CSE 410/565: Computer Security

Instructor: Dr. Ziming Zhao

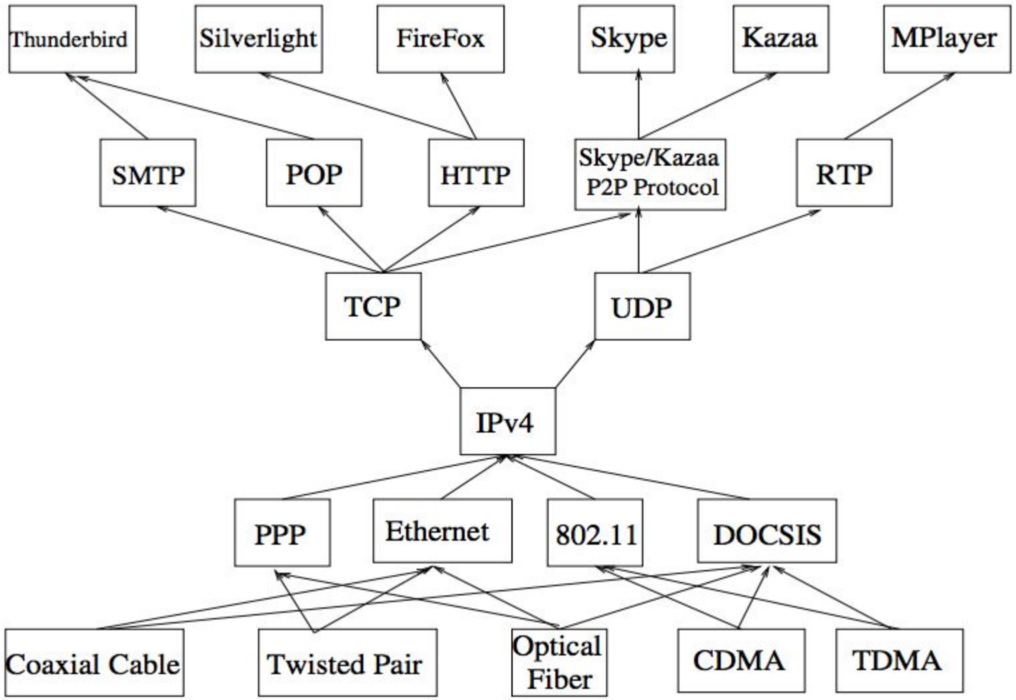
Network Layer Overview

- IP address and Subnetting
- Address Resolution Protocol (ARP)
- How a router works

The Postal Analogy

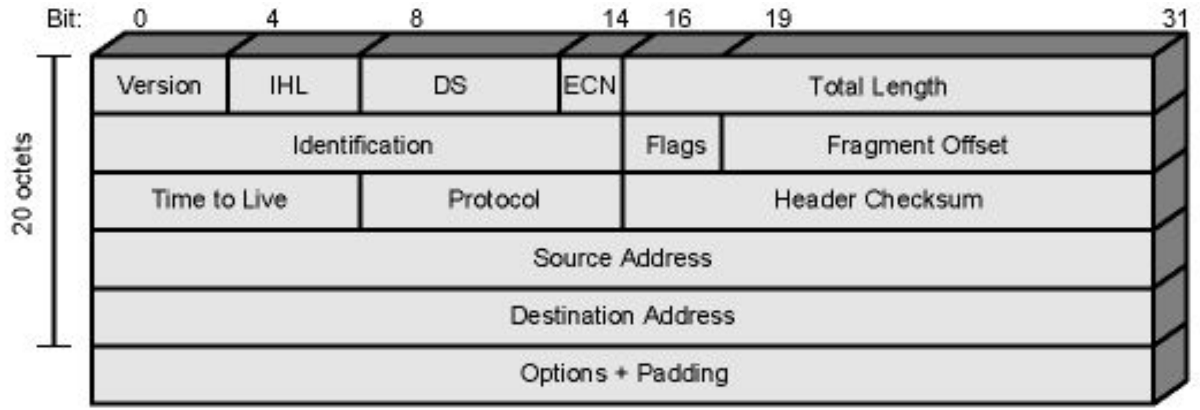
- A- Write a 20 page letter to a foreign country.
- P- Translate the letter so the receiver can read it.
- S- Insure the intended recipient can receive letter.
- T- Separate and number pages. Like registered mail, tracks delivery and requests another package if one is “lost” or “damaged” in the mail.
- **N- Postal Center sorting letters by zip code to *route* them closer to destination.**
- D- Local Post Office determining which vehicles to deliver letters.
- P- Physical Trucks, Planes, Rail, autos, etc which carry letter between stations.

IP (Internet Protocol)



IP (Internet Protocol)

- The core of the TCP/IP protocol suite
- Two versions co-exist
  - v4 – the widely used IP protocol
  - v6 – has been standardized in 1996, but still not widely deployed
- IP (v4) header minimum 20 octets (160 bits)



IPv4

- Less than 2^32 = 4,294,967,296 unique IP addresses
  - 2020, 40 Billion IoT devices?

IPv6

- Enhancements over IPv4 for modern high speed networks
- But the driving force behind v6 was to increase address space
  - 128-bit as compared to 32-bit of v4
- Network Address Translation (NAT)
- Not backward compatible: all equipment and software must change

What is an IP Address?

- An IP address is a unique global address for a network interface
  - Logical, not physical
  - There are private IP addresses

- An IP address is a **32 bit long** identifier

- An IP address encodes a network number (**network prefix**) and a **host number**

Dotted Decimal Notation

- IP addresses are written in a so-called **dotted decimal notation**
- Each byte is identified by a decimal number in the range [0..255]:

- **Example:**

10000000	10001111	10001001	10010000
1st Byte	2nd Byte	3rd Byte	4th Byte
= 128	= 143	= 137	= 144

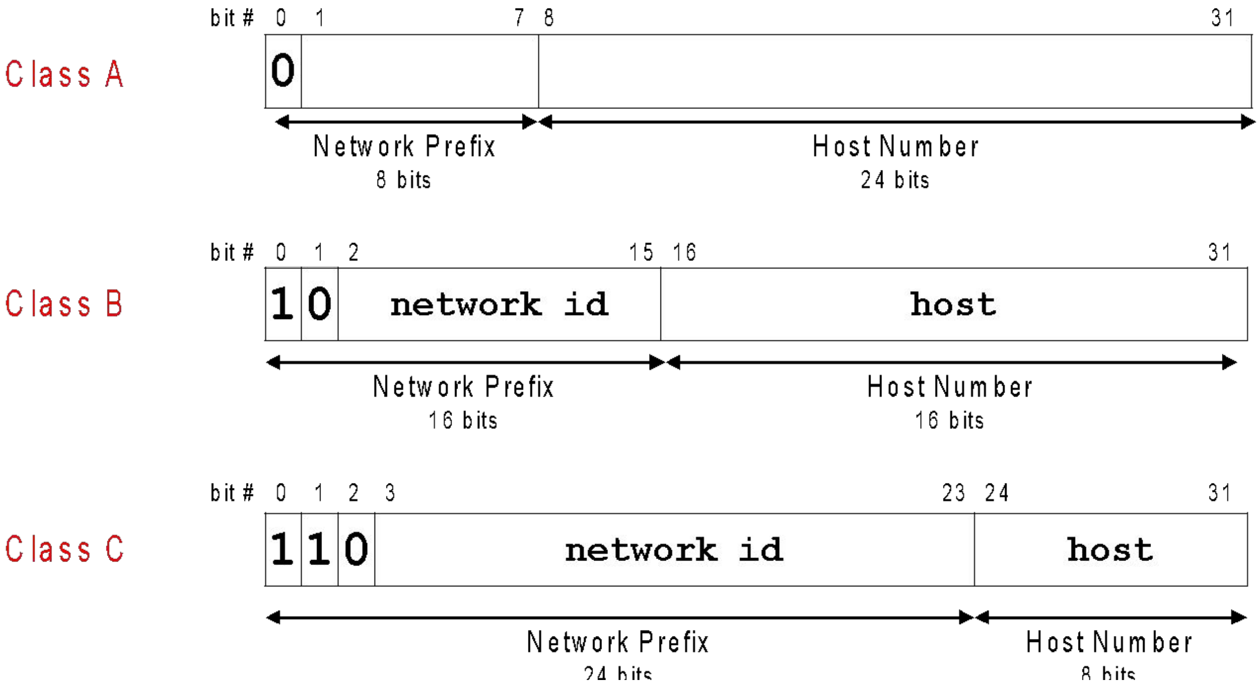
128.143.137.144

Network prefix and Host number

- The network prefix identifies a network and the host number identifies a specific host (actually, interface on the network).

- How do we know how long the network prefix is?
  - The network prefix used to be implicitly defined (class-based addressing, A,B,C,D…)
  - The network prefix now is flexible and is indicated by a prefix/netmask (classless).

The old way: Internet Address Classes



CIDR - Classless Interdomain Routing

- Goals:
  - Restructure IP address assignments to increase efficiency
  - Hierarchical routing aggregation to minimize route table entries

- Key Concept: The length of the network id (prefix) in IP addresses is **arbitrary/flexible** and is defined by the network hierarchy.

- Consequence:
  - Routers use the IP address and the length of the prefix for forwarding.
  - All advertised IP addresses must include a **prefix**

CIDR

- Address format:

a.b.c.d/x

where x is # bits in subnet portion of address

CIDR: Prefix Size vs. Host Space

CIDR Block Prefix	# of Host Addresses
/27	32 hosts
/26	64 hosts
/25	128 hosts
/24	256 hosts
/23	512 hosts
/22	1,024 hosts
/21	2,048 hosts
/20	4,096 hosts
/19	8,192 hosts
/18	16,384 hosts
/17	32,768 hosts
/16	65,536 hosts
/15	131,072 hosts
/14	262,144 hosts
/13	524,288 hosts

Private IP Addresses

- There are three IP network addresses reserved for private networks. The addresses are
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

Subnet Calculation

- Host IP Address: 138.101.114.250/26
- Subnet Mask: 255.255.255.192

	138.	**101.**	**114.**	**250**
IP Address	10001010	01100101	01110010	11111010
Mask	11111111	11111111	11111111	11000000
	255.	**255.**	**255.**	**192**

Step 1:

Translate Host IP Address and Subnet Mask into binary notation

Subnet Calculation

	138.	101.	114.	250
IP Address	10001010	01100101	01110010	11111010
Mask	11111111	11111111	11111111	11000000
Network	10001010	01100101	01110010	11000000
	138	**101**	**114**	**192**

Step 2:

Determine the Network (or Subnet) where this Host address lives:

1. Draw a line under the mask
2. Perform a bit-wise AND operation on the IP Address and the Subnet Mask

Note: 1 AND 1 results in a 1, 0 AND anything results in a 0

Subnet Calculation

	138.	101.	114.	250
IP Address	10001010	01100101	01110010	11111010
Mask	11111111	11111111	11111111	11000000
Network	10001010	01100101	01110010	11000000
	138	**101**	**114**	**192**

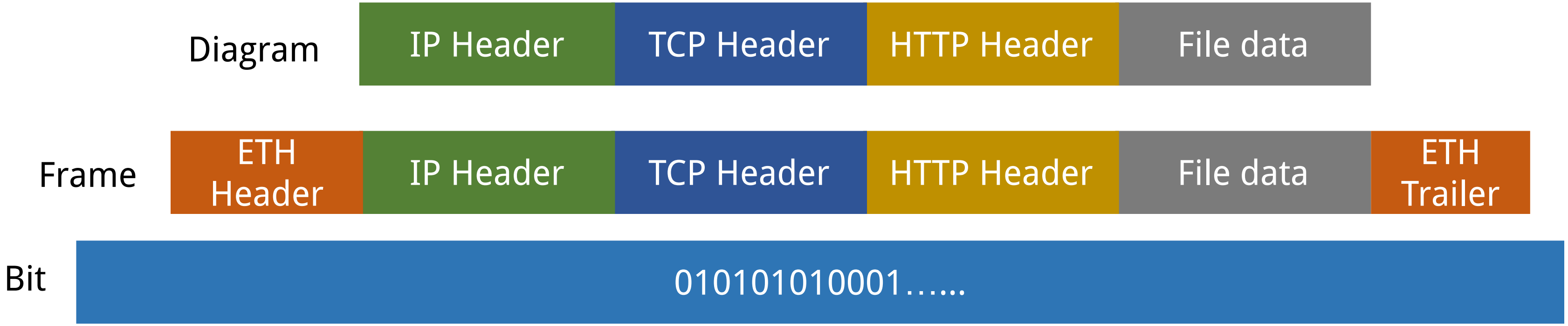
Step 2:

Determine the Network (or Subnet) where this Host address lives:

3. Express the result in Dotted Decimal Notation
4. The result is the **Subnet Address** of this Subnet, which is 138.101.114.192

64 IP Addresses: 138.101.114.192 – 138.101.114.255

IP Packet / Diagram



ARP (Address Resolution Protocol)

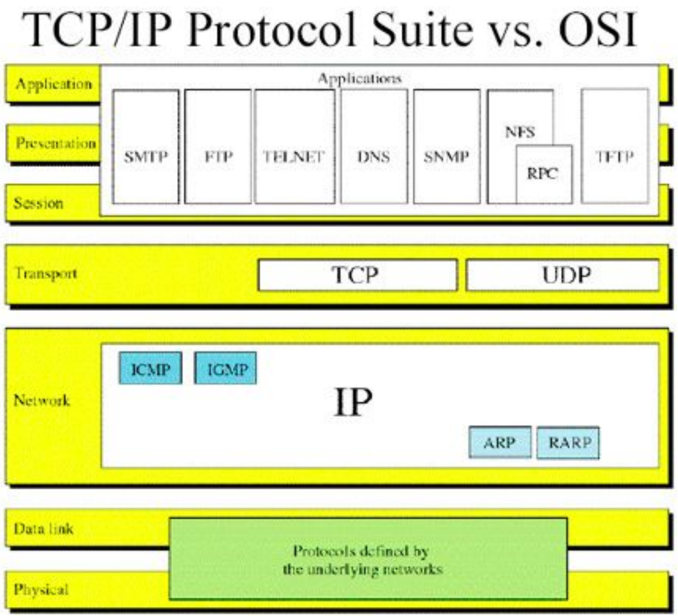
The delivery of a packet to a host or a router requires two levels of addressing:

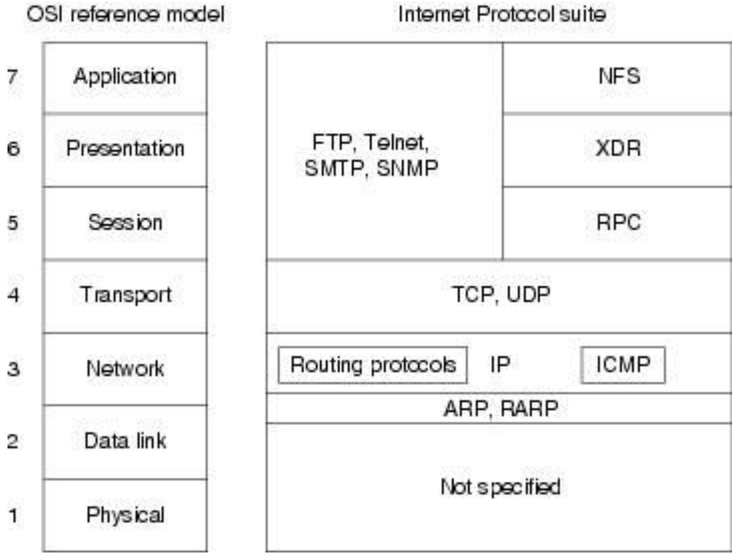
- logical and physical.
- We need to be able to map a logical address to its corresponding physical address and vice versa. These can be done using either static or dynamic mapping.

ARP (Address Resolution Protocol)

- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network.
- This means that the sender needs the physical address of the receiver.
- A mapping corresponds a logical address to a physical address.
- ARP accepts a logical address from the IP protocol, maps the address to the corresponding physical address and pass it to the data link layer.

Position of ARP in the TCP/IP Suite





Routers

- A router is a networking device that forwards data packets **between computer networks**.

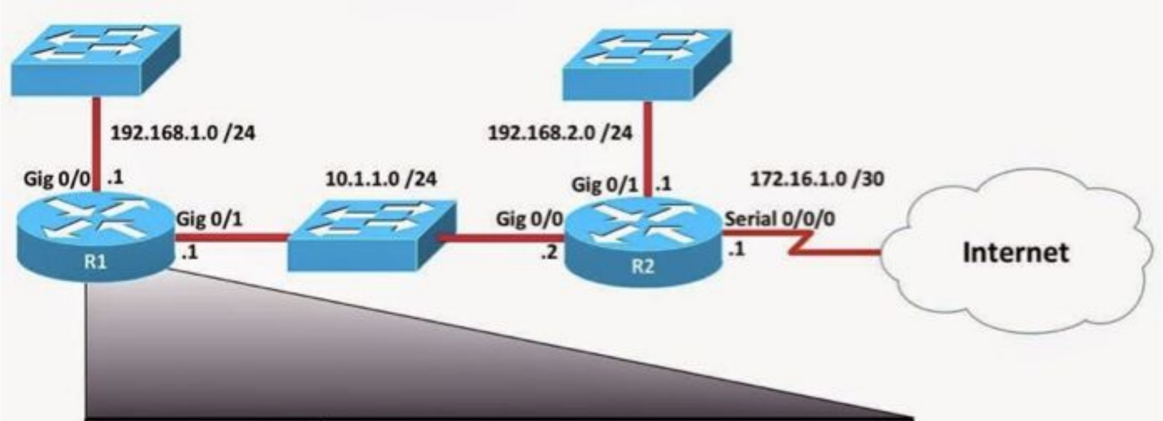
- Routers perform the **traffic directing** functions on the Internet.

- A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

Routers

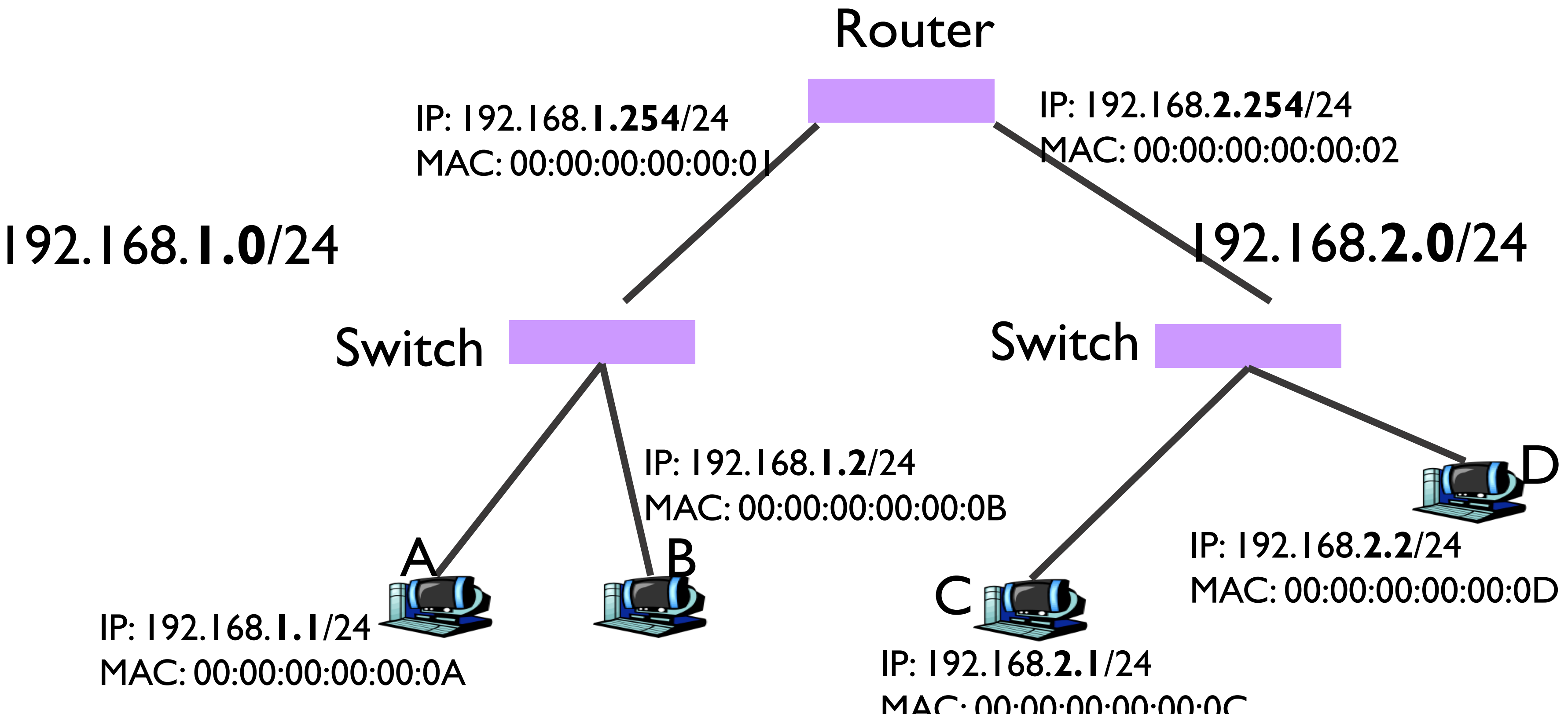
- **Dissimilar** computer networks may have different **network access and physical layers**, but they have to speak the same (inter)network protocol implemented in all end systems and routers
    - IP protocol

Routing Table



Network	Outgoing Interface or Next Hop
192.168.1.0 /24	Gig 0/0 (Directly Connected)
10.1.1.0 /24	Gig 0/1 (Directly Connected)
192.168.2.0 /24	10.1.1.2 (Next Hop)
172.16.1.0 /30	10.1.1.2 (Next Hop)
0.0.0.0 /0	10.1.1.2 (Next Hop)

Example



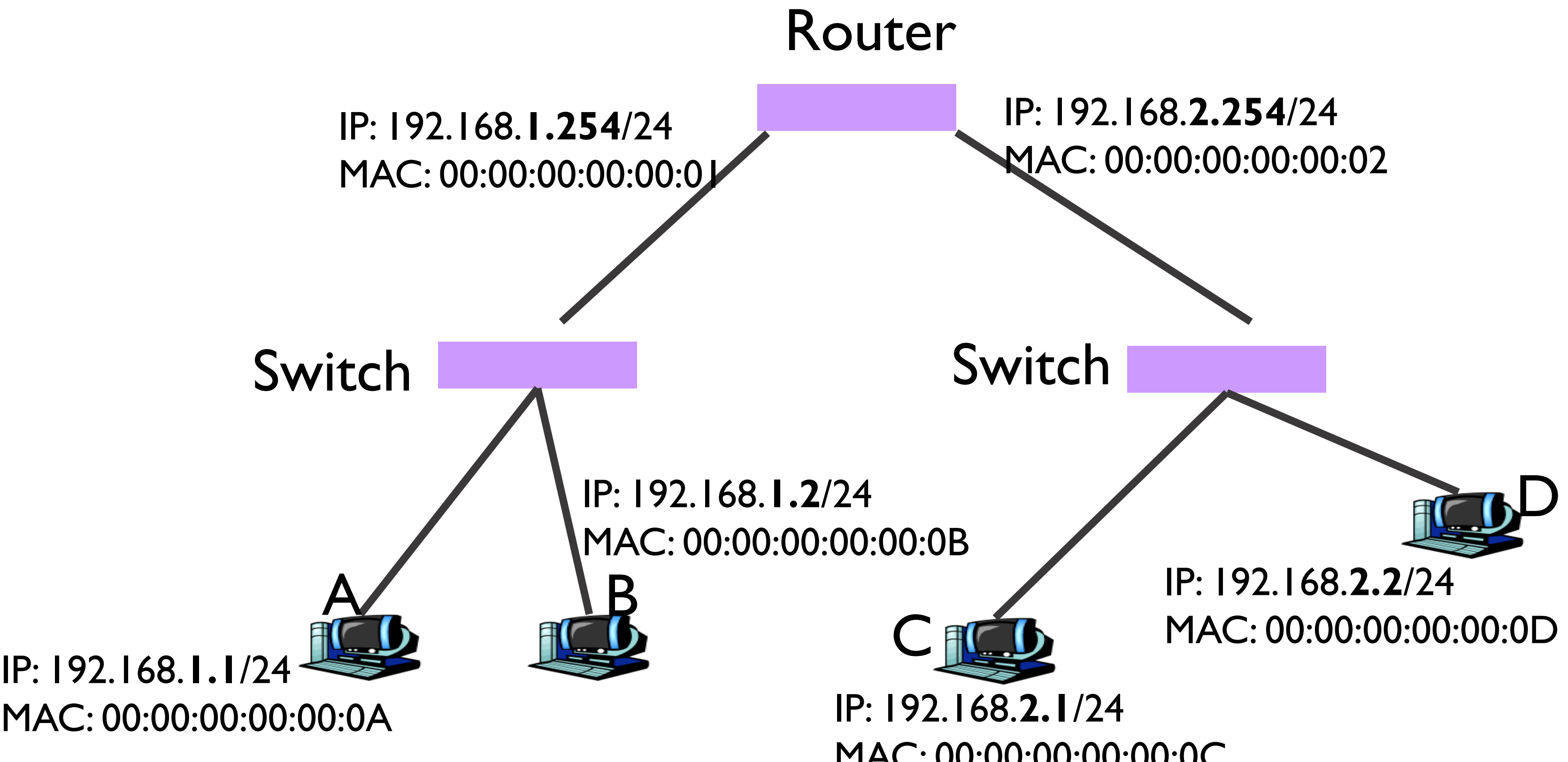
Router
IP: 192.168.**1.254**/24
MAC: 00:00:00:00:00:01
IP: 192.168.**2.254**/24
MAC: 00:00:00:00:00:02
192.168.**1.0**/24
192.168.**2.0**/24
Switch
Switch
IP: 192.168.**1.2**/24
MAC: 00:00:00:00:00:0B
D
IP: 192.168.**2.2**/24
MAC: 00:00:00:00:00:0D
A
B
C
IP: 192.168.**1.1**/24
MAC: 00:00:00:00:00:0A
IP: 192.168.**2.1**/24
MAC: 00:00:00:00:00:0C

Scenario 1: A B. In other words, 192.168.1.1 192.168.1.2

Step 1: Is 192.168.1.2 on my subnet?

Step 2: ARP Request: What is the MAC for 192.168.1.2?

Step 3: Construct packet with right src/dst MAC/IP

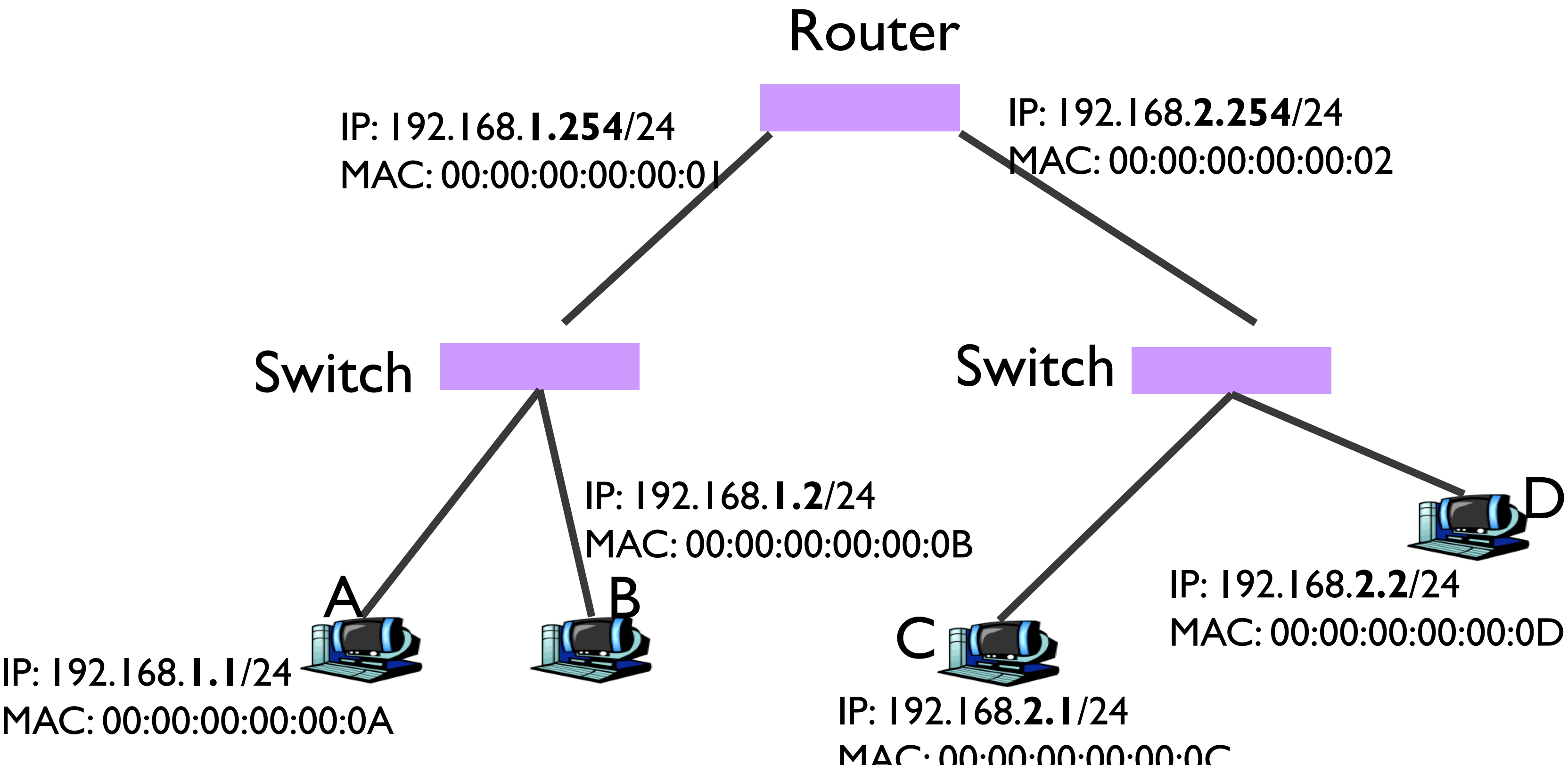


Scenario 2: A C. In other words, 192.168.1.1 192.168.2.1

Step 1: Is 192.168.2.1 on my subnet?

Step 2: ARP Request: What is the MAC for 192.168.1.254?

Step 3: R replies 01



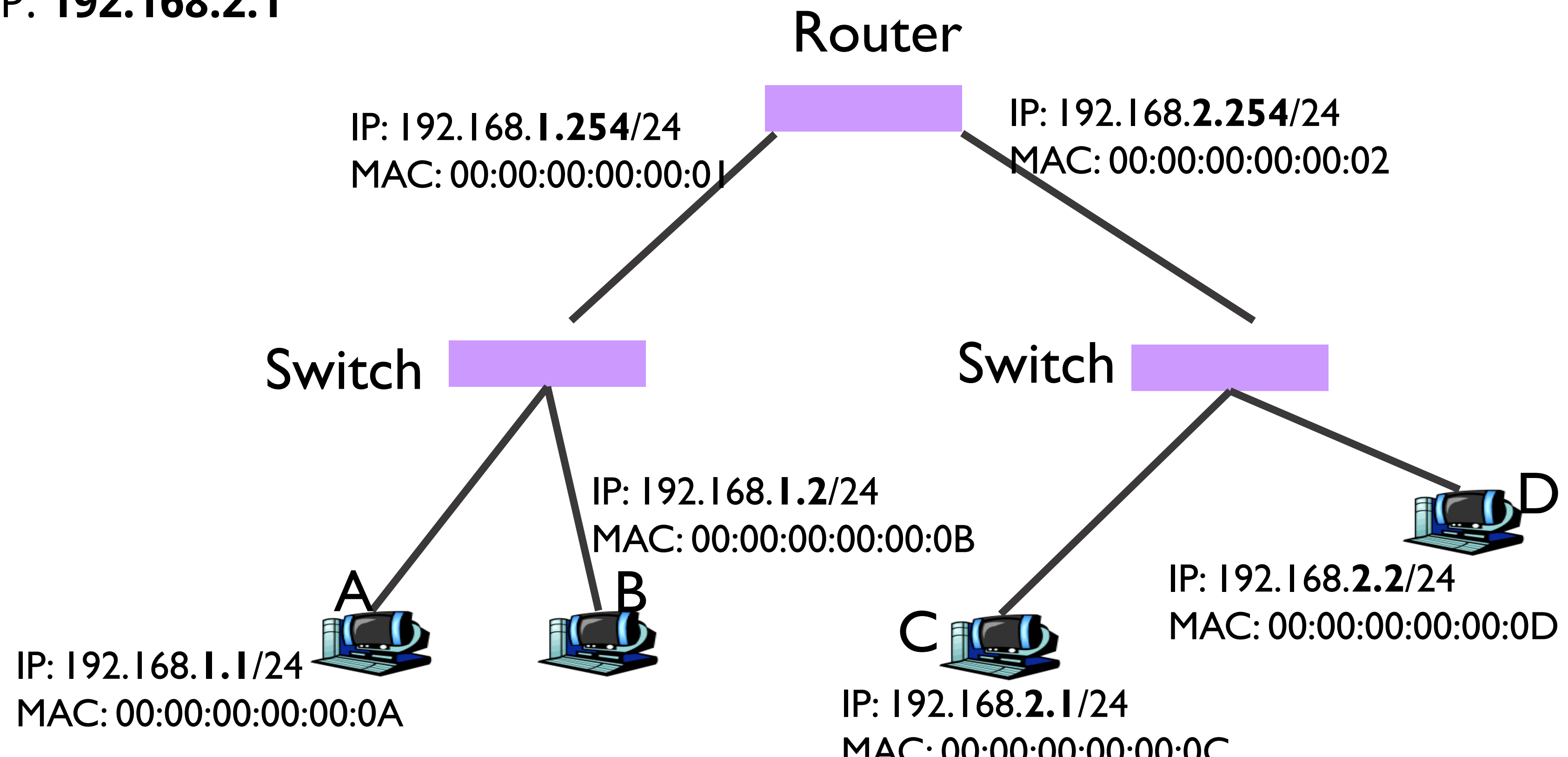
Scenario 2: A C. In other words, 192.168.1.1 192.168.2.1

Step 4: A sends the frame to R

SRC MAC: 0A, DST MAC: **01**

SRC IP: 192.168.1.1

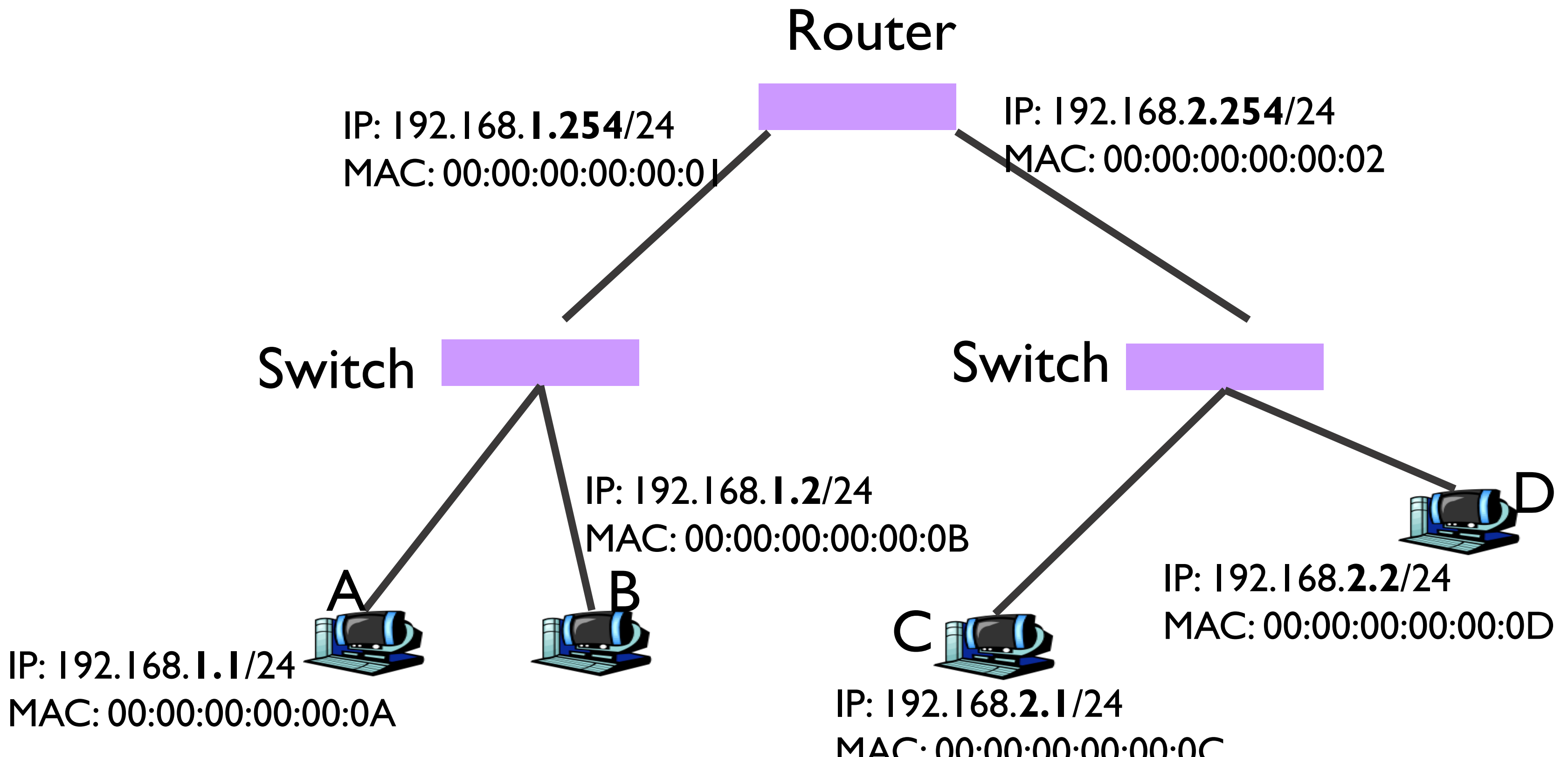
DST IP: **192.168.2.1**



Scenario 2: A □ C. In other words, 192.168.1.1 □ 192.168.2.1

Step 5: Router sends ARP: What is the MAC of 2.1

Step 6: 2.1 replies: My MAC is 0C



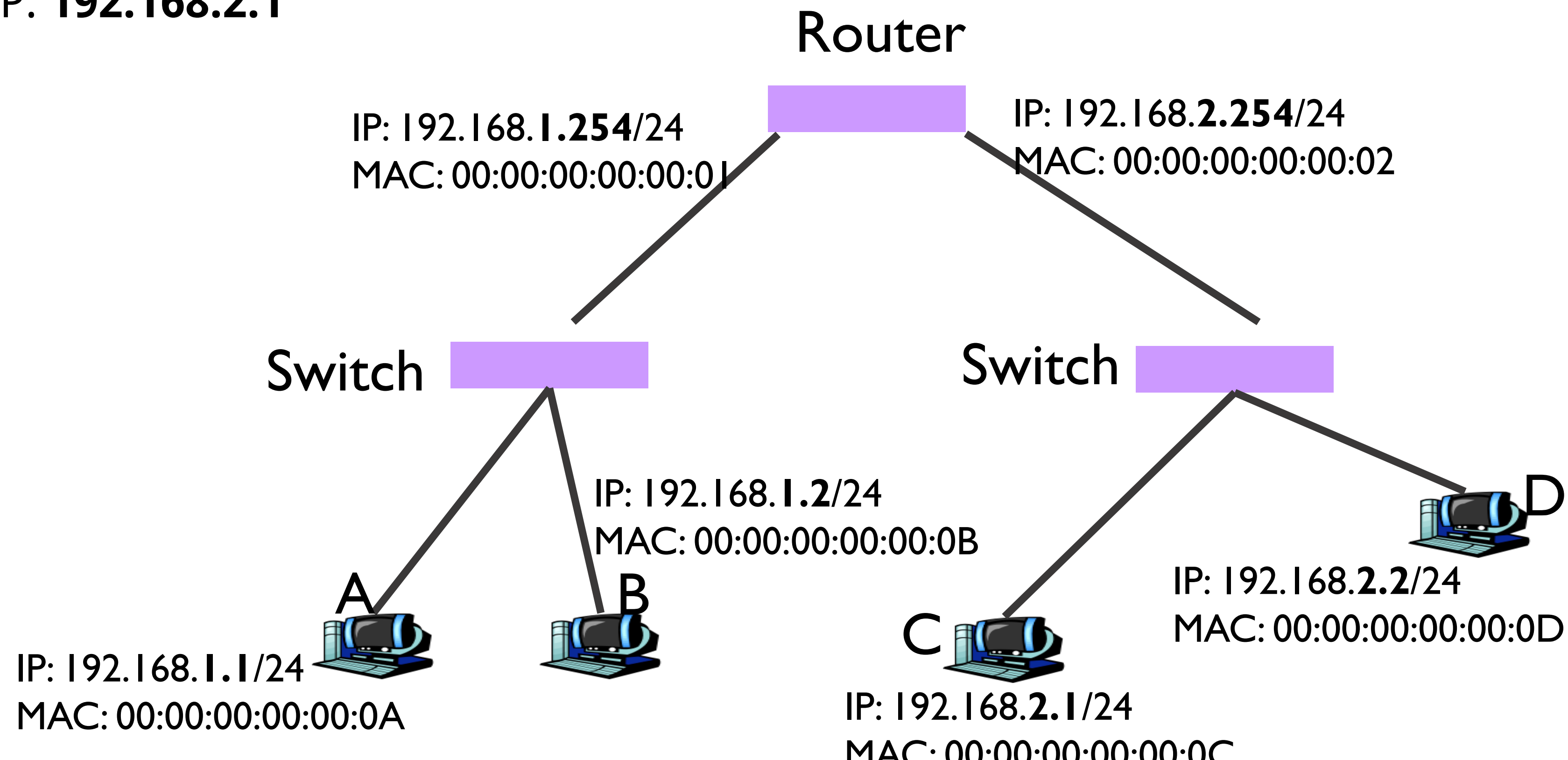
Scenario 2: A C. In other words, 192.168.1.1 192.168.2.1

Step 6: Router sends packet

SRC MAC: 02, DST MAC: **0C**

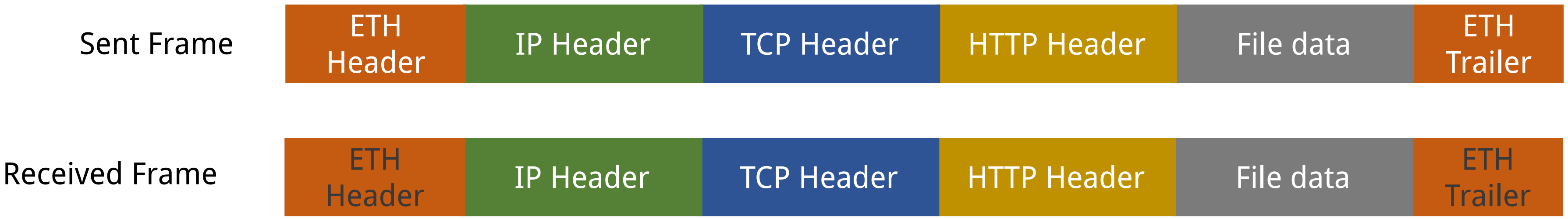
SRC IP: 192.168.1.1

DST IP: **192.168.2.1**

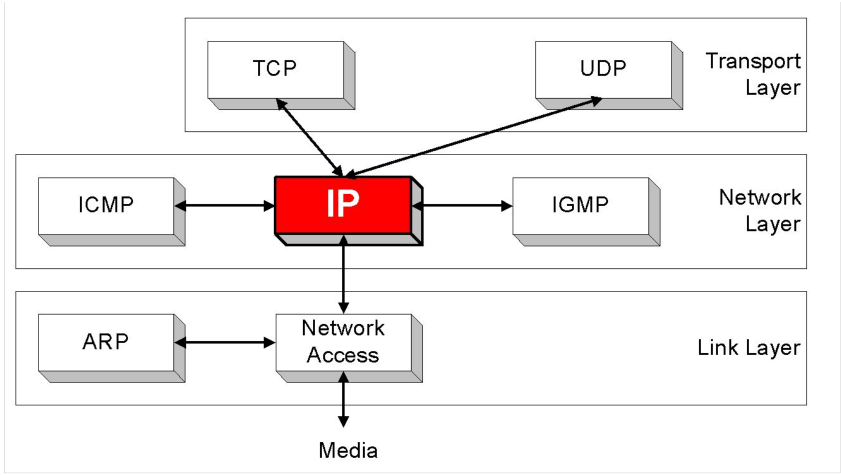


Takeaway

- IP Packet **crossed** the network boundary, but
- Data-link **frames do not**



Network Layer Protocols

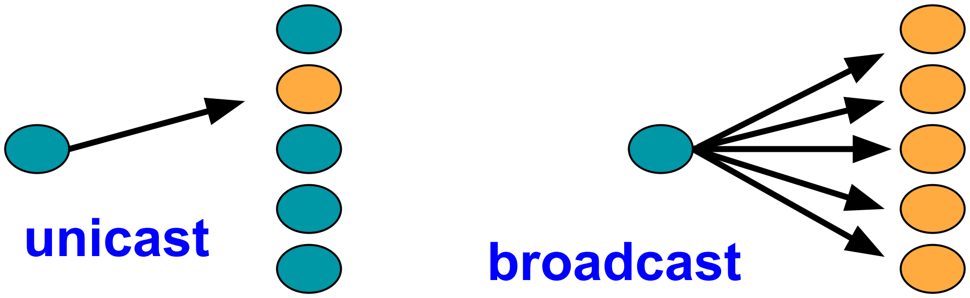


- IP
  - IP is the waist of the hourglass of the Internet protocol architecture. Multiple higher-layer protocols. Multiple lower-layer protocols. Only one protocol at the network layer for transmission.
- Internet Control Message Protocol
  - it is used by network devices, like routers, to send error messages (e.g., a requested service is not available or a host or router could not be reached)

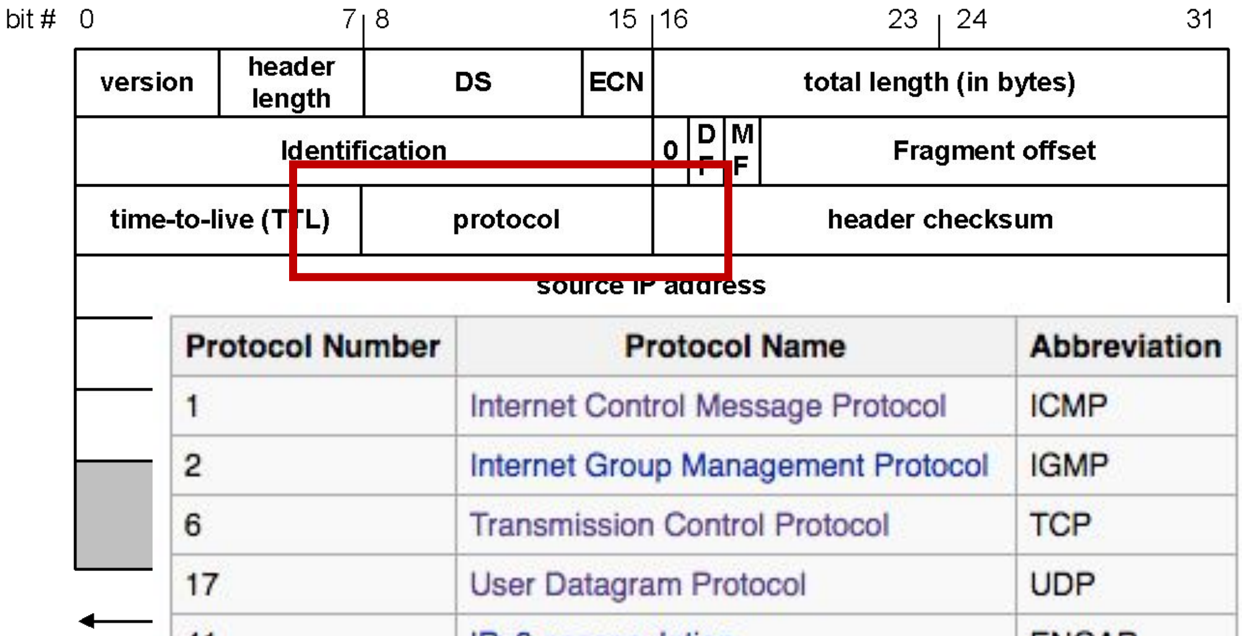
IP Service

IP supports the following services:

- one-to-one (unicast)
  - Source 192.168.0.2/24 to Destination 192.168.0.3/24
- one-to-all (broadcast)
  - Source 192.168.0.2/24 to Destination 192.168.0.255/24

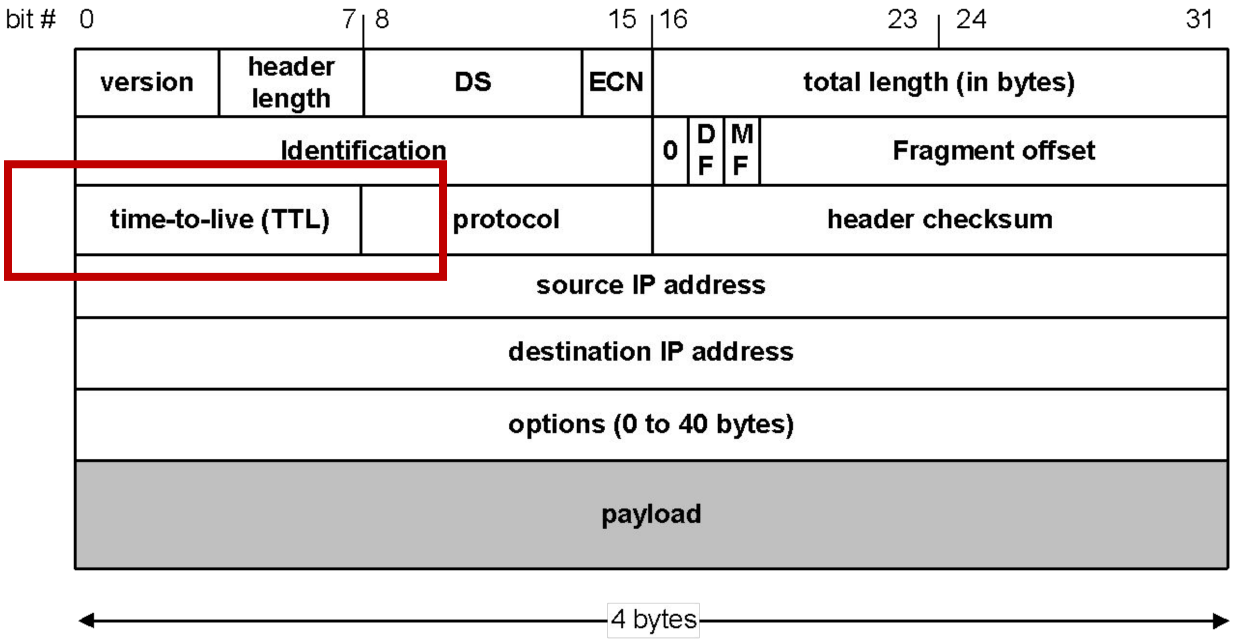


IP Datagram Format



Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

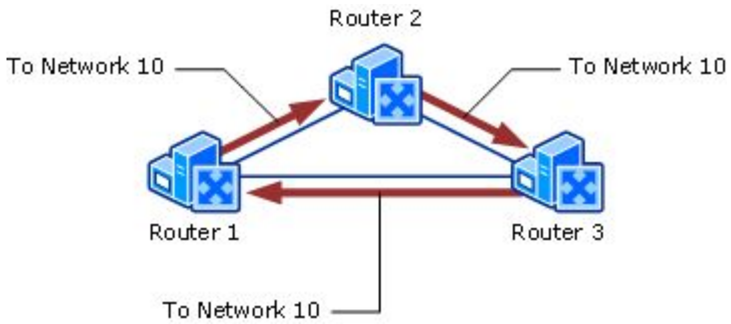
IP Datagram Format



IP Datagram Format

Time To Live (TTL) (1 byte):

- Role of TTL field: Ensure that packet is eventually dropped

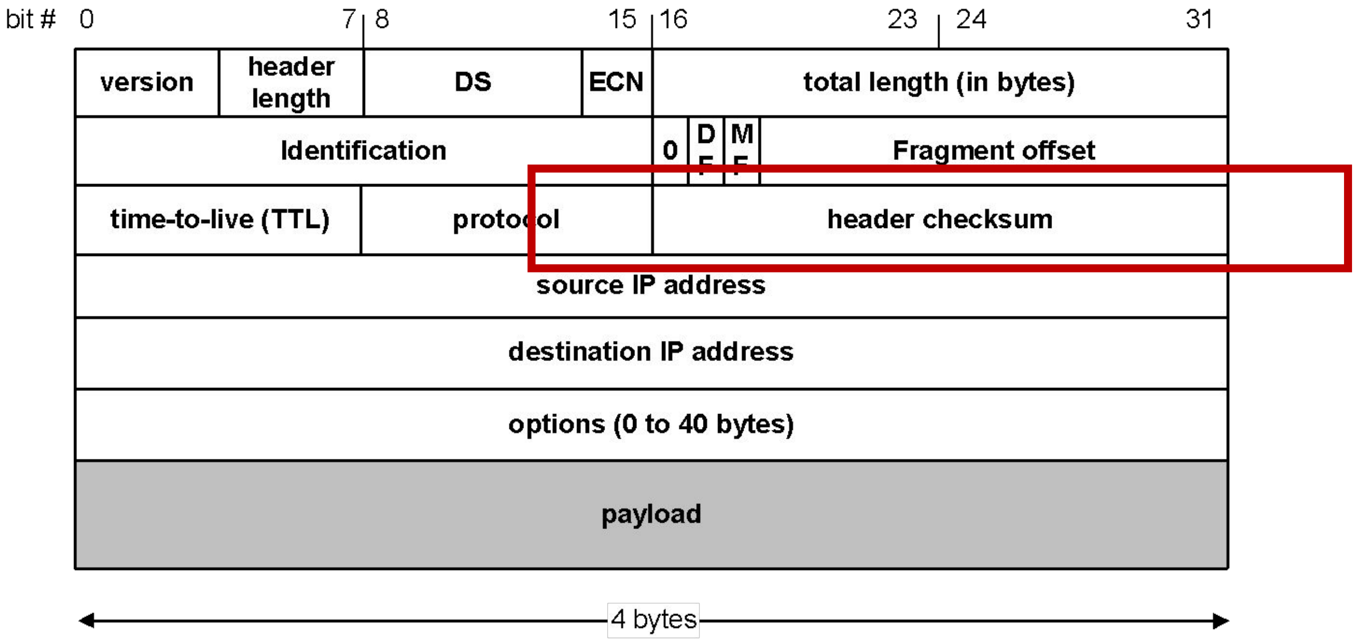


- Specifies longest paths before datagram is dropped

When a routing loop occurs

- Sender sets the value (e.g., 64)
- Each router decrements the value by 1 before sending
- When the value reaches 0, the datagram is dropped

IP Datagram Format



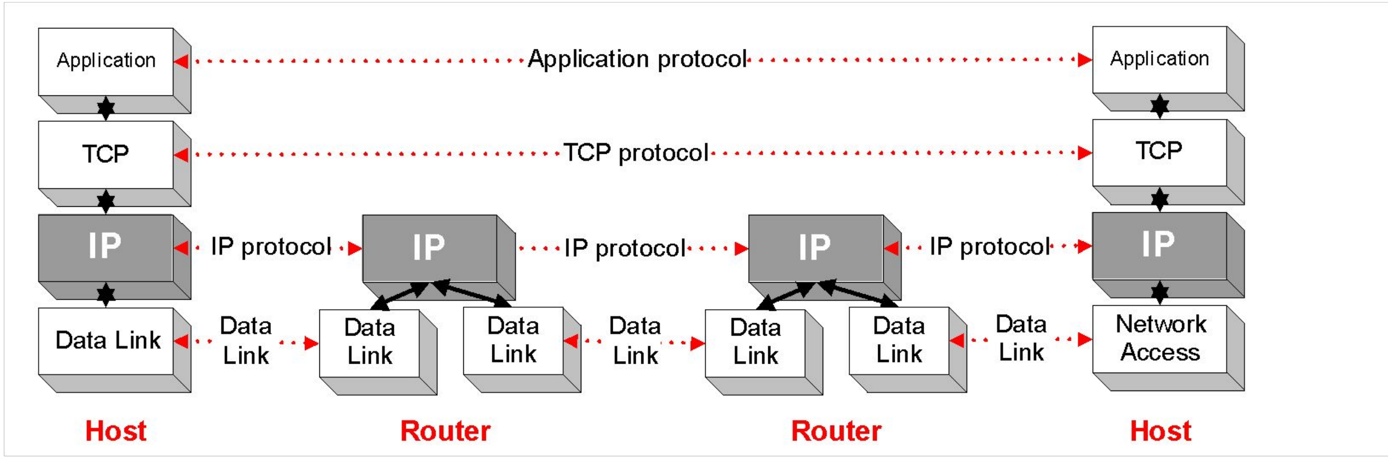
IP Datagram Format

- The 16-bit checksum field is used for error-checking of the header.
- When a packet arrives at a router, the router calculates the checksum of the header and compares it to the checksum field. If the values do not match, the router discards the packet.

- Is the checksum field designed to maintain the security objective Integrity?
  - No. It can not detect intentional modification.
  - It is used for data corruption introduced in transmission

IP Datagram

IP is the highest layer protocol which is implemented at both routers and hosts



Internet Protocol

IP provides an unreliable and connectionless service:

Connectionless:

- Each IP packet ("datagram") is handled independently.
- IP is not aware that packets between hosts may be sent in a logical sequence. Packets may be delivered out-of-sequence

Internet Protocol

IP provide provides an unreliable and connectionless service:

Unreliable:

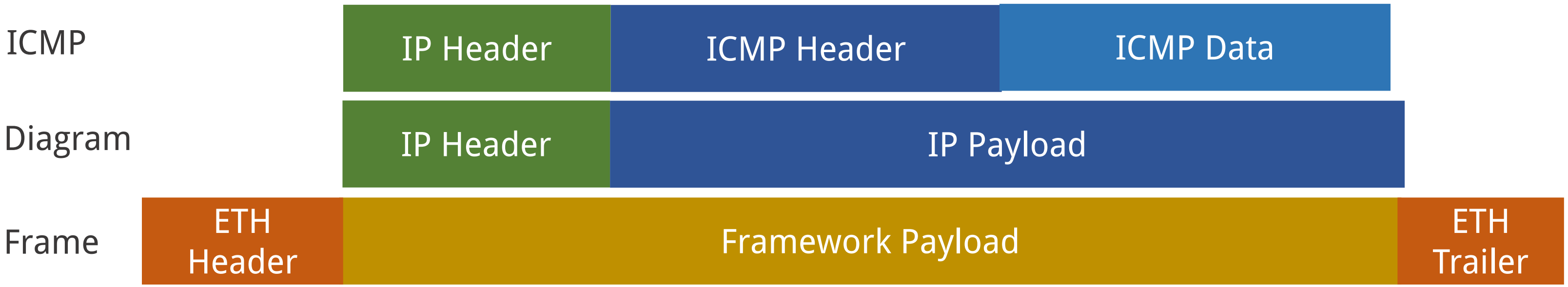
- IP does not make an attempt to recover lost packets.
- It has no built-in processes to ensure that data is delivered in the event that problems exist with network communication.
- If an intermediary device such as a router fails, or if a destination device is disconnected from the network, data cannot be delivered.

Internet Control Message Protocol (ICMP)

- ICMP is an error reporting protocol for IP
  - When datagram delivery errors occur, ICMP is used to report these errors back to the source of the datagram.
  - ICMP does not correct the encountered network problem; it merely reports the problem.
- ICMP reports on the status of the delivered packet only to the source device
- The ICMP software stack executes on all IP end system computers and all IP intermediate systems (i.e routers).

Note that: ICMP does not overcome the unreliability issues in IP. Reliability must be provided by upper layer protocols (TCP) if it is needed.

Internet Control Message Protocol (ICMP)



- ICMP messages are encapsulated into datagrams in the same way any other data is delivered using IP.
  - This creates a scenario where error reports could generate more error reports, causing increased congestion on an already ailing network.
  - For this reason, errors created by ICMP messages do not generate their own ICMP messages.
- It is thus possible to have a datagram delivery error that is never reported back to the sender of the data.

Internet Control Message Protocol (ICMP)

	Bit 0-7	Bit 8-15	Bit 16-23	Bit 24-31
IP Header	Version	Type of Service	Length	
	Identification		Flags & Offset	
	Time to Live	Protocol	Checksum	
	Source IP Address			
	Destination IP Address			
ICMP Payload	Type of Message	Code	Checksum	
	Identifier		Sequence Number	
	Data			

- The type field indicates the type of ICMP message being sent.
- The code field includes further information specific to the message type.

Failed to send an IP packet

Scenario:

Host A sends an IP packet to a destination Host B identified by an IP address. Instead of receiving IP packet response, it could receive an ICMP Type 3 message.

Type	Message Type	Code	Description
3	Destination Unreachable	0	Packet could not be delivered. Destination network unreachable
3	Destination Unreachable	1	Packet could not be delivered. Destination host unreachable.

Questions:

Who will send out Type-3 Code-1 ICMP message?

Who will send out Type-3 Code-0 ICMP message?

PING

Scenario:

Host A wants to check if Host B is reachable. Host A sends out a Type-8 Code-0 ICMP message. If Host B receives this message, it can reply a Type-0 Code-0 ICMP message.

Type	Message Type	Code	Description
8	Echo Request	0	Ask a machine if it is alive
0	Echo Reply	0	Yes, I am alive
13	Timestamp Request	0	Same as Echo request, but with timestamp
14	Timestamp Reply	0	Same as Echo reply, but with timestamp

PING

Most PING utilities send a series of several echo requests to the target in order to obtain an *average response time.*

```
→  paper-CortexM-Remote-Attestation git:(main) ping www.buffalo.edu
PING www.buffalo.edu(g2600-141b-e800-003b-0000-0000-17ce-7989.deploy.static.akamaitechnologies.com (2600:
141b:e800:3b::17ce:7989)) 56 data bytes
64 bytes from g2600-141b-e800-003b-0000-0000-17ce-7989.deploy.static.akamaitechnologies.com (2600:141b:e8
00:3b::17ce:7989): icmp_seq=1 ttl=53 time=35.7 ms
64 bytes from g2600-141b-e800-003b-0000-0000-17ce-7989.deploy.static.akamaitechnologies.com (2600:141b:e8
00:3b::17ce:7989): icmp_seq=2 ttl=53 time=44.8 ms
64 bytes from g2600-141b-e800-003b-0000-0000-17ce-7989.deploy.static.akamaitechnologies.com (2600:141b:e8
00:3b::17ce:7989): icmp_seq=3 ttl=53 time=37.5 ms
64 bytes from g2600-141b-e800-003b-0000-0000-17ce-7989.deploy.static.akamaitechnologies.com (2600:141b:e8
00:3b::17ce:7989): icmp_seq=4 ttl=53 time=38.8 ms
64 bytes from g2600-141b-e800-003b-0000-0000-17ce-7989.deploy.static.akamaitechnologies.com (2600:141b:e8
00:3b::17ce:7989): icmp_seq=5 ttl=53 time=35.7 ms
^C
--- www.buffalo.edu ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 35.736/38.502/44.807/3.351 ms
```

traceroute

- traces a *probable* path a packet takes between itself and a destination.

- *Probable*, because IP is a connectionless protocol, and different packets may take different paths between the same source and destination networks, although this is not usually the case.

traceroute

```
➜  paper-CortexM-Remote-Attestation git:(main) traceroute www.buffalo.edu
traceroute to www.buffalo.edu (23.219.82.225), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  2.241 ms  3.231 ms  3.214 ms
 2  142-254-216-225.inf.spectrum.com (142.254.216.225)  12.313 ms  18.878 ms  18.863 ms
 3  lag-63.lncsnycd02h.netops.charter.com (24.58.216.69)  34.417 ms  34.401 ms  34.386 ms
 4  lag-37.lncsnycd02r.netops.charter.com (24.58.38.28)  18.794 ms  18.780 ms  18.764 ms
 5  lag-29.rcr01rochnyei.netops.charter.com (24.58.32.62)  96.374 ms  96.359 ms  96.343 ms
 6  lag-15.chcgildt87w-bcr00.netops.charter.com (66.109.6.72)  33.195 ms lag-415.chcgildt87w-bcr00.netops
.charter.com (66.109.6.2)  30.449 ms lag-15.chcgildt87w-bcr00.netops.charter.com (66.109.6.72)  33.283 ms
 7  lag-11.nycmny837aw-bcr00.netops.charter.com (66.109.6.24)  40.225 ms lag-21.nycmny837aw-bcr00.netops.
charter.com (66.109.6.94)  59.287 ms  39.454 ms
 8  lag-0.pr2.nyc20.netops.charter.com (66.109.5.119)  39.393 ms  49.294 ms  39.362 ms
 9  66.75.151.227 (66.75.151.227)  84.745 ms 24.30.200.117 (24.30.200.117)  39.340 ms 24.30.200.39 (24.30
.200.39)  39.310 ms
10  ae2.coresite-ewr2.netarch.akamai.com (23.203.156.173)  84.700 ms a23-219-82-225.deploy.static.akamait
echnologies.com (23.219.82.225)  39.281 ms ae2.coresite-ewr2.netarch.akamai.com (23.203.156.173)  98.789
ms
```

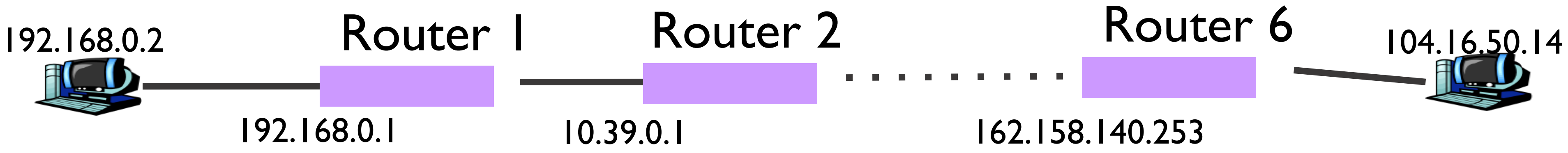
Traceroute - How it works

Type	Message Type	Code	Description
8	Echo Request	0	Ask a machine if it is alive
11	Time Exceeded	0	TTL expired in transit

Traceroute - How it works

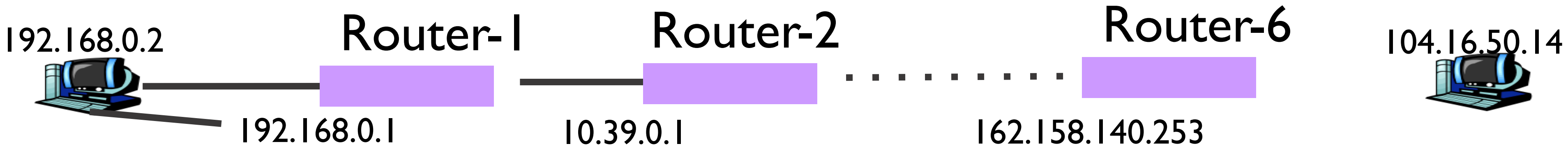
Fooling the routers & host!

- Traceroute uses ICMP Echo Requests
- Traceroute sets the TTL (Time To Live) field in the IP Header, initially to “1”
- When a router receives an IP Packet, it decrements the TTL by 1.
- If the TTL is 0, it will not forward the IP Packet, and send back to the source an ICMP “time exceeded” message.
  ICMP Message: Type = 11, Code = 0



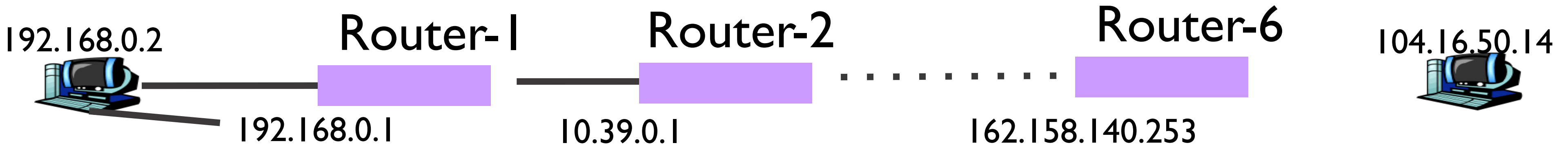
Traceroute - How it works

- After the traceroute is received by the Router-1, it decrements the TTL by 1 to 0.
- Noticing the TTL is 0, it sends back a ICMP Time Exceeded message back to the source, using its IP address for the source IP address.
- Router B's IP header includes its own IP address (source IP) and the sending host's IP address (dest. IP).



Traceroute - How it works

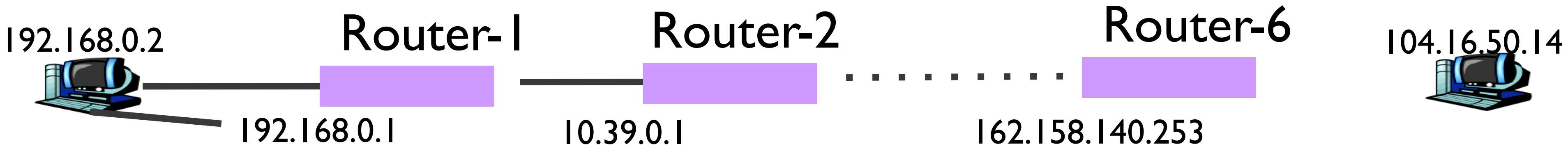
- The traceroute program increments the TTL by 1 (now 2) and resends the ICMP Echo Request packet.
- This time Router-1 decrements the TTL by 1 and it is NOT 0. (It is 1.) So it looks up the destination IP address in its routing table and forwards it on to the next router.



Traceroute - How it works

- Router-2 however decrements the TTL by 1 and it is 0. Router-2 notices the TTL is 0 and sends back the ICMP Time Exceeded message back to the source.

- The sending host will use the source IP address of this ICMP Time Exceeded message to display at the second hop.



Recon & Scanning

- Attackers can use ICMP as part of a reconnaissance process to learn about active network addresses

- These reconnaissance processes often precede a network break-in

- When hackers decide to infiltrate a network, they typically start with a list of the IP hosts on the network (unless the target is a single known system)

Ping of Death

- Worked in 1990s
- Attackers send a malformed or otherwise malicious ping to a computer
- Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented in RFC 791
- A software vulnerability

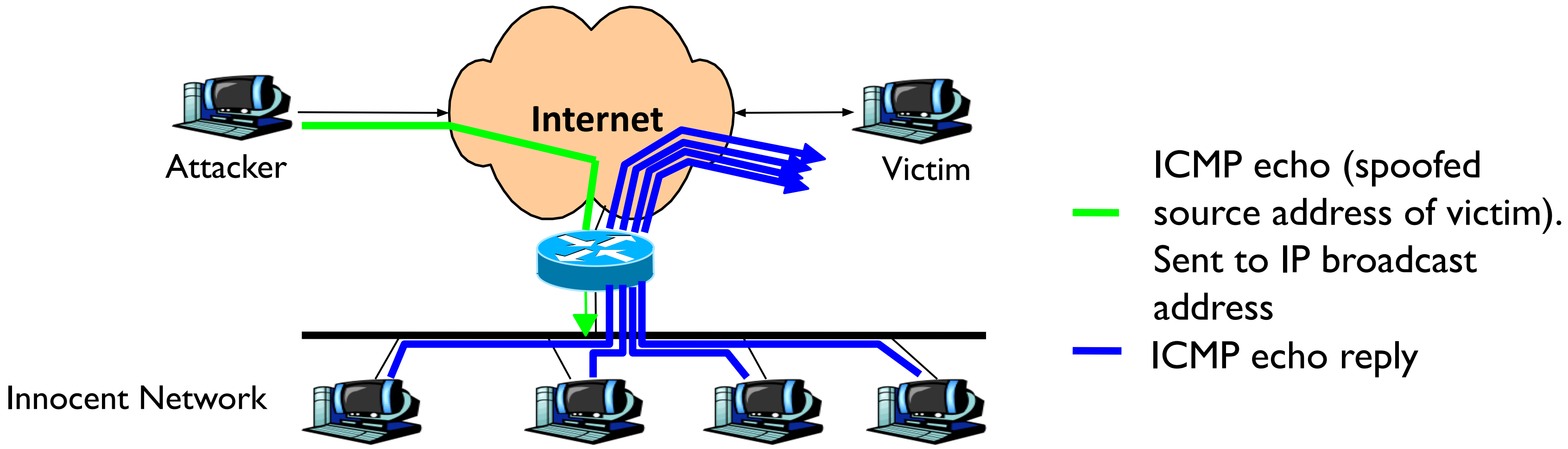
Ping Flood

- Worked in 1990s

- A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets.
- Using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies.
- It is most successful if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem).

Smurf Attack

- In this attack, spoofed IP packets containing ICMP Echo-Request with a source address equal to that of the attacked system and a broadcast destination address are sent to the intermediate network.
- Sending a ICMP Echo Request to a broadcast address triggers all hosts included in the network to respond with an ICMP response packet, thus creating a large mass of packets which are routed to the victim's spoofed address.
- It is a distributed denial-of-service attack



Next Class

- IP and its attacks