Network Media and Error Detection and Correction

3.1.1 Twisted-Pair Cable

Figure 1: Unshielded Twisted-Pair Cable

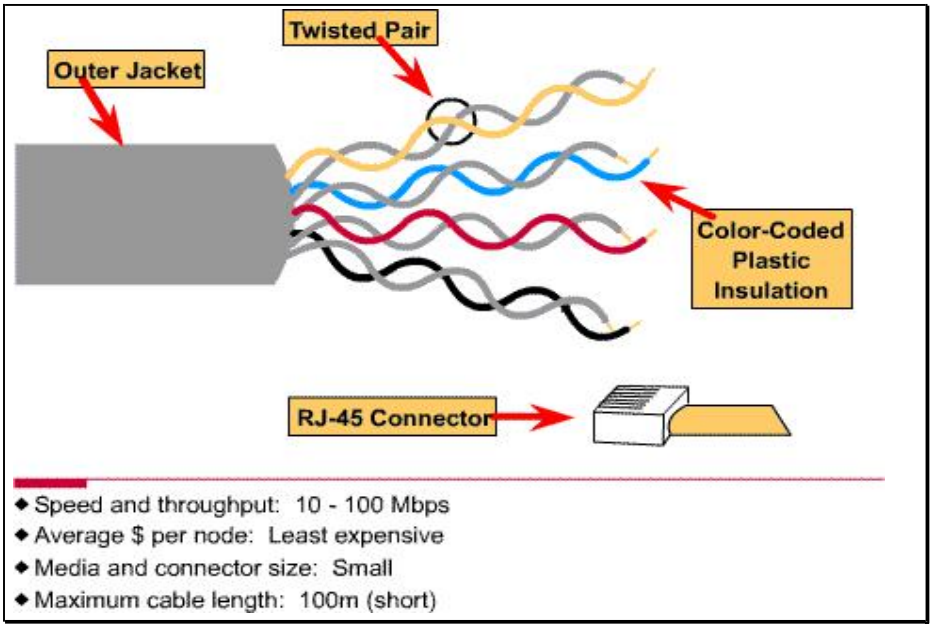
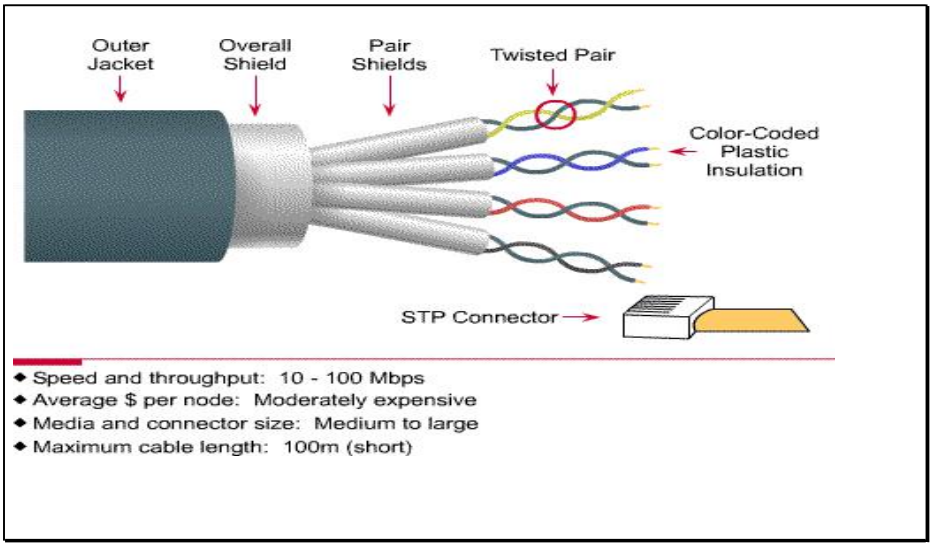


Figure 2: Shielded Twisted-Pair Cable



Twisted-pair is a copper wire-based cable that may be either shielded or unshielded.

Unshielded Twisted-Pair Cable [1]

Unshielded twisted-pair (UTP) cable is a four-pair wire medium—composed of pairs of wires—used in a variety of networks. Each of the eight individual copper wires in the UTP cable is covered by insulating material. In addition, each pair of wires is twisted around each other. This type of cable relies solely on the cancellation effect, produced by the twisted-wire pairs, to limit signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. Like STP cable, UTP cable must follow precisespecifications as to how many twists or braids are permitted per foot of cable. When used as a networking medium, UTP cable has four pairs of either 22- or 24-gauge copper wire. UTP used as a networking medium has an impedance of 100 ohms, differentiating it from other types of twisted-pair wiring such as that used for telephone wiring. Because UTP has an external diameter of approximately 0.43 cm, its small size can be advantageous during installation. Because UTP can be used with most of the major networking

architectures, it continues to grow in popularity.

UTP does not require the fixed spacing between connections that is necessary with coaxial-type connections. The types of UTP cabling that are commonly used aredescribed below:

- **Category 1**: Used for telephone communications; not suitable for Transmitting data
- **Category 2**: Capable of transmitting data at speeds up to 4 megabits per second (Mbps)
- **Category 3**: Used in 10BASE-T networks and can transmit data at speeds up to 10 Mbps
- **Category 4**: Used in Token Ring networks and can transmit data at speeds up to16 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])

Shielded Twisted-Pair Cable [2]

Shielded twisted-pair (STP) cable 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. It is usually 150-ohm cable. As specified for use in Ethernet network installations, STP reduces electrical noise, both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI). Token Ring runs on STP.

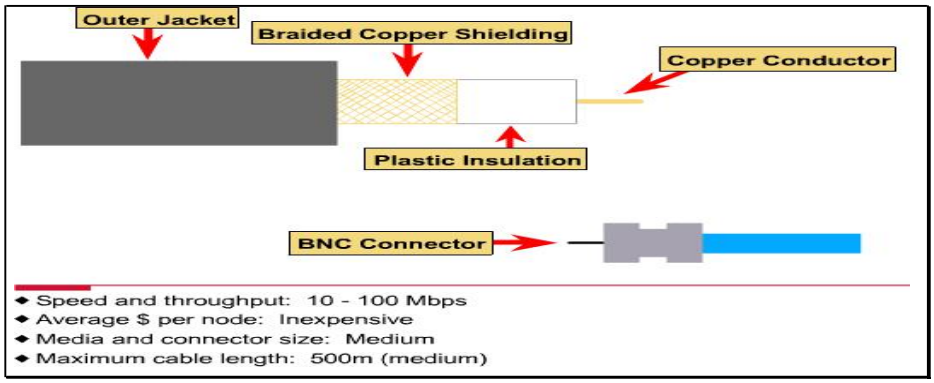
Using UTP and STP:

151

- Speed is usually satisfactory for local-area distances.
- These are the least-expensive media for data communication. UTP is cheaper than STP.
- Because most buildings are already wired with UTP, many transmission

3.1.2 Coaxial Cable

Figure 1: Coaxial Cable



Coaxial cable consists of a hollow outer cylindrical conductor that surrounds a single inner wire made of two conducting elements. One of these elements—located in the center of the cable—is a copper conductor. Surrounding it is a layer of flexible insulation. Over this insulating material is a woven copper braid or metallic foil that acts as the second wire in the circuit, and as a shield for the inner conductor. This second layer, or shield, can help reduce the amount of outside interference. Covering this shield is the cable jacket (see Figure [1]). Coaxial cable supports 10–100

Mbps and is relatively inexpensive, although it is more costly than UTP. Coaxial cable can be cabled over longer distances than twisted-pair cable.
For example,

Ethernet can run approximately 100 meters (m) or 300 feet using twisted pair. Using coaxial cable increases this distance to 500m. 194 For LANs, coaxial cable offers several advantages. It can be run, without as many boosts from repeaters, for longer distances between network nodes than either STP or UTP cable. Repeaters regenerate the signals in a network so that they can cover greater distances. Coaxial cable is less expensive than fiber-optic cable, and the technology is well known. It has been used for many years for all types of data communication.

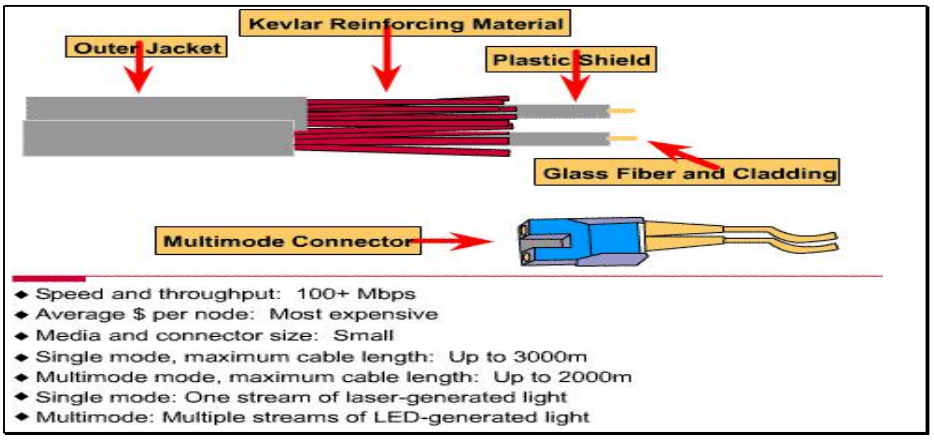
When working with cable, it is important to consider its size. As the thickness, or diameter, of the cable increases, so does the difficulty in working with it. You must remember that cable must be pulled through existing conduits and troughs that are limited in size. Coaxial cable comes in a variety of sizes. The largest diameter was specified for use as Ethernet backbone cable because historically it had greater transmission length and noise rejection characteristics. This type of coaxial cable is frequently referred to as *thicknet*. As its nickname suggests, this type of cable, because of its thickness, can be too rigid to install easily in some situations. The rule of thumb is: "The more difficult the network media is to install, the more expensive it is to install." Coaxial cable is more expensive to install than twisted-pair cable Thicknet cable is almost never used any more except for special-purpose installations.

In the past, coaxial cable with an outside diameter of only 0.35 centimeters (cm) (sometimes referred to as *thinnet*) was used in Ethernet networks. It was especially useful for cable installations that required the cable to make many twists and turns. Because it was easier to install, it was also cheaper to install. Thus it is sometimes referred to as *cheapernet*. However, because the outer copper or metallic braid in coaxial cable comprises half the electrical circuit, special care must be taken to ensure that it is properly grounded. This is done by ensuring that there is a solid electrical connection at both ends of the cable. Frequently, installers fail to do this.

As a result, poor shield connection is one of the biggest sources of connection problems in the installation of coaxial cable. Connection problems result in electrical noise that interferes with signal transmittal on the networking media. It is for this reason that, despite its small diameter, thinnet is no longer commonly used in Ethernet networks.

3.1.3 Fiber-Optic Cable

Figure 1: Fiber-Optic Cable



Fiber-optic cable used for networking consists of two fibers encased in separate sheaths. If viewed in cross section, you would see that each optical fiber is surrounded by layers of protective buffer material, usually a plastic such as Kevlar, and an outer jacket. The outer jacket provides protection for the entire cable. Usually made of plastic, it conforms to appropriate fire and building codes. The purpose of the Kevlar is to furnish additional cushioning and protection for the fragile hair-thin glass fibers (see Figure **[1]**). Wherever buried fiber-optic cables are required by codes, a stainless steel wire is sometimes included for added strength.

The light-guiding parts of an optical fiber are called the core and the cladding. The core is usually very pure glass with a high index of refraction. When the core glass is surrounded by a cladding layer of glass or plastic with a low index of refraction,

light can be trapped in the fiber core. This process is called total internal reflection, and it allows the optical fiber to act like a light pipe, guiding light for tremendous distances, even around bends.

Fiber-optic cable consists of glass fiber surrounded by shielding protection: a plastic shield, Kevlar reinforcing, and an outer jacket. Fiber-optic cable is the most expensive of the three types discussed in this section, but it supports 100+ Mbps line speeds.

There are two types of fiber cable:

- **Single mode**: Single-mode fiber cable allows only one mode (or wavelength) of light to propagate through the fiber; it is capable of higher bandwidth and greater distances than multimode; it is often used for campus backbones; it uses lasers as the light-generating method. Single-mode cable is much more expensive than multimode cable. Its maximum cable length is60+ kilometers (km).

- **Multimode**: Multimode fiber cable allows multiple modes of light to propagate through the fiber; it is often used for workgroup applications; it uses light-emitting diodes (LEDs) as a light-generating device. Its maximum cable length is 2 km.

The characteristics of the different transport media have a significant impact on the speed of data transfer.

Fiber-optic cable is a networking medium capable of conducting modulated light transmissions. Compared to other networking media, it is more expensive; however, it is not susceptible to electromagnetic interference and is capable of higher data rates than any of the other types of networking media discussed here. Fiber-optic cable does not carry electrical impulses, as other forms of networking media that employ copper wire do. Instead, signals that represent bits are converted into beams of light.

Note: Even though light is an electromagnetic wave, light in fibers is not considered wireless because the electromagnetic waves are guided in the optical fiber. The term wireless is reserved for radiated, or unguided, electromagnetic waves.

3.4 Wireless Communication

Figure 1: Wireless Network

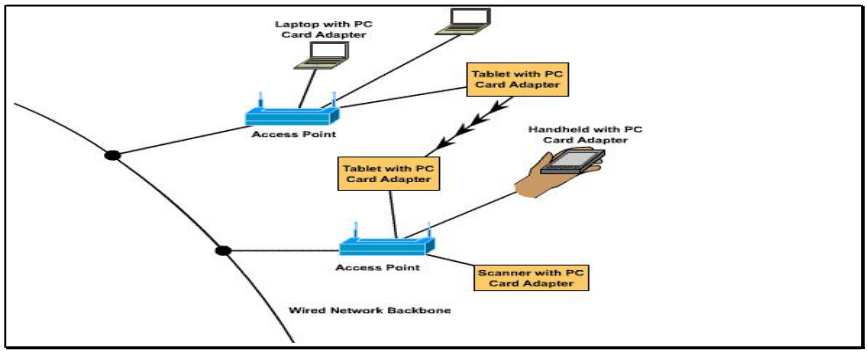
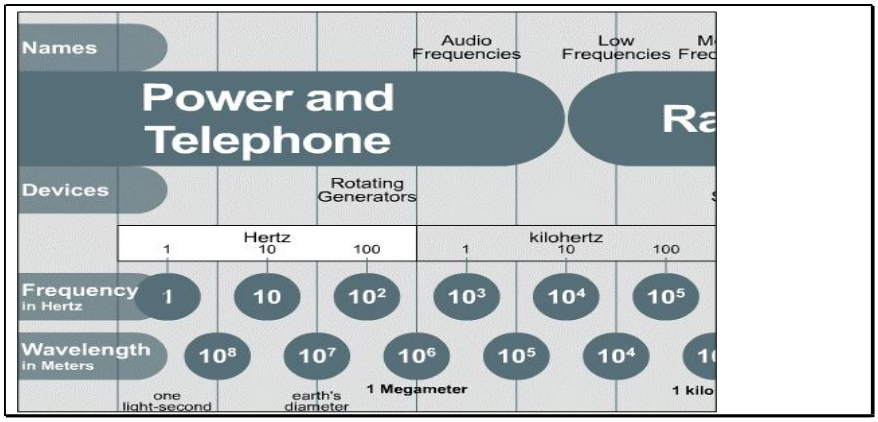


Figure 2: Electromagnetic Spectrum



Wireless uses radio frequencies (RF) or infrared (IR) waves to transmit data between devices on a LAN. Wireless signals are electromagnetic waves, which can travel through the vacuum of outer space and through media such as air. Therefore, no physical medium is necessary for wireless signals, making them a very versatile way to build a network. A key component is the wireless hub, or access point, for signal distribution (see Figure **[1]**).

Wireless signals are electromagnetic waves that can travel through the vacuum of outer space and through media such as air. Therefore, no physical medium is necessary for wireless signals, making them a very versatile way to build a network. They use portions of radio frequency spectrum to transmit voice, video, and data. Wireless frequencies range from 3 kilohertz (kHz) to 300 Gigahertz (GHz). The data-transmission rates range from 9 kbps to 11 Mbps. 325 Figure **[2]** illustrates one of the most important charts in all of science and technology, the Electromagnetic Spectrum chart.

The primary difference between the different electromagnetic waves is their frequency. Low-frequency electromagnetic waves have a long wavelength (the distance from one peak to the next on the sine wave), whereas high-frequency electromagnetic waves have a short wavelength.

A common application of wireless data communication is for mobile use. Some examples of mobile use include:

- People in cars or airplanes
- Satellites
- Remote space probes
- Space shuttles and space stations
- Anyone/anything/anywhere/anytime that requires network data
- Communications, without having to rely on copper or optical fiber tethers

Another common application of wireless data communication is wireless LANs (WLANs), which are built in accordance with the IEEE 802.11 standards. WLANs typically use radio waves (for example, 902 megahertz [MHz]), microwaves (for example, 2.4 GHz), and infrared waves (for example, 820 nanometers) for communication. Wireless technologies are a crucial part of the future of networking.

Comparing Media Types

Figure 1: Media Type Comparison

Media Type	Maximum Segment Length	Speed	Cost	Advantages	Disadvantages
UTP	100 meters	10 Mbps – 1 Gbps	Least expensive	Easy to install; widely available and used	Susceptible to interference; can cover only a limited distance
STP	100 meters	10 Mbps – 100 Mbps	More expensive than UTP	Reduced crosstalk; more resistant to EMI than thinnet or UTP	Difficult to work with
Coaxial	500 meters (thicknet) 185 meters (thinnet)	10 Mbps – 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); damage to cable can bring down entire network
Fiber-Optic	3 kilometers and further (single mode) 2 kilometers and further (multimode)	100 Mbps–100 Gbps (single mode) 100 Mbps–9.92 Gbps (multimode)	Expensive	Cannot be tapped, so security is better; can be used over great distances; not susceptible to EMI; higher data rate than coaxial and twisted-pair	Difficult to terminate
Wireless	50–global	1–10 Mbps	Expensive	Does not require installation of media	Susceptible to atmospheric conditions

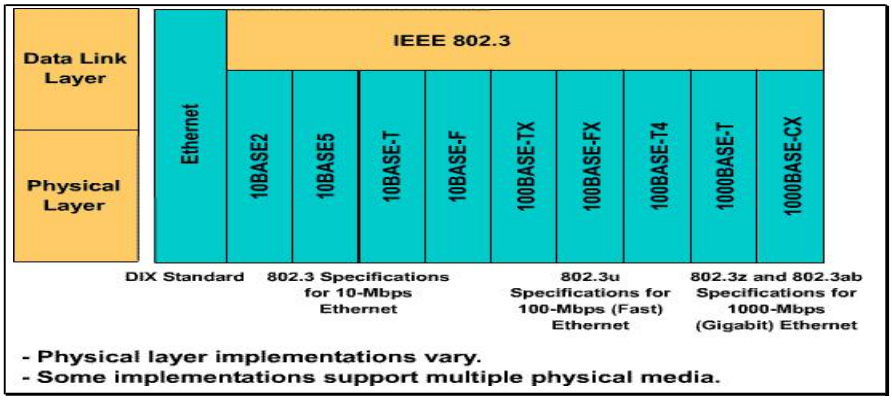
Presented within Figure [1] are comparisons of the features of the common network media. It provides an overview of various media to use as a reference.

Media is possibly the single most important long-term investment you will make in your network. Your choice of media type will affect the type of network interface cards (NICs) installed, the speed of the network, and the ability of the network to meet future needs.

3.2 CABLING LAN

3.2.1 LAN Physical Layer

Figure 1: LAN Physical Layer Implementation



Ethernet is the most widely used local-area network (LAN) technology. Ethernet was first implemented by a group call DIX (Digital, Intel, and Xerox). They created and implemented the first Ethernet LAN specification, which was used as the basis for the Institute of Electrical and Electronic Engineers (IEEE) 802.3 specification released in 1980. Later, the IEEE extended the 802.3 committee to two new committees known as 802.3u (Fast Ethernet), 802.3z (Gigabit Ethernet over fiber) and 802.3ab (Gigabit Ethernet over UTP).

The cabling aspect of the LAN exists at Layer 1 of the Open System Interconnection (OSI) reference model. Many topologies support LANs and many different physical media. Figure [1] shows a subset of physical layer implementations that can be deployed to support Ethernet.

3.2.2 Ethernet in the Campus

Figure 1: Ethernet Connectivity Recommendations

Ethernet 10BASE-T Position	Fast Ethernet Position	Gigabit Ethernet Position
Provide connectivity betwwent he end-user device and the user-level switch.	Given high-performacen PC worstations 100-Mbps access to the server.	-
-	Provides connectivity between end-user and workgroups. Provides connectivity from the workgroup to backbone. Provides connectivity from the server block to the backbone layer.	-
-	Provides inter-switch connectivity.	Provide backbone and inter-switch connectivity.

Given the variety of Ethernet speeds that can be deployed in the campus, you need to determine when, if, and where you want to upgrade to one or more of the Fast Ethernet implementations. Note that today you can run 10- or 100-Mbps Ethernet anywhere in the network, provided you have the correct hardware and cabling infrastructure.

As noted in Figure [1], 10-Mpbs Ethernet is typically implemented at the end-user to connect to desktops, and faster technologies are used to interconnect network devices, such as routers and switches.

In today's installations, although customers are considering putting Gigabit Ethernet from backbone to the end-user, costs for cabling and adapters can make this prohibitive. However, before making this decision, you must determine your network requirements. For example, if you are using a new generation of multimedia, imaging, and database products, these can easily overwhelm a network running at traditional Ethernet speeds of 10 Mbps.

In general, Ethernet technologies can be used in a campus network in several different ways:

- 10-Mbps Ethernet can be used at the user-level to provide good performance. 100-Mbps Fast Ethernet can be used for high-bandwidth-consuming clients or servers.
- Fast Ethernet is used as the link between the user-level and network devices, supporting the aggregate traffic from each Ethernet segment on the access link.
- Many client/server networks suffer from too many clients trying to access the same server, creating a bottleneck where the server attaches to the LAN. To enhance client/server performance across the campus network, enterprise servers are connected by Fast Ethernet links to ensure the

avoidance of bottlenecks at the server. Fast Ethernet, in combination with switched Ethernet, creates an effective solution for avoiding slow networks.

- Fast Ethernet links can also be used to provide the connection between the distribution layer and the core. Because the campus network model supports dual links between each distribution layer router and core switch, the aggregate traffic from multiple-access switches can be load-balanced across the links.
- Fast Ethernet (or Gigabit Ethernet) can be used between switches and backbone. The fastest media affordable should be implemented between backbone switches.

3.2.3 Ethernet Media and Connector Requirements

Figure 1: Comparing Ethernet Media Requirement

	10BASE-2	10BASE-5	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Media	50-ohm coaxial (thinnet)	50-ohm coax (thick)	EIA/TIA Category 3, 4, 5 UTP 2 pair	EIA/TIA Category 5 UTP 2 pair	62.5/125 micro multimode fiber	STP	EIA/TIA Category 5 UTP 4 pair	62.5/50 micro multimode fiber	9 micron single-mode fiber
Maximum Segment Length	185 meters	500 meters	100 meters	100 meters	400 meters	25 meters	100 meters	260 meters	3–10 km
Topology	Bus	Bus	Star	Star	Point to Point	–	–	–	–
Connector	Attachment unit interface (AUI)	AUI	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Duplex media interface connector (MIC) ST	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	–	–

In addition to network need, before selecting an Ethernet implementation you must consider the media and connector requirements for each implementation.

The cables and connector specifications used to support Ethernet implementations are derived from the Electronic Industries Association and the newer Telecommunications Industry Association (EIA/TIA) standards body. The categories of the cabling defined for Ethernet are derived from the EIA/TIA-568 (SP-2840) Commercial Building Telecommunications Wiring Standards. The EIA/TIA standard specifies an RJ-45 connector for UTP cable. The letters “RJ” stand for “registered jack,” and the number “45” refers to a specific wiring sequence.

Figure [1] compares the cable and connector specifications for the most popular Ethernet implementations. The important difference to note is the media used for10-Mbps Ethernet and 100-Mbps Ethernet. In today’s networks where you will see a mix of 10- and 100-Mbps needs, you must be aware of the need to change over to UTP Category 5 to support Fast Ethernet.

3.2.4 Connection Media

Figure 1: Differentiating between Connections

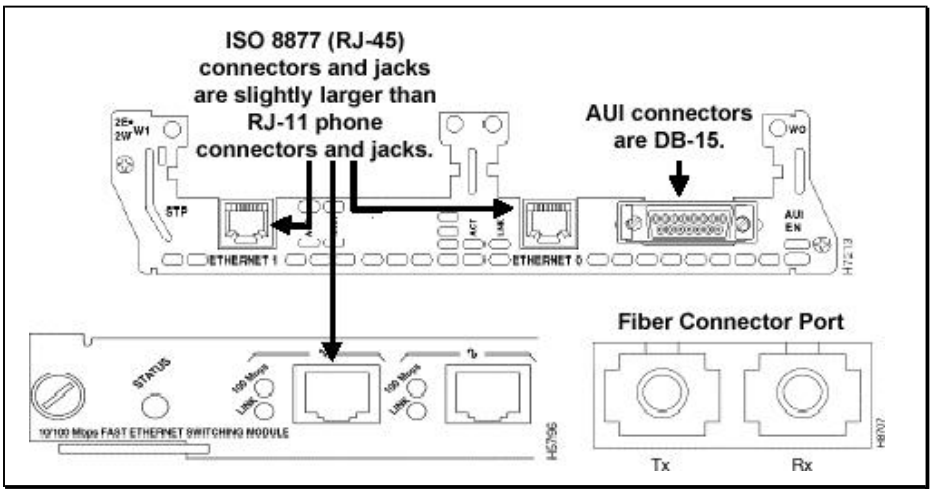
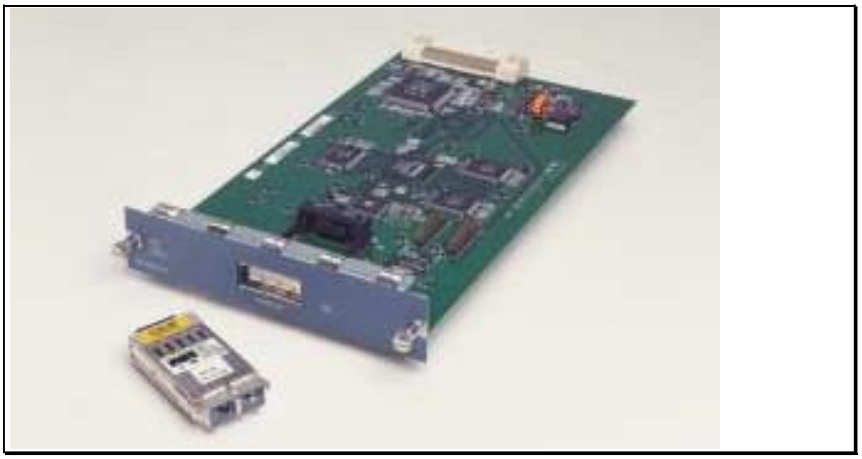


Figure 2: Cisco1000BASE-T GBIC

Figure 3: Cisco WS-X2931 Gigabit Ethernet Module with GBIC out



RJ-45

Figure [1] illustrates the different connection types used by each physical layer implementation. Of the three examples shown, the RJ-45 connector and jack are the most prevalent. RJ-45 connectors are discussed in more detail in the next section.

AUI

In some case, the type of the connector on a network interface card (NIC) does not match the type of the media needed to connect to. As shown in Figure [1], there is an interface for Attachment Unit Interface (AUI) connector. The AUI is the 15-pin physical connector interface between a computer's NIC and an Ethernet cable. On 10BASE-5 ("thicknet") Ethernet, a short cable is used to connect the AUI on the computer with a transceiver on the main cable. In 10BASE-2 or "thinnet" Ethernet networks, the NIC connects directly to the Ethernet coaxial cable at the back of the computer.

GBIC

Gigabit interface converter (GBIC) is a transceiver that converts serial electric currents to optical signals, and optical signals to digital electric currents. Typically, the GBIC is used to interface an Ethernet and fiber optic systems, such as Fibre Channel and Gigabit Ethernet.

Figure [2] shows a photo of Cisco 1000BASE-T GBIC and Figure [3] shows a Cisco WS-X2931 Gigabit Ethernet Module with BGIC out.

3.2.5 UTP Implementation

Figure 1: RJ-45 Connector

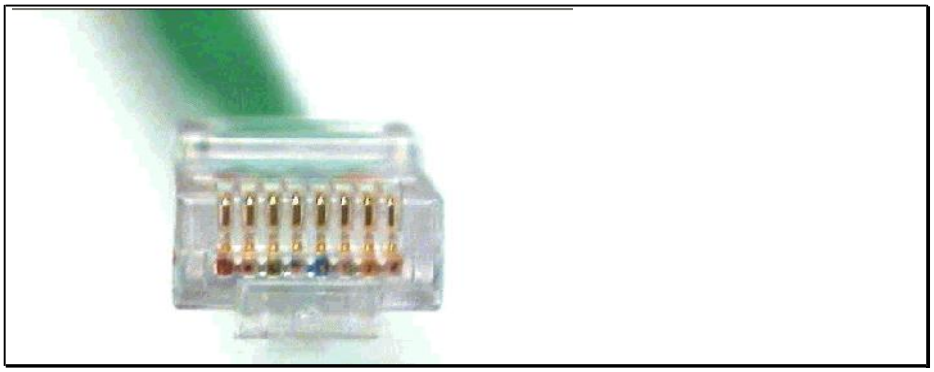


Figure 2: RJ-45 Jack

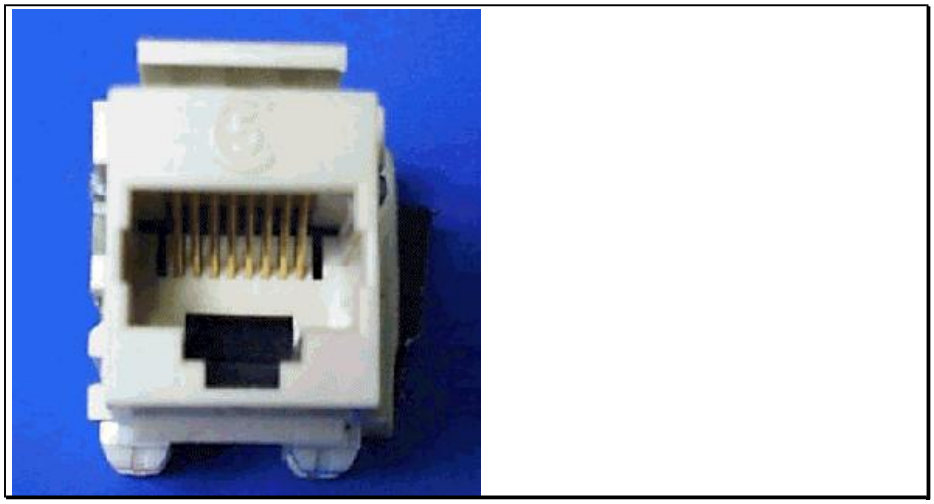


Figure 2: RJ-45 Jack

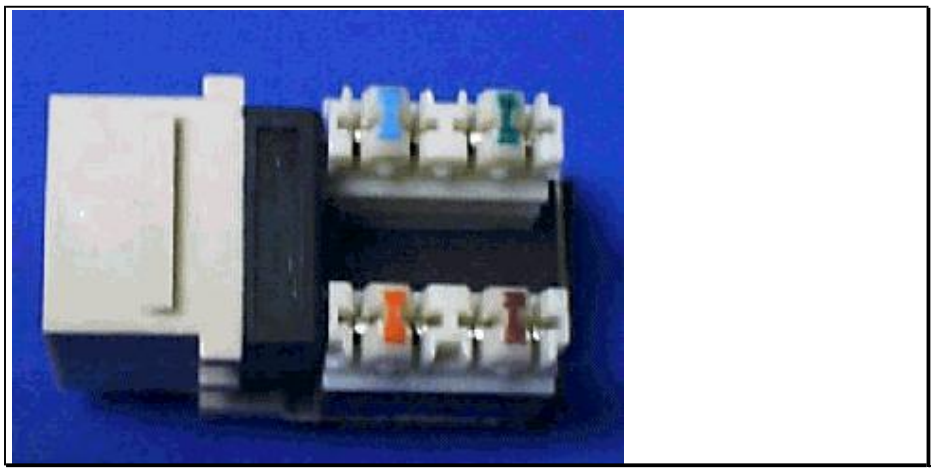


Figure 4: RJ-45 Connector

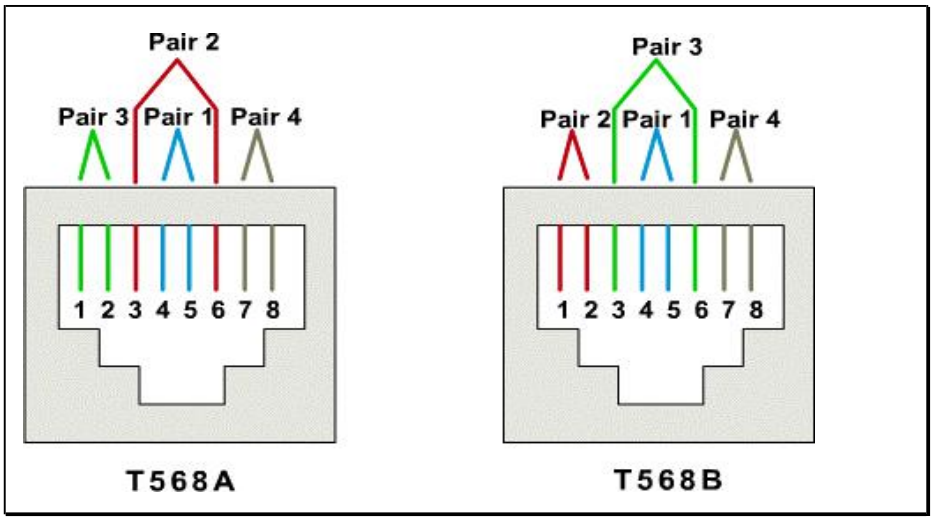


Figure 5: UTP Implementation – Straight-Through

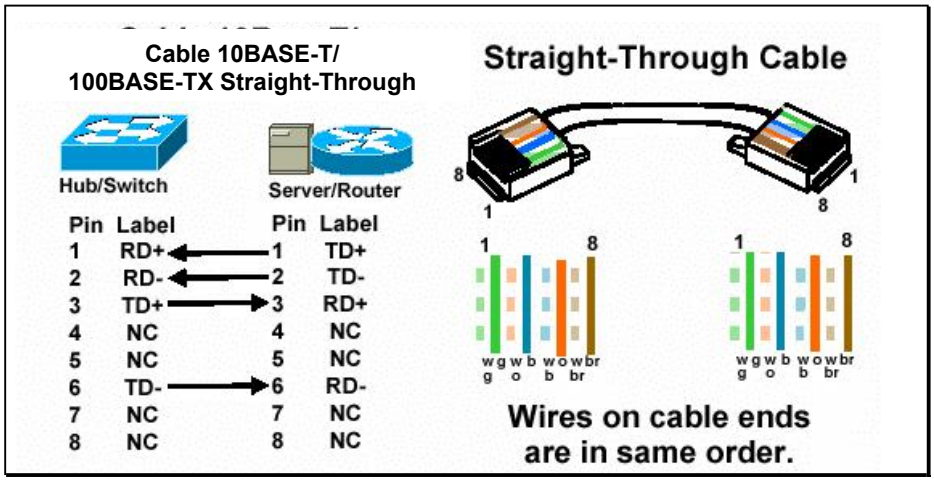


Figure 6: UTP Implementation – Crossover

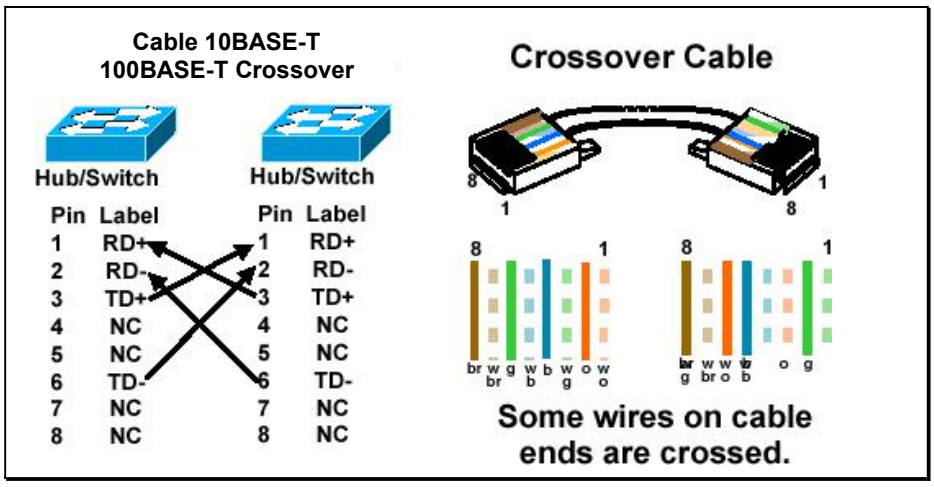


Figure 7: UTP Implementation – Straight-Through vs. Crossover

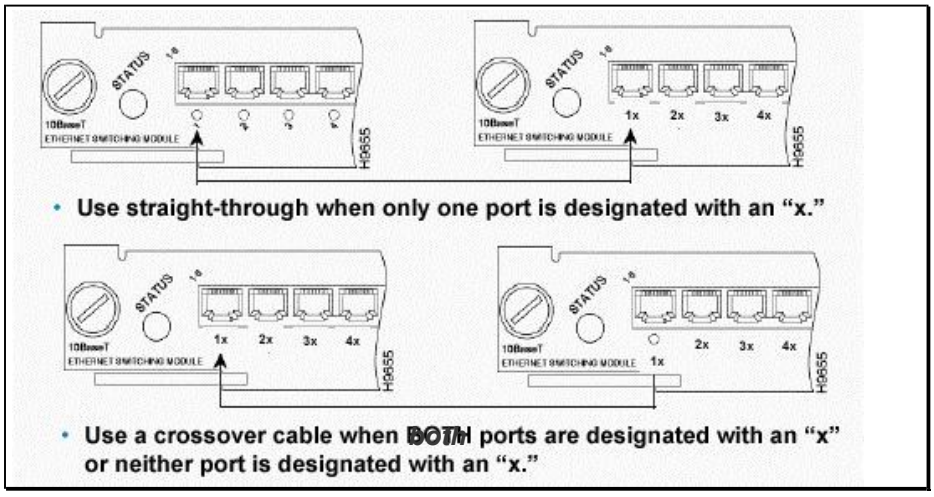
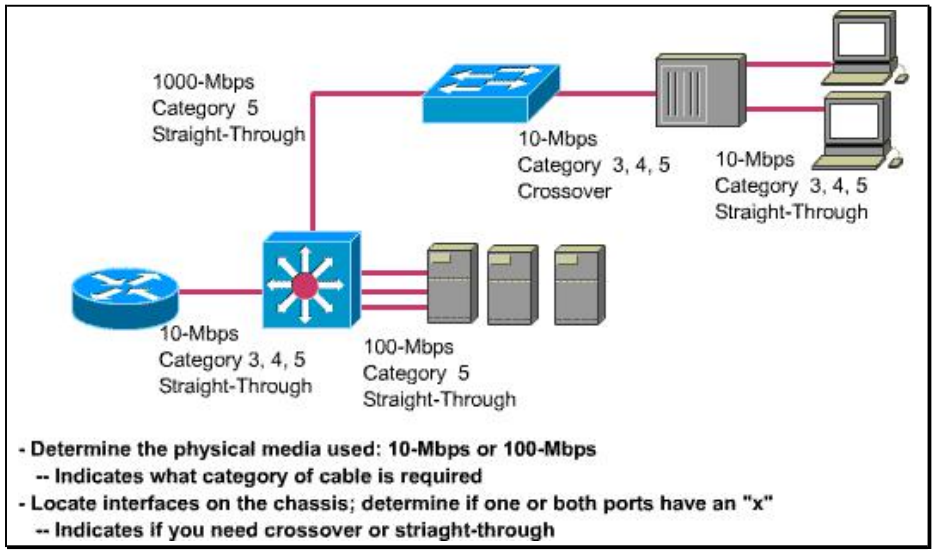


Figure 8: Cabling the Campus



If you look at the RJ-45 transparent end connector, you can see eight colored wires.These wires are twisted into four pairs. Four of the wires (two pairs) carry the voltage and are considered *tip* (T1 through T4) and the other four wires are grounded and are called *ring* (R1 through R4). Tip and ring are terms that originated in the early days of the telephone. Today, these terms refer to the positive and the negative wire in a pair. The wires in the first pair in a cable or a connector are designated as T1 and R1, the second pair is T2 and R2, and so on.

The RJ-45 connector is the male component crimped on the end of the cable. As you look at the male connector from the front, the pin locations are numbered 8 on the left down to 1 on the right (see Figure **[1]**). The jack is the female component in a network device, wall or cubicle partition outlet, or patch panel (see Figure **[2]**). As you look at the device port, the corresponding female plug locations are 1 on the left up to 8 on the right (see Figure 612 **[3]**).

In order for electricity to run between the connector and the jack, the order of the wires must follow the EIA/TIA-568-A and 568-B standards, as shown in Figure **[4]**. In addition to identifying the correct EIA/TIA category of cable to use for a connecting device, depending on what standard is being used by the jack on the network device, you will need to determine which of the following to use:

- A straight-through cable
- A crossover cable

The RJ-45 connectors on both ends show all the wires in the same order. If you hold the two RJ-45 ends of a cable side by side in the same orientation, you will see the colored wires (or strips or pins) at each connector end. If the order of the colored wires is the same at each end, then the cable is straight-through (see Figure **[5]**). With crossover, the RJ-45 connectors on both ends show that some of the wires on one side of the cable are crossed to a different pin on the other side of the cable. Specifically for Ethernet, pin 1 at one RJ-45 end should be connected to pin 3 at the other end. Pin 2 at one end should be connected to pin 6 at the other end, as shown in Figure **[6]**.

Figure **[7]** shows the guidelines for what type of cables to use when interconnecting Cisco devices. In addition to verifying the category specification on the cable, you must determine when to use a straight-through or crossover cable.

Use straight-through cables for the following cabling:

- Switch to router
- Switch to PC or server
- Hub to PC or server

Use crossover cables for the following cabling:

- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- PC to PC
- Router to PC

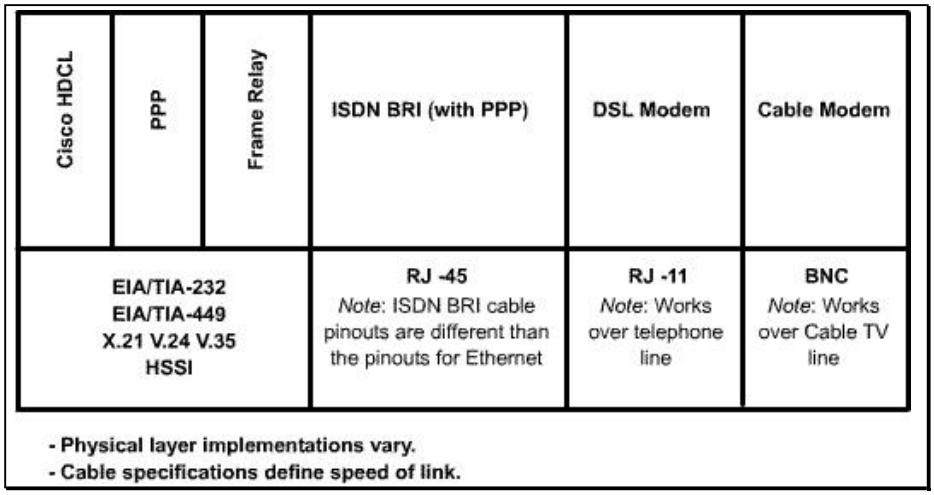
Cabling the campus

Figure **[8]** illustrates how a variety of cable types may be required in a given network. Note that the category of UTP required will be based on the type of Ethernet you choose to implement.

3.3 Cabling the WAN

3.3.1 WAN Physical Layer

Figure 1: WAN Physical Layer Implementations



Many physical implementations carry traffic across the WAN. Needs vary, depending on the distance of the equipment from the services, the speed, and the actual service itself. Figure [1] lists a subset of physical implementations that support some of the more prominent WAN solutions today.

Serial connections are used to support WAN services such as dedicated leased lines that run the Point-to-Point Protocol (PPP) or Frame Relay. The speed of these connections ranges from 2400 bps to T1 (1.544 Mbps).

Other WAN services, such as Integrated Services Digital Network (ISDN), offer dial-on-demand connections or dial backup services. An ISDN BRI is composed of two 64-Kbps bearer channels (B channels) for data, and one delta channel (D channel) at 16 Kbps used for signaling and other link-management tasks. The D channel is used for signaling and other link management tasks. PPP is typically used to carry data over the B channels.

With the increasing demands for residential broadband (high speed) services,Digital Subscriber Line (DSL) and Cable modem connections are becoming more popular. For example, typical residential DSL service can offer a speed up to 1.5 Mbps, which works over the existing telephone line. Cable services, which work over the existing coax Cable TV line, also offer high-speed connectivity matching that or surpassing the DSL speed. DSL and Cable modem will be covered in more detail in a later module.

3.3.2 WAN Serial Connections

Figure 1: WAN Serial Connection Options

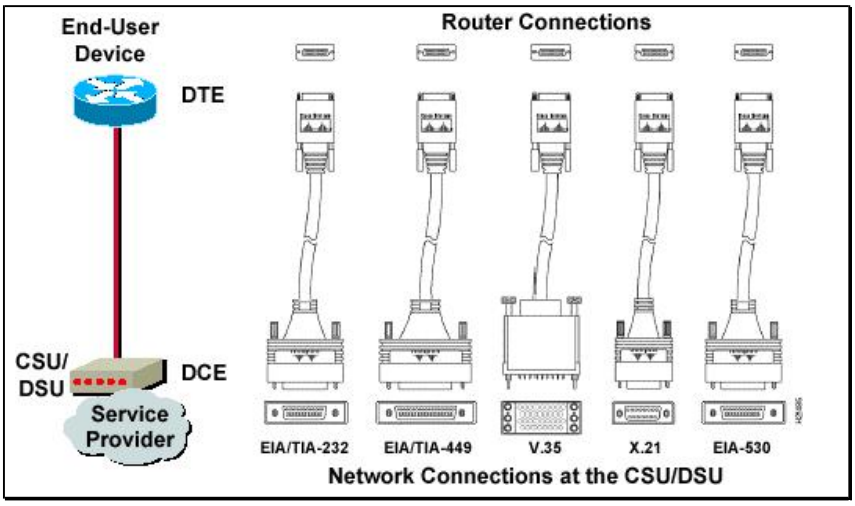


Figure 2: Comparison of Physical Standards

Data bps	Distance (Meters) EIA/TIA-232	Distance (Meters) EIA/TIA-449
2400	60	1250
4800	30	625
9600	15	312
19,200	15	156
38,400	15	78
115,200	3.7	N/A
T1 (1.544 Mbps)	N/A	15

Serial transmission is a method of data transmission in which bits of data are transmitted over a single channel. This one-at-a-time transmission contrasts with parallel data transmission that passes several bits at a time. For long-distance communication, WANs use serial transmission. To carry the energy represented in bits, serial channels use a specific electromagnetic or optical frequency range.

Frequencies, described in terms of their cycles per second (or Hertz), function as a band or spectrum for communication. For example, the signals transmitted over voice-grade telephone lines use up to 3 kHz (kilo, or thousand, Hertz). The size of this frequency range is called *bandwidth*.

Another way to express bandwidth is to specify the amount of data in bits per second that can be carried using two of the physical layer implementations shown in Figure [1]. Figure [2] compares physical standard for WAN serial connection ptions.

Several types of physical connections allow us to connect to serial WAN services Depending on the physical implementation you choose or the physical implementation imposed by your service provider, you will need to select the correct serial cable type to use with the router.

Figure [1] shows the different serial connector options available. Note that serial ports on Cisco routers use a proprietary 60-pin connector. The type of connector you have on the other end of the cable is dependent on your service provider or end-device requirements.

3.3.3 Routers and Serial Connections

Figure 1: Serial Implementation of DTE and DCE

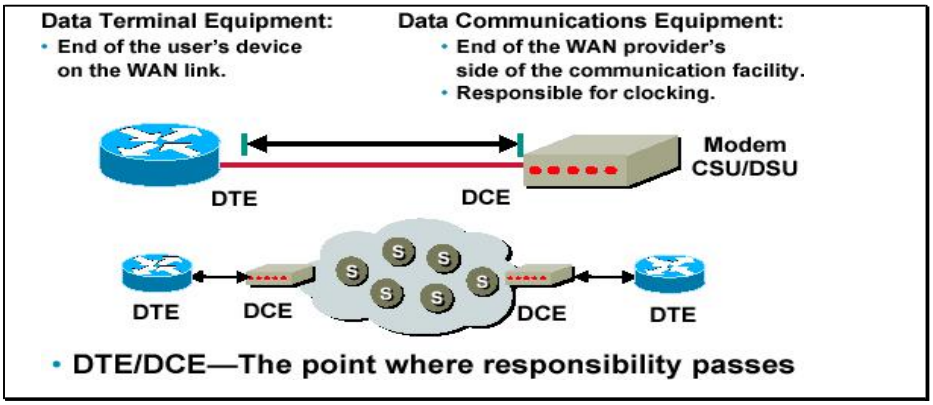


Figure 2: Fixed Interfaces

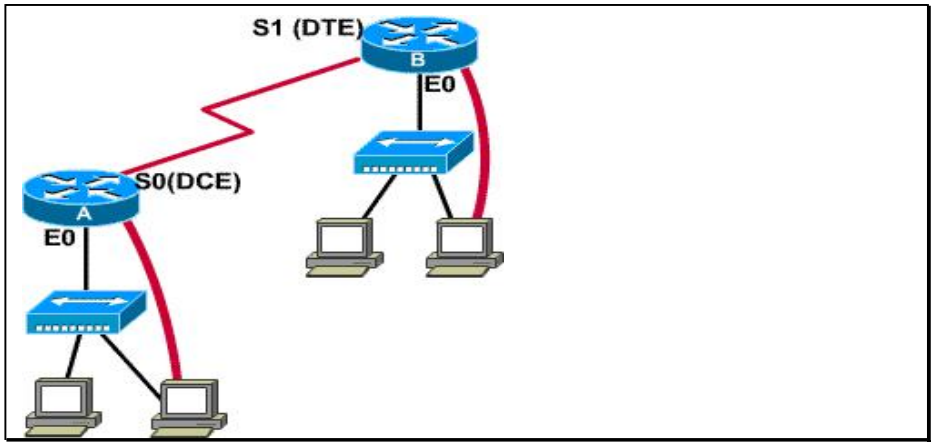
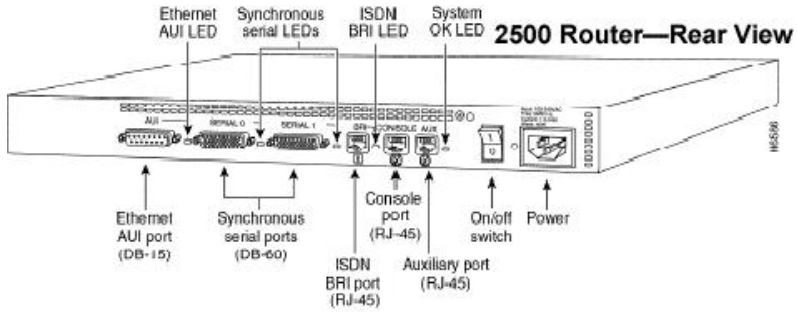
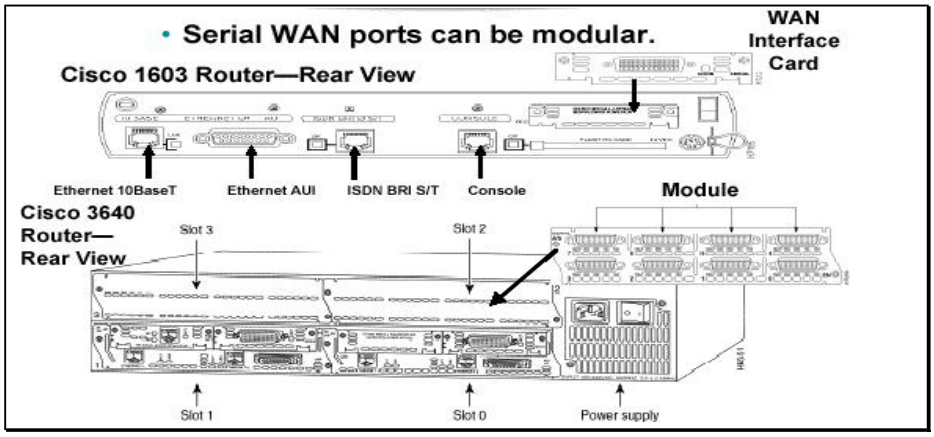


Figure 3: Fixed Interfaces



- **Serial WAN ports can be fixed.**

Figure 4: Modular Serial-Port Interfaces



In addition to determining the cable type, you will need to determine if you need data terminal equipment (DTE) or data circuit-terminating equipment (DCE) connectors for your equipment. The DTE is the endpoint of the user's device on the WAN link. The DCE is typically the point where responsibility for delivering data passes into the hands of the service provider.

As shown in Figure **[1]**, if you are connecting directly to a service provider or to a device (like a CSU/DSU) that will perform signal clocking, then the router is a DTE and needs a DTE serial cable. This is typically the case for routers.

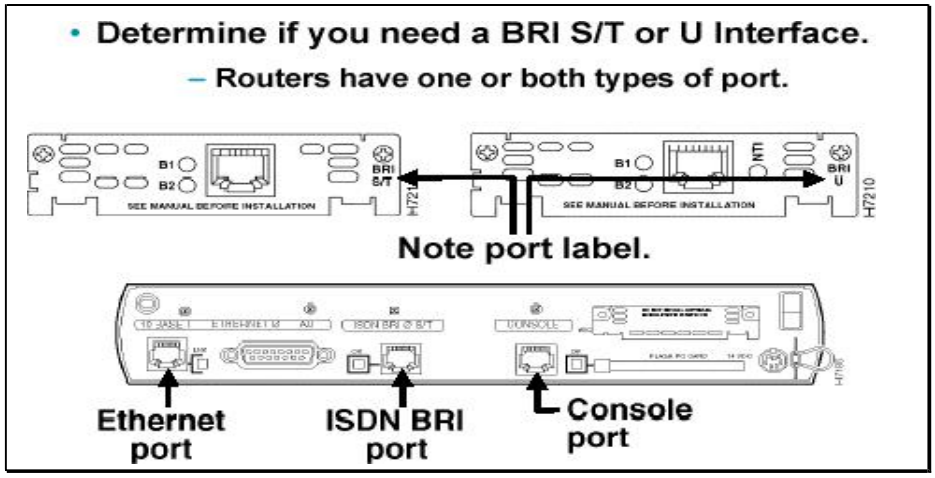
There are cases, however, where the router will need to be the DCE. For example, if you are performing a back-to-back router scenario in a test environment, one of the routers will be a DTE, and the other will be a DCE (see Figure **[2]**).

When cabling routers for serial connectivity, the routers will have either fixed or modular ports. The type of port being used will affect the syntax you use later to configure each interface.

Figure [3] shows an example of a router with fixed serial ports (interfaces). Each port is given a label of port type and port number, for example "serial 0." To configure a fixed interface, you specify the interface using this convention.
Figure [4] shows examples of routers with modular serial ports. Usually each port is given a label of port type, slot (the location of the module), and a port number. To configure a port on a modular card, you will be asked to specify the interface using the convention "*port type slot number/port number*," for example, "serial 1/0" where the type of the interface is a serial interface, the slot number where the serial interface module is installed in is slot 1, and the specific port we are referencing on that serial interface module is port 0.

3.3.4 Routers and ISDN BRI Connections

Figure 1: Cabling Routers for ISDN Connections



With ISDN BRI, there are two types of interfaces that you can use: BRI S/T and BRI U. To determine which interface type you need, you must determine whether you or the service provider will provide a Network Termination 1 (NT1) device.

An NT1 device is an intermediate device between the router and the service provider's ISDN switch (cloud) that is used to connect four-wire subscriber wiring to the conventional two-wire local loop. In North America, the customer typically provides the NT1, whereas in the rest of the world, the service provider provides the NT1 device.

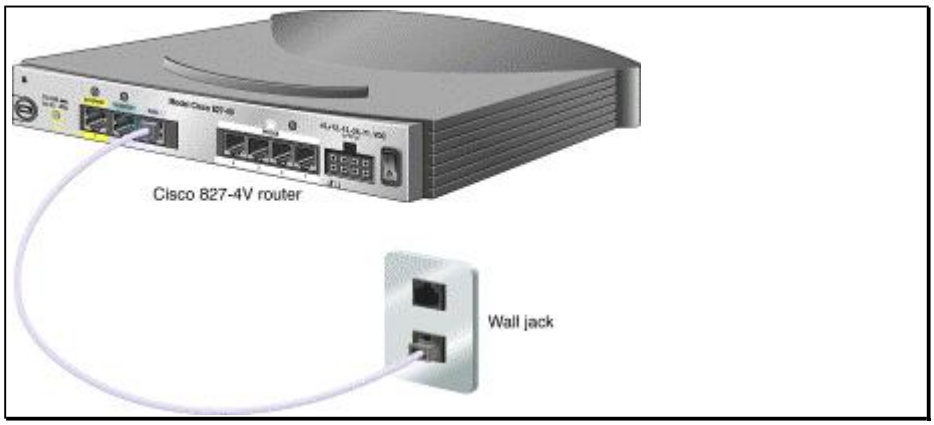
If you need to provide the NT1 device, you may use an ISDN BRI with a U interface; a U interface has an NT1 built in. If you are using an external NT1 device or your service provider uses an NT1 device, then the router needs an ISDN BRI S/T interface. Because routers can have multiple ISDN interface types, you need to determine which interface you need when you purchase the router. You can determine which type of ISDN connector the router has by looking at the port label. Figure [1] shows the different port types for the ISDN interface.

To interconnect the ISDN BRI port to the service-provider device, you will use a 869 UTP Category 5 straight-through cable.

> **Caution**: It is important to insert a cable running from an ISDN BRI port only to an ISDN jack or an ISDN switch. ISDN BRI uses voltages that can seriously damage non-ISDN devices.

3.3.5 Routers and DSL Connections

Figure 1: Cisco 827 Router



To connect a DSL to a router, you will need a DSL cable with RJ-11 connector.

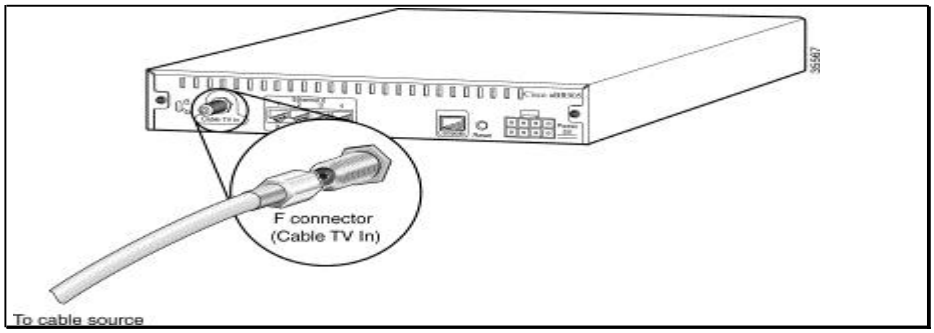
The Cisco 827 ADSL router has one ADSL interface. To connect a ADSL line to the ADSL port on a router, do the following:

1. Connect the ADSL cable to the ADSL port on the router.
2. Connect the other end of the ADSL cable to the external wall jack.

Note: The instructions above are for a straight-through ADSL cable, but they also apply if you are using a crossover cable to connect your ADSL line.

3.3.6 Routers and Cable Connections

Figure 1: Cisco uBR905 Router



Cisco's uBR905 cable access router provides high-speed network access on the cable television system to residential and small office/home office (SOHO) subscribers. It has a coaxial cable (F-connector) interface that can be connected to cable system. Coaxial cable and BNC connector are used to connect a router and cable system.

To connect the Cisco uBR905 cable access router to the cable system, do the following:

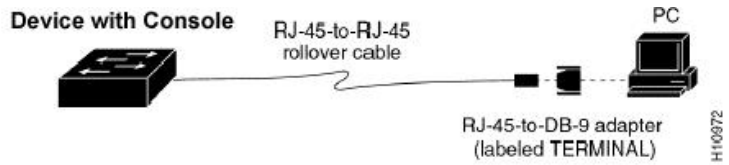
1. Verify that the router is not connected to power.
2. Locate the RF coaxial cable coming from the coaxial cable CATV wall outlet.
3. Install a cable splitter/directional coupler, if needed, to separate signals for TV and computer usage. If necessary, also install a high-pass filter to prevent interference between the TV and computer signals.
4. Connect the coaxial cable to the router's F-connector. Hand-tighten the connector, making sure that it is finger tight; then give it a 1/6 turn with awrench (see Figure **[1]**).

5. Make sure that all other coaxial cable connectors—all intermediate splitters, couplers, or ground blocks—are securely tightened from the distribution tap to the Cisco uBR905 router, following instructions in Step 4.

Caution Do not overtighten the connector because this can break off the connector. Using a torque wrench is not recommended because of the danger of tightening the connector more than the recommended 1/6 turn after it is finger tight.

3.3.7 Setting Up Console Connections

Figure: Setting Up a Console Connection



- **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.**

Note: The AUX port is used to provide out-of-band management via a modem. The AUX port must be configured using the console port before it can be used. The AUX port also uses the settings of 9600 bps, 8 data bits, no parity, and 1 stop bit. The speed can be set up to 38,400 bps.

Error Detection and Correction

1. Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed to a 1 or a 1 to a 0. The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

2. Redundancy

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits. The concept of including extra information in the transmission for error detection is a good one. But instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit. This technique is called redundancy because the extra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.

Figure 8 shows the process of using redundant bits to check the accuracy of a data unit. Once the data stream has been generated, it passes through a device that analyses it and adds on an appropriately coded redundancy check. The data unit, now enlarged by several hits, travels over the link to the receiver. The receiver puts the entire stream through a checking function. If the received hit stream passes the checking criteria, the data portion of the data unit is accepted and the redundant bits are discarded.

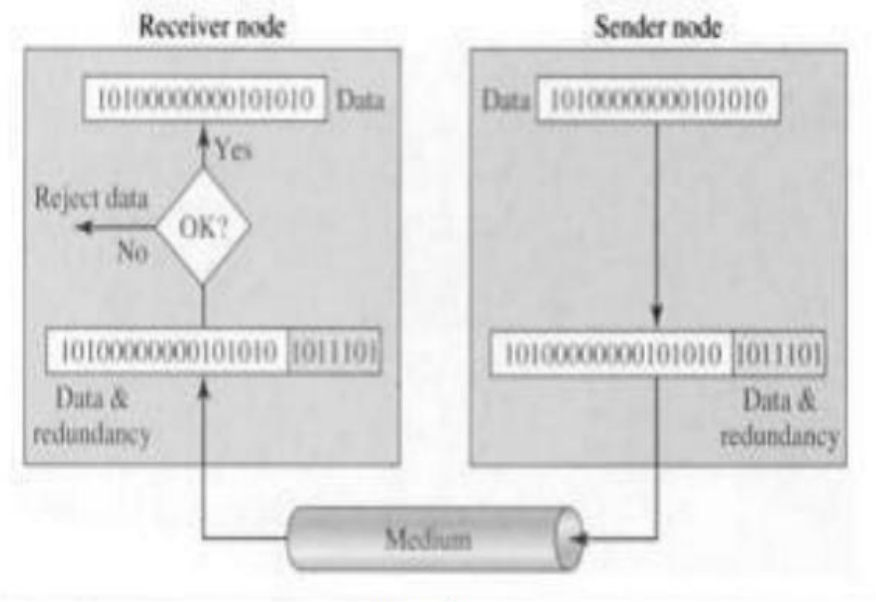


Fig. 8

Three types of redundancy checks are common in data communications: parity check, cyclic redundancy check (CRC. and checksum (see Fig. 9).

2.1 Simple Parity Check

In this technique, a redundant bit called a parity bit is added to every data unit so that the total number of 1's in the unit (including the parity bit) becomes even (or odd). Figure (10) shows this concept when transmit the binary data unit 1100001.

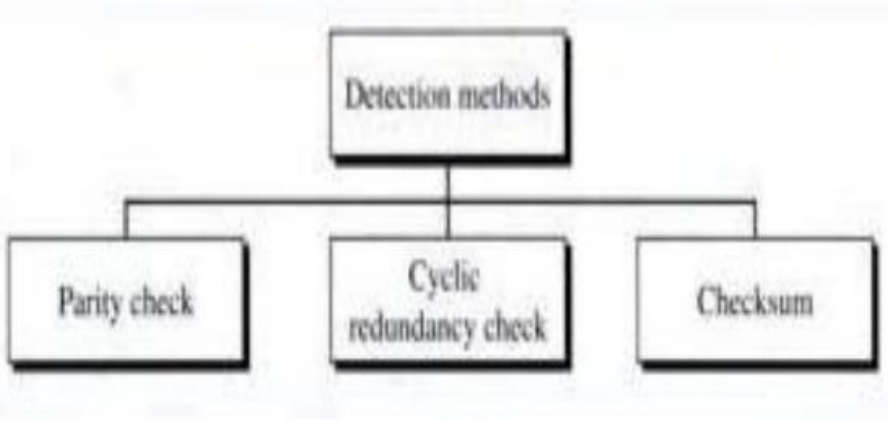


Fig.9

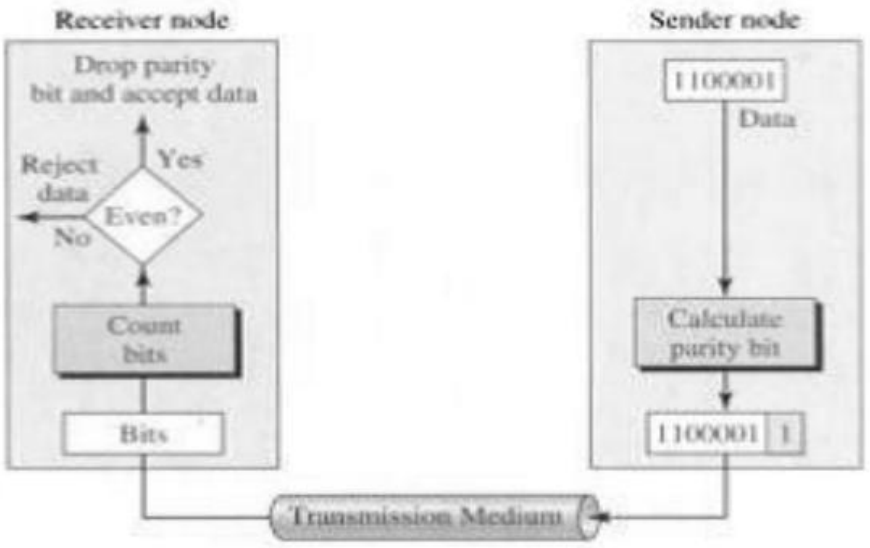
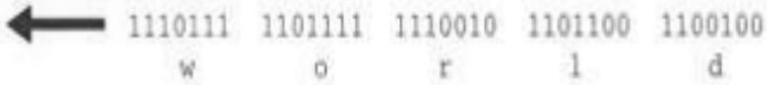


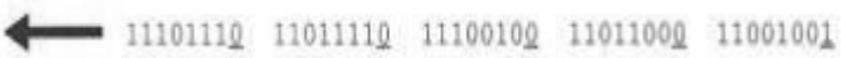
Fig. 10

Example 1

Suppose the sender wants to send the word *world*. In ASCII (see Appendix A), the five characters are coded as

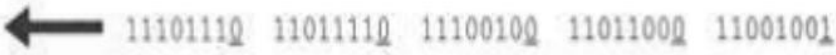


Each of the first four characters has an even number of 1s, so the parity bit is a 0. The last character (d), however, has three 1s (an odd number), so the parity bit is a 1 to make the total number of 1s even. The following shows the actual bits sent (the parity bits are underlined).



Example 2

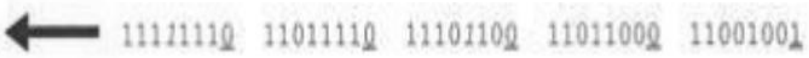
Now suppose the word *world* in Example 1 is received by the receiver without being corrupted in transmission.



The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4, 4). The data are accepted.

Example 3

Now suppose the word *world* in Example 1 is corrupted during transmission.



The receiver counts the 1s in each character and comes up with even and odd numbers (7, 6, 5, 4, 4). The receiver knows that the data are corrupted, discards them, and asks for retransmission.

Performance

Simple parity check can detect all single-bit errors. It can also detect burst errors as long as the total number of bits changed is odd. This method cannot detect errors where the total number of hits changed is even. If any two bits change in transmission, the changes cancel each other and the data unit will pass a parity check even though the data unit is damaged. The same holds true fur any even lumber of errors.

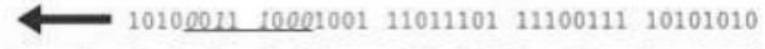
2.2 Two-Dimensional Parity Check

A belter approach is the two dimensional parity checks. In this method, a block of bits is organized in a table (rows and columns). First we calculate the parity bit for each data unit. Then we organize them into a table* For example, as shown in Figure 11. We have four data units shown in four rows and eight columns. We then calculate the parity bit for each column and create a new row of 8 bits; they are the pants bits for the whole block. Note that the first parity bit in the fifth row is calculated based on all first bits: the second parity bit is calculated based on all second bits: and so on. We then attach the 8 parity bits to the original data and send them to the receiver.

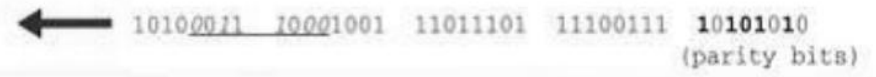
Example 4

Suppose the following block is sent:

However, it is hit by a burst noise of length 8, and some bits are corrupted.



When the receiver checks the parity bits, some of the bits do not follow the even-parity rule and the whole block is discarded (the nonmatching bits are shown in bold).



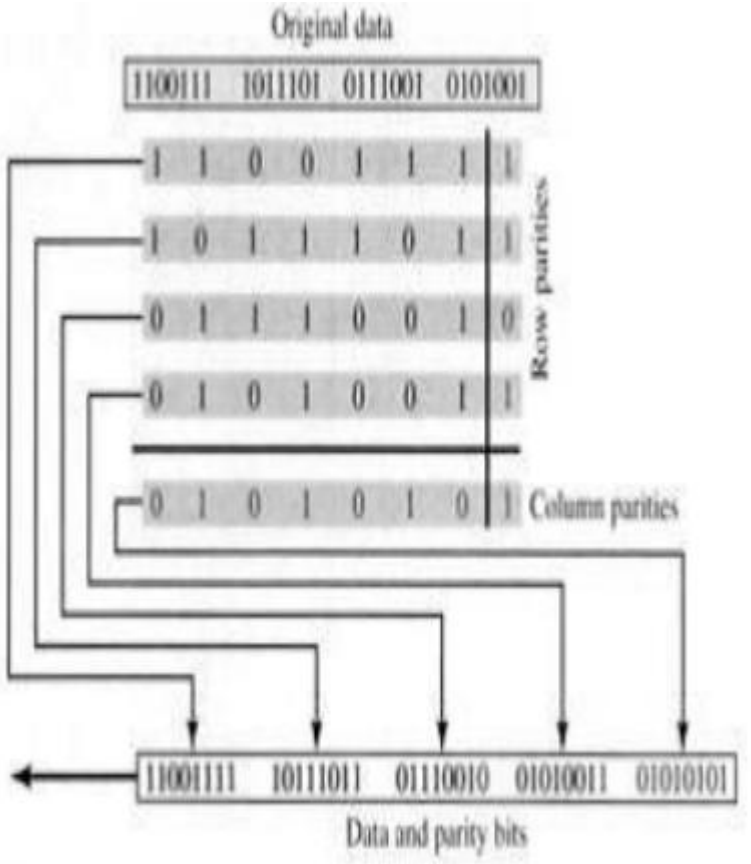


Fig . 11

Performance

Two-dimensional parity check increases the likelihood of detecting burst errors. As we showed in Example 4. a redundancy of n bits can easily detect a burst emir of n bils, A burst error of more than n hits is also detected by this method with a very high probability. There is. however, one pattern of errors that remains elusive. If 2 bits in one data unit arc damaged and two bits **in exactly the same positions** in another data unit are also damaged, the checker will not detect an error. Consider for example, two data units: 11110000 and 11000011. If the first and last bits in each of them are changed, making the units read 01110001 and 01000010 the errors cannot he detected by this method.

2.3 Cyclic Redundancy Check (CRC)

The third and most powerful of the redundancy checking techniques is the cyclic redundancy check (CRC). Unlike the parity check which is based on addition. CRC is based on binary division. In CRC, instead of adding bits to achieve a desired parity, a sequence of redundant bits, called the CRC or the CRC remainder, is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder the data unit is assumed to be intact and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor; the remainder is the CRC. To be valid, a CRC must have two qualities: It must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor.

Both the theory and the application of CRC error detection are straightforward. The only complexity is in deriving the CRC. To clarify this process, we will start with an overview and add complexity as we go. Figure 12 provides an outline of the basic steps.

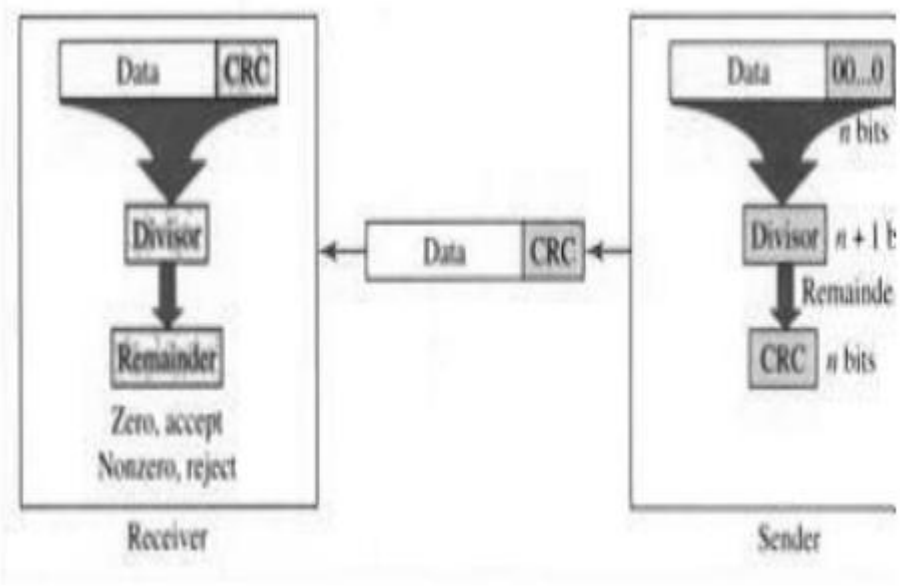


Fig. 12

First, a string of n 0's is appended to the data unit. The number **n is 1** less if-number of bits in the predetermined divisor which is n + 1 bits.

Second, the newly elongated data unit is divided by the divisor, using a p called binary division. The remainder resulting from this division is the CRC.

Third, the CRC of **n** bits derived in step 2 replaces the appended 0's at the data unit. Note that the CRC may consist of all 0's.

The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole siring as a unit and divides it by the same divisor that was used the CRC remainder. If the siring arrives without error, the CRC checker yields a remainder of zero, the data unit passes. If the string has been changed in transit, the division yields zero remainder and the data unit does not pass.

Figure 13 shows how we generate CRC.

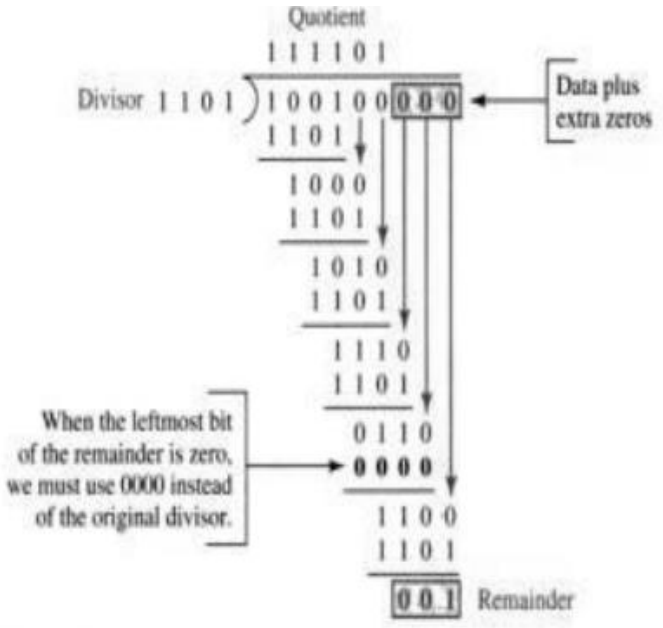


Fig. 13

A CRC checker functions exactly as the generator does. After receiving the data appended with the CRC, it does the same modulo-2 division. If the remainder is all 0's, the CRC is dropped and the data are accepted: otherwise, the received stream of bits is discarded and data are resent. Figure 14 shows the same process of division in the receiver. We assume that there is no error The remainder is therefore all 0's, and the data are accepted.

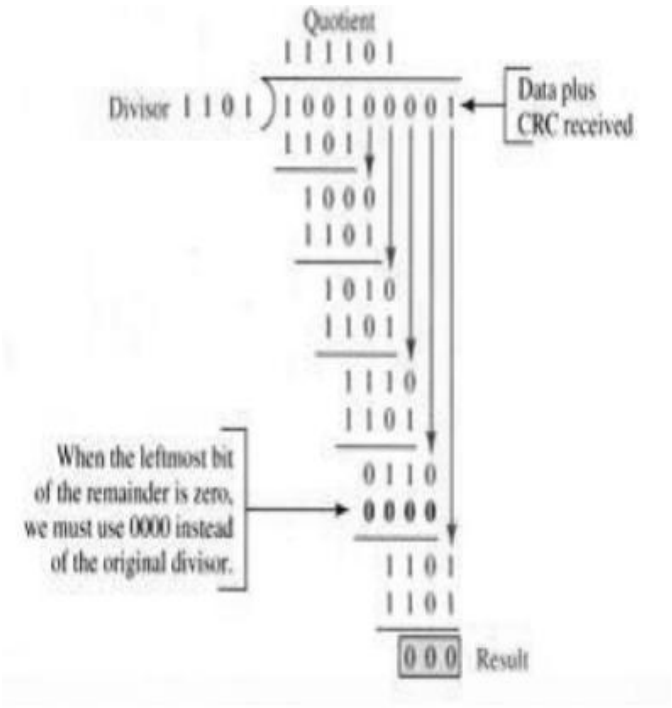


Fig .14

The divisor in the CRC generator is most often represented not as a siring of 1's and 0's, but as an algebraic polynomial (see Fig. 15). The polynomial format is useful for two reasons: It is short, and it can be used to prove the concept mathematically. The relationship of a polynomial to its corresponding binary representation is shown in Figure 16.

$$x^7 + x^5 + x^2 + x + 1$$

Fig.15

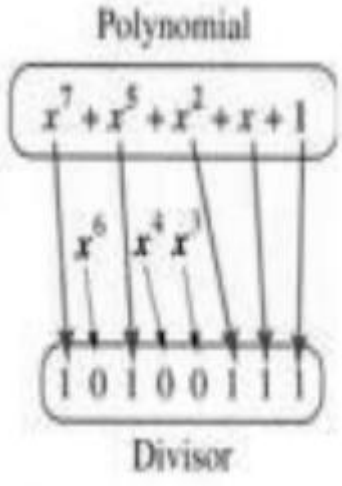


Fig.16

Performance of CRC

CRC is a very effective error detection method. If the divisor is chosen according to the previously mentioned rules,

1.CRC can detect all burst errors that affect an odd number of bits.

2.CRC can detect all burst errors of length less than or equal to the degree of the polynomial

3.CRC can detect, with a very high probability, burst errors of length greater than the degree of the polynomial.

3. Detection versus Correction

The correction of errors is more difficult than the detection. In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors. A single-bit error is the same for us as a burst error. In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message. The number of the errors and the size of the message are important factors. If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities. You can imagine the receiver's difficulty in finding 10 errors in a data unit of 1000 bits.

To calculate the number of redundancy bits **r** required to correct a given number of data bits m. we must find a relationship between **m** and **r**. With **m** bits of data and r bits of redundancy added to them, the length of the resulting code is m + r. If the total number of bits in a transmittable unit is **m + r**. then **r** must be able to indicate at least m+r+1 different states. Of these, one state means no error, and m + r states indicate the location of an error in each of the m + r positions.

So m+r+1 states must be discoverable by **r** bits: and r bits can indicate $\mathbf{2^r}$ different states. Therefore $\mathbf{2^r}$ must be equal to or greater than m + r + 1:

$$2^r => m + r + 1$$

For example, if the value of ***m*** is 7 (as in a 7-bit ASCII code), the smallest ***r*** value that can satisfy this equation is 4:

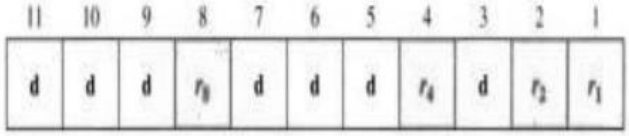
$$2^4 => 7 + 4 + 1$$

Table 1 shows some possible ***m*** values and the corresponding r values.

Number of Data Bits m	*Number of Redundancy Bits* r	*Total Bits* $m+r$
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Hamming Code

Hamming provides a practical solution. The Hamming code can be applied to data units of any length and uses the relationship between data and redundancy bits discussed above. For example, a 7-bit ASCII code requires 4 redundancy bits that can be added 10 the end of the data unit or interspersed with the original data bits. In Figure 17, these bits are placed in positions 1, 2 ,4, and 8 (the positions in an 11-bit sequence that are powers of 2). For clarity in the examples below, we refer to these bits as r_1, r_2, r_4, and r_8.



Fi.17

In the Hamming code, each ***r*** bit is the parity bit for one combination of data bits, is shown below:

r_1: bits 1, 3, 5, 7, 9, 11
r_2: bits 2, 3, 6, 7, 10, 11
r_4: bits 4, 5, 6, 7
r_8: bits 8, 9, 10, 11

Also Figures 18 and 19 explains the calculations of the redundancy bits.

Fig.18

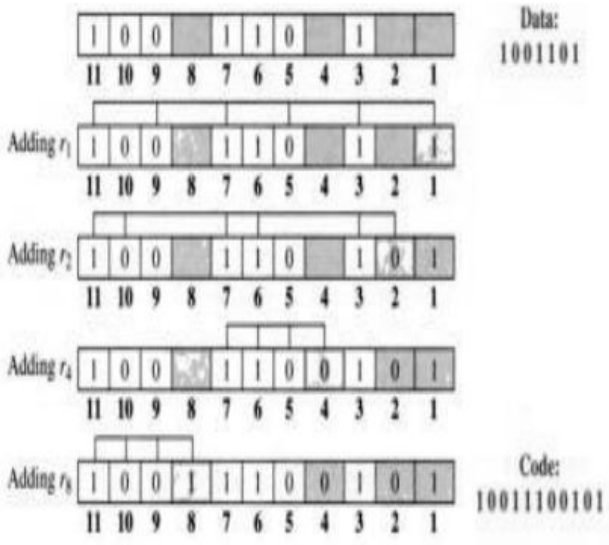


Fig. 19

Now imagine that by the time the above transmission is received, the number 7 bit has been changed from 1 to 0. The receiver takes the transmission and recalculates 4 new parity bits, using the same sets of bits used by the sender plus the relevant parity r bit for each set (sec Fig. 20). Then it assembles the new parity values into a binary number in order of r position(r8 r4, r2 , r1). In our example, this step gives us the binary number 0111 (7 in decimal), which is the precise location of the bit in error.

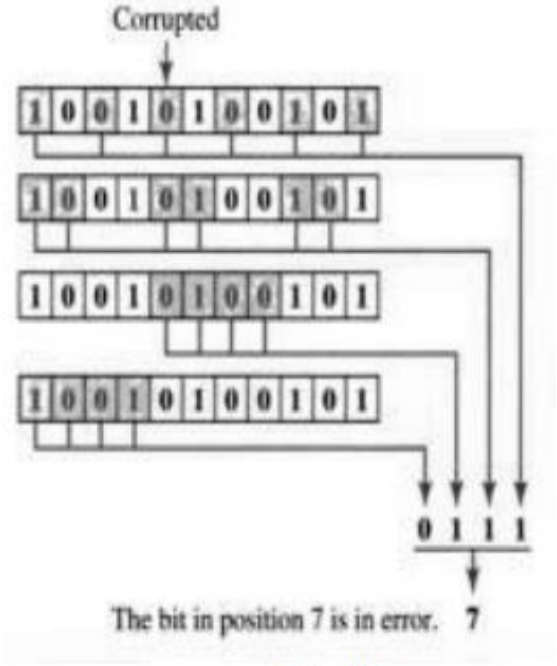


Fig .20

Once the bit is identified, the receiver can reverse its value and correct the error. The beauty of the technique is that it can easily be implemented in hardware and the code is corrected before the receiver knows about it.

FLOW CONTROL AND ERROR CONTROL

Flow control and Error control are the control mechanism at data link layer and transport layer. Whenever the sends the data to the receiver these two mechanisms helps in proper delivering of the reliable data to the receiver. The main difference between the flow control and error control is that the **flow control** observes the proper flow of the data from sender to receiver, on the other hand, the **error control** observes that the data delivered to the receiver is error free and reliable.

Definition of Flow Control

The flow control is a design issue at data link layer and transport layer. A sender sends the data frames faster then the receiver can accept. The reason can be that a sender is running on a powerful machine. In this case, even the data is received without any error; the receiver is unable to receive the frame at this speed and loose some frames.

There are two control methods to prevent the loss of frames they are feedback-based flow control and rate-based flow control.

Feedback-based control

In feedback-based control whenever the sender sends the data to the receiver, the receiver then sends the information back to the sender and permits the sender to send more data or inform the sender about how the receiver is doing. The protocols of feedback-based control are sliding window protocol, stop-and-wait protocol.

Rate-based flow control

In rate-based flow control, when a sender transmits the data faster to the receiver and receiver is unable to receive the data at that speed, then the built-in mechanism in the protocol will limit the rate at which data is being transmitted by the sender without any feedback from the receiver.

Definition of Error Control

Error Control is the issue that occurs at data link layer and transport level as well. Error Control is a mechanism for detecting and correcting the error occurred in frames that are delivered from sender to the receiver. The error occurred in the frame may be a single bit error or burst error. Single bit error is the error that occurs only in the one-bit data unit of the frame, where 1 is changed to 0 or 0 is changed to 1.

In burst error is the case when more than one bit in the frame is changed; it also refers to the packet level error. In burst error, the error like packet loss, duplication of the frame, loss of acknowledgment packet, etc. can also occur.The methods to detect the error in the frame are parity checking, cyclic redundancy code (CRC) and checksum.

Parity Checking

In parity checking, a single bit is added to the frame which indicates whether the number of '1' bit contained in the frame are even or odd. During transmission, if a single bit gets changed the parity bit also get change which reflects the error in the frame. But the parity checking method is not reliable as if the even number of bits are changed then the parity bit will not reflect any error in the frame. However, it is best for single bit error.

Cyclic Redundancy Code (CRC)

In Cyclic Redundancy Code the data undergoes a binary division whatever the remainder is obtained is attached with the data and send to the receiver. The receiver then divides the obtained data with the same divisor as with which the sender divided the data. If the remainder obtained is zero then the data is accepted. Else the data is rejected, and the sender needs to retransmit the data again.

Checksum

In checksum method, the data to be send is divided into equal fragments each fragment containing n bits. All the fragments are added using 1's complement. The result is complemented once again, and now the obtained series of bits is called checksum which is attached with the original data to be send and send to the receiver.

When the receiver receives the data, it also divides the data in equal fragment then add all the fragment using 1's complement; the result is again complemented. If the result comes out to be zero then the data is accepted else it is rejected, and the sender has to retransmit the data.

The error obtained in the data can be corrected using methods they are Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes.

Key Differences Between Flow Control and Error Control

1. Flow control is to monitor the proper transmission of data from sender to receiver. On the other hand, Error Control monitors the error-free delivery of data from sender to receiver.
2. Flow control can be achieved by the Feedback-based flow control and rate-based flow control approach whereas, to detect the error the approaches used are Parity checking, Cyclic Redundancy Code (CRC) and checksum

and to correct the error the approaches used are Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes.

3. Flow control prevents the receivers buffer from overrunning and also prevents the loss of data. On the other hand, Error control detects and corrects error occurred in the data.

Reliable data transfers is one of the primary concerns in computer networking. This service department lies in the hands of TCP. There major flow control protocols – Stop and Wait, Go Back N, and Selective Repeat.

1. **Stop and Wait –**

The sender sends the packet and waits for the ACK (acknowledgement) of the packet. Once the ACK reaches the sender, it transmits the next packet in row. If the ACK is not received, it re-transmits the previous packet again.

2. **Go Back N –**

The sender sends N packets which is equal to the window size. Once the entire window is sent, the sender then waits for a cumulative ACK to send more packets. On the receiver end, it receives only in-order packets and discards out-of-order packets. As in case of packet loss, the entire window would be re-transmitted.

3. **Selective Repeat –**

The sender sends packet of window size N and the receiver acknowledges all packet whether they were received in order or not. In this case, the receiver maintains a buffer to contain out-of-order packets and sorts them.The sender selectively re-transmits the lost packet and moves the window forward.