Web Server Administration

Author: Steve Silva

Revision: Scott Rysdahl, Luke LaValley &
Mark Anderson

8/1/2016

Second Revision: Tom Gustafson

8/1/2016

Table of Contents

Chapter 1 The Basics of Server and Web Server Administration

In this chapter, you will:

- ♦ Review the Internet and the World Wide Web
- ♦ Learn about server administration
- ♦ Learn about Web server administration
- ♦ Explore the common tasks and services performed by administrators
- ♦ Examine networking building blocks
- ♦ Discuss the Web server platforms Windows Server 2012 and Linux Debian Ubuntu
- ♦ Discuss the Importance of Virtualization and Cloud Hosting

This chapter introduces the basics of server administration and Web server administration for anyone interested in being a Web server administrator. Whereas a server administrator focuses on the computing needs inside the business, a Web server administrator focuses on making sure that a variety of services are available on the Internet. To offer these services, you may need to evaluate and select options from among a variety of hardware, such as servers, routers, and firewall products. You also need to choose a Web server platform, such as Windows or Linux. The Windows platform offers more than one operating system, while more than one company produces the Linux operating system. After you choose the server and operating system, you should select server software products, such as software needed to run and maintain the Web server and to offer other services, such as File Transfer Protocol (FTP), e-mail, database, programming languages, and security software. After you select and install the Web server software, you must maintain the server daily by monitoring its performance and usage, installing software updates and security patches, and generally making sure that the Web server environment continues to meet the needs of the organization.

When you administer a Web server, you need to understand the Web server environment, which includes the network on which the Web server runs. In this chapter, you will review the basic components of a

network and learn how the Web server fits into both the local area network (LAN), and the wide area network (WAN). A LAN is a group of computers along with the devices and media that connect them, which are all under the direct control of the administrator. The WAN is primarily a public, shared network that connects regions and countries. For example, the Internet is a WAN.

REVIEWING THE INTERNET AND THE WORLD WIDE WEB

The Internet is a worldwide network of networks. The term "World Wide Web" (or "Web" for short) refers to the part of the Internet used by the HTTP protocol. Web browsers and Web servers use the HTTP protocol to communicate with one another. When you use a Web browser, you are using the Web. For example, in a browser, you could type *www.technowidgets.com* to visit the Web site of TechnoWidgets Inc. When you do so, you use the Web to access information provided by TechnoWidgets Inc. When you send an e-mail message to *info@technowidgets.com,* your message may go to an e-mail server that TechnoWidgets Inc. runs. Although you use the same connection between you and the server at TechnoWidgets Inc. to send the message, in this case you use the Internet not the Web. The Web is not separate from the Internet, but rather represents a way to identify a type of communication on the Internet that relies on HTTP. Web administrators often manage applications that use more of the Internet than just the Web.

The Internet is not centrally controlled. Instead, it depends on the cooperation of many entities to make sure that the thousands of networks that make up the Internet function correctly. In some countries, market competition determines how the Internet is configured. In other countries, the national telecommunications monopoly controls the Internet. The Internet shares part of the WAN that is also used by the international telecommunications network, but is distinguished by its use of TCP/IP.

Although the Internet had its origins in the 1960s, major changes began in 1995 when a new backbone was created along with four **network access points (NAPs)**.A **backbone** is a high-speed network that connects to other networks—no users connect to a backbone. NAPs are of historical interest only since they were long ago replaced by Internet Exchange Points. This is facilitated by **peering agreements** which are agreements between network owners and Internet service providers (ISPs) to exchange traffic.

The Web comprises the network of Web servers on the Internet. The Internet is a very large WAN. However, a WAN serves purposes other than supplying the network for the Internet. Namely, it carries voice data for the telephone system and can be used to connect the main office of a business to a branch office.

UNDERSTANDING SERVER ADMINISTRATION

Server administrators focus on their LAN, provide access to the software and services their users need, and make sure that the users' environment is reliable and consistent. Although users must have enough network access to perform their work, server administrators must also control that access to minimize the harm that users can do to the network, either intentionally or unintentionally. Often the server administrator's job extends to the whole network because all components must work together.

Working with Users

Users are central to server administration because the purpose of the server—and of the LAN in general—is to make users productive. A LAN can serve hundreds or even thousands of users who need to perform their work as efficiently as possible, and the server administrator makes sure they can access the resources they need, whether those resources are on or controlled by the server. For example, many users need access to a single program on the server or to printers managed by the server.

Users like consistency. If they have to move from one computer to another, they usually want the desktop interface to be as familiar as possible. **Roaming profiles** provide this familiarity. A profile is stored on the user's hard disk and contains information such as the user's preferred desktop settings, Windows Explorer folder options, files stored in My Documents, and Internet Explorer Favorites. A roaming profile resides on the server and allows a user to access his or her profile from other computers on the LAN. If the LAN supports users who work from many computers, the server administrator can make sure that these users have roaming profiles. When the user logs on, the profile is transferred to his or her current hard disk. Because the profile includes all the files in My Documents, it can become very large and slow the logon step.

Establishing Access Control

Controlling access to the network is the principal job of server administrators. They need to give users just enough access to do their jobs, but not more. Access control prevents users from harming the system, and it lets everyone use the system efficiently. To ease administration, server administrators organize users into logical groups based on their common needs. For example, one group may consist of the users in accounting and another group may include everyone in marketing. The users in accounting need access to the accounting software and the printers in the accounting department, but they do not need the forecasting software that the marketing personnel use. Accounting users should not be able to modify marketing forecasts or access the printers in the marketing department, because it is inconvenient for the accounting group and ties up the printers for the marketing group, frustrating both groups of users. Users often need to share documents on the server. Server administrators can control access to these documents by assigning permission to users, thereby allowing some users to add documents, others to modify documents, and others to only read documents.

Understanding the Server Environment

All but the smallest network includes more than one server, meaning that the server administrator needs to manage many servers. To simplify this task, networks can group servers. Windows provides a number of ways to do so. In Windows, servers and the associated user computers are grouped into domains. Users log on to a domain, which can be completely separate from or related to other domains. Domains can be part of a larger group called a forest. Server groups, domains, and forests increase the complexity of a network, which complicates server administration because the server administrator must then manage thousands of users.

In addition to setting up servers, the server administrator must understand and often maintain the other devices that surround the server. For example, switches or hubs connect the computers to the network, and routers divide the network into manageable parts. These devices can be connected by wires, fiber-optic cables, or even wireless connections.

UNDERSTANDING WEB SERVER ADMINISTRATION

Whereas server administrators focus on LANs, Web server administrators focus on the Internet. The primary purpose of a Web server is to provide information to anyone who requests it on the Internet. As Web server administrator, this means you allow users outside of your organization to access your server when they visit the Web site that your organization hosts. Because this situation can be like opening your doors to allow anyone access to your computers, security and control become even more important with a Web server than when the computers that access your servers are on a LAN. Unlike server administrators, who have complete control over their environment, Web server administrators need cooperation from people outside the organization, such as the support personnel from an ISP, to solve problems with the Internet connection.

You need many technical skills to administer a Web server. You may need to control access to Web pages, create virtual Web sites on a single server, and make sure that the programming environment and e-mail services are functioning correctly. You must also set up and provide other services. For example, you might provide FTP services to allow users to transfer files from one computer to another across the Internet. You must also work with the domain name service (DNS), which translates host names such as *www.microsoft.com* into Internet Protocol (IP) addresses so that the server can find the appropriate computer when exchanging data across the Internet. You should also understand the roles played by firewalls and proxy servers, which protect the organization's computers from unauthorized users who try to access them via the Internet. These many Web server management tasks are often divided among a number of administrators.

Understanding the Web Environment

The connection that a network maintains to the Internet complicates your job as Web server administrator. Although you may control the Web server and related servers, you can't control the Internet. The best that you can do is to control the access that Internet users have to your servers. You do so by working with the Web environment, which contains all the server software that typically is accessed from outside the organization.

For Web administration, you install and maintain many types of software, such as databases and programming languages that create and update Web pages. You typically install each type of software on separate computers for two reasons. First, if you store your Web pages on the same computer containing the database that supplies data to the Web pages, along with e-mail, FTP, and firewall software, requests for using this software might slow the throughput to an unacceptable point. Second, if one software component malfunctions, it can't affect the other components. The steps and Hands-on Projects in this book simplify the lab environment by instructing you to store all components on a single computer, but you should not follow this practice outside of the lab.

Unlike server administrators, who primarily work with users, Web server administrators work with developers and other administrators, not users. Web developers need to access one or more programming languages and databases to create Web pages, then need to access your Web site to update the pages. Developers might also need to use test sites that remain separate from the production Web server. Web server administrators work with other administrators as well, including the database administrator who controls access to the databases that the Web developers use. The e-mail administrator makes sure that everyone can send and receive mail. Depending on the size of the organization, this administrator may not install and configure the software, but merely maintain the users. As Web server administrator, you need to support these development and administration activities. In particular, you need to determine how developers can access their Web pages securely. If any software develops a problem, you might be involved in troubleshooting to solve the problem.

Selecting Programs and Databases

Although Web server administrators do not necessarily need to know how to program, you do need to know how to install languages so that programmers can use them. Most Web sites display Web pages dynamically. For example, a Web page might display advertisements or products based on user preferences. A Web page is considered to be dynamic when it refers to stored data and then displays information based on that data. To display dynamic Web pages, a Web developer uses a programming language to access information in a database and then displays that information on a Web page. For example, suppose you visit an online bookstore and search for books on Linux. At the Web server, a program takes your search request and examines a database for books on Linux. It then displays a list of all the books that the bookstore has on Linux.

Web developers use a variety of programming languages. Perl was one of the first programming languages used to create dynamic Web pages. Web-based programming languages have evolved significantly since Perl was introduced in the mid-1990s, however. Although Perl was originally designed to process text, it remains popular today.

Microsoft has relied on **Active Server Pages (ASP)**, which uses a scripted environment that usually relies on VBScript, a subset of Visual Basic, for programming logic. Because it is scripted and not compiled, ASP does not offer the features or speed of a compiled language. Microsoft has addressed these concerns and more with ASP.NET, which compiles programs and supports more languages than ASP including VisualBasic.NET and C#.NET. ASP.NET increases its flexibility by using Web services and **Extensible Markup Language (XML)**. A **Web service** consists of one or more programming modules that reside on the Web server and can be accessed from a client computer. XML allows developers to create text files containing tags that define information. Developers can create their own tags within strict syntax guidelines which allow them to send data in text form to be interpreted by otherwise incompatible systems. Web services and XML work together so that data can be sent to a computer for processing. Of course, sending data with a Web page leaves the data vulnerable to hackers and the Web server administrator must work to keep the data secure.

Programs solve specific problems. For example, an accounting program performs calculations to solve accounting problems and a server program is software that runs on a server to solve data transfer problems. A Web server refers to both the software that runs on the server and the server hardware.

A **service** is a program that runs in the background. In the UNIX/Linux environment, a service is called a **daemon**. Web servers and e-mail servers are considered services because they are always running in the background. Because a Web service has come to mean a programming technique used on the Web, the Web server is not called a Web service.

Besides the Microsoft .NET languages, one of the most popular programming languages is Java, which is an object-oriented, standards-based language with industry-wide support. Web server environments often include Java because developers can use it to create dynamic Web pages. To write Java programs, developers can use Java Server Pages (JSP), which has a scripting language and a structure similar to Active Server Pages. One difference is that a JSP page is compiled into a servlet, which is then run on a server. A **servlet** is a program written in Java and designed to produce Web pages. A skilled programmer can write servlet programs to optimize code and precisely control the behavior of a Web page.

One of the easiest Web development languages to use is PHP, which was originally designed to allow relatively unsophisticated users to create home pages on a Web site. PHP originally meant Personal Home Page, but as its popularity grew and it evolved into a complete programming language, it came to stand for PHP Hypertext Preprocessor. PHP has a structure similar to that of ASP and JSP, and a syntax similar to that of Java.

Macromedia ColdFusion is another popular Web development language that was introduced before ASP. Although ColdFusion is more extensive than the other languages previously mentioned, it offers many features that make producing sophisticated Web pages relatively easy. The ColdFusion syntax is also similar to that of ASP and JSP, so programmers who know those languages can learn ColdFusion quickly.

All Web development programming languages are limited unless they can connect to a database to extract and save data. A **database management system (DBMS)** lets you store and access data on a computer. Relational databases contain data in table form and share a common language called **Structured Query Language (SQL)** that you can use to manipulate the data in the database. Many Web sites employ databases to perform tasks such as storing customer information, producing reports, and displaying

product information. Database management systems range from simple to complex in terms of features and capabilities, and from free to expensive in terms of price.

At the low end of DBMS capabilities is Microsoft Access. It is an appropriate choice for simple Web sites that do not have sophisticated needs.

Microsoft SQL Server is a Microsoft's Enterprise DBMS product. Combining SQL Server and ASP.NET provides a capable system because ASP.NET has code specifically optimized for SQL Server. For example, you can use ASP.NET to extract data from a database to produce a report in HTML. Although many organizations hire a database administrator (DBA) to manage their databases, SQL Server can be often installed without a DBA. In these cases, the Web server administrator may be tasked to install SQL Server and provide security measures while the developers create the databases and tables.

Oracle is another sophisticated DBMS that can be installed on a variety of server platforms, including Windows, UNIX, and Linux. Oracle products are built on a core database and they work with a family of related products such as application servers, e-commerce servers, and e-mail servers. When you install Oracle, it also installs an Apache Web server and associated modules configured to work with the database. Soon after installing the database, developers can test sample JSP pages and servlets to see how they connect to Oracle. Typically a DBA maintains Oracle.

While Access, SQL Server, and Oracle range in price from moderate to expensive, MySQL is a capable DBMS that is freely available. Where SQL Server and Oracle are suitable for large organizations with extensive and specific requirements, MySQL should be considered for smaller environments. The Web server administrator may be tasked to install MySQL and provide some support. Web developers can then provide the rest of the support.

Managing E-mail Servers

E-mail servers are common in many businesses. By design, they are open because users need to send e-mail to anyone and receive e-mail from anyone. The e-mail server generally sends and accepts messages without imposing any security, which can lead to abuse of the e-mail service. For example, most people are annoyed with the volume of spam they receive. Viruses and worms sent through e-mail continue to create problems. All of this unwanted traffic can cause problems for the Web server administrator. In smaller organizations, the Web administrator may also act as the e-mail administrator. Even in larger organizations, the two administrators need to work closely together. In some organizations, the Web administrator provides technical support while someone else performs maintenance tasks such as adding and deleting users to the system.

Working with Other Web Applications

In addition to programming languages, databases, and e-mail services, your Web server might support other applications that you need to manage, including firewall, FTP, and DNS services, depending on the size of your organization. Some organizations choose to have an ISP provide some of these applications, such as DNS, while large organizations often hire specialists to take charge of these applications.

Firewall is a general term for specialized software designed to control access to your Web environment. A firewall helps to control access to your Web environment as well as access from your internal network to the Internet. As Web server administrator, you need detailed information on what type of access the other Web applications need, such as e-mail and Web server software. The firewall makes sure that only the applications you specify can be accessed. Good firewall products help to prevent attacks on the Web environment by malicious hackers, and they can monitor access to and from your Web environment. This

means that you can track how internal users use the Web, which is particularly helpful if internal users are not using the Web for business purposes and slow your connection to the Internet.

FTP is a service that allows users to download files from and upload files to a server; the Web server administrator controls who can download and who can upload files. Many users employ FTP to download software programs, updates, data files, and software patches from Web sites. FTP can operate in two standard modes: anonymous and protected. The anonymous mode does not require a password and lets anyone access files. Protected mode requires a user to enter a user name and password to access files. Because the user name and password are sent as clear (unencrypted) text, hackers can easily find out the user name and password to download sensitive information or upload damaging files that could harm the FTP server. For this reason, it is difficult to make FTP secure.

A **DNS** server translates host names such as *www.technowidgets.com* into an IP address such as 38.246.165.12. DNS can also translate an IP address into a host name. An IP address is the way each computer is identified on a network. (IP addresses are covered in detail in Chapter 2.) The DNS server typically controls the hosts in a single domain. For example, the DNS server in an organization with the domain name technowidgets.com would control hosts such as *www.technowidgets.com*, *mail.technowidgets.com*, and *ftp.technowidgets.com*. A DNS server receives an IP address and responds with a host name; security programs and e-mail programs can take advantage of this feature to determine which host is sending the message. An ISP can readily maintain the DNS server because its information rarely changes.

Managing the Internet Connection

Naturally, the Web administrator needs to maintain a connection with the Internet. When a LAN experiences a problem, the LAN administrator is responsible for checking the wiring and connections. The Web administrator, on the other hand, works with many other administrators or organizations to connect a Web environment to the Internet and then to maintain that connection.

As a Web server administrator, your responsibility ends at your connection to the Internet. From that point, you need to contact your ISP to obtain additional support. Your ISP may have to contact other telecom providers to complete a connection or to solve a problem. In the WAN environment, many organizations are responsible for maintaining connectivity.

You may also need to contact your ISP to change your service. For example, you might want a faster Internet connection or multiple connections for redundancy. However, not all ISPs can offer all services. For example, an ISP that specializes in low-speed connections might not provide high-speed connections. Now that you've examined the differences between server administrators and Web server administrators, you can explore their similarities.

Exploring Administrators' Common Tasks and Services

While server administrators and Web server administrators work in different environments and perform different tasks, they share many types of tasks. In smaller organizations, the server administrator and the Web server administrator might be the same person. Although both administrators maintain security, for example, each takes a different approach to that task—both are interested in security, but security on a LAN can be different from security in a Web server environment.

Installing and Configuring Systems

The Web administrator needs to determine the hardware and software requirements of the environment. This includes not only the servers, but also everything that connects to the servers, such as switches that connect servers and other computers together, and routers that connect the server network with the internal LAN or Internet. Administrators install the operating system and applications on the servers.

For the Web server administrator, installing the operating system is a simple task because the Web server is more isolated than a typical server on a LAN. The more challenging task for the Web server administrator is to determine which other applications the organization needs and then to install them.

Both Web and server administrators need to maintain a correct configuration. Server administrators focus on configuring users and their environment. Web server administrators seek to maintain a correct configuration on a variety of applications. Unfortunately, knowing how to configure one application, such as e-mail, does not necessarily help to configure another application, such as DNS.

Maintaining Security

Everyone is concerned about security. However, an organization should be concerned about more than simply preventing a hacker from attacking its system. Disgruntled and inept employees can do damage, too. As a consequence, administrators need to consider both physical security and software security.

Physical security involves protecting your server environment from others. For example, you should stop outsiders from engaging in malicious behavior and prevent internal users from surfing the Internet and potentially downloading viruses. Some users with technical skills might want to change the server and create difficult-to-resolve problems. External users might try to detect the traffic between your Web server and the Internet.

Just as Web server administrators use firewalls to restrict access to the Web server, so should server administrators restrict access to the server environment. To do so, they can use a Demilitarized Zone (DMZ), a configuration where the servers are isolated from both outside attacks and inside attacks.

Monitoring the System

Systems can be monitored to track performance, troubleshoot problems, and record usage, for example. Server performance reflects the server's ability to perform its duties, such as transmitting Web pages or e-mail messages to users, with minimal delay. Although Web and server administrators have different criteria for adequate performance, their objective is the same. Users should find performance acceptable, while the cost for the performance must make business sense. For the server administrator, traffic typically travels at 100 Mbps in a LAN. For the Web administrator, traffic is often limited to much lower speeds. Both administrators want to keep their users happy. Users accessing Web pages, for example, will not accept significant delays while waiting for the pages to appear in their browsers. What is considered "significant" can vary depending on the environment. If the user constantly accesses a Web-based application that is critical to job performance, he or she may require very quick response times. If the user is ordering seat belts for a classic car, response time is less important.

As an administrator, you may use many methods to monitor your system for troubleshooting purposes. The operating system, whether Windows or Linux, monitors itself and communicates information to you using software tools and log files. Windows uses the Event Viewer to organize log files. Linux also maintains log files and can notify you about them through e-mail. Figure 1-1 shows an example of the Windows Event Viewer. To find out more about each message, you could double-click it.

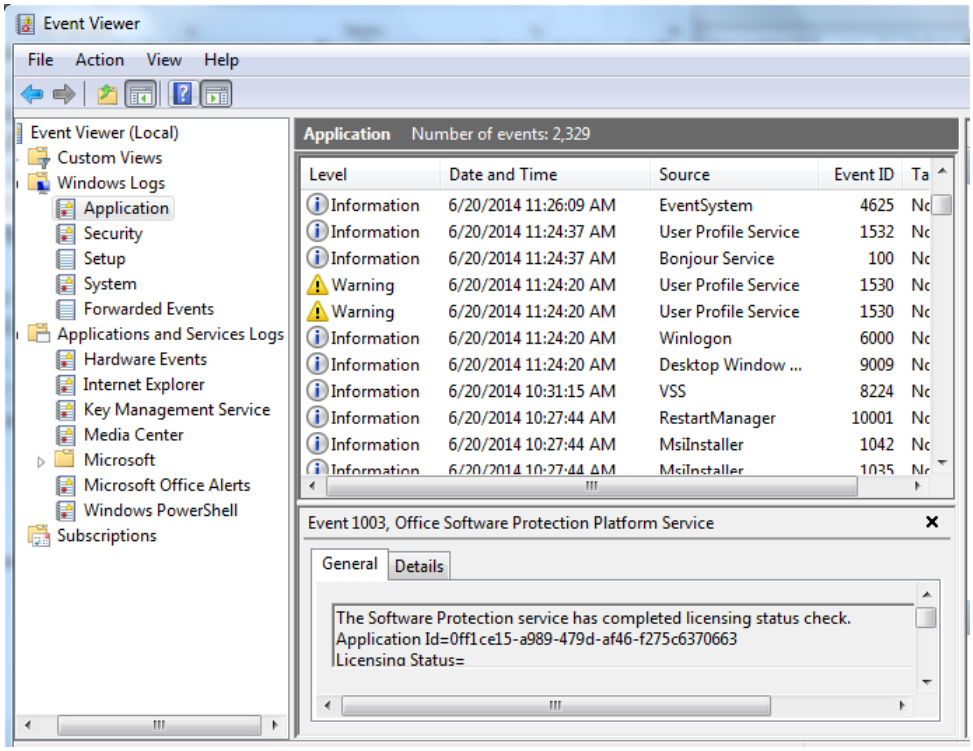


Figure 1-1 Event Viewer

Both Apache and Microsoft Internet Information Server (IIS) Web servers have extensive logging capabilities. Figure 1-2 shows an example of an Apache log file that you can track to see who is accessing what part of your site and how often.

```
10.2.5.3 - - [25/Sep/2002:10:16:52 -0400] "GET / HTTP/1.1" 304 - "-" "Mozilla/4.0"
10.2.5.3 - - [25/Sep/2002:10:16:52 -0400] "GET /icons/apache_pb.gif HTTP/1.1" 304 -
"http://10.11.22.33/" "Mozilla/4.0"
10.2.5.3 - - [25/Sep/2002:10:16:52 -0400] "GET /poweredby.png HTTP/1.1" 304 -
"http://10.11.22.33/" "Mozilla/4.0"
10.2.5.3 - - [25/Sep/2002:10:28:16 -0400] "GET /test.htm HTTP/1.1" 200 31 "-"
"Mozilla/4.0"
10.11.22.33 - - [16/Sep/2002:09:06:43 -0400] "GET / HTTP/1.1" 200 2890 "-" "Mozilla/4.0"
10.11.22.33 - - [16/Sep/2002:09:06:43 -0400] "GET /poweredby.png HTTP/1.1" 200 1154
"http://localhost:55555" "Mozilla/4.0"
10.11.22.33 - - [16/Sep/2002:09:06:43 -0400] "GET /icons/apache_pb.gif HTTP/1.1" 200 2326
"http://localhost:55555" "Mozilla/4.0"
```

Figure 1-2 Apache log file

Because system monitoring takes resources, you must balance the desire to understand certain aspects of your system against the resources required by that effort. Extensive system monitoring may decrease performance to an unacceptable level and quickly fill your hard disk with log files. Windows and Linux also provide software tools that monitor a system by gathering data about system usage or helping to troubleshoot a performance problem. For example, you can use the Windows System Monitor to create a graph that tracks processor usage over time, thereby enabling you to identify programs or resources that consume excessive processing power.

Maintenance and Backup

After you install and configure a computer system, you need to maintain it. For example, you should periodically upgrade your operating system and applications. You might also need to eliminate security holes by installing software patches and enhancements. While these changes usually improve a system, they can occasionally introduce new problems. For example, a patch designed to solve one problem might cause another. An upgrade that has produced no problems in other environments might unexpectedly cause serious problems in your environment. In general, you should plan for the worst and test changes thoroughly in isolation as much as possible before making them on the overall system. For example, schedule maintenance tasks during a slow time on the system, such as late at night, to avoid interrupting services. Because it can be difficult to determine which patches you need, you should monitor the Web sites of the manufacturers of your software to see what they suggest. User groups and e-mail notification can also prove useful.

In addition to performing software maintenance, server administrators typically create and maintain system backups. Backup software stores data from your server on another device such as a tape. You can use the tapes to restore data if someone accidentally overwrites Web pages or realizes that they need files deleted earlier. All the tasks related to backing up data and restoring it can be complex. For example, normally you cannot back up open files, although open files can be the most important ones on your server. Microsoft SQL Server and most other SQL servers keep their data files open so they can't be backed up. Thus, when you buy your backup software, you should either make sure that it can back up open files, such as those associated with SQL Server and Microsoft Exchange Server, or require the database administrator and mail server administrator to do their own backups.

System problems can be so severe that the only solution is to completely reinstall all the software and its associated data. As you set up a new server, you should always test your ability to reinstall software and data, including your operating system, DBMS, mail server, Web server, and other applications. Enter data in all the applications, and then install your backup software and do a complete backup. Format your drive to simulate a catastrophic failure, and then verify that you can restore the system from your backup. Take these steps to confirm that you can recover from a disaster:

1. Install the operating system.
2. Install applications such as the DBMS, e-mail, and others your organization uses, including backup software.
3. Create sample transactions and other data for all the applications.
4. Back up the complete system.
5. Format the hard disk and reinstall the operating system.
6. Reinstall the backup software.
7. Restore the system.
8. Test applications to make sure that the data was restored correctly.

EXAMINING NETWORK BUILDING BLOCKS

Many parts of the network need to work together in harmony. Administrators must understand how these parts fit together so they can determine how to create an efficient and balanced network. For example, you should not buy an extremely fast server when your connection to the Internet is very slow. Administrators must also prevent malicious hackers from penetrating or disrupting the Web environment. Because hackers exploit the basics of the TCP/IP model to do damage, you must understand these basics so you can protect your system.

This chapter provides an overview of networking and telecommunications. Chapter 2 focuses on the addressing part of the networking model. As a Web server administrator, you need to look at the network

as a logical model to understand how computers communicate, and as a physical structure to understand how network components work together. In the following section, you first examine the logical model, and then learn about the components of a LAN and a WAN.

Understanding the OSI Model and the TCP/IP Model

You use the **Open Source Interconnection (OSI)** model and **Transmission Control Protocol/Internet Protocol (TCP/IP)** model to understand network communication. The OSI model defines the building blocks that divide data communications into discrete parts. TCP/IP comprises a suite of protocols that are used in data communication. A **protocol** is a set of communication rules. For example, when you mail a letter, you follow a protocol to correctly address the envelope. In data communications, protocols define the details of how each task is performed.

The objective of the OSI and TCP/IP models is to show the division of tasks needed to communicate on a network. With networking models, each level communicates with its corresponding level at the other end without needing to understand what happens outside that level except to communicate to level(s) adjacent to it.

Examining the OSI Model

The OSI model was designed in the 1970s and implemented in the 1980s to show how networking protocols should function. It consists of seven layers, which separate the complex task of communication into manageable parts. By dividing the tasks into layers, a protocol needs to be concerned only with specific tasks and the way in which it communicates with the layer below and above it. The highest layer describes the link between the computer system and TCP/IP, and the lowest level describes the data as it is either leaving or entering the computer. See Table 1-1.

Table 1-1 OSI model

Layer	Name	Description
7	Application	Responsible for low-level application access to the network. An example of an application that works at this level would be FTP, which transfers files from one computer to another.
6	Presentation	Can convert data into a format that is understandable to the Application layer. Encryption and decryption occur at this layer.
5	Session	Can open communication with another computer, maintain it for a specified period, and then shut down the communication.
4	Transport	Responsible for transporting the data from one computer to another. Protocols at this level include TCP (used for communications between the browser and the Web server) and UDP (used for communication with a DNS server).
3	Network	Primarily responsible for addressing between two computers. It is also responsible for fragmentation and reassembly of packets if the devices through which the packets flow have different capabilities. The IP protocol is at this layer. Another protocol, ICMP, provides error messages.
2	Data Link	Responsible for the interface between the packets coming down through the upper layers and the physical layer. It puts the interface in a data frame that is designed for a specific medium and then sends it on to the Physical layer.
1	Physical	Responsible for transferring the data to the network medium. Ethernet is a common transfer method.

The OSI model is part of the networking vocabulary. For example, a switch is a device that takes data from one computer and sends it to another computer to which it is directly connected. This situation is analogous to sending a package in Phoenix to another place in Phoenix. Such communication takes place at Layer 2 of the OSI model. Other switches are Layer 3 switches, which means that they can work at the Network layer. This situation is analogous to moving the package from Phoenix to San Francisco. By stating that a product is a Layer 3 switch, you should understand that the term refers to Layer 3 of the OSI model and recognize what that entails.

Examining the TCP/IP Model

As opposed to the theoretical OSI model, the TCP/IP model is a real-world model based on how TCP/IP actually works. The TCP/IP model doesn't correspond exactly with the more common OSI model, as Table 1-2 shows. Actually TCP not only performs the tasks at the Transport level of the OSI model, but also handles some of the tasks at the Session level of the OSI model. The first three layers constitute the TCP/IP protocol suite.

Table 1-2 TCP/IP model

Layer	Common components	OSI reference layer
Application	HTTP, SMTP, POP3, FTP, DNS	Application Presentation Session
Transport	TCP, UDP	Transport
Network	IP, ICMP	Network
Physical	Ethernet, FDDI	Data Link Physical

Because the OSI model is a general-purpose model, you can use it to better understand other protocols. Most of the protocols will be explained in depth in the following chapters. For now, understand that the protocols provide the rules to make sure that all TCP/IP systems can interoperate. They need to interoperate both the application level and the lower level data communication layers. The following list briefly describes the main protocols:

- *Hypertext Transfer Protocol (HTTP)*—Web servers implement this protocol, which allows you to request a Web page or send a completed form to a Web server for processing. Examples include IIS and Apache.
- *Simple Mail Transfer Protocol (SMTP)*—E-mail servers implement this protocol, which allows you to send mail to another e-mail server.
- *Post Office Protocol Version 3 (POP3)*—E-mail servers implement this protocol, which allows users to retrieve mail from an e-mail server.
- *File Transfer Protocol (FTP)*—FTP servers implement this protocol, which is used to transfer files to and from a server. Both Windows and Linux have FTP servers that are included with the operating system.
- *Domain Name Service (DNS)*—DNS servers implement this protocol to translate names into IP addresses and IP addresses into names. For example, when you type *www.technowidgets.com* into a browser, a DNS server must first translate that name into an IP address before the request can be sent to the Web server. Berkeley Internet Name Domain (BIND) is the most popular program used to implement DNS. Microsoft also has a DNS server.

- *Transmission Control Protocol (TCP)*—This protocol creates a reliable connection between two computers. TCP is used as a primary means of communication by HTTP, SMTP, POP3, and FTP.
- *User Datagram Protocol (UDP)*—This protocol does not establish a connection between two computers as TCP does, but simply sends a message. This ability makes it a good protocol for sending short, discrete messages, such as requesting the IP address for *www.microsoft.com* from a DNS server. UDP relies on the application that implements it to make sure that the message gets to its destination.
- *Internet Protocol (IP)*—This protocol provides an addressing scheme so that it can determine whether the data packet should be sent to a computer that is physically connected on the same network or to another computer that can route it to the destination computer. It can also provide fragmentation and re-assembly of data. (See Chapter 2 for more information about IP and addressing.)
- *Internet Control Message Protocol (ICMP)*—This protocol provides error messages. When you use the ping utility and it returns an error, it is from ICMP.

Now that you have learned about the networking building blocks, you need to see how the components in a network come together to transfer the data from one computer to another.

Identifying Network Components

To design an appropriate Web environment for the needs of your organization, you must first understand the common network components. The overall design needs to be balanced so that a bottleneck will not cause problems with the rest of the network. In a Web server environment, data must travel between your Web server and the user's computer. This section discusses the common components you need to consider when designing a Web network environment. After considering the specifics of the network configuration, you must evaluate the performance of the network and determine its capacity. You also need to determine how to measure network performance.

Identifying Common LAN Components

Recall that a LAN is a network that spans a relatively small geographic area, such as an office, a single floor in a building, an entire building, or even multiple buildings in an office park or campus .The most common network technology in use today is **Ethernet**, which connects multiple devices, such as PCs and printers, on a LAN. With Ethernet, these devices can send information across the cables that connect them, thereby passing information from one device to another. Figure 1-4 diagrams a simple LAN.

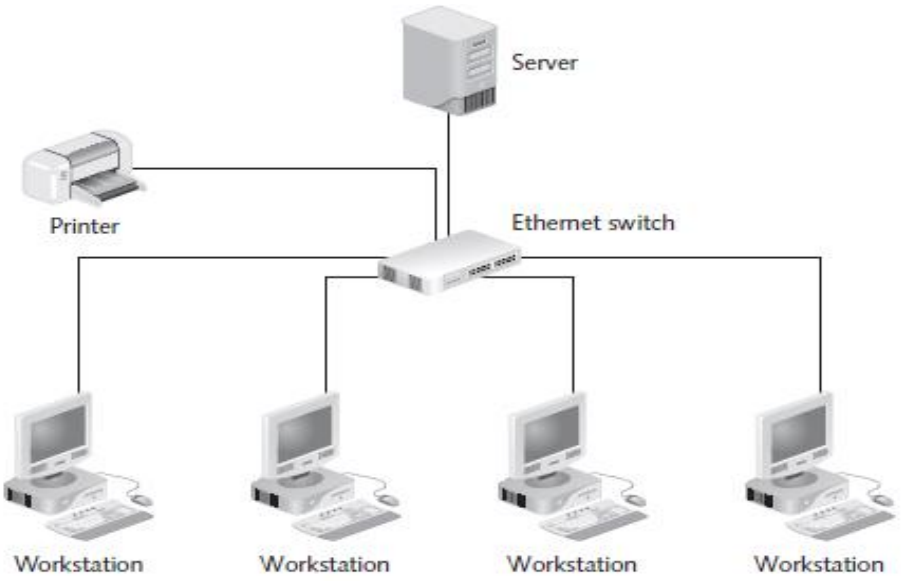


Figure 1-4 Simple network diagram

Note the Ethernet switch shown in Figure 1-4. A **switch** is a central device that allows PCs to communicate with one another. A data cable connects the NIC of each computer to the switch. Ethernet switches work at several speeds. Standard Ethernet communicates at 10 Mbps, but other Ethernet speeds include 100 Mbps and 1 Gbps. Switches operating at a speed of 100 Mbps are the most common today.

Whatever configuration your network uses, the server should have a higher connection speed than the workstations that are accessing it, because the server is a central resource. For example, suppose you have a network of 100 workstations and one server, all connected at 10 Mbps. If all 100 of those workstations wanted to access the server at the same time, they would overload the connection to the server. Even if the server had enough processing power to supply the data, its connection speed would allow it to send data only at 10 Mbps to the network, so the data would take longer to travel to each workstation. Although that number of workstations could technically overload a server even if it had a 100 Mbps connection, normally traffic is not so sustained that a 100 Mbps connection could not manage it. For this reason, it is common practice to connect servers at 100 Mbps, 1 Gbps, or even higher rates.

Your connection speed to the Internet is even more critical. The typical connection speed is merely a fraction of the speed possible with standard Ethernet. You want to make sure that your users and your Web server exchange data in an acceptable amount of time but minimize the cost of your Internet connection by purchasing only what you need in terms of the speed of your connection.

Connecting Your LAN to the Internet

A WAN is a telecommunications network operating over an area that can span a few miles or reach another country. Whereas you control the cabling in a LAN, the WAN is typically a shared, public network. You connect your LAN to a WAN that is connected to your ISP, and your ISP provides the connection to the Internet. In essence, a WAN is a network that begins where the connection at your building ends. Although your focus in using the WAN is to connect to the Internet, you could also use the WAN to connect your main office to your branch office.

A common method of connecting to a WAN from a business is through a T1 line, which is a digital connection that is used only for data and voice transmission. Alternatively, you could use other types of T-Carrier WAN connections, as listed in Table 1-3. You will learn about other WAN connection options shortly, but for now note these T-Carriers are the most common building blocks for WANs. Many other connection types exist as well, including ISDN, DSL, and cable modems.

When deciding which connection to use, you must consider your organization's overall needs for speed and cost. For instance, a small company with a small Web server could use a fractional T1 but a larger company with a much busier Web server might require multiple T1s.

Table 1-3 Common T-Carrier connections

Connection type	Speed	Description
Fractional T1	64 Kbps increments up to T1	Used when you do not need a full T1 connection. A T1 connection is divided into 24 channels, and one channel is 64 Kbps.
T1	1.544 Mbps	T1 is the most common digital leased-line service. Each channel in a T1 circuit can carry voice or data transmissions, and you can combine multiple T1s to provide additional speed.
T3	44.736 Mbps	T3 is equivalent to 28 T1 circuits. Its speed is often rounded and referred to as 45 Mbps. Like fractional T1s, fractional T3s allow customers to lease less than the full T3 rate.

The appropriate connection speed for your Web server is difficult to gauge accurately. Ask the following questions to determine the speed you need:

- How much data will a typical user request?
- How many users will access your Web server simultaneously?
- How many pages will the typical user view?
- What is the typical user's tolerance for delay?
- Will the access be spread throughout the day or will it be focused on a few hours in a day?
- How long will it take for the estimated number of users to double? A month? A year?
- What is the average size of your Web page?
- How will the average size of your Web page increase over the next year as you incorporate more graphics? (This factor could easily increase the average size of your Web pages by five or ten times.)
- If your Web server shares its connection with users in your organization who need a connection to the Internet, how will their needs change over time?

Selecting a connection type and determining the optimal connection speed are more of an art than a science for a company connecting its Web server to the Internet for the first time. The main thing to consider is the need for future growth.

Connecting Your Network to a WAN Using a T-Carrier Line

You use a few standard components when you connect your network to a WAN using any T-Carrier line, whether fractional T1, full T1, or T3. Even though T1 and Ethernet networks are digital, they send data in very different ways. You need certain components to translate the digital format of the data arriving via a T1 line to the digital format that is acceptable to your LAN. In an organization where users share the connection to the Internet, your Web server will share the network with users. Although Figure 1-5 shows one way to connect these devices, technology has advanced to the point that you can connect to the Internet many ways.

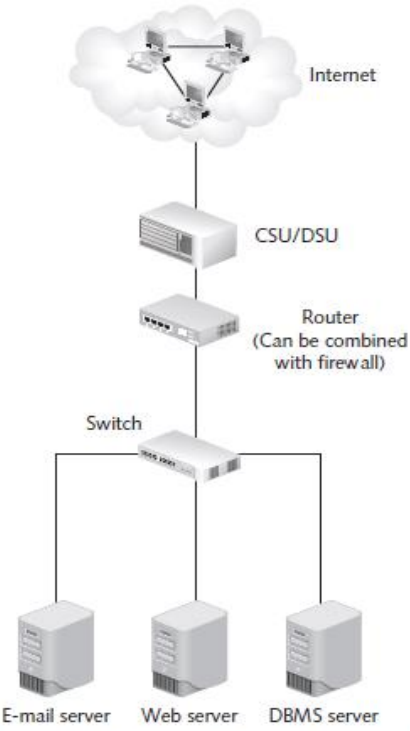


Figure 1-5 Network diagram showing T1 WAN components

The following list describes the typical components in a connection to a T-Carrier WAN line:

- *Channel Service Unit/Data Service Unit (CSU/DSU*)—This unit really includes two devices in one. The CSU portion is on the WAN side and serves two purposes: It transmits and receives the digital signal, and it provides an electrical buffer from either side of the device. The DSU translates between the digital signal on the T1 side and the serial connection on the LAN side.
- *Multiplexor*—This optional component provides a mechanism to load multiple voice and data channels into a single digital line. This strategy could be used in a case where you want to split your T1 line into two parts and then carry data across one part and phone traffic across the other part. A multiplexor is not required.
- *Router*—Although routers can serve a variety of functions, the router used to connect a T1 line to a WAN is specialized. A serial connection provides communication with the CSU/DSU or multiplexor. That connection routes to one or more Ethernet ports. The Ethernet port, in turn, provides the connection to your LAN. More details about routing are in the "IP Addressing" section of Chapter 2.

It is easiest to think of the CSU/DSU as being a kind of digital modem. Just as a modem provides an interface between the telephone line and your computer, so the CSU/DSU provides the same interface for your LAN. Likewise, a modem provides a serial connection to your computer just as a CSU/DSU device provides a serial connection to your LAN.

Using an Integrated Services Digital Network Connection

An integrated services digital network (ISDN) connection offers a digital service capable of carrying voice, video, or data communications. Although it was defined in 1984, ISDN connections became popular only in the 1990s as compatibility problems eased. ISDN still supports legacy applications where users need a private connection to a company network to telecommute. ISDN may also be used as a backup when the main line malfunctions. It is a dial-up service: You must dial a number to reach the system that accepts the ISDN connection and connect to the local telephone service. However, because ISDN is a digital service, it can provide higher capacity across the phone system's wires. ISDN lines connect to the LAN via a **terminal adapter (TA)**, sometimes referred to as an ISDN modem.

ISDN offers two service types:

- *Basic Rate Interface (BRI)*—This service provides three channels of data transfer. Two channels carry up to 64 Kbps of data and are referred to as "B" or "bearer" channels. The third channel carries data at a speed of 16 Kbps and is referred to as a "D" or "delta" channel. In a typical BRI connection, the two B channels transmit the data and the D channel manages the link.
- *Primary Rate Interface (PRI)*—This type of service provides a significantly higher amount of bandwidth and divides the equivalent of a T1 line into 24 channels. PRI uses 23 B channels, each capable of carrying data at 64 Kbps, and one 64 Kbps D channel to manage the link.

The BRI provides data transfers at a speed of 128 Kbps, which may be appropriate for a user to connect to a private company network, but probably is not adequate for a typical Web server. The PRI channels use a T1 line with the capacity of 1.544 Mbps.

Using a Digital Subscriber Line

As with ISDN, a **digital subscriber line (DSL)** allows you to transfer data at high speeds over conventional telephone lines. Many types of DSL connections are available, and they are characterized by their download and upload speeds. Download speed measures how fast you can transfer data from a server such as a Web page or a file, while upload speed indicates how fast you can send data to the server such as a Web page request or an e-mail message with attachments. Typically, download speeds are more important than upload speeds for users.

You can use the information in the preceding list to determine which types of DSL are appropriate for a home user and which are appropriate for a business user with a Web server. A Web server receives very small packets of data requesting Web pages. The Web server responds to each request by transmitting a relatively large Web page. The Web server needs more upload speed than download speed. Conversely the typical Web client user needs faster download speed than upload speed. Asynchronous DSL (ADSL) is therefore more appropriate for a Web client user. Download is often referred to as "downstream," and upload is often referred to as "upstream." The Web site *www.dslreports.com* is a good resource for information about DSL service and its providers.

One limitation of all varieties of DSL is **signal degradation**, although this concept is not unique to DSL. (ISDN is also particularly susceptible to signal degradation.) Signal degradation involves the loss of signal strength as the signal moves farther from the source. To use DSL, you must be located within a certain distance of a telephone switch to avoid signal degradation. The distances vary, but with some versions of DSL a client must be located within 3,000 meters of a switch. Some DSL variants allow distances of up to 8,000 meters. Generally, the DSL provider will conduct a line test to determine whether a business or home telephone line can handle a DSL connection. Telecommunication technology has advanced to the point that most business and home users can get DSL. Figure 1-6 shows a typical way to connect to the Internet using DSL.

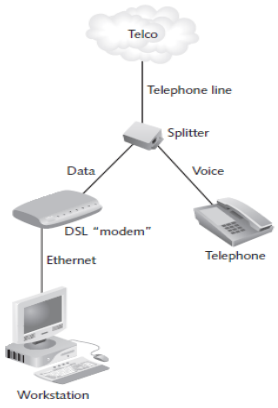


Figure 1-6 DSL connection

Using Cable Modems

Although cable modems are designed for the home user market, they are used in business as well. Like DSL, cable modems allow a wide range of communication speeds and often have different upstream and downstream speeds. Unlike DSL, cable modems do not use standard phone lines, but transmit a signal along the same line as your cable TV. See Figure 1-7.

Cable modems typically share access, which means that everyone receiving cable service from the same provider in the same area or neighborhood competes for the amount of capacity available. (Standard Ethernet operates in the same way.) This shared access won't be a problem if your service provider expands its service as it adds new users. Unlike with T-Carrier, ISDN, and DSL connections, however, the performance of cable modem connections can degrade significantly over time. You should therefore

make sure to work out a quality-of-service agreement with your cable provider that guarantees a certain level of performance.

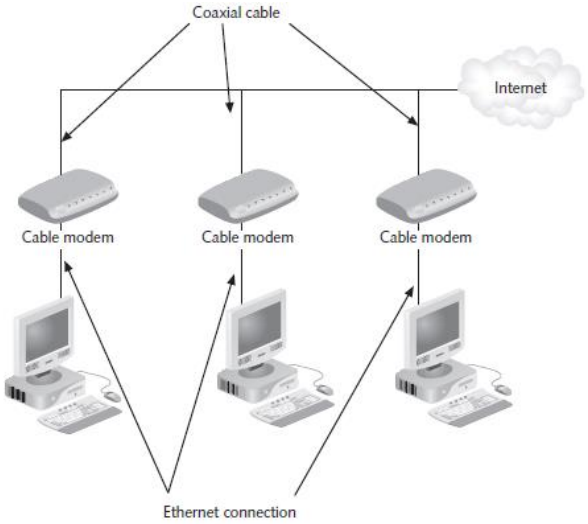


Figure 1-7 Cable modems share a connection to Internet

Much of the previous discussion focused on the speed of connections using a variety of technologies. Because this consideration is so important, you need a deeper understanding of how speed applies to connecting a Web server to the Internet.

Understanding Bandwidth and Throughput

Although **bandwidth** technically means the width of a band of frequencies, it is expressed in bits per second (bps)—that is, the theoretical maximum amount of bits that can be sent in a second. The speed estimates in the previous section were calculated in terms of their bandwidth. Another factor that affects the actual speed is **throughput**, which is the amount of data you can move from one place to another in a given time period. A pipe carrying water is a common analogy for bandwidth and throughput. In this case, the bandwidth is the total capacity of the pipe; the throughput is the amount of water flowing through the pipe in a certain amount of time. Both bandwidth and throughput are typically measured in units of bits per second: kilobits, megabits, or gigabits, as appropriate. Mbps and Gbps are typically used when specifying the speeds of the network.

Be sure to distinguish between measurements in bits (e.g., Mbps) and those in bytes (e.g., MBps). Measures relating to speed are usually expressed in bits per second when describing data transfer speeds for networks, whereas data transfer rates within a computer such as hard drive transfers are often expressed in bytes per second. There are eight bits in one byte, so 1 MBps is eight times faster than 1 Mbps.

Throughput as a percentage of bandwidth is a useful measure of how much data you can expect to transfer between your Web server and the user. This “bandwidth utilization” rate tells you how much of the bandwidth you are actually using. Keeping track of your utilization patterns allows you to plan for future growth. For instance, the bandwidth of a typical Internet connection is 1.544 Mbps. If you have an average throughput of 768 Kbps (meaning that 768 Kbps of a potential 1.544 Mbps of data is passing through the network), then your network has a utilization of approximately 50 percent. This bandwidth utilization rate is desirable because it shows that you are not overloading your connection. It is important to keep track of the utilization rate during times that your users are most often connecting to your server.

It can be misleading to analyze throughput over a 24-hour period if most of your traffic occurs in a 4-hour time span during the day. If your bandwidth utilization typically remains under 80 percent, your users should be able to display pages without too much of a delay. If the demand for Web pages exceeds these levels, your users will have to wait longer to see each page.

Your ISP can often provide you with software to monitor your throughput so that you can determine when your network experiences the heaviest traffic. You also need to realize that you can never reach 100 percent utilization. A difficult task when trying to select the ISP that will provide your Internet connection is finding out what the average throughput will be. Just because all the companies you are considering offer the same connection speed, it does not mean that your maximum throughput will be the same in all cases. Some ISPs sell more bandwidth than they can support.

The puzzle of identifying LAN components and connecting the LAN to the WAN has many pieces. The most complex piece is learning about the WAN connection. Because the ISP industry is highly competitive, pricing and services change rapidly. What is the most popular and cost-effective solution one year may not be as popular the next year. You can select between T1, SDSL, and a dedicated cable modem. Which option you choose depends on the combination of services that is available in your area.

For many organizations, setting up a Web environment on their own premises is not appropriate. These businesses may choose instead to have another business host their Web sites.

Understanding Web Hosting Solutions

Web hosting offers an alternative to setting up your own Web server environment. There are many types of Web hosting services to fit every budget. Web hosting can be a viable solution if you do not currently have the in house expertise necessary to install, configure, and maintain your own Web environment.

Having another company host your Web site offers some significant advantages. When you let another company host your Web site, you do only the Web site development. The Web hosting company can even help you register your domain name and supply e-mail for you. You do not have to worry about bandwidth, because the Web hosting company should have enough bandwidth for your Web site. The Web hosting company is also responsible for keeping you connected to the Internet and typically has technical support personnel available 24 hours a day to ensure connectivity. It can offer many services that you can add as you grow.

The following list includes some common types of Web hosting services:

- *Standard hosting*—Your site resides on the same computer with many other sites. This option is the cheapest solution, but your response times may vary depending on the popularity of the other sites. You will probably use FTP to upload and download pages. Standard hosting is similar to having a Web site like the one that is typically available when you sign up for a home connection.
- *Dedicated server*—You have a server that only you use. There are a variety of sizes from which to choose, so you get only the type of computer that you need.
- *Co-location*—Your own server is physically located at the company that does your Web hosting. The firm is responsible for maintaining the connection to the WAN, and you are responsible for configuring the software on the server. Co-location makes it easier to take the final step of moving the Web server to your own environment because the hosting company supplies only the connection.

Although Web hosting seems like an easy and straightforward solution, consider the problems it can present. Always remember that you are putting a system with significant importance to your organization in the hands of someone else. What happens if the Web hosting company suddenly goes out of business?

Also, if you want to create dynamic pages, what programming language do you use? Not all Web hosting companies offer the same languages, and some languages might cost more than others. What kind of DBMS can you use? Will Microsoft Access be sufficient? Will you need Microsoft SQL Server? Will you require a server just for your own use, or can you share it with one or more organizations? How will you get your data and Web pages to and from the server? How much traffic can you expect on your Web site? The more traffic you get, the more you will have to pay. Be sure to find answers to these types of questions before contracting with a Web hosting company.

A Web hosting company can also provide the following services:

- Help in registering your domain name—it probably has access to the two DNS servers required when you register the domain name
- E-mail setup for you and other members of your organization
- Templates to facilitate Web site development
- E-commerce services, including shopping carts and credit card processing

Web hosting solutions are an important option to consider for an organization that seeks to create a Web presence. They can be a cost-effective method to get started on the Web.

COMPARING WEB SERVER PLATFORMS

One of your major decisions as a Web server administrator is to select a computing platform for your Web server, a decision that usually involves choosing between Microsoft Windows or Linux operating system. Each platform has its strengths and weaknesses. In addition, you need to select which version of the platform you want to run. You would have to consider: cost, hardware compatibility, technical expertise, development environments and interoperability with enterprise applications. Windows Server 2012 is the sixth release of Windows Server. It is considered the server version of Windows 8 and shares the same Metro-based interface. Linux comes in many different versions and distributions. In this class we use Ubuntu which is a Debian derivative. It is a popular choice for Web Servers and includes programs such as Libre Office.

Microsoft Windows Server 2012 R2 - https://en.wikipedia.org/wiki/Windows_Server_2012

Windows Server is a good choice for a Web Server because it extends the Web-based application model by putting the Internet and all the related software at the center of the operating system.

Windows Server 2012 Features

Some significant Windows Server 2012 features include:

- **User Interface** – in addition to the metro-based interface, Microsoft has extended Windows PowerShell to include 2300 commandlets.

- **IPAM** – IP Address Management of Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers including both IPv4 and IPv6.

- **Hyper-V** – enhancements to Microsoft's Virtualization platform including network virtualization and cloud backup.

- **ReFS** - Resilient File System (ReFS) which is a new file system in Windows Server 2012 succeeding NTFS

- **Active Directory Domain Services (ADDS)**.You can use ADDS to support a much larger network with many more aspects to configure. ADDS provides a single point of management for Windows resources in very large network environments. This capability simplifies the management process and allows for a much higher level of scalability. Network resources including users and groups can be tracked. Domains can be broken down into organizational units (OUs). See Figure 1-8.

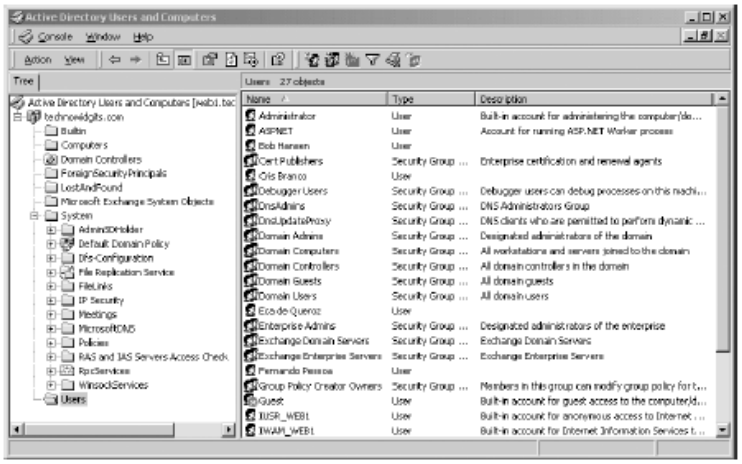


Figure 1-8 ADS computers and users

- Windows requires product activation. To use the product beyond a specified number of days, it must be activated with a special code from Microsoft. This requirement ensures that each server product purchased will be used on only a single computer.

- The .NET Framework is central to the .NET Web environment. This programming model allows sophisticated programs to be developed for use on the Web. One important aspect of .NET Framework is its use of XML, which basically turns data into text that can easily be transmitted from computer to computer. Instead of allowing users to connect to Web servers to view pages, computers can contact other computers to transfer purchase orders or a variety of other information. Because XML and its associated technologies have industry support, servers with different operating systems can communicate readily. ASP.Net is Microsoft's premiere Web Site development product.

UNIX/Linux

UNIX was introduced in 1969 and continues to evolve today. Many variations of the UNIX operating system have been introduced, and these multiuser operating systems are employed as network operating systems by most non-PC networks today. UNIX was the first open operating system.

UNIX consists of a kernel, a file system, and a shell. The **kernel** is a central high-security portion of the operating system that contains its core elements. By isolating the kernel from other applications so that computer processes or users cannot modify the core code and interrupt services, UNIX provides a stable platform. The **file system** provides the input and output mechanisms for the operating system. The **shell** provides the user interface to UNIX. Because UNIX uses more than 600 commands, graphical user interfaces (GUIs) were developed to simplify its operations. Even so, most UNIX administrators still perform a significant amount of their work at the command line.

Linux was developed separately from these other versions of UNIX. It is an operating system written to appear and act like UNIX. Linus Torvalds began his work on Linux in 1991, basing it on Minix. Because the source code is freely available, Linux has been successfully enhanced and supported by a number of organizations. For a complete listing of organizations that distribute their versions of Linux, see *www.linux.org*.

While each distribution of Linux has different strengths and weaknesses, all of them share several elements. Each Linux distribution is built on the same Linux core code and distributed under the **GNU General Public License**, which states that while companies can charge a fee for their customized versions of the core Linux code, they need to make the source code available. As a consequence, you can typically obtain the Linux distribution for a low price or for free. Companies that distribute the Linux code raise revenues by selling support for their software products. Linux's popularity has also been helped by ongoing announcements of support from large companies such as IBM and Oracle.

Linux has been gaining popularity for a number of other reasons other than its low cost. For one, it is very stable and is easier to make secure than a Windows server. Stability is important because you rely on your server to keep functioning correctly. You do not want it to stop running, nor do you want parts of the system to malfunction.

Noteworthy Debian/Ubuntu features - **https://en.wikipedia.org/wiki/Debian_Linux**

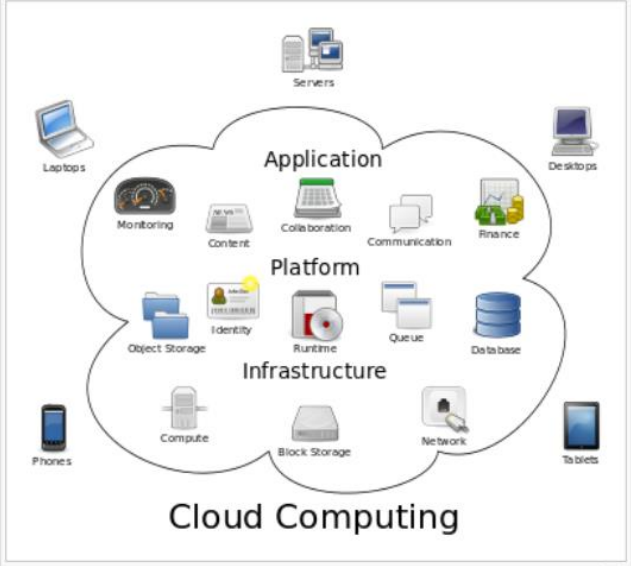
- Integrated package/dependency management system (apt) which simplifies server setups
- Over 30,000 packages currently available in the main repository
- A GUI that scales well on servers, laptops and tablets
- Availability of commercial support and a wide range of hardware is supported
- Long-term support releases every two years
- Supported as a virtual guest in VMWare and Citrix hypervisors – as you will see when you use VMWare's simple install of Ubuntu

Importance of Virtualization - https://en.wikipedia.org/wiki/Virtualization

Hardware virtualization or platform virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. You will build web servers on virtual machine versions of Windows Server and Ubuntu in this class. Some importance virtualization concepts:

- Dedicated servers are being replaced by virtual machines
- Significant cost savings are realized through server consolidation
- Electricity and cooling costs are reduced with fewer servers
- Server deployments and backups are easier
- High availability is possible through clustering
- CPU/RAM efficiencies are realized through scheduling and de-duplication
- Disk efficiencies are realized through thin-provisioning

Importance of Cloud Hosting - https://en.wikipedia.org/wiki/Cloud_hosting



Cloud computing metaphor: For a user, the network elements representing the provider-rendered services are invisible, as if obscured by a cloud.

Key concepts:

- Reduces need for on-site hardware resources
- Increases service availability compared to on-premise hosting
- Reduces costs through tiered pricing and pay-for-what-you-use contracts

CHAPTER SUMMARY

❒ Server administration involves managing local users and their access to network resources. The focus of the server administrator is within the organization.
❒ Web server administration involves managing the many applications that make up the Web environment. It can encompass managing not only the Web server, but also an e-mail server, FTP server, and others.
❒ Both server administrators and Web server administrators have to install, configure, and maintain their servers. They have to make sure that if data is lost on their servers, they can retrieve it. Security is always important, even though they may use different techniques to ensure security.
❒ Many pieces make up a network, and they must all work together. A Web server administrator must understand both the physical aspects of the network and the underlying logical aspects. Without this knowledge, problems that require a simple solution could seem baffling.
❒ There are many Web server platforms from which to choose. All have their strengths and weaknesses, and all are constantly evolving. As a Web server administrator, you should understand as much as possible about all the platforms. Review the Windows Server 2012 and Ubuntu feature lists.
❒ The Internet is a network of networks that is not controlled by a single organization. The cooperation of many entities, both governmental and private, ensures that it continues to function. Although it is amazing that the Internet works so well, it can also prove frustrating to a Web administrator who cannot find exactly who is to blame when an e-mail message does not reach its destination.
❒ Virtualization and Cloud Hosting both offer cost efficiencies

Hands On Projects – Chapter 1

For each question, record your answers or provide screenshots as requested. Format your text in **bold** or colored text.

1.1 Visit http://distrowatch.com/dwres.php?resource=major and find the list of Linux distributions. Choose three and briefly describe how they differentiate themselves. Which on would you choose for a Web Server and why? (3 points).

1.2 Complete the comparison matrix of Internet Service Providers available at your home address. Include at least three providers. Indicate which provider you use & why. (3 points).

		Internet	***Service***	***Providers***	
Provider	Download	Upload	Latency	DataCaps	Price
1.					
2.					
3.					

1.3 The purpose of tracert (trace route) is to display the names of router hops between two computers. Run tracert from the CMD prompt and insert a screenshot of the routers between your computer and www.google.com. Download a free graphical trace route program and repeat the exercise. Insert a screenshot below. (3 points).

1.4 We will use the standard edition of Windows Server 2012 R2. Refer to the hyperlink and Windows Server 2012 R2 Products & Features table below to answer these questions: (3 points).

- What are the editions that Microsoft is offering and what are their intended use?
- What is the maximum RAM addressable with the Standard edition?
- We're installing Domain Name Services in Chapter 3, Web Server in Chapter 6, and SQL Server in Chapter 7. Which Server Roles will we use?

http://www.techrepublic.com/blog/data-center/microsoft-announces-four-windows-server-2012-editions-what-you-need-to-know/

Windows Server® 2012 R2 Products and Editions

	Windows Server 2012 R2 Datacenter	Windows Server 2012 R2 Standard	Windows Server 2012 R2 Essentials	Windows Server 2012 R2 Foundation	Microsoft Hyper-V	Storage Server Standard	Storage Server Workgroup
Locks and Limits							
Maximum number of users	based on licenses	based on licenses	25	15	unlimited	unlimited	50
Maximum SMB Connections	16,777,216	16,777,216	16777216	30	16,777,216	16,777,216	250
Maximum RRAS Connections	unlimited	unlimited	50	50	250	50	50
Maximum IAS Connections	2,147,483,647	2,147,483,647	50	10	50	50	50
Maximum number of 64-bit sockets	64	64	2	1	64	64	1
Maximum RAM	4 TB	4 TB	64 GB	32 GB	4 TB	4 TB	32 GB
Server can join a domain	Yes	Yes	For migration only	For migration only	Yes	Yes	Yes
DirectAccess	Yes	Yes	See documentation	Yes	No	Yes	Yes
Server Roles							
Active Directory® Certificate Services	Yes	Yes	Yes	Yes	No	No	No
Active Directory Domain Services	Yes	Yes	Required	Yes (optional)	No	No	No
Active Directory Federation Services	Yes	Yes	Yes	Yes	No	No	No
AD Lightweight Directory Services	Yes	Yes	No	Yes	No	Yes	Yes
AD Rights Management Services	Yes	Yes	Yes	Yes	No	No	No
Application Server	Yes	Yes	Yes	Yes	No	No	No
DHCP Server	Yes	Yes	Yes	Yes	No	Yes	No
DNS Server	Yes	Yes	Yes	Yes	No	Yes	No
Fax Server	Yes	Yes	Yes	Yes	No	No	No
File Services	Yes	Yes	Yes	Yes	Limited features	Yes	Yes
Hyper-V	Yes	Yes	No	No	Yes	Yes	No
Network Policy and Access Services	Yes	Yes	Yes	Yes	No	No	No
Print and Document Services	Yes	Yes	Yes	Yes	No	Yes	Yes
Remote Access	Yes	Yes	Yes	Yes	No	No	No
Terminal Services Application Sharing	Yes	Yes	No	Yes	No	No	No
Terminal Services Gateway	Yes	Yes	No	See documentation	No	No	No
Web Services (IIS)	Yes	Yes	Yes	Yes	No	Yes	Yes
Windows Deployment Services	Yes	Yes	Yes	Yes	No	No	No
Windows Essentials	Yes	Yes	Default	No	No	No	No
Windows Media Services support (Streaming Media Services)	See Installation Options documentation	See Installation Options documentation	Yes	See Installation Options documentation	No	No	No
WINS Server	Yes	Yes	Yes	Yes	No	Yes	No
Features							
RODC – read only domain controller	Yes	Yes	No	No	No	No	No
Automatic Virtual Machine Activation	Both guest and host	As guest	As guest	No	No	No	No
Best Practices Analyzer	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BranchCache Hosted Server	Yes	Yes	Yes	Yes	No	Yes	No
BranchCache P2P Cache	Yes	Yes	Yes	Yes	No	Yes	Yes
Windows Control Panel	Yes	Yes	Yes	Yes	No	Yes	Yes
Distributed File System Replication	Yes	Yes	Yes	Yes	No	Yes	Yes
Data Deduplication	Yes	Yes	No	No	No	Yes	No
ISCSI target support	Yes	Yes	Yes	Yes	No	Yes	Yes
DirectAccess	Yes	Yes	Yes	Yes	No	Yes	Yes
Dynamic Memory (in virtualization)	Yes	Yes	Yes	No	No	Yes	No
Failover Clustering	Yes	Yes	No	No	Yes	Yes	No
"Hot" add/replace RAM	Yes	Yes	Yes	No	Yes	Yes	Yes
IPAM (IP Address Management)	Yes	Yes	Yes	Yes	No	Yes	Yes
Microsoft Management Console	Yes	Yes	Yes	Yes	Remote only	Yes	Yes
Minimal Server Interface	Yes	Yes	No	No	No	Yes	Yes
Network Load Balancing	Yes	Yes	Yes	Yes	No	Yes	Yes
Support for Non-volatile Memory Express	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows PowerShell	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Server Core mode	Yes	Yes	No	No	Yes--the only option	after setup	after setup
Server license logging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Server Manager	Yes	Yes	Yes	Yes	From a remote computer	Yes	Yes
SMB Direct and SMB over RDMA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Storage Management Service	Yes	Yes	Yes	Yes	Basic file server only	Yes	Yes
Storage Spaces	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Volume Activation Services	Yes	Yes	No	No	No	No	No
VSS (Volume Shadow Copy Service) integration	Yes	Yes	Yes	Yes	No	Yes	Yes
Windows Server Update Services	Yes	Yes	Yes	No	No	No	No

Go to D2L **Discussions** to respond to Ch 1 Technical Tips.

Go to D2L **Quizzes** to complete the Ch1 Review Questions. You are allowed three attempts at the chapter review questions. Your score will be the average of all three attempts.

Supplemental References:

No Web Server Administration course is complete without an introduction to the Father of HTTP, Tim Berners-Lee. See the links below:

https://www.youtube.com/watch?v=yF5-6AcohQw

https://en.wikipedia.org/wiki/Tim_berners_lee