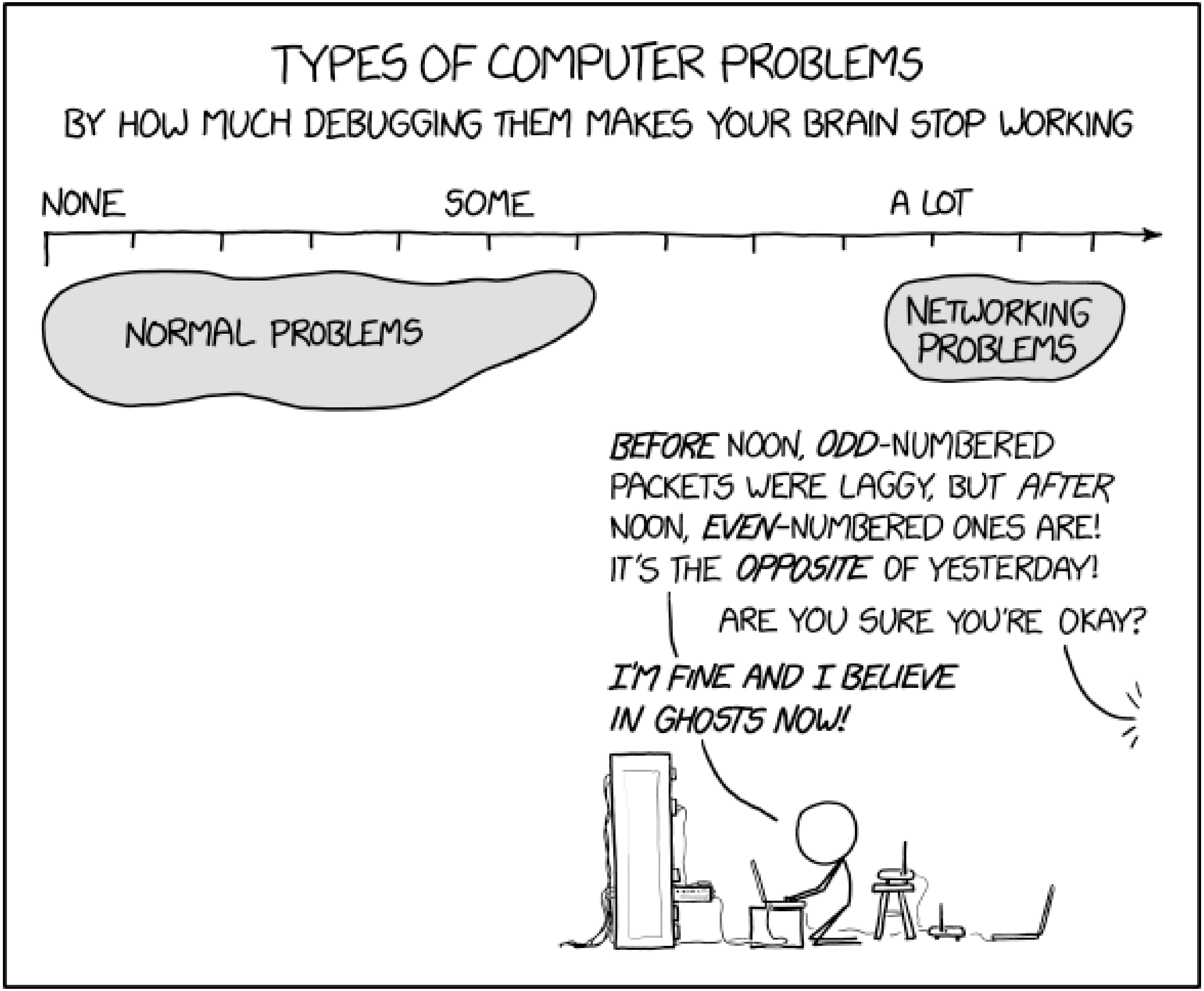

TYPES OF COMPUTER PROBLEMS
BY HOW MUCH DEBUGGING THEM MAKES YOUR BRAIN STOP WORKING
NONE
SOME
A LOT
NORMAL PROBLEMS
NETWORKING PROBLEMS
BEFORE NOON, *ODD*-NUMBERED PACKETS WERE LAGGY, BUT *AFTER* NOON, *EVEN*-NUMBERED ONES ARE! IT'S THE *OPPOSITE* OF YESTERDAY!
ARE YOU SURE YOU'RE OKAY?
I'M FINE AND I BELIEVE IN GHOSTS NOW!

https://xkcd.com/2259

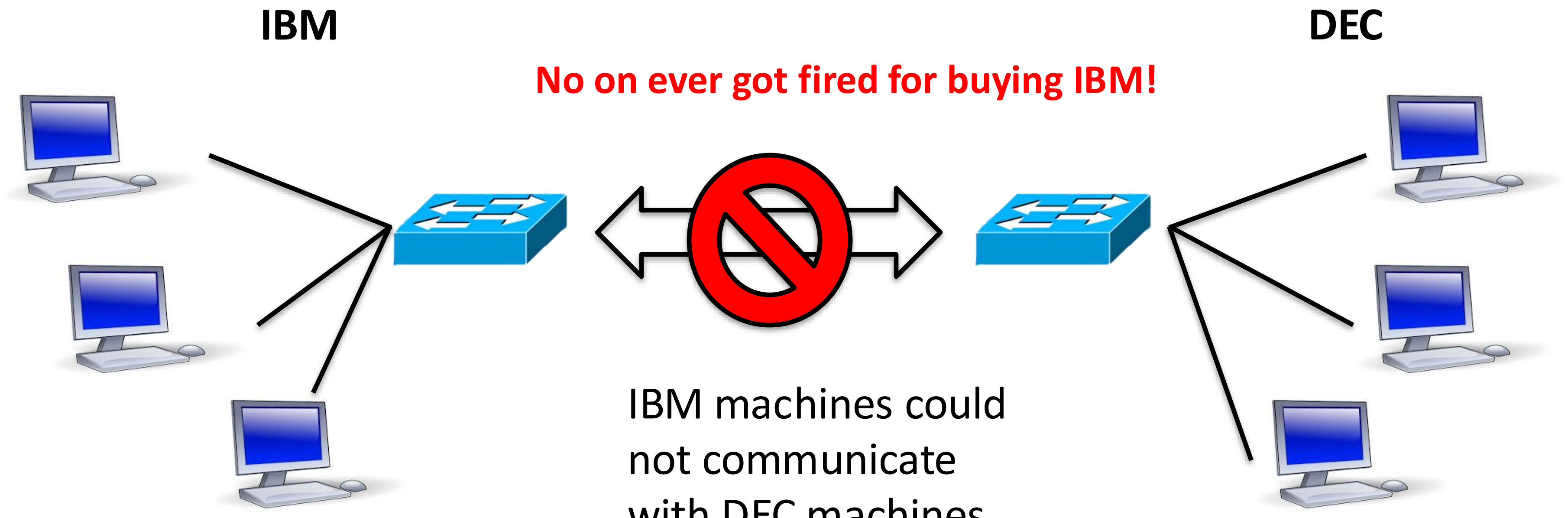
CS 60:
Computer Networks

Network layers

Agenda

1. Network layer overview
2. Ping and ARP
3. DHCP
4. Exercises

In the old days, networking protocols were proprietary to each manufacturer



No on ever got fired for buying IBM!

IBM machines could not communicate with DEC machines

IBM had protocols for communicating with other IBM machines

Example: SNA

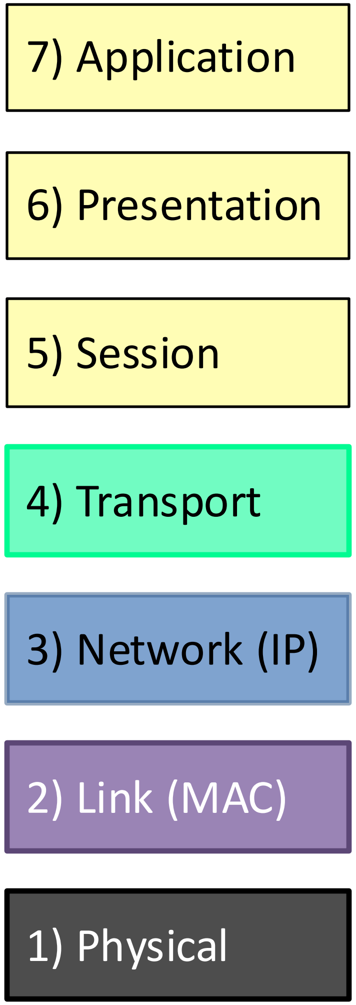
Incompatibility problems!

DEC had protocols for communicating with other DEC machines

Example: DECnet

Two frameworks were developed to remedy incompatibility problems

Open Systems Interconnection (OSI)



7) Application

6) Presentation

5) Session

4) Transport

3) Network (IP)

2) Link (MAC)

1) Physical

https://www.ibm.com/think/topics/osi-model

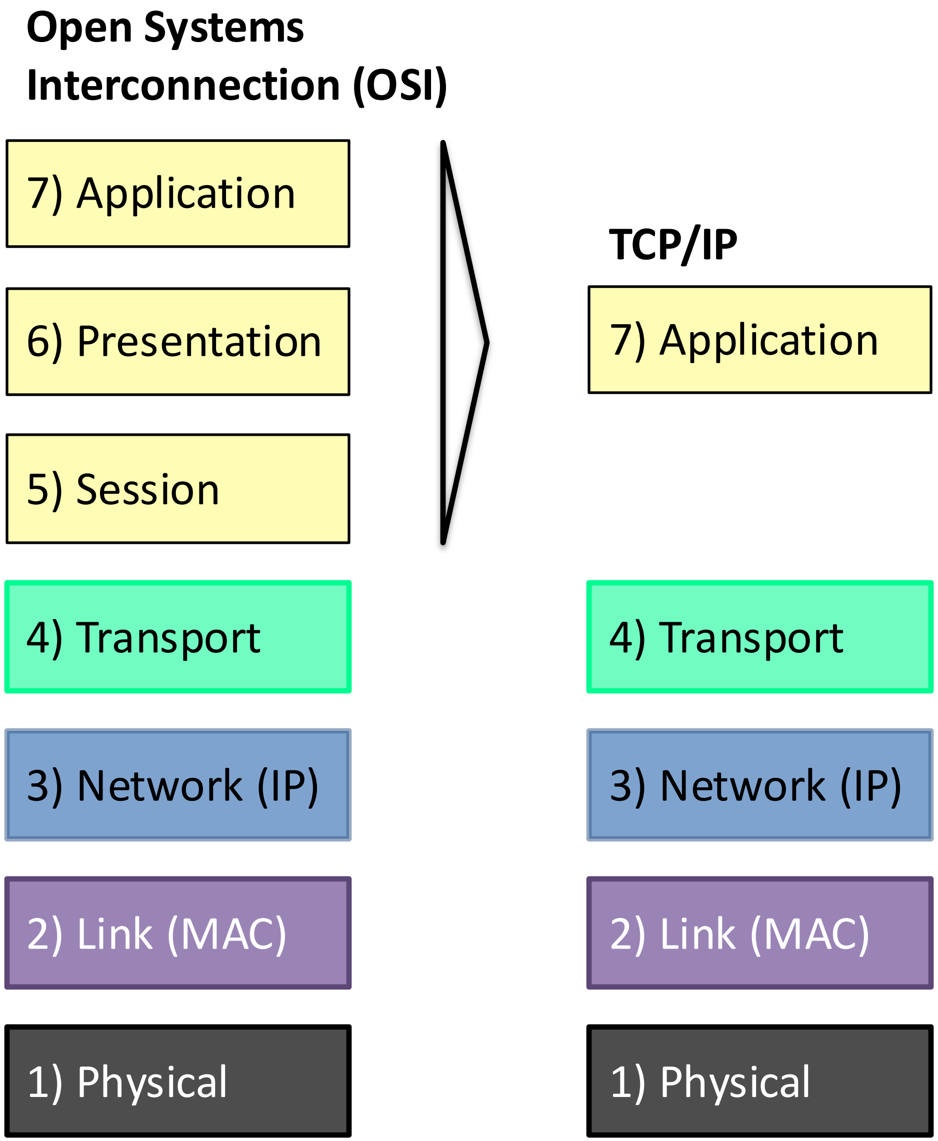
Goal: define each layer of network from the physical up to applications to standardize how communications work

International Organization for Standardization (ISO) published OSI model in 1984

Upper layers still function the same, even if lower layers change

For example: Link layer works the same regardless if using RF (Wi-Fi) or electrical (Ethernet cables)

Two frameworks were developed to remedy incompatibility problems



Open Systems Interconnection (OSI)

7) Application

6) Presentation

5) Session

4) Transport

3) Network (IP)

2) Link (MAC)

1) Physical

TCP/IP

7) Application

4) Transport

3) Network (IP)

2) Link (MAC)

1) Physical

https://www.ibm.com/think/topics/osi-model

TCP/IP Model

Five layers by combining Application layers (sometimes Physical and Link layers combined to four-layer model)

We still call Application layer, Layer 7!

TCP/IP model sometimes called:

- Network model
- Internet model
- Protocol stack
- Reference model

Maddingly, I may use all these 5-layer terms!

The OSI model's primary value lies in its educational utility and its role as a conceptual framework for designing new protocols to ensure compatibility

“TCP/IP model's practical focus and real-world applicability have made it the backbone of modern networking”

Physical layer transports bits

Conceptual network layers

7) Application

4) Transport

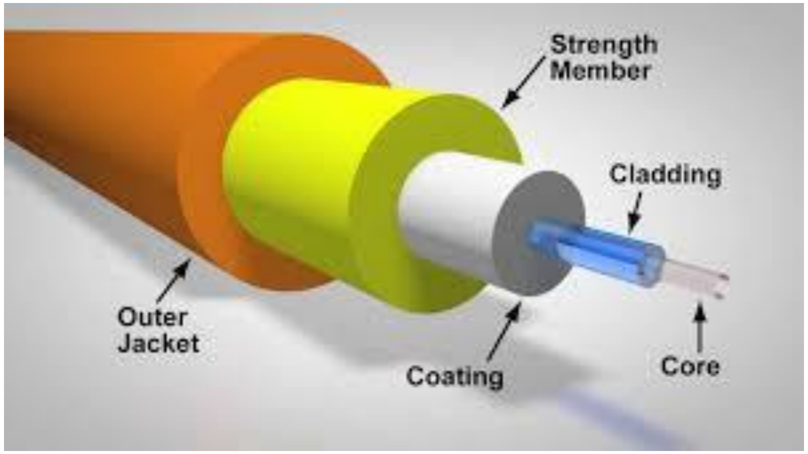
3) Network (IP)

2) Link (MAC)

1) Physical

DO NOT BEND FIBER CABLES They will break!

Fiber optic cable



Glass or plastic core channels light (from lasers or LEDs)

At a given time: light pulse = 1 , no light pulse = 0

Two types

- Single mode – one light frequency, small core (~9 microns), long-range (~40 km), useful for long haul
- Multimode – multiple freqs, large core (~60 microns), short range (~100m), useful in building/campus
- Theoretical speed in petabytes (practical about 10 Gb/sec)

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

Physical layer transports bits

Conceptual network layers

7) Application

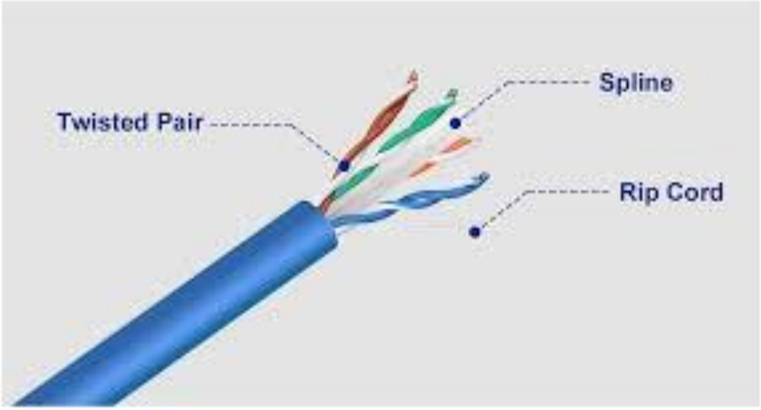
4) Transport

3) Network (IP)

2) Link (MAC)

1) Physical

Ethernet cable



Twisted pairs of copper wire
Unshielded twisted pair (UTP) or shielded twisted pair (STP)
Category 5e (1 Gb/sec) to Category 8 (40 Gb/sec)
Goes about 100m
Two kinds:

- Straight through (computer to switch/router)
- Crossover (computer to computer)

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

Physical layer transports bits

Conceptual network layers

7) Application

4) Transport

3) Network (IP)

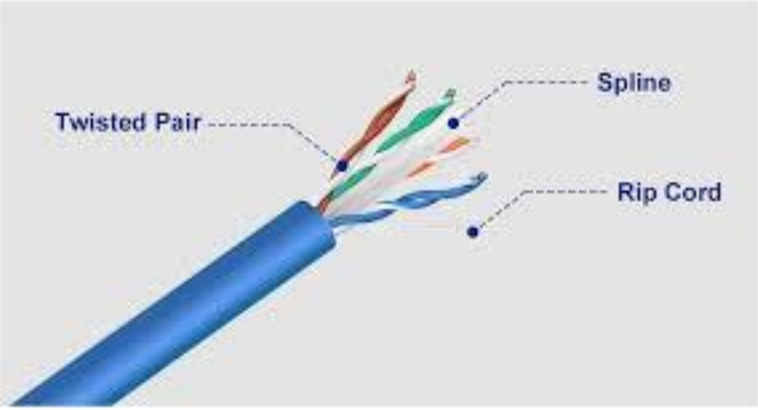
2) Link (MAC)

1) Physical

How would you tap an ethernet cable?

- **Use a hub!**
- **But you'll need to cut the wire**
- **Let's do that**

Ethernet cable



Twisted pairs of copper wire

Unshielded twisted pair (UTP) or shielded twisted pair (STP)

Category 5e (1 Gb/sec) to Category 8 (40 Gb/sec)

Goes about 100m (or may run into collisions)

Two kinds:

- Straight through (computer to switch/router)
- Crossover (computer to computer)

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Physical layer transports bits

Conceptual network layers

7) Application

4) Transport

3) Network (IP)

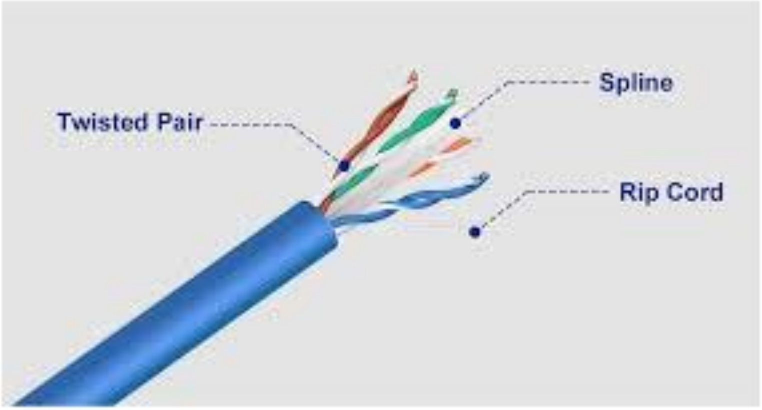
2) Link (MAC)

1) Physical

How would you tap an ethernet cable?

- **Use a hub!**
- **But you'll need to cut the wire**
- **Let's do that**

Ethernet cable



Twisted pairs of copper wire

Unshielded twisted pair (UTP) or shielded tw

Category 5e (1 Gb/sec) to Category 8 (40 Gb/

Goes about 100m (or may run into collisions)

Two kinds:

- Straight through (computer to switch/rou
- Crossover (computer to computer)

T568A:
1-White/Green
2-Green
3-White/Orange
4-Blue
5-White/Blue
6-Orange
7-White/Brown
8-Brown

T568B:
1-White/Orange
2-Orange
3-White/Green
4-Blue
5-White/Blue
6-Green
7-White/Brown
8-Brown

Straight (B to B)
Crossover(A to B)

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

Physical layer transports bits

Conceptual network layers

7) Application

4) Transport

3) Network (IP)

2) Link (MAC)

1) Physical

How would you tap an ethernet cable?

- **Use a hub!**
- **But you'll need to cut the wire**
- **Let's do that**
- **Could also use a Throwing Star instead (good if you don't have power available for the hub)**

Ethernet cable

Twisted pairs of copper wire

Unshielded twisted pair (UTP) or shielded tw

Category 5e (1 Gb/sec) to Category 8 (40 Gb/

Goes about 100m (or may run into collisions)

Two kinds:

- Straight through (computer to switch/rou
- Crossover (computer to computer)

T568A:
1-White/Green
2-Green
3-White/Orange
4-Blue
5-White/Blue
6-Orange
7-White/Brown
8-Brown

T568B:
1-White/Orange
2-Orange
3-White/Green
4-Blue
5-White/Blue
6-Green
7-White/Brown
8-Brown

Straight (A to A)
Crossover(A to B)

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://greatscottgadgets.com/throwingstar/

Physical layer transports bits

Conceptual network layers

7) Application

4) Transport

3) Network (IP)

2) Link (MAC)

1) Physical

Regardless of how physical layer works, received bits are decoded and sent to Layer 2 (Link Layer)

Radio Frequency (RF)

Sends data over the air using radio frequency
Examples: Wi-Fi, Bluetooth, Cellular, Satellite
Transmitter sends at known phase and amplitude
Receiver converts RF phase/amplitude into 1 and 0 bits
Wi-Fi ~100m, Bluetooth ~10m
Theoretical max Wi-Fi speed about 9.6 Gb/sec (802.11ax)

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

Each NIC has a unique MAC address burned into NIC’s ROM by the manufacturer, does not (normally) change

7) Application

Wired Network Interface Card

- Common on non-mobile devices such as desktops, IP phones, servers
- Network cable plugs into NIC

Wireless Wi-Fi Interface Card

- Common on mobile devices such as smart phones, tablets, IoT devices
- Connects to Wi-Fi Access Point (which normally acts as a router) via RF

4) Transport

3) Network (IP)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

Does the Link Layer care about how it got the bits from the PHY layer? No!

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

Find your MAC address with **ifconfig** (ifconfig Mac/Linxu, ipconfig Windows)

```
% ifconfig
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 5c:e9:1e:a2:4d:4f
        inet6 fe80::1421:7489:af6b:6a95%en0 prefixlen 64 secured scopeid 0xf
        inet 10.0.0.64 netmask 0xffffff00 broadcast 10.0.0.255
        inet6 2601:19e:8200:80d0:81b:df78:32be:289 prefixlen 64 autoconf secured
        inet6 2601:19e:8200:80d0:1cbd:e651:1f3f:8753 prefixlen 64 autoconf temporary
        inet6 2601:19e:8200:80d0::8ec8 prefixlen 64 dynamic
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

4) Transport

3) Network (IP)

MAC address uniquely identifies each host

Example: two iPhones of same model will have different MACs

2) Link (MAC)

Moves ***frames*** within a local area network (switching)

Each computer identified by a MAC address on its Network Interface Card (NIC)

Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

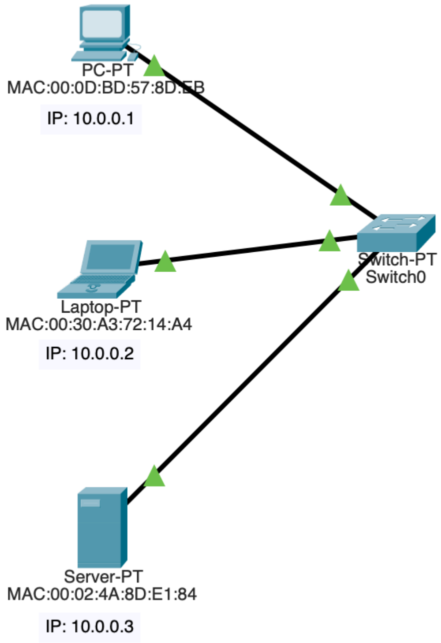
Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

Switches:

- Connect devices in a local area
- Send traffic to devices based on their MAC
- Switch learns the MAC address of a device when it first transmits



4) Transport

3) Network (IP)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

4) Transport

3) Network (IP)

Switches:

- Connect devices in a local area
- Send traffic to devices based on their MAC
- Switch learns the MAC address of a device when it first transmits
- Keep a table of which MAC is plugged into which port
- Switches do not know about higher layers (only Layer 2)

Switch port

Key point: Layer 2 deals with computers in the *same* LAN

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

4) Transport

3) Network (IP)

Moves ***packets*** between local area networks (routing)
Each computer on the Internet identified by an IP address (IP v4 or v6)
Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

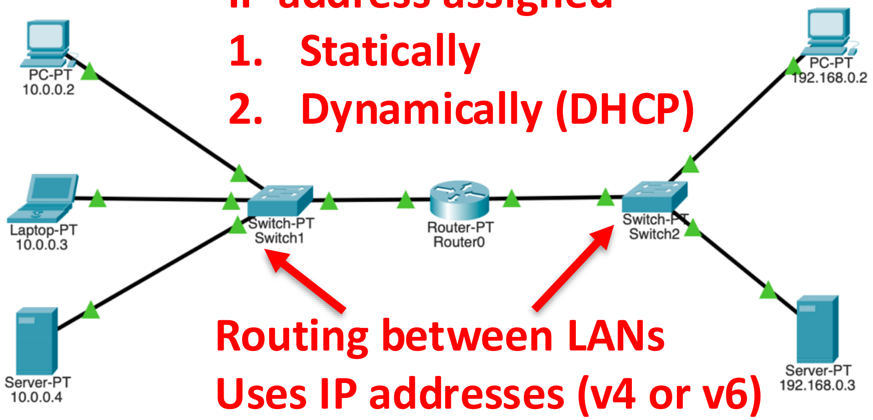
How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers



IP address assigned

1. **Statically**
2. **Dynamically (DHCP)**

Routing between LANs
Uses IP addresses (v4 or v6)
Layer 3 does not know about MACs

7) Application

4) Transport

3) Network (IP)

Moves ***packets*** between local area networks (routing)
Each computer on the Internet identified by an IP address (IP v4 or v6)
Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

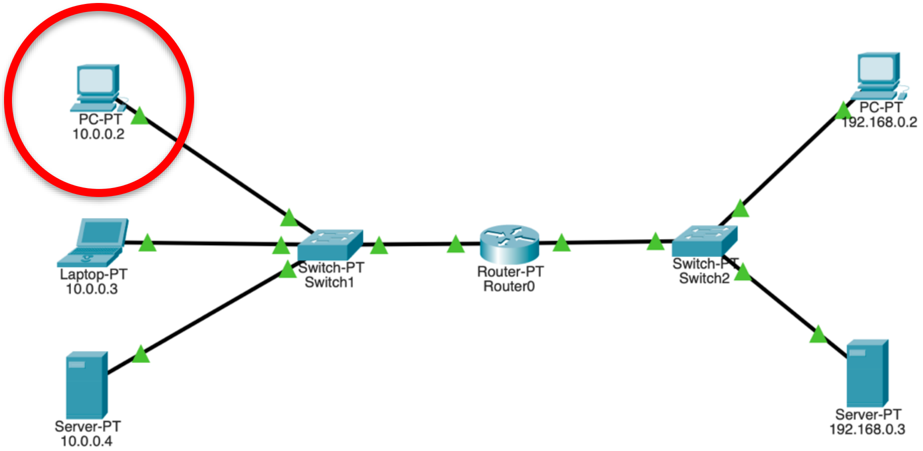
https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

Find a route between LANs from this PC



4) Transport

3) Network (IP)

Moves ***packets*** between local area networks (routing)
Each computer on the Internet identified by an IP address (IP v4 or v6)
Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

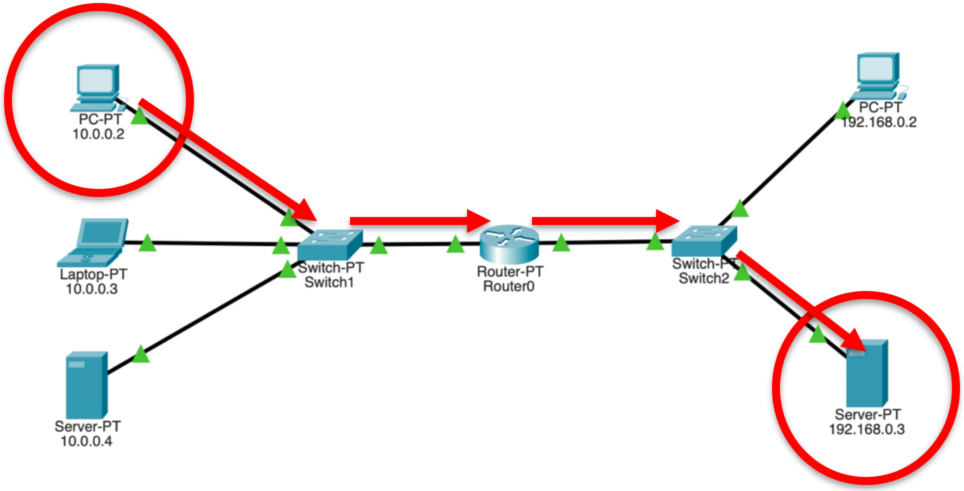
https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

Find a route between LANs from this PC



To this server

4) Transport

3) Network (IP)

Moves ***packets*** between local area networks (routing)
Each computer on the Internet identified by an IP address (IP v4 or v6)
Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

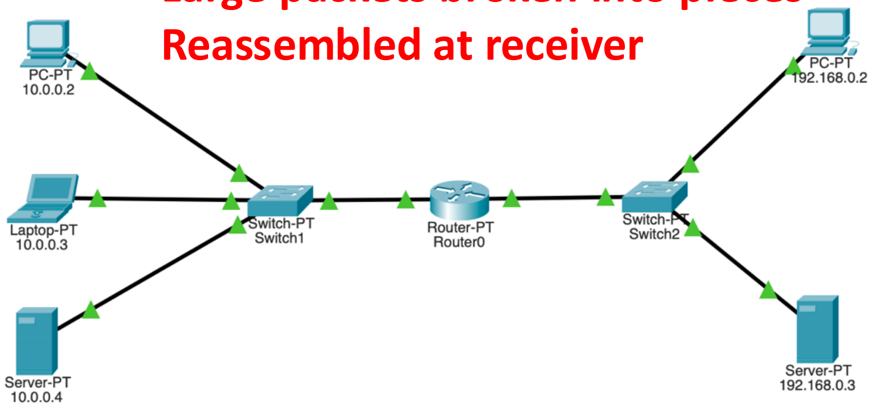
Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

Packet delivery is not guaranteed at Layer 3

Large packets broken into pieces
Reassembled at receiver



4) Transport

Routing finds efficient routes between LANs

3) Network (IP)

Moves ***packets*** between local area networks (routing)
Each computer on the Internet identified by an IP address (IP v4 or v6)
Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

Can you make a reliable channel over an unreliable channel? How?

TCP provides “guaranteed” delivery, UDP does not

Provides port to make sure data gets to right application (layer above)

Port at Layer 4 is a number, not a physical port like Layer 1

4) Transport

Moves ***segments*** *or* ***datagrams***

May provide error control, flow control, application addressing (ports)

Examples: TCP (connection-oriented), UDP (connectionless)

TCP provides sequencing, dropped packet resend, traffic congestion routing

3) Network (IP)

Moves ***packets*** between local area networks (routing)

Each computer on the Internet identified by an IP address (IP v4 or v6)

Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)

Each computer identified by a MAC address on its Network Interface Card (NIC)

Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Link layer connects computers in a Local Area Network (LAN)

Conceptual network layers

7) Application

Interacts with application programs to send ***messages***
Applications assigned a port, multiple instances can run (many browser pages)
Examples: HTTP, SSH, FTP, SMTP, DNS

4) Transport

Moves ***segments (or datagrams)***
May provide error control, flow control, application addressing (ports)
Examples: TCP (connection-oriented), UDP (connectionless)
TCP provides sequencing, dropped packet resend, traffic congestion routing

3) Network (IP)

Moves ***packets*** between local area networks (routing)
Each computer on the Internet identified by an IP address (IP v4 or v6)
Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

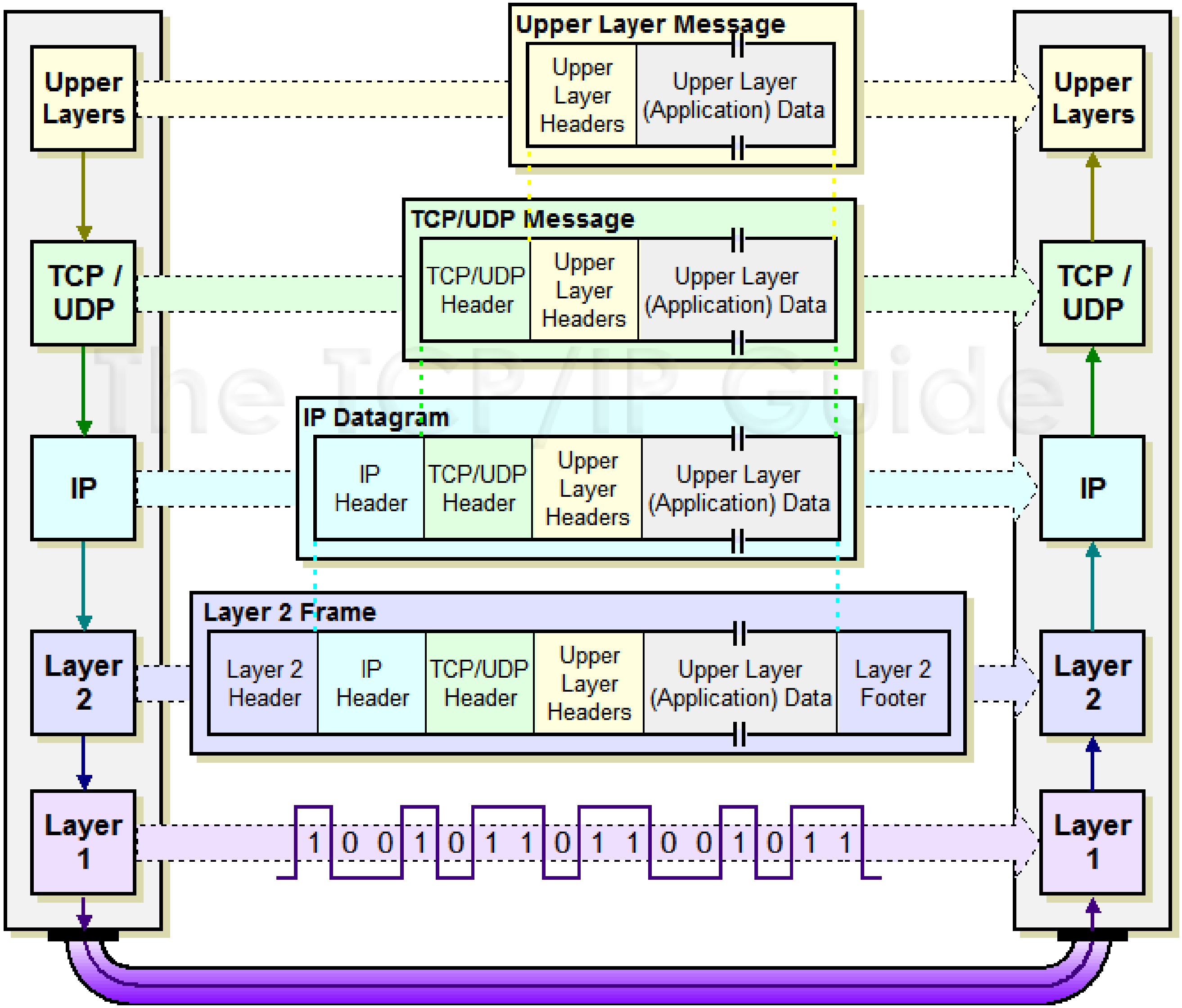
https://www.ibm.com/think/topics/osi-model

Messages travel down the stack from the transmitter and up the stack at the receiver

Transmitter
Wants to send message to receiver

Message starts at top and is encapsulated by each layer down the stack

Each layer adds it own headers



Receiver
Message starts at the physical layer and moves upward

Each layer strips off headers from prior layer

Adapted from http://www.tcpipguide.com/free/t_IPDatagramEncapsulation.htm

Agenda

1. Network layer overview
2. Ping and ARP
3. DHCP
4. Exercises

ICMP: Internet Control Message Protocol

Ping

- ping <IP address>
- Used by hosts and routers to communicate network-level information
  - Error reporting: unreachable host, network, port, protocol
- Ping uses ICMP echo request/reply
  - ICMP messages carried in IP (Layer 3) datagrams
  - Reply returns:
    - Type
    - Code
    - First 8 bytes of IP datagram

ping 8.8.8.8 (Google's DNS server)
Why that IP address?
Easy to remember!

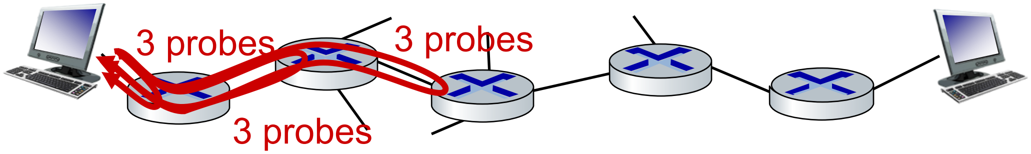
Shows roundtrip time to destination and back

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

You will write your own ping program in Lab 1

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

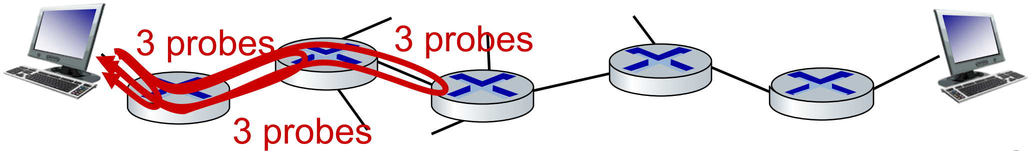
Traceroute and ICMP



- Pings shows if a host is reachable, but does not give the route to the host
- Can you determine the route packets take to the destination?
- Three useful pieces of information:
  1. Each ICMP ping request has a time to live (TTL) = max number of hops
  2. Routers decrement TTL when passing to next router
  3. Routers are *supposed* to return “TTL expired” with router’s name if TTL goes to 0

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Traceroute and ICMP



You will write your own traceroute program in Lab 1

- Source sends sets of UDP segments to destination
  - 1st set has TTL =1, 2nd set has TTL=2, etc.
- Datagram in *n*th set arrives to nth router:
  - Router discards datagram and sends source ICMP message (type 11, code 0 which is TTL expired)
  - ICMP message possibly includes name of router & IP address
- When ICMP message arrives at source: record RTT

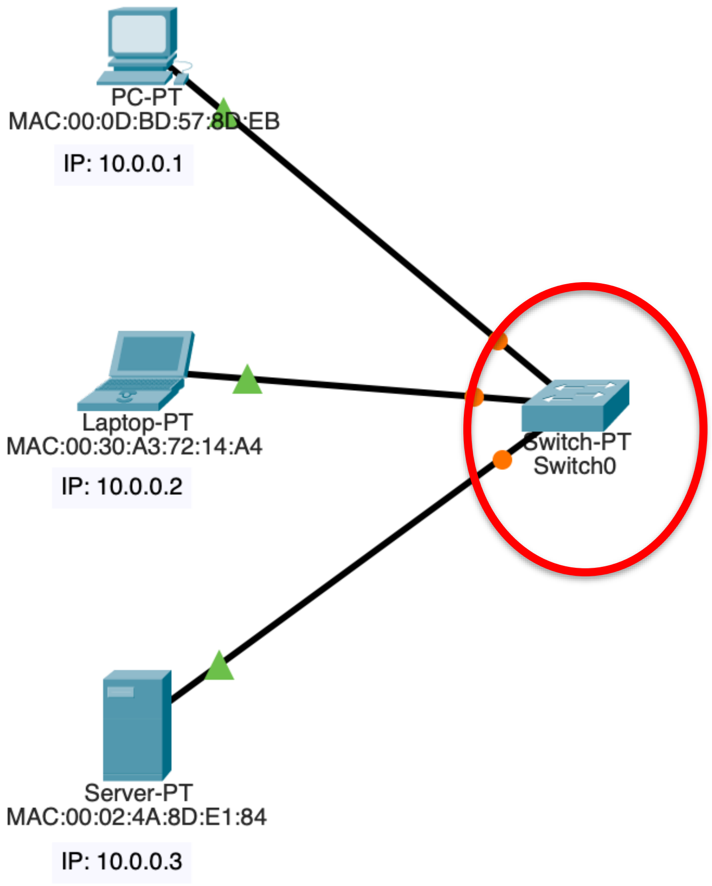
Stopping criteria:

- UDP segment eventually arrives at destination host
- Destination returns ICMP "port unreachable" message (type 3, code 3)
- Source stops sending
- Reach limit (Dartmouth blocks)

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

A small network example shows how layers work together

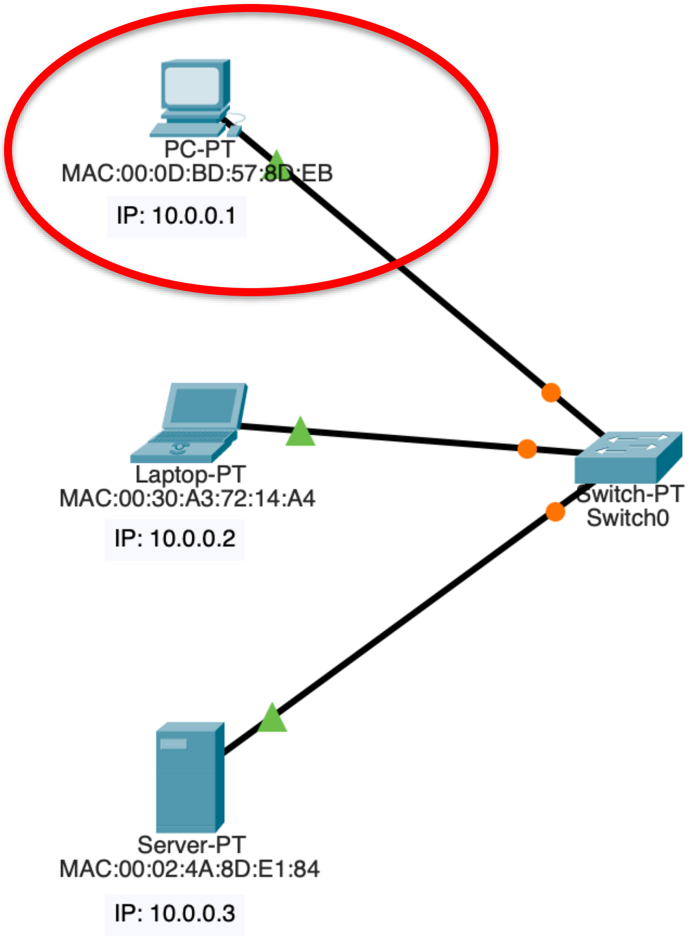
Cisco Packet Tracer



A Switch connects three hosts

A small network example shows how layers work together

Cisco Packet Tracer

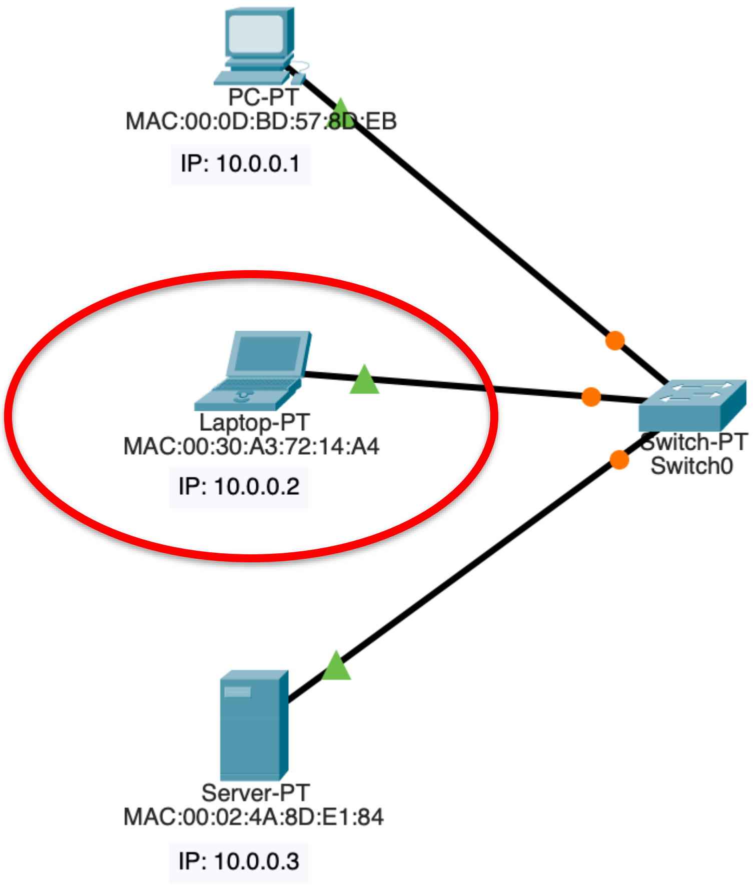


A Switch connects three hosts

- PC

A small network example shows how layers work together

Cisco Packet Tracer

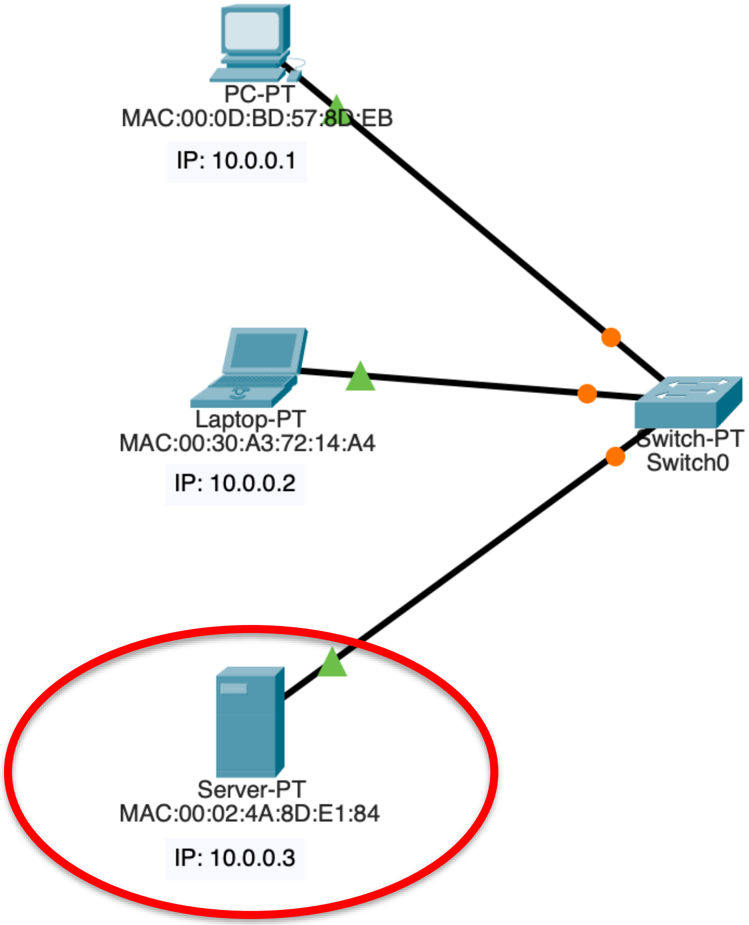


A Switch connects three hosts

- PC
- Laptop

A small network example shows how layers work together

Cisco Packet Tracer

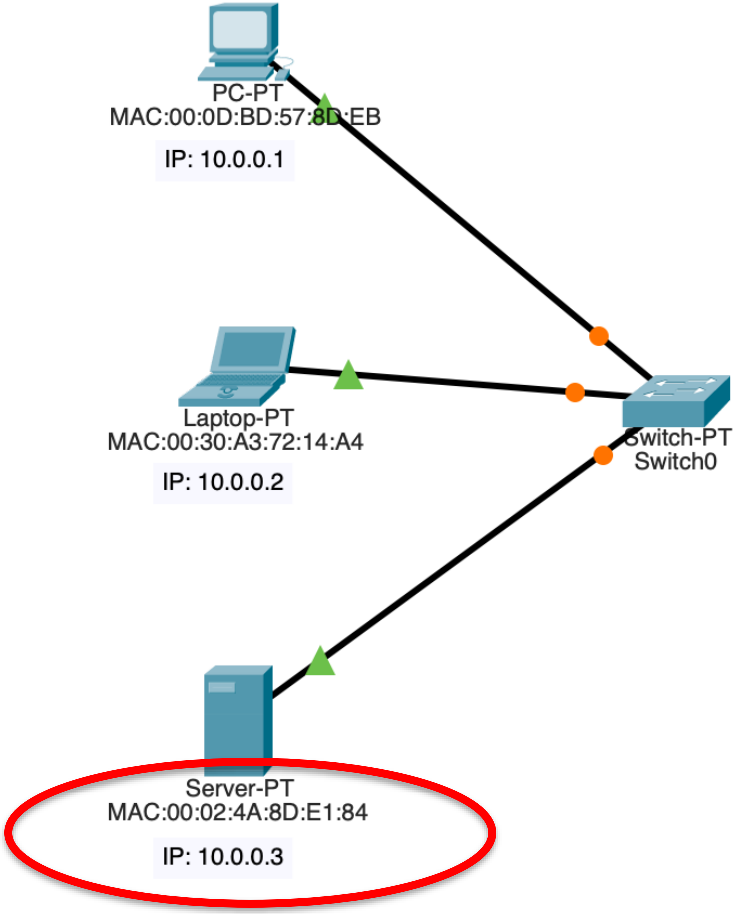


A Switch connects three hosts

- PC
- Laptop
- Server

MACs are burned into NIC ROM, IP addresses can be static

Cisco Packet Tracer



A Switch connects three hosts

- PC
- Laptop
- Server

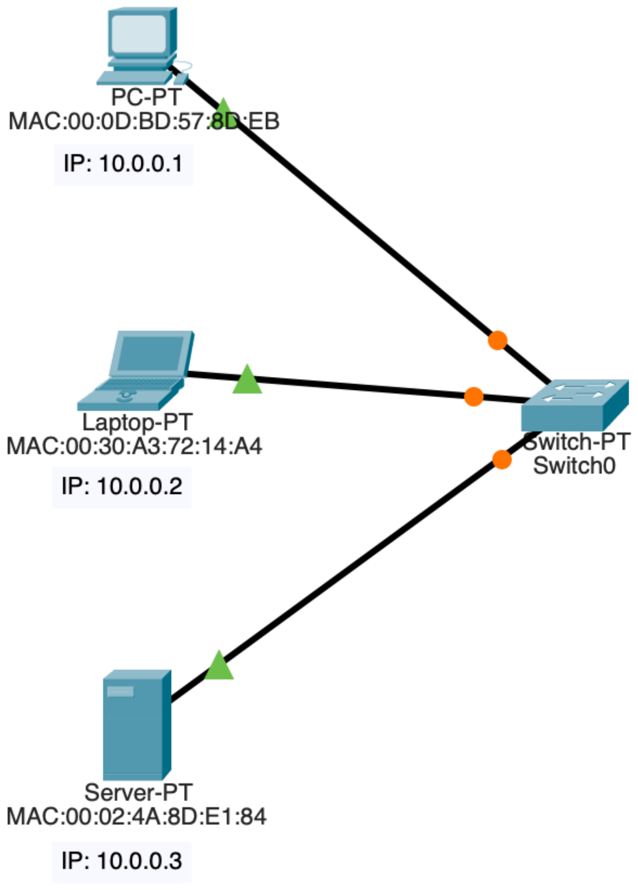
Each host has a unique MAC address burned into the NIC

I have manually assigned a static IP addresses to each host

All devices are on a single LAN, we will deal with routing between LANs soon

Switches operate at Layer 2

Cisco Packet Tracer



A Switch connects three hosts

- PC
- Laptop
- Server

Each host has a unique MAC address burned into the NIC

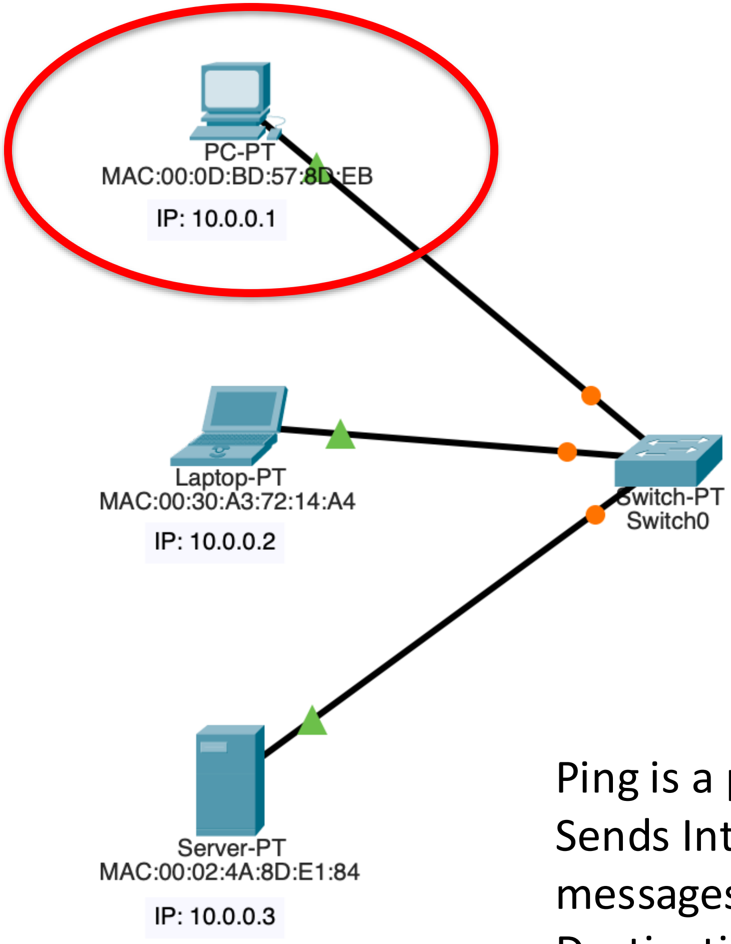
I have manually assigned a static IP addresses to each host

All devices are on a single LAN, we will deal with routing between LANs soon

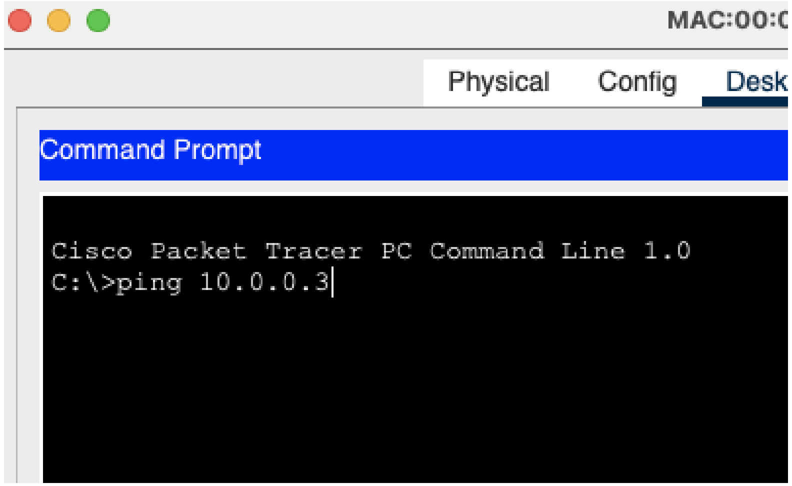
Recall the Switch operates at Layer 2 (uses MAC addresses to identify hosts in the local area network, does not know about IP at Layer 3)

Ping tests if hosts are reachable over the network

Cisco Packet Tracer



PC pings Server (IP address 10.0.0.3)



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3
```

Ping is a program that is often used to see if hosts are reachable

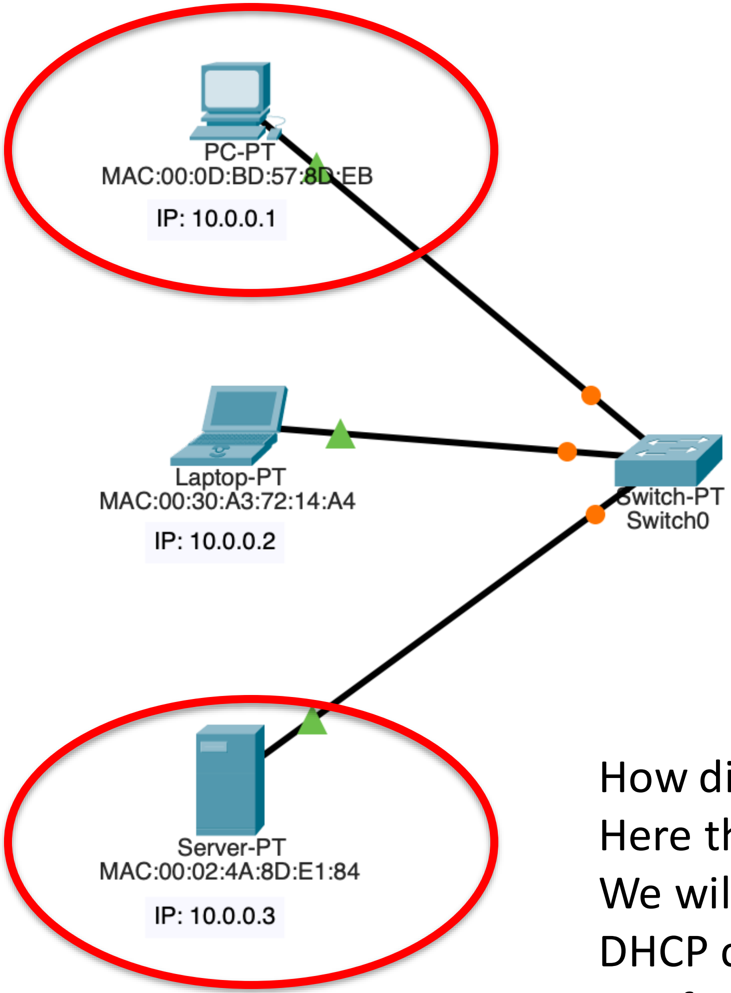
Sends Internet Control Message Protocol (ICMP) *echo request* messages to destination host

Destination replies with ICMP *echo reply* message

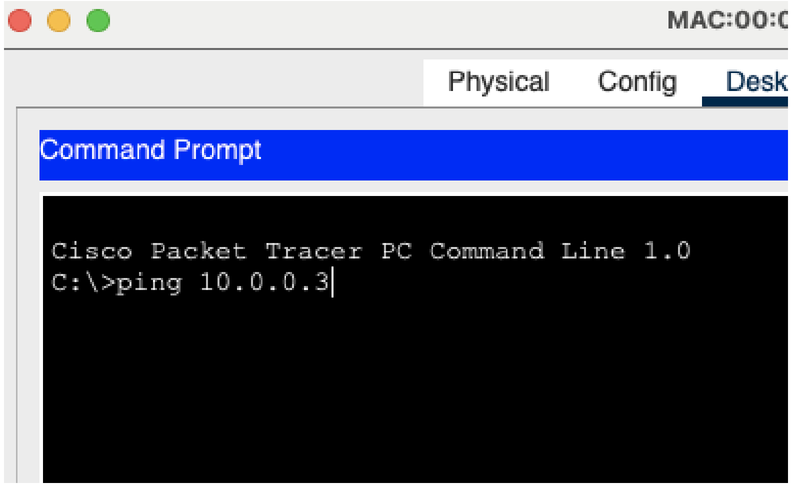
Ping times the round trip

How did the PC know the Server's IP address?

Cisco Packet Tracer



PC pings Server (IP address 10.0.0.3)



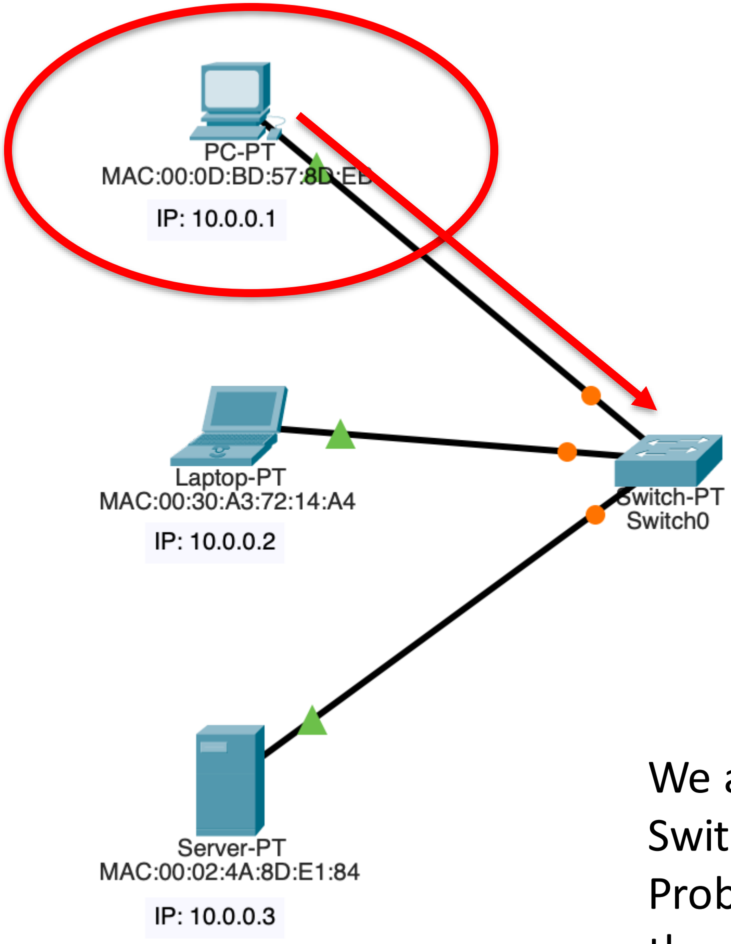
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3
```

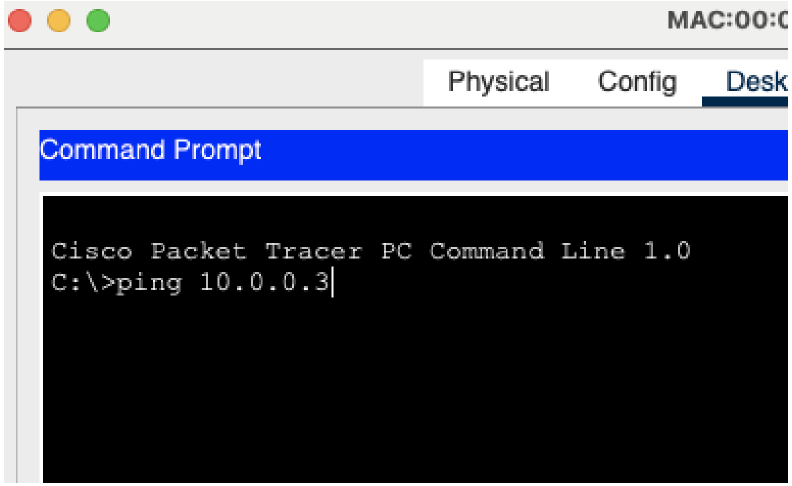
How did the PC know what IP address to ping (10.0.0.3)?
Here the IP addresses are statically (manually) assigned
We will soon see how DHCP gives dynamic IP addresses
DHCP can give a fixed IP address to things like servers (so we can find them)
Other hosts get a random IP address from DHCP server's address pool

Will discuss DNS soon

PC doesn’t know how to reach Server, so it asks who has IP address 10.0.0.3 with ARP

Cisco Packet Tracer



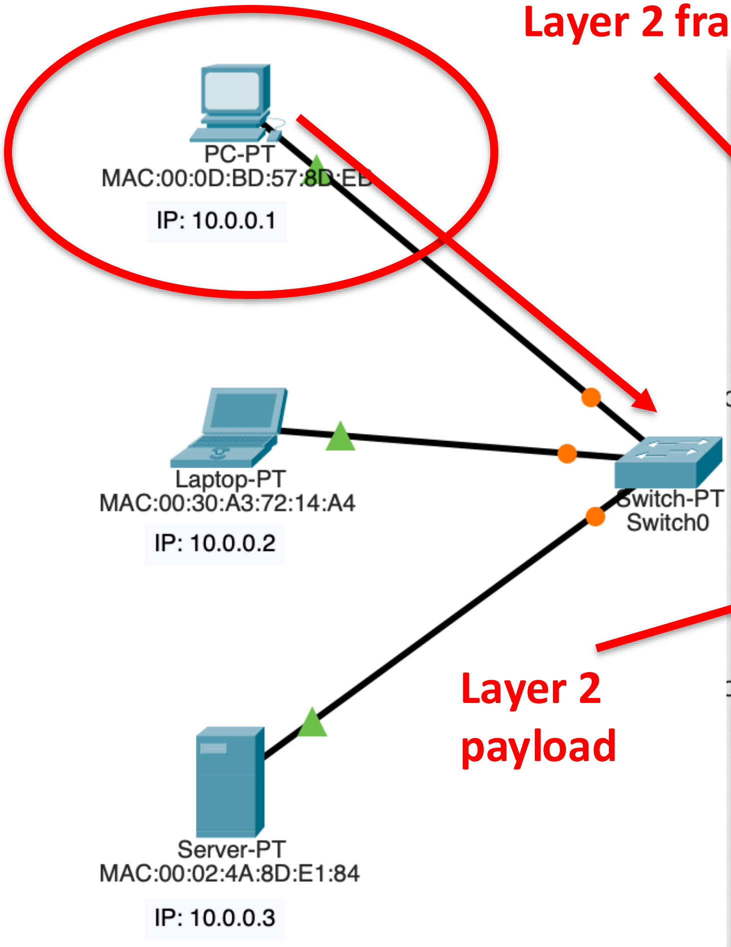


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3
```

We are using a Switch here, it operates at Layer 2 (MAC)
Switches do not know about IP addresses (those are Layer 3)
Problem: the PC does not the Server’s MAC (but does know the static IP address)
We need a way to map IP addresses to MACs
We use Address Resolution Protocol (ARP)

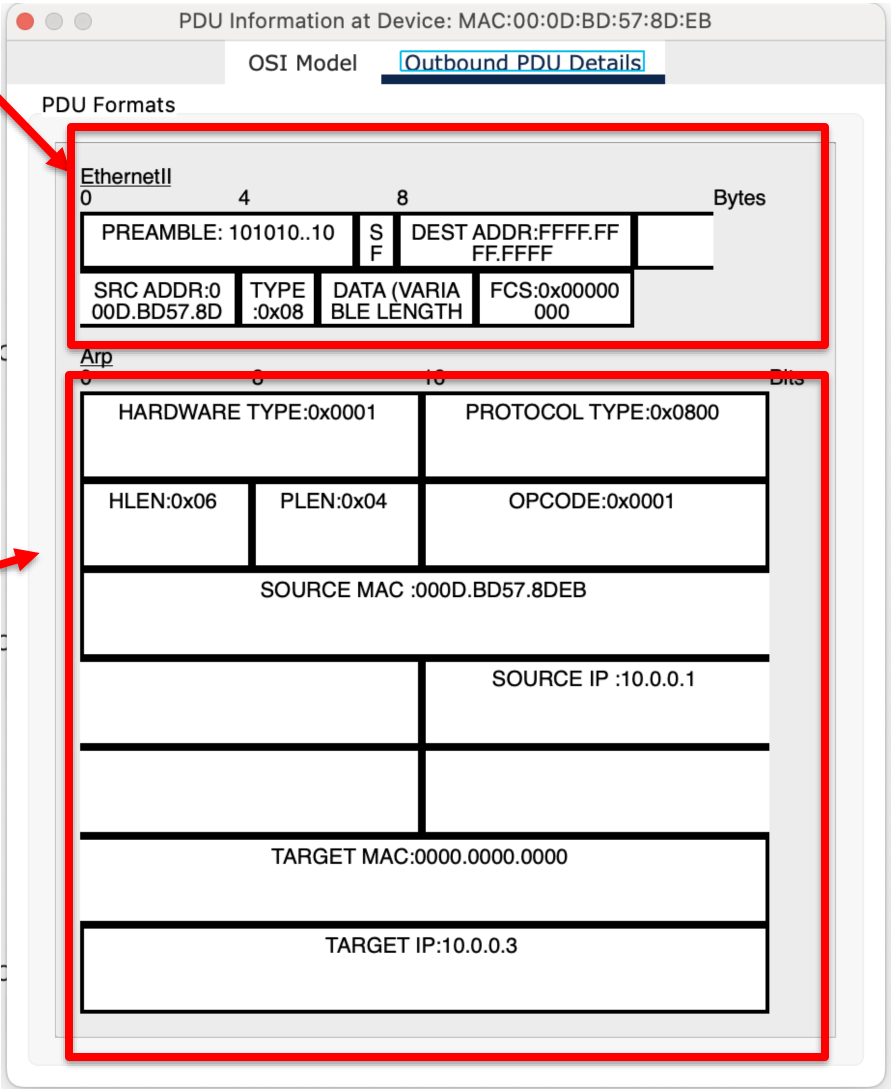
ARP request is sent to all hosts asking who has IP address 10.0.0.3

Cisco Packet Tracer



Layer 2 frame header

Layer 2 payload



PDU Information at Device: MAC:00:0D:BD:57:8D:EB

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:FFFF.FF FF.FFFF

SRC ADDR:0 00D.BD57.8D | TYPE :0x08 | DATA (VARIA BLE LENGTH | FCS:0x00000 000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0001

SOURCE MAC :000D.BD57.8DEB

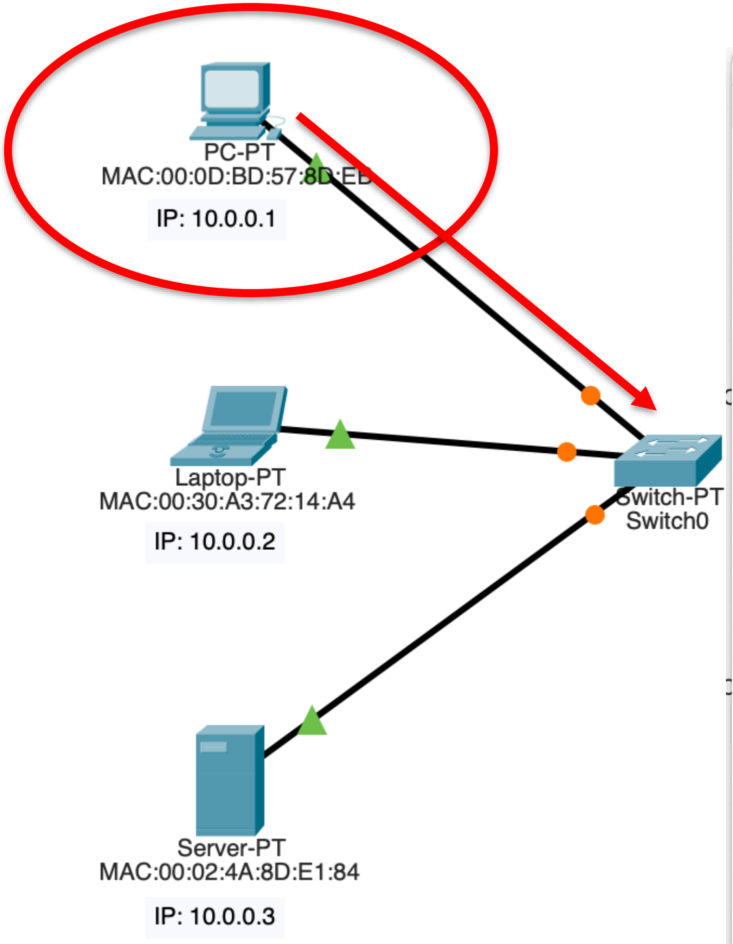
SOURCE IP :10.0.0.1

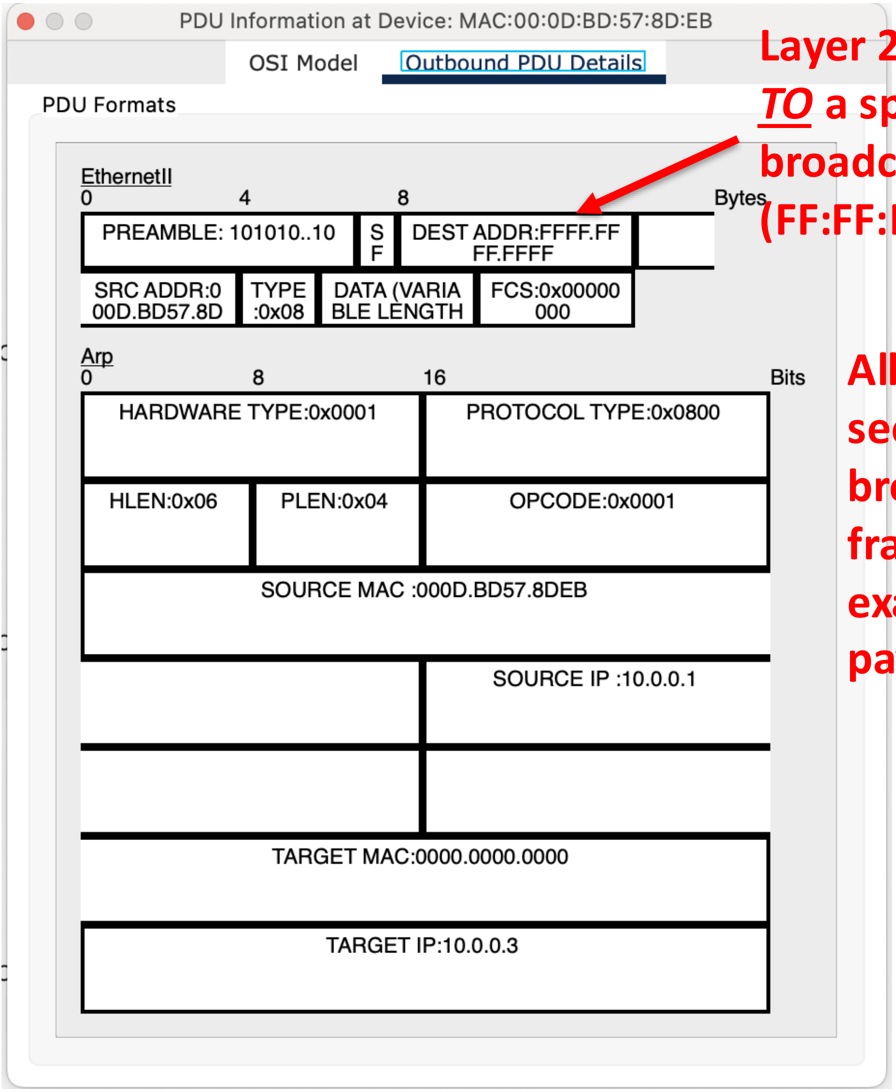
TARGET MAC:0000.0000.0000

TARGET IP:10.0.0.3

ARP request is sent to all hosts asking who has IP address 10.0.0.3

Cisco Packet Tracer





PDU Information at Device: MAC:00:0D:BD:57:8D:EB

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:FFFF.FF FF.FFFF

SRC ADDR:0 00D.BD57.8D | TYPE :0x08 | DATA (VARIA BLE LENGTH | FCS:0x00000 000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0001

SOURCE MAC :000D.BD57.8DEB

SOURCE IP :10.0.0.1

TARGET MAC:0000.0000.0000

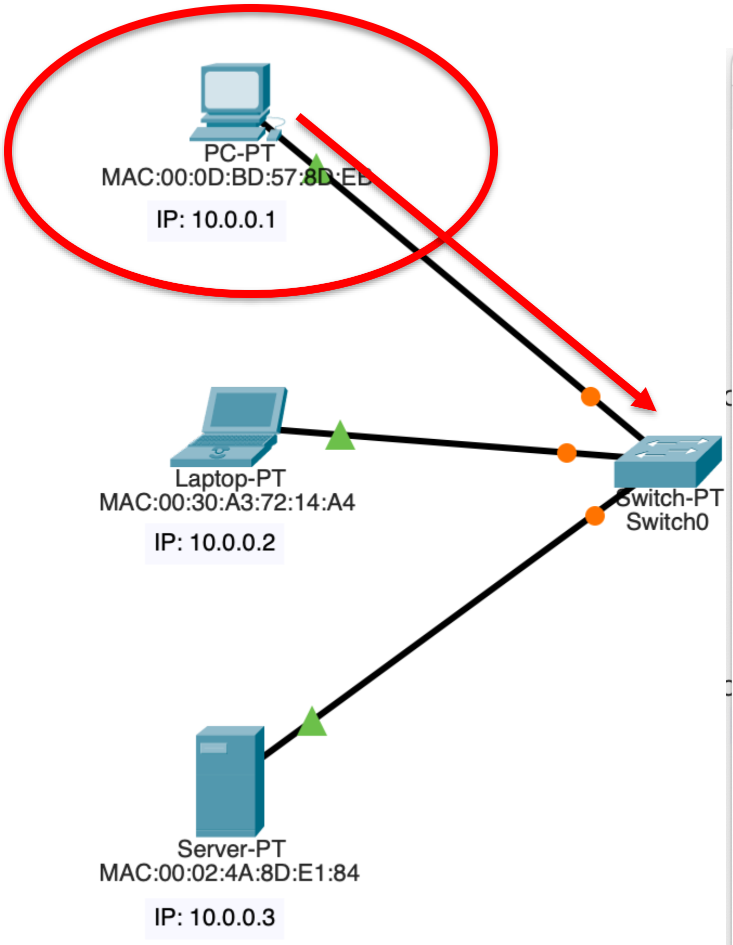
TARGET IP:10.0.0.3

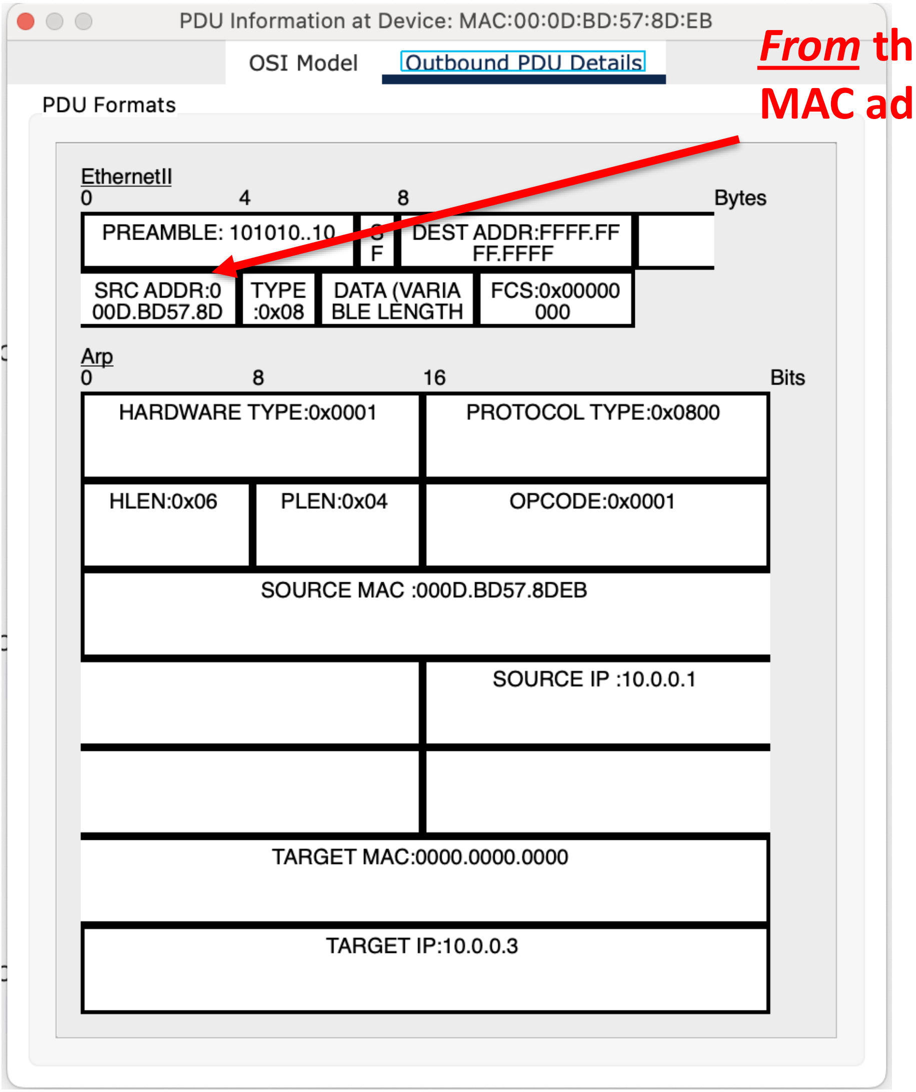
Layer 2 frame sent *TO* a special broadcast MAC (FF:FF:FF:FF:FF:FF)

All hosts that see this broadcast frame will examine payload

ARP request is sent to all hosts asking who has IP address 10.0.0.3

Cisco Packet Tracer




PDU Information at Device: MAC:00:0D:BD:57:8D:EB

OSI Model | Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | S F | DEST ADDR:FFFF.FF FF.FFFF

SRC ADDR:0 00D.BD57.8D | TYPE :0x08 | DATA (VARIA BLE LENGTH | FCS:0x00000 000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0001

SOURCE MAC :000D.BD57.8DEB

SOURCE IP :10.0.0.1

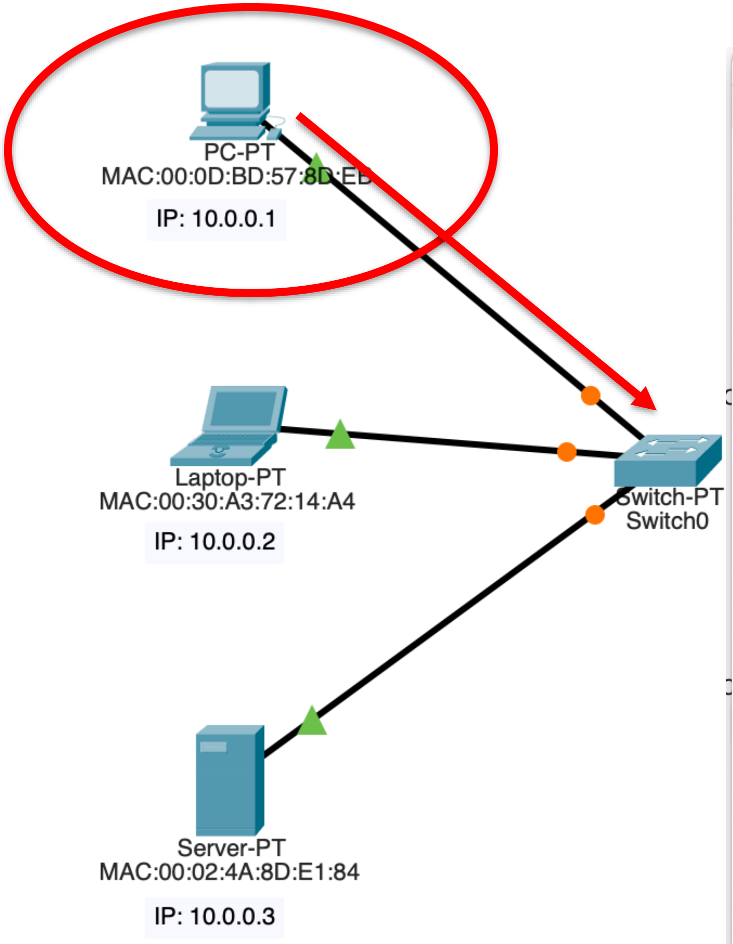
TARGET MAC:0000.0000.0000

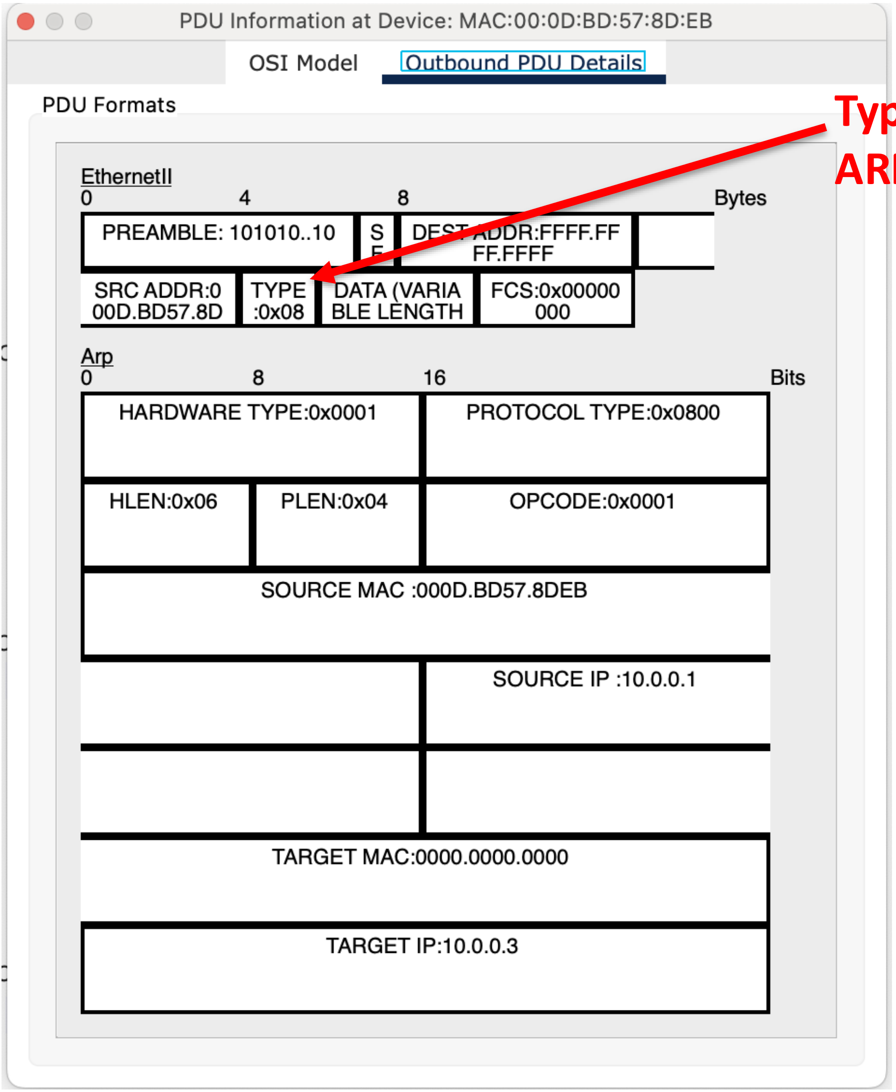
TARGET IP:10.0.0.3

From **the PC's MAC address**

ARP request is sent to all hosts asking who has IP address 10.0.0.3

Cisco Packet Tracer





EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | S F | DEST ADDR:FFFF.FF FF.FFFF

SRC ADDR:0 00D.BD57.8D | TYPE :0x08 | DATA (VARIA BLE LENGTH | FCS:0x00000 000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0001

SOURCE MAC :000D.BD57.8DEB

SOURCE IP :10.0.0.1

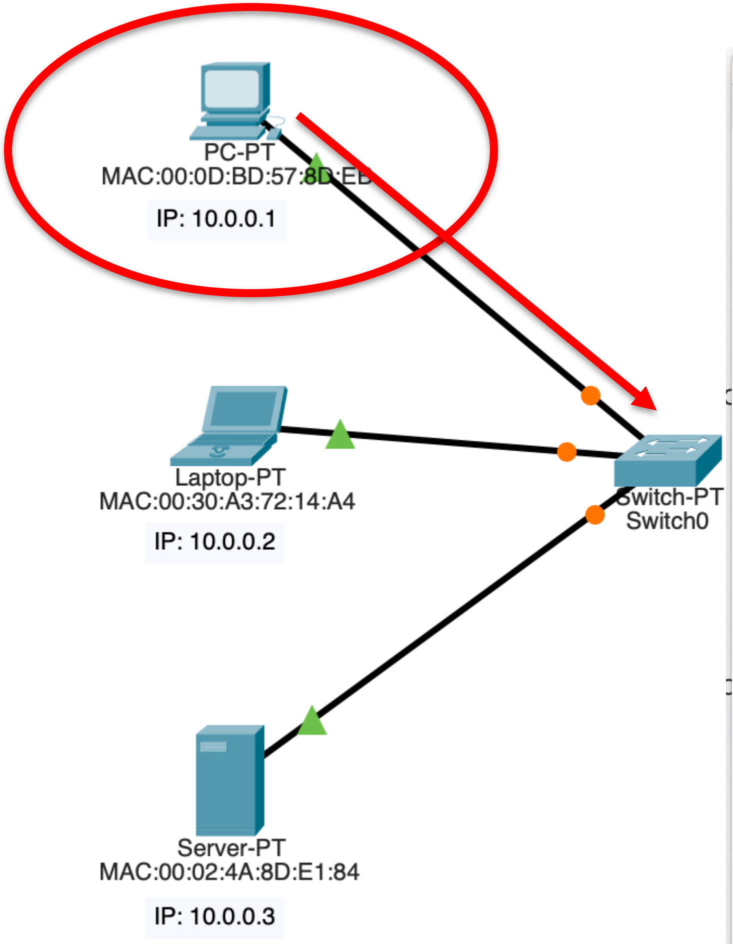
TARGET MAC:0000.0000.0000

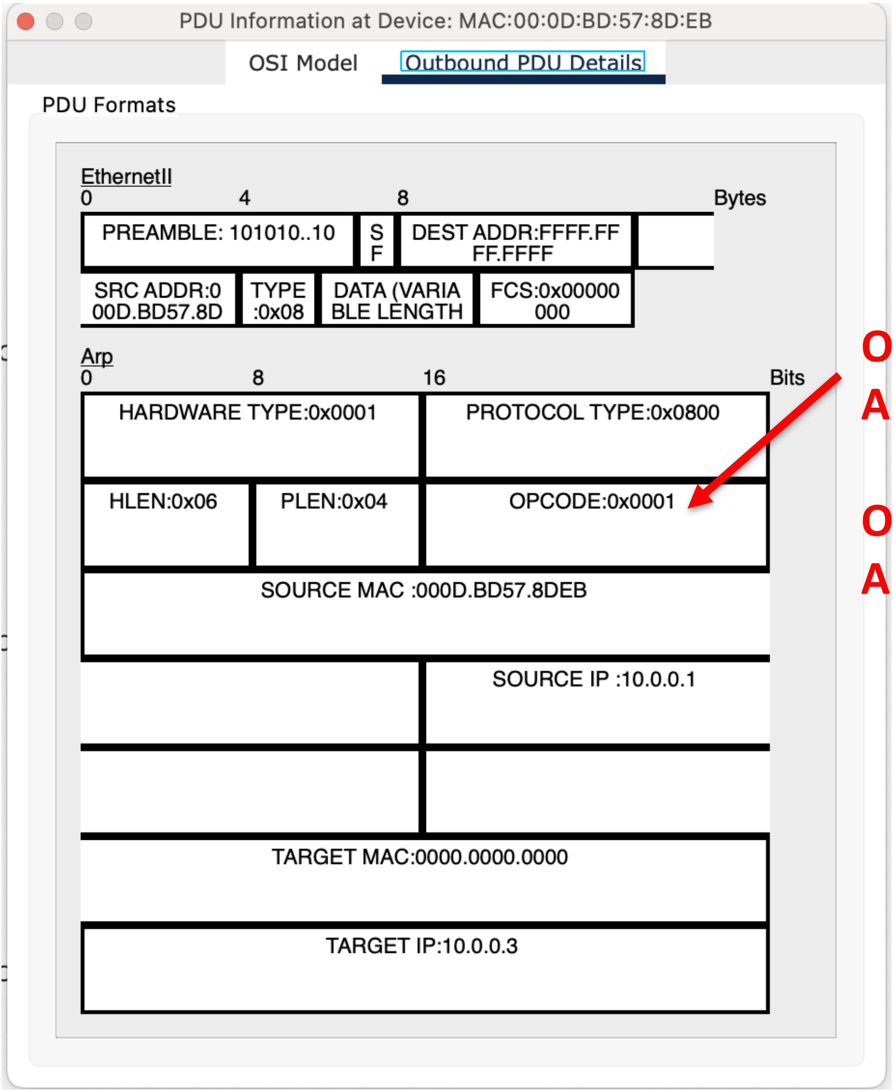
TARGET IP:10.0.0.3

Type x0806 is ARP

ARP request is sent to all hosts asking who has IP address 10.0.0.3

Cisco Packet Tracer





PDU Information at Device: MAC:00:0D:BD:57:8D:EB

PDU Formats

EthernetII

0	4	8		Bytes
PREAMBLE: 101010..10		S F	DEST ADDR:FFFF.FF FF.FFFF	
SRC ADDR:0 00D.BD57.8D	TYPE :0x08	DATA (VARIA BLE LENGTH	FCS:0x00000 000	

Arp

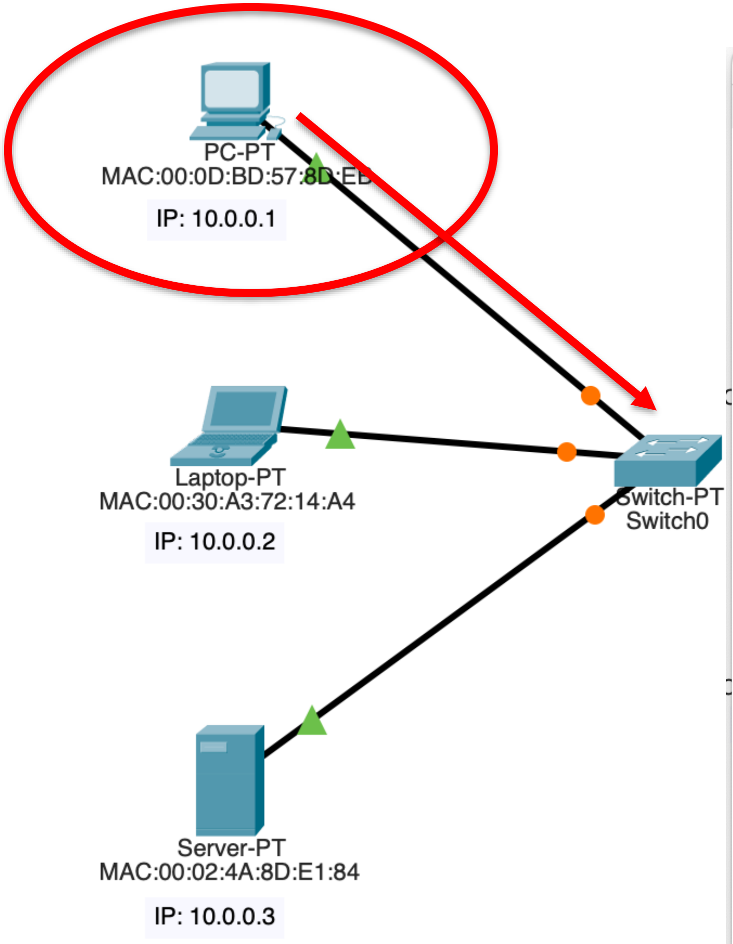
0	8	16	Bits
HARDWARE TYPE:0x0001		PROTOCOL TYPE:0x0800	
HLEN:0x06	PLEN:0x04	OPCODE:0x0001	
SOURCE MAC :000D.BD57.8DEB			
		SOURCE IP :10.0.0.1	
TARGET MAC:0000.0000.0000			
TARGET IP:10.0.0.3			

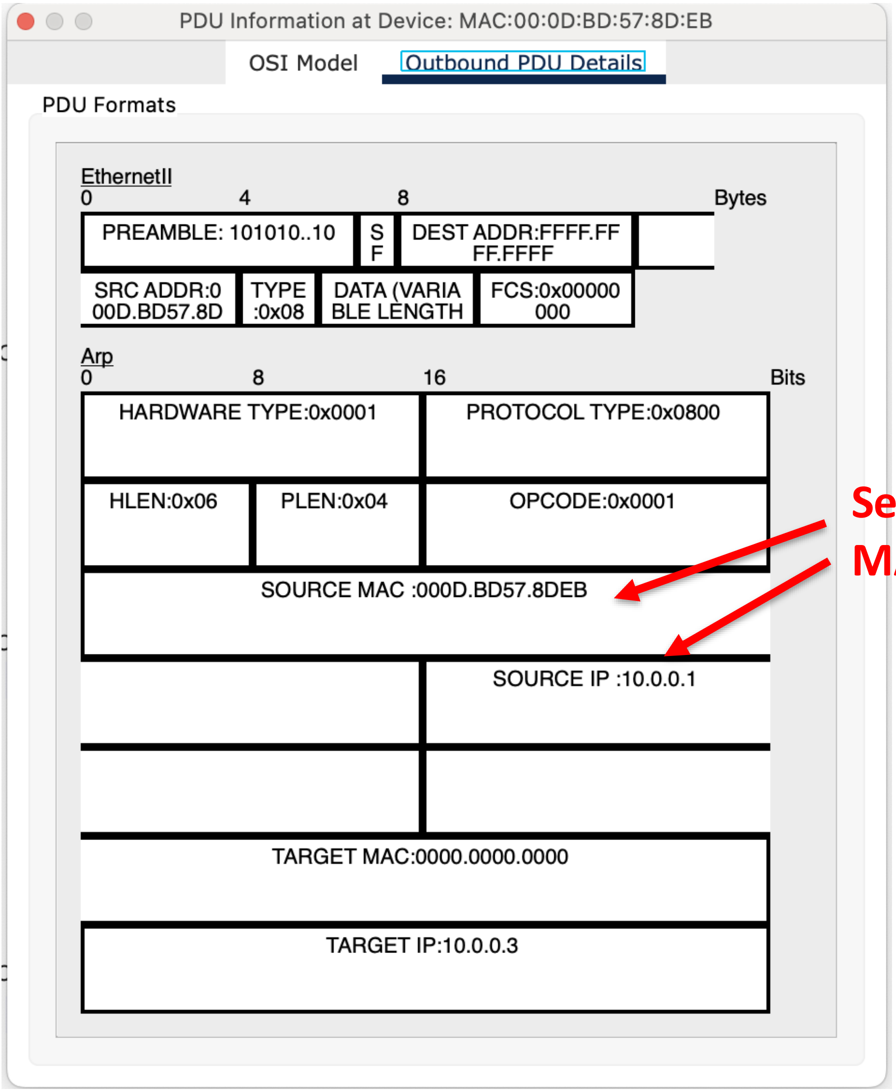
Op code 1 is ARP request

Op code 2 is ARP reply

ARP request is sent to all hosts asking who has IP address 10.0.0.3

Cisco Packet Tracer





PDU Information at Device: MAC:00:0D:BD:57:8D:EB

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:FFFF.FFFF.FFFF

SRC ADDR:000D.BD57.8D | TYPE :0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0001

SOURCE MAC :000D.BD57.8DEB

SOURCE IP :10.0.0.1

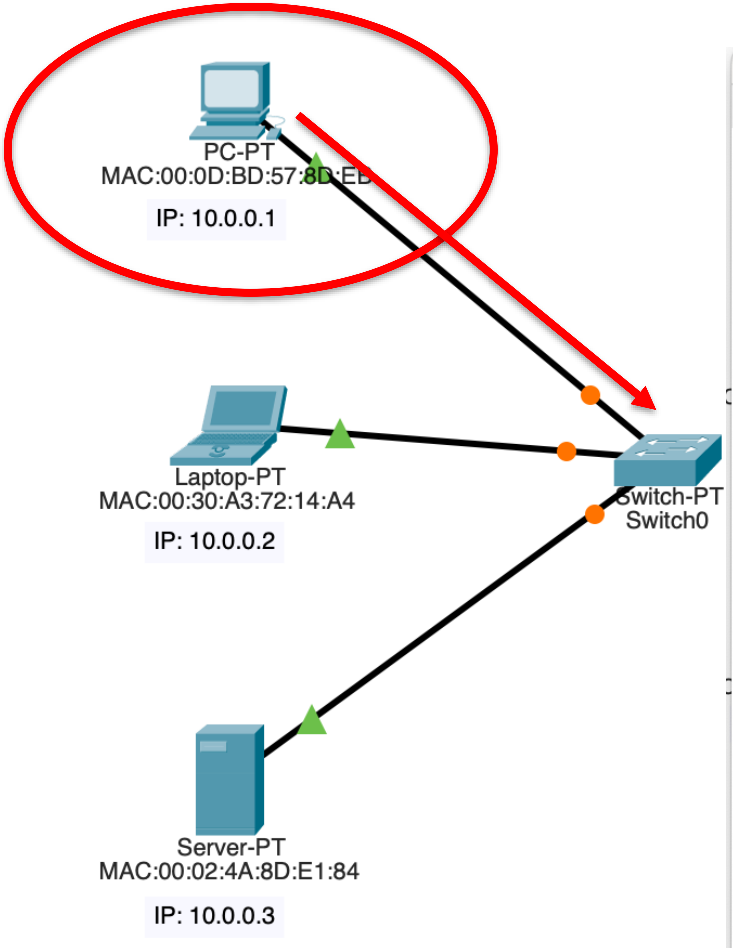
TARGET MAC:0000.0000.0000

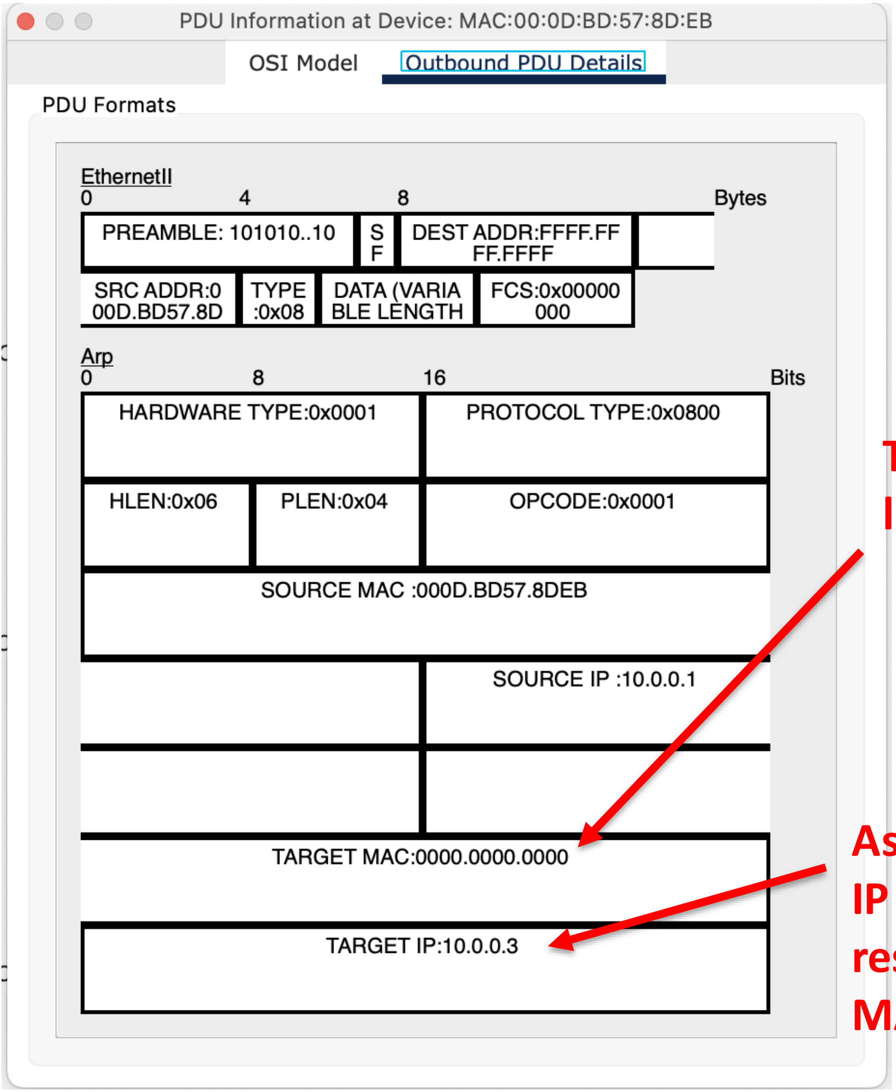
TARGET IP:10.0.0.3

Sender (PC) MAC and IP

ARP request is sent to all hosts asking who has IP address 10.0.0.3

Cisco Packet Tracer





PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10	SF	DEST ADDR:FFFF.FFFF.FFFF	
SRC ADDR:000D.BD57.8D	TYPE :0x08	DATA (VARIABLE LENGTH	FCS:0x00000000

Arp

0 8 16 Bits

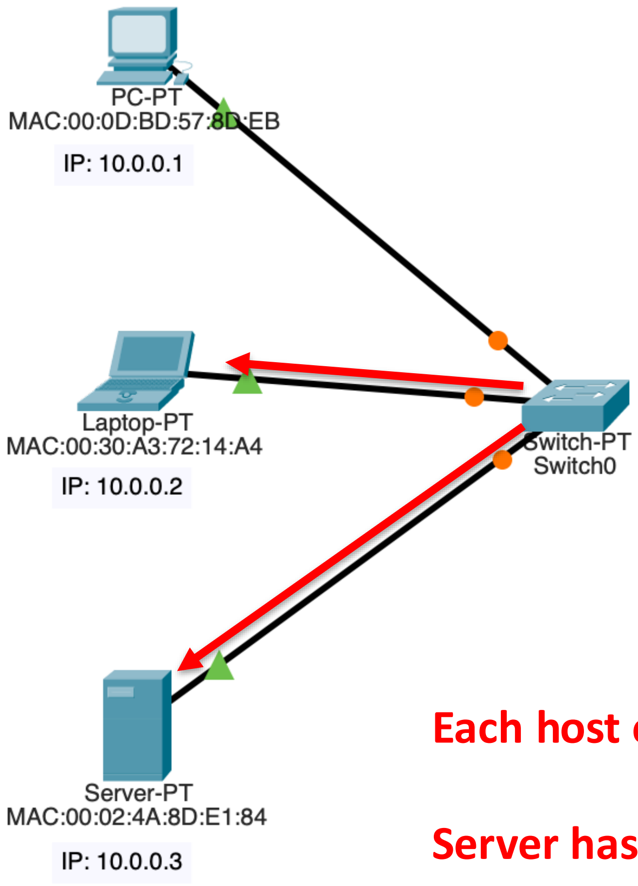
HARDWARE TYPE:0x0001		PROTOCOL TYPE:0x0800
HLEN:0x06	PLEN:0x04	OPCODE:0x0001
SOURCE MAC :000D.BD57.8DEB		
		SOURCE IP :10.0.0.1
TARGET MAC:0000.0000.0000		
TARGET IP:10.0.0.3		

Target MAC left blank

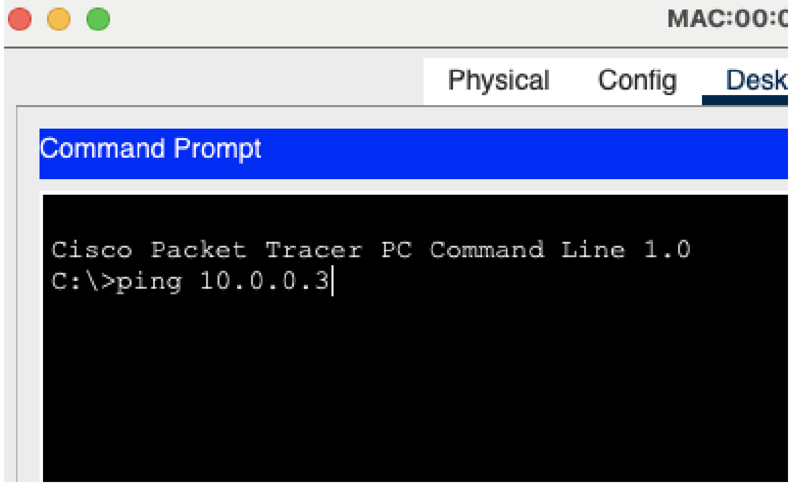
Asking Target IP (Server) to respond with MAC

All hosts decapsulate the broadcast frame, non-targets ignore, target replies

Cisco Packet Tracer



Address Resolution Protocol (ARP) sends message to each host and asks it to respond with MAC address if it has IP address 10.0.0.3



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3
```

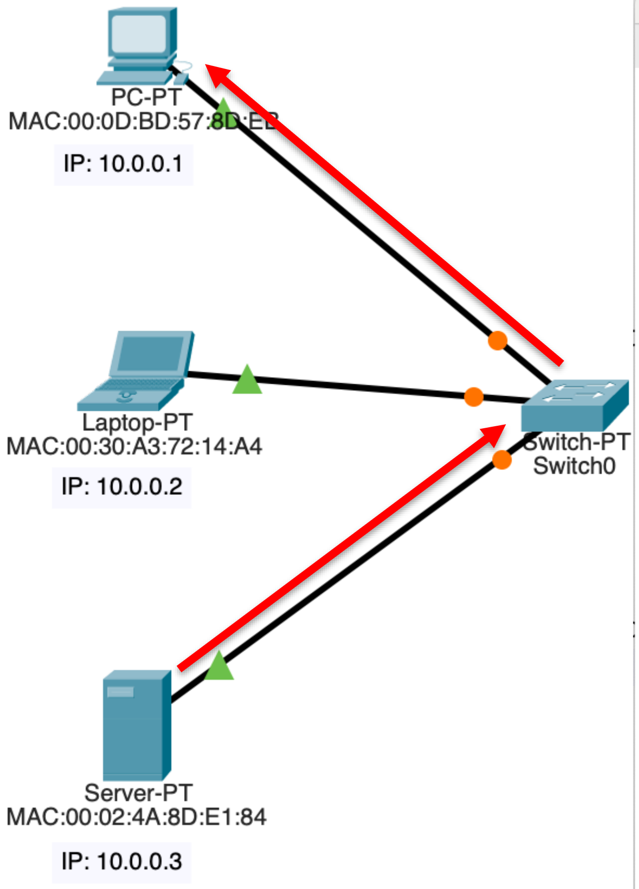
Each host examines the frame (because MAC was broadcast)

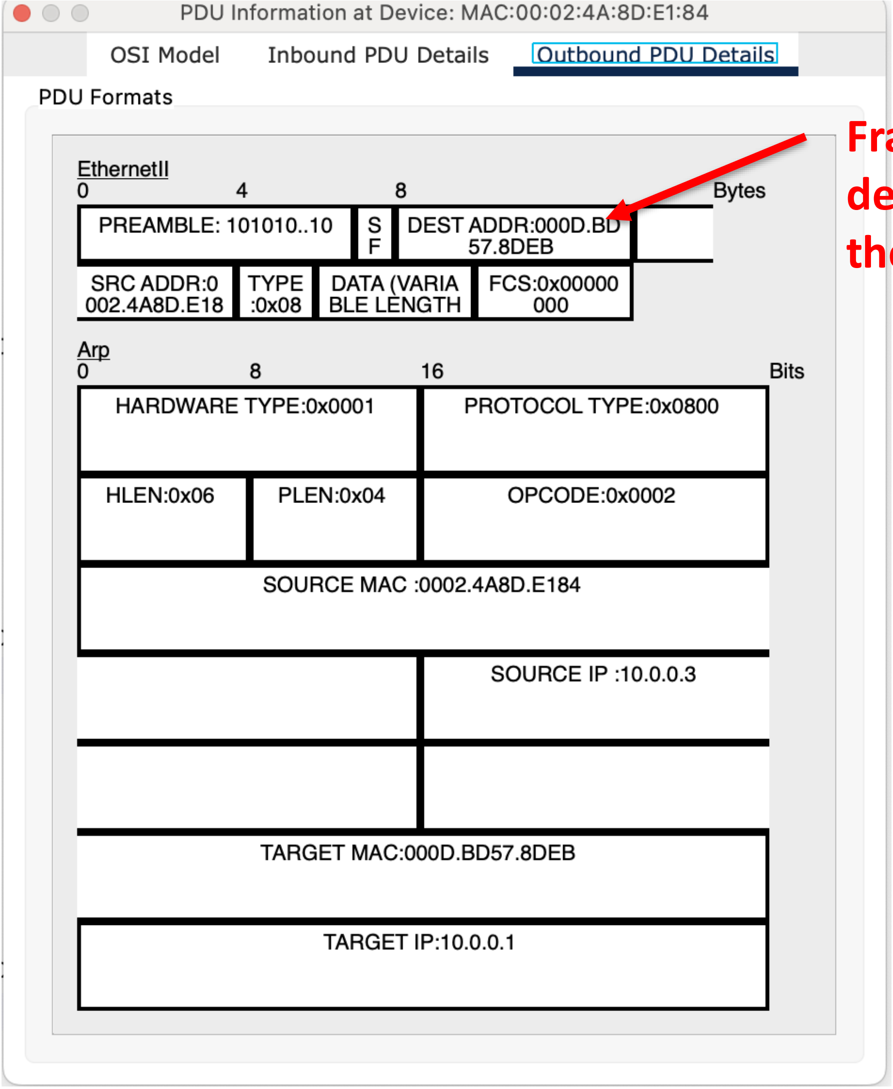
Server has address 10.0.0.3, so it responds with ARP reply

Laptop does not have 10.0.0.3, so it ignores the ARP request

ARP reply sends Server's MAC back to PC that made the ARP request

Cisco Packet Tracer





PDU Information at Device: MAC:00:02:4A:8D:E1:84

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:000D.BD57.8DEB

SRC ADDR:0002.4A8D.E18 | TYPE :0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0002

SOURCE MAC :0002.4A8D.E184

SOURCE IP :10.0.0.3

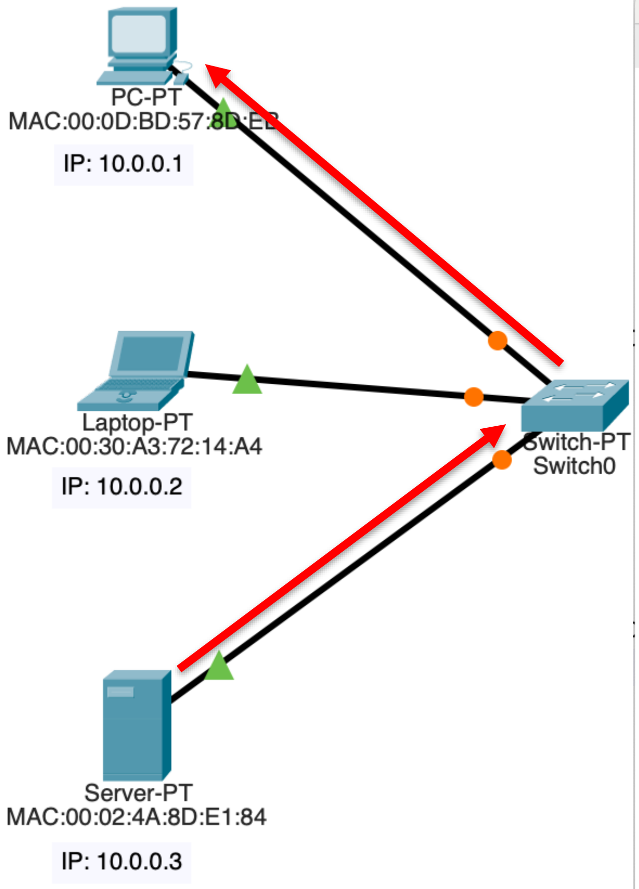
TARGET MAC:000D.BD57.8DEB

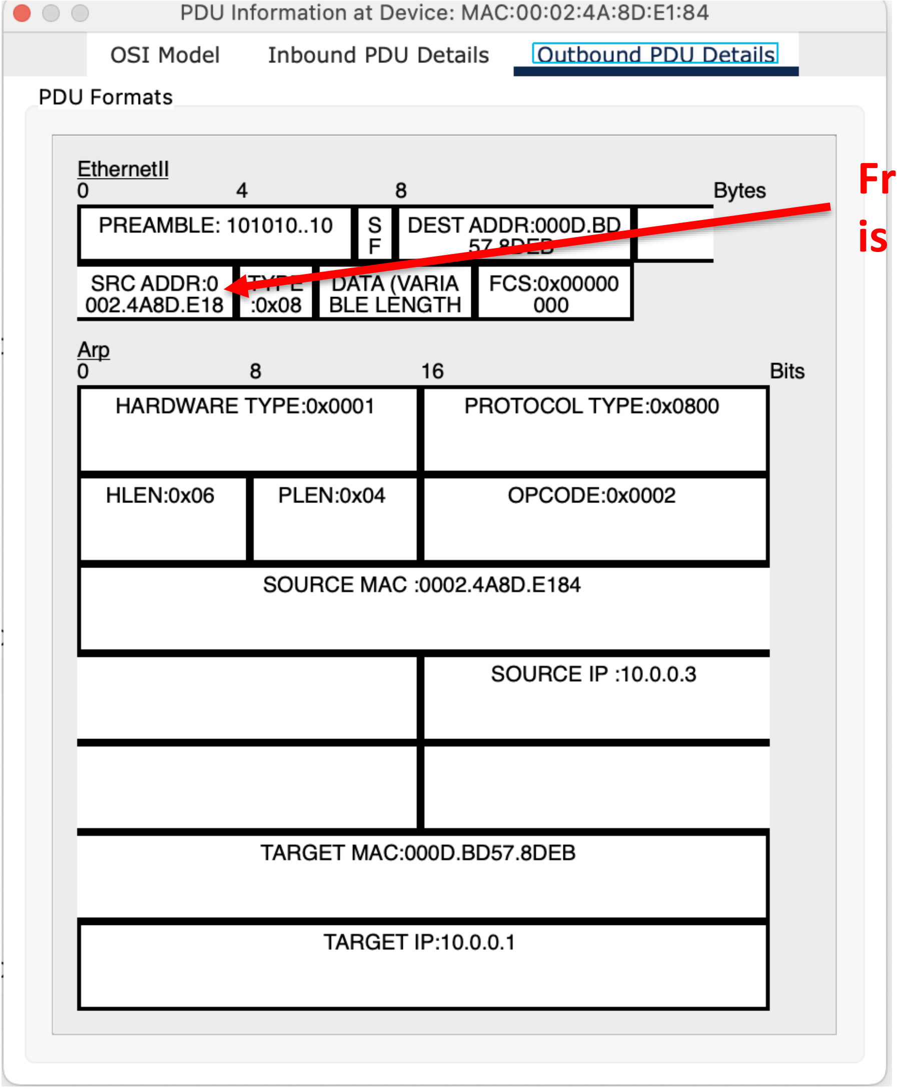
TARGET IP:10.0.0.1

Frame destination is the PC

ARP reply sends Server's MAC back to PC that made the ARP request

Cisco Packet Tracer





PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | S F | DEST ADDR:000D.BD 57.8DEB

SRC ADDR:0 002.4A8D.E18 | TYPE :0x08 | DATA (VARIA BLE LENGTH | FCS:0x00000 000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0002

SOURCE MAC :0002.4A8D.E184

SOURCE IP :10.0.0.3

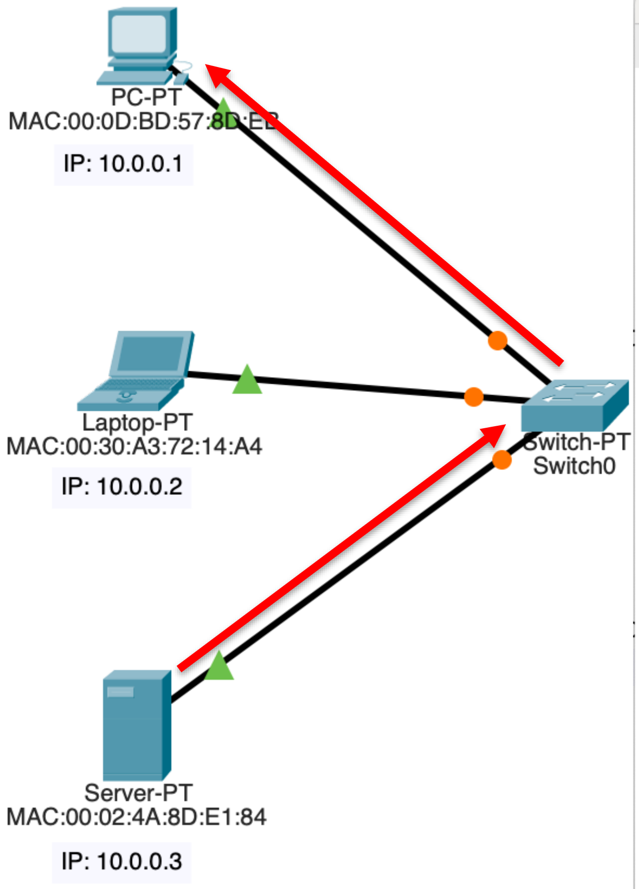
TARGET MAC:000D.BD57.8DEB

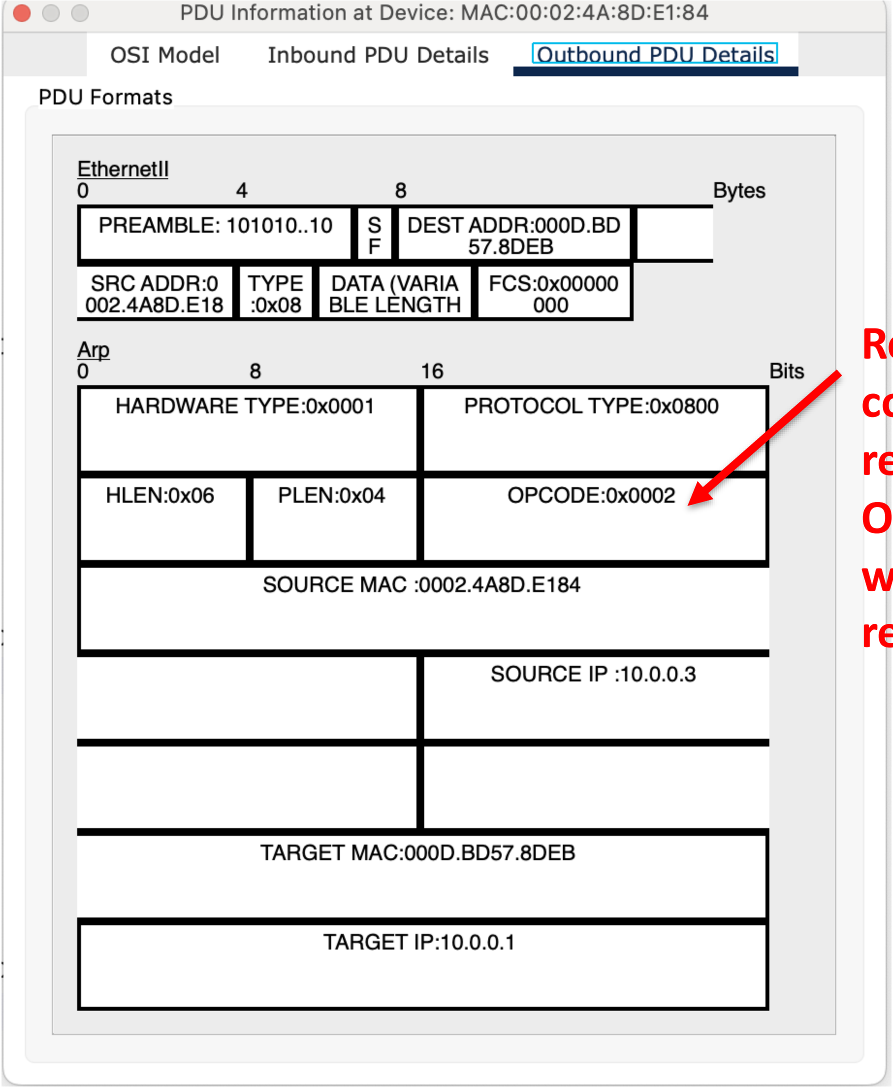
TARGET IP:10.0.0.1

Frame source is the Server

ARP reply sends Server's MAC back to PC that made the ARP request

Cisco Packet Tracer




PDU Information at Device: MAC:00:02:4A:8D:E1:84

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:000D.BD57.8DEB

SRC ADDR:0002.4A8D.E18 | TYPE :0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0002

SOURCE MAC :0002.4A8D.E184

SOURCE IP :10.0.0.3

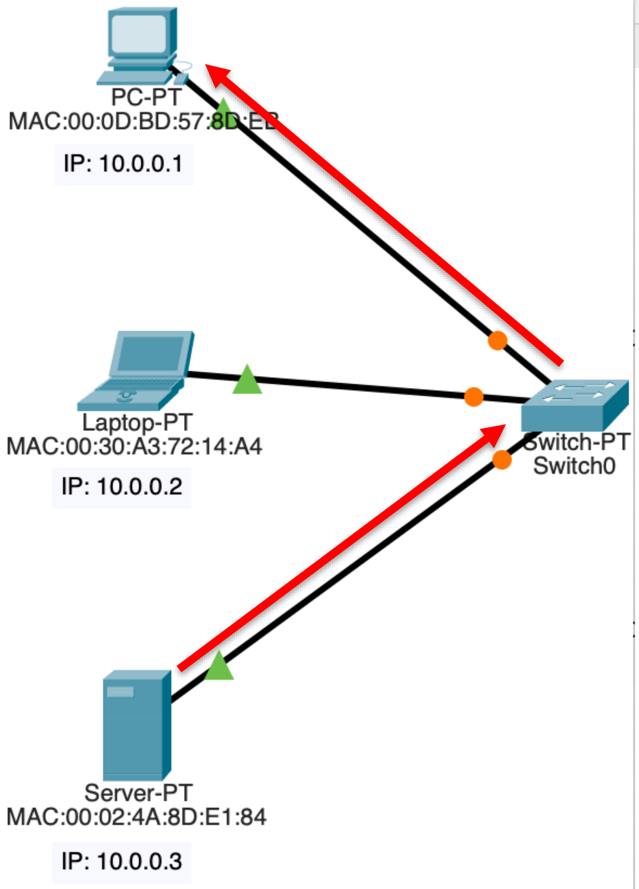
TARGET MAC:000D.BD57.8DEB

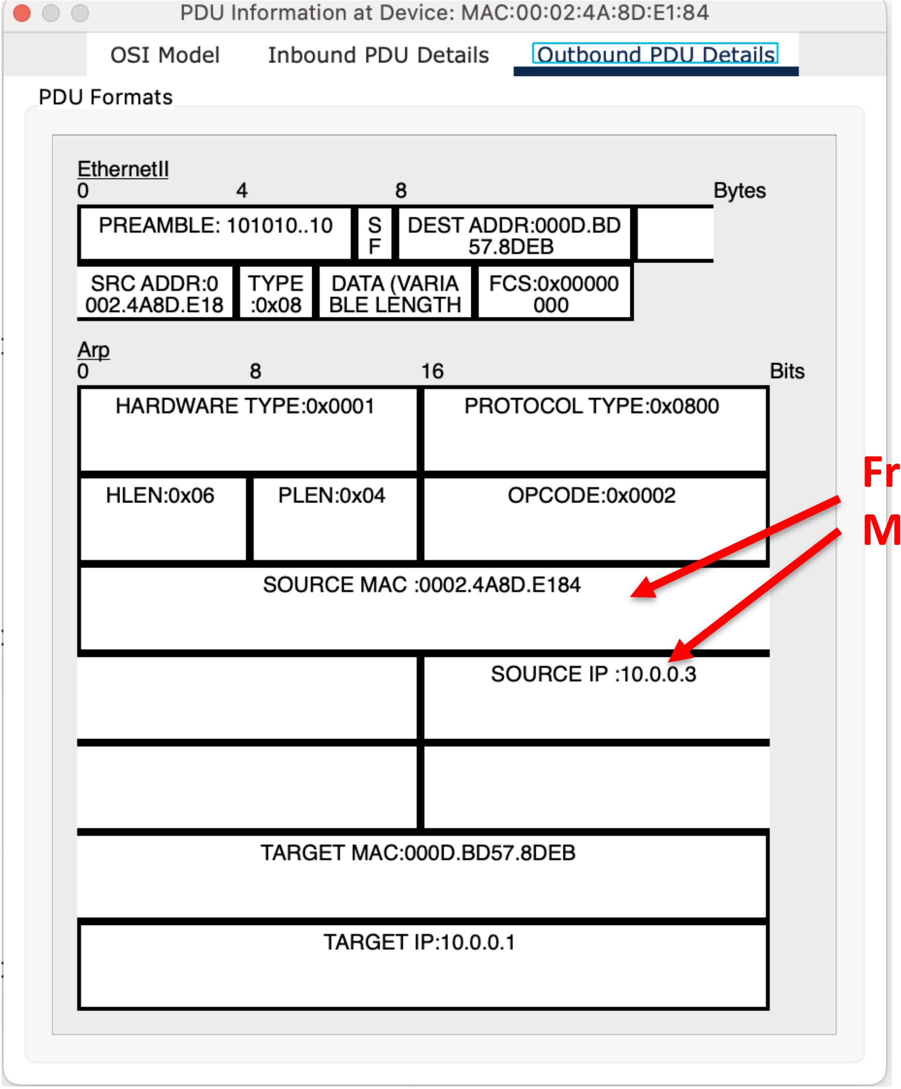
TARGET IP:10.0.0.1

Reply Op code 2 is ARP reply (recall Op code 1 was ARP request)

ARP reply sends Server’s MAC back to PC that made the ARP request

Cisco Packet Tracer





PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:000D.BD57.8DEB

SRC ADDR:0002.4A8D.E18 | TYPE :0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0002

SOURCE MAC :0002.4A8D.E184

SOURCE IP :10.0.0.3

TARGET MAC:000D.BD57.8DEB

TARGET IP:10.0.0.1

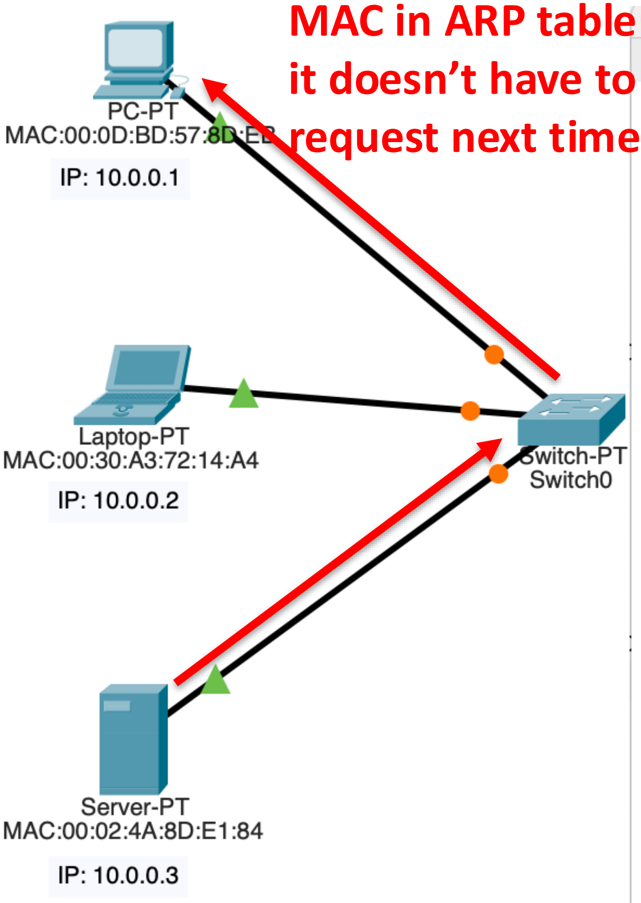
From Server’s MAC and IP

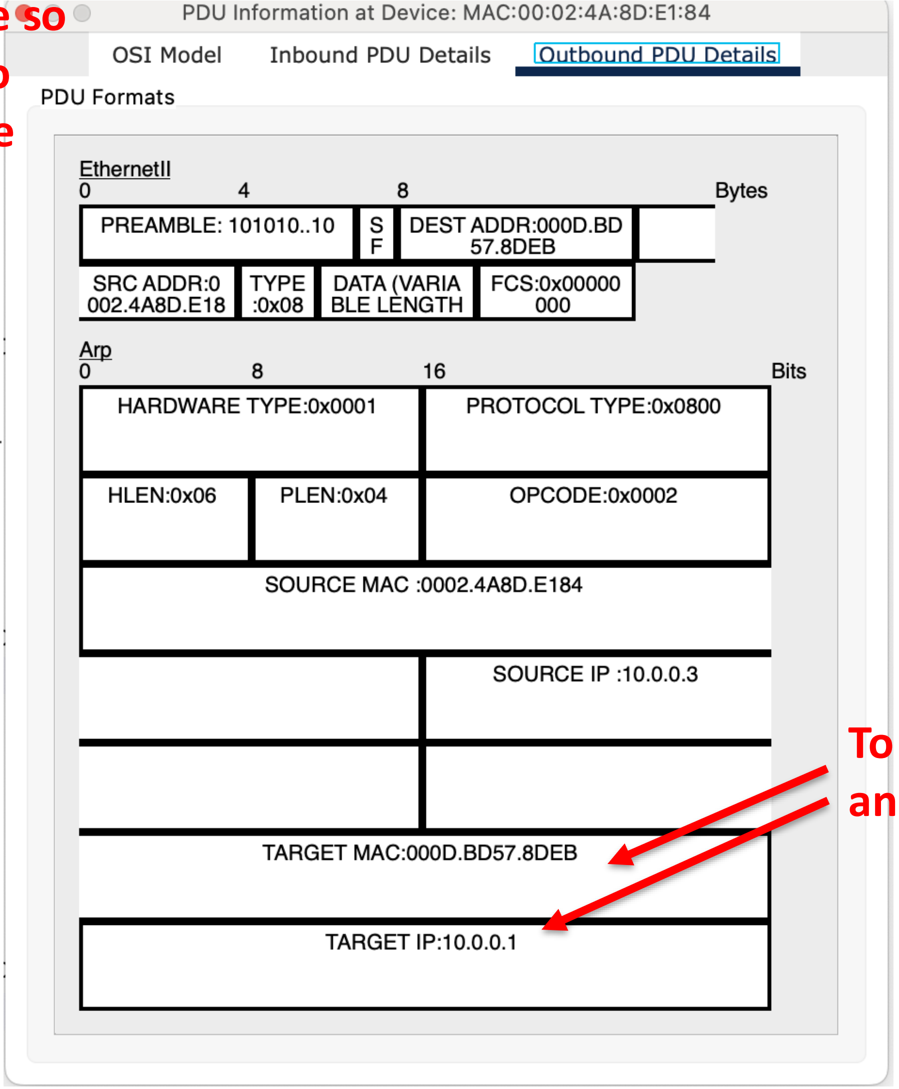
ARP reply sends Server’s MAC back to PC that made the ARP request

10.0.0.3 -> 00:02:4A:8D:E1:84

PC stores Server’s MAC in ARP table so it doesn’t have to request next time

Cisco Packet Tracer





PDU Information at Device: MAC:00:02:4A:8D:E1:84

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:000D.BD 57.8DEB

SRC ADDR:0 002.4A8D.E18 | TYPE :0x08 | DATA (VARIA BLE LENGTH | FCS:0x00000 000

Arp

0 8 16 Bits

HARDWARE TYPE:0x0001 | PROTOCOL TYPE:0x0800

HLEN:0x06 | PLEN:0x04 | OPCODE:0x0002

SOURCE MAC :0002.4A8D.E184

SOURCE IP :10.0.0.3

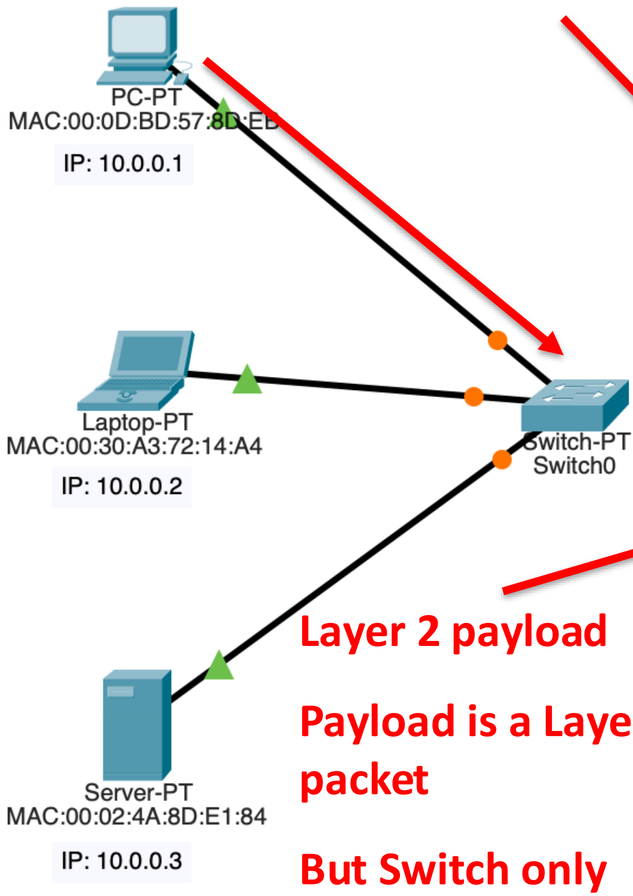
TARGET MAC:000D.BD57.8DEB

TARGET IP:10.0.0.1

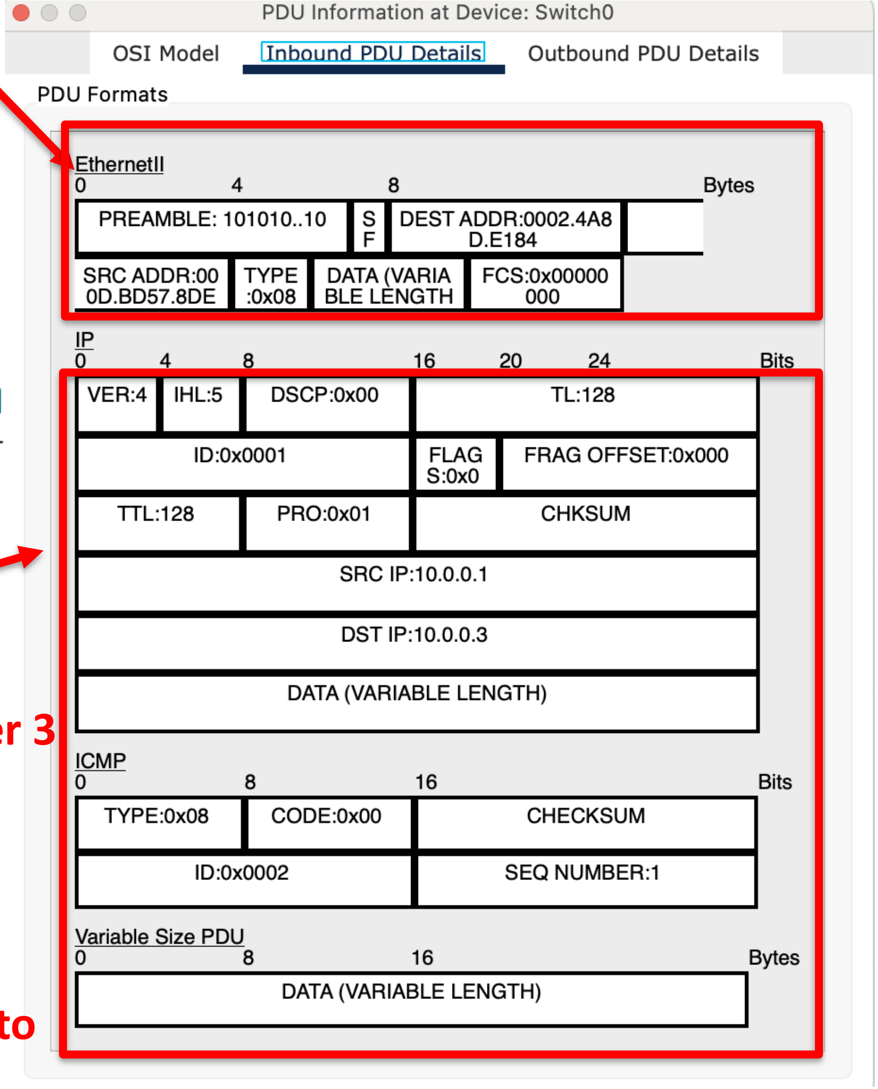
To PC’s MAC and IP

PC now knows the Server’s MAC and can send ICMP echo request (ping) Layer 3

ping 10.0.0.3



Layer 2 frame header



PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:0002.4A8D.E184

SRC ADDR:000D.BD57.8DE | TYPE:0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x0001 | FLAGS:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

SRC IP:10.0.0.1

DST IP:10.0.0.3

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

TYPE:0x08 | CODE:0x00 | CHECKSUM

ID:0x0002 | SEQ NUMBER:1

Variable Size PDU

0 8 16 Bytes

DATA (VARIABLE LENGTH)

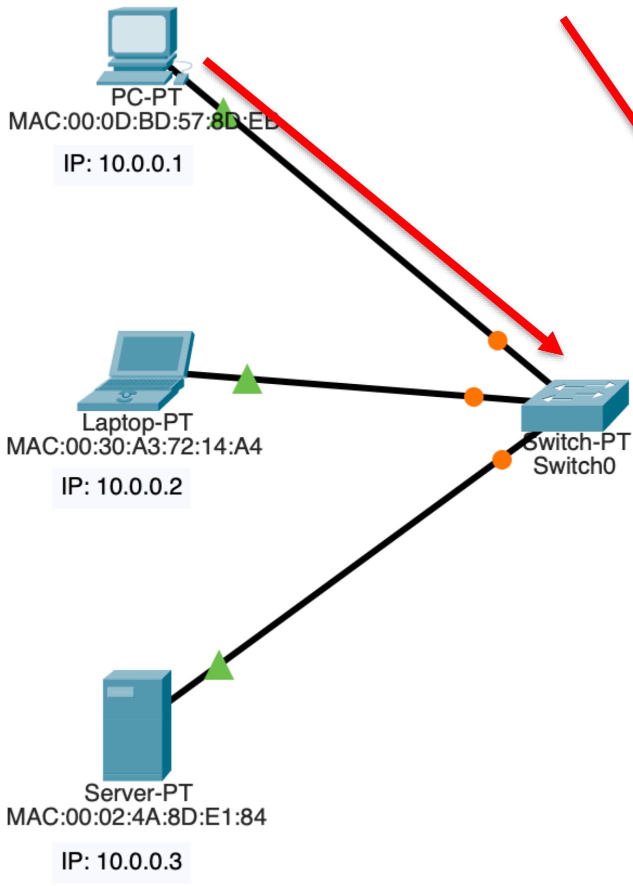
Layer 2 payload

Payload is a Layer 3 packet

But Switch only knows Layer 2

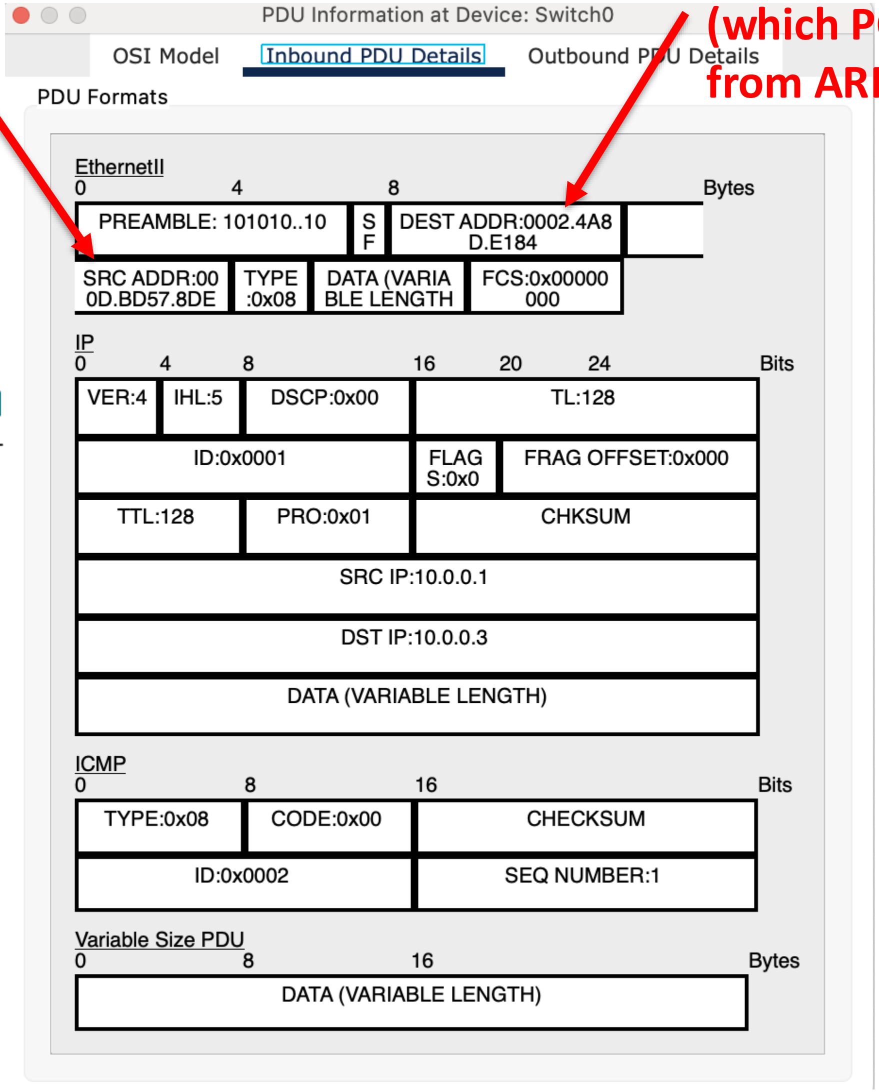
Forwards frame to Server

PC now knows the Server’s MAC and can send ICMP echo request (ping) Layer 3



From PC

To Server MAC (which PC learned from ARP reply)



PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:0002.4A8D.E184

SRC ADDR:000D.BD57.8DE | TYPE:0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x0001 | FLAGS:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

SRC IP:10.0.0.1

DST IP:10.0.0.3

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

TYPE:0x08 | CODE:0x00 | CHECKSUM

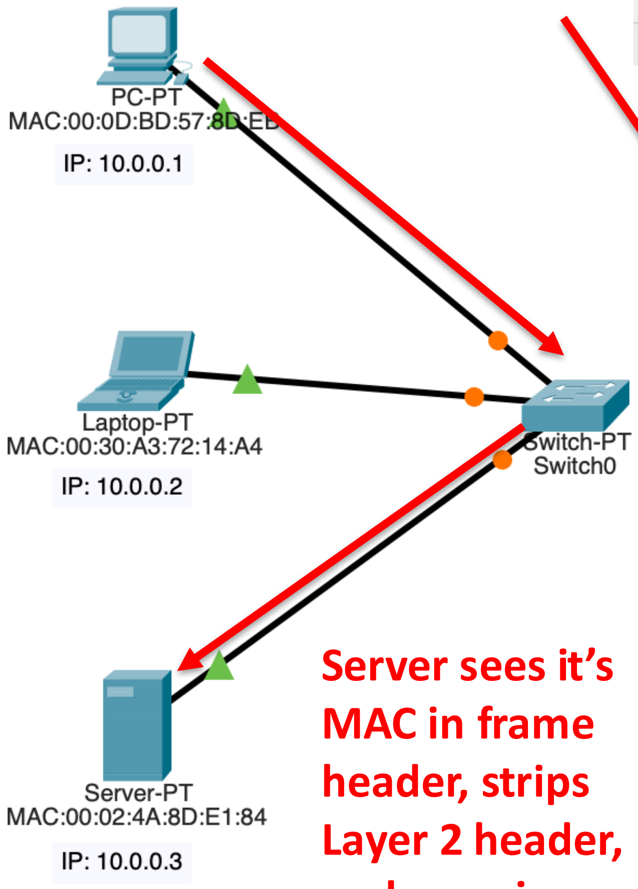
ID:0x0002 | SEQ NUMBER:1

Variable Size PDU

0 8 16 Bytes

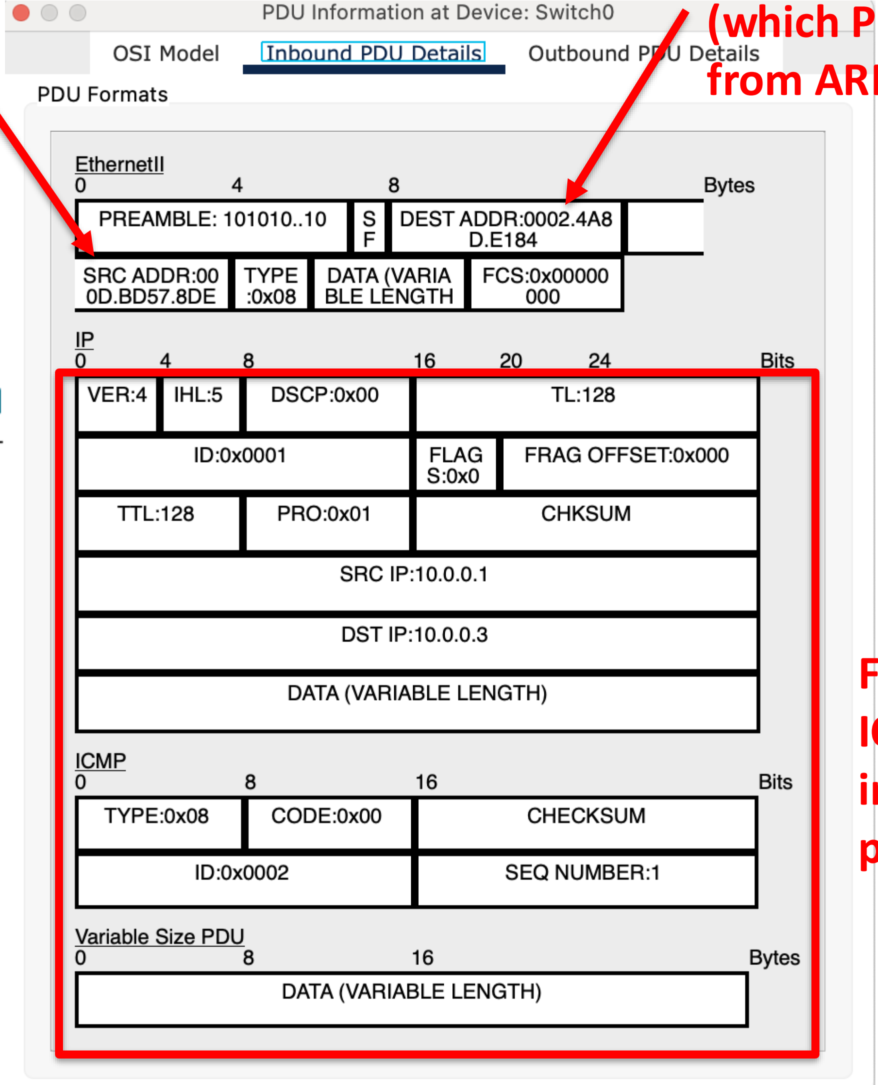
DATA (VARIABLE LENGTH)

Server sees its MAC in Layer 2 header and examines payload, finds Layer 3 packet



From PC

To Server MAC (which PC learned from ARP reply)



PDU Information at Device: Switch0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII
0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:0002.4A8D.E184
SRC ADDR:000D.BD57.8DE | TYPE:0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

IP
0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128
ID:0x0001 | FLAGS:0x0 | FRAG OFFSET:0x000
TTL:128 | PRO:0x01 | CHKSUM
SRC IP:10.0.0.1
DST IP:10.0.0.3
DATA (VARIABLE LENGTH)

ICMP
0 8 16 Bits

TYPE:0x08 | CODE:0x00 | CHECKSUM
ID:0x0002 | SEQ NUMBER:1

Variable Size PDU
0 8 16 Bytes

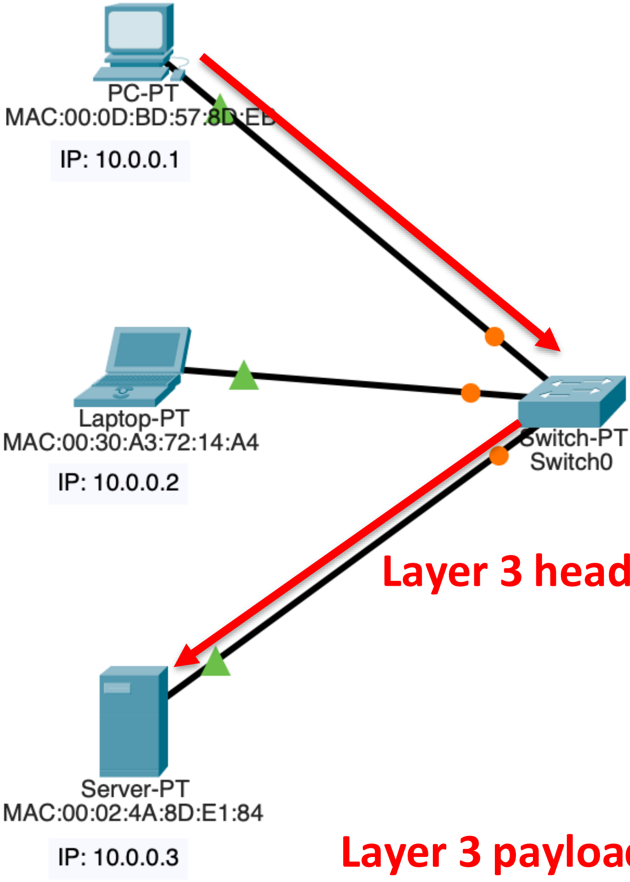
DATA (VARIABLE LENGTH)

Did Laptop see the ping request? No, switch send to Server only

Server sees it's MAC in frame header, strips Layer 2 header, and examines frame payload

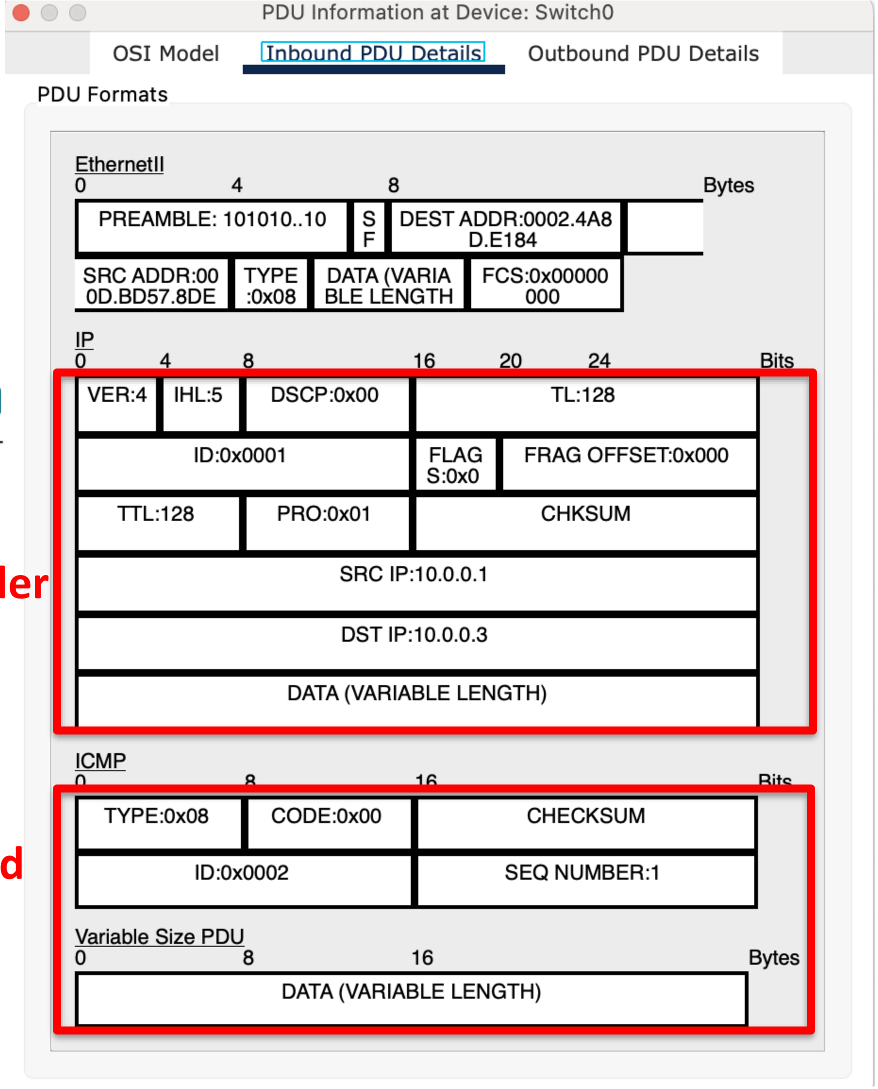
Finds Layer 3 ICMP packet inside Layer 2 payload

Server sees its MAC in Layer 2 header and examines payload, finds Layer 3 packet



Layer 3 header

Layer 3 payload



PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10	SF	DEST ADDR:0002.4A8D.E184	
SRC ADDR:000D.BD57.8DE	TYPE:0x08	DATA (VARIABLE LENGTH	FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4	IHL:5	DSCP:0x00	TL:128	
ID:0x0001			FLAGS:0x0	FRAG OFFSET:0x000
TTL:128		PRO:0x01	CHKSUM	
SRC IP:10.0.0.1				
DST IP:10.0.0.3				
DATA (VARIABLE LENGTH)				

ICMP

0 8 16 Bits

TYPE:0x08	CODE:0x00	CHECKSUM
ID:0x0002		SEQ NUMBER:1

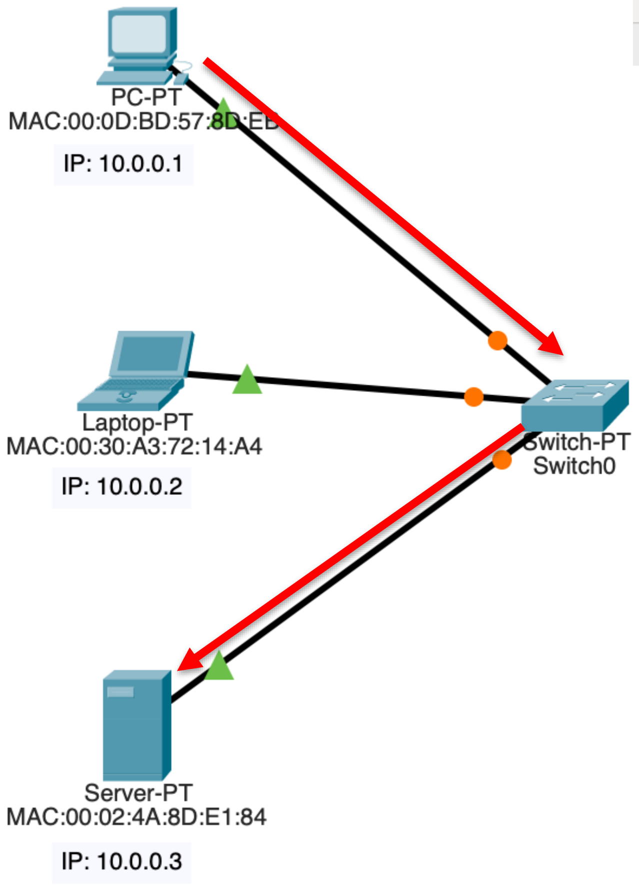
Variable Size PDU

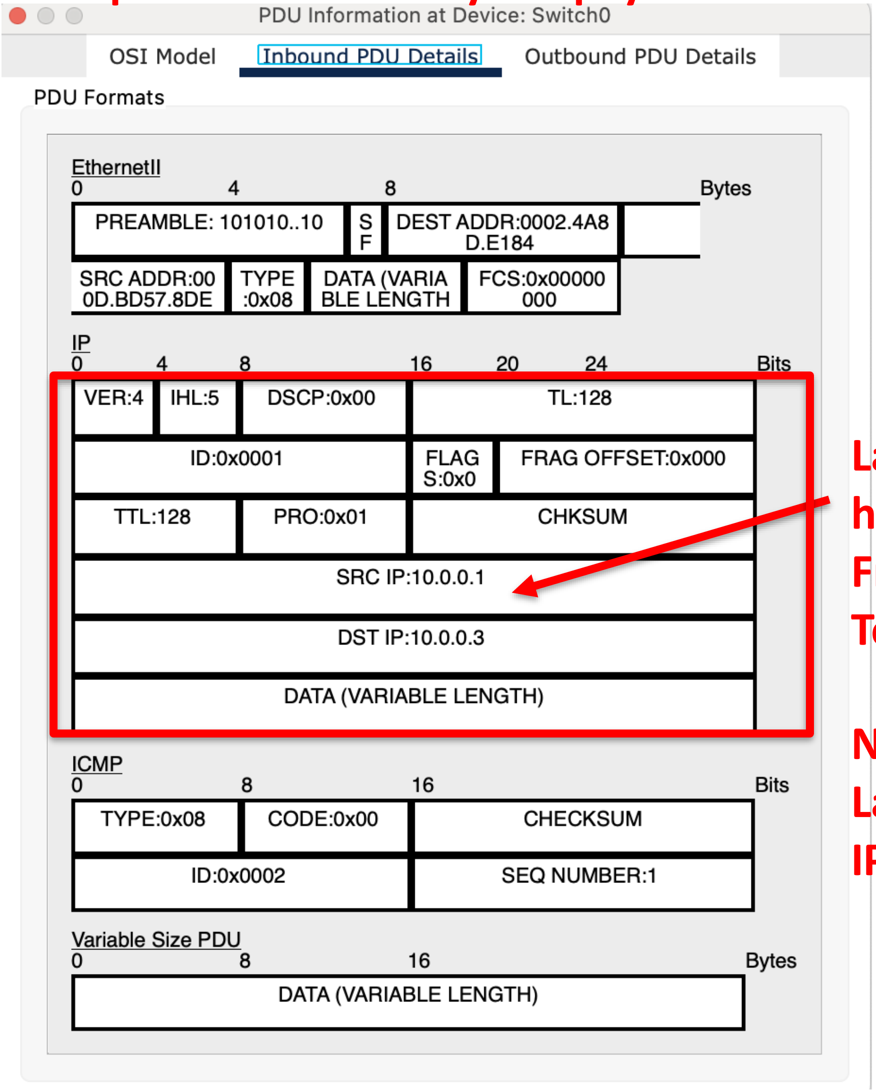
0 8 16 Bytes

DATA (VARIABLE LENGTH)

Server sees its MAC in Layer 2 header and examines payload, finds Layer 3 packet

Layer 3 packet encapsulated inside Layer 2 payload





PDU Information at Device: Switch0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:0002.4A8D.E184

SRC ADDR:000D.BD57.8DE | TYPE :0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x0001 | FLAGS:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

SRC IP:10.0.0.1

DST IP:10.0.0.3

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

TYPE:0x08 | CODE:0x00 | CHECKSUM

ID:0x0002 | SEQ NUMBER:1

Variable Size PDU

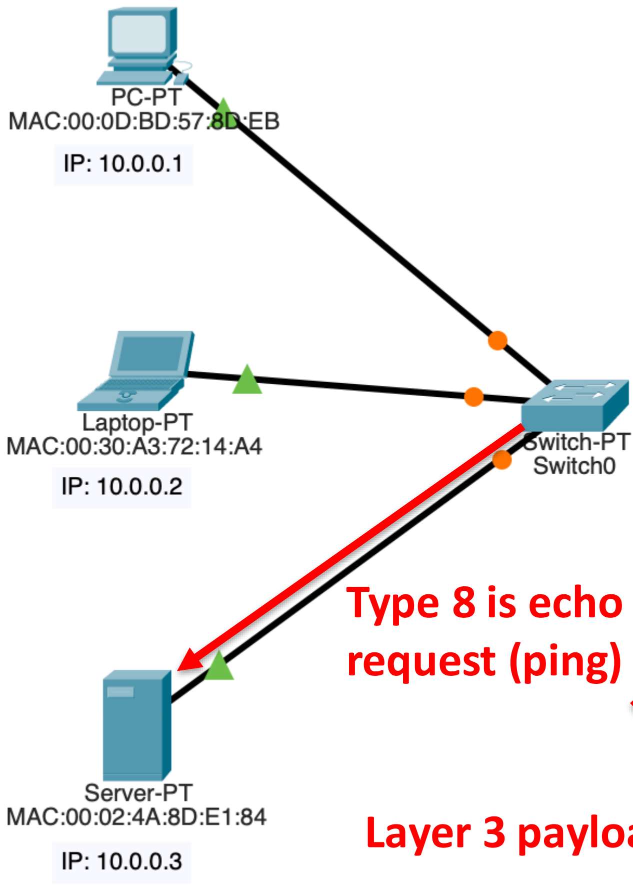
0 8 16 Bytes

DATA (VARIABLE LENGTH)

Layer 3 header From PC To Server

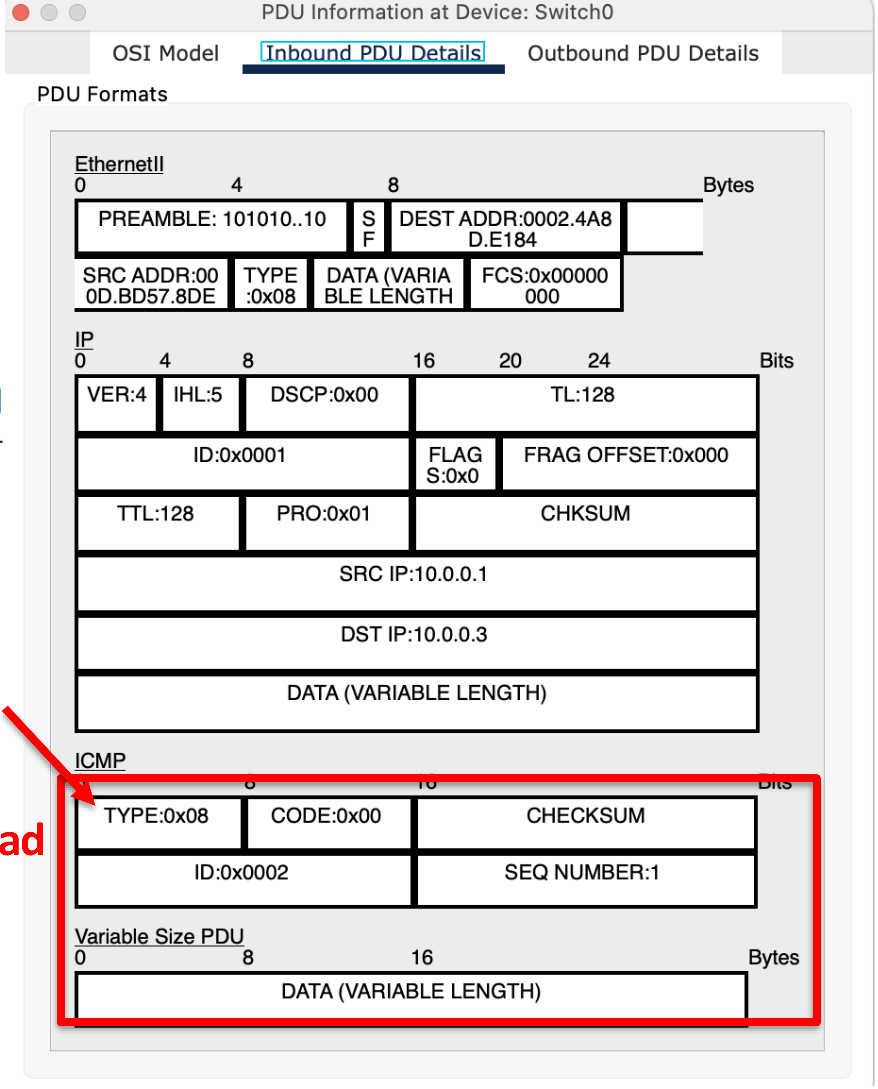
No MACs are Layer 3, only IP

Server finds ICMP request in Layer 3 payload



Type 8 is echo request (ping)

Layer 3 payload



PDU Formats

EthernetII
0 4 8 Bytes

PREAMBLE: 101010..10 | SF | DEST ADDR:0002.4A8D.E184

SRC ADDR:000D.BD57.8DE | TYPE:0x08 | DATA (VARIABLE LENGTH | FCS:0x00000000

IP
0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x0001 | FLAGS:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

SRC IP:10.0.0.1

DST IP:10.0.0.3

DATA (VARIABLE LENGTH)

ICMP
8 16 Bits

TYPE:0x08 | CODE:0x00 | CHECKSUM

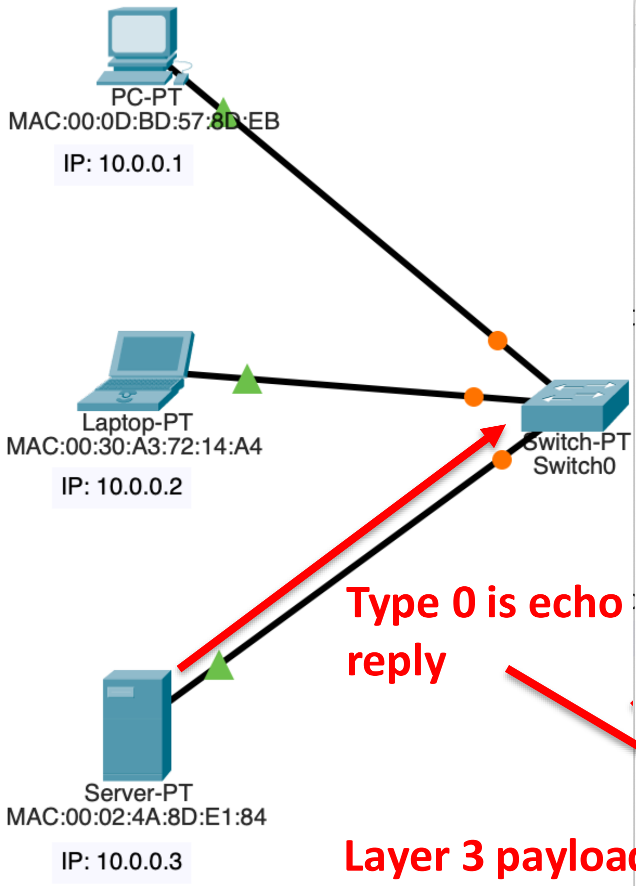
ID:0x0002 | SEQ NUMBER:1

Variable Size PDU
0 8 16 Bytes

DATA (VARIABLE LENGTH)

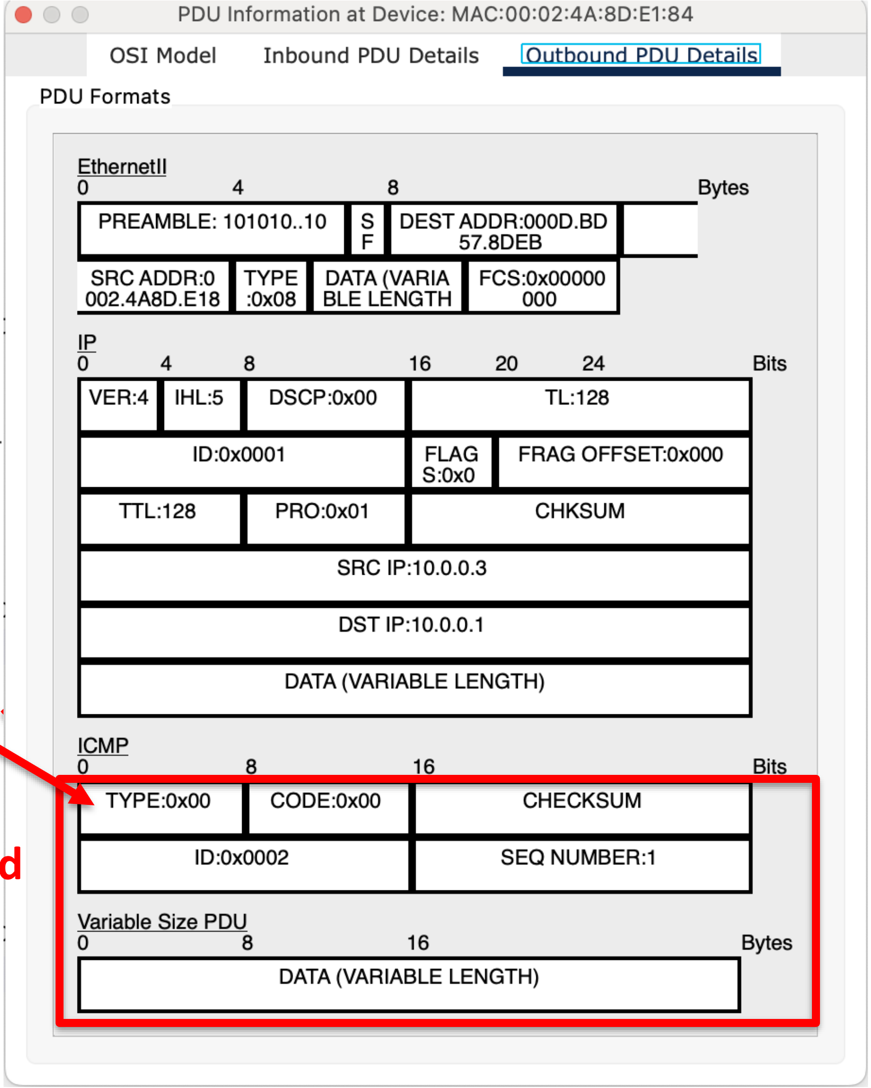
Type	Code	description
0	0	echo reply (ping)
8	0	echo request (ping)

Server replies to ICMP echo request (ping) with ICMP echo reply



Type 0 is echo reply

Layer 3 payload



PDU Information at Device: MAC:00:02:4A:8D:E1:84

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII

0	4	8	Bytes
PREAMBLE: 101010..10	S F	DEST ADDR:000D.BD 57.8DEB	
SRC ADDR:0 002.4A8D.E18	TYPE :0x08	DATA (VARIA BLE LENGTH	FCS:0x00000 000

IP

0	4	8	16	20	24	Bits
VER:4	IHL:5	DSCP:0x00	TL:128			
ID:0x0001			FLAG S:0x0	FRAG OFFSET:0x000		
TTL:128		PRO:0x01	CHKSUM			
SRC IP:10.0.0.3						
DST IP:10.0.0.1						
DATA (VARIABLE LENGTH)						

ICMP

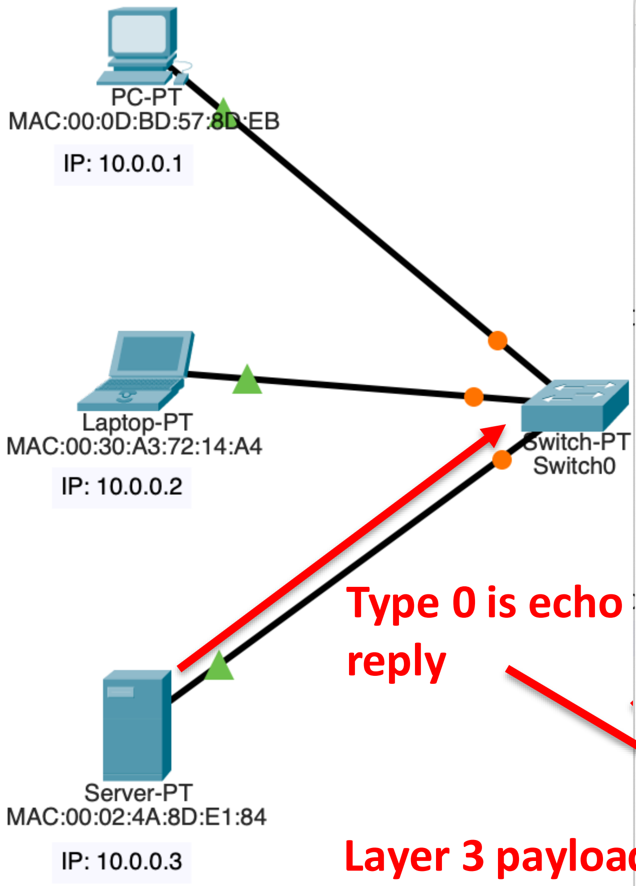
0	8	16	Bits
TYPE:0x00	CODE:0x00	CHECKSUM	
ID:0x0002		SEQ NUMBER:1	

Variable Size PDU

0	8	16	Bytes
DATA (VARIABLE LENGTH)			

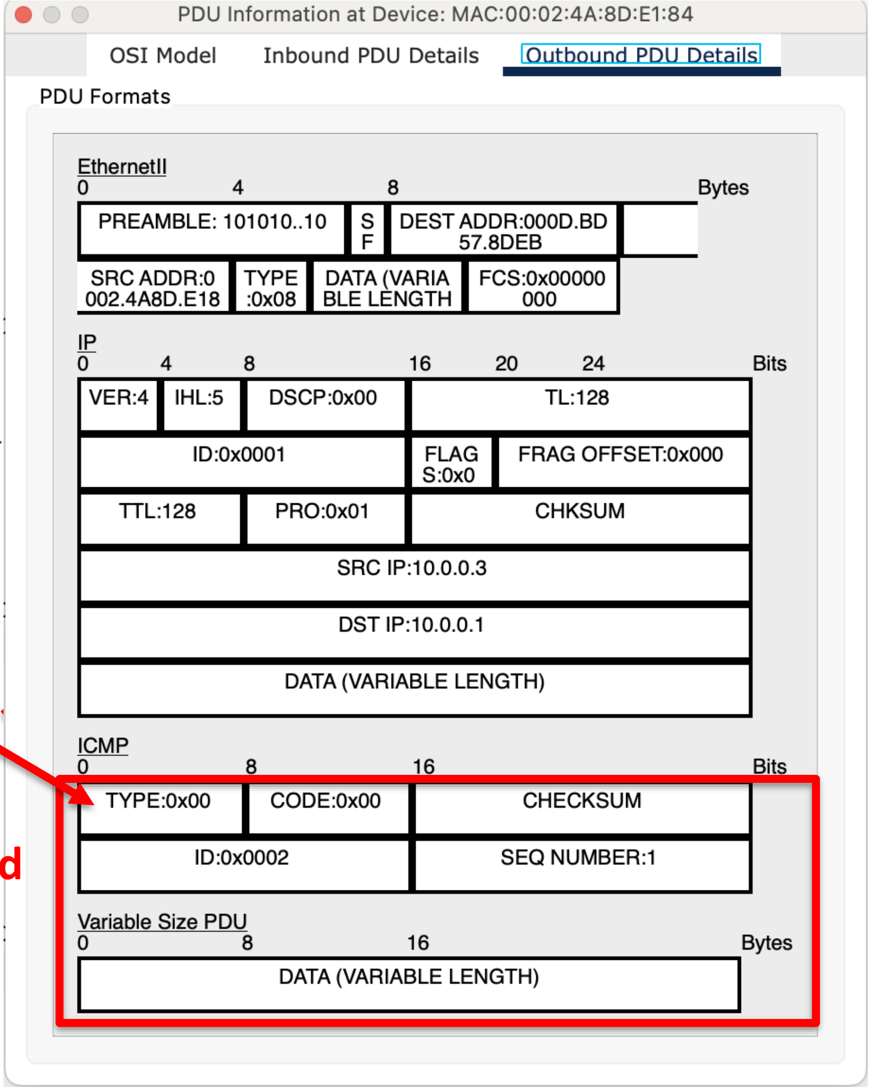
Type	Code	description
0	0	echo reply (ping)
8	0	echo request (ping)

Server replies to ICMP echo request (ping) with ICMP echo reply



Type 0 is echo reply

Layer 3 payload


PDU Information at Device: MAC:00:02:4A:8D:E1:84

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | S F | DEST ADDR:000D.BD 57.8DEB

SRC ADDR:0 002.4A8D.E18 | TYPE :0x08 | DATA (VARIA BLE LENGTH | FCS:0x00000 000

IP

0 4 8 16 20 24 Bits

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x0001 | FLAG S:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

SRC IP:10.0.0.3

DST IP:10.0.0.1

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

TYPE:0x00 | CODE:0x00 | CHECKSUM

ID:0x0002 | SEQ NUMBER:1

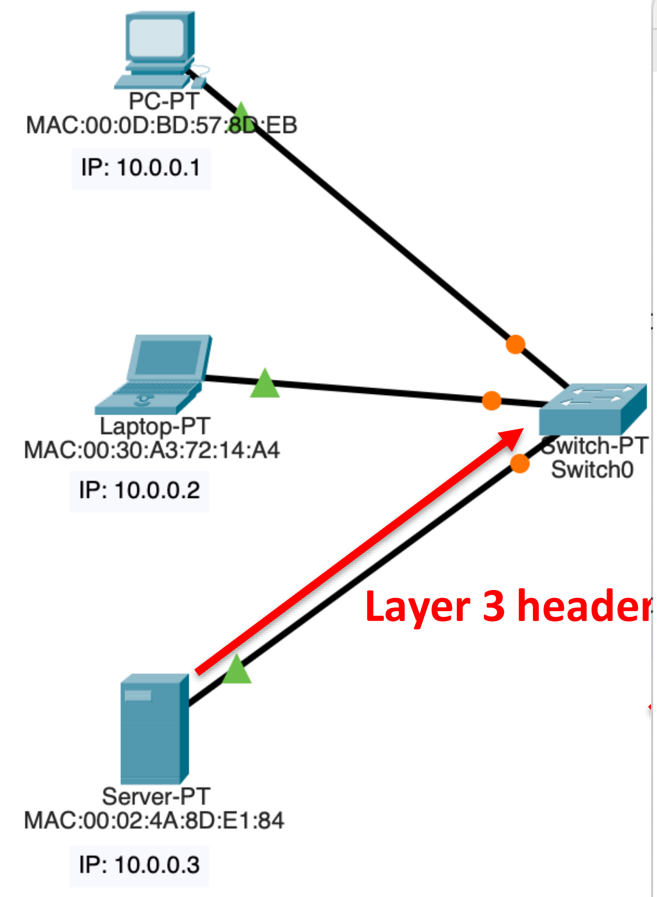
Variable Size PDU

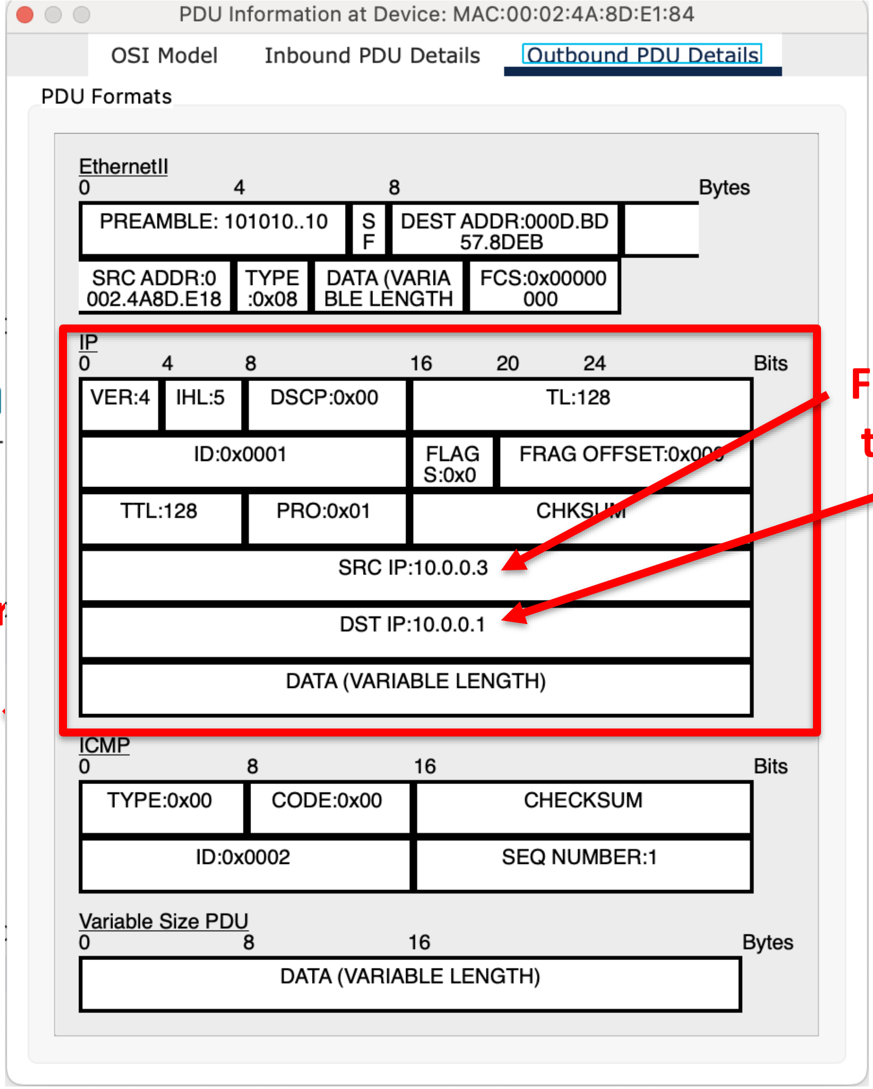
0 8 16 Bytes

DATA (VARIABLE LENGTH)

Type	Code	description
0	0	echo reply (ping)
8	0	echo request (ping)

Server encapsulates Layer 3 ICMP reply packet as payload inside Layer 2 frame





PDU Information at Device: MAC:00:02:4A:8D:E1:84

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10	S F	DEST ADDR:000D.BD 57.8DEB	
SRC ADDR:0 002.4A8D.E18	TYPE :0x08	DATA (VARIA BLE LENGTH	FCS:0x00000 000

IP

0 4 8 16 20 24 Bits

VER:4	IHL:5	DSCP:0x00	TL:128
ID:0x0001		FLAG S:0x0	FRAG OFFSET:0x000
TTL:128	PRO:0x01	CHKSUM	
SRC IP:10.0.0.3			
DST IP:10.0.0.1			
DATA (VARIABLE LENGTH)			

ICMP

0 8 16 Bits

TYPE:0x00	CODE:0x00	CHECKSUM
ID:0x0002		SEQ NUMBER:1

Variable Size PDU

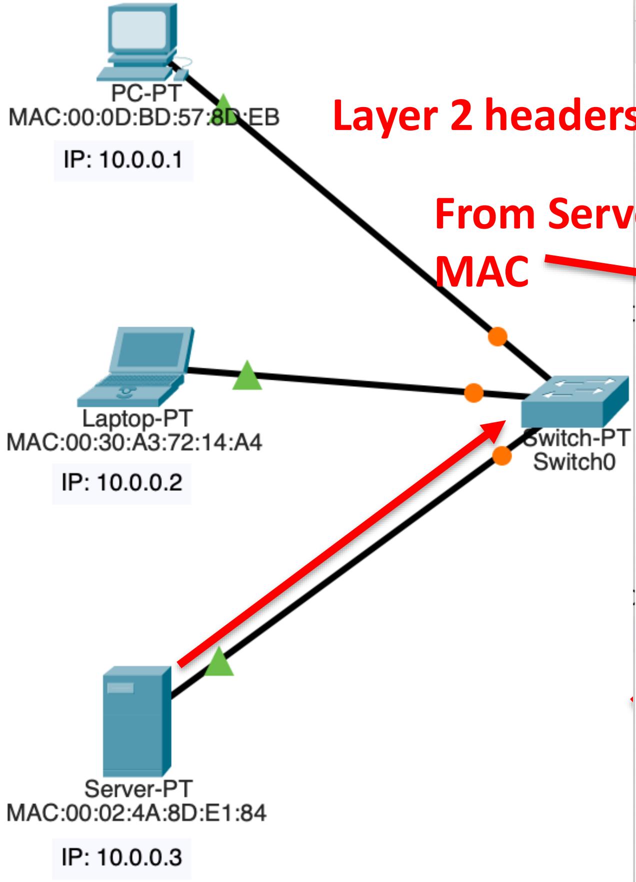
0 8 16 Bytes

DATA (VARIABLE LENGTH)

From Server IP to PC IP

Type	Code	description
0	0	echo reply (ping)
8	0	echo request (ping)

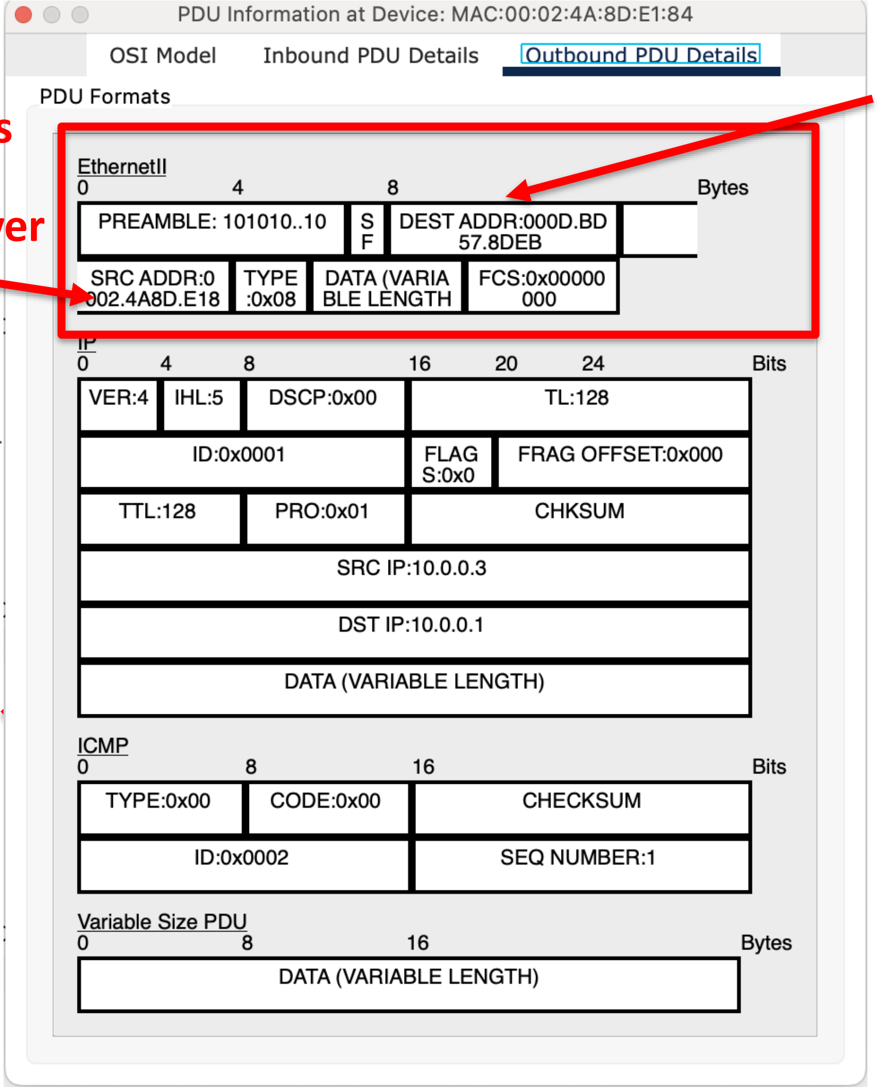
Server adds Layer 2 headers



Layer 2 headers

From Server MAC

To PC MAC



PDU Information at Device: MAC:00:02:4A:8D:E1:84

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10	SF	DEST ADDR:000D.BD57.8DEB	
SRC ADDR:0002.4A8D.E18	TYPE :0x08	DATA (VARIABLE LENGTH	FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4	IHL:5	DSCP:0x00	TL:128	
ID:0x0001			FLAGS:0x0	FRAG OFFSET:0x000
TTL:128		PRO:0x01	CHKSUM	
SRC IP:10.0.0.3				
DST IP:10.0.0.1				
DATA (VARIABLE LENGTH)				

ICMP

0 8 16 Bits

TYPE:0x00	CODE:0x00	CHECKSUM
ID:0x0002		SEQ NUMBER:1

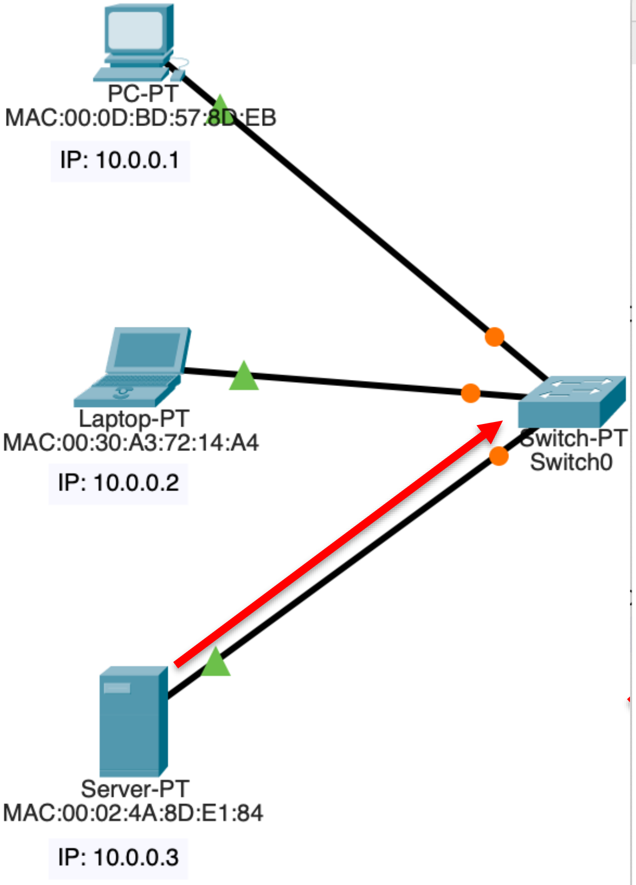
Variable Size PDU

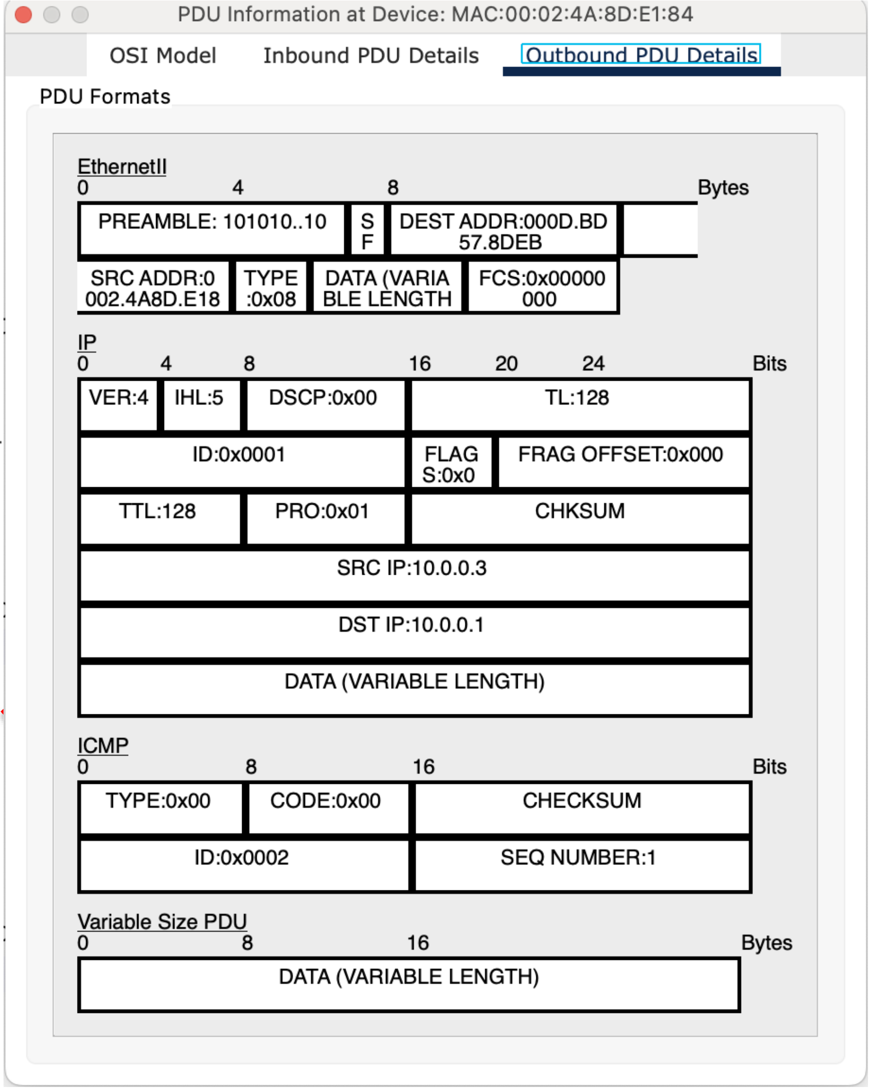
0 8 16 Bytes

DATA (VARIABLE LENGTH)

Type	Code	description
0	0	echo reply (ping)
8	0	echo request (ping)

Server sends frame to Switch





PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10	S F	DEST ADDR:000D.BD 57.8DEB	
SRC ADDR:0 002.4A8D.E18	TYPE :0x08	DATA (VARIA BLE LENGTH	FCS:0x00000 000

IP

0 4 8 16 20 24 Bits

VER:4	IHL:5	DSCP:0x00	TL:128
ID:0x0001		FLAG S:0x0	FRAG OFFSET:0x000
TTL:128	PRO:0x01	CHKSUM	
SRC IP:10.0.0.3			
DST IP:10.0.0.1			
DATA (VARIABLE LENGTH)			

ICMP

0 8 16 Bits

TYPE:0x00	CODE:0x00	CHECKSUM
ID:0x0002		SEQ NUMBER:1

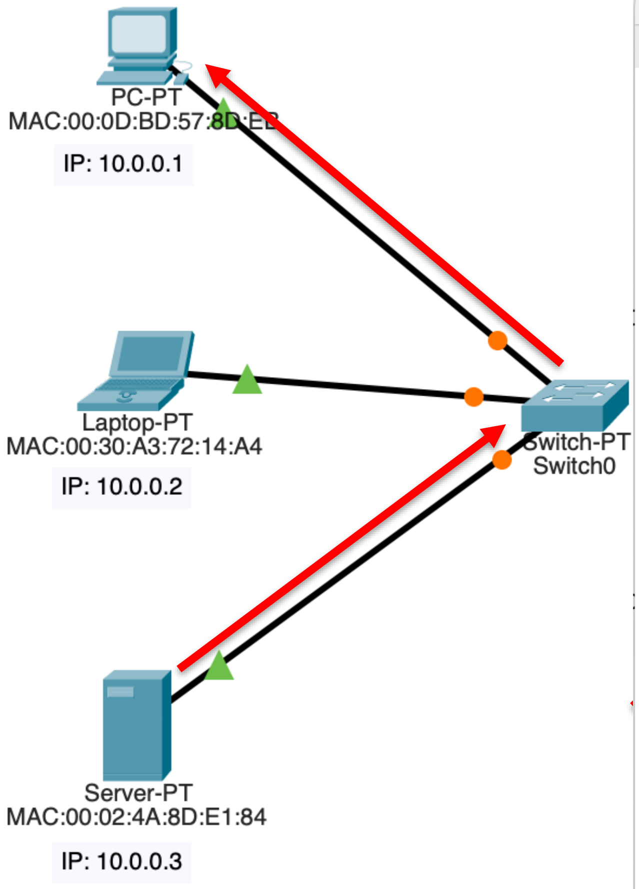
Variable Size PDU

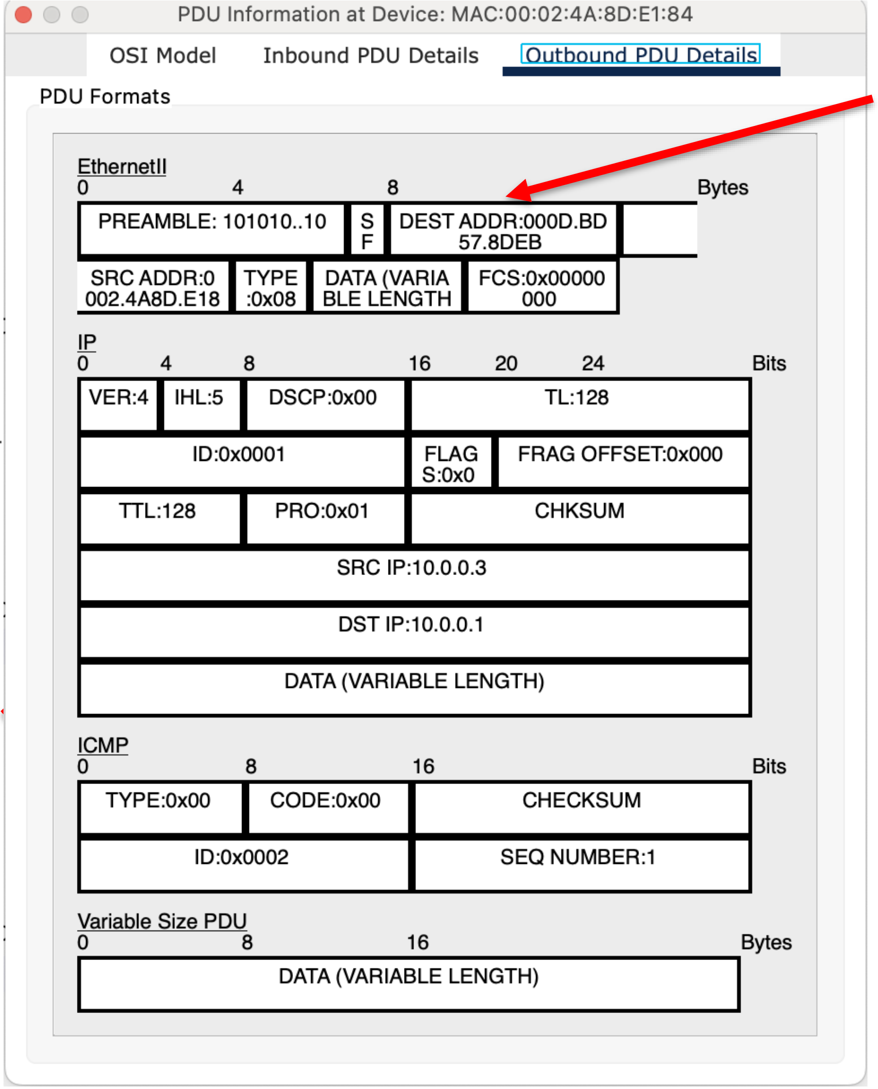
0 8 16 Bytes

DATA (VARIABLE LENGTH)

Type	Code	description
0	0	echo reply (ping)
8	0	echo request (ping)

Switch looks at Layer 2 headers, sends frame to PC





PDU Information at Device: MAC:00:02:4A:8D:E1:84

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10	SF	DEST ADDR:000D.BD57.8DEB	
SRC ADDR:0002.4A8D.E18	TYPE:0x08	DATA (VARIABLE LENGTH	FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4	IHL:5	DSCP:0x00	TL:128
ID:0x0001		FLAGS:0x0	FRAG OFFSET:0x000
TTL:128	PRO:0x01	CHKSUM	
SRC IP:10.0.0.3			
DST IP:10.0.0.1			
DATA (VARIABLE LENGTH)			

ICMP

0 8 16 Bits

TYPE:0x00	CODE:0x00	CHECKSUM
ID:0x0002		SEQ NUMBER:1

Variable Size PDU

0 8 16 Bytes

DATA (VARIABLE LENGTH)

To PC MAC

Type	Code	description
0	0	echo reply (ping)
8	0	echo request (ping)

Agenda

1. Network layer overview

2. Ping and ARP

3. DHCP

4. Exercises

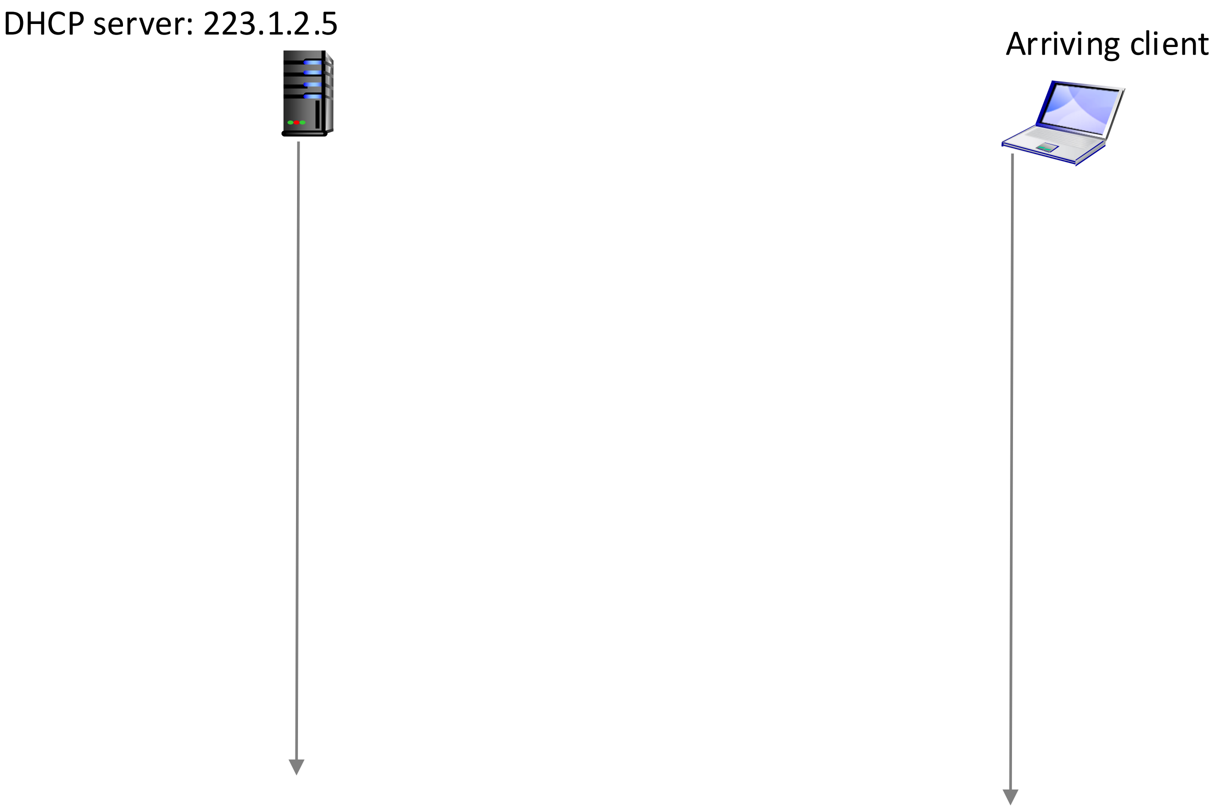
Two ways to an IP address: static or dynamic (DHCP)

Two ways to get an IP address:

1. Manually set a static IP
   - In the old days, a network admin manually set the IP for each host
   - Sometimes done today for things that shouldn’t change IP address like servers

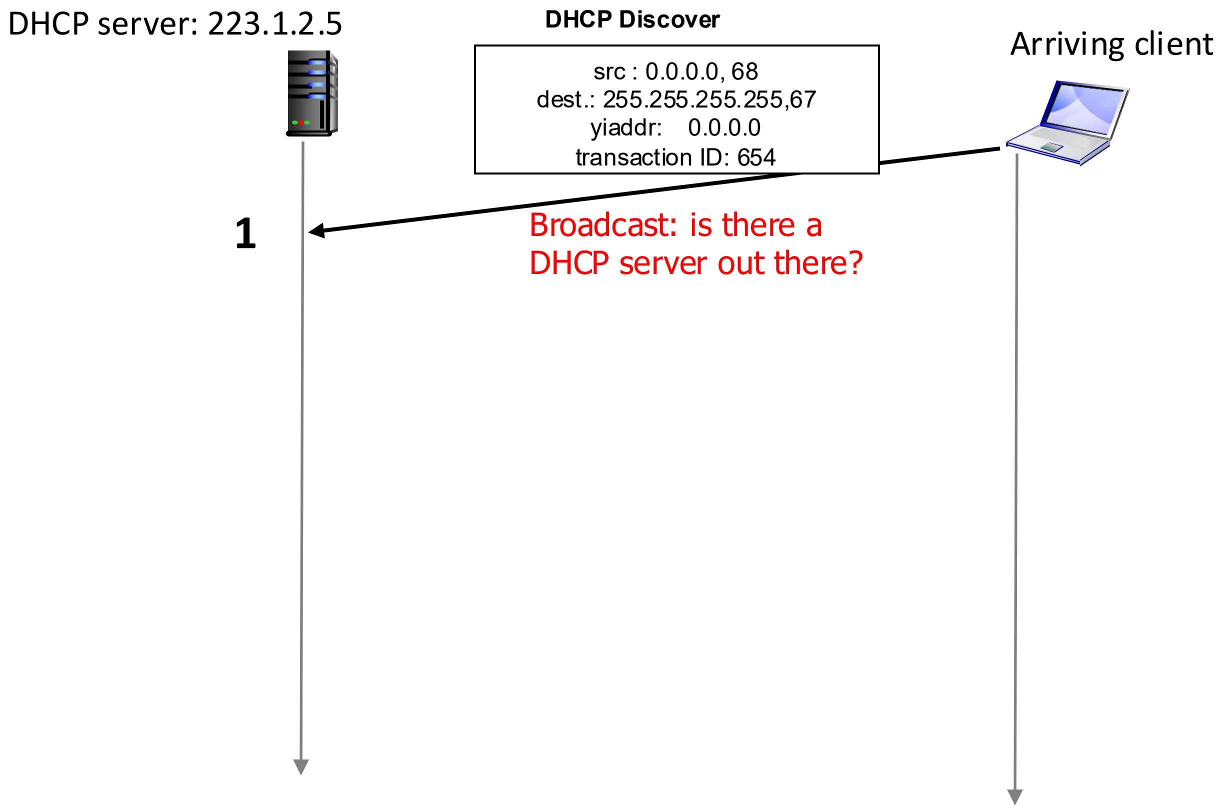
2. Use Dynamic Host Configuration Protocol (DHCP)
   - Assign a server to give out IP addresses from a pool
   - When hosts join the network, DHCP server gives it an IP address not already in use
   - Each IP has a lease with an expiration time so the IP address assign will expire (in case a device leaves the network)
   - Hosts can renew their lease

DHCP: Client wants to get an IP address, but doesn't know about DHCP server



Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

DHCP: 1) Arriving client sends DHCP Discover packet to broadcast



DHCP server: 223.1.2.5

DHCP Discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

Arriving client

1

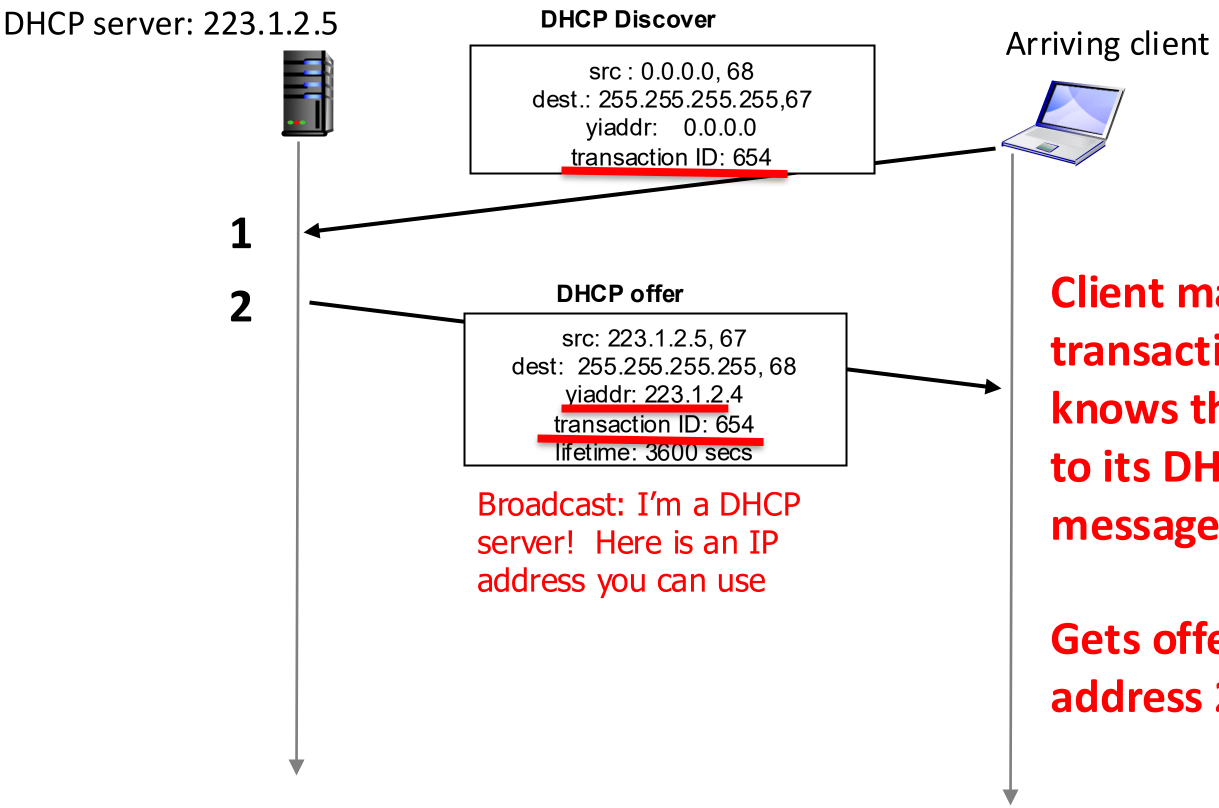
Broadcast: is there a DHCP server out there?

Why is src IP address 0.0.0.0?

Why is dst 255.255.255.255?

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

DHCP: 2) DHCP server replies with DHCP Offer packet



DHCP Discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

DHCP offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

Broadcast: I'm a DHCP server! Here is an IP address you can use

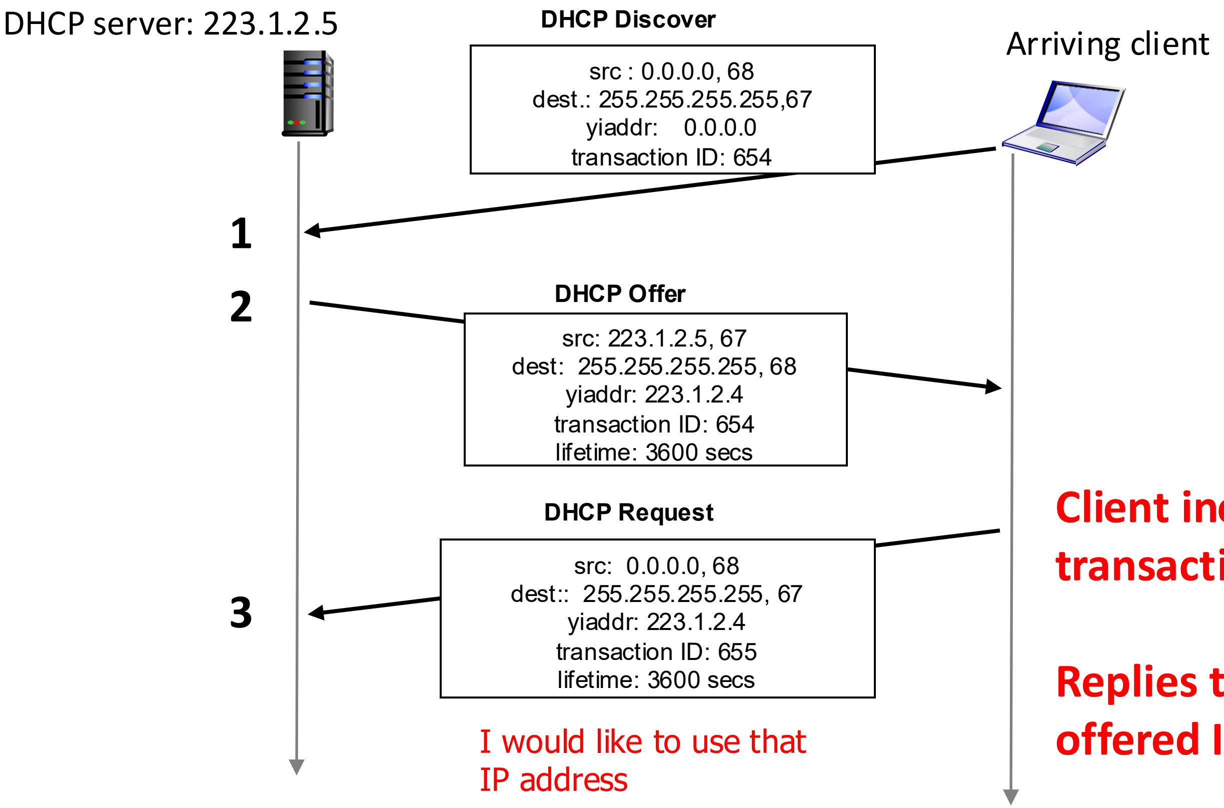
Client matches transaction ID so it knows this is a reply to its DHCP Discover message

Gets offered IP address 223.1.2.4

Note: clients use port 68, servers use port 67
More on ports soon

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

DHCP: 3) Client replies with DHCP Request to take the offered IP address



DHCP server: 223.1.2.5

Arriving client

DHCP Discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

1

2

DHCP Offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

DHCP Request

src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

3

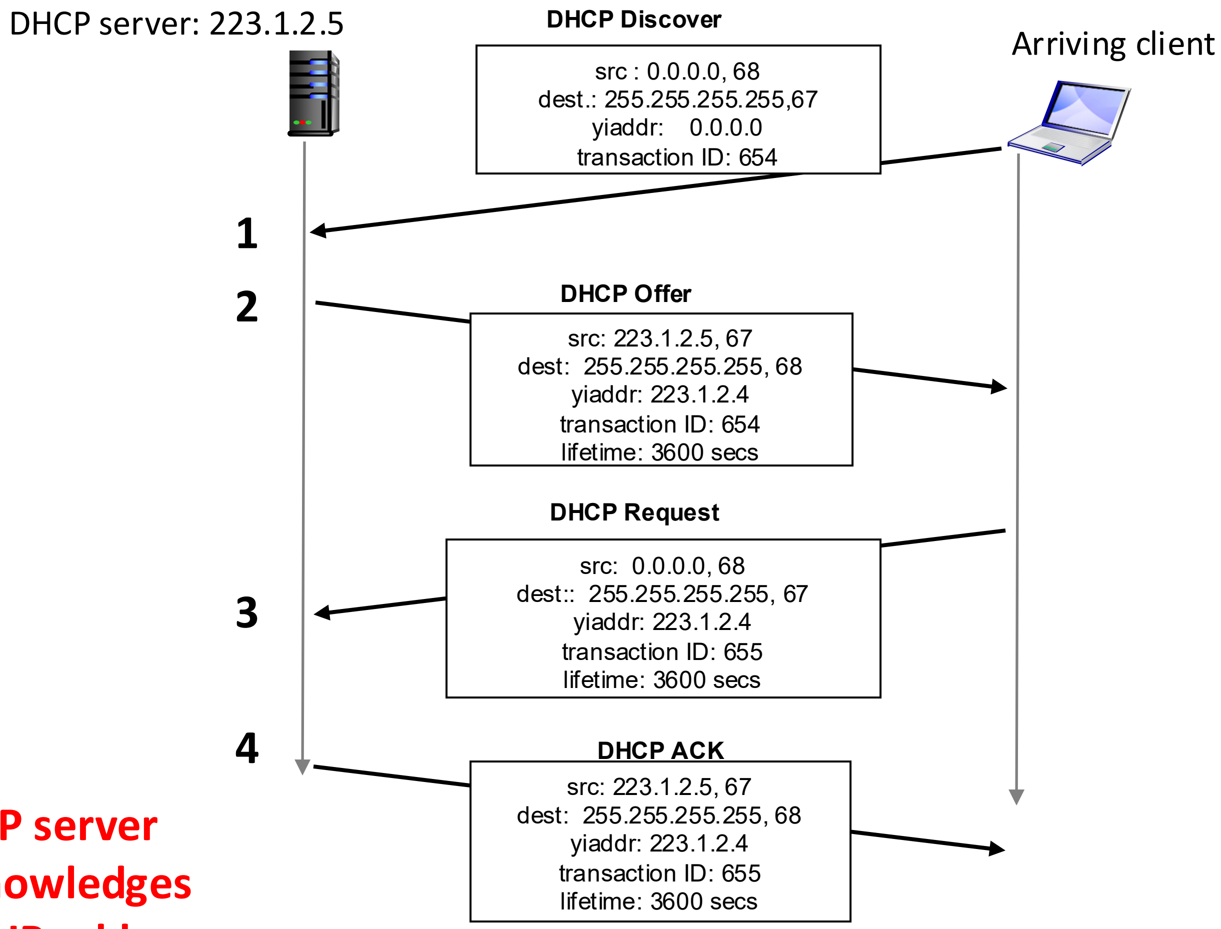
I would like to use that IP address

Client increments transaction ID

Replies that it will take the offered IP address 223.1.2.4

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

DHCP: 4) DHCP acknowledges client has new IP address with DHCP ACK



DHCP Discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

DHCP Offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

DHCP Request

src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP ACK

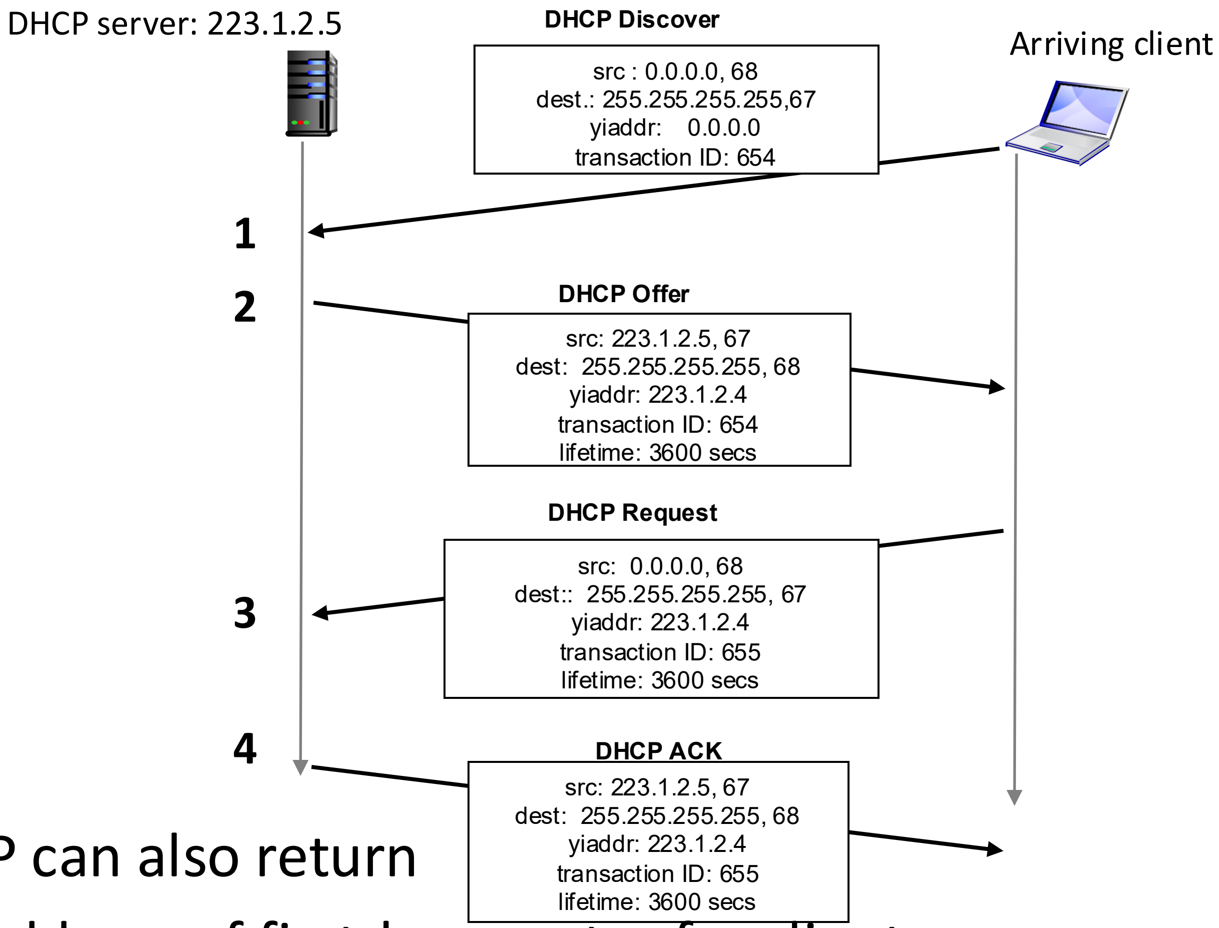
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP server acknowledges new IP address

Ok, you've got that IP address

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

DHCP: 4) DHCP acknowledges client has new IP address with DHCP ACK



DHCP Discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

DHCP Offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

DHCP Request

src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

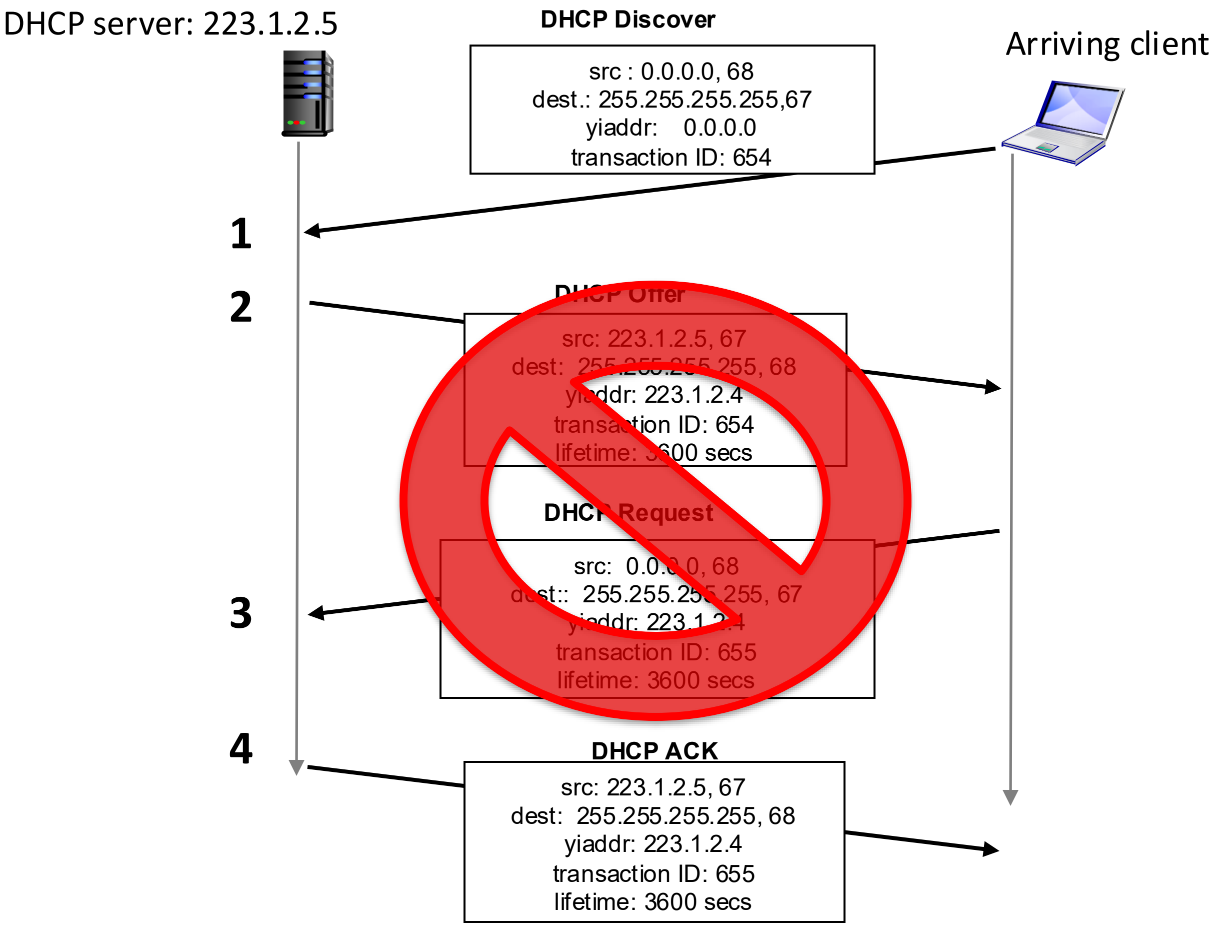
DHCP ACK

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP can also return

- Address of first-hop router for client
- Name and IP address of DNS sever
- Network mask (indicating network versus host portion of address)

DHCP: 4) DHCP acknowledges client has new IP address with DHCP ACK



DHCP server: 223.1.2.5

Arriving client

1

DHCP Discover

src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

2

DHCP Offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

3

DHCP Request

src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

4

DHCP ACK

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

Step 2 and 3 can be skipped "if a client remembers and wishes to reuse a previously allocated network address" [RFC 2131]
Dartmouth remembers your MAC

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Agenda

1. Network layer overview

2. Ping and ARP

3. DHCP

4. Exercises

Exercises

How does your computer get a MAC address? What is your MAC address?

How does your computer get an IP address? What is your IP address?

Start Wireshark capturing in your VM (blue fin at top)

- Ping 8.8.8.8 (let it run for a few pings)
- Stop Wireshark (red block at top)
- Set Wireshark filter ip.addr == 8.8.8.8 (Google)
- See ICMP requests from your computer and ICMP reply from Google
- Look at Layer 2 and Layer 3 for each line

Start Wireshark capturing again

- Start browser and go to https://vibrantcloud.org/ (might have to refresh browser)
- Stop Wireshark capture
- Set Wireshark filter to http
- Find the request your browser made for the web page
- See the web server’s response
- Look at the Layer 2 to 7
- Find the web page’s HTML text

Turn off Wi-Fi, Start Wireshark, turn on Wi-Fi, filter on DHCP to see request