

Chapter 3

Fundamentals of networks

Chapter summary

This chapter provides an introduction to computer networks and networking. When studying computer networking, it is important to understand that networking has evolved, and will continue to evolve, as the technology becomes available, and that the use to which the technology is being put and can be put will also evolve. A computer network can be categorised according to, for example, the geographical area it covers or by the access it provides to the outside world.

Learning outcomes

After studying this chapter you should aim to test your achievement of the following outcomes. You should be able to:

Outcome 1: Network basics

Understand the basics of computer networking and be familiar with some of the terms. Question 1 at the end of this chapter will test your ability to do this.

Outcome 2: Network topologies

Describe the common network topologies and be able to identify each. Question 2 at the end of this chapter will test your ability to do this.

Outcome 3: Network addressing

Understand the basics of network addressing and be able to discuss the addressing formats. Question 3 at the end of this chapter will test your ability to do this.

How will you be assessed on this?

The topics covered in this chapter form the fundamental principles of networking – how data is encoded, the different topologies and logical/physical addressing mechanisms. The most popular form of assessment for such topics is by examination or time-constrained test (TCT). The questions at the end of this chapter provide you with sample questions which may well be asked in such assessments.

Section 1

Understanding network basics

Computer networking is subject to the laws of physics, and therefore a basic understanding of the physics of networking will aid understanding. The laws of physics also govern the speed and development of networking. This section introduces some of the basic physics which impact on networking. It assumes that you understand binary – that binary is the basis of all data held and transmitted by a computer, digital signals, analogue signals and digital-to-analogue conversion. If this is not the case, it is recommended you read a book on computer architectures to pick up these basics before proceeding.

Encoding

Computer networking is about moving data (in the form of bits) along some sort of transmission media (most commonly, a piece of wire). For transmission, the data needs to be encoded into an electrical voltage which can then be carried by the wire.

CRUCIAL TIP

Although it might seem odd, a great deal can be gleaned from comparing networking to plumbing. Here, how a wire carries data (represented by a voltage) is likened to a pipe carrying water.

Figure 3.1 shows data encoding using +12 v to represent a 0 and -12 v to represent a 1. It is common usage to employ two voltages to differentiate a no signal state from a signal state. Thus, if the sender is at the right and the receiver at the left, the data 0101010 is being transmitted.

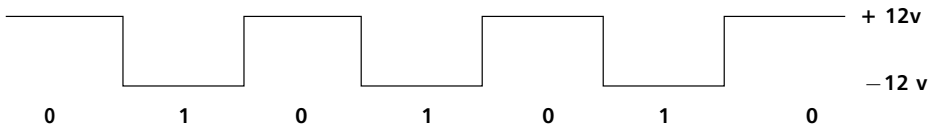


Figure 3.1 Data encoding
(diagram courtesy of Professor Peter Hodson, University of Glamorgan)

Any good computer architecture book will detail how alphanumeric characters are encoded using an encoding mechanism such as the American Std Code for Info Interchange (ASCII)

Circuits

To carry data a circuit is required. In most cases a circuit comprises two wires. Consider Figure 3.2, which is a simple torch circuit. Here, when the switch is closed, the electrons move, providing electricity to the bulb which lights up. Opening the switch stops the flow of electrons and the light goes out. This circuit could be used to represent basic binary digits (either 1 (on) or 0 (off)).

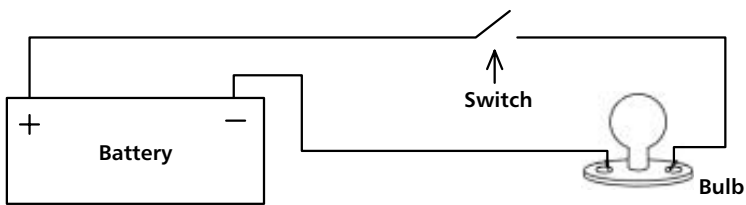


Figure 3.2 Simple torch circuit

Networking also needs complete circuits – we call the cables the 'signal' and the signal 'ground'. As can be seen from Figure 3.1, determining the height of the signal (the voltage) accurately is of crucial importance. The signal wire carries the signal whilst the signal ground completes the circuit and allows the height of the signal to be determined. In practice, networks often use multiple voltage levels to represent many bit patterns. For example, by using four voltages we can encode two bits to each voltage:

Voltage 1	00
Voltage 2	01
Voltage 3	10
Voltage 4	11

Three types of circuits are commonly used in networking:

- **Simplex** – can carry signals in one direction only (e.g. a one-way street).
- **Half duplex** – can carry signals in both ways but only one way at a time (e.g. a narrow bridge where traffic from only one direction can cross at a time – under traffic light control).
- **Full duplex** – carries signals in both directions simultaneously (e.g. dual carriage-way).

CRUCIAL TIP

You must understand these three types of circuits, as they are often referred to in a range of networking situations.

Signal problems

Electrical signals are susceptible to a wide range of interference. For example, as the signal travels along the wire it loses some of its strength and arrives at the destination weaker (a lower voltage), which makes it more difficult to determine how it was originally encoded – hence the big difference in the voltage levels used to represent a 0 and a 1. This loss of strength is known as **attenuation** and limits the distance a signal can travel without being amplified or regenerated. Attenuation can be addressed in analogue networks by amplifying the signal or, in digital networks, by repeating or regenerating the signal. Repeating is preferable as the signal generated by repeating is a perfect signal like the original, whereas amplifying also amplifies noise.

CRUCIAL TIP

Assessors quite like the topic of sources of error as an examination question.

The following is a summary of the common sources of error:

- **Attenuation** As the signal travels along the cable it becomes weaker. On long-distance runs, unless it is aided, the signal received can be too weak to use. On 100BaseT ethernet, it is recommended that the cable lengths be no more than 100 m.
- **Impulse noise** Sometimes known as electromagnetic interference (EMI), electrical signals given off by some electrical devices (e.g. fluorescent lights and electrical motors) can cause severe degradation to the signal or even destroy it. Lightning is also a cause of impulse noise. Care should be taken when routing the network cable to avoid close contact with such devices.
- **Thermal noise** Thermal noise is the interference that comes from the cable itself – the distortion caused by moving the electrons. Very little can be done to address this.
- **Crosstalk** Crosstalk is when two or more pairs of cables lying near each other interfere with the signals on the other cable. This used to be common on older telephone networks where you could hear someone else's conversation if you were quiet. Crosstalk can be largely eliminated by twisting the two wires in the circuit together.
- **Intermodulation noise** Similar to crosstalk except that, here, the signals which interfere are being transmitted on the same cable (see Broadband/baseband below). A good example of this in the UK is Channel 5 TV which is transmitted on a frequency used by most video recorders – if the video and Channel 5 are on together they often interfere with each other. This problem can be addressed by altering the frequencies used for transmission.
- **Radiation** Just as atmospheric conditions interfere with TV signals, they can also interfere with computer networks and telephone networks. Thankfully, such interference is rare and can be addressed by using shielded cabling.

- **Radio frequency interference (RFI)** RFI is interference caused by devices emitting radio signals in the proximity of the network cable. Again, electric motors and fluorescent lights can be a source of this. Other sources include mobile phones and other devices which transmit radio signals. Reduction of such interference is identical to impulse noise.
- **Signal reflection** If a network cable is not terminated correctly, the transmitted signal is reflected back from the open end of the cable and interferes with the remainder of the signal and others that follow. This was a particular problem with 10Base2 and 10Base5 networks.

Electrostatic discharge (ESD)

Often referred to simply as 'static' or 'static electricity', ESD is caused by the electrons becoming loosened and staying in one place, where they look for an opportunity to 'jump' to a conductor. ESD is the shock we feel when we have built up a charge from, for example, dragging our feet on a nylon carpet and then touching something – perhaps a metal stair banister. Other than a shock, it is usually harmless to human beings but, to sensitive electronic components such as those found inside a computer or networking devices, it can be fatal. ESD can be as high as 40 000 volts which can wreak havoc on a 5-volt computer circuit.

Broadband/baseband

A TV aerial cable carries many channels (for example, BBC1 and ITV). Although there is only one piece of cable the companies are able to transmit the channels using discrete frequencies – a different frequency for each channel. Technically, this is known as **broadband signalling**.

Computer networks can operate in a similar fashion – the available frequency range of the cable can be divided up and used to transmit different signals. Broadband services from telecommunications companies use this concept – one channel for Internet access and other, separate channels for telephones and (sometimes) fax. Thus a device needs to be employed at the socket to divide the signals.

Alternatively, a signal can occupy the entire frequency range, which is known as **baseband signalling**. This allows the signal to use all the frequency range available on the cable and, hence, it has a higher throughput (more bandwidth). Ethernet uses this principle.

Packets

Data to be transmitted across the network is broken down into chunks known as **packets**. There are two main reasons for breaking the data down into chunks. To

- reduce the amount of data lost to noise; and
- ensure fair access to the medium.

CRUCIAL TIP

Remember, data is measured in megabytes (MB) and data on a network is measured in megabits (Mb).

Let's imagine we need to transmit 2 Mb of data – 2×8 gives us 16 Mb. Let us assume that, on average, the network can transmit only 2 Mb before an error occurs. Thus we could never transmit the data as a 16 Mb entity successfully – each transmission will be corrupted by an error and require retransmission. If we break the data into packets of, say, .5 Mb each, on average we will successfully transmit three packets before an error occurs,

requiring only .5 Mb to be retransmitted. By reducing the size of the packet we can prevent even more data loss. However, as each packet needs to contain the sender and receiver addresses and some mechanism for detecting errors, if we reduce the packet size too much these overheads will also reduce performance. For this and other reasons, packet size is fixed by network technology designers and cannot be altered by the user.

Breaking data into packets also provides a fairer way of sharing the medium – users each send a packet at a time rather than ‘hogging’ the medium until their transmission is over.

Error detection/correction

We cannot prevent errors from occurring in data transmission and it is imperative we detect all errors, since data with an error must not be used. Consider a spreadsheet with financial information – if an error has occurred we don’t know that the amounts are correct and so it is unsafe to use the data. You will most likely have studied parity as an error detection method in the past. Parity is one method of error detection but it is not accurate enough for today’s networks because it does not detect all errors. Instead, we use Cyclic Redundancy Checks (CRCs) based on 32 bit polynomials to detect errors. All that needs to be known is that they detect 99.997% of all errors and that correction requires the data to be retransmitted.

Quick test

1. Briefly describe how data can be sent over a computer network. Your answer should include encoding.
2. Describe the differences between full duplex, half duplex and simplex circuits.
3. Briefly describe the kinds of interference that can occur in computer networks and how these can be addressed.

Section 2

Network topologies

The words ‘technology’ and ‘topology’ are often used when discussing networks, and it is important to clarify these terms. Technologies are the hardware devices and their operation, whereas topology is the physical shape of the network. Different technologies require different topologies. In this section, the differing topologies available for computer networks are discussed, and the differences between logical and physical topology are distinguished.

CRUCIAL TIP

Naming and drawing diagrams of various networking topologies is a popular type of examination question. Examiners may also ask you to discuss which topologies support a networking technology (see Chapter 5).

Early star networks

In Chapter 1, we discussed the ways that local interactive terminals were connected to the mainframe computer – each had its own cable running back to the central computer forming a star pattern (the star network – see Figure 3.3).

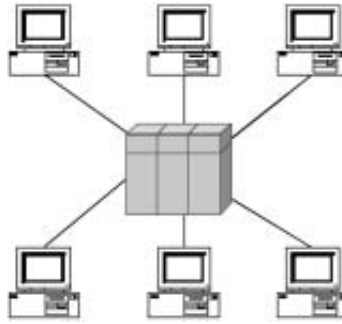


Figure 3.3 An early star network

Such cabling resulted in hundreds of cables descending upon the main computer and was costly in terms of cable and labour. Organisations often encountered problems in handling the sheer volume of cables, and relocating the central computer was a major issue.

The advantages of this type of topology, on the other hand, are:

- **robustness** – a cable break will only affect one machine;
- **performance** – each terminal has a dedicated cable.

RS232-C connectors (Figure 3.4) are the standard connectors used here (known as D.25). The cable used is twisted pair (see Figure 3.19).



Figure 3.4 D.25 serial connector

Point-to-point network

The point-to-point network is the simplest of all topologies. In the point-to-point topology (Figure 3.5), two computers are connected together via a physical wire. It is a network because it has networking hardware and software to facilitate the exchange of information. However, normally the overheads of a two-station network are greater than the benefits. Costing less than £30 at early 2003 prices (when based on ethernet technology – see Chapter 5), this topology is useful in small organisations or the home where two computers perhaps share costly resources, such as a colour laser printer, or to facilitate file transfer.



Figure 3.5 Point-to-point network

Bus network

The bus network (Figure 3.6) used to be very common and was used by a number of technologies – most notably, ethernet. In this topology a central ‘backbone’ cable spans

the area and computers 'tap' into this backbone for their connection. In a bus network, the communications medium is shared between the computers attached to it.

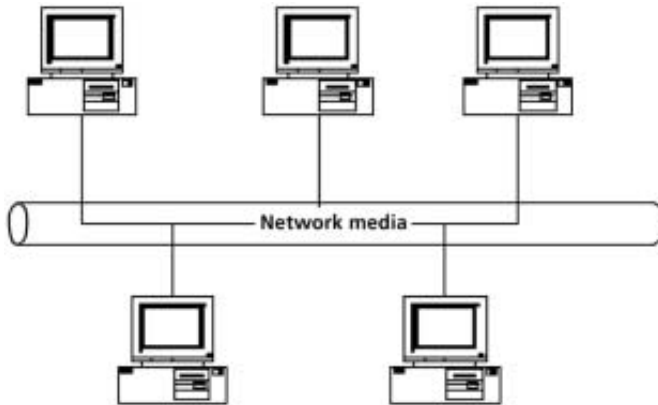


Figure 3.6 Bus network

The advantages of a bus network include the following:

- They are easy and inexpensive to install.
- It is easy to add further devices by tapping into the wire (avoiding the costs of expensive recabling).
- Bandwidth was higher than early star networks.
- Facilitates communication with the interconnected device without going through the central computer.

The disadvantages included the following:

- The media was shared – therefore there was contention for access which required an algorithm to ensure fairness.
- Data was sent in a broadcast fashion, meaning that all computers could 'see' the information.
- A cable break on the main bus cable took down the entire network.
- Although the cable was higher capacity, it was shared amongst many more users. As network traffic increased, capacity became an issue.

This kind of topology was popular (along with ring and tree networks) from the mid-1980s until around 1992, when the volume of network traffic started to increase dramatically and performance became an issue.

For cabling and connectors, see tree networks.

Tree network

It is possible to connect bus networks together to form a bus network that has branches with other bus networks. Such a topology is known as a tree network (Figure 3.7). As it is essentially a bus network, a tree network has the same advantages and disadvantages as a standard bus network. The devices used at the joints are known as **hubs** and are a specialist piece of hardware. The standard connector used in this type of network was the British Naval Connector (BNC) (Figure 3.8). The cable used was co-axial cable (similar to that used by TV aerials and cable TV) (Figure 3.9).

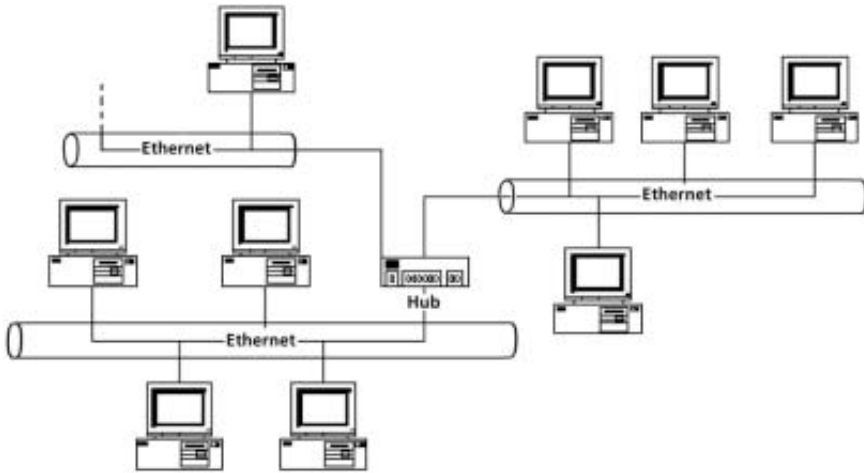
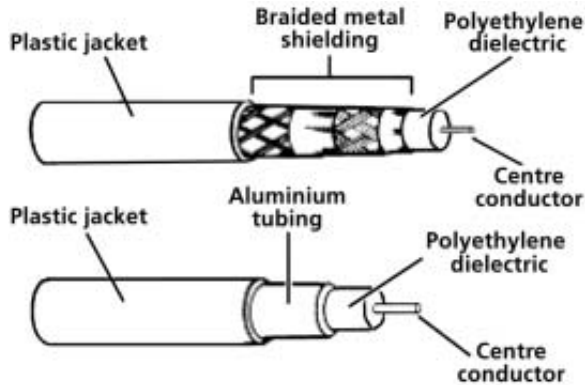


Figure 3.7 Tree network



Figure 3.8 British naval connector (BNC)

Figure 3.9 Coaxial cable
(diagram courtesy of Professor Peter Hodson, University of Glamorgan)

Ring network

In the ring topology (Figure 3.10), computers are connected to one another in a circular fashion and therefore form a ring. Although several companies and several implementations were involved, the two most notable were the Cambridge ring (developed in Cambridge University and used extensively by Acorn in the BBC microcomputer series) and the Token Ring (developed and used extensively by IBM). The dominant network in this topology was IBM's Token Ring network.

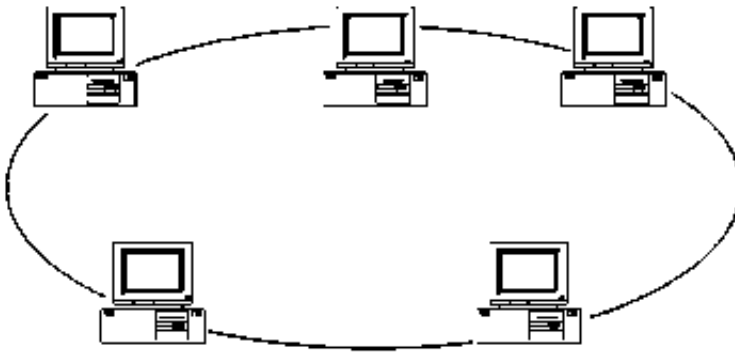


Figure 3.10 Ring network

The advantages of the ring topology are as follows:

- Robustness – there are two links to each PC.
- In the case of the Token Ring, higher capacity than standard ethernet.
- A fairer method of access than standard ethernet (see Chapter 5).

The major disadvantage was cost. As the equipment used in the topology was IBM propriety technology (which had a royalty fee attached to it), it was substantially more expensive than bus networks. Eventually, the ethernet gained the lion's share of the market (due to costs) and later versions of the ethernet outstripped the ring network's capacity.

Star with logical ring

Occasionally, ring networks (especially IBM's Token Ring) appear to be a star network (Figure 3.11) as they run to a piece of hardware called a multistation access unit (MAU). This essentially connects all the computers together and gives the network a star appearance. However, the network is still very much a ring and operates as such.

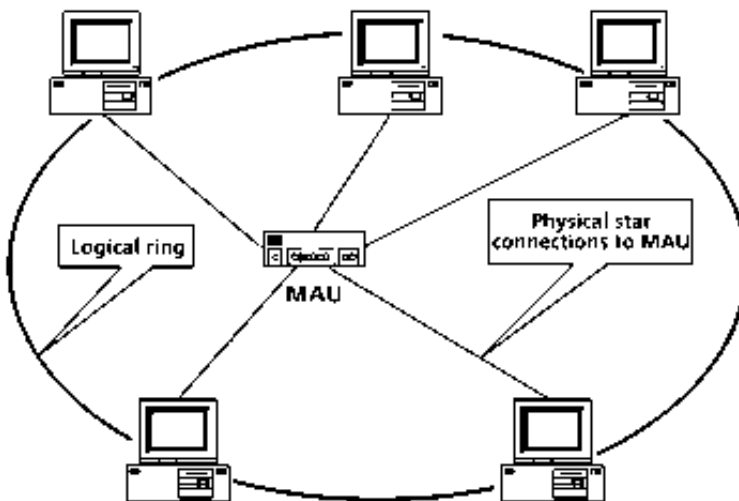


Figure 3.11 Logical ring

Connectors used in the IBM Token Ring are a proprietary technology (Figure 3.12), although most are now RJ-45. The cable used was shielded twisted pair (Figure 3.13). Shielded RJ-45 connectors are also commonly used with this technology (Figure 3.14).



Figure 3.12 Typical Token Ring connectors



Figure 3.13 STP cabling (diagram courtesy of Peter Hodson, University of Glamorgan)



Figure 3.14 STP RJ-45 connector (note the metal grounding)

Mesh network

The final topology is the mesh network (Figure 3.15). With a mesh network, a number of connections exist between machines and, in order to get from one machine to another, a route must be established. Mesh networks are complex and are designed to provide resilience in the event of a cable break. A mesh network can be either full or partial. In the case of a full mesh network, every node is directly connected to every other node – there is more than one route to every PC or network in the mesh. As its name suggests, a partial mesh network is not complete (Figure 3.15 shows a full mesh network). The Internet itself is a mesh network, as part of its original design specification was resilience. The major advantage of mesh networks is resilience, and the major disadvantages are cost and complexity. Mesh networks are almost always WAN links and, therefore, the cabling is by the service provider. A typical connector (V.35) is shown in Fig 3.16.

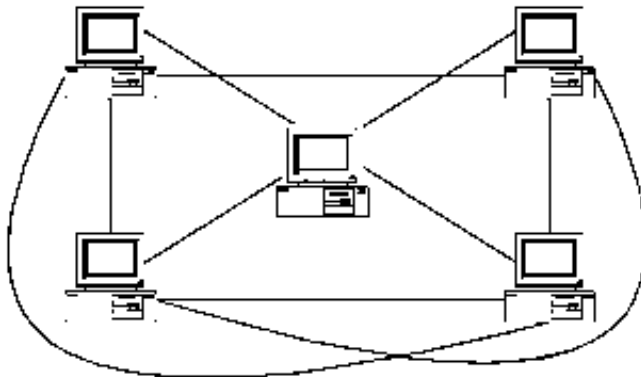


Figure 3.15 Full mesh network



Figure 3.16 Typical WAN serial connector (V.35)

Structured cabling solutions/modern star

Modern organisations experience a great deal of change during their lifetimes and have high demands for networks in terms of capacity and reliability. The original star network offered capacity that was dedicated to a terminal and that was extremely robust. Because of these advantages, the star network has been developed further and remains the preferred solution for modern cabling. A modern star network (see Figure 3.17) has, at its centre, a wiring closet to which all communications points (telephone sockets, computer sockets, etc.) on that floor are connected. Inside the wiring closet, each connection terminates in a patch panel which can then be connected to a service using a patch lead. Services would typically include different computer networks, telephone services and perhaps ISDN lines.

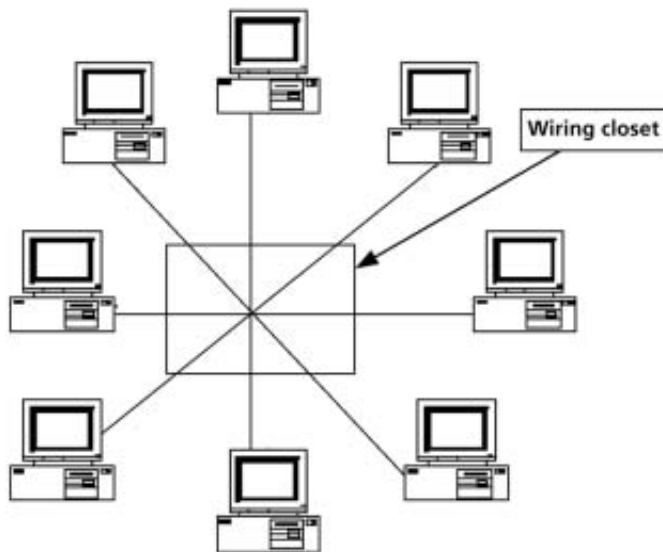


Figure 3.17 Modern star network

Known as a structured cabling solution, this is the recommended wiring structure for new installations, each installation requiring one wiring closet per 1000 m² floor interconnected by cable (usually fibre), known as backbone cabling. Structured cabling specifications require a minimum of two connection points to be installed per user and provide a very flexible communications solution. Figure 3.18 shows a typical structured cabling solution. The PC is connected through an interface card (see Chapter 5) via a 'drop cable' to the floor socket. This is connected directly to the patch panel in the wiring closet. A patch lead then 'patches' the required service from the service point to the patch panel. In this case, the service is an ethernet network. The standards for structured cabling recommend that Category 5 unshielded twisted pair (UTP) cabling (Figure 3.19) is used throughout the installation, terminated by RJ-45 plugs (Figure 3.20) and sockets.

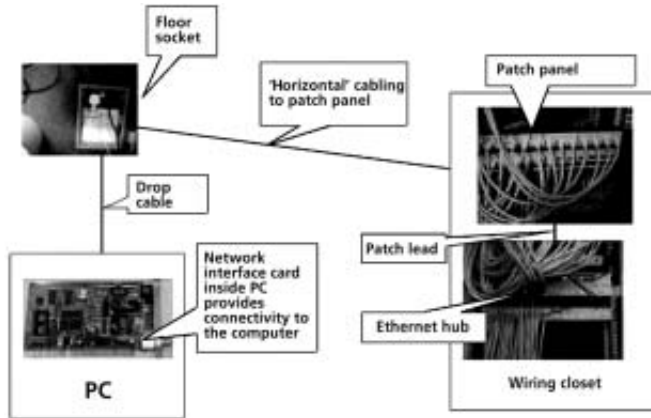


Figure 3.18 Typical structured cabling

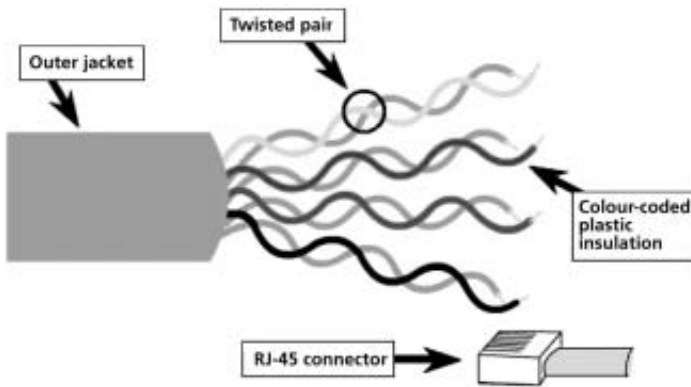


Figure 3.19 UTP cabling (diagram courtesy of CISCO Systems Inc.)



Figure 3.20 RJ-45 connector

CRUCIAL TIP

Structured cabling is now the standard in almost all new installations.

CRUCIAL CONCEPT

It is important to be able to remember the various topologies and to be able to draw these topologies.

Technologies

As well as having a physical shape, networks also need equipment in order for them to operate – for example, a network interface card (NIC), hub, etc. The equipment to support a network is known collectively as the technology (examples being the ethernet and token ring). The most popular technologies are discussed in detail in Chapter 5.

Quick test

1. Name the most common network topologies and discuss the differences between them.
2. For each of the topologies given, list any advantages/disadvantages.

Section 3

Network addressing and protocols

Computer networking is a complex business and requires rules to govern the communication. Such rules are known as protocols and are critical to computer networking. Most crucial of all is the open systems interconnection (OSI) seven-layer model for computer communication, which defines standards and protocols that are used extensively in the networking industry today.

Protocols

Computer communications are extremely complex, and there are many parameters that must be agreed before communication can take place. What was needed, therefore, was a standard (or protocol) for communication between computers. In other areas, this problem has been resolved by breaking down one large, complex problem into several smaller ones – for instance, with personal CD players the headphone jack is 3.5 mm, therefore, any headphones can be used; any audio-compatible CD played on a personal CD machine; any make of batteries can be used; and, if the player has a mains adaptor, it can be plugged into any mains outlet. This is because tight standards have been set that govern the production of all the pieces of equipment.

The same is true with networking: standards for networks were established and a model devised. This model, known as the open systems interconnection (OSI) seven-layer model, was devised by members of ISO (the International Standards Organisation). The layers of the OSI seven-layer model are shown in Figure 3.21, and the model is discussed in detail in Chapter 4. Prior to the model (which was devised in the early 1980s), vendors tended to produce proprietary network solutions, which reduced the end user's choice and limited the connectivity of the machine.

Application
Presentation
Session
Transport
Network
Data link
Physical

Figure 3.21 The ISO seven-layer model

The benefits the layered model brings are as follows:

- It breaks network communication down into smaller simpler parts that are easier to develop.
- It facilitates the standardisation of network components to allow multi-vendor development and support.
- It allows different types of hardware and software to communicate with each other.
- It prevents changes in one layer from affecting the other layers so that they can be developed more quickly.
- It makes networks easier to learn.

Whilst the seven-layer model brings many benefits, it has several disadvantages:

- Redundant functions and facilities are retained.
- Simple communication is made over-complicated because of structure overheads.
- The structure overheads reduce the overall performance.

CRUCIAL TIP

Apart from their importance in the real world of networking, the benefits and disadvantages of layered approaches to networking is a very common question in TCTs.

Logical and physical addressing

Devices on a network must be able to communicate directly with one another and must be uniquely identified. Communication can then take place in a way similar to the postal system: the sender addresses an envelope or package to a recipient (including a return address). The postal system examines the recipient's address and forwards the package as appropriate. This may involve the package being forwarded to another postal network or sorting office before being delivered to the recipient.

Computer networks operate on an almost identical principle. Each machine on the network has an address to which data can be forwarded. In order to reach its recipient, the package may have to cross multiple networks before it is delivered. On a computer, there are two possible addressing mechanisms:

- physical
- logical.

Physical addressing (also known as layer two addressing as it occurs in layer two of the model) mechanisms are used internally within an organisation. They use an address that is hardcoded on to the Media Access Control unit (MAC) – usually part of the networking card (i.e. the NIC). With ethernet networks, this is either a 16 or 48 bit field (usually the latter) that is unique across the world. Burnt into ROM and unable to be changed, the first half of the address identifies the manufacturer; the second half is the serial number within the manufacturer's ID. Thus replacing a card will change the MAC address. Whilst this is acceptable for local area networks where the address is circulated as the machine interacts, it would clearly be impossible to know the physical address of every machine in the world (and to keep that list up to date!). Thus another mechanism for addressing machines globally is needed – logical.

Logical addressing is used for three main reasons. To:

1. overcome the problem of a card change;
2. allow the demarcation of networks;
3. provide a structure to the addressing scheme.

The best analogy that can be drawn to logical addressing is the telephone network. If you purchased a phone and the serial number of that phone was your phone number, each time you changed the phone you would need to notify all your friends of your new number – something that is clearly undesirable. Also, as phones could be located anywhere in the world, when friends call the network would have to try every phone in the world to find out if it was yours – a huge waste of resources. Instead, the telephone network is structured. For example if you were to ring the University of Sunderland from outside the UK you would dial the following number:

00 44 191 5153000

The 00 routes the call from the local telephone exchange to an international one; the 44 routes the call to the UK; the 191 to the north east of England; the 515 to the University of Sunderland; and the 3000 is the number of the student helpline. This structure allows the telephone network to make much better use of its resources, and it allows demarcation of telephone networks – once the call has left one country/service provider it is the responsibility of another. Also, you can change your phone at will without having to notify your friends.

Logical addressing for networks is very similar. The most popular logical addressing mechanism is that used on the Internet – Internet Protocol (IP) addressing. With IP addressing, an organisation is issued a block of IP addresses from its Internet Service Provider (ISP), who is issued these by the Network Information Center in the USA (early in Internet development, the Network Info. Center would issue blocks of numbers, known as licences, directly to large organisations – see below). These numbers are 4 byte dotted decimal. For example:

157.228.102.1

CRUCIAL CONCEPT

We need to use logical addressing to provide a means by which we can structure traffic on the Internet and maintain independence from the MAC address.

Computers are thus grouped under the organisation's or ISP's network address, which are issued in licenses. Although these numbers are dotted decimal, they are actually a decimal representation of eight binary digits (a byte). The largest number that can be represented by a byte is 255 (all 0s are reserved for the network address and all 1s are reserved for the broadcast address; therefore the maximum available is 254). There are three possible types of licence:

- **Class A licences** These were intended for very large organisations and were mainly issued to universities in the US. In a class A licence, the first byte is fixed but the organisation is free to allocate addresses in the other bytes, giving it a maximum of $254 \times 254 \times 254 = 16.3$ million possible addresses on its network. Class A licences are no longer issued. In a class A licence, the leftmost bit is always zero. The largest number that can be represented is therefore 127 and thus the range is: 1–126. X. X. X (127 is reserved for the loopback address – a means of testing the network hardware and software on a computer).
- **Class B licences** These were also issued to large organisations – many universities in the UK hold a class B licence. With a class B licence, the first two bytes are fixed, giving the organisation a maximum of $254 \times 254 = 64\,516$ possible addresses on its network. Thus 157.228 uniquely identifies the University of Sunderland; the remaining parts of the address identify specific machines. Class B licences are very rarely issued now. The first two bits of a class B licence are always 10. Therefore the effective range is 128–191. X. X. X.

- **Class C licences** These are the most common and are still issued. In a class C licence, the first three bytes are fixed, giving the organisation 254 possible addresses on its network. The first three bits if a class C licence are always 110 therefore the effective range is 192–223. X. X. X.

Internet service providers (ISPs) either allocate IP addresses statically – that is to say, a machine always has the same IP address (a necessity for a web server), or dynamically – leased for a period (usually 24 hours), after which it needs to be reviewed. Logical addressing is also known as layer-three addressing because it occurs at layer-three of the OSI seven-layer model.

Subnetworks (subnets)

As can be seen from the above, with class A and B licences there would be a huge number of hosts on a network. If we take class A as an example, it is possible there could be 16.3 million computers on a single network. This is akin to having all the cars in the country on one road at the same time – there would be too much traffic and everything would grind to a halt. Just as the road network comprises many roads, the computer network can also be divided into smaller networks or subnetworks (often referred to as subnets). And just as with road networks, such a division reduces the load in each subnetwork enabling traffic to flow more freely. The key to good network design is traffic management (see Chapter 7).

The network is therefore divided using a subnetwork (or subnet) mask. As its name suggests, this is a mask (in the form of 4 bytes) that is applied to the IP number to determine the correct network for the traffic. The subnet mask is local to the organisation only (i.e. it is not transmitted outside the organisation) and is found in a computer's settings. In Windows this can be found in the Network Connections box or by running ipconfig (Windows XP and 2000) or winipcfg (in Windows 98) (Figure 3.22).

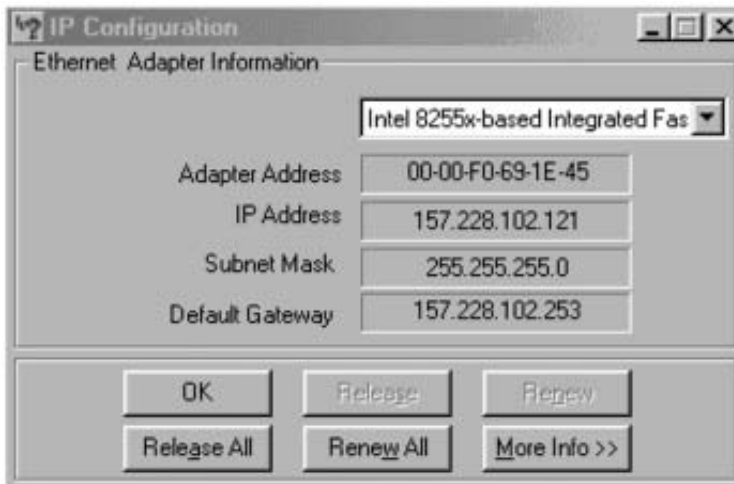


Figure 3.22 Ethernet settings (winipcfg in Windows 98)

In this example, we can see that the IP address is class B (157 is in the class B range). Where there is a value other than zero in the subnet mask, the corresponding part of the IP address is treated as part of the network. Each part of the IP address is a byte (with a maximum value of 255) – thus in the figure the subnet mask identifies that all the first, second and third bytes of the IP address relate to the network. Thus, host 121 is to be found on subnetwork 102 of major network 157.228 (see Chapter 11 for an example).

Section 4

End of chapter assessment

Questions

1. Discuss how data is encoded on to a medium and why a packet structure is used. You should use any necessary diagrams to illustrate your answer.
2. For each popular networking topology, draw a diagram illustrating the topology and highlight any advantages/disadvantages of the topology.
3. Discuss the terms 'logical' and 'physical' addressing. Highlight any differences and give an example of the use of each.

Answers

1. This question tests your knowledge of network basics. The assessor is trying to find out if you understand the fundamentals of computer communications – that we need to encode data as a voltage for transmission, that we use at least two voltages (and why); and that a packet structure is necessary. To answer it, you need to discuss how data is encoded on to the medium and why a packet structure is used. Wherever possible, you should illustrate your answer with diagrams.
2. Topologies are a common question and come in a variety of guises. Once you have learnt the topologies, tackling such a question is fairly easy – all you need to do is to draw a diagram of each of the topologies and to list their advantages and disadvantages. Drawing the diagrams is an essential part of the answer.
3. This particular question is trying to establish whether you know about the addressing mechanisms used in computer networking. The ideal answer to this question would discuss both terms separately, highlight any differences between them and discuss why these differences are necessary. You should illustrate your answer with examples of both addressing mechanisms and, for extra marks, highlight why the Internet could not run with physical addressing mechanisms. Comparing addressing schemes to either the postal service or the telephone network will impress the assessor and will earn you extra marks.

Section 5

Further reading and research

See the www.PhilipIrving.com website for up-to-date further reading and support for this chapter.

Cisco Networking Academy Program (2001) *First Year Companion Guide* (2nd edn) Cisco Press. ISBN: 1 58713 025 4. Chapters 1, 3 and 10.

Hodson, P. (2002) *Local Area Networks* (4th edn) Continuum. ISBN: 0 82645 866 1. Chapters 6 and 7.