Protocol Deep Dive: Address Resolution Protocol (ARP)

ADDRESS RESOLUTION PROTOCOL FUNDAMENTALS

James Rizzo
NETWORK ENGINEER

@jv_rizzo

Module Overview

Address Resolution Protocol Purpose and Function in the LAN

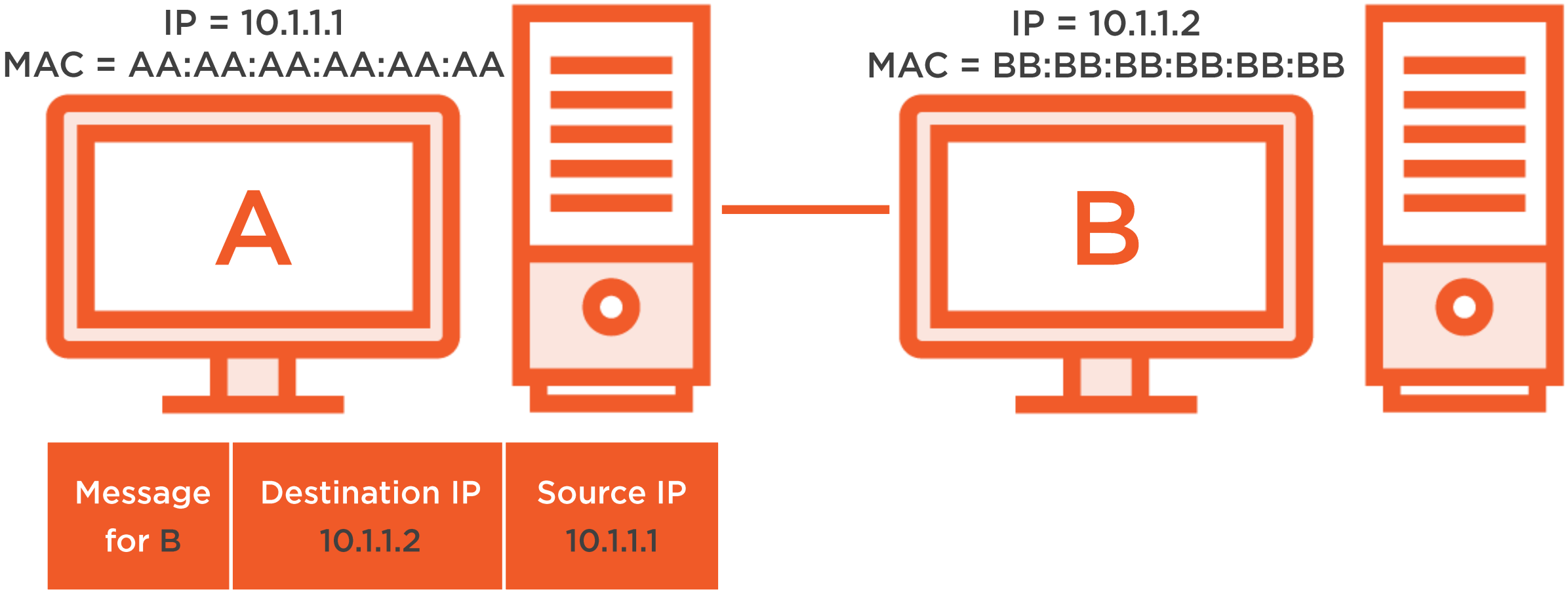
- ARP Messages
- ARP Cache on Hosts and Routers

Demonstrate ARP Protocol Captures and ARP Cache Configurations

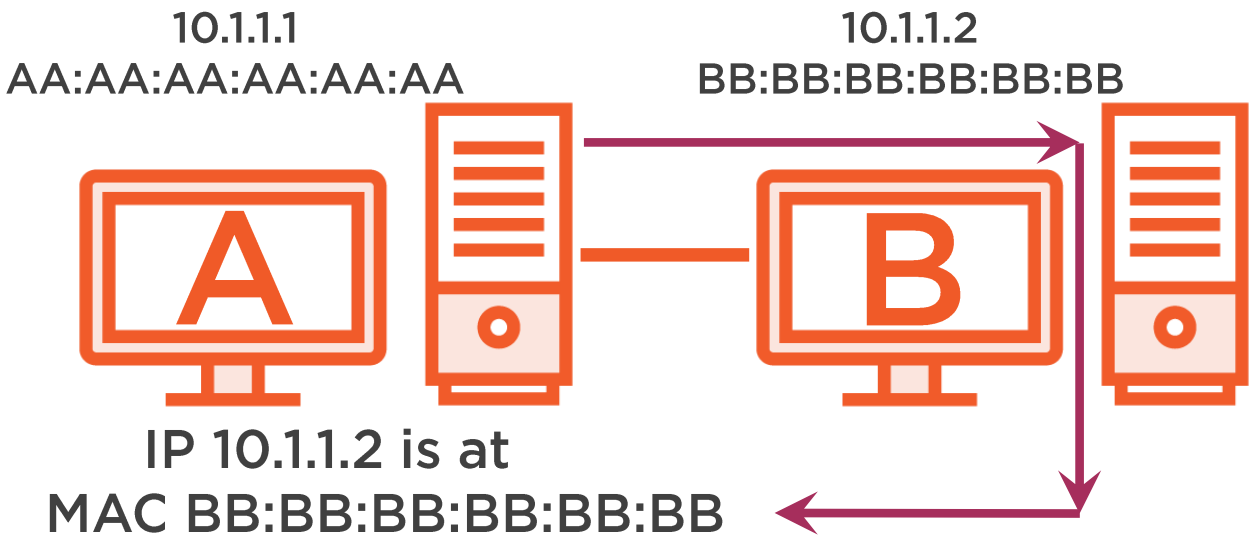
- Clear ARP Caches
- Add or Delete Static Entries
- View or Change Timers

Use ARP to Solve Common LAN Problems

Address Resolution Protocol (ARP) Purpose



Address Resolution Protocol (ARP) Purpose



Provides Method for Mapping Known

Logical (IP) Address

To an Unknown

Physical (MAC) Address

Message	Destination IP	Source IP	Source MAC	Destination MAC
for B	10.1.1.2	10.1.1.1	AA:AA:AA:AA:AA:AA	BB:BB:BB:BB:BB:BB

ARP Function and Process

A system process requires sending data to another node

IP headers (source and destination) are known

Destination physical LAN (MAC) address must be added to the data before sending

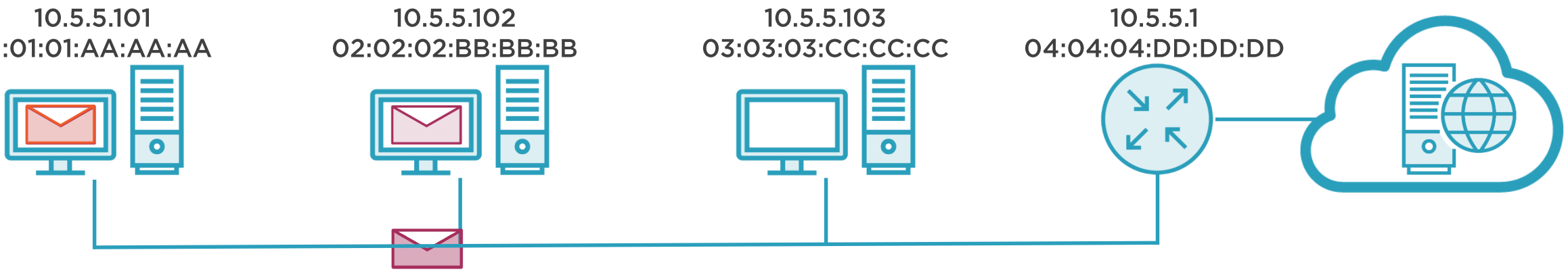
ARP provides the function to learn and cache that information

Address Resolution Protocol (ARP) Messages Resolving Hosts on the Local LAN

ARP Reply	Type	Source	Destination
Opcode = 2	ARP	02:02:02:BB:BB:BB	01:01:01:AA:AA:AA

Host ARP Cache

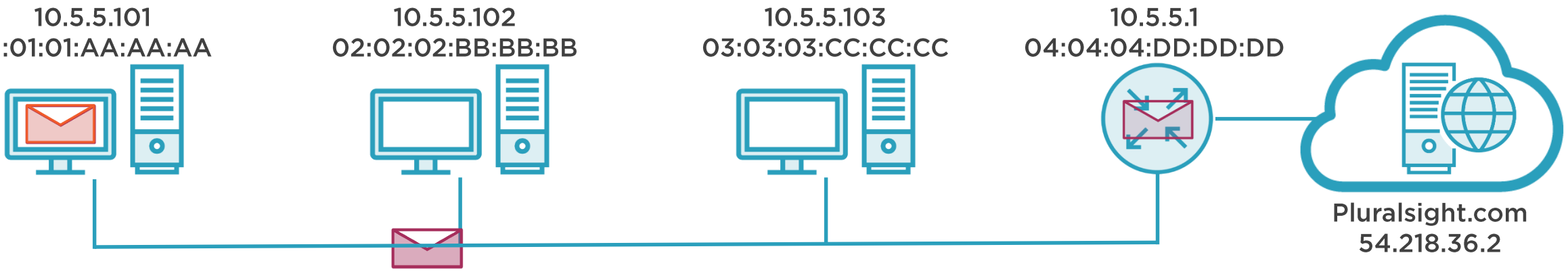
IP	MAC
10.5.5.102 is at	02:02:02:BB:BB:BB



Ping	Destination IP	Source IP	Source MAC	Destination MAC
10.5.5.102	10.5.5.102	10.5.5.101	01:01:01:AA:AA:AA	02:02:02:BB:BB:BB

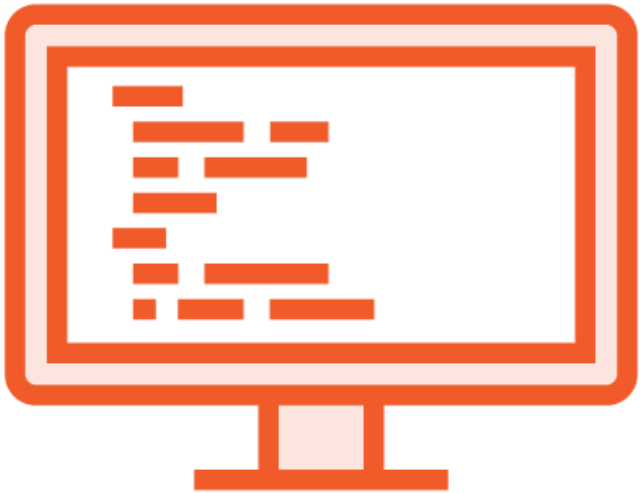
Address Resolution Protocol (ARP) Messages
Data Leaving the LAN

ARP Reply	Type	Source	Destination
Opcode = 2 10.5.5.1 is at 04:04:04:DD:DD:DD	ARP (0x0806)	04:04:04:DD:DD:DD	01:01:01:AA:AA:AA



GET	Destination IP	Source IP	Source MAC	Destination MAC
Pluralsight	54.218.36.2	10.5.5.101	01:01:01:AA:AA:AA	04:04:04:DD:DD:DD

Address Resolution Protocol (ARP) Cache



Administrator: Command Prompt

```
C:\>arp -a

Interface: 10.2.2.34 --- 0xc
  Internet Address      Physical Address      Type
  10.2.2.1              30-37-a6-de-59-c3     dynamic
  10.2.2.200            00-11-32-2f-76-83     dynamic
  10.2.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static

C:\>
```


Local NIC

IP = 10.2.2.34

MAC = 34-E6-D7-00-11-AA

Host ARP Cache

A Location in memory storing

IP to MAC address mappings

from dynamic and static sources

ARP Cache Details

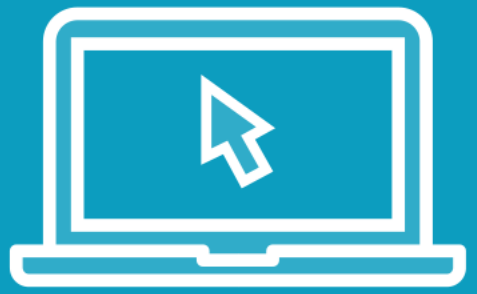
Each active interface has ARP cache entries which can include both static and dynamic mappings

Host's dynamic ARP cache entries have a timer

Dynamic ARP entries can be cleared forcing 're-learning'

Broadcast and multicast static entries exist, but an administrator can add or remove static entries

Demo



Capturing ARP

Viewing the ARP Cache on Hosts and Routers

Configuring ARP Cache Options

- Clearing ARP Caches
- Adding and Removing Static Entries
- Changing Timers
- Other ARP types

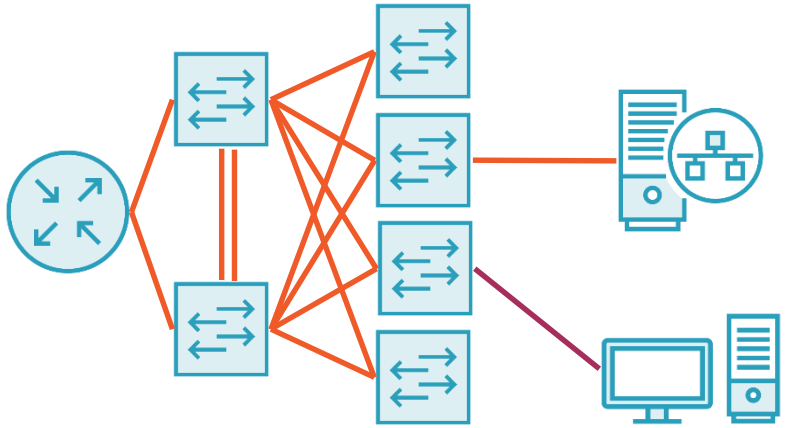
Demo

Problem: Track Down a LAN System

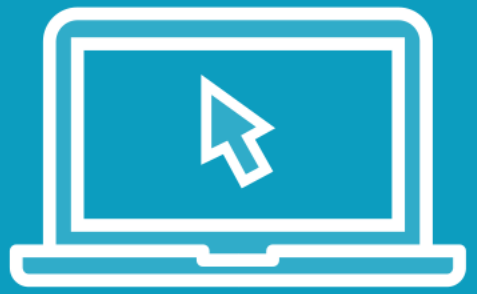
Symptoms:

- You Have a System Name or IP
- Must Find the Specific Switch Port to Which the System Is Connected
- The LAN May Be Complex, Large and/or Not Well Mapped

Solution: Router, Ping, ARP, Switch, MAC



Demo

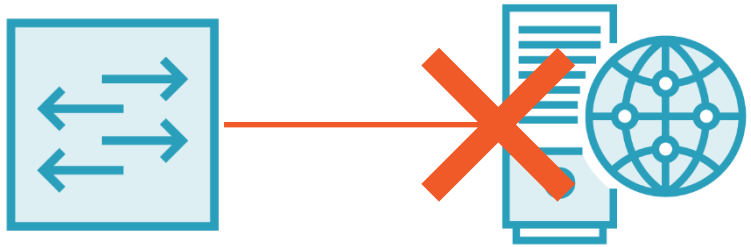


Problem: Host Not on or Has Left the LAN

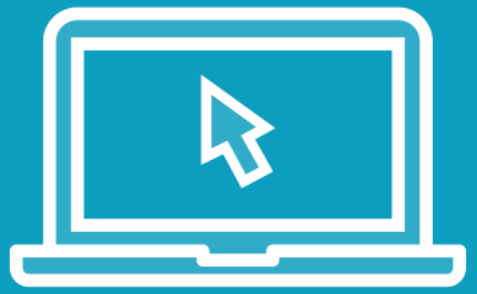
Symptoms:

- All Services on That Host Are Unavailable
- Pings to the Host Time Out
- Captures Show Continuous ARPs for That Host

Solution: Power-on or Connect the Host



Demo

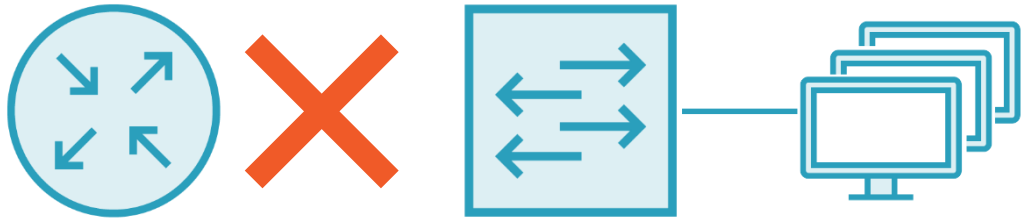


Problem: Default Gateway Misconfigured or Lost

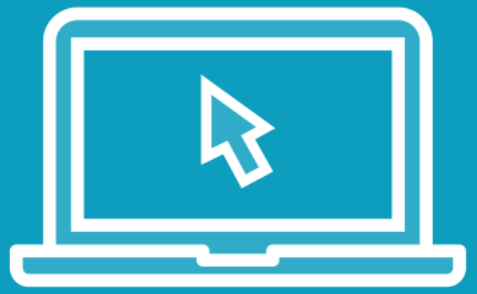
Symptoms:

- Anything Outside LAN Unavailable
- Pings to the Gateway Time Out
- Hosts Can Communicate with Each Other
- Captures Show All Hosts ARP'ing for the Gateway

Solution: Repair Connectivity to the Gateway



Demo



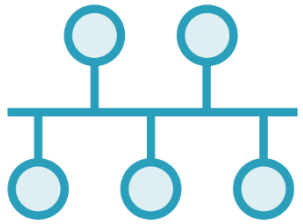
Problem: Incorrect Subnet Mask Configuration

Symptoms:

- Host/Network Connectivity Sporadic
- IP Dependent
- Captures Show Un-replied ARPs for Systems ‘on’ the Same Subnet

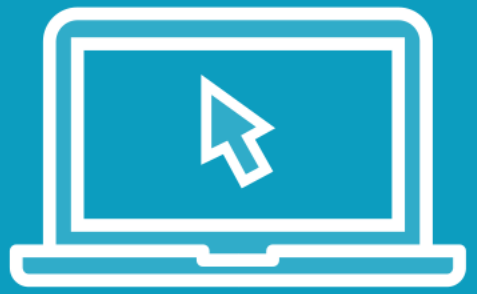
Solution: Correct the Mask

LAN IP: 10.5.5.0 /24



Host IP: 10.5.5.37 /8

Demo



Problem: Switch VLAN Misconfiguration

Symptoms:

- A
- B
- C

Solution: ??