Understanding InARP, GARP, RARP, and Proxy ARP

Jim Rizzo
NETWORK ENGINEER AND SECURITY LEADER

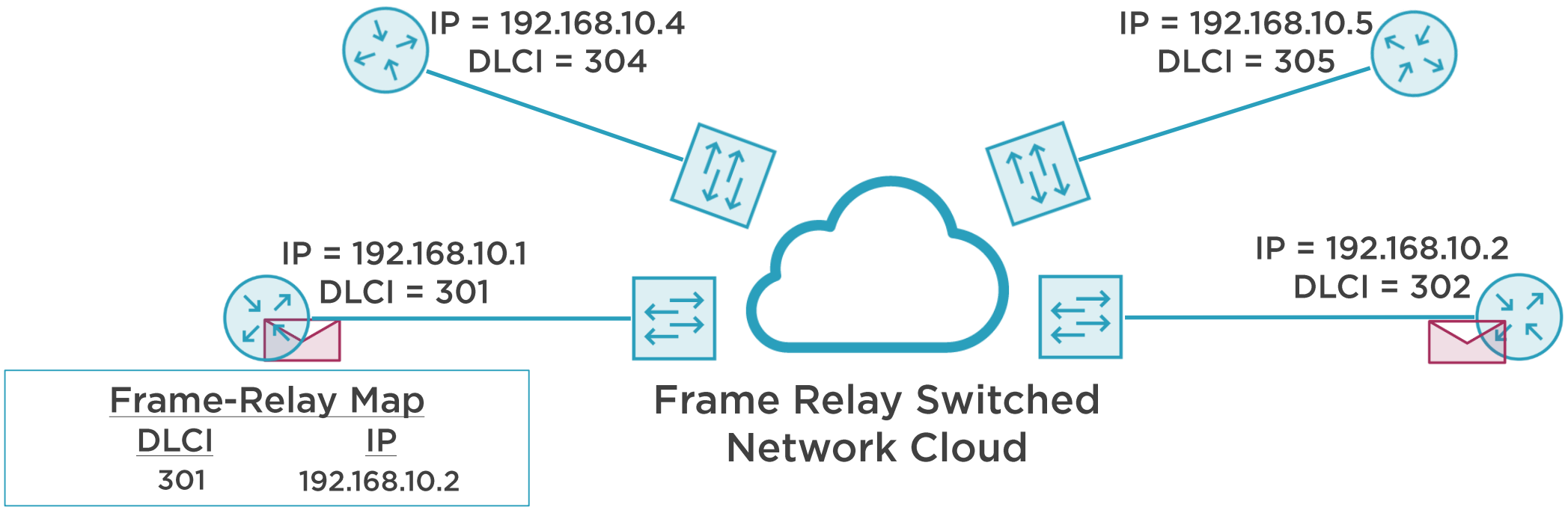
Overview

- Inverse ARP
- Reverse ARP
- Gratuitous ARP
- IP Conflict (DHCP) ARP
- Proxy ARP

ARP vs. Inverse ARP (InARP)

ARP	Inverse ARP (InARP)
Maps Layer-3 to Layer-2 address	Maps Layer-2 to Layer-3 address
Binds IP address to MAC address	Binds [virtual] circuit ID to IP address
Shared media broadcast LAN	Layer-2 switched networks
Ethernet networks	Frame-Relay or ATM networks
Can be static or dynamically mapped	Can be static or dynamically mapped

Inverse Address Resolution Protocol (InARP)

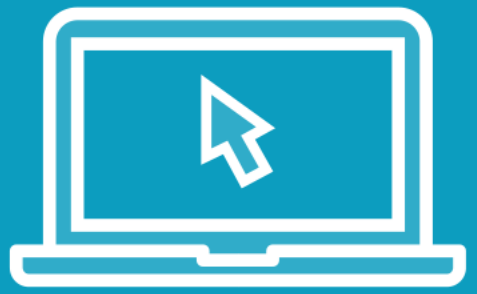


InARP Reply Opcode = 9 DLCI 302 is at 192.168.10.2	Source DLCI 302

Reverse Address Resolution Protocol (RARP) Obsoleted by BOOTP & DHCP

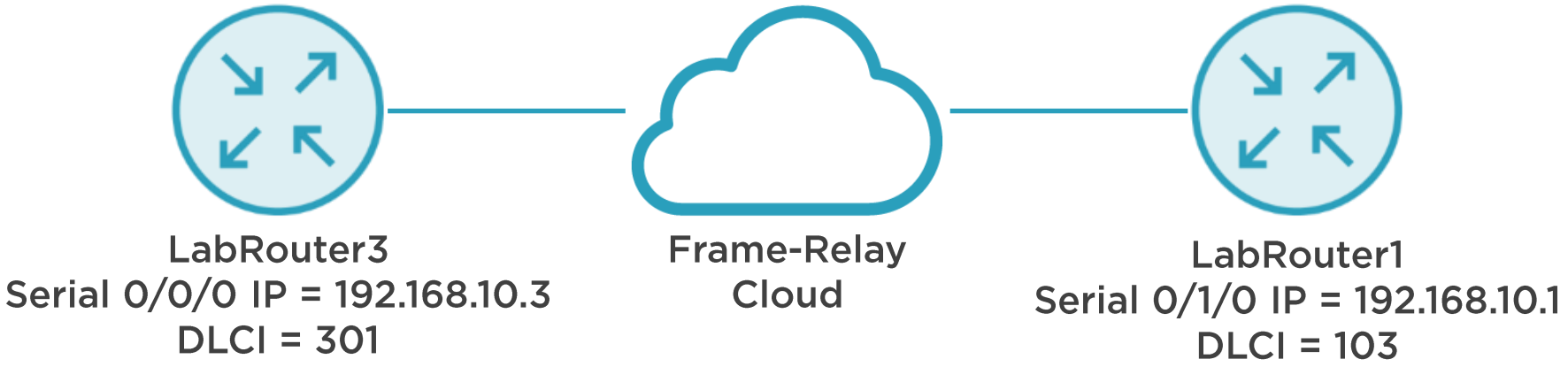
RARP Reply	Type	Source	Destination
Opcode = 4 01:01:01:AA:AA:AA Use IP = 10.2.2.97	RARP (0x0835)	02:02:02:BB:BB:BB	01:01:01:AA:AA:AA

Demo



- Cisco's IOS – frame-relay configuration
- Layer-2 DLCI is mapped to IP addresses
- Commands to configure dynamic InARP
- Debug InARP traffic
- View DCLI to IP mapping
- Disable InARP and create static maps

Frame Relay Configuration



Gratuitous ARP (GARP)

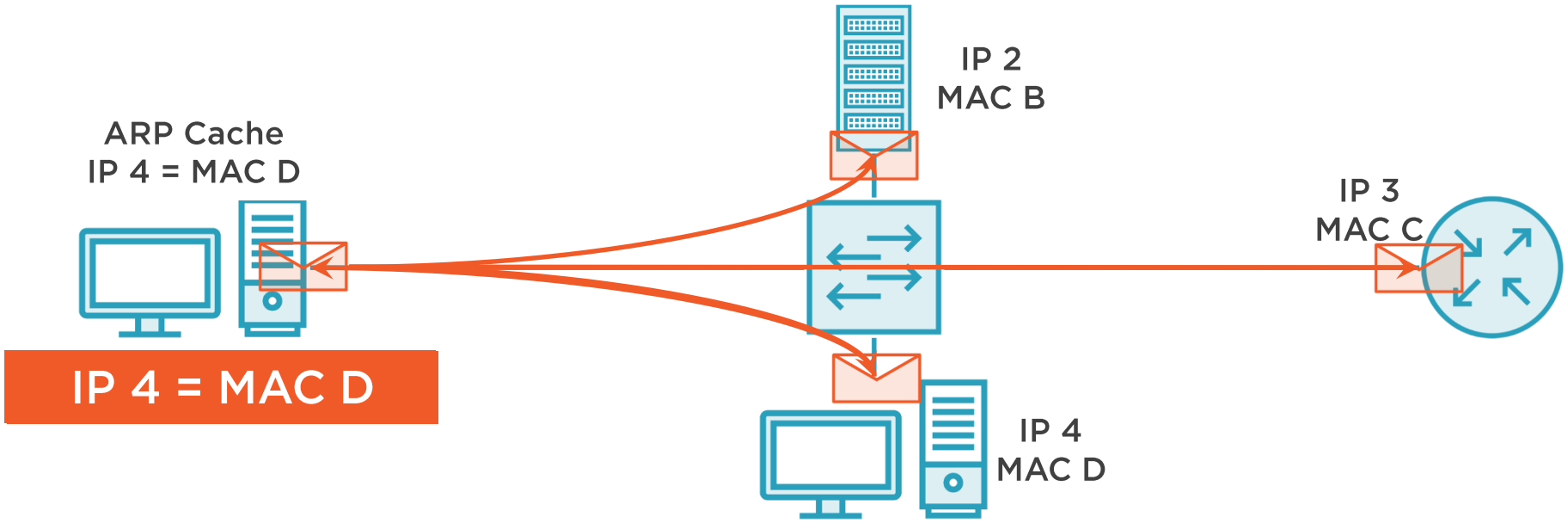
Broadcast from a node to advertise its IP & MAC addresses

Sent without request or expectation of response to synchronize network ARP and MAC address tables

The GARP header has the sender and target set as the issuer's IP

Format can be either GARP Request or GARP Reply

Traditional ARP Function



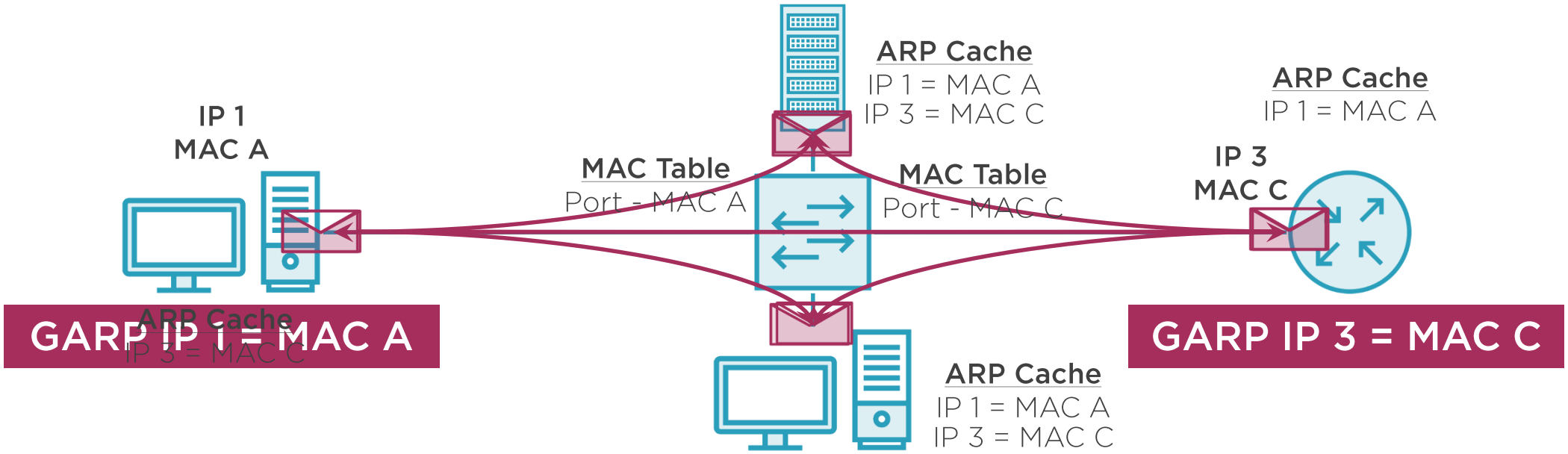
ARP Request (Who has?)	
Opcode Request	1
Sender MAC	A
Sender IP	1
Target MAC	00:00:00:00:00:00
Target IP	4

Dest.	ff:ff:ff:ff:ff:ff
Source	A
Type (ARP)	0x806

ARP Reply (My MAC is)	
Destination	A
Source	D
Type	0x806 (ARP)

Opcode Reply	2
Sender MAC	D
Sender IP	4
Target MAC	A
Target IP	1

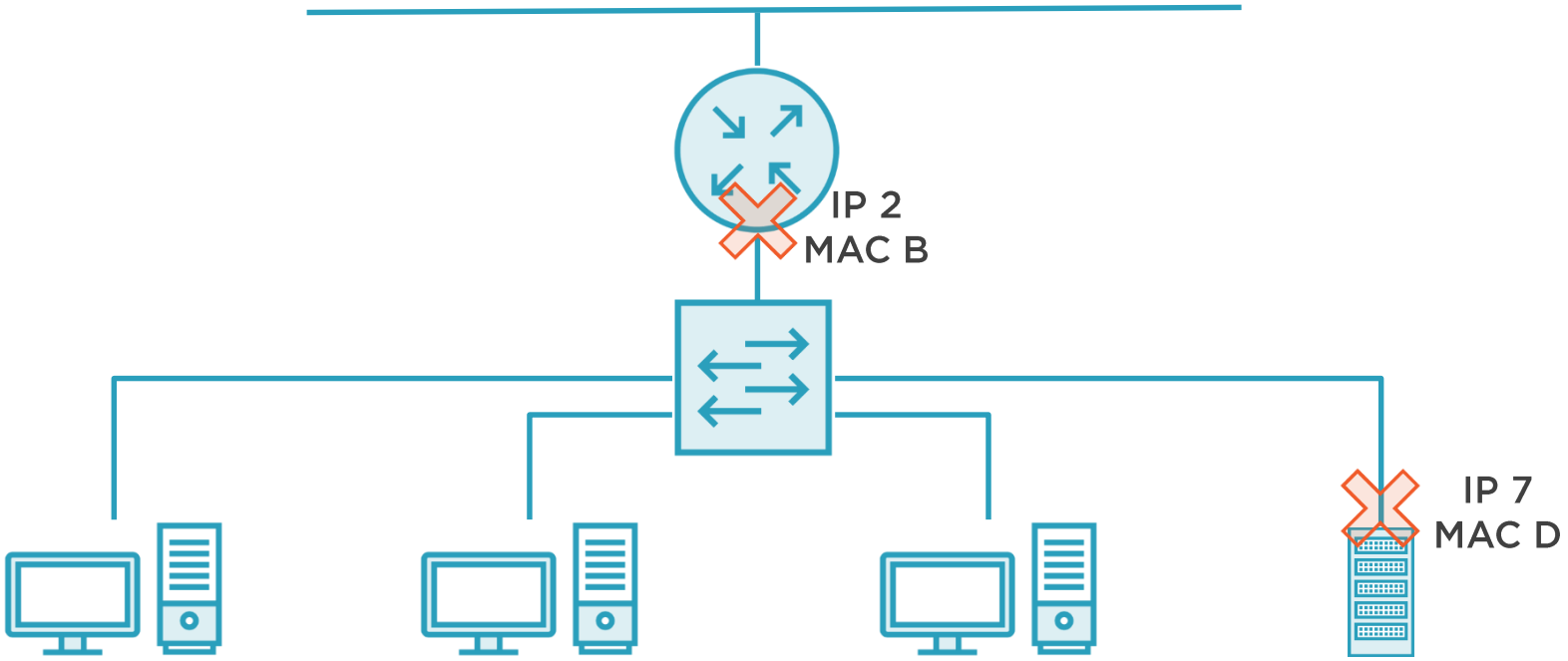
Gratuitous ARP (GARP) Function



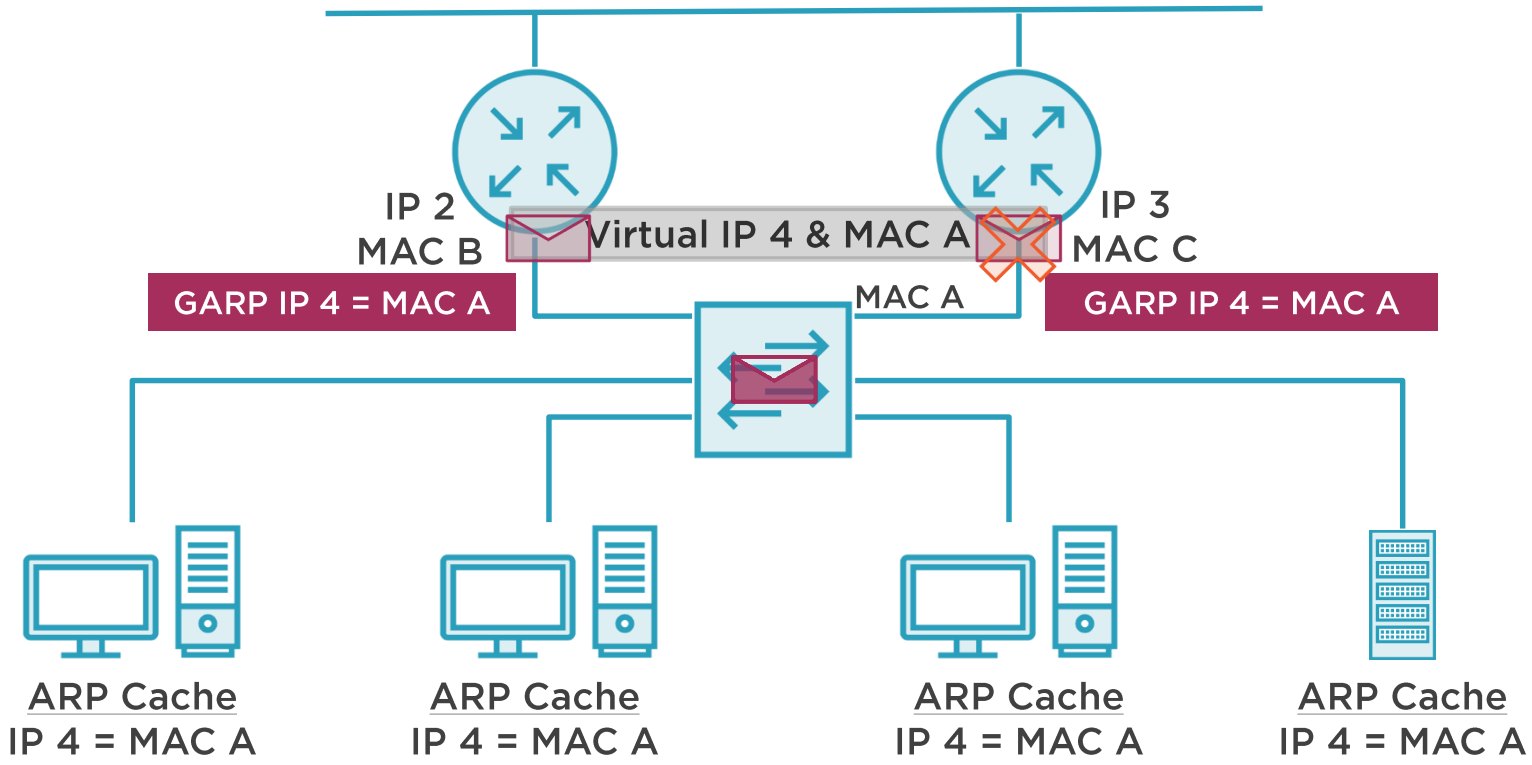
Gratuitous ARP Request			
Opcode Request	1	Dest.	ff:ff:ff:ff:ff:ff
Sender MAC	A	Source	A
Sender IP	1	Type	0x806
Target MAC	00:00:00:00:00:00	(ARP)	
Target IP	1		

Gratuitous ARP Reply			
Opcode Reply	2	Dest.	ff:ff:ff:ff:ff:ff
Sender MAC	C	Source	C
Sender IP	3	Type	0x806
Target MAC	ff:ff:ff:ff:ff:ff	(ARP)	
Target IP	3		

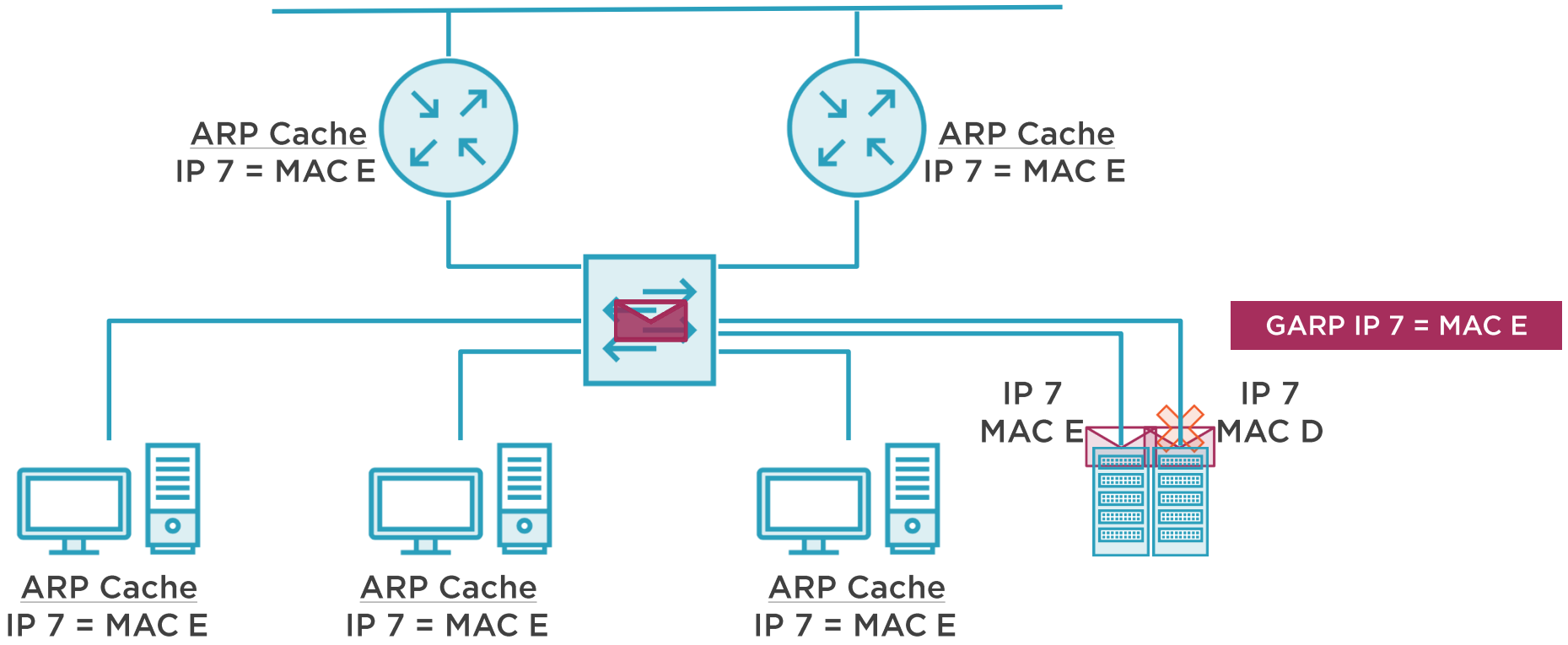
Gratuitous ARP (GARP) and Single Points of Failure



Gratuitous ARP (GARP) and Gateway Redundancy Protocols



Gratuitous ARP (GARP) and Server Redundancy Protocols



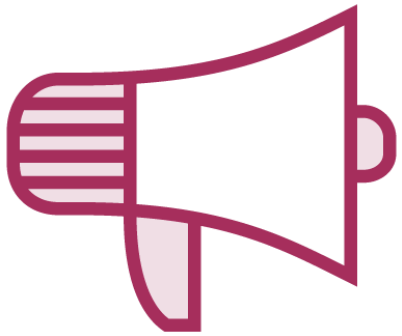
Traditional ARP vs. Gratuitous ARP

Traditional ARP

Functions to update a local machine's ARP cache

Maps known IP address to unknown MAC address

Request and Reply format



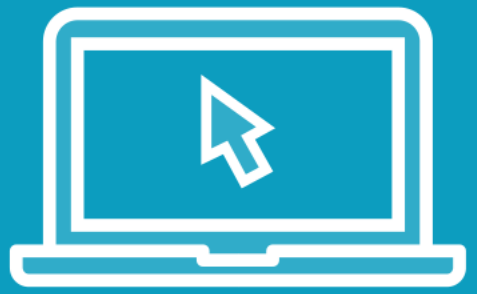
Gratuitous ARP

Functions to synchronize network hosts' ARP caches and MAC tables

Used for host state network state changes and failover redundancies

Request or Reply format

Demo



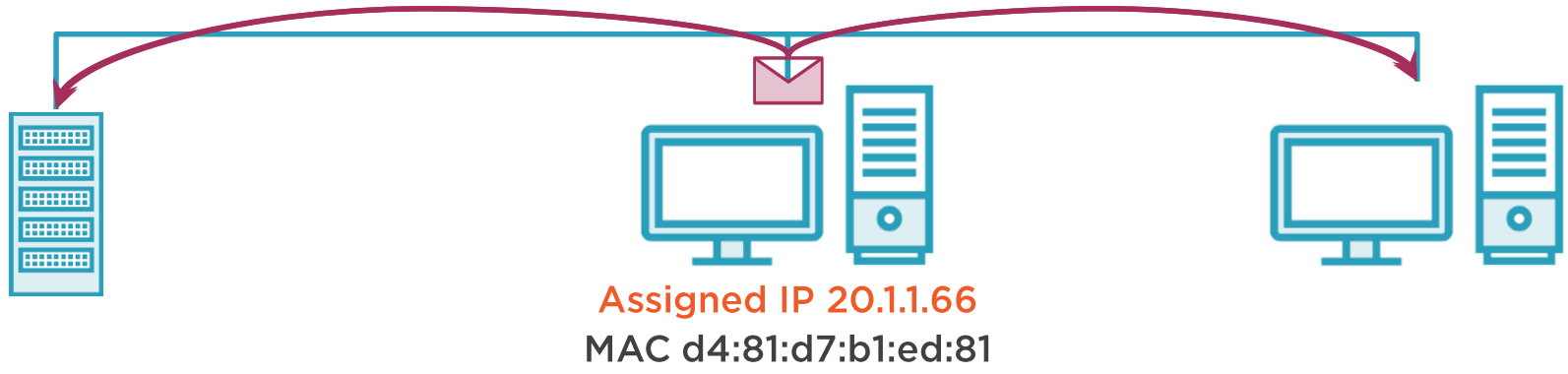
Wireshark captures of Gratuitous ARP

- GARP Request (Windows)
- GARP Reply (Cisco Gateway)

Gratuitous ARP in Router Redundancy

- HSRP Configuration
- GARP Capture of HSRP Failover

ARP Duplicate IP Detection Process



GARP Request			
Opcode Request	1		
Sender MAC	d4:81:d7:b1:ed:81	Dest.	ff:ff:ff:ff:ff:ff
Sender IP	20.1.1.66	Source	d4:81:d7:b1:ed:81
Target MAC	00:00:00:00:00:00	Type	0x806 (ARP)
Target IP	20.1.1.66		

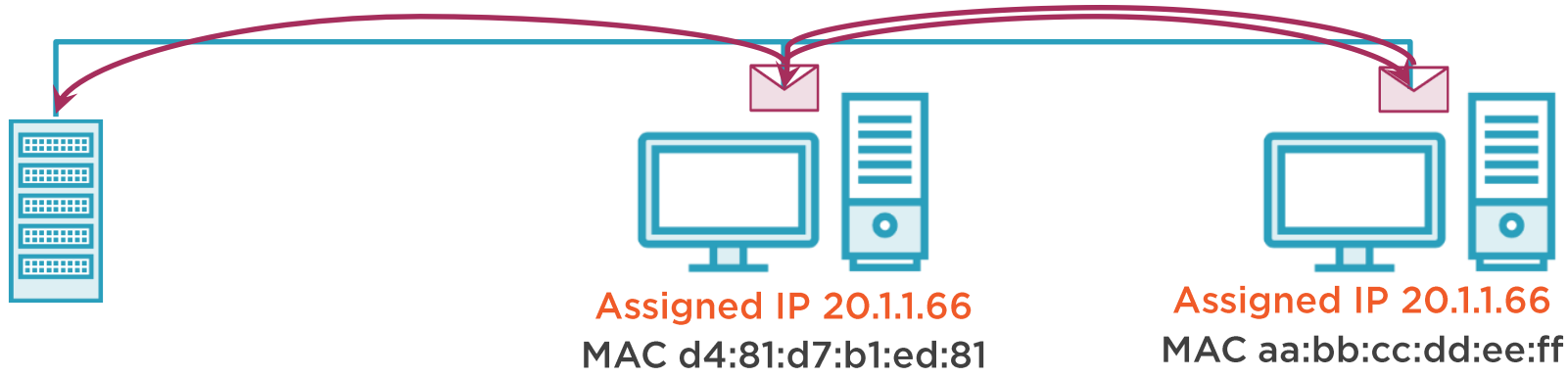
IP assignment (from any means)

Client broadcasts 3 duplicate IP detection ARPs

Without any ARP reply announcing the IP address is in use, client assigns the IP to its interface

Client GARPs to announce itself on the network

ARP Duplicate IP Detection Conflict!



ARP Reply – IP is in use!	
Opcode Request 2	
Sender MAC **aa:bb:cc:dd:ee:ff**	Dest. **d4:81:d7:b1:ed:81**
Sender IP **20.1.1.66**	Source **aa:bb:cc:dd:ee:ff**
Target MAC **d4:81:d7:b1:ed:81**	Type 0x806 (ARP)
Target IP **0.0.0.0**	

IP assignment (from any means)

Client [up to] broadcasts 3 of the duplicate IP detection ARPs

If the IP is already assigned the owner sends an ARP reply to notify the requestor

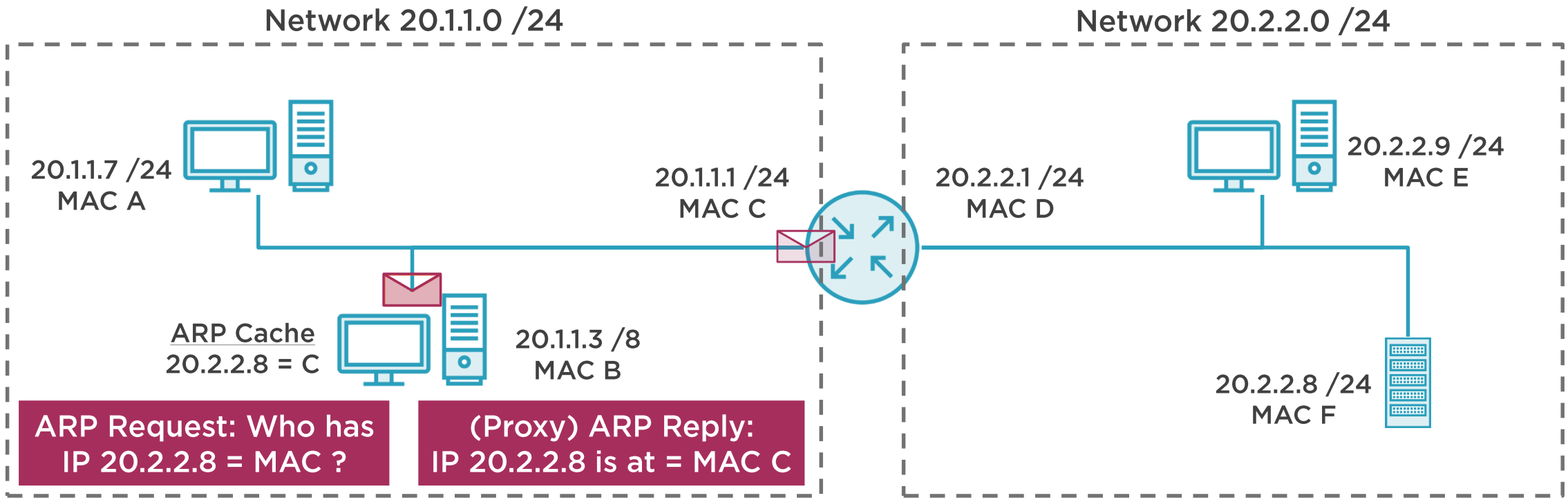
Requestor must use other IP assignment (APIPA)

Demo

Wireshark captures of ARP duplicate IP address detection

- No IP conflict on the LAN
- IP conflict

Proxy ARP – Gateway Bridging



Message	Source 20.1.1.3	Destination 20.2.2.8	Source MAC D	Destination MAC F

Proxy ARP

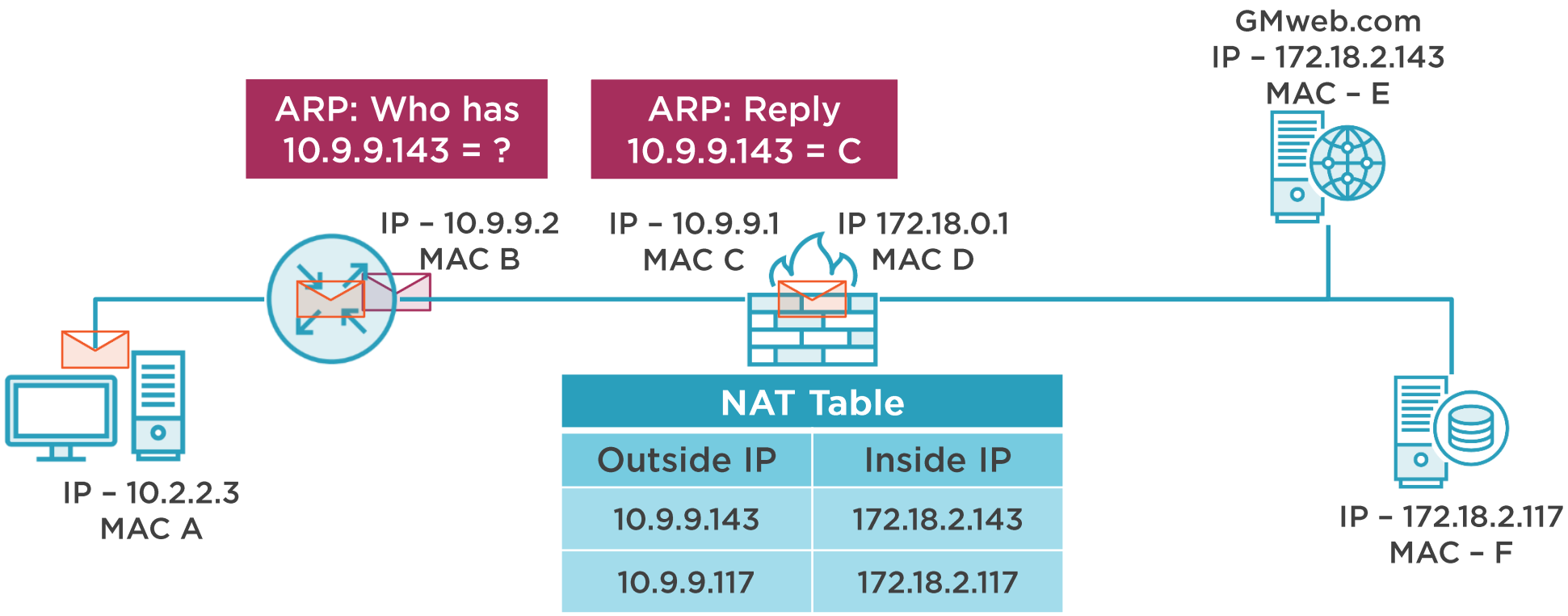
Proxy ARP is a method which permits a machine to answer ARP requests for other hosts not on the same broadcast network.

Proxy ARP increases traffic on your local networks, and clients must maintain larger ARP tables than they would if properly subnetted

A data blackhole can be created if proxy ARP server answers ARP requests but does not know how to forward data

Security risks include using router proxy to access systems inappropriately, and proxy spoofing intercept data

Proxy ARP – NAT



NAT Table	
Outside IP	Inside IP
10.9.9.143	172.18.2.143
10.9.9.117	172.18.2.117

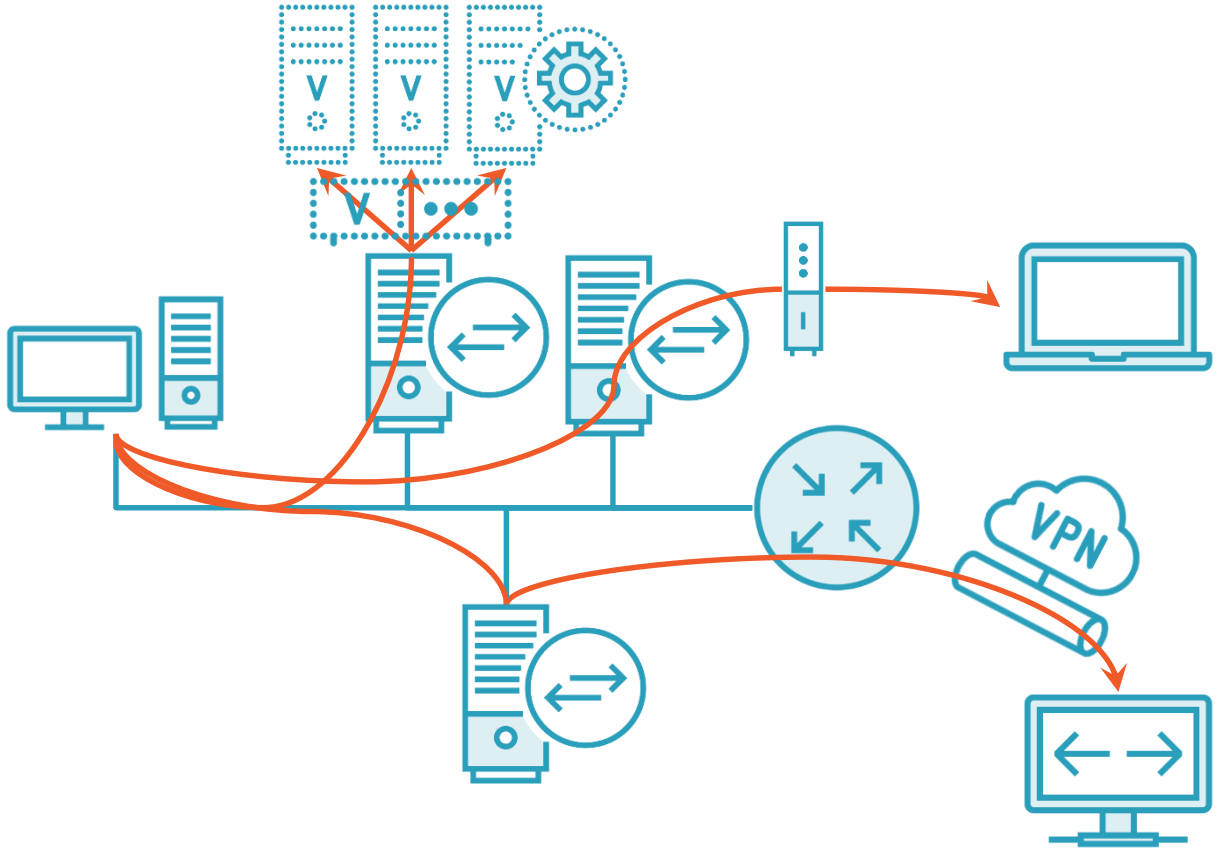
GMweb.com	Source 10.2.2.3	Destinatio 10.9.9.143	GMweb.com	Source 10.2.2.3	Destination 172.18.2.143	Source MAC D	Destination MAC E

Server ARP Proxy Applications

Applications or VMs with different IPs running on server

Bridge LAN to serial or dial-up hosts

Connect LAN nodes to VPN hosts



Proxy ARP Overview

A network node answers ARP queries with its own address as a proxy for one or more IP addresses not on the same network

Commonly found on routers, firewalls NAT, and server systems

Uncommonly used to bridge subnetwork mask differences. May be on by default creating unexpected issues and security concerns

Adds complexity in design and troubleshooting and may create a blackhole if proxy does not know how to deliver to destination

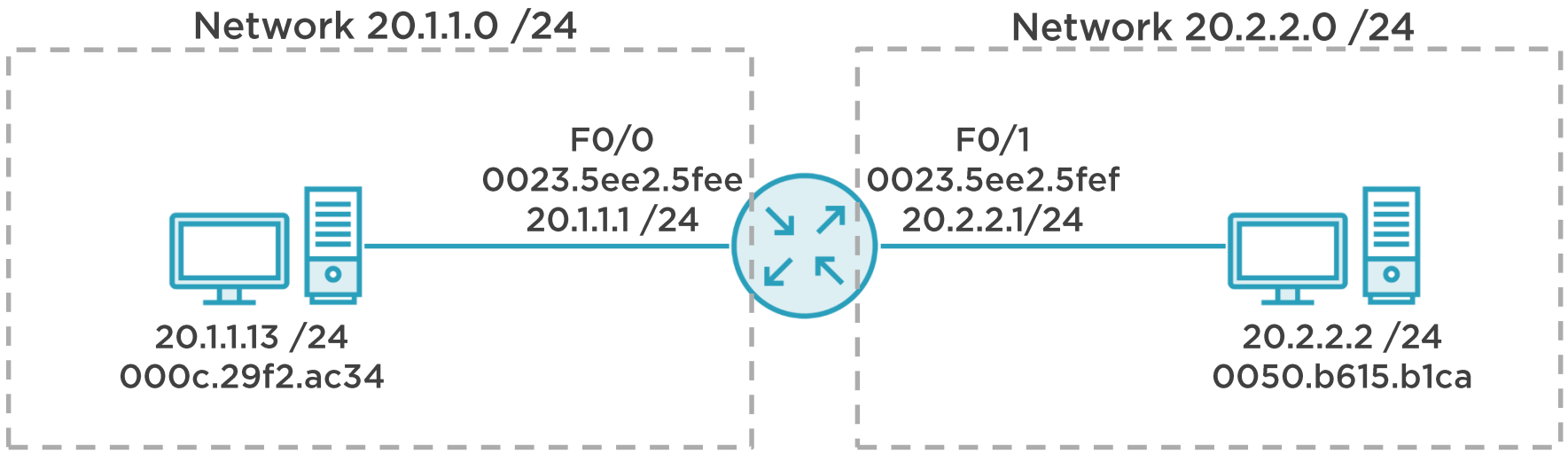
Demo

Normal LAN Functions

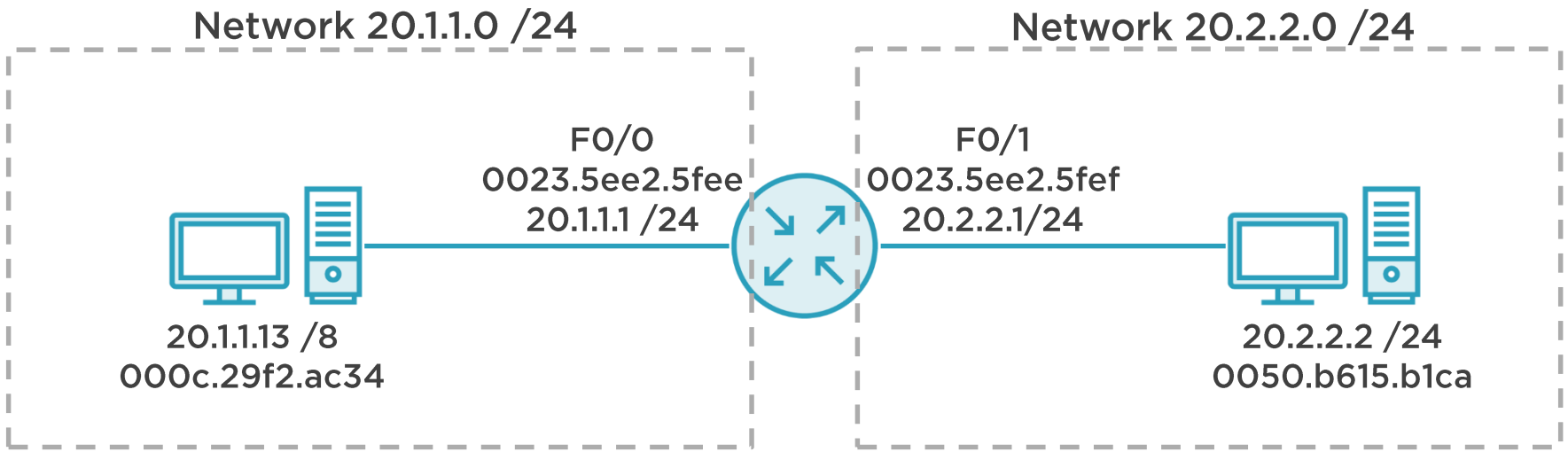
Proxy ARP Function

Disable proxy ARP on Cisco devices

Proxy ARP – Demo 1



Proxy ARP – Demo 1



Summary

- Inverse ARP
- Reverse ARP
- Gratuitous ARP
- IP Conflict (DHCP) ARP
- Proxy ARP