LESSON 2.1

98-366 Networking Fundamentals

2.1 Understand Switches Part 1

2.2 Understand Switches Part 2

2.3 Understand Routers

2.4 Understand Media Types

MTA Networking Fundamentals 2 Test

LESSON 2.1

98-366 Networking Fundamentals

Understand Switches
Part 1

Lesson Overview

In this lesson, you will learn about:

- Switches
- Transmission speeds
- Data transmission
- Cables
- Uplink speeds
- Managed and unmanaged switches
- VLANs

Switches

- A computer networking device that connects network segments
- Some make it possible to connect different types of networks, including Ethernet, fiber channel, ATM, ITU-T G.hn and 802.11.

- **Layer 2** switches are network bridges that process and route data at the data link layer (layer 2) of the OSI model.
- **Layer 3** switches (multilayer) process data at the network layer of 3 and above.
- **Layer 4** switches allows for policy-based switching and are based on the OSI "transport" layer. These switches limit different types of traffic on specific end-user switch ports.
  - The Layer 4 network switch does not work with unintelligent or passive network devices such as hubs and repeaters.

Open System Interconnection (OSI)

- A way of subdividing a communications system into smaller parts (called layers)
- Layers are defined when services are provided to the layer above it and receive services from the layer below it.
- On each layer an “instance” provides services to the instances at the layer above and requests service from the layer below.
- A repeater is an electronic device that receives a signal and retransmits it to the other side of an obstruction or to a higher level or at a higher power so that the signal can cover greater distances.

Transmission speed

- Data are moved across a communications channel at different rates.
- The rate is referred to as the bandwidth.

LAN Technologies	Bandwidth
Ethernet	10 Mbps/100 Mbps (shared)
Switched Ethernet	10 Mbps/100 Mbps
Gigabit Ethernet	1,000 Mbps
10 Gigabit Ethernet	10,000 Mbps
Token Ring	4, 16 Mbps
Fast Token Ring	100, 128 Mbps
FDDI/CDDI	100 Mbps

Data Transmission

- A standard 10/100 Ethernet switch operates at the data-link layer of the OSI model to create a different collision domain for each switch port.
- Ethernet is a family of frame-based computer networking technologies for local area networks.
- In the Ethernet networking protocol a collision domain is a physical network segment where data packets can "collide" with one another when being sent.

- A network collision is where one particular device sends a packet on a network segment, forcing every other device on that same segment to pay attention to it.
- The hub runs in half duplex sharing bandwidth, resulting in collisions, which would then necessitate retransmissions.
  - A half duplex is a system where only one device can talk to another at one time—they take turns talking.
- Using a switch is called microsegmentation.
  - Allows for dedicated bandwidth with every computer on point-to-point connections
  - Can run in full duplex with no collisions

Cables

- A straight-through cable has identical ends.
- A crossover cable has different ends.
- A PC can be connected to an uplink port with a crossover cable and to a regular port with a straight-through cable.

Uplink Speeds

- Ethernet standards on uplink speeds are of 10Mbps, 100Mbps, 1000 Mbps/1Gbps, 10Gbps since switches come with autosensing in various combinations.
- The access switch members have an uplink module installed.
  - There are two ports on each uplink module.
- The uplinks are configured to act as trunk ports by connecting the access switch with the distribution switch.

Managed and Unmanaged Switches

- An unmanaged switch is also called “dumb”—it allows all traffic to go through the network and the administrator has no control.
- The system administrator can take control of the network with a managed switch and allow ports to talk to other ports or none at all.
- The switch's benefits over a hub include full bandwidth to each port and methods to deal with collisions.
- The ports are allowed to talk to the print server or the personal computers.

98-366 Networking Fundamentals

- A managed switch has its own IP address, and has a telnet and maybe a web-based interface to monitor and secure access to each port on the switch.
- A managed switch can also be used to enable or disable specific ports without unplugging a cable.
- A managed switch can have virtual LANS (VLANs), which separate ports on a switch into different switches.
- A managed switch can tell you about excessive usage on certain ports.
- A managed switch can be used to limit the number of IP addresses that one port can service.

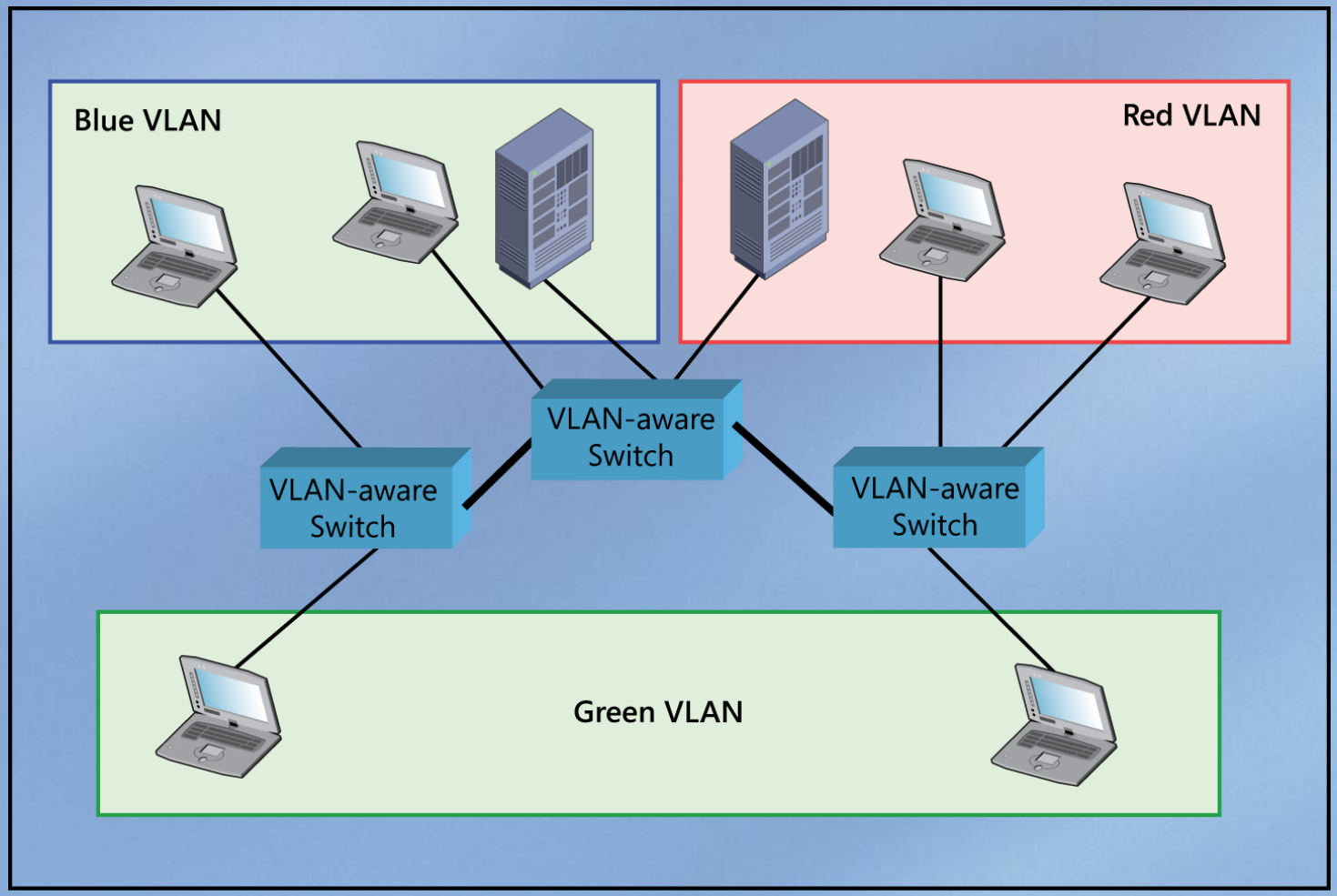
Virtual LAN (VLAN)

- Allows a separate logical network connectivity from a physical connectivity
- Not limited by its physical connectivity
- All users belong to a single broadcast domain and can communicate with each other at the data link layer or “layer 2.”
- Can be used to segment a complex network into smaller units for better manageability, improved performance, and security

Virtual LAN (VLAN)

- The ability to move is much simpler because of the dynamic nature of VLANs—no physical changes to network topology are necessary.
- Security domains can be constructed to provide various levels of security in the network.

Virtual LAN using VLANs to create broadcast domains across switches



Hubs vs. Switches

- A hub is like an ordinary junction box and just passes along what it receives to all the other ports (connections) on the hub.
- A switch is more intelligent and is selective about where it passes data.
  - It learns where certain equipment is located and passes along the data only to the ports that need to receive it, allowing multiple interactions at once.

Complete Student Activity 2.1

LESSON 2.2

98-366 Networking Fundamentals

Understand Switches
Part 2

Lesson Overview

In this lesson, you will learn about:

- Switches
- Backplane speed
- Hardware redundancy
- Layer 2 and layer 3 switches
- MAC table
- Security options
- Switching types
- Support
- Capabilities of hubs vs. switches

Switches

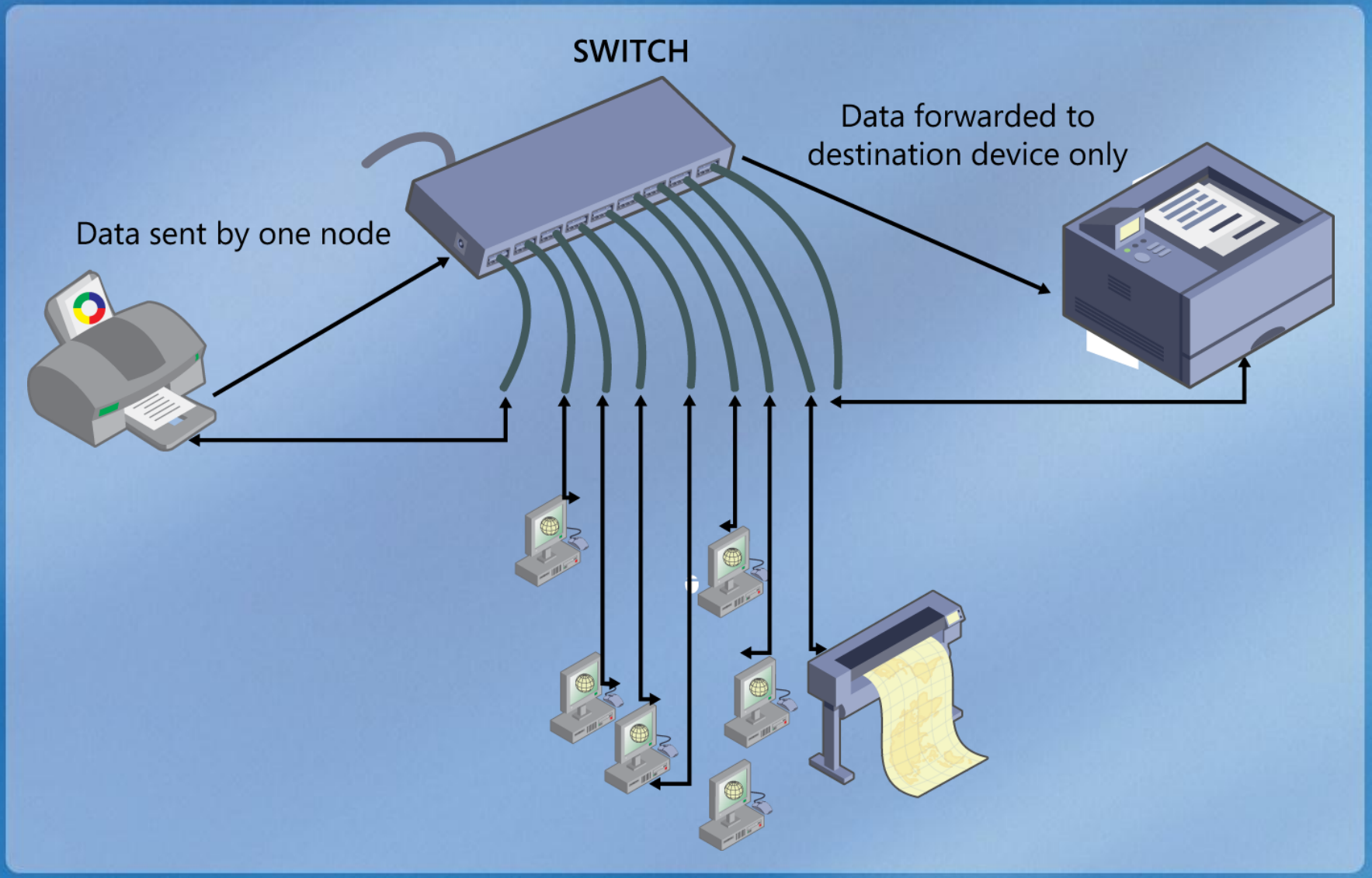
- A switch is a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model.
- Large switches have higher layer issues, router issues, backplanes, security and redundancy.
- Built-in or modular interfaces in large switches make it possible to connect different types of networks, including Ethernet, Fiber Channel, ATM, ITU-T G.hn and 802.11.

Layer 2 Switch

- Provides the same functionality as bridges
- Learns and forwards frames on each port just like a multiport bridge
- Multiple switching paths inside the switch can be active at the same time.
- Operates utilizing MAC addresses in its caching table to quickly pass information from port to port.

LESSON 2.2

98-366 Networking Fundamentals



Layer 3 Switch

- Utilizes IP addresses to perform the functions as layer 2 switches
- Are fast routers that do layer 3 forwarding in hardware
- Because IP is the most common among all layer 3 protocols today, most of the layer 3 switches perform IP switching at the hardware level and forward the other protocols at layer 2 (bridge them).

Bridging

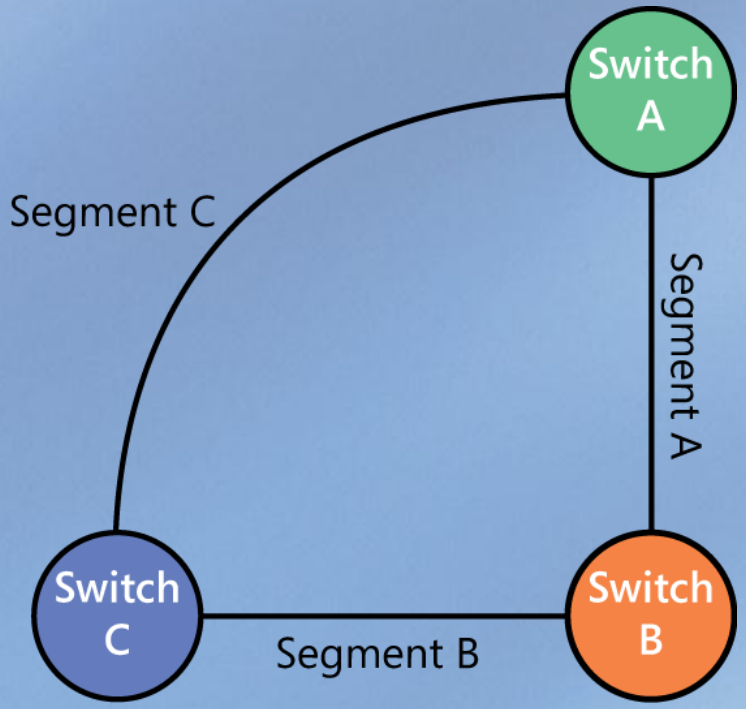
- Involves segmentation of local-area networks (LANs) at the Layer 2 level
- A multiport bridge learns about the media access control (MAC) addresses on each of its ports and transparently passes MAC frames destined to those ports.
- Ensures that frames destined for MAC addresses that lie on the same port as the originating station are not forwarded to the other ports

Switch Security

- Define virtual local area networks
- Two basic steps:
  1. Defining what users can see
  2. Defining where they can connect
- What you see—Security allows organizations to separate sensitive clusters of systems from the rest of the network.
- What you connect—Port security is available on business-class switches and some allow in-depth settings.

Hardware Redundancy

- Occurs when segment C is added to the network connecting switches A and C
- If one of the switches fails, the network will eliminate the point of failure.



Managed Switches

- Provide support for the network through:
  - Flexibility
  - Security
  - Reliability
  - Expandability
- Switches are supported by their manufacturer and with online manuals.

Three Types of Switching

- Circuit
- Packet
- Cell Relay

Circuit switching

- Used in voice networks
- Not an efficient method for routing any kind of data
- Is wasted because no transmission is using the bandwidth of the circuit 100 percent of the time
- In circuit failure during a transmission, the entire connection must be re-established, which means the conversation must start over again.

Packet Switching

- Used in data networks
- Has no dedicated circuits
- Each circuit carries many transmissions at the same time.
- Has the ability to route data units over any route
- More reliable because if a particular circuit in the network should fail, the routers in the network route data units over different circuits.
- The protocols have the ability to reassemble the data units into their proper order.

Cell Switching

- Voice
- Data transmission
- The cell is the data unit.
- Voice requires small data units.
  - In order to support voice, the data units must be small so that they can be processed quickly and sent through the network with minimal delay.
  - Whenever there is information to be transmitted, the switch simply sends the data units.
- Data favors large data units.

Complete Student Activity 2.2

LESSON 2.3

98-366 Networking Fundamentals

Understand Routers

Lesson Overview

In this lesson, you will learn about:

- Directly connected static routes
- Dynamic routes (routing protocols)
- Default routes, NAT, RRAS
- Routing tables
- Routing protocol
- Routing in Windows Server
- Transmission speed considerations

Routers

- A device that selectively interchanges packets of data in two or more computer networks while connecting the networks
- Connected to at least two networks, generally two LANs or WANs or a LAN and its ISP's network
- Wireless routers provide everything that a wired router provides, including ports for Ethernet connections and the attributes for wireless security such as Wi-Fi Protected Access (WPA) and wireless MAC address filtering.
- Many wireless routers can be configured for "invisible mode" so that your wireless network cannot be scanned by outside wireless clients.

LESSON 2.3

98-366 Networking Fundamentals

- Data can be transmitted through the router from place to place at a measured kilobits transmission speed called the bandwidth .
- Each interface on a router will impact overall performance, especially WAN connections.
- Data rate and data speed are the same in terms of transmission speed.
- Compared to data transmission, bandwidth or "capacity" means how wide the pipe is and how quickly the bits can be sent.
- These "speeds" are aggregate speeds. The data on the multiple signal channels are assigned by channel for different uses.
- Data transmission speed (or bandwidth) is measured in kilobits, 1,000s of bits per second, or megabits, Mbps, millions of bits per second.
- Because of software and protocols, actual transfers are considerably lower.

Routing

- A routing protocol is applied when passing data from one subnet (interface) to another subnet.
- When determining which route is preferable, directly connected networks have the highest priority, followed by static routes, and then other routes.
- If a corresponding interface command is contained under the router configuration stanza of that protocol, it is are advertised by IGP routing protocols, which are directly connected networks.
- IGP—Interior gateway protocol describes the fact that each system on the Internet can choose its own routing protocol.

Static Routing

- The process of manually entering routes into the routing table through a configuration file that is loaded when the routing device starts up
- Static routes are manually configured and cached when a router starts up and don’t change unless a user changes them.
- Static routing does not handle down connections well because they must be reconfigured manually to repair any lost connectivity.
- Does not work well when the routing information has to be changed or needs to be configured on a large number of routing devices.

Dynamic Routing Protocols

- Software applications that dynamically discover network destinations and how to get to them
- Have the ability to adapt to logical network topology changes, equipment failures, or network outages.
  1. A router will “learn” routes to all directly connected networks first.
  2. Secondly it will learn routes from other routers that run the same routing protocol.
  3. Next the router sorts through its list of routes and selects one or more “best” routes for each network destination it knows or has learned.
  4. Finally, dynamic protocols will distribute this “best route” information to other routers running the same routing protocol.

Routing Table

- Routing Information Base (RIB) is an electronic table *(file)* or that is stored in a networked computer or a router.
- The routes to network destinations are stored in the routing table.
- The function of the routing protocols and static routes is to create the routing tables.
- The most specific route to the destination IP address is the longest matching route.
- The router uses the lowest metric to select the best route when multiples occur.
- The router is free to choose which table entry to use if multiple entries exist that are the longest match and the lowest metric.

LESSON 2.3

98-366 Networking Fundamentals

- TCP/IP network routers use the routing table to calculate the destinations of messages it is responsible for forwarding.
- A computer must have an IP address to communicate with other computers and servers on the Internet.
- An IP address (Internet protocol) is a unique 32-bit number that identifies the location of your computer on a network.
- With the growth of the Internet and increased use, the number of available IP addresses is not enough—redesign for the address format to allow for more possible addresses is being developed (IPv6) and it will require modification of the entire infrastructure of the Internet.

- The network address translation (NAT) is the process of modifying network address information while in transit across a traffic routing device.

Routing and Remote Access in Windows Server

- Routing and remote access service (RRAS) in Windows Server supports remote user or site-to-site connectivity.
- RRAS is an open platform for routing and networking.
- By using secure VPN connections, routing services are provided to businesses in LAN and WAN environments or over the Internet.
- Routing is used for multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services.
- By using RRAS, VPN connections can be deployed to provide end users with remote access to your organization's network.
- A site-to-site VPN connection between two servers at different locations can also be created.

Complete Student Activity 2.3

LESSON 2.4

98-366 Networking Fundamentals

Understand Media Types

Lesson Overview

In this lesson, you will learn information about:

- Network media types
- Cable types and their characteristics
- Fiber optics
- Susceptibility to external interference
- Susceptibility to electricity
- Susceptibility to interception

Network Media types

- Media is the actual physical environment through which data travels as it moves from one component to another and connects network devices.
- Two categories of Media are wired network and wireless network.
- To determine what transmission media is right for particular networking environment you need to consider:
    - Required throughput
    - Cabling distance
    - Noise resistance
    - Security
    - Flexibility
    - Plans for growth

Common Network Cable Media

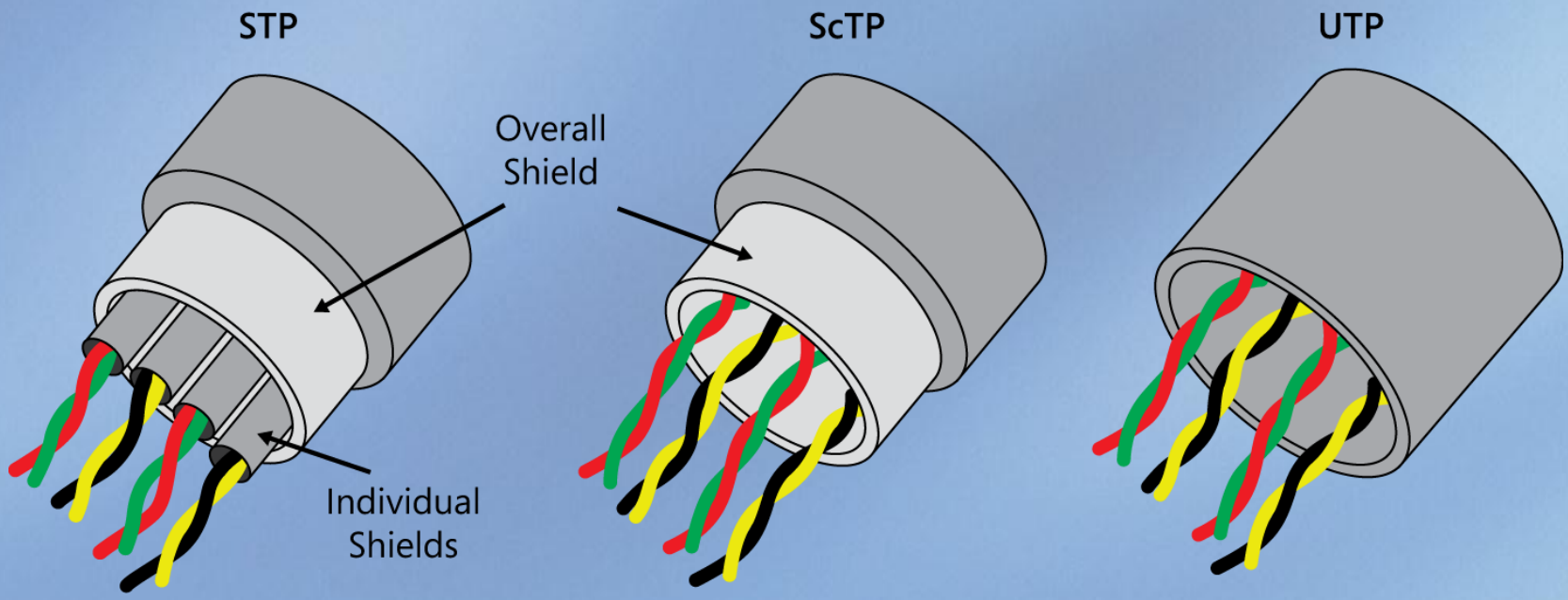
- Twisted-pair cable (shielded, unshielded, stranded copper, solid core copper)
- Coaxial cable and RFI
- Fiber-optic cable
- Wireless

Twisted pair cables

- Available unshielded (UTP) or shielded (STP)
- STP is used in noisy environments where the shield is around each of the wire pairs, plus an overall shield protects against excessive electromagnetic interference.
- A variation of STP, known as ScTP for "screened twisted pair" or FTP for "foil twisted pair," uses only the overall shield and provides more protection than UTP, but not as much as STP.
- Both UTP and STP come in **Stranded and Solid** wire.
  - The stranded copper wire is very flexible.
  - Solid wire cable has less attenuation and can span longer distances.

LESSON 2.4

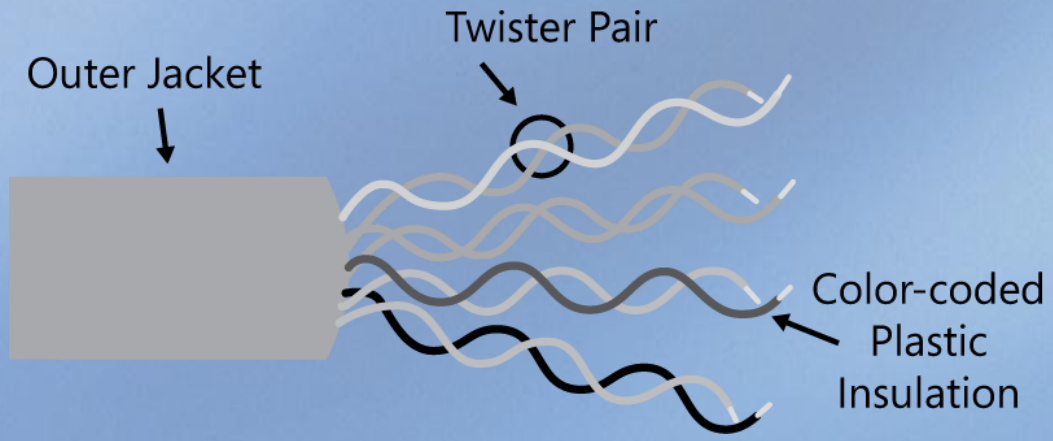
98-366 Networking Fundamentals



Shielded and Unshielded Twisted Pairs

Unshielded twisted pair cable (UTP)

- 8 individual copper wires covered by an insulating material
- Used for many different networks.



- The copper wire is color-coded plastic insulation and they are twisted in pairs. It is all covered with an outer jacket.

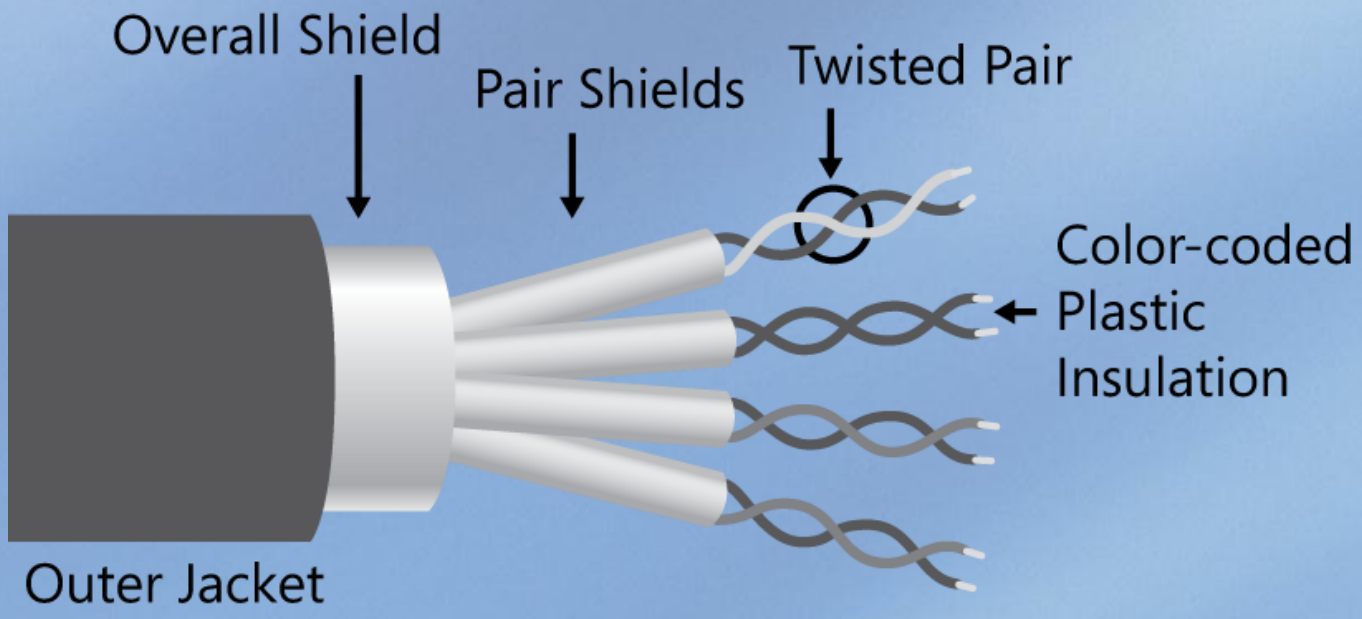
- UTP is the most common form of twisted pair wiring.
- It is less expensive and easier to work with than STP.
- It is used in Ethernet 10Base-T and 100Base-T networks, as well as in home and office telephone wiring.
- Two insulated copper wires are twisted around each other to decrease crosstalk or electromagnetic induction between pairs of wires.
- Every signal on a twisted pair involves both the wires.
- Twisted pair is installed in two or more pairs, all within a single cable, to offer multiple connections to computers.
- UTP cable is typically installed using a registered jack 45 (RJ-45) connector.
- The RJ-45 is an eight-wire connector used commonly to connect computers onto a local area network (LAN), especially Ethernets.

Types of UTP Cabling

- Category 1—Used for telephone communications
- Category 2—Data speed at 4 Mbps per second
- Category 3—Speeds of 10 Mbps, used for 10BASE-T
- Category 4—For Token Ring – transmit data at 16 Mbps
- Category 5—Can transmit data at speeds up to 100 Mbps
- Category 5e —Used in networks running at speeds up to 1000 Mbps (1 gigabit per second [Gbps])
- Category 6—Consists of four pairs of 24 American wire gauge (AWG) copper wires and fastest standard for UTP

Shielded twisted-pair (STP)

- Used in Ethernet networking and has shielding, cancellation, and wire twisting with each pair of wires wrapped in a metallic foil
- The four pairs of wires are wrapped in an overall metallic braid or foil, generally 150-ohm cable.



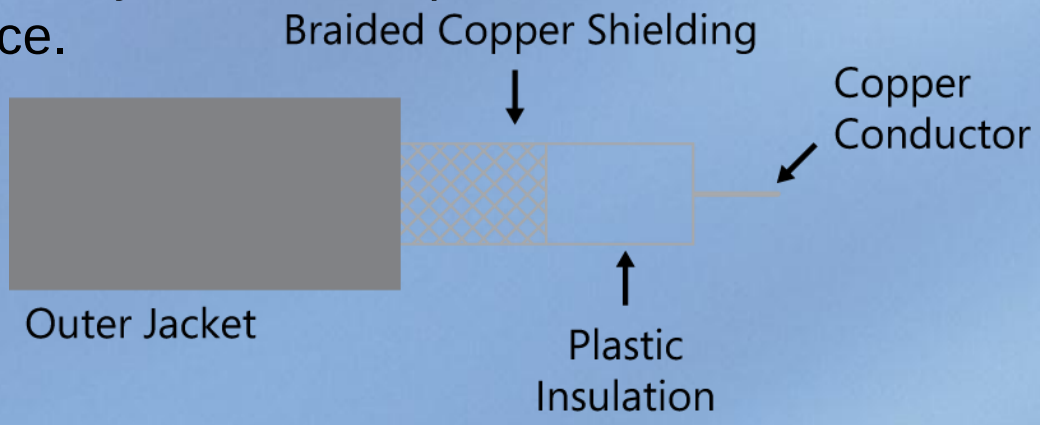
- Because of its cost and difficulty with termination, STP is rarely used in Ethernet networks.
- STP is primarily used in Europe.
- Because most buildings are already wired with UTP, many transmission standards are adapted to use it, to avoid costly rewiring with an alternative cable type.
- UTP and STP are not used together.

Coaxial cables

- Were the first cables used in Ethernet networks.
- Consists of an insulator that separates the braided inner conductor and the outer conductor, which is a woven copper braid
- Commonly used for cable TV connections and10 Base5 and 10 Base2 Ethernet networks.
- **Coaxial Thinnet** supports a maximum segment length of 185 meters, is less costly and easier to install
- **Coaxial Thicknet** can send signals up to 500 meters, is costlier and demands more efforts in installation
- The transmission speed these cables provide is between 2.5 Mbps and 10 Mbps.
- Coaxial cables are more resistant to EMI than the UTP cable, because of greater insulation to external interference.

Coaxial cable

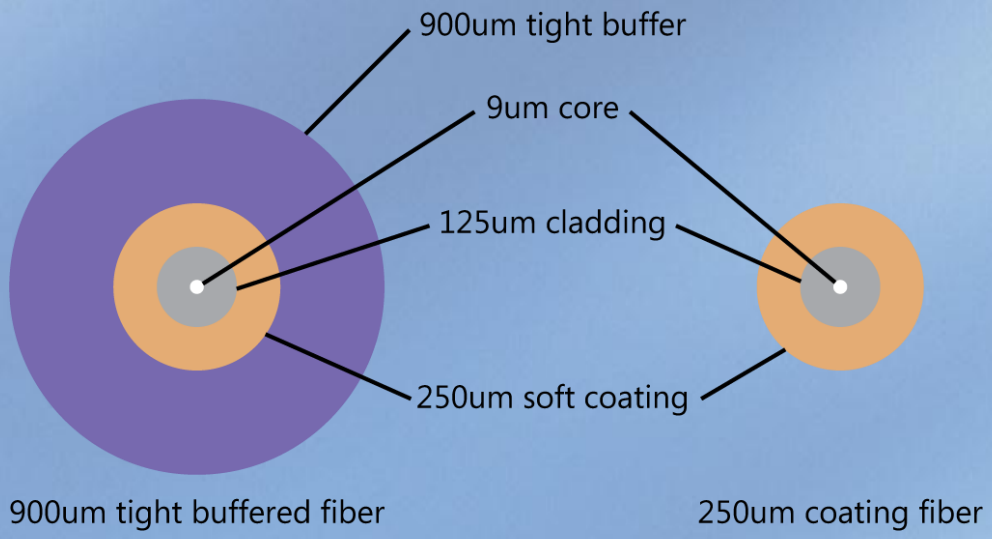
- Made of a hollow outer cylindrical conductor surrounding a single inner wire made of two conducting elements
- One element in the center of the cable is a copper conductor.
- A layer of flexible insulation surrounds the copper conductor.
- Over the insulation is a metallic foil or woven copper braid acting as both the second wire in the circuit and a shield for the inner conductor .
- This second layer/shield helps reduce the amount of outside interference.



Fiber Optics

- Cables are made up of glass or other light transmitting material.
- Transmit data in the form of light
- A reflective coating that allows light beams to travel without outer interference covers the glass cable.
- The advantages:
  - Faster
  - Very long distances without the risk of outer interference
- At one end of the fiber optics system is a transmitter that accepts coded electronic pulse data coming from copper wire.
- The information is processed and translated into equivalently coded light pulses.
- A light-emitting diode (LED) or an injection-laser diode (ILD) can be used for generating the light pulses.

- Fiber optic cable construction has these elements: core, cladding, coating, strengthening fibers, and a cable jacket.
- The center is glass fiber, the second ring is a fiber coating, and third ring is a thermoplastic over coating or buffer, the fourth ring is an Aramid strength member and the last ring has a PVC jacket or a fluoride co-polymer jacket.



Note: Coated fiber is also called "bare fiber"

The Difference Between Tight Buffered Fiber and Coated Fiber

- Single mode fiber (SMF) optic cable and multi-mode fiber (MMF):
  - SMF supports high-speed LAN covering long distances (3000+ meters) and WAN spread over different buildings or cities.
  - Uses a Laser light source.
  - Used in 10GBase-LR Ethernet specification, which runs at the speed of 10 Gbps and allows only one mode of light to transmit.
- The multi-mode fiber (MMF) optic cable :
  - Used for high-speed networks spread over short distances (less than 2000 meters).
  - Uses a LED light source.
  - Used for 10GBase-SR Ethernet standard that supports the transmission speed of 10 Gbps, it allows the light signals to travel in more than one path
  - Less costly than the SMF cable

Wireless communication

- The transfer of information over a distance without the use of physical media
- The distances involved may be short (a few meters as in television remote control) or long (thousands or millions of kilometers for radio communications)
- Wireless communication is considered to be a branch of telecommunications

Wireless communication

- Uses radio frequencies (RF) or infrared (IR) waves to transmit data between devices on a LAN
- Wireless signals are electromagnetic waves that can travel through the vacuum of outer space and through a medium such as air.
- A key module is the wireless hub for distributing signals through the wireless LAN.
- A computer can have a wireless adapter card (wireless NIC) installed to receive the signals from the access point.

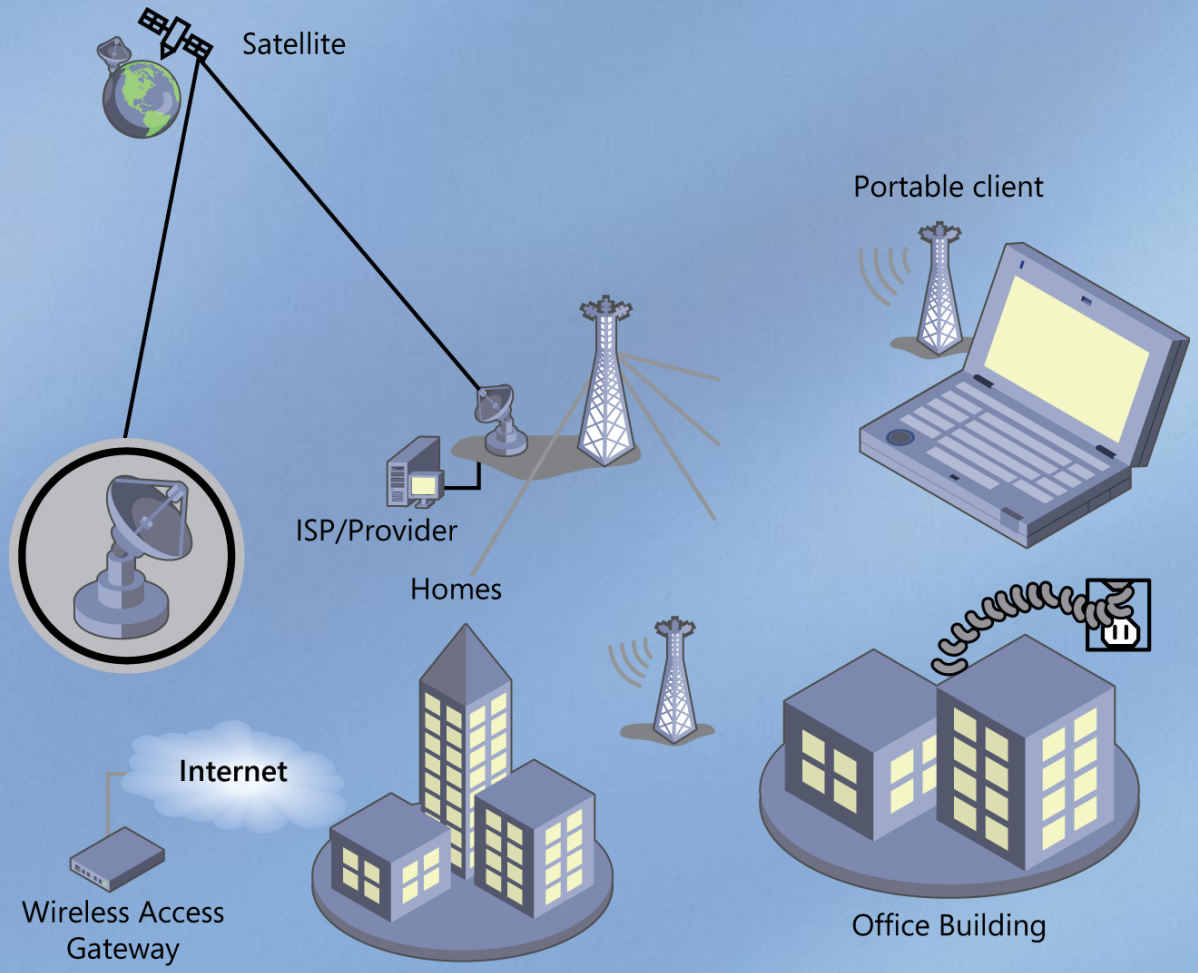
Applications of wireless data communication

- Accessing the Internet using a cellular phone
- Establishing Internet connection over satellite
- Beaming data between two handheld computing devices
- Wireless keyboard and mouse for the PC
- Wireless LAN (WLAN) use radio waves (902 MHz)
- Microwaves (2.4 GHz)
- IR waves (820 nanometers [nm]) for communication

LESSON 2.4

98-366 Networking Fundamentals

Wireless Distribution



External Interference

- Interference in telecommunication and electronics refers to anything that alters, modifies, or disrupts a message as it travels along a channel between a source and a receiver.
- External susceptibility comes from machinery and power cables.
- Tightly strapped cabling often causes interference from motors and solenoids jumping over to the signal cabling and disturbing sensors.
    - Jumping occurs when the high current can cause the rapid release of large volumes of hydrogen, which can be ignited by a nearby spark.
- See examples of external interference from equipment and cables at www.qedata.se/e_emi_bakgrund.htm.

Electromagnetic interference (EMI)

- Undesirable electromagnetic emission or any electrical or electronic disturbance.
- EMI can be man-made or natural and interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment.
- The source may be any object, artificial or natural, that carries rapidly changing electrical currents, such as an electrical circuit, the Sun or the Northern Lights.

- Twisted pair's susceptibility to electromagnetic interference greatly depends on the pair twisting schemes staying intact during the installation.
- As a result, twisted pair cables usually have stringent requirements for maximum pulling tension as well as minimum bend radius.
- The fragility of twisted pair cables makes installation practices an important part of ensuring the cable's performance.

Interception

- Data communication equipment emits modulated signals that carry information that an eavesdropper or hacker can intercept.
  - It is completely undetectable, requires little apparatus, and can be done at a considerable distance.
- Like fiber optics but without the fiber, LED indicators act as little free-space optical data transmitters.

LESSON 2.4

98-366 Networking Fundamentals

Media Type Comparison

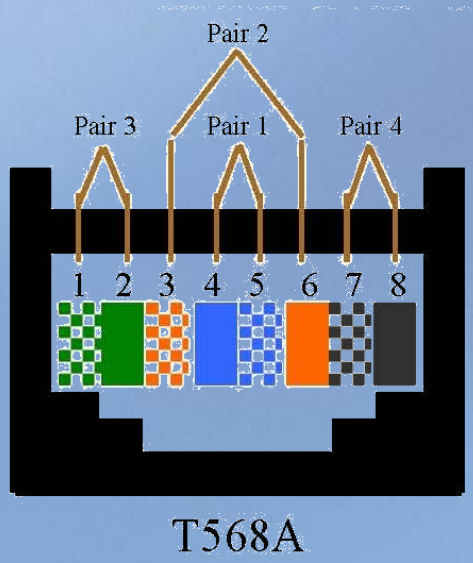
Media Type	Maximum Segment Length	Speed	Cost	Advantages	Disadvantages
UTP	100 m	10 Mbps to 1000 Mbps	Least expensive	widely available and widely used and easy to install	Susceptible to interference; can cover only a limited distance
STP	100 m	10 Mbps to 100 Mbps	More expensive than UTP	more resistant to EMI than Thinnet or UTP; Reduced crosstalk;	Difficult to work with; can cover only a limited distance
Coaxial	500 m (Thicknet) 185 m (Thinnet)	10 Mbps to 100 Mbps	Relatively inexpensive, but more costly than UTP	Less susceptible to EMI interference than other types of copper media	Difficult to work with (Thicknet); limited bandwidth; limited application (Thinnet);
Fiber-Optic	10 km and farther (single-mode) 2 km and farther (multimode)	100 Mbps to 100 Gbps (single mode) 100 Mbps to 9.92 Gbps (multimode)	Expensive	security is better; can be used over great distances; has a higher data rate than coaxial & twisted-pair cable	Difficult to terminate

Network Cabling Standards

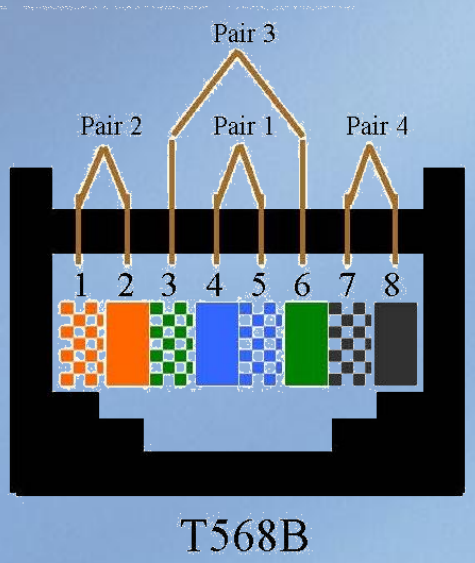
- The Electronic Industries Alliance (EIA) developed standards in 1991 for the cabling used in telecommunications applications.
- In 1995 it was updated by the EIA and later replaced with the current TIA/EIA 568-B standard.

T568A and T568B

- Based on TIA/EIA-568-B.1-2001, the wiring schemes define the pin out, or order of connections, for wires in eight-pin modular connector plugs and jacks.



T568A



T568B

- The wiring assignments in the RJ-45 plug are important. A colored wire must be placed in a specific pin location in the plug in order for the cable to meet the standard.
- It is these wiring assignments that differ between the T568A and T568B standard.
- The only difference between T568A and T568B is that pairs 2 and 3 (orange and green) are swapped.
- Both configurations wire the pins "straight through," i.e., pins 1 through 8 on one end are connected to pins 1 through 8 on the other end.
- The same sets of pins are paired in both configurations: pins 1 and 2 form a pair, as do 3 and 6, 4 and 5, and 7 and 8.

Cable Termination

- Cables that are terminated with differing standards on each end will not function normally.
- Standard RJ-45 pinouts describe the arrangement of the individual wires required when connecting connectors to a cable.
- RJ-45 is the standard connector for 10Base-T/100Base-TX Ethernet, ISDN, T1, and modern digital telephone systems.

Deciding to use T568 A or T568 B

1. If the installation is residential, choose T568B unless other conditions apply.
2. If there is preexisting voice/data wiring (remodel, moves, adds, changes), duplicate this wiring scheme on any new connection.
3. If project specifications are available, use the specified wiring configuration.
4. If components used within the project are internally wired either T568A or T568B, duplicate this wiring scheme.

Complete Student Activity 2.4

Microsoft

Complete Quia Test:

MTA NetFund2 Test