

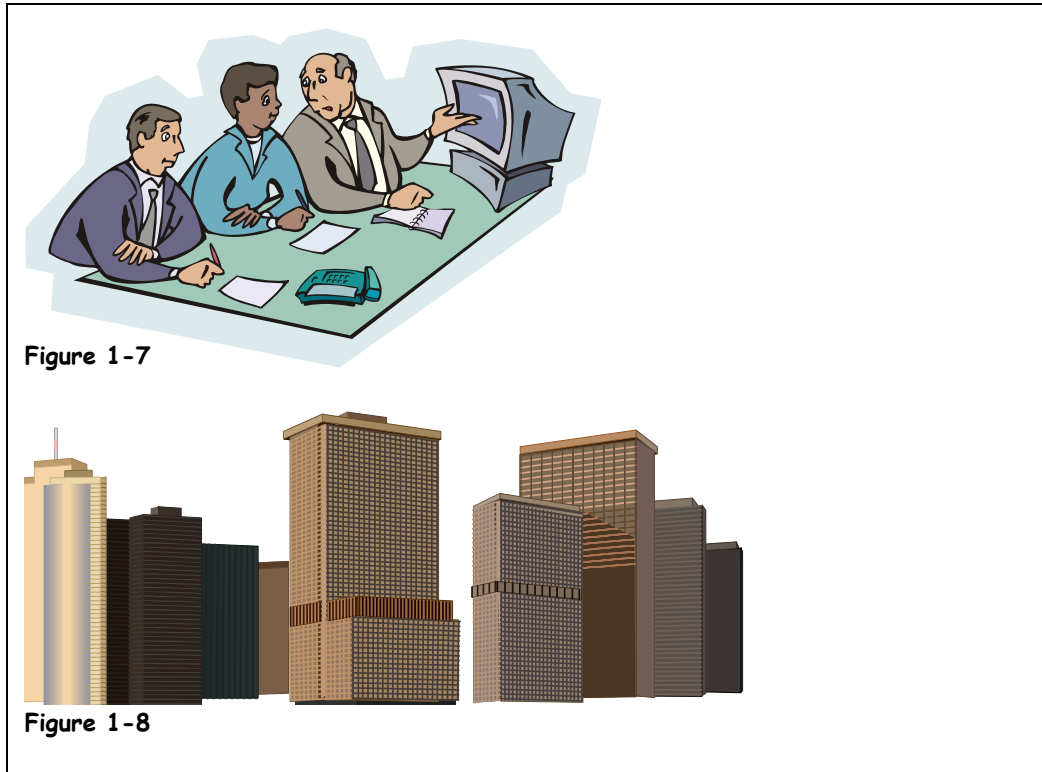
Lesson 1-3: Intranets, Extranets, and Security on a Network

Figure 1-7

An Intranet is a miniature version of the Internet that works within a company or organization.

Figure 1-8

An Extranet is also like a miniature version of the Internet, but Extranets are accessible to authorized users outside of a company or organization.



IC3

Objective: 3.1.1.2, 3.1.1.5, and 3.1.1.6

Req. File: None

An *Intranet* is a miniature version of the Internet that works within a company or organization. Web sites on an Intranet look and act just like any other Web sites, but can only be viewed by users within the company or organization. A *firewall* surrounds the Intranet and fends off unauthorized access.

An *Extranet* is similar to an Intranet, but while an Intranet is generally only accessible to users within same company or organization, an Extranet is accessible by authorized outside users. Business partners use Extranets to share information.

Like the Internet itself, Intranets and Extranets are used to share information. Secure Intranets are now the fastest-growing segment of the Internet because they are much less expensive to build and manage than private networks based on proprietary protocols.

So what are the advantages of Intranets and Extranets? Both Intranets and Extranets can:

- **Share Information:** Intranets and Extranets offer a very simple and inexpensive way to make internal company documents, such as a phone directory, available to employees.
- **Connect Documents:** Documents on an Intranet or Extranet can be connected by hyperlinks, so users can easily jump from one related document to another.
- **Use Special Software:** Some software can only be used on an Intranet or Extranet, such as Web based e-mail programs.

Working in a network environment isn't always fun and games, however; there are some important risks you need to consider and be aware of:

- **Potential loss of autonomy, privacy, and security:** The costs of connecting to a network are much greater than a standalone system.
- **Potential of network-wide systems failure:** This can result in a loss of access to network resources, such as network drives or modems.
- **Vulnerability to a network virus attack:** Because of the vast amounts of information being sent back and forth on a network, your chances for suffering a virus or hacking attack are much greater.

The risks of networks are managed through careful procedures performed by network administrators and other security personnel. A new user will be granted access to the network only after a network administrator has set up and authorized a login and password account. When a user properly logs on to the network, their login and password is authenticated against a list of known users.

- **Authorization of new users by a network administrator:** In order to be granted access to a network, every user must be authorized and assigned an account by a network administrator.
- **Authentication of users through proper login procedures:** When a user properly logs on to the network, their username and password are authenticated against a list of known users.
- **Protection from external threats using protective technology:** Networks are protected from unauthorized access using hardware and software security systems such as firewalls.
- **Regular monitoring of the network:** Network administrators and security personnel monitor activity on a network to protect against unauthorized access or other security violations.

Quick Reference

Intranet:

- A miniature version of the Internet that works on a network within a company or organization.

Extranet:

- A miniature version of the Internet that allows access to authorized outside users, such as business partners.

Risks Involved in Working in a Network Environment:

- Potential loss of autonomy, privacy, and security.
- Potential of network-wide systems failure.
- Vulnerability to a network virus attack.