**CHAPTER 3**

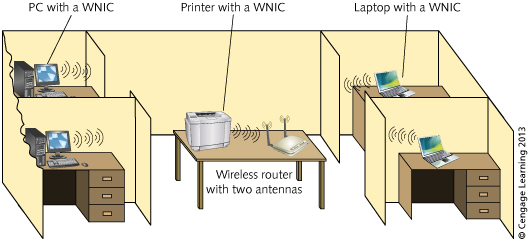
**SHARING RESOURCES ON A NETWORK**

**Learning Objectives:**

1. Explain how to use peer-to-peer networking in a home or office.
2. Configure user accounts.
3. Explain virtual private networks.
4. Explain storage area networks.

**DISCUSSION PROPER**

**What is Peer-to-Peer Networking?**

The peer-to-peer network is one of the easiest ways to configure a network, often used for home offices and small businesses. Workstations are used on a peer-to-peer network to share resources, such as files and printers, and to connect resources to other computers.

**Figure 3-1 A simple peer-to-peer network in a small office.**

Files, folders, software, printers, and peripherals on one computer can be shared and made available to others. No special host computer, such as a server, is needed to allow workstations to communicate and share resources, although in some cases the server can be used as a powerful workstation. Figure 3-1 above shows a peer-to-peer network.

**Peer-to-Peer Networking for Home Use**

Many people have set up a peer-to-peer network for home use. Even if your home has only two computers, a peer-to-peer network can make sense of sharing a printer, an Internet connection, and a file. If you have more computers in your home, the network makes even more sense for the same reasons plus others, such as keeping backup copies of financial files on two computers.

**Peer-to-Peer Networking for Office Use**

Peer-to-peer networking can make sense for a small office for many of the same reasons as home-based sharing of resources. Also, peer-to-peer networking can be valuable in a small office to help make users more productive, enabling them to share information without having to walk from one desk to another to exchange an external drive or flash drive.

**Configuring User Accounts**

Most operating systems, including Windows, UNIX/Linux and Mac OS X Systems, manage access to shared resources through user accounts. A computer user account could be compared to a bank account. A bank is a repository of resources that can be accessed through bank accounts. It is the number and security of the account used by the bank account.

When sharing resources over a network, you should first configure people's user accounts to access those resources.

**Configuring User Accounts in Windows 7**

User accounts are configure and managed through the Windows 7 Control Panel’s User Accounts too. Three actions performed with User Accounts tool: *Create an account, Modify an account,* such as the password and *Delete an account*.

**Configuring Accounts in UNIX/Linux**

Access to shared resources on the UNIX/Linux system is also managed via user accounts. Each UNIX/Linux user account is associated with the *User Identification Number (UID).* Also, users who have common access needs can be assigned to a group using the *Group Identification Number (GDI)* and then the access resource permissions are assigned to the group instead of to each user. When the user logs on to access resources, the password file is checked to allow l to access resources.

**Configuring Accounts in Mac OS X**

You can also configure Mac OS X Snow Leopard and Lion for multiple accounts using the Accounts utility in System Preferences. When using Mac OS X in a home, public library, or other child location, parental controls are useful features that can be configured. Types of accounts that can be created:

* **Administrator:** used to manage the computer and operating system.
* **Standard**: grants access privileges for general users.
* **Sharing only**: grants access only to shared resources (files and folders) but not applications.
* **Group**: contains only other users or groups.
* **Managed with parental controls**: establishes parental controls on an account.

**Implementing a Virtual Private Network (VPN)**

For organizations, one problem with sharing resources is how to make them securely available to users who travel or work from home. Another problem is secure communications for resources sharing between a main business location and its branch offices. One solution is to use a virtual private network.

A **Virtual Private Network** is a private network, which is like a private tunnel through a larger network, such as the *Internet,* an enterprise network or both, which is restricted to designated member clients only. Its purpose is to provide very secure networking for people connected through the Internet.

A VPN connection requires the use of a remote access protocol to carry packets over a WAN connection. The most common protocol for VPN security is *IP security (IPsec).*IPsec secures IP communications on the network layer of the OSI model.

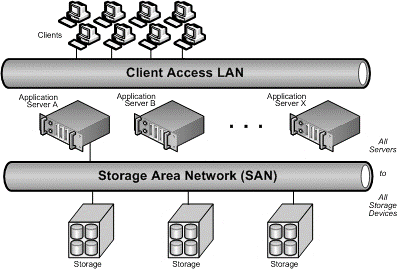
Some VPN networks use the *Layer Two Tunneling Protocol (L2TP)* running inside IPsec for extra security. L2TP is using an additional standard called Layer Two Forwarding. Allows forwarding on the basis of MAC address in addition to IP address.

**Storage Area Networks (SAN)**

Some server-based networks centralize storage on a network in arrays of disk drives that are shared by users through network servers. This arrangement is called a **Storage Area Network.** SAN, which is a grouping devices that forms a subnet.

The subnet containing the storage devices typically use *Fibre Channel* or *Internet Small Computer System Interface (iSCSI)* technology, is another high-speed technology in SANs that employs TCP/IP communications and Small *Computer System Interface (SCI)* disk drives.

In terms of the physical device, a SAN usually looks like a large box or chassis enclosure containing disk drives, disk controllers, and an interconnection device, such as a switch, that connects to one or more servers.

**Figure 3-2 A basic Storage Area Network**

**SUMMARY**

Peer-to-peer networks are relatively easy to set up and inexpensive to maintain.

As networks grow in size and require more centralized management, peer-to-peer is not a good option.

Also configure file permissions in Windows, Mac OS X, and UNIX/Linux systems.

A Virtual Private Network (VPN) enables remote users to access shared resources through secure tunnels.

A Storage Area Network (SAN) can be used to group storage devices on a subnet for sharing storage among multiple servers.