ELEC S212

Network Programming and Design

Unit 10

Network solution design and network marketing

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
Dr Philip Tsang, OUHK

Designer: Ross Vermeer, OUHK

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

After studying the previous units, you should be familiar with various concepts in computer networking. It's time to practise designing a network. The design process involves all network components, so this will help you consolidate everything you have learned.

Network design is an important phase in developing a network. It is important to know that there is no absolute answer in network design. However, one goal you must achieve is that *the network must work*!

In this unit, you will find that network design is actually a trade-off between *cost* and *availability*. What does availability mean? The answer may be different to a user and a network designer. A user may care about the response time, the throughput and the reliability of a network. A network designer, on the other hand, may be very concerned about the flexibility towards changes and the manageability of the network. Network designers should always try to maximize availability and minimize cost.

You can set up a network without having a design phase. However, it is not good practice, especially for the development of a large network. The flexibility and upgrade path of the network greatly depend on the initial design of a network. Network design is actually an iterative process. You must first analyse the requirements of the network. Then you have to make choices about technical options in designing the infrastructure. After building the network, proper maintenance and optimization can enhance its performance.

Indeed, requirements for network design solutions have changed a great deal in recent years as new technologies have emerged quickly. These changes make design more difficult than ever. The trend is towards increasingly complex environments involving multiple NOSs, multiple protocols, increasing multimedia-related content and interconnection to networks outside any single organization's domain of control. Carefully-designing networks can reduce the hardships associated with growth as a networking environment evolves.

This unit consists of two parts. In the first part of this unit, we try to give you an overview of planning and design guidelines. We present guidelines for designing and running a computer network, including both local area networks (LANs) and wide area networks (WANs). You will apply what you have learned in the previous units to design, implement and maintain a computer network.

Our discussion is divided into the following topics:

The first two sections present an introduction to network design and the goals of network design in general. Network requirements should be carefully analysed before the network is built.

The third section presents a detailed analysis of the requirements, which include determining users' requirements, the distribution of the nodes, the nature of the applications to be run on the network, future expansion of the network, and of course estimating the cost for implementing the network.

The fourth section goes into the details of the design phase of a network. In this phase, a network designer should decide what network technologies and architectures should be used. In addition, the type and bandwidth of the backbone to be used, and the trade-offs of bridging and routing, are of great concern.

The fifth section uses Windows Server 2003 as an example of the implementation of a network. Details of various issues concerning the implementation are presented.

In the sixth section, network maintenance and troubleshooting are discussed. These topics are important for improving network performance in the long run.

In the second part of this unit, the final section introduces the basic concepts in network marketing. You will see why it is important to design for marketing, and to design in a global environment based on a network marketing framework. A range of different approaches to network marketing will be discussed, and you will study the story of a successful networking company.

In short, this unit:

- outlines the network solution design process;
- analyses network requirements and existing network designs, and identifies areas for improvement;
- discusses basic network design issues, and identifies points of concerns in network design;
- discusses network solutions that satisfy both business and technical goals;
- discusses basic issues related to network solutions implementation;
- discusses basic issues related to testing, optimizing and documenting network design solutions, and to security issues related to network solution design; and
- identifies the key points in network maintenance, analyses simple network problems and implements corresponding troubleshooting procedures.

This unit is intended to take you five weeks (or approximately 44 hours) to complete.

The goals of network design

Design goals may be particular to a network. A national military agency may require its network to have the fastest response in order to have immediate control over their weapons. A stock market will need an extraordinarily reliable network, since billions of dollars may be lost if the network goes down. Nevertheless, there are still some general goals that a network designer should work toward.

Key goals in network design

Network designers have their own concerns about technical issues in designing a network. Some of these concerns match those of the users, but there may be others that the users don't even think of. Generally, a designer looks for several requirements:

- functionality
- scalability
- adaptability
- manageability
- cost-effectiveness.

Functionality

To designers, the network must work and meet the particular requirements of their users. Therefore, their basic concern will be the *functionality* of a network, which indeed matches users' concerns with capability and quality of services.

But note that it is *not* necessary to make all applications through the network. Some applications may be only available to some machines, and some may be installed only on a given machine's local hard disk.

Scalability

Scalability is the network's ability to cope with the growth of the organization, such as supporting more users and applications.

Adaptability

Adaptability is the network's ability to adopt future technologies. A network should not contain an element that would limit the adoption of new technologies. Scalability and adaptability match users' concerns about flexibility. Statistics gathered on monitoring, and experiences accumulated in management of a network will be important to the improvement or future redesign of the network.

Manageability

Designers may regard *manageability* as one of their design goals. Indeed, manageability is also important in ensuring the ongoing stability of operations and availability of resources of the network. However, users may not have the same concerns about the manageability of a network, since they only concentrate on what functions the network can provide, rather than on how the network is managed.

Cost-effectiveness

A designer is responsible for weighing the costs required and the benefits provided by the network, so *cost-effectiveness* is another main concern. Large organizations increasingly rely on electronic data for managing business activities, and a lot of companies even start their businesses on the Internet. It is foreseeable that the associated costs of developing a network will continue to rise, so it is increasingly important for designers to balance network capabilities and network development cost.

Tradeoffs in network design

In a perfect world, a competent network designer can design a dream network that satisfies all design goals and implement it. However, in the real world, there are always insufficient resources, budget and time to make the implementation of such a dream network possible. As such, network design in reality always involves tradeoffs among key network variables:

- capability;
- flexibility;
- quality of service; and
- cost.

Capability

Capability is the functions that can be delivered by the network. For example, can the network support voice or video applications? What about electronic mail and Internet access?

Flexibility

Flexibility is the ability of the network to adapt to changes or expansions. Can the new applications purchased be run on the network? Can the network adopt newly emerging technologies for enhancement?

Quality of service

Quality of service is concerned with whether the network can meet user requirements. Requirements may be different from user to user, but generally several aspects are common:

- reliability; that is, how well it can cope with errors;
- speed of responses;
- accessibility, that is, user-friendliness; and
- network security.

Cost

Cost is the most important key category of network design variables nowadays. You may think that the best design should maximize the network's capability, flexibility and quality of services. This may result in an ideal network. However, the cost may be too high, and it is important to be cost-effective in network design. In real life, network designers always have to make cost their main concern. The best design is one that can meet the main requirements of the users within budget. This involves trade-offs among the design variables.

Very often, there is a tradeoff between the first three variables and the last one. We cannot build a network with unlimited cost. In real life, the budget may actually be very limited!

Self-test 10.1

1 What is the key trade-off that must be made in most network design?

2 Describe the five goals of a network designer in designing a network.

Analysing network requirements

In order to assess all network requirements, a detailed analysis has to be undertaken. Networking aims at helping your organization achieve business goals, so the most important requirements come from the network users. The geographical distribution of the offices of your organization also affects the network structure, as different network technologies will be used to connect nodes nearby and far away. The nature of the applications to be run on the network indicates the bandwidth demand of the network, thus affecting the network technologies and the speed of the link to be used. A designer also has to know about the latest emerging technologies and whether the organization will be expanding in the near future.

To achieve cost-effectiveness, a designer needs to carry out a careful cost estimation. A cost estimation is done by dividing the costs into two parts: one-time and recurrent. The costs may be further broken down into individual items. In order to better predict network performance, a designer may perform simulations of network loading. First of all, let's look at these network requirements in more detail.

User requirements

Analysing a network's user requirements is very important, but it is usually ignored by network designers, who focus on the technologies of the network setting. The flexibility to connect different devices is always the first thing that designers consider. However, users are concerned with aspects such as:

- the response time;
- the reliability of the applications running on the network; and
- security.

Response time is generally considered the time between the entry of a user action and the host system execution of the command, or delivery, of a response. Indeed, it may be quite subjective to say that the network responds quickly or slowly. But some applications are very time-critical. Good examples are systems providing interactive online services like automated teller machines, ticket-selling systems and identity-verification systems used by customs officials. You can imagine such irritating scenes involving long queues even when you have to wait several minutes before an automated teller machine is free so that you can withdraw money.

For mission-critical applications such as financial services, users may put the *reliability* of the network as the first priority, since millions of dollars may be lost if one of these networks is down for even an hour. Determining the cost of any down time is essential in determining the relative importance of reliability to your network. A network designer has to make decisions on various technological options in order to meet

users' requirements. For example, a designer may decide to use high-speed links in order to give fast responses to the users, and to build redundant paths to the servers for fault tolerance in the network.

Users have more and more concerns about network security. This is especially true in organizations in which highly confidential data are kept, such as government security agencies and military agencies. If all corporate information is readily available to all employees, security violations and inappropriate data access may occur. There are procedures to avoid this happening. In *Unit 8* you got an overview of network security. There are things that we can do in the design stage to avoid security loopholes. For example, you may control the access to internetworking devices, like bridges and routers, and local traffic in individual LANs of the branches so that users cannot reach the backbone inappropriately.

You may find that your users need constant changes in network functionality, in response to changing business conditions and changing technologies. Upgrading and redesigning the existing network, rather than designing a network from scratch, is what designers usually face. For example, the increasing popularity of voice- and video-based network applications may add pressure to increase the bandwidth of the current network. In addition to considering the cost, a designer may have to work out a careful procedure for upgrading, to avoid disruption of the services provided to the users.

Geographical considerations

Network nodes may be confined to a single office within one floor or one building. However, nodes may also be distributed in several locations across cities, countries or even continents. As you learned in *Unit 2*, we cannot use Ethernet in a very large area, since the technology imposes a distance limit between the nodes. Very often, nodes in one location will be connected to form a LAN with technologies such as Ethernet and Token Ring. In such cases, several LANs in different geographical locations will be connected through internetworking devices like bridges and routers to form a WAN, as shown in Figure 10.1. Since data flow will usually be more intensive within the same location, such a design can isolate the network traffic to individual locations, and thus not overload the whole network. In WAN connections, WAN technologies such as dedicated lines, X.25 (to be discussed in the section on network technologies), and Digital Subscriber Lines (DSLs) have to be used. These technologies provide a speed of data transfer relatively slower than those of LAN technologies.

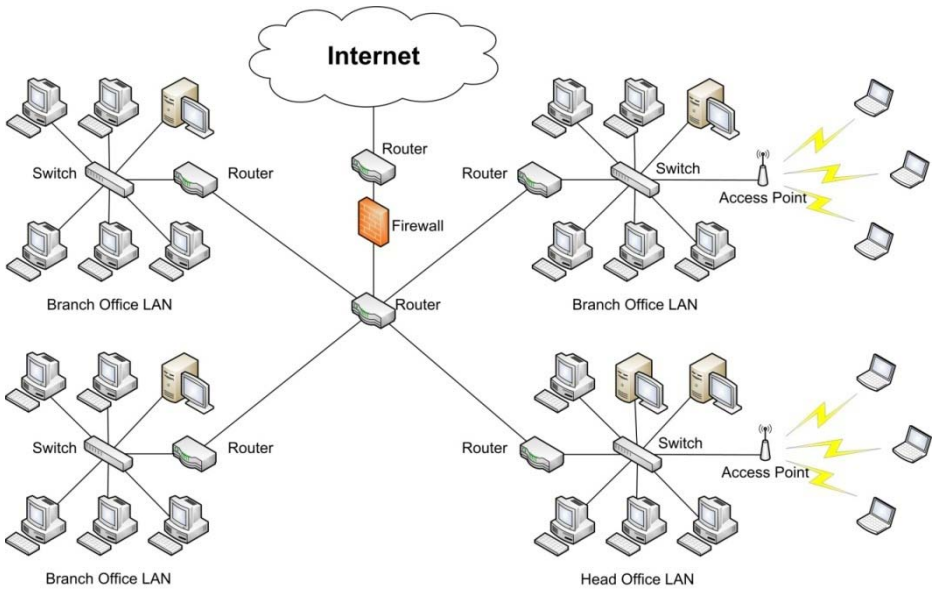


Figure 10.1 A typical network structure

In designing a network, maps and floor plans are usually needed to construct network plans in different stages of network design. This helps the designer have a clearer concept of the distribution of the nodes, what cables are needed and where they are needed.

Nature of applications

You may think that users' requirements are often based on the nature of the applications to be run on the network. As you've learned, though, users normally require a network designer to consider response time and fault tolerance before other factors in the design, if the network is going to support applications providing online services and mission-critical applications respectively.

The nature of the applications also determines the loading a network has to support. If an application supports a large number of users, very busy network traffic is expected. Therefore, good **segmentation** has to be planned into the design. Segmentation helps both in isolating the network traffic within a particular area of a network and in reducing the loading caused by broadcasts to the overall network.

Some applications may require a very intense data flow. In order to achieve a reasonable response time, it is necessary to design a network that has the capability of scheduling tasks. A typical example is the replication of database information between different hosts. The traffic involved in the replication represents a high-volume process. These applications can often be scheduled as day-end jobs, or at times when response-time-sensitive traffic is low.

Network applications usually use a client/server architecture. A central database located in a server, or distributed in several servers, is accessed by clients distributed across the network. In this case, the servers should be connected to the network through a link with a larger bandwidth and a

higher speed compared to links connecting the clients in a separate segment, as shown in Figure 10.2. So when multiple clients access the server database, the link connecting the server will not become a bottleneck slowing the response time of the application.

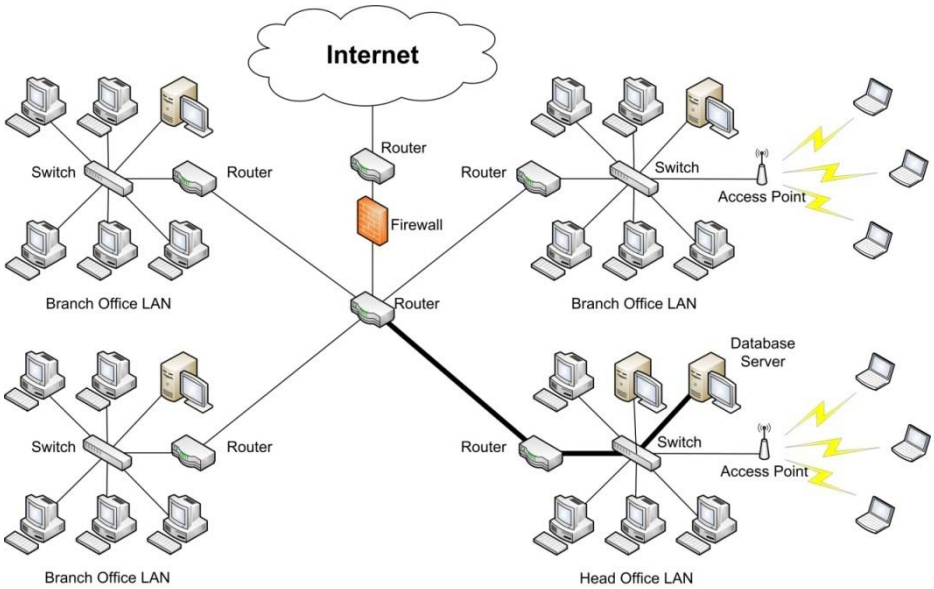


Figure 10.2 Network traffic in client/server architecture

Future expansion

Users have changing demands on the functions of a network in response to changing business conditions and information technologies that are developing very fast. It's obvious that a network design cannot cater for all future demands. However, the network should be designed with an eye toward *future technologies* so that new technologies can be adopted for upgrading the network when required.

As you learned in the section on design goals, scalability and adaptability should be catered for in designing a network. These are important metrics for measuring a network's ability in dealing with future expansion. Scalability involves the capability of the network to deal with the growth of the organization; that is, the increasing number of users, applications and data volume that lead to the increasing use of the network. For example, the organization may have a plan to use video-based applications in the future. The designer should pay more attention to the bandwidth requirement of the network to be designed, as video-based applications put high-volume data flows on the network. Also, although your organization may not have a plan for connecting to the Internet at present, it would probably be required in the near future, because of the increasing popularity of the Internet. The network should then be designed in a way that Internet access could be easily implemented.

Sometimes a designer may decide to adopt a new technology to cater for these demands, and this leads to the challenge of adapting the network. Adaptability involves the capability of the network in adopting new

technologies. If the network is designed in a way that new technologies cannot be applied on it, its future growth is seriously limited. The installation of Category 3 instead of Category 5 cables is a good example. Since the maximum speed of data transfer for a Category 3 cable is only 10 Mbps, it cannot support Fast Ethernet and Gigabit Ethernet, which is becoming more and more popular in LAN implementation for supporting 100 Mbps or even 1000 Mbps speed of data transfer. If the network has to be upgraded to Gigabit Ethernet, the cables have to be reinstalled. However, if Category 5 (or better yet, Category 5e) cables are installed at the beginning, the network can support the speed of up to 1000 Mbps.

To make good decisions on network design in catering for future expansion, a network designer should have up-to-date knowledge of both current and emerging technologies. Network designers may keep themselves current by attending professional conferences, seminars and by reading widely.

Cost estimation

As a network designer, you are required to provide the benefits of a network to the executives of your organization. In order to justify the development of the network, you may need to show them a brief list of the overall costs. The development costs of a network depend on equipment and types of service required.

You can categorize the costs according to the LAN and WAN implementation. For each of them, you should subdivide the costs into two parts:

- one-time (fixed); and
- recurring.

One-time costs for both LAN and WAN implementation include purchasing and installing network hardware and software. There is a fixed cost for the cabling in building a LAN, which is not required in a WAN.

Recurring costs for both LANs and WANs include the maintenance and upgrade costs for the network hardware and software, as well as their operating costs. After setting up a network, network specialists are required to monitor, configure and maintain the smooth operation of the network. This support cost is not a one-time charge. Iterative monitoring and tuning of the network performance is very time-consuming and expensive. As mentioned above, no fixed cabling cost is required for WANs because WAN connections, such as dedicated lines or X.25 connections, are usually rented from local telecommunication companies.

For both LANs and WANs, the recurring costs typically tend to dominate. Therefore, in considering the trade-offs among the design variables mentioned in the design goals section, you should first think of how to reduce the recurring costs.

Network simulation

Simulation of network loading can provide a lot of empirical information for designers. This helps the designers in their design development, as it can give them a rough estimate of the real network loading. The modelling should consist of the installation of a working network and monitoring traffic for a given number of users, applications and network topology. Simulation prevents over-complication of the design solution and highlights any areas where the network design solution does not meet the specified needs.

A simulation can give you a rough idea of the performance of the network. Certainly, if you input more information about the modelling, you can achieve better results. Furthermore, you can try extrapolating to the predicted future number of users, applications and topology.

A very popular (especially in academia) open source network simulation tool is OMNeT++. It is built on C++ to simulate large communication networks with detailed protocol modelling and performance analysis. Its features include graphical model specification and an integrated data analysis tool. It allows you to quickly create, simulate and analyse a network. We highly recommend that you download it from http://www.omnetpp.org, and try it out.

If you are looking for industrial-strength solutions for network planning, engineering, operations, and R&D, you are highly encouraged to look up OPNET's solutions. The following figure shows some screenshots of OPNET Modeler, which is OPNET's flagship product for network simulation. (Note: OPNET is now part of Riverbed, https://www.riverbed.com, and OPNET Modeler has been renamed Riverbed Modeler.)

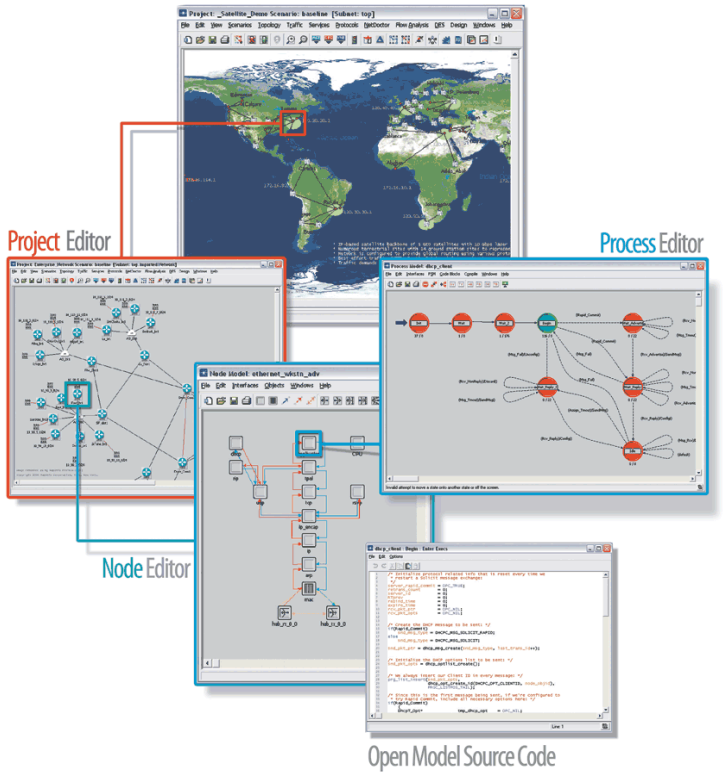


Figure 10.3 Screenshots of OPNET Modeler, a powerful network simulation tool

Source: OPNET Modeler

Needs assessment

The following reading introduces the concept of a needs assessment, which is the process of obtaining objective needs. In performing the assessment, you can investigate a network's needs and requirements as they relate to users, network performance, availability, scalability, integration and security. After the requirements are clarified, you can then draft your project plan for management approval.

Reading 10.1

Dean, T (2002) 'Managing network design and implementation' in Network+ Guide to Networks, 2nd edn, Course Technology, 810–18.

Self-test 10.2

1 How can a network design tool help in network design?

2 Why does it cost significantly more to achieve 99.99% availability than it does to achieve 99.5% availability?

3 Give two examples of projects that might be driven by security concerns.

Designing a network infrastructure

In designing a simple LAN, you need to make decisions on concerns like the media, the topology, Ethernet or Token Ring and the Network Operating System (NOS). What you have learned from *Units 1* to *4* should be enough to help you make informed decisions.

For a large network, we cannot simply connect all of the nodes on the media. As the media are shared among nodes, the immediate problem is excessive collisions on Ethernet or a long waiting time for the token in Token Ring. We call this media contention. You may have to break the network into segments and interconnect the segments with appropriate internetworking devices like bridges and routers. By doing this, local traffic is isolated in each segment, and communications between segments are enabled through internetworking devices.

Network broadcasts and multicasts are another matter that you have to pay serious attention to. A server may announce its services through a **broadcast**, and a client may look for services through broadcasts. Some communication protocols depend heavily on broadcasts to get information from or to send announcements to the network. All nodes receiving the broadcasts have to process them. However, not all nodes on the network are intended 'audiences' of these broadcasts. The same is true for multicasts. Excessive broadcasts and multicasts seriously downgrade network performance.

In designing the network infrastructure you also have to consider other issues like 'backbone' strategies, network technology, and network addressing. The word 'backbone' is very often used to describe the part of the network that interconnects the other parts of the network. Discussion of these infrastructure topics is divided into the following subsections:

- segmentation
- bridging, switching and routing
- Virtual Local Area Networks (VLANs)
- wireless networks
- backbone strategies
- hierarchical model
- network technologies
- connecting to the Internet.

Segmentation

On Ethernet, **collisions** in data transmission occur among nodes on the same cable segment. The cable segment forms a **collision domain**. Repeaters or hubs used to extend the cable segment cannot isolate the collisions within individual segments. Segments connecting through repeaters still form a single collision domain. All nodes in the collision domain (also known as a bandwidth domain) compete for the same network bandwidth. All traffic from any node in the bandwidth domain is visible to all of the other nodes. Table 10.1 below shows the effective bandwidth of an Ethernet network. Because of collisions among nodes in transmission, the standard bandwidth of 10 Mbps for an Ethernet network can only be achieved when there is only one node in the segment.

Table 10.1 Effective bandwidth of an Ethernet network

Number of nodes	Utilization rate in the segment	Effective (approximate)	Effective bandwidth per node
1	100%	10 Mbps	10 Mbps / 1 = 10 Mbps
10	70%	7 Mbps	7 Mbps / 10 = 700 Kbps
100	35%	3.5 Mbps	3.5 Mbps / 100 = 35 Kbps

Segmentation is the process of splitting a single collision domain into two or more collision domains. *Bridging* and *switching*, which operate in the data-link layer (layer 2 of the OSI model), can be used in segmentation and to create separate collision domains. This result is more bandwidth being available to individual nodes. Segmentation to the extreme puts each node in a separate collision domain. This is called **microsegmentation**. Switches can isolate each node connecting to one of its ports into a collision domain and thus are usually used in implementing microsegmentation.

Routers can also be used in segmenting a collision domain. However, it is a more intelligent device than is usually used in isolating **broadcast domains** and implementing segmenting policies.

You should notice that the packets broadcast using the network layer (layer 3 of the OSI model) address can still pass through all the collision domains. The segments connected through bridges or switches represent a single broadcast domain. Although bridges and switches will not forward collisions, they will forward broadcast packets. Here we introduce the term *broadcast radiation*, which is the way that the broadcasts are transmitted out from a source node causing all the nodes in the same broadcast domain to undertake extra processing. Routers can act as a broadcast filter to isolate broadcast radiation within a segment.

Routing, bridging and switching

Routing, bridging and switching are common internetworking processes in network segmentation. Switching is a relatively new technology. In previous units, you learned about the bridging, routing and switching technologies in detail. Therefore, we just review the key concepts of these technologies in this section. The capabilities of routers, bridges, and switches are different, so as a network designer, you must know when and where to use which device in internetworking.

The following subsections provide a summary of routing, bridging and switching.

Routing

Routing offers the following advantages over bridging and switching:

- Routers can choose the optimum path between source and destination, whereas bridges are restricted to a specific path through an internetwork. Bridges must learn the location of stations based on the direction from which traffic is received, and bridges are transparent (in other words, they are not permitted to modify a packet in any way).

- The convergence time of a routing table is much faster than the convergence time of a bridging table. This property is important, as it affects the network response time after a network reconfiguration. Routers are able to recognize new paths as soon as routing information is received.

- The number of hosts supported by a routed internetwork is not limited, but the maximum number of stations in a bridged internetwork is constrained to thousands of end stations. The reason is that routers can accommodate a much larger address space, because network layer addresses include information that groups nodes into areas or domains.

- Routers can provide a barrier against broadcast storms; bridges cannot. This can alleviate the problem of broadcast traffic from different network segments.

- Large packets can be divided into several small packets by routers. Since routers work at the network layer, this layer header includes fragmentation and reassembly information; the data link layer header does not.

Bridging

Bridges provide certain features that routers cannot achieve. Under certain circumstances, we may choose bridges to implement the internetwork. The advantages of using bridges are given below. These are useful guidelines when choosing between routing or bridging:

- The installations of bridges are very simple; they do not require configuration. You do not need special knowledge as is the case in the configuration of routers. You can simply take the bridge out of the box, power it up, and attach it to a network.

- *Pricing* for bridges is usually more attractive than for routers. A bridge is a good choice when reductions in costs are needed.

- Bridges are network layer protocol-independent, but routers are network layer protocol-dependent. Bridges can handle multiple protocols with almost no configuration.

- Some protocols are not routable; you cannot implement routers to connect these networks. However, bridges are able to forward non-routable protocols. This remains a compelling reason for implementing bridging capabilities for supporting certain end-to-end connectivity requirements.

Switching

Switching offers the same advantages as bridging. In addition, it can be used in microsegmentation and Virtual LAN implementation, discussed in the next section.

Integrated solutions

Since routers, switches and bridges are designed for different purposes, it is common to develop a network with a combination of these three technologies in order to fulfill requirements. Because of the simplicity of bridging, bridges may be used in remote site LANs. Routers may be relied on to provide a reliable, self-healing backbone, as well as a barrier against inadvertent broadcast storms in the networks.

In fact, bridging is becoming less common. Most network designers now use switching instead of bridging in most parts of their designs, and they use routing as a supplement to switching. Switching can perform the jobs done by bridging and at the same time provide a higher bandwidth for each node.

Virtual Local Area Networks (VLANs)

A **Virtual Local Area Network (VLAN)** is a logical grouping of network nodes, regardless of their physical locations, to form a single broadcast domain. The nodes within a VLAN communicate with each other like those in a LAN. But the nodes in a VLAN may be distributed anywhere in a campus or even across geographically-dispersed regions.

Most switches available now are capable of VLAN configurations. Usually, VLANs are configured according to the ports of a switch. More advanced switches allow the VLAN configuration based on the MAC address of the nodes or other criteria. For a multi-switch VLAN, VLAN

information has to be shared among the switches. However, the methods for sharing VLAN information have not yet been standardized. The traffic generated within a VLAN stays within the VLAN. Communications between VLANs have to be done through routers.

Reading 10.2

Edwards, J and Bramante, R (2009) *Networking Self-Teaching Guide*, Wiley, 514–18.

To summarize, VLANs are commonly used in implementing networks because of the following advantages:

- *Performance* — Some users in the network may need to use applications that generate intensive network traffic. These users may be distributed in different geographical locations, so you cannot group them in a physical LAN. You may then assign these users to their own VLANs to isolate their traffic. The traffic stays in its own VLAN, and does not affect the other network users.
- *Network management* — A user may change to another VLAN without physically relocating its machine. You may assign users to different VLANs through the software on the switch without any re-cabling. Users may stay at their current physical locations and join different VLANs according to the organization's policy.
- *Broadcast control* — A VLAN provides a single collision domain to the nodes attached, just like a physical LAN. Broadcast and multicast traffic can then be confined within the VLAN.
- *Security* — VLANs have to communicate with the outside network through a router. You may easily implement security measures on the router.

Self-test 10.3

What are the criteria that are commonly used to determine the membership to a particular VLAN?

To apply what you have learned about network infrastructure so far, try the following case study task.

Case study 10.1

Asia University

Background

There are four buildings in Asia University: Arts, Science, Engineering and Administration. These buildings are all within a few hundred meters of each other. AU needs a substantial upgrade to its network. This network upgrade should take the next three to five years of growth into consideration. It is expected that high-bandwidth demanding applications will be used.

Current network

The current network is flat and bridged. The LANs in Arts and Science are facing the problem of network congestion. The primary networking protocol is TCP/IP. The physical/data link layer is primarily Ethernet. The details of the network layout are as follows:

Arts

1 It has six floors strung together with 10Base2 Ethernet.

2 It has a cluster of multiprocessor UNIX servers.

3 150 PCs running TCP/IP are distributed throughout the building.

4 80 UNIX workstations are distributed throughout the building.

5 Traffic patterns are fairly stable; 75% of the traffic is to the local servers.

6 Connection to the Internet is available in this building. The connection is done through two dedicated PCs with V.90 modems. Students must physically go to the Arts building to use the Internet connection.

7 The Arts building is bridged to the Science and Administration buildings.

Science

1 It has eight floors with 10BaseT hubs on every second floor.

2 It has a cluster of multiprocessor UNIX servers.

3 It has 100 PCs running TCP/IP distributed throughout the building.

4 It has 50 UNIX workstations distributed throughout the building.

5 Traffic patterns are fairly stable; 75% of the traffic is to the local servers.

6 The Science building is bridged to the Art and Engineering buildings.

Engineering

1 Five floors are bridged through a bridges floor.

2 It has 100 PCs running TCP/IP distributed throughout the building.

3 It has 50 UNIX workstations distributed throughout the building.

4 Some end stations are connected through 10BaseT hubs; others are attached to Thick Ethernet that runs throughout the building.

5 Traffic patterns are fairly stable; 75% of the traffic is to the local servers.

6 The Engineering building is bridged to the Science and Administration buildings.

Administration

1 There is a Token Ring network that has three UNIX servers.

2 There are 50 PCs accessing the three UNIX servers on the Token Ring network.

3 The Token Ring network is not attached to the campus Ethernet bridged LAN. The Ethernet simply passes through this building, going to Engineering and Science. Any access to the Administration systems requires that you be in the Administration area.

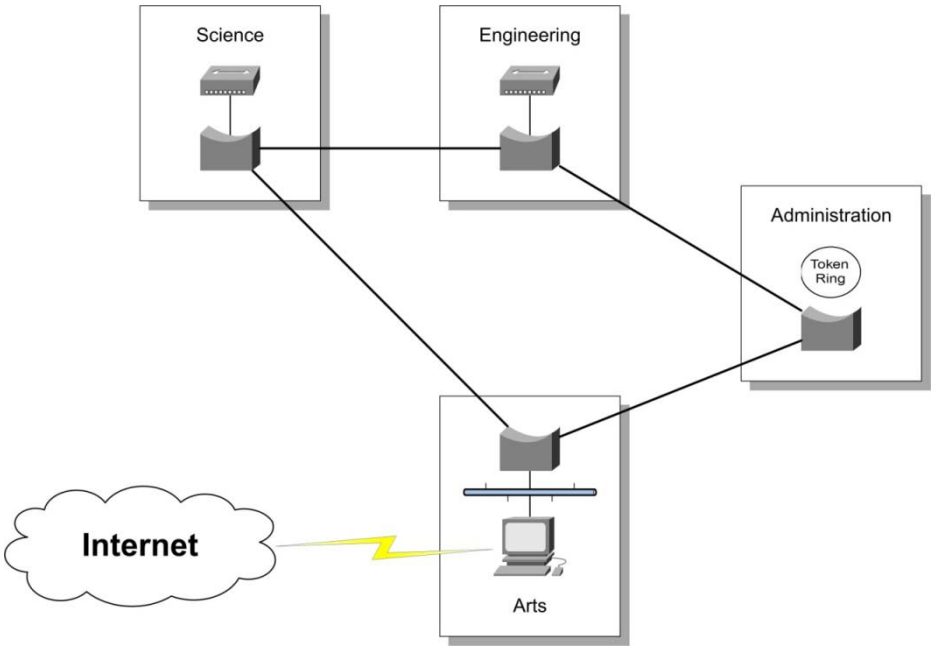


Figure 10.4 Original design of AU's campus network

New network requirements

AU is seeking a complete redesign of the network. The requirements for the new design are as follows:

1 The network congestion problem in Art and Science must be solved.

2 Any network user, in any building or department, must be able to communicate with any other user via email. In addition, all users must have access to the Internet.

3 The use of the buildings by departments will remain the same. More end stations in each building may be needed, but not at this time.

4 The positioning of servers may change. It is desirable to have the servers as centralized as possible for ease of management.

5 The LAN in Administration is incorporated into the enterprise network. In fact, the Token Ring LAN can be eliminated or replaced by a different network access technology if the alternative can provide better performance and reliability, but at a lower cost.

6 There must be a future upgrade path that can support new technology, more bandwidth demands, and possible remote users or other campuses via WAN connections.

Outline a design option to meet the network requirements.

Wireless LANs

In the recent years, the number of wireless local area networks (WLANs) in operation has been growing rapidly. Wireless LANs transmit data through the air using radio transmission rather than through twisted-pair cables or optical fiber cables. WLANs serve the same purpose as LANs: they connect a series of computers in the same small local area to each other and to a backbone network.

WLANs are usually not totally wireless in that they are most commonly used to connect a set of wireless computers into a wired network. However, WLANs enable you to use the network in places where it is impractical to put a wired network. WLANs also enable mobile staff to work at different locations in the office building or to easily move their computers from one location to another. WLANs are usually available in coffee shops, large shopping centers or the airport in Hong Kong, for example.

In *Unit 9* you learned that there are three principal WLAN technologies (802.11b, 802.11a and 802.11g) standards. In addition, there is a newer standard, IEEE 802.11n, which has recently been approved and published by IEEE. IEEE 802.11n-2009 is an amendment to the IEEE 802.11-2007 wireless networking standard to improve network throughput over previous standards, such as 802.11b and 802.11g, with a significant increase in the maximum raw OSI physical layer (PHY) data rate from 54 Mbit/s to a maximum of 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz.

In the past few years, the staff at the OUHK have conducted a number of WiFi surveys in Hong Kong (Tsang, White, Fox and Kwok 2009). The 2009 WiFi survey conducted by the OUHK and Caritas Institute of Higher Education (CIHE) was held during the Guinness World Records Week (9–12 Nov 2009). It was found that 20% of WiFi Access Points are using 802.11n standard. The following table shows the results of the survey.

Table 10.2 Results of 2009 Joint OUHK and CIHE Air-Land-Sea Survey

802.11 b	3.00%
802.11 g	76.70%
802.11 n	20.30%

Figure 10.5 Members and students of OUHK and CIHE who conducted the WiFi Air Survey on 12 Nov 2009.

What insights can be generated from these results from a network designer perspective?

We recommend you revisit the section on wireless network protocols in *Unit 9* if you need to refresh your memory about the details of this topic. In particular, review Table 9.5, which gives you a comparison of the common wireless networking standards, their ranges and throughputs.

Backbone strategy

The word **backbone** is often used to describe the part of the network that interconnects the other parts of the network. For example, an organization may have an FDDI ring that interconnects a number of Ethernet networks. The FDDI ring is then called the network's backbone. In addition to FDDI, thick Ethernet was commonly used as the network backbone in the past. Figure 10.6 shows an FDDI backbone connecting the LANs in each floor of a building. Here, the FDDI ring has to be built across the floors, providing an access point to each LAN.

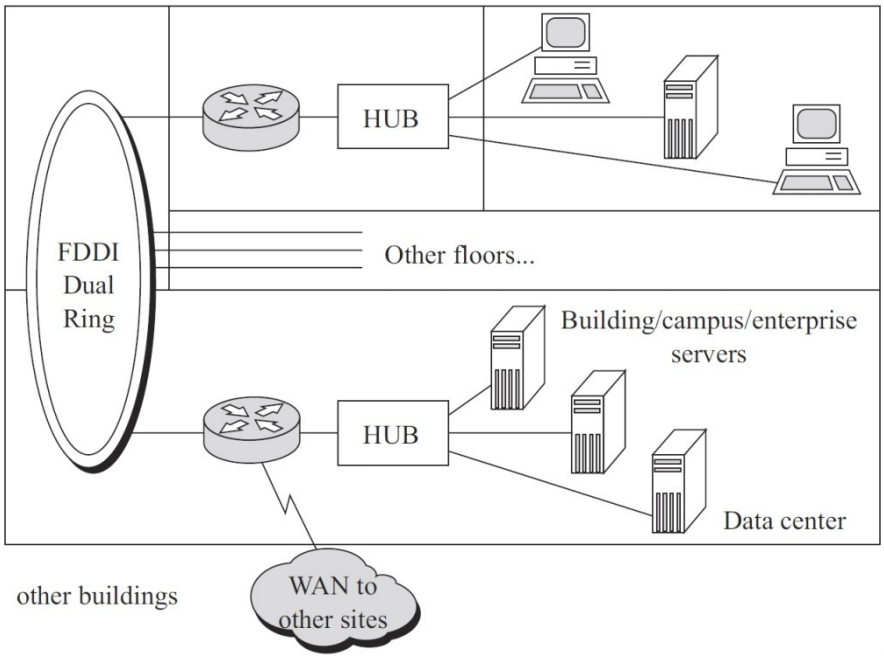


Figure 10.6 A distributed backbone in a building

Distributed versus collapsed backbones

Since the connections of the LANs are distributed throughout the backbone, this kind of backbone is referred to as a **distributed backbone**. This name is also useful in distinguishing it from a **collapsed backbone**, which provides network connections in a single central location. In reality, it is rare to build an FDDI backbone within a building because of the high cost. Figure 10.7 shows a more cost-effective design, an FDDI backbone connecting LANs in different buildings. Indeed, distributed backbones are seldom used in network implementations nowadays. Collapsed backbones are popularly used instead because of their advantages, which we will discuss later.

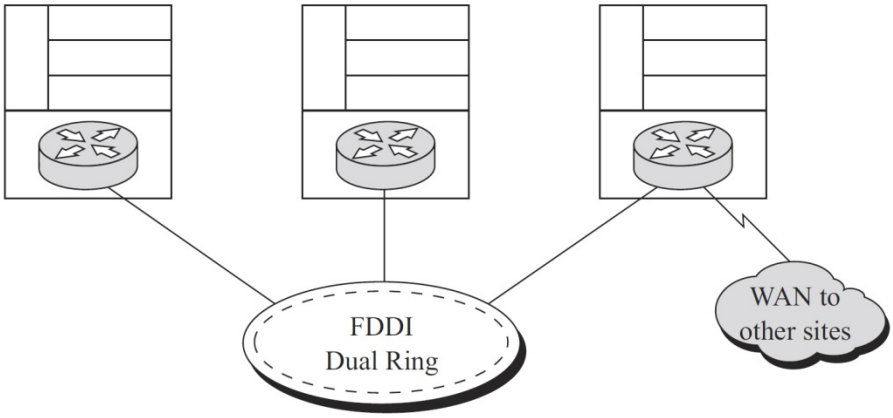


Figure 10.7 A distributed backbone in a campus

You can imagine that a collapsed backbone is a backbone being put inside a single device. Usually this device is a switch or router, which

performs the same functions as a distributed backbone that is interconnecting various parts of the network.

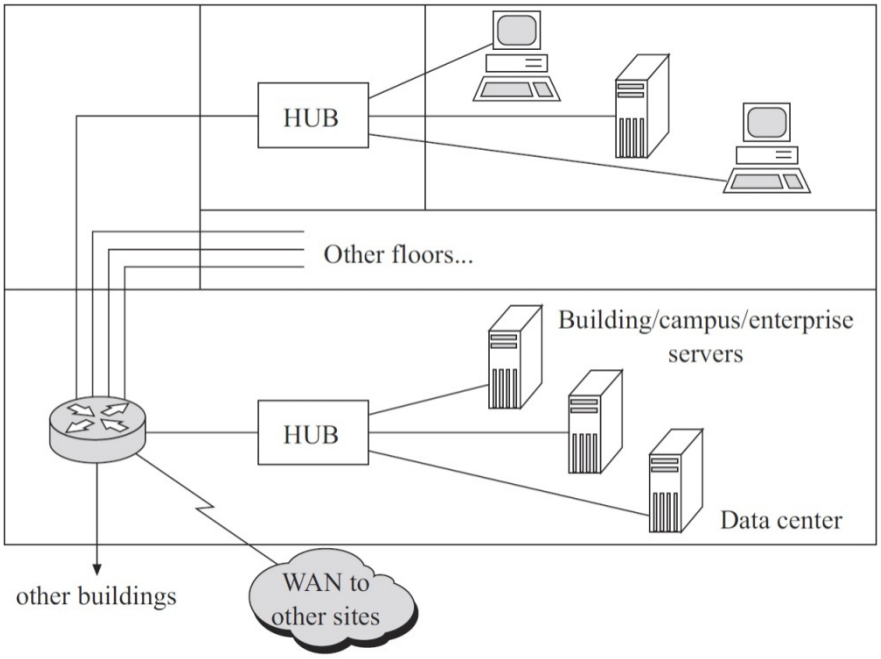


Figure 10.8 A collapsed backbone

Figure 10.8 shows the same floor plan as in Figure 10.6, but with the FDDI backbone replaced by a collapsed backbone. The LAN on each floor is connected to a separate port on the collapsed backbone. You may already be able to come up with several advantages of the collapsed backbone over the traditional distributed backbone. The following section discusses details of these advantages.

Advantages of a collapsed backbone

1 *Ease of management and maintenance* — A distributed backbone is a physical network involving cabling and connections with internetworking devices. Much effort has to be put into maintaining and monitoring each part of the network. A collapsed backbone is just a single device with ports connecting to various LANs of the corporate network. The network administrator may access the backbone remotely for monitoring the status of each connection and carry out troubleshooting procedures if problems arise. Also, the router or switch is always installed with management software for configuration and network management, which enables remote network configurations.

2 *Higher adaptability* — Backbone technology may be changed or upgraded easily. For example, some in the organization may want to upgrade to Fast Ethernet technology, as it provides higher bandwidth to the network. If its network is established with a thick Ethernet distributed backbone, adopting the new technology would mean the replacement of the old backbone, including the cabling and the internetworking devices. However, if the organization is currently

using a router as a collapsed backbone, the new technology can be adopted easily by replacing the router by a Fast Ethernet switch, and no re-cabling is needed.

3 *Higher scalability* — It is easier to add users or network segments to the network. If the collapsed backbone does not have enough ports for attaching all the LANs, an expansion module is always available for the backbone in order to cope with the expansion.

4 *Lower cost* — It is always cheaper to purchase a single device than to build a new physical network.

Backbone routing options

Nowadays, organizations commonly have LANs using different network protocols. There may be Windows and UNIX LANs running TCP/IP, Macintosh LANs running AppleTalk, Novell LANs running IPX/SPX, and others. In designing a backbone to interconnect all these LANs, you have to make a decision about the routing options for the backbone: that is, you need to choose between a multiprotocol backbone and a single protocol backbone.

A typical example of using a multiprotocol backbone is the combination of TCP/IP networks and IPX networks. The network layers for both protocols are different. In a multiprotocol backbone, the TCP/IP packets and the IPX packets can be routed throughout a common backbone without encapsulation. The environment is referred to as a multiprotocol backbone (or multiprotocol routing backbone). Encapsulation here means putting IPX packets as data frames into TCP/IP packets or vice versa. A multiprotocol backbone environment can use one of the two routing strategies, or both, depending on the routed protocol involved. Obviously, the routing speed is faster without having the encapsulation process.

In a multiprotocol backbone, you can expect to mix routers that support different combinations of multiple protocols existing in the network. A drawback of this is the creation of confusing situations, particularly for integrated routing. In general, integrated routing is easier to manage if all the routers attached to the integrated routing backbone support the same integrated routing scheme. It is a difficult task to debug the network connectivity with multiprotocols.

The design of routing can be significantly simplified for a single-protocol backbone. All routers are assumed to support a single routing protocol for a single network protocol. In this kind of routing environment, all other routing protocols are ignored. Although it is a single-protocol backbone structure, it is still allowed to support multiprotocol communication. If multiple protocols are to be passed over the network backbone, unsupported protocols must be encapsulated within the supported protocol, or they will be ignored by the routing nodes.

In simple network structures, the network services can be supported by a single network protocol. It is also recommended to develop a single

protocol backbone. However, encapsulation does add overhead to network traffic. If quite a number of network protocols are supported widely throughout a large network, a multiprotocol backbone approach is likely to work better.

A backbone is the main core of a corporate network. It is important that the backbone be stable, error-free, and has sufficient resilience to accommodate any unforeseen connectivity disruption.

Self-test 10.4

1 How does a bridge differ from a layer-2 switch?

2 How does a router differ from a routing switch?

3 Explain how collapsed backbones work.

4 What are the three technology layers important in backbone design?

A hierarchical model

Internetworking devices cannot be missed in an enterprise network design. In planning the positions of these devices in the network diagram, you have to think very carefully, as this affects the management and scalability of the network in the future. For small networks, internetworking devices may be casually assigned to interconnect network segments. All network devices perform more or less the same functions and no one device is assigned specific tasks like concentrating network traffic within a particular site. The network topology is said to be flat. An example is shown in Figure 10.9. In dealing with changes or expansions, the network structure may be varied arbitrarily to fit the immediate needs, without carefully considering the network structure as a whole in a systematic way.

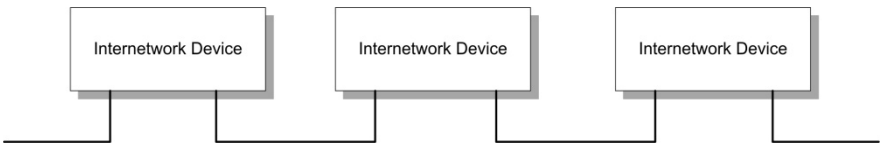


Figure 10.9 A flat model

It is obvious that we should work towards a well-organized network structure for large networks. The hierarchical model is frequently used in network designs for an enterprise network. This model arranges internetworking devices in a tree structure, as shown in Figure 10.10. Each device will be assigned specific tasks for the overall structure of the network.

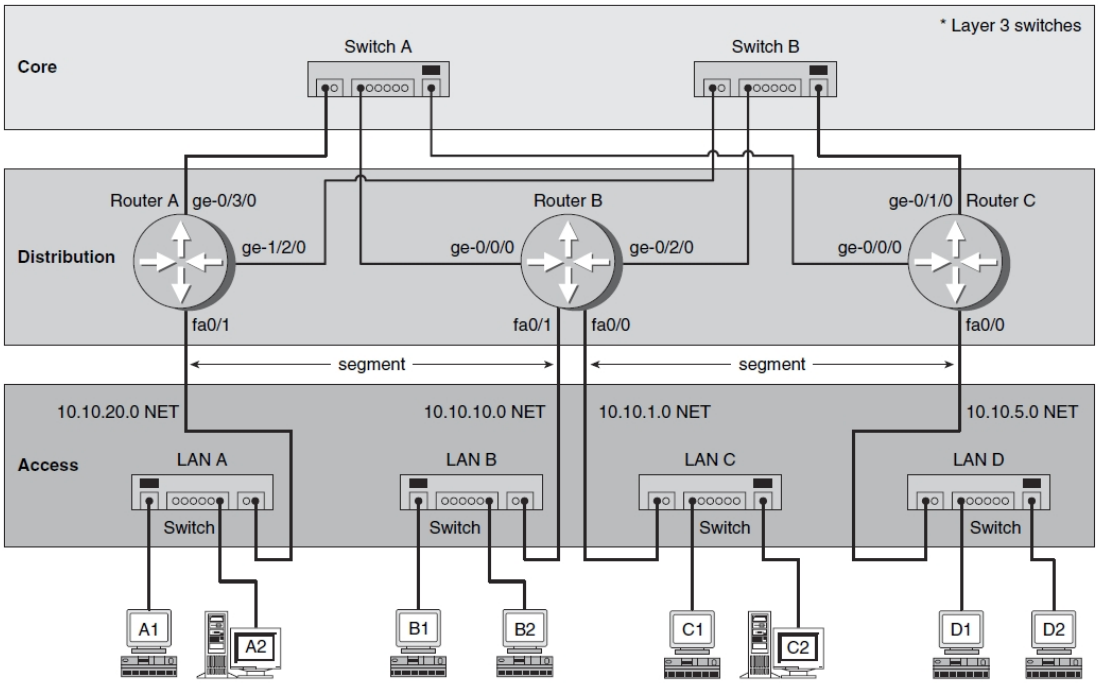


Figure 10.10 A three-layer hierarchical approach to network design

Source: Beasley 2009, Figure 9-1

Model components

A three-layer hierarchical model is generally applicable for most networks, from small office LANs to corporate networks. This layering actually focuses on the hierarchy of the routers, as it is the main device for connecting the networks. The layers include:

- core;
- distribution; and
- access.

Figure 10.10 above clearly shows three layers of routers connecting to form a hierarchical network. The functionality of each layer is explained as follows:

- *Core layer* — This layer provides the connections between remote sites and acts as the gateway between the internal and external networks. Core links are usually WAN connections, such as frame relay and ATM, which are typically rented from telecommunication companies. There are rarely any hosts directly connected to the routers in this layer. Since the main gateway is implemented in this layer, it is usual to install a firewall system, which you learned about in *Unit 8*. The firewall system is to protect the internal network from being hacked or cracked externally.

- *Distribution layer* — As the name implies, this layer is to distribute the network services to multiple LANs within a corporate network. This layer includes the network backbone of a branch and all its

connecting routers. Taking the OUHK as an example, the distribution layer may include the routers connecting different schools (Science and Technology, Business and Administration and so on) to the campus backbone. Each school may have its own backbone in the building for connecting to the distribution layer, or the hosts can be connected to the distribution layer directly.

- *Access layer* — The access layer is usually a LAN or a group of LANs, typically Ethernet and wireless LANs, that link up all users or servers to the network. Most hosts connect to the network at this layer. Grouping users based on organizational or functional units such as the faculties of a university can be done in this layer through network segmentation, either physically or logically through VLANs.

Not all environments require the building of a three-layer model. However, you have to keep in mind that a hierarchical structure should be maintained to allow scalability of the network infrastructure.

Variations of the model

In many small networks, a one-layer design may be sufficient. Figure 10.11 below and Figure 10.12 show two one-layer designs in which you may only find one layer of routers. In these simple structures, you have to consider another important design issue: the placement of servers. The servers may be distributed across several LANs, as shown in Figure 10.11, or centralized in a single site as shown in Figure 10.12. For distributing the servers, the server services will have a higher fault tolerance. There will also be a lower bandwidth requirement for the links connecting the sites. However, it is more difficult to manage the servers, and duplicated work may be done at each site.

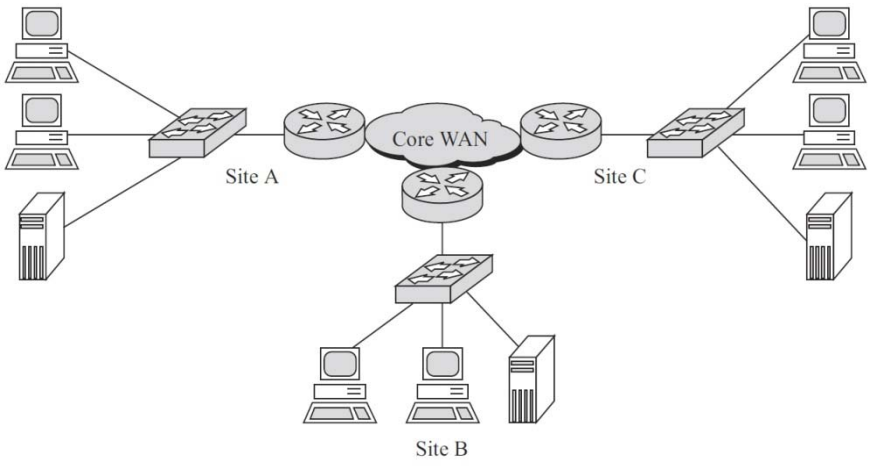


Figure 10.11 One-layer design option — distributed

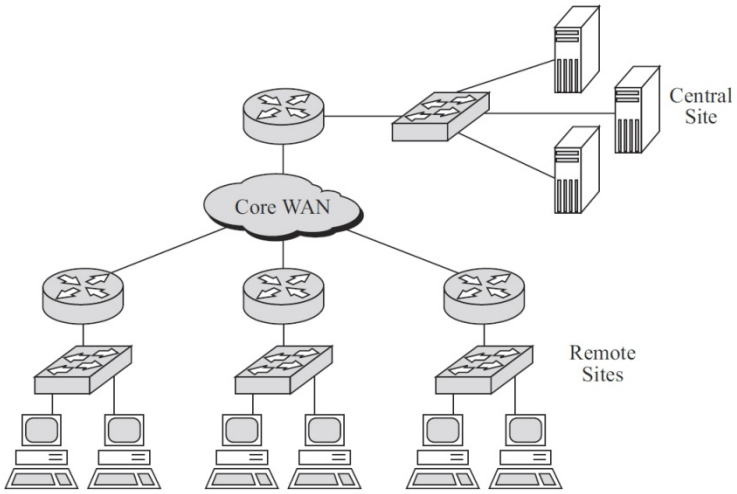


Figure 10.12 One-layer design option — centralized

The design in Figure 10.12 is usually used for higher management control. However, high bandwidth links and redundant paths are needed to protect the network from bandwidth shortage and single point of failure respectively.

Figure 10.13 shows a two-layer design in which a campus backbone is used to connect LANs in different buildings. In each building, there may be single or multiple LANs connected with bridges or switches. You may also set up VLANs to put users into logical groups without physically putting them into different network segments.

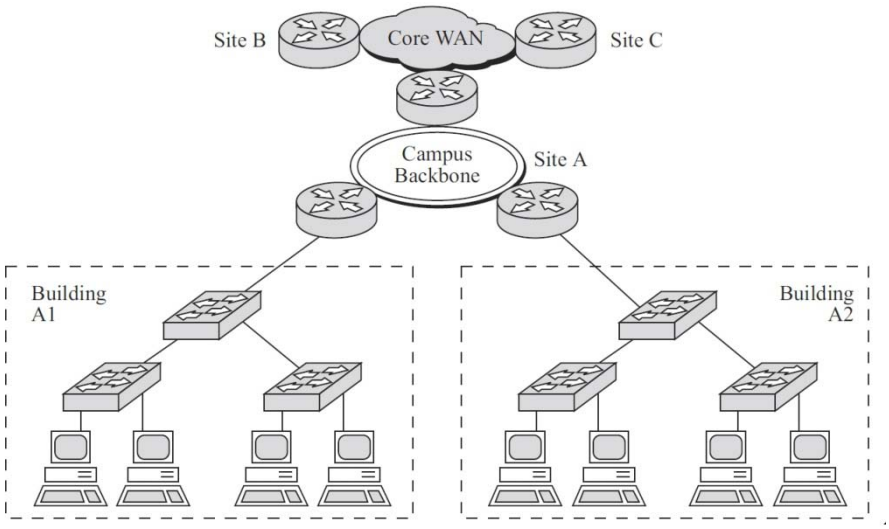


Figure 10.13 Two-layer design

Benefits of a hierarchical model

In general, the hierarchical model is recommended, since its benefits are:

- *Ease of development and management* — The hierarchical model divides the network into layers. The functionality of each layer can

be clearly defined. This is very useful for isolating problems in the network.

- *Scalability* — A hierarchical network can expand much more without sacrificing manageability, because of clearly defined functions in each layer and ease in isolating potential problems. The Public Switched Telephone Network (PSTN) is a good example of scalability.
- *Performance* — Nodes that operate in the hierarchical model are able to maintain close to wire speed transmissions to all of the nodes it supports.
- *Security* — Access control security is provided at the access layer. The distribution layer can support advanced security that meets the security needs of the LAN.
- *Predictability* — Since we can easily partition the hierarchical model into separate networks, modelling the behavior of the network is much more predictable.
- *Protocol support* — The interoperability of the current and new applications and protocols can be enhanced more easily. The reason is that you can easily isolate the traffic of a particular application or protocol in an area by setting up routing policies in the access or distribution layer.

Case study 10.2

Acme Accountants Ltd.

Background

Acme Accountants Limited currently has ten sites throughout Hong Kong. Each site has the same layout. There is a building with ten floors. Staff in each site use PCs primarily for word processing, database access and email. The database is primarily text. TCP/IP is used as the network protocol. The addresses are manually administered. They are currently using an arbitrary addressing scheme. They do not connect to the Internet.

Current network

Each floor has about 50 to 80 PCs and eight to ten servers that are connected by Ethernet networks. The servers on the floor are accessed only by users on that floor. There are also ten servers in the basement that are accessed by all users in the building. Each floor is installed with 10BaseT cables for the Ethernet. Each floor is then daisy chain-bridged to each adjacent floor and eventually to the basement. In each building is a single flat network. Broadcasts from any node will be propagated throughout the building.

The individual sites are not currently connected to each other. Any communication that must occur between sites is done by non-electronic methods like telephone (voice), conventional mail, or overnight express service.

Currently, each PC generates about 100kbps of traffic. Most of the traffic, about 90%, is for the local servers. Ten per cent is for a shared server in the basement. Figure 10.14 shows the block diagram of the current network.

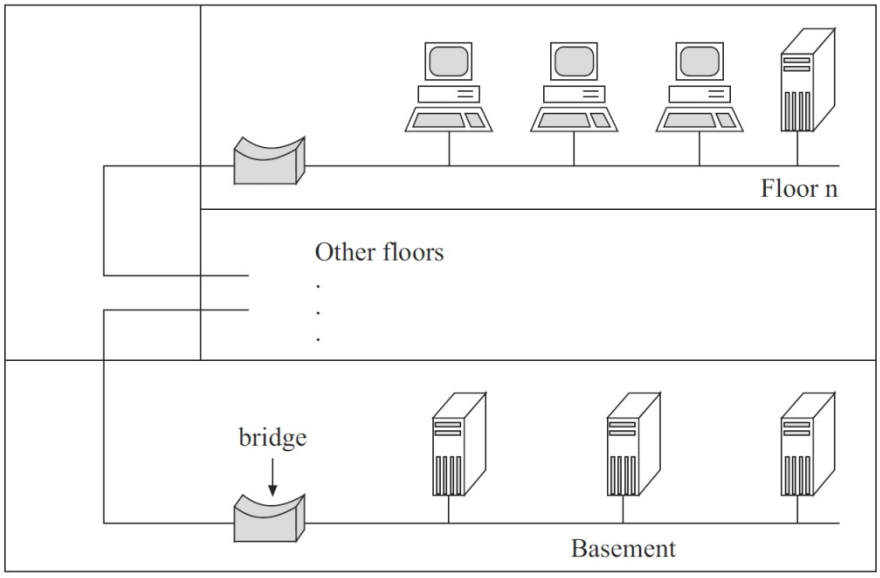


Figure 10.14 Original design of Acme's network

New network requirements

Acme Accountants Limited is experiencing extensive growth. They anticipate that there will be up to 200 user PCs and 20 servers per floor. They are also in the process of doing application upgrades. These new packages will do much more graphical presentation of data. They are finding that the addition of more users and newer applications is resulting in sever access performance problems in their network. They also see a need to interconnect the major sites, anticipating that one percent of the traffic from each building will go to some other building. It is anticipated that future company growth will result in more sites being added, up to a maximum of 30. Each site will have the same end-user requirements.

The new design must provide the following:

- an interconnection method within the building that is highly scalable;
- logical isolation between workgroups (floors) for administrative control;
- a dedicated recommendation for IP addressing of the network with possibility of future connection to the Internet; and

- alternatives for the Internet connection.

Details regarding the method of interconnecting sites (i.e. WAN connections) are not required. Any protocols recommended must be open (non-proprietary) standards that are readily available from multiple vendors.

Outline a design option to meet the network requirements.

Network technologies

You learned about LAN technologies such as Ethernet and Token Ring in *Unit 2*. With reference to the hierarchical model, these technologies can be applied to the access and distribution layers, but not to the core layer. The reason is that the remote site connection in the core layer may be across cities or even countries, which involves a distance far exceeding the distance limits of these technologies. In this section, we introduce you to various WAN technologies that are commonly used in connecting LANs in remote sites.

Dedicated lines

A dedicated line (also referred to as a leased line), once set up, 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 telephone company. The cost depends on the distance and bandwidth of the line, but it is usually expensive. Commonly used dedicated lines used in Hong Kong (and North America and parts of Asia) are shown in Table 10.3.

Table 10.3 Common dedicated line services

T carrier circuit	Speed (Mbps)
T-1	1.544
T-2	6.312
T-3	44.376
T-4	274.176

In the past, for many companies, the bandwidth of 1.544 Mbps provided by a T-1 circuit was too large for remote site connections. A fractional T-1 circuit might fit their needs better. A T-1 circuit could be divided into 24 separate 64 Kbps channels. At a much lower cost than T-1, a fractional T-1 circuit could provide a bandwidth of 64 Kbps, 128 Kbps etc. (with an increment of 64 Kbps), depending on your needs.

In recent years, however, dedicated T carrier lines have been largely superseded by dedicated broadband Internet access technologies such as cable modem and digital subscriber line (DSL), both of which offer higher bandwidth at a much lower cost. We will discuss broadband Internet access technologies in a later section.

In connecting several remote sites 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 10.15 shows three dedicated lines for three remote sites connecting directly to each other. The figure actually shows a full mesh topology; that is, each remote site has a direct connection to the others.

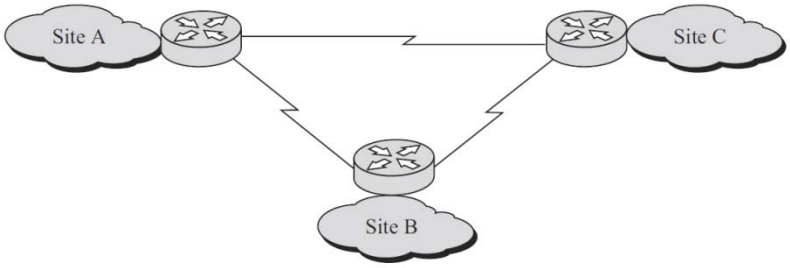


Figure 10.15 Dedicated line connections

In network design, a partial mesh topology is usually used instead of a full mesh. Referring to Figure 10.15, if there is no direct connection between sites B and C, network nodes in these two sites can still communicate through site A. Not every pair of remote sites requires a direct connection. For partial mesh, all sites are connected either directly or indirectly. Then you may wonder how you determine which pair of sites should have a direct connection. The answer is: It all depends on the network traffic. If the traffic between two sites is high, a direct link can give better support for their communications. If the traffic between two sites is low, an indirect link via a third site may be sufficient. Also, redundant paths may be built to ensure fault tolerance in the WAN connections. Figure 10.16 shows a partial mesh redundant connection among four sites.

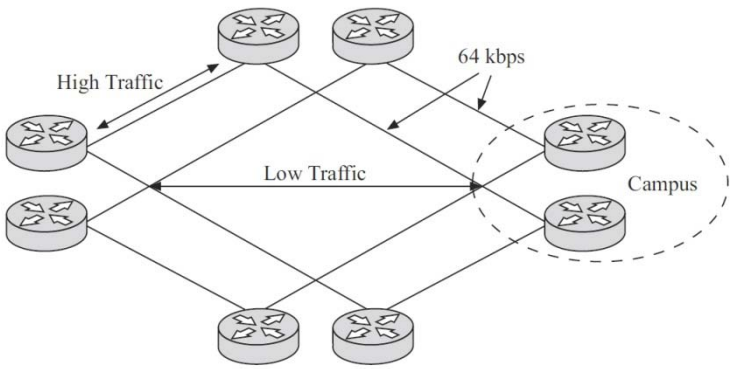


Figure 10.16 Partial mesh redundant connections

If the above T carrier circuits cannot meet the bandwidth requirement of your network, you can obtain a higher speed communication through Synchronized Optical Network (SONET), which is an ANSI standard, implemented over optical fibers. The term Optical Carrier-N (OCN), in which N is a positive integer, is usually used to designate the line speed in SONET. Table 10.4 shows SONET line speeds.

Table 10.4 SONET line services

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-18	933.12 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-96	4.976 Gbps
OC-192	9.953 Gbps

Dial-up connections

In the past, it might not be cost-effective or possible for small offices or mobile users to establish a dedicated line for their connections to the central office. In these cases, a dial-up line would be an ideal choice. While broadband access has become almost ubiquitous in Hong Kong, dial-up connections are still in common use in less developed countries and areas.

Dialup connections use the telephone network. For connections in computer networks, modems are needed at each end of the line, as shown in Figure 10.17. The modem at the sending side converts the digital signals from the computer network to analogue signals that can be transmitted on the telephone line. The modem at the receiving side converts the analogue signals received on the telephone line back to digital signals.

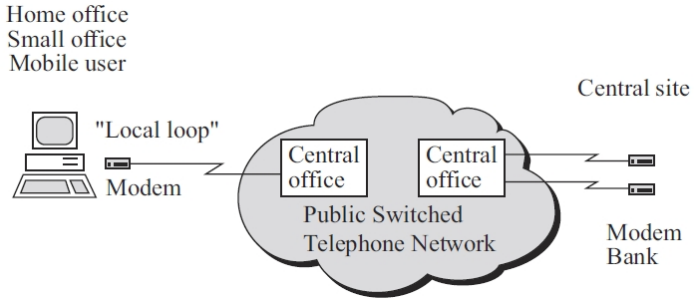


Figure 10.17 Dial-up connection overview

Dial-up lines provide the lowest speed WAN connections and the lowest cost. The fastest operating speeds for a dial-up modems is 56 kbps.

In practice, there may be more than one remote site connecting to the central site through dial-up lines. At each remote site, a stand-alone modem is used. But at the central site, a modem bank, which includes more than one modem, is needed for dealing with the simultaneous dial-up connections from these remote sites. Sometimes an access server — a device that integrates the functions of a modem bank and router — may also be used.

Dial-up connections are used primarily to connect small offices in remote sites and mobile users to the corporate network. However, very often they are also used as backup lines for high-speed connections such as dedicated lines and frame relay.

X.25

X.25 was developed in the 1970s to use the telephone network for data communications. X.25 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 an X.25 network is 64 Kbps, but it can provide a speed up to that provided by a T1 link.

We will not discuss the details of X.25 here. If you are interested in learning more about X.25, read the Wikipedia article on X.25 in the following optional reading.

Reading 10.3 (online)(optional)

Wikipedia, 'X.25':
http://en.wikipedia.org/wiki/X.25

Frame relay

Frame relay is a packet-switching network 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. 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 Mbps speed of data transfer.

Read the Wikipedia article on frame relay if you are interested in learning more about it.

Reading 10.4 (online) (optional)

Wikipedia, 'Frame relay':
http://en.wikipedia.org/wiki/Frame_relay

Broadband Internet 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 connection. 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, and higher speed uplink is not as important. Most ADSL's duplex bandwidth is devoted to the downstream direction, sending data to the user. The latest ADSL technology (as specified in ITU G.992.5 Annex M) can support downstream and upstream speeds of 24 Mbps and 3.5 Mbps respectively.

- *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. 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. It can support speeds up to around 4 Mbps (both upstream and downstream).

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 data transfer.

The data is then transported over telephone wires to the CO, no more than 18,000 feet away from the user 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 option, based on the coaxial cable wiring used for TV signals. Such cable connection requires that the customer use a special cable modem. The cable modem modulates and demodulates signals for transmission and reception via cable wiring. Such a connection could theoretically transmit as much as 36 Mbps downstream and as much as 10 Mbps upstream. Realistically, because it is shared, cable will allow approximately 3 to 10 Mbps downstream and 2 Mbps upstream. One advantage of cable is that, like DSL, it provides a dedicated or continuous connection that does not require dialing up a service provider. However, cable technology requires many subscribers to share the same line, thus raising concerns about security and actual throughput.

In summary, to determine which WAN technologies should be used, you have to consider the reliability, scalability and bandwidth required of your particular network. Of course, the cost is the most important thing in your consideration. You should first work out the bandwidth requirement in the connection of each pair of sites. Based on this information, you look for the technology to meet the requirement. For example, if the bandwidth required for the communications between two particular sites is about 1 Mbps, obviously dial-up connection can be deleted from the list of considerations. If you 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. Just remember that it is typical to use *all* available technologies to fit the particular needs of connections in different portions of your enterprise network.

Bandwidth/traffic engineering

As a network designer, your design is also guided by the bandwidth and network traffic requirements in various parts of your network. The decision about using a particular WAN technology discussed in the last section is a good example. In addition, decisions on aspects such as segmentation and grouping nodes by VLAN are affected by the bandwidth requirement of the network connections. Each node in the network places loading on the network. Nodes, like servers, may place a heavier network load, whereas workstations may place less. Thus, it is important to estimate network traffic and use the results of that traffic estimation to consider whether or not to subdivide the network by using various internetworking devices.

Among various network applications, multimedia applications place the heaviest loading on the network. There are always special considerations on the network design to cater to these applications. A simple case is given in the following example.

Example 10.1

AsiaCyber Ltd planned to deploy an application for video announcements that involves the installation of a video server in the office network. Video broadcasting of important announcements in the company will be done through this server to all workstations in the network. The director has stated that the quality of the video required does not need to be high, i.e. VCD quality is acceptable.

The office network is currently using an Ethernet switch as the backbone, and the video server will be connected to this backbone switch directly. As the network designer, you want to make a simple analysis of whether the existing network setup can support this additional loading. Through a network monitor, it is found that the average utilization rate of the network is about 50%. The following is the analysis:

Since an Ethernet switch is used as the backbone device, each workstation can receive a dedicated bandwidth of 10 Mbps.

Average utilization rate = 50%

Capacity of the network bandwidth for additional loading = $10 \times (1 - 50\%) = 5$ Mbps

Video quality video:

resolution — 320×240

color — 256 (8 bits)

frame rate — 15 frames per second

corresponding bandwidth required = $(320 \times 240 \times 8 \times 15)$
$= 9.26$ Mbps

video compression (in MPEG-1 format) = 6:1

actual bandwidth required = $9.26 \div 6 = 1.54$ Mbps

The capacity of network bandwidth for each workstation (5 Mbps) can still support this additional loading (1.54 Mbps).

Since each workstation in the network receives the same video announcement, the video server sends out the video stream in broadcast mode — one video stream for all workstations. The loading for the link of the video server to the backbone switch is also 1.54 Mbps, well below the dedicated bandwidth of 10 Mbps. From this simple analysis, you found that the existing network setup could still support the deployment of the application for video announcement.

Case study 10.3

AsiaCyber Ltd, after successfully deploying the video announcement application, now plans to use another video application on the video server. This application allows the users past video announcements on demand. During the broadcast of a video announcement, the server will disable the retrieval of past video announcements. There are 20 workstations in the network, and each one can only retrieve one past announcement at the same time.

Carry out a simple analysis, similar to the one in the above example, to evaluate whether or not the existing network setup can still support this additional loading. If not, suggest an upgrade to the network equipment to cater for such additional network loading.

Addressing issues

After working out the structure of a network, you should develop the overall addressing scheme. We discuss only the addressing issues in a TCP/IP network, as it is the protocol used in the Internet and in most private networks. The IP protocol identifies each host in the network with an IP address and uses this address to route data to them. The IP address assigned to each host must be unique.

Public and private addressing

In writing down the addressing scheme, the first decision you have to make is whether to use public or private addresses. If you use public addressing, the IP addresses should be obtained from the Internet Network Information Centre (InterNIC). Then your network can be connected to the Internet directly without address translation.

InterNIC is facing the problem of address storage in the Internet as more and more organizations and companies are joining the Internet. For a small- or medium-sized company, a class C address will probably be assigned. However, only 254 nodes can be accommodated with a class C address, but the size of your network may far exceed this number. In this case, private addressing may be used. The InterNIC has reserved some address ranges for private addressing which is specified in the RFC 1918 document. Refer to Table 3.3 in *Unit 3* for the reserved address ranges.

If your network is not going to connect to the Internet, you may use any address range you like. Just remember to keep the address of each node unique. However, if your network will be attached to the Internet, you must follow RFC 1918 in using private addressing; otherwise, there will be a problem for your network in communicating with the Internet. Can you think of what the problem will be? The following example outlines it.

Example 10.2

Your network:

- is connected to the Internet through a WAN link
- is assigned the class C address: 202.1.1.0 from InterNIC
- uses the class B address: 160.1.0.0 as the private address range
- has a proxy server installed in the network to translate the private address to public address when the nodes in the network communicate with the Internet.

Case one:

When the node 160.1.1.1 wants to communicate with a node in the Internet whose IP address is 170.100.5.10, the routers in the network know from the network ID of the destination address that the destination of the packet is outside the internal network, so they will deliver the packet to the proxy server for address translation. After translating the address 160.1.1.1 to a public address, say 202.1.1.1, the proxy server will send the packet to the Internet through the WAN link. The communication between the node 160.1.1.1 (private address) and 170.100.5.10 (public address) is then achieved.

Case two:

The node 160.1.1.1 now wants to communicate with a node in the Internet with an IP address 160.1.5.10 (public address). Since the destination address has the same network ID as the internal network, the routers treat it as a communication within the internal network, so they send the packet to the node 160.1.5.10 in the internal network. If 160.1.5.10 does not exist in the internal network, an error message will result.

From the above example, you can see the problem. If you use a private address range randomly, i.e. without following the specification in RFC 1918, that address range will no doubt already be a valid public address range in the Internet. Then your network will not be able to communicate with the network that uses this address range in the Internet.

Subnetting

As discussed in the section ‘Hierarchical model,’ the hosts in your network are usually connected in a hierarchy instead of a flat structure. In such cases, you may want to use subnet addressing to build a hierarchical addressing scheme. The addressing scheme can match the physical structure of your network and thus enable easier management and higher scalability. Each IP address is associated with a subnet mask to distinguish the network ID from host ID. A subnet mask is a 32-bit address with the bit positions corresponding to the network ID all set to

ones, and those corresponding to the host ID all set to zeros. Table 10.5 shows the default subnet mask for each class of addresses.

Table 10.5 Default subnet masks

Class	Subnet mask	
	Dotted decimal notation	**Bit pattern**
A	255.0.0.0	11111111 00000000 00000000 00000000
B	255.255.0.0	11111111 11111111 00000000 00000000
C	255.255.255.0	11111111 11111111 11111111 00000000

Subnetting involves borrowing bits from the host ID to extend the network ID. For example, you use the class A private address 10.0.0.0 for your network. With this address range, about 17 million nodes can be accommodated. Your network consists of about 200 sites throughout Hong Kong. You want to divide the address space into 256 subnets by using the subnet mask 255.255.0.0, so that each site can be assigned with one subnet. Table 10.6 summarizes the address range of each subnet.

Table 10.6 Address range for 10.0.0.0 subnets

Class	Address range
1	10.0.0.0 – 10.0.255.255
2	10.1.0.0 – 10.1.255.255
3	10.2.0.0 – 10.2.255.255
:	:
:	:
254	10.253.0.0 – 10.253.255.255
255	10.254.0.0 – 10.254.255.255
256	10.255.0.0 – 10.255.255.255

Connecting to the Internet

More and more organizations find that Internet access is important to their business. The Internet can provide them with a very fast channel for outside communications as well as an abundant information resource. They may even use the Internet as the backbone of their corporate networks.

In the following reading, the author discusses various issues related to connecting the network of an organization to the Internet. The reading includes a brief description of the business objectives of connecting to

the Internet, and outlines some technology issues. Let's preview a few of the technology issues before you proceed to the reading:

- *Network protocol* — The network protocol used in the Internet is TCP/IP. If the network of your organization is not running TCP/IP, is it possible for your network to connect to the Internet? You can find the answer in the reading.

- *Addressing* — The author has a more detailed description of this addressing issue and discusses how to get an address.

- *Connection method* — Depending on the structure of a network, the connection method to the Internet may be different from organization to organization. This also depends on the bandwidth required by your network for connecting to the Internet. As is the case with a WAN connection, you may choose between dedicated lines, dial-up lines or packet-switching connections like frame relay. You will always need an Internet Service Provider (ISP) to give you an access point to the Internet. The reading gives suggestions on how to choose a good ISP.

- *Providing Internet services for your users* — After your corporate network has access to the Internet, can your users enjoy the Internet services immediately? What services can they access? After physically connecting your network to the Internet, some configurations on your network have to be done before your users can enjoy the Internet services.

Network implementation

In addition to the network infrastructure, the network operating systems (NOSs) for both client and server machines play an important role in the network design. Under the scope of an NOS, there are also various issues concerning network design, such as the roles of the servers and the grouping of users. The level of these concerns is different from the issues discussed in the previous section. They are closer to the users, or we might say closer to the implementation level. These concerns are different for different NOSs. In *Unit 4* you studied the features of Windows Server 2003. Although Windows Server 2008 R2 has already released, we retain Windows Server 2003 as our featured example because of its large deployment base.

There are quite a few online readings in this section. Some of them are very useful in helping you understand the architecture of a Windows 2003 network. However, some of them only present the procedures for doing a particular configuration task in Windows 2003. The latter readings will be marked as optional, as they are not of great significance. You may read them for your own interest.

Planning

In planning the implementation of a Windows 2003 network, it is important to understand the concept of domains and active directory.

A domain is a logical grouping of users, servers and resources under a single centralized administration. Whereas small networks can store accounts and resources in a single domain, large organizations typically establish multiple domains. Windows 2003 active directory combines domains and stores all information about the network resources and services. This is one of the biggest changes from Windows NT to Windows 2003.

In addition to setting up the active directory, you have to make decisions about several design options, which were discussed in *Unit 4*:

1 the network protocol to be used

2 hardware requirements for the servers

3 the network services to be implemented, e.g., DNS, DHCP, HTTP, etc.

4 the administration tools to be used

5 interoperation with computers running other NOSs such as UNIX, Mac OS X, NetWare, etc.

Installation and configuration

After planning, you come to the actual installation and configuration of various parts of the network. For physical connections of the network, each network node should be equipped with a network adapter and a link to the networks. The physical grouping of the network nodes and the interconnection of the groups can be done through network devices such as hubs, bridges and routers, for example. *Unit 2* gave you detailed descriptions of these devices. For the physical structure of the network, you can follow the hierarchical model discussed earlier in this unit for systematic network implementations. In this section, we concentrate on the installations and configurations of Windows 2003 in the networking environment.

The following reading describes the basic steps in setting up a basic Windows 2008 server.

> ***Reading 10.5 (online) (optional)***
>
> Installing Windows Server 2008:
> http://technet.microsoft.com/en-us/library/cc755116(v=ws.10).aspx

In setting up a Windows 2003 server, you have to pay attention to several configuration options.

File system

Windows 2003 provides two choices of file system to be implemented: NT File System (NTFS) and File Allocation Table (FAT) File System. In addition, there are two kinds of FAT file systems: FAT16 and FAT32. FAT is a file system used in the operating system: DOS on IBM-compatible PCs, whereas NTFS is a file system introduced in Windows NT. NTFS provides better data security, so it is usually chosen in the configuration.

Server role

A Windows 2003 network has at least one domain controller and one DNS server when a server computer is installed in the domain. If you install Windows 2003 as a stand-alone server without joining a domain, you can join a domain later. If the server you are going to install is the first domain controller in the network, you can choose either to install it as a domain controller during the server installation process, or to promote the server to a domain controller after the initial installation.

User accounts

In order to give a user access the Windows 2003 network through a client computer, a user account must be assigned. This is a basic security

measure in a networking environment in which only authorized users can access the data and resources of the network. Windows 2003 provides two types of user account: domain user account and local user account. The domain user account can log on to a domain to gain access to the network resources. A local user account allows a user to log on and gain resources only to the computer in which he creates such an account. When using a local user account, you will be unable to access any of the network resources except on a peer-to-peer network.

After creating user accounts, it is necessary to create groups for grouping users. Groups help you manage a group of users effectively. For example, let's say you want to give permission only to users in the finance department of your company to read the financial data stored in the Windows 2003 server. If there are 100 users in the finance department, you have to make the permission assignment 100 times, once for each of the users. To perform this task more effectively, you may create a group called 'Finance' and put each user account of the Finance Department in this group at the time it is created. You can then assign the Finance group the permission to access the financial data in the network.

Client computers

After studying the concepts of user accounts and groups, you can proceed to setting up client machines. Windows 2000, Windows XP, Windows Vista and Windows 7 client computers are supported in the Windows 2003 network.

Connectivity

For small networks, it may be better to set up a peer-to-peer network, rather than a client/server one. The most important point is that no effort has to be made in the centralized administration for a small network. Central administration is very costly for a network containing only a few machines.

In Windows 2003, a peer-to-peer network can be set up through the workgroup configuration. A workgroup is a logical grouping of computers, a concept similar to domain, but with no central administration of the group implied. In actual configurations, all Windows 2003 servers are set up to be member servers. In addition to Windows 2003 servers, Windows 2000 servers, NT servers, NT workstations, Windows XP, Windows 2000 professional and Windows 98 can be members of the workgroup. In a workgroup, resources are shared among all the machines. That means each machine can be both a server and a client.

If your network contains tens of computers or even more, then you should seriously consider setting up a domain. In larger companies and organizations, more than one domain may be required. If more than one domain is set up in your network, you have to establish appropriate trust relationships between the domains in order to effectively manage the

users and resources. As organizations have grown, domain design requirements have become more complex. The system of manual trusts has grown rather cumbersome, particularly for organizations that have dozens or hundreds of domains. To address these issues, Windows 2003 has introduced the concepts of forests and trees — both of which are collections of domains. A tree is the population of domains that share a contiguous name space.

Reading 10.6 (online) (optional)

Active Directory Domain Services:
http://technet.microsoft.com/en-us/library/cc268216.aspx

Monitoring and optimization

Windows 2003 provides several tools to monitor and optimize its performance. Monitoring the server is a crucial part of server administration. By using appropriate monitoring tools, you can detect server problems, evaluate the result of changes to your website content, and plan upgrades to make your sites more accessible to users.

The best choice of monitoring tool and method depends on the information you need. For example, if you are trying to measure the overall load on your Web server, you can use System Monitor to render a week-long plot, showing information such as the number of computer connections and file transfers. As another example, if you notice a slowdown in your server's performance, you can check for errors in Event Viewer, the tool for viewing logs generated by Windows 2003.

In addition to the tools built into Windows 2003, you can use other performance monitoring tools. The following monitoring tools, available in Windows 2003, can provide both moment-to-moment and summary information:

- System Monitor

  System Monitor is a powerful tool that you can use to monitor your server's activity and summarize its performance at selected intervals. With this tool, you can display performance data in real-time charts or reports, collect data in files, and generate alerts that warn you when critical events occur.

- Event Viewer

  Windows 2003 includes an event-logging service, which records events such as errors or the successful starting of a service. These event logs are viewed by using Event Viewer. You can use Event Viewer to monitor System, Security, and Application event logs. With this information, you can better understand the sequence and types of event that led up to a particular performance problem.

- Task Manager

  Task Manager can be used to view ongoing tasks and threads. It can also be used to change the assigned priority of processes. However, once the process has completed, the new priority setting is lost. CPU and memory usage can be seen in real time, but information is not saved over time.

- Network Monitor

  Network Monitor captures information on traffic to and from a computer and gives detailed information about the frames being sent and received. This tool can help you analyse complex patterns of network traffic. By using it, you can view the header information included in HTTP and FTP requests to your server. Generally, you need to design a capture filter, which functions like a database query and singles out a subset of the frames being transmitted. You can also use a capture trigger that responds to events on your network by initiating an action, such as starting an executable file.

Activity 10.1

Work through Lab 5.1 — *SOHO LAN Design (Wired)* in the 'Lab Book' (Kwan et al. 2009).

Self-test 10.5

1 What is the Active Directory?

2 You notice that a new server is not performing as well as you expected. You need to obtain summary information on a server's performance, and you then want to use a utility to obtain detailed reports of performance bottlenecks. After you have resolved the performance problem, what should you do to track the performance of the server as more users begin to access the server?

Network maintenance and troubleshooting

Even after setting up a network, your job has not ended. You need to perform network maintenance tasks. The primary objectives for network maintenance are to:

- keep the network running smoothly and effectively; and
- look for potential problems and prevent them from happening.

To meet these objectives, you should have a good understanding of network management and monitoring. However, some planning of the following aspects may also help you a lot in doing the tasks.

Backups

A reliable backup system should be planned. This should also be included in the initial design of your network. It may impose duplicate costs on the network, but your organization may lose more in any case of data loss that occurs.

Standardization

It is important to keep everything on the network, including hardware and software components, operation procedures, configurations and file formats as uniform as possible. This makes network management, upgrading and troubleshooting much easier.

Documentation

Documentation is extremely important for network maintenance and troubleshooting. It should include:

- a map of the whole network that includes the details of the hardware components, addressing, cabling;
- server information, including the applications run and the data stored on each server and their backup plans; and
- a record of all past problems, including descriptions, solutions, dates and procedures.

Network management

Most network management systems use the architecture shown in Figure 10.18.

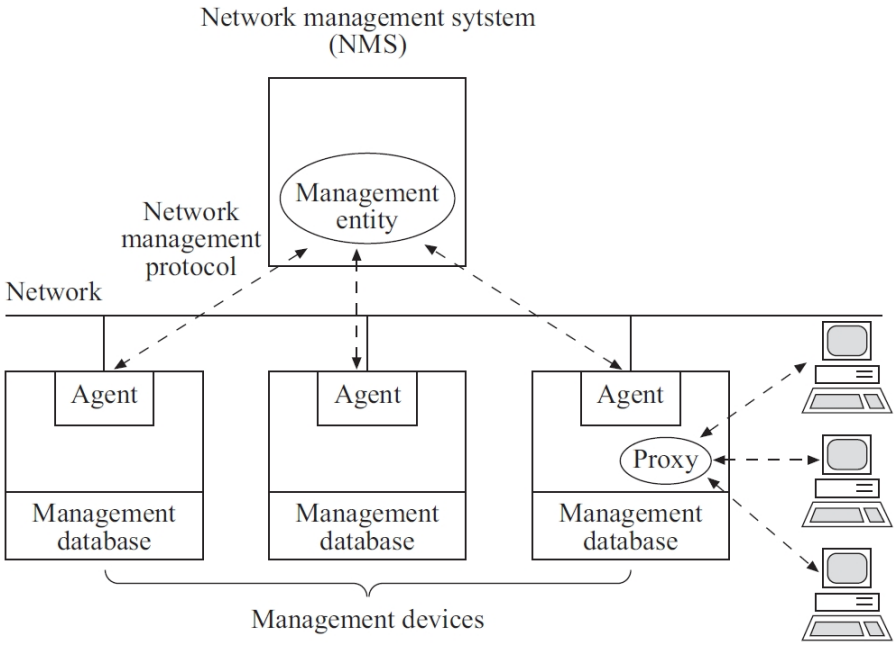


Figure 10.18 A network management system

The system consists of two parts: the management entity and the management agents. A management agent is installed on each managed device, which may be a computer or a network device such as a hub and router. The management agents monitor network traffic and behavior on the managed device and gather statistics. The data are stored in its management database. The management entity regularly sends requests to the agents, or does so upon user initiation. The agents respond to the request by providing the information in the management database to the management entity. This request-reply action is defined within a network management protocol. Management proxies are entities that provide management information on behalf of other entities. **Simple Network Management Protocol** (**SNMP**) is a very popular network management protocol.

The management agents may send alerts to the management entity when the information collected exceeds the threshold set by the network administrator. The management entities will then log the event and notify the administrator.

Monitoring performance

To determine whether or not your network performs properly, you have to know what healthy performance is. You therefore need to establish a baseline for your network. This baseline must be established by sampling on the network over a period, and before anything goes wrong. Once a baseline exists, the data gathered from ongoing monitoring of the network can be compared to it. From this, you can identify any part of the network declining in performance.

Network monitoring also helps you detect bottlenecks in the network. Network activities usually involve more than one device. Each device takes some time to perform the part of an activity it is responsible for. If

a device takes more time than it should to perform its tasks, it may be a performance bottleneck. Enhancing its performance will improve the performance of the whole activity. The possible reasons for a device to become a bottleneck include:

- It is not properly configured.
- A problem occurs in it.
- It is overloaded.

You can also study trends in different areas of your network through continuous monitoring. This helps you in future design work and to maintain an acceptable level of performance.

Self-test 10.6

1 Glendale College is planning to add a new client/server system (with new hardware), so that all 200 department chairs and administrative assistants can view the status of their budgets. How would you plan for the resulting effect on the network?

2 Describe four baseline statistics you would obtain as manager of a network. Why would this be valuable information?

Network troubleshooting

Though you may manage your network well, problems will still occur. You then have to start troubleshooting and recover the network as soon as possible to avoid interruptions to your users. It is more efficient to use a systematic approach than to try random solutions.

Troubleshooting depends a lot on experience. No doubt you have more confidence in solving a problem you have met before. Keeping records of the problems is important for long-term troubleshooting tasks. This section introduces some commonly-used troubleshooting tools. Procedures for troubleshooting common network problems such as cabling, network cards, Ethernet and Token Ring are discussed.

A systematic troubleshooting approach is particular to a company, so you will need to work out your own set of procedures. The following presents a sample of the issues that these procedures should address.

Gathering information

You have to be clear about the symptoms of a problem to identify its possible causes. You can gather information by questioning the users and by using statistics from monitoring tools. You should also scan the

network to look for obvious causes. A closer look at some network components may also be helpful in isolating the causes. You should check the history of the network to see whether the same or a similar problem has occurred and whether there is an existing solution.

Listing possibilities

After gathering all the information, you should be able to narrow the scope of interest to the parts of the network that are relevant to the problem. You can then work out a list of possible causes and sort them in order, putting the one that has the highest possibility at the top.

Isolating the problem

Based on your list of possible causes, you should work out an action plan to isolate the problem. You might simply test the most likely candidate on the list to see if that is the cause. If not, test the next one on the list. The best plan is to test only one variable at a time. This helps you find a given solution to a specific problem. If you change more than one variable at the same time, you may solve the problem, but identifying the specific change that eliminated the symptom becomes more difficult.

Studying the results

In this step you should determine whether or not your problem has been solved. If your test solves the problem, you have found a solution for future use. If your tests did not isolate the problem, you may need to adjust your action plan based on the test results and implement the plan again. If this does not work either, you may consider going back to the information-gathering stage or seek outside help.

The following reading from your textbook describes in more detail another example of troubleshooting steps. You should read it to gain a more thorough understanding of systematic troubleshooting steps.

> ***Reading***
>
> Dean (2012) 596–617.

Network troubleshooting tools

Several tools that are commonly used in network troubleshooting are outlined in the following subsections.

Time-Domain Reflectometers (TDRs) and Optical Time-Domain Reflectometers (OTDRs)

A TDR can quickly locate open and short circuits, sharp bends and imperfections in twisted pair and coaxial cables. It sends a signal along the cable. The defects on the cable reflect the signal to the TDR, at different amplitudes, depending on the problem. The TDR calculates the distance to a defect by measuring the time the signal travels. TDRs are commonly used in network troubleshooting as well as in network installation. OTDR is used to locate breaks, measure the attenuation and splice or connector losses in optical fibers.

Cable testers (scanners)

If you suspect the cables are causing a network problem, you can check them with a cable tester. In addition to physical connectivity, a cable tester can test and report on cable conditions such as near-end crosstalk (NEXT), attenuation and noise. A cable tester also performs the functions of a TDR. They are available for twisted pair and coaxial cables. Similar testing equipment is available for optical fibers.

Network monitors

Network monitors track packets crossing a network. They gather information about packet sizes and types, error packets, overall use and other information. But they do not decode the packet. The information gathered is useful for creating profiles for network traffic, planning for network expansion, detecting intruders, establishing a baseline and distributing traffic more efficiently.

Protocol analysers

A **protocol analyser** helps you in network traffic analysis by capturing and decoding the data frames. (Traffic analysis tracks and reports circuit use in relation to circuit capacity. Traffic analysis is essential for building and modifying networks in the most productive and cost-effective way. High traffic circuits can be upgraded and little used circuits can be cut back as part of this approach.) A protocol analyser presents the protocol layers information recorded in a frame in a readable format. This gives you information for analysing network behavior such as network bottlenecks, faulty network components and protocol problems, for example.

Tools and utilities in Windows Server operating systems

Windows 2000/2003/2008 provides a large collection of networking client tools to optimize and troubleshoot network performance. Several of the most useful tools are described in Table 10.7.

Table 10.7 Networking troubleshooting tools

Tool	Overview
Network Diagnostics (Netdiag.exe)	Helps isolate networking and connectivity problems by performing a series of tests to determine the state of your network client and whether it is functional.
IP Configuration (Ipconfig.exe)	Displays the current configuration of the installed IP stack on a networked computer using TCP/IP.
NetBT Statistics (Nbtstat.exe)	Displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP (NetBT), including NetBIOS name resolution to IP addresses.
Path Ping (Pathping.exe)	A route tracing tool that sends packets to each router and then computes results based on the packets returned from each hop.
IP Security Monitor (Ipsecmon.exe)	Confirms whether your secured communications are successful by displaying the active security associations on local or remote computers.

The following reading from your textbook describes common networking troubleshooting tools in more detail.

Reading

Dean (2012) 617–29.

Activity 10.2

Work through Lab 1.5 — *Network Traffic Analysis and Wireless Network Security* in the 'Lab Book' (Kwan et al. 2009).

Activity 10.3

In addition to Wireshark, there are a lot of protocol analysers available. Search the Internet to find some other open source and commercial alternatives. What are their strengths and weaknesses when compared to Wireshark?

Self-test 10.7

1 What is a TDR? How does it work? What is the difference between a TDR and an OTDR?

2 Why is it important to ensure that every node on a TCP/IP network has a unique IP address?

3 Let's say you are hired to audit an Ethernet network for a company located in a four-storey building because they are experiencing network communication problems. The network is entirely coax-based. As you examine the network, you find some sections of cable that have 54-ohm impedance. Describe why this might be a problem.

Introduction to network marketing

Nowadays information technology and communication professionals need more than just technical competence. They also need to have marketing sense. This kind of knowledge is needed not just for marketing oneself, as in the context of resume writing and interviews, but also for marketing any network product (such as network games) or service (such as online games, education, business conferences, etc.) designed or developed.

The first thing to consider is the marketability of the products and services designed. Marketability is, in fact, among the key criteria for judging most IT innovation competitions, such as the IT Awards organized by the HK Computer Society, and the Mobile Multimedia Design Competition organized by the HK Institution of Engineers.

The age-old law of marketing states that if you want to sell something, then potential clients must be aware of it first. This is certainly true of products and services related to the Internet / World Wide Web.

The president of MIT, for example, has advised MIT students to take serious courses in business and marketing as well as in their technical specialties. This is because he doesn't want MIT graduates to all end up working for Harvard's MBA graduates! This captures the essence of why technically-oriented students like those of you in *ELEC S212* also need to be equipped with marketing knowledge. In particular, you need to be familiar with the IT tools and resources used for marketing in the information age.

Given the increasing globalization of the market, it is important to make sure your designs are aimed at a global market.

A framework for network marketing

Successful network marketing isn't a simple matter. Designing a good network product or service is, of course, the crucial first step, but if no one knows about this product, or if there is no need in the market for such a product, you won't sell many.

To get you to start thinking beyond the technological aspects of network product/service design, this topic introduces you to a broader framework for network marketing.

In a typical network marketing framework, there are three important components:

1 network infrastructure and technology

2 network economics

3 marketing.

This is illustrated in Figure 10.19.

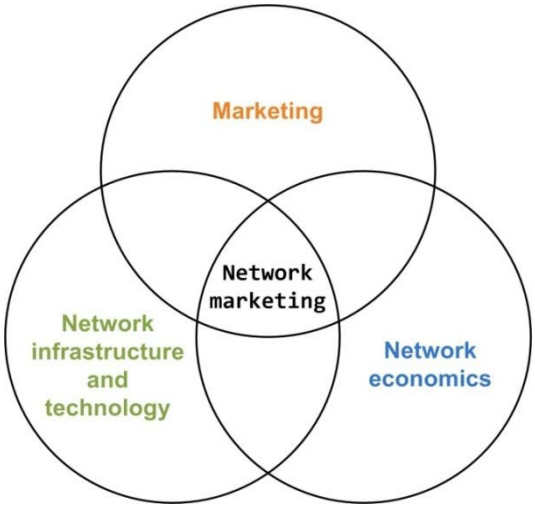


Figure 10.19 Framework of network marketing

Network infrastructure and technology

Since the previous nine units of this course have addressed the infrastructure and technology aspects of this framework, we will not spend much time on them now. Just recall that a typical network infrastructure consists of the following:

1 Type of computer network:
   - LAN;
   - MAN; or
   - WAN.

2 Type of network operating system:
   - peer-to-peer; or
   - client and server.

3 Network topology:
   - ring;
   - bus; or
   - tree.

4 Transmission media:
   - coaxial cable;
   - twisted pair cable; or
   - optical fibre.

5 Network transmission technology:
   - baseband or broadband

- Ethernet, Token Ring, FDDI or wireless.

6 Network architecture:

- OSI; or
- TCP/IP.

7 Network communications protocols:

- TCP/IP;
- IPX/SPX;
- NetBIOS and NetBEUI; or
- AppleTalk, etc.

8 Network devices:

- repeaters
- Bridges
- routers
- gateways
- hubs
- modems
- antennas, etc.

We have already covered both the physical network design and network applications designs and their associated issues in the previous units. For example, we covered the designs for setting up LANs, servers and wireless networks, as well as designs for network games and network services such as online conferencing.

Let's therefore go on to consider some of the broader economic factors that affect network marketing.

Network economics

There are four relevant concepts/laws related to network economics: **Moore's Law**, **Metcalfe's Law**, **the Law of Disruption** and the Law of Diminishing Firms. These four concepts are typically elaborated as follows.

Moore's Law:

> The law is named for Intel co-founder Gordon E. Moore, who introduced it in a 1965 paper.… It describes a long-term trend in the history of computing hardware, in which the number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every two years. Rather than being a naturally-occurring law that cannot be controlled, however, Moore's Law is effectively a business practice in which the advancement of transistor counts occurs at a fixed rate.… Moore's Law has since been used in

> the semiconductor industry to guide long term planning and to set targets for research and development.
> (Wikipedia, 'Moore's Law')

Metcalfe's Law:

> The law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). First formulated in this form by George Gilder in 1993, and attributed to Robert Metcalfe in regard to Ethernet, Metcalfe's law was originally presented, circa 1980, not in terms of users, but rather of 'compatibly communicating devices' (for example, fax machines).… Metcalfe's law characterizes many of the network effects of communication technologies and networks such as the Internet, social networking, and the World Wide Web. It is related to the fact that the number of unique connections in a network of a number of nodes (n) can be expressed mathematically as the triangular number $n(n - 1) / 2$, which is proportional to n^2 asymptotically.
> (Wikipedia, 'Metcalfe's Law')

These laws are not just abstractions; they have effects in the real world. The next law, the Law of Disruption, is based on the cumulative effects of Moore's Law and Metcalfe's Law.

The Law of Disruption:

> The law refers to the way in which innovative technologies disrupt the social order or status quo. It first appeared in the book *Unleashing the Killer App: Digital Strategies for Market Dominance* by Larry Downes and Chunka Mui. According to the authors, societal change is incremental (linear) while technological change is exponential. This disparity often leads to physical capabilities that far exceed the capacity societal norms can handle. For instance, technology such as trains or boats may bring a wave of immigrants to a country that is not yet comfortable with foreign cultures. Since attitudes of a population take time to evolve — through death, rebirth and adoption of new beliefs — while superior technology often proliferates rapidly, in this example the xenophobia would exist much longer than the antiquated means of transportation.
> (Wikipedia, 'Law of disruption')

Finally, the **Law of Diminishing Firms** carries the implications even further:

> Even before the digital revolution, technology played a central role in the development of firms. The enabling role of communications technologies like the telegraph and telephone reduced the cost of maintaining a large-scale organization across wide distances and thus made possible the creation of larger firms. Up until now, the role played by digital technology has been consistent with that history. Computers, networks, and large-scale data storage capabilities have made it possible for bigger and more complicated firms to emerge,

casting their shadow over a wider range of activities in an increasingly global market.

Think of the global financial markets and their dependence on such technology. They couldn't exist without technology, and they didn't. Large-scale industrial companies are also in some sense creations of digital technology.

So it is ironic that the long-standing servant of such firms has now become their worst nightmare. Just as technology reduces the costs of operating a firm, it reduces the costs of the market itself. It's not only firms that get more efficient, in other words; the market is also getting more efficient. Moore's Law (that the cost of a unit of computing power falls 50% every 18 months) and Metcalfe's Law (that the value of a network increases exponentially as people join it) are working to create a new marketplace. Transaction costs in this marketplace are reduced not incrementally (as they are in today's firms with reengineering and similar cost-cutting activities) but exponentially.

The resulting economic disruption is twofold:

1 Transaction costs are falling, in many cases dramatically, for nearly all goods and services.

2 They are doing so much faster in the open market than they are for firms.

Think of the Internet not as a network of connected computers but as the test bed for a new market economy, one that is global, continuously operating, and increasingly automating the processes of buying, selling, producing, and distributing. To return to the paper clip example, instead of leaving the building, you can now simply point yourself to Office Depot's website, click on the product you want, give them your credit card number, and get the paper clips the next day via UPS. Soon, that process will be enhanced by intelligent software agents, such as those being developed by start-up software companies like Firefly, which use sophisticated pattern-matching algorithms to make recommendations based on your past behavior and the behavior of other shoppers in their growing databases.

The concept of a firm as a physical entity, defined by its permanent employees and fixed assets, is giving way to what some have called a virtual organization, where employees may be part-time or contract workers, where assets may be jointly owned by many organizations, and where the separation between what is inside and what is outside the firm becomes increasingly hazy. Individuals will be participants in many enterprises, like today's entrepreneurs, and those enterprises will be formed around events much closer to transactions than to a sense of corporate immortality.
(Downes and Mui)

The point of drawing your attention to all these laws is threefold. First, due to advances in information and communications technology, small organizations can now be as powerful as big traditional organizations. Second, the number of small economic entities, down to the level of individuals, is increasing. Finally, globalization is happening, which means we must keep the global market in mind when designing products (such as online games) and network services.

Network marketing fundamentals

In this section you are introduced to some basic traditional marketing concepts and strategies.

First, however, it's best that you get some of the terminology associated with marketing clear in your mind. In the following, we have selected some marketing terms which are of particular relevance to our unit. Read through them quickly to get a general feel for what they mean.

Marketing:

Marketing is an organizational function and a set of processes for creating, communicating, and delivering value to customers and for managing customer relationships in ways that benefit the organization and its stakeholders.

Direct marketing:

1 *Retailing definition* — A form of non-store retailing in which customers are exposed to merchandise through an impersonal medium and then purchase the merchandise by telephone or mail.

2 *Channels of distribution definition*: The total of activities by which the seller, in effecting the exchange of goods and services with the buyer, directs efforts to a target audience using one or more media (direct selling, direct mail, telemarketing, direct-action advertising, catalog selling, cable selling, etc.) for the purpose of soliciting a response by phone, mail, or personal visit from a prospect or customer.

E-mail marketing (email marketing):

E-mail marketing is simply marketing via email.

Marketing of services:

The organizational structure for the marketing of intangible services is the same as, or similar to, the marketing of tangible products. The term product as used in the organizational definitions in this dictionary can be read to mean services as well. Also, the term production refers to manufacturing, assembly, or other means of creating a tangible product, while the term operations commonly refers to the functions that supply an intangible service. Hence, when substituting service for product in a definition, one can also substitute operations for production.

Comment: Service has meanings in marketing other than product. This can be seen in the definition for marketing services, in which service refers to auxiliary functions that aid in the sale, distributions, and customer usage of a product. Another meaning of service can be seen in the definition for marketing services department, in which a centralized department supplies assistance (i.e., services) to division marketing departments in a divisionalized company.

Online marketing:

A term referring to the Internet and e-mail based aspects of a marketing campaign. Online marketing can incorporate banner ads, e-mail marketing, search engine optimization, e-commerce and other tools.

Permission marketing:

Marketing centered around getting a customer's consent to receive information from a company.

Auction:

A market in which goods are sold to the highest bidder. The auction usually is well publicized in advance or held at specific times well known in the trade. Exchange is effected in accordance with definite rules, with sales made to the highest bidder.

(American Marketing Association)

The following reading provides a quick overview of marketing in general, and the 4Ps of marketing: product, price, place and promotion.

Reading 10.7 (online)

Volker, M, 'Business basics for engineers':
http://www.sfu.ca/~mvolker/biz/mktintro.htm

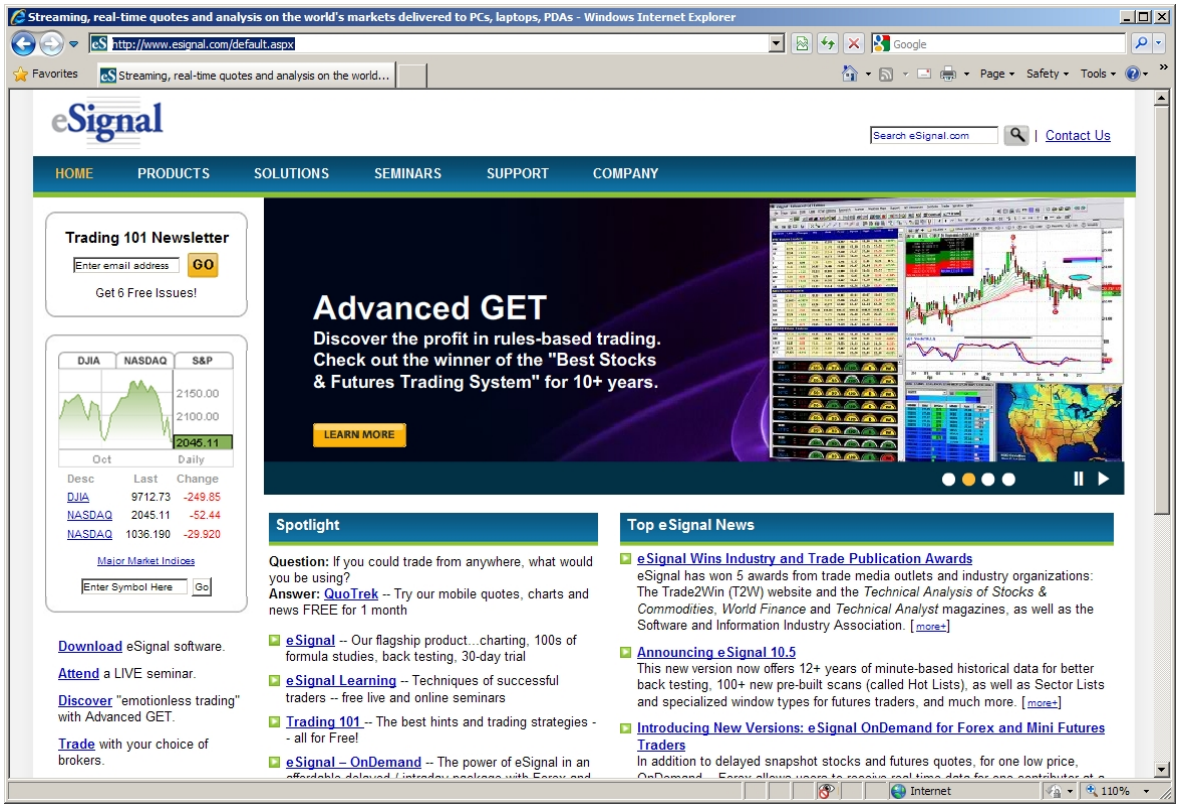
The following reading introduces you to another marketing approach that's increasingly important in network marketing.

Reading 10.8 (online)

Blankenhorn, D (1999) 'Affinity marketing comes to the Web':
https://www.clickz.com/clickz/column/1700469/affinity-marketing-comes-to-the-web

Activity 10.4

If you visit eSignal.com (http://www.esignal.com), you can find a number of products related to financial information, investment tools, and so on. See the illustration below.



Source: eSignal.com

Why do you think eSignal is on offer for a 30-day free trial, but there is no free trial for eSignal Pro?

As you can see, with the advance of network technologies, marketing has undergone fundamental changes. The Internet provides unique features — such as interactivity, instantaneousness, borderlessness, customizability and multimedia — that traditional media lack. Taking advantage of these capabilities has therefore led to changes in customer-to-customer, customer-to-business, as well as business-to-business relations.

Activity 10.5

How do you think Internet permission-based marketing might be related to spam messages?

Approaches to network marketing

Sales promotions, public relations, personal selling and advertisements are all vehicles employed by businesses and organizations to communicate with customers. The service or product needs to be made known to potential clients. This is certainly true of network products and services. For example, the author of this unit has often been asked by students, colleagues and clients questions such as, 'How do people on the Internet find out my website?' — whether that site is for individual, work or business purposes. Figure 10.20 shows a simplified model as to how a webpage is located by potential surfers or clients.

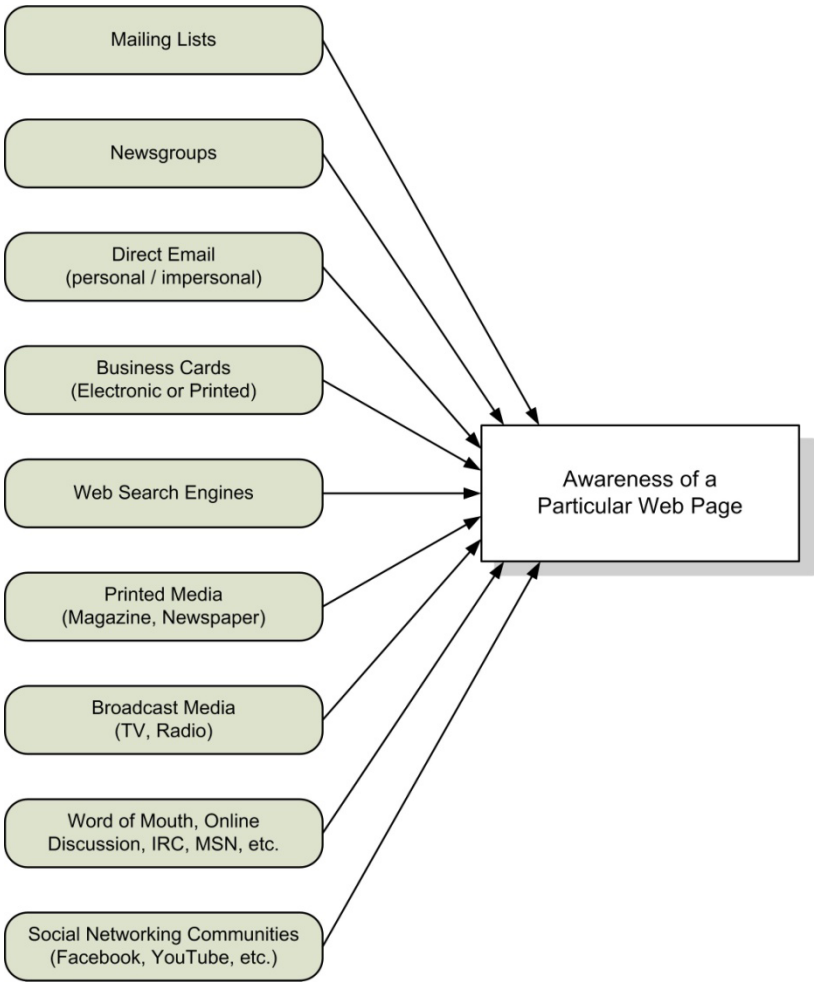


Figure 10.20 How people find out about a webpage

As you can see from this figure, there are lots of potential approaches a marketer can take. In this topic we will concentrate on five approaches that are particularly appropriate to marketing network products and services: email, websites, mobile networks, faxes and e-auctions.

Network marketing via email

Virtually everyone with Internet access has email access, so email has the potential to be a very powerful business communication tool. Not only can

it be used as an important part of one's online marketing strategy, it can also be used to cut long distance fax and telephone expenses, as email messages can be sent to any email address, anywhere in the world, with no long distance charges. As a hybrid of postal mail and the telephone, there's no doubt that email has at least the same value potential to business as the telephone did when it emerged some 100 or so years ago.

Let's begin with a short reading that introduces you to marketing on the Internet in general, and via email in particular.

> ***Reading 10.9 (online)***
>
> DeLegge, P, 'Internet marketing basics':
> http://www.marketingtoday.com/imarketing/imbasics.htm
>
> Read the first six paragraphs of the article, i.e. up to the section on email marketing.

We can broadly classify email marketing into the following three categories, according to the level of permission given to the sender:

1 **Permission-based email marketing:**

This refers to email sent to addresses that were obtained with the owners' implicit permission to receive email advertisements. This is often done in exchange for gifts or online services.

2 **Non-permission-based email marketing:**

This approach is often simply reduced to email spam, so you are strongly advised not to take up this approach!

3 **Passive advertisement:**

For example, when one responds to a query or posts a query in a discussion forum or newsgroup, it is perfectly legitimate to include an 'email signature' at the end of one's response or query. Below are some sample email signatures that include indirect email advertisements.

Example 1:

```
-------------------------------------------------------------------------------------------------------
Jessie Srader        | E-mail jsrader@intergate.com
6119 F.M. 1960 w.#6  | http://www.intergate.com/~jsrader/webdesg.html
Houston, Tx. 77069   | Web Page Design and Marketing Consultant
(713)893-6126        | E-mail for a free estimate using a proven system
-------------------------------------------------------------------------------------------------------
```

Example 2:

```
-------------------------------------------------------------------------------------------
'A Serious Business'     the international e-mail newsletter
by and for people in smaller businesses in over 70 countries
-------------------------------------------------------------------------------------------
To Request a FREE Sample Copy -> Sample@EarthOne.com
And a FREE Trial Subscription -> Trial@EarthOne.com
Visit Us on the Web at        -> http://www.EarthOne.com
-------------------------------------------------------------------------------------------
```

Example 3:

```
============================================================
       S I M P L Y   I N T E R A C T I V E ,   I N C .
 I N T E R N E T / I N T R A N E T   T E C H N O L O G I E S
============================================================
Simply Interactive, Inc.          | E-mailto:info@simply.com
Internet/Intranet Technologies    | Tel: 408.260.6500
http://www.simply.com             | Fax: 408.260.6501
                                  | Snail: 650 Saratoga Ave.
                                  | San Jose, CA. 95129
============================================================
```

For skilled practitioners, therefore, email can offer a marketing channel that is similar to direct marketing in traditional marketing (i.e. marketing via posted letters) but at a much lower cost.

Activity 10.6

1 What are some of the attributes of an effective permission-based email marketing campaign?

2 There are a number of well-established companies that help clients to conduct email marketing, for example, www.winet.com:

Search the World Wide Web and find two more such companies. What specific values would clients, such as the OUHK, receive for subscribing to the services offered by this kind of company?

Network marketing via websites

Web marketing is a relatively new form of 'non-intrusive' advertising in which the customer actively chooses to visit and interact with a company's marketing communication efforts. Recent efforts involve the merging of information and images in innovative ways. You can learn more by continuing with the DeLegge reading.

Reading 10.10 (online)

DeLegge, P, 'Internet marketing basics':
http://www.marketingtoday.com/imarketing/imbasics.htm

Read from the seventh paragraph of the article through the section 'Give it away free.'

You should also skim through the following humorous article, which compares designing networks with ants building communities:

Hafner, K (2001) 'Better network: Look to nature':
http://www.nytimes.com/2001/09/13/technology/better-networks-look-to-nature.html?pagewanted=all

One of the best ways to get people to visit one's website, for example, is to attract their attention by giving away something interesting, free, or useful. This is much like bees being attracted to a honeypot. However, this assumes the diffusion of the site's URL by means such as cross links to other websites, word of mouth, or editorial reviews in broadcast programmes, printed publications or electronic media.

Many of the earlier Web interface design approaches can be traced back to the proceedings of the International World Wide Web Conference series that started in early 1994. Foundational WWW interface articles came from Jakob Nielsen, e.g. his 1994 'Sun Web: User Interface Design for Sun Microsystem's Internal Web,' which he co-wrote with Darell Sano. Nielsen has subsequently published more Web interface-related work under the banner of usability. Among the most famous is his listing of the top ten common mistakes in Web design ('Top ten Web design mistakes of 2005', http://www.useit.com/alertbox/designmistakes.html). Many of you will have read an earlier version of Nielsen's usability article in courses such as *U234* or other e-commerce courses.

Since we have already covered most of the design and technical issues related to website design in earlier units and the course TMAs — such as how to develop interactive webpage applications, develop flat-file

databases, and set up Apache Web Server on Linux machines — we will not revisit them now.

There are ways, of course, of checking to see how well a website has been designed as an effective marketing tool. Measures of the duration of time spent at the site, the depth of searches through the site, navigation patterns through the site, navigation patterns through the site, and repeat visits to the site are crucial outcome measures for evaluating the effectiveness of such sites.

Activity 10.7

1 Take stock of the various email marketing messages you have received in the last two weeks. Did any of these messages include 'honeypot' offers or other 'give it away free' approaches?

2 Comment on the techniques that can be used to promote a particular website that provides one of the network products or services you're familiar with.

Hint: You can check out the examples below.

Network games conference service: http://www.gdconf.com/

Network marketing via wireless networks

In Hong Kong, the growth in the sales and use of mobile telephones has slowed to a very steady state; it's more or less stable in the eight million range, so we can say that the critical mass of mobile phone users has been reached. This has obviously created an increasing demand for wireless and mobile advertising. For example, the growth of Short Message Services (SMS) has increased by over 21% from July 2008 to July 2009, and this trend is expected to continue in the foreseeable future. This offers us new opportunities for network marketing.

Table 10.8 Key statistics for telecommunications in Hong Kong

End of month	Public mobile radio telephone subscriber units	Short message service	
		Sent	Received
12/2002	6,218,984	23,920,950	70,990,648
12/2003	7,194,335	60,989,502	127,303,535
12/2004	8,157,960	118,882,924	208,907,525
12/2005	8,544,255	173,790,031	277,383,505
12/2006	9,444,140	256,644,954	393,378,089
12/2007	10,588,504	334,773,143	504,974,534
12/2008	11,374,224	436,600,919	611,215,487
6/2009	11,705,058	472,990,941	649,870,848

Source: Office of the Telecommunications Authority, Hong Kong

The following reading analyses the business model for a mobile advertising firm, and highlights some of the key issues for modelling advertisement deliveries via wireless networks.

Reading 10.11 (online) (optional)

Tripathi, A K (2006) 'Advertising via wireless networks', *International Journal of Mobile Communications*, 4(1): 1–16:

This article is available in the OUHK E-Library. Log in to the OUHK E-Library. Select **E-Journals & Databases → Browse** (on the top left) **→ Database Providers → Inderscience Enterprises → International Journal of Mobile Communications (Inderscience) → Volume 4 Number 1 / 2006 →** select the article and choose to open the **Entire document** in pdf.

Activity 10.8

Review the last ten SMS messages you received. How many of them were wireless network advertising-related?

Among the types of SMSs that were delivered to your mobile phone:

1 Name the type of SMS marketing you liked the most. Why did it attract you?

2 Name the type of SMS marketing you disliked the most. Why did you dislike it?

Network marketing via fax

Hong Kong has a unique telecommunication payments policy. Unlike most of the rest of the world, in which a user pays for each individual local call, fixed telephone line users in Hong Kong are allowed unlimited calls for a nominal monthly fee. This has given rise to the popularity and viability of fax marketing in Hong Kong. There are many tools and services that help you use the Internet to send faxes locally as well as overseas. Some are free, while others require you to pay a subscription. The following reading introduces you to the basics of faxing via the Internet.

> ***Reading 10.12 (online) (optional)***
>
> 'How can I send a fax from the Internet':
> http://www.savetz.com/fax

Activity 10.9

1 Fax marketing: Where does it fit?

Fill in the following table to indicate whether or not fax marketing can be used in the following e-commerce models.

Model	Suitability
C2C	
C2B	
C2G	
B2C	
B2B	

B2G	
G2C	
G2B	
G2G	
C = Customer, B = Business, G = Government	

2 Tools and services for fax marketing in Hong Kong.

Name one Windows platform based fax tool, and name one commercial service for broadcast fax services in Hong Kong.

3 How cost-effective is fax marketing?

Network marketing via e-auctions

E-auctions have become a very popular consumer-to-consumer mode of e-commerce throughout the world. Locally, a recent news report stated that there are over 1 million Hong Kong Internet users actively engaged in e-auctioning. The opportunities offered by e-auctions are enormous.

Reading 10.13 (online)

Steiner, I (2004) 'AuctionBytes industry profile': http://www.ecommercebytes.com/cab/abu/y204/m12/abu0132/s04

Read from the paragraph labeled 'Can you share a tip, trick or tool that helps you buy or sell on eBay?' onwards to the end of the article.

Why are people using e-auctions?

The most quoted reasons for buying via e-auctions include:

- looking for bargains; and
- looking for hard-to-find items.

Reasons people sell via e-auctions include:

- the low cost of advertising;
- the large number of potential buyers;
- the very low cost to start one's own online business; and
- to be environmentally friendly, i.e. to try to get rid of usable items that are not needed.

There's a common marketing maxim that goes: 'to sell your product, you must sell at the right time and in the right place to promote your product.' This statement is actually very valid in the case of e-auctioning.

But what attracts a customer to bid for your products among the many others on offer? This is not so simple to answer. Due to the human propensity to be cautious about trusting strangers, sellers with good credit ratings online will certainly attract more bidders. Bidders are more often than not willing to pay a higher cost when dealing with sellers who have a high credit rating online. So how do people build up creditability online? There are ethical and non-ethical ways, and these can be learned after some months of using auction platforms.

Activity 10.10

Work through Lab 3.1 — 'Doing business on the Internet: E-auctions' in the 'Lab Book' (Kwan et al. 2009).

The sky is the limit

You are no doubt aware of how the founders of a number of famous software companies (Netscape, Yahoo!, Google, eBay, etc.) crafted their businesses on the Internet. It sometimes seems that business opportunities on the Net abound, and the sky is your limit.

To complete our study in this unit, read the following brief article, which introduces you to a recent example of a successful business that has made its name by both providing network services, and marketing itself effectively.

Reading 10.14 (online)

Baily, J (2005) 'As background checks get big, the little guys get bigger', New York Times: http://www.nytimes.com/2005/11/16/business/businessspecial/16bailey.html

Summary

In this final unit of the course, we have covered two broad topics: network design and network marketing.

In the first part of the unit we covered the network design process as a whole. We defined the design goals, which include both business and technical aspects. The important thing to remember is that network design is a trade-off between cost and availability.

Detailed network requirements have to be worked out through careful analysis from several aspects. User requirements are critical, as the network is built to serve them. However, you also have to consider technical aspects such as applications to be run on the network, and the capacity for future expansion. Analysing network requirements will give you a better idea of what should be included in the network solution. In the actual design, you have to make decisions on quite a lot of technical options. For easier management and higher scalability of the network, you are advised that the structure of your network should follow the hierarchical model. Your network need not include all three layers of the model. Depending on the size of your network, you may choose to implement just one layer or two layers of the model. After building the network framework, you have to select a suitable backbone, an appropriate addressing scheme and an efficient interconnection method.

Working through the design process should give you a better understanding of the positions of each component in a network. The coverage of implementation of a Windows 2003 network presented a practical example of the capabilities of the network construction.

After building a network, you need to make sure it continues to run effectively. This can be done through network monitoring and management. Even though you have done a very good maintenance job, problems can still occur. A network consists of a diversity of elements. It is impossible to have a solution that applies to all problems and scenarios. However, there are still general guidelines for network troubleshooting.

In the second part of this unit we introduced the basic concepts in network marketing. We discussed why it is important to design for marketing and to design in a global environment based on a network marketing framework. We then explained various components of network marketing: network infrastructure and technology, marketing, and network economics. We focused on the intersection of the three main components of the network marketing framework. You were then introduced to a range of different approaches to network marketing: email, websites, wireless networks, faxes and e-auctions. We finished the discussion on network marketing with a brief introduction to a successful networking company.

You have learned comprehensive theoretical concepts and practical techniques in network programming, design and marketing. After this

course, you should be able to carry out network planning, design and implementation independently. I hope you will find that the materials covered in this course are interesting and rewarding.

Feedback on case studies

The feedback here comprises suggested solutions. You may have come up with others. The main point is that you need to know the reasons for your choices and whether the reasons are strong enough to support your choices in the case given.

Case study 10.1

The LAN in the Arts building is connected using hubs, so all nodes in the LAN share the same collision domain. This is the cause of network congestion. To solve the problem, LAN switches should be used to replace the hubs. Microsegmentation is then achieved. In catering for future bandwidth requirements, 100BaseT switches may be used to provide a 100 Mbps bandwidth to each node. The same solution can be applied to the LAN in the Science building.

For the Engineering building, the LAN is connected using bridges, so it is not currently facing the network congestion problem. However, in planning for future expansion, the bridges on each floor should be replaced by switches to provide higher bandwidth to each node.

VLANS may be deployed for each department in the Art, Science and Engineering buildings. Traffic within a department can be isolated.

For the connections among the buildings, the following design provides three design solutions.

New design 1

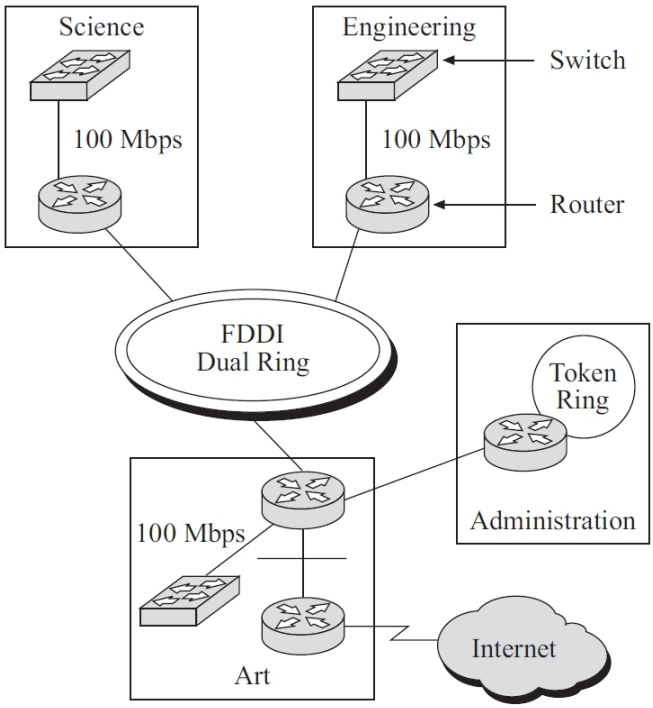


Figure 10.21 Case study 10.1: suggested design 1

In this design, an FDDI is implemented as a backbone to interconnect the LANs in each building. In this case, there is a router in each building for connecting to the backbone. The router is also used for the communications of the VLANs among the departments in each building. One router port in the Administration building is used to connect the Token Ring. In the Arts building, one more router is equipped. This router is attached to the central router of the Arts buildings and is used to give Internet access to the whole network.

New design 2

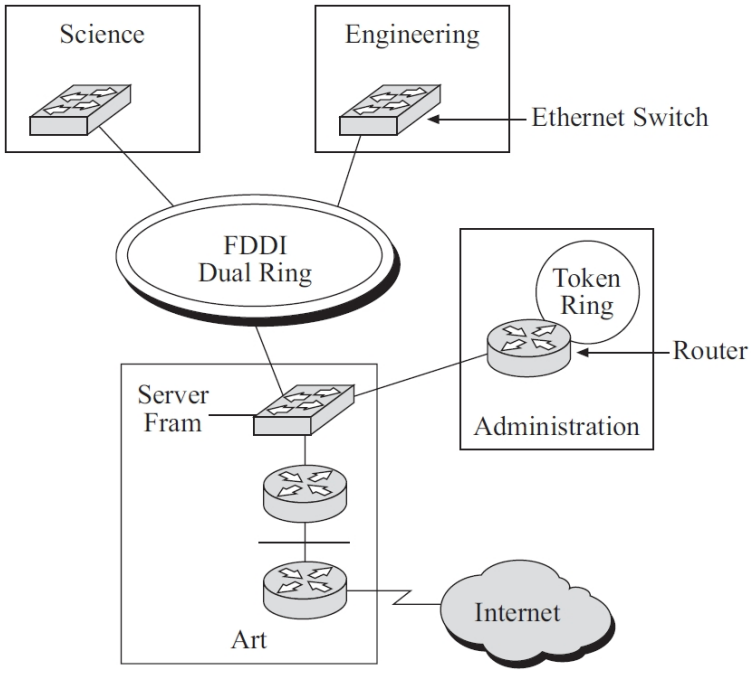


Figure 10.22 Case study 10.1: suggested design 2

In this design, the central routers in the Arts, Science and Engineering buildings are replaced by switches for connecting to the FDDI backbone. Two routers are equipped in the Arts building. One router is for the communications among the VLANs in all the buildings; the other is for connecting the enterprise network to the Internet. The servers from other buildings are moved to the Arts building to form a server group for easy management. In this design, higher speed communications among the buildings can be achieved through switches, compared to the previous design in which routers are used, because routing is a more complex process than switching.

New design 3

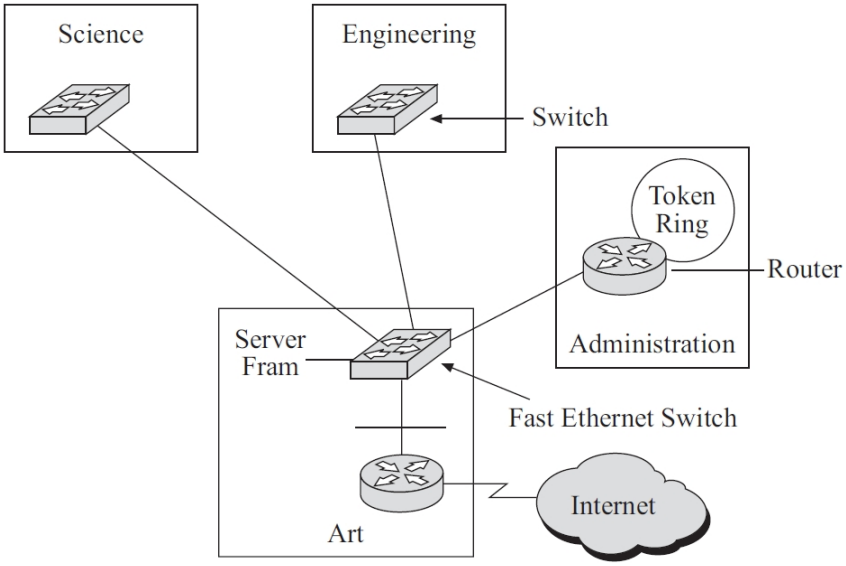


Figure 10.23 Case study 10.1: suggested design 3

This design is almost the same as the previous one, except that instead of an FDDI ring, a Gigabit Ethernet switch is used. This is a deployment of a collapsed backbone in place of a distributed backbone, discussed in the section 'Backbone strategy.' This provides a more cost-effective design and an easy upgrade path.

Case study 10.2

New design 1

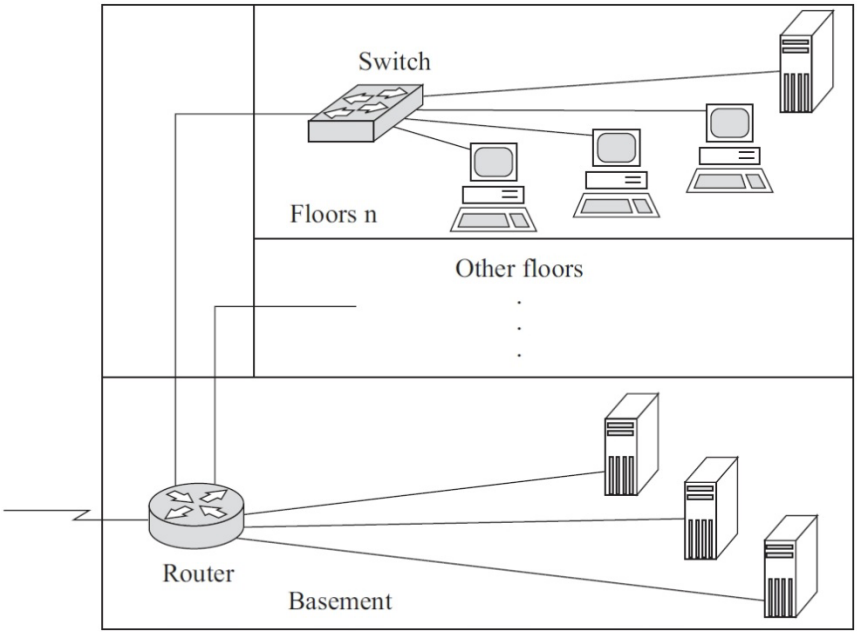


Figure 10.24 Case study 10.2: collapsed router backbone

This design uses a collapsed router backbone. A switch is deployed on each floor. This provides connectivity for the nodes on the floor.

Providing dedicated bandwidth will ensure capacity for future growth. One Fast Ethernet port on each floor switch is then connected to a dedicated Fast Ethernet port on the router, and the router provides the backbone for the building. With each workgroup attached to a separate router port there is isolation between the groups on each floor. Broadcasts are isolated to the workgroup and administrative controls may be implemented through software. The router also provides a WAN connection.

New design 2

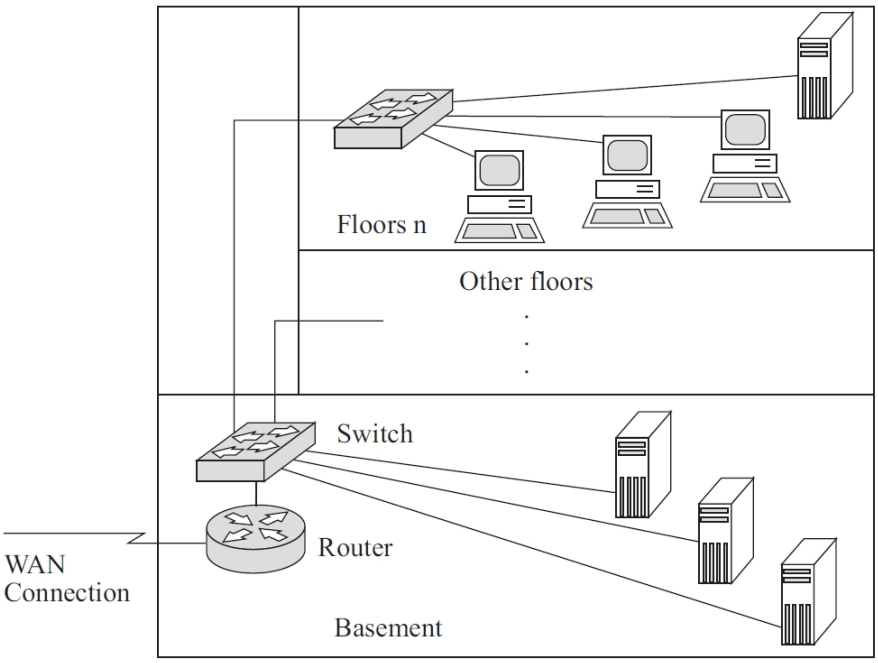


Figure 10.25 Case study 10.2: collapsed switch backbone

This design is similar to the previous one, except that a switch in the basement now provides the building backbone. This would permit the implementation of VLANs throughout the building, and centralized servers in the basement. The router would now have a single Fast Ethernet interface to connect to the basement Ethernet switch, and this serves as the routing capability between VLANs. The router also provides the WAN connection as before.

Addressing

By using Class A private address 10.0.0.0 they would have ample address space for allocation of addresses. By using a 24-bit subnet mask, that is 255.255.255.0, 65536 subnets are available:

```
10.0.0.z
10.0.1.z
   :
10.0.255.z
10.1.0.z
10.1.1.z
   :
10.1.255.z
```

```
 10.2.0.z
 10.2.1.z
     :
10.2.255.z
 10.3.0.z
 10.3.1.z
     :
10.3.255.z _______65536 subnets
     :
     :
10.254.0.z
10.254.1.z
     :
10.254.255.z:
 10.255.0.z
 10.255.1.z
     :
10.255.255.z
```

You may give each site 256 subnets for internal use. For example, the site in Causeway Bay is given the subnets:

```
 10.2.0.z
 10.2.1.z
     :
10.2.255.z
```

Each subnet can accommodate up to 254 nodes. You may implement one subnet or two subnets on each floor in each site, depending on the specific needs.

Case study 10.3

Each workstation can only retrieve one announcement at the same time, and the video server will disable this retrieval when there is a video broadcast. That means that, at the same time, there is still one video stream coming into each machine, and no additional loading placed on the links of each workstation to the backbone switch.

However, there is additional loading on the link of the video server to the backbone switch, since each workstation may retrieve different past announcements. At most there will be 20 video streams retrieved from the video server. The following is a simple analysis:

loading for one video stream = 1.54 Mbps

loading for 20 video streams = 1.54 × 20 = 30.8 Mbps

bandwidth for the link for server to switch = 10 Mbps

This simple analysis shows that the bandwidth for the link from the server to the backbone is not sufficient to support the deployment of this video application.

The network equipment has to be upgraded. One suggestion is to replace the Ethernet switch by a Fast Ethernet switch that provides 100 Mbps dedicated bandwidth to the machines connecting to it.

New design

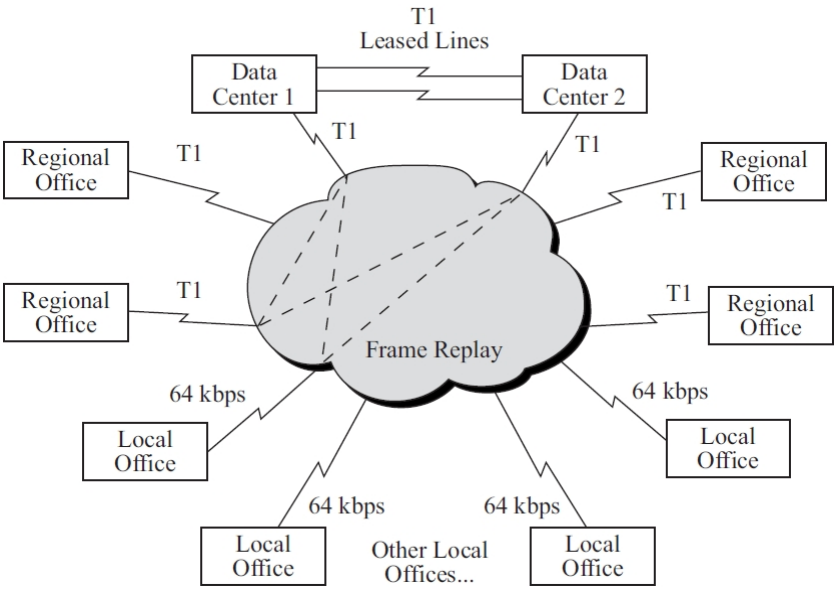


Figure 10.26 Case study 10.3: most cost-effective suggested design

The most cost-effective design that would meet the requirements would be deploy T1 leased line circuits between the two main data centers and use frame relay everywhere else. The access speed should be T1 for the main data centers and regional offices; the local offices could get 64kbps. A total of 40 PVCs is required to meet the redundant requirements.

Suggested answers to self-test questions

Self-test 10.1

1 The key trade-off is most often availability versus cost. The best technology available to solve a particular network design problem may not be within the budget.

2 The five goals of a network designer in designing a network are:

- *Functionality* — The design must produce a working network. That is, a network that provides end-to-end application availability of the services required by the users.
- *Scalability* — The network must be able to grow in size.
- *Adaptability* — The network design should be able to accommodate new technologies as they emerge.
- *Manageability* — There must be management capabilities in the network design.
- *Cost-effectiveness* — The network design must be within budget.

Self-test 10.2

1 Network design tools can perform a number of functions to help in the technology design process. Some network design tools can discover the existing network; that is, once installed on the network, they will explore the network to draw a network diagram. For example, simulation can be used to model the behavior of the communication network.

Network modelling and design tools can perform a number of functions to help in the technology design process. With most tools, the first step is to enter a map or model of the existing network or proposed network design. Some modelling tools require the user to create the network map from scratch. That is, the user must enter all of the network components by hand, placing each server, client computer, and circuit on the map, and defining each. Other tools can 'discover' the existing network. In this case, the user provides some starting point; the modelling software explores the network and automatically draws the map itself.

Once the map is complete, the next step is to add information about the expected network traffic and see if the network can support the level of traffic that is expected. Simulation is used to model the behavior of the communication network. Once the simulation is complete, the user can examine the results to see the estimated response times and throughput. It is important to note that these network design tools only provide estimates, which may vary from

the actual results. At this point, the user can change the network design in an attempt to eliminate bottlenecks and re-run the simulation.

Good modelling tools not only produce simulation results, but also highlight potential trouble spots (e.g. servers, circuits, or devices that experienced long response times). The best tools offer suggestions on how to overcome the problems that the simulation identified (e.g. network segmentation, increasing from T1 to T3).

2 It costs more because it requires buying much more redundant hardware and connectivity, which is more expensive than redundant components or using software-based fault tolerance techniques.

3 Examples of projects driven by security needs include:

- installation of firewalls at WAN locations
- modifications to firewall or router configurations or operating systems
- implementation of intrusion detection systems
- a company-wide effort to enforce security policies, such as good password selection.

Self-test 10.3

Membership to a particular VLAN can be based on the following criteria:

- Port-based
- MAC-based
- Protocol-based
- IP subnet-based.

Self-test 10.4

1 Both bridges and switches operate at the data link layer, may connect different types of cable, and can use the same data link and network protocol to connect computers or network segments. With the exception of new address encounters in an address-learning phase, layer-2 switches replace the Ethernet broadcast paradigm with a capability for simultaneous processing of multiple messages.

Bridges are commonly used to segment local area networks to improve performance. Bridges ‘learn’ whether to forward packets from one network segment to another. When a bridge receives a packet, it reads the packet’s data link layer source address and compares this address to its own internal address table. If the destination address is on the same network segment from which the packet arrived, the bridge discards the packet, which is a process known as filtering.

Layer-2 switches (or workgroup switches) typically provide ports for a small set of 16 to 24 computers. Layer-2 switches operate at the same layers as bridges but differ from them in two ways. First, most switches enable all ports to be in use simultaneously by managing paired combinations of ports as separate point-to-point circuits. Since all ports can be active at once, switches usually are faster than bridges. Like bridges, layer-2 switches 'learn' addresses; a layer-2 switch builds a forwarding table after it is first turned on. To learn addresses, a layer-2 switch retransmits to all ports (except to the one from which it was received) only for a packet with a destination address not already in the forwarding table. The resulting ACK from the destination computer (that recognized its address) is then used by the layer-2 switch to add the new port number and address to the forwarding table. As layer-2 switches become more powerful, they render bridges obsolete.

2 Routers work at the network layer and use network layer addresses. They keep routing tables, and operate through software control. A routing switch is also called a layer-3 switch; it does its routing with hardware. A routing switch operates at wire speed and is much faster than a router.

3 A collapsed backbone network uses a star topology with one device, usually a switch, at its center. The traditional backbone circuit and set of routers or bridges is replaced by one switch and a set of circuits to each LAN. The collapsed backbone has more cable but fewer devices. There is no backbone cable. The 'backbone' exists only in the switch, which is why this is called a collapsed backbone. The original collapsed backbone technology uses layer-2 switches and suffers some disadvantages because of the data link layer overhead message traffic load, and limitations on network segmentation. This weakness has been recognized, so collapsed backbone technology is adapting by evolving to the use of layer-3 switches to overcome these problems. The result is better performance and improved network management capabilities for collapsed backbone networks.

   Collapsed backbones are probably the most common type of backbone network used in the distribution layer (i.e. within a building). Most new building backbone networks designed today use collapsed backbones. They also are making their way into the core layer as the campus backbone, but routed backbones are still common.

4 The three technology layers are:

   - the access layer consisting of layer-2 technology of LANs connected to a backbone network (BN)
   - the distribution layer as the part of the BN technology that connects the LANs and contains 'TCP/IP gateways' (or, most likely, routers) that are usually located within a single building
   - the core layer that connects the different BNs, often from building to building.

Self-test 10.5

1 The Active Directory is Microsoft's directory service implementation. The Active Directory is designed to serve as an organization's central directory, combining authentication and email into a single directory structure.

2 To obtain summary information on a server's performance, run Task Manager to observe common data points contained under Performance tab. This can give you an idea of where your performance bottleneck is. Next, run the System Monitor snap-in and observe detailed performance metrics. Add resources as necessary, or remove applications that are creating the bottleneck(s). After you have resolved the performance problem, use the Performance Logs and Alerts to log performance activity. These logs serve as your baseline for future performance monitoring. To ensure that you are not caught off-guard by performance or a potential hardware failure, create alerts to track the activity of the server. If you think poor performance might be related to network activity, run the Network Monitor to analyse network activity.

Self-test 10.6

1 Determine the present capacity of the network in use, number of workstations, and the number of servers. Will the 200 users be new to the network, or only new to the client/server application? Obtain benchmarks on the new application and its hardware. Contact other locations using the application for information about performance. Find out about average file sizes used, typical reports to be run, the load on the network due to reports, and whether the application follows client/server development guidelines.

2 The baseline statistics should include:

- network utilization
- packet traffic
- bytes sent per second
- error rates
- peak times
- slow times
- disk access statistics
- disk and CPU access queue lengths
- traffic generated by specific servers and hosts.

Self-test 10.7

1 A time domain reflectometer tests impedance, shorts, opens, interference, cable distances, and other problems. It transmits a signal and assesses information from the returned signal reflection. An optical time domain reflectometer performs a similar function, but on fiber optic cable it transmits light instead of an electrical impulse.

2 If two nodes are connected with the same address, one or both nodes will experience high error rates, or may not communicate on the network at all.

3 The network does not match IEEE specs, so packet transmissions are not reliable. Portions of the network with 54 ohm cannot guarantee point-to-point packet transmission within the maximum time allotted for Ethernet. The 54-ohm cable should be removed and replaced with high quality 50-ohm cable.

Glossary

backbone — The part of a network to which segments and significant shared devices (such as routers, switches, and servers) connect. A backbone is sometimes referred to as 'a network of networks,' because of its role in interconnecting smaller parts of a LAN or WAN.

broadcast — A transmission that involves one transmitter and multiple receivers.

broadcast domain — A combination of ports on a switch (or multiple switches) that make up a Layer 2 segment. To be able to exchange data with each other, broadcast domains must be connected by a Layer 3 device, such as a router or Layer 3 switch. A VLAN is one type of broadcast domain.

collapsed backbone — A type of backbone that uses a router or switch as the single central connection point for multiple subnetworks.

collision — In Ethernet networks, the interference of one network node's data transmission with another network node's data transmission.

collision domain — A portion of a LAN encompassing devices that can cause and detect collisions among their group. Bridges and switches can logically separate collision domains.

distributed backbone — A type of backbone in which a number of connectivity devices (usually hubs) are connected to a series of central connectivity devices, such as hubs, switches, or routers, in a hierarchy.

Metcalfe's Law — This law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). Metcalfe's law characterizes many of the network effects of communication technologies and networks such as the Internet, social networking, and the World Wide Web.

microsegmentation — The segmentation of a collision domain into as many segments as there are circuits, minus one (number of segments = number of circuits − 1). This microsegmentation performed by the switch cuts the collision domain down so that only two nodes coexist within each collision domain. This way, collisions are decreased, and only the two NICs that are directly connected via a point-to-point link are contending for the medium.

Moore's Law — The law describes a long-term trend in the history of computer hardware in which the number of transistors can be placed inexpensively on an integrated circuit has doubled approximately every two years. Moore's law precisely describes a driving force of technological and social change in the late 20th and early 21st centuries. The trend has continued for more than half a century, and is not expected to stop until 2015 or later.

protocol analyser — A software package or hardware-based tool that can capture and analyse data on a network. Protocol analysers are more sophisticated than network monitoring tools, as they can typically interpret data up to Layer 7 of the OSI Model.

Simple Network Management Protocol (SNMP) — An Application layer protocol in the TCP/IP suite used to convey data regarding the status of managed devices on a network.

the Law of Disruption — Social, political, and economic systems change incrementally, but technology changes exponentially.

Virtual Local Area Network (VLAN) — A logical grouping of network nodes, regardless of their physical locations, to form a single broadcast domain.

segmentation — The process of splitting a single collision domain into two or more collision domains.

References

Beasley, J S (2009) *Networking*, 2nd edn, Prentice Hall.

Kwan, R et al. (2009) *A Practical Approach to Internet Programming and Multimedia Technologies*, The Open University Press.

Tsang, P, White, B, Fox, R and Kwok, P (2009) *An Educational Guide to IEEE 802.11 WLAN Survey & Visualisation Experiments*, Hong Kong: Pearson Prentice Hall Publishing.

Online materials

American Marketing Association, http://www.marketingpower.com.

eSignal.com, http://www.esignal.com/default.aspx.

Game Developers Conference, http://www.gdconf.com/.

Office of the Telecommunications Authority, Hong Kong, *Key Statistics for Telecommunications in Hong Kong*, http://www.ofca.gov.hk/filemanager/ofca/en/content_108/wireless_en.pdf.

OPNET Modeler, http://www.opnet.com/.

Wikipedia, 'Law of disruption', http://en.wikipedia.org/wiki/Law_of_disruption.

Wikipedia, 'Metcalfe's Law', http://en.wikipedia.org/wiki/Metcalfe's_law.

Wikipedia, 'Moore's law', http://en.wikipedia.org/wiki/Moore's_Law.

winet.com, http://www.winet.com/.