommendations in regards to temperature and humidity control systems, UPS to cable management.

- **Information Security Training:** corporate-wide security training is recommended to all users on security best practices they should follow. This includes such topics as (1) creating and using passwords with internal systems and applications. (2) Avoiding social engineering situations which will likely happen over the phone or by e-mail. This involves a deceitful person asking a user for sensitive information (personal, company, or client) that can be used for malicious purposes later on (e.g. Identity Theft). In short, no user should hand out any sensitive information. They should obtain more information on the caller's identity, their callback number, and who authorized them to ask you for the information. (3) Phishing. This is when someone sends a deceitful email to gain sensitive information from them (e.g. credit card info, passwords, SSN, etc).

Step 3-2

Define Access Policies

It's important to determine what access should be allowed between the different networks (e.g. User, Guest, Servers). This information gathered will be used for implementing the different levels of security policies that are needed.

(1) Determine the type of access policies that will be used based on the commonly used traffic flows:

- **Direct Access from User/Guest network(s) to Internal:** this would be traffic flows that originate from a user's endpoint (e.g. computer, mobile device) to other internal networks. Determine what networks/services users should access within the network.
- **Direct Access from User/Guest network(s) to Internet:** this would be traffic flows that originate from a user's endpoint (e.g. computer, mobile device) out to the Internet. Determine what users should access out to the Internet.
- **Direct Access from Server network(s) to Internal network(s):** this would be traffic flows that originate from the server to other internal networks. Determine what networks/services the servers should access within the network.
- **Direct Access from Server network(s) to Internet:** this would be traffic flows that originate from the server out to the Internet. Determine what the servers should access out to the Internet.
- **Direct Access from Public network(s) to Internal/DMZ:** this would be traffic flows that originate from a device on the Internet into the internal network. This would be allowing access to web or mail services located on the internal network from users on the Internet.

(2) Determine how each of the different access policies will be configured based on some of the following components (*Note: not all of these components need to be used*):

- **Action:**
 - o Permit
 - o Deny
- **Source:**
 - o Based on the Network and/or IP Address
 - o Based on the Identity of the User (via Active or Passive Authentication)
 - o Based on the Web Browser (e.g. Firefox, Chrome, MSIE)
 - o Based on the System (e.g. Windows, Linux, Mac) or Mobile device (e.g. Apple, Android)
- **Destination:**
 - o Based on the Network and/or IP Address

- **Application/Service:**
 - o Based on Protocol and Port number (e.g. TCP/80 for HTTP application)
 - o Based on URL site (facebook.com) or URL Category (e.g. Social Networking)
 - o Based on Application (e.g. HTTP, Dropbox, Facebook, Webmail)
 - o Based on Micro Application (e.g. Facebook Games, Postings, Liking, Chat)
 - o Based on File Types (e.g. PDF, ZIP)

Use these access policy profiles when implementing them into the design for network security (e.g. Firewall).

For example, let's focus on the details of an access policy for "**Direct Access from User network(s) to Internet**". For that policy we would want to determine what the policy action, source, destination, and/or application/service will be. Not all of these components need to be used. In one possible scenario we may select the following:

- **Action:** Deny
- **Source:** Based on the Identity of the User = DOMAIN/USER (GROUP1)
- **Destination:** Based on URL site or category = SOCIAL NETWORKING

In this case, any AD user assigned in GROUP1 trying to access Facebook or Twitter on the Internet will be denied.

Or this could be a scenario how that policy can be configured:

- **Action:** Deny
- **Source:** Based on the Network and/or IP Address = ANY
- **Destination:** Based on the Network and/or IP Address = ANY
- **Applications/Services:** FACEBOOK/FACEBOOK GAMES

In this case, any user trying to play games on Facebook will be denied.

Network policies are non-technical critical components to any design to ensure that the network infrastructure is organized through documentation, maintenance, to security best practices for how the network is used. Network policies deals more with documentation and regular maintenance through software/hardware updates. Below are recommended network management efforts to consider with your designed network.

- **Change Control:** any configuration change that must be completed on any network component must be reviewed and approved before applying. This can lower the chance of user-made errors on a network device that can cause an outage. Having a change control process can help others to understand what changes are being made and how to revert back if necessary. The configuration change process should provide some of the following details:
 - What is the impact of the change (high, medium, low)?
 - Why is the change needed?
 - What happens if the changes doesn't occur?
 - What will be the configuration applied?
 - What is the back-out plan?
 - What is the test plan to ensure that all critical components continue to work after the change?
- **Hardware Updates:** it's important to understand what devices on your network is still covered for warranty and has not reached end-of-life. Using end-of-life non-supported hardware could lead to exploits in a security related attack or with a software bug. Confirm when each device is set to expire and plan on replacing it with current hardware to maintain support with the vendor which is strongly recommended for a production/customer-based network.
- **Software Updates:** a common security threat to a network is exploits in its software and operating system that may come up. These exploits may affect the performance to a particular service causing an outage. It's highly recommended to perform frequent software updates to keep your devices up-to-date with the latest recommended release outlined by the vendor of that device/service (e.g. Cisco, Microsoft). Remember new security threats are found every day looking for exploits to bring down critical services and/or affect sensitive data.
- **Documentation:** creating documentation and keeping it updated is very important for understanding how your network is designed. This is good for troubleshooting purposes including planning like adding a new LAN distribution or a network solution. Documentation is also important plus mandatory when a company follows a particular compliancy such as SOX or HIPPA. Below are the main documentation pieces that should be constructed for your network:
 - **Network Diagram:** create high-level and detailed-level network diagrams of the network showing the hardware model, the connections, interfaces that are used, to the IP addresses giving a good representation of what the network looks like.
 - **IP Address Management:** create a spreadsheet document or use an IP Address Management (IPM) solution to manage the IP addresses that are assigned to all IP enabled nodes. Using an IPM is strongly recommended.
 - **Contact Lists (Vendors, Providers):** create a document with a list of all vendors, contract numbers, account managers, support numbers, to circuit ID information to use for quick easy access for troubleshooting an issue that may involve one of your vendors or service providers.
- **Network Management Solutions:** this is a system solution that is strongly recommended for proactive monitoring on the network in terms of faults, performance, security, configuration, to events for easy maintenance to understand how your network is *really* performing.

Step 5	Design Aspects for General Design

Step 5-1	Services to include

Below are recommended services that should be included with the design for implementation:

- General Best Practices
- Security Best Practices

Step 5-2	Naming Standards

#1	"Component-DeviceID-Location" Naming

- **<component>**: The network device type.
- **<device-ID>**: The network device number. Important if there are multiple devices on the network.
- **<location>**: The location or city where the device is located.

Recommended: This naming standard is ideal for small and SMB networks. **Example:** "*cs01tra*" which is the Core Switch (cs01) located in Tracy (tra)

#2	"Component-DeviceID-Room-Location-State" Naming

- **<component>**: The network device type.
- **<device-ID>**: The network device number. Important if there are multiple devices on the network.
- **<room>**: The room (with room number) where the network device is located.
- **<location>**: The location or city (with building number) where the device is located.
- **<state>**: The state where the device is located.

Recommended: This naming standard is ideal for Medium and Large networks, but can also work for Small and SMB business size networks. **Example:** "*as01-idf1-sc02-ca*" would be an Access Switch (as01) in IDF1 (idf1) located in building 2 in Santa Clara (sc02) California (ca).

#3	"Client-Component-DeviceID-Location-State" Naming

- **<client>**: The client name for the device using a short acronym.
- **<component>**: The network device type.
- **<device-ID>**: The network device number. Important if there are multiple devices on the network.
- **<location>**: The location or city where the device is located.
- **<state>**: The state where the device is located.

Recommended: This naming standard is ideal for consulting groups naming network devices for a client they manage.

Example: "*rh-er01-tra-ca*" would be the Edge Router (er01) for the client RouteHub (rh) located in Tracy (tra), California (ca)

- **<location>:** Site location of the device. This would either be HQ (for headquarters), RS (for remote site), or DC (for Data Center).
- **<hardware>:** The hardware model of the device. Recommended to use some type of abbreviation.
- **<device-ID>:** The network device number. Important if there are multiple devices on the network.

Example: "HQ-FGT100D-FW01" would be the primary firewall (FW01) located at the HQ office (HQ). This firewall model would be a Fortinet FortiGate 100D NGFW (FGT100D)

- **VLAN 10-49:** Data VLANs (e.g. Desktops for Users)
- **VLAN 50-99:** Voice VLANs (e.g. IP Phones for Users)
- **VLAN 100-149:** Internal Server VLANs
- **VLAN 150-199:** External Server VLANs (e.g. DMZ)
- **VLAN 200-249:** Other VLANs (e.g. Guest, Wireless, etc.)
- **VLAN 250-254:** Management and/or Interconnection (point-to-point) VLANs

Using this VLAN schema can align with the IP Addressing schema. For example, VLAN11 (Data VLAN) could have an IP address schema of 192.168.11.0 /24.

This VLAN standard can be used for Small, SMB, Medium, and some Large size networks where applicable.

#1

"192.168.N.H" IP Schema

- **N:** Network (e.g. Data, Voice, Guest)
- **H:** Host address

Recommended: Business Size (SOHO, Small, SMB networks). No WAN solution. Common IP schema used for Small networks. **Example:** 192.168.10.0 /24 (Data Subnet).

#2

"10.X.Y.H" IP Schema

- **X:** Site Code
- **Y:** Network (e.g. Data, Voice, Guest)
- **H:** Host address

Recommended: Business Size (Medium, Large). Has a WAN solution. Common IP Schema used for SMB, Medium, and Large networks using a WAN with remote sites. **Example:** 10.1.10.0 /24 (Data Subnet used at Site 1).

#3

"172.16(x).Y.H" IP Schema

- **X:** use 16-31 (15 subnets) for Networks (e.g. Data, Voice, DMZ)
- **Y:** Site Code
- **H:** Host address

Recommended: Business Size (SMB, Medium). Has a WAN solution. **Example:** 172.17.2.0 /24 (Data Subnet (17) used at Site 2)

7 Solutions

Complete the design for each solution that were discovered during the requirements phase of the design process. These solutions will be categorized as one of the following:

- **Business Solution:** this is a solution that is used for general marketing with business related terms focusing at a high level. This is aimed at business and management individuals. A business solution will reference other solutions such as system, foundation, and/or network solutions that can be deployed on the network. An example would be Collaboration. From a business perspective it provides communication and sharing of resources among their clients and employees for great customer service/support. Well from a network or technical perspective that involves network solutions such as Voice, Messaging, and Call Center to provide Collaboration to a network.
- **System Solution:** this is a solution that is heavily focused around the actual design of the server farm that will be plugged into the network. The design is specific to the server farm and less with the network besides basic network connectivity. For example, Cloud Computing using hosted email (SaaS) is a design that may include Exchange 2013, an Active Directory infrastructure, permissions, and other details all related to the server design and not the network.
- **Network Solution:** this is a solution that will provide a service that can be used. A network solution like Voice (Unified Communications) provides a function of placing and receiving voice calls with other people for collaboration. These solutions are heavily focused around the network protocols, technologies, and mechanisms it will use.

All of the solutions are listed in alphabetical order and will include the prerequisites before completing the design steps for that solution. For example, if you want to implement Wireless into the network design:

Category: Network Solution
Prerequisite(s): LAN Solution and/or Data Center Solution

It requires completing the LAN or Data Center solution design first. This is important to ensure that all other critical components are already designed and in place. In other words, you can't put furniture into a house that isn't built yet.

For each solution, complete each step listed for the design writing down any relevant details from that step that may be used in other steps including its configuration. If there is a step that does not apply then continue on until all steps are completed. Each step will be based on the technical objectives for that solution. The table below will show the technical objectives and the color code it will use for reference:

Scalability	Reliability	Performance	Security
Management	Flexibility	Hardware	Design Aspects

To read more on the technical objectives go to "2 The Architecture of Network Design > 2.2 Components > 2 Technical Objectives" in the design cookbook.



~ Solutions ~

Application Delivery

Category: Network Solution (Data Center)

Prerequisite(s): LAN and/or Data Center Solution, Internet Edge Solution

When to use: to provide load balancing capabilities among a group of servers (using SLB/LTM) and/or multiple data center locations (using GLB/GTM).

Complete the steps below for building the design for the network solution. First, determine what type of content switching (load balancing) is required on the network:

- **Local:** Load balancing between a group of servers (e.g. web) at a local site.
- **Global:** Load balancing between sites in the event a site goes down or local load balancing resources are exceeded.

Step 1

Scalability for Application Delivery Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

- **Server Load Balance (SLB) appliance:** this component for the solution is an appliance and usually exists in a web-based solution. This component can either be deployed in-line or out-of-band based on the following on how the appliance will be used:
 - *Hardware-based Local Load Balancing:* this component is typically deployed in-line between the server farm that require load balancing and with the Internet edge (or any other front-end facing solution).
 - *Software-based Local Load Balancing:* this component(s) are servers enabled with a load balancing protocol (e.g. NLB), so they are connected to the server farm or the Core switch.
- **Global Load Balance (GLB) appliance:** this component for the solution is an appliance that requires the use of a local hardware load balancer. This component is usually connected on the Internet edge close to the local load balancer(s).
- **Servers:** server systems that host the same type of content like a web server farm.

Determine the following details about the application delivery environment:

- What are the total number of servers that will be used?
- How many transactions per second (TPS) are expected to the load-balanced server farm environment?

This information is important to determine the appropriate hardware to use based on the TPS it can support.

Choose the type of local load balancing that will be used.

- **Hardware:** A load balancing solution that uses a hardware appliance to perform load balancing services. Recommended and ideal for medium to large networks to load balance between a large group of servers (and fast). The Cisco CSS or ACE module/appliance including the Barracuda Load Balancing appliance can provide hardware-based load balancing.
- **Software:** A load balancing solution that uses a service on a server like Microsoft's Network Load Balancer (NLB). Common for a small number of servers ideal for small or SMB networks mainly due to the cost, however, NLB has load balancing limitations that can affect overall performance and operations. A hardware load balancing option is strongly recommended for increased performance, scalability, and better administration. NLB can support up to 32 servers (advertised) using HTTP. Server hardware plays a big part of the 32 HTTP load balanced servers that can be supported.

Recommendations: Using a hardware-based load balancing solution is strongly recommended, but there are two considerations involved which (1) administration and (2) the cost.

- **Administration:** This deals with who will manage the load balancing device for configuration and troubleshooting. A network engineer may manage the load balancer device and would work closely with the server administrators and application people. Where the NLB option usually eliminates the network engineer entirely for most of the administration.
- **Cost:** This is the main reason why companies use a software-based load balancing solution; the cost is higher for a hardware option even though they are aware of the huge advantages it provides.

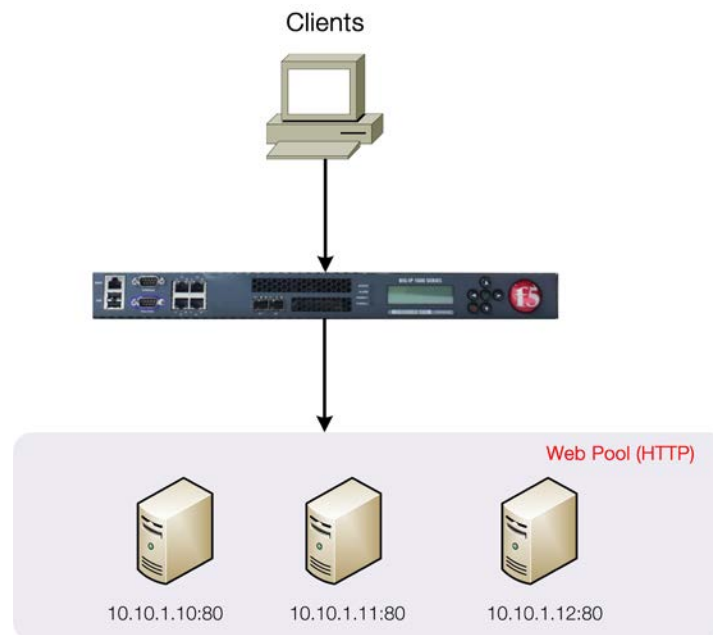
For small and SMB networks starting out, using NLB is okay with the understanding that you monitor the server resources (e.g. CPU, memory) and the number of connections. Including keeping an open mind of moving towards a hardware option in the future.

When to use: using hardware based Load-Balancer component

- **In-Line:** the SLB component uses two interfaces which is typically in-line between the server farm and the rest of the Data Center network. One interface connects to the internal (LAN) side where the load-balanced server farm exist. And the other is the external (WAN) facing side where client requests would be terminated to when accessing an application that will be load-balanced on the backend. This deployment is the most common that is used.
- **Out-of-Band:** the SLB component uses a single interface connected to the Data Center Core. This is the simplest deployment type to setup and it is not directly in the path of the traffic flow. It only receives traffic that is intended to be load balanced.

Define the different server pools (that are unique) that will be used within a server farm network in the Data Center. Within each server pool and server determine the application and ports that should be load-balanced.

Example: you may have a server pool with three web servers (TCP/80 - HTTP).

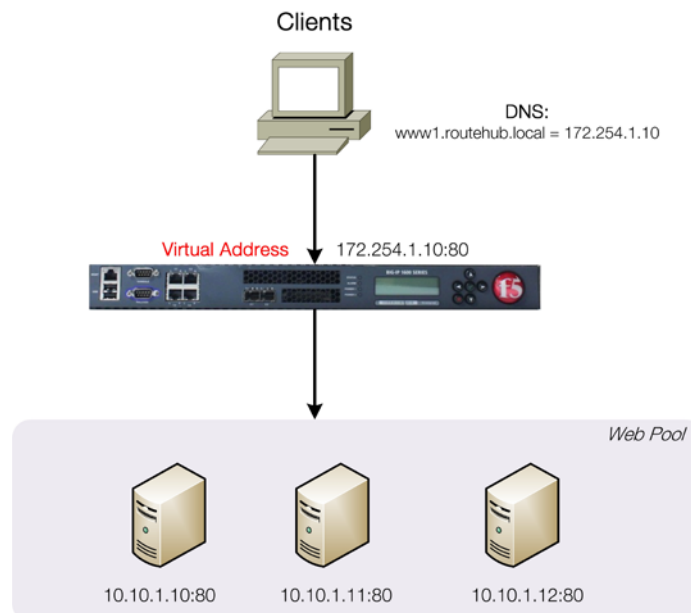


Determine how the servers within a pool will be load balanced based on the following methods:

- **Round Robin:** each new client request is sent to the next server in the pool regardless of performance or the number of connections established to that server.
- **Least Connections:** each new client request is sent to the server that has the least number of connections. If the server hardware is the same, this method is recommended to ensure an even distribution of load balancing among the servers.
- **Fastest:** each new client request is sent to the server that performs the fastest application requests.
- **Ratio:** each server is configured with a ratio or weight value. Therefore, each new client request will be sent more often to the server with the highest ratio/weight defined (or dynamically determined based on the least number of connections). This method should be used when the hardware for some servers within the pool have more resources (CPU, Memory). The high performing servers would be assigned a greater ratio/weight value compared to the lower performing servers.

For each server pool, determine the virtual address and port that will be used for how clients will access the server pool.

Example: the web server pool will be configured with a unique virtual address. Virtual address 172.254.1.10 will be associated to the web server pool.



Step 2	Reliability for Application Delivery Solution

Step 2-1	Redundancy Options

Below are some redundancy options for content switching to consider for the design.

- **Hardware:** The load balancer (LB) can be deployed in a redundant pair where one LB is active and the other is passive exchanging information (heartbeat, connection state, etc.) between the two appliances. If the primary LB fails then the second will automatically take over.
- **GLB:** Another option common for larger networks is using global load balancing (GLB) with a product like the Cisco GSS appliance. If a local load balancer should fail or if a site fails then load balancing requests can be sent to another site that has its own local load balancer available with connected servers.

Step 2-2	Health Monitors

It's recommended for each server pool to be setup with a health monitor. This would periodically monitor each server within a pool to verify if the application is working.

For example, if the HTTP services on a web server is turned off or has failed, the load balance component would put that server offline and will not use that server for load balancing within the pool. This provides reliability services for a server pool, so the client is always sent to a reliable server that is available.

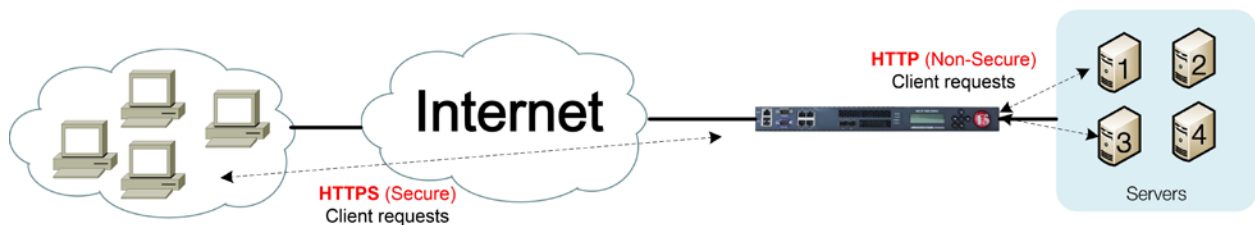
Step 3

Security for Application Delivery Solution

Step 3-1

SSL Termination and Processing

Determine if SSL termination to the virtual address (and its server pool) on the load balance component is required. In this solution, a single SSL certificate is installed on the load balancer for a virtual address, which can then load balance HTTP requests to the local servers within the pool. The web servers in the pool do not require SSL certificates unless end-to-end server-side security is required. In this case, the load balance component would build a secure SSL tunnel with the client and secure SSL tunnels with each of the servers in the pool.



Step 4

Network Management for Application Delivery Solution

The SLB and GLB components provides embedded network management and monitoring capabilities for viewing the statistics of the server pool and the connections. You can also view the logs and health monitor details performed on each server (if needed within a pool).

Step 5

Flexibility for Application Delivery Solution

Step 5-1

Integration with other solutions

Below are other solutions that are commonly deployed with the Application Delivery solution:

- Web and E-Commerce
- Server Solution

Step 6

Design Aspects for Application Delivery Solution

Below are specific design elements to complete for the solution.

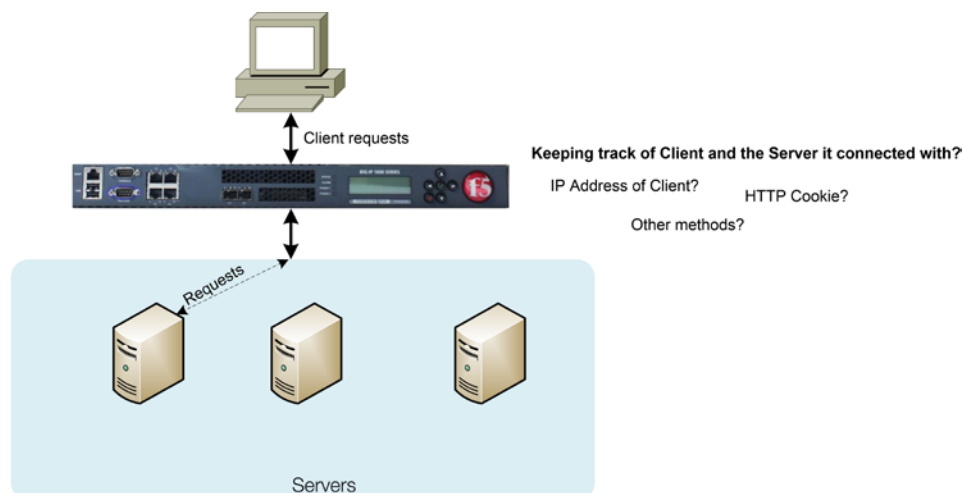
Step 6-1

Persistence

When to use: require the client to stay connected to the same server within a server pool

Persistence is the capability where the client stays connected to the same server within a pool. And to not be load-balanced to a different server. By default, every client request for a single connection will be load-balanced based on the method among the servers in the pool. Using persistence can change that behavior. Below are the common persistence types that can be setup:

- Source IP Address
- HTTP Cookies – when using a web farm



Step 7	Hardware for Application Delivery Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1	Hardware Options

Or you can select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a	Server Load Balance appliance

F5 BIG-IP 12000 *(Large)*

Performance	40-80Gbps 1GE, 10GE, 40GE support	Flexibility	--
Reliability	--	Management	Embedded
Scalability	TPS: 240,000	Security	SSL termination
Design Aspects	--		
Models	12250v Licensing		

F5 BIG-IP 10000 *(Large)*

Performance	40-84Gbps 1GE, 10GE, 40GE support	Flexibility	--
Reliability	--	Management	Embedded
Scalability	TPS: 20,000 – 42,000	Security	SSL termination
Design Aspects	--		
Models	11050, 10350v-N, 10250v, 10200v-SSL, 10050 Licensing		

F5 BIG-IP 7000 *(Medium, Large)*

Performance	20-40Gbps 1GE, 10GE support	Flexibility	--
Reliability	--	Management	Embedded
Scalability	TPS: 15,000 – 60,000	Security	SSL termination
Design Aspects	--		
Models	7250v, 7200v-SSL, 7050 Licensing		

F5 BIG-IP 5000 *(Medium)*

Performance	15-30Gbps 1GE, 10GE support	Flexibility	--
Reliability	--	Management	Embedded
Scalability	TPS: 10,000 – 21,000	Security	SSL termination
Design Aspects	--		
Models	5250v, 5200v, 5050 Licensing		

F5 BIG-IP 4000 *(Medium)*

Performance	10Gbps 1GE, 10GE support	Flexibility	--
Reliability	--	Management	Embedded
Scalability	TPS: 4,500 – 9,000	Security	SSL termination
Design Aspects	--		
Models	4200v, 4200s Licensing		

F5 BIG-IP 2000 *(SMB, Medium)*

Performance	5Gbps 1GE, 10GE support	Flexibility	--
Reliability	--	Management	Embedded
Scalability	TPS: 2,000 – 4,000	Security	SSL termination
Design Aspects	--		
Models	2200s, 2000s Licensing		

B

~ Solutions ~

Bring Your Own Device (BYOD)

Category: Business Solution
Prerequisite(s): --

Bring Your Own Device (BYOD) is a solution where a user can use their own personal devices (e.g. laptop, mobile devices like tablets or cell phones) to be used on a business network. This is similar to a guest network or wireless hot-spot where the users will gain Internet access.

This is a business solution that utilizes other network solutions to allow BYOD to operate. It includes one or more of the following solutions to be implemented on the network:

- Wireless
- Internet Edge
- Identity Access Control

A large, white, serif capital letter 'C' is centered within a dark gray rectangular box. The letter is slightly stylized with a small gap at the bottom right.

~ Solutions ~

Call Center

Category: Network Solution (Voice)
Prerequisite(s): Voice (Unified Communications) Solution

Complete the steps below for building the design for the network solution:

Step 1

Scalability for Call Center Solution

Step 1-1

Determine the components for the solution

Below are the components that exist within the solution:

1. **Contact Center server:** this is the main component for the solution that can provide call center capabilities to the Unified communication environment. This component usually connects into the LAN Core, Server Farm, or the Data Center Core/Access where the other Collaboration components exist.

Step 1-2

Choose how components will be deployed

Determine how the call center server(s) will be integrated with the phone system on the voice network:

- **Integrated with Phone System:** if the voice network has a standalone phone system that does not support call center services. The call center server(s) would be integrated with the phone system using either SIP or SCCP ports. If the call center components is Cisco Unified CCX, then it can integrate with Cisco Unified CM or Cisco Unified CM Express. This deployment method is recommended for medium/large sized networks.
- **Consolidated within Phone System:** when call center services are supported within the existing phone system. This is common for most Small/SMB voice networks with systems like Shortel, 3CX, and Allworx.

Step 1-3

Number of Agents (and Supervisors)

Determine the total number of agents and supervisors required on the voice network for the call center.

This is important to determine the correct licensing and solution to support the number of agents and supervisors needed.

When to use: using the “Integrated with Phone System” deployment type.

CTI Ports are virtual devices that integrate with a phone system (Cisco Unified CM & CME) for handling calls coming in/out of the call center. One CTI port is required for each call. Therefore, determine the following information for the call center environment:

- Maximum number of concurrent calls into the call center
- Maximum number of calls in queue

This information is important to help determine the number of CTI/IVR port licenses that are required.

Step 2	Reliability for Call Center Solution

Step 2-1	Cluster

The Call Center solution can be deployed in a cluster to provide reliability and scalability by using a **publisher server** which is setup first and using multiple **subscriber servers**.

Step 3	Performance for Call Center Solution

Step 3-1	Determine bandwidth services

Determine the bandwidth service that is required for each component for the solution. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)

Recommendations: use GE if supported and available on the LAN and/or Data Center network.

Step 4	Design Aspects for Call Center Solution

Step 4-1	Calling Queues (CSQ)

Determine the type of queues that will be implemented in the call center. They will likely be a Support queue and/or a Sales queue in a call center environment. Keep in mind that there may be multiple support/sales queues (e.g. IT support, product support, etc.) that may need to be considered.

Step 4-2	Configuration Aspects for Cisco Unified CCX

When to use: using Cisco Unified Contact Center Express for the call center server component.

The following are configuration aspects that should be implemented on the call center server component:

- **Agent Extension:** each agent should have a dedicated extension that will be part of a call center queue to receive calls.
- **Supervisor and Teams:** for each call queue, determine who would be the supervisor who would monitor the call activity for the queue. Next determine the agents that will be part of a team, covering the same queue that would be supervised.
- **Reason Codes:** its recommended to setup Reason codes which reflects the reason why an agent logs out. The recommended reason codes to setup should be: End of Shift, Break, Lunch, Meeting. For example, when an agent needs to logout of a queue, within the agent program a window would pop-up. The pop-up window would present a couple of choices which would be the reason codes. If the user selects "Lunch" then that would be recorded and can be viewed from the generated reports.
- **Resources:** each agent with its dedicated extension is created as a resource. It's important to assign the appropriate skills (e.g. support, sales) to the right agent/resource.
- **Queues:** For each call queue that is setup determine how one or more of the following will be used:
 - o **MOH, Announcement:** determine what is needed for the audio recording of the MOH files whether it is a music audio file or maybe a company announcement/advertisement.
 - o **Script:** determine how the call menu will be programmed when users call into a queue.

Step 4-3	Agent Selection Criteria

Determine how new calls should be routed to an agent within a specific CSQ based on one of the following:

- **Linear :** select agent from resource group from the top of the list then working down to the bottom.
- **Circular:** selects agent from resource group in a circular order.
- **Longest Available:** agent that has been in "ready state" the longest. This selection ensures that all calls are distributed fairly among all agents in a CSQ (Recommended).
- **Most Handled Contacts:** agent that answered the most calls.
- **Most Skilled:** agent categorized with the highest skill set. If you are offering an advanced support service for premium customers. You may want your most skilled (tier2, tier3) agents to answer new calls first before the least skilled (tier1) agents for providing premium level support.
- **Least Skilled:** agent categorized with the lowest skill set. With this selection you can have all new calls sent to tier1 support agents before they are routed to more skilled agents (tier2 support).

Step 4-4

Interactive Voice Response (IVR)

Determine if Interactive Voice Response (IVR) will be used. IVR involves recorded messages or text-to-speech in responding to caller inputs using DTMF signaling or speech within a CSQ menu tree.

Step 4-5

Services

The following services are required/recommended for the solution.

- Network Time Protocol (NTP) *required*

Step 5

Hardware for Call Center Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1

Hardware Options

Select the hardware for each component in the solution using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a

Call Center server

Cisco Unified Contact Center Express *(Small, SMB, Medium, Large)*

Performance	--	Flexibility	--
Reliability	Cluster	Management	--
Scalability	Up to 300 agents	Security	--
Design Aspects	Call Center Server		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance		

Cisco Unified Contact Center Enterprise *(Large)*

Performance	--	Flexibility	--
Reliability	Cluster	Management	--
Scalability	Unlimited number of agents	Security	--
Design Aspects	Call Center Server		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance		

Cisco Unified Communications Manager – Business Edition *(SMB, Medium)*

Performance	--	Flexibility	Messaging (CUC), Presence (IM&P), Voice & UC (CUCM)
Reliability	--	Management	--
Scalability	BE 6000: up to 100 agents	Security	--
Design Aspects	Phone System (Call Control), Voicemail, Unified Messaging (Exchange), AA, Presence Server		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance, Cisco Unified CM BE appliance		

Below is hardware options based on call duration and the number of agents on a Cisco Unified CCX MCS platform:

- **Cisco MCS-7845:** Call duration > 3 min
 - o 300 agents
 - o 32 supervisors
 - o 300 IVR ports
 - o 32 recording and monitoring sessions

- **Cisco MCS-7845:** Call duration < 3 min
 - o 150 agents
 - o 30 supervisors
 - o 300 IVR ports
 - o 30-32 recording and monitoring sessions

- **Cisco UCCX Virtual Machine:**
 - o 100 agents: 2 vCPU (900Mhz), 4GB, 146GB HD
 - o 100-300 agents: 2 vCPU (900Mhz), 4GB, 146GB HD (x2)
 - o 300-400 agents: 4 vCPU (900Mhz), 8GB, 146GB HD (x2)

Cloud Computing

Category: Business Solution
Prerequisite(s): --

Cloud Computing is a solution where hosting networks can provide a range of services and products that can be accessed over the Internet (aka Cloud). These services can be any of the following:

- **Software as a Service (SaaS):** usually an application or service (e.g. Email, Web, Conferencing) deployed within a hosted provider infrastructure connected to the Internet. Clients using a SaaS would connect to that hosted network to access the application or service provided. Cisco's solution, WebEx is considered as a SaaS providing web conferencing services.
- **Platform as a Service (PaaS):** usually a hardware device (e.g. Storage) deployed within a hosted provider infrastructure connected to the Internet. Amazon's Cloud Services (S3) is an example of a PaaS.
- **Desktop as a Service (DaaS):** this is a desktop virtual machine that exist within a virtualized environment unique for a user. For access users can remotely access their desktop from any network to launch their applications/data using a thin client system (e.g. Pano) along with software like VMware. DaaS requires VDI services and server virtualization to be configured.
- **Infrastructure as a Service (IaaS):** providing a virtualized network that can be utilized by the client. An example of this can with an isolated network within the Amazon Cloud E2 services. IaaS can also utilize advanced services such as VXLAN to provide a greater range of VLAN identifiers.

This is a business solution that utilizes other network solutions to allow Cloud Computing to operate. It includes one or more of the following solutions to be implemented on the network:

- Data Center
- Internet Edge
- Cisco WebEx (SaaS) – provide cloud-based web conferencing services
- VXLAN (IaaS) - used with an IaaS based solution to provide a greater range of VLAN identifiers for hosted networks.

The following are system solutions that are typically deployed to make up the Cloud Computing solution:

- Server Solution
- Virtualization (System)
- Storage
- Unified Computing

Below are other design resources for Cloud Computing:

1	Type of Cloud Computing

Determine the Cloud Computing solution that will be deployed on the network.

- **Public:** this is the most common type of cloud computing solution that can provide services (SaaS, PaaS) over the Internet (the Public network). There are concerns in regards to security with how the network is built and maintained by a hosting provider. This concern is addressed more with Private cloud computing since it is managed by the company itself.
- **Private:** a private network of services (SaaS, PaaS) within the cloud, but is privately accessed by an organization. It is usually built and maintained by the company itself where the services are located in a Data Center. This provides no compromise of security policies or lack of flexibility. However, a strong support model is required to maintain a Private Cloud infrastructure compared to a Public cloud solution where the hosted provider manages all aspects of the server infrastructure.

2	Cloud Management

This is more of a general recommendation to determine how the solution will be managed. What type of automated tools can help manage cloud-based tasks and managing cloud users with services on the network. This will depend on the SaaS or PaaS solution that is deployed.

3	Hardware Considerations

Below are some network products that can be deployed as a part of a Cloud Computing solution that involve other solutions such as system virtualization to cloud manage services of network appliances:

- **Cisco CSR 1000V:** virtual based router that is virtualized within a VMware ESXi server.
- **Cisco ASA 1000V:** virtual based firewall that is virtualized within a VMware ESXi server.
- **Cisco Nexus 1000V:** virtual based Cisco Nexus access switch that is virtualized within a VMware ESXi server.
- **Meraki Solutions:** Meraki was acquired by Cisco providing wireless access points, security appliances, and access switches that can be managed directly from the cloud consolidated in a single web interface.

Collaboration

Category: Business Solution
Prerequisite(s): --

Complete the steps below for building the solution:

Step 1

Network Solutions applicable for this Business Solution

This is a business solution which cannot be deployed directly. The solution will consist of one or more of the following network solutions that are applicable for deployment:

- Voice (Unified Communications)
- Messaging
- Conferencing
- Customer Care
- Presence
- Video

Add one or more of these solutions and reference those respective sections for the network design.

Conferencing

Category: Network Solution (Voice)

Prerequisite(s): Voice (Unified Communications) Solution

Complete the steps below for building the design for the network solution:

(1) First determine the conferencing functions required on the voice network based on the following:

- **Voice** (Audio): Standard conference call used with phones by all participants.
- **Video**: Provide video with audio for a conference call for some (or all) participants. This requires accurate bandwidth services to be in place and is the most expensive conferencing solution to be deployed out of the three options listed.
- **Web**: Capability to provide web collaboration for doing presentations or anything shown on the presenter's desktop with other users. Including the ability to share and control a desktop to any user.

Recommendations: If you are not sure which conferencing solution is needed, the most common type is simple audio/voice conference calls. Video conferencing has lot of requirements related to bandwidth and resources plus the cost can be very high (e.g. using Telepresence or using a Cisco IP phone with video capabilities). Voice conferencing is easily available within the phone system (e.g. Cisco UCM). If advanced conferencing is needed where users can easily create a conference bridge through a web interface or the capability of doing web conferencing then a solution such as Cisco MeetingPlace Express is required which would be an advanced conferencing option.

(2) Second, based on the conferencing functions needed for the voice network determine if a basic or advanced solution is needed for further design:

- **Basic**: Provide basic voice (and video) conferencing capabilities. Conference calls are built and managed directly through the IP phone endpoints. This solution is located directly on the phone system component (or Voice Gateway component). Therefore a dedicated conferencing solution is not needed and can be avoided from the design. This solution is ideal for all business size networks within low conferencing needs.
- **Advanced**: Provide voice, video, and web conferencing capabilities. A conferencing solution product is required to be deployed with the voice network. Conference calls are built and managed through a web interface from the conferencing solution (e.g. Cisco Unified MeetingPlace Express). Ideal for Medium and Large networks with high conferencing needs.

If Basic Conferencing is needed then you do not need this extra solution and it can be avoided from the design. If an advanced conferencing solution is required then continue with the remaining steps for this solution.

Step 1	Scalability for Conferencing Solution

Step 1-1	Determine the components for the solution

Determine the components for the solution:

- **Conferencing server:** this is the main component for the solution that can provide advanced conferencing to the Unified Communication environment.

Step 1-2	Choose how components will be deployed

#1	Conferencing Server

This component usually connects into the LAN Core, Server Farm, or the Data Center Core/Access where the other Collaboration components exist.

Step 1-3	Number of Conference Bridges

Determine the number of concurrent conference bridges that may occur in the voice environment.

This is important to determine the correct licensing for the conferencing hardware solution to support the number of conference bridges needed.

Step 1-4	Number of Estimated Concurrent Conference Users

Determine the anticipated number of participants per conference call that may occur.

This is important to determine the correct conferencing hardware solution to support the number of conference bridges and the number of participants per conference bridge.

Step 2	Performance for Conferencing Solution

Step 2-1	Determine bandwidth services

Determine the bandwidth service that is required for each component for the solution. Below are typical bandwidth services to choose between:

- **Fast Ethernet (100Mbps)**
- **Gigabit Ethernet (1Gbps)**

Recommendations: use GE if supported and available on the LAN and/or Data Center network.

Step 3	Design Aspects for Conferencing Solution

Step 3-1	Conference Pilot Number

Determine what pilot number(s) will be used with the solution. This is important to the phone system to know how to route conference calls. It's recommended to follow a type of extension schema scoped out from the Voice network design.

Step 4	Hardware for Conferencing Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Matrix Table Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1	Hardware Matrix Table Options

Select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a	Conferencing Server

Cisco MeetingPlace Express *(Small, SMB, Medium)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	20-200 users	Security	--
Design Aspects	Conferencing Server (Voice, Video, Web)		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance		

Cisco Unified MeetingPlace *(Medium, Large)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	960-1152 users	Security	--
Design Aspects	Conferencing Server (Voice, Video, Web)		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance		

Content Security

Category: Network Solution (Security)
Prerequisite(s): Internet Edge Solution

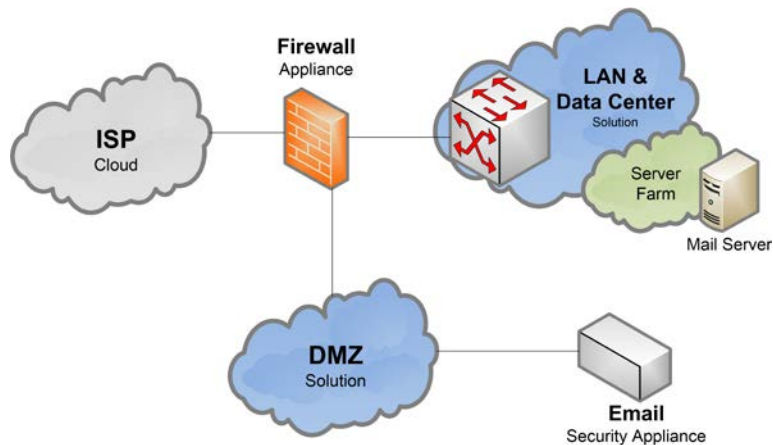
Complete the steps below for building the design for the network solution. First, determine the content security solution(s) that will be used on the network:

- **Email:** this security solution provides protection for the email infrastructure filtering against unsolicited (spam) and malicious email.
- **Web:** this security solution provides filtering of inappropriate web sites and web content on the Internet.

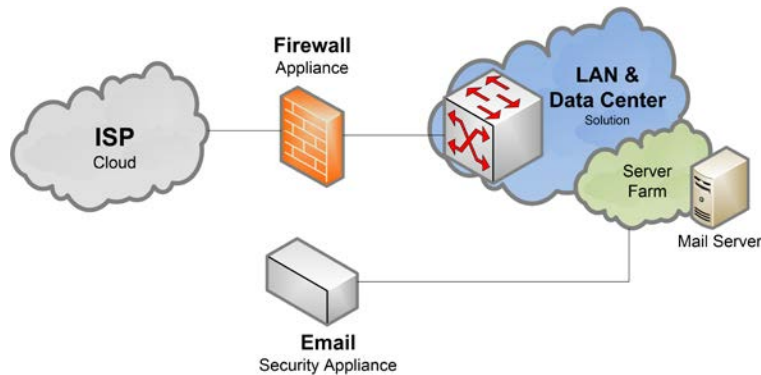
Recommendations: Both are recommended to provide Data Loss Prevention, but it will come down to whether it is required. Using either one of these content security solutions will require additional hardware, software, recurring subscriptions, and resources (maybe training) to manage the solutions. However, those overall costs are low and will provide an additional layer of security with your network including stopping internet abuse, spam, and viruses.

The Email Security Appliance (ESA) is the main component in this solution that provides protection for the email infrastructure filtering against unsolicited (spam) and malicious email. Determine how the ESA component will be deployed based on the following:

1. **DMZ** - the ESA can be plugged in a dedicated DMZ network that connects directly into the Firewall component or a DMZ VLAN that connects into a firewall interface. This is the most common deployment option and recommended.



2. **Server Farm** - the ESA component plugs into the Server Farm VLAN that exist on the LAN or Data Center.

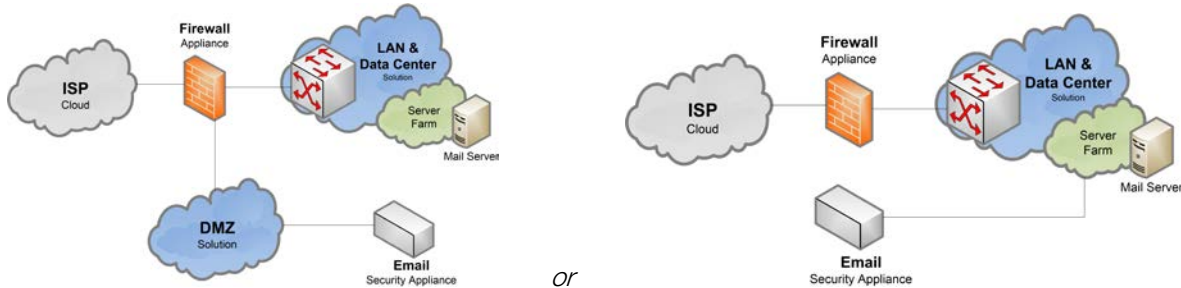


Step-2

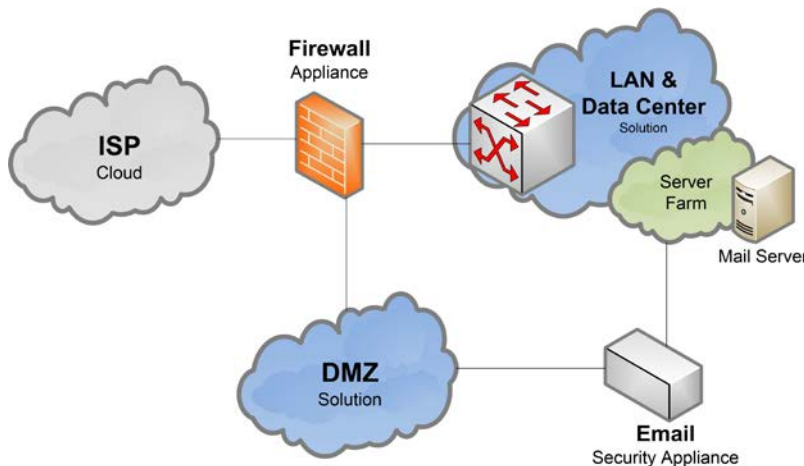
Determine interface deployment

Determine how the ESA interfaces will be deployed based on the following options:

1. **Single Interface** - the ESA component uses a single interface to filter email to and from the internal mail server. This option is more common for Small and SMB sized networks with minimal email traffic usage.



2. **Two Interfaces** - on the ESA component, one of the interfaces (the external facing interface) deals with email transfer and filter to/from the Internet. Where the second interface on the ESA component transfers emails and to/from the internal mail server. This option typically happens when the external facing interface of the ESA connects into the DMZ and the internal facing interface connects directly into the server farm where the internal farm exist. This option is recommended for SMB, Medium, and Large size networks with higher email traffic usage.

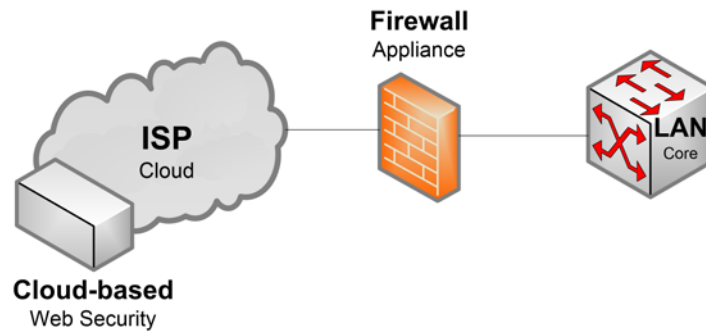


Determine which Web Security deployment will be used on the existing network based on the following options:

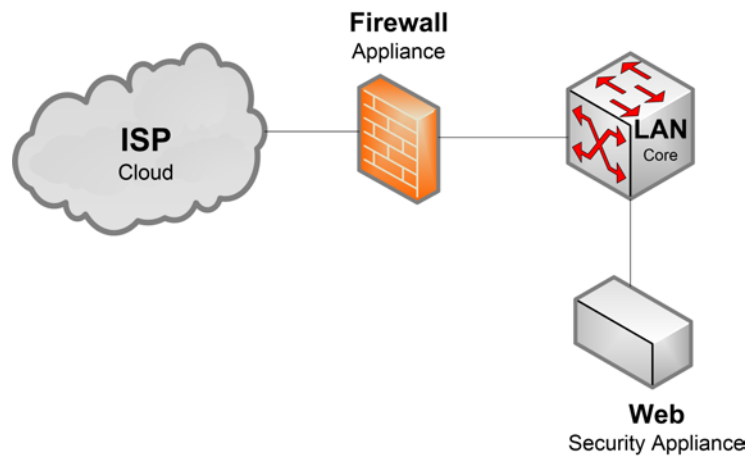
#1

Cloud Solution

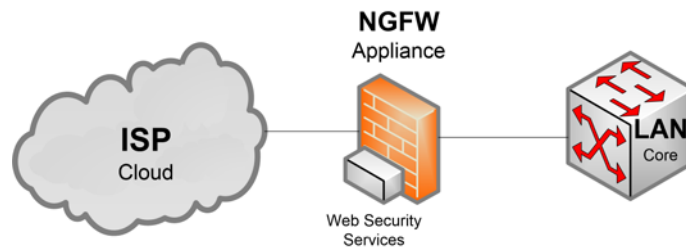
- **When to use:** (1) if you do not want to manage an on-premise web security appliance, and/or (2) if you want to enforce web filtering for connected remote-access VPN users including internal and guest wireless users.
- **Description:** This is a cloud based solution where the web filtering is redirected to a cloud service (Cisco Cloud Web Security or CWS) providing real-time dynamic web content classification.
- **Components & Deployment:** the main component utilizes a firewall appliance that supports connecting to a web filter cloud service.
- **Solution & Hardware Required:** Firewall using Cisco ASA



- **When to use:** common for large-sized networks wanting to enable web filtering services.
- **Description:** Uses a dedicated Web Security Appliance (WSA) that is plugged directly into the LAN/Data Center. The Cisco ASA firewall (or Cisco IOS router) can be configured for WCCP where any HTTP and HTTPS requests are redirected to the WSA appliance.
- **Components & Deployment:** the main component in the solution is the Web Security Appliance (WSA) which plugs directly into the LAN Core switch.
- **Services Required:** WCCP



- **When to use:** common for Small, SMB, and medium-sized networks for enabling web filtering services.
- **Description:** Next-Generation Firewall enabled for web security subscription to filter inappropriate web sites.
- **Components & Deployment:** solution enabled as a service on the Next-Generation Firewall Appliance that is connected to the Internet edge.
- **Solution Required:** Firewall (Next-Generation Firewall)



Step 2	Reliability for Content Security Solution

Step 2-1	Redundancy consideration for solution

Depending on the hardware for the component, determine the redundancy options available (if any). It will either provide Active/Passive or Active/Active Redundancy.

Active/Passive provide redundancy as a primary and secondary set. One device is active while the other device is in standby monitoring the operating conditions of the primary device and ready to transparently takeover when a failure occurs.

Active/Active provides both redundancy and load balancing operations where both devices are active.

Other options may include a **fail-open** if there is a failure. This means they will allow everything to pass through without security inspection.

Step 3

Performance for Content Security Solution

Follow the steps below to determine the bandwidth services for the Content Security solution.

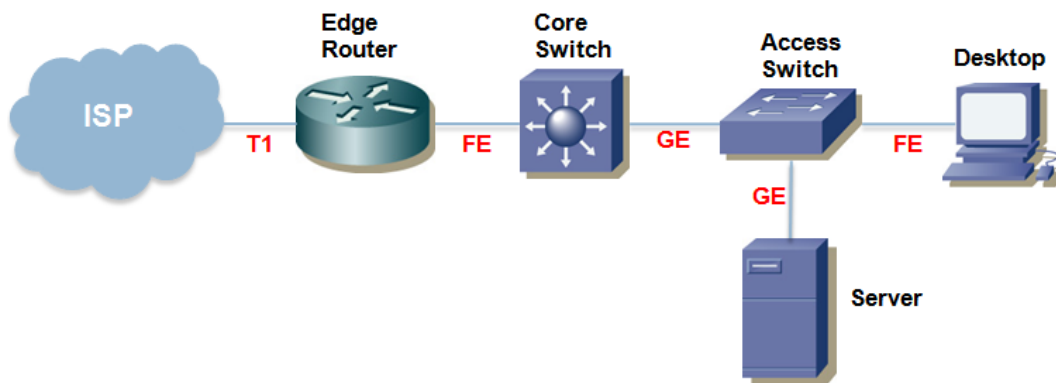
Step 3-1

Determine bandwidth services

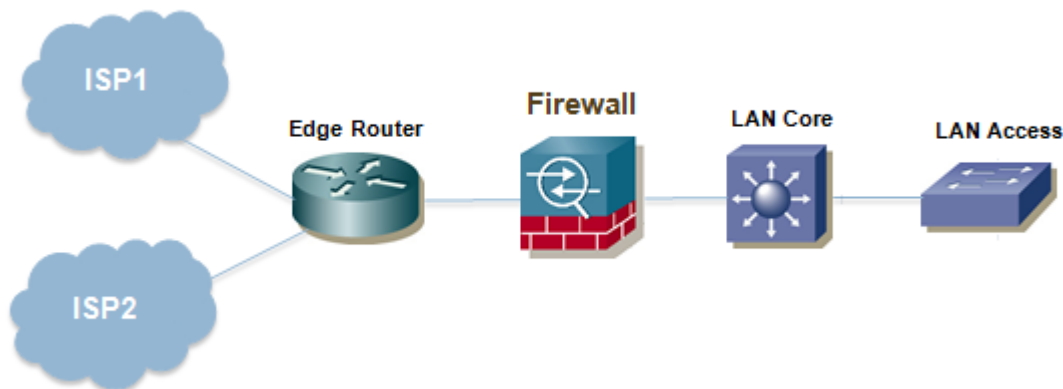
Determine the bandwidth service that is required for each component for the solution based on what exist in the topology. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)
- 10GigabitEthernet (10Gbps)

For example: below is a network design that involves two foundation solutions (LAN and Internet Edge). You will see the bandwidth identified for all connections in the design.



Now let's add the security component (e.g. Firewall, Content Security appliance) in-line between the Internet Edge router and the Core switch. The bandwidth service used between these devices is Fast Ethernet (FE). Therefore, the bandwidth services required for the security component's interfaces will also be Fast Ethernet (at a minimum).

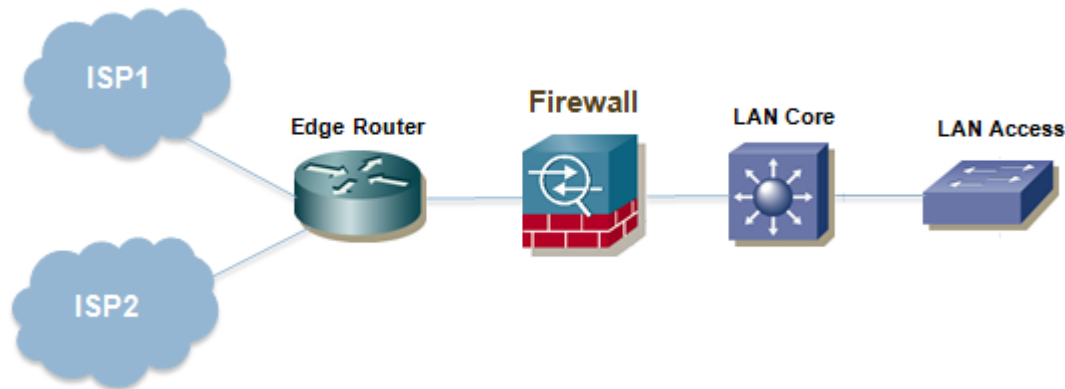


Next determine the required throughput expected through the solution component. This is based on the actual data flow and determining the lowest bandwidth service along the path. The following needs to be determined:

1. **Data Flow:** determine the expected data flow for certain services and applications through the network. For example, for Internet access the flow of data can occur from the LAN switches through the firewall, the edge router (if applicable), and out to the Internet.
2. **Bandwidth Services:** determine the bandwidth service that is used for all connections on the network along the data flow path.
3. **Lowest Bandwidth:** determine the lowest bandwidth service along the data path.

Performance (Throughput): based on the information gathered this will make up the throughput required for that in-line device. For example, if the bandwidth services on the LAN is Gigabit Ethernet (1Gbps), but the connection on the edge router is a T1 (1.544Mbps) then our expected throughput along the data path out to the Internet needs to be around 1Mbps.

Example: in the diagram below we want to determine the throughput needed on the security appliance (Firewall, Content Security):



If the bandwidth between the Edge router and the LAN Core is Fast Ethernet, then the security appliance interfaces would need to be Fast Ethernet (at a minimum). However, understanding what the performance should be for inspection is important. We might not need the security appliance to do inspection at 100Mbps. Also in the diagram let's assume that the Internet connection to ISP1 & ISP2 involves a T1 (1.544Mbps). With those details we can complete the three steps required to understand the throughput requirements for the security appliance:

1. The data flow will happen from the LAN out to the Internet (and vice versa) moving through the security appliance.
2. Along the data path, FE is used between the Edge Router and the Core switch. Let's say that GE is used between the Core and the Access switch. And a T1 is used on the Edge router's WAN facing interface up to each ISP.
3. The lowest bandwidth service along this data path is the T1 Internet connection on the edge router.

Performance (Throughput): Therefore, the required throughput through the security appliance needs to be ~1Mbps for its various security services and inspection.

Take note of the throughput requirements for the in-line device to determine the correct hardware model.

Step 4

Security for Content Security Solution

Step 4-1

Web Security

If a web security solution is chosen, determine the following for how the filtering will work:

- **Individuals:** Provide a web security policy unique for certain individuals that is different from other groups.
- **Subnets (or Groups):** Provide a web security policy for an entire subnet (or group).

This is important to understand especially when determining the product (or service) to support this requirement.

Recommendations: If you are not sure on which filtering option to use or if no requirements has been defined then all internal subnets should use an outbound Internet policy.

Step 4-2

Email Security

If an email security solution is chosen, determine the following:

#1

Mail Flow

Determine the inspection for mail flow:

- **Inbound (default):** All email messages from the Internet are inspected for spam and virus content.
- **Outbound:** All email messages from the internal mail server are routed to the email security appliance inspected for spam and virus content.

Recommendations: Inbound inspection for Anti-Spam and Anti-Virus is the default. This is recommended since we want to inspect any messages received from the untrusted network (Internet). It's also recommended to enforce outbound email flow through the email security appliance. In most environments with unmanaged laptops, users can bring them home where it could be infected with malicious content. This can then flood out spam or virus enabled email messages from the corporate network once it is plugged in.

#2

Services

Determine the email content security services required:

- **Anti-Spam:** Provide email content inspection of messages to determine if the message is clean (normal) or a potential spam message.
- **Anti-Virus:** Provide email content inspection of messages for any virus content embedded that can compromise desktop systems and spread internally.
- **Email Encryption:** provides a solution where email messages are encrypted and only the recipient of the message can open the encrypted message securely.

Recommendations: Enable both Anti-Spam and Anti-Virus services for email content inspection, which is the default for most deployments.

#3	Firewall

Implement Access Controls on the Internet Edge (inbound and outbound).

Configure a firewall policy (the firewall component) on the Internet edge allowing only SMTP from the email security appliance or from the internal mail server depending on the outbound mail flow. This can prevent users or other servers to send spam/virus enabled messages directly from your network causing congestion and potentially black-listing your mail servers.

Solutions Required: Firewall

Step 5	Network Management for Content Security Solution

There are management capabilities within the solution component that will provide reporting, logs, events, and alerts for managing/monitoring the solution proactively.

Step 6

Hardware for Content Security Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Matrix Table Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1

Hardware Consolidation Option

Some of the Content Security components can be consolidated with other components using one of the following services:

- The **Web Security appliance** component can be consolidated on the **Firewall appliance (Firewall solution)** using a security module.

Note: Reference the "Hardware Matrix Table" for any specific hardware that may be listed for consolidation.

#2

Hardware Matrix Table Options

Or you can select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a

Web Security appliance, Email Security appliance

SERIES	HW/MODEL	BUS	SER	ETH	HW
Cisco IronPort	C-Series	SM,M,L	E	F	Appliance
	S-Series	SM,M,L	W	F	Appliance
WebSense	Express	SM	W	--	Software, Appliance
	Enterprise	M,L	W	--	Software
Blue Coat	Blue Coat	M,L	W	--	Appliance
Open DNS	Open DNS	S,SM	W	--	DNS
Barracuda	Spam Filter	SM,M	E	F	Appliance
	Web Filter	SM,M	W	F	Appliance

- **SERIES:** vendor or vendor model series
- **HW/MODEL:** hardware model or line module in hardware model
- **BUS (Business size):** S (Small), SM (SMB), M (Medium), L (Large)
- **SER:** E (Email Security), W (Web Security)
- **ETH:** F (100Mbps), G (1Gbps + 100Mbps), T (10Gbps)
- **HW (Hardware model type):** Appliance, Software (on server), DNS

D

~ Solutions ~

Data Center

Category: Foundation Solution
Prerequisite(s): --

Complete the steps below for building the design for the foundation solution:

Step 1

Scalability for Data Center

Step 1-1

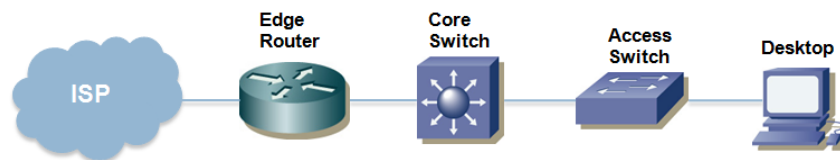
Choose a topology for the Data Center

Determine the topology for the Data Center solution. This is the actual look for what the solution will physically look like. Choose the topology that closely matches what is applicable to your environment and requirements. Below are the topology options tiers you can choose from:

1. Servers Connected to LAN Core
2. One-Tier Model
3. Two-Tier Model

The **most common tier-level topology is a two-tier** then a one-tier (mainly for the LAN and Data Center Solutions). Three-tier topologies, which are often discussed in networking textbooks are rarely used unless you have 100s to 1000s of nodes or buildings. I have seen cases where a 10,000 user environment with over 30,000 nodes was using a two-tier topology. The biggest reason for using a Two-Tier model is mainly due to cost and simplicity providing great reliability, scalability, and performance aspects.

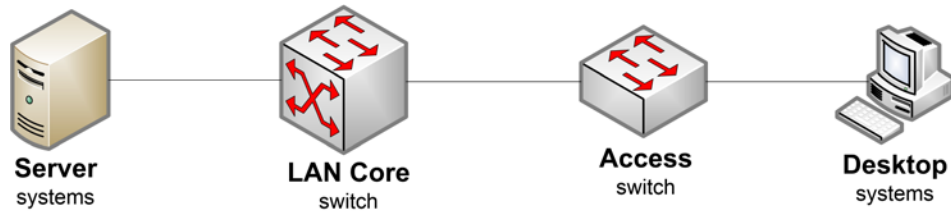
Below is an example of a network design diagram. Here it shows two foundation solutions, the LAN and the Internet Edge. The LAN is a two-tier topology consisting of a Core switch and an Access switch. The Internet Edge connects into the Core of the LAN:



#1

Servers Connected to LAN Core

In this topology option, the server farm can be connected directly into the LAN Core switch.



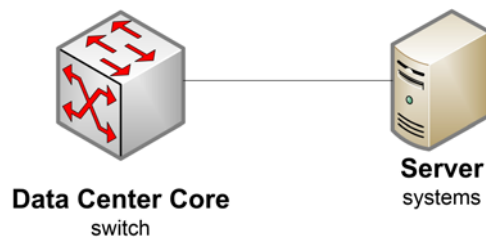
When to use:

- Business Size: Small, SMB
- When all servers will be plugged directly into the LAN Core switch.
- Common for small server farms.

#2

1-Tier Topology

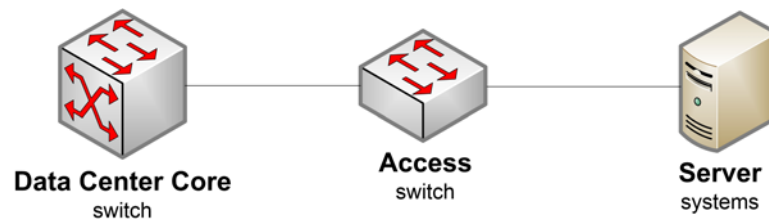
One-Tier consist of one level connecting various nodes. An example of a One-Tier topology would be a Data Center Collapsed Core.



When to use:

- Business Size: SMB, Medium, Large
- When all servers will be plugged into a dedicated Data Center/Server Farm switch.
- If the Data Center has a single row of racks
- Common for small/medium server farms

Two-Tier consist of two levels connecting to various nodes. An example of a Two-Tier topology would be a Data Center Collapsed Core connecting to a Data Center Access.



When to use:

- Business Size: Medium, Large
- When all servers will be plugged into a ToR/EoR access switch.
- If the Data Center has multiple rows of racks
- Common for large server farms
- To eliminate the 4:1 oversubscription ratio (uplink/downlink between Core and Distribution switches) used in a three-tier topology.

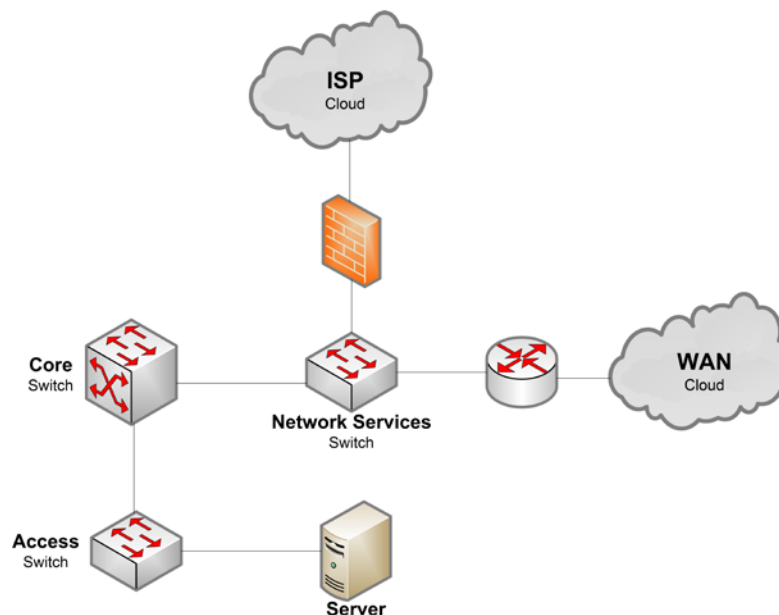
Within the topology chosen identify the components:

- Core
- Access
- Distribution/Aggregation

Here is a summary for each of these components:

- **Core:** the backbone component in the topology where all other components connect to including SAN storage components (e.g. Storage array).
- **Access:** the component in the topology that has connections to the servers and other data center type components. It has an uplink to the Core/Distribution layer switch.
- **Distribution (or Aggregation):** the component in the topology that has connections between the Core, Access layers, and SAN infrastructure (if used).

In a two-tier or three-tier topology you can add a network services branch connected off of the Data Center Core switch to provide a dedicated function. The network services switch would be dedicated for connecting the other network solutions together such as the Internet Edge, WAN, Wireless, to other network solutions keeping the Core less cluttered and organized by only aggregating between the other layers. Below is a sample topology for how the network services switch can be used in the existing topology tier that was determined for your design.



Determine how the topology will be deployment on the network. Below are the deployment types to choose between.

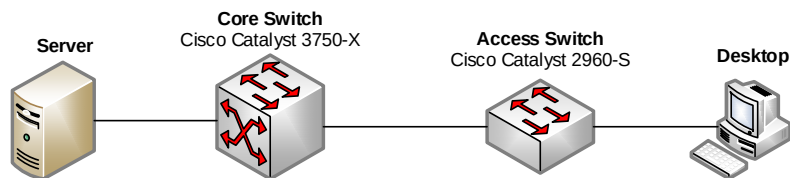
1. Traditional
2. Unified
3. Virtualized

#1

Traditional Topology

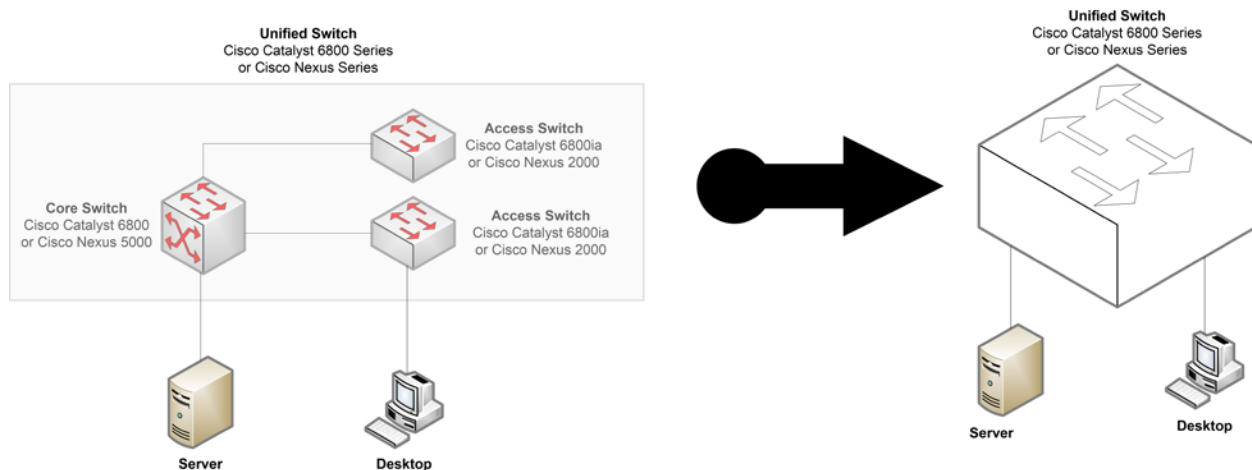
This type involves using physical standalone devices for each component in the topology. For example, let's say you have a 2-Tier topology with a Core switch and an Access switch (seen in the image below). Each of the components in the topology would be separate switch you would need to configure in the network individually. This is a legacy deployment type that is common for Small and SMB sized networks or environments using legacy hardware. Consider the following when selecting this deployment type:

- **Business** Size: Small, SMB, Medium, Large
- **Hardware** (examples): Any network hardware (e.g. Cisco Catalyst 6800, 4500, 2960).
- **Topology**: 2-Tier, 1-Tier, 3-Tier

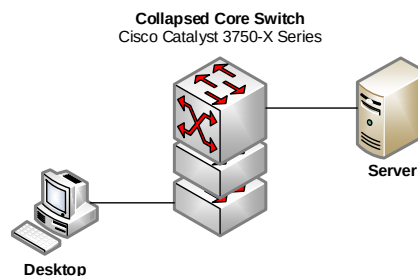


This is a next generation deployment type that deals with consolidating all of the components into the topology as one logically network component. This can be accomplished using a Chassis/Stack based switch or using the next generation unified capability. For example, let's say you have a 2-Tier topology with a Core switch and an Access switch (seen in the image below). In a Unified deployment type, the individual access switches are consolidated or treated as individual line modules to the Core switch. If we are using a 1-Tier topology (Collapsed Core) then all of the access switches are consolidated as physical line modules or bundled together on the Core switch. In either option, it would logically be seen as a single component that is unified internally. This allows the entire configuration to be done directly on the Core switch instead of each individual access switch in the environment. The Unified deployment option is recommended for Medium to Large networks running the latest hardware (e.g. Cisco Catalyst 6800, Cisco Nexus 5000 & 2000 Series). The Unified chassis/stack-based deployment option is common for Small, SMB, and some Medium sized networks using a 1-Tier topology model. Consider the following when selecting this deployment type:

- **Unified Option**
 - o **Business Size:** Medium, Large, Data Center
 - o **Hardware** (examples): Cisco Catalyst 6800/6800ia, Cisco Nexus 5000/2000
 - o **Topology:** 2-Tier, 3-Tier

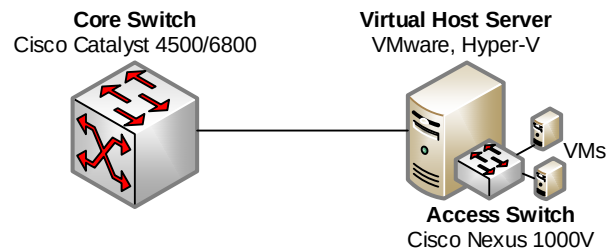


- **Chassis/Stack Option**
 - o **Business Size:** Small, SMB, Medium
 - o **Hardware** (examples): Cisco Catalyst 6800/4500 (Chassis), Cisco Catalyst 3750-X (Stack), Cisco Small Business 300 (Stack)
 - o **Topology:** 1-Tier



This type involves virtualizing one or more of the components in the topology. For example, let's say you have a 2-Tier topology with a Core switch and an Access switch (seen in the image below). The access switch can be virtualized inside of a Virtual Host Server (VMware, Hyper-V) using Cisco Nexus 1000V. The Virtual Host Server (with the virtualized access switch) would then plug directly into the physical Core switch (e.g. Cisco Catalyst 3750-X). This type is common for Medium to Large Data Centers with many Virtual Host Servers. Consider the following when selecting this deployment type:

- **Business Size:** Medium, Large, Data Center
- **Hardware** (examples): Cisco Nexus 1000V
- **Topology:** 2-Tier, 3-Tier

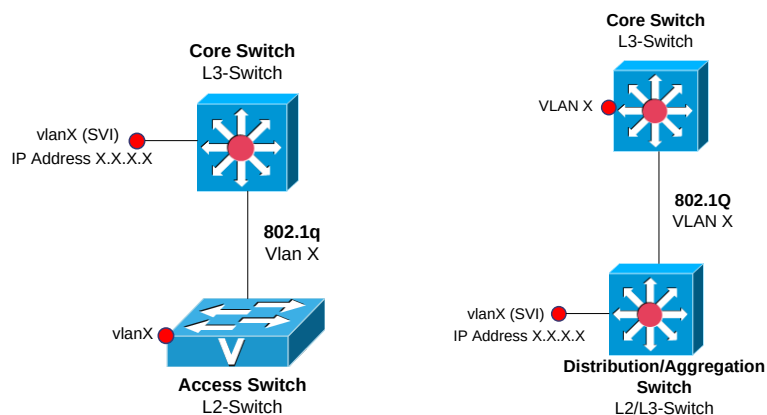


Determine the Layer 2/Layer 3 Topology you want to deploy on-top of the Data Center topology chosen earlier. Below are the topologies to choose between.

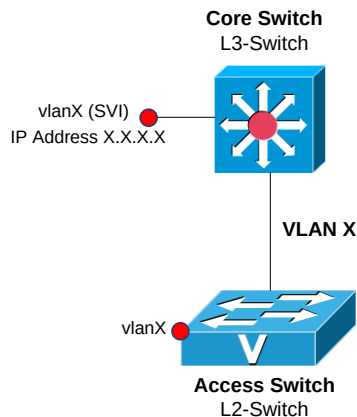
1. L3 Core/Distribution & L2 Access using 802.1Q
2. L3 Core/Distribution & L2 Access using VLAN
3. L3 Core/Distribution & L3 Access

#1

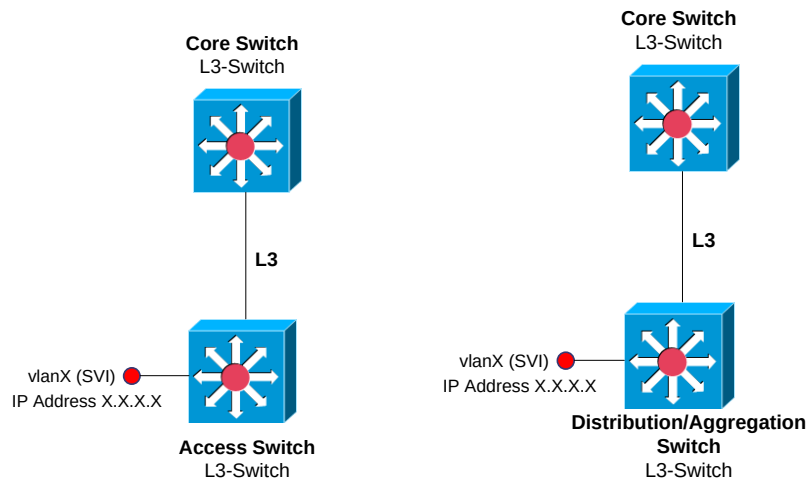
L3 Core/Distribution & L2 Access using 802.1Q



- **When to Use:** this is the most common L2/L3 topology. If VLANs will be extended across the network this is the topology model to use especially if Voice and Wireless solutions will be used. If service modules will be used at the Core (or Distribution/Aggregation) layer this topology is also required since the service modules heavily rely on VLANs for its various components.
- **Description:** In this topology, layer 2 loops will exist if using redundant hardware and links, therefore, it is required to implement the Spanning Tree Protocol. This sub-topology allows VLANs to be extended anywhere on the network.
- **Device Components:** the Core/Distribution switch in the topology would be L2/L3 device configured for routing and VLANs/802.1Q. The access switch would be a L2 device. The interconnection between these components would be an 802.1Q connection (use Trunk Security for what VLAN tags should be extended).
- **Services Required:**
 - o Routing
 - o Virtual LAN (VLAN)
 - o Trunking (802.1X)
 - o Spanning Tree Protocol



- **When to Use:** each Access layer switch exist in a single VLAN not enabled for 802.1Q Trunking not allowing multiple VLAN tags to pass. This creates more of a physical design than a logical design that can consist of multiple VLANs/networks. If you don't want VLANs to be extended across the network and/or if you are using a L2 access switch not configured for any VLANs or 802.1Q this is the L2/L3 topology to use. A single VLAN is configured on the L3 Core and the VLAN is assigned to the downlink port of the connected access switch.
- **Description:** In this topology, layer 2 loops will exist if using redundant hardware and/or links including if the configured VLAN will be extended across the L2 network. Therefore, it is required to implement the Spanning Tree Protocol. This sub-topology VLANs are not extended across the network
- **Device Components:** the Core/Distribution switch in the topology would be L2/L3 device configured for routing and VLAN assigned to ports. The access switch would be a L2 device. The interconnection between these components would be a VLAN interface with no VLAN tagging (802.1Q).
- **Services Required:**
 - o Routing
 - o Virtual LAN (VLAN)
 - o Spanning Tree Protocol



- When to Use:** this topology is mainly chosen for administration and preference reasons for avoiding L2 configuration (or minimal L2 configuration) on the network. However, using a pure L3 networks allows a better tool set (e.g. ping, traceroutes) for troubleshooting network issues and provides faster convergence over L2 services and increase of available bandwidth. It also provides a single control plane focused on L3. It's an easier implementation that doesn't require matching of STP, HSRP, or GLBP priorities. There are also no L2/L3 multicast topology inconsistencies. Using L3 allows using routing protocols like EIGRP or OSPF that can reconvergence within 200ms using sub-second timers. The down side is that VLANs cannot be extended on the network creating many limitations or flexibility. Another consideration is that a mixture of L2 and L3 services can be used on the same interface. The interface can be configured as an 802.1Q interface. One VLAN can be used for routing using EIGRP or OSPF. And the other VLANs can easily be extended across the interface where they need to go. Using this method requires using L2 services which may not be an option for consideration.
- Description:** In this topology, there are no Layer 2 loops since everything across the network is Layer 3. As a result VLANs are not extended across the network. The VLANs are confined to a single switch.
- Device Components:** all of the components are L3 devices and the interconnection between these components would be a L3 interface.
- Services Required:**
 - o Routing
 - o Virtual LAN (VLAN)

When to use: If the Data Center solution uses a two-tier topology (Core and Access layer) determine how the access switches will be deployed based on the following options:

1. Top of Rack (ToR)
2. End of Rack (EoR)

#1

Top of Rack (ToR)

An access switch is placed at the top of each rack in the data center or placed in every other rack. The servers in that rack will connect directly to the ToR switch. Each ToR switch would be connected back to the Core switch.

- **ToR utilizes Fixed Switches:** This method uses a fixed switch that is placed at the top of each rack (or every other rack) with servers directly connecting to it. This will provide lower port density resulting in more devices to manage. However, this lowers the amount of cabling used back to the Core/Distribution layer. Understanding the appropriate amount of downlink ports for the Core/Distribution node is important. This method will use many fixed switches resulting in higher spanning tree processing.
- **ToR Hardware (Examples):** Cisco Nexus 9300, Cisco Nexus 6001, Cisco Nexus 2000, Cisco Catalyst 6880ia
 - **Cisco Nexus 2000 series:** Cisco Nexus 2000 switch will plug into a Cisco Nexus 5500 switch using Fabric Extenders (FEX). It will act as a remote line card on the Cisco Nexus 5500UP switch.

Recommendations: Using Rack-based/Fixed Access switches is the most common method due to price of purchasing a fixed switch over a modular switch. Using a fixed switch at the top of racks does provide good scalability if the Core/Distribution node (recommended to be a modular hardware device) has enough ports with growth expectations. Using the Cisco Nexus 5000 and 2000 series can easily make Top Rack Switching simplified for configuration and management with non-blocking performance.

#2

End of Rack (EoR)

If there are many rows of racks, a single access switch is placed at the end of each row of racks. The servers in each rack would connect directly to the EoR switch. Each EoR switch would be connected back to the Core.

- **EoR utilizes Modular Switches:** This method uses a single chassis-based switch to feed network connections to each rack that the servers will connect to. This will provide higher port density and fewer devices to manage. However, this increases the challenges for cabling and cooling. It also provides lower spanning tree processing.
- **EoR Hardware (Examples):** Cisco Nexus 9508, Cisco Catalyst 6500/6800, Cisco Catalyst 4500

When to use: If the Data Center topology will include a storage solution (using iSCSI, Fibre Channel, Fibre Channel over Ethernet, and/or NAS).

If a storage solution will be used, stop at this point in the Data Center design process and proceed to the “Storage” Solution in the Design Cookbook (under Solutions > S > Storage).

Complete the design steps for that solution then continue with the Reliability design of the Data Center solution.

Step 2

Reliability for Data Center

Step 2-1

Choose Redundancy Model

Providing redundancy for the Data Center topology deals with making either the Core or Distribution/Aggregation components redundant based on which tier level the network is using. The Access layer is usually not redundant. Therefore, servers may be dual-homed into two separate access switches or Core switches to provide an increased level of redundancy.

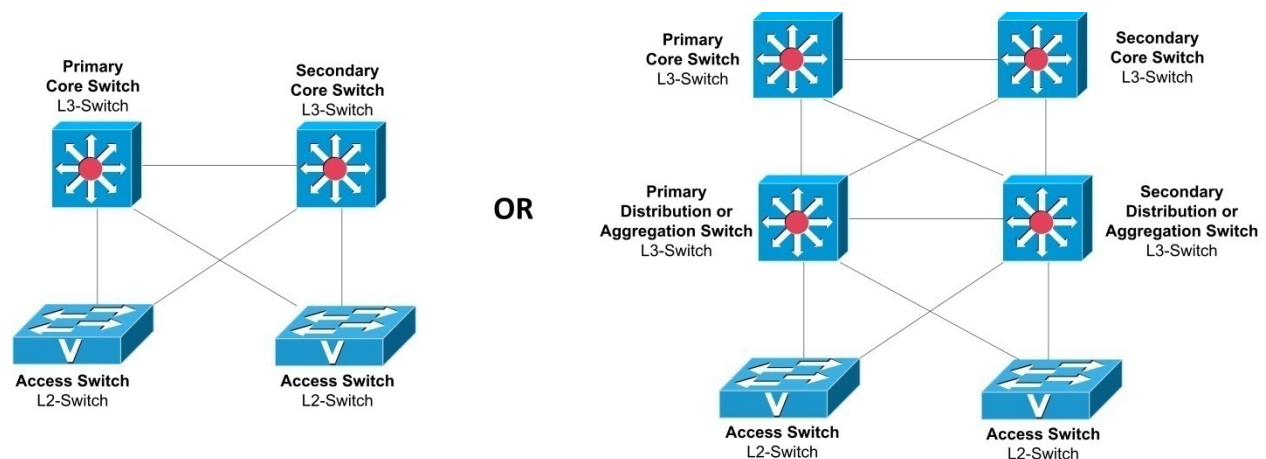
Determine which redundancy model should be used for the Data Center solution if reliability is important:

1. Traditional Redundancy
2. Resilient Redundancy

#1

Traditional Redundancy

Traditional Redundancy: this design was commonly used in the past to provide redundancy using redundant hardware for the Core/Aggregation layers. Below is what this redundancy model looks like:



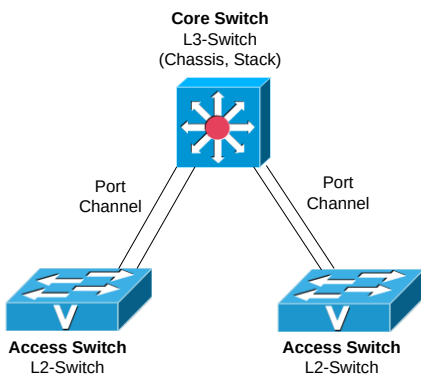
- **When to use:** using a traditional or virtualized topology for the deployment type to achieve full redundancy. This is applicable for Small, SMB, Medium, to Large business size networks.
- **Description:** in this redundancy topology, the access switches have redundant connections to a pair of redundant Core/Distribution switches. Since loops will exist in this topology, it's crucial that a Spanning Tree protocol like Rapid Spanning Tree is implemented on all L2 and L3-switch components, which will cause one of the downlink/uplink ports in the topology to be blocked. No load balancing occurs in this topology unless different root bridges per VLAN are configured on the Core/Distribution switches. It is also required that a First-Hop Redundancy Protocol is implemented that will be used by the edge devices to provide default gateway redundancy (e.g. Desktops, Servers). And all of the L3 components should be enabled routing (e.g. OSPF, EIGRP) and implemented for fast convergence.

- **Services Required:**
 - o Spanning Tree Protocol (STP)
 - o First Hop Redundancy Protocol (HSRP, VRRP, GLBP)
 - o Routing (EIGRP, OSPF, Static)

#2-1

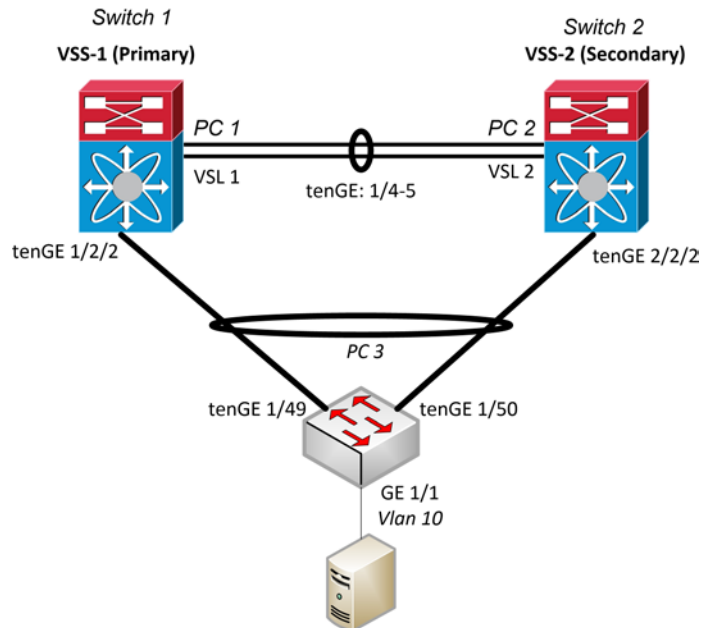
Resilient Redundancy using Unified (Chassis/Stack Option) or Traditional Deployment Types

Resilient Redundancy I: this is a new redundancy design that is ideal for next-generation networks where the Core/Aggregation layer consist of a single chassis switch or stack-based switch which includes using Port Channels with other devices. Below is what this redundancy model looks like:



- **When to use:** using a Unified (Chassis/Stack option) or Traditional topology for the deployment type to achieve redundancy. This is applicable for SMB, Medium, to Large business size networks.
- **Description:** in this redundancy topology, the Core/Aggregation layer consist of a single chassis-based switch (e.g. Cisco Catalyst 4500, 6500, 6800) or stack-based switches (e.g. Cisco Catalyst 3750-X). Port Channel can be implemented to the access switches from different line modules or stack switches on the Core/Distribution components appearing as a single logical switch from the perspective of the access switch. In this topology there are no spanning tree loops because all ports are active, but implementing Rapid STP is still recommended. Furthermore, this redundancy model doesn't require using a Default Gateway Protocol like HSRP.
- **Best Practices:**
 - o Within the stack-based switch, one of the switches operate as the master switch. The master switch should not have any uplink/downlink ports connected to it. It should be connected to the non-master switches in the stack.
 - o Set the persistent timer to "0" for the stack MAC address to ensure that the original master MAC address remains the stack MAC address after a failure has occurred.
- **Hardware Required:**
 - o Using Chassis-based (e.g. Cisco Catalyst 6800) or Stack-based hardware (e.g. Cisco Catalyst 3750-X Series).
- **Services Required:**
 - o Spanning Tree Protocol (STP)
 - o Port Channel (802.3ad)

Resilient Redundancy II: this is a new redundancy design that is ideal for next-generation networks where redundant Core/Aggregation switches are configured to act as a single logical switch that the access switches can connect to using a Port Channel connection.



- **When to use:** using a Unified (Unified option) or traditional topology for the deployment type to achieve redundancy. This is typically deployed for Medium and Large business size networks.
- **Description:** in this redundancy topology, redundant Core/Aggregation switches can be clustered together to appear as one logical switch using VSS or vPC depending on the hardware used. Port Channel can be implemented from the two redundant Core/Distribution switches to a single access switch increasing the overall availability for the connected hosts on the access switch. The access switch will assume it is connected to a single Core/Distribution switch.
- **Services Required:**
 - o Virtual Switching System (VSS) *OR* Virtual Port Channel (vPC)
 - o Port Channel (802.3ad)

Below are other services that can provide reliability and stability to the solution:

- Broadcast Suppression
- Unidirectional Link Detection (UDLD)
- Loop Guard
- NSF and SSO
- In-Service Software Upgrade (ISSU)
- Layer 2 Multi-Path (L2MP)
- Bi-Directional Forwarding Detection to improve L3 neighbor failure detection

Below is hardware redundancy considerations that can be done for any component in the topology.

- **Hardware:** using redundant hardware is very common to provide hardware level redundancy. This may also include redundant line modules and Supervisor engines (CPU). Here is a summary for what hardware can be redundant.
 - o Device/Chassis
 - o Line Modules (using a chassis model)
 - o Supervisor Modules (using Chassis model)
- **Power:** redundant power supplies, using a UPS (like APC), and connecting to different power circuits for the network equipment.

Step 3

Performance for Data Center

Determine the bandwidth service applicable for all connections and ports in our design. This section provides the resources to determine the bandwidth services and performance that will be used for the various ports in the solution. Mark this information on the network diagram for reference. This information is important when it comes time to determine the correct hardware model.

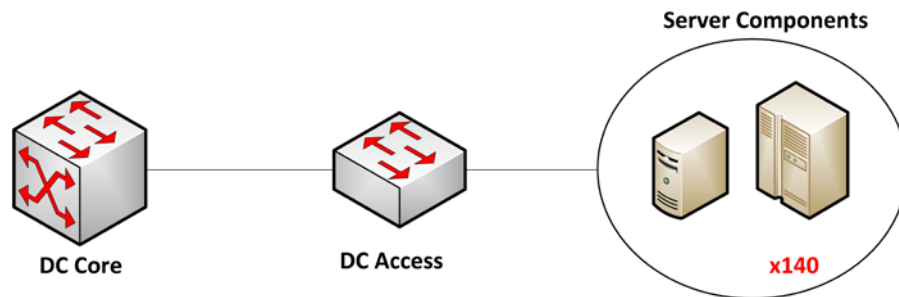
Step 3-1

Determine the number of server ports

Determine the total number of server ports that will be used in the Data Center network. The components that would plug into a server port are server components (or server systems). These components could be connected into the Data Center Core (for smaller server farms) or to the Data Center Access switches based on the topology that is used. For each server component consider the number of network/storage connections it may have:

- **Data:** Ethernet (Single NIC, Dual NIC (Teaming, Port Channel))
- **Storage:** FCoE using 10GE, FC using HBA

Example: Let's say that our Data Center design is using a 2-tier topology. The total number of server ports determined will be 140 ports connecting into the access layer (each with single NIC adapters). These servers will :



Step 3-2

Determine additional edge ports

With the total number of server ports calculated consider the following for additional ports to add to this total:

- Potential scalability of additional edge ports by adding at least 15-20% (or higher if necessary) more ports
- Potential redundancy used by network devices by adding between 10-15% more ports.

Next determine the bandwidth technology for the server ports based on the following classifications:

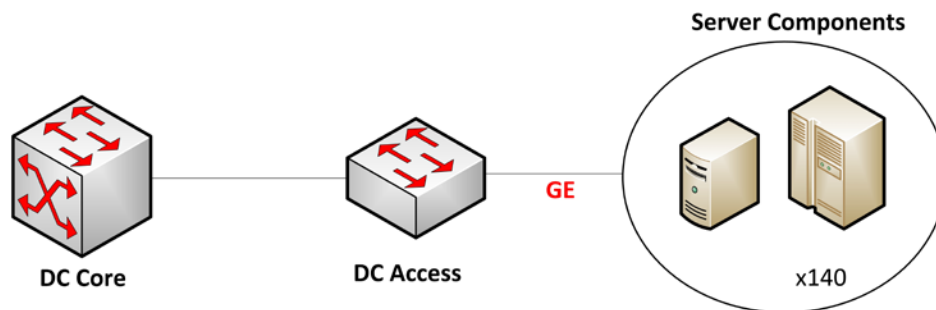
Data: If the server will be connected to an Ethernet network for all data communications with user and clients.

- **Fast Ethernet (100Mbps):** used for low-performing servers with minimal traffic or backup usage.
- **Gigabit Ethernet (1Gbps):** common bandwidth technology for most servers connected to the network. The servers may have backup or replication on the same NIC that provide data communications for users/clients.
- **10-Gigabit Ethernet (10Gbps):** used for high performing servers and for connecting to a storage network using Fibre Channel over Ethernet (FCoE). This will allow the servers to transport data traffic (using Ethernet) and storage traffic (using Fibre Channel) on the same NIC on the server.

Storage: If the server will be connected to a storage network using FCoE or Fibre Channel.

- **Fibre Channel over Ethernet (FCoE):** the server would have 10GE/FCoE adapter installed connected to a Data Center access switch. This will allow the servers to transport data traffic (using Ethernet) and storage traffic (using Fibre Channel) on the same port. If you are planning on deploying a storage network with Fibre Channel its recommended to use the Cisco Nexus 2000 Series for the Access which would connect to the Core using Fabric Extenders (FEX) providing FCoE.
- **Fibre Channel:** the server may have an HBA installed that may be connected directly into a SAN topology using Fibre Channel.
-

Example: continuing with our example, the 140 servers will use Gigabit Ethernet for the bandwidth technology.



For the bandwidth service determined for the server edge ports what media will be used:

- **Copper:** the most common and recommended media type to use for server ports when connecting computers or servers. It's recommended to use CAT6 cabling.
- **Fiber:** this is used for servers that may only support fiber NICs, but in today's networks Copper GE or 10GE (Twinax) is becoming common and recommended over using Fiber for GE/10GE unless the desktop/server is separated across a long distance that may require multi-mode or single-mode fiber connections.

Example: In our example, all of the servers will use Copper GE ports, so that will be needed for our Data Center Access switches.

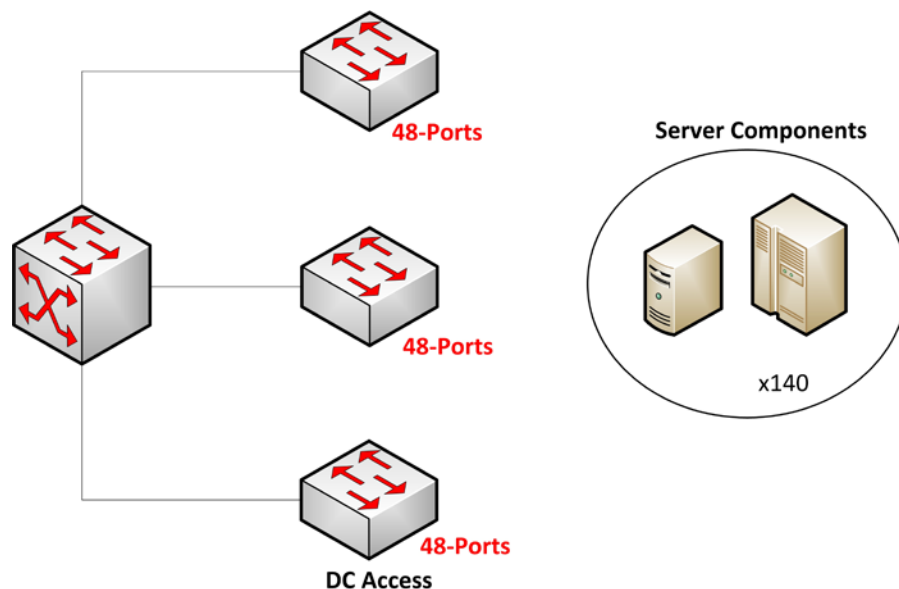
Now we need to divide the number of server ports into individual groups (or switches) for the server components based on the following increment values:

- **24 Ports:** a fixed switch that provides 24 Ethernet ports. The cost is lower, but may require many 24-Port switches to meet the edge port requirements. Hence increasing the complexities and concerns for scalability.
- **48 Ports:** a fixed switch that provides 48 Ethernet ports. The cost is higher over 24-Port switches, but may require fewer switches to meet the edge port requirements decreasing the complexities and concerns for scalability.
- **48+ Ports:** a switch that can support more than 48 Ethernet ports. A chassis-based switch or a stack-based switch can be used to provide the best number of edge ports needed. The cost is higher compared to a fixed 24 or 48 port switch, but provides a minimal (maybe just one Access switch) number of switches, providing lower complexity, higher scalability, and flexibility. This option is strongly recommended over the other switch options because it keeps a nice and simple infrastructure with minimal devices to manage.

The following considerations should be kept in mind for this selection process:

- The access switches would connect up to the Data Center Core, therefore, each port on the Core is considered as an aggregation point that needs to be considered for bandwidth.
- Consider adding additional ports for potential scalability and redundancy where needed.
- **Caution:** avoid using daisy chained switches which can cause poor performance related issues, spanning tree loops, and FHRP related issues. It is recommended to use either a chassis-based or a stack-based switch. If the LAN switches must be daisy-chained based on a unique requirement then no more than 2-3 switches should be used. In general there should be no more than 7 switches between systems on a network.

Example: we have 140 server ports. Therefore, we can use either three 48-Port switches, six 24-Port switches, or one Chassis/Stack switch. Let's focus on the 48 port switches in our example.



For the core switch, it's important to understand the total aggregate throughput for the downlink port to the connected access switch.

Remember the access switches would connect up to the Data Center Core switch, therefore, each port on the Core is considered as an aggregation point that we need to consider for its bandwidth. In general higher the bandwidth service used on the edge port, the more bandwidth is expected on the Core. But that depends on what the utilization will be. For example, many IT administrators will use Gigabit Ethernet for a server. But why is Gigabit needed and how much of that is being utilized? Most servers may use only 20% of the bandwidth (or less) through its GE interface. Rarely at 100% due to the basic operations of TCP. You may tune the TCP options to get more bandwidth, but it's not out of the box to setup easily.

To determine the expected aggregated bandwidth per access switch downlink port the following info needs to be obtained:

- **Number of Server Ports:** Determine the total number of server ports that will be used on that connected access switch, which will either be 24 ports, 48 ports, or 48+ ports.
- **Bandwidth for the Server Port:** determine the maximum bandwidth used for each server port.

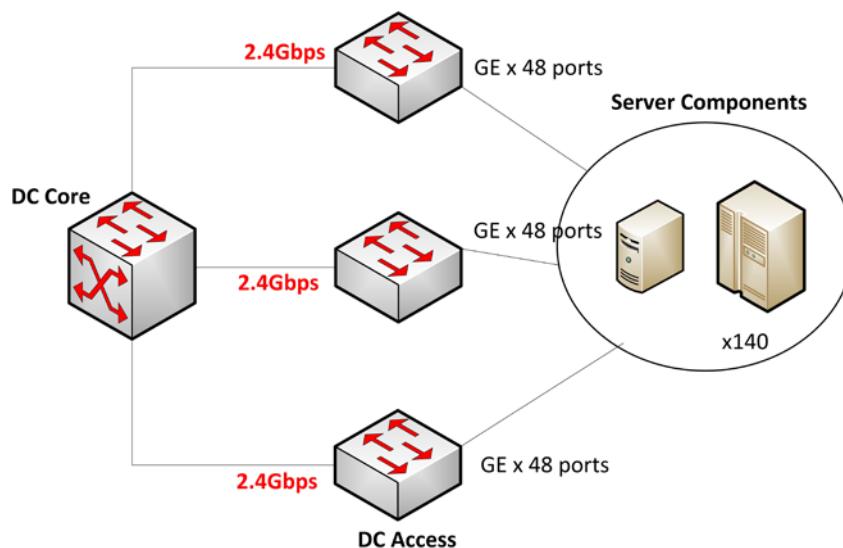
With the information gathered from the list above use the following formula to calculate the expected throughput required at each aggregated downlink port on the Core switch. The expected utilization is based on the recommended oversubscription ratio of 20:1 between the access layer and the Core/Distribution layer.

Data Center: $[(\# \text{ of Server Ports per Switch}) \times (\text{Max Bandwidth per Server Port})] / 20$

Example: continuing with our example we have 3 access switches connecting into our Core, therefore three aggregated downlink ports will exist on the Core switch. This throughput calculation would apply for each of these downlink ports. Focusing with one of these uplink/downlink ports we know the following:

- The total number of server ports is 48 because we are using a fixed switch with 48 ports.
- The maximum bandwidth used per server port will be Gigabit Ethernet (1Gbps).
- The oversubscription ratio would be 20:1

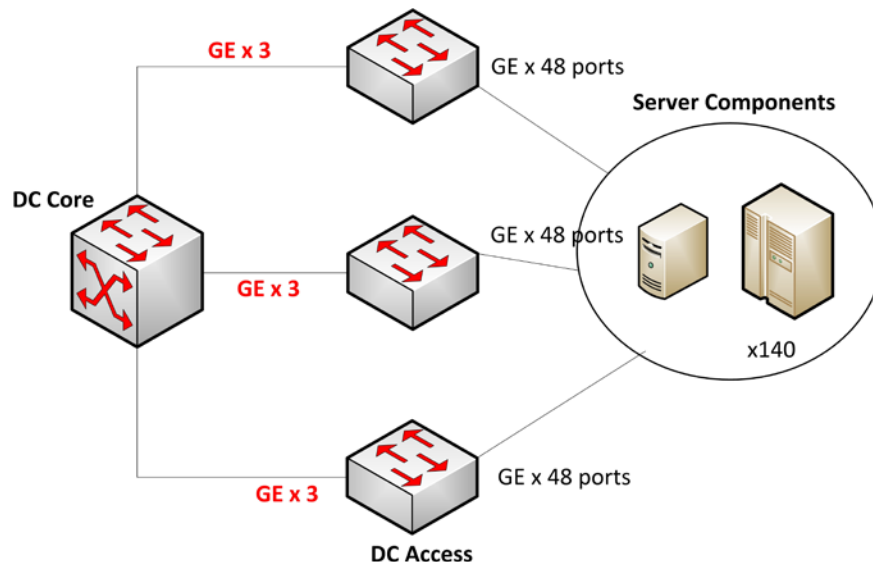
Therefore, the bandwidth for the aggregated uplink/downlink port will be 2.4Gbps $([48 \times 1\text{Gbps}] / 20 = 2.4\text{Gbps})$



With the bandwidth calculated in the previous step we can choose the appropriate bandwidth technology for that downlink port based on the following:

- **Gigabit Ethernet (1Gbps):** common for uplink/downlink ports on the Data Center switches for most networks.
- **10-Gigabit Ethernet (10Gbps):** (1) Common for uplink/downlink ports between switches in medium/large network environments. Provides an alternative over Port Channel with multiple Gigabit Ethernet interfaces. (2) This bandwidth technology is required if Fibre Channel over Ethernet (FCoE) will be used to transport Ethernet and Fibre Channel traffic between the Core and the Access layer. (3) This 10GE interface may be a Fabric Extender (FEX) interface that support 10GE/FCoE. Using FEX requires Cisco Nexus 5000+2000 hardware (Unified deployment type).
- **40-Gigabit Ethernet (40Gbps):** to provide bandwidth speeds up to 40Gbps. 40GE uses the same four multimode fiber pairs that are used with four 10GE links.
- **Port Channel:** Used with Ethernet connections for bundling multiple GE (up to 6) or 10GE (up to 4) connections for additional bandwidth if higher GE/10GE speeds are required on the downlink ports. Recommended to use LACP (industry standard protocol) for the port channel protocol.

Example: based on the uplink/downlink bandwidth calculated from the last step which was 2.4Gbps we can use a Port Channel with three GE interfaces up to the Core.



In this step determine the combined aggregated bandwidth (or switch capacity) for each access switch based on the number of edge ports, uplink ports, and the bandwidth technology chosen from the previous steps. This is important to help determine the best hardware to use for the access switches.

The following formula can be used to determine the minimum switch capacity (**Sc**) required for the access switch:

$$\text{Sc} : [(\# \text{ of Edge Ports}) \times (\text{Max Bandwidth per Edge Port})] + [(\# \text{ of Uplink Ports}) \times (\text{Max Bandwidth per Uplink port})] \times 2$$

Note: Ethernet ports in networks today will support full-duplex, which means each port is able to send and receive at the bandwidth rate of the switch port (e.g. 1Gbps, 10Gbps). Thus the “2” represents the full-duplex operation which doubles the bandwidth for the total switch capacity.

Example: To determine the aggregated bandwidth for one of our access switches in our topology we need to gather the required information:

- # of Edge ports = 48
- Maximum Bandwidth per Edge Port = 1Gbps
- # of Uplinks = 3
- Maximum Bandwidth per Uplink Port = 1Gbps

Now let's put that information into the formula: $[(48 \times 1\text{Gbps}) + (3 \times 1\text{Gbps})] \times 2 = 102\text{Gbps}$

Therefore, it is recommended that the hardware model for the access switch has a switch capacity of at least **102Gbps**.

When to use: if you are using a three-tier Data Center topology or if the Data Center topology consist of a traditional redundancy model.

Well this presents interesting challenges in terms of the bandwidth to use based on what has been determined for the downlink ports. For example, if there are a total of 4 GE downlinks to all access switches then that number should be considered for the bandwidth for the interconnection link. However, larger environments could have a total of 50 GE downlinks for all access switches or buildings hence 1GE Port Channeling will not work and using 10GE will be required.

To determine the bandwidth for all of the interconnection links in the topology obtain the following information:

- **Total Bandwidth for all Access Switch Downlinks:** Determine the total bandwidth service that was used for all of the access switch downlink ports. For example, let's say we have a Core switch connected to three access switches each using a 1GE connection. In this case, the total bandwidth for all access switch downlinks on the Core would be a 3Gbps.

With the information gathered from the list above use the following formula to calculate the expected throughput required for all of the interconnections in the topology. The expected utilization is based on the recommended **oversubscription ratio of 4:1 between the Distribution and the Core layer**.

$$\text{Data Center: } (\text{Total Bandwidth for all Access Switch Downlinks}) / 4$$

Example: continuing with our example we know that we have three connected access switches each with a bundled GE uplink. Therefore, the total aggregated bandwidth between all 3 access switches would be 9Gbps (using 3xGE port channel for each link). When we add a second Core switch to provide traditional redundancy it will require an interconnection link between the two Core switches.

Based on the bandwidth calculated from the last step for the interconnection ports, determine what bandwidth technologies will be used based on the following options, but read the **design considerations** first:

- **Gigabit Ethernet (1Gbps):** common for interconnections in small/SMB/medium-sized Data Center topologies.
- **10-Gigabit Ethernet (10Gbps):** (1) recommended for interconnections in medium/large-sized Data Center topologies. (2) This bandwidth technology is required if Fibre Channel over Ethernet (FCoE) will be used to transport Ethernet and Fibre Channel traffic from the Distribution to the Core layer where the storage array is attached.
- **40-Gigabit Ethernet (40Gbps):** to provide bandwidth speeds up to 40Gbps. 40GE uses the same four multimode fiber pairs that are used with four 10GE links.
- **Port Channel:** Used with Ethernet connections for bundling multiple GE (up to 6) or 10GE (up to 4) connections for additional bandwidth. Recommended to use LACP (industry standard protocol) for the port channel protocol.

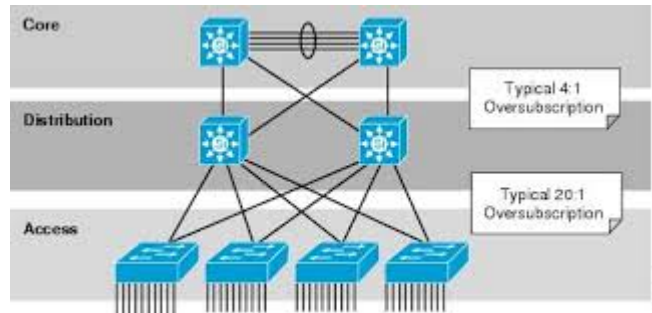
Design Considerations: The highest bandwidth technology you can use for an interconnection port can either be a single 40GE connection (requires expensive hardware) or four 10GE bundled in a Port-Channel (providing a total bandwidth of 40Gbps). The question is what if your total aggregated bandwidth from your access layer (desktops or servers) is 125Gbps even after you have calculated an oversubscription ratio of 4:1? Before I can answer that let me step back and explain what this means.

You probably realized that in many of the previous steps, each host on the network will not be able to send up to its maximum bandwidth speed. The reason for that is because the current bandwidth technologies are not there yet.

For example, in our Data Center scenario example we have a total of 140 server ports. We noted that each of those hosts could be high-performing devices utilizing Gigabit Ethernet which is possible because newer computer systems will likely have Gigabit Ethernet adapters. Those 140 GE edge ports will be spread out across three access switches, but the combined aggregated bandwidth would be 140Gbps. Well, if each of those computers were able to utilize 1Gbps throughput from their computer then you will be looking at a combined traffic rate of 140Gbps. Well there is no single bandwidth technology that can accommodate that. We are on the verge of 100 Gigabit Ethernet, but again we are talking about 140Gbps. That is why we do have the current bandwidth technology to support that model. Luckily, user desktops will never utilize up to 1Gbps speeds even for heavy file transfers.

But I can still use the same example when we talk about servers having 10GE NICs. Imagine those numbers. If you have just 50 servers each with 10GE NICs then that would be a total aggregate of 500Gbps if we are looking at 100% utilization. Even at 50% utilization that would be 250Gbps and still 100 Gigabit Ethernet still wouldn't be good enough. Therefore, what options are available that can be used for building high-performing interconnections with minimal delay:

1. **Two-Tier Topology:** these considerations is why two-tier topologies is becoming very popular and widely used. I have rarely seen a three-tier topology in today's modern networks because of this bandwidth limitation. Hence, try to always use a two-tier topology for any network.
2. **Oversubscription Ratio Best Practices:** The network industry has adapted an oversubscription ratio best practice to follow. It has become helpful to determine the bandwidth between the Access and Core/Distribution layer which would be an oversubscription ratio of 20:1. Or to determine the bandwidth with higher uplinks between a Core and Distribution layer which would be an oversubscription ratio of 4:1. These ratios represent a good baseline to follow and what the design cookbook utilizes for its bandwidth calculations.



3. **Blocking and Non-Blocking Hardware:** the performance of the hardware model will determine if the ports/interfaces on the hardware device provide non-blocking performance or blocking performance (shared bandwidth). Non-Blocking provide a 1:1 ratio meaning 1GE in and 1GE out for possible throughput with low-latency. This avoids possible oversubscription, increased delay, and drops. Hardware for non-blocking devices tend to be more expensive. Blocking means multiple ports share a common bandwidth resource. For example six 1GE connections coming in may share 1GE going out. So if 6 GE servers are forwarding at 100% then there will be oversubscription, buffering of packets resulting with possible delay and discards/drops. However the cost for blocking type hardware is cheaper. Non-Blocking is also known as line-rate or wire-speed. Non-blocking is something that is often discussed with L2/L3 switches more than with router devices.
 - a. **Non-Blocking:** recommended for Server Farm/Data Center networks and the LAN Core. Or if utilization is expected to be high.
 - b. **Blocking:** common for LAN topologies or if utilization is expected to be low.

Step 3-11

Determine bandwidth media for interconnection and other uplink ports

For the bandwidth service determined for the uplink/downlink ports on the Core/Aggregation, what media type will be used:

- **Copper:** the most common and recommended media type to use for edge ports. Copper can also be used for the uplink/downlink ports if copper wiring is supported and does not exceed 100 meters. Copper media for uplink/downlink connections is starting to become common for wiring if the equipment exist in the same room location.
- **Fiber:** common media type used for uplink/downlink ports when using 1GE and 10GE connections. It also depends on the distance between the components (e.g. Core and Access) that may require multi-mode or single-mode fiber connections.

Example: all of our uplink/downlink ports will use copper GE ports, so that will be needed for our Data Center Core switch ports.

Next we need to determine the total number of ports required on the Core device based on the following components connected.

- **Downlink to Access Layer:** the total number of access switches with uplinks to the Data Center Core switch, therefore, each port on the Core is considered as an aggregation point that needs to be calculated.
- **Infrastructure Components:** It's recommended to have up to 10 ports on the Core switch for these infrastructure components. This can be the interconnection between the Data Center Core/Distribution switches. It can also be the uplink/downlink ports to many of the main network components like the firewall appliance, Internet Edge Router, the WAN Aggregation/Branch router, and/or the LAN Core switch where the user network exist.
- **Storage Components:** If a storage solution will be deployed, the storage array (or SAN switch) would connect into the Core. Determine the number of Ethernet (10GE), FCoE, and/or Fibre Channel ports that are needed on the Core switch for the storage array switch ports. If you are planning on deploying a storage network with Fibre Channel its recommended to use the Cisco Nexus 5500 Series for the Core.

With the total number of ports determined on the core/aggregation layer consider the following for additional ports to add to the total:

- Potential scalability of additional ports adding at least 20% (or higher if necessary) more ports
- Potential redundancy used by network devices adding between 15-20% (or higher if necessary) more ports. For example if the firewall component in the design becomes redundant we want to consider that for the total port capacity needed for the hardware choice in a later step.

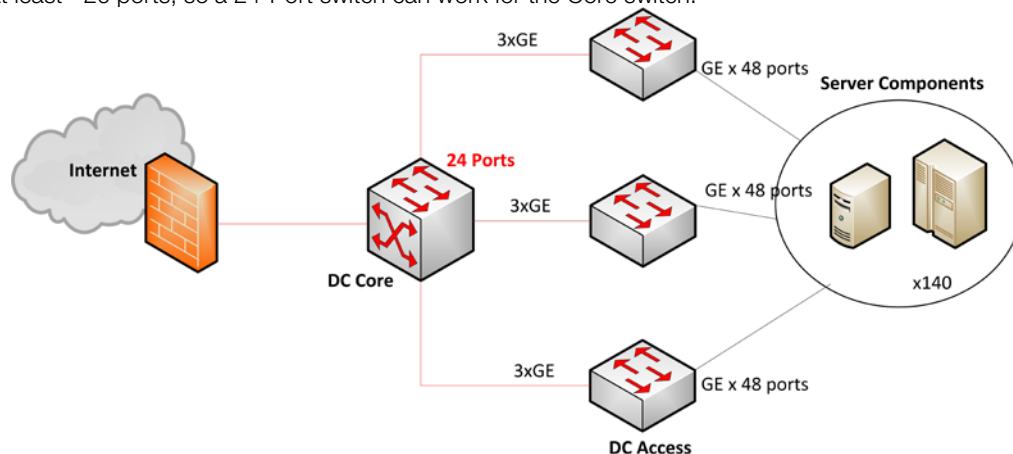
For the infrastructure and storage components that may be connected to the Core switch, determine if those ports will be Fast Ethernet/Gigabit Ethernet, Ten Gigabit Ethernet, or 40 Gigabit Ethernet.

- **Fast Ethernet (100Mbps) | Gigabit Ethernet (1Gbps):** common for most infrastructure components (e.g. Firewall, Internet Edge, WAN, and small/medium LAN Core switches).
- **10-Gigabit Ethernet (10Gbps):** recommended when using a large-sized Data Center topology. (2) This bandwidth technology is required if Fibre Channel over Ethernet (FCoE) will be used to transport Ethernet and Fibre Channel traffic.
- **40-Gigabit Ethernet (40Gbps):** to provide bandwidth speeds up to 40Gbps. 40GE uses the same four multimode fiber pairs that are used with four 10GE links.
- **Fibre Channel:** used for connecting directly into a Fibre Channel fabric (SAN switch) or to a storage array supported for Fibre Channel.

Next, determine the switch port capacity that will be needed for the Core switch:

- **24 Ports:** a fixed switch that provides 24 Ethernet ports. Ideal for smaller server farms connected into the Core.
- **48 Ports:** a fixed switch that provides 48 Ethernet ports.
- **48+ Ports:** a switch that can support more than 48 Ethernet ports. This would be a chassis-based switch or a stack-based switch.

Example: the Core switch will have one connection to the Internet Edge and nine 1GE downlink ports to the access switches. We also need to consider that 10 additional ports may be needed on the Core switch over time. Therefore, we need at least ~20 ports, so a 24-Port switch can work for the Core switch.



In this step determine the combined aggregated bandwidth (or switch capacity) for the Core switch based on the number of ports and the bandwidth technology chosen from the previous steps. This is important to help determine the best hardware to use for the Core switch.

The following formula can be used to determine the minimum switch capacity (**Sc**) required for the access switch:

$$\text{Sc} : [(\# \text{ of Ethernet Ports}) \times (\text{Max Bandwidth per Ethernet Port})] \times 2$$

Note: Ethernet ports in networks today will support full-duplex, which means each port is able to send and receive at the bandwidth rate of the switch port (e.g. 1Gbps, 10Gbps). Thus the “2” represents the full-duplex operation which doubles the bandwidth for the total switch capacity.

Example: To determine the aggregated bandwidth for our Core switch in the topology we need to gather the required information:

- # of Ethernet Ports = 24
- Maximum Bandwidth per Ethernet Port = 1Gbps

Now let's put that information into the formula: $(24 \times 1\text{Gbps}) \times 2 = 48\text{Gbps}$

Therefore, it is recommended that the hardware model for the Core Switch has a switch capacity of at least **48Gbps**.

The following performance related features/services should be implemented with the Data Center solution.

- Jumbo Frames
- Flow Control

Below are Security Services (and Solutions) that should be deployed within the solution:

- Port Security
- BPDU Guard or BPDU Filter
- Root Guard
- Trunking (802.1Q): Trunk Security
- Security Best Practices
- Access Control Lists (ACL)

Step 5	Network Management for Data Center

Below are the “Network Management Services” that should be deployed within the solution:

- SNMP
- NTP
- Syslog
- RADIUS *OR* TACACS+
- VTY Access
- GOLD, EEM, ERM, Configuration Rollback, RBAC
- Port Monitor

Step 6	Flexibility for Data Center

Step 6-1	Integration with other solutions

Below are other solutions that are commonly deployed within the foundation solution:

- Virtualization (Network)
- Application Delivery
- Web and E-Commerce
- Unified Computing
- Storage

Step 6-2	Integration with LAN

If a LAN solution (1, 2, or 3 tier topology) will be deployed, then the LAN Core would plug directly into the Data Center Core.

Step 7

Design Aspects for Data Center

Below are specific design elements to complete for the solution.

Step 7-1

Data Center Interconnect (DCI)

When to use: when using multiple Data center locations across the network.

Determine what Data Center Interconnects (DCI) service(s) should be used between the Data Center networks based on the provided list below:

- Overlay Transport Virtualization (OTV)
- Locator Identifier Separation Protocol (LISP)
- Virtual Extensible LAN (VXLAN)
- Cisco FabricPath
- L3VPN: MPLS (on Service Provider)
- L2VPN: VPLS, EoMPLS (on Service Provider)

Step 7-2

Other services to include with solution

These are additional services that can be implemented (if required) within the solution.

- General Best Practices
- Multicast
- IPv6
- Virtualization (Network): Layer 3 Virtualization

Step 7-3

Features

Below are Data Center features that can be used (based on the hardware supported):

- **Breakout feature:** ability to take a 40GE port and configure it as four independent 10GE interfaces. Focuses on 10G to 40G connectivity. This feature is supported on the F3 series modules for the Cisco Nexus 7000/7700 Data Center switches.
- **BiDi feature:** reduces cabling requirement required for 40GE to 40GE connections. BiDi optics supported on Nexus 7000/7700 F3 and M2 series modules

Determine the subnet types and the number of subnets that will be used on the Data Center.

- **Servers:** a dedicated subnet should be used for servers in the Data Center. Multiple server subnets can be used for different server groups based on the type of server (Infrastructure, Applications, Database).
- **Management:** a dedicated subnet used for managing all network devices including network management services such as SNMP and Syslog for monitoring.
- **Interconnection:** a dedicated subnet used between the redundant LAN components if routing is enabled.
- **Other:** other subnets can be created based on any unique requirement.

Step 8	Hardware for Data Center

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1	Hardware Options

Determine the hardware for each component in the solution using the tables below based on the technical objectives with some of the important details (supported services, bandwidth, etc).

Cisco Nexus 9000 Series *(Large, Data Center)*

Performance	30Tbps 1G/10G/40G/100G support	Flexibility	FCoE (Storage)
Reliability	Power, ISSU	Management	SDN (ACI)
Scalability	Topology (Unified), 488 ports (40GE), 1152 ports (10GE)	Security	Identity (TrustSec)
Design Aspects	L2, L3, Virtualization (NVGRE), VXLAN, ACI		
Models	9508, 9396PX, 93128TX ; chassis, NX-OS		

Cisco Nexus 7000 Series *(Large, Data Center)*

Performance	1.3Tbps/slot (7700 series) 83Tbps/chassis 550Gbps/slot (7000 series) 17.6Tbps/chassis 10G/40G/100G support	Flexibility	FCoE (Storage)
Reliability	Power, ISSU, vPC	Management	NAM (7000 series), SDN
Scalability	Topology (Traditional, Unified)	Security	Identity (TrustSec)
Design Aspects	L2, L3, Virtualization (MPLS, VPLS, VDC), DCI (OTV, VXLAN, LISP), FabricPath, DFA, Breakout support		
Models	7706, 7710, 7718, 7004, 7009, 7010, 7018, Fabric Modules (I, II) ; chassis, NX-OS		

Cisco Nexus 6000 Series *(Large, Data Center)*

Performance	7.68Tbps (6004/6004X series) 10G/40G support	Flexibility	FCoE (Storage)
Reliability	--	Management	Cisco Prime Data Center Network Manager
Scalability	Topology (Traditional, Unified) 6001: 48x 10GE 4x 40GE (16x 10GE) 6004: 96x 40GE 384 10GE (using breakout)	Security	--
Design Aspects	L2, L3, DCI (OTV, VXLAN, LISP), FabricPath, DFA, Breakout support, FEX support		
Models	6001, 6004, 6004X ; fixed, NX-OS		

Cisco Nexus 5000 Series *(Medium, Large, Data Center)*

Performance	960Gbps-1.92Tbps 10G/40G (uplink) support	Flexibility	FCoE (Storage)
Reliability	Power, vPC	Management	SDN
Scalability	Topology (Unified), up to 1152 ports 5548 : 48x 10GE	Security	Identity (TrustSec)
Design Aspects	L2, L3, Virtualization (NVGRE), DCI (VXLAN), FEX support, DFA		
Models	5672UP, 56128P, 5596T, 5596UP, 5548P, 5548UP ; fixed/modular, NX-OS		

Cisco Nexus 2000 Series *(Medium, Large, Data Center)*

Performance	88-176Gbps 10G/40G (uplink) support	Flexibility	FCoE (Storage)
Reliability	Power	Management	SDN
Scalability	Topology (Unified), ~24-48 ports 2248PQ-10G : 48x 10GE & 4x 40GE	Security	Identity (TrustSec)
Design Aspects	L2, L3, FEX		
Models	2232TM-F1, 2232PP, 2224TP, 2248TP, 2248PQ ; fixed, NX-OS		

Cisco Nexus 1000V Series *(Medium, Large, Data Center)*

Performance	--	Flexibility	--
Reliability	VSM (redundant)	Management	--
Scalability	Topology (Virtualized)	Security	Identity (TrustSec), ACL
Design Aspects	Components (VSM, VEM), L2, VXLAN, VN-Link		
Models	VMware vSphere, Microsoft Hyper-V, Licensing (Essentials, Advanced) ; NX-OS		

Cisco Catalyst 6800 Series *(Large, Data Center)*

Performance	880Gbps/slot 10G/40G/100G support	Flexibility	PoE, Wireless (WiSM), ACE30
Reliability	Power, VSS (VS40, MEC)	Management	NAM, SDN
Scalability	Topology (Unified)	Security	Firewall (ASA), Identity (TrustSec), AVC
Design Aspects	L2, L3, Virtualization (MPLS, VPLS, EVN)		
Models	6807-XL, 6880ia, 6880-X ; chassis		

Cisco Catalyst 6500 Series *(Medium, Large, Data Center)*

Performance	40-80Gbps/slot 10G/40G/100G support	Flexibility	PoE, PoE+, WiSM, ACE
Reliability	Power, VSS (VS40), ISSU	Management	NAM
Scalability	Topology (Traditional)	Security	Firewall (ASA), Identity (TrustSec)
Design Aspects	L2, L3, Virtualization (MPLS, VRF-lite, EVN), LISP		
Models	6513-E, 6509-E, 6506-E, 6504-E, 6503-E, Supervisor Engines (720, 2T) ; chassis		

Cisco Catalyst 4500-E Series *(SMB, Medium, Large)*

Performance	1.8Tbps (VSS), 928Gbps 1G/10G support	Flexibility	PoE/PoE+/UPoE, Wireless (WLC)
Reliability	Power, VSS (MEC), ISSU, NSF/SSO	Management	GOLD, SDN
Scalability	Topology (Traditional, Unified)	Security	Identity (TrustSec), FnF
Design Aspects	L2, L3, Virtualization (VRF-lite, EVN), Medianet		
Models	4503-E, 4506-E, 4507-E, 4510-E, Supervisor Engines (8E, 7E, 7LE, 6E, 6LE, V-10GE) ; chassis, IOS XE Licensing (LAN Base, IP Base, Security, Enterprise)		

Cisco Catalyst 4500-X Series *(SMB, Medium, Large)*

Performance	1.6Tbps (VSS), 800Gbps 1G/10G support	Flexibility	--
Reliability	Power, VSS (MEC, ISSU), NSF/SSO	Management	GOLD, DOM
Scalability	Topology (Traditional)	Security	Identity (TrustSec), FnF
Design Aspects	L2, L3, Virtualization (VRF-lite, EVN), Medianet		
Models	16 ports, 32 ports ; fixed, IOS XE Licensing (LAN Base, IP Base, Security, Enterprise)		

Cisco Catalyst 3850 Series *(Medium, Large)*

Performance	Stack: 480Gbps Uplink Ports: 1G/10G (2 or 4) Edge Ports: 10/100/1G (12, 16, 24, 36, 48)	Flexibility	Wireless (WLC), UPoE, PoE/PoE+
Reliability	Stack Power, Stack, Stateful Switchover (SSO)	Management	SDN
Scalability	Topology (Traditional, Unified), 24-192 ports Stack (up to 4 switches, planned for 9)	Security	Identity (TrustSec), FnF, AVC
Design Aspects	L2, L3		
Models	24 ports, 48 ports ; fixed, stack		

Cisco Catalyst 3750-X Series *(Medium, Large)*

Performance	Stack: 64Gbps 1G/10G (uplink) support	Flexibility	PoE/PoE+/UPoE
Reliability	StackPower, Stack	Management	--
Scalability	Topology (Traditional, Unified), 24-432 ports Stack (up to ~ 9 switches) Support for 600 users	Security	Identity (TrustSec)
Design Aspects	L2, L3		
Models	24 ports, 48 ports ; fixed, stack		

Cisco Catalyst 3650 Series *(SMB, Medium, Large)*

Performance	Stack: 160Gbps Uplink Ports: 1G/10G (2 or 4) Edge Ports: 10/100/1G (24, 48)	Flexibility	Wireless (WLC), PoE/PoE+
Reliability	Power, Stack, Stateful Switchover (SSO)	Management	SDN
Scalability	Topology (Traditional, Unified), 24-48 ports Stack	Security	Identity (TrustSec), FnF, AVC
Design Aspects	L2, L3		
Models	24 ports, 48 ports ; fixed, stack, IOS XE		

Cisco Catalyst 2960-X Series *(SMB, Medium, Large)*

Performance	Stack: 80Gbps Switch Capacity: 216Gbps Uplink Ports: 1G/10G (2 or 4) Edge Ports: 10/100/1G (24, 48)	Flexibility	PoE, PoE+ (up to 740W)
Reliability	StackPower, FlexStack-Plus	Management	SDN, NetFlow lite
Scalability	Topology (Traditional, Unified), 24-384 ports Stack (up to 8 switches)	Security	Identity (TrustSec, 802.1x), FnF
Design Aspects	L2, L3 (using 2960-XR)		
Models	2960-X, 2960-XR - 24 & 48 port models ; fixed/stack		

Cisco SG500XG Series – Small Business *(SMB)*

Performance	Stack: 80Gbps Switching Capacity: 320Gbps Uplink/Edge ports: 10GE (16 ports)	Flexibility	--
Reliability	VRRP, Stack	Management	GUI, CLI
Scalability	Topology (Traditional, Unified) Stack (up to 8 switches)	Security	ACL, Identity (802.1x), Web Auth
Design Aspects	L3, IPv6, USGv6		
Models	Hardware: SG500XG-8F8T (16 ports) Defaults: 8x 10GE (Copper, RJ-45), 8x 10GE (Fiber, SFP+), 1 GE (Management)		

For chassis hardware models (e.g. Cisco Nexus 7000 series) make sure they include the following:

- **Chassis:** determined based on the total number of ports and bandwidth services needed.
- **Line Modules:** modules that provide port capacity (Ethernet) and services.
- **Dual Supervisors:** utilizing redundant Supervisor Engines can provide redundancy for the chassis.
- **Fan Trays (System, Fabric):** these are required in order to cool the modules in the chassis.
- **Licensing:** Determine what services/features will be used on the device and ensure to get all of the needed licenses to support your configuration.
- **Power (Input Voltage):** determine the required power based on the modules in the chassis and the capabilities that will be used (e.g. PoE). If you are planning to use Cisco based switches use the Power Calculator Tool (<http://tools.cisco.com/cpc/>) to determine the power supplies and power source needed with the chassis

#1a

Hardware Options based on 10GE & 40GE

Below is hardware options based on 10GigabitEthernet and 40GigabitEthernet port capacity:

- **Cisco Nexus 6001:** 48x 10GE | 4x 40GE (or usable as 16x 10GE)
- **Cisco Nexus 6004:** 96x 40GE
- **Cisco Nexus 5548:** 48x 10GE
- **Cisco Nexus 3064X:** 48x 10GE

#2

Hardware Consolidation Option

Some of the Data Center components can be consolidated using one of the following options:

- **Data Center Access Layer:** using Cisco Nexus 1000V within a VMware ESXi/Microsoft Hyper-V infrastructure.

Note: Reference the "Hardware Table" for any specific hardware that may be listed for consolidation.

Resources

Cisco Nexus 9000 Series:

- Cisco Nexus 9500 (modular), Nexus 9300 (fixed)
- Run in ACI mode or NX-OS mode
- In ACI mode, the switches can be used with an Application Policy Infrastructure Controller (APIC) to provide an application centric infrastructure (ACI).
- In NX-OS mode, the switches function as classic switches.

Cisco Nexus 6000 Series:

- FCoE support. Recommended for FCoE networks (end-to-end) with 40GE links in the Core.
- *Forwarding Table support:*
 - o 128K entries supported for MAC address tables (default)
 - o 128K entries supported ARP, Network Discovery (ND) and Multicast (*,G) entries
 - o 50K entries supported for IPv6 entries (dual stack)

Data Loss Prevention

Category: Business Solution
Prerequisite(s): --

Complete the steps below for building the solution:

Step 1	Network Solutions applicable for this Business Solution

This is a business solution which cannot be deployed directly. The solution will consist of one or more of the following network solutions that are applicable for deployment:

- Firewall (using the Next-Generation type Firewall)
- Content Security (Email, Web)

Add one or more of these solutions and reference those respective sections for the network design.

Desktop Solution

Category: System Solution
Prerequisite(s): LAN Solution

Complete the steps below for building the solution:

Step 1

Desktop System Components

A user endpoint is a component that is used directly by a user to access services and applications over the network (or locally). The main user endpoint would be a desktop system (computer, laptop) and below would be the components that would be used for a desktop system that needs to be determined by the system engineer/desktop technician:

- Operating System (OS): Windows, Mac OS, Linux (*nix)
- Applications (Office, Business, Tools, Multimedia, etc)
- Accessories (Printers, USB, Scanner)

Step 2

Desktop Add-On Components

Below are some additional services that can be deployed for desktop systems in the environment:

- Drive Encryption
- Anti-Virus
- **Desktop Management:** solution that provides managing user desktop/laptop systems in terms of patching, Anti-Virus, applications on the system, to tools used by desktop technicians for troubleshooting a problem on a desktop/laptop remotely.
- **Data Mining:** Desktop search engine capabilities (e.g. Google Desktop)

Step 3

Other System Solutions applicable

The solution may also involve using other system solutions such as:

- Endpoint Security

Step 4

Foundation Solutions applicable for this System Solution

Below is the foundation solution(s) that is required:

- LAN Solution

User endpoints like desktops will exist in user VLANs connected into the Access layer.

Disaster Recovery

Category: Business Solution

Prerequisite(s): Data Center Solution, WAN Solution

Complete the steps below for building the solution:

Step 1

Foundation Solutions applicable for this Business Solution

This is a business solution which cannot be deployed directly. The solution will consist of one or more of the following network solutions that are applicable for deployment:

- Data Center
- Wide Area Network (WAN)

Add one or more of these solutions and reference those respective sections for the network design.

Step 2

System Solutions applicable for this Business Solution

This is a business solution which cannot be deployed directly. The solution will consist of one or more of the following system solutions:

- Server Solution
- Data Management (Storage) Solution

Add one or more of these solutions and reference those respective sections for the network design.

Step 3

Type of DR Site

Determine how the backup Data Center location (the DR site) will be deployed. Below are the options to choose from:

- **Hot:** An active Data Center that is running at full capacity and services ready to be used with minimal involvement. When a failover happens, all sites and users will continue to operate, almost transparently. Out of the three options this is the most expensive and requires more administration resources to maintain the two Data Center networks.
- **Warm:** A partially active Data Center that runs various services (that are more critical) and other services (less critical) are not turned on. When a failover occurs some configuration is required for getting the services running again.
- **Cold:** A passive Data Center where all services and servers are not turned on (or present at the site). Therefore, when a failure occurs the IT staff must follow the DR plans to restore critical services at a designated DR site. The down-time for this type of DR can last for numerous hours (or days); however, it is the cheapest out of the three.

Determine how users and sites will communicate with the DR site if a failure at the primary site occurs. Below are the options to choose from:

- **Private Connection:** Ideal and recommended when using a Hot and Warm DR site with remote sites on a private WAN. When a failure occurs at the main site the remote sites could automatically get re-routed to the DR site easily by using routing protocols. Using a private line can also be useful for server/SAN replication (or backup) to the DR site with guarantee SLA.
- **VPN Connection:** This can be used for Hot, Warm or Cold DR sites with minimal to no remote sites. This is ideal for light network usage and for light network backup/replication (where data doesn't change that much). DMVPN can be used for remote sites connected to the Internet for connecting to the DR site transparently.

Recommendations: Small and SMB sites tend to use VPN for connecting with remote sites since the cost for a DR site can be high. However, for Medium, Large, or any network that has an IP WAN should definitely consider adding another site to the WAN designated as the DR location (which may be a small rack) with only "critical to the business" services. For example, if Internet access is not a critical service then that shouldn't be considered in a DR plan. Most DR locations are usually Warm or Cold DR types.

For DR purposes, deploy a subscriber server at a DR site/location that all of the remote sites can communicate with if the primary voice site goes down. The remote sites can still place and receive calls through their local voice gateway router.

DMZ & Extranet

Category: Network Solution (Security)

Prerequisite(s): LAN and/or Data Center Solution, Internet Edge Solution

Complete the steps below for building the design for the network solution. First, determine the type of DMZ solution that will be used on the network:

- **DMZ:** used by a corporate network dedicated for public facing servers (e.g. mail server, web server, FTP server) that is accessed from the outside restricting direct access into the local LAN/Data Center. Typically not allowed to initiate connections to the internal network except for certain circumstances.
- **Business Partner:** A dedicated network used for business partners that manage their own equipment and circuits. It's a network that provides a place where users can access services within the business partner's network.

Recommendations: It's recommended to implement a DMZ where public facing servers exist, but it does increase the overall administration and potentially complicated firewall policies. For large and medium environment using a DMZ is highly recommended. The DMZ may communicate with other servers like a Domain Controller on the internal network (LAN and Data Center), therefore, implement firewall policies permitting what needs to be accessed between the two environments. Make sure to do on-going maintenance with the servers in terms of patching and updates to avoid any security exploits.

Step 1

Scalability for DMZ & Extranet Solution

Step 1-1

Determine the components for the solution

Determine the components for this solution and how it will be deployed:

- **Servers:** these are public facing servers designed and managed by the system engineering team.
- **Firewall/L3 Device:** the DMZ is just another network that can exist off of the Firewall or a L3 device (e.g. L3 switch or Router) with security policies enabled. This is based on the deployment of the DMZ.

Step 1-2

Choose a DMZ Topology

The DMZ can be deployed as a logical or physical solution to the network including how it will be secured. Below are the different DMZ topologies that can be deployed.

- **Physical (using a Firewall interface):** In this deployment all servers are plugged into a switch, which is then plugged directly into a new firewall interface configured with security policies for who can access the DMZ network and vice versa.

Solution Required: Firewall Solution

- **Logical (using a VLAN on the LAN or Data Center):** a VLAN is configured on the LAN/Data Center dedicated for the DMZ network. The VLAN Layer 3 interface (the SVI) can be configured with an ACL restricting access or that VLAN can be extended up to the firewall to provide firewall services.

Services Required: VLAN, Trunking (802.1Q)

Recommendations: Both options are recommended, but the first option is the most common DMZ deployment and used since the very beginning. However, using a VLAN is recommended for increased flexibility because we can extend that DMZ network to other buildings or locations securely. Or the DMZ can be deployed in a dedicated VLAN plugged into a new firewall interface consolidating the environment for simplicity.

Step 2	Design Aspects for DMZ & Extranet Solution

Step 2-1	IP Subnets

Determine the subnet types and the number of subnets that will be used:

- **DMZ:** a dedicated subnet used for public facing servers in the DMZ network.
- **Other:** other subnets created based on any unique requirement or preference.

Step 2-2	Business Partner – Connection Method

Determine the business partner connections that will be used. This basically defines what type of connection the business managed router will use for communicating back to their location. Here are some options and considerations:

- **Private Connection:** In this deployment the business partner is using a dedicated lease-line from your location (in the Business Partner network) to their network. This is a secure method and doesn't impact the internal network because the firewall is in place to allow only the traffic that is required to communicate with the internal network. Make sure to mention that the business partner is responsible for all ordering, maintaining, support, and extending the private connection to where the equipment is located. This is a business managed router therefore the support model and administration is with the partner.

Solution Required: WAN Solution

- **VPN Connection:** In this deployment, the most common, the business partner simply builds a VPN tunnel from their managed router back to their main office. The question is whether they will utilize your existing Internet connection or use a new Internet connection. It's recommended to use a separate Internet connection unless the traffic usage will be extremely low. Utilizing your existing Internet connection could lead to potentially slow performance that can create other Internet related issues.

Solution Required: VPN & Remote Access Solution

Recommendations: It depends on the business partner who manages the router. A VPN connection is very common for a business partner to utilize the customer's existing Internet connection. This is okay, just make sure that the traffic usage is low or a new Internet connection is required. In SOX compliance organizations (e.g. Banks, Financial Services) business partners may use a private connection for increased security including a VPN and other security components like security encrypters.



E

~ Solutions ~

Endpoint Security

Category: System Solution
Prerequisite(s): Desktop Solution

Complete the steps below for building the solution:

Step 1

Network Solutions applicable for this solution

The following are network solutions that can be used with this system solution:

- Identity Access Control
- Intrusion Prevention

Add one or more of these solutions to the design and reference those respective sections for completing the network design.

Step 2

Other System Solutions applicable

This solution will involve using other system solutions that include:

- Desktop Solution
- **Anti-Virus Solution:** Using Anti-Virus services for all endpoints is recommended and required. Make sure that Anti-Virus services are implemented for all end-points including regular updates.



F

~ Solutions ~

Firewall

Category: Network Solution (Security)

Prerequisite(s): LAN and/or Data Center, and Internet Edge Solutions

Complete the steps below for building the design for the network solution:

Step 1

Scalability for Firewall Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

1. **Firewall Appliance:** whether it is a L2 or L3 firewall, the component in this solution is a firewall appliance.

Step 1-2

Choose how components will be deployed

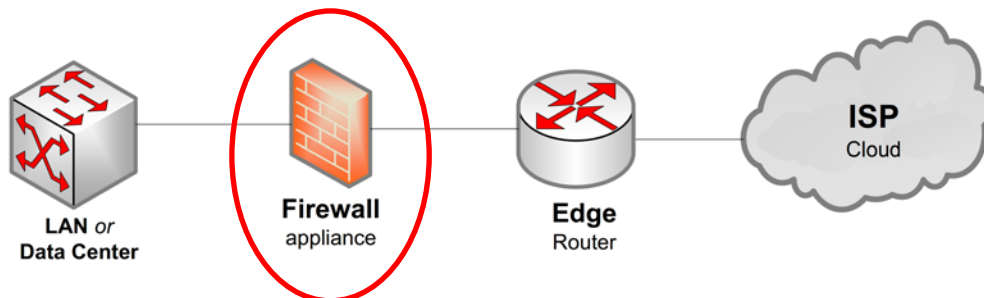
Determine how each component for the firewall solution will be deployed:

#1

Firewall Appliance

This component is usually deployed in-line between the LAN/Data Center and the Internet Edge solution. It can also be deployed between other solutions where needed.

Example: in the picture below you will see that the firewall appliance is deployed IN-LINE between the LAN and Internet Edge solutions.



Choose whether the firewall will be deployed as a Layer 3 (Routed) Firewall or Layer 2 (Transparent) Firewall. It determines whether the firewall deployed will route and/or support VLANs.

#1

Layer 3 Firewall

- **When to use:** most common type of firewall deployed on the Internet edge with IP addresses configured on all interfaces and can handle routing between other devices.
- **Description:** this is the most common firewall deployment to use that is typically deployed within the Internet Edge Solution. It is capable of routing using a dynamic routing protocol or static routes including support for VLAN tagging (using 802.1Q). L3 Firewall is also the default firewall behavior where a L2 Firewall must be configured that way. IP Routing is required to provide connectivity between the internal networks (e.g. LAN) and the Internet. NAT provides translation between the Public network (Internet) and the Private networks (LAN, Data Center, Wireless networks).

Services Required:

- Routing (Static, OSPF, EIGRP)
- Network Address Translation (NAT)

#2

Layer 2 Firewall

- **When to use:** allows adding the firewall appliance between other networks without re-addressing hosts/network devices.
- **Description:** A L2 Firewall is used between other network solutions such as between a LAN and Data Center network. It can extend a VLAN up to the firewall for security services such as a Guest network used on the LAN and/or with the Wireless network. This is a great option when adding a firewall into an existing network without re-addressing hosts or the default gateway.

Services Required: VLAN, Trunking (802.1Q)

Step 2	Reliability for Firewall Solution

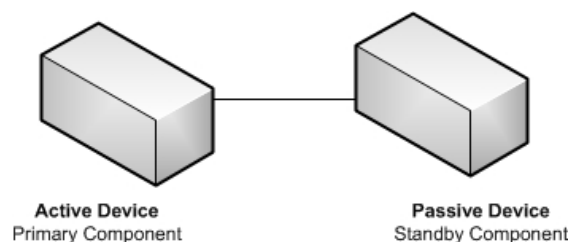
Step 2-1	Choose Redundancy Model

Determine which redundancy model should be used for the solution if reliability is important:

1. Active/Passive Redundancy
2. Active/Active Redundancy

#1	Active/Passive Redundancy

Many network solution products provide redundancy as a primary and secondary set. One device is active while the other device is in standby monitoring the operating conditions of the primary device and ready to transparently takeover when a failure occurs. This is called Active/Passive redundancy, which provides the easiest level of redundancy for a network component.



#2	Active/Active Redundancy

You can also configure the two firewall appliances in active/active mode which will allow both firewalls to be active at the same time providing both redundancy and load balancing. In an active/passive redundancy model, only one of the firewalls is active while the other remains dormant until it becomes active.

Firewall pairs configured in an active/active model will likely not support VPN tunnels since load balancing is performed between the two firewalls, so that consideration must be kept in mind. Also, troubleshooting issues between two active firewalls may pose a challenge for isolating a particular issue.

The active/passive redundancy model is often chosen as the common method for providing redundancy to a firewall application and simplicity with its configuration.

Step 3

Performance for Firewall Solution

Follow the steps below to determine the bandwidth services for the firewall solution.

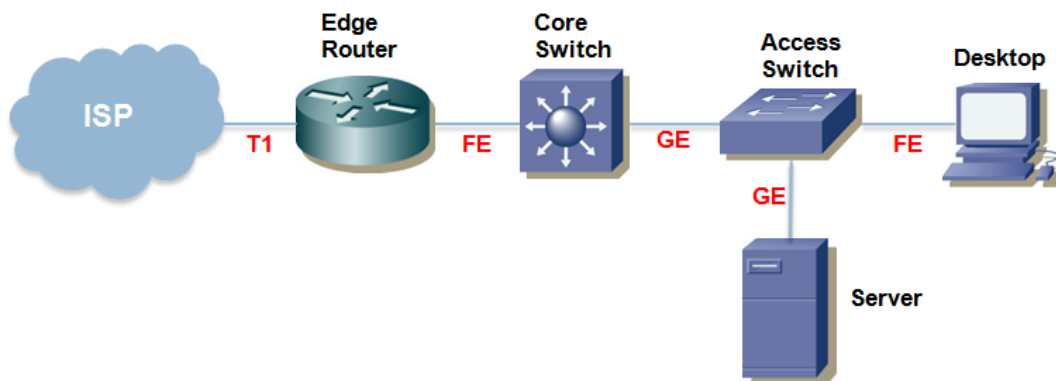
Step 3-1

Determine bandwidth services

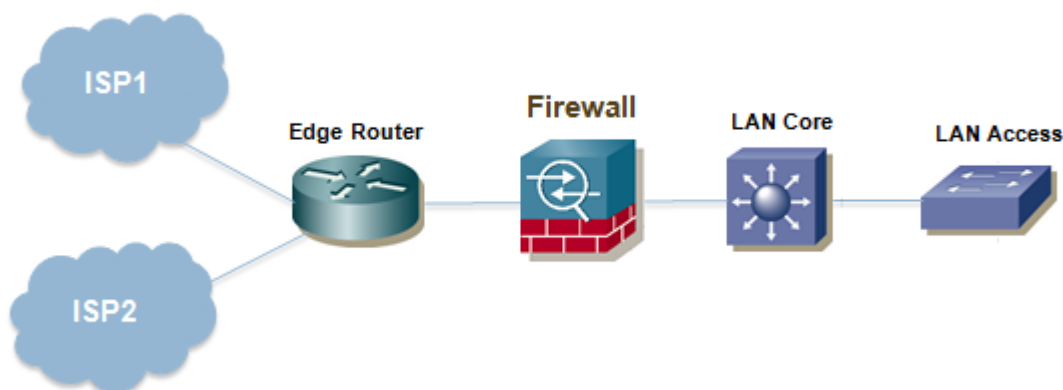
Determine the bandwidth service that is required for each component for the solution based on what exist in the topology. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)
- 10GigabitEthernet (10Gbps)

For example: below is a network design that involves two foundation solutions (LAN and Internet Edge). You will see the bandwidth identified for all connections in the diagram.



Now let's add the firewall component in-line between the Internet Edge router and the Core switch. The bandwidth service used between these devices is Fast Ethernet (FE). Therefore, the bandwidth services required for the firewall component's interfaces will also be Fast Ethernet (at a minimum).

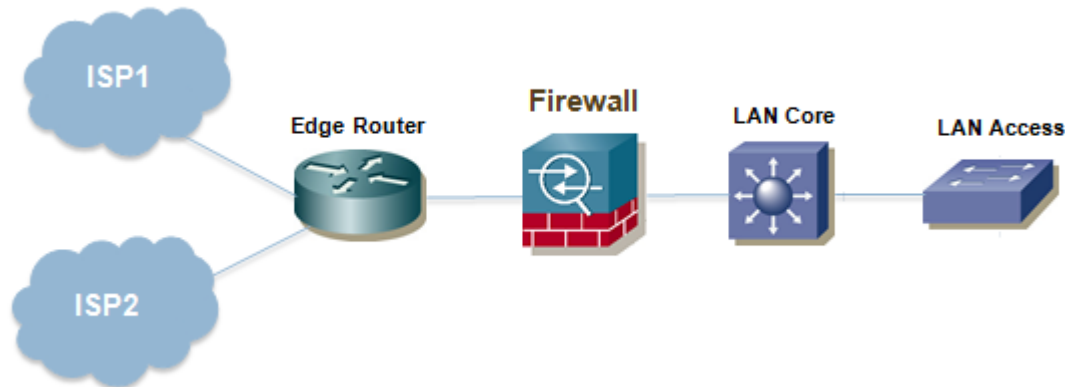


Next determine the required throughput or firewall performance expected through the firewall appliance. This is based on the actual data flow and determining the lowest bandwidth service along the path. The following needs to be determined:

1. **Data Path:** determine the expected data flow for certain services and applications through the network. For example, for Internet access the flow of data can occur from the LAN switches through the Firewall, the edge router (if applicable), and out to the Internet.
2. **Bandwidth Services:** determine the bandwidth service that is used for all connections on the network along the data path.
3. **Lowest Bandwidth:** determine the lowest bandwidth service along the data path.

Firewall Performance (Throughput): based on the information gathered this will make up the firewall performance required for that in-line device. For example, if the bandwidth services on the LAN is Gigabit Ethernet (1Gbps), but the connection on the edge router is a T1 (1.544Mbps) then our required firewall performance/throughput along the data path out to the Internet needs to be around 1Mbps.

Example: in the diagram below we want to determine the throughput needed on the firewall appliance:



If the bandwidth between the Edge router and the LAN Core is Fast Ethernet, then the firewall appliance interfaces would need be Fast Ethernet (at a minimum). However, understanding what the performance should be for firewall inspection is important. We might not need the firewall to inspect at 100Mbps. Also in the diagram let's assume that the Internet connection to ISP1 & ISP2 involves a T1 (1.544Mbps). With those details we can complete the three steps required to understand the throughput requirements for the firewall appliance:

1. The data flow will happen from the LAN out to the Internet (and vice versa) moving through the firewall appliance.
2. Along the data path, FE is used between the Edge Router and the Core switch. Let's say that GE is used between the Core and the Access switch. And a T1 is used on the Edge router's WAN facing interface up to each ISP.
3. The lowest bandwidth service along this data path is the T1 Internet connection on the edge router.

Firewall Performance (Throughput): Therefore, the required firewall performance or throughput through the firewall appliance needs to be ~1Mbps to handle all firewall inspection.

Take note of the throughput requirements for the in-line device to determine the correct hardware model.

Determine the firewall type based on the access policies that will be used:

- **1st Generation Firewall**
 - o **When to use:** when using access policies filtering based on the network/IP, protocol, and protocol number through the firewall component.
- **Next Generation Firewall (NGFW)**
 - o **When to use:** when using access policies filtering based on 1st generation components, URLs, applications, micro-application, and file content through the firewall component.
 - o **Requirements/Recommendations:** you must have the hardware to support this feature including the appropriate licensing for NGFW services.

Firewall policies are based on what should be allowed inbound and outbound between the various network zones (e.g. Trusted, Untrusted, DMZ). Below are some policies to consider when implementing firewall rules:

- **Access Policies (from General Security Design):** during the *General Design – Security* step you should have determined what services require direct inbound access from the untrusted network and only allow those services through with an inbound policy. This would also be considered as whitelist access policies which deals with blocking all traffic except what is allowed such as corporate sites and applications. Whitelist policies should always end with a rule to deny any traffic that has not specifically denied or allowed from a previous rule.
- Below are the type of access policies supported based on the firewall type desired for the design:
 - o **1st Generation FW Policies:** filtering based on network/IP, protocol, and protocol port number.
 - o **Next Generation FW Policies:** filtering based on 1st Generation FW policies, Applications, Micro-Application, URLs, File Content.
- **RFC1918 Filtering:** rules that should be added to Public facing interfaces to filter any private IP addresses sourced from the Internet which should only consist of Public IP addresses.
- **RFC2827 Filtering:** rules that should be added to Public facing interfaces to filter any source IP addresses that should only exist behind the firewall/trusted environment. For example, let's say that the trusted network is using Public IP Addresses from the 4.4.4.0 subnet. Any communication from that Public subnet should only be the source for outbound connections. For inbound connections it should appear in the destination field. If a new IP connection comes into the Public facing interface of the firewall/router and see's that the source is 4.4.4.X then the connection is likely being spoofed in some type of attack. Hence, that connection should be blocked. Configure RFC2827 filtering to protect against those types of attacks.
- **SMTP Outbound Filtering:** configure a rule to only allow SMTP outbound from a particular set of authorized SMTP servers. This ensures that SMTP related attacks caused by infected computers don't send large amounts of SPAM messages from the network causing network congestion. It can also potentially black list an email server for a company that uses a fixed IP address (common for small and SMB networks).
- **Blacklist Access Policies:** define what traffic should be explicitly denied outbound to the Internet that poses the greatest risk to network resources.

Determine if the firewall appliance should decrypt secure web pages for further inspection (e.g. URL, Files). This operation is accomplished when the firewall intercepts a secure session initiated by an internal user. In return, the secure tunnel is now established between the destination site and the firewall acting on behalf of the client. Furthermore, the firewall builds another secure tunnel with the user. This can provide enhanced security and Data Loss Prevention through the different zones on your network.

- **When to Use:** when you need the firewall to decrypt secure websites (HTTPS) for filtering/inspection against a configured access policy.
- **Components:** below are the components used with deploying the feature.
 - o Exist within the Firewall component.
- **Requirements/Recommendations:** to use this feature you must have the following:
 - o Must use a Next Generation Firewall including the appropriate licensing installed (if necessary)
- **Design Steps:** below are the steps for the design and implementation for the feature:
 - o Create Decryption policy with the URL/Application category for the type of secure sites that should be decrypted on the firewall. For example, adding Social Networking means the NGFW will decrypt only Social Networking sites like Facebook.
 - o Determine if all sites should be decrypted or if only malicious sites should be decrypted for deeper inspection.
 - o User endpoints must trust the certificate generated on the firewall component using group policies and/or manually importing the certificate into the user's web browsers to avoid receiving a security warning.

If VPN services are required to provide (1) remote access for users to access network resources remotely and/or (2) creating a secure connection between other sites for accessing network resources (Public or Private WAN).

Solutions Required: VPN & Remote Access

If a DMZ is required to provide a dedicated network for public facing servers (e.g. mail server, web server, FTP server) that is accessed from the outside restricting direct access into the local LAN/Data Center

Solutions Required: DMZ & Extranet

Determine what additional security features are needed or required to be enabled on the firewall component:

- **Anti-Virus:** this feature deals with looking into data packets searching for virus enabled content that is associated to a known threat. If there is a match, the data packet can be dropped.
- **File Blocking:** this feature deals with looking into files (PDF, ZIP) flowing through the firewall and allowing specific file types to pass.
- **Intrusion Protection (IPS):** this feature deals with looking into data packets searching for common patterns that is associated to a known threat. If there is a match, the IPS function can drop the data packet.
- **Endpoint Control:** provides endpoint security on the user endpoints regardless where they go. You can enforce your security policies for how they access applications and web sites on the Internet.
- **Web (URL) Filtering:** this feature deals with filtering of web pages based on a policy defined by the company.
- **Rate Limiting, Traffic Shaping:** this feature deals with rate limiting/shaping traffic to a specific bandwidth rate for a user or security policy.
- **Two Factor Authentication:** provide two levels of authentication that involve a static password and a one-time password (OTP) provided on a security token (or app). The OTP security token will provide a random generated number that you will need to enter while logging in within a specific time period.
- **DoS Protection:** this feature deals with protection of firewall network resources including devices on the network in the event of a security attack. These attacks can include port scans, floods, sweeps/discovery, and other DoS related threats.
- **Virtualization:** determine if the firewall needs to be partitioned (or virtualized) on the same physical firewall. Common for hosted networks with clients using a virtualized firewall.

Recommendations: Many of these security features commonly exist on a NGFW appliance. Many can be configured natively, however other features may require software licensing/subscriptions (e.g. Web Filtering).

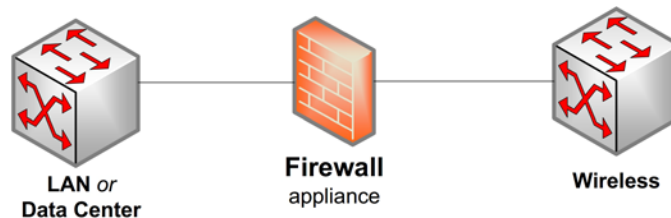
Step 5**Network Management for Firewall Solution**

Below are “Network Management Services” that should be deployed within the Firewall solution:

- SNMP
- NTP
- NetFlow
- Syslog
- RADIUS *OR* TACACS+
- Email Notification
- Management capabilities within security appliance

Step 6**Flexibility for Firewall Solution****Step 6-1****Integration with other solutions**

Determine if the solution will be deployed between other solutions based on any unique security requirements. For example, by default it is recommended to place a firewall solution between the Internet Edge and the LAN/Data Center. However, it may require placing a firewall solution between the LAN and the Data Center network or between the LAN and the Wireless network (as shown in the example below).



Step 7	Design Aspects for Firewall Solution

Step 7-1	Traffic Considerations

Most firewalls support application inspection on a firewall appliance. Understand what type of application traffic will travel through the firewall. Additional configuration may be required for the following applications to operate through a firewall appliance.

- **PPTP**, which uses GRE may require additional configuration by adding it to the application inspection list in order for PPTP VPN connections to operate correctly.
- **H.323** used for video conferencing may require additional configuration by adding it to the application inspection list in order for H.323 traffic to operate correctly.
- **SIP**: used for voice call control may require removing SIP from application inspection in order for SIP traffic to operate correctly.

Recommendations: All firewalls support some level of inspection for common applications such as HTTP, HTTPS, FTP, and SMTP, so nothing additional is needed unless unique or real-time applications are used.

Step 8	Hardware for Firewall Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

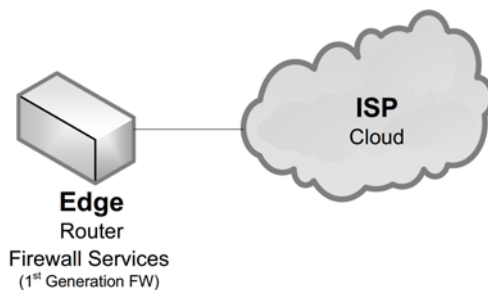
- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1	Hardware Consolidation Option

The Firewall appliance (1st Generation Firewall type) can be consolidated with the **Edge Router** located in the **Internet Edge** solution using one of the following services:

- **Access Control Lists (ACLs):** Reflexive ACL, CBAC, Zone Based Firewall, or using Standard/Extended ACLs.
- **Service Module:** Cisco Catalyst 6500/6800 Series using the ASA Service Module.

Note: Reference the "Hardware Table" for any specific hardware that may be listed for consolidation.



Or you can select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

Cisco ASA 5500-X Series *(SMB, Medium, Large)*

Performance	NGFW: 500Mbps – 1.5Gbps NGFW+IPS: 60Mbps – 600Mbps VPN: 200Mbps – 700Mbps FW+IPS: 250Mbps – 1.3Gbps 1G support	Flexibility	--
Reliability	Active/Passive, Active/Active	Management	Cisco Prime Security Manager (PRSM), ASDM
Scalability	VPN: 250 - 5000 tunnels (site, client) Virtualization: 5 - 50 instances	Security	FW, NGFW (CX), IPS, Content Security, VPN (IPSec, SSL), Identity (TrustSec, Policy), SSL Decryption
Design Aspects	Firewall Appliance (NGFW)		
Models	5512-X, 5515-X, 5525-X, 5545-X, 5555-X Licensing (AVC, Web Essentials, IPS)		

Cisco ASA 5585-X Series *(Large)*

Performance	NGFW: 2 - 13Gbps FW: 40Gbps, 320Gbps (clustered) IPS: 80Gbps 1G/10G support	Flexibility	--
Reliability	Active/Passive, Active/Active	Management	Cisco Prime Security Manager (PRSM), ASDM
Scalability	Virtualization: 250 instances	Security	FW, NGFW (CX), IPS, Content Security, VPN (IPSec, SSL), Identity (TrustSec, Policies), SSL Decryption
Design Aspects	Firewall Appliance (NGFW)		
Models	5585-X Licensing (AVC, Web Essentials, IPS)		

Cisco ASA 5505 Series *(Small)*

Performance	FW: 150Mbps IPS: 75Mbps VPN: 100Mbps	Flexibility	--
Reliability	Active/Passive	Management	ASDM
Scalability	VPN: 10 - 25 tunnels (site, client)	Security	FW, IPS, Content Security, VPN (IPSec, SSL)
Design Aspects	Firewall Appliance (1 st Gen FW)		
Models	5505 Licensing (Security Plus, AnyConnect)		

Palo Alto Networks *(SMB, Medium, Large)*

Performance	NGFW: 100Mbps - 120Gbps IPS (Threat): 50 - 60Gbps VPN: 50Mbps - 24Gbps 1G/10G support	Flexibility	--
Reliability	Active/Passive	Management	Panorama
Scalability	VPN (IPSec): 25-8000 tunnels (site, client) VPN (SSL): 25 - 120,000 tunnels Virtualization: 3-225 instances	Security	FW, NGFW, Content Security, VPN (IPSec, SSL), Identity (User-ID), SSL Decryption
Design Aspects	Firewall Appliance (NGFW)		
Models	200, 500, 2020, 2050, 3020, 3050, 4020, 4050, 4060, 5020, 5050, 5060, 7050 ; fixed/modular, PAN-OS VM-100, VM-200, VM-300 ; virtualized (VMware), PAN-OSTM Subscriptions (Threat Prevention, GlobalProtect, URL Filtering, Wildfire)		

Fortinet: FortiGate *(Small, SMB, Medium, Large)*

Performance	FW: 800Mbps - 160Gbps IPS: 150Mbps - 23Gbps IPSec VPN: 350Mbps - 100Gbps SSL VPN: 25Mbps - 6Gbps 1G/10G support	Flexibility	Wireless, DNS
Reliability	Active/Passive	Management	FortiManager
Scalability	Site VPN (IPSec): 20-10,000 tunnels Client VPN (IPSec): 250 - 64,000 tunnels VPN (SSL): 19 - 30,000 tunnels Virtualization: 10 - 500 virtual domains	Security	FW, NGFW, Content Security, VPN (IPSec, SSL), Identity, SSL Decryption, Two-Factor Authentication (using FortiTokens)
Design Aspects	Firewall Appliance (NGFW)		
Models	Standalone Firewall Appliances: FG/FWF-30D, FG/FWF-60C, FG/FWF-60D, FG/FWF-90D, FG, 100D, FG-200D, FG-240D, FG-280D-POE, FG-300C, FG-600-C, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3600C, FG-3700D, FG-3950B, FG-5001C, FG-5101C ; FortiOS Virtual Firewall Appliances (VMware, Citrix, MS Hyper-V): FG-VM01, FG-VM02, FG-VM04, FG-VM08		

#2a

Hardware Options based on Performance (Throughput)

Below is hardware options based on real-world firewall throughput (EMIX):

- Cisco ASA 5512-X: 500Mbps
- Cisco ASA 5515-X: 600Mbps
- Cisco ASA 5525-X: 1Gbps
- Cisco ASA 5545-X: 1.5Gbps

Below is hardware options based on firewall and IPS performance:

- Cisco ASA 5512-X: 250Mbps
- Cisco ASA 5515-X: 400Mbps
- Cisco ASA 5525-X: 600Mbps
- Cisco ASA 5545-X: 900Mbps



~ Solutions ~

Identity Access Control

Category: Network Solution (Security)

Prerequisite(s): LAN Solution and/or Data Center Solution

Complete the steps below for building the design for the network solution.

Step 1

Scalability for Identity Access Control Solution

Step 1-1

Determine the components for the solution

Determine the components for this solution:

- **Identity-Aware Security Appliance:** this is the main component that can provide identity access control for endpoints and users that exist on the LAN and/or Data Center. This appliance can be virtualized within the server farm or connected as a standalone appliance to the Core switch, Data Center Access switch, or a dedicated Server Farm switch that is connected off of the LAN Core.
- **Identity-Aware Network Devices:** these are switches, routers, or firewalls that support Identity-aware services (e.g. Cisco TrustSec) and can be integrated to work with the Identity-Aware Security appliance.
- **Endpoints:** these are wired or wireless endpoints that will be authenticated based on their identity. The endpoints should be connected to the access layer on the LAN/Data Center topology.

Step 1-2

Determine the vendor solution

Determine what vendor solution will be used in the environment to provide identity access control:

- **Cisco solution:** using Cisco Identity Service Engine (ISE) appliance [hardware] and Cisco TrustSec services including 802.1X and MAB
- **Fortinet solution:** using the FortiAuthenticator appliance [hardware]
- **Microsoft solution:** using Microsoft Network Policy Server (NPS) and 802.1X services

When to use: using Cisco solution

Determine which deployment model will be used based on the number of endpoints in the environment:

Standalone Deployment:

- **When to use:** the network has up to 2000 endpoints
- In this deployment, you can use a primary ISE server and a secondary ISE server to support all ISE personas (administration, policy service, and monitoring).

Redundant Deployment:

- **When to use:** the network has between 2,000 and 10,000 endpoints
- In this deployment, you need to divide the ISE personas across multiple appliances to support up to 10,000 endpoints. The personas can be divided out and provide redundancy based on the following:
 - o Primary ISE Administration and Policy service Server
 - o Secondary ISE Administration and Policy service Server
 - o Primary ISE Monitoring Server
 - o Secondary ISE Monitoring Server

Step 2	Reliability for Identity Access Control Solution

Step 2-1	Redundancy consideration for solution

Depending on the hardware for the component, determine the redundancy options available (if any). It will either provide Active/Passive or Active/Active Redundancy.

Active/Passive provides redundancy as a primary and secondary set. One device is active while the other device is in standby monitoring the operating conditions of the primary device and ready to transparently takeover when a failure occurs.

Active/Active provides both redundancy and load balancing operations where both devices are active.

Other options may include a **fail-open** if there is a failure. This means they will allow everything to pass through without security inspection.

Step 3

Performance for Identity Access Control Solution

Follow the steps below to determine the bandwidth services for the solution.

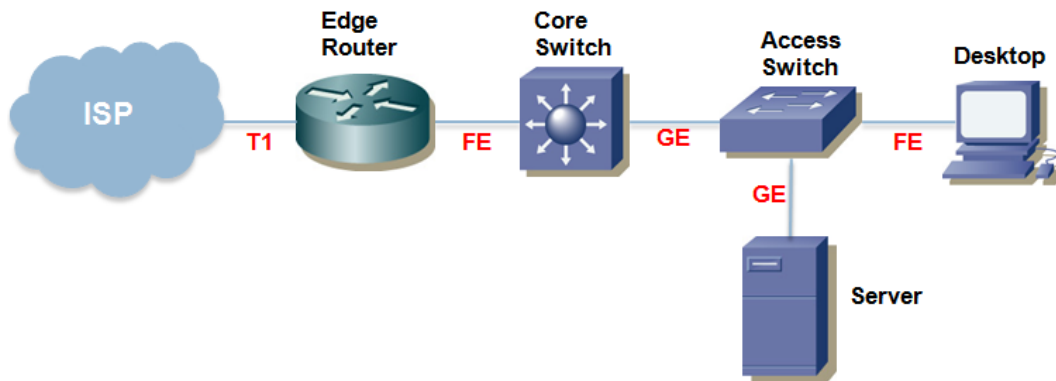
Step 3-1

Determine bandwidth services

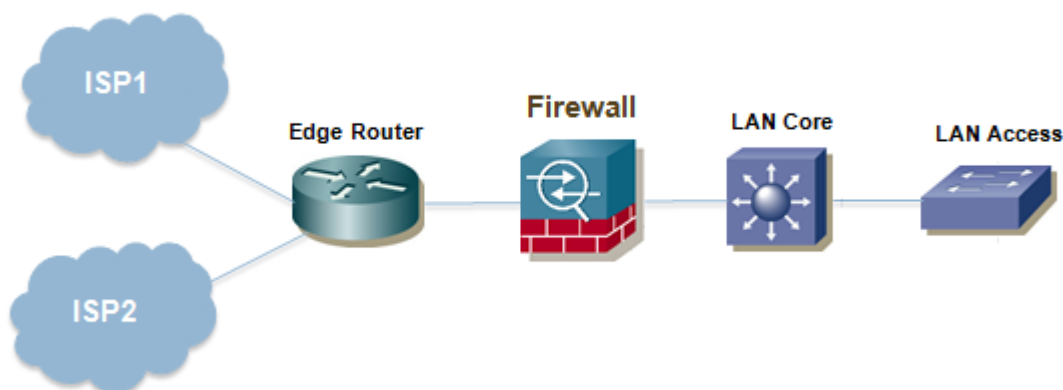
Determine the bandwidth service that is required for each component for the solution based on what exist in the topology. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)
- 10-Gigabit Ethernet (10Gbps)

For example: below is a network design that involves two foundation solutions (LAN and Internet Edge). You will see the bandwidth identified for all connections in the diagram.



Now let's add the firewall/VPN component in-line between the Internet Edge router and the Core switch. The bandwidth service used between these devices is Fast Ethernet (FE). Therefore, the bandwidth services required for the firewall component's interfaces will also be Fast Ethernet (at a minimum).

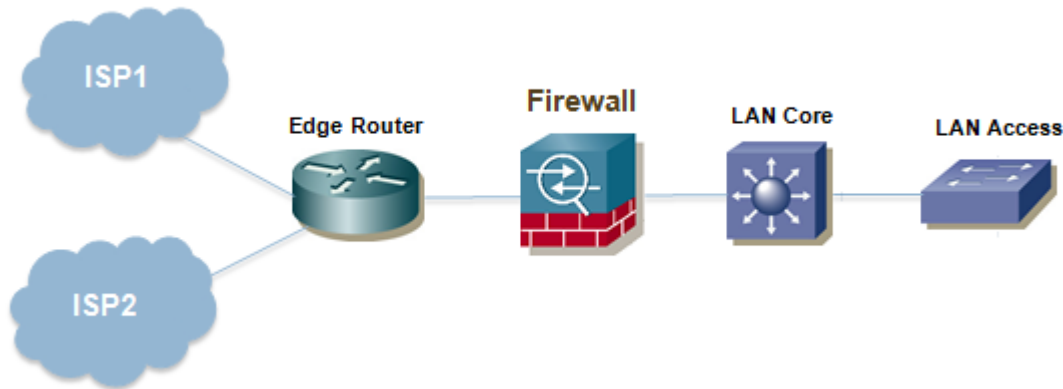


Next determine the required throughput expected through the solution component. This is based on the actual data flow and determining the lowest bandwidth service along the path. The following needs to be determined:

1. **Data Flow:** determine the expected data flow for certain services and applications through the network. For example, for Internet access the flow of data can occur from the LAN switches through the firewall, the edge router (if applicable), and out to the Internet.
2. **Bandwidth Services:** determine the bandwidth service that is used for all connections on the network along the data flow path.
3. **Lowest Bandwidth:** determine the lowest bandwidth service along the data path.

Performance (Throughput): based on the information gathered this will make up the throughput required for that in-line device. For example, if the bandwidth services on the LAN is Gigabit Ethernet (1Gbps), but the connection on the edge router is a T1 (1.544Mbps) then our expected throughput along the data path out to the Internet needs to be around 1Mbps.

Example: in the diagram below we want to determine the throughput needed on the security appliance (ISE):



If the bandwidth between the Edge router and the LAN Core is Fast Ethernet, then the security appliance interfaces need to be Fast Ethernet (at a minimum). However, understanding what the performance should be for identity services is important. We might not need the security appliance to do identity services at 100Mbps. Also in the diagram let's assume that the Internet connection to ISP1 & ISP2 involves a T1 (1.544Mbps). With those details we can complete the three steps required to understand the throughput requirements for the security appliance:

1. The data flow will happen from the LAN out to the Internet (and vice versa) moving through the security appliance.
2. Along the data path, FE is used between the Edge Router and the Core switch. Let's say that GE is used between the Core and the Access switch. And a T1 is used on the Edge router's WAN facing interface up to each ISP.
3. The lowest bandwidth service along this data path is the T1 Internet connection on the edge router.

Performance (Throughput): Therefore, the required throughput through the security appliance needs to be ~1Mbps for identity-based services and inspection.

Take note of the throughput requirements for the in-line device to determine the correct hardware model.

Determine what identity services to use for endpoint-based authentication on the network based on the following options:

1. MAC Address Bypass (MAB)
2. Profiling

#1

MAC Address Bypass (MAB)

- **When to use:** if you want the endpoint to be authenticated using only its MAC address and not be prompted to authenticate using a user account. This is common for servers or other network devices you don't want to be authenticated using a user account.
- **Description:** this option involves adding the MAC address of the endpoint into the Identity-Aware Security Appliance in order for the endpoint to bypass authentication.

#2

Profiling

- **When to use:** if you want the endpoint to be discovered for what it is (e.g. Phone, Access List) and apply a security policy based on what it is. This is common for implementing identity services with IP Phones or Access Points connected to the network.
- **Description:** this option involves setting up profiling profiles that will allow the identity-aware security appliance to pull information the identity-aware network devices to determine if the endpoint is an IP phone, an access, or maybe a Windows/Apple desktop system. Based on how the endpoint is profiled a specific security policy for that type of device can be applied to the switch port.
- **Services Required:**
 - o SNMP
 - o RADIUS
 - o CDP *AND/OR* LLDP

Determine what identity services to use that require user-based authentication based on the following options:

1. 802.1X
2. Web Authentication/Redirection

#1

802.1X

- **When to use:** if you require a user or endpoint to be authenticated using a user account (local accounts or from the existing Active Directory domain).
- **Description:** this option requires 802.1X to be enabled on the endpoint and the switch port configured for port authentication. The identity-aware security appliance also needs to be integrated with Active Directory or LDAP for user authentication.
- **Services Required:** 802.1x, RADIUS
- **System Features Required:** LDAP, Active Directory

#2

Web Authentication/Redirection

- **When to use:** for guest services and if an endpoint is not enabled for 802.1X or its MAC address not added into the identity-aware security appliance.
- **Description:** endpoints/users not enabled for 802.1X or its MAC address added into the security appliance will be redirected to a web portal for the user to authenticate before gaining access to network resources. In a Cisco solution, these guest accounts are managed through a web-based portal using a sponsor account.
- **Services Required:** RADIUS

Step 5	Network Management for Identity Access Control Solution

There are management capabilities within the solution component that will provide reporting, logs, events, and alerts for managing/monitoring the solution proactively.

Furthermore, below are the “Network Management Services” that should be deployed within the solution:

- SNMP
- NTP
- RADIUS

Step 7

Hardware for Identity Access Control Solution

Next we need to determine the hardware model that will be used for each component for the solution.

Use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

a

Identity-Aware Security Appliance

Cisco TrustSec using the Cisco Identity Services Engine (ISE) *(SMB, Medium, Large)*

Performance	GE support	Flexibility	--
Reliability	--	Management	--
Scalability	up to 5,000 – 20,000 endpoints (per server)	Security	Cisco TrustSec (MAB, Profiling, 802.1X, Web Authentication/Redirection)
Design Aspects	SXP, 802.1AE MACsec encryption		
Models	Cisco Secure Network Server 3315, 3335, 3395, 3415, 3495, Virtual Machine (VMware)		

Fortinet using the FortiAuthenticator *(SMB, Medium, Large)*

Performance	GE support	Flexibility	--
Reliability	--	Management	--
Scalability	500 – 100,000 users 25 – 10,000 user groups 50 – 10,000 Identity-Aware network devices 500 – 200,000 FortiTokens	Security	MAB, 802.1X, Web Authentication/Redirection
Design Aspects	--		
Models	FAC-200C, FAC-400C, FAC-1000D, FAC-3000D FAC-VM Base, FAC-VM-100-UG, FAC-VM-1000-UG, FAC-VM-10000-UG, FAC-VM-100000-UG		

b

Identity-Aware Network Devices

Cisco TrustSec using Cisco Hardware

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	--	Security	Cisco TrustSec (MAB, Profiling, 802.1X, Web Authentication/Redirection)
Design Aspects	--		
Models	Cisco Catalyst 2960 Plus, 2960-C, 2960-S/SF, 2960-X/XR Cisco Catalyst 3560-E, 3750-E, 3560-C, 3560-X, 3750-X, 3650, 3850 Cisco Catalyst 4500 (Supervisor 6-E, 7-E, 8-E), 4500-X Cisco Catalyst 6500 (Supervisor 32, 720, 2T), 6800-X, 6800ia Cisco Nexus 7000, 5000, 1000V Cisco ISR G2 890, 1900, 2900, 3900 Cisco 4451-X Cisco CSR 1000V Cisco ASR 1000V Cisco ASA 5500, 5500-X		

Internet Edge

Category: Foundation Solution
Prerequisite(s): LAN Solution and/or Data Center Solution

When to use: require access to the Internet (Public network).

Complete the steps below for building the design for the foundation solution.

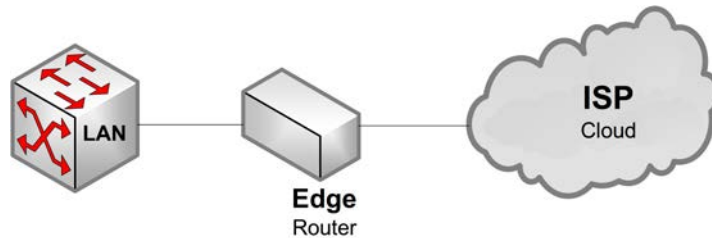
Step 1

Scalability for Internet Edge

Step 1-1

Determine topology for the Internet Edge

In the Internet Edge topology, the Edge router connects to an Internet cloud as shown below.



Here is a summary for all of the Internet Edge components and how they should be deployed:

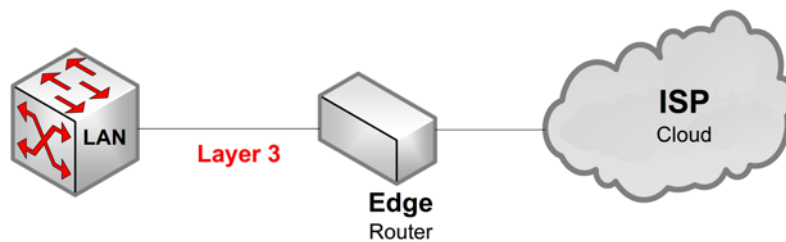
- **Edge Router:** a component that connects into the ISP cloud and the local network. The LAN facing interface on the edge router connects to the LAN/Data Center Core switch. If the ISP provides an Ethernet hand-off then a Firewall component can be used for this edge component depending on the overall requirements for the Internet Edge design (e.g. BGP).
- **ISP Cloud:** the provider network providing Internet access. The Edge Router and WAN router would connect into the ISP cloud.

Determine the Layer 2/Layer 3 Topology you want to deploy on-top of the Internet Edge topology chosen earlier. Below are the topologies to choose between.

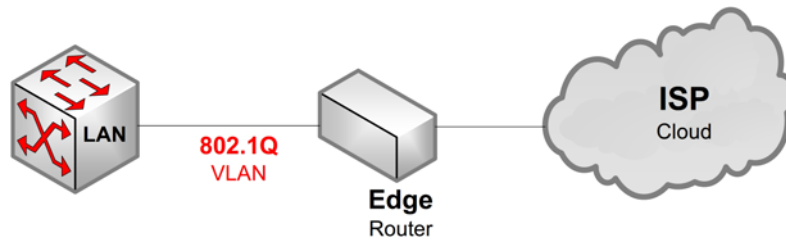
1. L3 without VLANs
2. L2 with VLANs

#1

L3 without VLANs



- **When to Use:** if you do not need to extend VLANs up to the Internet Edge and/or WAN (Aggregation, Branch) routers in the topology. A Layer 3 connection is configured with an IP subnet between the Core and the LAN facing interface on that router (Internet Edge, WAN). The routers can be configured with a routing protocol for exchanging routes with the L3 LAN/Data Center Core switch.
- **Services Required:**
 - o Routing



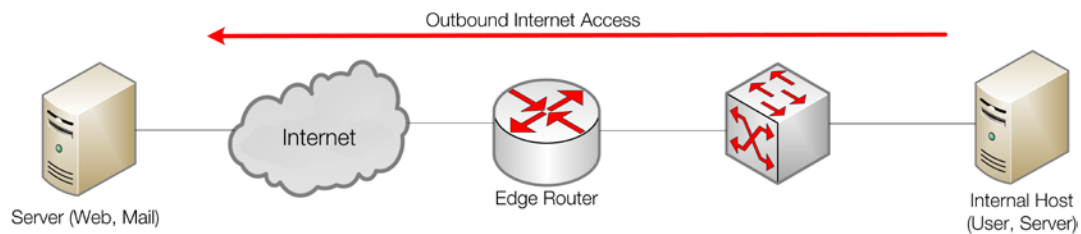
- **When to Use:** if you need to extend VLANs up to the Internet Edge and/or WAN (Aggregation, Branch) routers in the topology where multiple subnets for various networks (e.g. Guest, DMZ) can be configured on the router directly. Using multiple subnets configured as sub-interfaces is common for Small and SMB networks not using a L3 Core switch for routing between the different networks/VLANs due to cost.
- **Services Required:**
 - o VLAN
 - o 802.1Q Trunking
 - o Routing

Determine which redundancy model should be used for the Internet Edge if reliability is important. Below are the different redundancy options to choose from:

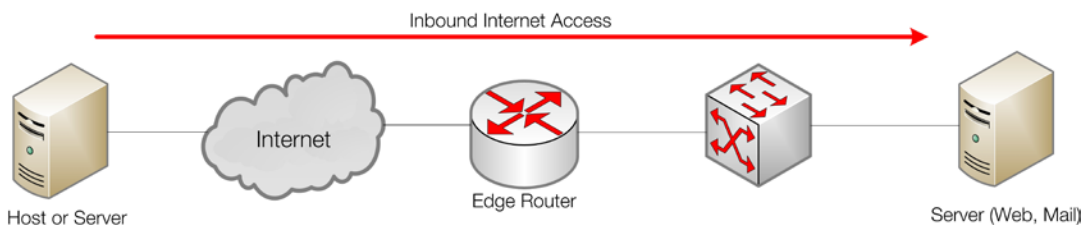
1. Two ISP using Single Edge Router (or Firewall)
2. Two ISP using Dual Edge Router
3. Full Redundancy with BGP Multi-Homing

Each of the redundancy options will include the following factors which is important to determine when to use that redundancy option. Some of these factors include:

- **Outbound Internet Access:** users and servers on the inside of the network accessing the Internet.



- **Inbound Internet Access:** how other users and servers on the Internet will access your network. This is important for public facing servers like web, email, storage to other applications.



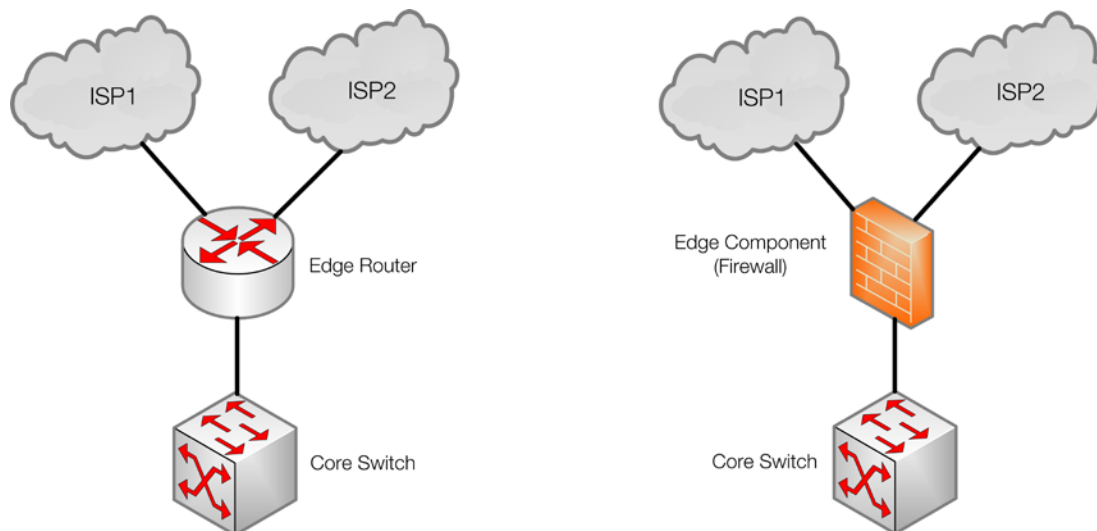
- **DNS Dependency:** for "Inbound Internet Access" are the users/server using a DNS domain name for accessing these services or using a dedicated IP address that may be configured within an application (if supported).

Description: In this redundancy option you can have one edge router connecting with two Internet providers (ISP) with two different Public subnets (one from each provider). This involves configuring two static default routes to each ISP. The secondary default route is configured with a higher administrative distance. NAT would be configured for each public subnet. The feature IP SLA can be added to provide better default gateway redundancy. In this case, the edge router would be configured for IP SLA with the primary default route only. If there is an issue/outage with the primary ISP, then the second default route would be used forcing all Internet traffic through the secondary connection. There are other options that can be used for load balancing such as IP CEF and Performance Routing (PfR).

If you are using the same provider but with two Internet connections then this redundancy option can work using the same IP subnet, if supported, but it will not help if there is a routing issue within the ISP.

Another option may involve using a firewall appliance instead of the edge router. The firewall can be configured for a "WAN failover" using IP SLA or some other similar feature. This allows the firewall to use one ISP as its primary path and the other as its secondary path. If the primary ISP goes down (or experience issues) it would automatically fail over to the second connection on the firewall.

This redundancy model provides and looks like the following:



When to use:

- **Business Size:** common for Small and SMB sized networks.
- **Public Addressing:** uses different Public IP subnets from each ISP. A single Public IP subnet cannot be used between two different ISPs.
- **DNS Dependency:** if users/server can use a dedicated IP address for accessing services within the internal network then this option can be used.
- See "**Redundancy Considerations**" for more details.

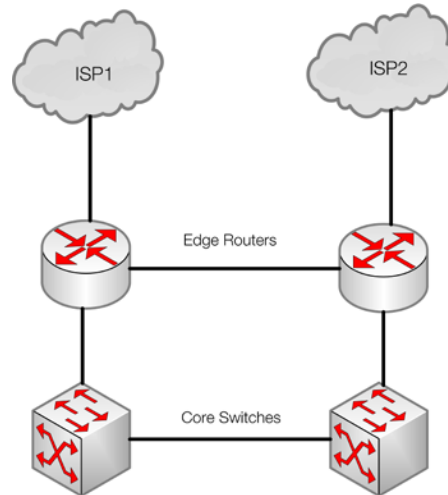
Redundancy Considerations: this option provides partial redundancy to the solution due to limitations of “Inbound Internet Access”.

- **Outbound Internet Access:** this option will provide transparent Internet redundancy for users/servers on the internal network accessing the Internet.
- **Inbound Internet Access:** this option does not provide transparent inbound Internet redundancy for host on the Internet accessing the network. This option is not ideal for environments that have a web or email server on the LAN/Data Center that require direct access from the outside. Therefore, when there is a failure, immediate DNS changes for inbound services is required. There are alternative options that can be considered to accomplish this which includes Global Load Balancing or Dynamic DNS (DDNS).
- **Single Points of Failure:** the edge router component is not redundant and is the single point of failure in this option. However, there is a higher chance of failure with the ISP itself or with the Internet connections (e.g. T1, etc.) compared to a hardware failure with the edge router.

Services Required:

- Network Address Translation (NAT)
- IP Service Level Agreements (SLA) *or* WAN Failover feature
- IP Cisco Express Forwarding (CEF)

Description: In this redundancy option we have two edge routers connecting to different Internet providers (ISP). Two separate Public subnets is used from each ISP. FHRP (using HSRP or VRRP) can be configured between the two edge routers where one is primary and the other in standby. If the Internet connection for ISP1 fails and HSRP tracking is, the secondary edge router would take over automatically routing through ISP2. The feature IP SLA can also be used in this option for further reliability between the two ISP networks. The redundancy for this option looks like the following:



When to use:

- **Business Size:** this option can be used for Small, SMB, and some Medium-sized networks.
- **Public Addressing:** uses different Public IP subnets from each ISP. A single Public IP subnet cannot be used between two different ISPs.
- **DNS Dependency:** if users/server can use a dedicated IP address for accessing services within the internal network then this option can be used.
- See “**Redundancy Considerations**” for more details.

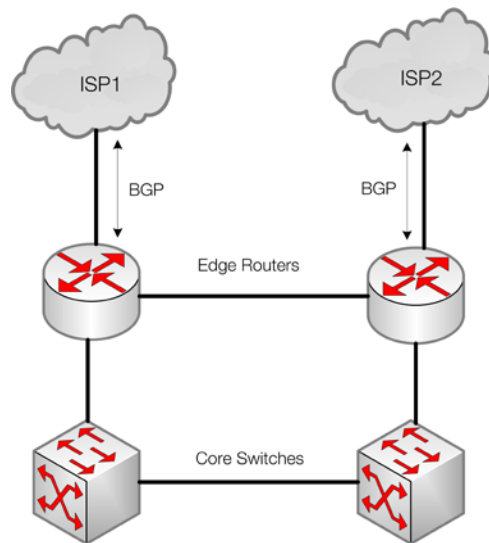
Redundancy Considerations: this option provides partial redundancy to the solution due to limitations of “Inbound Internet Access”.

- **Outbound Internet Access:** this option will provide transparent Internet redundancy for users/servers on the internal network accessing the Internet.
- **Inbound Internet Access:** this option does not provide transparent inbound Internet redundancy for host on the Internet accessing the network. This option is not ideal for environments that have a web or email server on the LAN/Data Center that require direct access from the outside. Therefore, when there is a failure, immediate DNS changes for inbound services is required. There are alternative options that can be considered to accomplish this which includes Global Load Balancing or Dynamic DNS (DDNS).
- **Single Points of Failure:** None

Services Required:

- Network Address Translation (NAT)
- IP Service Level Agreements (SLA)
- First Hop Redundancy Protocol (HSRP, VRRP, GLBP)

Description: In this redundancy option we have true Internet redundancy (inbound and outbound). We have redundant edge routers, ISPs, firewalls while utilizing the same public IP subnet through all ISP networks running BGP to provide both Internet and IP redundancy. Furthermore, BGP Attribute Local Preference should be used for outbound access and the BGP attribute AS Path Prepending or MED should be used for inbound access to the advertised subnets. FHRP (using HSRP or VRRP) is configured between the two edge routers where one is primary and the other in standby. If the Internet connection for ISP1 fails and HSRP tracking is, the secondary edge router would take over automatically routing through ISP2. The redundancy for this option looks like the following:



When to use:

- **Business Size:** this option is common for medium, large-sized networks, hosting, to service providers.
- **Public Addressing:** uses a single (or multiple) customer owned Public IP subnets between all ISP clouds. For the Public subnet(s), you need to obtain them through the ARIN website.
- **DNS Dependency:** users/server can use the DNS domain name or a dedicated IP address for accessing services within the internal network using this redundancy option.
- See "**Redundancy Considerations**" for more details.

Redundancy Considerations: this option provides full redundancy to the solution when BGP is implemented.

- **Outbound Internet Access:** this option will provide transparent Internet redundancy for users/servers on the internal network accessing the Internet.
- **Inbound Internet Access:** this option will provide transparent inbound Internet redundancy for host on the Internet accessing the network. You need to obtain a registered ASN from ARIN including having a large enough subnet that will be advertised via BGP and the equipment/memory to support the EGP routing protocol.
- **Single Point of Failure:** None

Services Required:

- BGP (IP Routing)
- IP Routing (OSPF, EIGRP) or First Hop Redundancy Protocol (HSRP, VRRP, GLBP)

Below are optional services that can provide reliability and stability to the solution:

- **Bi-Directional Forwarding Detection** to improve L3 neighbor failure detection

Below is hardware redundancy considerations that can be done for any component in the topology.

- **Hardware:** using redundant hardware is very common to provide hardware level redundancy. This may also include redundant line modules and Supervisor engines (CPU). Here is a summary for what hardware can be redundant.
 - o Device/Chassis
 - o Line Modules (using a chassis model)
 - o Supervisor Modules (using Chassis model)
- **Power:** redundant power supplies, using a UPS (like APC), and connecting to different power circuits for the network equipment.

Step 3

Performance for Internet Edge

Follow the steps below to determine the bandwidth service for all Internet connections in the design. Mark this information on the network diagram for reference. This information is important when it comes time to determine the correct hardware model.

Step 3-1

Determine the Internet Performance

Trying to determine the bandwidth for an Internet connection can be challenging because the traffic conditions cannot be easily calculated starting out. You have to establish a baseline to understand what type of traffic is typically used across your network and the amount of bandwidth utilized. This includes the number of concurrent users that typically access Internet resources at the same time. Doing all of that can take time which may not be possible for building new business network with no baseline established.

The table below will show three main groups based on the bandwidth usage for a user (low, moderate, or high). Each of these groups will list traffic services for what typically makes up low, moderate, or high traffic of volume performed by a user. You will also see an estimated bandwidth range per user that you can consider for calculating the bandwidth needed for the Internet connection.

Determine the total bandwidth needed for the edge router (WAN interface) based on the type of user and their traffic usage. Use the following table below as a reference:

User Type	Traffic Services	Bandwidth Per User
Low Performing User	Basic Email Services Basic Web Browsing Services	~90kbps
Moderate Performing User	Basic to Moderate Email Services Basic to Moderate Web Browsing Services Basic File Downloads Cloud Services VoIP Services Streaming Services (Audio, Video)	~ 130kbps to 256kbps Note: If a user will use more than one of the services from the traffic services list, you should consider a higher bandwidth rate within the bandwidth range provided.
High Performing User	Moderate to Heavy Email Services Moderate to Heavy Web Browsing Services Large File Downloads Internet Application Services Web Conferencing Services Cloud Services VoIP Services Streaming Services (Audio, Video)	~256kbps to 512kbps Note: If a user will use more than one of the services from the traffic services list, you should consider a higher bandwidth rate within the bandwidth range provided.

Design Consideration: if you are unsure of the number of low, moderate, or high performing users you can use 130kbps per user (the average baseline) which is typically used to calculate the total Internet performance.

Example: in our SMB-sized environment we will have ~140 users (or devices) that will access the Internet. We can do this from two different approaches for calculating what the Internet performance should be.

Approach #1: If we don't know how many users are low, moderate, or high performing users, we can consider the average bandwidth of 130Kbps per user. Doing the math that would be 140 users x 130Kbps. That would be ~19Mbps. This means we want to consider a bandwidth technology that can support 19Mbps or higher.

Approach #2: We can determine the estimated number of low, moderate, and high performing users. Let's say that we will have 100 low performing users that only require basic email and web browsing services. And let's say that we will have 40 high performing users based on what those users will do.

Since our high performing users has a recommended range of 256kbps to 512kbps, we need to consider how many of the traffic services will be used. Let's say that these 40 high performing users will use the following traffic services:

- Moderate to Heavy Email and Web Browsing Services
- Large File Downloads
- Cloud Services

Therefore, let's choose a bandwidth rate that is right in the middle or higher within the provided range (256kbps to 512kbps). That would be 384kbps, so that is the rate we will use for our high performing users. Doing the math, we will calculate the two groups of users then added them together:

- 100 users x 90kbps = 9Mbps
- 40 users x 384kbps = 15.3Mbps

9Mbps + 15.3Mbps = ~24Mbps for Internet Performance needed.

This means we want to consider a bandwidth technology that can support ~24Mbps or higher.

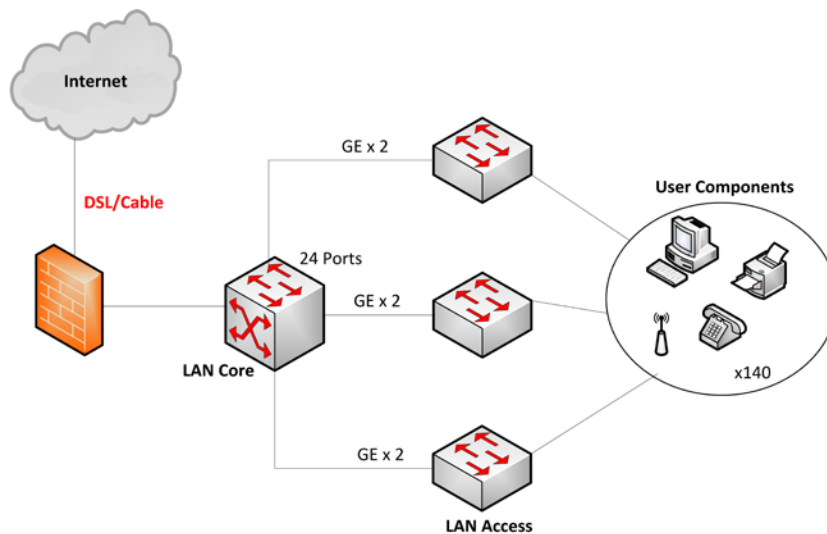
Summary: Based on the performance calculations completed for both methods, the Internet performance would range from 19 to 24Mbps that is needed for our connection in the environment.

Based on the Internet performance calculated from the last step, determine the best bandwidth technology that should be used for the edge router component (WAN facing interface).

Use the following table below as a reference to make your decision.

Bandwidth Services	Bandwidth Range	Business Size	Encapsulations	Notes
T1, E1	1Mbps – 3Mbps	Small, SMB, Medium	PPP, HDLC, Frame Relay Bundling (MLP, MFR)	--
Broadband (DSL, Cable)	10Mbps – 45Mbps	Small, SMB	ATM	--
DS-3	45Mbps	Medium, Large	ATM	--
Optical	155Mbps – 9.6Gbps	Large, Service Provider	ATM	--
DWDM	20Gbps – 400Gbps	Large, Service Provider	--	--
Ethernet (FE, GE, 10GE)	10Mbps – 100Mbps 1Gbps – 10Gbps	ALL	VLAN, 802.1Q	Recommended
Wireless (3G, 4G)	1Mbps - 10Mbps	Small, SMB	--	Backup

Example: we know that our environment requires an Internet performance ranging between 19 to 24Mbps. We want to aim for the high end of that range. Therefore, we can consider a DSL/Cable bandwidth technology for the Internet connection for our edge router component.

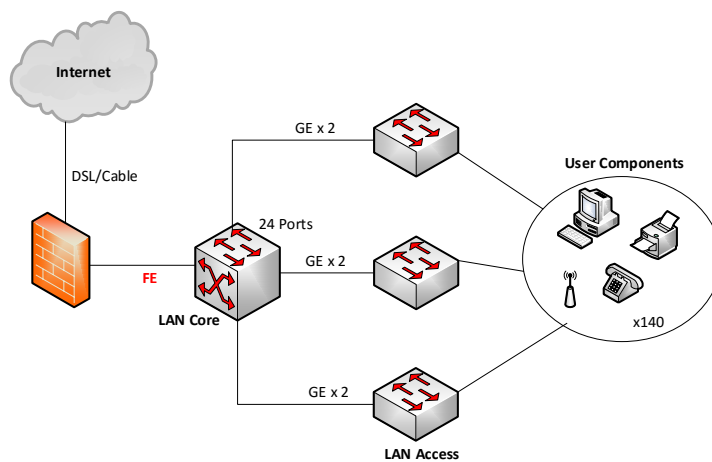


Determine the bandwidth service used between the Edge router connecting into the LAN/Data Center Core.

This is based on the bandwidth used on the Internet interface and the bandwidth must be within that range. Below are your typical bandwidth services to choose between:

- **Fast Ethernet (100Mbps):** commonly used when the Internet speed is 100Mbps or below (e.g. DSL/Cable, T1, WWAN, DS-3, Fast Ethernet).
- **Gigabit Ethernet (1Gbps):** used when the Internet speed is between 100Mbps to 1Gbps (e.g. OC-3, OC-12, Gigabit Ethernet).
- **10-GigabitEthernet (10Gbps):** used when the Internet speed is between 1Gbps to 10Gbps (e.g. OC-48, OC-192, Ten Gigabit Ethernet).

Example: if the Internet connection is using a DSL/Cable connection, then the bandwidth connection between the router/firewall and the LAN/Data Center can be a Fast Ethernet connection at a minimum.



Step 4	Security for Internet Edge

Below are Security Services/Solutions that should be deployed with the solution:

- Firewall Solution *OR* Access Control Lists (ACLs)
- Intrusion Prevention Solution
- Content Security Solution
- Security Best Practices
- Quality of Service: Policing and Markdown

Step 5	Network Management for Internet Edge

Below are "Network Management Services" that should be deployed within the Internet Edge solution:

- SNMP
- NTP
- NetFlow
- Syslog
- RADIUS *OR* TACACS+
- VTY Access

Step 6	Flexibility for Internet Edge

Step 6-1	Integration with other solutions

Below are other solutions that are be deployed with the foundation solution:

- Firewall Solution (common solution deployed with Internet Edge)
- Intrusion Prevention Solution
- Content Security Solution
- Proxy Solution

Step 7

Design Aspects for Internet Edge

Step 7-1

Other Services to include with solution

These are additional services that can be implemented (if required) within the solution.

- General Best Practices
- Multicast
- IPv6
- Virtualization (Network): L3VPN
- Medianet

Step 7-2

IP Subnets

Determine the subnet types and the number of subnets used for the Internet Edge.

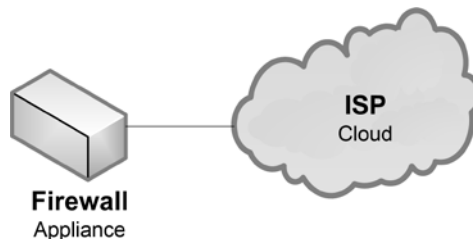
- **Public:** a subnet that is used and required to access the Internet and sharing services externally. Determine the sufficient Public address space that is needed. Smaller organizations or environments that don't heavily rely on web-based services can utilize a smaller address space. Larger organizations with heavy web-based services including email, remote-access, VPN services, and cloud-based services may utilize a larger address space.
- **DMZ:** a subnet dedicated for public facing servers isolated on a DMZ network.
- **Other:** other subnets created based on any unique requirement or preference.

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

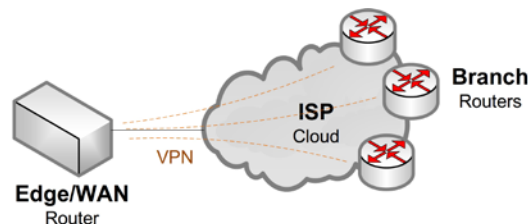
- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

The Edge router in this solution can be consolidated using one of the following:

1. **Edge router** can be consolidated with the **Firewall appliance**:
 - a. If the Edge device's WAN facing interface is Ethernet.
 - b. If you have plans for deploying a Next-Generation Firewall appliance.
 - c. Only supports the following VPN services: *IPSec (IKEv1, IKEv2)*



2. The **Edge router** can be consolidated with the **WAN router** that is using a Public WAN (Internet) cloud.
 - a. Supports the following VPN services: *DMVPN, FlexVPN, and IPSec (IKEv1, IKEv2)*



Or you can select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

Cisco ISR 4000 Series *(Large)*

Performance	IMIX: 980Mbps – 1Gbps T1/E1, T3/E3, Serial, xDSL, GE, 10GE support	Flexibility	Voice (CME, CUBE, SIP, SRST), Optimization (WAAS)
Reliability	--	Management	SDN (Cisco onePK), ISR-AX (monitoring services)
Scalability	--	Security	Firewall, VPN
Design Aspects	L3, AVC		
Models	Hardware: 4451, 4431, 4351, 4331, 4321 ; fixed/modular Defaults: Four built-in 10/100/1000 Ethernet ports Modules: Cisco Enhanced Services Module (SM-X), Cisco Network Interface Modules (NIMs) Software/OS: Universal IOS XE, ISR-AX (Application Experience) Licensing: Performance, Security, Voice, Application Experience (AX)		

Cisco ISR G2 3900 Series *(Medium, Large)*

Performance	IMIX: 100 – 350Mbps T1/E1, T3/E3, 4G/LTE, DSL, GE support	Flexibility	Voice, Messaging, UCS E-Series, Optimization (WAAS)
Reliability	--	Management	--
Scalability	20 sites (3925)	Security	Firewall, VPN, IPS, Content Security
Design Aspects	L3, Video, Medianet		
Models	Hardware: 3945, 3945E, 3925, 3925E ; fixed/modular Software/OS: Cisco IOS Licensing: IP Base, Security, Unified Communications, Data		

Cisco ISR G2 2900 Series *(SMB, Medium)*

Performance	IMIX: 25 – 75Mbps T1/E1, T3/E3, 4G/LTE, DSL, GE support	Flexibility	Voice, Messaging, UCS E-Series, Optimization (WAAS)
Reliability	--	Management	--
Scalability	Up to 25 users (2911)	Security	Firewall, VPN, IPS, Content Security
Design Aspects	L3, Video, Medianet		
Models	Hardware: 2901, 2911, 2921, 2951 ; fixed/modular Software/OS: Cisco IOS Licensing: IP Base, Security, Unified Communications, Data		

Cisco ISR G2 1900 Series *(Small, SMB)*

Performance	IMIX: 15 – 25Mbps T1/E1, 3G, DSL, GE support	Flexibility	Wireless (AP), Optimization (WAAS), PoE, ePOE
Reliability	--	Management	--
Scalability	--	Security	Firewall, VPN, IPS, Content Security
Design Aspects	L3		
Models	Hardware: 1905, 1941, 1941W, 1921 ; fixed/modular Software/OS: Cisco IOS Licensing: IP Base, Security, Unified Communications, Data		

Cisco ASR 1000 Series *(Large)*

Performance	Router/FW: up to 2.5 – 100Gbps+ VPN: up to 78Gbps T1/E1, T3/E3, GE, 10GE support OC-3, OC-12, OC-48, OC-12 support	Flexibility	Voice (CUBE)
Reliability	ISSU	Management	Cisco Prime Network Analysis Module
Scalability	VPN: 8000 tunnels	Security	Firewall, VPN
Design Aspects	L3, QoS, FPM, AVC, WAN Aggregation		
Models	Hardware: 1001, 1002, 1002-X, 1004, 1006, 1013 ; chassis Software/OS: Cisco IOS XE Modules: SIP (SPA Interface Processor), Route Processor (RP1, RP2), ESP		

Hardware Notes:

- **Cisco Router Performance:** reference the Routing Performance chart for the estimated throughput and PPS (packets-per-second) for your router selection. Those numbers should only serve as a baseline for your decision. You can view the chart here: <http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf>

Internet of Things (IoT)

Category: Business Solution
Prerequisite(s): --

Internet of Things (IoT) is a solution where consumer and business products are Internet enabled. That allows users to control devices in their homes or place of business for automation or other manual control. Some IoT enabled devices includes some of the following:

- Lighting
- Kitchen Appliances (e.g. Refrigerator)
- Home Appliances (e.g. TV, Media Players)
- Gaming (e.g. XBOX, Sony, Nintendo)
- Security (Video Cameras, Locks)
- Power Cords and Adapters
- Heating and Cooling (e.g. NEST)
- Computer Peripherals (e.g. Printers, Speakers)

This is a business/consumer solution that utilizes other network solutions to allow IoT to operate. It includes one or more of the following solutions to be implemented on the network:

- **Internet Edge**
- **Wireless**

***Note:** These solutions require the LAN/Data Center solution which is important for the foundation.*

Intrusion Prevention

Category: Network Solution (Security)

Prerequisite(s): LAN and/or Data Center Solution, Internet Edge Solution

Complete the steps below for building the design for the network solution:

Step 1

Scalability for IPS Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

1. **IPS/IDS Appliance:** the component in this solution is an IPS security appliance.
2. **Management:** this component is a server that exist in the server farm for managing the security appliance(s).

Step 1-2

Choose how components will be deployed

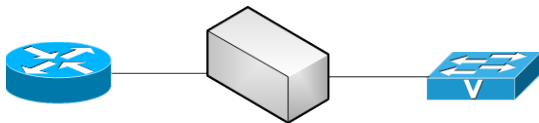
Determine how each component for the solution will be deployed.

#1

IPS/IDS Appliance

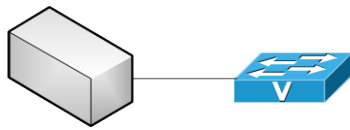
This component is usually deployed in-line between the LAN/Data Center solution and the Internet Edge solution. But it can also be deployed between other solutions where needed.

The picture below shows how the component can be deployed IN-LINE between different solutions (e.g. LAN/Data Center, Internet Edge).



The component can also be deployed out-of-band connected to an edge switch behind the edge router or connected to any of the Core/Distribution/Access layers enabled for port monitoring. Most environments will commonly use an in-line deployment if traffic conditions are moderate, but it depends on the IPS/IDS performance of the appliance. If there is large amounts of traffic coming in from many interfaces (e.g. 100+) then using an out-of-band deployment is more commonly used. The IPS appliance can also be added within a LAN and/or Data Center network itself for advanced network inspection.

The picture below shows how the component can be deployed OUT-OF-BAND on the network:



In this deployment, one of the component's interfaces is plugged directly into a L2/L3-switch like any other IP enabled device (e.g. router, server, desktop, access point).

#2

IPS/IDS Management Server

Any management server that works with the IPS/IDS appliances on the network should be connected into the server farm within the LAN/Data Center.

Step 1-3

Out-of-band IPS/IDS Options

If the IPS/IDS appliance will be deployed “out-of-band” on the Data Center network it can be done using one of the following options:

- **IDS Option A:** Placing the IDS appliances at the Distribution layer. This is used for spanning a lot of traffic to multiple IDS appliances to avoid packet discards. However, it will use more ports on the switch compared to option B.
- **IDS Option B:** Placing an IDS appliance at the Access layer. This will likely monitor all traffic from the uplink port towards the Core/Distribution, but packet discards are possible if traffic rates are high. If there is a lot of discards discovered then consider Option A which uses multiple IDS appliances.

Recommendations: Option A is the most common out-of-band deployment within the Data Center (or LAN Campus) which can SPAN a small group of ports to lower the overall packet discards. Packet discards are drops that happens on an interface due to saturation resulting in missed data that could be malicious.

Step 2

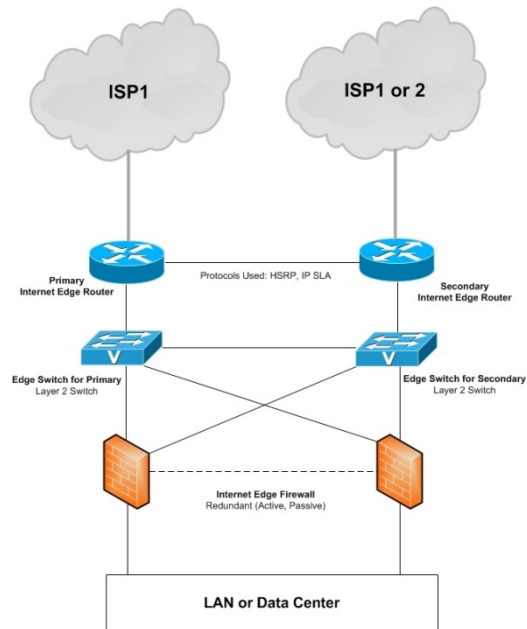
Reliability for IPS Solution

Step 2-1

Redundancy consideration for solution

IPS appliances are usually not configured in redundant pairs and will “fail-open” if there is a failure. This means they will allow everything to pass through without inspection. But IPS appliances can be placed in-line between all desired connections including backup connections that can continue to provide deep packet inspection.

Example: let’s say that our network consist of redundant edge routers and firewalls in our topology (below).



We can place an IPS appliance in-line between the “Primary Firewall and LAN” or between the “Primary Edge Router and the Primary Firewall”. No second IPS appliance is needed on the backup links between the Secondary Edge Routers or Firewalls, but we can still add an IPS appliance for that link if we want to ensure that IPS level inspection continues to operate even during a failure.

Step 3

Performance for IPS Solution

Follow the steps below to determine the bandwidth services for the IPS solution.

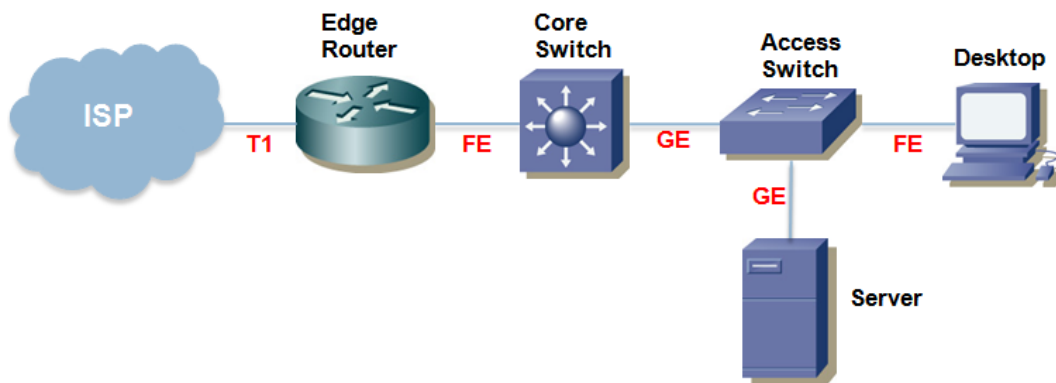
Step 3-1

Determine bandwidth services

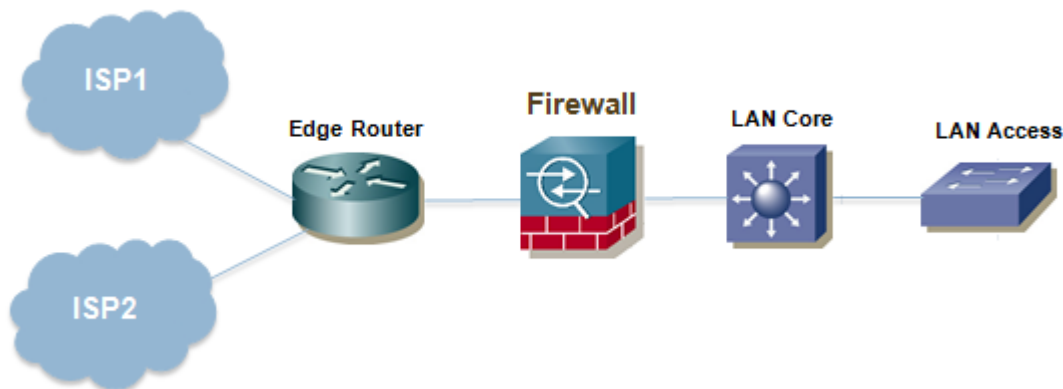
Determine the bandwidth service that is required for each component for the solution based on what exist in the topology. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)
- 10GigabitEthernet (10Gbps)

For example: below is a network design that involves two foundation solutions (LAN and Internet Edge). You will see the bandwidth identified for all connections in the design.



Now let's add the security component (e.g. Firewall, IPS) in-line between the Internet Edge router and the Core switch. The bandwidth service used between these devices is Fast Ethernet (FE). Therefore, the bandwidth services required for the security component's interfaces will also be Fast Ethernet (at a minimum).

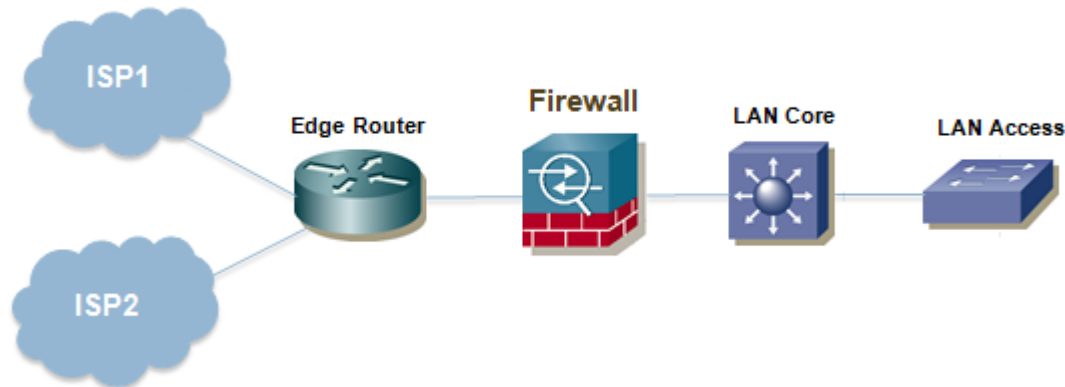


Next determine the required throughput or IPS performance expected through the IPS/IDS appliance. This is based on the actual data flow and determining the lowest bandwidth service along the path. The following needs to be determined:

1. **Data Path:** determine the expected data flow for certain services and applications through the network. For example, for Internet access the flow of data can occur from the LAN switches through the Firewall, IPS appliance, the edge router (if applicable), and out to the Internet.
2. **Bandwidth Services:** determine the bandwidth service that is used for all connections on the network along the data path.
3. **Lowest Bandwidth:** determine the lowest bandwidth service along the data path.

IPS Performance (Throughput): based on the information gathered this will make up the IPS performance required for that in-line device. For example, if the bandwidth services on the LAN is Gigabit Ethernet (1Gbps), but the connection on the edge router is a T1 (1.544Mbps) then our required IPS performance/throughput along the data path out to the Internet needs to be around 1Mbps.

Example: in the diagram below we want to determine the throughput needed on the security appliance (e.g. IPS):



If the bandwidth between the Edge router and the LAN Core is Fast Ethernet, then the security appliance interfaces need to be Fast Ethernet (at a minimum). However, understanding what the performance should be for IPS inspection is important. We might not need the IPS appliance to inspect at 100Mbps. Also in the diagram let's assume that the Internet connection to ISP1 & ISP2 involves a T1 (1.544Mbps). With those details we can complete the three steps required to understand the throughput requirements for the security appliance:

1. The data flow will happen from the LAN out to the Internet (and vice versa) moving through the security appliance.
2. Along the data path, FE is used between the Edge Router and the Core switch. Let's say that GE is used between the Core and the Access switch. And a T1 is used on the Edge router's WAN facing interface up to each ISP.
3. The lowest bandwidth service along this data path is the T1 Internet connection on the edge router.

IPS Performance (Throughput): Therefore, the required IPS performance or throughput through the security appliance needs to be ~1Mbps to handle all IPS inspection.

Take note of the throughput requirements for the in-line device to determine the correct hardware model.

Determine the IPS mode the appliance will operate in:

- **In-Line (Active) Mode:** In this mode the IPS appliance will inspect all traffic on the network. If there is any type of an attack or malicious activity it will proactively block the connection. This offers greater security protection for preventing attacks on the network.
- **Promiscuous (Passive) Mode:** In this mode the IPS/IDS appliance will only inspect traffic on the network and if there is any type of an attack it will only report back to the management server, send a log, or send an email to the security administrator. This is also called “promiscuous mode”.

Recommendations: If you are not sure which mode to use, start with Promiscuous mode for monitoring all traffic. That way you can passively view what type of traffic is normal and malicious. This will also help to understand the trending of traffic that moves through the network. Furthermore, running the IPS appliance in passive mode won't impact the availability of the network or create possible latency issues. Also most IPS services within Firewalls and Routers can provide some level of both Active and Passive modes, but start with passive monitoring. Keep in mind that you don't have to force the IPS appliance to actively drop connections on your network. However, using passive mode only is still a good option where you can use it as a tool when attacks happen, using it for auditing, and troubleshooting network/application issues.

The IPS appliance can make informed decisions based on the reputation of a traffic flow using the following mechanisms:

- **Reputation Filters:** checks to see if the packet has any IP address that has been compromised or owned by malicious groups. It will block any traffic from known bad IP addresses before any inspection is done.
- **Global Correlation Inspection:** a rating system is used for Public IP addresses in each packet based on prior behavior detected. This option should be turned off if the IPS appliance is deployed internally and only sees private IP addresses traversing through it.

Step 5	Network Management for IPS Solution

Step 5-1	Management options with solution

Determine what tools and software will be used for monitoring and managing the IPS appliance for some of the following tasks:

- **Events and Alerting:** Confirm the appropriate action if an attack is discovered by the IPS appliance such as receiving alerts via email, SMS messages, or logged depending on what capabilities are supported.
- **Signature Updates:** Determine and make sure that new attack signatures are updated with the IPS appliance so new attacks that occur are stopped.

If you are using the Cisco IPS appliance (or IPS integrated on the Cisco ASA), it can managed using one of the following solutions/options:

- Cisco IPS Manager
- Cisco IPS Manager Express
- Cisco Prime Security Manager (CPSM)
- Cisco ASDM

Other IPS vendors will have similar options with their product.

Step 5-2	Network Management Services to include with solution

Below are the “Network Management Services” that should be deployed within the solution:

- SNMP
- NTP
- Syslog

Step 6	Flexibility for IPS Solution

Step 6-1	Integration with other solutions

Determine if the solution will be deployed between other solutions based on any unique security requirements. For example, by default it is recommended to place the IPS/IDS appliance between the Internet Edge and the LAN/Data Center. However, it may require placing an IPS/IDS appliance between the LAN and the Data Center network or between the LAN and Wireless network.

Below are other solutions that can be deployed with this solution:

- Internet Edge Solution
- Data Center Solution

Step 7	Design Aspects for IPS Solution

Step 7-1	Services to include with solution

Below are the services that are required for this solution.

- Port Monitor

Port Monitoring is used to capture packets from specified switch ports if the security appliance is deployed out-of-band. This is configured on the LAN or Data Center switches where the IPS/IDS appliance(s) will be connected. And NTP is recommended to use a time server via NTP for accurate timestamps on IPS/IDS related events captured

Step 7-2	Network Participation

When security threats are detected by the IPS appliance, that data can be sent to a Global Correlation database (Cisco SensorBase network or equivalent) located in the cloud in order to increase reputation fidelity. Below are some of the modes that can be used:

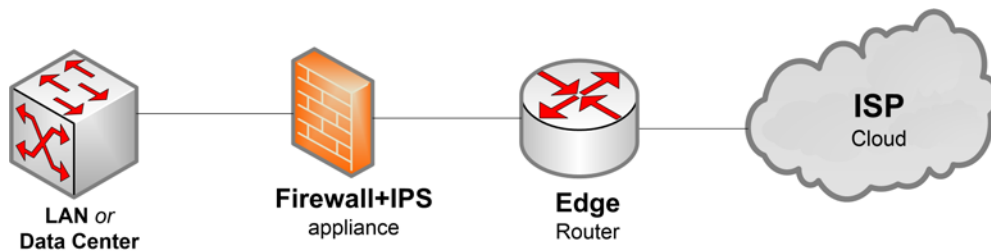
- **No Participation (Off):** IPS appliance does not collect data and does not communicate with the Cisco SensorBase network.
- **Partial Participation:** IPS appliance can collect data, statistics, and communicate with the Cisco SensorBase network. However, data that is considered sensitive is not sent.
- **Full Participation:** IPS appliance can collect data, statistics, and all data is sent to the Cisco SensorBase network.

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

The IPS/IDS appliance can be consolidated within the **Firewall appliance** (Firewall Solution) or the **Edge Router** located on the **Internet Edge** using one of the following services:

- Using the Firewall Appliance (Firewall) installed with a Security Module (e.g. Cisco AIM, SSM) – this is the most common consolidation option:



- Using the Edge Router (Internet Edge) configured with IPS Services
- **Service Module:** Cisco Catalyst 6500/6800 Series using the IPS/IDS Service Module

Note: Reference the "Hardware Matrix Table" for any specific hardware that may be listed for consolidation.

Or you can select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

Cisco ASA 5500-X Series *(SMB, Medium, Large)*

Performance	NGFW+IPS: 60Mbps – 600Mbps FW+IPS: 250Mbps – 1.3Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	--	Security	IPS
Design Aspects	Firewall Appliance		
Models	5512-X, 5515-X, 5525-X, 5545-X, 5555-X Licensing (AVC, Web Essentials, IPS)		

Cisco ASA 5585-X Series *(Large)*

Performance	IPS: 80Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	--	Security	IPS
Design Aspects	Firewall Appliance		
Models	5585-X Licensing (AVC, Web Essentials, IPS)		

Cisco ASA 5505 Series *(Small)*

Performance	IPS: 75Mbps	Flexibility	--
Reliability	--	Management	--
Scalability	--	Security	IPS
Design Aspects	Firewall Appliance		
Models	5505		

Palo Alto Networks *(SMB, Medium, Large)*

Performance	IPS (Threat): 50 – 60Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	--	Security	--
Design Aspects	Firewall Appliance		
Models	200, 500, 2020, 2050, 3020, 3050, 4020, 4050, 4060, 5020, 5050, 5060, 7050 ; fixed/modular, PAN-OS VM-100, VM-200, VM-300 ; virtualized (VMware), PAN-OSTM Subscriptions (Threat Prevention , GlobalProtect, URL Filtering, Wildfire)		

Hardware Notes:

- **Cisco IME (IPS Manager Express):** (1) manage up to 5 Cisco IPS sensors from a single GUI interface

Below is hardware options based on the average inspection throughput of the IPS appliance:

- **Cisco IPS 4345 Sensor:** 750Mbps
- **Cisco IPS 4360 Sensor:** 1.25Gbps
- **Cisco IPS 4510 Sensor:** 3Gbps
- **Cisco IPS 4520 Sensor:** 5Gbps

Below is hardware options based on firewall and IPS performance:

- **Cisco ASA 5512-X:** 250Mbps
- **Cisco ASA 5515-X:** 400Mbps
- **Cisco ASA 5525-X:** 600Mbps
- **Cisco ASA 5545-X:** 900Mbps



~ Solutions ~

Local Area Network (LAN)

Category: Foundation Solution
Prerequisite(s): --

Complete the steps below for building the design for the foundation solution:

Step 1

Scalability for LAN

Step 1-1

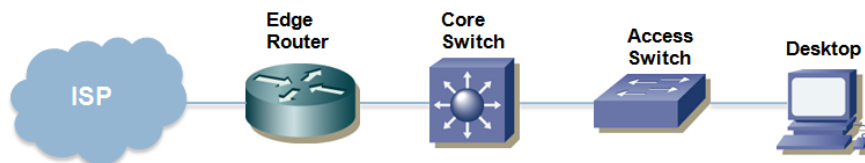
Choose a topology for the LAN

Determine the topology for the LAN solution. This is the actual look for what the solution will physically look like. Choose the topology that closely matches what is applicable to your environment and requirements. Also take note of the components in the topology whether it is a switch, a router, or some other component listed. Below are the topology tiers you can choose from:

1. One-Tier Model
2. Two-Tier Model
3. Three-Tier Model

The **most common tier-level topology is a two-tier** then a one-tier (mainly for the LAN and Data Center Solutions). Three-tier topologies, which are often discussed in networking textbooks are rarely used unless you have 100s to 1000s of nodes or buildings. I have seen cases where a 10,000 user environment with over 30,000 nodes was using a two-tier topology. The biggest reason for using a Two-Tier model is mainly due to cost and simplicity providing great reliability, scalability, and performance aspects.

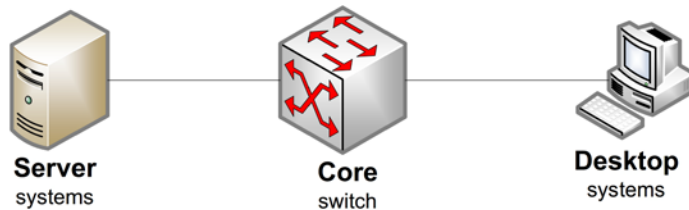
Below is an example of a network design diagram. Here it shows two foundation solutions, the LAN and the Internet Edge. The LAN is a two-tier topology consisting of a Core switch and an Access switch. The Internet Edge connects into the Core of the LAN:



#1

1-Tier Topology

One-Tier consist of one level connecting various nodes. An example of a One-Tier topology would be a LAN Collapsed Core.

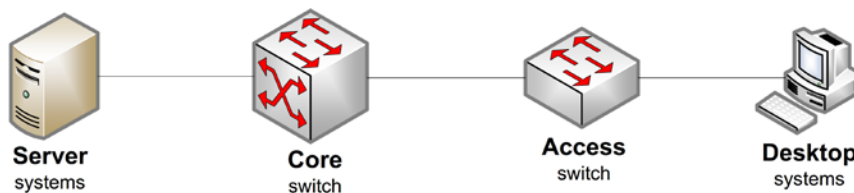
**When to use:**

- When the total devices (e.g. servers, computers, network devices) on the network are up to 48 nodes and requires a single switch.
- When using a single room (e.g. IDF, MDF, Data Center) in a single building.
- Used for the LAN at Small Branch Offices.
- Common for the LAN for Small business size networks.

#2

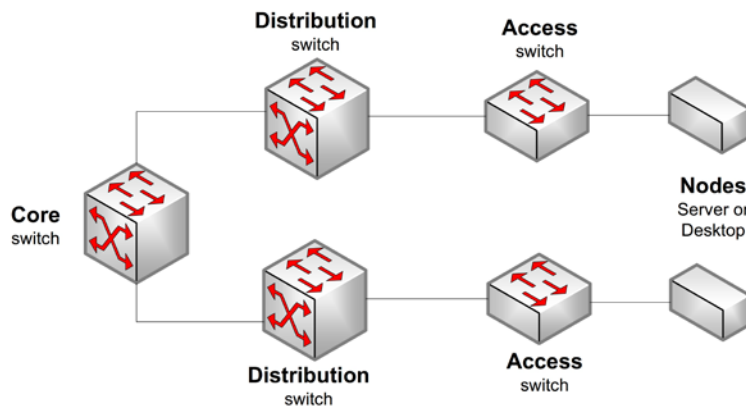
2-Tier Topology

Two-Tier consist of two levels connecting to various nodes. An example of a Two-Tier topology would be a LAN Collapsed Core connecting to a LAN Access.

**When to use:**

- Most common and recommended topology that is typically used.
- When using single or multiple rooms (e.g. IDF, MDF, Data Center) in a single building.
- Used for the LAN at Medium/Large Branch Offices.
- Common for the LAN for Small, SMB, Medium, & Large business size networks ; up to 1000 users
- To eliminate the 4:1 oversubscription ratio (uplink/downlink between Core and Distribution switches) used in a three-tier topology.

Three-Tier consist of three levels connecting to various nodes. An example of a Three-Tier topology would be a LAN Core, LAN Distribution, and LAN Access model. A Three-Tier topology is great for scalability and adding additional Aggregation/Distribution blocks to the Core when needed. Let's say that our Data Center has a Core, Aggregation, and Access layer hosting multiple server farms. What happens when your server farm and/or Data center out grows its current capacity and you need to add another distribution of server farms? Well, using a three-tier topology we simply add another aggregation switch with connected access switches to the Core allowing for easy scalability as seen in the three-tier topology below.



When to use:

- When using multiple buildings with rooms (e.g. IDF, MDF, Data Center).
- Used for the LAN for very large business size networks.
- Used for campus networks (e.g. School, Government, etc).

Recommendations: if using a three-tier topology, it's recommended to have no more than a 1000 users connected to a single distribution block (Distribution switch with connected Access switches). If it expands beyond 1000 users consider building another distribution block that will connect into the Core. Other recommendations reference 5000 users per distribution block, but that can potential create over-subscription that could lead to delay and performance issues. If the distribution block will have between 1000 to 5000 users, its best to closely monitor the hardware in terms of its performance, drops, and delay (through SNMP). If the delay, performance, and drops increase along with the increase of customer complaints over time its best to build another distribution block that many of the user can be migrated to.

Step 1-2**Identify components in the topology**

Within the topology chosen identify the components:

- Core
- Access
- Distribution

Here is a summary for each of these components:

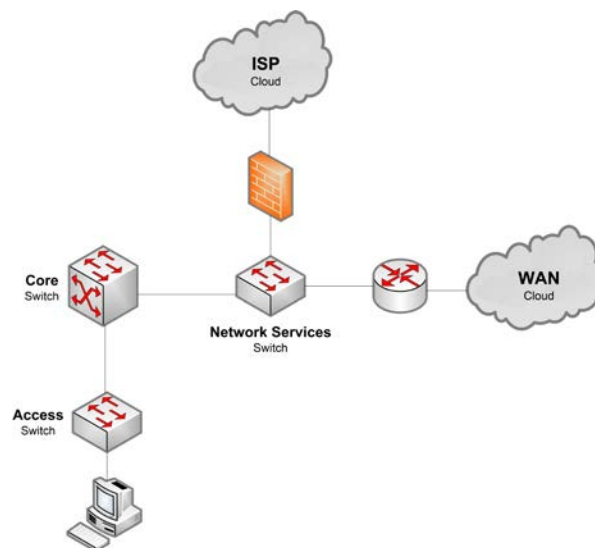
- **Core:** the backbone component in the topology where all other components connect to. Small server farms may connect into the Core directly without the use of a server farm switch.
- **Access:** the component in the topology that has connections to edge devices (e.g. computers, access points, IP phones). It has an uplink to the Core or Distribution layer switch.
- **Distribution (or Aggregation):** the component in the topology that has connections between the Core and Access layers. This can be dedicated for users or server farm aggregation blocks.

Step 1-3**Sub-Topology: Network Services Layer**

In a two-tier or three-tier topology you can add additional distribution (in a three-tier topology) or access layer (in a two-tier topology) connected off of the Core switch based on the functions it will provide.

#1**Network Services**

For larger-sized networks, you can also add a network services switch that will connect directly into the Core. The switch would be dedicated for connecting the other network solutions together such as the Internet Edge, WAN, Wireless, to other network solutions keeping the Core less cluttered and organized. Furthermore, using a network switch will minimize the number of ports needed on the Core switch. This could result in a possible cheaper switch model for the Core. Below is a sample topology for how the network services switch can be used in the existing topology tier that was determined for your design.



Determine how the topology will be deployment on the network. Below are the deployment types to choose between.

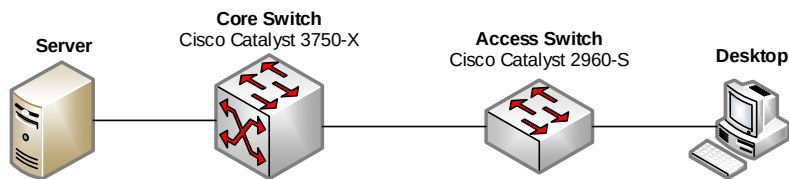
1. Traditional
2. Unified

#1

Traditional Topology

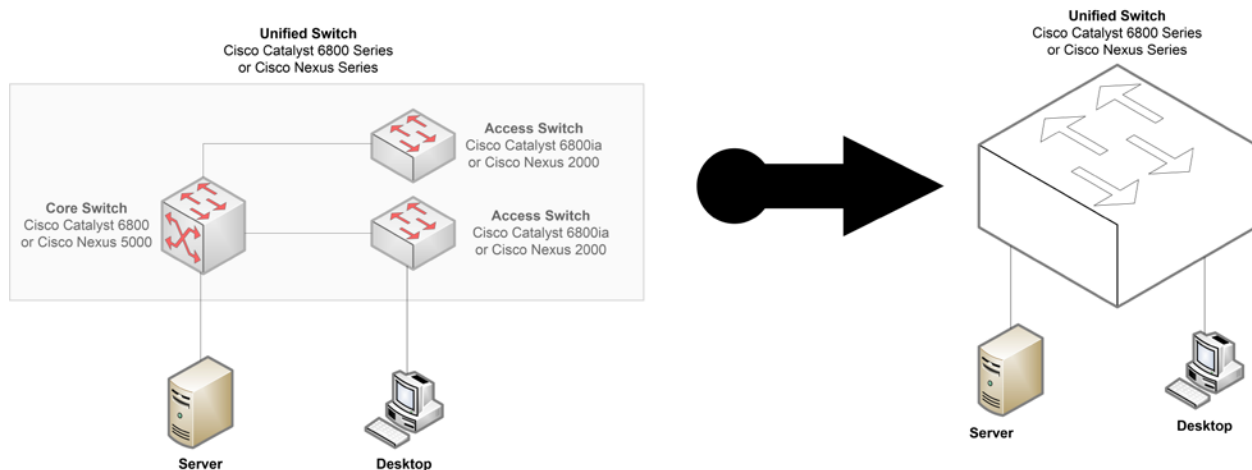
This type involves using physical standalone devices for each component in the topology. For example, let's say you have a 2-Tier topology with a Core switch and an Access switch (seen in the image below). Each of the components in the topology would be separate switch you would need to configure in the network individually. This is a legacy deployment type that is common for Small and SMB sized networks or environments using legacy hardware. Consider the following when selecting this deployment type:

- **Business** Size: Small, SMB, Medium, Large
- **Hardware** (examples): Any network hardware (e.g. Cisco Catalyst 6800, 4500, 2960).
- **Topology**: 2-Tier, 1-Tier, 3-Tier

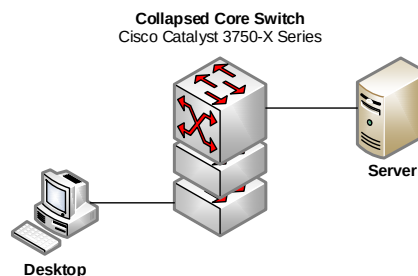


This is a next generation deployment type that deals with consolidating all of the components into the topology as one logically network component. This can be accomplished using a Chassis/Stack based switch or using the next generation unified capability. For example, let's say you have a 2-Tier topology with a Core switch and an Access switch (seen in the image below). In a Unified deployment type, the individual access switches are consolidated or treated as individual line modules to the Core switch. If we are using a 1-Tier topology (Collapsed Core) then all of the access switches are consolidated as physical line modules or bundled together on the Core switch. In either option, it would logically be seen as a single component that is unified internally. This allows the entire configuration to be done directly on the Core switch instead of each individual access switch in the environment. The Unified deployment option is recommended for Medium to Large networks running the latest hardware (e.g. Cisco Catalyst 6800, Cisco Nexus 5000 & 2000 Series). The Unified chassis/stack-based deployment option is common for Small, SMB, and some Medium sized networks using a 1-Tier topology model. Consider the following when selecting this deployment type:

- **Unified Option**
 - o **Business Size:** Medium, Large, Data Center
 - o **Hardware** (examples): Cisco Catalyst 6800/6800ia Series, Cisco Nexus 5000/2000 Series
 - o **Topology:** 2-Tier, 3-Tier



- **Chassis/Stack Option**
 - o **Business Size:** Small, SMB, Medium
 - o **Hardware** (examples): Cisco Catalyst 6800/4500 (Chassis), Cisco Catalyst 3750-X (Stack), Cisco Small Business 300 (Stack)
 - o **Topology:** 1-Tier

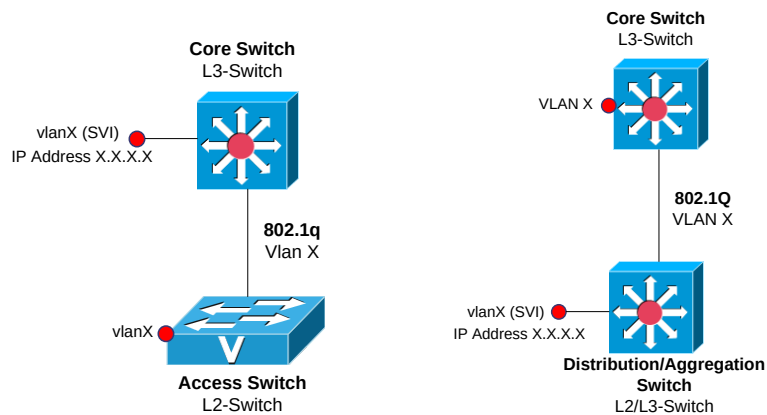


Determine the Layer 2/Layer 3 Topology you want to deploy on-top of the LAN topology chosen earlier. Below are the topologies to choose between.

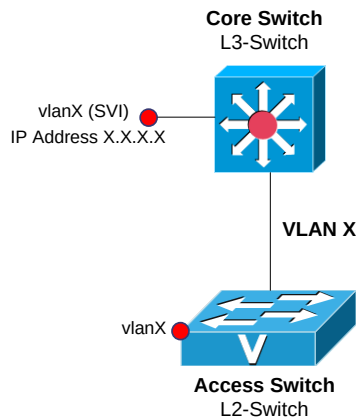
1. L3 Core/Distribution & L2 Access using 802.1Q
2. L3 Core/Distribution & L2 Access using VLAN
3. L3 Core/Distribution & L3 Access

#1

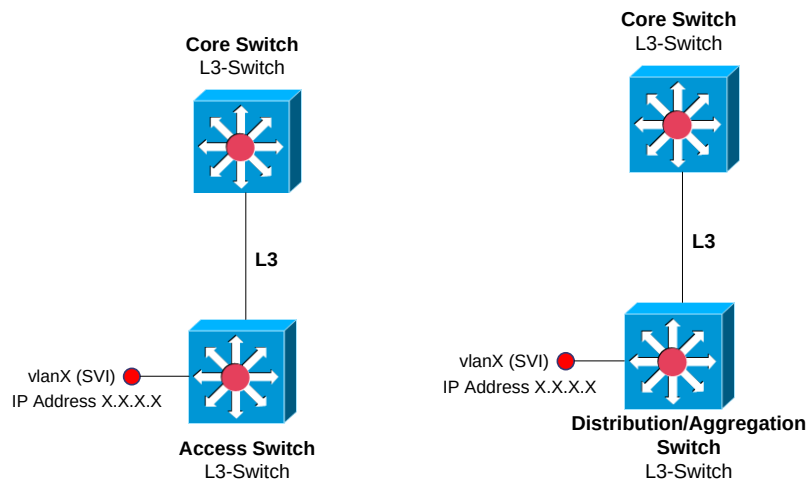
L3 Core/Distribution & L2 Access using 802.1Q



- **When to Use:** this is the most common L2/L3 topology. If VLANs will be extended across the network this is the topology model to use especially if Voice and Wireless solutions will be used. If service modules will be used at the Core (or Distribution/Aggregation) layer this topology is also required since the service modules heavily rely on VLANs for its various components.
- **Description:** In this topology, layer 2 loops will exist if using redundant hardware and links, therefore, it is required to implement the Spanning Tree Protocol. This sub-topology allows VLANs to be extended anywhere on the network.
- **Device Components:** the Core/Distribution switch in the topology would be L2/L3 device configured for routing and VLANs/802.1Q. The access switch would be a L2 device. The interconnection between these components would be an 802.1Q connection (use Trunk Security for what VLAN tags should be extended).
- **Services Required:**
 - o Routing
 - o Virtual LAN (VLAN)
 - o Trunking (802.1X)
 - o Spanning Tree Protocol



- **When to Use:** each Access layer switch exist in a single VLAN not enabled for 802.1Q Trunking not allowing multiple VLAN tags to pass. This creates more of a physical design than a logical design that can consist of multiple VLANs/networks. If you don't want VLANs to be extended across the network and/or if you are using a L2 access switch not configured for any VLANs or 802.1Q this is the L2/L3 topology to use. A single VLAN is configured on the L3 Core and the VLAN is assigned to the downlink port of the connected access switch.
- **Description:** In this topology, layer 2 loops will exist if using redundant hardware and/or links including if the configured VLAN will be extended across the L2 network. Therefore, it is required to implement the Spanning Tree Protocol. This sub-topology VLANs are not extended across the network
- **Device Components:** the Core/Distribution switch in the topology would be L2/L3 device configured for routing and VLAN assigned to ports. The access switch would be a L2 device. The interconnection between these components would be a VLAN interface with no VLAN tagging (802.1Q).
- **Services Required:**
 - o Routing
 - o Virtual LAN (VLAN)
 - o Spanning Tree Protocol



- When to Use:** this topology is mainly chosen for administration and preference reasons for avoiding L2 configuration (or minimal L2 configuration) on the network. However, using a pure L3 networks allows a better tool set (e.g. ping, traceroutes) for troubleshooting network issues and provides faster convergence over L2 services and increase of available bandwidth to users. It also provides a single control plane focused on L3. It's an easier implementation that doesn't require matching of STP, HSRP, or GLBP priorities. There are also no L2/L3 multicast topology inconsistencies. Using L3 allows using routing protocols like EIGRP or OSPF that can reconvergence within 200ms using sub-second timers. The down side is that VLANs cannot be extended on the network creating many limitations or flexibility. Another consideration is that a mixture of L2 and L3 services can be used on the same interface. The interface can be configured as an 802.1Q interface. One VLAN can be used for routing using EIGRP or OSPF. And the other VLANs can easily be extended across the interface where they need to go. Using this method requires using L2 services which may not be an option for consideration.
- Description:** In this topology, there are no Layer 2 loops since everything across the network is Layer 3. As a result VLANs are not extended across the network. The VLANs are confined to a single switch or wiring closet.
- Device Components:** all of the components are L3 devices and the interconnection between these components would be a L3 interface.
- Services Required:**
 - o Routing
 - o Virtual LAN (VLAN)

Step 2

Reliability for LAN

Step 2-1

Choose Redundancy Model

Providing redundancy for the LAN topology deals with making either the Core or Distribution/Aggregation components redundant based on which tier level the network is using. The Access layer is usually not redundant. Desktops are not seen as critical components compared to servers. Therefore, servers may be dual-homed into two separate access switches or Core switches to provide an increased level of redundancy.

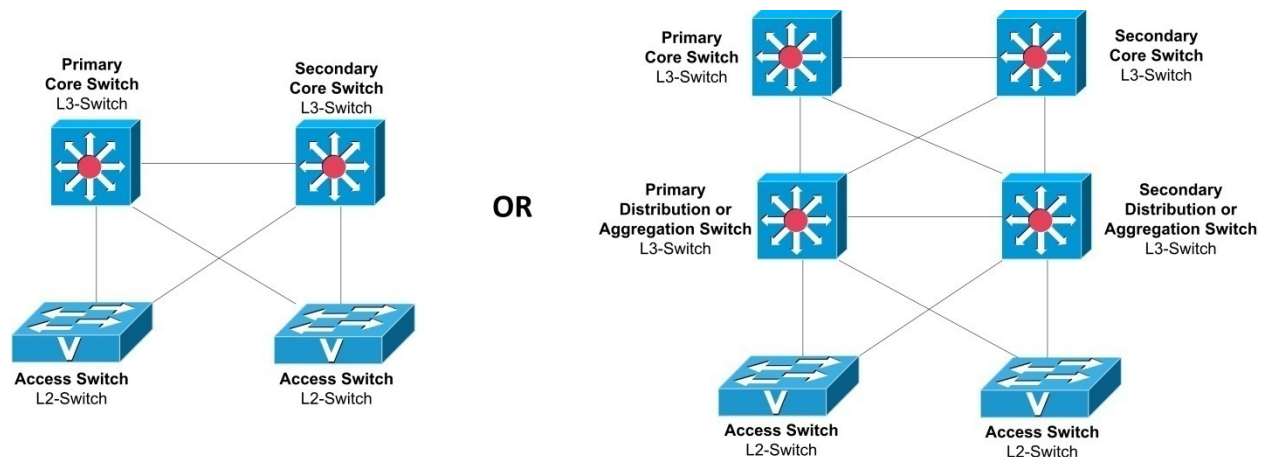
Determine which redundancy model should be used for the solution if reliability is important:

1. Traditional Redundancy
2. Resilient Redundancy

#1

Traditional Redundancy

Traditional Redundancy: this design was commonly used in the past to provide redundancy using redundant hardware for the Core/Aggregation layers. Below is what this redundancy model looks like:



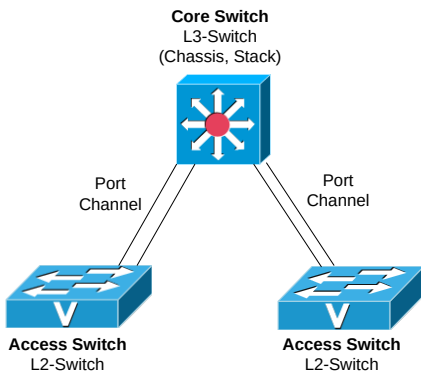
- **When to use:** using a traditional or virtualized topology for the deployment type to achieve full redundancy. This is applicable for Small, SMB, Medium, to Large business size networks.
- **Description:** in this redundancy topology, the access switches have redundant connections to a pair of redundant Core/Distribution switches. Since loops will exist in this topology, it's crucial that a Spanning Tree protocol like Rapid Spanning Tree is implemented on all L2 and L3-switch components, which will cause one of the downlink/uplink ports in the topology to be blocked. No load balancing occurs in this topology unless different root bridges per VLAN are configured on the Core/Distribution switches. It is also required that a First-Hop Redundancy Protocol is implemented that will be used by the edge devices to provide default gateway redundancy (e.g. Desktops, Servers). And all of the L3 components should be enabled routing (e.g. OSPF, EIGRP) and implemented for fast convergence.

- **Services Required:**
 - o Spanning Tree Protocol (STP)
 - o First Hop Redundancy Protocol (HSRP, VRRP, GLBP)
 - o Routing (EIGRP, OSPF, Static)

#2-1

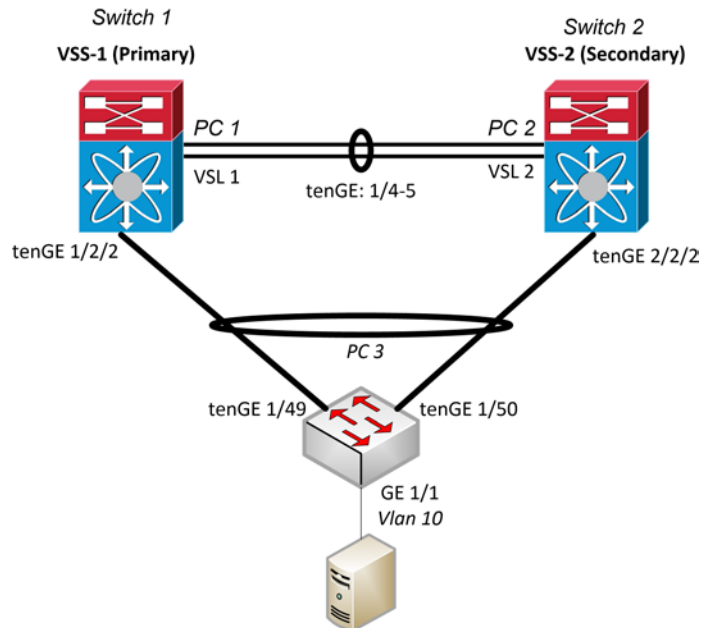
Resilient Redundancy using Unified (Chassis/Stack Option) or Traditional Deployment Types

Resilient Redundancy I: this is a new redundancy design that is ideal for next-generation networks where the Core/Aggregation layer consist of a single chassis switch or stack-based switch which includes using Port Channels with other devices. Below is what this redundancy model looks like:



- **When to use:** using a Unified (Chassis/Stack option) or Traditional topology for the deployment type to achieve redundancy. This is applicable for SMB, Medium, to Large business size networks.
- **Description:** in this redundancy topology, the Core/Aggregation layer consist of a single chassis-based switch (e.g. Cisco Catalyst 4500, 6500, 6800) or stack-based switches (e.g. Cisco Catalyst 3750-X). Port Channel can be implemented to the access switches from different line modules or stack switches on the Core/Distribution components appearing as a single logical switch from the perspective of the access switch. In this topology there are no spanning tree loops because all ports are active, but implementing Rapid STP is still recommended. Furthermore, this redundancy model doesn't require using a Default Gateway Protocol like HSRP.
- **Best Practices:**
 - o Within the stack-based switch, one of the switches operate as the master switch. The master switch should not have any uplink/downlink ports connected to it. It should be connected to the non-master switches in the stack.
 - o Set the persistent timer to "0" for the stack MAC address to ensure that the original master MAC address remains the stack MAC address after a failure has occurred.
- **Hardware Required:**
 - o Using Chassis-based (e.g. Cisco Catalyst 6800) or Stack-based hardware (e.g. Cisco Catalyst 3750-X Series).
- **Services Required:**
 - o Spanning Tree Protocol (STP)
 - o Port Channel (802.3ad)

Resilient Redundancy II: this is a new redundancy design that is ideal for next-generation networks where redundant Core/Aggregation switches are configured to act as a single logical switch that the access switches can connect to using a Port Channel connection.



- **When to use:** using a Unified (Unified option) or traditional topology for the deployment type to achieve redundancy. This is typically deployed for Medium and Large business size networks.
- **Description:** in this redundancy topology, redundant Core/Aggregation switches can be clustered together to appear as one logical switch using VSS or vPC depending on the hardware used. Port Channel can be implemented from the two redundant Core/Distribution switches to a single access switch increasing the overall availability for the connected hosts on the access switch. The access switch will assume it is connected to a single Core/Distribution switch.
- **Services Required:**
 - o Virtual Switching System (VSS) *OR* Virtual Port Channel (vPC)
 - o Port Channel (802.3ad)

Below are other services that can provide reliability and stability to the solution:

- Broadcast Suppression
- Unidirectional Link Detection (UDLD)
- Loop Guard
- NSF and SSO
- In-Service Software Upgrade (ISSU)
- Layer 2 Multi-Path (L2MP)
- Bi-Directional Forwarding Detection to improve L3 neighbor failure detection
- Flex Link

Below is hardware redundancy considerations that can be done for any component in the topology.

- **Hardware:** using redundant hardware is very common to provide hardware level redundancy. This may also include redundant line modules and Supervisor engines (CPU). Here is a summary for what hardware can be redundant.
 - o Device/Chassis
 - o Line Modules (using a chassis model)
 - o Supervisor Modules (using Chassis model)
- **Power:** redundant power supplies, using a UPS (like APC), and connecting to different power circuits for the network equipment.

Step 3

Performance for LAN

Determine the bandwidth service applicable for all connections and ports in our design. This section provides the resources to determine the bandwidth services and performance that will be used for the various ports in the solution. Mark this information on the network diagram for reference. This information is important when it comes time to determine the correct hardware model.

Step 3-1

Determine the number of edge ports

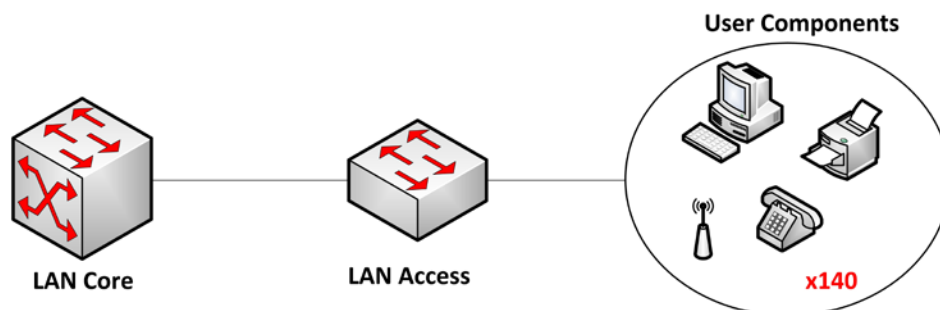
Determine the total number of edge ports that will be used on the network for each computer room (IDF, MDF, Data Center, Lab). The components that would typically plug into an edge port are desktops, laptops, printers, IP phones, and wireless access points. These devices usually connect into the access layer of the LAN.

Choose the number of edge ports based on the performance (low and/or high) of the user components that will be connected:

- **Low Performing:**
 - o User Desktop, Laptop ; common for most users
 - o Basic Printer2
 - o Basic IP Phones
 - o Wireless Access Point
 - o Other IP-enabled devices ; include Break rooms, Labs, Classes
- **High Performing:**
 - o User Desktop, Laptop
 - o Wireless Access Point (802.11n, 802.11ac)
 - o Advanced Printers
 - o Advanced IP Phones

To help you with this calculation you can determine the total number of patch panel ports that will be terminated to the computer room for a section or quadrant where computers and printers may be located. For example, a patch panel may have 50 ports (maybe 100 ports if two ports are terminated to each office or cubicle).

Example: Let's say that our LAN design will use a 2-tier topology. All edge ports will be low performing ports which is common for most environments. Therefore the total number of edge ports will be 140 ports (desktops, printers) that will connect into our LAN Access (in IDF1) shown below:



Step 3-2**Determine additional edge ports**

With the total number of edge ports (user and/or server components) calculated consider the following for additional ports to add to this total:

- Potential scalability of additional edge ports by adding at least 15-20% (or higher if necessary) more ports
- Potential redundancy used by network devices by adding between 10-15% more ports.

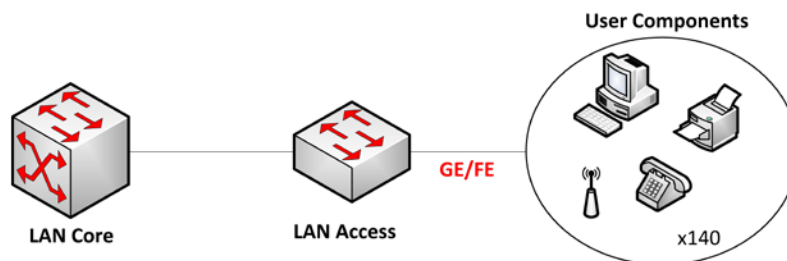
Step 3-3**Determine bandwidth technology for edge ports**

With the total number determined, what would be the bandwidth used for those edge ports (per computer room)? It will use one of the following technologies:

- **Fast Ethernet (100Mbps):** used for low performing devices such as desktops, IP Phones, and Printers on the network with minimal traffic or no backup usage on the NIC.
- **Gigabit Ethernet (1Gbps):** used for low or high performing devices connected into the network that may include backup, replication, and heavy file downloading. This is common for most desktops and some servers.

Note: Low performing and high performing only means the average bandwidth throughput that will be used by that device. So we can have a low performing desktop that has a GE NIC and connected as GE to the switch. But the user may only be using 5-10Mbps most of the time or rarely reaching up to 100Mbps.

Example: continuing with our 2-tier topology, the 140 desktops (low/high-performing) & printers will use Fast Ethernet/Gigabit Ethernet ports.

**Step 3-4****Determine bandwidth media for edge ports**

For the bandwidth service determined for the edge ports what media will be used:

- **Copper:** the most common and recommended media type to use for user edge ports. It's recommended to use CAT6 cabling.
- **Fiber:** this is used for servers/desktops that may only support fiber NICs, but Copper GE is common and recommended over using Fiber for GE unless the desktop/server is separated across a long distance that may require multi-mode or single-mode fiber connections.

Example: In our example, all of the edge ports will use Copper (FE, GE) ports, so that will be needed for our LAN Access switches.

Applicable for LAN Access with User Components connected.

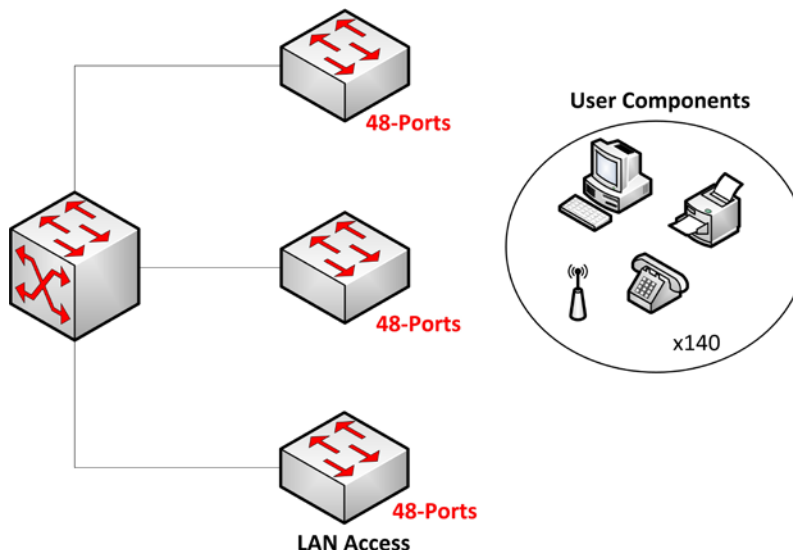
Now we need to divide the number of edge ports into individual groups (or switches) for the user/server edge port components based on the following increment values per computer room location:

- **24 Ports:** a fixed switch that provides 24 Ethernet ports. The cost is lower, but may require many 24-Port switches to meet the edge port requirements. Hence increasing the complexities and concerns for scalability.
- **48 Ports:** a fixed switch that provides 48 Ethernet ports. The cost is higher over 24-Port switches, but may require fewer switches to meet the edge port requirements decreasing the complexities and concerns for scalability.
- **48+ Ports:** a switch that can support more than 48 Ethernet ports. A chassis-based switch or a stack-based switch can be used to provide the best number of edge ports needed. The cost is higher compared to a fixed 24 or 48 port switch, but provides a minimal (maybe just one Access switch) number of switches, providing lower complexity, higher scalability, and flexibility. This option is strongly recommended over the other switch options because it keeps a nice and simple infrastructure with minimal devices to manage.

The following considerations should be kept in mind for this selection process:

- The access switches would connect up to the Core device (LAN), therefore, each port on the Core is considered as an aggregation point that needs to be considered for bandwidth.
- Consider adding additional ports for potential scalability and redundancy where needed.
- **Caution:** avoid using daisy chained switches which can cause poor performance related issues, spanning tree loops, and FHRP related issues. It is recommended to use either a chassis-based or a stack-based switch. If the LAN switches must be daisy-chained based on a unique requirement then no more than 2-3 switches should be used. In general there should be no more than 7 switches between systems on a network.

Example: we have 140 user edge ports. Therefore, for our 140 user edge ports we can use three 48-Port switches, six 24-Port Switches, or one Chassis/Stack switch. Let's focus on the 48 port switches.



For the core switch, it's important to understand the total aggregate throughput for the downlink port to the connected access switch.

Remember the access switches would connect up to the Core device (LAN or Data Center), therefore, each port on the Core is considered as an aggregation point that we need to consider for its bandwidth. In general higher the bandwidth service used on the edge port, the more bandwidth is expected on the Core. But that depends on what the utilization will be. For example, many IT administrators will use Gigabit Ethernet for a server. But why is Gigabit needed and how much of that is being utilized? Most servers may use only 20% of the bandwidth (or less) through its GE interface. Rarely at 100% due to the basic operations of TCP. You may tune the TCP options to get more bandwidth, but it's not out of the box to setup easily.

To determine the expected aggregated bandwidth per access switch downlink port the following information needs to be obtained:

- **Number of Edge Ports:** Determine the total number of edge ports that will be used on that connected access switch, which will either be 24 ports, 48 ports, or 48+ ports.
- **Bandwidth for the Edge Port:** determine the maximum bandwidth used for each edge port.

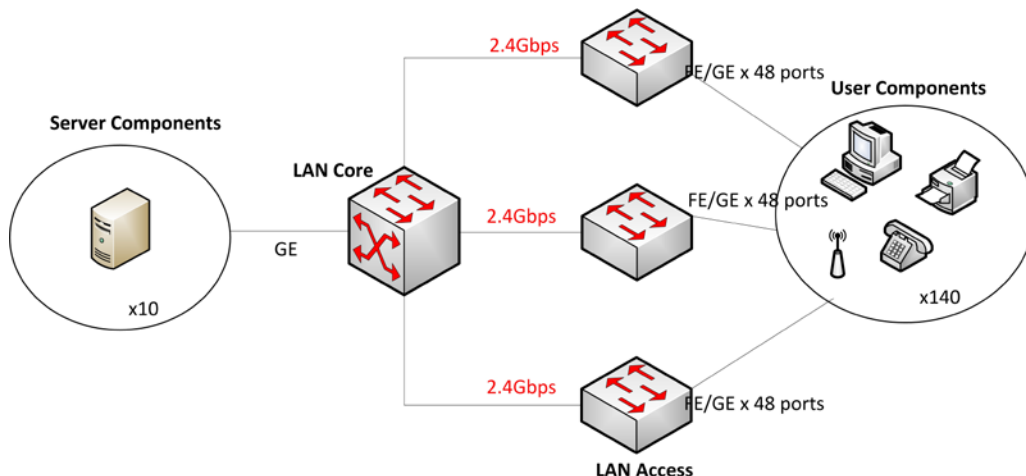
With the information gathered from the list above use the following formula to calculate the expected throughput required at each aggregated downlink port on the Core switch. The expected utilization is based on the recommended oversubscription ratio of 20:1 between the access layer and the Core/Distribution layer.

LAN: $[(\text{\# of Edge Ports per Switch}) \times (\text{Max Bandwidth per Edge Port})] / 20$

Example: continuing with our example we have 3 access switches connecting into our Core, therefore three aggregated downlink ports will exist on that Core. This throughput calculation would apply for each of these downlink ports. Focusing with one of these uplink/downlink ports we know the following:

- The total number of edge ports is 48 because we are using a fixed switch with 48 ports.
- The maximum bandwidth used per edge port will be Fast Ethernet/Gigabit Ethernet.
- The oversubscription ratio would be 20:1

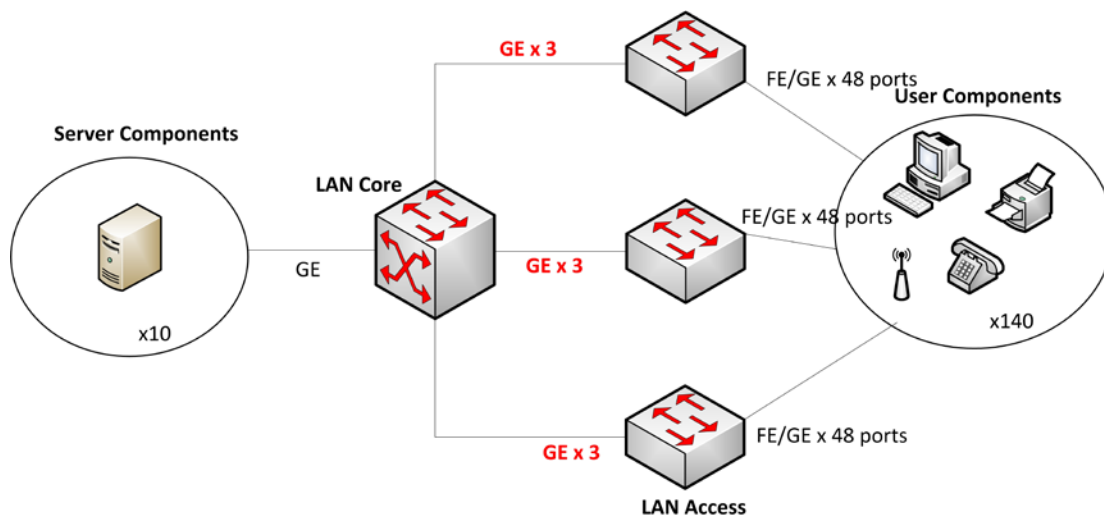
Therefore, the bandwidth for the aggregated downlink port will be 2.4Gbps ($[48 \times 1\text{Gbps}] / 20 = 2.4\text{Gbps}$)



With the bandwidth calculated in the previous step we can choose the appropriate bandwidth service for that downlink port based on the following:

- **Gigabit Ethernet (1Gbps):** common for uplink/downlink ports on the LAN switches for most networks.
- **10-Gigabit Ethernet (10Gbps):** Common for uplink/downlink ports between switches in large network environments. Provides an alternative over Port Channeling.
- **Port Channel:** Used with Ethernet connections for bundling multiple GE (up to 6) or 10GE (up to 4) connections for additional bandwidth if higher GE/10GE speeds are required on the downlink ports. Recommended to use LACP (industry standard protocol) for the port channel protocol.

Example: based on the uplink/downlink bandwidth calculated from the last step which was 2.4Gbps we can use a Port Channel with three GE interfaces up to the Core.



In this step determine the combined aggregated bandwidth (or switch capacity) for each access switch based on the number of edge ports, uplink ports, and the bandwidth technology chosen from the previous steps. This is important to help determine the best hardware to use for the access switches.

The following formula can be used to determine the minimum switch capacity (**Sc**) required for the access switch:

$$\text{Sc} : [(\# \text{ of Edge Ports}) \times (\text{Max Bandwidth per Edge Port})] + [(\# \text{ of Uplink Ports}) \times (\text{Max Bandwidth per Uplink port})] \times 2$$

Note: Ethernet ports in networks today will support full-duplex, which means each port is able to send and receive at the bandwidth rate of the switch port (e.g. 1Gbps, 10Gbps). Thus the “2” represents the full-duplex operation which doubles the bandwidth for the total switch capacity.

Example: To determine the aggregated bandwidth for one of our access switches in our topology we need to gather the required information:

- # of Edge ports = 48
- Maximum Bandwidth per Edge Port = 1Gbps
- # of Uplinks = 3
- Maximum Bandwidth per Uplink Port = 1Gbps

Now let's put that information into the formula: $[(48 \times 1\text{Gbps}) + (3 \times 1\text{Gbps})] \times 2 = 102\text{Gbps}$

Therefore, it is recommended that the hardware model for the access switch has a switch capacity of at least **102Gbps**.

When to use: using a three-tier LAN topology or if the LAN topology consist of a traditional redundancy model.

This presents interesting challenges in terms of the bandwidth to use based on what has been determined for the downlink ports. For example, if there are a total of 4 GE downlinks to all access switches then that number should be considered for the bandwidth for the interconnection link. However, larger environments could have a total of 50 GE downlinks for all access switches or buildings hence 1GE Port Channeling will not work and using 10GE will be required.

To determine the bandwidth for all of the interconnection links in the topology obtain the following information:

- **Total Bandwidth for all Access Switch Downlinks:** Determine the total bandwidth service that was used for all of the access switch downlink ports. For example, let's say we have a Core switch connected to three access switches each using a 1GE connection. In this case, the total bandwidth for all access switch downlinks on the Core would be a 3Gbps.

With the information gathered from the list above use the following formula to calculate the expected throughput required for all of the interconnections in the topology. The expected utilization is based on the recommended **oversubscription ratio of 4:1 between the Distribution and the Core layer**.

$$\text{LAN: } (\text{Total Bandwidth for all Access Switch Downlinks}) / 4$$

Example: continuing with our example we know that we have three connected access switches each with a bundled GE uplink. Therefore, the total aggregated bandwidth between all 3 access switches would be 9Gbps (using 3xGE port channel for each link). When we add a second Core switch to provide traditional redundancy it will require an interconnection link between the two Core switches.

Therefore, the bandwidth for all uplinks (to Core switch) and the interconnection link will be 2.25Gbps $(9 / 4 = 2.25\text{Gbps})$.

Based on the bandwidth calculated from the last step for the interconnection ports, determine what bandwidth technologies will be used based on the following options, but read the **design considerations** first:

- **Gigabit Ethernet (1Gbps):** common for interconnections in small/SMB/medium-sized LAN topologies.
- **10 Gigabit Ethernet (10Gbps):** recommended for interconnections in medium/large-sized LAN topologies.
- **40 Gigabit Ethernet (40Gbps):** recommended for interconnections in large-sized LAN topologies.
- **Port Channel:** Used with Ethernet connections for bundling multiple GE (up to 6) or 10GE (up to 4) connections for additional bandwidth. Recommended to use LACP (industry standard protocol) for the port channel protocol.

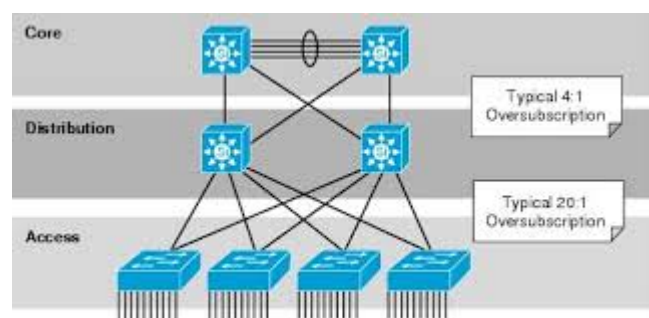
Design Considerations: The highest bandwidth technology you can use for an interconnection port can either be a single 40GE connection (requires expensive hardware) or four 10GE bundled in a Port-Channel (providing a total bandwidth of 40Gbps). The question is what if your total aggregated bandwidth from your access layer (desktops or servers) is 125Gbps even after you have calculated an oversubscription ratio of 4:1? Before I can answer that let me step back and explain what this means.

You probably realized that in many of the previous steps, each host on the network will not be able to send up to its maximum bandwidth speed. The reason for that is because the current bandwidth technologies are not there yet.

For example, in our LAN scenario example we have a total of 140 edge ports. We noted that each of those hosts could be high-performing devices utilizing Gigabit Ethernet which is possible because newer computer systems will likely have Gigabit Ethernet adapters. Those 140 GE edge ports will be spread out across three access switches, but the combined aggregated bandwidth would be 140Gbps. Well, if each of those computers were able to utilize 1Gbps throughput from their computer then you will be looking at a combined traffic rate of 140Gbps. Well there is no single bandwidth technology that can accommodate that. We are on the verge of 100 Gigabit Ethernet, but again we are talking about 140Gbps. That is why we do have the current bandwidth technology to support that model. Luckily, user desktops will never utilize up to 1Gbps speeds even for heavy file transfers.

But I can still use the same example when we talk about servers having 10GE NICs. Imagine those numbers. If you have just 50 servers each with 10GE NICs then that would be a total aggregate of 500Gbps if we are looking at 100% utilization. Even at 50% utilization that would be 250Gbps and still 100 Gigabit Ethernet still wouldn't be good enough. Therefore, what options are available that can be used for building high-performing interconnections with minimal delay:

1. **Two-Tier Topology:** these considerations is why two-tier topologies is becoming very popular and widely used. I have rarely seen a three-tier topology in today's modern networks because of this bandwidth limitation. Hence, try to always use a two-tier topology for any network.
2. **Oversubscription Ratio Best Practices:** The network industry has adapted an oversubscription ratio best practice to follow. It has become helpful to determine the bandwidth between the Access and Core/Distribution layer which would be an oversubscription ratio of 20:1. Or to determine the bandwidth with higher uplinks between a Core and Distribution layer which would be an oversubscription ratio of 4:1. These ratios represent a good baseline to follow and what the design cookbook utilizes for its bandwidth calculations.



3. **Blocking and Non-Blocking Hardware:** the performance of the hardware model will determine if the ports/interfaces on the hardware device provide non-blocking performance or blocking performance (shared bandwidth). Non-Blocking provide a 1:1 ratio meaning 1GE in and 1GE out for possible throughput with low-latency. This avoids possible oversubscription, increased delay, and drops. Hardware for non-blocking devices tend to be more expensive. Blocking means multiple ports share a common bandwidth resource. For example six 1GE connections coming in may share 1GE going out. So if 6 GE servers are forwarding at 100% then there will be oversubscription, buffering of packets resulting with possible delay and discards/drops. However the cost for blocking type hardware is cheaper. Non-Blocking is also known as line-rate or wire-speed. Non-blocking is something that is often discussed with L2/L3 switches more than with router devices.
 - a. **Non-Blocking:** recommended for Server Farm/Data Center networks and the LAN Core. Or if utilization is expected to be high.
 - b. **Blocking:** common for LAN topologies or if utilization is expected to be low.
4. **Server Farm connected to Core:** if a small server farm (~10-24 servers or less) will be connected directly into the LAN Core instead of a dedicated Data Center/Server Farm switch. If there is a large number of servers (25-30+ servers) then using a dedicated Data Center (Server Farm) topology is recommended. A server farm connected to the LAN Core eliminates the oversubscription problems when you connect a Data Center (Server Farm) switch into the LAN Core.

Step 3-11

Determine bandwidth media for interconnection and other uplink ports

For the bandwidth service determined for the uplink/downlink ports on the Core/Distribution, what media type will be used:

- **Copper:** the most common and recommended media type to use for edge ports. Copper can also be used for the uplink/downlink ports if copper wiring is supported and does not exceed 100 meters. Copper media for uplink/downlink connections is starting to become common for wiring if the equipment exist in the same room location.
- **Fiber:** common media type used for uplink/downlink ports when using 1GE and 10GE connections. It also depends on the distance between the components (e.g. Core and Access) that may require multi-mode or single-mode fiber connections.

Example: all of our uplink/downlink ports will use Copper GE ports, so that will be needed for our LAN Core switch ports.

Step 3-12

Determine total ports needed on Core switch

Next we need to determine the total number of ports required on the Core device based on the following components connected.

- **Downlinks to Access Layer:** the total number of access switches with uplinks to the Core device (LAN), therefore, each port on the Core is considered as an aggregation point that needs to be calculated.
- **Infrastructure Components:** Its recommended to have up to 13-15 ports on the Core switch for these infrastructure components. This can be the interconnection between the LAN Core/Distribution switches. It can also be the uplink/downlink ports to many of the main network components like the firewall appliance, Internet Edge Router, the WAN Aggregation/Branch router, and/or the Data Center Core switch.
- **Server Components:** if the network consist of a small server farm (~24-50 servers recommended) and/or if there are 1-5 racks in the Data center (or computer room), the server can be connected directly into the LAN Core switch. Therefore, determine the number of servers that will be connected.

With the total number of ports determined on the core/distribution layer consider the following for additional ports to add to the total:

- Potential scalability of additional ports adding at least 20% (lower/higher if necessary) more ports.
- Potential redundancy used by network devices adding between 15-20% (or higher if necessary) more ports. For example if the firewall component in the design becomes redundant we want to consider that for the total port capacity needed for the hardware choice in a later step.

For the infrastructure and server components that may be connected to the Core switch, determine if those ports will be Fast Ethernet/Gigabit Ethernet (100Mbps/1Gbps) or Ten Gigabit Ethernet (10Gbps).

- **Fast Ethernet (100Mbps) | Gigabit Ethernet (1Gbps):** common for most infrastructure components (e.g. Firewall, Internet Edge, WAN, Wireless, and small/medium Data Center Core switches) and for all server components.
- **10 Gigabit Ethernet (10Gbps):** recommended when using a larger Data Center topology where the Data Center Core will connect into the LAN Core.
- **40 Gigabit Ethernet (40Gbps):** ideal for large-sized network when the expected utilization is within 40GE speeds.

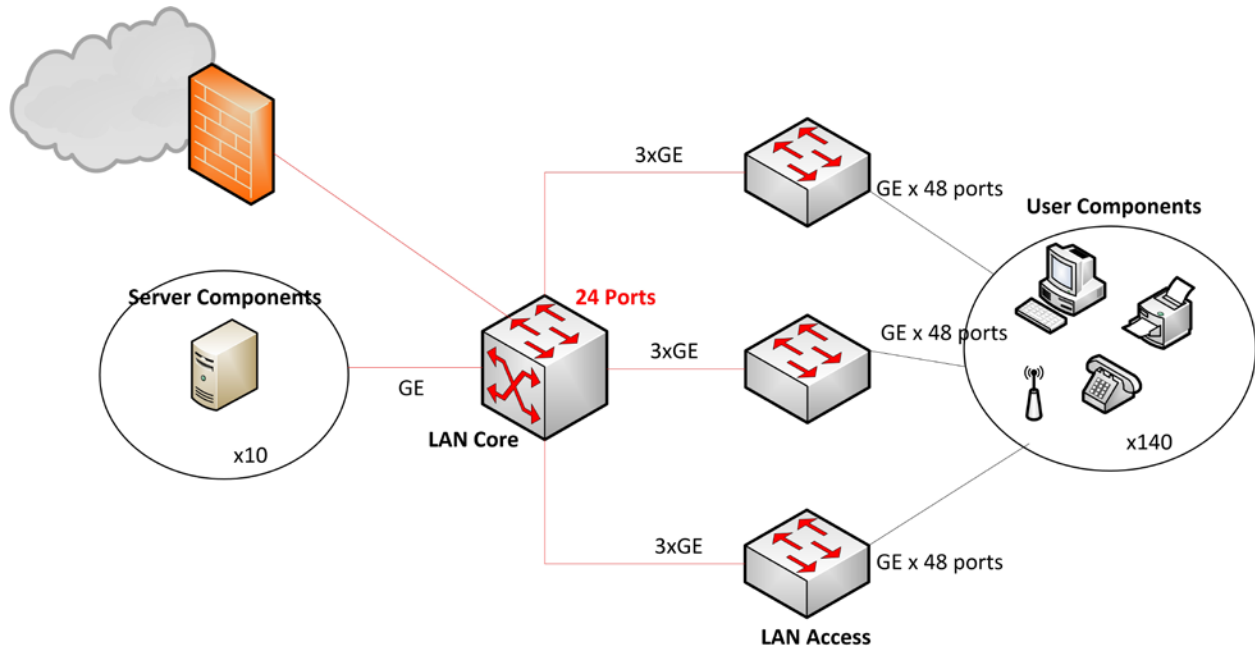
Next, determine the switch port capacity that will be needed for the Core switch:

- **24 Ports:** a fixed switch that provides 24 Ethernet ports.
- **48 Ports:** a fixed switch that provides 48 Ethernet ports.
- **48+ Ports:** a switch that can support more than 48 Ethernet ports. This would be a chassis-based switch or a stack-based switch.

The following considerations should be kept in mind for this process.

- If there is a large number of servers then either a 48+ port type switch is needed for the LAN Core. Or using a Data Center topology (with a Core and/or Access layer) for the server infrastructure.

Example: our Core switch will have 1 connection to other solutions (e.g. Internet Edge), 10 GE ports for the servers, and 9 GE downlink ports to the access switches. That would be a total of 20 ports. Therefore, a 24-Port switch will work for the LAN Core switch in this example.



Step 3-16

Determine the switch capacity for Core layer

In this step determine the combined aggregated bandwidth (or switch capacity) for the Core switch based on the number of ports and the bandwidth technology chosen from the previous steps. This is important to help determine the best hardware to use for the Core switch.

The following formula can be used to determine the minimum switch capacity (**Sc**) required for the access switch:

$$\text{Sc} : [(\# \text{ of Ports}) \times (\text{Max Bandwidth per Port})] \times 2$$

Note: Ethernet ports in networks today will support full-duplex, which means each port is able to send and receive at the bandwidth rate of the switch port (e.g. 1Gbps, 10Gbps). Thus the “2” represents the full-duplex operation which doubles the bandwidth for the total switch capacity.

Example: To determine the aggregated bandwidth for our Core switch in the topology we need to gather the required information:

- # of Ports = 24
- Maximum Bandwidth per Port = 1Gbps

Now let's put that information into the formula: $(24 \times 1\text{Gbps}) \times 2 = \mathbf{48\text{Gbps}}$

Therefore, it is recommended that the hardware model for the Core Switch has a switch capacity of **48Gbps** or greater.

Step 4	Security for LAN

Below are Security Services (and Solutions) that should be deployed within the LAN solution:

- Port Security
- BPDU Guard or BPDU Filter
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard
- Root Guard
- Trunking (802.1Q): Trunk Security
- Security Best Practices
- Access Control Lists (ACL)
- Identity Access Control Solution

Step 5	Network Management for LAN

Below are the “Network Management Services” that should be deployed within the LAN solution:

- SNMP
- NTP
- Syslog
- RADIUS *OR* TACACS+
- VTY Access
- GOLD, EEM, ERM, Configuration Rollback, RBAC
- Hardware: NAM for Cisco Catalyst 6000 Series

Step 6	Flexibility for LAN

Step 6-1	Integration with other solutions

Below are solutions that are commonly deployed within the foundation solution:

- Identity Access Control Solution
- Voice (IP Communications)
- Wireless
- Virtualization (Network)

Step 6-2	Integration with Data Center

If a Data Center solution (1, 2, or 3 tier topology) will be deployed then the Data Center Core would plug directly into the LAN Core.

Step 7	Design Aspects for LAN

Below are specific design elements to complete for the solution.

Step 7-1	Other Services to include with solution

These are additional services that can be implemented (if required) within the solution.

- General Best Practices
- Multicast
- IPv6
- Virtualization (Network): Layer 3 Virtualization
- Port Monitor

If Voice (Unified Communications) and Wireless solutions will be implemented into the design then the following services and hardware features are required:

- Power over Ethernet (PoE), PoE+, or Cisco Universal PoE (UPOE)
- Quality of Service (QoS)
- Cisco Medianet - recommended for voice and video deployments

Determine the subnet types and the number of subnets that will be used on the LAN.

- **Users:** a dedicated subnet should be used for users on the LAN using desktop/computer/laptop systems including printers. Multiple user subnets should be considered based on the department, building, or quadrant.
- **Transit:** a subnet for interconnections to other solutions like the Internet Edge and the WAN. The network subnet can also be used for managing all of the network devices under the same IP subnet.
- **Management:** a dedicated subnet used for managing all network devices including network management services such as SNMP and Syslog for monitoring.
- **Interconnection:** a dedicated subnet used between the redundant LAN components if routing is enabled.
- **Other:** other subnets can be created based on any unique requirement or preference such as a subnet dedicated for Guest users or a subnet used for a lab network.

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

For each component in the solution using the tables below based on the technical objectives with some of the important details (supported services, bandwidth, etc).

Cisco Catalyst 6800 Series *(Large, Data Center)*

Performance	880Gbps/slot 10G/40G/100G support	Flexibility	PoE, Wireless (WiSM), ACE30
Reliability	Power, VSS (VS40, MEC)	Management	NAM, SDN
Scalability	Topology (Unified)	Security	Firewall (ASA), Identity (TrustSec), AVC
Design Aspects	L2, L3, Virtualization (MPLS, VPLS, EVN)		
Models	6807-XL, 6880ia, 6880-X ; chassis		

Cisco Catalyst 6500 Series *(Medium, Large, Data Center)*

Performance	40-80Gbps/slot 10G/40G/100G support	Flexibility	PoE, PoE+, WiSM, ACE
Reliability	Power, VSS (VS40), ISSU	Management	NAM
Scalability	Topology (Traditional)	Security	Firewall (ASA), Identity (TrustSec)
Design Aspects	L2, L3, Virtualization (MPLS, VRF-lite, EVN), LISP		
Models	6513-E, 6509-E, 6506-E, 6504-E, 6503-E, Supervisor Engines (720, 2T) ; chassis		

Cisco Catalyst 4500-E Series *(SMB, Medium, Large)*

Performance	1.8Tbps (VSS), 928Gbps 1G/10G support	Flexibility	PoE/PoE+/UPoE, Wireless (WLC)
Reliability	Power, VSS (MEC), ISSU, NSF/SSO	Management	GOLD, SDN
Scalability	Topology (Traditional, Unified) Support for 500-1000 users	Security	Identity (TrustSec), FnF
Design Aspects	L2, L3, Virtualization (VRF-lite, EVN), Medianet		
Models	4503-E, 4506-E, 4507-E, 4510-E, Supervisor Engines (8E, 7E, 7LE, 6E, 6LE, V-10GE) ; chassis, IOS XE Licensing (LAN Base, IP Base, Security, Enterprise)		

Cisco Catalyst 4500-X Series *(SMB, Medium, Large)*

Performance	1.6Tbps (VSS), 800Gbps 1G/10G support	Flexibility	--
Reliability	Power, VSS (MEC), ISSU, NSF/SSO	Management	GOLD, DOM
Scalability	Topology (Traditional)	Security	Identity (TrustSec), FnF
Design Aspects	L2, L3, Virtualization (VRF-lite, EVN), Medianet		
Models	16 ports, 32 ports ; fixed, IOS XE Licensing (LAN Base, IP Base, Security, Enterprise)		

Cisco Catalyst 3850 Series *(Medium, Large)*

Performance	Stack: 480Gbps Uplink Ports: 1G/10G (2 or 4) Edge Ports: 10/100/1G (12, 16, 24, 36, 48)	Flexibility	Wireless (WLC), UPoE, PoE/PoE+
Reliability	Stack Power, Stack, Stateful Switchover (SSO)	Management	SDN
Scalability	Topology (Traditional, Unified), 24-192 ports Stack (up to 4 switches, planned for 9)	Security	Identity (TrustSec), FnF, AVC
Design Aspects	L2, L3		
Models	24 ports, 48 ports ; fixed, stack		

Cisco Catalyst 3750-X Series *(Medium, Large)*

Performance	Stack: 64Gbps 1G/10G (uplink) support	Flexibility	PoE/PoE+/UPoE
Reliability	StackPower, Stack	Management	--
Scalability	Topology (Traditional, Unified), 24-432 ports Stack (up to ~ 9 switches) Support for 600 users	Security	Identity (TrustSec)
Design Aspects	L2, L3		
Models	24 ports, 48 ports ; fixed, stack		

Cisco Catalyst 3650 Series *(SMB, Medium, Large)*

Performance	Stack: 160Gbps Uplink Ports: 1G/10G (2 or 4) Edge Ports: 10/100/1G (24, 48)	Flexibility	Wireless (WLC), PoE/PoE+
Reliability	Power, Stack, Stateful Switchover (SSO)	Management	SDN
Scalability	Topology (Traditional, Unified), 24-48 ports Stack	Security	Identity (TrustSec), FnF, AVC
Design Aspects	L2, L3		
Models	24 ports, 48 ports ; fixed, stack, IOS XE		

Cisco Catalyst 2960-X Series *(SMB, Medium, Large)*

Performance	Stack: 80Gbps Switch Capacity: 216Gbps Uplink Ports: 1G/10G (2 or 4) Edge Ports: 10/100/1G (24, 48)	Flexibility	PoE, PoE+ (up to 740W)
Reliability	StackPower, FlexStack-Plus	Management	SDN, NetFlow lite
Scalability	Topology (Traditional, Unified), 24-384 ports Stack (up to 8 switches)	Security	Identity (TrustSec, 802.1x), FnF
Design Aspects	L2, L3 (using 2960-XR)		
Models	2960-X, 2960-XR - 24 & 48 port models ; fixed/stack		

Cisco Catalyst 2960-S Series *(SMB, Medium)*

Performance	Stack: 88-176Gbps 1G/10G (uplink) support	Flexibility	PoE, PoE+
Reliability	StackPower, FlexStack	Management	
Scalability	Topology (Traditional, Unified), 24-192 ports Stack (up to 4 switches)	Security	Identity (TrustSec, 802.1x)
Design Aspects	L2		
Models	24 & 48 port models ; fixed/stack		

Cisco SG500XG Series – Small Business (SMB)

Performance	Stack: 80Gbps Switching Capacity: 320Gbps Uplink/Edge ports: 10GE (16 ports)	Flexibility	--
Reliability	VRRP, Stack	Management	GUI, CLI
Scalability	Topology (Traditional, Unified) Stack (up to 8 switches)	Security	ACL, Identity (802.1x), Web Auth
Design Aspects	L3, IPv6, USGv6		
Models	Hardware: SG500XG-8F8T (16 ports) Defaults: 8x 10GE (Copper, RJ-45), 8x 10GE (Fiber, SFP+), 1 GE (Management)		

Cisco SG500/X Series – Small Business (Small, SMB)

Performance	28.8-320Gbps 1G/10G (uplink) support	Flexibility	PoE/PoE+
Reliability	Stack, FHRP (VRRP)	Management	GUI, CLI
Scalability	Topology (Traditional, Unified), 24-200 ports Stack (up to 8 switches)	Security	ACL, Identity (802.1x), Web Auth
Design Aspects	L2, Basic L3, PVE		
Models	SG500/500X: 24, 28, 48, & 52 port models ; fixed/stack		

Cisco SG300 Series – Small Business (Small, SMB)

Performance	1.6-104Gbps 1G support	Flexibility	PoE/PoE+
Reliability	--	Management	GUI, CLI
Scalability	Topology (Traditional), 8-52 ports	Security	ACL, Identity (802.1x), Web Auth
Design Aspects	L2, Basic L3, PVE		
Models	8, 10, 20, 24, 28, 48, & 52 port models ; fixed		

Cisco SG200 Series – Small Business (Small, SMB)

Performance	8.8-100Gbps 1G support	Flexibility	PoE
Reliability	--	Management	GUI
Scalability	Topology (Traditional), 8-50 ports	Security	Identity (802.1x)
Design Aspects	L2		
Models	200/200E: 8, 10, 18, 24, 26, 48, & 52 port models ; fixed		

For chassis hardware models (e.g. Cisco Catalyst 4500, 6500, 6800 series) make sure they include the following:

- **Chassis:** determined based on the total number of ports and bandwidth services needed.
- **Line Modules:** modules that provide port capacity (Ethernet) and services.
- **Dual Supervisors:** utilizing redundant Supervisor Engines can provide redundancy for the chassis.
- **Fan Trays (System, Fabric):** these are required in order to cool the modules in the chassis.
- **Licensing:** Determine what services/features will be used on the device and ensure to get all of the needed licenses to support your configuration.
- **Power (Input Voltage):** determine the required power based on the modules in the chassis and the capabilities that will be used (e.g. PoE). If you are planning to use Cisco based switches use the Power Calculator Tool (<http://tools.cisco.com/cpc/>) to determine the power supplies and power source needed with the chassis

Quick & Recommended Hardware Options

You can choose the hardware for each component based on the recommendations below:

Core	Access	Business Size
Cisco Nexus 7000	Cisco Nexus 5000/2000	Large
Cisco Catalyst 6800 (6807-XL, 6880-X)	Cisco Catalyst 6800ia	Medium, Large
Cisco Catalyst 6500	Cisco Catalyst 4500-X, 4500-E Cisco Catalyst 3560 Cisco Catalyst 3750	Medium, Large
Cisco Catalyst 3650 Cisco Catalyst 3750-X Cisco Catalyst 4500-X Cisco Catalyst 4500-E	Cisco Catalyst 2960-S Cisco Catalyst 2975	Medium, SMB
Cisco Catalyst 4900/M	Cisco Catalyst 2350 Cisco Catalyst 2360	Medium

A large, white, serif capital letter 'M' is centered within a dark gray rectangular box.

~ Solutions ~

Messaging

Category: Network Solution (Voice)

Prerequisite(s): Voice (Unified Communications) Solution

Complete the steps below for building the design for the network solution. First, determine the type of messaging used with the voice environment:

- **Voicemail Messaging:** Provide voicemail capabilities for users if they are not available or if their line is busy including accessing those voicemail messages via their email client.
- **Unified Messaging:** Provide TTS (Text-to-Speech) capabilities for users to have their actual email messages read back to through from any phone endpoint. Unified messaging also provides syncing voicemail messages with a user's email inbox. If a user hears a new message through their email client, it will automatically sync that status back to the VM/UM server turning off the email notification (MWI) on their local phone.

Step 1

Scalability for Messaging Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

- **VM/UM Server:** this is the main component for the solution that can provide either Voicemail (VM) and/or Unified Messaging (UM) to the Unified communication environment. This component usually connects into the LAN Core, Server Farm, or the Data Center Core/Access layer where the other Collaboration components exist.
- **Mail Server:** this is a server component that is managed by a system engineering team connected to a server farm. The mail server in the design is applicable if we are using Unified Messaging.

Step 1-2

Determine the VM/UM Server option

Choose the appropriate messaging solution based on the business size and function required.

- **Small, SMB (up to 240 users):** Use the product Cisco Unity Express (CUE) which is a module installed on the Cisco Unified CME router to support only Voice messaging.
- **SMB, Medium (300 to 1000 users):** Use the product Cisco Unity Connection integrated with the Cisco Unified CM BE appliance supporting both Voice and Unified Messaging.
- **Medium, Large (up to 3000 users):** Use the product Cisco Unity Connection in a standalone deployment supporting both Voice and Unified Messaging services.
- **Very Large (up to 15K users per server, 250K users networked):** Use the product Cisco Unity supporting both Voice and Unified Messaging services. Recommended to use Cisco Unity Connection.

Determine the number of users that require voicemail and other messaging features:

- **Voice Messaging:** Capabilities for callers to leave a voice message for a subscriber. They can be alerted via their phone (using MWI) and/or receive a voicemail message that can be sent via email.
- **Unified Messaging:** Capabilities for subscribers to call into the voicemail system and use the TTS (Text-to-Speech) function to have their actual email messages read back to them over the phone.
- **Unity Inbox:** Provides a web interface for users to access their voicemail messages and/or send messages to other subscribers on the system.

This is important to understand for licensing purposes and creating subscriber templates on the VM/UM server.

Applicable if using Cisco Unity or Cisco Unity Connection.

Determine the number of ports used between the voicemail server and the phone system. The ports relate to the total concurrent number of calls between the two solutions for the following conditions:

- Calls sent to a subscriber's voice mailbox
- Subscribers/Users checking their voicemail messages
- Message Waiting Indicator (MWI) notifications
- Callers routed to an Auto-Attendant (AA) menu

Recommendations: For the total voice ports that is needed as a best practice dedicate 25% of the voice ports for MWI and the other 75% used for voicemail and AA purposes.

Step 2	Reliability for Messaging Solution

Below are possible redundancy options when using Messaging on the voice network.

Step 2-1	Active/Active Cluster

The Messaging solution can be deployed in a cluster to provide reliability and scalability by using a **publisher server** which is setup first and using multiple **subscriber servers**. Using Cisco Unity Connection, all servers in the cluster are active providing not only redundancy, but also load balancing.

Step 3	Performance for Messaging Solution

Step 3-1	Determine bandwidth services

Determine the bandwidth service that is required for each component for the solution. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)

Recommendations: use GE if supported and available on the LAN and/or Data Center network.

Step 4	Security for Messaging Solution

Step 4-1	Voicemail Accounts

Voicemail accounts on the VM/UM server should be enabled for the following:

- Accounts should be reset every 180 days requiring a new password/PIN.
- Account lockout should be enabled if three failed login attempts occur.
- Complex password/PIN should be enabled for increased security.

Step 5	Network Management for Messaging Solution

Below are Network Management services that can be used with the solution:

- **Backups:** always do scheduled backups (using DiRT or the DR system) on the VM/UM server. That way you can rebuild the server in a couple of hours if the component has a failure. Cisco Unity Connection provides scheduled backups through the Disaster Recovery System, which is highly recommended.
- **Real-Time Monitoring Tool (RTMT):** an application which connects to the VM/UM server to provide system resource reports (CPU, Memory), logs, and call activity.

Step 6	Flexibility for Messaging Solution

Step 6-1	Integration with other solutions

Below are required solutions that need to be deployed prior to building the design for messaging:

- Voice (Unified Communications)

Step 6-2	Integration with Voice (Unified Communications)

Determine what protocol will be used for integrating the VM/UM server with the phone system (e.g. Cisco UCM).

- **SCCP:** Recommended if using Cisco Unity or Cisco Unity Connection with Cisco Unified CM.
- **SIP:** Use if connecting between different vendor solutions such as Cisco UCM (the phone system) and Microsoft Exchange for Unified Messaging (the VM/UM server).

Step 7	Design Aspects for Messaging Solution

Step 7-1	Features

Determine the messaging features that will be used:

- **Auto-Attendant (AA):** Provide an automated menu for callers to access a directory listing and other information/resources available.
- **Voice Recognition:** Provide the capability for users/subscribers to use voice commands when accessing voice features and placing calls. Cisco Unity Connection provides voice recognition built in, however if using Cisco Unity a separate server is required.
- **Speech Connect:** Provide the capability for callers to use voice commands when calling users within the Directory. Cisco Unity Connection provides voice recognition built in, however if using Cisco Unity a separate server is required.
- **Email Notification:** Provide voicemail messages to be sent via email as an attachment or receive a notification email that a new message is waiting to be heard.

Step 7-2	Pilot Number

Determine the pilot numbers and other directory numbers that will be used in the voice+messaging environment:

- Voicemail
- Auto Attendant (AA)
- Greeting Administrator
- Other automated menus created

This would follow the extension schema format scoped out from the Voice network design.

Step 7-3	Subscriber Template and Class of Service (COS)

Based on the number of users and what features are required (VM, UM, Unity Inbox) create different groups and Class of Service (COS) templates within the solution.

For example, all users will need VM support, so that would be considered as one group. 10 voice users may need VM and the Unity Inbox feature which would be another group. And last we have 20 voice users that require both VM and UM capabilities, so that would be a third group. Therefore the following groups created would be:

- **VM-ONLY:** Subscriber template and COS associated to subscribers to provide only VM capabilities.
- **VM-UI:** Subscriber template and COS associated to subscribers to provide VM capabilities and access to the Unity Inbox feature.
- **VM-UM:** Subscriber template and COS associated to subscribers to provide both VM and UM capabilities.

Create the groups based on what is required in the design then associate the correct subscribers to those groups.

Step 8	Hardware for Messaging Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Table Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1	Hardware Table Options

Select the hardware for each component in the solution using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a	VM/UM server

Cisco Unity Express *(Small, SMB, Medium)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	ISR2 3900: 500 mailboxes, 32 ports ISR2 2900: 100-500 mailboxes, 10-32 ports	Security	--
Design Aspects	Voicemail, Unified Messaging (Exchange), AA		
Models	3945, 3945E, 3925, 3925E, 2901, 2911, 2921, 2951, UC500 ; module		

Cisco Unity Connection *(SMB, Medium, Large)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	Up to 3000 users	Security	--
Design Aspects	Voicemail, Unified Messaging (Exchange), AA		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance, Cisco Unified CM BE appliance		

Cisco Unified Communications Manager – Business Edition *(SMB, Medium)*

Performance	--	Flexibility	Contact Center (CCX), Voice & UC (CUCM), Presence (IM&P)
Reliability	--	Management	--
Scalability	BE 6000: 1000 mailboxes, 24 ports	Security	--
Design Aspects	Phone System (Call Control), Voicemail, Unified Messaging (Exchange), AA, Presence Server		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance, Cisco Unified CM BE appliance		

Some of the messaging components can be consolidated with other components in the design using one of the following options:

- **VM/UM Server** (using Cisco CUE for Messaging) can be consolidated with the **WAN Router** (Hub, Spoke) installed with a CUE module.
- **VM/UM Server** (using Cisco CUE for Messaging) can be consolidated with the **Edge Router** (Internet Edge) installed with a CUE module.
- **VM/UM Server** (using Cisco Unity Connection) can be consolidated with a Cisco Unified CM Business Edition appliance providing other voice services like Call Center and Presence.

Note: Reference the "Hardware Matrix Table" for any specific hardware that may be listed for consolidation.

A large, white, serif capital letter 'N' is centered within a dark gray rectangular box.

~ Solutions ~

Network Management

Category: System Solution
Prerequisite(s): --

Complete the steps below for building the solution. First, determine what NMS solutions will be used in the design:

1. **Fault Management:** solution that monitors the availability of a network device and basic information such as utilization of the device and its interfaces. This solution is commonly deployed for most networks.
2. **Performance Management:** solution that provides advanced monitoring of actual traffic usage through the network. It provides a way to see “who” is using the most bandwidth on the network and what they are doing. This is starting to gain huge interest for deploying for deeper troubleshooting.
3. **Configuration Management:** solution that provides an easy method for making simple to bulk configuration changes on the network to auditing configuration for best practices or security exploits.
4. **Events and Logging:** solution that provides events from a network device that can be used for troubleshooting issues.
5. **Desktop Management:** solution that provides managing user desktop/laptop systems in terms of patching, Anti-Virus, applications on the system, to tools used by desktop technicians for troubleshooting a problem on a desktop/laptop remotely.
6. **Security Management:** solution that provides managing security solutions, authentication, and authorization on the network.

1

Fault Management

NMS solution that provides the following using SNMP and ICMP (e.g. Ping, Traceroute) services:

- Checks whether a network device is UP or DOWN on the network
- Uptime on the device
- Latency/Delay, Round Trip Time (RTT)
- Bandwidth utilization
- Memory, CPU usage

2

Performance Management

NMS solution that provides the following using SNMP and Flow technologies (NetFlow, sFlow, J-Flow):

- Bandwidth usage
- Top-Talkers (Conversations, Protocols, Applications)
- Application Response

NMS solution that provides the following using SNMP and Telnet/SSH:

- Configuration changes and audits
- Best Practices
- Automated Scripts

NMS solution that provides the following using Syslog or events in a network device's local buffer.

- Hardware events (e.g. hardware issues or failure)
- Software events (e.g. OS bugs or failures)
- Configuration events (e.g. configuration changes)
- Protocol events (e.g. Routing protocol neighbor changes)
- Interface events (e.g. when an interface goes up or down on a network device)

NMS solution that provides managing user desktop/laptop systems in terms of:

- OS Patching
- Application Updates
- Anti-Virus Updates
- Troubleshooting Tools for Desktop Technicians

NMS solution that provides managing many of the security aspects of the network. Security Management can include one or more of the following:

1. Policy Management
2. Protection and Enablement

Controls threats by working with solutions to translate raw security data into actionable threat intelligence to include some of the following:

- Reports for PCI or HIPPA compliances
- Overlapping firewall policies
- Unused firewall policies

Complete the steps below for building the policy management solution for NMS:

1) Components & Deployment: Determine the components for this solution and how it will be deployed:

- **Server (Cisco MARS, Firemon):** the component in this solution is a server/appliance that is usually connected to a server farm or directly into the Core switch (for smaller server farms).

2) Hardware Option: Cisco MARS is typically used by medium and larger networks. Or following a particular compliancy mandate like PCI or SOX. Firemon is another similar policy management product aimed for SMB to large networks.

3) Services: below are services that are used with this solution.

- **Syslog:** Used for displaying system and service related events that can be stored locally or sent to a server (e.g. to one of the hardware options).
- **SNMP**

Solution that provides authenticating users into network devices or solutions like remote access.

1) Solutions: Determine the solutions used for protection and enablement:

- **Network Authentication:** Solution that provides network authentication services through the use of RADIUS (Cisco ACS, IAS) or TACACS+ (Cisco ACS). This solution is typically used by medium to larger network environments.

2) Components & Deployment: Determine the components for this solution and how it will be deployed:

- **Server (ACS/IAS):** the component in this solution is a server/appliance that is connected to a server farm or directly into the Core switch (for smaller server farms). This component provides network authentication services through the use of RADIUS or TACACS+ which is required on the network.

3) Hardware Option (Cisco ACS): The ACS component provides centralized user authentication for accessing network devices (e.g. Routers, Switches, Firewalls) including authentication services for remote access. This is recommended and ideal for medium and large networks that have many network devices.

Recommendations: The Cisco ACS solution is available as an enterprise version (for large and medium networks) and an express version (for SMB networks). If you are managing more than 25 devices it's recommended to deploy an ACS (or IAS) solution to provide a centralized option for network authentication. For example, if an employee leaves a company, you can simply change the password on the server. Or delete the user's account on the ACS server or on the LDAP server. Without using this solution, you will need to log into all network devices to change or remove the password. You can use scripts or tools like Kiwi CatTools to accomplish most of these tasks. You can also use a RADIUS server, like Microsoft's IAS to provide user authentication against Active Directory than using a separate local database.

4) **Services:** below are services that can be used with this solution.

- **RADIUS:** network authentication protocol used by Cisco or other vendor devices to authenticate users into a network device or for remote access. This is an industry standard protocol that uses UDP.
- **TACACS+:** network authentication protocol used by Cisco devices to authenticate users into a network device or for remote access. This is a Cisco based protocol that uses TCP.

7	Out-of-Band (OOB) Management

It's recommended to build a dedicated OOB management network that is isolated from the production network for remote monitoring and access.

This can be a dedicated switch with external connections (Internet, analog) for accessing servers and network equipment if there is an emergency where the network cannot be reached from the outside.

	Services

The following are tools/services that can be used for a NMS solution and for troubleshooting purposes.

- Network Management Services:
 - o SNMP
 - o NetFlow
 - o Syslog
 - o NTP
 - o RADIUS *OR* TACACS+
- Port Monitor
- Use “**show**” and “**debug**” commands on the network devices for advanced troubleshooting and real-time monitoring of network operations.

These are services that are implemented on all components in the topology except for NetFlow. NetFlow is commonly implemented on the Internet edge and WAN routers to capture traffic flow details.

SERIES	HW/MODEL	BUS	FM/S	PM	CM	SM	NP-DD	OTH	COST
Manage Engine	Opmanager	S,SM,M	X	--	--	--	--	--	F,M
	NetFlow Analyzer	S,SM	--	X	--	--	--	--	F,H
	Device Expert	SM,M	--	--	X	--	--	--	M
SolarWinds	ipMonitor	S,SM,M	X	--	--	--	--	--	M
	Orion	L	X	X	--	--	--	IP	H
	NetFlow Analyzer	S,SM	--	X	--	--	--	--	H
Zenoss	Zenoss OS	S,SM,M	X	--	--	--	--	--	OS
SpiceWorks	SpiceWorks	S,SM	X	--	--	--	--	--	F
Woodstone	Servers Alive	S,SM,M	X	--	--	--	--	--	L
What's Up	Gold	S,SM	X	--	--	--	--	--	M
Fluke	NetQoS	L	--	X	--	--	--	--	H
Opsware	Opsware	L	--	--	X	--	--	--	H
Cisco	CSM	M,L	--	--	--	X	--	--	H
NetBrain	Map Edition	M,L	--	--	--	--	X	--	H
Path Cloud	Path Cloud	SM,M,,L	--	--	--	--	--	T	M-H
Network Instr.	Network Sniffer	M,L	--	--	--	--	--	T	H
Wireshark	Wireshark	ALL	--	--	--	--	--	T	F
Infoblox	IPAM	ALL	--	--	--	--	--	IP	M
Firemon	Firemon	SM,M,L	--	--	--	X	--	--	--

- **SERIES:** vendor or vendor model series
- **HW/MODEL:** hardware model or line module in hardware model
- **BUS (Business size):** S (Small), SM (SMB), M (Medium), L (Large)
- **FM/S:** Fault management support , Logging support
- **PM:** Performance management support
- **CM:** Configuration management support
- **SM:** Security management support, Policy Management support
- **NP-DD:** Network planning support, auto network diagram support
- **OTH (Other):** IP (IP Address Management), T (Tools, Troubleshooting)
- **COST:** F (Free), L (Low cost), M (Moderate cost), H (High cost), OS (Open Source, Free)

Recommendations: I recommend Opmanager for many reasons. One, for Small business networks they can utilize the FREE edition over using an expensive NMS system. The setup and implementation of Opmanager is very easy and more organized for monitoring bandwidth and hardware resources. Larger environments can use Opmanager or Solarwinds, but will require spending over \$5,000 for the solution. The Open Source products such as Zenoss or OpenNMS are free, but they are not off-the-shelf products and cannot be configured easily by any person. It's not clean or organized for a typical network engineer to deploy unless they have experience with Linux-based open-source systems and other similar configuration.

A large, white, serif capital letter 'O' is centered within a dark gray rectangular box.

~ Solutions ~

Optimization

Category: Network Solution (Data Center, WAN)
Prerequisite(s): WAN Solution

Complete the steps below for building the design for the network solution.

Step 1

Scalability for Optimization Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

1. **WAN Optimization Head-end appliance:** this component is located at the main office or Data center where optimization is needed.
2. **WAN Optimization Spoke-end appliance:** this component is located at the branch office.
3. **WAN Optimization Manager:** this component is a management system that manages all of the WAN Optimization appliances on the WAN.

Step 1-2

Choose how components will be deployed

Determine how each component for the solution will be deployed.

#1

WAN Optimization Head-end Appliance

This component is usually connected into the Core switch communicating with the WAN Aggregation router using WCCP.

#2

WAN Optimization Spoke-end Appliance

This component is connected into the Core switch at the branch office or integrated with the WAN branch router.

#3

WAN Optimization Manager

This component usually exist at the location that has the Head-end appliance. It connects into the Core switch or the Server Farm.

Step 2	Flexibility for Optimization Solution

Step 2-1	Integration with WAN

Optimization over the **WAN solution** will provide traffic engineering for a WAN between sites to accelerate application traffic such as Exchange, replication, and downloading which can be slow.

Determine the application and traffic that will be used across the WAN. Below are some of the most common traffic and applications that often experience performance issues that improve when deploying optimization:

- Microsoft Exchange
- File Services
- FTP Services
- Replication and Backup
- Latency sensitive applications
- Heavy traffic volume

Using optimization makes good use of bandwidth resources on the WAN by filling up or efficiently using the WAN connection by tuning the TCP window options to obtain increased throughput.

Step 3	Design Aspects for Optimization Solution

Step 3-1	Checklist

Below are questions to determine if the WAN Optimization solution can support some of the following, which is important when choosing a WAN Optimization appliance during the hardware selection phase.

- Does the appliance provide compression and/or caching as part of its optimization?
- Can you create and/or preserve QoS tags that are used on the network?
- Can the appliance optimize both TCP and UDP based traffic?
- Can the appliance optimize web traffic with improved caching?
- Can the appliance accelerate CIFS and NFS traffic across the WAN?
- Can the appliance shift to use local cache if the WAN connection for a site fails?

Step 3-2	Traffic Engineering Services

Determine what traffic engineering services should be enabled on the optimization appliances. Below are the most common services deployed:

- **Transport Flow Optimization (TFO):** terminates TCP sessions locally and optimizes TCP flows that goes across the WAN to lower end-user performance issues.
- **Persistent Lempel-Ziv (LZ):** provides compression to data packets which can save 10-20% of the WAN bandwidth.
- **Data Redundancy Elimination (DRE):** this service identifies redundant patterns in the data going across WAN and eliminating if it is cached. This can reduce traffic between the HQ and the remote sites.

Step 3-3	Licensing Considerations

Depending on the WAN Optimization solution that is deployed it's important to understand the licensing requirements. This may be based on the services to the type of traffic that is inspected to be optimized. Below are the licensing options when deploying the Cisco WAAS solution:

- Enterprise
- Enterprise and Video
- Enterprise and Virtual Blade
- Enterprise, Video, and Virtual Blade

Below are services that are used when deploying the solution.

- WCCP

WCCP is used to transparently send traffic (e.g. HTTP, FTP) to the optimization appliance. This service is usually configured on the WAN router component in the topology.

Step 4

Hardware for Optimization Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Matrix Table Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1

Hardware Consolidation Option

Some of the WAN Optimization components can be consolidated with other components in the design using the following hardware options:

- The **WAN Optimization appliance (Hub, Spoke)** component can be consolidated on the **WAN Router (Hub, Spoke)** using a WAE module installed.

Note: Reference the "Hardware Matrix Table" for any specific hardware that may be listed for consolidation.

#2

Hardware Matrix Table Options

Or you can select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a

WAN Optimization Appliance (Head-end, Spoke-end)

SERIES	HW/MODEL	BUS	RAM	STORAGE	PERF	SITE
Cisco	WAAS	S,SM	2GB	160GB	--	S
	WAE 500	SM,M	1-2GB	250GB	--	S
	WAE 600	SM,M,L	2-6GB	300-650GB	--	S,H
	WAE 7000	L	12-24GB	900-1.5TB	--	H
Riverbed	Steelhead 250	S,SM	1GB	140GB	1-2Mbps	S
	Steelhead 550	SM,M	2GB	160GB	2-4Mbps	S
	Steelhead 1050 – 2050	M	2-6GB	250GB-1TB	4-45Mbps	S,H
	Steelhead 5050,6050,7050	L	8-48GB	2-5TB	90Mbps-1Gbps	H
SilverPeak	NX-1000	S,SM	--	500GB	4Mbps	S
	NX-2000,NX-3000	M,L	--	1TB	10-20Mbps	S,H
	NX-5000 – NX-9000	M,L	--	4-5TB	500Mbps-1Gbps	H

- **SERIES:** vendor or vendor model series
- **HW/MODEL:** hardware model or line module in hardware model
- **BUS (Business size):** S (Small), SM (SMB), M (Medium), L (Large)

- **RAM:** memory size
- **STORAGE:** disk storage size
- **PERF:** WAN throughput
- **SITE:** H (Hub), S (Spoke, Remote Office)

P

~ Solutions ~

PCI/DSS

Category: Business Solution
Prerequisite(s): --

Complete the steps below for building the solution:

Step 1

Network Solutions applicable for this Business Solution

This is a business solution which cannot be deployed directly. The solution will consist of one or more of the following network solutions that are applicable for deployment:

- Firewall
- Intrusion Prevention
- Content Security
- VPN & Remote Access
- Identity Access Control
- Wireless

Add one or more of these solutions and reference those respective sections for the network design.

Resources

PCI Level

Determine the PCI level that fits with your business or company in terms of credit card processing:

- **Level 1:** Process more than 6 million MasterCard (or VISA, AMEX, JCB, or Discover) transactions annually. Any company that has suffered a credit card breach in the last 12 months
- **Level 2:** Process 1 million to 6 million MasterCard (or other card brand listed above) transactions annually
- **Level 3:** Process 20,000 to 1 million e-commerce transactions annually
- **Level 4:** Process less than 20,000 e-commerce transactions annually

PCI Requirements

Below are the 12 PCI requirements for implementing on the network to be PCI compliant:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.

4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Physical Security

Category: Business Solution
Prerequisite(s): --

Complete the steps below for building the solution:

Step 1	Network Solutions applicable for this Business Solution

This is a business solution which cannot be deployed directly. The solution will consist of one or more of the following network solutions that are applicable for deployment:

- Video
- Wireless

Add one or more of these solutions and reference those respective sections for the network design.

Presence

Category: Network Solution (Voice)

Prerequisite(s): Voice (Unified Communications) Solution

Complete the steps below for building the design for the network solution.

Step 1

Scalability for Presence Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

- **Presence server:** this is the main component for the solution that can provide presence capabilities to the Voice Unified communication environment.

Step 1-2

Choose how components will be deployed

#1

Presence Server

This component usually connects into the LAN Core, Server Farm, or the Data Center Core/Access where the other Collaboration components exist.

Step 1-3

Product for Solution

Choose the appropriate presence solution based on the business size.

- **Cisco Unified Presence Server:** standalone presence server recommended for SMB, Medium, or Large networks.
- **Cisco UCM BE 6000 Series:** voice solution appliance that can support up to 1000 presence users. This is recommended for Medium and Large networks (on the low end).

Step 2	Reliability for Presence Solution

Step 2-1	Cluster

The Presence solution can be deployed in a cluster to provide reliability and scalability by using a **publisher server** which is setup first and using multiple **subscriber servers**.

Step 3	Performance for Presence Solution

Step 3-1	Determine bandwidth services

Determine the bandwidth service that is required for each component for the solution. Below are typical bandwidth services to choose between:

- **Fast Ethernet (100Mbps)**
- **Gigabit Ethernet (1Gbps)**

Recommendations: use GE if supported and available on the LAN and/or Data Center network.

Step 4

Hardware for Presence Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Matrix Table Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1

Hardware Table Options

Select the hardware for each component in the solution using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a

Presence Server

Cisco Unified Communications Manager – IM and Presence *(Medium, Large)*

Performance	--	Flexibility	--
Reliability	Cluster	Management	--
Scalability	500-5000 users	Security	--
Design Aspects	Presence Server		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance		

Cisco Unified Communications Manager – Business Edition *(SMB, Medium)*

Performance	--	Flexibility	Messaging (CUC), Contact Center (CCX) Voice & UC (CUCM)
Reliability	--	Management	--
Scalability	BE 6000: up to 1000 users	Security	--
Design Aspects	Phone System (Call Control), Voicemail, Unified Messaging (Exchange), AA, Presence Server		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance, Cisco Unified CM BE appliance		

Proxy

Category: Network Solution (Security)

Prerequisite(s): LAN and/or Data Center Solution, Internet Edge Solution

Complete the steps below for building the design for the network solution.

Step 1

Scalability for Proxy Solution

Step 1-1

Determine the components for the solution

Determine the components for this solution:

- **Proxy Appliance:** the component in this solution is a proxy appliance which is a dedicated server or a “black box” server where the proxy server application is available on the front-end for administration.

Step 1-2

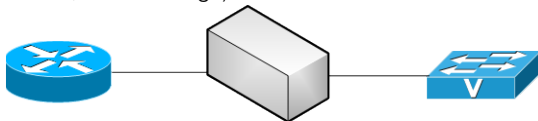
Choose how components will be deployed

Determine how each component for the proxy solution will be deployed.

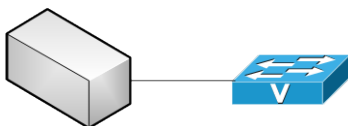
#1

Proxy Server or Appliance

This component can be deployed in-line between the Internet Edge and the LAN. Smaller to SMB/Medium environments will commonly use an in-line deployment where medium to larger environments may use an out-of-band deployment. The picture below shows how the component can be deployed IN-LINE between different solutions (e.g. LAN/Data Center, Internet Edge).



The security appliance for the proxy solution can also be deployed out-of-band connected to an edge switch behind the edge router or connected to any of the Core/Distribution/Access layers enabled for port monitoring and/or using WCCP. The picture below shows how the component can be deployed OUT-OF-BAND on the network:



In this deployment, one of the component's interfaces is plugged directly into a L2/L3 switch like any other IP enabled device (e.g. router, server, desktop, access point).

Step 2	Reliability for Proxy Solution

Step 2-1	Redundancy consideration for solution

Depending on the hardware for the component, determine the redundancy options available (if any). It will either provide Active/Passive or Active/Active Redundancy.

Active/Passive provide redundancy as a primary and secondary set. One device is active while the other device is in standby monitoring the operating conditions of the primary device and ready to transparently takeover when a failure occurs.

Active/Active provides both redundancy and load balancing operations where both devices are active.

Other options may include a **fail-open** if there is a failure. This means they will allow everything to pass through without security inspection.

Step 3

Performance for Proxy Solution

Follow the steps below to determine the bandwidth services for the proxy appliance.

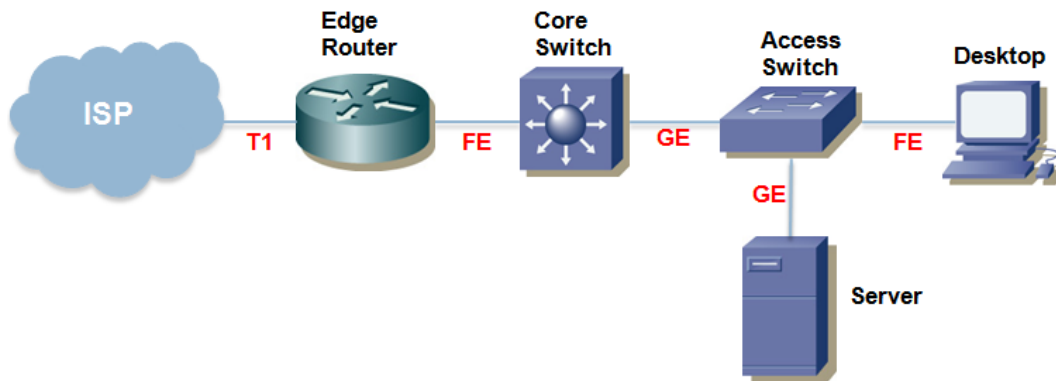
Step 3-1

Determine bandwidth services

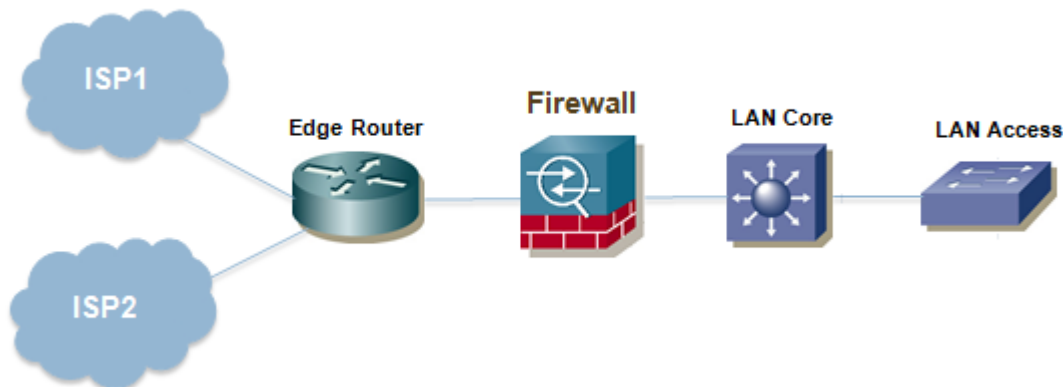
Determine the bandwidth service that is required for each component for the solution based on what exist in the topology. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)
- 10GigabitEthernet (10Gbps)

For example: below is a network design that involves two foundation solutions (LAN and Internet Edge). You will see the bandwidth identified for all connections in the design.



Now let's add the security component (e.g. Firewall, proxy appliance) in-line between the Internet Edge router and the Core switch. The bandwidth service used between these devices is Fast Ethernet (FE). Therefore, the bandwidth services required for the security component's interfaces will also be Fast Ethernet (at a minimum).

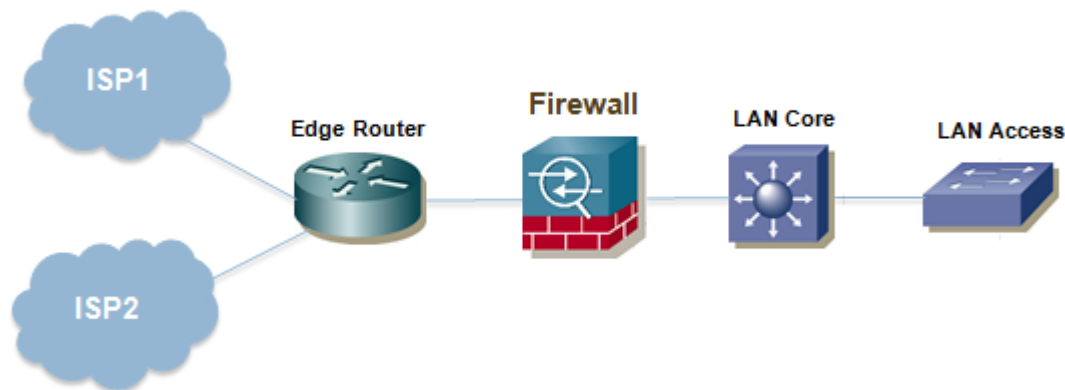


Next determine the required throughput expected through the solution component. This is based on the actual data flow and determining the lowest bandwidth service along the path. The following needs to be determined:

1. **Data Flow:** determine the expected data flow for certain services and applications through the network. For example, for Internet access the flow of data can occur from the LAN switches through the firewall, the edge router (if applicable), and out to the Internet.
2. **Bandwidth Services:** determine the bandwidth service that is used for all connections on the network along the data flow path.
3. **Lowest Bandwidth:** determine the lowest bandwidth service along the data path.

Performance (Throughput): based on the information gathered this will make up the throughput required for that in-line device. For example, if the bandwidth services on the LAN is Gigabit Ethernet (1Gbps), but the connection on the edge router is a T1 (1.544Mbps) then our expected throughput along the data path out to the Internet needs to be around 1Mbps.

Example: in the diagram below we want to determine the throughput needed on the security appliance (Firewall, Proxy):



If the bandwidth between the Edge router and the LAN Core is Fast Ethernet, then the proxy appliance interfaces would need be Fast Ethernet (at a minimum). However, understanding what the performance should be for proxy services is important. We might not need the proxy appliance to do proxy services at 100Mbps. Also in the diagram let's assume that the Internet connection to ISP1 & ISP2 involves a T1 (1.544Mbps). With those details we can complete the three steps required to understand the throughput requirements for the proxy appliance:

1. The data flow will happen from the LAN out to the Internet (and vice versa) moving through the proxy appliance.
2. Along the data path, FE is used between the Edge Router and the Core switch. Let's say that GE is used between the Core and the Access switch. And a T1 is used on the Edge router's WAN facing interface up to each ISP.
3. The lowest bandwidth service along this data path is the T1 Internet connection on the edge router.

Performance (Throughput): Therefore, the required throughput through the proxy appliance needs to be ~1Mbps for its various security services (proxy, cache, monitor, etc).

Take note of the throughput requirements for the in-line device to determine the correct hardware model.

Step 4	Design Aspects for Proxy Solution

Step 4-1	Cache or Inspection (or Both)

When traffic is forwarded to the proxy server will it cache, proxy, and/or inspect it. Consider the following for what is needed for the design.

- Should the proxy server cache and proxy all user requests for the application defined by the proxy server like HTTP.
- Should the proxy server only passively monitor traffic for trending or audit purposes for the applications defined by the proxy like HTTPS.
- Should the proxy server inspect all user requests for the applications defined by the proxy in terms of Web Content security and Anti-Virus.

Recommendations: All proxy appliances usually deal with cache and proxy user requests. Advanced configuration is required if the proxy will use content security controls or passively monitor connections.

Step 4-2	Required Services

Below are the services that are used with a proxy network solution.

- WCCP
- Port Monitor

These are services that can be implemented either on the LAN/Data Center Core component or the Internet edge router depending where the proxy appliance is located on the network.

S

~ Solutions ~

Server Solution

Category: System Solution

Prerequisite(s): LAN Solution and/or Data Center Solution

Complete the steps below for building the solution:

Step 1	Type of Servers

Every server that is deployed into a server farm will likely be one or more of the following types:

- **Infrastructure Server(s):** this type of server provides core services that other servers, desktops, to even network devices will utilize. Below are some of the Infrastructure Servers that can be deployed:
 - DNS
 - DHCP
 - Directory Services (LDAP, Active Directory, Open Directory)
- **Application Server(s):** this type of server provides specific services that is used by a user or other servers. Application servers may also require connections with an Infrastructure and/or Database server(s) to operate. Below are some of the Application Servers that can be deployed among others not listed here:
 - Email
 - Web, Web 2.0
 - Social Networking
 - Third-Party Applications
- **Database Server(s):** this could be treated as an application server, but is more of a backend system that could connect directly with infrastructure and application servers in the environment. The database servers provide storing large amounts of data and information in an organized manner.

As the system engineer or administrator determine the type of servers that should be implemented based on a recommended system design for a particular solution.

Step 2	Server Add-On Components

With the different type of servers deployed below are additional services and best practices that should be considered for each server in the environment:

- Installing an Anti-Virus program
- Administrator Account Access
- Permissions
- Performing software and OS patching

Below are redundancy options that can be used for servers on the network:

- **Power:** like network devices servers can use multiple power supplies to provide redundant power options.
- **NIC Teaming:** something often debated among system engineers due to reliability. NIC teaming can either be setup to provide fault tolerance (also called Switch Fault Tolerance or SFT) if the NIC, cable, or its connected switch fails. A redundant NIC can be connected between two Access switches providing redundancy. NIC teaming can be configured for port channeling (servers may call it port aggregation) for increased bandwidth. And NIC teaming can also be configured for load balancing (Adaptive Load Balance) where one port receives traffic and all other ports on the server will transmit traffic.
- **Load Balancing:** servers with the same role that can be part of a group to provide load balancing using such protocols like Network Load Balancing (NLB). Hardware load balancing is still recommended for better performance and scalability. NLB can support up to 25-32 server (advertised) using HTTP.
- **RAID:** Server's internal hard drives or external drives can be setup (if supported) in a RAID. RAID has many different types, but RAID5 is the most common which provides drive redundancy where if one drive fails the content is still in-tact and active on another installed drive.
- **Hardware:** the server may be redundant on another hardware device based on the nature of the application that is used.

Below is the foundation solution(s) that is required:

- LAN and/or Data Center

The server farms will exist in one or more server VLANs within the LAN/Data Center network. The servers will be connected into either (1) a dedicated Server Farm switch (for small to medium-sized server farms), (2) into the Core switch (for smaller server farms), or (3) into the Data Center Access layer (for larger server farms).

Social Networking

Category: System Solution
Prerequisite(s): Server Solution

Complete the steps below for building the solution:

Step 1	Other System Solutions applicable

This is a server based solution that is primarily designed and deployed by a system engineering team. Below are the required system solutions that are used for the Social Networking design:

- Server Solution

Social Networking is simply an application design that exist on one or more servers providing what the system solution will serve to users/clients on the network.

Software Defined Networking (SDN)

Category: Network/Server Solution
Prerequisite(s): Data Center Solution

When to use: Migrating the control plane functions (routing, switching, management) from all network devices to a centralized network controller. This allows the SDN controller to manage and view the entire network as one logical switch. Below are other use-cases for SDN:

- To provide network programmability
- To provide traffic management based on performance or latency across the network
- To provide faster provisioning of network services, slicing, and network topologies/segments for specific applications

SDN provides many advantages for Data Center networks that include:

- To provide central network intelligence
- To provide a global view of the network which is seen as one logical switch (or network)
- To provide better scalability
- Increased bandwidth requirements
- Provide faster provisioning of network services, slicing, and network topologies

#1	Deployment Model

Determine which deployment model will be used:

- **Software-based:** SDN software deployment using OpenFlow defined by the Open Networking Forum or other options like VMware.
- **Hardware-based:** SDN hardware deployment by Cisco using an Application Centric Infrastructure (ACI). This involves ACI enabled Cisco switches like the Nexus 9000 series and a SDN controller called the Application Policy Infrastructure Controller (APIC). The APIC resides between the network and the applications making the data center switches appear as one logical network. The ACI model provides API support for XML and JSON.

Below are the components in the solution and how they are deployed:

- **SDN Controller** (e.g. APIC): a dedicated appliance(s) responsible for handling the control operations (routing, switching, management) for all network devices in the Data center. SDN controller manages and views the entire network as one logical switch. The SDN controller will either be integrated with the Core switch (if supported) or connected directly into the Core layer of the network.
- **SDN enabled Network Devices** (e.g. Cisco Nexus 9000 series): these would be any network switch or router that is SDN enabled. They would be managed from a centralized controller for its control plane operations. It is also responsible for forwarding data packets based on the decisions of the SDN controller and APIs.
- **Application Program Interface (API)**: the application servers will use API scripts to interface with the SDN controller. It is used to influence how traffic flow is provisioned across the network.

Below are some caveats to keep in mind while using this service:

- SDN isn't a solution that is widely accepted nor deployed within Data Center networks. SDN is based upon open standards.
- Takes control away from the network devices. If the controller(s) experience issues it could create global network instability.

Storage

Category: Foundation Solution

Prerequisite(s): Data Center Solution (up to Step 1-6)

Complete the steps below for building the design for the foundation solution:

Step 1

Scalability for Storage Solution

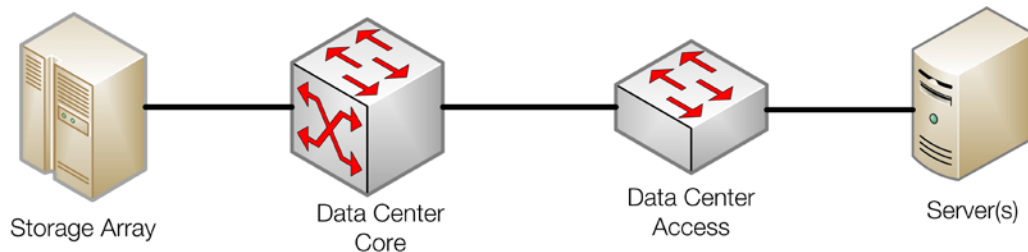
Step 1-1

Determine the storage components

Determine the storage components that exist in the solution:

- **Storage Array:** component that will connect into the Data Center Core and/or to a SAN switch topology.
- **Servers:** components that connect into a Data Center access layer.
- **Desktops:** components that connect into a LAN access layer.

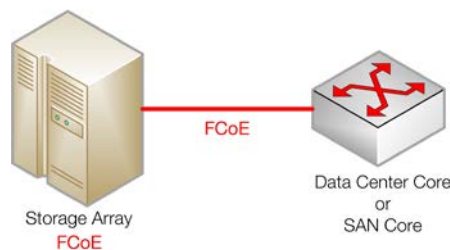
Below shows how some of these components are connected:



Determine which storage technology(s) on the storage array will be used on the network for the solution:

- **iSCSI**
 - o **Description:** a storage technology that extends SCSI traffic over an IP network for accessing a pool of shared storage. This is commonly used for low to moderate performing servers in a Small, SMB, Medium, and Large sized environment. iSCSI provides a low-cost alternative compared to using Fibre Channel if server performance isn't high. iSCSI services on the server must contend for CPU and bandwidth resources along with other network applications. The Ethernet NICs in these systems can offload iSCSI to a separate processor for increased performance.
 - o **Transport Media:** Ethernet
 - o **Storage Solution Type:** SAN (provides a shared pool of storage for servers on the network with block level storage access to raw data on a storage array)
- **Fibre Channel**
 - o **Description:** a storage technology that uses Fibre channel (FC) for accessing a pool of shared storage allowing multiple servers to share a single storage array. This is recommended for high performing production and database servers that need to access storage resources across the Fibre channel network. This technology choice provides the best performance over Ethernet, but the cost are higher. This includes support for advanced services like using Fibre Channel over long distances across a WAN (FCoIP), hardware accelerated encryption, to I/O acceleration within a SAN. Common for Medium and Large sized network environments.
 - o **Transport Media:** Fibre Channel
 - o **Storage Solution Type:** SAN (provides a shared pool of storage for servers on the network with block level storage access to raw data on a storage array)
- **Fibre Channel over Ethernet (FCoE)**
 - o **Description:** extends Fibre Channel across a 10GE connection to a switch that supports FCoE. Not recommended for Data Center networks with heavy (high bandwidth) FCoE traffic. FCoE traffic can only use a subset of the FEX uplinks up to the Data Center Core switch (using the Cisco Nexus 5500 series).
 - o **Transport Media:** 10 Gigabit Ethernet (FCoE support)
 - o **Storage Solution Type:** SAN (provides a shared pool of storage for servers on the network with block level storage access to raw data on a storage array)
- **NAS (NFS, CIFS)**
 - o **Description:** when accessing storage for desktop systems across an IP network. NFS provides file-level storage access which would only exist as part of a LUN. It would avoid the issue of "locking out" the entire LUN for read/write actions by other devices. Using NFS can also be used for low to moderate performing servers as an alternative over iSCSI. Recommended for desktop storage access usage.
 - o **Transport Media:** Ethernet
 - o **Storage Solution Type:** NAS (provides a common storage group for desktop systems across an IP network with file-level storage access to files on a storage array/NAS)

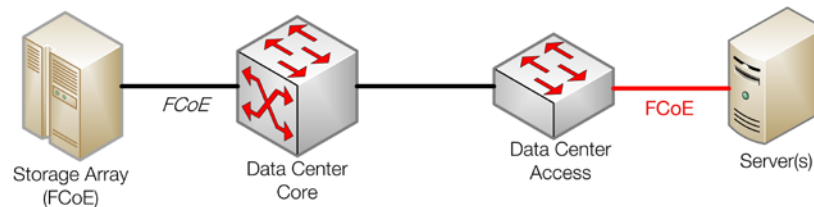
Example: the storage technology that our storage array will use and support in our environment will be Fibre Channel over Ethernet (FCoE).



Based on the storage technology for the storage array, determine the storage connectivity for the server components in the Data Center topology.

- **Using iSCSI and/or NAS:**
 - The connection from the server component to the access switch would be Ethernet.
- **Using FCoE**
 - The connection from the server component to the access switch would be a FCoE supported adapter or a Converged Network Adapter (CNA) card. The CNA cards can provide server connectivity for Data traffic (using Ethernet) and Storage traffic (using Fibre Channel). The server component (with a CNA card) can only connect using 10-Gigabit Ethernet (using Fiber optic or Twinax cabling) into the access switch.
- **Using Fibre Channel:**
 - The connection from the server component to the access switch would be a Fibre Channel adapter also called a Host Bust Adapter (HBA) card.

Example: continuing with our example, since our Storage array will use FCoE, our servers will connect into the Data Center access layer using FCoE (for Storage and Data services).

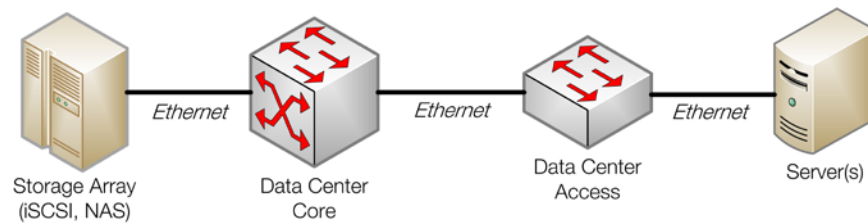


Determine how the solution will be deployed whether it will be converged within the Data Center topology or deployed as an isolated network:

#1

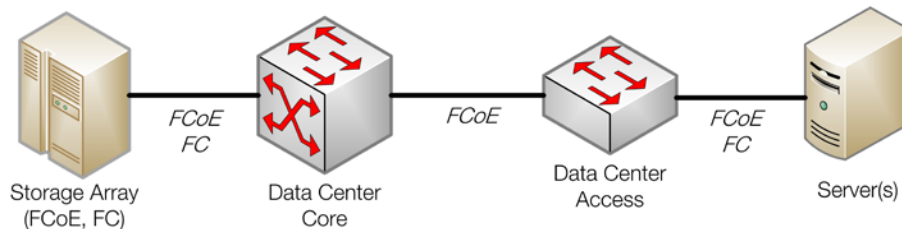
Converged Deployment (recommended)

Using iSCSI and/or NAS: the storage array component connect directly into the Data Center Core switch using Ethernet. Desktops connect into the LAN Access layer using Ethernet, The servers will connect into the LAN/Data Center Core switch or to the Data Center Access layer (for medium-larger server farms).

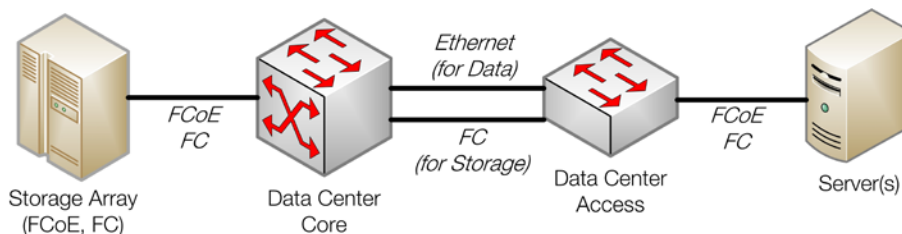


Using Fibre Channel and/or FCoE: the storage array components connect directly into the Data Center Core switch using Fibre Channel (or FCoE) depending on what storage technology is supported. Servers will use 10GE/FCoE adapters connected into the Data Center Access layer for data traffic (Ethernet) and storage traffic (FCoE). The hardware within the Data Center (Core, Access) must support FCoE like the Cisco Nexus 5500 and 2000 series which has universal ports (10GE, FCoE). Universal ports support either Ethernet+FCoE or Fibre Channel on a per-port basis. By default, all switch ports are enabled for Ethernet only.

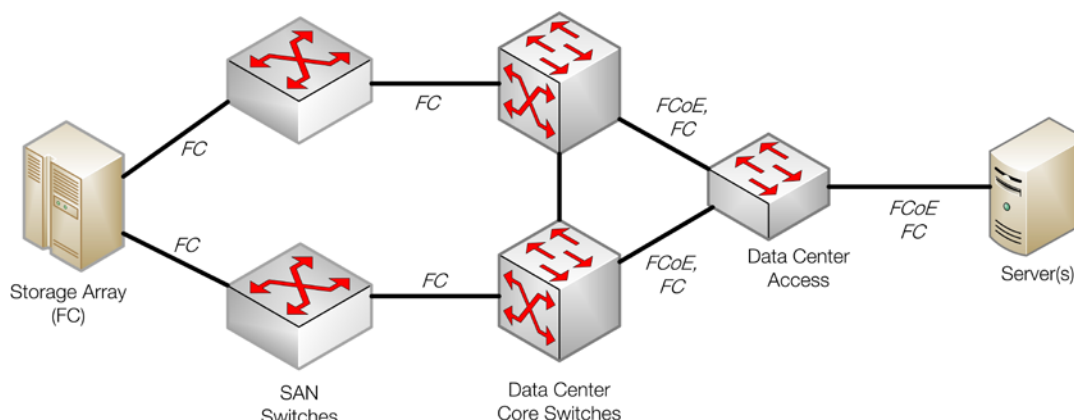
For the interconnection between the Data center switches, it can be a FCoE connection that can support Fibre Channel (for storage traffic) and Ethernet (for data traffic) as seen in the picture below. This option is recommended.



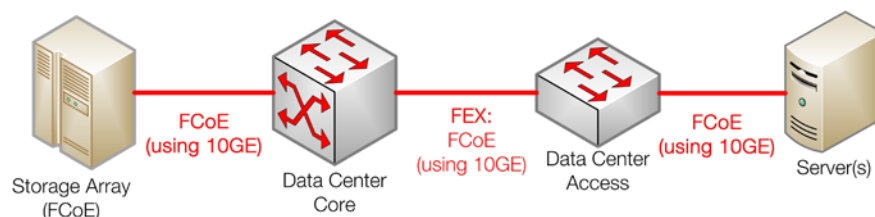
Or the interconnection between the Data center switches can be two dedicated connections. One Fibre Channel connection supporting only storage traffic and a GE/10GE connection only supporting data traffic as seen in the picture below.



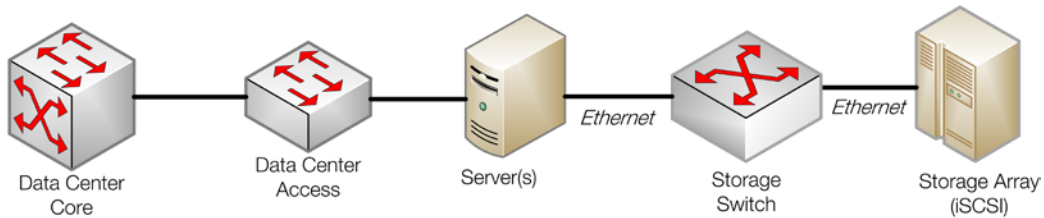
Using Fibre Channel (Large): a redundant pair of SAN switches would connect directly into the Data Center Core switch using Fibre Channel. If the Fibre Channel SAN requires a higher density of Fibre Channel port connectivity, its recommended to deploy a SAN switch (e.g. Cisco MDS 9124 or 9148). The Fibre Channel Storage array would plug directly into the SAN switches. It's recommended to have each physical SAN switch/fabric operate independently providing two distinct paths to the storage array. Fibre Channel fabric services should operate independently on each fabric. This helps to prevent against possible failures or misconfigurations in one fabric from affecting the other fabric. Servers will use Converged Network Adapters (Ethernet+FCoE support) connected into the Data Center Access layer for data (Ethernet) and storage (FCoE) traffic. The hardware within the Data Center (Core, Access) must support FCoE like the Cisco Nexus 5000 and 2000 series which has universal ports (10GE, FCoE). Universal ports support either Ethernet+FCoE or Fibre Channel on a per-port basis. By default, all switch ports are enabled for Ethernet only. Fibre Channel ports must be enabled on high numbered ports in a contiguous range on the switch. Or high numbered ports of a universal port expansion module. Changing port type to Fibre Channel (FC) requires a reboot.



Example: In our example network, we will use a Converged Deployment using FCoE. Therefore, the FCoE connections in our topology will use a 10GE type of interface that must connect to a FCoE supported switch (Cisco Nexus 5500, 2000 Series).

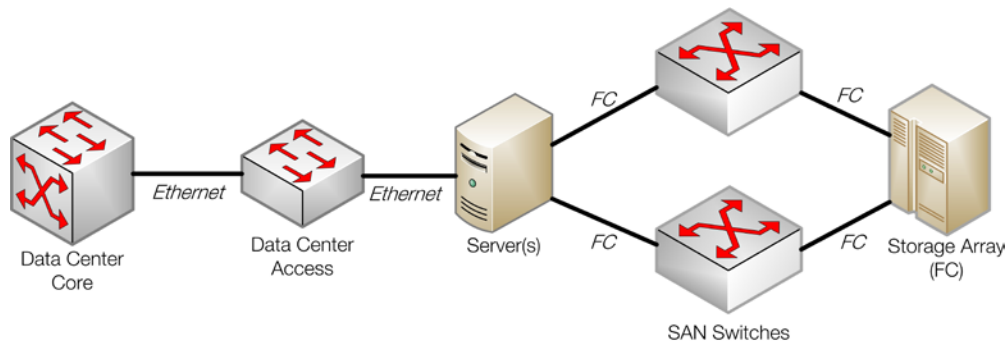


Using iSCSI: a separate Ethernet switch is used not connected into the existing Data Center topology with the exception of management connections. The storage array (iSCSI) and the servers (using a different NIC) would connect into the storage switch. This is not ideal for desktops which should use the existing LAN & Data Center topology for accessing storage resources.



Using Fibre Channel (Medium, Large): a SAN switch is used not connected into the existing Data Center topology with the exception of management connections. If the Fibre Channel SAN requires a higher density of Fibre Channel port connectivity, it's recommended to deploy a SAN switch (e.g. Cisco MDS 9124 or 9148). The storage array (Fibre Channel) would plug directly into each of the SAN switches. Each server will use a Host Bus Adapter (HBA) with a multi-mode fiber cable connected into a Fibre Channel switch port (on the SAN switch). Each Fibre Channel switch port will have a unique Port Worldwide Name (pWWN) that will be used to be uniquely identified on the SAN.

You can use redundant SAN switches which would operate independently providing different paths for storage traffic between the array and the servers. This helps to prevent against possible failures or misconfigurations in one fabric from affecting the other fabric.



Step 2	Design Aspects for Storage Solution

Step 2-1	Fibre Channel Configuration

When to use: using Fibre Channel storage technologies.

Determine the necessary details for implementing Fibre Channel on the storage network.

#1	WAN Connectivity

When to use: extending Fibre Channel traffic over a WAN.

Fibre Channel connections can be extended across long distances (in a WAN solution) using Fibre Channel over IP (FCoIP) offered on a supported SAN switch (e.g. Cisco MDS 9148).

#2	Virtual SAN (VSAN)

When to use: Large sized network, SAN/Fibre Channel, Cisco MDS 9100 SAN switch

Works similar to a VLAN in Layer 2 networks, but creates logical fabric on a single SAN switch (e.g. Cisco MDS 9100). Each VSAN has its own set of services and address space, which prevents an issue in one VSAN from affecting other VSANs. So each VSAN is completely isolated which is a SAN recommendation. You can create a VSAN for production storage traffic, development/lab storage traffic, and other usages similar to a network VLAN.

#3	Zoning

Zoning provides a means for a SAN fabric to restrict visibility and connectivity among devices connected to a SAN. This can be done for controlling which initiators can see which targets.

Targets are basically disks or tape devices. Initiators are servers that connect to a disk (or tape) on the storage array. You can configure a single initiator and a single target per zone. Or you can configure a single initiator to multiple targets in the same zone. You should limit zoning to a single initiator with a single target.

Initiator-based zoning allows a switch port to be independent by using the world wide name (WWN) of the end host.

Caution: any configuration change to zone can be disruptive to the entire SAN fabric

#4

Device Aliases

It's recommended to use a user-friendly naming format for pWWNs in a SAN fabric. You can consider the following naming standard:

Naming Standard: <rack>-<host_type>-<host_name>-<hba_card>-<hba_port>

Example: r1a-c210-srv1-hba0-p1

This means our server named SRV1 (Cisco UCS 210) is located in rack 1A in our data center. This server is plugged into a FC switch port from its primary HBA (hba0) on port 1.

Step 2-2

FCoE Configuration

#1

General Configuration

When to use: using Cisco Nexus 5500 & 2200 series switches and Fibre Channel over Ethernet (FCoE) storage technologies.

The server/host with a CNA adapter (FCoE supported) would plug into an Ethernet port on a Cisco Nexus 2200 switch.

A VLAN would be mapped to a VSAN where the Fibre Channel storage traffic would be located. The Ethernet interface would be configured as a trunk port with VSAN (for FC traffic) and VLANs (for Data traffic). You need to create a virtual Fibre Channel (vFC) interface for all Fibre Channel traffic which will be associated to the Ethernet interface that the server/host is connected to. This is important in order to map a FCoE interface to Fibre Channel.

Note: if you are using a Cisco UCS C-Series server with CNA (Cisco P81E) you must have the FCoE VSANs configured for the vHBA operation in order for it to connect to the Fibre Channel fabric.

#2

Services

Below are the recommended services to add with the storage solution (using FCoE):

- **QoS:** It's recommended to provide lossless data for all FCoE traffic end-to-end within the Data Center.

When to use: using iSCSI storage technologies.

These are services that can be used when deploying a storage solution.

- Jumbo Frames
- Flow Control

For iSCSI or NAS storage technologies that resides over Ethernet its recommended to enable Jumbo frame support globally on the switch and enable Flow control for all Gigabit Ethernet ports. These are services that are configured on the Ethernet switches where the storage unit and servers are connected.

When to use: using Cisco MDS and/or Cisco Nexus SAN switches in a storage solution for Fibre Channel.

Cisco Data Center Network Manager (DCNM) for SAN Essentials Edition can be used to manage and configure the storage solution. This includes the Cisco MDS Device Manager and Cisco SAN Fabric Manager.

There is no cost if you are managing a single SAN switch. If you will be managing multiple SAN switches at the same time, it will require a licensed version.

Step 4	Hardware for Storage Solution

#1	Hardware Options

Below are hardware considerations for the components in the solution:

#1	SAN switches (Fibre Channel only)

- **Cisco MDS 9148 Multilayer Fabric Switch:** Fibre Channel SAN switching can be supported on a Fibre Channel only switch like the Cisco MDS 9148. The Cisco MDS 9148 Multilayer Fabric Switch is ideal for a larger SAN fabric with up to 48 Fibre Channel ports providing 48 line-rate 8-Gbps Fibre Channel ports. Plus this SAN switch offers advanced options like hardware-based encryption services, tape acceleration, to Fibre Channel over IP (FCoIP) support for longer distance SAN extension.

#2	Data Center switches (FCoE support)

- **Cisco Nexus 5500UP:** Fibre Channel SAN switching can also be converged with Ethernet, FCoE, and Fibre Channel connections on a Cisco Nexus 5500UP (and Nexus 2000 series with Fabric Extenders). This hardware choice can be determined during the Data Center solution design.

#3	Storage Array

- EMC VNX-5300
- NetApp FAS3200

NetApp FAS3200: Below are some of the main aspects and properties of the NetApp Storage Array:

- **Hardware:** FAS3200
- Supports up to 3-Petabytes of versatile storage
- Supports NAS (NFS, CFS) and SAN (FC, FCoE, iSCSI) in a single pool of storage
- **RAID Data Protection (RAID-DP):** protects against the concurrent loss of two drives in a single RAID group. RAID-DP is also safer than data stored on RAID 5 and more cost effective than RAID 10.
- NetApp Unified Connect delivers data access using NFS, CIFS, iSCSI, and FCoE protocols concurrently over a shared network port using the NetApp unified target adapter (UTAs). Requires Data ONTAP 8.0.1 and later. The FC protocol license is required for FCoE functionality. Below are other aspects for UTAs:
 - UTA is also known as a converged network adapter (CNA).
 - Each UTA has a dual-port 10 Gbps NIC and a 10-Gb FCoE target adapter which is installed in a PCI-express (PCI-E) expansion slot.
- **Virtual Interface (VIF) and Port-Channel:** The storage array would be connect into the Data Center switches (e.g. Cisco Nexus 5500UP series) using dual 10-Gb Ethernet interfaces in a port-channel. The NetApp controller would configure this as a Virtual Interface (VIF). This deployment can provide redundancy because of the dual links and support carrying storage traffic for FCoE or iSCSI.

The design for the storage solution is completed.

Please continue with the Data Center design starting at "**Step 2: Reliability for Data Center**"



~ Solutions ~

Teleworker

Category: Network Solution
Prerequisite(s): WAN and/or Internet Edge Solution

Complete the steps below for building the design for the network solution.

Step 1

Performance for Teleworker Solution

Step 1-1

Determine bandwidth services

Determine the broadband or leased line connection that will be used at the teleworker's home office:

- DSL
- Cable
- T1

Recommendations: A teleworker will likely have a broadband connection (e.g. DSL, Cable) due to fast speeds and low cost. Using a T1 may provide better guarantee of service, but the cost is higher. The T1 could be a private T1 connecting back to the main office, but the cost is still high plus the home network is considered as an untrusted network because we are not aware of the network activity or security at the home office.

Based on the bandwidth services, determine the appropriate deployment for the teleworker office.

- **Integrated Unit Model:** Using DSL (no Cable) where the teleworker is using one device where the DSL is plugged directly into the router that also handles all QoS and VPN services. This avoids the need to use the DSL modem, which tends to be unreliable.
- **Dual Unit Model:** Using DSL (no Cable) with two devices. One device is a router directly connected into the DSL network configured for routing and QoS services. The second device which connects into the first router and into the LAN providing VPN services. The first router device is usually a managed router controlled by the ISP and is less common for most teleworker environments.
- **Integrated Unit and Access Model:** Using DSL or Cable requiring two devices. One is the broadband modem (provided by the ISP) and the other is the router providing VPN and QoS services managed by the teleworker/client. This is the most common setup used for Teleworker networks today. This is the simplest model of the three, but there are concerns with the different upload/download speeds which require traffic shaping on the VPN router.

Determine the components for the solution based on the deployment:

- **ISP Equipment:** this may be one or more components managed by the ISP that will connect into the Teleworker Router.
- **Teleworker Router:** the main component for the solution requiring VPN, QoS and DHCP services. This component connects into the ISP equipment through a particular bandwidth service. The LAN of the teleworker router connects to the computers directly or to a dedicated switch.
- **Bandwidth:** this component specifies the bandwidth services that will be used for the solution. This component exist between the Teleworker Router and the ISP equipment.
- **Head-end Router:** this component exist at the main office location (Hub) across a WAN or through the Internet using a VPN. This component is connected into the Teleworker Router via a site-based VPN (or a private WAN connection).

Step 3	Flexibility for Teleworker Solution

Step 3-1	Integration with Voice

The teleworker can use voice services at their virtual office, however, QoS is required on the Teleworker router and the main office network to ensure proper delivery and quality of voice calls.

Services Required: Quality of Service (QoS)

Step 3-2	Integration with WAN and/or VPN

If the Teleworker will connect back to the main office to access network resources determine the method in which the Teleworker's network will connect:

- **Site-Based VPN:** The teleworker uses its Internet connection where its VPN router automatically establishes a secure tunnel (VPN) across the Internet to access network resources without the user needing to do anything. The VPN is seen as a private point-to-point connection.
- **Client-Based VPN:** The teleworker uses its Internet connection, but the client needs to use a VPN application to establish a secure tunnel (VPN) across the Internet before accessing network resources.

Services Required: Virtual Private Network (VPN)

- **Private WAN:** A private leased line (e.g. T1) is provisioned between the teleworker location and the main office. The teleworker network is treated as another branch office.

Recommendations: Using a Site-Based VPN is recommended because it is cost effective and provide a secure connection to access internal network resources for a teleworker.

Step 4

Reliability for Teleworker Solution

This solution can be configured with redundant routers, service providers, and connections (private connection, VPN connection) if desired.

Step 5

Design Aspects for Teleworker Solution

Step 5-1

IP Addressing

Determine the IP addressing assignment the teleworker will receive from the ISP. This depends on the ISP and what the teleworker has ordered from the provider. Below are the IP addressing options available:

- Static
- Dynamic (DHCP, PPPoE) ; most common and recommended

Recommendations: Understanding this will help to determine the best VPN solution to use. If the IP assignment to the Teleworker's equipment is dynamic then we know that Client-VPN, Easy VPN, or DMPVN are ideal VPN services to deploy. Using a standard IPSec VPN tunnels will require a static IP address for best results.

Step 5-2

Services to include with solution

Below are network services used for the Teleworker solution.

- Network Address Translation (NAT)
 - NAT Transparency (NAT-T)
- DHCP

These are services that are implemented on the Teleworker router component.

A large, white, serif capital letter 'U' is centered within a dark gray rectangular box. The letter is bold and has a classic, slightly flared top.

~ Solutions ~

Unified Computing

Category: System Solution
Prerequisite(s): Data Center Solution

Complete the steps below for building the solution. First, determine what type of computing solution is needed for the design and focus on that section(s) only:

1. **Blade Server:** a unit (or chassis) that consist of many physical servers inside a single chassis. This allows placing all of your servers into a chassis for single point of management. These servers can further be virtualized using VMware or Hyper-V.
2. **Unified Computing System (UCS):** recommended Unified Computing solution to use when deploying full rack of 200+ servers in your data center. This solution also supports easy management, scalability, and performance to the computing environment. UCS is considered as the next generation of blade services, switches, storage adapters, and a network fabric logically seen as one logical unit for easy management. Disk space, CPU, memory can be easily allocated for a particular server. In a UCS solution you can also scale when needed by adding additional blade services to the system.

1	Blade Server Solution

Step 1	Network Connectivity

Determine how the blade server will connect into the network (usually the Data Center):

- **Pass-Through:** each Blade server has its own NIC port that would be connected into the Data Center Access switch.
- **Blade Switch:** the blade server has an integrated switch installed providing a single connection from the blade server to the Data Center Aggregation layer, which can also be configured for 802.1Q if the servers in the blade server will be configured in different VLANs. Note: The integrated switch in the blade server chassis generates spanning-tree BPDUs and therefore cannot be connected to Cisco Nexus 2000 fabric extenders.

Step 2	Services

These are the services that can be used when deploying the blade server solution.

- Virtual LAN (VLAN)
- Trunking (802.1Q)

These are services that are implemented on all Data Center switches.

2	Unified Computing Solution

Step 1	Considerations and Design Resources

Design resources for independent consultants or network engineers within companies is not easily obtained as of today unfortunately. There are a lot of great resources available for building a Cisco UCS solution using the NetformX program for building a build of materials (or BOM) for Cisco UCS. There are great training labs and documentation only available to these advanced partners. So there are a lot of great resources available, but it's very restricted for those Cisco partners. These resources should be easily available to consultants/engineers to increase their knowledge and skill set for deploying ideal Cisco UCS designs. This includes the ordering process. You can't just order a Cisco UCS system from any reseller like you can do for a router or switch. Again you must work through a valid UCS Authorized Partner, but in return they have to work with Cisco and with a special Cisco UCS sales team. This "special" team is responsible for validating the UCS configuration, approving the UCS build, then placing the order for the client. Therefore, any consideration for deploying a Cisco UCS solution will require working with an authorized UCS partner.

Step 2	Components: UCS System Deployment Model

Determine what UCS system deployment model will be used in the Data Center:

1. Standalone UCS System (Cisco C-Series)
2. Chassis UCS System (Cisco UCS 5100 Chassis and B-Series)

#1	Standalone UCS System

This is a standalone rack-mount server (Cisco UCS C-Series) that is ideal for small to medium-sized server farm environments including branch offices. The standalone servers can be added on an incremental bases when additional server resources are needed.

The standalone can also be used as part of the Cisco Unified Computing System where everything is unified and managed as single logical system unit.

#2	Chassis UCS System

This UCS system involves two components. The main component is the Cisco UCS 5100 Series Blade Server Chassis which consist of fabric extenders modules and four power supplies. The chassis will also support half-size or full-size Cisco UCS B-Series Blade Servers used as part of the Cisco Unified Computing environment.

The half-slot blade servers (Cisco UCS B22, B200, and B230) provide one 10GE/Fibre Channel connection to each Fabric Extender (max of 2) in a chassis. They provide high density and computing resources. The full-slot blades servers (Cisco UCS B250, B420, and B440) provide two 10GE/Fibre Channel connections to each Fabric Extender (max of 2) in a chassis. They provide extended memory along with increases CPU, storage and I/O throughput resources.

Based on the deployment model determine the network adapters will be used in the UCS system.

#1

Using Standalone UCS System Option

The standalone C-Series rack-mount server can be equipped with one or more of the following type of network adapters.

- **Host Bus Adapter (HBA):** a network adapter that support Fibre Channel (FC) connections. This adapter should be used when the standalone system is connected directly into a Fibre Channel storage fabric (or SAN switch).
- **Converged Network Adapter (CNA):** a network adapter which allows Ethernet data and Fibre Channel over Ethernet (FCoE) storage traffic to share the same physical cabling (up to two 10-Gigabit Ethernet interfaces to a server). This is also called a Unified wire. This adapter should be used when the standalone server will be connected to either a Cisco Nexus 2232PP FEX (Data Center Access) or directly to the Cisco Nexus 5500UP (Data Center Core) for data and storage traffic. The Cisco Nexus 5500UP switch fabric would be responsible for splitting the FCoE traffic off to the Fibre Channel attached storage array. If FCoE will be used, the uplinks must use a fiber optic or Twinax connection to maintain the bit error rate (BER) thresholds for Fibre Channel transport.

#2

Using Chassis UCS System Option

The UCS Blade Chassis and B-Series blade servers can be equipped with one or more of the following type of network adapters:

- **Fabric Extender (or IOM):** the Cisco UCS 2200 Series Fabric Extenders is like a mini fabric interconnect switch that exist within the Cisco UCS 5100 Series Blade Server Chassis with four 10GE/Fibre Channel ports. This module would then connect into a Fabric Interconnect switch. So the Fabric Extenders extends the fabric from the fabric interconnects into each of the chassis for Ethernet, FCoE, and management purposes. Only two IOM can exist in a single UCS chassis.
- **Server Adapter or Mezzanine Card:** these are virtual adapters that build a virtual NIC on the blade servers and bind them to the Fabric Extender for network connectivity.
- **Cisco Virtual Interface Cards (VICs):** Allows each virtual adapter to appear as a separate virtual interface on the fabric interconnects. It can support up to 256 total virtual interfaces split between the virtual network interface cards (vNICs) and vHBAs.

#1

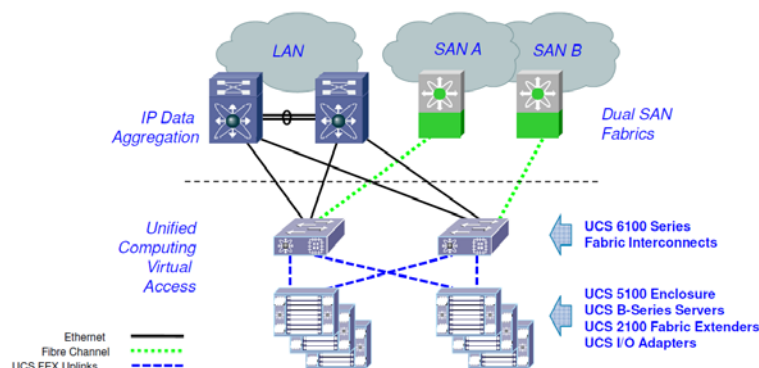
Using Standalone UCS System Option

The standalone UCS server, can be connected directly into an access switch (e.g. Cisco Nexus 2200 FEX) within a two-tier Data Center topology. Or directly into the core switch (e.g. Cisco Nexus 5500UP) within a one-tier Data Center topology. The standalone UCS server would connect into one of these switches from a converged network adapter that can provide Ethernet data and FCoE storage traffic over the same physical cabling.

#2

Using Chassis UCS System Option

- **Fabric Interconnect Switch:** the Cisco UCS 6200 Series Fabric Interconnects is considered as the Core switch for the UCS topology providing both network connectivity (10-Gb Ethernet, Fibre Channel, and FCoE) and management capabilities. Below are other aspects:
 - o (1) The Fabric Interconnect switch can connect to a Data (Ethernet) network and to a Storage (Fibre Channel) network converged together.
 - o (2) The default and recommended configuration for the fabric interconnects is End-Host mode which don't operate as full LAN switches but rely on the upstream data center switching fabric. This will make the Cisco UCS appear as a virtualized computing system with multiple physical connections.
 - o (3) It's also recommended that multiple fabric interconnects be clustered together as a pair.
 - o (4) The Fibre Channel ports, on the fabric interconnects, that connect into the SAN will operate in N-port Virtualization (NPV) mode. NPV allows multiple Fibre Channel port IDs to share a common physical port.



Below are the available management capabilities for how the UCS system can be managed.

#1

Using Standalone UCS System Option

- **Cisco UCS Manager:** the standalone server can be managed by the Cisco UCS Manager if the server is connected to the fabric interconnects via Cisco 2232PP Fabric Extenders. The newer Cisco UCS C-Series M3 servers, equipped with the Cisco UCS VIC 1225, can be managed with a single cable connected to the Cisco 2232PP fabric extenders.
- **Cisco Integrated Management Controller (CIMC):** an embedded OOB sub-system that provides KVM capabilities to the server for controlling power to viewing server properties, monitoring faults and alarms. The CIMC can be access via a web-based GUI or SSH Protocol-based CLI for administration and monitoring of the server.

#2

Using Chassis UCS System Option

- **Cisco UCS Manager:** this is how the UCS topology is managed in terms of the UCS chassis, blade servers, fabric interconnections, and server adapters. This is software that is embedded on the fabric interconnects providing complete configuration and management capabilities to the UCS system. This configuration can be replicated between two fabric interconnects that may exist in the topology to provide redundancy. To perform basic tasks, you can access the UCS Manager using a Java-based Web GUI or a command-line interface (CLI). You can also use XML APIs which are included with the system. The Cisco UCS Manager GUI provides role-based access control (RBAC) which supports multiple levels of administrative rights to the system based on a user's access level or area of expertise. For advanced level tasks, you can use a software application called Cisco UCS Central which provides a centralized user interface for managing multiple UCS domains with thousands of servers. Cisco UCS Central can also be integrated with Cisco UCS Manager to provide global configuration capabilities for pools, policies, and firmware.

Determine the number of servers needed for the Data Center based on whether they will use an entire physical blade server or if servers will be virtualized within a single blade server:

- **Physical Server:** dedicated server on a single blade server
- **Virtual Server:** multiple servers virtualized on a physical blade server.

Recommendations: if there is a mixture of both physical and virtual servers include both numbers. Cisco UCS servers have been certified to use the following hypervisor systems: VMware ESX, Microsoft Hyper-V, Citrix Xen

Example: let's create a scenario for how to build a simple UCS solution. Let's say that our Data Center consist of 50 servers that we want to consolidate into a Cisco UCS solution. 25 of the servers will be physical servers and the other 25 servers will be virtual machines.

From the total number of servers calculated whether they are physical and/or virtual servers determine if a common group of servers share similar performance and resources. For example, let's say that 50 physical servers are needed. Well within that number 25 servers will be high performing with high CPU and memory resources. And the other 25 servers will be standard performing within limited CPU processing and memory resources.

Determine these server groups based on some of the following criteria:

- High Performance (e.g. 24-48GB+ of memory, Dual 4-8 Core CPU) ; Recommended for physical server running Virtual machines.
- Medium Performance (e.g. 8-12GB of memory, Dual CPU or Dual 4-Core CPU) ; Physical server running Virtual machines
- Standard Performance (e.g. 3-4GB of memory, Single/Dual CPU)
- Energy Efficient & Performance
- Other (based on any unique requirements)

Example: Continuing with our UCS example, 25 physical servers will be standard performance and our 25 virtual servers will also be standard performance servers residing on a medium-to-high performance server.

Determine the resource requirements for each physical and virtual server(s) type that will be used based on the following:

- **CPU:** determine the CPU processing speed, the number of CPUs (1-2 CPU processors), and the number of CPU cores (4-8 cores)
- **Memory:** the amount of memory resources required on the server.
- **LAN connectivity:** determine what LAN bandwidth service will be used. This will likely be 1GE.
- **SAN connectivity:** determine what SAN bandwidth service will be used. This will be 1G, 2G, or 4G Fibre Channel interfaces.
- **Boot media:** will the server boot from the SAN or locally from the hard disk.
- **LAN throughput:** determine the throughput expected with the server on the LAN.
- **SAN throughput:** determine the throughput expected with the server on the SAN fabric.

Example: let's determine the resources for each of our server types. For the "Standard Performance Server Type for the Physical Servers" below are the resource requirements we need for each server:

- **CPU:** Single CPU processor
- **Memory:** 4GB
- **Boot media:** Local media
- **LAN throughput:** 500Mbps
- **SAN throughput:** up to 400Mbps

For the "Virtual Machine Server Type" below are the resource requirements:

- **CPU:** dual 4-Core CPU
- **Memory:** between 3-4 GB
- **Boot media:** SAN
- **LAN throughput:** 300Mbps
- **SAN throughput:** 400Mbps

Redundancy with the Cisco UCS is strongly recommended to provide high availability with the UCS cluster. The following needs to be considered if redundancy will be used.

- Two separate fabric interconnect switches are required.
- Only one of the fabric interconnect switches are active at any given time, thus, no load-balancing is possible.
- The Server Blade chassis consist of two fabric extenders (I/O modules or IOM) each one connecting into one of the fabric switches NOT both.
- A passive interconnection link exist between the fabric switches to learn about its availability.
- Fabric interconnect switches must be the Cisco UCS 6100 switches and not the Cisco Nexus 5000 if they will be managed as a centralized solution (recommended).

Example: we do want redundancy for our UCS solution, therefore two fabric interconnect switches will be required in our UCS design.

Determine the server blade hardware for each server type:

You can use one of the templates below for reference based on other UCS deployments that may align with the resource requirements for the solution design.

Server Blade Templates:

Server Template	Performance	CPU	Memory	LAN	SAN	Blade Server To Use	Power	Disk
ST-1	High	Xeon X5680 (x2)	96GB 24x 4GB DIMM	UCS VIC M81KR	n/a	UCS-B250-M2	130W	n/a
ST-2	Standard	Xeon X5650 (x2)	24GB 12x 2GB DIMM	UCS VIC M81KR	n/a	UCS-B200-M2	95W	n/a
ST-3	Energy	Xeon X5620 (x2)	12GB 6x 2GB DIMM	UCS M71KR-Q	n/a	UCS-B200-M2	60W	n/a
ST-4	High	Dual 4-Core Fast CPU Xeon X5570 (x2)	48GB 12x 4GB DIMM	3Gbps 1.5Gbps	FC 1Gbps 1Gbps	B200-M1	n/a	146GB 2x 73GB
ST-5	Medium	Single Fast CPU Xeon E5520	8GB 4x 2GB DIMM	1Gbps 1Gbps	FC 1Gbps 400Mbps	B200-M1	n/a	146GB 2x 73GB
ST-6	Standard	Single CPU Xeon L5520	4GB 2x 2GB DIMM	1Gbps 500Mbps	FC 1Gbps 400Mbps	B200-M1	n/a	n/a

Virtual Server Templates:

VM Server Template	# of VM?	Memory per VM	LAN	Blade Server To Use	Using Server Blade Template
VM-1	67	3GB	300Mbps	B440-M1	N/A
VM-2A	32	3GB	--	--	ST-1
VM-2B	24	4GB	--	--	ST-1
VM-3A	16	3GB	--	--	ST-4
VM-3B	12	4GB	--	--	ST-4

Note: reference cisco.com for the most recent Cisco UCS chassis and B-Series Blade server hardware available.

Example: based on our requirements let's use one of Server Blade Templates available from the chart. For our 25 physical server (Standard Performance) let's use Server Template "ST-6" which aligns with our requirements. This uses a half-size blade server.

For our 25 virtual servers (standard performance) we can use the Virtual Server Template "VM-1" that can support up to 67 VM if using 3GB of memory for each virtual machine on VMware ESX. However, we want 4GB per virtual machine, so the total memory required is 100GB, which is still supported with the B440-M1 Blade Server which has 32 DIMM slots.

Or we can use Virtual Server Template "VM-2A" giving us 32 virtual machines allocating 3GB per VM. Another option involves using two Virtual Server Templates, "VM-3A" for 16 virtual servers using 3GB and "VM-3B" for 12 virtual machines using 4GB.

For simplicity let's choose virtual server template "VM-2A" which uses a full-sized blade server.

For each server type summarize the following before continuing to the next step:

- Total number of blade servers
- The total number of Blade server chassis' needed, which can hold up to 8 half-size blade servers or 4 full-size blade servers
- Total LAN throughput
- Total SAN throughput
- Total Server throughput (LAN throughput + SAN throughput)
- Total number of 10 GE LAN uplinks; based on the total LAN throughput
- Total number of 4G/8G FC uplinks; based on the total SAN throughput
- Total number of 10 GE server downlinks; based on the combined LAN & SAN throughput

Example: here is a summary of our server blades needed based on our requirements:

- **Total number of blade servers:** Physical Servers (x25 of the UCS-B200-M1), Virtual Servers (x1 of the UCS-B250-M2 for our 25 virtual machines).
- **The total number of Blade server chassis:** 4+ Blade server chassis are needed
- **Total LAN throughput:** $(25 \times 500\text{Mbps}) + (25 \times 300\text{Mbps}) = 20\text{Gbps}$
- **Total SAN throughput:** $(25 \times 400\text{Mbps}) + (25 \times 400\text{Mbps}) = 20\text{Gbps}$
- **Total Server throughput:** $20\text{Gbps (LAN)} + 20\text{Gbps (SAN)} = 40\text{Gbps}$
- **Total number of 10 GE LAN uplinks:** we need two 10GE LAN uplinks
- **Total number of 4G/8G FC uplinks:** we need five 4G FC uplinks or three 8G FC uplinks.
- **Total number of 10 GE server downlinks:** four 10GE server downlinks

- (1) Build the UCS chassis considering the server types and blade servers involved. Also reference the LAN and SAN throughput requirements when building the chassis that align with the 10GE server downlinks to the fabric interconnect switches. Determine the following:

- The server blades populated in the chassis
- The **number of IOM in the chassis**. If there is redundancy requirements then two are required.
- **LAN throughput:** calculated using the LAN throughput for each blade server based on the number determined in “Step 8” for the LAN throughput for each server.
- **SAN throughput:** calculated using the SAN throughput for each blade server based on the number determined in “Step 8” for SAN throughput for each server.
- The **number of 10GE server downlinks**; this is based on the total LAN and SAN throughput determined above.

- (2) **Oversubscription** may occur if the combined LAN and SAN throughput exceed 40Gbps through one IOM.

The performance of the UCS chassis is based on the following:

- **Mid-plane:** each half-blade server (through the Mezzanine card) has a single 10GE/FC connection to each IOM in the chassis. Or for each full-blade server (through two Mezzanine cards) it has two 10GE/FC connections to each IOM in the chassis. This means the combined performance through the mid-plane to the IOM is 80Gbps and happens “behind-the-scenes”.

- **IOM Uplink:** On the front-end, each IOM has four 10GE/FC ports that extend to a single Fabric Interconnect switch providing 40Gbps performance throughput to the Fabric Interconnect.

If there is oversubscription the following can be considered:

- Accept the oversubscription, which could result in potentially longer delay and buffering of LAN/SAN packets on the fabric extender.
- Re-evaluate the throughput requirements for the LAN and SAN. Maybe the utilization is a lot lower thus changing the combined throughput values.
- Use an additional UCS chassis to create minimal to no oversubscription not exceeding 40Gbps through the mid-plane of the chassis through the IOM. This option is the better choice, but the costs will drastically be higher and provide an additional component to manage in the cluster.

Example: here we will populate our server blades into the UCS chassis based on our requirements and what we gathered:

- **Chassis 1:**
 - **Blade Servers:** 8x UCS-B200-M1 (Half-Blade) used for 8 physical standard servers
 - **IOM:** 2x IOM for UCS chassis redundancy
 - **LAN Throughput:** 500Mbps x 8 = 4Gbps
 - **SAN Throughput:** 400Mbps x 8 = 3.2Gbps
 - **The number of 10 GE server downlinks needed:** 4Gbps + 3.2Gbps = 7.2Gbps. Only one 10GE is needed per IOM up to one of the fabric interconnect switches.
 - **Oversubscription:** None, the combined total of 7.2Gbps is below 40Gbps
- **Chassis 2:**
 - **Blade Servers:** 8x UCS-B200-M1 (Half-Blade) used for 8 physical standard servers
 - **IOM:** 2x IOM for UCS chassis redundancy
 - **LAN Throughput:** 500Mbps x 8 = 4Gbps
 - **SAN Throughput:** 400Mbps x 8 = 3.2Gbps
 - **The number of 10 GE server downlinks needed:** 4Gbps + 3.2Gbps = 7.2Gbps. Only one 10GE is needed per IOM up to one of the fabric interconnect switches.
 - **Oversubscription:** None, the combined total of 7.2Gbps is below 40Gbps
- **Chassis 3:**
 - **Blade Servers:** 8x UCS-B200-M1 (Half-Blade) used for 8 physical standard servers
 - **IOM:** 2x IOM for UCS chassis redundancy
 - **LAN Throughput:** 500Mbps x 8 = 4Gbps
 - **SAN Throughput:** 400Mbps x 8 = 3.2Gbps
 - **The number of 10 GE server downlinks needed:** 4Gbps + 3.2Gbps = 7.2Gbps. Only one 10GE is needed per IOM up to one of the fabric interconnect switches.
 - **Oversubscription:** None, the combined total of 7.2Gbps is below 40Gbps
- **Chassis 4:**
 - **Blade Servers:** 1x UCS-B200-M1 (Half-Blade) used for 1 physical standard servers
 - **Blade Servers:** 1x UCS-B250-M2 (Full-Blade) used for our Virtual server environment (with 25 virtual machines)
 - **IOM:** 2x IOM for UCS chassis redundancy
 - **LAN Throughput:** (500Mbps x 1 = 500Mbps) + (25 x 300Mbps) = 8Gbps
 - **SAN Throughput:** (400Mbps x 1 = 400Mbps) + (25 x 400Mbps) = 10.4Gbps
 - **The number of 10 GE server downlinks needed:** 8Gbps + 10.4Gbps = ~20Gbps. Therefore, two 10GE is needed per IOM up to one of the fabric interconnect switches.
 - **Oversubscription:** None, the combined total of ~20Gbps is below 40Gbps
 - We also have open chassis slots available for additional expansion.

For each Blade Chassis summarize the following before continuing with the next step:

- Determine the **total number of UCS blade chassis** built to accommodate all of the required blade servers.
- Determine the number of interconnect uplink/downlink ports that are required on the fabric interconnect switches:
 - **10GE server downlinks:** the total number of 10GE uplinks from one IOM (not both) based on the number of chassis' and uplink ports needed from the last step that will connect into one of the fabric interconnect switches.
 - **10GE LAN uplinks:** based on the grand total of LAN throughput from the blade server determined in "Step 11". These are interfaces that will connect up to the LAN/Data Center switches (e.g. Nexus 7000 switch) using Ethernet.
 - **4G/8G FC uplinks:** based on the grand total of SAN throughput from the blade server determined in "Step 11". These are interfaces that will connect up to the SAN fabric (e.g. Cisco MDS switches) using Fibre Channel.

Example: here is a summary for our UCS chassis that will be used including the breakdown of our uplink and downlink ports:

- We are using a total of 4 UCS chassis' in our design.
- **10GE server downlinks:** five 10GE server downlink ports ($1+1+1+2 = 5$)
- **10GE LAN uplinks:** two 10GE uplink ports to the LAN/Data Center Core switch (e.g. Cisco Nexus 7010).
4G/8G FC uplinks: five 4G FC uplink ports to the SAN Core switch or three 8G FC uplinks to the SAN Core switch (e.g. MDS 9000 series).

- Determine the **total number of 10GE ports** needed (server downlink and LAN ports) on the switch.
- Determine the **total number of Fibre Channel ports** needed (SAN ports) on the switch.

Example: here is a summary of the fabric interconnect ports that are needed on our switch:

- **Total 10GE ports:** seven 10GE ports needed in total.
- **Total 4G/8G FC ports:** five 4G FC ports or three 8G FC ports needed.

(1) **Server downlinks:** these are ports on the fabric interconnect that will connect into the UCS chassis' IOM.

- From the **total number of 10GE ports**, determine the number of ports that are dedicated for the server downlinks to the IOM.
- Determine the **distance** (in meters) between the fabric interconnect switches and the UCS IOM.
- Determine the appropriate **cabling and optics** based on the distance including other recommendations provided:
 - **Twinax** (SFP+ Copper): Distance 1, 3, or 5 meters. *Recommended*
 - **MM OM2** (SFP+ SR): Distance: up to 82 meters
 - **MM OM3** (SFP+ SR): distance up to 300 meters
 - **SMF** (SFP+ LR): distance over 300 meters

(2) **LAN uplinks:** these are ports on the fabric interconnect that will connect via Ethernet up to a LAN/Data Center switch (Cisco Nexus 7000 or Cisco Catalyst 6500 series).

- From the **total number of 10GE ports**, determine the number of ports that are dedicated for the LAN uplink to the LAN/Data Center Ethernet switches.
- Determine the **distance** between the fabric interconnect switches and the Ethernet switches.
- Determine the appropriate **cabling and optics** based on the distance including other recommendations provided:
 - **Twinax** (SFP+ Copper): Distance 1, 3, or 5 meters.
 - **MM OM2** (SFP+ SR): Distance: up to 82 meters. *Recommended*
 - **MM OM3** (SFP+ SR): distance up to 300 meters. *Recommended*
 - **SMF** (SFP+ LR): distance over 300 meters

Example: here are the cables and optics needed for the 10GE ports on our Fabric Interconnect switch based on the questions asked.

- **Server Downlinks:** below are the 10GE ports and cables we will use:
 - Five 10GE ports will be dedicated for the server/chassis downlink.
 - **Distance:** within 5 meters
 - **Cabling/Optics:** we will use a SFP+ copper optic with Twinax cables for these ports.
- **LAN uplinks:** below are the 10GE ports and cables we will use for the uplink to the LAN/DC
 - Two 10GE ports will be dedicated for the LAN/DC uplink
 - **Distance:** within 5 meters
 - **Cabling/Optics:** we will use a SFP+ copper optic with Twinax cables for these ports.

Step 16

Fabric Interconnect – Fibre Channel (FC) Ports

FC uplinks: these are ports on the fabric interconnect that will connect via Fibre Channel (FC) up to a SAN switch (e.g. Cisco MDS).

- Determine the **number of ports** that are dedicated for the SAN uplink ports.
- Determine the FC speeds that are required for the uplink:
 - **Speeds:** 1, 2, 4, and 8
- Determine the **distance** between the fabric interconnect switches and the SAN switches.
- Determine the appropriate **cabling and optics** based on the distance including other recommendations provided:
 - **MMF 4G** (SFP 4G SW): speed (1/2/4), distance (70-860 m)
 - **SMF 4G** (SFP 4G LW): speed (1/2/4), distance (10 km)
 - **MMF 8G** (SFP 8G SW): speed (2/4/8), distance (21-520 km)
 - **SMF 8G** (SFP 8G LW): speed (2/4/8), distance (10 km)

Example: here are the cables and optics needed for Fibre Channel ports on our Fabric Interconnect switch based on the questions asked.

- Five 4G FC ports or three 8G FC ports will be used for the SAN uplink ports.
- **FC speed:** 4Gbps FC (or 8Gbps FC)
- **Distance:** within 100 meters
- **Cabling/Optics:** we will use the SFP 4G SW optics with MMF 4Gbps Fibre channel cables for these ports. Or the SFP 8G SW optics with MMF 8Gbps Fibre channel cables for those ports.



Based on the total number of 10GE and FC ports choose the appropriate fabric interconnect switch model:

Cisco UCS 6200 Series Fabric Interconnects *(Large, Data Center)*

Performance	960Gbps – 1.92Tbps Ethernet (1G/10G), FCoE, Fibre Channel	Flexibility	--
Reliability	Power	Management	Cisco UCS Manager
Scalability	48 port model, 96-port model 6248UP : 32-ports (fixed) + 16-ports (EM) 6296UP : 48-ports (fixed) + 16-ports x3 (EM) Support up to 20 chassis' per system	Security	--
Design Aspects	L2, QoS, VM-FEX		
Models	6248UP, 6296UP, Expansion Module (EM)		

Example: Lastly we will choose the best Fabric Interconnect switch model based on the optics that will connect with our UCS chassis', LAN, and SAN environments.

- We will use the 48-port fixed model (Cisco UCS 6248UP) providing additional unified ports in the future.
- **10GE port capacity:** Seven of the fixed ports will be 10GE ports using 10GE SFP+ copper optics and Twinax cables.
- **FC port capacity:** Three of the fixed ports will be FC ports using 8-Gbps Fibre Channel SW SFP optics and FC 8G cables. Or we can use five of the fixed ports using 4-Gbps Fibre Channel SW SFP optics and FC 4G cables.



As we mentioned before, Cisco UCS resources and tools are only available to Advanced UCS partners. However, once the hardware has been selected for the Cisco UCS infrastructure determine the power and cooling requirements, which includes some the following considerations:

- Use the UCS Power Calculator for the:
 - Server Blades
 - Chassis
 - Fabric Interconnect switches
- Determine the power and cooling based on:
 - Idle load or usage
 - 50% load usage
 - Maximum (100%) load usage



~ Solutions ~

Video

Category: Network Solution (Voice)

Prerequisite(s): Voice (Unified Communications) Solution

Complete the steps below for building the design for the network solution.

Step 1	Scalability for Video Solution
Step 1-1	Video Solution Deployment Model

Determine the Video Solution that will be deployed based on the needs of the solution:

- **Immersive Video Deployment:** this is a centralized deployment model that is ideal for very large conference room environments. It presents a real-life in-person video collaboration experience as if all attendees are in the same room. Out of all of the deployment models this is the most advanced and expensive which is ideal for very large environments. In this deployment model, a particular room environment is required to provide the highest quality experience which include the following elements:
 - o Camera angles
 - o Audio speakers
 - o Lighting
 - o Acoustics
 - o Heating and A/C designed to run quietly
 - o Wall painting and carpet color
 - o Matching furniture

These are elements that will enhance the virtual room experience to provide a real-life feel of an actual conference.

Below is an example of this setup or use:



- **Multipurpose Video Deployment:** this is a centralized deployment model that is ideal for medium to large conference room environments. This solution allows one or two video endpoints be present in the room for individual high quality point-to-point conference calls. This deployment model can be used in meeting rooms, boardrooms, auditoriums, and other shared environments. Below are other design points about this deployment model:
 - o This deployment type allows the shortest amount of time to setup into any conference room environment.
 - o Provides multipoint video collaboration with content sharing.
 - o The video endpoints in this deployment are given a unique phone number range to simplify the routing between our endpoints.

Below is an example of this setup or use:



- **Individual Video Deployment:** this is a simple solution where some clients on the voice network will have IP phones with video telephony capabilities or using an executive telepresence system (common for large sized networks). Below is an example of this setup or use:



These would be server endpoints that will handle video client registration, call control, and advanced conferencing capabilities. The video server endpoints will be connected in a server farm (Voice server VLAN).

Based on the Video Solution Deployment model chosen, determine the video server endpoints that are required with the solution:

- **Using Immersive Video Deployment:** there are two required server endpoints for this deployment model: (1) a Cisco Unified CM system is required to provide call control for the video client endpoints. (2) And a Cisco Telepresence Server (CTS) is required for conferencing capabilities with the solution. The communication between the components including the video endpoints involve Session Initiation Protocol (SIP) connections.
- **Using Multipurpose Video Deployment:** there are two required server endpoints for this deployment model: (1) Video Communication Servers (VCS) is needed to provide call control for the video client endpoints. (2) And a Codian Multipoint Control Unit (MCU) is required for conferencing capabilities with the solution. The MCU server component can join multiple video and voice participants into a single conference. Basically you will be able to see all of the people in your conference call on the same screen.
- **Using Individual Video Deployment:** the video server endpoint only requires the Cisco Unified CM phone system if you are using Cisco Video endpoints.

Step 2	Performance for Video Solution

Step 2-1	Determine bandwidth services

Determine the bandwidth service that is required for each component for the solution. Below are typical bandwidth services to choose between:

- Gigabit Ethernet (1Gbps)
- 10-Gigabit Ethernet (10Gbps)
- 40-Gigabit Ethernet (40Gbps)

Step 2-2	Bandwidth Considerations over WAN

When to use: using WAN solution

It's recommended to allow 23% of the WAN bandwidth for video calls. Each video call will typically consume up to 1.5Mbps. This is a general baseline to start with.

For example, let's say there is a site that is connected into a WAN using a 30Mbps WAN connection. Therefore, the site will be able to support up to four video calls (each using 1.5Mbps) over the WAN. This would be a total of ~6Mbps for video calls over the WAN which is roughly 23% of the WAN bandwidth (30Mbps) at the site.

Resource	Video Performance Requirements

QoS is a best practice that should be implemented on the LAN network for all ports according to the QoS design (edge ports, interconnection ports, and Router WAN ports if applicable) running video. Below are additional QoS requirements for video in terms of the amount of delay, loss, and jitter that can be acceptable to allow good video quality across the network.

For Interactive Video:

- **Latency/Delay:** less than 150ms (one-way)
- **Jitter:** 30ms
- **Packet Loss:** less than 1%
- **Bandwidth:** minimum bandwidth of the video bit rate plus add 20%. For example, if the video bit-rate is 384Kb/s then 460Kb/s should be required for priority bandwidth per video stream.

For Streaming Video:

- **Latency/Delay:** 4-5 seconds
- **Jitter:** no significant jitter requirements
- **Packet Loss:** less than 5%

The video solution will be plugged into the LAN solution. The following services are required and recommended for the LAN switches in the topology.

- **Network Time Protocol (NTP):** to provide logging consistency.
- **Domain Name System (DNS):** to provide name resolution
- **Syslog:** to store logging events for troubleshooting purposes
- **Quality of Service (QoS)** *recommended*
- **Multicast:** should be implemented to provide broadcast video delivery efficiency across the network.
- **Medianet (Performance Monitor):** used to help to simply and improve the quality of the video deployment. It can also help to provide better troubleshooting tools when issues arise on the video network. This includes using media traces for viewing the health of the network components along the path. Medianet services should be enabled on all components within the WAN (HQ & remote site) and LAN topologies.

Below are other add-on components and capabilities that can be used with the video solution.

- **Media services:** content recording server where you can record and stream video meetings.

Using Multipurpose Video Deployment:

- **Duo-Video for Sharing Presentations**
- **Far End Camera Control (FECC):** allows remote sites to change their viewing angle during a video call
- **Multisite Conferencing:** allow video endpoints with conference capabilities to add a third device into a video call
- **Multiway conferencing:** allow video endpoints to start ad-hoc multi-point calls using a standard MCU

Below are best practices and consideration for building the video solution design:

- Its recommended to run your video collaboration traffic over an IP network rather than a public ISDN.
- For budgetary considerations, the price for Telepresence is very expensive. Therefore, if the total travel cost (air travel, hotel, car rental, food, misc. taxes and fees) per person exceeds the price of the video endpoint itself then purchasing the Telepresence product makes business sense.
- Interoperability

Step 4	Hardware for Video Solution

Next we need to determine the hardware model that will be used for each component for the solution.

Step 4-1	Video Client Endpoint

These would be the actual video displays that will connect into the LAN access layer. These client endpoints could be IP phone's with video capabilities or a HDTV type unit (e.g. Cisco Telepresence) setup in a conference room.

Based on the Video Solution Deployment model chosen, determine the client endpoints that will be used:

Using Immersive Video Deployment: below are common client endpoints that can be used with this deployment

- Cisco TelePresence IX5000 Series
- Cisco TelePresence TX9000 Series
- Cisco TelePresence TX1300 Series

Using Multipurpose Video Deployment: below are common client endpoints that can be used with this deployment

- Cisco TelePresence System MX Series
- Cisco TelePresence SX Series
- Cisco Telepresence System Integrator C Series

Virtualization (Network)

Category: Network Solution (Data Center)
Prerequisite(s): LAN and/or Data Center Solution

When to use: when you need to virtualize or create isolated network zones within the same physical hardware or across the network. Below are other use-cases for implementing network virtualization:

- When migrating to a new network infrastructure
- When you want to consolidate multiple network topologies (e.g. DMZ) and devices to a single network infrastructure
- For hosting provider type networks where each client is assigned to an isolated virtual domain.

You can virtualize using one or more of the following technology types:

1. Layer 3 (L3VPN)
2. Layer 2 (L2VPN)
3. Hardware

#1	Layer 3 Virtualization

When to use: if you need to create isolated network zones extended across an entire Layer 3 (routing) domain within a LAN and/or WAN.

#1-1	L3VPN: MPLS VPN (RFC2547)

- **When to use:** ideal for large networks and service providers using 12 or more VRF instances on the network.
- **Description:** Using MPLS provides better scalability of VRF instances within a location or across a WAN to other sites. MPLS support is limited to high-end network devices like the Cisco Catalyst 6500 series and Cisco 7200 series.
- **Services Required:** MPLS VPN

#1-2

L3VPN: Easy Virtual Network (EVN)

- **When to use:** used for creating up to 32 virtual networks (per platform) on the LAN/Data Center topology. Recommended over VRF-lite if supported on hardware platform.
- **Description:** Easy Virtual Network (EVN) combines VRF-lite and MPLS VPN into a single virtualization feature that can be implemented on next-generation networks. EVN implementation works by using something called a VNET trunk which automatically creates sub-interfaces for each VRF instance that is added to a EVN enabled device.
- **Services Required:** Easy Virtual Network (EVN)

#1-3

L3VPN: Multi-CE VRF (VRF-lite)

- **When to use:** Used for SMB to Medium/Large networks that require at least 10-12 virtual domains (recommended) to virtualize on the physical network.
- **Description:** VRF-lite is commonly deployed to provide 10-12 separate networks consolidated (or virtualized) on the same hardware. One or two VRFs on smaller-end routers like the Cisco ISR series is okay, but if 5-10 VRFs will be used then higher-end hardware is recommended. This is important because if we are running 5 virtualized networks on the same hardware that means it is working 5 times harder, so we will need enough resources available. If one or two VRFs will be extended across a WAN or VPN (e.g. DMVPN or GET VPN) then using VRF-lite is a good choice unless the VRF numbers are expected to grow. VRF-lite also provides limited multicast support in a VRF domain unless the Cisco Catalyst 6500 series is used on the LAN/Data Center.
- **Services Required:** Multi-CE VRF (VRF-lite)

#1-4

Basic Tunneling

- **When to use:** used for creating a point-to-point unencrypted connection between two networks across a public or private network.
- **Services Required:** IP Tunnels (GRE)

#2	Layer 2 Virtualization

When to use: if you need to create isolated network zones extended across an entire Layer 2 (switching) domain within a LAN or if you want to extend VLAN tags across a Private WAN to other remote sites.

#2-1	Virtual LAN (VLAN)

- **When to use:** used on the LAN or any Ethernet network to create an isolated network in the switching environment.
- **Description:** using VLANs on the LAN or any Ethernet network is used to create an isolated network in the switching environment. If the VLAN is routed then it can communicate with other networks. However, using VLANs is only local to a site and cannot be extended across a WAN unless L2VPNs, OTV, or VXLAN is used.
- **Services Required:** VLAN

#2-2	L2VPN

- **When to use:** need to extend VLANs across a WAN.
- **Description:** provides the capability to extend VLANs across a network whether it is a LAN or WAN. There are many L2VPN protocols which depends on the type of communication needed between sites. L2VPN are often used and deployed by Service Providers.
- **Services Required:** L2VPN

#3	Hardware Virtualization

When to use: if you need to create isolated network zones within the same physical hardware and don't need to extend across a Layer2 or Layer 3 network domain.

- **Security Context:** used by a Firewall (e.g. Cisco ASA 5510 and higher) by partitioning the firewall into a number of virtual firewalls (based on the hardware model and licensing).
- **VDC:** supported on the Cisco Nexus product line. The Nexus 7000 can support up to 4 virtual switches that can be used for routing and switching operations isolated from other VDCs. For high secured environments reserve the default VDC for administration purposes from other non-default VDCs. Furthermore, when using VDC it's recommended to assign different accounts with minimum privileges necessary to accomplish operational tasks needed on the default VDC.

Virtualization (System)

Category: System Solution

Prerequisite(s): LAN and/or Data Center Solution, Server Solution, Desktop Solution

Complete the steps below for building the solution.

First, determine what type of virtualization is needed for the design and focus on that section(s) only:

1. Server Virtualization
2. Desktop Virtualization

1	Server Virtualization

This is a server based solution that is primarily designed and deployed by a system engineering team. The details provided is informational and is listed as a design consideration:

Step 1	Other System Solutions applicable

This is a server based solution that is primarily designed and deployed by a system engineering team. Below are solutions that can be virtualized in the design:

- Server Solution

Step 2	Software

Determine the Server Virtualization software that will be used (or installed) on a physical server:

- VMware
- Microsoft's Hyper-V
- Citrix XenServer

Recommendations: both products provide a good virtualization offering for the physical servers. VMware has been the pioneers that started the idea of virtualizing systems. It has many advantages and capabilities for how virtual machines are built, managed, and moved. Moving a virtual machine from one physical server to another using VMotion, for example, allows this to happen in a production environment. Many may choose Hyper-V since it is free and part of Windows 2008 server (and higher).

Here are additional details and best practices to consider for server virtualization:

- **For Microsoft Hyper-V:** Disable Receive-side Scaling (RSS), TCP-Acceleration (TCPA), TCP offload, and TCP chimney on the host and the virtual machine for increased performance. Especially if an ISA server is being virtualized (note: reported by some system engineers).

Step 3	Hardware Considerations

When building a virtual machine determine the appropriate hardware resources and how it will be networked.

For the virtual server determine the resources needed:

- **Resources:** Disk, CPU, Memory, Throughput

Will the physical server contain multiple virtual machines in different networks using a VLAN tag with the connected switch fabric. If so the following services are required: LAN Switching (VLAN, 802.1Q). These are services that are implemented on all LAN/Data Center switch components where the virtualized servers exist (likely the Server Farm).

2	Desktop Virtualization

This is a server/desktop based solution that is primarily designed and deployed by a system engineering team in conjunction with a desktop team. The details provided is informational and is listed as a design consideration:

Step 1	Other System Solutions applicable

This is a server based solution that is primarily designed and deployed by a system engineering team in conjunction with a desktop team. Below are solutions that can be virtualized in the design:

- Desktop Solution

Step 2	Desktop Virtualization (VDI) Options

Below are the different options for how desktop systems can be virtualized in the design. Determine the best option that would be used:

- **Thin-Client:** solution that involve using thin-clients like the Pano Cube systems that can connect to a virtual desktop for a specific user. The Pano Cube is like a KVM+ access device that can consist of USB, VGA, network, and audio/microphone ports. Using Thin-Clients and virtual machines can allow for robust monitoring and troubleshooting. If a user is experiencing an issue on their computer they can simply logout and the system administrator can log into their session to see what is going on. This virtualize desktop can either be a Microsoft Terminal Server or the popular Citrix. Based on the virtual desktop that is used, it may support Universal PoE providing 60 watts of power provided by the connected switch to the virtual desktop.
- **Virtual Machine:** another type of VDI solution using virtual machine software to provide virtual desktops such as Parallels or VMware Fusion running both Mac and Window systems. This is more common for specific users than a large group of users.

Services Required/Recommended: Universal Power over Ethernet (UPOE)

Voice (Unified Communications)

Category: Network Solution (Voice)
Prerequisite(s): LAN and/or Data Center Solution

Complete the steps below for building the design for the network solution.

Step 1

Scalability for Voice Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

- **Phone System (Call Control):** this is the main component that will act as the backbone of the voice network for all other voice components. The phone system usually connects into the LAN Core, Server Farm, or the Data Center Core/Access.
- **Voice Gateway:** this component connects to a PSTN cloud to provide external calling for the internal voice environment. The voice gateway usually connects into the Core switch.
- **PSTN cloud:** a phone provider network that connects into the voice gateway.
- **Endpoints:** an IP phone that is used by a user and is usually connected to a LAN Access switch enabled for Power over Ethernet (PoE). Computers/laptops are connected to the phone that has an integrated switch port.

Step 1-2

Determine the Phone System Option

Choose the appropriate voice solution based on the business size and the number of remote sites. Below are the options to choose from:

- **Small, SMB**
 - Option A (up to 450 users): Cisco Unified CM Express (CME)
 - Provides: Voice, Messaging (CUE)
 - Option B: (2 to 400 users): Fortinet FortiVoice
 - Provides: Voice, Messaging, Call Center, Auto Attendant
- **Medium**
 - Option A (up to 1000 users): Cisco Unified CM BE 6000 Series [50 sites]
 - Provides: Voice, Messaging (CUC)
 - Option B (up to 2000 users): Fortinet FortiVoice 200 Series
 - Provides: Voice, Messaging, Call Center, Auto Attendant
- **Enterprise/Large**
 - Option A (up to 2000 users): Fortinet FortiVoice 200 Series
 - Provides: Voice, Messaging, Call Center, Auto Attendant
 - Option B (1,000-5,000 users): Cisco Unified CM BE 7000 Series
 - Provides: Voice, Messaging (CUC), Presence, Call Center
 - Option C (1,000-10,000 users): Cisco Unified CM Series
 - Provides: Voice

Choose the appropriate topology of the voice solution based on the following selections:

- **Single-Site/Multi-Site (Decentralized) using Small/SMB Phone System:**
 - **When to Use:** using the CME option within a single location or with multiple sites. Access connections (PRI and/or Analog) used locally at each site for placing and receiving calls.
 - **Details:** In this topology a CME router (with CUE for Voicemail and AA services) exist in all locations supplying unified communications for that local site. Each CME router will connect into the PSTN and the WAN (Private or Public). Each site can place calls among each other through H.323 or SIP trunks configured, but all external calls are routed through the local CME router. This option deals with managing phone systems for each site increasing the overall administration and complexity of the environment.
- **Single-Site/Multi-Site (Centralized) using Medium/Large Phone System:**
 - **When to Use:** using the Cisco Unified CM option within a single location or with multiple sites. In this topology the Cisco Unified CM phone system exist in only one site supplying Voice communications for all sites managed from a central location. This is the most common and recommended topology to use if using Cisco Unified CM or Unified CM Business Edition (BE).
 - **Details:** Each site has a voice gateway router connecting into the PSTN and the Private WAN. Each site can place calls among each other, but all external calls are routed through the local voice gateway. The voice gateway at the remote sites should be enabled for SRST. This will allow the phones at the remote site to register with their local voice gateway if it loses connection with the phone system at the main office or Data Center.
- **Single-Site/Multi-Site (Decentralized) using Medium/Large Phone System:**
 - **When to Use:** using a Cisco Unified CM (cluster) that will trunk with another Cisco Unified CM or voice cluster. This is used when there is an International location with connected other International remote sites, a Backup data center, or another phone system where call routing is required.
 - **Details:** the Cisco Unified CM cluster builds a H.323 interconnection with the remote cluster for call routing. Remote sites will still peer with the Cisco UCM cluster (or the other phone system). Each site has a voice gateway router connecting into the PSTN and the Private WAN. Each site can place calls among each other or through the H.323 interconnection with phones registered on the other cluster. All external phone calls will go through their local voice gateway. The voice gateway at the remote sites should be enabled for SRST that allows the phones at the remote site to register with its local voice gateway if it loses connection with the Cisco Unified CM system.
- **Single-Site/Multi-Site (Centralized) using Small/SMB Phone System:**
 - **When to Use:** using the CME option within a single location or with multiple sites but with no additional access connections (PRI and/or Analog lines) used at the remote site. All calls placed and received are through the main office which will have an access connection (PRI and/or Analog) to the PSTN cloud for external calling.
 - **Details:** in this topology a CME router (with CUE for voicemail and AA services) is only located at the main office with a small group of IP phones at a few remote sites communicating back to the main office through a Private WAN (recommended) or Public WAN (using the Internet Edge with VPN services) to connect to the phone system. Keep in mind that this topology option is not recommended due to the best effort Internet and VPN overhead which can result in delay or packet loss affecting voice quality.

Determine the phone system topology that will be used based on the phone system and the number of users:

1. Using Cisco Unified CME or any Small/SMB Phone System: up to 400 users.
2. Using Cisco Unified CM Series: up to 500 users
3. Using Cisco Unified CM Series: 500 to 1,000 users
4. Using Cisco Unified CM Series: 1,000 to 2,500 users
5. Using Cisco Unified CM Series: 2,500 to 5,000 users
6. Using Cisco Unified CM Series: 5,000 to 10,000 users

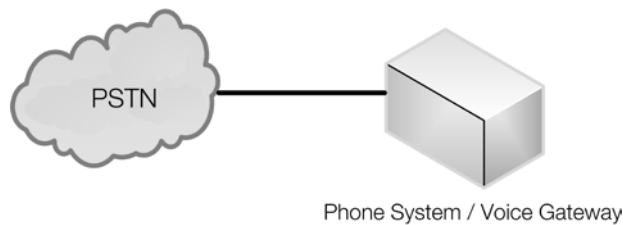
#1

Using Cisco Unified CME or any Small/SMB Phone System: up to 400 Users

When to use: up to 400-450 users.

In this topology, a single voice appliance, aimed for small and SMB networks, is used to provide many of the following capabilities:

- Voice
- Voice Messaging
- Auto Attendant
- Call Center, Queuing
- Voice Gateway (FXO, PRI, SIP)

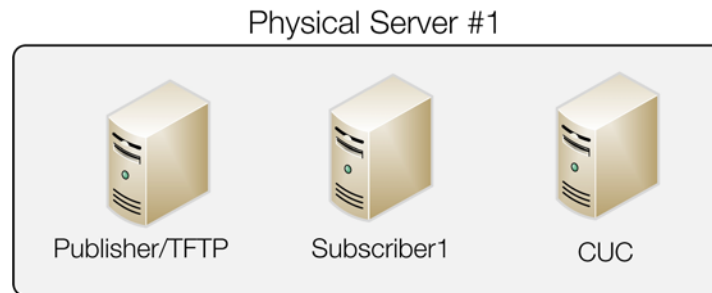


Below are some of the Small/SMB voice appliances that can be used:

- Fortinet: FortiVoice
- Shortel
- Barracuda: CudaTel
- 3CX
- Allworx

When to use: up to 500 users (and up to 50 Remote Sites)

In this topology, a single physical server is used with multiple virtual machine instances based on the following functions:



Physical Server #1:

- Virtual Machine #1: Cisco Unified CM (CUCM) - Publisher/TFTP1
- Virtual Machine #2: Cisco Unified CM (CUCM) - Subscriber1
- Virtual Machine #3: Cisco Unity Connection (CUC)

Cisco Unified Groups:

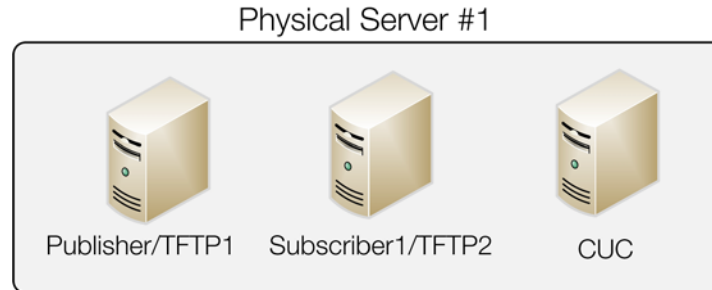
- Group A: (1) Subscriber1, (2) Publisher

Physical Server Hardware Details:

- Cisco Unified CM - Business Edition 6000
- Cisco UCS C220 M3 (1RU)
- Hardware for each CUCM Virtual Machine: vCPU (2), CPU (800 MHz), RAM (4GB), HD (80GB)
- Hardware for each CUC Virtual Machine: vCPU (1-2), CPU (2.13 or 5.06 GHz), RAM (4-6GB), HD (160-200GB)

When to use: 500 to 1000 users (and/or with 50 to 90 Remote Sites)

In this topology, a single physical server is used with multiple virtual machine instances based on the following functions:



Physical Server #1:

- Virtual Machine #1: Cisco Unified CM (CUCM) - Publisher/TFTP1
- Virtual Machine #2: Cisco Unified CM (CUCM) - Subscriber1/TFTP2
- Virtual Machine #3: Cisco Unity Connection (CUC)

Cisco Unified Groups:

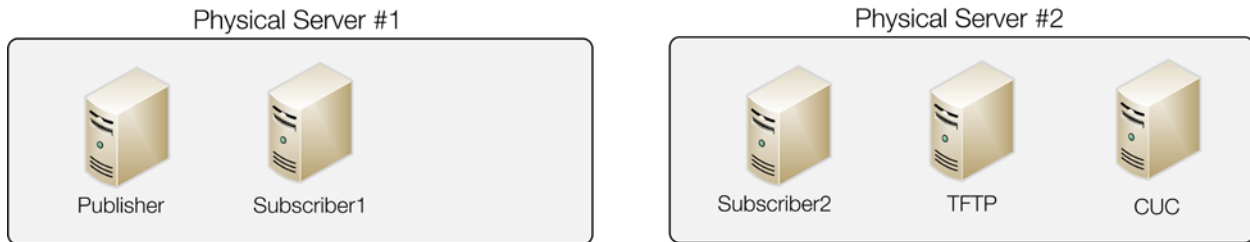
- Group A: (1) Subscriber1, (2) Publisher

Physical Server Hardware Details:

- Cisco UCS C220 M3 (1RU)
- Hardware for each CUCM Virtual Machine: vCPU (1), CPU (800 MHz), RAM (4GB), HD (80GB)
- Hardware for each CUC Virtual Machine: vCPU (1-2), CPU (2.13 or 5.06 GHz), RAM (4-6GB), HD (160-200GB)

When to use: 1000 to 2500 users (and with 90 to 500 Remote Sites)

In this topology, multiple physical servers are used with five virtual machine instances running based on the following functions:



Physical Server #1:

- Virtual Machine #1: Cisco Unified CM (CUCM) – Publisher
- Virtual Machine #2: Cisco Unified CM (CUCM) - Subscriber1

Physical Server #2:

- Virtual Machine #3: Cisco Unified CM (CUCM) - Subscriber2
- Virtual Machine #4: Cisco Unified CM (CUCM) – TFTP
- Virtual Machine #5: Cisco Unity Connection (CUC)

Cisco Unified Groups:

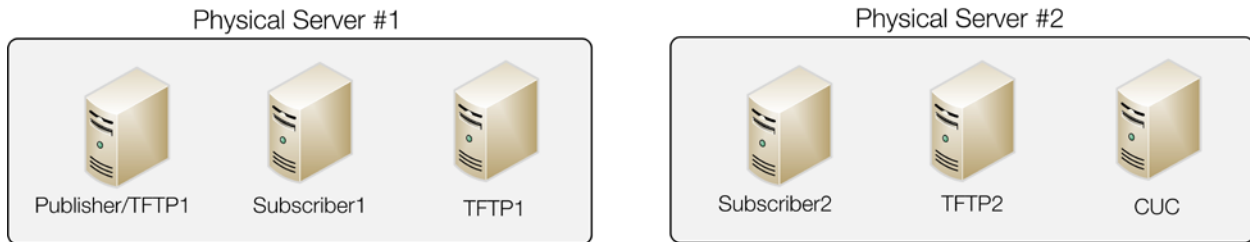
- Group A: (1) Subscriber1, (2) Subscriber2
- Group B: (1) Subscriber2, (2) Subscriber1

Physical Server Hardware Details:

- Cisco UCS C240 M3 (2RU)
- Hardware for each CUCM Virtual Machine: vCPU (1), CPU (800 MHz), RAM (4GB), HD (80GB)
- Hardware for each CUC Virtual Machine: vCPU (2), CPU (5.06 GHz), RAM (6GB), HD (200GB)

When to use: 2500 to 5000 users (and with up to 500 Remote Sites)

In this topology, multiple physical servers are used with six virtual machine instances running based on the following functions:



Physical Server #1:

- Virtual Machine #1: Cisco Unified CM (CUCM) – Publisher
- Virtual Machine #2: Cisco Unified CM (CUCM) - Subscriber1
- Virtual Machine #3: Cisco Unified CM (CUCM) - TFTP1

Physical Server #2:

- Virtual Machine #4: Cisco Unified CM (CUCM) - Subscriber2
- Virtual Machine #5: Cisco Unified CM (CUCM) – TFTP2
- Virtual Machine #6: Cisco Unity Connection (CUC)

Cisco Unified Groups:

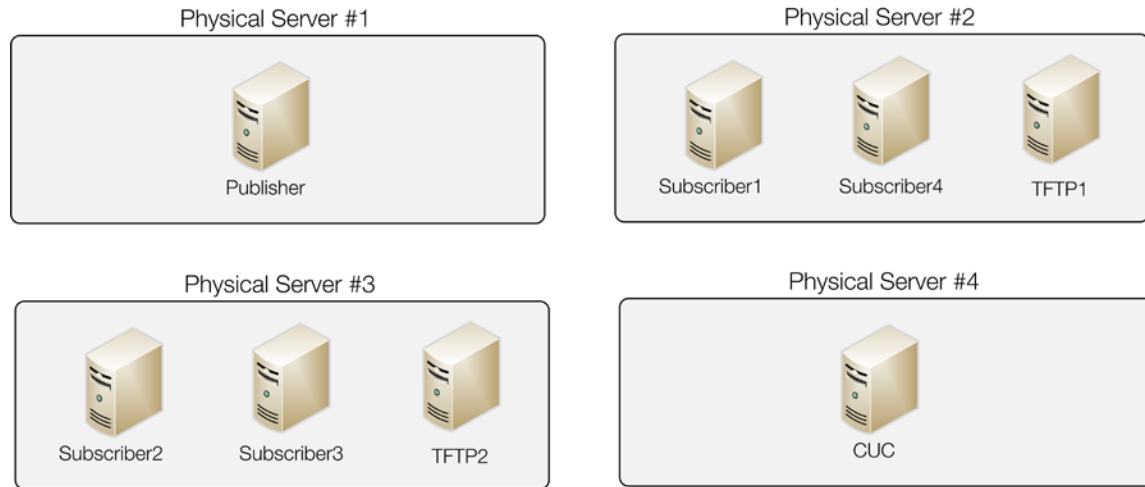
- Group A: (1) Subscriber1, (2) Subscriber2
- Group B: (1) Subscriber2, (2) Subscriber1

Physical Server Hardware Details:

- Cisco UCS C240 M3 (2RU)
- Hardware for each CUCM Virtual Machine: vCPU (2), CPU (3600 MHz), RAM (6GB), HD (80GBx2)
- Hardware for each CUC Virtual Machine: vCPU (2), CPU (5.06 GHz), RAM (6GB), HD (200GB)

When to use: 2500 to 5000 users (and with up to 500 Remote Sites)

In this topology, multiple physical servers are used with eight virtual machine instances running based on the following functions:



Physical Server #1:

- Virtual Machine #1: Cisco Unified CM (CUCM) – Publisher

Physical Server #2:

- Virtual Machine #2: Cisco Unified CM (CUCM) - Subscriber1
- Virtual Machine #3: Cisco Unified CM (CUCM) - Subscriber4
- Virtual Machine #4: Cisco Unified CM (CUCM) - TFTP1

Physical Server #3:

- Virtual Machine #5: Cisco Unified CM (CUCM) - Subscriber2
- Virtual Machine #6: Cisco Unified CM (CUCM) - Subscriber3
- Virtual Machine #7: Cisco Unified CM (CUCM) - TFTP2

Physical Server #4:

- Virtual Machine #8: Cisco Unity Connection (CUC)

Cisco Unified Groups:

- Group A: (1) Subscriber1 (Primary), (2) Subscriber2 (Backup)
- Group B: (1) Subscriber3 (Primary), (2) Subscriber4 (Backup)

Physical Server Hardware Details:

- Cisco UCS C240 M3 (2RU)
- Hardware for each CUCM Virtual Machine: vCPU (2), CPU (3600 MHz), RAM (6GB), HD (80GBx2)
- Hardware for each CUC Virtual Machine: vCPU (4), CPU (10.12 GHz), RAM (6GB), HD (300GBx2)

Step 2	Reliability for Voice Solution

Below are the redundancy options when using Voice (Unified Communications) on the network.

Step 2-1	Cluster

The Cisco Unified CM solution can be deployed in a cluster to provide reliability and scalability. Below are the recommended options for deploying a Cisco Unified CM cluster.

- **Publisher** (Required): A Publisher server is setup first and is where all of the configuration occurs. Furthermore, it's recommended to setup the Publisher to be the secondary voice server if the primary voice server is down.
- **Subscriber**: You can have multiple subscriber servers. These are read-only servers where its configuration is pulled from the Publisher. This should be the primary voice server that all IP phones and gateway register with for voice services.

Other Recommendations: If you are using a Cisco Unified CM cluster that will support more than 1,000 users then multiple phone system servers are used. Therefore, its recommended to plug each voice server to different switches within the Data Center topology to provide for high availability. It's also recommended to use Redundant Array of Independent Disks (RAID) and dual power supplies with the phone system components.

Step 2-2	PRI and PSTN

It's recommended to use a second PRI or analog lines if the primary PSTN circuit should fail. Using different PSTN providers can provide higher reliability, but there may be challenges for using the same DID block between two different PSTN providers.

This redundancy option is common for most business size networks with moderate voice calling requirements. Redundant PRIs can also be helpful if high call volume is expected.

Step 2-3	SRST (SCCP, SIP)

If the phone system fails (with no secondary phone system available) or if the WAN connection fails for a remote site the IP Phones can use SRST fallback. In SRST fallback mode, the phones will register with the local voice gateway to place and receive calls until the phone system is available again. Below are some additional considerations and notes to keep in mind when using SRST:

- PSTN using PRI and/or Analog line can be used on a SRST-enabled voice gateway router.
- Voice Gateway router must support SRST
- SRST does not support video
- H.323 patterns are used for call routing on the voice gateway router

This redundancy option is common and recommended for all branch offices using a WAN to communicate back to the phone system cluster. This can also be used for a HQ office if the number of IP Phones registering with the voice gateway isn't high (matching what is supported on the router) and doesn't have a voice cluster deployed.

Step 3

Performance for Voice Solution

Follow the steps below to determine the bandwidth services for the solution.

Step 3-1

Determine bandwidth services

Determine the bandwidth service that is required for each component for the solution. Below are typical bandwidth services to choose between:

- Fast Ethernet (100Mbps)
- Gigabit Ethernet (1Gbps)

Recommendations: use GE if supported and available on the LAN and/or Data Center network.

Step 3-2

Voice Requirements

QoS is a best practice that should be implemented on the LAN for all ports according to the QoS design (edge ports, interconnection ports, and Router WAN ports if applicable) running voice. Below are additional QoS requirements for voice in terms of the amount of delay, loss, and jitter that can be accepted to allow good call quality across the network.

- **Latency/Delay:** less than 150ms (one-way)
- **Jitter:** 30ms
- **Packet Loss:** less than 1%
- **Bandwidth:** at least 17-106Kb/s (or 320kb/s) should be guaranteed bandwidth for Voice RTP and 150b/s for Voice Control. Recommended that Voice RTP traffic use LLQ at 33% of the bandwidth connection. This is shown with the different QoS policies under the QoS service section in the design cookbook.

Partitions and CSS pertains to Cisco Unified CM/Unified CM BE deployments and provide a level of security where voice endpoints (e.g. IP Phones) can only place calls with devices (or directory numbers) within their group called a Calling Search Space (CSS). Each directory number (e.g. extension) or route pattern is associated to a partition. These partitions are assigned to a CSS group. With Cisco Unified CM Express (aka Cisco CallManager Express) uses Class of Restriction (CoR) lists to provide calling restrictions.

Below are the recommended Partitions (or CoR tag) that should be created on the voice system:

- Phones or Phones based on Groups (e.g. RHG-P-PHONES)
- Local Calling (e.g. RHG-P-LOCAL)
- Emergency (911) Calling
- Long Distance (LD) Calling
- International Calling
- Total Free Calling
- 411, 611 Calling

Next, create a CSS group that will associate a certain set of partitions based on what type of calls a user can place. The design for CSS can be done in many ways depending on the requirements and what each user on the voice network can do.

Method 1: This is the most simple and easiest to manage. This is used if the voice network is small, if there is a single location, and if all users share the same type of policy for whom they can call.

- Internal CSS

Method 2: This method introduces a medal class of Gold, Silver, and Bronze based on the following breakdown:

- Gold CSS: Allows calls anywhere.
- Silver CSS: Allows only Local, 911, LD, and Internal calling. Ideal for most phones and employees.
- Bronze CSS: Allows only Local, 911, and Internal calling. Ideal for phones in the lobby or public space areas.

Method 3: This method is the same as Method 2, but uses more common names that are based on groups.

- Employee CSS: Allows only Local, 911, LD, and Internal calling. Ideal for most phones and employees.
- Executive CSS: Allows calling to anywhere.
- Support CSS: Allows calling to anywhere.

Method 4: create the following CSS groups based on the partitions assigned to them.

- **CSS_Base:** 911 partitions, All Phones (On-NET)
- **CSS_LocalPSTN:** Local
- **CSS_NationalPSTN:** Local, National
- **CSS_InternationalPSTN:** Local, National, International

Next, all phone endpoints should be assigned to the "CSS_Base" CSS group. Then you can assign the appropriate line/extension with an additional CSS group (e.g. CSS_LocalPSTN) needed for providing additional call restriction.

Phone Proxy: requires the Cisco ASA firewall appliance allowing a remote IP Phone to connect into the Cisco Unified CM cluster without using a VPN router/firewall. The phone will create a secure tunnel with the Cisco ASA where the firewall will then proxy requests between the phone and the voice cluster on the internal network.

Step 5	Network Management for Voice Solution

Below are Network Management services that can be used with the solution

- **Call Recording and Monitoring:** provide the ability to monitor and record phone conversations.
- **Call Detailed Records (CDR):** provide reports of calls placed and received by phones connected to the voice environment.
- **Real-Time Monitoring Tool (RTMT):** an application which connects to the phone system to provide system resource reports (CPU, Memory), logs, and active call activity.
- **Services Required:** NTP, SNMP (for Voice Gateway)

Step 6	Flexibility for Voice Solution

Step 6-1	Integration with other solutions

Below are other solutions that can be deployed with the voice solution:

- Messaging
- Conferencing
- Customer Care
- Presence
- Video

Step 6-2	Integration with WAN Solution

The following should be considered and configured if VoIP traffic will be used across a WAN.

- **Regions:** G.711 (for internal calling), G.729 (calling between sites).
- End-to-End QoS configuration should be configured.
- The remote site requires a Voice Gateway router that can be connected into the WAN and the PSTN cloud.
- The Voice gateway can be setup to use SRST to have all the phones fallback to their local router if the WAN is not available.
- Users at the remote site can place/receive all calls through a PRI or analog line (using FXO cards) through their local voice gateway. If the PRI fails, users can use the analog lines on the Voice Gateway for placing calls until the PRI is restored.
- Determine if the remote site is considered as a:
 - **Standard remote site:** using a single voice gateway, PRI, and maybe FXO lines for backup.
 - **Critical remote site:** the voice gateway router and PRI connections are redundant.
- If an International site is included in the topology, setup a separate Unified CM cluster at the international location and use H.323 to build an inter-cluster trunk between the environments for call routing.
- **AAR:** if the call volume increases for a remote site on the WAN (bandwidth number configured) additional calls can be automatically re-routed across the PSTN instead.

Step 7

Design Aspects for Voice Solution

Step 7-1

Voice Connections

Determine the number of concurrent voice calls expected through the voice gateway. Based on that number determine the number of voice circuits (from the list below) that should be used on the voice gateway:

- **PRI:** support up to 23 concurrent calls (placed or received). Common for high call volume such as call centers and SMB/medium/large-sized networks.
- **Analog:** support up to 1 concurrent call (placed or received) per line. Common for low call volume and smaller networks.

Example: if our environment is expected to support up to 50 concurrent voice calls. Then we are looking at up to three T1 PRI connections from the PSTN.

Step 7-2

Media Resources

Below are the media resource services that may be used with the voice solution:

- **Music On-Hold (MoH):** MoH at the main office should be streamed using multicast from the phone system. MoH at the branch offices should be streamed directly from its local voice gateway and not across the WAN consuming network resources.
- **Conferencing:** provides the ability to share a single call with multiple participants. Conferencing can either be hardware based (from the voice gateway) or software based (from the phone system).
- **Transcoding:** provides the ability to translate one codec (like G.729) into another codec (like G.711). If using the Software conferencing solution among the remote sites transcoding can be enabled on the WAN Aggregation router (or Voice Gateway) where a conference call from a remote site to the main office would use G.729. At the main office, the router would transcode that stream to use G.711 since the software conferencing solution only supports G.711.

Step 7-3

Basic Conferencing (Hardware or Software)

When to use: expected to use conferencing services within the voice environment.

Determine the number of conference bridges (and people per conference bridge) that will be used in the voice network?

Next, determine if the conferencing services will be hardware or software based::

- **Hardware:** Conferencing used on a Voice Gateway supporting a mixture of different codecs (G.711, G.729). For branch offices using a voice gateway, its recommended to use local conference bridges (Hardware) to avoid unnecessary voice traffic over the WAN.
- **Software:** Conferencing used on the phone system directly (Cisco Unified CM server) supporting only the G.711 codec. Below are the different software conferencing options that can be used:

- o **MeetMe:** Basic conferencing feature where a user can build a conference bridge and have callers call directly into the conference. No password/passcode is required to join into a MeetMe conference. Supports a maximum of 8 participants per conference bridge, which can be changed with caution.
- o **Ad Hoc:** Basic conferencing feature where a user can build a conference directly on their phone and join callers into the same active call.

If advanced conferencing needs are required reference the Conferencing Solution for completing the design.

Step 7-4

DSP Resources for Voice Gateway

All voice gateway routers requires to have packet voice digital signal processor (DSP) modules installed in order to perform any voice, transcoding, or conferencing services.

The number of DSP and PVDMS needed is based on the total number of voice sessions expected. These voice sessions can be (1) voice calls, (2) transcoding, and (3) conferencing. This is info that was determined from a previous step.

The number of PVDMS resources needed will determine the total voice sessions it can support. You can also use multiple PVDMS inside of the voice gateway based on what hardware you use.

For example a "PVDMS3-64" can support up to 64 voice sessions. This means, that PVDMS can accommodate up to one voice T1 (24 voice sessions) and five 8-party conference sessions (40 voice sessions).

Recommendations: Use the DSP Calculator to determine the amount of DSP resources needed.

Step 7-5

Signal Protocol between Phone System and Voice Gateway

If you are using the Cisco Unified CM or Unified CM BE products determine the communication protocol that will be used between the phone system (Cisco Unified CM) and the Voice Gateway (e.g. Cisco ISR 2900).

- **MGCP:** Used with Cisco Voice Gateways, PRI (for all 24 channels), and Analog lines.
- **H.323:** Used between different vendor Voice gateways for call routing. Used when PRI is utilizing fractional channels (not all 24 channels) or a full PRI. Also used for call routing between phone system clusters and gatekeepers.
- **SIP:** alternative and recommended signal protocol over H.323 used for call routing between the phone system and the voice gateway. Typically used when connecting to VoIP providers for external calling.

Recommendations: Use SIP between the voice gateway and the voice cluster for increased stability and support for advanced services like FoIP (Fax over IP) including SRST (Remote Site Fallback mode).

Determine the codec used for calls within a location or between other locations on the WAN. As a best practice configure the following:

- **Calling within a site:** For calls within a site, the region should be configured for the G.722 or G.711 codec running at 80 kbps (per call). There are no limits to the number of calls allowed within a site.
- **Calling between other sites:** For calls between the sites, the region should be configured for the G.729 codec running at 24 kbps. (per call). For sites with 500 users, the default setting is two inter-site calls (48 kbps); for sites with 10,000 users, the default is eight inter-site calls (192 kbps).

Determine the appropriate extension schema to use for the voice network.

- **3-Digit Extension:** Ideal for Small and SMB networks (10-500 users). For example, extension 301 could be a user's extension at a single location.
- **4-Digit Extension:** Ideal for SMB and Medium networks (300-999 users). For example, extension 5100 could be a user's extension at a single location. A site ID could be used with this schema.
- **6-Digit Extension:** for networks with 90 sites or less. Ideal for Medium to Large networks (1000+)
 - Extension Schema: SS + XXXX
 - SS = Two-digit site code to accommodate up to 90 sites (10-99 sites).
 - XXXX = Four digits for the site extension
 - Example: 106778. Site code would be 10 and the extension at the site would be 6778.
- **7-Digit Extension:** for networks with greater than 90 sites. Ideal for Large networks (1000+)
 - Extension Schema: SSS + XXXX
 - SSS = Three-digit site code to accommodate up to 900 sites (100 to 999 sites)
 - XXXX = Four digits for the site extension
 - Example: 1016778. Site code would be 101 and the extension at the site would be 6778.

Step 7-8**End Users (Integration with Active Directory)**

For end user authentication integrate the Directory Services (e.g. Active Directory, Open Directory) environment using LDAP with the phone system (Cisco Unified CM and Unified CM BE). This will allow users to access the “User Options” page using their AD credentials to make changes to their IP Phone and directory number.

This is a best practice for maintaining a single centralized location for all user authentication on the network.

Step 7-9**Voice and Data VLAN**

As a best practice configure a Voice VLAN for all voice traffic (e.g. IP Phones, Voice Gateway) separate from the production data network configured in one (or more) Data VLANs.

Cisco Discovery Protocol (CDP) is required as it provides the Cisco IP phone with configuration details such as the Voice VLAN it should use, power requirements, and the ability to prioritize traffic from the IP phone.

Services Required: VLAN, Trunking (802.1Q), CDP

Step 7-10**DHCP**

DHCP is required in order for the IP Phones to know how to connect to the phone system (e.g. Cisco Unified CM). DHCP can be configured either on the network or on a DHCP server (recommended). Make sure that the following is configured with the DHCP scope:

- **“Option 150”** pointing to the IP address of the TFTP server (in most cases the phone system like Cisco Unified CM) which is responsible for the phones to download their configuration and the latest firmware.

Determine the necessary details for the voice endpoints (the IP phones) that will be used on the voice network.

#1

Number of IP Phones and Type of Phones

First, determine the following details:

- Number of IP Phones dedicated to a user?
 - o Employee Users
 - o Executive Users
 - o Receptionist Users
- Number of Conference room phones?
- Number of phones for the Lobby, Break Room, Kitchen, etc?
- Number of fax machines (and other analog devices)?

#2

Phone Firmware

Next, determine the protocol (or firmware) that the IP Phones should use:

- **SCCP** (recommended): when using a Cisco phone endpoint connecting to a Cisco based phone system.
- **SIP**: when the phone endpoint will connect to a different phone system vendor (industry standard).
- **MGCP**: uncommon firmware option for phone endpoints.

#3

Phone Hardware Requirements

Determine the necessary IP Phone hardware requirements based on the following:

- Line Appearances (for extensions and speed dials)
- Display (Color, Gray Scale, Touchscreen)
- Speakerphone support
- Intergraded Switch port
- Protocol support

#4

Phone models based on Phone Type

Below are typical Cisco IP Phone model choices to choose from based on what has been gathered.

- **Employee**: Cisco 7941G or 6941
- **Executive**: Cisco 7961G, 7965G, 7975G
- **Receptionist**: Cisco 7931G or 6961
- **Conference Room**: Cisco 7937G
- **Lobby/Break Room/Kitchen**: Cisco 7911G, 6921, 6901
- **Teleworker**: Cisco IP Communicator (CIPC)
- **Mobility**: 7925

Power over Ethernet (PoE) is a required component in the LAN, but understanding the power draw requirements is important. It is needed for selecting the right LAN switches to support the PoE class and power draw supported. Below are the PoE classes for reference:

PoE Classes

- Class 2 (7W)
- Class 3 (15.4W)

Class 2 PoE Phones

- Cisco 7906/7911 = 5W
- Cisco 7912/7940/7960 = 6.3W
- Cisco 7941/7961 = 6.3W

Class 3 PoE Phones

- Cisco 7970G = 10.25W
- Cisco 7937G Conference Phone = 10.5W
- Cisco 7965G/7975G = 12W
- Cisco 7971G-GE = 14.9W

For outbound calling through the PSTN define the route patterns that will be used based on the recommended dial plan and the country. These route patterns would be assigned to their appropriate route partition that was defined earlier under the Voice security design section.

Dial Plan: North American Numbering Plan (NANP)

Below are the recommended patterns to add to the phone system for a NANP Dial Plan:

- **Emergency Dialing:** 911, 9.911
- **Local Dialing:** 9.[2-9]XXXXXX
- **National (Long Distance) Dialing:** 9.1[2-9]XX[2-9]XXXXXX
- **International Dialing:** 9.011!, 9.011#
- **Toll Free Dialing:** 9.1888[2-9]XX XXXX, 9.1877[2-9]XX XXXX, 9.1866[2-9]XX XXXX

Note: The Access Code used in these patterns are "9"

International Dialing: two international patterns should be configured: (1) 9.011! = for variable-length dialed digits and (2) 9.011# = to allow users to bypass the inter-digit timeout period.

Emergency Dialing: the route patterns should be created with Urgent Priority to prevent inter-digit timeout delays.

Determine the following for inbound calls from the PSTN into the voice network.

- **Digits to Forward:** The number of digits you want the PSTN provider to pass down. Most PSTN providers will pass the last four digits of the DID number to the client's voice gateway. For example, if someone is calling DID 925-230-2203 then the PSTN provider will only forward "2203" to the voice gateway.
- **Location:** Determine if incoming calls should be routed at the local site or through another site (e.g. HQ). For most deployments incoming calls arrive at the site's local voice gateway.

The following are common voice features that can be used with the solution:

- **Basic Features:** Placing/Receiving Calls, Call Forward, Transfer, Call Park, Speed Dial, Redial
- **Call Pickup:** provides the ability to pick-up a ringing call from your phone within the same group.
- **Extension Mobility:** dynamically configures a phone according to an authenticated user's device profile. When a user logs into an IP phone with their username and PIN, their device profile will be uploaded to the IP phone.
- **Single Number Reach (Mobile Connect):** provides the ability that a ringing extension will ring other phone devices such as mobile phones.
- **Device Mobility:** an enhanced voice feature that allows a user's IP phone to roam between sites. This feature works when the Cisco Unified CM phone system uses the IP Phone's IP subnet to determine the physical location for where the phone is located.

Paging allows callers to send one-way broadcast messages across the voice network. Paging options will vary depending on the voice product that will be deployed.

- **Cisco Unified CM and Unified CM-BE Solutions:** Requires a third-party Paging system (e.g. Bogen TAMB is the most common Paging system used) which connects into a stereo amp and to an FXO port on the voice gateway router. The phone system uses a H.323 connection to the voice gateway for the Paging. When a user wants to page they can simple dial "#6" (or any number), which would translate to an extension. That extension would be configured as a route pattern, which is routed to the H.323 gateway (the voice gateway). The voice gateway will have the FXO port configured with that extension used for the paging system.
- **Cisco Unified CME Solutions:** Paging capabilities are built-in with the solution, but uses the IP phones as the speaker system. Paging is configured and associated to the IP phones that will hear that broadcast message. A third-party paging system like Bogen TAMB can also be used with this solution and configured similar to the UCM & UCM/BE solution.

Faxing allows users to send and receive digital documents through the voice network. Below are some of the faxing options that can be used.

- **Standard Fax Server:** If using Cisco Unified CM (or UCM/BE) it can support many third-party fax machines such as the Castelle Fax Server.
- **Standalone Analog Fax devices:** A standalone-analog fax machine would be plugged into an FXS port for sending and receiving fax messages. This fax option is the most common for small and SMB networks plus it is the most simplest to deploy out of the three.
- **T.37 and T.38 Faxing (FoIP):** Used where fax messages are sent and received over IP (Fax over IP or FoIP). The fax messages are converted to a TIFF format then emailed to the intended fax user. Cisco UC520 & CME offer T.37 fax support where a new fax would go into the CME router then converts the fax to a TIFF image. This TIFF image is then emailed to the user with the message attached. Cisco Fax Server (CFS) is an example of a FoIP solution. Cisco Unity Connection only supports the CFS where Cisco Unity can support a greater range of FoIP products.

When to use: using Cisco Unified CM for the Phone System component.

Below are the recommended services that should be enabled for the **Cisco Unified CM component running as the Publisher without TFTP:**

- **CM Services:** Cisco CallManager, Cisco Unified Mobile Voice Access Service, Cisco IP Voice Media Streaming App, Cisco CTIManager, Cisco Extension Mobility, Cisco Extended Functions, Cisco Intercluster Lookup Service, Cisco Location Bandwidth Manager
- **CTI Services:** Cisco IP Manager Assistant, Cisco WebDialer Web Service
- **CDR Services:** Cisco SOAP - CDRonDemand Service, Cisco CAR Web Services
- **Database and Admin Services:** Platform Administrative Web Service, Cisco Bulk Provisioning Service, Cisco AXL Web Service, Cisco UXL Web Service
- **Performance and Monitoring Services:** Cisco Serviceability Reporter, Cisco CallManager SNMP Service
- **Security Services:** Cisco CTL Provider, Cisco Certificate Authority Proxy Function
- **Directory Services:** Cisco DirSync

Below are the recommended services that should be enabled for the **Cisco Unified CM component running as a Subscriber without TFTP:**

- **CM Services:** Cisco CallManager, Cisco IP Voice Media Streaming App, Cisco CTIManager, Cisco Extension Mobility, Cisco Extended Functions, Cisco Intercluster Lookup Service, Cisco Location Bandwidth Manager

Below are the recommended services that should be enabled for the **Cisco Unified CM component running as a standalone TFTP server:**

- **CM Services:** Cisco IP Voice Media Streaming App, Cisco CTIManager, Cisco Extension Mobility, Cisco Extended Functions, Cisco Intercluster Lookup Service, Cisco Location Bandwidth Manager, Cisco TFTP

Below are the recommended services that should be enabled for the **Cisco Unified CM component running as a Publisher with TFTP**:

- **CM Services:** Cisco CallManager, Cisco Unified Mobile Voice Access Service, Cisco IP Voice Media Streaming App, Cisco CTIManager, Cisco Extension Mobility, Cisco Extended Functions, Cisco Intercluster Lookup Service, Cisco Location Bandwidth Manager, Cisco TFTP
- **CTI Services:** Cisco IP Manager Assistant, Cisco WebDialer Web Service
- **CDR Services:** Cisco SOAP - CDRonDemand Service, Cisco CAR Web Services
- **Database and Admin Services:** Platform Administrative Web Service, Cisco Bulk Provisioning Service, Cisco AXL Web Service, Cisco UXL Web Service
- **Performance and Monitoring Services:** Cisco Serviceability Reporter, Cisco CallManager SNMP Service
- **Security Services:** Cisco CTL Provider, Cisco Certificate Authority Proxy Function
- **Directory Services:** Cisco DirSync

Step 7-18

General Best Practices

Below are other best practices to consider for the Voice design.

- **Change host name to IP address:** its recommended to change the Cisco Unified CM Publisher/Subscriber/TFTP server host name to its IP address, which removes the dependency of DNS for the phones.

Step 7-19

Subnets

Determine the IP subnets that will be used for the voice network.

- **Phones:** all phones on the voice network should exist in their own private network isolated from the data network. If there is a large collection of IP Phones then multiple voice subnets is recommended.
- **Servers:** It's also recommended to deploy a separate voice subnet for the Unified Communication servers, but they can also exist in the same server VLAN that may have other systems such as file servers or domain controllers.
- **Other:** other subnets created based on any unique requirement or preference.

Step 7-20

Services

The voice solution will be plugged into the LAN solution. The following services are required and recommended for the LAN switches in the topology.

- Virtual LAN (VLAN) *required*
- Trunking (802.1Q) *required*
- Network Time Protocol (NTP) *required*
- Quality of Service (QoS) *recommended*
- Multicast *recommended*
- Cisco Discovery Protocol (CDP) *required*
- Medianet *recommended*

VLANs and 802.1Q Trunking is used between all switches and the IP Phone to provide Data and Voice VLAN assignment. QoS should be implemented on all edge ports (on the Access switch) and all interconnection ports plus the Router WAN ports. Recommended to use AutoQoS for all L2/L3 switches. Multicast (and IGMP snooping) should be enabled on all switches with Multicast routing enabled on the L3 Core switch for Music on Hold (MoH) services.

Using Medianet technologies within the network will help to simply and improve the quality of the voice deployment. If Cisco Medianet will be implemented on the LAN switches, the following QoS settings are recommended for providing optimal voice and video quality. These QoS settings are default for Voice/Video endpoints on a Cisco network:

- Voice (Signaling): QoS CS3
- Voice (Payload): QoS EF
- Video: QoS AF41

Step 7-21

Hardware Features (Required)

The following hardware features are also required:

- Power over Ethernet (PoE), PoE+, or Cisco Universal PoE (UPOE) *required*

PoE is recommended to provide power to the IP Phones from its connected access switch.

Resources

#1

Voice Network Ports

- **SIP:** 5060 (TCP/UDP),
- **Secure SIP:** 5061 (TCP/UDP)
- **SCCP:** 2000 (TCP)
- **Secure SCCP:** 2443 (TCP),
- **Standard RTP ports:** 16384-32767 (UDP)

#2

QoS for Voice

- Voice (Signaling): QoS CS3
- Voice (Payload): QoS EF
- Video: QoS AF41

Step 8

Hardware for Voice Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Table Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1

Hardware Table Options

Select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

a

Phone System (Call Control)

Cisco Unified Communications Manager *(Large)*

Performance	--	Flexibility	--
Reliability	Cluster	Management	--
Scalability	Up to 40,000+ users	Security	--
Design Aspects	Phone System (Call Control), Video		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance, Licensing (UCL, UWL)		

Cisco Unified Communications Manager – Business Edition *(SMB, Medium, Large)*

Performance	--	Flexibility	Messaging (CUC), Contact Center (CCX) except on BE 6000S, Presence (IM&P)
Reliability	--	Management	--
Scalability	BE 6000S: up to 150 users BE 6000H/M: up to 1000 users, 50 sites BE 7000: 1000-5000 users	Security	--
Design Aspects	Phone System (Call Control), Voicemail, Unified Messaging (Exchange), AA, Presence, Video		
Models	Virtual Machine, Cisco MCS appliance, Cisco UCS appliance, Licensing (UCL, UWL)		

Cisco Unified Communications Manager Express *(Small, SMB, Medium)*

Performance	--	Flexibility	--
Reliability	HSRP	Management	--
Scalability	Cisco ISR G2 3900: 250-450 users Cisco ISR G2 2900: 35-150 users Cisco ISR 3800: 168-240 users Cisco ISR 2800: 24-96 users	Security	--
Design Aspects	Phone System (Call Control)		
Models	3945, 3945E, 3925, 3925E, 2901, 2911, 2921, 2951, UC500		

Fortinet - FortiVoice *(Small, SMB, Medium, Large)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	40, 40S: 40 users 70, 70D4: 70 users 100, 100T: 100 users (~\$21,000) VM: 50 – 300 users 2000E-T2, 200D, 200D-T: 2000 users ----- SIP: 8 to 100 lines AA: 20 to 100 FXO, FXS, T1/E1 PRI	Security	--
Design Aspects	Phone System (Call Control), Messaging, Call Center, AA Pricing: 25-users (~\$6,000), 50-users (~\$12,000), 100-users (~\$21,000), FortiCall (\$25 per line per month)		
Models	40, 40S, 70, 70D4, 100, 100T, VM, 2000E-T2, 200D, 200D-T		

b	Voice Gateway

Cisco ISR G2 3900 *(SMB, Medium, Large)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	SRST: 730-1500 endpoints SIP/CUBE: 800-2500 sessions FXS: 64-112 ports FXO: 40-64 ports	Security	--
Design Aspects	--		
Models	3945, 3945E, 3925, 3925E		

Cisco ISR G2 2900 *(SMB, Medium, Large)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	SRST: 35-250 endpoints SIP: 100-600 sessions FXS: 16-40 ports FXO: 16-28 ports	Security	--
Design Aspects	--		
Models	2901, 2911, 2921, 2957		

Cisco ISR 800 *(Small, SMB)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	SRST: 4 endpoints SIP: 4 sessions FXS: 4 ports FXO: 1 ports	Security	--
Design Aspects	--		
Models	880		

Cisco ISR 3800 *(SMB, Medium, Large)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	CME/SRST: 168-240 users	Security	--
Design Aspects	--		
Models	3825, 3845		

Cisco ISR 2800 *(SMB, Medium)*

Performance	--	Flexibility	--
Reliability	--	Management	--
Scalability	CME/SRST: 24-96 users	Security	--
Design Aspects	--		
Models	2801, 2811, 2821, 2851		

#1a Hardware Options (Voice Gateway) based on Number of Users

Below are voice gateway hardware options based on the number of users followed by recommended voice circuits and conference bridge ports.

- **4 users:** Cisco 880, Conference bridge ports (2)
- **50 users:** Cisco 2911, Voice T1/E1 (4), Conference bridge ports (25)
- **100 users:** Cisco 2921, Voice T1/E1 (6), Conference bridge ports (50)
- **250 users:** Cisco 2951, Voice T1/E1 (8), Conference bridge ports (75)
- **730 users:** Cisco 3925, Voice T1/E1 (12), Conference bridge ports (100)
- **1200 users:** Cisco 3945, Voice T1/E1 (18), Conference bridge ports (150)

#2 Hardware Consolidation Option

Some of the voice components can be consolidated with other components in the design using one of the following options:

- The **Voice Gateway** component can be consolidated with the **WAN Router** (Hub, Spoke) which connects into the PSTN. The decision to integrate the Voice Gateway into an existing router (WAN router, Edge Router) depends on the voice capacity and the overall performance of the router. If a router is consistently running above 40% CPU, then it's recommended to use a standalone Voice Gateway router to avoid processing delays for voice traffic.
- **Phone System** (using Cisco CME for Voice & CUE for Messaging) can be consolidated with the **WAN Router** (Hub, Spoke) which connects into the PSTN.
- **Phone System** (using Cisco CME for Voice & CUE for Messaging) can be consolidated with the **Edge Router** (Internet Edge) which connects into the PSTN.

Note: Reference the "Hardware Table" for any specific hardware that may be listed for consolidation.

Cisco Unified 9951 and 9971:

- Five-line phone (on 9971)
- Support for video telephony by adding a USB camera
- Support for Bluetooth and USB
- Supports WIFI (on 9971 model)

Cisco Unified 8945:

- Four-line phone
- Support for video telephony with built-in camera
- High resolution color display
- Deep-sleep power-save option ; can reduce power consumption by up to 90 percent

Cisco Unified 6900:

- Uses less power (up to 50%)
- Support deep-sleep mode (6921 and above).
- Single-line (on 6901) ; cost-effective phone
- Two-lines (on 6921)
- Four-lines (on 6945)
- Six-lines (on 6961)

VPN & Remote Access

Category: Network Solution (Security)

Prerequisite(s): Internet Edge, Firewall, and WAN (if using Site VPN) Solutions

Complete the steps below for building the design for the network solution. First, determine the VPN solution(s) that will be used on the network:

- **Client VPN (Remote Access):** a remote access solution where users can access network resources remotely using VPN software.
- **Site VPN:** a solution which creates a permanent secure connection between locations with multiple users using VPN hardware like a router or firewall appliance.

Step 1

Scalability for VPN Solution

Step 1-1

Determine the components for the solution

Within the existing topology determine which components will support VPN termination (client and/or site). It will be one (or more) of the following existing component(s):

- WAN Router
- Internet Edge Router
- Firewall



or



Example: In our network design, VPN termination will exist within the **WAN router** in the topology.

Step 2	Security for VPN Solution

Step 2-1	Encryption

The process where a key (cipher) is used to encrypt and decrypt an IP packet across a VPN connection. Encryption provides confidentiality for IP packets. Choose one of the following encryption protocols for the VPN solution:

- **AES** (Advanced Encryption Standard): Cipher algorithm that uses either 128-bit keys (AES-128), 192-bit keys (AES-192), or 256-bit keys (AES-256) for encrypting IP packets.
- **3DES**: Cipher algorithm that uses 168-bit keys for encrypting IP packets.

Recommendations: This ultimately comes down to what encryption protocol is supported on the VPN device. Using 3DES or AES are good encryption protocols to use. 3DES was commonly used for VPN tunnels in the past. However in today's VPN solutions, AES is used and recommended over 3DES due to the high encryption it supports.

Step 2-2	Authentication

The process where a key (hash) is used to verify the integrity (and its origin) of an IP packet. Choose one of the following authentication protocols for the VPN solution:

- **SHA-1** (Secure Hash Algorithm): Hash algorithm that provides a 160-bit hash function.
- **MD5** (Message Digest Algorithm): Hash algorithm that provides a 128-bit hash function.

Recommendations: Use SHA-1 (or SHA-2) which provides a higher hash function operation. Though MD5 is commonly used for VPN tunnels, so that can also be considered.

Step 2-3	Key Management

Used with all VPN protocols for Site VPN or Client VPN (if IPSec VPN is chosen) for key management. Choose one of the following methods the VPN solution will use for key management:

- **Pre-Share (ISAKMP)**: a pre-shared key is configured and used between two sites for establishing a VPN tunnel.
- **RSA (Certificates)**: the VPN components use certificates for establishing VPN tunnels between sites.

Recommendations: Using Pre-Share (ISAKMP) is the most common key management method and the easiest to setup, but not for managing many VPN sites. Using RSA is more secure and easier to manage, but requires additional configuration that can be complex from a support model perspective.

Step 3	Design Aspects for VPN Solution

Step 3-1	VPN Services

Use the table below to determine the VPN technologies that will be used for the Client or Site-based VPN solution. This will be based on the requirements gathered for this solution and other solutions completed (e.g. WAN):

VPN Type	Technology	Technology Add-Ons	WAN Cloud Design	Services Required
Client VPN	<i>IPSec VPN</i>	IKEv1, IKEv2	--	IPSec VPN
	<i>SSL VPN (Recommended)</i>	Tunnel, Clientless	--	SSL VPN
Site VPN	<i>DMVPN</i>	DMVPN GET VPN over DMVPN	#1a, 2ii, 4, 5ii	DMVPN
	<i>IPSec VPN</i>	IPSec VPN (IKE1, IKE2) IPSec VTI / IPSec over GRE FlexVPN (IKE2)	#1a, 2ii, 4, 5ii	IPSec VPN
	<i>GET VPN</i>	GET VPN	#1b, 2i, 3	Using L3 WAN, GET VPN
		GET VPN over DMVPN	#1a, 4	DMVPN
		GET VPN over LISP	#1a, 4	LISP

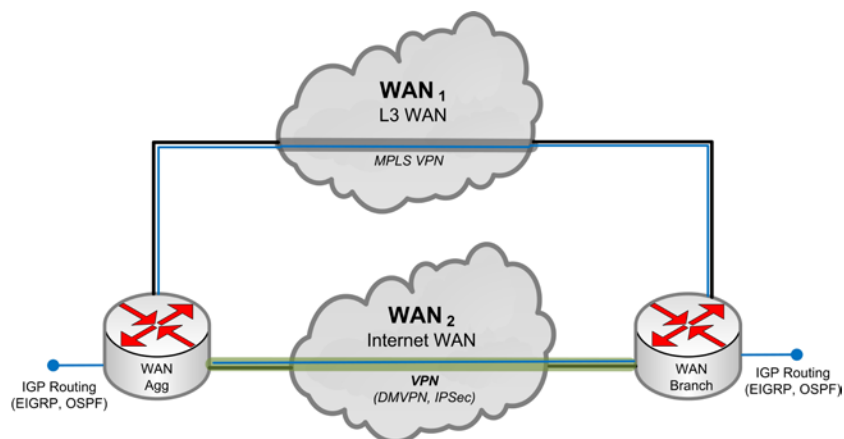
VPN Services Considerations:

- **Client VPN:** SSL VPN and IPSec VPN (IKEv1, IKEv2) are recommended solutions depending on the OS client that is used. Overall SSL VPN is recommended, but offers higher cost for SSL user counts compared to using IPSec VPN. There are now affordable options for Cisco's SSL VPN solution that has recently changed making SSL VPN an option to consider.
- **Site VPN:** It is strongly recommended to use FlexVPN (IKEv2) or DMVPN between sites for easy administration and deployment compared to IPSec VPN tunnels, which are static and not dynamic. With DMVPN the remote sites does not have to use a static IP, they can use a dynamic IP allowing the remote site to register with the hub router. From there all sites that are registered with the DMVPN hub which will know how to connect to other remote sites. If a firewall is used based on the requirements, existing hardware, or any preferences then you are limited to building only IPSec VPN tunnels.

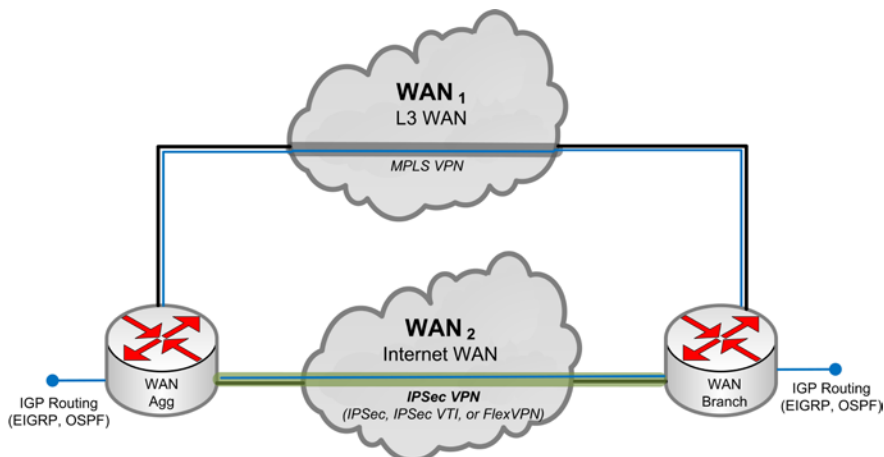
Example #1: continuing with our previous WAN design, we know that the secondary WAN cloud will be an Internet WAN. That will require some type of VPN technology to build secure communication between all sites on the WAN. This VPN technology can be DMVPN or IPsec based on the WAN cloud design we determined earlier (**WAN Cloud Design #2**).

<i>DMVPN</i>	DMVPN GET VPN over DMVPN	#1a, 2ii, 4, 5ii	DMVPN
<i>IPSec VPN</i>	IPSec VPN (IKE1, IKE2) IPSec VTI / IPSec over GRE FlexVPN (IKE2)	#1a, 2ii, 4, 5ii	IPSec VPN

The Internet WAN component makes up WAN Cloud Design #2ii. As a recap, this is what our WAN topology looks like:



From the table above, let's say that we will choose **IPsec VPN** for the VPN technology. Well there are different options for how that can implemented over our Internet WAN. We can setup static IPsec VPN tunnels, IPsec VTI (or IPsec over GRE) tunnels, or maybe FlexVPN tunnels which is based on IKEv2. Choosing which one can be determined later, but this will require IPsec VPN services to be added to our design.



Below is the VPN configuration relevant based on what is supported with the VPN technology that will be used:

- **Split Tunnel** (Client VPN): applies to remote access solutions where the VPN device specifies what traffic should use the established VPN tunnel. For example, for a Client VPN connection we may only want them to use the VPN tunnel when accessing internal network resources. For all other access like to the Internet that would route through their local Internet connection. This is a hot-topic debate where some say it should not be enabled and some say it should be enabled. The most common deployment is enabling Split Tunnel if content security is not implemented on the corporate network for filtering websites that users may access in conjunction with doing their work responsibilities.
- **IP Pool** (Client VPN): applies to remote access where a dedicated subnet is assigned for clients who are connected into the network.
- **VPN traffic** (Site VPN): determine what subnets need to communicate with other subnets across the VPN. This is configured in an Access Control List (ACL) for all sites accordingly. All subnets not listed will not use the VPN tunnel.
- **NAT** (Client & Site VPN): This info will be similar to what is defined for the VPN traffic, but additional ACLs are configured for the same subnet-to-subnet communications to NOT use NAT when using the VPN tunnel. Otherwise, the VPN device will try to translate all communication between the sites.

Services Required: Network Address Translation (NAT)

Step 4	Hardware for VPN Solution

Next we need to determine the hardware model that will be used for each component for the solution.

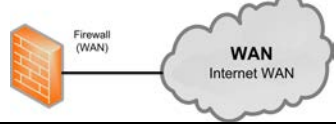
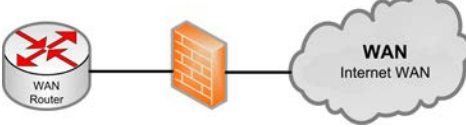
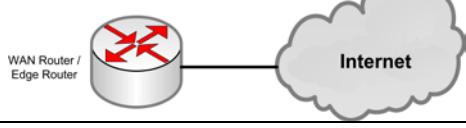
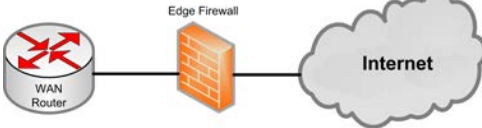
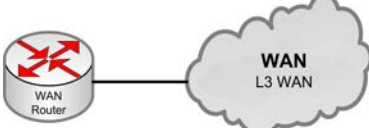
#1	Hardware Deployment Option

a	Client VPN

Determine where Client VPN services will be enabled based on the options below including what VPN services are supported:

#	Network Deployment	Description and VPN Support
#1	 Internet Edge firewall OR  Internet Edge router	Description: Client VPN termination exist on the Edge router or Firewall appliance (on Internet edge).
		VPN Support: IPSec VPN (IKEv1, IKEv2), SSL VPN
#2	 Client VPN Firewall	Description: Client VPN termination exist on a dedicated Client VPN firewall appliance to provide remote access services. This is ideal for large sized networks.
		VPN Support: IPSec VPN (IKEv1, IKEv2), SSL VPN

Determine where Site VPN services will be enabled based on the WAN topology already designed and its hardware deployment:

#	Network Deployment	Description and VPN Support
#1		Description: WAN router is plugged directly into an Internet WAN cloud. VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#2		Description: WAN router is a firewall appliance that is plugged directly into an Internet WAN cloud. VPN Support: IPSec (IPSec or IPSec VTI)
#3		Description: WAN router connects into a dedicated VPN firewall appliance which is plugged directly into an Internet WAN cloud. VPN termination still goes to the WAN router. VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#4		Description: WAN router is consolidated into the existing firewall appliance connected within the Internet edge. VPN Support: IPSec (IPSec or IPSec VTI)
#5		Description: WAN router is consolidated into the existing edge router within the Internet edge. VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#6		Description: WAN router is plugged into a DMZ interface on the existing firewall appliance that exist within the Internet edge. VPN termination still goes to the WAN router. VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#7		Description: WAN router is plugged directly into a L3 WAN cloud. VPN Support: IPSec, DMVPN, GET VPN

When to use: using Hardware Deployment (Client VPN) #2 and/or Hardware Deployment (Site VPN) #2

If the VPN appliance will be separate from the firewall appliance select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

Cisco ASA 5500-X Series *(SMB, Medium, Large)*

Performance	VPN: 200Mbps – 700Mbps	Flexibility	--
Reliability	--	Management	--
Scalability	VPN: 250 - 5000 tunnels (site, client)	Security	VPN (IPSec, SSL)
Design Aspects	Firewall Appliance		
Models	5512-X, 5515-X, 5525-X, 5545-X, 5555-X		

Cisco ASA 5505 Series *(Small)*

Performance	VPN: 100Mbps	Flexibility	--
Reliability	--	Management	--
Scalability	VPN: 10 - 25 tunnels (site, client)	Security	VPN (IPSec, SSL)
Design Aspects	Firewall Appliance		
Models	5505 Licensing (Security Plus, AnyConnect)		

Palo Alto Networks *(SMB, Medium, Large)*

Performance	VPN: 50Mbps – 24Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	VPN (IPSec): 25-8000 tunnels (site, client) VPN (SSL): 25 – 120,000 tunnels	Security	VPN (IPSec, SSL)
Design Aspects	Firewall Appliance		
Models	200, 500, 2020, 2050, 3020, 3050, 4020, 4050, 4060, 5020, 5050, 5060, 7050 ; fixed/modular, PAN-OS VM-100, VM-200, VM-300 ; virtualized (VMware), PAN-OSTM		

Fortinet: FortiGate *(Small, SMB, Medium, Large)*

Performance	IPSec VPN: 350Mbps – 100Gbps SSL VPN: 25Mbps – 6Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	Site VPN (IPSec): 20-10,000 tunnels Client VPN (IPSec): 250 – 64,000 tunnels VPN (SSL): 19 – 30,000 tunnels	Security	VPN (IPSec, SSL)
Design Aspects	Firewall Appliance (NGFW)		
Models	Standalone Firewall Appliances: FG/FWF-30D, FG/FWF-60C, FG/FWF-60D, FG/FWF-90D, FG, 100D, FG-200D, FG-240D, FG-280D-POE, FG-300C, FG-600-C, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3600C, FG-3700D, FG-3950B, FG-5001C, FG-5101C Virtual Firewall Appliances (VMware, Citrix, MS Hyper-V): FG-VM01, FG-VM02, FG-VM04, FG-VM08		

Below are hardware options based on the number of IPSec and/or SSL VPN sessions supported:

- **Cisco ASA 5512-X:** 250 SSL VPN sessions
- **Cisco ASA 5515-X:** 250 SSL VPN sessions
- **Cisco ASA 5525-X:** 750 SSL VPN sessions
- **Cisco ASA 5545-X:** 2500 SSL VPN sessions

A large, stylized white letter 'W' is centered within a dark gray rectangular box. The 'W' is composed of three distinct 'V' shapes joined together, with a slightly irregular, hand-drawn appearance.

~ Solutions ~

Web & E-Commerce

Category: Network Solution (Data Center)

Prerequisite(s): LAN and/or Data Center Solution, Internet Edge Solution

Complete the steps below for building the design for the network solution.

Step 1

Scalability for Web/E-Commerce Solution

Step 1-1

Determine the components for the solution

Determine the components for the solution:

- **Servers (Web, Application, Database):** these are three groups of servers providing a web farm (front-end facing towards the Internet), application farm (located in the middle), and a database farm (located in the backend). These components are managed by the system engineering team.
- **Load Balancing:** this component will likely exist within the web farm load balancing across a group of servers. Requires the "Content Switching" solution with this design.
- **Firewalls:** this component is used between each of the server groups to provide frontend and backend security. Requires the "Firewall" solution with this design.

Step 1-2

Web Farm Topology

Choose the web farm solution that would be deployed on the network. Below are the options to choose from:

- **Three-Tier Web Farm:** a web farm that consist of three layers, one for Web services, one for the Application services, and another for the Database services. Each layer is separated by a firewall appliance or polices. The Frontend Firewall connects between the Internet and the Web server farm. The backend firewall connects between all three networks. The Web servers usually communicate with the application servers which then pulls data or information from the Database servers. This web farm is one of the most commonly deployed solutions to provide web services. Load balancing often resides within the Web services layer to provide load balancing between the web servers.
- **Collapsed Multi-Tier Web Farm:** This solution is the same as the three-tier design, but it's more virtualized. Each layer is configured in a VLAN on the Data Center network with firewall services (physical firewall or ACLs) implemented between the different VLANs. This consolidates the environment and relies on the fast processing of the L2 or L3-switches for communicating with other networks. This solution can lower the overall complexity and devices to manage.

Recommendations: Both solutions are great options, but the three-tier solution was very common back in the Data Center 2.0, but as services are becoming more consolidated, the Collapsed Multi-Tier Web Farm is recommended. Network hardware (Switches and Routers) are getting faster in terms of processing, traffic forwarding in hardware, and

providing multi-protocol and services support using firewall services. Some web farms do not consist of all three components and using VLANs can still easily work for these environments. A three-tier model is often chosen when the engineer/administrators feel more comfortable to manage a network where they can “physical” see the design and how everything is connected.

Step 2	Design Aspects for Web/E-Commerce Solution

Step 2-1	Services to include with solution

Below are services that are used when deploying a web server farm infrastructure:

- VLAN
- Trunking (802.1Q)

These are services that are implemented on the Data Center switch components (Core, Distribution, Access).

Web 2.0

Category: System Solution
Prerequisite(s): Server Solution

Complete the steps below for building the solution:

Step 1	Other System Solutions applicable

This is a server based solution that is primarily designed and deployed by a system engineering team. Below are the required system solutions that are used for the Web 2.0 design:

- Server Solution

Web 2.0 is simply an application design that exist on one or more servers providing what the system solution will serve to users/clients on the network.

Step 2	Web 2.0 Components

Below are components used for a Web 2.0 solution that can be considered with the overall implementation:

- Blogs
- RSS
- Wiki
- Tagging
- Social Bookmarking
- Instant Messaging (IM)
- Forums
- Widgets
- AJAX

WebEx

Category: Network Solution (Voice)
Prerequisite(s): Internet Edge Solution

When to use: to provide cloud-based web conferencing services

Cisco WebEx is a solution that provides web based conferencing and collaboration services. Most of the applications are cloud based hosted on a dedicated Cisco WebEx network which is geographically spread out across different Data Centers. Therefore, it is treated as a Software as a Service (SaaS) under a Cloud Computing solution. This means Cisco manages the servers and applications within the WebEx Data Center. The only thing required from a client perspective is an Internet Edge solution and a web browser.

The Cisco WebEx applications exist in a Cisco WebEx Collaboration Cloud which can provide real-time interaction and connecting to the best Data Center location based on performance/latency. Another WebEx infrastructure component is the Cisco WebEx Global Site Backup (GSB) which can automatically and transparently switch all meeting activity to a backup site if there is a failure/issue.

Below are some of the Cisco WebEx applications that can be used on the network:

- **Cisco WebEx Meeting Center:** web-based application that allows you to schedule on-line meetings. You can invite people to join a meeting by email, instant message, or as a text message. This application also allows you to share your screen for presentations or any other interaction that you do on your desktop during a scheduled meeting. This application is ideal for training sessions or events.
- **Cisco WebEx Training Center:** has the same capabilities as the "Cisco WebEx Meeting Center" application, but focused for training events. Can support up to 1,000 participants.
- **Cisco WebEx Event Center:** has the same capabilities as the "Cisco WebEx Meeting Center" application, but focused for special events. Can support up to 3,000 participants.

Wide Area Network (WAN)

Category: Foundation Solution

Prerequisite(s): LAN Solution and/or Data Center Solution

When to use: a network that is shared among a group of sites (privately or publically using VPN).

Complete the steps below for building the design for the foundation solution:

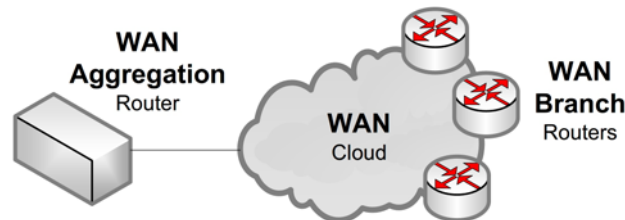
Step 1

Scalability for WAN

Step 1-1

WAN Components and Deployment

In the WAN topology, a WAN router (Aggregation or Branch router) connects to a WAN cloud as shown below.



Here is a summary for all of the WAN components and how they should be deployed:

- **Aggregation (or Hub):** a component that exist at the Hub (main office) location. This component connects into the LAN or Data Center Core component.
- **Branch (or Spoke):** a component that exists at a Spoke (remote/branch office) location. This component connects into the LAN or Data Center Core component at the remote site.
- **WAN cloud:** the WAN Aggregation and Branch router components would connect into a WAN cloud. The WAN cloud(s) in the topology will be one or more of the following types:
 - o **Internet WAN:** a public WAN cloud that uses the Internet for access between all sites. Using an Internet WAN cloud doesn't offer any explicit guarantees of performance and delay (SLA) between sites.
 - o **L3 WAN:** a private WAN cloud that uses L3 technologies (e.g. IP, MPLS) for access between sites.
 - o **L2 WAN:** a private WAN cloud that uses L2 technologies (e.g. VLAN/802.1Q, VPLS) for access between sites.

The design of the WAN cloud will happen in a later design step.

Step 2	Reliability for WAN

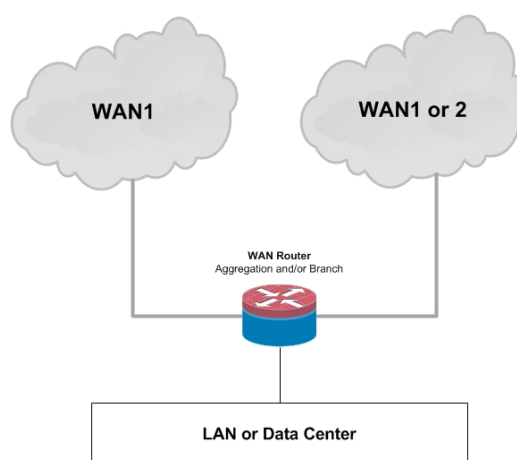
Step 2-1	Choose Redundancy Model

Determine which redundancy model should be used for the WAN if reliability is important:

1. Dual WAN Clouds using Single WAN Router
2. Dual WAN Clouds and Routers

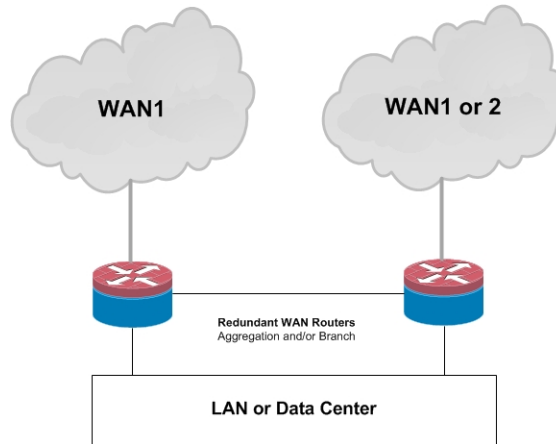
#1	Dual WAN Clouds using Single WAN Router

Description: In this redundancy option we have a single WAN router (Aggregation or Branch) connecting with two different/same WAN providers. The main redundancy for this option is with the WAN cloud and enabling a dynamic routing protocol (EIGRP or OSPF) to provide dynamic re-routing if a network fails. The biggest concern here is the recurring cost for getting another provider, however, if there is an outage which last for a long period of time then it may impact the business overall. There is a higher chance of failure with the WAN provider itself or with any of the WAN connections (e.g. T1, etc) compared to a failure happening on the WAN router itself.



- **When to use:** using a single edge router connecting to two service providers providing partial redundancy. This redundancy option is common for any size network or if WAN redundancy is moderately important to the business.
- **Services Required:**
 - IP Routing

Description: In this redundancy option we have redundant WAN routers (Aggregation or Branch) with two different/same WAN providers. The main redundancy for this solution besides the hardware and provider is enabling a dynamic routing protocol (EIGRP or OSPF) to provide dynamic re-routing if a network fails. If there is a failure the network between the sites will continue to operate transparently. Furthermore, if the branch office(s) will be deployed with redundant branch routers without a Layer 3 Core switch then implementing an FHRP is recommended to provide default gateway redundancy for the office.



- **When to use:** redundant WAN routers (Aggregation or Branch) connected with two different/same WAN providers providing full redundancy (if using two different service providers). This redundancy option is common for Medium and large networks or if WAN redundancy is critical for the business.
- **Services Required:**
 - o IP Routing
 - o First-Hop Redundancy Protocol (FHRP) ; used for Branch office routers

Below is hardware redundancy considerations that can be done for any component in the topology.

- **Hardware:** using redundant hardware is very common to provide hardware level redundancy. This may also include redundant line modules and Supervisor engines (CPU). Here is a summary for what hardware can be redundant.
 - Device/Chassis
 - Line Modules (using a chassis model)
 - Supervisor Modules (using Chassis model)
- **Power:** redundant power supplies, using a UPS (like APC), and connecting to different power circuits for the network equipment.

Step 3

Performance for WAN

Follow the steps below to determine the bandwidth service for all WAN connections in the design. Mark this information on the network diagram for reference. This information is important when it comes time to determine the correct hardware model.

Step 3-1

Determine the number of remote sites

Determine the total number of branch offices on the WAN including additional branch offices that may be added to the network over time.

Example: let's say that our WAN will consist of 5 branch offices and 1 main office.

Step 3-2

Determine the bandwidth at each Branch office

Determine the total bandwidth needed for each Branch WAN router (WAN interface) based on the type of user and their traffic usage. Use the following table below as a reference:

Note: if you already know what bandwidth technology (e.g. T1, Ethernet) will be used for each Branch office router, you can skip this step.

User Type	Traffic Services	Bandwidth Per User
Low Performing User	Basic Email and Web Usage Basic Application Usage Basic File Server Usage (less than ~1KB) Basic Voice Usage	~90kbps
Moderate Performing User	Moderate Email and Web Usage Moderate File Server Usage (less than ~1MB) Moderate Application Usage Basic Voice Usage	~ 130kbps to 256kbps Note: If a user will use more than one of the services from the traffic services list, you should consider a higher bandwidth rate within the bandwidth range provided.
High Performing User	High Email and Web Usage High File Server Usage (more than ~1MB) High Application Usage Moderate Voice Usage (Voice, Web Conferencing) Video Streaming Usage	~256kbps to 512kbps Note: If a user will use more than one of the services from the traffic services list, you should consider a higher bandwidth rate within the bandwidth range provided.

Design Consideration: if you are unsure of the number of low, moderate, or high performing users you can use 130kbps per user (the average baseline) which is typically used to calculate the total WAN performance for each site.

Example: each Branch office we will have ~6 users that will access various services over the WAN. We can do this from two different approaches for calculating what the WAN performance should be for each site.

Approach #1: If we don't know how many users are low, moderate, or high performing users, we can consider the average bandwidth of 130Kbps per user. Doing the math that would be 6 users x 130Kbps. That would be ~780Kbps. This means we would consider a bandwidth technology that can support 780Kbps or higher.

Approach #2: We can determine the estimated number of low, moderate, and high performing users. Let's say that we will have 4 low performing users that will do basic email and web services over the WAN. And let's say that we will have 2 high performing users based on what those users will do.

Since our high performing users has a recommended range of 256kbps to 512kbps, we need to consider how many of the traffic services will be used. Let's say that these 2 high performing users will use the following traffic services:

- High Email and Web Usage
- High File Server Usage

Therefore, let's choose a bandwidth rate that is right in the middle or higher within the provided range (256kbps to 512kbps). That would be 384kbps, so that is the rate we will use for our high performing users. Doing the math, we will calculate the two groups of users then added them together:

- 4 users x 90kbps = 360Kbps
- 2 users x 384kbps = 768Kbps

360Kbps + 768kbps = ~1.3Mbps for the WAN Performance at each site.

This means we want to consider a bandwidth technology that can support ~1.3Mbps or higher.

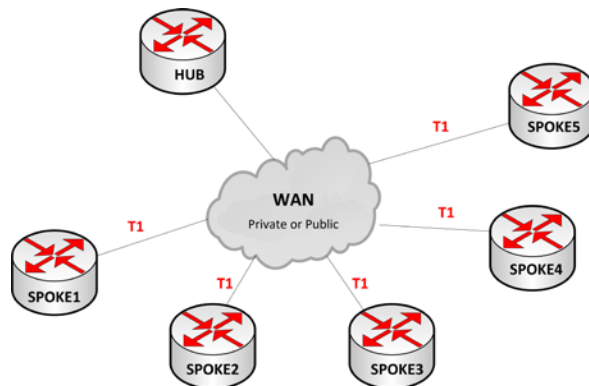
Summary: Based on the performance calculations completed for both approaches, the WAN performance at each site would range from 768Kbps to 1.3Mbps that is needed for each WAN connection.

Based on the WAN performance calculated from the last step, determine the best bandwidth technology that should be used for each Branch WAN router component (WAN facing interface).

Use the following table below as a reference to make your decision.

Bandwidth Services	Bandwidth Range	WAN Cloud Support	Encapsulations	Notes
T1, E1	1Mbps – 3Mbps	Internet WAN, L3 WAN	PPP, HDLC, Frame Relay Bundling (MLP, MFR)	--
Broadband (DSL, Cable)	10Mbps – 45Mbps	Internet WAN	ATM	--
DS-3	45Mbps	Internet WAN, L3 WAN	ATM	--
Optical	155Mbps – 9.6Gbps	Internet WAN, L3 WAN	ATM	--
DWDM	20Gbps – 400Gbps	L3 WAN	--	--
Ethernet (FE, GE, 10GE)	10Mbps – 100Mbps 1Gbps – 10Gbps	Internet WAN, L3 WAN, L2 WAN	VLAN, 802.1Q	Recommended
Wireless (3G, 4G)	1Mbps - 10Mbps	Internet WAN	--	Backup

Example: each of our branch offices require a WAN performance of ~1.3Mbps. Therefore, at a minimum, a single T1 (1.544Mbps) can be used for connecting into the WAN cloud (Internet WAN or L3 WAN):



To determine the expected WAN Aggregation bandwidth, the following needs to be obtained:

- **Number of WAN Branch Offices:** determine the number of branch offices that will connect to the main office.
- **Bandwidth Speed:** determine the WAN bandwidth technology and/or throughput used for each branch office.
- **WAN Oversubscription:** determine the amount of oversubscription (if any) required based on how active the branch offices will be. This can be based on having high oversubscription (4:1 ratio) which is ideal when only a few branch offices will concurrently connect through to the main site (or Data Center). There is low oversubscription (2:1 ratio) which is ideal if at least half of the branch offices will concurrently connect through to the main site (or Data Center). Or maybe no oversubscription (1:1 ratio) if you know that all branch offices will be concurrently connecting through to the main site (or Data Center). Overall it's recommended to use a lower oversubscription if you expect more of the branch offices will be concurrently connecting to the main site (or Data Center) for various services.

With the information gathered from the list above use the following formula to calculate the expected throughput on the WAN Aggregation router.

It's recommended to calculate the expected throughput for one or two of these oversubscription ratio types listed in the table. This will help to see the range of throughput that is needed. You will also see in the table that for each oversubscription type, it will show a formula for L3 WAN and Internet WAN (using VPN). In a later design step, you will determine what the WAN cloud(s) will be in the topology.

#	Oversubscription Ratio	Formulas
1	None (1:1)	L3 WAN: (# of Branch offices) x (Bandwidth speed at each site)
		Internet WAN: (# of Branch offices) x (Upload + Download Bandwidth speed at each site)
2	Low (2:1)	L3 WAN: [(# of Branch offices) x (Bandwidth speed at each site)] / 2
		Internet WAN: [(# of Branch offices) x (Upload + Download Bandwidth speed at each site)] / 2
3	High (4:1)	L3 WAN: [(# of Branch offices) x (Bandwidth speed at each site)] / 4
		Internet WAN: [(# of Branch offices) x (Upload + Download Bandwidth speed at each site)] / 4

Example: We have 5 branch offices using a T1 (1.544Mbps) connecting into the WAN. Let's calculate the throughput for the WAN Aggregation router (using Internet WAN or L3 WAN) using no oversubscription and low oversubscription.

- **Oversubscription Ratio (1:1):**
 - o **L3 WAN:** $5 \times 1.544\text{Mbps} = \sim 7.5\text{Mbps}$
 - o **Internet WAN (using VPN):** $5 \times (1.544 + 1.544) = \sim 15\text{Mbps}$
- **Oversubscription Ratio (2:1):**
 - o **L3 WAN:** $[5 \times 1.544\text{Mbps}] / 2 = \sim 3.8\text{Mbps}$
 - o **Internet WAN (using VPN):** $[5 \times (1.544 + 1.544)] / 2 = \sim 7.5\text{Mbps}$

Determine the bandwidth technology that will be used at the main office based on what was calculated from the previous step. Use the following table below as a reference to make your decision:

Bandwidth Services	Bandwidth Range	WAN Cloud Support	Encapsulations	Notes
T1, E1	1Mbps – 3Mbps	Internet WAN, L3 WAN	PPP, HDLC, Frame Relay Bundling (MLP, MFR)	--
Broadband (DSL, Cable)	10Mbps – 45Mbps	Internet WAN	ATM	--
DS-3	45Mbps	Internet WAN, L3 WAN	ATM	--
Optical	155Mbps – 9.6Gbps	Internet WAN, L3 WAN	ATM	--
DWDM	20Gbps – 400Gbps	L3 WAN	--	--
Ethernet (FE, GE, 10GE)	10Mbps – 100Mbps 1Gbps – 10Gbps	Internet WAN, L3 WAN, L2 WAN	VLAN, 802.1Q	Recommended
Wireless (3G, 4G)	1Mbps - 10Mbps	Internet WAN	--	Backup

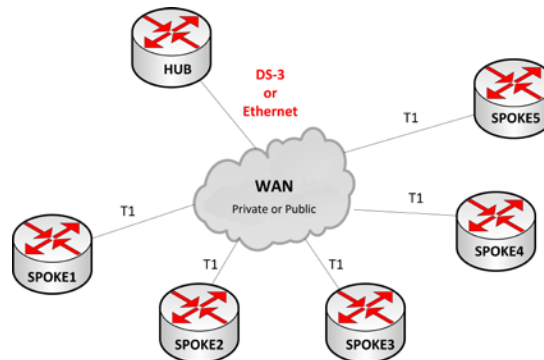
Example: we can determine the best bandwidth technology to use based on what we calculated in the last step.

- Using Oversubscription Ratio (1:1): the bandwidth ranges from 7.5 to 15Mbps
- Using Oversubscription Ratio (2:1): the bandwidth ranges from 3.8 to 7.5Mbps

This means the following bandwidth technologies can work based on the WAN cloud support:

- **Internet WAN cloud support:** Broadband (10-45Mbps), DS-3 (up to 45Mbps), or Ethernet (FE,GE,10GE)
- **L3 WAN cloud support:** DS-3 (up to 45Mbps), or Ethernet (10 – 100Mbps, 1 – 10Gbps)

We don't know what our WAN cloud will be, so the bandwidth technology will either be a fractional DS-3 (up to 15Mbps) or an Ethernet handoff from the WAN provider. Broadband is not ideal for WAN aggregation due to its asynchronous bandwidth speeds.

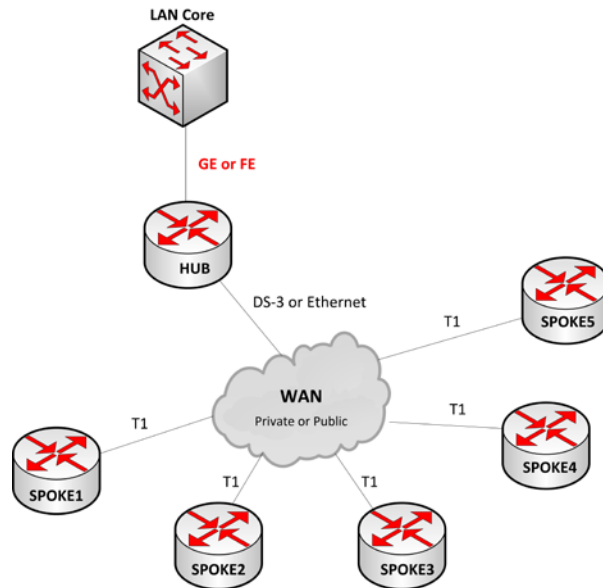


Determine the bandwidth service used between the WAN router connecting into the LAN/Data Center Core.

This is based on the bandwidth used on the WAN interface and the bandwidth must be within that range. Below are your typical bandwidth services to choose between:

- **Fast Ethernet (100Mbps):** used when the WAN speed is 100Mbps or below (e.g. DSL/Cable, T1, WWAN, DS-3, Fast Ethernet).
- **Gigabit Ethernet (1Gbps):** used when the WAN speed is between 100Mbps to 1Gbps (e.g. OC-3, OC-12, Gigabit Ethernet).
- **10-Gigabit Ethernet (10Gbps):** used when the WAN speed is between 1Gbps to 10Gbps (e.g. OC-48, OC-192, Ten Gigabit Ethernet).

Example: if the WAN speed for the WAN aggregation router will be a fractional DS-3 circuit (<45Mbps) or an Ethernet handoff, then the bandwidth connection between the router and the LAN/Data Center can be Fast Ethernet (at a minimum) or Gigabit Ethernet (recommended).



You can include a WAN optimization solution to the network to improve performance of traffic usage over the WAN between the client and the servers.

Required Solution: Optimization

Step 4	Security for WAN

Step 4-1	Security services to include with solution

Below are Security Services/Solutions that should be deployed with the solution:

- Security Best Practices
- Access Control Lists (ACLs)
- Virtualization (Network): Layer 3 Virtualization

Step 5	Network Management for WAN

Below are "Network Management Services" that should be deployed within the WAN solution:

- SNMP
- NTP
- NetFlow
- Syslog
- RADIUS *OR* TACACS+
- VTY Access

Step 6	Design Aspects for WAN

Below are specific design elements to complete for the solution.

Step 6-1	WAN Cloud Design

Determine which WAN Cloud Design to use based on the number of WAN clouds in the topology:

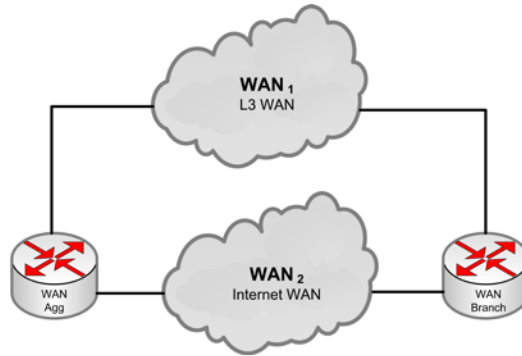
- **Design #1a:** Using a single WAN cloud that will be an Internet WAN.
- **Design #1b:** Using a single WAN cloud that will be a L3 WAN
- **Design #2:** (i) The primary WAN cloud will be a L3 WAN and (ii) the secondary cloud will be an Internet WAN
- **Design #3:** Both primary and secondary clouds are L3 WANs.
- **Design #4:** Both primary and secondary clouds are Internet WANs.
- **Design #5:** (i) The primary WAN cloud will be a L2 WAN and (ii) the secondary cloud will be an Internet WAN

Use the table below to determine the technology including the routing/switching configuration that will be supported with the design that will be used:

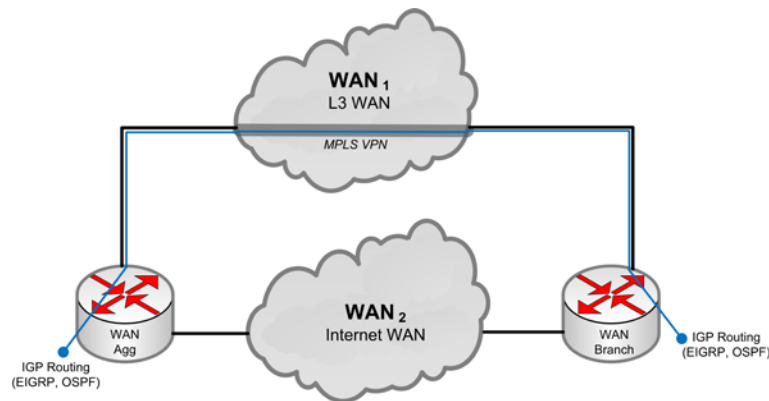
#	WAN Cloud	Technology:	Connectivity between Sites	Add-ons
#1a, #4	Internet WAN	VPN Solution Required (DMVPN, IPSec)	Routing (IGP, Static)	--
		or VPN Solution Required (GET VPN: GETVPN over LISP)	Routing (LISP)	--
#2	L3 WAN (Primary)	MPLS Ethernet, IP	Routing (IGP)	VPN Solution (GET VPN)
	Internet WAN (Secondary)	VPN Solution Required (DMVPN, IPSec)	Routing (IGP, Static)	--
#1b, #3	L3 WAN	MPLS Ethernet, IP	Routing (IGP)	VPN Solution (GET VPN)
#5	L2 WAN (Primary)	VPLS, EoMPLS, L2TPv3	Switching (802.1Q, VLAN), Routing (IGP)	--
	Internet WAN (Secondary)	VPN Solution Required (DMVPN, IPSec)	Routing (IGP, Static)	--

Example: let's say that our WAN will consist of two WAN clouds to provide redundancy. Therefore, we would consider design # 2, 3, 4, or 5. Let's choose design #2 where our primary cloud will be a L3 WAN and the secondary cloud will be an Internet WAN.

Therefore, the topology would look something like this:

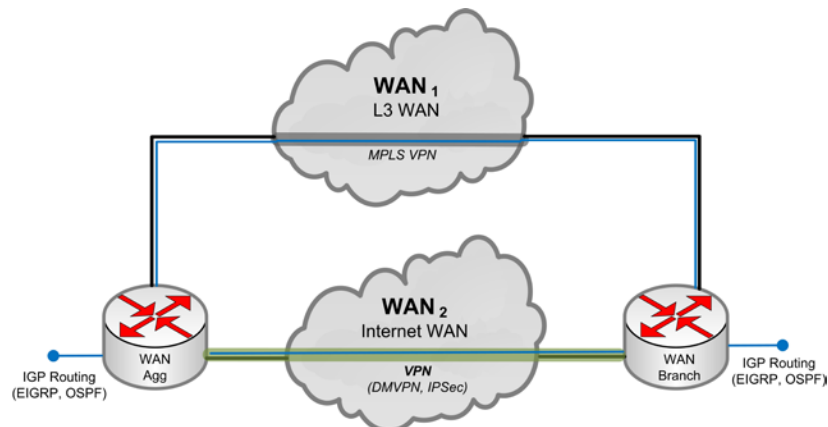


For design of the L3 WAN cloud (primary), the private WAN provider we choose may support MPLS or some other layer 3 service that our WAN router will be plugged into. MPLS is the most common for modern networks today. Using this design option it can allow us to implement IGP routing between our sites for communication.



Furthermore, we can even add GET VPN on-top of this network to provide tunnel-less encryption for increased security.

For the design of the Internet WAN cloud (secondary), our WAN router would be plugged into a Public network (Internet). To build the communication between all the remote sites it would require a specific VPN technology supported with this option such as DMVPN or IPSec. But it does have further options where we can implement IGP routing between our sites for communication.

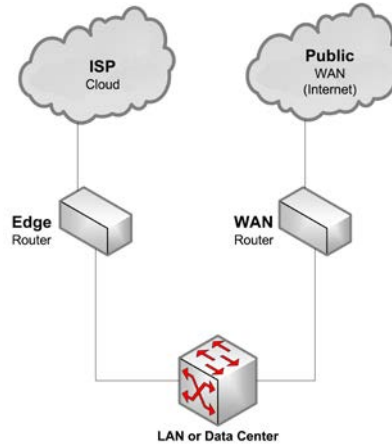


This is how you can use this provided chart to determine how the WAN clouds will be setup.

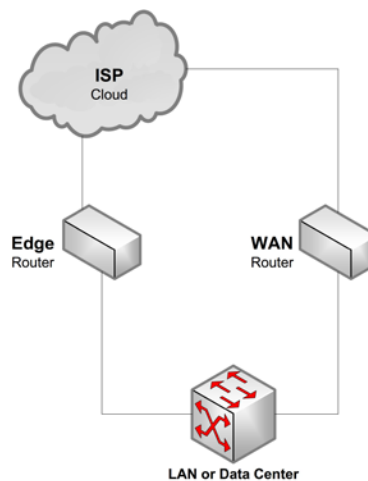
When to use: if the WAN topology is using an Internet WAN cloud(s).

If the network already has an Internet cloud (Internet Edge Solution), determine if the Internet WAN will be a separate Internet connection or shared with the Internet Edge.

1. **Separate Internet Cloud:** The Internet WAN cloud will use a separate Internet connection with the WAN router.



2. **Shared Internet Cloud:** The Internet WAN will use the same Internet cloud that exist in the Internet Edge solution (most common).



These are additional services that can be implemented (if required) within the solution.

- General Best Practices
- Multicast
- IPv6
- Quality of Service (QoS)

Determine the subnet types and the number of subnets used for the WAN.

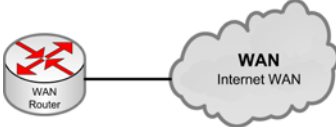
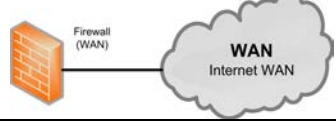
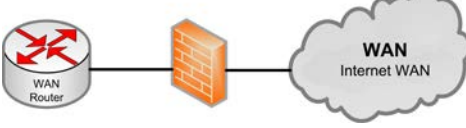
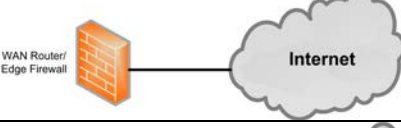
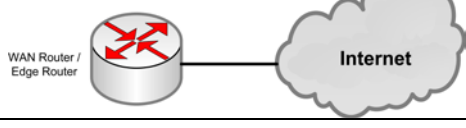
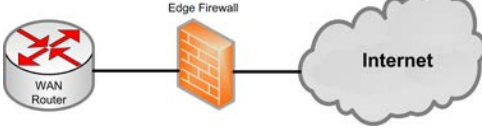
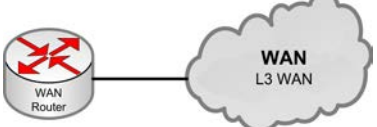
- **WAN Network:** a subnet that is used on the WAN between other WAN routers (Aggregation, Spoke).
- **Transit Network:** a small subnet that is used between the WAN components and the LAN/Data Center Core switch component.
- **Other:** other subnets created based on any unique requirement or preference.

Step 7	Hardware for WAN

Next we need to determine the hardware model that will be used for each component for the solution.

#1	Hardware Deployment

Determine the hardware deployment for the WAN router (with its WAN cloud type) based on the following options including what VPN services are supported. This will become important when you build out the VPN solution design (if using an Internet WAN).

#	Network Deployment	Description and VPN Support
#1		Description: WAN router is plugged directly into an Internet WAN cloud.
		VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#2		Description: WAN router is a firewall appliance that is plugged directly into an Internet WAN cloud.
		VPN Support: IPSec (IPSec or IPSec VTI)
#3		Description: WAN router connects into a dedicated VPN firewall appliance which is plugged directly into an Internet WAN cloud. VPN termination still goes to the WAN router.
		VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#4		Description: WAN router is consolidated into the existing firewall appliance connected within the Internet edge.
		VPN Support: IPSec (IPSec or IPSec VTI)
#5		Description: WAN router is consolidated into the existing edge router within the Internet edge.
		VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#6		Description: WAN router is plugged into a DMZ interface on the existing firewall appliance that exist within the Internet edge. VPN termination still goes to the WAN router.
		VPN Support: IPSec (IPSec, IPSec VTI, FlexVPN), DMVPN, GET VPN (GET VPN over LISP)
#7		Description: WAN router is plugged directly into a L3 WAN cloud.
		VPN Support: IPSec, DMVPN, GET VPN

When to use: choosing the WAN router hardware when using Hardware Deployment # 1, 3, 6, or 7

Select the hardware for each component using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

Cisco ISR 4000 Series *(Large)*

Performance	IMIX: 980Mbps – 1Gbps T1/E1, T3/E3, Serial, xDSL, GE, 10GE support	Flexibility	Voice (CME, CUBE, SIP, SRST), Optimization (WAAS)
Reliability	--	Management	SDN (Cisco onePK), ISR-AX (monitoring services)
Scalability	--	Security	Firewall, VPN
Design Aspects	L3, AVC		
Models	Hardware: 4451, 4431, 4351, 4331, 4321 ; fixed/modular Defaults: Four built-in 10/100/1000 Ethernet ports Modules: Cisco Enhanced Services Module (SM-X), Cisco Network Interface Modules (NIMs) Software/OS: Universal IOS XE, ISR-AX (Application Experience) Licensing: Performance, Security, Voice, Application Experience (AX)		

Cisco ISR G2 3900 Series *(Medium, Large)*

Performance	IMIX: 100 – 350Mbps T1/E1, T3/E3, 4G/LTE, DSL, GE support	Flexibility	Voice, Messaging, UCS E-Series, Optimization (WAAS)
Reliability	--	Management	--
Scalability	20 sites (3925)	Security	Firewall, VPN, IPS, Content Security
Design Aspects	L3, Video, Medianet		
Models	Hardware: 3945, 3945E, 3925, 3925E ; fixed/modular Software/OS: Cisco IOS Licensing: IP Base, Security, Unified Communications, Data		

Cisco ISR G2 2900 Series *(SMB, Medium)*

Performance	IMIX: 25 – 75Mbps T1/E1, T3/E3, 4G/LTE, DSL, GE support	Flexibility	Voice, Messaging, UCS E-Series, Optimization (WAAS)
Reliability	--	Management	--
Scalability	Up to 25 users (2911)	Security	Firewall, VPN, IPS, Content Security
Design Aspects	L3, Video, Medianet		
Models	Hardware: 2901, 2911, 2921, 2951 ; fixed/modular Software/OS: Cisco IOS Licensing: IP Base, Security, Unified Communications, Data		

Cisco ISR G2 1900 Series *(Small, SMB)*

Performance	IMIX: 15 – 25Mbps T1/E1, 3G, DSL, GE support	Flexibility	Wireless (AP), Optimization (WAAS), PoE, ePOE
Reliability	--	Management	--
Scalability	--	Security	Firewall, VPN, IPS, Content Security
Design Aspects	L3		
Models	Hardware: 1905, 1941, 1941W, 1921 ; fixed/modular Software/OS: Cisco IOS Licensing: IP Base, Security, Unified Communications, Data		

Cisco ASR 1000 Series *(Large)*

Performance	Router/FW: up to 2.5 – 100Gbps+ VPN: up to 78Gbps T1/E1, T3/E3, GE, 10GE support OC-3, OC-12, OC-48, OC-12 support	Flexibility	Voice (CUBE)
Reliability	ISSU	Management	Cisco Prime Network Analysis Module
Scalability	VPN: 8000 tunnels	Security	Firewall, VPN
Design Aspects	L3, QoS, FPM, AVC, WAN Aggregation		
Models	Hardware: 1001, 1002, 1002-X, 1004, 1006, 1013 ; chassis Software/OS: Cisco IOS XE Modules: SIP (SPA Interface Processor), Route Processor (RP1, RP2), ESP		

Cisco CSR 1000V Series *(Medium, Large)*

Performance	Small: 10-100Mbps 1 vCPU, 2.5GB RAM Large: 250Mbps-1Gbps 4 vCPU, 4GB RAM Amazon EC2: 10-50Mbps	Flexibility	Optimization (WAAS)
Reliability	FHRP	Management	--
Scalability	--	Security	Firewall, VPN
Design Aspects	L2, L3, Virtualization (MPLS, VPLS, VRF, BFD, EoMPLS), OTV, LISP		
Models	Virtual Machine (VMware ESXi, Citrix XenServer, Red Hat KVM, Amazon EC2 cloud ; Cisco IOS-XE Technology Packages (Standard, Advanced, Premium) Pricing is ~\$3,000 (five-year license with support)		

Hardware Notes:

- **Cisco Router Performance:** reference the Routing Performance chart for the estimated throughput and PPS (packets-per-second) for your router selection. Those numbers should only serve as a baseline for your decision. You can view the chart here: <http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf>

Wireless

Category: Network Solution

Prerequisite(s): LAN Solution and/or Data Center Solution

Complete the steps below for building the design for the network solution.

Step 1	Scalability for Wireless Solution
Step 1-1	Determine the Wireless Solution Architecture

Determine the type of Wireless solution that will be deployed:

- **Internal (WLAN) - Centralized Solution:** A wireless network that is used internally (local) within a site's WAP (Wireless Access Point) coverage area. In this internal WLAN solution, all Access Points are managed and configured on a Wireless LAN Controller (WLC). The administration and setup is extremely easy, but the cost is higher because of the WLC. It also provides the ability for users to transparently roam (Fast Secure Roaming) between APs within the WLAN. This solution can provide some of the following attributes:
 - o Provides visibility into the wireless spectrum to manage RF interference for preventing unexpected downtime.
 - o Provides self-healing and optimization.
- **Internal (WLAN) - Decentralized Solution:** A wireless network that is used internally (local) within a site's WAP (Wireless Access Point) coverage area. In this WLAN solution all access points are configured and managed individually increasing the overall administration. However, the cost is lower compared to the Centralized WLAN Solution.
- **External (WWAN):** A wireless network that is used externally with a cellular network (e.g. AT&T, Verizon). The WWAN is seen as another Internet or Untrusted network. Common for providing a backup Internet connection for small and SMB environments.

Determine the components for the solution based on the wireless architecture:

Using Centralized WLAN Solution:

- **Lightweight Access Points (LWAP):** The access point is what wireless clients will connect to for joining a specific network. This component connects into the LAN Access switches enabled for PoE. A LWAP requires a wireless LAN controller (WLC) to be managed. They cannot operate independently.
- **Wireless LAN Controller (WLC):** This component is responsible for managing all of the Lightweight Access Points on the network. The WLC is usually connected into the Core switch.

Using Decentralized WLAN Solution:

- **Standalone Access Point(s):** The access point is what wireless clients will connect to for joining a specific network. This component connects into the LAN Access switches enabled for PoE. It doesn't require a centralized wireless controller to be managed.

Using External WWAN Solution:

- **External Wireless Radio:** this component is only applicable for a WWAN solution. It involves a cellular radio (e.g. 3G) that exist inside of the edge router, firewall appliance, or a dedicated router within the Internet edge solution to provide Internet services.

Determine what wireless networks (SSIDs) will be configured based on the type of user groups.

- **Corporate Users:** a wireless network used by internal employees to access internal network resources and the Internet.
- **Guests:** a wireless network that only allows access to the Internet. Access to other networks (e.g. internal networks) is restricted.
- **Custom:** a wireless network based on a custom policy and/or group of users defined by the company.

Each wireless network (SSID) should be associated to a VLAN. 802.1Q Trunking is used to support multiple VLANs. This is configured on the WAP switch ports, WLC switch ports, and all inter-connection ports.

Services Required: VLAN, 802.1Q Trunking

#2

WLC (separate or shared)

When to use: using a Centralized WLAN solution

Determine if those wireless user groups will use a separate WLC or shared together on the same WLC.

- **Dedicated WLC for each User Group:** in this option, each of the wireless user groups will be managed on a dedicated WLC. This is common for very large wireless environments with thousands of clients. Or using a dedicated WLC for one of the user groups like Guests which may be connected into a DMZ on a firewall.
- **Shared WLC for all User Groups** (recommended): in this option, all of the wireless user groups will be managed on a the same WLC. This is common and recommended for most business size networks (small, SMB, medium, and large).

#3

WLC Deployment

When to use: using a Centralized WLAN solution

Determine how the WLC component(s) will be deployed on the network:

- **WLC connected to LAN** (recommended): the WLC component(s) would be plugged into the LAN or Data Center Core switch. This is the most common and recommended deployment approach for the WLC.
- **WLC connected to DMZ:** the WLC component(s) would be plugged into a DMZ or interface of a firewall appliance. This is sometimes used for deploying a dedicated WLC for the Guest network and connected them to a DMZ to provide policy enforcement on the firewall.

Step 1-4

Wireless Client Traffic

When to use: using a Centralized WLAN solution

Determine how wireless client traffic will be switched on the network based on the following options:

- **Local Mode:** a CAPWAP (Control and Provisioning of Wireless Access Points) connection is established between the wireless controller and each access point. The WLC will operate in local-mode. Wireless user traffic will be tunneled back to the wireless controller. This will provide a central data-point where all wireless client traffic will go to provide possible policy enforcement. Below are requirements for using this mode on the WLC:
 - o The site has more than 50 access points
 - o The site is using a two-tier LAN topology (or higher)
- **Non-Local Mode:** a CAPWAP (Control and Provisioning of Wireless Access Points) connection is established between the wireless controller and each access point. Wireless user traffic will be locally switched from its connected access switch and not tunneled back to the controller. This is the most typical mode that is used on wireless networks.

When to use: (1) using a Centralized WLAN solution and (2) have a WAN with remote sites

Determine how the wireless network will be deployed at the remote sites based on the different sections below:

#1

Access Point Management

Determine which WLC will manage the access points at a remote site based on the following options:

- **WLC at HQ/Data Center (Shared WLC):** the remote-site access points will connect to a WLC that exist at the HQ office or Data Center. This will involve enabling Cisco FlexConnect groups on the WLC. Also determine if a dedicated WLC will be used for each user group (e.g. Corp User, Guest) or shared on the same WLC (recommended). Below are requirements for using this option:
 - o The remote site is using a one-tier LAN topology
 - o The remote site is a small branch office
 - o The site has fewer than 50 access points
 - o The site has a WAN latency less than 100ms round-trip to the wireless controller
- **WLC at Remote Site (Dedicated WLC):** remote-site access points will connect to a dedicated WLC located at the same remote site office. Also determine if a dedicated WLC will be used for each user group (e.g. Corp User, Guest) or shared on the same WLC (recommended). Below are requirements for using this option:
 - o The remote site is a large branch office

#2

Wireless Client Traffic

Determine how wireless client traffic at the remote-site will be switched on the network based on the following options:

- **Local Mode:** a CAPWAP (Control and Provisioning of Wireless Access Points) connection is established between the wireless controller and each access point. The WLC will operate in local-mode. Wireless user traffic will be tunneled back to the wireless controller. This will provide a central data-point where all wireless client traffic will go to provide possible policy enforcement. Below are requirements for using this mode on the WLC (must match all conditions):
 - o Using a WLC at the Remote Site (Dedicated WLC)
 - o The remote site has more than 50 access points
 - o The remote site is using a two-tier LAN topology (or higher)
- **Non-Local Mode:** a CAPWAP (Control and Provisioning of Wireless Access Points) connection is established between the wireless controller and each access point. Wireless user traffic will be locally switched from its connected access switch and not tunneled back to the controller. Below are requirements for using this mode on the WLC:
 - o Using a WLC at the Remote Site (Dedicated WLC) or using a WLC at HQ/Data Center (Shared WLC)

One of the most critical steps for the wireless design is conducting a simple (and affordable) wireless site survey for WAP placement among other design considerations. The following should be done or considered:

1. **Number of Users:** determine the number of potential wireless users and concurrent wireless users in a particular area of the building.
2. **Pre-Planning:** consider the following before starting an on-site site survey of the building.
 - o Obtain building blueprints and determine square footage for the area you want the wireless network to cover.
 - o Determine the potential locations in the building where the Access Points can be placed based on where the cabling can be run to.
 - o Determine noise and interference components: other 802.11 devices, building material such as glass, concrete, and metal.
 - o Determine if the wireless coverage will be used internal or extended to be used outside.
 - o If applicable, use WAP Planning Tools (e.g. Aruba WLAN Planning Tool)
3. **Post-Planning (Site Survey):** this is the actual in-person site-survey and what mechanisms can be used.
 - o One option can include using a tripod and an access point that is moved to various locations within the building testing the coverage, signal, noise level, and SNR. This method is very effective and affordable.
 - o During the site survey measure the signal strength and noise level (in dBm) using tools like NetStumbler, Fluke Networks, Ekahau, or WirelessMon (www.passmark.com) which is very affordable for individuals. The cost is between \$24 to \$50.
 - o Determine Signal-to-Noise Ratio (SNR); reference under "Resources". Determine if the SNR for a wireless connection is good in various areas for possible AP placement.
4. **Access Point count:** From the site survey of the building and the information gathered in regards to the estimated number of wireless users determine the number of wireless access points (WAP) required for the network based on some of the following notes:
 - o Recommend to have between 15 - 20 users per Access Point
 - o Cisco recommends no more than 25 users per Access Point due to bandwidth and wireless overhead.
 - o For most environments 1-2 APs can cover up to 2700 sq. ft.
 - o 3 Wireless APs on an 802.11b/g network can ideally support ~180 users.
 - o A single Access Point can typically cover a 100-foot radius for best results.

Resource

Site Survey Information

Signal

- **Signal** : *measure of how much power is being transmitting*
- A GOOD WIFI signal is -70dBm or more positive
- A POOR WIFI signal is -90dBm or more negative
- Example: -20dBm is a stronger signal than -65dBm

Noise

- **Noise** : *measure of how strong the interference is on the signal*
- Caused from interference devices like neighboring 802.11 devices, metal, glass, and concrete material.
- Example: -90dBm is a better noise level than -65dBm

Signal to Noise Ratio (SNR)

- $Noise - Signal = SNR$ (e.g. $96dBm - 56dBm = SNR$ is $40dbm$)
- $> 40dB$ SNR = Excellent signal (5 bars); always associated

- 25dB to 40dB SNR = Very good signal (3 - 4 bars); always associated
- 15dB to 25dB SNR = Low signal (2 bars); always associated
- 10dB - 15dB SNR = Very low signal (1 bar); mostly associated
- 5dB to 10dB SNR = no signal; not associated

When to use: using a Centralized WLAN solution

For redundancy, multiple Wireless Controller components can be configured together to provide redundancy for the Access Points. You can also add additional access points to the environment to provide continued coverage if (1) one or more AP fails and (2) if an AP gets oversubscribed with connected users.

Below are the different redundancy options that can be implemented:

- **Stateful WLC Redundancy:** redundant WLCs are implemented to provide stateful failover for access points and wireless clients using a High Availability feature called Access Point Stateful Switchover (AP-SSO). The Primary WLC will synchronize its configuration, AP license count, and the AP database to the Secondary WLC through a dedicated redundancy port. The access points will establish a single CAPWAP tunnel to WLC that is currently active in the cluster. When a failure occurs with the primary WLC, the access points will quickly reconnect to the Secondary WLC which will become active. This redundancy model provides the fastest recovery compared to the other option listed.
- **Non-Stateful WLC Redundancy:** for WLCs that do not support AP-SSO (e.g. Cisco 2500 series), the WLC must be peered with another WLC using a mobility group. Therefore, the access points must be configured to point to the IP addresses for each of the non AP-SSO WLC.

Determine the bandwidth services that should be used for the wireless radios based on the following selections:

- **802.11g/b:** most common WIFI bandwidth service used today. If using 802.11g radios they are also backwards compatible with 802.11b radios. 802.11g can provide data rates of 54Mb/s per access point. 802.11b (legacy) can provide data rates of 11Mb/s per access point.
- **802.11n (recommended):** a WLAN bandwidth service that provides higher WIFI bandwidth throughput over 802.11g (2.4 GHz) or 802.11a (5GHz) technologies. 802.11n can provide data rates up to 300Mb/s per access point by using wider WIFI channels (40 MHz wide channels).
- **802.11a:** older WIFI technology not often used except for unique purposes and requirements. 802.11a can provide data rates of 54Mb/s per access point.
- **802.11ac** (future, final ratification set for late 2013-2014): titled "Gigabit WIFI" providing fast data rates up to 433Mbps - 1.3Gbps. To achieve these high data rates, bigger channels are used by combining two of the 40 MHz wide channels to 80 MHz and supporting only 5GHz (not 2.4GHz).

Determine the bandwidth service for the wired connections between the wireless components (WLC, Access Points) and the LAN/Data Center. This is based on the bandwidth used on the wireless component's Ethernet interface and the Wireless radio speed. Below are bandwidth services to choose from:

- **Fast Ethernet (100Mbps):** recommended if using 802.11b.
- **Gigabit Ethernet (1Gbps):** recommended if using 802.11a, 802.11g, and/or 802.11n. Also consider Port Channeling with the LAN/Data Center if additional Gigabit speeds are needed.
- **10GigabitEthernet (10Gbps):** recommended if using 802.11ac and 802.11n
- **Port Channel:** Used for bundling multiple Ethernet connections to provide additional bandwidth resources. Requires Port Channel (802.3ad).

Step 4

Security for Wireless Solution

Determine the security used (and required) on the wireless network based on the following options:

Step 4-1

Wireless Encryption

Choose one of the encryption methods for the wireless network:

- **WPA/TKIP:** Wireless encryption protocol pair that uses a pre-shared key that must be configured on all Wireless clients.
- **WPA2/AES (802.11i):** recommended wireless encryption mechanism to use for WLAN networks.

Step 4-2

Wireless Authentication

Choose one of the client authentication methods for the wireless network:

- **Open:** no additional client authentication is required by the wireless user.
- **PEAP MS-CHAPv2:** EAP authentication that forces a user to authenticate (against Active Directory using RADIUS) before gaining network access. Certificates are required only on the RADIUS server.
- **EAP-TLS:** EAP authentication that requires a certificate on both the RADIUS server and the Wireless clients increasing the overall administration, but the wireless client does not have to manually authenticate.
- **EAP-TLS and PEAP MS-CHAPv2:** The most secure wireless authentication out of the three and is the most complex to administer. This method uses certificates on the RADIUS server and the wireless clients, plus users must authenticate before gaining network access.

Note: the RADIUS/LDAP server is another component that is connected into the server farm.

Services Required: RADIUS, LDAP

Step 4-3

Basic Security

Below are additional basic security mechanisms that can be deployed with the wireless solution:

- **MAC Filtering:** specifying what wireless MAC addresses are allowed to be associated with a Wireless network. This is not often used since it can be easily exploited with common tools today.
- **Guest Portals:** provide a method where connected Guest users access a centralized portal page before gaining network access. The portal page may contain required user authentication or accepting a disclaimer defined by a security policy.
- **Firewall Filters:** firewall policies can be configured on the WLC to control what users can access on the network without needing a dedicated firewall to manage those policies.

Step 4-4**Additional Security Services and Solutions**

Determine if the additional security services/solutions are required to be deployed with the wireless network. Below are some of the security services/solutions that can be used:

- **Solution:** Identity Access Control
- **Solution:** Intrusion Prevention
- **Service:** Access Control Lists (ACLs)

Recommendations: This is common for large wireless networks or companies that follow a regulatory compliancy (PCI, SOX, HIPPA) with high security requirements.

Step 4-5**VPN across Wireless Solution**

Wireless provides a lot of robust security options, but there are unique requirements where business owners feel comfortable for the wireless solution (centralized or distributed) to be connected outside of the network behind a firewall port.

When the Wireless network is connected to the outside network this may require users to VPN (using IPSec or SSL VPN) into the network to access internal resources. This does provide an additional layer of security (integrity and confidentiality) for the Wireless network.

Services Required: Virtual Private Network (VPN)

Step 5**Network Management for Wireless Solution****Step 5-1****Wireless Location Management**

Determine if the following management services are required to be deployed with the wireless network.

- **Location:** the ability to track wireless devices by location on the wireless network.

Recommendations: This is common for larger wireless networks to better manage the wireless infrastructure. Small, SMB, including some Medium size networks will likely not use any separate Wireless Management solution like the WLSE product due to additional hardware that needs to be managed including the higher cost associated with it.

These are additional services that can be implemented (if required) within the solution.

- RADIUS
- SNMP
- **DHCP** - DHCP Option 43 is used to map the access points to the WLCs.
- VLAN
- Trunking (802.1Q)

The following hardware features are also required:

- Power over Ethernet (PoE), PoE+, or Cisco Universal PoE (UPOE)
- Quality of Service (QoS)

PoE is recommended to provide power to the access points compared to using power bricks (or adapters) causing complexity with cable management. PoE should exist within the Access layer of the LAN where the access points are connected.

When to use: using a Cisco Centralized WLAN solution

Below are some of the initial configuration elements when setting up the Cisco WLC. These should be used as a consideration for implementation of the WLC component:

- **Link Aggregation (LAG):** if you need to bundle multiple Ethernet connections between the WLC and the Core switch.
- **Virtual Interface:** used by the WLC to provide mobility DHCP relay, guest web authentication and inter-controller communication.
- **Multicast support:** tunnels all traffic between the Access Point and WLC. As a result, the WLC will issue all multicast joins on behalf of the wireless client.
- DHCP snooping
- SNMP
- Configure wireless user authentication using RADIUS
- Enable the radio resource management (RRM) Auto-RF feature

When to use: using a Centralized Wireless solution

Determine how the LWAP components in the centralized solution will discover the Wireless LAN Controller (WLC) based on the following options:

Option 1

Dynamic Host Configuration Protocol (DHCP) - Option 43

When to use: using DHCP scopes on a Cisco IOS L3-device (router, L3-switch) to map access points to a WLC(s).

DHCP Option 43 is used to map access points to a WLC. Using this option can allow remote sites and or a campus LAN to use a unique mapping. DHCP Option 43 uses a hexadecimal string comprised of "Type + Length + Value" (TLV) values.

- **Type:** This sub-option code will always be 0xf1
- **Length:** This sub-option reflects the number of Wireless LAN Controllers (WLC) that the LWAP should connect to. The number of WLC would then be multiplied by "4" for its final value.
- **Value:** this reflects the management IP address of each Wireless LAN Controller (WLC) listed in sequential order. The decimal IP address for these WLC must be converted to a hexadecimal string.

Example: let's say we have two WLCs on our network using the following management IP addresses: 172.17.203.11 and 172.17.203.12

To build out the Option 43 hexadecimal string, the TLV values would be the following:

- **Type:** 0xf1 (or f1)
- **Length:** Two WLCs x 4 = 8. In hexadecimal it would be represented as 0x08 (or 08)
- **Value:** The hexadecimal value for WLC1's management IP address "172.17.203.11" would be "ac11cb0b". The hexadecimal value for WLC2's management IP address "172.17.203.12" would be "ac11cb0c".

Next, combine the TLV hexadecimal values together into a single string: **f108ac11cb0bac11cb0c**

That hexadecimal string can be used in a Cisco IOS DHCP scope for the network that has the LWAPs connected:

```
ip dhcp pool DHCP_LWAP
option 43 hex f108ac11cb0bac11cb0c
```

When a LWAP gets an IP address from this scope it will also receive option 43. It will then know that there are two WLCs where the primary WLC is 172.17.203.11 and the secondary WLC is 172.17.203.12.

Option 2

Using a DNS record

Below are some of the main aspects and requirements for this WLC discovery option:

- **When to use:** (1) using only one WLC on the network and (2) Cisco LWAP running software version 6.0 and higher.
- Create a DNS record resolving the host name "cisco-capwap-controller" to the management IP address of the WLC.

Option 3

DHCP - Using Microsoft DHCP server

Below are some of the main aspects and requirements for this WLC discovery option:

- **When to use:** using multiple WLCs on the network
- Microsoft DHCP scope configured with vendor-specific information to the lightweight Cisco Aironet 1600, 2600, and 3600 Series Access Points

Step 6-4

Antennas

Antennas provide wireless coverage in unique areas with interference and building material such as glass or concrete. It can also provide wireless coverage across long distances if the WAP network extends outside (or inside). If the site survey and the building has any of these components consider external antennas for the WAPs in the design.

Step 6-5

Multiple SSIDs

Determine if multiple wireless networks (SSIDs) are needed and if so what type of wireless networks will be used. Below are common wireless networks that are implemented:

- **Internal (Private):** A wireless network used by internal employees to access internal network resources and the Internet.
- **Guest (Public):** A wireless network that only allows access to the Internet. Access to other networks (e.g. internal networks) is restricted.

Each wireless network (SSID) should be associated to a VLAN. And 802.1Q Trunking is used to support multiple VLANs. This is configured on the WAP switch ports, WLC switch ports, and all inter-connection ports.

Step 6-6

Subnets

A dedicated subnet should be used for each wireless network separate from the wired internal subnets for security purposes. Below are some of the WLAN subnets that can be deployed:

- **Internal (Users):** subnets used for internal access for employees and other users.
- **Guest:** subnets used for guest or public access with limited or no internal access.
- **Infrastructure:** subnet used for wireless access points and WLC communication.
- **Other:** other subnets created based on any unique requirement or preferences.

When to use: using a Cisco Centralized Wireless Solution and Products

- **Data Traffic:** recommended to use the default QoS settings on the WLC.
- **Voice Traffic:** recommended to use the Platinum QoS settings on the WLC.
- **Guest Traffic:** recommended to use Bronze (background) QoS settings on the WLC.

When to use: using a Guest user group on the wireless network

Below are some of the additional configuration aspects that are included with the guest wireless network:

- **Web Authentication:** before a guest user can access the Internet, they should login through a splash page or accept the terms for accessing this guest network. This includes presenting Internet plans that the guest user can purchase.
- **Temporary Guest Accounts:** In most environments, guest accounts should be created by the first person (lobby administrator) who will interact with the guest users.
- **Guest network access:** determine what level of access is needed. In most environments, guest users can only access the Internet including the internal DHCP and DNS servers. They are denied access to corporate internal resources.

Below are additional services that can be enabled on the wireless controller:

- **Port Channeling (LAG):** if there will be a high number of 802.11a/n connections among all the access points it's recommended to configure a Link Aggregation Group (LAG) to bundle multiple GE connections between the switch and the controller to accommodate the high throughput needed. **Services Required:** Port Channel (802.3ad).
- **FlexConnect:** used to locally switch wireless packets at remote sites. This should be used if Lightweight access points are deployed at the remote site connecting to a controller located at the HQ site. If FlexConnect is not enabled for the remote site WAPs, then traffic could be routed back to the HQ site then to the remote site even for simple local traffic within that site. Furthermore, with a remote site WAP enabled for FlexConnect, if the WAN is down and/or cannot communicate with the Wireless LAN Controller it will act as a standalone WAP.
- **Cisco CleanAir:** a Cisco wireless tool built into an access point. It monitors radio interference acting as a built-in spectrum analyzer to provide self-healing and self-optimization on the wireless network. It doesn't eliminate wireless interference nor pollution in the air, but it allows the access point to dynamically adjust its signal to avoid it. Cisco CleanAir also provides performance protection for 802.11n networks.

Step 7	Hardware for Wireless Solution

Next we need to determine the hardware model that will be used for each component for the solution. This selection can be determined using some of the following ways:

- **Hardware Consolidation Option:** the components in the solution could be consolidated with other components determined in other solutions. This could be considered as one design option that could be applicable to the environment.
- **Hardware Options:** use the hardware matrix table(s) provided for selecting the potential hardware for the components in the topology based on the technical objectives, services, and features it will use. Keep in mind that new hardware models are released all the time by all hardware vendors, so not all products will be listed here and may be out-of-date in some cases. You can also reference other product guides if it still supports everything the component will provide to the solution.

#1	Hardware Consolidation Option

Some of the Wireless components can be consolidated within other components in the design using one of the following options:

- The **Wireless Controller** component can be consolidated within the **LAN Core (or Distribution)** using either a Cisco Catalyst switch with the WLC integrated or the Wireless Service Module (WiSM) for the Cisco Catalyst 6500/6800 Series.
- The **Wireless Controller** component can be consolidated on the **WAN Router (Hub, Spoke)** using a WLC module/card installed.
- The **Wireless Controller** component can be consolidated on the **Edge Router (Internet Edge)** using a WLC module/card installed.
- One of the **Wireless Access Points** can be consolidated on the **WAN Router (Hub, Spoke)** or **Edge Router (Internet Edge)** using a Wireless AP module/card installed.

Note: Reference the "Hardware Table" for any specific hardware that may be listed for consolidation.

Select the hardware for each component in the solution using the tables below referenced with important details of supported services, bandwidth, interfaces, and more.

Virtual Cisco Wireless LAN Controller (vWLC) *(Small, SMB, Medium)*

Performance	500Mbps	Flexibility	--
Reliability	--	Management	--
Scalability	5-200 Access Points 3000 wireless clients 512 WLANs	Security	ACL, Rate Limiting, DTLS
Design Aspects	QoS, Guest Services, Cisco FlexConnect group support		
Models	Virtualized (VMware)		

Cisco 2500 Wireless LAN Controller *(Small, SMB)*

Performance	1Gbps GE support	Flexibility	--
Reliability	--	Management	--
Scalability	5-75 Access Points 500 wireless clients 16 WLANs	Security	ACL, Rate Limiting, AVC, DTLS
Design Aspects	QoS, Guest Services, LAG, Local-mode support		
Models	Appliance		

Cisco 5500 Wireless LAN Controller *(Medium, Large)*

Performance	8Gbps GE support	Flexibility	--
Reliability	AP-SSO support	Management	--
Scalability	12-500 Access Points 5000 wireless clients 512 WLANs	Security	ACL, Rate Limiting, AVC, DTLS
Design Aspects	QoS, Guest Services, LAG, Local-mode support,		
Models	Appliance		

Cisco 5760 Wireless LAN Controller *(Medium, Large)*

Performance	60Gbps GE, 10GE support	Flexibility	--
Reliability	--	Management	--
Scalability	25-1000 Access Points 7000 wireless clients 512 WLANs	Security	ACL, AVC, DTLS
Design Aspects	QoS, Guest Services, LAG		
Models	Appliance		

Cisco Flex 7500 Cloud Controller *(Large)*

Performance	1Gbps 10GE support	Flexibility	--
Reliability	AP-SSO support	Management	--
Scalability	300-6000 Access Points 64,000 wireless clients 512 WLANs	Security	ACL, Rate Limiting, AVC, DTLS
Design Aspects	QoS, Guest Services, LAG, Cisco FlexConnect group support		
Models	Appliance		

Cisco 8500 *(Large, Service Provider)*

Performance	10Gbps 10GE support	Flexibility	--
Reliability	--	Management	--
Scalability	300-6000 Access Points 64,000 wireless clients 512 WLANs	Security	ACL, Rate Limiting, AVC, DTLS
Design Aspects	QoS, Guest Services, LAG		
Models	Appliance		

Cisco Catalyst 6500/6800 – Service Module: WiSM2 *(Medium, Large)*

Performance	20Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	100-1000 Access Points 15,000 wireless clients 512 WLANs	Security	ACL, Rate Limiting, AVC, DTLS
Design Aspects	QoS, Guest Services		
Models	Service Module for Cisco Catalyst 6500/6800 series		

Cisco ISR G2 – WLC Module *(Small, SMB)*

Performance	500Mbps	Flexibility	--
Reliability	--	Management	--
Scalability	5-200 Access Points 500 wireless clients 512 WLANs	Security	ACL, Rate Limiting, DTLS
Design Aspects	QoS, Guest Services		
Models	Module for Cisco ISR G2 series		

Cisco Catalyst 3650 – WLC Module *(Small, SMB)*

Performance	20 – 40Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	1-25 Access Points 1000 wireless clients 64 WLANs	Security	ACL, AVC, DTLS
Design Aspects	QoS, Guest Services, LAG		
Models	Cisco Catalyst 3650 with WLC		

Cisco Catalyst 3850 – WLC Module *(Small, SMB, Medium, Large)*

Performance	20 – 40Gbps	Flexibility	--
Reliability	--	Management	--
Scalability	1-50 Access Points 2000 wireless clients 64 WLANs	Security	ACL, AVC, DTLS
Design Aspects	QoS, Guest Services, LAG		
Models	Cisco Catalyst 3850 with WLC		

b

Wireless Access Points

Cisco Aironet 3700 *(Medium, Large)*

Performance	1.3Gbps 802.11a/b/g/n/ac support	Flexibility	--
Reliability	--	Management	--
Scalability	200 clients per AP MIMO: 4x4:3	Security	wIPS, Rogue AP Detection
Design Aspects	CleanAir, Office Extend, Band Select		
Models	Indoor, Dual Radios (2.4Ghz and 5Ghz)		

Cisco Aironet 3600 *(Medium, Large)*

Performance	1.3Gbps 802.11a/b/g/n/ac support	Flexibility	--
Reliability	--	Management	--
Scalability	50-200 clients per AP MIMO: 4x4:3, 3x3:3	Security	wIPS, Rogue AP Detection
Design Aspects	CleanAir, Office Extend, Band Select		
Models	Indoor, Dual/Triple Radios (2.4Ghz and 5Ghz)		

Cisco Aironet 2600 *(Small, SMB, Medium, Large)*

Performance	450Mbps 802.11a/b/g/n support	Flexibility	--
Reliability	--	Management	--
Scalability	200 clients per AP MIMO: 3x4:3	Security	wIPS, Rogue AP Detection
Design Aspects	CleanAir, Office Extend, Band Select		
Models	Indoor, Dual Radios (2.4Ghz and 5Ghz)		

Cisco Aironet 1600 *(Small, SMB, Medium)*

Performance	300Mbps 802.11a/b/g/n support	Flexibility	--
Reliability	--	Management	--
Scalability	128 clients per AP MIMO: 3x3:2	Security	wIPS, Rogue AP Detection
Design Aspects	CleanAir, Office Extend, Band Select		
Models	Indoor, Dual Radios (2.4Ghz and 5Ghz)		

Cisco Aironet 600 (Small)

Performance	300Mbps 802.11a/b/g/n support	Flexibility	--
Reliability	--	Management	--
Scalability	15 clients per AP MIMO: 2x3:2	Security	--
Design Aspects	Office Extend		
Models	Indoor, Dual Radios (2.4Ghz and 5Ghz)		

c

Wireless Management

- Cisco Prime Infrastructure (CPI)

Resources

Hardware Checklist

- WIFI Standards
- RF Band(s) (Single, Dual-Band)
- Dual-Band (Selective or Concurrent)
- MIMO Support
- Maximum Number of Active Wireless Clients
- Number of SSIDs supported
- Ethernet ports
- Guest Portal capabilities
- Maximum Number of APs supported in a cluster (if supported)

8 Services

Complete the design for each service that was gathered from the requirements and the solution design phase.

All of the services are listed in alphabetical order and will include the prerequisites before completing the design steps for that service. For example, if you want to implement VLANs into the network design:

Category: Routing and Switching
Prerequisite(s): VTP (under Services)

It requires completing the VTP service design first. This is important to ensure that all other critical components are already designed and in place. In other words, you can't put furniture into a house that isn't built yet.

For each service that will be used, complete each step listed for the service design writing down any relevant details that may be used in other steps including its configuration. If there is a step that does not apply then continue on until all steps are completed. For each step you will see colored boxes on the upper right side reflecting what technical objectives the step is focused on. The table below will show the color and the symbol it will reference:

Scalability (SC)	Reliability (R)	Performance (P)	Security (SEC)
Management (NM)	Flexibility (F)	Hardware (H)	Design Aspects (DA)



~ Services ~

Access Control Lists (ACL)

Category: Network Service (Security)
Prerequisite(s): --

SEC

Firewall Services are used to filter network traffic based on IP addresses, ports, or content with low performance requirements. A firewall solution can be consolidated using software (IOS) within a router platform. Below are the firewall services that can be used with a router (or some L3-switches).

- **Reflexive ACL (rACL):** provide stateful firewall capabilities on a Cisco IOS device.
- **Context Based Access Control (CBAC):** provide stateful firewall capabilities using inspection functionality on a Cisco IOS device.
- **Zone Based Policy Firewall (ZFW):** firewall feature that creates a stateful firewall by creating zones on the interfaces of a router. This is considered as a next generation firewall service for Cisco IOS Firewalls.
- **Standard or Extended ACL:** basic security policies (limited stateful behavior) configured either inbound and/or outbound on an interface. It's recommended to use either rACL, CBAC, or ZFW.

Recommendations: ZFW is next generation and creating zones is recommended, however, the administration of policies is higher compared to rACL or CBAC. However, ZFW does provide other integrated functionality not available with CBAC or rACL such as rate limiting certain firewall policies to use a certain amount of bandwidth. For example we can rate limit all HTTP traffic out to the Internet to use 1Mbps. CBAC and rACL are two good solutions that provide stateful firewall capabilities with easier administration. From the two, I would recommend rACL for a software-based stateful firewall on a router. I encountered some low throughput and HTTP related issues when using CBAC as a stateful firewall, which was easily fixed when using rACL.

B

~ Services ~

BGP

Category: Network Service (Routing and Switching)
Prerequisite(s): Routing, IP (under Services)



Complete the steps below if BGP is selected as the EGP routing protocol for the design:

#1	Infrastructure Design

Build the BGP network, its peers, and the networks that will be advertised and received. These are considered as critical components for the BGP design at a high-level.

- **ASN:** determine the Autonomous System Network (ASN) the router will belong to. This ASN is obtained through ARIN among other IP requirements. A private ASN can be used internally if BGP is configured with a provider that will translate it to a Public ASN. This seems to be a rare case, but is possible based on unique requirements.
- **Peer (IBGP, EBGP):** determine what BGP routers will be connected peers. If the router will peer with other BGP routers located in the same ASN then that neighbor would be seen as an IBGP peer. If the BGP router will peer with another router in a different ASN, that would be an EBGP peer. Draw out and determine the peer type between all BGP routers in the design.
- **Routes Advertised (Networks):** determine what subnets will be advertised from your ASN.
- **Routes Received (Full, Partial, Default):** determine what routes should be received from the ISP or EBGP peer. The ISP can either send the entire routing table (requires high-end router hardware with a lot of memory), a partial routing table, or just a BGP default route. A BGP default route is recommended for most small, SMB, and medium BGP networks. This is more common with BGP deployments and doesn't require high-end router hardware. Large network or hosting/cloud provider networks will typically obtain full routing tables for better control of routing to certain networks.

#2	iBGP Peering

Used when peering with other BGP routers located in the same ASN. This is usually the second BGP router that is added to the network connected to the same (or different) ISP for redundancy purposes. Routers within the same ASN can be configured together using one of the following ways:

- **Standard:** a BGP neighbor is configured to each IBGP router on the network. Common for Internet edge routers peering with an ISP(s) and with the other redundant edge router.
- **Route Reflectors:** eliminates the need for configuring a BGP neighbor to each IBGP router on the network. A BGP router would simply peer with one BGP router that would act as the route reflector.
- **Confederations:** eliminates the need for configuring a BGP neighbor to each IBGP router on the network. In this option the BGP routers are configured in groups and ideal for larger networks using BGP routers within the same ASN.

#3

eBGP Peering

Used when peering with other BGP routers in a different ASN. This is usually the ISP's BGP router.

- **EBGP Multi-hop:** by default EBGP peers must be directly connected (TTL of 1) for configuration. If the EBGP peer is not directly connected then this option must be enabled on the neighbor interface reflecting the number of hops away the EBGP peer is located (up to 255 hops).

#4

Route Summarization

To summarize multiple routes as a single route. This is recommended when advertising many subnets within a customer's ASN. The routes can be summarized as a single route to other BGP neighbors for creating smaller routing tables hence less CPU and memory processing.

#5

MD5 Authentication

Configures a password with the connected BGP peer for establishing a neighbor to exchange routing information. This is recommended to prevent against peering with rogue BGP devices.

#6

Synchronization

By default, routes on a BGP router that are not learned via an IGP routing protocol will not be injected into the BGP routing table.

Recommendations: the key thing to understand is that BGP will only inject routes into its routing table then out to other BGP peers (IBGP or EBGP) if it has a match in the global routing table. For example, if you add a new network under the BGP routing process such as 10.10.0.0 /16, an actual route must exist for that entry even if one of the actual routes is 10.10.100.0 /24. We would need to add a static route configured for 10.10.0.0 /16 pointing to a NULL interface. This route will match the configured network statement under the routing process which will then be injected into the BGP routing table and advertised to its peers.

#7

Soft Reconfiguration

Allows graceful BGP neighbor restarts when changes occurs.

Recommendations: this is recommended to be enabled for all BGP peers to eliminate the need to reset a BGP neighbor and the routing table in a production environment.

#8

Timers

Tune BGP neighbor timers for increased convergence in the event of a neighbor failure.

- Use the following values with the configuration: 15 seconds and 45 seconds.

#9

iBGP: Using Route Reflectors

iBGP routers that learn about routes from a connected iBGP peer will not advertise those learned to other iBGP peers. Therefore, full-mesh peering is required for all iBGP routers on the network. Using a Route Reflector can help to prevent the need for full-mesh iBGP peering in an ASN.

- **Server:** one BGP router on the network is the Route Reflector Server which is usually a Core or Distribution/Aggregation device.
- **Client:** all other iBGP routers on the network would peer with the Route Reflector server.

#10

Conditional Advertisement

A BGP feature where it will only advertise its configured subnets through another provider (EBGP peer) if certain routes (configurable) does not exist in the BGP routing table. Services required would be Policy Base Routing (PBR) and ACL

#11

Fast Failover

A feature used to help improve BGP convergence over a point-to-point connection compared to the default BGP timers. Uses BGP Selective Address Tracking and Fast External Neighbor Loss Detection to provide Fast Failover functionality.

#12

Attribute using Weight

BGP attribute that is only relevant to the local router itself. Helps to determine which BGP peer to use for outbound access (out to the Internet).

Recommendations: this is recommended when peering with 2+ service providers (or EBGP peers) from the same physical router. The neighbor with the highest weight defined is preferred for outbound access.

#13

Attribute using Local Preference

BGP attribute that is only relevant for BGP routers in the same ASN. Helps to determine which BGP router in the ASN to use for outbound access (out to the Internet).

Recommendations: this is used when routers within the same ASN need to determine which router to use for outbound routing between multiple ISPs. The BGP router with the highest local preference defined is preferred for outbound access.

#14

Attribute using Metrics (MED)

BGP attribute advertised to eBGP neighbor(s) for dictating inbound access into an ASN (e.g. client/company network).

Recommendations: this is recommended when using 2+ connections with the same service provider (EBGP peers) to provide a primary and secondary relationship. Lower the MED value configured on the client/company BGP router towards the ISP, the more preferred path (primary) it will take.

#15

Attribute using AS Prepending (AS Padding)

BGP attribute advertised to eBGP neighbor(s) for dictating inbound access into an ASN (e.g. client/company network).

Recommendations: this is recommended when using 2+ connections with different service providers (EBGP peers) to provide a primary and secondary relationship. Lower the AS Path from the Internet into the client/company ASN, the more preferred path (primary) it will take.

#16

Route Control/Filtering

Controls what routes are advertised and received from other EBGP and IBGP peers.

- **Prefix List or ACL:** configure ACL or prefix list with what routes should be received or advertised (using permit) or not (using deny) on the BGP ASN.
- **Distribute List:** the ACL of allowed/restricted routes are associated to a distribute list configured with the BGP peer. This is an alternative to using Prefix lists for route control.
- **Direction (Inbound, Outbound):** to restrict what routes are injected into the BGP ASN. Use “inbound” with the distribute or prefix list. To restrict what routes are advertised to other BGP ASNs use “outbound” with the distribute or prefix list. This is applied to the BGP neighbor.

Recommendations: this is strongly recommended to provide better control of what routes are sent and received into the ASN. This can prevent rogue BGP routes potentially bringing down the entire network. Configure BGP policies for what should be advertised and received.

BPDU

Category: Network Service (Routing and Switching)
Prerequisite(s): Spanning Tree Protocol (under Services)

1

BPDU Guard

Used on host or server ports to prevent unauthorized (rogue) switches being plugged into the network. By default any L2 switch plugged into the network will broadcast BPDU messages because it's assuming it is the root bridge. If a switch port enabled for BPDUGuard receives any BPDU messages it will disable the port. This is recommended to prevent possible global switching failures and should be enabled globally on all Access Switches.

2

BPDU Filter

This is an alternative to apply to an edge port instead of BPDU guard which deals with filtering inbound and outbound BPDU messages. This feature is good for applying to known host edge ports or switches you don't want to include as part of your L2 domain. However, BPDU Filter isn't good against stopping potential Layer 2 loops where BPDUGuard can shutdown any enabled port that receives a BPDU message to prevent a global meltdown from occurring on the network.

Bridge Assurance (BA)

Category: Network Service (Routing and Switching)
Prerequisite(s): Spanning Tree Protocol (under Services)

DA R

Bridge Assurance (BA) deals with what ports should send BPDU messages when STP PortFast is configured. Determine the PortFast port type for each switch port on the network based on the following options:

- **Edge:** enabled for all edge ports (e.g. desktop, server) where BPDU messages are not sent.
- **Network:** enabled for switch uplink and downlink ports where BPDU messages are sent.

Recommendations: again the edge ports should be enabled for “PortFast Edge” and uplink/downlink ports should be enabled for “PortFast Network”. However, as a best practice it is recommended to set the global default to “Network” which helps to avoid unidirectional links and potential software issues. Only configure BA on an interface if it is supported on the other connected device. These recommendations also apply when using Cisco Nexus hardware.

Broadcast Suppression

Category: Network Service: Routing and Switching
Prerequisite(s): LAN and/or Data Center (under Solutions)

DA R

To avoid the spread of a broadcast storm it is important to control the amount of broadcast traffic across the L2 network. Broadcast suppression should be implemented based on the following considerations:

- **Downlink port:** (1) broadcast suppression should be configured on the downlink port towards the LAN Access switch since a broadcast storm is more likely to be caused by an end user creating a loop. (2) Or apply storm control on STP blocked ports in the topology. Between the two, #1 would be recommended since the block port could likely be on the Access switch's uplink port.
- **Percentage:** for most networks (small, SMB, medium, and large) you can start with **20%** and adjust (up or down) as needed.

A large, white, serif capital letter 'C' is centered within a dark gray rectangular box. The letter is slightly stylized with a small gap at the top and bottom.

~ Services ~

CEF, IP

Category: Network Service (Routing and Switching)
Prerequisite(s): Routing, IP (under Services)

P

Enable IP CEF for hardware forwarding and load sharing for the following:

- **Core, Distribution/Aggregation:** enable full IP CEF load sharing using L3/L4 hash algorithm to prevent CEF polarization. This uses the command “ip cef load-sharing full”. CEF polarization occurs when redundant paths are ignored for traffic forwarding. CEF will be able to load balance up to 8 parallel paths. Provides **ECMP** where a maximum of 8 paths is used by CEF when using a L3+L4 hash.
- **CEF Forwarding options:**
 - o **Per-Packet:** use CEF per-packet load balancing across parallel connections terminated to the same router or point-to-point connection on the other end. Not recommended to be used between multiple service providers, which can result in out-of-order packets resulting in a high count of TCP retransmissions. Used with router devices and not L2/L3-switches.
 - o **Per-Destination:** use CEF per-destination load balancing when using multiple service providers and/or different terminating routers for load balancing services. Used with router devices and not L2/L3 switches.

D

~ Services ~

DFC

Category: Hardware

Prerequisite(s): Cisco Catalyst 6500/6800 (Hardware)

P

DFC: utilize DFC daughter-cards with Cisco Catalyst 6500 series hardware for increased performance and low latency ideal for Data Center and HPC networks.

DHCP

Category: User Service

Prerequisite(s): LAN and/or Data Center (under Solutions)

DA SC

DHCP is a protocol used to dynamically assign an IP Address and additional info for a DHCP-enabled device. The DHCP server can be configured on one of the following devices:

- **Server:** this is the recommended choice for deploying DHCP services. However, this is common for medium and large networks or if there are multiple networks/subnet that will hand out IP addresses dynamically.
- **Layer 3 Device:** DHCP services can be enabled on L3 devices like a Router, L3-switch, or Firewall. This is common for small and SMB sized networks. This avoids setting up an individual server to handle DHCP for a small set of subnets.

On the DHCP server a scope is configured for each subnet that will need DHCP capabilities. Below are some of the details handed to an IP host enabled for DHCP.

- **IP Address:** the range of IP addresses that can be assigned to a host on the network which includes the subnet mask and the default gateway. The default gateway would be the device and interface where that subnet is configured (or routed) at.
- **Lease:** specify the length of time an IP address will be assigned dynamically to a host (based on its MAC address).
- **Options:** specific DHCP options that may be required with the DHCP scope for objects like IP Phones or Access points to a centralized server for registration. For example, option 150 is used by most phone systems for IP Phones to know the location of the TFTP server.
- **IP Helper:** if the DHCP server is located on a different network from where the hosts are located then an IP helper is required on the routed interface with the connected DHCP-enabled devices. IP helper will forward DHCP broadcast requests to the dedicated DHCP server.
- **VRF-Aware:** DHCP services are not VRF-aware.

DHCP Snooping

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)

A DHCP security feature that blocks DHCP replies on a untrusted interface. This is used to prevent rogue DHCP servers from being plugged into the network that is not trusted which can cause DHCP starvation attacks. Any server trying to hand out IP addresses those requests will be blocked. This feature tracks the MAC addresses, IP addresses, lease time, to the VLAN id and stores that information in a DHCP binding table.

Below are the design points for implementing DHCP snooping:

- DHCP snooping should be enabled on the LAN Access where DHCP services should not exist.
- Make sure to mark all uplink/downlink switch ports on the Access switch to be “trusted”.
- DHCP snooping inspection should also be rate limited to “100” to protect the control plane and the switch itself.

Example: in this topology, DHCP snooping is enabled globally on the Access switch and port Gi0/1, uplink to the Core switch, would be a “trusted” port.



DMVPN

Category: Network Service (Security)
Prerequisite(s): VPN & Remote Access (under Solutions)



When to use: using a full-mesh topology in an Internet or L3 WAN where any site can communicate with each for accessing resources securely.

Description: This is a dynamic VPN technology supported on Cisco routers that creates a permanent secure tunnel with the hub router and dynamically builds temporary VPN tunnels between other sites when needed. This allows support for VRF, MPLS, dynamic routing, and some support for multicast and QoS. Using DMVPN allows minimal administration of VPN tunnels. Requires Cisco IOS router hardware and not supported on firewall platforms.

Hardware Required: Cisco Routers

Step 1	Topology/Deployment

#1	Components

For all devices within the WAN topology determine the DMVPN components that will be used:

- **DMVPN Hub:** this is usually the main office/location (WAN Aggregation) where the remote sites will connect to for accessing network resources like email or application services.
- **DMVPN Spoke:** these are usually the WAN spokes that need a permanent connection to the main office (DMVPN Hub) and some connectivity needed between other sites.

#2	Tier for DMVPN Hub

Determine the tier level for the DMVPN hub router for the VPN and DMVPN/GRE services that is used:

- **Single:** the WAN Aggregation router has VPN and DMVPN/GRE services consolidated on the same router. This tier is recommended from the two, but will require robust routers to support many DMVPN spokes connecting into the DMVPN Hub. Using this tier will simplify the configuration and provisioning of new branch routers. For the configuration use mGRE and tunnel protection for the Hub component. The configuration for the spoke component to the Hub will be point-to-point GRE interface with tunnel protection enabled. For spoke-to-spoke configuration use mGRE.
- **Dual:** The WAN Aggregation router is broken out into two routers, one dedicated for VPN services and another dedicated for DMVPN/GRE services. Using this tier will reduce the amount of IPSec configuration required. For this configuration you will need to use dynamic crypto maps.

DMVPN uses multipoint generic routing encapsulation (mGRE) tunnels to connect the hub to all of the spoke routers. These mGRE tunnels are sometimes referred to as DMVPN clouds. Determine if a single DMVPN cloud or a dual DMVPN cloud if redundancy with two DMVPN hub routers are used:

Single:

- **When to use:** using WAN cloud design #1a, 2ii, or 5ii
- **Description:** one DMVPN cloud is used for each WAN Aggregation router (used for redundancy). In this design option two headend routers connect into the same DMVPN cloud using the same IP subnet. The one advantage to this cloud topology is that only one tunnel interface needs be configured on the DMVPN spoke router connecting to both of the DMVPN hub routers. If you are using redundant Internet WAN clouds and WAN routers, then this cloud option is not recommended. This can cause redundancy issues if one DMVPN hub router fails creating possible asynchronous routing issues.

Dual:

- **When to use:** using WAN cloud design #4
- **Description:** two DMVPN clouds are used connecting to each of the WAN/DMVPN Aggregation routers. This cloud option is recommended for providing the best redundancy for DMVPN that rely on routing protocols inside of the VPN tunnels. The two headend routers would connect into one of the DMVPN clouds that will use its own IP subnet. The one downside is that the DMVPN spokes will need to use tunnel interfaces configured to each of the DMVPN hub routers.

It's recommended to use EIGRP instead of OSPF for dynamic routing over DMVPN. If deploying OSPF over DMVPN consider the following:

- A single area should not contain more than 50 routers.
- An OSPF router should have no more than 3 areas attached.
- The DMVPN Hub (WAN Aggregation) is configured as the OSPF DR. The WAN Branch routers should be configured using a priority of "0".
- OSPF Stub or Totally Stub areas are recommended for the WAN Branch offices.
- Confirm and match the MTU size for the WAN Aggregation (Hub) and WAN Branch (Spokes).
- Can support up to 500 OSPF, LDP, NHRP, IPSec, and MP-BGP sessions.

Below are best practices for using DMVPN on the network.

- Use Dead Peer Detection (DPD)
- Use Path MTU Discovery (PMTU) to keep IPSec fragmentation to a minimum.
- Use Digital Certs (PKI) for better scalability if possible.
- If using 254 spokes for the DMVPN use a /24 subnet for the DMVPN cloud. If there are 400 spokes use a /22 subnet.

- For WAN Branch routers (DMVPN Spoke) setup IKE CAC to avoid overloading the Spoke router. IKE CAC will limit the number of ISAKMP SAs to 25 (lower or higher as needed). Configure the System CAC to limit the number of SAs on the system to be 80% (lower or higher as needed).
- DMVPN can support up to 350-500 EIGRP peers when using the Cisco 7200 (NPE-GE, VAM2) and higher for possible increased number of peers, but carefully monitor the CPU and resources on the router.
- **MTU**: the safest and recommended MTU to use for GRE interfaces to avoid fragmentation is 1400 bytes. Or use 1392 bytes (for unicast) or 1368 bytes (for multicast) depending what is applicable if using MPLS over DMVPN.

Step 4	Topology/Deployment Add-Ons

Below are other common technologies that can be implemented or overlay with DMVPN:

Technology	Description	Prerequisite(s)
DMVPN per VRF	Used to extend a VRF (not configured in a MPLS solution) across a DMVPN network using VRF-lite (Multi-VRF CE).	Virtualization (Network) [Solution]
MPLS over DMVPN	Used to connect two MPLS networks together across the Internet over DMVPN.	--
GET VPN over DMVPN	DMVPN is deployed as the framework between all sites without encryption. GET VPN is built on-top of the DMVPN topology providing tunnel-less encryption between sites.	--

DNS

Category: User Service

Prerequisite(s): LAN and/or Data Center (under Solutions)

DA

DNS is a protocol used for translating a domain name (e.g. routehub.net) to an IP address. This is required in order for hosts on the network to access the Internet. Below are design details for deploying DNS services on the network.

- **DNS:** a DNS server that is usually deployed internally to access internal resources. The internal DNS server is configured to use an external DNS server as a DNS forwarders. Therefore users on the internal network who want to access the Internet their DNS request would be sent to the external DNS servers based on the DNS forwarders configured. This is a common DNS deployment for Small, SMB, and Medium sized networks. For large networks, two DNS servers (or more) may be deployed. There could be an internal DNS server used for internal access and resolution. Then there is an external DNS server used (managed by the company) placed in the DMZ for external resolution. The internal DNS server can use the external DNS server in the DMZ as a DNS forwarder if needed.
- **DDNS (Dynamic DNS):** A dynamic DNS service where a host (or router) configured for DDNS would connect periodically to a DDNS provider to register its IP address. This is common for networks that use a dynamic IP (via DHCP or PPPoE), but have public facing servers (e.g. Web server) that need to be accessed by clients. DDNS can help to update the new IP with the DNS record automatically.

Dynamic ARP Inspection

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN and/or Data Center (under Solutions), DHCP Snooping (under Services)

Dynamic ARP Inspection (DAI) prevents against ARP spoofing, poisoning, and starvation on the network. ARP poisoning happens when the attacker sends false ARP information to a local segment affecting the ARP cache on the LAN. This allows the attacker to perform man-in-the-middle attacks with the devices on the segment.

DAI uses data that is generated by the DHCP snooping service to intercept and validate the IP-to-MAC address relationship of all ARP packets on all untrusted interfaces. If invalid ARP packets are received on a untrusted interface they will be discarded.

Below are the design points for implementing Dynamic ARP Inspection (DAI):

- This feature should be configured on all Access Switches.
- DAI should also be rate limited to "100" to protect the control plane and the switch itself.
- Make sure to mark all uplink/downlink switch ports on the Access switch to be "trusted".

E

~ Services ~

Easy Virtual Network (EVN)

Category: Network Service (Tunneling)
Prerequisite(s): Network Virtualization (under Solutions)

When to use: used for creating up to 32 virtual networks (per platform) on the LAN/Data Center topology.

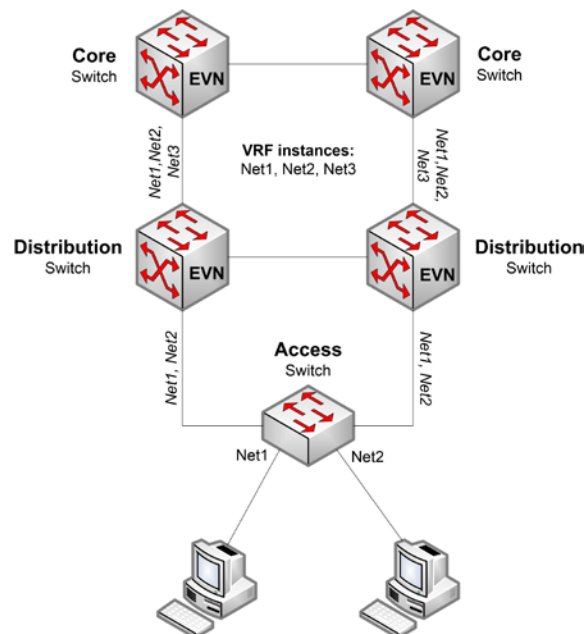
Description: Easy Virtual Network (EVN) combines VRF-lite and MPLS VPN into a single virtualization feature that can be implemented on next-generation networks. EVN virtualizes a control plane and data plane for each VRF instance per platform allowing a hop-by-hop (or multi-hop) data path through the network. Each EVN enabled device has two types of routing tables. There is a global routing table (also called the VNET global table) which contains all routes not learned from a VRF instance and there is a VRF routing table which contains routes/interfaces within a VRF instance.

Build the EVN design based on the following design steps:

Step 1

Topology Design

EVN should be enabled on each L3 device within the LAN or Data Center topology that will support transporting a single VRF domain across the network.



Step 2	Configuration

#1	General Configuration

Go through each sub-step below for configuring the service on the topology:

1. **VRF Definition:** define all of the VRF instances for each virtual network that will be used on the network. Each VRF should be configured on each EVN enabled device globally in the topology.
2. **Assign VRF to Interfaces:** assign the VRF to all of the necessary Layer 3 interfaces that will be part of a particular virtual network.
3. **VNET trunk:** enable VNET trunk on all uplink/downlink ports in the topology to support extending the virtual network (VRF) across the network. This will automatically create sub-interfaces for each VRF instance that is added to a EVN enabled device. The sub-interfaces cannot be created manually. Each sub-interface inherits the same characteristics from the main interface that is configured.
4. **Routing Protocol:** for each VRF instance it should be configured with a routing protocol supporting VRF.
 - a. **Services Required:** Routing, IP

#2	Security Configuration

Determine which security related configuration with the service should be included (recommended):

1. **VNET List:** implement VNET trunk security to specify what VRFs are allowed across an interface which works similar to 802.1Q trunk security. VNET trunk security must be configured equally between the connected devices.

#3	Additional Configuration

Determine what other additional configuration with the service should be included (optional):

1. **Route Replication:** Sharing routes from other VRFs using EVN is possible using the option called "Route Replication" which deals with specifying what routes within one VRF can be redistributed into another VRF instance. This does not require route targets, imports, nor exports under the VRF definition

Step 3	Best Practices & Considerations

1. 32 virtual networks are supported per platform.
2. EVN is backward compatible with VRF-Lite. However, the 802.1Q tag (used on the VRF-lite enabled device) and the VNET tag (used on the EVN enabled device) must match between the connected devices.
3. Flexible NetFlow (FnF) not supported on a VNET trunk enabled interface.
4. If the VNET tag ID will change which will affect how the sub-interface is configured, its recommended to remove the old VNET tag then configure the new desired VNET tag.
5. When creating a VRF name do not use the name "global"

EIGRP

Category: Network Service (Routing and Switching)
Prerequisite(s): Routing, IP (under Services)



Complete the steps below if EIGRP is selected as the IGP (internal) routing protocol for the design:

#1

Determine the infrastructure design

Build the EIGRP framework on the network infrastructure.

- **ASN:** determine the Autonomous System Network (ASN) that all EIGRP routers will belong to for exchanging route information. If an EIGRP router is not in the same ASN with other EIGRP routers it will not be able to participate in forming a neighbor or exchanging routes.
- **Networks:** determine the networks configured on each L3 device that should be advertised to other EIGRP routers.

Recommendations: all networks configured on the interfaces (physical or SVI interfaces) are essentially added as networks under the EIGRP routing process. Also make sure that all EIGRP routers exist in the same ASN.

#2

Equal Cost Path (ECP)

Provide fast convergence and load balancing of traffic through the network. This is accomplished by creating multiple paths through the network using the same metric values, which will inject two paths for a destination into the global routing table. To accomplish this the following must be implemented with the design.

- Create multiple interconnections on the LAN and Data Center switches based on the topology.
- **EIGRP Delay:** Configure the EIGRP delay (and bandwidth) with the same value for all L3 interfaces to create ECP on the network when there are multiple paths.

#3

Fast Convergence

If a failure occurs anywhere on the network it's important to tune EIGRP to quickly react to the failure by transparently re-routing traffic across a different path in sub-second numbers. Below are some of the methods that can provide fast convergence with EIGRP.

- **Equal Cost Path (ECP):** see ECP for more details.
- **IP CEF:** see "Step 6" for details on IP CEF.
- **Route Summarization**

- Enable **Bidirectional Forwarding Decision (BFD)**
- **Hello/Hold Timers:** tune timers for the neighbor interfaces to provide fast convergence when there is a failure. The hold timer is important to trigger a convergence when a failure occurs with an established neighbor. Below are recommended timer values that can be used for the configuration.
 - o **Small/Medium/Large:** Hello (1 second), Hold (3 seconds).
 - o Other timer values that can be used: Hello (2 seconds), Hold (8 seconds)

Cisco Nexus Best Practices: recommended to use the default IGP timers in a dual-supervisor Nexus system to avoid any unnecessary convergence.

#4	Summarization

Summarize multiple routes as a single route to create smaller routing tables (resulting in less memory, bandwidth, & processing requirements) and prevent EIGRP queries to go beyond the Core. It can also help to provide fast convergence from failures that may occur on the layer 3 network.

Recommendations: summarize routes from the Distribution (or Aggregation) layer up to the Core (LAN or Data Center). If no summarization is configured, EIGRP queries (which determines the best path for a route) can go beyond the Core which can cause potential traffic drops until EIGRP finishes with its convergence process. With route summarization configured on the Distribution/Aggregation it will stop queries up to the Core because the Distribution/Aggregation only sends a summarized route to the Core. So if an individual subnet (part of the summarized route) goes down for whatever reason it does not advertise its loss of connectivity to the Core. The Core switch does not know it cannot send traffic to the Distribution/Aggregation node where the link has failed, but will still route to that subnet using a summarized route. The routes on the Distribution/Aggregation switches are not summarized and with FHRP configured it will still be able to route to the appropriate node. That is why it is important to include an interconnection link between the Distribution/Aggregation switches, which allows the Distribution/Aggregation node that loses connectivity to a given VLAN/Subnet to route across the interconnection instead.

#5	Stub Routing

Enabled to prevent route transits and to not receive EIGRP queries if a route re-calculation occurs.

Recommendations: EIGRP stub areas are recommended for WAN spokes and LAN Access networks enabled for L3 services. Or it can be enabled on EIGRP routers where routing should NOT travel (or become a transit) through to reach other networks. Hence, WAN spokes or L3 LAN Access networks should not be a transit area nor respond to EIGRP queries.

#6	Passive Interfaces

Passive Interfaces: a best practice that prevents rogue routing devices from injecting bad routes into the network.

Recommendations: Passive interfaces can provide a great level of security to prevent rogue routing devices from bringing down the entire network. For example, if EIGRP is enabled without any security, then someone could plug in a Cisco router in their office that could potentially impact the routing environment and affecting the production network. Therefore, EIGRP routing capabilities on subnets where no routers should exist (e.g. user subnets) should be enabled as a passive interface.

#7

Routing Authentication

Configure **MD5 Authentication** on all EIGRP routers which will create a one-way hash password. This password is required in order to form a neighbor relationship with other EIGRP routers in the AS domain. MD5 authentication also provides higher security compared to implementing just Passive Interfaces.

#8

Route Control/Filtering

Controls what routes are sent and received by the routing protocol.

- **ACL:** configure an ACL with what routes should be received or advertised (using permit) or not (using deny).
- **Distribute List:** the ACL is used with a distribute list configured under the EIGRP routing protocol.
- **Direction (Inbound, Outbound):** to restrict what routes are injected into the EIGRP router use “inbound” with the distribute list. To restrict what routes are advertised to other routers use “outbound” with the distribute list.

Recommendations: this is strongly recommended to provide better control of what routes are being sent and received on the network. This can prevent rogue EIGRP routers and routes that can potentially bring down the entire network. This is common and recommend for LAN/Data Center networks configured in a Customer/Building model where many buildings may have their own routing devices using EIGRP for exchanging route information. The distribute-list is configured for those interfaces for what routes can be received from that building network including what routes will be advertised to that building network. If you are using L3 Access switches for your L2/L3 topology, it's recommended to enable route filtering mechanisms towards the L3 access switches.

#9

NSF with EIGRP

When a supervisor switches over to the standby supervisor it will continue to forward IP traffic flows in hardware. However, the supervisor needs time to reestablish two-way peering with all connected EIGRP routing neighbors. Enabling NSF with EIGRP can signal with other peers when it switches over to a hot-standby supervisor and to allow time to reestablish connections.

A large, white, serif capital letter 'F' is centered within a dark gray rectangular box. The box is positioned in the upper half of the page.

~ Services ~

FabricPath

Category: Network Service (DCI)

Prerequisite(s): Data Center (Solution), VLAN (Services)

FabricPath (FP) is a next-generation Layer 2 technology providing multi-path capabilities in L2 networks without using the Spanning Tree Protocol. FabricPath makes the layer 2 domain be seen as one giant switch within the L2 Ethernet domain.

When to use: to connect several layer 2 domains together using a layer 3 technology called FabricPath. This allows the environment to be seen as one logical switch.

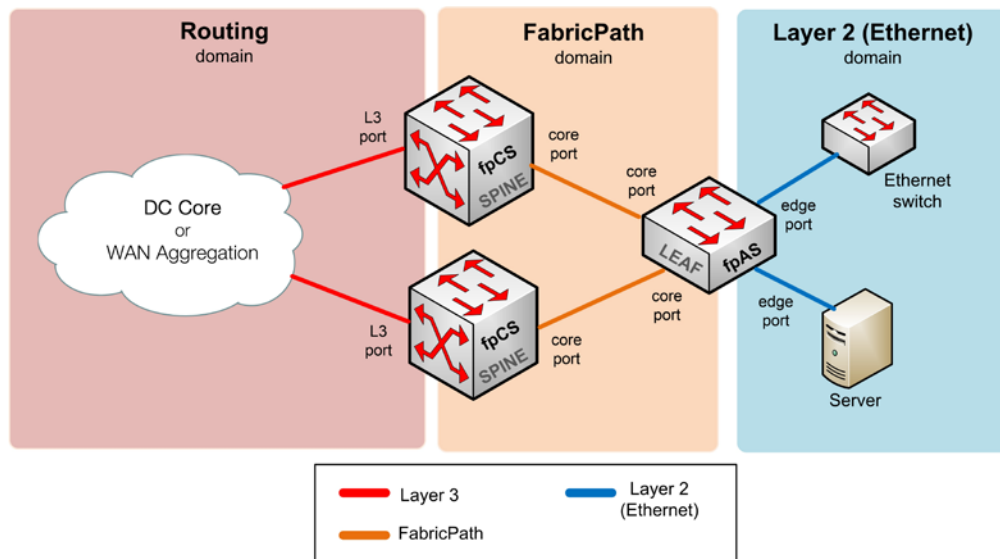
FabricPath provides many advantages for Data Center networks that include:

- Provides a scalable fabric for the Data Center network
- Multipath Load Balancing: uses multiple uplinks to forward traffic which can increase the bandwidth availability on the network
- Using VLANs anywhere without trunk ports needed across the network
- Spanning Tree does not run inside of a FabricPath topology
- FP is transparent to Layer 3 protocols
- Provides fast convergence if there are failures

Below are the components in the solution and how they are deployed:

- FabricPath SPINE (FP Core or fpCore):** these are components that exist within the FP domain carrying FP VLAN traffic encapsulated. The FP SPINE will connect into the FP domain using FP core ports. These ports will carry traffic encapsulated in FP frames and must be connected to another FP core port within the FP domain. This component will likely be an Aggregation switch within a three-tier Data Center topology. Or exclusive FP switches that will operate as FP Core switches (fpCore). The FP SPINE is also responsible for the following functions:
 - Responsible for forwarding traffic based on a Switch-ID.
- FabricPath LEAF (FP Access or fpAccess):** these are components that exist between the Ethernet L2 domain and the FP domain. The WAN facing interface of this component will connect into the FP domain using FP core ports. It will connect to the FP SPINE or other LEAF switches using FP core ports. The LAN facing interface of this component will connect to the L2 domain using standard Ethernet ports (or FP edge ports). This is where standard Ethernet switches or servers would connect to. This component will likely be the access switches within the Data Center topology. Or exclusive FP switches that will operate as FP Access switches (fpAccess). This component is also responsible for the following functions:
 - Responsible for mapping MAC addresses to switch ports.
 - Support Classical Ethernet (CE) VLANs which are locally used among the FP edge ports and not extended across the FP domain.
- Data Center Core or WAN:** The FP Core (SPINE) switches will connect into a routing domain using L3 ports. This will likely be your Data Center Core switch or WAN aggregation router connecting to the rest of the layer 3 network.

Below is a sample topology for how these components are connected together.



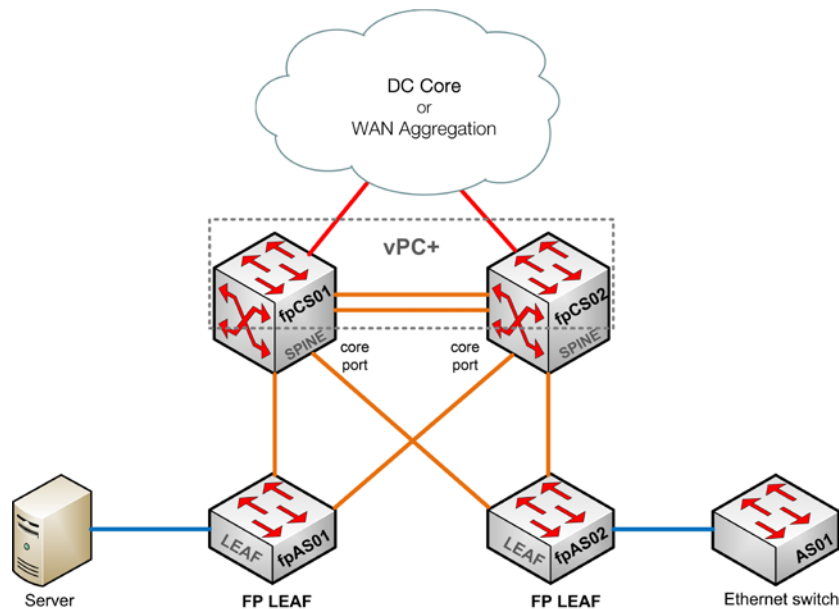
Determine which deployment model will be used for the FP topology within the Data Center:

1. Using two FP Core (SPINE) switches
2. Using four FP Core (SPINE) switches
3. Using Dedicated FP Core (SPINE) switches
4. Using Multiple FP Topologies

In this deployment model, two FP Core (SPINE) switches are used within the Data Center aggregation layer configured in a vPC+ domain. The two FP Core switches will connect to each of the FP Access (LEAF) switches using FP core ports. And it will connect into the Data Center Core (or WAN Aggregation) using layer 3 interfaces. Below are other design points for the FP Core (SPINE):

- All VLAN SVIs are configured on the FP Core (SPINE) switches
- Layer 4 - 7 services (e.g. firewall) are typically placed within this layer

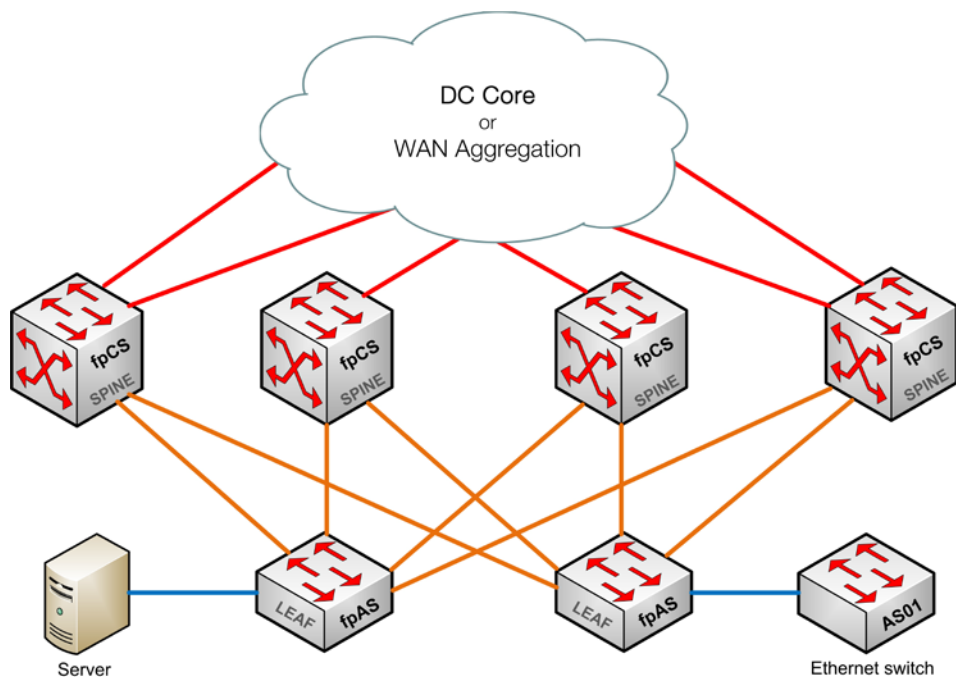
The FP Access switches will connect into the FP domain using FP core ports and into the L2 domain (Classical Ethernet) using FP edge ports. This model is the simplest of the other deployment models and the most common for Data Center networks.



In this deployment model, four FP Core (SPINE) switches are used within the Data Center aggregation layer configured with Anycast HSRP sharing the same VIP and VMAC. The four FP Core switches will connect to each of the FP Access (LEAF) switches using FP core ports. It will also connect into the Data Center Core (or WAN Aggregation) using layer 3 interfaces. Below are other design points for the FP Core (SPINE):

- All VLAN SVIs are configured on the FP Core switches
- Layer 4 - 7 services (e.g. firewall) are typically placed within this layer

The FP LEAF switches will connect into the FP domain using FP core ports and into the L2 domain (Classical Ethernet) using FP edge ports. Traffic from the FP Access switches are routed to all of the FP Core switches based on ECMP and the Anycast HSRP providing load distribution. This model provides higher scalability for larger L2 domains in a Data Center topology.



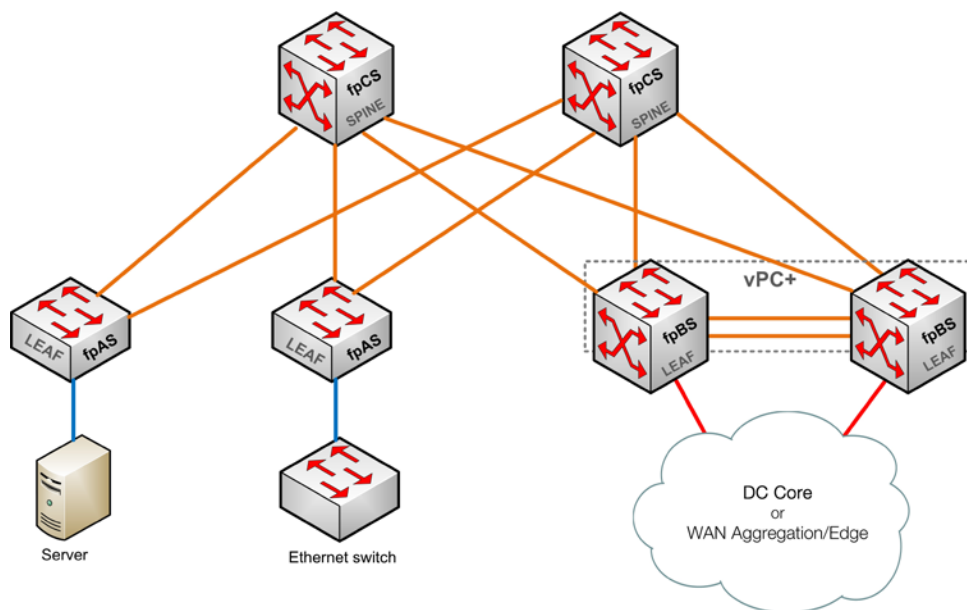
In this deployment model, a dedicated FP Core (SPINE) layer is added to the FP topology. The dedicated FP Core switches will exist inside of the FP domain using FP core ports between all of the FP Access & Border (LEAF) switches.

Two different LEAF distributions are implemented in this topology providing different functions. There are FP Access (LEAF) switches (fpAS) which will connect into the FP domain using FP core ports and into the L2 domain (Classical Ethernet) using FP edge ports.

And there are FP border (LEAF) switches (fpBS) on the border that are connected into the FP domain using FP core ports. But they also connect directly into the Data Center Core (or WAN Aggregation) using layer 3 interfaces. Below are other design points for the FP Border (LEAF) switches:

- All VLAN SVIs are configured on the FP border (LEAF) switches
- Layer 4 - 7 services (e.g. firewall) are typically placed within this layer

This model provides simplicity to the FP Core (SPINE) including ensuring that most servers are two-hops away.



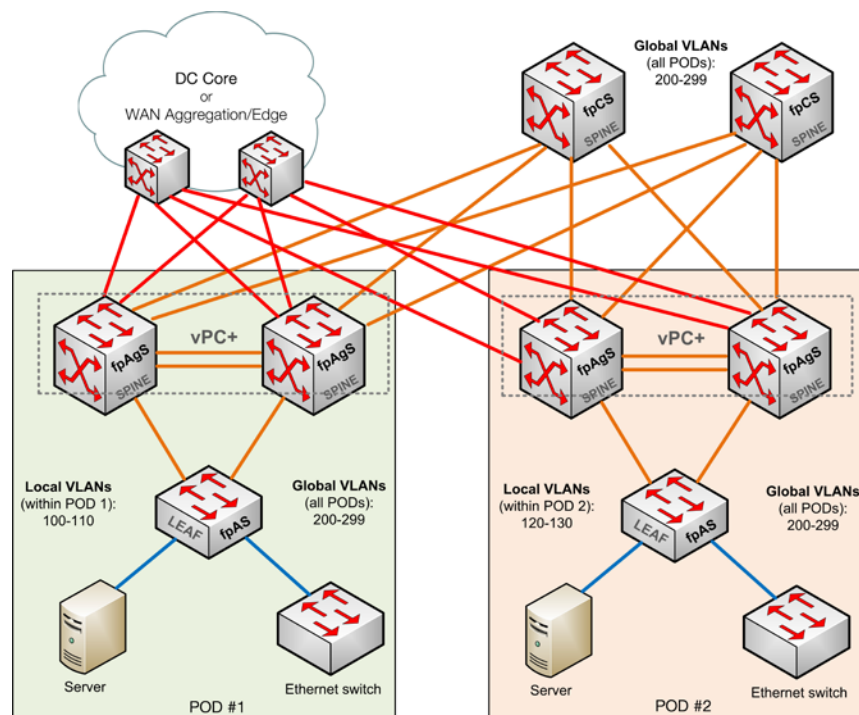
When to use: ideal for hosted provider and IaaS networks.

In this deployment, several miniature FabricPath topologies called PODs are used. Each POD will consist of their own FP Core (SPINE) and FP Access (LEAF) switches. But the FP Core switches within a POD is labeled as a FP Aggregation (SPINE) switch sharing the same attributes as a FP Core switch. Below are other design points for the FP components within each POD:

- There are local VLANs that are used only within a POD.
- There are global VLANs (the default topology or Data Center wide VLANs) that are used across the network and other PODs.
- The FP Aggregation (SPINE) switches are enabled using vPC+ or Anycast to provide active-active HSRP within a local POD.
- The FP Aggregation (SPINE) switches will connect to the local FP access (LEAF) switches within the POD using FP core ports. This is part of the local FP domain.
- The FP Aggregation (SPINE) switches will connect into a layer 3 domain using routed ports. The layer 3 domain may be the Data Center core switch or WAN Aggregation/Edge router that exist in the Data Center.
- The FP Aggregation (SPINE) switches will also connect into a dedicated pair of FP Core (SPINE) switches using FP core ports. This is part of the global FP domain that is used with all other PODs and their FP Aggregation switches. It is the FP Core (SPINE) where the global VLANs are routed and extended to all of the PODs in the FP topology. The FP Core switches in this deployment option is also called a FP Super SPINE.
- The FP Access (LEAF) switches will connect into the Ethernet network (layer 2 domain) using FP edge ports.

Below are design points for the FP Core (SPINE) component and the global VLANs (default topology):

- The FP Core (SPINE) switches are enabled using vPC+ or Anycast to provide active-active HSRP for all PODs.



Below are other features and technologies that can be implemented within the FP topology:

- **Anycast HSRP:** provides up to four active default gateways (active-active HSRP) on the network to achieve increased high-availability. This feature is recommended on the following deployment models:
 - o **Deployment #1 & 2:** implemented on the FP Core (SPINE) switches
 - o **Deployment #3:** implemented on the FP Access (LEAF) and Border (LEAF) switches
 - o **Deployment #4:** implemented on the FP Aggregation (SPINE) and FP Core (SPINE) switches
- **EvPC+:** extends vPC+ down to the connected classical Ethernet switches. Operates similar to Enhanced vPC. This feature is optional and can be added to any of the following deployment models:
 - o **Deployment #1-4:** implemented on any of the FP Access (LEAF) switches
- **Fabric Extenders (FEX):** if the FP Access (LEAF) switches are Cisco Nexus 5500 switches, they can connect with Cisco Nexus 2000 through FEX connections on the L2 domain (Classical Ethernet). This feature is optional depending on what hardware is used and can be added to any of the following deployment models:
 - o **Deployment #1-4:** implemented on any of the FP Access (LEAF) switches using Cisco Nexus 5500 hardware.
- **vPC+:** vPC+ is an extension of vPC for FabricPath providing two primary functions:
 - o (1) Provide dual-homed connections from Classical Ethernet (CE) switches and hosts capable of port channels. vPC+ can also be used for devices that do not support FabricPath. This feature is optional and can be added to any of the following deployment models:
 - **Deployment #1-4:** implemented on any of the FP Access (LEAF) switches
 - o (2) Provide active-active HSRP for high-availability. This feature is recommended on the following deployment models:
 - **Deployment #1:** implemented on FP Core (SPINE) switches if Anycast HSRP isn't already configured
 - **Deployment #3:** implemented on FP Border (LEAF) switches if Anycast HSRP isn't already configured
 - **Deployment #4:** implemented on the FP Aggregation (SPINE) and FP Core (SPINE) switches if Anycast HSRP isn't already configured
- **Traffic Engineering:** provides capability to statically configure routes into the forwarding table to specify how traffic should be routed (paths and/or interfaces) across the FP domain. Operates similar to Traffic Engineering with MPLS. This feature is optional and can be added to any of the following deployment models:
 - o **Deployment #1-4**

Below are best practices for using FabricPath on the network.

- Configure the switch ID manually on all FabricPath switches.
- FP VLANs must be configured on all switches in the FP domain.
- Use the default reference bandwidth (400 Gbps). FP will always take the path with the lowest metric through the FP domain.
- Do not use UDLD.
- Disable IP redirects on all VLAN SVIs.
- Use passive interfaces on VLAN SVIs to avoid any routing adjacency over any VLAN SVI
- **Fast Convergence:** tune Layer 2 IS-IS SPF and LSP timers to provide fast convergence if there is a failure within the FP topology. The timers should be tuned to 50msec (for the initial wait and second wait timers).
- Disable ISIS hello padding on Cisco Nexus 7000 when jumbo frames is enabled.
- The MAC timer should be consistent on all devices in the Layer 2 topology.
- Make the FP LEAF switch the primary root bridge for all VLANs that are used.
- Use port channels between the FP components to decrease the number of direct IS-IS adjacencies.
- vPC+ ARP sync feature is recommended for improved traffic convergence during failure and restoration.
- Configure the highest and second highest MDT root priority on the FP SPINE-LEAF switches.

Below are some caveats to keep in mind while using this service:

- The FabricPath feature must be enabled on the default and non-default VDC
- FabricPath interfaces can only carry FabricPath traffic
- There is no support of hierarchical static MAC addresses or static routes
- Devices that do not support FabricPath can be redundantly connected to two separate FabricPath switches using vPC+.
- VLANs must still be locally managed within the L2 domain.

Below are requirements for implementing this service on the network:

- **Hardware:** Using Nexus 6000, Nexus 7000 series switches using F-Series modules (e.g. F1 and F2 modules) or using the Nexus 5500 series switches
- **Licensing:** Enhanced Layer 2 license is required

Below are hardware considerations for using FabricPath:

FP Core and Border Switches: the following hardware can be used for the FP Core (SPINE) and FP Border LEAF switches in the FP topology:

- Cisco Nexus 6000
- Cisco Nexus 7000 (M-series, F2-series or F2E-series modules)

FP Access: the following hardware can be used for the FP Access (LEAF) switches in the FP topology:

- Cisco Nexus 5500 (FP Access only)
- Cisco Nexus 6000
- Cisco Nexus 7000 (using M-series, F2-series or F2E-series modules)

First-Hop Redundancy Protocol (FHRP)

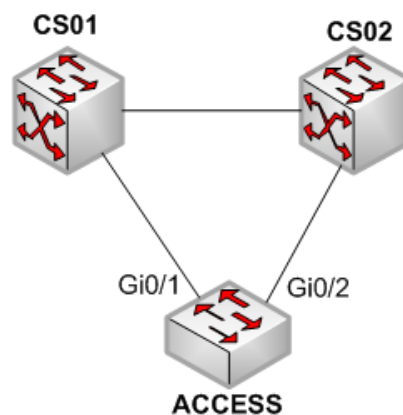
Category: Network Service (Routing and Switching)

Prerequisite(s): LAN, Data Center, WAN, and/or Internet Edge Solution

R

Determine the default gateway redundancy protocol that will be used or already determined for the required redundancy on the network.

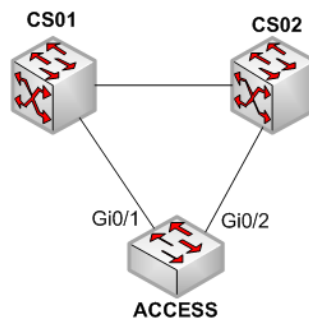
- **HSRP:** used to provide redundancy for the default gateway if the primary router fails. This is commonly used between Cisco devices.
- **VRRP:** used to provide redundancy for the default gateway if the primary router fails. This is commonly used between Cisco devices or any other L3 device that supports the feature.
- **GLBP:** used to provide redundancy and load balancing for the default gateway. This is commonly used for Cisco devices in medium to large size networks.



Flex Link

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)

A locally significant feature that creates a primary and backup switch port on a L2/L3 switch. This is an optional feature that can be implemented on Access switches if it is supported. For the configuration specify the uplink to the primary Core/Aggregation/Distribution switch to be the primary port and the secondary Core/Aggregation/Distribution switch that the Access switch is connected to will be the backup port. Keep in mind that this feature does not create a loop-free network, so using STP is still recommended for the design.



In this topology example, the Access switch is configured for FlexLink where Gi0/1 would be the primary path to the Core and Gi0/2 would be the secondary path.

FlexVPN

Category: Network Service (Security)

Prerequisite(s): VPN & Remote Access (under Solutions)

When to use: ideal for full-mesh, point-to-point, or point-to-multipoint connectivity between sites providing higher security over IPsec VPN using IKEv1.

Description: this is a next-generation extension of building IPsec VPNs that uses IKEv2 instead of IKEv1 which is more secure providing added authentication, reliability, minimum bandwidth consumption, to flexibility support with MOBIKE and NAT-T. MOBIKE extends IKEv2 capabilities with mobile devices.

FlexVPN also provides support of multiple VPN solution technologies such as using Virtual Tunnel Interfaces (VTI), EZVPN, to DMVPN supported to work with IPv4 and IPv6. One consideration in regards to using FlexVPN is that there is no backwards compatibility support for IKEv1, its only supported for IKEv2.

G

~ Services ~

General Best Practices

Category: General Practices
Prerequisite(s): --



Below are general best practice services that should be implemented and considered for the design.

- **RFC1918 Addressing:** recommended that all servers and desktops utilize RFC 1918 private IP addressing on the network and not public IP addressing.
- **Speed and Duplex:** majority of network performance issues are related to speed and duplex mismatching between the network port and the device. The following should be considered and recommended:
 - o **Desktops:** desktops and the connected switch port should be configured for AUTO speed and duplex.
 - o **Servers:** servers and the connected switch port should be manually configured to use 100/FULL or AUTO if Gigabit Ethernet is used.
 - o **Uplinks/Downlinks:** connections between other switches or network devices like routers should be manually configured to use 100/FULL or AUTO if Gigabit Ethernet is used.
- **Link Redundancy and Failure Detection:** use Cisco IOS Throttling (by configuring the Carrier Delay Timer to the value of zero) and Linecard Throttling (using the Debounce Timer). Linecard Throttling is a default behavior and the recommended configuration for the debounce timer is disabled. This will result in minimum time between link failures and notification to the upper layer protocols. GE and 10GE operate with a 10ms debounce timer configured.
- **ARP Aging/Timeout:** Tune ARP aging timers close or equal to the CAM/MAC-address aging value (default is 200 seconds). The default ARP age/timeout is 4 hours, so tune the timeout to be 200 seconds
- **Out-of-Band (OOB) Management:** another best practice is to implement OOB management for critical network devices. For example, if there is a network failure and you cannot access the equipment over the network, you can dial into a modem connected to the device's CON or AUX port to manage the equipment. This is similar to servers with OOB management ports like iLO (for HP servers).
- **Event Detection & Event Dampening:** uses the concept of BGP route dampening and applies it to an interface/system, so IGP routing protocols can benefit. Event Dampening is applied on the network device and nothing is exchanged with the IGP routing protocols.
- **Loopback Interface:** Each device on the network should have a management address associated to its device ID (a logical number that you can identify for each network device). The management interface should be a loopback interface configured with a /32 address.
- **Interconnections:** The interconnections between the Core and Distribution should be L3 connections using a /30 subnet.
 - o If using OSPF configure the interconnection links to use "point-to-point" for the network type.

GET VPN

Category: Network Service (Security)

Prerequisite(s): (i) VPN & Remote Access Solution *and* (ii) LISP, DMVPN, or using L3 WAN

SEC SC F

When to use: to create a tunnel-less VPN topology between sites over a private network framework (e.g. LISP, DMVPN, L3 WAN such as MPLS).

Below are advantages for deploying GET VPN across a WAN:

- It provides end-to-end data encryption for a network infrastructure while maintaining any-to-any communication between sites.
- It provides low latency and jitter with direct traffic communication between sites.
- It provides a centralized encryption policy and membership management using key servers.

#1

Components in GET VPN Topology

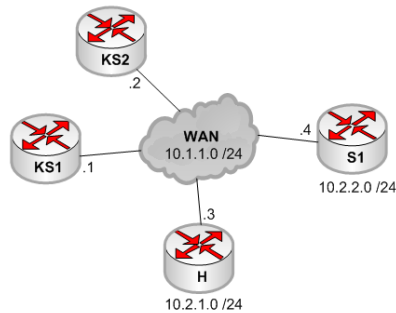
Build the GET VPN topology based on the components and protocols that will be used:

- **Group Members (GM):** all of the WAN routers (Aggregation and Branch) will be group members that will encrypts and decrypts data traffic between the sites.
- **Key Servers (KS):** this is the key component within the GET VPN topology. This would be one or more dedicated routers connected into the IP WAN. It is not recommended to deploy the WAN Aggregation routers as key server routers. They need to be separate routers added to the network.

The key server is responsible for authenticating the Group Members and managing the security policies for what traffic should be encrypted between the sites. The key servers sends out a key encryption key (KEK) and a traffic encryption key (TEK) to the group members in the topology. The KEK is used to secure communication between the KS and GMs. The group members use the TEK for bulk data encryption of traffic traversing between the GMs.

Its recommended to deploy redundant key servers within the topology operating in cooperative mode. They would become Cooperative key servers (COOP KSs) which will share the group members' registration load by jointly managing the GDOL registration of the group. Among a group of key servers, the key server with the highest priority assumes the primary role, while the other KSs remain in secondary roles. The primary KS is responsible for creating and redistributing the security policies and keys to the GMs, as well as synchronizing with the secondary KSs.

- **Group Domain of Interpretation (GDOL):** protocol used to create secure communication among the GET VPN components. This is used by the key servers to distributes session keys for traffic encryption and for security policies pushed to the Group Members.



In this example topology, the **Group Members** would be router's "H" and "S1". And the **Key Servers** would be router's "KS1" and "KS2".

#2	Caveats

Below are some caveats to keep in mind while using this service:

- If the key server(s) are unavailable then new group members will not be able to register and participate in the secure communication with other group members that are registered. Plus the existing group members will not receive new rekeys and updated security policies when the existing ones expire. Therefore its recommended to deploy redundant key servers within the topology operating in cooperative mode (also called COOP Key servers).

#3	Add-Ons

Below are other common technologies that can be implemented or overlay with GET VPN:

Technology	Description	Prerequisite(s)
GET VPN per VRF	Used when implementing VRFs (VRF-lite) over the GET VPN network.	Virtualization (Network) [Solution]
GET VPN over DMVPN	DMVPN is deployed as the framework between all sites without encryption. GET VPN is built on-top of the DMVPN topology providing tunnel-less encryption between sites.	DMVPN [Service]
GET VPN over LISP	LISP is deployed as the framework between all sites without encryption. GET VPN is built on-top of the LISP topology providing tunnel-less encryption between sites.	LISP [Service]

GLBP

Category: Network Service (Routing and Switching)

Prerequisite(s): First-Hop Redundancy Protocol (under Services)



GLBP provides greater uplink utilization for traffic exiting the access layer by load balancing across multiple uplinks. It can only be used in non-looped topologies (e.g. L3 Topology).

Below are best practices can be designed and deployed using GLBP on the network:

- Use sub-second timers with the GLBP configuration using a hello timer of 250ms and a dead timer of 750ms in environments with less than 150 VLAN instances. If those sub-second timers are not supported due to IOS limitation or hardware set the hello timer to 1 second and the dead timer to 3 seconds. This will provide a good balance of fast failover and sensitivity for traffic being sent to the control plane.
- Tune the preempt and keepalive timers to prevent black holes.
- If GLBP is used for a L3 Core, L3 Distribution, L2 Access (VLANs extended) topology, configure the STP blocking state between the Distribution switches using the following configuration:
 - *Configuration:* "spanning-tree cost 2000" should be implemented on the Secondary STP root bridge switch to ensure that both uplinks from the L2 switches are active/active.

Cisco Nexus Best Practices: if you are using a large number of FHRP groups in the environment, the control plane and FHRP timers should not be less than 1 second for the hello timer and 3 seconds for the hold timer.



~ Services ~

HSRP

Category: Network Service (Routing and Switching)

Prerequisite(s): First-Hop Redundancy Protocol (under Services)



Below are best practices can be designed and deployed using HSRP on the network:

- HSRP is SSO aware, which will help to avoid HSRP flapping.
- Use sub-second timers with the HSRP configuration using a hello timer of 250ms and a dead timer of 750ms in environments with less than 150 VLAN instances. If those sub-second timers are not supported due to IOS limitation or hardware set the hello timer to 1 second and the dead timer to 3 seconds. This will provide a good balance of fast failover and sensitivity for traffic being sent to the control plane.
- Tune the preempt and keepalive timers to prevent black holes.
- When using Multicast and HSRP force unicast including multicast communication to use the same path.
 - HSRP active router should be the Designated Router (DR) ; highest IP on subnet
 - HSRP standby router should be the non-Designated Router (DR) ; lowest IP on subnet
- Configure HSRP tracking on the Core/Distribution/Aggregation for critical interfaces (uplinks) for robust failover between FHRP peers.
- 500 HSRP sessions can be supported on the Core/Distribution/Aggregation devices using the Cisco Catalyst 6500 (Sup720 and higher), but monitor the overall CPU and performance on the switch.

Cisco Nexus Best Practices: if you are using a large number of FHRP groups in the environment, the control plane and FHRP timers should not be less than 1 second for the hello timer and 3 seconds for the hold timer.



~ Services ~

IPSec VPN

Category: Network Service (Security)

Prerequisite(s): VPN & Remote Access (under Solutions)

SEC

When to use: Used for point-to-point (or point-to-multipoint) connectivity between a small number of sites for accessing resources securely. Or to require direct access to resources on the internal network(s) using a VPN program installed on the client.

Overview

Description: supported on all VPN devices (e.g. Routers or Firewalls), however, there are limitations for using routing protocols and multicast. Thus, IPSec VPN can be configured as a Virtual Tunnel Interface (VTI) or using a GRE tunnel to allow the use of routing protocols and minimal use of multicast. This will treat the connection like a logical point-to-point connection. This is also a common VPN protocol used by clients (using a VPN program installed on their system) to connect into the network to access network resources remotely. IKEv2 is recommended over IPSec using IKEv1 which is more secure providing added authentication and reliability. This involves configuring either a IPSec VPN profile for IKEv2 or implementing FlexVPN.

Hardware Required: Routers *OR* Firewalls

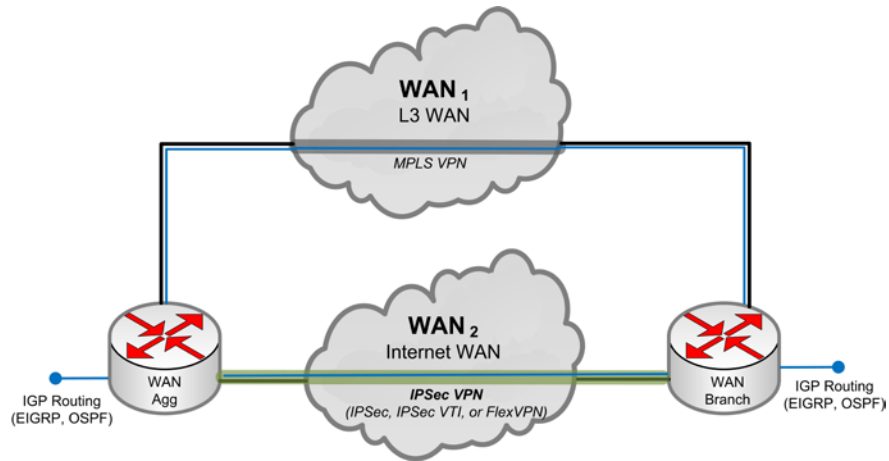
Determine the IPSec VPN (Client and/or Site) technology that will be implemented:

VPN Type	Technology	Description	IGP Routing Support
Client VPN	<i>IPSec VPN (IKEv1, IKEv2)</i>	IPSec VPN profiles configured on the VPN device to allow clients using a VPN program installed on the client's computer (Windows, Mac) to access network resources remotely. IKEv2 is recommended over IKEv1 which is more secure providing added authentication and reliability.	--
	<i>EZVPN</i>	A simplified IPSec VPN solution that allows minimal configuration on the VPN spoke sites or clients connecting to a main office. This provides easy configuration with support for dynamic IP addresses at the remote sites or with VPN clients. This level of configuration can be used with DMVPN, but EZVPN is only supported on Cisco hardware.	--
Site VPN	<i>IPSec VPN (IKEv1, IKEv2)</i>	Ideal for point-to-point (or point-to-multipoint) connectivity between a small number of sites (1-2 sites) for accessing resources securely. unable to support the use of dynamic routing protocols, multicast, and QoS.	No
	<i>IPSec VTI / IPSec over GRE</i>	A virtual tunnel interface (VTI) is configured to build an IPSec over GRE tunnel between locations to allow the use of dynamic routing protocols, multicast, and QoS. This is recommended over IPSec VPN if the equipment (routers) can support VTI and there are no restrictions for using GRE over the Internet. For configuration use Tunnel mode (default) which supports pre-fragmentation ideal for larger packets. Using Transport mode does not support pre-fragmentation, but saves 20 bytes over Tunnel mode.	Yes
	<i>FlexVPN (IKEv2)</i>	Ideal for full-mesh, point-to-point, or point-to-multipoint connectivity between sites providing higher security over IPSec VPN using IKEv1. It provides added authentication, reliability, minimum bandwidth consumption, to flexibility support with MOBIKE and NAT-T.	Yes

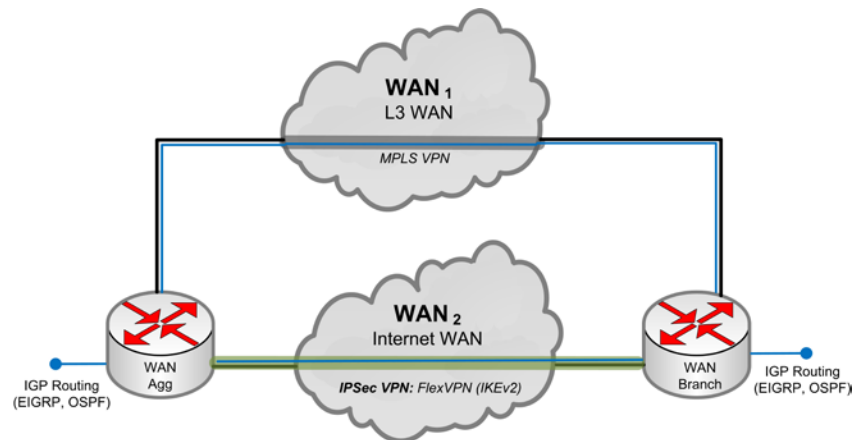
Example #1: continuing with our previous WAN and VPN topology, the design includes the following aspects:

- **WAN Cloud Design:** Primary WAN (using L3 WAN) and Secondary WAN (using Internet WAN)
- **VPN technology for Internet WAN:** IPSec VPN (IPSec VPN, IPSec VTI, or FlexVPN)

As a recap, this is what our WAN topology looks like:



Using the table above, we can determine which specific IPsec VPN technology will be used and it should consider IGP routing. We want our WAN to support an IGP routing protocol that will be configured within all LANs plus across our L3 WAN and Internet WAN. Therefore only IPsec VTI and FlexVPN supports IGP routing capabilities. Between the two we can select **FlexVPN** as the IPsec VPN technology that will be used connectivity among our sites:



Below are some redundancy options to consider when using IPsec VPN on the network:

- **Dead Peer Detection (DPD):** Configured in the IPsec policy on the redundant VPN router.
- **HSRP and RRI:** Configure HSRP (on the LAN ports, not WAN ports) between the two VPN routers. The virtual IP is used for the remote sites to peer with. Using HSRP will require Reverse Route Injection (RRI), which is used to determine which VPN router to route to that has the active tunnel established. RRI is also used for VPN tunnel state tracking.
- **Routing Cost/Delay:** if using IPsec over GRE then you can configure dynamic routing protocols like OSPF or EIGRP, which has redundancy components built in. In the topology, the remote site will have two IPsec over GRE tunnels established with the two head-end VPN routers. On the head-end VPN routers tune the OSPF cost or EIGRP delay values on the GRE interfaces to create a primary and secondary path for the remote sites. This redundancy method is highly recommended over using HSRP (with RRI) since the configuration is simpler and with OSPF/EIGRP they can provide fast convergence with the redundant VPN tunnels established.

Below are best practices to use with IPsec VPN services on the network.

- **Pre-Fragmentation:** Enabled globally (default) which increases the decrypting router's performance by using CEF switching (high performance) instead of the process switching.
- **NAT-T:** configured when using IPsec for Client remote access. NAT-T provides support for IPsec traffic to travel through NAT or PAT devices by encapsulating both the IPsec SA and the ISAKMP traffic in a UDP packet. This option is enabled by default.
- **MTU:** the safest and recommended MTU to use for GRE interfaces to avoid fragmentation is 1400 bytes. This is applicable when using IPsec over GRE or DMVPN as a solution.
- **Main Mode:** if you want to setup highly secure IPsec VPN tunnels by protecting the identity of the hosts setting up the VPN, its recommended to disable Aggressive mode on the VPN enabled devices. Aggressive mode does not protect the identity of the host setting up the VPN, sending the host identities in clear text across the network. Disabling Aggressive mode is what many security audits will recommend especially if the network is under a particular compliancy (e.g. SOX, PCI, HIPPA).

Resources

#1 VPN Port Numbers

- **ISAKMP:** UDP/500
- **NAT-T:** UDP/4500
- **ESP:** IP/50
- **AH:** IP/51
- **GRE:** IP/47

IPv6

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN, WAN, and/or Data Center (under Solutions)

Complete the steps below if IPv6 services will be implemented in the design:

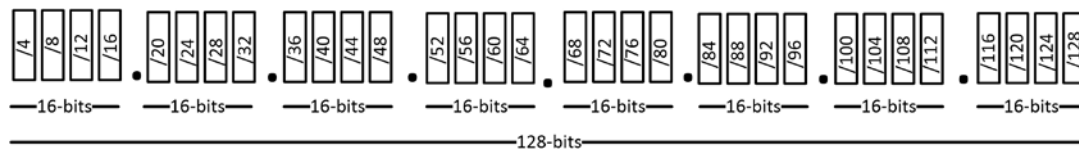
Step 1

Overview of IPv6 Addressing Structure

Below is a quick overview of the IPv6 addressing structure:

The total bits within a IPv6 address is 128-bits consisting of 8 separate fields each consisting of 16-bits. Within each 16-bit field it consist of four sub-fields that is 4-bits. Hence, that would equal a total of 16-bits per field. (8 fields * 16 bits/field = 128 bits).

An IPv6 address uses hexadecimal values which ranges from 0 to 9 and A to F which are 16 possible values that can be used for each sub-field in the address.



An IPv6 address is broken up into two main parts: Network-ID + Interface-ID



The Network-ID is broken down further based on: Network Prefix + Subnet Prefix



For example, the Network-ID may be fd00:1::/64. In this network-ID, the network prefix would be "fd00" and the subnet prefix would be "1". Together they make up the network-ID, similar to IPv4.

The /64 indicates that the first 64-bits are being used to represent the network-ID and the last 64-bits are being used to represent the interface-ID.

Your network will likely be mixed with IPv4 and IPv6 traffic for the network topologies. If you are building an IPv6-only network for all communication then you can skip this step.

Below are the different transition mechanisms that can be used with IPv4 and IPv6 environments.

1. Dual Stack
2. Tunneling: ISATAP
3. Tunneling: IPv6 over IPv4 Tunnels using GRE
4. Tunneling: 6to4
5. Tunneling: 6RD
6. Translation: Stateful NAT64

Go through each option to view the description, caveats and when to use (or use-cases) to determine which option will work better in your environment based on your requirements. You can choose more than more depending on your network topology and the solutions that are used.

#1

Dual Stack

When to use: this is the most common and recommended mechanism for IPv4/IPv6 transition. It requires all network hardware to be supported and enabled for IPv6.

Description: In this transition deployment, each network device runs both protocol stacks (IPv4 and IPv6). Furthermore, the end user nodes (e.g. Microsoft Windows, Apple OS X, Linux) will also run IPv4 and IPv6 protocol stacks.

Below are some caveats and considerations to keep in mind while using this transition method:

- It requires powerful network hardware with CPU and memory resources to support the dual protocol stacks.
- You must apply the same security policies across both protocol stacks, hence increasing the overall administration in the environment. Otherwise, a computer could be comprised from the IPv4 stack which can then exploit the IPv6 stack regardless if security is implemented on that stack.
- **DNS queries consideration:** if a dual-stack host receives a DHCP reply for a request that contains both IPv4 and IPv6 addresses, it will use IPv6.

#2

Tunneling: ISATAP

When to use: when most of the network hardware is IPv4 enabled. This will likely be for environments that are using older network hardware that doesn't support IPv6. In networks today, dual-stack is recommended over using ISATAP tunnels.

Description: In this transition deployment, the end-user's computer is ISATAP enabled. The system will establish a ISATAP tunnel to a ISATAP server/device component. This ISATAP server component may be the Core switch, distribution switch, or a dedicated switch handling all ISATAP services. The ISATAP server component runs in a dual-stack mode supporting both protocol stacks. The end-user node is configured with a IPv4 address, but they will automatically be assigned an IPv6 address from the ISATAP server once the tunnel is established.

#3

Tunneling: IPv6 over IPv4 Tunnels using GRE

When to use: this is used in unique cases where you may need to quickly extend your existing IPv6 network to other sites over an IPv4-only WAN or Internet infrastructure.

Description: In this transition deployment, IPv6 traffic is encapsulated over the IPv4 network infrastructure using GRE tunnels. This IPv6 over IPv4 tunnel is terminated between two routers that has IPv6 networks residing behind it.

Below are some caveats and considerations to keep in mind while using this transition method:

- Does not provide any data encryption or integrity services with the established tunnel. Its recommended to implement IPSec with the tunnel to make it secure.
- This is not a scalable transition method if there are dozens to hundreds of sites.

#4

Tunneling: 6to4

When to use: when you want to extend your IPv6 network over an existing IPv4 Internet or WAN. Or for sites to connect quickly into the IPv6 Internet. This transition deployment is typically deployed by the service provider and not a customer network. If this type of deployment needs to be used then 6RD would be recommended over using 6to4 tunnels.

Description: In this transition deployment, IPv6 enabled sites build automatic 6to4 tunnels with other sites over an IPv4 network (Internet WAN or L3 WAN). Or for sites to connect quickly into the IPv6 Internet.

Below are some caveats and considerations to keep in mind while using this transition method:

- Lack of flexibility to specify what the IPv6 prefix will be. 6to4 requires the 2002::/16 IPv6 prefix.
- Does not provide any data encryption or integrity services with the established 6to4 tunnels.

#5

Tunneling: 6RD

When to use: when you want to extend your IPv6 network over an existing IPv4 Internet or WAN. Or for sites to connect quickly into the IPv6 Internet. This is typically deployed by the service provider and not by a customer directly.

Description: In this transition deployment, IPv6 enabled sites build automatic 6RD tunnels with other sites over an IPv4 network (Internet WAN or L3 WAN). Or for sites to connect into the IPv6 Internet (6BONE). This is similar to 6to4, but 6RD can accept any global IPv6 network prefix besides 2002::/16. Overall, 6RD is commonly used today by service providers to provide automatic tunnel termination with customer networks needing access to the IPv6 Internet.

Below are some caveats and considerations to keep in mind while using this transition method:

- Does not provide any data encryption or integrity services with the established 6RD aggregated tunnels.

When to use: (1) when IPv4 host(s) are accessing the IPv6 Internet or network. (2) when IPv6 host(s) are accessing the IPv4 Internet or network. (2) recommended translation protocol for NAT64.

Description: In this transition deployment, a translation protocol is used to allow communication between IPv4-only hosts and IPv6-only hosts by putting a translator in-between. It performs IP header and address translation between the two protocol stacks. Below are other aspects for this translation protocol:

- It creates and maintains a session state table while performing translations
- It can support 1:Many translations where stateless NAT64 supports 1:1 translations
- Used for TCP, UDP, and ICMP communication between the IPv4 and IPv6 hosts.
- Relies on DNS64 to manage DNS requests with "A" and "AAAA" records being created

The NAT64 prefix that can be used for mapping between address families are:

- (1) **Well Known Prefix (WKP)** using the 64:ff9b::/96 prefix which is not routable over the Internet.
- (2) **Network Specific Prefix (NSP)** using an organization address space (global, unique-local, or site-local) which can be routable over the Internet if a global address is used.

Another note to understand is that the IPv4 address is converted to a IPv6 address for the Interface-ID section.

For example, if the IPv4 host IP address is 10.10.1.10 (hex: 0a.0a.01.0a). It can be translated to:

- **Using WKP:** 64:ff9b::10.10.1.10 or 64:ff9b::0a0a:010a
- **Using NSP (with global):** 2001:db8:1::0a0a:010a

Below are some caveats and considerations to keep in mind while using this transition method:

- If FTP and SIP applications will be used through a NAT64 enabled device, it will require application-layer gateway (ALG) support for the translation.

There are different IPv6 addressing types which includes Unicast, Multicast, and Anycast. For IPv6 Unicast addressing, you can assign either an internal (private) and/or external (public) addresses to your IPv6 nodes. Below is a list of the IPv6 Unicast Addressing types can be used:

Local (Private): addressing that is locally significant to a segment used for neighbor discovery and route advertisements. It is not routable across other networks and should not be used for internal addressing. Below are the IPv6 private addressing types that are considered as local addressing:

- Link-Local Addressing (fe80::/10)

Internal (Private): addressing that is used internally within an organization unlike link-local addressing. It is not routable across the Internet which is similar to the IPv4 RFC 1918 addressing schema. Below are the IPv6 private addressing types that can be used:

- Site-Local Addressing (fec0::/10)
- Unique-Local Addressing (fc00::/7)

External (Public): addressing that is used externally with the Internet to access public services. The global address space is allocated from the regional registries (RIPE, ARIN, APNIC) where they can be obtained directly or indirectly from a service provider. Note: Typically a /48 block is assigned which gives the organization 2^{16} (65536) /64 subnet prefixes that can be used. Below are the IPv6 public addressing types that can be used:

- Global Addressing (2000::/3)

Determine what IPv6 addressing will be assigned to the hosts on the network. The structure of IPv6 was designed to provide more addressing that can be assigned to nodes without using a translation protocol (e.g. NAT). Basically each host or network device should be assigned a global (public) address for accessing not only external resources but also internal resources. However, traditional network engineers may prefer to use private addressing on the internal devices and implement a translation protocol (e.g. NPTv6). The options available are:

1. Global IP only
2. Internal IP only
3. Internal and Global IP assigned
4. Internal IP translation to Global IP

Go through each option to view the description, caveats and when to use (or use-cases) to determine which option will work better in your environment based on your requirements. Can you choose multiple options for different nodes that may exist in the environment.

#1

Global IP only

When to use: (1) recommended option for IPv6 addressing for nodes. (2) If it is less likely that you will change service providers and your global IPv6 address space.

Description: In this option, the hosts are configured with a global IPv6 address which allows them to have access to internal and external resources. This option is recommended over the other options listed.

Below are some caveats and considerations to keep in mind for this option:

- If you are using a global address space that is Provider Assigned (PA) and you change service providers, it may require re-addressing all nodes on the network using an address from that global address space. This can cause a significant increase of administration and support during the transition to a new service provider and global address space.

#2

Internal IP only

When to use: for internal devices that do not require Internet access such as printers, sensors, access-points, to engineering labs.

Description: In this option, the host is configured with an internal/private IPv6 address only. This can be a site-local or unique-local address (ULA), but a ULA is recommended between the two.

When to use: if global IPv6 multicast and PMTUD services will not be used on the IPv6 host.

Description: In this option, the host is configured with an internal IPv6 address for internal communication. And a global IPv6 address for external communication or Internet access. This option provides the most complexity from the other options due to several limitations which are highlighted under the caveats.

Below are some caveats and considerations to keep in mind for this option:

- **Path MTU Discovery (PMTUD):** if you are using Path MTU Discovery (PMTUD) with unique local addresses, the operation of PMTUD may not work properly. Therefore, if you are using a ULA its recommended to configure a global address for the loopback interfaces to allow PMTUD to operate correctly.
- **Global IPv6 Multicast:** the unique-local address is chosen over the global address for the source address selection. This selection can cause issues for Internet bound multicast traffic and disrupt the ability to pass the multicast RPF checks.

When to use: (1) to avoid re-addressing all nodes if the global address space and service provider changes for an organization. (2) Desired for pro-NAT network engineers who want to use private IPv6 addressing and use a IPv6 NAT protocol (e.g. NPTv6) to translate to a Public IPv6 address space for Internet access.

Description: In this option, the hosts are configured with an internal IPv6 address (e.g. site-local or unique local). On the edge of the network, a router or firewall component is configured with a translation protocol called NPTv6. NPTv6 is a translation protocol that can translate the private internal organization prefixes to public global addresses. The translation mechanism is stateless providing a 1:1 relationship between the internal addresses and external addresses. Hence, no session state is created nor maintained on the router/firewall.

When to use: using global IPv6 addressing on the network

Description: If you are using global addressing, determine what global addressing assignment will be used. This is based on how you obtain the global address space that will be used for your hosts to access the Internet. Or to host network services that outside users can access from the IPv6 Internet. The options available are:

1. Provider Assigned (PA)
2. Provider Independent (PI)

Go through each option to view the description, caveats and when to use (or use-cases) to determine which option will work better in your environment based on your requirements.

#1

Provider Assigned (PA)

When to use: common for small, SMB, and medium-sized networks using a single service provider

Description: In this global assignment, the global address space is provided by the service provider that your network will connect to. The global address space can only be used with that service provider and no other provider that is used. The biggest advantage for using this global assignment option is that the service provider would deal with the development and managing the address space that is used.

Below are some caveats and considerations to keep in mind for this assignment option:

- Global address space can only be used with the connected service provider who provided the address space.
- If your network will be connected with two or more service providers, you will need to obtain another address space from the other service provider. This can lead to higher address management overhead. An alternative approach would be to use a provider independent (PI) assignment.

#2

Provider Independent (PI)

When to use: when an organization has a single global address space connecting with multiple service providers (multi-homing) to provide Internet redundancy.

Description: In this global assignment, the global address space is provided by the regional registry (e.g. ARIN, RIPE, APNIC) that can be used between multiple service providers. It isn't tied directly to a specific service provider like the PA assignment. This allows an organization to switch to a different ISP without re-addressing all of the global nodes on the network.

It's important to understand from the service provider what IPv6 prefix announcements can be accepted. Most providers have settled on a /48 as the longest prefix that is accepted from customers or peering partners.

If you are choosing a PI assignment it's important to determine from the service provider what IPv6 prefix policies do they have. Below are standard questions to ask:

- Do you accept IPv6 prefixes that has been obtained from a regional registry?
- What is the longest prefix length you will accept from customer networks?
- What is the longest prefix length you will accept from other service providers you are peering with?
- What is the longest prefix length your service provider peers will accept?

Furthermore, if an organization has presence across different countries they should get a PI assignment from their regional registry (e.g. ARIN), split up the address space, and advertise them through the country's service provider if the IPv6 prefix is long enough. Again it's important to communicate with the service provider on their policies.

There may be other policies by the regional registries for the length of the IPv6 prefix that can be obtained if justified. Below is the breakdown of ARIN's policy of IPv6 assignment based on the number of sites that exist for an organization:

- 1-12 sites: receive a /44 assignment
- 12 -192 sites: receive a /40 assignment
- 192 - 3,072 sites: receive a /36 assignment
- 3,072 - 49,152 sites: receive a /32 assignment

Note: It's important to view the current ARIN (and other regional registries) policies in regards to IPv6 address assignment and recommendations as this info may have changed. The other regional registries typically assign a /48 prefix to customers.

Below are some caveats and considerations to keep in mind for this assignment option:

- Understanding the service provider policy for what PI advertisements are accepted including what the peering partners will accept.

Step 6	IPv6 Addressing Interface-ID Assignment

Determine how the interface-ID will be assigned to the IPv6 address for a host. This can be assigned statically or dynamically based on the following options:

1. Static
2. Dynamic using SLAAC
3. Dynamic using DHCPv6

Go through each option to view the description, caveats and when to use (or use-cases) to determine which option will work better in your environment based on your requirements.

#1	Static

When to use: ideal for servers and network infrastructure components (e.g. routers, switches, firewalls)

Description: In this option, the interface-ID along with the network prefix is manually configured on the host.

When to use: ideal for the following use-cases (1) used for mobile environments. (2) used for printers, sensors, and access points. (3) guest network where clients are connected for a short period of time.

Description: Stateless Address Auto Configuration (SLAAC) is one dynamic method where the host is able to automatically assign an IPv6 address to itself. This process works when the node listens for route advertisement messages containing the IPv6 network prefixes. The node can use those network prefixes and build its own interface-ID dynamically. The following are the different SLAAC processes can be used to provide dynamic assignment of the interface-ID:

- EUI-64
- Privacy Extensions
- Secure Neighbor Discovery/Cryptographically Generated Address (SEND/CGA)

The biggest consideration to keep in mind about SLAAC is that the three processes only advertise network prefix information that the node can use to build its interface-ID. Below are caveats to keep in mind while using SLAAC:

- DNS server and domain information: the SLAAC processes do not advertise any DNS server or domain information to the hosts on a segment. This is a concern because DNS is extremely important in a IPv6 infrastructure with hosts and servers. This information can be advertised by adding stateless DHCPv6 onto the network.
- Does not provide IP address tracking and accounting making it complicated to track back a host based on its IPv6 address.

If you will use SLAAC for dynamic interface-ID assignment, determine which process should be used from the sub-sections below.

SLAAC using EUI-64

When to use: the most common of the three SLAAC dynamic options. This is ideal for the following use-cases (1) used for mobile environments. (2) used for printers, sensors, and access points. (3) guest network where clients are connected for a short period of time.

Description: In this SLAAC dynamic option, the MAC address of the host is used to build its interface-ID. It does this by performing two specific operations:

- The MAC address is split in half and "FFFE" is inserted in the middle
- The universal/local bit, the seventh bit in the first octet, is set to identify if the address is universally or locally administered.

Below are some caveats and considerations to keep in mind for this dynamic option:

- Does not send DNS server and domain information to the IPv6 host. It will require stateless DHCPv6 to be used on the network to advertise those details.
- Does not provide IP address tracking and accounting

SLAAC using Privacy Extensions

When to use: this is ideal for the following use-cases (1) used for communication with hosts on the IPv6 Internet. (2) to address privacy concerns for tracking a IPv6 host when the interface-ID doesn't change (e.g. EUI-64).

Description: In this SLAAC dynamic option, the interface-ID is randomly generated and used for a fixed period of time before a new pseudo random interface-ID is generated. Privacy extensions are used to address privacy concerns for tracking a IPv6 host when its interface-ID doesn't change in the case of the EUI-64 process.

Below are some caveats and considerations to keep in mind for this dynamic option:

- Does not send DNS server and domain information to the IPv6 host. It will require stateless DHCPv6 to be used on the network to advertise those details.
- Does not provide IP address tracking and accounting

SLAAC using SEND/SGA

When to use: recommended over EUI-64 if supported on the L3 network device (e.g. router, L3 switch) and IPv6 hosts providing increased security for the neighbor discovery process. Thus, EUI-64 is typically more common over SEND/CGA.

Description: In this SLAAC dynamic option, the interface-ID is randomly generated. SEND/CGA is used to validate the identity of the nodes for the neighbor discovery process. This can be seen as an equivalent to implementing passive interfaces and routing MD5 authentication with EIGRP/OSPF. For this process, it uses public/private keys and certificates to validate the identities of all nodes associated with the neighbor discovery process. SEND is a PKI-based mechanism that provides protection against router spoofing. And CGA is a mechanism that provides protection against layer 3 spoofing. The two mechanisms work together to provide extra security for the neighbor discovery process.

Below are some caveats and considerations to keep in mind for this dynamic option:

- Does not send DNS server and domain information to the IPv6 host. It will require stateless DHCPv6 to be used on the network to advertise those details.
- Does not provide IP address tracking and accounting
- Must be supported on both the L3 device (e.g. router, L3 switch) and IPv6 hosts
- Involves a higher level of administration compared to EUI-64

When to use: this is ideal for the following use-cases (1) when user accounting and IP tracking capabilities is important. (2) implemented with SLAAC to advertise DNS server and domain name information to hosts.

Description: The interface-ID can also be assigned using DHCPv6 providing more control on how the addressing is assigned. Below are two types of DHCPv6 services that can be used:

1. Stateful DHCPv6
2. Stateless DHCPv6

If you will use DHCPv6 determine which type will be used or supplemented with SLAAC from the sub-sections below.

Stateful DHCPv6

When to use: when user accounting and IP tracking capabilities is important

Description: In this dynamic option, a dedicated DHCPv6 server is responsible for handing out IPv6 addresses, DNS servers, and domain information to hosts on a network. This can provide many advantages such as tracking an IPv6 address and what is currently in use.

Stateless DHCPv6

When to use: implemented with SLAAC to advertise DNS server and domain name information to hosts.

Description: In this dynamic option, it is implemented with any of the SLAAC options (e.g. EUI-64) to dynamically provide DNS server and domain name information to the hosts.

Below are some caveats and considerations to keep in mind for this dynamic option:

- Does not hand out any IPv6 address information like in a stateful DHCPv6 deployment.
- Does not provide user accounting and IP tracking capabilities to the IPv6 network.

Overall Recommendations

It comes down to whether you want to have IP tracking and accounting capabilities on the IPv6 network. From the options listed the following are recommended choices you can consider if you are unsure of which one is the best option:

- **SLAAC using SEND/CGA or EUI-64 with Stateless DHCPv6**
 - Does not provide IP tracking and accounting capabilities
- **Stateful DHCPv6**
 - Provides IP tracking and accounting capabilities

If IPv6 communication will occur between other networks then routing is required which can be internal or external.

Determine the routing protocols that will be used on the network.

IGP (Internal): routing that is used internally (privately) on the network within the LAN, Data Center and with other sites across the WAN.

- **EIGRP**: when routing with multiple Cisco devices on the network.
- **OSPFv3**: when routing with multiple Cisco or non-Cisco devices on the network.
- **Static**: when routing with one or two devices. Or if no other routing devices exist on the network.
- **Connected**: when there are no other routing devices on the network and all subnet interfaces are configured on the same L3 device (e.g. L3-switch, router).

EGP (External): routing that is used for accessing the public network (Internet) including advertising public address information to internet providers for reachability.

- **BGPv4+**: when routing with an ISP using an owned (or lease) public subnet that will be advertised through the Internet. This includes Internet redundancy using the same Public subnet for hosts on the LAN or Data Center network. This is common for medium and large networks including hosting providers.
- **Static**: when routing to an ISP using a small subnet for communicating out to the Internet. Common for small and SMB sized networks.

Below are other best practices that can be designed and deployed with IPv6 services on the network:

- The case of the characters does not matter. Lower case "a" is the same as a capital "A", though lower case should be used.
- Do not use easily guessed interface-IDs like "DEADBEEF", "CAFE", or "COFFEE" for example to ensure it isn't found easily on a network scan.
- Below are some of the accepted ways that the IPv6 address can be shorten:
 - Leading zeroes within each 16-bit group can be omitted
 - Trailing zeroes within each 16-bit group must be represented
 - Successive fields of zeroes within a IPv6 address can be shortened down to "::". And it can only be used once
- Disable route advertisements on point-to-point connections (e.g. between LAN Core and LAN Distribution) using the command "ipv6 nd suppress-ra".
- Tune the ARP table by setting the timeout to 200 seconds matching the MAC-address aging timer (default) which is 200 seconds.
- Use general prefixes for easy management.
- Block the use of Microsoft Teredo.
- Configure IPv6 VTY access controls to use the management (loopback) interface only.
- Enable Neighbor Unreachability Detection (NUD).
- **Blocking Hop-by-Hop and Routing Header Type 0 Packets:** it's recommended to block potentially malicious traffic that could be directed towards the network itself such as the Routing Header Type 0 (RH0) and the Hop-by-Hop (HbH) values that can be set in the IPv6 Extension Header.

Below are recommendations for using IPv6 prefixes on the network:

/64 prefixes:

- Recommended for user and server networks.
- Required for SLAAC using SEND/CGA or EUI-64
- Required for ISATAP. Embeds the IPv4 address in the last 32-bits of the IPv6 address
- Embedded RP (RFC 3956)

/127 prefixes:

- Recommended for point-to-point connections between network devices which can help against ping-pong Network Discovery attacks.
- Only accommodates two IPv6 addresses.

/128 prefixes:

- Recommended for loopback addresses on network devices.

With the IPv6 design nearly completed, determine what IPv6 addressing schema will be used to provide address organization. The addressing schema can be based on the following aspects:

- **Locations:** the schema can include details about the location or site (e.g. locations, regions, city, sites)
- **Organization:** the schema can include details about the department or groups within an organization (engineering, sales, legal, etc)
- **Services:** the schema can include details about the services or functions that are used (voice, wireless, servers, etc)

Below are some IPv6 schemas that can be used:

#1

Schema #1

Description: this schema is heavily focused on the locations and service aspects for larger networks.

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZA] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
 - o X = 4 Bits to define regional prefix (0-F) ; /52
 - o Y = 4 Bits to define site prefix (0-F) ; /56
 - o Z = 4 Bits for service/function prefix (Users, Wireless, Voice, Guest, DMZ, Servers) (0-F) ; /60
 - o A = 4 Bits for subnet ID prefix ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::1161:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local (fd00::/8)
- 1 = Region #1 (e.g. North America)
- 1 = Site #1 (e.g. San Francisco office)
- 6 = Server network
- 1 = Server network - voice server farm
- aaaa:bbbb:cccc:1 = interface-ID of voice server

#2

Schema #2

Description: this schema is heavily focused on the location based on the country, state, and city for larger networks.

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZA] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
 - o X = 4 Bits to define country prefix (0-F) ; /52
 - o Y = 4 Bits to define state prefix (0-F) ; /56
 - o Z = 4 Bits to define city prefix (0-F) ; /60
 - o A = 4 Bits for service/function prefix (Users, Wireless, Voice, Guest, DMZ, Servers) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::1116:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local (fd00::/8)
- 1 = United States (US)
- 1 = California
- 1 = San Francisco office
- 6 = Voice server network
- aaaa:bbbb:cccc:1 = interface-ID of voice server

#3

Schema #3

Description: this schema is heavily focused on the organization or type including the service aspects

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZZ] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
 - o X = 4 Bits to define type prefix (building/department, infrastructure, site) (0-F) ; /52
 - o Y = 4 Bits to define organization/department prefix (0-F) ; /56
 - o ZZ= 8 Bits for service/function prefix (Users, Wireless, Voice, Guest, DMZ, Servers) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::1106:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local (fd00::/8)
- 1 = Building/Department type network
- 1 = Engineering department
- 06 = QA server network
- aaaa:bbbb:cccc:1 = interface-ID of QA server

#4

Schema #4

Description: this schema is heavily focused on the location, organization and service aspects.

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XYZZ] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
 - o X = 4 Bits to define site code prefix (0-F) ; /52
 - o Y = 4 Bits to define organization/department prefix (0-F) ; /56
 - o ZZ = 8 Bits to define service/function prefix (Users, Wireless, Voice, Guest, DMZ, Servers) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::106:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local (fd00::/8)
- 1 = Site #1
- 06 = Engineering department
- 06 = QA server network
- aaaa:bbbb:cccc:1 = interface-ID of QA server

#5

Schema #5

Description: this schema is heavily focused on the service aspects in a smaller network.

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XXZZ] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
 - o XX = 8 Bits to define site code prefix (0-F) ; /52
 - o ZZ = 8 Bits to define service/function prefix (Users, Wireless, Voice, Guest, DMZ, Servers) (0-F) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::0106:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local (fd00::/8)
- 01 = Site #1
- 06 = Voice server network
- aaaa:bbbb:cccc:1 = interface-ID of voice server

Description: this schema is heavily focused on the service aspects in a smaller network.

Schema: [IPv6 network prefix] [IPv6 subnet prefix = XXXX] [Interface-ID] /64

- [IPv6 network prefix] - this can be a global prefix, unique-local prefix, or site-local prefix
- [IPv6 subnet prefix]
 - XXXX = 16 Bits to define service/function prefix (Users, Wireless, Voice, Guest, DMZ, Servers) ; /64
- [Interface-ID] - this is the unique host ID

Example: fd00::6:aaaa:bbbb:cccc:1

- fd00 = this is a private IPv6 address using a unique-local (fd00::/8)
- 6 = Voice server network
- aaaa:bbbb:cccc:1 = interface-ID of voice server

Resources

Below are the IPv6 addresses or prefixes that are reserved:

- ::1 - Reserved for the loopback interface (RFC 4291)
- ::- Unspecified address (RFC 4291)
- 2002::/16 - For 6to4 automatic tunneling (RFC 3964)
- 2001::/32 - For the Teredo tunneling mechanism (RFC 4380)
- ff02::1- Link local, all nodes Multicast address
- ff02::2 - Link local, all routers Multicast address
- ff02:0:0:0:1:ffXX:XXXX - Link local, solicited-node Multicast address

The L bit is set to 1 if the address is locally assigned. RFC 4193 reserves the 0 bit for future usage:

- fc00::/8—Reserved for future usage
- fd00::/8—Locally assigned unique local addresses

In-Service Software Upgrade (ISSU)

Category: Network Service (Network Management)

Prerequisite(s): Cisco Catalyst 4500/6500/6800, Cisco Nexus 7000 (Hardware)

In-Service Software Upgrade (ISSU): a software capability that allows doing an OS upgrade on Cisco L3-switches without bringing down the entire switch. It allows for a new software version to be tested and verified before completing an upgrade to a Cisco switch. Full image ISSU requires a dual supervisor environment which is well suited for single points of failure in the access layer.

This feature is supported on the Cisco Catalyst 4500, 6500, and the Nexus 7000 series.

Intrusion Prevention

Category: Network Service (Security)

Prerequisite(s): Intrusion Prevention (under Solutions)

SEC

Intrusion Prevention Services can identify, classify, and stop threats such as worms, network viruses, application threats, system intrusion attempts, and application abuse. The IPS solution can be consolidated using software (IOS) within a router platform if there is minimal traffic and enough memory on the router. This may include additional hardware modules to add to the router to provide IPS services.

Recommendations: Using IPS functions on a router is ideal for small, SMB, and some medium size networks. It is recommended to use a dedicated IPS daughter-card which acts for like an IPS accelerator and offload's the IPS operations to a dedicated module. If traffic conditions tend to be higher than using a dedicated IPS appliance is strongly recommended.



~ Services ~

Layer 2 Multi-Path (L2MP)

Category: Network Service (Routing and Switching)
Prerequisite(s): Cisco Nexus 5000 (Hardware)

Layer 2 Multi-Path (L2MP): allows switches to use multiple L2 paths for switching traffic rather than using a single path. Provides fast convergence if failures occur within the switching network. Supported on the Cisco Nexus 5000 platform.

Layer 2 VPN (L2VPN)

Category: Network Service (Tunneling)

Prerequisite(s): Network Virtualization (under Solutions)



Determine the L2VPN service that would be used in the design:

- **L2TPv3:** creates an isolated point-to-point L2 tunnel between two sites.
 - L2TPv3 tunnels can be static or dynamic.
 - L3VPN can be used over L2TPv3 tunnels.
- **VPLS:** creates isolated point-to-multipoint L2 tunnels between sites. To maximize the forwarding memory and CPU resources on the MPLS PE devices use a few number of sites and a large number of networks/prefixes (e.g. several hundred) instead.
- **VPWS:** creates an isolated point-to-point L2 tunnel between two sites.
- **EoMPLS:** extends Ethernet or L2 services (e.g. VLANs) across an existing MPLS network. Commonly used and recommended for L2 tunneling services between two WAN Core locations.
- **Local Switching:** creates a L2 tunnel between an Ethernet port and a serial/T1 port.

Recommendations: use L2VPN if you want the ability to extend L2 services like VLANs across a L3 network. This type of solution is usually deployed on a Service Provider network and less likely on a customer's network. It's a matter of asking the provider if they offer any point-to-point or point-to-multipoint L2VPN services. Also the hardware requirement for using L2VPN requires high-end routers not feasible for small, SMB, or Medium networks who want to use L2VPN within their own network.

Locator/ID Separation Protocol (LISP)

Category: Network Service (DCI)

Prerequisite(s): Data Center, WAN (under Solutions)

When to use: A Data Center Interconnect (DCI) to provide better mobility and resiliency for networks at a site that may move to a different ISP network with minimal configuration and downtime. Below are other use-cases for LISP:

- Used as a mechanism for transiting between IPv4 to IPv6

LISP provides many advantages for Data Center networks that include:

- Provides Host/VM mobility (for IPv4 and IPv6) by using the shortest routing path to the end system
- Provides the ability to move devices to a different ISP without requiring any re-addressing
- Using LISP doesn't require a large routing table with uses more memory resources. Only a default route is required.
- Allows for IPv6 Internet Access when the ISP doesn't natively offer it.
- More flexible for applying unique security policies
- Provides EID and RLOC virtualization

#1

Overview

LISP is like a name server used by a router to get routing information. Similar to how DNS is a name server used by a computer, server, or any IP device. Before I get into the details let me expand on this further. In a DNS model, we have a DNS Server and we have DNS clients. The DNS clients will be your computer, a server, a router, or anything that has an IP address configured. These DNS clients will point to a DNS server to provide name resolution for reaching websites or servers. The DNS server has records which contains a domain name mapping to an IP address.

For LISP it is very similar, but with different components. So, in a LISP model, we have a LISP server and we have LISP clients. The LISP clients will be routers enabled and configured for LISP services. These LISP clients would point to a LISP server to provide IP address lookup for reaching a specific network. The LISP server has records which contains a network mapping to a WAN facing IP address of a LISP client router.

This means, using LISP, we have the ability to move devices to a different ISP without requiring any re-addressing. The only thing required would be to update the LISP records pointing to the new IP of the site. With LISP, only a default route is required. So we don't need to have a large routing table requiring higher memory. A typical routing table is estimated around 350,000 routes. If a route to a destination is not known on a LISP router then it will do a query to the LISP server, which is more formally called the map resolver.

LISP has several components and terminology that is important to understand for its configuration. The first component is the LISP router types. A router supporting LISP can either be a LISP client or a LISP server.

Now those aren't the official terms used, so a LISP client router can be configured as a:

- **Ingress Tunnel Router or an ITR**, which is responsible for encapsulating an IP packet from the internal network into a LISP packet out to the WAN.
- **Egress Tunnel Router or an ETR**, which is responsible for removing an encapsulated LISP packet that is received from external hosts from the WAN facing interface of the router packet to an IP packet
- Or it can be configured as an **ITR and ETR called an xTR**. x meaning ingress and egress.

Most LISP client routers will typically be an xTR device.

A LISP server can either be a map server, a map resolver, or it can be configured for both which is typically how it is deployed.

There are other LISP components that are important which would be the:

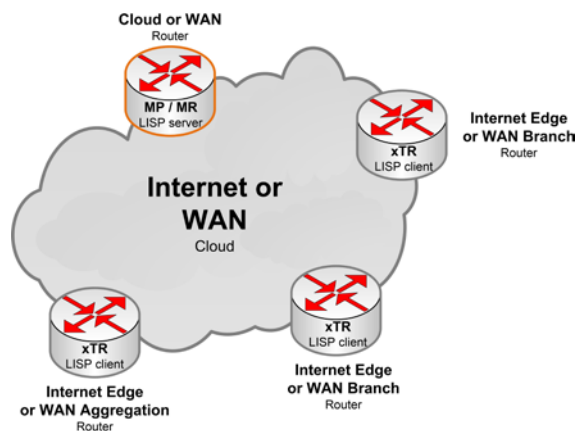
- **Endpoint Identifier (EID):** The EID would be a the network prefix that exist within the LAN or Data Center behind the xTR. This EID prefix would be registered with the LISP map server
- **Routing Locator (RLOC):** The RLOC is the outside or WAN facing interface IP address of the ETR. This would be the IP address that would be provided for how to reach the registered EID prefix.

Therefore, it is the map server that builds the EID-to-RLOC mapping. It is the ETR component that is responsible for registering its EID prefixes with the map server. And the map resolver deals with handling queries from the ITR components when resolving EID-to-RLOC mappings. Map resolver would act as the DNS server in the network environment.

#2	Components in LISP Topology

Below are the components used in the service and how they are deployed:

- **LISP Server Component:** this will be a Cisco router device that will act as the LISP map server and map resolver. It can be connected into the network in one of the following ways:
 - o Using a cloud based router (e.g. Cisco CSR 1000V) that is attached to the Amazon EC2 cloud.
 - o Using a dedicated Cisco router or the WAN router that is connected to the WAN (L3 WAN, Internet WAN) to provide the LISP server operations.
 - o Using a dedicated Cisco router or the Internet edge router that is connected to the Internet to provide the LISP server operations.
- **LISP Client Component:** this would be the Internet Edge routers or WAN routers (aggregation, branch) connected to the Internet WAN or L3 WAN cloud. They would operate as a LISP xTR which is comprised of both ITR and ETR functions. The LISP client components would connect to the LISP server component for resolving and connecting with other sites.



#3	Caveats

Below are some caveats to keep in mind while using this service:

- Does not provide data encryption, only data encapsulation

#4	Add-Ons

Below are other common technologies that can be implemented or overlay with LISP:

Technology	Description	Prerequisite(s)
OTV and LISP	OTV can be implemented with LISP to provide a robust shortest routing path method for extending VLANs between Data Centers.	OTV
GET VPN over LISP	GET VPN can be implemented on-top of LISP to provide encryption. The crypto map can be applied to either the EID facing interface which is created as a LISP0 virtual interface. Or the crypto map can be applied to the RLOC facing interface(s). Between the two applying crypto maps to the LISP0 virtual interface is common for implementing GET VPN over LISP. When crypto services are applied to the LISP0 interface, GETVPN encryption happens first followed by LISP encapsulation. LISP is deployed as the framework between all sites without encryption. GET VPN is built on-top of the LISP topology providing tunnel-less encryption between sites.	LISP [Service]
Virtualization	The EID and RLOC namespaces can be virtualized within a LISP topology. -EID virtualization: Mapping a LISP Instance-ID to an EID VRF enables EID virtualization. This is also referred to a LISP shared model because many EID namespaces are segmented by VRFs and the Instance-IDs share a common RLOC. Instance-IDs are numerical tags used to maintain EID address space segmentation in the control plane and data plane. -RLOC virtualization: multiple RLOCs can be segmented by VRFs. This can allow many EID namespaces to be mapped to a specific RLOC.	

Loop Guard

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)

Enabled globally on all Access switches and the Core switch to prevent a blocked port from transitioning to listening after the MaxAge timer has expired. This should be implemented if Bridge Assurance is not supported on the switch.

Cisco Nexus Best Practices: Loopguard should be enabled globally on all Access switches if Bridge Assurance (BA) is not supported.

M

~ Services ~

MAC-in-MAC

Category: Network Service (Routing and Switching)

Prerequisite(s): Data Center Solution, Virtualization (Server) Solution

Below are some of the main aspects of MAC-in-MAC encapsulation:

- VMware has an existing proprietary equivalent to VXLAN. It is deployed today with vCloud Director called vCloud Director Network Isolation (vCDNI).
- vCDNI uses a MAC-in-MAC encapsulation.

Medianet

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN Solution, Voice and/or Video Solution

When to use: Cisco Medianet technologies is recommended for video and voice deployments

Cisco Medianet has many capabilities such as media monitoring and awareness to provide increased visibility for the voice engineer. This provides proactive management and troubleshooting of network resources.

The Cisco Medianet media monitoring capabilities consist of Performance Monitor, Mediatrace, and using the IP SLA Video Operation (VO). These capabilities can provide monitoring the faults and quality of voice/video calls across the network. It can discover the path of voice/video traffic across the network and provide a detailed hop-by-hop analysis of the media flows. And it can provide capacity planning and troubleshooting before voice/video applications are deployed in the production network.

The Cisco Medianet media awareness capabilities consist of Flow Metadata, the Media Services Interface (MSI), and the Media Services Proxy (MSP). These capabilities can provide deep inspection of the voice/video signaling across the network and it can be configured with QoS.

MPLS VPN

Category: Network Service (Tunneling)
Prerequisite(s): Network Virtualization (under Solutions)



MPLS is a L3VPN solution that provides great scalability of VRF instances for large networks. MPLS support is limited to high-end network hardware like the Cisco Catalyst 6500 series and the Cisco 7200 series among others. Build the MPLS VPN design based on the following steps:

Step 1	Components in MPLS Topology

#1	Determine the components for MPLS

Below are the components that should be identified within the topology that will use MPLS:

- **P Router:** a router that connects to a PE router(s) and to other P routers making up the MPLS Backbone. VRF's are not configured on the P routers only LDP is configured for extending the MPLS tags between the PE routers. The MPLS P router is usually the LAN/Data Center Core or the WAN Aggregation.
- **PE Router (VRF):** a router that connects to the MPLS P router and to the CE router (customer equipment). The VRF instances are configured directly on the PE routers and uses MP-BGP for communicating with other PE routers to exchange VRF routing information. The MPLS PE router is usually the Distribution/Aggregation or the WAN branch router.
- **CE:** this is the customer equipment, which can be a router or switch. This device is not configured or aware of MPLS in any way.

#2	Determine the service components

Below are the services and protocols that are required for deploying MPLS:

- **VRF:** Each network that is virtualized is configured as a VRF creating a separate routing table instance separate from other networks by default. The VRF can be associated to a VLAN SVI or any L3 interface. Determine what the virtualized networks will be such as Internal, Guest, and/or Development. The VRFs are only configured on the PE routers.
- **LDP:** label distribution protocol configured on all MPLS P and PE router interfaces used for forwarding labels between the MPLS devices.
- **IGP:** an IGP routing protocol (EIGRP or OSPF) is required on the network between the MPLS P and PE devices in order for the MPLS PE routers to establish MP-BGP sessions.
- **MP-BGP:** IBGP peers is required between all MPLS PE routers for exchanging VPNv4 route information for a VRF instance. Use the loopback interfaces for peering between the MPLS PE routers.

Step 2	Services

#1	Quality of Service (QoS)

The ISP will use one of the following QoS mechanisms on the MPLS network if the CE/C devices will mark packets within the network and will be sent through the MPLS WAN. It's important to understand which MPLS DiffServ Mode will be implemented and how the CE/C device marked packets will be treated through the MPLS network.

- **Uniform Mode:** default MPLS QoS operation. When the service provider and the CE are part of the same DiffServ domain.
- **Short Pipe Mode:** the service provider and the CE are part of different DiffServ domains.
- **Pipe Mode:** same as Short Pipe mode, but the PE egress policies towards the CE is provisioned according to the service provider's explicit markings.

#2	Multicast

Below are design considerations if Multicast will be used over MPLS.

- **Data Multicast Distribution Tree (MDT):** to avoid unnecessary multicast flows to bandwidth-sensitive remote sites.
- Use PIM SSM or PIM Sparse Mode when using MPLS over L2 (e.g. EoMPLS).
- Use PIM SSM or Bi-Directional PIM when using MPLS over DMVPN.
- Use Anycast RP as it's RP configured on the LAN Core/MPLS Core.
- Use PIM NBMA for DMVPN per VRF or MPLS over DMVPN.
- Use MPLS MTU to deal with increased IP packet sizes that may exist.

Below are other common technologies that can be implemented or overlay with MPLS:

#	Technology/Feature	Description	Prerequisite(s)
1	MPLS over GRE	Used to connect two MPLS networks together via GRE. Commonly used and recommended for tunneling services between two Large WAN locations.	GRE
2	MPLS over DMVPN	Used to connect two MPLS networks together over DMVPN across the Internet.	DMVPN [Service]
3	MPLS over L2TPv3	Used to connect two MPLS networks together over L2TPv3 (L2VPN).	L2VPN [Service]
4	Route Reflectors	It's a <u>best practice</u> for all PE routers to peer via IBGP with a dedicated BGP router configured as a route reflector. This provides better scalability, management, and redundancy with the IBGP peering which is required between the PE routers. The RR routers would be connected into the Core.	--
5	Extranet	Used to route between other VRF instances.	--
6	Traffic Engineering	Provide IntServ QoS by creating tunnels along the LSP through the MPLS network. <u>RSVP services is required</u> for configuration to implement TE services. The TE tunnels can either be: • Static: configured along a specified LSP (path) through specific MPLS routers and interfaces. • Dynamic: dynamically configures a TE tunnel through the MPLS network based on available bandwidth resources (RSVP).	--
7	VRF Selection	Used to support multiple VRFs on a single interface.	--

Below are further design details based on the table above:

#4	Route Reflectors Topologies

It's a best practice for all PE routers to peer via IBGP with a dedicated BGP router configured as a route reflector. This provides better scalability, management, and redundancy with the IBGP peering which is required between the PE routers. The RR routers would be connected into the Core.

Larger MPLS networks using Route Reflectors can be deployed in two ways.

- **Option A:** In this option there are redundancy RR routers separated across two sites. The primary peering for the PE routers will be the local RR at their site and the secondary peering will be the RR at the other site.
- **Option B:** In this option there are two RR routers at each location (total of 4). All MPLS PE routers located at one site will peer with the primary and secondary RR at their local site. Then the RR routers at each site will peer with the RR routers at the other sites.

Step 4	Best Practices and Considerations

Below are general best practices for using MPLS services on the network.

- **VRF RD Naming Standard:** it is recommended to create a naming standard for naming the VRF Route Distinguishers (RD) on the network.
- **MPLS MTU:** leverage the MPLS MTU feature to deal with increased IP packet sizes and set the MTU for labeled packets if GRE interfaces are used.
- **MTU:** the safest and recommended MTU to use for GRE interfaces to avoid fragmentation is 1392 bytes (for unicast) or 1368 bytes (for multicast). This is applicable when using MPLS over DMVPN.

Below are other considerations to keep in mind:

#1	VRF and Voice

Voice and VRF are not supported on the same router platform, it has to be separated or configured not to use both. Below are some option if using voice and VRF together on the same network:

- **Option 1:** VRF and VPN services are terminated to one router (WAN Router) then another router (Core Router) is configured for Cisco CallManager Express (CME). The uplink interface on the CME router connects into a port on the VRF/VPN router that is assigned to the Voice VRF.
- **Option 2:** Use a single WAN branch router where VRFs exist for all networks except for Voice, which is not in a VRF.

Recommendations: From the two options presented option 2 would be recommended because the Voice network is usually local for a remote site and doesn't need to be extended in a VRF across the WAN. Plus it avoids managing two routers at the remote site increasing the complexities involved.

Multicast, IP

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN, WAN, and/or Data Center (under Solutions)

When to use: to provide efficient data, voice, and video delivery for supported services/applications across the network. Recommended to be implemented when using voice and video solutions within the LAN.

Complete the steps below if Multicast services will be implemented in the design:

Step 1

Identify Components

DA SC

Determine the multicast components on the network based on the following:

- **Source (Server):** the system(s) that is streaming the actual data using a multicast address.
- **Receiver (Member):** a node or host that will receive the data via multicast.
- **L2, L3, L2/L3 devices:** identify all L2 and L3 network devices on the network.

Step 2

Multicast Topology

DA SC

Determine which Multicast topology will be used on the network:

- **Any Source Multicast (ASM):** Multicast receivers on the network can receive multicast data from any source/server that is streaming traffic. This model can build a shared or source tree across the network. For shared multicast trees, it requires using a Rendezvous Point (RP). When a receiver wants to receive specific traffic they only need to use the provided Multicast IP Address. This model is used for most networks that don't require which source is streaming traffic.
- **Specific Source Multicast (SSM):** Multicast receivers on the network can only receive multicast data from a specific source/server that are streaming traffic. When a receiver wants to receive specific traffic they need to use the provided IP address of the Source/Server and the Multicast IP Address. This model does not build a shared tree nor requires a Rendezvous Point (RP). Offers more restrictions and security that a receiver has to specify which source/server it wants to receive data from. And not from any source/server that is streaming data.

Depending on the Multicast topology determined, choose which Multicast Routing Protocol will be implemented on the network:

Any Source Multicast (ASM):

In order to receive a particular IP multicast data stream, endpoints must join a multicast group by sending an IGMP message to their local multicast router. The local router will consult another router acting as the Rendezvous Point (RP) to map the receivers to active sources so they can join their data streams. The RP is a control plane operation that should be placed at the Core or close to the multicast sources on a pair of Layer 3 switches.

- **Protocol Independent Multicast Sparse Mode (PIM-SM):** recommended multicast routing protocol. PIM-SM was used when minimal bandwidth and resources were available which is not true for networks today. This is implemented on all L3 devices on the network and requires Rendezvous Point (RP) management.
- **Bi-Directional PIM:** used when there are applications doing real-time streaming (e.g. trading) for thousands of members throughout the network. Each source sends multiple streams. Bi-Directional PIM is often used by large networks or environments with many-to-many (multiple sources, multiple members) scattered throughout the network. This is implemented on L3 devices and requires Rendezvous Point (RP) management.

Source Specific Multicast (SSM):

- **PIM Source Specific Multicast (PIM-SSM):** Multicast receivers on the network can only receive multicast data from a specific source/server that are streaming traffic. When a receiver wants to receive specific traffic they need to use the provided IP address of the Source/Server and the Multicast IP Address. This model does not build a shared tree nor requires a Rendezvous Point (RP). Used for high-traffic, audio/video streaming, and one-to-many (one source with many members) environments. Ideal for large networks or if using a DMVPN solution. This is implemented on all L3 devices. Using PIM-SSM requires IGMPv3 and using the Multicast Address range of 232.0.0.0/8.

When to use: using a ASM topology and a multicast routing protocol that requires a Rendezvous Point (RP).

Below are best practices for how the RP should be designed and configured:

- Use Anycast RP to provide RP scalability and redundancy.
- MSDP is required to provide RP redundancy on the network.
- Discover the IP Multicast RP using **"autorp"**. Auto RP is used to announce candidate RPs.
- Use a loopback interface for the RP address. It should be configured as a host address mask (32 bits).
- **"send rp announce"** is used to advertise the RP address with the Multicast range the router is willing to serve as a candidate RP to the Auto RP mapping agents. The Auto RP mapping agent listens for candidate RPs and then advertises across the network the list of available RPs.
- The RP location including MSDP should be configured on the LAN Core (or Data Center Core) running PIM-SM and Anycast RP. Enable PIM-SM on all L3 devices pointing to the Anycast RP IP address which is configured of the Core switches. If you are using a single Core switch it's recommended to use Auto-RP on the network
- MSDP should be configured between the two LAN/Data Center Core switches to provide fast convergence if one of the RPs fails.

Below are the RP types that can be used on the network:

- **Static RP:** used for multicast networks by specifying the RP router statically on a multicast enabled L3 device that is part of the shared tree network (e.g. PIM-SM). The static RP is usually deployed on the Core. Using static RPs will increase the administration required for the multicast network, but it is ideal for small, SMB, and medium sized environments.
- **Auto RP:** used for multicast networks to provide auto-RP (used in IPv4) for dynamic RP management. This is used and supported on networks using Cisco hardware. This is ideal for medium to large networks (including small or SMB) for better administration, flexibility, and scalability for managing the RP on L3 devices on the multicast network.
- **Bootstrap Router (BSR):** used for multicast networks to provide Auto-RP (used in IPv4 networks) for dynamic RP management. This can be used with Cisco and other vendor devices which is an industry standard protocol. This is also recommended for IPv6 Multicast environments used for dynamic RP management where Auto-RP is not supported with IPv6.
- **Multicast Source Discovery Protocol (MSDP):** used when connecting to other multicast (RP) domains. MSDP can be used to provide multicast redundancy within a multicast network using an Anycast RP. This is configured between the Core (LAN or Data Center) devices and synchronizes the SA states between them.
- **Embedded RP:** used with IPv6 multicast networks that need to route across domain boundaries like remote sites on the WAN.
- **Anycast RP:** provide multicast redundancy and to load balance the RP allowing for fast failover. This is configured between the Core (LAN or Data Center) devices and includes configuring MSDP.

Step 5

Group Membership Management

Determine the group membership management protocol to use on the network. The group membership is responsible for multicast group memberships and forwarding of multicast data.

- **Internet Group Management Protocol (IGMP):** used for IPv4 networks that will use Multicast for the source and receivers on the network. This is used on L3 devices enabled for multicast. This will either be IGMPv2 or IGMPv3 (required for PIM-SM).
- **Multicast Listener Discovery (MLD):** used for IPv6 networks that will use Multicast for the source and receivers on the network. This is used on L3 devices enabled for multicast.

Step 6

Multicast Support at Layer 2

A multicast mechanism that can forward multicast data to only the switch ports with connected members that requested the multicast stream freeing network resources and bandwidth. Without these mechanisms a multicast stream would be forwarded to all ports on a switch. This is a best practice and recommended to be configured. Below are the mechanisms that will provide multicast support on layer 2 devices.

- **Snooping (IGMP, MLD):** recommended when using IGMP (or MLD) for the group membership management protocol.
- **Cisco Group Management Protocol (CGMP):** used on older L2 switches that does not support IGMP snooping. CGMP needs to be enabled on the interface for that subnet on the L3 device.

Multicast deployment with IPv6 can be done using one of the following solutions:

(1) **Any Source Multicast (ASM):** used when multicast sources are not always located in the Data Center and using well-known addresses. Below are some of the design specifics:

- Recommended for IPv6 networks.
- Uses PIM-SM and MLDv2 for multicast routing and Group Membership.
- Uses BSR for delivering the RP-to-group mapping information within the LAN/Campus or Data Center.
- Uses Embedded RP for multicast traffic routing across domain boundaries with remote sites (if using WAN).
- Use OSPFv3 in the LAN and eBGP to exchange routing info with the remote sites and the Internet for BGP.
- Use BSR to block multicast flooding beyond the Internet Edge router's WAN interface.
- Configure the Candidate RP routers to advertise their willingness to be the RP for certain multicast groups.

(2) **Source Specific Multicast (SSM):** used for content distribution on the multicast network.

When to use: using a ASM topology

Mechanisms for providing additional security to the Multicast environment:

- **Rogue Source Protection:** configure "Accept Register" to allow what valid sources and multicast group addresses should register with the RP.
- **Rogue RP Protection:** configure IGMP group access control for what multicast groups members/receivers can join.
- **Auto-RP Protection:** configure an RP Announce Filter for valid RPs and multicast group addresses that should be used on the network.

Below are design considerations if Multicast will be used over VPN tunnels.

- Use GRE tunnels encrypted by IPSec VPN for multicast to work over VPN tunnels.
- Use PMTU which will dynamically discover the smallest MTU size to use to avoid high fragmentation.
- Use administratively scoped addresses (239.0.0.0/8) to differentiate multicast applications based on the type and bandwidth of the stream.
- Use the Anycast RP (located on the Core).
- Use IGMP snooping and/or CGMP on all switches.
- Use IP multicast boundaries to control where certain multicast traffic can go.

Below are design considerations for deploying Multicast within the LAN or Data Center that have redundant Core/Distribution switches:

- The Core or Distribution/Aggregation L3-switch with the highest address on the segment will be the PIM Designated Router (DR)
- The Core or Distribution/Aggregation L3-switch with the lowest address on the segment will be the IGMP querier.

The PIM DR and IGMP querier functions (using IGMPv2/v3) do not exist on the same switch unless a single Core/Aggregation switch is used.

Below are design considerations if Multicast will be used over the WAN.

- Use administratively scoped addresses (239.0.0.0/8) to differentiate multicast applications based on the type and bandwidth of the stream.
- Use the Anycast RP (for the WAN Aggregation and branch routers)
 - Use PIM-SM for Multicast routing
 - Identify the RP for each WAN router using the Anycast RP located on the Core.
- Use IGMP snooping and/or CGMP for all switches.
- Use IP multicast boundaries to control where certain multicast traffic can go.
- MSDP filters: should be applied if the network is connected to an IP Multicast domain on the Internet. MSDP filters are used to reduce the excessive amount of (S,G) states that is passed between the MSDP peers.

Below are design considerations if Multicast will be used over MPLS.

- **Data Multicast Distribution Tree (MDT):** to avoid unnecessary multicast flows to bandwidth-sensitive remote sites.
- Use PIM SSM or PIM Sparse Mode when using MPLS over L2 (e.g. EoMPLS).
- Use PIM SSM or Bi-Directional PIM when using MPLS over DMVPN.
- Use Anycast RP as it's RP configured on the LAN Core/MPLS Core.
- Use PIM NBMA for DMVPN per VRF or MPLS over DMVPN.
- Use MPLS MTU to deal with increased IP packet sizes that may exist.

Below are design considerations if Multicast will be used over Wireless.

- Use IP multicast boundaries to control where certain multicast traffic can go. This is implemented on the egress L3 interface connected to the Wireless network.
- Wireless user traffic should exist in a separate subnet (VLAN) on the network.

Below are other best practices that can be designed and deployed with Multicast services on the network:

- Use administratively scoped addresses (239.0.0.0/8) unless PIM-SSM is used which requires 232.0.0.0/8 addresses.
- Tune PIM query internal timers to 1 second.
- For Auto-RP tune the PIM RP announce internal timer to be between 3 to 5 seconds (default is 60 seconds).
- Keep multicast traffic on the shared path (optional). This will reduce the number of multicast states (S,G) from the leaf routers by keeping traffic on the shared tree.
- Multicast Fast Drop (MFD) should be enabled to rate limit non-RPF traffic. Many cases it is enabled by default.
- Enable Anycast and MSDP for fast recovery of IP Multicast traffic.
- Place multicast sources on separate VLANs.

Resources

- **224.0.0.1**: Sent to all nodes on a subnet
- **224.0.0.2**: Sent to all routers on a subnet
- **224.0.0.5**: Sent to all OSPF routers
- **224.0.0.6**: Sent to all OSPF Designated Routers (DRs)
- **224.0.0.9**: Sent to all RIPv2 routers
- **224.0.0.10**: Sent to all EIGRP routers
- **224.0.0.13**: Sent to all PIMv2 routers
- **224.0.0.22**: Sent to all IGMPv3 devices
- **232.0.0.0/8**: used for PIM-SSM
- **239.0.0.0 – 239.255.255.255**: Administrative scoped addresses
 - o **239.192.0.0 – 239.251.255.255**: Organizational-local scope used within private/internal networks
 - o **239.255.0.0 – 239.255.255.255**: Site-local scope isolated within a site/region

RP Memory Considerations: Consider the memory impact for the selected RP router in the environment based on the following:

- **Each (*,G)** entry requires 380 bytes + 150 bytes per outgoing interface
 - *Formula: (# of multicast groups) x (380 + (# of outgoing interfaces x 150))*
- **Each (S,G)** entry requires 220 bytes + 150 bytes per outgoing interface
 - *Formula: ("# of multicast sources" x "# of multicast groups") x (220 + (# of outgoing interfaces x 150))*

For example, let's say that on our RP we will have 20 multicast groups with 3 sources per group and 6 outgoing interfaces on our RP router. Below would be our memory resource requirements that are needed:

- **# of (*,G):** $(20) \times (380 + (6 \times 150)) = 25,600$ bytes
- **# of (S,G):** $(3 \times 20) \times (220 + (6 \times 150)) = 67,200$ bytes

Therefore, our RP router will need at least 92,800 bytes of memory for the multicast routing table (mroute).

Multi-CE VRF (VRF-lite)

Category: Network Service (Tunneling)
Prerequisite(s): Network Virtualization (under Solutions)



VRF-lite is a L3VPN solution that creates isolated L3 segments without the need of MPLS. This is the most common L3VPN design mainly due to the hardware support. VRF-lite is supported on a lot of hardware (that is affordable) such as the Cisco ISR series. MPLS which has limited hardware availability, but in fairness MPLS is ideal for large L3VPN deployments. Build the VRF-lite design based on the following steps:

Step 1

Components in VRF-lite Topology

#1

Determine the components for VRF-lite

Below are the components that should be determined with the VRF-lite design:

- **Zone Router:** a router which is not enabled for VRF and contains all routes on the network connecting to a firewall for each VRF on a VLAN. This is used for routing between other networks forcing them to route through the firewall for policy enforcement. This will likely be a separate device that is plugged directly into the Core switch (LAN or Data Center).
- **Firewall:** security appliance that is connected between the LAN (or Data Center) and the Zone router to provide policy protection for what users in one VRF can access in another VRF. Make sure the firewall supports 802.1Q.
- **CE (VRF):** All L3-switches in the network (LAN or Data Center) is created as a CE device where the PE roles has been pushed down to the CE component. All VRF instances (the virtual networks) is configured on the CE devices. The CE device can be the LAN Distribution (or Data Center Aggregation), LAN Core (or Data Center Core), or the WAN Aggregation.

#2

Determine the service components

Below are the services and protocols that are required for deploying VRF-lite:

- **VRF:** Each network that is virtualized is configured as a VRF creating a separate routing table instance separate from other networks by default. The VRF can be associated to a VLAN SVI or any L3 interface. Determine what the virtualized networks will be such as Internal, Guest, and/or Development. The VRFs are only configured on the CE/PE routers.

Step 2	Add-Ons

Below are other common technologies that can be implemented or overlay with VRF-lite:

Technology	Description	Prerequisite(s)
DMVPN per VRF	Used to extend a VRF across a DMVPN network using VRF-lite (Multi-VRF CE). The WAN Aggregation is configured as the CE/PE device.	Virtualization (Network) [Solution]
GET VPN per VRF	Used when implementing VRFs (VRF-lite) over the GET VPN network.	Virtualization (Network) [Solution]

Step 3	Best Practices and Considerations

#1	VRF and Voice

Voice and VRF are not supported on the same router platform, it has to be separated or configured not to use both. Below are some option if using voice and VRF together on the same network:

- **Option 1:** VRF and VPN services are terminated to one router (WAN Router) then another router (Core Router) is configured for Cisco CallManager Express (CME). The uplink interface on the CME router connects into a port on the VRF/VPN router that is assigned to the Voice VRF.
- **Option 2:** Use a single WAN branch router where VRFs exist for all networks except for Voice, which is not in a VRF.

Recommendations: From the two options presented option 2 would be recommended because the Voice network is usually local for a remote site and doesn't need to be extended in a VRF across the WAN. Plus it avoids managing two routers at the remote site increasing the complexities involved.

N

~ Services ~

Network Address Translation (NAT)

Category: Network Service (Routing and Switching)
Prerequisite(s): Firewall and/or Internet Edge (under Solutions)



When to use: when translating one IP address to another address.

NAT is a protocol used to translate one IP Address to another address. This is needed if hosts (servers or desktops) need external access to the Internet or have unique requirements for translating one IP to another IP. Below are the design details for deploying NAT services on the network.

#1	Static and Dynamic

Determine if NAT will use a dynamic group of IP addresses for translation or a static one-to-one translation.

- **Static:** Used to dedicate a specific internal IP address to a public facing server (Email or Web server). It's recommended to consider port forwarding if static NAT is needed as a possible alternative.
- **Dynamic:** Used to translate one IP to another IP from a range of available IP addresses. This is something more common for large networks or environments with heavy Internet session usage. Dynamic NAT is starting to become very rare and should be avoided in most cases.

#2	Determine the Outside and Inside interfaces

Determine the NAT interface on the router/firewall that needs to translate an IP address to another address. This is usually the Edge router or the Firewall on the Internet Edge. Below are the NAT interfaces that needs to be identified.

- **Inside:** the interface facing towards the internal network or the point on the network where we want to translate to another IP address if it travels to another network (e.g. through an "outside" interface) that requires the address to be changed.
- **Outside:** the interface facing towards the external network (e.g. Internet) or the point on the network where the packets will already be translated using the new IP address.

#3	NAT Features

Additional services can be configured with NAT to provide other functions or requirements where needed. Below are some of the additional features that can be used with NAT:

- **PAT (or NAT Overload):** Used for mapping many private IP addresses to a single IP address. This is a best practice and recommended especially when one or a few Public IP addresses are available.

- **Port Forwarding (or NAT Port Redirect):** Used for translating the IP address and a TCP/UDP port to another IP/TCP/UDP port. This furthermore improves the use of IP addresses on the network and is recommended to use over static NAT.
- **NAT Transparency (NAT-T)**

#4	NAT and VPN

If a VPN tunnel and NAT are configured on the same device, the following needs to be considered for the configuration or the VPN tunnel will not work.

- For the ACL configured with the NAT translations (static, dynamic, PAT, port forwarding), the VPN networks need to be explicitly denied to use NAT. For example, let's say that the LAN at site-1 is 192.168.1.0 and the LAN at site -2 is 192.168.2.0. The NAT configuration (to not translate) for the Site-1 router would be "deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255". For Site-2 it would be "deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255".
- **NAT Transparency (NAT-T):** disable NAT-T if bandwidth conservation is required.

NSF & SSO

Category: Network Service (Network Management)

Prerequisite(s): Cisco Catalyst 4500/6500, Cisco Nexus 7000 (Hardware)

When to use: recommended to be implemented on supported hardware enable Non Stop Forwarding (NSF) for L3 services and Stateful Switchover (SSO) for L2, L3, & L4 services to provide increased reliability of services on the network.

SSO provides fast transparent data plane switchover when a hardware failures. It can synchronize its active processes and configuration between two redundant supervisor engines inside of a Cisco Catalyst supported chassis switch. For the Cisco Catalyst 4500+E series, to enable SSO you must have a license level of ipbase or entservices installed on the switches.

If a failure occurs the NSF/SSO convergence is between 1-3 seconds, but the links are not dropped and no convergence occurs on the network. Furthermore, some features and protocols may be NSF-aware like HSRP, so those considerations should be kept in mind for anything that is used with NSF enabled devices.

Network Management

Category: Network Service (Network Management)
Prerequisite(s): --

Choose the Network Management services that will be used in the network design.

- **SNMP:** used for monitoring a network device's performance and operational status. SNMPv3 is recommended to provide increased security over SNMPv2c which uses clear text communication.
- **Network Time Protocol (NTP):** all network components should use a time server to pull their date and time for accurate timestamps and internal communication.
- **NetFlow:** used for monitoring traffic flows through a network interface.
- **IP SLA:** provides intelligent re-routing/failover between connections based on a pre-configured probe.
- **VTY Access:** used for administering a network device remotely using Telnet or SSH. It is recommended to use SSH over Telnet which provides a secure connection between the client and the network device for administration.
 - *Role-Based CLI Access:* provides further restricted CLI access with different privilege levels for technicians and engineers where certain commands are allowed. This will simplify administration, but also avoid potential configuration mistakes resulting in outages.
- **Syslog:** used for displaying system and events that can be stored locally or sent to a server.
- **Accounting:** used for gathering basic network statistics (Packets, Bytes) for Source/Destination IP Addresses. Great to determine top-talkers through a Cisco router quickly without NetFlow being enabled.
- **RADIUS:** protocol used for network authentication (and accounting) into a network device or it can be used for remote access. This is an industry standard protocol that uses UDP.
- **TACACS+:** protocol used for network authentication into Cisco network devices or it can be used for remote access. This is a Cisco based protocol that uses TCP.
- **RBAC:** a role-based feature for accounts created on a Cisco Nexus switch. It's recommended to create local user accounts for AAA fail back authentication. Also create an admin account for the "network-admin" role and a netop account for the "network-operator" role.
- **GOLD:** an advanced feature supported on the Cisco Catalyst 6500 series (and higher models) that provides diagnostics of the hardware. This should be implemented for increased reliability and awareness.
- **EEM:** another advanced feature supported on the Cisco Catalyst 6500 series that monitors key system components such as the CPU, interface errors, and counters. EEM can do TDR/cable testing for ports, it will run loopback tests (using GOLD), and can send the results via email.
- **In-Service Software Upgrade (ISSU):** a software capability that allows doing an OS upgrade on Cisco L3-switches without bringing down the entire switch. Full image ISSU requires a dual supervisor environment which is well suited for single points of failure in the access layer. This is supported on the Cisco Catalyst 4500, 6500, and the Nexus 7000 series.
- **Embedded Resource Manager (ERM):** monitors system resources (e.g. CPU, memory, buffer) on a device in terms of its usage to better understand needs for scalability. Supported in Cisco IOS 12.3(14)T and later.
- **Configuration Rollback:** a feature that allows replacing an active running config file with any saved configuration file to return to its previous configuration if needed. It can automatically save the configuration file locally or to a server on the network. This feature is supported on the Cisco Catalyst 6500 and the Nexus series.

A large, white, serif capital letter 'O' is centered within a dark gray rectangular box.

~ Services ~

OSPF

Category: Network Service (Routing and Switching)
Prerequisite(s): Routing, IP (under Services)



Complete the steps below if OSPF is selected as the IGP routing protocol for the design:

#1 Infrastructure Design for OSPF Areas

Determine the OSPF areas that will be used on the network based on the following:

- **Backbone:** the OSPF backbone area on the network. All other areas (standard or stub areas) are required to be directly connected to the OSPF backbone or a virtual link is required. The OSPF backbone area should be configured for all Core, Distribution/Aggregation, and WAN Aggregation L3 devices.
- **Standard:** an OSPF area that connects into the OSPF backbone.
- **Stub:** a standard OSPF area that connects into the OSPF backbone that only injects an OSPF default route (Stub, Totally Stub Area) and/or intra-area routes (Stub area only). Stub areas are recommended for WAN spokes and LAN Access networks enabled for L3 services. Below are the stub areas that can be used on the OSPF network:
 - o **Stub:** stub area that can accept only an OSPF default route and intra-area routes.
 - o **Totally Stub:** stub area that is more restricted that accepts only an OSPF default route. This stub area is recommended for WAN spokes or L3 enabled Access networks that are directly connected into the LAN/DC Aggregation/Core or the WAN Aggregation.
 - o **Not So Stubby Area (NSSA):** stub area used when you need to redistribute a routing protocol into an OSPF stub area. For example, this can be used for unique cases where a new acquired network is running a different routing protocol (like EIGRP) that needs to be integrated with the current network (or site) running OSPF as a stub area. This site can be converted to a Not So Stubby Area (NSSA). This area type is recommended for Data Center Access networks.

#2 Infrastructure Design for OSPF Routers

Determine the routing device type on the OSPF network based on the following:

- **Backbone:** a routing device(s) that exist in the OSPF backbone area only. These are usually the Core devices (LAN and Data Center).
- **Standard:** a routing device that exist in a single OSPF area. This is usually a L3 Access device or a WAN branch router.
- **Area Border Router (ABR):** a routing device that is connected between standard OSPF areas and the OSPF backbone area. This is usually the Distribution/Aggregation devices used on the LAN, Data Center, or WAN.
- **Autonomous System Border Router (ASBR):** a routing device that is connected between the OSPF backbone area and with another routing protocol (e.g. EIGRP). This is usually a WAN that is connected with another network configured using a different routing protocol that needs to be merged with the existing OSPF network.

#3

Infrastructure Design for OSPF Network Types

Determine the OSPF network type for each interface enabled for OSPF based on the following:

- **Broadcast:** default OSPF network type for Ethernet networks. On an OSPF broadcast network, a DR and a BDR is established. This is recommended if there are a lot of L3 devices on the LAN/Data Center on the same network.
- **Point-to-Point:** An OSPF network that is ideal to be configured for true point-to-point connections. This is recommended for WAN point-to-point or L3 point-to-point connections on the LAN/Data Center.
- **Point-to-Multipoint:** an OSPF network that is recommended for hub-and-spoke (or point-to-multipoint) WAN topologies. This is common for WAN networks using Frame Relay.

#4

Infrastructure Design for OSPF Networks

Determine the networks configured on each L3 device that should be advertised to other OSPF routers.

Recommendations: all networks configured on the interfaces (physical or SVI interfaces) are essentially added as networks under the OSPF routing process associated to the OSPF area it will reside in.

#5

Equal Cost Path (ECP)

Provide fast convergence and load balancing of traffic through the network. This is accomplished by creating multiple paths through the network using the same metric values, which will inject two paths for a destination into the global routing table. To accomplish this the following must be implemented with the design.

- Create multiple interconnections on the LAN and Data Center switches based on the topology.
- **OSPF Cost:** Configure the OSPF cost with the same value for all L3 interfaces to create ECP on the network when there are multiple paths.

#6

Fast Convergence

If a failure occurs anywhere on the network it's important to tune OSPF to quickly react to the failure by transparently re-routing traffic across a different path in sub-second numbers. Below are some of the methods that can provide fast convergence with OSPF.

- **Equal Cost Path (ECP):** see ECP for more details.
- **IP CEF:** see "Step 6" for details on IP CEF.
- **Route Summarization**
- Enable **Bidirectional Forwarding Decision (BFD)**
- **Hello/Dead Timers:** tune timers for the neighbor interfaces to provide fast convergence when there is a failure. The dead timer is important to trigger a convergence when a failure occurs with an established neighbor. Below are recommended timer values that can be used for the configuration.
 - o **Small/Medium/Large:** Hello (1 second), Dead (3 seconds).

- o Other timer values that can be used: Hello (2 seconds), Dead (8 seconds)

Cisco Nexus Best Practices: recommended to use the default IGP timers in a dual-supervisor Nexus system to avoid any unnecessary convergence.

#7	Stub Routing

OSPF Totally Stub areas should be configured for LAN Access networks including WAN branch offices (spokes) which will provide the following:

- This will help to minimize the routing and forwarding tables
- Limits LSA propagation and prevents unnecessary SPF calculations that can have an undesirable side effect if the Distribution/Aggregation node is restored.

#8	Summarization

Summarize multiple routes as a single route to create smaller routing tables (resulting in less memory, bandwidth, & processing requirements) and to limit LSA flooding. It can also help to provide fast convergence from failures that may occur on the layer 3 network. You can summarize multiple routes as a single route using the following:

- **Intra Summarization** (range command): to summarize routes learned internally.
- **Inter Summarization:** to summarize routes learned externally.

Recommendations: summarize routes from the Distribution (or Aggregation) layer up to the Core layer (LAN or Data Center) to minimize the number of LSAs and routes that are sent. It reduces the need for SPF calculations due to internal Distribution/Aggregation changes. Intra-summarization will be more common unless there are other routing protocols that are configured on the network redistributed into OSPF. It's recommended that the network use a single routing protocol for simplicity and administration. Without summarization any link change within the LAN/Data Center is propagated to the entire OSPF network via an LSA flood beyond its local area. With summarization enabled no flooding is required to the other OSPF areas. It's important to include an interconnection link between the redundant Distribution/Aggregation switches to allow continued connectivity for a given VLAN/Subnet if there is a link failure.

#9	Best Practices

Below are additional services and configuration used with OSPF that is recommended in the design.

- **Passive Interfaces:** a best practice that prevents rogue routing devices from injecting bad routes into the network.
- **MD5 Authentication:** configures a password in order to form a neighbor with other OSPF routers before exchanging routes. This can be configured with either a MD5 or a clear-text password. It's recommended to use a MD5 password.
- **Interconnections:** use the OSPF "point-to-point" network type for interconnections between network devices.

Recommendations: these mechanisms are recommended for implementation. Passive interfaces can provide a great level of security to prevent rogue routing devices from bringing down the entire network. For example, if OSPF is enabled without any security, then someone could plug in an OSPF enabled router in their office that could potentially impact the routing environment and affecting the production network. Therefore, OSPF routing capabilities on subnets where no routers should exist (e.g. user subnets) should be enabled as a passive interface.

Below are some advanced OSPF features/timers related to LSA and SPF operations recommended for large OSPF environments.

- **LSA Timers:** Tune to minimize the number of LSA's sent (Router and Network LSAs) during a convergence. Otherwise with the LSAs generated, resulting in SPF calculation for best possible paths through the network, it could cause a significant outage as OSPF converges around a node or link failure in a hierarchical topology. By default, there is a 500ms delay before generating router and network LSAs; the wait timer is used to collect changes during a convergence event and minimize the number of LSAs sent. Make sure that "lsa-arrival" is less than "lsa-hold".
- **SPF Timers:** When a link or node has failed, an OSPF peer cannot take action until the SPF timer has expired. In the past the OSPF SPF timer did not allow an OSPF environment to converge as quickly compared to EIGRP. With recent changes with OSPF in later IOS releases it can provide sub-second timer configuration for the LSA and SPF timers. OSPF has an SPF throttling timer designed to dampen route recalculation (preserving CPU resources) when a link bounces. After a failure, the router waits for the SPF timer to expire before recalculating a new route.
- **Incremental SPF (iSPF):** mechanism to reduce the computational load of larger OSPF areas. More applicable to a WAN than a Campus network.

If OSPF will be deployed over a Frame Relay network then additional configuration is required in regards to the network type. It's recommended to use an OSPF network type of point-and-multipoint for the configuration with Frame Relay.

Recommendations: Frame Relay in networks today is becoming obsolete due to IP WAN solutions utilizing L3VPN or L2VPN technologies. However, if Frame Relay is deployed for the private WAN then the OSPF network type of point-to-multipoint is needed for its configuration.

Controls what routes are sent and received by the routing protocol.

- **ACL:** configure an ACL with what routes should be received or advertised (using permit) or not (using deny).
- **Distribute List:** the ACL is used with a distribute list configured under the OSPF routing protocol.
- **Direction (Inbound, Outbound):** to restrict what routes are injected into the OSPF router use "inbound" with the distribute list. To restrict what routes are advertised to other routers use "outbound" with the distribute list.

Recommendations: this is strongly recommended to provide better control of what routes are being sent and received on the network. This can prevent rogue OSPF routers and routes that can potentially bring down the entire network. This is common and recommend for LAN/Data Center networks configured in a Customer/Building model where many buildings may have their own routing devices using OSPF for exchanging route information. The distribute-list is configured for those interfaces for what routes can be received from that building network including what routes will be advertised to that building network. If you are using L3 Access switches for your L2/L3 topology, it's recommended to enable route filtering mechanisms towards the L3 access switches.

OTV

Category: Network Service (DCI)

Prerequisite(s): Data Center and WAN (under Solutions)

DA F

When to use: to extend VLANs between multiple Data Center across a L3 routing domain (over long distances).

OTV provides many advantages for Data Center networks that include:

- It runs over IP
- Work better over long distances for extending VLANs (up to 4094) between Data Centers
- It prevents flooding of unknown destinations across the Internet by advertising MAC address reachability using routing protocol extensions (IS-IS)
- Cisco's latest version is able to interconnect datacenters without relying on IP multicast which is not always available across the Internet

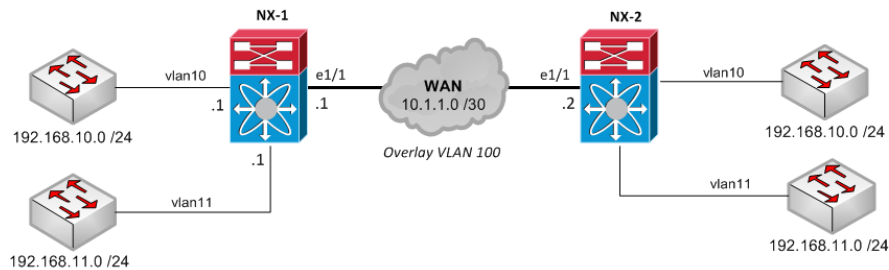
#1

Components in OTV Topology

Below are the components in the solution and how they are deployed:

- **OTV Edge Device:** The components in this topology would be the WAN router (aggregation, branch) acting as a OTV edge device(Router, Switch). It would connect into the private WAN cloud for extending VLANs between other Data Centers. Below shows an example of OTV in a design where NX-1 and NX-2 would be the OTV edge device components.

Below shows an example of OTV in a design where NX-1 and NX-2 would be the OTV edge device components:



#2	Requirements

Below are requirements for implementing this service on the network:

- You must have the hardware to support this feature including the appropriate license installed.
- **Services:** Multicast routing services and IGMP version 3.

#3	Configuration

General Configuration: below are the steps for the design and implementation of this feature:

- Have a Private IP WAN cloud between Data Centers
- Use a OTV enabled router/switch with the supported licensing to support OTV
- IGMPv3 (and Multicast services) enabled on OTV edge device.
- Configure OTV overlay virtual interface referencing the WAN facing interface.
- If multiple OTV edge devices (multi-homing capabilities) exist within a Data Center connected into the WAN cloud then Authoritative Edge Device (AED) should be enabled to avoid end-to-end loops not sending STP BPDU messages.
- Setup the OTV site VLAN
- Define the VLANs that should be extended over the IP WAN cloud.

#4	Add-Ons

Below are other common technologies that can be implemented or overlay with OTV:

Technology	Description	Prerequisite(s)
OTV and LISP	OTV can be implemented with LISP to provide a robust shortest routing path method for extending VLANs between Data Centers.	LISP

A large, white, serif capital letter 'P' is centered within a solid gray rectangular box. The letter is stylized with a thick vertical stem and a rounded, slightly flared top.

~ Services ~

Policy Based Routing (PBR)

Category: Network Service (Routing and Switching)
Prerequisite(s): Routing, IP (under Services)

DA

Used to force unique routing based on some of the following parameters:

- IP Address, Subnet
- Port Number
- QoS
- Packet Size

Recommendations: this is used for unique routing requirements not easily accomplished through static or dynamic routing protocols. In most environments PBR is not needed and should be avoided to keep the routing environment simplified.

Port Channel (802.3ad)

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)



When to use: to bundle up to 8 interfaces/ports together to appear as a single interface. It's recommended to bundle interfaces in multiples of 2 to a port channel group. A Port Channel is commonly done to provide increased bandwidth and is often used between Core & Distribution/Aggregation devices for the interconnections. A Port Channel can provide sub-second failover between links in a configured bundle.

A Port Channel can also be called a Link Aggregation (LAG) in some discussions for design and configuration. If port channel is required determine the protocol that will be used to handle bundling the interfaces including monitoring the health of the link:

#1	Determine the protocol

- **LACP:** this is the recommended protocol to use since it is an industry standard protocol that can be used with Cisco and other vendor devices. This can include dual-homed servers that may need to be port channelled to the Data Center switch.
 - *Configuration:* Set the mode to "active" on both ends.
- **PAgP:** this protocol is often used between two Cisco L2/L3-switches to provide port channeling for the interconnection. This protocol can be used for port channeling if the switches involved are Cisco switches even though LACP is still recommended.
 - *Configuration:* set the mode to "desirable" on both ends.

Recommendations: (1) use LACP, but 10G connections are preferred over EtherChannel (or Port Channel) because the OSPF/EIGRP cost will change if one interface is lost. Therefore using one high-bandwidth interface (10G) is ideal. (2) Place the interfaces used in a Port Channel to separate switches and/or line modules. If using stackable switches like the Cisco Catalyst 3750-X series then the Port Channel should not go on the stack master switch. (3) Configure the STP link type for the Port Channel interface to be "point-to-point". (4) If using Cisco Nexus hardware, configure the mode for a L3 port channel to be "on".

#2	Other Attributes

- **Load Balance Hash:** a port channel is really load balancing between multiple connections bundled. The recommended hash algorithm to use for the port channeling bundle is "src-dst-ip" or "src-dst-port" depending on what hash algorithm is supported based on the hardware platform.
- **Layer 2 or Layer 3:** depending on the Interconnections used on the LAN/Data Center network determine if the Port Channel interface will be a Layer 2 or Layer 3.

Port Monitor

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)

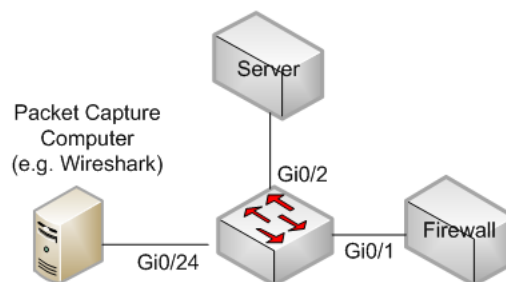
NM

Port monitoring is usually configured for network troubleshooting purposes using a packet analyzer or using IDS/IPS appliances capturing network traffic. Using an IPS appliance is more ideal for medium and large networks including companies that follow a regulatory compliancy (e.g. PCI, SOX, HIPPA). Determine the details on how port monitoring will be setup.

1. **L2/L3 Switch Device:** this can vary depending on the size of the environment to the amount of traffic that will be captured where port monitoring will be configured. It could be the Core Switch, Access Switch, or perhaps the switch connected behind the Edge Router.
2. **Source:** what interfaces on the device should be captured. This is usually the uplink/downlink ports on the switch to capture all traffic to/from that interface.
3. **Destination:** the interface(s) with the connected TAPS, IDS/IPS, or a network sniffer that will receive the monitored traffic from the source interface(s).

Determine the port monitoring mechanism that will be used on the network.

- **SPAN:** local to a switch (most common selection).
- **RSPAN:** port monitoring across the L2 network using a dedicated VLAN.
- **ERSPAN:** port monitoring across the L3 network.



In this example topology, the “L2/L3 switch device” would be the switch seen in the diagram. The “source” could be the server (Gi0/2) and/or the firewall (Gi0/1) switch ports. And the “destination” would be the packet capturing device connected on Gi0/24.

Port Security

Category: Network Service (Routing and Switching, Security)
Prerequisite(s): LAN and/or Data Center (under Solutions)

SEC

Use Port Security to allow a specific host a dedicated switch port based on the MAC address (also called a secure MAC address) or to limit the number of MAC addresses that can be active on a port. The secure MAC address can be configured statically on the switch port or the it can dynamically learn the addresses (called “sticky addresses”).

If a different host is plugged into a secure port then that port will be placed in a shutdown (or restricted) state. If the secure host plugs into a non-secure port on the same switch, that port would be placed in a shutdown (or restricted) state.

This will help against CAM attacks (e.g. MAC flooding) and DHCP starvation.

Power over Ethernet (PoE)

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN (under Solutions)

Power over Ethernet (PoE) is a capability that can provide power to a connected device (e.g. IP Phone, Wireless Access Point, Virtual desktop). Below are the different type of PoE technologies that can be used and what they support:

- **PoE** support up to 15 watts per port
- **PoE+** (IEEE 802.3at) support up to 30 watts per port
- **Unified (UPoE)** support up to 60 watt per port. This is commonly used for virtual desktops and is used over the same cabling utilized by PoE+

Q

~ Services ~

Quality of Service

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN, WAN, Data Center, and/or Internet Edge (under Solutions)

When to use: handling for real-time traffic and network congestion.

Complete the steps below if QoS services will be implemented in the design:

Step 1

Applications for QoS

For some of the solutions you probably determined what requires QoS such as Voice and Video. Before you start with the QoS network design, the following applications are recommended for implementing QoS mechanisms.

- **Voice and Video** (Recommended, Required)
- **Business-critical applications**
- **Other Data:** FTP, Backup, Peer-to-Peer (P2P), Citrix, ERP (Optional)

Step 2

Device and Port Identification

Determine the device ports and their type within the topology based on the following:

#1

Determine the Layer2/Layer3 Switch Port Types

Determine the port type for all ports on the L2/L3-switches in the design based on the following:

- **Edge port:** a port connecting to a host device such as a desktop, server, IP phone, or printer.
- **Interconnection (ICT) port:** a port connecting to another switch, router, or solution. This would be an uplink or downlink port on the L2/L3 switch.

#2

Determine the Layer2/Layer3 Switch Port Trust Type

For each port type determined from the last step determine the trust level for those ports based on the following:

- **Trusted port:** a port that we trust the markings from the connected device. This is usually Interconnection ports, Access Points (AP), Network Devices (e.g., Routers, Firewalls), or servers based on unique requirement.
- **Conditional Trusted port:** an edge port that has a connected IP Phone and desktop.
- **Untrusted port:** an edge port where we do not trust the markings from the connected device. This can be a desktop or server. We don't want users or servers explicitly marking packets with high priority, which should be dedicated for real-time applications such as voice and video.

#3

Determine the Router Port Type

For router devices (e.g. WAN router, Edge router) where voice traffic will travel through to access other voice/video endpoints determine what is the WAN port and the LAN port. For example, if voice will be used across the WAN, then we need to determine the port type on the WAN router. No voice traffic will typically be used through an edge router, so that does not need to be included. Determine the port types based on the following:

- **LAN port:** a port connected towards the internal side of the network (e.g. LAN or Data Center).
- **WAN port:** a port connected towards the ISP or WAN provider.

#4

Determine the WAN connection for all WAN routers

For the router WAN ports gathered (if applicable) from the last step determine the bandwidth service and technology that will be used based on the following:

- Leased line
- Frame Relay
- ATM
- Broadband (DSL, Cable)
- VPN
- MPLS

#5

Determine the WAN connection speed on all WAN routers

For the router WAN port (if applicable) determine the speed of the WAN connection to the provider based on the following:

- **Low Speed:** up to 768kbps.
- **Medium Speed:** up to T1 (1.544Mbps).
- **High Speed:** 1.544Mbps and higher.
- **Very High Speed:** DS-3 to OC-3 & higher.

Step 3

AutoQoS

DA

AutoQoS is a QoS mechanism supported on L2/L3 switches that makes deploying QoS with all best practices nice and simple. AutoQoS applies all of the applicable configuration in terms of trust boundaries, queuing, and dropping. From what has been identified from the last step, AutoQoS for L2/L3 switches can be configured based on the following:

- **AutoQoS Cisco Phone:** implement this profile on all edge ports with connected IP Phones and Desktops.
- **AutoQoS Trust:** implement this profile on all uplink and downlink ports on the LAN switch ports.

Complete the QoS design for the Classification and Marking needed on the network based on the following:

QoS mechanism that will classify what traffic (e.g. Voice, Video, Data) should be marked with a particular priority for special treatment (queuing and dropping) if congestion occurs on the network.

(1) Below are the locations on the network where traffic should be classified and marked:

- **LAN Access Edge port:** traffic should be classified and marked closer to the source. Therefore, it is recommended to classify and mark on the LAN Access switch edge ports with connected IP Phones and desktops.
- **Router WAN/LAN port:** traffic can be classified and marked on a WAN router's WAN port if there are no previous markings on the network and the WAN router only has one WAN facing interfaces. Applicable for Internet Edge and WAN routers.
- **Router LAN port:** traffic can be classified and marked on a WAN router's LAN port if there are two or more WAN interfaces and there are no previous markings on the network. Applicable for Internet Edge, VPN, Teleworker, and WAN routers.

(2) Traffic can be classified using one of the following methods:

- **L2:** for L2 networks traffic can be classified using COS (802.1P).
- **L3:** for L3 networks traffic can be classified using DSCP (recommended) or IP Precedence.
- **ACL:** traffic can be classified using ACLs, but is not common for LAN deployments when using Voice.
- **NBAR:** traffic can be classified using NBAR which is common when using Routers on the network.

(3) Once the traffic has been classified determine how it will be marked using one of the following methods:

- **MQC (Modular QoS Configuration):** this is the most common method for marking classified traffic used on L2/L3-switches and routers. MQC provides a three level process for configuration. First, there is a class-map which defines what will be classified. Second, a policy-map is used to list the class-maps and what actions (like marking) will be done. And third, apply the policy map and direction (inbound, outbound) to the interface that will classify and mark the traffic.

Please keep in mind that no marking is needed for the voice endpoints. Voice packets are automatically marked by the IP Phone endpoint (control and data stream), so all marking will likely occur for specific Data traffic based on the policies determined (done in a later step).

QoS mechanism that will only classify traffic (e.g. voice, video, data, etc) based on previous QoS markings.

- (1) Below are the locations on the network where traffic can be classified based on the previous markings on the network:
 - **Router with 1 WAN port:** traffic can be classified on a WAN router's WAN port if there are no previous markings on the network and the WAN router only has one WAN facing interface. Applicable for Internet Edge, VPN, Teleworker, and WAN routers.
 - **Router with 2 WAN ports:** traffic can be classified on a WAN router's WAN port if there are no previous markings on the network and the WAN router only has two or more WAN facing interfaces. Applicable for Internet Edge, VPN, Teleworker, and WAN routers.
- (2) Traffic can be classified using one of the following methods:
 - **L2:** for L2 networks traffic can be classified using COS (802.1P).
 - **L3:** for L3 networks traffic can be classified using DSCP (recommended) or IP Precedence.
 - **ACL:** traffic can be classified using ACLs, but is not common for LAN deployments when using Voice.
 - **NBAR:** traffic can be classified using NBAR which is common when using Routers on the network.
 - **Frame Relay (DE):** if using Frame Relay implement the use of Discard Eligible (DE) for QoS.
 - **ATM:** If using ATM use CLP and Virtual Circuits (VC) for QoS.
 - **MPLS:** If using MPLS use EXP bits for QoS. This is something that is used within a service provider network and less with a company network.

QoS mechanism that will drop (or markdown) packets that exceed the configured threshold. This is optional, but can be implemented for rate limiting traffic on the network running voice. Below are the locations where policing may be used on the network:

- **LAN Access edge ports:** recommended rate limiting implemented closer to the source.
- **LAN downlink/uplink ports:** rate limiting can also be implemented on the Core or Distribution/Aggregation switches for easier administration, but requires robust hardware to provide per-user policing.
- **Router WAN ports:** ideal for implementing rate limiting on the Internet Edge router's WAN port for the amount of bandwidth certain applications can use.

If policing will be implemented determine the mechanism that will be used:

- **Committed Access Rate (CAR):** legacy policing feature configured directly on interfaces.
- **Class-based Policing (CBP):** recommended policing configured within MQC.
- **User-Based Rate Limiting (UBRL):** Aggregate policing can be configured on the Distribution or Core switch using the Cisco Catalyst 6500 Series (or higher like the Cisco Nexus series) to provide policing for individual nodes on the LAN (e.g. user, computer, laptop).
- **Control Plane Policing (CoPP):** implement CoPP on all capable hardware to protect control plane traffic (e.g. IP routing, switching, SNMP, Telnet/SSH).

Cisco Nexus Best Practices: configure CoPP to limit all management/control plane traffic (e.g. SNMP, Telnet/SSH) to the default VRF on the Nexus switch.

Step 6

Queuing and Dropping

R P

Queuing and Dropping mechanisms are implemented almost everywhere on the network and is the main function for what QoS provides.

#1

Congestion Management

QoS mechanism that provides queuing and scheduling of marked (or unmarked) packets if congestion occurs on a port. Queuing can also help against serialization delay which is the amount of time to clock or put a frame on the physical media. Below is where congestion management should be implemented on the network. This is applicable for all switch ports on the LAN (edge ports, uplinks, downlinks) and the Router WAN ports.

- **Hardware Queuing:** applicable for L2/L3 switches on the network. Hardware queuing uses the xPyQzT model where “P” is the priority queue recommended for voice traffic and “Q” is the individual queues that can be used for data and video traffic. The xPyQzT model in terms of the number of queues will vary depending on the hardware that is used.
- **Software Queuing:** applicable on routers. Use LLQ for real-time traffic like Voice and Video. Use CBWFQ for data traffic.

Recommendations: Always try to use Hardware based queuing over software based queuing if applicable. Use AutoQoS on L2/L3 switches, which will automatically configure all of the recommended options needed for congestion management.

CBWFQ Considerations: there is some latency when using CBWFQ when you guarantee the minimum bandwidth. Using shaping mechanism works better with lower latency.

#2

Congestion Avoidance

QoS mechanism for gracefully dropping low priority packets when there is congestion on a port. This is applicable for all switch ports and the Router WAN ports. Determine the congestion avoidance mechanism that will be used based on whether it is on a switch or a router.

- **Hardware Dropping:** applicable for L2/L3 switches on the network. Hardware dropping uses the xPyQzT model where “T” is the threshold used for randomly dropping packets with lower priority allowing high priority packets to travel promptly through the network. The xPyQzT model in terms of the number of thresholds will vary depending on the hardware that is used.
- **Software Dropping:** applicable on routers. Use WRED for TCP type traffic where TCP has mechanisms for doing retransmissions if data packets are dropped due to congestion or loss.

Recommendations: Always try to use Hardware based dropping over software based dropping if applicable. Use AutoQoS on L2/L3 switches, which will automatically configure all of the recommended options needed for congestion avoidance.

Traffic shaping is the method where packets that do not conform to policies will be stored in the buffers for a short period of time rather than dropping them compared to policing.

- Applicable for private WAN connections
- Applicable for Teleworker Integrated Unit + Access topology
- Applicable for WAN Aggregation using IPSec/GRE or DMVPN on the VPN GRE interface.

Traffic shaping can be configured using one of the following mechanisms:

- **Frame Relay Traffic Shaping (FRTS):** when Frame Relay is used on the WAN.
- **Class Based Shaping (CBS):** traffic shaping configured under the MQC and not using Frame Relay for the WAN.

Configuration: to determine the FRTS values for the recommended CIR, Bc, and Be values we will need the following information:

- **PVC Speed:** this will be the speed (e.g. 768kbps) of the WAN connection guaranteed by the provider.

To determine the traffic shaping values needed use the following formula:

- $CIR = PVC \text{ speed} \times 95\%$
- $Bc = CIR / 100$
- $Be = 0$

If using the **Teleworker Integrated Unit + Access** topology consider the following for traffic Shaping:

- For Cable connections, shape to 95% (for the CIR calculation)
- For DSL connections, shape to 70% (for the CIR calculation)

QoS mechanism that will fragment or break-up large packets into smaller packets to allow smaller packets (e.g. Voice) to be transmitted to avoid high serialization delay and jitter. Serialization delay is the amount of time to clock or put a frame on to the physical media.

- Applicable for Router WAN ports with Private WAN connections
- Required for Slow speed connections
- Optional for Medium speed connections
- Must be enabled on both ends of a connection

If Fragmentation is needed use one of the following mechanisms below:

- **Frame Relay Fragmentation (FRF.12):** when using Frame Relay
- **Link Fragmentation Interleaving (LFI):** used with PPP encapsulated connections. Set to 10ms

Configuration: to calculate the Fragmentation packet size (in Bytes) we will need the following information:

- **PVC Speed:** this would be the speed (e.g. 768kbps) of the WAN connection guaranteed by the provider.

To determine the fragmentation packet size use the following formula:

- $(PVC\ speed \times 10ms) / 8 = \text{Fragment Packet Size (in Bytes)}$
- Example: $(768kbps \times 10ms) / 8 = 960\ Bytes$

Notes: for Serialization delay use 10ms

QoS mechanism that will compress Voice RTP packets to smaller sized packets. For example, using cRTP it will reduce a G.729 call from 24Kbps to 11Kbps.

- Applicable for Router WAN ports with Private WAN connections
- Required for Low speed connections
- Optional for Medium speed connections
- Does not work with VPN solutions
- Must be enabled on both ends of a connection

If compression is needed the following mechanism(s) can be used:

- Compression RTP (cRTP)

Step 10

Link Efficiency – TX-Ring Tuning

DA

QoS mechanism that automatically sizes the final interface output buffer (Tx-ring) to optimal lengths for real-time applications.

- Applicable for Router WAN ports
- Applicable for Teleworker/Broadband (using either the IU or DU topology model)
- Required for Low speed connections using ATM

Configuration: the default Tx-Ring is 64. Tune to use 3.

Step 11

Link Efficiency – Maximum Reserve Bandwidth

DA

By default, interfaces on a Cisco device with a total bandwidth allocation cannot exceed 75% allowing 25% of network control related traffic. You can change the maximum reserve bandwidth to be 100% instead of 75% if CBWFQ is configured within a QoS policy.

- Applicable for Router WAN ports
- Required for Low and Medium speed connections using ATM
- Required for High speed connections (leased line)

Step 12

Link Efficiency – ATM VBR

P

QoS mechanism that provides QoS traffic shaping capabilities with ATM PVCs.

- Applicable for Router WAN ports
- Required for Low, Medium, & High speed connections using ATM

QoS mechanism that classifies traffic on the packet's header after encryption.

- Applicable for Router WAN ports used for VPN (e.g. IPSec, DMVPN).
- Applicable for all Teleworker/Broadband topology models.
- Applicable for WAN Aggregation using IPSec/GRE or DMVPN on the VPN GRE interface.

QoS mechanism that identifies whether a packet is being replayed by a hacker and confirms the integrity of the connection.

- Applicable for Router WAN ports used for VPN.
- Applicable for Teleworker/Broadband (all topology models).

QoS mechanism that provides tuning of the MSS for better TCP packet delivery across the VPN. It also helps against serialization delay which is the amount of time a router will put packets onto the physical media for transit.

- Applicable for Router WAN ports using IPSec/GRE or DMVPN on the VPN GRE interface.
- Applicable for Teleworker/Broadband (all topology models).

Configuration:

- **IPSec VPN:** configure an MTU size of either 1400 or 1412 on the GRE interface to avoid MTU related issues with the VPN tunnel.
- **Teleworker:** set MSS to 542 to help against serialization delay. This needs to be applied to the WAN and LAN facing Ethernet interfaces.

Step 16

Link Efficiency – Path MTU Discovery (PMTU)

DA

QoS mechanism that provides VPN tunnels the ability to determine the best/smallest MTU size to use.

- Applicable for Router WAN ports used for VPN.
- Applicable for Teleworker/Broadband (all topology models).

Step 17

Link Efficiency – PAK_Priority

R

This is an internal Cisco IOS mechanism for protecting the routing and control traffic which auto-assigns to CS6/IP Precedence 6. Nothing needs to be configured by the network engineer.

Step 18

MPLS QoS

DA

The ISP will use one of the following QoS mechanisms on the MPLS network if the CE/C devices will mark packets within the network and will be sent through the MPLS WAN. It's important to understand which MPLS DiffServ Mode will be implemented and how the CE/C device marked packets will be treated through the MPLS network.

- **Uniform Mode:** default MPLS QoS operation. When the service provider and the CE are part of the same DiffServ domain.
- **Short Pipe Mode:** the service provider and the CE are part of different DiffServ domains.
- **Pipe Mode:** same as Short Pipe mode, but the PE egress policies towards the CE is provisioned according to the service provider's explicit markings.

When to use: using Cisco Nexus 5500 series switch and FCoE

It's recommended to provide lossless data for all FCoE traffic end-to-end within the Data Center. It uses the 802.1Q Priority Code Point or CoS bits in the Layer 2 header.

The Cisco Nexus 5500 series switches can map traffic into one of six hardware queues. One queue is predefined for default traffic that is not marked and there is one priority hardware queue assigned for FCoE traffic. The remaining four queues can be used for other non-FCoE traffic that you can configure. Traffic classified by DSCP can be associated to one of the four internal queues with guaranteed queuing.

The Cisco Nexus 5500 series switches also support Jumbo frames on a per-class basis. It can provide per-CoS MTU configuration that can be applied system-wide for FCoE traffic instead of per-port MTU configuration.

For QoS operations within the LAN/Campus solution determine the best QoS policy to implement for the design.

Class Model	QoS Details	Applicable
Voice, Data (Basic), Default	Auto QoS: Conditional Trust (IP Phone+Desktop), Trust (uplinks/downlinks) Voice: DSCP EF (46), IPP/CoS 5 Voice Control (Call Signaling): DSCP AF31/CS3 (26/24), IPP/CoS 3 Best Effort: DSCP 0 (0), IPP 0, CoS 0	LAN Access
Voice, Video, Data (Advanced)	Auto QoS: Conditional Trust (IP Phone+Desktop), Trust (uplinks/downlinks) IP Routing: DSCP CS6 (48), IPP/CoS 6 Voice: DSCP EF (46), IPP/CoS 5 Interactive Video: DSCP AF41 (34), IPP/CoS 4 Streaming Video: DSCP CS4 (32), IPP/CoS 4 Mission Critical Data: DSCP 25, IPP/CoS 3 Voice Control (Call Signaling): DSCP AF31/CS3 (26/24), IPP/CoS 3 Transactional Data: DSCP AF21 (18), IPP/CoS 2 Network Management: DSCP CS2 (16), IPP/CoS 2 Bulk Data: DSCP AF11 (10), IPP/CoS 1 Scavenger: DSCP CS1 (8), IPP/CoS 1 Best Effort: DSCP 0 (0), IPP 0, CoS 0	LAN Access

Example: Voice, Video, Data (Advanced):

class-map match-any VOICE match ip dscp ef class-map match-any VOICE-CONTROL match ip dscp af31 match ip dscp cs3 class-map match-any ROUTING match ip dscp cs6 class-map match-any INTERACTIVE-VIDEO match access-group ACL-INTERACTIVE-VIDEO class-map match-any STREAMING-VIDEO match access-group ACL-STREAMING-VIDEO class-map match-any DATA-MISSION-CRITICAL match access-group ACL-MISSION-CRITICAL class-map match-any DATA-TRANSACTIONAL match access-group ACL-TRANSACTIONAL class-map match-any NETWORK-MGMT match access-group ACL-NETWORK-MGMT class-map match-any DATA-BULK match access-group ACL-BULK-DATA class-map match-any DATA-SCAVENGER match access-group ACL-SCAVENGER	policy-map LAN-POL class INTERACTIVE-VIDEO set ip dscp af41 class STREAMING-VIDEO set ip dscp cs4 class DATA-MISSION-CRITICAL set ip dscp 25 class DATA-TRANSACTIONAL set ip dscp af21 class DATA-BULK set ip dscp af11 class DATA-SCAVENGER set ip dscp cs1 class NETWORK-MGMT set ip dscp cs2

For QoS operations within the WAN solution determine the best QoS policy to implement for the design.

Class Model	QoS Details	Applicable
Voice, Data (3 Class)	Voice RTP (DSCP EF, LLQ=33%, cRTP) Voice Control (DSCP CS3/AF31, CBWFQ=5%) Best Effort (DSCP 0, WFQ, DSCP-WRED)	WAN (slow & medium speed)
Voice, Data (5 Class)	Voice RTP (DSCP EF, LLQ=33%) Voice Control (DSCP CS3, CBWFQ=5%) Critical Data (DSCP AF21/AF22/CS6/CS2/25, CBWFQ=36%, DSCP-WRED) Scavenger (DSCP CS1, CBWFQ=1%) Best Effort (DSCP 0, 25%, CBWFQ=25%, WRED)	WAN (slow & medium speed)
Voice, Video, Data (8 Class)	Voice RTP (DSCP EF, LLQ=18%) Voice Control (DSCP CS3/AF31, CBWFQ=5%) Critical Data (DSCP AF21/AF22/25, CBWFQ=27%, DSCP-WRED) Bulk Data (DSCP AF11/AF12, CBWFQ=4%, DSCP-WRED) Network Control (DSCP CS6/CS2, CBWFQ=5%) Interactive Video (DSCP AF41/AF42, LLQ=15%) Scavenger (DSCP CS1, CBWFQ=1%) Best Effort (DSCP 0, CBWFQ=25%, WRED)	WAN (high speed)
Voice, Video, Data (11 Class)	Voice RTP (DSCP EF, LLQ=18%) Voice Control (DSCP CS3/AF31, CBWFQ=5%) Mission Critical Data (DSCP 25, CBWFQ=10%, WRED) Bulk Data (AF11/AF12, CBWFQ=4%, DSCP-WRED) Network Control (DSCP CS6, CBWFQ=3%) Interactive Video (DSCP AF41/AF42, LLQ=15%) Scavenger (DSCP CS1, CBWFQ=1%) Best Effort (DSCP 0, CBWFQ=25%, WRED) Streaming Video (DSCP CS4, CBWFQ=10%) Transactional Data (DSCP AF21/AF22, CBWFQ=7%, DSCP-WRED) Network Management (DSCP CS2, CBWFQ=2%)	WAN (high speed)
Voice, Video, Data (10 Class)	Voice RTP (DSCP EF, LLQ=18%) Voice Control (DSCP CS3/AF31, CBWFQ=5%) Mission Critical Data (DSCP 25, CBWFQ=15%, WRED) Bulk Data (DSCP AF11, CBWFQ=4%, DSCP-WRED) Network Control (DSCP CS6, CBWFQ=3%) Interactive Video (DSCP AF41/AF42, LLQ=15%) Scavenger (DSCP CS1, CBWFQ=1%) Best Effort (DSCP 0, CBWFQ=25%, WRED) Transactional Data (DSCP AF21, CBWFQ=12%, DSCP-WRED) Network Management (DSCP CS2, CBWFQ=2%)	WAN Branch

Example: Voice, Data (3 Class)

class-map match-all voice-rtp match ip dscp ef class-map match-any voice-control match ip dscp cs3 match ip dscp af31	policy-map WAN-POL class voice-rtp priority percent 33 compress header ip rtp class voice-control bandwidth percent 5 class class-default fair-queue random-detect dscp-based

For QoS operations within the VPN solution determine the best QoS policy to implement for the design.

Class Model	QoS Details	Applicable
Voice, Data (6 Class)	Voice-RTP (DSCP EF, LLQ = 33%) Voice-Control (DSCP AF31/CS3, CBWFQ = 5%) Transactional Data (DSCP AF21/AF22, CBWFQ = 31%, Anti-Replay Tuning = 20) Internetwork Control (DSCP CS6, CBWFQ = 5%) Scavenger (DSCP CS1, CBWFQ = 1%, Anti-Replay Tuning = 1) Best-Effort (DSCP 0, CBWFQ = 25%, Anti-Replay Tuning = 16)	VPN (medium& high speed)
Voice, Video, Data (8 Class)	Voice-RTP (DSCP EF, LLQ=18%) Voice-Control (DSCP AF31/CS3, CBWFQ = 5%) Transactional Data (DSCP AF21/AF22, CBWFQ = 27%, Anti-Replay Tuning = 18) Best-Effort (DSCP 0, CBWFQ = 25%, Anti-Replay Tuning = 16) Scavenger (DSCP CS1, CBWFQ = 1%, Anti-Replay Tuning = 1) Interactive Video (DSCP AF41/AF42, LLQ = 15%) Network-Control (DSCP CS6, CBWFQ = 5%) Bulk Data (DSCP AF11/AF12, CBWFQ = 4%, Anti-Replay Tuning = 3)	VPN (high speed) ; 3Mbps or higher
Voice, Video, Data (11 Class)	Voice-RTP (DSCP EF, LLQ=18%) Voice-Control (DSCP AF31/CS3, CBWFQ = 5%) Critical Data (DSCP 25, CBWFQ = 10%) Best-Effort (DSCP 0, CBWFQ = 25%, Anti-Replay Tuning = 16) Scavenger (DSCP CS1, CBWFQ = 1%, Anti-Replay Tuning = 1) Interactive Video (DSCP AF41/AF42, LLQ = 15%) Routing (DSCP CS6, CBWFQ = 5%) Bulk Data (DSCP AF11/AF12, CBWFQ = 4%, Anti-Replay Tuning = 3) Streaming Video (DSCP CS4, CBWFQ = 10%, Anti-Replay = 6) Transactional Data (DSCP AF21/AF22, CBWFQ = 5%, Anti-Replay Tuning = 3) Network Management (DSCP CS2, CBWFQ = 2%)	VPN (high speed) ; 3Mbps or higher
Voice, Data, Routing (Teleworker Basic for IU and DU)	Voice (DSCP EF, LLQ = 150kbps or 40%) Voice Control (DSCP AF31/CS3, CBWFQ = 5%) Internetwork Control (DSCP CS6, CBWFQ = 5%) Best-Effort (DSCP 0, WFQ, Anti-Replay Tuning = 30)	Teleworker/Broadband (IU and DU)
Voice, Data, Routing (Teleworker Basic for IUA)	Voice (DSCP EF, LLQ = 128kbps or 35%) Voice Control (DSCP AF31/CS3, CBWFQ 5%) Internetwork Control (DSCP CS6, CBWFQ 5%) Best-Effort (DSCP 0, Anti-Replay Tuning = 30)	Teleworker/Broadband (IUA)

Example: Voice, Data, Routing (Basic) I:

class-map match-all voice-rtp match ip dscp ef class-map match-any voice-control match ip dscp cs3 match ip dscp af31 class-map match-any internetwork-control match ip dscp cs6	policy-map VPN-POL class voice-rtp priority percent 40 class voice-control bandwidth percent 5 class internetwork-control bandwidth percent 5 class class-default fair-queue

For QoS operations within the Internet Edge solution determine the best QoS policy to implement for the design.

Class Model	QoS Details	Applicable
Data, Voice, & Best Effort	Real-Time (18%) : Voice (EF, LLQ= 18%) Critical Data (57%) : Routing (CS6, CBWFQ=3%), Critical Data (25, CBWFQ=54%, WRED) Best Effort (25%) : Best Effort (DSCP 0), Scavenger (CS1)	Internet Edge, Routers
Data and Best Effort (Basic)	Data (75%) : Routing (CS6, CBWFQ=3%), Critical Data (25, CBWFQ=72%, WRED) Best Effort (25%) : Best Effort (DSCP 0), Scavenger (CS1)	Internet Edge, Routers
Data and Best Effort (Advanced)	Routing (CS6, CBWFQ=3%) GOLD Data (AF25, CBWFQ=42%, WRED) SILVER Data (AF21, CBWFQ=30%, WRED) ; these percentages for GOLD and SILVER can be adjusted Best Effort (25%) : Best Effort (DSCP 0), BRONZE Data (CS1)	Internet Edge, Routers
Data and Voice (Optional) ; activated only when congestion occurs	PLATINUM (for Voice) : DSCP EF (for Voice), AF41 (for Video), LLQ = usually 18-33% GOLD (for Critical Data) : DSCP 25, PREF 4, LLQ = 50% SILVER (for Medium Critical Data) : DSCP AF21, PREF 3, CBWFQ/LLQ = 25% BRONZE (for Very Low Data) : DSCP CS1, CBWFQ=1% Best-Effort (everything else) : DSCP 0, CBWFQ=24%, WRED	Internet Edge
Data and Voice (Optional) ; bandwidth guarantees at all times	Warning: Exceeding Police will drop packets PLATINUM (for Voice) : DSCP EF (for Voice), AF41 (for Video), Police usually 128kbps GOLD (for Critical Data) : DSCP 25, PREF 4, Police = 50% of Bw SILVER (for Medium/Somewhat Critical Data) : DSCP AF21, PREF 3, Police = 25% of Bw BRONZE (for Very Low Data) : DSCP CS1, Police = 1% of Bw Best-Effort (everything else) : DSCP 0, Police = 24% of Bw, WRED	Internet Edge

Example: Data and Voice (Optional) I:

class-map match-any platinum match ip dscp ef match ip dscp af41 match access-group ACL-PLATINUM class-map match-any gold match ip dscp 25 match access-group ACL-GOLD class-map match-any silver match ip dscp af21 match access-group ACL-SILVER class-map match-any bronze match ip dscp cs1 match access-group ACL-BRONZE	policy-map IE-POL class platinum priority percent 33 class gold priority percent 50 class silver bandwidth percent 25 class bronze bandwidth percent 1 class class-default fair-queue bandwidth percent 24

For QoS operations within the MPLS VPN solution determine the best QoS policy to implement for the design.

Solution or Service	Class Model	Applicable
Voice & Data (3 Class)	Real-Time (35%) : Voice RTP (EF, LLQ=18%), Voice Control (AF31/CS3 > CS5, LLQ=2%), Interactive Video (AF41 >CS5, LLQ=15%) Critical Data (40%) : Routing (CS6, CBWFQ=3%), Critical Data (25 >AF31, CBWFQ=20%, WRED), Transactional Data (AF21 >CS3, CBWFQ=15%, WRED), Network Mgmt. (CS2 > CS3, CBWFQ=2%) Best Effort (25%) : Best Effort (DSCP 0, CBWFQ=24%, WRED), Scavenger (CS1, CBWFQ=1%)	MPLS (CE)
Voice, Video, Data (4 Class)	Real-Time (35%) : Voice RTP (EF, LLQ=18%), Voice Control (AF31/CS3 > CS5, LLQ=2%), Interactive Video (AF41 >CS5, LLQ=15%) Critical Data (20%) : Routing (CS6, CBWFQ=3%), Critical Data (25 >AF31, CBWFQ=12%, WRED), Transactional Data (AF21 >CS3, CBWFQ=10%, WRED) Video (15%) : Streaming Video (CS4>AF21, CBWFQ=13%), Network Mgmt. (CS2 >CS3, CBWFQ=2%) Bulk Data (5%) : Bulk Data (AF11) Best Effort (25%) : Best Effort (DSCP 0, CBWFQ=24%, WRED), Scavenger (CS1, CBWFQ=1%)	MPLS (CE)
Voice, Video, Data (5 Class)	Real-Time (35%) : Voice RTP (EF, LLQ=18%), Voice Control (AF31/CS3 > CS5, LLQ=2%), Interactive Video (AF41 >CS5, LLQ=15%) Critical Data (25%) : Routing (CS6, CBWFQ=3%), Critical Data (25 >AF31, CBWFQ=12%, WRED), Transactional Data (AF21 >CS3, CBWFQ=5%, WRED) Video (15%) : Streaming Video (CS4>AF21, CBWFQ=13%), Network Mgmt. (CS2 >CS3, CBWFQ=2%) Best Effort (25%) : Best Effort (DSCP 0, CBWFQ=24%, WRED), Scavenger (CS1, CBWFQ=1%)	MPLS (CE)
Voice, Video, Data (3 Class)	Real-Time (35%) : DSCP EF/CS5, LLQ=35% Critical Data (40%) : DSCP CS6/AF31/CS3, CBWFQ=40%, DSCP-WRED Best Effort : WFQ, WRED	MPLS (PE) >3Mb/s on access link
Voice, Video, Data (4 Class)	Real-Time : DSCP EF/CS5, LLQ=35% Critical Data : DSCP CS6/AF31/CS3, CBWFQ=25%, DSCP-WRED Video : DSCP AF21/CS2, CBWFQ=15%, DSCP-WRED Best Effort : WFQ, WRED	MPLS (PE) >3Mb/s on access link
Voice, Video, Data (5 Class)	Real-Time : DSCP EF/CS5, LLQ=35% Critical Data : DSCP CS6/AF31/CS3, CBWFQ=20%, DSCP-WRED Video : DSCP AF21/CS2, CBWFQ=15%, DSCP-WRED Bulk Data : DSCP AF11/CS1, CBWFQ=5%, DSCP-WRED Best Effort : WFQ, WRED	MPLS (PE) >3Mb/s on access link
Short Pipe Mode (5 Class)	Real-Time : DSCP EF/CS5 > EXP 5 (conform), Drop (exceed) Critical Data : DSCP CS6/AF31/CS3 > EXP 3 (conform), EXP 7 (exceed) Video : DSCP AF21/CS2 > EXP 2 (conform), Drop (exceed) Bulk Data : DSCP AF11/CS1, > EXP 1 (conform), EXP 6 (exceed) Best Effort : DSCP 0 > EXP 0 (conform), EXP 4 (exceed)	Short Pipe (PE)
Pipe Mode (5 Class)	Real-Time : DSCP EF/CS5 > EXP 5 (conform) > QG5, Drop (exceed) Critical Data : DSCP CS6/AF31/CS3 > EXP 3 (conform) > QG3, EXP 7 (exceed) > QG3/DC1 Video : DSCP AF21/CS2 > EXP 2 (conform) > QG2, Drop (exceed) Bulk Data : DSCP AF11/CS1, > EXP 1 (conform) > QG1, EXP 6 (exceed) > QG1/DC1 Best Effort : DSCP 0 > EXP 0 (conform) > QG0, EXP 4 (exceed) > QG0/DC1	Pipe Mode (PE)

Example: Voice & Data (3 Class) for MPLS CE

class-map match-any VOICE match ip dscp ef class-map match-any VOICE-CONTROL match ip dscp af31 match ip dscp cs3 class-map match-any INTERACTIVE-VIDEO match ip dscp af41 class-map match-any ROUTING match ip dscp cs6 class-map match-any DATA-MISSION-CRITICAL match ip dscp 25 class-map match-any DATA-TRANSACTIONAL match ip dscp af21 class-map match-any DATA-NETWORK-MGMT match ip dscp cs2	policy-map MPLS-POL class VOICE priority percent 18 class VOICE-CONTROL priority percent 2 set ip dscp cs5 class INTERACTIVE-VIDEO priority percent 15 set ip dscp cs5 class ROUTING bandwidth percent 3 class DATA-MISSION-CRITICAL bandwidth percent 20 set ip dscp af31 random-detect class DATA-TRANSACTIONAL bandwidth percent 15 set ip dscp cs3 random-detect class DATA-NETWORK-MGMT bandwidth percent 2 set ip dscp cs3

class-map match-any DATA-SCAVENGER match ip dscp cs1	class DATA-SCAVENGER bandwidth percent 1 class class-default bandwidth percent 24 random-detect

Resources

Application	DSCP	PHB	CoS
Network Control	CS7	56-63	7
Internetwork Control	CS6	48-55	6
Voice (Payload)	EF	46	5
Video Conferencing	AF41-43	34,36,38	4
Voice Signaling	CS3	24	3
High Priority Data	AF21-23	18,20,22	2
Medium Priority Data	AF11-13	10,12,14	1
Best-Effort	0	0	0

R

~ Services ~

Root Guard

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN and/or Data Center Solution

Configured on the LAN Distribution downlink ports to the LAN Access switches to prevent the port connected to the LAN Access in becoming a root port, hence acting as a root bridge on the L2 network.

Routing, IP

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN, Data Center, WAN, and/or Internet Edge (under Solutions)

Complete the steps below if IP Routing related services will be implemented in the design:

Step 1

Gather all subnets that will be used

Gather all the subnets determined from the chosen foundation and network solution designs. Below are some of the solutions where subnet details were determined.

- LAN/Campus
- WAN
- Data Center
- Internet Edge
- Voice (Unified Communications)
- Wireless
- DMZ & Extranet

Step 2

Where will each subnet be routed?

Determine where the subnet will be routed based on the topology and the components that exist. This would be one of the following Layer 3 (L3) devices in the design:

- **Router:** the subnet is configured on a router's interface, but will depend if there are enough interfaces on the router. Common for Internet Edge or WAN routers in small sized networks.
- **L3-Switch:** the subnet is configured on the Core switch as a L3 port or on a VLAN SVI port (recommended). This is recommended for better flexibility and scalability configured on the Core (or Distribution/Aggregation for larger networks). This is very common for SMB, medium, and large networks using a lot of subnets on the network.
- **Firewall:** the subnet is configured on one of the firewall interfaces or as a sub-interface (using 802.1Q) like a DMZ network. This is common for small and SMB networks using 1 or 2 subnets on the network.
- **None:** no IP routing is required for communication with other networks and the subnet is not configured on any network devices. It's only configured on the systems within an isolated network or VLAN.

Determine the routing protocols that will be used within the network topology. This is important to allow routing capabilities between other networks (internal or external) that may exist:

Type	Protocol	Description
Static	<i>Static</i>	Provide static routing among a small set of L3 devices on the network. Or if no routing devices exist on the network.
IGP (internal)	<i>OSPF or IS-IS</i>	Provide dynamic routing with multiple Cisco or non-Cisco routing devices on the network.
	<i>EIGRP</i>	Provide dynamic routing with multiple Cisco routing devices on the network.
EGP (external)	<i>BGP</i>	Provide routing with an ISP using a registered (or leased) public subnet that will be advertised through the Internet. This includes Internet redundancy using the same Public subnet for hosts on the LAN or Data Center.
LISP	<i>LISP</i>	Provides many robust capabilities such as (1) reducing the global routing table size. (2) Provide host and VM mobility across the network. (3) Provide shortest routing path to a node. (4) Support for multi-homing and load balancing. (5) Ideal for IPv4 to IPv6 transition.

Design Notes:

- **IGP** (Internal): routing that is used internally within the LAN, Data Center and sites across the WAN.
- **EGP** (External): routing that is used to the public network (Internet) including advertising public address information to all internet providers.

For each L3 device determine how the default gateway will be configured based on one of the following routing types:

- **Static:** default static route is configured towards another L3 device for accessing any network doesn't exist in the routing table. This is common for edge routers or firewalls that are not using BGP on the edge.
- **IGP (OSPF, EIGRP):** a dynamic routing protocol can be configured to advertise a default route to all L3 devices enabled for that routing protocol. Or receive a default route dynamically from another router. This is recommended for medium networks, large networks, or any environment running a dynamic routing protocol (e.g. OSPF, EIGRP).
- **EGP (BGP):** if BGP is configured to the Internet provider(s), a BGP default route can be advertised by the ISP and can be used for the default gateway internally by the other devices.

Default Gateway Root: for each L3 device on the network, their default gateway will eventually be pointed towards one single point. Whether it is statically configured or dynamically received from a dynamic routing protocol (IGP, EGP). Determine where the root of the default gateway will exist in the network topology. It will point to one of these components:

- Core Switch
- Edge Router
- Firewall appliance

Example: a network topology consist of a 2-tier LAN and WAN running OSPF (IGP). In the topology, the **Core switch** will advertise a default route to all L3 devices on the network. The default gateway root would be the Core switch in this topology. The Core switch may have its own static default route pointing to an Edge router or firewall perhaps.

Determine if any security filtering should be applied to or from the subnet that would be routed between other networks. Below are methods that can be used for providing security for a subnet's L3 interface:

- **Using ACLs:** when the subnet's routed interface is on a router or L3-switch. This is recommended especially if the subnet is configured on a L3-switch.
- **Using a Firewall:** when the subnet's routed interface is on the firewall.
- **Virtualization (VLAN, VRF):** (1) the subnet is in a VLAN (without an SVI interface) isolated from other subnets (VLANs). If communication with other subnets is required then the VLAN SVI interface can be configured with ACLs. (2) Or the subnet can also be configured in a VRF which is isolated using a different routing table. Subnets in a VRF can communicate with other networks by implementing various sub-services used by VRF-lite and MPLS with changes to the route targets. Using VRF is common for larger size networks.
- **None:** no security configuration is needed on the subnet's routed interface.
- **Isolated:** the subnet is completely separated (a closed network) not connected to any other network. Common for high security and classified networks, but provides limited flexibility for accessing other networks if needed.

Below are additional routing related services that are optional or recommended to be included for the routing design:

- **IP CEF** (recommended): an advanced Layer 3 switching technology that provides hardware forwarding of traffic for increased performance and scalability for networks.
- **Policy Based Routing** (optional): this is used for unique routing requirements not easily accomplished through static or dynamic routing protocols. For example, you can force routing for a particular computer/server to be routed through a specific interface not chosen by a routing protocol. In most environments PBR is not needed and should be avoided to keep the routing environment simplified.

Below are additional security control that can be implemented with the routing environment:

- **NULL (Black Hole) Routing**: this is an optional security measure where you can configure static routes for host IP Addresses (internal or external) that should be restricted for access. The next hop for these addresses would be the NULL interface where packets to that IP would be discarded.

S

~ Services ~

Security Best Practices

Category: General Practices, Network Service (Security)
Prerequisite(s): --

SEC NM

Below are security best practices that should be implemented into the design for deployment.

- **Proxy ARP:** disable proxy-arp services on all interfaces especially Firewall interfaces which can cause performance related issues on the network.
- **Unicast Reserve Path Forwarding (uRPF):** used to protect against source IP spoofing attacks. Checks the source IP address of each packet received against the routing table. If the source IP is not right for the interface on which it is received the packet is dropped. Enable on outbound facing interfaces for untrusted WAN ports this includes the Internet Edge Router and the Firewall's untrusted/outside port.
- **Scheduler:** configure a scheduler on a Cisco router/switch to prevent against fast flooding attacks and processes. This will allow adequate processor time for control plane services. Set schedule interval to 500ms.
- **ACL for Services:** for tighter security implement ACL policies for SNMP and NTP services.
- **Time Services:** configuring time related functions on all network devices is highly recommended. It will provide proper timestamps for logs and events reported. Therefore configure NTP, service timestamps, and timezones for all network devices (router, switch, firewall) on the network.
- **Unused Interfaces:** any interface not used on a network device should either be placed in a shutdown state or configured in a disabled VLAN.
- **Banner:** configuring a Message of the Day (MOTD) banner is recommended using a message of unauthorized access into the device. Never use words like "Welcome" for a message banner as it illustrates that anyone can access the device without any authorization.
- **Macros:** configure macros which are like configuration templates for common switch ports (or router interfaces) based on whether it is a server, desktop, or a desktop with an IP Phone connected. This will help with the overall administration on the network devices.
- **Interfaces:** Proxy-ARP, IP Unreachables, Directed Broadcast, and IP Mask Reply should be disabled.
 - *IP Unreachables:* should be disabled to prevent denied ACL traffic being leaked to the control plane (e.g. MFSC at 10pps per VLAN)
- **Disable Services:** as a general best practice the following services should be disabled globally on all network devices:
 - TCP and UDP small services
 - BOOTP services
 - Finger
 - Configuration Autoload
 - PAD
 - HTTP services
 - CDP: it can be enabled globally, but disabled on the interface level
- **Other Best Practice Services**
 - Password Encryption: enable globally on all network devices to provide basic encryption, but configuring MD5 passwords for increased security is strongly recommended.
- **Control Plane Protection:** below are services that can be implemented to protect control plane related traffic on a network device:
 - Cisco Express Forwarding (CEF)
 - Software/Hardware Control Plane Policing (CoPP)
 - Hardware Rate Limiters (MLS rate limiters)
 - Access Control Lists (ACL)
 - Storm Control

- Selective Packet Discard (SPD) checks
- **Data Plane Protection:** below are services that can be implemented to protect the data plane were traffic is forwarded in hardware:
 - DHCP Snooping
 - Dynamic ARP Inspection (DAI)
 - IP Source Guard

SNMP

Category: Network Service (Network Management)
Prerequisite(s): --

Go to “Network Management Services”

Spanning Tree Protocol (STP)

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN and/or Data Center (under Solutions), VLAN (under Services)

Step 1

Spanning Tree Protocol

DA R SC

Determine the Spanning Tree Protocol (STP) that will be used on the switching network.

- **R-PVST+ (Rapid Spanning Tree Protocol) or 802.11w:** recommended STP to provide fast convergence (around 900ms) in the event of a failure on the layer 2 network. It is also backwards compatible with the legacy STP (PVST), but for newer switching devices they will support RSTP. RSTP can scale up to 10,000 logical ports and 1800 virtual ports per switching module. Cisco NX-OS supports 16,000 logical ports.
- **PVST (Per VLAN Spanning Tree):** this is a legacy STP and if RSTP is not supported use this protocol, which is the default for all switches. If a failure occurs on the L2 networks it will result in longer convergence (45 seconds to a minute or longer depending on the size of the L2 network).
- **MST (Multiple Spanning Tree) or 802.11s:** used with very large L2 networks which operates similar to BGP Confederations by creating multiple spanning tree domains. If the STP active logical ports and virtual ports per line card (applicable for Cisco Catalyst 4500 and 6500 series models) is high it's recommended to use MST. MST can scale up to 50,000 logical ports and 6,000 virtual ports per switching module. Cisco NX-OS supports 75,000 logical ports.

Recommendations: use Rapid Spanning Tree Protocol (RSTP), however, calculate the expected number of active logical ports and virtual ports which is found below under “STP Scalability” to confirm the correct STP to use on the network. However, majority of networks will fall within the requirements for using R-PVST+ (RSTP). Furthermore, do not change the STP timers, keep the default timers in place.

Cisco Nexus Best Practices: the dispute mechanism is enabled by default to detect uni-directional link failures. Configure the port type “network” for bridge assurance (BA) on interfaces if the feature is supported on both end.

STP Scalability – Calculate Active Logical Ports

Formula: (Total trunk ports on switch) x (active VLANs on trunk) + (total of non-Trunking ports)

Active Logical Port Best Practices:

- **R-PVST+ (802.11w):** 10,000 total
- **MST (802.11s):** 50,000 total

Example: let's say that the network consist of a two-tier Data Center topology (Core and Access layer). We have two Core switches for redundancy connecting down to 4 access switches. These are trunk connections including the inter-connection between the two Core switches. The Data Core switch will also have two non-trunk connections to a WAN router and a firewall appliance.

In this environment we will only use 10 VLANs. Therefore, what is the total number of active logical ports using the formula and info from our scenario?

- **Trunk Interfaces:** 5 (to all 4 access switches and 1 for the interconnection)
- **VLANs:** 10
- **Non-Trunk Interfaces:** 2 (one to the WAN router and the other to the firewall appliance).

$5 * 10 + 2 = 52$ active logical ports.

We are well below 10,000 so we can use RSTP for the STP.

However, always consider potential scalability that can exist with the Access switches. Let's consider that our Data Center Access doubles from 4 to 8 access switches plus we double our VLAN size from 10 to 20 VLANs. Let's re-calculate using this new information:

- **Trunk Interfaces:** 9 (to all 8 access switches and 1 for the interconnection)
- **VLANs:** 20
- **Non-Trunk Interfaces:** 2 (one to the WAN router and the other to the firewall appliance)

$9 * 20 + 2 = 182$ active logical ports.

Still applicable for us to use RSTP

To view the number of active logical ports issue the command: **"show spanning-tree summary total"**. This command is supported on certain Cisco hardware.

STP Scalability – Calculate Virtual Ports

Formula: (sum of all ports used as trunks on the line module) x (active VLANs on the trunk ports)

Active Logical Port Best Practices:

- **R-PVST+ (802.11w):** 1,800 per switching module
- **MST (802.11s):** 6,000 per switching module

Applicable: Chassis switches (Cisco Catalyst 6500 series) using line modules

Example: let's say we have a Data Center Core switch using the Cisco Catalyst 6500 with 48-Port GE line modules. All 48 ports will either be trunk ports or edge ports. In this environment we will use 10 VLANs. Therefore, what is the total number of virtual ports per line module using the formula and the info from our scenario?

- **Trunk and Switch Ports:** 48
- **VLANs:** 10

$48 * 10 = 480$ virtual ports.

We are well below 1,800 for that line module so we can use RSTP for the STP.

However, always consider potential scalability of switch ports and VLANs added to the environment. Let's say that we double our VLAN size from 10 to 20 VLANs. Let's re-calculate using this new information:

- **Trunk and Switch Ports:** 48
- **VLANs:** 20

48 x 20 = 960 virtual ports.

Still applicable for us to use RSTP

To view the number of virtual ports for a line module (like slot 3) issue the command **“show vlan virtual-port slot 3”**. This command is applicable to the Cisco Catalyst 6500 series switches.

Step 2

Root Bridge

SC

Each VLAN configured on the network must use a L2/L3 switch to be the root bridge. This is an important operation for preventing loops by determining what ports should be forwarding and what ports should be blocked for each VLAN. Below are the recommended locations where the root bridge (for each VLAN) should be implemented.

- **Core:** common for small, SMB, and medium networks that are using a two-tier topology with a collapsed core with connected access switches. Each VLAN root bridge would be configured on the Core device.
- **Distribution (or Aggregation):** common for medium and large networks (or any size) that is using a three-tier topology with a Core, Distribution/Aggregation, and Access layer. If VLANs are used for users or servers within the access layer it is recommended to configure the root bridge for those VLANs on the Distribution (or Aggregation) devices.

Step 3

STP Path Cost

DA R

Recommended to optimize the STP Path Cost method to “long” globally on Data Center switches (LAN Switches can also be considered). This causes SPT to use 32-bit based values when determining the port path cost compared to the default 16-bit value which improves the root path selection when Port Channeling using PAgP is configured.

SSL VPN

Category: Network Service (Security)
Prerequisite(s): VPN & Remote Access (under Solutions)

SEC

When to use: require direct or limited access to resources on the internal network(s). Depending on the level of access, the client can either use a VPN program installed on their endpoint or using a web browser with minimal software installed on the client.

Description: Next-Generation VPN protocol used by clients using their web browser or an installed application (for full network access) to connect into a network to access network resources.

Hardware Required: Routers *OR* Firewalls

SSL VPN is a client VPN (remote access) solution where clients can use HTTPS/SSL for remote access connectivity which uses a SSL tunnel rather than the many ports required for IPsec VPN. Below are the methods for how SSL VPN can be setup and used.

- **Web Client or Web Mode (Clientless):** client doesn't need to install any software and can simply use a web browser to access any web-based service through a secure web session.
- **Tunnel Mode (SVC):** client installs a SSL VPN program on their system (or during the login process it will automatically install the program) which establishes a SSL VPN tunnel. This allows the client to access any network resource other than web-based applications. This mode operates the same way as the Client IPsec VPN solution and is the most common deployment for SSL VPN out of the three.
- **Thin-Client Mode:** this is a mixture between Clientless and Tunnel mode. In this mode, login is done through a web browser with certain ports (e.g. SMTP, TCP/25) opened to allow access to applications like Outlook. This requires a bit of work and is not commonly used out of three unless limited port forwarding will be used.

SLA, IP

Category: Network Service (Routing and Switching)

Prerequisite(s): Firewall, Internet Edge, and/or WAN (under Solutions)

IP SLA: provides intelligent re-routing/failover between connections based on a pre-configured probe.

Source Guard, IP

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN and/or Data Center (under Solutions), DHCP Snooping (under Services)

When to use: to prevent against IP address spoofing attacks on the network. This feature should be configured on all Access Switches.

IP Source Guard (also called IP Spoofing) prevents a packet from using an incorrect source IP address to change its true source address. It gathers information from DHCP snooping to dynamically configure a port access control list (PACL) on the interface that restricts any traffic from IP addresses that are not in the DHCP binding table.

Stacking Technology

Category: Network Service (Hardware)

Prerequisite(s): LAN and/or Data Center (under Solutions)

When to use: using resilient redundancy for the LAN and/or Data Center topology.

Below are some hardware details about using different stack technologies with hardware that supports it:

- **Cisco StackWise Plus** – supported on selected number of Cisco Catalyst switches that can stack up to 9 switches with sub-second failure recovery.
- **Cisco StackPower** – shares power across a stack of Cisco Catalyst 3750-X switches for allowing flexible use of the power supplies.

Stateful Switchover (SSO)

Category: Network Service (Network Management)

Prerequisite(s): --

Go to “NSF & SSO”

Static Routing

Category: Network Service (Routing and Switching)
Prerequisite(s): Routing, IP (under Services)

DA

When routing with none, one, or a few routing devices.

Recommendations: this is the simplest form of routing to setup for small sized networks. For larger networks the administration will be very high. This is common for small and SMB environments or networks with 1-3 routing devices (e.g. routers, L3-switch, firewall).

Syslog

Category: Network Service (Network Management)
Prerequisite(s): --

Go to *"Network Management Services"*



~ Services ~

Trunking (802.1Q)

Category: Network Service (Routing and Switching)
Prerequisite(s): VLAN and VTP (under Services)

DA SEC

If more than one VLAN will be used on the network then 802.1Q is required. 802.1Q and ISL are two Trunking protocols that support what is called VLAN tagging. ISL is a Cisco based protocol that is not commonly used or recommended. 802.1Q is recommended and is the most common Trunking protocol to use for supporting up to 4000 VLANs. Below are the design points relevant for 802.1Q:

- **Native VLAN:** the Native VLAN is the only VLAN that is untagged and can be exploited in VLAN Hopping attacks. Therefore as a best practice configure the native VLAN for 802.1Q ports to use a bit-bucket VLAN (e.g. VLAN999) that is in a shutdown state and not routable with other networks/VLANs. You can also force all native VLANs to be tagged and 802.1q should be disabled on all edge ports. *Note:* if you want to tag the native VLAN for additional security then you can enable the command “vlan dot1q tag native” on the L2/L3 switches.
- **Trunk Mode** (if applicable): you can configure the Trunking mode to be “on” for both ends, but it's recommended to use the mode “desirable” for the trunk ports.
- **Dynamic Trunk Port (DTP):** as a best practice configure DTP to not negotiate and trust the encapsulation protocol that is used for the Trunking interface, which is 802.1Q. This will put the port into a permanent Trunking mode and does not allow the port to generate DTP frames. In general always try to avoid any type of negotiation of protocols between critical devices.
- **Extended VLANs:** if 1000 to 4000 VLANs will be used on the network then the system ID needs to be extended on all L2/L3 switches, which is something that is configured with the Spanning Tree Protocol (STP).
- **VLAN Trunk Security:** it's a good practice to allow only the VLANs that are needed for a device (e.g. Wireless AP, switch) and nothing more. For example, if the WLAN uses only two VLANs then only those VLANs should be allowed to the access point.

TrustSec (Cisco)

Category: Network Service (Security)
Prerequisite(s): Identity Access Control Solution

DA SEC

#1

Overview

Cisco TrustSec (CTS) provides security based on the identity of a user/group role in an organization with a network topology. Security policies for what a user or group can access is managed from an identity-aware appliance which are pushed down to the network equipment for enforcement. It provides IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption using the higher-end network equipment (e.g. Cisco Catalyst 6500 using Sup-2T, Nexus 7000) to prevent against attacks within a security policy and group transactions. In a nutshell, CTS is a feature that basically uses Access Control Lists (ACL) which are applied to switch ports for what that connected port can access. This security policy is pushed down from a dedicated security appliance based on that user's assigned group on the directory server (e.g. Active Directory). This feature is strongly recommended for environments seeking high security and following a required compliancy (e.g. SOX, HIPPA, PCI).

Below are some of the main aspects and terminologies of Cisco TrustSec:

- **Security Group Access (SGA):** allows user identity information to be associated with their network traffic and then passed throughout the network. That information can be used to enforce an access policy using Security Group Tags (SGT) and Security Group Access Control Lists (SGACL).

#2

Best Practices and Considerations

Below are best practices for using Cisco TrustSec on the network.

- Use digital certificates when deploying 802.1X to provide a higher level of assurance than just a username and password.

#3

Caveats

Below are some caveats to keep in mind while using this service:

- **Disable port security timers:** If port security and 802.1X are both enabled on a switch port, their set of timers that could conflict with each other. The conflict causes 802.1X to re-authenticate every time the port security time out is reached. To avoid this issue, the port security timers should be disabled.

#4	Add-Ons

Below are other features that can be implemented or overlay with Cisco TrustSec:

- **SGT Exchange Protocol (SXP):** used to propagate the IP-to-SGT bindings to network devices that do not support SGTs like a Cisco ASA firewall. SXP establishes a peering relationship between two devices to exchange the IP-to-SGT bindings. The peer will either operate in a speaker role or a listener role. The speaker (e.g. Cisco Core or Access switch) will pass the IP-to-SGT bindings to the listener (e.g. Cisco ASA).
- IEEE 802.1AE MACsec encryption

U

~ Services ~

UDLD

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)

R

UDLD is a feature that monitors the physical configuration of the network cable (ideal for fiber based ports) to detect for unidirectional links that can cause problems with STP and creating possible loops. If there is a unidirectional link detected on a physical interface it will disable the affected interface providing faster link failure detection. The following should be considered when using UDLDs on the network between devices.

- UDLD Aggressive (recommended) should be configured on a per-port bases (between switches) not globally.
- UDLD should be enabled between two directly connected devices. If a Transparent (L2) device like a Firewall is deployed then UDLD should not be enabled.

Cisco Nexus Best Practices: implement UDLD normal mode on L2 switch-to-switch interfaces including switch-to-switch connections using Copper wiring. Configure UDLD aggressive mode on L2 and L3 port channel member ports to avoid traffic being black-holed.

Uplink Fast

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)

R

Enable on Access switches to quickly move a blocked port to a forwarding port automatically if there is a direct link failure.



~ Services ~

Virtual Extensible LAN (VXLAN)

Category: Network Service (DCI)

Prerequisite(s): Data Center and WAN (under Solutions)

When to use: using a IaaS cloud solution for a large multi-tenant data center with thousands of potential customers networks. Below are other use-cases for VXLAN:

- Using virtual access switches with virtual machines assigned to a particular VXLAN

Below are advantages for deploying VXLANs instead of VLANs in a Data Center topology:

- It runs over IP
- It is more scalable compared to VLANs. It supports up to 16 million unique identifiers.
- Virtual machines connected to a VXLAN will be unaware they are on a VXLAN, so virtual machines can move across different subnets. Other alternatives include vCDNI (VMware solution) including the combination of EVB (802.1Qbg) and PBB (802.1ah) working together.

#1

Overview

VXLAN is the next-generation of VLANs to provide network isolation on a Data Center network.

It provides Layer 2 connectivity across a Layer 3 network supported on most Cisco Nexus series switches. VXLAN provides higher scalability to allow more Layer 2 segments. VLANs use a 12-bit VLAN ID which limits to only 4096 VLANs. VXLAN uses a 24-bit segment ID known as the VXLAN network identifier (VNID) which enables up to 16 million VXLAN segments to coexist in the same administration domain.

VXLAN packets (including the original L2 frame and the VXLAN header) are encapsulated inside of a UDP/IP packet. The UDP packet is then encapsulated inside of a IP packet. And the IP packet is encapsulated into an Ethernet frame with a MAC header and FCS trailer. This is also called MAC address-in-UDP (MAC-in-UDP) encapsulation which allows VXLAN packets to be transported across a L3 network. This is great for taking advantage of Layer 3 routing, ECMP, and link aggregation protocols to use all available paths. Where with VLANs, it uses the Spanning Tree Protocol (STP) which blocks redundant paths for loop prevention and not using all network links available.

VXLAN has a 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes into the UDP payload.

Below are the components for how the VXLAN topology is deployed:

- **VXLAN Tunnel End Point (VTEP):** this component has two interfaces. The LAN facing interface of the VTEP connects towards the end systems (e.g. customer network). The WAN facing interface of the VTEP connects directly into the IP transport network. Within the Data Center topology, the VTEP component would likely be integrated with the Data Center access switch (physical or virtual). But it would be logically separated from the access switch. This component is also responsible for the following functions:
 - o Responsible for inserting and removing (or interpreting) the VXLAN header within the IP/UDP payload.
 - o Each VTEP has a unique IP address which is used to identify each VTEP device on the network. It is also used for encapsulating Ethernet frames and transmitting the encapsulated packets across the Layer 3 network through the IP interface.
 - o Discover other VTEP devices to learn about remote MAC Address-to-VTEP mappings through its IP enabled interface. It builds stateless tunnels between other VTEP devices to transmit traffic.
 - o Uses Internet Group Membership Protocol (IGMP) to join IP multicast groups. VXLAN ID to be carried over the IP interface between VTEPs, each VXLAN is associated with an IP multicast group. The IP multicast group is used as communication bus between each VTEP to carry broadcast, multicast and unknown unicast frames to every VTEP participating in the VXLAN. VXLANs Multicast group (for unknown/broadcast/multicast). The VTEP function also works the same way as a learning bridge, in that if it doesn't know where a given destination MAC is, it floods the frame.

Below are some caveats to keep in mind while using this IaaS based service:

- Not ideal to be used over long distances. It is designed to operate within a single administrative domain (e.g. a Data Center) and not across the Internet. But can still be extended beyond the typical reach of VLANs and 802.1Q today.
- Cannot be translated (or mapped) to a specific VLAN (not yet).
- Lack of native VXLAN support on desktop and server endpoints.
- **Multicast:** It is possible to have multiple VXLAN segments share a single IP multicast group in the network, though there are scalability concerns. It can help to conserve multicast control plane resources, but it doesn't provide optimal multicast forwarding resulting in possible higher utilization. For example, packets from a VTEP could be forwarded to a multicast group for one tenant (a VXLAN segment), but it is also sent to all other VTEP devices that share the same multicast group. This can result in higher utilization of multicast data plane resources. Including VXLAN traffic being sent needlessly to a VTEP component that has no end systems connected to that VXLAN.
- **MTU:** Due to the MAC-to-UDP encapsulation, VXLAN introduces a 50-byte overhead to the original frames. The transport network needs to be configured to use 1550-byte packets (minimum). Jumbo frame support in the Layer 3 network is required if the overlay applications will use larger frame sizes than 1500 bytes.

#4	Add-Ons

Below are other add-ons that can be implemented or overlay with VXLAN:

Technology/Feature	Description	Prerequisite(s)
VXLAN Gateway	A VXLAN gateway connects VXLAN and VLAN segments as one forwarding domain across the layer 3 network. It can be enabled on a VTEP device to combine a VXLAN segment and a classic VLAN segment into one common layer 2 domain. A Cisco Nexus 9000 series switch can function as a hardware-based VXLAN gateway (and VTEP device) providing encapsulation and de-encapsulation with line-rate performance for all frame sizes.	--

#5	Best Practices and Considerations

Below are best practices to consider while deploying this service:

- Ideal to use one VXLAN segment mapping to one IP multicast group to provide optimal multicast forwarding

Virtual LAN (VLAN)

Category: Network Service (Routing and Switching)
Prerequisite(s): VTP (under Services)



For each subnet that is determined from the solutions they can be configured as a VLAN on the L2 network. In general the following should be considered when using VLANs on the network:

- Do not use VLAN1 (the default).
- Use separate VLANs for Data and Voice traffic.
- **Private VLANs:** creates sub-VLANs within a single VLAN. Private VLANs are used to provide stronger security between hosts within the same VLAN. This is an uncommon VLAN mechanism deployed in LAN/Data Center switching environments unless unique security requirements call for it.
- As a best practice configure a small set of VLANs per switch (<30 VLANs should be created).
- Create user VLANs per Department, Building, Floor, or Quadrant.
- Use different Server Farm VLANs for Infrastructure, Applications, Database, Management, and Security.

VLAN Trunking Protocol (VTP)

Category: Network Service (Routing and Switching)
Prerequisite(s): LAN and/or Data Center (under Solutions)

DA SEC

VLAN Trunking Protocol (VTP) is used for administrating VLANs (added or removed) on the layer 2 network. Determine the VTP mode that will be configured for each L2 device on the network based on the following options.

- **Transparent:** this is the recommended VTP mode to use for all L2 devices on the network. The drawback is VLANs are administered for each device, but it avoids losing an entire VLAN (hence subnet) on the network that can occur when using VTP Server and Client modes. In transparent mode, adding (or removing) VLANs is done manually from each L2 device where needed.
- **Server:** a VTP mode that allows creating and removing VLANs on a L2 device that is propagated to other L2 devices in the same domain. These VTP changes can update other L2 devices that operate in either the VTP client mode or server mode. This is ideal for large environments when administrating large number of VLANs. However, there are serious dangers that a rogue switch (using a higher configuration revision value) could be plugged into the network and quickly removing VLANs on all switches in the same VTP domain. If a VTP server is used it should be enabled on the Core or Distribution/Aggregation devices only.
- **Client:** a VTP mode that is read-only and cannot create (or remove) VLANs. They receive all VLAN information created from a VTP server in the same domain. If a VTP server is used on the layer 2 network then the Access switches should be enabled as VTP Clients.

Other VTP deployment details include the following:

- **Domain:** a VTP domain must be defined for each L2 device regardless of the VTP mode that is configured. It becomes very important when using VTP Servers and Clients on the L2 network.
- **VTP Password:** If VTP Server and Client modes are used then you can configure a VTP password that each L2 device in that domain must have for creating or accepting VLAN changes.

Recommendations: (1) use VTP Transparent mode for all L2/L3 switches on the network. Try to avoid using VTP Server/Client mode configuration on switches. If it is desired for simpler VLAN management then enforce VTP passwords in your VTP domain. (2) For larger switching networks using a three-tier topology and a server-client VTP model its recommended to configure a VTP domain per distribution block (Distribution/Aggregation and Access switches) than using a single VTP domain for all distribution blocks.

Cisco Nexus Best Practices: configure VTP transparent mode if the VTP domain needs to be extended across other Nexus switches configured are VTP server and client modes.

Virtual Port Channel (vPC)

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN and/or Data Center (under Solutions), Cisco Nexus (Hardware)

R

When to Use: to provide the ability to build a L2 Port Channel from two different Cisco Nexus switches to a single access switch.

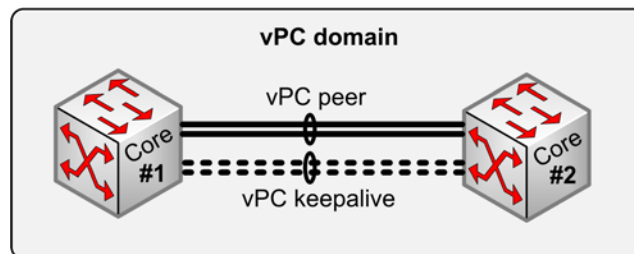
Virtual Port Channel (VPC) is a feature that can span a Port Channel between two Cisco Nexus switches (with 10GE interfaces). This provides the ability to build a L2 Port Channel from two different Cisco Nexus switches to a single access switch. The access switch assumes it is really peering with a single switch increasing the overall availability if there is a failure. VPC uses two independent control planes and like VSS does not rely on STP.

Step 1

Build vPC domain within Core layer

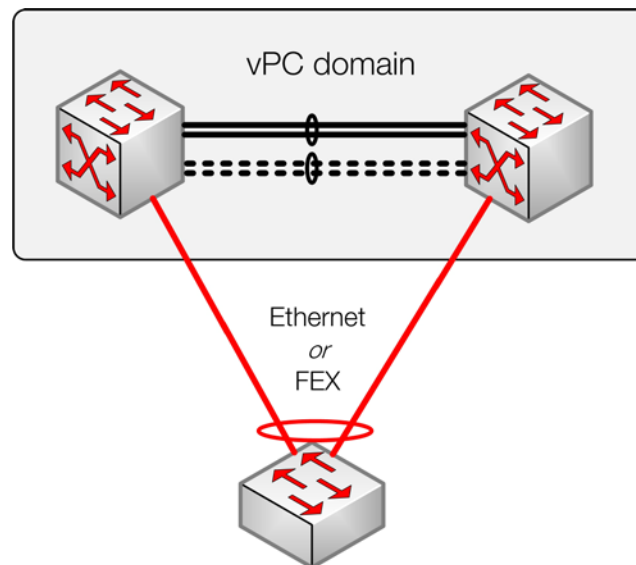
Implement vPC between the two Core switches (or Distribution in a Three-Tier Topology). The following vPC components need to be defined:

- **vPC domain:** includes the two vPC enabled devices, the vPC peer link, the vPC peer keepalive link, and all of the Port Channels created from the two vPC peers.
- **vPC peer link:** an interface used between the vPC peer devices for synchronizing control traffic. You should have at least two 10 Gigabit Ethernet interfaces for the peer links.
- **vPC peer keepalive:** dedicated interface used to monitor the health of the other vPC peer by sending periodic keepalive messages. No data traffic is synchronized over this link.



With the vPC domain established on the Core layer, determine what type of connections will be connected to the vPC domain. It can be one (or both) of the following options:

1. Ethernet
2. Fabric Extenders (FEX)



Design Considerations (using FEX connections):

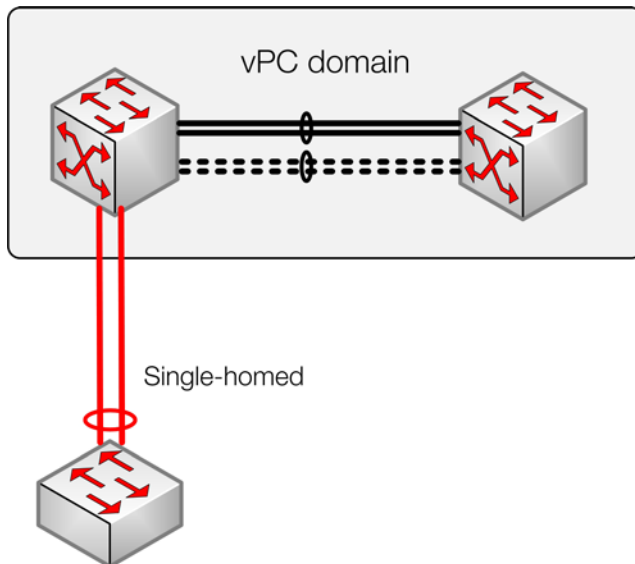
- Cisco FEX ports do not support connectivity to LAN switches that generate spanning-tree BPDU packets. It will shut down with an Error Disable.
- Cisco FEX ports are only supported on Layer 2 ports and not Layer 3 routed ports.
- Supports up to sixteen connected Cisco FEXs (using Cisco NX-OS release 5.2(1)N1(1) or later)
- Cisco FEX can support up to four or eight uplinks to the Cisco Nexus 5500UP core switches.
- FEX can support Ethernet and FCoE when using 10GE optics (fiber, Twinax).
- At least two Cisco FEX uplinks to the data center core are recommended for minimum resiliency.
- It's recommended to configure the maximum number of fabric uplinks using either Twinax (CX-1) cabling or the Fabric Extender Transceiver (FET) and OM3 multimode fiber.

Determine if those connections will be single-homed and/or dual-homed from the Access layer to the Core layer:

1. Single-homed Connection
2. Dual-homed Connection ; Multi-chassis EtherChannel (MEC)

#1

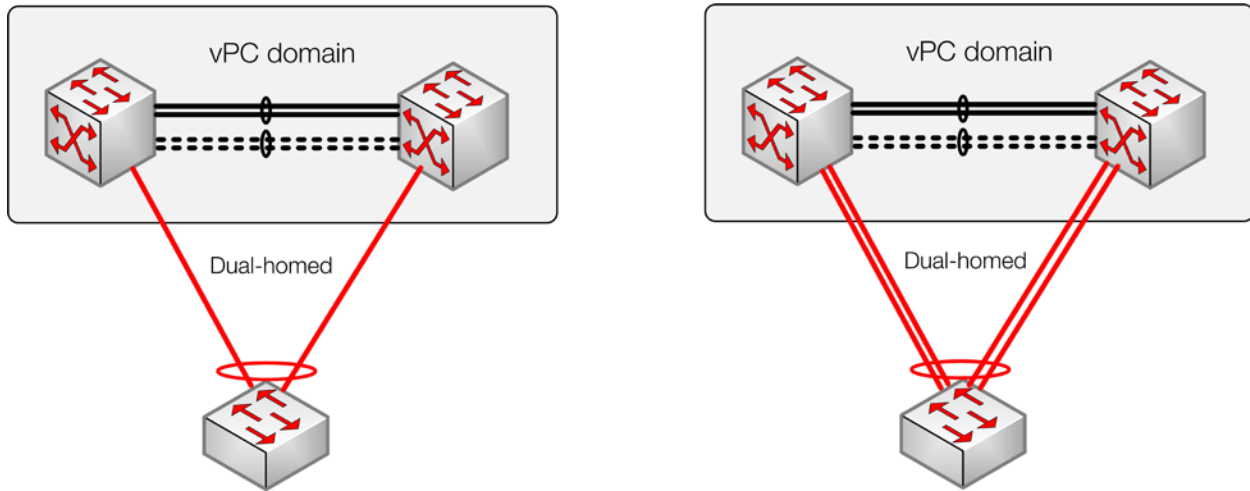
Single-homed (L2, L3)



Using FEX Connections:

- If the Cisco FEX will be single-homed to only one of the vPC switches, it should be configured as a standard port channel.
- At least two Cisco FEX uplinks to the data center core are recommended for minimum resiliency.

This is also called a **Multi-chassis EtherChannel (MEC)**



If using FEX Connections:

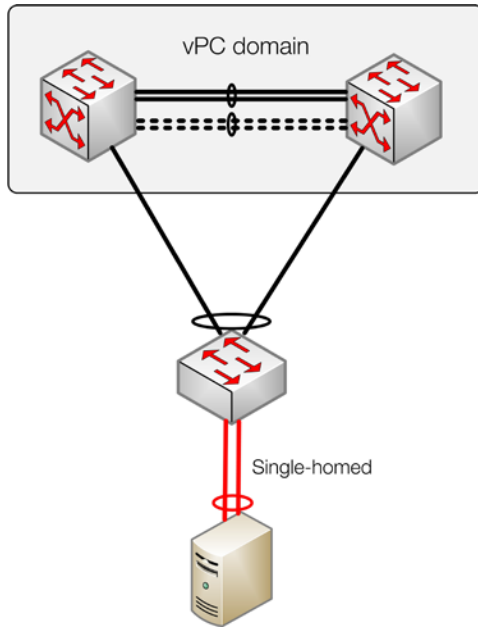
- If the Cisco FEX will be dual-homed to both of the vPC switches, it must be configured as a vPC on the port channel.
- At least two Cisco FEX uplinks to the data center core are recommended for minimum resiliency.

Determine how the Servers (using Port Channel) will be connected to the Access layer:

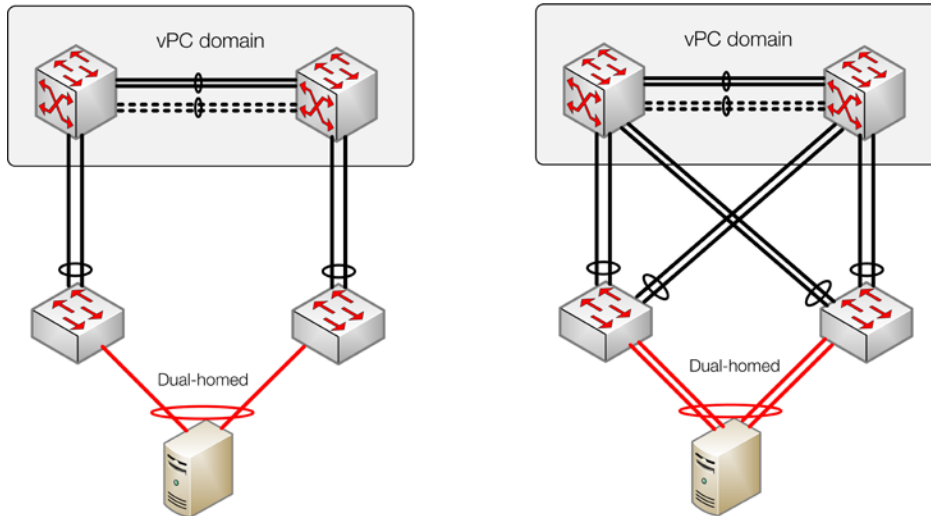
1. Single-homed Servers
2. Dual-homed Servers ; Enhanced vPC

#1

Single-homed Server Connection



This is also called an **Enhanced vPC** (vPC functions are pushed down to the access layer for connected servers to use Port Channel.)



If you are using dual-homed server connections, below are some considerations:

- Requirements: using a L2 Dual-homed vPC topology (on Access Layer)
- Enhanced vPC only supported on Cisco Nexus 5000/5500 series.
- Using dual-homed server using EtherChannel to two single-homed FEX Access switches:
 - The server is dual-homed with one access layer switch.
 - The dual-homed connection is configured as a vPC Port Channel.
 - This configuration must be done on both Cisco Nexus 5500UP Core switches.
- Using dual-homed server using EtherChannel to two dual-homed FEX Access switches:
 - The server is dual-homed with two access layer switches.
 - The dual-homed connection is configured as an Enhanced vPC.
 - Requires Cisco NX-OS release 5.1(3)N1(1) or later for the Cisco Nexus 5500 switches
- If EtherChannel servers will use FCoE, then the storage traffic must be isolated and cannot connect to both Core switches.

When to use: Recommended if the Data Center vPC Core will connect to a LAN Core.

Object Tracking is a vPC feature that can monitor the state of critical interfaces on the Data Center Core (using Cisco Nexus 5500). It can track interfaces and perform an action which could relinquish vPC domain control to the other vPC switch.

Requirements: vPC peer keepalive link within the vPC domain.

Recommendations: enable vPC object tracking on the ports connecting into the LAN Core switch.

STP and BPDU

- Allows a pair of Cisco Nexus 5500 Series switches to appear as a single spanning tree root in the Layer 2 topology.
- BPDUs are sent from both vPC switches, but needs to be blocked.
- To avoid loops, the vPC peer link is excluded from the spanning tree process.

Multicast

- A unused VLAN for IP Multicast replication synchronization should be used between the vPC switches.
- The VLAN used for the IP Multicast ("bind-vrf") cannot appear anywhere in the configuration. It must not be defined in the VLAN database and will not get included in the VLAN allowed list. It will automatically setup packet replication across the vPC peer link trunk when needed.

- You must have the hardware (e.g. Supervisor Engine, Line modules) to support this feature including the appropriate license installed.
- **Services:** UDLD, Port Channel, Bridge Assurance (BA), FHRP

Virtual Switching System (VSS)

Category: Network Service (Routing and Switching)

Prerequisite(s): LAN and/or Data Center (under Solutions), Cisco Catalyst 6500/6800 (Hardware)

R

When to Use: when you need cluster two switches together to appear as one logical switch.

Cisco Virtual Switching System (VSS) is a feature that can cluster two Cisco Catalyst 6500E switches together to appear as one logical switch. Recommended for LAN Distribution/Core switches connecting into a LAN Access or Building network. This feature is supported on Cisco Catalyst 6500 series using the Supervisor 2T with 10GB interfaces between the two Catalyst switches. VSS does not rely on STP and is limited to be configured between only two switches. If Port Channeling is configured between the two VSS switches to a single access switch, the access switch will assume it is really peering with a single switch increasing the overall availability for the connected hosts on the switch.

Step 1

Topology Design

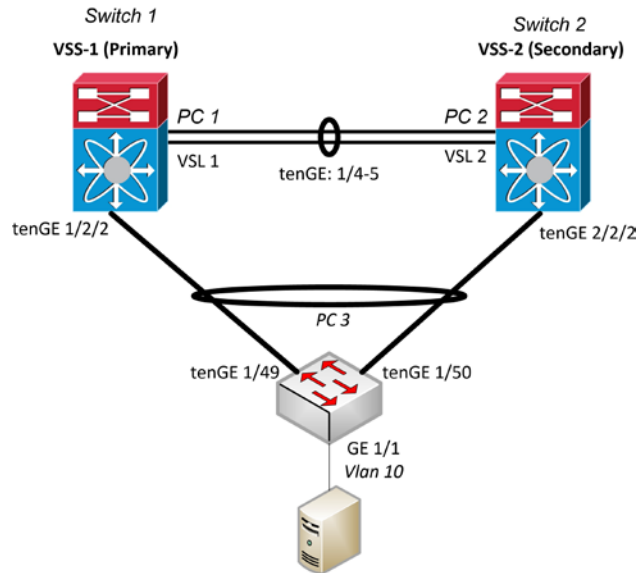
The components in this service would be the Collapsed Core and/or Distribution switch (enabled for VSS) in the LAN/Data Center topology using Cisco Catalyst supported hardware. Select how VSS will be deployed based on the following options.

1. Multi-chassis EtherChannel (MEC)
2. VSS Quad-Supervisor SSO (VS4O) ; requires Cisco Catalyst 6800 hardware
3. Enhanced Fast Software Upgrade (EFSU)

Below are the details about this resilient redundancy option:

- Two Core switches are bundled together.
- L2 Port Channel can span between two Cisco Catalyst switches connecting to a single access switch.
- Creates a spanning tree loop free topology.

Below shows an example of VSS using MEC:



Connect two Cisco Catalyst switches (e.g. Cisco Catalyst 6500 VSS 4T) together using 10GE connections supporting VSS to provide the Virtual Switch Link (VSL).

Below are the steps for the design and implementation of this feature:

1. **VSS Domain & Switch ID:** Define a unique domain shared by both switches including a unique number (e.g. switch ID) for each switch in the VSS domain.
2. **VSL link:** Configure VSL link between the two VSS switches. The VSL allows the supervisors to communicate using SSO redundancy to keep the control plane synchronized between the two supervisor engines. To build the VSL, use unique port channel numbers on each VSS switch.

3. **Virtual Mode Operation:** Enable the virtual mode operation which will renumber the interfaces to the format of interface [switch number]/[module number]/[interface on module]. Doing this operation will reboot both of the switches operation and the standby switch will display a "Standby" prompt.
4. **Dual-Active Detection Mechanism:** Setup Dual-Active detection mechanism using Fast Hello (VLSP) between the two VSS switches. If the VSL link fails, both supervisors would resume the active control plane role creating a dual-active condition. To prevent dual-active scenarios, VSS supports dual-active detection mechanisms which will trigger a VSS recovery mode. In VSS recovery mode, only one supervisor is allowed to remain active while the other supervisor on the other VSS switch will be in recovery mode. As a result the VSS switch in recovery mode will shutdown all of its interfaces except for the VSL link to prevent instability. Once the VSL is restored, VSS would reload the supervisor that was in recovery mode and return to a normal operating mode. Fast Hello (VLSP) is recommended which uses a GE interface on each VSS switch and cabled together. This does not require high bandwidth because it's only a detection link with control plane hello messages exchanged.
5. **Virtual MAC Address:** By default, the active switch in the VSS domain uses the default chassis-based MAC address pool assigned to the switch. Its recommended to set a virtual MAC address for the VSS system, so that either active supervisor will use the same MAC address pool.

VRF-lite

Category: Network Service (Tunneling)
Prerequisite(s): --

Go to *"Multi-CE VRF"*

A large, stylized white letter 'W' is centered within a dark gray rectangular box. The 'W' is composed of three distinct 'V' shapes joined together, with a slightly irregular, hand-drawn appearance.

~ Services ~

WCCP

Category: Network Services (Routing and Switching)

Prerequisite(s): LAN, WAN, Internet Edge, Proxy and/or Optimization (under Solutions)

Used to transparently send traffic (e.g. HTTP, FTP) to an optimization appliance or proxy appliance. This service is usually implemented on the Internet Edge and/or WAN router in the topology depending on the solution deployed.

0 - 9

~ Services ~

802.1X

Category: Network Service (Security)

Prerequisite(s): Identity Access Control (under Solutions)

802.1X is used to authenticate users before gaining network access. Below is what should be configured when deploying 802.1X services on the network.

- **Services Required:** RADIUS
- **Guest:** if a non-802.1x user is connected to a 802.1X enabled switch port or they do not authenticate they will be placed in a Guest VLAN on the network that is specified in the configuration.
- **Authentication Fail:** this is an option that is similar to the Guest option which specifies which VLAN a user who fails authentication will be placed.
- **MAC Authentication Bypass:** an option administrated from the RADIUS server that can bypass any user authentication via 802.1X using the MAC address of the connected system.

Design Options

Once the network design has been completed for all solutions and services, you need to prepare a couple of design options. These different options may include consolidation to redundancy within the topology.

Prepare up to 3 design options based on one or more of the following criteria:

1. **Engineers Recommendation:** prepare a design option that you would recommend based on your experience and preferences still aligned with the requirements by the business. This can include specific hardware, consolidation, or redundancy that you recommend.
2. **Lowest Cost:** if applicable, provide a design option showing the lowest cost.
3. **Best Scalable Design:** provide a design option that considers scalability if the networks grows and additional services/solutions are added in the future. The cost may be a higher compared to the “Best Fit Design” because it is considering growth and additional services that may be used in the future.
4. **Best Fit Design:** provide a design option that accommodates the services and requirements aligned today with no consideration for growth or flexibility of additional services. The cost will likely be lower compared to the “Best Scalable Design”, however if requirements sudden change in the near future the company may end up spending more overall.
5. **Based on Redundancy:** provide a design option where majority of the solution components in the design have redundancy.
6. **Based on Hardware Consolidation:** provide a design option where most of the hardware components are consolidated with other components in the design.
7. **Based on Hardware without Consolidation:** provide a design option where the hardware components are *not consolidated* with other components in the design.
8. **Other Design:** any other design option based on some other criteria not listed here.

For each of the design options, prepare one or more of following that will be presented back to the business for further consideration:

- **Description:** provide a list of design aspects and why it is listed as an option.
- **Risks and Consideration:** provide a list of aspects of the design that should be considered as a potential risk and the consequences for what to expect. This provides a good level of information and awareness because if a company does not want to engage with a particular design option that has redundancy because the costs are higher they have to understand the risks involved and accept the consequences that may come about, which could result in losing business.
- **Network Diagram(s):** provide diagram pictures showing the network design, hardware, connections, addressing, and more.
- **Costs:** specify the estimated cost involved for the hardware and any other related costs.
- **Hardware list:** provide a list of hardware that is being considered for the design option (if applicable). This is also called the Bill of Materials (BOM).

10 Design Resources

Below are additional resources that can be used in the design process.

Service Provider (ISP) List

The following is a list of service providers that can be used to provide Internet or WAN cloud services.

- **AT&T:** provide Internet, WAN, and phone services. Their service can also include a managed router providing an Ethernet hand-off to the CPE.
- **Telepacific (TPAC):** provide Internet, WAN, and phone services. Their service can also include a managed router providing an Ethernet hand-off to the CPE. I have seen many TPAC deployments for clients using Voice and Data on the network. The customer service from this provider is very good with a great turn-up process.
- **Cogent:** provide Internet services and is a very reliable provider.
- **Hurricane Electric:** provide Internet and colocation services.
- **Data Pipe:** provide Internet services. Provide a great simple support portal with fast response times.
- **Savvis Communications:** provide Internet services with good customer service.
- **CBeyond:** provide Internet services and is constantly brought up as an affordable alternative.

Tools and URLs

Below is a list of network tools and sites that can be used for troubleshooting/reference.

- **DNS Stuff:** provides a detailed portal with dozen of resources beyond just nslookup, ping, traceroute, and SPAM blocking list. It was a free service in the past, now it is a paid monthly service.
 - www.dnsstuff.com
 - **Alternative:** <http://legacy.zoneedit.com/lookup.html?ad=whois>
- **NTAP:** provide copper and fiber taps (passive monitoring)
 - www.networktaps.com
- **Looking Glass** by Hurricane Electric to view BGP routing paths, Pings, and traceroutes.
 - <http://lg.he.net/>
- **Bandwidth Test:** performing a bandwidth throughput test between two nodes across the network with easy instructions and examples.
 - <http://clintboessen.blogspot.com/2010/01/how-to-test-bandwidth-between-two.html>
 - <http://openmaniak.com/iperf.php>
- **Online Data transfer rate Converter:** converting transfer rate values between bits & bytes including data transfer times:
 - http://www.convert-me.com/en/convert/data_transfer_rate
- **Speed Test:** viewing upload and download speed for Internet connectivity including latency/delay:
 - <http://speedtest.net/>
- **MAC Address Vendor Search:** input the MAC address to view who is the vendor. Very useful for troubleshooting and trying to determine what the hardware device could be.
 - http://www.coffer.com/mac_find/

Other Resources

1

Router vs Firewall

Below are a few points to consider when choosing between a router and a firewall on the network:

a

Router

- Support for DMVPN, GET VPN, GRE, IPSec, SSL VPNs
- Stateful Firewall (configuration needed using rACL or CBAC if using Cisco IOS routers)
- Advanced QoS
- CEF entries
- Feature count: High
- Deeper Port Buffers
- Mainly used for the WAN, LAN Campus, Internet Edge

b

Firewall

- Support for IPSec, SSL VPNs (client, site)
- Stateful Firewall (default operation)
- Basic QoS
- Based on connection counts
- Feature count: Low
- Light Port Buffers
- Mainly used for the Data Center and Internet Edge
- Offers advanced content filtering services (AVS, Spyware, URL Filtering)

Hardware and Software

- Vendor Stability ; have they been around for awhile
- User Connection Limitations
- Licensing
- Throughput Capacity (backplane traffic), Performance, Bandwidth
- Traffic per Second (averages)
- Configuration and Management structure
- Maintenance
- Compatibility
- Request for Information (White Papers, Data Sheets, etc)
- Cost
- Support Model: Parts, Labor
- Case Studies
- Network Solutions the product is used in
- Vendor Consultation
- Customization
- Quality of Service
- Services & Features Supported
- Product comparison with another vendor device (if applicable)

Service Provider

- Tier Provider
- Reliability (SLA – Availability)
- Performance (SLA – Latency and Packet Loss)
- Security
- Support (Customer Service)
- Installation and Repairs (Maintenance)
- Pricing
- Services
- Length of Contracts
- Case Studies

1. **Non-Blocking/Blocking:** the performance of the hardware model will likely determine if the ports/interfaces on the hardware device provide non-blocking performance or blocking performance (shared bandwidth). Non-Blocking provide a 1:1 ratio meaning 1GE in and 1GE out for possible throughput with low-latency. This avoids possible oversubscription, increased delay, and drops. Hardware for non-blocking devices tend to be more expensive. Blocking means multiple ports may share a common bandwidth resource. For example six 1GE connections coming in may share 1GE going out. So if 6 GE servers are forwarding at 100% then there will be oversubscription, buffering of packets resulting with possible delay and discards/drops. However the cost for blocking type hardware is cheaper. Non-Blocking is also known as line-rate or wire-speed. Non-blocking is something that is often discussed with L2/L3 switches more than router devices.
 - a. **Non-Blocking:** recommended for Server Farm/Data Center networks including SAN solutions (iSCSI). Or if utilization is expected to be high (50%, 100%).
 - b. **Blocking:** common for LAN and User networks. Or if utilization is expected to be low ~33%.
2. **Packets Per Second (PPS):** Another important factor to consider is the packets per second (PPS) for a hardware device than looking at the generic throughput numbers advertised for that product because packet sizes can vary from 100 bytes to 1400 byte packets (or higher if Jumbo frames are used) which can change the overall throughput for the device. Understanding the PPS and possible packet sizes we can determine the possible throughput. *For example, 20Kpps for a device forwarding 100 Byte packets will provide a possible throughput of the following: $20 \times 8 \times 100 = 16\text{Mb/s}$ (on the low end) or if we are using 1400 bytes then our possible throughput will be $20 \times 8 \times 1400 = 224\text{Mb/s}$.*

1. Traffic coming in is inspected by a Cisco ASA firewall policy.
2. If the traffic is denied by a firewall policy, the traffic is dropped.
3. Permitted traffic matching a firewall policy is sent to the IPS/NGFW module for deeper inspection.
4. Traffic that matches a policy/filter list will be dropped.
5. Clean traffic will be sent back to the Cisco ASA.
6. VPN access policies are applied (If VPN services are configured).
7. Lastly, traffic is forwarded out of the firewall onto the network.

- **Leased Line:** T1/E1 (1.544Mbps), DS3 (45Mbps). Light to medium traffic use. Common for Small, SMB, Medium, and some large sized networks.
- **Optical:** OC-3 (155Mbps), OC-12 (622Mbps), OC-48 (2.5Gbps), and OC-192 (9.6Gbps). Common for large networks and ISP networks.
- **Wireless (WWAN):** 3G (1.4Mbps to 3.1Mbps), 4G (3Mbps to 10Mbps). This would be a public network and a VPN will be required for connecting between sites. This can also be used as a backup for connecting to the Internet.
- **Ethernet:** FE, GE, 10GE. This is common for any size network. Usually occurs when the ISP provides a managed router supplying an “Ethernet” handoff to the customer’s equipment (CE).
- **Broadband:** DSL (up to 10Mbps), Cable (up to 30Mbps). A common attribute of broadband is that it provides different upload and download speeds. “Download” speeds are usually higher which is what users are pulling down from the Internet where “Upload” speeds are usually smaller which is what users are pushing up to the Internet (including people accessing your network). Common bandwidth service for most small and SMB sized networks.

Configuration Checklist

1

Checklist for Routers

- ☐ **General**
 - ☐ General Best Practices
 - ☐ Security Best Practices
 - ☐ Hostname
 - ☐ Time-zone
 - ☐ Password Encryption
 - ☐ Banner
 - ☐ Alias ("c" for config t)
 - ☐ User Accounts (Local, RADIUS, TACACS+)
 - ☐ Enable Secret Password
 - ☐ ACL: SNMP, VTY
 - ☐ Logging
 - ☐ Domain Name
 - ☐ DNS
 - ☐ RSA keys for SSH
 - ☐ VTY ; enable SSH
 - ☐ Console
 - ☐ SNMP
 - ☐ NTP
 - ☐ IP CEF
 - ☐ IP Routing (EIGRP, OSPF, Static)
 - ☐ Default IP route (static, BGP)
- ☐ **QoS**
 - ☐ Class (ACL, NBAR)
 - ☐ Policy
- ☐ **WAN facing interface**
 - ☐ Description
 - ☐ IP Address (Static, DHCP)
 - ☐ Encapsulation (T1, PPP/MLP, HDLC, DSL/Ethernet)
 - ☐ Stateful Firewall (rACL, CBAC) ; Internet/Public
 - ☐ QoS policy
- ☐ **LAN facing interface**
 - ☐ Description
 - ☐ IP Address
- ☐ **Other IP and Security Services**
 - ☐ DHCP
 - ☐ Site VPN
 - ☐ Client VPN (EZVPN, SSL)
 - ☐ Multicast: enable PIM-SM on L3 interfaces
 - ☐ IPv6
 - ☐ IP SLA
 - ☐ Wireless
 - ☐ Bridging, IRB
 - ☐ VLANs
 - ☐ SSID
 - ☐ Security
 - ☐ AppFw & URL filtering

- ☐ FHRP (HSRP)
- ☐ Bridging
- ☐ NAT
- ☐ PBR
- ☐ NetFlow
- ☐ WAAS (WCCP)
- ☐ **Voice Services**
 - ☐ CME
 - ☐ SCCP, SIP
 - ☐ DN
 - ☐ Phones
 - ☐ CUE
 - ☐ VM
 - ☐ AA
 - ☐ Voice Circuits
 - ☐ PRI
 - ☐ FXO
 - ☐ FXS
 - ☐ SIP Trunk
 - ☐ H.323 Dial peers (route patterns)
 - ☐ MGCP, H.323, SIP
 - ☐ Translation Patterns
 - ☐ SRST
 - ☐ Fax
 - ☐ Conferencing, Transcoding

- ☐ **General**
 - ☐ General Best Practices
 - ☐ Security Best Practices
 - ☐ Hostname
 - ☐ Time-zone
 - ☐ Password Encryption
 - ☐ Banner
 - ☐ Alias ("c" for config t)
 - ☐ User Accounts (Local, RADIUS, TACACS+)
 - ☐ Enable
 - ☐ ACL: SNMP, VTY
 - ☐ Logging
 - ☐ Domain Name
 - ☐ DNS
 - ☐ RSA keys for SSH
 - ☐ VTY ; enable SSH
 - ☐ Console
 - ☐ SNMP
 - ☐ NTP
 - ☐ QoS (Global)
 - ☐ VTP Transparent mode
 - ☐ QoS globally
 - ☐ VLANs
 - ☐ Management Interface, VLAN SVI
 - ☐ ErrDisable Recovery
 - ☐ Macros
 - ☐ UDLD aggressive (global)
 - ☐ Default Gateway
- ☐ **LAN Switching**
 - ☐ Enable Rapid Spanning Tree
 - ☐ Extend system ID
 - ☐ Loopguard (Global)
 - ☐ Source Guard
- ☐ **Uplink/Downlink Ports**
 - ☐ Description
 - ☐ Access or 802.1Q Trunking
 - ☐ Encapsulation: 802.1Q
 - ☐ Trunk Security
 - ☐ Native VLAN
 - ☐ Turn off DTP
 - ☐ AutoQoS – Trust
 - ☐ Dynamic ARP Inspection and DHCP snooping – Trust, Limit rate
- ☐ **Data Edge Ports**
 - ☐ Description
 - ☐ Access
 - ☐ Data VLAN ID
 - ☐ STP PortFast
 - ☐ STP BPDUGuard (or BPDUFilter)
 - ☐ L2 Interface Best Practices
 - ☐ AutoQoS – Trust ; for trusted data ports only!
- ☐ **Voice+Data Edge Ports**
 - ☐ Description
 - ☐ Access
 - ☐ Data VLAN ID
 - ☐ Voice VLAN ID

- ☐ STP PortFast
- ☐ STP BPDUGuard
- ☐ AutoQoS ; Cisco-phone
- ☐ L2 Interface Best Practices
- ☐ **Other Services**
 - ☐ Medianet (Auto-Configuration)

- ☐ **General**
 - ☐ General Best Practices
 - ☐ Security Best Practices
 - ☐ Hostname
 - ☐ Time-zone
 - ☐ Password Encryption
 - ☐ Banner
 - ☐ Alias ("c" for config t)
 - ☐ User Accounts (Local, RADIUS, TACACS+)
 - ☐ Enable
 - ☐ ACL: SNMP, VTY
 - ☐ Logging
 - ☐ Domain Name
 - ☐ DNS
 - ☐ RSA keys for SSH
 - ☐ VTY ; enable SSH
 - ☐ Console
 - ☐ SNMP
 - ☐ NTP
 - ☐ QoS (Global)
 - ☐ VTP Transparent mode
 - ☐ QoS globally
 - ☐ VLANs
 - ☐ ErrDisable Recovery
 - ☐ Macros
 - ☐ Default Gateway
 - ☐ Set the stack master switch ; if using a stack-based switch
- ☐ **CEF**
 - ☐ CEF load-sharing full
- ☐ **LAN Switching**
 - ☐ Enable Rapid Spanning Tree
 - ☐ Root Bridge (primary, secondary)
 - ☐ Extend system ID
 - ☐ Loopguard (Global) ; Collapsed Core or Core (with Agg)
- ☐ **VLAN SVIs**
 - ☐ L3 Interface Best Practices
- ☐ **MLS**
 - ☐ Flow IP Full ??
- ☐ **Uplink/Downlink Ports**
 - ☐ Description
 - ☐ Access or 802.1Q Trunking
 - ☐ Encapsulation: 802.1Q
 - ☐ Trunk Security
 - ☐ Native VLAN
 - ☐ Turn off DTP
 - ☐ Port Channel (LACP; "active" mode) ; Load Distribution "src-dst-ip"
 - ☐ L2 Interface Best Practices
 - ☐ STP: Link-Type Point-to-Point (if supported) ; not under PC
 - ☐ RootGuard ; if connecting to Access
 - ☐ Dynamic ARP Inspection and DHCP snooping - Trust
- ☐ **Server Edge Ports**
 - ☐ Description
 - ☐ Access
 - ☐ Data VLAN ID

- ☐ STP PortFast
- ☐ STP BPDUGuard, BPDUFilter
- ☐ L2 Interface Best Practices
- ☐ **Multicast**
 - ☐ Enable multicast routing globally
 - ☐ Enable PIM-SM (Sparse mode) on interfaces
 - ☐ Configure AutoRP
 - ☐ Configure MSDP
- ☐ **Other Services**
 - ☐ Storm Control (broadcast)
 - ☐ Multicast
 - ☐ IGP Routing (EIGRP, OSPF, Static)
 - ☐ IPv6
 - ☐ Advanced Services (Service Modules, etc)
 - ☐ Hardware Specifics (Redundancy, SSO/NSF)
 - ☐ Jumbo Frames
 - ☐ Port Security
 - ☐ DHCP server, IP Helper
 - ☐ DHCP (Voice): DHCP Option 150
 - ☐ Port Monitor
 - ☐ Power Supply (Redundant)

- ☐ General Best Practices
- ☐ Security Best Practices
- ☐ Hostname
- ☐ Passwords
- ☐ Time-zone
- ☐ NTP
- ☐ Logging
- ☐ Interfaces
- ☐ Routing (static, EIGRP, OSPF)
- ☐ Default gateway
- ☐ Turn off Proxy-ARP (Zone: inside/trusted)
- ☐ NAT (Static, PAT)
- ☐ Failover
- ☐ Firewall Policies
 - ☐ RFC1918
 - ☐ RFC2728
 - ☐ Objects (Address, Services)
- ☐ VPN Services
 - ☐ Site VPN
 - ☐ Client VPN (IPSec, SSL)
- ☐ Advanced Security Services
 - ☐ Anti-Virus
 - ☐ Intrusion Prevention (IPS) ; Prevent, Detect
 - ☐ Anti-Spyware
 - ☐ Content Filtering