ELEC S212

Network Programming and Design

Unit 9

Wide area network access and wireless technologies

香港公開大學
THE OPEN UNIVERSITY OF HONG KONG
科技學院 School of Science and Technology

Course team

Developer: Jacky Mak, 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 what has seemed the blink of an eye, we've now come to *Unit 9*, i.e. the penultimate unit in this course. In this unit, we will cover the topics related to Wide Area Networks (WANs) and wireless communications. Understanding the power of these technologies helps explain how computer networks can stretch their reach across long geographical distances, connecting distant homes, offices and other premises. In some areas in which laying network cables is either infeasible or impractical (e.g. providing network connectivity to the public at a busy main street in a central business area), wireless networks can overcome networking problems. This unit will explain how.

WAN and LAN technologies are complementary in nature. They work together to provide long- and short-haul network connections to meet the varying needs of different businesses and organizations. Enterprises can use a WAN to connect their headquarters and branch offices together while using LANs for connections within each of these offices.

We start the unit with a comparison of these two complementary technologies. Then we go on to explore different types of WAN technologies. In particular, we cover the local landscape of WAN services, and introduce Metro Ethernet, which is a new kind of WAN technology whose usage is skyrocketing (though it is not mentioned in your textbook).

Throughout this unit, we focus our attention primarily on wireless communications. The reason for so doing is obvious: wireless communication has been proliferating at an unprecedented speed over the past few years. For example, the OUHK completed the provision of Wi-Fi connectivity throughout its campus last year. Many other local institutions and organizations have endeavoured to complete similar initiatives to exploit the benefits of wireless technologies. The government also embarked on its own Wi-Fi program in 2007, and started to provide free wireless Internet access services to citizens at designated government premises in early 2008. This unit will enable you to understand these wireless technologies, especially those that have been infused into our daily lives. A range of wireless network protocols and wireless LAN design models are discussed in the unit, and you'll learn that, after six years, IEEE will finally approve the 802.11n standard in mid-October 2009, meaning that the era of high speed wireless LAN connectivity will be coming soon.

Another topic that we cannot afford to miss is wireless network security, because wireless medium is more vulnerable to attack than physical medium.

In short, this unit:

- describes the operation and types of WAN technology;
- outlines the local developments in WAN services;

- discusses basic issues related to wireless communication;
- outlines wireless network protocols and standards;
- describes common wireless security measures and standards; and
- analyses security issues for wireless networks.

In addition, some labs on wireless technology, with reference to the textbook *A Practical Approach to Internet Programming and Multimedia Technologies*, have been incorporated into the unit to help you consolidate what you have learned.

Last but not least, we end the unit with a discussion of a WLAN survey in the educational context, with reference to another textbook, *IEEE802.11 WIFI Survey & Visualisation Experiments*.

WAN (Wide Area Network) essentials

A WAN is a network that traverses some distance and that usually connects LANs, whether across buildings, the city or the country. Most WANs arise from the simple need to connect one building to another. As an organization grows, its WAN might grow to connect more and more sites, located across the city or around the world.

LANs and WANs lie at Layers 1 and 2 of the OSI Model. The following table shows their differences.

Table 9.1 A comparison of LAN and WAN technologies

	LAN	WAN
Coverage	Covers a small geographic area, like a home, office, or group of buildings	Covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries)
Technology	Tend to use certain connectivity technologies primarily Ethernet, Wi-Fi, etc. covering a relatively small area	WANs tend to use technology like Metro Ethernet, Leased Line, ATM, Frame Relay, etc. for connectivity over the longer distances
Operation	Typically operated, controlled, and managed by a single person or organization	Typically operated by public network server providers (also known as carriers) For the Internet, which is also regarded as a WAN, it is not owned by any one organization but rather exist under collective or distributed ownership and management
Transfer rate	LANs have a high data transfer rate	WANs have a lower data transfer rate as compared to LANs
Cost	If there is a need to set-up a couple of extra devices on the network, it is not very expensive to do that	In this case since networks in remote areas have to be connected hence the set-up costs are higher

WAN topology

The individual geographic locations connected by a WAN are known as WAN sites. A WAN link is a connection between a WAN site (or point) and another site (or point). A WAN link is typically described as point-to-point link — because it connects one site to only one other. Today, however, there are other types of WAN links that support point-to-multi-point connections, which allow more flexible connections among different points.

WAN topologies resemble LAN topologies, both of which are concerned with how to connect the communicating entities together so that they can exchange data with each other over the network. In the context of a LAN, such entities are network nodes within a small area, while in the context of a WAN, the entities refer to sites (or points) which were explained in the previous paragraph.

The typical WAN topologies include bus, ring, star, full mesh, partial mesh, tiered, some of which are depicted in the figures below.

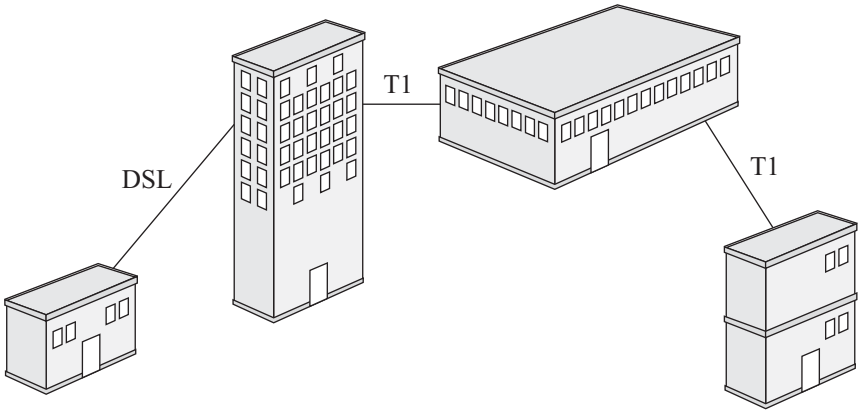

Figure 9.1 A bus topology WAN

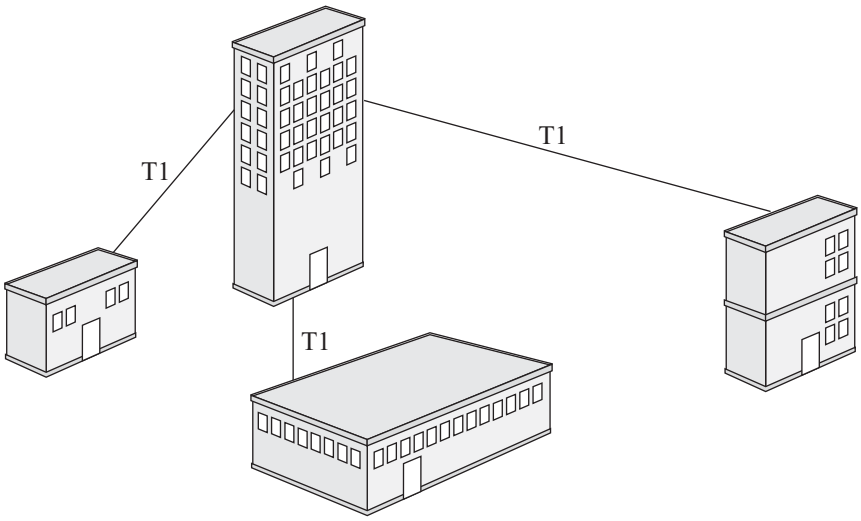

Figure 9.2 A star topology WAN

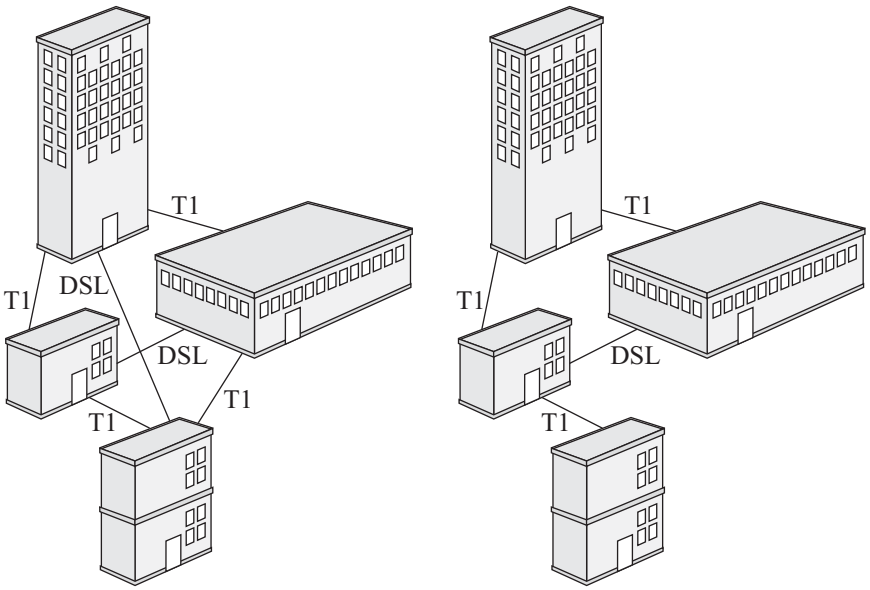

Figure 9.3 Full mesh and partial mesh WANs

Please refer the reading below for more detail on these WAN forms.

> ***Reading***
>
> Dean (2010) 301–5.

Major types of WAN access

In the following sections we will introduce you to major types of WAN access. But you should realize that our survey is by no means exhaustive, since there are various types of access that have arisen over the years and in different parts of the world.

PSTN

PSTN stands for Public Switched Telephone Network. It refers to the network of typical telephone lines and carrier equipment that service most homes and business organizations. Today, except for the lines connecting homes or offices (the consumers) to the **network carrier**'s telecommunications facilities (also known also the last mile), nearly all PSTNs use digital transmission and fibre optics as the typical network media that enable their throughout to be on par with the aggregated networking requirements of their consumers. The following figure illustrates the network configuration of a PSTN.

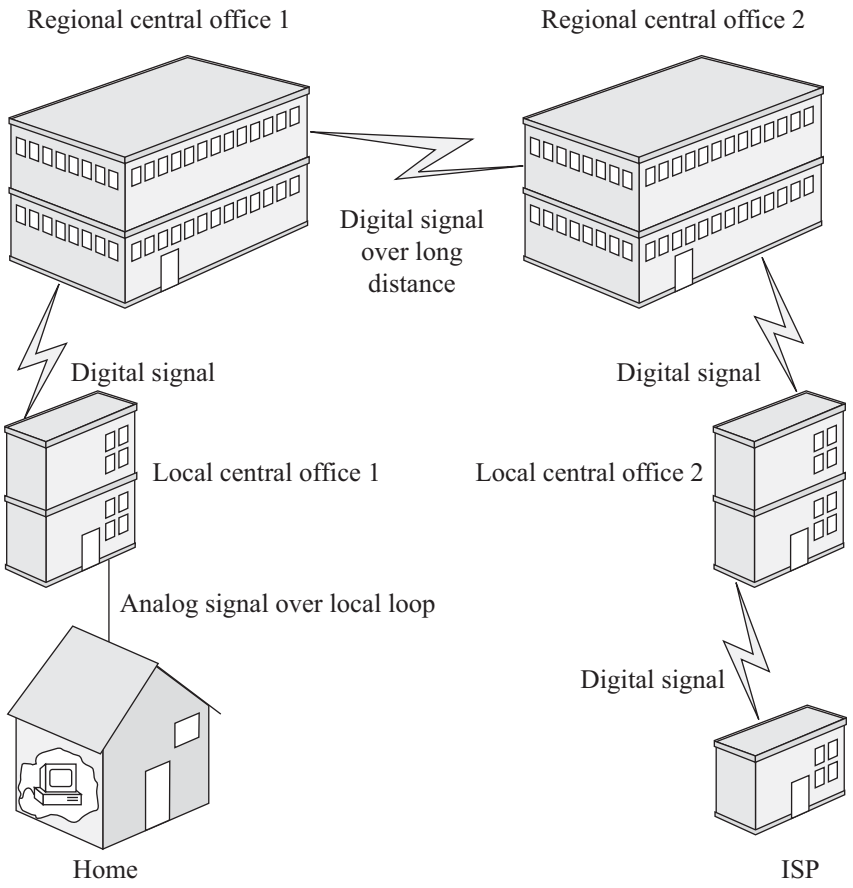

Figure 9.4 Network configuration of PSTN

We seldom use a PSTN directly as the WAN link to provide WAN connection. But, for the sake of discussion, we can quote a rare example of such a use: it's a dial-up connection, in which a user connects, via a modem, to a distant network from a computer. The rarity of this arrangement comes from the fact that the network carriers have made available other much better WAN connectivity options for consumers to choose from. These options use PSTNs in a more effective way than dial-up networking, enabling higher transmission rates and better service quality.

T-carriers

T-carriers offer a WAN transmission method that grew from a need to transmit digital data at high speeds over a PSTN. T-carrier standards specify a method of signaling, using TDM (time division multiplexing) over two wires, with one for transmitting and another for receiving, that divides a single channel into multiple channels. Each such channel carries a transmission rate of 64Kps. For instance, a T-1 lines comprises 24 channels, with the aggregated throughput of 1.544Mbps.

A T-carrier link is a dedicated line (also referred to as a leased line). Once set up, the link is a permanent point-to-point link established for connecting two remote sites in a network. Dedicated lines provide a fixed bandwidth and fulltime service for remote site connections. Usually a dedicated line is rented from a public network carrier. The cost depends

on the distance and bandwidth of the line. Commonly-used dedicated lines used in Hong Kong (and North America and parts of Asia) are shown in Table 9.2.

Table 9.2 Common T-carrier circuit speeds

	T-carrier circuit speed (Mbps)	Number of channels
T-1	1.544	24
T-2	6.312	96
T-3	44.736	672
T-4	274.176	4032

For many companies, the bandwidth of 1.544 Mbps provided by a T-1 circuit may still be too large for remote site connections. A fractional T-1 circuit may fit their needs better. A T-1 circuit can be divided into 24 separate 64 Kbps channels.

At a much lower cost than T-1, a fractional T-1 circuit can provide a bandwidth of 64 Kbps, 128 Kbps etc. (with an increment of 64 Kbps), depending on the user's needs. If several remote sites must be connected using dedicated lines, the costs may be high. Since a dedicated line is a point-to-point link, it has to be established whenever one remote site requires a direct link to another.

Figure 9.5 shows three dedicated lines for three remote sites that connect directly to each other. The figure actually shows a full mesh topology; that is, each remote site has a direct connection to the others.

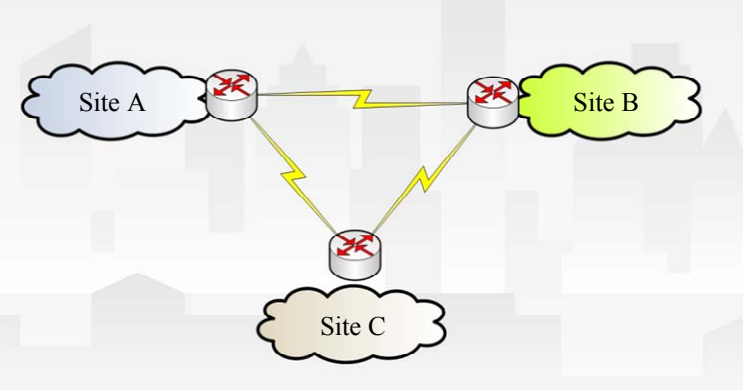

Figure 9.5 Dedicated T-carrier connections

To set up a T1 connection, we need to use the CSU/DSU (Channel Service Unit/Data Service Unit). Although CSUs and DSUs are actually two separate devices, they are typically combined into a single stand-alone device. The CSU provider provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the T-carrier frames into frames that the LAN can interpret.

The following diagram depicts a T-carrier connection to a LAN.

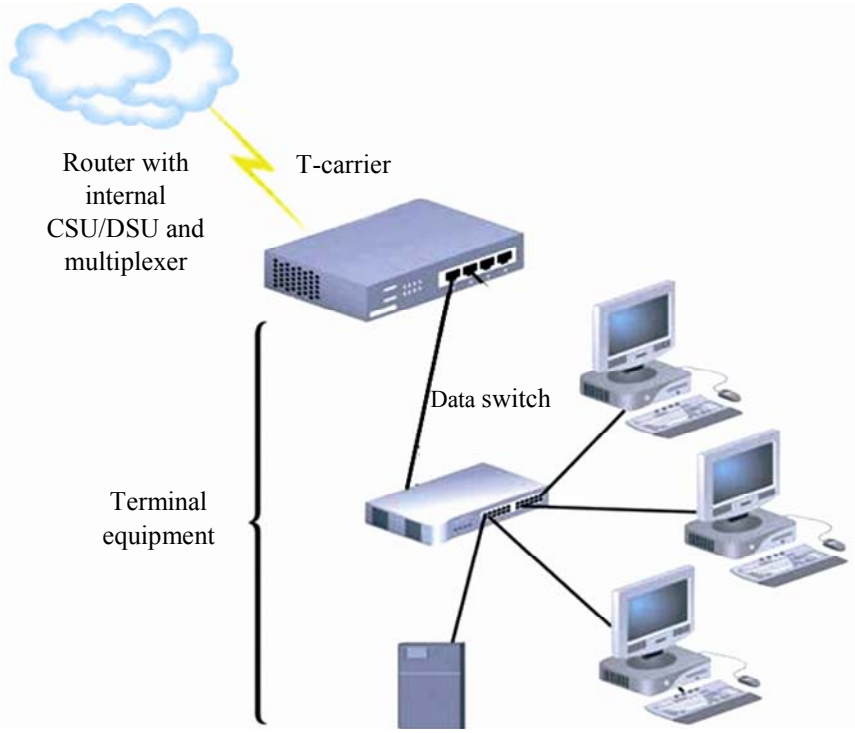

Figure 9.6 A T-carrier connection to a LAN

X.25

In a packet-switching network, data frames are broken into packets for transmission. Each packet goes through a series of switching devices and finally reaches the destination. At the destination, the packets are reassembled to the original data. In reaching its destination, each packet may pass along a different path. In contrast to dedicated lines that are dedicated to one organization, a packet-switching network can be shared by many organizations; that is, the switching devices can switch the packets from multiple organizations.

X.25 was developed in the 1970s to make use of the telephone network for data communications, and was designed with an aim of working well with all types of system, regardless of their manufacturers. Because it is international, it is still very popular and is used all over the world. X.25 networks may be set up privately or using public services provided by telephone companies. An X.25 network is called a public data network (PDN) if it is built on the public network. The common speed of X.25 networks is 64 Kbps, but it can provide a speed up to that provided by a T1 link. The X.25 specification defines a point-to-point interaction between data terminal equipment (DTE) and data circuit-terminating equipment (DCE). DTE refers to a terminal or a host that can transmit data. A DTE is attached to a DCE, which is in turn connected to a series of switching devices called packet-switching exchanges (PSEs). DCEs and PSEs together form a packet-switched network (PSN), with DCEs acting as connection points for the DTEs, and PSEs as the elements for creating the transmission path inside the PSN.

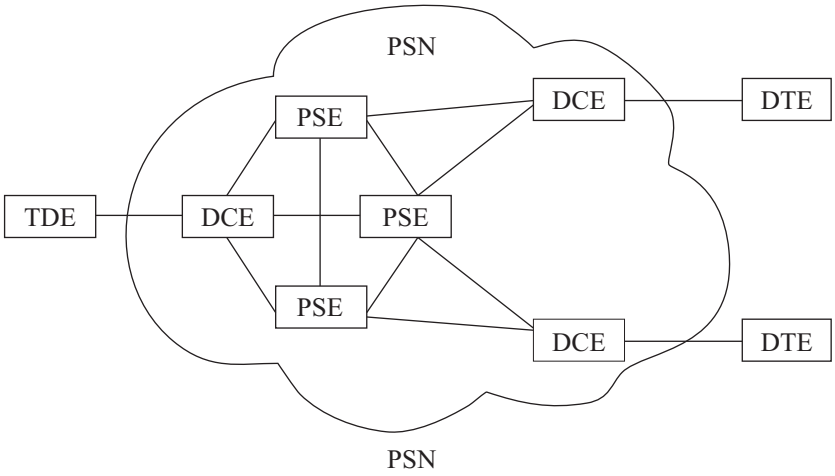

Figure 9.7 X.25 network structure

Figure 9.7 shows a block diagram of the structure of an X.25 network. Very often, an X.25 network is imagined as a packet-switched cloud. The internal operations within the cloud may be transparent to the users: they only need to make a connection from their LANs to the cloud, and they can then transmit data to all the other sites that are connected to the same cloud. Compared with dedicated lines in which point-to-point connections have to be established, only a single connection from each site is needed to connect to the cloud, thus imposing a relatively lower cost.

When Computer A, which is a DTE, wants to send data to Computer B through the X.25 network, it calls Computer B to request a communication session. On receiving the call, Computer B can accept or refuse the connection. If it accepts, Computer A can then begin to transfer data. Either side can terminate the connection at any time. The communication between two DTEs inside the X.25 network is enabled by the establishment of a virtual circuit. This circuit is composed of the DCEs connecting the communicating DTEs, plus the series of PSEs connecting in between. Each virtual circuit is assigned a number. Once a virtual circuit is established, the DTE sends the data packets to the other end of the connection by sending them to the DCE. The DCE then looks at the virtual circuit number to determine how to route the packets through the X.25 network. All packets sent between the two communicating DTEs go through the same path. Virtual circuits may be permanent or switched – that is, temporary. Permanent virtual circuits (PVCs) are typically used for the most often-used data transfers, whereas switched virtual circuits (SVCs) are used for sporadic data transfers.

X.25 was developed at the time when the telephone lines did not provide a reliable medium for data transmission. For this reason, error-checking and reliability functions are built into the X.25 protocols, making it a very complex protocol.

X.25 protocol maps to the first three layers of the OSI seven-layer model. The physical layer defines the physical media for the connection between the DTEs and DCEs. The data link layer transfers and checks the data, and the network layer is concerned with the routing of data packets as

well as the establishment of the PVCs and SVCs. X.25 performs a heavy load on ensuring reliability. Indeed, error checking is carried out even in the transmission of packets from one PSE to another. It is estimated that up to two-thirds of its bandwidth is dedicated to error checking. As telephone lines are much more reliable nowadays, such intensive error-checking mechanisms may not be necessary. A more efficient packet-switching technology, designed with the aim of providing a higher speed link, is frame relay.

Frame relay

Frame relay is a packet-switching network operating over PTSN that has a similar structure to X.25. However, frame relay is a much simpler protocol than X.25. It does not provide any of the reliability features that are available in X.25. Instead, it depends on the higher layer protocols, for example the application layer, for ensuring reliability. As all the work in error-checking is done by the data link layer in X.25, frame relay provides a much more efficient data transfer than X.25. Frame relay can provide 56 Kbps, 64 Kbps or 1.544 Kbps speed of data transfer.

Similar to X.25, frame relay consists of DTEs and DCEs. Frame relay DTEs may be routers or frame relay access devices (FRADs), whereas DCEs are frame relay switches. A PVC is established for the communication of two nodes in a frame relay network. Each PVC is identified by a data-link connection identifier (DLCI) number. The DLCI number is assigned to a link connecting the DTE and DCE or connecting between two DCEs. The DLCI number will be updated according to the switching table stored in the frame relay switches.

The following figure shows the operation of a frame relay switch. The packet comes into the switch from port P0 and the DLCI number 100. The switch then checks its switching table and finds the corresponding record that notes that this incoming packet should be out to port P1, with the DLCI updated to 200. The next frame relay switch receives this packet and does the same processing to pass the packets on to another switch. In this way, the packet can finally reach its destination.

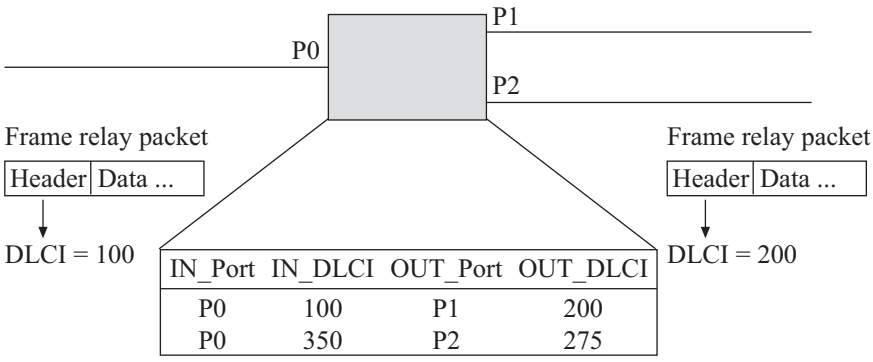

Figure 9.8 Operation in a frame relay switch

A more practical example is shown in Figure 9.9. Two PVCs are established, one between Los Angeles and Atlanta, and one between San

José and Pittsburgh. Los Angeles sends data to Atlanta using DLCI number 12, whereas Atlanta sends data to Los Angeles using DLCI number 82 through the same PVC. Since no PVC is built between Los Angeles and Pittsburgh, they cannot transfer data to each other through this frame relay cloud. To establish a connection between these two sites, therefore, a new DLCI number has to be assigned to each of these sites, say 13 for Los Angeles and 63 for Pittsburgh, as shown in Figure 9.10. Then Los Angeles can send data to both Atlanta and Pittsburgh with reference to DLCI numbers 12 and 13 respectively. You may note that San José also refers to DLCI number 12 to send data to Pittsburgh. This shows that DLCI numbers are local to the DTEs and DCEs and so may be the same for different DTE and DCEs.

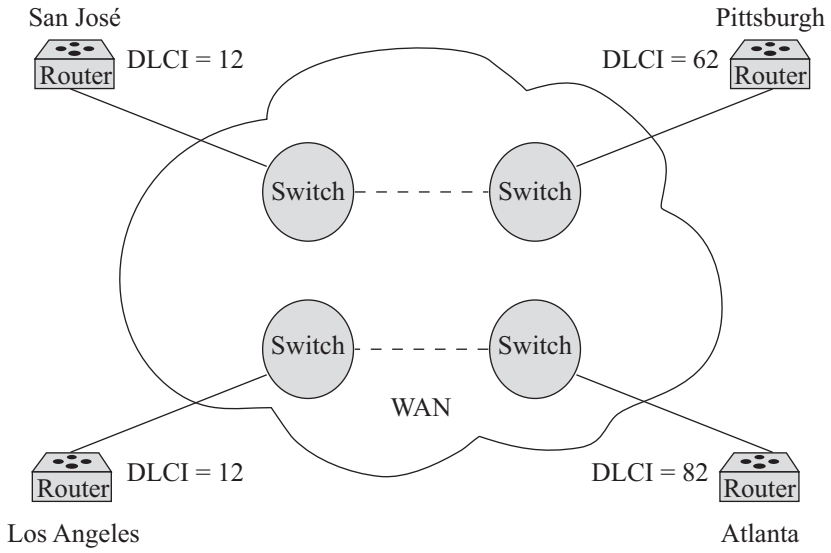

Figure 9.9 Frame relay connections

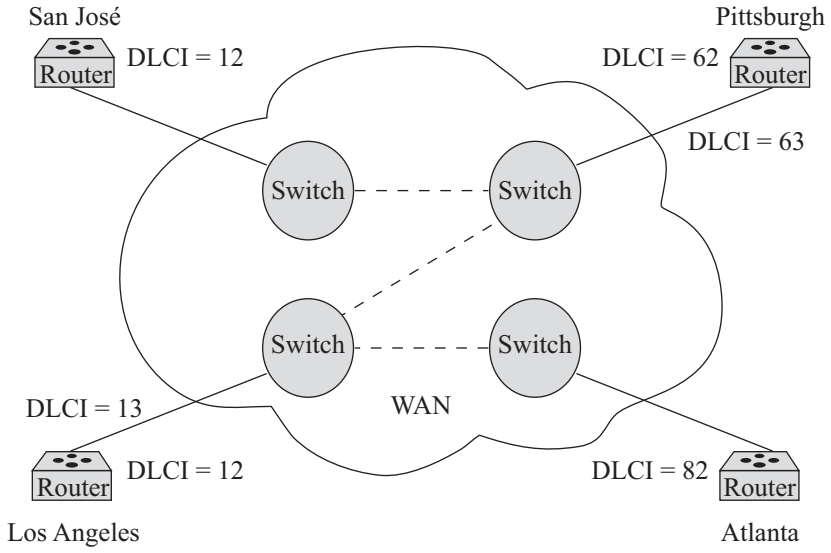

Figure 9.10 A permanent virtual circuit in a frame relay network

The bandwidth provided by the frame relay network is defined by the committed information rate (CIR) associated with the DLCI numbers for

a PVC. The CIR defines a guaranteed bandwidth for the corresponding PVC, but not the maximum available bandwidth. When a DTE requires a bandwidth that is larger than the one specified in CIR for a particular PVC, the frame relay switches can still process it without dropping the packets. Since a frame relay switch is shared by more than one PVC, the switches will allow a PVC to use other PVCs' bandwidth if those PVCs are idle. This is called over-subscription. However, when all PVCs going through a particular switch are busy, over-subscription is then not possible, but each PVC can still have the bandwidth specified by the CIR.

With limited throughput, the Frame Relay technology is gradually fading out, along with the downtrend on their deployment.

Metro Ethernet

Metro Ethernet is a WAN technology based on the Ethernet standard. It is commonly used as a metropolitan access network to connect subscribers and businesses to a larger service network or the Internet. Businesses can also use Metro Ethernet to connect branch offices to their internal networks.

Ethernet has been a well-established technology for decades. An Ethernet interface is much less expensive than a T-carrier of the same bandwidth. Ethernet also supports higher bandwidths with fine granularity, which is not available from Frame Relay solutions. Another distinct advantage of an Ethernet-based access network is that it can be easily connected to the customer network, due to the prevalent use of Ethernet in corporate and, more recently, residential networks. Bringing Ethernet in to the WAN therefore introduces a lot of advantages to both the service provider and to customers (corporate and residential).

Unsurprisingly, Metro Ethernet adoption has been skyrocketing, displacing many of the traditional WAN connections based on T-carriers, Frame Relay, etc.

The next figure is an excerpt of the Metro Ethernet service provision offered by a local service provider.

Products & Services > Data Connectivity > Ethernet Service

Metro Ethernet service provides a flexible, scalable and cost-effective point-to-point, point-to-multipoint as well as any-to-any networking solution. It also gives customers secure Layer 2 Ethernet connectivity while leaving tremendous capacity available for expansion. The guaranteed data transfer rate ranges from 512Kbps to 1Gbps and supports a wide range of interface options.

Features

Secure
Provides secure layer 2 connections for point-to-point, point-to-multipoint, or any-to-any network

Scalable and guaranteed bandwidth
Scalable and guaranteed bandwidth from 512Kbps to 1Gbps

On-line traffic
Provides on-line traffic utilisation reports

Interconnectivity
Interconnectivity with Wharf T&T's ATM network

Various access methods
Various access methods: nx64kbps up to E1, Ethernet, Fast Ethernet and Gigabit Ethernet

Bandwidth-on-demand
Bandwidth-on-demand for greater bandwidth within a short period

Fixed or burstable bandwidth
Fixed or burstable bandwidth charging models

Optional internet access
Optional Internet access and router on loan

Optional Class of Service
Optional Class of Service (CoS) for different application requirements

7X24 proactive networking monitoring
7x24 proactive network monitoring and support

Figure 9.11 A sample service provision of Metro Ethernet offered by a local provider

Source: http://www.wharftt.com/wtt2/pages/en/products_and_services_data_services_metro_ethernet.html

SONET

If the above T-carrier circuits cannot meet a network's bandwidth requirement, higher speed communication can be obtained through Synchronized Optical Network (SONET), which is an ANSI standard that is implemented over optical fibre cables. The term Optical Carrier-N (OCN), in which N is a positive integer, is usually used to designate the line speed in SONET.

The following table shows SONET line speeds.

Table 9.3 Typical SONET line rates

	Optical carrier level speed
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-18	933.12 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-96	4.976 Gbps
OC-192	9.953 Gbps

Residential broadband access

Digital subscriber line (DSL) is another type of WAN connection introduced in the late 1990s that competes directly with T1 services, particularly for Internet connections. DSL provides a dedicated digital circuit between a user and a telephone company's central office (CO), allowing for high-speed Internet data transfer over existing 2-wire copper telephone lines. The family of DSL technologies is referred to as xDSL. Within this family, the two primary categories are ADSL and SDSL. The key difference between these two groupings is the asymmetrical or symmetrical transfer of Internet data, respectively.

ADSL

Asymmetric Digital Subscriber Line, or ADSL, is called asymmetric because the download speed is significantly higher than the upload speed. The speed inequity makes this technology more suitable for residential or small business users, since higher speed uplinks are not as important. Most of an ADSL's duplex bandwidth is devoted to the downstream direction, i.e. in sending data to the user. An ADSL can support speeds of 1.544 to 6.1 Mbps for downstream (the speed increases closer to CO) and 16 Kbps to 1.5 Mbps for upstream transmissions. ADSL is used a number of local Internet service providers (ISP) in Hong Kong.

SDSL

Symmetric Digital Subscriber Line or SDSL is a commercial grade DSL solution, suitable for businesses that may be running servers or applications that send out large amounts of data. An SDSL does not provide voice capabilities, so an additional phone line must be installed.

Uplink and downlink speeds are equivalent, with reliable service along the dedicated line. Generally SDSL solutions will also offer the user a number of static IP addresses. An SDSL can support speeds of 1.544 Mbps both upstream and downstream.

How does it work? Inside the user's ADSL modem is a POTS splitter, which divides the existing phone line into two bands: one for voice and one for data. A channel separator within the modem then divides the data channel into two parts — a larger part for downstream data and the smaller part for upstream data — which explains the asymmetric nature of the data transfer. The data is then transported over telephone wires to the CO, which must be no more than 18,000 feet away from the user's connection site. At the CO, the data is received by another ADSL modem. Within this modem is another POTS splitter, which separates voice calls from data. Voice calls are directed to the public switched telephone network (PSTN), and data are passed on to the digital subscriber line access multiplexer (DSLAM).

The DSLAM links many ADSL lines to a single high-speed asynchronous mode (ATM) line, which in turn connects to the Internet backbone at high speeds. Information from the Internet to the user follows this route back to the user.

Whereas local and long-distance phone companies promote DSL as the preferred method of Internet access, cable companies are pushing their own connectivity options, based on the coaxial cable wiring used for TV signals. Such cable connection requires that the customer use a special cable modem, which we discuss next.

Cable modem

A cable modem modulates and demodulates signals for transmission and reception via cable wiring. Such connection could theoretically transmit as much as 36 Mbps downstream and as much as 10 Mbps upstream. Realistically, cable will allow approximately 3 to 10 Mbps downstream and 2 Mbps upstream, because it is shared. One advantage of cable is that, like DSL, it provides a dedicated or continuous connection that does not require dialling up a service provider. However, cable technology requires many subscribers to share the same line, thus raising concerns about security and actual throughput.

Choosing a WAN technology

In summary, determining which WAN technologies should be used, we have to consider the reliability, scalability and bandwidth required of the particular network in question. Of course, the cost is the most important thing in our consideration. We need to first work out the bandwidth requirement in the connection of each pair of sites. Based on this information, we look for a technology to meet the requirement. For example, if the bandwidth required for the communications between two particular sites is about 1Mbps, obviously dial-up connection can be deleted from the list of considerations. If we notice that the bandwidth requirement for a particular connection varies from time to time, a link with a bandwidth that can take care of the peak requirement may be a waste at all other times. Then relay may be suitable, as it provides a flexible bandwidth. Backup jobs may be done once a day or even once a week; a dedicated line that provides a permanent connection may be a waste for such a connection. A dial-up line may be a good solution in this case, and the cost is lower. It is usual to use all the technologies to fit the particular needs of connections in different portions of an enterprise network.

The landscape of local WAN services

Hong Kong is one of the most sophisticated and competitive telecommunications markets in the world. Hong Kong residents get good services in terms of capacity, speed and price. The Office of Telecommunications Authority (OFTA) (www.ofta.gov.hk) is the legislative body responsible for regulating the telecommunications industry in Hong Kong. The OFTA has liberalized all telecom sectors and there are no foreign ownership restrictions. In the local fixed-carrier market there is neither a pre-set limit on the number of licenses issued nor deadline for applications. Currently, there are around ten fixed-carrier licensees: PCCW-HKT, New World Telephone Limited, Wharf T&T Limited, Hutchison Global Crossing Limited, HK Cable Television Ltd., Hong Kong Broadband Network Limited, Eastar Technology Limited, CM Tel. (HK) Limited, TraxComm Limited and HKC Network Limited. These fixed carriers are licensed to, among other things, offer WAN services to their customers in Hong Kong.

Please refer to Figure 9.11 for a local offering of the Metro Ethernet service; this type of service is the most popular type of WAN service used by businesses these days.

Virtual private networks (VPNs)

VPNs allow two network end points, which are separate from each other at a significant physical distance, to be connected over the Internet or other untrustworthy networks. The Internet has literally attained ubiquitous availability and reached the commodity level of pricing around the global. This makes VPN solutions very cost-effective, thus appealing to small and medium-sized enterprises for which cost has to be factored in when deciding on a technology solution. Thanks again to the Internet, as it enables WAN technologies to diffuse into business organizations of different sizes, making networking technologies become an integral part of the business operations, thereby enabling higher efficiency and better responsiveness. It is no wonder that many organizations of varying size nowadays spearhead their information technology as a strategic means to raise their business advantages, or as a differentiator from their competitors.

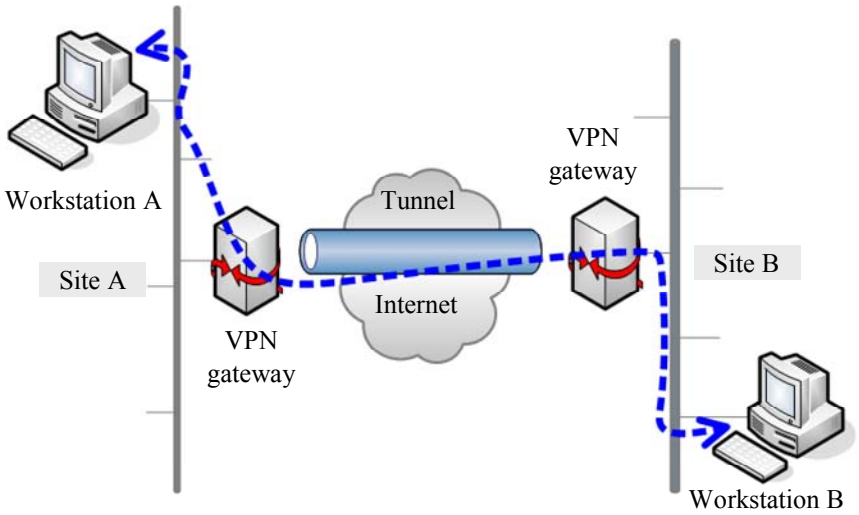

Figure 9.12 A site-to-site VPN channel

Please refer back to *Unit 8* if you need to revise your knowledge of VPN technology and its applications. You should also read the following sections from your textbook.

> ***Reading***
>
> Dean (2012) 465–68.

Self-test 9.1

1 Compare WANs and LANs. State three differences between them.

2 What technique enables DSL to achieve high throughput over PSTN lines?

3 Suppose you establish a home network and you want all three of your computers to share one broadband cable connection to the Internet. You decide to buy a router to make this sharing possible. Where on your network should you install the router?

4 You work for an Internet service provider that wants to lease a T3 over a SONET ring. What is the minimum Optical Carrier level that the SONET ring must have to support the bandwidth of a T3?

5 What technique does T1 technology use to transmit multiple signals over a single telephone line?

6 A VPN is designed to connect 15 film animators and programmers from around the state of California. At the core of the VPN is a router connected to a high performance server used for storing the animation files. The server and router are housed in an ISP's data centre. The ISP provides two different T3 connections to the Internet backbone. What type of connection must each of the animators and programmers have to access the VPN? (*Hint*: Don't get confused by the information provided by the question. Just go back to the fundamental of VPN. What is the network connection it operates over?)

Introduction to wireless networks

As the name implies, wireless networks do not need to use wire lines to transmit signals. Rather, a wireless network uses the atmosphere as the network medium for transmitting data. But, considering that wired networks have been working so well for so far, why do we need to go wireless? What are the advantages of wireless networks?

The most obvious advantage of wireless networking is *mobility*. Wireless network users can connect to existing networks and are then allowed to roam freely. Wireless data networks free users from the tethers of an Ethernet cable at a desk. They can work in the library, in a conference room, in the airport, or even in the coffee house across the street. As long as the wireless users remain within the range of the base station, they can take advantage of the network. Wireless networks typically have a great deal of *flexibility*, which can translate into rapid deployment. Wireless networks use a number of base stations to connect users to an existing network. With the infrastructure built, adding a user to a wireless network is a matter of configuring the infrastructure, but it does not involve running cables, punching down terminals, and patching in a new jack as wired networks need to. Only could such flexibility make possible the public hot spot operation, through which public users can gain access to the network connections wirelessly provided by service providers in various locations or premises.

However, wireless networks do not replace fixed networks. Servers and other data centre equipment are very static in terms of their location; they may as well be connected to wires that do not move. The speed of wireless networks is constrained by the available bandwidth. Information theory can be used to deduce the upper limit on the speed of a network. Wireless-network hardware tends to be slower than wired hardware. Unlike the 10-GB Ethernet standard, wireless-network standards must carefully validate received frames to guard against loss due to the unreliability of the wireless medium.

Comparison of wireless and wired networks

Furthermore, security on any network is a prime concern. On wireless networks, it is often a critical concern because the network transmissions are available to anyone within range of the transmitter with the appropriate antenna. On a wired network, the signals stay in the wires and can be protected by strong physical-access control (locks on the doors of wiring closets, and so on). On a wireless network, sniffing is much easier because the radio transmissions are designed to be processed by any receiver within range. Table 9.4 provides a comparison of the features of wireless and wired networks.

Table 9.4 Comparison of wireless and wired networks

	Wireless networks	Wired networks
Mobility	High	Low
Flexibility	High	Low
Speed	Moderate	High
Security	Poor	Good

Wireless transmission

The following sections introduce some basic concepts relating to the operation of wireless networks, including data transmission.

Radio spectrum

Like all networks, wireless networks transmit data over a network medium. The medium is a form of electromagnetic radiation. The wireless spectrum is a continuum of electromagnetic waves used for data and voice communication. On the spectrum, waves are arranged according to their frequencies. The wireless spectrum spans frequencies 9KHz and 300 GHz, which is shown in the figure below.

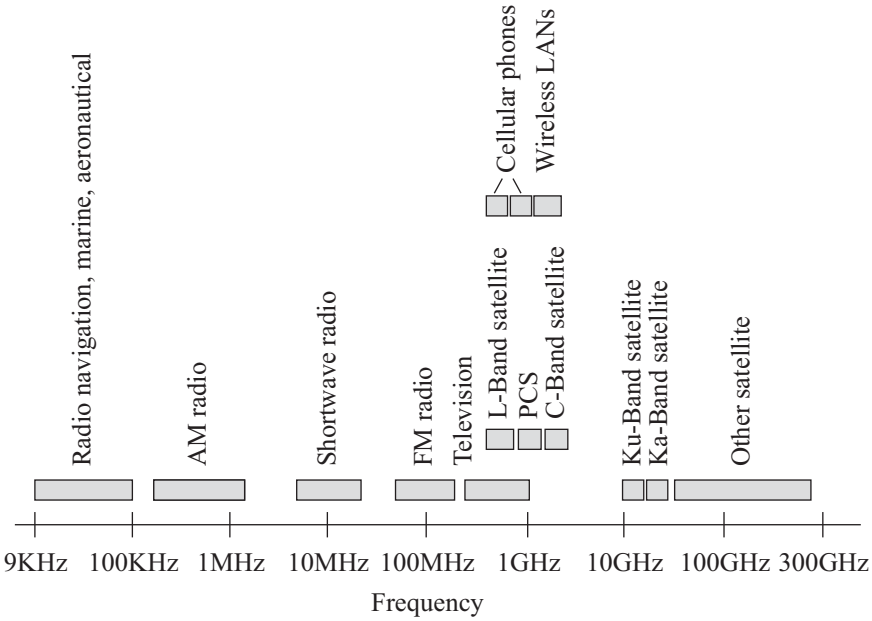

Figure 9.13 The wireless spectrum

Radio waves can penetrate most office obstructions and offer a wider coverage range. It is no surprise that most, if not all, 802.11 products on the market use the radio wave physical layer. 802.11b and 802.11g use the 2.4 GHz frequency band, while 802.11a uses the 5GHz frequency band. 802.11 divides each of the frequency bands into channels, analogously to how radio and TV broadcast bands are sub-divided, but

with greater channel width and overlap. For example the 2.4000–2.4835 GHz band is divided into 13 channels each of width 22 MHz but spaced only 5 MHz apart, with channel 1 centred on 2.412 GHz and channel 13 on 2.472 GHz, to which Japan adds a 14th channel, i.e. 12 MHz above channel 13.

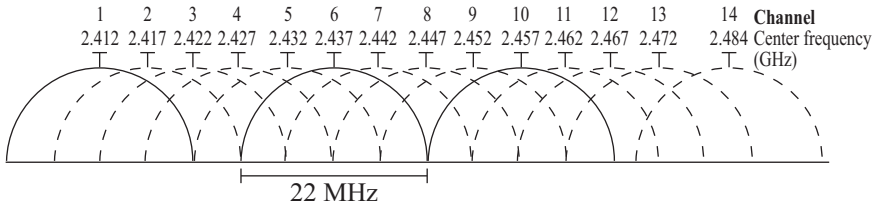

Figure 9.14 2.4 GHz Wi-Fi channels (802.11b or g)

Access methods

802.11 does not depart from the previous IEEE 802 standards in any radical way. The standard successfully adapts Ethernet-style networking to radio links. Like Ethernet, 802.11 uses a Carrier Sense Multiple access (CSMA) scheme to control access to the transmission medium. However, collisions waste valuable transmission capacity, so rather than implementing the collision detection (CSMA/CD) employed by Ethernet, 802.11 uses collision avoidance (CSMA/CA). Also like Ethernet, 802.11 uses a distributed access scheme with no centralized controller. Each 802.11 station uses the same method to gain access to the medium.

The major differences between 802.11 and Ethernet therefore stem from the differences in the underlying medium. To tackle the vulnerability of wireless communications to external interference, 802.11 incorporates positive acknowledgments (i.e. all transmitted frames must be acknowledged) to ensure the reliable transmission of data.

In CSMA/CA, before a node begins to send data, it checks the medium. If it detects no transmission activity, it waits a brief, random amount of time, and then sends its transmission. If the node does detect activity, it waits a brief period of time before checking the channel again. CSMA/CA does not eliminate the potential for collisions — it only minimizes them. This is the major difference between CSMA/CA and CSMA/CD (used by Ethernet). In CSMA/CD, when a node finds out that the medium is idle, the node immediately starts to send data, but in CSMA/CA it waits for a brief, random amount of time before doing so.

Association

At any physical location– whether it is an Internet cafe, airport lounge, etc. — there could be many different wireless networks providing network coverage. A user therefore has to go through an association process to establish a link with a particular existing wireless network before he can use it to transmit data. Each wireless network is identified with a SSID (Service Set Identifier) — that is, a unique character string through which he can decide which wireless network he wants to

associate with. During the association, the access point (AP) of the wireless network may or may not (depending on how the security protection is configured) authenticate the user before granting him access to the network connectivity. Such security protection will be discussed further in a later part of this unit. The figure below illustrates how wireless access points work.

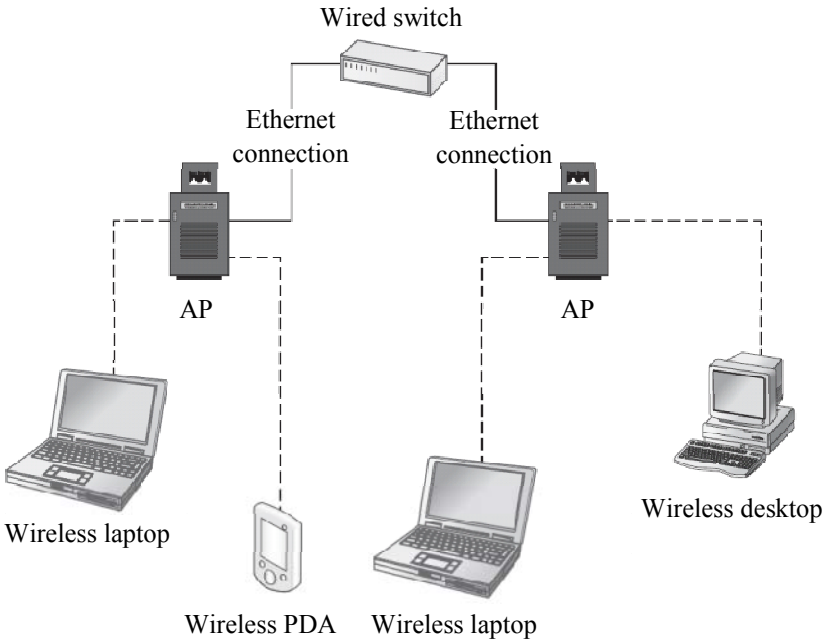

Figure 9.15 A wireless network with multiple access points (Carpenter 2008)

The figure below shows some popular AP products.

Figure 9.16 Some samples of AP products (Carpenter 2008)

Reading

Dean (2012) 344–54.

Self-test 9.2

1 What is an SSID?

2 What is the Access Point?

3 What frequency range is shared by the most popular type of wireless LAN?

Activity 9.1

Do you know how to improve your Wi-Fi connection without having spending a lot of money? In this short video — https://www.youtube.com/watch?v=yqnHz75dmQY — you can see how to make a parabolic reflector using some aluminium foil, and then use it to boost the reception of Wi-Fi signal by two bars on a Windows desktop.

Wireless network protocols

Wireless networking is a hot industry segment. Several wireless technologies have been targeted primarily for data transmission. The IEEE 802.11 standards define how wireless LAN should work. They are analogous to their wired counterpart 802.3 Ethernet standard, which defines how wired network should work. Bluetooth is another standard of wireless networking, which is used to build small networks between peripherals: a form of wireless wires, if you will. Infrared serves the similar purpose of Bluetooth, but is regarded as an older technology. We will explore each of them in the following sections and walk through their major functions and features.

Wireless LANs (802.11 technologies)

802.11, also known as wireless LAN (WLAN) technology, goes by a variety of names, depending on who is talking about it. Some people call it 802.11 wireless Ethernet, to emphasize its shared lineage with the traditional wired Ethernet (802.3). The Wireless Ethernet Compatibility Alliance (WECA) has been pushing its Wi-Fi (wireless fidelity) certification program. Any 802.11 vendor can have its products tested for interoperability. Equipment that passes the test suite can use the Wi-Fi mark. So, today we often use the term ‘Wi-Fi’ interchangeably with the term ‘wireless LAN.’ There are three principal wireless LAN technologies (802.11b, 802.11a and 802.11g) standards. We will explain each of them below.

802.11b

The IEEE 802.11b standard is the dominant standard for WLANs. It reuses many of the Ethernet Logical Link Control (LLC) components, and is designed to easily connect into Ethernet LANs. For these reasons, IEEE 802.11b is usually called ‘wireless Ethernet’, but its official name is wireless LAN. Some vendors selling 802.11b equipment have trademarked the name Wi-Fi to refer to 802.11b. There are two versions of 802.11b: frequency-hopping spread-spectrum (FHSS) systems run at 1 Mbps and 2 Mbps; and direct-sequence spread-spectrum (DSSS) systems run at 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps. DSSS systems dominate the marketplace because they are faster.

802.11a

The IEEE 802.11a standard for WLAN is newer than 802.11a. It operates in a 5-GHz frequency range. The total bandwidth is 300 MHz, substantially more than the 22 MHz of 802.11b. This means that it can transmit data faster than 802.11b. The possible data rates would be 6 Mbps to 54 Mbps. However, as it operates in 5-GHz range, it requires more power for transmission.

802.11g

The IEEE 802.11g comes after 802.11b and 802.11a. 802.11g is designed to combine many of the advantages of 802.11b and 802.11a. It can attain a transmission rate of 54Mbps, while it operates in the 2.4-GHz range and thus has more moderate power consumption than 802.11b. Currently, 802.11g is the most widely-used WLAN protocol.

802.11i

802.11i is a security protocol designed to protect the wireless network. It uses Extensible Authentication Protocol (EAP) with strong encryption scheme, and dynamically assigns every transmission its own key to heighten the protection of the data in transmit against taping or tampering. With 802.11i enabled, logging on to a wireless network is more complex than with WEP (Wired Equivalent Privacy) and, in return, a higher level of security protection can be achieved. We will cover this protocol further, together with the subject of wireless security, in a later part of this unit.

802.11n

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. Enterprises have begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal. An 80211n network operates at either 5GHz or 2.4GHz frequency bands, achieving a sustainable throughput of 144Mbps and a peak transmission rate of 600Mbps. The maximum indoor and outdoor ranges go up to 300 feet and 500 feet, respectively.

The current state of the art supports a maximum transmission rate of 450 Mbps, with the use of three spatial streams at a channel width of 40 MHz. Depending on the environment, this may translate into a sustainable throughput for TCP/IP of 110 Mbps.

The IEEE 802.11n task group has completed their work, and the amendment was approved by IEEE in September 2009. It will be followed by publication in mid October 2009. In other words, the IEEE 802.11n standard will finally be released after six years' deliberation, which is an exceptionally long process of standardization in the telecommunications industry.

Major networking manufacturers have been releasing 'pre-N', 'draft n' or 'MIMO-based' products based on early specs. These vendors anticipated that the final version would not be significantly different from the draft, and in a bid to get the early mover advantage they pushed ahead with many of the new technologies. Depending on the manufacturer, a firmware update should make current 'Draft-N' hardware compatible with the final version. More importantly, the incompatibility issues among products from different manufacturers that have hindered the

wide adoption of 802.11n will vanish gradually, and the era of 802.11n, representing high speed wireless LAN connectivity, will come soon.

Bluetooth

A wireless PAN (personal area network) (WPAN) provides hands-free connectivity and communications within a confined range and limited throughput capacity. Bluetooth is a perfect example of a wireless PAN technology that is both beneficial and that is in widespread use. Everything from Bluetooth mouses to headsets are being used on a daily basis throughout the world. Bluetooth has been codified by the IEEE in their 802.15.1 standard, which describes WPAN technology. A Bluetooth PAN is also known as a piconet. The simplest type of piconet is one that contains one master and one slave, which communicate in a point-to-point fashion with each other.

Figure 9.17 A wireless personal area network (WPAN)

Source: Dean 2006, 4e

Infrared (IR)

It is a common experience for us to use infrared (IR) signalling to change channels on a TV via a TV remote. IR signals depend on a line-of-sight transmission path between the sender and receiver. This has in fact hindered the application of IR from advancing beyond remote controlling and peripherals connection. IR signals occur at very high frequencies, in the 300- to 300,000-Ghz range, just above the visible spectrum of light.

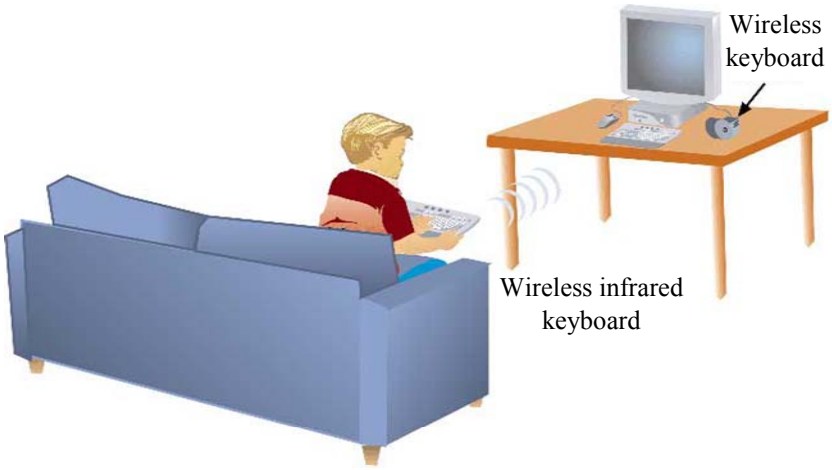

Figure 9.18 Infrared transmission

Source: Dean 2006, 4e

The following table offers a comparison of the common wireless networking standards, their ranges and throughputs.

Table 9.5 Infrared transmission

Standard	Frequency range	Theoretical maximum throughput	Effective throughput (approximate)	Average geographic range
802.11b ("Wi-Fi")	2.4 GHz	11 Mbps	5 Mbps	100 meters (or approximately 330 feet)
802.11a	5 GHz	54 Mbps	11–18 Mbps	20 meters (or approximately 66 feet)
802.11g	2.4 GHz	54 Mbps	20–25 Mbps	100 meters (or approximately 330 feet)
Bluetooth ver. 1.x	2.4 GHz	1 Mbps	723 Kbps	10 meters (or approximately 33 feet)
Bluetooth ver. 2.0	2.4 GHz	2.1 Mbps	1.5 Mbps	30 meters (or approximately 100 feet)
IrDA	300–300,000 GHz	4 Mbps	3.5 Mbps	1 meter (or approximately 3.3 feet)

Source: Dean 2006, 4e

Reading

Dean (2012) 354–64.

Self-test 9.3

1 In the 802.3 Ethernet, the IEEE specifies CSMA/CD as the access method. In the 802.11 standard, the IEEE specifies what type of access method?

2 What are the theoretical maximum throughputs of 802.11 a, b, g, and n?

3 What is MIMO?

Activity 9.2

Investigate why the 802.11b and 802.11g wireless transmission technologies are more commonly used in business LANs than Bluetooth. This is an open question. You can try to come up with at least two reasons.

Wireless LAN design models

To help you put together the pieces of information you have learned so far in this unit, this section presents how the WLAN models that have evolved over time. We start with the first model implemented using IEEE 802.11 technology, and then progress through the second stage of WLAN design models.

Intelligent edge

The first devices to be released to the market were standard APs that are still used heavily today. This kind of AP contains the entire logic system needed to implement, manage, and secure (according to the original IEEE 802.11 specification) a WLAN. The benefit of this type of WLAN is that implementation is very quick when you are implementing only one AP.

The drawback to this type of WLAN is that implementation is very slow when you are implementing dozens or hundreds of APs. There are many networks around the world that have more than 1000 APs. You can imagine the time involved if you have to set up each AP individually. At stage one, intelligent edge, this is your only choice. The APs implemented in this model are also known as autonomous APs.

Wireless LAN management systems

When we arrive at stage two in the evolution of WLAN management, we encounter centralized configuration management with distributed intelligence. The devices and software that provide this functionality are known as a WLAN Network Management System (WNMS). This stage provides much faster implementations of traditional APs, and works using SNMP or other proprietary communication protocols to configure the APs across the network. The WNMSs usually supports the rollout of firmware so that the APs can be updated without having to visit each one individually. This model provides scalability, but does not cause much impact to the topologies, and to the infrastructure cost of the APs. In short, this model centralizes management, but distributes processing.

A lab on setting up an *ad hoc* wireless network

Sometimes we need to create a network among a small group of notebook computers, for example, for file sharing or sharing an Internet connection, as shown in Figure 9.19.

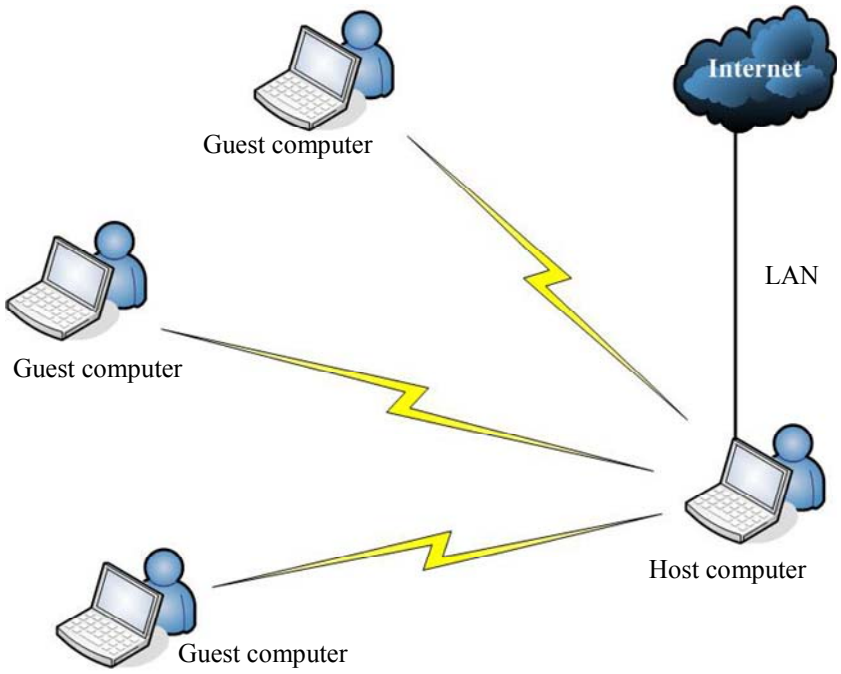

Figure 9.19 An adhoc wireless network design

In the following activity, we will do this using *ad hoc* technology to temporarily create a Wi-Fi network that does not need other network devices such as routers and switches.

Activity 9.3

Complete 'Lab 5.2 – Creating a small network between notebook computers with *ad hoc* technology' from the textbook *A Practical Approach to Internet Programming and Multimedia Technologies*. This exercise helps you learn how to make a connection between notebook computers directly through Wi-Fi, and to share the Internet connectivity among the users connected to the Wi-Fi network.

Wireless access to the Internet

Wi-Fi

Wi-Fi, also known as wireless broadband, wireless networking or wireless fidelity, simply means broadband without the wires. The advantage of small, portable devices such as laptops and PDAs is that they can be used anywhere around the house. But if you want to access the Internet on them as well, you'll need a Wi-Fi transmitter.

Wi-Fi has become very popular because once you have a base station, any number of desktop or laptop computers can be connected to your broadband service without the need for any cables or installing extra phone lines. So if you have a second computer in an upstairs room, or a laptop as well as a desktop, the same broadband service will be available on all your machines at the same time.

On the other hand, Wi-Fi is a trademark of the Wi-Fi Alliance for certified products based on the IEEE 802.11 standards. This certification warrants interoperability between different wireless devices. In some countries the term Wi-Fi is often used by the public as a synonym for IEEE 802.11-wireless LAN (WLAN).

Not every IEEE 802.11 compliant device is certified by the Wi-Fi Alliance, which may be because of certification costs that must be paid for each certified device type. The lack of the Wi-Fi logo does not imply that a device is incompatible to certified Wi-Fi devices.

Wi-Fi is used by most personal computer operating systems, many video game consoles, laptops, smartphones, printers, and other peripherals.

Hotspots

A *hotspot* provides wireless Internet access in public areas. Some hotspots are free and wide open, while others are free and secured. Yet other hotspots are subscription-based, pay-as-you-go, or a mixture of these. PDAs and laptops are usually the devices used to connect to hotspots. These hotspots are found everywhere, from coffee shops to libraries to public parks. It is important to remember that a hotspot is defined as a wireless network that is *intended to give* wireless Internet access either free or for a fee. There are many locations where you can connect to a wireless network, but many, if not most, of these are *inadvertently giving* wireless Internet access. Examples of these inadvertent networks include homes, businesses, and even government installations that are not properly secured. Specialty devices have been created that can print receipts, authenticate users, and even disconnect users after time limits expire. These devices are often called hotspot

gateways. There are many business models associated with the implementation of a hotspot. Following are a few examples:

- ***Paid Access*** — This model profits from the fees for access to the Internet. This is very common today in airports, coffee shop, major shopping centres, etc..

- ***Traffic Generation*** — This model profits from the sales of items like coffee, books, music, and other items to the individual who come to the hotspot location for Internet access. The customers who patronize the shop will be provided a fixed-period of free or discounted access to wireless Internet connection.

WiMax

Wireless MANs (metropolitan area networks) differ from wireless LANs and wireless PANs in that they are not usually implemented by the organization that wishes to use the network. Instead, they are generally implemented by a service provider, and then access to the network is leased by each subscribing organization. However, unlike with wireless WANs, this does not have to be the case. For example, 802.16-compliant hardware could be purchased and frequency licenses could be acquired in order to implement a private wireless MAN, but the expense is usually prohibitive. WiMAX is the most commonly referenced wireless MAN technology. Now, in 2007, WiMAX solutions are just beginning to see production and installation. In fact, the first WiMAX Professional Certification training class was held in Hawaii, in January and February 2007. WiMAX is based on the IEEE 802.16 standard and provides expected throughput of approximately 40 Mbps for fixed, line of sight connections and approximately 15 Mbps for mobile, non-line of sight connections. In addition to the throughput speeds, WiMAX incorporates QoS mechanisms that help to provide greater throughput for all users and important applications using the network.

A wireless Internet service provider (WISP) is an Internet service provider (ISP) that is accessed using wireless technologies. WISPs often fulfil the need at the ‘last mile’, which refers to the last section that must be spanned to reach remote customers. It can be very expensive and, without wireless, sometimes impractical. Sometimes these WISPs lease bandwidth to businesses that require Internet access, but that are too far from DSL stations and have no other options. WISPs may use IEEE 802.11 technologies for the entire delivery, or they may use other wireless technologies, like WiMAX (IEEE 802.16), from the operations centre to the delivery area and then use IEEE 802.11 technologies within the delivery area. Other WISPs use WiMAX all the way to the end destination, meaning it is then up to the subscriber whether to use IEEE 802.11 technologies within their house or business. Since WiMAX and IEEE 802.11 use different frequencies (if the 802.11 devices use the 2.4 GHz spectrum), there should be no conflicts or interference.

To help you understand last-mile delivery, consider the home where my friend grew up in West Virginia of the United States. They lived on a very old country road. It was not paved; it was a gravel road. They lived in the last house on the road, which was approximately 2.5 miles from the nearest paved road. They had to pay a large fee just to get electricity to the house. The electric company required such a fee since there were no other houses close to theirs. This is an example of the problems related to last-mile delivery. It's no different for the Internet today than it was for electricity then. Wireless technologies provide an excellent solution to the problem of last-mile delivery of Internet access.

In Hong Kong, the above example may not be so convincing since the density of population is extremely high here, and ISPs have enough incentive to pave the last mile for nearly every household. But another strength of WiMAX that does apply to Hong Kong is that it can offer the last mile connection for those endpoints that are 'on the move' (e.g. PDAs, notebooks, etc.). As you might expect, this capability is well-received by local users, given the high popularity of handheld devices here. Currently, the wireless connections used by these handheld devices are mainly provided by the existing mobile networks. However, the throughput of the mobile networks, even 3G, can reach only a few mega bits per second, which is much lower than WiMAX (45Mbps). It is therefore foreseen that WiMax will have plenty of scope to develop in Hong Kong.

Reading

Dean (2012) 371–73.

Self-test 9.4

1 Which access technology(ies) is currently used to provide Internet access in wireless hot spots such as cafes and libraries?

2 What is the current status of WiMax development in Hong Kong? Do a desktop research on the Internet.

Activity 9.4

The Government Wi-Fi Programme (GovWiFi) is one of the major initiatives under the 2008 Digital 21 Strategy to build Hong Kong into a wireless city. This programme aims to provide free wireless Internet access services to all citizens by installing Wi-Fi facilities at designated government premises. Its aims are as follows:

- People can surf the web freely for business, study, leisure or accessing government services whenever they visit the designated Government premises.
- Business organisations can extend their services to a wireless platform to reach and connect with their clients.
- ICT industry players can make use of this new wireless platform to develop and provide more Wi-Fi applications, products and supporting services to their clients, and open up more new business opportunities.
- Foreign visitors can enjoy Internet access at the designated tourist spots.

Visit the GovWiFi http://www.gov.hk/en/theme/wifi/program/index.htm and answer the following questions:

1 How many government premises have been installed with Wi-Fi facilities?

2 What types of premises are included?

3 What kind of security protection is enabled?

Wireless network security

Wireless communications are particularly susceptible to eavesdropping. For example, a hacker can search for unprotected wireless networks by driving around with a laptop configured to receive and capture wireless data transmission. In this topic, therefore, we introduce to you some common protection mechanisms that apply to wireless networks.

WEP

By default, 802.11standard does not offer security, but it allows for optional encryption using WEP (Wired Equivalent Privacy). WEP uses keys both to authenticate network clients and to encrypt data in transit. When configuring WEP, you establish a character string required to associate with the AP, also known as the network key. When the client detects the presence of the AP, the user is prompted to provide a network key before the client can gain access to a network via the AP. The early implementation of WEP allowed for 64-bit keys, which was not so secure. Current versions allows for 128-bit keys, which are relatively more secure. However, WEP's use of shared and static keys is still more susceptible to discovery than a dynamically generated, random, or single-use key, which is adopted by the WPA (Wi-Fi Protected Access) and will be introduced in the next section.

IEEE 802.11i and WPA

802.11i uses Extensible Authentication Protocol (EAP) with strong encryption scheme and dynamically assigns every transmission its own key to heighten the protection of the data in transmit against taping or tampering. With 802.11i enabled, logging on to wireless network is more complex than with WEP. The AP acts as proxy between a remote access server and station until the station has successfully authenticated with the remote access server. It requires mutual authentication — the station authenticates with the remote access server, and vice versa. After authentication, remote access server instructs AP to allow traffic from the client into network. Following that, the client and server agree on an encryption key for subsequent data transmission. WPA (Wi-Fi Protected Access) is a subset of 802.11i standard that is endorsed by the Wi-Fi Alliance, an international organization dedicated to ensuring the interoperability of 802.11-capable device. WPA2 is an updated version that has already gained wide support by commercial products.

Reading

Dean (2012) 531–33.

Self-test 9.5

1 Let's say you are designing an 802.11g wireless network for a local cafe. You want the wireless network to be available to the cafe's customers, but not to anyone with a wireless NIC who happens to be in the vicinity. Which security measures would require customers to enter a network key to gain access to your network via the access point?

2 What is the main difference between WPA and WEP?

A lab on wireless network security

Network analysis (also known as traffic analysis, protocol analysis, packet analysis, packet sniffing and so on) is the process of capturing network traffic and examining it closely in order to deduce information from it. A packet sniffer (also known as a network analyser, protocol analyser or network protocol analyser) is a hardware device or software that captures, records and analyses network traffic.

Network analysis can be used for both good and evil. A network administrator performs network analysis to monitor network usage, analyse network problems and debug client/server communications. A network security practitioner performs it to detect network intrusion attempts and violations against network usage policies. But hackers also perform it to gain information for effecting network intrusion and other unauthorized (and often illegal) activities. An engineer (or a student like you) can also use network analysis to investigate, study and reverse engineer protocols used over the network.

In the following lab activity you will use a powerful and free packet sniffer, Wireshark, to capture and analyse the traffic between your PC and selected remote hosts on the Internet. In addition, you will use a wireless networking tool, NetStumbler, to detect the wireless LANs in your neighbourhood. You will be surprised that many people are not running their wireless LANs in secure mode and hence are vulnerable to wireless sniffing.

Activity 9.5

Complete the 'Lab 1.5 — Network Traffic Analysis and Wireless Network Security' from the textbook *A Practical Approach to Internet Programming and Multimedia Technologies*. This exercise will help you realize how easy it is to intercept and analyse the data transmitted in networks and how to protect a wireless network.

Wireless LAN survey

Wireless LAN (WLAN) network survey is a means of collecting data about the growth and the distribution of wireless local areas networks of a particular region, or community. Furthermore, the survey results can help determine the extent to which detected network are secure. For example, under the leadership of Prof. Paul Kwok (OUHK), Dr Philip Tsang (OUHK), Prof. Reggie Kwan (Caritas Francis Hsu College) and Prof. Bebo White (Stanford University), the OUHK has conducted annual wireless LAN Survey in Hong Kong since early 2000s.

Some of the typical ways in which wireless LAN survey data can be used are to:

- support research into Wi-Fi usage by providing temporal demographic data
- map Wi-Fi access point data
- 'mashup' Wi-Fi data with a wide variety of other types of social, economic, commercial, political, etc. data.

WLAN survey tools

The following tools are used in conducting WLAN survey:

- A laptop with 802.11a, b, g card
- GPS (Geographical Position Sytem) — to locate where you are collecting survey data
- Netstumbler — a software tool to detect APs
- Wireshark — a software tool to analyse the collected network traffics data
- The vehicle of your choice — could be a car, a ferry or a helicopter. The OUHK's past surveys had been conducted using each of these types of vehicles.

WLAN survey strategy

Here are some features of the approach the OUHK team follows in conducting its surveys:

- A surveyor first uses Netstumbler while driving around in order to map out active wireless networks.
- Netstumbler locates a strong signal from target WLANs.

- Not only does Netstumbler have the ability to monitor all active networks in the area, but it can also be integrated with a GPS device to map APs.

Survey results

The following is a summary of the 2006 OUHK 802.11 Survey:

- Data collection was conducted via driving, flying and ferrying.
- Access points using basic security increased from 29% in 2002 to 64% in 2006.
- 62% of WLANs use 802.11g.
- 72% of networks using 802.11g were secured.
- 51% of networks using older 802.11 products were secured.
- Access point data mapped onto Google Earth.

Self-test 9.6

1 Why do organizations provide free Wi-Fi services? What are some of the risks in providing unrestricted Wi-Fi services to the public?

2 When conducting a Wi-Fi survey, how can the survey data be used? Give two examples.

3 What software tools can be used to help analyse Wi-Fi survey data?

Summary

In this unit you looked into a number of fundamental concepts and issues surrounding WANs and wireless network communications. Throughout the topics we covered, we focused our attention on wireless LAN technologies.

To begin with, you reviewed some topics concerning with WANs. We provide you with a brief comparison of WANs and LANs. This should have given you a sense of where WAN technologies can fit it into broader computer networks.

What followed was a survey of the host of WAN technologies that can help organizations link up their offices and premises which may be separated by a wide range of geographical distance. Before switching to wireless communications, we described the local landscape of WAN services provisioning, to see what we can get from market offers.

You then went on to study the wireless network technologies. We began by discussing the wireless LAN technologies that fall under the IEEE 802.11 series, including 802.11 a, b, g and, the latest member, n. After that, we covered Bluetooth and Infrared (IR), which are in common use for connecting peripherals to the main computer unit.

Next was a topic concerned with wireless LAN design. We concluded this part with a lab aimed at setting up an *ad hoc* wireless network. The Internet has become a mainstream use of the wireless network technologies. In addition to Wi-Fi, we also discussed WiMax, an upcoming wireless broadband access technology, and made a brief note of the local development of the wireless broadband access service provisioning.

You then learned how network security is a very important topic that can't be separated from wireless communications, simply because of the plain fact that a signal transmitted over the air can be intercepted by anyone, including those with malicious intentions.

We ended the unit with by introducing a wireless LAN survey, which is an important academic exercise conducted by the OUHK since early 2000s. You saw what kinds of benefits we can gain from such research activities.

Answers to self-test and activity questions and exercises

Self-test 9.1

1 Any three of the following are accepted.

	LAN	WAN
Coverage	Covers a smaller area	Covers a wider area
Technology	Primarily Ethernet, Wi-Fi, etc.	Metro Ethernet, Leased Line, ATM, Frame Relay, etc.
Operation	Typically operated, controlled, and managed by a single person or organization	Typically operated by public network server providers (also known as carriers)
Transfer rate	High data transfer rate	Lower data transfer rate as compared to LANs
Cost	Not very expensive	Higher costs

2 Data modulation

3 The router should be installed between the cable modem and the workstations.

4 OC1

5 Time division multiplexing

6 Any type of Internet connection. The two end points of VPN are often connected by the Internet, which makes VPN so cost-effective.

Self-test 9.2

1 Each wireless network is identified with a SSID (Service Set Identifier) — a unique character string — through which users can decide which wireless network they would associate with.

2 The AP is a device used on wireless LANs that transmits and receives wireless signals to and from multiple nodes, and retransmits them to the rest of the network segment. Access points can connect a group of nodes with a network or two networks with each other. They may use directional or omni-directional antennas.

3 2.4–2.4835 GHz.

Self-test 9.3

1 CSMA/CA

2 802.11a: 54Mbps, 802.11b: 11Mbps, 802.11g: 54Mbps, 802.11n: 600Mbps,

3 MIMO (multiple-input and multiple-output) is the use of multiple antennas at both the transmitter and receiver to improve communication performance. MIMO technology has to be used in wireless communications (e.g. 802.11n), since it offers significant increases in data throughput and link range without additional bandwidth or transmit power.

Self-test 9.4

1 IEEE 802.11 (any of 802.11a, b or g).

2 In late 2008, OFTA issued Broadband Wireless Access licences to three local service providers, i.e. Genius Brand Ltd., CSL Ltd. And China Mobile Hong Kong Company Ltd. It is believed some of the providers will use WiMAX technology to deliver their wireless broadband service to the local community. The licensees will provide BWA services within five years from the date of the issue of the licenses.

Self-test 9.5

1 WEP

2 WPA dynamically assigns every transmission its own key to heighten the protection of the data in transmit against taping or tampering, while WEP uses a static key for all transmissions.

Self-test 9.6

1 Some governments provide free Wi-Fi service to widen the access to the Internet among their citizens for the benefit of the community at large. Some network operators providing such services for free intend to uphold their social responsibility or to be part of their marketing campaign. In this way, free Wi-Fi service can help attract more business. Service providers face such risks in that users may abuse the services by, for example, downloading files of huge volume, distributing unlicensed materials through BT, sniffing the data of other Wi-Fi users, etc.

2 The collected can be used to:

   i support research into Wi-Fi usage by providing temporal demographic data

   ii map Wi-Fi access point data to understand their geographical distribution

iii ‘mashup’ Wi-Fi data with a wide variety of other types of social, economic, commercial, political, etc. data.

3 Such tools include Netstumber, AirSnare, Wireshark (ie. Ethereal), OmniPeek, etc.

Activity 9.2

This is an open question. You should come up with your own answer. The following are some example of the reasons:

1 802.11 signals travel farther than Bluetooth signals.

2 802.11 technologies transmit data at higher throughputs than Bluetooth.

Activity 9.4

1 Around 350 premises, at June of 2009.

2 These premises include public libraries, public enquiry service centres, sports centres, cultural and recreational centres, cooked food markets and cooked food centres, job centres, community halls, large parks and Government joint-user buildings.

3 WPA2-Enterprise.

Glossary

access point — A device used on wireless LANs that transmits and receives wireless signals to and from multiple nodes and retransmits them to the rest of the network segment. Access can connect a group of nodes with a network or two networks with each other. They may use direction or omni-directional antennas.

analogue data — Information composed of continuous varying values such as voice and video.

analogue link — A link on which analogue signals can be transmitted.

analogue signal — A continuous signal varies constantly in voltage. The value of the signal varies all the time during transmission.

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

ANSI — American National Standards Institute.

AP — See Access Point

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. Simpler and cheaper than broadband, Ethernet is a baseband network.

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

broadband — Sometimes also referred to as wideband. It's 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, broadband refers to a system in which multiple channels access a medium, for example coaxial cable, that has a large bandwidth using Radio Frequency (RF) modems. This may allow the coaxial cable to carry multiple separate LANs whose transmission is being modulated at different frequencies. In cable television (CATV), broadband describes the ability to carry 30 or more TV channels and is synonymous with wideband.

broadcast — A message (e.g. packet or frame) sent to all the nodes on a network.

broadcast domain — The part of a network which receives the same broadcasts.

browser — A computer program providing access to sites on the World Wide Web.

byte — A group of eight bits.

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

client/server network — A networking system in which one or more PCs (the client) is the requesting machine and the server is the supplying machine, both of which are connected via a local area network (LAN) or wide area network (WAN).

CSMA/CD — Carrier Sense Multiple Access/Collision Detect, a common **Ethernet** protocol.

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

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

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

fibre optic cable — A cable, consisting of a centre 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.

frame — A term for the unit of data transferred on a network; its 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 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.

Hotspot — A hotspot is a physical location that offers internet access over a wireless LAN through the use of a shared internet connection and a single router. Hotspots can typically be found in coffee shops and various other public establishments throughout a city.

Internet — A global network of networks used to exchange information using the TCP/IP protocol. It allows for electronic mail and the accessing and retrieval of information from remote sources.

LAN — See Local Area Network.

Local Area Network — A network connecting computers in a relatively small area such as a building.

Mbps — Megabit per second.

Megabit — One million bits.

modem — A device that convert 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 — End point of a network connection. Nodes include any device attached to a network such as file servers, printers, or workstations.

optical fibre — See fibre optic cable.

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

ports — A connection point for a cable.

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

segment — A section of cable on a network. In Ethernet networks, two types of segment are defined. A populated or trunk segment is a network cable that has one or more nodes attached to it. A link segment is a cable that connects a computer to an interconnecting device, such as a router, bridge or switch.

UNIX — Operating system developed in 1969 at Bell Laboratories. UNIX has gone through several iterations since its inception. These include UNIX 4.3 BSD (Berkeley Standard Distribution), developed at the University of California at Berkeley, and UNIX System V, Release 4.0, developed by AT&T.

URL — Universal Resource Locator. Standardized addressing scheme for accessing hypertext documents and other services using a WWW browser. See also browser.

VPN — Virtual Private Network. A means for establishing a secure network connection between two end points over an unsecure public or open network.

WAN — See Wide Area Network.

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

WLAN — A short form of wireless LAN.

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

References

Carpenter, T (2008) *CWNA — Certified Wireless Network Administrator Official Study Guide*, 4th edn, New York: McGraw Hill

Dean, T (2012) *Network+ Guide to Networks*, 6th edn, Thomson Course Technology.

Kwan, R, White, B, Tsang, P, Kwok, P, Eustace, K and White C (2009) *IEEE 802.11 WIFI Survey & Visualisation Experiments*, Hong Kong: Pearson Prentice Hall Publishing.

Kwan, R, Tsang, P, Kwok, P, Koong, K, Mak, J and Wu, J (2009) *A Practical Approach to Internet Programming and Multimedia Technologies*, Hong Kong: Open University of Hong Kong Press.