

Previous Section

### 2.3 -- Networks

Networks are the means by which users are connected to each other for the exchange of data and sharing of resources. Networks can range from very small (a few users in a single office sharing a printer) to very large (the Internet).

#### 2.3.1 -- LAN

A LAN is required when there are several users who need to share data, application software, and equipment. The LAN network devices commonly used are printers, disk drives, modems, and other Management Information System (MIS) equipment (see Figure 3-1). As the name LAN suggests, this type of network is contained within a small area (usually within the same building or floor).

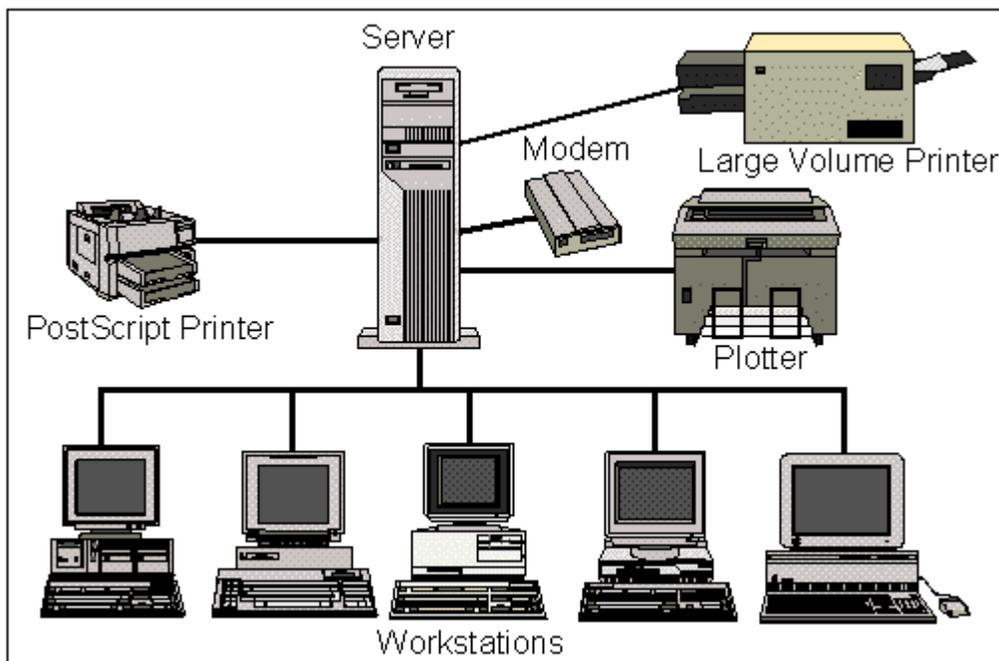


Figure 3-1. -- Example of Basic LAN Layout.

LANs are based on the needs of the user. Some LANs may only need to be connected to share resources such as modems or printers. A primary capability of LANs is to allow users to transfer data files electronically rather than downloading files onto diskettes and carrying them from place to place. Network servers are also commonly used to store large software applications and databases that can be accessed by all authorized LAN users, allowing them to both share applications and save space on their local hard drives.

A common need for organizations is to transfer data from one LAN to another or to connect to a large mainframe computer. These functions can be achieved with what is commonly referred to as a bridge.

Also, a router is often desirable for large networks to reduce network traffic on individual segments.

A Network File System (NFS) (may come with UNIX operating system) allows network file transfer and a file server's storage device to become a local device transparent to the user available on the PC.

### **2.3.2 -- WAN**

A WAN is required when there are multiple users who need to share data or equipment over a large area (usually many miles). A WAN should only be considered if there is a need to transfer large amounts of data for long periods of time. If occasional or limited use or access to remote data or equipment is needed, then a modem or ISDN connection will suffice. WANs are typically made up of a series of connected LANs.

There are several existing and planned Government WANs that are being heavily utilized, especially in the Washington, DC, area. Some of the Services also have their own WANs that connect Program Offices, support activities, and selected contractors. The most well known WAN is the Internet, which is accessible worldwide.

### **2.3.3 -- Network Protocols**

Network protocols are essentially the software standards that enable users to communicate over LANs or WANs. There are several types of network protocols that are acceptable in the CALS community. Factors to consider when choosing the type of network protocol needed include current facility LAN/WAN compatibility, interface requirements, data to be transferred, and distance of network. The following are common protocols and their capabilities.

- . **POSIT:** The Profile for Open Systems Internetworking Technologies (POSIT) has replaced the Government Open Systems Interconnection Profile (GOSIP) as the Government standard for networking protocols (FIPS PUB 146-2). POSIT continues to include OSI protocols. It encompasses the Industry-Government Open Systems Specification. POSIT also lets agencies specify standards of the Internet Engineering Task Force and other open, voluntary standards.

- . **TCP/IP:** Transmission Control Protocol/Internet Protocol (TCP/IP) is the general protocol (IEEE 802.3) for most engineering workstations and servers. It allows UNIX computers to connect to each other for remote login with 'rlogin' and 'rsh' UNIX commands. It also allows a PC with X-windowing software to establish an X-window session on a UNIX server. TCP/IP is the protocol used for Internet connectivity.

### **2.3.4 -- Internet/Intranet**

The Internet is an example of a very large WAN. The Internet was a product of a research and development requirement by the government, universities and large corporations to network computers together as a means to exchange data. It is an interconnected web of data-carrying pathways and intermediate nodes which route and filter packets of data traffic as they travel from pathway to pathway from a source to a destination.

Many Government organizations now have Internet Home Pages that are used to disseminate information about the organization and its programs, as well as providing access to reference information, documents under review, and software applications.

An Intranet includes internet technology with the addition of filtering and security. An intranet usually restricts access to critical data sources to a limited collection of hosts. Traffic crossing an intranet should be secure from release beyond the limited collection of authorized destinations. Intranets are a good way for geographically diverse organizations to exchange data in a fairly secure environment.

The hardware and software required for an Internet connection through a LAN are:

- . Router (see para. 2.1.8)
- . Communication device -- this can be:
  - a modem,
  - a network termination unit (NT1) in conjunction with a terminal adapter which provides for ISDN access, or
  - a channel service unit/data service unit (CSU/DSU) to connect to a switched 56 kbps service (similar to ISDN).
- . An Internet Service Provider (ISP)
- . Internet software interface such as a web browser (e.g., Netscape)
- . Transmission Control Protocol/Internet Protocol (TCP/IP) software which is a suite of protocols that facilitate the passing of data between computers on a network.

## 2.4 -- Telecommunications

Telecommunications includes the hardware required to connect to other computer systems as well as the lines used to transmit the data. Modems are the primary hardware needed to connect with other locations. The lines used to transmit the data vary widely in terms of capacity and cost. The choice of line type will be based on factors such as data volume, speed, and cost. The Program Manager must keep in mind that telecommunications connections are only as fast as their slowest link, and the more routers the data must go through, the slower the response times will be.

### 2.4.1 -- Modems

The minimum equipment required for long distance telecommunications is a modem. The modem is used to link two or more computer systems, typically via an analog phone line. Normal uses could include connection to larger computer systems via a terminal emulation program, connection to a remote site to send/receive files, connection to the Internet to exchange e-mail and data files, or to access Contractor Integrated Technical Information Service (CITIS).

The speed requirement of the modem is directly related to the size of the data files that will be transferred and frequency that the modem will be used. If data is only to be accessed and viewed remotely using a terminal emulation program, then existing 14.4 kbps (kilobytes per second) modems may be acceptable.

However, if there is a requirement to send/receive large data files, a faster modem with built-in data compression is required. A majority of computers sold today are equipped with a 28.8 kbps modem, and programs should not purchase anything less than this. Before purchasing a modem, the Program Manager should ensure compatibility with the modems at remote locations.

#### **2.4.2 -- Integrated Services Digital Network (ISDN) Lines**

Integrated Services Digital Network (ISDN) lines are another method for sending and receiving data. A standard ISDN line, called a BRI (Basic Rate Interface) is actually three phone lines wrapped into one. Two of the lines, called RB channels, are used for transmission of data. The remaining line, called the RD channel, is used to send switching and format information. Each RB channel is capable of transferring data at 64 kbps. This is 2.25 times as fast as a high-speed analog modem. Both RB channels can be bonded together to achieve a transfer speed of 128 kbps. With data compression, ISDN can reach transfer speeds up to 512kbps.

An ISDN connection uses a digital modem and digital telecommunication lines. The signal is never converted to an analog format, thus traveling much quicker and without the static and noise inherent to analog transmissions. The cost of an ISDN is only slightly higher than the cost for a typical analog phone line. For video-teleconferencing (VTC) applications (transmission of voice, video, and data), ISDN lines, as a minimum, are required.

#### **2.4.3 -- T1 Lines**

T1 lines are a point-to-point digital communications circuit that carries twenty-four 64 kbps -- 1.54 Mbps (though sometimes only 56,000 bits/s are accessible to end users) --- channels, each of which may be used for data or digitized voice. The T1 circuit line usually consists of two (often shielded) twisted pairs of copper conductors (one for each direction). Some newer T1 lines employ new techniques that require more sophisticated equipment and lower the line length, but make low-tech wiretaps less a threat.

The term "T1" is usually used interchangeably with "DS-1," though strictly speaking T1 refers to the medium (the bit rate and the copper transmission system described above) and DS-1 refers to the bit format and framing. The similar European service is sometimes called E1.

T1 lines directly linking organizations together provide fast, reliable service readily available today. However, they are also the most expensive of the options discussed here in terms of installation and usage costs (approx. 30-40 times more expensive than an ISDN line). Also note that a T3 line exists that delivers data at a rate of 45 Mbps for about 15 to 20 times the cost of a T1 line.

#### **2.4.4 -- Other Modes of Telecommunications**

Some alternative modes of telecommunications include:

- . **FDDI** (Fiber Data Distribution Interface), a LAN data-link protocol, is designed to run on multi-mode fiber. The rate of data transmission is 100 Mbps.
- . **ATM** (Asynchronous Transfer Mode) is a method for switching fixed-size packets (cells)

around. Like T1 and T3, digitized voice was a major consideration in its design, but it can be used for data. It can be run at different speeds over different media including T1 and T3 as well as 51 Mbps, 100 Mbps, 155 Mbps, and 622 Mbps standards. The fixed cell size is 53 bytes. Though ATM is really designed for voice and WANs, there are schemes to use it in LANs. ATM is still immature and not yet widely available.

**SONET** (Synchronous Optical Network) is a set of standard fiber-optic-based serial standards planned for use with ATM in North America. Different types of SONET run at different speeds (OC1 runs at 51 Mbps, OC3 runs at 155 Mbps, OC12 runs at about 600 Mbps, OC48 runs at over 2 Gbps), and use different types of fiber (OC3 has several variants for use with different fibers & different distances; there are versions for both single mode and multimode fiber).

#### **2.4.5 -- Electronic Mail**

Another means of data exchange is through the use of Electronic mail or e-mail. E-mail is the facility enabling one to send messages to other computer users. E-mail is fast -- messages sent anywhere in the world are usually delivered within minutes. The computer system of the person being contacted will accept and store the e-mail message in a mail file without any interaction from the receiver. As a minimum, e-mail systems should allow users to compose and read mail, send and receive messages and data files, reply to mail, and forward mail to other users.

Many types of information can be exchanged via e-mail, including text, data files, and programs. E-mail is especially useful for weapons system programs supported at geographically diverse locations, and it is currently widely implemented throughout the Government and Industry. E-mail can be used to perform some of the functions typically required by a CITIS, such as acknowledge and notice of delivery.

For external e-mail connection on a LAN, all the items required for an Internet connection (see para.2.3.4) are needed except the Internet service. Also, instead of the internet software interface, an e-mail server software with a Simple Mail Transfer Protocol (SMTP) packet is used (e.g., CC:Mail). For internal e-mail on a LAN, e-mail server software and SMTP is needed; no additional hardware is required.

### **2.5 -- Security Considerations**

Studies show that as network usage grows, network security deteriorates. Threats to networks come from many sources including hackers, international industrial espionage agents, disgruntled employees and human error. Sensitive data on networks are at risk and need to be protected against the risk of loss.

Protecting enterprise data transmission on local- and wide-area networks is a complex undertaking. Planning for a secure data networking environment must account for the following:

- . Heterogeneous network topologies supporting multiple protocol architectures;
- . Large user populations with diverse network access requirements;
- . Data from multiple sources combined within public and private networks; and
- . Increasing number of access points in the network.

### 2.5.1 -- LAN Security

These realities suggest the need to explore a range of alternatives for protecting information assets transmitted or stored on a network. Security planners must be prepared to explore far-reaching policy and practices issues before selecting an appropriate security strategy. Should a workstation be secure from its neighbor, or is it adequate to secure small groups? Is the main concern the protection of data transmission over the wide area, or are there too many access points which suggest securing the LANs as well? Does the enterprise need different levels of security for different business units? Should e-mail be secure, or only protected to make certain it always gets delivered to the proper destination?

- . Determining where to place security services in the network raises many important considerations:
- . Data can be protected with encryption before it leaves a node or network and decrypted only as it arrives at its pre-specified destination.
- . Packet structures from the node or network conform to international standards allowing a properly-designed security device to protect different platforms and applications.
- . The security device at the network or the node can also be used for access control.
- . A software-based solution increases the risk as software is changeable without the knowledge of the user; requires regular maintenance and integrity validation; and typically has user involvement in activating the security provisions.

#### **2.5.1.1 -- Secure Network Management**

When developing a plan for secure data transmission and access control across enterprise-wide networks, the system should provide:

- . High-level of protection without burdening users with new procedures or impeding network performance;
- . Application, operating system and protocol independence;
- . Network transparency without impacting the network functions;
- . Hubs, bridges, routers and other network devices should not need to be modified;
- . Industry standard cryptographic technology to ensure maximum protection for end-to-end data transmission; and
- . Scalable solutions that will provide enterprise-wide network protection, no matter how complex and dispersed the network.

For a secure environment, the security devices will have to parse every element of data traffic to validate its movement on the network. This protection mandates that network managers know all details of their

network data traffic. When access control and encryption technology are being added to a network, processes should be initiated to evaluate and update the security standards of the enterprise. These tasks include key management, monitoring or auditing the system, and choosing the methods for controlling access to network nodes or sites. The following paragraphs describes some of the general requirements of a secure network environment.

### **2.5.1.2 -- Key Management**

Key management involves the creation, distribution, protection, and maintenance of access control and encryption keys. Access control keys establish limits on which nodes or sites are allowed to communicate. The encryption keys are used to "lock" and "unlock" the secure data traffic, with the sender of data using the key to encrypt the data, and the recipient using the same key to restore the data to its original form.

A system should provide an ability to optimize the management of the encryption keys using techniques to distribute the keys to each security device by sending them over the network using a protected method. This method has the keys being encrypted before they are sent, which requires that another key be distributed to decrypt the keys. The distribution methodology which permits automated key distribution is known as Public Key Encryption.

Public Key Encryption technology allows two devices to communicate securely even if they have never communicated before. It serves as the mechanism for securely distributing encryption keys across an "unsecured" path. Public key systems use two encryption key segments: A public key and a private key.

While satisfactory for securing key distribution, public key technology is not fast enough to encrypt high volumes of network data traffic, even when implemented in hardware. However, secret key encryption, which involves communication between two users who both possess the same secret key, does perform at speeds suitable for today's networking systems when implemented in hardware.

Public-key cryptography can be used with secret-key cryptography to get the best of both worlds. For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. The public-key system can be used to encrypt a secret key which is used to encrypt the bulk of a file or message.

### **2.5.2 -- Internet Security**

The Internet suffers from severe security-related problems. Some of the problems with Internet security are a result of inherent vulnerabilities in the services (and the protocols that the services implement), while others are a result of host configuration and access controls that are poorly implemented or overly complex to administer. This is further aggravated by the tremendous growth of the Internet and how the Internet is used; businesses and agencies now depend on the Internet for communications and research and thus have much more to lose if their sites are attacked.

The more systems that are connected, obviously the harder it is to control their security. Equally, if a site is connected to the Internet at several points, it likely would be more vulnerable to attacks than a site with a single gateway. At the same time, though, how well prepared a site is, and the degree to which the site relies on the Internet, can increase or decrease the risk.

Sites that use recommended procedures and controls for increasing computer security have significantly lower risks of attack. Firewalls, combined with one-time passwords that are immune from monitoring or guessing, can increase greatly a site's overall level of security and make using the Internet quite safe.

### **2.5.3 -- Firewalls**

A firewall can significantly improve the level of site security while at the same time permitting access to vital Internet and network services. It helps implement a larger security policy that defines the services and access to be permitted. It is an implementation of that security policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to control access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

A firewall system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet. A firewall system is usually located at a higher-level gateway, such as a site's connection to the Internet, although firewall systems can be located at lower-level gateways to provide protection for some smaller collection of hosts or subnets.

In general, a firewall should have the following features or attributes:

- . Be able to support a "deny all services except those specifically permitted" design policy. The firewall should support your security policy, not impose one.
- . Be flexible; it should be able to accommodate new services and needs if the security policy of the organization changes.
- . Contain advanced authentication measures or should contain the hooks for installing advanced authentication measures.
- . Employ filtering techniques to permit or deny services to specified host systems as needed.
- . Contain an IP filtering language that is flexible, user-friendly to program, and should filter on as many attributes as possible, including source and destination IP address, protocol type, source and destination TCP/User Datagram Protocol (UDP) port, and inbound and outbound interface.
- . Use proxy services for services such as FTP and TELNET, so that advanced authentication measures can be employed and centralized at the firewall. If services such as NNTP, X, http, or gopher are required, the firewall should contain the corresponding proxy services.
- . Contain the ability to centralize SMTP (Simple Mail Transfer Protocol which is used to transfer electronic mail between computers) access, to reduce direct SMTP connections between site and remote systems. This results in centralized handling of site e-mail.

- . Accommodate public access to the site, such that public information servers can be protected by the firewall but can be segregated from site systems that do not require the public access.
- . Contain the ability to concentrate and filter dial-in access.
- . Contain mechanisms for logging traffic and suspicious activity, and should contain mechanisms for log reduction so that logs are readable and understandable.
- . Be developed in a manner that its strength and correctness is verifiable. It should be simple in design so that it can be understood and maintained.
- . Be updated with patches and other bug fixes in a timely manner.

There are undoubtedly more issues and requirements, however, many of them will be specific to each site's own needs. A thorough requirements definition and high-level risk assessment will identify most issues and requirements, however it should be emphasized that the Internet is a constantly changing network. New vulnerabilities can arise, and new services and enhancements to other services may represent potential difficulties for any firewall installation. Therefore, flexibility to adapt to changing needs is an important consideration.

[Next Section](#)