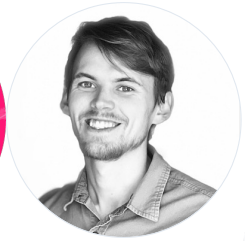
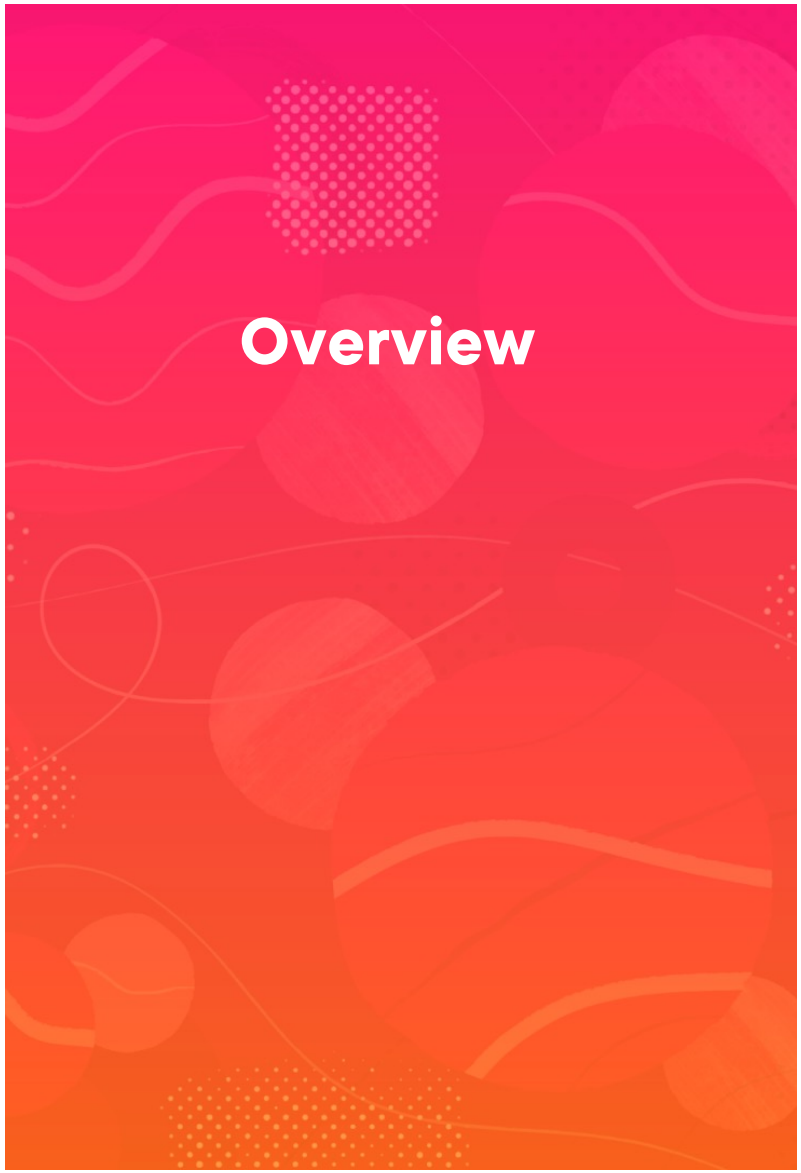
Troubleshooting Network Issues



Jacob Petrie
Network Administrator

@pwsh1996



Diagnosing Network Services

Understanding Latency and Bandwidth Issues

Protocol Problems

Troubleshoot Routing in Cloud Networks

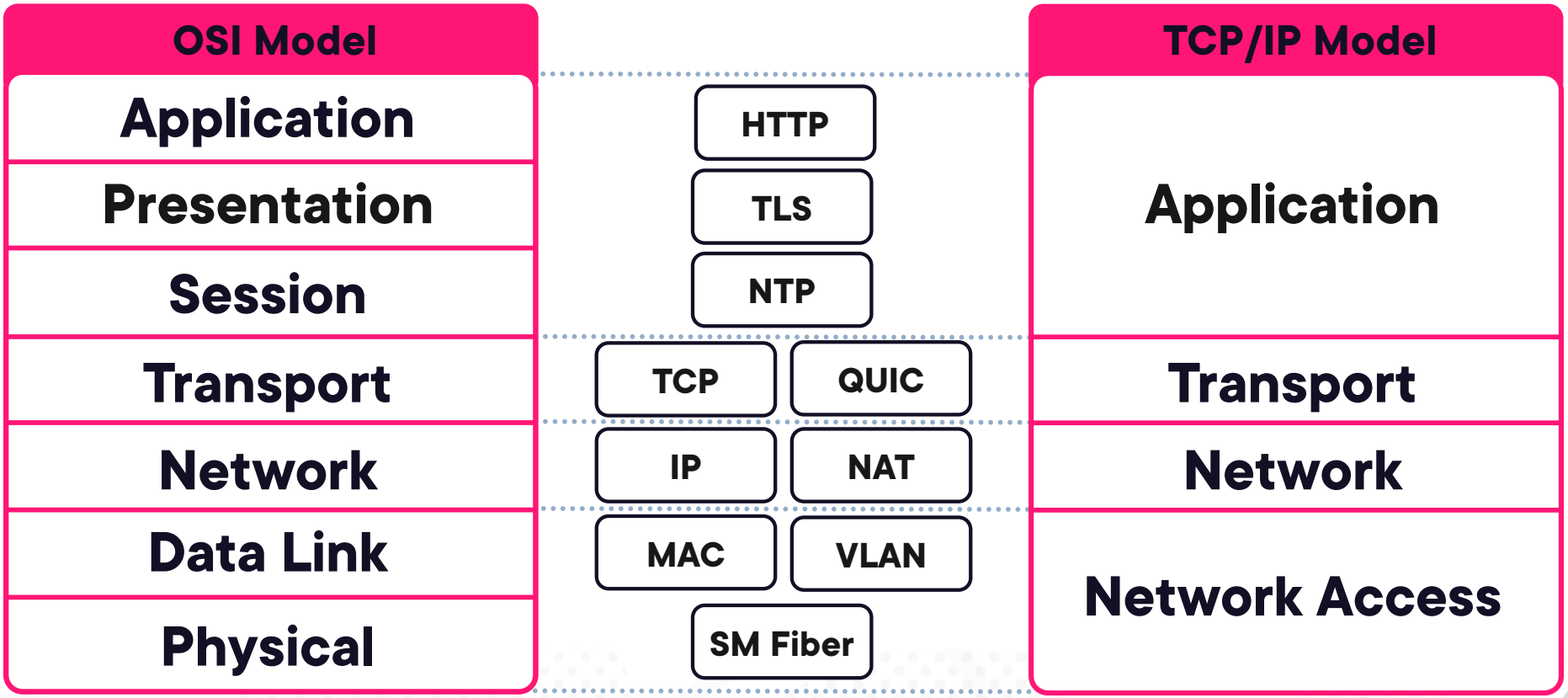
Identifying Network Switching Problems

Finding Issues with IP Addressing

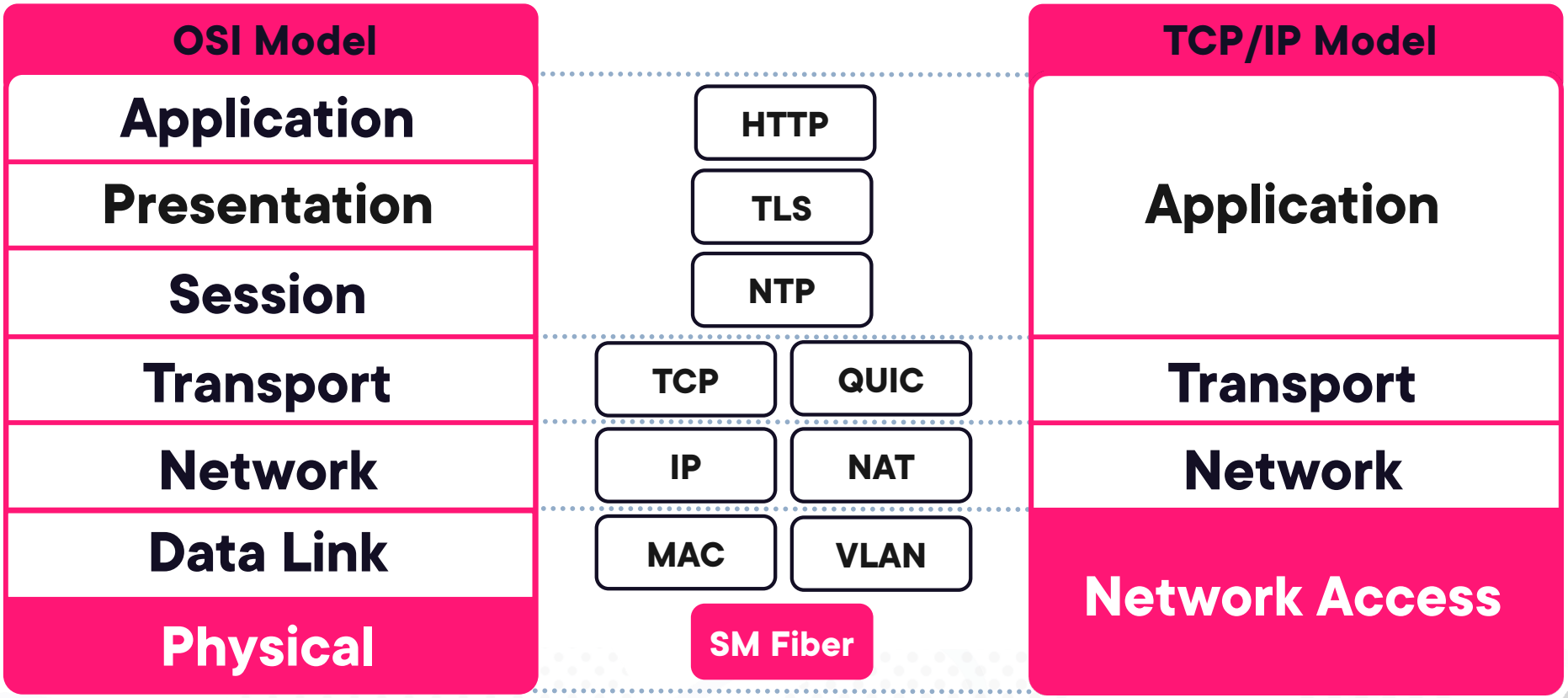
CompTIA Cloud+

Given a scenario, troubleshoot network issues.

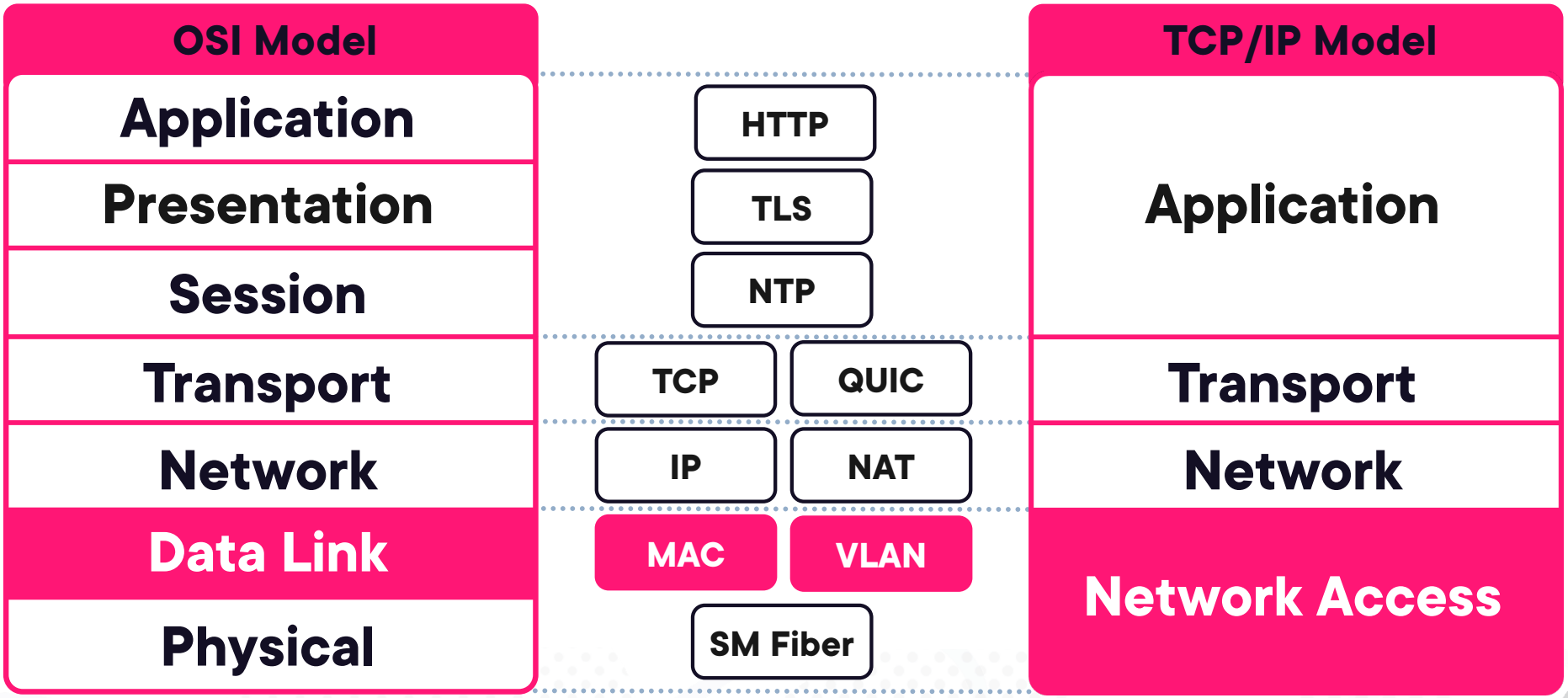
Network Layers



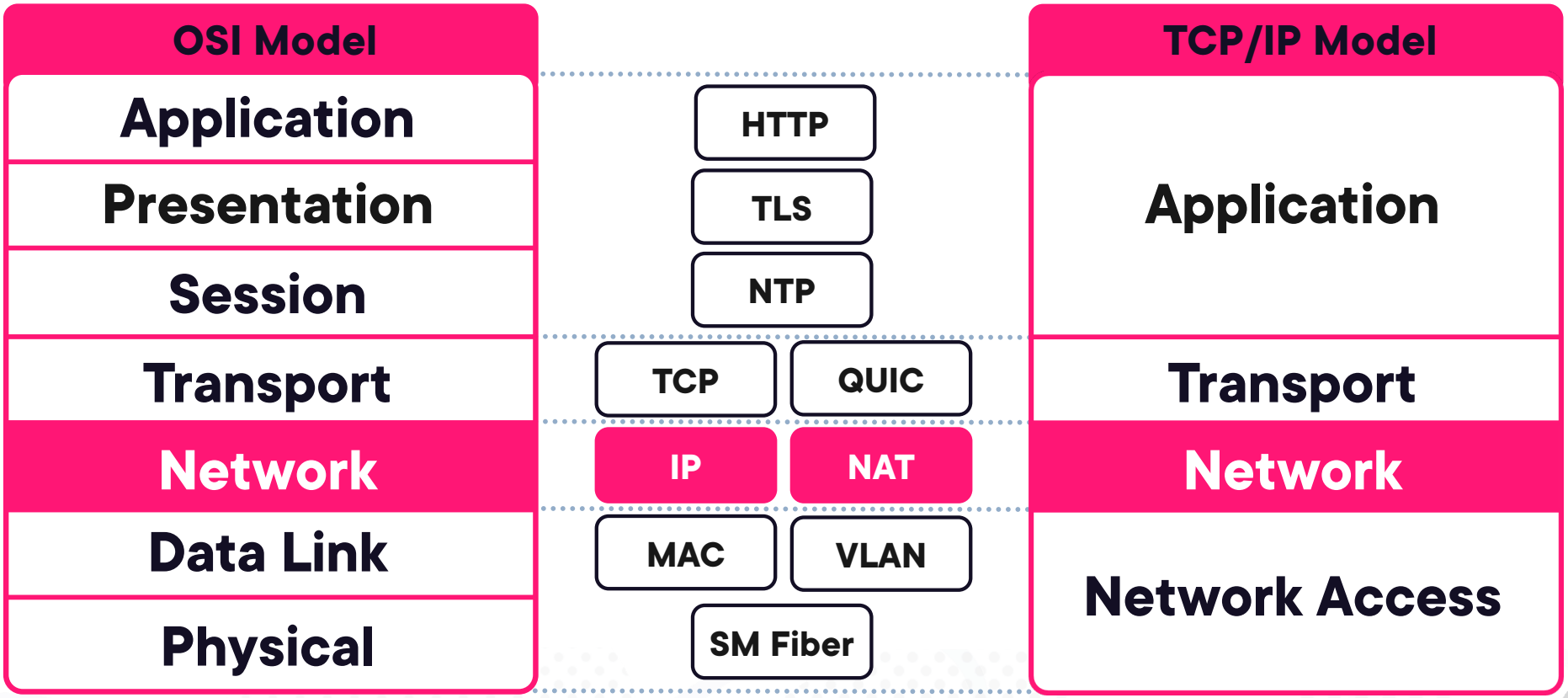
Network Layers



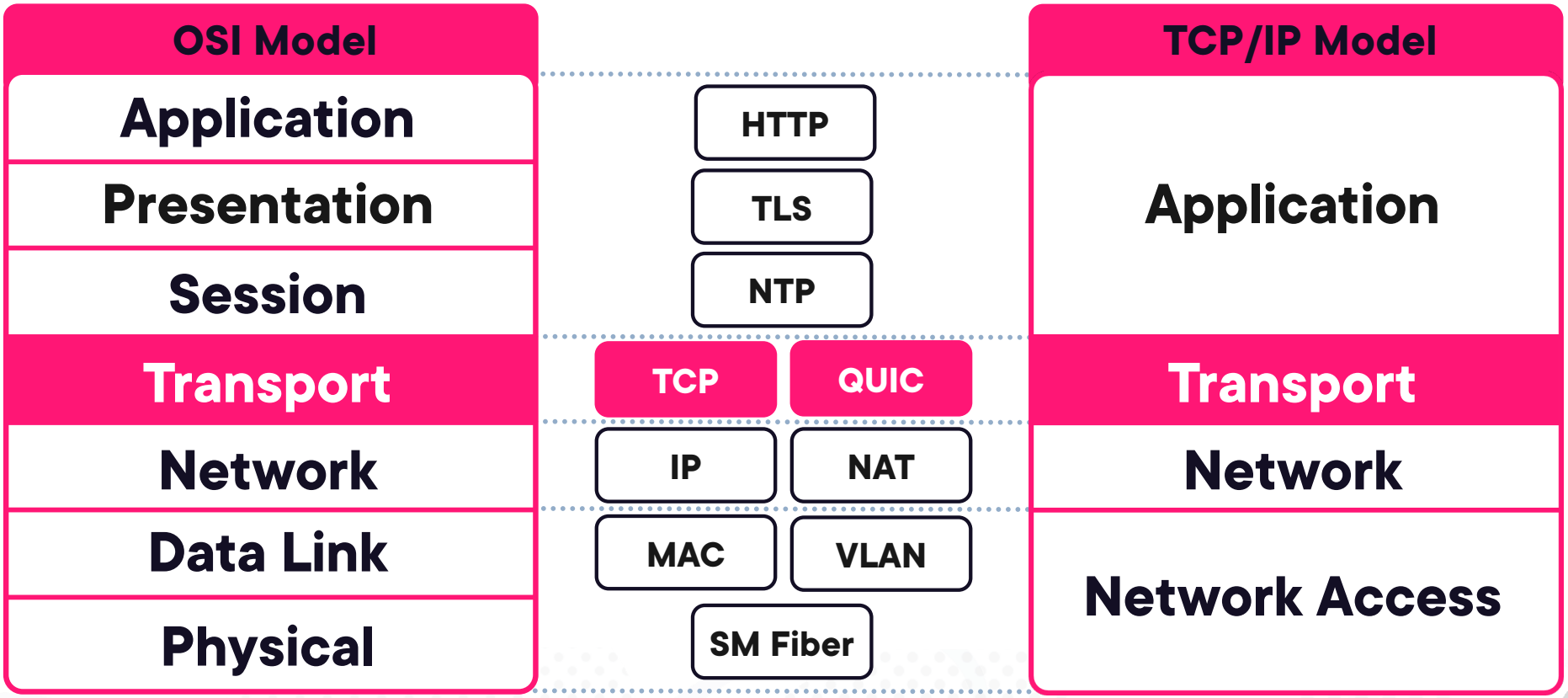
Network Layers



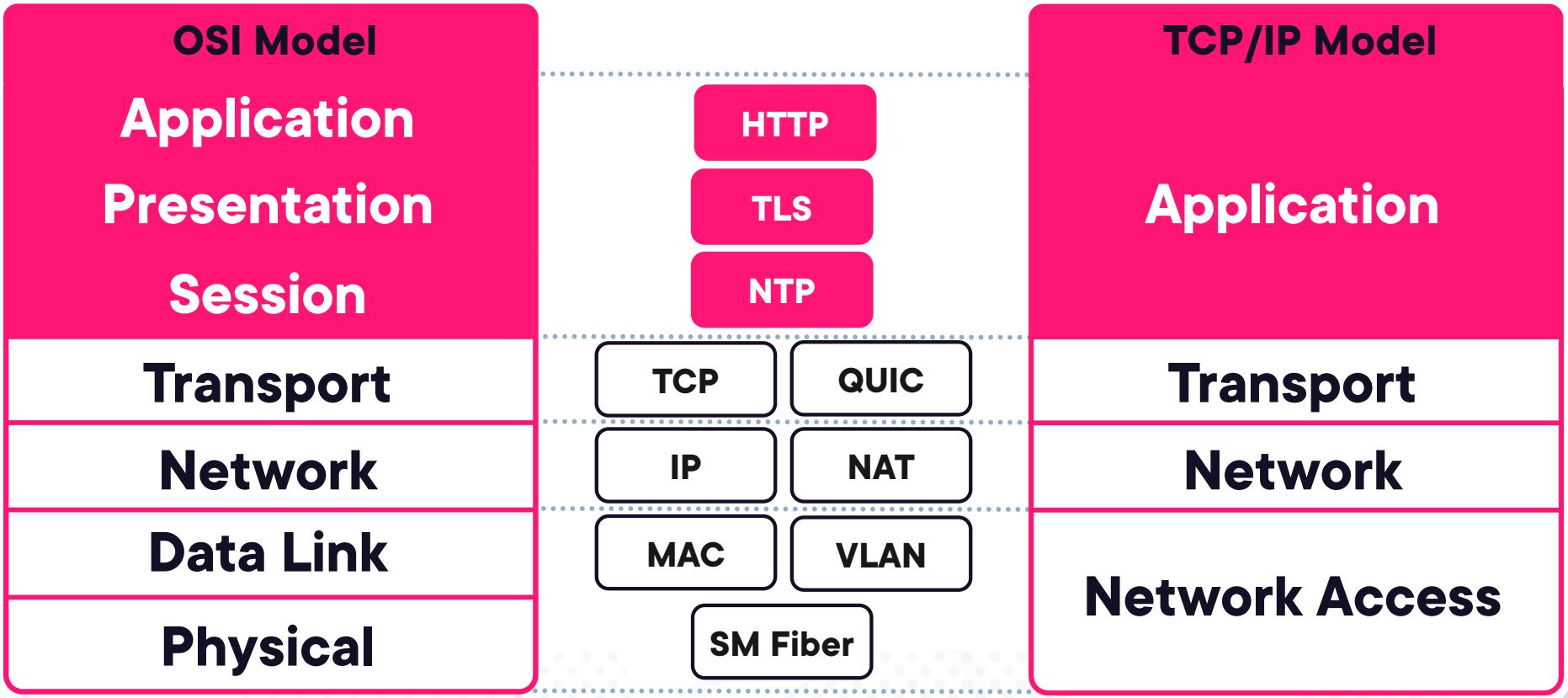
Network Layers



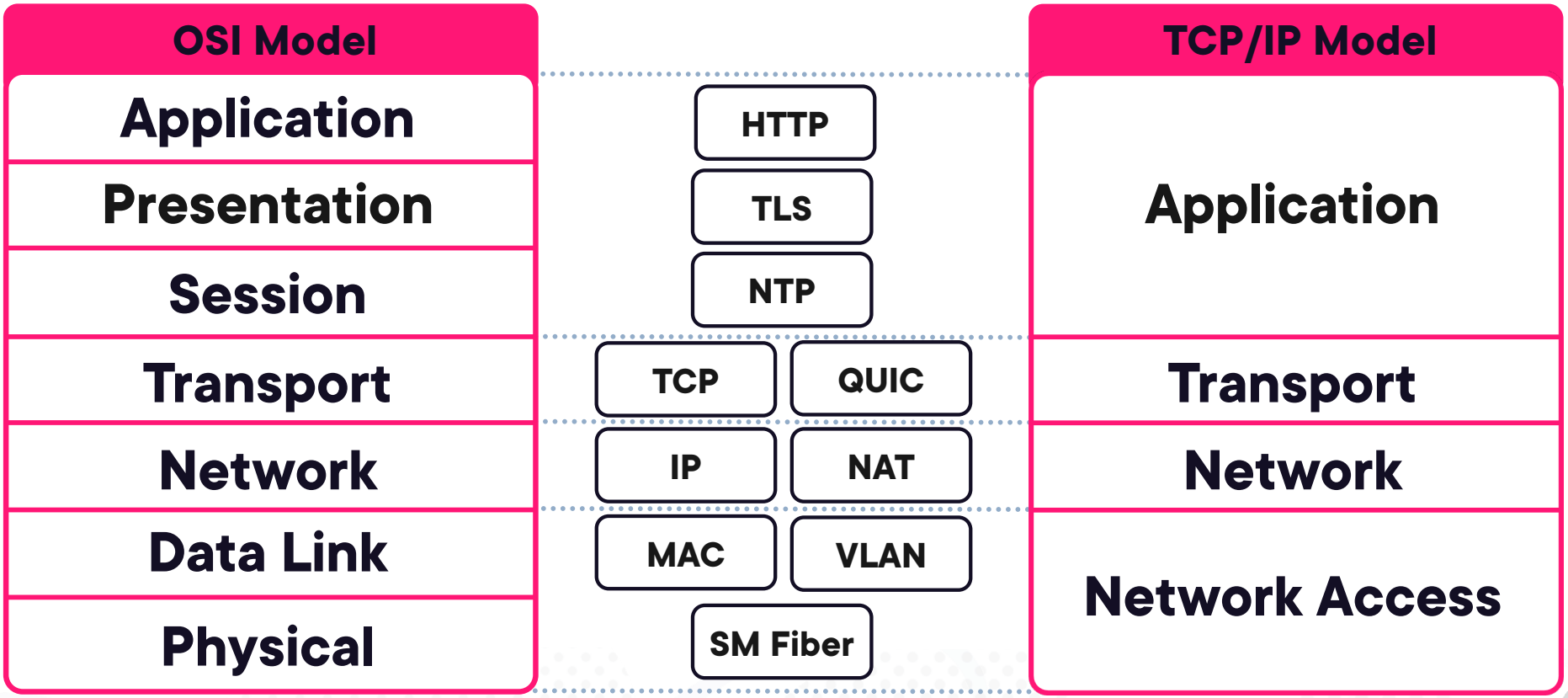
Network Layers



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 DCHP 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 DCHP 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

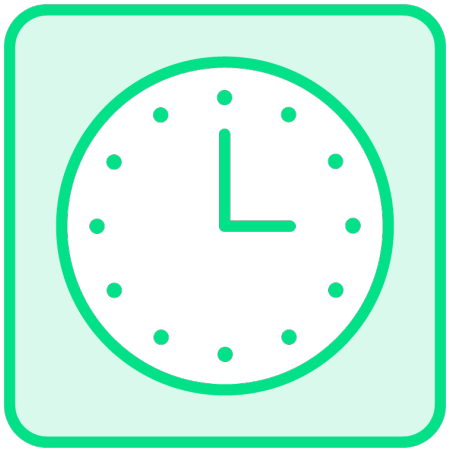
If you can connect via IP address but not DNS name, it's a problem with DNS

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

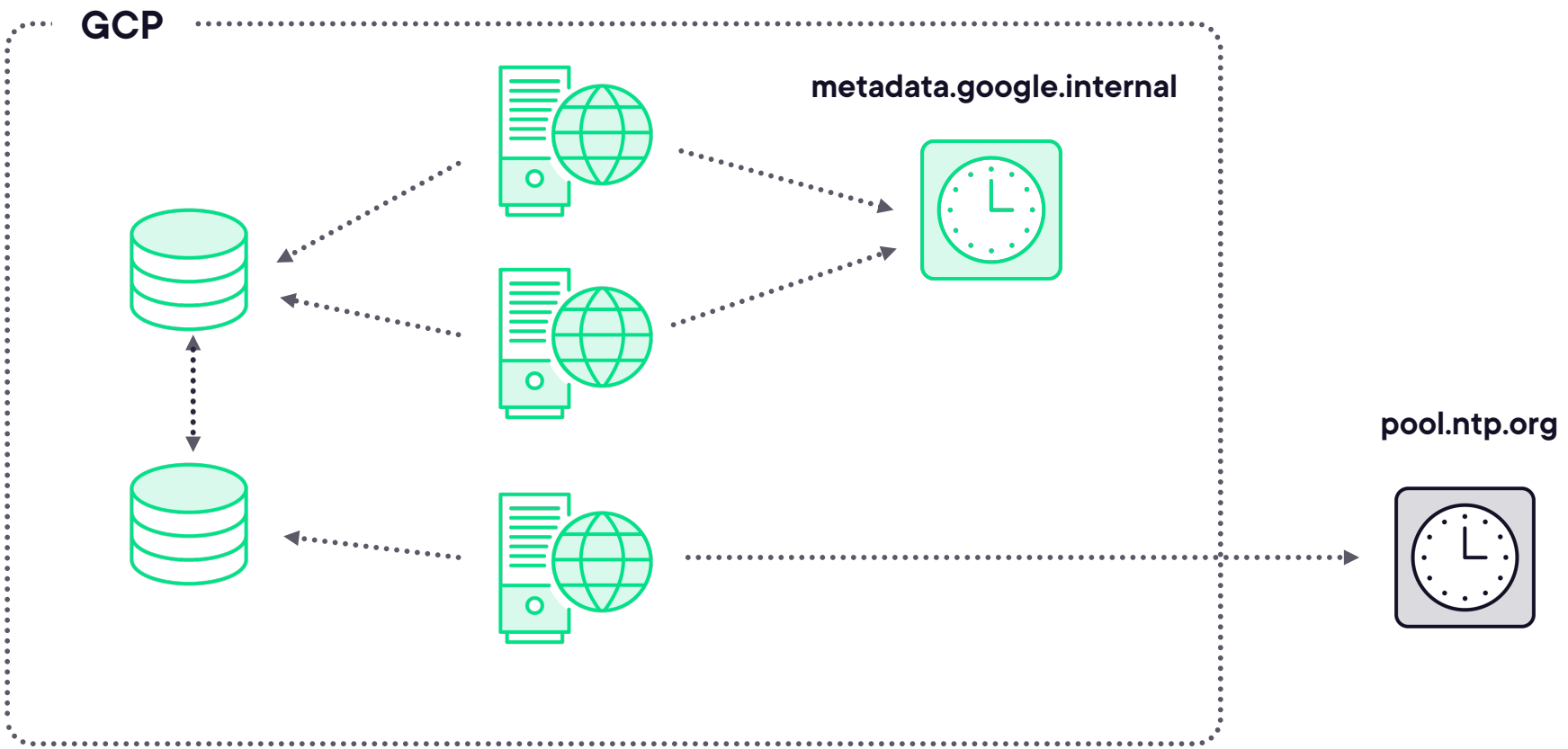


Correct time synchronization is important for time series databases

Reading logs from multiple systems is challenging when time is off

Read cloud provider documentation for NTP settings

NTP Issues



NTP Tips and Tricks

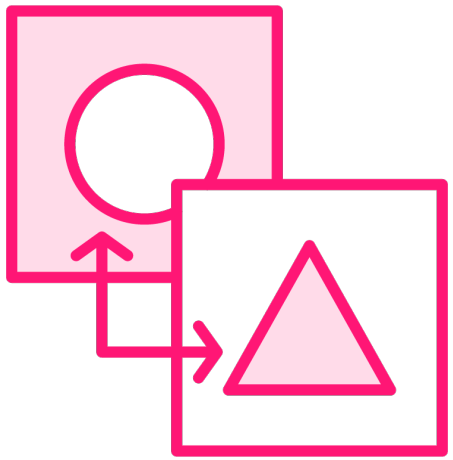
Use templates and infrastructure as Code (IaC) to keep settings from changing

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

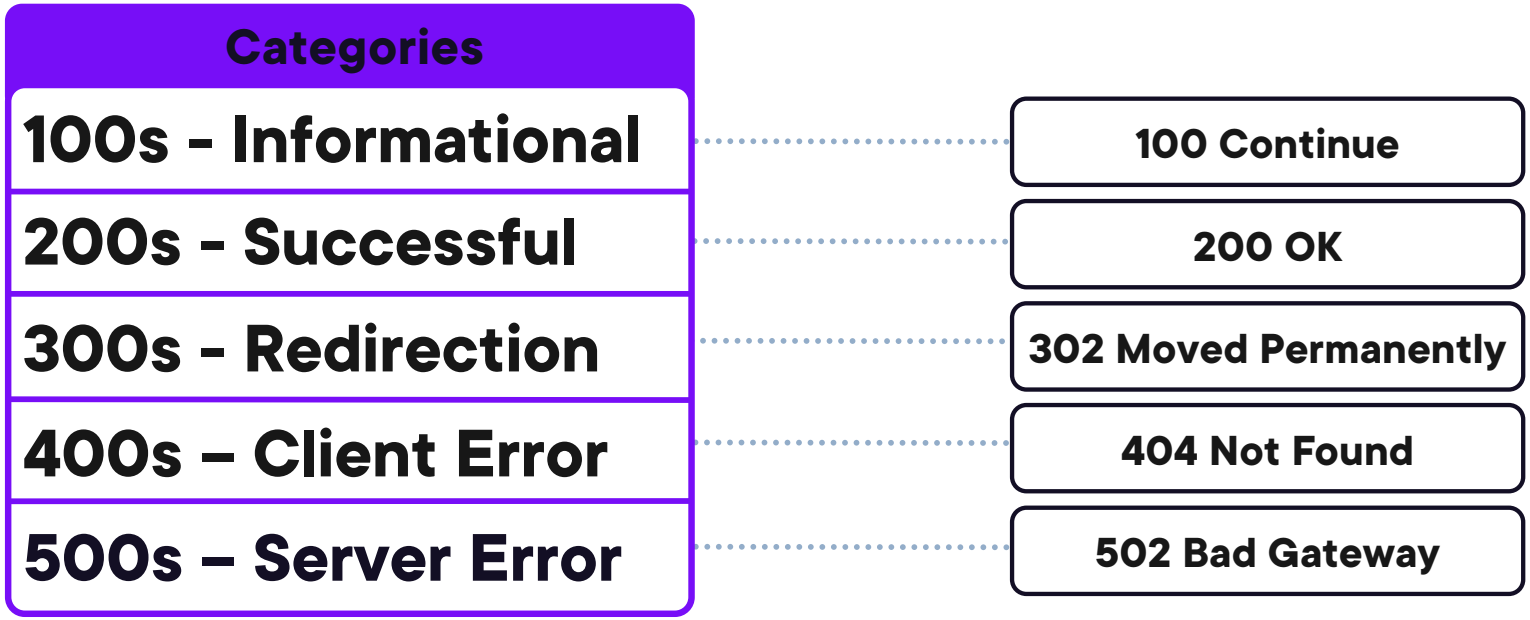
HTTP issues affect more than just website availability

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

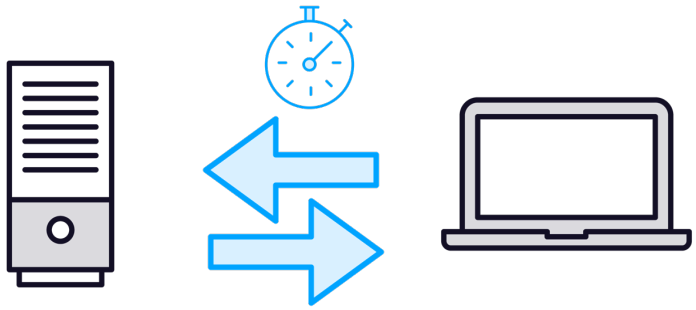
Ross Bagurdes

Understanding Latency and Bandwidth Issues

Latency and Bandwidth Comparison

Latency

Delay between sending and receiving

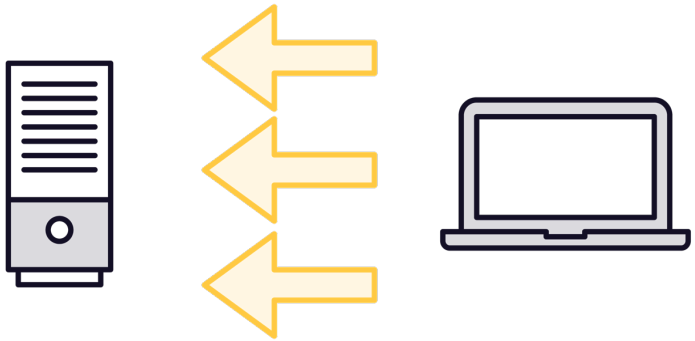


Tools: ping and traceroute(tracert)

VS.

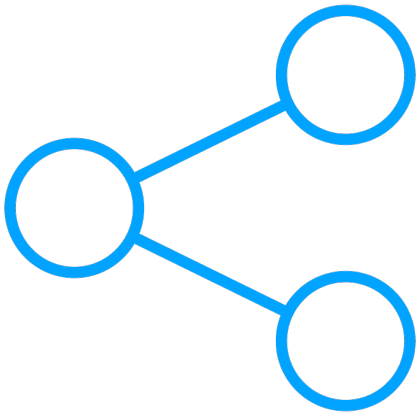
Bandwidth

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



Tools: iperf

Latency



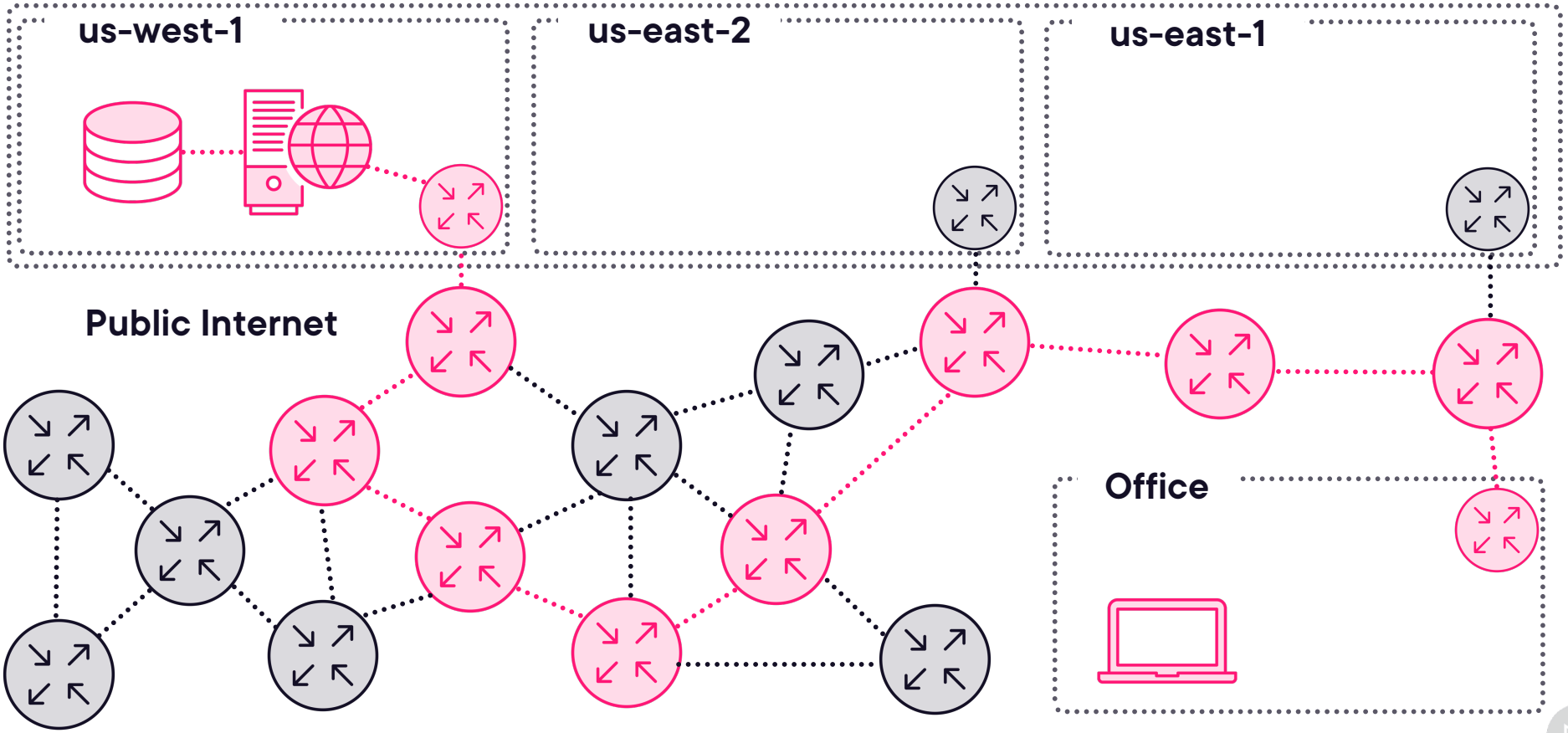
The farther a resource, the higher the latency

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

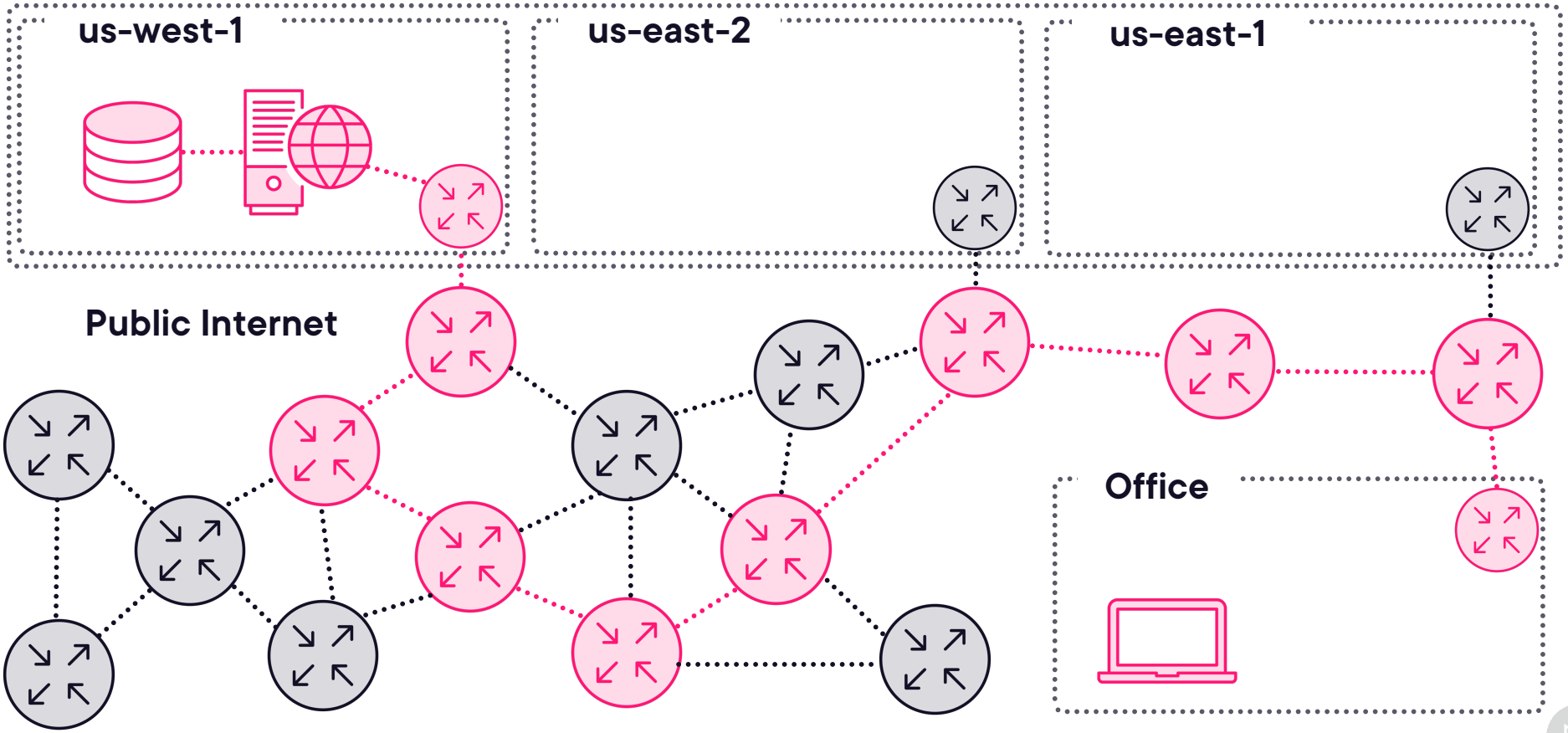
Use templates and scripts to build new resources, allowing only certain regions

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

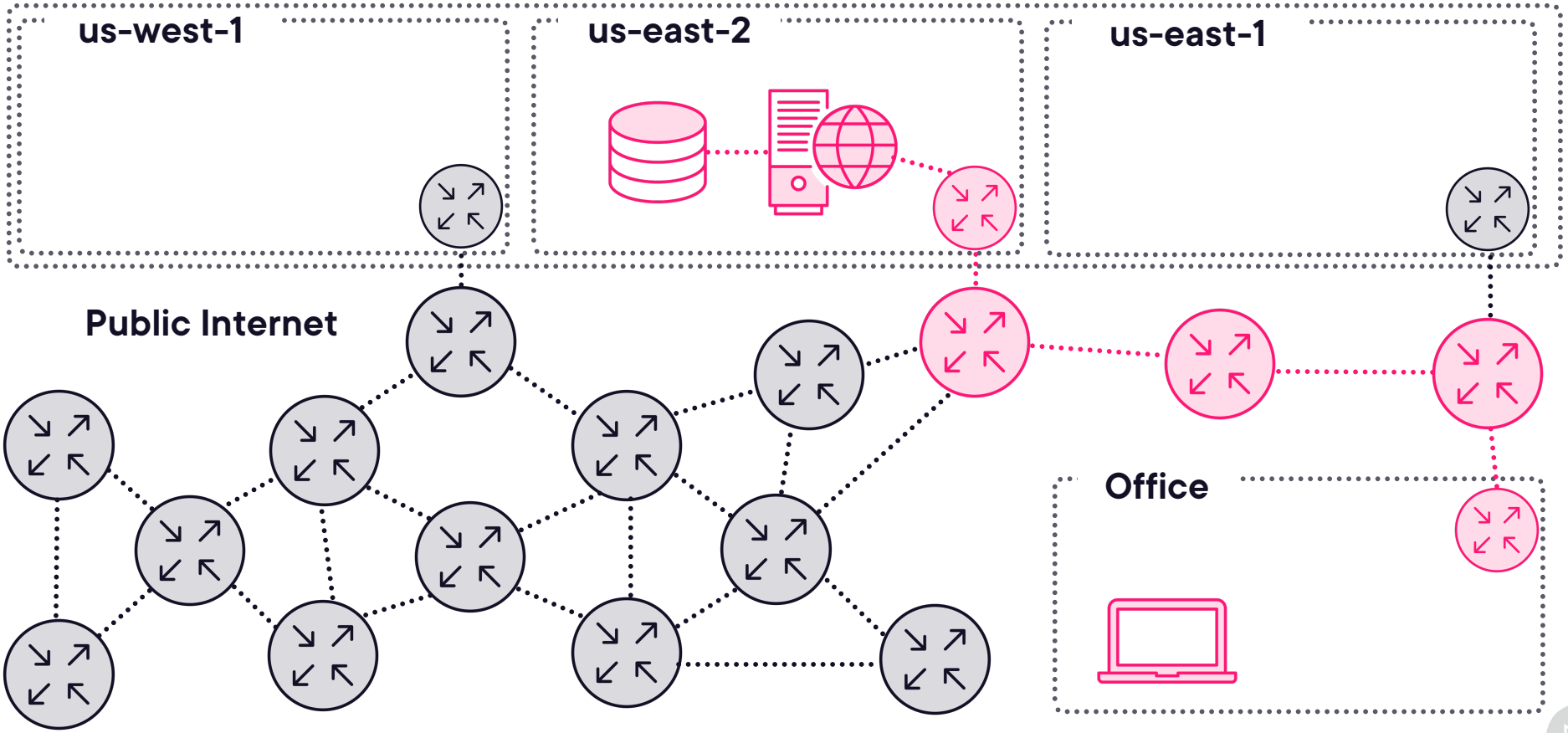
Latency Issues



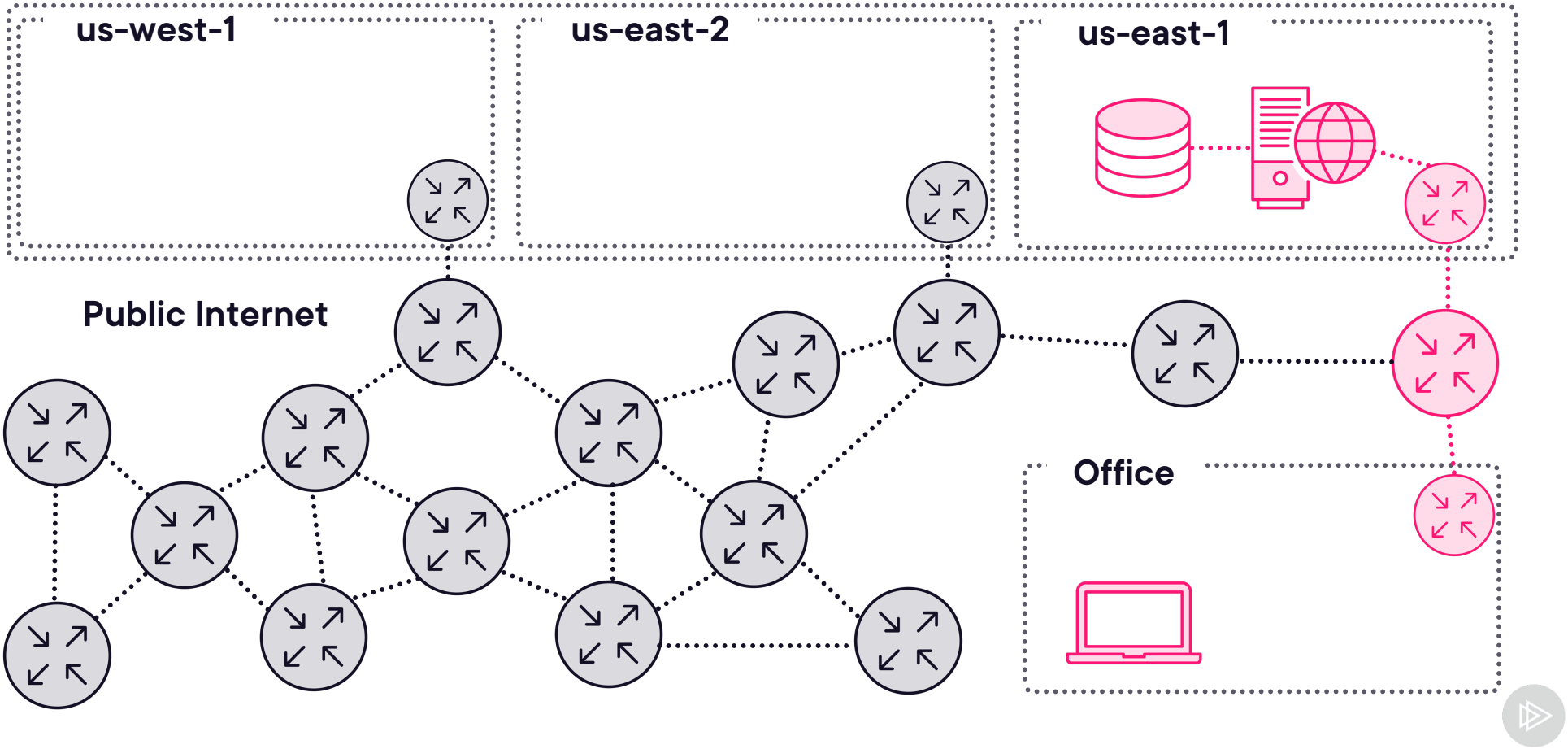
Latency Issues



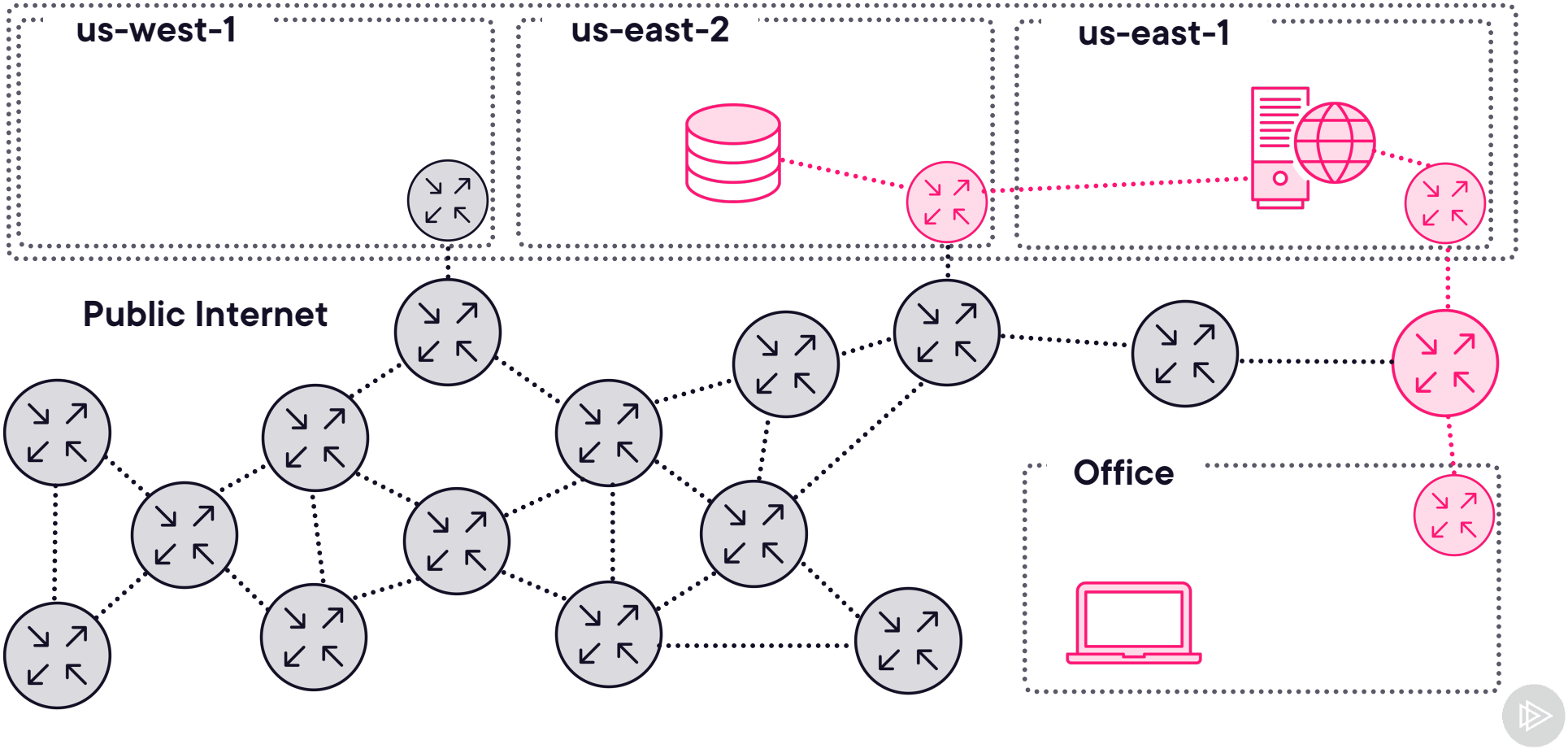
Latency Issues



Latency Issues



Resources Deployed in Separate Regions



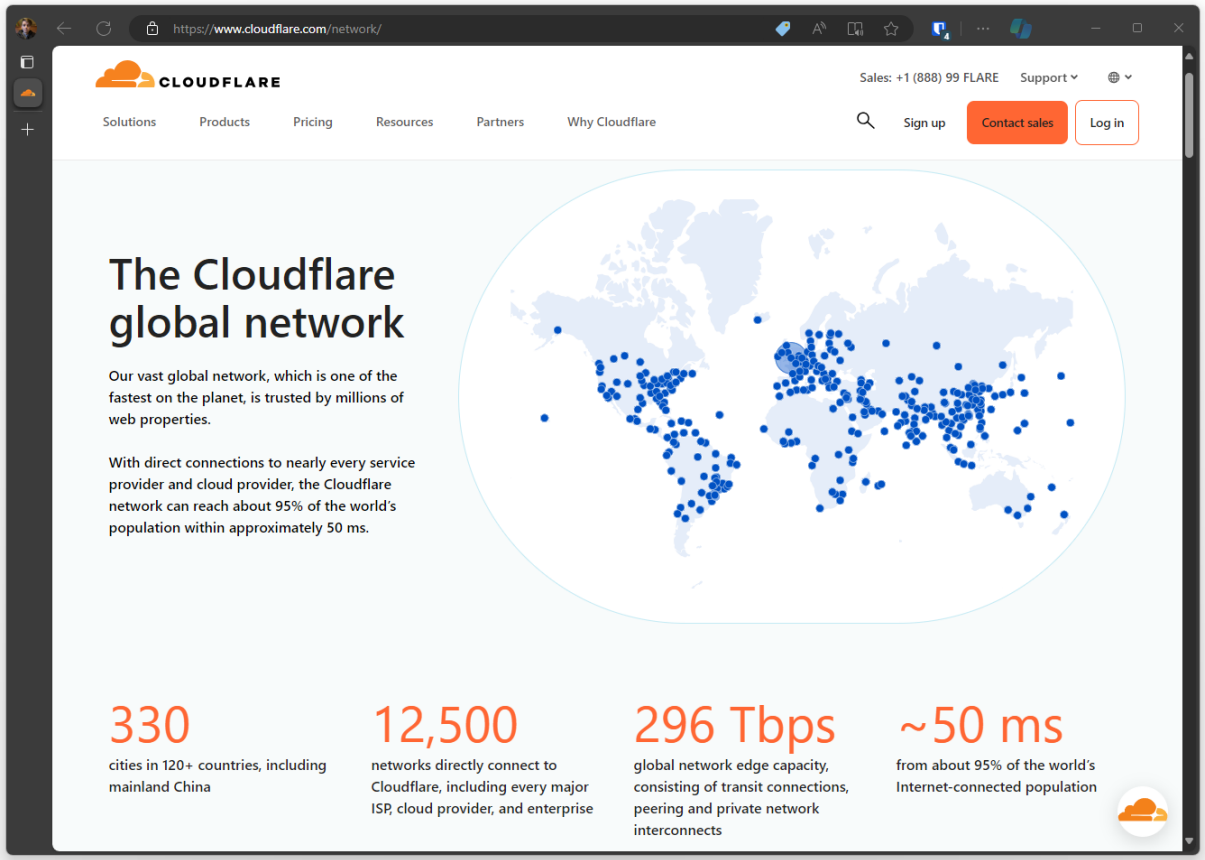
Tools to Fix Bandwidth and Latency Issues

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

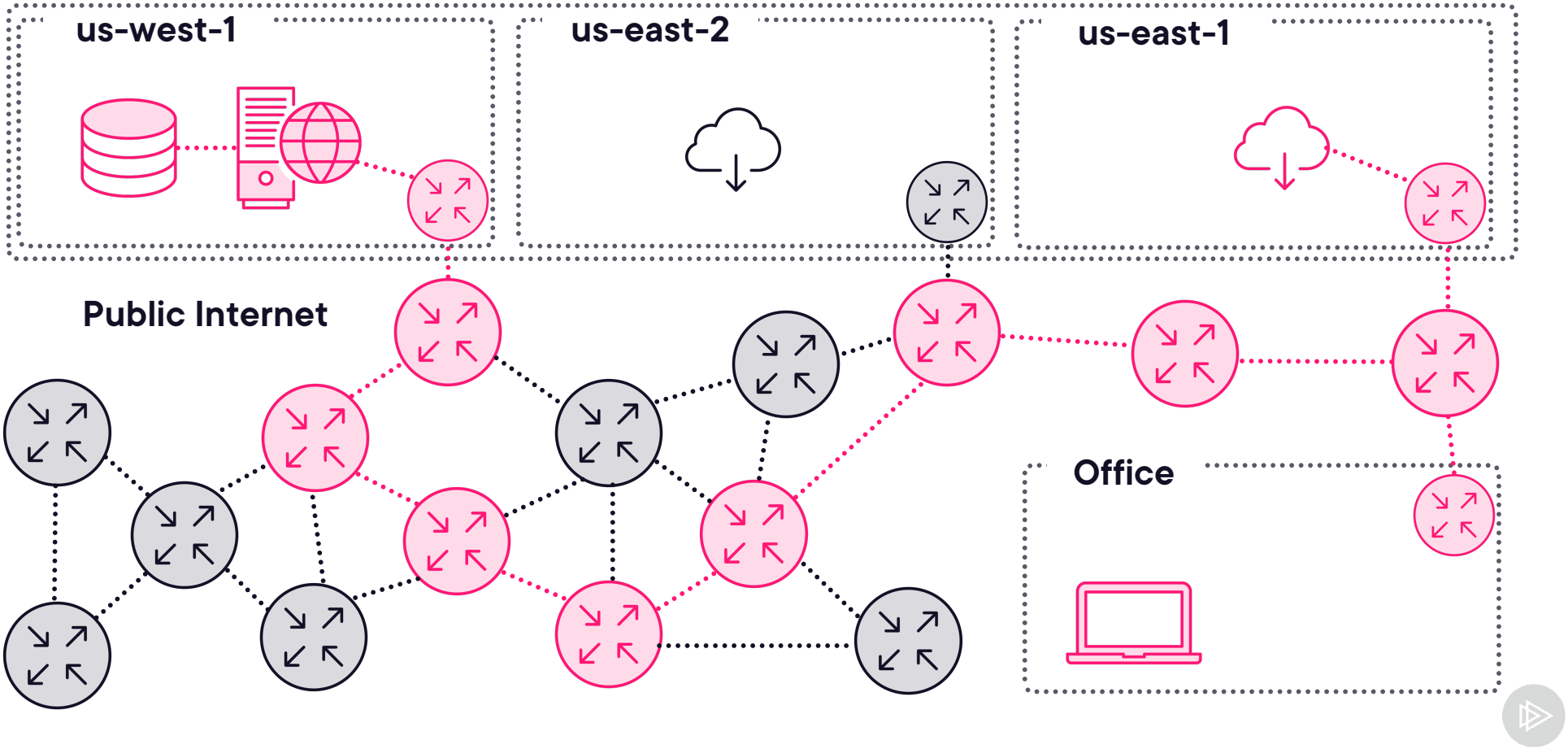
Edge compute using serverless functions at the edge

Scaling horizontally allows for better bandwidth sharing

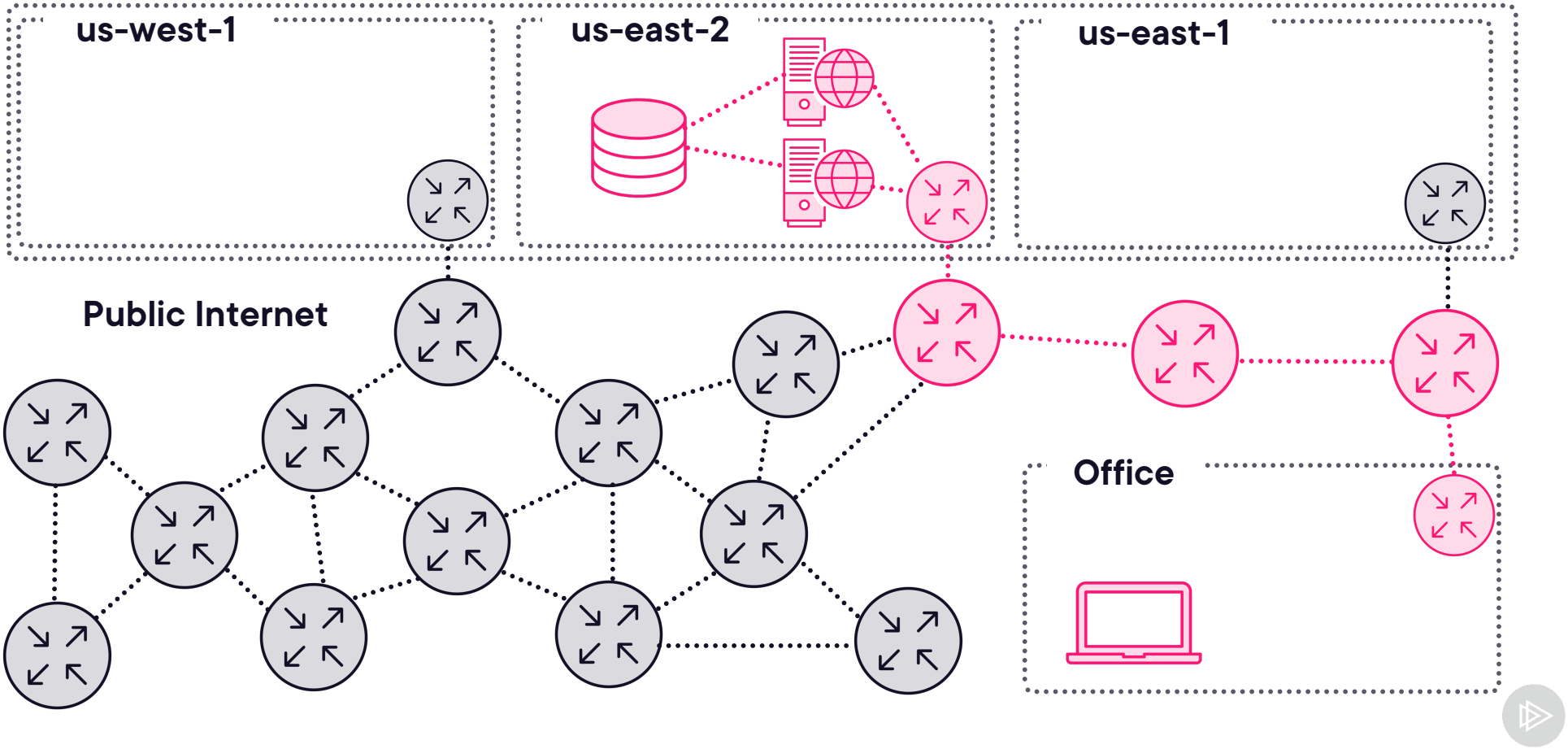
Content Delivery Network (CDN)



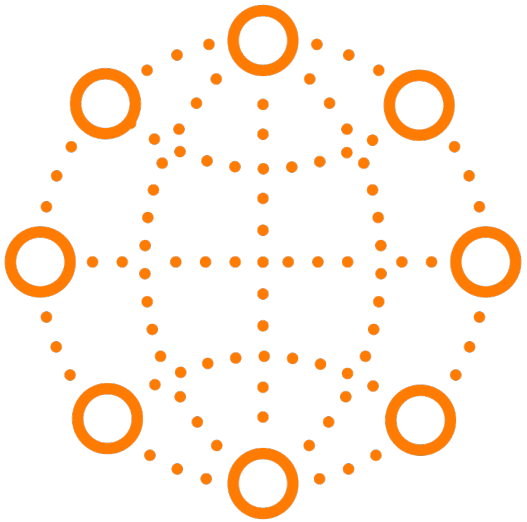
Content Delivery Network (CDN)



Scaling Horizontally



Global Traffic Management



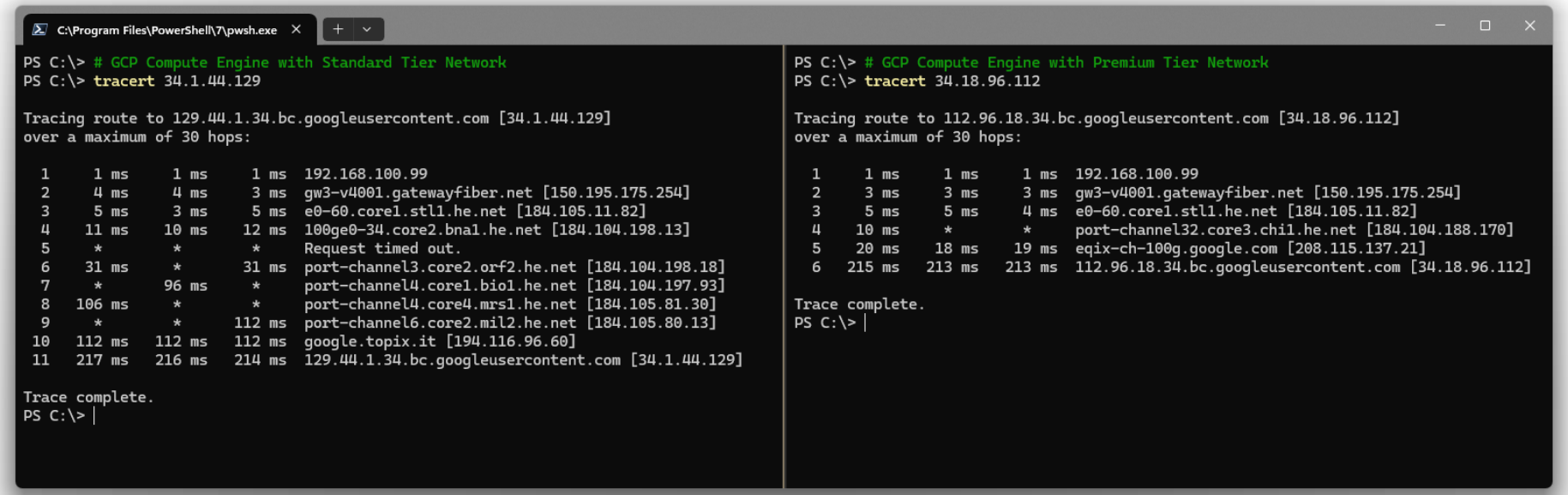
Routes traffic using cloud provider's private network instead of public internet

Can be used for global load balancing

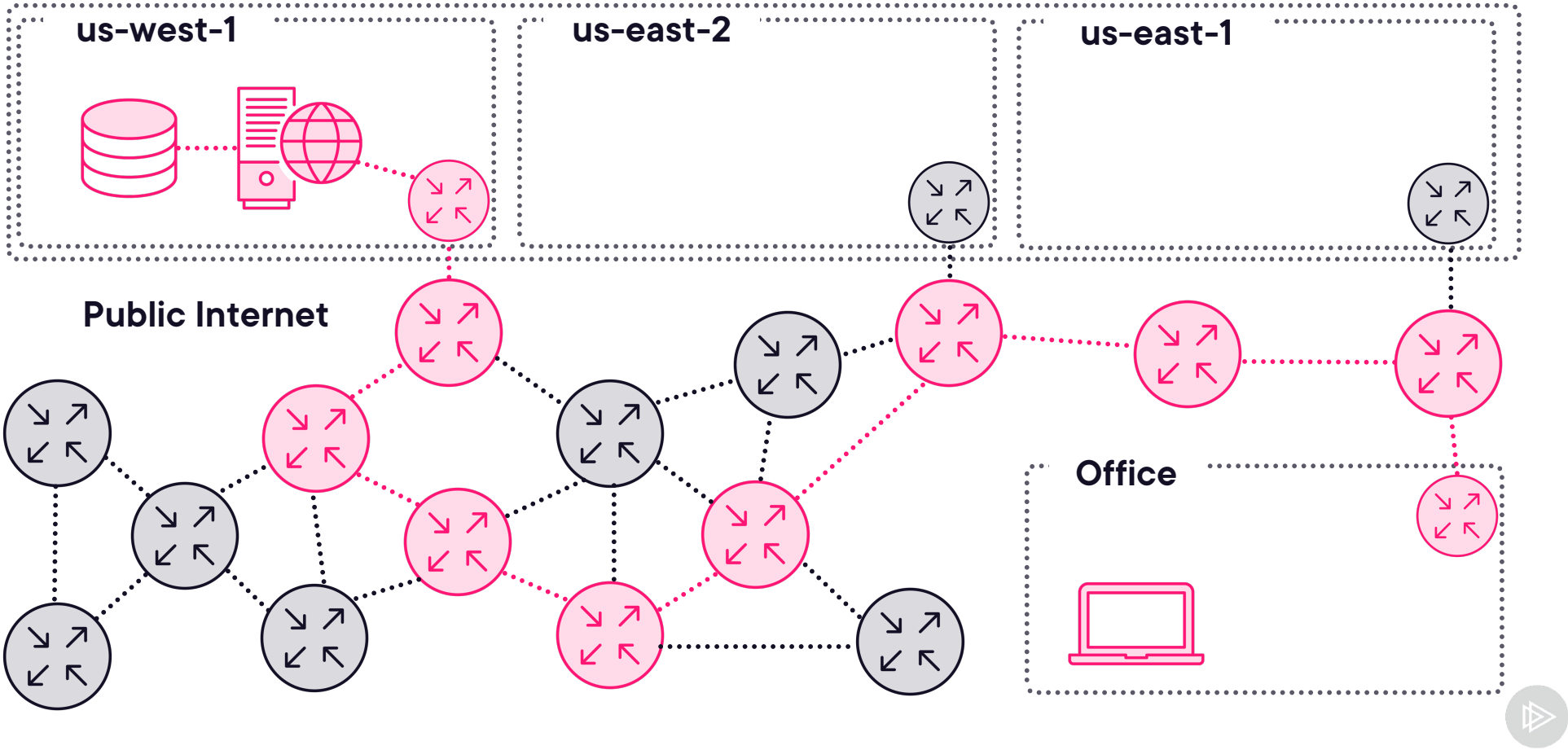
Examples of this type of service

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

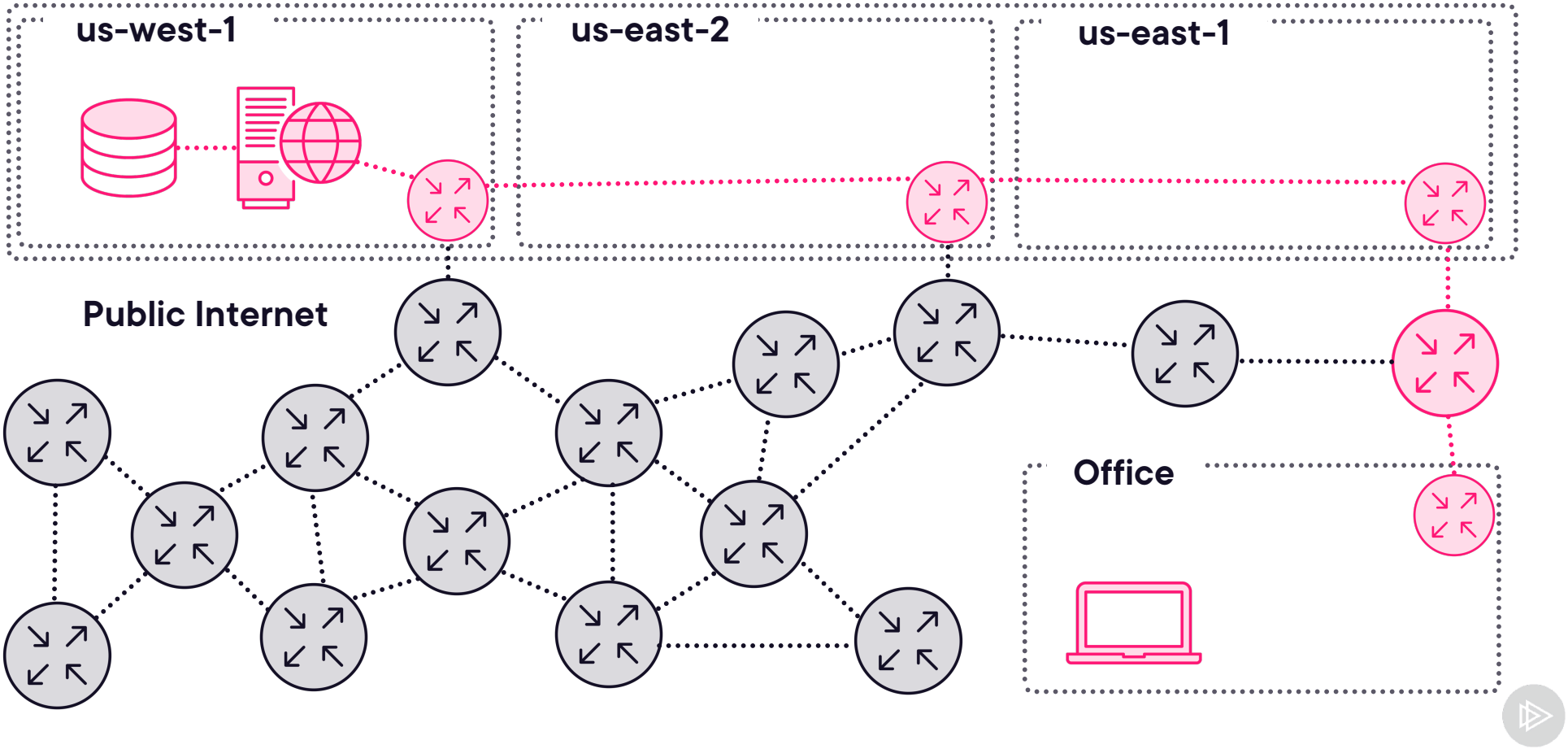
Global Traffic Management

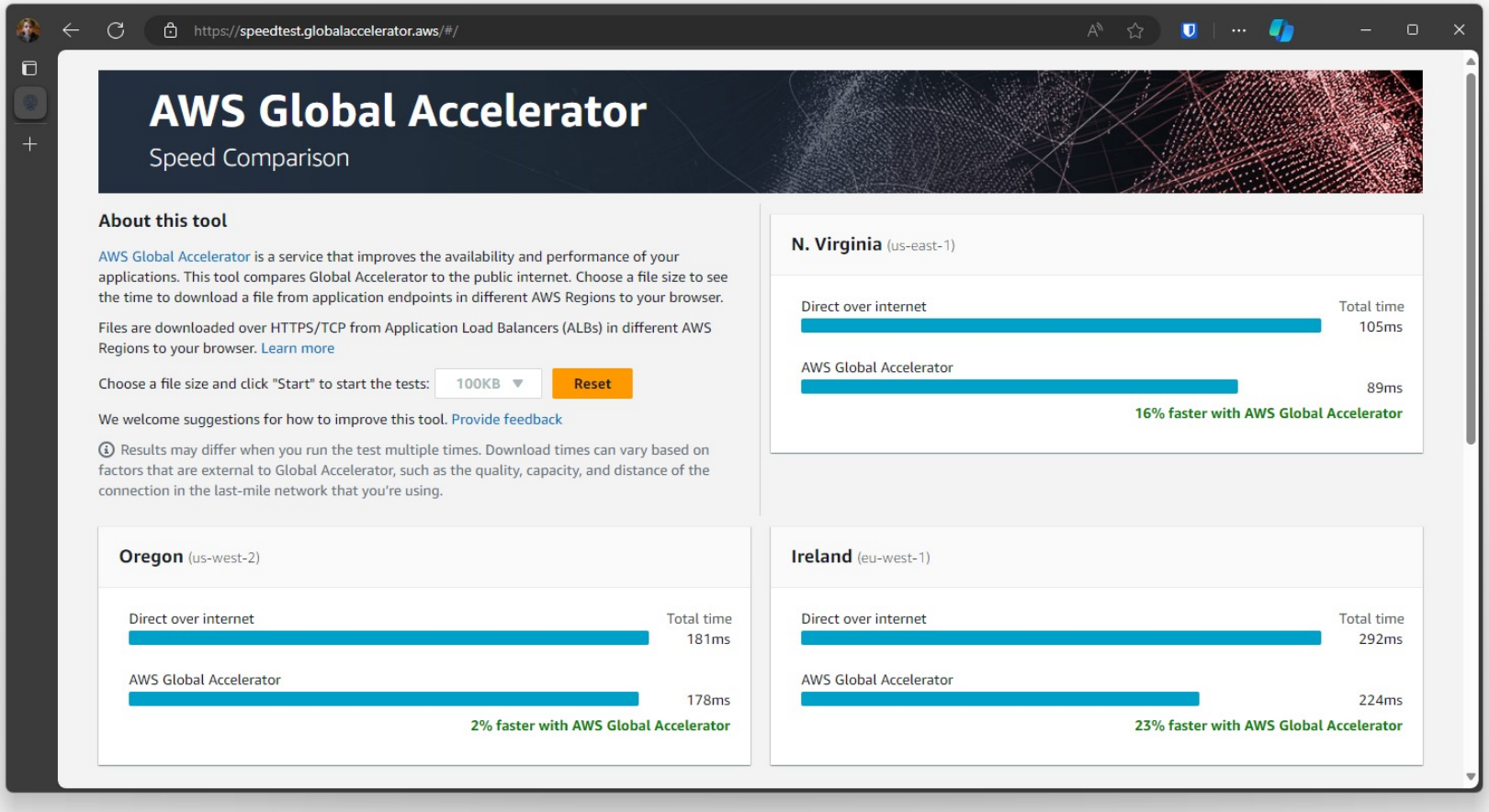


Global Traffic Management



Global Traffic Management





https://speedtest.globalaccelerator.aws/

Direct Cloud Connectivity

Dedicated connection to the cloud, bypassing public internet

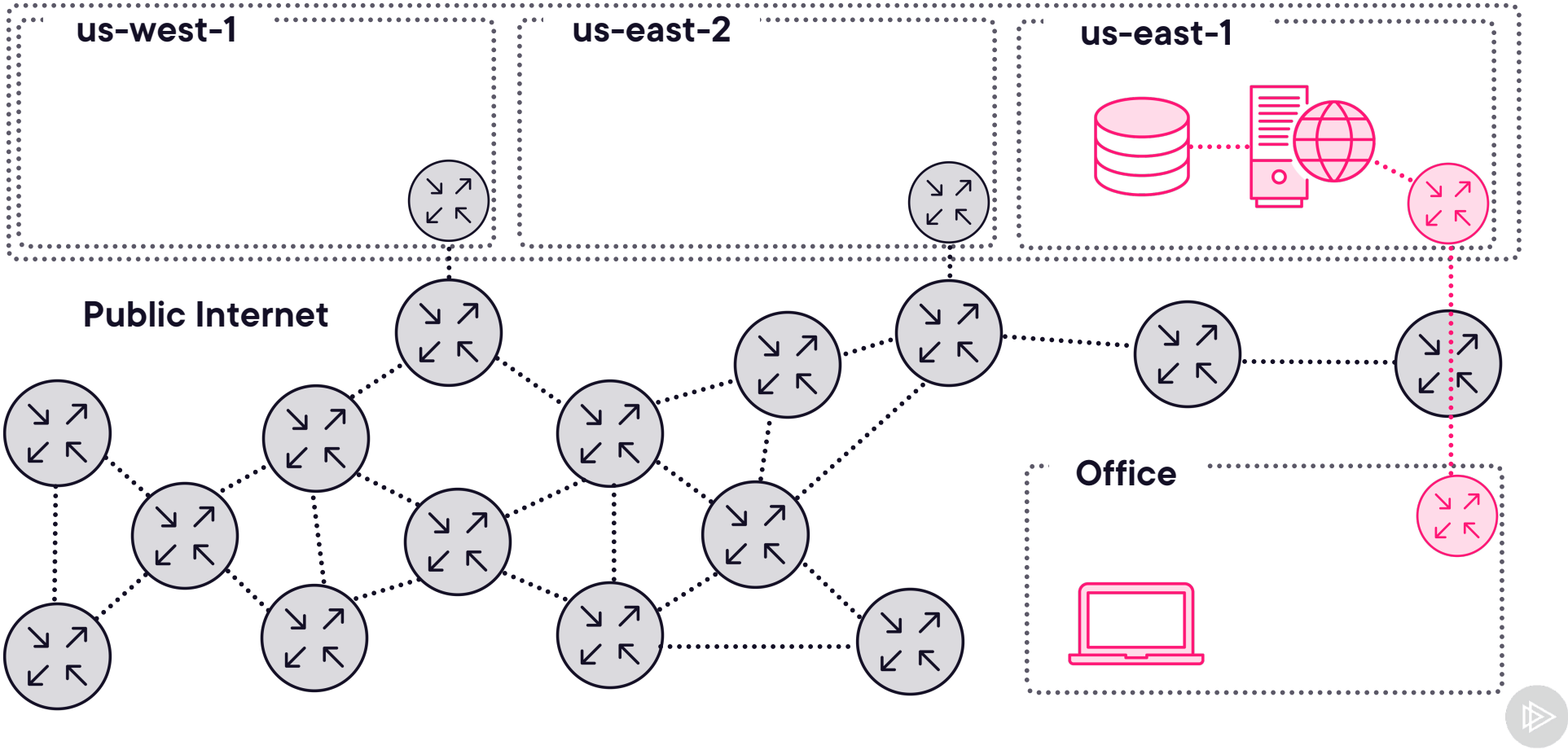
Optimizes traffic between on-premise and the cloud

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



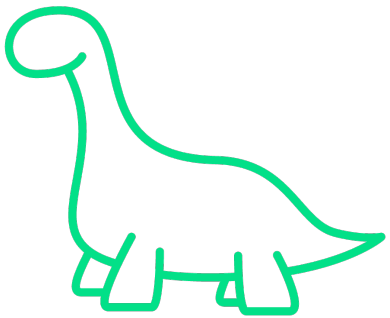
Get Hands On

Build a Bandwidth Monitoring Tool with iPerf and PowerShell

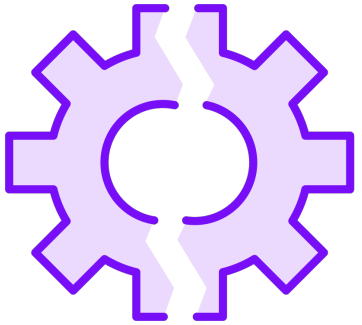
Adam Bertram

Protocol Problems

Protocol Issues



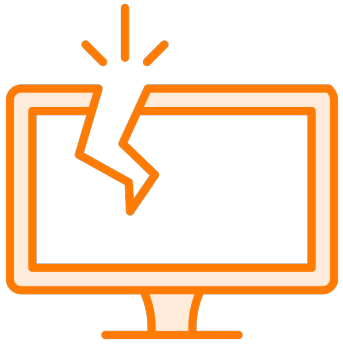
Deprecated Protocol
Old and Insecure protocols tend to be deprecated



Incompatible Protocols
Some cloud providers may be incompatible with certain protocols

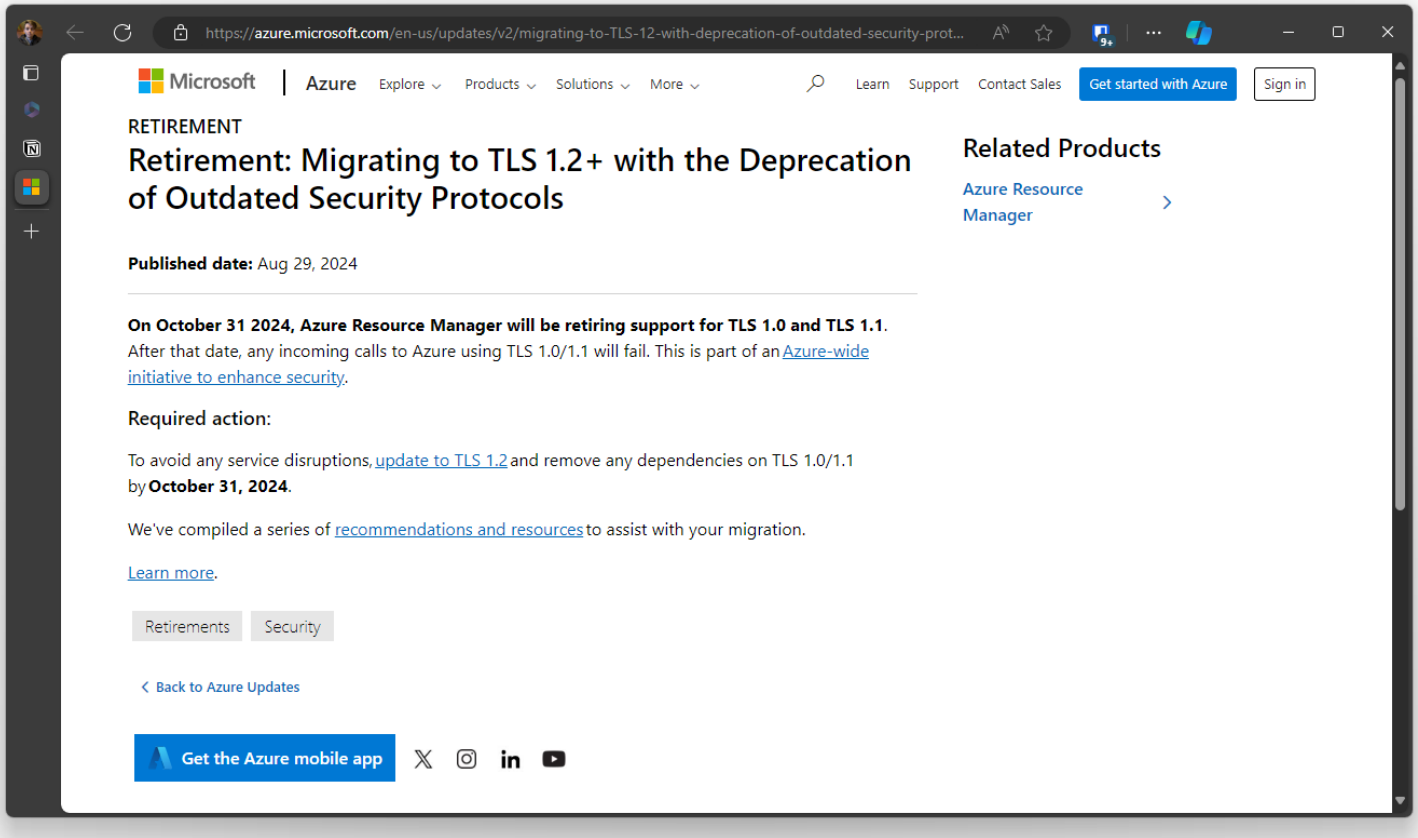
Signs of Protocol Problems

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



Solving Protocol Deprecations/Incompatibilities

Keep up to date on announcements of features and platform changes

Set alerts and monitor protocol lifecycles in cloud environments

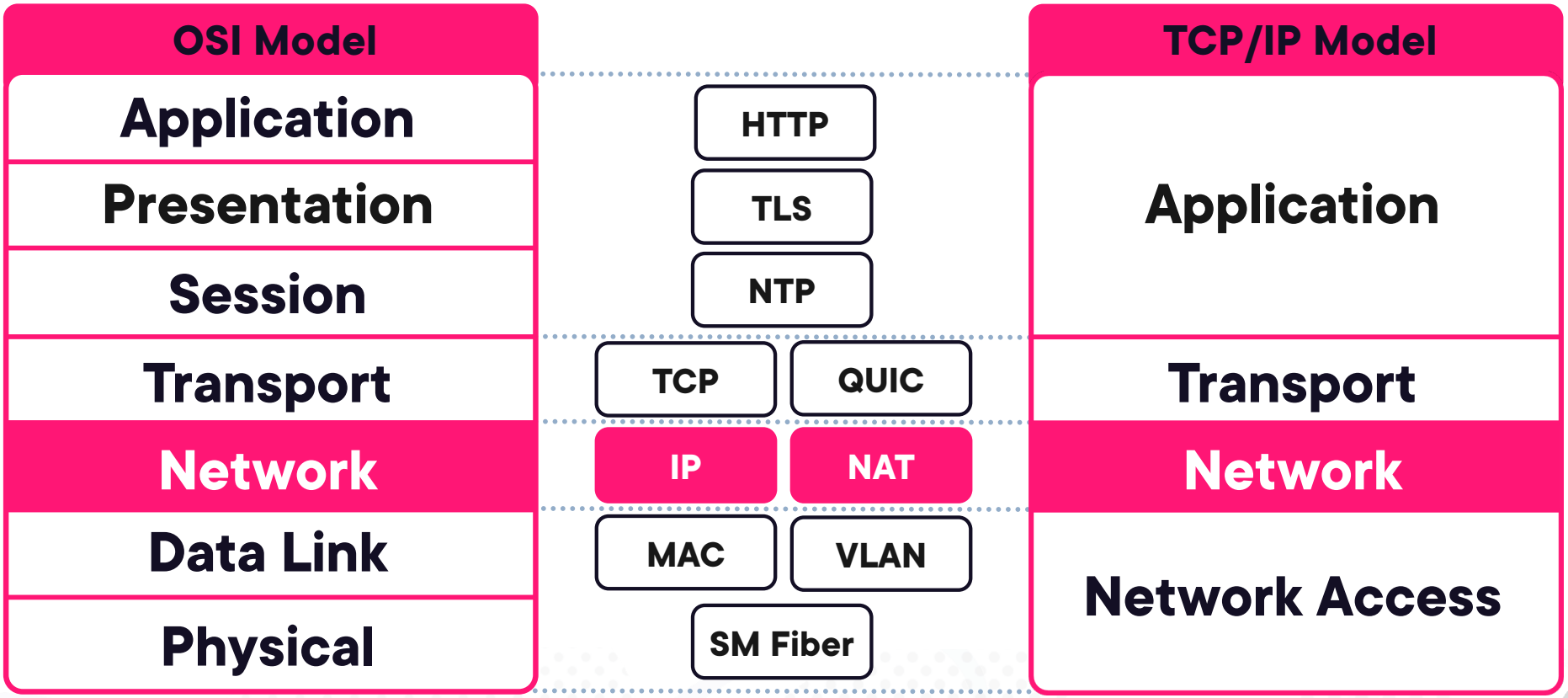
Audit your environment for protocols that you may be unaware you are using.

Plan and test a migration of the protocol

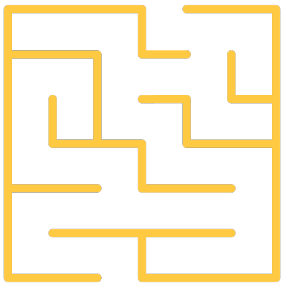
Reading the documentation about the supported protocols will help prevent issues that arise from trying to use them

Troubleshooting Routing in Cloud Networks

Network Layers



Issues That Arise from Bad Routes



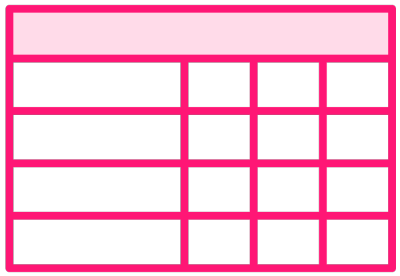
Unreachable Networks

Misconfigured routes can make a network unreachable

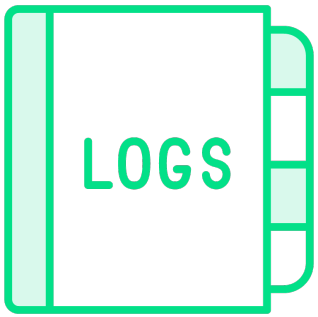
Latency Issues

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

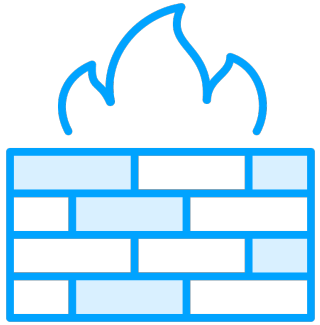
Troubleshoot Routes



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

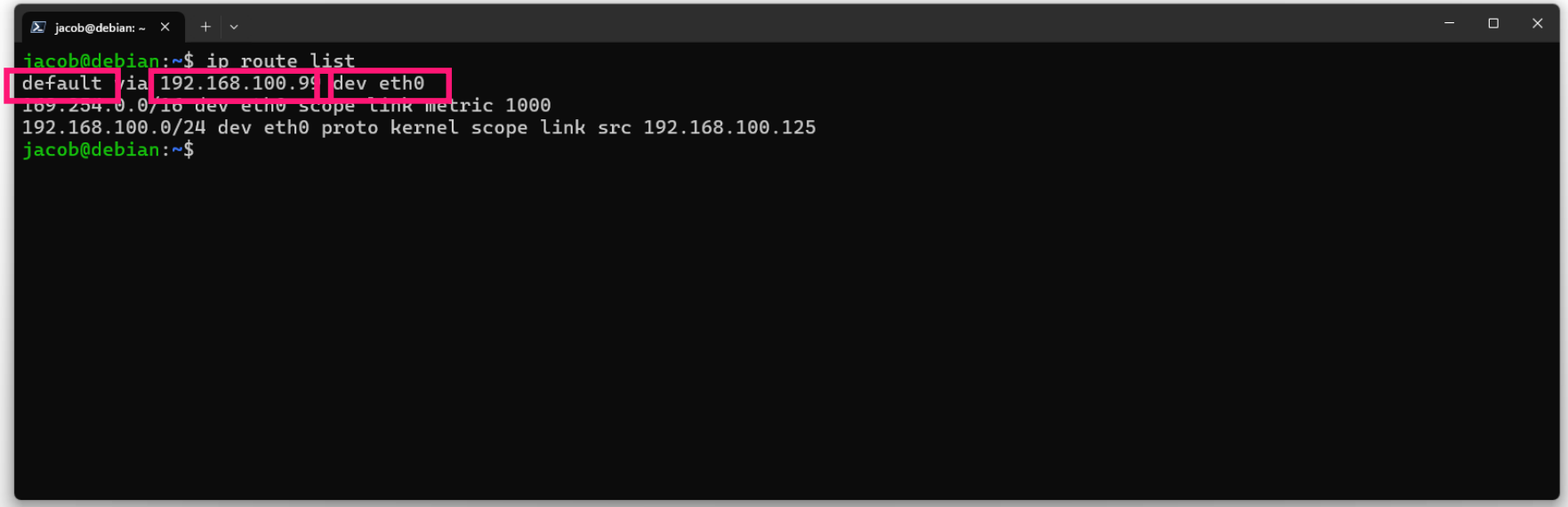
Static Routes

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

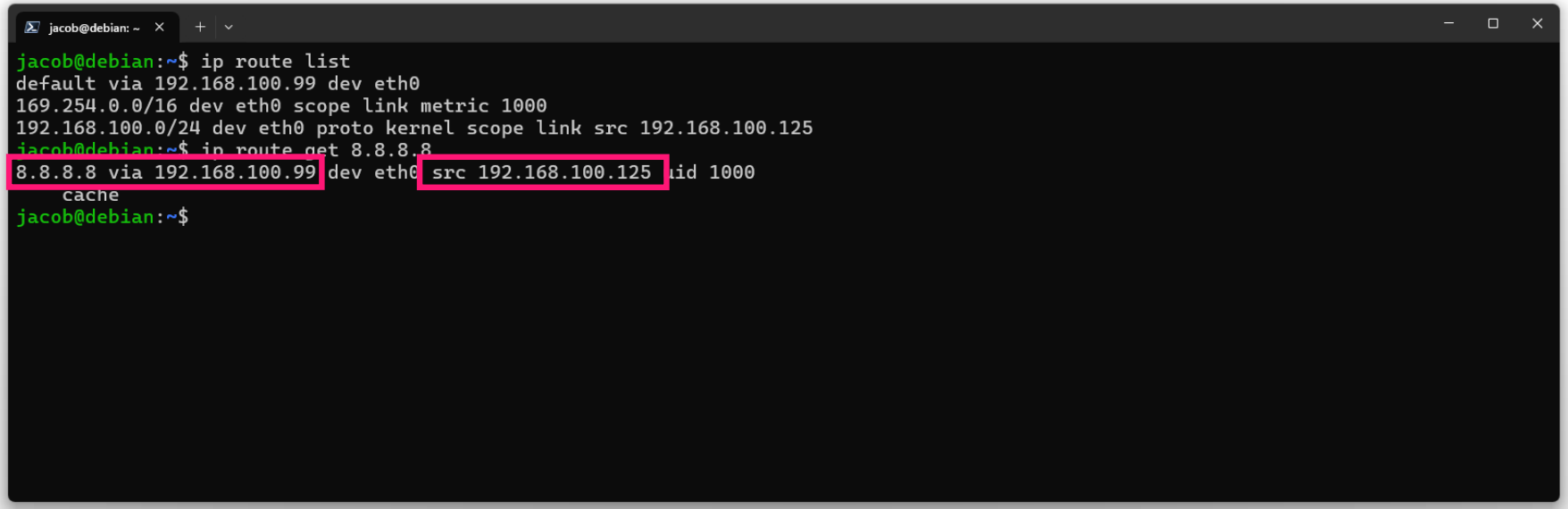
Dynamic Routes

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

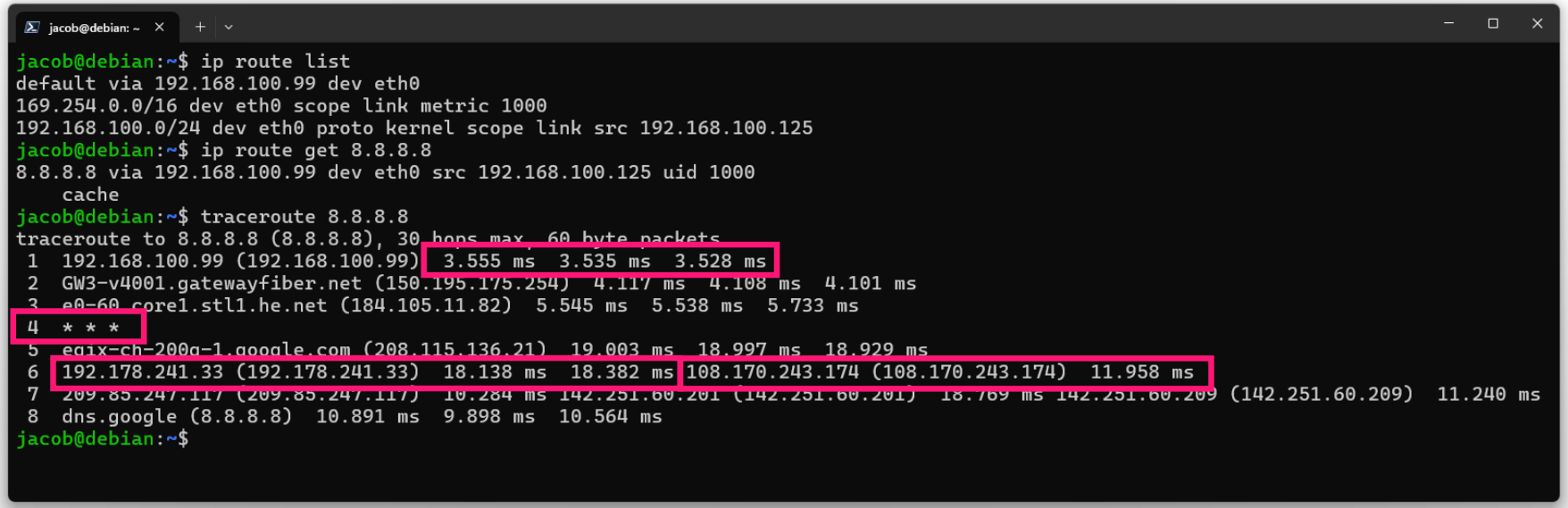
Troubleshooting Routes on a VM



Troubleshooting Routes on a VM



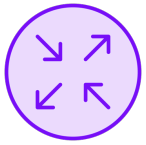
Troubleshooting Routes on a VM



Checking Routes Across the Cloud

On the virtual network or the subnet

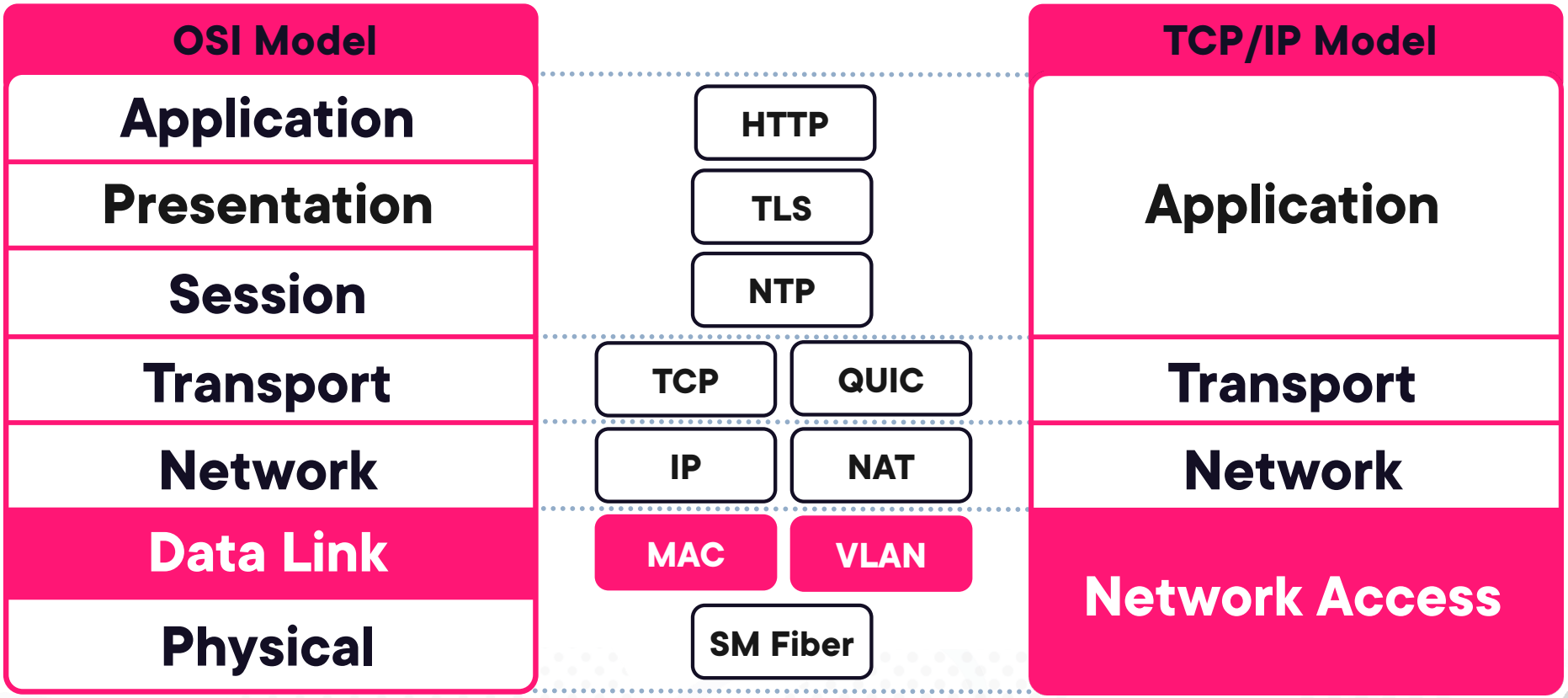
On network security groups



On cloud gateways and routers

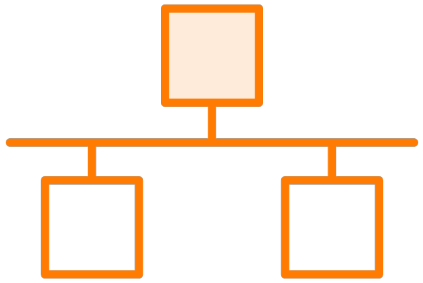
Identifying Network Switching Problems

Network Layers



Network Switching Problems

Virtual LAN (VLAN) Issues
Issues caused by misconfigured VLAN tags



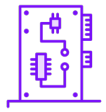
Switch Port Issues
Issues caused the misconfiguration of network trunk and access ports

Key VLAN Terms

Virtual LAN (VLAN) – A virtual layer 2 network

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

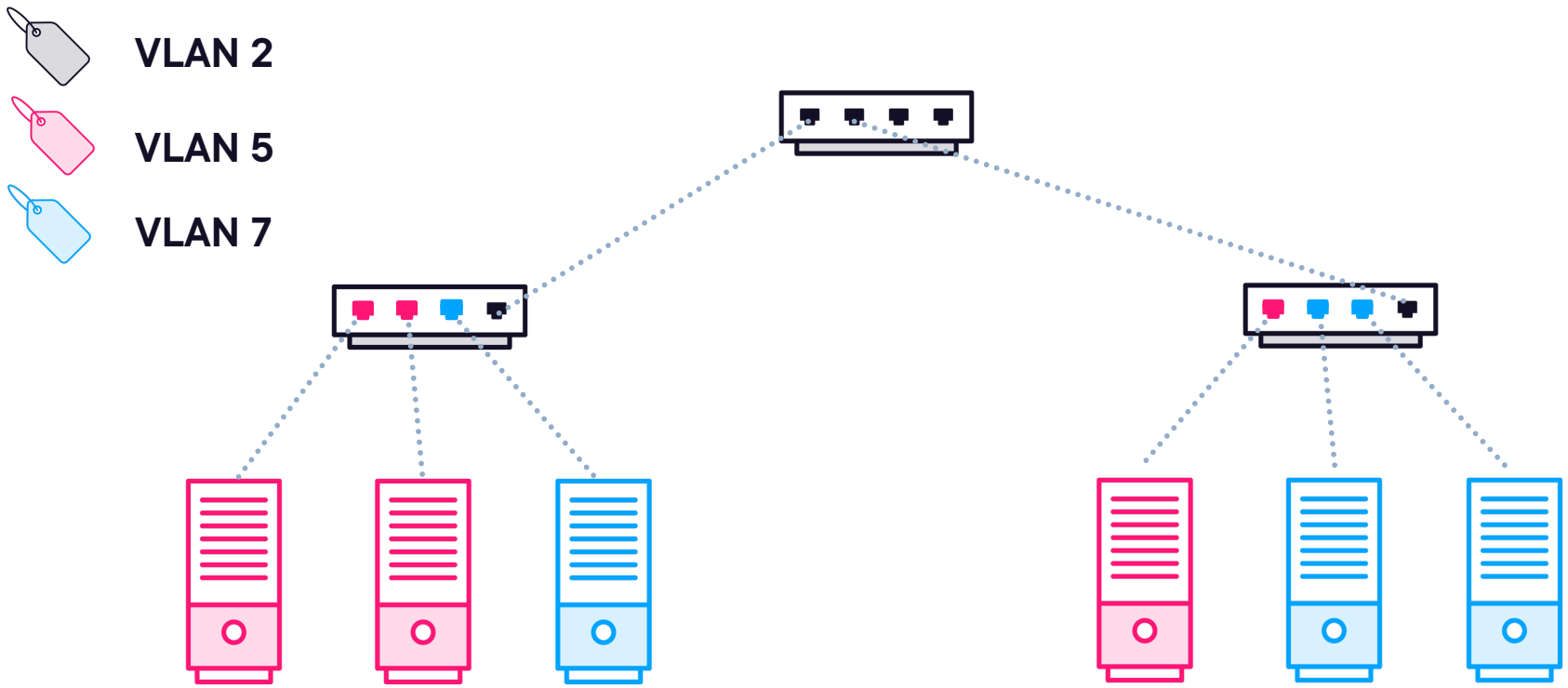
Trunk Port – A switchport that carries traffic for all (or some) VLANs



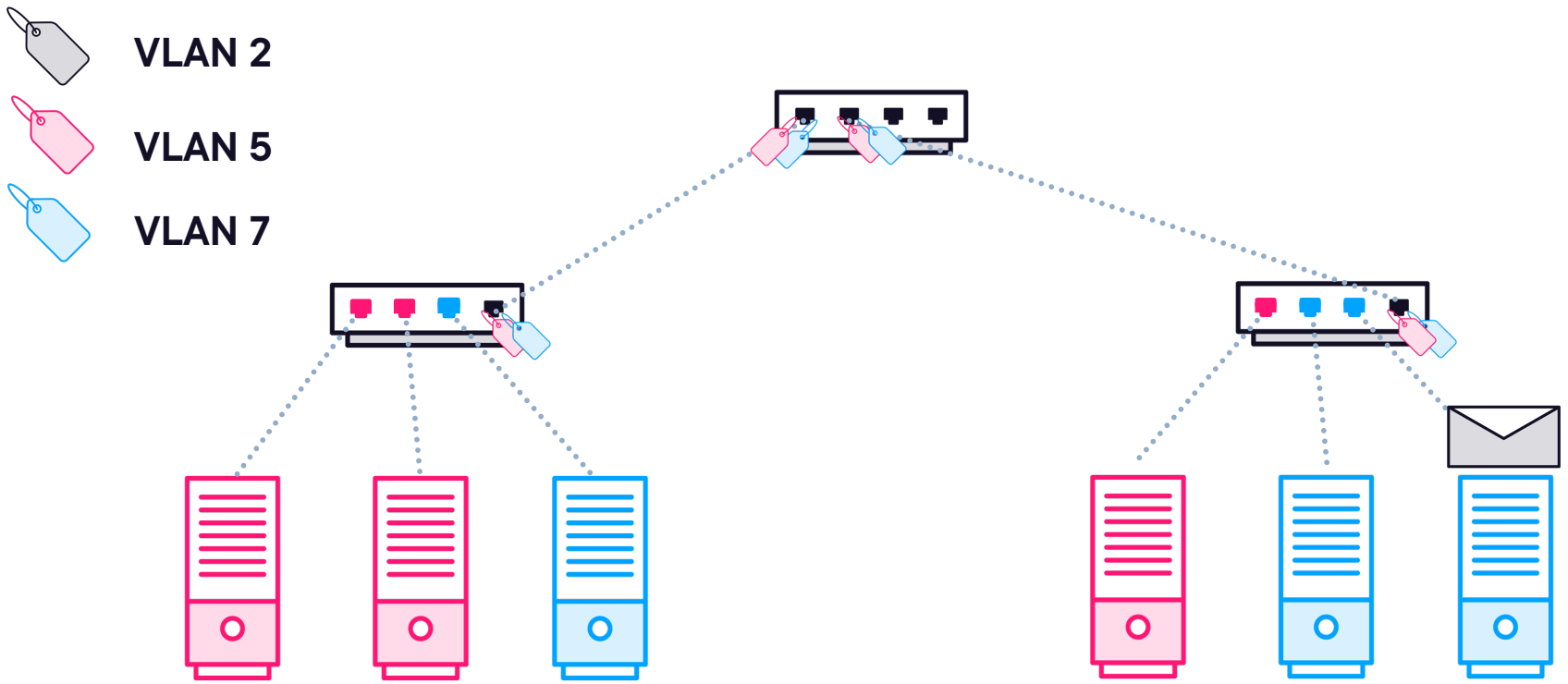
Native VLAN – Default VLAN for frames that aren't tagged already

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

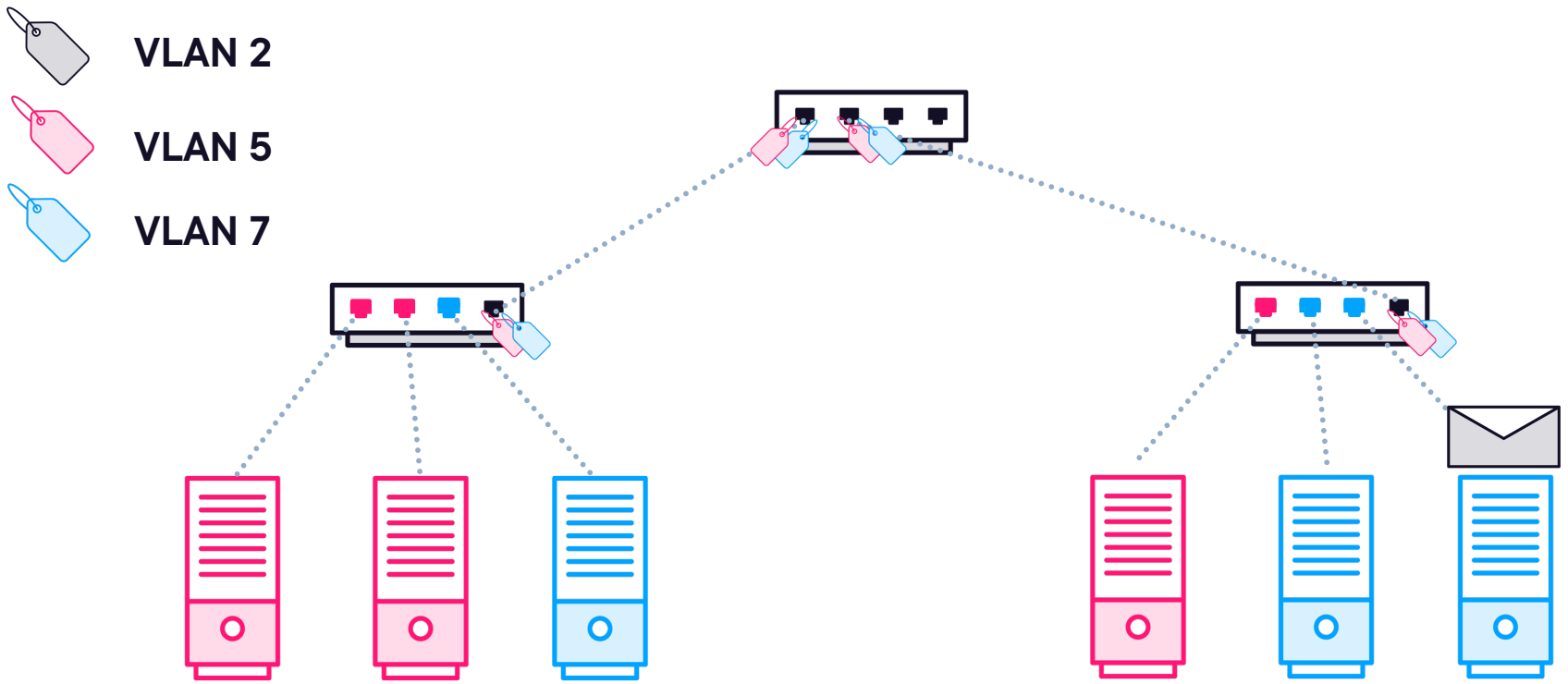
Troubleshooting VLANs



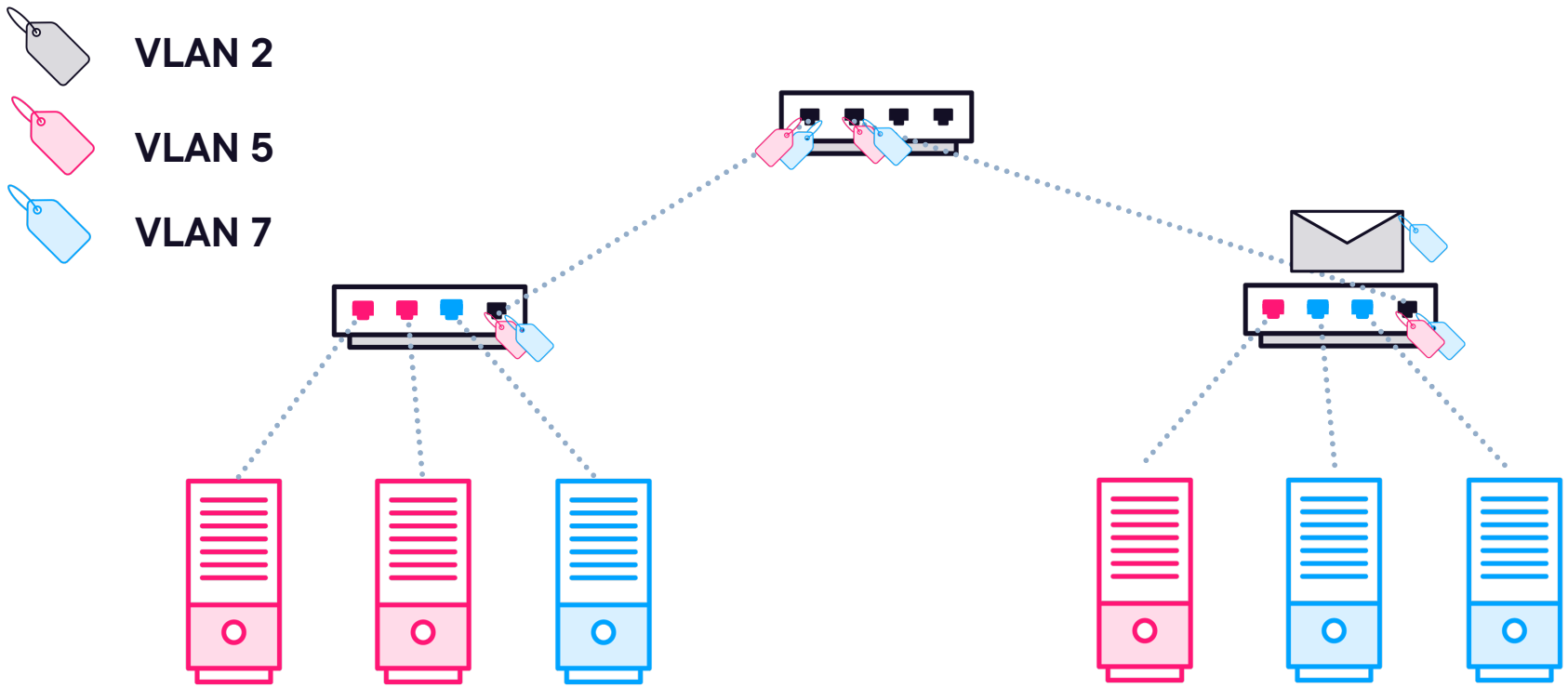
Troubleshooting VLANs



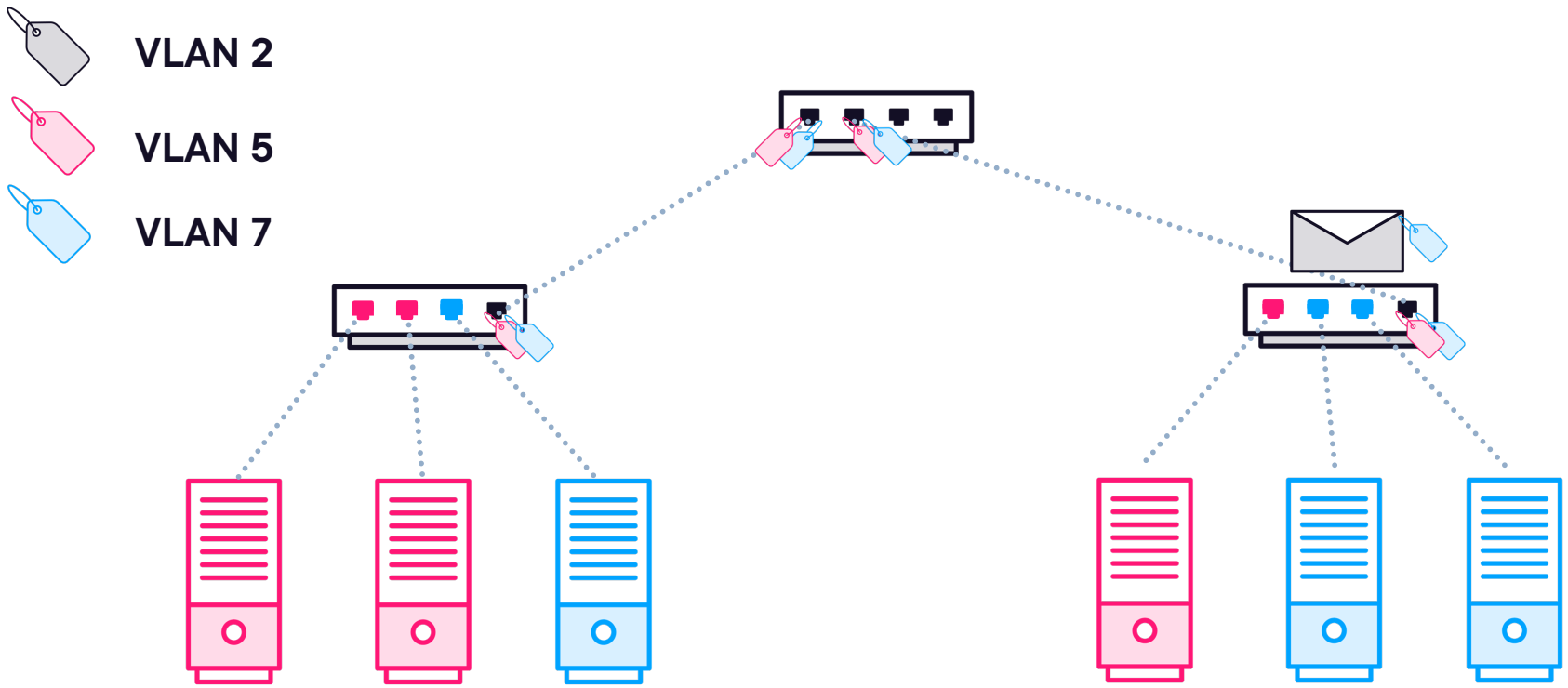
Troubleshooting VLANs



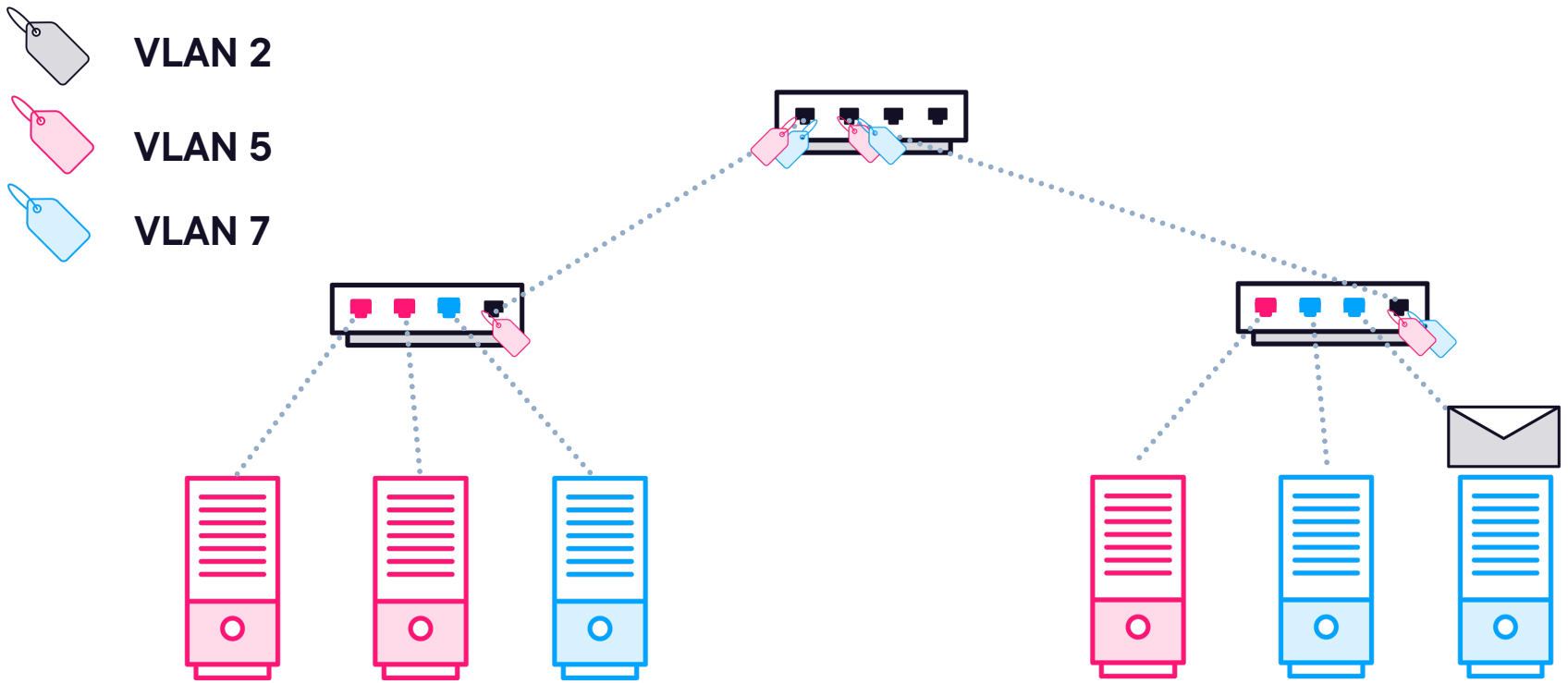
Troubleshooting VLANs



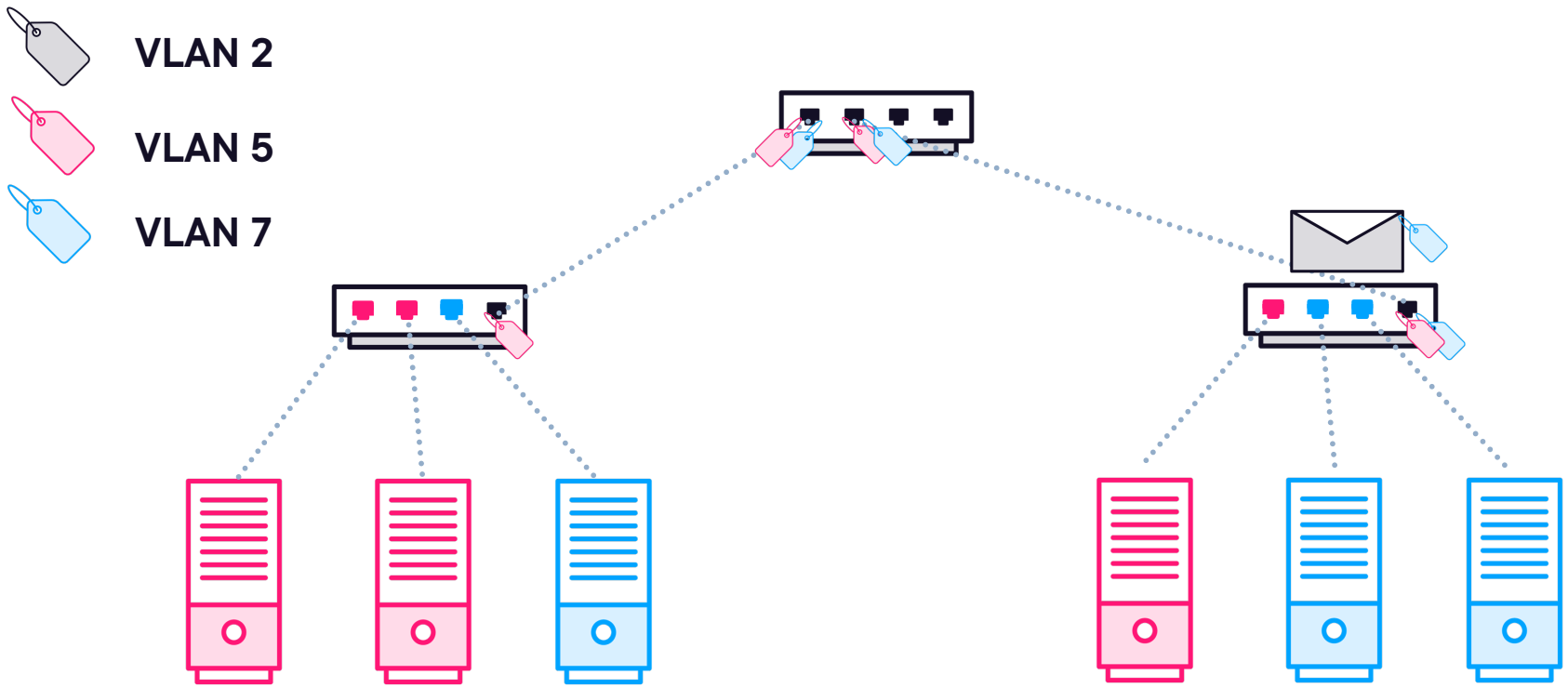
Troubleshooting VLANs



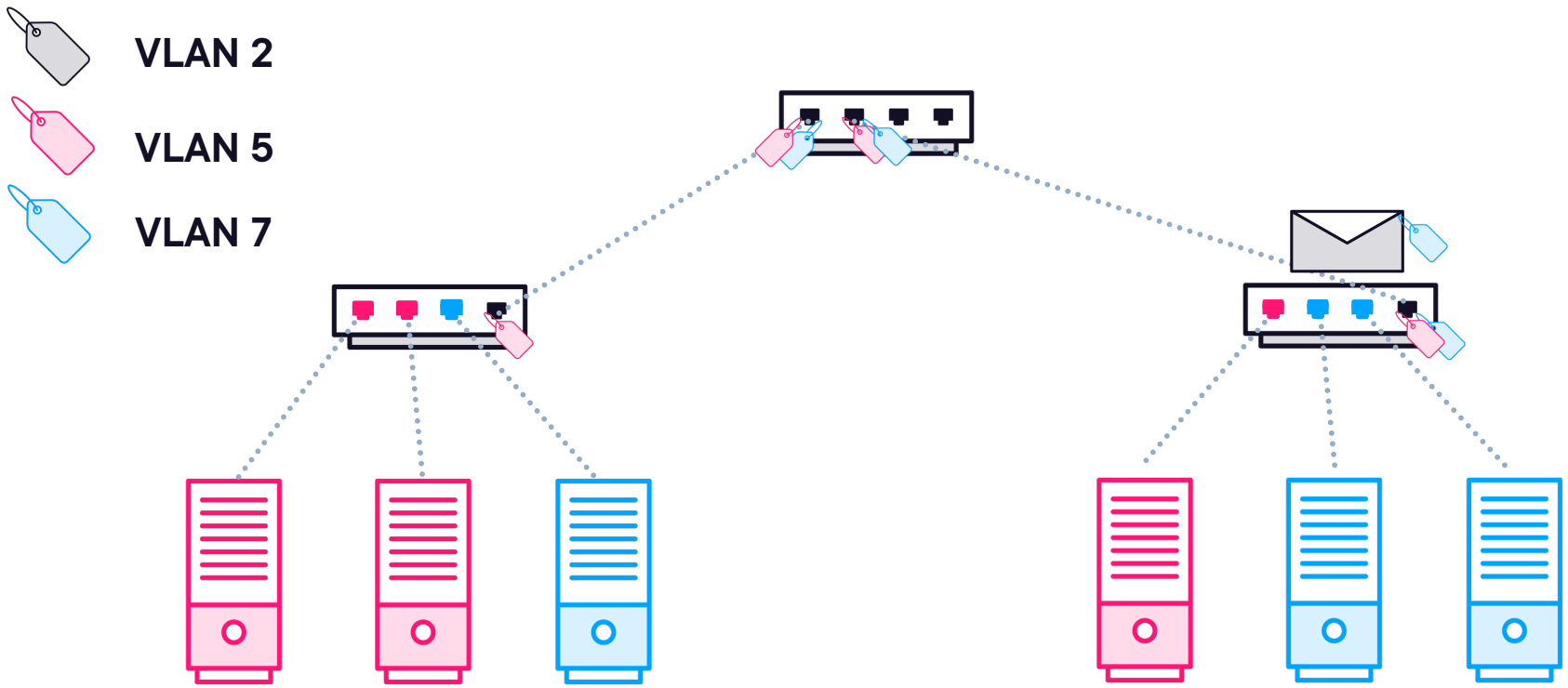
Troubleshooting VLANs



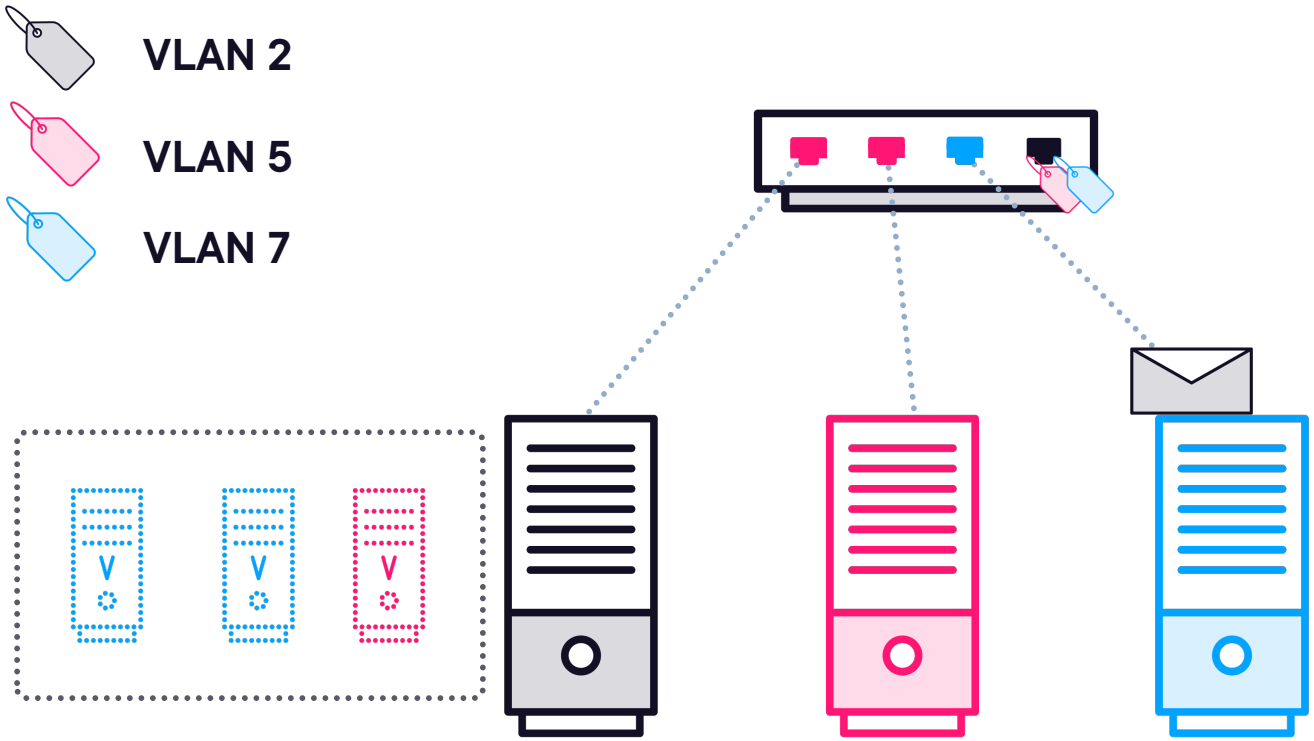
Troubleshooting VLANs



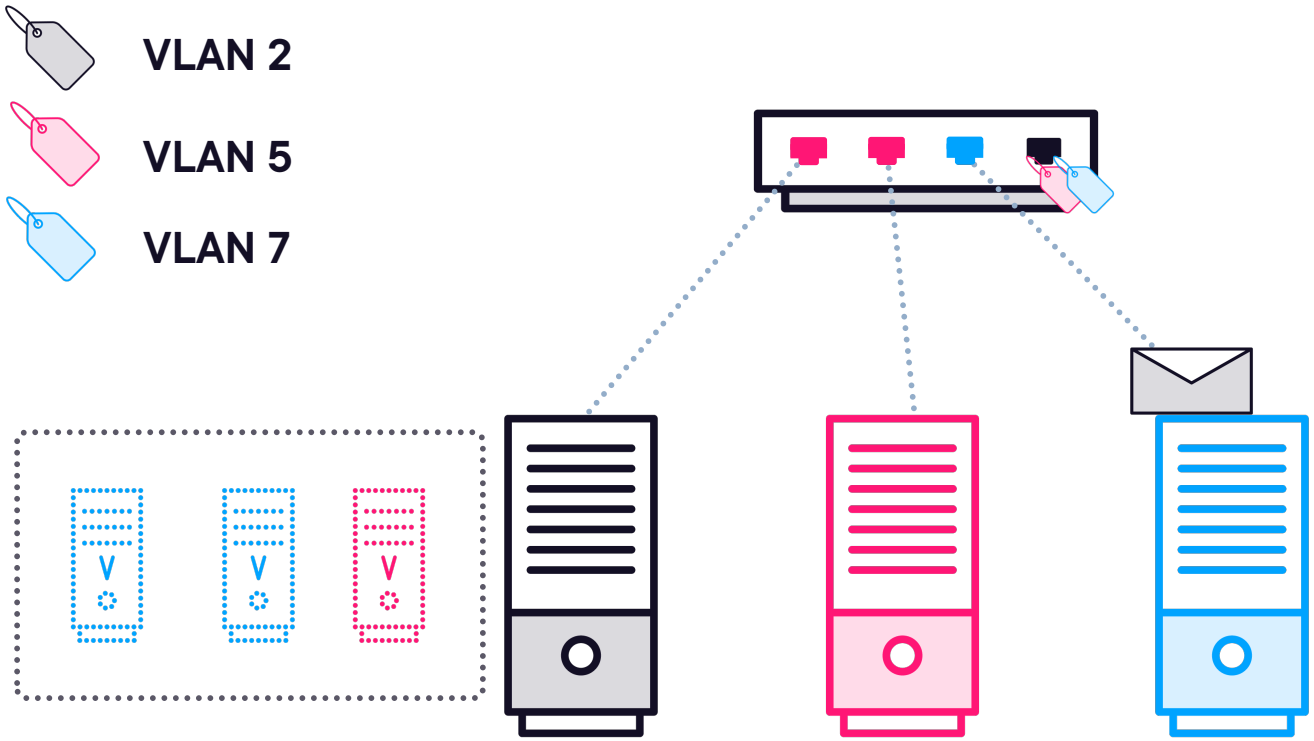
Troubleshooting VLANs



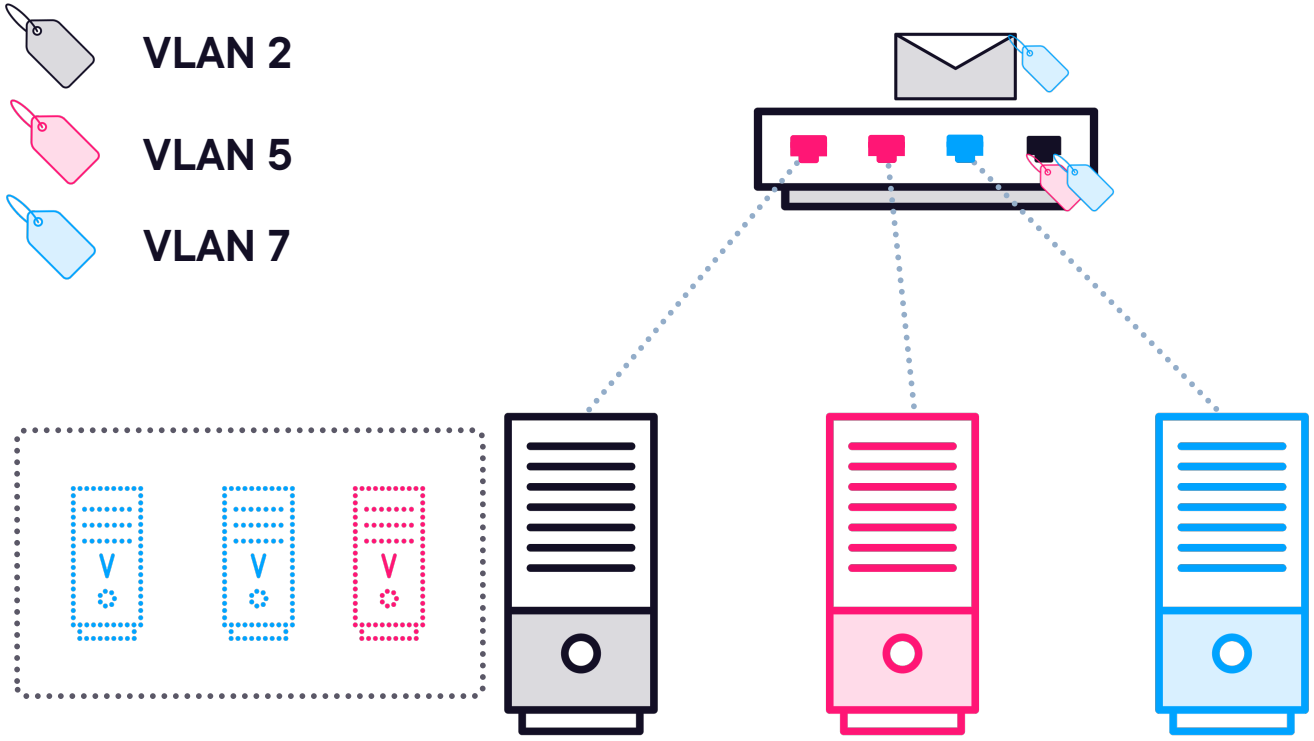
Hypervisor with Access Ports



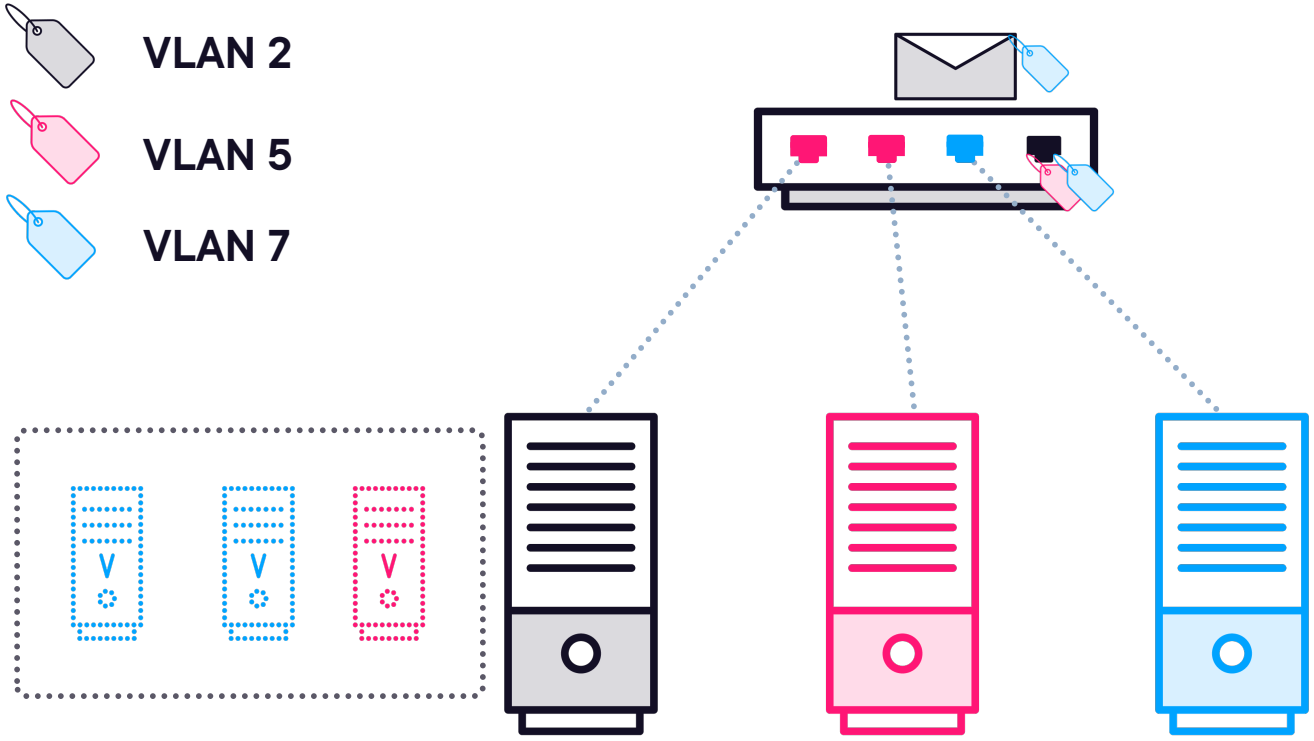
Hypervisor with Access Ports



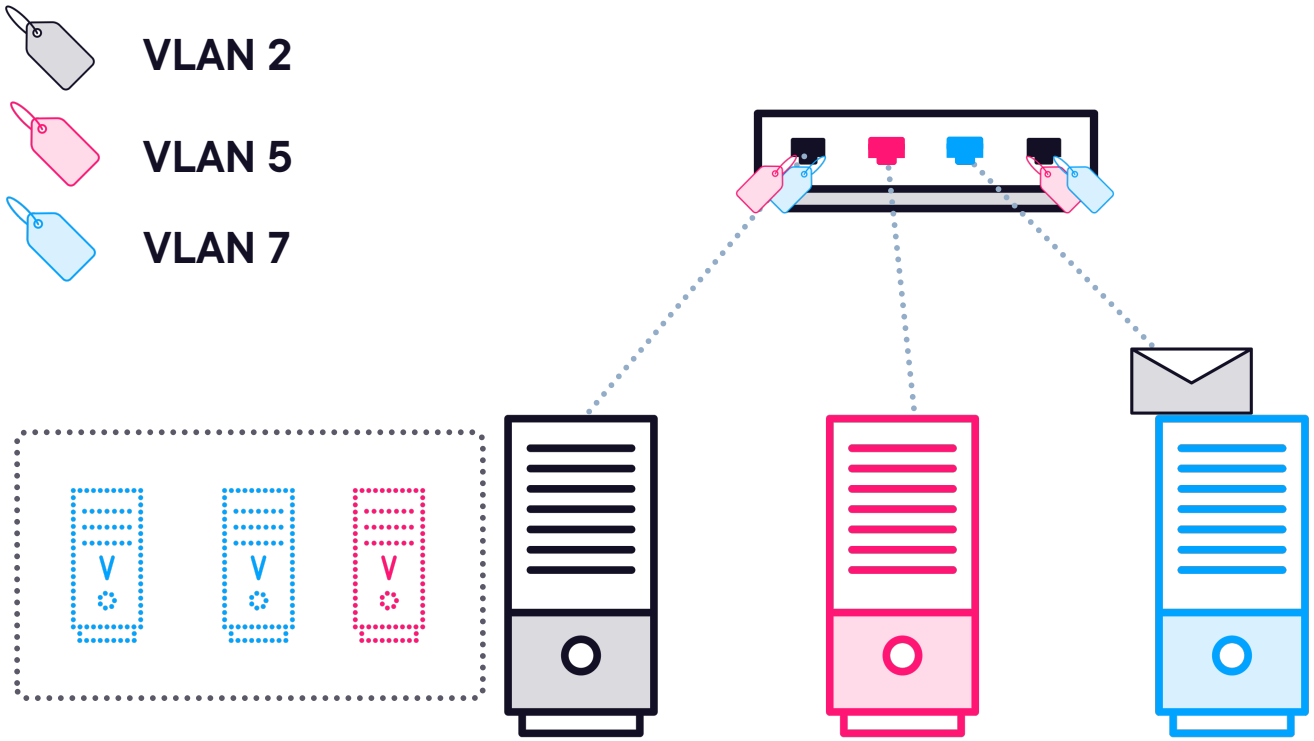
Hypervisor with Access Ports



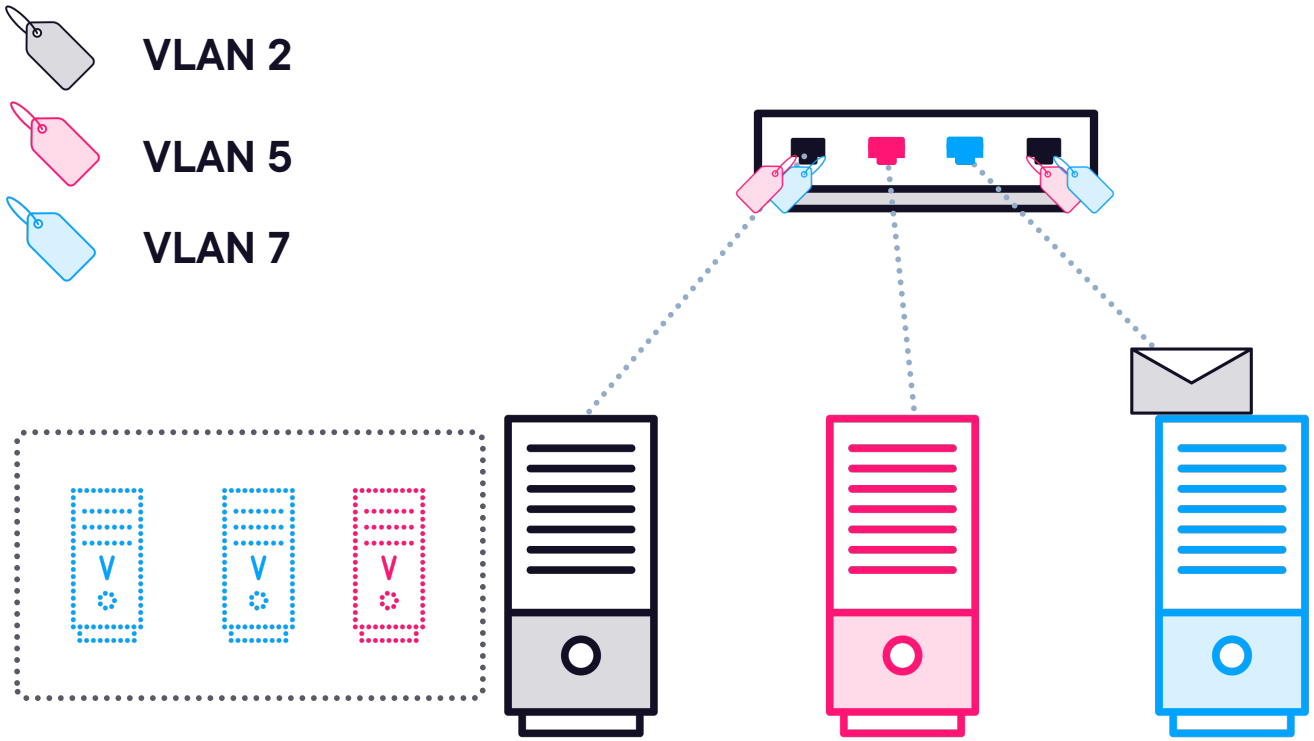
Hypervisor with Access Ports



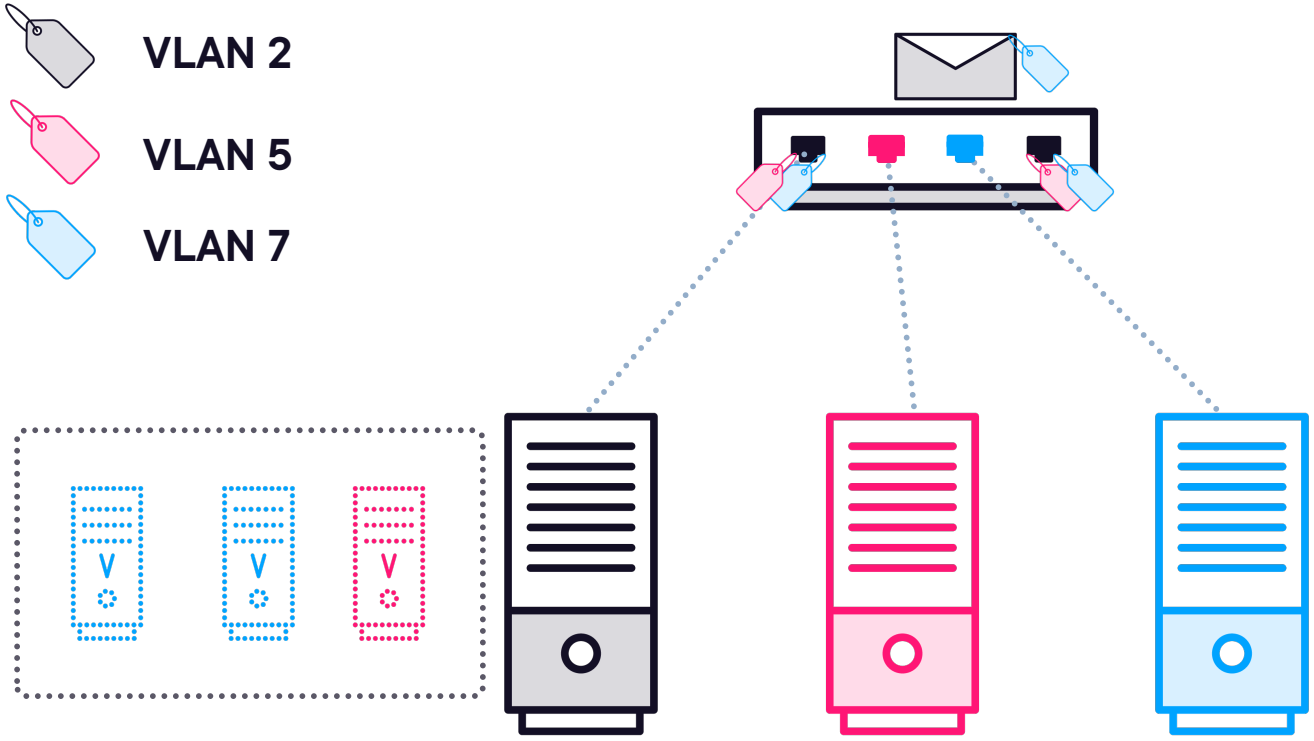
Hypervisor with Trunk Ports



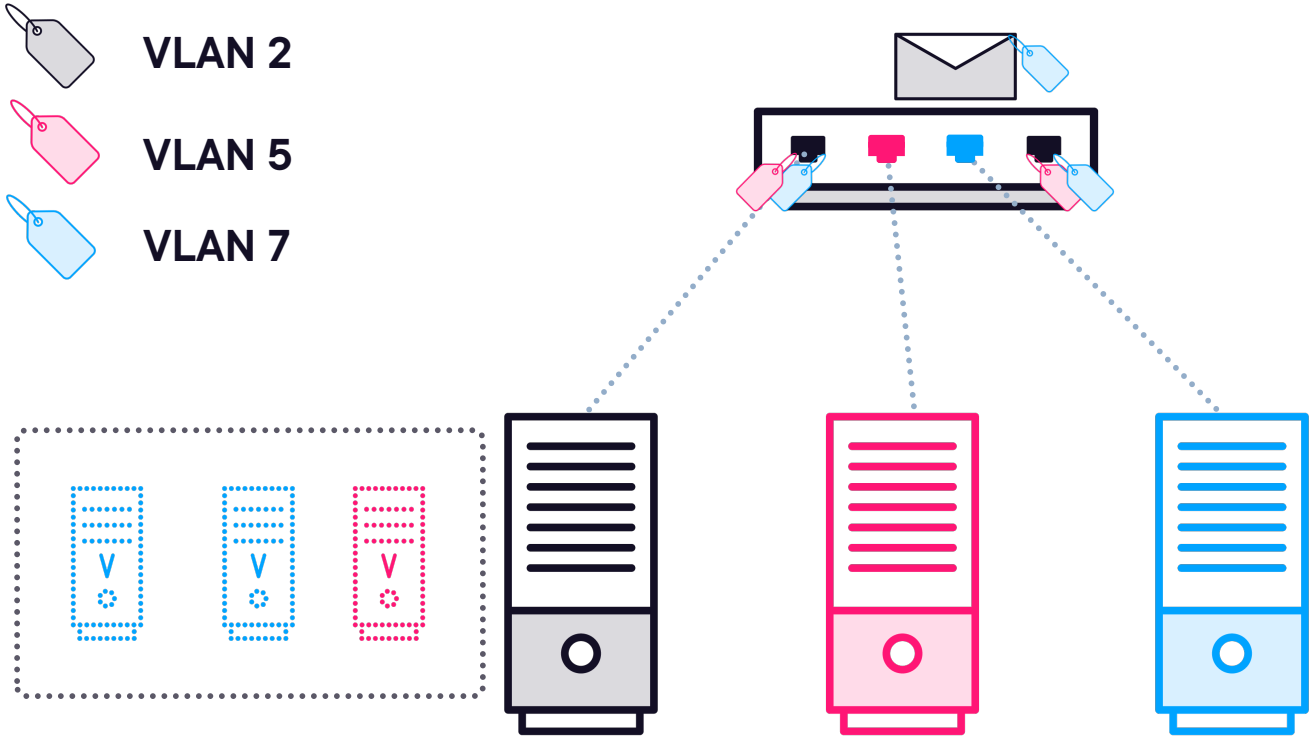
Hypervisor with Trunk Ports



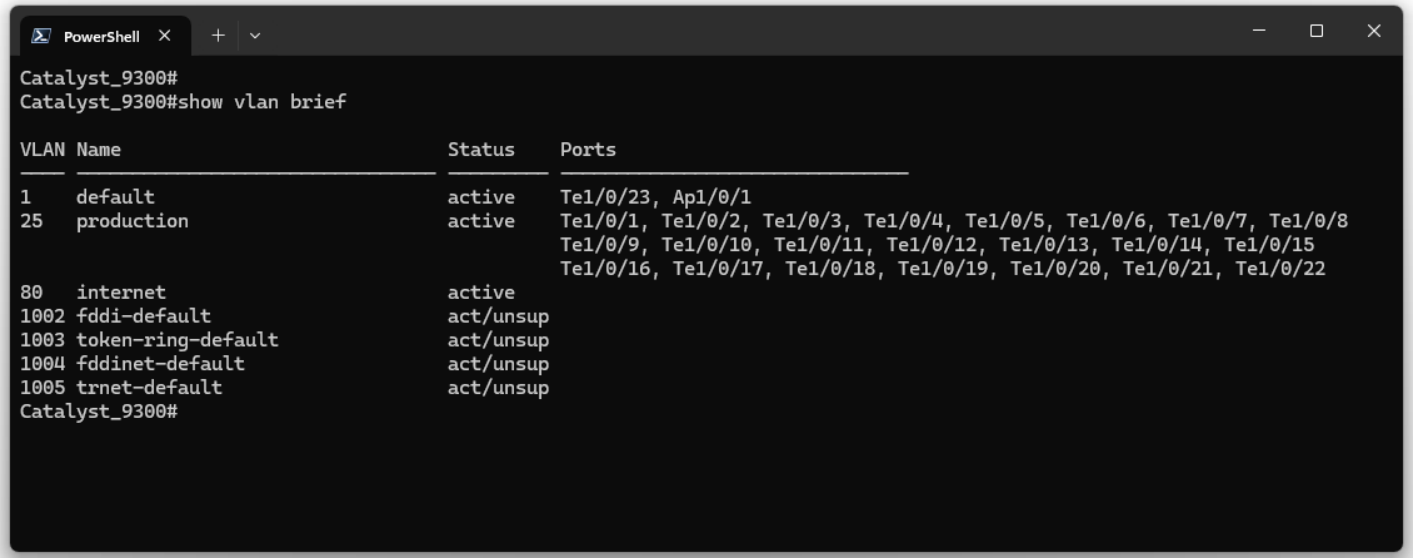
Hypervisor with Trunk Ports



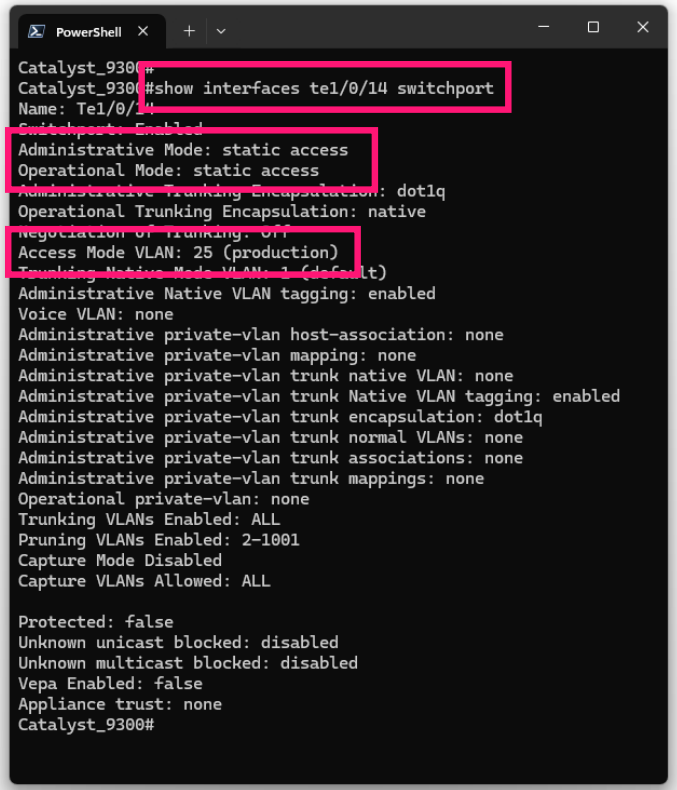
Hypervisor with Trunk Ports

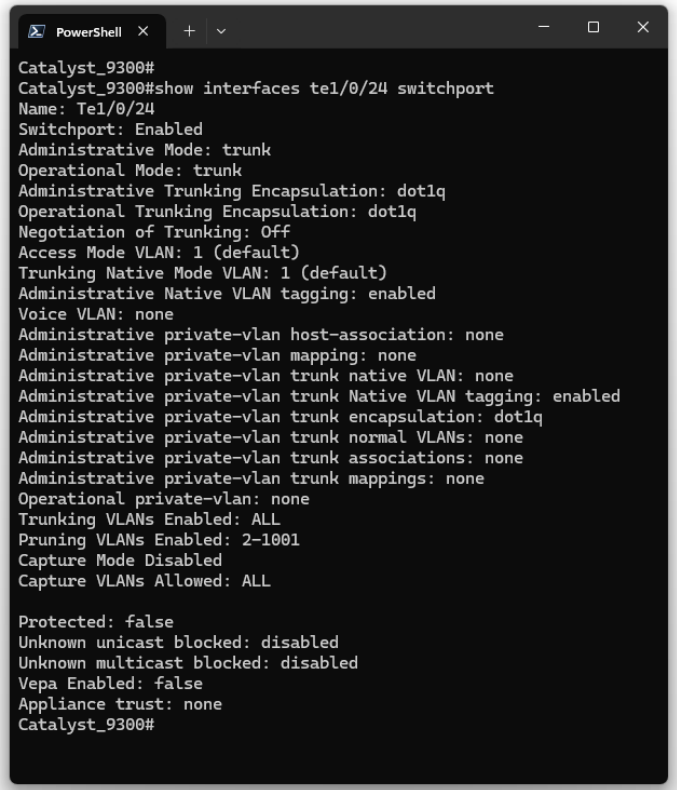


Network Switching Problems

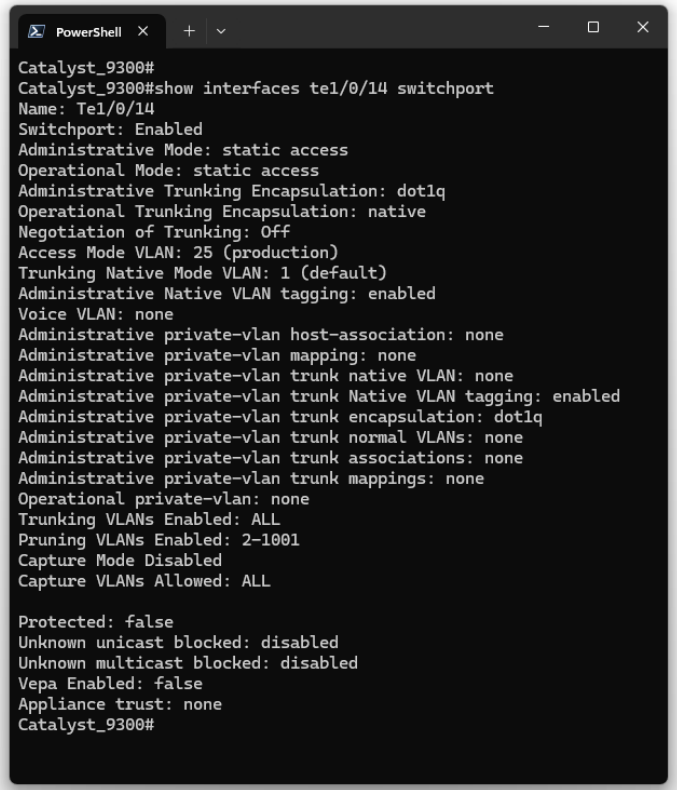


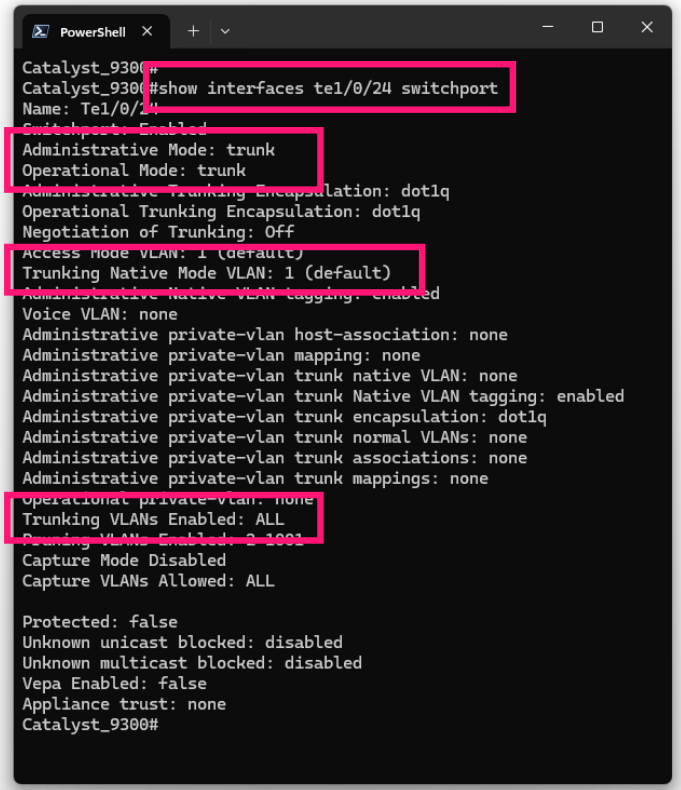
Network Switching Problems





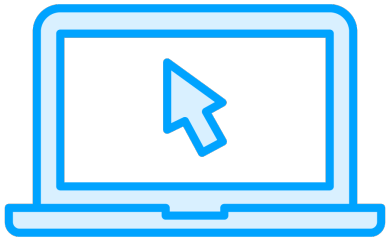
Network Switching Problems





Additional Switching Help

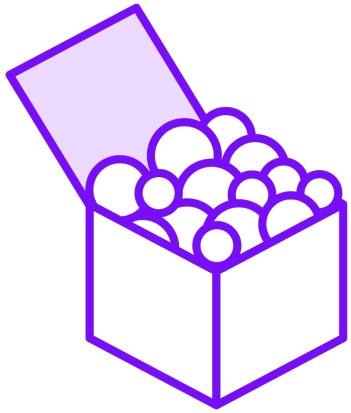
Infrastructure as Code (IaC)
Version control can help you track changes



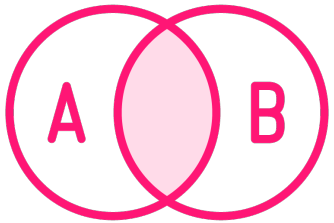
Virtual Labs
Use tools like Cisco Packet Tracer and GNS3 to try out what you learn

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



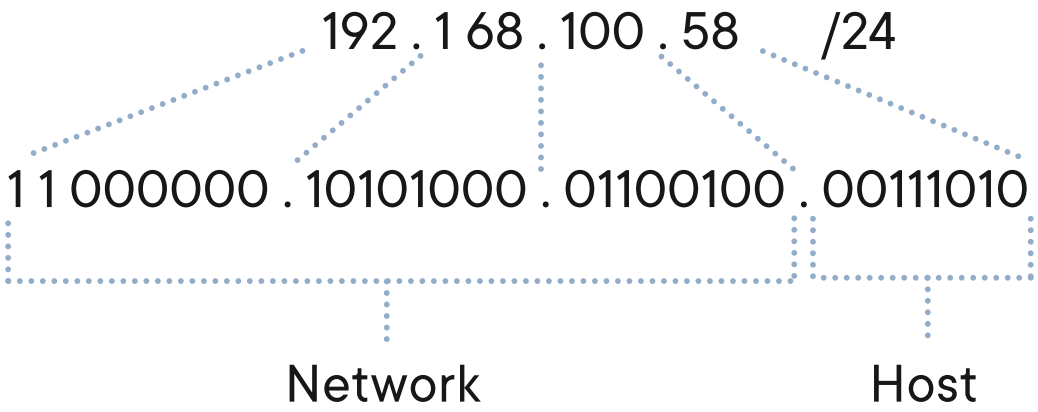
Network Overlap
When there are two or more networks that all use the same IP address space

Private IPv4 Addresses

10.0.0.0/8	172.16.0.0/12	192.168.0.0/16
10.0.0.0 – 10.255.255.255	172.16.0.0 – 172.31.255.255	192.168.0.0 – 192.168.255.255
Hosts : 16,777,216	Hosts : 1,048,574	Hosts : 65,534
Subnet /24s : 65,536 Subnet /20s: 4096 Subnet /16s: 256	Subnet /24s : 4,096 Subnet /20s: 256 Subnet /16s: 16	Subnet /24s : 256 Subnet /20s: 16 Subnet /16s: 1

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

Subnetting with CIDR Notation

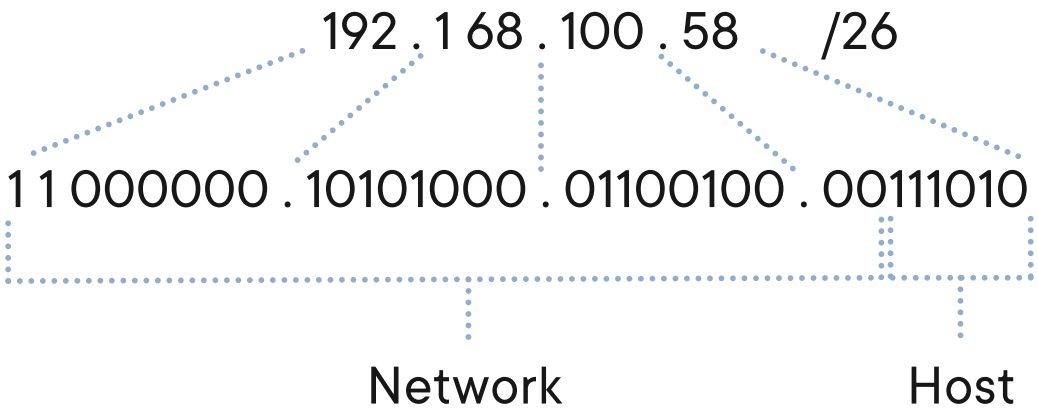


Network Address: 192.168.100.0

Broadcast Address: 192.168.100.255

Usable Addresses: 192.168.100.1 – 192.168.100.254

Subnetting with CIDR Notation

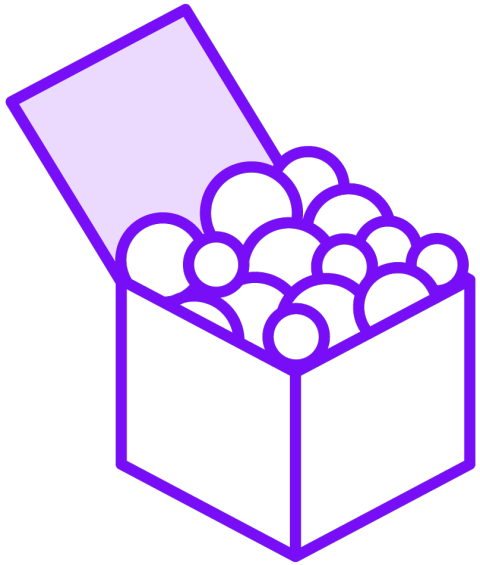


Network Address: 192.168.100.0

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

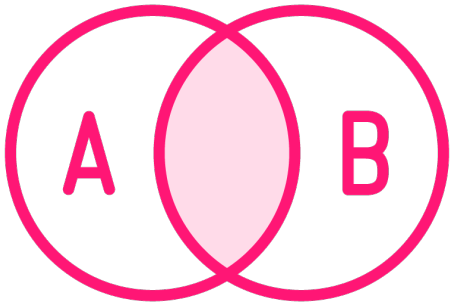
Reduce Lease Time

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

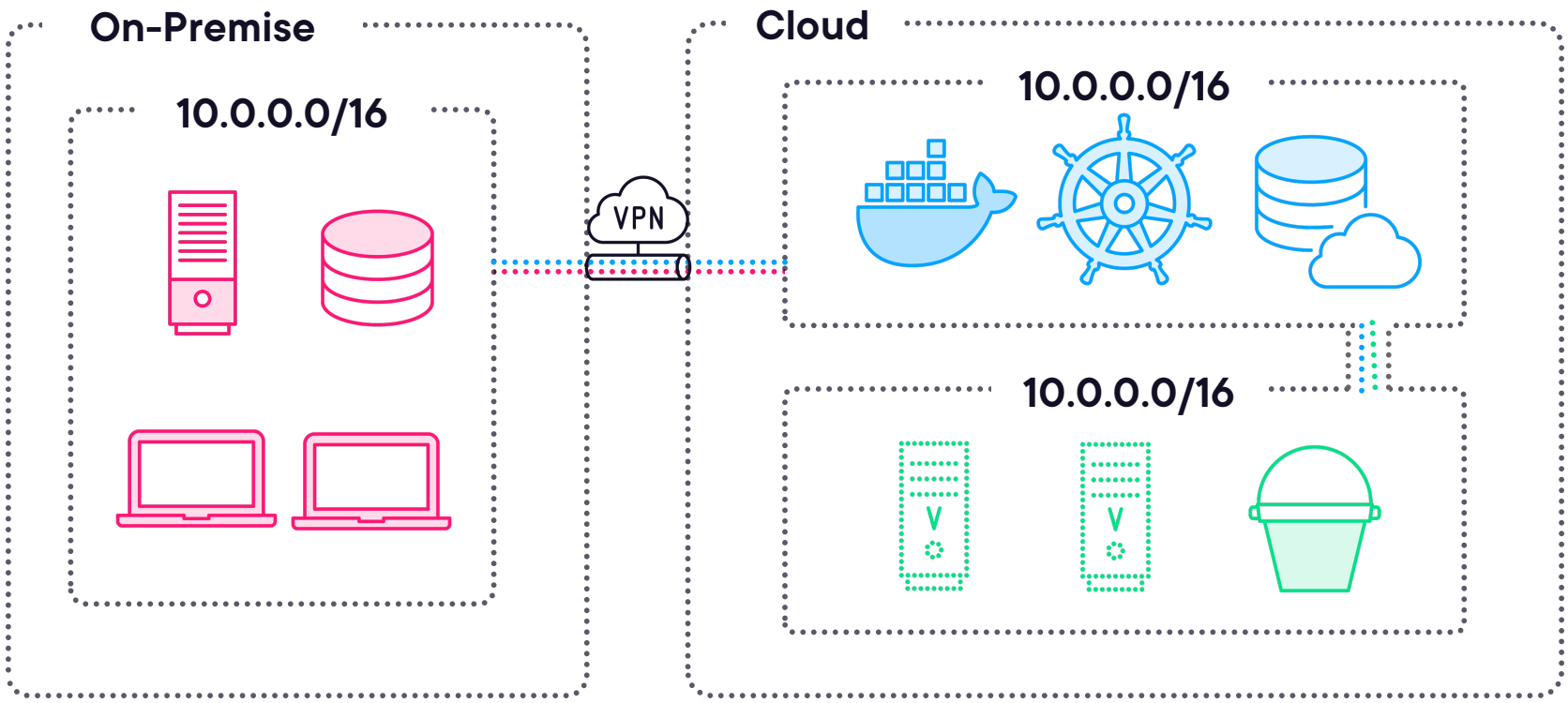


Where you have two or more networks using the same IP address space

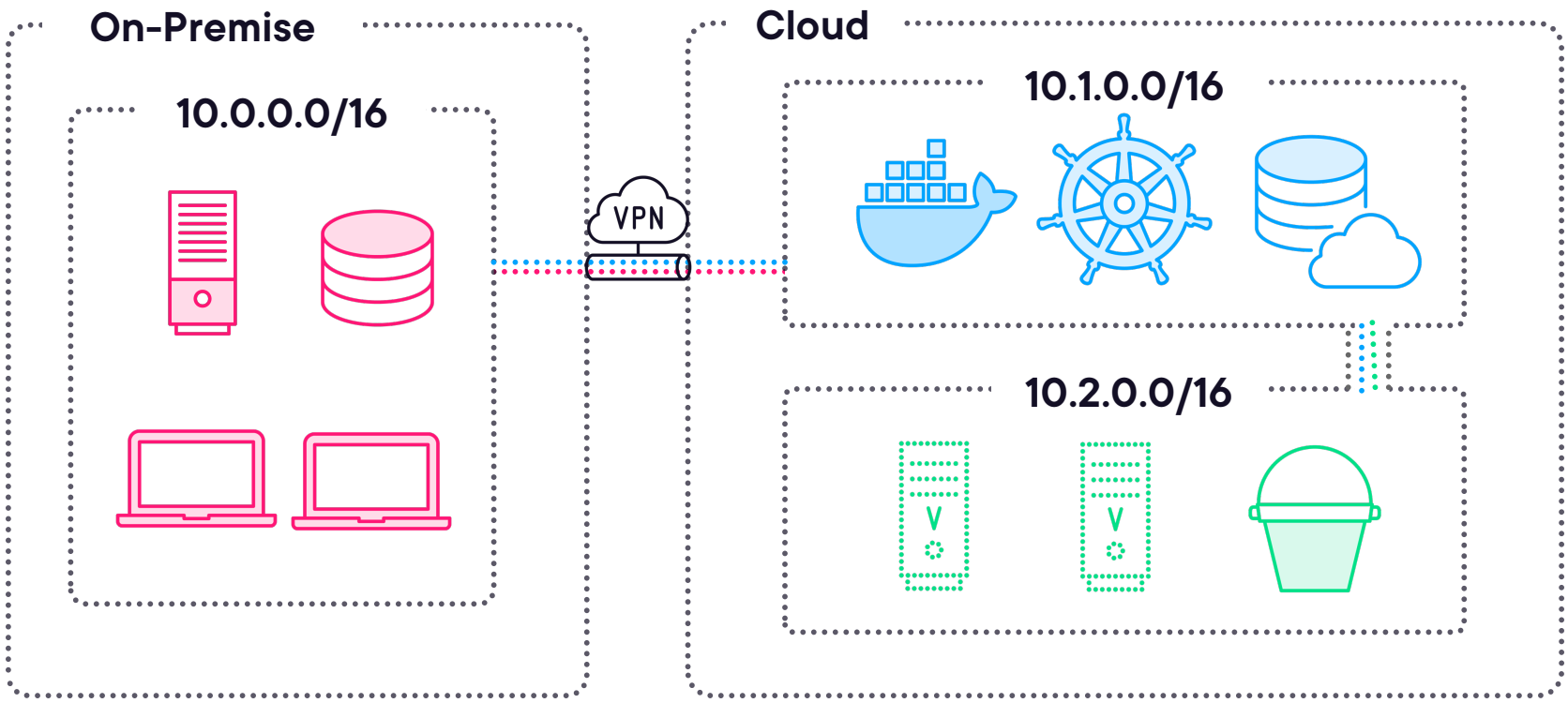
This causes problems communicating due to IP address conflicts

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