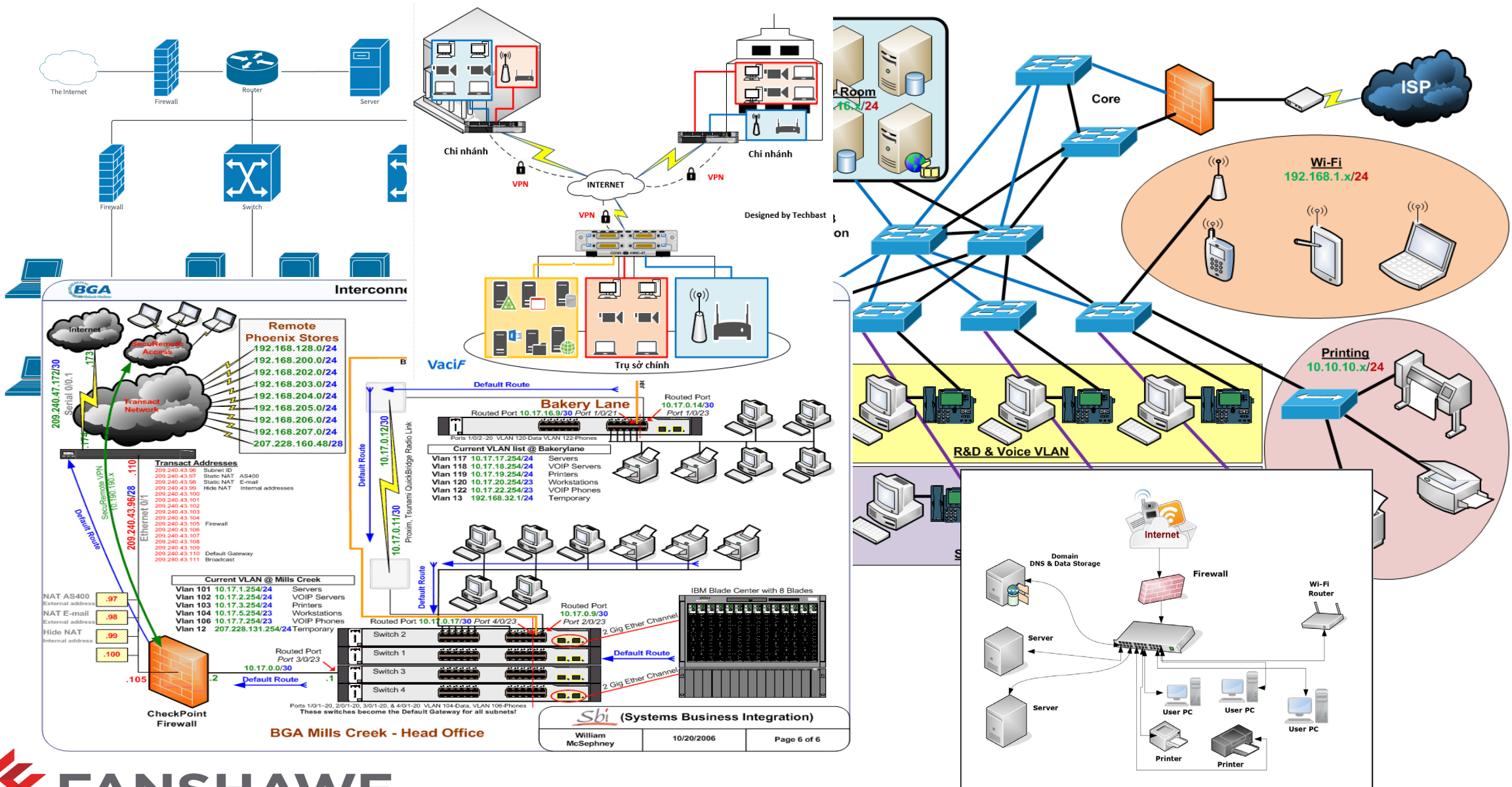


Introduction - 01

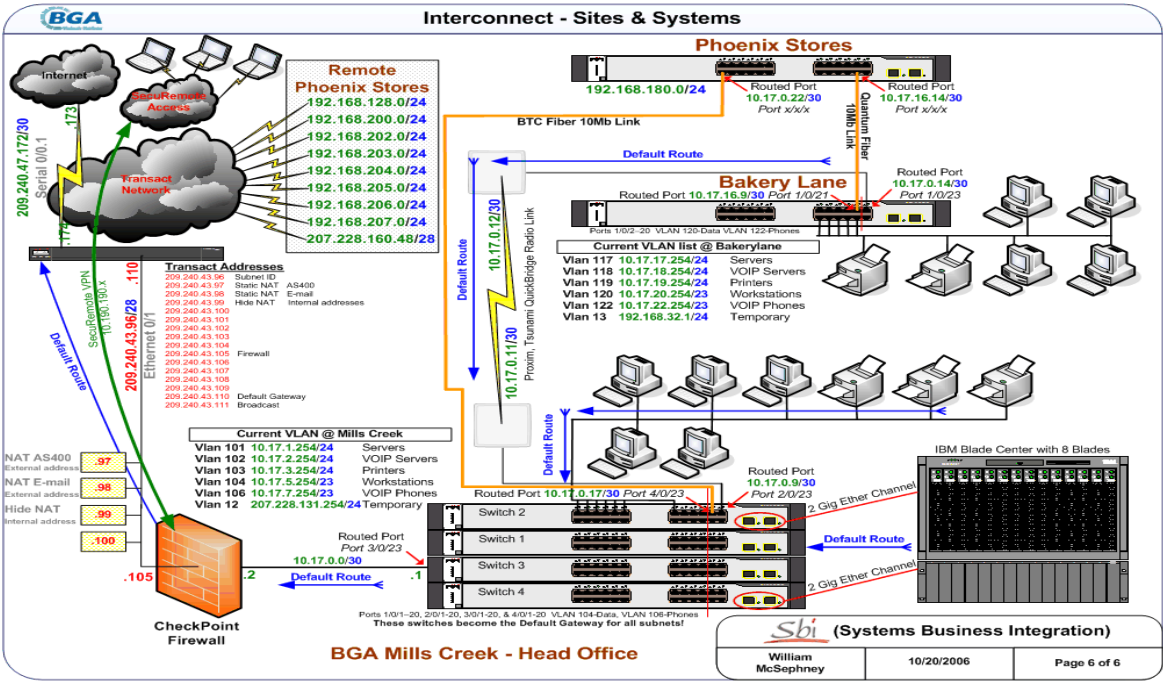


Summery - Introduction -01

- Calendar
- Professor
- Class Times
- Environment
- Equipment
- Your Equipment
- Some History (History of the Ethernet Video)
- OSI Model vs TCP Model
- OSI Model
- TCP/IP Communication Process
- Collision Domain
- Broadcast Domains
- Switches & Duplex
- MDI & MDI-X Auto
- Complexity of Networks
- Borderless Switched Networks
- Role of Switched Networks
- Tools and Commands
- Configuring your PC for the Lab
- Lab
- Cleaning out your switches & Routers

House Keeping

- Packet Tracer (PT)
- Wireshark
- Local Loopback
- Ping
- Ping (Extended/Enhanced)
- Traceroute
- CDP (Cisco Discovery Protocol)
- LLDP (Link Layer Discovery Protocol)
- Telnet
- Troubleshooting



House Keeping (continued)

- Professor
- Jeff Grose
Contact: j_grose@fanshaweonline.ca
- E-mails must come from the students fanshaweonline.ca account.
- Email must have a subject that includes
 - Subject: "INFO-6047-**xx** <then your subject>"
 - Where **xx** is your **section number**
- If your subject line is not configured as above, **your message will be ignored!**

House Keeping (continued)

- Class Times
- Wednesdays I will be posting the weekly lecture
- I will release the Lab and lab quiz the same day
- For each lab there is a quiz that will be available from Wednesday through to Sunday evening at 23:59 EDT (12 labs & Lab Quizzes @ 3% each = 36%)
- Exams will be held during week 7 and 15. Check the weekly content in FOL for details of the exams/tests (2 exams/test @ 32% each = 64%)

House Keeping (continued)

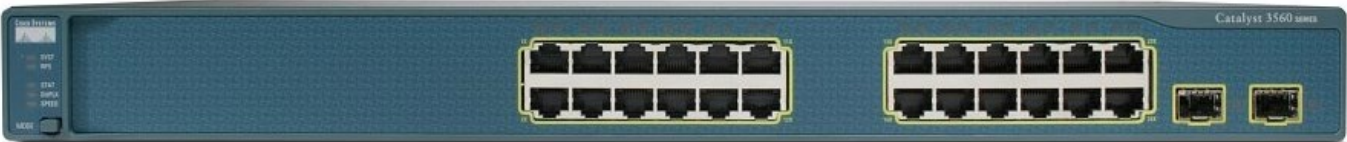
- Environment
- Lab time:
 - 3 hours of lab in class(lab quiz, to be completed by the end of the lab time)
 - Lab full of Cisco equipment for doing the labs
- Lectures
 - Will be recorded and posted to the appropriate section of FOL
(BUT there may be parts of the lecture not included in the recordings...)
- Labs are written for both the normal classes (in-house) and on-line students
 - Will walk you through the configuration of the equipment in the labs
 - Labs are designed to cover what we talked about during the lecture for that week
 - Labs may or may not cover the reading material for the week

House Keeping (continued)

- Environment (continued)
- Quizzes
 - There will be a quiz for each Lab (12 labs = 12 quizzes x 3% = 36% of you final grade)
 - Quizzes are 10 minute (10 Point “**NOT 10 questions**”)
 - Quizzes will cover that weeks Lecture / Lab / and **Reading Material**
 - Quizzes can be done any time in the 85 hours plus after the lab and quiz open. The catch is you get one chance to do the quiz and only 10 minutes to finish once you start.
 - If you miss a quiz, you miss the quiz! **You lose that 3% of your final grade!**
- Exams
 - Please read the content of Week 7 and the last week in FOL for details of the exams
 - All test/quizzes/exams are Open Book
 - Exams are **not** done in the Responds Browser
 - Exams have a **START** and a **STOP** time (even if FOL still says you have 20 minutes left on the clock you will stop at the given time)
 - Don't be late, **more that 30 minutes** late to the start of an exam, **you lose the chance to do the exam!**

House Keeping (continued)

- Equipment
- Routers
 - We will be working with the 2901 Cisco router
- Switches
 - We will be working with 2960 Layer 2 switches
 - We will be working with 3560 Layer 3 switches



House Keeping (continued)

- Your Equipment

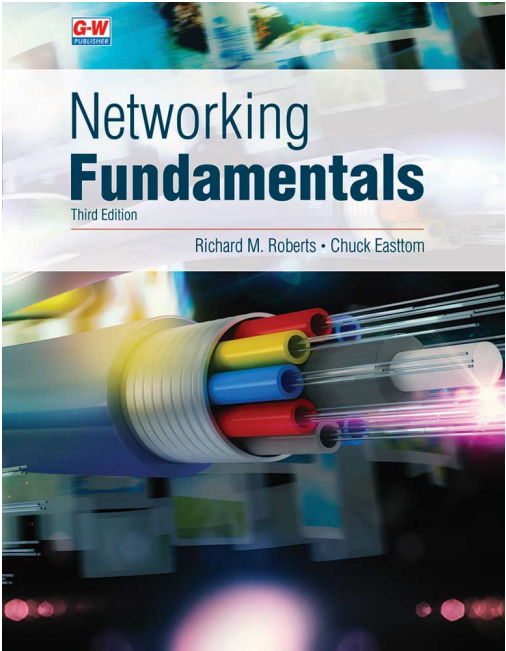
- Your laptop or Desktop
 - This is over kill for this course but is not for some of the other ISM/NSA courses
- It is your equipment
 - Keep it up to date
 - Keep it in good working order

- Your Reading Material

- Electronic version of the G-W Networking Fundamentals (Third Edition)
www.g-w.com/networking-fundamentals-2020
- Optional: available on Amazon in paper as a hard cover book, search for ISBN 978-1-63563-443-3

ISM - Information Security Management

- **Processor:** 64 bit Multicore Intel® w/ Intel-VT or 64 bit Multicore AMD with AMD-V support
- **Memory:** 16GB Minimum
- **Optical Drive:** DVD Multi Dual Layer or external USB Optical Drive (Optional)
- **Operating System:** Microsoft Windows 10 Enterprise, Pro, or Education
- **Hard Disk Drive:** 256GB SSD or greater HDD with external USB Storage Drive
- **Display:** 14" XGA (1024x768), DirectX11 and OpenGL 4.0 (or higher) compatible or better
- **Communication devices:**
 - Wireless (802.11a/b/g/n compliant)
 - Ethernet 10/100/1000 Mbps with standard RJ45 jack
- **USB Ports:** 2 x USB 3.0 ports (additional USB 2.0 ports optional)



End of the **House Keeping** for this week

On with the first lecture

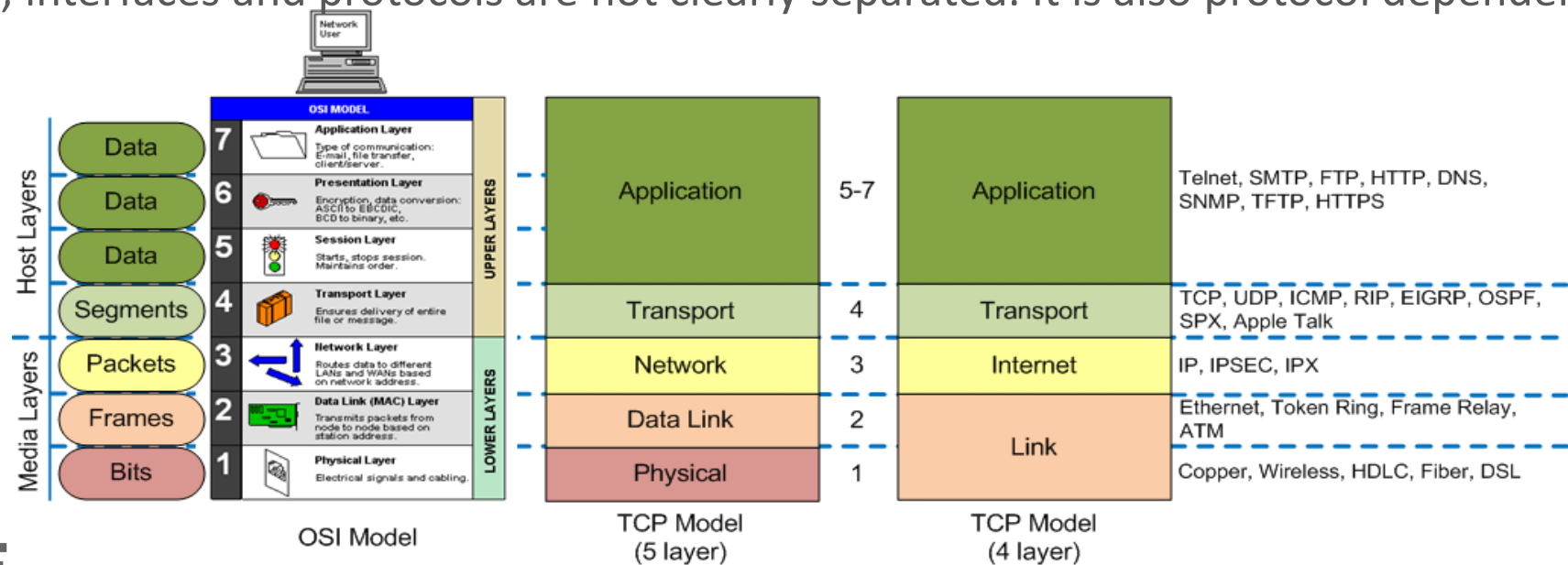
Lecture – 01 - Introduction

IEEE 802.3 Ethernet – History of the Ethernet



OSI Model vs TCP Model

- OSI Model
 - **Open System Interconnect** Model
 - Layered and abstract description for communications and network protocol design.
 - Each layer has its own set of functions.
 - Each layer only communicates with the layers directly above or below.
- TCP Model
 - **Transport Control Protocol** Model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
 - TCP model is, in a way implementation of the OSI model.
 - In TCP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.



OSI Model

- L1 Physical
 - Defines **Bits** specifications to **access** the **physical** communication **medium**.
 - Transmission mode: full duplex, half duplex...
 - Transmission encoding: Manchest, QAM...
 - Network topology used: mesh, bus, ring...
 - Example of the most common medium.
 - Copper (Ethernet, ATM, Token-Ring, Sonnet ect...)
 - Fiber Optic
 - Radio Frequency



Ethernet Cable



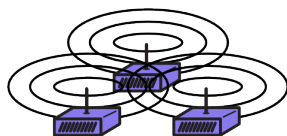
Fiber Cable



Token Ring Cable



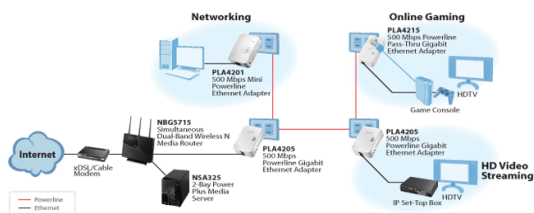
HDMI Cable



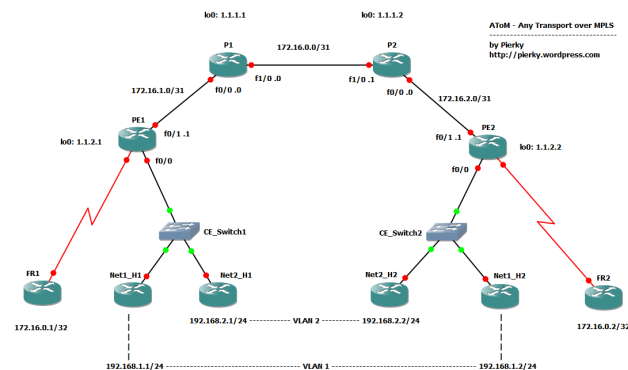
802.11 Wireless



Bluetooth Wireless



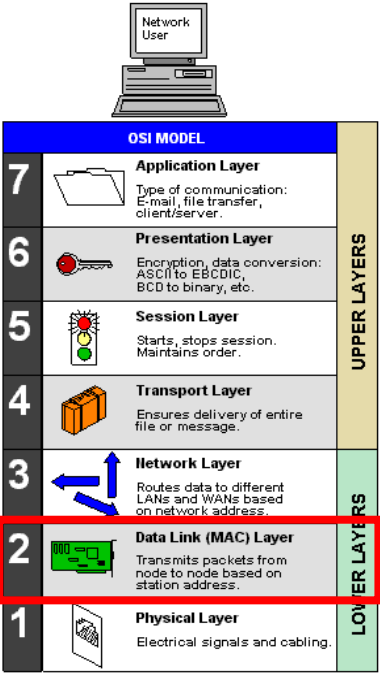
Ethernet over Power Line / Mains



ATM / MPLS / HDLC / Sonet

OSI MODEL		UPPER LAYERS
7	Application Layer Type of communication: E-mail, file transfer, client/server.	
6	Presentation Layer Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.	
5	Session Layer Starts, stops session. Maintains order.	
4	Transport Layer Ensures delivery of entire file or message.	LOWER LAYERS
3	Network Layer Routes data to different LANs and WANs based on network address.	
2	Data Link (MAC) Layer Transmits packets from node to node based on station address.	
1	Physical Layer Electrical signals and cabling.	

- L2 Data Link
 - Use of **Frames** and **physical addresses** (Ex: MAC address)
 - Purposes of the data link layer
 - Organize the physical layer’s bits into logical groups of information (**Frames**).
 - Detect and correct errors that might happen on the physical layer.
 - Control data flow.
 - Identifies devices on the network.
- Example of the most common L2 protocols
 - 802.3 (Ethernet)
 - 802.11 (Wi-Fi)
- Example of the less common L2 protocols
 - 802.5 (Token Ring)
 - 802.15 (Wireless PAN)
 - 802.15.1 (Bluetooth Certification)
 - 802.16 (WiMAX)
 - 802.14 (Cable Modems)

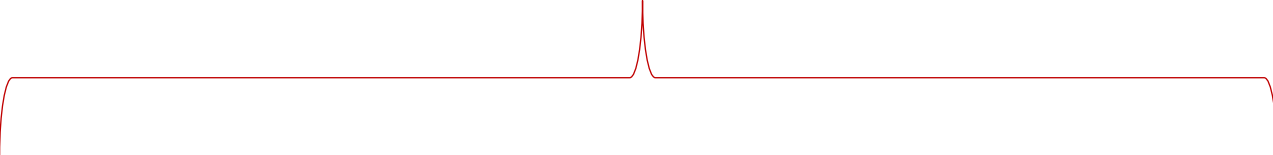


OSI Model (continued)

- L2 Data Link (continued)
 - Media access control address (**MAC** address)
 - uniquely identifies a node in a network
 - Can be permanently encoded into a ROM chip on a NIC
 - **48-bits** written as **12 hexadecimal** digits
 - Format varies:
 - 00-05-9A-3C-78-00
 - 00:05:9A:3C:78:00
 - 0005.9A3C.7800
 - Two parts
 - Organizational Unique Identifier (OUI) (24 bits)
 - Number assigned by manufacturer (24 bits)

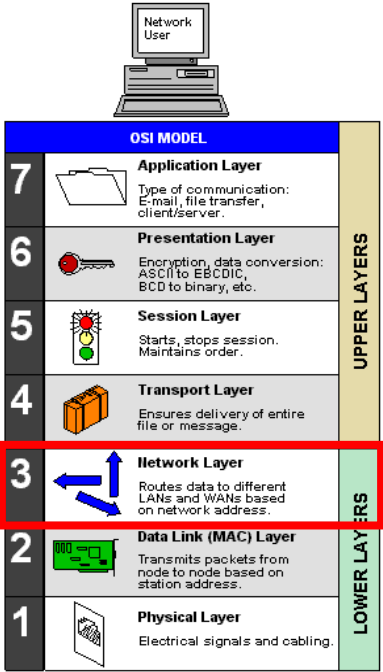
MAC address	
OUI	Vendor Assigns
24 bits	24 bits

- L2 Data Link (continued)
 - Ethernet II Frame Fields
 - Minimum Ethernet frame size is 64 bytes or it is “Collision Frame or Runt”
 - Maximum Ethernet frame size is 1518 bytes or it becomes a “Jumbo or Baby Giant”
 - 802.2 is data link layer LLC sublayer



IEEE 802.3 (Data link layer, MAC sublayer)						
7 bytes	1	6	6	2	46 to 1500	4
Preamble	Start of frame delimiter	Destination address	Source address	Length	802.2 header and data	CRC
Frame header						Trailer

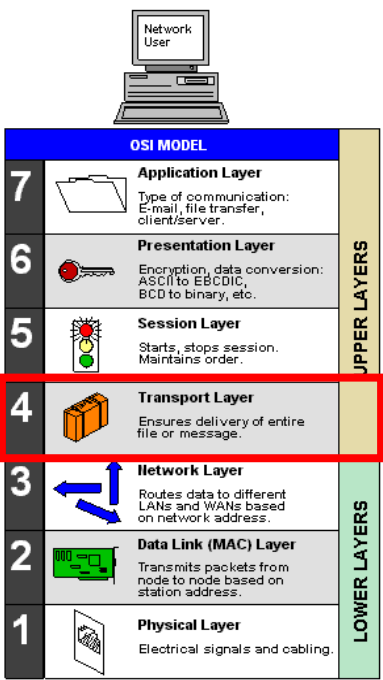
- L3 Network
 - Defined as **Packets**
 - Translates logical address into physical machine address
 - Establish logical connections to other networks to send larger data sequences (**datagrams**).
 - A large amount of data can be fragmented and sent via multiple packets.
 - Introduction of **routing**.
 - Fragmentation
 - Example of the most common L3 protocols
 - Internet Protocol (IP)
 - Address Resolution Protocol (ARP)
 - Routing protocols (RIP, OSPF, BGP, HSRP, VRRP...)
 - Internet Control Message Protocol (ICMP)
 - Internet Protocol Security (IPsec)
 - Network Address Translation (NAT)
 - Example of some of the uncommon L3 protocols
 - Internetwork Packet Exchange (IPX)
 - Signaling Connection Control Part (SCCP)
 - Connectionless Networking Protocol (CLNP)



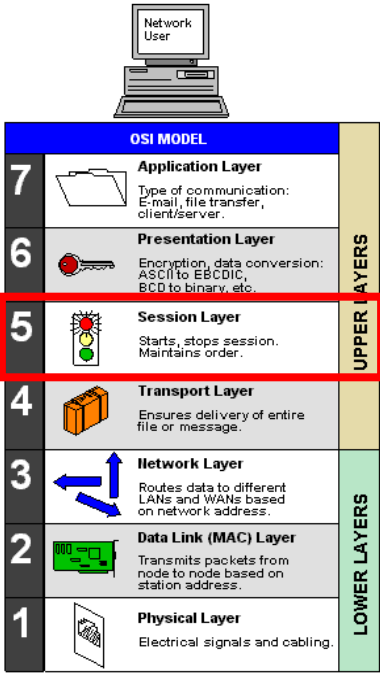
- L4 Transport
 - Use of **Segments** and **ports**
 - Data is broken down into packets that are the maximum size that the network layer can handle.
 - Controls the reliability of a link using flow control, sequencing and error control (Last chance for error recovery).
 - Example of most common L4 protocols
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP)
 - Others less known L4 Protocols
 - AppleTalk Echo Protocol (APE)
 - Authentication Header over IP or IPSec (AH)
 - Datagram Congestion Control Protocol (DCCP)
 - Encapsulating Security Payload over IP or IPSec (ESP)
 - Fiber Channel Protocol (FDP)
 - NetBIOS, File Sharing and Name Resolution (NetBios)
 - Internet Small Computer System Interface (iSCSI)
 - NetBIOS Frames protocol (NFP)
 - Stream Control Transmission Protocol (SCTP)
 - Telephone User Part (TUP)
 - Sequenced Packet Exchange (SPX)
 - Name Binding Protocol {for AppleTalk} (NBP)



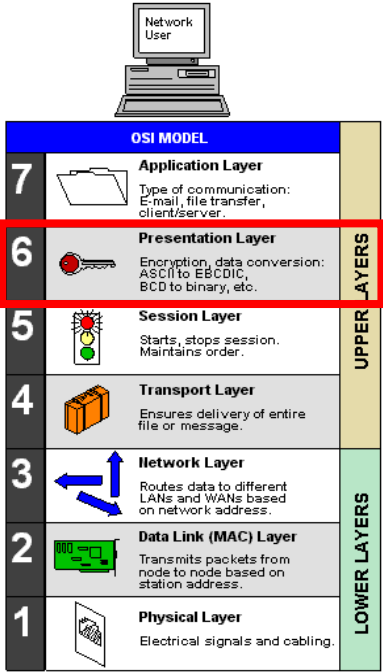
Depending on the Protocol ensures the end to end communications and control



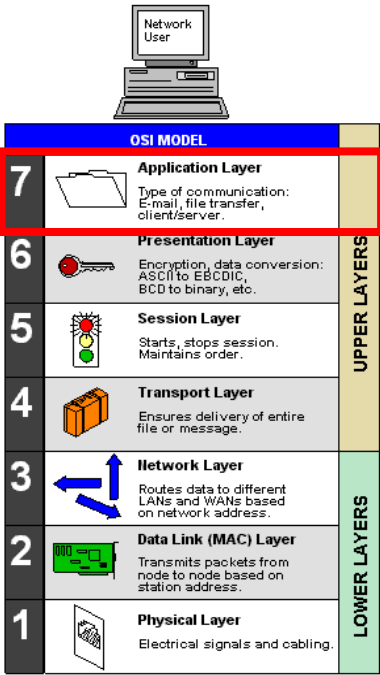
- L5 Session
 - Session refers to a connection for data exchange
 - Responsible for **establishing** and **maintaining communication** between 2 stations on a network.
 - Control which stations talk first.
 - Play a key part in **connection recovery**.
 - Helps the upper layers to connect to the services available on the network.
 - Example of most common L5 protocols.
 - Remote Procedure Call (RPC)
 - Session Control Protocol (SCP)
 - Server Message Block (SMB)
 - Sockets (SOCKS)
 - Example of some uncommon L5 protocols.
 - File Sharing and Name Resolution protocol (NetBIOS)
 - NetBIOS Enhanced User Interface (NetBEUI)
 - NetWare Core Protocol (NCP)
 - Printer Access Protocol (PAP)
 - Short Message Peer-to-Peer (SMPP)



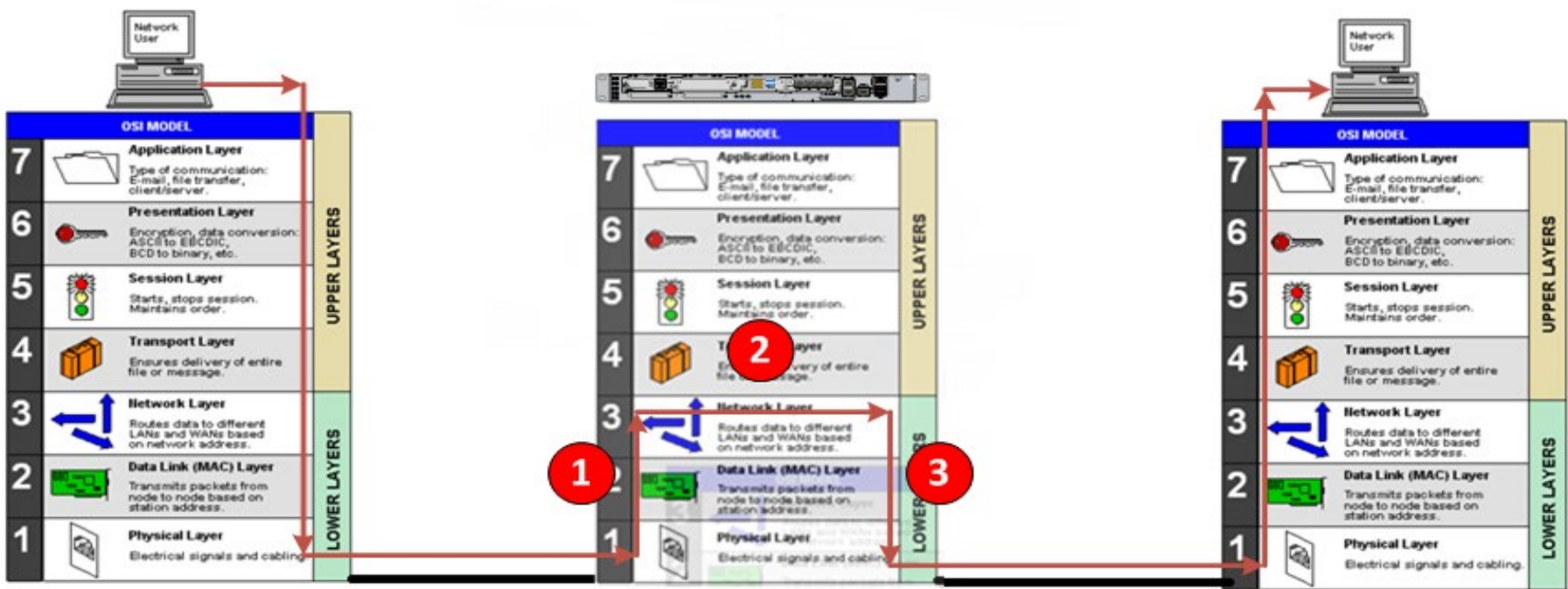
- L6 Presentation
 - **Data** gets **formatted** in a way that the network can understand
 - Some **data encryption/decryption** is taking place (Ex: system password scrambling)
 - Sometimes called the **syntax layer**
 - Example of most common L6 protocols
 - Secure Sockets Layer (SSL)
 - Multipurpose Internet Mail Extensions (MIME)
 - Transport Layer Security (TLS)
 - Apple Filing Protocol (AFP)



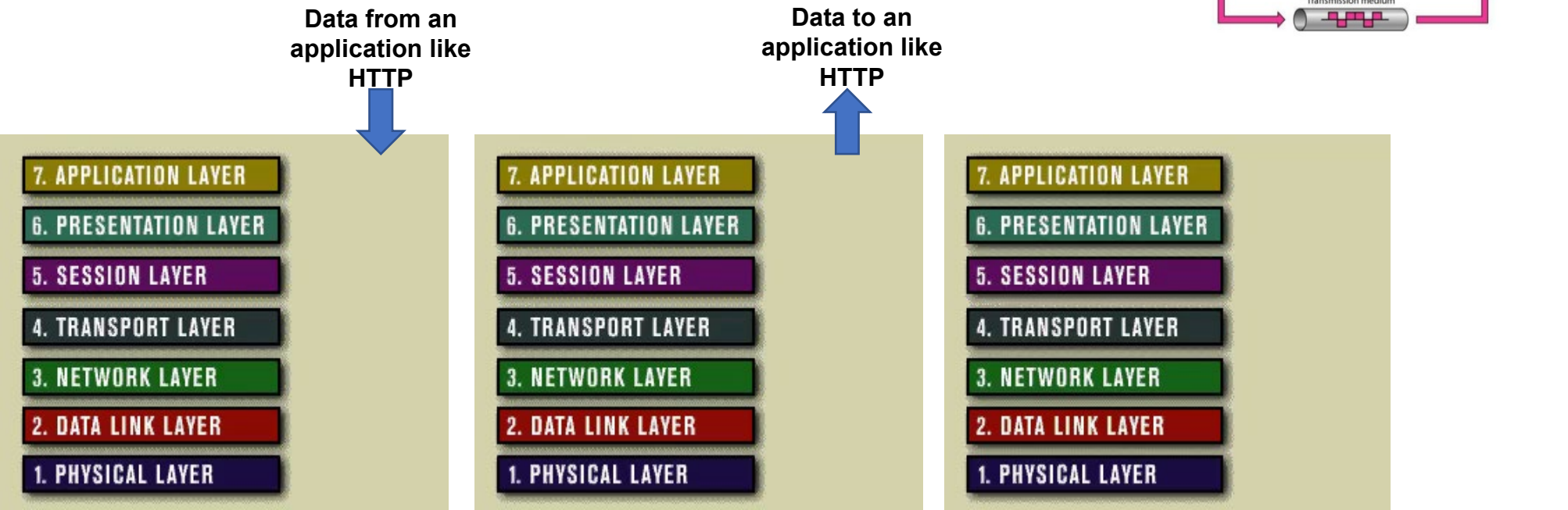
- L7 Application
 - Provides an **interface to the software** that needs to use network services
 - Everything is application oriented
 - Quality of service
 - User authentication and privacy
 - Identify communication partners
 - Example of the most common L7 protocols
 - Hypertext Transfer Protocol (HTTP)
 - Domain Name System (DNS)
 - Dynamic Host Configuration Protocol (DHCP)
 - Simple Mail Transfer Protocol (SMTP)
 - File Transfer Protocol (FTP)
 - Simple Network Management protocol (SNMP)
 - Network Time Protocol (NTP)
 - Telnet
 - Secure Shell (SSH)
 - Trivial File transfer Protocol (TFTP)
 - Simple Object Access Protocol (SOAP)
 - Simple Service Discovery Protocol (Powered by UPnP)



- Example of a routed communication
 1. Any information about the media (Layer 1) and the MAC addresses (layer 2) are stripped out
 2. The router looks up the destination IP address in its table, and passes the datagram back to Layer 2
 3. The router encapsulate the L3 datagram into a Layer 2 frame (adds the new MAC addresses) to send it back Layer 1 where and media information is added back the on the packed goes to the next router or computer



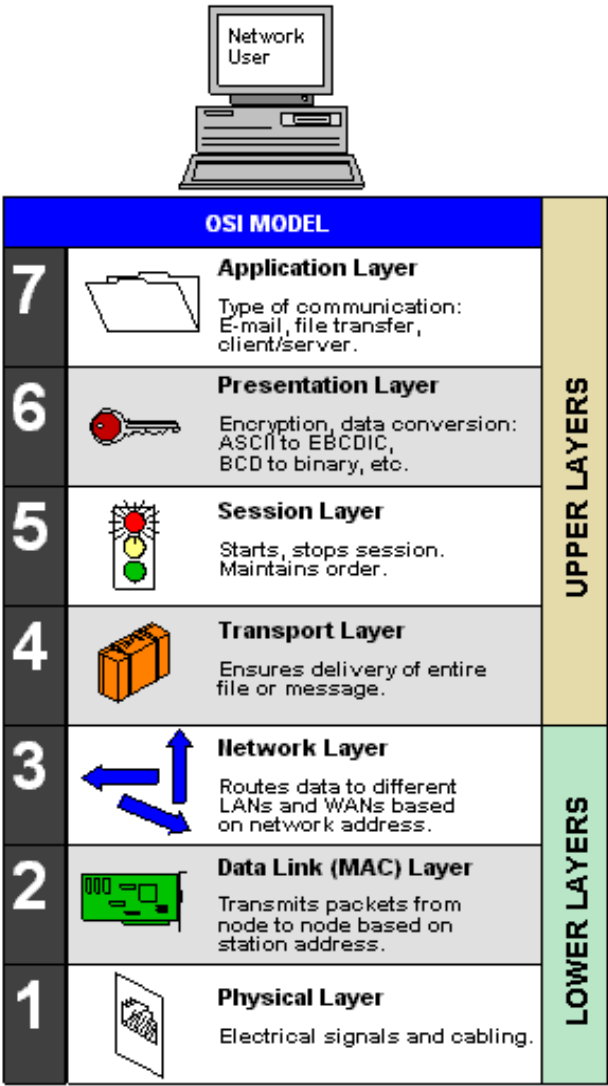
- Communication between 2 stations
 - Data is passed to the application layer.
 - Each layer is encapsulated into the layer below.
 - Headers and possibly footers are added as the encapsulation process takes place.
 - Until it is passed out as 1s and 0s at the Physical Layer.



OSI Model (continued)

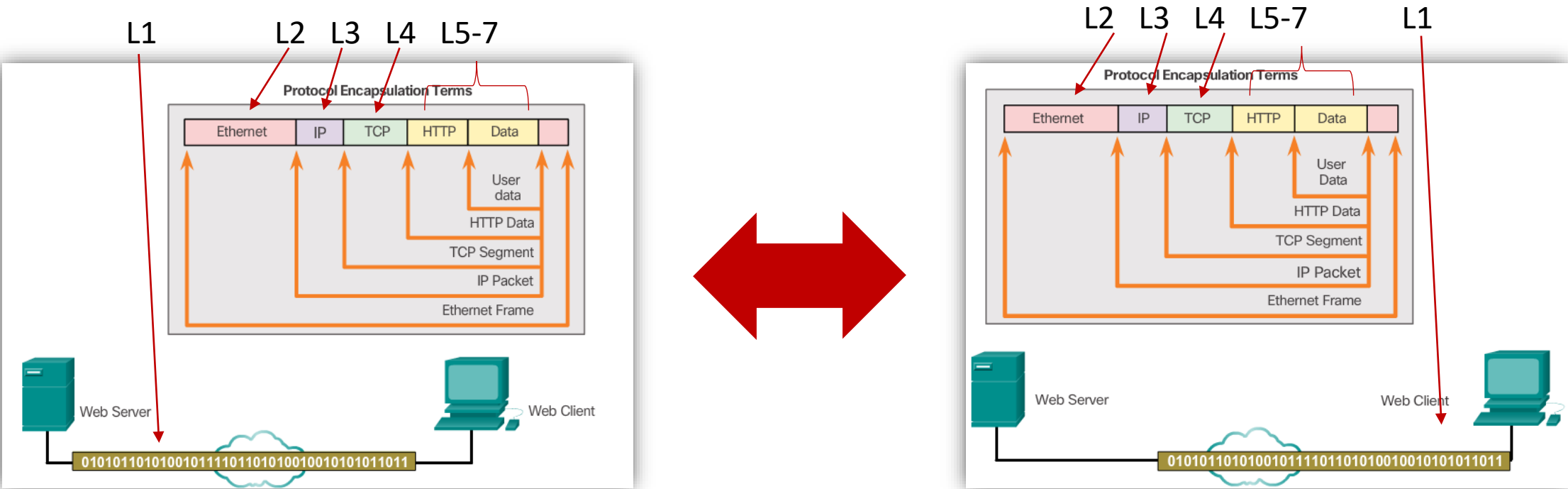
- **Layer 2 vs Layer 3**

- Yes we are talking about the layers in the OSI model
 - A Layer 3 device (a Layer 3 switch) or a router can and may have to deal with IP addresses (IPv4 and or IPv6) to be able to accomplish its goals
 - Layer 3 implies routing
 - Whereas a Layer 2 switch only works with MAC addresses it does not care what the IP address (IPv4 or IPv6) is for it to do its task at the time.
 - Layer 2 implies the movement of data



TCP/IP Communication Process

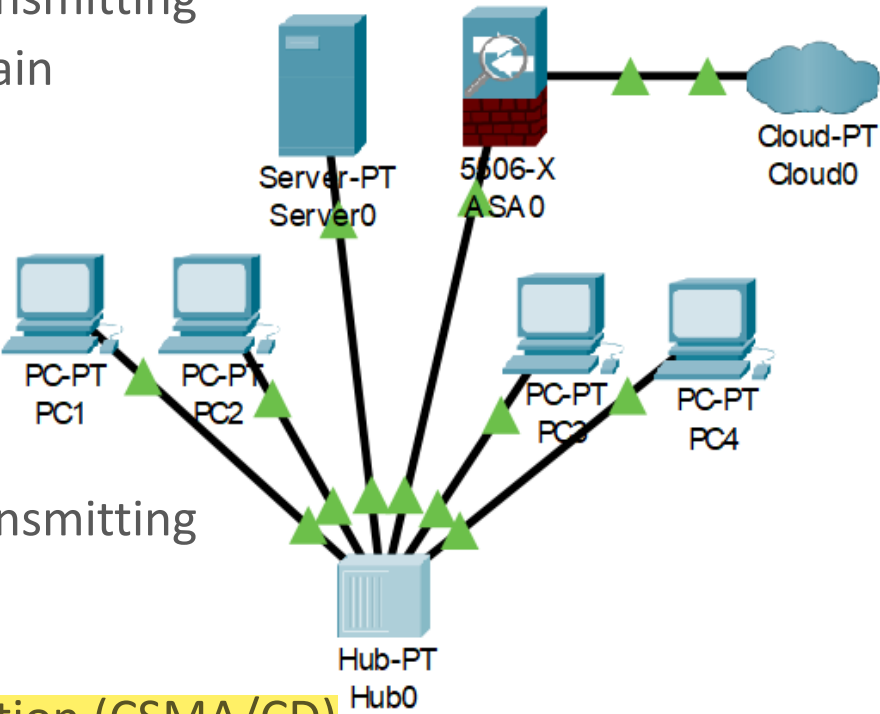
- Look at the names of the sections and the layers of the OSI model



Collision Domain

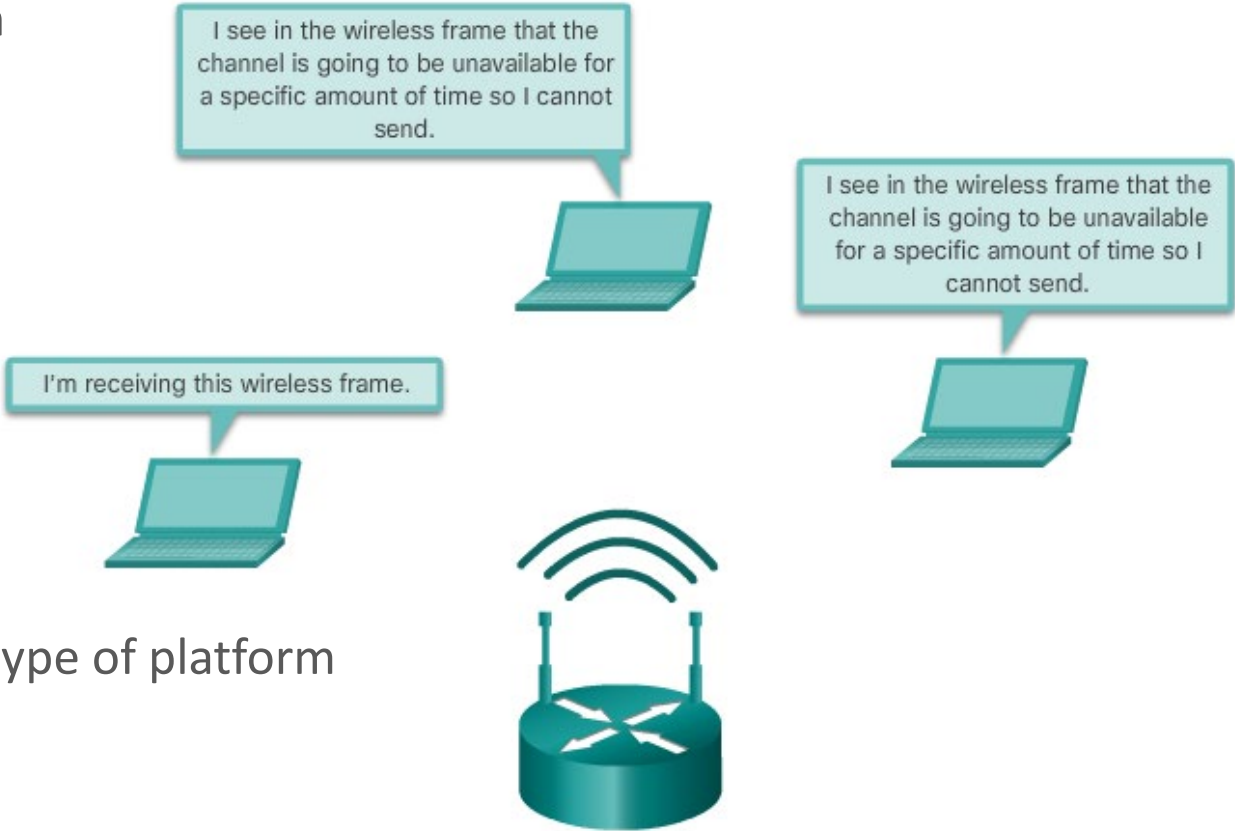
- In shared Ethernet segments devices must compete to communicate
 - Shared medium (hub) – devices must take turns transmitting
 - All ports of a **hub** belong to the same collision domain
 - The more devices – the more collisions
 - Collisions reduce throughput

- The fix ➡ CSMA/CD
 - Shared medium (hub) – devices must take turns transmitting
 - Collisions – the more devices the more collisions
 - Ethernet uses
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



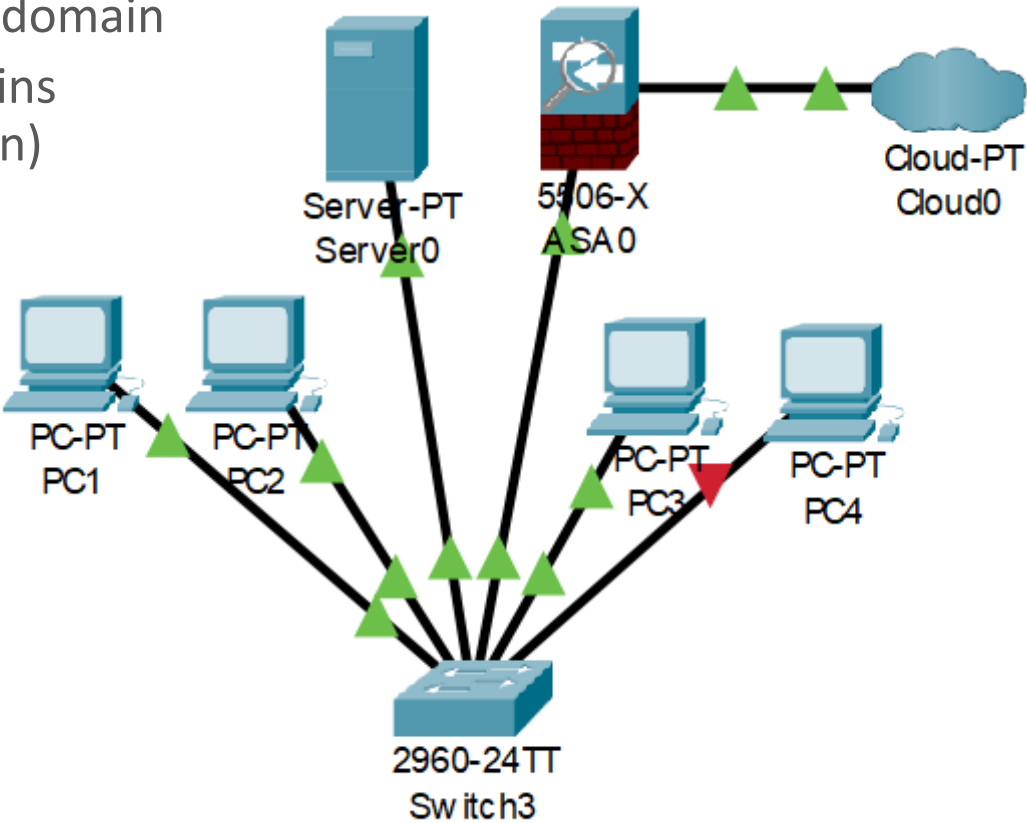
Collision Domain (Continued)

- CSMA/CD (Continued)
 - You thought there were no more problems... switches fixed the Collision problem “YES”?
 - **NO!** Most of us still use hubs every day..... Yes, **Wireless Access Points** work like **HUBs**
 - Device needs to transmit
 - It “listens” for signals on the medium
 - If finds signals – it waits
 - If clear – it sends
 - Carry on listening
 - When collision detected
 - stop sending frame
 - send jam signal
 - wait for random time
 - try again
 - Worst of all... Wireless is not only a HUB type of platform BUT it is half duplex at the same time.



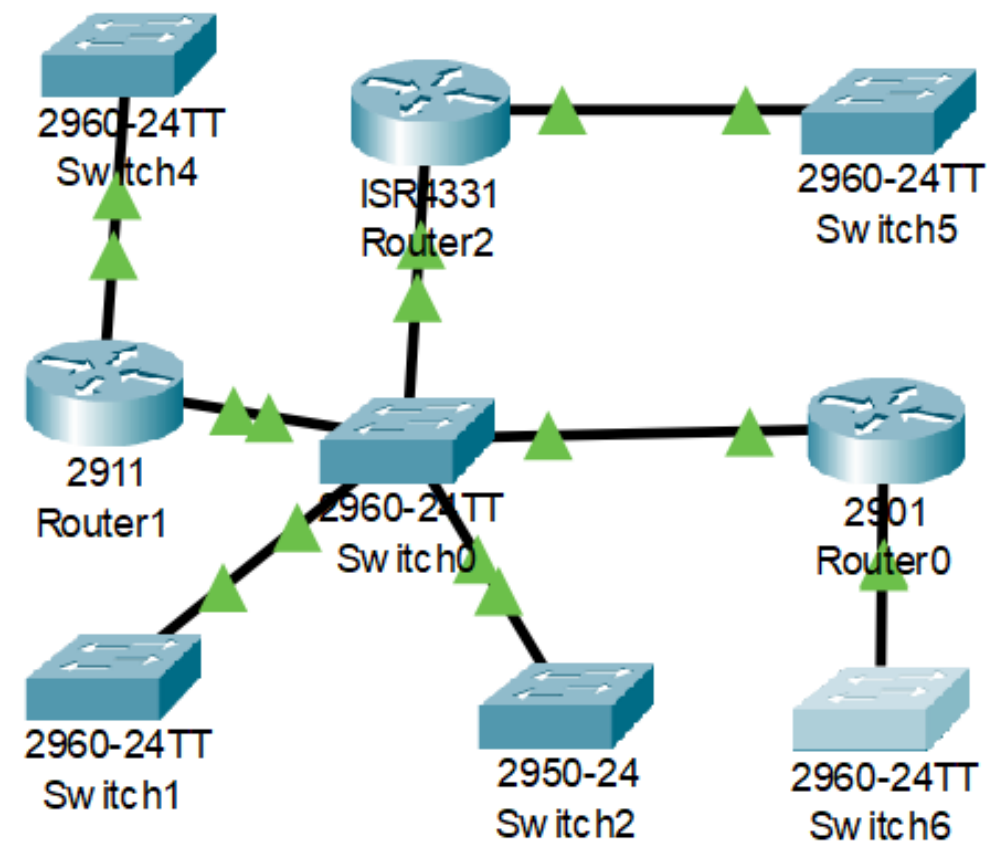
Collision Domain (continued)

- The better fix ➡ Switches
 - Each port is regarded as an individual collision domain
 - Break the segment into smaller collision domains easing device competition (micro-segmentation)



Broadcast Domains

- Broadcast Domains
 - Area in a network where all devices can reach each other at the data link layer by using broadcast
 - Switches forward broadcast frames to all ports, therefore switches don't split broadcast domains
 - All ports of a switch (with its default configuration) belong to the same broadcast domain
 - All ports on a router are in the different broadcast domains as routers don't forward broadcasts from one broadcast domain to another

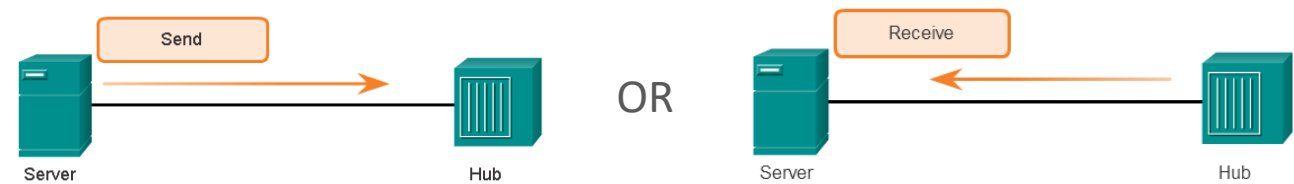


Switches & Duplex

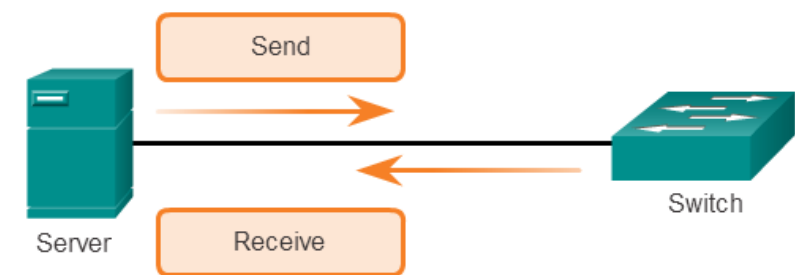
- Switches
 - Operate at the data link layer of the OSI model to create a separate collision domain for each switch port
 - Micro segmentation - a separate collision domain on each of port allows computers to have dedicated bandwidth on point-to-point connections and also to run in full-duplex without collisions
 - Each networked device connected to a switch can be identified using a MAC address, allowing the switch to regulate the flow of traffic

- Duplex

- This is an example of half duplex

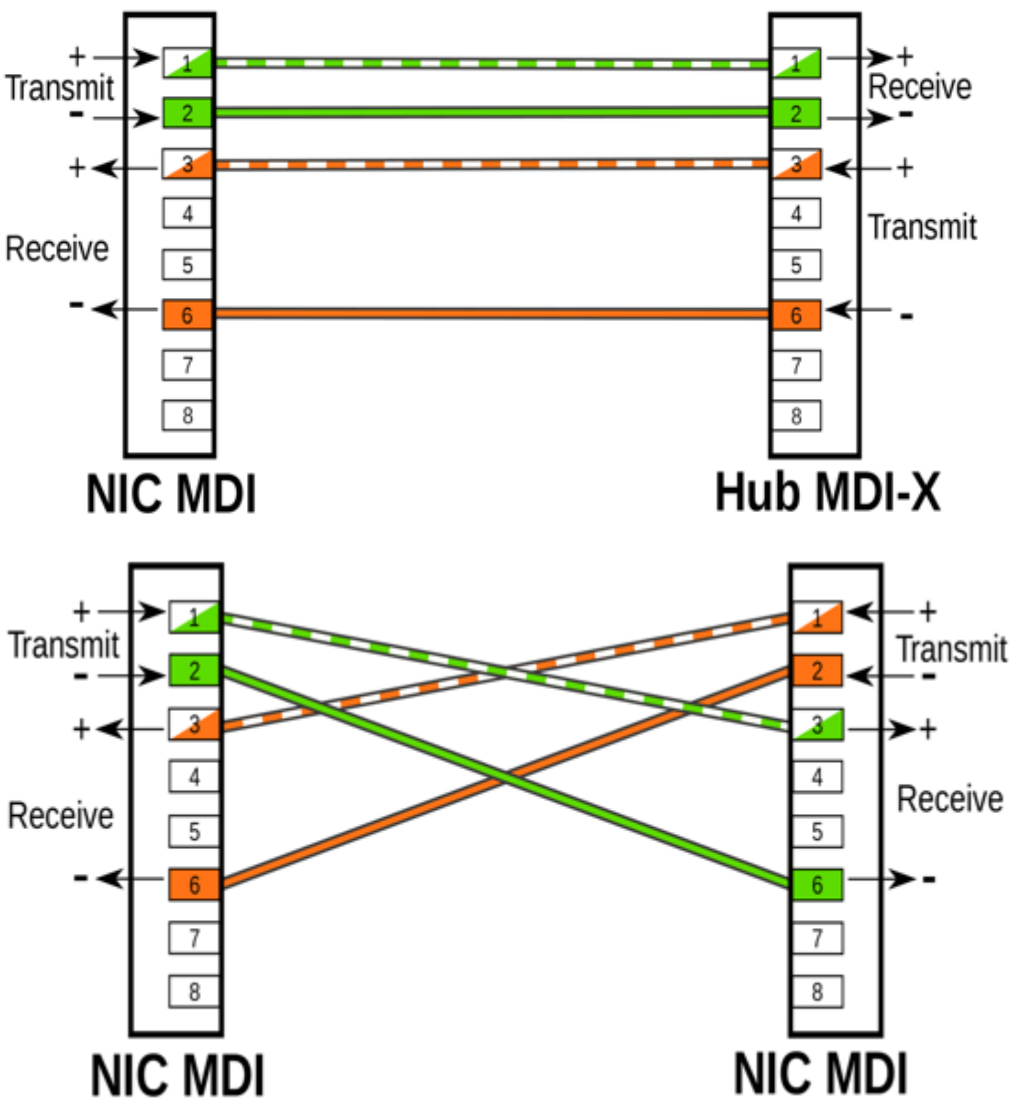


- This is what is preferred full duplex



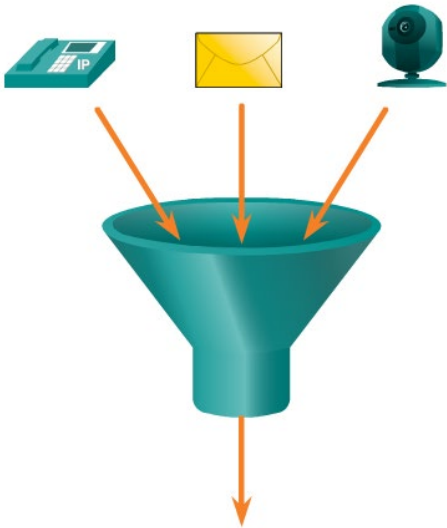
MDI & MDI-X Auto

- **Media Dependent Interface (MDI)**
 - type of Ethernet port found on network devices
 - **MDI** – pins 1 & 2 transmit, pins 3 & 6 receive
 - PCs, Routers
 - **MDI-X** – pins 1 & 2 receive, pins 3 & 6 transmit
 - Hubs, Switches
- **MDI-X Auto**
 - Detects whether cable is straight through or crossover
 - Depends on IOS version
 - Enabled by default from 12.2(18)SE on
 - Disabled from 12.1(14)EA1 to 12.2(18)SE
 - Not available in earlier versions
 - Should work on all Gigabit ports



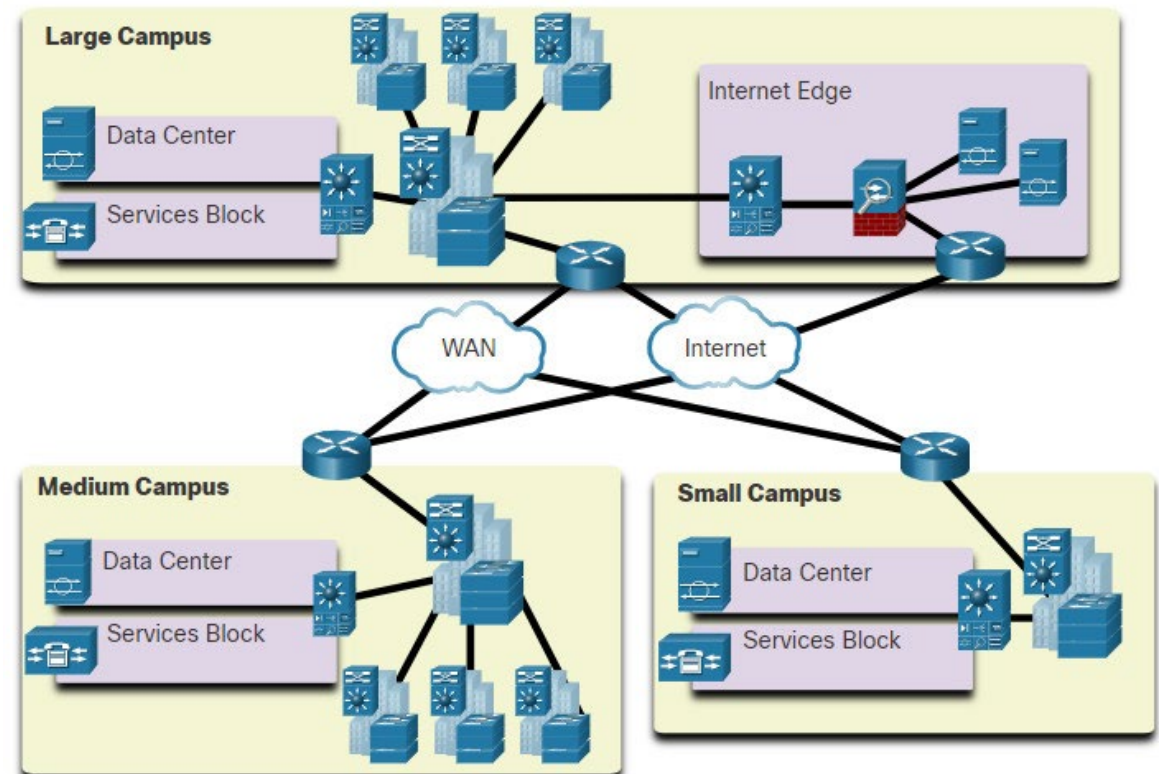
Growing Complexity of Networks

- **Complex Networks**
 - Our digital world is changing.
 - Information must be accessed from anywhere in the world.
 - Networks must be secure, reliable, and highly available.
- **Converging of complex networks**
 - Collaboration is a requirement
 - To support collaboration, networks employ converged solutions
 - Data services such as voice systems, IP phones, voice gateways, video support, and video conferencing
 - Call control, voice messaging, mobility and automated attendant are also common features
- **Benefits include:**
 - Multiple types of traffic; only one network to manage
 - Substantial savings over installation and management of separate voice, video and data networks
 - Integrates IT management



Cisco's Borderless Switched Networks

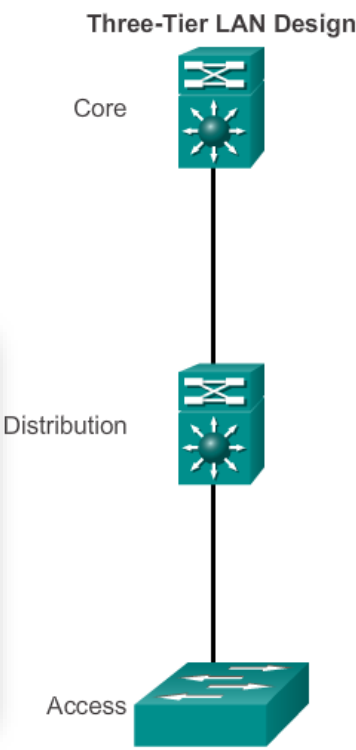
- Cisco's Borderless Switched Networks
 - Cisco's Borderless Network is a network architecture that allow organizations to connect anyone, anywhere, anytime, and on any device securely, reliably, and seamlessly
 - It is designed to address IT and business challenges, such as supporting the converged network and changing work patterns



Borderless Switched Networks (continued)

- Cisco's Borderless Switched Networks
 - Borderless switched network design guidelines are built upon the following principles:
 - Hierarchical
 - Modularity
 - Resiliency
 - Flexibility

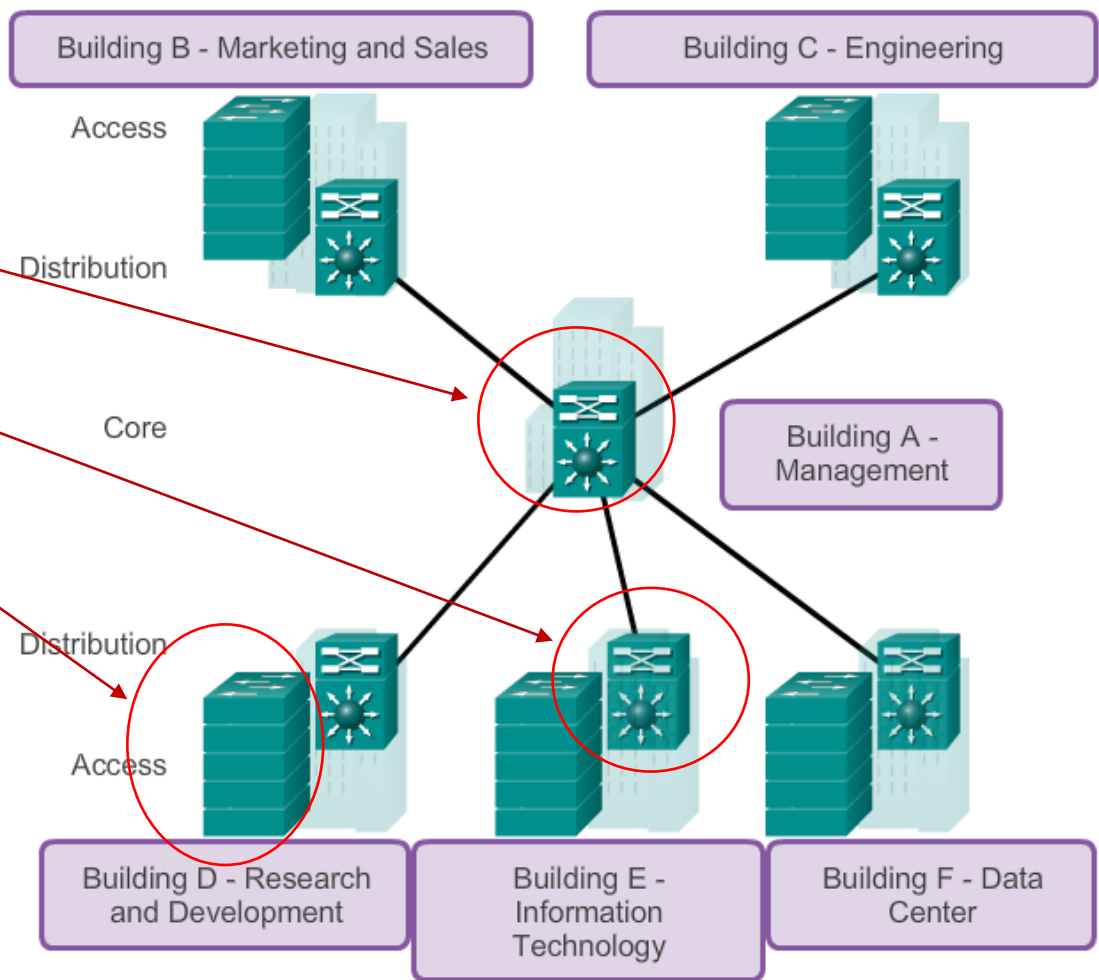
	Hierarchical	Modularity	Resiliency	Flexibility
Provides a way for the network to always be accessible.			✓	
Allows networks to expand and provide on-demand services.		✓		
Helps for every device on every tier to employ a specific role.	✓			
Uses all network resources available to provide data traffic load sharing.				✓



Borderless Switched Networks (continued)

- Cisco's Borderless Switched Networks (continued)

- **Core**
- **Distribution**
- **Access**
- Hierarchical Design Model
 - Includes the following three layers:
 - **access** layer provides users access to the network
 - **distribution** layer provides policy-based connectivity
 - **core** layer provides fast transport between sites -often referred to as the backbone



Borderless Switched Networks (continued)

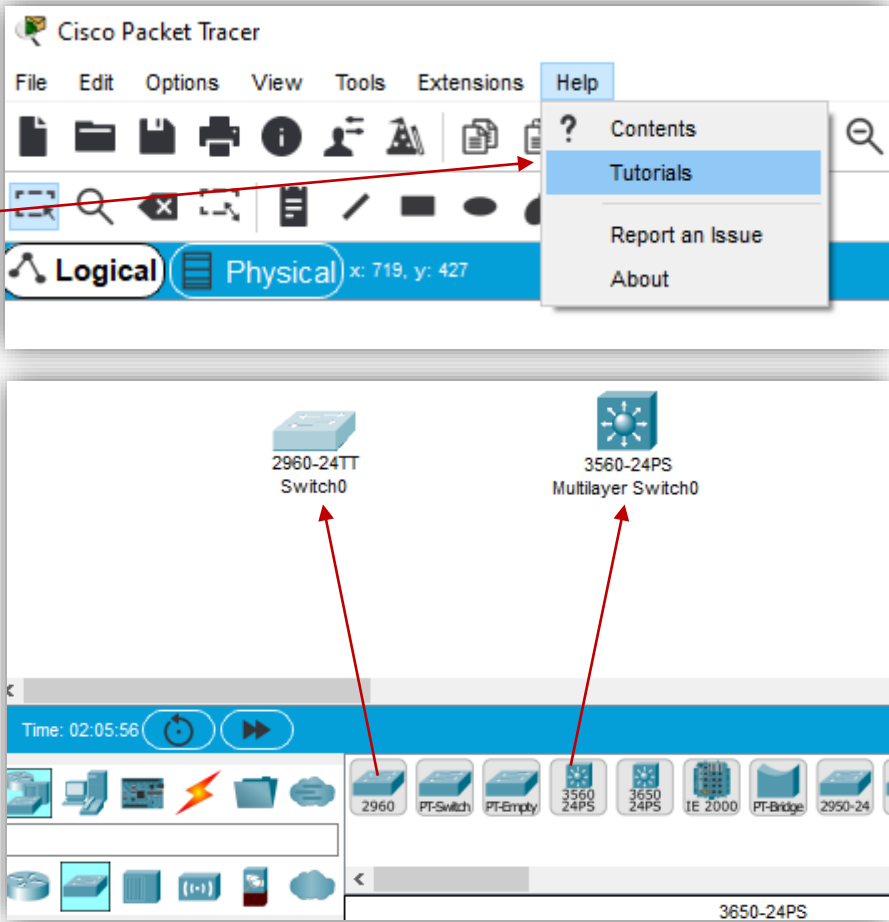
- Cisco's Borderless Switched Networks (continued)
 - **Access Layer**
 - Operate at Layer 2 of the OSI model
 - Provide services such as VLAN membership
 - Main purpose is to allow end users, devices into the network
 - Should provide this with low cost and high port density
 - **Distribution Layer**
 - Provide a boundary definition in which packet manipulation can take place
 - Segmented into broadcast domains (VLANs)
 - Policies and access control lists
 - Prevents problems from affecting the core layer
 - Security
 - Operate at Layer 2 and Layer 3
 - **Core Layer**
 - High-speed switching backbone
 - Layer 3 switch or external router is used
 - Should not perform any packet manipulation
 - Redundant paths gives stability to the network in the event of a single device failure

Role of Switched Networks

- Switched Networks
 - Switching technologies are crucial to network design.
 - Switching allows traffic to be sent only where it is needed in most cases, using fast methods.
 - A switched LAN:
 - Allows more flexibility
 - Allows more traffic management
 - Supports quality of service, additional security, wireless, IP telephony, and mobility services

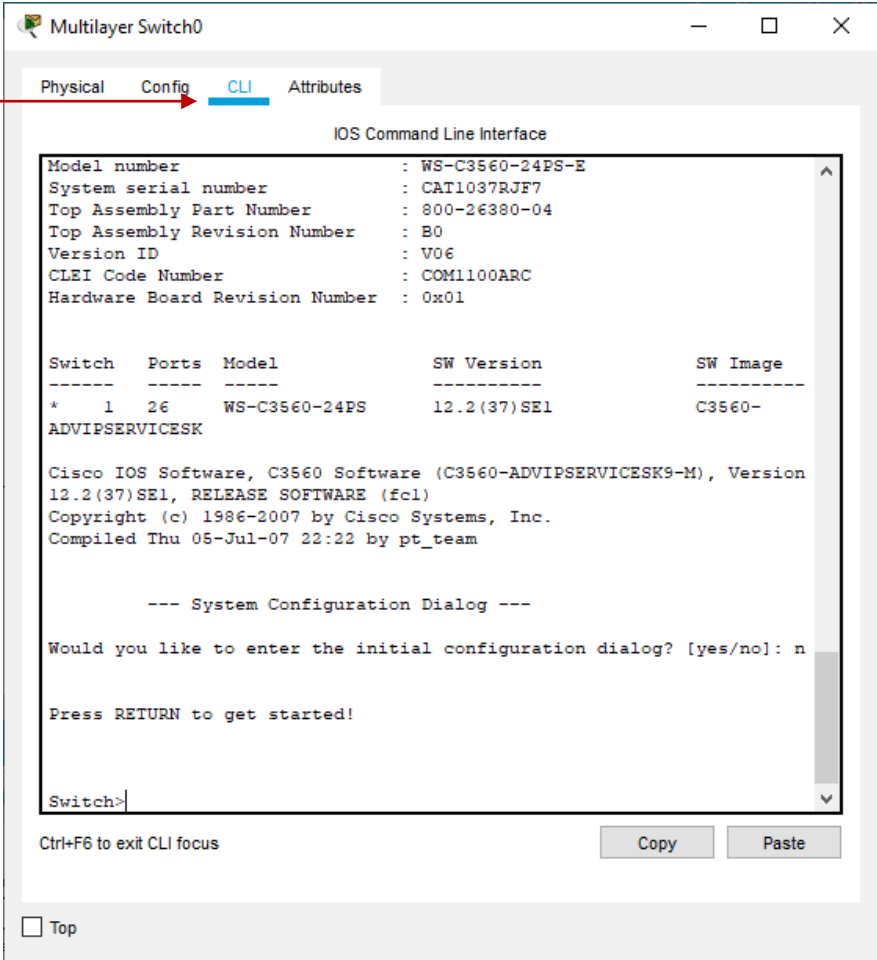
Tools and Commands

- Packet Tracer (PT)
 - Please watch the pre-recorded “Lecture-00-Introduction” for how to acquire this software and sign up for the 10 hour course on the use of PT
 - You are not required to do the 10 hour PT course, but if you know nothing about this software, it is a good resource
 - Also there are some great tutorials accessible through the help on the tool
 - There are a bunch of devices you can drag onto the PT working area
 - You can then click on the device in the PT work area to gain access to the device and to be able to configure the device



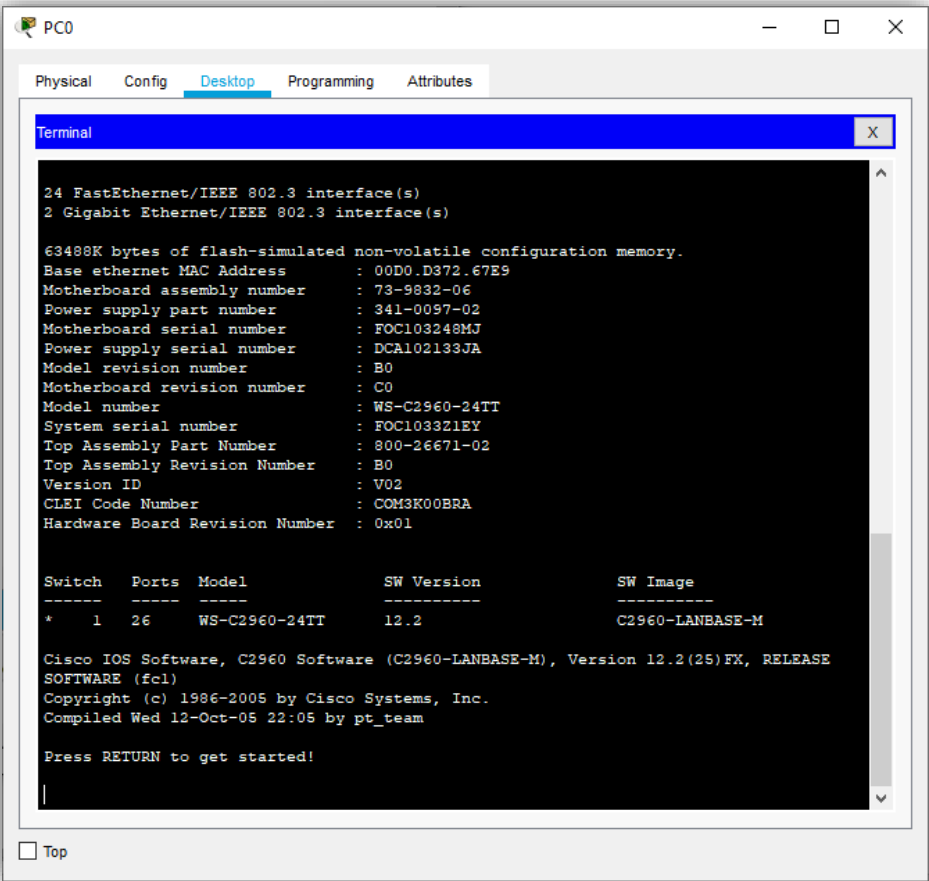
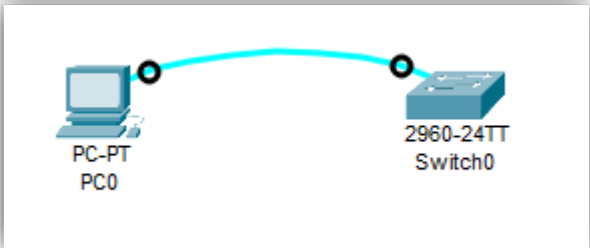
Tools and Commands (continued)

- Packet Tracer (PT) (Continued)
 - The Command Line Interface (CLI) is where you will do most of the configuration of the devices.
 - Please play with the other tabs to see what else you can do
 - In the first lab will ask you not to use the CLI as shown above
 - I would like you to see what you would do in the lab at the college in the real equipment lab



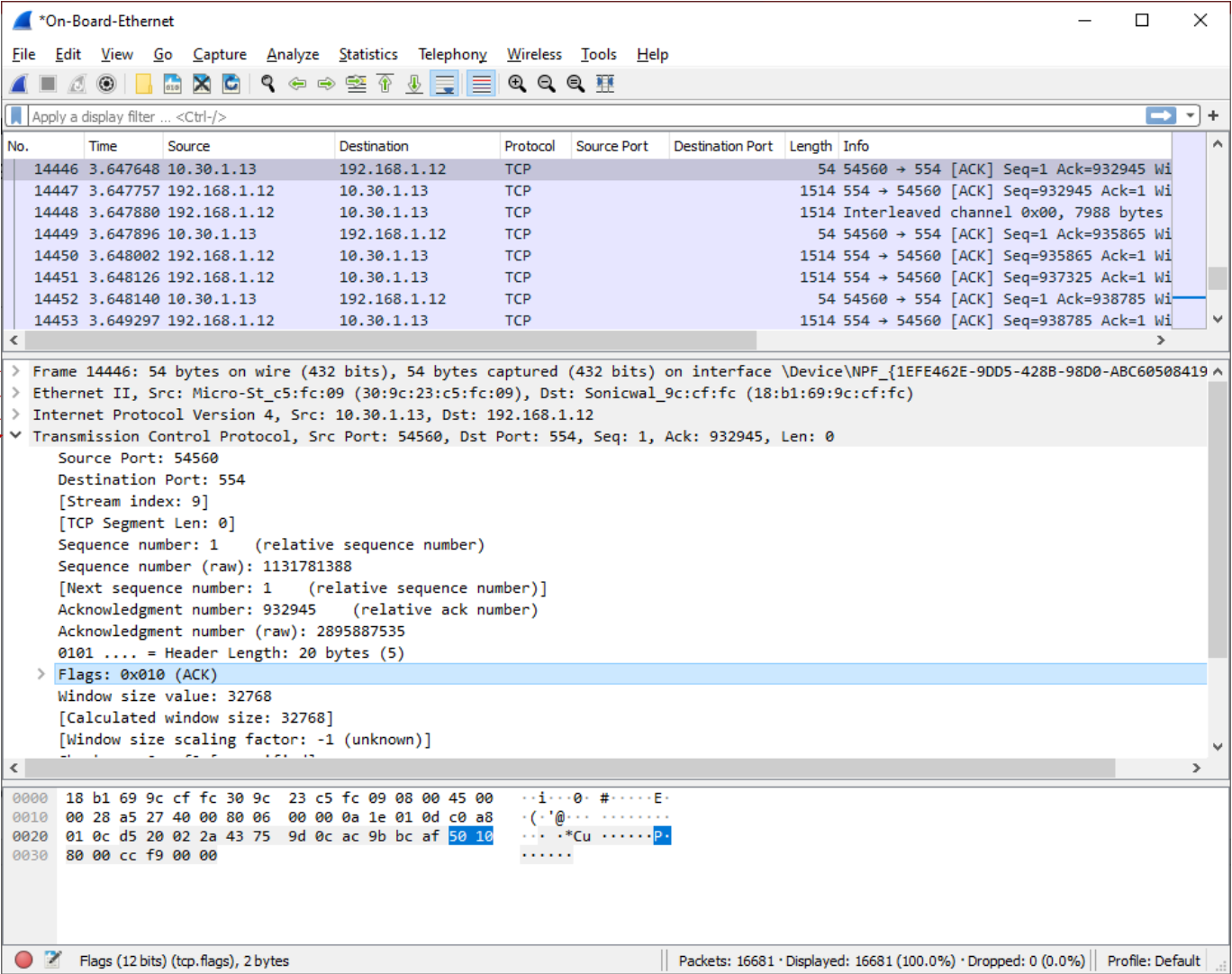
Tools and Commands (continued)

- Packet Tracer (PT) (Continued)
 - In this first lab you will connect to the devices using the blue rollover cable and then using a terminal communication tool in the desktop of the device to acutely “program the device (quite similar to the way it is done in the physical lab at the college)
 - For the labs in the coming week you can use the CLI tab on the devices them selves (it is simpler)



Tools and Commands (continued)

- Wireshark
 - This a tool that can be used in the real world to test and check what is going on/through the network connection on your systems
 - In the OSI model
 - Layer 1
 - Layer 2
 - Layer 3
 - Layer 4
 - Layer 5-7 (Sometimes depending on data captured)



Tools and Commands (continued)

- Wireshark (Continued)
 - Yes you can do some what the same things as Wireshark in PT, but it is not as comprehensive
 - You can see the OSI model layers
 - You can open the PDU and look at more of the data But not as much as what you can see in Wireshark

PDU Information at Device: Router0

OSI Model

Outbound PDU Details

At Device: Router0

Source: Router0

Destination: 192.168.1.1

In Layers

Out Layers

Layer7

Layer6

Layer5

Layer4

Layer3

Layer2

Layer1

Layer 7: TELNET

Layer6

Layer5

Layer 4: TCP Src Port: 23, Dst Port: 1026

Layer 3: IP Header Src. IP: 192.168.1.254, Dest. IP: 192.168.1.1

Layer 2: Ethernet II Header 00E0.F98C.A701 >> 00D0.FF48.E05B

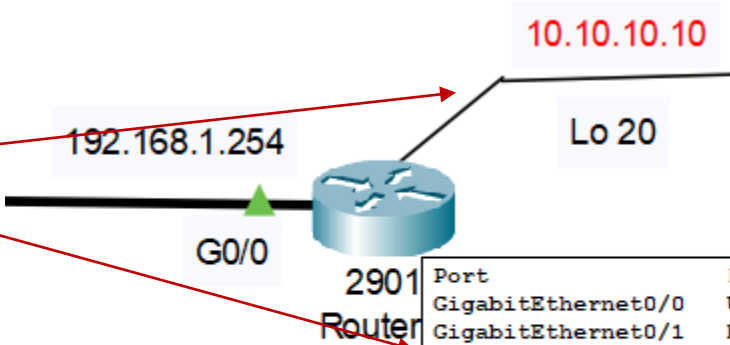
Layer 1: Port(s): GigabitEthernet0/0

1. The TELNET server sends data to the TELNET client.

Tools and Commands (continued)

- Local Loopback

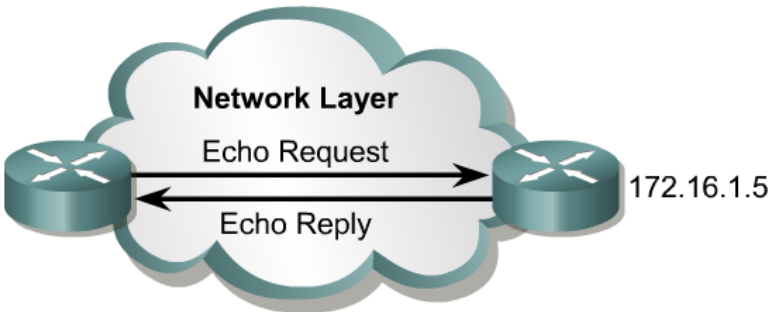
- An interface that is virtual
- Is usually programmed on to a system for testing
- The command to add a local loopback:
 - enable
 - config terminal
 - interface lo 20
 - ip address 10.10.10.10 255.255.255.0
 - no shut
 - exit



Port	Link	VLAN	IP Address	I
GigabitEthernet0/0	Up	--	192.168.1.254/24	<
GigabitEthernet0/1	Down	--	<not set>	<
Loopback20	Up	--	10.10.10.10/24	<
Vlan1	Down	1	<not set>	<
Hostname: Router				
Physical Location: Intercity, Home City, Corporate Offi				

Tools and Commands (continued)

- Ping (connectivity tests)
 - As an aid to diagnosing basic network connectivity, many network protocols support an echo protocol.
 - The ping target 172.16.1.5 in Figure responded successfully to all five datagrams sent.
 - The exclamation points (!) indicate each successful echo.
 - If one or more periods (.) are received instead of exclamations on the display, the application on the router (or source device) timed out waiting for a given packet echo from the ping target.



```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Tools and Commands (continued)

- Ping (continued)

- Extended/Enhanced **PING**

- Allows users to ping from a virtual device
 - Example of using this PING command

```
Router0# ping ↵
Protocol [ip]: ↵
Target IP address: 192.168.1.1 ↵
Repeat count [5]: ↵
Datagram size [100]: ↵
Timeout in seconds [2]: ↵
Extended commands [n]: Y ↵
Source address or interface: 10.10.10.10 ↵
Type of service [0]: ↵
Set DF bit in IP header? [no]: ↵
Validate reply data? [no]: ↵
Data pattern [0xABCD]: ↵
Loose, Strict, Record, Timestamp, Verbose[none]: ↵
Sweep range of sizes [n]: ↵
```

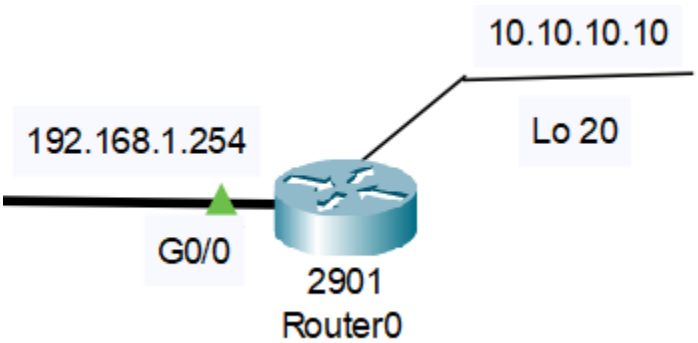
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.10.10

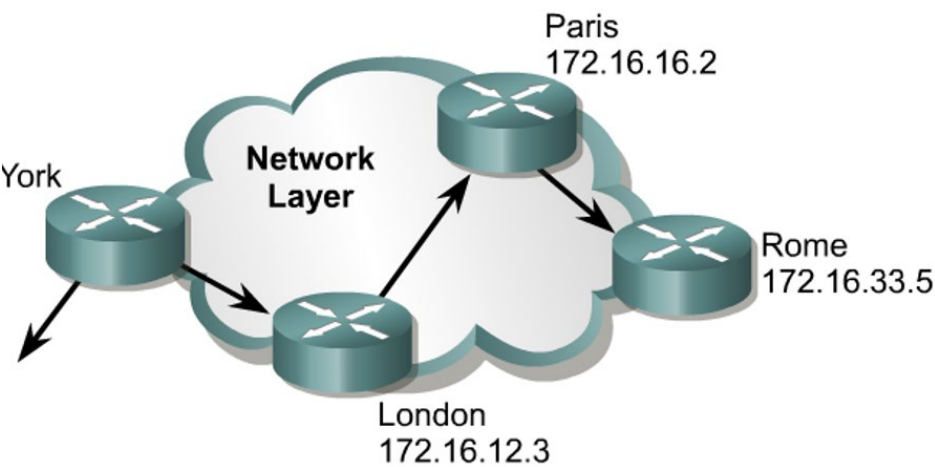
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms



(↵ = Carriage Return or Enter key)

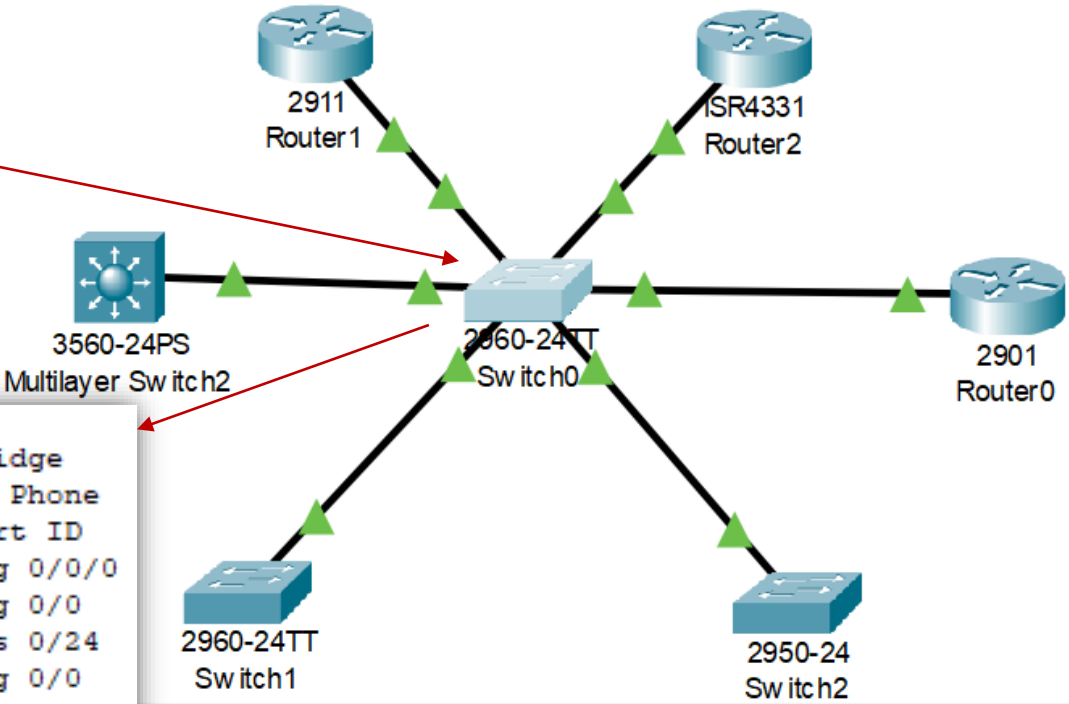
- Traceroute (connectivity tests)
 - The **traceroute** command is the ideal tool for finding where data is being sent in a network.
 - If one of these routers is unreachable, three asterisks (*) will be returned instead of the name of the router.
 - The **traceroute** command will continue attempting to reach the next step until the **Ctrl-Shift-6** escape sequence is used.



```
York#traceroute ROME
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
 1 LONDON (172.16.12.3) 8 msec 8 msec 4 msec
 2 PARIS (172.16.16.2) 8 msec 8msec 8msec
 3 ROME (172.16.33.5) 8msec 8msec 4msec

York#
```

- CDP (Cisco Discovery Protocol)
 - CDP is a Cisco proprietary tool to see what other devices are directly attached to a given device
 - In this case the center “Switch0”
 - **show cdp neighbors**



```
Switch0#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce    Holdtme    Capability    Platform    Port ID
Router2          Fas 0/20          165        R             ISR4300     Gig 0/0/0
Router1          Fas 0/21          150        R             C2900       Gig 0/0
Switch1          Fas 0/23          124        S             2960        Fas 0/24
Router0          Fas 0/19          167        R             C2900       Gig 0/0
Switch2          Fas 0/24          175        S             2950        Fas 0/23
L3-Switch2      Fas 0/22          122        S             3560        Fas 0/24
Switch0#
```

Tools and Commands (continued)

- **CDP** (continued)
 - Introduction to CDPInformation obtained with CDP

**Upper Layer
Entry
Addresses**

**Cisco
Proprietary
Data-Link
Protocol**

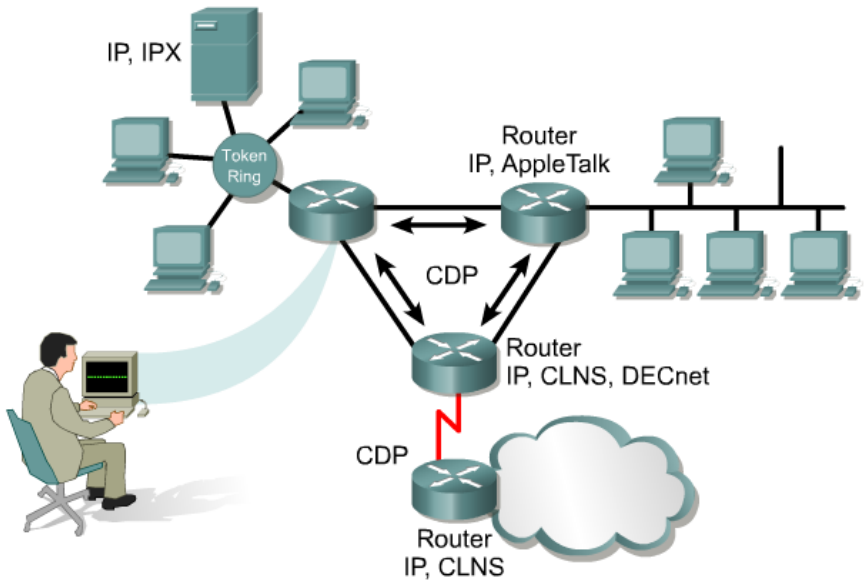
**Media
Support
SNAP**

Layer 3 - IP			
TCP/IP	Novell IPX	AppleTalk	Others
Layer 2 - MAC			
CDP discovers and shows information about directly connected Cisco devices			
Layer 1 - Physical			
LANS	Frame Relay	ATM	Others

- Cisco Discovery Protocol (CDP) is a Layer 2 protocol that connects lower physical media and upper network layer protocols.
- CDP is used to obtain information about neighboring devices, such as:
 - the types of devices connected
 - the router interfaces they are connected to
 - the interfaces used to make the connections
 - the model numbers of the devices
- CDP is media and protocol independent, and runs on all Cisco equipment over the Subnetwork Access Protocol (SNAP).

Tools and Commands (continued)

- CDP (continued)
 - Information obtained with CDP
 - Single command summarizes protocols and addresses on target (for example, neighboring Cisco devices)
 - CDP Version 2 (CDPv2) is the most recent release of the protocol. Cisco IOS (Release 12.0(3)T or later) supports CDPv2.
 - CDP Version 1 (CDPv1) is enabled by default with Cisco IOS (Release 10.3 to 12.0(3)T).
 - Implementation, monitoring, and maintenance of CDP
 - The `cdp run` command is used to enable CDP globally on the router.
 - By default, CDP is globally enabled.
 - The `cdp enable` command is used to enable CDP on a particular interface.
 - On Cisco IOS Release 10.3 or higher, CDP is enabled by default on all supported interfaces to send and receive CDP information.
 - CDP could be enabled on each of the devices interfaces by using the `cdp enable` command.



```
Router
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capablt Platform Port ID
Rt3      Ser0/1      152    R      2500    Ser1
Rt1      Ser0/0      121    R      2620    Ser0/0
Rt2#
```

↑ This router's interface ↑ Remote router's interface

- CDP (continued)
 - Implementation, monitoring, and maintenance of CDP

```
Router
CDP Version 1
Rt3#show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
Rt3#
CDP Version 2
Rt1#show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Rt1#
```

```
Router
Rt1#show cdp traffic
CDP counters:
  Total packets output: 6, Input:6
  Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
  No memory: 0, Invalid packet: 0, Fragmented:0
  CDP version1 advertisements output: 0, Input:0
  CDP version2 advertisements output: 6, Input:6
Rt1#clear cdp counters
Rt1#show cdp traffic
CDP counters:
  Total packets output: 0, Input:0
  Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
  No memory: 0, Invalid packet: 0, Fragmented:0
  CDP version1 advertisements output: 0, Input:0
  CDP version2 advertisements output: 0, Input:0
Rt1#
```

```
Router
Rt1#show cdp entry Rt2
-----
Device ID: Rt2
Entry address(es):
IP address: 192.168.2.2
Platform: cisco 2621, Capabilities: Router
Interface: Serial0/0, PortID(outgoing port): Serial0/0
Holdtime: 139 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software(C2600-DO3S-M), Version 12.0(5)TI,
RELEASE
SOFTWARE(fc1)
Copyright(c) 1986-1999 by cisco System, Inc.
Compiled Tue 17-Aug-99 13:18 bycmong
```

```
Router
Rt1#show cdp interface serial0/0
Serial0/0 is up, line protocol is up
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Rt1#show cdp interface fastethernet0/0
FastEthernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Rt1#
```

- CDP (continued)
 - Disabling CDP

- Troubleshooting CDP

Command	Description
clear cdp table	Deletes the CDP table of information about neighbors.
clear cdp counters	Resets the traffic counters to zero.
show cdp traffic	Displays CDP counters, including the number of packets sent and received and checksum errors.
show debugging	Displays information about the types of debugging that are enabled.
debug cdp adjacency	CDP neighbor information
debug cdp events	CDP events
debug cdp ip	CDP IP information
debug cdp packets	CDP packet-related information
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
cdp holdtime	Specifies the hold time to be sent in the CDP update packet.
show cdp	Displays global CDP information, including timer and hold-time information.

```
Rt1
Rt1#show cdp
Global CDP information
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Rt1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z
Rt1(config)#no cdp run
Rt1(config)#^Z
Rt1#show cdp
%CDP is not enabled
Rt1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z
Rt1(config)#cdp run
Rt1(config)#^Z
Rt1#show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Rt1#
```

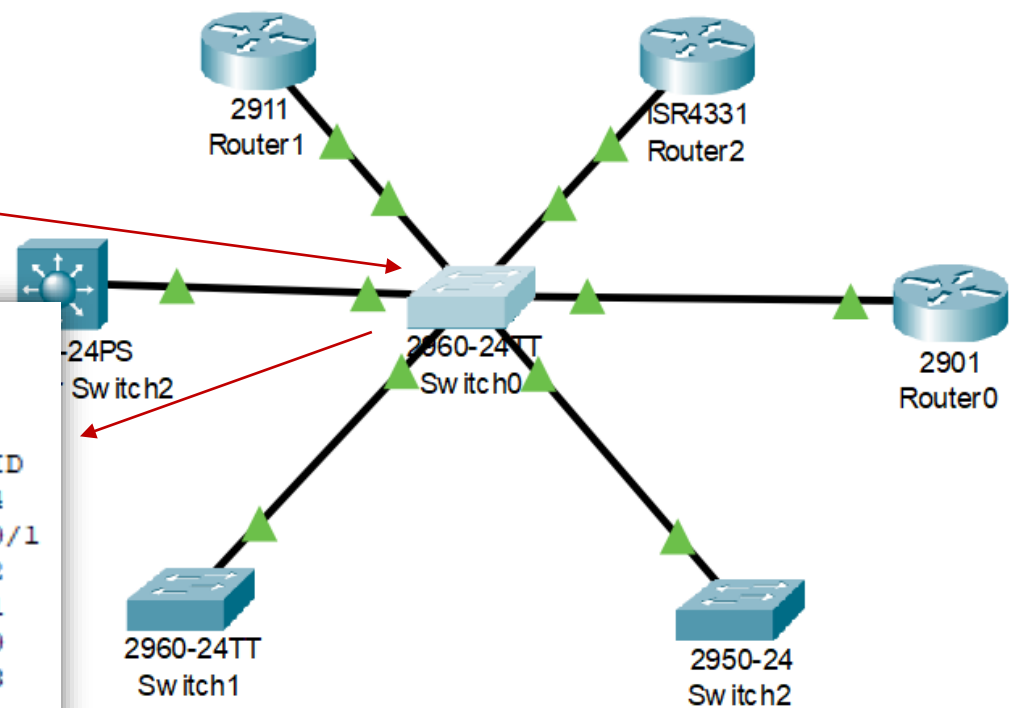
To disable CDP on a specific interface after it has been enabled, use the **no CDP enable** command in interface configuration mode.

```
Rt2
Rt2#show cdp traffic
CDP counters:
Total packets output: 526, Input: 323
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid packet: 0, Fragmented: 0
CDP version 1 advertisements output: 168, Input: 153
CDP version 2 advertisements output: 358, Input: 170
```

- LLDP (Link Layer Discovery Protocol)
 - LLDP is a generic tool to see what other devices are directly attached to a given device
 - In this case the center “Switch0”
 - In global config mode **lldp run** on every device
 - **show lldp neighbors**

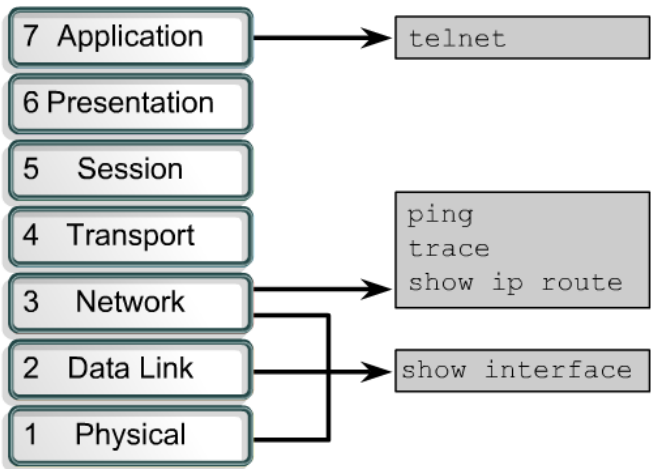
```
switch8#sh lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf    Hold-time    Capability    Port ID
switch4        Fa0/24        120          B             Fa0/24
router2         Fa0/2         120          R             Gig0/0/1
switch0        Fa0/22        120          B             Fa0/22
router1         Fa0/1         120          R             Gig0/1
router0         Fa0/3         120          R             Gig0/0
switch2        Fa0/23        120          R             Fa0/23

Total entries displayed: 6
```



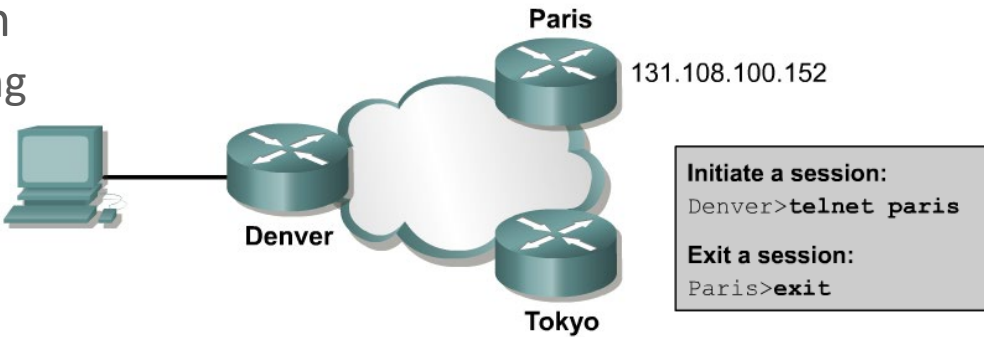
Tools and Commands (continued)

- Telnet
 - Telnet is a virtual terminal protocol that is part of the TCP/IP protocol suite.
 - It allows connections to be made to remote hosts.



- Establishing and verifying a Telnet connection
 - To initiate a Telnet session any of the following alternatives can be used:

```
Denver>connect paris
Denver>paris
Denver>131.108.100.152
Denver>telnet paris
```



- A hostname table or access to DNS for Telnet must be present for a name to work.
- Otherwise, the IP address of the remote router must be entered.

Tools and Commands (continued)

- Telnet (continued)
 - Establishing and verifying a Telnet connection
 - This is where the **ip host** commands can be helpful.
 - Advanced Telnet operation
 - If the resume command is used it requires a connection ID.
 - The connection ID is shown by using the show sessions command.

```
RouterA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#ip host RouterA 10.1.1.1
RouterA(config)#exit

RouterA#telnet routera
Trying RouterA (10.1.1.1)... Open

User Access Verification

Password:
RouterB>
```

Does not have to be the router-name but it is generally a good idea.

Not case sensitive.

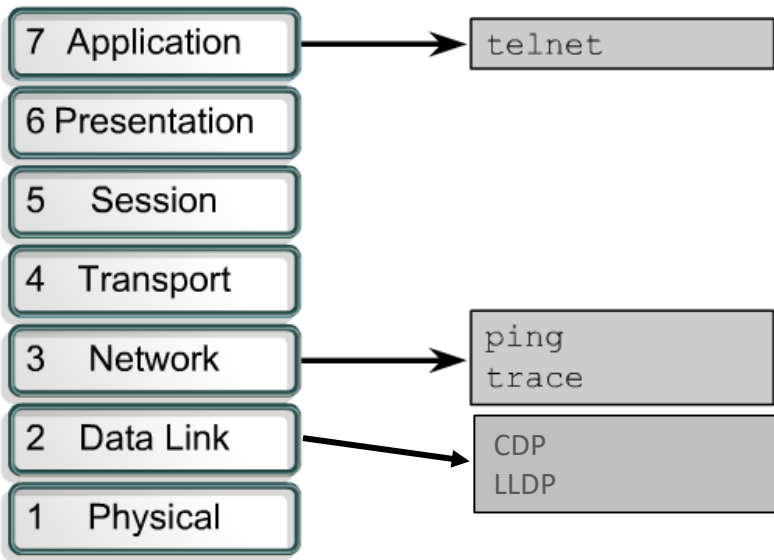
Command	Purpose
Ctrl-Shift-6 then x	Escapes the current connection and returns to the EXEC prompt
Resume	Makes the connection

Router

```
Denver>telnet Paris
Trying Paris (131.108.100.152)...Open
User Access Verification
Password: xxxxx
Paris> (User pressed Ctrl-Shift- 6, then x)
Denver>telnet Tokyo
Trying Tokyo (127.102.57.63)...Open
User Access Verification
Password: xxxxx
Tokyo> (User pressed Ctrl-Shift-6, then x)
Denver>show sessions
Conn Host Address      Idle      Conn Name
1  131.108.100.152      0         Paris
2  127.102.57.63       0         Tokyo
```

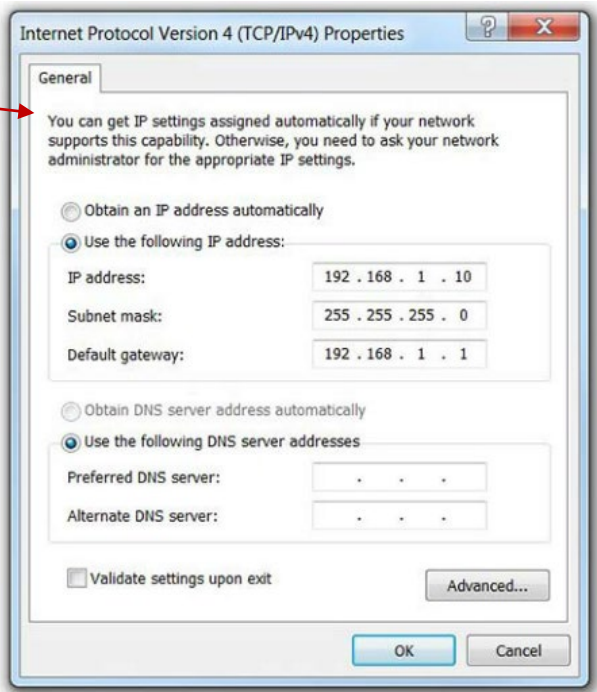
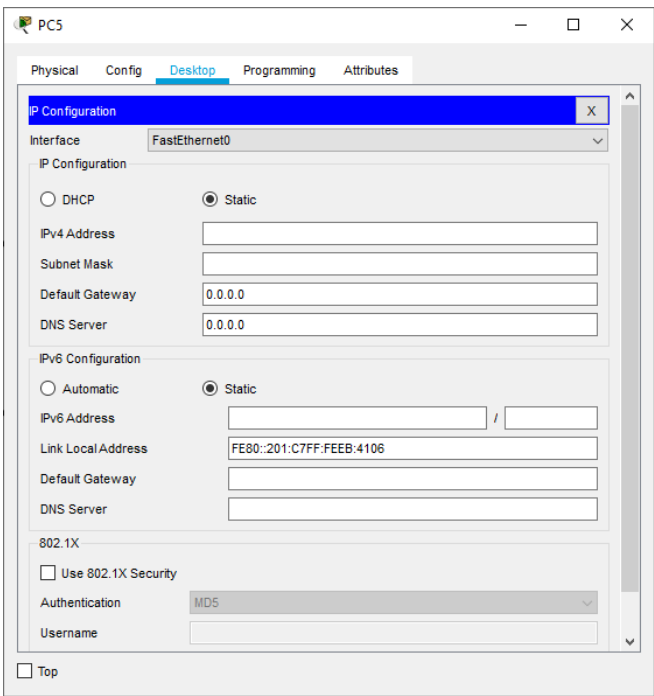
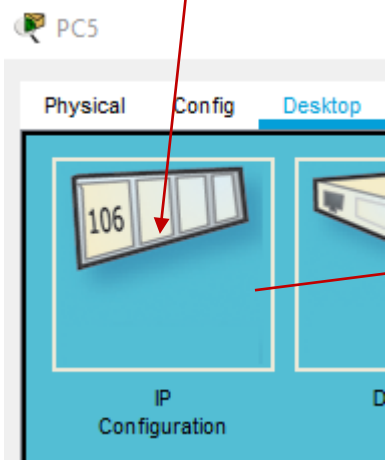
Tools and Commands (continued)

- Troubleshooting IP addressing issues
 - **ping** uses the ICMP protocol to verify the hardware connection and the IP address of the network layer. This is a basic testing mechanism.
 - **telnet** verifies the application layer software between source and destination. This is the most complete test mechanism available.
 - **tracert** allows the location of failures in the path from the source to the destination. Trace uses Time to Live values to generate messages from each router along the path.
 - **CDP/LLDP** check connection from device to device, works at layer 2, no IP addresses needed (as long as the port are enabled (not shutdown, and cables connected)). Are the correct ports being used? If the incorrect port are connected from device to deceive you will not have access to the correct IP addresses



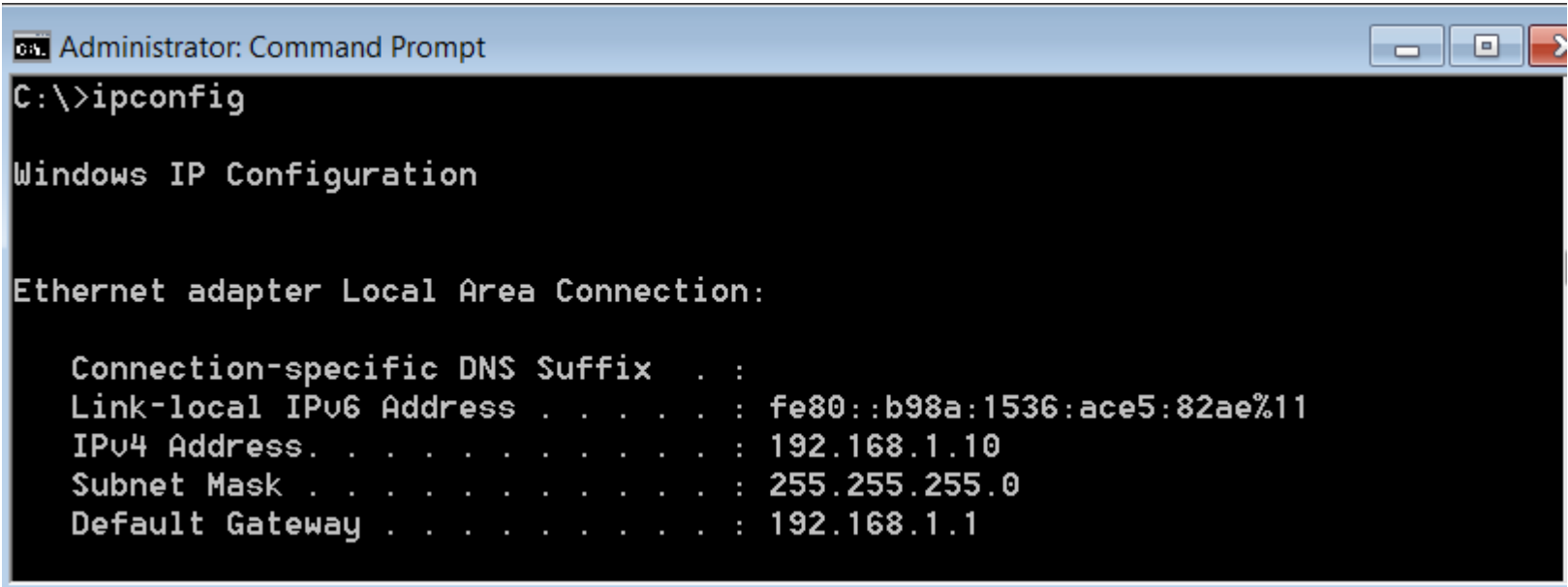
Configuring your PC for the Lab

- In the LAB environment
 - At time you will need to manually, you will have to manually assign an IP address and other data to you PC/Laptop
- In the Packet Tracer environment
 - You will have to manually assign an IP address and other data to your PC/Laptop



Configuring you PC for the Lab (continued)

- In the both the LAB & Packet Tracer environment
 - The “**ipconfig /all**” command in a command window should verify any changes you have made

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The command "C:\>ipconfig" has been entered. The output displays the "Windows IP Configuration" section for the "Ethernet adapter Local Area Connection:". It lists the "Connection-specific DNS Suffix" as empty, the "Link-local IPv6 Address" as "fe80::b98a:1536:ace5:82ae%11", the "IPv4 Address" as "192.168.1.10", the "Subnet Mask" as "255.255.255.0", and the "Default Gateway" as "192.168.1.1".

```
Administrator: Command Prompt
C:\>ipconfig

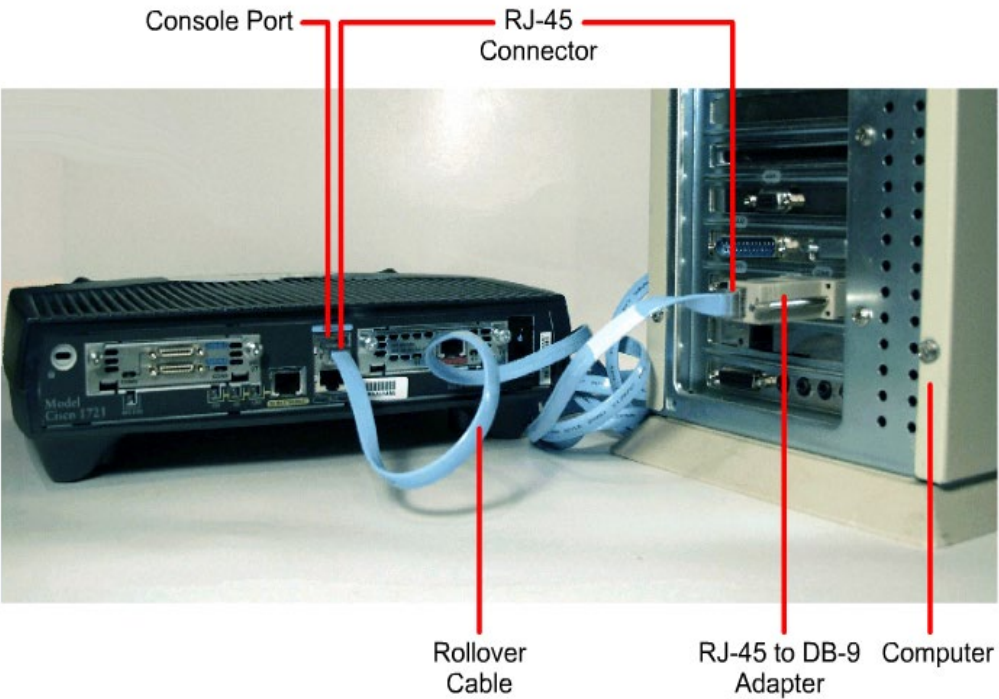
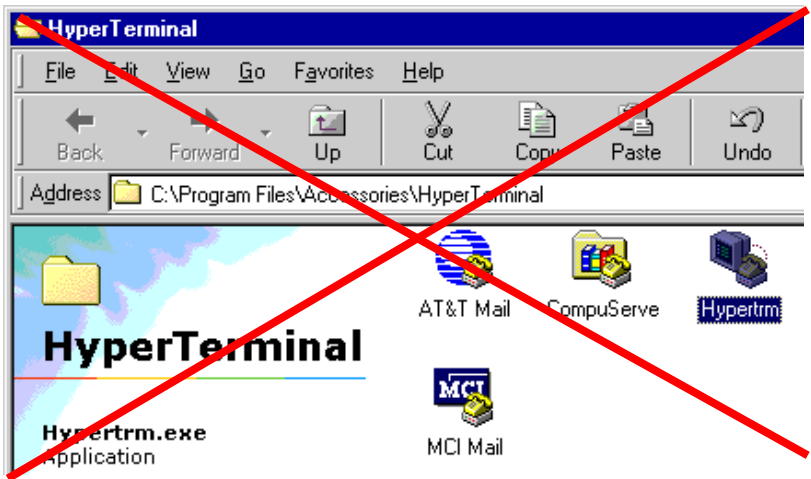
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b98a:1536:ace5:82ae%11
    IPv4 Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

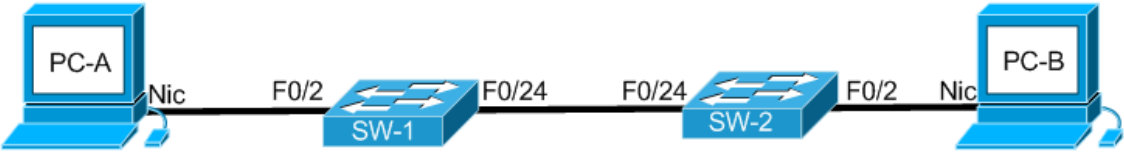
Configuring you PC for the Lab (continued)

- When connection the blue rollover cable to a router
 - When connected using the console interface, the computer is acting as a “dumb terminal”
 - Use Terminal Emulation Software: Putty, TeraTerm there are others but these are free
 - Which ever you decide to install and use you need to know all of the functions (How to use it).
 - Please do not use Hyper Terminal, it was a poor terminal emulator when it came out and it never did get better!



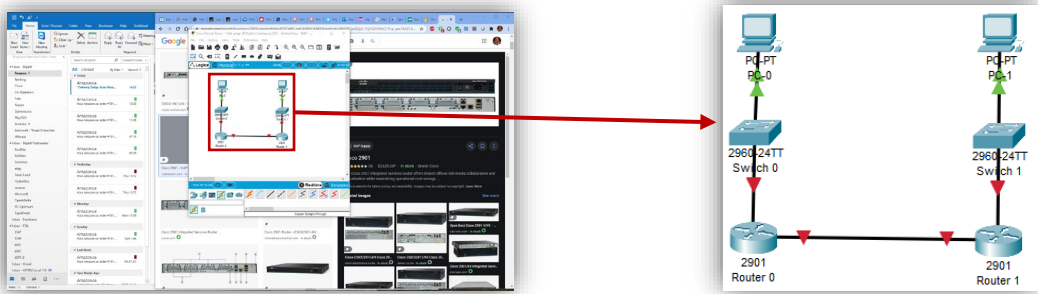
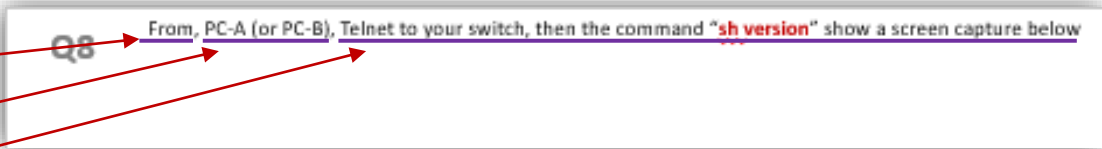
LAB

- This weeks lab
 - If we are working on-line:
 - Find the “**Lab-01 – Students.pkt**” file in this weeks section of FOL
 - If we are working in the classroom/lab:
 - You will have to build this configuration in the equipment room
 - Work in pairs today in the lab, pick weather you are PC-A or PC-B. you will also be responsible for the switch closes to your PC in the diagram
- Follow the instructions in the lab documentation
 - Following the instructions step by step
 - Do any gathering od data at the point in the lab where requested, you may not get the correct information if you wait to the end of the lab and gather all the data.



LAB (Continued)

- PowerPoint Questions
 - From
 - This device / location
 - Do this instruction
- This should make sense... BUT there have been students in the past that could not figure out what was being asked of themselves?
 - “From, This device / location, Do this instruction” is one of the forms of questions
 - Other types of questions may be a list of question and a place for you to fill in the answerer
 - Yet other question could even ask you to provide a screen snap shot figure out how to use the built in snipping tool.
 - Snip out only the important information hence you can then make what you have snipped out as large as possible in the space provided, making it easier to read later, when doing review.



Cleaning out your switches & Routers

SW-1# **erase startup-config**

The response from the switch will be
Erasing the nvram file system will remove all files! Continue [confirm]
Press enter to confirm

SW-1# **delete vlan.dat**

Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
Press the enter key for both the prompts above
You may get an error message if there was no vlan.dat file found, this is OK

SW-1# **reload**

If the response says: "System configuration has been modified. Save?[yes/no]:"

Enter "no"

QUESTIONS

