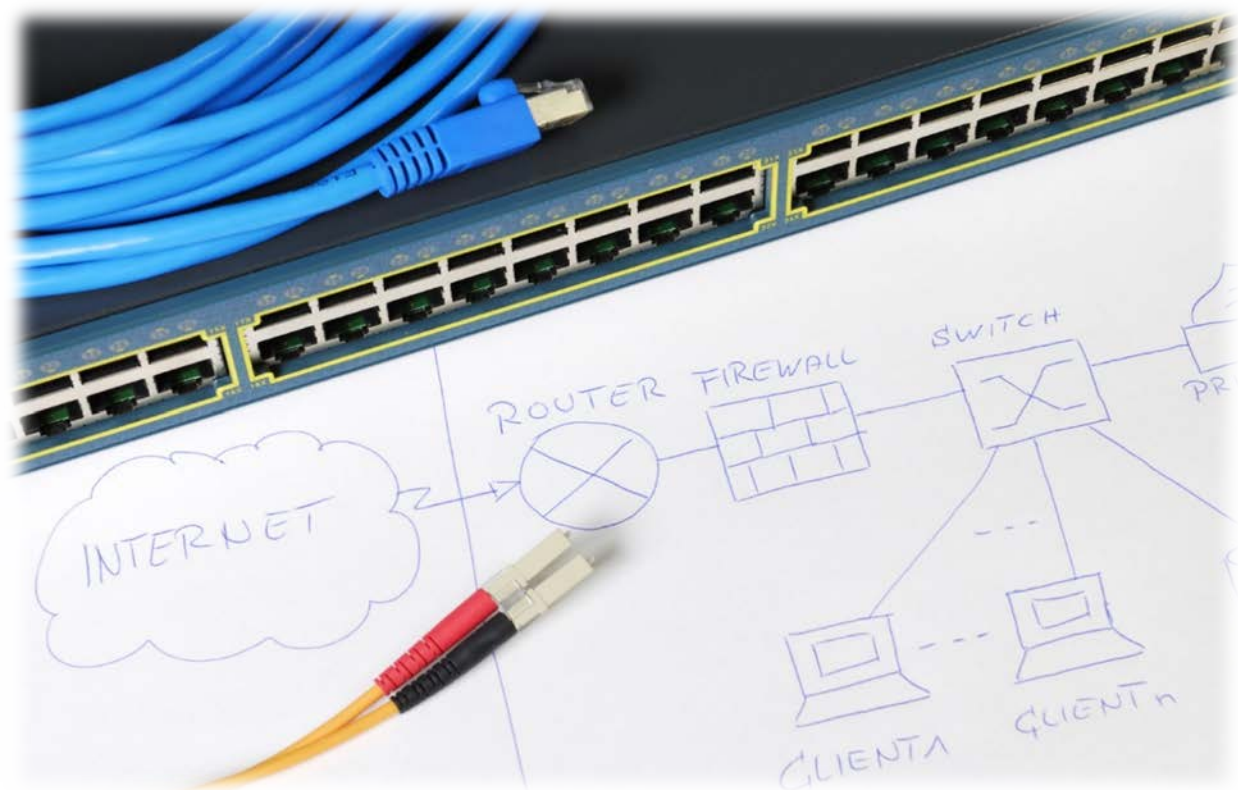


Cisco Configuration Reference Guide

Version 4.0.9 (Updated: September 30, 2015)



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



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 superceded 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.

TOPICS

TOPICS	5
[A].....	11
AAA	11
ACL.....	12
ADSL	20
ALIAS	21
APPLETALK.....	22
ARCHIVE	23
ARP TIMEOUT.....	24
ATM	25
AUX.....	29
[B].....	30
BFD.....	30
BGP	31
BPDU	53
[C]	54
CARRIER DELAY	54
CBAC	55
CEF.....	57
CELLULAR.....	58
CGMP	59
CISCO ACE SERIES	60
CISCO ASA/FWSM SERIES.....	63
CISCO CATALYST 3750 SERIES	93
CISCO CATALYST 4500 SERIES	94
CISCO CATALYST 6500 SERIES	96
CISCO CATALYST XL SERIES.....	101
CISCO GSR SERIES.....	103
CISCO IP PHONES.....	104
CISCO NEXUS SERIES	105
CISCO UCM EXPRESS	134

CISCO UNITY EXPRESS.....	175
COMMITTED ACCESS RATE (CAR).....	184
CONTENT FILTERING	185
CBWFQ.....	186
COPY.....	187
cRTP	188
[D].....	189
DAMPING	189
DEFAULT INTERFACE	190
DELETE	191
DHCP	192
DHCP SNOOPING.....	194
DMVPN	195
Do	201
DS-3.....	202
DYNAMIC ARP INSPECTION.....	204
DYNAMIC DNS (DDNS)	205
[E].....	206
EEM	206
EIGRP.....	207
ERROR DISABLE.....	215
ETHERNET OVER MPLS (EoMPLS)	216
EXTREME SWITCHES SOLUTIONS.....	219
EZVPN.....	220
[F]	222
FLEX LINK	222
FLOW CONTROL.....	223
FOUNDRY SOLUTIONS	224
FRF.12.....	226
FRAME RELAY	227
FRAME RELAY TRAFFIC SHAPING (FRTS)	233
FWSM	234
FXO.....	237
FXS	238
[G]	240
GET VPN.....	240
GLBP.....	244
GOLD	246
GRE	247
GROUNDSTART	249

[H]	250
HSRP	250
HTTP	254
[I]	255
IGMP SNOOPING	255
IOS RECOVERY	256
INCLUDE	257
INTERFACES	258
INTERFACE RANGE	259
IP ACCOUNTING	260
IP HELPER	261
IP SLA	262
IPSEC VPN	264
IPv6: GENERAL	276
IPS	279
IPX	280
IRB	281
ISATAP	282
ISDN PRI	284
[J]	285
JUMBO FRAMES	285
JUNIPER	286
[L]	288
LAN CAMPUS DESIGN	288
LINUX SOLUTIONS	292
LLDP	293
LLQ	294
LOAD INTERVAL	295
LOGGING	296
LOOPGUARD	297
L2TPv3	298
[M]	301
MACROS	301
MD5 FILE VALIDATION	303
MGCP	304
MICROSOFT SOLUTIONS	305
MLPPP	309
MODULES	311
MPLS VPN	312
MULTI-VRF CE (VRF-LITE)	318

MULTICAST	326
MULTICAST: MONITORING	330
MULTICAST: RP	331
MULTICAST: SECURITY	333
MSDP	336
[N]	341
NAM	341
NAT	342
NEC (VOICE) SOLUTIONS	350
NETFLOW	351
NETGEAR SOLUTIONS	354
NTP	356
[O]	357
OSPF	357
[P].....	370
PIM	370
PPPoE.....	372
PPTP	378
POLICY BASED ROUTING (PBR)	379
PORT CHANNEL	380
PORT MONITOR.....	385
PORT SECURITY	388
PROTECTED PORTS.....	390
[Q]	391
QoS: GENERAL	391
QoS: CLASSIFICATION & MARKING	392
QoS: LINK EFFICIENCIES.....	394
QoS: POLICING	398
QoS: QUEUING & DROPPING	401
[R].....	404
RADIUS	404
REFLEXIVE ACL (RACL)	405
RIP	407
ROOTGUARD	409
ROUTE TAGGING	410
[S].....	415
SCHEDULER	415
SECONDARY IP	416

SENDING MESSAGE IN IOS.....	417
SIP	418
SLB (Cisco IOS).....	419
SMTP	421
SNMP	422
SONICWALL SOLUTIONS	424
SOURCE GUARD, IP	425
SPANNING TREE PROTOCOL.....	426
SRST	430
SSH	432
SSL VPN	433
STATIC ROUTING.....	437
STORM CONTROL	439
[T]	440
TACACS+	440
TEMPLATES.....	441
TERMINAL SERVER ROUTER	454
TFTP.....	455
TIME-ZONE	456
TRUNKING (802.1Q)	457
T-1	460
[U].....	462
UNICAST RPF, IP	462
UDLD.....	463
URBL.....	463
[V].....	466
VLAN	466
VLAN TRUNKING PROTOCOL (VTP)	471
VOICE GATEWAY	472
VPLS.....	474
VRRP	484
VSS.....	485
[W].....	492
WCCP	492
WIRELESS	494
WRED.....	506
[0-9]	507
802.1x	507

[A]

AAA

Solution/Services: Administration/System
Related: RADIUS, TACACS+

Lower Case

- Enable local accounts to be case sensitive

```
aaa authentication login default group tacacs+ local-case
```

Testing AAA

- Testing RADIUS (or TACACS+ if configured) using the username "alynn" in the domain of "RHG"

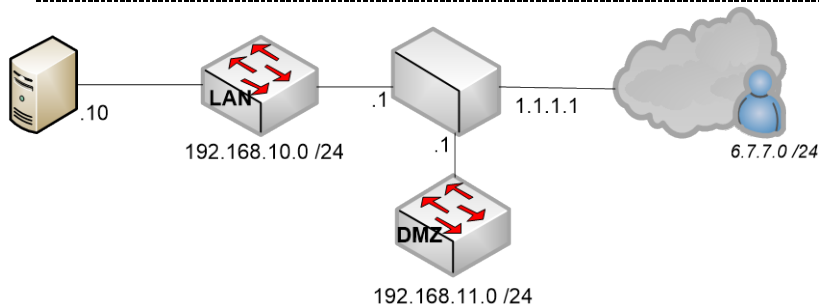
```
test aaa group radius RHG\alynn
```

ACL

Solution/Services: Security
Related: CBAC, Reflexive ACL

Public Interface: Guest/DMZ ACL Policy

- DMZ/Guest network exist in VLAN11 (192.168.11.0)
- On DMZ/Guest network will only allow the following: (1) DMZ/Guest can access host 192.168.10.10 located on the LAN. (2) Allow DHCP services for the DMZ. (3) Restrict all other access to the LAN (192.168.10.0). And all other traffic (UDP, TCP) is allowed and be stateful to be allowed back in



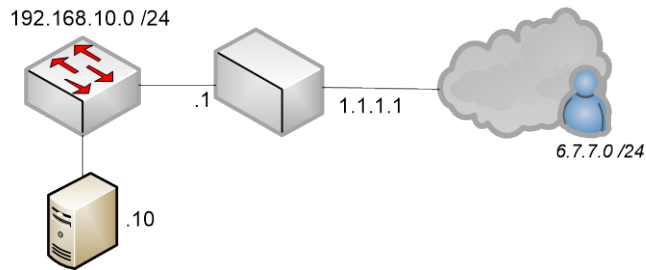
```
ip access-list extended public-ingress-acl
permit ip 192.168.11.0 0.0.0.255 host 192.168.10.10 reflect reflexive-public-acl
permit udp any eq bootpc host 255.255.255.255 eq bootps
deny ip 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255
permit udp any any reflect reflexive-public-acl
permit tcp any any reflect reflexive-public-acl
deny ip any any log
```

```
ip access-list extended public-egress-acl
permit icmp any any
evaluate reflexive-public-acl
deny ip any any log
```

```
interface Vlan11
ip address 192.168.11.1 255.255.255.0
ip access-group public-ingress-acl in
ip access-group public-egress-acl out
```


Internal Interface: Outbound ACL Policy

- Outbound ACL policy for (1) allowing SMTP from one mail server (192.168.10.10) to send emails. (2) Any other systems sending emails will be dropped. And (3) allow everything else
- Apply policy to LAN facing interface (FE0/1) outbound

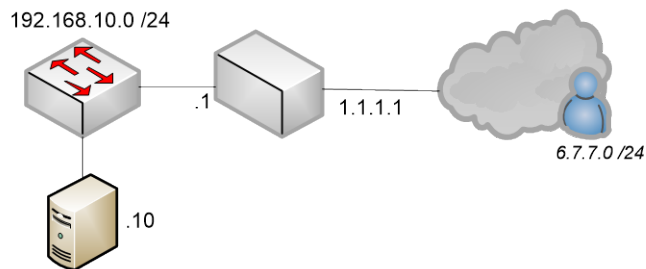


```
ip access-list extended hfc-outgoing-acl
permit tcp host 192.168.1.10 any eq smtp
deny tcp any any eq smtp log
permit ip any any
```

```
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip access-group hfc-outgoing-acl in
```

Public Interface: RFC1918 Filtering

- Configure ACL to restrict any source address using a private IP Address.
- Apply ACL policy inbound on WAN facing interface (FE4)



```
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 224.0.0.0 31.255.255.255 any
access-list 100 permit ip any any
```

```
interface FastEthernet4
ip address 1.1.1.1 255.255.255.0
ip access-group 100 in
```

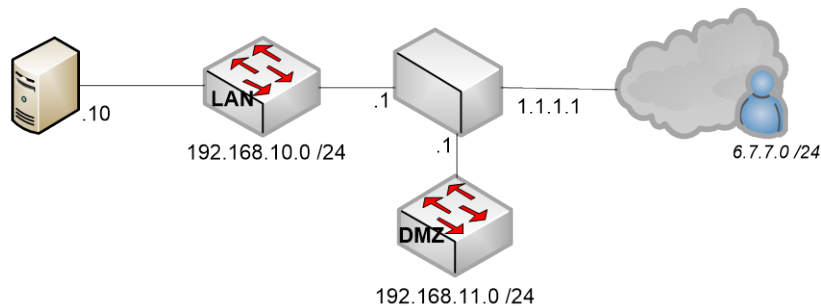
Black Hole (NULL) Routing

- Any host trying to route to any host on the 6.7.7.0 network will be dropped.
- Any host trying to route to host 7.7.7.7 will be dropped

```
ip route 6.7.7.0 255.255.255.0 null0
ip route 7.7.7.7 255.255.255.255 null0
```

Time-Based ACL

- Configure Time-Based ACL to (1) allow VNC (TCP/5900, 5800) access to server 192.168.10.10 starting at 12/9/2009 at 10AM and ending at 12/9/2009 at 12PM. (2) restrict all traffic to server 192.168.10.10 once the time-based ACL has expired. (3) Allow other traffic
- Apply policy to LAN facing interface (FE0/1) outbound



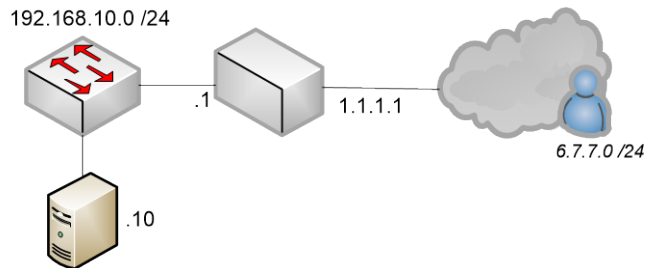
```
time-range "lab-time"  
absolute start 10:00 09 December 2009 end 12:00 09 December 2009
```

```
ip access-list extended lab-acl  
permit tcp any host 192.168.10.10 eq 5800 5900 time-range lab-time  
deny ip any host 192.168.10.10 any  
permit ip any any
```

```
interface FastEthernet0/1  
ip address 192.168.11.1 255.255.255.0  
ip access-group lab-acl in
```

Using Random TCP/UDP Ports

- Configure ACL to allow HTTP, HTTPS, & SMTP to server 192.168.10.10 (on LAN)
- Apply ACL policy inbound on WAN facing interface (FE0/0)

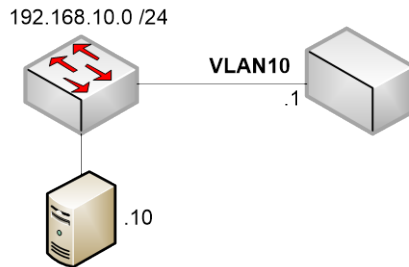


```
ip access-list extended ACL-FW
permit tcp any host 192.168.10.10 eq 80 443 25
```

```
interface FastEthernet0/0
ip address 1.1.1.1 255.255.255.0
ip access-group ACL-FW in
```

ACL on VLAN Interface (In and Out directions)

- Configure two-way ACL on VLAN 10.
- Configure ACL policy (INBOUND) to allow host in VLAN 10, 192.168.10.10, access to the 192.168.11.0 network.
- Configure ACL policy (OUTBOUND) to allow the 192.168.11.0 network access to 192.168.10.10 for HTTP only.
- Apply ACLs under VLAN10 interface



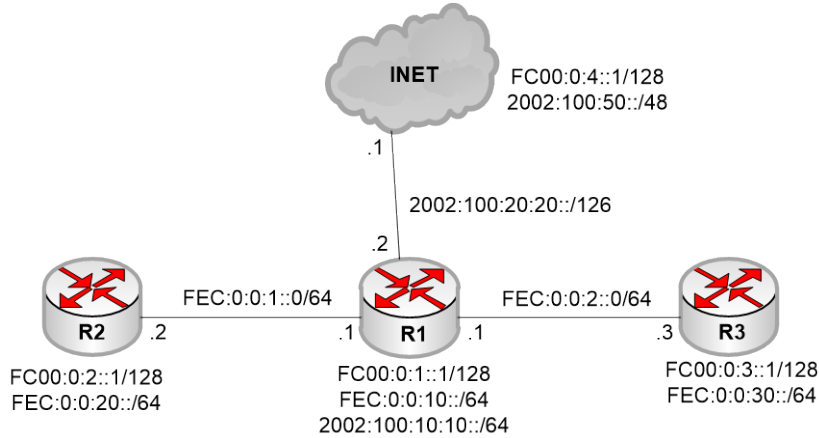
```
ip access-list extended RHG-VLAN10-ACL-IN
permit ip host 192.168.10.10 192.168.11.0 0.0.0.255
```

```
ip access-list extended RHG-VLAN10-ACL-OUT
permit tcp 192.168.11.0 0.0.0.255 host 192.168.10.10 eq 80
```

```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
ip access-group RHG-VLAN10-ACL-IN in
ip access-group RHG-VLAN10-ACL-OUT out
```

IPv6 ACL

- Policy #1: Allow ICMP from 2002:100:50::/48 subnets (ISP) to the 2002:100:10::/48 subnets (internal)
- Policy #2: Allow ISP Router (2002:100:20:20::1) to establish a BGP session with the R1 router (2002:100:20:20::2)
- Apply ACL inbound on WAN facing interface on R1



ipv6 unicast-routing
ipv6 cef

```
ipv6 access-list ROUTEHUB-ACL-IPV6
permit icmp 2002:100:50::/48 2002:100:10::/48
permit tcp host 2002:100:20:20::1 host 2002:100:20:20::2 eq bgp
```

```
interface GigabitEthernet0/0
ipv6 traffic-filter ROUTEHUB-ACL-IPV6 in
```

Permit Even Numbered Routes and Deny Odd Numbered Routes

- 172.17.X.X /16
- Even Numbered Networks: 172.17.2.0, 172.17.4.0, 172.17.6.0
- Odd Numbered Networks: 172.17.1.0, 172.17.3.0, 172.17.5.0

```
access-list 1 deny 172.17.1.0 0.0.254.255
access-list 1 permit 172.17.0.0 0.0.254.255
```

LAND.c Attack ACL

- A **LAND.c** attack occurs when the source and destination IP address are the same.

```
access-list 101 remark LAND ATTACK ACL
access-list 101 deny ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255 log
access-list 101 permit ip any any
```

```
interface serial 0
ip access-group 101 in
```

SMURF Attack ACL

- A typical **SMURF** attack occurs when the destination IP address in a packet goes to a broadcast or network address.

```
access-list 101 remark SMURF ATTACK ACL
access-list 101 deny ip any host 192.168.10.255 log
access-list 101 deny ip any host 192.168.10.0 log
access-list 101 permit ip any any
```

```
interface serial 0
ip access-group 101 in
```

VLAN ACL

- Allow all TCP and UDP traffic for VLAN 200
- Supported on selective Layer 2/3 switches like the Cisco Catalyst 6500 series. Not all switch models support this.
- Note: Configuring Standard or Extended ACLs then applying it to a VLAN SVI interface is more common than using VLAN ACLs.

```
ip access-list extended vlan-tcp
permit tcp any any
```

```
ip access-list extended vlan-udp
permit udp any any
```

```
vlan access-map 1 10
match ip address vlan-tcp
action forward
```

```
vlan access-map 1 20
match ip address vlan-udp
action forward
```

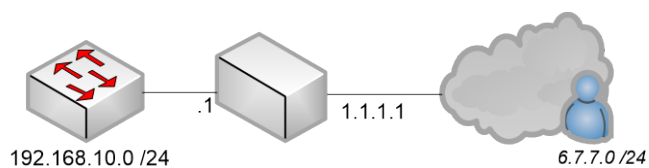
```
vlan filter map 1 vlan-list 200
```

ADSL

Solution/Services: Media Connection, Broadband
Related: N/A

ADSL on Cisco 877 (ATM)

- ADSL configuration on a Cisco 877 ATM interface



```
interface ATM0
no ip address
no atm ilmi-keepalive
dsl operating-mode auto
no shutdown
```

```
interface ATM0.35 point-to-point
ip address 1.1.1.1 255.255.255.0
pvc 0/35
```


ALIAS

Solution/Services: Administration/System
Related: N/A

Alias (EXEC)

- Alias where entering the command "c" will go into the config mode

```
alias exec c config t
```

- Configure alias where typing in "acl" will translate to "show access-list"

```
alias exec acl show access-list
```

- Configure alias called "run-tftp" which will automatically copy the running config to the TFTP server

```
alias exec run-tftp copy system:running-config tftp://192.168.10.10/RHG-config
```

```
show aliases
```

APPLETALK

Solution/Services: Other Protocols

Related: N/A

- Enable AppleTalk
- Define AppleTalk address range and zone on FE1/1

appletalk routing

```
interface FastEthernet1/1
ip address 192.168.10.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
appletalk cable-range 11219-11219 11219.97
appletalk zone Classroom 4
```

ARCHIVE

Solution/Services: Administration/System

Related: N/A

Viewing Configuration Differences

`show archive config differences nvram:start-up system:running-config`

"+" means lines in "run config" not in "start config"

"-" means lines in "start config" not in "run config"

ARP TIMEOUT

Solution/Services: Administration/System

Related: N/A

- Changes ARP timeout from 4 hours (default) to 200 seconds

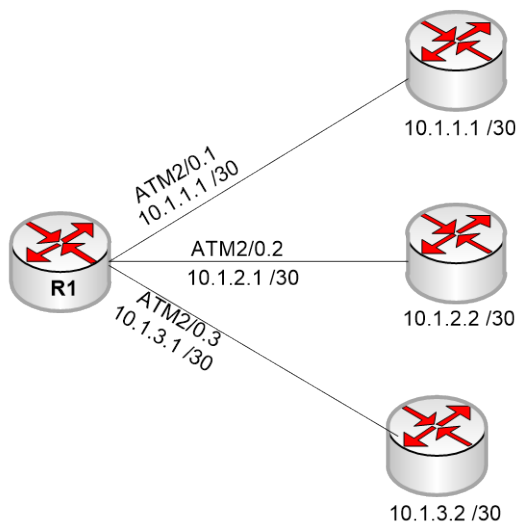
arp timeout 200

ATM

Solution/Services: Media Connection, WAN
Related: N/A

ATM PVC

- Configure ATM in the topology (see below)
- On R1 configure a 1Mbps PVC to 10.1.1.2 (VPI=2,VCI=100)
- On R1 configure a 50Mbps PVC to 10.1.2.1 (VPI=2,VCI=200)
- On R1 configure a 512kbps PVC to 10.1.3.1 (VPI=2,VCI=300)



```
>> R1 <<
interface ATM2/0
no ip address
no ip directed-broadcast
load-interval 30
no atm ilmi-keepalive
no atm enable-ilmi-trap

interface ATM2/0.1 point-to-point
ip address 10.1.1.1 255.255.255.252
no ip directed-broadcast
no atm enable-ilmi-trap
pvc Peer1 2/100
vbr-nrt 1000 1000
```

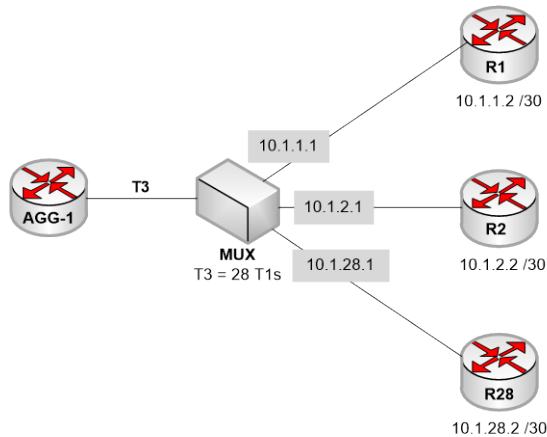
```
interface ATM2/0.2 point-to-point
ip address 10.1.2.1 255.255.255.252
no ip directed-broadcast
no atm enable-ilmi-trap
pvc Peer2 2/200
vbr-nrt 50000 50000
```

```
interface ATM2/0.3 point-to-point
bandwidth 512
ip address 10.1.3.1 255.255.255.252
no ip directed-broadcast
pvc Peer3 2/300
vbr-nrt 512 512
```

```
show atm pvc
show atm map
```

T-3 MUX

- Cisco 7200 with a T3 MUX module (in slot6), running IOS 12.2
- Create 28 T1 circuit interfaces from T3
- T1 interface (channel group #1) from T3 connecting to R1 (10.1.1.0/30)
- T1 interface (channel group #2) from T3 connecting to R2 (10.1.2.0/30)
- T1 interface (channel group #3) from T3 connecting to R28 (10.1.28.0/30)



>> AGG-1 <<

controller T3 6/0

framing m23

clock source line

t1 1 channel-group 0 timeslots 1-24

t1 2 channel-group 0 timeslots 1-24

...

t1 28 channel-group 0 timeslots 1-24

t1 1 clock source Line

t1 2 clock source Line

...

t1 28 clock source Line

interface Serial6/0/1:0

description R1

ip address 10.1.1.1 255.255.255.252

interface Serial6/0/2:0

description R2

ip address 10.1.2.1 255.255.255.252

...

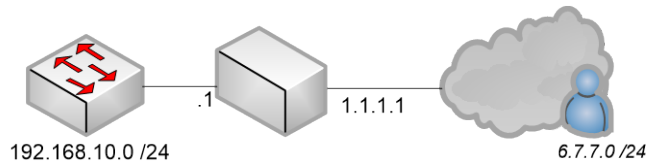
interface Serial6/0/28:0

description R28

ip address ip address 10.1.28.1 255.255.255.252

Packet Over Sonet (POS) for OC-3 and OC-12

- POS (using OC-3 or OC-12) connection to ISP



```
interface POS4/0
description OC-12
bandwidth 622000
ip address 1.1.1.1 255.255.255.0
crc 16
```

OR

```
interface POS4/0
description OC-3
bandwidth 155000
ip address 1.1.1.1 255.255.255.0
crc 16
```


AUX

Solution/Services: Administration/System
Related: N/A

Enable AUX port on Cisco 800

- Enable AUX port

```
line con 0  
modem enable
```

[B]

BFD

Solution/Services: Feature
Related: N/A

Bi-Directional Forwarding Decision (BFD)

- Provides protocol independent mechanism.

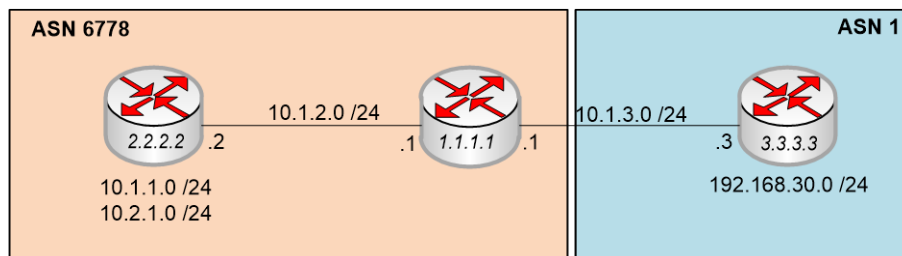
```
interface GigabitEthernet0/1
ip address 10.1.1.1 255.255.255.252
bfd interval 100 min_rx 100 multiplier 3
bfd neighbor 10.1.1.2
```

```
router eigrp 100
brf interface GigabitEthernet0/1
```

BGP

Solution/Services: IP Routing (EGP)

Related: N/A



EBGP Routing

- Configure R1 (1.1.1.1) in ASN 6778 and R3 (3.3.3.3) in ASN 1
- Configure EBGP (connecting between two different ASN) between the R1 and R3

```
>>R1 (1.1.1.1)<<
router bgp 6778
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 10.1.3.3 remote-as 1
  neighbor 10.1.3.3 description EBGP TO ISP
  neighbor 10.1.3.3 version 4
```

```
>>R3 (3.3.3.3)<<
router bgp 1
  bgp router-id 3.3.3.3
  bgp log-neighbor-changes
  neighbor 10.1.3.1 remote-as 6778
  neighbor 10.1.3.1 description EBGP TO CPE
  neighbor 10.1.3.1 version 4
```

IBGP Routing

- Configure IBGP (connecting in the same ASN) between the R1 (1.1.1.1) and R2 (2.2.2.2)

```
>>R1 (1.1.1.1)<<
router bgp 6778
neighbor 2.2.2.2 remote-as 6778
neighbor 2.2.2.2 description IBGP TO R2
neighbor 2.2.2.2 update-source Loopback0
neighbor 2.2.2.2 next-hop-self
```

```
>>R2 (2.2.2.2)<<
router bgp 6778
neighbor 1.1.1.1 remote-as 6778
neighbor 1.1.1.1 description IBGP TO R1
neighbor 1.1.1.1 update-source Loopback0
neighbor 1.1.1.1 next-hop-self
```

BGP Route Advertisement

- Specify what networks will be advertised from R1 to other BGP routers

```
>>R1<<
router bgp 6778
network 10.1.0.0 mask 255.255.255.0
network 10.2.0.0 mask 255.255.255.0
```

- The exact network must exist in the routing table. A network of 10.1.1.0/24 will not match what is configured under BGP, therefore, NULL static routes should be configured so the BGP routes can be advertised

```
ip route 10.1.0.0 255.255.0.0 Null0 253
ip route 10.2.0.0 255.255.0.0 Null0 253
```

Synchronization

- Disables synchronization, but routes need to have an exact routing entry for what will be advertised
- Reference: BGP Route Advertisement

```
>>R1<<  
router bgp 6778  
no synchronization
```

MD5 Authentication

- Enables MD5 authentication with the configured BGP peer(s)

```
>>R1<<  
router bgp 6778  
neighbor 10.1.3.3 password cisco123  
neighbor 2.2.2.2 password cisco123
```

Timers

- Tune BGP timers to 15 seconds for keepalives and 45 seconds for holdtime to provide fast convergence.

```
>>R1<<  
router bgp 6778  
timers bgp 15 45
```

Soft Reconfiguration

- Soft reconfiguration configured on all BGP peers

>>R1<<

router bgp 6778

neighbor 10.1.3.3 soft-reconfiguration inbound

neighbor 2.2.2.2 soft-reconfiguration inbound

Route Control/Filtering (Inbound)

- Only receive routes listed in the prefix list on R1

>>R1<<

ip prefix-list ISP-ROUTES seq 10 permit 192.168.30.0/24

ip prefix-list ISP-ROUTES seq 11 permit 0.0.0.0/0

router bgp 6778

neighbor 10.1.3.3 prefix-list ISP-ROUTES in

Route Control/Filtering (Outbound)

- Configure R1 to only advertise routes that are listed in the prefix list to R3

>>R1<<

ip prefix-list CL-ROUTES seq 10 permit 10.1.0.0/16

ip prefix-list CL-ROUTES seq 11 permit 10.2.0.0/16

router bgp 6778

neighbor 10.1.3.3 prefix-list CL-ROUTES out

Route Summarization

- Summarizes all 10.x.x.x BGP routes as a single route, 10.0.0.0/8 to all EBGp peers

>>R1<<

router bgp 6778

aggregate-address 10.0.0.0 255.0.0.0 summary-only

iBGP: Next Hop Self

- Configures iBGP peer to use the next hop IP of R1 for routes learned from an EBGp peer

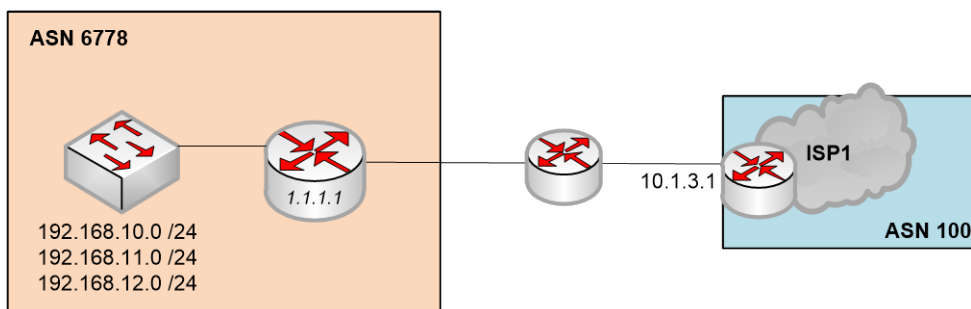
>>R1<<

router bgp 6778

neighbor 2.2.2.2 next-hop-self

EBGP: Multi-Hop

- Max hop value = 255
- The EBGp peer is not directly connected and is about 10 hops away



router bgp 6778

neighbor 10.1.3.1 ebgp-multihop 10

Changing Admin Distance

- Specify custom admin distance (external to ASN, internal to ASN, & local routes)

```
router bgp 6778
distance bgp 100 200 50
```

Peer Groups

- Create BGP peer group profile with typical neighbor configuration for peer group
- Assign the BGP peer group to the IBGP peer

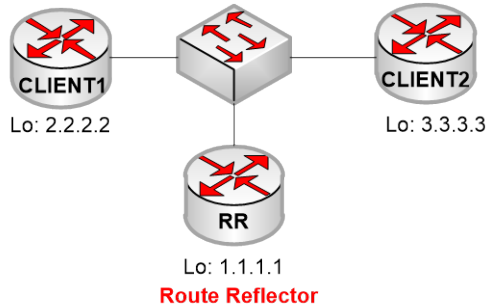
```
interface Loopback0
ip address 1.1.1.1 255.255.255.255

router bgp 6778
neighbor RHG-IBGP-PEER peer-group
neighbor RHG-IBGP-PEER version 4
neighbor RHG-IBGP-PEER next-hop-self
neighbor RHG-IBGP-PEER soft-reconfiguration inbound
neighbor RHG-IBGP-PEER update-source Loopback0
neighbor 2.2.2.2 remote-as 6778
neighbor 2.2.2.2 peer-group RHG-IBGP-PEER
```

```
show ip bgp peer-group
```


Route Reflectors

- Configures RR as the BGP Route Reflector (RR) router with two connected Clients for IBGP peering.
- Client1 and Client2's IBGP peer points to the RR BGP router



>> RR <<

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
```

```
router bgp 6778
```

```
neighbor 2.2.2.2 remote-as 6778
neighbor 2.2.2.2 update-source Loopback0
neighbor 2.2.2.2 route-reflector-client
neighbor 3.3.3.3 remote-as 6778
neighbor 3.3.3.3 update-source Loopback0
neighbor 3.3.3.3 route-reflector-client
```

>> CLIENT1 <<

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
```

```
router bgp 6778
```

```
neighbor 1.1.1.1 remote-as 6778
neighbor 1.1.1.1 update-source Loopback0
```

>> CLIENT2 <<

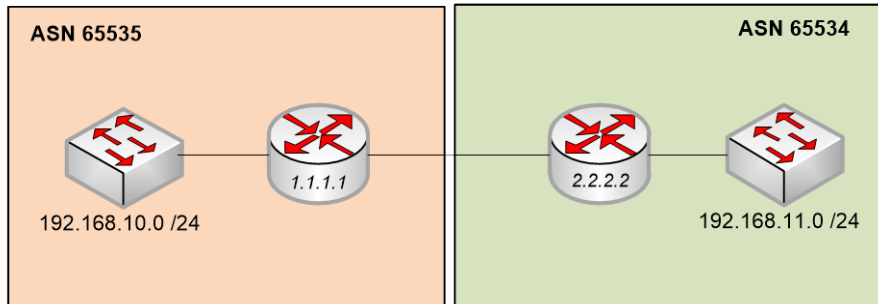
```
interface Loopback0
ip address 3.3.3.3 255.255.255.255
```

```
router bgp 6778
```

```
neighbor 1.1.1.1 remote-as 6778
neighbor 1.1.1.1 update-source Loopback0
```

Private ASN

- *Private ASN: 64512 – 65535*



>> R1 <<

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
```

router bgp 65535

```
neighbor 2.2.2.2 remote-as 65534
neighbor 2.2.2.2 update-source Loopback0
```

>> R2 <<

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
```

router bgp 65534

```
neighbor 1.1.1.1 remote-as 65535
neighbor 1.1.1.1 update-source Loopback0
```

Maximum Paths Per Route

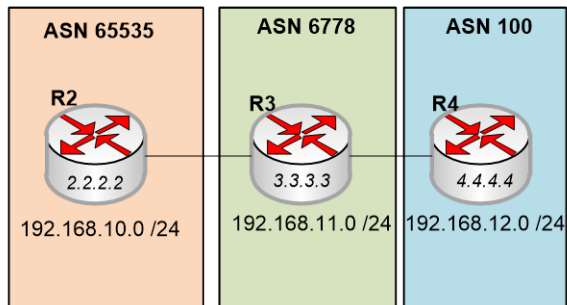
- Define the number of paths to be 2 for a single route to be injected into the routing table
- Define the number of paths to be 2 for a single route learned via EBGp
- Define the number of paths to be 4 for a single route learned via IBGP

router bgp 6778

```
maximum-paths 2
maximum-paths ebgp 2
maximum-paths ibgp 4
```

Removing Private ASN

- Configure R2 in Private ASN 65535
- Configure R3 to remove any Private ASN towards ASN100 and replace it with its own ASN (6778) when forwarding from R2



>> R2 <<

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
```

```
router bgp 65535
neighbor 3.3.3.3 remote-as 6778
neighbor 3.3.3.3 update-source Loopback0
network 192.168.10.0
```

>> R3 <<

```
interface Loopback0
ip address 3.3.3.3 255.255.255.255
```

```
router bgp 6778
neighbor 4.4.4.4 remote-as 100
neighbor 4.4.4.4 remove-private-as
neighbor 2.2.2.2 remote-as 65535
neighbor 2.2.2.2 update-source Loopback0
neighbor 2.2.2.2 next-hop-self
network 192.168.11.0
```

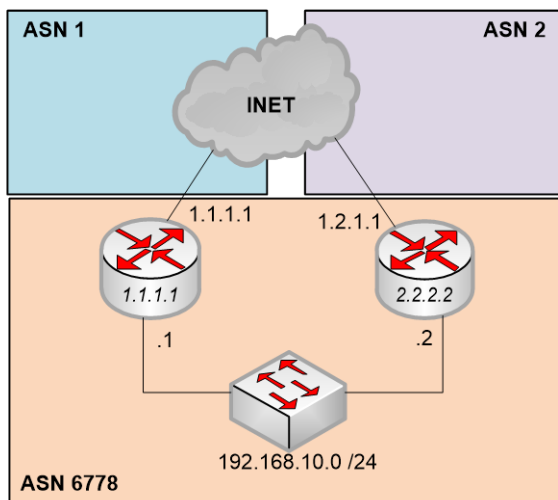
>> R4 <<

```
interface Loopback0
ip address 4.4.4.4 255.255.255.255
```

```
router bgp 100
neighbor 3.3.3.3 remote-as 6778
neighbor 3.3.3.3 update-source Loopback0
network 192.168.12.0
```

BGP Attribute: Local Preference

- **Local Preference:** Higher the value, the more preferred
- **When to Use:** When all routers exist in the same ASN for Internet redundancy (see diagram)
- Configure R1 (1.1.1.1) as the primary path for Internet access
- Configure R2 (2.2.2.2) as the secondary path for Internet access



```
>>R1 (1.1.1.1)<<
```

```
route-map RM-BGP-PRI-IN permit 10  
set local-preference 100
```

```
router bgp 6778  
address-family ipv4  
neighbor 1.1.1.2 remote-as 1  
neighbor 2.2.2.2 remote-as 6778  
neighbor 2.2.2.2 next-hop-self  
network 192.168.10.0  
neighbor 1.1.1.2 route-map RM-BGP-PRI-IN in
```

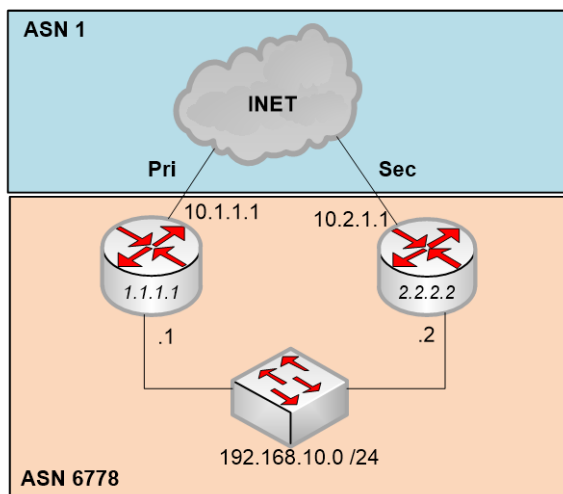
```
>>R2 (2.2.2.2)<<
```

```
route-map RM-BGP-SEC-IN permit 10  
set local-preference 10
```

```
router bgp 6778  
address-family ipv4  
neighbor 1.2.1.2 remote-as 2  
neighbor 1.1.1.1 remote-as 6778  
neighbor 1.1.1.1 next-hop-self  
network 192.168.10.0  
neighbor 1.2.1.2 route-map RM-BGP-SEC-IN in
```

BGP Attribute: MED

- **MED:** Lower the value, the more preferred
- **When to Use:** When peering with the same ISP ASN for Internet redundancy (see diagram)
- Configure R1 (1.1.1.1) as the primary path for devices on the Internet to access ASN 6778
- Configure R2 (2.2.2.2) as the secondary path for devices on the Internet to access ASN 6778



>>R1 (1.1.1.1)<<

```
route-map RM-BGP-PRI-OUT permit 10
set metric 10
```

```
router bgp 6778
address-family ipv4
neighbor 10.1.1.2 remote-as 1
neighbor 2.2.2.2 remote-as 6778
network 192.168.10.0
neighbor 10.1.1.2 route-map RM-BGP-PRI-OUT out
```

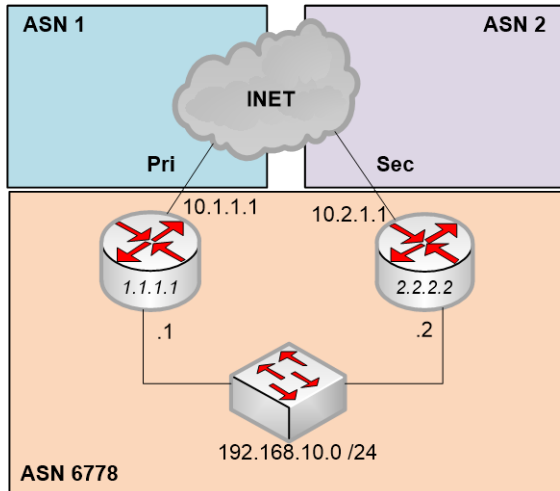
>>R2 (2.2.2.2)<<

```
route-map RM-BGP-SEC-OUT permit 10
set metric 100
```

```
router bgp 6778
address-family ipv4
neighbor 10.2.1.2 remote-as 1
neighbor 1.1.1.1 remote-as 6778
network 192.168.10.0
neighbor 10.2.1.2 route-map RM-BGP-SEC-OUT out
```

BGP Attribute: AS PATH (Prepending, Padding)

- **AS PATH:** Lower the path to the ASN, the more preferred
- **When to Use:** When peering with different ISP ASNs for Internet Redundancy (see diagram)
- Configure R1 (1.1.1.1) as the primary path for devices on the Internet to access ASN 6778
- Configure R2 (2.2.2.2) as the secondary path for devices on the Internet to access ASN 6778



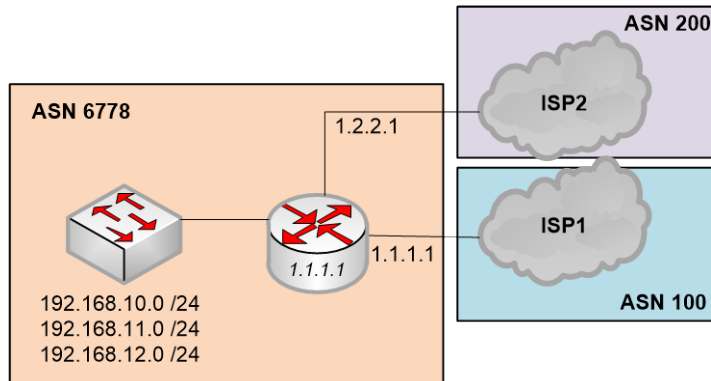
```
>>R1 (1.1.1.1)<<
router bgp 6778
address-family ipv4
neighbor 10.1.1.2 remote-as 1
neighbor 2.2.2.2 remote-as 6778
network 192.168.10.0
neighbor 10.1.1.2 route-map RM-BGP-PRI-OUT out
```

```
>>R2 (2.2.2.2)<<
route-map RM-BGP-PRI-OUT permit 10
set as-path prepend 6778 6778 6778 6778 6778
```

```
router bgp 6778
address-family ipv4
neighbor 10.2.1.2 remote-as 2
neighbor 1.1.1.1 remote-as 6778
network 192.168.10.0
neighbor 10.2.1.2 route-map RM-BGP-SEC-OUT out
```

Conditional Advertisement

- We are only accepting a default route from the BGP peers (ASN 200 and ASN 100)
- Primary BGP Routing (inbound/outbound) through ASN 100
- Secondary BGP Routing (inbound/outbound) through ASN 200
- R1 (1.1.1.1) will only advertise its BGP routes out to ISP1 and not ISP2
- If R1 (1.1.1.1) does not receive a default BGP route from ISP1 (ASN100), advertise BGP routes from ASN6778 out to ISP2



```
ip as-path access-list 1 permit ^100
```

```
ip access-list standard RHG-ACL-DEFAULT
permit 0.0.0.0
```

```
ip access-list standard RHG-ACL-SUBNETS
permit 192.168.10.0 0.0.0.255
permit 192.168.11.0 0.0.0.255
permit 192.168.12.0 0.0.0.255
```

```
route-map RHG-RM-DEFAULT-PRI permit 10
match ip address RHG-ACL-DEFAULT
set weight 100
```

```
route-map RHG-RM-DEFAULT-PRI permit 11
```

```
route-map RHG-RM-DEFAULT-SEC permit 10
match ip address RHG-ACL-DEFAULT
set weight 50
```

```
route-map RHG-RM-DEFAULT-SEC permit 11
```

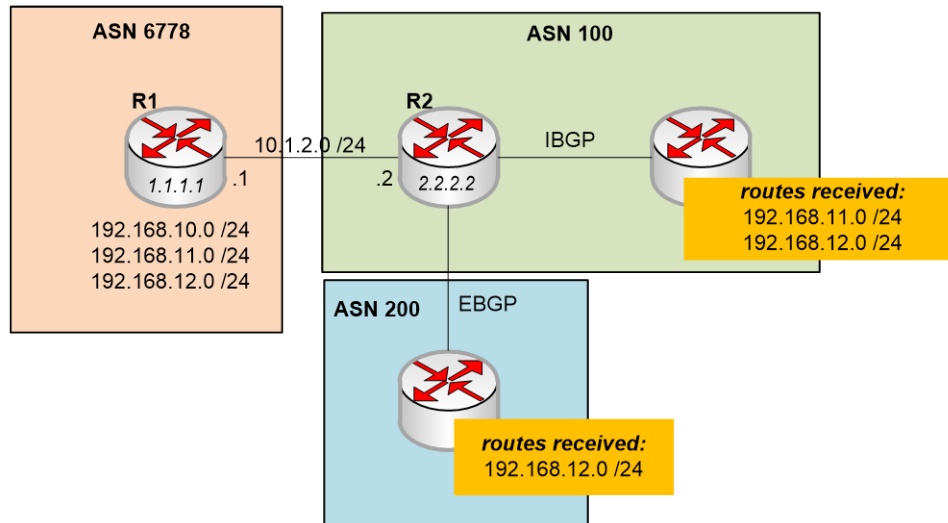
```
route-map RHG-RM-ADVERTISE permit 10
match ip address RHG-ACL-SUBNETS
```

```
route-map RHG-RM-NON-EXIST permit 10
match ip address RHG-ACL-DEFAULT
match as-path 1
```

```
router bgp 6778
no synchronization
bgp log-neighbor-changes
network 192.168.10.0
network 192.168.11.0
network 192.168.12.0
neighbor 1.1.1.2 remote-as 100
neighbor 1.1.1.2 ebgp-multihop 5
neighbor 1.1.1.2 route-map RHG-RM-DEFAULT-PRI in
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 ebgp-multihop 255
neighbor 2.2.2.2 soft-reconfiguration inbound
neighbor 2.2.2.2 route-map RHG-RM-DEFAULT-SEC in
neighbor 2.2.2.2 advertise-map RHG-RM-ADVERTISE non-exist-map RHG-RM-NON-EXIST
no auto-summary
```


BGP Communities

- BGP Community "No Advertise": do not advertise BGP routes to ANY BGP peer
- BGP Community "No Export": do not advertise BGP routes to any other EBGP peer. Only IBGP peer(s) if configured
- BGP Community "Internet": advertise BGP route to ANY BGP peer.
- Configure R1 to inform R2 to not advertise subnet 192.168.10.0 to ANY other BGP peer
- Configure R1 to inform R2 to not advertise subnet 192.168.11.0 to other EBGP peers
- Configure R1 to inform R2 to advertise subnet 192.168.12.0 to ANY BGP peer



```
>> R1 (1.1.1.1)<<
interface Loopback0
ip address 1.1.1.1 255.255.255.255

ip access-list standard RHG-ACL-NET-10
permit 192.168.10.0 0.0.0.255

ip access-list standard RHG-ACL-NET-11
permit 192.168.11.0 0.0.0.255

ip access-list standard RHG-ACL-NET-12
permit 192.168.12.0 0.0.0.255

route-map RHG-RM-BGP-COM permit 10
match ip address RHG-ACL-NET-10
set community no-advertise

route-map RHG-RM-BGP-COM permit 11
match ip address RHG-ACL-NET-11
set community no-export

route-map RHG-RM-BGP-COM permit 12
match ip address RHG-ACL-NET-12
set community internet
```

```
router bgp 6778
neighbor 10.1.2.2 remote 100
neighbor 10.1.2.2 send-community
neighbor 10.1.2.2 route-map RHG-RM-BGP-COM out
network 192.168.10.0
network 192.168.11.0
network 192.168.12.0
```

```
>> R2 <<
interface Loopback0
ip address 2.2.2.2 255.255.255.255
```

```
router bgp 100
neighbor 10.1.2.1 remote-as 6778
neighbor 10.2.3.2 remote-as 100
neighbor 10.2.4.2 remote-as 200
```

Monitoring Commands for BGPv4

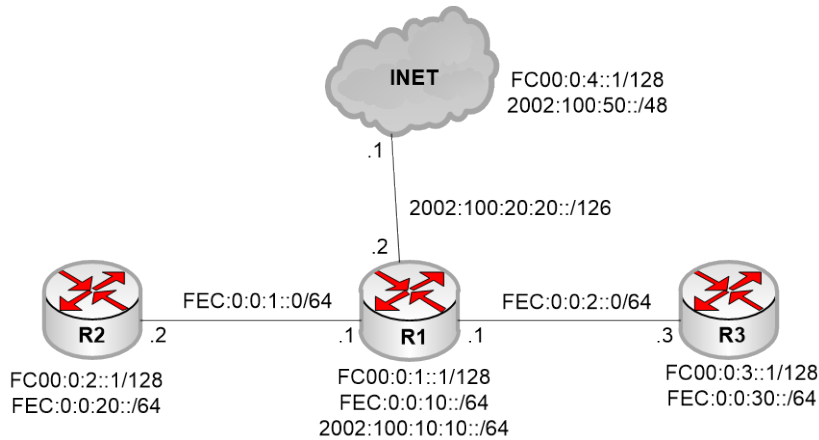
show ip route bgp
show ip bgp
show ip bgp summary
show ip bgp neighbors

! view what routes are received from the BGP peer
show ip bgp neighbors <x.x.x.x> received-routes

! view what routes will be advertised to the BGP peer
show ip bgp neighbors <x.x.x.x> advertised-routes

BGPv4+ (IPv6)

- Configure BGPv4+ between R1 and ISP router
- ISP exist in ASN 1
- R1 exist in ASN 6778
- R1 will advertise prefixes 2002:100:10:10::/64 and FC00:0:1::1/128 to ISP
- ISP1 will advertise prefixes 2002:100:50::/48 and FC00:0:4::1/128 to R1



>> ISP <<

```
ipv6 unicast-routing
ipv6 cef
```

```
interface Loopback0
ipv6 address FC00:0:4::1/128
ipv6 enable
```

```
interface GigabitEthernet0/0
ipv6 address 2002:100:10:10::1/126
ipv6 enable
```

```
router bgp 1
neighbor 2002:100:20:20::2 remote-as 6778
neighbor 2002:100:20:20::2 password cisco123
no auto-summary
```

```
address-family ipv6
neighbor 2002:100:20:20::2 activate
network 2002:100:20:20::/126
network 2002:100:50::/48
network FC00:0:4::1/128
no synchronization
exit-address-family
```

>> R1 <<

```
ipv6 unicast-routing
ipv6 cef
```

```
interface Loopback0
  ipv6 address FC00:0:1::1/128
  ipv6 enable
```

```
interface GigabitEthernet0/0
  ipv6 address 2002:100:20:20::2/126
  ipv6 enable
```

```
router bgp 6778
  neighbor 2002:100:20:20::1 remote-as 1
  neighbor 2002:100:20:20::1 password cisco123
  no auto-summary
```

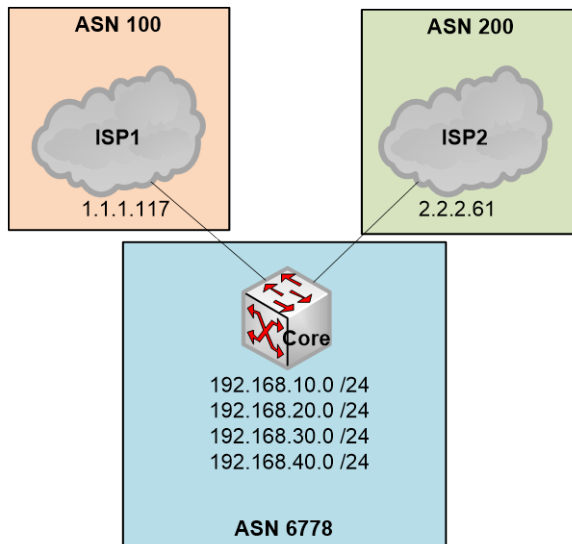
```
address-family ipv6
  neighbor 2002:100:20:20::1 activate
  network 2002:100:20:20::/126
  network 2002:100:10::/48
  network FC00:0:1::1/128
  no synchronization
  exit-address-family
```

```
ipv6 route 2002:100:10::/48 Null0
```

```
show ip bgp ipv6 unicast summary
show ip bgp ipv6 unicast
show ipv6 route
```

Solution: Advanced BGP with Dual Providers and PBR

- In this scenario we have two ISP providers enabled for BGP.
- In our network we have four subnets which are: 192.168.10.0, 192.168.20.0, 192.168.30.0, & 192.168.40.0
- These will be the IP Addresses for our two ISP routers: ISP1 (1.1.1.117), ISP2 (2.2.2.61)
- Outbound: this is for access from our LAN/DC out to the Internet. Primary Internet access will be routed through ISP1. Secondary Internet access will be routed through ISP2
- Inbound: this is for access from the Internet into our LAN/DC. Access to networks 192.168.10.0 and 192.168.20.0 will be routed through ISP1. Access to network 192.168.30.0 and 192.168.40.0 will be routed through ISP2.
- If any of the providers fail, the networks will be routed through the other provider.



```
route-map RHG-PBR-OUT-ISP2 permit 10
match ip address RHG-acl-ISP2
set ip next-hop 2.2.2.61
```

```
interface Vlan123
description "RHG Servers"
ip address 192.168.10.1 255.255.255.224
no ip redirects
no ip unreachable
no ip proxy-arp
ip policy route-map RHG-PBR-OUT-ISP2
```

```
ip access-list standard RHG-acl-ISP2
permit 192.168.10.0 0.0.0.255
permit 192.168.20.0 0.0.0.255
```

```
ip access-list standard RHG-acl-ISP1
permit 192.168.30.0 0.0.0.255
```

```
permit 192.168.40.0 0.0.0.255
```

```
access-list 2 permit any
```

```
route-map RHG-ISP1-SEC permit 10  
match ip address RHG-acl-ISP2  
continue  
set as-path prepend 6778 6778 6778 6778 6778 6778
```

```
route-map RHG-ISP1-SEC permit 20  
match ip address 2
```

```
route-map RHG-ISP2-SEC permit 10  
match ip address RHG-acl-ISP1  
continue  
set as-path prepend 6778 6778 6778 6778 6778 6778
```

```
route-map RHG-ISP2-SEC permit 20  
match ip address 2
```

```
ip access-list standard RHG-acl-default  
permit 0.0.0.0
```

```
route-map RHG-RM-DEFAULT-PRI permit 10  
match ip address RHG-acl-default  
set weight 100
```

```
route-map RHG-RM-DEFAULT-PRI permit 11
```

```
route-map RHG-RM-DEFAULT-SEC permit 10  
match ip address RHG-acl-default  
set weight 50
```

```
route-map RHG-RM-DEFAULT-SEC permit 11
```

```
router bgp 6778  
no synchronization  
bgp log-neighbor-changes  
aggregate-address 192.168.10.0 255.255.255.0 summary-only  
aggregate-address 192.168.30.0 255.255.255.0 summary-only  
aggregate-address 192.168.40.0 255.255.255.0 summary-only  
aggregate-address 192.168.20.0 255.255.255.0 summary-only  
redistribute connected  
redistribute static  
neighbor 1.1.1.117 remote-as 100  
neighbor 1.1.1.117 ebgp-multihop 5  
neighbor 1.1.1.117 route-map RHG-ISP1-SEC out  
neighbor 1.1.1.117 route-map RHG-RM-DEFAULT-PRI in
```

```
neighbor 2.2.2.61 remote-as 200
neighbor 2.2.2.61 soft-reconfiguration inbound
neighbor 2.2.2.61 route-map RHG-RM-DEFAULT-SEC in
neighbor 2.2.2.61 route-map RHG-ISP2-SEC out
default-information originate
no auto-summary
```


BPDU

BPDU Guard (global)

- Enables BPDU Guard on all edge ports on a switch

spanning-tree portfast edge bpduguard default

[C]

CARRIER DELAY

Solution/Services: Feature
Related: N/A

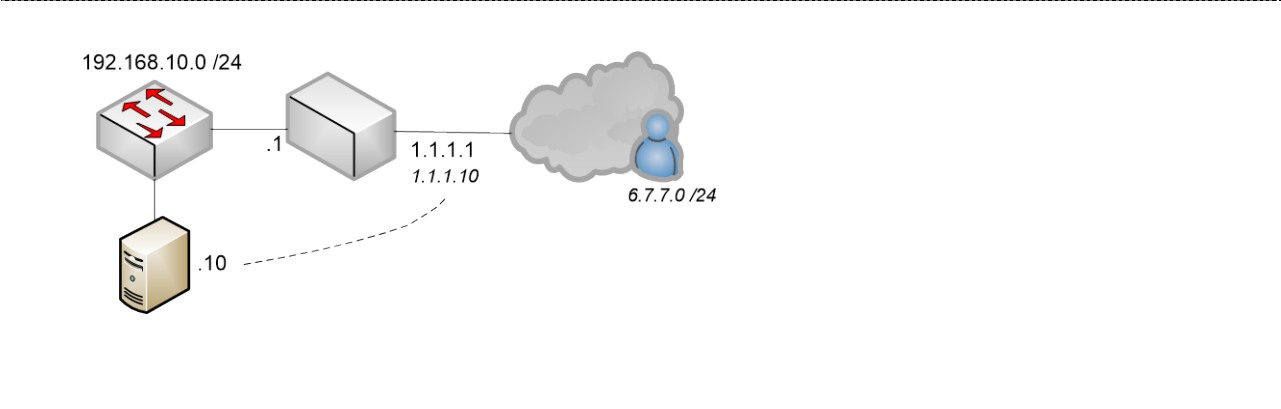
- Ensures no additional delay in the notification of a down link for interface GE1/1

```
interface GigabitEthernet1/1  
  carrier-delay msec 0
```

```
show interfaces GigabitEthernet1/1 debounce
```

CBAC

Solution/Services: Security: Cisco IOS Firewall Related: ACL



- Stateful Firewall configuration using Context-Based Access Control (CBAC)
- Specify traffic that will be inspected as Stateful traffic to be allowed back in

```
ip inspect name FW http timeout 3600
ip inspect name FW ftp timeout 3600
ip inspect name FW rcmd timeout 3600
ip inspect name FW realaudio timeout 3600
ip inspect name FW esmtp timeout 3600
ip inspect name FW tftp timeout 30
ip inspect name FW tcp timeout 3600
ip inspect name FW udp timeout 15
ip inspect name FW h323 timeout 3600
ip inspect name FW snmp timeout 3600
```

- Specify inbound ACL policy for any traffic that originates from the outside into our network

- _____

```
ip access-list extended ingress-acl
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
permit tcp any host 1.1.1.10 eq smtp
permit tcp any host 1.1.1.10 eq 443
permit tcp any host 1.1.1.10 eq www
permit icmp any any echo-reply
permit udp any host 1.1.1.1 eq isakmp
permit udp any host 1.1.1.1 eq 4500
permit esp any host 1.1.1.1
permit udp host 6.7.7.8 any eq snmp
permit tcp any eq ftp-data any
deny ip any any log
```

- Apply Stateful policy (using CBAC) outbound and the ACL policy (ingress-acl) inbound on WAN facing interface

```
interface Serial0/0
ip address 1.1.1.1 255.255.255.0
ip access-group ingress-acl in
ip inspect FW out
```

CEF

Solution/Services: Feature
Related: N/A

CEF Load Sharing: L3/L4 Hash

- Enable CEF load-sharing algorithm to use L3+L4 information for load balancing traffic in hardware

```
mls ip cef load-sharing full
```

CEF Route Path

- Confirm the CEF route entry (based on the CEF table) when 192.168.10.10 (src) is communicating with 192.168.20.10 (dst).

```
show mls cef exact-route 192.168.10.10 192.168.20.10
```

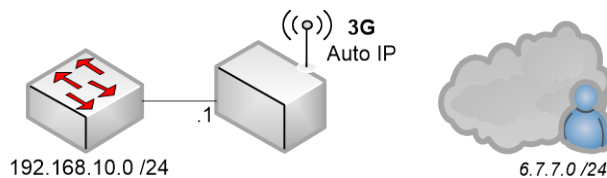
CELLULAR

Solution/Services: Media Connection, WWAN

Related: N/A

3G Wireless Card in Cisco Router

- Configure Cisco router with 3G Wireless WAN card for connecting to the Internet. Obtain IP dynamically.



```
chat-script cdma "" "ATDT#777" TIMEOUT 60 "CONNECT"
```

```
access-list 10 permit any
dialer-list 10 protocol ip list 1
```

```
interface Cellular0/0/0
ip address negotiated
encapsulation ppp
dialer in-band
dialer idle-timeout 0
dialer string cdma
dialer-group 1
async mode interactive
ppp chap password cisco
```

```
ip route 0.0.0.0 0.0.0.0 Cellular0/0/0
```

```
line 0/0/0
exec-timeout 0 0
script dialer cdma
modem InOut
no exec
transport input all
rxspeed 3100000
txspeed 1800000
```

```
show cellular 0/0/0 all
```

CGMP

Solution/Services: Multicast

Related: N/A

- Enable CGMP

```
interface fastethernet0/1
```

```
ip cgmp
```

```
show cgmp
```

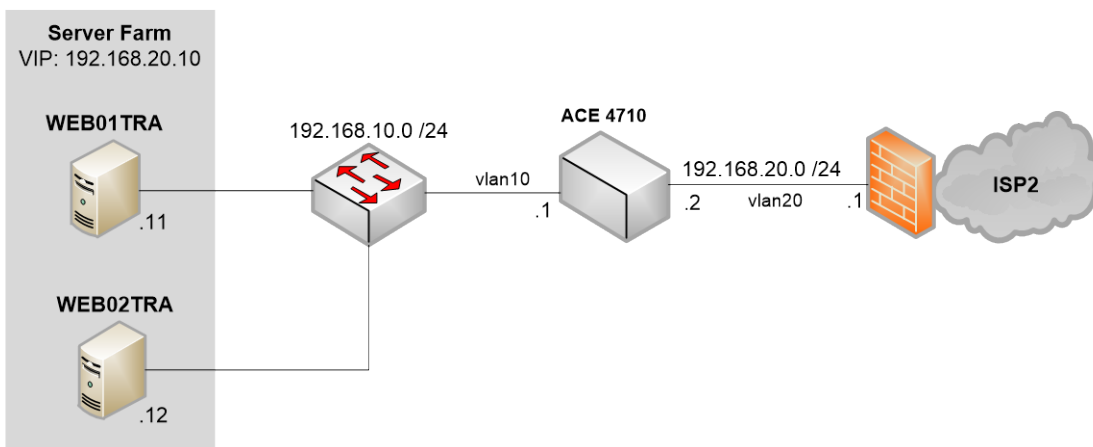
CISCO ACE SERIES

Solution/Services: Cisco ACE Series

Related: N/A

Routed Mode

- Configure the ACE 4710 to load balance between two web servers (WEB01TRA and WEB02TRA) running HTTP (TCP port 80)
- Only load balance between servers that active via a ICMP reply
- The VIP used for the load-balanced web server farm will be 192.168.20.10
- Configure ACL policy allowing only HTTP to the VIP through the ACE appliance



```
interface vlan 20
description OUTSIDE INTERFACE
ip address 192.168.20.2 255.255.255.0
no shutdown
```

```
interface vlan 10
description INSIDE INTERFACE
ip address 192.168.10.1 255.255.255.0
no shutdown
```

```
interface gigabitEthernet 1/1
switchport access vlan 20
switchport mode access
no shutdown
```



```
interface gigabitEthernet 1/2
switchport access vlan 10
switchport mode access
no shutdown
```

```
rserver host WEB01TRA
ip address 192.168.10.11
inservice
```

```
rserver host WEB02TRA
ip address 192.168.10.12
inservice
```

```
serverfarm host RHG-SF-WEB
rserver WEB01TRA
inservice
rserver WEB02TRA
inservice
```

```
class-map match-all RHG-CLASS-VIP-WEB
2 match virtual-address 192.168.20.10 tcp eq www
```

```
policy-map type loadbalance http first-match RHG-POL-LB-WEB
class class-default
serverfarm RHG-SF-WEB
```

```
policy-map multi-match RHG-POL-LB
class RHG-CLASS-VIP-WEB
loadbalance vip inservice
loadbalance policy RHG-POL-LB-WEB
loadbalance vip icmp-reply active
```

```
access-list RHG-ACL-WAN extended permit tcp any host 192.168.20.10 eq 80
```

```
interface vlan 20
ip address 192.168.20.2 255.255.255.0
access-group input RHG-ACL-WAN
service-policy input RHG-POL-LB
no shutdown
```

```
ip route 0.0.0.0 0.0.0.0 172.16.10.1
```

Management Traffic

- Define class map for management traffic which is blocked by default then associate it to a policy.
- Associate policy to WAN facing interface (in the design) to allow Management traffic specified in the class-map

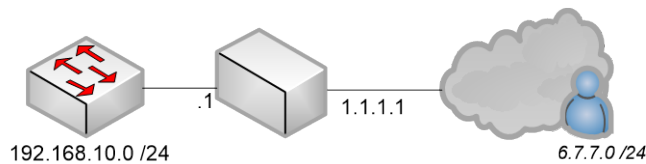
```
class-map type management match-any RHG-CLASS-MGMT
2 match protocol ssh any
3 match protocol telnet any
5 match protocol https any
6 match protocol http any
7 match protocol icmp any
```

```
policy-map type management first-match RHG-POL-MGMT
class RHG-CLASS-MGMT
permit
```

```
interface vlan 20
service-policy input RHG-POL-MGMT
```

CISCO ASA/FWSM SERIES

Solution/Services: Cisco ASA 5500, Cisco PIX 500, Cisco FWSM
Related: N/A



Base Configuration

- Base configuration applied first on ASA. Configuration includes the hostname, enable password, telnet/ssh password (if AAA is not configured), timezone, logging, and permitting the “outside” interface to be pingable

```
hostname EFW01TRA
```

```
enable password cisco123
```

```
passwd cisco123
```

```
clock timezone PST -8
```

```
logging enable  
logging monitor debugging  
logging buffered debugging  
logging asdm information
```

```
icmp permit any outside
```

Install a License

- Cisco ASA OS 8.3
- Apply new ASA license using provided “activation key”

```
activation-key 0x81234567 0x81234567 0x81234567 0x81234567 0x81234567
```

```
show activation-key
```

Interfaces

- *Cisco ASA OS 8.3+*
- Configures WAN facing interface using the alias "outside"
- Configures LAN facing interface using the alias "inside"

```
interface Ethernet0
nameif outside
ip address 1.1.1.1 255.255.255.0
```

```
interface Ethernet1
nameif inside
ip address 192.168.10.1 255.255.255.0
```

Static Routing

- *Cisco ASA OS 8.3*
- Configures default gateway through the WAN interface (outside)

```
route outside 0.0.0.0 0.0.0.0 1.1.1.2 1
```

Device Access (SSH, Telnet)

- Enable Telnet access from 192.168.10.0 (from the inside)
- Enable SSH access from host 6.7.7.8 (from the outside) and 192.168.10.0 (from the inside)
- Telnet and SSH access will use local database.
- User account "admin" will be added to the local user database

```
telnet 192.168.10.0 255.255.255.0 inside
telnet timeout 60
```

```
domain-name routehub.local
```

```
crypto key generate rsa modulus 1024
```

```
ssh 6.7.7.8 255.255.255.255 outside
ssh 192.168.10.0 255.255.255.0 inside
ssh timeout 40
```

```
username admin password cisco123 privilege 15
```

```
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
```

ASA Image

- *Cisco ASA OS 8.3*
- Specify the ASA OS version that will be loaded.
- *Note: after the change is completed a reload of the ASA is required*

```
boot system disk0:/asa804-k8.bin
```

HTTP and ASDM

- *Cisco ASA OS 8.3*
- Enable ASDM on the ASA to use TCP port 8080
- Anyone on the Internet (outside) can access the ASDM, but on the inside only users on the 192.168.10.0 network can access the ASDM for administration
- Specify the ASDM image that will be loaded and used on ASA

```
http server enable 8080
http 192.168.10.0 255.255.255.0 inside
http 0.0.0.0 0.0.0.0 outside
```

```
asdm image disk0:/asdm-613.bin
```

RADIUS

- *Cisco ASA OS 8.3*
- Enable RADIUS using RADIUS server is 192.168.10.11 using the key "cisco123"
- Use RADIUS for Telnet and SSH access into the ASA firewall

```
aaa-server IAS protocol radius
aaa-server IAS host 192.168.10.11
timeout 5
key cisco123
```

```
aaa authentication telnet console IAS
aaa authentication ssh console IAS
```

DHCP Server

- *Cisco ASA OS 8.3*
- Specify DHCP scope for the IP subnet (192.168.10.0), interface (inside), DNS, WINS, and domain
- Apply DHCP services on "inside" interface

```
dhcpd address 192.168.10.0 inside
dhcpd dns 192.168.10.10 4.2.2.2 interface inside
dhcpd wins 192.168.10.10 interface inside
dhcpd domain routehub.local interface inside
dhcpd update dns both override interface inside
```

```
dhcpd enable inside
```

PPPoE

- Enable PPPoE on WAN facing (outside) interface
- PPP username will be "pppoeuser" and password will be "Cisco123"

```
vpdn group Internet request dialout pppoe
vpdn group Internet localname pppoeuser
vpdn group Internet ppp authentication pap
vpdn username pppoeuser password Cisco123 store-local
dhcpd auto_config outside
```

```
interface Ethernet0
 nameif outside
 security-level 0
 pppoe client vpdn group Internet
 ip address pppoe setroute
```

Copy using FTP

- FTP server (192.168.10.10), FTP username/password (cisco/cisco123)
- Copy ASA file (e.g. ASA OS, ASDM) from FTP server to local flash (disk0)

```
copy ftp://cisco:cisco123@192.168.10.10 disk0:
```

LDAP

- Enable LDAP authentication pointing to Microsoft LDAP server (192.168.10.10) located on the inside
- Specify LDAP domain (dc=routehub,dc=local)
- User account names will be based on "samAccountName" in Active Directory
- Authenticating with LDAP will use the Administrator account located in the "Users" containers. The AD password for the Administrator account is cisco123

```
aaa-server RHG-AAA-LDAP protocol ldap
aaa-server RHG-AAA-LDAP (inside) host 192.168.10.10
server-port 389
```

```
ldap-base-dn dc=routehub,dc=local
ldap-scope subtree
```

```
ldap-naming-attribute samAccountName
```

```
ldap-login-dn cn=Administrator,cn=Users,dc=routehub,dc=local
server-type Microsoft
ldap-login-password cisco123
```

Rate Limiting (Policing)

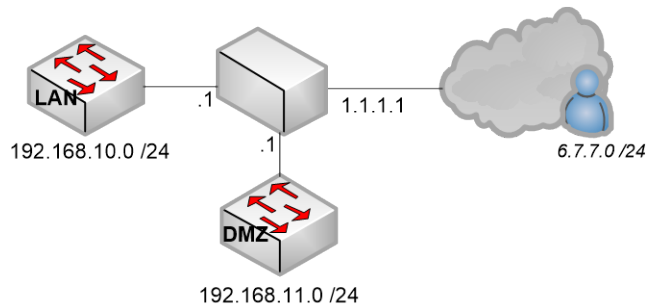
- *Cisco ASA OS 8.3*
- Rate limit all traffic (in/out) of the "outside" interface to 700Kbps

```
policy-map rate-limit-policy
class class-default
  police input 700000 1000
  police output 700000 1000
```

```
service-policy rate-limit-policy interface outside
```

OSPF Routing

- Enable OSPF routing on ASA for the LAN (192.168.10.0) and DMZ (192.168.11.0) networks.
- LAN will exist in Area 0 and the DMZ will exist in Area 11
- Advertise a OSPF default route to other OSPF neighbors using the ASA as the gateway of last resort

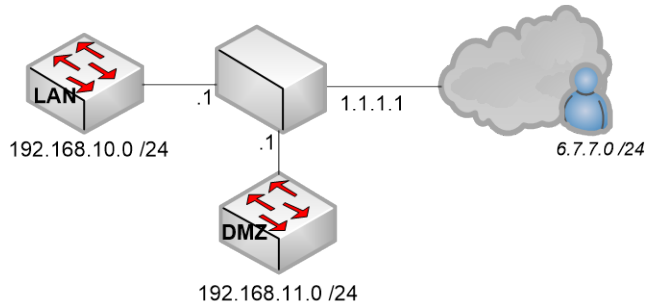


```
router ospf 1
network 192.168.11.0 255.255.255.0 area 11
network 192.168.10.0 255.255.255.0 area 0
log-adj-changes
default-information originate always
```

```
interface Ethernet1
ip address 192.168.10.1 255.255.255.0
nameif inside
ospf hello-interval 1
ospf dead-interval 3
```


EIGRP Routing

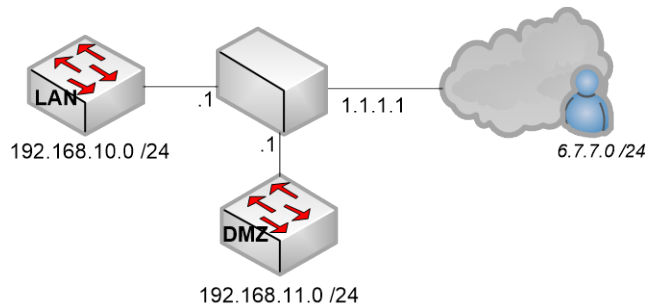
- Enable EIGRP routing on ASA for the LAN (192.168.10.0) and DMZ (192.168.11.0) networks.
- EIGRP ASN 1
- Disable EIGRP communication through Outside and DMZ interfaces. EIGRP neighbor will only be established to router on the LAN.
- Redistribute any configured static routes on the ASA firewall into EIGRP



```
router eigrp 1
no auto-summary
network 192.168.11.0
network 192.168.10.0
passive-interface outside
passive-interface dmz
redistribute static
```

RIPv2 Routing and Authentication

- Enable RIPv2 routing on ASA for the LAN (192.168.10.0) and DMZ (192.168.11.0) networks.
- Configure RIP MD5 Authentication between other RIPv2 routers using the password "cisco123"
- Advertise a RIP default route to other OSPF neighbors using the ASA as the gateway of last resort

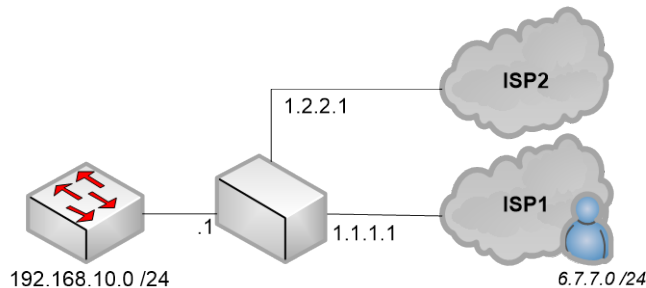


```
interface Ethernet0/1
 nameif RHG-LAN
 security-level 100
 ip address 192.168.10.1 255.255.255.0
 rip authentication mode md5
 rip authentication key cisco123 key_id 1
```

```
router rip
 network 192.168.10.0
 network 192.168.11.0
 passive-interface default
 no passive-interface RHG-LAN
 default-information originate
 version 2
```

IP SLA with Dual ISP

- Configure IP SLA with two connected ISP's for Internet redundancy.
- Primary Internet access through ISP1. Secondary Internet access through ISP2.
- If 1.1.1.2 is not pingable by the ASA then declare ISP1 down and change default route towards ISP2



```
sla monitor 100
type echo protocol iplcmpEcho 1.1.1.2 interface outside-isp1
num-packets 3
frequency 10
```

```
sla monitor schedule 100 life forever start-time now
```

```
track 1 rtr 100 reachability
```

```
route outside-isp1 0.0.0.0 0.0.0.0 1.1.1.2 10 track 1
route outside-isp2 0.0.0.0 0.0.0.0 1.2.2.2 254
```

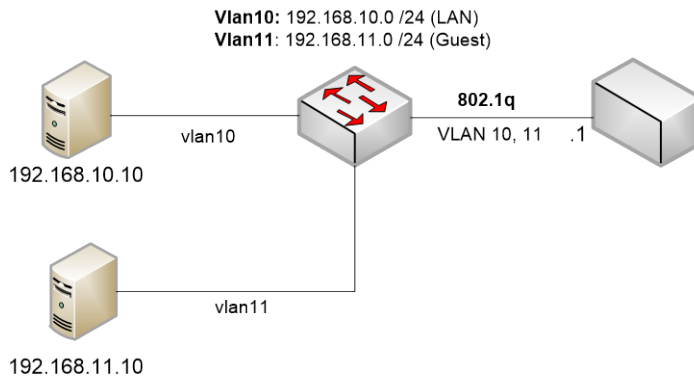
Factory Defaults for ASA 5500

- Putting ASA back to factory defaults
- Completed in the "config mode"
- The ASA will return to factory defaults using the default IP "192.168.1.1"

```
config factory-default
reload save-config noconfirm
```

802.1q (VLAN tagging)

- *Cisco ASA OS 8.3*
- Configure 802.1Q Trunking (VLAN tagging) on physical interface ethernet0/1 for VLAN 10 (192.168.10.0; LAN) and VLAN20 (192.168.11.0; Guest)



```
interface Ethernet0/1
no nameif
no ip address
no shutdown
```

```
interface Ethernet0/1.10
description RHG VLAN LAN
vlan 10
nameif RHG-LAN
security-level 100
ip address 192.168.10.1 255.255.255.0
```

```
interface Ethernet0/1.11
description RHG VLAN GUEST
vlan 11
nameif RHG-GUEST
security-level 50
ip address 192.168.11.1 255.255.255.0
```

DNS Requests

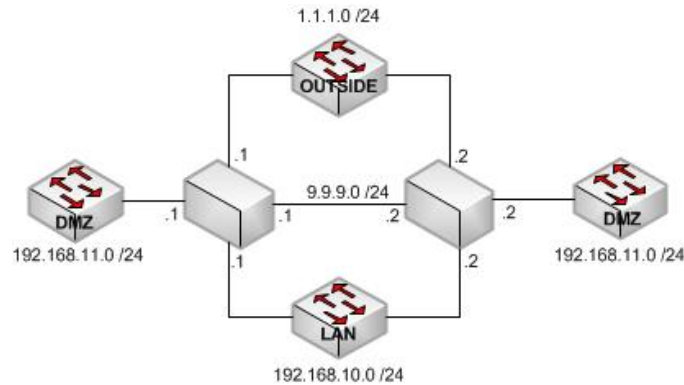
- *Cisco ASA OS 8.3*
- Static NAT will provide the internal IP if accessing this Public IP from the inside network

```
static (inside,outside) 1.1.1.10 192.168.10.10 netmask 255.255.255.255 dns
```

Active/Passive Failover

note

- Configure ASA Active Passive failover providing redundancy for the OUTSIDE (1.1.1.0), LAN (192.168.10.0), and DMZ (192.168.11.0).
- Failover interface for exchanging state and heart-beats will use ethernet0/3 on both firewalls.



>>Primary ASA<<

interface Ethernet0/0

speed 100

duplex full

nameif outside

security-level 0

ip address 1.1.1.1 255.255.255.248 standby 1.1.1.2

interface Ethernet0/1

speed 100

duplex full

nameif inside

security-level 100

ip address 192.168.10.1 255.255.255.0 standby 192.168.10.2

interface Ethernet0/2

speed 100

duplex full

nameif dmz

security-level 60

ip address 192.168.11.1 255.255.255.0 standby 192.168.11.2

interface Ethernet0/3

description LAN/STATE Failover Interface

failover

failover lan unit primary

failover lan interface failover Ethernet0/3

failover link failover Ethernet0/3

failover key cisco6778

failover interface ip failover 9.9.9.1 255.255.255.252 standby 9.9.9.2

failover replication http

failover polltime unit msec 200 holdtime msec 800

failover polltime interface msec 500 holdtime 5

>>Secondary ASA<<

```
failover
failover lan unit secondary
failover lan interface failover Ethernet0/3
failover key cisco6778
failover link failover Ethernet0/3
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover interface ip failover 9.9.9.1 255.255.255.252 standby 9.9.9.2
```

show failover state

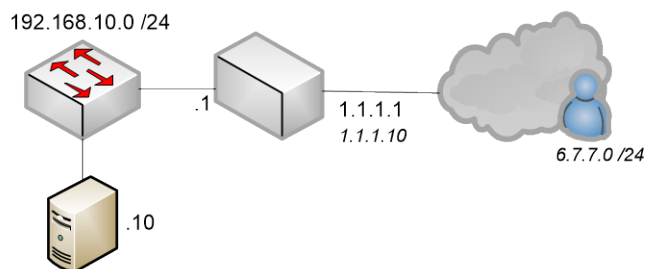
Banner

- Cisco ASA OS 8.3
- Define the ASA banner to display upon login into the firewall

```
banner exec          **WARNING**
banner exec YOU ARE ATTEMPTING TO LOG INTO A PRIVATE SYSTEM.
banner exec          AUTHORIZED USERS ONLY!!
banner exec ALL UNAUTHORIZED USE WILL BE PROSECUTED TO THE
banner exec          FULLEST EXTENT OF THE LAW!!
```

Standard Firewall Policy

- Cisco ASA OS 8.3
- Configure firewall policy to allow any Internet host to access the web server at 1.1.1.10



```
access-list ingress-acl extended permit tcp any host 1.1.1.10 eq 80
access-group ingress-acl in interface outside
```

Standard Firewall Policy using Objects (Hosts)

- *Cisco ASA OS 8.3*
- Add server (1.1.1.10) in an object group called "RHG-SERVERS1"
- Configure group listing TCP and UDP ports for services used on the server (1.1.1.10) such as WWW (TCP/80)
- Configure firewall policy using the object groups for allowing any Internet host to access the web server at 1.1.1.10

```
object-group network RHG-SERVERS1  
network-object host 1.1.1.10
```

```
object-group service RHG-APPS tcp-udp  
port-object eq www
```

```
access-list ingress-acl extended permit tcp any object-group RHG-SERVERS1 object-group RHG-APPS
```

```
access-group ingress-acl in interface outside
```

Standard Firewall Policy using Objects (Network)

- *Cisco ASA OS 8.3*
- Add server network (1.1.1.0) in an object group called "RHG-SERVERS2"
- Configure group listing TCP and UDP ports for services used on the server (1.1.1.10) such as WWW (TCP/80)
- Configure firewall policy using the object groups for allowing any Internet host to access any web service on the 1.1.1.0 network

```
object-group network RHG-SERVERS2  
network-object 1.1.1.0 255.255.255.0
```

```
object-group service RHG-APPS tcp-udp  
port-object eq www
```

```
access-list ingress-acl extended permit tcp any object-group RHG-SERVERS2 object-group RHG-APPS
```

```
access-group ingress-acl in interface outside
```


PAT (NAT Overload) using Outside Interface

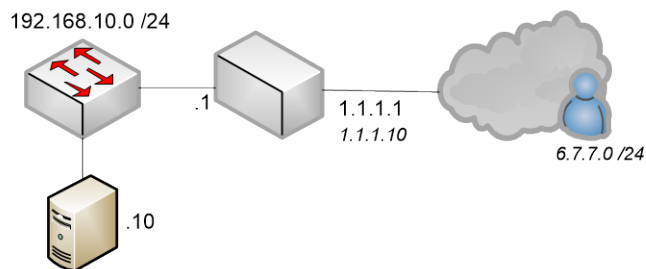
- *Cisco ASA OS 8.3*
- Configure PAT (NAT Overload) using the IP configured on the “outside” interface. Any inside host on the LAN (192.168.10.0) will use the IP on the “outside” interface for Internet access

```
global (outside) 1 interface
```

```
nat (inside) 1 192.168.10.0 255.255.255.0
```

Static NAT

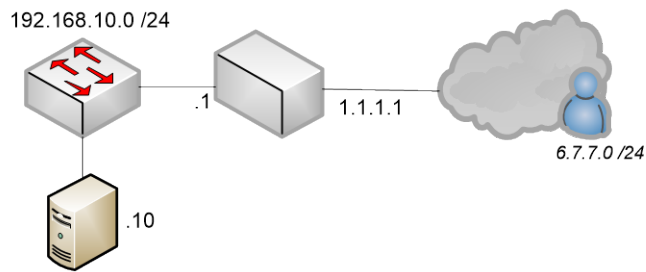
- *Cisco ASA OS 8.3*
- Configure a static translation where the inside host is 192.168.10.10 is mapped to the Public IP of 1.1.1.10



```
static (inside,outside) 1.1.1.10 192.168.10.10 netmask 255.255.255.255
```

NAT Port Redirect: using Outside Interface

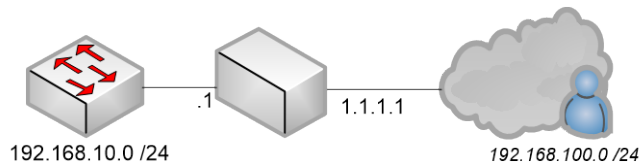
- *Cisco ASA OS 8.3*
- Any access to the IP configured on the “outside” interface for HTTPS (TCP/443) will be redirected to the inside server of 192.168.10.10.



```
static (inside,outside) tcp interface https 192.168.10.10 https netmask 255.255.255.255
```

Remote Access: SSL VPN (Tunnel Mode or SVC) using Local Authentication

- *Cisco ASA OS 8.3*
- Configure Client VPN solution using SSL VPN (Tunnel Mode)
- Specify the SSL VPN client image that can be used on a Windows or Mac system
- The VPN pool for connected users will be 192.168.100.10 – 192.168.100.13
- LAN subnet behind the VPN device is: 192.168.10.0/24
- Enable split tunnel to allow VPN users access to the 192.168.10.0 network over the established VPN tunnel
- VPN user authentication will be local. One of the local user accounts will be "user1"



```
access-list split-tunnel standard permit 192.168.10.0 255.255.255.0
```

```
access-list nonat extended permit ip 192.168.10.0 255.255.255.0 192.168.100.0 255.255.255.0  
nat (inside) 0 access-list nonat
```

```
ip local pool routehub-pool 192.168.100.10-192.168.100.13 mask 255.255.255.0
```

```
webvpn  
enable outside  
svc image disk0:/anyc-win.pkg 1  
svc image disk0:/anyc-mac.pkg 2  
svc enable  
tunnel-group-list enable
```

```
group-policy RHG-GP-SSL internal  
group-policy RHG-GP-SSL attributes  
dns-server value 192.168.10.10  
vpn-tunnel-protocol webvpn  
split-tunnel-policy tunnelspecified  
split-tunnel-network-list value split-tunnel  
default-domain value routehub.local  
webvpn  
svc required  
svc keep-installer installed  
svc rekey time 30  
svc rekey method ssl
```

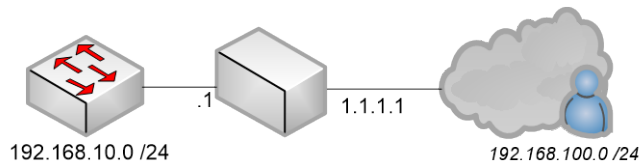
```
username user1 password cisco123
```

```
tunnel-group RHG-TG-SSL type remote-access  
tunnel-group RHG-TG-SSL general-attributes  
address-pool routehub-pool  
default-group-policy RHG-GP-SSL
```

```
tunnel-group RHG-TG-SSL webvpn-attributes  
group-alias ROUTEHUB enable
```

Remote Access: IPsec VPN using RADIUS Authentication

- *Cisco ASA OS 8.3*
- Configure Client VPN solution using IPsec VPN
- The VPN pool for connected users will be 192.168.100.10 – 192.168.100.13
- LAN subnet behind the VPN device is: 192.168.10.0/24
- Enable split tunnel to allow VPN users access to the 192.168.10.0 network over the established VPN tunnel
- VPN user authentication will be using RADIUS (192.168.10.11)
- For the VPN software client: The “Group Authentication” name will be ROUTEHUB and the “Group Authentication Password” will be cisco123



```
access-list split-tunnel standard permit 192.168.10.0 255.255.255.0
```

```
access-list nonat extended permit ip 192.168.10.0 255.255.255.0 192.168.100.0 255.255.255.0  
nat (inside) 0 access-list nonat
```

```
ip local pool routehub-pool 192.168.100.10-192.168.100.13 mask 255.255.255.0
```

```
crypto isakmp nat-traversal 300
```

```
crypto isakmp enable outside  
crypto isakmp policy 30  
authentication pre-share  
encryption 3des  
hash md5  
group 2  
lifetime 86400
```

```
crypto ipsec transform-set RHG-TS-3DES-MD5 esp-3des esp-md5-hmac
```

```
crypto dynamic-map RHG-DMAP-VPN 10 set transform-set RHG-TS-3DES-MD5  
crypto map RHG-VPN 65535 ipsec-isakmp dynamic RHG-DMAP-VPN  
crypto map RHG-VPN interface outside
```

```
group-policy RHG-GP-VPN internal  
group-policy RHG-GP-VPN attributes  
dns-server value 192.168.10.10 4.2.2.2  
vpn-idle-timeout 30  
vpn-session-timeout 480  
split-tunnel-policy tunnelspecified  
split-tunnel-network-list value split-tunnel  
default-domain value routehub.local
```

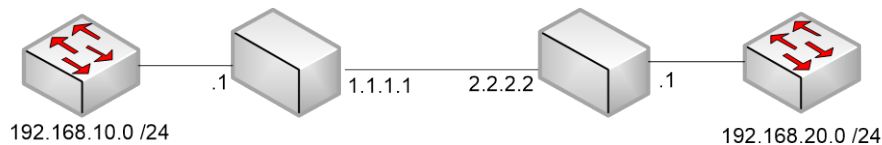
```
aaa-server RADIUS protocol radius  
aaa-server IAS protocol radius  
aaa-server IAS host 192.168.10.11  
timeout 5  
key cisco123
```

```
tunnel-group ROUTEHUB type remote-access
tunnel-group ROUTEHUB general-attributes
address-pool routehub-pool
authentication-server-group IAS
default-group-policy RHG-GP-VPN
```

```
tunnel-group ROUTEHUB ipsec-attributes
pre-shared-key cisco123
```

Site-Based VPN (ASA-to-ASA)

- Cisco ASA OS 8.3
- Configure IPSec VPN tunnel between two Cisco ASA Firewalls
- Site #1: WAN IP is 1.1.1.1. The LAN subnet is 192.168.10.0
- Site #2: WAN IP is 2.2.2.2. The LAN subnet is 192.168.20.0
- Disable NAT for routing between the two LAN subnets across the VPN
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- The VPN shared key will be "cisco123"
- Enable VPN on outside" interface



>>Site #1<<

```
interface Ethernet0/0
ip address 1.1.1.1 255.255.255.252
speed 100
duplex full
nameif outside

interface Ethernet0/1
ip address 192.168.10.1 255.255.255.0
speed 100
duplex full
nameif inside
```

```
access-list ACL-NONAT extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
nat (inside) 0 access-list ACL-NONAT
```

```
crypto isakmp identity address
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 86400
```

```
crypto ipsec transform-set RHG-TS-ESP-MD5 esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
```

```
access-list RHG-ACL-VPN extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
```

```
crypto map vpn 10 match address RHG-ACL-VPN
crypto map vpn 10 set pfs
crypto map vpn 10 set peer 2.2.2.2
crypto map vpn 10 set transform-set RHG-TS-ESP-MD5
crypto map vpn interface outside
```

```
tunnel-group 2.2.2.2 type ipsec-l2l
tunnel-group 2.2.2.2 ipsec-attributes
pre-shared-key cisco123
```

>>Site #2<<

```
interface Ethernet0/0
ip address 2.2.2.2 255.255.255.252
speed 100
duplex full
nameif outside
```

```
interface Ethernet0/1
ip address 192.168.20.1 255.255.255.0
speed 100
duplex full
nameif inside
```

```
access-list ACL-NONAT extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0 255.255.255.0
nat (inside) 0 access-list ACL-NONAT
```

```
crypto isakmp identity address
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 86400
```

```
crypto ipsec transform-set RHG-TS-ESP-MD5 esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
```

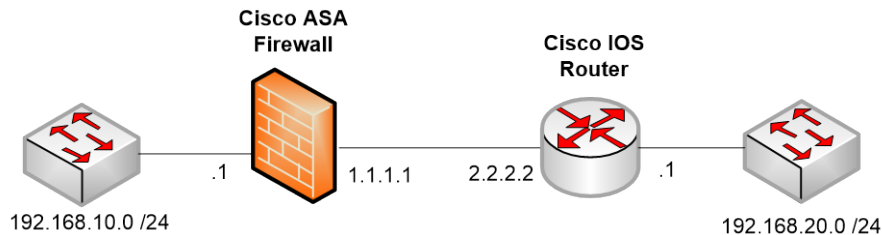
```
access-list RHG-ACL-VPN extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0 255.255.255.0
```

```
crypto map vpn 10 match address RHG-ACL-VPN
crypto map vpn 10 set pfs
crypto map vpn 10 set peer 1.1.1.1
crypto map vpn 10 set transform-set RHG-TS-ESP-MD5
crypto map vpn interface outside
```

```
tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 ipsec-attributes
pre-shared-key cisco123
```

Site-Based VPN (ASA to Cisco IOS)

- *Cisco ASA OS 8.3*
- Configure IPSec VPN tunnel between a Cisco ASA Firewall & a Cisco IOS router
- Site #1: WAN IP is 1.1.1.1. The LAN subnet is 192.168.10.0
- Site #2: WAN IP is 2.2.2.2. The LAN subnet is 192.168.20.0
- Disable NAT for routing between the two LAN subnets across the VPN
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- The VPN shared key will be "cisco123"
- Enable VPN on outside" interface



>>Site #1 (Cisco ASA)<<

```
interface Ethernet0/0
ip address 1.1.1.1 255.255.255.252
speed 100
duplex full
nameif outside

interface Ethernet0/1
ip address 192.168.10.1 255.255.255.0
speed 100
duplex full
nameif inside
```

```
access-list ACL-NONAT extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
nat (inside) 0 access-list ACL-NONAT
```

```
crypto isakmp identity address
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 86400
```

```
crypto ipsec transform-set RHG-TS-ESP-MD5 esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
```

```
access-list RHG-ACL-VPN extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
```



```
crypto map vpn 10 match address RHG-ACL-VPN
crypto map vpn 10 set pfs group2
crypto map vpn 10 set peer 2.2.2.2
crypto map vpn 10 set transform-set RHG-TS-ESP-MD5
crypto map vpn interface outside
```

```
tunnel-group 2.2.2.2 type ipsec-l2l
tunnel-group 2.2.2.2 ipsec-attributes
pre-shared-key cisco123
```

>>Site #2 (Cisco IOS Router)<<

```
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
```

```
crypto isakmp key ciscokey address 1.1.1.1
```

```
crypto ipsec transform-set ipsec-ts esp-3des esp-md5-hmac
```

```
access-list 112 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
crypto map VPN 10 ipsec-isakmp
  set peer 1.1.1.1
  set transform-set ipsec-ts
  set pfs group2
  match address 112
```

```
access-list 110 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 permit ip 192.168.20.0 0.0.0.255 any
```

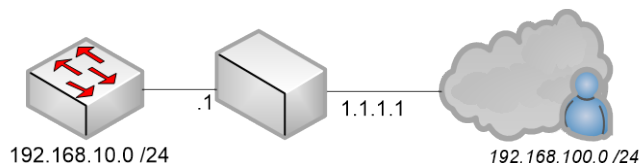
```
ip nat inside source list 110 pool NATPOOL overload
```

```
interface FastEthernet0/1
  description LAN interface
  ip address 192.168.20.1 255.255.255.0
```

```
interface FastEthernet0/0
  description WAN interface
  ip address 2.2.2.2 255.255.255.0
  crypto map vpn
```

Remote Access: L2TP over IPSec using RADIUS Authentication

- *Cisco ASA OS 8.3*
- Configure Client VPN solution using L2TP over IPSec VPN
- The VPN pool for connected users will be 192.168.100.10 – 192.168.100.13
- LAN subnet behind the VPN device is: 192.168.10.0/24
- VPN users should have access to the 192.168.10.0 network over the established VPN tunnel
- VPN user authentication will be using RADIUS (192.168.10.10)
- The L2TP secret (configured on client) will be cisco123



```
access-list nonat extended permit ip 192.168.10.0 255.255.255.0 192.168.100.0 255.255.255.0
nat (inside) 0 access-list nonat
```

```
ip local pool routehub-pool 192.168.100.10-192.168.100.13 mask 255.255.255.0
```

```
aaa-server RADIUS protocol radius
aaa-server IAS protocol radius
aaa-server IAS host 192.168.10.10
timeout 5
key cisco123
```

```
crypto ipsec transform-set 3desmd5 esp-3des esp-md5-hmac
crypto ipsec transform-set 3desmd5 mode transport
crypto ipsec transform-set aes128sha esp-aes esp-sha-hmac
crypto ipsec transform-set aes128sha mode transport
crypto ipsec transform-set aes256sha esp-aes-256 esp-sha-hmac
crypto ipsec transform-set aes256sha mode transport
```

```
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map RHG-DMAP-VPN 10 set transform-set 3desmd5 aes128sha aes256sha
crypto map RHG-VPN 65000 ipsec-isakmp dynamic RHG-DMAP-VPN
crypto map RHG-VPN interface outside
```

```
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 86400
```

```
crypto isakmp policy 65535
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

```
crypto isakmp enable outside
crypto isakmp identity address
```

```
group-policy DefaultRAGroup internal
group-policy DefaultRAGroup attributes
  dns-server value 192.168.10.10
  vpn-tunnel-protocol IPSec l2tp-ipsec
```

```
tunnel-group DefaultRAGroup general-attributes
  address-pool routehub-pool
  authentication-server-group IAS
  default-group-policy DefaultRAGroup
```

```
tunnel-group DefaultRAGroup ipsec-attributes
  pre-shared-key Cisco123
```

```
tunnel-group DefaultRAGroup ppp-attributes
  no authentication chap
  authentication ms-chap-v2
```

```
show vpn-sessiondb summary
show vpn-sessiondb l2l
show vpn-sessiondb remote
show vpn-sessiondb full remote
show vpn-sessiondb
show vpn-sessiondb svc
```

IPSec over TCP

- Enable IPSec over TCP using port number 10,000

```
crypto isakmp ipsec-over-tcp port 10000
```

Packet Capture

- Capture all IP traffic between hosts 192.168.10.10 and 6.7.7.8 (through inside interface)

```
ASA(config)# access-list INET permit ip host 192.168.10.10 host 6.7.7.8
```

```
ASA(config)# access-list INET permit ip host 6.7.7.8 host 192.168.10.10
```

```
ASA# capture inside access-list INET interface inside
```

```
ASA# show capture
```

VPN Monitoring

```
show isa sa
```

```
show crypto ipsec sa
```

```
show isakmp ipsec-over-tcp stats
```

```
show isakmp stats
```

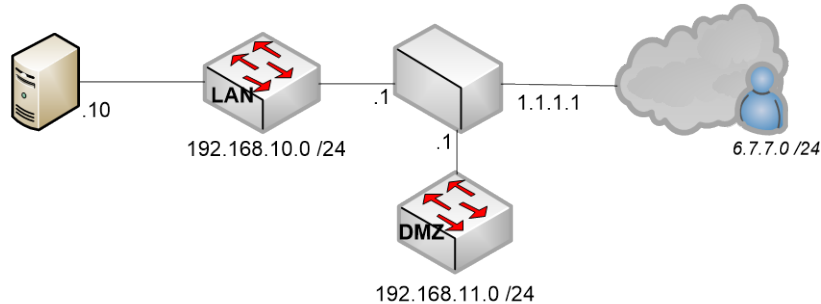
```
show isakmp ipsec stats
```

```
show crypto protocol statistics ipsec
```

```
show crypto accelerator statistics
```

IPS using the Security Module

- Inspect traffic from the LAN (192.168.10.0) and DMZ (192.168.11.0) networks
- Enable Promiscuous monitoring and permit all traffic if the IPS service module fails (fail-open)



```
access-list RHG-ACL-IPS-LAN extended permit ip 192.168.10.0 255.255.255.0 any
access-list RHG-ACL-IPS-DMZ extended permit ip 192.168.11.0 255.255.255.0 any
```

```
class-map RHG-CMAP-IPS-LAN
match access-list RHG-ACL-IPS-LAN
```

```
class-map RHG-CMAP-IPS-DMZ
match access-list RHG-ACL-IPS-DMZ
```

```
policy-map RHG-POL-IPS-LAN
class RHG-CMAP-IPS-LAN
ips promiscuous fail-open sensor vs0
```

```
policy-map RHG-POL-IPS-DMZ
class RHG-CMAP-IPS-DMZ
ips promiscuous fail-open sensor vs0
```

```
service-policy RHG-POL-IPS-LAN interface inside
service-policy RHG-POL-IPS-DMZ interface dmz
```

Application Inspection: Using PPTP

- *Cisco ASA OS 8.3*
- Update Application Inspection list to inspect PPTP

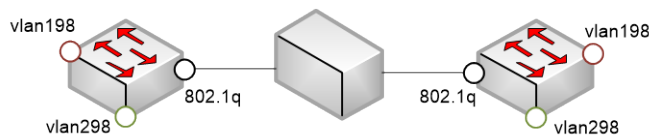
```
class-map ROUTEHUB-CLASS-VPDN  
match port tcp eq pptp
```

```
policy-map global_policy  
class ROUTEHUB-CLASS-VPDN  
inspect pptp
```

```
service-policy global_policy global
```

Virtualization: Configuration to Support Virtual Firewalls

- Enable Cisco ASA firewall to operate in L2 mode ("firewall transparent")
- Add two new virtual firewall instances. One for Client 1 (CL1-FW) and another for Client 2 (CL2-FW)
- Client 1 Virtual Firewall will use interfaces GE0.198 (for the outside) and GE1.198 (for the inside)
- Client 1 Virtual Firewall will use interfaces GE0.298 (for the outside) and GE1.298 (for the inside)



```
mode multiple  
firewall transparent
```

```
interface gigabitethernet 0.198  
no shutdown
```

```
interface gigabitethernet 1.198  
no shutdown
```

```
context CL1-FW  
allocate-interface gigabitethernet 0.198  
allocate-interface gigabitethernet 1.198  
configure disk0://CL1-FW.cfg
```

```
interface gigabitethernet 0.298  
no shutdown  
interface gigabitethernet 1.298  
no shutdown
```

```
context CL2-FW  
allocate-interface gigabitethernet 0.298  
allocate-interface gigabitethernet 1.298  
configure disk0://CL2-FW.cfg
```

Virtualization: Accessing a Virtual Firewall Instance

- To access one of virtual firewalls type in "context" followed by the context name.
- In this example we will access the CL1-FW instance
- Client 1 Virtual Firewall will use interfaces GE0.198 (for the outside) and GE1.198 (for the inside) allocated on the main firewall including other firewall configuration like firewall policies

context CL1-FW

hostname CL1-FW
domain c1.routehub.local

passwd cisco123
enable password cisco123

interface gigabitethernet 0.198
nameif outside
security-level 0
no shutdown

interface gigabitethernet 1.198
nameif inside
security-level 100
no shutdown

access-list CL1-ACL extended permit 89 any any
access-list CL1-ACL extended permit tcp any host 192.168.10.10 eq 8080
access-list CL1-ACL extended permit tcp any host 192.168.10.11 eq 22
access-list CL1-ACL extended permit tcp any host 192.168.10.12 eq 3389

access-group CL1-ACL in interface outside

Troubleshooting: Proxy ARP

- *Cisco ASA OS 8.3*
- Disable Proxy-ARP functions on inside interface (recommended)

```
sysopt noproxyarp inside
```

Troubleshooting: Allow Polycom Video Conferencing

- *Cisco ASA OS 8.3*
- Update Application Inspection list to inspect all H.323 traffic to allow Polycom Video Conferencing through firewall

```
policy-map global_policy  
class inspection_default  
inspect h323 h225  
inspect h323 ras
```

```
service-policy global_policy global
```


CISCO CATALYST 3750 SERIES

Solution/Services: Cisco Catalyst 3750

Related: N/A

Stack Master

- Global command to force a Cisco Catalyst 3750 as the Stack Master switch
- Higher the priority value = the more preferred switch to be the Stack Master in the stack

`switch [switch number] priority 15`

`show switch stack-ports`
`show switch`

Re-number the switch number

- Change the current switch number to be switch #2

`switch [switch number] renumber 2`

Stack MAC address Persistent

- 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

`stack-mac persistent timer 0`

CISCO CATALYST 4500 SERIES

Solution/Services: Cisco Catalyst 4500
Related: N/A

Power Supply Redundancy

- Makes one of the power supplies active while the other is a backup

power redundancy-mode redundant

Supervisor Redundancy: Stateful Switchover (SSO)

- *Must have two Supervisor Engines installed*
- Enables Supervisor Engine Redundancy

redundancy
main-cpu
auto-sync startup-config
auto-sync bootvar
auto-sync standard
mode sso

show redundancy states

! reloads standby supervisor engine and brings it back on-line
redundancy reload peer

! force the standby supervisor engine in the chassis to be active
redundancy force-switchover

Supervisor Redundancy: RPR

- *Must have two Supervisor Engines installed*
- Enables Supervisor Engine Redundancy in RPR mode. Recommended to use SSO.

```
redundancy
mode rpr
```

Quality of Service (QoS)

- Enable QoS on Cisco Catalyst 4500 Series

```
qos
qos dbf
qos dbf exceed-action ecn
qos map dscp 0 to tx-queue 2
qos map dscp 16 18 20 22 24 25 26 32 to tx-queue 4
qos map dscp 34 36 38 to tx-queue 4
```

```
policy-map DBL
class class-default
dbf
```

```
interface GigabitEthernet2/1
qos trust dscp
service-policy input DBL
```

```
interface GigabitEthernet6/14
qos trust dscp
tx-queue 1
bandwidth percent 5
tx-queue 2
bandwidth percent 25
tx-queue 3
bandwidth percent 30
priority high
shape percent 30
tx-queue 4
bandwidth percent 40
service-policy output DBL
```

CISCO CATALYST 6500 SERIES

Solution/Services: Cisco Catalyst 6500 Series

Related: N/A

Power Supply: Redundancy

- Make one of the power supplies active while the other is a backup

power redundancy-mode redundant

Power Supply: Combined

- Combined both power supplies to power the line modules if additional power is needed.
- Using combined mode is not recommended due to lack of redundancy. If one of the power supplies fail then one or more of the line modules may not be available. Redundant mode is therefore recommended.

power redundancy-mode combined

Supervisor Redundancy: Stateful Switchover (SSO)

- *Must have two Supervisor Engines installed*
- *Enabling SSO will automatically enable CEF NSF*
- Enables Supervisor Engine Redundancy

redundancy
mode sso
main-cpu
auto-sync startup-config
auto-sync running-config
auto-sync bootvar
auto-sync standard

show redundancy states
show cef state

System Switchover

- Failover to other available Supervisor Engine

redundancy force-switchover

Non-Stop Forwarding (NSF)

- *Enable SSO first on Supervisor Engine*
- Enables NSF under the routing protocol(s) that is configured

```
>> BGP <<
router bgp 6778
bgp graceful-restart
```

```
>> OSPF <<
router ospf 1
nsf
```

```
>> EIGRP <<
router eigrp 1
nsf
```

ACL Merge Tuning & Configuration

- Order Dependent Merge (ODM) – recommended

```
mls aclmerge algorithm odm
mls aclmerge odm opti
```

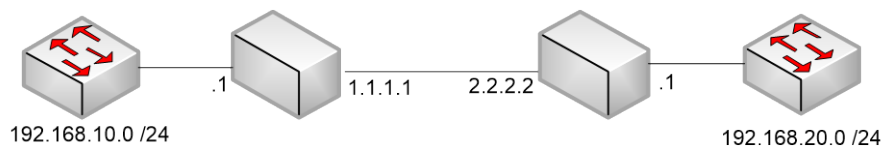
- Order Independent Merge (OIM)

```
mls aclmerge algorithm bdd
```

```
show tcam counts (on Native)
show security acl resource-usage (for Hybrid OS)
show fm summary
```

Service Module: FlexVPN Module (DS3) and IPsec VPN Module

- Service Module: FlexVPN with DS3 module (in slot 1), IPsec VPN module (in slot 2)
- ATM PVC 1/101
- Configure IPsec VPN tunnel between two Cisco Catalyst 6500 switches
- Site #1: WAN IP is 1.1.1.1. The LAN subnet is 192.168.10.0
- Site #2: WAN IP is 2.2.2.2. The LAN subnet is 192.168.20.0
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- The VPN shared key will be "cisco123"
- Enable VPN on WAN facing interface



>> SITE1 <<

```
crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
```

```
crypto isakmp key cisco123 address 2.2.2.2
```

```
crypto ipsec transform-set VPN-TS esp-3des esp-sha-hmac
```

```
ip access-list extended VPN-ACL
permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
crypto map VPN-MAP 10 ipsec-isakmp
set peer 2.2.2.2
set transform-set VPN-TS
set pfs group2
match address VPN-ACL
```

```
interface ATM1/0/0
no ip address
ip route-cache flow
load-interval 60
atm clock INTERNAL
```

```
interface ATM1/0/0.250 point-to-point
crypto connect vlan 250
pvc 1/101
```

```
interface Vlan250
ip address 1.1.1.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
crypto map VPN-MAP
crypto engine slot 2
```

>> SITE2 <<

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
```

```
crypto isakmp key cisco123 address 1.1.1.1
```

```
crypto ipsec transform-set VPN-TS esp-3des esp-sha-hmac
```

```
ip access-list extended VPN-ACL
  permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
crypto map VPN-MAP 10 ipsec-isakmp
  set peer 1.1.1.1
  set transform-set VPN-TS
  set pfs group2
  match address VPN-ACL
```

```
interface ATM1/0/0
  no ip address
  ip route-cache flow
  load-interval 60
  atm clock INTERNAL
```

```
interface ATM1/0/0.250 point-to-point
  crypto connect vlan 250
  pvc 1/101
```

```
interface Vlan250
  ip address 2.2.2.2 255.255.255.0
  no ip redirects
  no ip unreachable
  no ip proxy-arp
  crypto map VPN-MAP
  crypto engine slot 2
```

Monitor Commands:

```
show crypto vlan
show crypto ipsec sa
show crypto isakmp sa
show crypto sessions
show crypto engine connections active
show interface gigabitethernet <module>/1
show interface gigabitethernet <module>/2
```

Monitoring the Fabric Status

- Shows line module speed, fabric status, hotstandby support, and other details

show fabric status

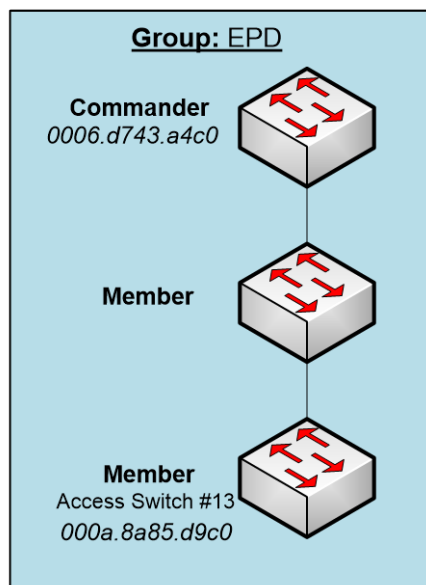
CISCO CATALYST XL SERIES

Solution/Services: Cisco Catalyst 2900/3500 XL Switches

Related: N/A

Cisco Catalyst XL Clustering

- When using the stack feature among a group of Cisco Catalyst XL series switches there is a single CONTROLLER switch which controls the stack.
- The Commander switch has MAC address 0006.d743.a4c0
- The group name for the cluster will be called "EPD"
- The Commander switch will list all Member switches using that switches MAC address



COMMANDER:

```
cluster enable epd 0
cluster member 1 mac-address 0006.53c5.2440
cluster member 2 mac-address 0006.d743.89c0
cluster member 3 mac-address 000b.5f76.ef80
cluster member 4 mac-address 0006.53c5.1d00
cluster member 5 mac-address 0006.53c4.cb40
cluster member 6 mac-address 0006.28d4.2f40
cluster member 7 mac-address 0005.dd40.4540
cluster member 8 mac-address 0006.53c5.2340
cluster member 9 mac-address 0005.dd44.d740
cluster member 10 mac-address 0006.d7a4.a980
cluster member 11 mac-address 0009.4493.2f00
```

```
cluster member 12 mac-address 0009.b751.6e8
cluster member 13 mac-address 000a.8a85.d9c0
```

- On Access switch #13, within the cluster, define the MAC address of the Commander switch and the cluster name "EPD". Also define the member # that the switch will use

MEMBER:

```
cluster commander-address 0006.d743.a4c0 member 13 name epd
```

- From the COMMANDER switch, if we want to connect into Access Switch 13 within the cluster we would type in the following:

```
rcommand 13
```

- Show command to view all members in the cluster

```
switch_commander#show cluster members
```

```
      |---Upstream---|
SN MAC Address  Name      Portlf FEC Hops  SN Portlf FEC State
0 0006.d743.a4c0 b5475r1271gb      0      Up (Cmdr)
1 0006.53c5.2440 b5475SierraR      255      Up
2 0006.d743.89c0 b5475r1271gb      1      Down
3 000b.5f76.ef80 Switch    Gi0/1      1 0 Gi0/1      Down
4 0006.53c5.1d00 b5475r1328tx Gi0/1      1 0 Gi0/3      Up
5 0006.53c4.cb40 b5475r1348tx Gi0/1      1 0 Gi0/6      Up
6 0006.28d4.2f40 b5426r100      1      Down
7 0005.dd40.4540 b5475r1305      255      Up
8 0006.53c5.2340 b5475r1222      255      Up
9 0005.dd44.d740 b5425r100      2      Down
10 0006.d7a4.a980 b5475r1151 Gi0/2      1 0 Gi0/4      Up
11 0009.4493.2f00 b5475r1328cg      2      Down
12 0009.b751.6e80 b5475r1328cg      2      Down
```

CISCO GSR SERIES

Solution/Services: Cisco GSR Series

Related: N/A

Reloading a Cisco GSR Module

```
hw-module slot x reload  
diag x {verbose}
```

CISCO IP PHONES

Solution/Services: Cisco IP Phones, Voice & Unified Communications
Related: N/A

Unlocking the Configuration on a Cisco IP 7900 Series Phone

****#** (under Settings button)

Or go to "Settings" scroll down to "Unlock Config" (if applicable). Password (default): cisco

CNF file for SIP Phones

- You can configure the SIP details using either the config file (CNF) as shown below in the example or through the config menu on the phone.
- Phone system IP: 192.168.10.3
- SIP Username: 6778
- SIP password: 1234
- Extension: 6778

#Proxy Server

proxy1_address: "192.168.10.3"

#Line 1 Settings

line1_name: "6778"

line1_shortcode: "6778"

line1_displayname: "6778"

line1_authname: "6778"

line1_password: "1234" ; SIP password for user

CISCO NEXUS SERIES

Solution/Services: Cisco Nexus, Data Center
Related: N/A

L2 Interface

- Configures L2 interface

```
interface e1/1
switchport
switchport access vlan 10
switchport mode access
```

L3 Interface

- Configures L3 interface

```
interface e1/1
no switchport
ip address 10.1.1.1/24
```

Saving Configuration

- To save the configuration on NX-OS

```
copy running-config startup-config
```

Alias

- Create an alias called "wrmem" that will save the configuration.

```
cli alias name wrmem copy run start
```

10GE: Dedicated Mode

- Dedicate 10GE for port e1/1, but disable ports 3, 5, & 7 on slot 1

```
interface e1/1  
rate-mode dedicated
```

Install License

- Install license on Nexus located in bootflash

```
install license bootflash:license_file.lic
```

Specify a Range of Interfaces

- Add ports 10 to 48 on slot 2 to VLAN10 and enable them as "access" ports

```
interface e2/10-48  
switchport  
switchport access vlan 10  
switchport mode access
```

VLAN (L2) and VTP

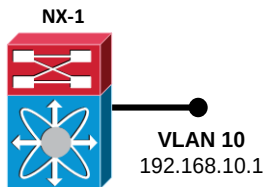
- Enable VTP. Disabled by default
- Add VLAN 10 to Nexus switch's VLAN Database

```
feature vtp
```

```
vlan 10  
name RHG-VLAN-DC1
```

VLAN SVI (L3)

- Enable VLAN L3 support
- Configures VLAN SVI (L3) interface for VLAN10 using 192.168.10.1/24

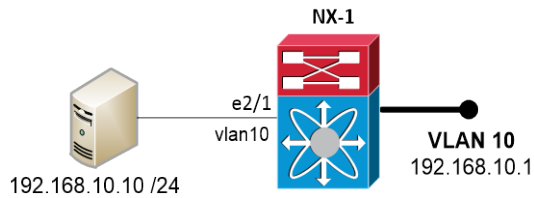


```
feature interface-vlan
```

```
interface Vlan10  
ip address 192.168.10.1/24
```

Access/Edge Port

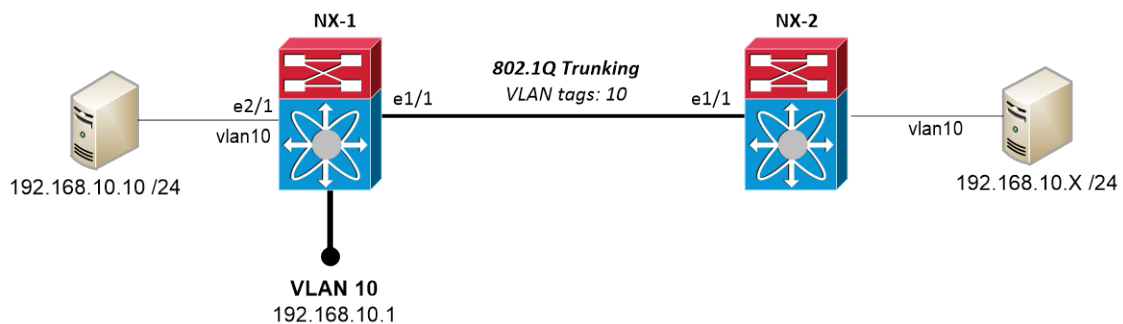
- Put port e2/1 into VLAN10 and enable as an "access" port



```
interface e2/1
switchport
switchport access vlan 10
switchport mode access
```

802.1q (Trunking) Port

- Configure 802.1Q trunking between NX-1 and NX-2
- Tag VLANs: 10
- Native VLAN (untagged): 999



```
interface e1/1
switchport
switchport trunk native vlan 999
switchport trunk allowed vlan 10
switchport mode trunk
```


Spanning Tree: Root Bridge

- Configure NX-1 to be the Primary Root Bridge for VLANs 10 and 11
- Configure NX-2 to be the Secondary Root Bridge for VLANs 10 and 11

>> NX-1 <<

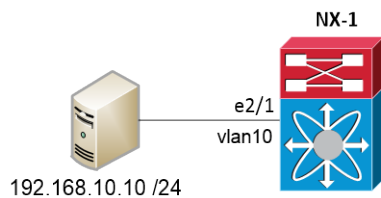
```
spanning-tree vlan 10-11 priority 8192
```

>> NX-2 <<

```
spanning-tree vlan 10-11 priority 16384
```

Spanning Tree: Port Type (Edge)

- Specify interface e2/1 as an edge port intended for host devices (e.g. desktop, servers)



interface e2/1

```
spanning-tree port type edge
```

BPDU Guard

- Enable BPDUGuard globally for all edge ports

```
spanning-tree port type edge bpduguard default
```

Storm Control

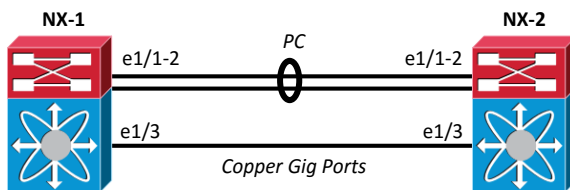
- Restricts no more than 20% of e1/1 interface's bandwidth for broadcast traffic

interface ethernet1/1

storm-control broadcast level 20

UDLD

- Enable UDLD
- Configure UDLD aggressive for port channeling ports between switches (e1/1-2)
- Configure UDLD normal for Copper ports between switches (e1/3)



>> NX-1 <<

feature udld

interface e1/1-2

udld aggressive

interface e1/3

udld enable

MAC Aging

- Configures the global aging time for MAC addresses on the Nexus switch

mac address-table aging-time 120

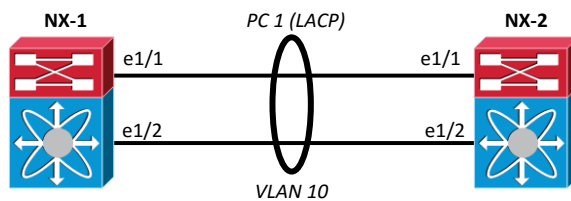
Static MAC Entry

- Configures a static entry for the MAC address, switch port, and VLAN it should be mapped to

```
mac address-table static 1234.5678.9ABC vlan 10 interface ethernet 1/10
```

L2 Port Channel

- Configures L2 LACP Port Channel between NX-1 and NX-2 extending only VLAN10



```
>> NX-1 <<
```

```
feature lacp
```

```
interface e1/1-2
```

```
switchport
```

```
channel-group 1 mode active
```

```
interface port-channel 1
```

```
switchport
```

```
switchport trunk native vlan 999
```

```
switchport trunk allowed vlan 10
```

```
switchport mode trunk
```

```
>> NX-2 <<
```

```
feature lacp
```

```
interface e1/1-2
```

```
switchport
```

```
channel-group 1 mode active
```

```
interface port-channel 1
```

```
switchport
```

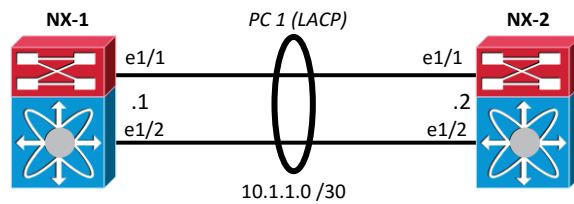
```
switchport trunk native vlan 999
```

```
switchport trunk allowed vlan 10
```

```
switchport mode trunk
```

L3 Port Channel

- Configures L3 LACP Port Channel between NX-1 and NX-2



>> NX-1 <<

feature lACP

interface e1/1-2

no switchport

channel-group 1

interface port-channel 1

ip address 10.1.1.1 255.255.255.252

>> NX-2 <<

feature lACP

interface e1/1-2

no switchport

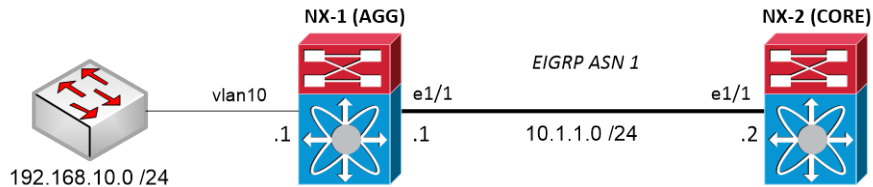
channel-group 1

interface port-channel 1

ip address 10.1.1.2 255.255.255.252

EIGRP

- Enable EIGRP in network topology (see diagram) in ASN 1
- Configure MD5 Authentication
- Configure Route Control (prefix-list) specifying what routes should be advertised and received



>> NX-1 (AGG) <<

```
feature eigrp
```

```
key chain SEIGRP
```

```
key 1
```

```
key-string Cisco123
```

```
ip prefix-list PL-EIGRP-OUT seq 10 permit 10.1.1.0/24
```

```
ip prefix-list PL-EIGRP-OUT seq 11 permit 192.168.0.0/16
```

```
ip prefix-list PL-EIGRP-IN seq 10 permit 0.0.0.0/0
```

```
interface e1/1
```

```
no switchport
```

```
ip address 10.1.1.1/24
```

```
ip router eigrp 1
```

```
ip authentication mode eigrp 1 md5
```

```
ip authentication key-chain eigrp 1 SEIGRP
```

```
ip distribute-list eigrp 1 prefix-list PL-EIGRP-OUT out
```

```
ip distribute-list eigrp 1 prefix-list PL-EIGRP-IN in
```

```
ip summary-address eigrp 1 192.168.0.0/16
```

```
interface Vlan10
```

```
ip address 192.168.10.1/24
```

```
ip router eigrp 1
```

```
ip passive-interface eigrp 1
```

```
router eigrp 1
```

```
address-family ipv4 unicast
```

```
graceful-restart
```

```
timers nsf converge 180
```

```
timers nsf route-hold 200
```

```
>> NX-2 (CORE) <<
```

```
feature eigrp
```

```
key chain SEIGRP
```

```
key 1
```

```
key-string Cisco123
```

```
ip prefix-list PL-EIGRP-OUT seq 10 permit 0.0.0.0/0
```

```
ip prefix-list PL-EIGRP-IN seq 10 permit 10.1.1.0/24
```

```
ip prefix-list PL-EIGRP-IN seq 11 permit 192.168.0.0/16
```

```
interface e1/1
```

```
no switchport
```

```
ip address 10.1.1.1/24
```

```
ip router eigrp 1
```

```
ip authentication mode eigrp 1 md5
```

```
ip authentication key-chain eigrp 1 SEIGRP
```

```
ip distribute-list eigrp 1 prefix-list PL-EIGRP-OUT out
```

```
ip distribute-list eigrp 1 prefix-list PL-EIGRP-IN in
```

```
router eigrp 1
```

```
address-family ipv4 unicast
```

```
graceful-restart
```

```
timers nsf converge 180
```

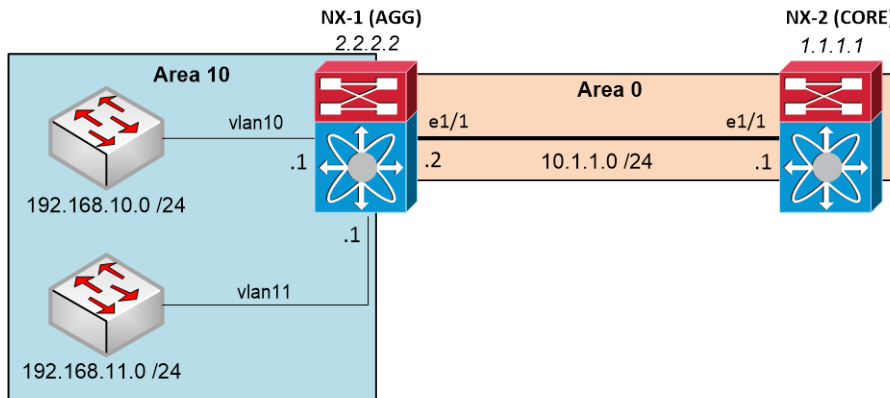
```
timers nsf route-hold 200
```

```
show ip route
```

```
show ip eigrp neighbors
```

OSPF

- Enable OSPF in network topology based on the Areas in the diagram (see below)
- Configure MD5 Authentication
- Configure Route Control (prefix-list) specifying what routes should be advertised and received
- Configure Area 10 as a Totally Stub Area
- Configure Route Summarization for 192.168.0.0/16 on NX-1 towards the Nexus Core Switch



>> NX-1 (AGG) <<

```
feature ospf
```

```
interface loopback0
```

```
ip address 2.2.2.2/32
```

```
ip prefix-list PL-OSPF-OUT seq 10 permit 10.1.1.0/24
```

```
ip prefix-list PL-OSPF-OUT seq 11 permit 192.168.0.0/16
```

```
ip prefix-list PL-OSPF-IN seq 10 permit 0.0.0.0/0
```

```
router ospf 2
```

```
router-id 2.2.2.2
```

```
log-adjacency-changes
```

```
auto-cost reference-bandwidth 100000
```

```
area 0 authentication message-digest
```

```
area 10 stub no-summary
```

```
area 10 range 192.168.0.0/16
```

```
interface e1/1
```

```
no switchport
```

```
ip address 10.1.1.2/24
```

```
ip router ospf 2 area 0
```

```
ip ospf authentication message-digest
```

```
ip ospf message-digest-key 1 md5 0 Cisco123
```

```
ip distribute-list ospf 2 prefix-list PL-OSPF-OUT out
```

```
ip distribute-list ospf 2 prefix-list PL-OSPF-IN in
```

```
interface Vlan10
ip address 192.168.10.1/24
ip router ospf 2 area 10
ip ospf passive-interface
```

```
interface Vlan11
ip address 192.168.11.1/24
ip router ospf 2 area 10
ip ospf passive-interface
```

```
>> NX-2 (CORE) <<
feature ospf
```

```
interface loopback0
ip address 1.1.1.1/32
```

```
ip prefix-list PL-OSPF-OUT seq 10 permit 0.0.0.0/0
```

```
ip prefix-list PL-OSPF-IN seq 10 permit 10.1.1.0/24
```

```
ip prefix-list PL-OSPF-IN seq 11 permit 192.168.0.0/16
```

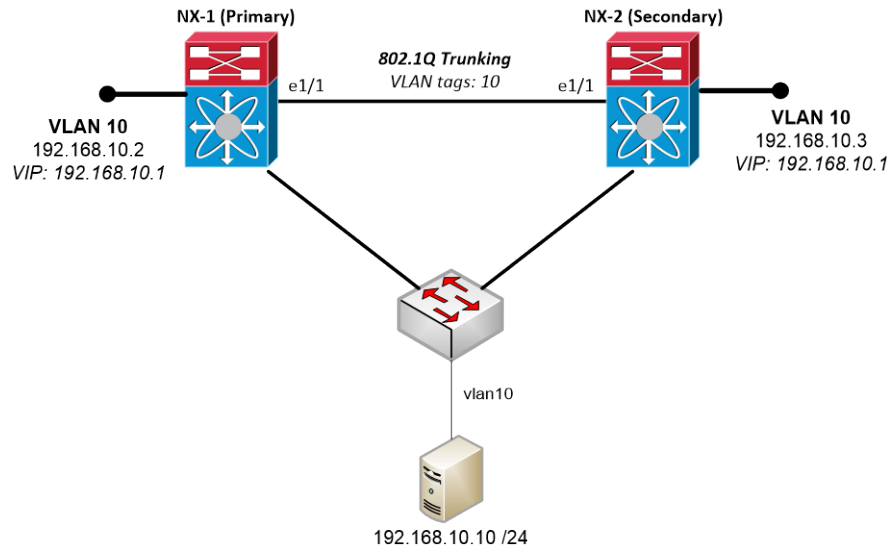
```
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
auto-cost reference-bandwidth 100000
area 0 authentication message-digest
default-information originate always
```

```
interface e1/1
no switchport
ip address 10.1.1.1/24
ip router ospf 1 area 0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 0 Cisco123
ip distribute-list ospf 1 prefix-list PL-OSPF-OUT out
ip distribute-list ospf 1 prefix-list PL-OSPF-IN in
```

```
show ip route
```


HSRP

- Configure HSRP between NX-1 and NX-2 for VLAN10
- The Primary HSRP router for VLAN10 will be NX-1. The Secondary HSRP router will be NX-2
- The HSRP (VIP) IP for VLAN10 will be 192.168.10.1



>> NX-1 <<

```
feature hsrp
feature interface-vlan
```

```
interface Vlan10
ip address 192.168.10.2/24
hsrp 1
ip 192.168.10.1
priority 110
preempt delay minimum 180
authentication md5 key-string Cisco123
timers 1 3
```

>> NX-2 <<

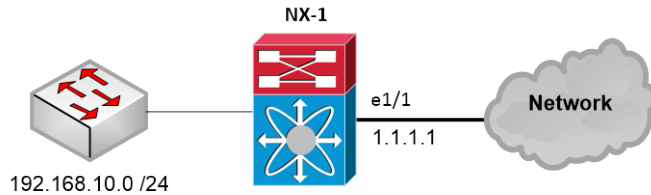
```
feature hsrp
feature interface-vlan
```

```
interface Vlan10
ip address 192.168.10.3/24
hsrp 1
ip 192.168.10.1
preempt
authentication md5 key-string Cisco123
timers 1 3
```

```
show hsrp
```

Access Control List (ACL)

- Configure an ACL policy and apply inbound on interface e1/1



```
ip access-list RHG-ACL
10 permit udp any 192.168.10.10/32 eq snmp
20 permit tcp any 192.168.10.10/32 eq 443
30 permit tcp any 192.168.10.10/32 eq 80
40 permit tcp any 192.168.10.10/32 eq 25
```

```
interface e1/1
ip address 1.1.1.1/24
ip access-group RHG-ACL in
```

Out-of-Band (OOB) Management

- Configure the OOB Management Interface (mgmt. 0)
- The IP configured for the mgmt. interface will be 192.168.99.2
- Configure ACL for what management traffic is allowed to the management interface. We will allow SSH and SNMP from the 192.168.10.0 network. And we will also ICMP.

```
ssh key rsa 2048
```

```
vrf context management
ip route 0.0.0.0/0 192.168.99.1
```

```
ip access-list ACL-MGMT
10 permit tcp 192.168.10.0/24 any eq 22
20 permit udp 192.168.10.10/32 any eq snmp
30 permit icmp any any
```

```
interface mgmt 0
ip access-group ACL-MGMT in
ip address 192.168.99.2/24
```

Control Plane Policing (CoPP)

- Traffic allowed to the control plane will be SNMP from NMS server 192.168.10.10. Rate limit that traffic to 10Mbps
- Traffic not allowed to the control plane will be any other SNMP access
- Apply policy to control plane interface

```
ip access-list COPP-ACL-ALLOWED
10 permit udp 192.168.10.10/32 any eq snmp
```

```
ip access-list COPP-ACL-DENIED
10 permit udp any any eq snmp
```

```
class-map type control-plane match-any copp-system-class-management
no match access-group name copp-system-acl-snmp
```

```
class-map type control-plane match-any COPP-CM-ALLOWED
match access-group name COPP-ACL-ALLOWED
```

```
class-map type control-plane match-any COPP-CM-DENIED
match access-group name COPP-ACL-DENIED
```

```
policy-map type control-plane COPP-PM-SYSTEM
class COPP-CM-ALLOWED
  police cir 10000 kbps bc 250 ms conform transmit violate drop
class COPP-CM-DENIED
  police cir 10000 kbps bc 250 ms conform drop violate drop
```

```
control-plane
service-policy input COPP-PM-SYSTEM
```

NTP

- Specify NTP server (192.168.10.10)

```
ntp server 192.168.10.10 use-vrf management
```

Logging (SYSLOG)

- Enable logging using msec timestamps
- Specify IP of Syslog Server (192.168.10.10) enabled for debugging (level 7)

```
logging timestamp milliseconds
logging 192.168.10.10 7 use-vrf management
logging event link-status default
logging event trunk-status default
```

SNMPV2

- Define SNMP RW (network-admin) community string and SNMP RO (network-operator) community string
- Send SNMP traps to server 192.168.10.10

```
snmp-server community RHG-SNMP-RW group network-admin
snmp-server community RHG-SNMP-RO group network-operator
snmp-server location TRACY, CA
snmp-server contact ROUTEHUB
```

```
snmp-server host 192.168.10.10 version 2 RHG-SNMP-RW
snmp-server enable traps link
```

Telnet

- Enable Telnet

```
feature telnet
```

VTY

- Set session timeout for Telnet and SSH sessions to 15 minutes

```
line vty
session-limit 15
exec-time 15
```

AAA and TACACS+

- Enable TACACS+
- TACACS+ server is 192.168.10.10 using the key "Cisco123"
- Use TACACS for Telnet/SSH and console network access into the Nexus switch

```
feature tacacs+
no feature telnet
```

```
tacacs-server key 0 Cisco123
tacacs-server host 192.168.10.10
tacacs-server directed-request
```

```
aaa group server tacacs+ RHG-AAA
server 192.168.10.10
use-vrf management
```

```
aaa authentication login default group RHG-AAA
aaa authentication login console group RHG-AAA
aaa accounting default group RHG-AAA
aaa authentication login error-enable
```

AAA and RADIUS

- Enable RADIUS
- RADIUS server is 192.168.10.10 using the key "Cisco123"
- Use RADIUS for Telnet/SSH and console network access into the Nexus switch

feature radius

radius-server host 192.168.10.10 key 7 Cisco123 authentication accounting

aaa group server radius RHG-RADIUS
server 192.168.10.10
use-vrf management

aaa authentication login default group RHG-AAA
aaa authentication login console group RHG-AAA
aaa accounting default group RHG-AAA

Line Card ID

- *Used for identifying a line module in the Nexus chassis*
- Turn on (or off) the blue ID LED for the module in slot 1

locator-led module 1

no locator-led module 1

Role Based Access Control (RBAC)

- Add user account "rootadmin" with Read-Write access (network-admin role)
- Add user account "opsadmin" with Read-Only access (network-operator role)

username rootadmin password Cisco123 role network-admin
username opsadmin password Cisco456 role network-operator

Configuration Rollback

- Create checkpoint for the current configuration on the Nexus

`checkpoint Initial`

- To rollback to the configuration in the "Initial" checkpoint

`rollback running-config checkpoint Initial`

- Create checkpoint for the current configuration and save it to the bootflash

`checkpoint file bootflash:RHG_Checkpoint01`

- To rollback to the configuration in the checkpoint, RHG_Checkpoint01, saved in the bootflash

`rollback running-config file bootflash:RHG_Checkpoint01`

- View current checkpoints created on the Nexus switch

show checkpoint summary

System Switchover

- Switchover to redundant supervisor

`system switchover`

Fabric Extenders (NX-5000) Using Static Pinning

- Configured on Nexus 5000 with connected NX-2000 switches
- Configure "static pinning" by building a fabric extender to the NX-2000 switch
- We will configure a virtual FEX group using ID 100 that will be associated to the downlink ports to the NX-2000 switch



```
fex 100
  pinning max-links 2
  description Fabric Extender to NX-2000-1
  type "Nexus 2148T"
```

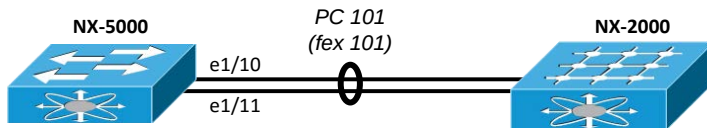
```
interface Ethernet1/10
  switchport mode fex-fabric
  fex associate 100
```

```
interface Ethernet1/11
  switchport mode fex-fabric
  fex associate 100
```

```
show fex
sh int ex/x fex-intf
```


Fabric Extenders (NX-5000) Using Port Channel

- Configured on Nexus 5000 with connected NX-2000 switches
- Configure "port channel" by building a fabric extender to the NX-2000 switch
- We will configure a virtual FEX group using ID 101 that will be associated to the downlink ports to the NX-2000 switch



```
feature fex
```

```
fex 101
```

```
pinning max-links 1
```

```
description Fabric Extender to NX-2000-1
```

```
interface port-channel 101
```

```
switchport mode fex-fabric
```

```
fex associate 101
```

```
interface Ethernet1/10
```

```
channel-group 101
```

```
interface Ethernet1/11
```

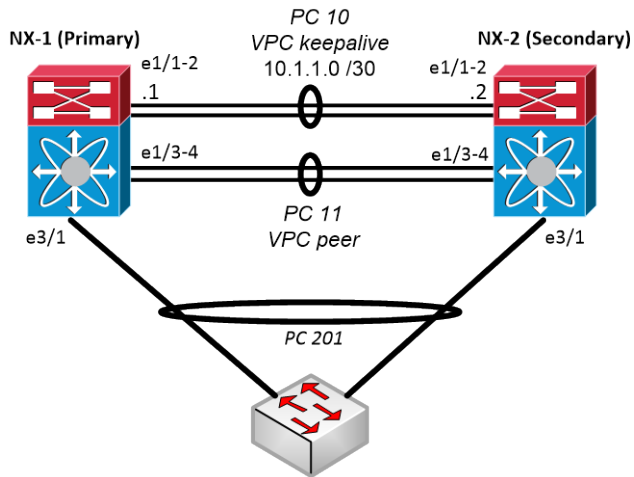
```
channel-group 101
```

```
show fex
```

```
sh int ex/x fex-intf
```

VPC

- Configure VPC between Nexus switches.
- Interfaces e1/1-2 will be used for the VPC keep-alive link on Port-Channel 10
- VPC domain will use ID "10"
- NX-1 will be the primary VPC switch (using priority 8192) and NX-2 will be the secondary VPC switch (16384) ; *lower the priority, the more preferred as primary VPC switch*
- Interfaces e1/3-4 will be used for the VPC peer-link on Port-Channel 11
- Configure a port channel from the VPC domain to the Access Switch on Port-Channel 201



>>NX-1<<

feature vpc

vrf context vpc-keepalive

vpc domain 10

role priority 8192

peer-keepalive destination 10.1.1.2 source 10.1.1.1 vrf vpc-keepalive

delay restore 360

auto-recovery

graceful consistency-check

peer-gateway

ip arp synchronize

interface port-channel 10

vrf member vpc-keepalive

ip address 10.1.1.1 255.255.255.252

interface e1/1-2

no switchport

channel-group 10

no shutdown

```
interface port-channel 11
switchport mode trunk
vpc peer-link
```

```
interface e1/3-4
switchport
channel-group 11 mode active
```

```
interface port-channel 201
switchport
switchport trunk native vlan 999
switchport trunk allowed vlan 10
switchport mode trunk
vpc 201
```

```
interface e3/1
switchport
channel-group 201 mode active
```

```
>>NX-2<<
feature vpc
```

```
vrf context vpc-keepalive
```

```
vpc domain 10
role priority 16384
peer-keepalive destination 10.1.1.1 source 10.1.1.2 vrf vpc-keepalive
delay restore 360
auto-recovery
graceful consistency-check
peer-gateway
ip arp synchronize
```

```
interface port-channel 10
vrf member vpc-keepalive
ip address 10.1.1.2 255.255.255.252
```

```
interface e1/1-2
no switchport
channel-group 10
no shutdown
```

```
interface port-channel 11
switchport mode trunk
vpc peer-link
```

```
interface e1/3-4
switchport
channel-group 11 mode active
```

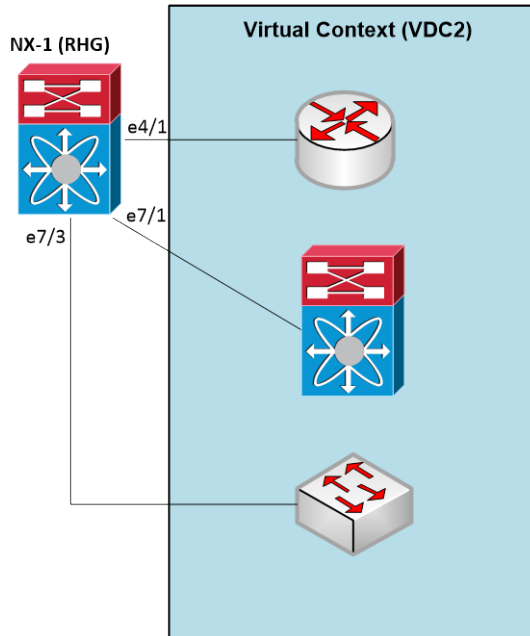
```
interface port-channel 201
switchport
switchport trunk native vlan 999
switchport trunk allowed vlan 10
switchport mode trunk
vpc 201
```

```
interface e3/1
switchport
channel-group 201 mode active
```

```
show hardware feature-capability
show vpc <id>
show vpc brief
show vpc peer-keepalive
```

VDC

- Create a new virtual context called “VDC2”
- Interfaces e4/1, 7/1, and 7/3 added to VDC2



```
hostname RHG
```

```
vdc RHG.VDC2
```

```
allocate interface ethernet 4/1, ethernet 7/1, ethernet 7/3
```

```
show vdc RHG.VDC2 membership
```

```
show vdc RHG.VDC2
```

- To access the virtual context for further network configuration

```
switchto vdc RHG.VDC2
```

- Connect back to the main/global context

```
switchback
```

Jumbo Frame Support for Nexus 5000 Series

- Enable Jumbo frame support on Cisco Nexus 5000 series

```
policy-map type network-qos jumbo  
class type network-qos class-default  
mtu 9216
```

```
system qos  
service-policy type network-qos jumbo
```

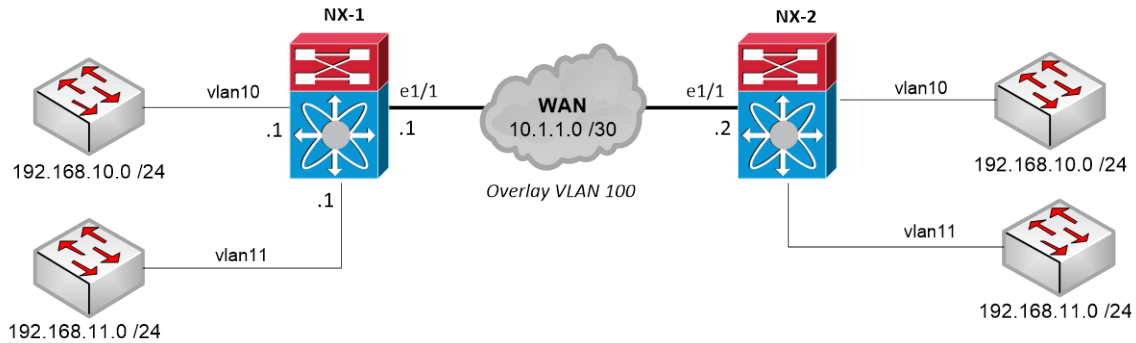
Jumbo Frame Support for Nexus 7000 Series

- Enable Jumbo frame support on Cisco Nexus 7000 series

```
system jumbomtu 9216
```

OTV

- Requires the Transport Services license to be installed
- Extend VLANs 10 and 11 between the two sites
- The Overlay VLAN will be 100 used between the two sites for extending VLAN10-11



```
>> NX-1 <<
interface ethernet 1/1
ip address 10.1.1.1/30
ip igmp version 3
no shutdown
```

```
vlan 10-11
vlan 100
```

```
feature otv
```

```
otv site-vlan 100
```

```
interface Overlay1
otv control-group 239.1.1.1
otv data-group 232.1.1.0/28
otv join-interface ethernet 1/1
otv extend-vlan 10-11
no shutdown
```

```
show otv
show otv overlay
show otv adjacency
show otv site
show otv vlan
show otv arp
show mac address-table
```

QoS for 48-Port GE (1P3Q4T)

- Recommended QoS for Nexus 7000 48-Port 10/100/1000 Modules (1P3Q4T)
- CoS to queue mapping for all interfaces with same hardware ASIC
- BW, queue-limit and drop threshold are performed using the policy-map
- Apply to all interfaces with same hardware ASIC

```
class-map type queuing match-any 1p3q4t-out-pq1  
  match cos 5  
class-map type queuing match-any 1p3q4t-out-q2  
  match cos 3,6-7  
class-map type queuing match-any 1p3q4t-out-q3  
  match cos 2,4  
class-map type queuing match-any 1p3q4t-out-q-default  
  match cos 0-1
```

```
policy-map type queuing GE-outbound  
  class type queuing 1p3q4t-out-pq1  
    priority level 1  
    queue-limit percent 15  
  class type queuing 1p3q4t-out-q2  
    queue-limit percent 25  
    queue-limit cos 6 percent 100  
    queue-limit cos 7 percent 100  
    queue-limit cos 3 percent 70  
  class type queuing 1p3q4t-out-q3  
    queue-limit percent 25  
    queue-limit cos 4 percent 100  
    queue-limit cos 2 percent 50  
    bandwidth remaining percent 33  
  class type queuing 1p3q4t-out-q-default  
    queue-limit percent 35  
    queue-limit cos 1 percent 50  
    queue-limit cos 0 percent 100  
    bandwidth remaining percent 45
```

```
Nexus 7K(config-if)#service-policy type queuing output GE-outbound
```


Fibre Channel over Ethernet (FCoE)

- Configuration for Nexus 5000 Series

! Enable FCoE on the Nexus switch

```
feature fcoe
```

! Map a VSAN for FCoE traffic onto a VLAN

```
vlan 10
```

```
fcoe vsan 110
```

! Create virtual Fibre Channel interfaces to carry the FCoE traffic

```
interface vfc 1
```

```
bind interface ethernet 1/10
```

```
no shutdown
```

! Map VSAN to vFC interface

```
vsan database
```

```
vsan 110 interface vfc 1
```

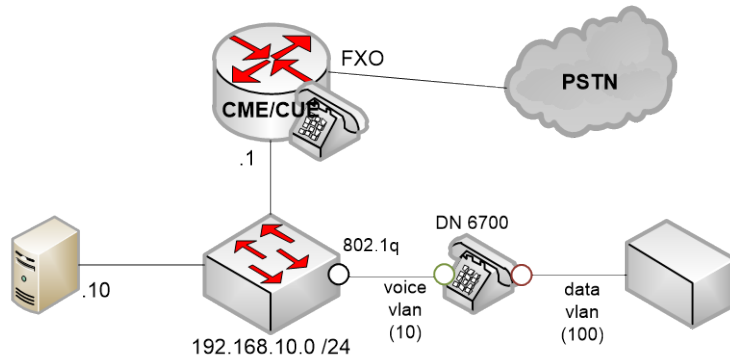
! Monitoring FCoE

```
show flogi database
```

CISCO UCM EXPRESS

Solution/Services: Voice & Unified Communications

Related: Cisco Unity Express



Base Configuration

- Configure VLAN and interfaces for Voice network. Voice VLAN will be VLAN10 (192.168.10.0)
- "ip source-address": Specify source IP address for CME and list SCCP port number (2000)
- "max-ephone": specify the maximum number of phones supported on the router
- "max-dn": specify the maximum number of directory numbers supported on router
- "timeout interdigit": specify the amount of time (in seconds) for setting up a call
- "system message": configure banner on bottom of the phone
- "video": enable video support for phone endpoints
- "time-zone": specify correct time-zone. 5 = PST (GMT -8)
- "voicemail": specify the main voicemail pilot number.
- "web admin system": configures username and password to access the CME Integrated GUI page

```
vlan 10
name ROUTEHUB-VLAN
```

```
interface FastEthernet0/1/1
description IP Phone Port
switchport access vlan 10
```

```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
```

```
telephony-service
ip source-address 192.168.10.1 port 2000
max-ephones 14
max-dns 56
timeouts interdigit 5
```

```
system message RouteHub UC520
auto assign 19 to 19
video
time-zone 5
voicemail 6000
web admin system name admin secret cisco123
moh music-on-hold.au
call-forward pattern .T
call-forward system redirecting-expanded
transfer-system full-consult dss
transfer-pattern 9.T
secondary-dialtone 9
```

Directory Numbers

- Configure directory number (extension) 6700
- Configure extension as a dual-line number to accept up to 2 concurrent calls
- Any call to extension 6700 that is “busy” or there is “no answer (noan)” send to voicemail (6000)
- “label”: specify what text will be displayed on the phone for the configured extension.

```
ephone-dn 10 dual-line
number 6700
label 6700 (Main)
description 2091236700
call-forward busy 6000
call-forward noan 6000 timeout 15
```

IP Phone Configuration

- Add Cisco IP 7970 Phone using mac-address 001C.58F0.7619
- Associate the extension (6700) in “ephone-dn 10” to line 1 on the Cisco phone

```
ephone 1
mac-address 001C.58F0.7619
type 7970
button 1:10
```

Call Forward All

- All calls made to extension 6700 will be forwarded to 4001

```
ephone-dn 10 dual-line  
number 6700  
call-forward all 4001
```

Voice and Data VLAN Configuration

- Voice VLAN = 10, Data VLAN = 100

```
vlan 10  
name RHG-VOICE-VLAN
```

```
vlan 100  
name RHG-DATA-VLAN
```

```
interface FastEthernet0/1  
description TO: IP Phone and Desktop  
switchport access vlan 100  
switchport mode access  
switchport voice vlan 10  
spanning-tree portfast
```

```
interface GigabitEthernet0/1  
description TO: UPLINK (Core, Distribution)  
switchport trunk allowed vlan 10,100  
switchport mode trunk  
switchport nonegotiate  
spanning-tree portfast trunk
```

Configuring DHCP on Cisco IOS

- Configure DHCP scope for Voice Network (192.168.10.0/24)
- Configure "option 150" to point to the CME router IP (192.168.10.1)

```
ip dhcp excluded-address 192.168.10.1 192.168.10.29
```

```
ip dhcp pool ROUTEHUB-DHCP-LAN-POOL
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
option 150 ip 192.168.10.1
dns-server 4.2.2.2 4.2.2.3
lease 5
```

Mapping an Analog Line (DID) to an IP Phone

- When user at extension 6700 dials any outgoing call it will route through FXO port 1/0/0 ; dedicated for 6700
- All incoming calls on FXO port 1/0/0 would go to extension 6700

```
voice translation-rule 1
rule 1 /^9/ /19/
```

```
voice translation-profile TP-6700
translate called 1
```

```
dial-peer voice 1 voip
translation-profile incoming TP-6700
answer-address 6700
```

```
dial-peer voice 19 pots
destination-pattern 19T
port 1/0/0
```

```
voice-port 1/0/0
supervisory disconnect dualtone pre-connect
pre-dial-delay 0
no vad
timeouts call-disconnect 2
timeouts wait-release 2
connection plar opx 6700
caller-id enable
```

Configuring FXS port as a SCCP port

- Configure FXS port 0/0/0 as a SCCP port
- Plug analog phone into FXS port 0/0/0. Type: ANL, MAC Address: determine from the command "show stcapp device summary"

```
sccp local Vlan10
sccp ccm 192.168.10.1 identifier 1 priority 1 version 4.1
sccp
```

```
sccp ccm group 1
bind interface Vlan10
associate ccm 1 priority 1
keepalive retries 5
switchback method graceful
stcapp ccm-group 1
stcapp
```

```
dial-peer voice 14 pots
service stcapp
port 0/0/0
```

```
voice-port 0/0/0
caller-id enable
```

```
ephone 2
device-security-mode none
mac-address D456.7C69.0000
type anl
button 1:10
```

CME as SIP Server for SIP Clients

- Enable SIP
- Configure CME as SIP Server (using 192.168.10.1) for SIP IP Phones
- Add new directory number (extension) 8700 used for SIP Phones
- Associate extension 8700 to SIP phone (using register pool 1) with id "000C.F179.1682"
- SIP phone will require using account "8700" for the username and password being "cisco6778"

```
voice service voip
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
supplementary-service h450.12
```

```
voice register global
mode cme
source-address 192.168.10.1 port 5060
max-dn 12
max-pool 12
timezone 47
time-format 24
date-format YY-M-D
dst start Oct week 8 day Sun time 02:00
dst stop Mar week 8 day Sun time 02:00
```

```
voice register dn 1
number 8700
name ROUTEHUB SIP client (X-lite)
```

```
voice register pool 1
id mac 000C.F179.1682
number 1 dn 1
username 8700 password cisco6778
codec g711ulaw
```

Blocking Incoming Calls from PSTN

- Block outside number "1-800-123-4567" from coming into CME router FXO port 0/1/0

```
voice translation-rule 5  
rule 1 reject /8001234567/
```

```
voice translation-profile call_block  
translate calling 5
```

```
dial-peer voice 100 pots  
call-block translation-profile incoming call_block  
call-block disconnect-cause incoming call-reject  
destination-pattern 9.T  
incoming called-number .  
port 0/1/0
```

Phone Directory

- Phone directory will list entries based on first name
- Phone directory entries reflecting the speed-dial number and label

```
telephony-service  
directory first-name-first  
directory entry 1 919252302203 name ROUTEHUB (Main)  
directory entry 2 912091234567 name Other Number (Cell)
```

Single Number Reach (SNR)

- If some calls extension 6700 it will also ring the number 919252302203 (access code is 9 for outbound calls)
- If there is no answer, the call will be forwarded to internal voicemail (6000)

```
ephone-dn 10 dual-line  
number 6700 no-reg primary  
mobility  
snr 919252302203 delay 2 timeout 30 cfwd-noan 6000
```


Fast Dial

- Configure fast dial entry 6702 (USER2) on the phone configured under “ephone 1”

ephone 1

```
fastdial 1 6702 name USER2
```

Call Park

- Call Park number will be 6002
- A call can be parked for 30 seconds and support up to 10 concurrent parked calls

ephone-dn 14

```
number 6002
```

```
park-slot timeout 30 limit 10
```

```
name ROUTEHUB CALL PARK
```

Setting up SIP Trunk to SIP Provider (with CME/CUE)

- *IOS: 15.1*
- “allow-connections sip to sip”: Enable SIP connections to/from CME router “
- Configure SIP trunk to SIP provider (sipproxy.routehub.local) on Internet.
- Our SIP phone number will be “19252302204”
- Our SIP username will be our SIP number and our SIP password will be “cisco6778”

```
voice-card 0
dspfarm
dsp services dspfarm
```

```
sip-ua
authentication username 19252302204 password cisco6778
no remote-party-id
retry invite 2
retry register 10
timers connect 100
registrar dns:sipproxy.routehub.local expires 3600
sip-server dns:sipproxy.routehub.local
host-registrar
```

```
voice service voip
ip address trusted list
ipv4 0.0.0.0 0.0.0.0
allow-connections sip to sip
supplementary-service h450.12
no supplementary-service sip moved-temporarily
no supplementary-service sip refer
sip
registrar server expires max 3600 min 3600
localhost dns:sipproxy.routehub.local
```

- Configure translation rule for incoming calls to translate SIP number to extension 6700 which is configured on a phone

```
voice translation-rule 1
rule 1 /19252302204/ /6700/
```

```
voice translation-profile RHG-TP-SIP-IN
translate called 1
```

- Configuring translation for outgoing calls to (1) allow users to dial 911, (2) any call placed over the SIP trunk will strip off the access code "9" before routing the call, and (3) any extension or DID placing a call through the SIP trunk will be translated to our SIP phone number (shown in translation rule #3)

```
voice translation-rule 2
rule 1 /^911$/ /911/
rule 2 /^9\(.*)$/ ^1/
```

```
voice translation-rule 3
rule 1 /^.* /19252302204/
```

- Translation rule used for outgoing calls from Cisco Unity Express (CUE): (1) local calls will automatically include the local area code, (2) calls from directory number 6001 (the AA pilot) will map to DID 925-230-2204, (3) calls from directory number 6000 (the Voicemail pilot) will map to DID 925-230-2204, and (4) any call placed over the SIP trunk will strip off the access code "9" before routing the call.

```
voice translation-rule 4
rule 1 /^9\(.*)$/ /925\1/
rule 2 /6001/ /19252302204/
rule 3 /6000/ /19252302204/
rule 4 /^9\(.*)$/ ^1/
```

```
voice translation-profile RHG-TP-SIP-OUT
translate called 2
translate calling 3
translate redirect-target 4
translate redirect-called 4
```

```
voice translation-profile RHG-TP-SIP-CUE
translate redirect-target 4
translate redirect-called 4
```

- Specify supported codec to use with the SIP trunk

```
voice class codec 1
codec preference 1 g711ulaw
```

- Dial peer for incoming calling from SIP trunk

```
dial-peer voice 1 voip
description INCOMING: All Incoming Calling
translation-profile incoming RHG-TP-SIP-IN
destination-pattern .%
voice-class codec 1
voice-class sip dtmf-relay force rtp-nte
session protocol sipv2
session target sip-server
dtmf-relay rtp-nte
no vad
```

- Dial peer for 7-digit Local calling through SIP trunk

```
dial-peer voice 7 voip
description OUTGOING: 7-Digit Local Calling
translation-profile outgoing RHG-TP-SIP-OUT
destination-pattern 9[2-9].....
voice-class codec 1
voice-class sip dtmf-relay force rtp-nte
session protocol sipv2
session target sip-server
dtmf-relay rtp-nte
no vad
```

- Dial peer for Long Distance calling through SIP trunk

```
dial-peer voice 11 voip
description OUTGOING: Long Distance Calling
translation-profile outgoing RHG-TP-SIP-OUT
destination-pattern 91[2-9]..[2-9].....
voice-class codec 1
voice-class sip dtmf-relay force rtp-nte
session protocol sipv2
session target sip-server
dtmf-relay rtp-nte
no vad
```

- Dial peer for Emergency 911 calling through SIP trunk

```
dial-peer voice 9911 voip
description OUTGOING: Emergency Calling
translation-profile outgoing RHG-TP-SIP-OUT
destination-pattern 9911
voice-class codec 1
voice-class sip dtmf-relay force rtp-nte
session protocol sipv2
session target sip-server
dtmf-relay rtp-nte
no vad
```

- Dial peer for Emergency 911 calling through SIP trunk

```
dial-peer voice 911 voip
description OUTGOING: Emergency Calling
translation-profile outgoing RHG-TP-SIP-OUT
destination-pattern 911
voice-class codec 1
voice-class sip dtmf-relay force rtp-nte
session protocol sipv2
session target sip-server
dtmf-relay rtp-nte
no vad
```

- Dial peer for International calling through SIP trunk

```
dial-peer voice 9011 voip
description OUTGOING: International Calling
translation-profile outgoing RHG-TP-SIP-OUT
destination-pattern 9011T
voice-class codec 1
voice-class sip dtmf-relay force rtp-nte
session protocol sipv2
session target sip-server
dtmf-relay rtp-nte
no vad
```

- Dial peer for Voicemail (on CUE)

```
dial-peer voice 6000 voip
description CUE: Voicemail
translation-profile outgoing RHG-TS-SIP-CUE
destination-pattern 6000
b2bua
session protocol sipv2
session target ipv4: 192.168.10.2
dtmf-relay sip-notify
codec g711ulaw
no vad
```

- Dial peer for AA (on CUE)

```
dial-peer voice 6001 voip
description CUE AA
translation-profile outgoing RHG-TS-SIP-CUE
destination-pattern 6001
b2bua
session protocol sipv2
session target ipv4: 192.168.10.2
dtmf-relay sip-notify
codec g711ulaw
no vad
```

- MWI notification

```
dial-peer voice 800 voip
incoming called-number 800[0,1]....
codec g711ulaw
no vad
```

```
ephone-dn 16
number 8000.... no-reg primary
mwi on
```

```
ephone-dn 17
number 8001.... no-reg primary
mwi off
```

- Directory number 6700 used for placing and receiving calls from the SIP trunk

```
ephone-dn 10 dual-line
number 6700 no-reg primary
name 6700
call-forward busy 6000
call-forward noan 6000 timeout 15
```

```
ephone-dn 18
number 9252302204
description "Main Number"
```

- Preserves caller-ID of a call when it is transferred or forwarded
- Enable translation rule features for forwarding

```
telephony-service
calling-number initiator
call-forward system redirecting-expanded
```

- CUE configuration on CME router

```
interface Integrated-Service-Engine0/0
description RHG: CUE interface
ip unnumbered Vlan10
service-module ip address 192.168.10.2 255.255.255.0
service-module ip default-gateway 192.168.10.1

ip route 192.168.10.2 255.255.255.255 Integrated-Service-Engine0/0
```

- Monitoring commands

```
show sip-ua register status
debug ccsip message
show ephone registered
show voice rtp connection
show sip-ua call
show call active voice brief
debug ccsip message
```

Sending Calls to Voicemail (CUE)

- If a caller dials a number like extension 6700 and the line is busy ("busy") or not answered ("noan") the call will forward to the voicemail pilot (using 6000) on CUE (192.168.10.2)

```
dial-peer voice 600 voip
destination-pattern 6000
session protocol sipv2
session target ipv4:192.168.10.2
dtmf-relay sip-notify
codec g711ulaw
no vad
```

```
telephony-service
voicemail 6000
```

```
ephone-dn 10 dual-line
number 6700 no-reg primary
call-forward busy 6000
call-forward noan 6000 timeout 15
```

```
dial-peer voice 800 voip
incoming called-number 800[0,1]....
codec g711ulaw
no vad
```

```
ephone-dn 20
number 8000.... no-reg primary
mwi on
```

```
ephone-dn 21
number 8001.... no-reg primary
mwi off
```


Hardware Conferencing

- Configure DSP resources for hardware conferencing
- Specify max number of conference bridges to be 8 (based on the number of DSP resources installed)

```
sccp local Vlan10
sccp ccm 192.168.10.1 identifier 1 priority 1 version 4.1
sccp
```

```
sccp ccm group 1
bind interface Vlan10
associate ccm 1 priority 1
associate profile 1 register MTP_CME
keepalive retries 5
switchback method graceful
```

```
voice class custom-cptone routehub-leave
dualtone conference
frequency 900 900
cadence 150 50 150 50
```

```
voice class custom-cptone routehub-join
dualtone conference
frequency 1200 1200
cadence 150 50 150 50
```

```
dspfarm profile 1 conference
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec g729r8
codec g729br8
maximum sessions 8
conference-join custom-cptone routehub-join
conference-leave custom-cptone routehub-leave
associate application SCCP
```

```
telephony-service
max-conferences 8 gain -6
sdspfarm conference mute-on 11 mute-off 12
sdspfarm units 3
sdspfarm tag 1 MTP_CME
conference hardware
```

Conferencing: MeetMe

- *Requires hardware conferencing to be configured first*
- Configure the Meetme Conference Numbers to be 6999

ephone-dn 22 dual-line
number 6999
conference meetme
no huntstop

ephone-dn 23 dual-line
number 6999
conference meetme
preference 1
no huntstop

ephone-dn 24 dual-line
number 6999
conference meetme
preference 2
no huntstop

Conferencing: Adhoc

- *Requires hardware conferencing to be configured first*
- Configure the Ad-hoc conferencing to use directory number 6998

ephone-dn 26 dual-line
number 6998
conference ad-hoc
preference 1
no huntstop

ephone-dn 27 dual-line
number 6998
conference ad-hoc
preference 2
no huntstop

Paging

- Enabling Paging using directory number 6001 (ephone-dn 1)
- Specify Multicast IP and port number 2000 (SCCP) with Paging feature
- Apply Paging group (ephone-dn 1) to all phones that should be paged if someone dials 6001

```
ephone-dn 1
number 6001
name ROUTEHUB Paging System
paging ip 239.192.2.1 port 2000
```

```
ephone 1
paging-dn 1
```

```
ephone 3
paging-dn 1
```

Intercom

- Configure Intercom connection between Cisco phone1 (ephone 1) and Cisco Phone2 (ephone 2).
- Phone 1 will use the Intercom Directory number of A5001. Intercom to Phone 2 will be on button 2
- Phone 2 will use the Intercom Directory number of A5002 . Intercom to Phone 1 will be on button 2

```
ephone-dn 12
number A5001 no-reg primary
label Intercom
name Intercom
intercom A5002
```

```
ephone-dn 13
number A5002 no-reg primary
label Intercom
name Intercom
intercom A5001
```

```
ephone 1
type 7970
button 1:10 2:11
```

```
ephone 3
type 7970
button 1:10 2:12
```

Hunt Group

- Configure hunt group to call one extension at a the same time.
- The extensions in the hunt group will be: 6702 and 6700
- The hunt group pilot number will be 6701
- If there is no answer within 15 seconds forward to the voicemail pilot number (6000)

```
ephone-hunt 1 sequential
pilot 6701
list 6702, 6700
final 6000
preference 1
timeout 15, 15
```

How to Setup Phone Softkey Templates

- Configure new Softkey Template for Cisco Phones
- Softkey will list options that will be available when a call is (1) on Hold, (2) the phone is IDLE, (3) if a call is seized, or (4) when a call is connected.
- Apply Softkey template to Cisco phone (using ephone 1) and reset phone to use the new template

```
ephone-template 1
softkeys hold Newcall Resume Select Join
softkeys idle Redial Newcall Cfwdall Pickup ConfList Dnd
softkeys seized Redial Pickup Meetme Endcall
softkeys connected Endcall ConfList Confrn Hold Join Park RmLstC
```

```
ephone 1
ephone-template 1
type 7970
```

```
ephone 1
reset
```

Phone Services

- Add XML URL that will be listed under "Phone Services" on the Cisco Phones

```
telephony-service
url services http://phone-xml.berbee.com/menu.xml
```

Call Center

- Download the needed files and copy to flash on CME router.

app-b-acd-aa-2.1.2.3.tcl

app-b-acd-2.1.2.3.tcl

uc01tra#copy tftp flash:

Address or name of remote host []? 192.168.10.10

Source filename []? app-b-acd-aa-2.1.2.3.tcl

Destination filename [app-b-acd-aa-2.1.2.3.tcl]

- Agent 1 will use extension 2001, Agent 2 will use extension 2002
- Added both agents into Hunt Group (based on idle the longest) using pilot number 6721
- Send statistics of the hunt group to the TFTP server (192.168.10.10) under the "data" folder

ephone-dn 15 dual-line
number 2001

ephone-dn 16 dual-line
number 2002

ephone-hunt 1 longest-idle
pilot 6721
list 2001, 2002
timeout 10, 10
statistics collect

telephony-service

hunt-group report url prefix tftp://192.168.10.10/data

hunt-group report url suffix 0 to 200

hunt-group report every 2 hours

- Call Center application configuration
- "param aa-hunt2": if caller presses "2" they will access the call center support group (hunt group) at 6721
- "param queue-len": The number of callers in the queue at one time will be "5"
- "param dial-by-extension-option": if the caller presses "1" you can dial by extension to call a user directly
- "param aa-pilot": the main number to reach the AA call center queue will be 6720
- "param max-time-call-retry": specify the amount of time a caller will wait in the queue until it dials the pilot number again. We will configure our value to be 300 seconds
- "param max-time-vm-retry": specify the retry time to be "2", so after another 300 seconds, the caller will be forwarded to voicemail (at 6000). Voicemail pilot is specified in "param voice-mail"

application

service aa flash:app-b-acd-aa-2.1.2.3.tcl

param aa-hunt2 6721

paramspace english index 1

param number-of-hunt-grps 1

param queue-len 5

param handoff-string aa

param dial-by-extension-option 1

paramspace english language en

param aa-pilot 6720

```
param space english location flash:
param second-greeting-time 30
param queue-manager-debug 1
param call-retry-timer 15
param max-time-call-retry 300
param max-time-vm-retry 2
param voice-mail 6000
```

```
param service-name queue
service queue flash:app-b-acd-2.1.2.3.tcl
param queue-len 5
param queue-manager-debug 1
param aa-hunt2 6721
param number-of-hunt-grps 1
```

- Configure dial peer to specify the main number (6720) to reach the AA call center queue. This is the number callers would dial into
- Apply the call center application to this dial peer

```
dial-peer voice 1009 voip
service aa
destination-pattern 6720
session target ipv4:192.168.10.1
incoming called-number 6720
dtmf-relay h245-alphanumeric
codec g711ulaw
no vad
```

How to Setup A Custom Ring Tone

- Create two XML files (RingList.xml and DistinctiveRingList.xml) listing the ring tone file name and label. Ring tone must be in “.raw” format.

```
<CiscoIPPhoneRingList>
<Ring>
  <DisplayName>24</DisplayName>
  <FileName>24.raw</FileName>
</Ring>
</CiscoIPPhoneRingList>
```

- Copy the ring tone file and XML files to the flash memory on the CME router from TFTP server (192.168.10.10)
- Each file copied, configure TFTP entry that will be used by Cisco Phones to select the ring tone “24”

```
copy tftp://192.168.10.10/24.raw flash:
copy tftp://192.168.10.10/ RingList.xml flash:
copy tftp://192.168.10.10/ DistinctiveRingList.xml flash:
```

```
tftp-server flash:RingList.xml
tftp-server flash:DistinctiveRingList.xml
tftp-server flash:24.raw
```

Extension Mobility

- Configure Extension Mobility profile listing the pin (6778), login account (user=78, password=78), and the extensions (6700, A5001, 7700, & 2001) that will be associated to this profile.
- Configure “logout” profile with the same details also include username and password for Extension Mobility login to load this profile on the phone.
- Associate the “logout” profile to the actual phone (ephone 1) using the listed extensions today

```
voice user-profile 1
pin 6778
user 78 password 78
number 6700,A5001,7700,2001 type feature-ring
```

```
voice logout-profile 1
pin 6778
user 16778 password 6778
number 6700,A5001,7700,2001 type feature-ring
```

```
ephone 1
logout-profile 1
```

```
telephony-service
url authentication http://192.168.10.1/voiceview/authentication/authenticate.do
```

Fax to Email using T.37 (Voice and FAX on Same FXO port)

- Download the following TCL scripts from the Cisco software center then copy them to the flash memory of the CME router.

```
app_faxmail_onramp.2.0.1.3.tcl
app_fax_detect.2.1.2.2.tcl
```

```
uc01tra#copy tftp flash:
Address or name of remote host []? 192.168.10.10
Source filename []? app_faxmail_onramp.2.0.1.3.tcl
Destination filename [app_faxmail_onramp.2.0.1.3.tcl]
```

- Enable TCP script application for T.37 faxing

```
application
service onramp flash:app_faxmail_onramp.2.0.1.3.tcl
service fax_detect flash:app_fax_detect.2.1.2.2.tcl
param fax-dtmf 2
param mode listen-first
param voice-dtmf 1
```

- Configure Fax to Email using T.37
- IP of mail server (SMTP; TCP/25) will be 192.168.10.10
- Specify the subject of the email to read "You Received a Fax!"
- Specify other parameters such as postmaster email address, mail-from, and aliases

```
fax interface-type fax-mail
mta send server 192.168.10.10 port 25
mta send subject You Received a Fax!
mta send with-subject both
mta send postmaster sales@routehub.local
mta send mail-from hostname routehub.local
mta send mail-from username IncomingFax
mta send return-receipt-to hostname routehub.local
mta send return-receipt-to username ROUTEHUB
mta receive aliases routehub.local
mta receive aliases 192.168.10.10
mta receive maximum-recipients 10
mta receive generate permanent-error
```


- FXO port 0/1/0 is connected to PSTN.
- Any incoming call (voice or fax) is forwarded to 6700

```
voice-port 0/1/0
supervisory disconnect dualtone pre-connect
pre-dial-delay 0
no vad
timeouts call-disconnect 2
timeouts wait-release 2
connection plar opx 6700
caller-id enable
```

- All incoming calls are sent to the following dial-peer from the FXO port 0/1/0
- It will use the TCL script to determine if the call is a voice call or a fax call

```
dial-peer voice 100 pots
service fax_detect
destination-pattern 9.T
incoming called-number 6700
direct-inward-dial
port 0/1/0
```

- Configure a MMIOIP dial peer for fax-to-email if the incoming call to FXO port 0/1/0 is a fax
- Send converted fax message to email address sales@routehub.local

```
dial-peer voice 7 mmoip
description FAX
service fax_on_vfc_onramp_app out-bound
destination-pattern 6700
information-type fax
session target mailto:sales@routehub.local
```

Fax to Email using T.37 (FAX on a different FXO port)

- Download the following TCL scripts from the Cisco software center then copy them to the flash memory of the CME router.

app_faxmail_onramp.2.0.1.3.tcl

uc01tra#copy tftp flash:

Address or name of remote host []? 192.168.10.10

Source filename []? app_faxmail_onramp.2.0.1.3.tcl

Destination filename [app_faxmail_onramp.2.0.1.3.tcl]

- Enable TCP script application for T.37 faxing

application

service onramp flash:app_faxmail_onramp.2.0.1.3.tcl

param fax-dtmf 2

param mode listen-first

param voice-dtmf 1

- Configure Fax to Email using T.37
- IP of mail server (SMTP; TCP/25) will be 192.168.10.10
- Specify the subject of the email to read "You Received a Fax!"
- Specify other parameters such as postmaster email address, mail-from, and aliases

fax interface-type fax-mail

mta send server 192.168.10.10 port 25

mta send subject You Received a Fax!

mta send with-subject both

mta send postmaster sales@routehub.local

mta send mail-from hostname routehub.local

mta send mail-from username IncomingFax

mta send return-receipt-to hostname routehub.local

mta send return-receipt-to username ROUTEHUB

mta receive aliases routehub.local

mta receive aliases 192.168.10.10

mta receive maximum-recipients 10

mta receive generate permanent-error

- FXO port 0/1/1 is connected to PSTN.
- All incoming fax calls are forwarded to 6700

```
voice-port 0/1/1  
connection plar opx 6700  
caller-id enable
```

- All incoming calls are sent to the following dial-peer from the FXO port 0/1/1
- It will use the TCL script for receiving fax calls

```
dial-peer voice 101 pots  
service onramp  
incoming called-number 6700  
direct-inward-dial  
port 0/1/1
```

- Configure a MMIOIP dial peer for fax-to-email if the incoming call to FXO port 0/1/0 is a fax
- Send converted fax message (TIFF format) to email address sales@routehub.local

```
dial-peer voice 7 mmioip  
description FAX  
service fax_on_vfc_onramp_app out-bound  
destination-pattern 6700  
information-type fax  
session target mailto:sales@routehub.local
```

Cisco CME using Exchange 2007 UM

- Configuration for Cisco CME to use Exchange UM for Voicemail and Unified Messaging.
- 6711 (for voicemail) and 6712 (for AA) will exist on the Exchange UM server
- IP of Exchange Server is 192.168.10.10
- SIP connection will exist between CME and Exchange UM

```
interface Vlan10
description Voice network
ip address 192.168.10.1 255.255.255.0
```

```
voice service voip
allow-connections sip to sip
supplementary-service h450.12
sip
bind control source-interface Vlan10
bind media source-interface Vlan10
header-passing
```

```
dial-peer voice 303 voip
description EXCH-UM
destination-pattern 671[1-2]
session protocol sipv2
session target ipv4:192.168.10.10
session transport tcp
dtmf-relay rtp-nte
codec g711alaw
```

PLAR

- Send all incoming calls from voice port 0/1/0 to extension 6000

```
voice-port 0/1/0
connection plar 6000
```

Using a XML Menu File For Phone Services

- Create two XML files (menu.xml) consisting of the phone service URLs (VoiceView, BerBee).
- Upload "menu.xml" to a web server.

! XML file (menu.xml) consisting of phone service URLs (VoiceView, BerBee)

```
<?xml version="1.0" encoding="utf-8" ?>
<CiscoIPPhoneMenu>
  <Title>Phone Services</Title>
  <Prompt>Please make your selection.</Prompt>
  ! phone service for VoiceView
  <Menuitem>
    <Name>VoiceView</Name>
    <URL>http://192.168.10.2/voiceview/common/login.do</URL>
  </Menuitem>
  ! phone service for Berbee
  <Menuitem>
    <Name>Weather,News,Stocks</Name>
    <URL>http://phone-xml.berbee.com/menu.xml</URL>
  </Menuitem>
</CiscoIPPhoneMenu>
```

- Configure CME to point to the menu.xml file on our web server (www.routehub.local)
- Reset all phones to use the new Phone Services location

telephony-service

```
url services http://www.routehub.local/menu.xml Phone Services
restart all
```

MoH Port on Cisco UC520

- Default configuration on Cisco UC520 to use the MoH port

```
voice-port 0/4/0
auto-cut-through
signal immediate
input gain auto-control -15
description Music On Hold Port
```

```
dial-peer voice 5 pots
description ** MOH Port **
destination-pattern ABC
port 0/4/0
no sip-register
```

```
ephone-dn 9
number BCD no-reg primary
description MoH
moh ip 239.10.16.8 port 2139 out-call ABC
```

Num Exp

- Not applicable for incoming call translations. Only when digits are dialed internally
- When a user dials 6778 it will translate/forward the call to extension 201

num-exp 6778 201

Monitor and Watch

- Monitor: monitor the line status (in-use or not) for another extension used by a user.
- Watch: to watch all lines on another phone configured to primary directory number on that phone.
- For the receptionist phone (ephone 10) on button 2, watch all activities on the phone that is using extension 6701 (using ephone-dn 11) for their primary extension (on line 1). One button 3, monitor the line status of extension 6702 (using ephone-dn 12)

ephone-dn 10 dual-line
number 6700
label 6700 (Main)
description 2091236700
call-forward busy 6000
call-forward noan 6000 timeout 15

ephone-dn 11 dual-line
number 6701
label 6701 (User1)
description 2091236701
call-forward busy 6000
call-forward noan 6000 timeout 15

ephone-dn 12 dual-line
number 6702
label 6702 (User2)
description 2091236702
call-forward busy 6000
call-forward noan 6000 timeout 15

ephone 10
button 1:10 2w11 3m12

Presence

- Enable directory number 6701 to be watched by the Presence service
- Cisco Phone, using ephone 1, can monitor extension 6701 (ephone-dn 11)

```
sip-ua  
presence enable
```

```
presence  
max-subscription 100  
presence call-list
```

```
ephone-dn 11  
number 6701  
label 6701 (User1)  
allow watch
```

```
ephone 1  
blf-speed-dial 1 6701 label "Duncan Rockwell"
```

Parallel Hunt Group (Call Blast)

- Configure hunt group that will call all extensions and numbers configured in the hunt group at the same time.
- The extensions/numbers in the hunt group will be: 6702, 6700, and 919252302203
- The hunt group pilot number will be 6701

```
voice hunt-group 1 parallel  
list 6702, 6700, 919252302203  
pilot 6701
```

Whisper Intercom

- *Whisper Intercom allows a user to intercom to a busy extension*
- Perform a Whisper Intercom call to extension 6701 which will be labeled as "User1"
- Assign Whisper Intercom speed-dial to button 2 on the Cisco Phone (using ephone 1)

```
ephone-dn 10  
number 6700  
whisper intercom speed-dial 6701 label "User1"
```

```
ephone 1  
button 1:1 2:10
```

After Hours

- If any call placed by a user begins with "91" which would be an outside call after hours, it will be blocked
- If any person dials 1-900 numbers any time of the day, will be blocked
- Define After hour calling through CME starting at 7PM and ends at 8AM
- Phone1 (ephone 1) will use the after-hours rules
- Phone2 (ephone 2) will not use any of the after hour rules
- Phone3 (ephone 3) can input PIN number 677 to place calls except for 1-900 numbers

```
telephony-service  
after-hours block pattern 1 91  
after-hours block pattern 2 91900 7-24  
after-hours day mon 19:00 8:00  
after-hours day tue 19:00 8:00  
after-hours day web 19:00 8:00  
after-hours day thu 19:00 8:00  
after-hours day fri 19:00 8:00  
after-hours day sat 00:00 24:00  
after-hours day sun 00:00 24:00
```

```
ephone 1
```

```
ephone 2  
after-hours exempt
```

```
ephone 3  
pin 677
```


Transfer Pattern (.T)

- Allow call transfers to any calling destination

```
telephony-service  
transfer-pattern .T
```

Call Forward Max Length

- Extension 6700 can only forward a call with 4-digits or less. Anything beyond 4 digits will be dropped.
- Example: Extension 6700 can forward calls to extension 6701, but not to a Local or Long Distance number

```
ephone-dn 10  
number 6700  
call-forward max-length 4
```

```
ephone 1  
button 1:1
```

Enhanced Music On Hold

- Configure two groups (Consulting & Training) that will use a different MOH audio stream
- MOH group 1 will be for the Consulting group. User using extension 6700 will exist in this MOH group.
- MOH group 2 will be for the Training group. User using extension 6701 will exist in this MOH group
- Any phone not assigned to a MOH group will use the default MOH audio file (music-on-hold.au)

telephony-service

moh music-on-hold.au

voice moh-group 1

description Consulting for MOH

moh music-on-hold-consulting.au

multicast moh 239.1.1.1 port 2000

ephone-dn 10

number 6700

moh-group 1

voice moh-group 2

description Training for MOH

moh music-on-hold-training.au

multicast moh 239.1.1.2 port 2000

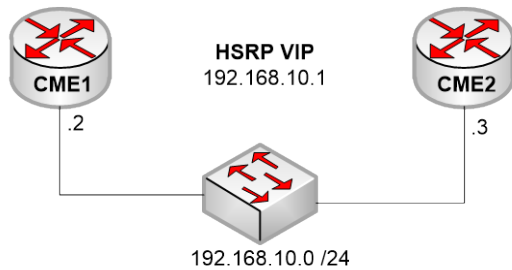
ephone-dn 11

number 6701

moh-group 2

IP Phone Redundancy Using HSRP

- Configure CME redundancy using HSRP
- The HSRP IP of 192.168.10.1 will be the source address used for Cisco Phones
- Primary CME router will be CME1. The Secondary will be CME2



```
>>CME1<<
interface fastethernet0/1
ip address 192.168.10.2 255.255.255.0
standby ip 192.168.10.1
standby priority 150
standby preempt
```

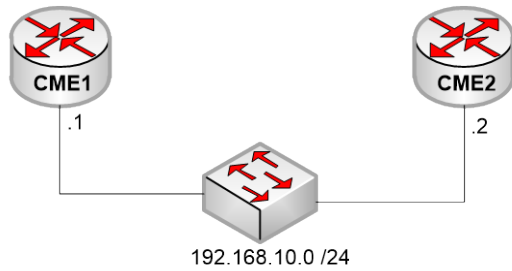
```
telephony-service
ip source-address 192.168.10.1 port 2000
```

```
>>CME2<<
interface fastethernet0/1
ip address 192.168.10.3 255.255.255.0
standby ip 192.168.10.1
standby priority 100
```

```
telephony-service
ip source-address 192.168.10.1 port 2000
```

IP Phone Redundancy using Secondary CME

- Configure CME redundancy using the Secondary command
- Primary CME router will be CME1 (192.168.10.1) and the Secondary will be CME2 (192.168.10.2)

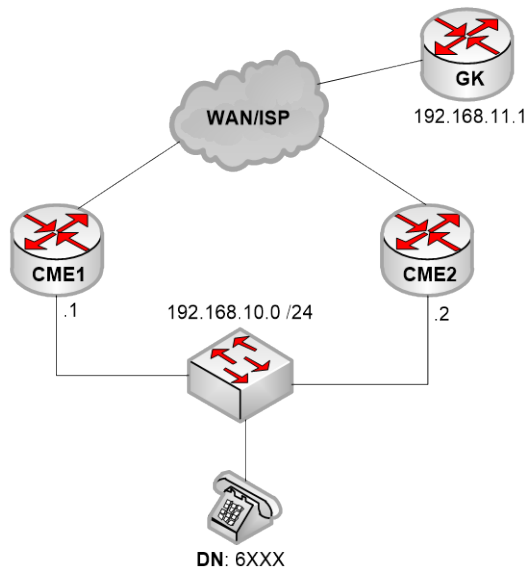


telephony-service

ip source-address 192.168.10.1 port 2000 secondary 192.168.10.2

Redundant CME using Gatekeepers

- CME1 and CME2 pointing to H.323 Gatekeeper Router (192.168.11.1)



>>CME1<<

```
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0
h323-gateway voip interface
h323-gateway voip id siteA ipaddr 192.168.11.1 1719
h323-gateway voip h323-id CME1
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 192.168.10.1
```

>>CME2<<

```
interface FastEthernet0/1
ip address 192.168.10.2 255.255.255.0
h323-gateway voip interface
h323-gateway voip id siteA ipaddr 192.168.11.1 1719
h323-gateway voip h323-id CME2
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 192.168.10.2
```

- Define the local zone for the site with the CME routers as "TRA"
- Specify primary call routing to IP Phones using 6XXX extensions through CME1 (access code is 8)
- Specify secondary call routing to IP Phones using 6XXX extensions through CME2 (access code is 8)

>>GK<<

```
gatekeeper
zone local TRA routehub.local 192.168.11.1
zone prefix TRA 86... gw-priority 10 CME1
zone prefix TRA 86... gw-priority 9 CME2
zone gw-type prefix 1# default-technology
```

VoiceView

- Enable VoiceView on CUE

```
service voiceview
enable
session idletimeout 30
end
```

- Add URL for VoiceView authentication on CME router
- Enable VoiceView URL on CME to be accessed under Phone Services

```
telephony-service
url authentication http://192.168.10.2/voiceview/authentication/authenticate.do
http://192.168.10.2/voiceview/common/login.do
```

MWI on Second Line

- Enable MWI red-light notification if a new voicemail comes in for the extension on line 2 (using ephone-dn 15)

```
ephone 10
1:14 2:15
mwi-line 2
```

IP Phone Backlight Display

- Keeps the backlight turned on instead of turning off on the Cisco Phone display

```
Router(config)# telephony-service
Router(config-telephony)# service phone displayOnWhenIncomingCall 1
```

SIP: Call Transfer

- CME by default will send a SIP REFER message to the SIP server. Most Service SIP Provider don't support the REFER method, therefore, it must be forced on the CME to hairpin the call.

```
voice service voip
no supplementary-service sip refer
```

Class of Restriction (CoR)

- *1: Configure the CoR objects which are equivalent to partitions in Cisco UCM*
- We will define an object for each outgoing call type (911, TOLL, LOCAL, LONG DISTANCE)

```
dial-peer cor custom
name RHG-P-911
name RHG-P-TOLL-1800
name RHG-P-TOLL-1900
name RHG-P-LOCAL
name RHG-P-LD
```

- *2: Configure the CoR groups which are equivalent to a CSS in Cisco UCM*
- We will define an group for each outgoing call type (911, TOLL, LOCAL, LONG DISTANCE)
- We will configure a group for OPEN areas (Lobby, Break Room, Kitchen) allowing only 911 and Local calls
- We will configure a group for Executives (CEO, VP, Directors, Managers) allowing 911, Local, Toll and LD calls.
- We will configure a group for Employees allowing only 911, Local, and LD calls

```
dial-peer cor list RHG-CSS-EMERGENCY
member RHG-P-911
```

```
dial-peer cor list RHG-CSS-1800
member RHG-P-TOLL-1800
member RHG-P-TOLL-1900
```

```
dial-peer cor list RHG-CSS-LOCAL
member RHG-P-LOCAL
```

```
dial-peer cor list RHG-CSS-LD
member RHG-P-LD
```

```
dial-peer cor list RHG-CSS-OPEN
member RHG-P-911
member RHG-P-LOCAL
```

```
dial-peer cor list RHG-CSS-EXEC
member RHG-P-911
member RHG-P-LOCAL
member RHG-P-TOLL-1800
member RHG-P-TOLL-1900
member RHG-P-LD
```

```
dial-peer cor list RHG-CSS-EMPLOYEES
member RHG-P-911
member RHG-P-LOCAL
member RHG-P-LD
```


- *3: Associate CoR group to the correct dial peer based on its calling pattern*
- Apply Local CoR group to the Local Dial Peer (7)
- Apply Long Distance CoR group to the Long Distance Dial Peer (11)
- Apply 911 CoR group to the 911 Dial Peers (911, 9911)
- Apply 1-800 TOLL CoR group to the 1-800 TOLL Dial Peer (118)
- Apply 1-900 TOLL CoR group to the 1-900 TOLL Dial Peer (119)

```
dial-peer voice 7 pots
destination-pattern 9[2-9].....
port 0/3/0:23
forward-digits 7
corlist outgoing RHG-CSS-LOCAL
```

```
dial-peer voice 11 pots
destination-pattern 91[2-9]..[2-9].....
port 0/3/0:23
forward-digits 11
corlist outgoing RHG-CSS-LD
```

```
dial-peer voice 911 pots
destination-pattern 911
port 0/3/0:23
forward-digits 3
corlist outgoing RHG-CSS-EMERGENCY
```

```
dial-peer voice 9911 pots
destination-pattern 9911
port 0/3/0:23
forward-digits 3
corlist outgoing RHG-CSS-EMERGENCY
```

```
dial-peer voice 118 pots
destination-pattern 91800&
port 0/3/0:23
forward-digits 11
corlist outgoing RHG-CSS-TOLL-1800
```

```
dial-peer voice 119 pots
destination-pattern 91900&
port 0/3/0:23
forward-digits 11
corlist outgoing RHG-CSS-TOLL-1900
```

- 4: Associate CoR group to corresponding extension based if it is used for an OPEN area, used by an EXEC or EMPLOYEE
- Extension 1001 used by EMPLOYEE. Can make only make Local, LD and 911, 1-800, 1-900 calls
- Extension 1002 used for OPEN areas. Can make only make Local and 911 calls
- Extension 1003 used by EXECUTIVE. Can make any call (Local, LD, 911, 1-800, 1-900)
- Extension 1004 is not assigned to a CoR group, so can make any outgoing call without restrictions

ephone-dn 1
number 1001
cor incoming RHG-CSS-EMPLOYEES

ephone-dn 2
number 1002
cor incoming RHG-CSS-OPEN

ephone-dn 3
number 1003
cor incoming RHG-CSS-EXEC

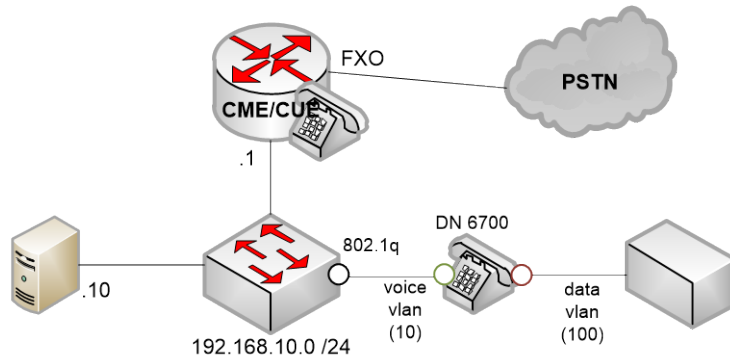
ephone-dn 4
number 1004

Monitor

show ephone-dn summary
show telephony-service dial-peer
show dial-peer cor
debug voip ccapi inout
debug ephone detail

CISCO UNITY EXPRESS

Solution/Services: Voice & Unified Communications
Related: Cisco UCM Express



Access to CUE

- Interface VLAN10 used for voice network
- CUE interface will use IP 192.168.10.2 (from VLAN10 interface) and default gateway pointing to the IP configured on the CME router (192.168.10.1)
- Configure static route for the CUE IP configured pointing to the service module

```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
```

```
interface Integrated-Service-Engine0/0
description ROUTEHUB: CUE interface
ip unnumbered Vlan10
ip nat inside
service-module ip address 192.168.10.2 255.255.255.0
service-module ip default-gateway 192.168.10.1
```

```
ip route 192.168.10.2 255.255.255.255 Integrated-Service-Engine0/0
```

- To console into the CUE module from the CME router. Done from the enable mode

```
service-module integrated-Service-Engine 0/0 session
```

Upgrade CUE to Version 7.x

- Specify FTP location, username, and password where CUE 7 files are located

software download server url ftp://192.168.10.10/cue7 username admin password cisco123

- Files to download from Cisco.com if using CUE 7.x and CUE on ISE (UC520)

The CUE zip file: cue-cm-k9.ise.7.0.1.zip

The Language pack: cue-vm-en_US-langpack.ise.7.0.1.prt1

The License file: cue-vm-license_50mbx_cme_7.0.1.pkg

- Download CUE version 7.0.1 package from FTP server
- Install CUE version 7.0.1 to CUE module

software download upgrade cue-vm-k9.ise.7.0.1.pkg

software install upgrade cue-vm-k9.ise.7.0.1.pkg

Copying Files to CUE via CLI

- Copy a file via FTP to the CCN subsystem. Here we are copying a new AA prompt file (AAprompt1.wav) to use on CUE
- FTP server with our prompt file is 192.168.10.10

ccn copy url ftp://192.168.10.10/AAprompt1.wav prompt AAPrompt1.wav

Base Configuration

- Base Configuration for initial configuration on CUE (hostname, domain_name, timezone, language)
- Create account "admin" and add to the group "Administrators"
- Create a new group called "Users" that all voicemail users will exist
- Enable SIP to CME router (default gateway for CUE)

```
hostname cue01tra
ip domain-name routehub.local
clock timezone America/Los_Angeles
system language preferred "en_US"
```

```
username admin create
groupname Administrators member admin
groupname Users create
```

```
ccn subsystem sip
gateway address "192.168.10.1"
end subsystem
```

Enable Voicemail Services

- Enable Voicemail application on CUE
- Support up to 6 concurrent voicemail sessions
- Specify voicemail pilot number to be 6000
- Enable MWI application for voicemail notification on CUE. MWI ON will use DN 8000 and MWI OFF will use DN 8001

```
ccn application voicemail
description "voicemail"
enabled
maxsessions 6
script "voicebrowser.aef"
parameter "logoutUri" "http://localhost/voicemail/vxmlscripts/mbxLogout.jsp"
parameter "uri" "http://localhost/voicemail/vxmlscripts/login.vxml"
end application
```

```
ccn trigger sip phonenumber 6000
application "voicemail"
enabled
maxsessions 6
end trigger
```

```
ccn application ciscoMWIapplication
description "ciscoMWIapplication"
enabled
maxsessions 4
script "setmwi.aef"
```

```
parameter "CallControlGroupID" "0"  
parameter "strMWI_OFF_DN" "8001"  
parameter "strMWI_ON_DN" "8000"  
end application
```

Sending Calls to Voicemail (CUE)

- If a caller dials a number like extension 6700 and the line is busy ("busy") or not answered ("noan") the call will forward to the voicemail pilot (using 6000) on CUE (192.168.10.2)

```
dial-peer voice 600 voip  
destination-pattern 6000  
session protocol sipv2  
session target ipv4:192.168.10.2  
dtmf-relay sip-notify  
codec g711ulaw  
no vad
```

```
telephony-service  
voicemail 6000
```

```
ephone-dn 10 dual-line  
number 6700 no-reg primary  
call-forward busy 6000  
call-forward noan 6000 timeout 15
```

```
dial-peer voice 800 voip  
incoming called-number 800[0,1]....  
codec g711ulaw  
no vad
```

```
ephone-dn 20  
number 8000.... no-reg primary  
mwi on
```

```
ephone-dn 21  
number 8001.... no-reg primary  
mwi off
```

Create User Voice Mailboxes

- Create a voice mailbox for user at extension 6700 (DID: 12091236700).
- The user account name for this mailbox will be "routehub"
- Create mailbox supporting up to 420 seconds in total for all messages
- Maximum size for a single voicemail message will be 60 seconds
- Specify the default mailbox to be 420 seconds and default message size to be 240 seconds (if not defined under mailbox).

```
username routehub create
groupname Users member routehub
```

```
username routehub phonenumber "6700"
username routehub phonenumberE164 "12091236700"
```

```
voicemail mailbox owner "routehub" size 420
description "User DN6700 mailbox"
messagesize 60
end mailbox
```

```
voicemail callerid
voicemail default language en_US
voicemail default mailboxsize 420
voicemail broadcast recording time 300
voicemail default messagesize 240
voicemail notification restriction msg-notification
voicemail operator telephone 0
```

- Configure full name to support "Dial-by-Name" dialing.
- Done in the enable mode and NOT the config mode

```
username routehub fullname first Routehub last Group display "RHG" password cisco6778
```

Basic Auto Attendant (AA)

- AA pilot number will be 6003.
- One CME router, all calls coming into FXO port 0/0/3 will be forwarded to 6003 which will match its dial-peer pointing to the CUE module via SIP

```
voice-port 0/0/3
supervisory disconnect dualtone pre-connect
pre-dial-delay 0
no vad
timeouts call-disconnect 2
timeouts wait-release 2
connection plar 6003
caller-id enable
```

```
dial-peer voice 600 voip
destination-pattern 6...
session protocol sipv2
session target ipv4: 192.168.10.2
dtmf-relay sip-notify
codec g711ulaw
no vad
```

- Default AA script configuration
- Enable AA application on CUE
- Support up to 6 concurrent sessions to the AA
- Define AA pilot number to be 6003

```
ccn application autoattendant aa
description "autoattendant"
enabled
maxsessions 6
script "aa.aef"
parameter "busClosedPrompt" "AABusinessClosed.wav"
parameter "holidayPrompt" "AAHolidayPrompt.wav"
parameter "welcomePrompt" "AAWelcome.wav"
parameter "disconnectAfterMenu" "false"
parameter "dialByFirstName" "false"
parameter "allowExternalTransfers" "false"
parameter "MaxRetry" "3"
parameter "dialByExtnAnytime" "false"
parameter "busOpenPrompt" "AABusinessOpen.wav"
parameter "businessSchedule" "systemschedule"
parameter "dialByExtnAnytimeInputLength" "4"
parameter "operExtn" "0"
end application
```

```
ccn trigger sip phonenumber 6003
application "autoattendant"
enabled
locale "en_US"
maxsessions 4
end trigger
```


- Prompt Management: used for creating custom prompts for the AA menu
- Enable prompt management application on CUE
- Prompt Management pilot will be 6006

```
ccn application promptmgmt
description "promptmgmt"
enabled
maxsessions 1
script "promptmgmt.aef"
end application
```

```
ccn trigger sip phonenummer 6006
application "promptmgmt"
enabled
idletimeout 5000
locale "en_US"
maxsessions 1
end trigger
```

Resetting CUE Mailbox PIN

- Done from the EXEC mode, not the config mode
- Reset CUE mailbox user "U103" PIN to 103

```
username U103 pin 103
```

Voicemail Email Notifications

- Enable Voicemail notification
- When a new voicemail is left for user "routehub" at 6700 send email to vm@routehub.local
- The "from" email address for voicemail emails will be support@routehub.local
- The Mail server is 192.168.10.10 and doesn't require any authentication

```
voicemail notification enable
voicemail notification preference all
voicemail notification allow-login
voicemail notification email attach
```

```
smtp server address 192.168.10.10 authentication none
```

```
voicemail configuration outgoing-email from-address support@routehub.local
```

```
username routehub create
username routehub phonenumber "6700"
```

```
voicemail notification owner routehub enable
```

- Apply the following at the enable mode and not the config mode

```
username routehub profile VM-6700 email address vm@routehub.local
username routehub profile VM-6700 email enable
username routehub profile VM-6700 email preference all
username routehub profile VM-6700 email attach
username routehub profile VM-6700 email schedule day 1 active from 01:00 to 24:00
username routehub profile VM-6700 email schedule day 2 active from 01:00 to 24:00
username routehub profile VM-6700 email schedule day 3 active from 01:00 to 24:00
username routehub profile VM-6700 email schedule day 4 active from 01:00 to 24:00
username routehub profile VM-6700 email schedule day 5 active from 01:00 to 24:00
username routehub profile VM-6700 email schedule day 6 active from 01:00 to 24:00
username routehub profile VM-6700 email schedule day 7 active from 01:00 to 24:00
```

```
show voicemail notification owner routehub profile
show voicemail notification owner routehub email
```

Live Record

- Configure softkey template to include Live Record (LiveRcd) when a call is connected.
- Apply that template to a phone that will use Live record and reset the phone

```
ephone-template 1  
softkeys connected LiveRcd Confm Hold Park Trnsfer TrnsfVM
```

```
ephone 1  
ephone-template 1  
reset
```

- Specify Live Record number which will be 6005
- Make sure Voicemail pilot number, in our case will be 6000, is also configured.
- Configure 6005 as a directory number that will forward directly to CUE.

```
telephony-service  
live-record 6005  
voicemail 6000
```

```
ephone-dn 16  
number 6005  
call-forward all 6000
```

```
dial-peer voice 600 voip  
destination-pattern 6...  
session protocol sipv2  
session target ipv4:192.168.10.2  
dtmf-relay sip-notify  
codec g711ulaw  
no vad
```

- Configured on CUE
- The number of seconds a beep will occur during a recorded call will be "1000" seconds
- Specify Live Record pilot number to be 6005

```
voicemail live-record beep duration 1000  
voicemail live-record pilot-number 6005
```

COMMITTED ACCESS RATE (CAR)

Solution/Services: QoS: Policing
Related:

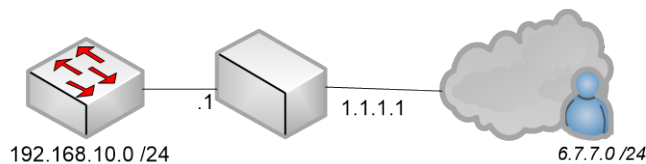
Go to [“QoS: Policing”](#)

CONTENT FILTERING

Solution/Services: Security: Content Filtering
Related:

Cisco IOS URL Filtering using Web Sense

- Enable HTTP content filtering using a WebSense server (192.168.10.10) located on the LAN.
- Any access on youtube.com should be blocked.
- Any access to www.routehub.local should be always permitted
- Apply URL filtering on LAN interface that user's are connected to



```
ip inspect name websec http urlfilter
```

```
ip urlfilter cache 5
```

```
ip urlfilter exclusive-domain deny .youtube.com
```

```
ip urlfilter exclusive-domain permit www.routehub.local
```

```
ip urlfilter audit-trail
```

```
ip urlfilter alert
```

```
ip urlfilter server vendor websense 192.168.10.10
```

```
interface Vlan10
```

```
ip address 192.168.10.1 255.255.255.0
```

```
ip inspect websec in
```

CBWFQ

Solution/Services: QoS: Queuing and Dropping
Related:

Go to [“QoS: Queuing and Dropping”](#)

COPY

Solution/Services: Administration/System
Related:

Copy using FTP

- *Alternative to TFTP, more reliable using TCP instead of UDP*
- Copy active config file to FTP server (192.168.10.10) using the account admin & cisco123

```
copy running-config ftp://admin:cisco123@192.168.10.10
```

Copy and Install TAR File

- Used with some Cisco Catalyst Switches and Access Points
- Copy, extract, and install TAR images with HTTP and IOS bin files

```
archive tar /xtract tftp://192.168.10.10/c1200-k9w7-tar.123-8.JA2.tar flash:
```

Copying a Config from Flash to DRAM

- Copy custom config file CS01.cfg stored in the folder "RHG" (on the flash memory) to the running config (DRAM)

```
Switch#copy flash:RHG/CS01.cfg running-config
```

CRTP

Solution/Services: QoS: Life Efficiencies

Related:

Go to [“QoS: Link Efficiencies”](#)

[D]

DAMPING

Solution/Services: Feature

Related: N/A

- Controls the rate in which the interface state changes are propagated to the routing protocols in the event of a flapping link condition. This should be enabled on all L3 interfaces on the LAN/Data Center network.

```
interface GigabitEthernet1/1  
  dampening
```

DEFAULT INTERFACE

Solution/Services: Administration/System

Related: N/A

- Removes all configuration from interface (factory default)

default interface serial 0/0

DELETE

Solution/Services: Administration/System

Related: N/A

Deleting a Directory in the Flash Memory

- Removes the directory titled "MyFiles" in the flash memory of a Cisco IOS device

```
delete /force /recursive flash:MyFiles
```

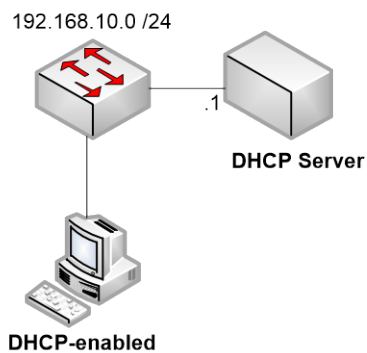
DHCP

Solution/Services: Feature

Related: N/A

DHCP Server on Cisco IOS

- Enable DHCP server on Cisco IOS L3 device
- Define DHCP scope for 192.168.10.0 (192.168.10.10 – 192.168.10.254)

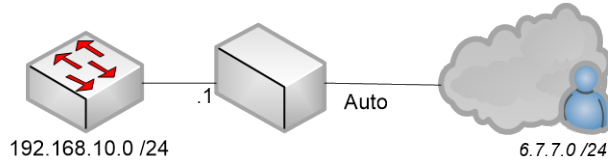


```
ip dhcp excluded-address 192.168.10.1 192.168.10.9
```

```
ip dhcp pool RHG-DHCP
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 192.168.10.10
domain-name routehub.local
lease infinite
```

DHCP on Cisco Interface

- Enable interface FE4 to get it's IP Address via DHCP



```
interface FastEthernet4  
ip address dhcp
```

DHCP SNOOPING

Solution/Services: LAN Switching

Related: N/A

- Enable DHCP snooping on Access Switch for VLANs 10 and 11
- Trust DHCP requests from uplink interface to the Core switch



>>ACCESS<<

no ip dhcp snooping information option

ip dhcp snooping vlan 10-11

ip dhcp snooping

interface GigabitEthernet0/1

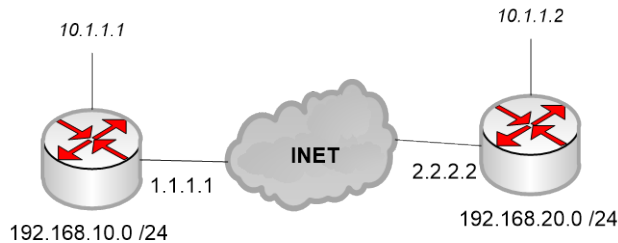
ip dhcp snooping limit rate 100

ip dhcp snooping trust

DMVPN

Solution/Services: Security: VPN

Related:



DMVPN

- Configure router on the left (see picture above) as the DMVPN hub router that DMVPN spokes can connect to.
- Tunnel Interface IP for Hub router will be 10.1.1.1
- WAN facing interface is FastEthernet4
- Configure static route pointing to the network 192.168.20.0 via 10.1.1.2 (the DMVPN spoke)

>> DMVPN HUB <<

```
crypto keyring dmvpnspokes
pre-shared-key address 0.0.0.0 0.0.0.0 key RHGauth

crypto isakmp policy 10
encr 3des
authentication pre-share
group 2

crypto ipsec transform-set ipsec-ts esp-3des esp-md5-hmac
mode transport

crypto isakmp profile dmvpn-isakmp
keyring dmvpnspokes
match identity address 0.0.0.0

crypto ipsec profile dmvpn
set security-association lifetime seconds 120
set transform-set ipsec-ts
set isakmp-profile dmvpn-isakmp
```

```

interface Tunnel0
ip address 10.1.1.1 255.255.255.0
no ip redirects
ip mtu 1412
ip nhrp authentication RHGauth
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 300
ip tcp adjust-mss 1360
tunnel source FastEthernet4
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile dmvpn

```

```
ip route 192.168.20.0 255.255.255.0 10.1.1.2
```

- Configure router on the right (see picture above) as the DMVPN spoke router. Other spoke routers would have a similar configuration to this one.
- Tunnel Interface IP for Spoke router will be 10.1.1.2
- DMVPN Hub router IP is 10.1.1.1
- WAN facing interface is FastEthernet4
- Configure static route pointing to the network 192.168.10.0 via 10.1.1.1 (the DMVPN spoke)

>> DMVPN SPOKE <<

```

crypto isakmp policy 10
encr 3des
authentication pre-share
group 2

```

```

crypto isakmp key RHGauth address 0.0.0.0 0.0.0.0
crypto isakmp xauth timeout 45

```

```

crypto ipsec transform-set ipsec-ts esp-3des esp-md5-hmac
mode transport

```

```

crypto ipsec profile dmvpn
set security-association lifetime seconds 120
set transform-set ipsec-ts

```

```

interface Tunnel0
ip address 10.1.1.2 255.255.255.0
no ip redirects
ip mtu 1412
ip nhrp authentication RHGauth
ip nhrp map multicast dynamic
ip nhrp map 10.1.1.1 1.1.1.1
ip nhrp map multicast 1.1.1.1
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp nhs 10.1.1.1

```



```
ip nhrp cache non-authoritative
ip tcp adjust-mss 1360
tunnel source FastEthernet4
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile dmvpn

ip route 192.168.10.0 255.255.255.0 10.1.1.1
```

>> MONITOR <<

>> DMVPN Hub

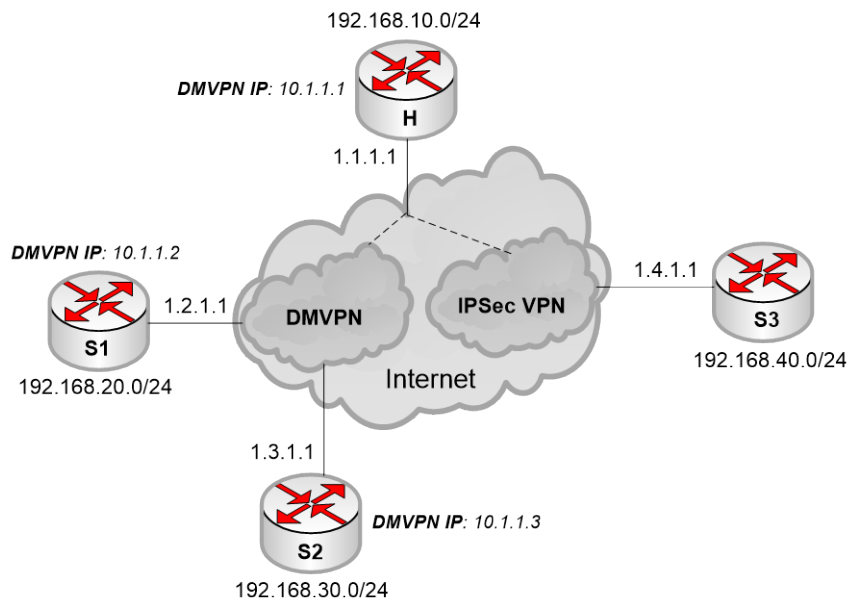
```
show ip nhrp
show ip nhrp multicast
```

>> DMVPN Spoke

```
show ip nhrp nhs
show ip nhrp
show ip nhrp multicast
```

Using DMVPN and IPsec VPN Tunnels

- HQ: configured for DMVPN and IPsec VPN tunnels ; LAN: 192.168.10.0/24, WAN: 10.1.1.1 (for DMVPN)
- S1: configured for DMVPN ; LAN: 192.168.20.0/24, WAN: 10.1.1.2 (for DMVPN)
- S2: configured for DMVPN ; LAN: 192.168.30.0/24, WAN: 10.1.1.3 (for DMVPN)
- S3: configured for IPsec VPN only ; LAN: 192.168.40.0/24



- General VPN and Interface configuration on HQ router

```
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0
no ip redirects
no ip unreachables
no ip proxy-arp
```

```
interface FastEthernet0/0
ip address 1.1.1.1 255.255.255.0
no ip redirects
no ip unreachables
no ip proxy-arp
```

```
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
```

```
crypto isakmp policy 20
encr aes
authentication pre-share
group 2
lifetime 28800
```

- DMVPN (Hub) configuration on HQ router

```
crypto keyring dmvpnspokes  
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

```
crypto isakmp profile dmvpn-isakmp  
keyring dmvpnspokes  
match identity address 1.2.1.1 255.255.255.255  
match identity address 1.3.1.1 255.255.255.255
```

```
crypto ipsec profile dmvpn  
set security-association lifetime seconds 120  
set transform-set ipsec-ts  
set isakmp-profile dmvpn-isakmp
```

```
crypto ipsec transform-set ipsec-ts esp-3des esp-md5-hmac  
mode transport
```

```
interface Tunnel0  
ip address 10.1.1.1 255.255.255.0  
no ip redirects  
ip mtu 1412  
ip nhrp authentication cisco123  
ip nhrp map multicast dynamic  
ip nhrp network-id 1  
ip nhrp holdtime 300  
ip tcp adjust-mss 1360  
tunnel source FastEthernet0/0  
tunnel mode gre multipoint  
tunnel key 0  
tunnel protection ipsec profile dmvpn
```

```
ip route 192.168.20.0 255.255.255.0 10.1.1.2  
ip route 192.168.30.0 255.255.255.0 10.1.1.3
```

- Static IPSec VPN configuration on HQ router

```
crypto isakmp key cisco123 address 1.4.1.1 no-xauth  
crypto isakmp invalid-spi-recovery  
crypto isakmp keepalive 20 10  
crypto isakmp xauth timeout 45
```

```
crypto ipsec transform-set ipsec-ts2 esp-3des esp-sha-hmac
```

```
ip access-list extended ACL-IPSEC-VPN  
permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
```

```
crypto map vpnmap 5 ipsec-isakmp  
set peer 1.4.1.1  
set transform-set ipsec-ts2  
set pfs group2  
match address ACL-IPSEC-VPN
```

```
interface FastEthernet0/0
ip address 1.1.1.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
crypto map vpnmap
```

- For the other sites, S1 and S2 will have a standard DMVPN configuration pointing to the HQ site
- For site S3, this will have a standard IPsec VPN configuration pointing to the HQ site and using the same ISAKMP key of "cisco123"

DO

Solution/Services: Administration/System

Related:

- Run "show" commands from configuration mode

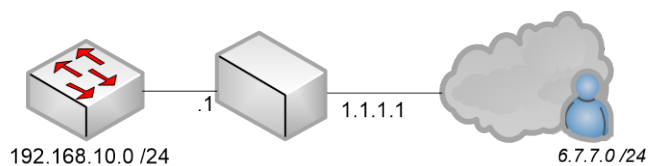
Router(config)#do show ip route

DS-3

Solution/Services: Media Connection
Related:

Serial DS3

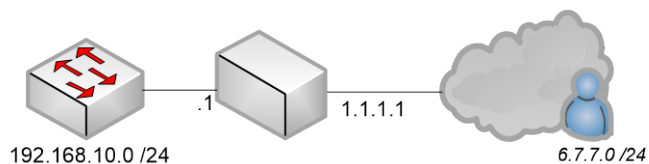
- Serial DS3+ port adapter in a Cisco 7200 series router



```
interface serial 1/0
ip address 1.1.1.1 255.255.255.252
encapsulation ppp
framing c-bit
cablelength 50
dsu bandwidth 44210
clock source internal
serial restart-delay 0
```

HSSI

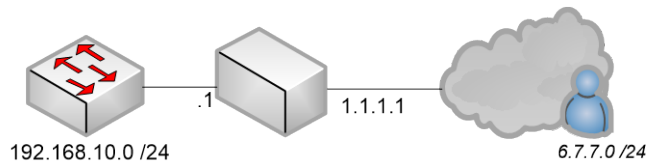
- HSSI interface enabled for PPP with service provider



```
interface Hssi1/0
ip address 1.1.1.1 255.255.255.0
encapsulation ppp
serial restart-delay 0
```

ATM Interface

- Two configuration examples using an DS-3 ATM interface (e.g. Cisco 7200) configured with an ATM PVC to the service provider



```
interface ATM2/0
description DS-3 6Mbps connection to Internet
ip address 1.1.1.1 255.255.255.252
ip accounting output-packets
atm scrambling cell-payload
atm framing cbitplcp
no atm ilmi-keepalive
pvc RHG 5/101
protocol ip 1.1.1.2 broadcast
vbr-nrt 6000 6000
```

OR

```
interface ATM1/0
description DS-3 6Mbps connection to Internet
ip address 1.1.1.1 255.255.255.252
ip accounting output-packets
load-interval 60
atm scrambling cell-payload
no atm ilmi-keepalive
pvc SVB 5/101
vbr-nrt 6000 6000
```

DYNAMIC ARP INSPECTION

Solution/Services: LAN Switching

Related: N/A

- Enable Dynamic ARP Inspection (DAI) on Access Switch for VLANs 10 and 11
- Disable DAI on uplink interface to the Core switch



>>ACCESS<<

```
ip arp inspection vlan 10-11
ip arp inspection validate ip
```

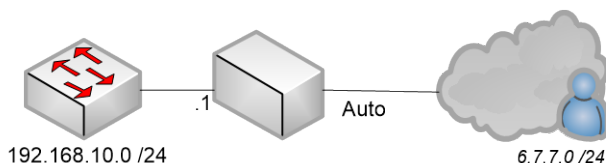
```
interface GigabitEthernet0/1
ip arp inspection limit rate 100
ip arp inspection trust
```


DYNAMIC DNS (DDNS)

Solution/Services: Feature
Related:

DDNS on Cisco IOS

- Requires a DDNS account to be created with a DDNS provider (e.g. dyndns.org)
- DDNS account details: user1 / cisco123
- DDNS server/URL: members.dyndns.org/nic/update
- DDNS domain name for account: rhg-er01.selfip.com
- FE4 interface enabled for DHCP and DDNS. The new IP dynamically configured on FE4 will be synchronized to DDNS service every day for DNS domain rhg-er01.selfip.com



```
hostname rhg-er01
```

```
ip ddns update method RHG-DDNS
```

```
HTTP
```

```
add http://user1:cisco123@members.dyndns.org/nic/update
```

```
<CTRL-V> then
```

```
?
```

```
system=dyndns&hostname=rhg-er01.selfip.com&myip=
```

```
interval maximum 1 0 0 0
```

```
interface FastEthernet4
```

```
ip ddns update hostname rhg-er01.selfip.com
```

```
ip ddns update RHG-DDNS host members.dyndns.org
```

```
ip address dhcp
```

[E]

EEM

Solution/Services: Network Management
Related: N/A

Interface monitoring and email notification

- If interface GE 8/1 on the Core switch goes down (based on a syslog event) run a TDR cable test on the port including running diagnostics (GOLD).
- Send an email to support@routehub.local that the interface went down
- Mail server IP is 192.168.10.10

event manager applet LINK_DOWN_MOD_8_1

event syslog pattern "%LINK-3-UPDOWN: Interface GigabitEthernet8/1" maxrun 20

action 1.0 cli command "en"

action 2.0 cli command "test cable-diagnostics tdr interface g8/1"

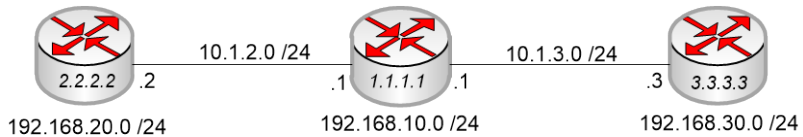
action 3.0 cli command "diagnostic start module 8 test 2 port 1"

action 4.0 mail server "192.168.10.10" to "support@routehub.local" from "Core Switch" subject "Urgent! Interface went down" body "G8/1 went down"

EIGRP

Solution/Services: IP Routing (IGP)

Related: N/A



EIGRP Routing

- Enables EIGRP routing process and place router into ASN 1
- Specify what routes to advertise and build neighbors with other EIGRP routers
- Disable auto-summarization for EIGRP

```
>>R1 (1.1.1.1)<<
```

```
router eigrp 1
network 192.168.10.0 0.0.255.255
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
network 1.1.1.1 0.0.0.0
no auto-summary
```

Passive Interface

- Disables OSPF routing for all interfaces on R1 except for FE0/1 and FE0/2

```
>>R1<<
```

```
router eigrp 1
passive-interface default
no passive-interface FastEthernet0/1
no passive-interface FastEthernet0/2
```

Neighbor Timers

- Configures sub-second timers (hello & hold timers) with neighbors for fast convergence

```
>>R1<<
interface FastEthernet0/1
ip hello-interval eigrp 1 1
ip hold-time eigrp 1 3
```

MD5 Authentication

- Define a key chain (e.g. SEIGRP) using the password cisco123
- Enable MD5 authentication and associate key-chain to EIGRP enabled interface with a connected neighbor

```
>>R1<<
key chain SEIGRP
key 1
key-string cisco123

interface FastEthernet0/1
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 SEIGRP
```

Changing Admin Distance

- Specify custom admin distance (internal and external routes)

```
router eigrp 1
distance eigrp 90 170
```

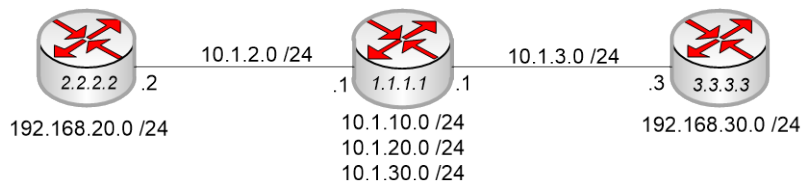
Maximum Paths Per Route

- Define the number of paths for a single route to injected into the routing table

```
router eigrp 1
maximum-paths 2
```

Route Summarization

- Summarizes all subnets 10.1.x.x as 10.1.0.0/16 and advertise summarized route to R2 (2.2.2.2)



```
>>R1<<
interface FastEthernet0/1
ip summary-address eigrp 1 10.1.0.0 255.255.0.0 5
```

Bandwidth Utilization

- Define interface bandwidth usage to be 45% for EIGRP

```
interface FastEthernet0/1
ip bandwidth-percent eigrp 1 45
```

Route Control/Filtering

- Only advertise routes listed in the ACL to all neighbors

>>R1<<

```
ip access-list standard ACL-EIGRP-ROUTES
permit 192.168.10.0 0.0.0.255
permit 192.168.20.0 0.0.0.255
permit 192.168.30.0 0.0.0.255
```

```
router eigrp 1
  distribute-list ACL-EIGRP-ROUTES out
```

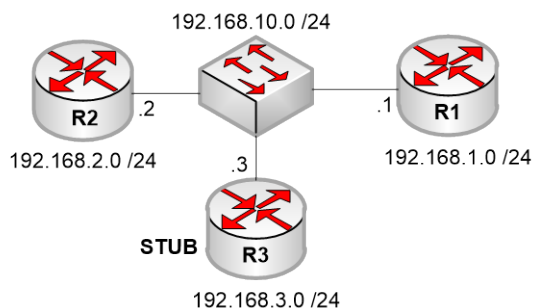
OR

- Only advertise routes listed in the ACL to all neighbors out of the interface FastEthernet0/1

```
router eigrp 1
  distribute-list ACL-EIGRP-ROUTES out FastEthernet0/1
```

EIGRP Stub

- Do not receive EIGRP queries nor act as a transit
- Configures R3 as a EIGRP stub router in ASN1 and will advertise its connected subnets (192.168.3.0/24)



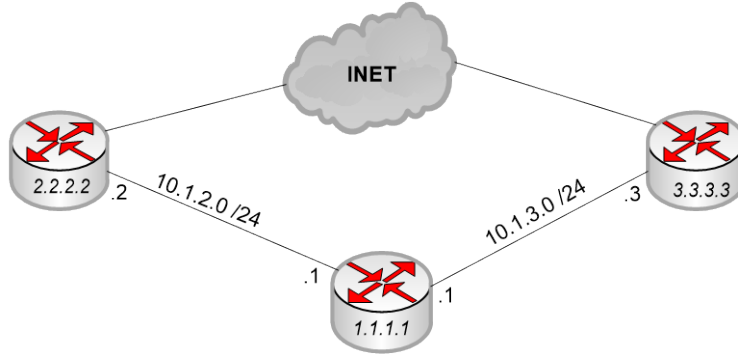
>> R3 <<

```
router eigrp 1
  eigrp stub connected
```

```
show ip eigrp neighbors detail <intf> <intf-id>
```

EIGRP Bandwidth and Delay

- On R1's FE0/1 configure delay on interface towards uplink to be more preferred ; no ECP
- On R1's FE0/2 configure delay on interface towards uplink to be less preferred ; no ECP

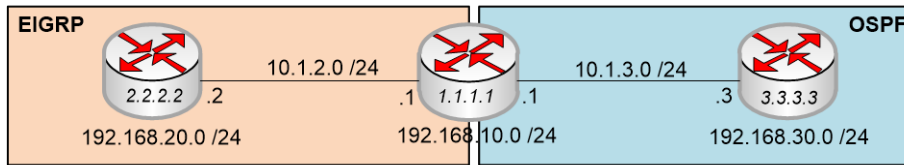


```
>>R1 (1.1.1.1)<<
interface FastEthernet0/1
ip address 10.1.2.1 255.255.255.0
delay 10

interface FastEthernet0/2
ip address 10.1.3.1 255.255.255.0
delay 100
```

Route Redistribution

- Redistribute OSPF routes that are listed in the ACL and Policy Map into EIGRP



```
>>R1 (1.1.1.1)<<
```

```
ip access-list standard ACL-OSPF-ROUTES  
permit 192.168.30 0.0.0.255
```

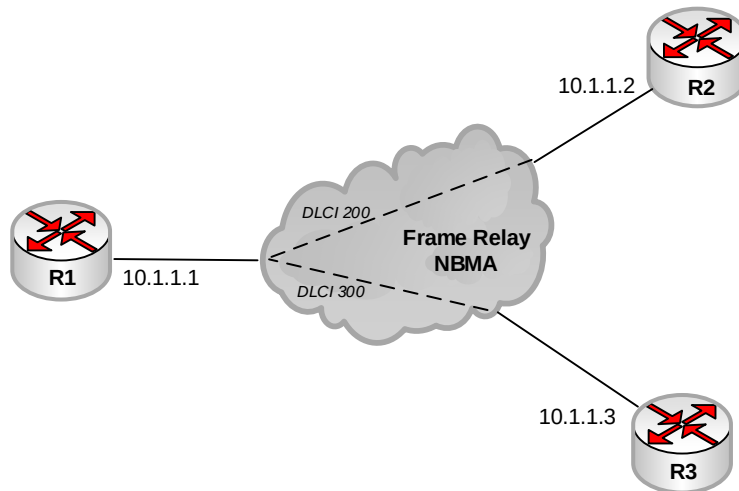
```
route-map RM-OSPF-ROUTES permit 10  
match ip address ACL-OSPF-ROUTES
```

```
router ospf 1  
network 10.1.3.0 0.0.0.255 area 0  
network 192.168.10.0 0.0.0.255 area 10
```

```
router eigrp 1  
network 192.168.10.0 0.0.0.255  
network 1.1.1.1 0.0.0.0  
network 10.1.2.0 0.0.0.255  
redistribute ospf 1 metric 1000 1 255 1 1500 route-map RM-OSPF-ROUTES
```


EIGRP on NBMA

- Enabling EIGRP over a Frame Relay NBMA network
- Disable EIGRP split horizon
- EIGRP neighbors defined under routing process matching the Frame Relay map statements under serial interface



```
>> R1 <<
interface Serial0/1
 ip address 10.1.1.1 255.255.255.0
 encapsulation frame-relay
 no ip split-horizon eigrp 10
 frame-relay map ip 10.1.1.2 200
 frame-relay map ip 10.1.1.3 300

router eigrp 10
 network 192.168.10.0 0.0.0.255
 network 10.1.1.0 0.0.0.255
 neighbor 10.1.1.2
 neighbor 10.1.1.3
```

NSF with EIGRP

- Enabling Non-Stop Forwarding (NSF) with the EIGRP routing process

```
router eigrp 1
```

```
nsf
```

ERROR DISABLE

Solution/Services: Administration/System

Related: N/A

Error Disable All

- Enable Error Disable recovery for all causes

`errdisable recovery cause all`

Error Disable for Individual Events

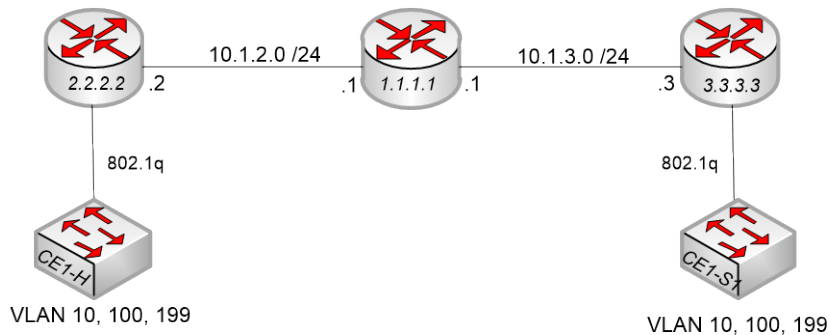
- Enable Error Disable recovery for individual events (based on what is supported on the switch)

`errdisable recovery cause uddid`
`errdisable recovery cause bpduguard`
`errdisable recovery cause security-violation`
`errdisable recovery cause channel-misconfig`
`errdisable recovery cause pagp-flap`
`errdisable recovery cause dtp-flap`
`errdisable recovery cause link-flap`
`errdisable recovery cause gbic-invalid`
`errdisable recovery cause l2ptguard`
`errdisable recovery cause psecure-violation`
`errdisable recovery cause gbic-invalid`
`errdisable recovery cause dhcp-rate-limit`
`errdisable recovery cause unicast-flood`
`errdisable recovery cause vmps`
`errdisable recovery cause storm-control`
`errdisable recovery cause arp-inspection`

ETHERNET OVER MPLS (EOMPLS)

Solution/Services: Tunneling: L2VPN

Related: N/A



EoMPLS

- *Ethernet over MPLS (EoMPLS): extends VLAN over an existing MPLS VPN service provider network*
- Customer network (Customer Edge 1) using CE1-Hub (Hub) and CE1-S1 (Spoke 1)
- Customer network connected into Layer 2 Service Provider configured for EoMPLS
- Customer network will extend VLANs 10 (Internal), 100 (Guest), 199 (Management) between the sites across service provider's MPLS network

>>PE1<<

```
interface FastEthernet0/0
description TO: CE1-H
no ip address
no shutdown
```

```
interface FastEthernet0/0.10
encapsulation dot1Q 10
xconnect 3.3.3.3 10 encapsulation mpls
```

```
interface FastEthernet0/0.100
encapsulation dot1Q 100
xconnect 3.3.3.3 100 encapsulation mpls
```

```
interface FastEthernet0/0.199
encapsulation dot1Q 199
xconnect 3.3.3.3 199 encapsulation mpls
```

>>PE2<<

```
interface FastEthernet0/0
description TO: CE1-S1
no ip address
no shutdown
```

```
interface FastEthernet0/0.10
encapsulation dot1Q 10
xconnect 2.2.2.2 10 encapsulation mpls
```

```
interface FastEthernet0/0.100
encapsulation dot1Q 100
xconnect 2.2.2.2 100 encapsulation mpls
```

```
interface FastEthernet0/0.199
encapsulation dot1Q 199
xconnect 2.2.2.2 199 encapsulation mpls
```

>>CE1-H<<

```
vlan 10
name RHG-CE1-INTERNAL
```

```
vlan 100
name RHG-CE1-GUEST
```

```
vlan 199
name RHG-CE1-MGMT
```

```
interface FastEthernet1/0/1
description TO: PE1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,100,199
switchport nonegotiate
spanning-tree portfast trunk
no shutdown
```

```
interface Vlan 10
description RHG VLAN SVI INTERNAL
ip address 192.168.10.1 255.255.255.0
no shutdown
```

```
interface Vlan 100
description RHG VLAN SVI GUEST
ip address 192.168.100.1 255.255.255.0
no shutdown
```

```
interface Vlan 199
description RHG VLAN SVI MGMT
ip address 192.168.199.1 255.255.255.0
no shutdown
```

```
>>CE1-S1<<
```

```
vlan 10
```

```
name RHG-CE1-INTERNAL
```

```
vlan 100
```

```
name RHG-CE1-GUEST
```

```
vlan 199
```

```
name RHG-CE1-MGMT
```

```
interface FastEthernet1/0/1
```

```
description TO: PE2
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 10,100,199
```

```
switchport nonegotiate
```

```
spanning-tree portfast trunk
```

```
no shutdown
```

```
interface FastEthernet1/0/2
```

```
description Internal network switch port
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
no shutdown
```

```
interface FastEthernet1/0/3
```

```
description Guest network switch port
```

```
switchport access vlan 100
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
no shutdown
```

```
interface Vlan 199
```

```
description RHG VLAN SVI MGMT
```

```
ip address 192.168.199.10 255.255.255.0
```

```
no shutdown
```

```
ip default-gateway 192.168.199.1
```

Monitoring Commands

```
show mpls ldp neighbor
```

```
show xconnect peer <IP> all
```

```
show xconnect interface
```

```
show mpls l2transport vc <VC-ID>
```

```
show mpls l2transport vc <VC-ID> detail
```

```
ping
```

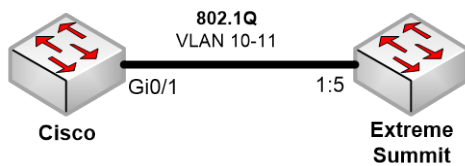
```
traceroute, tracert
```

EXTREME SWITCHES SOLUTIONS

Solution/Services: Extreme Solutions
Related: N/A

802.1Q between Cisco and Extreme

- Configure 802.1Q trunking between Cisco switch and Extreme Summit switch for VLANs 10 and 11



>> CISCO SWITCH <<

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,10-11
switchport mode trunk
```

>> EXTREME SUMMIT 400-48T SWITCH <<

```
configure vlan RHG-LAN add ports 1:5 tagged
configure vlan RHG-GUEST add ports 1:5 tagged
```

```
configure vlan RHG-LAN tag 10
configure vlan RHG-GUEST tag 11
```

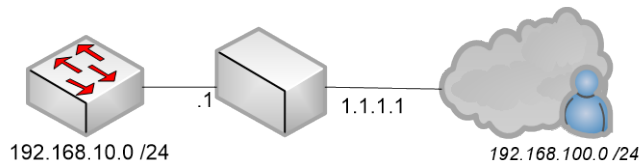
EZVPN

Solution/Services: Security: VPN

Related: N/A

EZVPN using Local Authentication

- Configure Client VPN solution using IPSec VPN
- The VPN pool for connected users will be 192.168.100.10 – 192.168.100.13
- LAN subnet behind the VPN device is: 192.168.10.0/24
- Enable split tunnel to allow VPN users access to the 192.168.10.0 network over the established VPN tunnel
- VPN user authentication will be using Local user database. Add user1
- For the VPN software client: The “Group Authentication” name will be ROUTEHUB and the “Group Authentication Password” will be cisco123



```
username user1 password cisco123
```

```
aaa new-model
aaa authentication login userauthen local
aaa authorization network groupauthen local
```

```
ip local pool routehub-pool 192.168.100.10 192.168.100.50
```

```
ip access-list extended split-tunnel-acl
permit ip 192.168.10.0 0.0.0.255 any
```

```
access-list 110 deny ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 110 permit ip 192.168.10.0 0.0.0.255 any
```

```
route-map no-NAT permit 10
match ip address 110
```

```
ip nat inside source route-map no-NAT interface FastEthernet1 overload
```



```
crypto isakmp client configuration group ROUTEHUB
key cisco123
dns 192.168.10.10 4.2.2.2
domain routehub.local
pool routehub-pool
acl split-tunnel-acl
```

```
crypto isakmp profile VPNclient
match identity group userauthn
match identity group ROUTEHUB
client authentication list userauthn
isakmp authorization list groupauthor
client configuration address respond
```

```
crypto ipsec transform-set 3des esp-3des esp-sha-hmac
```

```
crypto dynamic-map ezvpn 10
set transform-set 3des
set isakmp-profile VPNclient
reverse-route
```

```
crypto map ezvpn 1 ipsec-isakmp dynamic ezvpn
```

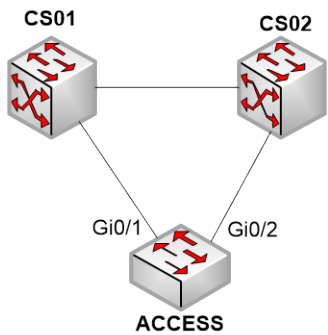
```
interface FastEthernet1
crypto map ezvpn
```

[F]

FLEX LINK

Solution/Services: LAN Switching
Related: N/A

- Configure Gi0/1 to be the Primary Interface to Core switch
- Configure G0/2 to be the Secondary Interface to the Core switch



```
interface gigabitethernet 0/1
switchport backup interface gigabitethernet 0/2
```

```
show interfaces switchport backup
```

FLOW CONTROL

Solution/Services: Feature

Related: N/A

- Flow control can be used on GE interfaces to instruct the other connected device to slow down its current rate of traffic flow. Helps to prevent congestion and packet drops.

```
interface GigabitEthernet1/0/2
flowcontrol receive on
flowcontrol send off
```

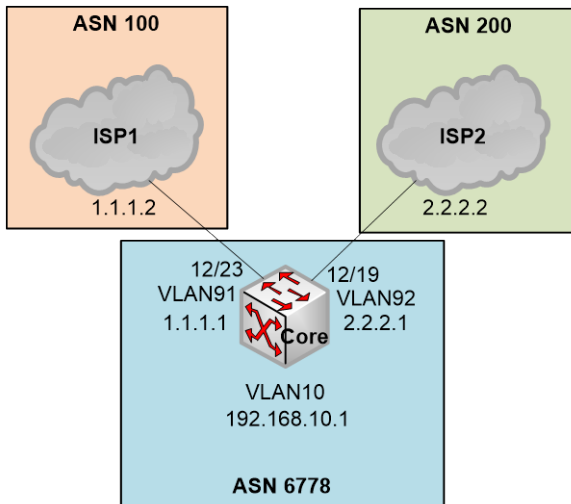
FOUNDRY SOLUTIONS

Solution/Services: Foundry Solutions

Related: BGP

BGP

- Configure path towards ISP1 as the primary path for devices on the Internet to access ASN 6778 using AS Path Prepending. Secondary path through ISP2
- Configure path towards ISP1 as the primary path for Internet access using BGP Weights. Secondary path through ISP2.



```
interface ve 91
ip address 1.1.1.1 255.255.255.252
```

```
interface ve 92
ip address 2.2.2.1 255.255.255.252
```

```
vlan 91 name ISP1
untagged ethe 12/23
router-interface ve 91
```

```
vlan 92 name ISP2
untagged ethe 12/19
router-interface ve 92
```

```
interface ethernet 12/23
port-name ISP1 PORT
no flow-control
```

```
interface ethernet 12/19
port-name ISP2 PORT
no spanning-tree
no flow-control
```

```
interface ve 10
ip address 192.168.10.1 255.255.255.0
```

```
ip prefix-list RHG-SAC-PL-NET seq 5 permit 192.168.10.0/24
```

```
route-map RHG-SAC-RM-BGP-SEC permit 10
set as-path prepend 6778 6778 6778
```

```
router bgp
local-as 6778
maximum-paths 2
multipath ebgp
neighbor 1.1.1.2 remote-as 100
neighbor 1.1.1.2 weight 200
neighbor 1.1.1.2 prefix-list RHG-SAC-PL-NET out
neighbor 1.1.1.2 soft-reconfiguration inbound
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 weight 100
neighbor 2.2.2.2 route-map out RHG-SAC-RM-BGP-SEC
neighbor 2.2.2.2 prefix-list RHG-SAC-PL-NET out
neighbor 2.2.2.2 soft-reconfiguration inbound
network 192.168.10.0 255.255.255.0
```

FRF.12

Solution/Services: QoS: Link Efficiencies
Related:

Go to ["QoS: Link Efficiencies"](#)

FRAME RELAY

Solution/Services: WAN

Related: N/A

Frame Relay Multipoint (Static)

- Frame Relay NBMA (point-to-multipoint) between Aggregation and Branch router
- LMI Type: ANSI
- For WAN Aggregation, PVC to WAN Branch router (10.1.1.2) will use DLCI 100 (shown below)
- For WAN Branch, PVC to WAN Aggregation router (10.1.1.1) will use DLCI 200
- Disable Inverse ARP capabilities



>> WAN AGG <<

```
interface Serial0/0
ip address 10.1.1.1 255.255.255.0
encapsulation frame-relay IETF
ip ospf network point-to-multipoint
frame-relay map ip 10.1.1.2 100 broadcast
no frame-relay inverse-arp
frame-relay lmi-type ansi
```

```
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
```

Frame Relay Multipoint (Dynamic)

- Dynamic Frame Relay NBMA (point-to-multipoint) between Aggregation and Branch router
- LMI Type: ANSI
- For WAN Aggregation, PVC to WAN Branch router (10.1.1.2) will use DLCI 100 (shown below)
- For WAN Branch, PVC to WAN Aggregation router (10.1.1.1) will use DLCI 200



>> WAN AGG <<

interface Serial0/0

no ip address

encapsulation frame-relay IETF

frame-relay lmi-type ansi

interface Serial0/0.1 multipoint

ip address 10.1.1.1 255.255.255.0

frame-relay inverse-arp ip 100

router ospf 1

network 10.1.1.0 0.0.0.3 area 0

Frame Relay Point-to-Point

- Frame Relay Point-to-Point between Aggregation and Branch router
- LMI Type: ANSI
- For WAN Aggregation, PVC to WAN Branch router will use DLCI 100 (shown below)
- For WAN Branch, PVC to WAN Aggregation will use DLCI 200



>> WAN Aggregation <<

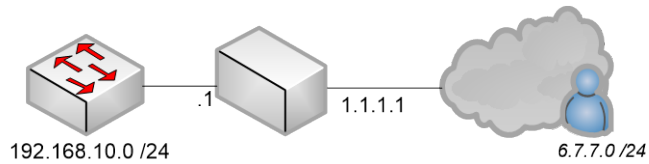
```
interface Serial0/0/0
no ip address
encapsulation frame-relay IETF
frame-relay lmi-type ansi
```

```
interface Serial0/0/0.100 point-to-point
ip address 10.1.1.1 255.255.255.252
frame-relay interface-dlci 100
```

```
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
```

Frame Relay Multi-Link (MFR)

- Configure multiple Frame Relay interfaces (Serial 0/0/0 and 0/0/1) configured in a bundle (also called an MFR)
- The local DLCI will be 100



```
interface MFR0
no ip address
encapsulation frame-relay IETF
frame-relay multilink bid test
frame-relay lmi-type ansi
```

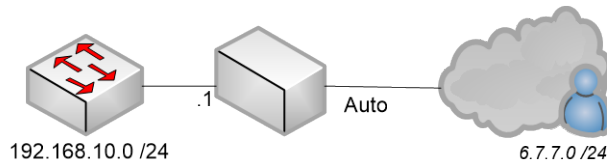
```
interface MFR0.100 point-to-point
ip address 1.1.1.1 255.255.255.0
frame-relay interface-dlci 100 IETF
```

```
interface Serial0/0/0:0
no ip address
encapsulation frame-relay MFR0
no arp frame-relay
frame-relay multilink lid link1
```

```
interface Serial0/0/1:0
no ip address
encapsulation frame-relay MFR0
no arp frame-relay
frame-relay multilink lid link2
```

PPP over Frame Relay

- Configure PPP over Frame Relay (PPPoFR) using DLCI 100
- PPP user details: Username=user@realm, Password=cisco123



```
interface Serial0/0/0
ip address 1.1.1.1 255.255.255.0
encapsulation frame-relay IETF
service-module t1 timeslots 1-24
service-module t1 fdl both
frame-relay lmi-type ansi
```

```
interface Serial0/0/0.1 point-to-point
frame-relay interface-dlci 100 ppp Virtual-Template1
```

```
interface Virtual-Template1
ip address negotiated
ppp chap hostname user@realm
ppp chap password 0 cisco123
ppp ipcp dns request
ppp ipcp route default
ppp ipcp address accept
```

```
ip route 0.0.0.0 0.0.0.0 Serial0/0/0.1
```

Adaptive Traffic Shaping and BECN/FECN Integration

- Frame Access rate is 256kps and CIR is 64kbps
- Throttle back to the CIR if it receives BECNs.



>> WAN Aggregation <<

```
map-class frame-relay afrrs
frame-relay traffic-shape rate 256000
frame-relay traffic-shape adaptive 64000
```

```
interface Serial0/0/0
no ip address
encapsulation frame-relay IETF
frame-relay lmi-type ansi
```

```
interface Serial0/0/0.100 point-to-point
ip address 10.1.1.1 255.255.255.252
frame-relay interface-dlci 18 IETF protocol ip 10.10.10.2
frame-relay class afrrs
```

```
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
```

Monitoring

```
show frame-relay lmi
show frame-relay pvc
show frame-relay map
debug frame-relay lmi
show frame-relay qos-autosense
```

FRAME RELAY TRAFFIC SHAPING (FRTS)

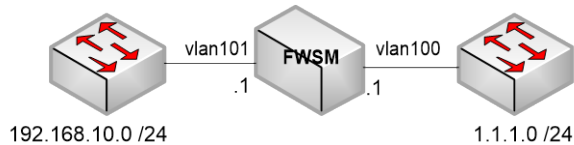
Solution/Services: QoS: Link Efficiencies
Related:

Go to ["QoS: Link Efficiencies"](#)

FWSM

Solution/Services: Cisco Catalyst 6500 Series

Related:



Base Configuration for Cisco Catalyst 6500

- Add VLAN 100 (used for outside) and VLAN 101 (used for inside) that will be used by the FWSM. Reference network diagram (above)
- Associate the VLANs to be used by the FWSM located in slot 4

```
vlan 100  
name FWSM-OUTSIDE
```

```
vlan 101  
name FWSM-INSIDE
```

```
firewall multiple-vlan-interfaces  
firewall vlan-group 1 100-101
```

```
firewall module 4 vlan-group 1 100-101
```

Access FWSM from Catalyst 6500

- Access FWSM service module (located in slot 4) from Cisco Catalyst 6500 console

```
session slot 4 processor 1
```

Interfaces

- Configure VLAN interfaces that has been allocated to the FWSM to use for the outside and inside interfaces

```
interface Vlan100
nameif outside
security-level 0
ip address 1.1.1.1 255.255.255.0
```

```
interface Vlan101
nameif inside
security-level 100
ip address 192.168.10.1 255.255.255.0
```

Security Context

- Allocate VLANs 10 and 11 to FWSM (located in slot 4)

```
firewall vlan-group 1 10-11
firewall module 4 vlan-group 1 10-11
```

- Configure a virtualized firewall for Client1 specifying the VLAN interfaces that will be used for the outside and the inside.

```
context Client1
allocate-interface vlan10 outside
allocate-interface vlan11 inside
config-url disk:/Client1.cfg
```

- To access the Client1 firewall instance from the FWSM.

```
ch context Client1
```

Failover

- Failover configuration for peering with a redundant FWSM

```
failover
failover lan unit primary
failover lan interface failover vlan 100
failover polltime unit msec 500 holdtime 3
failover polltime interface 3
failover interface-policy 100%
failover replication http
failover link state vlan 101
failover interface ip failover 9.9.9.1 255.255.255.252 standby 9.9.9.2
failover interface ip state 9.9.8.1 255.255.255.252 standby 9.9.8.2
```

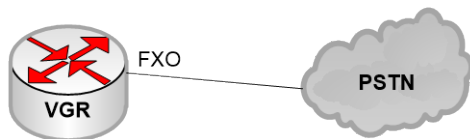

FXO

Solution/Services: Voice and Unified Communications

Related: N/A

Voice Gateway and FXO Ports (CO/PSTN)

- FXO port 0/2/0 connected to PSTN
- All incoming calls will be redirected to extension 5000



```
voice-port 0/2/0
supervisory disconnect dualtone pre-connect
pre-dial-delay 0
no vad
timeouts call-disconnect 2
timeouts wait-release 2
connection plar 5000
caller-id enable
```

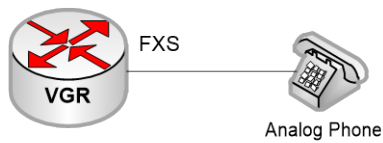
FXS

Solution/Services: Voice and Unified Communications

Related: N/A

Voice Gateway and FXS Ports (Analog Devices)

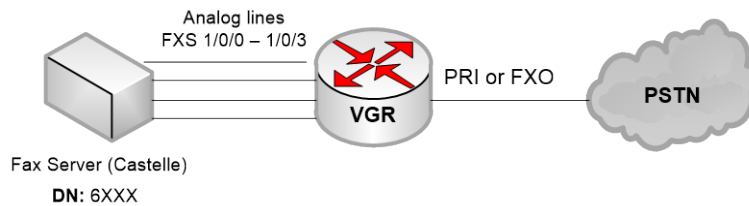
- FXS port with connected analog phone using extension 3001 (Caller ID: Analog 3001)



```
voice-port 0/1/0  
station-id name Analog 3001  
station-id number 3001  
caller-id enable
```

FXS ports connecting to FAX Server (Castelle)

- FXS ports connecting to analog ports on a Fax Server (e.g. Castelle Fax Server)
- Example: we have 4 ports connecting into the fax server. 4-digits are passed from the PSTN. If someone sends a fax to 209-123-6111, 6111 will be passed to the gateway and towards one of the 4 FXS ports connected to the fax server.



```
dial-peer voice 101 pots
preference 4
destination-pattern 6...
fax rate disable
no digit-strip
direct-inward-dial
port 1/0/0
forward-digits all
```

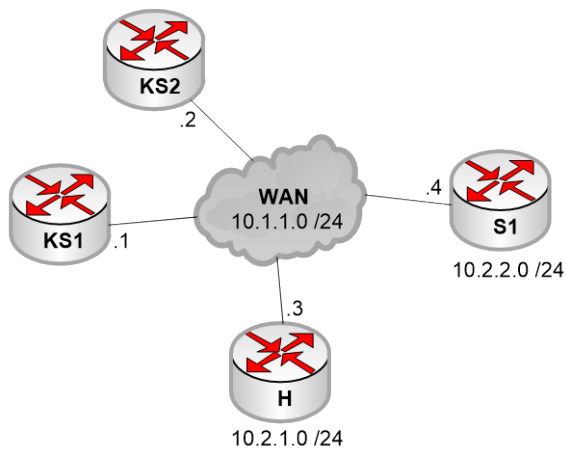
...

```
dial-peer voice 104 pots
preference 7
destination-pattern 6...
fax rate disable
no digit-strip
direct-inward-dial
port 1/0/3
forward-digits all
```

[G]

GET VPN

Solution/Services: Security: VPN
Related: N/A



Key Server (Primary)

- Configure Primary Key Server on KS1 (10.1.1.1)
- GETVPN ID will be "1"
- Primary Key Server builds VPN with each of the VPN Group member routers

```
interface FastEthernet0/0  
ip address 10.1.1.1 255.255.255.0
```

```
crypto isakmp policy 10  
encr 3des  
authentication pre-share  
group 2
```

```
crypto isakmp key cisco123 address 10.1.1.2  
crypto isakmp key cisco123 address 10.1.1.3  
crypto isakmp key cisco123 address 10.1.1.4
```

```
crypto ipsec transform-set GVPN-TS esp-3des esp-sha-hmac
```

```
crypto ipsec profile gdoi-profile-gvpn1  
set security-association lifetime seconds 1800  
set transform-set GVPN-TS
```

```
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

```
crypto gdoi group gvpn1  
identity number 1  
server local  
  rekey lifetime seconds 10800  
  rekey retransmit 10 number 2  
  rekey authentication mypubkey rsa gvpn1-export-general  
  rekey transport unicast  
sa ipsec 1  
  profile gdoi-profile-gvpn1  
  match address ipv4 101  
  replay counter window-size 64  
  address ipv4 10.1.1.1  
  redundancy  
  local priority 10  
  peer address ipv4 10.1.1.2
```

Key Server (Secondary)

- Configure Secondary Key Server on KS1 (10.1.1.2)
- GETVPN ID will be "1"
- Secondary Key Server builds VPN with each of the VPN Group member routers

```
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0

crypto isakmp policy 10
encr 3des
authentication pre-share
group 2

crypto isakmp key cisco123 address 10.1.1.1
crypto isakmp key cisco123 address 10.1.1.3
crypto isakmp key cisco123 address 10.1.1.4

crypto ipsec transform-set GVPN-TS esp-3des esp-sha-hmac

crypto ipsec profile gdoi-profile-gvpn1
set security-association lifetime seconds 1800
set transform-set GVPN-TS

access-list 101 permit ip 10.2.0.0 0.0.255.255 10.2.0.0 0.0.255.255

crypto gdoi group gvpn1
identity number 1
server local
    rekey lifetime seconds 10800
    rekey retransmit 10 number 2
    rekey authentication mypubkey rsa gvpn1-export-general
    rekey transport unicast
sa ipsec 1
profile gdoi-profile-gvpn1
match address ipv4 101
replay counter window-size 64
address ipv4 10.1.1.2
redundancy
local priority 1
peer address ipv4 10.1.1.1
```

Group Members

- Group Member routers enabled for GET VPN and build VPN tunnels to the Key Servers (Primary & Secondary)

```
crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
```

```
crypto isakmp key cisco123 address 10.1.1.1
crypto isakmp key cisco123 address 10.1.1.2
```

```
crypto gdoi group gvpn1
identity number 1
server address ipv4 10.1.1.1
server address ipv4 10.1.1.2
```

```
crypto map vpn 10 gdoi
set group gvpn1
```

```
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
crypto map vpn
```

Monitor

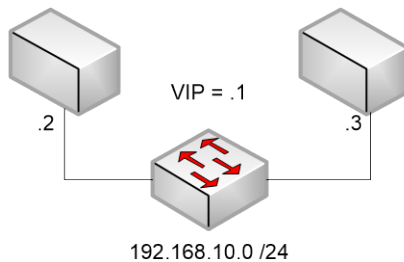
```
>>KEY SERVER<<
show crypto gdoi ks
show crypto isakmp sa
show crypto gdoi group <gdoi-group>
show crypto gdoi ks members
show crypto gdoi ks policy
show crypto gdoi ks acl
```

```
>>GROUP MEMBER<<
show crypto isakmp sa
show crypto gdoi group <gdoi-group>
```

GLBP

Solution/Services: First Hop Redundancy Protocol (FHRP)

Related: HSRP, VRRP



GLBP with Authentication

- **Priority:** higher the value, the more preferred primary default gateway device
- SW1 would be the primary GLBP router and SW2 would be the secondary GLBP router
- Configure GLBP for network 192.168.10.0 (VLAN 10) and use GLBP Authentication (password=cisco123)
- The GLBP IP address will be 192.168.10.1 (this would be the IP devices would use for their default gateway)

>> SW1 <<

```
key chain GLBP1
key 1
key-string cisco123
```

```
interface Vlan10
ip address 192.168.10.2 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
glbp 10 ip 192.168.10.1
glbp 10 timers msec 200 msec 850
glbp 10 priority 150
glbp 10 preempt delay minimum 600
glbp 10 authentication md5 key-chain GLBP1
```

>> SW2 <<

```
key chain GLBP1
key 0
key-string cisco123
```

```
interface Vlan10
ip address 192.168.10.3 255.255.255.0
no ip redirects
no ip unreachable
```



```
no ip proxy-arp
glbp 10 ip 192.168.10.1
glbp 10 timers msec 200 msec 850
glbp 10 preempt delay minimum 600
glbp 10 authentication md5 key-chain GLBP1
```

GOLD

Solution/Services: Network Management

Related: N/A

- Bootup diagnostics
- Run during system bootup against all of the line cards or when a supervisor switchover occurs.
- Makes sure that all hardware is working properly

diagnostics bootup level complete

- Runtime diagnostics
- Non-disruptive test that runs in the background

diagnostics monitor module 5 test 2

diagnostics monitor internal module 5 test 2 00:00:15

- Runtime diagnostics
- Diagnostics test can be run on demand for troubleshooting purposes

diagnostics start module 4 test 8

diagnostics stop module 4

show diagnostics result module 4

- Runtime diagnostics
- Schedule diagnostic tests for verification and troubleshooting

diagnostics schedule module 4 test 1 port 3 on Jan 3 2005 23:32

show diagnostic content module [module_number]

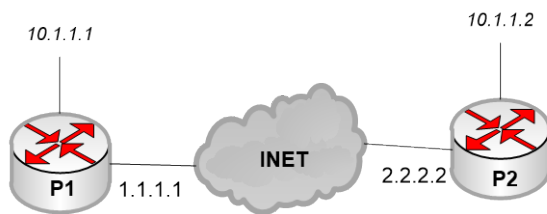
GRE

Solution/Services: Tunneling

Related: N/A

GRE Tunnel

- Required IP port 47 (GRE) to be allowed through a firewall (if configured)
- Build GRE logical point-to-point tunnel between P1 and P2 where other protocol (e.g. IPv4, IPv6, IPX) can route through.



>> P1 <<

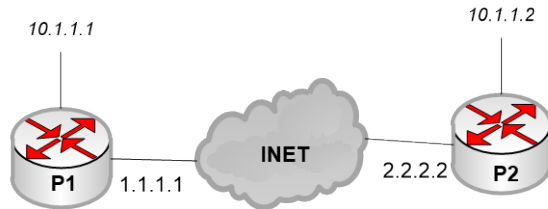
```
interface Tunnel0
ip address 10.1.1.1 255.255.255.252
tunnel source 1.1.1.1
tunnel destination 2.2.2.2
```

>> P2 <<

```
interface Tunnel0
ip address 10.1.1.2 255.255.255.252
tunnel source 2.2.2.2
tunnel destination 1.1.1.1
```

IP Tunnel (IPIP)

- Build IP enabled point-to-point logical tunnel (not GRE) between P1 and P2 where traffic can route through.



>> P1 <<

```
interface Tunnel0
ip address 10.1.1.1 255.255.255.252
tunnel source 1.1.1.1
tunnel destination 2.2.2.2
tunnel mode ipip
```

>> P2 <<

```
interface Tunnel0
ip address 10.1.1.2 255.255.255.252
tunnel source 2.2.2.2
tunnel destination 1.1.1.1
tunnel mode ipip
```

GROUNDSTART

Solution/Services: Voice & Unified Communications

Related: N/A

- Specify that this FXO port is using a Groundstart signaling on the analog line

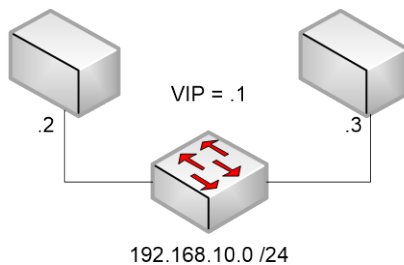
voice-port 0/1/0

signal groundStart

[H]

HSRP

Solution/Services: First Hop Redundancy Protocols (FHRP)
Related: VRRP, GLBP



HSRP

- **Priority:** *higher the value, the more preferred primary default gateway device*
- SW1 would be the primary HSRP router and SW2 would be the secondary HSRP router
- Configure HSRP for network 192.168.10.0 (VLAN 10)
- The HSRP IP address will be 192.168.10.1 (this would be the IP devices would use for their default gateway)

>>SW1<<

```
interface Vlan10
ip address 192.168.10.2 255.255.255.0
standby ip 192.168.10.1
standby timers msec 250 msec 750
standby priority 110
standby preempt delay minimum 180
```

```
>>SW2<<
interface Vlan10
ip address 192.168.10.3 255.255.255.0
standby ip 192.168.10.1
standby timers msec 250 msec 750
standby preempt delay minimum 180
```

HSRP Authentication

- Configure HSRP authentication using the password "cisco123"

```
>>SW1<<
interface Vlan10
standby authentication cisco123
```

```
>>SW2<<
interface Vlan10
standby authentication cisco123
```

Redirecting ICMP

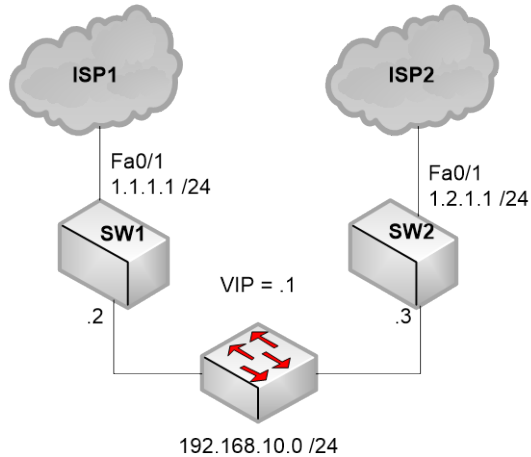
- Enable redirecting ICMP under the HSRP interfaces

```
>>SW1<<
interface Vlan10
standby redirects enable
```

```
>>SW2<<
interface Vlan10
standby redirects enable
```

Tracking

- If the WAN facing interface (Fa0/1) goes down on SW1, the primary HSRP router, subtract "20" from the priority which will cause SW2 to be the primary HSRP router with the highest priority value.

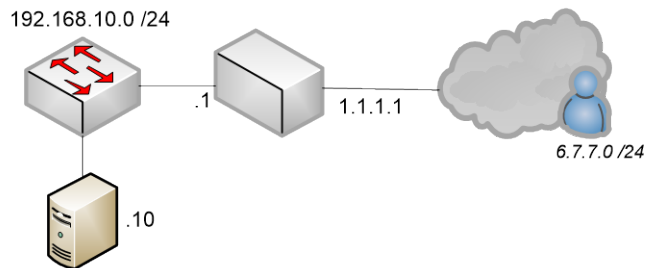


```
>>SW1<<
interface Vlan10
ip address 192.168.10.2 255.255.255.0
standby ip 192.168.10.1
standby timers msec 250 msec 750
standby priority 110
standby preempt delay minimum 180
standby track FastEthernet0/1 20
```

```
>>SW2<<
interface Vlan10
ip address 192.168.10.3 255.255.255.0
standby ip 192.168.10.1
standby timers msec 250 msec 750
standby preempt delay minimum 180
```


Using HSRP with Multiple IP Addresses and Unique MAC Addresses

- This is applicable if you have a router/firewall that you manage that will be plugged into an ISP router/modem that is provided for DSL or Cable with a block of IP addresses. Most of the ISP (AT&T, Comcast) routers require a unique mac address for each public IP address that you will use. Thus, using NAT is not possible. You have to manually configure a router/firewall for each IP address you want to use.
- Or you can use the following configuration example using a Cisco IOS router where the Internet facing interface is configured for HSRP and using different mac addresses for each public IP address that will be used.
- Example: ISP IP address block starting from 1.1.1.0 /24



```
interface FastEthernet0/0
description INET facing interface
ip address 1.1.1.1 255.255.255.0
ip nat outside
standby version 2
standby 10 ip 1.1.1.10
standby 10 timers 254 255
standby 10 preempt
standby 10 mac-address 0000.1111.1111
standby 11 ip 1.1.1.11
standby 11 timers 254 255
standby 11 preempt
standby 11 mac-address 0000.1111.2222
standby 12 ip 1.1.1.12
standby 12 timers 254 255
standby 12 preempt
standby 12 mac-address 0000.1111.3333
```

```
ip nat inside source static 192.168.10.10 1.1.1.10
ip nat inside source static 192.168.10.11 1.1.1.11
ip nat inside source static 192.168.10.12 1.1.1.12
```

HSRP Monitoring Commands

```
show standby
show standby brief
show track
```

HTTP

Solution/Services: Feature
Related: N/A

HTTP on Cisco IOS

- Enable HTTP and HTTPS on Cisco IOS device using local authentication. One of the user account will be "user1"
- Only users from the network 192.168.10.0/24 can access this Cisco device using HTTP

```
username user1 password cisco123
```

```
access-list 23 permit 192.168.10.0 0.0.0.255
```

```
ip http server  
ip http secure-server  
ip http access-class 23  
ip http authentication local
```



IGMP SNOOPING

Solution/Services: Multicast

Related: N/A

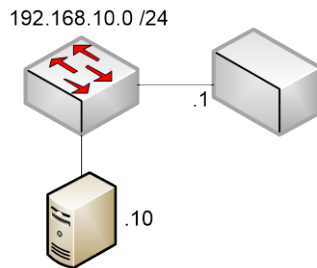
- Enables IGMP snooping globally on L2/L3 switches

`ip igmp snooping`

IOS RECOVERY

Solution/Services: Administration/System

Related: N/A



- If the IOS image is missing or corrupted on a Cisco device, it can be recovered from the ROMMON using a TFTP server connected to the LAN
- All of this is done from the ROMMON prompt
- In our example, the Cisco IOS device will use IP 192.168.10.1/24, the TFTP server on our LAN is 192.168.10.10, and the IOS image filename to download is "c2801.bin"

```
IP_ADDRESS=192.168.10.1
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=192.168.10.1
```

```
TFTP_SERVER=192.168.10.10
TFTP_FILE=c2801.bin
```

```
tftpdnld
```

INCLUDE

Solution/Services: Administration/System

Related: N/A

- Issue the command "show ip route" but only display lines that contains "28416"

show ip route | include 28416

```
D 10.25.1.0/24 [90/28416] via 10.25.99.1, 7w0d, Vlan1
D 10.25.100.0/24 [90/28416] via 10.25.99.1, 7w0d, Vlan1
D 10.25.150.0/24 [90/28416] via 10.25.99.1, 7w0d, Vlan1
D 10.25.200.0/24 [90/28416] via 10.25.99.1, 7w0d, Vlan1
```

INTERFACES

Solution/Services: Best Practices

Related: N/A

Interfaces (L3) Best Practices

- Recommended configuration to apply on a Layer 3 interface (configured with an IP)

```
interface GigabitEthernet1/1
no ip redirects
no ip unreachable
no ip proxy-arp
```

Interfaces (L2) Best Practices

- Recommended configuration to apply on a Layer 2 interface

```
interface GigabitEthernetX/Y
description L2 port
switchport
carrier-delay msec 0
```

INTERFACE RANGE

Solution/Services: Administration/System

Related: N/A

- Configure multiple ports/interfaces at once
- Below will specify GE ports 1 to 10 to be configured at once.

```
interface range gi0/1 – 10
```

IP ACCOUNTING

Solution/Services: Feature

Related: N/A

- Enable IP Accounting

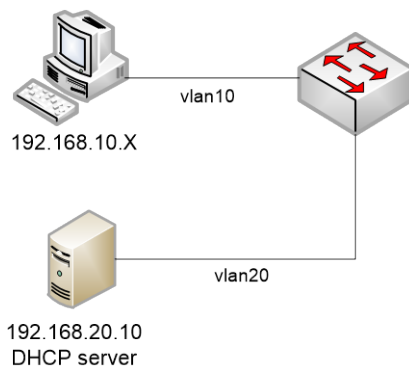
```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
ip accounting output-packets
```


IP HELPER

Solution/Services: Feature

Related: N/A

- Specify IP of DHCP server located on another network



```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
ip helper-address 192.168.20.10
```

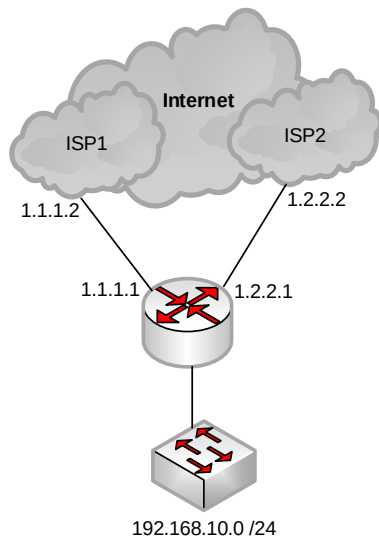
IP SLA

Solution/Services: Feature

Related: N/A

IP SLA with Dual ISP

- Configure IP SLA with two connected ISP's for Internet redundancy.
- Primary Internet access through ISP1 (FA0). Secondary Internet access through ISP2 (FA1).
- If IP address 1.1.1.2 (IP on ISP1 router) is not pingable by the Cisco Router then declare ISP1 down and change default route towards ISP2
- Using NAT overload based on path to the Internet



IP SLA Configuration

```
track timer interface 5
```

```
ip sla 10  
icmp-echo 1.1.1.2 source-ip 1.1.1.1  
timeout 1000  
threshold 40  
frequency 3
```

```
ip sla schedule 10 life forever start-time now
```

```
track 1 rtr 10 reachability  
delay down 15 up 10
```

```
ip route 0.0.0.0 0.0.0.0 1.1.1.2 track 1
ip route 0.0.0.0 0.0.0.0 1.2.2.2 254
```

NAT Configuration

```
access-list 110 permit ip 192.168.10.0 0.0.0.255 any
```

```
route-map RM-NAT-1 permit 10
match ip address 110
match interface FastEthernet0
```

```
route-map RM-NAT-2 permit 10
match ip address 110
match interface FastEthernet1
```

```
ip nat inside source route-map RM-NAT-1 interface FastEthernet0 overload
ip nat inside source route-map RM-NAT-2 interface FastEthernet1 overload
```

Interface Configuration

```
interface FastEthernet0
description primary ISP path
ip address 1.1.1.1 255.255.255.252
ip nat outside
```

```
interface FastEthernet1
description secondary ISP path
ip address 1.2.2.1 255.255.255.0
ip nat outside
```

IP SLA Monitoring Commands

```
show track timer
show track brief
show track <ID>
```

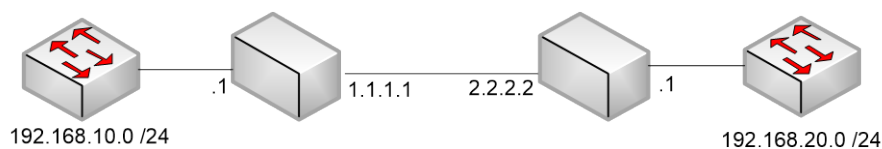
IPSEC VPN

Solution/Services: Security: VPN

Related: N/A

Site-Based VPN using Cisco IOS

- Configure IPsec VPN tunnel between two Cisco IOS routers
- Site #1: WAN IP is 1.1.1.1. The LAN subnet is 192.168.10.0
- Site #2: WAN IP is 2.2.2.2. The LAN subnet is 192.168.20.0
- Disable NAT (using NAT Overload & Static NAT) for routing between the two LAN subnets across the VPN
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- The VPN shared key will be "cisco123"
- Enable VPN on WAN facing interface



>> SITE1 <<

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
```

```
crypto isakmp key ciscokey address 2.2.2.2
```

```
crypto ipsec transform-set ipsec-ts esp-3des esp-md5-hmac
```

```
access-list 112 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
crypto map VPN 10 ipsec-isakmp
  set peer 2.2.2.2
  set transform-set ipsec-ts
  set pfs group2
  match address 112
```

```
access-list 110 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 110 permit ip 192.168.10.0 0.0.0.255 any
```

```
ip nat inside source list 110 pool NATPOOL overload
```

```
route-map no-NAT permit 10  
match ip address 110
```

```
ip nat inside source static tcp 192.168.10.10 25 1.1.1.10 25 route-map no-NAT extendable
```

```
interface FastEthernet0/1  
ip address 192.168.10.1 255.255.255.0
```

```
interface FastEthernet0/0  
ip address 1.1.1.1 255.255.255.0  
crypto map vpn
```

>> SITE2 <<

```
crypto isakmp policy 10  
encr 3des  
authentication pre-share  
group 2
```

```
crypto isakmp key ciscokey address 1.1.1.1
```

```
crypto ipsec transform-set ipsec-ts esp-3des esp-md5-hmac
```

```
access-list 112 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
crypto map VPN 10 ipsec-isakmp  
set peer 1.1.1.1  
set transform-set ipsec-ts  
set pfs group2  
match address 112
```

```
access-list 110 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255  
access-list 110 permit ip 192.168.20.0 0.0.0.255 any
```

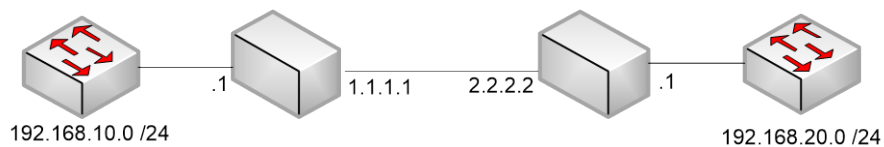
```
ip nat inside source list 110 pool NATPOOL overload
```

```
interface FastEthernet0/1  
ip address 192.168.20.1 255.255.255.0
```

```
interface FastEthernet0/0  
ip address 2.2.2.2 255.255.255.0  
crypto map vpn
```

Tunnel End-Point Discovery (TED), One-Way Site VPN using Cisco IOS

- Configure IPSec VPN tunnel where VPN can only be established from SITE2 (LAN: 192.168.20.0) to SITE1 (192.168.10.0). Not possible from SITE1
- Site #1: WAN IP is 1.1.1.1. The LAN subnet is 192.168.10.0
- Site #2: WAN IP is 2.2.2.2. The LAN subnet is 192.168.20.0
- Disable NAT for routing between the two LAN subnets across the VPN
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- The VPN shared key will be "cisco123"
- Enable VPN on WAN facing interface



>> SITE1 <<

```
crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
```

```
crypto isakmp key Cisco123 address 0.0.0.0 0.0.0.0
```

```
crypto ipsec transform-set RHG-TS-3DES-MD5 esp-3des esp-md5-hmac
```

```
access-list 112 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
crypto dynamic-map RHG-DMAP-VPN 10
set transform-set RHG-TS-3DES-MD5
match address 112
```

```
crypto map RHG-VPN 10 ipsec-isakmp dynamic RHG-DMAP-VPN
```

```
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0
```

```
interface FastEthernet0/0
ip address 1.1.1.1 255.255.255.0
crypto map RHG-VPN
```

>> SITE2 <<

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
```

```
crypto isakmp key Cisco123 address 1.1.1.1
```

```
crypto ipsec transform-set ipsec-ts esp-3des esp-md5-hmac
```

```
access-list 112 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
crypto map VPN 10 ipsec-isakmp
  set peer 1.1.1.1
  set transform-set ipsec-ts
  set pfs group2
  match address 112
```

```
access-list 110 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 permit ip 192.168.20.0 0.0.0.255 any
```

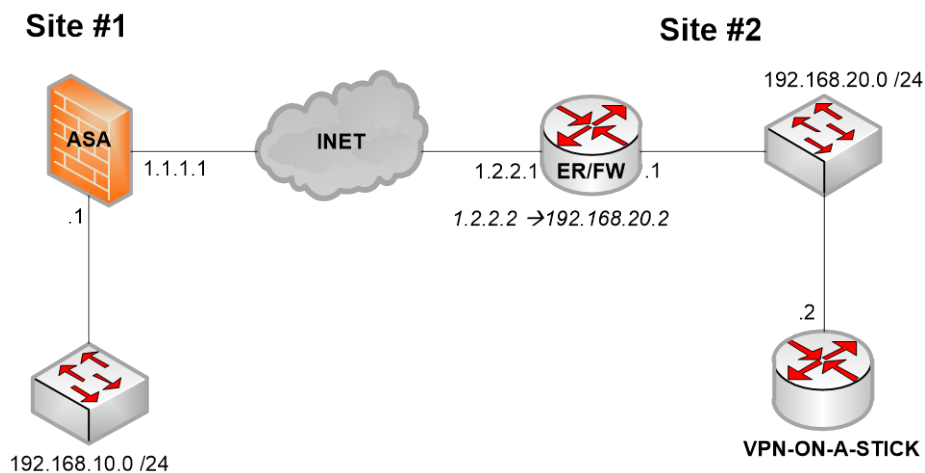
```
ip nat inside source list 110 pool NATPOOL overload
```

```
interface FastEthernet0/1
  ip address 192.168.20.1 255.255.255.0
```

```
interface FastEthernet0/0
  ip address 2.2.2.2 255.255.255.0
  crypto map VPN
```

>> MONITOR <<

```
show crypto isakmp sa
show crypto ipsec sa
show crypto engine connections active
```



- Configure IPSec VPN tunnel between a Cisco ASA firewall and Cisco IOS router that exist connected to the LAN at Site #2.
- Site #1 LAN subnet is 192.168.10.0, Site #2 LAN subnet is 192.168.20.0
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- The VPN shared key will be "Cisco123"
- Enable VPN on interface that's connected to the LAN at Site #2

>> CISCO 871 (VPN on a stick device) <<

```
hostname VPN-ON-A-STICK
```

```
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
```

```
crypto isakmp key Cisco123 address 1.1.1.1
```

```
crypto ipsec transform-set RHG-TS-3DES-MD5 esp-3des esp-md5-hmac
```

```
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
crypto map RHG-VPN 10 ipsec-isakmp
  set peer 1.1.1.1
  set transform-set RHG-TS-3DES-MD5
  match address 101
```

```
interface FastEthernet4
  ip address 192.168.20.2 255.255.255.0
  crypto map RHG-VPN
```

```
ip route 0.0.0.0 0.0.0.0 192.168.20.1
```


- Edge router at Site #2 configured with a static NAT using an outside address of 1.2.2.2 mapping to the IP configured the Cisco 871 router (192.168.20.2)
- Configure ACL policy on edge router following ESP and ISAKMP (UDP/500) to the NATed address of the Cisco 871 router which is 1.2.2.2

>> EDGE ROUTER <<

```
ip nat inside source static 192.168.20.2 1.2.2.2 extendable
```

```
ip access-list extended ingress-acl
permit udp any host 1.2.2.2 eq 500
permit esp any host 1.2.2.2
```

```
interface FastEthernet0/0
ip address 1.2.2.1 255.255.255.0
ip access-group ingress-acl in
ip nat outside
```

```
interface FastEthernet0/1
ip address 192.168.20.1 255.255.255.0
ip nat inside
```

```
ip route 192.168.10.0 255.255.255.0 192.168.20.2
```

- IPSec VPN tunnel between a Cisco ASA firewall and Cisco IOS router that exist connected to the LAN at Site #2.
- Build VPN to NATed IP for Cisco 871 (1.2.2.2)
- Site #1 LAN subnet is 192.168.10.0, Site #2 LAN subnet is 192.168.20.0
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- The VPN shared key will be "Cisco123"
- Enable VPN on WAN (outside) facing interface

>> ASA <<

```
interface Ethernet0/0
nameif RHG-WAN
security-level 0
ip address 1.1.1.1 255.255.255.0
```

```
interface Ethernet0/1
nameif RHG-LAN
security-level 100
ip address 192.168.10.1 255.255.255.0
```

```
access-list ACL-NONAT extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
nat (RHG-LAN) 0 access-list ACL-NONAT
```

```
crypto isakmp identity address
crypto isakmp enable RHG-WAN
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 86400
```

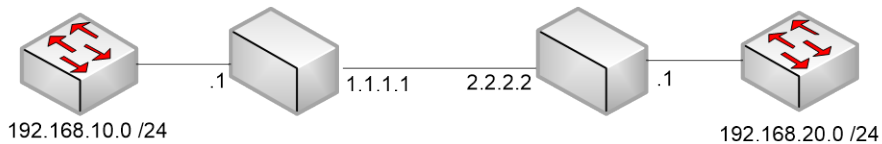
```
access-list ACL-VPN extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
```

```
crypto map RHG-VPN 10 match address ACL-VPN  
crypto map RHG-VPN 10 set peer 1.2.2.2  
crypto map RHG-VPN 10 set transform-set RHG-TS-VPN  
crypto map RHG-VPN interface RHG-WAN
```

```
tunnel-group 1.2.2.2 type ipsec-l2l  
tunnel-group 1.2.2.2 ipsec-attributes  
pre-shared-key Cisco123
```

IPSec over GRE

- Configure IPSec VPN over GRE tunnel between two Cisco IOS routers
- Site #1: WAN IP is 1.1.1.1. Tunnel IP: 10.1.1.1. The LAN subnet is 192.168.10.0
- Site #2: WAN IP is 2.2.2.2. Tunnel IP: 10.1.1.2. The LAN subnet is 192.168.20.0
- Encrypt GRE tunnel between the two Cisco router's WAN interface
- Configure EIGRP between the two routers across the IPSec over GRE tunnel
- The VPN shared key will be "cisco123"
- Enable VPN on WAN facing interface



>> SITE1 <<

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
```

```
crypto isakmp key cisco123 2.2.2.2
```

```
crypto ipsec transform-set TS-3DES-SHA esp-3des esp-sha-hmac
```

```
access-list 100 permit gre host 1.1.1.1 host 2.2.2.2
```

```
crypto map VPN 1 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set TS-3DES-SHA
 match address 100
```

```
interface Tunnel0
 ip address 10.1.1.1 255.255.255.252
 ip mtu 1412
 ip tcp adjust-mss 1360
 tunnel source Fastethernt0/0
 tunnel destination 2.2.2.2
 crypto map VPN
```

```
interface Fastethernt0/0
 ip address 1.1.1.1 255.255.255.0
 crypto map VPN
```

```
interface Fastethernt0/1
 ip address 192.168.10.1 255.255.255.0
```

```
router eigrp 1
 network 192.168.10.0
 network 10.1.1.0 0.0.0.3
 no auto-summary
```

```
>> SITE2 <<
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2

crypto isakmp key cisco123 1.1.1.1

crypto ipsec transform-set TS-3DES-SHA esp-3des esp-sha-hmac

access-list 100 permit gre host 2.2.2.2 host 1.1.1.1

crypto map VPN 1 ipsec-isakmp
  set peer 1.1.1.1
  set transform-set TS-3DES-SHA
  match address 100

interface Tunnel0
  ip address 10.1.1.2 255.255.255.252
  ip mtu 1412
  ip tcp adjust-mss 1360
  tunnel source Fastethernt0/0
  tunnel destination 1.1.1.1
  crypto map VPN

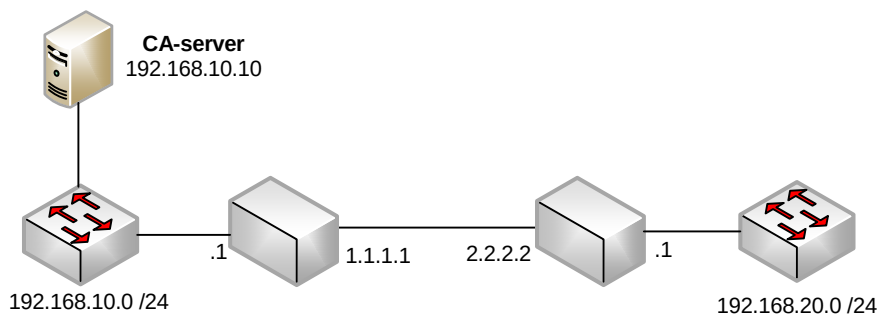
interface Fastethernt0/0
  ip address 2.2.2.2 255.255.255.0
  crypto map VPN

interface Fastethernt0/1
  ip address 192.168.20.1 255.255.255.0

router eigrp 1
  network 192.168.20.0
  network 10.1.1.0 0.0.0.3
  no auto-summary
```

Site-Based VPN using RSA Signatures (CA) on Cisco IOS

- Configure IPSec VPN tunnel between two Cisco IOS routers using Certificates (RSA Signature authentication) instead of pre-share authentication
- CA server (Microsoft CA Server) is 192.168.10.10 (ca-server)
- Recommended to enable NTP for time servers for all VPN routers
- Site #1: WAN IP is 1.1.1.1. The LAN subnet is 192.168.10.0
- Site #2: WAN IP is 2.2.2.2. The LAN subnet is 192.168.20.0
- LAN subnets at Site #1 will communicate with the LAN subnets at Site #2
- LAN subnets at Site #2 will communicate with the LAN subnets at Site #1
- Enable VPN on WAN facing interface



>> SITE1 <<

hostname R1

ip domain-name routehub.local

clock timezone pst -8

clock summer pst recurring

ip host ca-server 192.168.10.10

crypto key generate rsa

crypto ca identity ipsec-ca

enrollment mode ra

enrollment url http://ca-server:90/certsrv/mscep/mscep.dll

crypto ca authenticate ipsec-ca

crypto ca enroll ipsec-sa

interface fastethernet0

description WAN interface

ip address 1.1.1.1 255.255.255.252

crypto map vpn

no shutdown

interface fastethernet1

description LAN interface

ip address 192.168.10.1 255.255.255.0

no shutdown

```
crypto isakmp policy 10
authentication rsa-sig
hash md5
encryption 3des
group 2
```

```
crypto isakmp key Cisco123 address 2.2.2.2
```

```
crypto ipsec transform-set ts esp-3des esp-sha-hmac
```

```
access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
crypto map vpn 10 ipsec-isakmp
set peer 2.2.2.2
match address 100
set transform-set ts
set pfs group2
```

```
ntp server 192.168.10.10
```

>> SITE2 <<

```
hostname R2
ip domain-name routehub.local
```

```
clock timezone pst -8
clock summer pst recurring
```

```
ip host ca-server 192.168.10.10
```

```
crypto key generate rsa
crypto ca identity ipsec-ca
enrollment mode ra
enrollment url http://ca-server:90/certsrv/mscep/mscep.dll
crypto ca authenticate ipsec-ca
crypto ca enroll ipsec-sa
```

```
interface fastethernet0
description WAN interface
ip address 2.2.2.2 255.255.255.252
crypto map vpn
no shutdown
```

```
interface fastethernet1
description LAN interface
ip address 192.168.20.1 255.255.255.0
no shutdown
```

```
crypto isakmp policy 10
authentication rsa-sig
hash md5
encryption 3des
group 2
```

```
crypto isakmp key Cisco123 address 1.1.1.1
```

```
crypto ipsec transform-set ts esp-3des esp-sha-hmac
```

```
access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
crypto map vpn 10 ipsec-isakmp
set peer 1.1.1.1
match address 100
set transform-set ts
set pfs group2
```

```
ntp server 192.168.10.10
```

Disabling ISAKMP Aggressive Mode

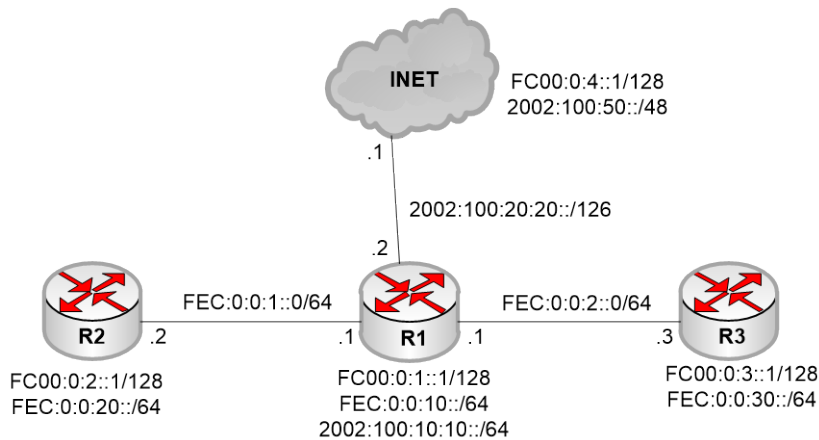
- How to disable ISAKMP aggressive mode and use Main Mode for IPSec VPN connections on a Cisco IOS device.

```
crypto isakmp aggressive-mode disable
```

IPSec VPN Monitoring Commands

```
show crypto isakmp sa
show crypto ipsec sa
```

IPV6: GENERAL



Base Configuration

- Enable IPv6 globally

```
ipv6 unicast-routing  
ipv6 cef
```

Interface using Static IPv6 Address

- Configure static IPv6 Site-Local address (Private IP) on GE0/1

```
>> R1 <<  
ipv6 unicast-routing  
ipv6 cef  
  
interface GigabitEthernet0/1  
  ipv6 address FEC:0:0:1::1/64  
  ipv6 enable
```


Interface using Dynamic IPv6 Address (EUI-64)

- Configure dynamic IPv6 Addresses on Vlan10 using EUI-64 (ICMP Stateless)

>> R1 <<

```
ipv6 unicast-routing  
ipv6 cef
```

```
interface Vlan10
```

```
  ipv6 address FEC:0:0:10::/64 eui-64
```

```
  ipv6 address 2002:100:10:10::/64 eui-64
```

```
  ipv6 enable
```

General Prefixes

- Configure alias for IPv6 prefix FEC:0:0:2/48 that can be used for easy configuration to the GE0/1 where the IPv6 address is configured using the alias followed by the interface-ID of the IP

>> R1 <<

```
ipv6 general-prefix RHG-R1-R3 FEC:0:0:2/48
```

```
interface GigabitEthernet0/2
```

```
  ipv6 address RHG-R1-R3 ::1/64
```

Disable Route Advertisements on Point-to-Point Links

- Disable route advertisement messages ; recommended for any point-to-point connection (e.g. Interface, Tunnel)

```
interface GigabitEthernet0/1
```

```
  ipv6 nd-suppress-ra
```

Tuning Neighbor Discovery

- Setting the "ipv6 nd reachable-time" to a more aggressive value allows the speed-up of the switch-over time, but it has the downside of significantly increasing the overhead of ND traffic.

```
interface GigabitEthernet0/1
  ipv6 nd reachable-time 15000
```

Monitor

```
show ipv6 routers
show ipv6 interface brief
show ipv6 neighbors
show ipv6 interface <interface-name>
```

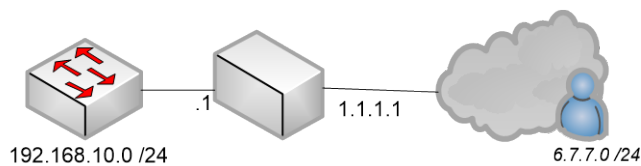
IPS

Solution/Services: Security

Related: N/A

IPS Module in Cisco ISR Series

- Enable IPS module in Cisco ISR router
- IP address that will be used on the IPS will be 192.168.10.12
- Permit all traffic if the IPS service module fails (fail-open)
- Only inspect HTTPS traffic, all other traffic will bypass IPS inspection
- Enable Promiscuous monitoring



```
ip route 192.168.10.12 255.255.255.255 ids-sensor0/0
```

```
interface IDS-Sensor0/0
ip unnumbered Loopback0
service-module fail-open
```

```
access-list 100 permit tcp any any eq 443
access-list 100 deny ip any any
```

```
ids-service-module monitoring promiscuous access-list 100
```

- Use this command for connecting to IPS module on the Cisco router

```
service-module ids-Sensor 0/0 session
```

IPX

Solution/Services: Other Protocols

Related: N/A

- Enable IPX
- On LAN facing interface (ethernet0) using IPX network 10 encapsulation SAP on R1
- On LAN facing interface (ethernet0) using IPX network 20 encapsulation SAP on R2
- On WAN facing interface (serial0) using IPX network 100
- Enable IPX EIGRP routing between R1 and R2

>> R1 <<

ipx routing

interface ethernet 0

ip address 192.168.10.1 255.255.255.0

ipx network 10 encapsulation sap

interface serial 0

description TO: R2

ip address 10.1.1.1 255.255.255.0

ipx network 100

no ipx router rip

ipx router eigrp 1

network all

>> R2 <<

ipx routing

interface ethernet 0

ip address 192.168.20.1 255.255.255.0

ipx network 20 encapsulation sap

interface serial 0

description TO: R1

ip address 10.1.1.2 255.255.255.0

ipx network 100

no ipx router rip

ipx router eigrp 1

network all

IRB

Solution/Services: LAN Switching

Related: N/A

- Configure bridging and routing for VLAN 10 interface

```
bridge irb
```

```
bridge 10 protocol ieee
```

```
bridge 10 route ip
```

```
interface FastEthernet1
```

```
switchport access vlan 10
```

```
interface Vlan10
```

```
no ip address
```

```
bridge-group 10
```

```
bridge-group 10 spanning-disabled
```

```
interface BVI10
```

```
ip address 192.168.10.1 255.255.255.0
```

```
no ip redirects
```

```
no ip unreachable
```

```
no ip proxy-arp
```

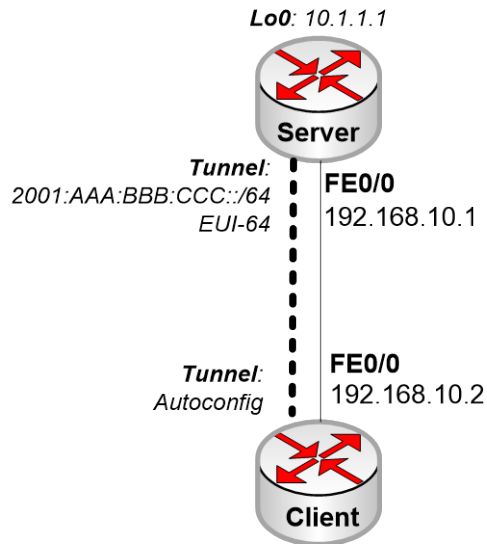
ISATAP

Solution/Services: IPv6

Related: N/A

ISATAP (Server and Client) on Cisco IOS

- ISATAP Server IPv4 Address: 10.1.1.1
- IPv6 Prefix (2001:AAA:BBB:CCC::/64 EUI-64) ISATAP Client will receive from ISATAP server



>> ISATAP Server <<

```
ipv6 unicast-routing
```

```
interface Loopback0  
ip address 10.1.1.1 255.255.255.255
```

```
interface fastethernet0/0  
ip address 192.168.10.1 255.255.255.0
```

```
interface Tunnel1  
no ip address  
no ip redirects
```

```
ipv6 address 2001:AAA:BBB:CCC::/64 eui-64
no ipv6 nd ra suppress
tunnel source Loopback0
tunnel mode ipv6ip isatap
```

>> ISATAP Client <<

```
interface fastethernet0/0
ip address 192.168.10.2 255.255.255.0

interface Tunnel1
no ip address
ipv6 address autoconfig
ipv6 enable
tunnel mode ipv6ip
tunnel source fastethernet0/0
tunnel destination 10.1.1.1

ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

ISDN PRI

Solution/Services: Media Connection

Related: Voice Gateway

Voice Gateway and PRI

- ISDN PRI (configured as a T1 CSS) connected to PSTN for only 3 channels for placing & receiving calls
- Channel 24 used for call signaling



```
controller T1 0/0/0  
framing esf  
clock source line primary  
linecode b8zs  
pri-group timeslots 1-3,24
```




JUMBO FRAMES

Solution/Services: Administration/System

Related: N/A

Jumbo Frames on Cisco Catalyst Switches for 10/100 Ports

- Configured globally for 10/100 switch ports. Requires restart for changing to take effect.

`system mtu 1998`

Jumbo Frames on Cisco Catalyst Switches for 1G Ports

- Configured globally for 1G switch ports. Requires restart for changing to take effect.

`system mtu jumbo 9000`

JUNIPER

Solution/Services: Firewall, VPN, Networking
Related: N/A

Troubleshooting High CPU Utilization on a Juniper NetScreen Firewall

- View the current CPU usage on the firewall appliance

get perf cpu detail

- Provide information on the hardware ASICs inside the appliance.

get sat 0 x

get sat 1 x

- Run these commands a few times. This will provide some details on the kind of packets going to the CPU.

get sat 0 d

get sat 0 d

get sat 1 d

get sat 1 d

get os task

get mem

get net-pak s

get ipak

get gate

get socket

get tcp

get pport

get route

get arp

get arp asic 0

get arp asic 1

- To view a specific session based on the source IP address

get session src-ip x.x.x.x

- Information to give to Juniper support if you have a valid support contract

get tech
set console page 50

! Get the few two pages to provide to support

get session
get alarm event
get log event
get log sy

Juniper NetScreen Firewall Troubleshooting Commands

get clock
get perf cpu all detail
get perf sess detail
get counter stat
get os task
get arp
get socket
get session info
get mem
get net-pak s

get arp asic 0
get arp asic 1
get sat 0 d
get sat 1 d
get sat 0 x-c
get sat 1 x-c
get sat 0 fr
get sat 1 fr

get log sys
get alarm event
get log event

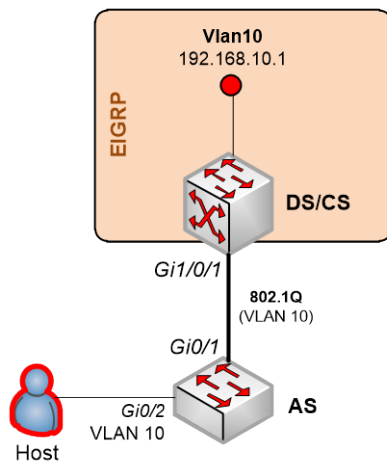
[L]

LAN CAMPUS DESIGN

Solution/Services: LAN
Related: N/A

Campus Design: Layer 2 Access with Layer 3 Distribution/Core

- Two-tier topology with routing (L3) enabled on the Core/Distribution only.
- L2 configured between Access and Core extending VLAN 10 which is routed on the Core.



>> ACCESS <<

```
vtp mode transparent  
vtp domain ROUTEHUB
```

```
vlan 10
name VLAN-10-USER1

interface GigabitEthernet0/1
description UPLINK: L3 Distribution/Core Switch
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10
no shutdown

interface GigabitEthernet0/2
description HOST
switchport mode access
switchport access vlan 10
no shutdown
```

>> DISTRIBUTION/CORE <<

```
ntp mode transparent
ntp domain ROUTEHUB

vlan 10
name VLAN-10-USER1

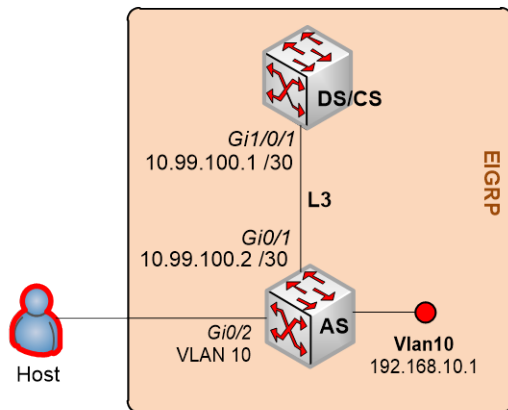
interface GigabitEthernet1/0/1
description UPLINK: L2 Access Switch
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10
no shutdown

interface Vlan10
ip address 192.168.10.1 255.255.255.0
no ip proxy-arp
no ip redirects
no ip unreachable
no shutdown

router eigrp 1
network 192.168.10.0
no auto-summary
```

Campus Design: Layer 3 Access with Layer 3 Distribution/Core

- Two-tier topology with routing (L3) enabled between the Core/Distribution and Access switches.
- VLAN 10 configured and routed on Access switch
- No L2 loops or VLAN management needed across topology.



>> ACCESS <<

```
vtp mode transparent
vtp domain ROUTEHUB
```

```
vlan 10
name VLAN-10-USER1
```

```
interface GigabitEthernet0/1
description UPLINK: L3 Distribution/Core Switch
no switchport
ip address 10.99.100.1 255.255.255.252
no shutdown
```

```
interface GigabitEthernet0/2
description HOST
switchport mode access
switchport access vlan 10
no shutdown
```

```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
no ip proxy-arp
no ip redirects
no ip unreachable
```

```
router eigrp 1
network 10.99.100.0 0.0.0.3
network 192.168.10.0
no auto-summary
```

```
>> DISTRIBUTION/CORE <<
interface GigabitEthernet1/0/1
description UPLINK: L3 Access Switch
no switchport
ip address 10.99.100.2 255.255.255.252
no shutdown

router eigrp 1
network 10.99.100.0 0.0.0.3
no auto-summary
```

LINUX SOLUTIONS

Solution/Services: Systems: Linux

Related: N/A

Adding Static Routes

- Static route defining subnet (192.168.20.0) and next-hop IP (192.168.10.1) to reach destination subnet

```
sudo route add -net 192.168.20.0/24 192.168.10.1
```


LLDP

Solution/Services: Protocol

Related: N/A

- LLDP Globally enabled on switch
- Voice VLAN: 10
- Data VLAN: 11

lldp run

```
interface FastEthernet1/0/1
description TO: Uplink with another switch
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,11
switchport mode trunk
```

```
interface FastEthernet1/0/5
description TO: Non-Cisco IP Phone
switchport access vlan 11
switchport mode access
switchport voice vlan 10
spanning-tree portfast
```

```
show lldp traffic
show lldp interface
show lldp neighbors detail
```

LLQ

Solution/Services: QoS: Queuing and Dropping
Related:

Go to [“QoS: Queuing and Dropping”](#)

LOAD INTERVAL

Solution/Services: Administration/System

Related: N/A

- View interface statistics every 60 seconds instead of 5 minutes (default)

```
interface FastEthernet0/0
```

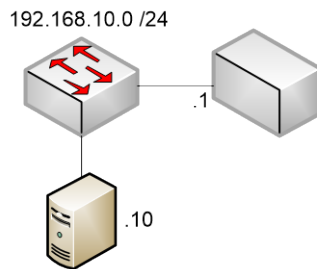
```
load-interval 60
```

LOGGING

Solution/Services: Administration/System, Management

Related: N/A

- Enable logging on Cisco IOS device (
- Sends level 0-7 (debugging) log messages to the buffer (up to 6KB before it overwrites what currently exists)
- Disable log messages to be disabled on the console or Telnet/SSH sessions (called "monitor")
- Send level 0-5 (warning) log message to the SYSLOG server at 192.168.10.10 sourced from the VLAN10 interface



```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

```
logging buffered 16384 debugging
no logging console
no logging monitor
logging trap warning
logging facility local4
logging source-interface Vlan10
logging 192.168.10.10
```

LOOPGUARD

Solution/Services: LAN Switching

Related: Spanning Tree Protocol

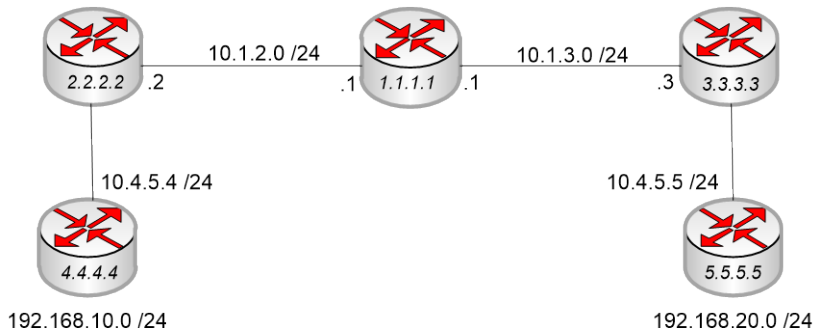
- Enable LoopGuard globally for all ports on L2/L3 Switch

spanning-tree loopguard default

L2TPV3

Solution/Services: Tunneling: L2VPN

Related: N/A



L2TPv3 using Static Tunnels

- L2TPv3: creates an isolated point-to-point L2 tunnel between two sites
- Build a logical ethernet connection (using L2TPv3 on service provider's network) between the two CE routers (4.4.4.4 and 5.5.5.5) configured on subnet 10.4.5.0/24.

```
>>PE1 (2.2.2.2)<<
interface Loopback0
ip address 2.2.2.2 255.255.255.255

interface FastEthernet0/1
description TO: MPLS P (1.1.1.1)
ip address 10.1.2.2 255.255.255.0
no shutdown

l2tp-class manual
cookie size 4

pseudowire-class manual
encapsulation l2tpv3
protocol none
ip local interface Loopback0

interface FastEthernet0/0
description TO: CE1-H (4.4.4.4)
no ip address
duplex auto
speed auto
xconnect 3.3.3.3 1 encapsulation l2tpv3 manual pw-class manual
l2tp id 1 1
```

```
l2tp cookie local 4 1
l2tp cookie remote 4 1
l2tp hello manual
```

>>PE2<<

```
interface Loopback0
ip address 3.3.3.3 255.255.255.255
```

```
interface FastEthernet0/1
ip address 10.1.3.3 255.255.255.0
no shutdown
```

```
l2tp-class manual
cookie size 4
```

```
pseudowire-class manual
encapsulation l2tpv3
protocol none
ip local interface Loopback0
```

```
interface FastEthernet0/0
no ip address
duplex auto
speed auto
xconnect 2.2.2.2 1 encapsulation l2tpv3 manual pw-class manual
l2tp id 1 1
l2tp cookie local 4 1
l2tp cookie remote 4 1
l2tp hello manual
```

>>CE1<<

```
interface Loopback0
ip address 4.4.4.4 255.255.255.255
```

```
interface FastEthernet0/0
ip address 10.4.5.4 255.255.255.0
```

```
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0
```

```
router eigrp 1
network 4.4.4.4 0.0.0.0
network 10.4.5.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

```
>>CE2<<
interface Loopback0
ip address 5.5.5.5 255.255.255.255

interface FastEthernet0/0
ip address 10.4.5.5 255.255.255.0

interface FastEthernet0/1
ip address 192.168.20.1 255.255.255.0

router eigrp 1
network 5.5.5.5 0.0.0.0
network 10.4.5.0 0.0.0.255
network 192.168.20.0
no auto-summary
```

L2TPv3 Monitoring Commands

```
show xconnect all
show l2tun tunnel
show l2tp session
show mpls l2transport vc <VC-ID> detail
```


[M]

MACROS

Solution/Services: Administration/System
Related: N/A

Macros for running Static Commands

- **Macro Summary:** Ping a list of IP addresses automatically

```
macro name macro_PING
```

```
do ping 192.168.1.1
```

```
do ping 4.2.2.2
```

```
@
```

```
macro global apply macro_PING
```

Macro using Parameters

- **Macro Summary:** this Macro will add new VLANs and VLAN SVIs automatically on a L2/L3 switch. This macro will also include parameters where we can enter specific details with the macro that will be applied.
- **"\$V"** = VLAN ID
- **"\$D"** = Name (Description)

```
macro name macro_new_VLAN
```

```
vlan $V
```

```
name $D
```

```
interface vlan $V
```

```
ip address 192.168.$V.1 255.255.255.0
```

```
no shutdown
```

```
@
```

- Apply macro on a L2/L3 switch. This will create a new VLAN, which will be VLAN123 and the description for this VLAN will be called TEST_VLAN.
- The subnet for this new VLAN will be 192.168.123.0 which includes the VLAN ID we will define in the macro.
- Note: the syntax "trace" means we want to see the output which is shown below

```
UC01TRA(config-if)#macro trace macro_new_VLAN $V 123 $D TEST_VLAN
```

```
Applying command... 'vlan 123'
```

```
Applying command... ' name TEST_VLAN'
```

```
Applying command... 'interface vlan 123'
```

```
Applying command... ' ip address 192.168.123.1 255.255.255.0'
```

```
Applying command... ' no shutdown '
```

Macro for Voice Port

- **Macro Summary:** this macro will create a configuration that can be applied to a voice switch port with connected IP phones and endpoints which will include VLANs and QoS. This can allow an engineer to define the macro with all the necessary configuration then allow a technician to simply apply the macro where needed on ports that are considered as voice ports
- DATA VLAN = 10, VOICE VLAN = 100

```
macro name macro_PORT_VOICE
```

```
switchport access vlan 10
```

```
switchport voice vlan 100
```

```
switchport priority extend cos 1
```

```
mls qos trust cos
```

```
mls qos trust device cisco-phone
```

```
@
```

```
SW1(config)#interface range fa0/6-8
```

```
SW1(config)#macro apply macro_PORT_VOICE
```

MD5 FILE VALIDATION

Solution/Services: Administration/System
Related:

- To verify the checksum of an IOS image

```
Router# verify /md5 flash:  
Verify filename []? c2900_ios.bin  
.....  
.....  
.....  
.....  
.....  
.....Done!  
verify /md5 (flash:c2900_ios.bin) = 0f369ed9e98756f179d4f29d6e7755d3
```

- To confirm if the specified MD5 checksum is valid with the IOS image

```
router# verify /md5 flash:c2900_ios.bin 0f369ed9e98756f179d4f29d6e7755d3  
.....  
.....  
.....  
.....  
.....  
.....Done!  
Verified (flash:c2900_ios.bin) = 0f369ed9e98756f179d4f29d6e7755d3
```

MGCP

Solution/Services: Voice & Unified Communications

Related: Voice Gateway

- Enable MGCP on Cisco IOS router on T1 0/3/0
- Point to Primary Cisco Unified CM server (192.168.10.10) and Secondary Cisco Unified CM (192.168.10.11)

```
hostname vgr01
```

```
ip domain name routehub.local
```

```
mgcp
```

```
mgcp call-agent 192.168.10.10
```

```
mgcp sdp simple
```

```
ccm-manager mgcp
```

```
ccm-manager fax protocol cisco
```

```
ccm-manager music-on-hold
```

```
ccm-manager config server 192.168.10.10
```

```
ccm-manager config
```

```
ccm-manager redundant-host 192.168.10.11
```

```
ccm-manager fallback-mgcp
```

```
ccm-manager switchback immediate
```

```
network-clock-participate wic 3
```

```
controller T1 0/3/0
```

```
framing esf
```

```
linecode b8zs
```

```
pri-group timeslots 1-24 service mgcp
```

MICROSOFT SOLUTIONS

Solution/Services: Systems: Microsoft
Related: N/A

Change MTU on Windows 7/Vista

- Change MTU on the NIC to 1452 Bytes

```
netsh interface ipv4 set subinterface "Local Area Connection" mtu=1452 store=persistent
```

MSConfig

- Access Microsoft startup configuration and services

```
msconfig
```

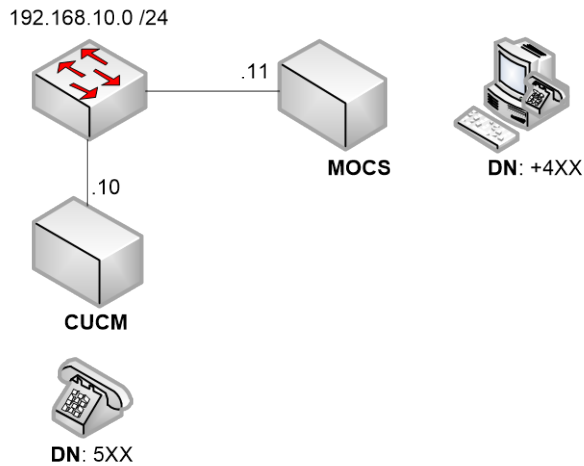
How to manually set the time server on Windows (from DOS)

- Adding 2 NTP servers: 0.pool.ntp.org and 1.pool.ntp.org

```
w32tm /config /update /manualpeerlist:"0.pool.ntp.org,0x8 1.pool.ntp.org,0x8" /syncfromflags:MANUAL
```

Voice between Cisco Unified CM and Microsoft OCS

- DID: 209-123-70XX
- OCS: 192.168.10.11 | DN 4XX
- UCM: 192.168.10.10 | DN 5XX



```
voice service voip
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
redirect ip2ip
h323
h225 timeout setup 20
h245 tunnel disable
h245 caps mode restricted
sip
rel1xx supported "rel100"
```

```
voice translation-rule 4
rule 1 /^.*(...)/ ^1/
```

```
voice translation-profile RHG-TP-OCS-CCM-internal
translate calling 4
```

```
dial-peer voice 900 voip
description Calling from OCS to CCM (internal)
translation-profile outgoing RHG-TP-OCS-CCM-internal
destination-pattern 5..
session protocol sipv2
session target ipv4:192.168.10.10
session transport tcp
codec g711ulaw
```

```
voice translation-rule 1
rule 1 /^\(1[2-9].....\)$/ /9\1/
rule 2 /^\[2-9].....\)$/ /9\1/
```

```
voice translation-rule 3
rule 1 /^.*\(.\) /20912360\1/
```

```
voice translation-profile RHG-TP-OCS-CCM-external
translate calling 3
translate called 1
```

```
dial-peer voice 901 voip
description LD Calling from OCS to CCM (external)
translation-profile outgoing RHG-TP-OCS-CCM-external
destination-pattern 1[2-9].....
session protocol sipv2
session target ipv4:192.168.10.10
session transport tcp
dtmf-relay sip-kpml
codec g711ulaw
```

```
dial-peer voice 903 voip
description Local Calling from OCS to CCM (external)
translation-profile outgoing RHG-TP-OCS-CCM-external
destination-pattern [2-9].....
session protocol sipv2
session target ipv4:192.168.10.10
session transport tcp
dtmf-relay sip-kpml
codec g711ulaw
```

```
voice translation-rule 2
rule 1 /^424/ /+424/
rule 2 /^418/ /+418/
rule 3 /^404/ /+404/
```

```
voice translation-profile RHG-TP-CCM-OCS-internal
translate called 2
```

```
dial-peer voice 902 voip
description Calling from CCM to OCS (internal)
translation-profile outgoing RHG-TP-CCM-OCS-internal
destination-pattern 4..
session protocol sipv2
session target ipv4:192.168.10.11
session transport tcp
dtmf-relay sip-kpml
codec g711ulaw
no vad
```

802.1x with Microsoft NPS

- Enable 802.1X on switch and interface GE7/1
- 802.1X user authentication will use RADIUS server 192.168.10.10 (shared key=Cisco123)
- Using Microsoft NPS solution
- **Networks:** User Network (VLAN 10), Guest Network (VLAN 11)

```
aaa group server radius IAS
server-private 192.168.10.10 key Cisco123
ip radius source-interface Vlan99
```

```
aaa authentication login default local
aaa authentication dot1x default group IAS
aaa authorization exec default local
aaa authorization network default none
aaa accounting dot1x default start-stop group IAS
```

```
aaa server radius policy-device
client 192.168.10.10 key Cisco123
```

```
authentication mac-move permit
authentication logging verbose
```

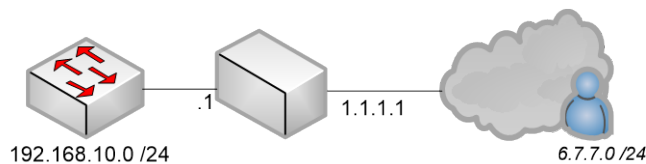
```
interface GigabitEthernet7/1
switchport access vlan 10
switchport mode access
authentication event no-response action authorize vlan 11
authentication event server alive action reinitialize
authentication host-mode multi-domain
authentication priority dot1x
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
authentication violation restrict
dot1x pae authenticator
dot1x timeout tx-period 3
spanning-tree portfast
```


MLPPP

Solution/Services: Media Connection: Bundles
Related: N/A

MLPPP

- Bundle two PPP enabled interfaces (Serial0/0/0 & Serial 0/0/1) using Multilink PPP (MLPPP) connecting to the ISP using group #1



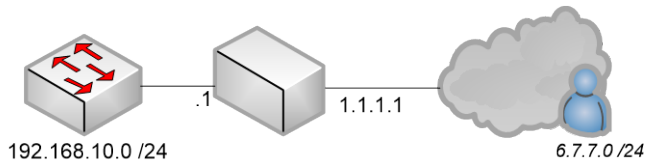
```
interface Multilink1
ip address 1.1.1.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
no cdp enable
ppp multilink
ppp multilink group 1
```

```
interface Serial0/0/0:0
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

```
interface Serial0/0/1:0
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

MLPPP using Cisco IOS 12.1

- MLPPP configuration using IOS 12.1
- Bundle two PPP enabled interfaces (Serial0 & Serial1) using Multilink PPP (MLPPP) connecting to the ISP using group #1



```
interface Multilink1
ip address 1.1.1.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
no cdp enable
ppp multilink
multilink-group 1
```

```
interface Serial0
no ip address
encapsulation ppp
no fair-queue
ppp multilink
multilink-group 1
```

```
interface Serial1
no ip address
encapsulation ppp
no fair-queue
ppp multilink
multilink-group 1
```

MODULES

Solution/Services: Administration/System

Related: N/A

Using Third-Party Optics in Cisco Devices

- Unsupported/Undocumented IOS command
- Allow support for third-party optics (SFP, GBIC)

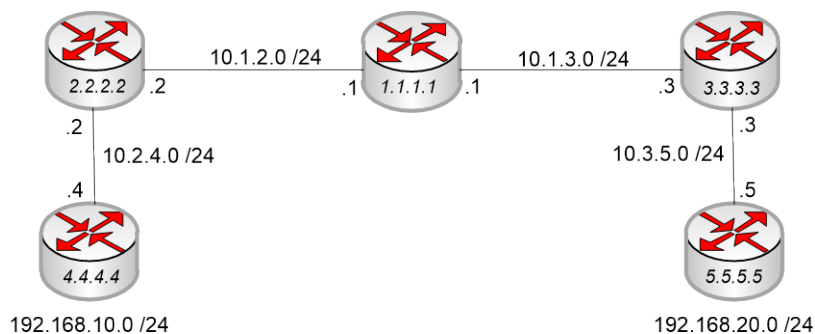
```
service unsupported-transceiver  
no errdisable detect cause gbic-invalid
```

MPLS VPN

Solution/Services: Tunneling: L3VPN

Related: N/A

MPLS VPN



- Enable MPLS on router (1.1.1.1) as a MPLS Provider (P) router
- Enable OSPF processing across the MPLS routers

>>P1 (1.1.1.1)<<

```
mpls label protocol ldp
```

```
interface Loopback0
```

```
ip address 1.1.1.1 255.255.255.255
```

```
interface FastEthernet0/0
```

```
ip address 10.1.2.1 255.255.255.0
```

```
mpls ip
```

```
interface FastEthernet0/1
```

```
ip address 10.1.3.1 255.255.255.0
```

```
mpls ip
```

```
router ospf 1
```

```
log-adjacency-changes
```

```
network 1.1.1.1 0.0.0.0 area 1
```

```
network 10.1.2.0 0.0.0.255 area 0
```

```
network 10.1.3.0 0.0.0.255 area 0
```

- Enable MPLS on routers (2.2.2.2 and 3.3.3.3) as Provider Edge (PE) routers with connected
- Enable OSPF processing across the MPLS routers

>>PE1<<

mpls label protocol ldp

interface Loopback0

ip address 2.2.2.2 255.255.255.255

interface FastEthernet0/0

ip address 10.1.2.2 255.255.255.0

mpls ip

router ospf 2

log-adjacency-changes

network 2.2.2.2 0.0.0.0 area 2

network 10.1.2.0 0.0.0.255 area 0

>>PE2<<

mpls label protocol ldp

interface Loopback0

ip address 3.3.3.3 255.255.255.255

interface FastEthernet0/0

ip address 10.1.3.2 255.255.255.0

mpls ip

router ospf 3

log-adjacency-changes

network 3.3.3.3 0.0.0.0 area 3

network 10.1.3.0 0.0.0.255 area 0

- Configure VRF on MPLS PE routers for Client A using an RD of 10:100. VRF will be called CEA for Client A
- Associate the "Client A" VRF to the Client downlink router ports.

>>PE1<<

ip vrf CEA

rd 10:100

route-target export 10:100

route-target import 10:100

interface FastEthernet0/1

ip vrf forwarding CEA

ip address 10.2.4.2 255.255.255.0

>>PE2<<

ip vrf CEA

rd 10:100

route-target export 10:100

route-target import 10:100

```
interface FastEthernet0/1
ip vrf forwarding CEA
ip address 10.3.5.3 255.255.255.0
```

- Configure MP-BGP between the MPLS PE routers extending the advertised networks for Client A
- Client A sites will be configured to use EIGRP
- On MPLS PE routers, all learned EIGRP ASN 10 routes from Client A would be redistributed into MP-BGP to be advertised to the other MPLS PE router with a connected Client A device. And BGP redistribution into the EIGRP ASN 10 for Client A (in VRF CEA).

>>PE1<<

```
router bgp 6778
no synchronization
bgp log-neighbor-changes
neighbor 3.3.3.3 remote-as 6778
neighbor 3.3.3.3 update-source Loopback0
no auto-summary
```

```
address-family vpnv4
neighbor 3.3.3.3 activate
neighbor 3.3.3.3 send-community extended
exit-address-family
```

```
address-family ipv4 vrf CEA
redistribute eigrp 10
no synchronization
exit-address-family
```

```
router eigrp 1
address-family ipv4 vrf CEA
redistribute bgp 6778
network 10.2.4.0 0.0.0.255
default-metric 10000 1 255 1 1500
no auto-summary
autonomous-system 10
exit-address-family
```

>>PE2<<

```
router bgp 6778
no synchronization
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 6778
neighbor 2.2.2.2 update-source Loopback0
no auto-summary
```

```
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
exit-address-family
```

```
address-family ipv4 vrf CEA
redistribute eigrp 10
no synchronization
exit-address-family
```

```
router eigrp 1
address-family ipv4 vrf CEA
redistribute bgp 6778
network 10.3.5.0 0.0.0.255
default-metric 10000 1 255 1 1500
no auto-summary
autonomous-system 10
exit-address-family
```

- Customer network devices (CE1 and CE2) configured for EIGRP in ASN 10 peering with its connected MPLS PE router.

>>CE1<<

```
interface Loopback0
ip address 4.4.4.4 255.255.255.255

interface FastEthernet0/0
description TO: PE1
ip address 10.2.4.4 255.255.255.0

interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0

router eigrp 10
network 4.4.4.4 0.0.0.0
network 192.168.10.0 0.0.0.255
no auto-summary
no eigrp log-neighbor-changes
```

>>CE2<<

```
interface Loopback0
ip address 5.5.5.5 255.255.255.255

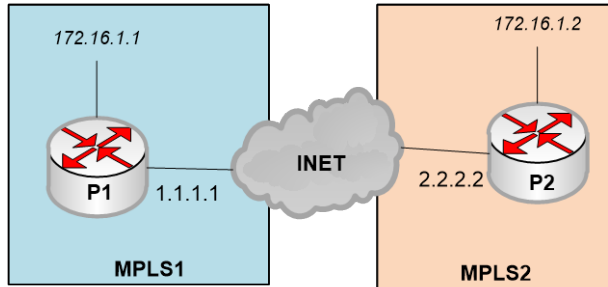
interface FastEthernet0/0
description TO: PE2
ip address 10.3.5.5 255.255.255.0

interface FastEthernet0/1
ip address 192.168.20.1 255.255.255.0

router eigrp 10
network 5.5.5.5 0.0.0.0
network 192.168.20.0 0.0.0.255
no auto-summary
no eigrp log-neighbor-changes
```

MPLS over GRE

- Configure MPLS over GRE tunnel between P1 and P2 which each exist in different MPLS networks



>>P1 in MPLS1<<

```
mpls label protocol ldp
```

```
interface Tunnel0
```

```
ip address 172.16.1.1 255.255.255.0
```

```
tunnel source FastEthernet1/0
```

```
tunnel destination 2.2.2.2
```

```
mpls ip
```

```
interface FastEthernet1/0
```

```
ip address 1.1.1.1 255.255.255.0
```

```
router ospf 1
```

```
network 172.16.1.0 0.0.0.255 area 0
```

>>P2 in MPLS2<<

```
mpls label protocol ldp
```

```
interface Tunnel0
```

```
ip address 172.16.1.2 255.255.255.0
```

```
tunnel source FastEthernet1/0
```

```
tunnel destination 1.1.1.1
```

```
mpls ip
```

```
interface FastEthernet1/0
```

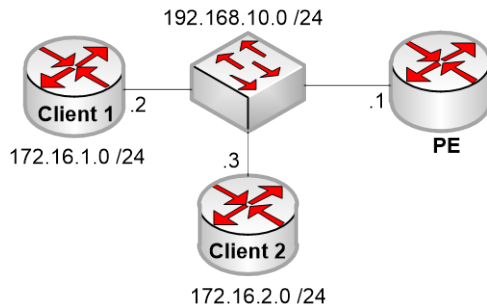
```
ip address 2.2.2.2 255.255.255.0
```

```
router ospf 1
```

```
network 172.16.1.0 0.0.0.255 area 0
```


VRF Selection

- On the MPLS PE router two VRF instances are configured. One for Client 1 or A (VRF CEA) and one for Client 2 or B (VRF CEB)
- On MPLS PE, any communication from the Client A network (172.16.1.0) will be assigned to VRF CEA. Any communication from the Client B network (172.16.2.0) will be assigned to VRF CEB.



>>PE<<

```

ip vrf CEA
rd 50:500
route-target export 50:500
route-target import 50:500
  
```

```
access-list 1 permit 172.16.1.0 0.0.255.255
```

```

route-map ROUTEHUB-PBR-VS permit 10
match ip address 1
set vrf CEA
  
```

```
ip route vrf Client1 172.16.1.0 255.255.255.0 192.168.10.2
```

```

ip vrf CEB
rd 60:600
route-target export 60:600
route-target import 60:600
  
```

```
access-list 2 permit 172.16.2.0 0.0.255.255
```

```

route-map ROUTEHUB-PBR-VS permit 20
match ip address 2
set vrf CEB
  
```

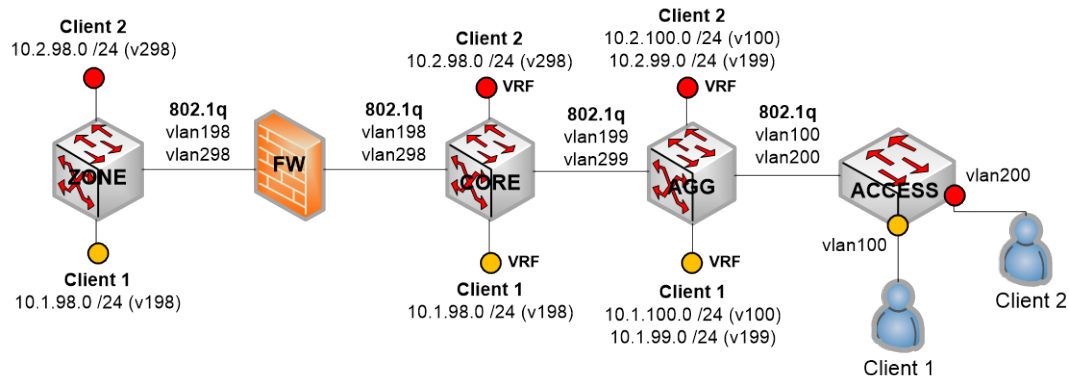
```
ip route vrf Client2 172.16.2.0 255.255.255.0 192.168.10.3
```

```

interface FastEthernet0/0
ip vrf receive CEA
ip vrf receive CEB
ip address 192.168.10.1 255.255.255.0
ip policy route-map ROUTEHUB-PBR-VS
  
```

MULTI-VRF CE (VRF-LITE)

Solution/Services: Tunneling: L3VPN
Related: N/A



Access Configuration (No VRF)

- Access Switch configured for two client networks. Client1 will exist in VLAN 100 and Client2 will exist in VLAN 200.
- VLANs extended across 802.1Q connection to the Aggregation switch

```
vlan 100  
name VLAN-CL1
```

```
vlan 200  
name VLAN-CL2
```

```
interface FastEthernet0/1  
description TO: LAN Distribution  
switchport trunk allowed vlan 100,200  
switchport mode trunk  
switchport nonegotiate  
carrier-delay msec 0
```

```
interface FastEthernet0/2  
description HOST: Client 1  
switchport access vlan 100  
switchport mode access  
spanning-tree portfast  
spanning-tree bpduguard enable  
spanning-tree bpdufilter enable
```

```

interface FastEthernet0/3
description HOST: Client 2
switchport access vlan 200
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree bpdufilter enable

```

Distribution/Aggregation Configuration (VRF)

- VRF enabled
- A separate routing table of learned routes will exist for Client1 network and Client2 network. They are not shared in the global routing table.
- Client 1 will exist in VLAN 100. All routing within Client 1 network will be isolated in VRF CL1 configured for OSPF. The uplink/downlink to the Core for Client 1 traffic will exist in VLAN199.
- Client 2 will exist in VLAN 200. All routing within Client 2 network will be isolated in VRF CL2 configured for OSPF. The uplink/downlink to the Core for Client 2 traffic will exist in VLAN299.

```

vlan 100
name VLAN-CL1

```

```

vlan 199
name VLAN-CL1-ICT1

```

```

ip vrf CL1
rd 10:100
route-target export 10:100
route-target import 10:100

```

```

interface Vlan100
description VLAN: Client 1 LAN
ip vrf forwarding CL1
ip address 10.1.100.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp

```

```

interface Vlan199
description VLAN: Client 1 ICT with Core
ip vrf forwarding CL1
ip address 10.1.99.2 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp

```

```

router ospf 10 vrf CL1
area 10 range 10.1.0.0 255.255.0.0
network 10.1.99.0 0.0.0.3 area 0
network 10.1.100.0 0.0.0.255 area 10

```

```
vlan 200  
name VLAN-CL2
```

```
vlan 299  
name VLAN-CL2-ICT1
```

```
ip vrf CL2  
rd 10:200  
route-target export 10:200  
route-target import 10:200
```

```
interface Vlan200  
description VLAN: Client 2 LAN  
ip vrf forwarding CL2  
ip address 10.2.200.1 255.255.255.0  
no ip redirects  
no ip unreachable  
no ip proxy-arp
```

```
interface Vlan299  
description VLAN: Client 2 ICT with Core  
ip vrf forwarding CL2  
ip address 10.2.99.2 255.255.255.252  
no ip redirects  
no ip unreachable  
no ip proxy-arp
```

```
router ospf 20 vrf CL2  
area 20 range 10.2.0.0 255.255.0.0  
network 10.2.99.0 0.0.0.3 area 0  
network 10.2.200.0 0.0.0.255 area 20
```

```
interface GigabitEthernet0/1  
description TO: LAN Core  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 100,200,199,299  
switchport mode trunk  
switchport nonegotiate  
carrier-delay msec 0
```

```
interface GigabitEthernet0/2  
description TO: LAN Access  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 100,200  
switchport mode trunk  
switchport nonegotiate  
carrier-delay msec 0
```

Core Configuration (VRF)

- VRF enabled
- A separate routing table of learned routes will exist for Client1 network and Client2 network. They are not shared in the global routing table.
- All routing within Client 1 network will be isolated in VRF CL1 configured for OSPF. The uplink to the Zone Router will exist in VLAN 198. The downlink to the Aggregation for Client 1 traffic will exist in VLAN199.
- All routing within Client 2 network will be isolated in VRF CL2 configured for OSPF. The uplink to the Zone Router will exist in VLAN 298. The downlink to the Aggregation for Client 1 traffic will exist in VLAN299.

```
vlan 198  
name VLAN-CL1-ICT2
```

```
vlan 199  
name VLAN-CL1-ICT1
```

```
ip vrf CL1  
rd 10:100  
route-target export 10:100  
route-target import 10:100
```

```
interface Vlan198  
ip vrf forwarding CL1  
ip address 10.1.98.2 255.255.255.252  
no ip redirects  
no ip unreachableables  
no ip proxy-arp
```

```
interface Vlan199  
ip vrf forwarding CL1  
ip address 10.1.99.1 255.255.255.252  
no ip redirects  
no ip unreachableables  
no ip proxy-arp
```

```
router ospf 10 vrf CL1  
network 10.1.98.0 0.0.0.3 area 0  
network 10.1.99.0 0.0.0.3 area 0
```

```
vlan 298  
name VLAN-CL2-ICT2
```

```
vlan 299  
name VLAN-CL2-ICT1
```

```
ip vrf CL2  
rd 10:200  
route-target export 10:200  
route-target import 10:200
```

```
interface Vlan298  
ip vrf forwarding CL2  
ip address 10.2.98.2 255.255.255.252  
no ip redirects  
no ip unreachableables  
no ip proxy-arp
```

```
interface Vlan299
ip vrf forwarding CL2
ip address 10.2.99.1 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp

router ospf 20 vrf CL2
network 10.2.98.0 0.0.0.3 area 0
network 10.2.99.0 0.0.0.3 area 0
```

```
interface GigabitEthernet0/1
description TO: LAN Core
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 198,298
switchport mode trunk
switchport nonegotiate
carrier-delay msec 0
```

```
interface GigabitEthernet0/2
description TO: LAN Access
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 199,299
switchport mode trunk
switchport nonegotiate
carrier-delay msec 0
```

Zone Configuration (No VRF)

- No VRF configuration
- Zone Router's global routing table will contain both client network's learned routes.
- All routes learned via OSPF for Client1 will be redistributed into the OSPF domain for Client2. The downlink to the Core Router will exist in VLAN 198.
- All routes learned via OSPF for Client2 will be redistributed into the OSPF domain for Client1. The downlink to the Core Router will exist in VLAN 298.

```
ip access-list standard CL1-ACL
permit 10.1.0.0 0.0.255.255
```

```
ip access-list standard CL2-ACL
permit 10.2.0.0 0.0.255.255
```

```
vlan 198
name VLAN-CL1-ICT2
```

```
interface Vlan198
ip address 10.1.98.1 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
```

```
router ospf 10
redistribute ospf 20 subnets
default-information originate always
distribute-list CL2-ACL out ospf 20
```

```
vlan 298
name VLAN-CL2-ICT2
```

```
interface Vlan298
ip address 10.2.98.1 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
```

```
router ospf 20
redistribute ospf 10 subnets
network 10.2.98.0 0.0.0.3 area 0
default-information originate always
distribute-list CL1-ACL out ospf 10
```

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 198,298
switchport mode trunk
switchport nonegotiate
carrier-delay msec 0
```

Firewall Between Zone and Core

- Two virtual firewalls defined for each client network using the tagged VLANs that are configured between the Core and the Zone router (Client1 is using VLAN198 and Client2 is using VLAN298)

```
mode multiple
firewall transparent
```

```
interface gigabitethernet 0.198
no shutdown
```

```
interface gigabitethernet 1.198
no shutdown
```

```
context CL1-FW
allocate-interface gigabitethernet 0.198
allocate-interface gigabitethernet 1.198
configure disk0://CL1-FW.cfg
```

```
interface gigabitethernet 0.298
no shutdown
```

```
interface gigabitethernet 1.298
no shutdown
```

```
context CL2-FW
allocate-interface gigabitethernet 0.298
allocate-interface gigabitethernet 1.298
configure disk0://CL2-FW.cfg
```

- Firewall policy and configuration for Client1 network

```
context CL1-FW
```

```
hostname CL1-FW
domain c1.routehub.local
```

```
passwd secret123
enable password secret123
```

```
interface gigabitethernet 0.198
nameif outside
security-level 0
no shutdown
```

```
interface gigabitethernet 1.198
nameif inside
security-level 100
no shutdown
```



```
access-list CL1-ACL extended permit 89 any any
access-list CL1-ACL extended permit tcp any host 10.2.200.100 eq 8080
access-list CL1-ACL extended permit tcp any host 10.2.200.101 eq 22
access-list CL1-ACL extended permit tcp any host 10.2.200.102 eq 3389

access-group CL1-ACL in interface outside
```

- Firewall policy and configuration for Client2 network

```
context CL2-FW
```

```
hostname CL2-FW
domain c2.routehub.local
```

```
passwd secret123
enable password secret123
```

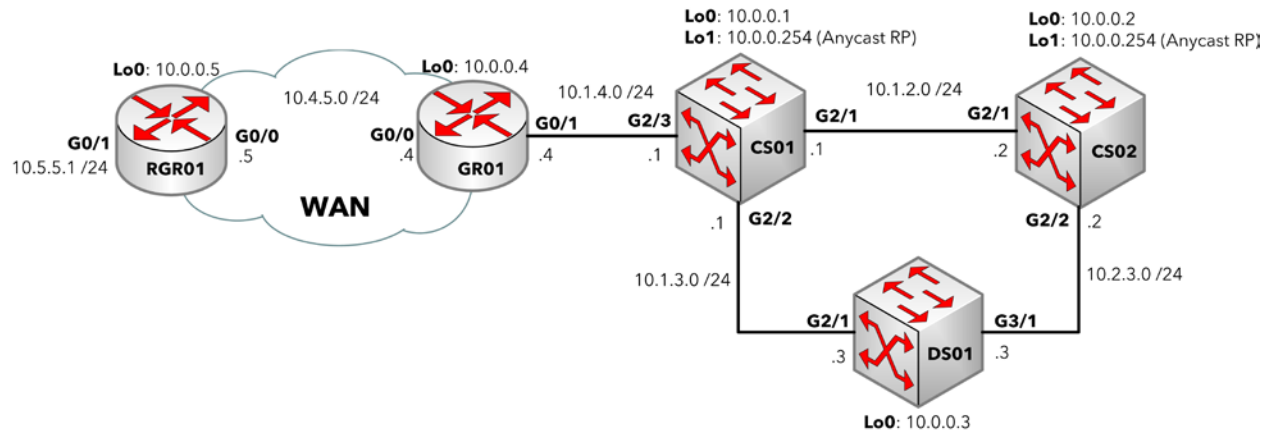
```
interface gigabitethernet 0.298
 nameif outside
 security-level 0
 no shutdown
```

```
interface gigabitethernet 1.298
 nameif inside
 security-level 100
 no shutdown
```

```
access-list CL2-ACL extended permit 89 any any
access-list CL2-ACL extended permit tcp any host 10.1.100.100 eq 8080
access-list CL2-ACL extended permit tcp any host 10.1.100.101 eq 22
access-list CL2-ACL extended permit tcp any host 10.1.100.102 eq 3389
```

```
access-group CL2-ACL in interface outside
```

MULTICAST



Below reflects a practical deployment and configuration of IPv4 Multicast:

CS01

```
ip multicast-routing
```

```
interface Loopback0
ip address 10.0.0.1 255.255.255.255
ip pim sparse-mode
```

```
interface Loopback1
ip address 10.0.0.254 255.255.255.255
ip pim sparse-mode
```

```
interface GigabitEthernet2/1
description TO: CS02
ip address 10.1.2.1 255.255.255.0
ip pim sparse-mode
```

```
interface GigabitEthernet2/2
description TO: DS01
ip address 10.1.3.1 255.255.255.0
ip pim sparse-mode
```

```
interface GigabitEthernet2/3
description TO: GR01
ip address 10.1.4.1 255.255.255.0
ip pim sparse-mode
```

! configure switch to discover multicast RP

```
ip pim autorp listener (or ip pim auto-rp listener)
```

```
ip pim register-source Loopback0
```

! advertise RP address with multicast groups that this switch is willing to serve as the candidate RP to the AutoRP mapping agents.

```
access-list 10 permit 239.1.0.0 0.0.255.255
```

```
ip pim send-rp-announce Loopback1 scope 32 group-list 10
```

! configures AutoRP mapping agent which will listen for the RP and then advertise it to the rest of the network.

```
ip pim send-rp-discovery Loopback0 scope 32
```

! configure Multicast Source Discovery Protocol (MSDP) for RP redundancy

```
ip msdp peer 10.0.0.2 connect-source Loopback0
```

```
ip msdp cache-sa-state
```

```
ip msdp originator-id Loopback0
```

CS02

```
ip multicast-routing
```

```
interface Loopback0
```

```
ip address 10.0.0.2 255.255.255.255
```

```
ip pim sparse-mode
```

```
interface Loopback1
```

```
ip address 10.0.0.254 255.255.255.255
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet2/1
```

```
description TO: CS01
```

```
ip address 10.1.2.2 255.255.255.0
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet2/2
```

```
description TO: DS01
```

```
ip address 10.2.3.2 255.255.255.0
```

```
ip pim sparse-mode
```

```
access-list 10 permit 239.1.0.0 0.0.255.255
```

```
ip pim autorp listener (or ip pim auto-rp listener)
```

```
ip pim register-source Loopback0
```

```
ip pim send-rp-announce Loopback1 scope 32 group-list 10
```

```
ip pim send-rp-discovery Loopback0 scope 32
```

```
ip msdp peer 10.0.0.1 connect-source Loopback0
```

```
ip msdp cache-sa-state
```

```
ip msdp originator-id Loopback0
```

DS01

```
ip multicast-routing
```

```
ip pim autorp listener
```

```
ip pim register-source Loopback0
```

```
interface Loopback0
```

```
ip address 10.0.0.5 255.255.255.255
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet2/1
```

```
description TO: CS01
```

```
ip address 10.1.3.3 255.255.255.0
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet3/1
```

```
description TO: CS02
```

```
ip address 10.2.3.3 255.255.255.0
```

```
ip pim sparse-mode
```

GR01

```
ip multicast-routing
```

```
ip pim autorp listener
```

```
ip pim register-source Loopback0
```

```
interface Loopback0
```

```
ip address 10.0.0.4 255.255.255.255
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet0/0
```

```
description TO: WAN (RGR01)
```

```
ip address 10.4.5.4 255.255.255.0
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet0/1
```

```
description TO: CS01
```

```
ip address 10.1.4.4 255.255.255.0
```

```
ip pim sparse-mode
```

RGR01

ip multicast-routing

ip pim autorp listener

ip pim register-source Loopback0

interface Loopback0

ip address 10.0.0.5 255.255.255.255

ip pim sparse-mode

interface GigabitEthernet0/0

description TO: WAN (GR01)

ip address 10.4.5.5 255.255.255.0

ip pim sparse-mode

interface GigabitEthernet0/1

description TO: LAN

ip address 10.5.5.1 255.255.255.0

ip pim sparse-mode

MULTICAST: MONITORING

Solution/Services: Multicast

Related: PIM

Layer 2 Switch Commands

show ip igmp profile
show ip igmp snooping
show igmp mode
show igmp querier information
show igmp stat
show cgmp
show mls multicast
show mls multicast entry
show mls multicast statistics
show multicast group <mac-address>
show multicast group count
show multicast protocols status
show multicast router

Layer 3 Router/Switch Commands

show ip mroute
show ip mroute count
show ip mroute <multicast-address> count
show ip mroute active
show ip mcache
show ip mpcket
show ip pim interface
show ip pim neighbor
show ip pim rp
show mls rp ip multicast
show ip rpf

MSDP Commands

show ip msdp count
show ip msdp peer
show ip msdp sa-cache
show ip mdp summary

Other Commands

show ip igmp group
show ip igmp interface vlan3
show igmp groupinfo <vlan> <mac-address>
show cam static <vlan>
show ip igmp group
show mls ip multicast group <multicast-address>

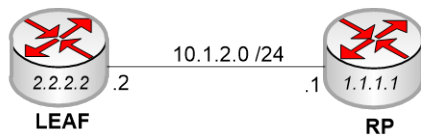
MULTICAST: RP

Solution/Services: Multicast

Related: PIM

Static RP

- Multicast Routing: PIM Sparse Mode
- Static RP pointing to RP router (1.1.1.1)



>> RP ROUTER <<

```
ip multicast-routing
```

```
interface Loopback0
```

```
ip address 1.1.1.1 255.255.255.255
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet0/1
```

```
no switchport
```

```
ip address 10.1.2.1 255.255.255.0
```

```
ip pim sparse-mode
```

```
ip pim rp-address 1.1.1.1
```

>> LEAF ROUTER (R2) <<

```
ip multicast-routing
```

```
interface Loopback0
```

```
ip address 2.2.2.2 255.255.255.255
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet0/2
```

```
no switchport
```

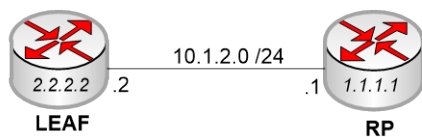
```
ip address 10.1.2.2 255.255.255.0
```

```
ip pim sparse-mode
```

```
ip pim rp-address 1.1.1.1
```

Auto-RP

- Multicast Routing: PIM Sparse Mode
- Auto RP pointing to RP router
- Auto RP IP will be 1.1.1.1
- Auto RP will announce multicast group 239.192.240.0 to all PIM enabled routers



>> RP ROUTER <<

```
ip multicast-routing
```

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
ip pim sparse-dense-mode
```

```
interface GigabitEthernet0/1
no switchport
ip address 10.1.2.1 255.255.255.0
ip pim sparse-mode
```

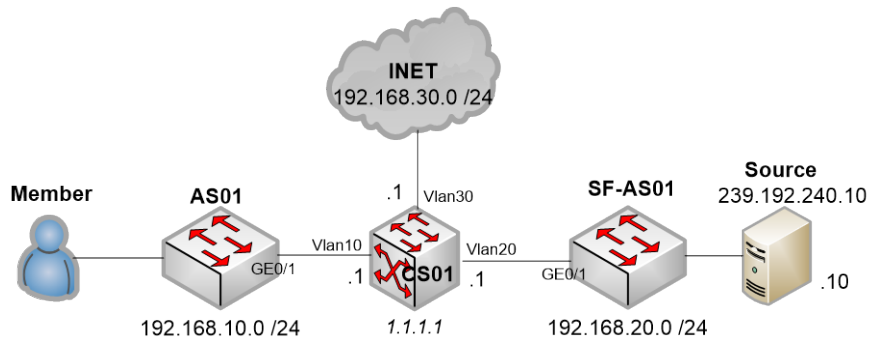
```
access-list 1 permit 239.192.240.0 0.0.0.255
```

```
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback0 scope 16
```


MULTICAST: SECURITY

Solution/Services: Multicast: Security

Related: N/A



Rogue Source Protection

- Configured on RP router (CS01)
- Only Multicast servers (source) from the 192.168.20.0/24 network are permitted to announce Multicast networks 224.X.X.X for Multicast Registration to the RP router (CS01)

```
ip access-list extended permitted-ucast-sources
permit ip 192.168.20.0 0.0.0.255 224.0.0.0 15.255.255.255
```

```
ip pim accept-register list permitted-ucast-sources
```

Rogue Source Protection for Auto-RP

- Configured on RP router (CS01)
- Specify the valid Auto-RP router(s) on the network
- Specify valid multicast groups the Auto-RP can advertise

```
access-list 10 permit 1.1.1.1
access-list 11 permit 239.192.240.10
```

```
ip pim rp-announce-filter rp-list 10 group-list 11
```

IGMP Group Security (On Routers)

- Configured on Multicast routers with connected hosts that could join a multicast group.
- Specify the multicast groups (239.192.240.10) that members off of the connected interface (VLAN10) can join

```
access-list 10 permit 239.192.240.10
```

```
interface Vlan10  
ip address 192.168.10.1 255.255.255.0  
ip igmp access-group 10
```

IGMP Filter (On Switches)

- Configured on Cisco Catalyst Switches with connected hosts that could join a multicast group.
- Specify the multicast groups (239.192.X.X) that members off of GE0/1 can join

```
>> AS01 <<  
access-list 1 permit 239.192.0.0 0.59.255.255
```

```
interface GigabitEthernet0/1  
description TO: R1  
ip igmp filter 1
```

RP Multicast Group Registration Protection

- Specify what multicast groups (224.X.X.X) can register with the RP (CS01; 1.1.1.1)

```
ip access-list standard ROUTEHUB-ACL-MCAST  
permit 224.0.0.0 15.255.255.255
```

```
ip pim rp-address 1.1.1.1 ROUTEHUB-ACL-MCAST override
```

Multicast Boundary Protection

- Filter multicast groups (224.X.X.X) to not be transmitted nor received beyond the interface VLAN30

```
ip access-list standard pim-local-domain  
permit 224.0.0.0 15.255.255.255
```

```
interface Vlan30  
ip address 192.168.30.1 255.255.255.0  
ip pim bsr-border  
ip multicast boundary pim-local-domain  
ip multicast ttl-threshold 32
```

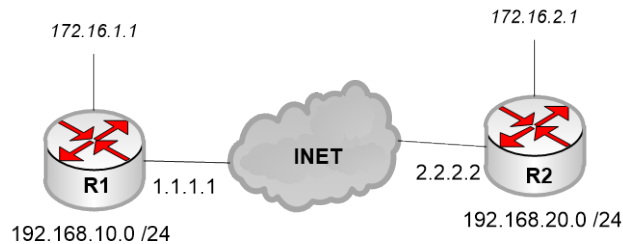
MSDP

Solution/Services: Multicast

Related: PIM

MSDP

- R1 exist in one Multicast domain acting as the RP
- R2 exist in another Multicast domain acting as the RP
- Configure MSDP to connect the two Multicast domains together



>> R1 <<

```
ip multicast-routing
```

```
interface Loopback0
```

```
ip address 172.16.1.1 255.255.255.255
```

```
ip pim sparse-mode
```

```
interface FastEthernet0/0
```

```
ip address 1.1.1.1 255.255.255.0
```

```
ip pim rp-address 172.16.1.1
```

```
ip msdp peer 172.16.2.1 connect-source Loopback0
```

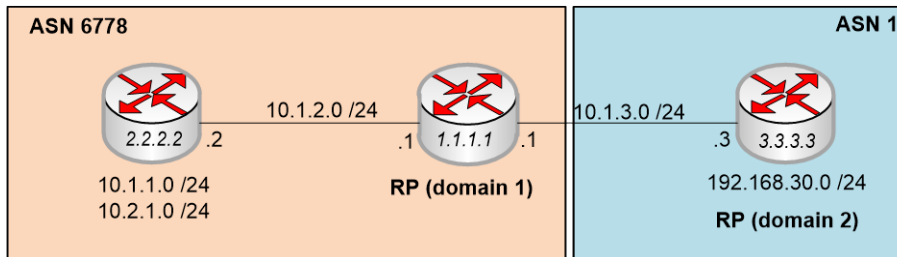
```
ip msdp description 172.16.2.1 Connecting to remote RP router
```

```
ip msdp cache-sa-state
```

```
ip msdp originator-id Loopback0
```

MSDP and MBGP (External Design)

- MSDP and MBGP External Design Configuration Example
- R1 (1.1.1.1) and R2 (2.2.2.2) exist in Multicast domain 1 where R1 is the RP
- R3 (3.3.3.3) exist in Multicast domain 2 and acting as the RP
- Configure MSDP to connect the two Multicast domains together
- **Reference:** For additional Multicast Security go to "Multicast: Security"



>> R1 <<

```
ip multicast-routing
```

```
interface Loopback0
```

```
ip address 1.1.1.1 255.255.255.255
```

```
ip pim sparse-mode
```

```
ip pim rp-address 1.1.1.1
```

```
ip msdp peer 3.3.3.3 connect-source Loopback0
```

```
ip msdp description 3.3.3.3 ISP RP ROUTER
```

```
ip msdp cache-sa-state
```

```
ip msdp originator-id Loopback0
```

```
router bgp 6778
```

```
neighbor 10.1.3.3 remote-as 1
```

```
address-family ipv4
```

```
neighbor 10.1.3.3 activate
```

```
exit-address-family
```

```
address-family ipv4 multicast
```

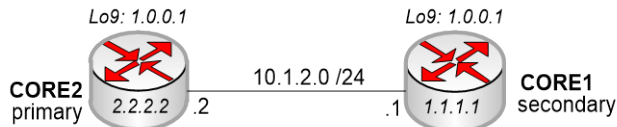
```
neighbor 10.1.3.3 activate
```

```
no auto-summary
```

```
exit-address-family
```

Redundancy using MSDP and Anycast (Internal Design)

- MSDP Internal Design Configuration Example to provide RP Redundancy
- CORE2 will be the Primary RP router and CORE1 will be the Secondary RP router
- RP will be 1.0.0.1 (Anycast)
- MSDP peer IP for CORE1 will be 1.1.1.1 (Loopback interface)
- MSDP peer IP for Core2 will be 2.2.2.2 (Loopback interface)
- Anycast RP will announce multicast group 239.0.0.0 to all PIM enabled routers
- **Reference:** For additional Multicast Security go to "Multicast: Security"



>> CORE1 <<

ip multicast-routing distributed

interface Loopback0

ip address 1.1.1.1 255.255.255.255

ip pim sparse-mode

interface Loopback9

ip address 1.0.0.1 255.255.255.255

ip pim sparse-mode

interface GigabitEthernet1/0/1

no switchport

ip address 10.1.2.1 255.255.255.0

ip pim sparse-mode

ip access-list standard ROUTEHUB-ACL-MCAST

permit 239.0.0.0 0.255.255.255

ip pim rp-address 1.0.0.1 ROUTEHUB-ACL-MCAST override

ip msdp peer 2.2.2.2 connect-source Loopback0

ip msdp description 2.2.2.2 routehub-csr02

ip msdp cache-sa-state

ip msdp originator-id Loopback0

ip msdp ttl-threshold 10.1.2.2 32

access-list 100 permit ip 239.0.0.0 0.255.255.255 host 2.2.2.2

ip msdp sa-filter out 2.2.2.2 list 100

>> CORE2 <<

ip multicast-routing distributed

interface Loopback0

ip address 2.2.2.2 255.255.255.255

ip pim sparse-mode

interface Loopback9

ip address 1.0.0.1 255.255.255.255

ip pim sparse-mode

interface GigabitEthernet1/0/1

description CORE1

no switchport

ip address 10.1.2.2 255.255.255.0

ip pim sparse-mode

interface GigabitEthernet1/0/2

description WAN-ROUTER

no switchport

ip address 10.1.3.1 255.255.255.0

ip pim sparse-mode

ip access-list standard ROUTEHUB-ACL-MCAST

permit 239.0.0.0 0.255.255.255

ip pim rp-address 1.0.0.1 ROUTEHUB-ACL-MCAST override

ip msdp peer 1.1.1.1 connect-source Loopback0

ip msdp description 1.1.1.1 routehub-csr01

ip msdp cache-sa-state

ip msdp originator-id Loopback0

ip msdp ttl-threshold 10.1.2.1 32

access-list 100 permit ip 239.0.0.0 0.255.255.255 host 1.1.1.1

ip msdp sa-filter out 1.1.1.1 list 100

>> OTHER ROUTERS & L3 SWITCHES <<

```
hostname WAN-ROUTER
```

```
ip multicast-routing
```

```
interface loopback 0
description "network-mgmt"
ip address 3.3.3.3 255.255.255.255
no ip redirects
no ip unreachable
no ip proxy-arp
ip pim sparse-mode
```

```
interface GigabitEthernet3/1
description CORE2
ip address 10.1.3.3 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
ip pim sparse-mode
```

```
interface Serial0/0.1 point-to-point
description WAN CLOUD
ip address 10.250.3.1 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
ip pim sparse-mode
```

```
ip access-list standard ROUTEHUB-ACL-MCAST
permit 239.0.0.0 0.255.255.255
```

```
ip pim rp-address 1.0.0.1 ROUTEHUB-ACL-MCAST override
```


[N]

NAM

Solution/Services: Cisco Catalyst 6500 Series
Related:

- NAM service module in slot 7
- NAM will use VLAN 99 for managing the service module
- NAM module will capture traffic for VLANs 10-11,100-102

analysis module 7 management-port access-vlan 99

analysis module 7 data-port 1 capture allowed-vlan 10,100

analysis module 7 data-port 2 capture allowed-vlan 11,101-102

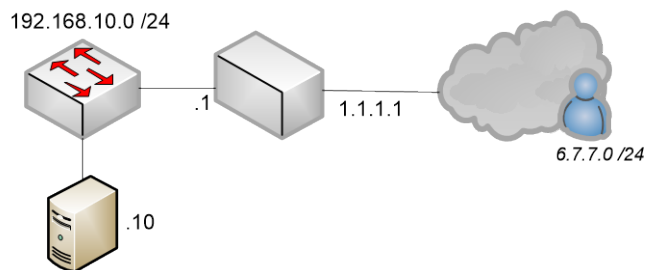
NAT

Solution/Services: Feature

Related: N/A

NAT Overload using Pool of IP Addresses

- Configure NAT Overload for all inside addresses on the 192.168.10.0 network to use one of the outside IP's in the defined pool (1.1.1.5 – 1.1.1.6) for accessing the Internet.



```
access-list 101 permit ip 192.168.10.0 0.0.0.255 any
```

```
ip nat pool NATPOOL 1.1.1.5 1.1.1.6 netmask 255.255.255.0  
ip nat inside source list 101 pool NATPOOL overload
```

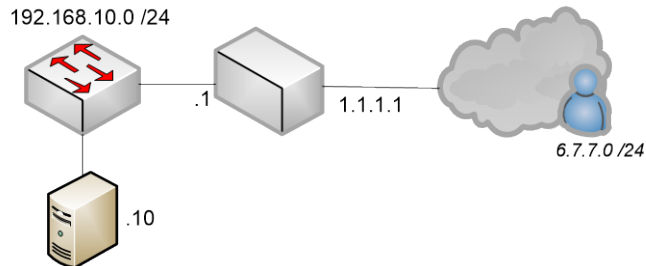
```
interface GigabitEthernet0/0  
ip address 1.1.1.1 255.255.255.0  
ip nat outside
```

```
interface GigabitEthernet0/1  
ip address 192.168.10.1 255.255.255.0  
ip nat inside
```

```
show ip nat translations
```

NAT Overload using WAN interface

- Configure NAT Overload for all inside addresses on the 192.168.10.0 network to use the IP address on the WAN facing interface of the Cisco router (1.1.1.1) for accessing the Internet.



```
access-list 101 permit ip 192.168.10.0 0.0.0.255 any
```

```
ip nat inside source list 101 interface GigabitEthernet0/0 overload
```

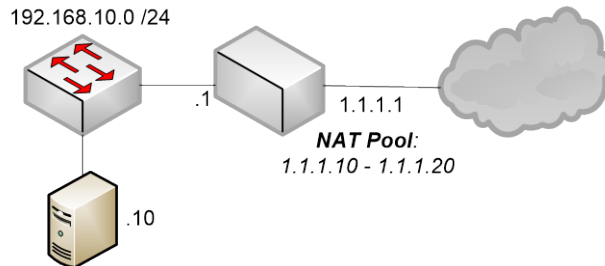
```
interface GigabitEthernet0/0  
ip address 1.1.1.1 255.255.255.0  
ip nat outside
```

```
interface GigabitEthernet0/1  
ip address 192.168.10.1 255.255.255.0  
ip nat inside
```

```
show ip nat translations
```

Dynamic NAT Pool

- Define range of dedicated IP's (1.1.1.10 - .20) to assign to inside IP addresses on the inside network (192.168.10.0) when accessing the Internet

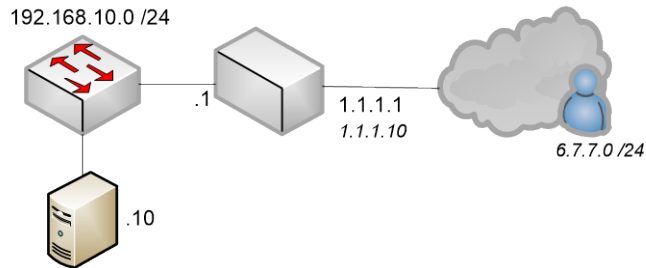


```
ip access-list extended RHG-ACL-NET  
permit ip 192.168.10.0 0.0.0.255 any
```

```
ip nat pool RHG-NAT-POOL 1.1.1.10 1.1.1.20 netmask 255.255.255.0  
ip nat inside source list RHG-ACL-NET pool RHG-NAT-POOL
```

Static NAT

- Configure a static NAT translation between 192.168.10.10 (inside) and 1.1.1.10 (outside)



```
ip nat inside source static 192.168.10.10 1.1.1.10
```

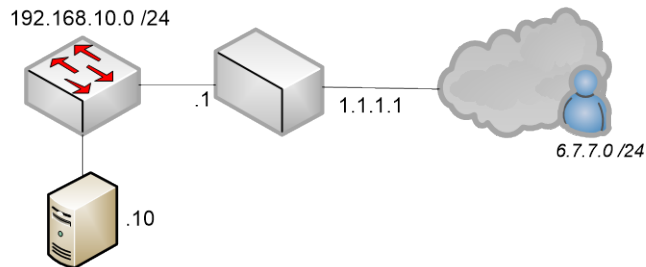
```
interface GigabitEthernet0/0  
ip address 1.1.1.1 255.255.255.0  
ip nat outside
```

```
interface GigabitEthernet0/1  
ip address 192.168.10.1 255.255.255.0  
ip nat inside
```

```
show ip nat translations
```

NAT Port Redirect using WAN interface

- Any access to the IP address configured on the WAN interface (1.1.1.1) for HTTPS (TCP/443) will be redirected to the inside server of 192.168.10.10



```
ip nat inside source static tcp 192.168.10.10 443 1.1.1.1 443 extendable
```

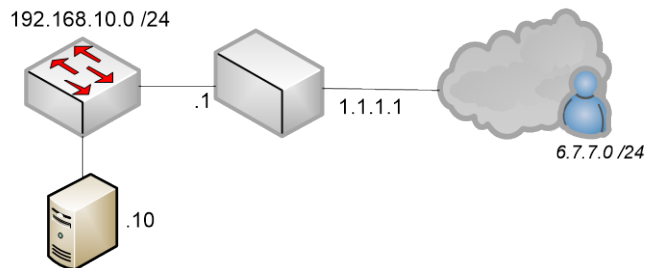
```
interface GigabitEthernet0/0  
ip address 1.1.1.1 255.255.255.0  
ip nat outside
```

```
interface GigabitEthernet0/1  
ip address 192.168.10.1 255.255.255.0  
ip nat inside
```

```
show ip nat translations
```

NAT Port Redirect using Dedicated IP

- Any access to the dedicated IP address of 1.1.1.10 for HTTPS (TCP/443) will be redirected to the inside server of 192.168.10.10



```
ip nat inside source static tcp 192.168.10.10 443 1.1.1.10 443 extendable
```

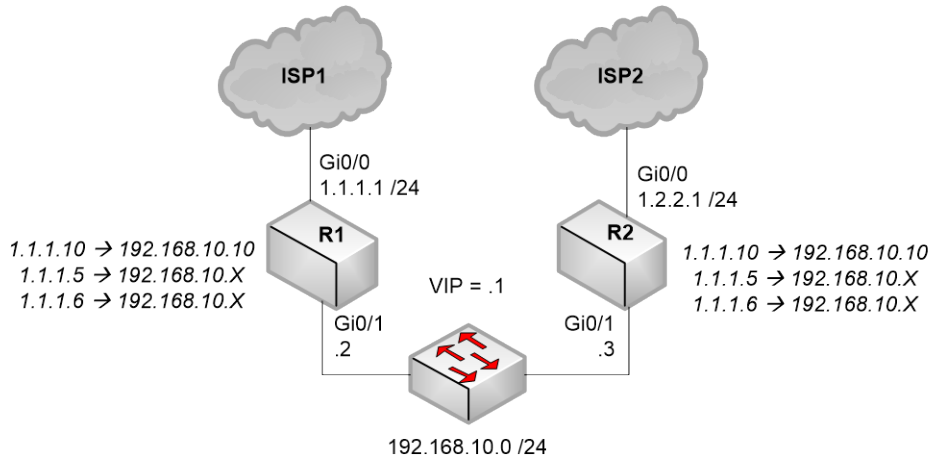
```
interface GigabitEthernet0/0  
ip address 1.1.1.1 255.255.255.0  
ip nat outside
```

```
interface GigabitEthernet0/1  
ip address 192.168.10.1 255.255.255.0  
ip nat inside
```

```
show ip nat translations
```

Stateful Failover

- No NAT Overload (PAT) support
- Configure NAT stateful failover between R1 and R2 using HSRP
- R1 will be the primary router and R2 will be the secondary router
- Stateful NAT group name will be "SF-NAT"



>>R1<<

```
ip nat stateful id 1
redundancy SF-NAT
mapping-id 1
interface GigabitEthernet0/1
protocol udp
```

```
ip nat pool NATPOOL 1.1.1.5 1.1.1.6 netmask 255.255.255.0
```

```
access-list 110 permit ip 192.168.10.0 0.0.0.255 any
ip nat inside source list 110 pool NATPOOL mapping-id 1
ip nat inside source static 192.168.10.10 1.1.1.10 mapping-id 1
```

```
interface GigabitEthernet0/0
ip address 1.1.1.1 255.255.255.0
ip nat outside
```

```
interface GigabitEthernet0/1
ip address 192.168.10.2 255.255.255.0
ip nat inside
standby ip 192.168.10.1
standby timers msec 250 msec 750
standby priority 110
standby preempt delay minimum 180
standby name SF-NAT
```



```
>>R2<<
```

```
ip nat stateful id 1  
  redundancy SF-NAT  
  mapping-id 1  
interface GigabitEthernet0/1  
  protocol udp
```

```
ip nat pool NATPOOL 1.1.1.5 1.1.1.6 netmask 255.255.255.0
```

```
access-list 110 permit ip 192.168.10.0 0.0.0.255 any  
ip nat inside source list 110 pool NATPOOL mapping-id  
ip nat inside source static 192.168.10.10 1.1.1.10 mapping-id 1
```

```
interface GigabitEthernet0/0  
  ip address 1.2.2.1 255.255.255.0  
  ip nat outside
```

```
interface GigabitEthernet0/1  
  ip address 192.168.10.3 255.255.255.0  
  ip nat inside  
  standby ip 192.168.10.1  
  standby timers msec 250 msec 750  
  standby preempt delay minimum 180  
  standby name SF-NAT
```

NAT Monitoring Commands

```
show ip nat translations  
show ip nat statistics
```

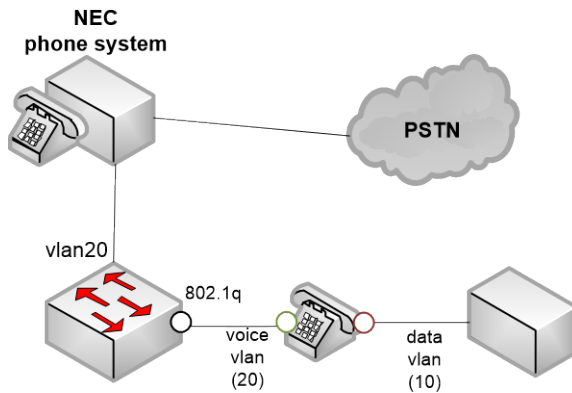
NEC (VOICE) SOLUTIONS

Solution/Services: NEC Solutions

Related: N/A

Voice Switch port using NEC Phone System

- Data VLAN: 10
- Voice VLAN 20



```
interface GigabitEthernet5/14
description DTOP and IPPHONE PORT
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20
switchport mode trunk
spanning-tree portfast
spanning-tree bpduguard enable
```

NETFLOW

Solution/Services: Management

Related:

Netflow on Cisco IOS

- Recommended Netflow applied on Cisco IOS Routers
- Set Netflow version to 5. Source Netflow communication from Loopback0 interface
- Send Netflow data to Netflow server 192.168.10.10 using port 9996

```
ip flow-export destination 192.168.10.10 9996
```

```
ip flow-export source Loopback0
```

```
ip flow-export version 5
```

```
ip flow-cache timeout active 1
```

```
ip flow-cache timeout inactive 15
```

```
interface FastEthernet0/0
```

```
ip route-cache flow
```

```
show ip flow export
```

```
show ip cache flow
```

```
show ip cache verbose flow
```

Netflow on Cisco Catalyst 6500 (Native OS)

- Recommended Netflow applied on Cisco Catalyst 6500 using Supervisor 720 ; IOS version 12.1.13(E) or higher
- Set Netflow version to 7 (if supported on Netflow server). Source Netflow communication from Loopback0 interface
- Send Netflow data to Netflow server 192.168.10.10 using port 9996

```
mls nde sender version 7
mls aging long 64
mls aging normal 32
mls flow ip full
ip flow-export destination 192.168.10.10 9996
ip flow-export source Loopback0
```

```
interface FastEthernet3/1
ip route-cache flow
```

```
show ip flow export
show ip cache flow
show ip cache verbose flow
```

Netflow on Cisco Catalyst 4500

- Recommended Netflow applied on Cisco Catalyst 4500 using Supervisor IV, Netflow daughter-card ; IOS version 12.1.1(EW) or higher
- Set Netflow version to 5. Source Netflow communication from Loopback0 interface
- Send Netflow data to Netflow server 192.168.10.10 using port 9996

```
ip flow-export destination 192.168.10.10 9996
ip flow-export source Loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
```

```
interface FastEthernet3/1
ip route-cache flow infer-fields
```

```
show ip flow export
show ip cache flow
show ip cache verbose flow
```

Top Talkers on Cisco IOS

- Enable top-talkers details on Netflow enabled interfaces
- Only show the top 5 traffic talkers based on Bytes used per top talker

```
ip flow-top-talkers
top 5
sort-by bytes
```

```
show ip flow top-talkers
```

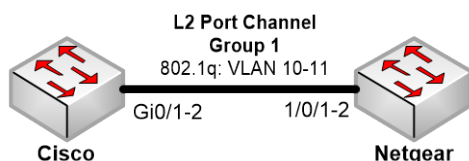
NETGEAR SOLUTIONS

Solution/Services: Netgear

Related: Port Channel, Trunking (802.1Q)

L2 Port Channel between Cisco and Netgear

- Configure Layer 2 LACP Port Channel (using Group #1) between Cisco Switch and Netgear Switch
- Netgear calls a Port Channel a Link Aggregation (LAG)
- Configure 802.1Q Trunk between the Cisco and Netgear Switch
- Configure Trunk Security to allow VLANs 10 and 11



>> CISCO SWITCH <<

```
interface Port-channel1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,10-11
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk
```

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,10-11
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk
channel-protocol lacp
channel-group 1 mode passive
```

```
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,10-11
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk
channel-protocol lacp
channel-group 1 mode passive
```

>> NETGEAR SWITCH <<

```
vlan database
```

```
vlan 10
```

```
vlan 11
```

```
port-channel Stack 1
```

```
interface 1/0/1
```

```
addport 0/1/1
```

```
interface 1/0/2
```

```
addport 0/1/1
```

```
exit
```

```
interface lag 1
```

```
description 'Stack 1'
```

```
vlan participation include 10
```

```
vlan tagging 10
```

```
vlan participation include 11
```

```
vlan tagging 11
```

```
exit
```

```
interface 1/0/1
```

```
vlan participation include 10
```

```
vlan tagging 10
```

```
vlan participation include 11
```

```
vlan tagging 11
```

```
exit
```

```
interface 1/0/2
```

```
vlan participation include 10
```

```
vlan tagging 10
```

```
vlan participation include 11
```

```
vlan tagging 11
```

```
exit
```

NTP

Solution/Services: Administration/System
Related:

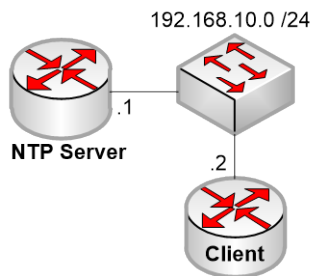
NTP Server (using Local Clock)

- Confirm that the local time is correct on Cisco device.
- Define NTP stratum level to be 3 on NTP server
- Source all NTP communication from interface BVI 10

```
ntp source BVI10  
ntp master 3
```

NTP Client

- Configure Cisco router "CLIENT" to point to the NTP server (192.168.10.1) on the LAN for time services



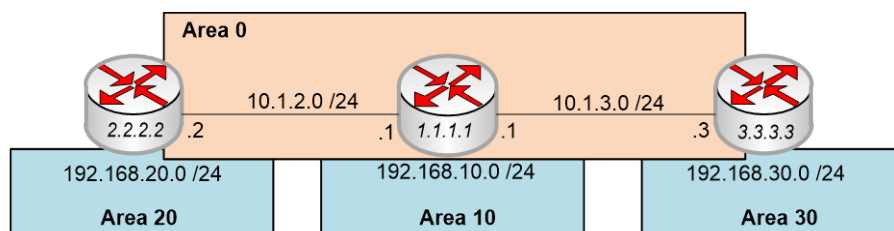
```
access-list 10 permit 192.168.10.1  
  
ntp source Vlan10  
ntp access-group peer 10  
ntp server 192.168.10.1 prefer
```


[O]

OSPF

Solution/Services: IP Routing (IGP)

Related: N/A



OSPF Routing

- Enables OSPF routing process using PID of "1"
- Specifies the router ID IP address to use
- Specify what routes to advertise and build neighbors with other OSPF routers

```
>>R1 (1.1.1.1)<<
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 10
network 10.1.2.0 0.0.0.255 area 0
network 10.1.3.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 10
```

Router ID

- Specifies the IP Address to use for the OSPF neighbor ID

```
>>R1<<
router ospf 1
router-id 1.1.1.1
```

Default Routing

- Configure R1 to advertise an OSPF default route to all OSPF neighbors

```
>>R1<<
router ospf 1
default-information originate always

show ip ospf database external
```

OSPF Network: Point-to-Point

- Enables OSPF network type to be point-to-point

```
>>R1<<
interface FastEthernet0/1
ip ospf network point-to-point
```

Passive Interfaces

- Disables OSPF routing for all interfaces on R1 except for FE0/1 and FE0/2

>>R1<<

```
router ospf 1
passive-interface default
no passive-interface FastEthernet0/1
no passive-interface FastEthernet0/2
```

MD5 Authentication

- Enables MD5 authentication with other OSPF routers
- Specify the MD5 password

>>R1<<

```
interface FastEthernet0/1
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco123

router ospf 1
area 10 authentication message-digest
```

SFP and LSA Timers

- Recommended/Best Practice values for tuning LSA and SFP timers

>>R1<<

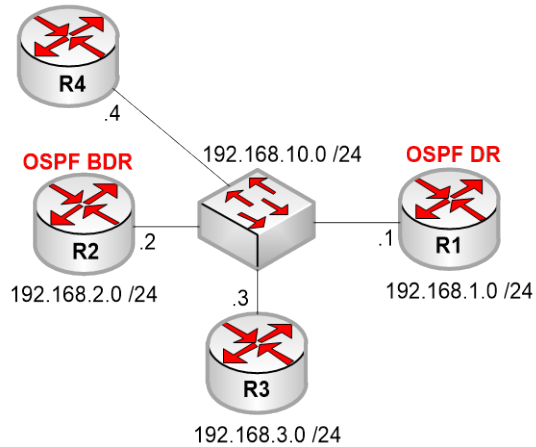
```
router ospf 1
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
```

show ip ospf

DR and BDR Selection

- Default OSPF priority is 1
- Higher preferred (the DR)
- R1 would be DR (higher priority), R2 would be the BDR (next highest priority), and R4 would never participate in the DR/BDR election (priority = 0)

Never a DR or BDR



```
>> R1 <<
interface fastethernet0/1
ip ospf priority 10
```

```
>> R2 <<
interface fastethernet0/1
ip ospf priority 5
```

```
>> R3 <<
interface fastethernet0/1
ip ospf priority 2
```

```
>> R4 <<
interface fastethernet0/1
ip ospf priority 0
```

Neighbor Timers

- Configures sub-second timers with neighbors for fast convergence

>>R1<<

interface FastEthernet0/1

ip ospf dead-interval minimal hello-multiplier 4

OR

- Specify the interval to send OSPF hello packets
- Specify the interval to wait to declare an OSPF neighbor dead if it doesn't receive a hello message

interface FastEthernet0/1

ip ospf hello-interval 2

ip ospf dead-interval 6

Changing Admin Distance

- Specify custom admin distance (internal and external routes)

router ospf 1

distance ospf intra-area 100

distance ospf inter-area 101

distance ospf external 102

Maximum Paths Per Route

- Define the number of paths for a single route to injected into the routing table

router ospf 1

maximum-paths 2

Auto Cost Reference

- Default "auto cost" is 100 (or 100Mbps)
- Change the bandwidth reference to 1000. Therefore 1000/BW will be used to determine the OSPF cost for an interface

```
router ospf 1  
auto-cost reference-bandwidth 1000
```

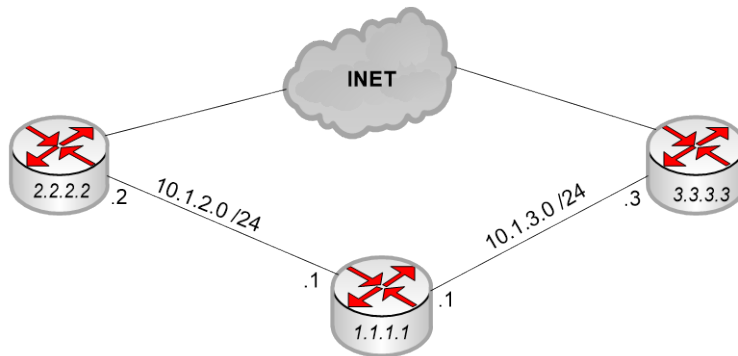
Reduce OSPF Flooding

- Reduce OSPF flooding

```
interface fastethernet0/1  
ip ospf flood-reduction
```

OSPF Cost

- *Cost: lower the value, more preferred*
- On R1's FE0/1 configure cost on interface towards uplink to be more preferred ; no ECP
- On R1's FE0/2 configure cost on interface towards uplink to be less preferred ; no ECP

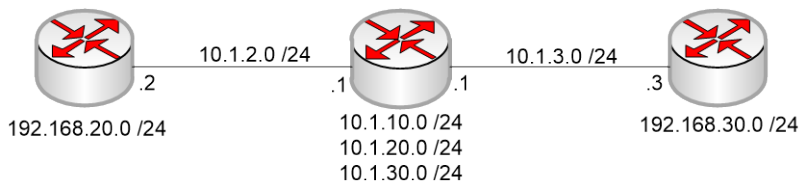


```
>>R1 (1.1.1.1)<<
interface FastEthernet0/1
ip address 10.1.2.1 255.255.255.0
ip ospf cost 10

interface FastEthernet0/2
ip address 10.1.3.1 255.255.255.0
ip ospf cost 100
```

Internal Route Summarization

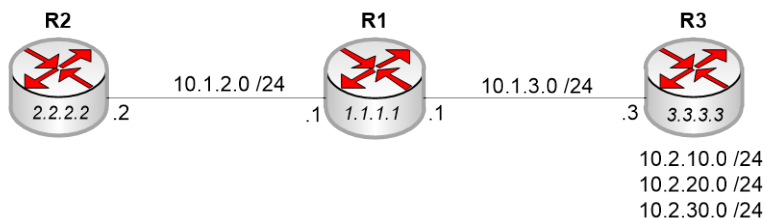
- Applies to OSPF routes (O, O IA)
- Configured on OSPF ABRs
- Summarizes all subnets 10.1.x.x (Area 10) to 10.1.0.0/16 on R1
- Advertises the cost with the summary route to provide Equal Cost Path (ECP) to the network where redundant paths exist.



```
>>R1<<
router ospf 1
area 10 range 10.1.0.0 255.255.0.0 cost 10
```

External Route Summarization

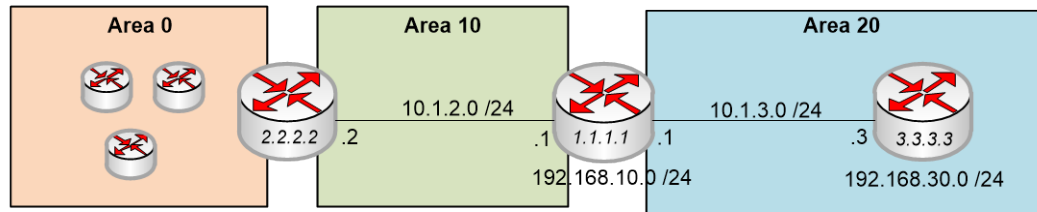
- Applies to OSPF routes (O E1, O E2)
- Configured on OSPF ASBRs
- Summarizes all subnets 10.2.x.x to 10.2.0.0/16 on R3
- Advertises the cost with the summary route to provide Equal Cost Path (ECP) to the network where redundant paths exist.



```
>>R1<<
>> R3 <<
router ospf 1
summary-address 10.2.0.0 255.255.0.0
```


Virtual Link

- R1: Specify the OSPF router whose area is not directly connected to the OSPF backbone area.
- R3: Specify the OSPF router whose area is directly connected to the OSPF backbone area



>> R1 <<

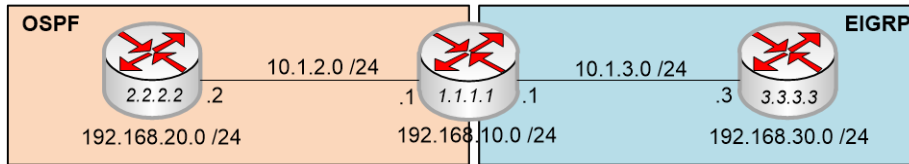
```
router ospf 1
area 20 virtual-link 3.3.3.3
network 192.168.10.0 0.0.0.255 area 10
network 10.1.3.0 0.0.0.255 area 20
network 1.1.1.1 0.0.0.0 area 10
```

>> R3 <<

```
router ospf 2
area 20 virtual-link 1.1.1.1
network 192.168.30.0 0.0.0.255 area 20
network 10.1.3.0 0.0.0.255 area 20
network 3.3.3.3 0.0.0.0 area 20
```

Route Redistribution

- Redistribute EIGRP routes that are listed in the ACL and Policy Map into OSPF



```
>>R1 (1.1.1.1)<<
ip access-list standard ACL-EIGRP-ROUTES
permit 192.168.30.0 0.0.0.255

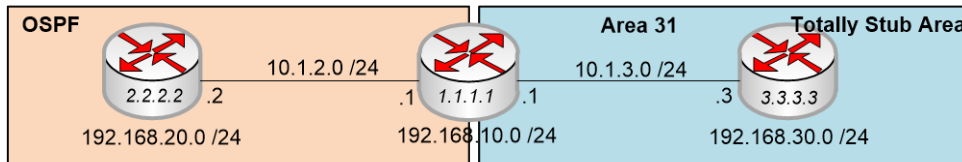
route-map RM-EIGRP-ROUTES permit 10
match ip address ACL-EIGRP-ROUTES

router eigrp 1
network 10.1.3.0 0.0.0.255
network 192.168.10.0

router ospf 1
network 192.168.10.0 0.0.0.255 area 10
network 1.1.1.1 0.0.0.0 area 10
network 10.1.2.0 0.0.0.255 area 0
redistribute eigrp 1 subnets route-map RM-EIGRP-ROUTES
```

OSPF Stub: Totally Stub

- Configures Area 31 as a Totally Stub Area
- R1 (1.1.1.1) would only advertise a OSPF default route to R3 (3.3.3.3)



>>R1<<

```
router ospf 1
network 10.1.2.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 10
network 10.1.3.0 0.0.0.255 area 31
area 31 stub no-summary
```

>>R3<<

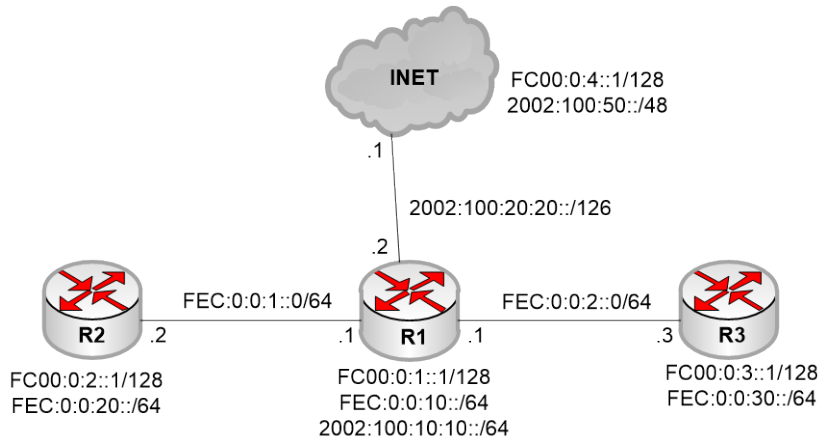
```
router ospf 3
network 192.168.30.0 0.0.0.255 area 31
network 10.1.3.0 0.0.0.255 area 31
area 31 stub no-summary
```

Monitoring Commands for OSPFv2

```
show ip ospf
show ip route ospf
show ip ospf neighbor
show ip ospf interface
show ip ospf database
```

OSPFv3 (IPv6)

- Configure network (see diagram) for OSPFv3 (IPv6) focusing on R1
- Segments connecting to R2 and R3 placed into Area 0
- Networks under Loopback interface placed into Area 1
- Configuration also includes tuned OSPF timers to provide fast convergence
- Passive interface applied to all interfaces except for GE0/1 and GE0/2



>> R1 <<

```
ipv6 unicast-routing
ipv6 cef
```

```
interface Loopback0
```

```
  ipv6 address FC00:0:1::1/128
  ipv6 address FEC0:0:0:10::1/64
  ipv6 address 2002:100:10:10::1/64
  ipv6 enable
  ipv6 ospf 1 area 1
```

```
interface GigabitEthernet0/1
```

```
  description TO: R2
  ipv6 address FEC0:0:0:1::1/64
  ipv6 enable
  ipv6 ospf hello-interval 1
  ipv6 ospf dead-interval 3
  ipv6 ospf 1 area 0
```

```
interface GigabitEthernet0/2
```

```
  description TO: R3
  ipv6 address FEC0:0:0:2::1/64
  ipv6 enable
  ipv6 ospf hello-interval 1
  ipv6 ospf dead-interval 3
  ipv6 ospf 1 area 0
```

```
ipv6 router ospf 1
log-adjacency-changes
default-information originate always
passive-interface default
no passive-interface GigabitEthernet0/1
no passive-interface GigabitEthernet0/2
```

[P]

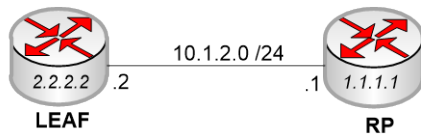
PIM

Solution/Services: Multicast: Multicast Routing

Related: Multicast RP

PIM Sparse Mode

- Configure PIM Sparse Mode
- RP router will be R2 (1.1.1.1)



>> RP ROUTER <<

```
ip multicast-routing
```

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
ip pim sparse-mode
```

```
interface GigabitEthernet0/1
no switchport
ip address 10.1.2.1 255.255.255.0
ip pim sparse-mode
```

```
ip pim rp-address 1.1.1.1
```

>> LEAF ROUTER (R2) <<

ip multicast-routing

interface Loopback0

ip address 2.2.2.2 255.255.255.255

ip pim sparse-mode

interface GigabitEthernet0/2

no switchport

ip address 10.1.2.2 255.255.255.0

ip pim sparse-mode

ip pim rp-address 1.1.1.1

SPT Threshold Infinity

- Reduces Multicast state (S,G) from Leaf routers by keeping traffic on the shared tree

ip pim spt-threshold infinity

PIM Query Interval

- Configure frequency of PIM Router Query message interval to recommended value of 1 minute (60 seconds)

interface Fastethernt0/0

ip pim query-interval 60

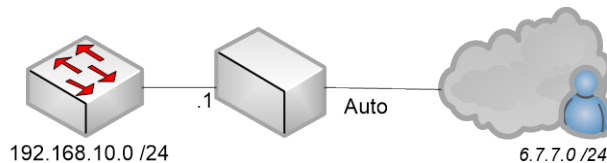
PPPOE

Solution/Services: WAN

Related: N/A

PPPoE on Cisco IOS (Ethernet)

- Enable PPPoE on Ethernet WAN facing interface
- PPP username will be "user1" and password will be "Cisco123"
- Enable CHAP and PAP authentication for PPP



Interface FastEthernet4

Description TO: WAN

no ip address

pppoe enable

pppoe-client dial-pool-number 1

interface Vlan10

description TO: LAN

ip address 192.168.10.1 255.255.255.0

ip nat inside

interface Dialer1

ip address negotiated

ip mtu 1492

ip nat outside

encapsulation ppp

dialer pool 1

ppp authentication chap pap callin

ppp pap sent-username user1 password cisco123

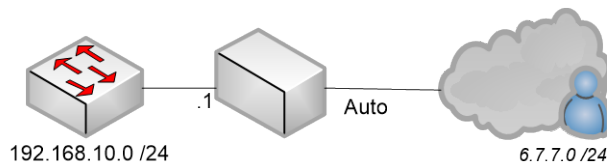
ppp chap hostname user1

ppp chap password cisco123

ip route 0.0.0.0 0.0.0.0 dialer 1

PPPoE on Cisco IOS (ATM) I

- Enable PPPoE on ATM WAN facing interface
- ATM PVC (8/35)
- PPP username will be "user1" and password will be "Cisco123"
- Enable CHAP and PAP authentication for PPP



```
interface ATM 0
description TO: WAN
no ip address
dsl operating-mode auto
pvc 8/35
no shutdown
pppoe-client dial-pool-number 1
```

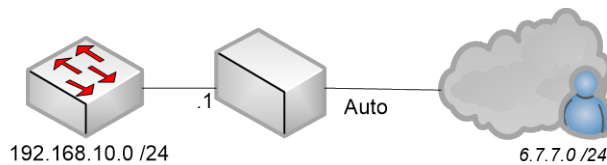
```
interface Vlan10
description TO: LAN
ip address 192.168.10.1 255.255.255.0
ip nat inside
```

```
interface Dialer1
ip address negotiated
ip mtu 1492
ip nat outside
encapsulation ppp
dialer pool 1
ppp authentication chap pap callin
ppp pap sent-username user1 password cisco123
ppp chap hostname user1
ppp chap password cisco123

ip route 0.0.0.0 0.0.0.0 dialer 1
```

PPPoE on Cisco IOS (for ADSL)

- Enable PPPoE on ADSL interface connecting to ISP.
- Configured on a Cisco 877 ADSL router
- ATM PVC details (VPI=0, VC=38)
- PPP username will be "user1" and password will be "Cisco123"
- Enable CHAP authentication for PPP



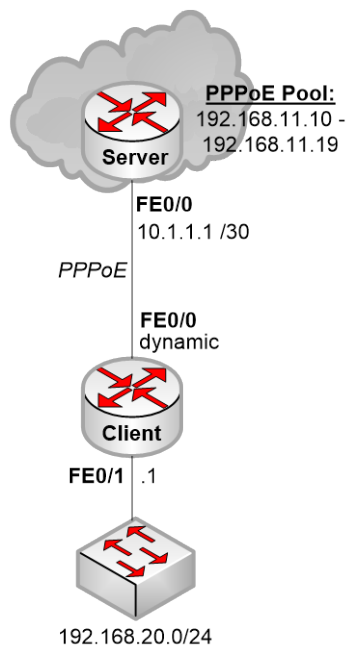
```
dialer-list 1 protocol ip permit
```

```
interface ATM0/2/0
no ip address
no ip mroute-cache
no atm ilmi-keepalive
dsl operating-mode auto
pvc 0/38
encapsulation aal5mux ppp dialer
dialer pool-member 1
```

```
interface Dialer1
ip address negotiated
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap callin
ppp chap hostname user1
ppp chap password cisco123
```

```
ip route 0.0.0.0 0.0.0.0 dialer 1
```

PPPoE Server and Client Cisco IOS



- PPPoE server configuration on Cisco IOS router
- Address pool for PPPoE authenticated users: 192.168.11.10 - 19
- Configure PPPoE user account: michel / cisco
- Enable PAP authentication

```
hostname pppoe-server
```

```
ip local pool pppoe-pool 192.168.11.10 192.168.11.19
```

```
username michel password cisco
```

```
vpdn enable  
no vpdn logging
```

```
vpdn-group 1  
accept-dialin  
protocol pppoe  
virtual-template 1
```

```
interface FastEthernet0/0  
description "Connected to PPPoE enabled devices"  
ip address 10.1.1.1 255.255.255.252  
pppoe enable  
no ip mroute-cache  
no shutdown
```

```
interface virtual-template 1
ip unnumbered ethernet0/0
mtu 1492
peer default ip address pool pppoe-pool
ppp authentication pap
```

```
ip classless
no ip http server
```

```
ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

- PPPoE client configuration on Cisco IOS router
- Specify PPPoE user account to use for authentication (michel / cisco)
- Enable PAP authentication
- Configure NAT Overload (PAT) from then LAN using the IP assigned to the WAN interface (FE0/0)

```
hostname pppoe-client
```

```
vpdn enable
no vpdn logging
```

```
vpdn-group 1
request-dialin
protocol pppoe
```

```
interface FastEthernet0/1
description TO: LAN
ip address 192.168.20.1 255.255.255.0
ip nat inside
```

```
access-list 1 permit 192.168.20.0 0.0.0.255
dialer-list 1 protocol ip permit
```

```
interface Dialer1
ip address negotiated
ip nat outside
ip mtu 1492
encapsulation ppp
no ip mroute-cache
dialer pool 1
dialer-group 1
ppp authentication pap callin
ppp pap sent-username michel password cisco
```

```
interface FastEthernet0/0
description TO: WAN
no ip address
pppoe enable
pppoe-client dial-pool-number 1
```

```
ip classless
no ip http server
```

```
ip nat inside source list 1 interface Dialer1 overload
```

```
ip route 0.0.0.0 0.0.0.0 dialer1
```

- Monitoring commands

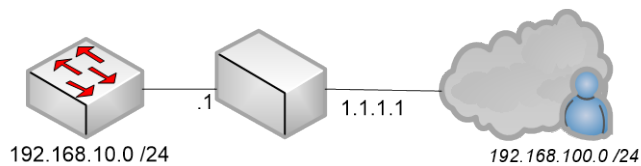
```
show vpdn
show ip interface brief
show ip address outside pppoe
show vpdn tunnel pppoe
show vpdn session pppoe
show vpdn pppinterface
show vpdn group
show vpdn username
```

PPTP

Solution/Services: Security: VPDN

Related: N/A

PPTP using Local Authentication



- Configure Client VPN solution using PPTP
- PPTP will support MS-CHAP PPP authentication
- The VPN pool for connected users will be 192.168.100.60 – 192.168.100.69
- LAN subnet behind the VPN device is: 192.168.10.0/24
- VPN user authentication will be using RADIUS server (192.168.10.11). RADIUS shared key will be cisco123

```
username user1 password cisco123
```

```
vpdn enable
```

```
vpdn logging
```

```
ip local pool PPTP-POOL 192.168.100.60 192.168.100.69
```

```
interface FastEthernet0
```

```
ip address 1.1.1.1 255.255.255.0
```

```
ip nat outside
```

```
interface Virtual-Template1
```

```
ip unnumbered FastEthernet0
```

```
peer default ip address pool PPTP-POOL
```

```
ppp encrypt mppe 128
```

```
ppp authentication ms-chap-v2
```

```
vpdn-group 1
```

```
accept-dialin
```

```
protocol pptp
```

```
virtual-template 1
```

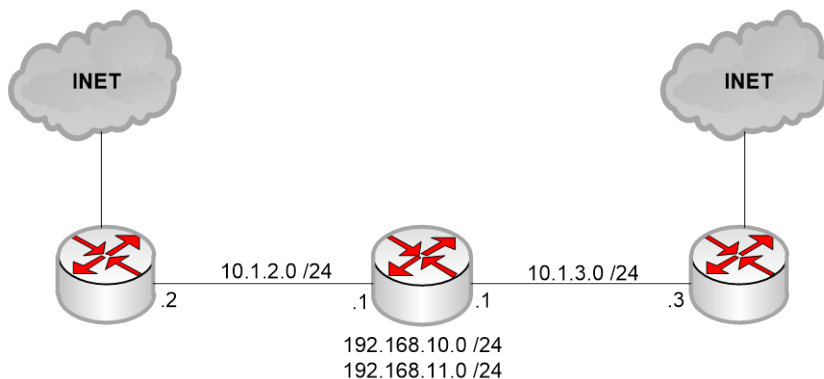
POLICY BASED ROUTING (PBR)

Solution/Services: Feature

Related: N/A

Policy Based Routing (PBR)

- Configure a policy route where any HTTP, HTTPS, traffic to 4.2.2.3, and traffic to 192.168.20.10 will be routed to the 10.1.3.3 router.
- Traffic to 192.168.11.0 for HTTP services or traffic from 192.168.10.11 will not use the policy routed defined.
- All other unmatched internet traffic will be routed to the 10.1.2.2 router.



```
ip access-list extended PBR-ACL-INET
deny tcp any 192.168.11.0 0.0.0.255 eq www
deny ip host 192.168.10.11 any
permit tcp any any eq www
permit tcp any any eq 443
permit ip any host 4.2.2.3
permit ip any host 192.168.20.10
```

```
route-map PBR-RM-INET permit 10
match ip address PBR-ACL-INET
set ip next-hop 10.1.3.3
```

```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
ip policy route-map PBR-RM-INET
```

```
ip route 0.0.0.0 0.0.0.0 10.1.2.2
```

```
show ip policy
show route-map
```

PORT CHANNEL

Solution/Services: LAN Switching

Related: N/A

Hash Algorithm: Source and Destination IP

- Configures the Port Channel hash algorithm based on Source and Destination IP Addresses

```
port-channel load-balance src-dst-ip
```

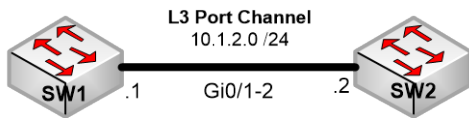
Hash Algorithm: Source and Destination IP Plus Port

- Configures the Port Channel hash algorithm based on Source and Destination IP Addresses plus TCP/UDP ports

```
port-channel load-balance src-dst-port
```


L3 Port Channel between two Cisco Switches (using LACP)

- Configure L3 Port Channel between two Cisco Switches
- Port Channel protocol is LACP
- Port Channel group will be "1"
- Interfaces GE0/1 & GE0/2 will be added to Port Channel group between the switches



>>SW1<<

```
interface Port-Channel1
no switchport
ip address 10.1.2.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
```

```
interface GigabitEthernet0/1
no switchport
no ip address
channel-protocol lacp
channel-group 1 mode active
```

```
interface GigabitEthernet0/2
no switchport
no ip address
channel-protocol lacp
channel-group 1 mode active
```

>>SW2<<

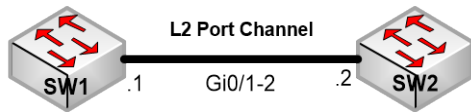
```
interface Port-Channel1
ip address 10.1.2.2 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
```

```
interface GigabitEthernet0/1
no switchport
no ip address
channel-protocol lacp
channel-group 1 mode active
```

```
interface GigabitEthernet0/2
no switchport
no ip address
channel-protocol lacp
channel-group 1 mode active
```

L2 Port Channel between two Cisco Switches (using LACP)

- Configure L2 Port Channel between two Cisco Switches
- Port Channel protocol is LACP
- Port Channel group will be "1"
- Interfaces GE0/1 & GE0/2 will be added to Port Channel group between the switches
- Allow VLAN tags 10,11,50,200, and 250 between SW1 and SW2



>>SW1<<

```
interface Port-Channel1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-11,50,200,250
switchport mode trunk
switchport nonegotiate
```

```
interface range GigabitEthernet0/1 - 2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-11,50,200,250
switchport mode trunk
switchport nonegotiate
channel-protocol lacp
channel-group 1 mode active
```

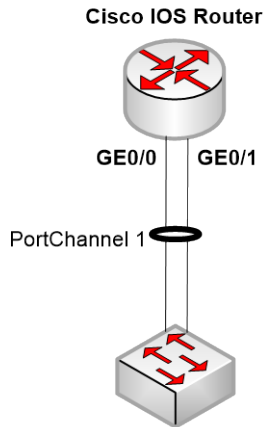
>>SW2<<

```
interface Port-Channel1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-11,50,200,250
switchport mode trunk
switchport nonegotiate
```

```
interface range GigabitEthernet0/1 - 2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-11,50,200,250
switchport mode trunk
switchport nonegotiate
channel-protocol lacp
channel-group 1 mode active
```

Port Channel on Cisco IOS Routers

- Configure Port Channel between a Cisco Switch and a Cisco IOS Router
- Port Channel protocol is PAgP (default)
- Port Channel group will be "1"
- Interfaces GE0/0 & GE0/1 will be added to Port Channel group
- Extend VLANs 10



```
interface Port-channel1  
no ip address  
hold-queue 150 in
```

```
interface Port-channel1.10  
encapsulation dot1Q 10  
ip address 192.168.10.1 255.255.255.0
```

```
interface GigabitEthernet0/0  
no ip address  
duplex auto  
speed auto  
media-type rj45  
channel-group 1
```

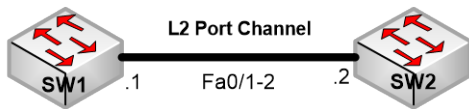
```
interface GigabitEthernet0/0.10  
channel-group 1
```

```
interface GigabitEthernet0/1  
no ip address  
duplex auto  
speed auto  
media-type rj45  
channel-group 1
```

```
interface GigabitEthernet0/1.10
channel-group 1
```

Port Channel on Cisco 2900/3500XL Switches

- Configuration applicable for Cisco Catalyst 2900XL/3500XL switches ; older IOS
- Configure L2 Port Channel between two Cisco Switches
- Port Channel group will be "1"
- Interfaces FA0/1 & FA0/2 will be added to Port Channel group between the switches



```
>>SW1<<
interface fastethernet 0/1
port group 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
interface fastethernet 0/2
port group 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
>>SW2<<
interface fastethernet 0/1
port group 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
interface fastethernet 0/2
port group 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

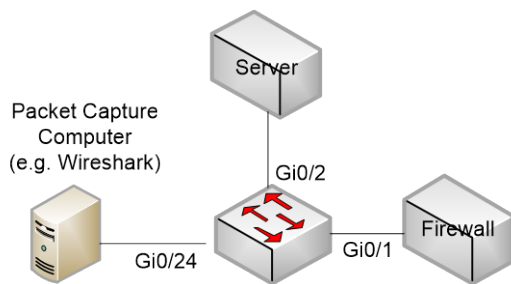
PORT MONITOR

Solution/Services: Administration/System

Related: N/A

Port Monitor

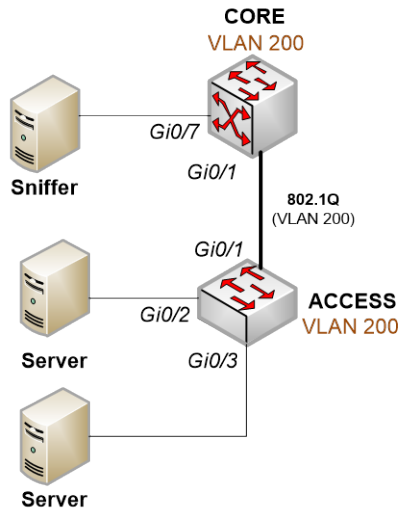
- We want to capture all traffic from the server and firewall on interfaces Gi0/1 and Gi0/2
- Send the captured traffic from those interface(s) to Gi0/24 which has a connected SNIFFER running



monitor session 1 source interface Gi0/1 – 2
monitor session 1 destination interface Gi0/24

RSPAN

- RSPAN allows capturing traffic from ports connected on another switch.
- RSPAN VLAN will be 200
- We want to capture all traffic from all Server switch ports (Gi0/2, Gi0/3) on the Access Switch which is placed into VLAN200
- Send the captured traffic from those interface(s) to Gi0/7 on the Core switch which has a connected SNIFFER running



>>AS01TRA<< Source

vlan 200

remote span

interface GigabitEthernet 0/1

description TO: CS01TRA

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 200

switchport mode trunk

monitor session 1 source interface gigabitethernet0/2

monitor session 1 source interface gigabitethernet0/3

monitor session 1 destination remote vlan 200

>>CS01TRA<< *Destination*

vlan 200
remote span

interface GigabitEthernet 0/1
description TO: AS01TRA
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 200
switchport mode trunk

monitor session 1 source remote vlan 200
monitor session 1 destination interface gigabitethernet0/7

PORT SECURITY

Solution/Services: LAN Switching, Security

Related: N/A

Port Security using Maximum Value

- Enable interface for Port Security and restrict no more than 5 connected devices

```
interface GigabitEthernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security maximum 5
switchport port-security aging time 20
```

Port Security using Mac Address

- Enable interface for Port Security for only a connected device with the MAC address 0014.1cc1.0e00

```
interface GigabitEthernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address 0014.1cc1.0e00
switchport port-security aging time 20
```


Port Security using Sticky Mac Address

- Enable interface GE0/1 for Port Security using Sticky MAC address method. This means, the first MAC address learned on this interface will be added for port security.

```
interface GigabitEthernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
```

PROTECTED PORTS

Solution/Services: LAN Switching, Security

Related: N/A

```
interface fastethernet 0/X  
switchport mode access  
switchport protected  
switchport block unicast  
switchport block multicast
```

[Q]

QOS: GENERAL

Solution/Services: QoS
Related: N/A

Enabling QoS on L2/L3 Switches

- Enable QoS on L2/L3 switches

mls qos

Monitoring QoS

```
show policy-map interface <interface>
show mls qos input-queue
show mls qos interface <interface> statistics
show mls qos interface <interface> buffers
show mls qos interface <interface> queuing
show mls qos queue-set
show frame-relay fragment
```

QOS: CLASSIFICATION & MARKING

Solution/Services: QoS

Related: N/A

Classification using ACLs

- Classify all HTTP traffic using Extended ACL
- Mark classified traffic using DSCP AF11

```
ip access-list extended RHG-ACL-DATA-BRONZE
permit tcp any any eq www
```

```
class-map match-all RHG-CLASS-DATA-BRONZE
match access-group name RHG-ACL-DATA-BRONZE
```

```
policy-map RHG-POL
class RHG-CLASS-DATA-BRONZE
set ip dscp af11
```

Classification using NBAR

- Classify all Microsoft RDP traffic (TCP/3389) and FTP using NBAR
- Mark classified traffic using DSCP AF21

```
ip nbar port-map custom-01 tcp 3389
```

```
class-map match-any RHG-CLASS-DATA-SILVER
match protocol ftp
match protocol custom-01
```

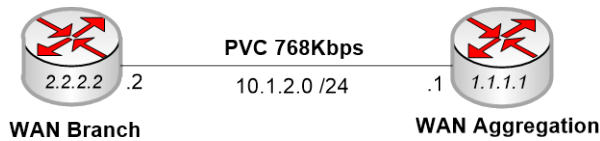
```
policy-map RHG-POL
class RHG-CLASS-DATA-SILVER
set ip dscp af21
```

Classification using DSCP

- Classify any traffic that is marked with DSCP EF

```
class-map match-all RHG-CLASS-VOICE-RTP  
match ip dscp ef
```

QOS: LINK EFFICIENCIES



FRTS and FRF.12

- Configure Frame Relay Traffic Shaping (FRTS) to shape WAN connection to 768kbps for all traffic (Voice, Data) in QoS policy
- Configure Frame Relay Fragmentation based on the PVC speed 768kbps. $(PVC\ Speed/10ms)/8 = 960\ bytes$

```
class-map match-all RHG-CLASS-VOICE-RTP
match ip dscp ef
class-map match-any RHG-CLASS-VOICE-CONTROL
match ip dscp af31
match ip dscp cs3
```

```
policy-map RHG-POLICY
class RHG-CLASS-VOICE-RTP
priority percent 33
class RHG-CLASS-VOICE-CONTROL
bandwidth percent 5
class class-default
bandwidth percent 25
random-detect
```

```
policy-map RHG-POLICY-FRTS
class class-default
shape average 729600 7296 0
service-policy RHG-POLICY
```

```
map-class frame-relay RHG-CLASS-FRTS-768
frame-relay fragment 960
service-policy output RHG-POLICY-FRTS
```

```
interface Serial0/0/0
bandwidth 768
ip address 10.1.2.1 255.255.255.0
encapsulation frame-relay
frame-relay class RHG-CLASS-FRTS-768
frame-relay map ip 10.1.2.2 101 broadcast
```

```
show frame-relay fragment
```

LFI

- Configure LFI on PPP Multilink interface

```
interface Multilink1
ip address 10.1.2.1 255.255.255.0
ppp multilink
ppp multilink interleave
ppp multilink fragment delay 10
ppp multilink group 1
```

```
interface Serial0/0/0
bandwidth 768
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

Compression using cRTP

- *Recommended for slow-speed WAN connections*
- Enable RTP Compression (cRTP) for Voice RTP traffic (DSCP EF)
- QoS policy applied outbound on WAN facing interface

```
class-map match-all RHG-CLASS-VOICE-RTP
match ip dscp ef
```

```
policy-map RHG-POLICY
class RHG-CLASS-VOICE-RTP
compress header ip rtp
```

```
interface Multilink1
ip address 10.1.2.1 255.255.255.0
service-policy output RHG-POLICY
```

Max Reserve Bandwidth

- Change default max-reserve bandwidth percentage from 75% to 100% when using CBWFQ

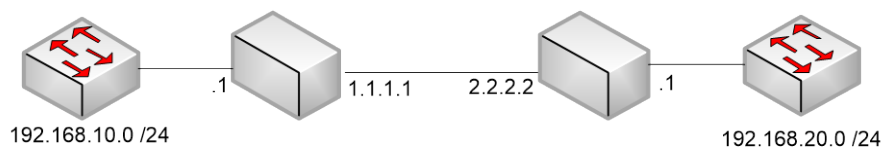
```
class-map match-any RHG-CLASS-VOICE-CONTROL
match ip dscp af31
match ip dscp cs3
```

```
policy-map RHG-POLICY
class RHG-CLASS-VOICE-CONTROL
bandwidth percent 5
```

```
interface Multilink1
ip address 10.1.2.1 255.255.255.0
max-reserved-bandwidth 100
service-policy output RHG-POLICY
```

QoS Pre-Classification on IPSec VPN

- Provide QoS across VPN for Voice.
- The outbound physical interface sees only a single flow and doesn't see the actual flows.
- ACL defines what traffic will be classified for QoS for transit over the VPN tunnel.
- QoS policy will enable LLQ for Voice RTP traffic (defined in ACL 100) for 50kbps. WFQ will be enabled for all other unspecified traffic. QoS policy is applied under the physical interface where the VPN tunnel is terminated from.
- Note: Partial VPN configuration shown using a Tunnel interface.



>> SITE1 (On Left) <<

```
access-list 100 permit udp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 range 16384 20000
access-list 100 permit udp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 range 53000 56000
```

```
class-map voice
match access-group 100
```

```
policy-map qos-policy
class voice
priority 50
class class-default
fair-queue
```



```
interface ethernet0/0
description WAN interface
ip address 1.1.1.1 255.255.255.0
ip service policy output qos-policy

interface Tunnel 0
ip address 10.1.1.1 255.255.255.252
qos pre-classify
tunnel mode ipsec ipv4
tunnel source ethernet0/0
tunnel destination 2.2.2.2
tunnel protection ipsec profile vpn
```

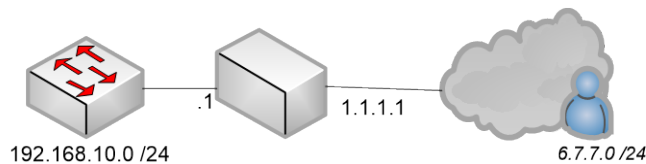
QOS: POLICING

Solution/Services: QoS

Related:

Policing using MQC

- Police (or rate limit) ICMP traffic to 64kbps on the WAN interface.
- Any ICMP traffic that is exceeded should be dropped



```
ip access-list extended RHG-ACL-ICMP
permit icmp any any
```

```
class-map match-any RHG-CLASS-ICMP
match access-group name RHG-ACL-ICMP
```

```
policy-map RHG-POL
class CLASS-ICMP
  police 64000 8000 exceed-action drop
```

```
interface GigabitEthernet1/0/1
ip address 1.1.1.1 255.255.255.0
service-policy input RHG-POL
```

Policing using MQC (Bi-Directional)

- Rate limit an interface/switchport to 500kbps for upload and download speeds

```
policy-map RHG-POL-POLICE
```

```
class class-default
```

```
  police rate 500000
```

```
  conform-action transmit
```

```
  exceed-action drop
```

```
interface FastEthernet0/0
```

```
  service-policy input RHG-POL-POLICE
```

```
  service-policy output RHG-POL-POLICE
```

>>Speakeasy Speed Tests:<<

Download Speed: 488 kbps (61 KB/sec transfer rate) ; input

Upload Speed: 431 kbps (53.9 KB/sec transfer rate) ; output

>> Monitor Command(s):<<

show policy-map interface fastEthernet 0/0

CAR

- Legacy command to use. Recommended to use policing under MQC
- Using CAR, rate limit all ICMP traffic to 2Mbps with some bursting allowed

```
access-list 101 permit icmp any any
```

```
interface POS4/0
```

```
  rate-limit input access-group 101 2000000 512000 786000 conform-action transmit exceed-action drop
```

OC-3 Shaping

- Applied on OC-3 interface with no sub-interfaces configured
- Traffic shape to OC-3 connection speed (155Mbps)

```
policy-map RHG-OC3-TS-POLICY
class class-default
  police cir 149760000 bc 74880 be 74880 conform-action transmit exceed-action drop
```

Control Plane Policing (CoPP)

- Rate limit ICMP control plane traffic to 1.5kbps
- Do not rate limit ICMP traffic to the control plane if source IP is 192.168.10.10
- All other control plane traffic not specified will be rate limited to 1.2Mbps with bursts up to ~4KB
- Apply policy to Control Plane interface

```
ip access-list extended coppacl-mon
remark ICMP rate limiting on control-plane
deny icmp host 192.168.10.10 any
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit icmp any any echo-reply
permit icmp any any echo
```

```
class-map match-all coppclass-mon
match access-group name coppacl-mon
```

```
policy-map copp-policy
class coppclass-mon
  police 1500 1500 conform-action transmit exceed-action drop
class class-default
  police 125000 3906 3906 conform-action transmit exceed-action drop
```

```
control-plane
  service-policy input copp-policy
```

QOS: QUEUING & DROPPING

Solution/Services: QoS

Related:

AutoQoS for IP Phone+Desktop Ports

- Configure Auto-QoS on switch ports with connected Cisco IP Phones and Desktops
- Data VLAN = 100
- Voice VLAN = 200

mls qos

```
interface FastEthernet0/7
switchport access vlan 100
switchport mode access
switchport voice vlan 200
auto qos voip cisco-phone
```

AutoQoS for Uplink/Downlink Ports

- Configure Auto-QoS on uplink/downlink switch ports

mls qos

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 100,200
switchport mode trunk
auto qos voip trust
```

LLQ

- Configure LLQ for Voice RTP traffic (marked using DSCP EF) to 33% of the interface's bandwidth.
- The value after the "priority" syntax can be based on a bandwidth value (kbps) or a percentage value from the total bandwidth.
- After the bandwidth or percent value you can add a burst value in bytes. If you don't add this value, it will be calculated automatically.
- LLQ can only be applied "outbound" to an interface.

```
class-map match-all RHG-CLASS-VOICE-RTP  
match ip dscp ef
```

```
policy-map RHG-POLICY  
class RHG-CLASS-VOICE-RTP  
priority percent 33
```

```
interface Multilink1  
service-policy output RHG-POLICY
```

CBWFQ

- Configure CBWFQ for Voice Control traffic (marked with DSCP AF31 or CS3) to 5% of the interface's bandwidth

```
class-map match-any RHG-CLASS-VOICE-CONTROL  
match ip dscp af31  
match ip dscp cs3
```

```
policy-map RHG-POLICY  
class RHG-CLASS-VOICE-CONTROL  
bandwidth percent 5
```

```
interface Multilink1  
service-policy output RHG-POLICY
```

WRED

- Enable WRED for Congestion Avoidance under the default class for any traffic not matched in the QoS policy

```
policy-map RHG-POLICY  
class class-default  
random-detect
```

WRED (DSCP-Based)

- Enable WRED (DSCP based) for Congestion Avoidance for all FTP traffic

```
class-map match-all RHG-CLASS-DATA-GOLD  
match protocol ftp
```

```
policy-map RHG-POLICY  
class RHG-CLASS-DATA-GOLD  
random-detect dscp-based
```

[R]

RADIUS

Solution/Services: Administration/System
Related: AAA

Basic RADIUS Configuration

- Enable RADIUS for user authentication (e.g. Telnet/SSH)
- All RADIUS communication will be sourced from the FastEthernet0/0 interface
- RADIUS server is 192.168.10.10 and shared key is cisco123
- If RADIUS server is not available, use local user database

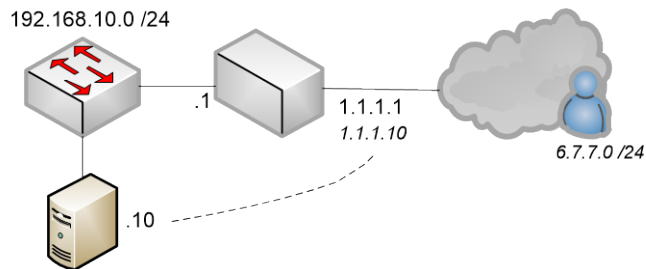
```
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default local
```

```
ip radius source-interface FastEthernet0/0
radius-server host 192.168.10.10 auth-port 1812 acct-port 1813 key cisco123
```


REFLEXIVE ACL (RACL)

Solution/Services: Security: Cisco IOS Firewalls

Related: N/A



- Stateful Firewall configuration using Reflexive ACL (rACL)
- Specify traffic that will be inspected as Stateful traffic to be allowed back in

```
ip reflexive-list timeout 120
```

```
ip access-list extended egress-acl
permit icmp any any reflect reflexive-acl
permit tcp any any reflect reflexive-acl
permit udp any any reflect reflexive-acl
permit gre any any
permit esp any any
```

- Specify inbound ACL policy for any traffic that originates from the outside into our network

```
ip access-list extended ingress-acl
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
permit tcp any host 1.1.1.10 eq smtp
permit tcp any host 1.1.1.10 eq 443
permit tcp any host 1.1.1.10 eq www
permit icmp any any echo-reply
permit udp any host 1.1.1.1 eq isakmp
permit udp any host 1.1.1.1 eq 4500
permit esp any host 1.1.1.1
permit udp host 6.7.7.8 any eq snmp
permit tcp any eq ftp-data any
evaluate reflexive-acl
deny ip any any log
```

- Apply Stateful policy (egress-acl) outbound and the ACL policy (ingress-acl) inbound on WAN facing interface

```
interface Serial0/0
ip address 1.1.1.1 255.255.255.0
ip access-group ingress-acl in
ip access-group egress-acl out
```

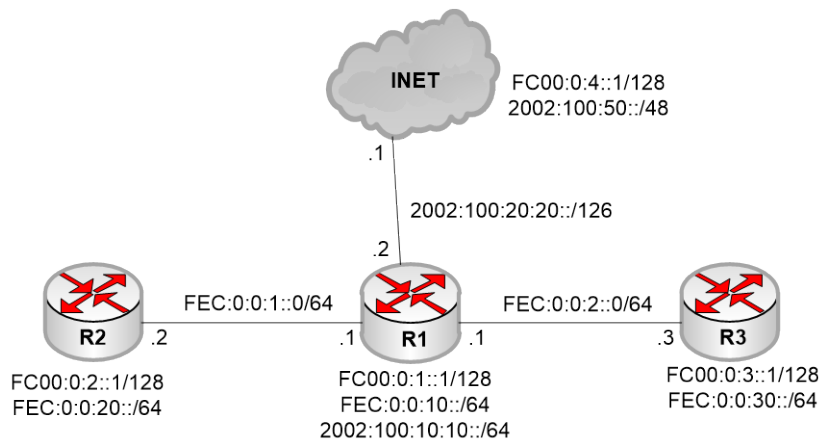
RIP

Solution/Services: Core Network Services: IP Routing

Related: N/A

RIPng (IPv6)

- Configure network (see diagram) for RIPng (IPv6) focusing on R1.
- Advertise RIP default route sourced from Loopback0 interface/network on R1 to other RIPng enabled routers.



>> R1 <<

```
ipv6 unicast-routing
ipv6 cef
```

```
ipv6 router rip RIPNG
```

```
interface Loopback0
  ipv6 address FC00:0:1::1/128
  ipv6 address FEC0:0:0:10::1/64
  ipv6 address 2002:100:10:10::1/64
  ipv6 enable
  ipv6 rip RIPNG enable
  ipv6 rip RIPNG default-information originate
```

```
interface GigabitEthernet0/1
  description TO: R2
  ipv6 address FEC0:0:0:1::1/64
  ipv6 enable
  ipv6 rip RIPNG enable
```

```
interface GigabitEthernet0/2
description TO: R3
ipv6 address FEC:0:0:2::1/64
ipv6 enable
ipv6 rip RIPNG enable
```

```
debug ipv6 rip
```

ROOTGUARD

Solution/Services: LAN Switching

Related: Spanning Tree Protocol

- Enables RootGuard on interface connecting to another switch we don't want to consider as the Root Bridge for any VLANs

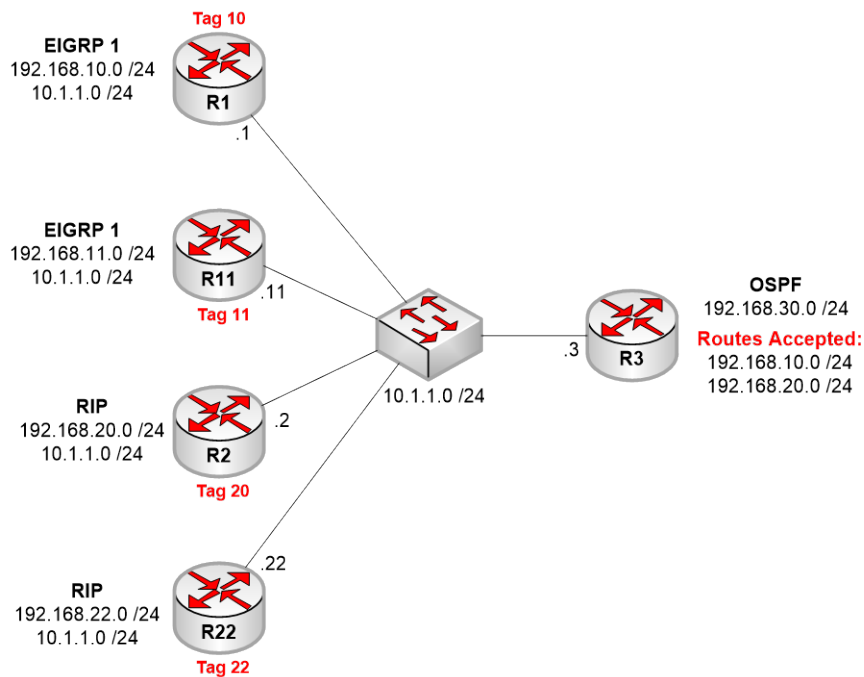
```
interface GigabitEthernet 0/4  
spanning-tree guard root
```

ROUTE TAGGING

Solution/Services: Feature
Related: N/A

Route Tagging from the Source

- On R1 tag EIGRP routes using Tag #10
- On R11 tag EIGRP routes using Tag #11
- On R2 tag RIP routes using Tag #20
- On R22 tag RIP routes using Tag #22
- On R3 only redistribute routes using Tag 10 and Tag 20



>> R1 <<

```
route-map EIGRP-TAG permit 10
set tag 10
```

```
router eigrp 1
network 192.168.10.0
network 10.0.0.0
no auto-summary
distribute-list route-map EIGRP-TAG out
```

```
>> R11 <<
route-map EIGRP-TAG permit 10
set tag 11

router eigrp 1
network 192.168.11.0
network 10.0.0.0
no auto-summary
distribute-list route-map EIGRP-TAG out
```

```
>> R2 <<
route-map RIP-TAG permit 10
set tag 20

router rip
version 2
network 192.168.20.0
network 10.0.0.0
no auto-summary
distribute-list route-map RIP-TAG out
```

```
>> R22 <<
route-map RIP-TAG permit 10
set tag 22

router rip
version 2
network 192.168.22.0
network 10.0.0.0
no auto-summary
distribute-list route-map RIP-TAG out
```

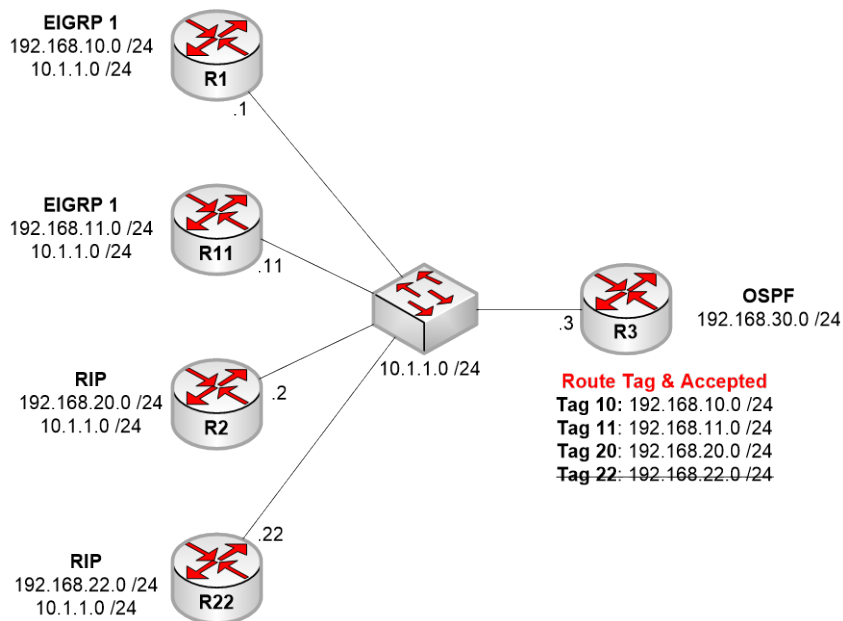
```
>> R3 <<
router eigrp 1
network 10.0.0.0
no auto-summary

router rip
version 2
network 10.0.0.0
no auto-summary

router ospf 3
redistribute eigrp 1 metric 10 subnets tag 10
redistribute rip metric 10 subnets tag 20
network 192.168.30.0 0.0.0.255 area 0
```

Route Tagging from the Destination

- On tag EIGRP routes from R1 using Tag #10
- On tag EIGRP routes from R11 using Tag #11
- On tag RIP routes from R2 using Tag #20
- On tag EIGRP routes from R22 using Tag #22
- On R3 only redistribute routes using Tags 10, 11, and 20.



>> R1 <<

```
interface fastethernet 0/0
ip address 10.1.1.1 255.255.255.0
```

```
router eigrp 1
network 192.168.10.0
network 10.0.0.0
no auto-summary
```

>> R11 <<

```
interface fastethernet 0/0
ip address 10.1.1.11 255.255.255.0
```

```
router eigrp 1
network 192.168.11.0
network 10.0.0.0
no auto-summary
```


>> R2 <<

```
interface fastethernet 0/0
ip address 10.1.1.2 255.255.255.0
```

```
router rip
version 2
network 192.168.20.0
network 10.0.0.0
no auto-summary
```

>> R22 <<

```
interface fastethernet 0/0
ip address 10.1.1.22 255.255.255.0
```

```
router rip
version 2
network 192.168.22.0
network 10.0.0.0
no auto-summary
```

>> R3 <<

```
access-list 1 permit 10.1.1.1
```

```
route-map ROUTES-EIGRP permit 10
match ip route-source 1
set tag 10
```

```
access-list 11 permit 10.1.1.11
```

```
route-map ROUTES-EIGRP permit 11
match ip route-source 11
set tag 11
```

```
access-list 2 permit 10.1.1.2
```

```
route-map ROUTES-RIP permit 10
match ip route-source 2
set tag 20
```

```
router eigrp 1
network 10.0.0.0
no auto-summary
```

```
router rip
version 2
network 10.0.0.0
no auto-summary
```

```
router ospf 3
 redistribute eigrp 1 metric 10 subnets route-map ROUTES-EIGRP
 redistribute rip metric 10 subnets route-map ROUTES-RIP
 network 192.168.30.0 0.0.0.255 area 0
```

[S]

SCHEDULER

Solution/Services: Feature
Related: N/A

- If the network is under heavy load it may not give adequate CPU time to process system-level tasks (e.g. routing protocols). Lower this effect by configuring 20 percent of the CPU available to process system-level tasks.

`scheduler allocate 2000 500`

SECONDARY IP

Solution/Services: Feature

Related: N/A

- Configures a secondary IP on interface

```
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip address 192.168.11.1 255.255.255.0 secondary
```

SENDING MESSAGE IN IOS

Solution/Services: Administration/System

Related: N/A

- Send a message to all open CON/VTY sessions established

send *

- Send a message to open CON/VTY session using connection ID 1

send 1

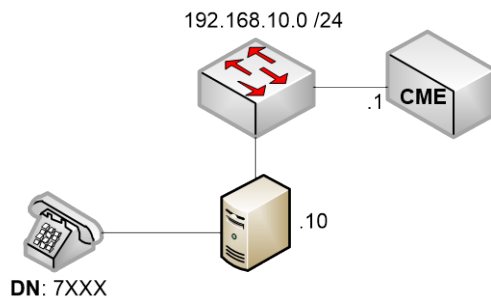
SIP

Solution/Services: Voice & Unified Communications

Related: Voice Gateway

SIP Trunk

- Build SIP trunk from Cisco IOS router to another phone system (e.g. Cisco UCM, Exchange UM) using IP 192.168.10.11
- If any user dials a number in the range of 7000 to 7999 will be routed across the SIP trunk



```
dial-peer voice 601 voip
destination-pattern 7...
session protocol sipv2
session target ipv4:192.168.10.11
session transport udp
```

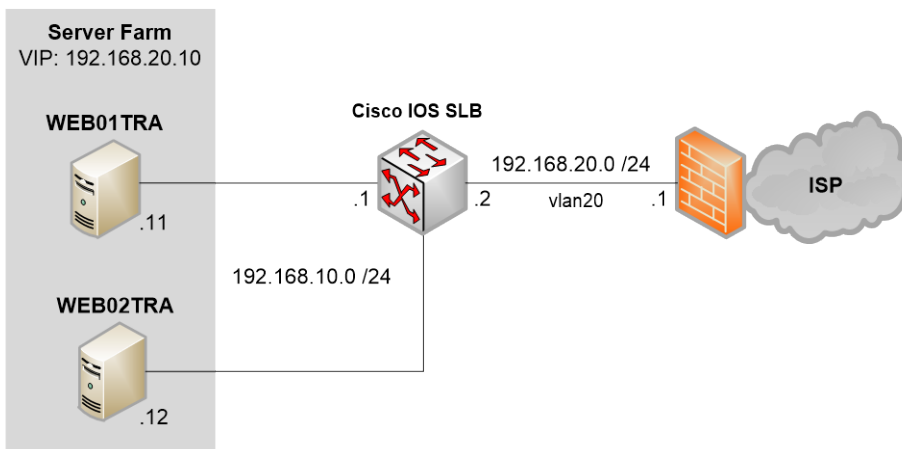
SLB (CISCO IOS)

Solution/Services: Feature

Related: Cisco ACE Series

Cisco IOS SLB

- Configure Cisco IOS SLB to load balance between two web servers (WEB01TRA and WEB02TRA) running HTTP (TCP port 80)
- The VIP used for the load-balanced web server farm will be 192.168.20.10



```
ip slb serverfarm RHG-WEB
real 192.168.10.11
inservice
real 192.168.10.12
inservice
```

```
ip slb vserver RHG-VIP-WEB
virtual 192.168.20.10 tcp www service www
serverfarm RHG-WEB
inservice
```

```
interface Vlan20
ip address 192.168.20.2 255.255.255.0
```

```
interface FastEthernet1/1
description "Uplink to the Default Gateway"
no ip address
switchport
switchport access vlan 20
```

```
ip route 0.0.0.0 0.0.0.0 192.168.20.1
```

```
interface Vlan10
ip address 192.168.10.1 255.255.255.0
```

```
interface FastEthernet1/2
description "Connection to Web server 1"
no ip address
switchport
switchport access vlan 10
```

```
interface FastEthernet1/3
description "Connection to Web server 2"
no ip address
switchport
switchport access vlan 10
```

```
show ip slb vserver
show ip slb serverfarm
```


SMTP

Solution/Services: System

Related:

Troubleshooting SMTP

1. Do a telnet to the mail server on port 25: "telnet mail.server.com 25"
2. Type in "helo" and press enter (you might not see what you type). And yes "helo" is spelled correctly.
3. Type in "mail from:youraddress@whatever.com" and press enter.
4. Type in "rcpt to:billgates@microsoft.com" substituting their address
5. Type in "data" and press enter.
6. Type in "Subject: Your subject message here" and press enter TWICE.
7. Type a short message. When you are done, press enter, input a period, and press enter again to end the message.
8. Type in "quit" and press enter to exit.

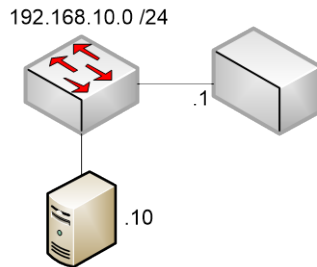
Nslookup

To see what mail server a domain is using (based on the DNS MX record) nslookup. Below is an example of looking for the mail server on the domain routehub.local.

```
nslookup
set type=mx
routehub.local
```

SNMP

Solution/Services: Management
Related:



SNMPv2

- Enable SNMPv2 using the community name "RHG-SNMP"
- Allow host 192.168.10.10 to query this device using SNMPv2
- Send SNMP traps to 192.168.10.10

```
ip access-list standard ACL-SNMP
permit 192.168.10.10
```

```
snmp-server community RHG-SNMP RO ACL-SNMP
snmp-server location Tracy, CA
snmp-server contact RHG Management
snmp-server host 192.168.10.10 RHG-SNMP
```

SNMP ifindex for Interface

- View the SNMP ifindex number for an interface (in this case for Loopback0)

```
show snmp mib ifmib ifindex loopback0
```

SNMPv3

- Enable SNMPv3
- Allow to query all objects (Internet) from this Cisco device enabled for SNMPv3
- Allow host 192.168.10.10 to query this device using SNMPv3
- SNMPv3 user will be RHGUSER. Authentication password (SHA) will be RHGPASSWORD1. Encryption password (AES 128) will be RHGPASSWORD2

```
access-list 10 permit 192.168.10.10
```

```
snmp-server view RHG-VIEW internet included
```

```
snmp-server group RHG-GROUP v3 priv read RHG-VIEW access 10
```

```
snmp-server user RHGUSER RHG-GROUP v3 auth sha RHGPASSWORD1 priv aes 128 RHGPASSWORD2
```

```
snmp-server ifindex persist
```

```
snmp-server location TRACY, CA
```

```
snmp-server contact support@routehub.local
```

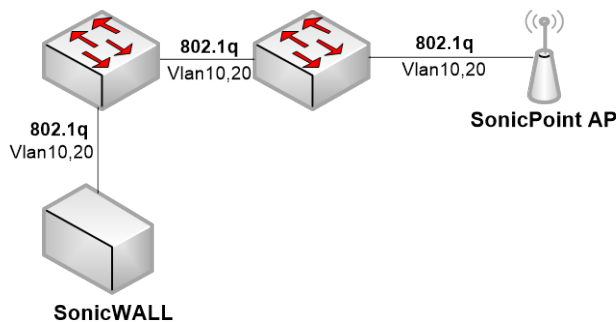
SONICWALL SOLUTIONS

Solution/Services: SonicWALL Solutions

Related: N/A

SonicPoint Cisco Switch Port

- VLAN 10 is used for the Public Wireless network
- VLAN 20 is used for the Private Wireless network
- Configure 802.1Q trunking to the SonicWALL firewall that is also acting as the Wireless Controller for the Access Points for VLANs 10 and 20
- Configure 802.1Q trunking to the Access Point(s) for VLANs 10 and 20



```
vlan 10  
name RHG-VLAN-PUBLIC
```

```
vlan 20  
name RHG-VLAN-PRIVATE
```

```
interface FastEthernet0/1  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 10,20  
switchport mode trunk  
switchport nonegotiate
```

```
interface FastEthernet0/4  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 10  
switchport trunk allowed vlan 10,20  
switchport mode trunk  
switchport nonegotiate
```

SOURCE GUARD, IP

Solution/Services: LAN Switching

Related: N/A

- Enable IP Source Guard on uplink interface to Core switch



```
interface GigabitEthernet0/1  
ip verify source
```

OR

```
interface GigabitEthernet0/1  
ip verify source vlan dhcp-snooping
```

SPANNING TREE PROTOCOL

Solution/Services: LAN Switching
Related: VLAN

Rapid Spanning Tree PVST+ (RSTP)

- Recommended configuration on L2 network

```
spanning-tree mode rapid-pvst
```

Root Bridge

- Recommended configuration on L2 network
- Lower the Bridge Priority (among all switches), the more preferred switch for the Root Bridge
- Configure Core Switch to be the Root Bridge for VLANs 100 to 200
- Configure Core switch to be the Root Bridge for VLANs 201 and 203

```
spanning-tree vlan 100-200 priority 8192
```

OR

```
spanning-tree vlan 201,203 priority 8192
```

Edge Port

- Common configuration for End User Switch Port
- Configure switch port as an Access port
- Enable STP Portfast
- Enable BPDU filter to not receive nor listen to any BPDU messages.

```
interface FastEthernet 0/10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

STP Path Cost

- Enable STP port path method to use 32-bits instead of 16-bits (default)

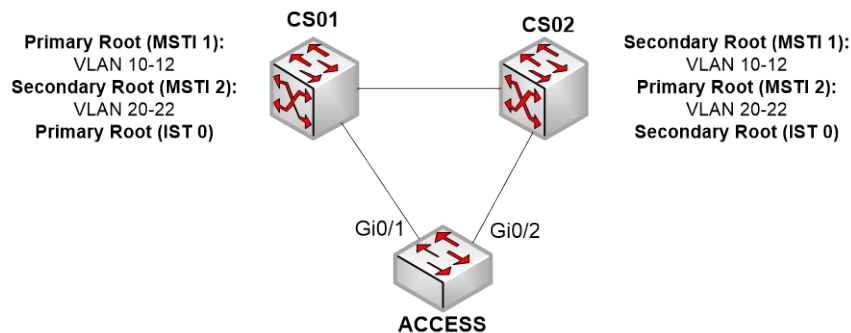
```
spanning-tree pathcost method long
```

STP Link Type

```
interface GigabitEthernet1/0/1
spanning-tree link-type point-to-point
```

MST

- Create Multiple Spanning Tree instance #1 for VLANs 10, 11, and 12
- Create Multiple Spanning Tree instance #2 for VLANs 20, 21, and 22
- CS01 will be the Primary Root Bridge for VLANs in MST Instance #1 and Secondary Root Bridge for VLANs in MST Instance #2
- CS02 will be the Primary Root Bridge for VLANs in MST Instance #2 and Secondary Root Bridge for VLANs in MST Instance #1
- For the default MST Instance (IST 0), CS01 will be the Primary Root Bridge for any VLANs in IST 0 and CS02 will be the Secondary Root Bridge for any VLANs in IST 0



>> CORE1 <<

spanning-tree mode mst

spanning-tree mst configuration

name RHG-REGION

instance 1 vlan 10, 11, 12

instance 2 vlan 20, 21, 22

spanning-tree mst 0 priority 8192

spanning-tree mst 1 priority 8192

spanning-tree mst 2 priority 16384

interface GiabitEthernet0/1

description TO: CS02

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10-29

switchport mode trunk

interface GiabitEthernet0/2

description TO: ACCESS SWITCH

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10-29

switchport mode trunk

>> CORE2 <<

spanning-tree mode mst

spanning-tree mst configuration

name RHG-REGION

instance 1 vlan 10, 11, 12

instance 2 vlan 20, 21, 22

spanning-tree mst 0 priority 16384

spanning-tree mst 2 priority 8192

spanning-tree mst 1 priority 16384

interface GiabitEthernet0/1

description TO: CS01

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10-29

switchport mode trunk

interface GiabitEthernet0/2

description TO: ACCESS SWITCH

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10-29

switchport mode trunk

>> ACCESS <<

spanning-tree mode mst

spanning-tree mst configuration

name RHG-REGION

instance 1 vlan 10, 11, 12

instance 2 vlan 20, 21, 22

interface GiabitEthernet0/1

description TO: CS01

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10-29

switchport mode trunk

interface GiabitEthernet0/2

description TO: CS02

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10-29

switchport mode trunk

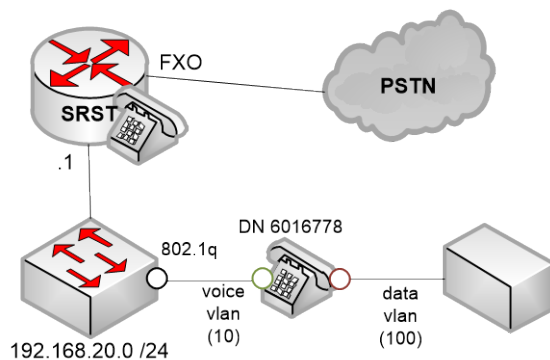
show spanning-tree mst configuration

SRST

Solution/Services: Voice & Unified Communications

Related: Voice Gateway

- Main Office: EXT (209XXXX) DID (1-209-124-XXXX) ; example 2096778 (1-209-124-6778)
- Remote Office: EXT (601XXXX), DID (1-601-510-XXXX) ; example 6016778 (1-601-510-6778)
- Enable SRST on remote voice gateway if the router loses access with the Cisco UCM server



```
hostname vgr01ms
```

```
voice class h323 1  
h225 timeout tcp establish 3
```

```
voice translation-rule 1  
rule 1 /^209\(...\) / /1209124\1/
```

```
voice translation-profile ROUTEHUB-TP-INTERSITE  
translate called 1
```

```
voice translation-rule 100  
rule 1 /^1601510\(...\) / /1/
```

```
voice translation-profile voice  
translate called 100
```

```
dial-peer voice 1 pots  
translation-profile incoming voice  
incoming called-number .  
direct-inward-dial  
port 0/3/0:23
```

```
dial-peer voice 911 pots
destination-pattern 911
port 0/3/0:23
forward-digits all
```

```
dial-peer voice 100 pots
destination-pattern 9[2-9].....
port 0/3/0:23
forward-digits 7
```

```
dial-peer voice 101 pots
destination-pattern 91[2-9]..[2-9].....
port 0/3/0:23
forward-digits 11
```

```
dial-peer voice 201 pots
translation-profile outgoing ROUTEHUB-TP-INTERSITE
destination-pattern 209....
port 0/3/0:23
```

```
call-manager-fallback
secondary-dialtone 9
max-conferences 4 gain -6
transfer-system full-consult
timeouts interdigit 5
timeouts busy 22
timeouts ringing 22
ip source-address 192.168.20.1 port 2000
max-ephones 5
max-dn 5
dialplan-pattern 1 16015106... extension-length 4
keepalive 10
moh Nightmares.wav
multicast moh 239.1.1.1 port 16384 route 192.168.20.1
time-zone 8
```

SSH

Solution/Services: Administration/System

Related:

- Enable SSHv2 on Cisco device

```
ip domain-name routehub.local
```

```
crypto key generate rsa general-keys modulus 2048
```

```
ip ssh time-out 120
```

```
ip ssh authentication-retries 3
```

```
ip ssh version 2
```

```
ip ssh logging events
```

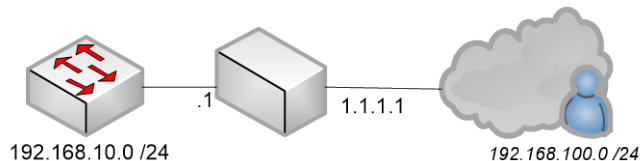
SSL VPN

Solution/Services: Security: VPN

Related: N/A

WebVPN using SVC (Tunnel Mode)

- Configure Client VPN solution using SSL VPN (Tunnel Mode)
- Specify the SSL VPN client image that can be used on a Windows system
- The VPN pool for connected users will be 192.168.100.10 – 192.168.100.13
- LAN subnet behind the VPN device is: 192.168.10.0/24
- Enable split tunnel to allow VPN users access to the 192.168.10.0 network over the established VPN tunnel
- VPN user authentication will be local. One of the local user accounts will be "user1"



```
username user1 password cisco123
```

```
aaa new-model
```

```
aaa authentication login RHG-AAA-SSL local
```

```
ip local pool RHG-POOL-VPN 192.168.100.30 192.168.100.50
```

```
webvpn gateway gateway_1
```

```
ip address 1.1.1.1 port 443
```

```
http-redirect port 80
```

```
inservice
```

```
webvpn install svc flash:/webvpn/svc.pkg
```

```
webvpn context routehub
```

```
title "RouteHub SSL VPN"
```

```
logo file logo_routehub.gif
```

```
title-color #669999
```

```
secondary-color white
```

```
text-color black
```

```
ssl authenticate verify all
```

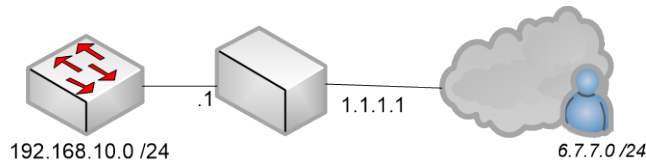
```
login-message "RouteHub Group Use Only"
```

```
policy group policy_1
functions svc-enabled
banner " RouteHub Group Use Only!"
svc address-pool "RHG-POOL-VPN"
svc keep-client-installed
svc split include 192.168.10.0 255.255.255.0
svc dns-server primary 4.2.2.2
svc dns-server secondary 4.2.2.3
```

```
default-group-policy policy_1
aaa authentication list RHG-AAA-SSL
gateway gateway_1 domain routehub.local
inservice
```

Clientless SSL VPN

- Configure Client VPN solution using SSL VPN (Clientless)
- Specify the SSL VPN client image that can be used on a Windows or Mac system
- The VPN pool for connected users will be 192.168.100.10 – 192.168.100.13
- LAN subnet behind the VPN device is: 192.168.10.0/24
- VPN user authentication will be local. One of the local user accounts will be "user1"
- Add URL to SSL VPN portal address pointing to <http://192.168.10.10>
- Create port forwarding for TCP ports 443 and SSH redirecting to 192.168.10.10



```
username user1 password cisco123
```

```
aaa new-model
```

```
aaa authentication login RHG-AAA-SSL local
```

```
webvpn gateway gateway_1
```

```
ip address 1.1.1.1 port 443
```

```
http-redirect port 80
```

```
inservice
```

```
webvpn context routehub
```

```
title "RouteHub SSL VPN"
```

```
logo file logo_routehub.gif
```

```
title-color #669999
```

```
secondary-color white
```

```
text-color black
```

```
ssl authenticate verify all
```

```
url-list "RHG-VPN-URL"
```

```
heading "ROUTEHUB URL LIST"
```

```
url-text "RHG SRV1 (HTTP)" url-value "http://192.168.10.10"
```

```
port-forward "RHG-VPN-PF"
```

```
local-port 5010 remote-server "192.168.10.10" remote-port 443 description "RHG SRV1 HTTPS"
```

```
local-port 5011 remote-server "192.168.10.10" remote-port 22 description "RHG SRV1 SSH"
```

```
policy group ROUTEHUB
```

```
url-list "RHG-VPN-URL"
```

```
port-forward "RHG-VPN-PF" auto-download
```

```
banner " RouteHub Group Use Only!"
```

```
default-group-policy ROUTEHUB
```

```
aaa authentication list RHG-AAA-SSL
```

```
gateway gateway_1
```

```
inservice
```

Cisco IOS SSL VPN Monitoring Commands

```
show webvpn context <context-name>
show webvpn context
show webvpn gateway
show webvpn gateway <gateway-name>
show webvpn session context <context-name>
show webvpn session user <username> context <context-name>
show webvpn stats
show webvpn stats httpauth
show webvpn stats tunnel
show webvpn stats sockets
show webvpn policy group <group-name> context <context-name>
```

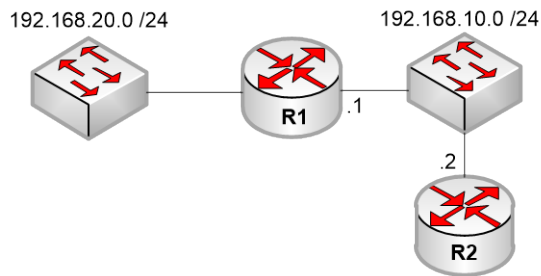

STATIC ROUTING

Solution/Services: IP Routing, IPv6

Related: N/A

Static Routing

- To access the network 192.168.20.0 go through R1 (using IP 192.168.10.1)
- Default Gateway: For access to any other network not found in routing table go to R1



>> R2 <<

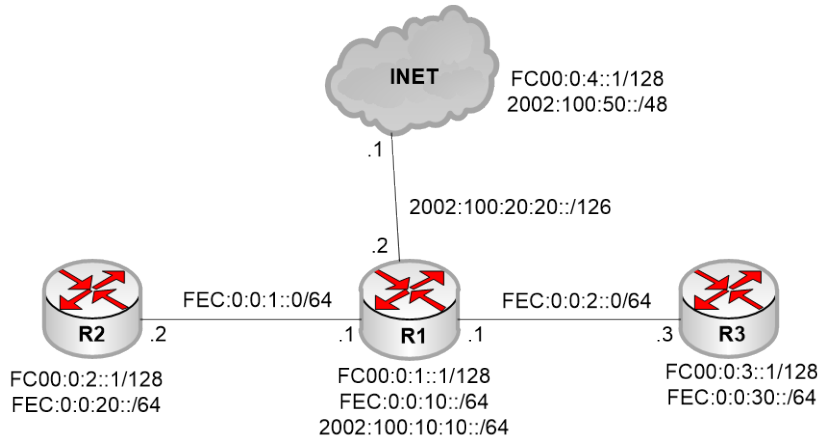
```
ip route 192.168.20.0 255.255.255.0 192.168.10.1
```

```
ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

```
show ip route static
```

IPv6 Static Route

- To access the network FEC0:0:0:20::/64 go through R2 (using IP FEC0:0:0:1::2)



```
ipv6 unicast-routing  
ipv6 cef
```

```
ipv6 route FEC0:0:0:20::/64 FEC0:0:0:1::2
```

```
show ipv6 route
```

STORM CONTROL

Solution/Services: LAN Switching

Related: N/A

Storm Control

- Restricts no more than 20% of the interface's bandwidth to broadcast traffic

```
interface GigabitEthernet0/2
storm-control broadcast level 20.00
```

Action (Shutdown)

- If there is a broadcast storm detected on interface GE0/2 based on the preconfigured percentage level (20%) shutdown the interface immediately

```
interface GigabitEthernet0/2
storm-control broadcast level 20.00
storm-control action shutdown
```



TACACS+

Solution/Services: Administration/System

Related: AAA

- Enable TACACS+ for user authentication (e.g. Telnet/SSH)
- All TACACS+ communication will be sourced from the Ethernet0/1 interface
- TACACS+ server is 192.168.10.10 and shared key is cisco6778
- If TACACS+ server is not available, use local user database (create user account called "admin")
- Console interface will use local user authentication

Basic TACACS+ Configuration

```
username admin privilege 15 secret cisco6778
```

```
aaa new-model
```

```
aaa group server tacacs+ ACS-TACACS  
server 192.168.10.10
```

```
aaa authentication login default group ACS-TACACS local  
aaa authentication login console line  
aaa authorization exec default group ACS-TACACS local  
aaa accounting exec default start-stop group ACS-TACACS  
aaa accounting commands 15 default start-stop group ACS-TACACS  
aaa accounting network default start-stop group ACS-TACACS  
aaa accounting system default start-stop group ACS-TACACS
```

```
ip tacacs source-interface Ethernet0/1
```

```
tacacs-server host 192.168.10.10 key cisco6778  
tacacs-server directed-request
```

```
line con 0  
password cisco123
```

TEMPLATES

Solution/Services: Templates, Base Configurations
Related:

Base Configuration: Cisco Catalyst Switches

```
hostname RHG-CS01-TRA-CA
vtp domain ROUTEHUB
```

```
username admin privilege 15 secret cisco123
```

```
ip domain-name ROUTEHUB
```

```
banner motd ^C
```

```
-----
This system is for ROUTEHUB GROUP use only!
```

All telecommunications and automated information systems and related equipment are for the communication, transmission, processing, and storage of ROUTEHUB information only. The systems and equipment are subject to authorized monitoring to ensure proper functioning, to protect against unauthorized use, and to verify the presence and performance of applicable security features. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of unauthorized use or criminal activity, such evidence may be provided to appropriate law enforcement personnel. Anyone using this system expressly consents to such monitoring.

```
-----
^C
```

```
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
no service tcp-small-servers
no service udp-small-servers
service sequence-numbers
```

```
logging buffered 16384
no logging console
no logging monitor
```

```
no aaa new-model
```

```
clock timezone PDT -8
clock summer-time PDT recurring

vtp mode transparent

no ip subnet-zero
no ip bootp server
no ip domain-lookup

ip routing

mls qos

errdisable recovery cause all

spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
spanning-tree backbonefast

ip tcp synwait-time 10
ip telnet quiet
ip telnet hidden addresses

ip tftp source-interface Vlan10

no cdp run
ip classless
no ip http server

alias exec c config t

ip domain-name routehub.local
crypto key generate rsa general-keys modulus 2048
ip ssh time-out 15
ip ssh version 2

ntp server 192.43.244.18 prefer

logging facility local4

line con 0
exec-timeout 15 0
password cisco123
logging synchronous

line vty 0 4
exec-timeout 15 0
login local
transport input telnet
transport output all
```

Base Configuration: Cisco Routers

```
hostname cs-cs01-mp-ca
vtp domain ROUTEHUB
```

```
username admin privilege 15 secret cisco123
```

```
ip domain-name ROUTEHUB
```

```
banner motd ^
```

```
-----
This system is for ROUTEHUB GROUP use only!
```

All telecommunications and automated information systems and related equipment are for the communication, transmission, processing, and storage of ROUTEHUB information only. The systems and equipment are subject to authorized monitoring to ensure proper functioning, to protect against unauthorized use, and to verify the presence and performance of applicable security features. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of unauthorized use or criminal activity, such evidence may be provided to appropriate law enforcement personnel. Anyone using this system expressly consents to such monitoring.

```
-----
^
```

```
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
```

```
logging buffered 16384
no logging console
no logging monitor
```

```
no aaa new-model
```

```
clock timezone PDT -8
clock summer-time PDT recurring
```

```
no ip subnet-zero
no ip bootp server
no ip domain lookup
```

```
ip tcp synwait-time 10
ip telnet quiet
ip telnet hidden addresses
```

```
no cdp run
```

```
alias exec c config t
```

```
ip domain-name routehub.local  
crypto key generate rsa general-keys modulus 2048  
ip ssh time-out 15  
ip ssh version 2
```

```
ntp server 192.43.244.18 prefer
```

```
line con 0  
exec-timeout 15 0  
password cisco123  
logging synchronous
```

```
line vty 0 4  
exec-timeout 15 0  
login local  
transport input telnet  
transport output all
```


Base Configuration: Standalone Cisco Access Point (AP)

>> on switch

```
hostname cs-cs01-mp-ca

vlan 10
 name RHG-VLAN-WLAN-PROD

vlan 110
 name RHG-VLAN-WLAN-GUEST

vlan 99
 name RHG-VLAN-WLAN-MGMT

default interface FastEthernet0/24

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,99,110
 switchport mode trunk
```

>> config on standalone AP

```
hostname rhg-ap01-sf-ca

interface BVI1
 ip address 192.168.99.21 255.255.255.0
 no ip redirects
 no ip unreachable
 no ip proxy-arp
 no ip route-cache
 no shutdown

ip default-gateway 192.168.99.1

no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption

enable secret cisco123

ip subnet-zero

no aaa new-model

dot11 vlan-name rhgpublic vlan 10
dot11 vlan-name rhgwlan vlan 110
```

```
dot11 ssid rhgwlan
vlan 110
authentication open
authentication key-management wpa
wpa-psk ascii cisco123
```

```
dot11 ssid rhgpublic
vlan 10
authentication open
authentication key-management wpa
wpa-psk ascii cisco123
```

```
dot11 network-map
dot11 arp-cache
```

```
username admin priv 15 secret cisco123
```

```
line vty 0 4
login local
```

```
bridge irb
```

```
bridge 1 protocol ieee
bridge 10 protocol ieee
bridge 110 protocol ieee
```

```
interface Dot11Radio0
no shutdown
encryption vlan 110 mode ciphers tkip
encryption vlan 10 mode ciphers tkip
ssid rhgpublic
ssid rhgwlan
```

```
station-role root access-point
no dot11 extension aironet
no cdp enable
```

```
interface Dot11Radio0.10
encapsulation dot1Q 10
no ip route-cache
no cdp enable
```

```
bridge-group 10
bridge-group 10 subscriber-loop-control
bridge-group 10 block-unknown-source
no bridge-group 10 source-learning
no bridge-group 10 unicast-flooding
bridge-group 10 spanning-disabled
```

```
interface Dot11Radio0.110
encapsulation dot1Q 110
no ip route-cache
no cdp enable
bridge-group 110
bridge-group 110 subscriber-loop-control
bridge-group 110 block-unknown-source
no bridge-group 110 source-learning
no bridge-group 110 unicast-flooding
bridge-group 110 spanning-disabled
```

```
interface FastEthernet0.99
encapsulation dot1Q 99 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
```

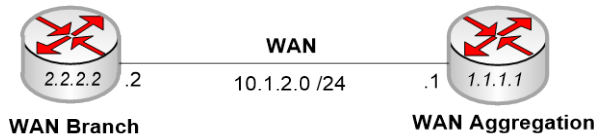
```
interface FastEthernet0.10
encapsulation dot1Q 10
no ip route-cache
bridge-group 10
no bridge-group 10 source-learning
bridge-group 10 spanning-disabled
```

```
interface FastEthernet0.110
encapsulation dot1Q 110
no ip route-cache
bridge-group 110
no bridge-group 110 source-learning
bridge-group 110 spanning-disabled
end
```

```
write mem
```

QoS on WAN Router (I)

- WAN QoS policy: (1) Voice RTP = LLQ 33% & cRTP, (2) Voice Control = CBWFQ 5%, and (3) all other traffic = WFQ & WRED for TCP traffic



>> WAN AGG <<

```
class-map match-all RHG-CM-VOICE-RTP
match ip dscp ef
```

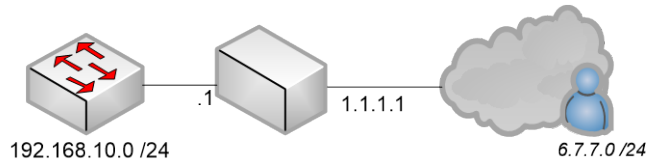
```
class-map match-any RHG-CM-VOICE-CONTROL
match ip dscp cs3
match ip dscp af31
```

```
policy-map RHG-PM-QOS
class RHG-CM-VOICE-RTP
priority percent 33
compress header ip rtp
class RHG-CM-VOICE-CONTROL
bandwidth percent 5
class class-default
fair-queue
random-detect dscp-based
```

```
interface Serial0/0
ip address 10.1.2.1 255.255.255.0
service-policy output RHG-PM-QOS
```

QoS on Internet Edge

- Internet Edge QoS policy: (1) WWW, POP3, FTP, & SMTP = CBWFQ 60% and (2) all other traffic = CBWFQ 15%



```
ip access-list extended ACL-TRAFFIC
permit tcp any any eq www
permit tcp any any eq pop3
permit tcp any any eq ftp
permit tcp any any eq smtp
```

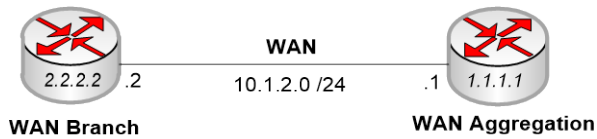
```
class-map match-all CMAP-TRAFFIC
match access-group name ACL-TRAFFIC
```

```
policy-map POL-TRAFFIC
class CMAP-TRAFFIC
bandwidth percent 60
class class-default
bandwidth percent 15
```

```
interface GigabitEthernet0/0
ip address 1.1.1.1 255.255.255.0
service-policy output POL-TRAFFIC
```

QoS on WAN Router (II) using ACL

- WAN QoS policy using a medal class (GOLD) SMTP & HTTPS = LLQ %50, (SILVER) POP3 & FTP = LLQ 15%, (BRONZE) WWW = LLQ 10%, (Everything Else) all other traffic = WFQ
- Classification based on ACL



```
ip access-list extended ACL-BRONZE
permit tcp any any eq www
```

```
class-map match-all BRONZE
match access-group name ACL-BRONZE
```

```
ip access-list extended ACL-SILVER
permit tcp any any eq pop3
permit tcp any any eq ftp
```

```
class-map match-all SILVER
match access-group name ACL-SILVER
```

```
ip access-list extended ACL-GOLD
permit tcp any any eq 443
permit tcp any any eq smtp
```

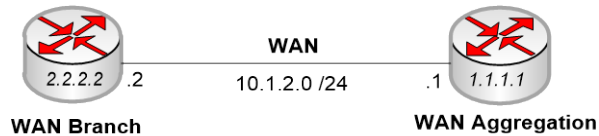
```
class-map match-all GOLD
match access-group name ACL-GOLD
```

```
policy-map POLICY1
class GOLD
priority percent 50
set precedence 5
class SILVER
priority percent 15
set precedence 4
class BRONZE
priority percent 10
set precedence 3
class class-default
set precedence 0
fair-queue
```

```
interface Serial0/1/0
ip address 10.1.2.1 255.255.255.0
service-module t1 timeslots 1-24
service-policy output POLICY1
```

QoS on WAN Router (II) using NBAR

- WAN QoS policy using a medal class (GOLD) SMTP,HTTPS,SIP,RTP = LLQ %50. (SILVER) POP3 & FTP = LLQ 15%. (BRONZE) WWW =LLQ 10%, (Everything Else) all other traffic = WFQ
- Classification based on NBAR



```
class-map match-all BRONZE
match protocol http
match protocol http host "*google.com*"
match protocol http host "*live.com*"
match protocol http host "*hotmail.com*"
match protocol http host "*yahoo.com*"
```

```
class-map match-all SILVER
match protocol pop3
match protocol ftp
```

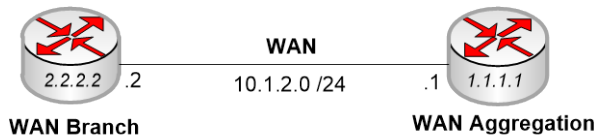
```
class-map match-all GOLD
match protocol smtp
match protocol secure-http
match protocol rtp
match protocol sip
```

```
policy-map POLICY1
class GOLD
priority percent 50
set precedence 5
class SILVER
priority percent 15
set precedence 4
class BRONZE
priority percent 10
set precedence 3
class class-default
set precedence 0
fair-queue
```

```
interface Serial0/1/0
ip address 10.1.2.1 255.255.255.0
service-module t1 timeslots 1-24
service-policy output POLICY1
```

QoS Policy for WAN Branch Router

- Recommended QoS policy #3 for a WAN Branch Router
- Traffic is already marked on the LAN
- Traffic classified for Interactive Video, Network Control, Critical Data, Voice Control, and Voice Data (RTP)
- Map L2 QoS (CoS) to L3 QoS (DSCP) between the router and the local L2 switch



```
class-map match-all Interactive-Video
match ip dscp af41 af42
class-map match-any Network-Control
match ip dscp cs6
match ip dscp cs2
class-map match-all Critical-Data
match ip dscp af21 af22
class-map match-all Call-Signalling
match ip dscp cs3
class-map match-all Voice
match ip dscp ef
```

```
policy-map LAN
class class-default
set cos dscp
```

```
policy-map WAN
class Voice
priority percent 7
compress header ip rtp
class Interactive-Video
priority percent 31
class Network-Control
bandwidth percent 5
class Critical-Data
bandwidth percent 25
random-detect dscp-based
class Call-Signalling
bandwidth percent 5
class class-default
bandwidth percent 25
random-detect
```

```
interface Serial0/0/0:0
description WAN interface
ip address 10.1.2.2 255.255.255.252
load-interval 30
max-reserved-bandwidth 100
service-policy output WAN
```



```
interface GigabitEthernet0/0
description LAN interface
ip address 192.168.20.1 255.255.255.0
service-policy output LAN
```

Layer 2 Edge Port

- Common configuration for End User Switch Port
- Configure switch port as an Access port
- Enable STP Portfast
- Enable BPDU filter to not receive nor listen to any BPDU messages.

```
interface FastEthernet 0/10
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

TERMINAL SERVER ROUTER

Solution/Services: Administration/System

Related: N/A

- Configuration on terminal server router with async ports which maps IP address 192.168.10.71 to TTY port 2001.
- This means if we do a telnet to 192.168.10.71 it will automatically connect to the console session off of port 2001

```
chat-script router-logout "" exit "" exit "" exit ""
```

```
interface FastEthernet0/0  
ip address 192.168.10.1 255.255.255.0
```

```
ip host TTY-1 23 192.168.10.71  
ip alias 192.168.10.71 2001
```

```
line 33 63  
script reset router-logout  
modem Host  
transport input telnet  
stopbits 1  
flowcontrol hardware
```

TFTP

Solution/Services: Administration/System

Related: N/A

Router as TFTP Server

- Automatically makes Cisco IOS router act as a TFTP server
- Specify file (e.g. IOS image) that will exist in the TFTP root folder on the Cisco IOS router

```
tftp-server flash:c2801-advipservicesk9-mz.151-3.T.bin
```

Load IOS from TFTP server over the network

- Removes all previous boot system statements from the configuration file.
- Specifies that the client router load a system image from the server.
- Specifies that the client router loads its own ROM image if the load from a server fails.
- Sets the configuration register to enable the client router to load a system image from a network server.

```
no boot system  
boot system flash:CiscoIOS.bin 192.168.10.10  
boot system rom  
config-register 0x010F
```

TIME-ZONE

Solution/Services: Administration/System

Related: N/A

- Specify timezone (PST using -8) and enable Daylight Savings

clock timezone pst -8

clock summer-time pst recurring

TRUNKING (802.1Q)

Solution/Services: LAN Switching
Related: N/A

802.1Q

- Enables 802.1Q Trunking (or VLAN tagging) on GE0/1

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
```

Dynamic Trunk Protocol (DTP)

- Disable DTP and establish interface as a Trunk without negotiation

```
interface GigabitEthernet0/1
switchport nonegotiate
```

Trunk Security

- Only allow VLAN tags 100 to 102 to be extended across GE0/1 with the connected device. All other VLAN access will be restricted

```
interface GigabitEthernet0/1
switchport trunk allowed vlan 100-102
```

Native VLAN

- Configure bit-bucket VLAN (VLAN999) and shutdown VLAN
- Configure Native VLAN on interface GE0/1 to be VLAN999

```
vlan 999  
name bit-bucket  
shutdown
```

```
interface GigabitEthernet0/1  
switchport trunk native vlan 999
```

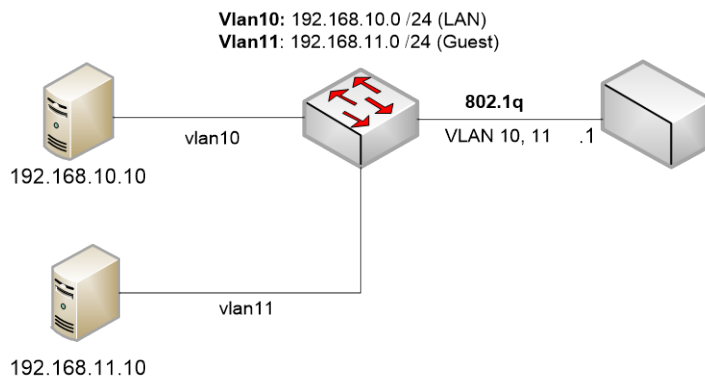
Tag Native VLAN

- Force all VLANs including the Native VLAN to be tagged

```
vlan dot1q tag native
```

802.1Q Interfaces on Cisco Routers

- Configure 802.1Q trunking with Cisco Router for VLANs 10 and 11



```
interface GigabitEthernet0/0
no ip address
duplex full
speed 100
```

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
```

```
interface GigabitEthernet0/0.11
encapsulation dot1Q 11
ip address 192.168.11.1 255.255.255.0
```

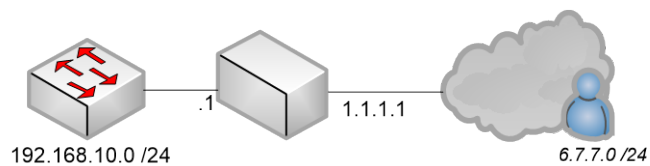
T-1

Solution/Services: Media Connection

Related: N/A

Serial T-1 (i)

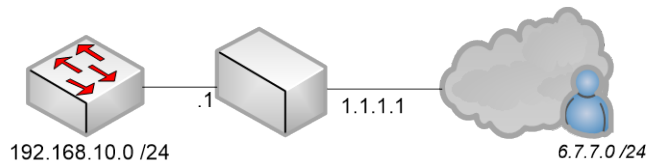
- Integrated CSU/DSU T1 module
- T1 using PPP encapsulation, 24 time-slots



```
interface Serial0/1
ip address 1.1.1.1 255.255.255.0
encapsulation ppp
fair-queue
service-module t1 clock source internal
service-module t1 timeslots 1-24
```


Serial T-1 (ii)

- Integrated CSU/DSU T1 module
- T1/E1 module located in slot 0, wic 0. Specify using a T1 instead of a E1
- Define channel group ID "0" and the number of time-slots of the T1 circuit (up to 24)



```
card type t1 0 0
```

```
network-clock-participate wic 0  
network-clock-select 1 T1 0/0/0
```

```
controller T1 0/0/0  
framing esf  
linecode b8zs  
clock source line primary  
channel-group 0 timeslots 1-24
```

```
interface Serial0/0/0:0  
ip address 1.1.1.1 255.255.255.0  
encapsulation ppp
```

T1 using CAS

- T1 using CAS
- DS0 group #0 with 1-4 timeslots
- Signaling: E&M

```
controller T1 1/0  
framing esf  
linecode b8zs  
ds0-group 0 timeslots 1-4 type e&m-wink-start
```

[U]

UNICAST RPF, IP

Solution/Services: Security

Related: N/A

- Helps in defense against spoofing attacks

```
interface GigabitEthernet1/1
description Untrusted facing interface
ip verify unicast reverse-path
```

UDLD

Solution/Services: LAN Switching
Related: N/A

UDLD Aggressive

- Enables UDLD aggressive mode between connected switches on the interfaces (not globally)

```
>>SW1<<  
interface GigabitEthernet0/1  
udld port aggressive
```

```
>>SW2<<  
interface GigabitEthernet0/1  
udld port aggressive
```

URBL

Solution/Services: Cisco Catalyst 6500 Series
Related: QoS

User-Based Rate Limiting (URBL)

- Rate limit each IP from subnet (192.168.10.0) to 10Mbps with bursting up to 5KB
- URBL applied to interface with that connected subnet
- *Note: doesn't impact rate limiting to a user, only rate limiting from a user.*



```
ip access-list extended ubrl-dept1-acl
remark department1 - 10Mb connection
permit ip 192.168.10.0 0.0.0.255 any
```

```
class-map match-any ubrl-dept1-class
match access-group name ubrl-dept1-acl
```

```
policy-map ubrl-policy
class ubrl-dept1-class
police flow mask src-only 10000000 5000 conform-action transmit exceed-action drop
```

```
interface gigabitethernet3/1
service-policy input ubrl-policy
```

User-Based Rate Limiting (URBL) Bi-Directional

- Rate limit each IP to and from subnet (192.168.10.0) to 10Mbps with bursting up to 5KB
- URBL policies applied to interface with that connected subnet
- *Note: this will rate limit to and from a user*



```
ip access-list extended ubrl-university-egress-acl
remark department1 - 10Mb connection
permit ip 192.168.10.0 0.0.0.255 any
```

```
class-map match-any ubrl-university-egress-class
match access-group name ubrl-university-egress-acl
```

```
ip access-list extended ubrl-university-ingress-acl
remark department1 - 10Mb connection
permit ip any 192.168.10.0 0.0.0.255
```

```
class-map match-any ubrl-university-ingress-class
match access-group name ubrl-university-ingress-acl
```

```
policy-map ubrl-policy
class ubrl-university-egress-class
  police flow mask src-only 1000000 1000 conform-action transmit exceed-action drop
class ubrl-university-ingress-class
  police flow mask dst-only 1000000 1000 conform-action transmit exceed-action drop
```

```
interface gigabitethernet3/1
service-policy input ubrl-policy
```

[M]

VLAN

Solution/Services: LAN Switching
Related: VTP, Trunking (802.1Q), Spanning Tree

VLAN (L2)

- Add VLAN 100 to switch and associate a name to the VLAN
- Put switch port FE0/10 into VLAN 100

```
vlan 100  
name ROUTEHUB-VLAN-USER1
```

```
interface FastEthernet 0/10  
switchport mode access  
switchport access vlan 100
```

- To view all VLAN configured (or learned via VTP) on the switch

```
show vlan
```

VLAN SVI (L3)

- Make L2 VLAN routable with other networks and VLANs

```
interface Vlan100
ip address 192.168.100.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
no shutdown
```

Disable VLAN AutoState

- Disable auto-state capability. This will force the VLAN1 interface to automatically come up without having a switch port assigned to VLAN1 and in a connected state.

```
interface Vlan1
no autostate
```

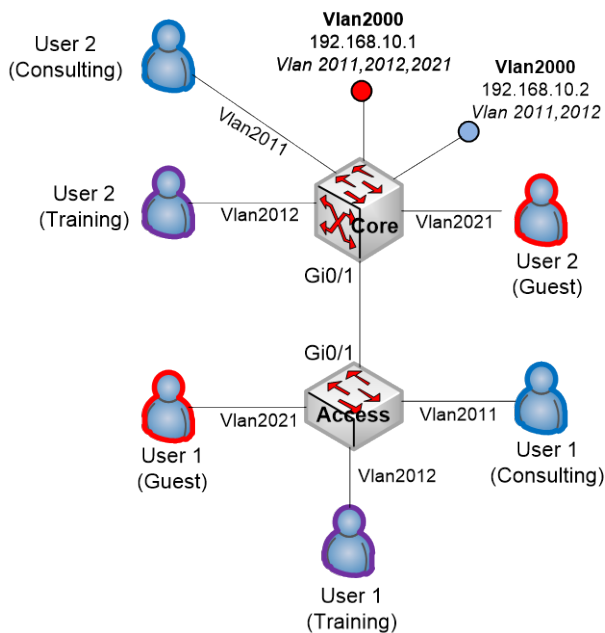
Support 4000+ VLANs

- **Requirements:** 802.1Q encapsulation for Trunking
- Allows support of 4000+ VLANs when using 802.1Q

```
spanning-tree extend system-id
```

Private VLANs

- **Community:** hosts can communicate with other hosts in the same community including the promiscuous router port.
- **Isolated:** hosts can only communicate with the promiscuous router port
- The primary VLAN that will be used by all private VLANs will be VLAN 2000
- VLAN 2011 will be a Community Private VLAN (for Consulting Group)
- VLAN2012 will be another Community Private VLAN (for Training Group)
- VLAN2021 will be an Isolated Private VLAN (for Guest Users)
- On Core & Access Switches configure Private VLAN switch ports based on network diagram (see below)
- Core: VLAN2000 (192.168.10.1) = interface that hosts in the two VLAN communities including the hosts in the isolated VLANs can use for communicating with each other. 192.168.10.1 would be the IP they would use for their default gateway.
- Core: VLAN2000 (192.168.10.2) = interface that hosts in the two VLAN communities for communicating with each other. 192.168.10.2 would be the IP they would use for their default gateway.



>>ACCESS<<

vlan 2000
private-vlan primary

vlan 2011
private-vlan community

vlan 2012
private-vlan community

vlan 2021
private-vlan isolated

vlan 2000
private-vlan association 2011,2012,2021


```

interface fastethernet0/1
description Consulting Host1
switchport private-vlan host association 2000 2011
switchport mode private-vlan host

interface fastethernet0/2
description Training Host1
switchport private-vlan host association 2000 2012
switchport mode private-vlan host

interface fastethernet0/3
description Guest Host1
switchport private-vlan host association 2000 2021
switchport mode private-vlan host

interface gigabitethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk

```

>>CORE<<

```

interface fastethernet0/2
description Consulting Host2
switchport private-vlan host association 2000 2011
switchport mode private-vlan host

interface fastethernet0/3
description Training Host2
switchport private-vlan host association 2000 2012
switchport mode private-vlan host

interface fastethernet0/4
description Guest Host2
switchport private-vlan host association 2000 2021
switchport mode private-vlan host

interface gigabitethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk

```

```

interface vlan2000
ip address 192.168.10.1 255.255.255.0
private-vlan mapping 2011,2012,2021

```

```

interface vlan2000
ip address 192.168.10.2 255.255.255.0
private-vlan mapping 2011,2012

```

```
show interfaces private-vlan mapping  
show vlan private-vlan
```

VLAN TRUNKING PROTOCOL (VTP)

Solution/Services: LAN Switching

Related: VLAN, Trunking (802.1Q)

VTP

- **Recommendation:** use VTP transparent mode over Server mode to avoid L2 issues
- **Mode:** Other VTP modes can be Client (ideal for Access Switches) and Server (ideal for Core/Distribution)
- **Transparent Mode:** Adding/Removing VLANs are done locally on the switch.
- Configure VTP mode to be transparent and specify VTP domain to be ROUTEHUB

vtp domain ROUTEHUB

vtp mode transparent

VOICE GATEWAY

Solution/Services: Voice & Unified Communications
Related: N/A

Monitor

```
debug voip ccapi inout
debug isdn q931
show voice dsp group all
show voice dsp voice
test voice translation-rule X
```

Test Calling on Voice Gateway

- From the Cisco voice gateway dial a DID number (access code of 9)

```
csim start 919252302203
```

Hardware Conferencing & Transcoding

- Enable Conferencing and Transcoding services on voice gateway router
- Primary CUCM server is 192.168.10.10, Secondary CUCM server is 192.168.10.11

```
voice-card 0
dsp services dspfarm
```

```
sccp local FastEthernet0/0
sccp ccm 192.168.10.10 identifier 1 priority 1
sccp ccm 192.168.10.11 identifier 2 priority 2
sccp
```

```
dspfarm profile 1 transcode
codec g711ulaw
codec g711alaw
codec g729ar8
```

```
codec g729abr8
maximum sessions 8
associate application SCCP
```

```
dspfarm profile 2 conference
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec g729r8
codec g729br8
codec g722-64
codec ilbc
maximum sessions 2
associate application SCCP
```

```
sccp ccm group 1
bind interface FastEthernet0/0
associate ccm 1 priority 1
associate ccm 2 priority 2
associate profile 1 register RHG_CFB
associate profile 2 register RHG_MTP
keepalive retries 5
switchover method graceful
switchback interval 60
```

Ringback Issue for H.323

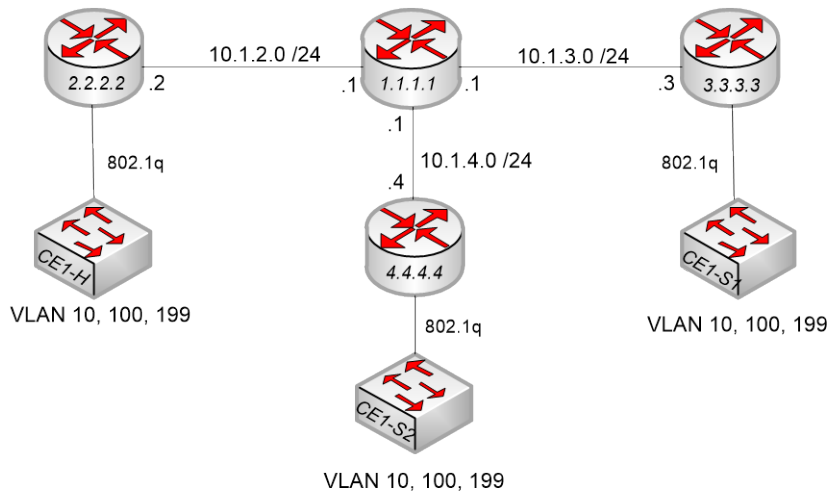
- Enable commands under H.323 dial peer if a ringback issue is reported.

```
dial-peer voice 70 pots
incoming called-number .
destination-pattern 9T
progress_ind alert enable 8
progress_ind progress enable 8
progress_ind connect enable 8
direct-inward-dial
port 0/0:23
forward-digits all
```

VPLS

Solution/Services: Tunneling: L2VPN

Related: N/A



VPLS (VLAN-Based)

- VPLS: creates isolated point-to-multipoint L2 tunnels between sites
- Customer network (Customer Edge 1) using CE1-Hub (Hub), CE1-S1 (Spoke 1), and CE1-S2 (Spoke 2)
- Customer network connected into Layer 2 Service Provider configured for VPLS (VLAN-based)
- Customer network will extend VLANs 10 (Internal), 100 (Guest), 199 (Management) between the sites
- VPLS provider will use ID "50" for the CE1 customer network for extending VLANs 10,100,199

```
>>PE1 (2.2.2.2)<<
interface Loopback0
ip address 2.2.2.2 255.255.255.255
```

```
I2 vfi VPLS-CLIENT1 manual
vpn id 50
neighbor 3.3.3.3 encapsulation mpls
neighbor 4.4.4.4 encapsulation mpls
```

```
vlan 10
name RHG-CE1-INTERNAL
state active
```

```
vlan 100
name RHG-CE1-GUEST
state active
```

```
vlan 199
name RHG-CE1-MGMT
state active
```

```
interface Vlan10
xconnect vfi VPLS-CLIENT1
```

```
interface Vlan100
xconnect vfi VPLS-CLIENT1
```

```
interface Vlan199
xconnect vfi VPLS-CLIENT1
```

```
interface FastEthernet4/1
description TO: CE1-H
switchport
switchport mode trunk
switchport trunk encapsulation dot1q
switchport allowed vlan 10,100,199
no shutdown
```

>>PE2 (3.3.3.3)<<

```
interface Loopback0
ip address 3.3.3.3 255.255.255.255
```

```
I2 vfi VPLS-CLIENT1 manual
vpn id 50
neighbor 2.2.2.2 encapsulation mpls
neighbor 4.4.4.4 encapsulation mpls
```

```
vlan 10
name RHG-CE1-INTERNAL
state active
```

```
vlan 100
name RHG-CE1-GUEST
state active
```

```
vlan 199
name RHG-CE1-MGMT
state active
```

```
interface Vlan10
xconnect vfi VPLS-CLIENT1
```

```
interface Vlan100
xconnect vfi VPLS-CLIENT1
```

```
interface Vlan199
xconnect vfi VPLS-CLIENT1
```

```
interface FastEthernet4/1
description TO: CE1-S1
switchport
switchport mode trunk
switchport trunk encapsulation dot1q
switchport allowed vlan 10,100,199
no shutdown
```

```
>>PE3 (4.4.4.4)<<
interface Loopback0
ip address 4.4.4.4 255.255.255.255
```

```
I2 vfi VPLS-CLIENT1 manual
vpn id 50
neighbor 2.2.2.2 encapsulation mpls
neighbor 3.3.3.3 encapsulation mpls
```

```
vlan 10
name RHG-CE1-INTERNAL
state active
```

```
vlan 100
name RHG-CE1-GUEST
state active
```

```
vlan 199
name RHG-CE1-MGMT
state active
```

```
interface Vlan10
xconnect vfi VPLS-CLIENT1
```

```
interface Vlan100
xconnect vfi VPLS-CLIENT1
```

```
interface Vlan199
xconnect vfi VPLS-CLIENT1
```

```
interface FastEthernet4/1
description TO: CE1-S2
switchport
switchport mode trunk
switchport trunk encapsulation dot1q
switchport allowed vlan 10,100,199
no shutdown
```


>>CE1-H<<

vlan 10

name RHG-CE1-INTERNAL

vlan 100

name RHG-CE1-GUEST

vlan 199

name RHG-CE1-MGMT

interface FastEthernet1/0/1

description TO: PE1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 10,100,199

switchport nonegotiate

spanning-tree portfast trunk

no shutdown

interface Vlan 10

description RHG VLAN SVI INTERNAL

ip address 192.168.10.1 255.255.255.0

no shutdown

interface Vlan 100

description RHG VLAN SVI GUEST

ip address 192.168.100.1 255.255.255.0

no shutdown

interface Vlan 199

description RHG VLAN SVI MGMT

ip address 192.168.199.1 255.255.255.0

no shutdown

>>CE1-S1<<

vlan 10

name RHG-CE1-INTERNAL

vlan 100

name RHG-CE1-GUEST

vlan 199

name RHG-CE1-MGMT

interface FastEthernet1/0/1

description TO: PE2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 10,100,199

switchport nonegotiate

spanning-tree portfast trunk

no shutdown

```

interface FastEthernet1/0/2
description Internal network switch port
switchport access vlan 10
switchport mode access
spanning-tree portfast
no shutdown

interface FastEthernet1/0/3
description Guest network switch port
switchport access vlan 100
switchport mode access
spanning-tree portfast
no shutdown

interface Vlan 199
description RHG VLAN SVI MGMT
ip address 192.168.199.10 255.255.255.0
no shutdown

ip default-gateway 192.168.199.1

```

>>CE1-S2<<

```

vlan 10
name RHG-CE1-INTERNAL

vlan 100
name RHG-CE1-GUEST

vlan 199
name RHG-CE1-MGMT

interface FastEthernet1/0/1
description TO: PE3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,100,199
switchport nonegotiate
spanning-tree portfast trunk
no shutdown

interface FastEthernet1/0/2
description Internal network switch port
switchport access vlan 10
switchport mode access
spanning-tree portfast
no shutdown

interface FastEthernet1/0/3
description Guest network switch port
switchport access vlan 100
switchport mode access
spanning-tree portfast
no shutdown

```

```
interface Vlan 199
description RHG VLAN SVI MGMT
ip address 192.168.199.11 255.255.255.0
no shutdown

ip default-gateway 192.168.199.1
```

VPLS (QinQ, Port-Based)

- *VPLS: creates isolated point-to-multipoint L2 tunnels between sites*
- Customer network (Customer Edge 1) using CE1-Hub (Hub), CE1-S1 (Spoke 1), and CE1-S2 (Spoke 2)
- Customer network connected into Layer 2 Service Provider configured for VPLS (VLAN-based)
- Customer network will extend VLANs 10 (Internal), 100 (Guest), 199 (Management) between the sites
- VPLS provider will use ID "50" for the CE1 customer network for extending VLANs 10,100,199
- VPLS provider will configured QinQ which basically encapsulates a customer's 802.1Q connection in a single VLAN that is switched across the provider's L2 network.

>>PE1<<

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
```

```
I2 vfi VPLS-CLIENT1 manual
vpn id 50
neighbor 3.3.3.3 encapsulation mpls
neighbor 4.4.4.4 encapsulation mpls
```

```
vlan 900
name RHG-CE1-QinQ
state active
```

```
interface Vlan900
xconnect vfi VPLS-CLIENT1
```

```
interface FastEthernet4/1
description TO: CE1-H
switchport
switchport mode dot1qtunnel
switchport access vlan 900
l2protocol-tunnel-stp
no shutdown
```

>>PE2<<

```
interface Loopback0
ip address 3.3.3.3 255.255.255.255
```

```
I2 vfi VPLS-CLIENT1 manual
vpn id 50
neighbor 2.2.2.2 encapsulation mpls
neighbor 4.4.4.4 encapsulation mpls
```

```
vlan 900
name RHG-CE1-QinQ
state active
```

```
interface Vlan900
xconnect vfi VPLS-CLIENT1
```

```
interface FastEthernet4/1
description TO: CE1-S1
switchport
switchport mode dot1qtunnel
switchport access vlan 900
l2protocol-tunnel-stp
no shutdown
```

```
>>PE3<<
interface Loopback0
ip address 4.4.4.4 255.255.255.255

l2 vfi VPLS-CLIENT1 manual
vpn id 50
neighbor 2.2.2.2 encapsulation mpls
neighbor 3.3.3.3 encapsulation mpls
```

```
vlan 900
name RHG-CE1-QinQ
state active
```

```
interface Vlan900
xconnect vfi VPLS-CLIENT1
```

```
interface FastEthernet4/1
description TO: CE1-S2
switchport
switchport mode dot1qtunnel
switchport access vlan 900
l2protocol-tunnel-stp
no shutdown
```

```
>>CE1-H<<
vlan 10
name RHG-CE1-INTERNAL

vlan 100
name RHG-CE1-GUEST

vlan 199
name RHG-CE1-MGMT

interface FastEthernet1/0/1
description TO: PE1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,100,199
switchport nonegotiate
spanning-tree portfast trunk
no shutdown
```

```
interface Vlan 10
description RHG VLAN SVI INTERNAL
ip address 192.168.10.1 255.255.255.0
no shutdown
```

```
interface Vlan 100
description RHG VLAN SVI GUEST
ip address 192.168.100.1 255.255.255.0
no shutdown
```

```
interface Vlan 199
description RHG VLAN SVI MGMT
ip address 192.168.199.1 255.255.255.0
no shutdown
```

```
>>CE1-S1<<
```

```
vlan 10
name RHG-CE1-INTERNAL
```

```
vlan 100
name RHG-CE1-GUEST
```

```
vlan 199
name RHG-CE1-MGMT
```

```
interface FastEthernet1/0/1
description TO: PE2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,100,199
switchport nonegotiate
spanning-tree portfast trunk
no shutdown
```

```
interface FastEthernet0/2
description TO: Internal network switch port
switchport access vlan 10
switchport mode access
spanning-tree portfast
no shutdown
```

```
interface FastEthernet0/3
description TO: Guest network switch port
switchport access vlan 100
switchport mode access
spanning-tree portfast
no shutdown
```

```
interface Vlan 199
description RHG VLAN SVI MGMT
ip address 192.168.199.10 255.255.255.0
no shutdown
```

```
ip default-gateway 192.168.199.1
```

```
>>CE1-S2<<
```

```
vlan 10
```

```
name RHG-CE1-INTERNAL
```

```
vlan 100
```

```
name RHG-CE1-GUEST
```

```
vlan 199
```

```
name RHG-CE1-MGMT
```

```
interface FastEthernet1/0/1
```

```
description TO: PE3
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 10,100,199
```

```
switchport nonegotiate
```

```
spanning-tree portfast trunk
```

```
no shutdown
```

```
interface FastEthernet0/2
```

```
description TO: Internal network switch port
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
no shutdown
```

```
interface FastEthernet0/3
```

```
description TO: Guest network switch port
```

```
switchport access vlan 100
```

```
switchport mode access
```

```
spanning-tree portfast
```

```
no shutdown
```

```
interface Vlan 199
```

```
description RHG VLAN SVI MGMT
```

```
ip address 192.168.199.11 255.255.255.0
```

```
no shutdown
```

```
ip default-gateway 192.168.199.1
```

VPLS Monitoring Commands

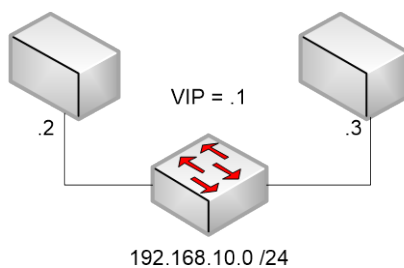
```
show mpls l2transport vc <VC-ID> detail
```

VRRP

Solution/Services: Core Network Services: First Hop Redundancy Protocols (FHRP)

Related: HSRP, GLBP

- **Priority:** higher the value, the more preferred primary default gateway device
- SW1 would be the primary VRRP router and SW2 would be the secondary VRRP router
- Configure VRRP for network 192.168.10.1 (VLAN 10)
- The VRRP IP address will be 192.168.10.1 (this would be the IP devices would use for their default gateway)

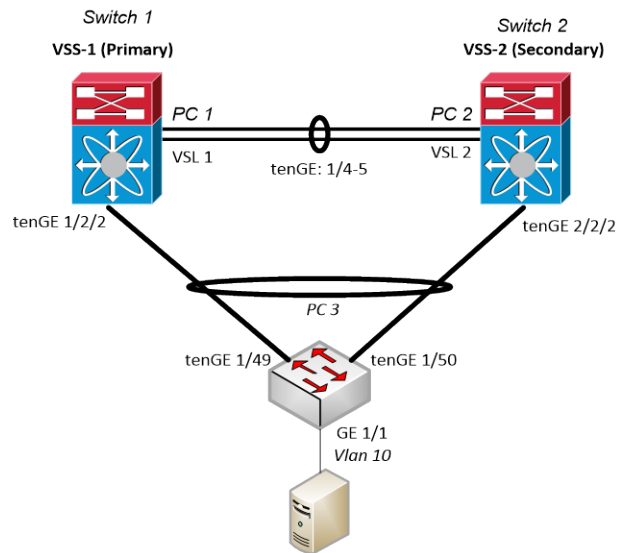


```
>>SW1<<
interface Vlan10
ip address 192.168.10.2 255.255.255.0
vrrp 1 ip 192.168.10.1
vrrp 1 priority 110
vrrp 1 preempt
```

```
>>SW2<<
interface Vlan10
ip address 192.168.10.3 255.255.255.0
vrrp 1 ip 192.168.10.1
vrrp 1 preempt
```

```
show vrrp
```


VSS



VSS

- **Step #1 for Primary VSS (SW1):**
- Create domain ID (100) that will be shared with all VSS switches
- SW1 will use the switch identity of "1" and will be our primary VSS switch (using priority 110). SW2 will be the Secondary VSS switch (using priority 100) in the cluster.
- Configure a Port Channel with 2 10GE interfaces connecting to the other VSS switch.

>> SW1 <<

switch virtual domain 100

switch 1

switch 1 priority 110

switch 2 priority 100

interface port-channel 1

switch virtual link 1

no shutdown

interface range tenGigabitEthernet 1/4 - 5

channel-group 1 mode on

no shutdown

- **Step #2 for Primary VSS (SW1):**
- Start the VSS conversion process on SW1
- At this time the switch will restart to merge the two switches configuration, renumber the interfaces from slot/port to switch-number/port/slot, and the negotiation of the active and standby roles through NSF/SSO

switch convert mode virtual

- **Step #3 for primary VSS (SW1):**
- Complete conversion process which will bring VSL configuration from the standby switch and populate it into the running config file.

switch accept mode virtual

- Port Channel (using ID 3) configuration to Access/Distribution switch
- 10GE ports 1/2/2 (from SW1) and 2/2/2 (from SW2) will be associated to the Port Channel

```
interface port-channel 3
description TO: AS01TRA
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

```
interface range tenGigabitEthernet 1/2/2, tenGigabitEthernet 2/2/2
switchport
channel-group 3 mode desirable
no shutdown
```

- Port Channel (using ID 4) configuration to a VMware ESXI host server connected off of the two VSS switches
- 10GE ports 1/3/2 (from SW1) and 2/3/2 (from SW2) will be associated to the Port Channel

```
interface port-channel 4
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

```
interface range GigabitEthernet 1/3/1, GigabitEthernet 2/3/1
switchport
channel-group 4 mode active
no shutdown
```

- Other VLAN and interface configuration completed on SW1 for all the VLANs that will be used and trunked down to the Access switch

```
vtp mode transparent
spanning-tree mode rapid-pvst
```

```
vlan 10
 name SF1
vlan 20
 name SF2
```

```
interface vlan10
ip address 192.168.10.1 255.255.255.0
no shutdown
```

```
interface vlan20
ip address 192.168.20.1 255.255.255.0
no shutdown
```

- *Step #1 for Secondary VSS (SW2):*
- Create domain ID (100) that will be shared with all VSS switches
- SW1 will use the switch identity of “2” and will be our Secondary VSS switch (using priority 100). SW1 will be the Primary VSS switch (using priority 110) in the cluster.
- Configure a Port Channel with 2 10GE interfaces connecting to the other VSS switch.

>> SW2 <<

```
switch virtual domain 100
switch 2
switch 1 priority 110
switch 2 priority 100
```

```
interface port-channel 2
switch virtual link 2
no shutdown
```

```
interface range tenGigabitEthernet 1/4 - 5
channel-group 2 mode on
no shutdown
```

- **Step #2 for Secondary VSS (SW2)**
- Start VSS conversion process on switch.
- At this time the switch will restart to merge the two switches configuration, renumber the interfaces from slot/port to switch-number/port/slot, and the negotiation of the active and standby roles through NSF/SSO. After the reboot is completed the console on the standby VSS switch will be disabled all further configuration is done on the primary VSS switch

```
switch convert mode virtual
```

- Configuration on access switch using a Port Channel (ID 3) connecting to the VSS switches.

```
>> AS01 <<
```

```
vtp mode transparent  
spanning-tree mode rapid-pvst
```

```
vlan 10  
name SF1  
vlan 20  
name SF2
```

```
interface port-channel 3  
switchport  
switchport trunk encapsulation dot1q  
switchport mode trunk  
no shutdown
```

```
interface range tenGigabitEthernet 1/49 - 50  
switchport  
channel-group 3 mode desirable  
no shutdown
```

```
interface GigabitEthernet 1/1  
switchport access vlan 10  
switchport mode access  
spanning-tree portfast
```

```
show etherchannel summary
```

VSS Monitoring Commands

```
show module switch 1
show module switch 2
show run switch 1
show run switch 2
show switch virtual
show switch virtual link
show switch virtual role
show vslp lmp summary
show vslp lmp neighbors
show vslp lmp counters
show vslp rrp summary
```

! confirm VLS connectivity between switch 2 on 10GE 2/1/4
ping vslp output interface tenGigabitEthernet 2/1/4

! reboots the active VSS switch (using switch ID 1)
redundancy reload shelf 1

Enhanced Fast Software Upgrade (eFSU)

- **Step #1**
- Make sure the new IOS image is copied to both the primary and secondary VSS switches flash memory specify boot variable for new image IOS image

```
boot system flash sup-bootdisk:new-image.bin
```

- Execute "issu loadversion" 1/1 & 2/1 is the VSS-switch/slot. If you are not sure what they are type in "show switch virtual redundancy". From that command look for something like "Switch X Slot Y Processor Information" Use X for the first number and Y for the second.
- Example: Switch 1 Slot 1 Processor Information would be 1/1 and Switch 2 Slot 1 Processor Information would be 2/1. That command will also show which VSS switch is ACTIVE and which one is STANDBY HOT

```
issu loadversion 1/1 sup-bootdisk:new-image 2/1 slavesup-bootdisk:new-image
```

- Secondary VSS switch will reload with new IOS image. VSS cluster will operate in 50% bandwidth capacity as the primary VSS is only running. This activity can be seen from the console.
- After the secondary VSS is booted up with the new IOS image verify the peer relationship between Supervisors are in a SSO state (Hot standby). The VSS cluster should now be operating at 100% bandwidth capacity

```
show switch virtual redundancy
```

- Verify current eFSU state, which should reflect "Load Version" next to ISSU

```
show issu state
```

- **Step #2**
- When secondary VSS is booted up completely run "issu runversion" command to cause the supervisor/chassis switchover, so the secondary VSS switch can be the active VSS switch while switch1 is being reloaded.
- Switchover will cause ~200msec traffic loss

```
issu runversion 2/1
```

! confirm redundancy state with switch1 (should be "sso")

```
show switch virtual redundancy
```

- **Step #3**
- If the new IOS image is good accept the new IOS version. If it is not accepted within the rollback timer, the eFSU software upgrade will terminate and go back to the older IOS image

issu acceptversion 2/1

show issu rollback-timer

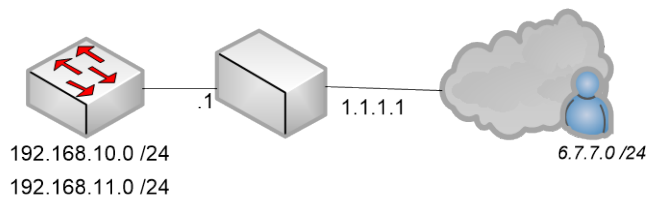
- **Step #4**
- Final step which will reload switch1 to run the new IOS image. At this point the VSS cluster will operate at 50% bandwidth capacity until switch1 comes back up

issu commitversion

[W]

WCCP

Solution/Services: Security
Related:



WCCP using ACLs for Security

- Configure WCCP for sending users transparently to a proxy server (enabled for WCCP)
- Hosts 192.168.10.23 and 10.74 on the LAN will bypass the proxy server
- All hosts on network 192.168.11.0 will be redirected to the proxy server
- All hosts on the network 192.168.10.0 for HTTP traffic will be redirected to the proxy server
- All hosts on the network 192.168.10.0 for HTTPS traffic will bypass the proxy server
- Any host on the LAN trying to access an outside server using the IP 6.7.7.10 will bypass the proxy server
- All other requests to the Internet should bypass the proxy for inspection

```
ip access-list extended wccp-acl
deny ip host 192.168.10.23 any
deny ip host 192.168.10.74 any
permit 192.168.11.0.0.0.255 any
permit tcp 192.168.10.0 0.0.0.255 any eq www
deny tcp 192.168.10.0 0.0.0.255 any eq 443
deny ip any host 6.7.7.10
deny ip any any
```

```
ip wccp 9 redirect-list wccp-acl
```



```
interface GigabitEthernet3/1
description TO: INTERNET
ip address 1.1.1.1 255.255.255.0
ip wccp 9 redirect out

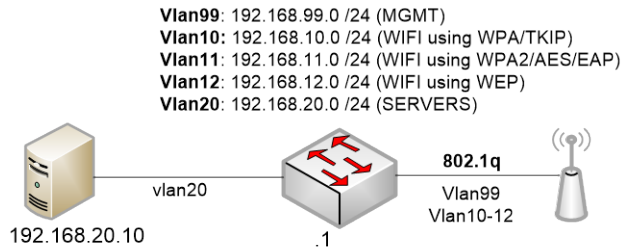
interface GigabitEthernet3/2
description TO: LAN
ip address 192.168.10.1 255.255.255.0
ip address 192.168.11.1 255.255.255.0 secondary
```

WCCP on Bluecoat Proxy Appliance

- Syntax for enabling WCCP on a Bluecoat proxy server
- Specify WCCP group ID as 9
- All permitted HTTP (TCP/80) and HTTPS (TCP/443) traffic send to this proxy server
- Build WCCP (GRE) tunnel with Internet Edge Router (192.168.10.1)

```
wccp enable
wccp version 2
service-group 9
forwarding-type GRE
priority 1
protocol 6
service-flags destination-ip-hash
service-flags ports-defined
ports 80 443 0 0 0 0 0 0
interface 0
home-router 192.168.10.1
```

WIRELESS



Base Configuration

- Base Configuration to apply initially on a standalone AP. Reference the network diagram picture above under "Wireless"
- Configure management network (192.168.99.0) that will use VLAN 99 and bridge group # 1.
- VLAN 99 will be the native VLAN (untagged)
- Enable Wireless radio for 802.11b and 802.11g

```
bridge 1 protocol ieee
```

```
interface BVI1
```

```
ip address 192.168.99.10 255.255.255.0
```

```
ip default-gateway 192.168.99.1
```

```
interface FastEthernet0
```

```
no shutdown
```

```
interface FastEthernet0.99
```

```
encapsulation dot1Q 99 native
```

```
no ip redirects
```

```
no ip unreachable
```

```
no ip proxy-arp
```

```
no ip route-cache
```

```
no cdp enable
```

```
bridge-group 1
```

```
no bridge-group 1 source-learning
```

```
bridge-group 1 spanning-disabled
```

```
interface Dot11Radio0
```

```
no shutdown
```

```
station-role root access-point
```

```
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
```

```
channel least-congested
```

WLAN using WPA/TKIP

- Configure Wireless network “private” for WPA using TKIP encryption. TKIP PSK will be “Cisco123”
- Wireless network “private” will exist in VLAN 10 based on the network diagram. Bridge group will be “10”
- Reference the network diagram picture above under “Wireless”

```
dot11 vlan-name private vlan 10
```

```
dot11 ssid private  
vlan 10  
authentication open  
authentication key-management wpa  
wpa-psk ascii Cisco123
```

```
bridge 10 protocol ieee
```

```
interface Dot11Radio0  
encryption vlan 10 mode ciphers tkip  
ssid private
```

```
interface Dot11Radio0.10  
encapsulation dot1Q 10  
no ip route-cache  
no cdp enable  
bridge-group 10  
bridge-group 10 subscriber-loop-control  
bridge-group 10 block-unknown-source  
no bridge-group 10 source-learning  
no bridge-group 10 unicast-flooding  
bridge-group 10 spanning-disabled
```

```
interface FastEthernet0.10  
encapsulation dot1Q 10  
no ip redirects  
no ip unreachable  
no ip proxy-arp  
no ip route-cache  
no cdp enable  
bridge-group 10  
no bridge-group 10 source-learning  
bridge-group 10 spanning-disabled
```

WLAN using WPA2/AES and EAP

- Configure Wireless network “private2” for WPA2 using AES encryption.
- Enable EAP 802.1X using RADIUS server 192.168.20.10 and the shared key is “Cisco123”
- Wireless network “private2” will exist in VLAN 11 based on the network diagram. Bridge group will be “11”
- Reference the network diagram picture above under “Wireless”

```
dot11 vlan-name private2 vlan 11
```

```
aaa group server radius RADIUS-EAP  
server 192.168.20.10 auth-port 1812 acct-port 1813
```

```
ip radius source-interface BVI1
```

```
radius-server host 192.168.20.10 auth-port 1812 acct-port 1813 key 7 Cisco123  
radius-server attribute 32 include-in-access-req format %h  
radius-server vsa send accounting
```

```
aaa authentication login ROUTEHUB-EAP group RADIUS-EAP
```

```
dot11 ssid private2  
vlan 11  
authentication open eap ROUTEHUB-EAP  
authentication key-management wpa
```

```
bridge 11 protocol ieee
```

```
interface Dot11Radio0  
encryption vlan 11 mode ciphers aes-ccm  
ssid private2
```

```
interface Dot11Radio0.11  
encapsulation dot1Q 11  
no ip route-cache  
no cdp enable  
bridge-group 11  
bridge-group 11 subscriber-loop-control  
bridge-group 11 block-unknown-source  
no bridge-group 11 source-learning  
no bridge-group 11 unicast-flooding  
bridge-group 11 spanning-disabled
```

```
interface FastEthernet0.11  
encapsulation dot1Q 11  
no ip redirects  
no ip unreachable  
no ip proxy-arp  
no ip route-cache  
no cdp enable  
bridge-group 11  
no bridge-group 11 source-learning  
bridge-group 11 spanning-disabled
```

WLAN using WEP

- Configure Wireless network “private-wep” using WEP (Open Authentication)
- WEP key will be: 12345678901234567890123456
- Wireless network “private-wep” will exist in VLAN 12 based on the network diagram. Bridge group will be “12”
- Reference the network diagram picture above under “Wireless”

```
dot11 vlan-name private-wep vlan 12
```

```
dot11 ssid private-wep  
vlan 12  
authentication open
```

```
bridge 12 protocol ieee
```

```
interface Dot11Radio0  
encryption vlan 12 key 1 size 128bit 12345678901234567890123456 transmit-key  
encryption vlan 12 mode wep mandatory  
ssid private-wep
```

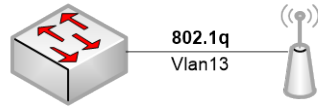
```
interface Dot11Radio0.12  
encapsulation dot1Q 12  
no ip route-cache  
no cdp enable  
bridge-group 12  
bridge-group 12 subscriber-loop-control  
bridge-group 12 block-unknown-source  
no bridge-group 12 source-learning  
no bridge-group 12 unicast-flooding  
bridge-group 12 spanning-disabled
```

```
interface FastEthernet0.12  
encapsulation dot1Q 12  
no ip redirects  
no ip unreachable  
no ip proxy-arp  
no ip route-cache  
no cdp enable  
bridge-group 12  
no bridge-group 12 source-learning  
bridge-group 12 spanning-disabled
```

EAP-FAST

- Configure Wireless network "rhg-eap-fast" for WPA/WPA2 using TKIP or AES encryption.
- Enable EAP 802.1X using a local RADIUS server 192.168.99.10 and the shared key is "Cisco123"
- Wireless network "rhg-eap-fast" will exist in VLAN 13 based on the network diagram.

Vlan13: 192.168.13.0 /24 (WIFI using EAP-FAST)



```
aaa-server
aaa-group server radius RHG-AAA-RADIUS
server-private 192.168.99.10 auth-port 1812 acct-port 1813
key 0 Cisco123

aaa authentication login eap RHG-AAA-EAP group RHG-AAA-RADIUS
aaa authorization exec default local
ip radius source-interface BVI1

radius-server local
nas 192.168.99.10 key 0 Cisco123
username user1 password Cisco123

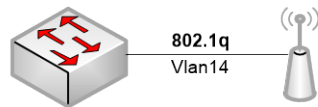
encryption vlan 13 mode ciphers aes-ccm tkip

dot11 ssid rhg-eap-fast
vlan 13
authentication open eap RHG-AAA-EAP
authentication key-management wpa
```

EAP-LEAP

- Configure Wireless network "rhg-eap-leap" for WPA/WPA2 using TKIP or AES encryption.
- Enable EAP 802.1X using a local RADIUS server 192.168.99.10 and the shared key is "Cisco123"
- Wireless network "rhg-eap-leap" will exist in VLAN 14 based on the network diagram.

Vlan14: 192.168.14.0 /24 (WIFI using EAP-LEAP)



```
aaa-server  
aaa-group server radius RHG-AAA-RADIUS  
server-private 192.168.99.10 auth-port 1812 acct-port 1813  
key 0 Cisco123
```

```
aaa authentication login eap RHG-AAA-EAP group RHG-AAA-RADIUS  
aaa authorization exec default local  
ip radius source-interface BVI1
```

```
radius-server local  
nas 192.168.99.10 key 0 Cisco123  
username user1 password Cisco123
```

```
encryption vlan 14 mode ciphers aes-ccm tkip
```

```
dot11 ssid rhg-eap-leap  
vlan 14  
authentication open eap RHG-AAA-EAP  
authentication network-eap RHG-AAA-EAP  
authentication key-management wpa
```

MAC Filtering

- Configure MAC Filtering with Wireless network
- Allow Wireless client with MAC address 0013.ce00.6c98 to associate with Wireless network "RHG-WPA"

```
username 0013ce006c98 password 0013ce006c98
username 0013ce006c98 autocommand exit
```

```
aaa authentication login RHG-MAC-AUTH local
```

```
interface Dot11Radio0
no ip address
```

```
ssid RHG-WPA
vlan 10
authentication open mac-address RHG-MAC-AUTH
```

LAN Switch Port for Standalone AP

- LAN switch port configuration for a connected standalone AP based on the network diagram
- Allow and tag VLANs 99,10,11, and 12
- Untagged Native (native VLAN) will be VLAN 99 ; used for managing the AP
- Reference the network diagram picture above under "Wireless"

```
interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport trunk allowed vlan 99,10-12
switchport mode trunk
```


Broadcast Multiple SSID

- Enable Wireless networks PRIVATE and PRIVATE2 to broadcast its SSID for clients to connect to it.

```
dot11 ssid private
vlan 10
authentication open
authentication key-management wpa
mbssid guest-mode
```

```
dot11 ssid private2
vlan 11
authentication open eap ROUTEHUB-EAP
authentication key-management wpa
mbssid guest-mode
```

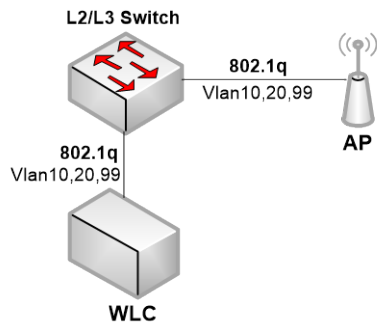
```
interface Dot11Radio0
no ip address
ssid private
ssid private2
mbssid
```

Cisco IOS Wireless Monitoring Commands

```
show dot11 associations
show dot11 network-map
show dot11 statistics client-traffic
show dot11 associations <mac-address>
```

Cisco Switch Ports for Cisco WLAN Controllers & APs

- FE0/2 connected to the Cisco WLC. FE0/3 connected to the Lightweight AP
- Corporate/Private Wireless exist in VLAN 10. Guest wireless exist in VLAN 20.
- Management network exist in VLAN 99
- DHCP enabled on WLC for VLAN 99 used for AP address assignment



```
vlan 10
name RHG-VLAN-WLAN-PROD
```

```
vlan 20
name RHG-VLAN-WLAN-GUEST
```

```
vlan 99
name RHG-VLAN-WLAN-MGMT
```

>> WLC switch port

```
interface FastEthernet0/2
description TO: rhg-wlc01-sj-ca ; WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,99
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk
```

>> Lightweight AP port

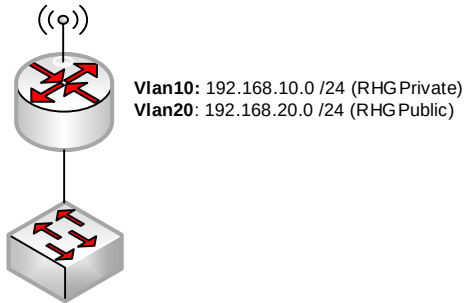
```
interface FastEthernet0/3
description rhg-ap03-sj-ca
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,99
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk
```

Wireless on Cisco ISR WIFI Models (Cisco 871W)

- Wireless configuration on Cisco ISR 871W router
- Private network will be 192.168.10.0 (VLAN 10) ; SSID: RHGPrivate
- Public/Guest network will be 192.168.20.0 (VLAN 20) ; ; SSID: RHGPublic

Cisco ISR WFI Model

(e.g. Cisco 800W)



```
bridge 10 protocol ieee
bridge 20 protocol ieee
```

```
bridge irb
```

```
bridge 10 route ip
bridge 20 route ip
```

```
interface Vlan10
description VLAN: Private network
no ip address
bridge-group 10
bridge-group 10 spanning-disabled
```

```
interface Vlan20
description VLAN: Public network
no ip address
bridge-group 20
bridge-group 20 spanning-disabled
```

```
interface BVI10
description Private network
ip address 192.168.10.1 255.255.255.0
```

```
interface BVI20
description Public network
ip address 192.168.20.1 255.255.255.0
```

```
interface Dot11Radio0
no ip address
no shutdown
encryption vlan 10 mode ciphers tkip
encryption vlan 20 mode ciphers tkip
```

```
ssid RHGPrivate
vlan 10
authentication open
authentication key-management wpa
guest-mode
wpa-psk ascii CiscoPrivate
```

```
ssid RHGPublic
vlan 20
authentication open
authentication key-management wpa
guest-mode
wpa-psk ascii CiscoPublic
```

```
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
```

```
interface Dot11Radio0.10
encapsulation dot1Q 10
no snmp trap link-status
no cdp enable
bridge-group 10
bridge-group 10 subscriber-loop-control
bridge-group 10 spanning-disabled
bridge-group 10 block-unknown-source
no bridge-group 10 source-learning
no bridge-group 10 unicast-flooding
```

```
interface Dot11Radio0.20
encapsulation dot1Q 20
no snmp trap link-status
no cdp enable
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
```

Clearing a DHCP Lease on a Cisco WLC

- Syntax for clearing a DHCP lease on the WLC

```
(WiSM-slot2-2) >config dhcp clear-lease ?  
  <IP Address>  Enter the IP address.  
  all           Clear all Leases.
```

QoS on Wireless Access Point

- Recommended QoS configuration for voice traffic on Wireless Access Point

```
class-map match-all voice-rtp  
  match ip dscp ef
```

```
policy-map ap-downstream  
  class voice-rtp  
    set cos 6
```

```
interface dot11radio0  
  traffic-class best-effort cw-min 5 cw-max 8 fixed-slot 2  
  traffic-class background cw-min 9 cw-max 10 fixed-slot 6  
  service-policy output ap-downstream
```

WRED

Solution/Services: QoS: Queuing and Dropping

Related:

Go to [“QoS: Queuing and Dropping”](#)

[0-9]

802.1X

Solution/Services: Security
Related:

802.1x

- Enable 802.1X on switch and interface GE0/4
- 802.1X user authentication will use RADIUS server 192.168.10.10 (shared key=cisco123)
- If the host connected to port GE0/4 is not enabled for 802.1X place port into VLAN 900

```
aaa new-model
aaa group server radius ACS-RADIUS
server 192.168.10.10 auth-port 1812 acct-port 1813
```

```
aaa authentication dot1x default group ACS-RADIUS
aaa authorization network default group ACS-RADIUS
```

```
ip radius source-interface Vlan100
radius-server host 192.168.10.10 auth-port 1812 acct-port 1813 key cisco6778
```

```
dot1x system-auth-control
```

```
interface GigabitEthernet0/4
switchport access vlan 100
switchport trunk native vlan 100
switchport mode access
dot1x port-control auto
dot1x reauthentication
dot1x guest-vlan 900
```