

Computer Networking: Fundamentals

(H17A 34)

Section 1: Characteristics of LANs

Introduction to this section

Assessment information for this section

Network concepts

Networking models

Summary of this section

Introduction to this section

What this section is about

This section describes the characteristics of LANs that are in use in homes and industry. Throughout the section there are activities to be undertaken on existing networks and it is advisable to maintain a logbook of your research findings and a glossary of terms that you encounter. This logbook will assist you in revising for the final assessment of 50 multiple choice questions.

**Network concepts**

To start with, let us look at some of the network terminology and types.

**Networking basics**

A network is two or more computers that have been connected for the purposes of exchanging data and sharing resources. Networked shared resources range from printers, CD-roms and modems to files and hard drives. Networks vary in size and scope.

**Peer-to-peer network:** This type of network includes two or more PCs that are connected to share data files, a printer or other resources. This type of network is also called a workgroup (*Figure 1.1*).

*Figure 1.1 Example of a peer-to-peer network (workgroup).*

|  |  |
| --- | --- |
| *Computer 1MP900402149[1]* | *Computer 1 has a shared local printer called*  *comp1epsonlx2000 and a shared area called*  *comp1data, which is a folder on the C drive called*  *data. The naming convention is entirely up to the*  *network administrator.* |
| *Computer 2MP900402149[1]* | *Computer 2 has no local printer and a shared area*  *called comp2data, which is a folder on the C drive*  *called data.* |

Computer 2 can be set up to use the printer on computer 1 and a network drive can be created using comp1data. Similarly computer 1 can create a network drive using comp2 data. For this to happen in a secure network the user accounts must be available on both computers or when creating the network drive, the log-on under a different name is selected and a user account on that computer used. To access their data, the user has to use the same computer each time.

**Server/domain network**: A network can be classified as being either a peer-to-peer or a client/server architecture. When all nodes on a network are equal and resources are shared equally, the network is a peer-to-peer network. When one computer is designated to host programs or files for the rest of the network, it is a server and the other nodes are clients. This can also be a domain server where users and devices have to be registered with the server (*Figure 1.2*).

|  |  |
| --- | --- |
| *Computer 1MP900402149[1]* | *Computer 1 is the domain server. It has a shared local printer called domainepsonlx2000 and a shared area called serverdata, which is a folder on the C drive called data.* |
| *Computer 2MP900402149[1]* | *Computer 2 is a client and the account for the user must be present in the domain. The computer must also be registered with the domain by a domain administrator before it can be used by a user.* |

area on the server for all data to be stored. The user profile identifies the area for a particular user to store/share data, the settings and the permissions of the user environment. This increases the security of the network and allows users to log on to any client machine to access their data. Backing up of the data is more secure as all data is located in one folder on one computer. For larger networks a computer can be added to the network as a file server, which reduces the workload of the domain server.

LAN: A small business or corporate department may install a LAN that interconnects from two to hundreds of PCs, using permanently installed cabling or perhaps a wireless technology. This can be either a peer-to-peer or a domain network. It is usually located within one building but can be spread over several buildings within the same locality.

Wide area network (WAN): A business may maintain a WAN using dial-up, leased or other dedicated communication means. The Internet is the largest WAN in the world and most company WANs use the Internet backbone to create a secure network. The uses of WANs extend beyond sending data. They can be used, for example, for telephone communications within an organisation. A person dials a long distance number; the computer managing the local phone system contacts the computer managing the phone system at the organisation’s nearest office to the number being dialled. The number is then dialled locally. The people at both ends of the phone will not notice anything different.

Topology

The geometric arrangement of any network is its topology. The most common

topologies are shown in Figure 1.3.

|  |  |
| --- | --- |
| **Bus**  Central cable terminated at both ends. The packet (see below) passes along the cable and each workstation listens to the signal. If the start of the packet contains its address (or name) then it reads the rest of the packet. This type of network uses BNC connections and coaxial cable. If the central cable is damaged (disconnected), the entire network is unavailable. |  |
| **Ring**  Similar to bus except all machines accept all packets and pass on any that are not theirs. **Token ring**, another name for ring, uses copper and fibreoptic cabling, operates at 4 Mbps to 16 Mbps, and supports about 260 nodes. This network is reliable but is difficult to troubleshoot. |  |
| **Star**  Originally a star network was a LAN in which all nodes (workstations) were directly connected to a common central computer. Every workstation was indirectly connected to every other through the central computer. Today most networks use switches and hubs to create a star network that does not require a computer at the centre to manage it. This type of network uses twisted-pair cable with RJ45 connections |  |
| **Star-wired ring**  A star-wired ring affords the same function as ring communication, while providing a well-designed cable layout for the network. The basic ring function is to allow every node an equal time to communicate on the network but does not require each node to pass on every packet.  *.* |  |

. *Figure 1.3 Common network topologies*

Connecting to the Internet You can connect to the Internet and other computers in a variety of ways. The main one is by using cable connected to a network card within the computer. This cable can be coaxial, Cat 5, Cat 6 or fibre depending on the type of network. Connection to the Internet can be either by modem (dial-up), integrated services digital network (ISDN), digital subscriber line (DSL) or cable depending on the size of the network and the bandwidth (speed of transfer) required. With the introduction of satellite and wireless there are now networks that are completely wire free. Mobile technology can also be used to connect to the Internet either by phone or by connecting a laptop, for example, to the Internet using infrared, Bluetooth or Universal Serial Bus (USB).

NIC

The NIC is a physical and logical link for a PC to a network. It is installed inside the computer in an open expansion slot. NICs are available for most of the expansion bus architectures, so getting a card for an available slot is easy. The most commonly used bus for NICs is the peripheral component interconnect (PCI) bus, but many legacy industry standard architecture (ISA) cards are still in use.

The setup that is needed for the NIC is controlled by two factors: the PC itself and the network operating system (NOS), such as Windows NT/2000 or Novell NetWare. The NIC is a translator that works between the network and the PC. Networks transmit data in a serial data format (1 bit at a time), and the data bus of the PC moves data in a parallel format (8 bits at a time). The NIC acts as a go-between to convert the signal from serial to parallel format or from parallel to serial format, depending on its direction. The NIC also formats the data as required by the network architecture. Media access control (MAC) address: Each NIC is physically encoded with a unique identifying address that is used to locate it on the network. This address is 48 bits (6 bytes) long.

System resources: A NIC is configured to the computer with an interrupt request line (uses IRQ3, IRQ5 or IRQ10, and an I/O address of 300h.RQ), an I/O address and a direct memory access (DMA) channel. A NIC commonly uses IRQ3, IRQ5 or IRQ10, and an I/O address of 300h.

Data speed: The NIC must be compatible with the data speed of the network. The data transfer speeds of a network are determined by several factors, including the cable media, the network topology and the network connectivity devices that are in use. For example an Ethernet network using Cat 5 attaches its workstations through hubs or switches and runs at either 10 Mbps or 100 Mbps. Most new computers have the network card (wireless and/or Ethernet) on board the motherboard with connection type RJ45.

The main types of connectors used in networks are BNC, D connection and RJ45

(Figure 1.4).

.

BNC D connection RJ45

Figure 1.4

|  |  |
| --- | --- |
| T Connector    Terminator | BNC  This connector is used in bus networks with the main cable connecting all the computers together and terminated at each end. The T connector shown here can be connected to the network card of the computer or a connecting cable can be used to connect the T junction to the computer. It will depend on the installation whether there is enough room to have the main cable going to the back of each computer. One way that I found to be a simple but practical method is to attach junction boxes to the skirting boards with the main cable running along or under the floor with a connecting cable to the computer. This reduces the safety risks as the amount of loose cabling is reduced and as the main cable is fixed, the risk of disconnecting the network is reduced. |
|  | Sub D  This connector is used in token ring networks, depending on the type of ring. In a star ring, the ring can consist of Ethernet bridges that allow the computers to be connected using RJ45 and Cat 5 cable to the ring. This bridge acts as the central control for the star segment. |
|  | RJ45  This connection is used in star networks. It is very similar to the connectors (RJ11) used on telephones but they are not interchangeable. These are connected to an 8-core cable of which only four are used in Cat 5 networks. You can buy a splitter which allows you to connect two devices to the same Cat 5 connection. This requires a splitter at the other end of the Cat 5 connection. More details are in the wiring section. |

Figure 1.5 Main types of connectors.







BNC D connection RJ45

Dial-up connectivity

Dial-up connectivity through a modem depends greatly on the quality of the phone line and, to increase the quality, dedicated data lines were made available and ISDN was introduced, which was an expensive alternative but, for companies, essential. This has now been replaced with DSL and cable, which have greater bandwidths. The cost of accessing the Internet has been reduced with the introduction of broadband and a bandwidth of 128 kB to 10 Mb is easily affordable. These connections are usually permanent and have a fixed charge not based on usage but on the amount of bandwidth you have.

When using dial-up, your modem dials the Internet service provider (ISP) you are signed up with and waits for their end to answer. After checking protocols (baud rate for example) the connection is made and you will be asked to log on using a user ID and password. Once approved, you will have an Internet connection. There are different ways of ensuring that the person dialling up has the authorisation required apart from the user ID and password. The receiving computer knows the telephone number from where the call is being made and can have a record of all numbers that are approved. If the number is not authorised, the connection will be dropped. Another method is to use callback, which will disconnect and then call the phone number if authorised.

Other connectivity technologies

DSL: Digital subscriber line allows high-bandwidth information to be transmitted to homes and small businesses over ordinary copper telephone lines. There are several variations of DSL including asymmetric digital subscriber line (ADSL) and high bit-rate digital subscriber line (HDSL).

ISDN: Integrated services digital network allows for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who use ISDN receive web pages at up to 128 kbps compared with the maximum 56 kbps rate of a modem connection. This is an expensive method for connecting to the Internet and is being replaced by DSL.

Cable: This requires you to have a connection installed to a cable television company’s network. The cable is attached to a cable modem, which is connected to the computer either by USB or more commonly RJ45 (normal network connection). This allows access to the Internet using a bandwidth from 128 kbps to 4 Mbps depending on how much you want to pay/use the Internet. Upload speeds are lower, usually 128 kbps. Satellite: A satellite Internet connection is an arrangement in which the outgoing and the incoming data are sent from, and arrive at, a computer through a satellite. To transmit and receive data you must have a dish and transmitter/receiver connected to your computer. Upload speeds are nominally 50 to 150 kbps if using a single computer and download speeds range from about 150 kbps to more than 1200 kbps. This method is expensive as you need to buy connection time to the satellite but ideal for remote locations where all you need is enough power to run the computer and the transmitter/receiver.

As mentioned before, the quality of the telephone cable can affect connectivity as can the interference of walls in a wireless network. Crosstalk (interference from traffic on one wire crossing over to another) can also result in the information being corrupted and having to be sent again. One method of testing connectivity is to use the DOS

Open up a DOS command window. Type in ipconfig and press return (enter).



You will see information similar to that shown in the screen shot. The IP address shows you the address (just like a postal address) of your computer. There will be more about the make-up of this address later. The third line shows you the address of the gateway.

This gateway is the computer or router that connects your network to another including the Internet.

We can test the connectivity by seeing how long it takes for a packet (set of data) to reach this gateway. Type the following into your DOS window, replacing the number with the gateway on your screen.

Ping 192.168.1.1.



The screen shows that the time it took to send and receive a reply was 1 millisecond. You can also ping an Internet site. Try it with a few that you know.

Here we are pinging [www.learn-on.co.uk](http://www.learn-on.co.uk).







Computer Networking: Fundamentals

(H17A 34)

LANS

Devices

Repeater: This electronic echo machine has no function other than to retransmit whatever it hears. A repeater is used to extend the signal distance of the cable by regenerating the signal. It is normally found in a bus or ring network where the next node is beyond the maximum distance between nodes.

Hub: This device is used to connect workstations and peripheral devices to the network. Each workstation or device is plugged in to one of the hub's ports. A hub receives a signal from one port and passes the signal on to all of its other ports and therefore to the device or workstation that's attached to the port. For example, if an 8- port hub receives a signal on port 4, the hub immediately passes the signal to ports 1, 2, 3, 5, 6, 7 and 8. Hubs are common to Ethernet networks.

Bridge: Bridges are used to connect two different LANs or two similar network segments, to make them operate as though they were one network. The bridge builds a bridging table of physical device addresses that is used to determine the correct bridging or MAC destination for a message. Because a bridge sends messages only to on which the destination node exists, the overall effect of a bridge on a network is reduced network traffic and fewer message bottlenecks. To do this it uses a spanning tree algorithm. ng special messages known as configuration bridge protocol data units. These contain enough information to enable the bridges to elect one bridge in the network to be the root. Each then calculates the shortest path distance to the root bridge from each bridge. A designated bridge for each subnet on that LAN is used for forwarding packets towards the root. The port on each bridge that gives the shortest path to the root is assigned as the forwarding port and is included in the spanning tree.

Router: This device sends data across networks using the logical or network address of a message to determine the path that the data should take to arrive at its destination. Routers make forwarding and filtering decisions based on the network numbers for IP addresses. To achieve this each segment is assigned a port on the router, which is assigned a network number. Each device connected in that segment is identified by this network number and a unique node number.

Each node needs to be aware of the router to be able to communicate with other devices not on the same segment.

Routers reduce the amount of traffic on a network by keeping internal segment traffic from being broadcast to the entire network and, by maintaining information about the topology of the network, find the optimal path for communication to take place between devices.

Switch: A switch is a device that segments a network. The primary difference between a hub and a switch is that a switch does not broadcast an incoming message to all ports but instead sends the message out only to the port on which the addressee workstation exists, based on a MAC table that is created by listening to the nodes on the network.

Gateway: This is a combination of hardware and software that enables two networks with different protocols to communicate with one another. A gateway is usually a dedicated server on a network because it typically requires large amounts of system resources. The following types of gateways exist:

• Address gateway: Connects networks with different directory structures and file-management techniques.

• Protocol gateway: Connects networks that use different protocols. This is the most common type of gateway.

IP address: Many internal and all external networks use IP addresses to identify nodes on both LANs and WANs.

Network names: The most common type of network name is computer names, which are also called network names. A network name is the name assigned to a workstation or other networked device and used to identify that node by other network users.

Network names are network basis input/output system (NetBIOS) names. NetBIOS uses unique 15-character names that are periodically broadcast over the network so the names can be catalogued by the network neighbourhood function. NetBIOS names are the names that show up in Windows Network Neighbourhood. You will find when using Windows 98 that this catalogue takes a while to be created and you may not see the computer just added on to the other computers immediately.

DHCP: This protocol is used to automatically configure a network workstation with its IP address data if the NIC is set to auto assign. Domain name system (DNS): DNS is used to resolve (translate) Internet names to their IP address equivalents.

WINS: WINS is Microsoft's network name resolution software that converts NetBIOS names to IP addresses. Windows machines are assigned NetBIOS names, which are converted into IP addresses for use on a network using TCP/IP.



Computer Networking: Fundamentals

(H17A 34)

Introduction to this section

What this section is about

This section describes the characteristics of the media that are used in networks.

Outcomes, aims and objectives

You will learn about the different types of connection media and examples of copper (wired), optical (fibre) and wireless (radio).

Layer 1 copper media:

• Voltage, resistance, impedance, coaxial, shielded copper and unshielded twisted pair (UTP) cable.

Layer 1 optical media:

• Electromagnetic spectrum, reflection, refraction, multimode and single mode fibre.

Layer 1 wireless media:

• Wireless devices, topologies, authentication, association, radio and microwaves.

Other resources required

Physical examples of media.

Layer 1 copper media

Data is transferred by electrical current passing along the cable. Several factors can affect the robustness of the network infrastructure. The cable itself may become damaged resulting in a decrease in the voltage between the end points by current leaking from the cable.

Voltage is an electric potential difference between two points. Poor end connections (wires not making a clean contact with the plug/socket) can increase the resistance to the current being carried.

Electrical resistance is a measure of the degree to which a cable opposes the passage of an electric current.

Impedance is the measurement of resistance to the flow of electric current when a voltage is impressed across its terminals. It is the impedance of a cable that limits the length that can be used before the signal strength is lost.

Network devices

Network hardware consists of NICs, cabling, and other devices that assist and improve communications.

Connectors

|  |  |
| --- | --- |
| Patch panel front.  A patch panel is a convenient way of organising the wiring of your network cables. Without a patch panel every cable would be connected directly into a hub or switch, making error checking and tracing where each cable goes to difficult. Using the labels on the front of the panel you can identify where each cable terminates and by labelling the other end where it originates from. |  |
| Patch panel back. |  |
| Switches in rack. |  |
| Patch panel connectors.  The same colour coding is used on the socket. |  |

Cabling

For one computer to carry on a conversation with another computer, both computers must be able to transmit and receive electrical impulses that represent commands or data. The computers and peripherals of a network are interconnected with a transmission medium to enable data exchange and resource sharing.

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Description | Types | |
| Coaxial (coax) | This is similar to the cable that is used to connect your TV set to the cable television service. | thick | 10Base5 ThickWire ThickNet |
| thin | 10Base2 ThinWire ThinNet |
| Twisted-pair | Cable with four sets of twisted-pair wires. Similar in appearance to telephone wire. Shielded has a metal film surrounding the wires to reduce external electrical interference. | Unshielded twisted pair (UTP) | 10baseT 100BaseT  Cat 3 Cat 5 Cat 6 has recently been introduced |
| Shielded twisted pair (STP) |

Cabling speeds

|  |  |
| --- | --- |
| Cat 3 | 16 Mbps |
| Cat 5 | 100 Mbps  1000 Mbps (4 pair) |
| Cat 5E | 1000 Mbps |
| Cat 6 | Up to 400 MHz for super-fast broadband applications |

Wiring

|  |  |
| --- | --- |
| Coaxial cable consists of an inner wire, usually solid, and an outer plaited cable to reduce interference. The outer cable is stripped back and the centre core is fed into the centre of the connector (and soldered or crimped) and the outer wire is crimped to the outer casing which also acts as a cable clamp. |  |
| Cat 5 cable consists of four twisted pairs of wire. They are twisted to reduce the amount of crosstalk as the signals travel down the cable. There are two wiring conventions that are in use and although they can be used in the same network, you must use the same convention Cat 5 cable consists of four twisted pairs of wire. They are twisted to reduce the amount of crosstalk as the signals travel down the cable. |  |

Figure 2.2 Coaxial and Cat 5 cable.

Layer 1 optical media

|  |  |  |
| --- | --- | --- |
| Fibreoptic  . | With this cable, glass or polymer fibres carry modulated  pulses of light to represent digital data signals | 10BaseF  100BaseF |
| FDDI  CDDI For a LAN, copper distributed data interface (CDDI) is a standard for  data transmission based on FDDI that uses twisted-pair copper wire  instead of fibre-optic lines. | Fibre distributed data interface (FDDI) is a set of standards for data transmission on fibre-optic lines in a LAN that can extend in range up to 200 km. The protocol is based on the token ring. It is used in the backbone for large networks. There are two token rings in an FDDI network and they can either be used together to produce double the bps or the second can be used as a back-up in case the first ring fails. | |
| CDDI  . | For a LAN, copper distributed data interface (CDDI) is a standard for data transmission based on FDDI that uses twisted-pair copper wire instead of fibre-optic lines | |

Fibre-optic cable uses glass (or plastic) threads (fibres) to transmit data. The cable consists of a group of glass threads, each of which is capable of transmitting messages modulated into light waves.

Fibre-optic cables have several advantages over traditional copper cables:

• They have a greater bandwidth.

• They are less susceptible to interference.

• They are much thinner and lighter.

• Data can be transmitted digitally.

They have the following disadvantages:

• They are more expensive to install.

• They are difficult to split and reconnect.

• The fibres are easier to break thus making the signal disintegrate.

Multi-mode optical fibre is used when communicating over short distances. It is easier to connect than single-mode optical fibre but the speed of data transfer is reduced as the length is increased. Multi-mode fibre has a larger core than single-mode fibre, which allows it to support more than one path for data within the fibre.

Single-mode

fibres are best at retaining the fidelity of each light pulse over longer distances.

Layer 1 wireless media

This technology is on the increase with companies providing access points throughout the world for mobile users to link to the Internet. More and more laptops and personal digital assistants (PDAs) are being installed with wireless technology allowing the user to connect to the Internet wherever they can find a wireless access point. Some points will be free but most providers require online payment before giving you the access codes to the service. Most sell time in a similar way to pay-as-you-go mobile phones. If

you want a private wireless network then you need a secure connection that uses a wired equivalent privacy (WEP) key to connect. This technology is also being used as part of a LAN as, in certain situations, it is cheaper to install wireless than run cable. A wireless router can have a range of 90 m indoors for 1 Mbps to 30 m for 11 Mbps (802.11b) or 54 Mbps (802.11g). These speeds are lower than normal cabling which can be up to 100 Mbps and large networks will have a 1 Gbps backbone using fibre optics to ensure that the user has the highest bandwidth possible at their computer. Remember every time you add a hub, all the computers on that hub share the bandwidth of the connecting cable.

Wireless works with the 802.11b and 802.11g standards, transmitting at 2.4 GHz and the 802.11a standard transmitting at 5 GHz. The transmitters/receivers used for WiFi have the ability to change frequencies. Cards using 802.11b can transmit directly on any of three bands or they can split the available radio bandwidth into numerous channels and frequency hop rapidly between them. The advantage of frequency hopping is that it is much more immune to interference and increases the number of WiFi cards that can talk simultaneously without interfering with each other.

Interference can reduce the speed to 1 to 2 Mbps on an 802.11b WiFi. Another aspect to consider is the reduction in signal strength between rooms in a building in which you are using a WiFi network. To compensate for this most networks using WiFi also use wired connections called hotspots as a connection point for the network. This connection contains an 802.11 radio that can simultaneously talk to up to 100 or so 802.11 cards.

Authentication

Regardless of the network media used, each device has to be identifiable on a network and has to be approved before being allowed to communicate on the network. This approval is called authentication. For example, in a Windows domain network a computer’s name must be present in the directory’s computer folder and an association (relationship) made between the directory and the computer. This relationship has to be made by a domain administrator and information is stored in the directory and computer which uniquely defines this association. This prevents another computer with the same name pretending to be an authorised computer.

Summary of this section

You will now have an understanding of the characteristics of the media that is used in Networks. You will have learnt about the different types of connection media and

examples of Copper (wired), Optical (fibre) and Wireless (radio).

You will be able to relate these characteristics to the media type as indicated below:-

• Copper media

􀂃 Voltage

􀂃 Resistance

􀂃 Impedance

􀂃 Coaxial

􀂃 Shielded

􀂃 UTP cable

• Optical media

􀂃 Electromagnetic spectrum

􀂃 Reflection

􀂃 Refraction

􀂃 Multimode

􀂃 Single mode

• Wireless media

􀂃 Wireless devices

􀂃 Topologies

􀂃 Authentication

􀂃 Association

􀂃 Radio

􀂃 Microwaves

|  |  |
| --- | --- |
| Convention T-568A  Pin Colour Pair Transmits  1 white/green 3 RxData + 2 green 3 RxData – 3 white/orange 2 TxData + 4 blue 1 Unused 5 white/blue 1 Unused 6 orange 2 TxData - 7 white/brown 4 Unused |  |
| Convention T-568B  Pin Colour Pair Transmits  1 white/orange 2 TxData + 2 orange 2 TxData - 3 white/green 3 RxData + 4 blue 1 Unused 5 white/blue 1 Unused 6 green 4 Unused 8 brown 4 Unused |  |

As mentioned earlier, you can make use of the unused wires by making or buying a splitter. The splitter connects the normal wires to one socket and the others to the same connections in the other socket.

## Ethernet fundamentals

The term Ethernet refers to the family of LAN products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fibre and twisted-pair cables.

### Media access control

Media access control happens in layer 2 and is handled by one of the following:

* + **CSMA/CD** is a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously. Standard networks use CSMA/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular station can transmit. If two stations attempt to transmit simultaneously, this causes a collision which is detected by all participating stations. The stations whose data collided will attempt to transmit again after a random time delay. This will be repeated if another collision happens. The delay interval will be increased every time this collision happens.
  + **CSMA/CA** is a network contention protocol that listens to a network in order to avoid collisions, unlike CSMA/CD that deals with network transmissions once collisions have been detected. CSMA/CA contributes to network traffic because it broadcasts a signal onto the network in order to listen for collision scenarios and to tell other devices not to broadcast.

To carry data across a network a network card passes an electronic signal onto a cable via a connector. The way data travels is identified as:

* + **simplex**, which refers to data moving in a single direction;
  + **half duplex**, which means data travels both ways on the medium but in only one direction at a time;
  + **full duplex**, which means data travels in both directions simultaneously.

## Cable types

Cabling is the wire or fibre medium that is used to connect computers and other network devices of a network together, as well carry the data that is transmitted between them.

There are three types of physical media that can be used on a network:

* + coaxial cable
  + twisted-pair cable
  + fibre-optic cable.

### Coaxial cable

**Coaxial cable** (or coax) looks like the cable used to bring the TV signal to a television. One strand (a solid-core wire) runs down the middle of the cable. Around that strand is insulation. Covering that insulation is braided wire and metal foil, which shields against electromagnetic interference. A final layer of insulation covers the braided wire.

Coaxial cable is resistant to the interference and signal weakening that other cabling, such as UTP cable, can experience. In general, coax is better than UTP cable at connecting longer distances. It is also more reliable when supporting higher data rates with less sophisticated equipment.

Network coaxial cable has very specific requirements including gauge, impedance and attenuation. The following are two network coaxial cables:

* + **Thinnet** refers to RG-58 cabling, which is a flexible coaxial cable about 0.6 cm thick. Thinnet is used for short-distance communication and is flexible enough to facilitate routing between workstations.
  + **Thicknet** coaxial cable can support data transfer over longer distances better than Thinnet can and is usually used as a backbone to connect several smaller Thinnet-based networks. 10Base5 refers to Ethernet LANs that use Thicknet cabling. A backbone segment is made up of high-speed lines and equipment normally located at the very centre of a network.

### Twisted-pair cable

**Twisted-pair cable** is a type of cabling that is used for telephone and network communications. Twisted-pair cables have one or more pairs of copper wires that are insulated and twisted around one another and this prevents the signals on the wires from interfering with one another. Twisted-pair cabling may be shielded or unshielded.

**UTP** cabling is the most common type of physical media on networks today. The typical twisted-pair cable for network use contains three or four pairs of wires. Each pair of wires contained in the cable is twisted around each other, which helps shield against crosstalk and other forms of electromagnetic interference.

The difference between UTP and **shielded twisted-pair (STP)** is that STP has an extra layer of aluminium/polyester between the wire and the plastic covering. This shield protects the wires inside from EMI caused by outside sources.

### Fibre-optic cable

There are two different types of fibre-optic cabling that may be used to carry data:

* + **Single mode fibre (SMF)** is optical fibre that is designed to transmit a single beam of light from a laser. The beam of modulated light provides greater bandwidth and allows cable to be run over longer distances.
  + **Multimode fibre (MMF)** is used to carry multiple beams of light at the same time, using a light-emitting diode (LED) as a light source. Each of the beams is at a slightly different reflection angle within the core of the fibre. Because the light tends to disperse over distance, MMF is used for connecting locations within relatively short distances.

## Cable speed

**Fast Ethernet** is a standard that provides transmission of data at speeds of 100 Mbps. It also uses full duplex transmission, which enables data to pass in both directions at the same time. This is generally used as a backbone on LANs.

**Gigabit Ethernet** supports speeds of one billion bits per second, making it ideal as the backbone for many larger networks. Gigabit Ethernet uses fibre-optic cabling to transmit data while Fast Ethernet runs on twisted pair.

Various types of 10 Gigabit Ethernet include:

* + 10GBaseSR which supports short distances over MMF cable and has a range of 26 m and 82 m depending on the cable type. It also supports distances of 300 m over a new 2000 Mhz km MMF.
  + 10GBaseLX4 uses wavelength division multiplexing and supports ranges of 240 m and 300 m over MMF or 10 km over SMF.
  + 10GBaseLR supports 10 km over SMF.
  + 10GbaseER supports 40 km over SMF.

Media, cable type and bandwidth capacity is summarised below.

|  |  |  |
| --- | --- | --- |
| **Media code** | **Cable type** | **Bandwidth capacity** |
| 10Base2 | Coax | 10 Mbps |
| 10Base5 | Coax | 10 Mbps |
| 10BaseT | UTP (Cat 3 or higher) | 10 Mbps |
| 100BaseTX | UTP (Cat 5 or higher) | 100 Mbps |
| 10BaseFL | Fibre optic | 10 Mbps |
| 100BaseFX | Fibre optic | 100 Mbps |
| 1000BaseT | UTP (Cat 5E or higher)  Cat 5 using 4 pairs of wires | 1000 Mbps |
| 1000BaseSX | Fibre optic | 1000 Mbps |
| 1000BaseLX | Fibre optic | 1000 Mbps |
| 1000BaseCX | Fibre optic | 1000 Mbps |
| 10GbaseSR | Fibre optic | 10 Gbps or 10000 Mbps |
| 10GbaseLX4 | Fibre optic | 10 Gbps |

## TCP and UDP

Connection-oriented and connectionless are two types of connection services used at the transport layer of the OSI model. It depends on whether reliability or speed is of highest priority. As discussed previously, data is sent over the network as a sequence of datagrams. Each datagram is sent separately across the network.

A connection-oriented protocol such as TCP offers better error control than UDP but its higher overhead means a loss of performance. A connectionless protocol such as UDP, on the other hand, suffers in the reliability department but, unhampered by error-checking duties, is faster.

TCP establishes a virtual connection between the sending and receiving computers by the use of acknowledgments and response messages. An acknowledgment message is sometimes referred to as an ACK. UDP performs the same basic function but does not acknowledge receipt of the messages and should be used when speed is of high priority and assured delivery of the messages is less critical. Since UDP doesn't sequence the packets that the data arrives in, an application program that uses UDP has to be able to make sure that the entire message has arrived and is in the right order. To save processing time, network applications that have very small data units to exchange may use UDP instead of TCP as checking that everything has been received requires little processing. For example, DNS hostname may use UDP for look-up messages that will fit in a single datagram. For these very short queries, the complexity of TCP is not required as you can just ask for the information again if you have had no reply.