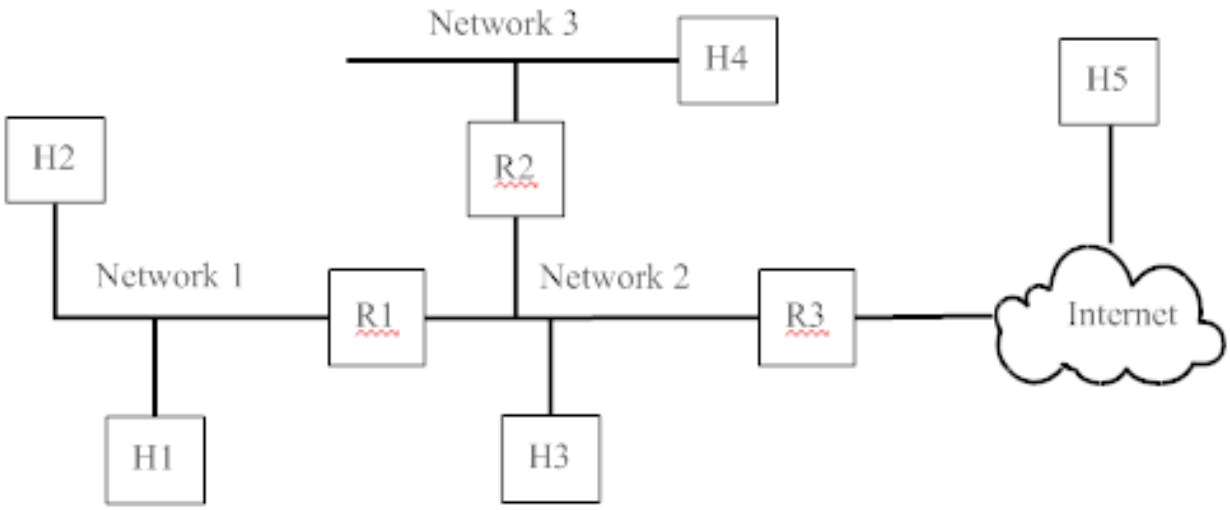
CprE 530

Lecture 11

Topics

- Packet Flow Scenarios
- IP Attacks & countermeasures
- BOOTP
- DHCP

Putting it all together



Route tables

Route Table H1 & H2

Destination	Next Hop
Network 1	Me
default	R1

Route Table H4

Destination	Next Hop
Network 3	Me
default	R2

Route Table H3

Destination	Next Hop
Network 1	R1
Network 2	H3
Network 3	R2
default	R3

Route Table Router R1

Destination	Next Hop	Interface
Network 1	R1	Int 1
Network 2	R1	Int 2
Network 3	R2	Int 2
default	R3	Int 2

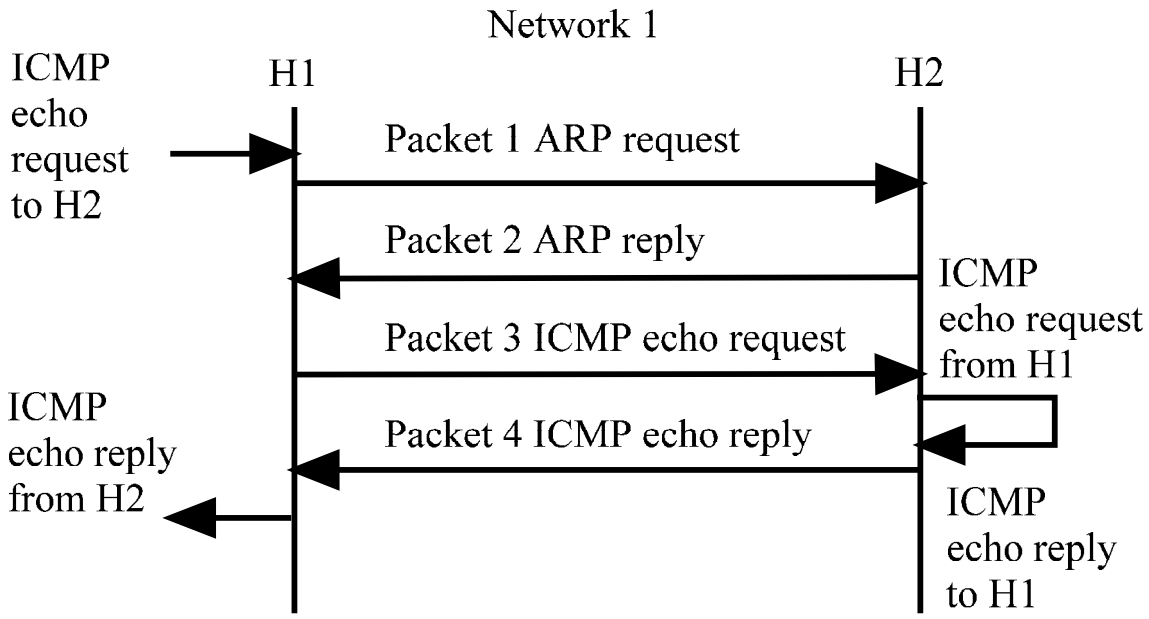
Route Table Router R2

Destination	Next Hop	Interface
Network 1	R1	Int 1
Network 2	R2	Int 1
Network 3	R2	Int 2
default	R3	Int 1

Route Table Router R3

Destination	Next Hop	Interface
Network 1	R1	Int 1
Network 2	R3	Int 1
Network 3	R2	Int 1
default	Next Hop	Int 2

Scenario 1 (H1 to H2)



Scenario 1 (H1 to H2)

Packet	Hardware Addresses		IP Addresses		Payload
	DST	SRC	DST	SRC	
1	Broadcast	H1	N/A	N/A	ARP
2	H1	H2	N/A	N/A	ARP
3	H2	H1	H2	H1	ICMP
4	H1	H2	H1	H2	ICMP

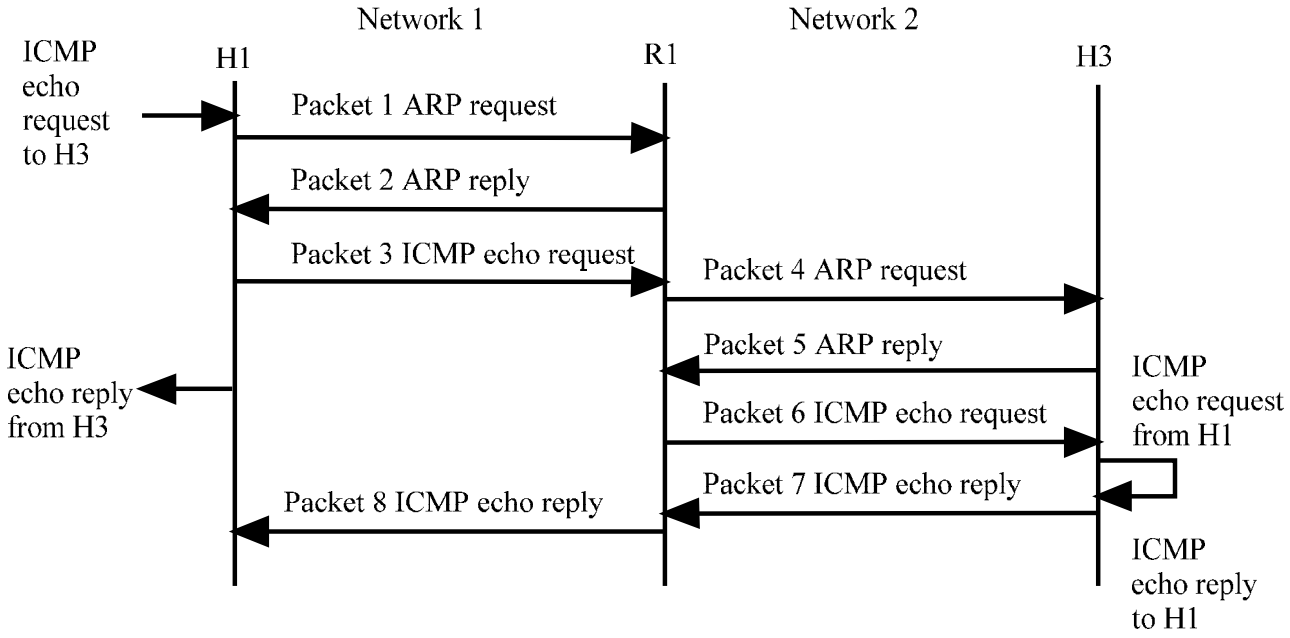
ARP table for H1

Time	Destination	HW Address
Start	Empty	Empty
After P2	H2	H2

ARP table for H2

Time	Destination	HW Address
Start	Empty	Empty
After P1	H1	H1

Scenario 2 (H1 to H3)



Scenario 2 (H1 to H3)

Packet	Hardware Addresses		IP Addresses		Payload
	DST	SRC	DST	SRC	
1	Broadcast	H1	N/A	N/A	ARP
2	H1	R1 (Int 1)	N/A	N/A	ARP
3	R1 (Int 1)	H1	H3	H1	ICMP
4	Broadcast	R1 (Int 2)	N/A	N/A	ARP
5	R1 (Int 2)	H3	N/A	N/A	ARP
6	H3	R1 (Int 2)	H3	H1	ICMP
7	R1 (Int 2)	H3	H1	H3	ICMP
8	H1	R1 (Int 1)	H1	H3	ICMP

ARP table for H1

Time	Destination	HW Address
Start	H2	H2
After P2	R1	R1 (Int 1)

ARP table for H3

Time	Destination	HW Address
Start	Empty	Empty
After P4	R1	R1 (Int 2)

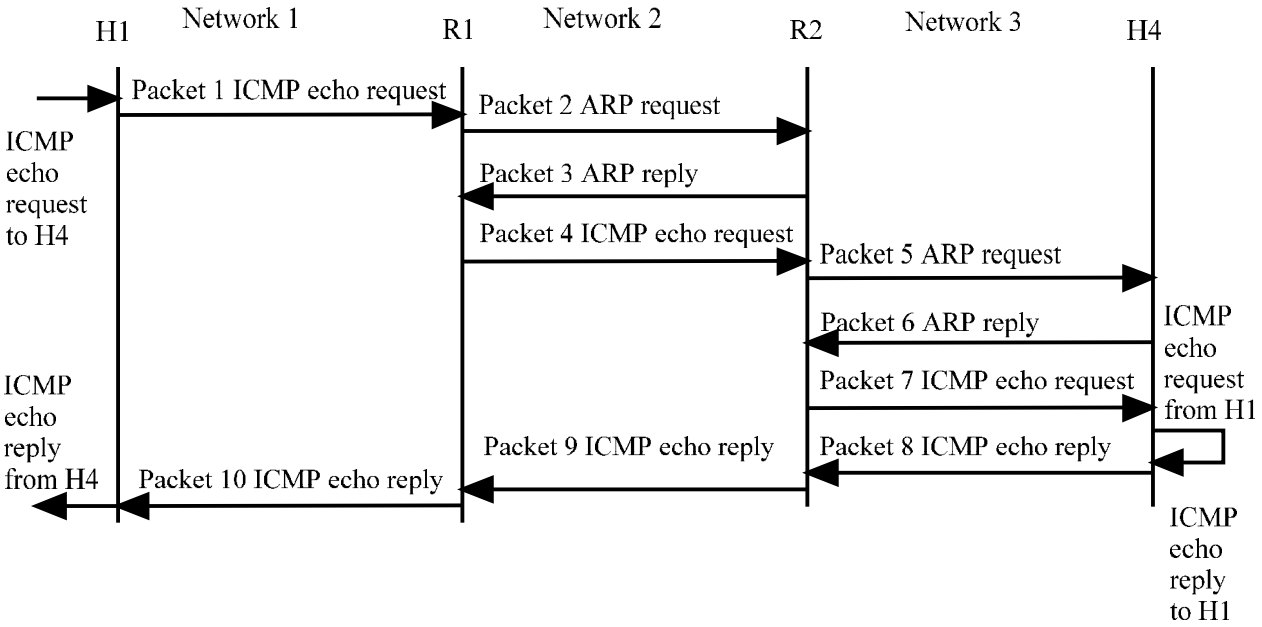
ARP table for R1 (int 1)

Time	Destination	HW Address
Start	Empty	Empty
After P1	H1	H1

ARP table for R1 (int 2)

Time	Destination	HW Address
Start	Empty	Empty
After P5	H3	H3

Scenario 3 (H1 to H4)



Scenario 3 (H1 to H4)

Packet	Hardware Addresses		IP Addresses		Payload
	DST	SRC	DST	SRC	
1	R1 (Int 1)	H1	H4	H1	ICMP
2	Broadcast	R1 (Int 2)	N/A	N/A	ARP
3	R1 (Int 2)	R2 (Int 1)	N/A	N/A	ARP
4	R2 (Int 1)	R1 (Int 2)	H4	H1	ICMP
5	Broadcast	R2 (Int 2)	N/A	N/A	ARP
6	R2 (Int 2)	H4	N/A	N/A	ARP
7	H4	R2 (Int 2)	H4	H1	ICMP
8	R2 (Int 2)	H4	H1	H4	ICMP
9	R1 (Int 2)	R2 (Int 1)	H1	H4	ICMP
10	H1	R1 (Int 1)	H1	H4	ICMP

ARP table for H1

Time	Destination	HW Address
Start	H2	H2
	R1	R1 (Int 1)

ARP table for H4

Time	Destination	HW Address
Start	Empty	Empty
After P5	R2	R2 (Int 2)

ARP table for R1 (int 1)

Time	Destination	HW Address
Start	H1	H1

ARP table for R1 (int 2)

Time	Destination	HW Address
Start	H3	H3
After P3	R2	R2 (Int 1)

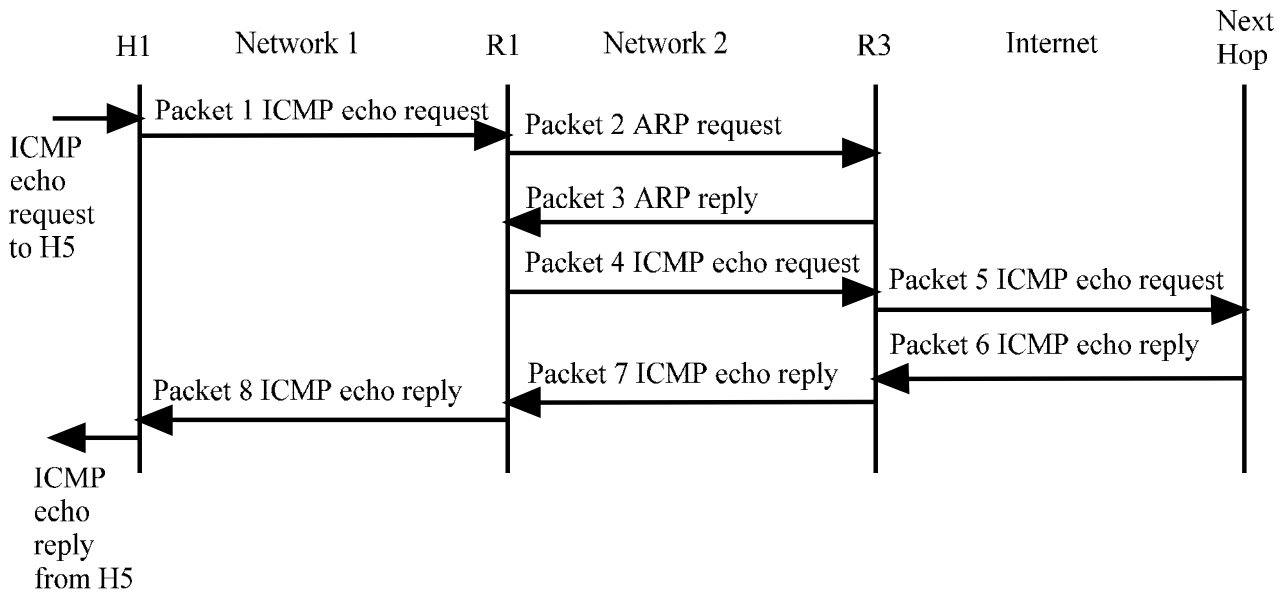
ARP table for R2 (int 1)

Time	Destination	HW Address
Start	Empty	Empty
After P2	R1	R1 (Int 2)

ARP table for R2 (int 2)

Time	Destination	HW Address
Start	Empty	Empty
After P6	H4	H4

Scenario 4 (H1 to H5)



Scenario 4 (H1 to H5)

Packet	Hardware Addresses		IP Addresses		Payload
	DST	SRC	DST	SRC	
1	R1 (Int 1)	H1	H5	H1	ICMP
2	Broadcast	R1 (Int 2)	N/A	N/A	ARP
3	R1 (Int 2)	R3 (Int 1)	N/A	N/A	ARP
4	R3 (Int 1)	R1 (Int 2)	H5	H1	ICMP
5	Next hop	R3 (Int 2)	H5	H1	ICMP
6	R3 (Int 2)	Next hop	H1	H5	ICMP
7	R1 (Int 2)	R3 (Int 1)	H1	H5	ICMP
8	H1	R1 (Int 1)	H1	H5	ICMP

ARP table for H1

Time	Destination	HW Address
Start	H2	H2
	R1	R1 (Int 1)

ARP table for H4

Time	Destination	HW Address
Start	Empty	Empty
	R2	R2 (Int 2)

ARP table for R1 (int 1)

Time	Destination	HW Address
Start	H1	H1

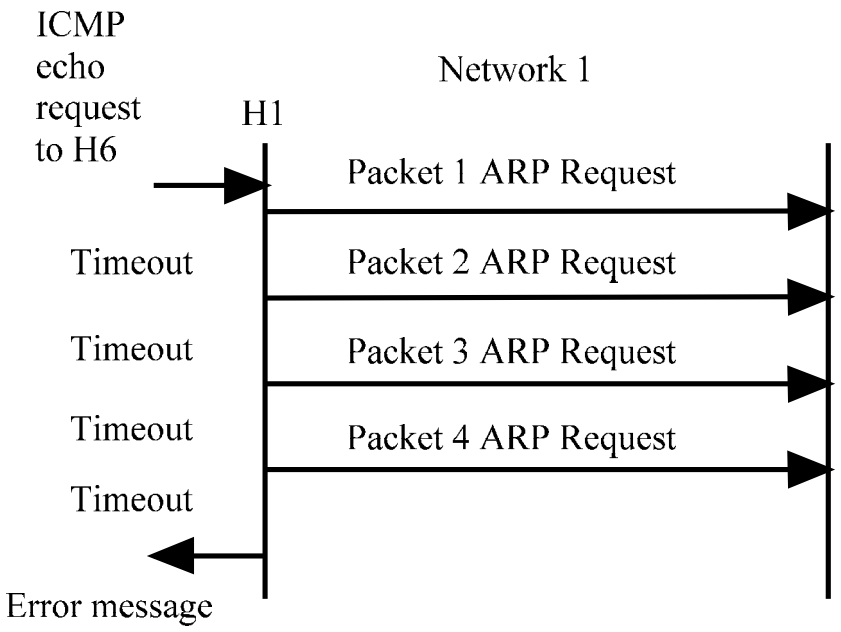
ARP table for R1 (int 2)

Time	Destination	HW Address
Start	H3	H3
	R2	R2 (Int 1)
After P3	R3	R3 (Int 1)

ARP table for R3 (int 1)

Time	Destination	HW Address
Start	Empty	Empty
After P2	R1	R1 (Int 2)

Scenario 5 (H1 to no host on net 1)



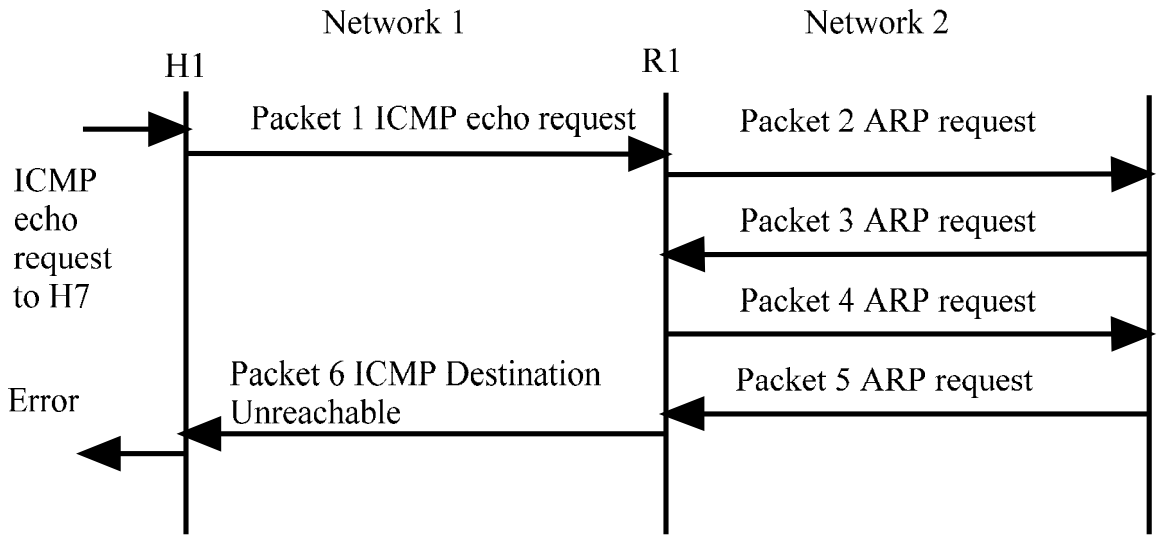
Scenario 5 (H1 to no host on net 1)

Packet	Hardware Addresses		IP Addresses		Payload
	DST	SRC	DST	SRC	
1	Broadcast	H1	N/A	N/A	ARP
2	Broadcast	H1	N/A	N/A	ARP
3	Broadcast	H1	N/A	N/A	ARP
4	Broadcast	H1	N/A	N/A	ARP

ARP table for H1

Time	Destination	HW Address
Start	H2	H2
	R1	R1 (Int 1)

Scenario 6 (H1 to no host on net 2)



Scenario 6 (H1 to no host on net 2)

Packet	Hardware Addresses		IP Addresses		Payload
	DST	SRC	DST	SRC	
1	R1 (Int 1)	H1	H7	H1	ICMP
2	Broadcast	R1 (Int 2)	N/A	N/A	ARP
3	Broadcast	R1 (Int 2)	N/A	N/A	ARP
4	Broadcast	R1 (Int 2)	N/A	N/A	ARP
5	Broadcast	R1 (Int 2)	N/A	N/A	ARP
6	H1	R1 (Int 1)	H1	R1	ICMP

ARP table for H1

Time	Destination	HW Address
Start	H2	H2
	R1	R1 (Int 1)

ARP table for R1 (int 2)

Time	Destination	HW Address
Start	H3	H3
	R2	R2 (Int 1)
	R3	R3 (Int 1)

ARP table for R1 (int 1)

Time	Destination	HW Address
Start	H1	H1

Header Based

- There have been some IP header attacks.
- Most famous is the ping of death
- Most have been fixed
- Fewer ARP and ICMP header attacks

Protocol Based

- Even though the IP protocol is simple, the routing is complex.
- There are a large number of protocol based attacks involving sending packets the confuse the receiver or interjects packets into the receiver.
- They work because there is no authentication of the sender and receiver.

Protocol Based

- ICMP:
  - Using redirect
- ARP
  - ARP cache poisoning (better classified as an authentication attack

Authentication Based

- This is a big problem, since we often use the IP address as authentication.
- IP
  - Address spoofing is very difficult to implement unless you can “see” the traffic
  - IP address spoofing is very hard to stop if the attacker is in the right place.
- ARP
- DHCP

IP Spoofing

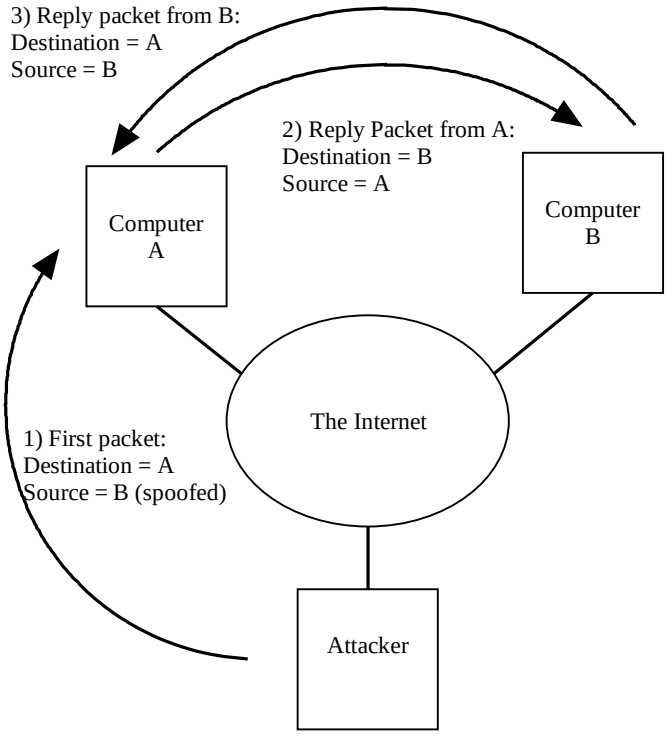


Figure 6.20 IP Address Spoofing

IP Spoofing Mitigation

- Check source IP address before allowing packet into the Internet

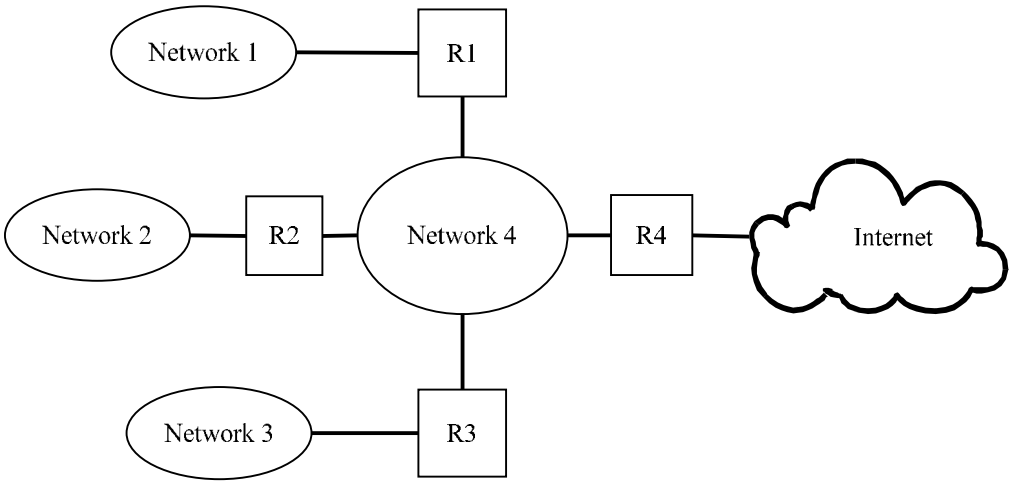


Figure 6.21 IP Address Spoofing Mitigation

Traffic Based

- Sniffing is a problem
- Broadcast traffic can cause flooding
- Flooding is a problem with unicast packets also. They can cause routers to hosts to quit.

ARP Broadcast Flood

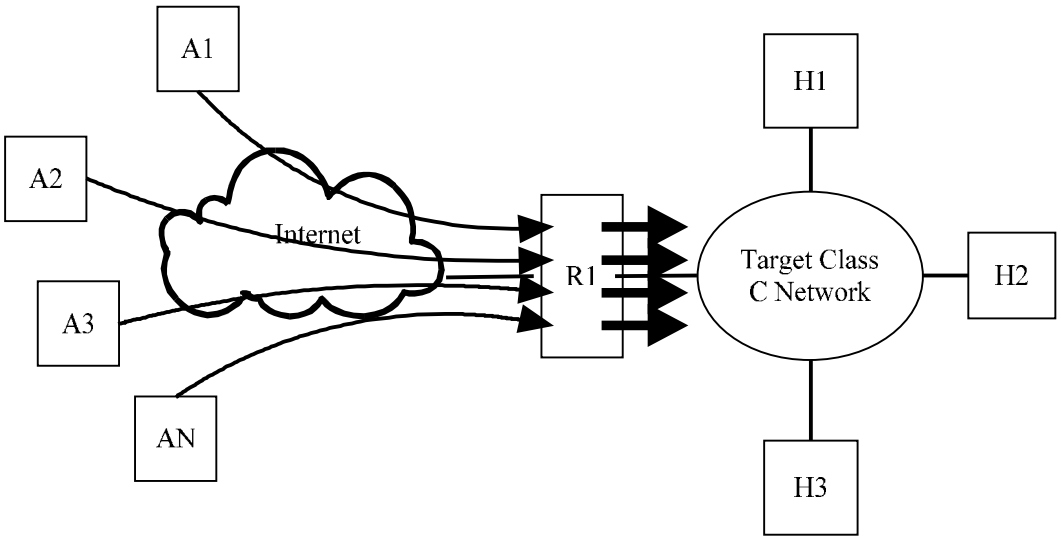


Figure 6.23 ARP Broadcast Flood Attack

BOOTP

- Bootstrap Protocol
- Allows a networked machine to automatically acquire an IP address
- Client-server program
- Server has configuration file which contains a one-to-one mapping between the hardware address of the client and an IP address
- Used for networked laser printers and other diskless machines

BOOTP

- BOOTP server provides client with:
  - IP address
  - Subnet mask
  - IP address of a router
  - IP address of a nameserver

BOOTP

Sample configuration for a printer

```
hp255:\
  :hn:ht=ether:vm=rfc1048:\
  :ha=0800094ce9f5:\
  :ip=129.186.5.7:\
  :sm=255.255.255.0:\
  :gw=129.186.5.254:\
  :lg=129.186.5.2:\
  :T144="hp.printer":
```

Hardware address

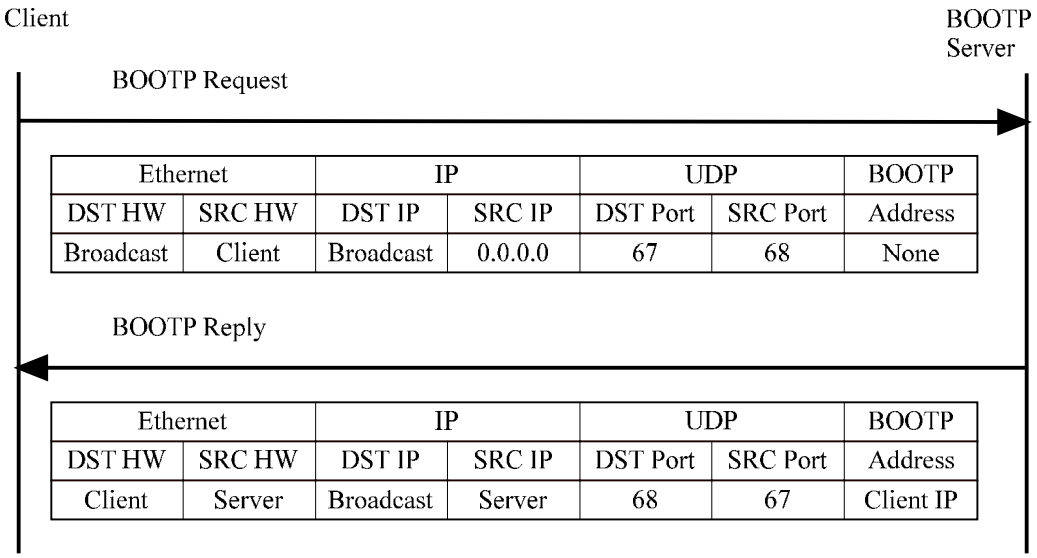
IP

Netmask

Gateway

Logging device

BOOTP Protocol



Ethernet		IP		UDP		BOOTP
DST HW	SRC HW	DST IP	SRC IP	DST Port	SRC Port	Address
Broadcast	Client	Broadcast	0.0.0.0	67	68	None

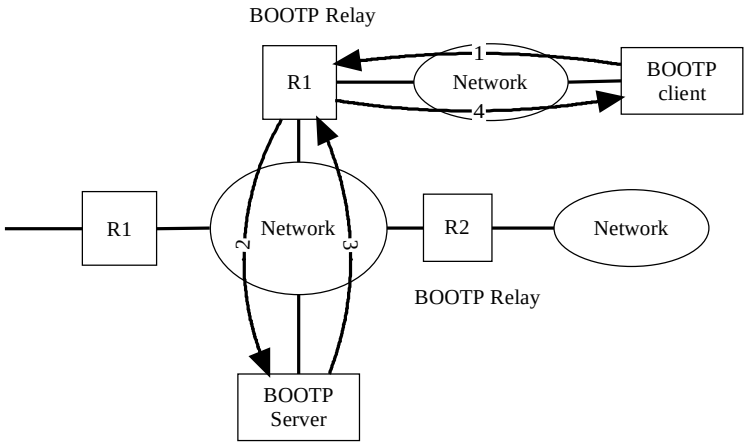
Ethernet		IP		UDP		BOOTP
DST HW	SRC HW	DST IP	SRC IP	DST Port	SRC Port	Address
Client	Server	Broadcast	Server	68	67	Client IP

Figure 6.24 BOOTP Protocol

BOOTP

- Note that the client must broadcast it's request, since it does not know who the local router is
- The server cannot use ARP to determine the client's hardware address, so it gets it from the client's request packet
- BOOTP relay
  - Used when client and server are on different subnets
  - Relay receives requests, appends its address, sends requests to server
  - Server replies to relay who then replies to client

BOOTP Relay



	Ethernet		IP		UDP		BOOTP
Packet	DST HW	SRC HW	DST IP	SRC IP	DST Port	SRC Port	Address
1	Broadcast	Client	Broadcast	0.0.0.0	67	68	none
2	Server	Relay	Server	Relay	67	68	none
3	Relay	Server	Relay	Server	68	67	Client IP
4	Client	Relay	Broadcast	Relay	68	67	Client IP

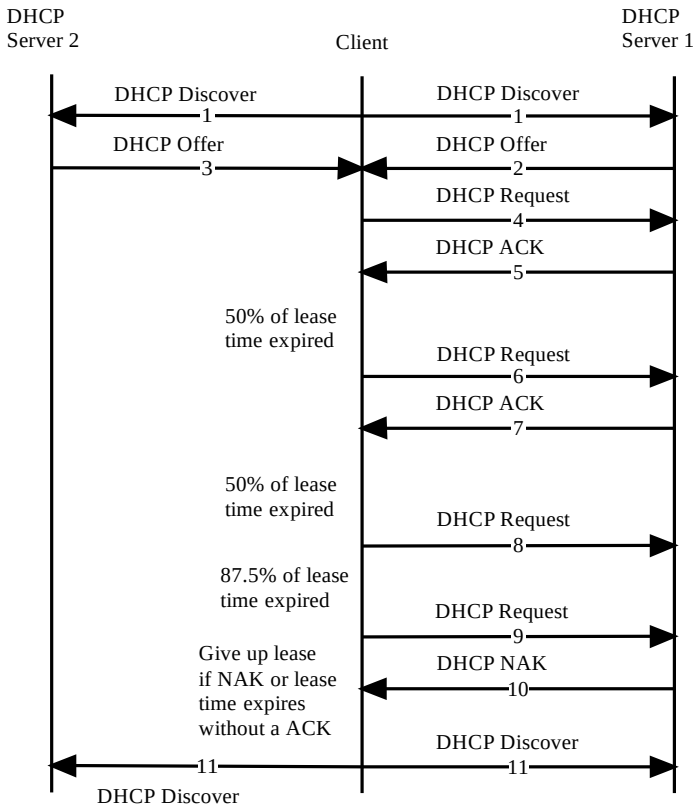
DHCP

- Dynamic Host Configuration Protocol
- An enhancement to BOOTP
- Leases IP addresses to hosts requesting an address
- Dynamic leases (not a one-to-one mapping)

DHCP

- Two databases for each DHCP server:
  - Static IP pool (like bootp)
  - Dynamic pool
- Server checks static pool for match before dynamic pool
- Dynamic pool
  - Addresses are temporary (default lease = 1 hr)
  - After lease expires, client must ask for a renewal
  - If renewal is rejected, client must give up the IP address

DHCP Operation



DHCP Operation

	Ethernet		IP		UDP		DHCP
Packet	DST HW	SRC HW	DST IP	SRC IP	DST Port	SRC Port	
1	Broadcast	Client	Broadcast	0.0.0.0	67	68	Discover
2	Client	Server 1	Broadcast	Server 1	68	67	Offer
3	Client	Server 2	Broadcast	Server 2	68	67	Offer
4	Server 1	Client	Server 1	0.0.0.0	67	68	Request
5	Client	Server 1	Broadcast	Server 1	68	67	ACK
6	Server 1	Client	Server 1	Client	67	68	Request
7	Client	Server 1	Broadcast	Server 1	68	67	ACK
8	Server 1	Client	Server 1	Client	67	68	Request
9	Server 1	Client	Server 1	Client	67	68	Request
10	Client	Server 1	Broadcast	Server 1	68	67	NAK
11	Broadcast	Client	Broadcast	0.0.0.0	67	68	Discover

DHCP Operation

- Client sends DHCP discover up to 5 times at 2 sec intervals until the DHCP offer is received. If it fails, it will try again after 5 minutes
- The DHCP offer contains the lease time
- After the offer is sent, the server locks that IP address
- Client chooses one offer and sends a DHCP request to the server. (If there are multiple servers, the client may receive more than one offer)
- Server responds with DHCP ack, and creates the binding between the HW address and IP address
- Client can now use the IP address

DHCP Operation

- Before 50% of the lease has expired, the client must send another DHCP request to ask for renewal
- If the server responds with a DHCP ack, the client resets its timer
- If the server responds with a DHCP nak, the client must immediately stop using the IP address and find another server
- If the server does not respond, the client sends another DHCP request after 87.5% of lease has expired
- If the lease expires before the server responds, the client gives up the IP address
- Client sends DHCP release to give up IP address (can do this at any time)

DHCP Packet Format

Op Code	Hardware type	Hardware Len	Hop Count
ID			
Number of Seconds		Flag + Unused	
Client IP Address			
Client IP Address (used in reply packet)			
Server IP Address			
Gateway IP Address			
Client Hardware Address (16 bytes)			
Server Name (64 bytes)			
Boot File Name (128 bytes)			
Options (contains DHCP message types)			

Figure 6.27 DHCP/BOOTP Header Format

Header based attacks

- Very simple header, no attacks

Protocol / Auth based attacks

- BOOTP is a simple protocol
  - An attacker could try and give false information causing a host to get the wrong IP address. (really an authentication attack)
- DHCP is more complex
  - An attacker could give false information
  - An attacker could reserve all of the addresses
  - An attacker could send fake release packets

Traffic Based

- Sniffing in not an issue since the information is not a secret
- Not any real good flooding based attacks due to the slow nature of the protocol