Mod 3 – Networking Media

CCNA 1 version 3.0

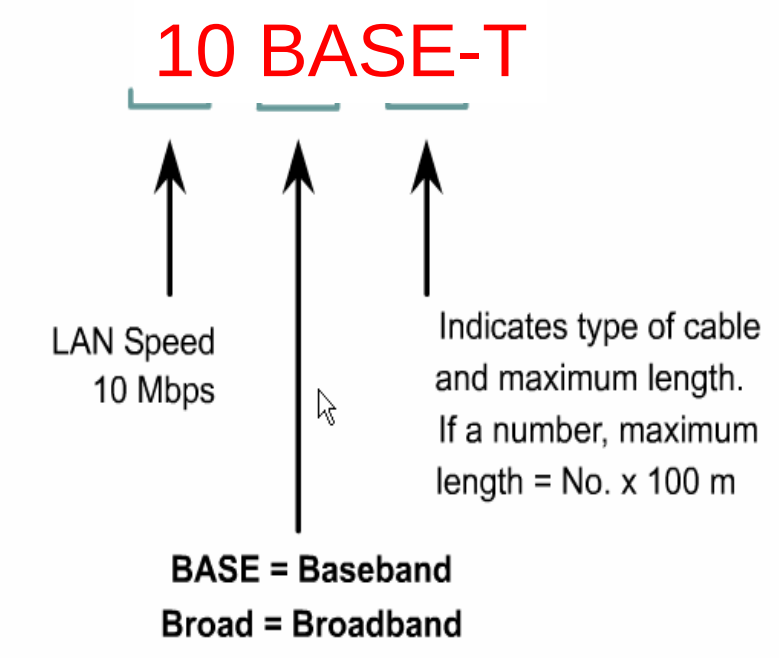
Copper Media - Objectives

- Describe the specifications and performances of different types of cable.
- Describe coaxial cable and its advantages and disadvantages over other types of cable.
- Describe shielded twisted-pair (STP) cable and its uses.
- Describe unshielded twisted-pair cable (UTP) and its uses.
- Discuss the characteristics of straight-through, crossover, and rollover cables and where each is used.

Cable Specifications in LAN Technology Specifiers

Cables have different specifications:

- Bandwidth limitations on transmitted signals:
  - depends on cable type
  - digital signals needs more bandwidth (in Hertz) than analog signals
- Attenuation:
  - causes signal become degraded in amplitude
  - depends on cable type
  - increases with cable length and frequency
  - Signal Degradation is directly related to the distance the signal travels and the type of cable used.
  - The recipient device might not be able to accurately receive and interpret the degraded signal when the signal reaches that device?



Examples:
10 BASE 2: 200 m maximum
10 BASE 5: 500 m maximum

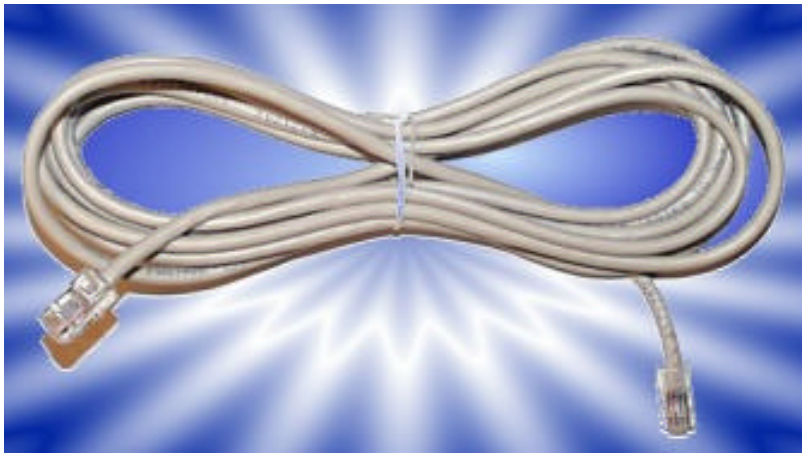
Cable Specifications

Cables have different specifications and expectations pertaining to performance:

- What speeds for data transmission can be achieved using a particular type of cable?
  - The **speed of bit transmission through the cable** is affected by the kind of cable and the transmission technology used.
- How far can a signal travel through a particular type of cable before attenuation of that signal becomes a concern?
  - The attenuation of a transmitted signal depends on
    - the type of cable used (Coax, twisted pair, optical fiber),
    - the signals frequency content (frequency spectrum): the higher the frequencies, the higher the attentuation
    - the len

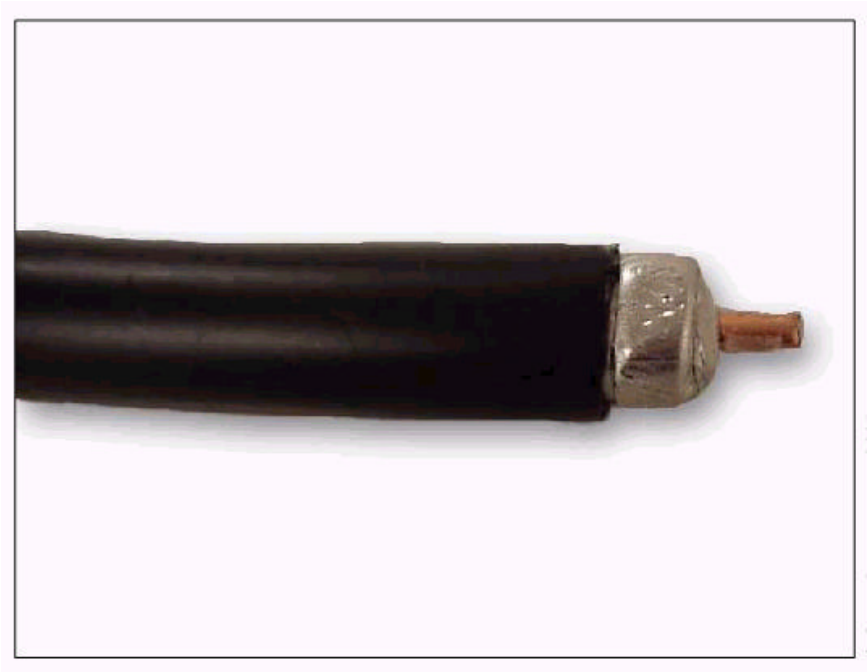
The distance the signal travels through the cable directly affects attenuation of the signal.

Cable used for Ethernet 10 Base-T LAN Standard



- **10BASE-T**
  - speed of transmission is 10 Mbps
  - type of transmission is BASEband, or digitally interpreted
  - T stands for Twisted pair

Cable used for Ethernet 10 Base5 LAN Standard

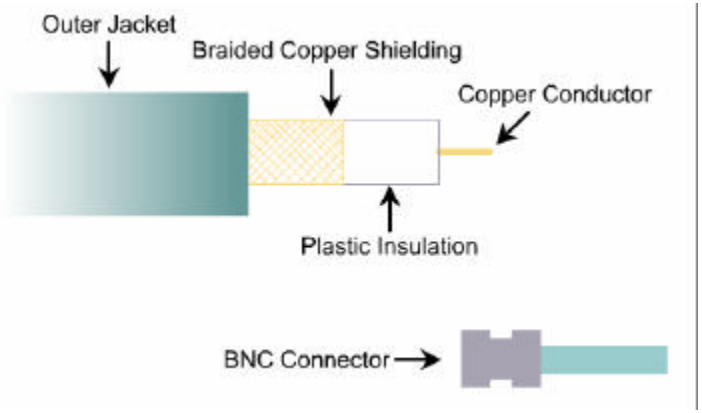


- **10BASE5**
  - speed of transmission at 10 Mbps
  - type of transmission is BASEband
  - 5 represents the capability of the cable to allow the signal to travel for approximately 500 meters before attenuation could disrupt the ability of the receiver to appropriately interpret the signal being received.
  - often referred to as **Thicknet**
  - antiquated technique

Cable used for Ethernet 10 Base2 LAN Standard

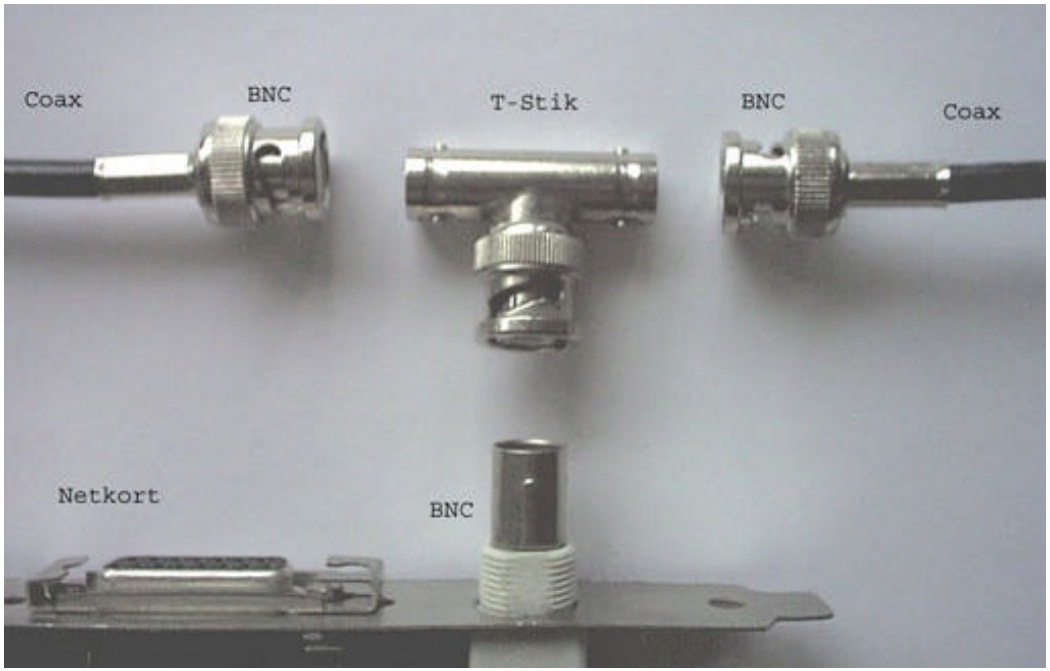
- **10BASE2**
  - speed of transmission at 10 Mbps
  - type of transmission is BASEband
  - The 2, in 10BASE2, represents the capability of the cable to allow the signal to travel for approximately 200 meters (185 m), before attenuation could disrupt the ability of the receiver to appropriately interpret the signal being received.
  - often referred to as **Thinnet**.
  - antiquated technique

Coaxial Cable



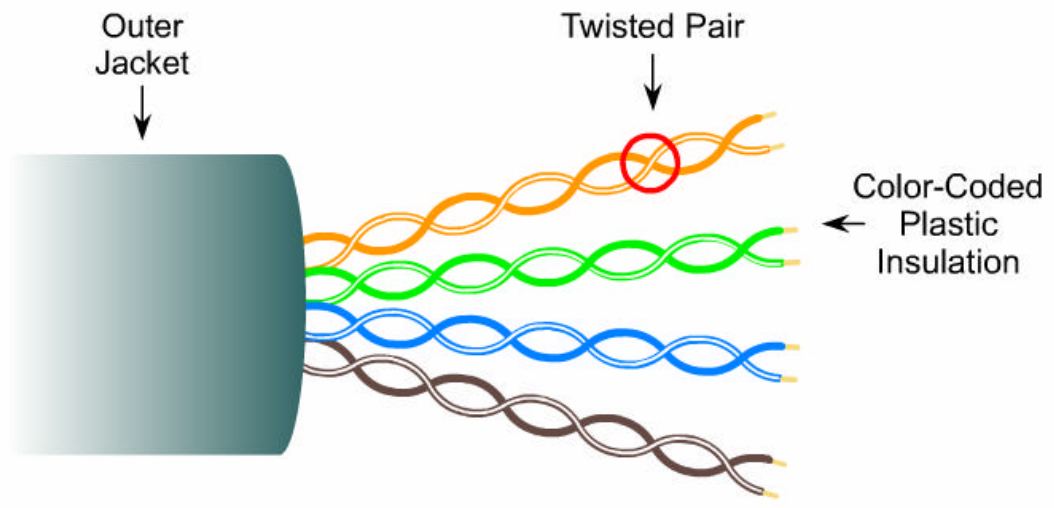
- 10 … 100 Mbps speed and throughput with Ethernet technologies
- Inexpensive
- Medium media and connector size
- Maximum transmission distance : 500 m when used with 10Base5 technology
- Woven **copper braid** (ge: Geflecht) or metallic foil
  - Acts as the second wire in the circuit
  - Acts as a shield for the inner conductor.
  - Reduces the amount of outside electro-magnetic interference.
  - Special care must be taken to ensure a solid electrical connection a both ends resulting in proper grounding
  - Poor shield connection is one of the biggest sources of connection problems in the installation of coaxial cable.

Coaxial Cable



- **Advantages**:
  - lower attentuation than twisted pair (→ Requires fewer repeaters)
  - Less expensive than fiber
  - has been used for many years for many types of data communication, including cable TV
- **Disadvantages**:
  - More expensive and more difficult to install than twisted pair
  - Needs more room in wiring ducts (ge: Kabelkanäle) than twisted pair

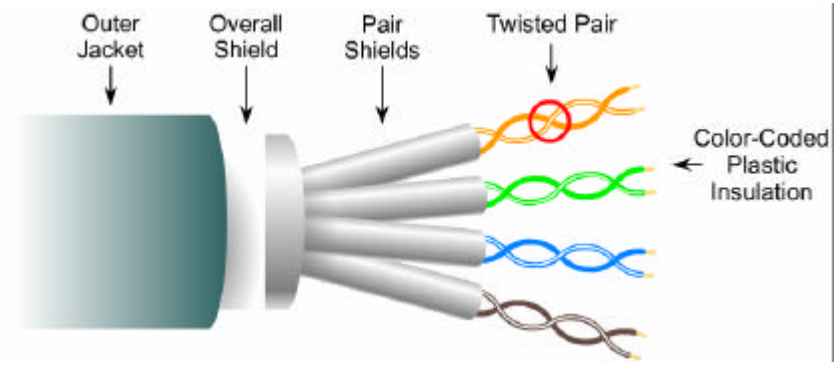
Unshielded Twisted Pair (UTP)



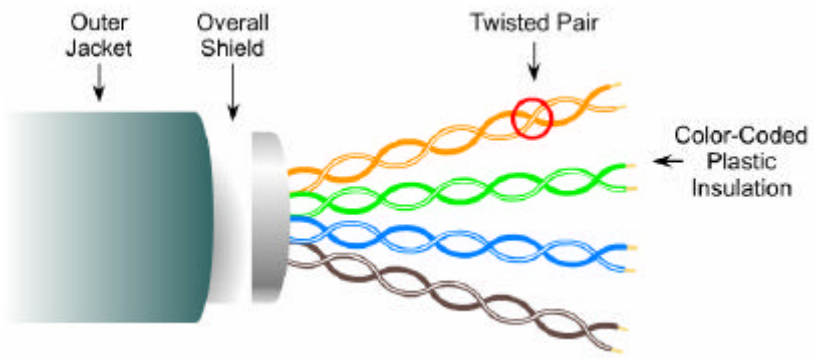
- **Unshielded twisted-pair cable (UTP)**
  - is a four-pair wire medium used in a variety of networks.
  - TIA/EIA-568-B contains specifications governing cable performance.
  - RJ-45 connector
  - 10 … 1000 Mbps speed and throughput with Ethernet technologies

Shielded Twisted Pair (STP and ScTP)

STP – Shielded Twisted Pair



ScTP – Screened Twisted Pair

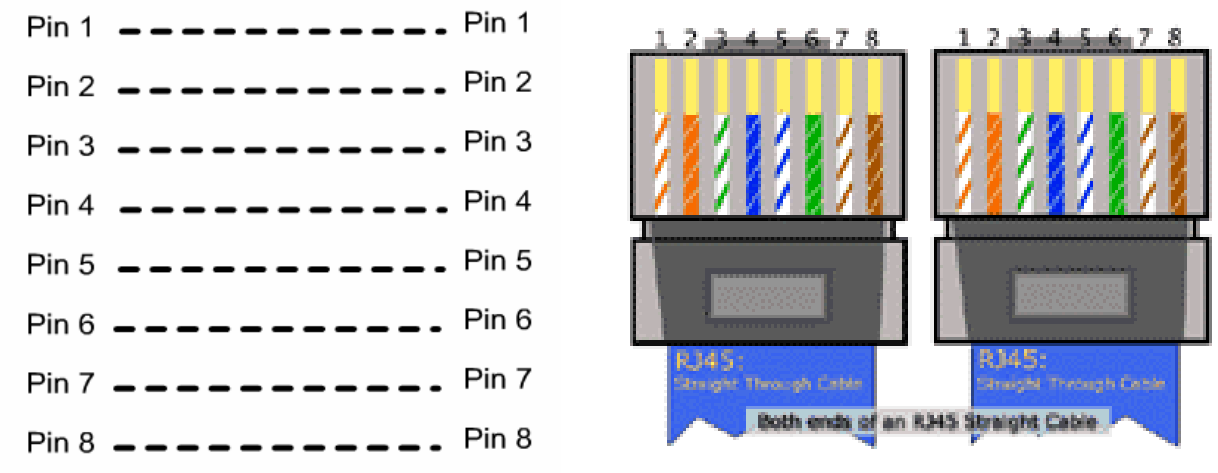


- Greater protection from all types of external and internal interference than UTP.
  - Reduces electrical noise within the cable such as pair to pair coupling and crosstalk.
  - Reduces electronic noise from outside the cable, for example electromagnetic interference (EMI) and radio frequency interference (RFI).
- More expensive and difficult to install than UTP.
- Needs to be grounded at both ends

- **Shielded twisted-pair cable (STP)**
  - combines the techniques of shielding, cancellation, and twisting of wires.
  - Each pair of wires is wrapped in metallic foil.
  - The four pairs of wires are wrapped in an overall metallic braid or foil.
- **Screened UTP (ScTP),**
  - A new hybrid of UTP with traditional STP
  - also known as **Foil Twisted Pair (FTP).**
  - ScTP is essentially UTP wrapped in a metallic foil shield, or screen.

Straight-through Cable

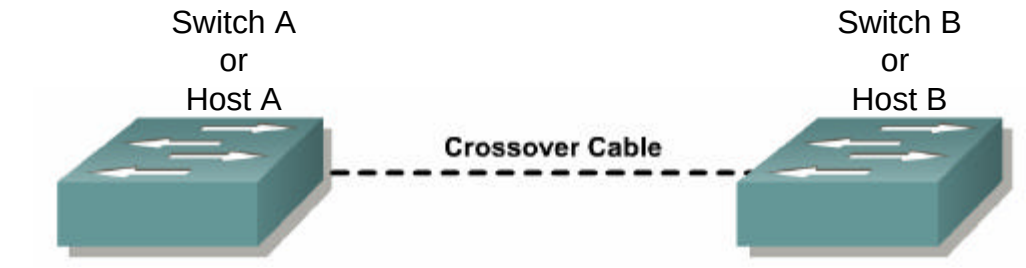
Typical Application Area



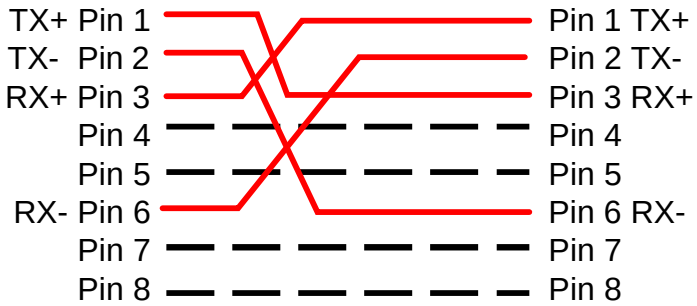
- The cable that connects from the switch port to the computer NIC port is called a straight-through cable.

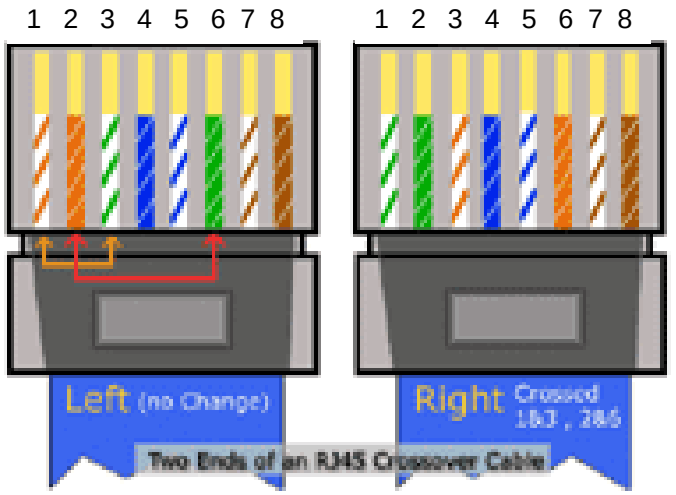
UTP Cross-over Cable

Typical Application Area
- Two computers
- Two hubs
- A hub to a switch
- A cable modem to a router
- Two router interfaces



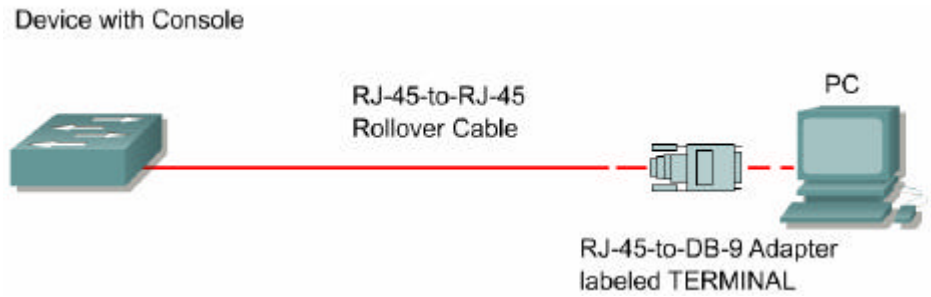
An Ethernet (10BASE-T and 100BASE-TX) cross-connect cable has only four active wires 1, 2, 3, and 6



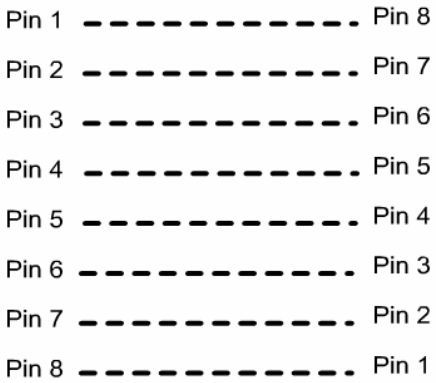


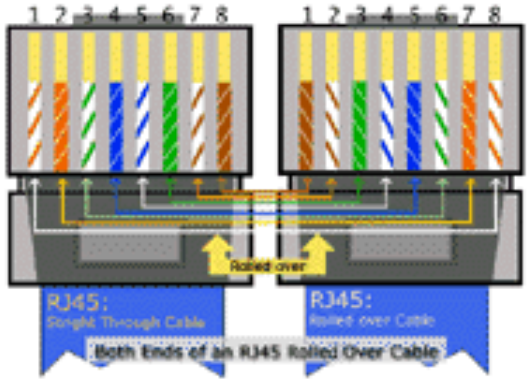
- The cable that connects from one switch port to another switch port is called a crossover cable.

UTP Rollover Cable



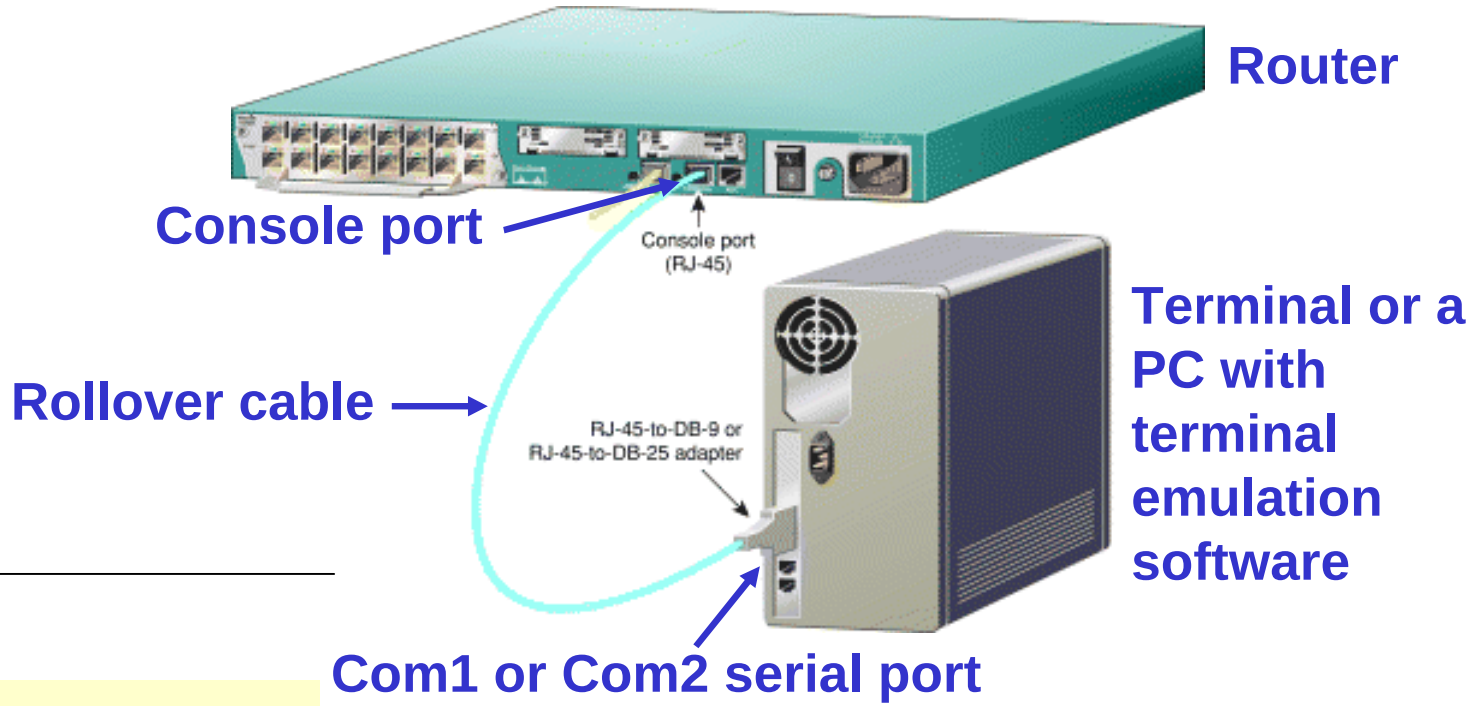
- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

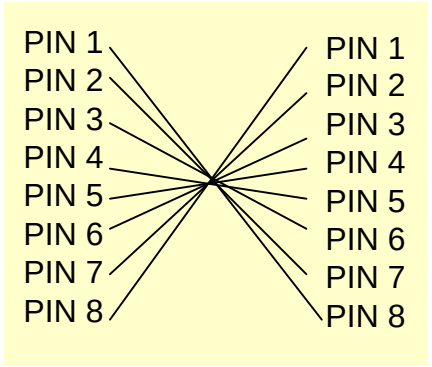




- The cable that connects the RJ-45 adapter on the COM port of the computer to the console port of the router or switch is called a rollover cable.

UTP Rollover Cable





Lab Activities

- **Lab Exercise: Fluke 620 Basic Cable Testing**
  - In this lab, the student will use a simple cable tester to verify whether a straight-through or crossover cable is good or bad.

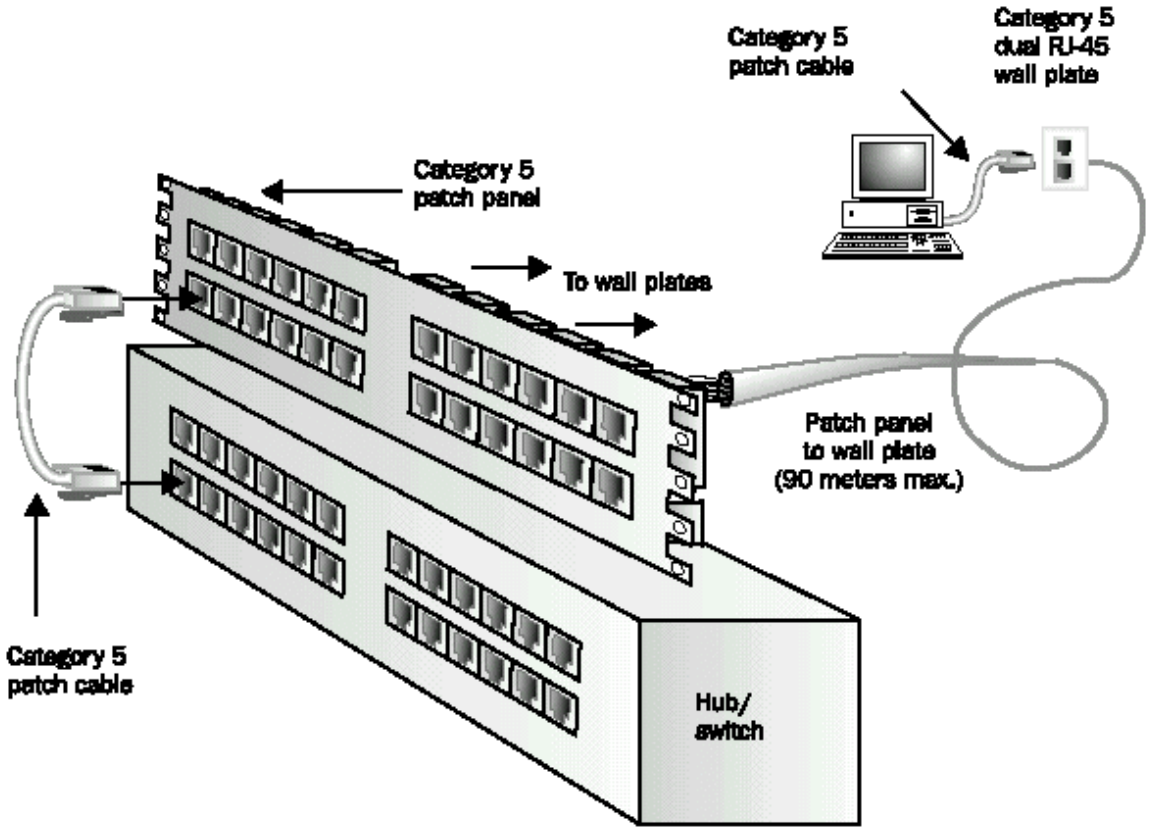
- Lab Exercise: Straight-Through Cable Construction
  - In this lab, the student will build a Category 5 or Category 5e (CAT 5 or 5e) unshielded twisted pair (UTP) Ethernet network patch cable or patch cord and test the cable for continuity and correct pinouts, the correct color of wire on the right pin.

- Lab Exercise: Rollover Cable Construction
  - In this lab, the student will build a Category 5 or Category 5e (CAT 5 or 5e) unshielded twisted pair (UTP) console rollover cable and test the cable for continuity and correct pin-outs, the correct wire on the right pin.

- Lab Exercise: Crossover Cable Construction
  - In this lab, the student will build a Category 5 or Category 5e (CAT 5 or 5e) unshielded twisted pair (UTP) Ethernet crossover cable to T568-B and T-568-A (now obsolete) standards and test the cable for continuity and correct pin-outs, correct wire on the right pin.

- **Lab Exercise: UTP Cable Purchase**
  - This lab will introduce the variety and prices of network cabling and components in the market. The student will gather pricing information for UTP patch cables and bulk cable.

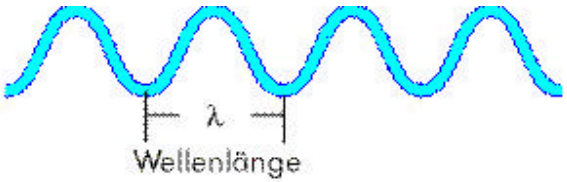
Example: Horizontal Cabling



Optical Media: Objectives

- Explain the basics of fiber-optic cable.
- Describe how fibers can guide light for long distances.
- Describe multimode and single-mode fiber.
- Describe how fiber is installed.
- Describe the type of connectors and equipment used with fiber-optic cable.
- Explain how fiber is tested to ensure that it will function properly.
- Discuss safety issues dealing with fiber-optics.

The electromagnetic spectrum

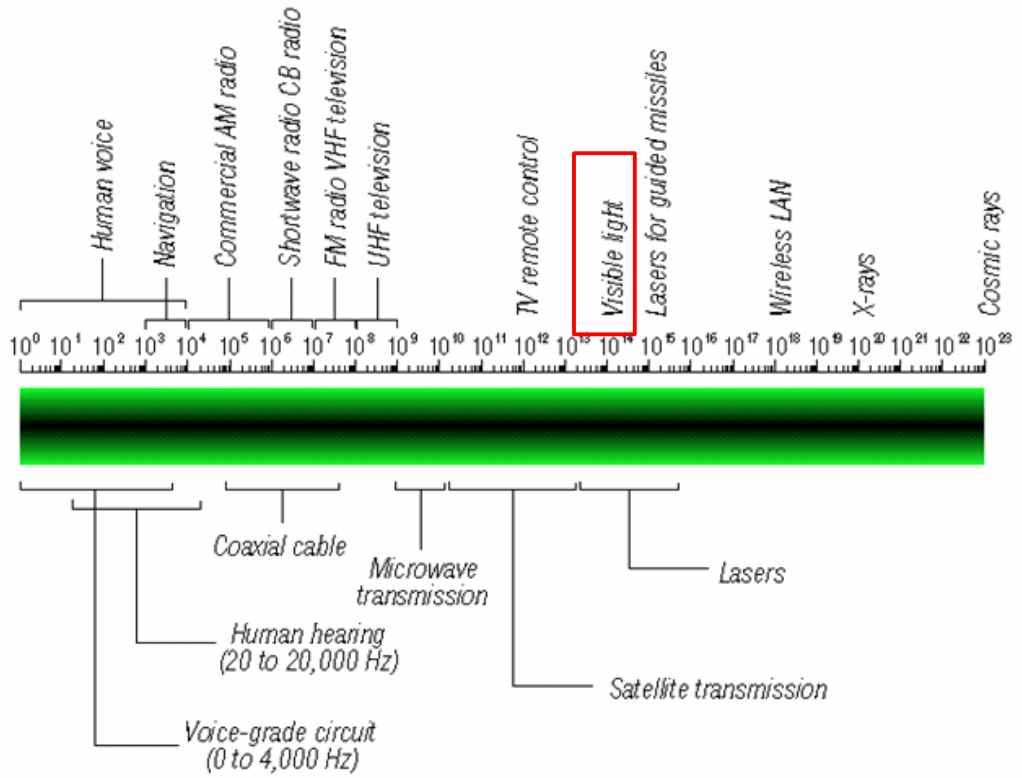


Wichtige Beziehung:

$c = f \cdot \lambda$	c	= Lichtgeschwindigkeit	[m/sec]
	λ	= Wellenlänge	[m]
	f	= Frequenz	[Hz]

- The light used in optical fiber networks is one type of electromagnetic energy.
- Light is electromagnetic energy which can travel in the form of waves through a vacuum, the air, and through some materials like glass.
- An important property of any energy wave is the wavelength.
- Radio, microwaves, radar, visible light, x-rays are all types of electromagnetic energy.

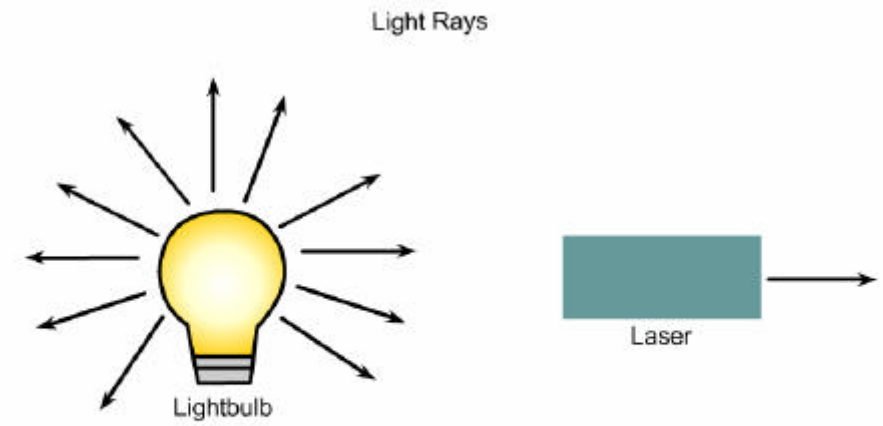
The electromagnetic spectrum



- Wavelengths that are not visible to the human eye are used to transmit data over optical fiber.
- *These wavelengths are slightly longer than red light and are called* **infrared light.**
- Infrared light is also used in TV remote controls.
- These wavelengths were selected because they travel through optical fiber better than other wavelengths.

Ray model of light

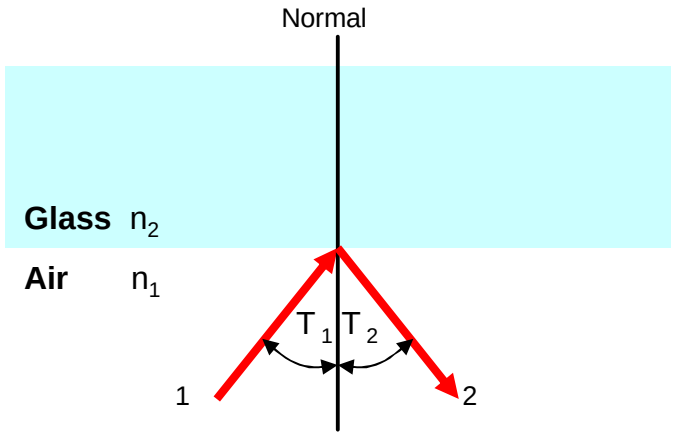
- In the vacuum of empty space, light **rays** travels continuously in a straight line at *300,000 kilometers per second*.
- Light travels at slower speeds through other materials like air, water, and glass. **Optical density** refers to how much a light ray slows down when it passes through a substance.
- The greater the optical density of a material, the more it slows light down from its speed in a vacuum.
- *The ratio of the speed of light in a material to the speed of light in a vacuum* is called the **Index of Refraction** and is a measure of the optical density.



$$\text{Index of Refraction} = n = \frac{\text{Speed of light in vacuum}}{\text{Speed of light in material}}$$

Law of Reflection

- When a light ray called the incident ray, crosses the boundary from one material to another, will be partly reflected back.
- That is why you can see yourself in window glass.
- *The angle between the incident ray and a line perpendicular to the surface of the glass at the point where the incident ray strikes the glass* is called the **angle of incidence**.
- The light that is reflected back is called the **reflected ray**.



Ray 1: Incident ray
Ray 2: Reflected ray

Law of Reflection: $T_1 = T_2$

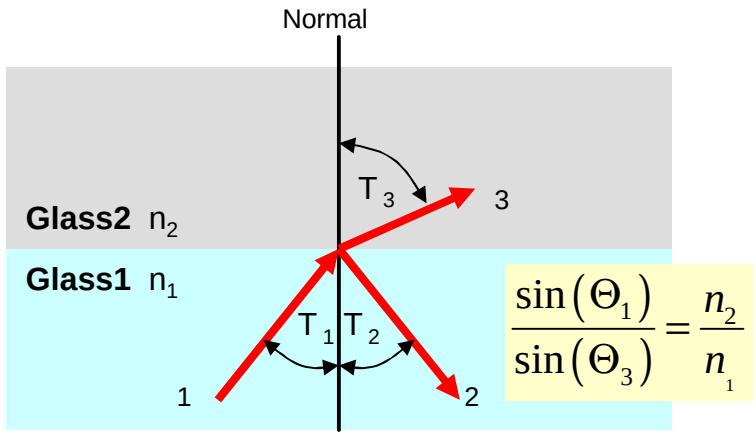
Law of Reflection

Angle of incidence = angle of reflection
or
$T_1 = T_2$

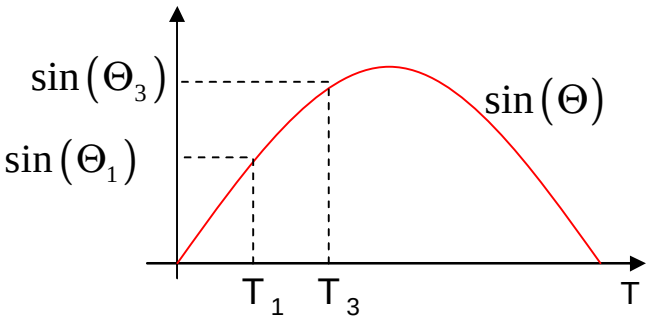
Law of Refraction

- The light energy in the incident ray that is not reflected will enter the Glass2.
- The part entering the Glass2 is called **refracted ray** *because it will be bent at an angle from its original path.*
- How much the incident light ray is bent depends on the angle of the incident ray and the ratio of the refraction index of the two substances
- Law of Refraction:

$$\frac{\sin(\Theta_1)}{\sin(\Theta_3)} = \frac{n_2}{n_1}$$



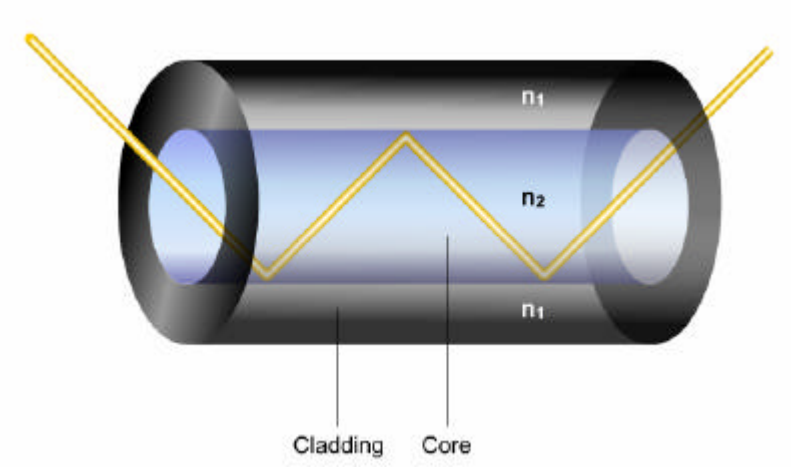
Ray 1: Incident ray
Ray 2: Reflected ray
Ray 3: Refracted ray



$T_3 < T_1$ if $n_2 < n_1$

Total internal reflection

- A light ray that is being turned on and off to send data (1s and 0s) into an optical fiber must stay in the core of the fiber until it reaches the far end.
- The ray must not refract into the cladding material wrapped around the outside of the fiber.



- Refraction would cause the loss of part of the light energy of the ray and therefore contributes to signal attentuation.
- Therefore the interface between the core and the cladding of the fiber must act like a mirror to the light ray reflecting it back into the fiber.
- Fibers acting this way on light rays would be a good “pipe” or “wave guide” for the light waves.

Total internal reflection

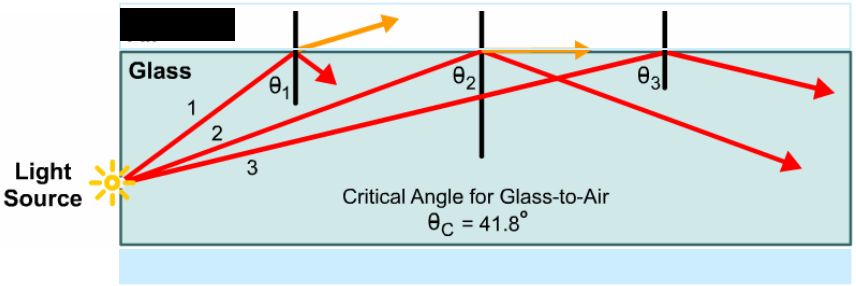
- **Conditions to be met for the light rays in a fiber to be totally reflected back into the fiber without any loss due to refraction**:
  - The core of the optical fiber has to have a larger index of refraction (n) than the cladding material that surrounds it.

$$n_{core} > n_{cladding}$$

  - The angle of incidence of the light ray must be greater than the critical angle for the core and its cladding.
  - The critical angle can be computed from refraction law:

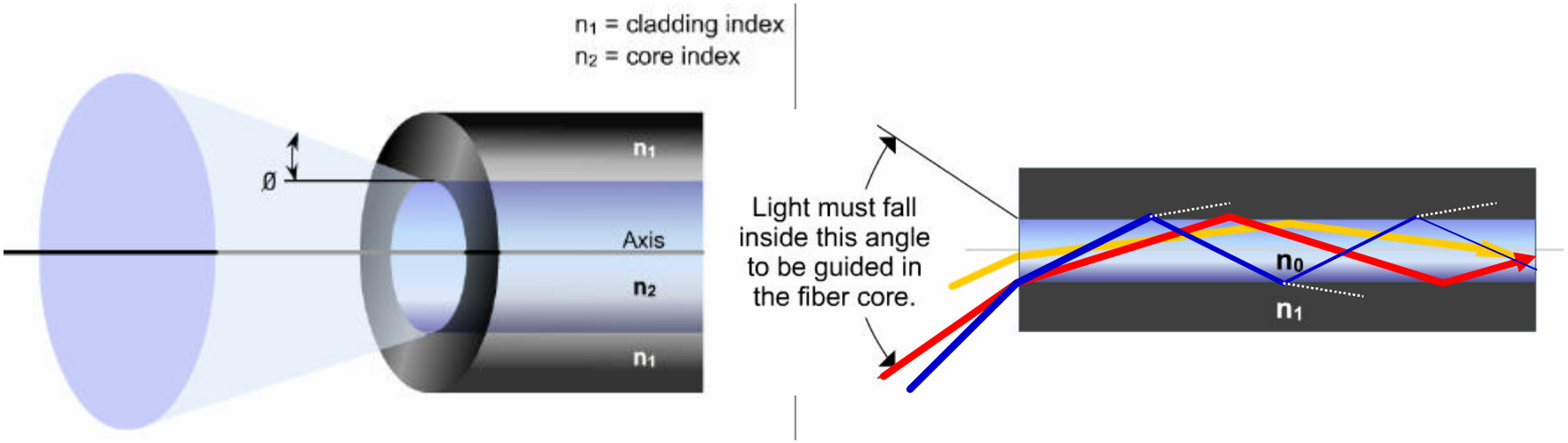
$$\frac{\sin\left(\Theta_{core}\right)}{\sin\left(\Theta_{cladding}\right)} = \frac{\sin\left(\Theta_{core,crit}\right)}{\sin\left(90^0\right)} = \frac{n_{cladding}}{n_{core}}$$

$$\sin\left(\Theta_{core,crit}\right) = \frac{n_{cladding}}{n_{core}}$$



Ray 1: $\theta_1 < \theta_C$, so ray reflects and refracts
Ray 2: $\theta_2 = \theta_C$, so ray reflects and refracts
Ray 3: $\theta_3 > \theta_C$, so ray is totally internally reflected

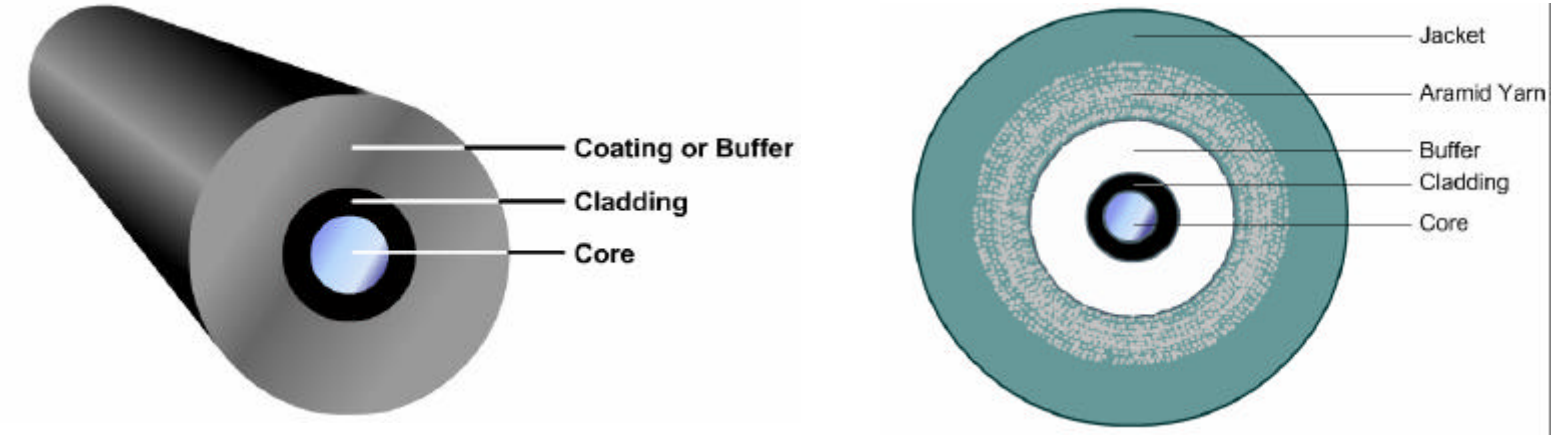
Total internal reflection



NA measures the range of angles that will be totally internally reflected.

- Restricting the following two factors controls the angle of incidence:
  - **The numerical aperture of the fiber** – The numerical aperture of a core is the range of angles of incident light rays entering the fiber that will be completely reflected.
  - **Modes** – The paths which a light ray can follow when traveling down a fiber.
- By controlling both conditions, the fiber run will have total internal reflection. This gives a light wave guide that can be used for data communications.

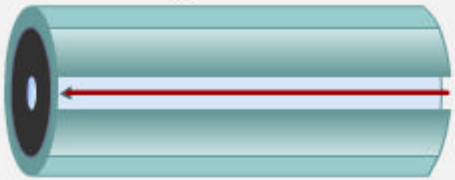
Fiber Optic Cabling



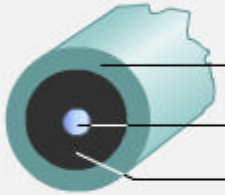
- The **core** is the light transmission element at the center of the optical fiber. All the light signals travel through the core.
- **Cladding** is also made of silica but with a lower index of refraction than the core. Light rays traveling through the fiber core reflect off this core-to-cladding interface as they move through the fiber by total internal reflection.
- Surrounding the cladding is a **buffer** material that is usually plastic. The buffer material helps shield the core and cladding from damage.
- The strength material surrounds the buffer, preventing the fiber cable from being stretched when installers pull it. The material used is often **Kevlar**, the same material used to produce bulletproof vests.
- The **outer jacket** surrounds the cable to protect the fiber against abrasion, solvents, and other contaminants.

Fiber Optic Cabling

Single-mode



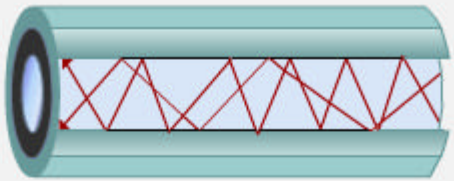
Requires very straight path



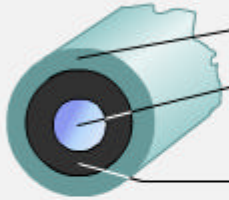
- Small core
- Less dispersion
- Suited for long distance applications (up to ~3km, 9,840 ft)
- Uses lasers as the light source often within campus backbones for distances of several thousand meters

Higher bandwidth.

Multimode

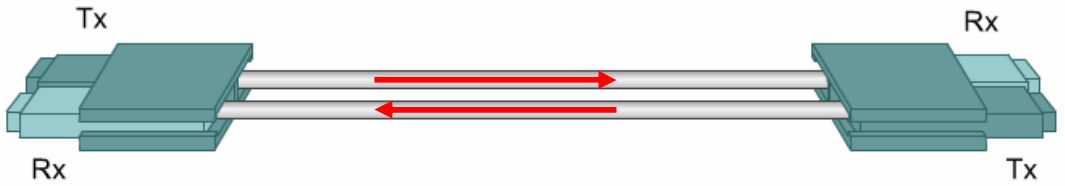


Multiple paths-sloppy

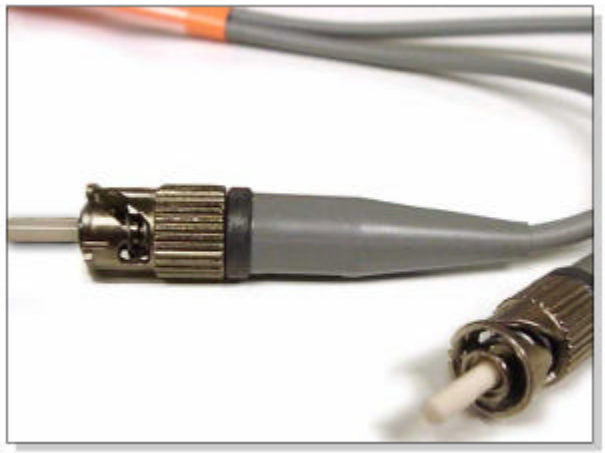


- Larger core than single-mode cable (50 or 62.5 microns or greater)
- Allows greater dipersion and therefore, loss of signal
- Used for long distance application, but shorter than single-mode (up to ~2km, 6,560 ft)
- Uses LEDs as the light source often within LANs or distances of a couple hundred meters within a campus network

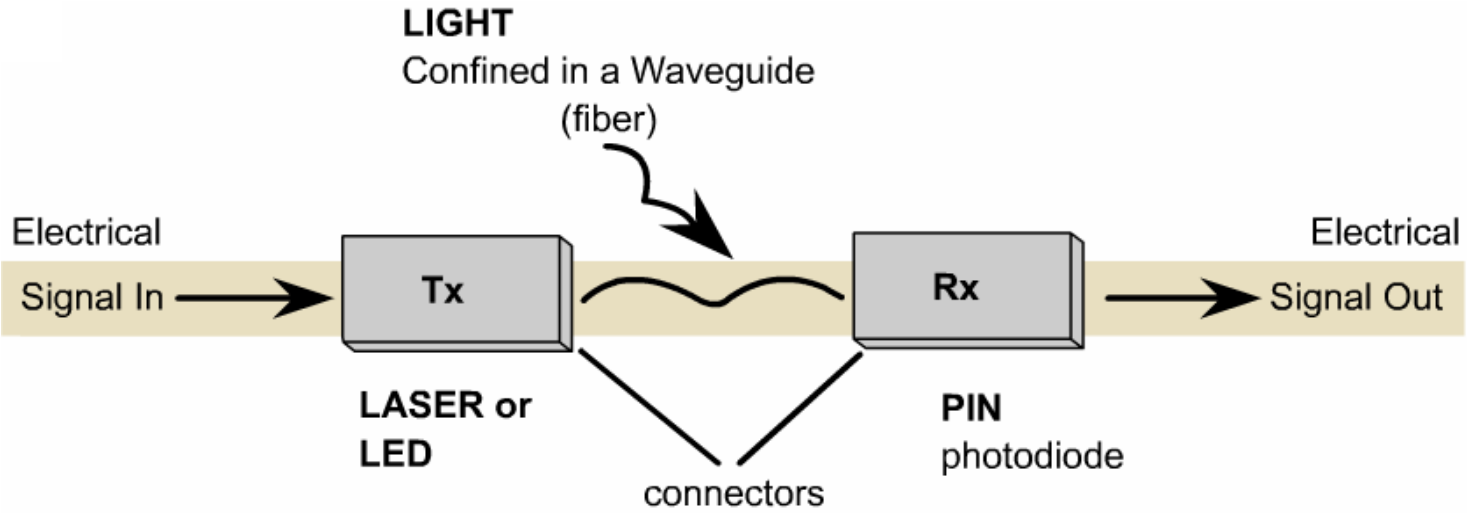
Fiber Optic Cabling



- Every fiber-optic cable used for networking consists of two glass fibers encased in separate sheaths (ge: Hülle)., one for each direction.
- This provides a full-duplex communication link.
- Typically, these two fiber cables will be in a single outer jacket until they reach the point at which connectors are attached.



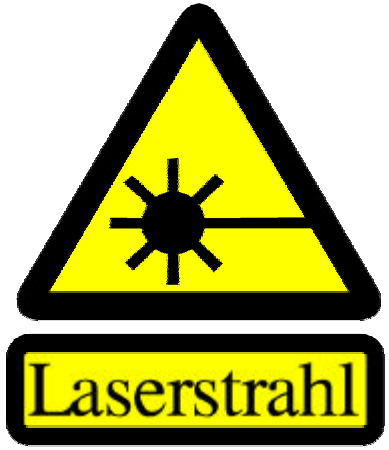
Transmitting Devices



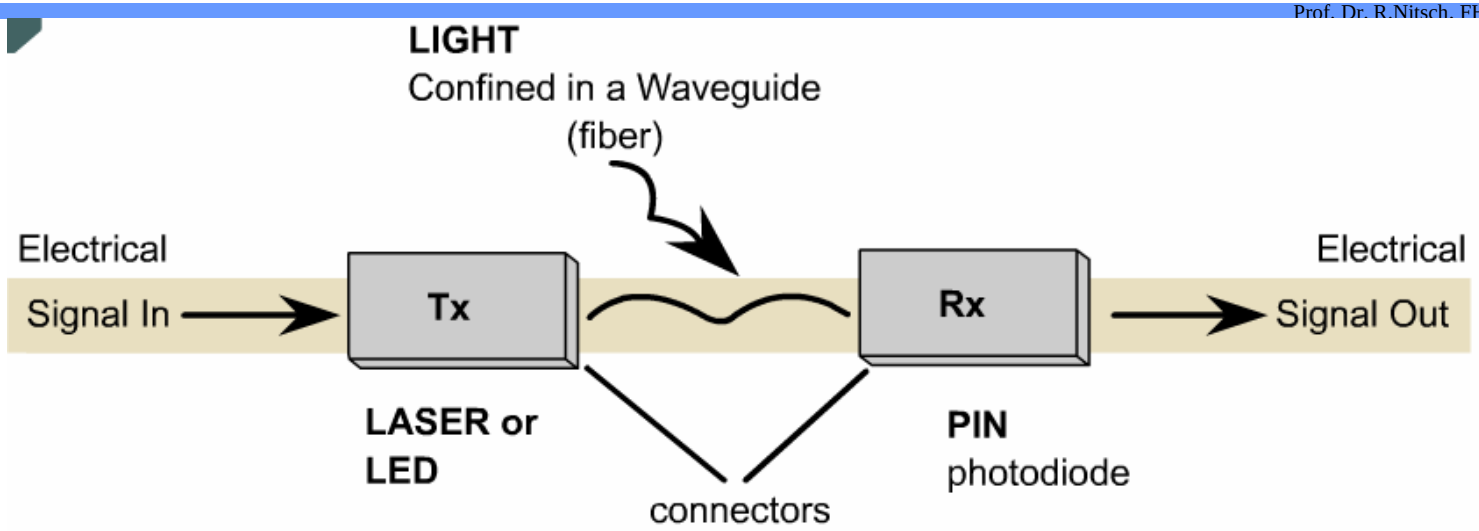
- The **transmitter** Tx converts the electronic signals into their equivalent **light pulses**.
- Two types of light sources are commonly used to transmit the data through the cable:
  - A light emitting diode (**LED**) producing infrared light (~800 nm).
  - Light Amplification by Stimulated Emission Radiation (**LASER**) a light source producing a thin beam of intense infrared light usually with wavelengths of 1310nm or 1550 nm.
  - Lasers are used with single-mode fiber over the longer distances involved in WANs or campus backbones.

Laser Security

- **Warning:** The laser light used with single-mode has a longer wavelength than can be seen.
- The laser is so strong that it can seriously damage eyes.
- **Never** look at the near end of a fiber that is connected to a device at the far end.
- **Never** look into the transmit port on a NIC, switch, or router.
- Remember to keep protective covers over the ends of fiber and inserted into the fiber-optic ports of switches and routers.

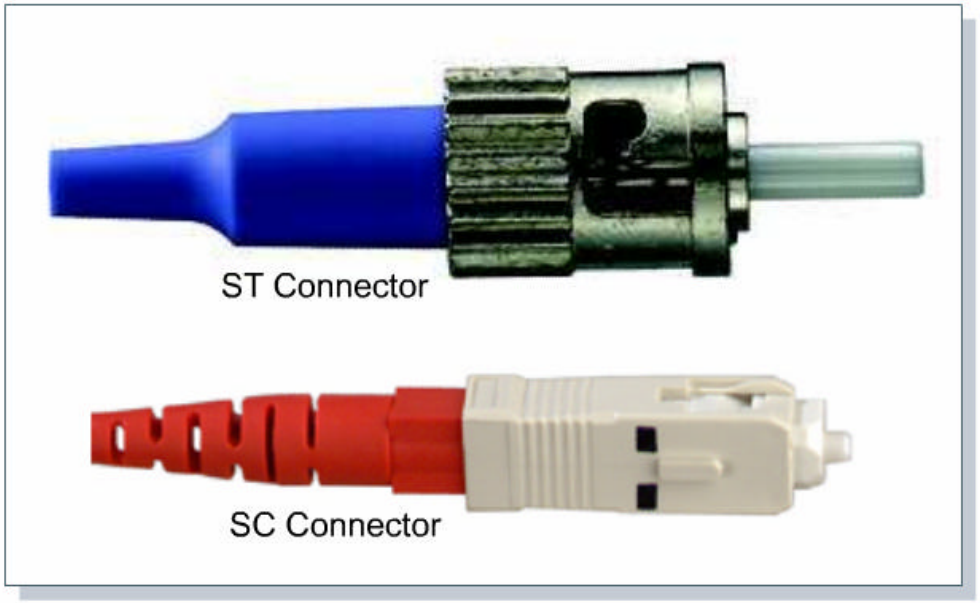


Receiving Devices



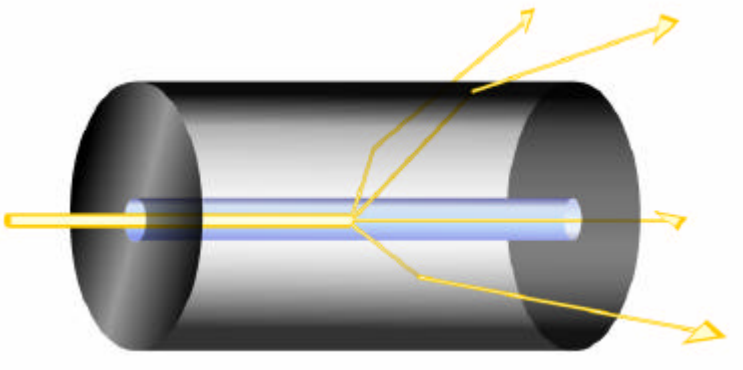
- The receiver functions something like the photoelectric cell in a solar powered calculator: When light strikes the solar cell, it produces electrical current.
- The semiconductor devices that are usually used as receivers with fiber-optic links are called **p-intrinsic-n diodes (PIN photodiodes).**
- *When struck by a pulse of light at the proper wavelength, the PIN photodiode quickly produces an equivalent pulse of electric current for the network.*
- Flowing through a resistor this current pulse generates the voltage changes that represent the data 1s and 0s on a copper cable.

ST and SC Connectors



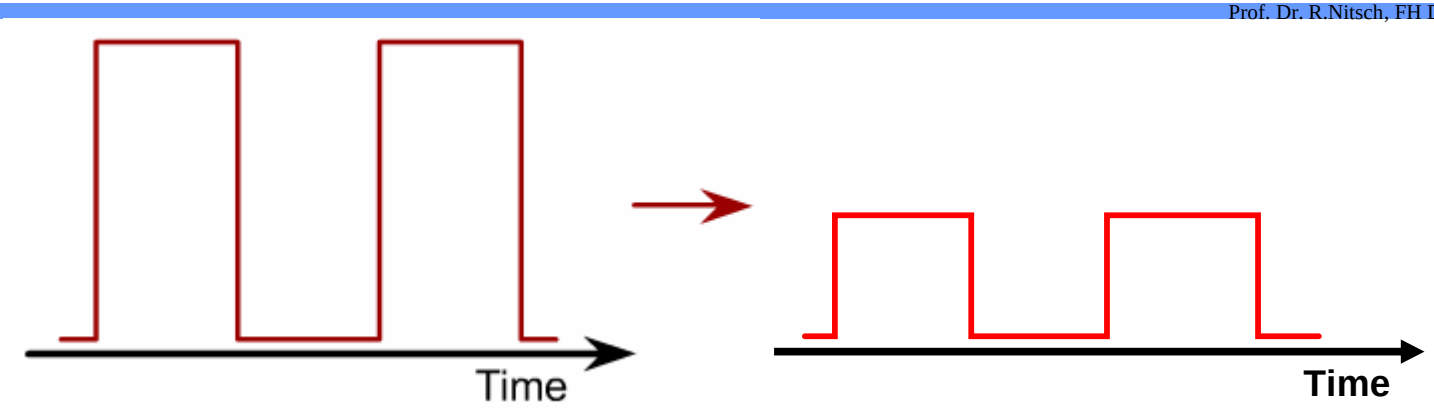
- The type of connector most commonly used with multimode fiber is the Subscriber Connector (SC connector).
- On single-mode fiber, the Straight Tip (ST) connector is frequently used.

Problems with fibers: Signals and noise in optical fibers



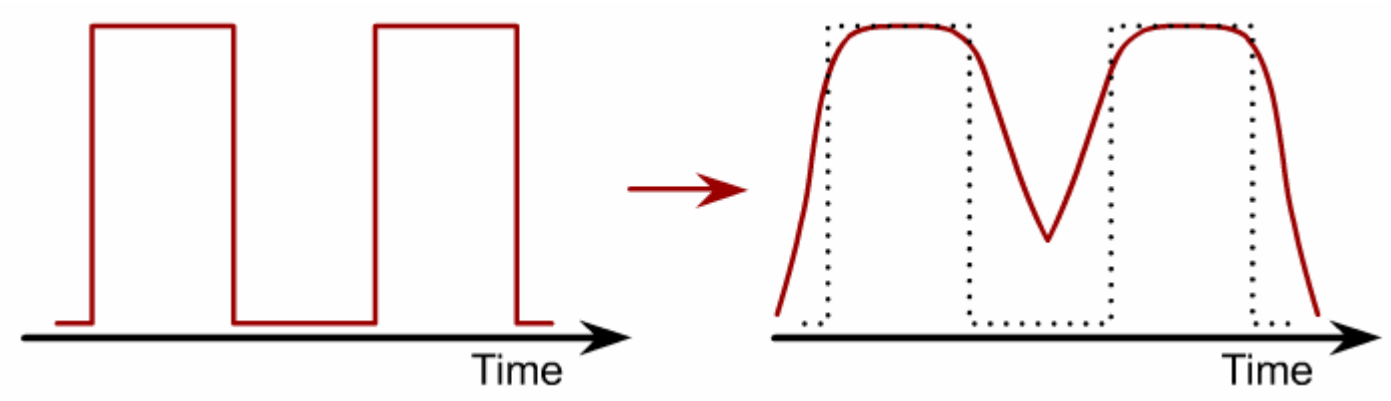
- Fiber-optic cable is not affected by the sources of external noise that cause problems on copper media because external light cannot enter the fiber except at the transmitter end.
- Although fiber is the best of all the transmission media at carrying large amounts of data over long distances, fiber is not without problems. When light travels through fiber, some of the light energy is lost.
- The most important factor is **scattering**.
  - The scattering of light in a fiber is caused by microscopic non-uniformity (distortions) in the fiber that reflects and scatters some of the light energy.
  - This scattering introduces signal attentuation.

Problems with fibers: Signals and noise in optical fibers



- **Absorption** is another cause of signal attenuation.
  - When a light ray strikes some types of chemical impurities in a fiber, the impurities absorb part of the energy.
  - This light energy is converted to a small amount of heat energy.
- Another factor that causes attenuation of the light signal is **manufacturing irregularities** or roughness in the core-to-cladding boundary.
  - Any microscopic imperfections in the thickness or symmetry of the fiber will cut down on total internal reflection and the cladding will absorb some light energy.

Problems with fibers: Signals and noise in optical fibers



- **Dispersion** of a light flash also limits transmission distances on a fiber.
  - Dispersion is the technical term for the spreading of pulses of light as they travel down the fiber

Installation, care, and testing of optical fiber

- Once the fiber-optic cable and connectors have been installed, the connectors and the ends of the fibers must be kept spotlessly clean.
- The ends of the fibers should be covered with protective covers to prevent damage to the fiber ends.
- When these covers are removed prior to connecting the fiber to a port on a switch or a router, the fiber ends must be cleaned with pure isopropyl alcohol.
- The fiber ports on a switch or router should also be kept covered when not in use.
- Dirty ends on a fiber will cause a big drop in the amount of light that reaches the receiver.

- When a fiber-optic link is being planned, the amount of signal power loss that can be tolerated must be calculated. This is referred to as the **optical link loss budget**.
- The **decibel (dB)** is the "unit" used to measure the amount of power loss.
  - It tells indirectly what percent of the power that leaves the transmitter actually enters the receiver.
- Testing fiber links is extremely important and records of the results of these tests must be kept.
- Two of the most important instruments are
  - Optical Loss Meters
  - Optical Time Domain Reflectometers (OTDRs).

Wireless Media - Objectives

- Wireless LAN organizations and standards
- Wireless devices and topologies
- How wireless LANs communicate
- Authentication and association
- The radio wave and microwave spectrums
- Signals and noise on a WLANs
- Wireless security

Wireless WAN Standards

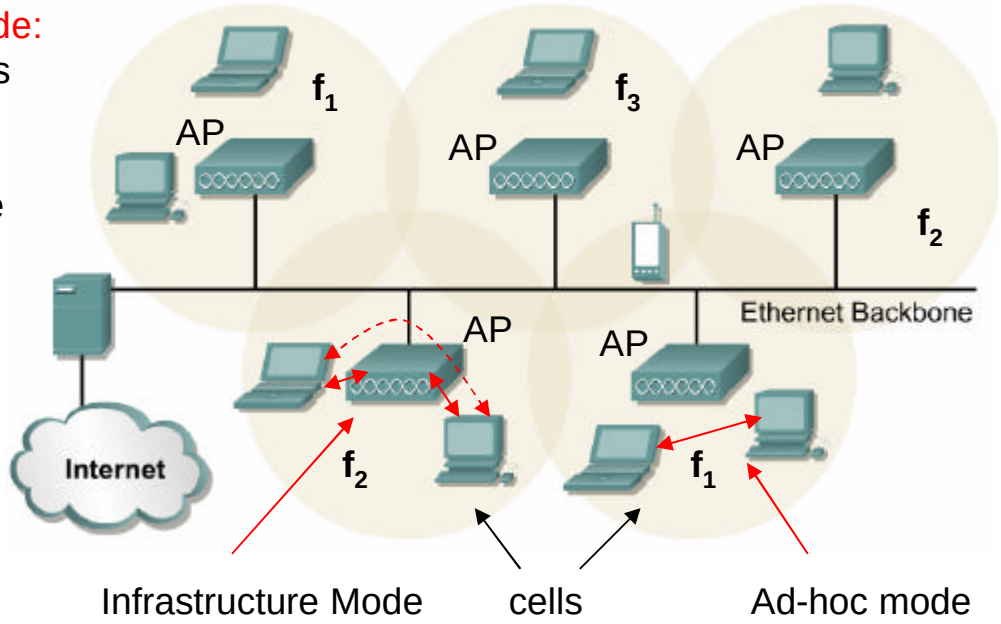
- IEEE is the prime issuer of standards for wireless networks.
- **802.11b** may also be called Wi-Fi™ or high-speed wireless and refers to DSSS systems that operate at *1, 2, 5.5 and 11 Mbps*.
  - The majority of 802.11b devices still fail to match the 11 Mbps throughput and *generally function in the 2 to 4 Mbps range.*
  - Operates in the 2,4 GHz transmission band; larger coverage area than 802.11a
  - Available in Europe; Supports roaming
- **802.11a** covers WLAN devices operating in the 5 GHz transmission band.
  - 802.11a is capable of supplying data throughput of *54 Mbps* and with proprietary technology known as "*rate doubling*" has achieved *108 Mbps*.
  - In production networks, a more standard rating is *20-26 Mbps*.
  - Used in North Amerika and Japan
- **802.11g** provides the same throughput as 802.11a (54 Mbps) but operates in the 2,4 GHz band with backward compatibility for 802.11b devices.

The global picture: a multiplicity of WLAN standards

Features	802.11a North America Japan	802.11g Europe	802.11b Europe
Operating Frequency Band	5 GHz Industrial, Scientific and Medical Band	2,4 GHz	2,4 GHz
Data Rates	6, 9, 12, 18, 24, 36, 48 and 54 Mbps	6, 9, 12, 18, 24, 36, 48 and 54 Mbps	1, 2, 5.5 and 11 Mbps
System	Orthogonal Frequency Division Multiplexing (OFDM)	OFDM	Frequency Division Multiple Access (FDMA)
Approximate Range	50 m	>= 100 m	100m

Wireless devices and topologies

Infrastructure Mode:
Wireless end-points communicate via a wireless relaying Access Point device



Ad-hoc Mode:
Wireless end-points communicate directly with each other. An Access Point is not involved.

- Overlapping service areas, on multiple Access Point (AP) networks, are critical to allow for movement of devices within the WLAN.
- Although not addressed in the IEEE standards, a 20-30% overlap is desirable.
- This rate of overlap will permit roaming between cells, allowing for the disconnect and reconnect activity to occur seamlessly without service interruption.
- A minumum of 2 devices exists in a wireless network.

Wireless devices and topologies

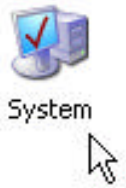
- **Access point (AP)** is commonly installed to act as a central hub for the WLAN "infrastructure mode".
- The AP is hard wired to the cabled LAN to provide Internet access and connectivity to the wired network. APs are equipped with antennas and provide wireless connectivity over a specified area referred to as a cell.
- Depending on the structural composition of the location in which the AP is installed and the size and gain of the antenna, the size of the cell could greatly vary.
- Most commonly, the range will be from 90 to 150 meters (300 to 500 feet).

- When a client is activated within the WLAN, it will start "listening" for a compatible device with which to "associate".
- This is referred to as "**scanning**" and may be active or passive.
- Active scanning causes a request to be sent from the wireless node seeking to join the network.
- The request will contain the **Service Set Identifier (SSID)** of the network it wishes to join.
- When an AP with the same SSID is present, the AP will issue a response.
- The **authentication and association** steps are completed.
- From webpedia.com
  - SSID: a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a "password" when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network.

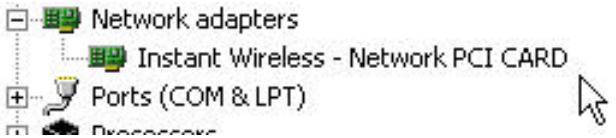
Configuring the SSID on the PC (depends on Operating System!)

1

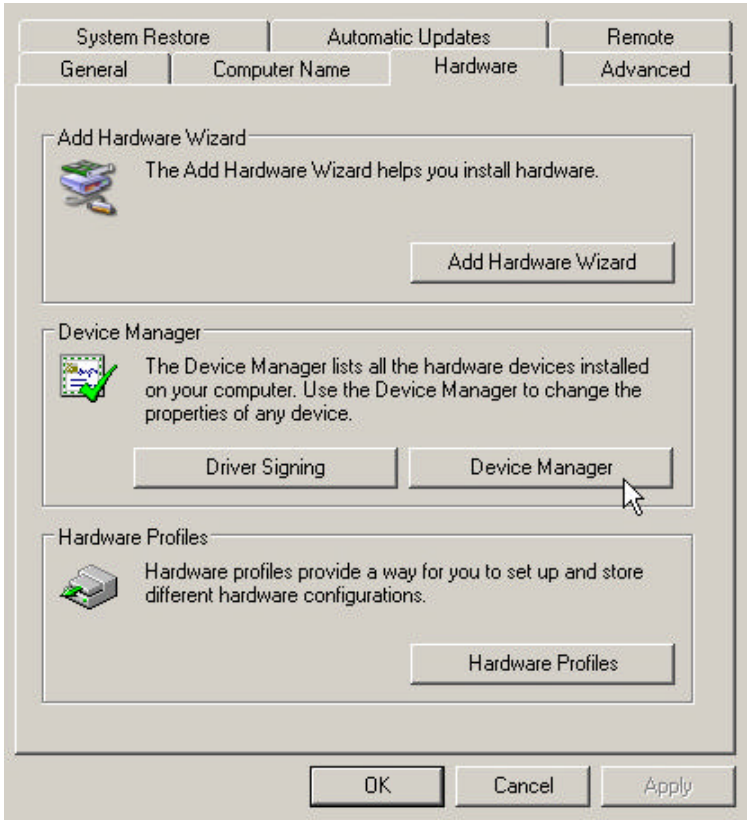
2



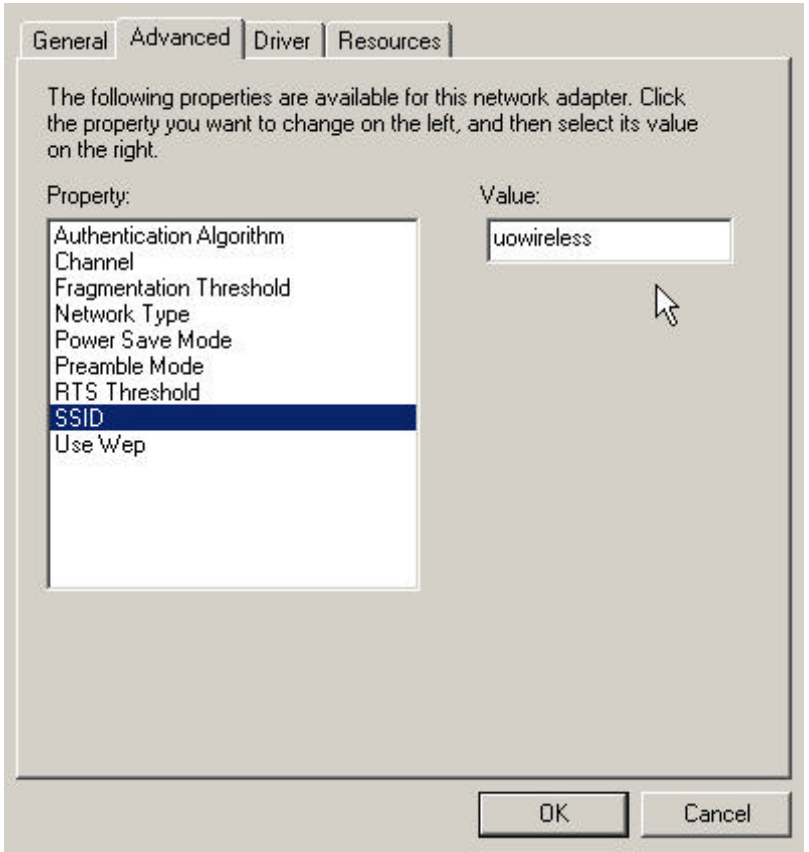
4



3



5



micro.uoregon.edu/ wireless/windows/

How Wireless LANs communicate

- WLANs do not use a standard 802.3 frame.
- Therefore, using the term wireless Ethernet is misleading.
- There are three types of frames: control, management, and data.
- Only the data frame type is similar to Ethernet 802.3 frames.

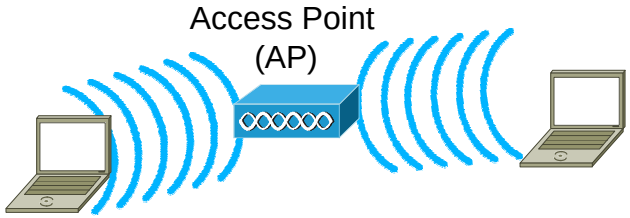
Management Frames
- Association request frame
- Association response frame
- Probe request frame
- Probe response frame
- Beacon frame
- Authentication frame

Control Frames
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment

Data Frames

How wireless LANs communicate

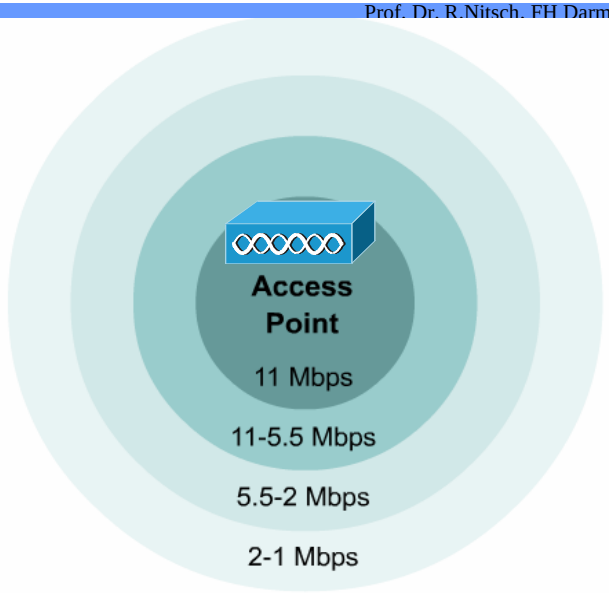
- Since radio frequency (RF) is a shared medium, collisions can occur just as they do on wired shared medium.
- The **major difference** is that there is no method by which the source node is able to detect that a collision occurred.
- For that reason WLANs use Carrier Sense Multiple Access / **Collision Avoidance** (CSMA/CA). This is somewhat like Ethernet CSMA/CD):



  - When a source node sends a frame, the receiving node returns a *positive acknowledgment (ACK).*
  - This can cause *consumption of 50% of the available bandwidth*.
  - This overhead when combined with the collision avoidance protocol overhead reduces the *actual data throughput to a maximum of 5.0 to 5.5 Mbps* on an 802.11b wireless LAN rated at 11 Mbps.

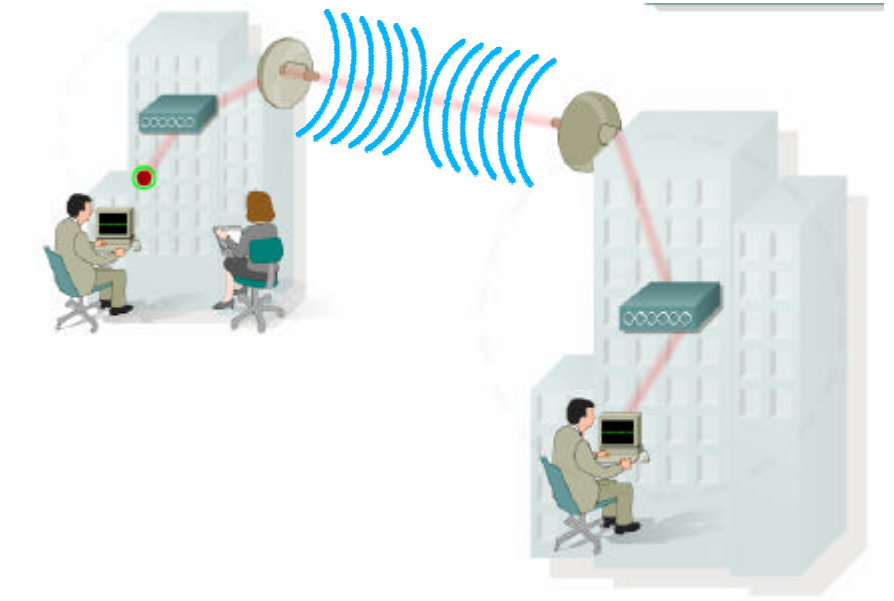
How wireless LANs communicate

- Performance of the network will also be affected by signal strength and degradation in signal quality due to distance or interference.
- As the signal becomes weaker, Adaptive Rate Selection (ARS) may be invoked.
- The transmitting unit will drop the data rate from 11 Mbps to 5.5 Mbps, from 5.5 Mbps to 2 Mbps or 2 Mbps to 1 Mbps.



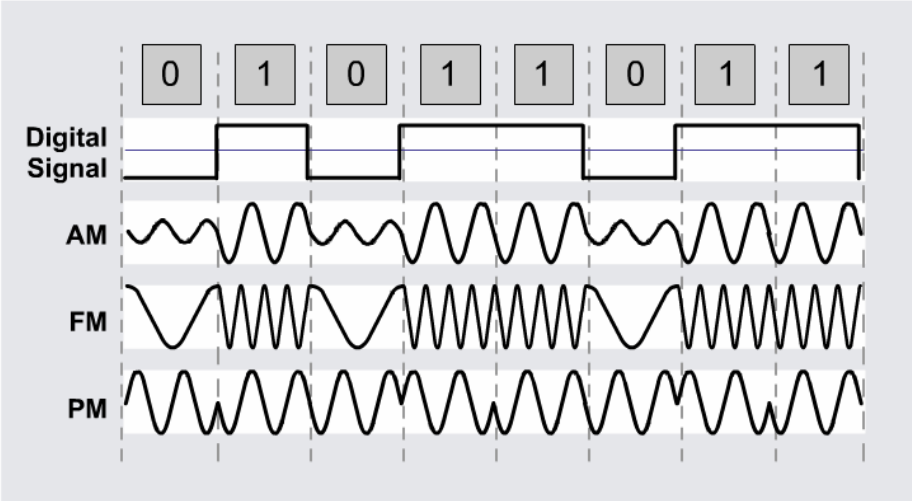
The radio wave and microwave spectrums

- Computers send data signals electronically.
- Radio transmitters convert these electrical signals to radio waves.
- However, radio waves attenuate as they move out from the transmitting antenna.
- In a WLAN, a radio signal measured at a distance of just 10 meters (30 feet) from the transmitting antenna would be only 1/100th of its original strength.



Modulation

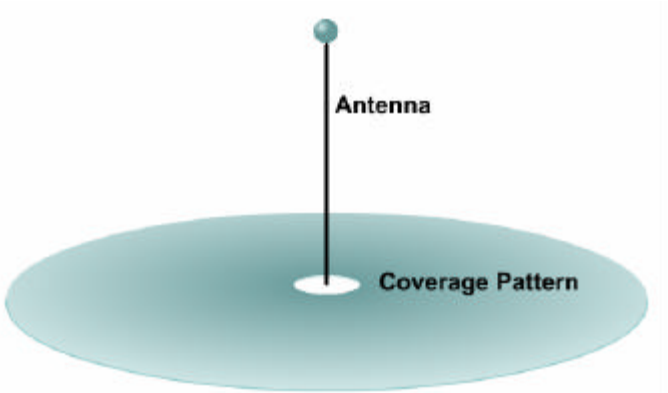
- The process of altering the carrier signal that will enter the antenna of the transmitter is called modulation.
- There are three basic ways in which a radio carrier signal can be modulated.
- **Amplitude Modulated (AM)** radio stations modulate the *height (amplitude) of the carrier signal*.



- **Frequency Modulated (FM)** radio stations modulate the *frequency of the carrier signal* as determined by the electrical signal from the microphone or data source.
- In WLANs, a third type of modulation called **Phase Modulation (PM)** stations modulate the *phase of the carrier signal* as determined by the electrical signal from the microphone or data source.

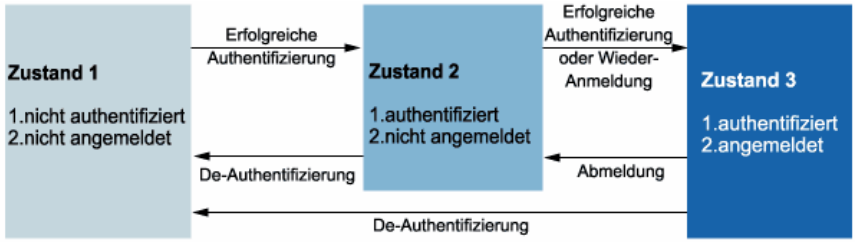
Radio Interference: Signals and noise on a WLAN

- When using RF technology many kinds of interference must be taken into consideration.
- In homes and offices, a device that is often overlooked as causing interference is the standard microwave oven.
- Leakage from a microwave oven of as little as one watt into the RF spectrum can cause major network disruption.
- Wireless phones operating in the 2.4 GHz spectrum can also cause network disorder.
- The RF signal can be affected by some extreme weather conditions such as fog or very high moisture conditions. Lightning can also charge the atmosphere and alter the path of a transmitted signal.



Authentication and association

- WLAN authentication occurs at Layer 2.
- WLAN authentication authenticates the device not the user.
- The client will send an authentication request frame to the AP and the frame will be accepted or rejected by the AP.
- The client is notified of the response via an authentication response frame.
- Association, performed after authentication, is the state that permits a client to use the services of the AP to transfer data.
- Possible states are:
  - Unauthenticated and unassociated
    - The node is disconnected from the network and not associated to an access point.
  - Authenticated and unassociated
    - The node has been authenticated on the network but has not yet associated with the access point.
  - Authenticated and associated
    - The node is connected to the network and able to transmit and receive data through the access point.



Methods of Authentication

- WLAN authentication occurs at Layer 2.
- WLAN authentication authenticates the device not the user.
- IEEE 802.11 lists two types of authentication processes.
- The first authentication process is the **open system**.
  - This is an open connectivity standard in which only the **SSID** must match.
  - This may be used in a secure or non-secure environment despite the ability of low level network 'sniffers' to discover the SSID of the WLAN is high.
- The second process is the **shared key**.
  - This process requires the use of **Wireless Equivalency Protocol (WEP) encryption**.
  - WEP is a fairly simple algorithm using 40 and 128 bit keys.
  - The AP is configured with an encrypted key and nodes attempting to access the network through the AP must have a matching key.
  - Statically assigned WEP keys provide a higher level of security than the open system but are ***definitely not hack proof***.
- The problem of unauthorized entry into WLANs is being addressed by a number of new security solution technologies.

Wireless security

- A number of new security solutions and protocols, such as Virtual Private Networking (VPN) and Extensible Authentication Protocol (EAP) are emerging.
- With EAP, the access point does not provide authentication to the client, but passes the duties to a more sophisticated device, possibly a dedicated server, designed for that purpose.
- **EAP-MD5 Challenge** – Extensible Authentication Protocol is the earliest authentication type, which is very similar to CHAP password protection on a wired network.
- **LEAP (Cisco)** – Lightweight Extensible Authentication Protocol is the type primarily used on Cisco WLAN access points. LEAP provides security during credential exchange, encrypts using dynamic WEP keys, and supports mutual authentication.
- **User authentication** – Allows only authorized users to connect, send and receive data over the wireless network.
- **Data authentication** – Ensures the integrity of the data (data cannot be altered without detection) and additionally authenticates source devices.
- **Encryption** – Provides encryption services further protecting the data from intruders.

Summary 1 of 3

An understanding of the following key points should have been achieved:

- All matter is composed of atoms, and the three main parts of an atom are: protons, neutrons, and electrons. The protons and neutrons are located in the center part of the atom (nucleus)
- Electrostatic discharge (ESD) can create serious problems for sensitive electronic equipment
- Attenuation refers to the resistance to the flow of electrons and why a signal becomes degraded as it travels
- Currents flow in closed loops called circuits, which must be composed of conducting materials and must have sources of voltage
- A multimeter is used to measure voltage, current, resistance, and other electrical quantities expressed in numeric form
- Three types of copper cables used in networking are: straight-through, crossover, and rollover
- Coaxial cable consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor
- UTP cable is a four-pair wire medium used in a variety of networks
- STP cable combines the techniques of shielding, cancellation, and twisting of wires

Summary 2 of 3

- Optical fiber is a very good transmission medium when it is properly installed, tested, and maintained
- Light energy, a type of electromagnetic energy wave, is used to transmit large amounts of data securely over relatively long distances
- The light signal carried by a fiber is produced by a transmitter that converts an electrical signal into a light signal
- The light that arrives at the far end of the cable is converted back to the original electrical signal by the receiver
- Fibers are used in pairs to provide full duplex communications
- Light rays obey the laws of reflection and refraction as they travel through a glass fiber, which allows fibers with the property of total internal reflection to be manufactured
- Total internal reflection makes light signals stay inside the fiber, even if the fiber is not straight
- Attenuation of a light signal becomes a problem over long cables especially if sections of cable are connected at patch panels or spliced
- Cable and connectors must be properly installed and thoroughly tested with high quality optical test equipment before their use
- Cable links must be tested periodically with high quality optical test instruments to check whether the link has deteriorated in any way
- Care must always be taken to protect eyes when intense light sources like lasers are used

Summary 3 of 3

- Understanding the regulations and standards that apply to wireless technology will ensure that deployed networks will be interoperable and in compliance
- Compatibility problems with NICs are solved by installing an access point (AP) to act as a central hub for the WLAN
- Three types of frames are used in wireless communication: control, management, and data
- WLANs use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
- WLAN authentication is a process that authenticates the device, not the user