Chapter 4: Network Access

Introduction to Networks 6.0
Planning Guide

Chapter 4 - Sections & Objectives

- 4.1 Physical Layer Protocols
  - Explain how physical layer protocols and services support communications across data networks.
  - Identify device connectivity options.
  - Describe the purpose and functions of the physical layer in the network.
  - Describe basic principles of the physical layer standards.
- 4.2 Network Media
  - Build a simple network using the appropriate media.
  - Identify the basic characteristics of copper cabling.
  - Build a UTP cable used in Ethernet networks. (scope - does not include cabling area discussion)
  - Describe fiber optic cabling and its main advantages over other media.
  - Connect devices using wired and wireless media.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 4 - Sections & Objectives (Cont.)

- 4.3 Data Link Layer Protocols
  - Explain the role of the data link layer in supporting communications across data networks.
  - Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.
- 4.4 Media Access Control
  - Compare media access control techniques and logical topologies used in networks.
  - Compare the functions of logical topologies and physical topologies.
  - Describe the basic characteristics of media access control methods on WAN topologies.
  - Describe the basic characteristics of media access control methods on LAN topologies.
  - Describe the characteristics and functions of the data link frame.

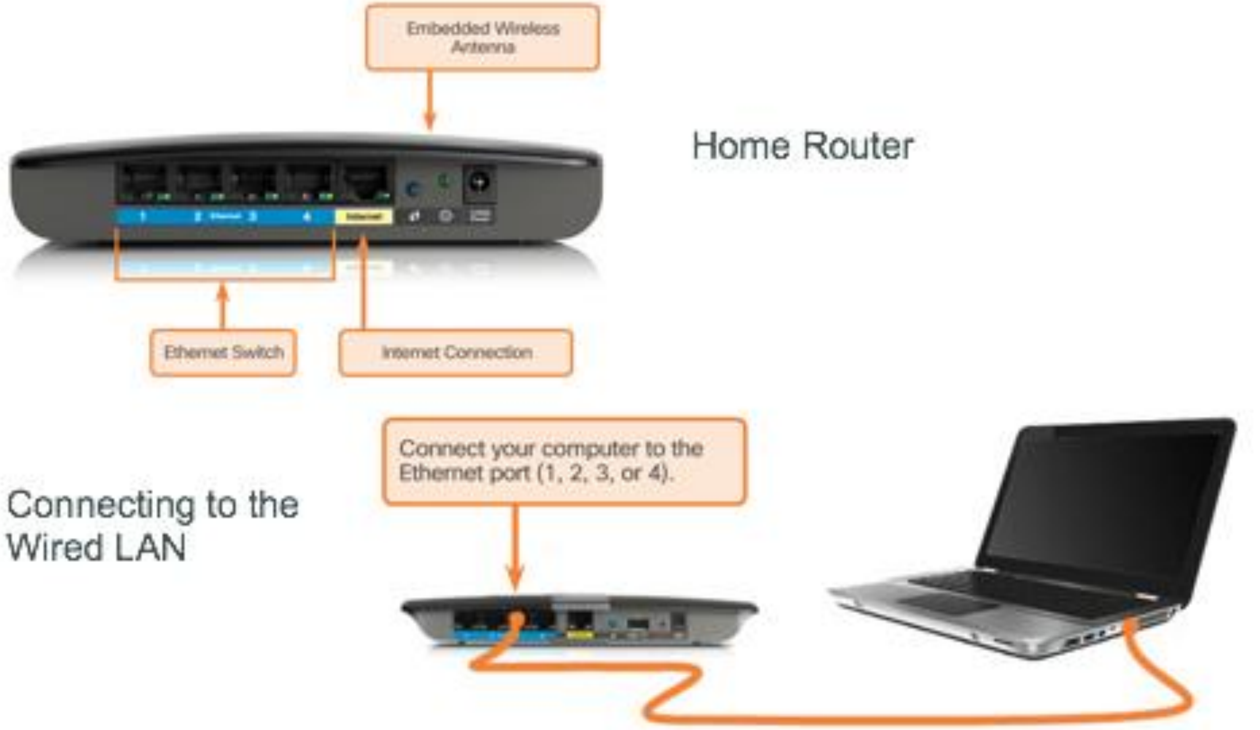
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.1 Physical Layer Protocols

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of Connections

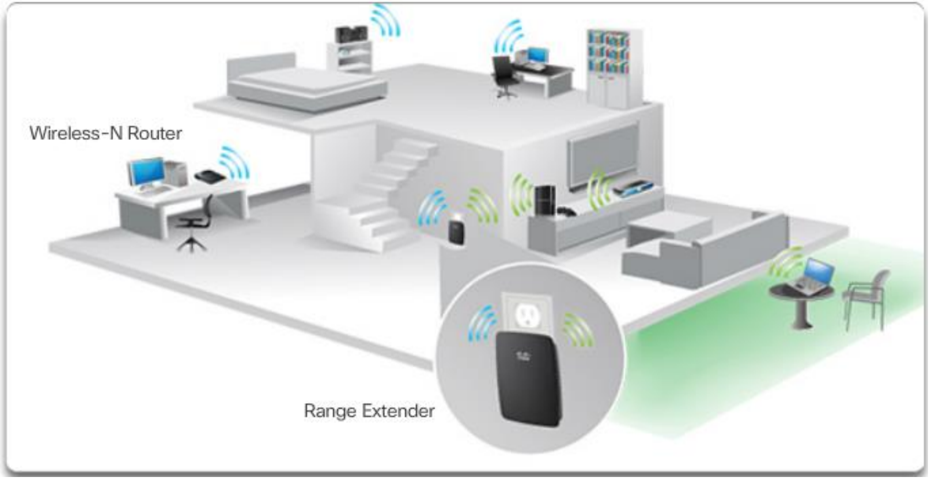
- Before network communications can occur, a physical connection to a local network must be established.
- A physical connection can be a wired connection using a cable or a wireless connection using radio waves.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Interface Cards

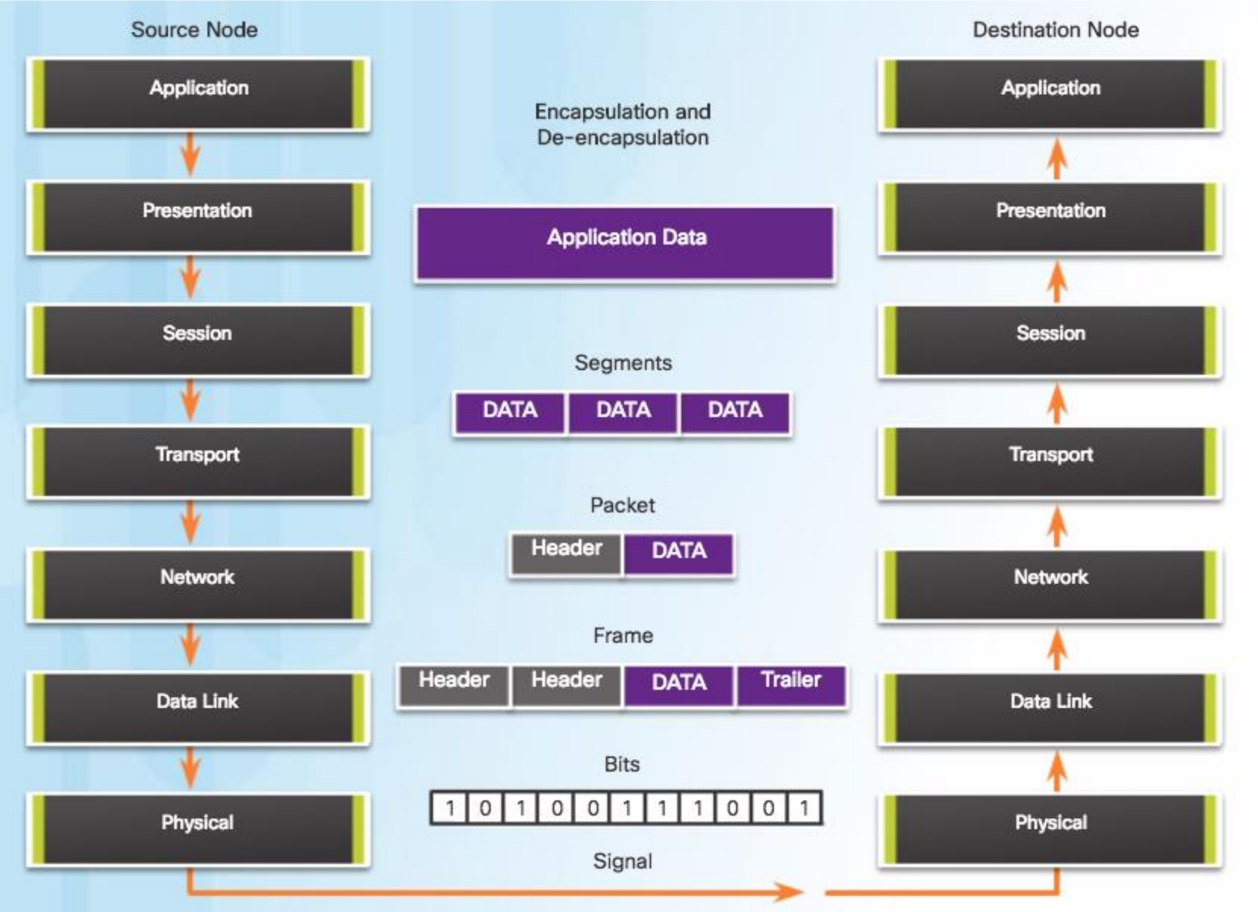
- Network Interface Cards (NICs) connect a device to a network.
- Used for a wired connection.



- Wireless Local Area Network (WLAN) NICs are used for wireless connections.

The Physical Layer

- Provides the means to transport the bits that make up a data link layer frame across the network media.
- Accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted onto the local media.
- Encoded bits that comprise a frame are received by either an end device or an intermediate device.

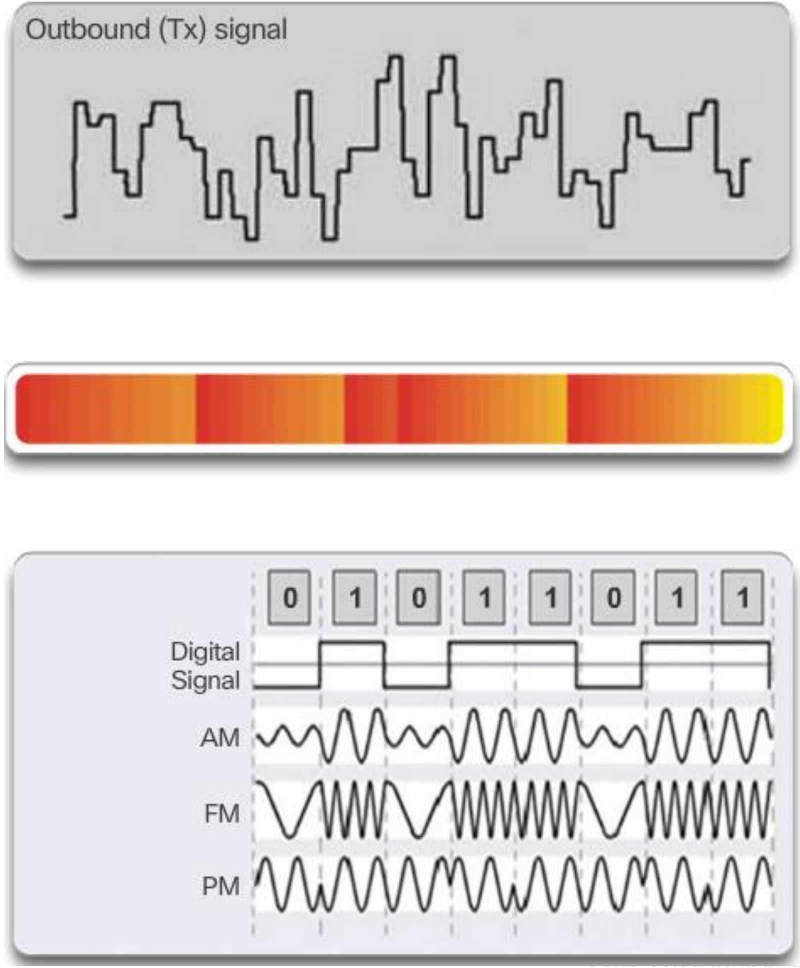


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Purpose of the Physical Layer

Physical Layer Media

Three basic forms of network media



Electrical Signals - Copper cable

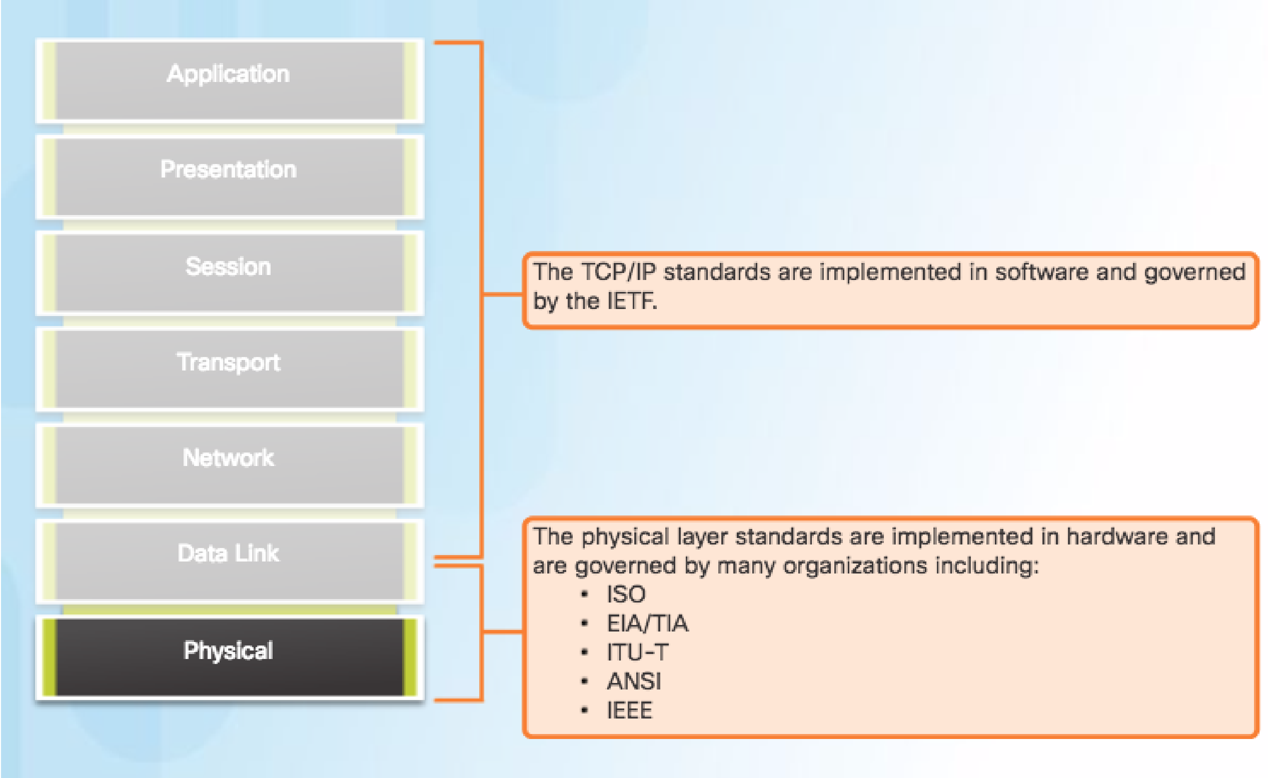
Light Pulse - Fiber-optic cable

Microwave Signals - Wireless

Purpose of the Physical Layer

Physical Layer Standards

- International Organization for Standardization (ISO)
- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)
- International Telecommunication Union (ITU)
- American National Standards Institute (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab - Identifying Network Devices and Cabling

Cisco Networking Academy®

Mind Wide Open™

Lab A - Identifying Network Devices and Cabling

Objectives

Part 1: Identify Network Devices

Part 2: Identify Network Media

Background / Scenario

As a member of the networking support staff, you must be able to identify different networking equipment. You must also understand the function of equipment in the appropriate part of the network. In this lab, you will have access to network devices and media. You will identify the type and characteristics of the network equipment and media.

Part 1: Identify Network Devices

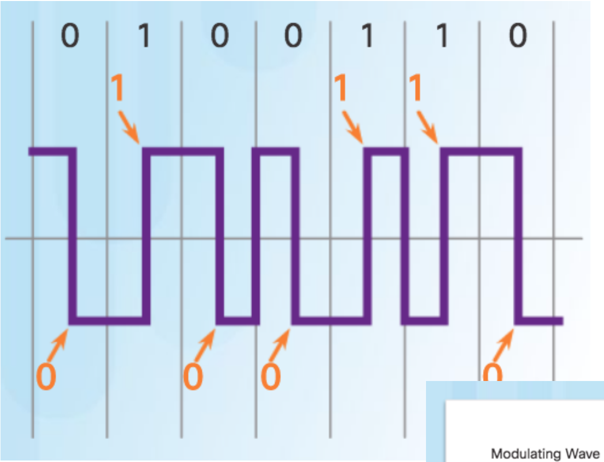
Your instructor will provide various network devices for identification. Each will be tagged with an ID number.

Fill in the table below with the device tag ID number, manufacturer, device model, type (hub, switch, and router), functionality (wireless, router, switch, or combination), and other physical characteristics, such as number of interface types. The first line is filled out as a reference.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

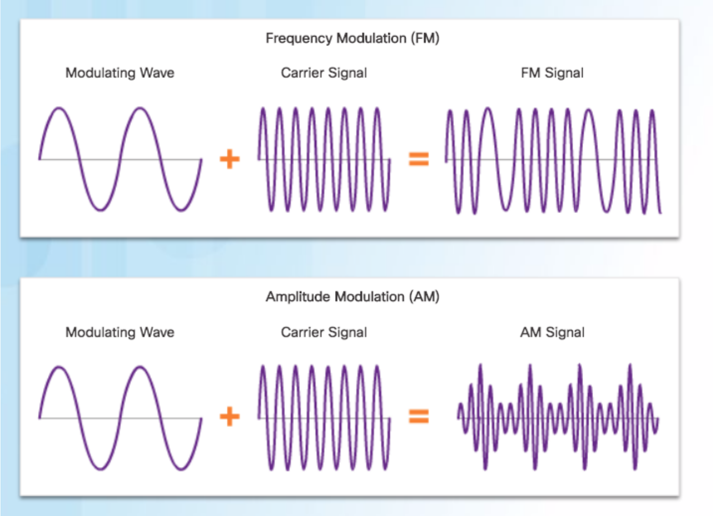
Functions

- Encoding
  - Method of converting a stream of data bits into a predefined "code".
- Signaling Method
  - Method of representing the bits.
  - Physical layer standards must define what type of signal represents a "1" and what type of signal represents a "0".
  - Long pulse might represent a 1 whereas a short pulse represents a 0.



The transition occurs at the middle of each bit period.

Modulation is the process by which the characteristic of one wave (the signal) modifies another wave (the carrier).



Bandwidth

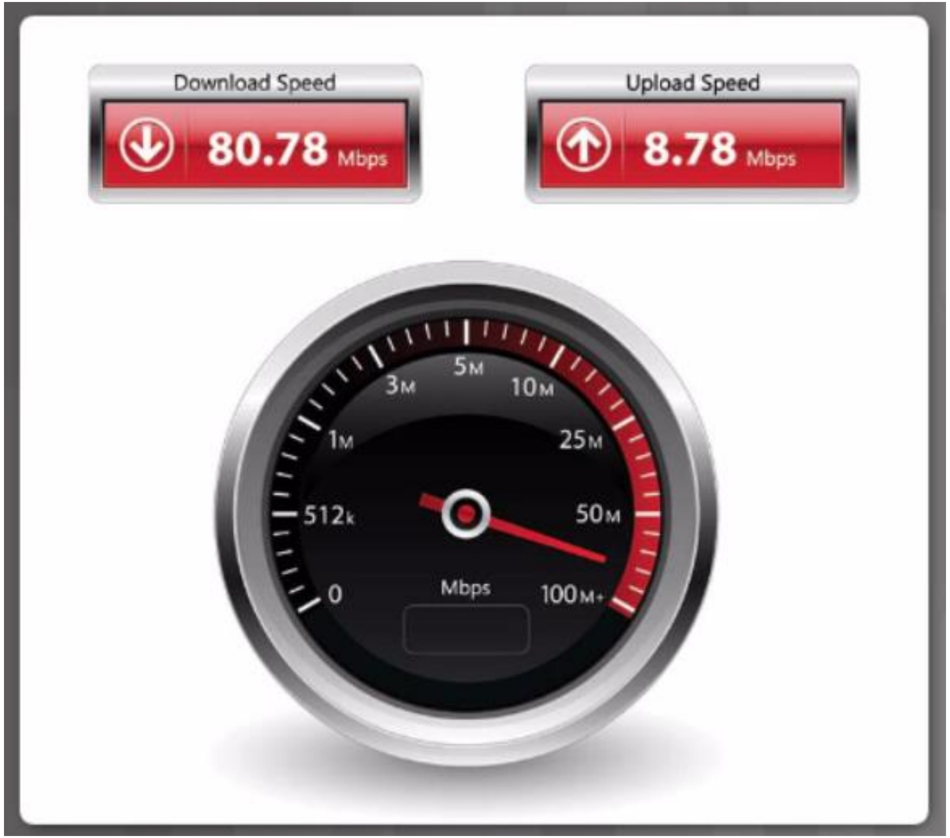
- Capacity of a medium to carry data.
- Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time.
- Bandwidth is sometimes thought of as the speed that bits travel, however this is not accurate. In both 10Mb/s and 100Mb/s Ethernet, the bits are sent at the speed of electricity. The difference is the number of bits that are transmitted per second.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	b/s	1 b/s = fundamental unit of bandwidth
Kilobits per second	kb/s	1 kb/s = 1,000 bps = 10^3 bps
Megabits per second	Mb/s	1 Mb/s = 1,000,000 bps = 10^6 bps
Gigabits per second	Gb/s	1 Gb/s = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tb/s	1 Tb/s = 1,000,000,000,000 bps = 10^12 bps

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Throughput

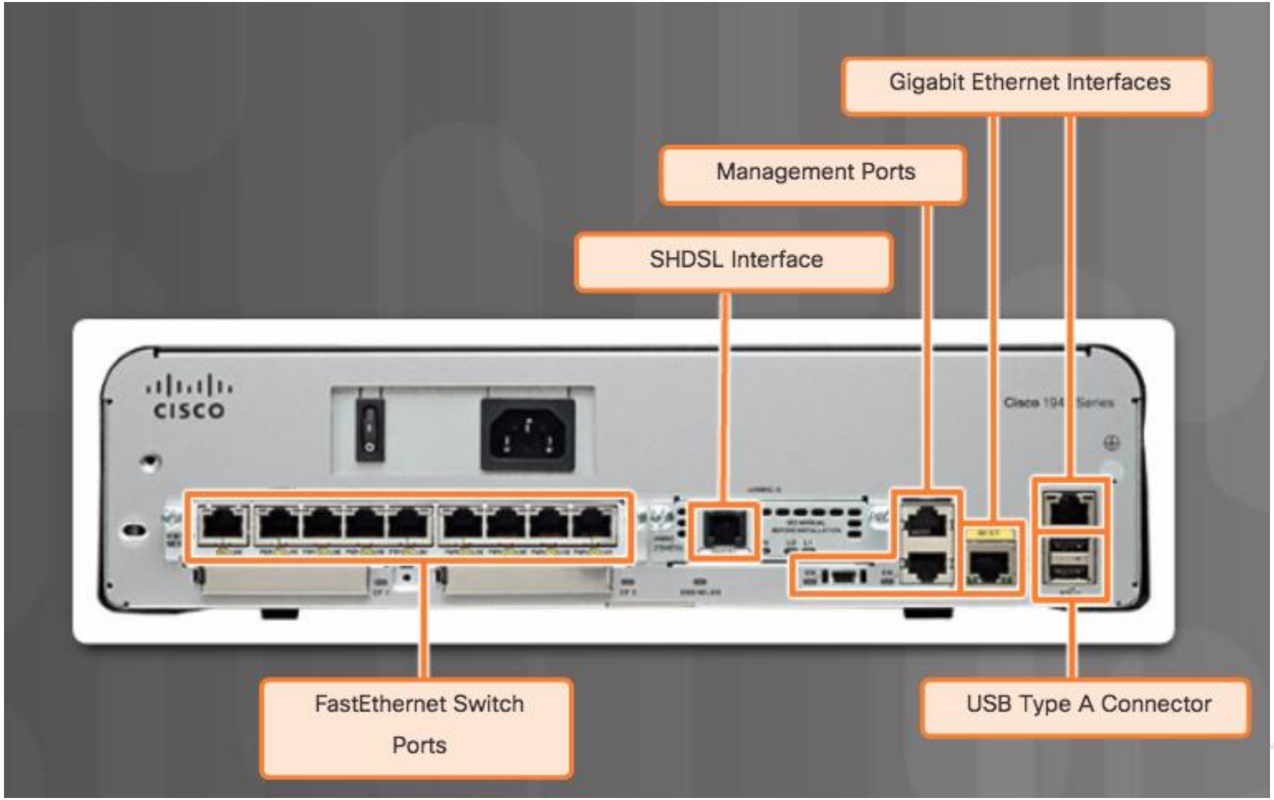
- Measure of the transfer of bits across the media over a given period of time.
- Usually does not match the specified bandwidth in physical layer implementations due to many factors.
  - Amount of traffic
  - Type of traffic
  - Latency created by network devices encountered between source and destination
- **Goodput** is throughput minus traffic overhead for establishing sessions, acknowledgments, and encapsulation.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of Physical Media

The figure shows different types of interfaces and ports available on a 1941 router.

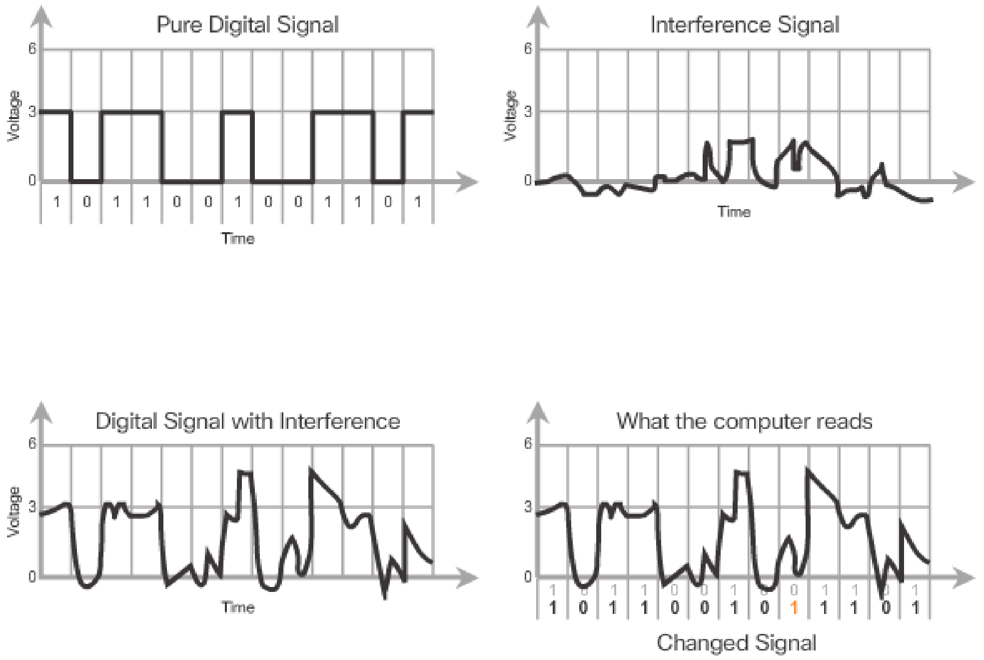


4.2 Network Media

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Characteristics of Copper Media

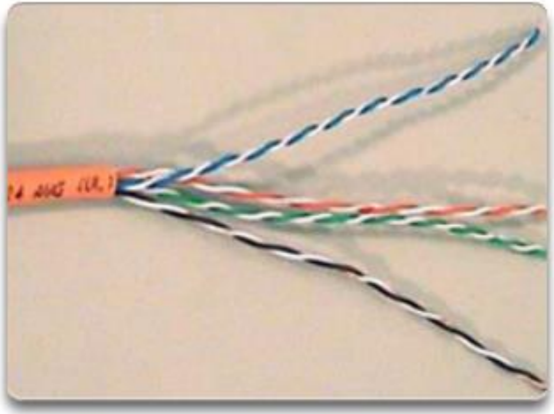
- Transmitted on copper cables as electrical pulses.
- Attenuation - the longer the signal travels, the more it deteriorates.
- All copper media must follow strict distance limitations.
- Electromagnetic interference (EMI) or radio frequency interference (RFI) - distorts and corrupts the data signals being carried by copper media.
  - To counter copper cables wrapped in shielding.
- Crosstalk - disturbance caused by the electric or magnetic fields of a signal on one wire to the signal in an adjacent wire.
  - To cancel crosstalk opposing circuit wire pairs twisted together.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

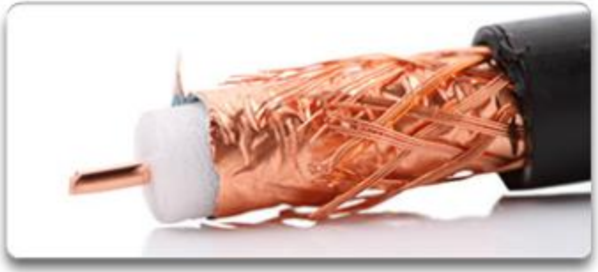
Copper Media

There are three main types of copper media used in networking.



Unshielded Twisted-Pair (UTP) cable

Shielded Twisted-Pair (STP) cable

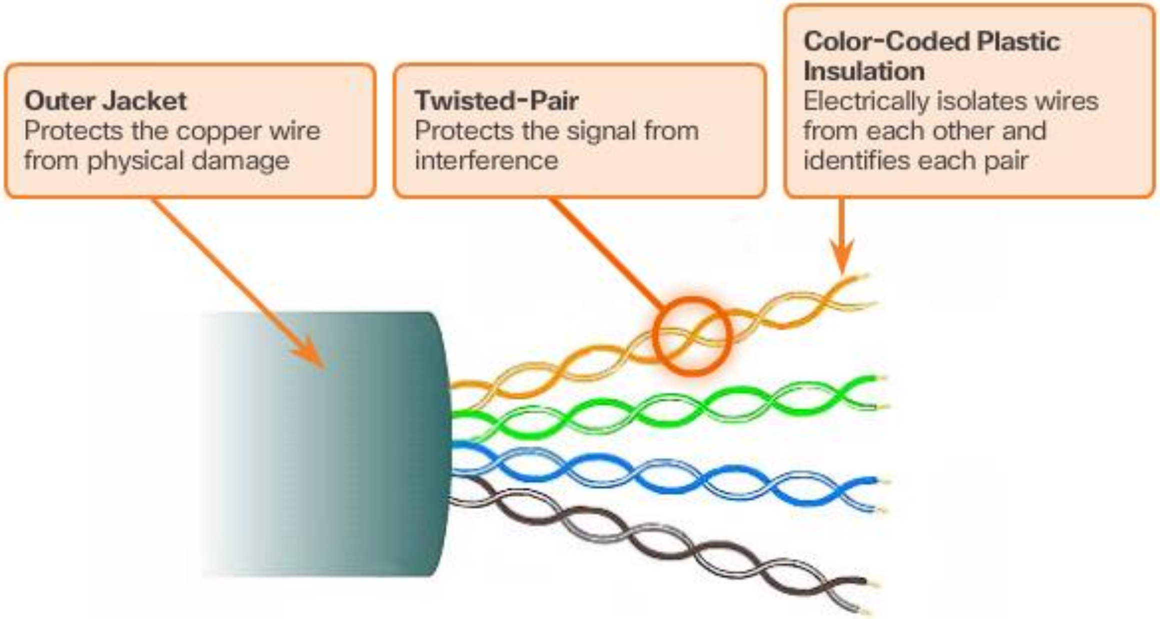


Coaxial cable

es. All rights reserved. Cisco Confidential

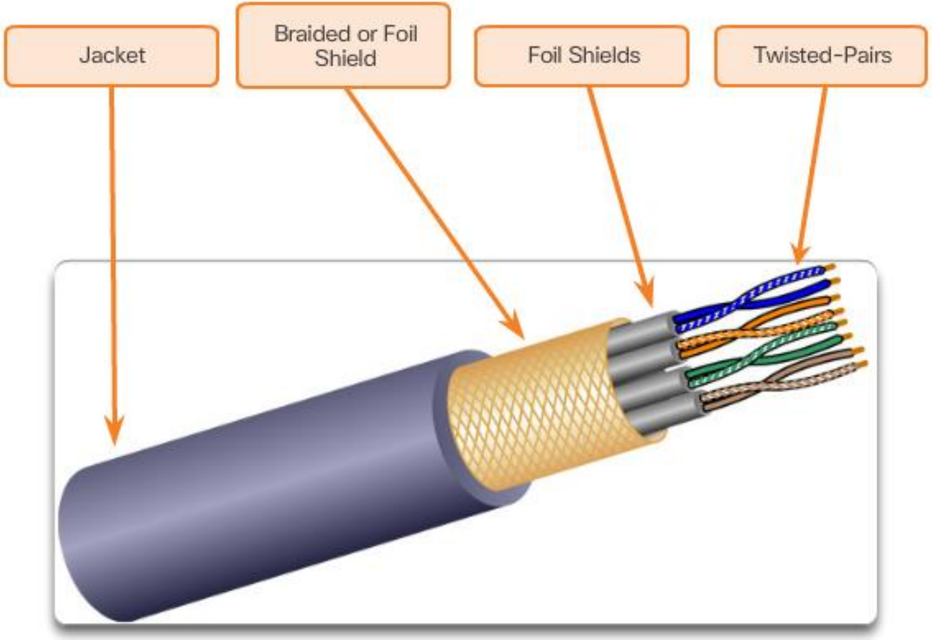
Unshielded Twisted-Pair Cable

- UTP cabling is the most common networking media.
  - Terminated with RJ-45 connectors.
  - Used for interconnecting network hosts with networking devices such as switches.
  - Consists of four pairs of color-coded wires that have been twisted together to help protect against signal interference from other wires.
  - Color codes aid in cable termination.



Shielded Twisted-Pair (STP) Cable

- STP provides better noise protection than UTP.
- STP cable is significantly more expensive and difficult to install.
- Uses an RJ-45 connector.
- Combines the techniques of shielding to counter EMI and RFI, and wire twisting to counter crosstalk.
- Uses four pairs of wires, each wrapped in a foil shield, which are then wrapped in an overall metallic braid or foil.

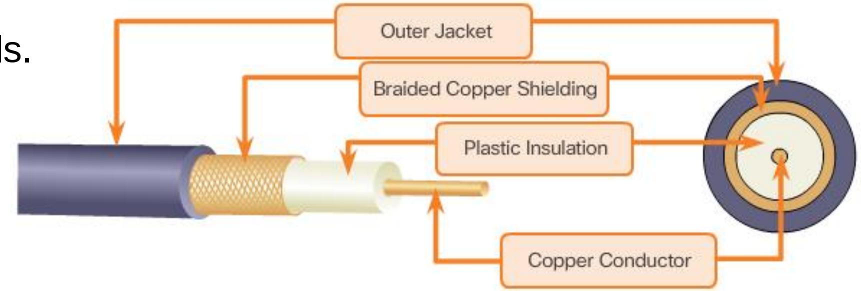


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Copper Cabling

Coaxial Cable

- Coax consists of:
  - A copper conductor used to transmit the electronic signals.
  - A layer of flexible plastic insulation surrounding a copper conductor.
  - The insulating material is surrounded in a woven copper braid, or metallic foil, that acts as the second wire in the circuit and as a shield for the inner conductor.
  - The entire cable is covered with a cable jacket to prevent minor physical damage.
- UTP cable has essentially replaced coaxial cable in modern Ethernet installations but is used in:
  - Wireless installations: Coaxial cables attach antennas to wireless devices.
  - Cable Internet installations



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Copper Media Safety

Copper media are susceptible to fire and electrical hazards.

The separation of data and electrical power cabling must comply with safety codes.

Cables must be connected correctly.

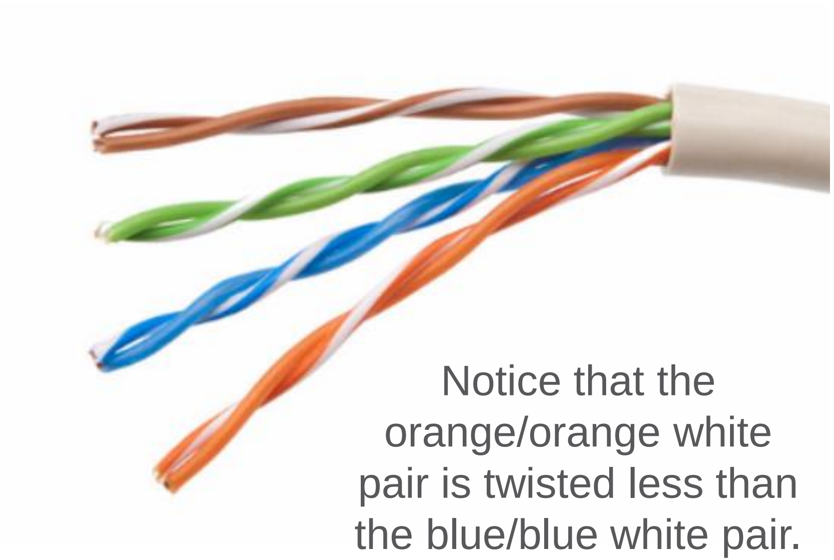
Installations must be inspected for damage.

Equipment must be grounded correctly.

s. All rights reserved. Cisco Confidential

Properties of UTP Cabling

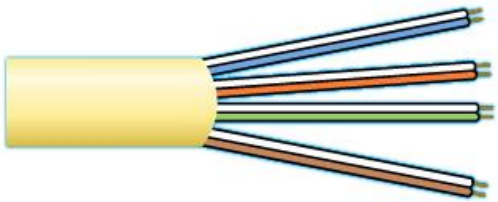
- Consists of four pairs of color-coded copper wires that have been twisted together and then encased in a flexible plastic sheath.
- Small size can be advantageous during installation.
- UTP cable does not use shielding to counter the effects of EMI and RFI.
  - Cancellation: When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other and cancel out any outside EMI and RFI signals.
  - Varies the number of twists per wire pair to further enhance the cancellation effect of a paired circuit.



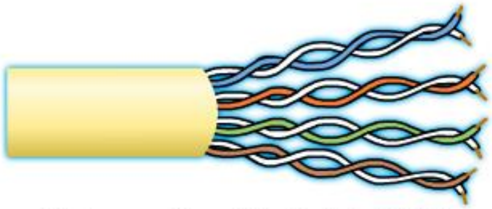
Notice that the orange/orange white pair is twisted less than the blue/blue white pair. Each colored pair is twisted a different number of times.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

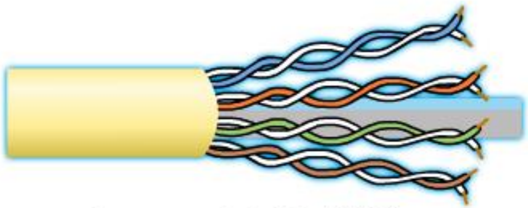
UTP Cabling Standards



Category 3 Cable (UTP)



Category 5 and 5e Cable (UTP)



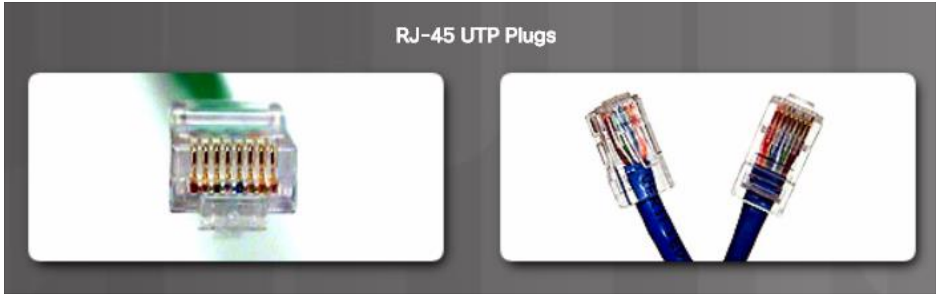
Category 6 Cable (UTP)

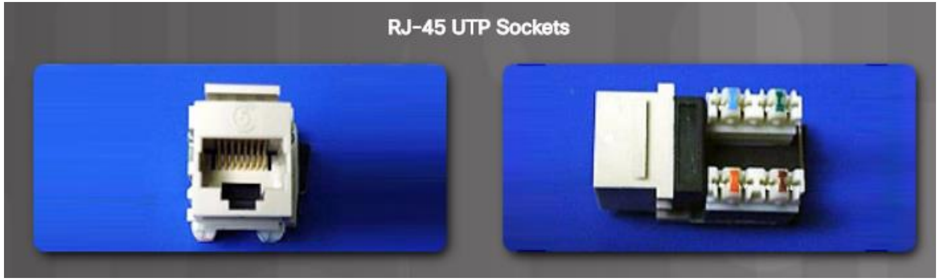
- UTP cabling conforms to the standards established by TIA/EIA.
  - TIA/EIA-568 stipulates the cabling standards for LAN installations
- Cat 3 Cable
  - Used for voice communication
  - Most often used for phone lines
- Cat 5 and 5e Cable
  - Used for data transmission
  - Cat5 supports 100 Mb/s and can support 1000Mb/s, but it is not recommended
  - Cat5e supports 1000 Mb/s
- Cat 6 Cable
  - Used for data transmission
  - An added separator is between each pair of wires allowing it to function at higher speeds
  - Support 1000 Mb/s – 10 Gb/s, though 10 Gb/s is not recommended

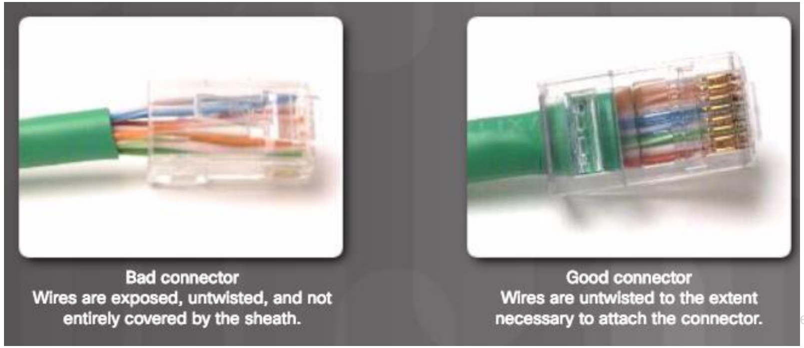
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UTP Connectors

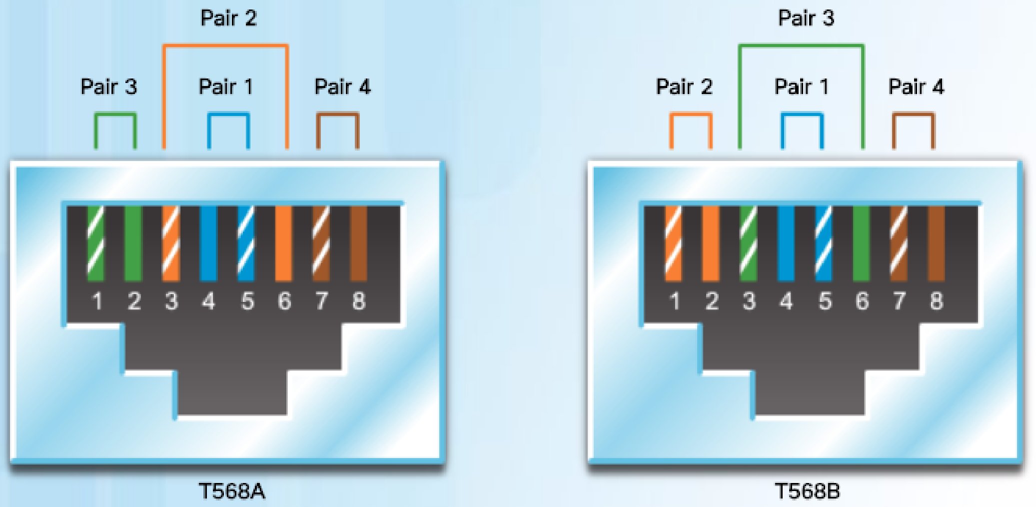
- UTP cable terminated with an RJ-45 connector.
- TIA/EIA-568 standard describes the wire color codes to pin assignments (pinouts) for Ethernet cables.
- RJ-45 connector is the male component, crimped at the end of the cable.
- Socket is the female component of a network device, wall, cubicle partition outlet, or patch panel.
- Essential that all copper media terminations be of high quality to ensure optimum performance with current and future network technologies.







Types of UTP Cable



Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, Other end T568B	• Connects two network hosts • Connects two network intermediary devices (switch to switch, or router to router)
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter.

Testing UTP Cables

UTP Testing Parameters:

- Wire map
- Cable length
- Signal loss due to attenuation
- Crosstalk

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

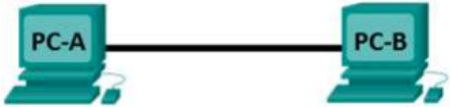
Lab - Building an Ethernet Crossover Cable

Cisco Networking Academy®

Mind Wide Open™

Lab - Building an Ethernet Crossover Cable

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC-A	NIC	192.168.10.1	255.255.255.0	N/A
PC-B	NIC	192.168.10.2	255.255.255.0	N/A

Objectives

Part 1: Analyze Ethernet Cabling Standards and Pinouts

Part 2: Build an Ethernet Crossover Cable

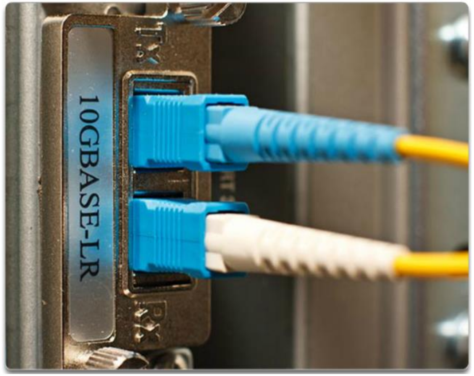
Part 3: Test an Ethernet Crossover Cable

Background / Scenario

In this lab, you will build and terminate an Ethernet crossover cable and test it by connecting two PCs together and pinging between them. You will first analyze the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) 568-A and 568-B standards and how they apply to Ethernet cables. You will then construct an Ethernet crossover cable and test it. Finally, you will use the cable you just constructed to connect two PCs together and test it by pinging between them.

Note: With autosensing capabilities available on many devices, such as the Cisco 1941 Integrated Services Router (ISR) switch, you may see straight-through cables connecting like devices.

Properties of Fiber Optic Cabling

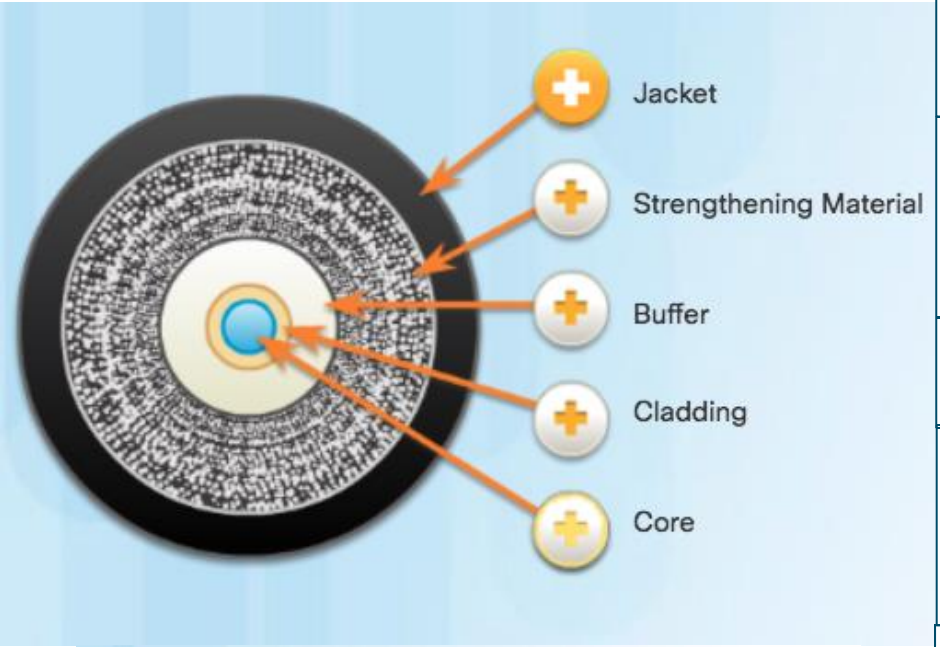


- Fiber-optic cabling is now being used in four types of industry:
  - Enterprise Networks
  - Fiber-to-the-Home (FTTH)
  - Long-Haul Networks
  - Submarine Cable Networks

- Transmits data over longer distances and at higher bandwidths.
- Transmit signals with less attenuation and is completely immune to EMI and RFI.
- Used to interconnect network devices.
- Flexible, but extremely thin, transparent strand of very pure glass, not much bigger than a human hair.
- Bits are encoded on the fiber as light pulses.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fiber Media Cable Design



Jacket
Protects the fiber against abrasion, moisture, and other contaminants. Composition can vary depending on the cable usage.

Strengthening Material
Surrounds the buffer, prevents the fiber cable from being stretched when it is being pulled. Often the same material used to produce bulletproof vests.

Buffer
Used to help shield the core and cladding from damage.

Cladding
Tends to act like a mirror by reflecting light back in the core of the fiber. Keeps light in the core as it travels down the fiber.

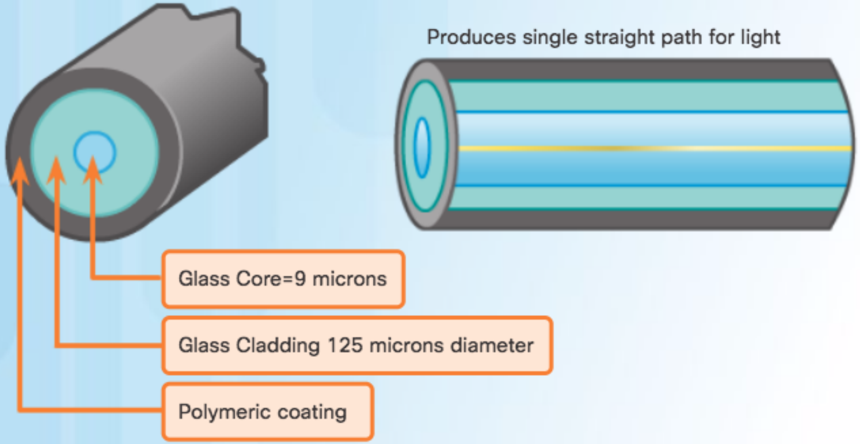
Core
Light transmission element at the center of the optical fiber. Core is typically silica or glass. Light pulses travel through the fiber core.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fiber Optic Cabling

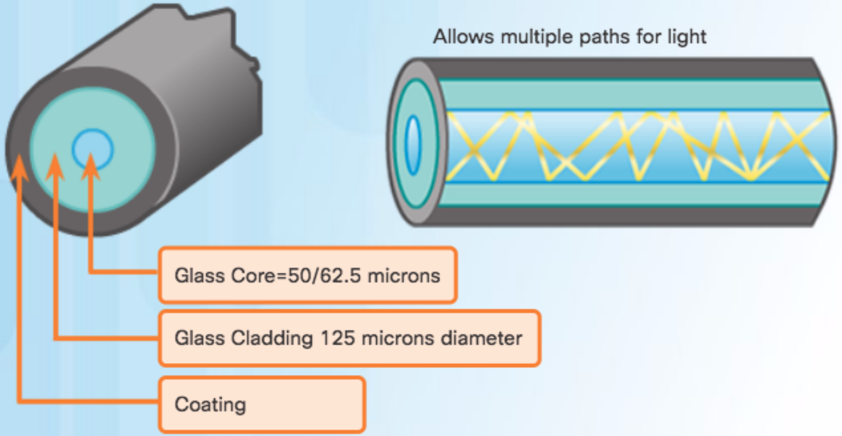
Types of Fiber Media

Single Mode



- Small core
- Less dispersion
- Suited for long distance applications
- Uses lasers as the light source
- Commonly used with campus backbones for distances of several thousand meters

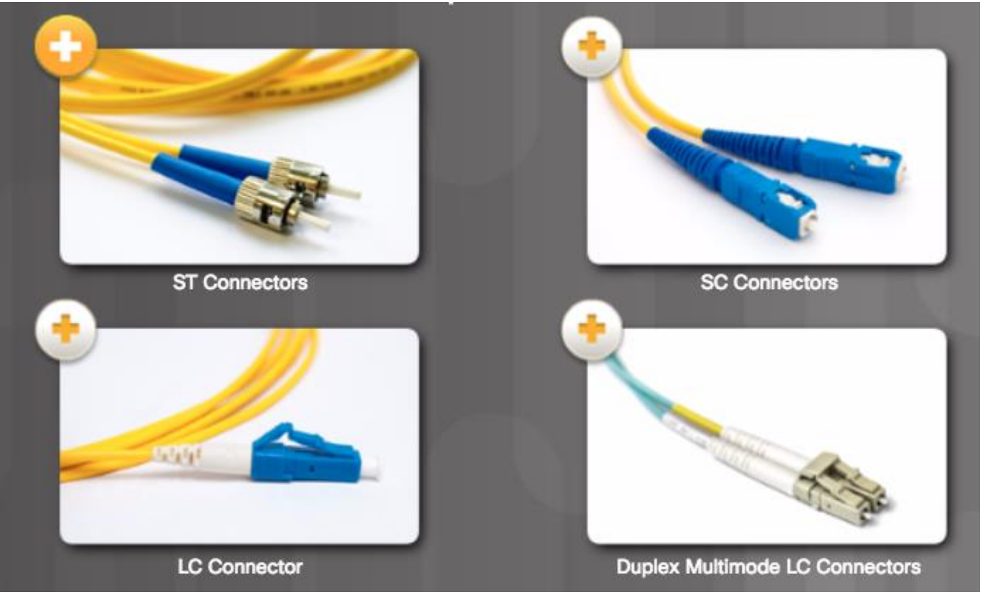
Multimode



- Larger core than single mode cable
- Allows greater dispersion and therefore, loss of signal
- Suited for long distance applications, but shorter than single mode
- Uses LEDs as the light source
- Commonly used with LANs or distances of a couple hundred meters within a campus network

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

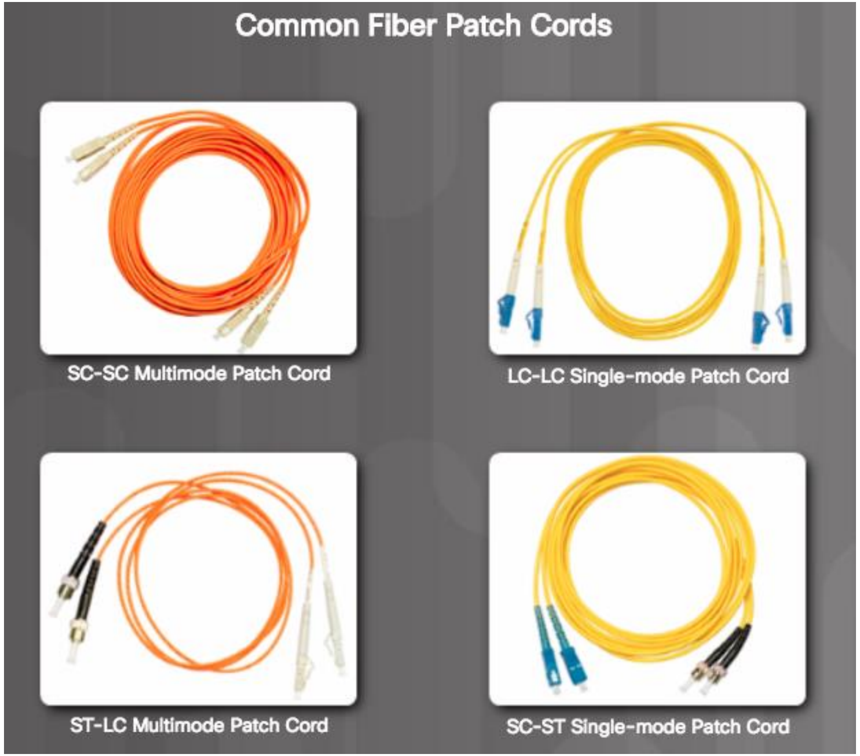
Fiber-Optic Connectors



- Light can only travel in one direction over optical fiber, two fibers are required to support the full duplex operation.
- Straight-Tip (ST) Connectors
  - One of the first connector types used.
  - Locks securely with a “twist-on/twist-off”.
- Subscriber Connector (SC) Connectors
  - Referred to as square or standard connector.
  - Uses a push-pull mechanism to ensure positive insertion.
  - Used with multimode and single-mode fiber.
- Lucent Connector (LC) Simplex Connectors
  - Smaller version of SC and popular due to size.
- Duplex Multimode LC Connectors
  - Similar to LC but using a duplex connector.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fiber-Optic Connectors (Cont.)



- Fiber patch cords are required for interconnecting infrastructure devices.
- Yellow jacket is for single-mode fiber cables
- Orange (or aqua) for multimode fiber cables.
- Fiber cables should be protected with a small plastic cap when not in use.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Testing Fiber Cables

Optical Time Domain Reflectometer (OTDR) can be used to test each fiber-optic cable segment

- Terminating and splicing fiber-optic cabling requires special training and equipment.
- Three common types of fiber-optic termination and splicing errors are:
  - **Misalignment**: The fiber-optic media are not precisely aligned to one another when joined.
  - **End gap**: The media does not completely touch at the splice or connection.
  - **End finish**: The media ends are not well polished, or dirt is present at the termination.
- Can be field tested by shining a bright flashlight into one end of the fiber while observing the other end.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fiber Optic Cabling

Fiber versus Copper

Implementation Issues	UTP Cabling	Fiber-optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively high (1 - 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Properties of Wireless Media

- Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies.
- Wireless areas of concern:
  - **Coverage area:** Construction materials used in buildings and structures, and the local terrain, will limit the coverage.
  - **Interference:** Disrupted by such common devices as fluorescent lights, microwave ovens, and other wireless communications.
  - **Security:** Devices and users, not authorized for access to the network, can gain access to the transmission.
  - **Shared medium:** Only one device can send or receive at a time and the wireless medium is shared amongst all wireless users.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of Wireless Media

- Wi-Fi: Standard IEEE 802.11
  - Uses Carrier/Sense Multiple Access/Collision Avoidance (CSMA/CA).
  - Wireless NIC must wait till channel is clear.
- Bluetooth: Standard IEEE 802.15
  - Wireless Personal Area Network (WPAN)
  - Uses a device pairing process for distances 1 to 100 meters
- WiMAX: Standard IEEE 802.16
  - Worldwide Interoperability for Microwave Access
  - Wireless broadband access.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Wireless LAN

Home and small business wireless routers integrate the functions of a router, switch, and access point into one device.

- Wireless LAN requires the following network devices:
  - **Wireless Access Point (AP)**: Concentrates the wireless signals from users and connects to the existing copper-based network infrastructure, such as Ethernet.
  - **Wireless NIC adapters**: Provide wireless communication capability to each network host.

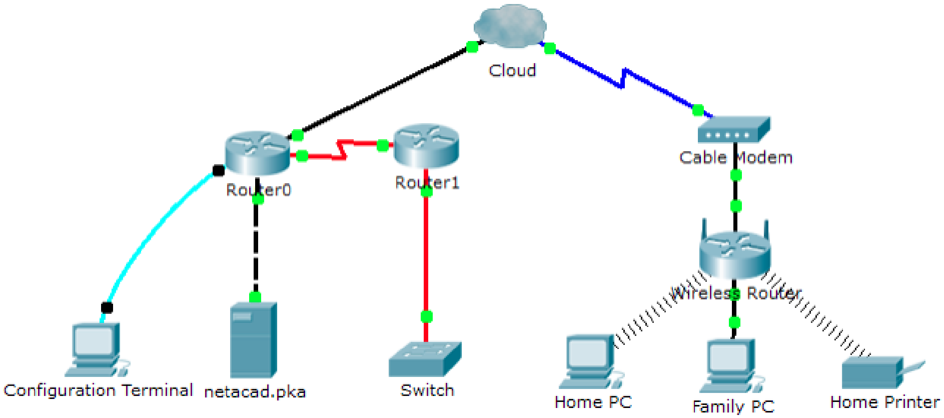
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer - Connecting a Wired and Wireless LAN

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Connecting a Wired and Wireless

Topology



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab - Viewing Wired and Wireless NIC Information

Cisco Networking Academy® Mind Wide Open™

Lab – Viewing Wireless and Wired NIC Information

Objectives

Part 1: Identify and Work with PC NICs

Part 2: Identify and Use the System Tray Network Icons

Background / Scenario

This lab requires you to determine the availability and status of the network interface cards (NICs) on the PC that you use. Windows provides a number of ways to view and work with your NICs.

In this lab, you will access the NIC information of your PC and change the status of these cards.

Required Resources

- 1 PC (Windows 7 or 8 with two NICs, wired and wireless, and a wireless connection)

Note: At the start of this lab, the wired Ethernet NIC in the PC was cabled to one of the integrated switch ports on a wireless router and the Local Area Connection (wired) was enabled. The wireless NIC was disabled initially. If the wired and wireless NICs are both enabled the PC will receive two different IP addresses and the wireless NIC will take precedence.

Part 1: Identify and Work with PC NICs

In Part 1, you will identify the NIC types in the PC that you are using. You will explore different ways to extract information about these NICs and how to activate and deactivate them.

Note: This lab was performed using a PC running on the Windows 7 operating system. You should be able to perform the lab with one of the other Windows operating systems listed; however, menu selections and screens may vary.

Step 1: Use the Network and Sharing Center.

a. Open the **Network and Sharing Center** by clicking the Windows **Start** button > **Control Panel** > **View network status and tasks** under Network and Internet heading in the Category View.

b. In the left pane, click the **Change adapter settings** link.

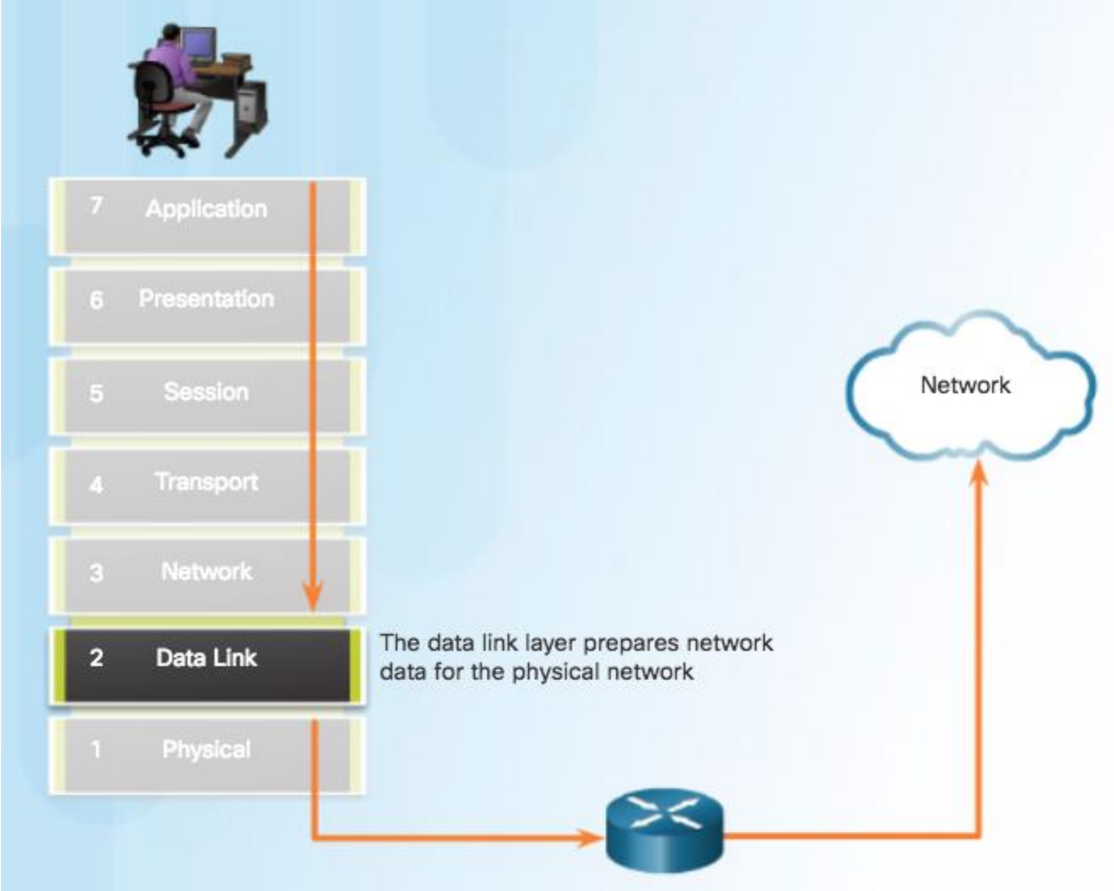
c. The Network Connections window displays, which provides the list of NICs available on this PC. Look for your Local Area Connection and Wireless Network Connection adapters in this window.

All rights reserved. Cisco Confidential

4.3 Data Link Protocols

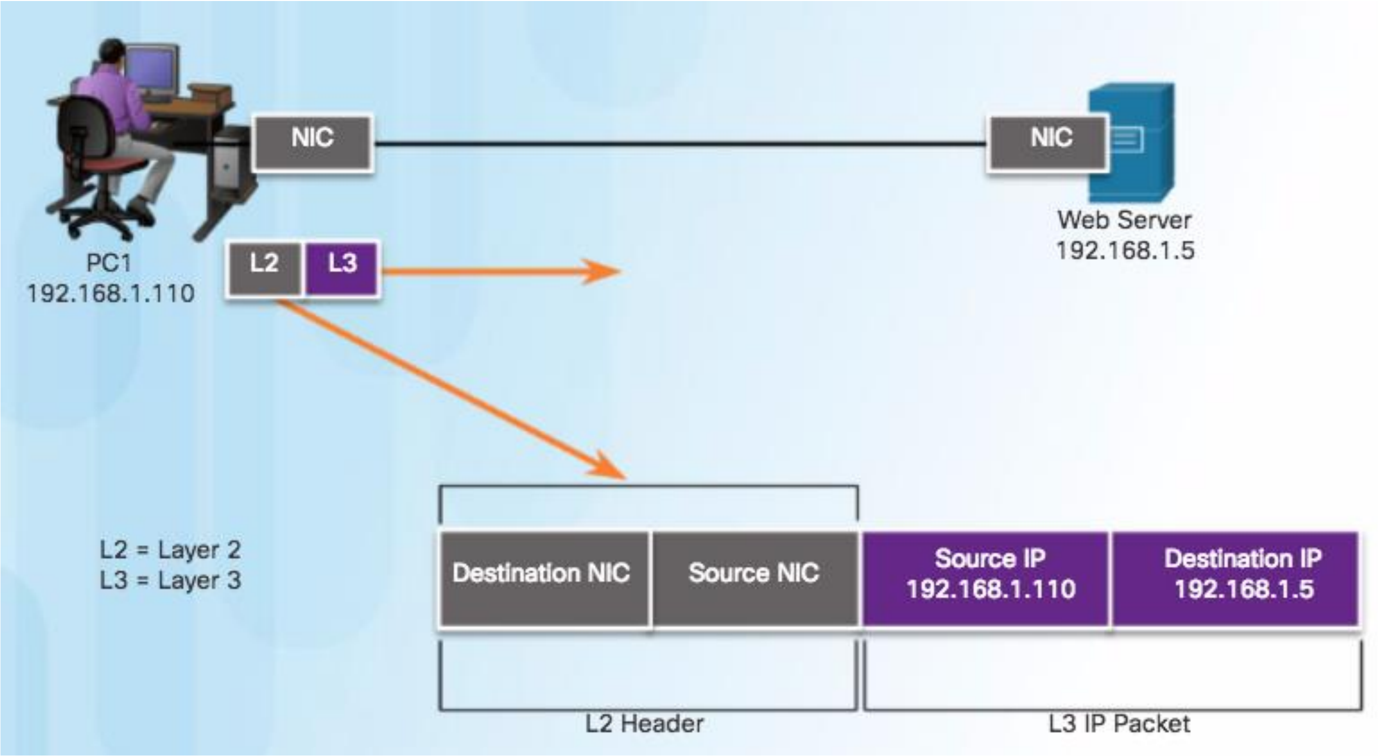
Purpose of the Data Link Layer

The Data Link Layer



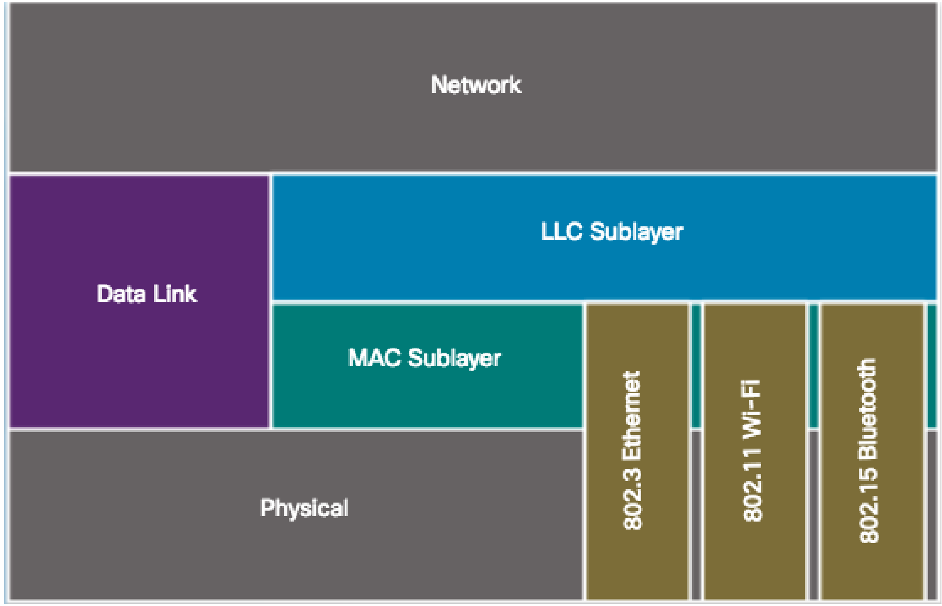
The Data Link Layer (Cont.)

Layer 2 Data Link Addresses



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

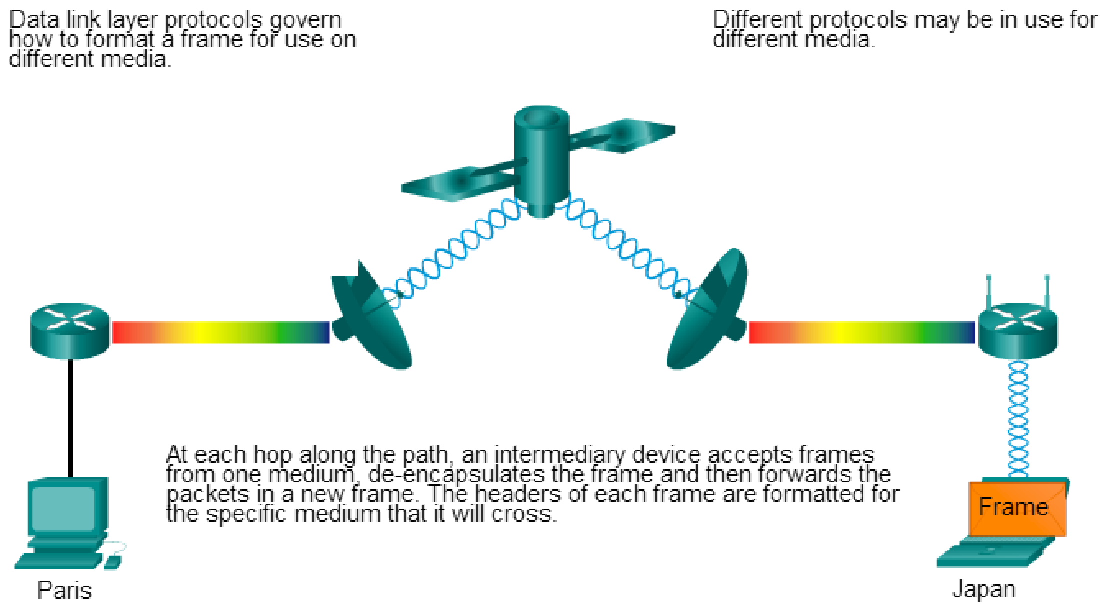
Data Link Sublayers



- Data link layer is divided into two sublayers:
  - **Logical Link Control (LLC)**
    - Communicates with the network layer.
    - Identifies which network layer protocol is being used for the frame.
    - Allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.
  - **Media Access Control (MAC)**
    - Defines the media access processes performed by the hardware.
    - Provides data link layer addressing and access to various network technologies.
    - Communicates with Ethernet to send and receive frames over copper or fiber-optic cable.
    - Communicates with wireless technologies such as Wi-Fi and Bluetooth.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

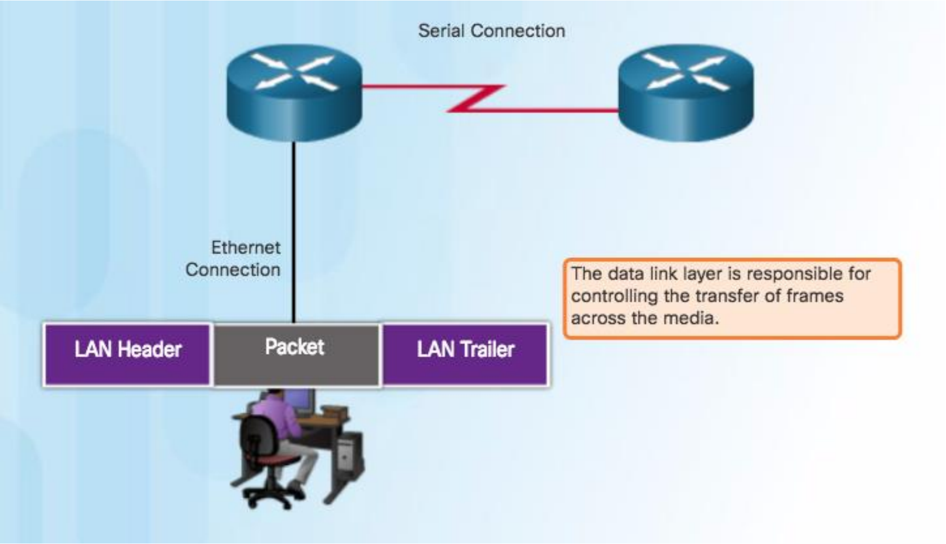
Media Access Control

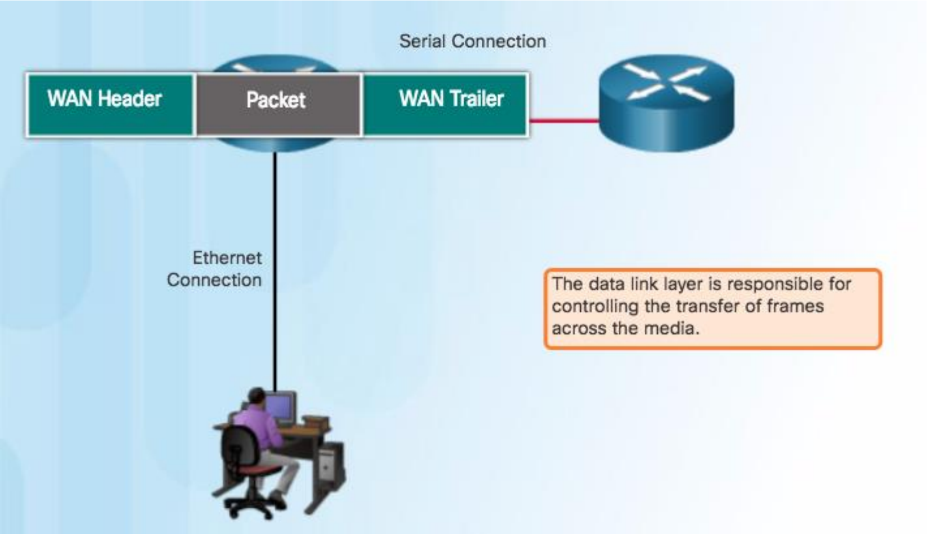


- As packets travel from the source host to the destination host, they travel over different physical networks.
- Physical networks can consist of different types of physical media such as copper wires, optical fibers, and wireless consisting of electromagnetic signals, radio and microwave frequencies, and satellite links.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Providing Access to Media





- At each hop along the path, a router:
  - Accepts a frame from a medium
  - De-encapsulates the frame
  - Re-encapsulates the packet into a new frame
  - Forwards the new frame appropriate to the medium of that segment

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Data Link Layer Standards

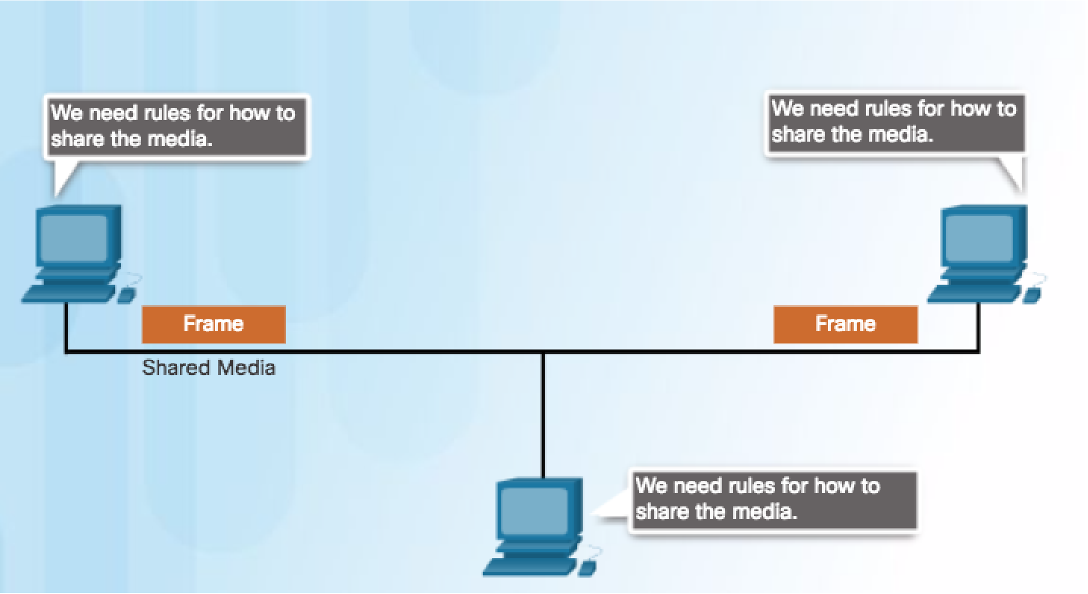
- Engineering organizations that define open standards and protocols that apply to the network access layer include:
  - Institute of Electrical and Electronics Engineers (IEEE)
  - International Telecommunication Union (ITU)
  - International Organization for Standardization (ISO)
  - American National Standards Institute (ANSI)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.4 Media Access Control

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Controlling Access to the Media

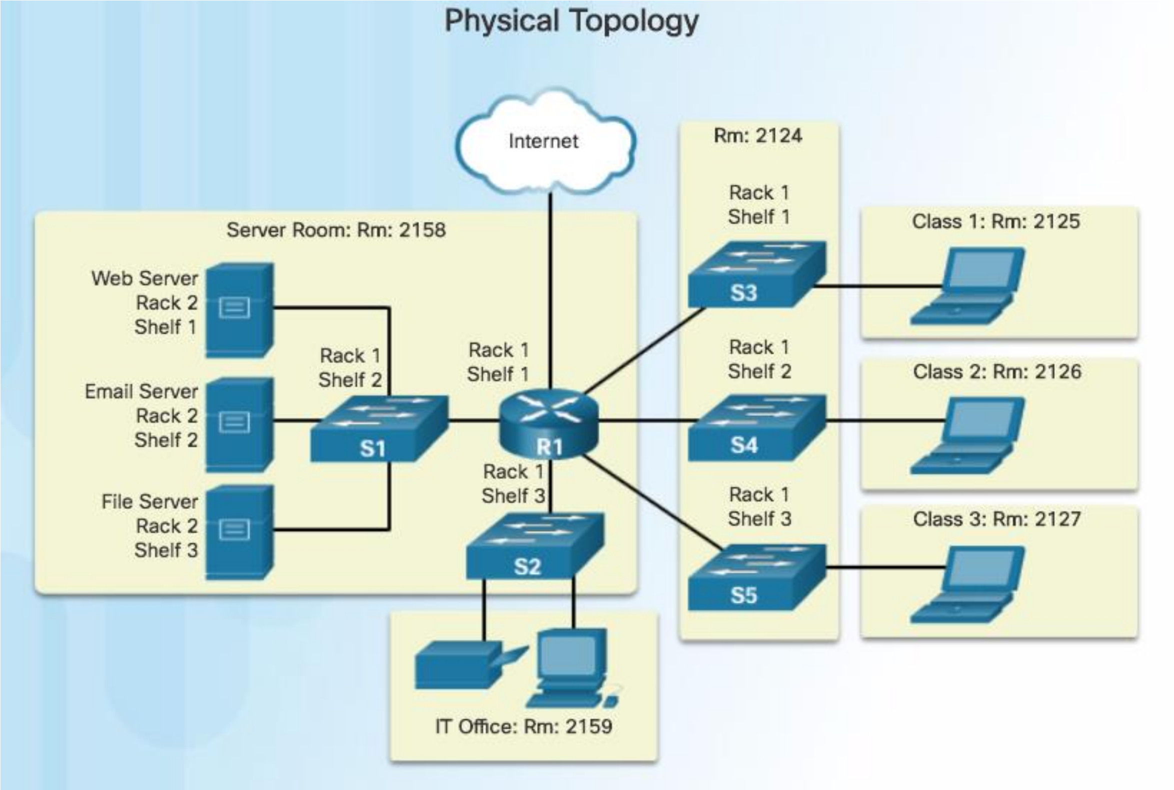


Sharing the Media

- Media access control is the equivalent of traffic rules that regulate the entrance of motor vehicles onto a roadway.
- The absence of any media access control would be the equivalent of vehicles ignoring all other traffic and entering the road without regard to the other vehicles.
- However, not all roads and entrances are the same. Traffic can enter the road by merging, by waiting for its turn at a stop sign, or by obeying signal lights. A driver follows a different set of rules for each type of entrance.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

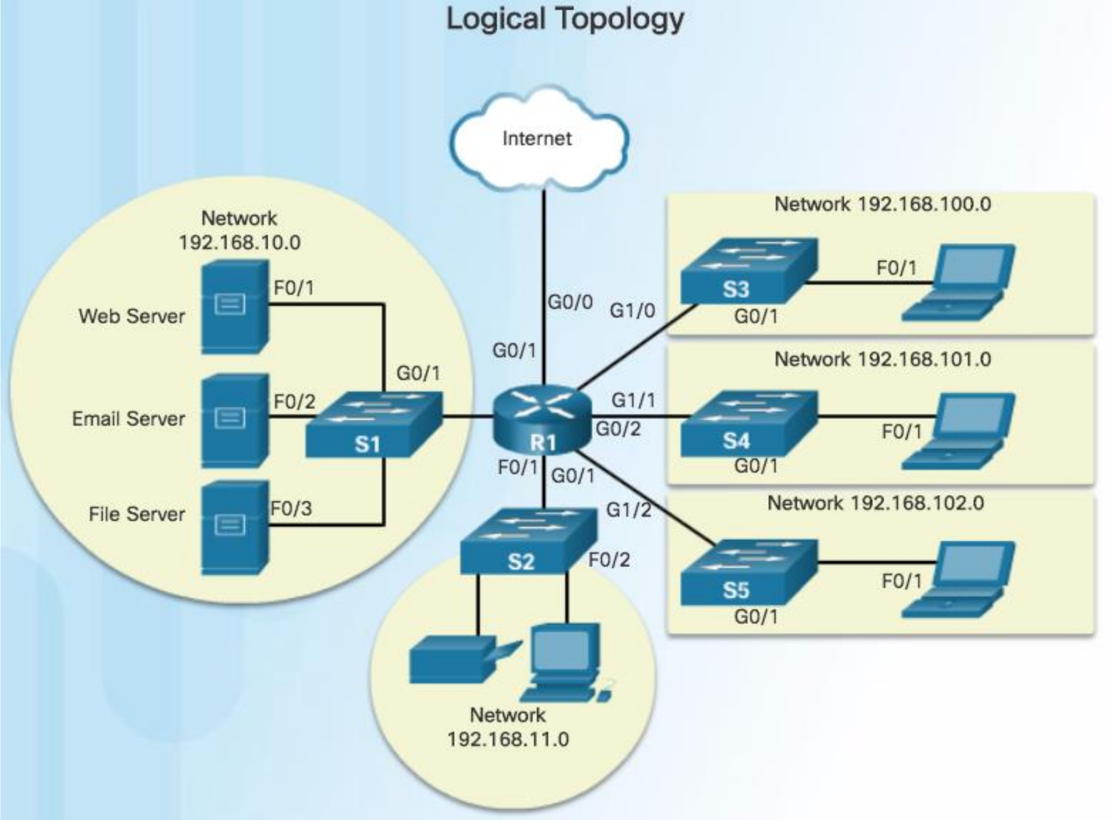
Physical and Logical Topologies



- **Physical topology** - Refers to the physical connections and identifies how end devices and infrastructure devices such as routers, switches, and wireless access points are interconnected.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

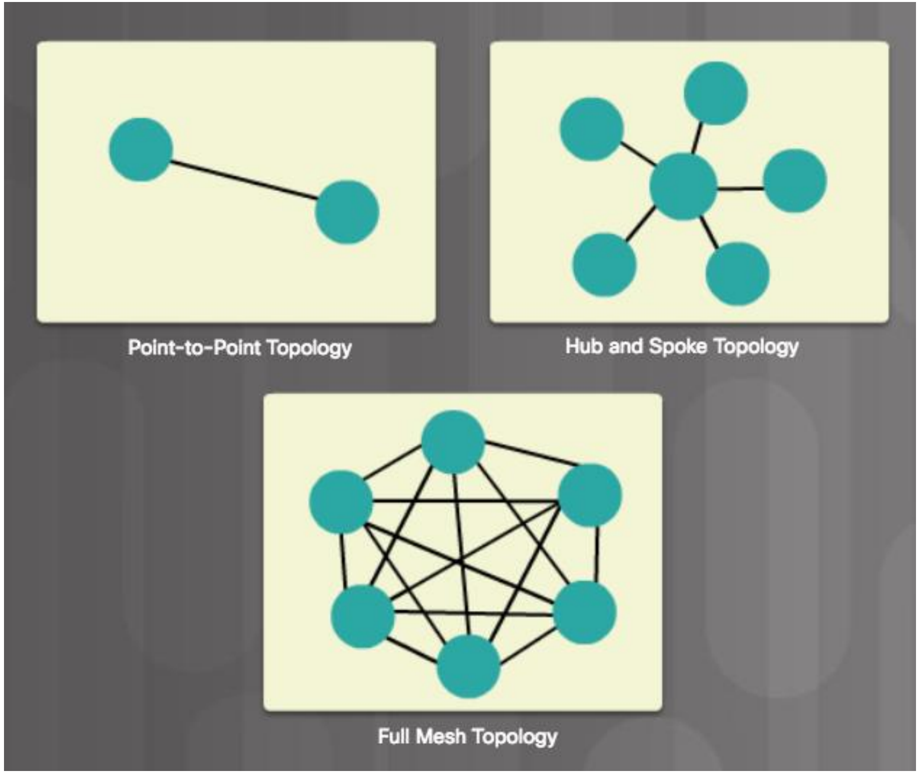
Physical and Logical Topologies (Cont.)



- **Logical Topology:** Refers to the way a network transfers frames from one node to the next. These logical signal paths are defined by data link layer protocols.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

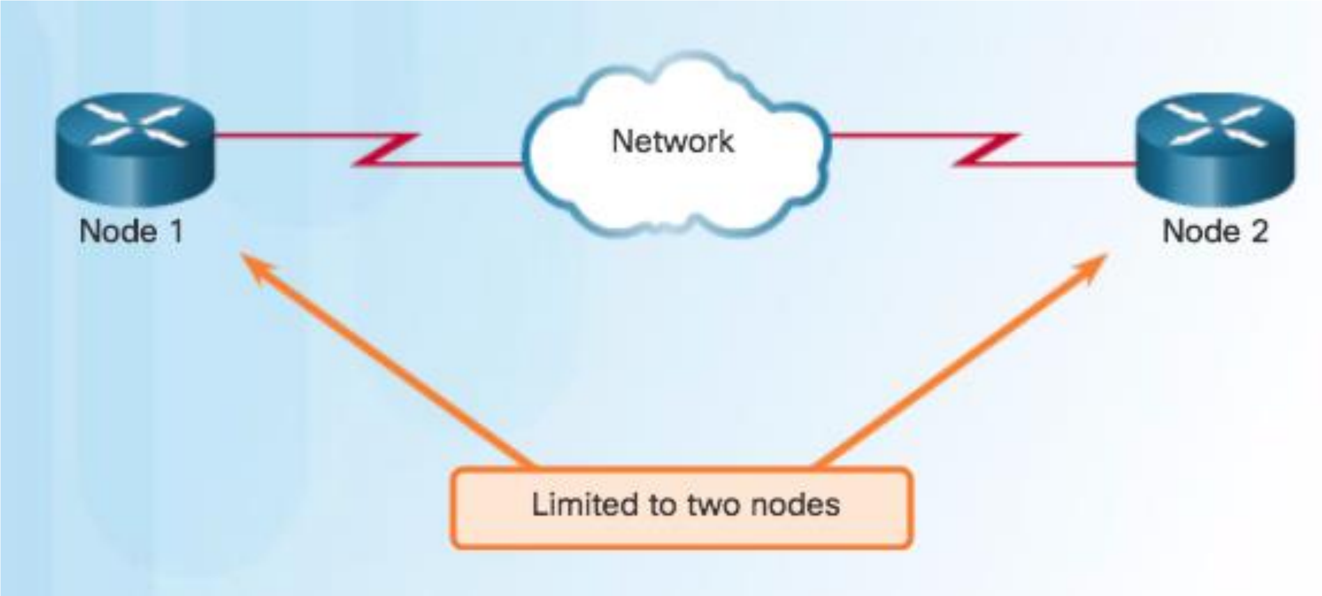
Common Physical WAN Topologies



- **Point-to-Point -** Permanent link between two endpoints.
- **Hub and Spoke** - A central site interconnects branch sites using point-to-point links.
- **Mesh** - Provides high availability, but requires that every end system be interconnected to every other system. Administrative and physical costs can be significant.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Physical Point-to-Point Topology



- Frames are placed on the media by the node at one end and taken from the media by the node at the other end of the point-to-point circuit.

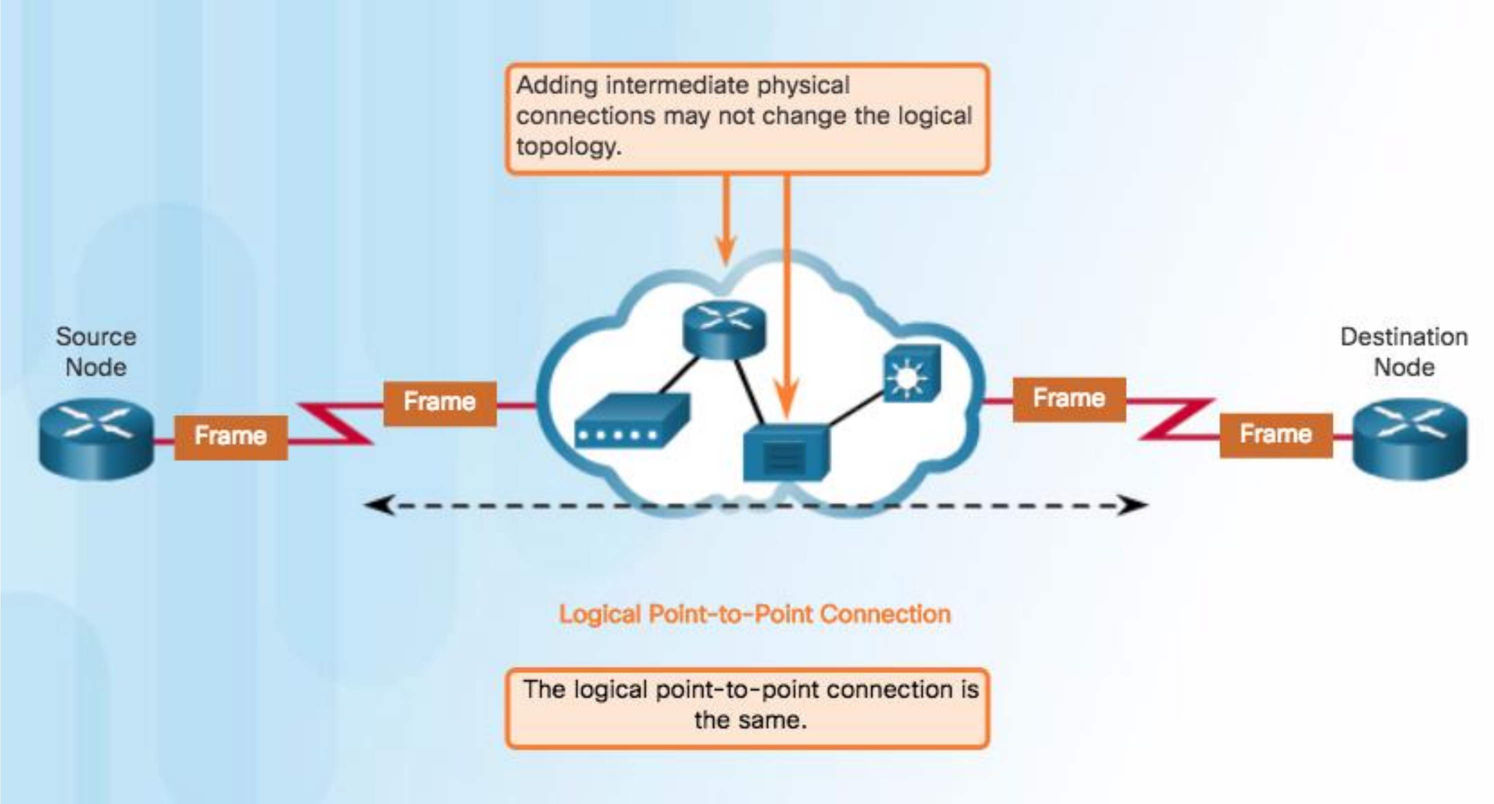
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Logical Point-to-Point Topology

- End nodes communicating in a point-to-point network can be physically connected via a number of intermediate devices.
- However, the use of physical devices in the network does not affect the logical topology.
- The logical connection between nodes forms what is called a virtual circuit.

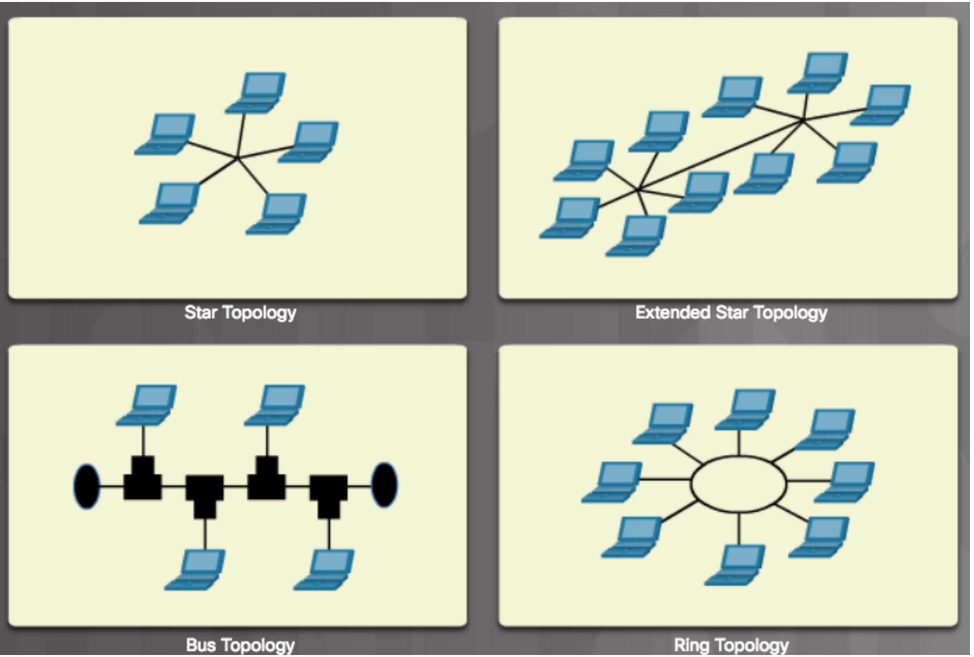
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Logical Point-to-Point Topology (Cont.)



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

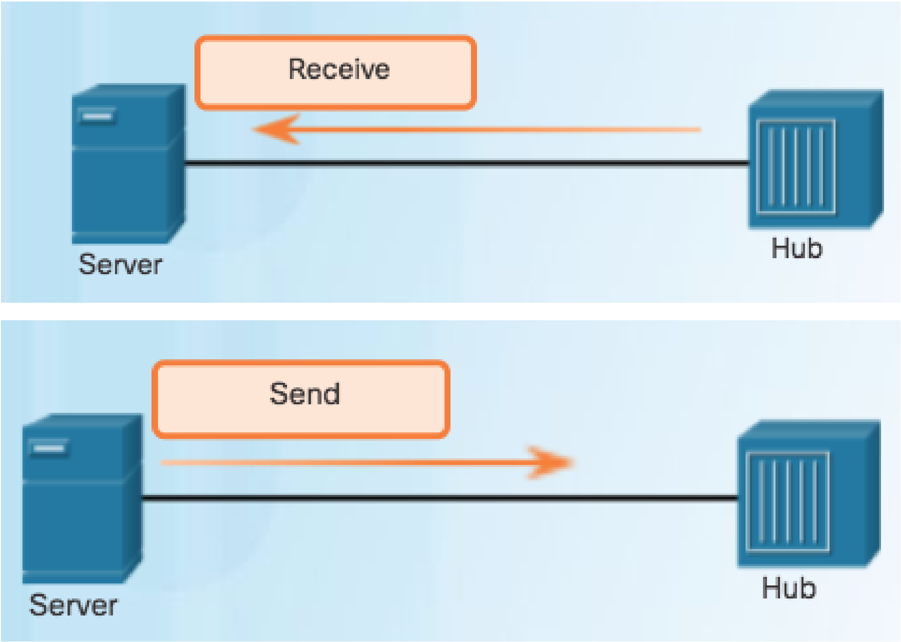
Physical LAN Topologies



- **Star** - End devices are connected to a central intermediate device. Use Ethernet switches.
- **Extended Star** - Additional Ethernet switches interconnect other star topologies.
- **Bus** - Used in legacy networks. All end systems are chained to each other and terminated in some form on each end. Switches are not required to interconnect the end devices. Bus topologies using coax cables were used in legacy Ethernet networks because it was inexpensive and easy to set up.
- **Ring** - End systems are connected to their respective neighbor forming a ring. Unlike the bus topology, the ring does not need to be terminated. Ring topologies were used in legacy Fiber Distributed Data Interface (FDDI) and Token Ring networks.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

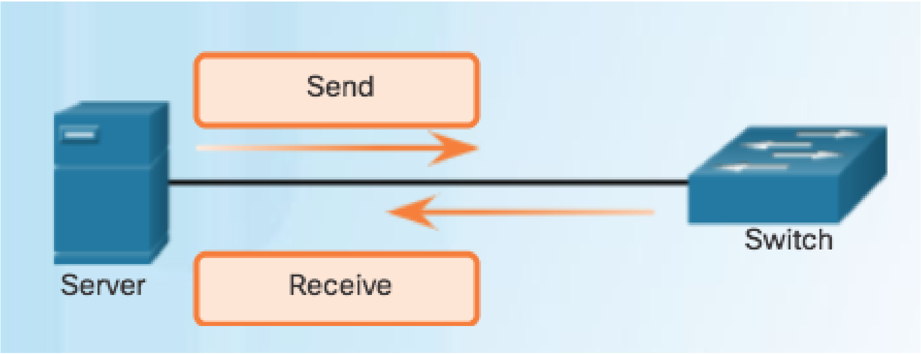
Half and Full Duplex



- **Half-Duplex Communication**
  - Both devices can transmit and receive on the media but cannot do so simultaneously.
  - Used in legacy bus topologies and with Ethernet hubs.
  - WLANs also operate in half-duplex.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

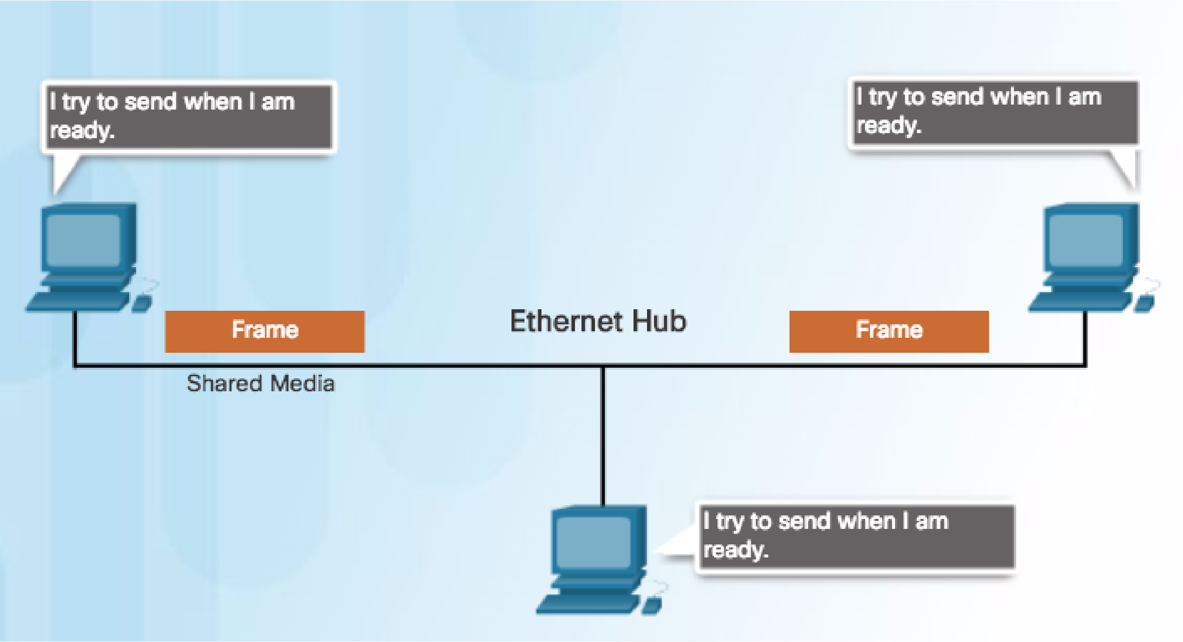
Half and Full Duplex (Cont.)



- **Full-Duplex Communication**
  - Both devices can transmit and receive on the media at the same time.
  - Data link layer assumes that the media is available for transmission for both nodes at any time.
  - Ethernet switches operate in full-duplex mode by default, but can operate in half-duplex if connecting to a device such as an Ethernet hub.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

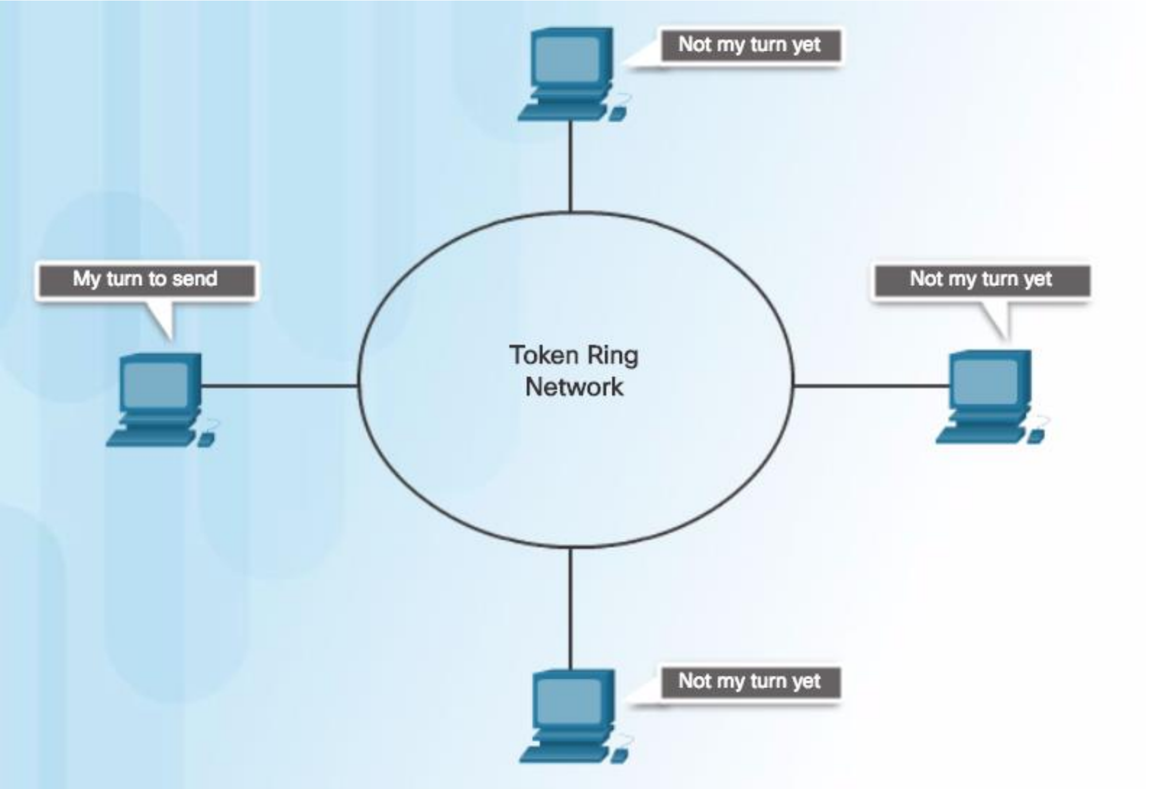
Media Access Control Methods



- Contention-Based Access
  - Nodes operate in half-duplex.
  - Compete for the use of the medium.
  - Only one device can send at a time.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

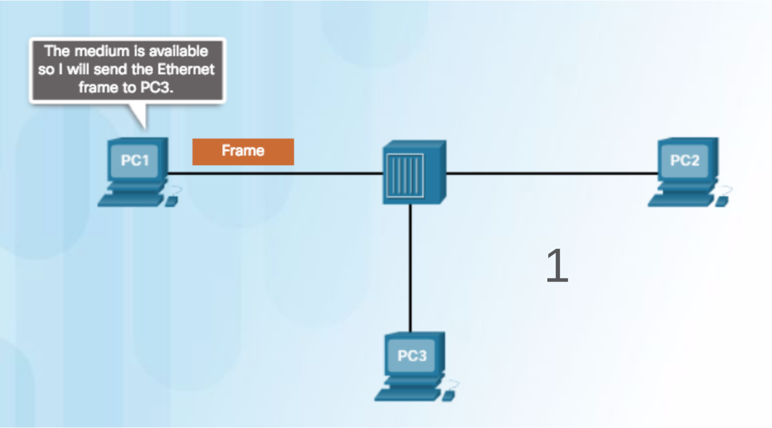
Media Access Control Methods (Cont.)



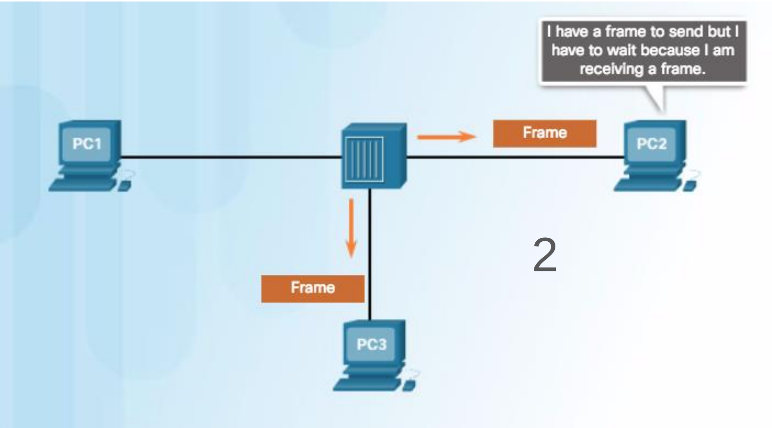
- Controlled Access
  - Each node has its own time to use the medium.
  - Legacy Token Ring LANs are an example

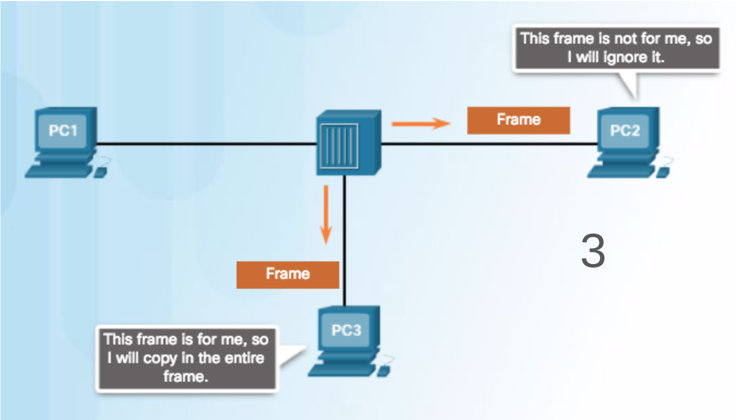
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Contention-based Access - CSMA/CD

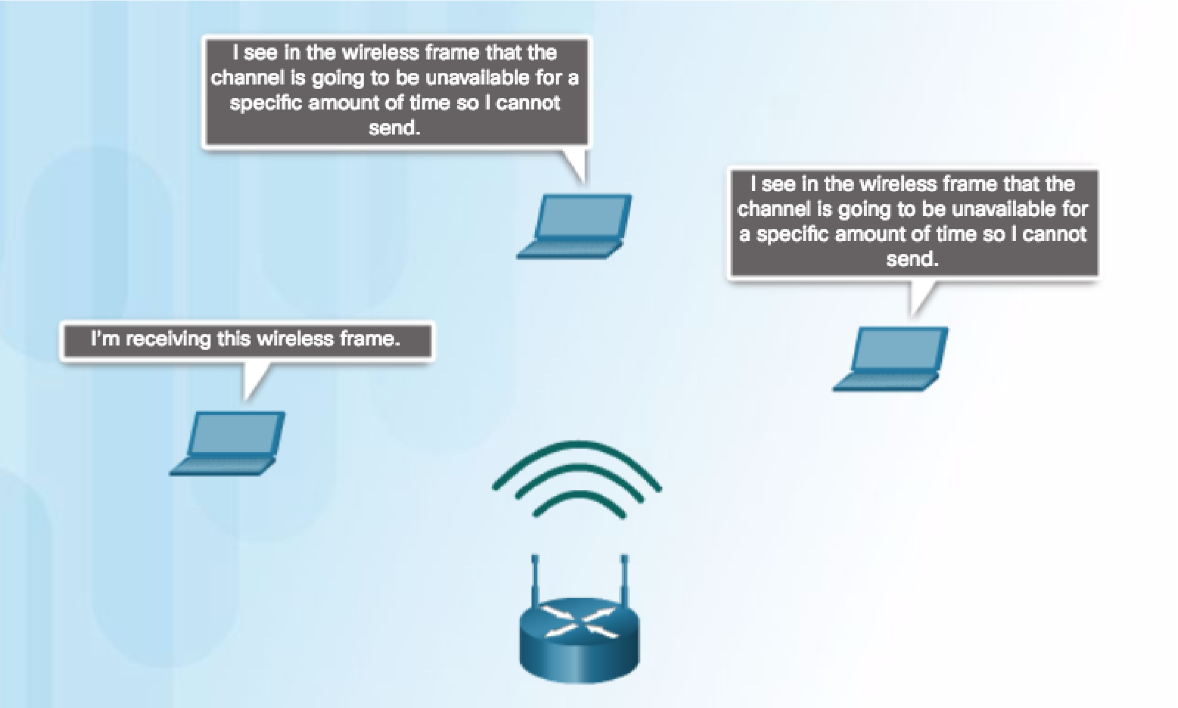


- Carrier Sense Multiple Access/Collision Detection (CSMA/CD) process is used in half-duplex Ethernet LANs.
  - If two devices transmit at the same time, a collision will occur.
  - Both devices will detect the collision on the network.
  - Data sent by both devices will be corrupted and will need to be resent.





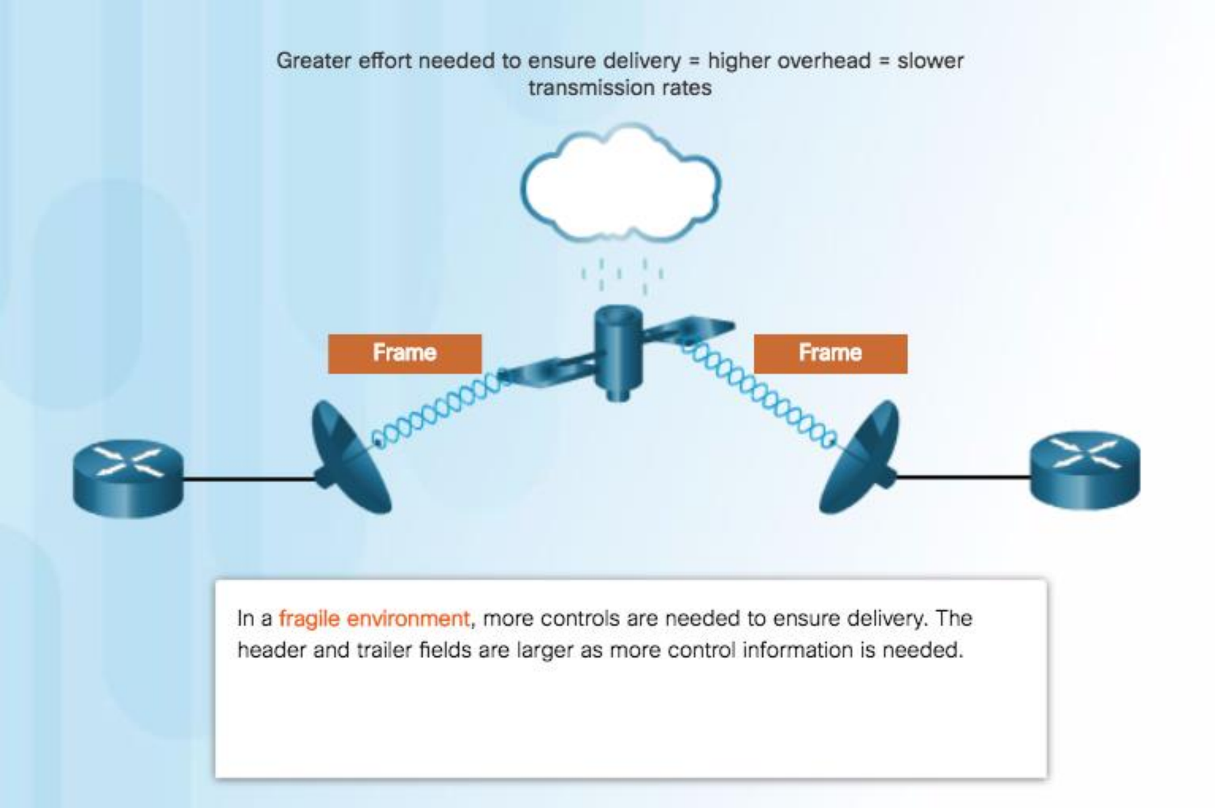
Contention-based Access - CSMA/CA



- **CSMA/CA**
  - Uses a method to detect if the media is clear.
  - Does not detect collisions but attempts to avoid them by waiting before transmitting.
- **Note**: Ethernet LANs using switches do not use a contention-based system because the switch and the host NIC operate in full-duplex mode.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

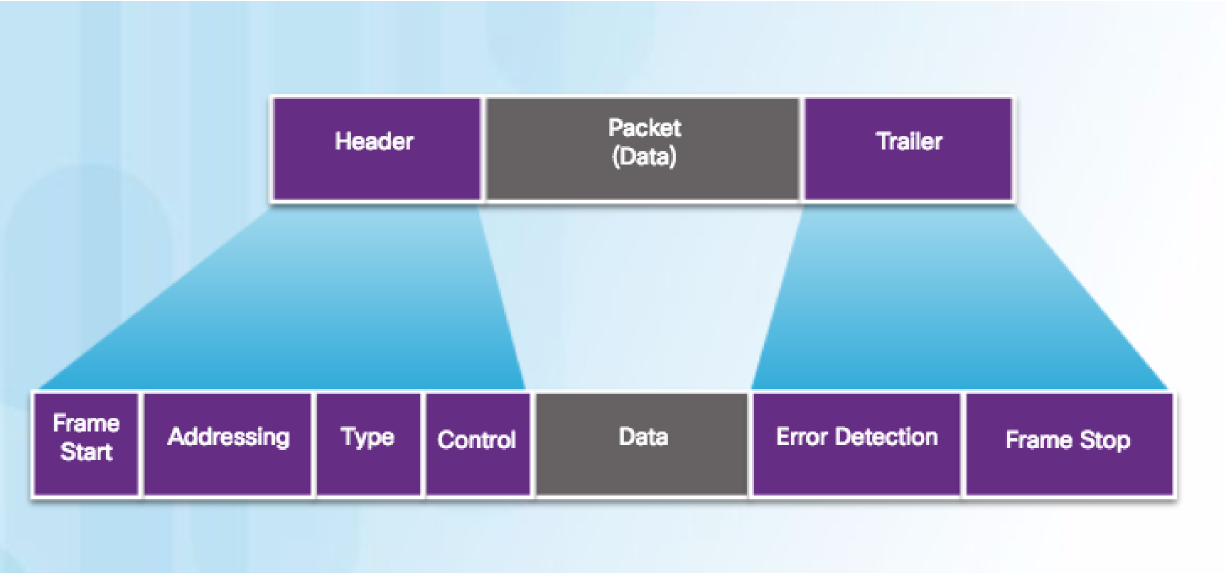
The Frame



- Each frame type has three basic parts:
  - Header
  - Data
  - Trailer
- Structure of the frame and the fields contained in the header and trailer depend on Layer 3 protocol.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

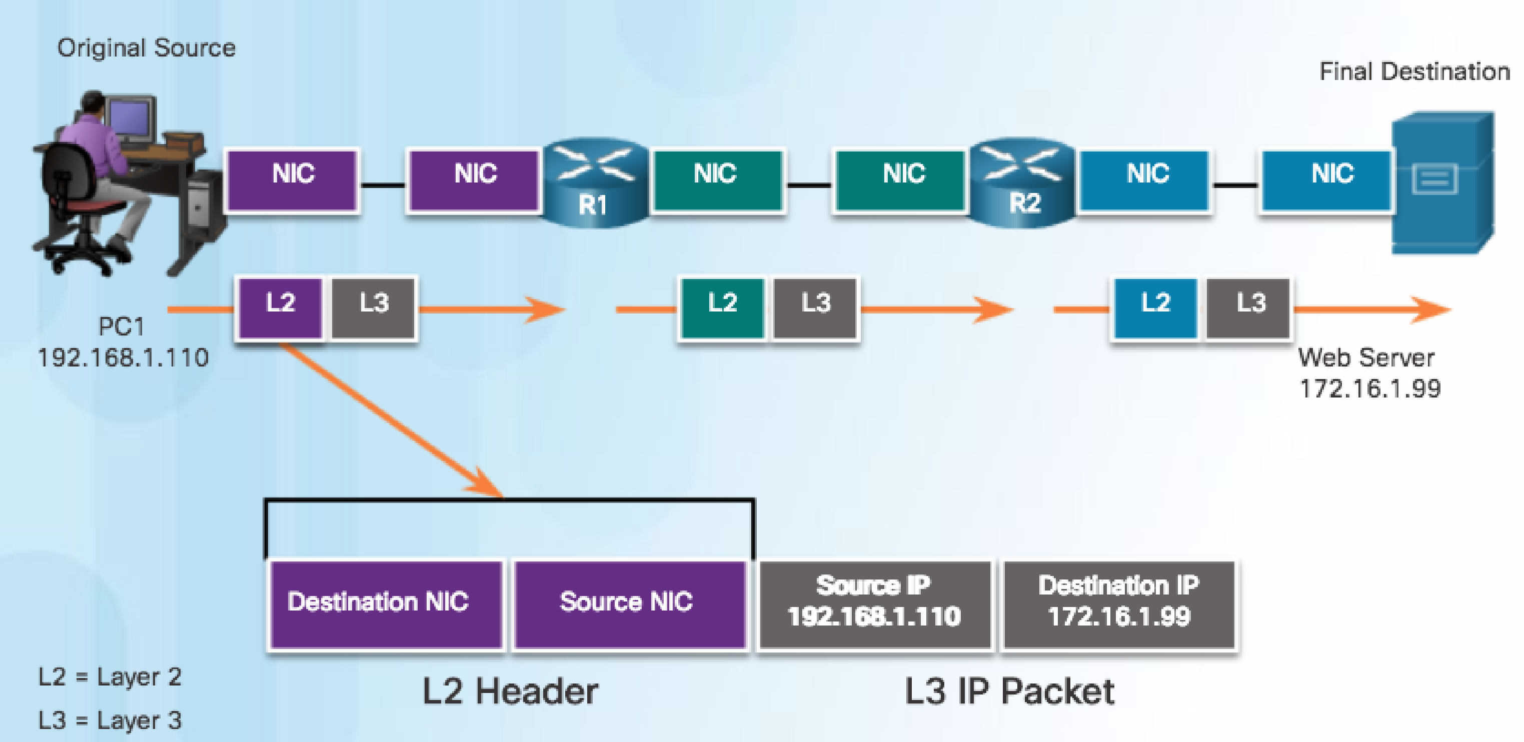
Frame Fields



- **Frame start and stop indicator flags** - Identifies the beginning and end limits of the frame.
- **Addressing** - Indicates the source and destination nodes.
- **Type** - Identifies the Layer 3 protocol in the data field.
- **Control** - Identifies special flow control services such as QoS.
- **Data** - Contains the frame payload (i.e., packet header, segment header, and the data).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

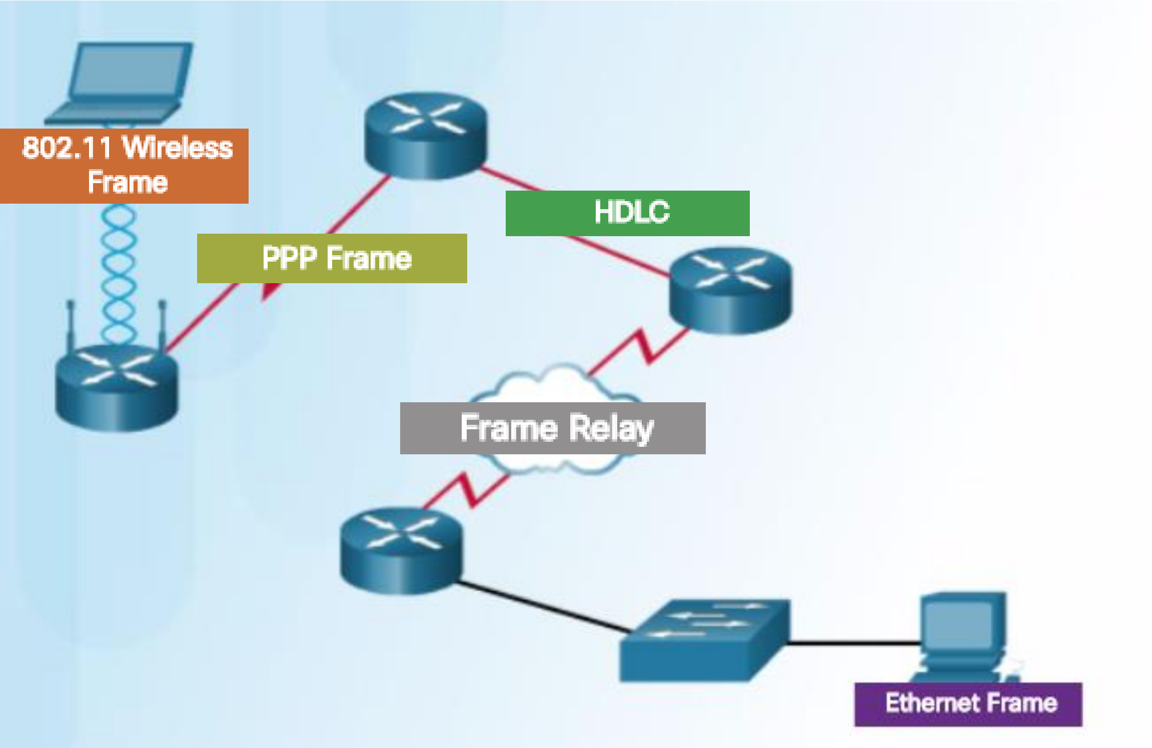
Layer 2 Addresses



Each data link frame contains the source data link address of the NIC card sending the frame, and the destination data link address of the NIC card receiving the frame.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

LAN and WAN Frames



- Layer 2 protocol used for a topology is determined by the technology.
- Data link layer protocols include:
  - Ethernet
  - 802.11 Wireless
  - Point-to-Point Protocol (PPP)
  - HDLC
  - Frame Relay

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.5 Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Conclusion

Chapter 4: Network Access

- Explain how physical layer protocols and services support communications across data networks.
- Build a simple network using the appropriate media.
- Explain the role of the data link layer in supporting communications across data networks.
- Compare media access control techniques and logical topologies used in networks.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential