Troubleshooting Common ARP Issues

Jim Rizzo
NETWORK ENGINEER AND SECURITY LEADER

Overview

Unreachable machines: connectivity loss to hosts and default gateways

False stale and static ARP cache entries

Proxy ARP issues and solutions

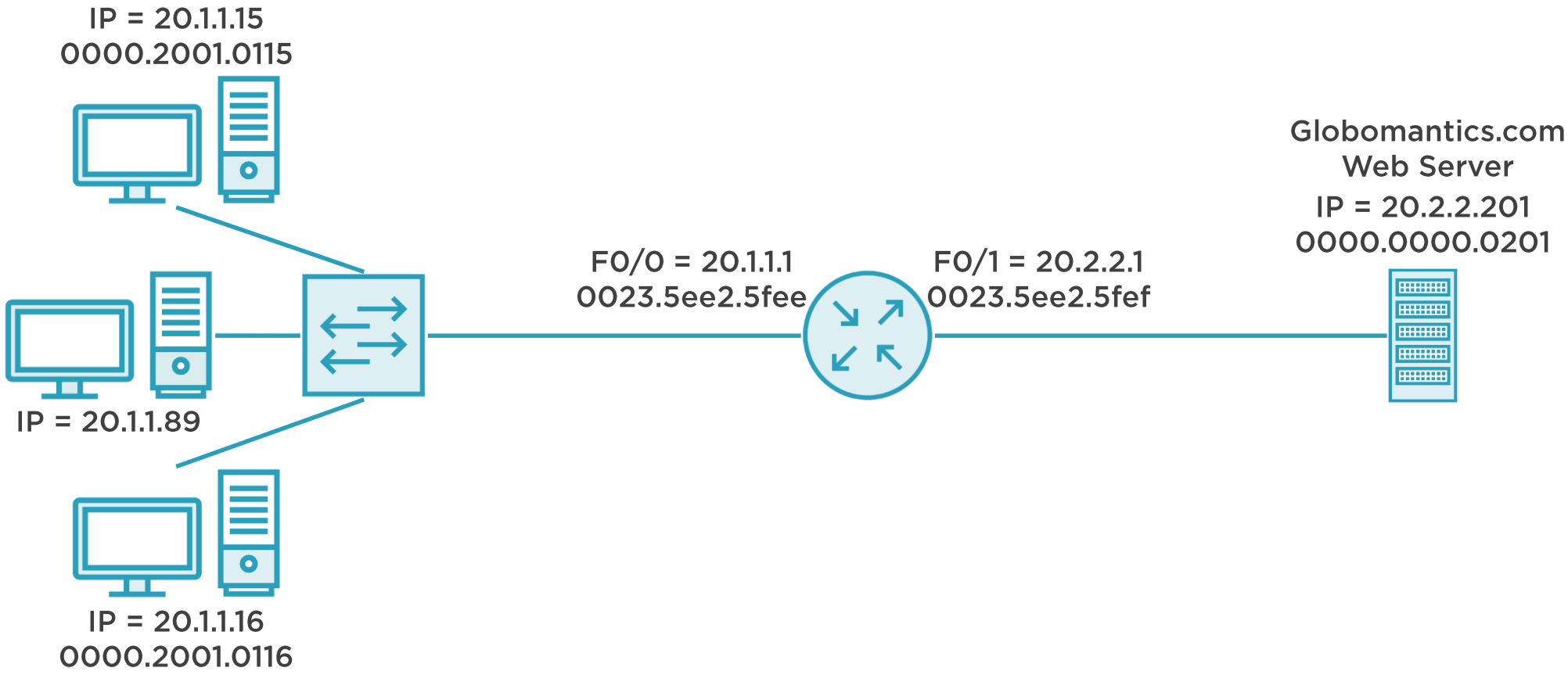
Finding stations in a complex LAN

Demo

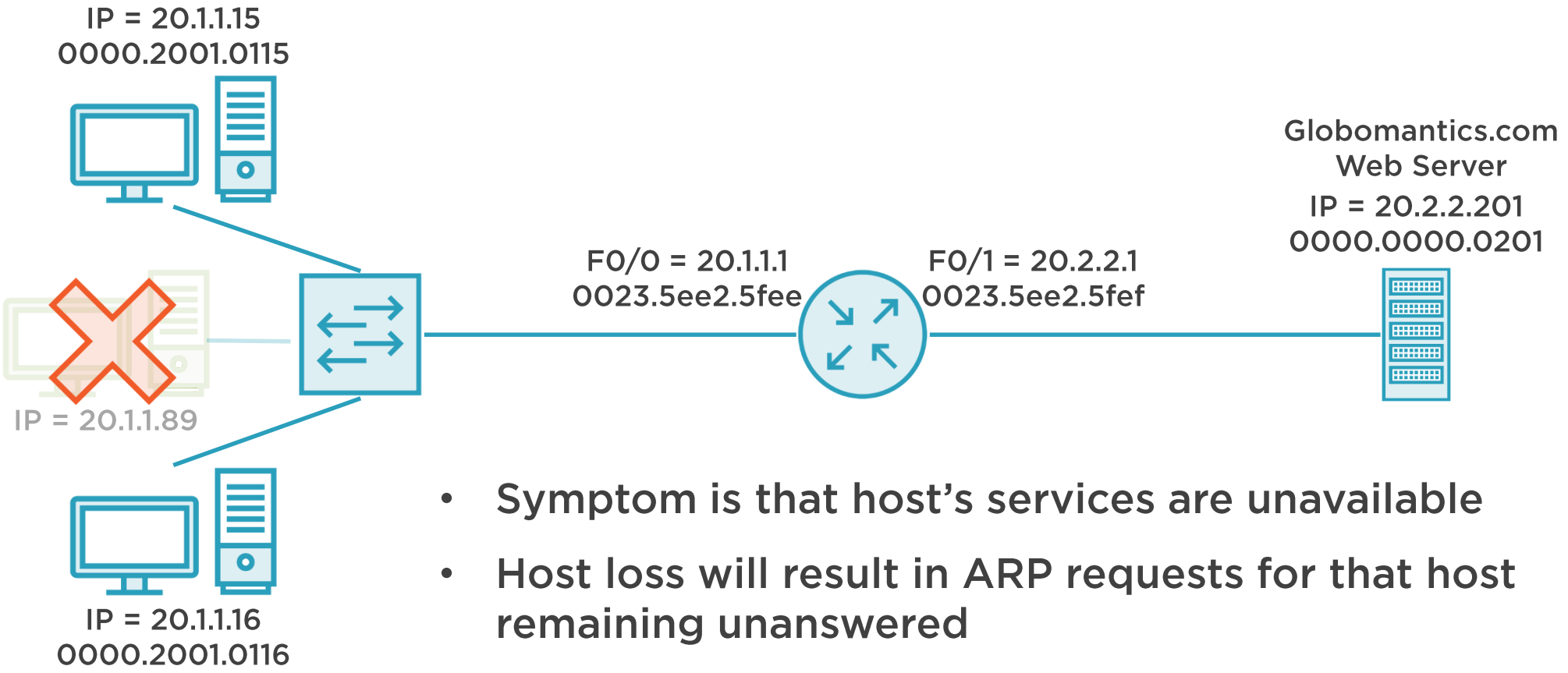
Loss of connectivity to LAN host(s)

Loss of the default gateway

Host and Gateway Connectivity Loss

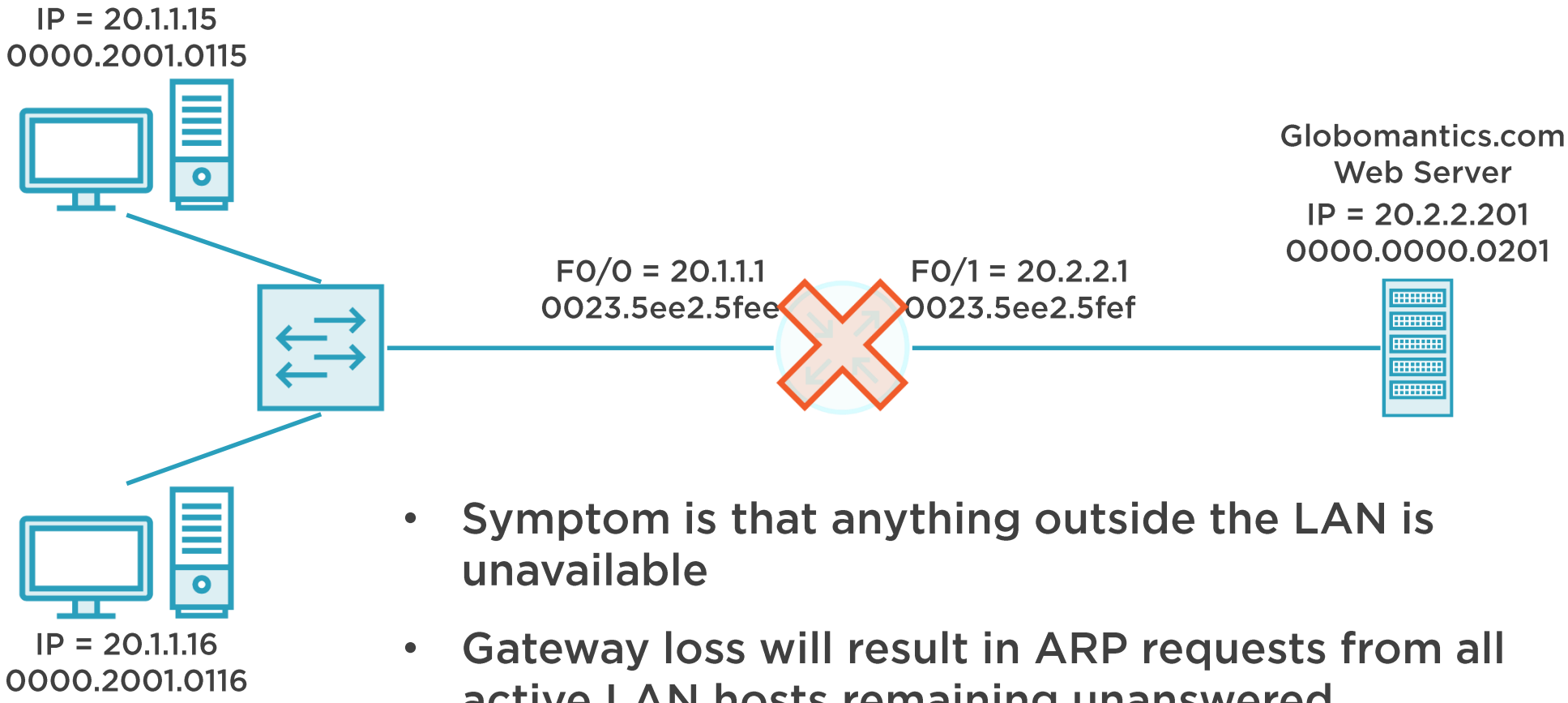


Host Connectivity Loss



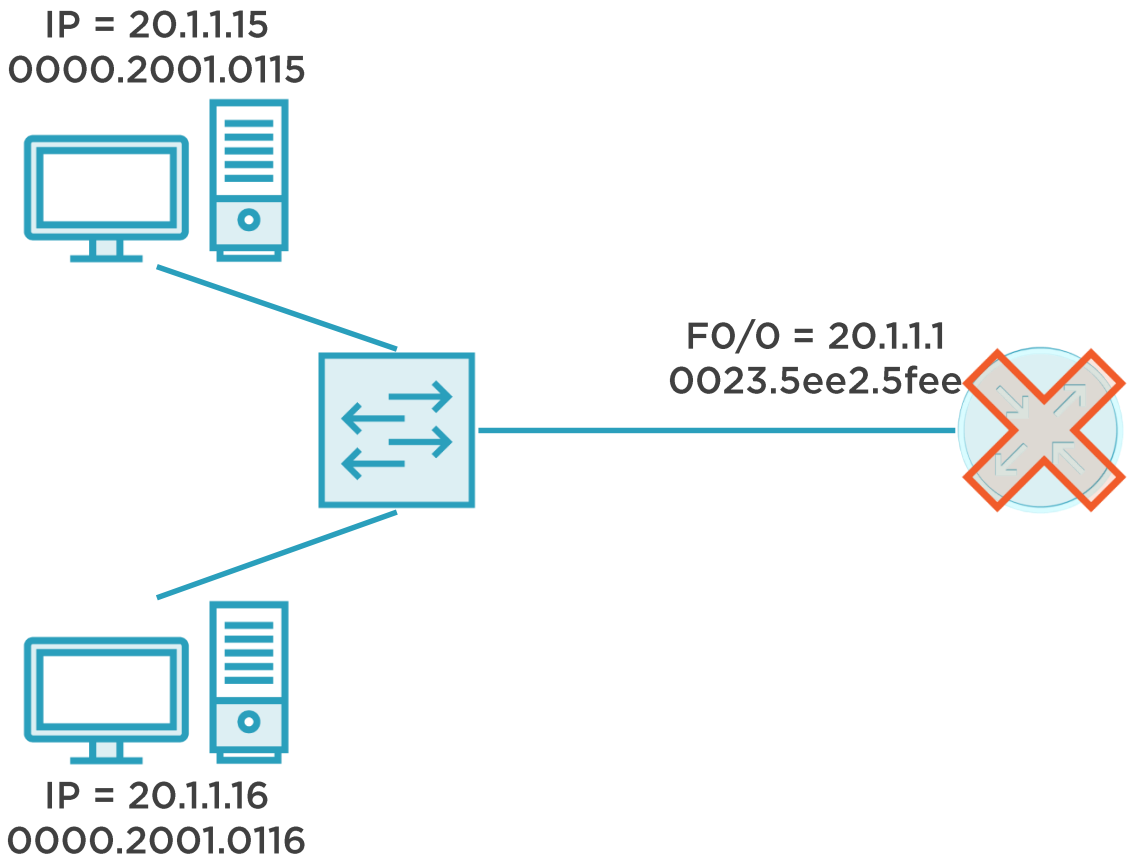
- Symptom is that host's services are unavailable
- Host loss will result in ARP requests for that host remaining unanswered
- Solution is to fix disconnected host or any firewalls

Gateway Connectivity Loss

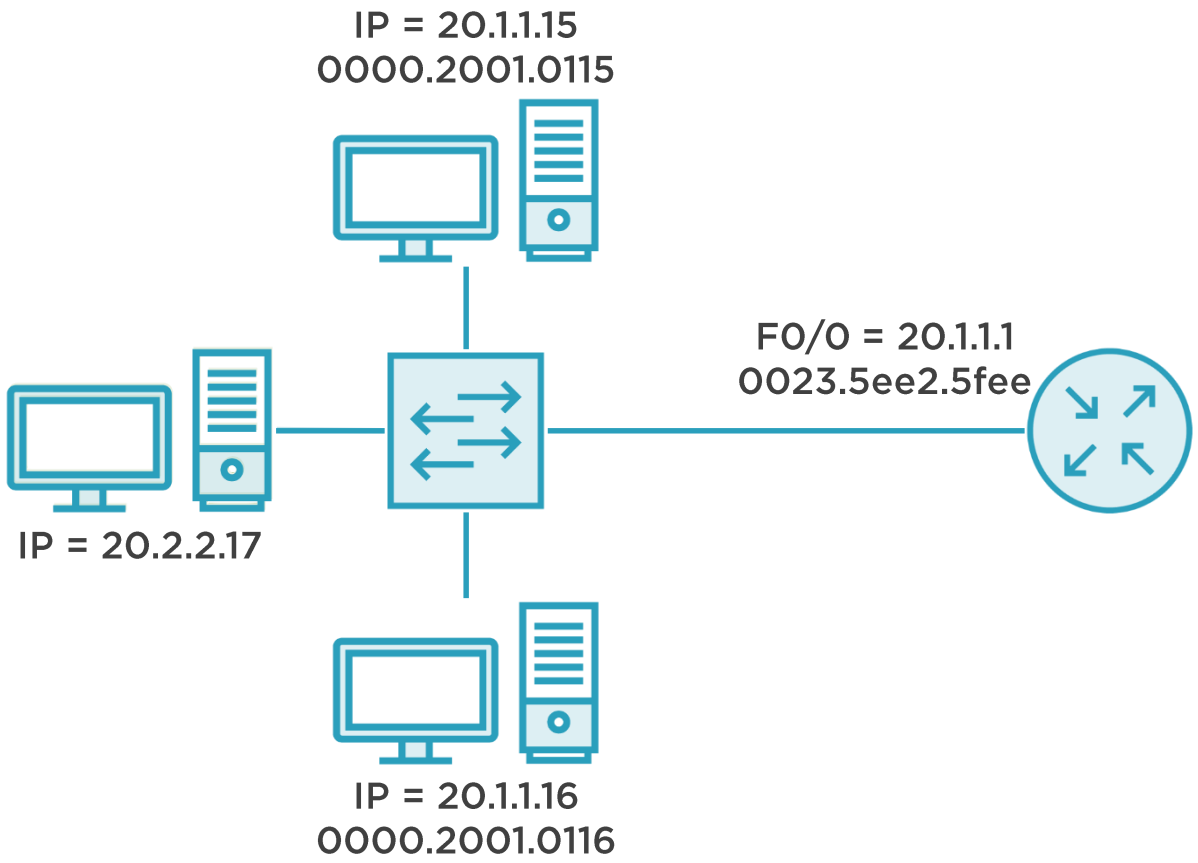


- Symptom is that anything outside the LAN is unavailable
- Gateway loss will result in ARP requests from all active LAN hosts remaining unanswered
- Solution is to fix the default gateway

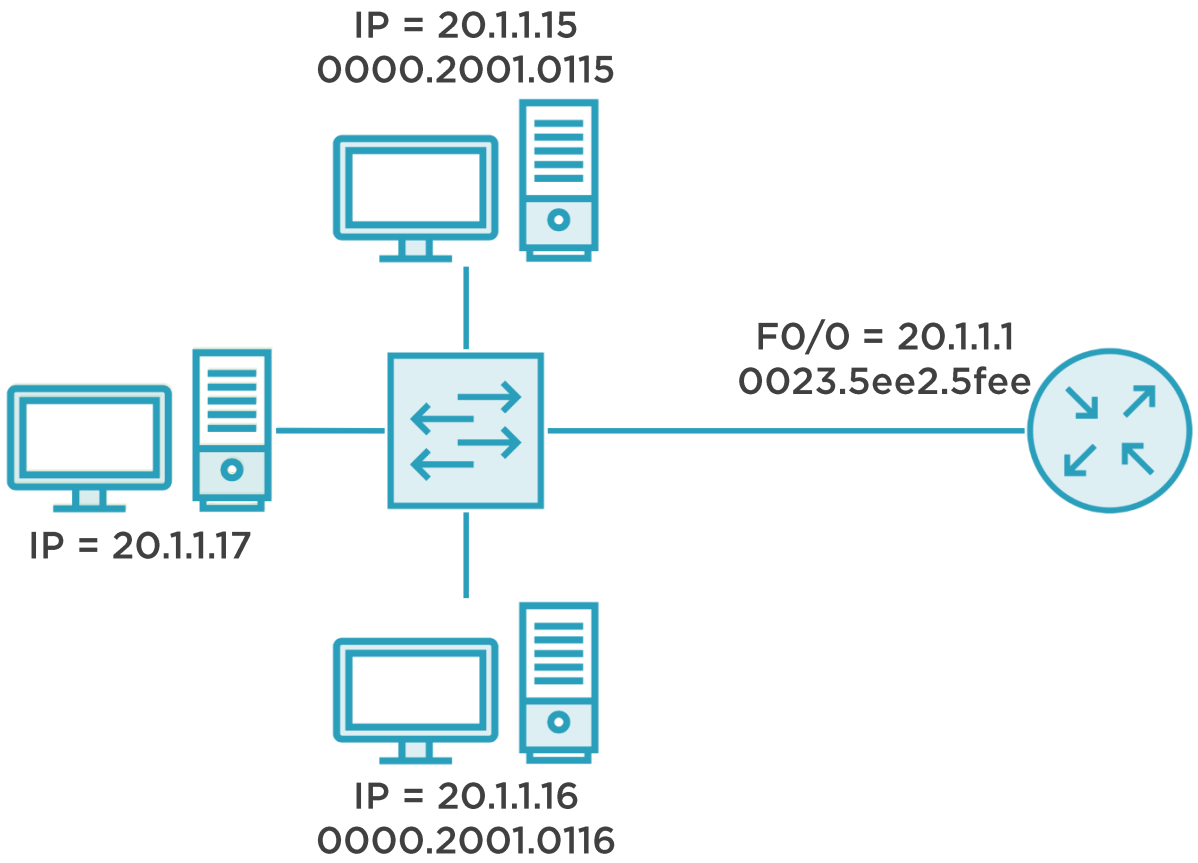
Gateway Connectivity Loss



Incorrect VLAN or IP Assignment



Incorrect VLAN or IP Assignment



Overview

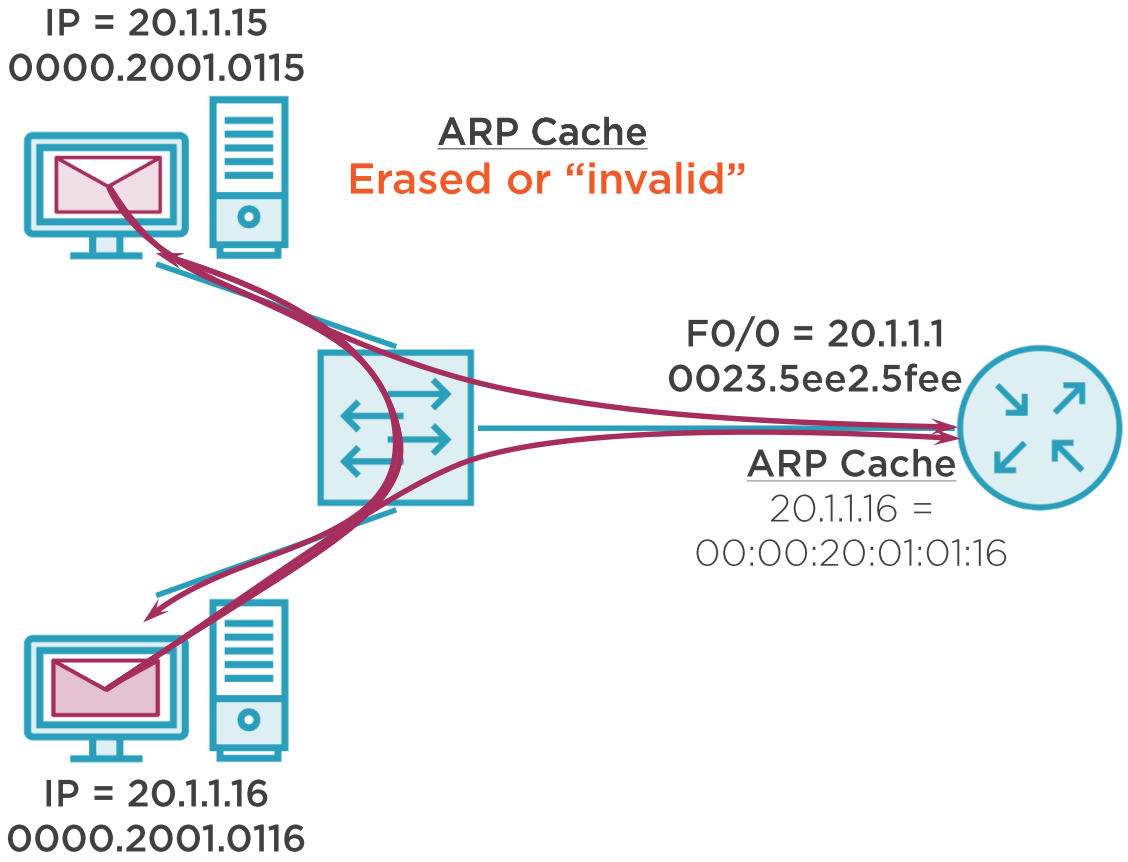
Dynamic ARP behaviors keep entries current

Stale ARP cache entries can lead to lost communication

Fixes

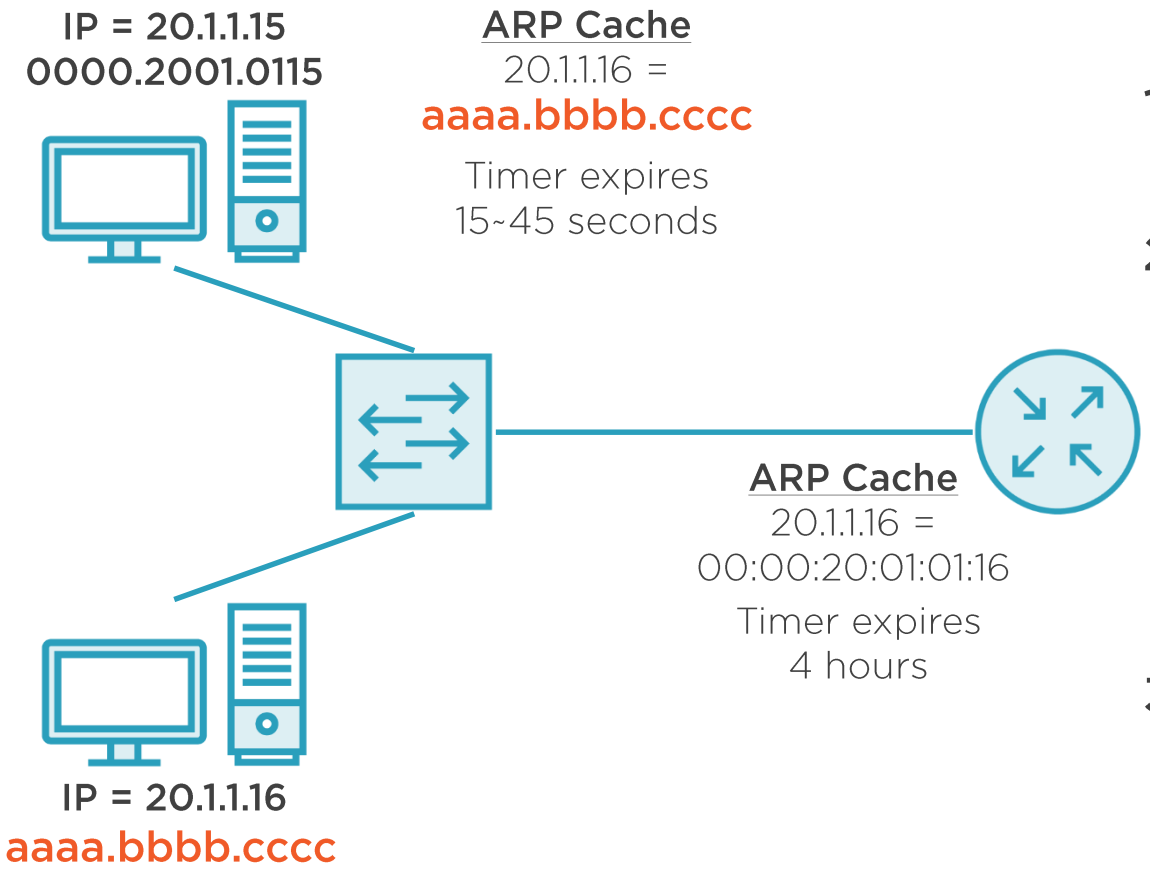
- Clearing ARP cache
- Changing ARP cache timers
- Changing end systems

Keeping ARP Entries Current



1. Send ARP Request if no entry exists in ARP Cache
2. ARP cache entry timers force:
   a. ARP requests for update (rule 1)
   b. Stale/erase the entry (leads to rule 1)
3. Gratuitous ARP updates network on significant NIC changes

Stale ARP Entries



1. Dynamic ARP entry timers allow updates & refreshes
2. Some changes to NICs do NOT force gratuitous ARPs
   a. Some Linux MAC address changes (without interface bounce)
   b. Some redundancy failover software
3. Long timers retain false ARP information

Summary

Stale ARP cache entries rarely cause problems due to dynamic ARPs robustness

Problems occur when lack of dynamic updates cross with long ARP cache timers

Fixes include:

- Clearing ARP caches
- Changing timers
- Change software or people processes to force updates
- Create stability in the LAN

Demo

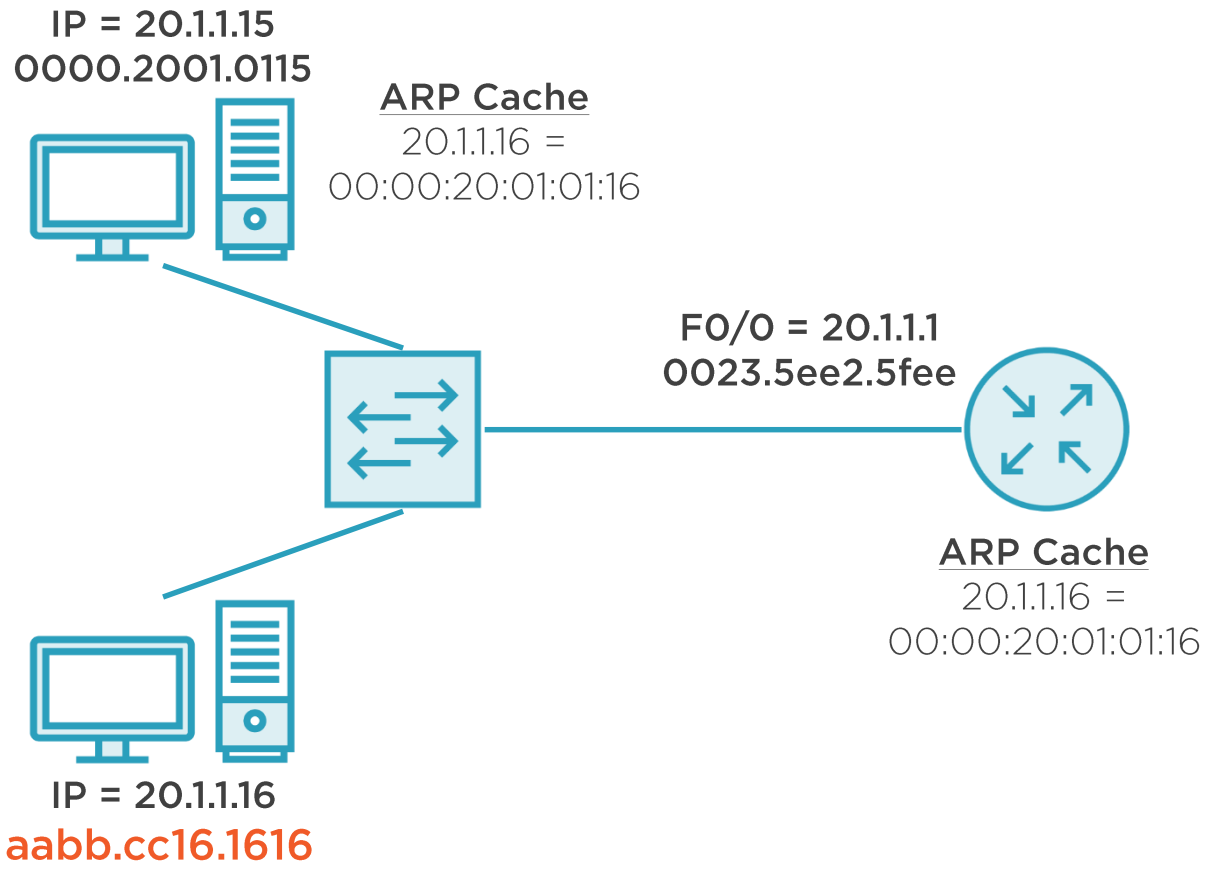
Stale ARP cache entries

Variations in ARP error handling

Clearing the ARP Cache

Fix problems with ARP cache timers

Stale ARP Entries



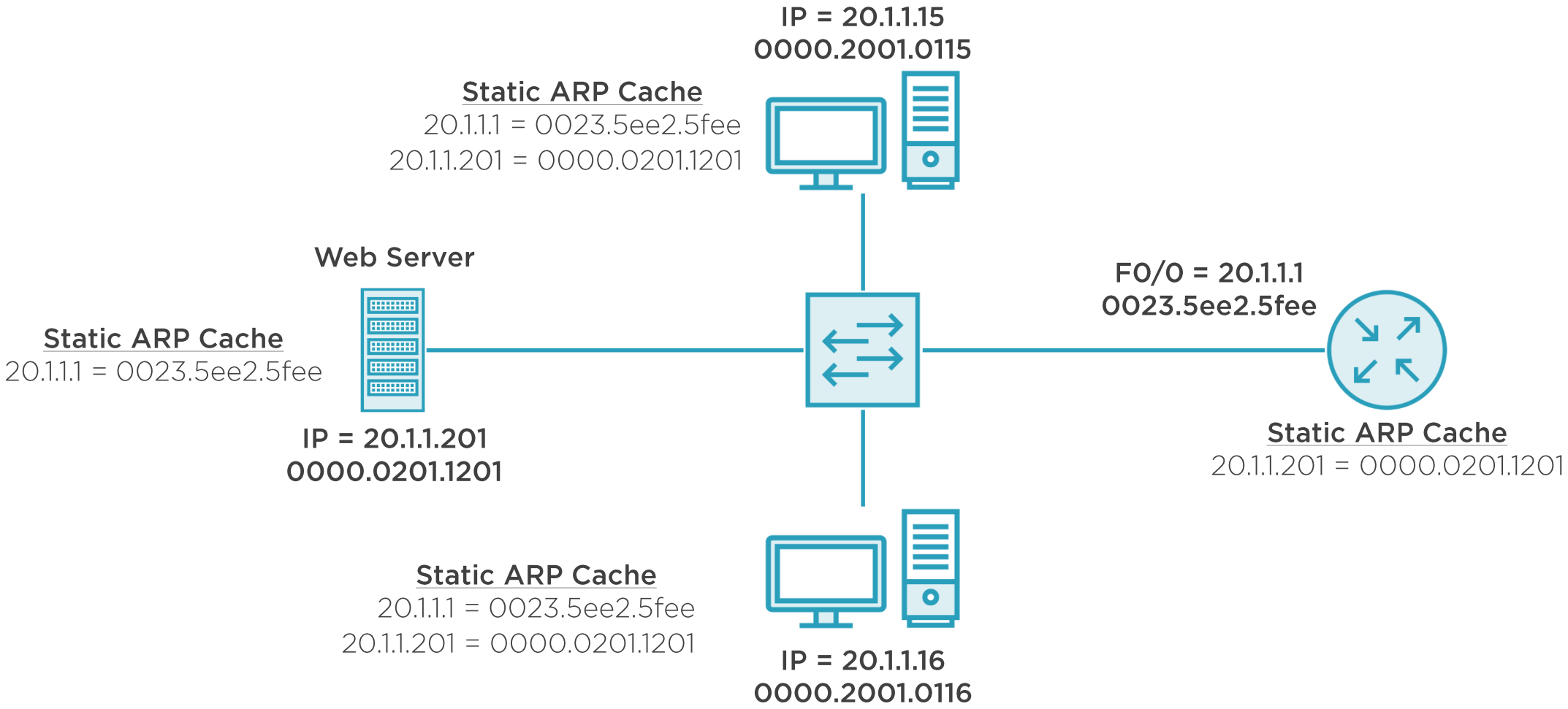
Overview

Static ARP use cases (pros & cons)

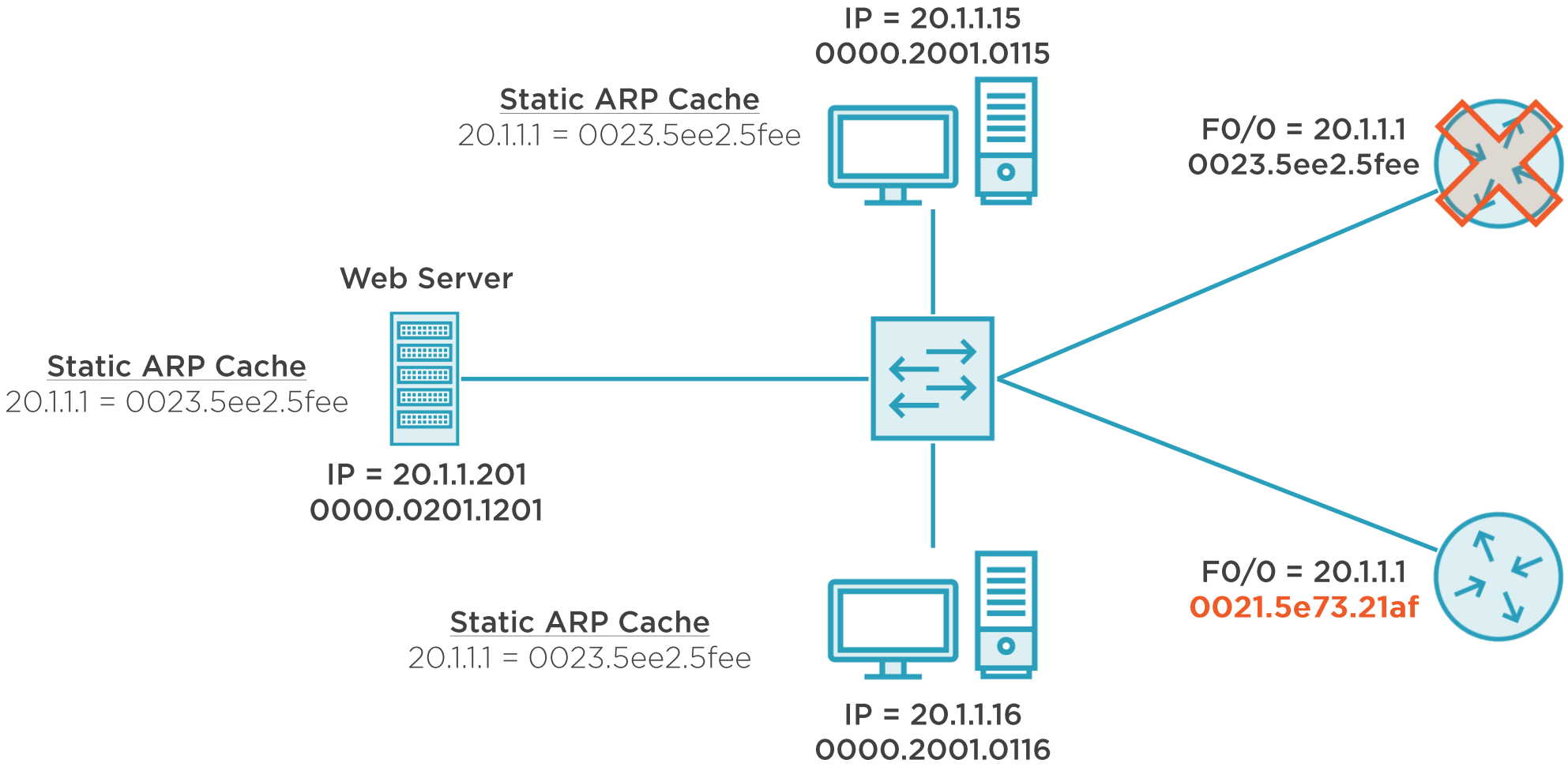
Static ARP problems

Identification and correction

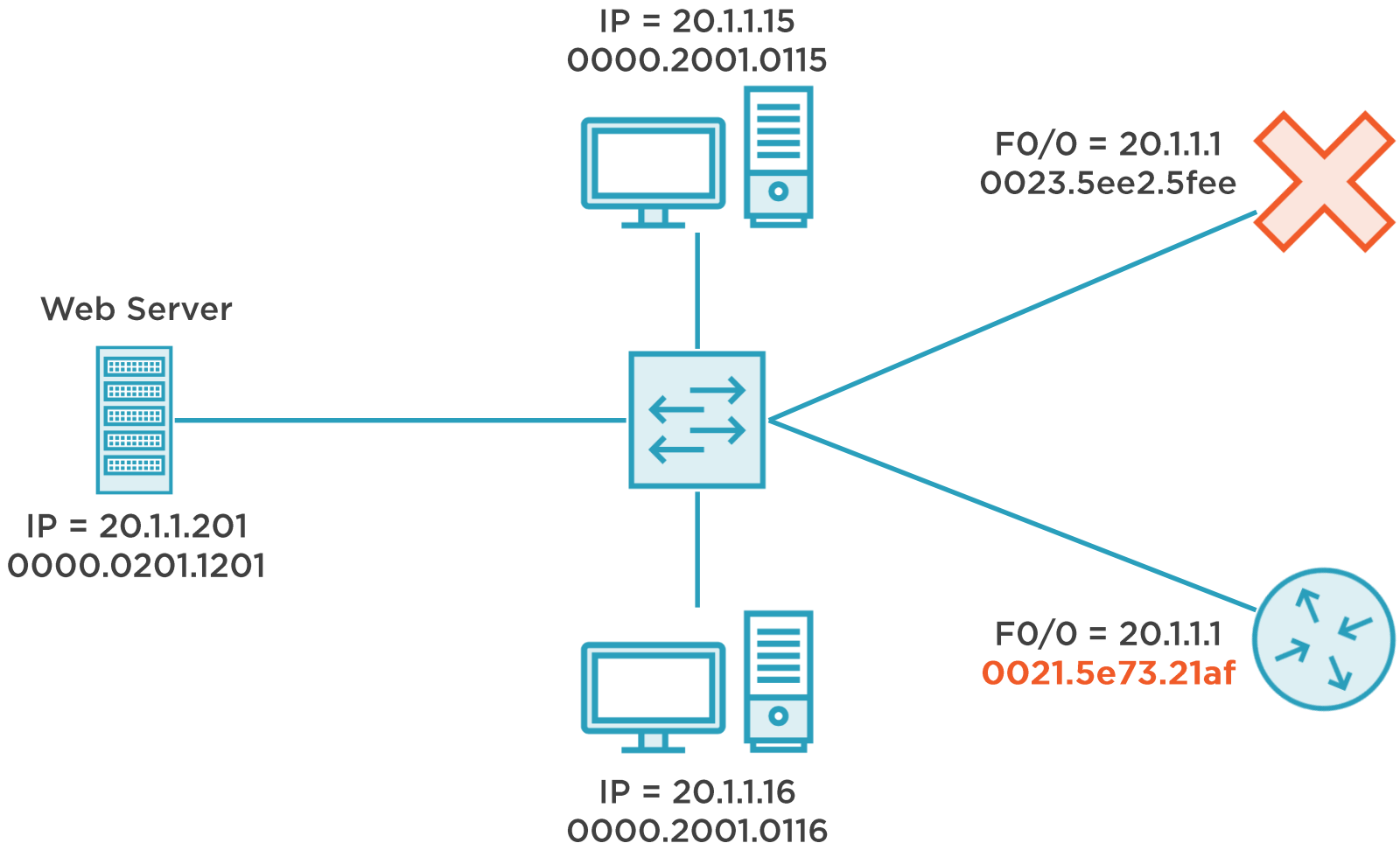
Static ARP Use Cases



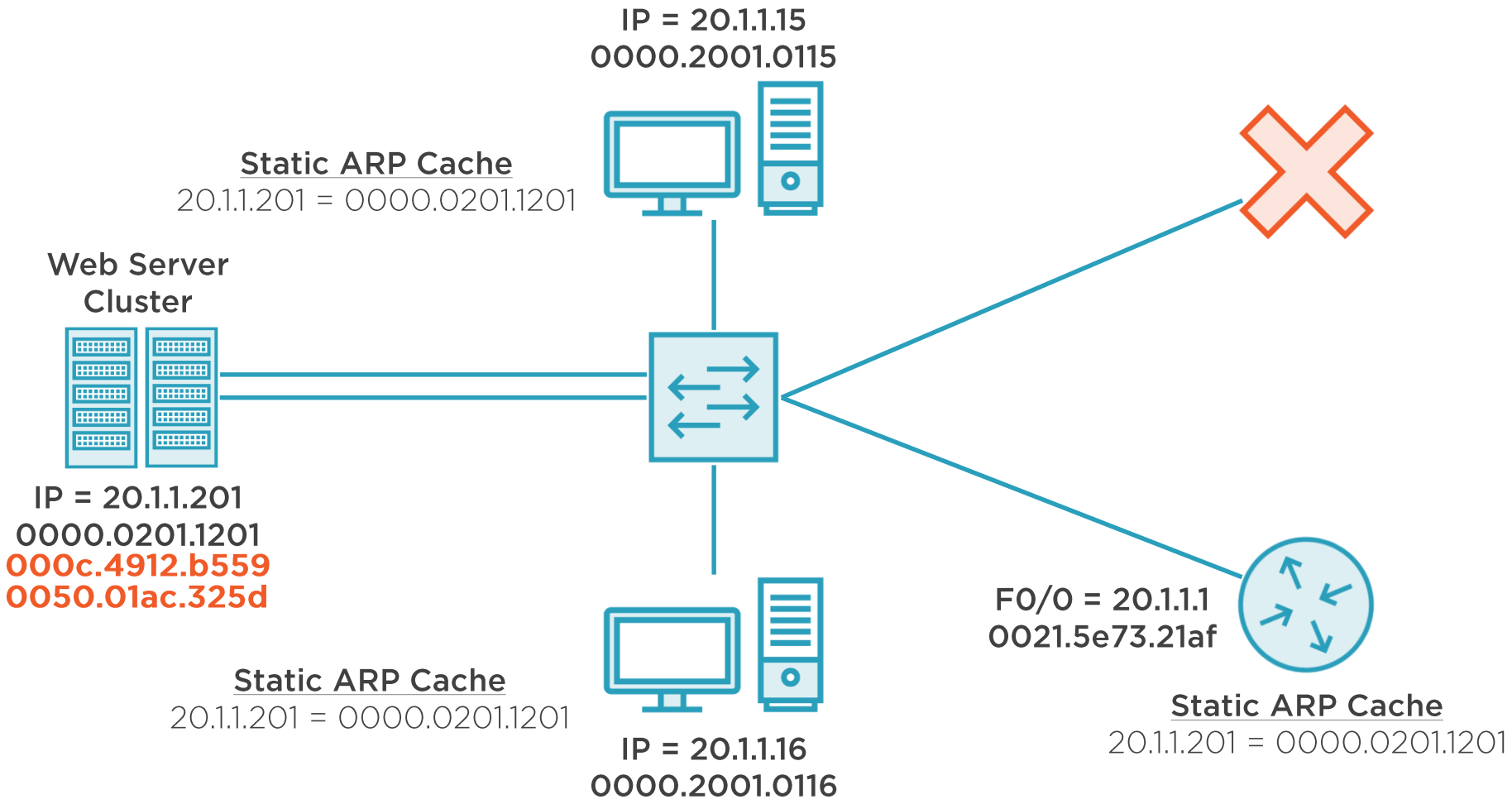
Static ARP Problems



Static ARP Problems



Static ARP Problems



Summary

IP-to-MAC binding changes require static ARP updates or problems occur

Symptoms include losses of connectivity which may appear sporadic

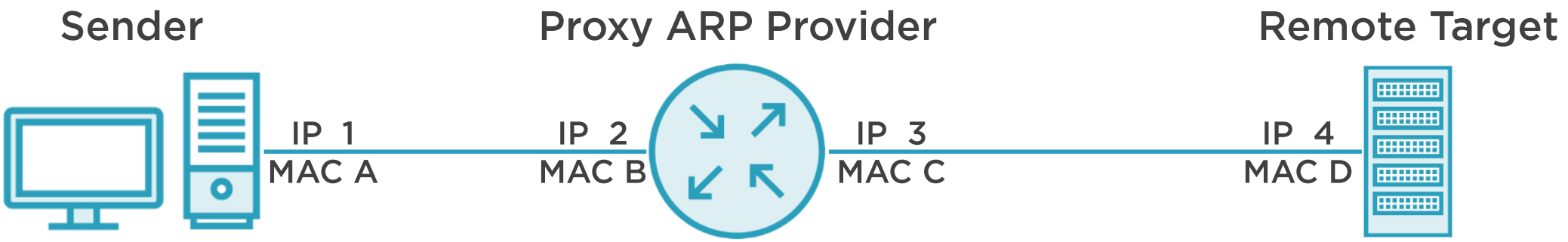
Static ARP management overhead exceeds value of any benefits

Overview

Issues with proxy ARP

- Knowing when you need it
- Consequences of disabling proxy ARP
- Blackholes
- Overhead

Proxy ARP – Basics

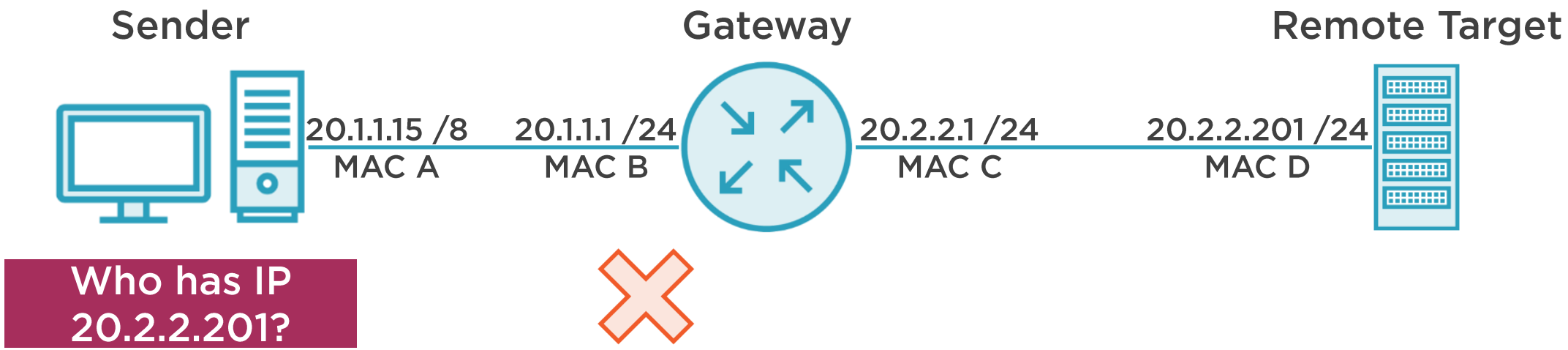


IP 4 is at B

IP 4 is at MAC B

1. Sender must believe the remote target is on the same local broadcast subnet
2. Proxy ARP provider must have some knowledge* of the target
3. Proxy ARP provider must be able to respond to ARP requests as a proxy

Proxy ARP – Unavailable



ARP Scenario

Sender believes target is on the SAME broadcast subnet and sends ARP requests

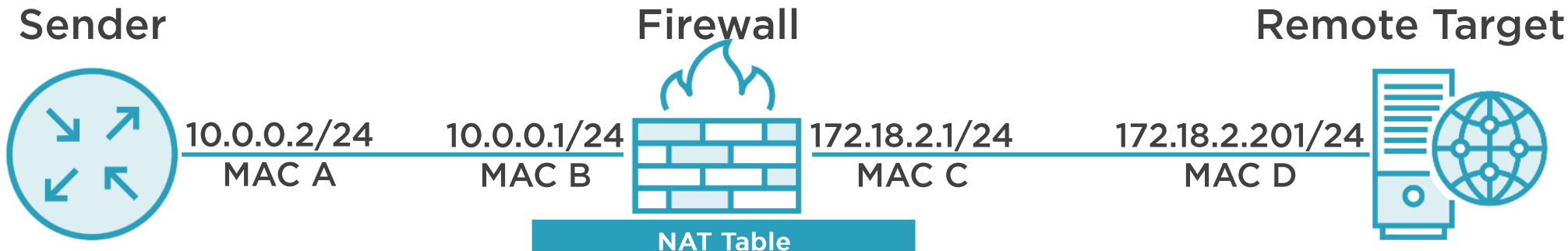
Problem

Gateway has proxy ARP disabled.
It will NOT respond to ARP requests for target

Solutions

1. Enable proxy ARP on gateway
2. Correct senders mask, disable proxy ARP and use routing

Proxy ARP – Firewalls & NAT



Route to 50.5.5.201

NAT Table	
Outside IP	Inside IP
50.5.5.201	172.18.2.201
50.5.5.202	172.18.2.202

ARP Scenario

Sender believes target is on the SAME broadcast subnet and sends ARP requests

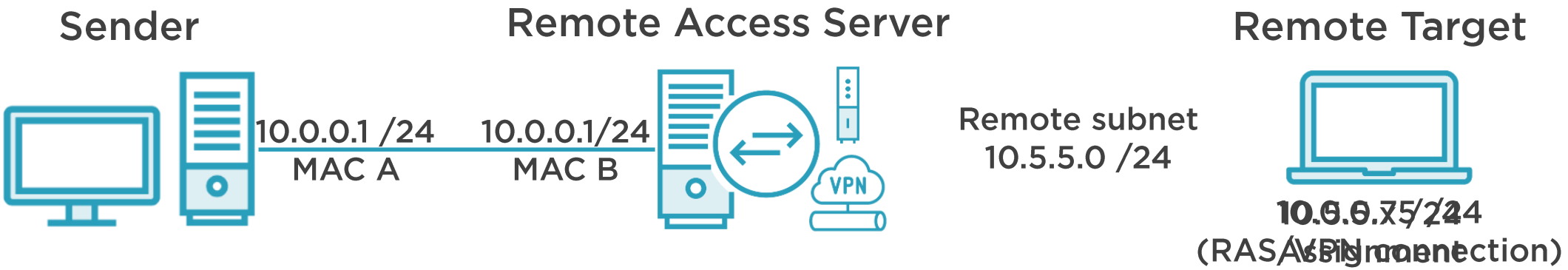
Problem

Firewall has proxy ARP disabled. It will NOT respond to ARP requests for target

Solutions

1. Enable proxy ARP provider
2. Disable proxy ARP. Use different subnet* for NAT translation. Use routing

Proxy ARP – Remote Access



Who has 10.0.0.75 **Route to 10.5.5.0 subnet**

ARP Scenario

Sender believes target is on the SAME broadcast subnet and sends ARP requests

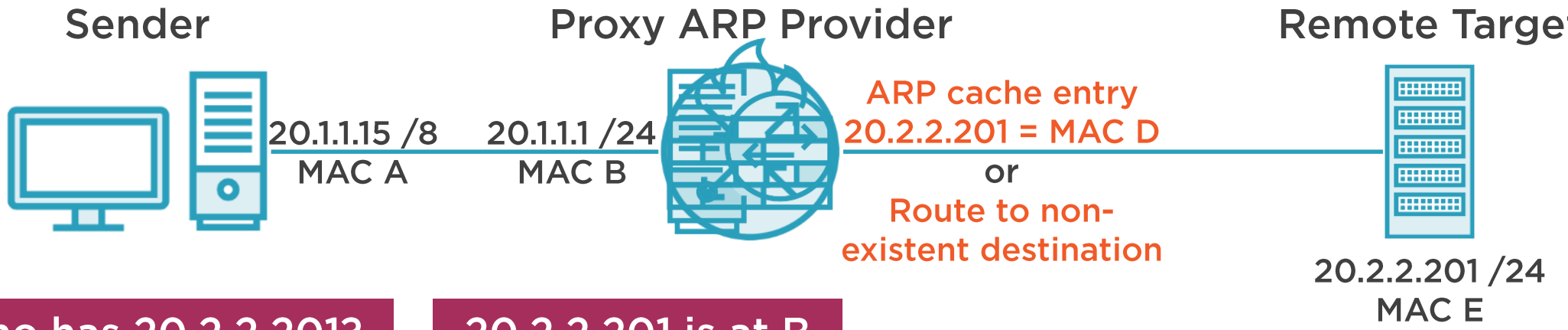
Problem

Remote Access Server has proxy ARP disabled.
It will NOT respond to ARP requests for target

Solutions

1. Enable proxy ARP provider.
2. Disable proxy ARP. Use different subnet* for remote clients. Use routing

Proxy ARP – Blackhole



ARP Scenario

Sender believes target is on the SAME broadcast subnet and sends ARP requests

Problem

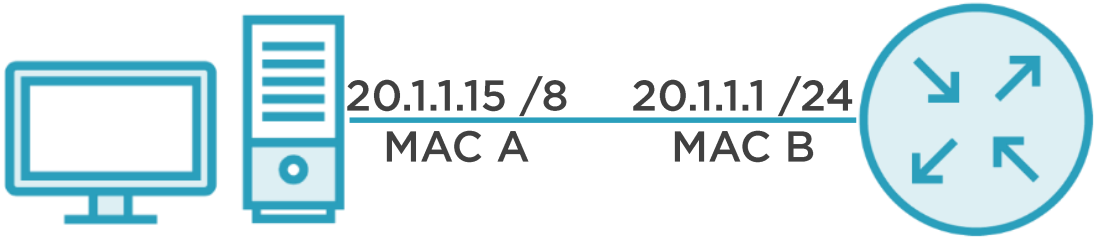
The proxy ARP provider falsely believes it has connection or route to remote host

Solutions

1. Remove false information
   1. Route to destination
   2. Clear cache inconsistencies
2. Disable Proxy ARP and correct the sender's mask to use routing

Proxy ARP – Overhead

Sender



Gateway Proxy ARP

Remote Subnets

20.2.2.0 /24
20.4.37.0 /24
20.88.123.0/24
20.3.18.0 /23
20.5.96.0 /19
20.17.0.0 /16

Who has 20.x.x.x?

20.x.x.x is at C

<u>ARP Scenario</u>

Sender believes target is on the SAME broadcast subnet and sends ARP requests

<u>Problem</u>

Gateway has large subnets related to sender. Overhead required on router CPU/interface, network traffic and sender ARP cache

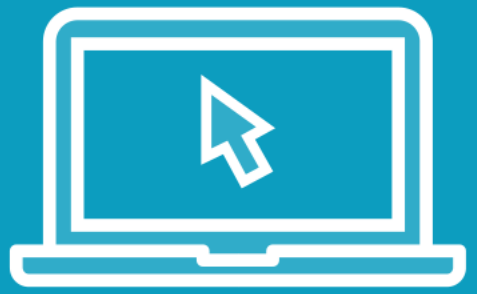
<u>Solutions</u>

1. Correct the sender's mask, disable proxy ARP and use routing

Proxy ARP Problems & Solutions

Proxy ARP is disabled	Blackhole	Firewall/RAS target in same subnet	Overhead
Enable Proxy ARP or Use routing	Repair false information or Use routing	Enable Proxy ARP or Switch target subnet	Disable and use routing

Demo

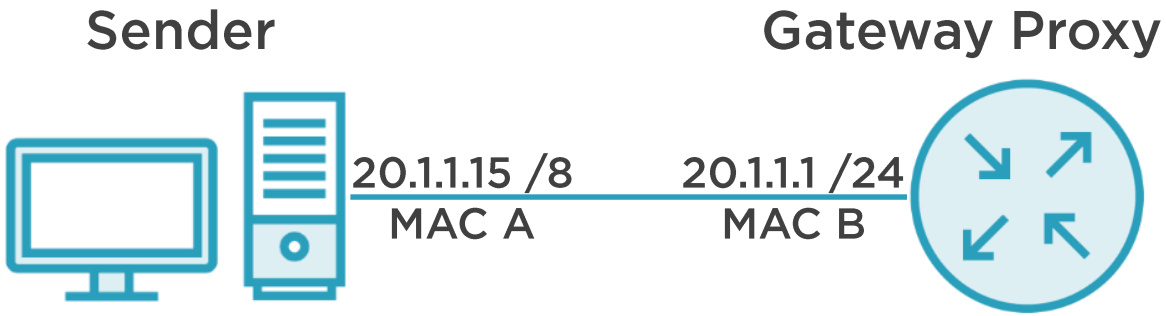


Proxy ARP Overhead

- Decreased router performance
- Increase in ARP network utilization
- Increase in host ARP caches

Remove Proxy ARP for routed solution

Proxy ARP – Overhead



Remote Subnets

Fastethernet 0/1 - 20.2.2.0 /24
Loopback 37 - 20.4.37.0 /24
Loopback 123 - 20.88.123.0/24
Loopback 96 - 20.5.96.0 /19

Demo

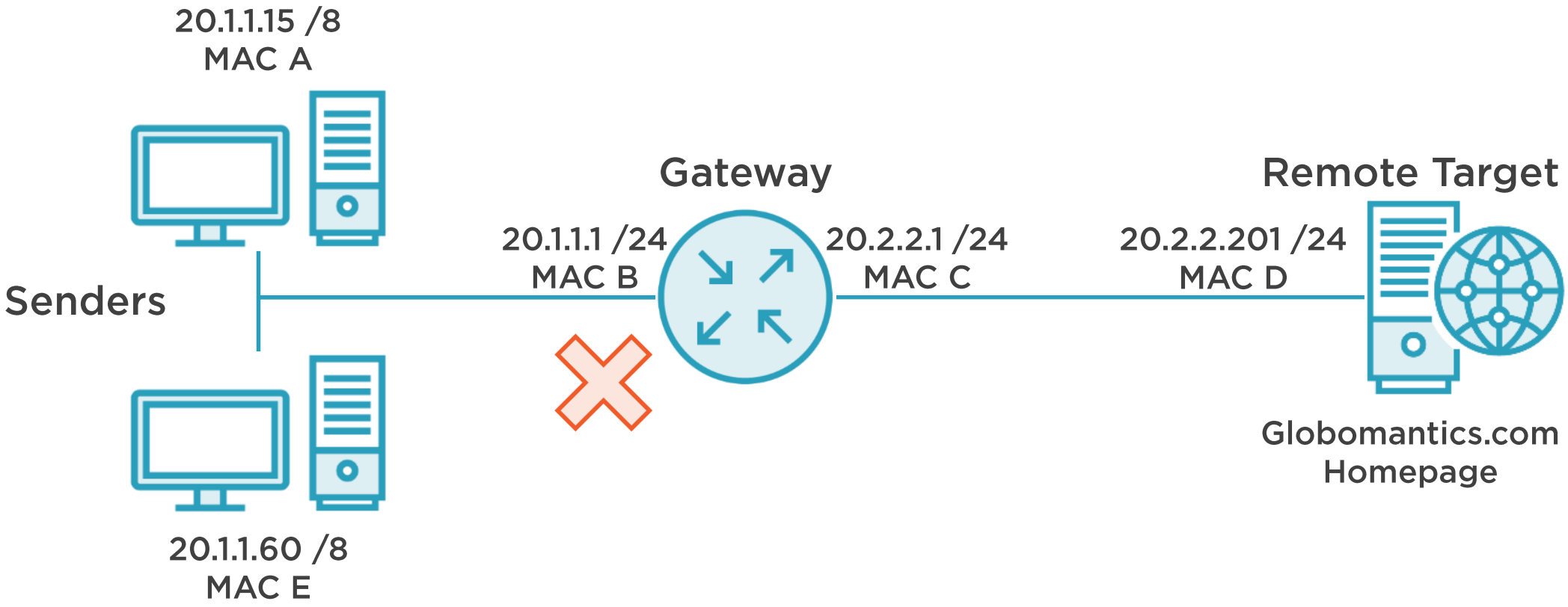
Proxy ARP Unavailable

- Windows 10 reaction
- Ubuntu Linux reaction

Fixing the problem

- Return proxy ARP
- Fix endpoints

Proxy ARP – Unavailable



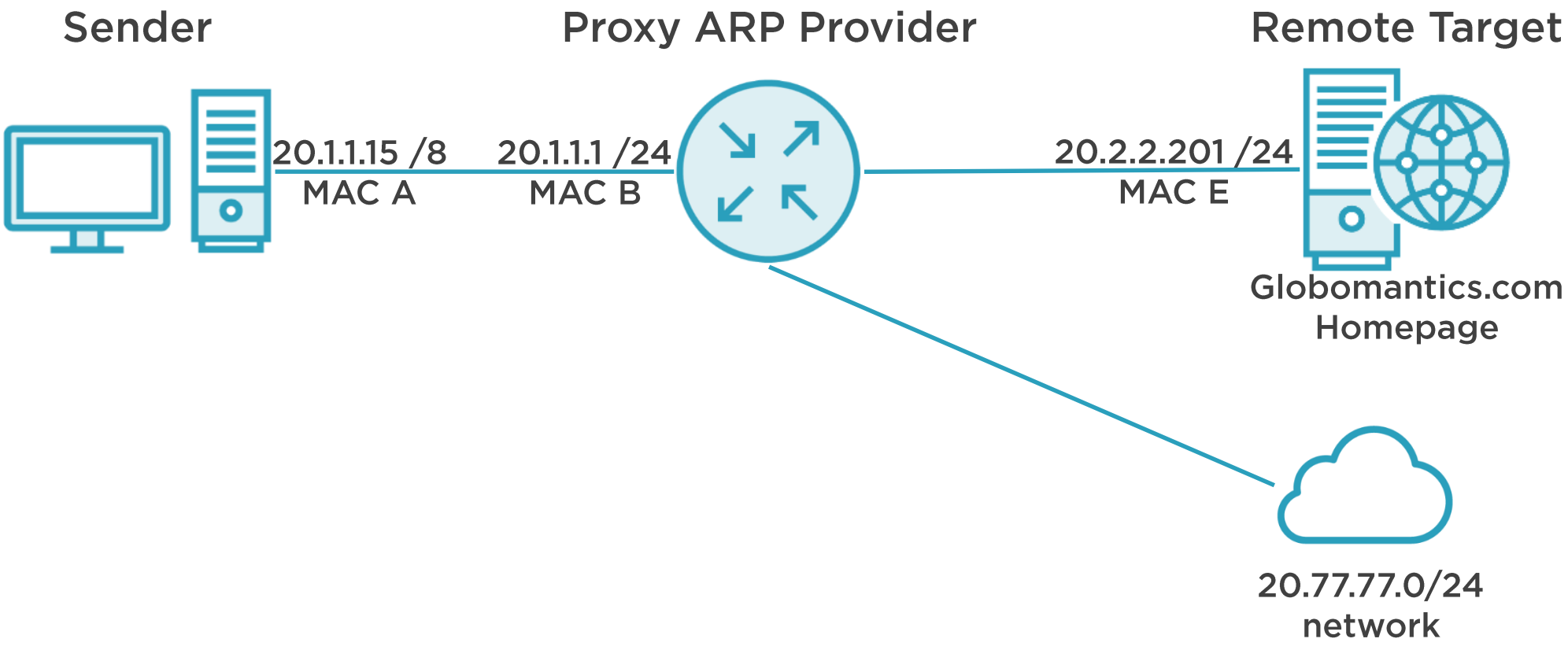
Demo

Proxy ARP and data blackholes

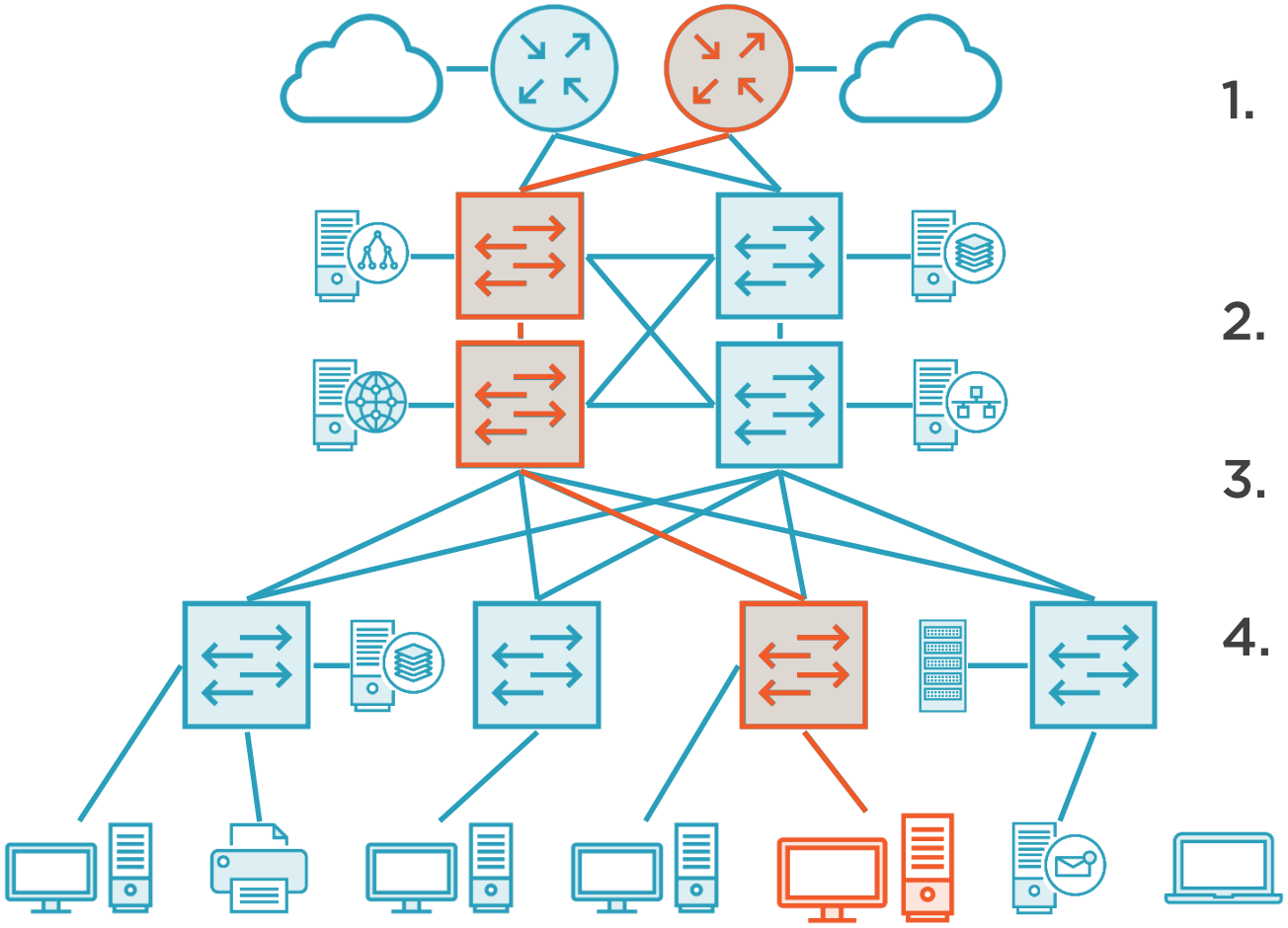
- Confusion when troubleshooting
- Basis for attacks

Solutions

Proxy ARP – Blackhole



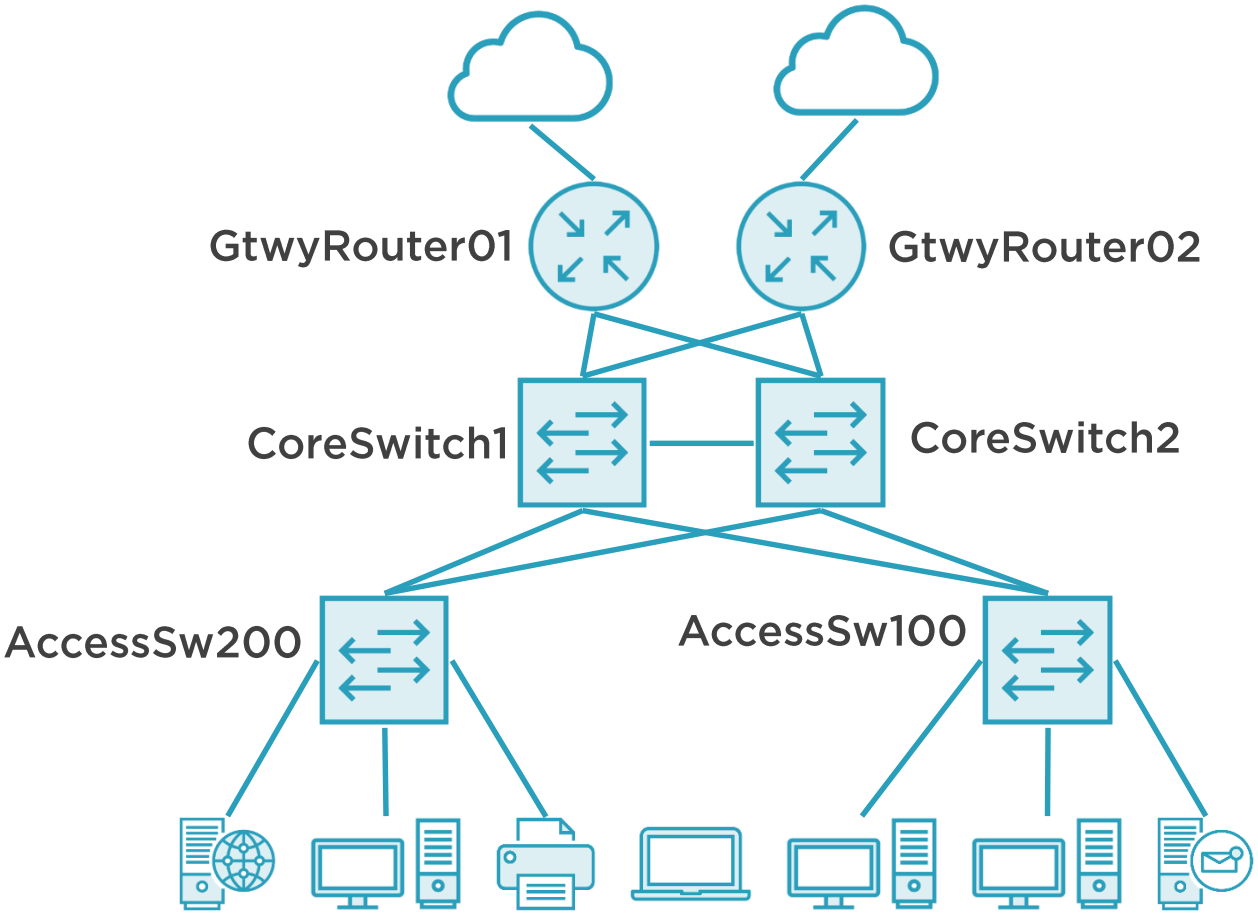
Finding a Host in the Complex LAN



Methodology

1. Start with the gateway router or layer-3 switch for the selected network or VLAN
2. Ping the target to ensure target's IP & MAC up-to-date and in local ARP cache
3. Inspect ARP cache on gateway for the matching IP and associated MAC
4. Interrogate switch MAC address tables along path to find port with ONLY that MAC address!

Finding a Host in the Complex LAN



Target

Find 20.1.1.5 in the internetwork

1. Ping 20.1.1.5
2. Show arp 20.1.1.5 (to get MAC)
3. Jump to a core switch
4. Find target MAC in switch tables
5. Jump to each switch until target is on one physical interface

“Using quotes in your slides can be powerful if used sparingly.”

Heather Ackmann