Chapter 1

Network Topologies

One of the first steps in creating good network design is to choose your network topology, or network map. How will you start your design? Is it a small LAN with a few workstations? Is it a campus LAN or a massive enterprise implementation? Is scalability important? How about network management? What about cost? Certainly, cost is always an issue in a network design project.

In most situations, you'll find yourself with a network already in existence. There will certainly be opportunities to develop a network from scratch, but more than likely you'll end up inheriting an existing network. This network will probably have been created with a long line of additions and upgrades that somehow work together.

This chapter will cover some of the more common network topology models. No one topology is right for every network environment, but based on the material in this chapter, you should be able to decide which design is best for your network project. Along with your new decision-making ability, you'll have the knowledge and understanding as to why a certain topology is best. This gives you the ability to discuss and present the issues to clients, employers, and coworkers.

Each of the network topologies discussed can be integral parts of another topology design. Redundant and secure topologies should be part of every network design. For the purposes of discussion, each topology is presented in a separate section of the chapter. The network topologies are discussed in this order:

- Flat network topology
- Hierarchical network topology
- Mesh network topology

- Redundant network topology
- Campus/LAN network topology
- Enterprise/WAN network topology
- Secure network topology

Flat Network Topology

A flat network topology design is generally used for very small networks. Each network device, such as a hub, bridge, switch, or router is used for a general rather than specific purpose. In flat networks, modular units or discrete functions are usually non-existent. Most network components in a flat network design are used for simple broadcasting and providing limited switching capabilities. The flat network design is based on a common broadcast domain. Each of the network components is brought together within a common layer. More often that not, the flat network design is relegated to earlier and simpler network designs without complex switching requirements.

Description

In a flat network topology, network components usually communicate in a looping fashion. If routers are used, each router will send routing updates throughout the internetwork. Since the internetwork is usually small, routing updates will occur quickly. Convergence is not often an issue since updates and changes in a flat network are minimal. Communication through routing loops requires a limited number of routers or switches to route traffic or send routing updates.

Flat network designs are not generally created in a modular fashion. Flat networks provide a consistent and easy-to-manage network environment, but they provide limited modularity to reduce cost.

Also, scalability is not usually an important design factor for flat network designs. If you need a network that will grow and scale well, a flat network topology is limited in its ability to scale to enterprise-wide infrastructures and is usually not a good design option. Routing protocol convergence is generally fast and efficient as long as the flat internetwork is small and compact. Figure 1-1 shows a sample flat network topology.

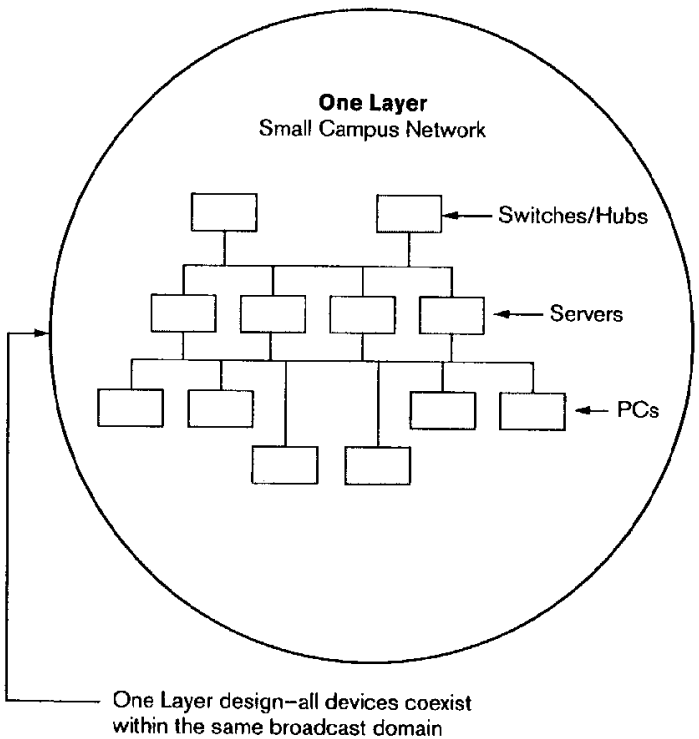

Figure 1-1 *Flat network topology*

Summary

A flat network topology design is generally used for very small networks. More often than not, the flat network design is relegated to older and simpler network designs without complex switching requirements. Flat networks provide a consistent and easy-to-manage network environment, but they provide limited modularity in order to reduce cost. If you need a network that will grow and scale well, a flat network topology is limited in its ability to scale to enterprise-wide infrastructures and is usually not a good design option.

Advantages

The following list summarizes the advantages of the flat network design model:

- Lower cost — A flat network topology is lower in initial cost due to the smaller size of the network and lower equipment costs. Special routing and switching components are not used to a wide extent in a flat network topology design.
- Reliability — Flat networks are reliable due to the simplistic design and general static nature of the topology.
- Easy to design — Flat networks do not generally incorporate modularity; therefore, the design is easy to create and implement. Flat networks aren't usually concerned with scalability either, which contributes to the ease of design.
- Easy to implement — Implementation is generally easier due to the lack of specialized switching equipment and configuration anomalies.

Disadvantages

The following list summarizes the disadvantages of the flat network design model:

- Not modular — Changes to the environment will usually affect all internetworking devices.
- Bandwidth domain — In a flat network design, most if not all devices are usually in the same bandwidth domain. This can cause a problem if applications require specific bandwidth resources.
- Broadcast domain — All systems are in the same broadcast domain and can cause broadcast congestion.

Hierarchical Network Topology

Hierarchical network typologies are created in layers to allow specific functions and features to be implemented in each of the layers. Each component is carefully placed in a hierarchical design for maximum efficiency and specific purpose. Routers, switches, and hubs all play a specific role in routing and distributing data and packet information. In a hierarchical design, each layer of the hierarchy has a purpose and works together with the other layers of the hierarchy to bring order and maximum performance in the internetwork. Most Cisco networks today are built on the hierarchical design philosophy, at least in part. With changing technologies and complex corporate network environments, a true-layered hierarchical design may be uncommon, but certainly worth the effort to attain.

Description

A hierarchical network design incorporates three key layers for internetworking component communication, and Cisco adheres to the three-layer design philosophy for its hierarchical networks. The three hierarchical layers are the core layer, the distribution layer, and the access layer. The core layer provides the backbone, or high-speed switching component, to the network. In a pure hierarchical design, this core layer will provide only the specialized task of switching data. The distribution layer is the demarcation point between the core layer and the end-user access layer. The distribution layer components provide packet manipulation, filtering, addressing, policy enforcement, and other data-manipulation tasks. The access layer provides end-user access to the network. But, prioritization and bandwidth switching can also be configured at the access layer to optimize use of network resources.

Modularity is important in a network that will need to grow and evolve with business needs and new technology implementations. Networks today are increasingly complex and have evolved as rapidly as the technology. With modularity, hierarchically designed networks can limit the effect of each component change to the immediate area of the change only. This means that the entire network won't be affected as it would be in a flat network design. Routers, switches, and other internetworking devices can be added to complement the design when needed. Hierarchical network designs are created to be scalable.

Scalability will allow new components and applications to be integrated into the existing network design with limited reconstruction or design. One of the key advantages to hierarchical topologies of any network size is the ability to scale to new business requirements while using the existing technology investment that's already in place. Because of the complexity and size of the network design, routing protocols used in a hierarchical network must have quick convergence and low processor utilization for

routing updates. Most newer routing protocols have been designed with hierarchical topologies in mind and require fewer resources to maintain a current network routing table or map.

Figure 1-2 shows a hierarchical network topology.

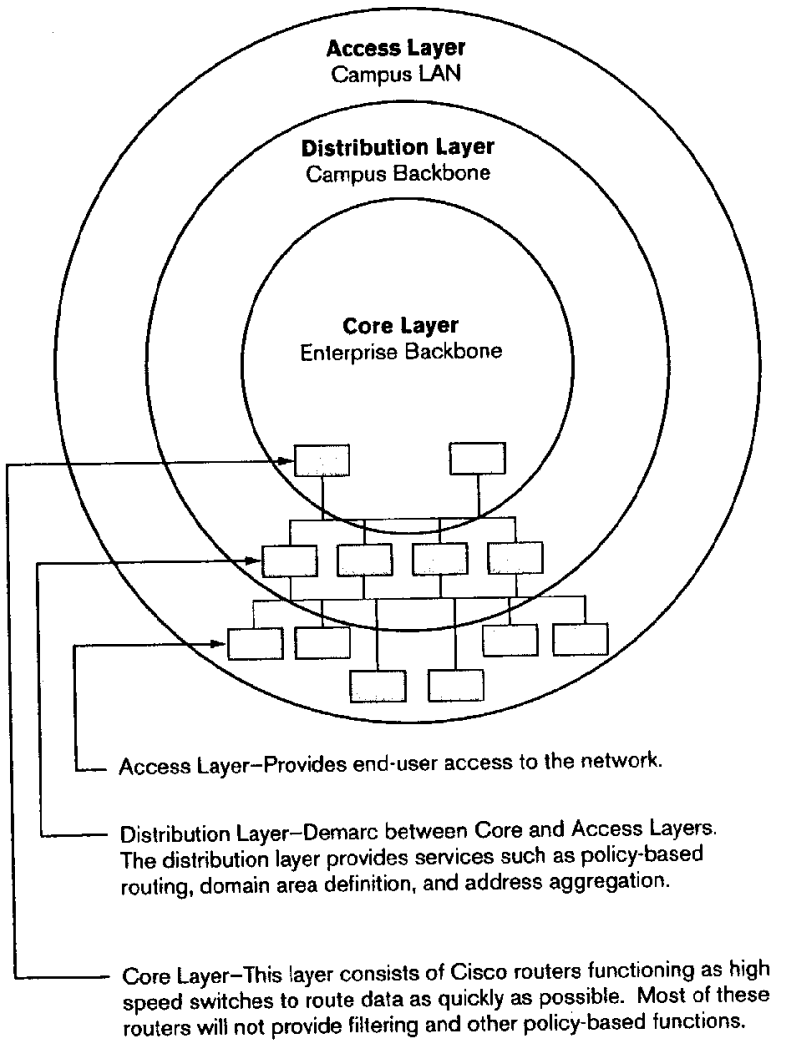

Figure 1-2 *Hierarchical network topology*

Summary

Hierarchical network typologies are created in layers to allow specific functions and features to be implemented in each of the layers. Most networks today are built on the hierarchical design philosophy, or at least part of the hierarchical design. A hierarchical network design incorporates three key layers for internetworking component communication. Cisco adheres to the three-layer design philosophy for designing hierarchical networks. The three hierarchical layers are the core layer, the distribution layer, and the access layer. The core layer provides the backbone, or high-speed switching component, to the network. In a pure hierarchical design, this core layer will provide only the specialized task of switching data. The distribution layer is the demarcation point between the core layer and the end-user access layer. The distribution layer components provide packet manipulation, filtering, addressing, policy enforcement, and other data manipulation tasks. The access layer provides end-user access to the network. One of the key advantages to hierarchical topologies of any network size is the ability to scale to new business requirements while using the existing technology investment that is already in place.

Advantages

The following list summarizes the advantages of the hierarchical network design model:

- Scalable—The modular aspect of a hierarchical-designed network enables routers, switches, and other internetworking devices to be added to complement the design when needed.
- High availability—Redundancy, alternate paths, optimization, tuning, filtering, and other network processes contribute to the overall high availability in hierarchical networks.
- Low delay—With routers delineating broadcast domains, and multiple paths for switching and routing, traffic moves quickly with very little delay.
- Fault isolation—Using a hierarchical design can facilitate changes and improve fault isolation. A modular design will promote quick problem resolution through logical problem-solving and component isolation.

- Modular—The modular design of hierarchical networks allows each component to perform a specific purpose in the internetwork, thereby increasing performance and allowing easier and more organized network management.
- Cost efficient—Certain bandwidth utilization reductions can be realized with optimization and tuning of switching and routing paths in a hierarchical network.
- Network management—With an efficient and well-designed network in place, the management of the components will be more automated and easier to deploy. This can result in cost reductions for staff and training.

Disadvantages

With the redundancy that is often integrated into a hierarchical network topology and specialized switching equipment, the initial cost of a hierarchical network is significantly higher than a flat network design. With the higher investment in a hierarchical design, it's important to choose routing protocols, components, and processes carefully.

Mesh Network Topology

Mesh network topologies are constructed with many different interconnections between network nodes. Fully meshed and partially meshed are the two types of mesh network topologies.

Description

A fully meshed network is typically the backbone of the enterprise network. Fully meshed networks provide excellent redundancy and reliability. Mission-critical services and applications are frequently running on fully meshed network topologies. Partially meshed networks are much like fully meshed networks except that each network node or switch does not necessarily have an immediate connection to each other network node or switch.

Fully Meshed Networks

In a fully meshed network, each network node or switch will have a path to every other network node or switch. Typically, the nodes are located at the core level or backbone level of the network. Fully meshed network topologies are generally not a cost-effective solution. Although you can (for the most part) assure that certain service-level agreements are met with a fully meshed design, you can't guarantee that server or application failures will be redundant with just a fully meshed backbone. A fully meshed design would be best for a specific WAN application that could not operate in a lower or reduced bandwidth scenario. Fully meshed designs are expensive to implement due to circuit cost. Figure 1-3 shows a fully meshed network topology between WAN switches.

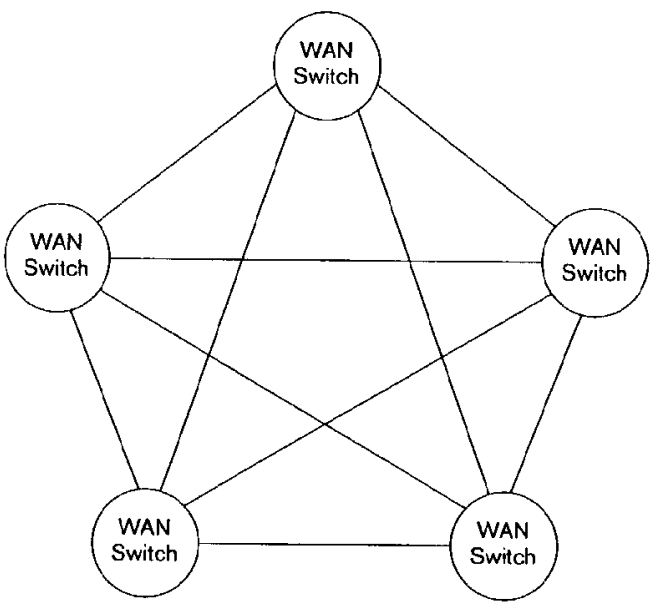

Figure 1-3 *Fully meshed network topology*

Partially Meshed Networks

Partially meshed networks can still provide redundancy through alternate paths. Usually in this design, if a network connection fails, the network will remain operational with reduced bandwidth and service levels. Partially meshed network topologies are more likely to be implemented in an enterprise network. In a partially meshed network design, if a circuit or component fails, the data is routed through an alternate path. The alternate path may not be able to provide the bandwidth required for all network services, but will generally maintain connectivity and allow mission critical applications to continue processing. Of course, circuit failures and component failures do occur on occasion, so partially meshed network designs need to be planned carefully to assure that if outages do occur, either the effect is minimal or an alternate or redundant configuration is available. Figure 1-4 shows a partially meshed network topology.

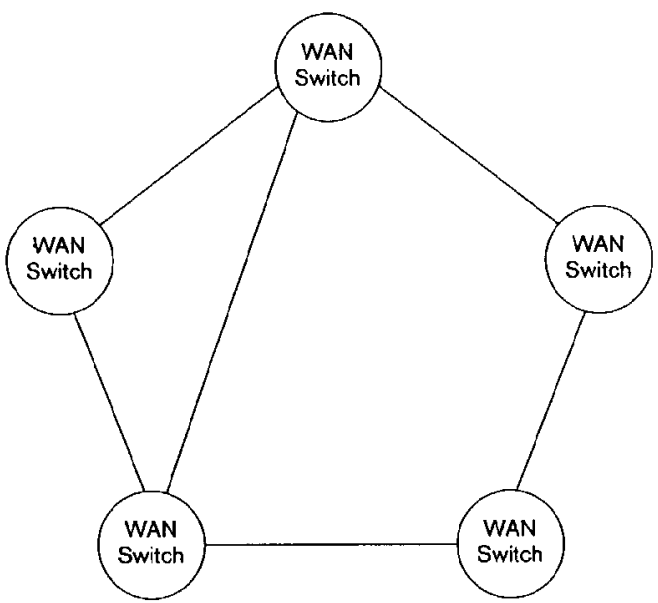

Figure 1-4 *Partially meshed network topology*

Summary

Meshed network topologies are constructed with many different interconnections between network nodes. Fully meshed and partially meshed are the two types of mesh network topologies. Fully meshed networks provide excellent redundancy and reliability. A fully meshed design would be best for a specific application that could not operate in a lower or reduced bandwidth scenario. Partially meshed networks are much like fully meshed networks except that each network node or switch does not necessarily have an immediate connection to each other network node or switch. Partially meshed network designs need to be planned carefully to assure that if outages do occur, either the effect is minimal or an alternate or redundant configuration is available.

Advantages

The main advantage of the meshed network topology is the redundancy that is provided by having multiple links connecting each network site. Especially with the fully meshed configuration, network availability is enhanced with redundant paths.

Disadvantages

Meshed network topologies can be expensive due to high circuit costs. If a fully meshed design is constructed, the redundancy and full network availability may not be worth the extra cost. Data circuit costs, implementation costs, and support costs may be higher than the cost of the service degradation that a fully meshed design was implemented to prevent.

Redundant Network Topology

Redundant network topologies should be incorporated into all network designs. Because businesses run critical applications and services, every one of their networks needs some type of redundant topology to ensure bandwidth is available to deliver required network services. When early network provider companies first designed networks, they made redundancy a key element in their marketing strategy for new and existing clients.

Description

Transmission media, routers, servers, and workstations are several areas where you can incorporate redundancy into network design.

Redundancy at the core or backbone layer is of extreme importance. Some type of data circuit or media will connect each of your routers or WAN switches. Most of the time, the transmission media (especially in very large networks) is supported by a third-party vendor, such as a telco carrier or network service provider. When provisioning transmission media, it is very important to know and understand the routes that the data links travel. Often, circuit vendors will provide a route through their "network cloud," but you won't have a clear understanding of what path your data is traveling to reach its destination.

Caution

Be sure you are aware of "single points of failure" in the data circuits that you provision for your network. Even using multiple network providers won't guarantee that your network redundancy is intact.

Even having a map provided by your network provider won't guarantee that the circuits are redundant. Often when network outages occur (such as a fiber cut or other failure), backup circuit paths are put into service, used as the primary path, and not returned to backup status once the primary path has been repaired. It's possible that your redundant network design (at the core media level) was based on the primary path on the network providers' network. Once the primary network path is unavailable, your network may not be redundant at the most-basic level. Stay in contact with your network service provider representative and be sure that you have the most current network map available.

As an alternative to using multiple data circuits or multiple network providers, you can select two media types to provide redundancy. Satellite and data circuits are good combinations for redundancy since the satellite link won't travel over the same geographic area as the data circuits. Again, be cautious. Some satellite links eventually do connect to data circuits before they reach your network. In serious network outage situations, redundancy may fail on both network paths. If you are connecting to areas outside of the United States, you'll have to rely on your international support team to get network redundancy information, as the international carriers will be reluctant to give out circuit path information. To create an even stronger redundancy into your network design, and depending on the size and critical nature of your network, you may want to consider have multiple vendors, multiple circuits, and multiple technologies. Often, cost considerations prohibit multiple technologies, but you'll need to weigh the cost of an outage versus the cost of the technology that may prevent the outage.

Once you have created a redundant network design for your backbone or core layer, you'll need to take a look at your routers. Cisco routers can provide load balancing and multiple path routing depending on the protocols being used in your internetwork.

Another area of concern is the workstation and server level of your network. More than likely, the workstation will be not designed for redundancy, since a failure at that level will only affect that particular workstation. So, limited or intermittent failures won't generally affect any other network users or services. However, as we all know, full data backups are important, especially at the workstation and server level where users keep their most sensitive data.

At the server level, a redundant hardware design is also critical. Use a mirrored disk or system to provide the minimum redundancy needed. Sometimes, a software solution for mirroring data can lead to disastrous results when hardware fails. Servers should be designed to withstand disk outages and power failures. Redundant Array of Inexpensive Disks (RAID) technology will allow disk mirroring and disk striping. RAID disk striping is used to write data across several physical disks. If one disk fails, the network operating system will request a new disk be inserted and then re-create lost data that is based on parity information from the remaining disks. There are different RAID standards for network operating systems as well as applications. Check with your application vendor for more specific information on how the application works with RAID technology.

Figure 1-5 shows a redundant network topology.

Summary

Redundant network topologies are incorporated into all network designs. With businesses running critical applications and services, every network will need some type of redundant topology to ensure that services and bandwidth are available to deliver required network services. Transmission media, routers, servers, and workstations are several areas of the network design where you can incorporate redundancy.

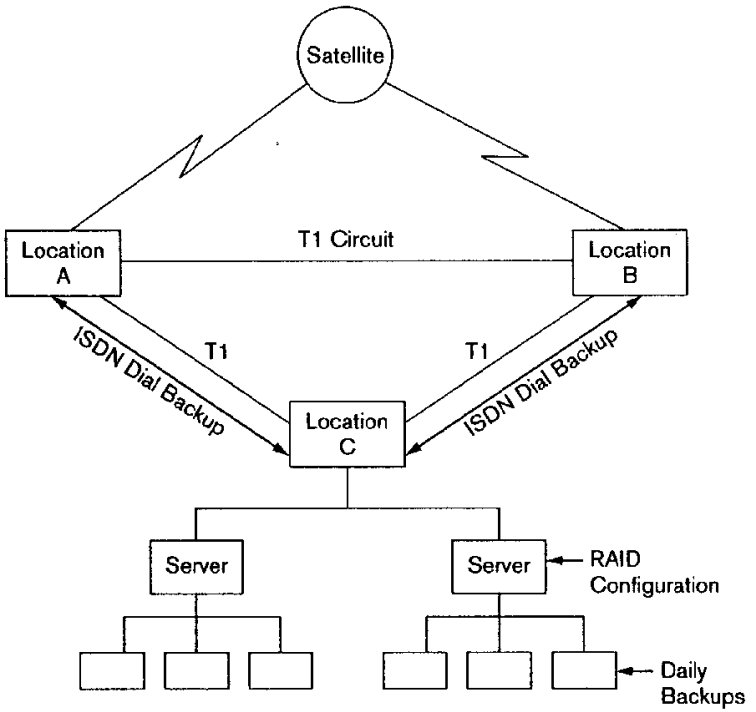

Figure 1-5 *Redundant network topology*

Advantages

The following list summarizes the advantages of the redundant network design model:

- Provides high network availability
- Secures data transactions from hardware failures
- Allows easier and more cost-effective network management of redundant nodes

Disadvantages

Redundancy should be approached with caution and should be developed as a strategy that will provide service-level enhancements and cost savings. Redundancy should not be designed into a network for the sake of redundancy. If the cost of an outage or data loss is less than the cost of the redundant technology to prevent it, you should carefully consider whether the redundant technology is worth installing.

Campus/LAN Network Topology

Campus and LAN network topologies have typically been limited in size and complexity due to the smaller amount of network nodes and network services. Current technologies such as ATM and switched LANs are increasing network complexity while providing end users increased bandwidth for multimedia and other resource-intensive applications.

Description

LAN networks have moved out of the traditional one-server, multi-user environment in one building to multiple-building campus environments that require more specific technology that is not necessary broadcast based. The progression of network complexity at the LAN level can be broken down into three general areas. First, the more traditional LANs, such as ring, bus, and star topologies, started the LAN environments years ago when networking personal computers began to appear in most businesses. When user requirements for bandwidth exceeded the traditional limits, the next major LAN technology involved switched LANs. Switched LANs, or campus LANs, also came about as corporations moved out of the one-room LAN to multiple buildings and areas. Finally, VLANs were introduced. VLANs allow like-users across a campus environment to share a common broadcast domain.

Traditional LANs

Traditional LANs are those LAN environments that allow workgroup access to network services. Most of these LANs were implemented years ago when Novell created NetWare for multiple users to share data. Later, Microsoft developed Windows NT Server as an alternative for file, print, and application services on a LAN. Small businesses can use these traditional LAN topologies to share data within an office, building, or smaller internetworking environments. Ring, bus, and star LAN network topologies are typical traditional LAN designs.

Ring The ring network topology describes Token Ring as well as FDDI designs. Ring networks provide media access methods that do not create a collision-based network. Each station on the ring transmits data at the required time and processes packets according to a token-passing methodology. Token Ring networks are traditional IBM technology networks. Token Ring networks connect all the user stations to the ring. FDDI ring networks are higher speed but use the same token-passing methodology that allows only one user to transmit data on the ring at any one time.

Bus A bus topology network is traditionally Ethernet. A bus network connects all stations together on the same cable media. Each station taps into the bus (or wire) to send and receive data on the network. Like the Token Ring environments, each station processes each and every data packet that is sent across the media wire. However, unlike Token Ring, the bus networks use a media access method called Carrier Sense Multiple Access/Collision Detection (CSMA/CD). In a CSMA/CD network, each station listens to the media for traffic that is being transmitted. When a station wants to send data, it will wait until there is no traffic being transmitted on the network before sending data. If it happens to send data at the same time as another station, both stations will back off and wait a specified period of time before transmitting again.

Star Star topology networks depend on a central switching component to deliver network services to each end station. Each end station is connected to the central switching component independent of any other end station. If one end station fails, there will be no effect on the other end stations. However, in the star topology configuration, if the central switching component fails, all stations attached will also lose communication to the network.

Campus LANs – Switched LANs

Campus LAN environments have exploded over the past several years due to the demand for networked PCs and instant business communication. Most of the move to switched internetwork LANs is a result of the demand for higher bandwidth to the desktop. More and more users require high-speed access to Internet and other business applications. The traditional 80/20 rule of network design, where 80 percent of the traffic remains within a local network segment, has been challenged by the consolidation of data and services within corporate intranets.

Generally, switched internetworks are more highly managed and efficient as compared to its predecessor, the shared bandwidth network. Switches are able to handle increased data speed and more traffic, and can provide dedicated bandwidth to specific users based on business need. Switches can also prioritize traffic and provide increased performance throughout the internetwork. Many switches today have OSI layer 3 routing capabilities built into them. Layer 3 Switching will be discussed in Chapter 6.

Asynchronous Transfer Mode (ATM) can provide LAN as well as WAN capabilities, and therefore presents itself as a unique technology alternative for the campus/LAN environment. Some network designers are choosing ATM for its bandwidth-on-demand capabilities as well as its ability to support multimedia to the desktop.

Figure 1-6 shows a campus/LAN network topology.

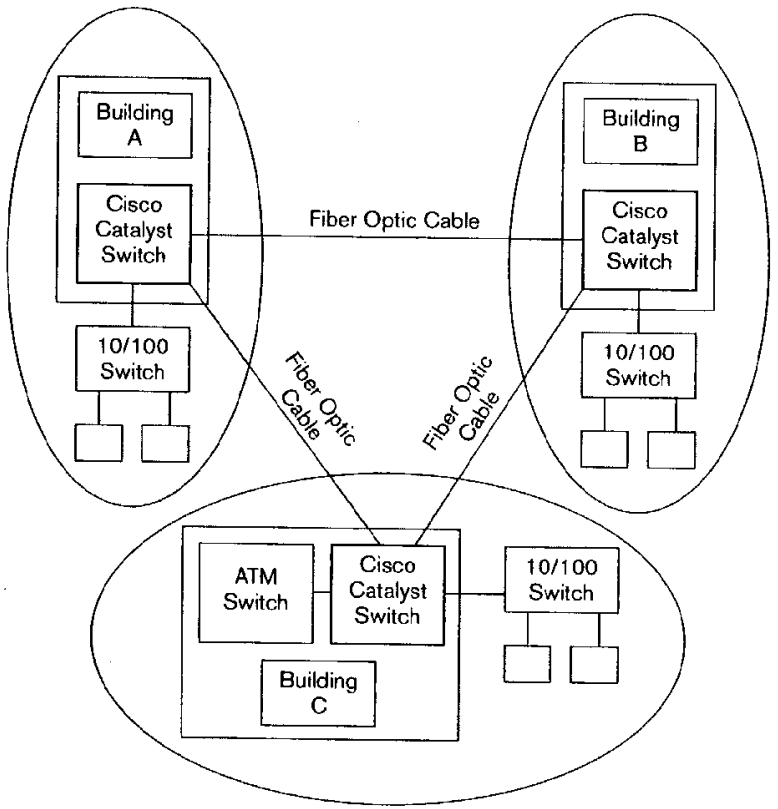

Figure 1-6 *Campus/LAN network topology*

VLANs

VLANs have been introduced into campus/LAN design scenarios due to the ease of administration and flexibility when personnel are reassigned or move frequently. With VLANs, an end-user's unique network services are available in any geographical location regardless of physical location. VLANs allow businesses to link departments and project staff onto the same virtual segment. A VLAN management interface is available for network personnel to configure VLANs. VLANs are basically a way for broadcast traffic to be limited to a certain domain of users. Often, groups of users are connected through a VLAN for projects and temporary assignments. For this reason, VLANs need to be flexible and scalable. Routers are not required to implement a VLAN infrastructure. Only cross-segment traffic would require a router for networking and addressing functions.

From port-based traffic to policy-based traffic, VLANs can be configured in a number of ways. Some of the more popular VLAN configurations are port-based, protocol-based, and policy-based designs.

Port-based VLANs The port that the user has a physical connection to defines port-based VLANs. Implementation of this type of VLAN is probably the easiest of all types of VLAN implementations. An example of a VLAN configuration would be VLAN-X running on Switch A ports 1,3,5,7 and Switch B ports 1,3,5,7. VLAN-Y would be configured as running on Switch A ports 2,4,6,8 and Switch B ports 2,4,6,8. This type of configuration provides very high security due to the static nature of the VLAN assignment. Manual intervention will be required to move a user to another VLAN. Port-based VLANs are not as flexible as other VLAN implementations and are more useful with smaller and more permanent switching environments. You can also assign ports to multiple VLANs.

Protocol-based VLANs Protocol-based VLANs are based on protocol type. User groups can be defined by network personnel based on whether the protocol is IP, IPX, or the like. Protocol-based VLANs don't relate well to real-world scenarios where end systems are running multiple protocols and multiple applications. Of course, protocol-based VLANS do allow end-user systems to be members of multiple VLAN networks. Protocol-based VLANs also allow protocol segmentation and isolation that in several situations can provide better throughput and also limit broadcast traffic.

Policy-based VLANs Policy management is by far the most powerful type of VLAN implementation. Switches that operate on policy-based VLANs can determine VLAN membership based on certain policies such as configuration detail, security, and performance. Policy-based VLANs are more flexible and business-friendly. Software applications often change or are upgraded, and the associated VLAN switches can dynamically determine the most appropriate VLAN for the application. Policy-based VLAN switches check data frames to determine the most efficient VLAN membership based on policy filters.

Summary

Campus and LAN network topologies have typically been limited in size and complexity due to the smaller amount of network nodes and network services. Traditional LANs are those LAN environments that allow workgroup access to network services and include bus, star, and ring LAN implementations. Current technologies such as ATM and switched LANs are increasing network complexity while providing end-users increased bandwidth for multimedia and other resource intensive applications. VLANs allow businesses to link departments and project staff onto the same virtual segment. A VLAN management interface is available for network personnel to configure VLANs.

Advantages

The following list summarizes the advantages of campus/LAN network topologies:

- Switched internetworks can provide dedicated bandwidth to the desktop.
- More efficient use of network resources at the LAN level.
- Reduced cost due to easier physical implementation.

Disadvantages

One of the main disadvantages to campus/LAN topologies is the possibility that newer technologies are implemented too early and do not take full advantage of the network components that are already in place. Frequently,

interoperability issues arise, and equipment, processes, and applications are discarded in favor of a new technology that promises to cure all network issues and problems.

Enterprise/WAN Network Topology

With multiple network technologies and applications that run through them, enterprise networks are as varied as the businesses they serve and the network personnel that run them.

Description

Enterprise networks grow and evolve as company services and locations change and expand. Early enterprise networks were handled by service providers, such as GE, Tymnet, and others. Early timesharing mainframe services are much like the Internet Service Providers (ISPs) of today. Since the cost of data transmission and equipment was high, most companies accessed their data from massive mainframe computers at remote locations. As time progressed and information services grew more and more important to companies and their businesses, each company began to develop its own computer system infrastructure. The enterprise networks of today are the end result of the business growth and the heavy reliance on information processing and flow. Enterprise networks can take on many different designs depending on the business need. It's important to remember that enterprise networks should be built to serve the applications that are needed to support the business, not the other way around. "If you build it, they will come" is not a good enterprise network design philosophy.

Enterprise Networks

Three main types of enterprise class network topologies are popular today. Remote access networks, Intranet/Internet, and WAN topologies all work together to provide needed business services and communication capabilities. In this section, each topology will be discussed separately.

Remote Access Networks Remote access is a growing area of network design. With telecommuters and increased business travel, what was once a luxury has become a necessity to conduct business. Traditional access

methods such as dialup are used, as well as ISDN and cable access to corporate networks. ISDN is a high-speed dial-up access method using digital phone lines. The one main advantage is the ability for home users and telecommuters to have high-speed access to the Internet and corporate WANs. Digital Subscriber Line (DSL) uses existing telephone lines to provide multimedia service to end subscribers.

Intranet/Internet Intranet web servers are becoming the standard for internal business communications. Online learning, employee orientation Web sites, and time tracking are just a few of the many applications that are available through corporate intranets.

Internet access is everywhere. Companies over the past years have moved from a wait-and-see attitude about the Internet to allowing access to desktops all across organizational levels. Of course, tracking and security is of extreme importance when implementing an Internet solution for your company or client. To reduce the possibility of lost time due to Internet web site surfing, a standard policy of tracking Web access should be implemented. Be sure that all employees are aware of the conditions of Internet usage when on company time.

Internet servers that are used to transact e-commerce solutions are becoming as important to the business as the storefront. Online sales will continue to increase and be more and more of a profit center for all types of businesses and industries.

WAN WAN implementations take on many shapes and sizes. Depending on the application, client, and business, WAN implementations can be as varied as the businesses that implement them. WANs combine intranet services, Internet access, remote access, and mainframe applications to allow corporations to communicate with distributors, clients, and suppliers. Technologies that are commonly implemented in WAN infrastructures include Asynchronous Transfer Mode (ATM) and Frame Relay. ATM is a newer technology that provides a technology solution for voice, data, and video, and has still not gained widespread acceptance. Frame Relay is a packet-switching technology that takes advantage of the increased reliability and stability in transmission media. WAN technologies are discussed in Chapter 2.

Figure 1-7 shows an Enterprise/WAN network topology that incorporates remote access, Internet, intranet, and WAN services.

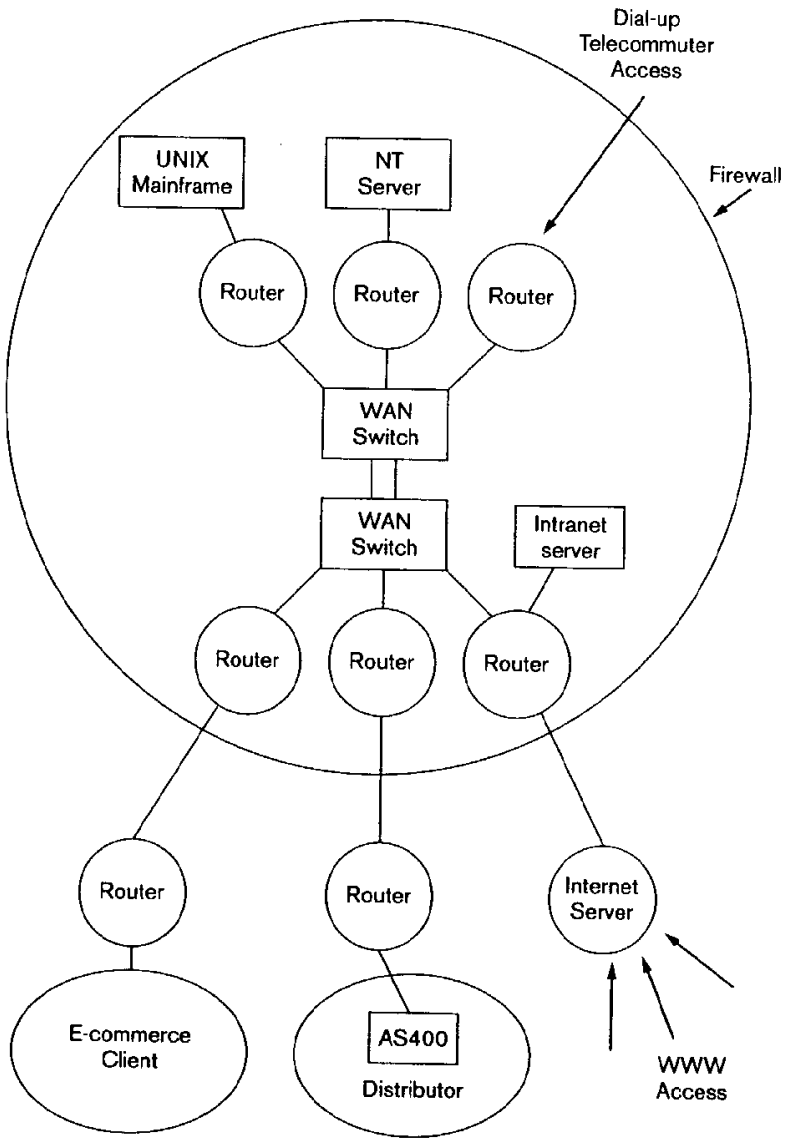

Figure 1-7 *Enterprise/WAN network topology*

VPNs

Virtual Private Networks (VPNs) are becoming more popular as a network design alternative due to the widespread availability of the Internet and the associated cost savings. VPNs can connect business suppliers and distributors through a third-party proprietary network. VPNs save money in a variety of ways. Businesses that use VPNs don't require a support staff for the backbone infrastructure. Equipment cost savings, as well as keeping up on the latest technology for backbone speed and service offerings, contribute to the popularity of VPN technology.

Early timesharing companies such as Tymnet and GE were the first to offer VPN services. Although not thought of as VPNs, early service providers built networks on X.25 technology, and corporations would link offices and locations through a proprietary infrastructure.

Of course, one of the drawbacks to a VPN is the control of the network infrastructure. Service providers control backbone connections and service availability. Another concern with VPNs is the possible lack of security. Data encryption is one security feature that will allow businesses to process secure transactions within VPNs at a low cost.

The Internet is the ultimate VPN. Using tunneling and encryption, companies can conduct business without providing network infrastructure components.

Figure 1-8 shows a Virtual Private Network topology.

Summary

No two enterprise networks are alike. With multiple network technologies and applications that run through them, enterprise networks are as varied as the businesses and network personnel that run them. Three main types of enterprise class network topologies are popular today. Remote access networks, Intranet/Internet, and WAN topologies all work together to provide needed business services and communication capabilities. Virtual Private Networks (VPNs) are becoming more popular as a network design alternative due to the widespread availability of the Internet and the associated cost savings. VPNs can connect business suppliers and distributors through a third-party proprietary network. The Internet is the ultimate VPN. Using tunneling and encryption, companies can conduct business without providing network infrastructure components.

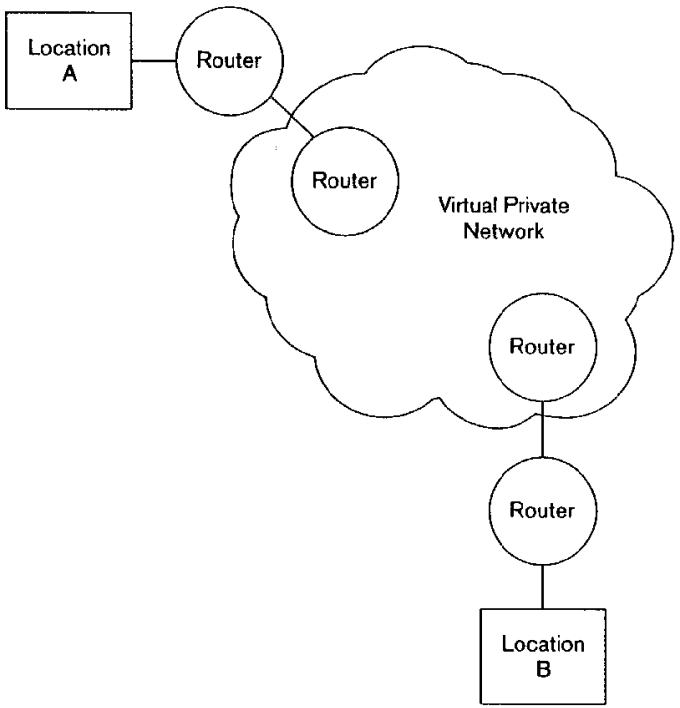

Figure 1-8 *VPN topology*

Advantages

The advantages to having an Enterprise/WAN network topology are not as important as the fact that they are becoming an absolute necessity to conduct business. Intranets, extranets, Internet, and VPNs are all ways that businesses use enterprise-wide infrastructure solutions to remain competitive.

Disadvantages

A disadvantage to Enterprise/WAN network topologies is the staffing and support that is needed to implement and maintain the network. The outsourcing of staff and support functions continues to be discussed with wide-ranging views. Outsourcing limits your control over your network, but allows non-technical businesses to concentrate on core business strategies rather than spending business resources on information technology management.

Secure Network Topology

Security is one of the most important considerations in a network design, especially as businesses move sensitive data to intranet servers for internal employee use. With the relatively new use of Internet technology and access, security will play a more active role in choosing technologies and methods for employee productivity, customer support, and online business transactions.

Description

Policy and standardization, implementation, and audit are three main areas to consider when designing a secure network topology.

Policy and Standardization

When designing a secure network topology, putting policies and standards in place is not only a good idea for security, but also a best practice for network management. Policies and standards will allow network users the freedom to use network services and to perform company business in a secure environment.

There are other issues when implementing network policies and standards. The culture, or the way of doing business for a particular company, will many times influence secure topology design. When an executive cannot access important sales data because of a user account lockout due to an excessive number of failed logins, certain security policies must be in place so that the executive can still conduct business. Remote access has become an increasingly important issue for many businesses. With more extensive networks and telecommuters, secure topologies must allow access to sensitive data at any time and from any place.

There are several key areas of network policies and standardization that need to be addressed when designing a secure network. Software features such as data encryption and authentication are important, as well as hardware solutions such as firewalls. It is also important to remember physical security when implementing secure networks. Is your physical network hardware in a place where no one can access it? Are there limits to the number of people who have access to the computer room, wiring closets, and servers? Is access to those rooms and wiring closets audited?

Implementation

Implementation of a secure network topology will be the next step once the standards, policies, and procedures are in place. Be sure that these policies are communicated as appropriate. Company executives or your clients should be aware of the security policies and the reasons for them. Be sure that you get agreement from key personnel before any security policies are in place. As much as you want a secure network, personnel must have access to critical business data. Once you've designed a solution to provide consistent and reliable service, the next step is to set policies and procedures in place to assure a secure networking environment.

Firewalls are a common implementation of network security. Firewalls, of course, provide limited access to data. Cisco has hardware and software firewall solutions. Firewalls and the technology to limit user access are key components to a secure network topology. Firewalls will be discussed further in Chapter 8.

Mainframe systems, network servers, and business-critical workstations need to have a security system of some type implemented. It may not be necessary to have an audit log for each and every workstation, or even every network server. You'll need to identify the risk to the business if the network resource is compromised. It is a good idea to keep the security mechanisms low-key for most of the end-user population. End-users, except for key management, do not need to know what level of security is implemented on the network. You may want to check with the corporate legal department before monitoring or accessing specific user data. Be sure that employees have been notified that the data that they are working with is company property and can be seized or accessed as necessary for business purposes. Let the legal department take the necessary steps to communicate certain security policies, or at least be sure that your implementation does coincide with your company's business practices and culture.

Audit and Review

Once your security policies and procedures have been decided and are in place, it will be critical to review and audit your network security. Often, you will have a security officer take responsibility for specifically auditing your network policies, or you will have an external agency audit your network.

Caution

There is a difference between being paranoid and being aware. Often, security threats are internal to the company. Creating a review process for internal security should be taken on with both caution and an awareness that your critical network systems can be compromised by internal employees.

Certainly, you should be aware of the latest news on hacker activity and threats to your network systems. Stay current on new technologies as well as the latest software patches, security holes, and enhancements to your implemented systems.

Figure 1-9 shows a secure network topology.

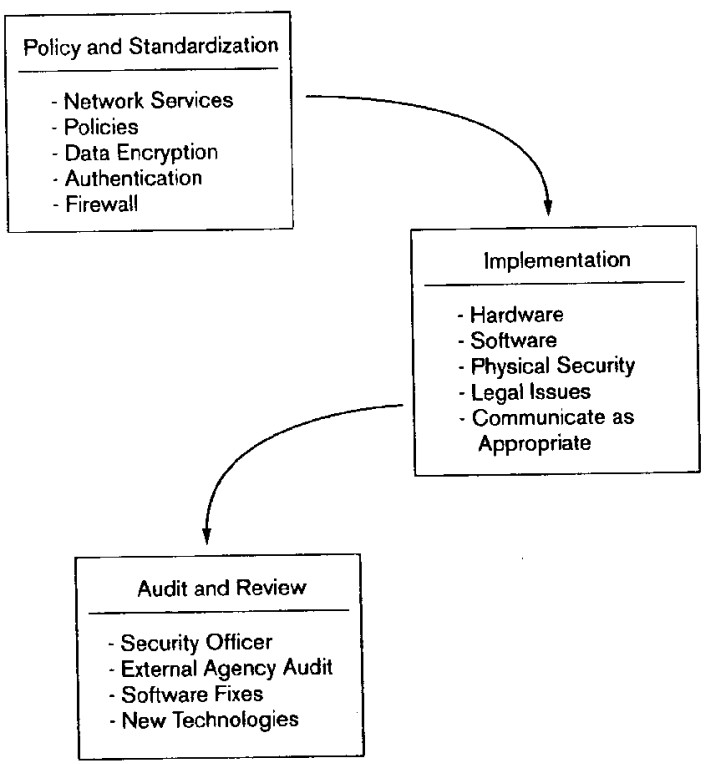

Figure 1-9 *Secure network topology*

Summary

Security is one of the most important considerations in a network design, especially as businesses move sensitive data to intranet servers for internal employee use. Policy and standardization, implementation, and audit are three main areas to consider when designing a secure network topology. Policies and standards will allow network users the freedom to use network services and to perform company business in a secure environment. Implementation of a secure network topology will be the next step once the standards, policies, and procedures are in place. Once your security policies and procedures have been decided and are in place, it will be critical to review and audit your network security.

Advantages

The main advantage to a secure network topology is the fact that business can be conducted electronically and much quicker than in non-secure environments. If a network topology has no security, then it has really no effective means to conduct important business. Secure network topologies that are implemented over the next few years will be able to take advantage of the Internet market and all the possibilities that it has to offer.

Disadvantages

The main disadvantage to a secure network topology is the cost associated with the implementation and support. You'll have to make tradeoffs in regards to security versus the effect that is has on day-to-day business. In creating secure network topologies and processes, the effect should be seamless and enhance, if possible, rather than hinder, business processes and productivity.

Key Points

The network topologies discussed in this chapter all work together to provide reliable network services. Depending on the applications and services that you'll provide to your end-user community, you can choose to implement portions of each network topology type. Secure network topologies are increasingly important as more and more businesses put proprietary information on departmental servers and corporate intranets. Here is a summary of the network topologies that were discussed:

- Flat Network Topology—A flat network topology design is generally used for very small networks. More often that not, the flat network design is relegated to earlier and simpler network designs without complex switching requirements. Flat networks provide a consistent and easy-to-manage network environment, but they provide limited modularity to reduce cost. If you need a network that will grow and scale well, a flat network topology is limited in its ability to scale to enterprise-wide infrastructures and is usually not a good design option.
- Hierarchical Network Topology—Hierarchical network typologies are created in layers to allow specific functions and features to be implemented in each of the layers. Most networks today are built on the hierarchical design philosophy, or at least part of the hierarchical design. A hierarchical network design incorporates three key layers for internetworking component communication. Cisco adheres to the three-layer design philosophy for designing hierarchical networks. The three hierarchical layers are the core layer, the distribution layer, and the access layer. The core layer provides the backbone, or high-speed switching component, to the network. In a pure hierarchical design, this core layer will provide only the specialized task of switching data. The distribution layer is the demarcation point between the core layer and the end-user access layer. The distribution layer components provide packet manipulation, filtering, addressing, policy enforcement, and other data manipulation tasks. The access layer provides end-user access to the network. One of the key advantages to hierarchical topologies of any network size is the ability to scale to new business requirements while using the existing technology investment that is already in place.
- Mesh Network Topology—Mesh network topologies are constructed with many different interconnections between network nodes. Fully meshed and partially meshed are the two types of mesh network topologies. Fully meshed networks provide excellent redundancy and reliability. A fully meshed design would be best for a specific application that could not operate in a lower or reduced bandwidth scenario. Partially meshed networks are much like fully meshed networks except that each network node or switch does not necessarily have an immediate connection to each other network node or switch. Partially meshed network designs need to be planned carefully to assure that if outages do occur, either the effect is minimal or an alternate or redundant data path is available.

- Redundant Network Topology—Redundant network topologies are incorporated into all network designs. With businesses running critical applications and services, every network will need some type of redundant topology to ensure services and bandwidth are available to deliver required network services. Transmission media, routers, servers, and workstations are several areas of the network design where you can incorporate redundancy.
- Campus/LAN Network Topology—Campus and LAN network topologies have typically been limited in size and complexity due to the smaller amount of network nodes and network services. Traditional LANs are those LAN environments that allow workgroup access to network services and include bus, star, and ring LAN implementations. Current technologies such as ATM and switched LANs are increasing network complexity while providing end-users increased bandwidth for multimedia and other resource-intensive applications. VLANs allow businesses to link departments and project staff onto the same virtual segment.
- Enterprise/WAN Network Topology—With multiple network technologies and applications that run through them, enterprise networks are as varied as the businesses and network personnel that run them. Three main types of enterprise class network topologies are popular today. Remote access networks, Intranet/Internet, and WAN topologies all work together to provide needed business services and communication capabilities. Virtual Private Networks (VPNs) are becoming more popular as a network design alternative due to the widespread availability of the Internet and the associated cost savings. VPNs can connect business suppliers and distributors through a third-party proprietary network. The Internet is the ultimate VPN. Using tunneling and encryption, companies can conduct business without providing network infrastructure components.
- Secure Network Topology—Security is one of the most important considerations in a network design, especially as businesses move sensitive data to intranet servers for internal employee use. Policy and standardization, implementation, and audit are three main areas to consider when designing a secure network topology. Policies and standards will allow network users the freedom to use network services and to perform company business in a secure environment. Implementation of a secure network topology will be the next step once the standards, policies, and procedures are in place. Once your security policies and procedures have been decided and are in place, it will be critical to review and audit your network security at regular intervals.