ELEC S212

Network Programming and Design

Unit 2

Network infrastructure

香港公開大學
THE OPEN UNIVERSITY
OF HONG KONG

科技學院 *School of Science and Technology*

Course team

Developers:	Jacky Mak, Consultant John Wu, Consultant
Designer:	Ross Vermeer, ETPU
Coordinator:	Dr Philip Tsang, OUHK
Member:	Dr Steven Choy, OUHK

External Course Assessor

Prof. Cheung Kwok-wai, The Chinese University of Hong Kong

Production

ETPU Publishing Team

The Open University of Hong Kong
Ho Man Tin, Kowloon
Hong Kong

This course material is printed on environmentally friendly paper.

Contents

Overview

In this unit we continue on our journey into the subject of computer networking, by focusing on technologies related to the bottom layers of the OSI network model.

We will begin by addressing some fundamentals of data transmission, especially how to encode data into signals and transmit them from one end to the other over network media.

We will then explore different methods of physically arranging multiple parties and providing them with ways of accessing the network in a coordinated fashion. 'Switching', which is a key technology in the network access layer, will also be covered in this section.

The unit will end with an introduction to some networking equipment which provides the building blocks to construct real-life networks. Different types of devices have different characteristics and functions in taking up their roles in data networking.

In short, this unit:

- describes the core elements of a network infrastructure;
- explains basic network signal transmission concepts;
- discusses the most appropriate transmission media in respect to different circumstances;
- describes different network topologies;
- describes different types of access networks, and identifies their differences;
- explains the functionality of networking equipment including hubs, switches and routers; and
- outlines basic network design principles and tools.

Although the topics covered in this unit are fundamental in nature, from time to time there are new developments. For instance, there have been quite substantial advances in wireless technologies over the past few years. More and more cities, including Hong Kong, are mounting campaigns to make available ubiquitous Wi-Fi Internet access for the local community.

Transmission basics

In data networking, signals are used to represent data; ‘transmission’ is the processing required to pass signals from one end to the other over a transmission medium. Two signalling methods — analog and digital — are employed to execute transmissions. You will learn how both of these methods work in this section.

Signalling

Types of signalling

Both analog and digital signals are generated by an electric current, meaning that they are electromagnetic (EM) waves in nature. An analog signal, like other waveforms, is characterized by four basic properties: **amplitude**, **frequency**, **wavelength** and **phase**. The figure below depicts a typical analog signal, which takes the shape of a sine function.

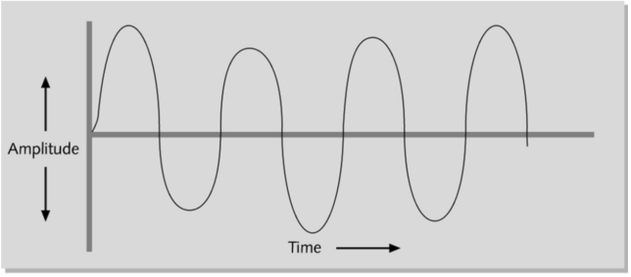


Figure 2.1 An example of an analog signal

Source: Figure 3.1, Dean 2004

In contrast to analog signals, digital signals take the shape of a series of pulses with precise positive and zero levels. The figure below shows you an example. This simple form of digital signal correlates well with the binary system of digital information, which is composed mainly of a train of digits, i.e. 0 and 1 (e.g. ‘1010101’). Converting binary data into a digital signal is therefore relatively straightforward.

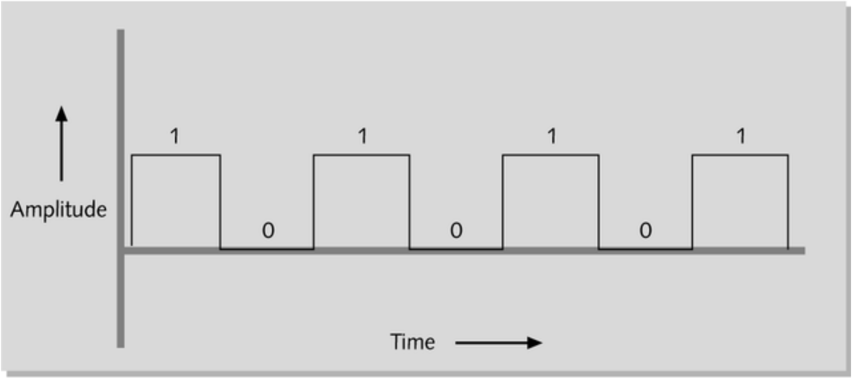


Figure 2.2 An example of a digital signal

Source: Figure 3.3, Dean 2004

While data transmission often relies on digital signals, in some cases analog signals must be used to suit specific types of transmission (e.g. dial-up networking on an ISP's network) or to support advance signal processing techniques (e.g. multiplexing). In such cases, data modulation is applied to combine an analog signal representing the original data (also known as a data wave) with another carrier wave to produce an output signal for transmission. The carrier wave has some preset properties including frequency, amplitude and phase which are subject to modulation. In FM (frequency modulation), the frequency of the carrier signal is modified by the application of data signal, while in AM (amplitude modulation), the amplitude is modified.

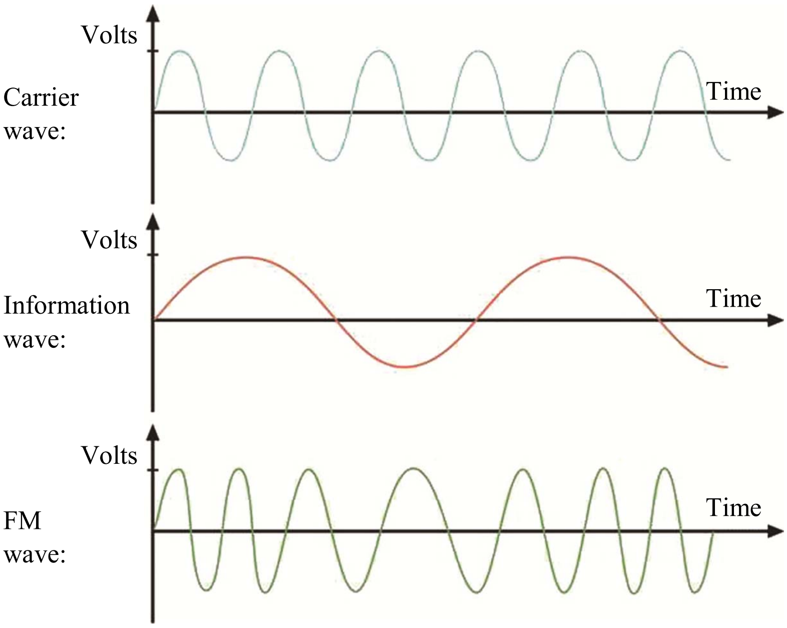


Figure 2.3 A carrier wave modified through frequency modulation

Source: Figure 3.5, Dean 2004. Alternative source: http://en.wikipedia.org/wiki/Image:Frequency-modulation.png

Transmission direction

Transmission direction is another important characteristic of data transmission. There are basically four types of transmission direction:

1 Simplex — signals can travel in only one direction.

2 Half-duplex — signals can travel in both directions over a medium, but in only one direction at a time.

3 Full-duplex — signals can travel in both directions over a medium at the same time.

4 Multiplex — multiplex signals are allowed to travel at the same time over one medium, with each signal assigned to a sub-channel.

Modern Ethernet networks are capable of full-duplex transmission when network switches are used to connect the network nodes. If network hubs are used, however, only half-duplex can be used. Later on, when you learn more about Ethernet, you will find out how this difference arises.

Throughput and bandwidth

Throughput is the measure of how much data is transmitted during a given period of time, often expressed as a quantity of bits transmitted per second (bps). For data networking, we often use the number of bits (using a small letter ‘b’ as short form) as measurement, for example Kbps, Mbps, etc. For data storage (e.g. hard disks, memory) on the other hand, we often use Bytes (using a capital letter ‘B’ as the short form), for example, KB, MB, etc.

In data transmission, it usually takes 10 bits to transfer 1 Byte of data. For 10 Mbps Ethernet, it takes one second to transmit 10 million bits or 1 million Bytes. The term ‘bandwidth’ is often used interchangeably with throughput, though to be exact, bandwidth is a measure of the difference between the highest and lowest frequencies that a medium can support.

Baseband and broadband

Baseband is a transmission form in which digital signals are sent through a wire without any adaptation. Baseband uses the wire capacity exclusively, thus allowing only one channel to transmit at a time. Traditional Ethernet is an example of a baseband system.

Broadband, on the other hand, is another transmission form in which data signals are modulated by carrier signals to become the output signals that hinge on different frequency ranges of the carrier signals. Broadband supports multiple signals, or channels, over one connection. ‘Broadband’ carries another meaning in reference to technologies (e.g. DSL for Internet access) capable of transmitting data at high transmission rates, in contrast with the ‘narrow band’ technologies (e.g. dial-up networking for Internet access).

You should now read the following pages from your Dean textbook for more in-depth information on these forms of transmission.

Reading

Dean (2012) 77–93.

Self-test 2.1

1 What are the advantages of analog transmission over digital transmission?

2 What are the advantages of digital transmission over analog transmission?

3 Give one example for each of the following: simplex, half-duplex and full-duplex transmission.

4 What is the main function of a modem?

5 Let's say you need to send a sequence of computer screen images over an optical fibre. The image files are in a raw format, i.e. without any compression. The screen is 480 × 640 pixels, each pixel being 24 bits. There are 60 screen updates per second. How much bandwidth is needed?

6 For 100BaseT Ethernet, what do '100' and 'Base' mean?

Transmission media

Media characteristics

When selecting a transmission medium, you should ensure that the characteristics of the medium can meet the technical and environment requirements. Different media vary in characteristics such as throughput, cost, size and scalability, connectors and noise immunity.

The reading below explains these characteristics.

> ***Reading***
>
> Dean (2012) 93–96.

Types of network cables

Three main types of cables are commonly used as guided media in data networks: coaxial cable, twisted pair cable and fibre-optic cable. Read on for details of each.

Coaxial cable

Coaxial cable has been in use in modern networks for a long time, but it rapidly gained in popularity due to the emergence of Ethernet in 1970s and 1980s. The enormous spread of Local Area Networks (LANs) that we see today would not be possible without coaxial cable. It therefore has a central place in the history of networking!

A coaxial cable consists of a central core copper wire surrounded by a hollow outer cylindrical conductor with dielectric materials filling the space between them, plus an outer plastic cover to protect the cable from physical damage. The figure below shows the structure of coaxial cable.

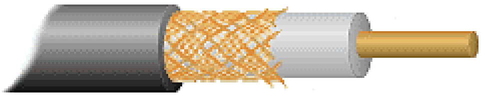


Figure 2.4 A coaxial cable

There are two types of coaxial cable: Thicknet and Thinnet. Thicknet, the original Ethernet medium, is designated as 10BASE-5, but it isn't used on modern networks. Thinnet cable has a smaller diameter, about 0.25 inches, with a designation as 10BASE-2 (i.e. 10 Mbps, baseband transmission, with maximum transmission length roughly at 200 metres). It relies on a bus topology. Thinnet is also almost never used in modern networks.

Currently, some broadband service providers such as Cable TV in Hong Kong elect to use coaxial cable. For example, the RG-6 coaxial cable leads from the wall terminator to the cable modem using an F-Type Connector (see the figure below). The modem then connects to the PC to provide broadband access.

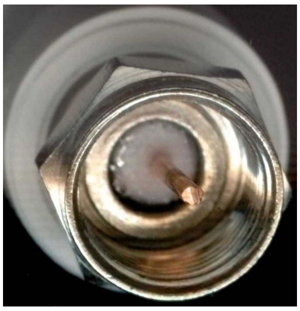


Figure 2.5 An F-type connector for coaxial cable

Source: http://en.wikipedia.org/wiki/Image:F_Connector.jpg

Twisted pair cable

Twisted pair cable is the most common media installed in modern LANs. It falls into two types: Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP). Twisted pair cables are relatively inexpensive, flexible and easy to install. They're frequently used in star or star-hybrid topologies.

The Telecommunications Industries Association and Electronic Industries Association's Commercial Building Wiring Standard 568 (EIA/TIA-586 standard) defines UTP as a standard in building and wiring. The following table lists some (just some, not all) of the UTP categories specified in the EIA/TIA-586 standard. Modern LANs use CAT 5 (i.e. Category 5) for Fast Ethernet and CAT 5e for Giga Ethernet.

Table 2.1 The EIA/TIA-568 standard for some of UTP cable types

Standard	Data rate	Digital/Analog	Brief description
CAT 1	Very low	Analog	Telephone line cables for analog voice communications
CAT 5	100 Mbps	Digital	Commonly used for Fast Ethernet
CAT 5e	1000 Mbps	Digital	Commonly used for Giga Ethernet
CAT 6/6e	> 1000 Mbps	Digital	Similar to CAT 5e with more stringent shielding against crosstalk and attenuation
CAT 7	> 1000 Mbps	Digital	Even higher standard then CAT 6, but its standardization is still in progress. It requires other types of connectors, but not RJ45.

A twisted pair cable consists of pairs of insulated copper wires, with every two wires twisted together to form twisted pairs. All pairs are encased in a plastic sheath. The number of twists per metre is known at the **twist ratio**. The higher the number, the better the protection against the 'crosstalk problem' (i.e. electrical interference) that may arise in adjacent wires. On the other hand, too many twists can also lead to a shorter transmission distance.

A shielded twisted pair (STP) cable not only has a protective sheath around each pair of wires, but also a shielding surrounding the whole bunch of wires. Unshielded twisted pair cable (UTP) does not have this protection.

Reading (optional) 2.1

You have just come across the names of two organizations: the Electronics Industries Association (EIA) and the Telecommunications Industries Association (TIA). They are both United States-based associations.

The EIA represents the entire spectrum of companies involved in the design and manufacture of electronic components, parts, systems and equipment. If you want to know more about this organization, refer to its homepage: https://www.ecianow.org/.

The TIA supports the growth and competitiveness of the communications and information technology industry through various activities, such as legislative efforts, international marketing opportunities, trade show sponsorship and standards development. TIA has a number of member companies that produce virtually all of the products used in modern communications networks. If you are interested in knowing more about this association, its homepage URL is http://www.tiaonline.org/.

A UTP cables has one RJ-45 connector (RJ stands for Registered Jack or Remote Jack) at each of its two ends (shown in the figure below). One is for connecting to the Network Interface Card (NIC) of the network node, and the other one is for connecting to a port of a hub and a switch.

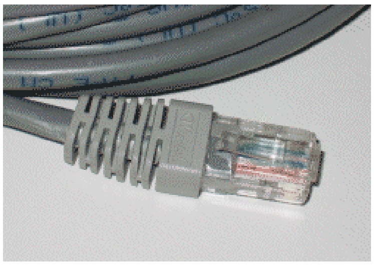


Figure 2.6 A RJ-45 Connector

Source: Figure 7.5, Dean 2004, 176

The EIA/TIA-T568 standards also provide a convention for wiring UTP cables in a RJ45 connector for Ethernet, which is shown in Table 2.2 below.

Table 2.2 EIA/TIA-T568-B wiring

Pin	Pair	Colour
1	2	white/orange
2	2	orange
3	3	white/green
4	1	blue
5	1	white/blue
6	3	green
7	4	white/brown
8	4	brown

When a UTP cable is used in Ethernet, the length limit for the cable is around 100 metres since signal attenuation makes long distance transmission unreliable. This limit may be extended by connecting the cables together with repeaters or hubs. For 100BASE-T Ethernet, such extensions are subject to the 3-2-1 rule, which means that between two communicating nodes, the network can contain at most three network segments connected by two repeating devices, and at most two out of the three segments can be populated with workstations. In total, around 300 metres of distance can be attained. Please see the figure below for an illustration.

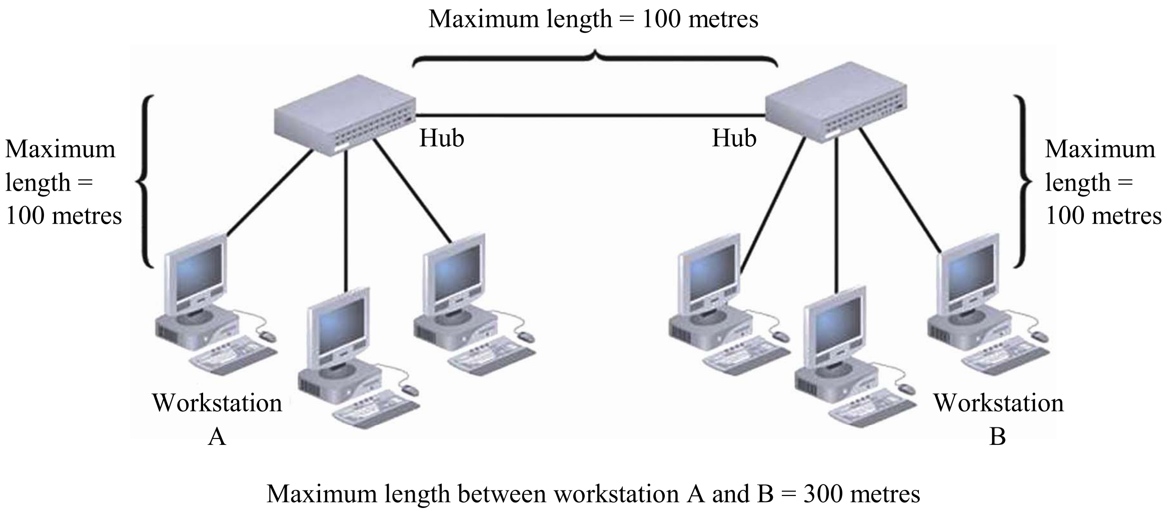

Maximum length = 100 metres
Maximum length = 100 metres
Hub
Hub
Maximum length = 100 metres
Workstation A
Workstation B
Maximum length between workstation A and B = 300 metres

Figure 2.7 A 100BASE-T network

Source: Figure 3.23, Dean 2004, 104

We will explain the distance limitations of UTP cable further in the section entitled ‘Shared Ethernet’.

With better shielding, STP cables have strong resistance to external interference and are thus capable of transmitting data for a longer distance. STP is also suitable for environments that have a high electromagnetic background, such as power plants.

Fibre optics

A fibre-optic cable contains one or more optical fibres. Each optical fibre is made up of an extremely thin strand of glass fibre, as shown in the figure below. Since it transmits data by sending modulated pulses of light, but not electromagnetic signals, a fibre-optic cable is immune to electromagnetic interference (EMI) and also less vulnerable to attenuation. The benefits of fibre optics are summarized below:

- high throughput
- high resistance to noise
- excellent security
- long distance transmission
- industry standard for high-speed networking, especially for backbone networks.

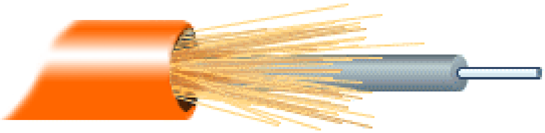


Figure 2.8 A fibre-optic cable

Source: Figure 3.24, Dean 2004

Fibre-optic cables are the most expensive type of cables, but they are capable of supporting higher data rates over longer distances. They fall into two categories: single-mode and multimode. The term ‘mode’ is used to describe the number of light paths supported by the medium:

- Single-mode fibre (SMF) has a smaller core that allows only one light pulse to propagate on its own path. It is suitable for accommodating high bandwidths and long distances such as connecting two carriers’ facilities.
- Multimode fibre (MMF) has a core with a larger diameter that allows many light pulses to propagate on their own paths. It is often used to connect a router to a switch or a server on the backbone of a network.

Connecting fibre-optic cables is difficult because of the fine precision required in alignment, and because light travels in a straight line. The implementation cost is therefore higher.

As is the case for coaxial cables and twisted pair cables, the IEEE also has defined standards for fibre-optic cables. 1000Base-LX refers to the Ethernet specification for fibre-optic cables, which is part of the IEEE 802.3 specification. The '1000' stands for 1000 Mbps, 'Base' for baseband and the 'LX' for the use of 'long wavelength' of 1300 nanometres. For 1000Based-LX, a multimode fibre supports a distance of up to 500 metres while a single-mode fibre up to 5 kilometres. The table below lists some cable standards.

Table 2.3 Physical layer networking standards

Standard	Maximum transmission speed (Mbps)	Maximum distance per segment (m)	Physical media	Topology
10BASE-T	10	100	CAT 3 or higher UTP	Star
10BASE-FL	10	2000	MMF	Star
100BASE-TX	100	100	CAT 5 or higher UTP	Star
1000BASE-T	1,000	100	CAT 5 or higher UTP (CAT 5e is preferred)	Star
1000BASE-CX	1,000	25	Twinaxial cable	Star
100BASE-FX	100	2000	MMF	Star
1000BASE-LX	1,000	Up to 550, depending on wavelength and fiber core diameter	MMF	Star
		5000	SMF	Star
1000BASE-SX	1,000	Up to 500, depending on modal bandwidth and fiber core diameter	MMF	Star
10GBASE-SR	10,000	Up to 300, depending on modal bandwidth and fiber core diameter	MMF	Star
10GBASE-LR	10,000	10,000	SMF	Star
10GBASE-ER	10,000	40,000	SMF	Star

Source: Figure 3.3, Dean 2004

The following reading summarizes the characteristics and limitations of physical layer networking standards that use coaxial cable, twisted-pair cable and fibre-optic cable.

Reading

For different types of transmission media read Dean (2012) 96–115.

Cable design and installation

Network cabling design is concerned with the selection of networking media, and how the selected media can be best used to maximize performance and minimize efforts on upkeep. Careful cabling design is important since it is not easy to relocate cables once they are laid. Proper documentation and labelling of cabling installations are also important for ongoing management. TIA/EIA 568 also covers various aspects related to structural cabling design, including entrance facilities, backbone cabling (or vertical cabling), equipment rooms, telecommunications closets, horizontal cabling and work areas.

In summary, there are numerous considerations in planning a cabling system:

- What types of cable should be used to fit the network topology and other technical requirements?
- How large an area should be covered?
- How many users is the network going to support?
- How heavy will the network traffic be?
- What level of resilience is required?
- What is the budget for the cabling work?

In the figure below, you can see a cable plant in an equipment room.

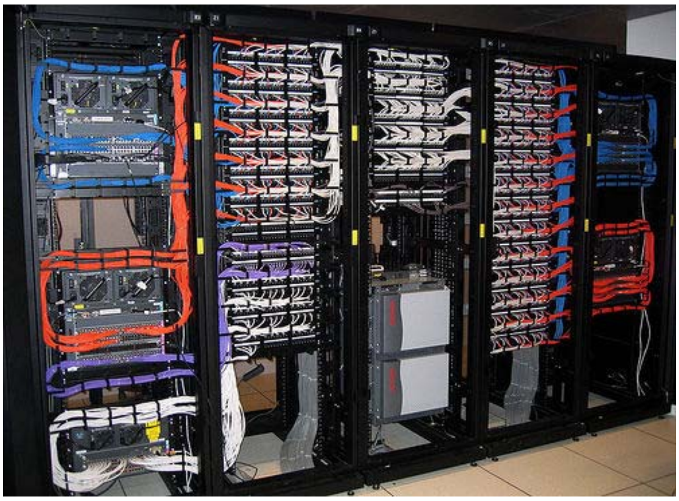


Figure 2.9 A cabling system in action

Source http://www.flickr.com/photos/51035711964@N01/16518187/

Reading

Dean (2012) 116–22.

Activity 2.1

At the link below you will find a tutorial on how to make CAT 5 UTP network cables. If you can gather the required tools, you can follow the tutorial to practice cable making. In particular, try to make a cross-cable, which may not be handily available at your office, but which is useful for troubleshooting network problems. What is a 'cross-cable'?

http://www.duxcw.com/digest/Howto/network/cable/

Self-test 2.2

1 Why do twisted pair cables need to have their wires twisted?

2 What is the standard EIA/TIA 568 concerned with? Why is it so important?

3 Do UTP CAT 1 (telephone line) and CAT 5 cables use the same type of connector? If not, what types do they use?

4 How does CAT5e cable differ from CAT5 cable?

5 Give an example of the use of coaxial cable for network transmission in Hong Kong.

Network topology

Network topology is concerned with how network nodes are physically arranged when connecting to a network, and how data is transmitted back and forth among the nodes within a network. Remember that all of the technologies and standards you have studied so far are confined to a single network segment. We have not yet considered the situation when different network segments operate together. We will do so later in this unit after we have introduced you to a few more basic topics.

Physical topologies

The physical topology refers to the physical arrangement for nodes connecting to a network. The choice of the physical topology should be in alignment to the transmission media, cabling design and network type. Different physical topologies vary in their scalability and implementation. Three basic types of topology are: bus, star and ring; we'll consider each in turn.

Bus

In the bus topology, a single cable (the bus) runs across the area, and nodes can be tapped into it at any point. This topology should be implemented with a transmission medium that allows physical multipoint access. On a bus topology network, every node receives the message sent over the network. A node will only respond to messages intended for it, and will ignore the rest. For transmitting data, a node first has to alert other nodes by sending a special signal. After it is clear that no other node is sending data, the node will start its transmission.

At both ends of a bus, a terminator is used to stop the signal bouncing back. Otherwise, the residual signalling bouncing around in the network will interfere with the current message under transmission. Refer to Figure 2.10 for the configuration of bus topology.

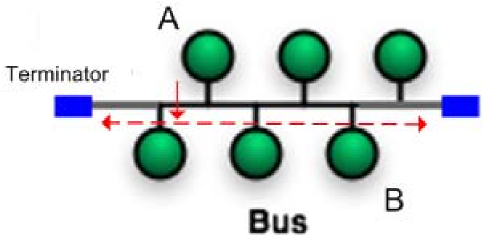


Figure 2.10 Bus topology

Source: http://en.wikipedia.org/wiki/Image:NetworkTopologies.png

Suppose Node A has a message to send to Node B. Node A delivers the message to the network bus through its network adaptor. The message propagates in both directions on the bus. All nodes tapped into the bus can receive the message, but only Node B, which finds itself as the recipient of the message, copies the message into its memory. You should note that Node B does not *remove* the message. The signal will continue its propagation in both directions until it arrives at the terminators, which then absorb the signal and thus clear up the bus.

Although a number of nodes can connect to a single bus, only one node can transmit data at one time. If two nodes send messages at the same time, a clash of the signals results. Because of this limitation, a bus cannot afford to include many nodes. Otherwise, the network will have too many clashes, making it of little use. Furthermore, a bus network is fairly fragile. A break in a bus (e.g. one of the joints connecting to a network node is broken) brings down the whole network.

Due to these shortcomings, you will rarely see a network run on a pure bus topology. However, you can see it in hybrid topologies in which the bus topology is used in combination with some other topology.

Ring

In contrast to the bus topology, the ring topology does not have 'ends' since the nodes are arranged into a circular shape. Each node has two links to its adjacent nodes. A message is transmitted in one direction, starting from the sending node and passing by each node down the chain until arriving at the destination node. Please see the figure below for a ring topology.

Similar to bus topology, if any node fails in the ring topology, it brings the whole network down. Also, the more nodes added to the ring, the slower the network performance will be. Unreliability and inferior scalability makes a pure ring topology impractical.

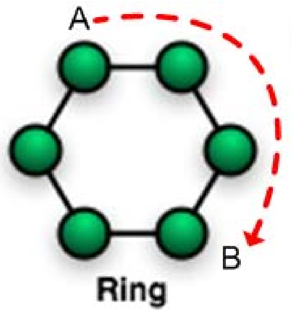


Figure 2.11 A typical ring topology

Source: http://en.wikipedia.org/wiki/Image:NetworkTopologies.png

Star

In a star topology, there is a central device to which all other network nodes are connected, resulting in a star shape, as shown in the figure below. Each connecting node attaches itself to the central device through a network cable (e.g. a twisted pair or optical fibre cable), which thus forms a point-to-point link. The central device has a number of physical **ports** for plugging into by one of the ends of a network cable, while the other end of the cable is plugged into the Network Interface Card (NIC) of the network node. A message sent out from a network node is first received by the central device, which then forwards the message to other connected nodes.

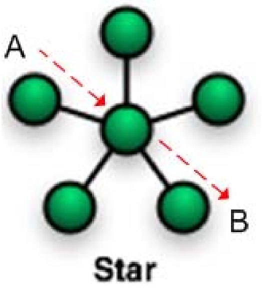


Figure 2.12 A typical star topology (using a network switch as the central device)

Source: http://en.wikipedia.org/wiki/Image:NetworkTopologies.png

If there is a defect in a network cable or a workstation malfunctions, it affects only the attaching workstation in question, but *not* any other network nodes connecting to the same central device. This ability to confine the impact of a defect or a problem makes the star topology more fault-tolerant than other topologies. Also, since it uses a centralized connection, networks can be easily reconfigured to add in more network nodes, or can be joined together with other networks, thus providing better scalability. Given these benefits, the star topology has become the mainstream topology deployed on modern networks, even though it often requires more cabling effort and higher costs.

Hybrid topologies

Except in very small networks, you will rarely encounter a network that follows a strict bus, ring or star topology. Simple topologies are too restrictive, particularly if the LAN must accommodate a large number of devices. More likely you will work with a complex combination of these topologies, known as a hybrid topology. Here are a couple of common hybrid configurations:

- **Star-wired ring topology**

  Physically, a star-wired ring topology may appear to be identical to a star topology. The MAU (multistation access unit) of a star-wired ring, which serves as the central device, contains wiring that allows information to pass from one device to another in a circle or ring. This topology is used in Token Ring networks.

- **Star-wired bus topology**

  Network nodes can be connected to several central devices, which are then linked together to form a bus link, namely a trunk. If one network node goes down, the other nodes will not be affected. But, if one central device goes down, the whole network will be at least partially paralyzed since the trunk is broken up by the dysfunctional device. In practice, redundancy has to be built into the trunk to ensure that it is fault-tolerant. Nevertheless, the star-wired bus topology still enjoys the advantage of being scalable and flexible. It is often used in modern Ethernet networks.

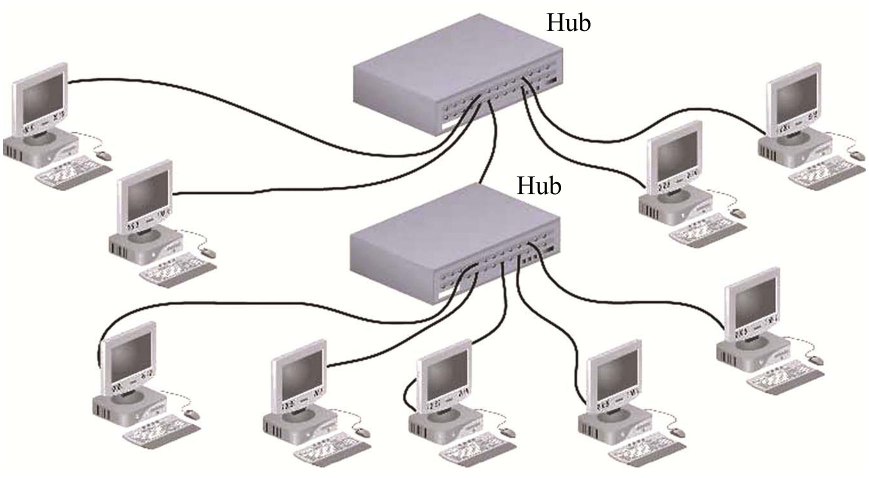


Figure 2.13 A star bus topology

Source: Figure 6.5, Dean 2004, 291

Backbone networks

A network backbone is the cabling that interconnects various central devices including hubs, switches and routers on a network. Normally, the backbone's capacity should be greater than the networks connected to it so that it can handle the relatively high network traffic that aggregates from the connecting segments. Otherwise it may become a bottleneck and impede the performance of the whole network.

Among its other functions, a network backbone can provide a path for the exchange of information between different sub-networks. Designing a backbone network for an enterprise environment is challenging since such an environment will typically consist of many network nodes, various computer systems, and a number of sub-offices. Two typical types of backbone networks are introduced below.

Collapsed backbone

In a collapsed backbone, there is only a single router or switch that serves as the single central connection point for multiple sub-networks. This central point is the potential single point of failure, so it has to handle very heavy network traffic. A collapsed backbone supports the interconnection of different types of sub-networks and eases the management efforts by centralization.

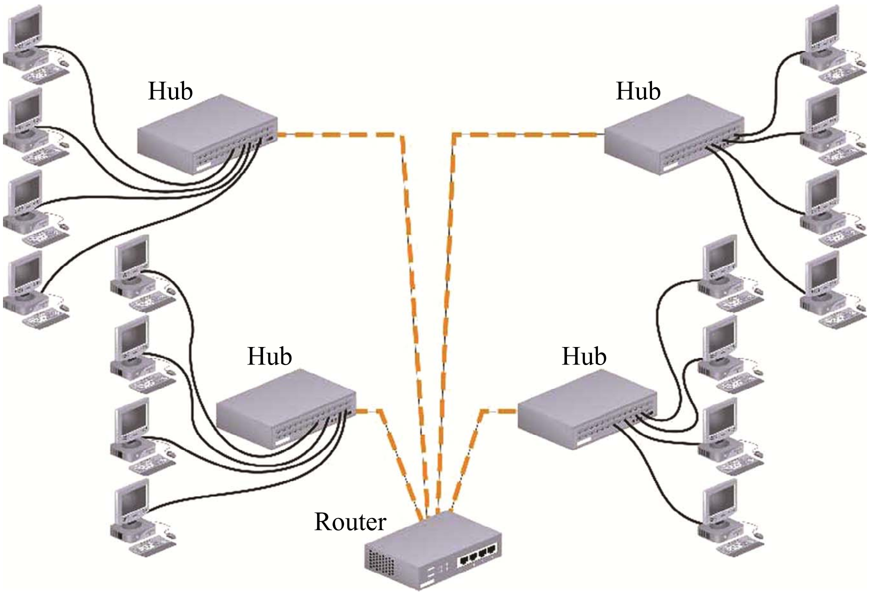


Figure 2.14 A collapsed backbone

Source: Figure 6.9, Dean 2004, 295

Parallel backbone

This is a variation of the collapsed backbone that builds in more than one connection from the central router or switch to each sub-network. Given these redundant links, the network becomes fault-tolerant because it eliminates the 'single point of failure' problem that the collapsed backbone bears. In return for their higher reliability, however, parallel backbones are more expensive to implement. They are commonly used in networks with high availability requirements.

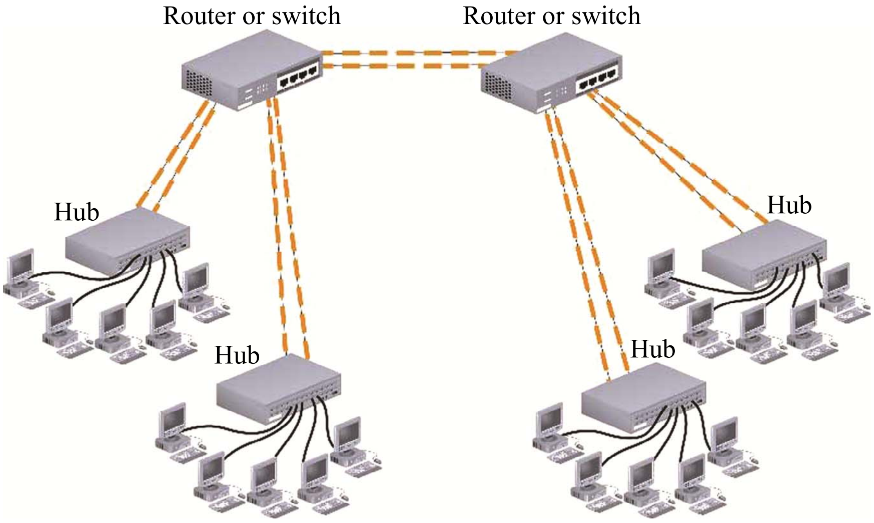


Figure 2.15 A parallel backbone

Source: Figure 6.10, Dean 2004, 296

Reading

Dean (2012) 199–209.

Self-test 2.3

1 What are the primary advantages of using a star topology network over a ring or bus topology?

2 What happens if a node in a star topology network fails?

3 Which type of cable are you most likely to find on networks that use a bus topology?

Logical topologies

Logical topology refers to how data is transmitted back and forth among the nodes within a network. It is concerned with how a network's logical interconnections between nodes are formed, rather than its physical interconnection. Bus and ring are the two most common logical topologies. Token Ring networks use the ring logical topology although they also normally use the star physical topology using a MAU (multistation access unit) as the central point.

Network switching

The bus or star logical topologies mentioned above suffer scalability problems. They allow only one node in the network to transmit data at a time. If there are a large number of nodes in the network, the contention among the nodes will become so acute that the network performance will decline significantly.

Network switching is another logical topology that offers a solution with better scalability. In effect, it creates a temporary connection between any two connecting devices whenever they need to transmit data between each other. Logically, a point-to-point link is formed between the two connecting devices in which contention will not occur.

Packet switching

You should note that the preceding discussion of logical topologies has been confined to the data transmission between the nodes within a single sub-network. But what about the logical topologies for transmission across different sub-networks? Think about the transmission of data from the originating node to the destination node in which the path may span a number of interconnected networks.

This is not a new issue. Telephone systems addressed this kind of issue decades ago through circuit switching technology. For data networking, however, packet switching is used to solve the problems. The next reading introduces three switching methods: circuit switching, message switching and packet switching.

Reading

Dean (2012) 209–11.

Be very careful: the **packet switching** described in the above reading is targeted at the Internet layer operation (or Layer 3). It is associated with network routers in practical implementation. Meanwhile, the **network switching** described in last section happens at the Data Link layer (or Layer 2), in association with network switches in practice. Both of these employ switching as the underlying technique, but they deal with *different layers of operation*. Just don't get confused!

Self-test 2.4

1 What is the essential difference between message switching and packet switching?

2 What are the key differences between circuit switching and packet switching?

Network access technologies

Now that you have worked through some fundamental concepts in data networking, you may want to know how networks work in the real world. Our textbook introduces you to a number of technologies including Ethernet, Token Ring, FDDI, ATM and Wireless Networks. While you will learn about each of them in detail by referring to the readings recommended at the end of this section, we will first select two of them for further examination: Ethernet and Wireless Networks.

Introduction to Ethernet

Ethernet is a networking transport method originally developed by Xerox in the 1970s and later improved by Xerox, Digital Equipment Corporation (DEC) and Intel. Although it came into existence over 30 years ago, Ethernet is far from dying. On the contrary: it has been flourishing with new advances arising from time to time. Ethernet's access method has evolved from shared Ethernet to switched Ethernet. Its speed has increased from 10 Mbps to up to 10 Gbps. Its scope has expanded from LANs to WANs (e.g. Metro Ethernet).

In view of all these developments, Ethernet is inarguably one of the most influential technologies in modern data networking, and thus worthy of further examination. It is still used extensively for LAN access all over the world for all kind of organizations, business corporations and households. You may have an Ethernet network in your home!

The Ethernet employs CSMA/CD (Carrier Sense Multiple Access/Collision Detection) and a back-off strategy as its access method for governing the shared use of the network media among the network nodes.

Carrier Sense (CS)

Each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If another node is already transmitting on the cable, the computer will wait and try again when the line is clear.

Multiple Access (MA)

MA is a technology that supports the ability of multiple nodes accessing the network together, especially if they need to share the use of network media in a coordinated fashion.

Collision Detection (CD) and back-off

Sometimes two nodes attempt to transmit at the same instant. When this happens, a collision occurs. The nodes stop transmitting, and send a jam signal down the network to notify others of the collision. Each node then backs off and waits a random amount of time before attempting to retransmit. The delay caused by a collision and retransmitting is small and does not normally affect the speed of transmission on the network. In the figure below, two nodes listen to ensure that the cable is idle, and then transmit. However, when Node 1 transmitted a portion of the signal, Node 2 did not receive it and thus began its own transmission. This resulted in a collision.

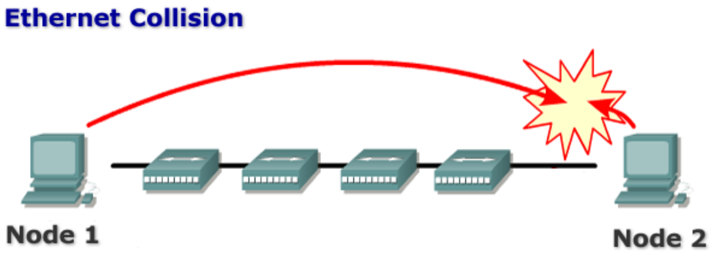


Figure 2.16 An Ethernet collision

Collision domain

The shared Ethernet protocol normally uses the star-wired bus topology in which the nodes are linked together by hubs. The so-formed Ethernet network is under a **collision domain**. Therefore, one cannot expand an Ethernet network too far, i.e. it cannot serve too many users. If too many users send a message, too many collisions will arise due to intensive contention among the nodes. A collision domain can be split up using higher-layer connectivity devices such as switches and routers to reduce collisions.

IEEE 802.3 specifications

Ethernet comes in a variety of implementations. Each Ethernet version follows a slightly different IEEE 802.3 specification with variation in its speed and cabling characteristics. The following list describes some of the Ethernet physical layer varieties:

- **10BaseT** — uses twisted-pair cabling (the source of the letter ‘T’ in its name) and a star topology to transmit data. Its data rate is up to 10 Mbps. It’s in common use.

- **100BaseTX** — Fast Ethernet was developed to drive throughput from 10 Mbps to 100 Mbps. It comes in a number of variants. The most commonly-used of these is 100BASE-TX, which uses two pairs of Cat 5 cable, one in each direction. There is also 100BASE-T4, in half-duplex transmission with 100 metres over the four pairs of Cat 3 or above cable, and 100BASE-T2 in full-duplex with 100 metres over two pairs of Category 3 or above, but they were developed too late to make much of an impact. 100BaseFX is similar to 100BaseTX except it uses fibre optics as the media.

- **1000Base-T** — Also known as Gigabit Ethernet, supporting a data transfer rate of 1 Gbps. The most commonly-used standard over twisted pair is 1000BASE-T, which uses four pairs of Cat 5e. There is also 1000BASE-TX, which is cheaper to implement, but requires Cat 6 cable and therefore has met with little success. On the other hand, 1000BaseFX and 1000BaseSX offer alternatives that ride on fibre optics. They are suitable for use in backbone cabling which may need to span long distances.

- **10GBase-CX4** — 10G Ethernet is still under development. 10GBase-CX4 is the first standard for 10-gigabit Ethernet over copper cable, which offers a cheaper alternative to optical fibre cables. It uses four pairs of twin-axial cable (coax with the centre core replaced by a twisted pair) with a connector based on that used for Infiniband (a type of high-performance cable connector).

The following table summarizes these Ethernet specifications:

Table 2.4 Ethernet specifications summary

	Speed	**Distance**	**Media**	**Connector**
10BaseT	10 Mbps	100 m	UTP Cat 3 or better	RJ45
100BaseTX (Fast Ethernet)	100 Mbps	100 m	Two pairs of UTP Cat 5 or Type 1 STP	RJ45
1000Base-T (Gigabit Ethernet)	1G bps		UTP Cat 5 or better	RJ45
1000BaseFX/SX	1G bps	500 m/3 km	Optical fibre	SFF MT-RJ or Duplex SC
10GBase-CX4	10G bps	15 m	Twin-axial cable	XAUI (10 Gig Attachment Unit Interface)
10GBase-SR	10G bps	26 m–82 m	Optical fibre	SFF MT-RJ or Duplex SC

Shared Ethernet

Traditional Ethernet LANs (shared Ethernet) supply a fixed amount of bandwidth that must be shared by all devices on a segment. Stations cannot send and receive data simultaneously, nor can they transmit a signal when another station on their segment is sending or receiving data. This is therefore half-duplex transmission.

The worst-case scenario happens when the two most-distant nodes on the network both need to send a signal, and the second node does not begin transmitting until just before the signal from the first station arrives.

Referring to the figure below, we assume the end-to-end propagation delay to be τ. At time t_0, Node A finds the link idle and transmits data. Node B still finds the link idle until it receives the first bit of the frame from Node A. If B starts transmitting data at a time just before the frame from Node A arrives (at a time near $t_0 + \tau - \varepsilon$), a collision occurs, and Node B detects it immediately. However, Node A will not see the collision until the corrupted frame reaches it at a time about $t_0 + 2\tau - \varepsilon$.

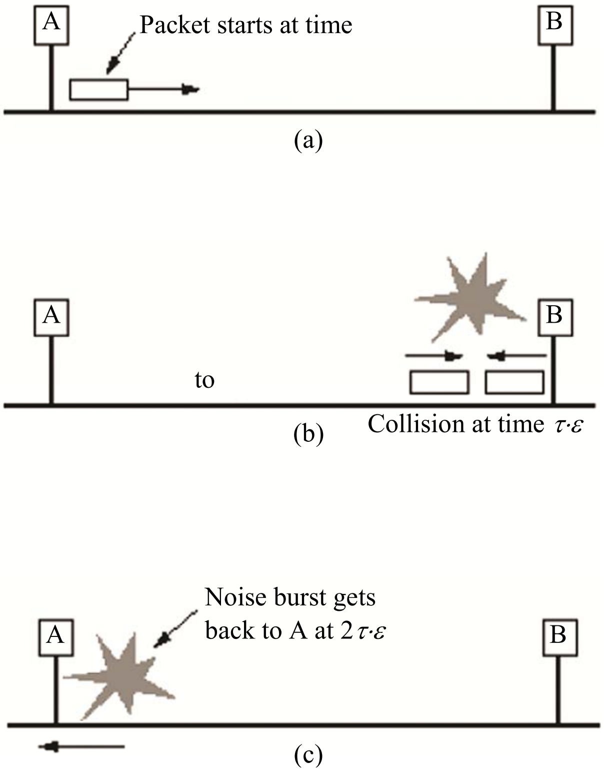

A
Packet starts at time
B
(a)
A
B
to
(b)
Collision at time $\tau{\cdot}\varepsilon$
Noise burst gets
back to A at $2\tau{\cdot}\varepsilon$
A
B
(c)

Figure 2.17 An illustration of shared Ethernet collision

If the transmission time for Node A is shorter than 2τ, Node A will complete the transmission before knowing about the collision. This results in an unreliable transmission: Node A thinks that the transmission is successful, but actually it is not. So, the transmission time has to be greater than 2τ. This imposes a minimum frame size in the Ethernet.

The following example shows that the minimum size for an Ethernet frame should be $2\tau C$, where C is the speed of the link in bits per second.

Assume the time for transmitting a frame be t and the frame size be s:

$$t = s/C$$

As discussed above, the transmission time has to be greater than '2τ':

$$t >= 2\tau$$

$$s/C >= 2\tau$$

$$s >= 2\tau C \quad \ldots\ldots\ldots \; (*)$$

In 10 Mbps Ethernet, the maximum transmission distance is defined in IEEE 802.3 as 2.5 km, while the propagation speed is 2 x10^8m/s. So:

τ = 2.5 km/2 x 10^8m/s = 12.5μs

$s >= 2\tau C$, i.e. 500 bits

The minimum frame size for 10 Mbps Ethernet is 512 bits. But what happens for Fast Ethernet (100 Mbps)? It increases the transmission speed (i.e. *C*) by 10 times, while the maximum propagation speed (which depends only on the characteristics of the transmission medium) and thus the delay τ should be about the same. By the equation (*) above, either the minimum frame size is increased by the same factor (10 times), or the transmission distance is reduced by around that factor. The actual solution for Fast Ethernet over UTP is to set the maximum transmission distance to around 300 metres. But why not 250 metres (2.5 km/10)? It's because the propagation speed of the UTP (made of copper wire) is lower than 2 x 10^8m/s (which is light speed), thus allowing a bit longer transmission distance.

Switched Ethernet

Switched Ethernet has emerged as a newer Ethernet model that enables multiple nodes to simultaneously transmit and receive data and individually take advantage of more bandwidth because it forms temporary circuits (i.e. point-to-point links) between the two communicating nodes through network switching topology. Do you remember 'network switching'? Go back and revise that section if necessary.

Switched Ethernet can also support full-duplex operation for Ethernet. With UTP cables, Ethernet can use two separate wires for sending and receiving, thus allowing simultaneous two-way transmission between two nodes. As a result, there is no media contention, no collisions, and no need for extension bits on the end of short frames to meet the minimum frame size requirement. This not only makes more time available for transmission, but also effectively doubles the link bandwidth, because each link can now support full-rate, simultaneous, two-way transmission. As switch hardware costs drop, switched Ethernet has been widely adopted in various environments.

Power over Ethernet (PoE)

The IEEE has defined 802.3af for PoE (Power over Ethernet). Supplying electricity over an Ethernet network to the end devices can be useful in making it possible for certain types of application. The prime example is VoIP (Voice Over IP) application. Currently, a VoIP end device (i.e. a telephone set) can directly connect to a network switch over a RJ 45 connector for both data communication and power supply. This makes the implementation much simpler.

Wireless access

Other than physical cables (i.e. guided medium), the atmosphere (also known as an unguided medium) can be used to provide an intangible means of transporting data over networks. This type of network is known as a wireless network. For LAN scale implementation, a wireless network typically uses radio frequency (RF) or infrared for signalling. Unguided media are suited to specific environments in which physical cabling may not be feasible, or operation requirements require a network connection to be made over the air so that it is more flexible (e.g. Internet connectivity for visitors in an open area).

We need not to go into the details of wireless networking now since we have a dedicated unit on wireless network technology coming later in the course. For the moment, you just need to get familiar with a couple of basic concepts and technologies.

IEEE 802.11 WLAN standards

The IEEE has released a series of standards in the name of 802.11 on Wireless Local Area Network (WLAN). 802.11b and 802.11g are the most popular ones for public adoption.

Table 2.5 WLAN standards

Standard	Speed/ operating frequency	Features
802.11b (Wi-Fi)	11 Mbps, 2.4 GHz	Original WLAN standard
802.1g	up to 54 Mbps, 2.4 GHz	Most popular standard
802.1a	up to 54 Mbps, 5 GHz	In rare use now

CSMA/CA

802.11 standards specify the use of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). It works in similar fashion to Ethernet CSMA/CD. In this case, however, whenever a network node wants to send out data, it will hold back for a brief, random period, even though it knows the media are clear. Also, the receiving node will explicitly acknowledge the receipt of data to the sending node. This increases the network overheads, causing slower network performance, but it can provide better reliability, which is more essential considering the volatility of the wireless medium.

Association

On a wireless network, network nodes first have to associate themselves to one of the Access Points (APs) of the wireless network. Each wireless network identifies itself with a SSID (Service Set Identifier). Network nodes should select the SSID corresponding to the wireless network they intend to join to carry out the association.

Please refer to the reading below for more about other wireless network access technologies.

Reading

Dean (2012) 354–64.

You should now be ready to tackle the following activity and self-test before you go on to the next topic.

Activity 2.2

A medical instrument company operates a warehouse in which a network infrastructure using wireless LAN (WLAN) capability has been implemented. After the company received a huge contract, the operation of its warehouse become very busy and various activities took place non-stop. The inventory shelves are being stocked to the ceiling. Machines that carry merchandise along a conveyor belt are working round the clock.

As a result of all this activity, the company has faced quite a few network problems. Several inventory specialists in the warehouse are complaining that occasionally their handheld computers will not connect to the network, or that they suddenly lose their connection. It is especially frustrating because more personnel than ever are trying to use the network.

How would you help solve these problems?

Self-test 2.5

1 What are the two potential causes of collisions in Ethernet networks?

2 What is the difference between a logical and a physical topology?

3 What is the main advantage of switched Ethernet over shared Ethernet?

4 Ethernet (10 Mbps) frames should be at least 64 bytes long to ensure that the transmitter is still going in the event of a collision at the far end of the cable. Fast Ethernet (100 Mbps) has the same 64-byte minimum frame size, but can get the bits out ten times faster. How it is possible to maintain the same minimum frame size?

5 Which radio frequency bands are specified for use by the 802.11a, b and g standards?

6 At what layer of the OSI model do 802.11 (wireless) standards operate?

7 Which of the 802.11 (wireless) transmission requirements contributes to its inefficiency?

Networking equipment

After studying the fundamental network concepts and technologies, you now move on to look into the networking equipment that comprises the building blocks for constructing real, operable networks. In data networks, repeaters, hubs, bridges, switches and routers handle the task of directing information to the correct destinations. You will learn what these devices are meant for, and how they work. You will also study network interface cards (NICs) in detail, including how to physically connect a workstation's NIC to a network.

Repeaters and hubs

A repeater is a connectivity device with only two ports: one for input and one for output. It operates at the Physical layer to regenerate and amplify an analog or digital signal. Repeaters are mainly used in the bus topology to extend a network's physical span. However, they are in rare use nowadays.

A hub functions in similar ways to a repeater, except that it supports multiple ports. Network nodes that are wired to a hub share a single network segment and belong to the same **collision domain**. That means they may crash with one another when they try to send data over the network. Advanced-model hubs support management functions. An administrator can easily configure and monitor a sizeable number of hubs in an enterprise environment. Hubs can also be stacked together to form a bigger hub to support more network nodes.

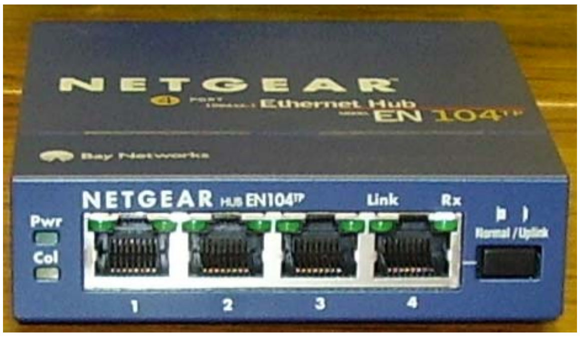


Figure 2.18 A 4-port hub

Source: http://en.wikipedia.org/wiki/Image:4_port_netgear_ethernet_hub.jpg

Bridges

A bridge is a device that connects two physical network segments by analysing incoming frames and making decisions about where to direct them based on each data frame's Media Access Control (MAC) address. Each NIC bears a global unique MAC address and each data frame, which represents a unit data in Data Link layer (Layer 2), will have both a source MAC address and a destination MAC address to determine from which node the frame has departed, and to which node the frame is destined. A bridge can intelligently make a decision about whether or not to forward a frame based on this pair of addresses, in contrast to repeaters and hubs which merely regenerate any received data signals without looking into them.

As you can see from the figure below, a bridge establishes a forwarding table of known MAC addresses and their locations on the network. If Node 1 sends data to Node 2, the bridge will not forward the data from Port A to Port B. But, if Node 1 sends data to Node 5, the bridge will do the forwarding.

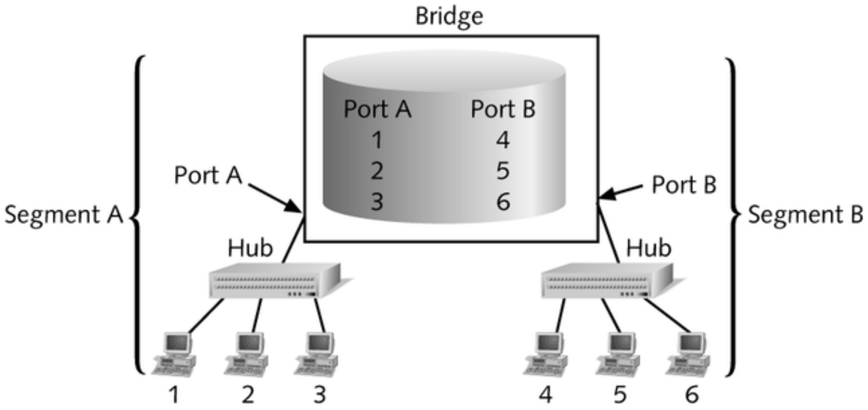


Figure 2.19 A bridge's use of a forwarding database

In effect, a bridge can break down a large network into two smaller and more efficient ones. Or, to be more precise, it splits up a collision domain into smaller ones and thus improves the performance of the network by lessening the chance of collisions among the connecting nodes. Like a repeater, a bridge has a single input and single output port. Unlike a repeater, however, a bridge can interpret the data it retransmits. Bridges are rare now, since they have mostly been replaced by switches, which are introduced in the next section.

Physical vs logical network segments

Note that a bridge simply disjoins two physical network segments, breaking them into separate collision domains. A bridge doesn't do anything about the logical network segment, however. Referring to the figure above, all network Nodes 1 to 6 belong to the same sub-network, or the same broadcast domain. To break up a logical network segment, you have to use a Network layer (Layer 3) networking device, i.e. a router.

Don't worry if you are not completely comfortable with these statements. You will be able to understand them all after you finish some more units later in the course.

Switches

In the previous section, i.e. ‘Switched Ethernet’, you learnt that instead of each network node vying for the shared channel on a single segment of 10 Mbps Ethernet, switch devices allow single nodes (or groups of devices) to ‘own’ their own dedicated channels (e.g. 100 Mbps in Fast Ethernet). They also support inter-segment communication in a fashion similar to the operation of the bridge, as explained in last section.

Operating like bridges, switches can subdivide a network into smaller collision domains. Through this subdivision, a switch prevents the unnecessary flow of network traffic from one segment to another, but only allows those intended for cross-domain transmission.

A switch has many more ports than a bridge. Modern switches can also support management functions that make them easy to manage. This is an important feature considering the fact that there often are tens of switches and networking devices existing in a single enterprise environment. Another key switch feature is their support of Virtual Network (VLAN), which will be explained in the next section.

Figure 2.20 A 48-port enterprise grade switch

Source: http://en.wikipedia.org/wiki/Image:Linksys48portswitch.jpg

Virtual networks (VLANs)

Even if switches are used, we still cannot put too many nodes on a single network. We may still need to group nodes into separate virtual networks (logical network segments). In addition to boosting performance, virtual networks can address the need to allocate network nodes in multiple network segments, thereby providing the following advantages:

- better security
- alignment with organizational structure to ease resources management
- isolation of heavy traffic from others
- support for legacy systems.

The network segment referred to here is the Layer 2 segment, which is also called a broadcast domain. All nodes within a broadcast domain receive network broadcast messages altogether (e.g. ARP and RARP broadcasts, which will be introduced in a later unit dealing with TCP/IP), even though they may belong to different collision domains. (Check out what a collision domain is from previous sections if you have forgotten it!) Each VLAN represents a subnet in TCP/IP.

VLANs can be designed flexibly. We can logically group the ports of a switch into one or more VLANs. Also, you can include ports from more than one switch to form a VLAN. See the figure below for an illustration of this point. Nodes attached to different VLANs cannot communicate with each other, but by using a Layer 3 or above device (e.g. a router) inter-VLAN communication can be made possible. VLANs have gained huge popularity nowadays.

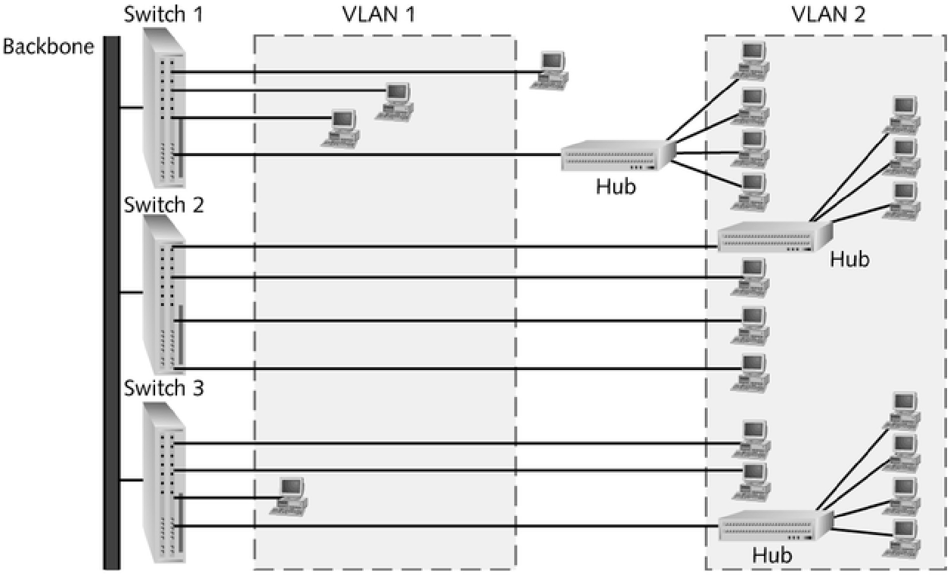


Figure 2.21 A simple VLAN design

Routers

A router is also a multiport connectivity device, operating at Layer 3. A router translates information from one logical network segment (i.e. sub-network) to another, with each segment comprising a broadcast domain. In other words, a router can be used to subdivide a broadcast domain into two or more. It can stop network broadcast messages at its boundary, without letting them get into other logical network segments.

The main function of routers is to cooperate with each other to select the best path to route a packet from the source network to the destination network. This path can be composed of a number of intermediate networks, with different transmission speeds and using a variety of protocols. Routers make internetworking possible, that is the ability to form a 'network of networks'. A prime example of such internetworking is the Internet, which actually consists of numerous numbers of networks joined together by routers. Communication between routers is often made according to routing protocols. The typical ones include RIP, OSPF, EIGR and BGP. You can refer to the next reading to learn more about them.

There are some types of switches that can also perform routing functions, e.g. routing switches, brouters (bridge router), etc. However, dedicated hardware routers are also in broad use, due to their higher performance.

The basic functions of a router include:

- connect networks, including dissimilar ones
- interpret Layer 3 addressing and other information
- determine the best path from source to destination networks
- reroute traffic if a primary path is not available
- filter out network broadcasts.

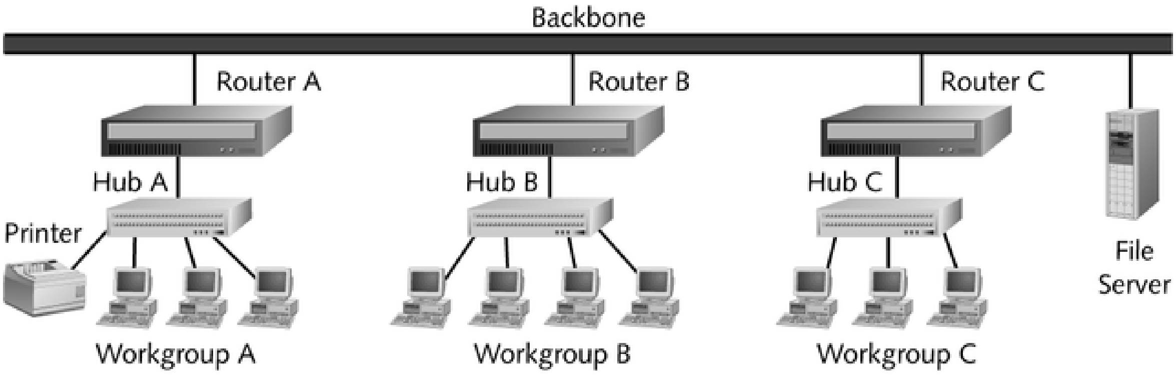


Figure 2.22 A simple router configuration

Reading

For different types of networking equipment read Dean (2012) 254–74.

Activity 2.3

Please access the Internet to find out more about the latest technology developments from Cisco, a major networking equipment manufacturer. Some suggested links are:

http://www.cisco.com/c/en/us/products/index.html

What networking trends or new products did you notice from information above? Discuss your findings with your tutor during the next tutorial, or with other students through the OLE discussion forum.

Self-test 2.6

1 What are the major differences between hubs and switches?

2 Assume your office is running an Ethernet LAN. If you need to connect five additional stations on the next floor into the existing network, what is the most effective way to do so?

3 State the major differences between switches and routers.

4 Do you know of any standards relating to Virtual Networks (VLAN)?

You should now be ready to undertake your next lab activity. You'll need your ICT Lab Book.

Activity 2.4

Lab: Networking fundamentals

Please complete *Lab 2.2 — Networking I: Fundamentals of the ICT.* Upon completing the lab, you will be able to learn some basic networking tasks on a UNIX/Linux system, and understand more about how computer networks operate in the real world.

Activity 2.5

Case study: Network design for ACME Engineering Ltd (an imaginary company)

ACME Engineering Ltd is a company newly founded by a group of electrical engineers. They have selected a new office in Kwun Tung, occupying one single floor comprising about 5,000 square feet. The founders have planned to employ around 20 staff with about 10 of them being professional engineers.

A network infrastructure and a few essential network applications need to be set up in the office. The applications needed include file/print and data backup services for all staff, and an engineering application for the engineers. More applications might be added in the future, depending how the business plays out. Since it is a start-up company, the budget is not generous! In order to outsource the work to a contractor, ACME's founders have to come up with some requirements. Let's see how far you can help them in this task.

1 Transmission medium

Cables and trunks should be laid so that servers as well as workstations for all staff can be connected to the network. Considering the number of staff, type of applications, and physical environment, what type of medium should be used?

2 Physical topology

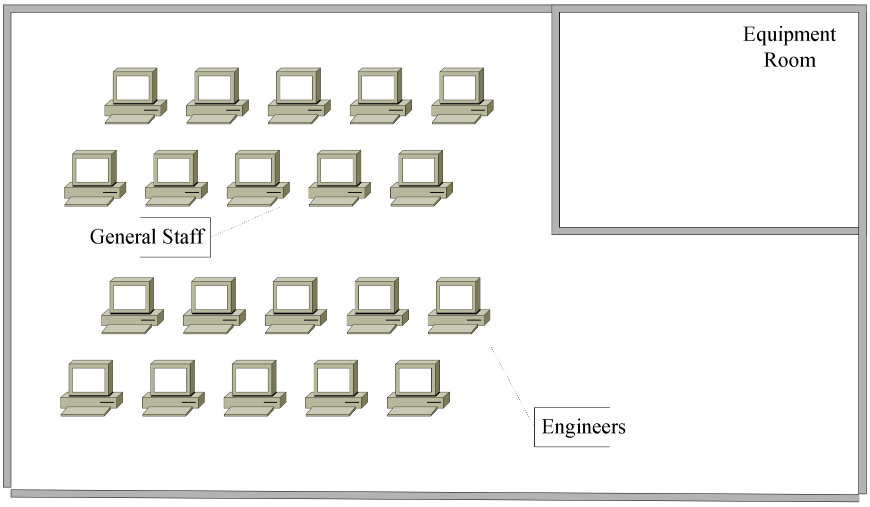
All 20 staff will be provided with a networked PC, and the number of staff may eventually grow to around 40. A small equipment room will be available to house the servers and network equipment centrally. What type of network topology would you recommend?

3 Network access technology

Network access technology needs to work in tandem with the transmission medium and physical topology. It should also support the required number of network nodes, future growth and types of applications. What would you recommend for ACME, and why?

4 Networking equipment

After considering the above requirements and provisions, you will need to select the networking equipment to get the network design implemented in a cost-effective manner. What type of networking equipment should be used, and why?



ACME Company

Summary

In this unit you have studied a number of fundamental networking concepts and technologies. This foundational study will help you go on to tackle further networking and programming topics in coming units.

To start off, you learned about technologies related to the Physical layer, including signalling, transmission media and physical topologies. You looked into different types of network cable including coaxial, shielded and unshielded twisted pairs and optical fibres. All of these cable types have different characteristics that can suit different environments and technical requirements. Physical topology is concerned with how to use the selected cables to connect the nodes together physically to form a network. You should now be able to visualize block diagrams of a computer network with these topologies, and be aware of the pros and cons of each of them.

Getting further down the protocol stack, we started to see something logical and conceptual, rather than physical. Different network access methods, which are related to the logical topology of a network, were introduced. A network is shared by multiple nodes. The access methods provide ways different nodes can share the use of the physical transmission media in an efficient manner. You studied Ethernet in detail, including shared Ethernet, switched and Ethernet at different speeds such as 10 Mbps, 100 Mbps and 1 Gbps. This is on a par with Ethernet's substantial influence in modern networking technology, and its vast popularity. Wireless access was also examined briefly, with key issues highlighted. Wireless technology is believed likely to become the mainstream access technology in the near future.

Finally you were introduced to some of the major types of networking equipment that provide the building blocks of real networks. This equipment includes repeaters, hubs, bridges, switches and routers. Each has different functions and features, with particular roles in data networking. Go back to read through these descriptions again if you still feel unsure of them, since they are indispensable to practical network design.

In next unit you will study TCP/IP, which is the defining network model nowadays, and which has made possible what the Internet has become today. You will start from the top of the stack, the Application layer, and then work down one by one through the Transport layer, Network layer, and finally the Link layer.

Suggested answers to self-tests and activities

Self-test 2.1

1 Analog signals can convey greater subtleties with less energy than digital signals. An analog signal can vary its amplitude continuously, while a digital signal can only vary its amplitude on predetermined discrete levels — but not anywhere in-between these levels. In addition, digital transmission requires many pulses to transmit the same amount of information that an analog signal can transmit with a single wave. That means analog transmission is more efficient.

2 Digital transmission is less susceptible to transmission flaws such as noise or any type of interference that may degrade a signal, than are analog signals. Also, digital signals are in much better alignment with the format of digital data, which is composed of a series of 0s and 1s.

3 Simplex transmission: TV broadcasts

Half-duplex transmission: Walkie-talkies, original Ethernet networks

Full-duplex transmission: telephone communication, switched Ethernet networks

4 A modem's main purpose is to function as a modulator and demodulator.

5 The data rate is 480 x 640 x 24 x 60 bps, which is 442 Mbps.

6 '100' and 'Base' means 100 Mbps and baseband respectively.

Self-test 2.2

1 The wires of twisted pair cables are twisted to reduce interference both between pairs, and from external sources such as electric motors or fluorescent lights.

2 EIA/TIA is regarded as the master standard on 'Structure Cabling', which is in common use nowadays. In 1991 EIA/TIA released their joint 568 Commercial Building Wiring Standard, AKA structured cabling, for uniform, enterprise-wide, multivendor cabling systems. The standard suggests how cabling may best be installed to maximize performance and minimize upkeep. It's based on a hierarchical design that divides cabling into six subsystems: entrance facility, backbone (vertical) wiring, equipment room, telecommunications closet, horizontal wiring and work area.

3 No, UTP CAT 5 cables use RJ-45 connectors, while UTP CAT 1 cables uses RJ-11 connectors.

4 CAT5e has a higher twist ratio, a better grade of copper and more EMI shielding.

5 Hong Kong Cable Television Limited (HKCTV) offers telecommunications services, including broadband services, using cable modem technology over its coaxial cable network that covers extensive residential and business areas in Hong Kong.

Self-test 2.3

1 A star topology network is more reliable because it connects each node or device to the network with a separate physical connection. Any failed node will not cause the whole network to go down, as will happen with a ring or a bus topology network. It is also more scalable because additional devices can be added inexpensively without affecting the performance of the network.

2 As mentioned above, any failed node will not impact the network except that the node itself will not be able to use the network to send/receive data properly.

3 The coaxial cable.

Self-test 2.4

1 Message switching sends data units that can be arbitrarily long. Packet switching has a maximum packet size. Any message longer than that is split up into multiple packets.

2 Below is a brief comparison showing the differences between circuit switching and packet switching.

	Circuit switching	**Packet switching**
1 Need call setup process?	Required	Not required
2 Need dedicated physical paths?	Required	Not required
3 Data arrives in order?	Yes	No
4 Charging also depends on transmission distance?	Yes (e.g. IDD)	No (e.g. broadband Internet)

Self-test 2.5

1 The first cause is propagation delay, which is the time a signal takes to traverse from a source PC to a destination PC. For example, Node A may sense that the medium is free and start to transfer while the fact is that Node B has already sent out a signal onto the network that has not yet reached Node A due to propagation delay. This will become more apparent if the length of the network is long. Another potential cause is when two PCs both sense a free line and access the media at the same instant. The chance of this happening increases if the number of nodes in the network is large.

2 Logical topology is concerned with how a message will be passed from the source node to the destination node. Physical topology is concerned with the physical layout of the network, and how nodes are physically connected to each other.

3 Its higher network throughput. In shared Ethernet, all nodes with a network share the network bandwidth. For a 10 Mbps shared Ethernet with 10 nodes, each node can effectively enjoy around 1 Mbps. But for a 10 Mbps switched Ethernet, each node can effectively enjoy the bandwidth in full, i.e. 10 Mbps.

4 The maximum length in Fast Ethernet should be cut down to around 1/10 as long as in Ethernet. For 802.3 10 Mbps Ethernet, it has a maximum length of 2500 m. Therefore, the maximum length for Fast Ethernet should be around 250 m–300 m. However, this is also subject to the characteristics of the media selected for transmission.

5 802.11a–5G, 802.11b–2.4G, 802.11g–2.4G.

6 The Data Link layer.

7 A destination node must issue an acknowledgement (the ACK packet) for every packet that is received intact.

Self-test 2.6

1 Hubs are Layer 1 devices, which simply regenerate the received signals and broadcast them to all other connected nodes. All connected nodes share the network under the same collision domain. Whereas, switches are Layer 2 devices, which can not only regenerate a received signal but also look into it in order to determine which connect node is the destination and send it to that intended node only. Switches can split a collision domain into smaller ones to lessen the contention among the connected nodes. Other differences lie in the fact that switches are added with management functions and the support of VLANs (Virtual Networks).

2 There are a number of different ways to extend an Ethernet segment. To determine which method is best, we should consider such factors as physical distances, cost, number of new stations and future growth. Since the five additional stations are connected to the existing network, the most effective way to link them with the network is by adding another new hub or switch, which can have either eight ports or 12 ports, depending on anticipated growth in the future. We also assume that the physical distance between the floor with the existing network and the next one will not be longer than 100 metres so that 10BaseT can be used. Considering that the difference in cost between a hub and a switch is not significant, and that the switch offers better performance, we should select the switch in this case.

In short, adding an 8-port switch will be a cost effective way to expand the network to accommodate the new users. In fact, the cost of a moderate 8-port switch is only a thousand Hong Kong dollars or so.

3 Switches are designed to provide services up to the Data Link layer (Layer 2). It works on the data transmission amongst the nodes within the same logical network segment, i.e. *intra*-segment. All nodes are within the same broadcast domain. In contrast, routers are designed to provide services up to the Network layer (Layer 3). Routers handle data transmissions amongst nodes that may be located in different logical network segments, i.e. *inter*-segment transmission. Nodes can belong to different broadcast domains. We can use a switch if there is only one network segment. As the number of nodes grows up to certain levels, however, we need another network segment to accommodate the new users, where a router will come into play.

In addition to expansion, security and ease of management are other reasons that influence the requirements of additional network segments. As a result, we will often see switches and routers in large networks, especially those at the enterprise scale, that need to take up different networking roles.

4 IEEE 802.1Q is a standard that defines the operation of Virtual LAN (VLAN), which permits the definition, operation and administration of Virtual LAN topologies within a Bridged/Switched Ethernet LAN infrastructure. Please also note that there are other standards defined on VLAN by other organizations or hardware vendors.

Activity 2.1

A crossover cable is a type of network cable used to connect computing devices together directly where they would normally be connected via a network switch, hub or router. For example, one would use a crossover cable to directly **connect two personal computers** via their network adapters. A crossover cable may be envisioned as a cable with one connector following T568A and the other T568B.

Activity 2.2

In designing a WLAN, we should select Access Points (APs) that have sufficient power, and strategically place them so that receiving devices can communicate with them. Obstacles standing in the way of signals between the APs and receiving devices will affect the communication adversely. So, the company may consider *relocating the APs* in order to get around the blocking effect caused by the inventory shelves whose height has reached the ceiling. In addition, the conveyor belt system may generate EM interference, which may weaken the WLAN signal. Advice should be given to the staff to *avoid using the wireless handhelds around the area near the system*. Lastly, check the number of users that the existing APs can accommodate. If necessary, put in some more APs *to expand the capacity of the WLAN* to meet the growth in the user population.

Activity 2.3

Unified communication, especially VoIP (Voice over IP), and next generation WLAN standard IEEE 802.11n are the 'flavour of the month' these days. They will remain major trends in coming years.

Activity 2.5

Feedback on the case study

The following sections include some related discussion and suggested answers for the questions in the case study. They may differ from your ideas and answers. However, this may not matter as long as you can substantiate your answers with sound reasons since there are various ways to go about those questions. Do consult your tutor if in doubt.

1 Transmission medium

The number of workstations is around 40 total. The physical distance between nodes should be within tens of metres (floor size: 22 m x 22 m, or about 5,000 sq. ft). Only office automation applications are required, which are not too demanding on network services. Based on these factors, using optical fibre cables is not justified, because of their high cost, and because they are usually used for cross floor connections or connecting locations in different buildings. Coaxial cables are actually not used now. UTP CAT 5e cables would be a good choice. They are low cost while supporting around 100 m and high speed up to 1GMbps. Wireless is a viable alternative, but it is less reliable and secure. Also, wireless equipment is more expensive (e.g. NIC for UTP is one quarter the cost of that for wireless).

2 Physical topology

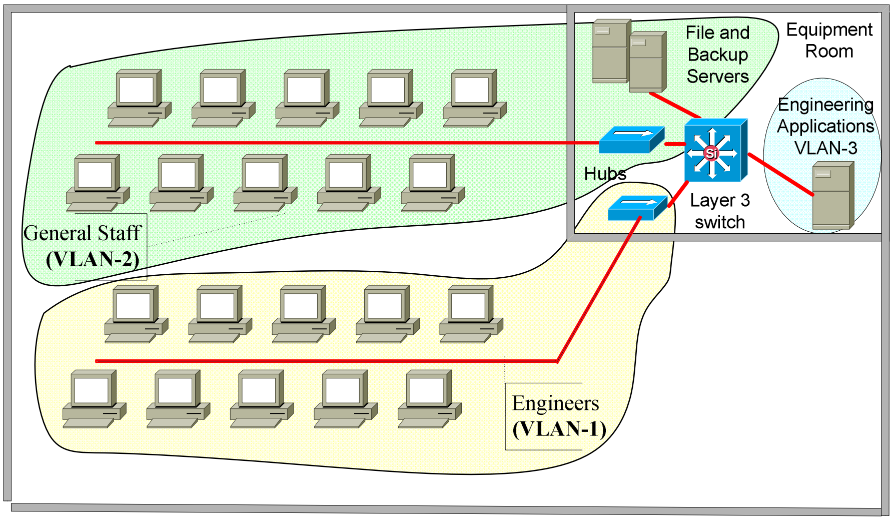
Star and bus topologies can be considered for their flexibility in installation. However, UTP works better with a star topology, and it also provides flexibility for adding PCs to the network when more staff are added. So a star topology is recommended.

3 Network access technology

Considering the client's requirements and the above choices, Fast Ethernet should be recommended. Not only can it meet all requirements, but it also offers very good performance with transmission rates of 100 Mbps. As Fast Ethernet is becoming more common, its implementation cost is affordable and its products are mature. 10 Mbps Ethernet is a bit too conservative, while 1GMbps may not be a cost effective choice.

4 Networking equipment

Hubs will be used to connect the workstations together and link them up to the backbone switch. Direct switch ports will be given to the servers. VLANs will be implemented to separate the general staff from the engineers to ease ongoing management. Also, the engineering applications are put under a single VLAN (i.e. VLAN-3), which is allowed to communicate with VLAN-1 only where the engineers reside. A Layer-3 backbone switch will be chosen so that it can act as the router to handle inter-VLAN traffic. All of this equipment will be housed in the equipment room. Below is a diagram that illustrates the design.



ACME Company

Glossary

10Base2 — Ethernet specification for thin coaxial cable. Transmits signals at 10 Mbps with a distance limit of 185 metres per segment.

10Base5 — Ethernet specification for thick coaxial cable. Transmits signals at 10 Mbps with a distance limit of 500 metres per segment.

10BaseF — Ethernet specification for fibre-optic cable. Transmits signals at 10 Mbps with a distance limit of 1000 metres per segment.

10BaseT — Ethernet specification for unshielded twisted pair cable (category 3, 4 or 5). Transmits signals at 10 Mbps with a distance limit of 100 metres per segment.

access control methods — rules that govern how nodes on a network access the cable.

analog data — information composed of continuous varying values, such as voice and video.

analog signal — a continuous signal that varies constantly in voltage. The value of the signal varies all the time during transmission.

analog transmission — transmission of analog signals over wires or through the air in which information is conveyed through variation of some combination of signal amplitude, frequency and phase.

baseband — a term defining any network in which only a single signal is allowed to transmit in a single cable at the same time. It is common in LANs and is simpler and cheaper than broadband. Ethernet is an example of a baseband network.

bit — a binary digit in the binary numbering system. A bit's value can be 0 or 1. In an 8-bit character scheme, it takes 8 bits to make a byte of data.

BNC connector — a standard connector used to connect 10Base2 coaxial cable. Different sources expand BNC as Bayonet Navy Connector, British Naval Connector, Bayonet Neill Concelman or Bayonet Nut Connection.

bridge — a device that connects and passes packets between two network segments that use the same communications protocol.

broadband — also referred to as wideband; a term describing any network that allows multiple signals to be transmitted on a single cable at the same time. Different frequencies of electromagnetic waves are used to encode the signals, and transmissions do not interfere with each other. In LAN terminology, 'braodband' refers to a system in which multiple channels access a medium, e.g. coaxial cable that has a large bandwidth using Radio Frequency (RF) modems. This allows the coaxial cable to carry multiple separate LANs whose transmission is being modulated at different frequencies. In cable television, broadband describes the ability to carry 30 or more TV channels and is synonymous with wideband.

bus topology — a network topology in which each node attaches directly to a common cable.

byte — a group of 8 bits.

cable — transmission medium of copper wire or optical fibre wrapped in a protective cover.

Carrier Sense Multiple Access with Collision Detect (CSMA/CD) — a network access method in which devices that are ready to transmit data first check the channel for a carrier. If no carrier is sensed, a device can transmit. If two devices transmit at once, a collision occurs, and each computer backs off and waits a random amount of time before attempting to retransmit. This is the access control method used by Ethernet.

client/server network — a networking system in which one or more file servers (the server) provide services, such as network management, application and centralized data storage for workstations (the clients).

coaxial cable — cable consisting of a single copper conductor in the centre surrounded by a plastic layer for insulation and a braided metal outer shield.

digital data — information composed of discrete values such as bits.

digital link — a link on which digital signals can be transmitted.

digital signal — a discrete signal, such as a sequence of voltage pulses, varying between two constant values, usually denoted as 0 and 1. A digital signal changes between two set values without intermediate variations.

digital transmission — transmission of digital signals over wires or through the air.

Ethernet — a network protocol invented by the Xerox Corporation and developed jointly by Xerox, Intel and the Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types originally at 10 Mbps.

Fast Ethernet — a new Ethernet standard that supports 100 Mbps using category 5 twisted pair or fibre-optic cable

Fibre Distributed Data Interface (FDDI) — a 100 Mbps/ANSI standard LAN architecture, defined in X3T9.5. The underlying medium is optical fibre (though it can be copper cable, so it may be called CDDI) and the topology is a dual-attached, counter-rotating Token Ring.

fibre-optic cable — see optical fibre cables.

frame — a term for the unit of data transferred on a network. The size depends on the type of network implemented — hundreds or thousands of bytes long (any particular type of network will have a limit on the frame size; e.g. Ethernet's 1500 byte limit). The terms 'cell', 'datagram', 'message', 'packet' and 'segment' are also used to describe logical information groupings at various layers of the OSI reference model.

gateway — a device that connects two systems, especially if the systems use different protocols.

gigabit — one billion bits of information; one thousand megabits.

hub — a hardware device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (when they repeat signals sent through them) or passive (when they do not repeat but merely split signals sent through them).

Protocol — allows for electronic mail and the accessing and retrieval of information from remote sources.

link — transmission link composed of physical media such as coaxial cable for connecting nodes in a network.

Local area network (LAN) — a network connecting computers in a relatively small area, such as a building.

megabit — one million bits.

Megabit per second (Mbp) — one million bits per second; a unit of information transfer rate. For example, Ethernet can carry 10 Mpbs.

modem — a device that converts digital and analog signals. Modems allow computer data (digital) to be transmitted over voice-grade telephone lines (analog). The name comes from modulator/demodulator.

network topology — the physical layout of the network; how the cables are arranged, and how the computers are connected.

node — the end point of a network connection; nodes include any device attached to a network such as file servers, printers or workstations.

optical fibre cable — a cable, consisting of a central glass core surrounded by layers of plastic, that transmits data using light rather than electricity. It has the ability to carry more information over much longer distances.

packet — originally, a unit of data sent across a packet-switching network. Currently, the term may refer to a protocol data unit at any layer.

point-to-point — a direct link between two objects in a network.

ports — connection points for a cable.

protocol — a formal description of a set of rules and conventions that govern how devices on a network exchange information.

repeater — a device which propagates electrical signals from one cable to another; less intelligent than a bridge, gateway or router.

ring topology — network topology in which a series of repeaters are connected to one another by unidirectional transmission links to form a single closed loop. Each station on the network connects to the network as a repeater.

RJ-45 — standard connectors used for unshielded twisted pair cable. RJ stands for 'Registered Jack' or 'Remote Jack'.

router — a device that routes information between interconnected networks. It can select the best path to route a message, as well as translate information from one network to another. It is similar to a super-intelligent bridge.

shielded twisted pair (STP) — See twisted pair cable.

star topology — network topology in which each node on a network is connected directly to a central network hub or concentrator.

switches — network device that filters, forwards and floods frames based on the destination address of each frame. The switch operates at the data link layer of the OSI model.

terminator — a device that provides electrical resistance at the end of a transmission line. Its function is to absorb signals on the line, thereby keeping them from bouncing back and being received again by the network.

transceiver — from transmitter/receiver; a device that receives and sends signals over a medium. In networks, it is generally used to connect two different types of cable connectors, such as RJ-45.

Transmission Control Protocol over Internet Protocol (TCP/IP) — the *de facto* standard Ethernet protocol incorporated into 4.2BSD UNIX. TCP/IP was developed by the Defense Advanced Research Project Agency (DARPA) for internetworking, encompassing both network layer and transport layer protocols. Whereas TCP and IP specify two protocols at specific layers, TCP/IP is often used to refer to the entire US Department of Defense (DoD) protocol suite based on these, including Telnet, FTP and UDP.

tree topology — a network topology similar to bus topology, except that tree networks can contain branches with multiple nodes.

twisted pair cable — network cabling that consists of four pairs of wires that are manufactured with the wires twisted to certain specifications; available in shielded and unshielded versions. The shielded version (STP) has a stronger outer protective coating than the unshielded (UTP) version.

unshielded twisted pair (UTP) — see twisted pair cable.

Wide Area Network (WAN) — a network connecting computers within very large areas, such as states, countries and the world.

workstation — a computer connected to a network at which users interact with software stored on the network.

References

Online materials

https://www.ecianow.org/

http://www.tiaonline.org/