IT 609
Network and System Administration

Address Resolution Protocol (ARP)

Tuesday October 19, 2021

Address Resolution Protocol

Why do we need Internet Protocol?

IP - Why its needed?

Level 2 (Data Link)

- Computers to talk to computers
- Limited to a local network segment

IP and other Level 3 protocols allow networks to talk to networks

More effective to address communications to groups (networks) than individual devices

IP to Level 2

Level 2 (Ethernet) must communicate using MAC addresses

Can only talk to **local devices** !!!!

IP is used to connect networks to networks, but ultimately, we still need to get the message to a specific host.

Each IP host has a unique IP address on its network, but that address is useless to Ethernet.

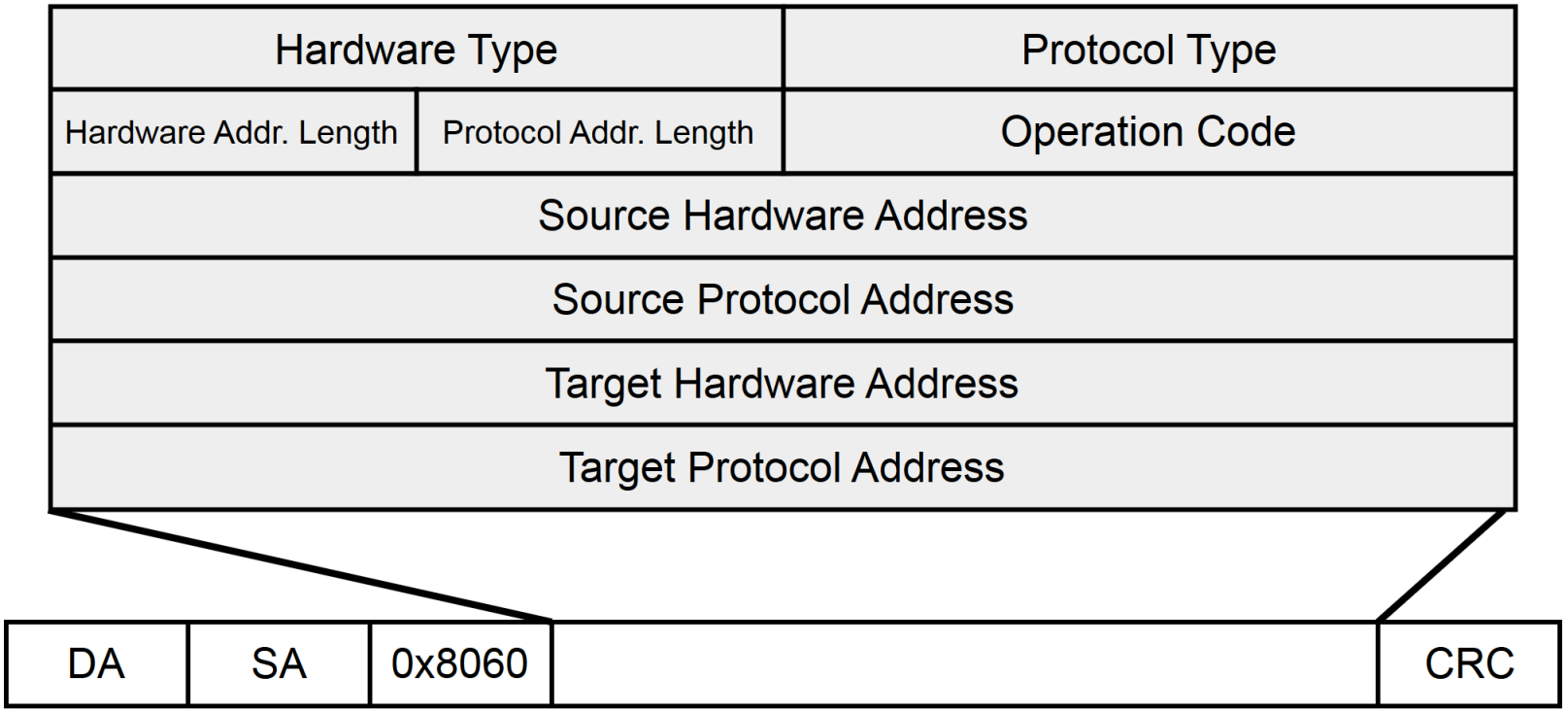
“Layer 2.5”

Address Resolution Protocol (ARP)

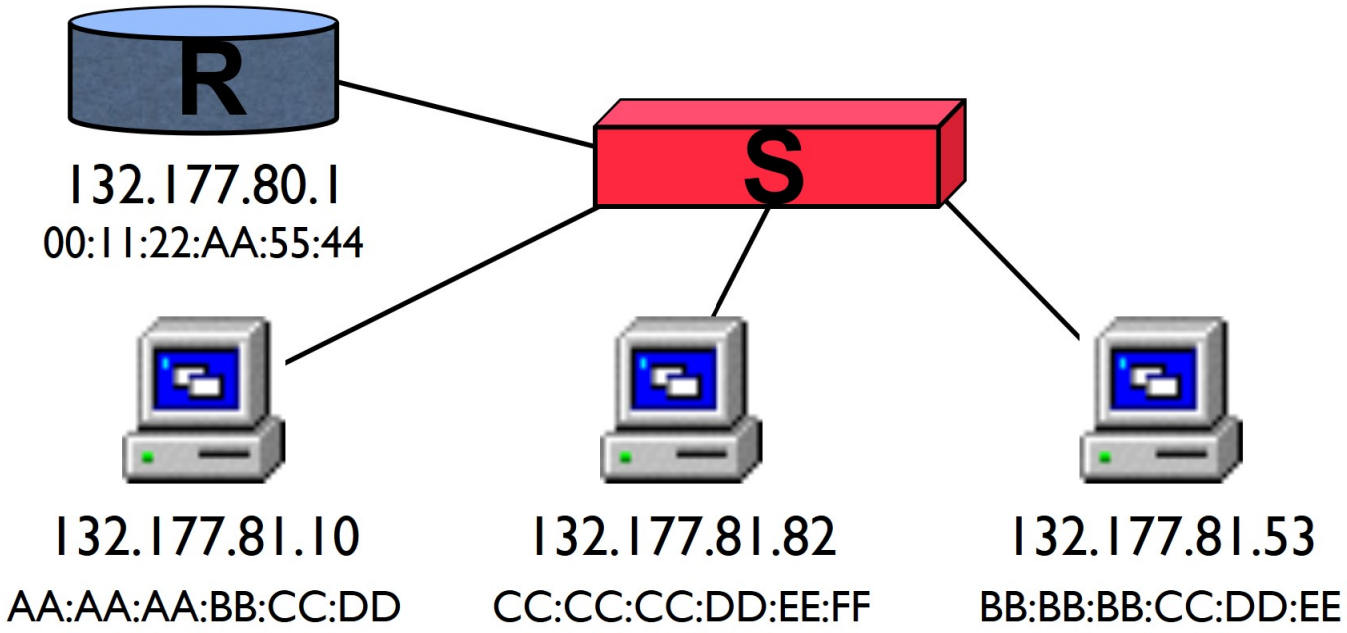
- Initiate a Level 2 broadcast - Who is X.X.X.X?
- Only the matching host replies
- The reply includes that machine’s MAC

Can be used with Data Link layers and Network layers other than Ethernet and IP

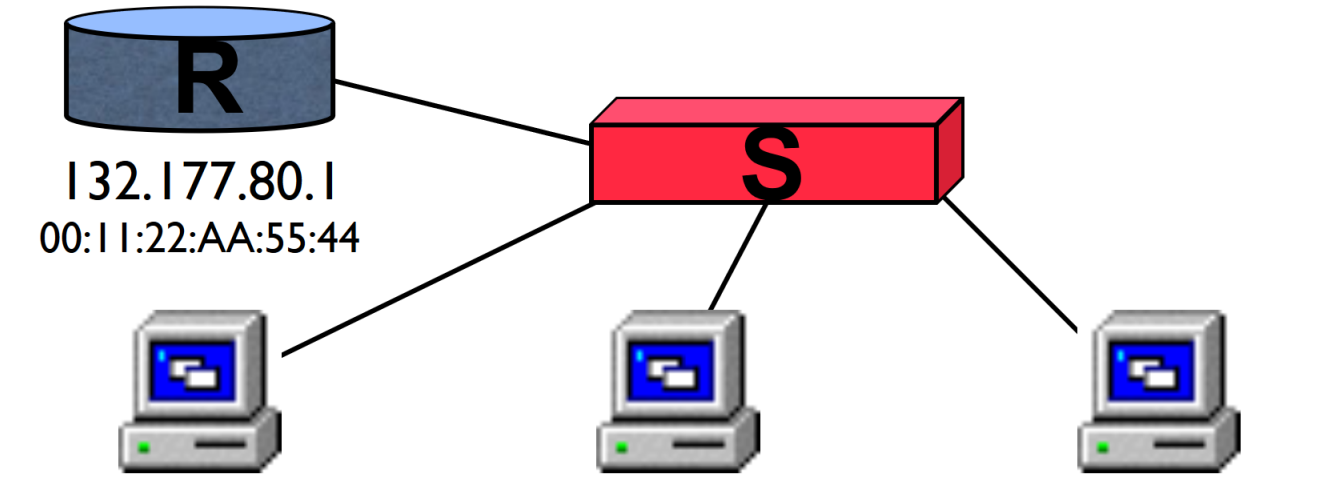
ARP Packet


Hardware Type
Protocol Type
Hardware Addr. Length
Protocol Addr. Length
Operation Code
Source Hardware Address
Source Protocol Address
Target Hardware Address
Target Protocol Address
DA
SA
0x8060
CRC

ARP Example


R
S
132.177.80.1
00:11:22:AA:55:44
132.177.81.10
AA:AA:AA:BB:CC:DD
132.177.81.82
CC:CC:CC:DD:EE:FF
132.177.81.53
BB:BB:BB:CC:DD:EE

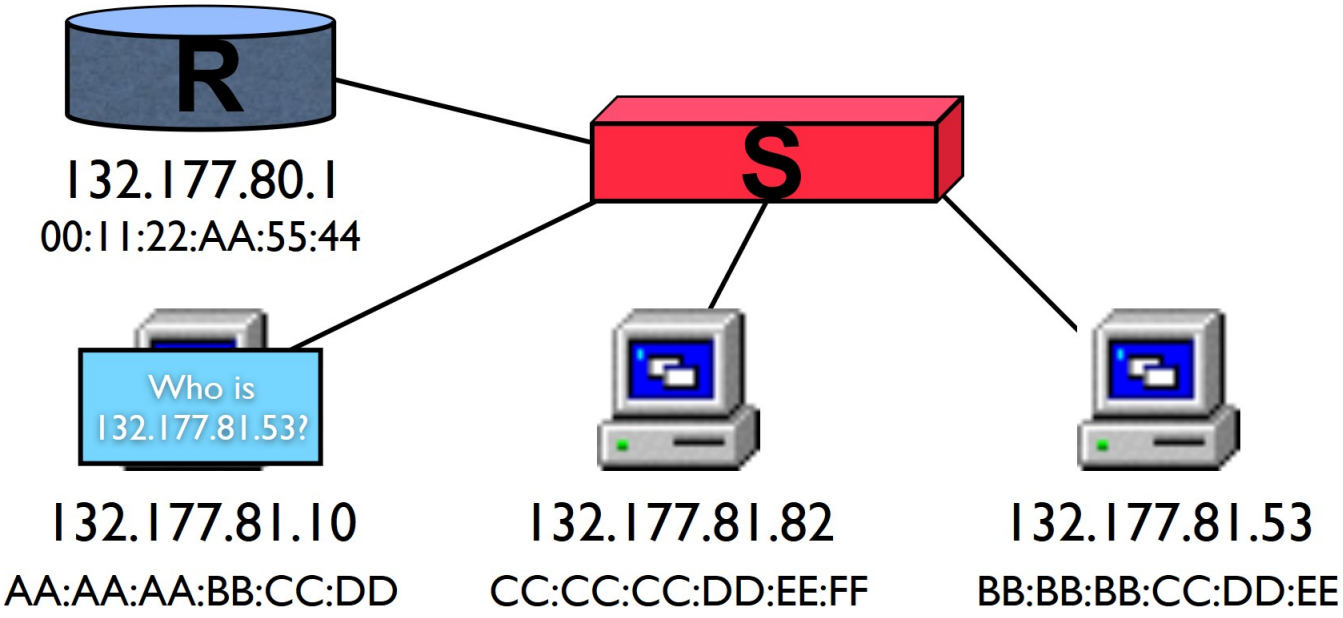
ARP Example



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

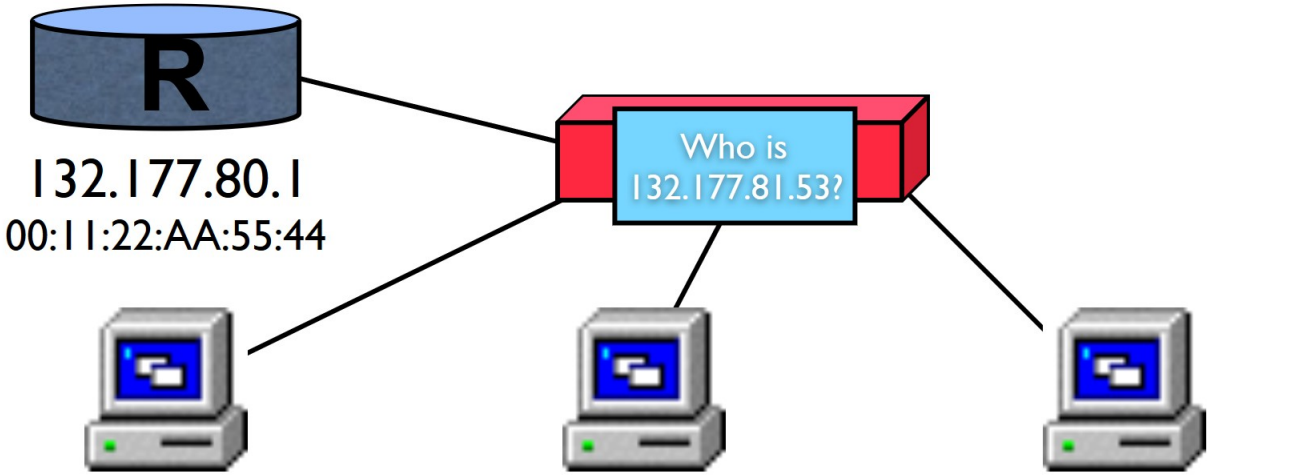
ARP Example



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

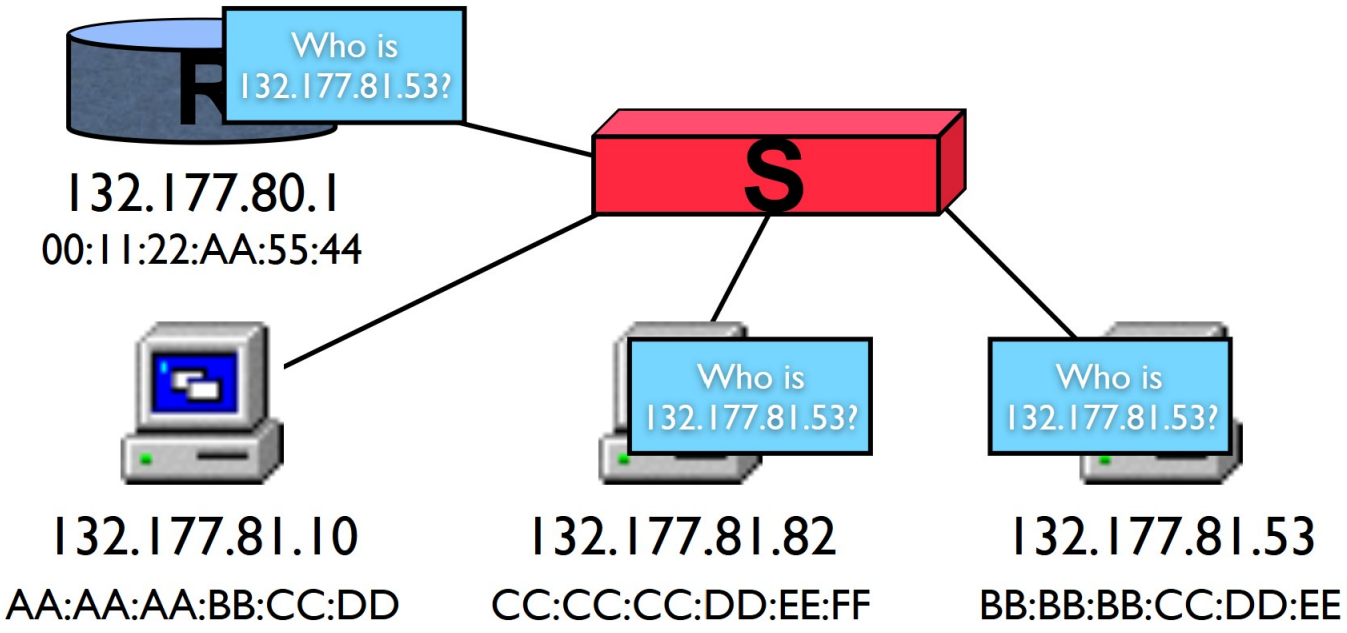
ARP Example



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

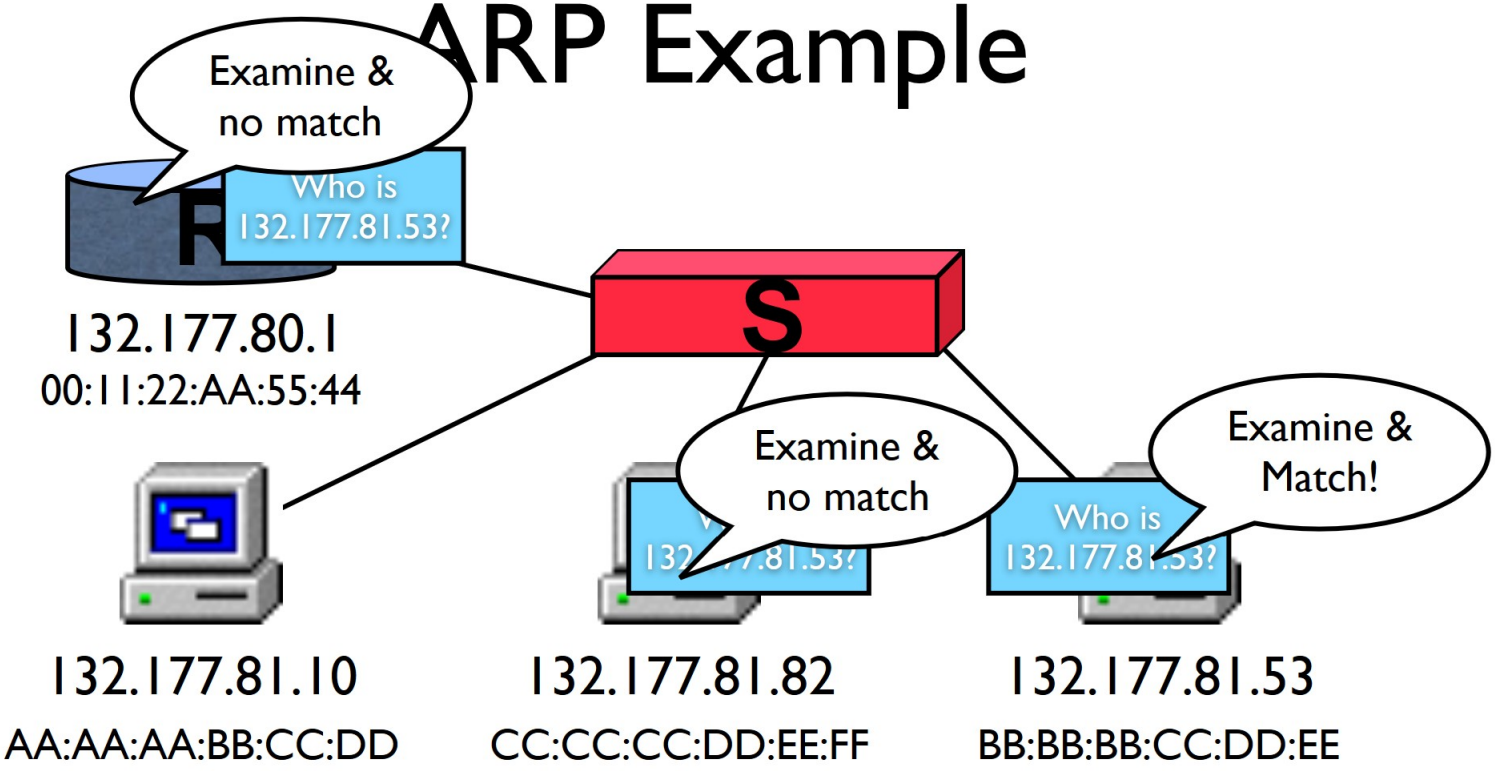
ARP Example



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

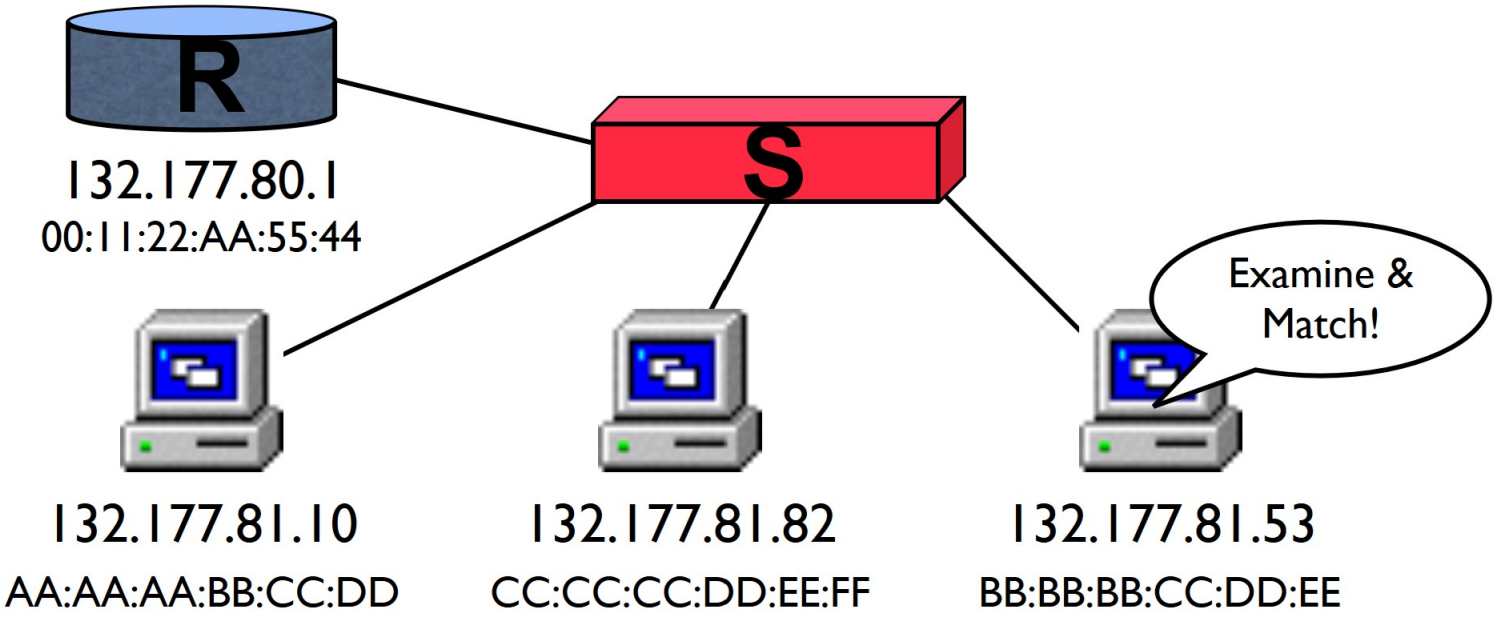
ARP Example



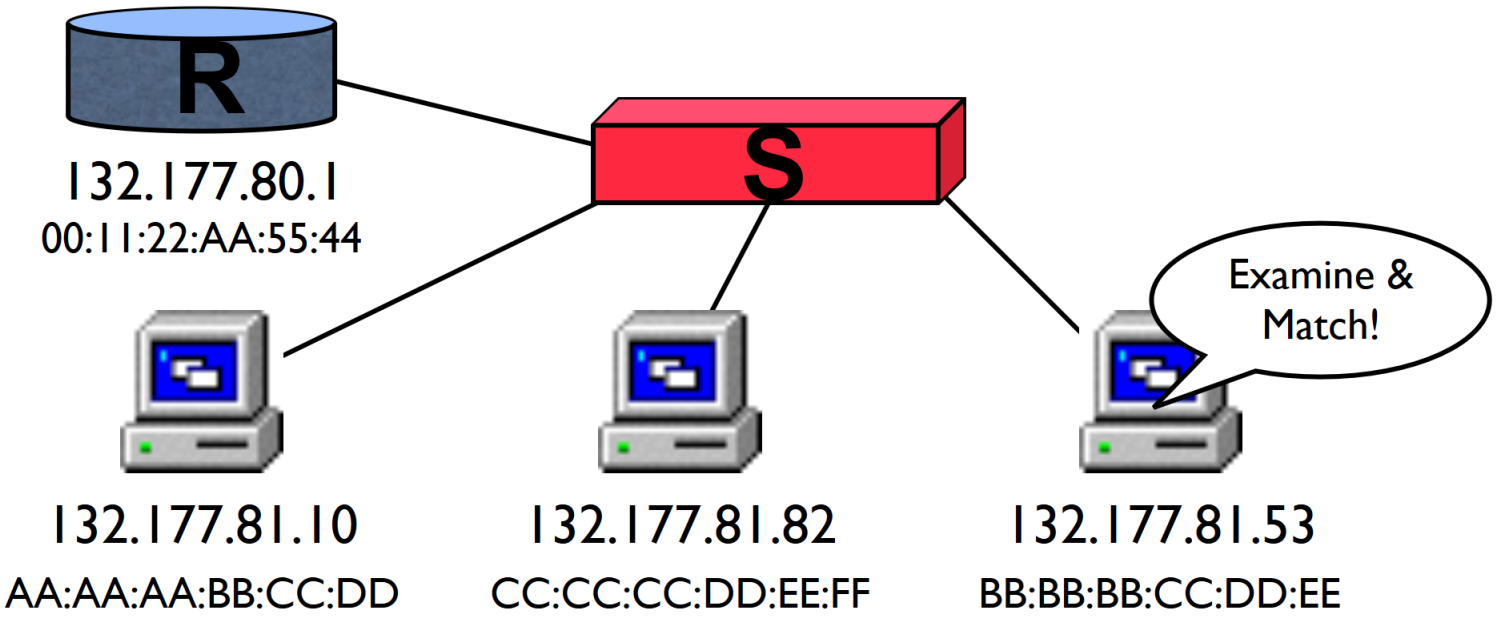
Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

ARP Example


R
132.177.80.1
00:11:22:AA:55:44
S
Examine &
Match!
132.177.81.10
AA:AA:AA:BB:CC:DD
132.177.81.82
CC:CC:CC:DD:EE:FF
132.177.81.53
BB:BB:BB:CC:DD:EE

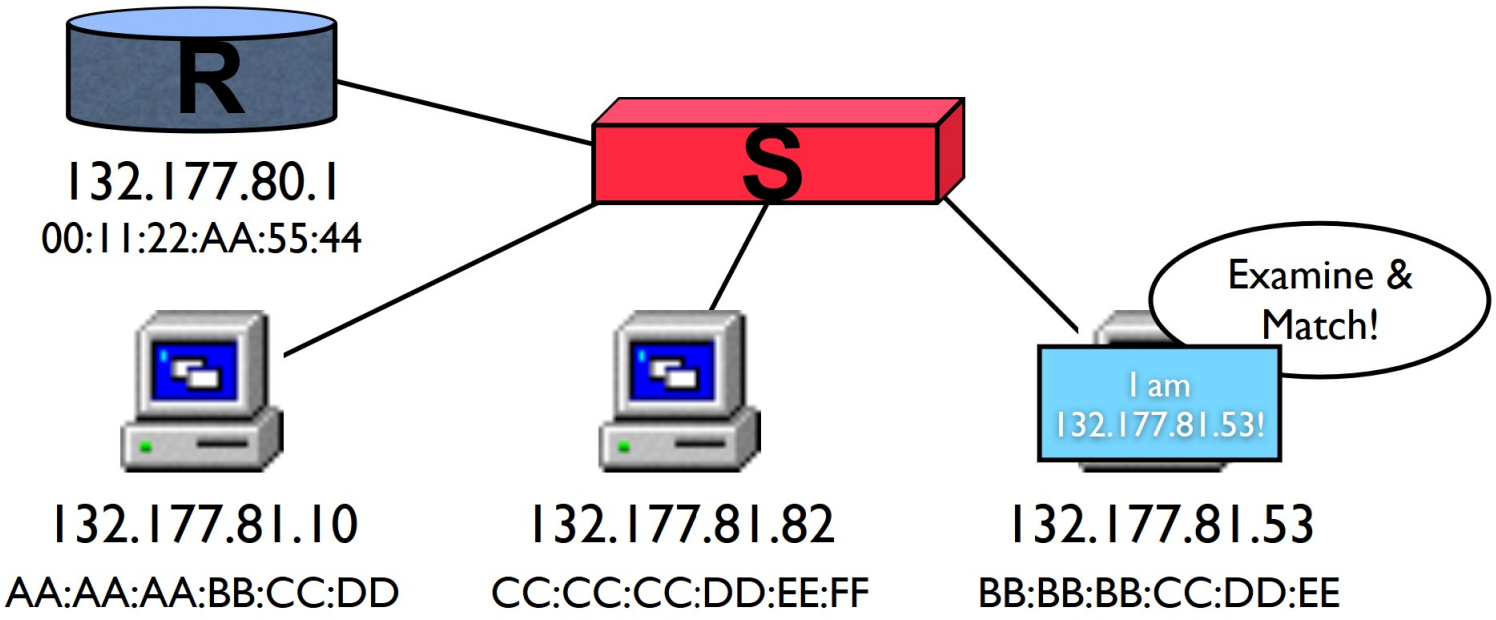
ARP Example



Station "BB" responds to "AA"

AA:AA:AA:BB:CC:DD	BB:BB:BB:CC:DD:EE	0x8060	1	0x0800	6	4	2 = ARP Reply
BB:BB:BB:CC:DD:EE	132.177.81.53	AA:AA:AA:BB:CC:DD	132.177.81.10				

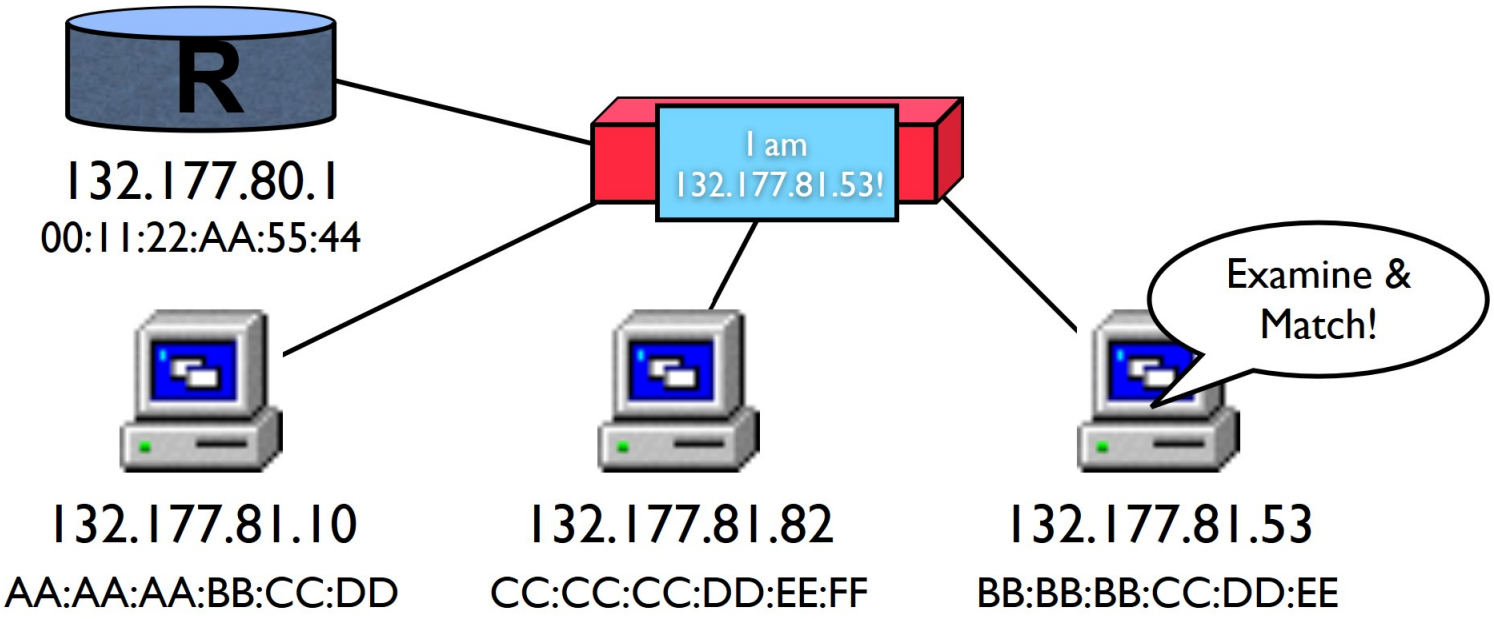
ARP Example



Station "BB" responds to "AA"

AA:AA:AA:BB:CC:DD	BB:BB:BB:CC:DD:EE	0x8060	1	0x0800	6	4	2 = ARP Reply
BB:BB:BB:CC:DD:EE	132.177.81.53	AA:AA:AA:BB:CC:DD	132.177.81.10				

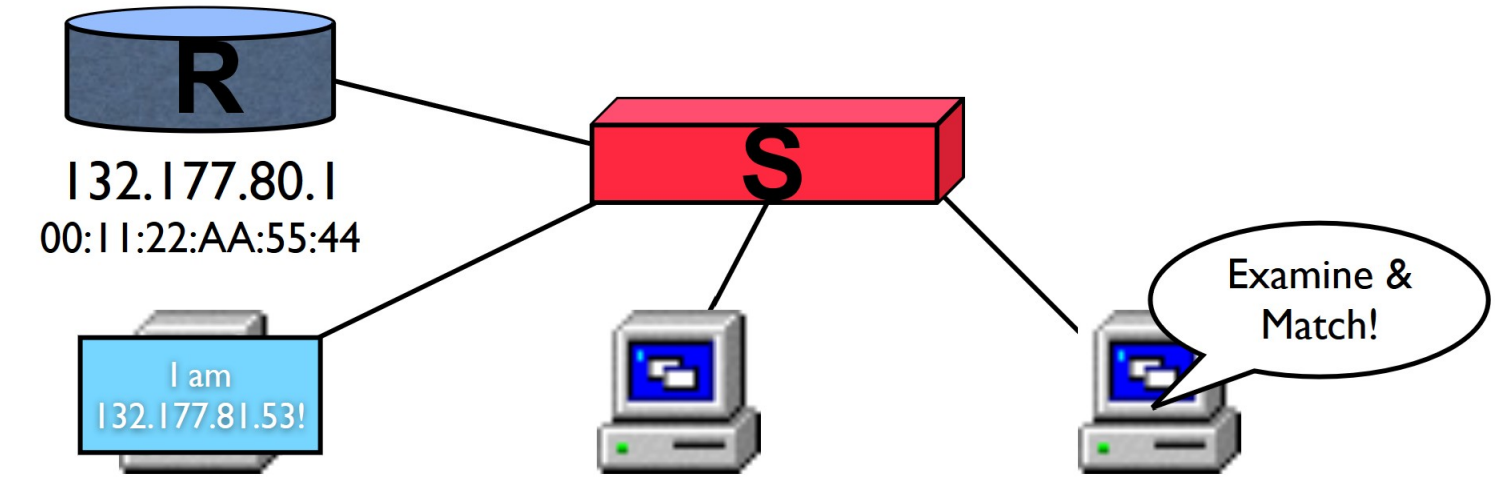
ARP Example



Station "BB" responds to "AA"

AA:AA:AA:BB:CC:DD	BB:BB:BB:CC:DD:EE	0x8060	1	0x0800	6	4	2 = ARP Reply
BB:BB:BB:CC:DD:EE	132.177.81.53	AA:AA:AA:BB:CC:DD	132.177.81.10				

ARP Example



Station "BB" responds to "AA"

AA:AA:AA:BB:CC:DD	BB:BB:BB:CC:DD:EE	0x8060	1	0x0800	6	4	2 = ARP Reply
BB:BB:BB:CC:DD:EE	132.177.81.53	AA:AA:AA:BB:CC:DD	132.177.81.10				

ARP Caching

ARP is simple, and fast, but doing ARP before each packet is wasteful

IP addresses generally don't change

ARP caches responses on each computer for a short period

If an IP is in the cache, then the cached value is used

Caching happens both on the "source" and the "target" side

Check ARP cache with the "`arp`" command

ARP & Routers

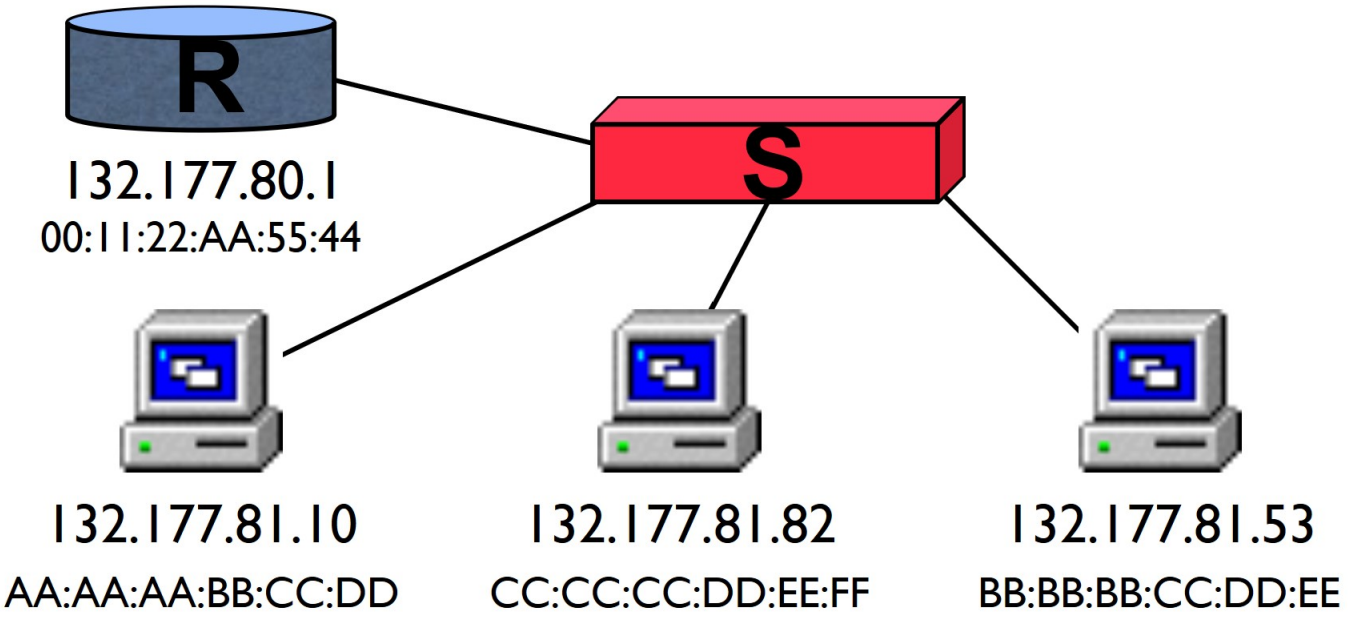
If you need to leave the network:

- ARP request for the gateway IP address
- Router responds with the MAC of the interface
- Remember - all IP hosts must be configured with a gateway address to talk to non-local devices

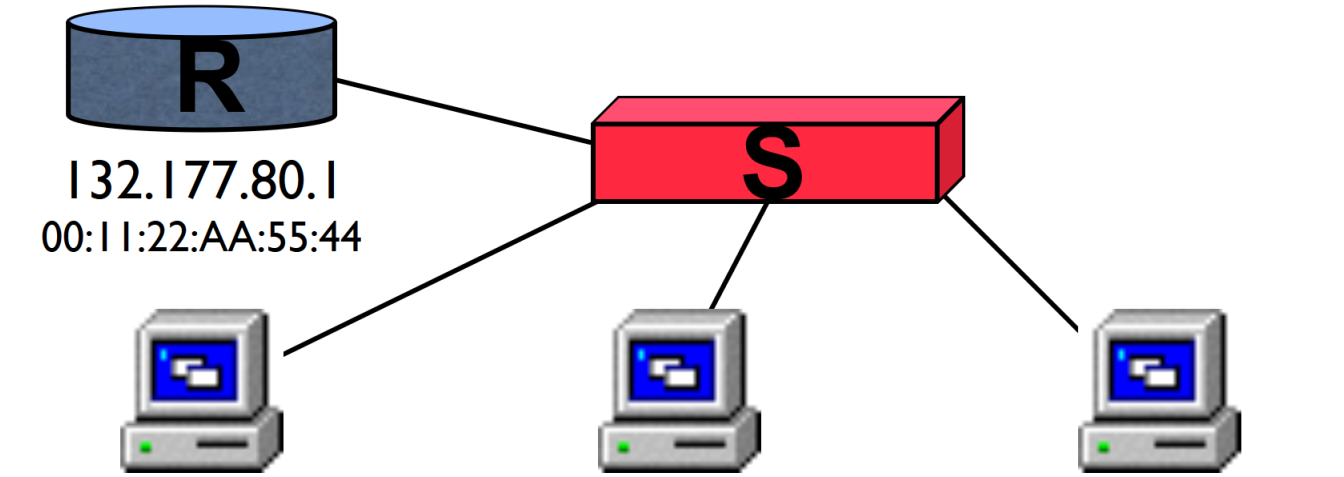
Coming to the network:

- A router has an IP packet for a device
- The router sends an ARP request for the destination IP
- Destination computer responds with its MAC

ARP Example


R
S
132.177.80.1
00:11:22:AA:55:44
132.177.81.10
AA:AA:AA:BB:CC:DD
132.177.81.82
CC:CC:CC:DD:EE:FF
132.177.81.53
BB:BB:BB:CC:DD:EE

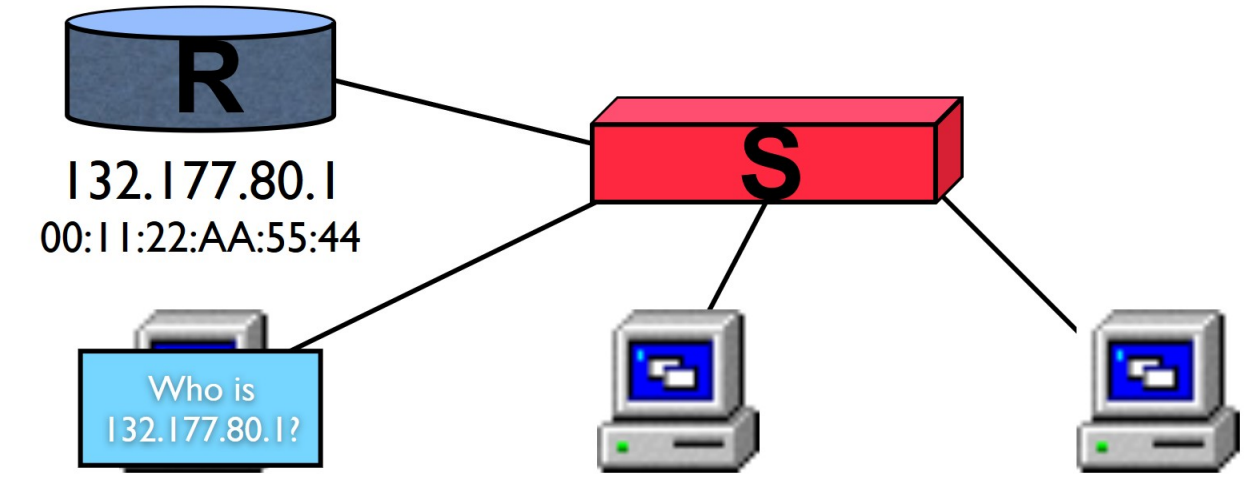
ARP Example



Station "AA" wants to talk to something off the network

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.80.1			

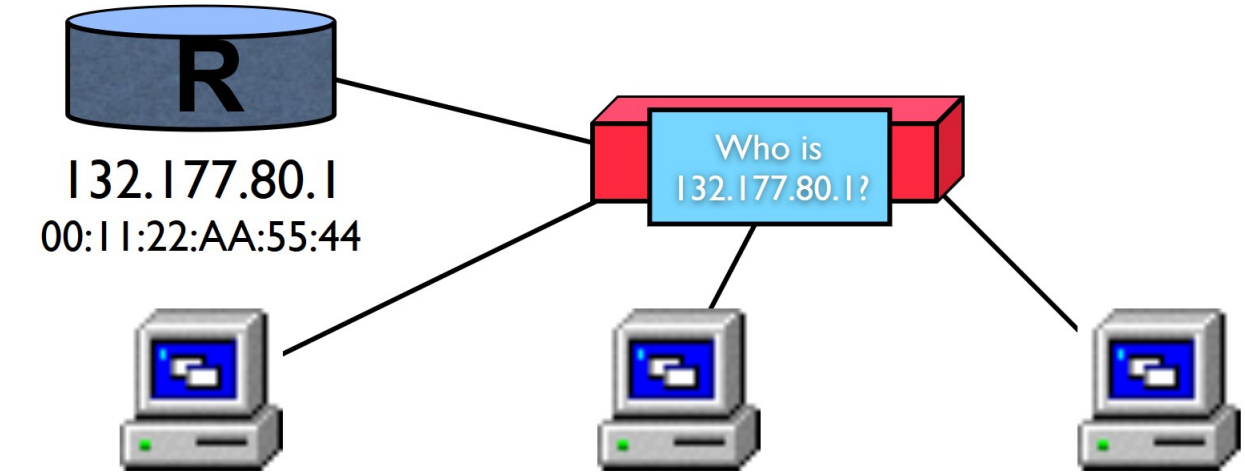
ARP Example



Station "AA" wants to talk to something off the network

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.80.1			

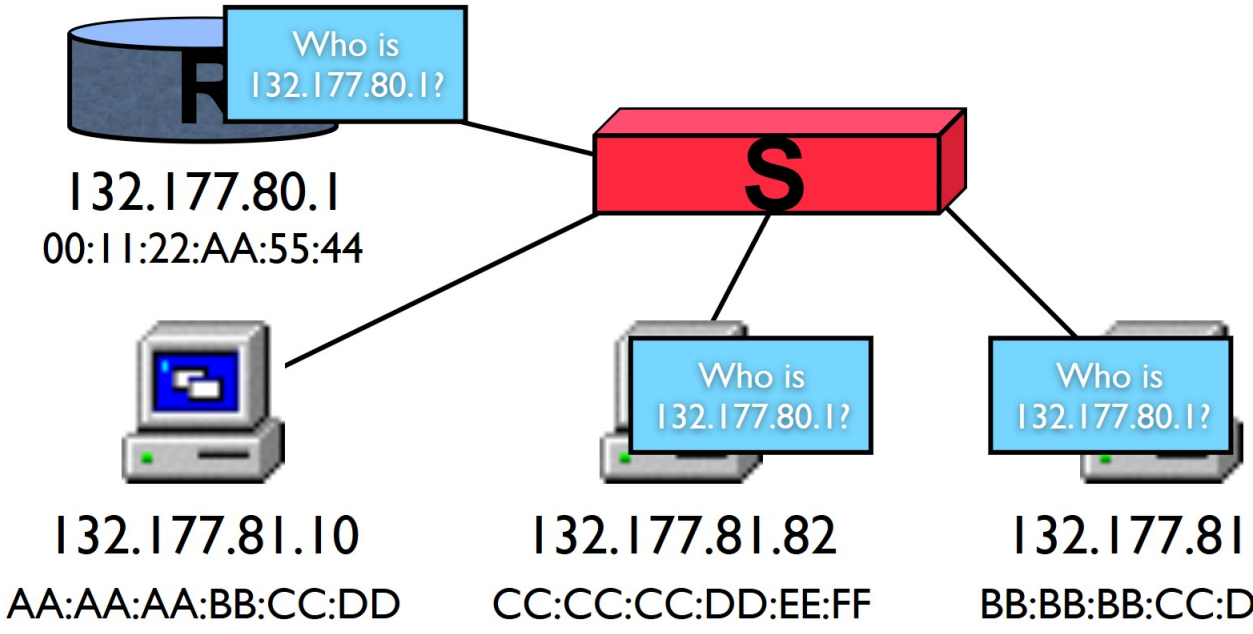
ARP Example



Station "AA" wants to talk to something off the network

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.80.1			

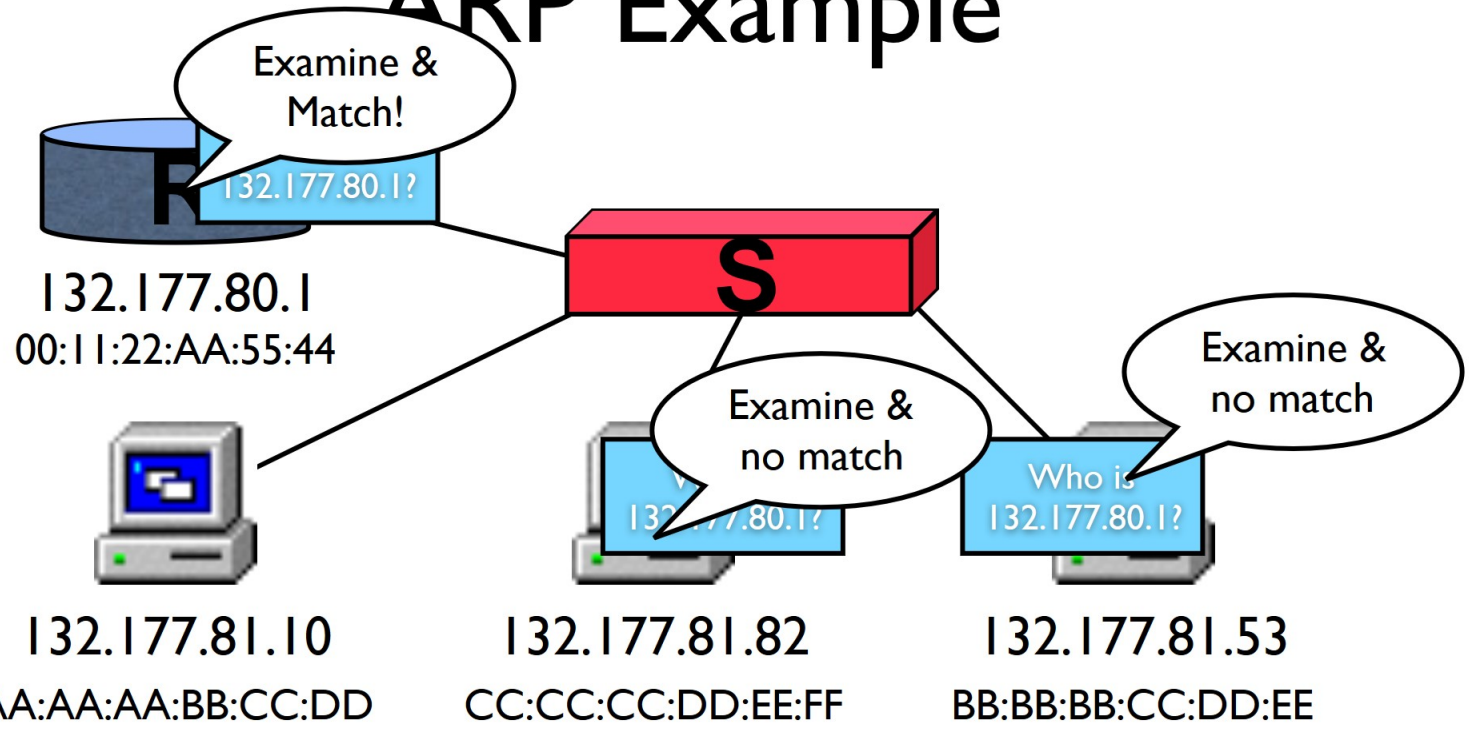
ARP Example



Station "AA" wants to talk to something off the network

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.80.1			

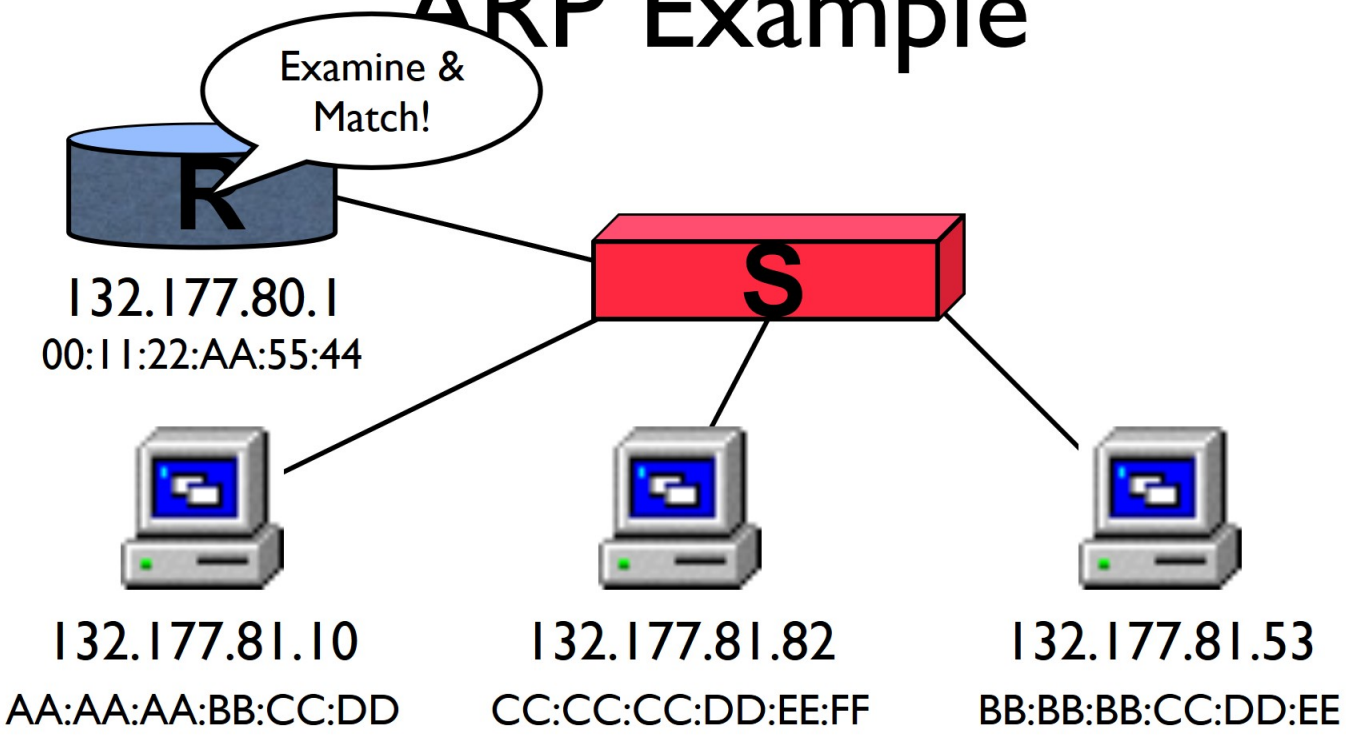
ARP Example



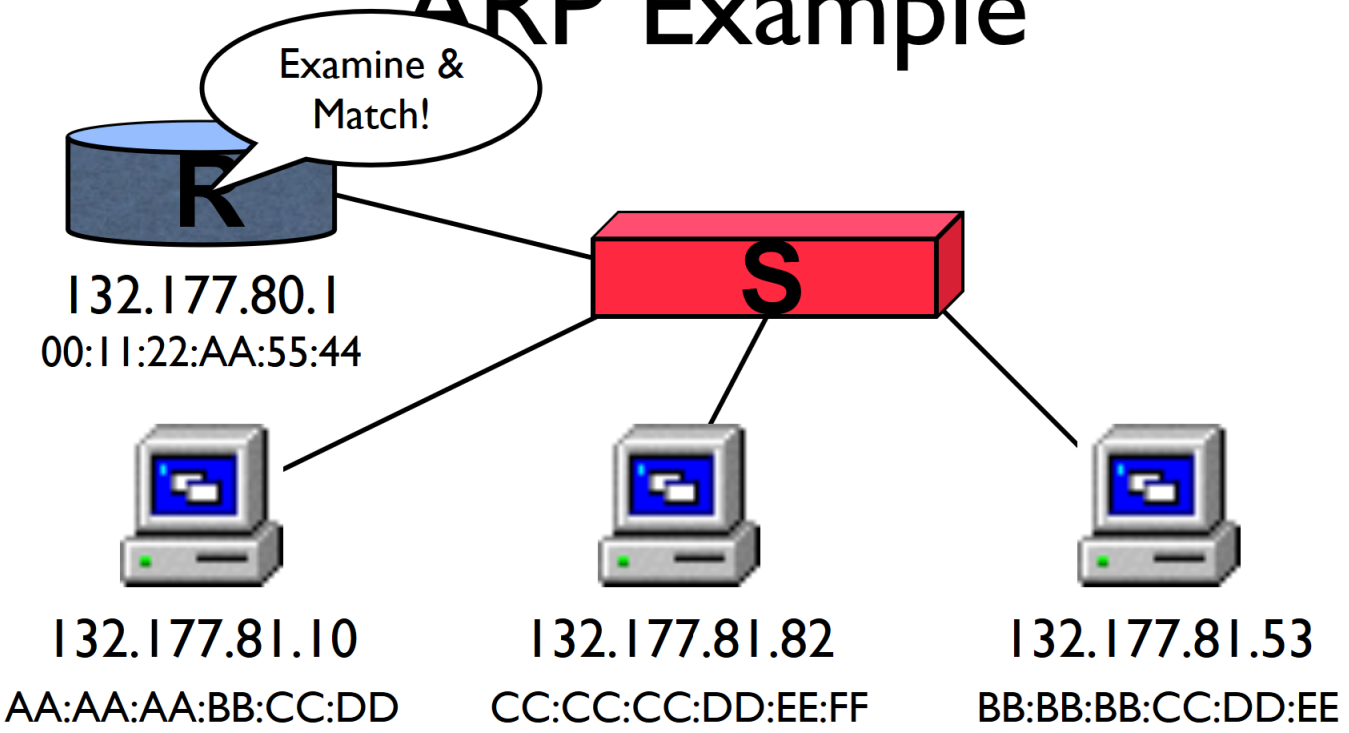
Station "AA" wants to talk to something off the network

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.80.1			

ARP Example


Examine &
Match!
R
S
132.177.80.1
00:11:22:AA:55:44
132.177.81.10
AA:AA:AA:BB:CC:DD
132.177.81.82
CC:CC:CC:DD:EE:FF
132.177.81.53
BB:BB:BB:CC:DD:EE

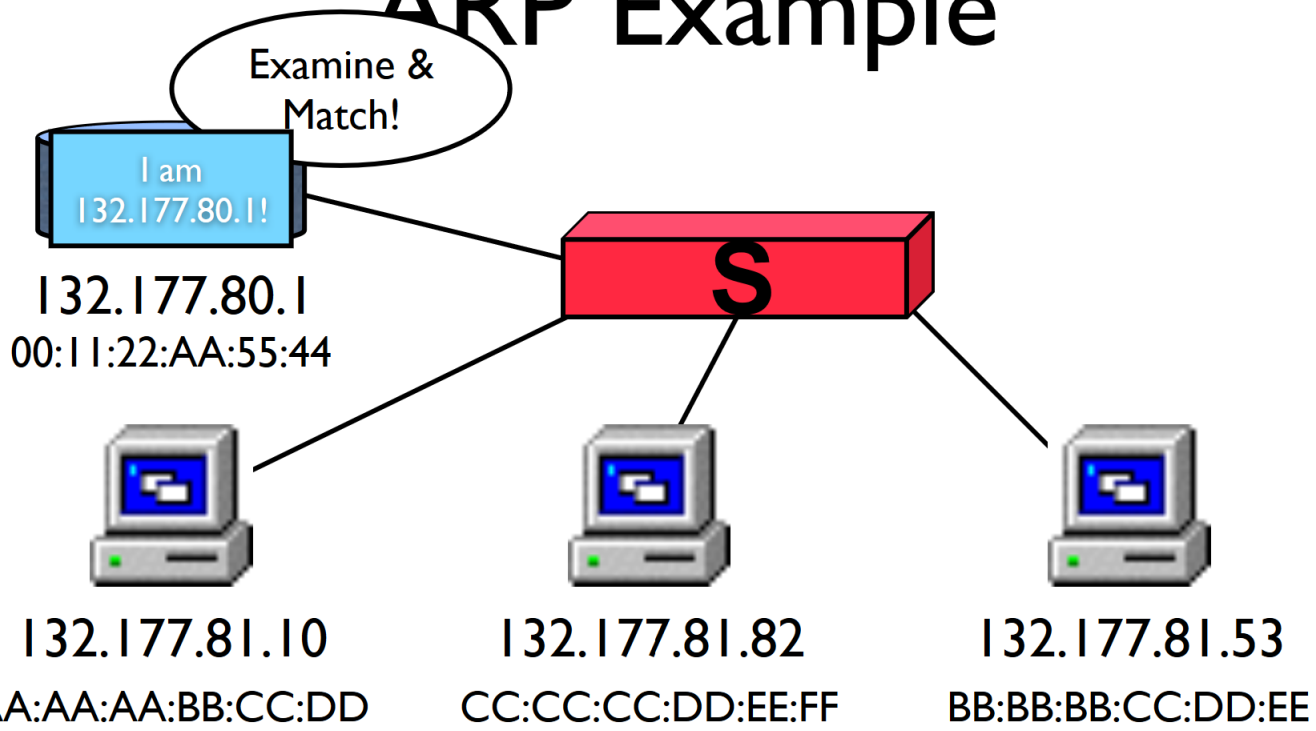
ARP Example



Router responds to "AA"

AA:AA:AA:BB:CC:DD	00:11:22:AA:55:44	0x8060	1	0x0800	6	4	2 = ARP Reply
00:11:22:AA:55:44	132.177.80.1	AA:AA:AA:BB:CC:DD	132.177.81.10				

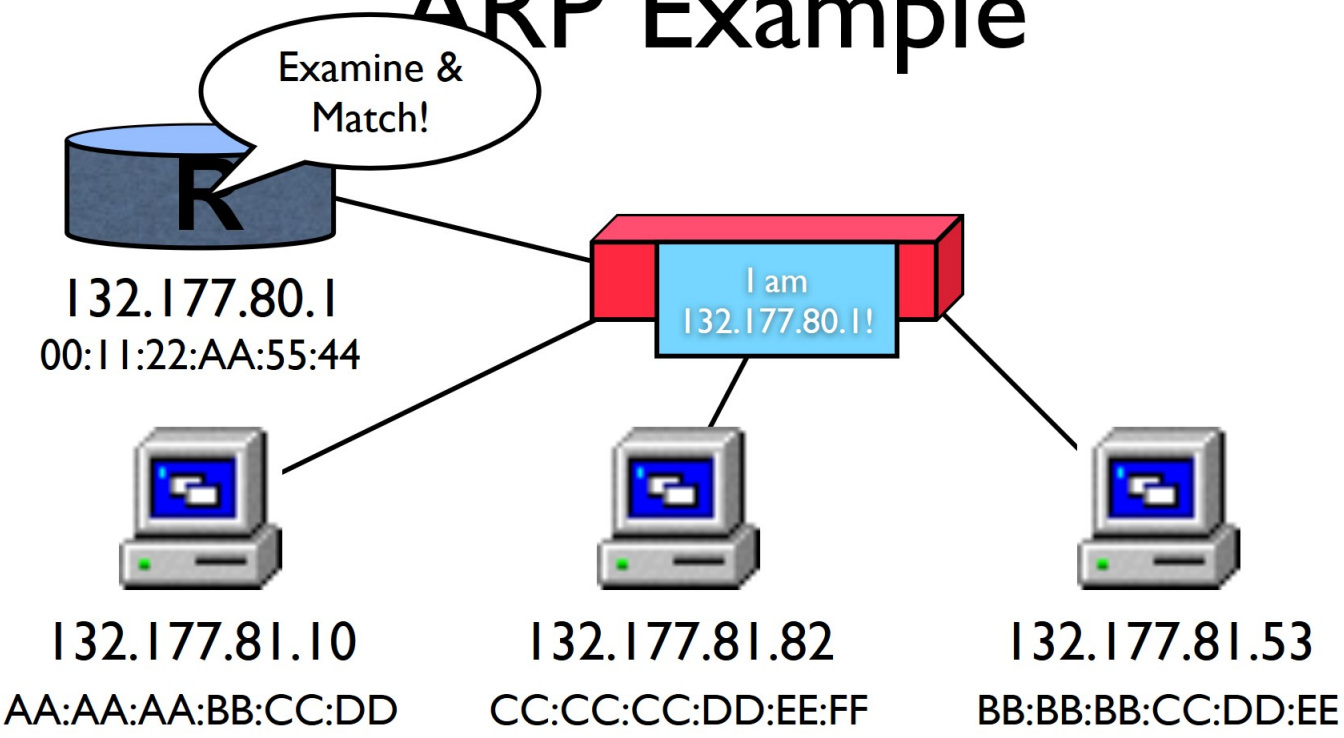
ARP Example



Router responds to "AA"

AA:AA:AA:BB:CC:DD	00:11:22:AA:55:44	0x8060	1	0x0800	6	4	2 = ARP Reply
00:11:22:AA:55:44	132.177.80.1	AA:AA:AA:BB:CC:DD	132.177.81.10				

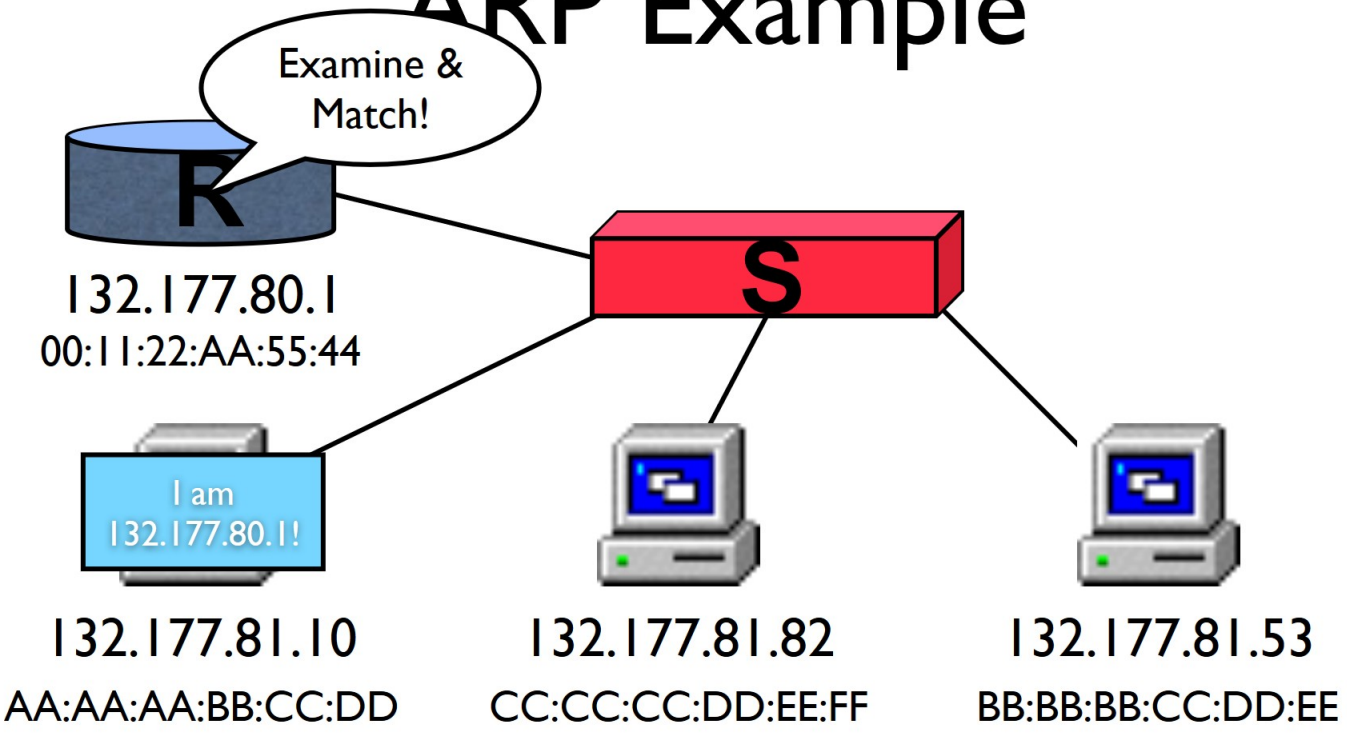
ARP Example



Router responds to "AA"

AA:AA:AA:BB:CC:DD	00:11:22:AA:55:44	0x8060	1	0x0800	6	4	2 = ARP Reply
00:11:22:AA:55:44	132.177.80.1	AA:AA:AA:BB:CC:DD	132.177.81.10				

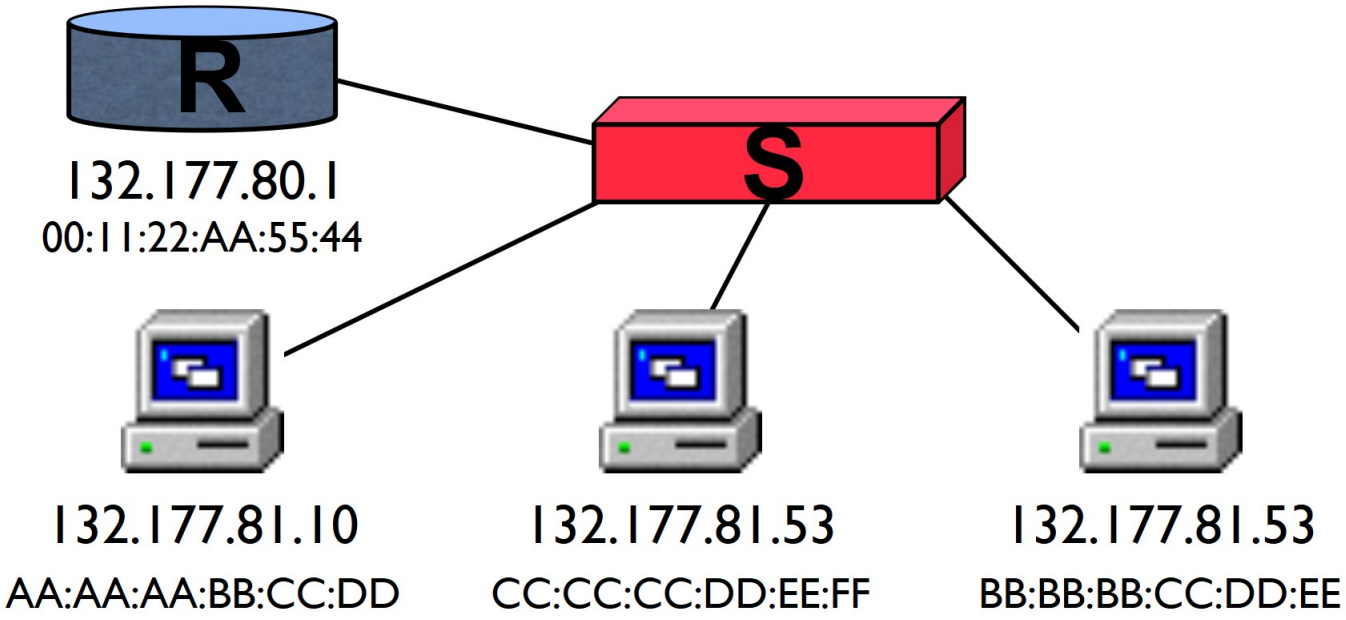
ARP Example



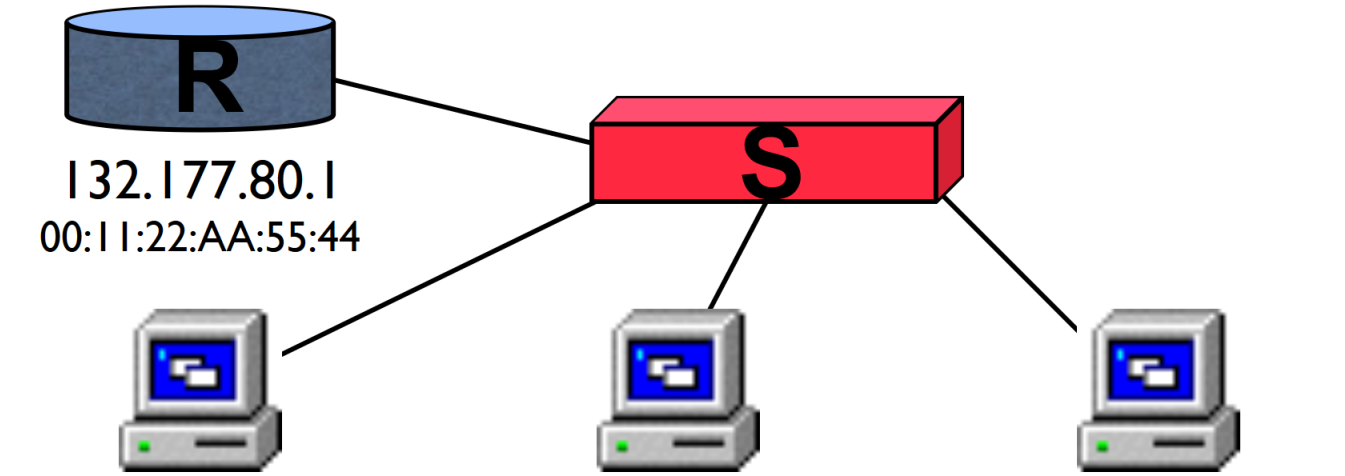
Router responds to "AA"

AA:AA:AA:BB:CC:DD	00:11:22:AA:55:44	0x8060	1	0x0800	6	4	2 = ARP Reply
00:11:22:AA:55:44	132.177.80.1	AA:AA:AA:BB:CC:DD	132.177.81.10				

When ARP Goes Bad…



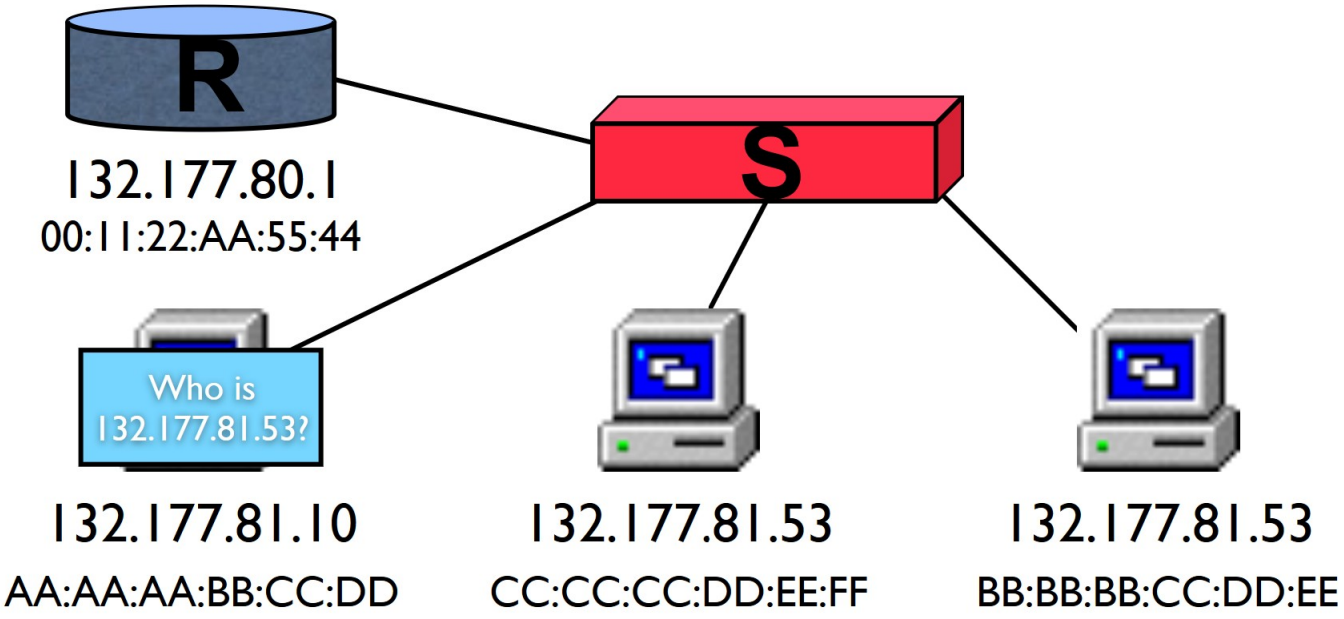
When ARP Goes Bad…



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

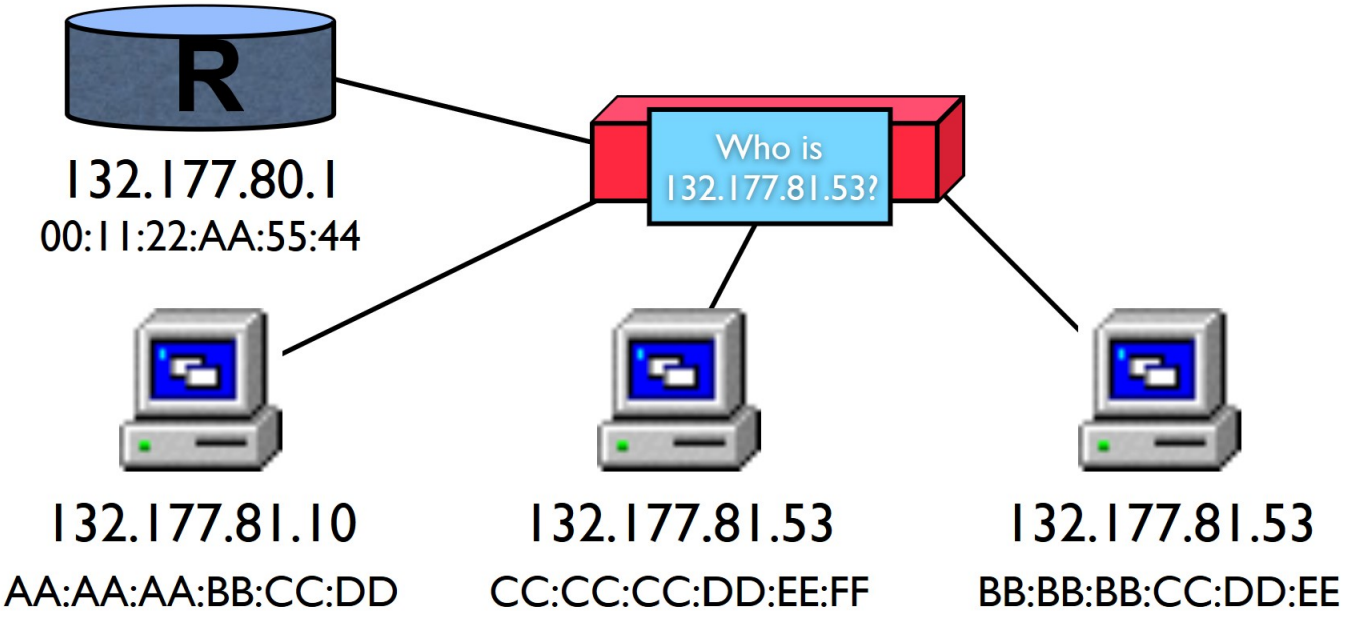
When ARP Goes Bad…



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

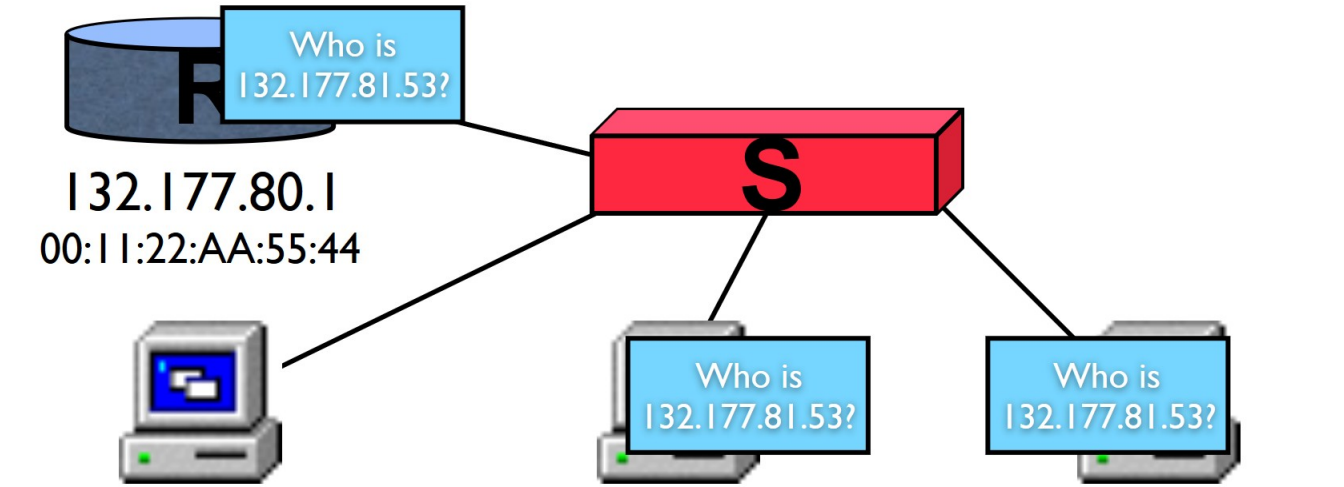
When ARP Goes Bad…



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

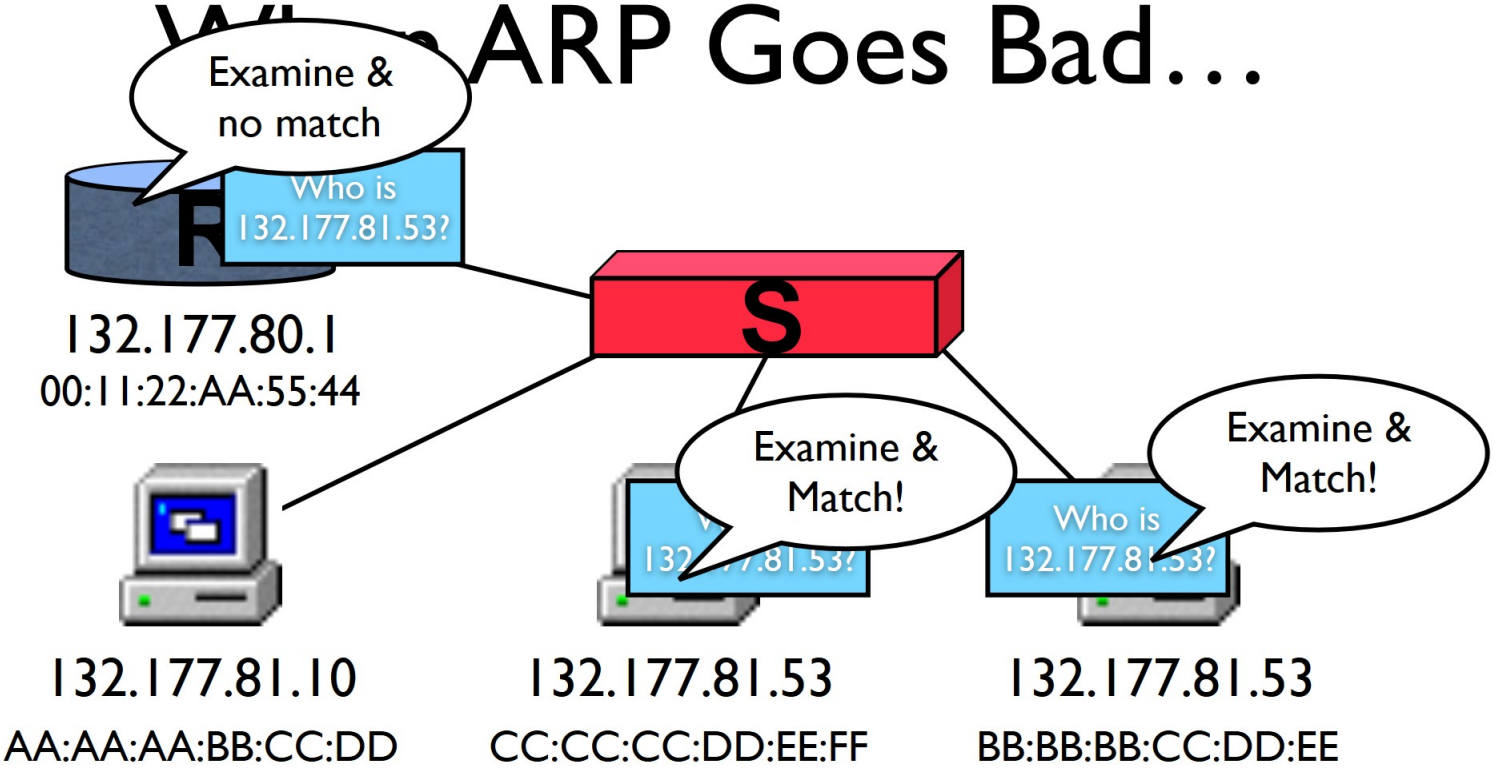
When ARP Goes Bad…



Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

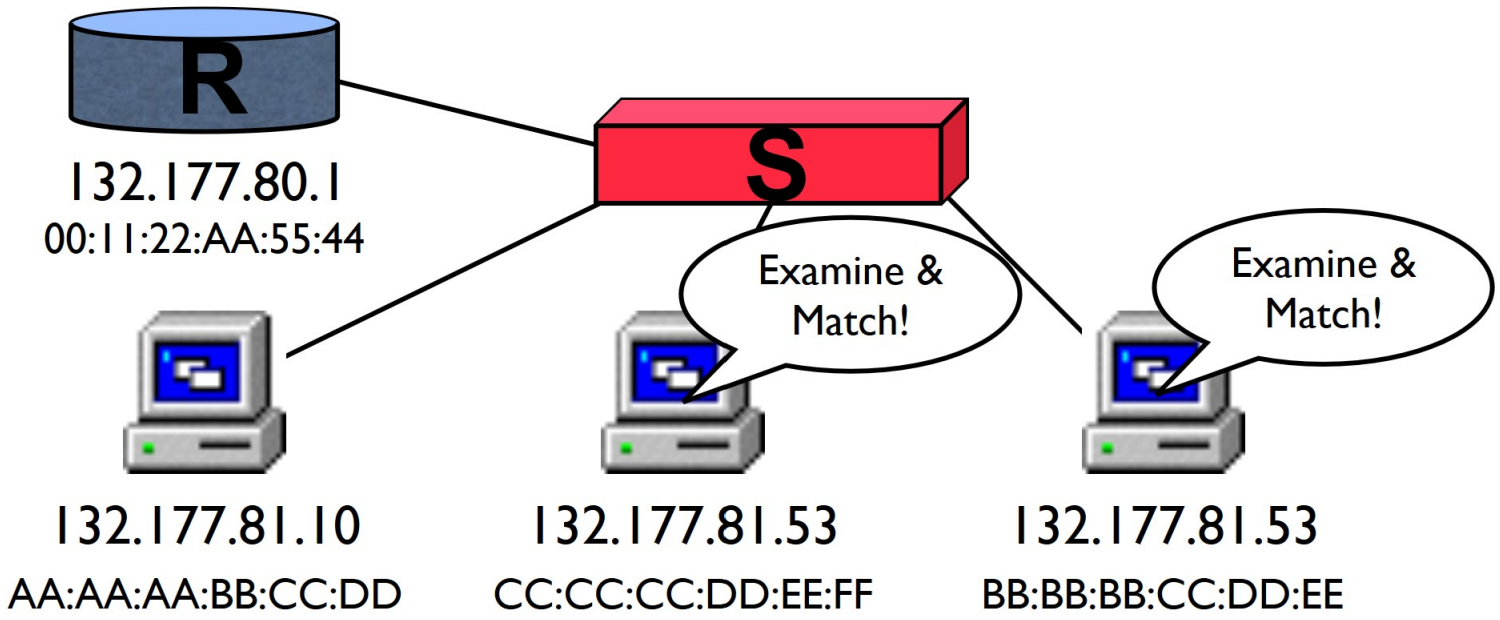
When ARP Goes Bad…



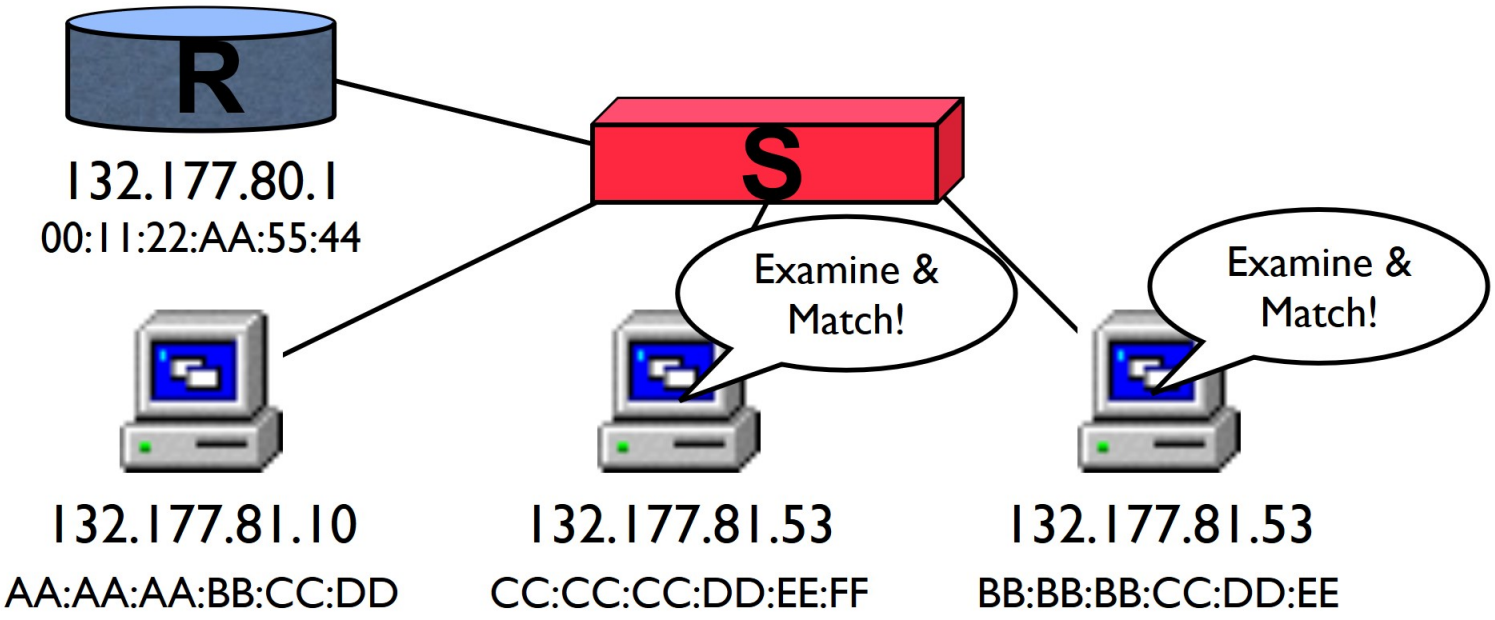
Station "AA" wants to talk to 132.177.81.53

FF:FF:FF:FF:FF:FF	AA:AA:AA:BB:CC:DD	0x8060	1	0x0800	6	4	1 = ARP Request
AA:AA:AA:BB:CC:DD	132.177.81.10			132.177.81.53			

When ARP Goes Bad…

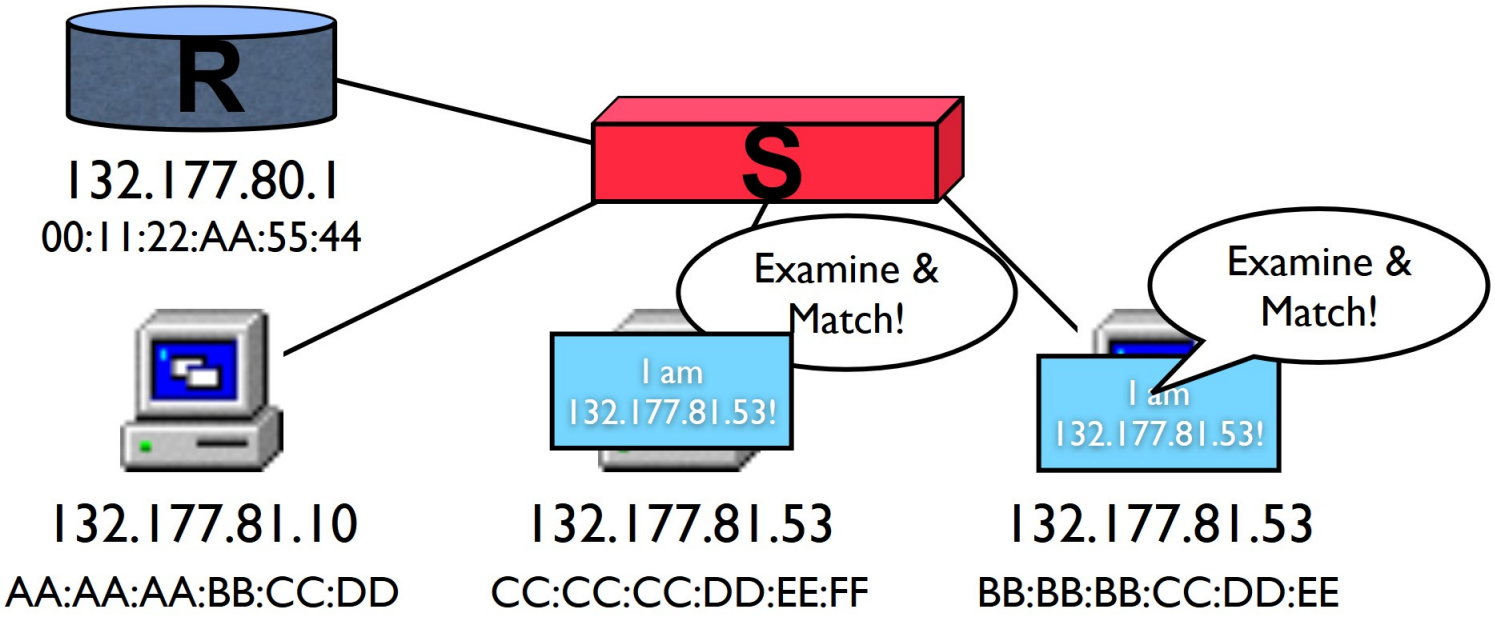


When ARP Goes Bad…



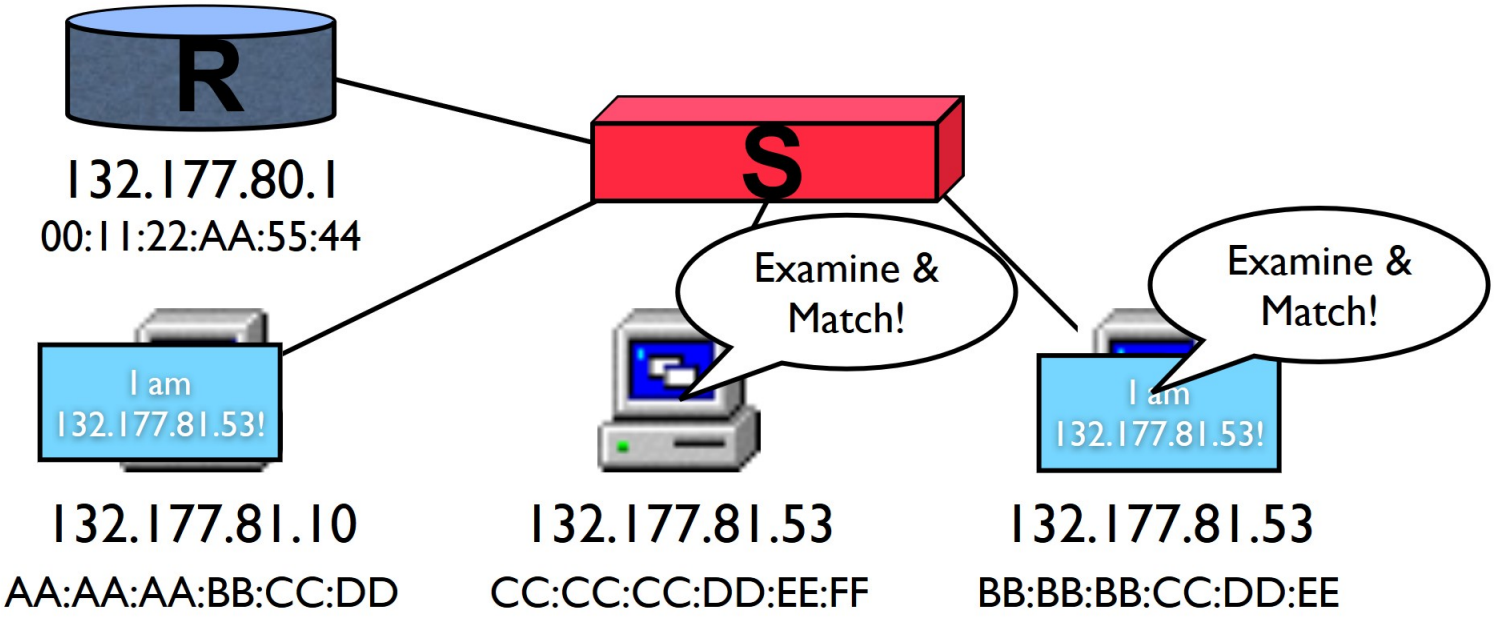
Both "CC" and "BB" respond! Let's see who gets there first!

When ARP Goes Bad…



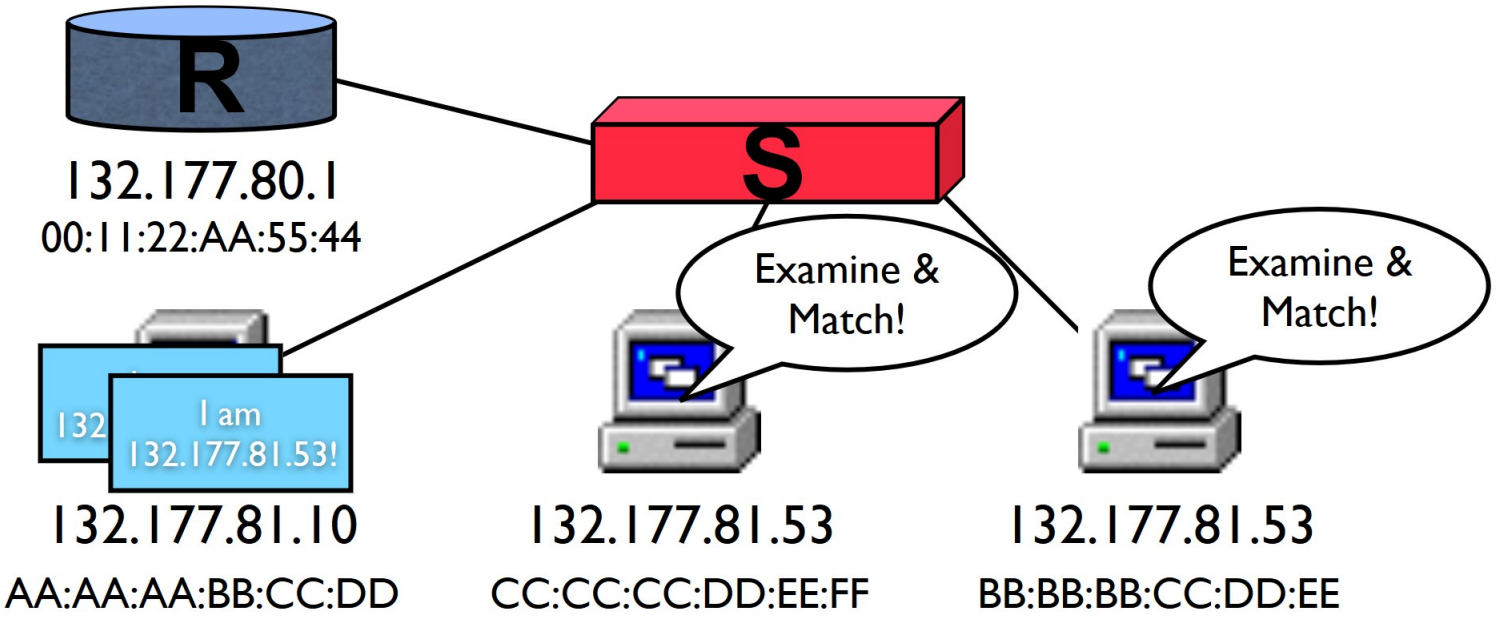
Both "CC" and "BB" respond! Let's see who gets there first!

When ARP Goes Bad…



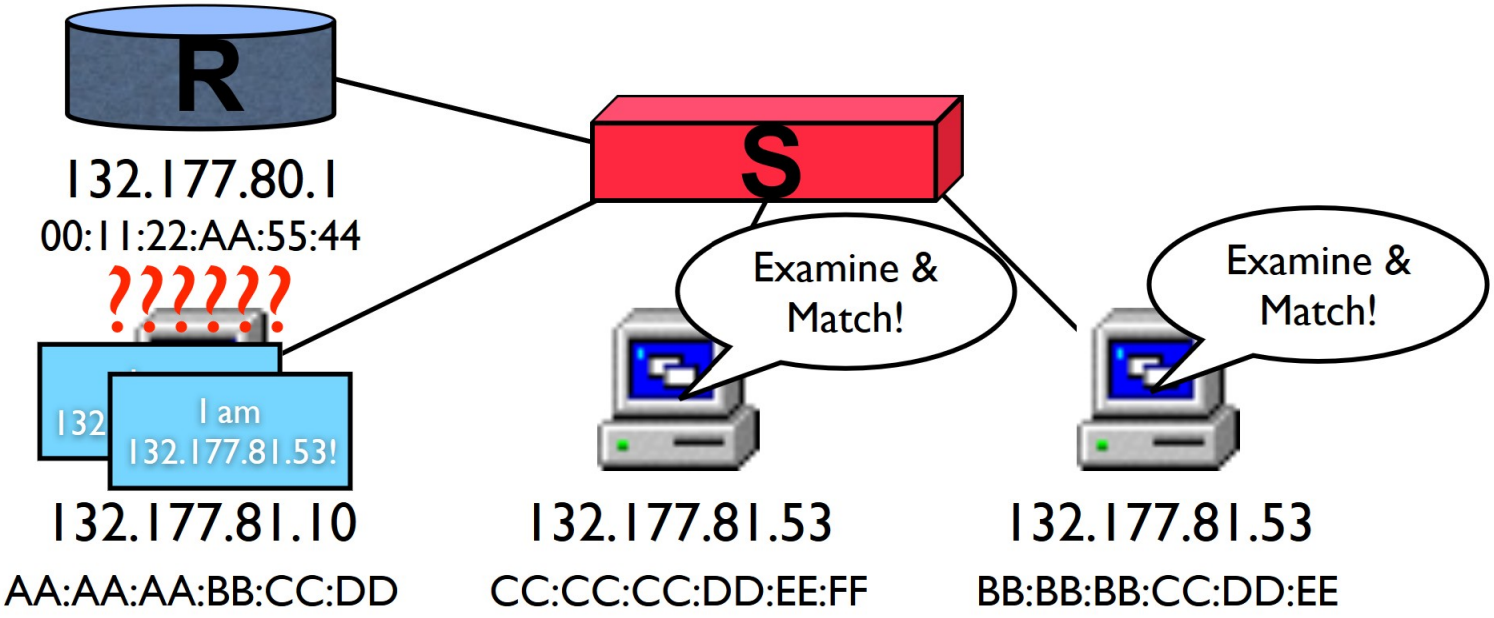
Both "CC" and "BB" respond! Let's see who gets there first!

When ARP Goes Bad…



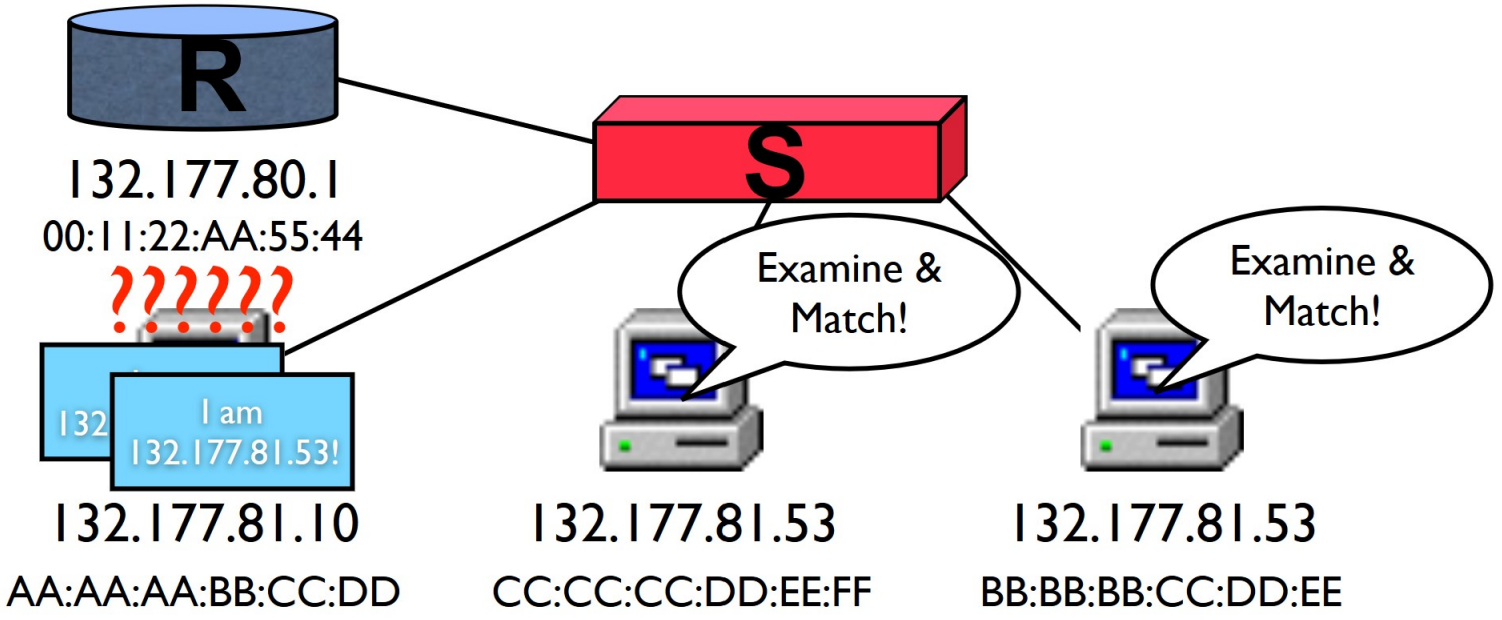
Both "CC" and "BB" respond! Let's see who gets there first!

When ARP Goes Bad…



Both "CC" and "BB" respond! Let's see who gets there first!

When ARP Goes Bad…



Both "CC" and "BB" respond! Let's see who gets there first!

ARP is the reason you cannot have the same IP address on multiple computers on a network!

Some more on ARP

ARP can be a security attack vector

- If I can get the ARP cache of a computer to have the wrong IP/MAC information, then I can direct traffic to the wrong place
- ARP has no security or validation!

ARP means you can have multiple IP addresses assigned to a single interface

If you change IP settings, you can force an ARP (`arping`) to update all local ARP caches