

Troubleshooting Network Issues



Jacob Petrie
Network Administrator

@pwsh1996



Overview

Diagnosing Network Services

Understanding Latency and Bandwidth Issues

Protocol Problems

Troubleshoot Routing in Cloud Networks

Identifying Network Switching Problems

Finding Issues with IP Addressing



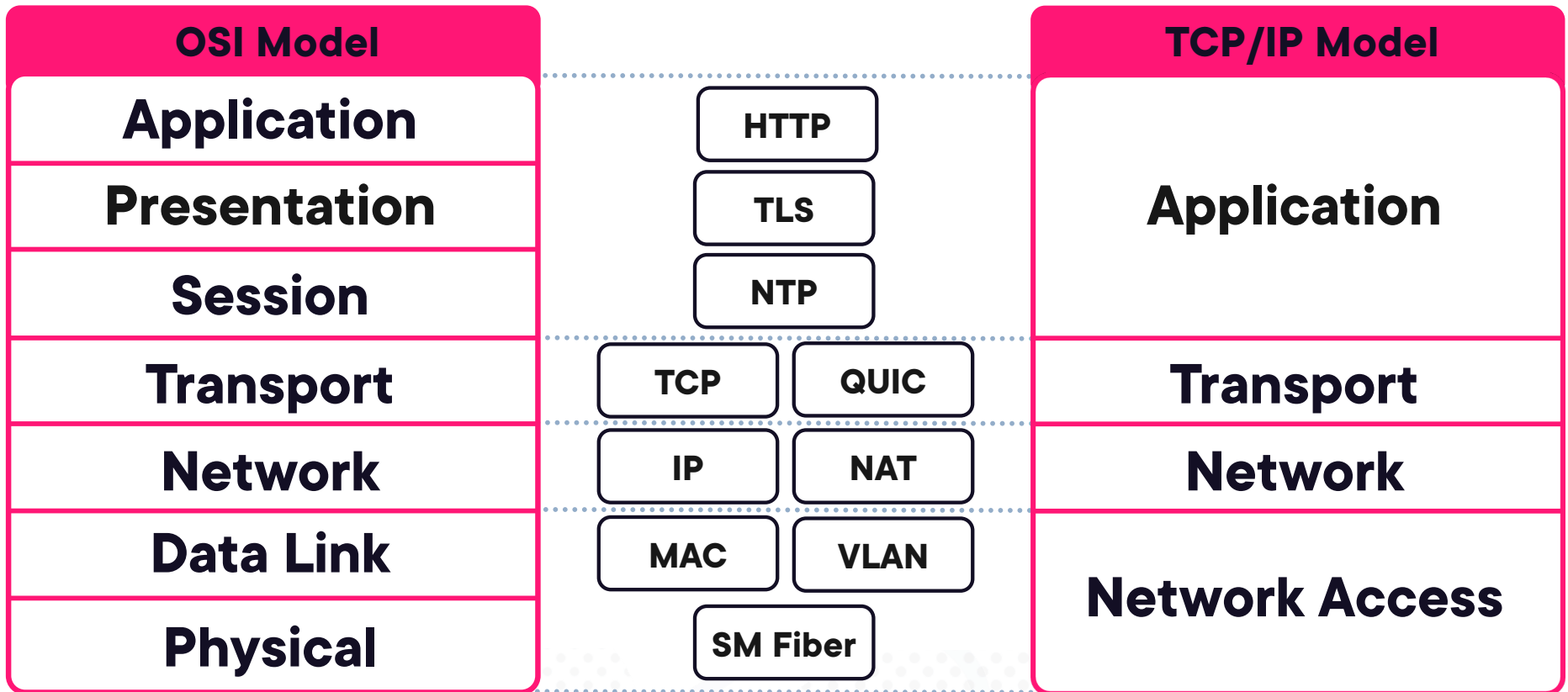


CompTIA Cloud+

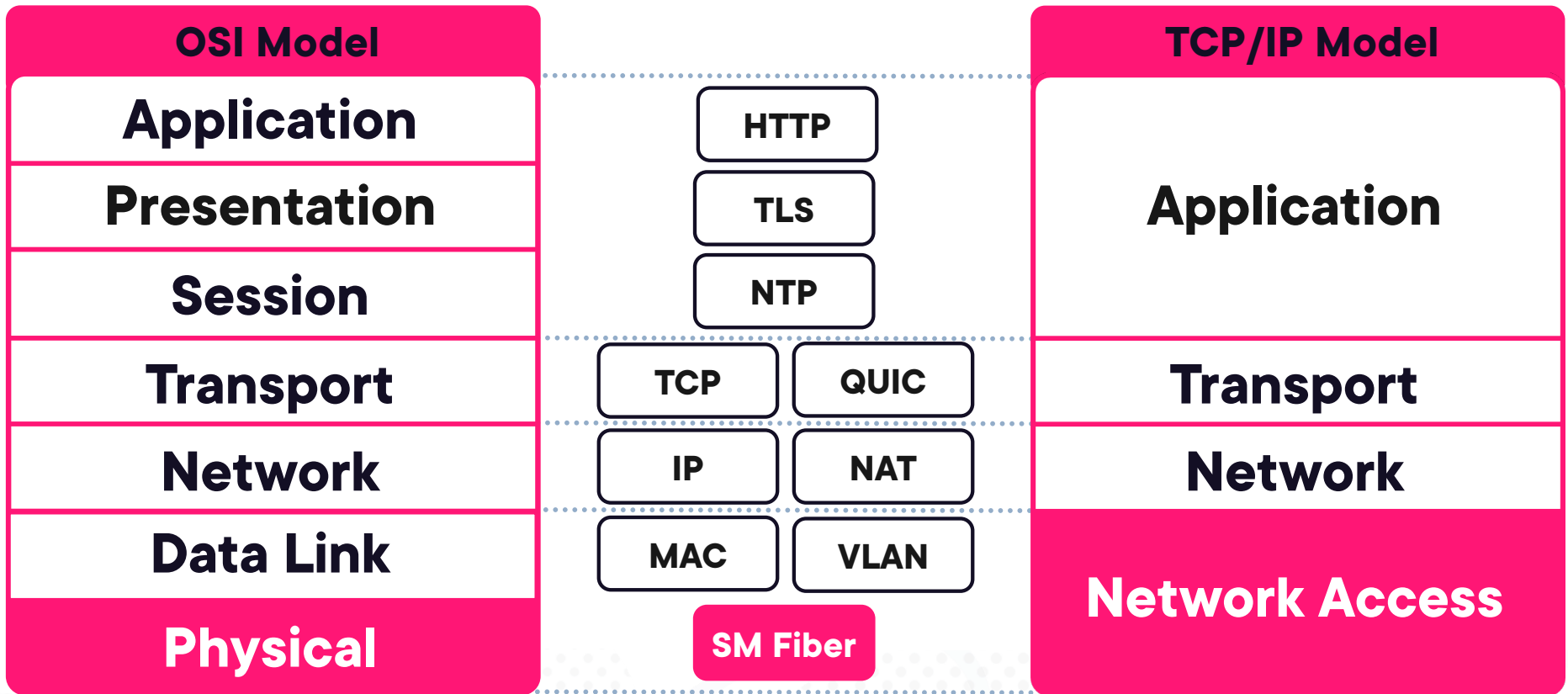
Given a scenario, troubleshoot network issues.



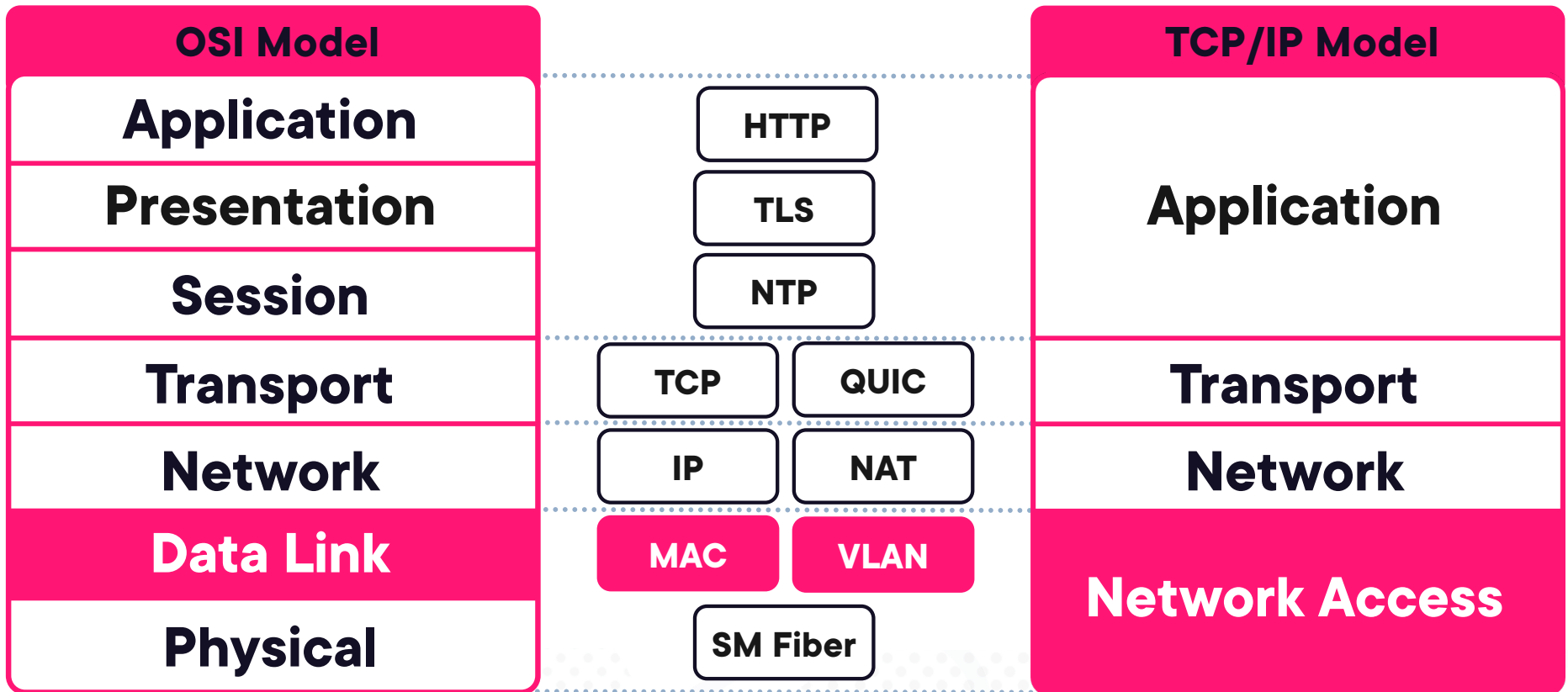
Network Layers



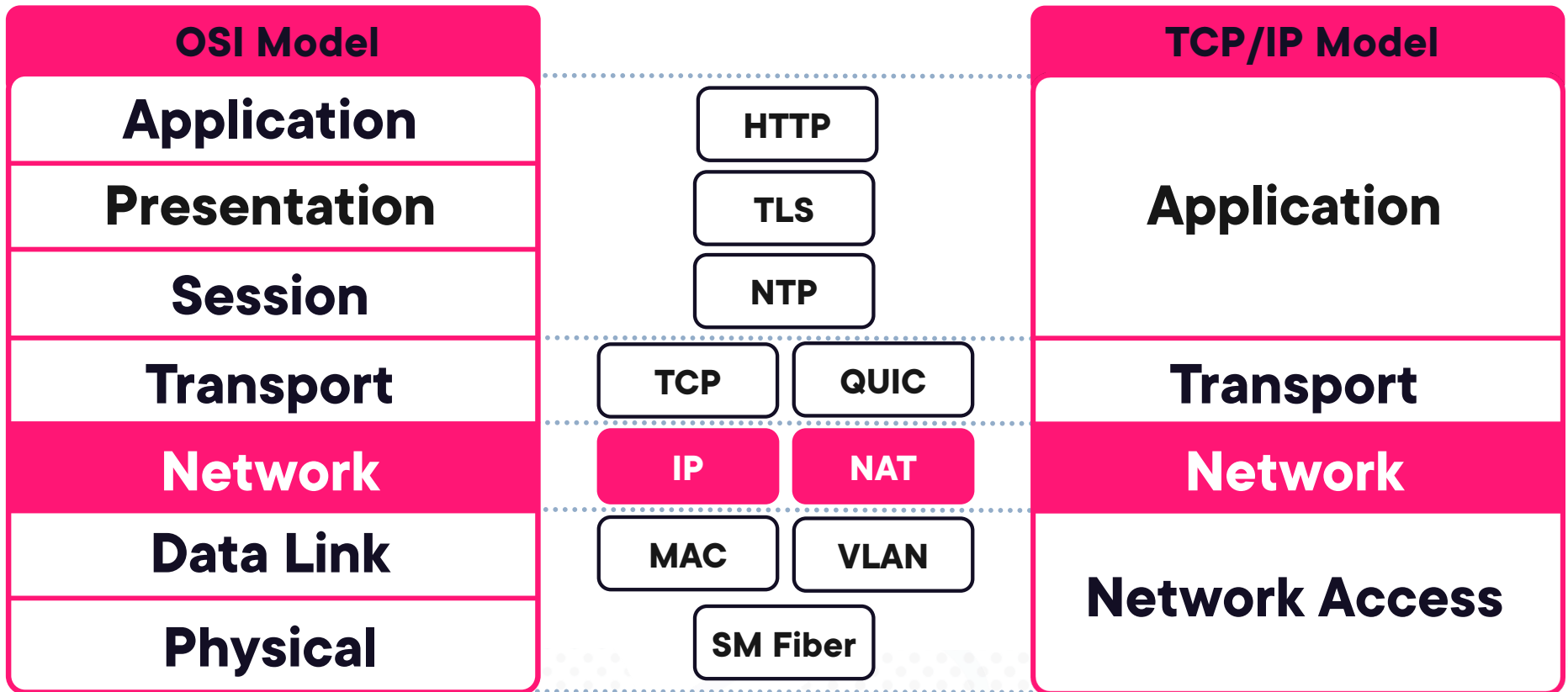
Network Layers



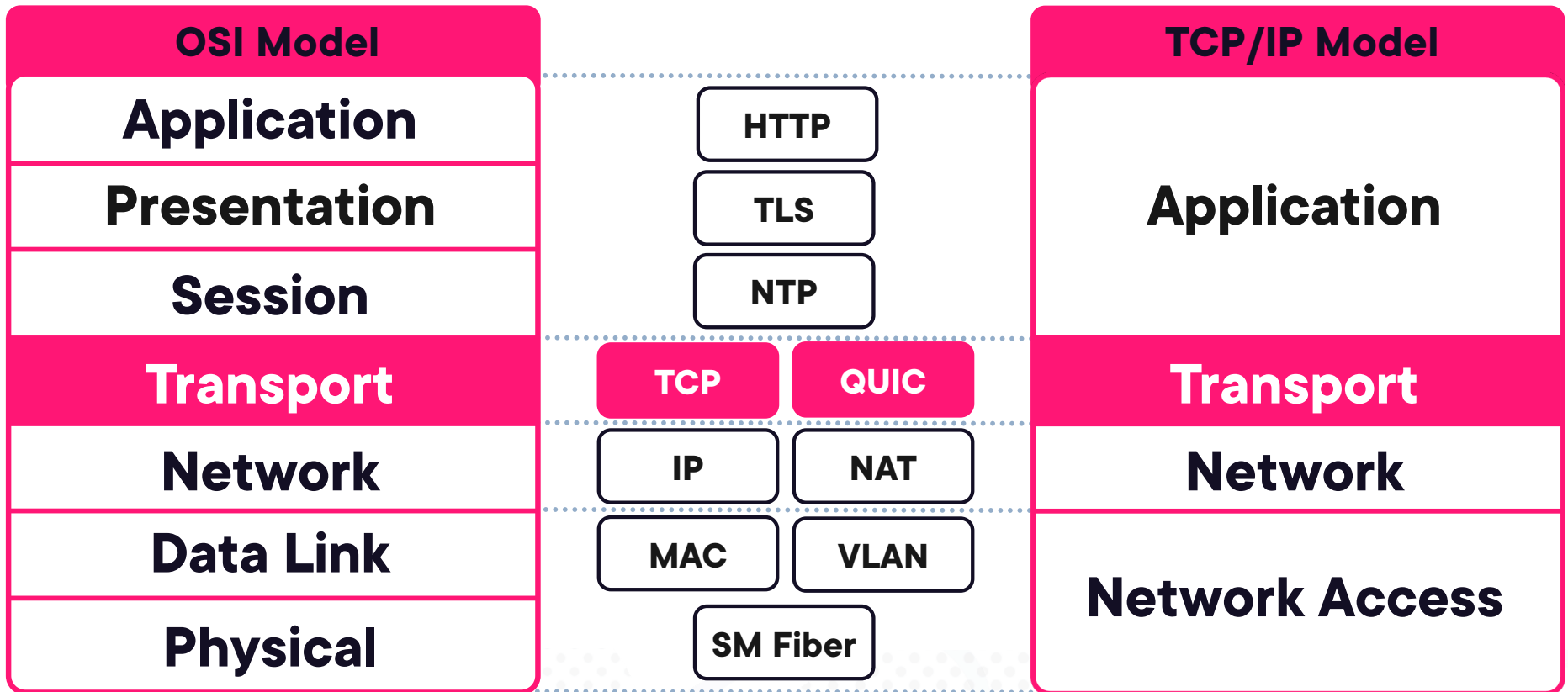
Network Layers



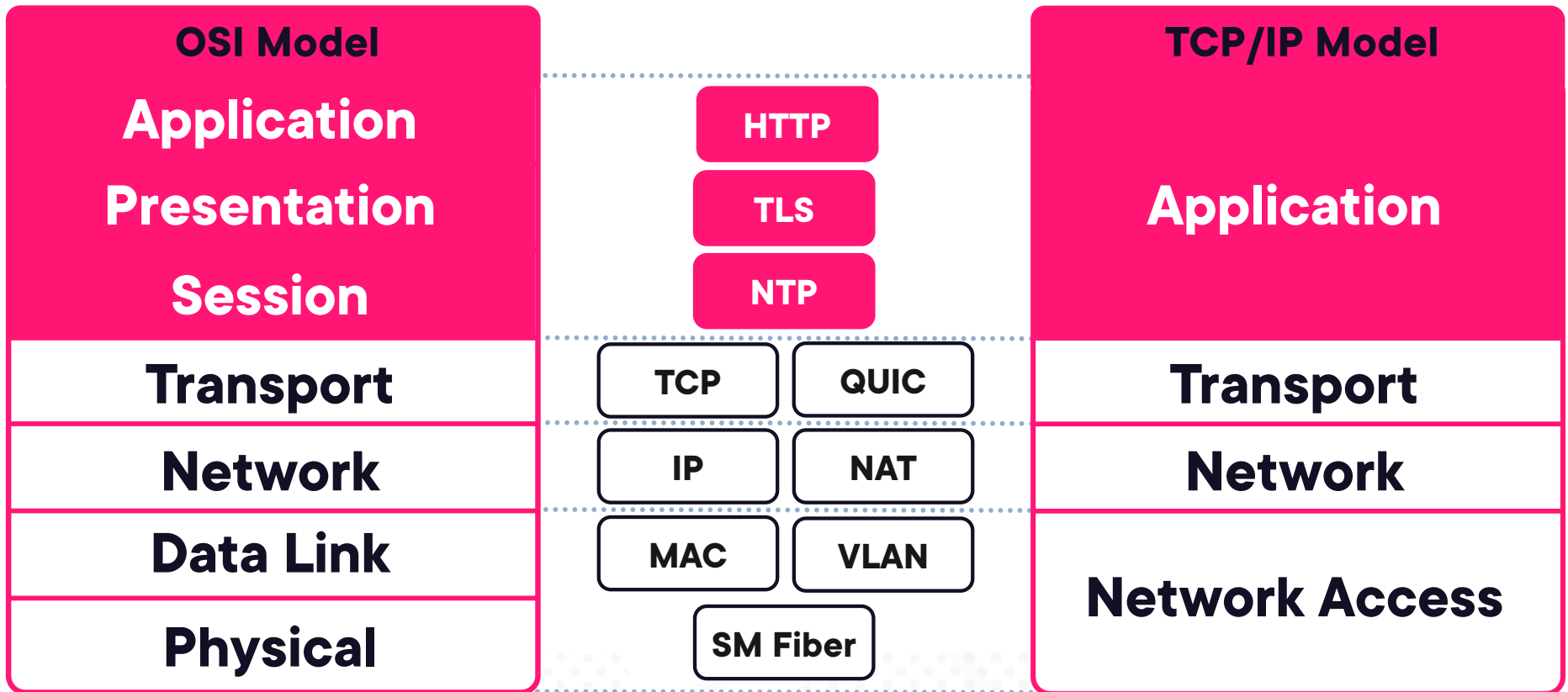
Network Layers



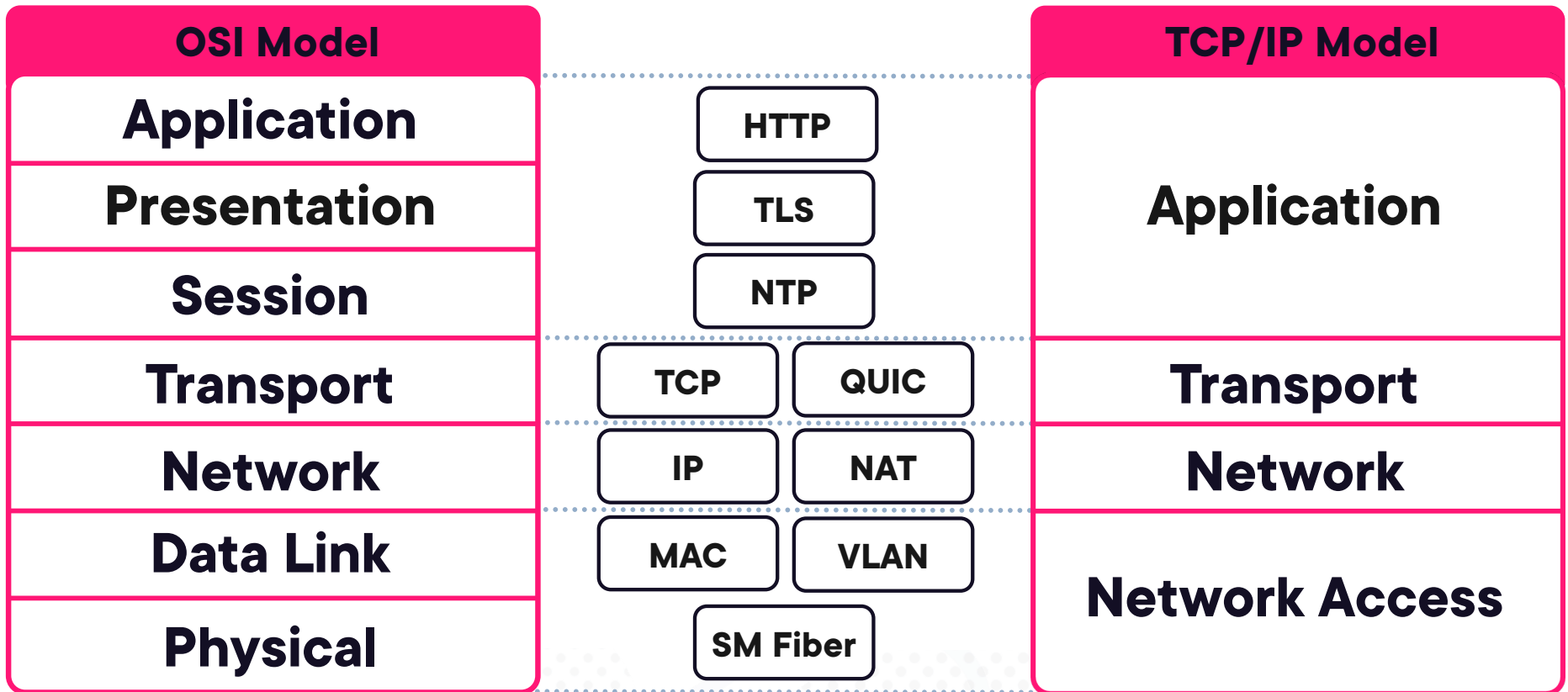
Network Layers



Network Layers



Network Layers





Diagnosing Network Services

Some Common Network Services



Dynamic host control protocol (DHCP)



Domain name service (DNS)



Network time protocol (NTP)



Network address translation (NAT)



Hypertext transport protocol (HTTP)



DHCP Issues



DHCP dynamically hands out IP addresses in response to layer 2 broadcasts

Unavailability of DHCP can cause resources to lose network connectivity

DHCP not only hands out IP addresses but has options for DNS, Syslog, PXE Boot, and more



```
network:
  version: 2
  ethernets:
    all-en:
      match:
        name: en*
      dhcp4: true
      dhcp4-overrides:
        use-domains: true
      dhcp6: true
      dhcp6-overrides:
        use-domains: true
    all-eth:
      match:
        name: eth*
      dhcp4: true
      dhcp4-overrides:
        use-domains: true
      dhcp6: true
      dhcp6-overrides:
        use-domains: true
```

◀ /etc/netplan/90-default.yaml

◀ Matching predictable network interface names like ens4 or enp0s4

◀ Setting DHCP for IPv4 to True

◀ Setting DHCP for IPv6 to True

◀ Matching legacy network interfaces names like eth0

◀ These are telling it to use the “Option 15 Domain Name” the DHCP server is giving out as a search domain



DHCP Troubleshooting Pointers

Scan network for rogue DHCP servers, packet capture tools can help identify them

Ensure DHCP relay is configured on routers if the DHCP server and clients are on different networks

Shorter leases can help prevent IP exhaustion in high-turnover environments

Configure DHCP exclusions to avoid conflicts with statically assigned IP addresses

DNS Issues



DNS is usually used over IP Addresses as they can be dynamically changed

DNS issues can disrupt connectivity

Tools like dig and nslookup can be used to check records on a DNS server



Common DNS Records



A Record – Points to an IPv4 address



AAAA Record – Points to an IPv6 address



CNAME Record – Points to another DNS name, like an Alias



MX Record – Points to an email server



TXT Record – Stores information for auth, domain verification, etc.

DNS Troubleshooting Tips

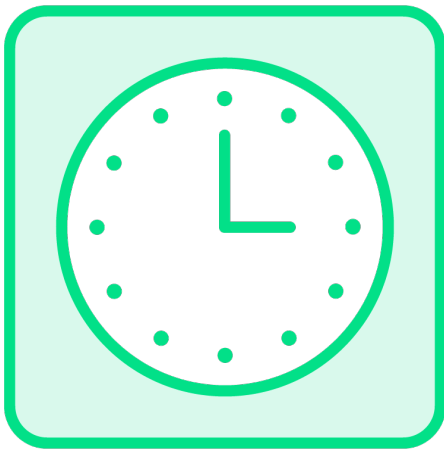
If you can connect via IP address but not DNS name, it's a problem with DNS

Verify you are using the correct server, and use tools to check other DNS servers

If the problem is related to a recent change in DNS check the Time To Live (TTL) in the cache

Check the local hosts file

NTP Issues



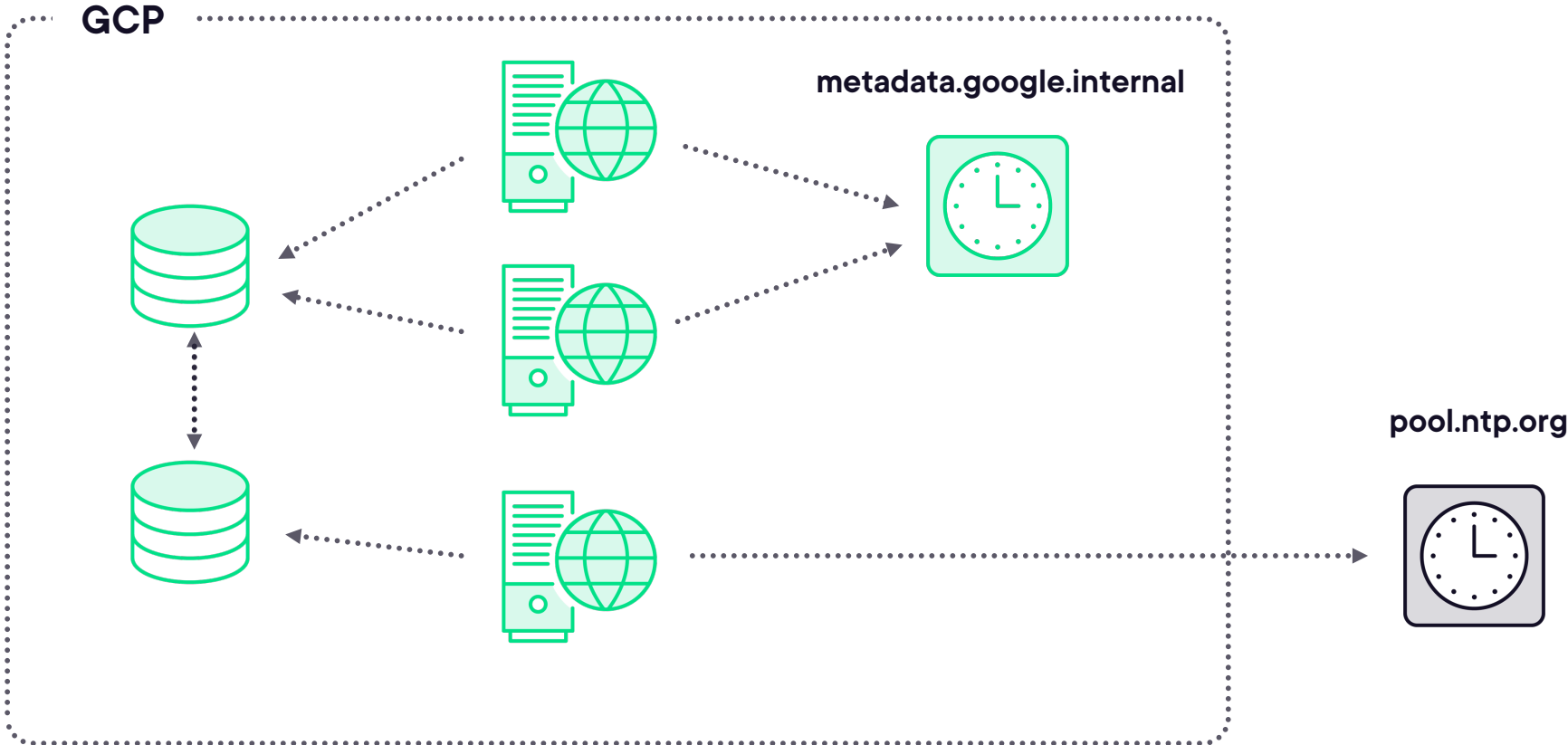
Correct time synchronization is important for time series databases

Reading logs from multiple systems is challenging when time is off

Read cloud provider documentation for NTP settings



NTP Issues



NTP Tips and Tricks

Use templates and infrastructure as Code (IaC) to keep settings from changing

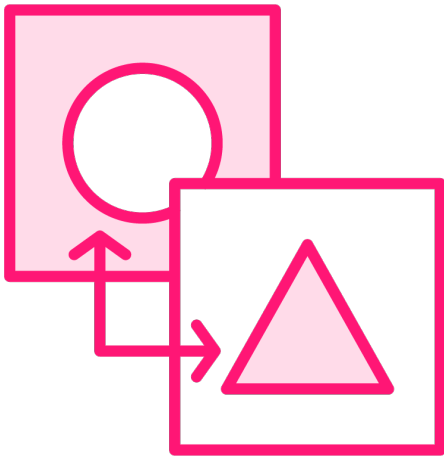
Internal cloud NTP servers usually have lower latency

Avoid mixing “Time Smearing” NTP servers with ones that don’t smear leap seconds

Monitor time synchronization and clock drift



NAT Issues



NAT is used when you need hosts on private IP addresses to communicate with the Internet

Types of NAT:

- Source NAT (inside network to outside)
- Destination Nat (outside to inside)
- Port Address Translation

Issues with NAT can cause systems to not communicate with the outside or vice versa



Help for NAT Implementations

Checking the logs on the firewall or NAT gateway to see what is happening with the traffic

Commands like Netcat and Test-NetConnection can help test if traffic on a port is going through

NAT reflection allows internal IPs to access internal resources using the external IP addresses

NAT can also be used to sit between two internal networks



HTTP Issues



HTTP issues affect more than just website availability

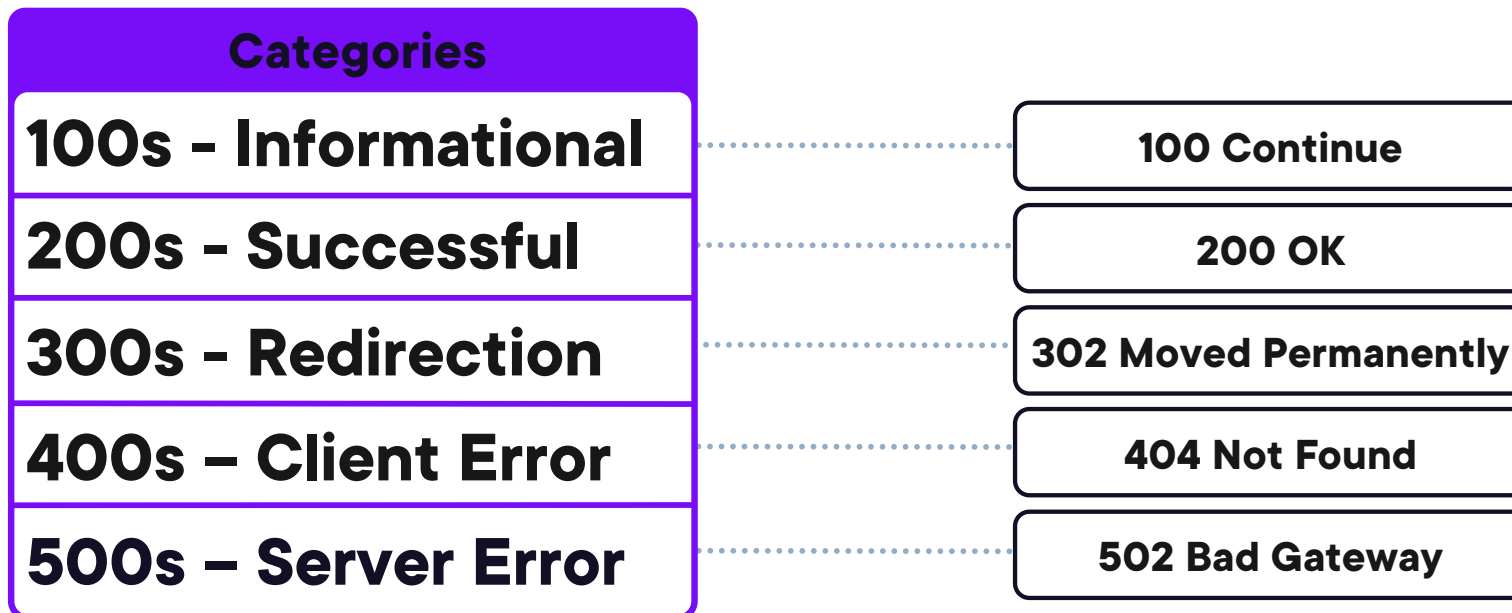
Issues can also be with APIs and other services that use HTTP

Use tools like curl and Invoke-WebRequest to read HTTP responses

Reading and interpreting the status codes



HTTP Status Codes



Common HTTP Issues and Troubleshooting Steps

429 – Too Many Requests

Check the Retry-After header, so you know how long to wait

404 Not Found

Check that the URL is correct and that it hasn't changed

500 Internal Server Error

Check the server logs for an error or check the status page

403 Forbidden

Means you're missing the necessary permissions





More Information

Network Troubleshooting and Tools

Ross Bagurdes



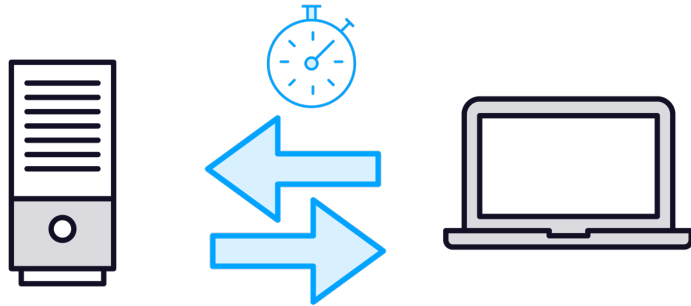


Understanding Latency and Bandwidth Issues

Latency and Bandwidth Comparison

Latency

Delay between sending and receiving

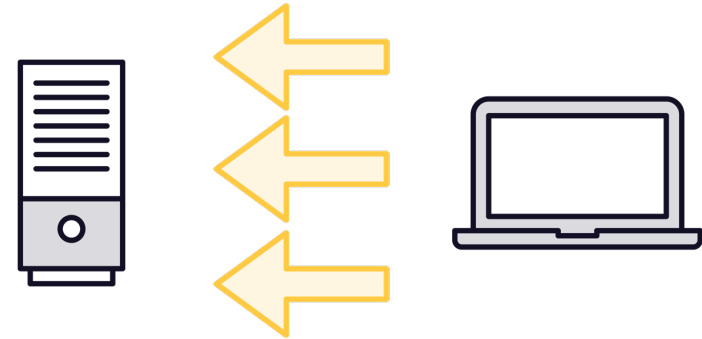


Tools: ping and traceroute(tracert)

VS.

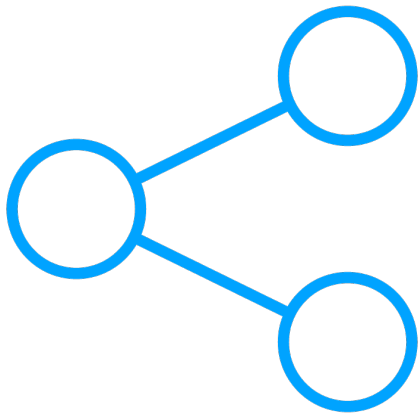
Bandwidth

Amount of data that can be transferred in a given amount of time



Tools: iperf

Latency



The farther a resource, the higher the latency

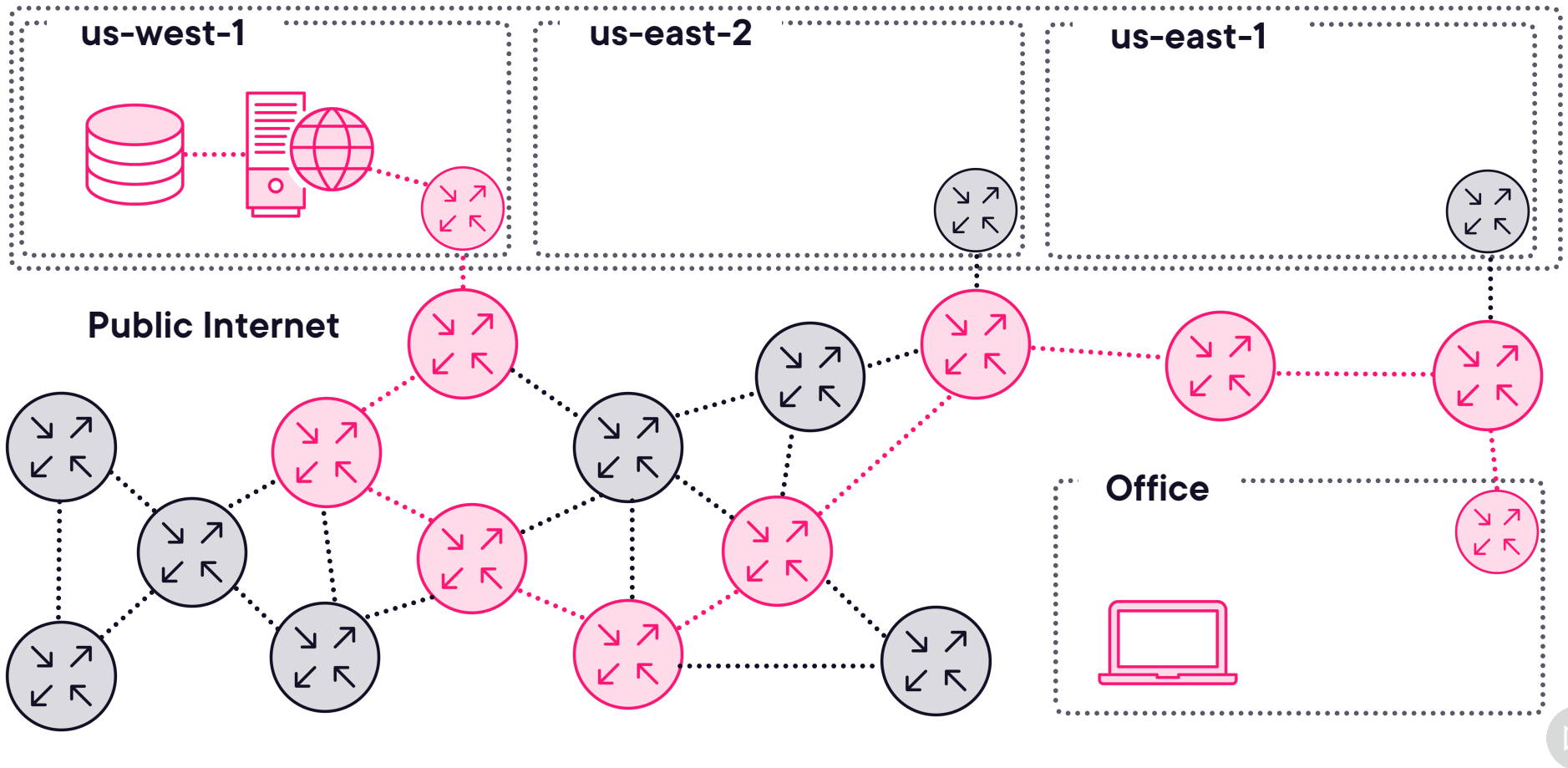
Moving resources closer to the end users can solve many latency issues

Use templates and scripts to build new resources, allowing only certain regions

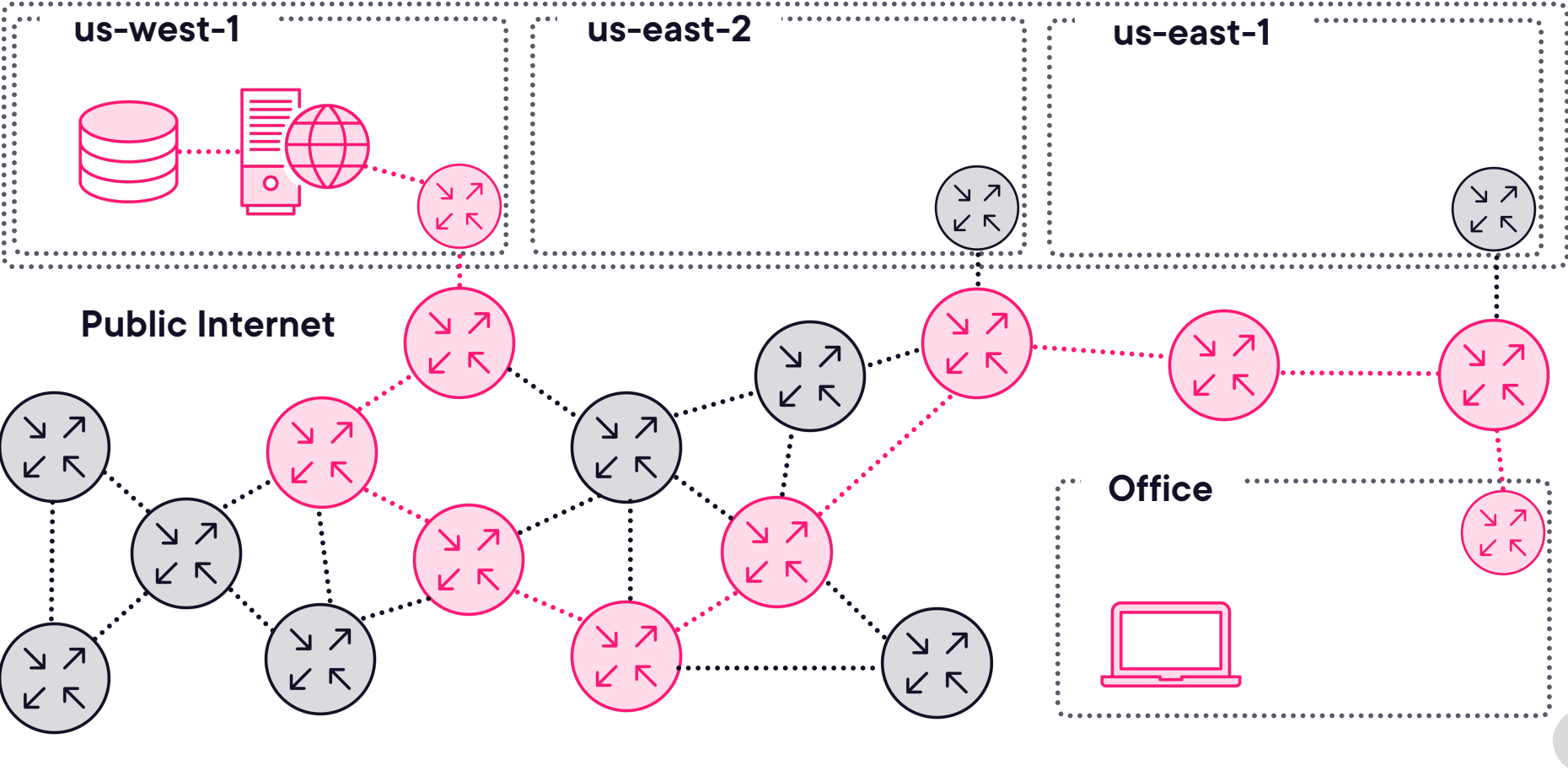
Tools like ping to see basic latency or tracert to see how many hops between the resources



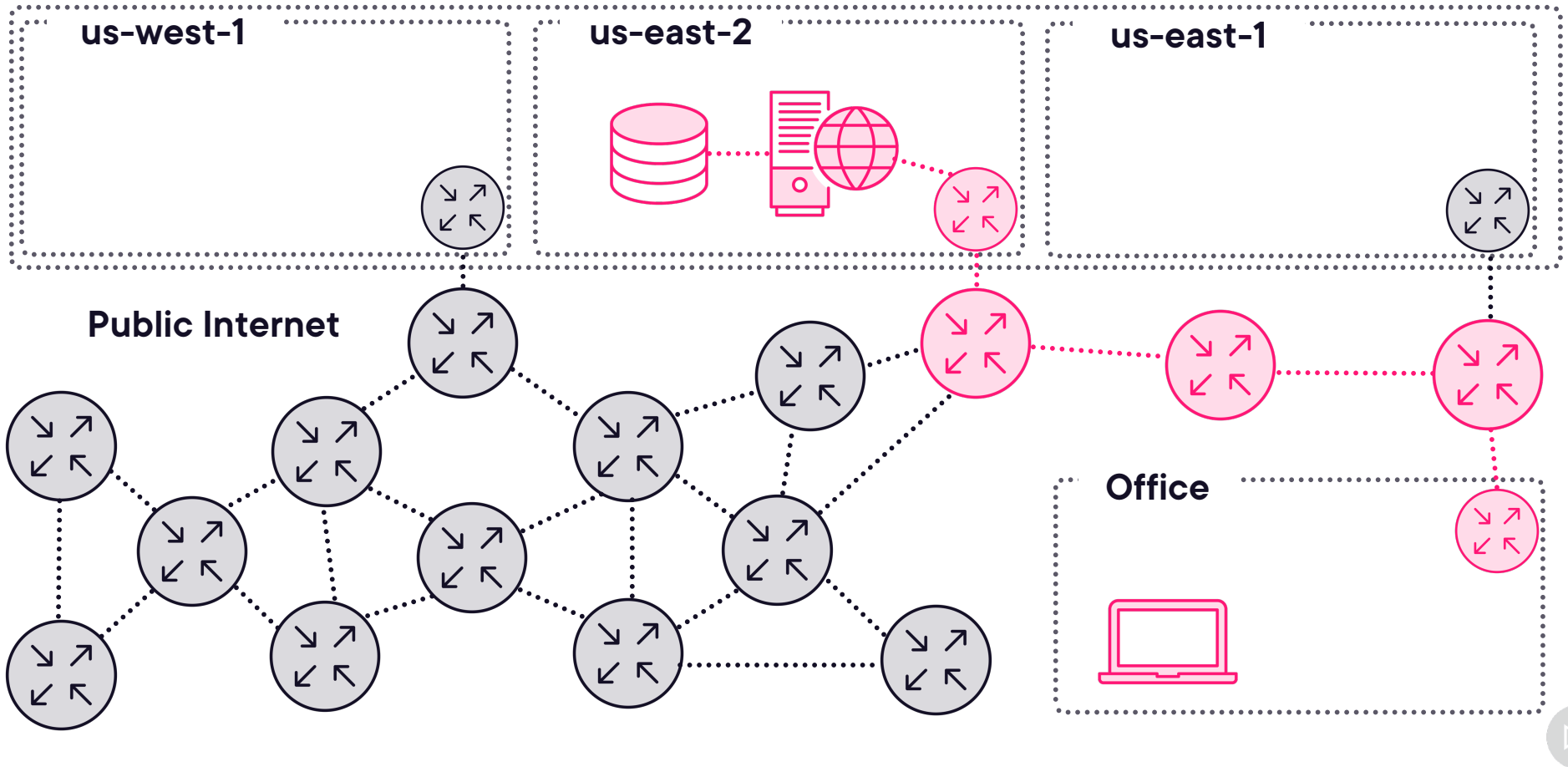
Latency Issues



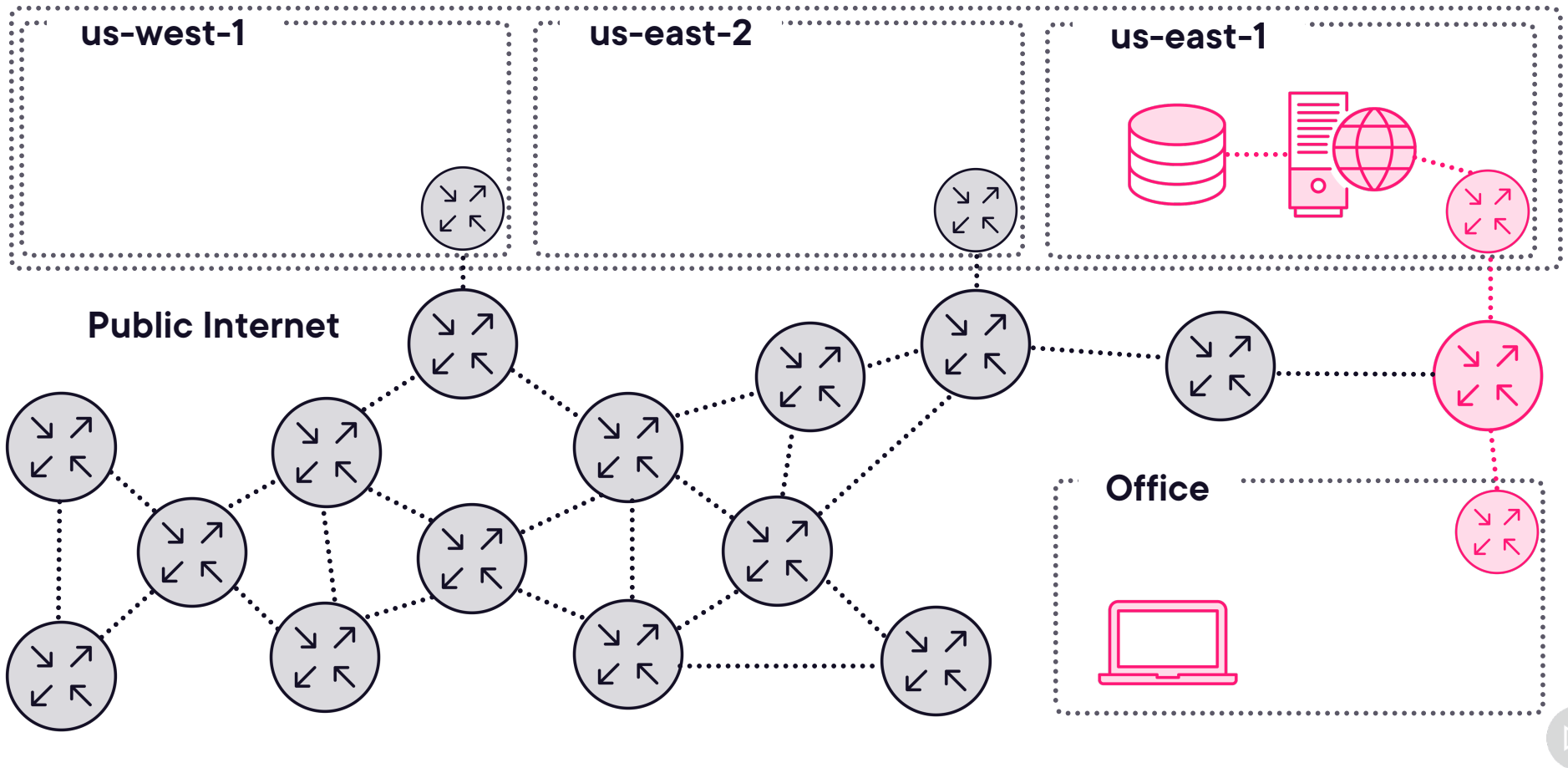
Latency Issues



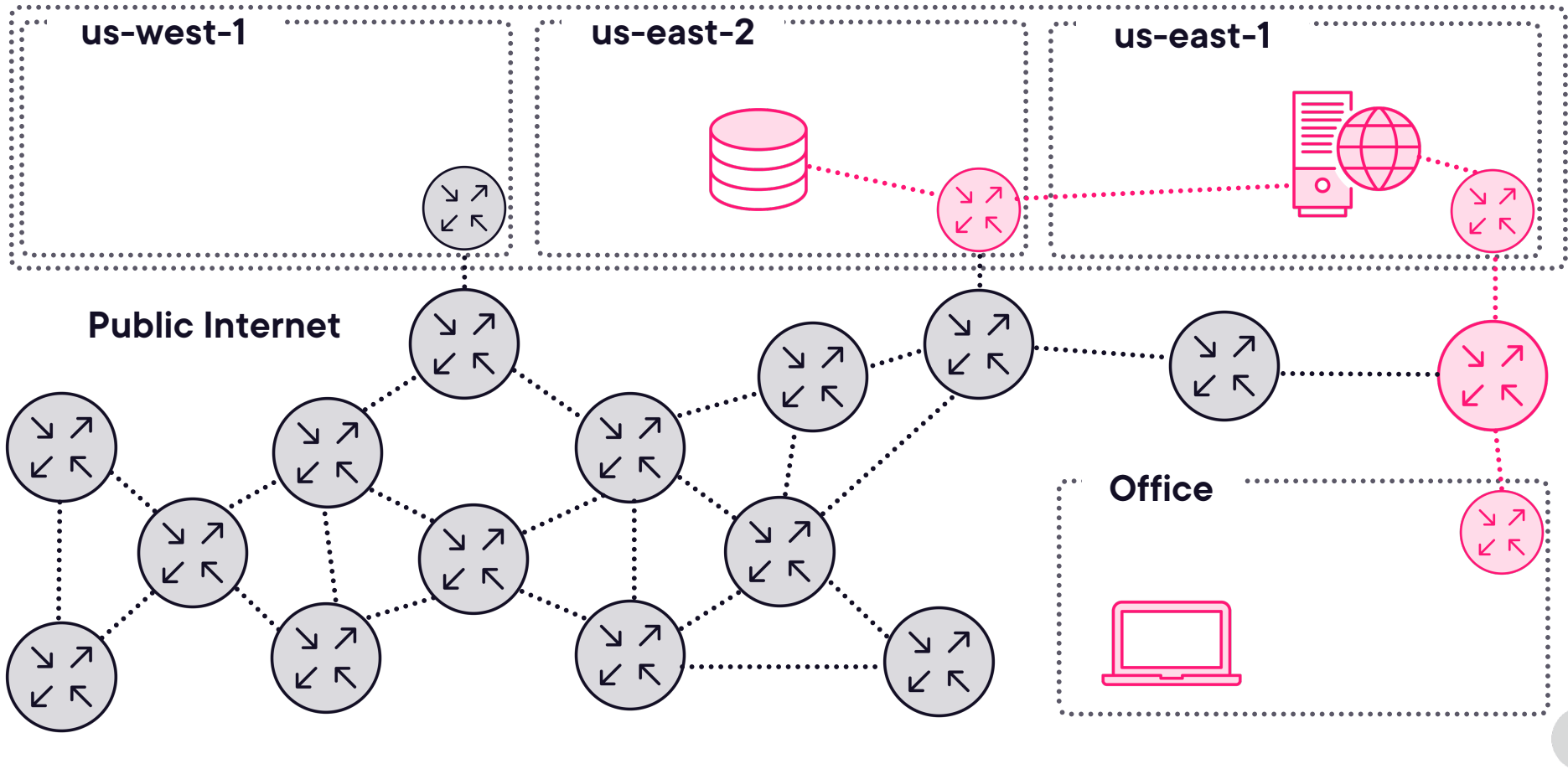
Latency Issues



Latency Issues



Resources Deployed in Separate Regions



Tools to Fix Bandwidth and Latency Issues



Content Delivery Networks (CDN) allow users to pull static resources from locations close by

Edge compute using serverless functions at the edge

Scaling horizontally allows for better bandwidth sharing



Content Delivery Network (CDN)

The screenshot shows the Cloudflare website's 'network' page. The header includes the Cloudflare logo, navigation links (Solutions, Products, Pricing, Resources, Partners, Why Cloudflare), and utility links (Sales: +1 (888) 99 FLARE, Support, Sign up, Contact sales, Log in). The main content area features a world map with blue dots representing data centers. Text on the left describes the network as one of the fastest on the planet, reaching 95% of the world's population within 50ms. Below the map are four key statistics: 330 cities in 120+ countries, 12,500 direct network connections, 296 Tbps of edge capacity, and ~50ms reach to 95% of the world's population.

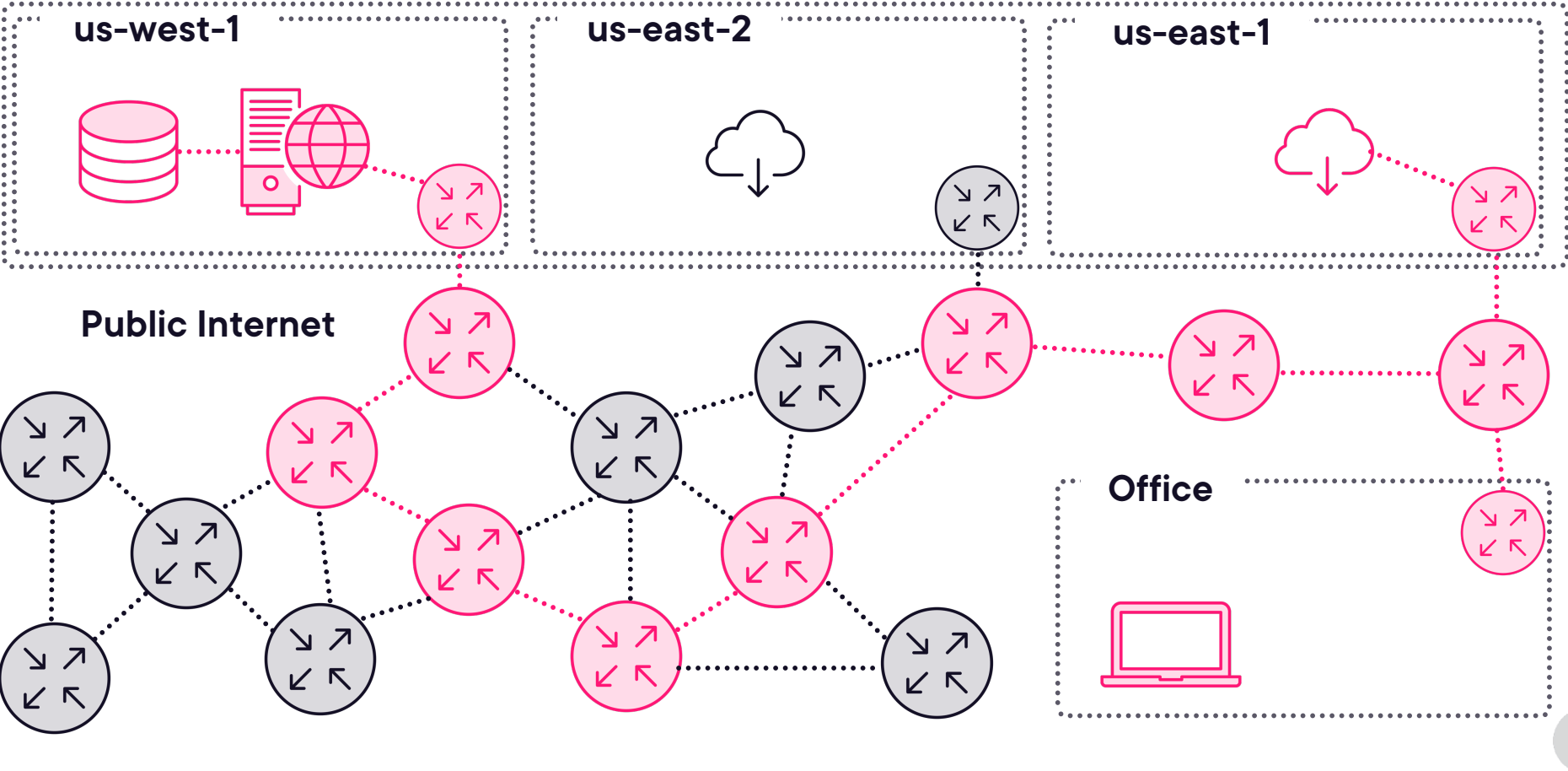
The Cloudflare global network

Our vast global network, which is one of the fastest on the planet, is trusted by millions of web properties.

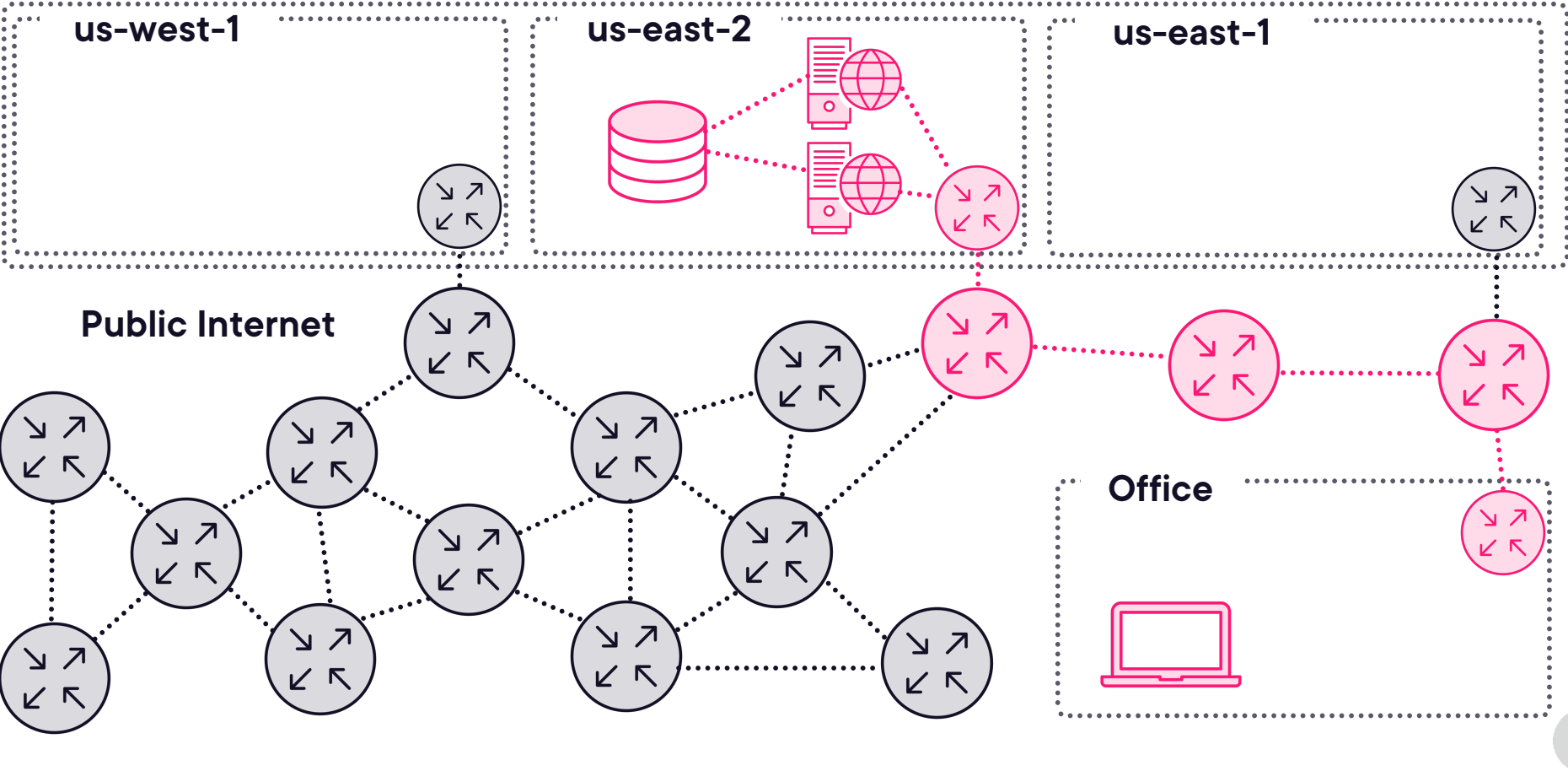
With direct connections to nearly every service provider and cloud provider, the Cloudflare network can reach about 95% of the world's population within approximately 50 ms.

330 cities in 120+ countries, including mainland China	12,500 networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise	296 Tbps global network edge capacity, consisting of transit connections, peering and private network interconnects	~50 ms from about 95% of the world's Internet-connected population
--	---	---	--

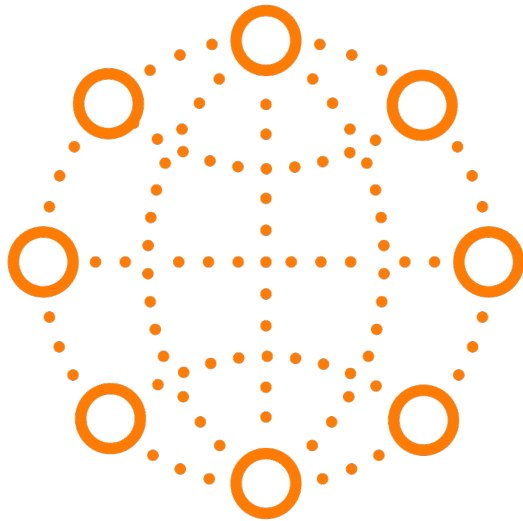
Content Delivery Network (CDN)



Scaling Horizontally



Global Traffic Management



Routes traffic using cloud provider's private network instead of public internet

Can be used for global load balancing

Examples of this type of service

- AWS Global Accelerator
- Azure Front Door
- Google Premium Network Tier



Global Traffic Management

```
C:\Program Files\PowerShell\7\pwsh.exe x + v
PS C:\> # GCP Compute Engine with Standard Tier Network
PS C:\> tracert 34.1.44.129

Tracing route to 129.44.1.34.bc.googleusercontent.com [34.1.44.129]
over a maximum of 30 hops:

  1  1 ms  1 ms  1 ms  192.168.100.99
  2  4 ms  4 ms  3 ms  gw3-v4001.gatewayfiber.net [150.195.175.254]
  3  5 ms  3 ms  5 ms  e0-60.core1.stl1.he.net [184.105.11.82]
  4  11 ms 10 ms 12 ms 100ge0-34.core2.bna1.he.net [184.104.198.13]
  5  *      *      *      Request timed out.
  6  31 ms *      31 ms port-channel3.core2.orf2.he.net [184.104.198.18]
  7  *      96 ms *      port-channel4.core1.bio1.he.net [184.104.197.93]
  8  106 ms *      *      port-channel4.core4.mrs1.he.net [184.105.81.30]
  9  *      *      112 ms port-channel6.core2.mil2.he.net [184.105.80.13]
 10 112 ms 112 ms 112 ms google.topix.it [194.116.96.60]
 11 217 ms 216 ms 214 ms 129.44.1.34.bc.googleusercontent.com [34.1.44.129]

Trace complete.
PS C:\> |

PS C:\> # GCP Compute Engine with Premium Tier Network
PS C:\> tracert 34.18.96.112

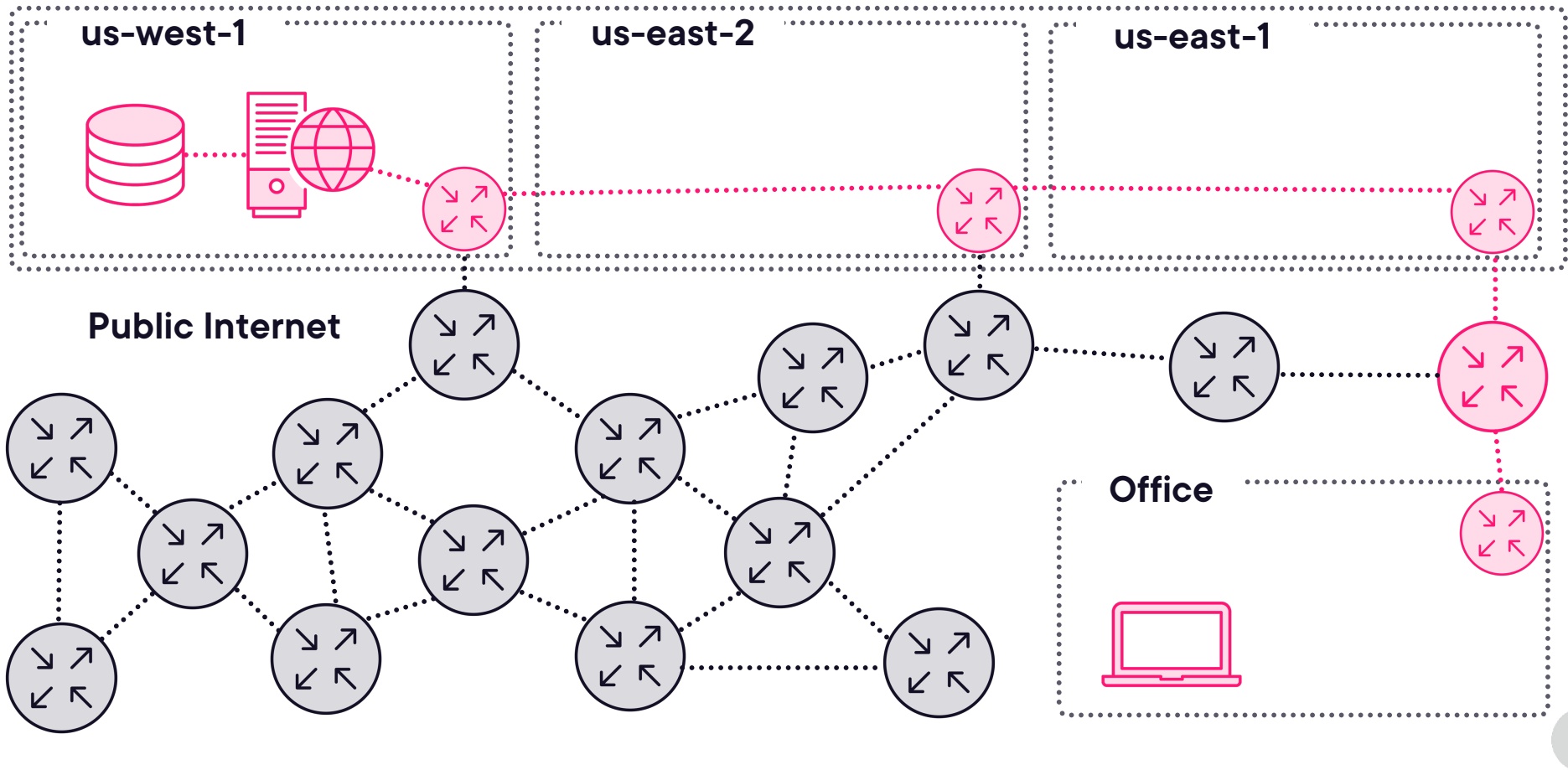
Tracing route to 112.96.18.34.bc.googleusercontent.com [34.18.96.112]
over a maximum of 30 hops:

  1  1 ms  1 ms  1 ms  192.168.100.99
  2  3 ms  3 ms  3 ms  gw3-v4001.gatewayfiber.net [150.195.175.254]
  3  5 ms  5 ms  4 ms  e0-60.core1.stl1.he.net [184.105.11.82]
  4  10 ms *      *      port-channel32.core3.chi1.he.net [184.104.188.170]
  5  20 ms 18 ms 19 ms  eqix-ch-100g.google.com [208.115.137.21]
  6  215 ms 213 ms 213 ms 112.96.18.34.bc.googleusercontent.com [34.18.96.112]

Trace complete.
PS C:\> |
```



Global Traffic Management



AWS Global Accelerator

Speed Comparison

About this tool

AWS Global Accelerator is a service that improves the availability and performance of your applications. This tool compares Global Accelerator to the public internet. Choose a file size to see the time to download a file from application endpoints in different AWS Regions to your browser.

Files are downloaded over HTTPS/TCP from Application Load Balancers (ALBs) in different AWS Regions to your browser. [Learn more](#)

Choose a file size and click "Start" to start the tests:

We welcome suggestions for how to improve this tool. [Provide feedback](#)

ⓘ Results may differ when you run the test multiple times. Download times can vary based on factors that are external to Global Accelerator, such as the quality, capacity, and distance of the connection in the last-mile network that you're using.

Region	Method	Total time
Oregon (us-west-2)	Direct over internet	181ms
	AWS Global Accelerator	178ms 2% faster with AWS Global Accelerator
N. Virginia (us-east-1)	Direct over internet	105ms
	AWS Global Accelerator	89ms 16% faster with AWS Global Accelerator
Ireland (eu-west-1)	Direct over internet	292ms
	AWS Global Accelerator	224ms 23% faster with AWS Global Accelerator

<https://speedtest.globalaccelerator.aws/>



<https://t.me/learningnets>

Direct Cloud Connectivity



Dedicated connection to the cloud, bypassing public internet

Optimizes traffic between on-premise and the cloud

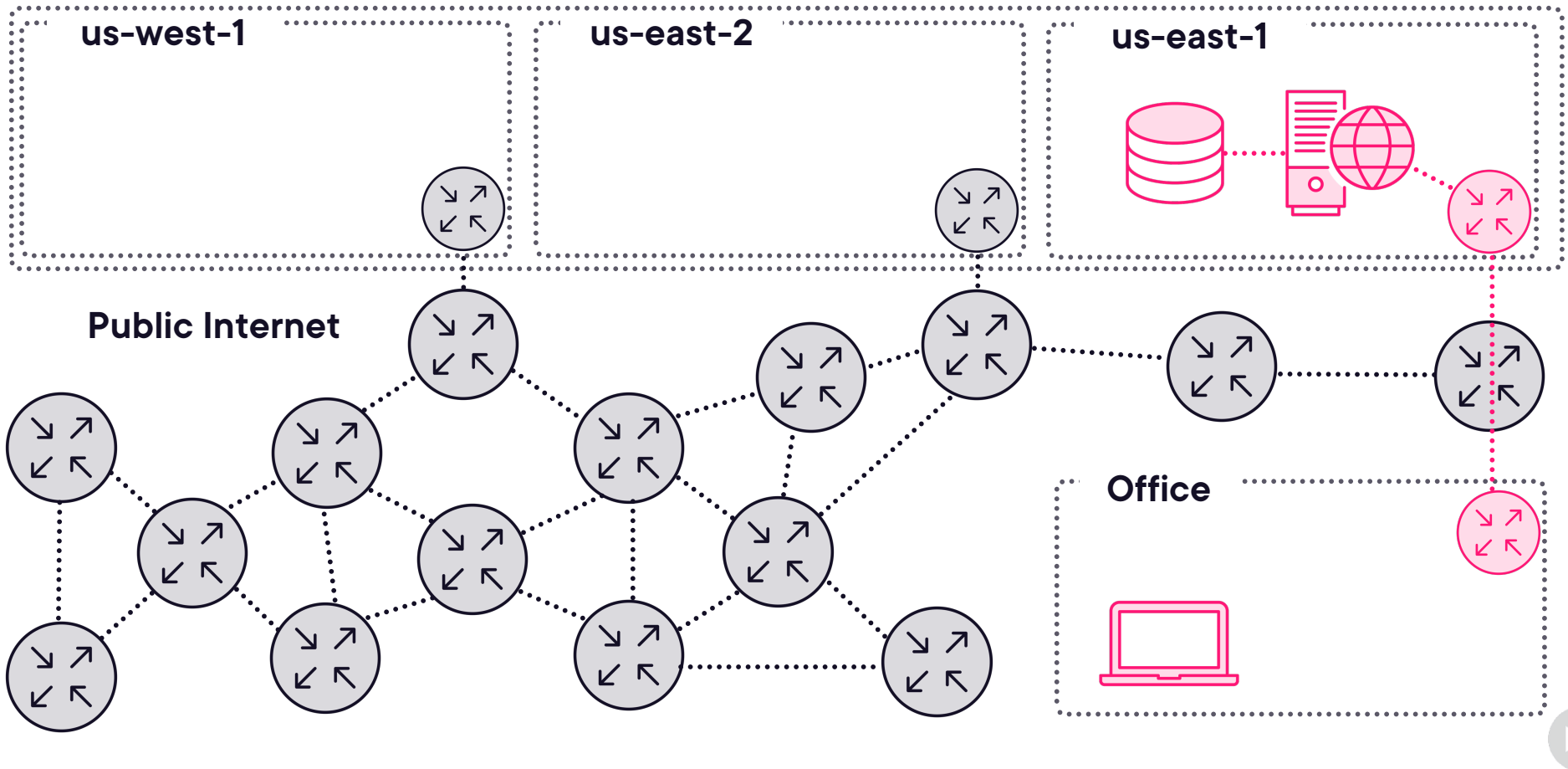
Requires setup with a compatible ISP or partner

Examples of this type of service

- AWS Direct Connect
- Azure ExpressRoute
- Google Cloud Interconnect



Dedicated Cloud Connectivity





Get Hands On

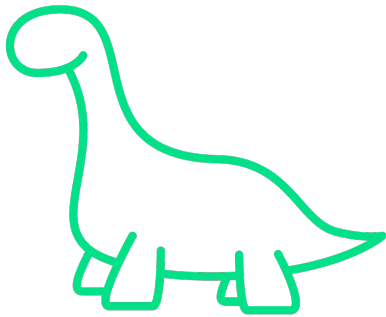
Build a Bandwidth Monitoring Tool with iPerf and PowerShell

Adam Bertram



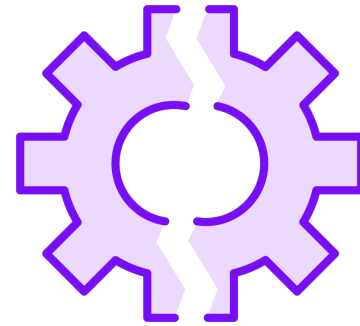
Protocol Problems

Protocol Issues



Deprecated Protocol

Old and Insecure protocols
tend to be deprecated



Incompatible Protocols

Some cloud providers may be
incompatible with certain protocols

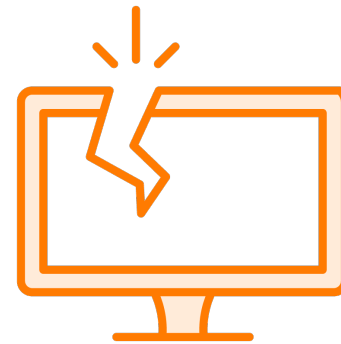


Signs of Protocol Problems



Broken Authentication

Security and Authentication protocols being deprecated can break sign in on your service

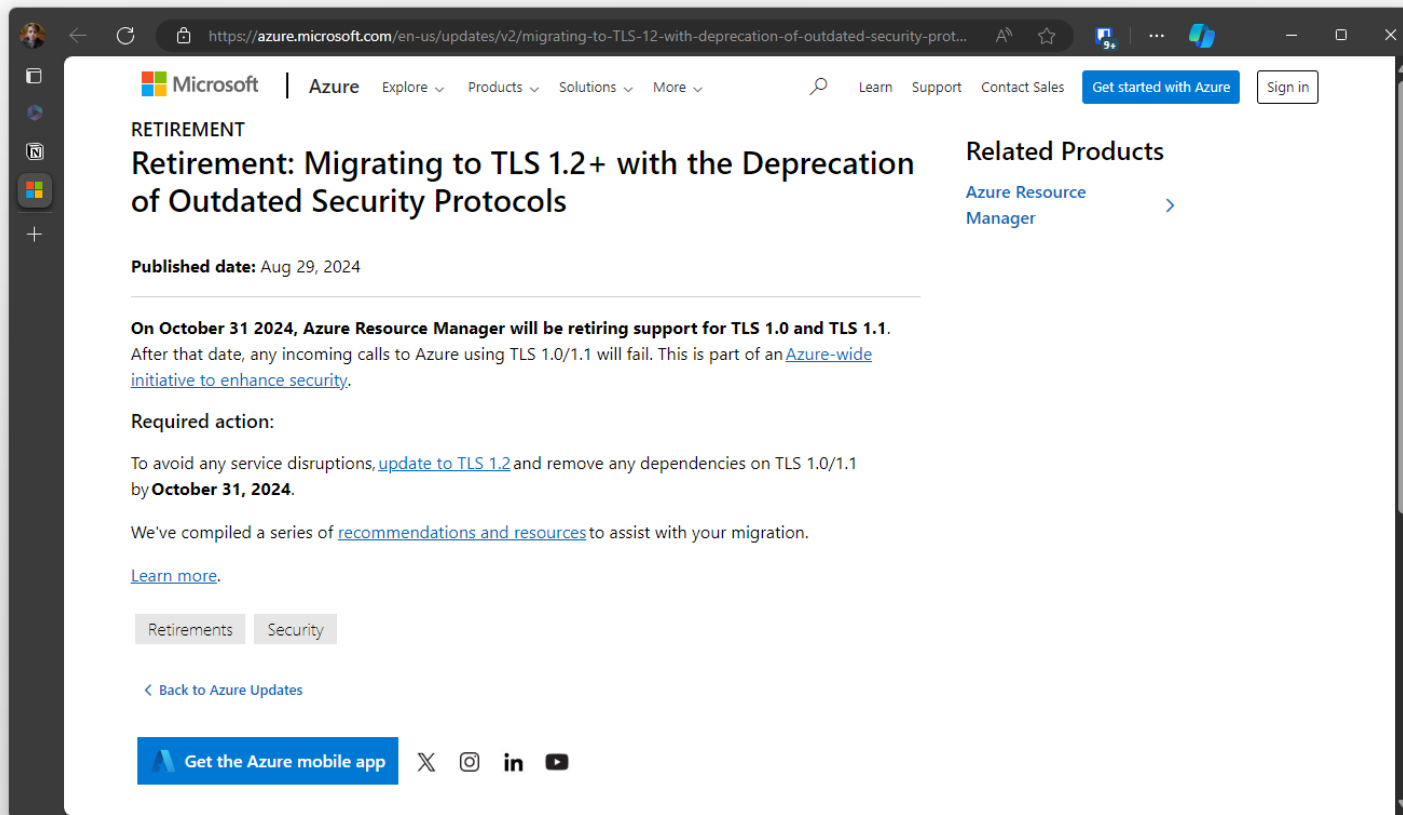


Broken Functionality

A protocol you're currently using being deprecated can cause many things to break



Protocol Deprecation



The screenshot shows a web browser window displaying a Microsoft Azure update. The page title is "Retirement: Migrating to TLS 1.2+ with the Deprecation of Outdated Security Protocols". The update is dated August 29, 2024. The main content states that on October 31, 2024, Azure Resource Manager will retire support for TLS 1.0 and TLS 1.1. It explains that after this date, any incoming calls to Azure using TLS 1.0/1.1 will fail, as part of an initiative to enhance security. The required action is to update to TLS 1.2 and remove dependencies on TLS 1.0/1.1 by October 31, 2024. The page also includes a "Learn more" link, a "Back to Azure Updates" link, and social media icons for X, Instagram, LinkedIn, and YouTube. A "Get the Azure mobile app" button is also present.

Microsoft | Azure Explore Products Solutions More Learn Support Contact Sales Get started with Azure Sign in

RETIREMENT

Retirement: Migrating to TLS 1.2+ with the Deprecation of Outdated Security Protocols

Published date: Aug 29, 2024

On October 31 2024, Azure Resource Manager will be retiring support for TLS 1.0 and TLS 1.1. After that date, any incoming calls to Azure using TLS 1.0/1.1 will fail. This is part of an [Azure-wide initiative to enhance security](#).

Required action:

To avoid any service disruptions, [update to TLS 1.2](#) and remove any dependencies on TLS 1.0/1.1 by **October 31, 2024**.

We've compiled a series of [recommendations and resources](#) to assist with your migration.

[Learn more.](#)

Retirements Security

[Back to Azure Updates](#)

Get the Azure mobile app X Instagram LinkedIn YouTube

Related Products

[Azure Resource Manager](#)

Solving Protocol Deprecations/Incompatibilities



Keep up to date on announcements of features and platform changes



Set alerts and monitor protocol lifecycles in cloud environments



Audit your environment for protocols that you may be unaware you are using.



Plan and test a migration of the protocol

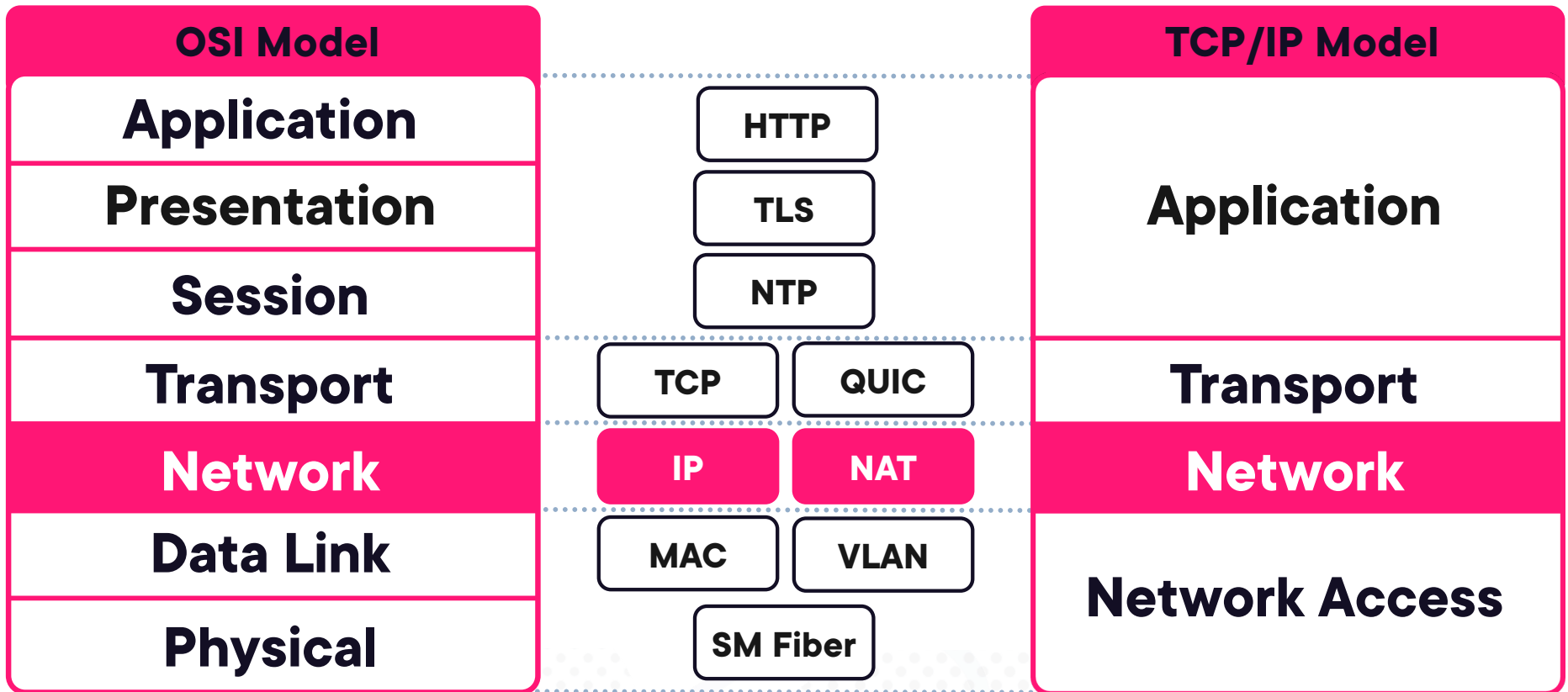


Reading the documentation about the supported protocols will help prevent issues that arise from trying to use them

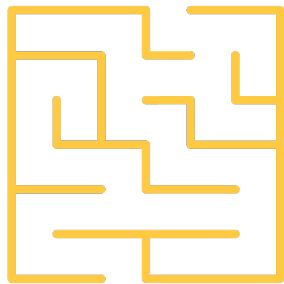


Troubleshooting Routing in Cloud Networks

Network Layers

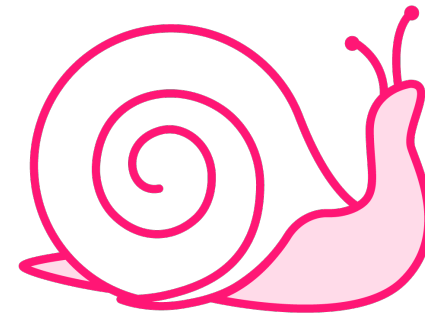


Issues That Arise from Bad Routes



Unreachable Networks

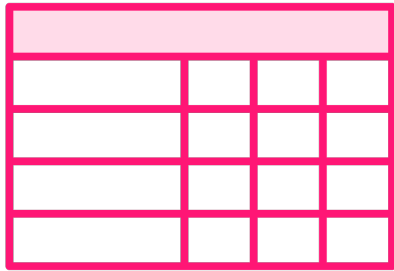
Misconfigured routes can make a network unreachable



Latency Issues

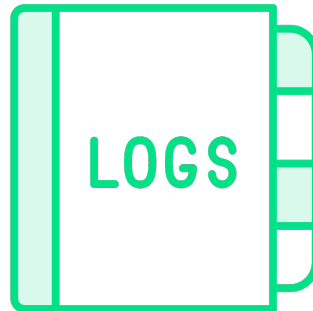
Suboptimal routes can lead to higher latency as traffic doesn't take the best path

Troubleshoot Routes



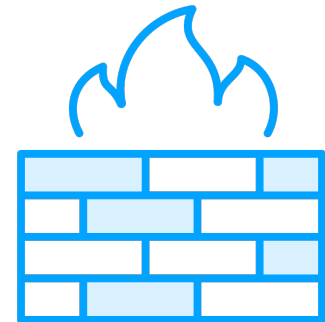
Route Tables

Verify the route tables are correct



Network Flow Logs

May contain useful information that can aid in troubleshooting



Firewall Rules

Routes may be correct, but the firewall is blocking it



Types of Routes

Static Routes

Routes manually entered into the routing table, by an admin or by some software

Dynamic Routes

Routes given to you automatically, whether handed down from the DHCP or by a BGP peer



Troubleshooting Routes on a VM

```
jacob@debian: ~$ ip route list
default via 192.168.100.9 dev eth0
109.254.0.0/16 dev eth0 scope link metric 1000
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.125
jacob@debian:~$
```

Troubleshooting Routes on a VM

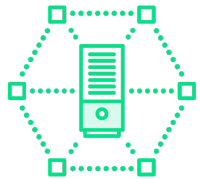
```
jacob@debian: ~$ ip route list
default via 192.168.100.99 dev eth0
169.254.0.0/16 dev eth0 scope link metric 1000
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.125
jacob@debian: ~$ ip route get 8.8.8.8
8.8.8.8 via 192.168.100.99 dev eth0 src 192.168.100.125 uid 1000
cache
jacob@debian: ~$
```

Troubleshooting Routes on a VM

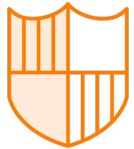
```
jacob@debian: ~$ ip route list
default via 192.168.100.99 dev eth0
169.254.0.0/16 dev eth0 scope link metric 1000
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.125
jacob@debian:~$ ip route get 8.8.8.8
8.8.8.8 via 192.168.100.99 dev eth0 src 192.168.100.125 uid 1000
  cache
jacob@debian:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 192.168.100.99 (192.168.100.99) 3.555 ms 3.535 ms 3.528 ms
 2 GW3-v4001.gatewayfiber.net (150.195.175.254) 4.117 ms 4.108 ms 4.101 ms
 3 e0-60.core1.stl1.he.net (184.105.11.82) 5.545 ms 5.538 ms 5.733 ms
 4 * * *
 5 eaix-ch-200a-1.google.com (208.115.136.21) 19.003 ms 18.997 ms 18.929 ms
 6 192.178.241.33 (192.178.241.33) 18.138 ms 18.382 ms 108.170.243.174 (108.170.243.174) 11.958 ms
 7 209.85.247.117 (209.85.247.117) 10.284 ms 142.251.60.201 (142.251.60.201) 18.769 ms 142.251.60.209 (142.251.60.209) 11.240 ms
 8 dns.google (8.8.8.8) 10.891 ms 9.898 ms 10.564 ms
jacob@debian:~$
```



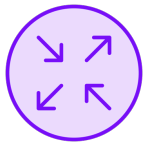
Checking Routes Across the Cloud



On the virtual network or the subnet



On network security groups



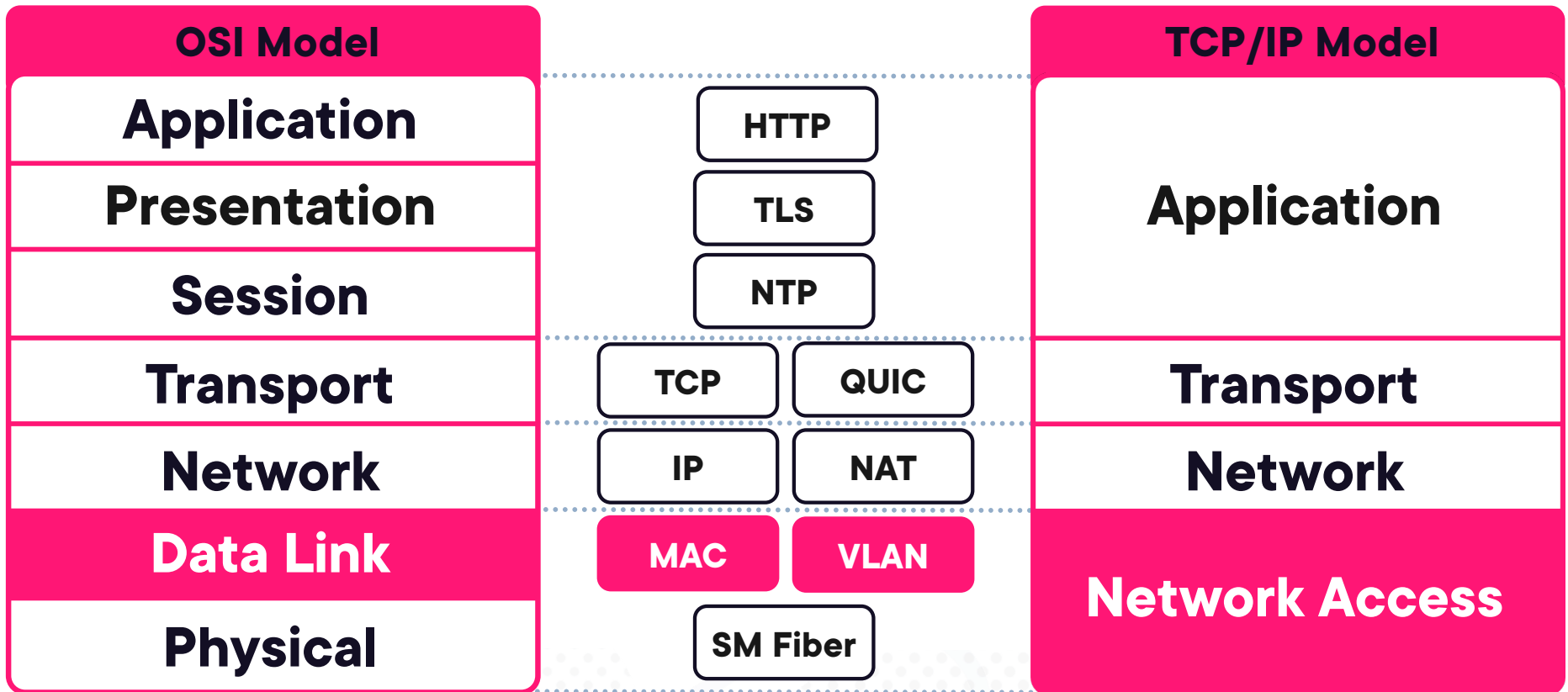
On cloud gateways and routers





Identifying Network Switching Problems

Network Layers

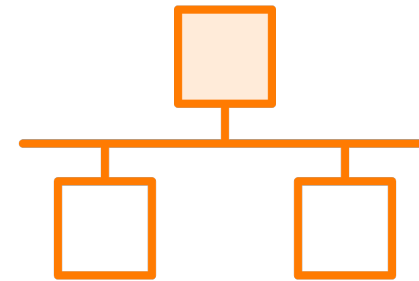


Network Switching Problems



Virtual LAN (VLAN) Issues

Issues caused by
misconfigured VLAN tags



Switch Port Issues

Issues caused the misconfiguration
of network trunk and access ports



Key VLAN Terms



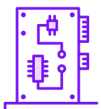
Virtual LAN (VLAN) – A virtual layer 2 network



Access Port – A switchport that only carries traffic for one VLAN



Trunk Port – A switchport that carries traffic for all (or some) VLANs



Native VLAN – Default VLAN for frames that aren't tagged already



Tagged VLAN – Allows frames tagged with that VLAN to use that port



Troubleshooting VLANs



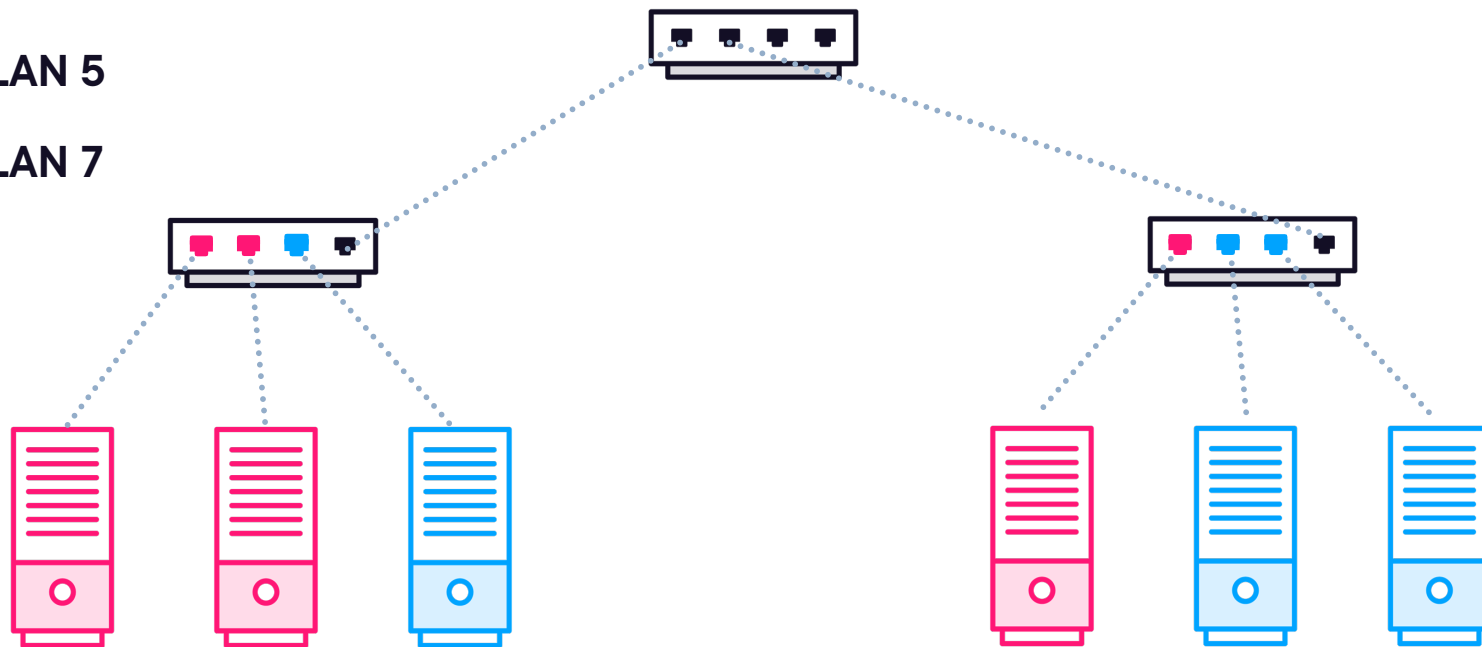
VLAN 2



VLAN 5



VLAN 7



Troubleshooting VLANs



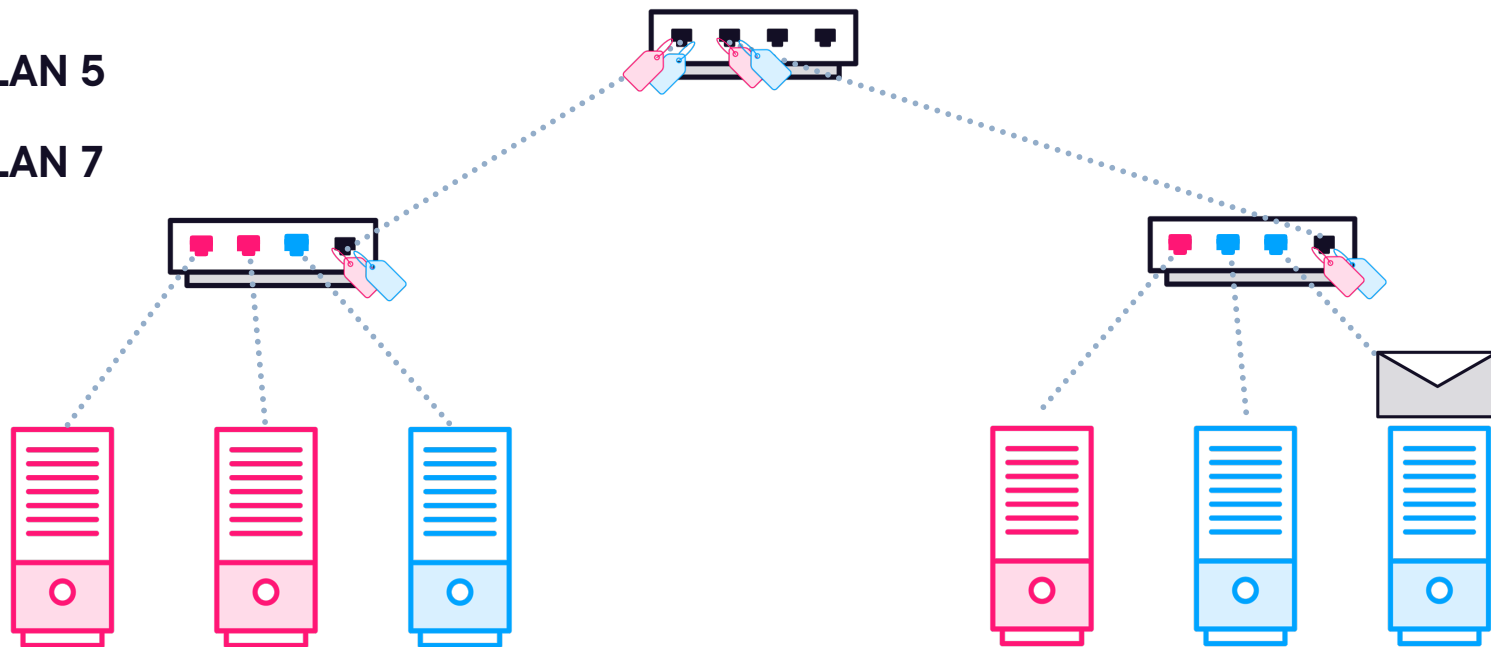
VLAN 2



VLAN 5



VLAN 7



Troubleshooting VLANs



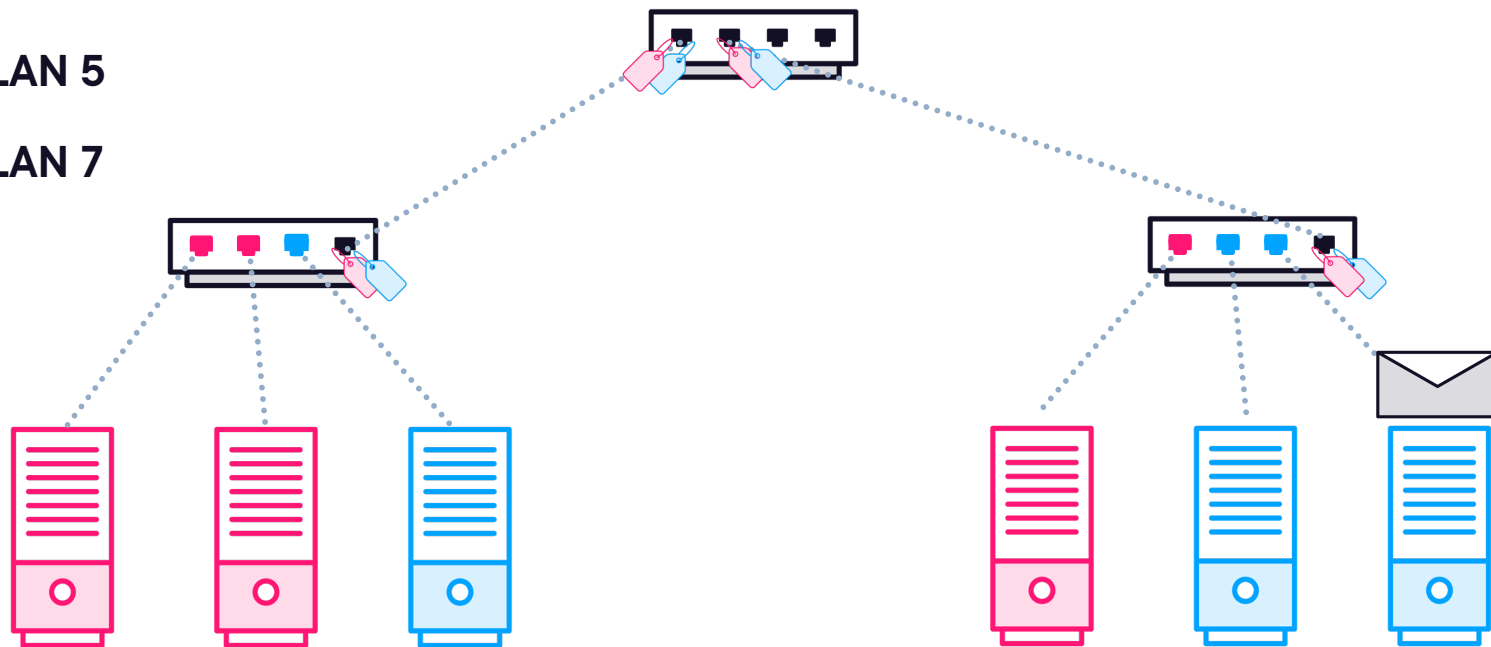
VLAN 2



VLAN 5



VLAN 7



Troubleshooting VLANs



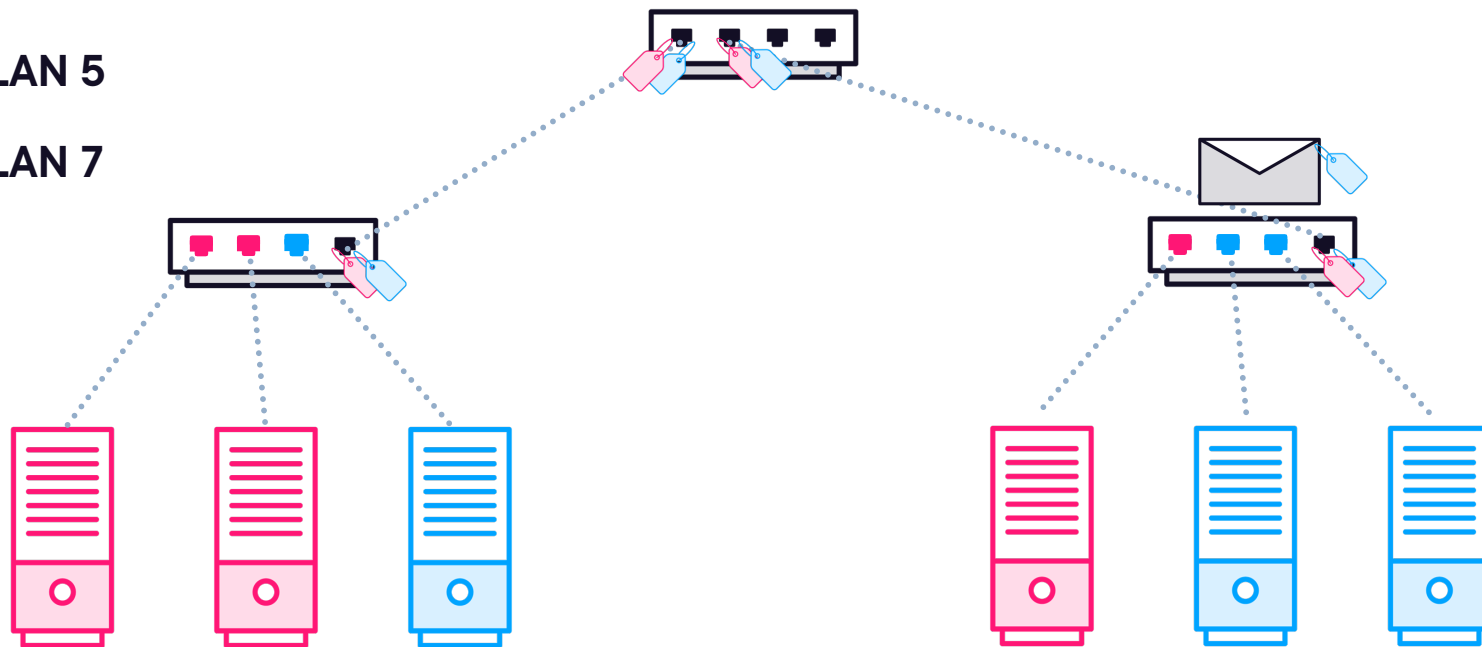
VLAN 2



VLAN 5



VLAN 7



Troubleshooting VLANs



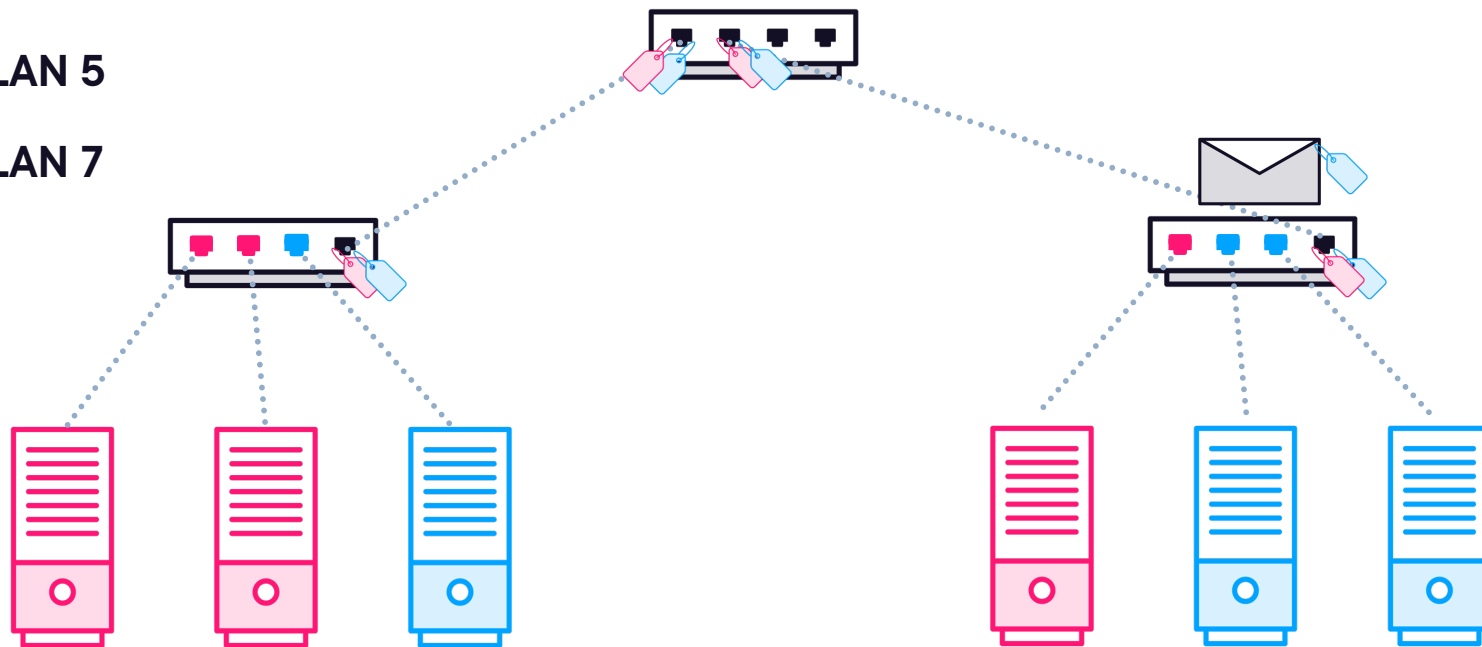
VLAN 2



VLAN 5



VLAN 7



Troubleshooting VLANs



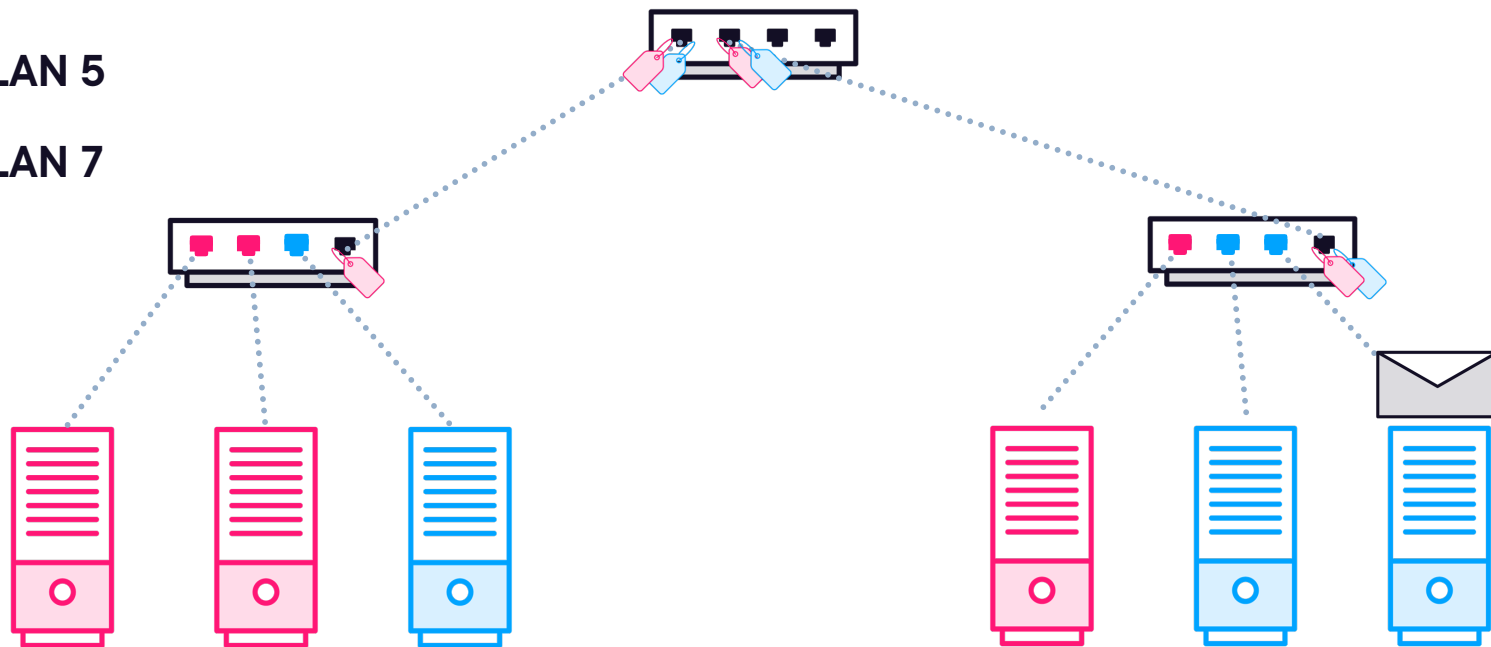
VLAN 2



VLAN 5



VLAN 7



Troubleshooting VLANs



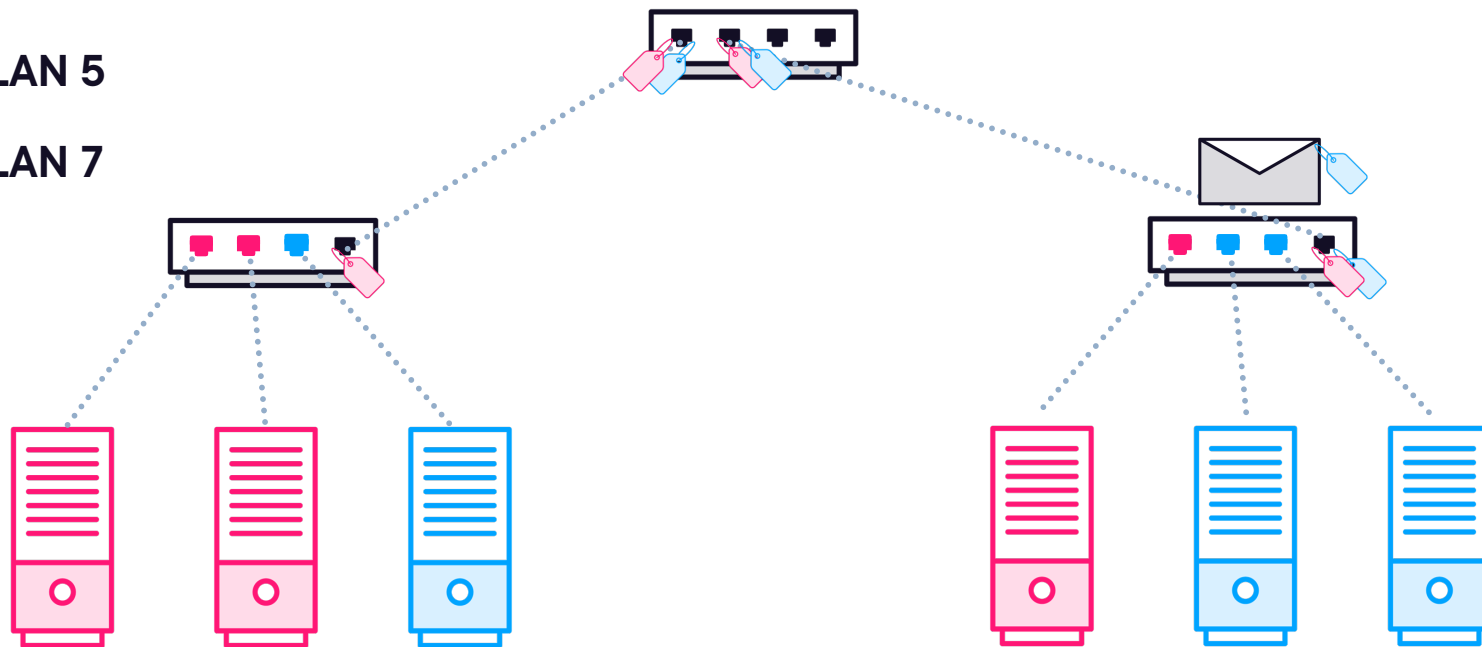
VLAN 2



VLAN 5



VLAN 7



Troubleshooting VLANs



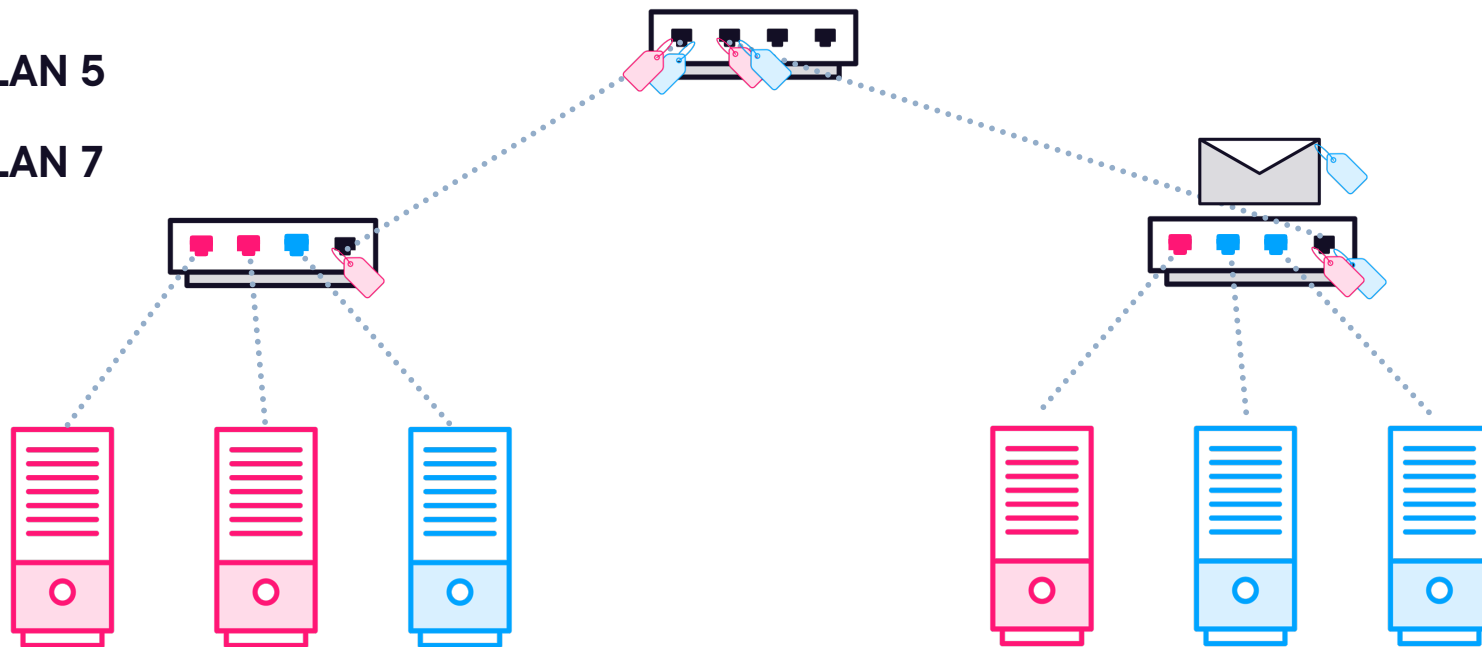
VLAN 2



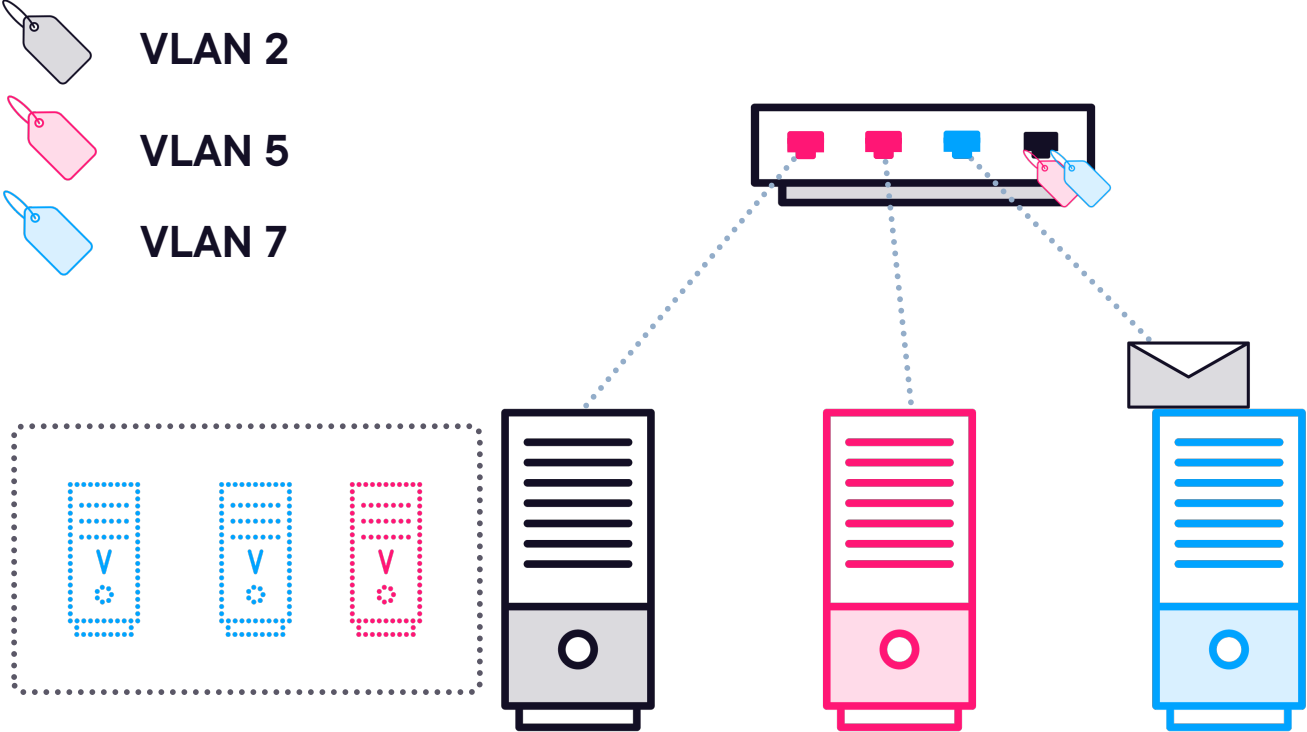
VLAN 5



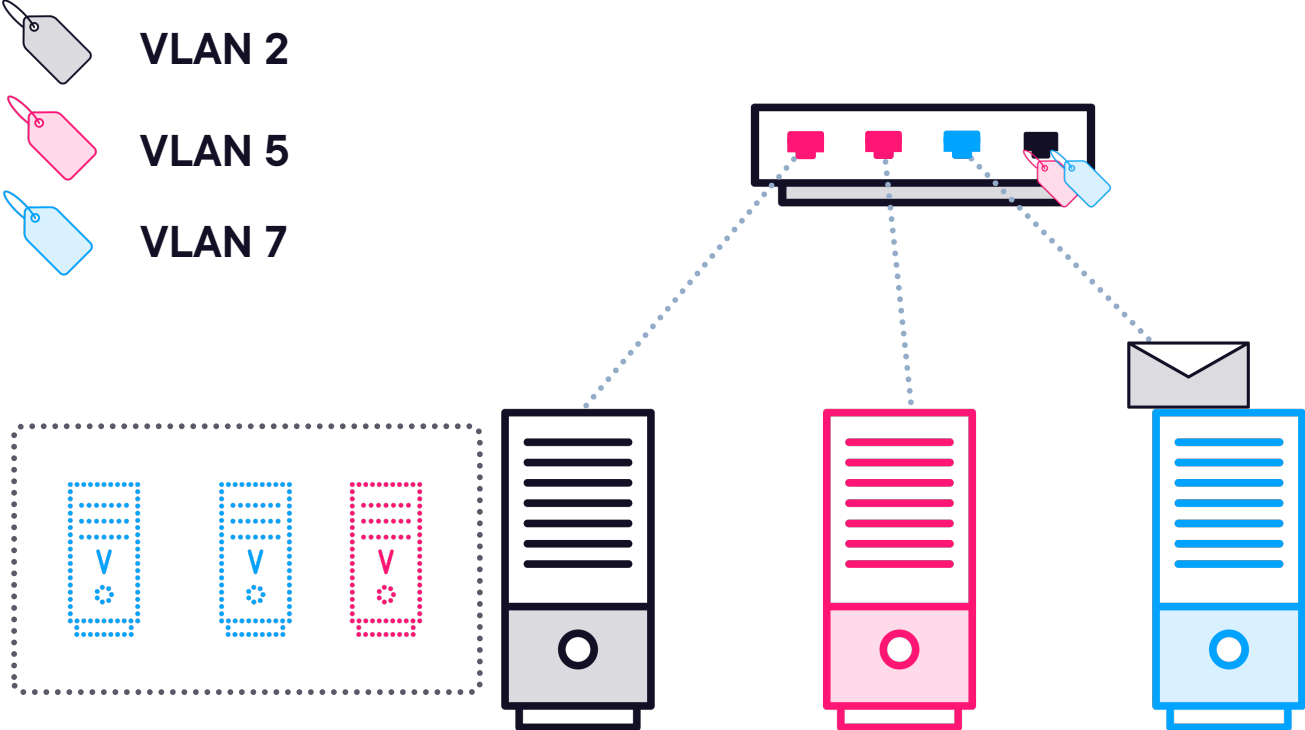
VLAN 7



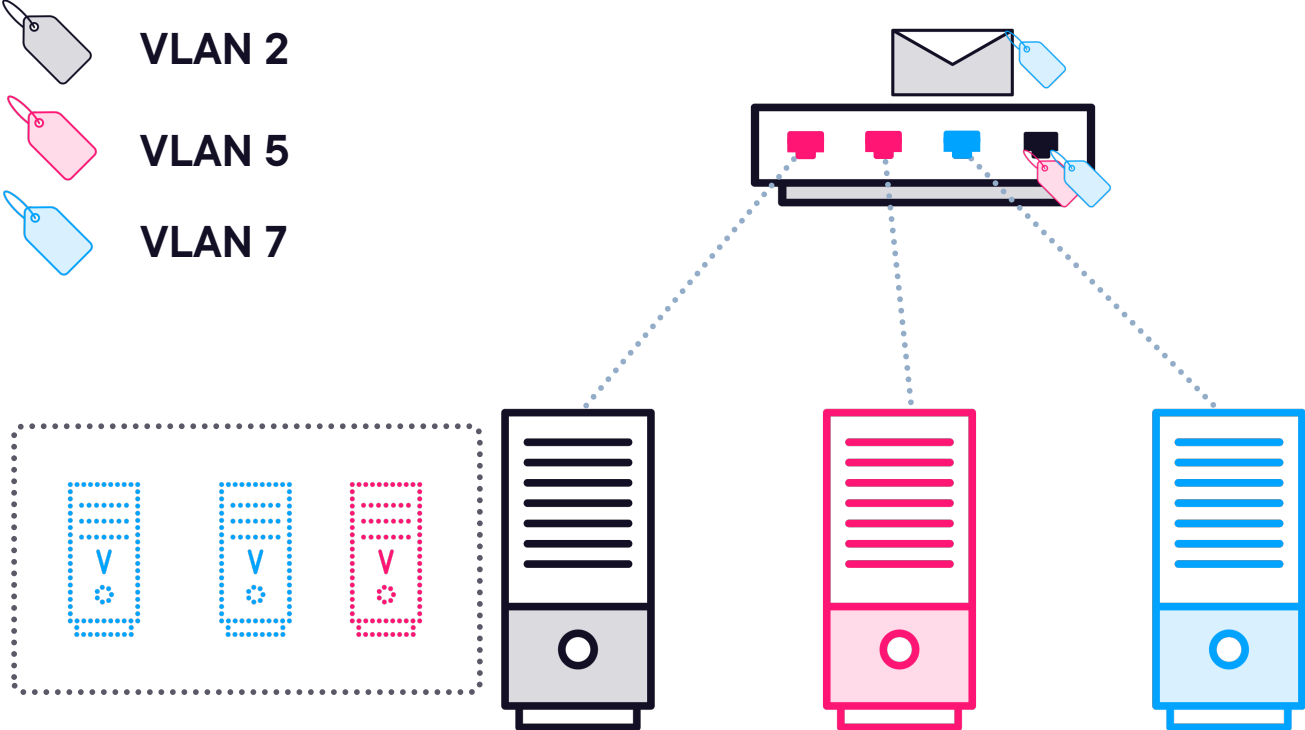
Hypervisor with Access Ports



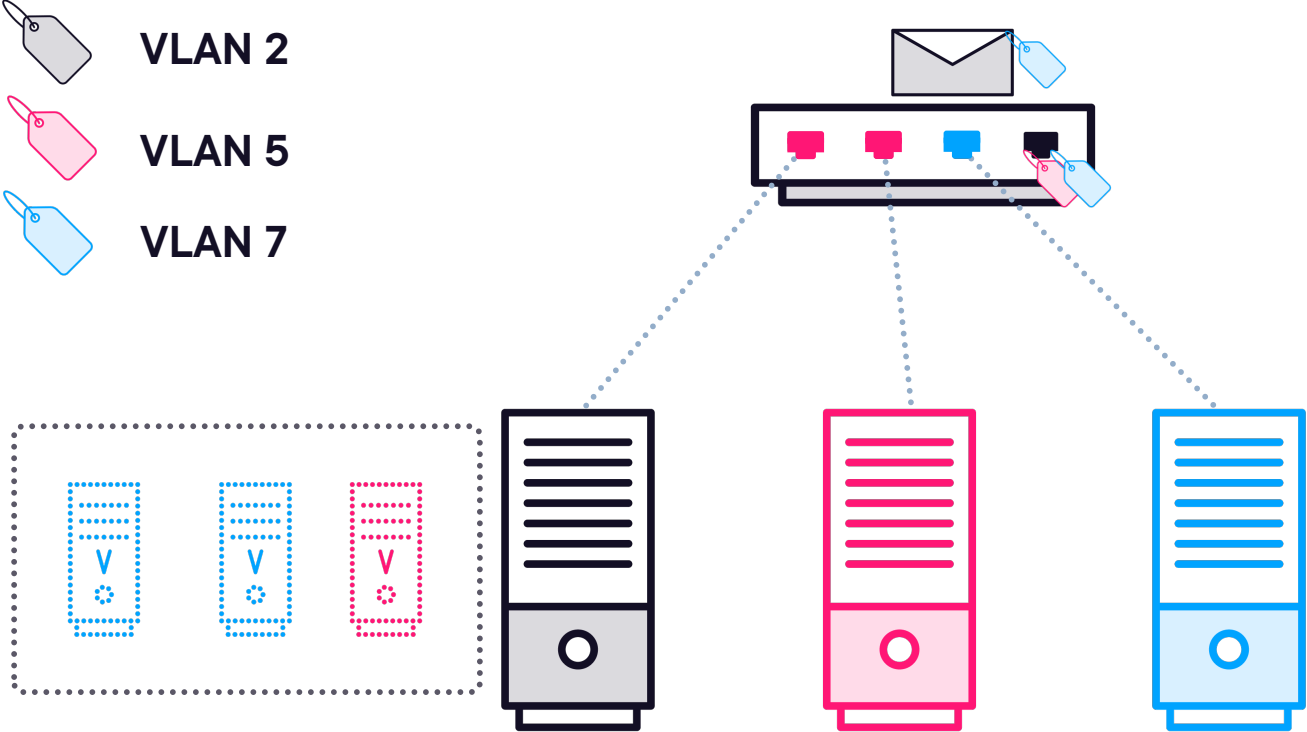
Hypervisor with Access Ports



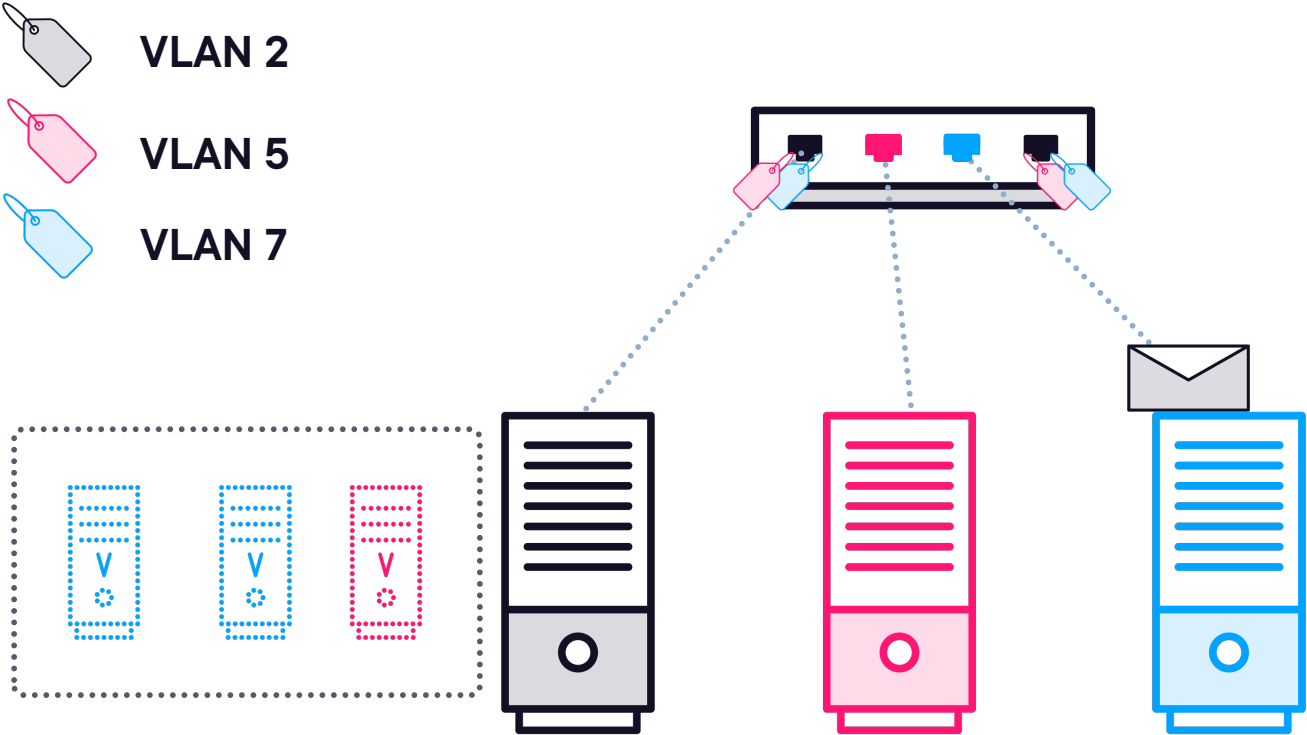
Hypervisor with Access Ports



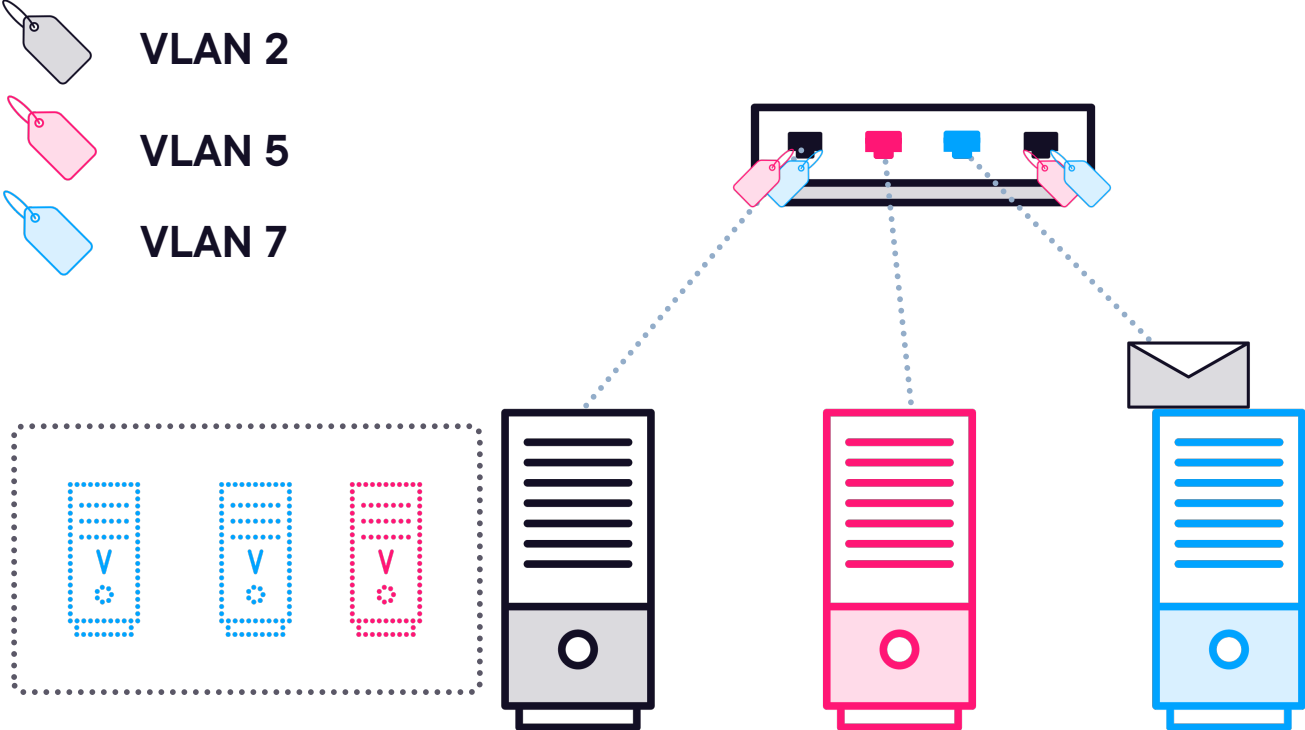
Hypervisor with Access Ports



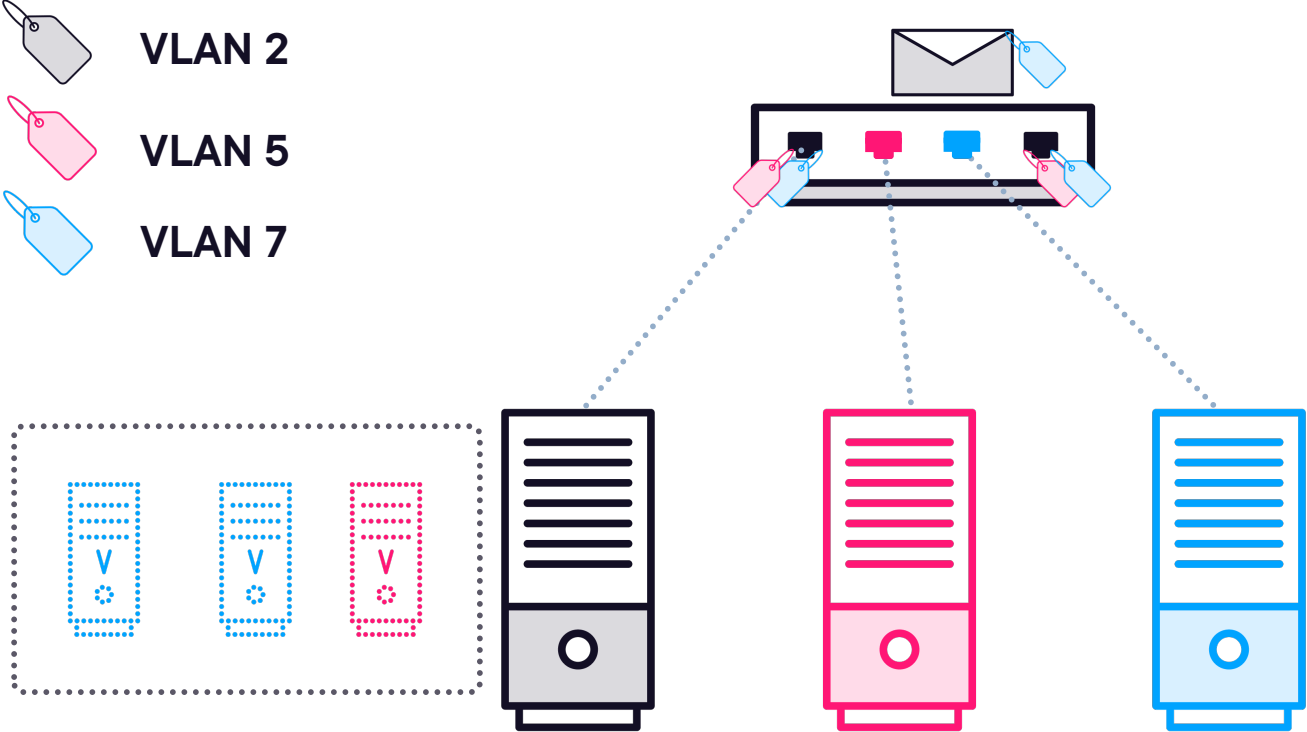
Hypervisor with Trunk Ports



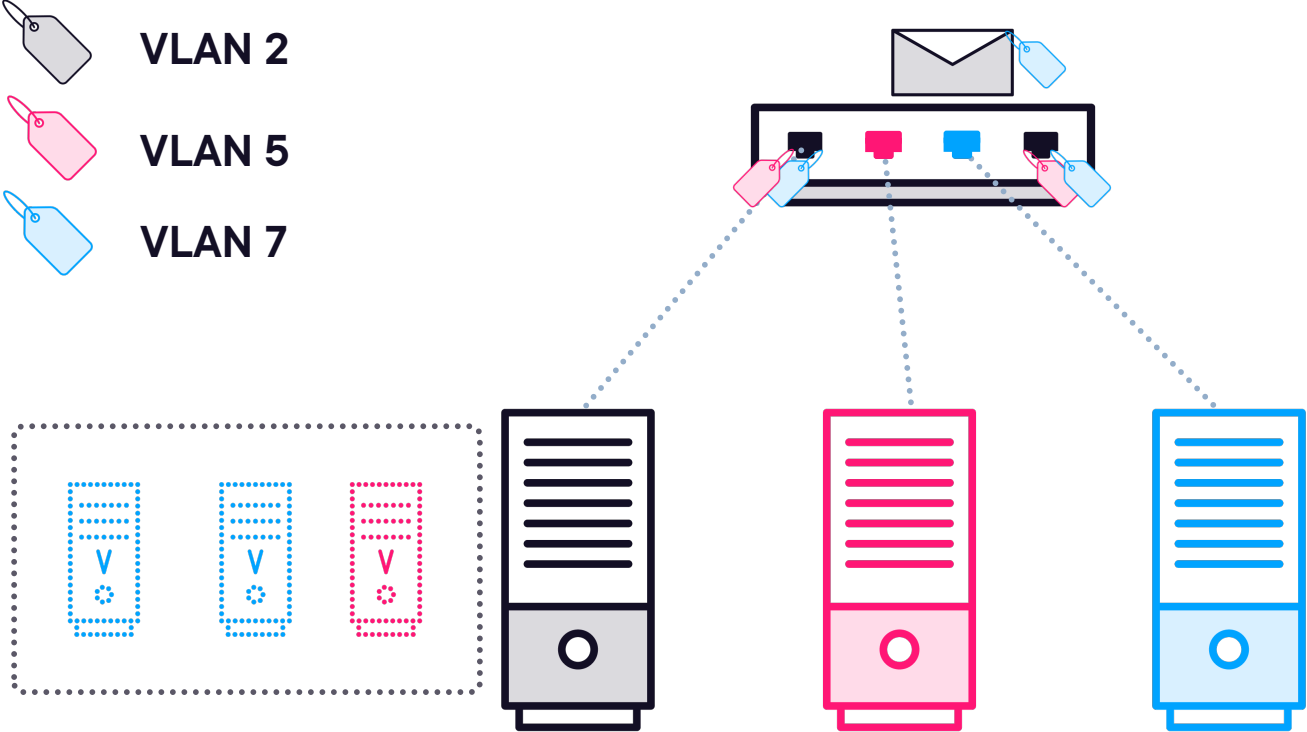
Hypervisor with Trunk Ports



Hypervisor with Trunk Ports



Hypervisor with Trunk Ports



Network Switching Problems

```
PowerShell x + v
Catalyst_9300#
Catalyst_9300#show vlan brief

VLAN Name                Status    Ports
-----
1    default                 active    Te1/0/23, Ap1/0/1
25   production              active    Te1/0/1, Te1/0/2, Te1/0/3, Te1/0/4, Te1/0/5, Te1/0/6, Te1/0/7, Te1/0/8
                                           Te1/0/9, Te1/0/10, Te1/0/11, Te1/0/12, Te1/0/13, Te1/0/14, Te1/0/15
                                           Te1/0/16, Te1/0/17, Te1/0/18, Te1/0/19, Te1/0/20, Te1/0/21, Te1/0/22
80   internet                active
1002 fddi-default            act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default        act/unsup
Catalyst_9300#
```

Network Switching Problems

```
PowerShell x + -
Catalyst_9300#
Catalyst_9300#show interfaces te1/0/14 switchport
Name: Te1/0/14
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 25 (production)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
Appliance trust: none
Catalyst_9300#
```

```
PowerShell x + -
Catalyst_9300#
Catalyst_9300#show interfaces te1/0/24 switchport
Name: Te1/0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
Appliance trust: none
Catalyst_9300#
```

Network Switching Problems

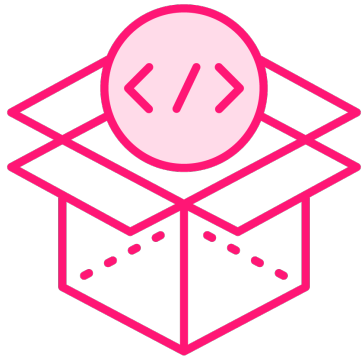
```
PowerShell x + -
Catalyst_9300#
Catalyst_9300#show interfaces te1/0/14 switchport
Name: Te1/0/14
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 25 (production)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
Appliance trust: none
Catalyst_9300#
```

```
PowerShell x + -
Catalyst_9300#
Catalyst_9300#show interfaces te1/0/24 switchport
Name: Te1/0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

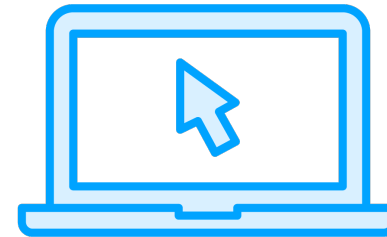
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Vepa Enabled: false
Appliance trust: none
Catalyst_9300#
```

Additional Switching Help



Infrastructure as Code (IaC)

Version control can help
you track changes



Virtual Labs

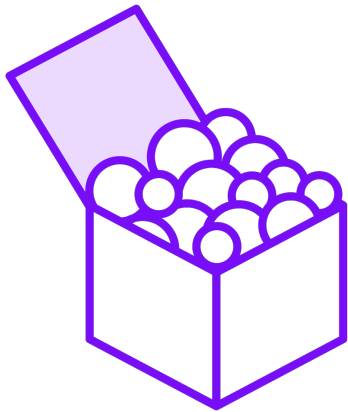
Use tools like Cisco Packet Tracer
and GNS3 to try out what you learn





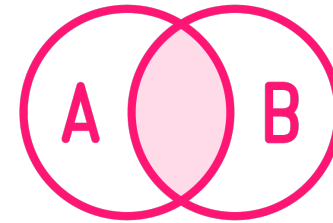
Finding Issues with IP Addressing

Main IP Addressing Problems



Scope Exhaustion

When a DHCP address pool is used up, and new resources can't get an IP address



Network Overlap

When there are two or more networks that all use the same IP address space

Private IPv4 Addresses

10.0.0.0/8

10.0.0.0 – 10.255.255.255

Hosts : 16,777,216

Subnet /24s : 65,536
Subnet /20s: 4096
Subnet /16s: 256

172.16.0.0/12

172.16.0.0 – 172.31.255.255

Hosts : 1,048,574

Subnet /24s : 4,096
Subnet /20s: 256
Subnet /16s: 16

192.168.0.0/16

192.168.0.0 – 192.168.255.255

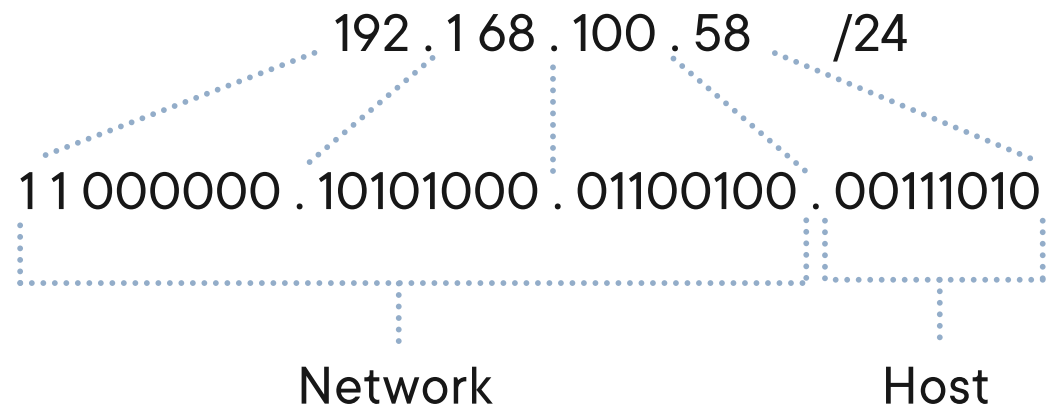
Hosts : 65,534

Subnet /24s : 256
Subnet /20s: 16
Subnet /16s: 1

<https://www.rfc-editor.org/rfc/rfc1918>



Subnetting with CIDR Notation

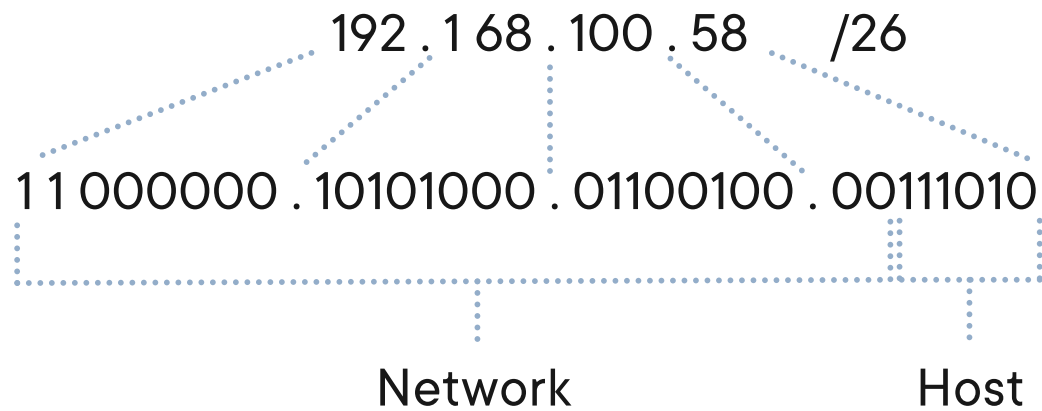


Network Address: 192.168.100.0

Broadcast Address: 192.168.100.255

Usable Addresses: 192.168.100.1 – 192.168.100.254

Subnetting with CIDR Notation



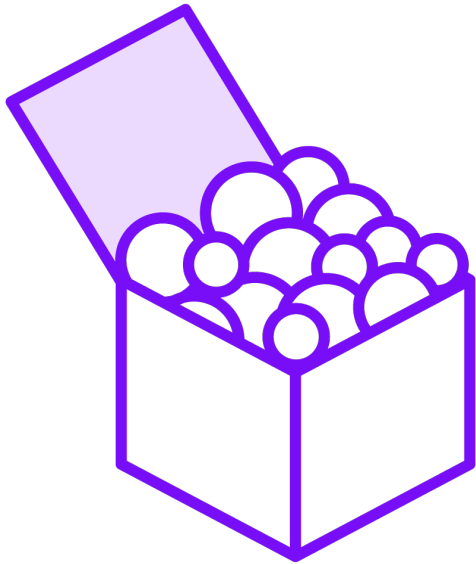
Network Address: 192.168.100.0

Broadcast Address: 192.168.100.63

Usable Addresses: 192.168.100.1 – 192.168.100.62



Scope Exhaustion



Occurs when your DHCP server runs out of IP addresses to lease

In a public cloud environment these settings are likely on the virtual networks for private IPs

Setting up monitoring to alert when the DHCP scope is getting close to full

Troubleshooting Scope Exhaustion

Reduce Lease Time

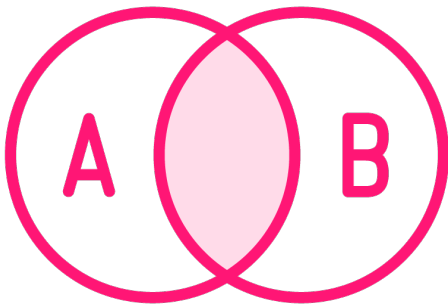
For dynamic environments
with frequent server
spin-ups and spin-down

Expand Subnet Size

If you are frequently exhausting
the scope with long-lived servers



Network Overlap



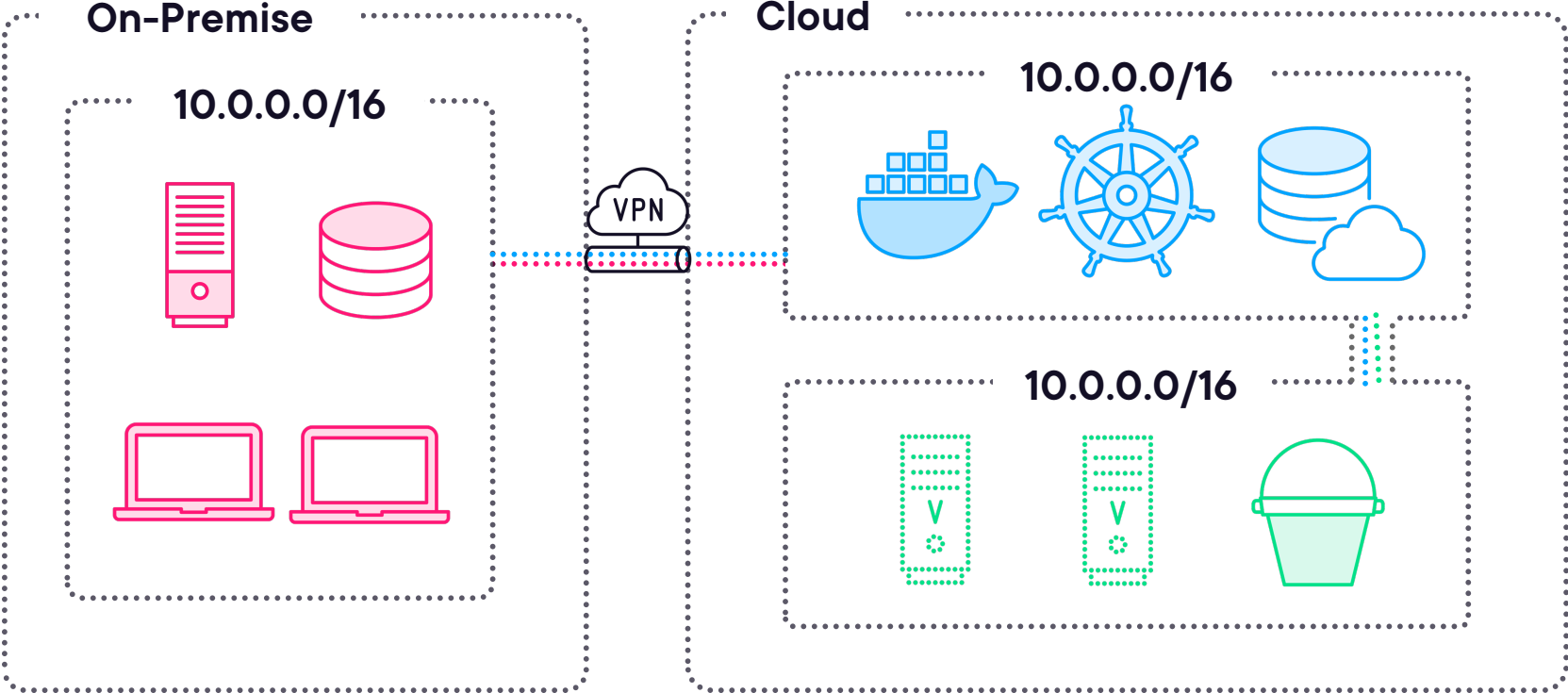
Where you have two or more networks using the same IP address space

This causes problems communicating due to IP address conflicts

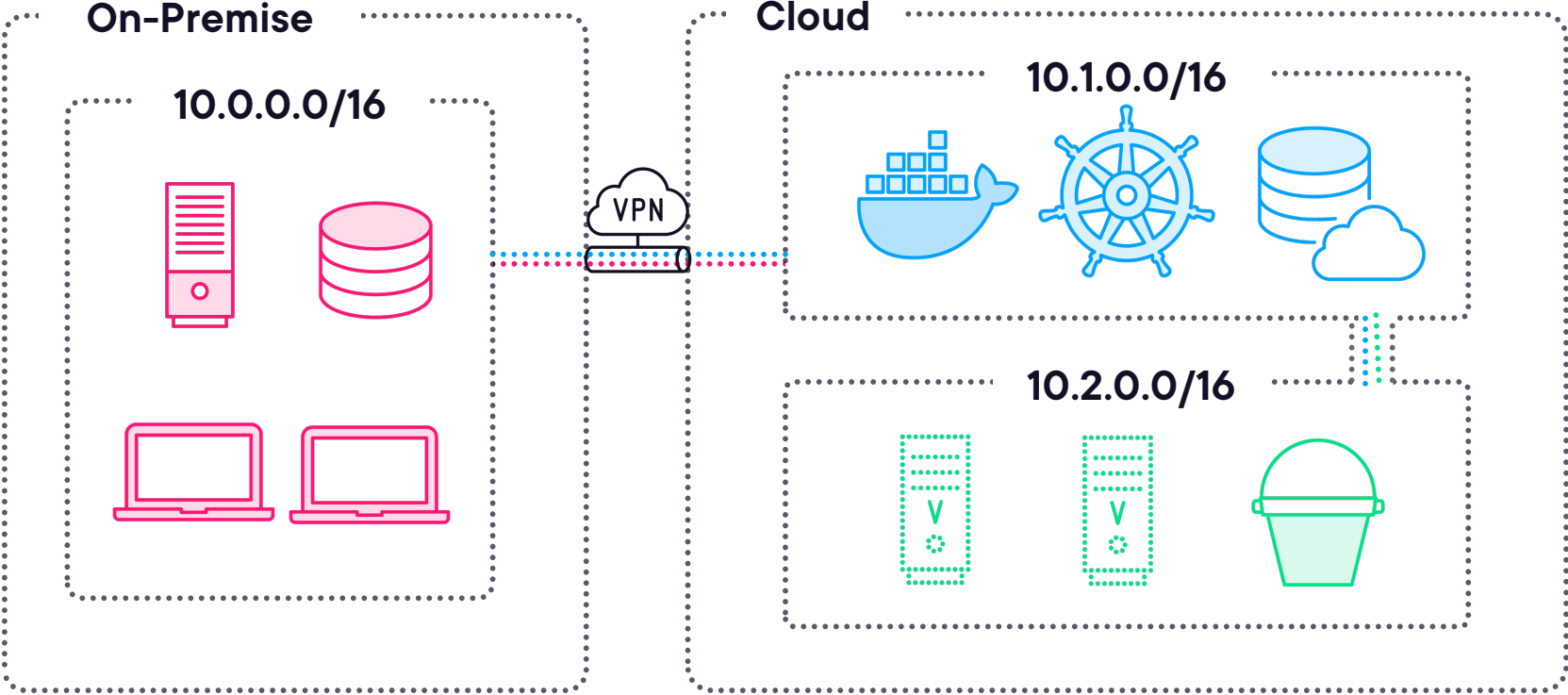
Can be due to separate teams working in the cloud with a standard IP addressing scheme



Network Overlap



Network Overlap



Troubleshooting Network Overlap

Check Networks Before Peering

When connecting two networks check their IP addressing

IP Address Management (IPAM)

When a new virtual net gets spun up, it doesn't overlap

Network Scanners

Use to scan IP ranges to see what IP addresses are being used

Use NAT

Used internally to fix some issues if changing IPs is not an option



Summary

Troubleshooting common network services

Fixing latency and bandwidth issues

Dealing with deprecated protocols

Solving network configuration issues with

- Routing (layer 3)
- Switching (layer 2)

Identify issues caused by IP addressing



Up Next:

Troubleshooting Security Issues in the Cloud

