CHAPTER

13

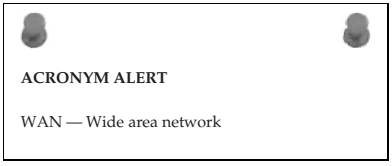
Implementation

First, have a definite, clear, practical idea – a goal, an objective. Second, have the necessary means to achieve your ends – wisdom, money, materials, and methods. Third, adjust all your means to that end.

– Aristotle

Aristotle lived many centuries before the age of computer networking, but his wisdom rings true when it comes to implementing any new network infrastructure. For the most part, organizations have used an evolutionary approach to growing their networks, adding capability when it was needed. As a result, many of today's networks are poorly laid out and maintained, often with little or no documentation.

Many executives like to think of their networks as they do any other utility, such as electrical power, telephone service, etc. There is no mistake about it: corporate networks are part of the ingrained infrastructure in running any type of business. However, unlike these other utilities, which have large organizations behind them in their support, the network infrastructure is the sole responsibility of the organization that owns it. Unfortunately, they tend to look at it as an overhead function, and when budget cuts are required, it is always the overhead areas that get chopped first. That is all well and good as long as things keep humming along without interruption. But there comes a day when something decides to burp. If there is network equipment stored in accessible closets, you may have the following scenario occur. The janitor thinks he should clean out the back of a closet that has collected a lot of junk along with some portions of the company's network infrastructure. He inadvertently kicks out some cables



and plugs them back where he thought they were connected. All of a sudden no one is getting e-mail and the CEO is on the horn trying to find out what is going on. I know this sounds comical and perhaps a bit far-fetched, but we can assure you that it does happen and it can get downright ugly before things are running again.

13.1 Planning

Planning is where you place Aristotle's first line into action: ''have a definite, clear, practical idea — a goal, an objective.'' Good network planning begins with a top-down approach. Today's complex networks evolved from very basic networks and were patched together as more networking capability was needed. This was far from a top-down design. We have seen network installations that would have made Rube Goldberg[1] cringe at the thought of adding his name to its design. Many of these networks became this way primarily by a ''if it ain't broke, don't fix it''[2] mentality.

Figure 13-1 illustrates a network planner in the initial planning phase to implement the design approach he decided on using the information provided in Chapter 12 on design methodologies. There is a natural dividing line as far as planning goes; one side involves a current network infrastructure and the other side a total new design. If this is a totally new design, the planning task only involves how to implement the new network design. If there is a preexisting network, however, several considerations need to be reviewed prior to implementing the new network design. Because the totally new network implementation requires only a subset of a network design that would be required for an older network infrastructure, it will be covered first.

RANDOM BONUS DEFINITION

100BASE-TX — A baseband Ethernet system operating at 100 Mbps over two pairs of STP or Category 5 UTP cable.

The initial planning phase should consider not only the current network requirements, but also what may be needed in the future, both near-term and long-term. Think of where the growth areas will be and see how that growth can be easily accommodated while growing the network infrastructure in an orderly manner. Remember, you should plan ahead for network growth, rather than cobbling together networking capability as required.

[1]Reuben Garret Lucius Goldberg, born July 4, 1883, died December 7, 1970. American cartoonist noted for his cartoons of involved and complex machines, most of them just accomplishing a mundane task in a convoluted manner.
[2]An expression popularized by President Jimmy Carter's advisor Bert Lance.

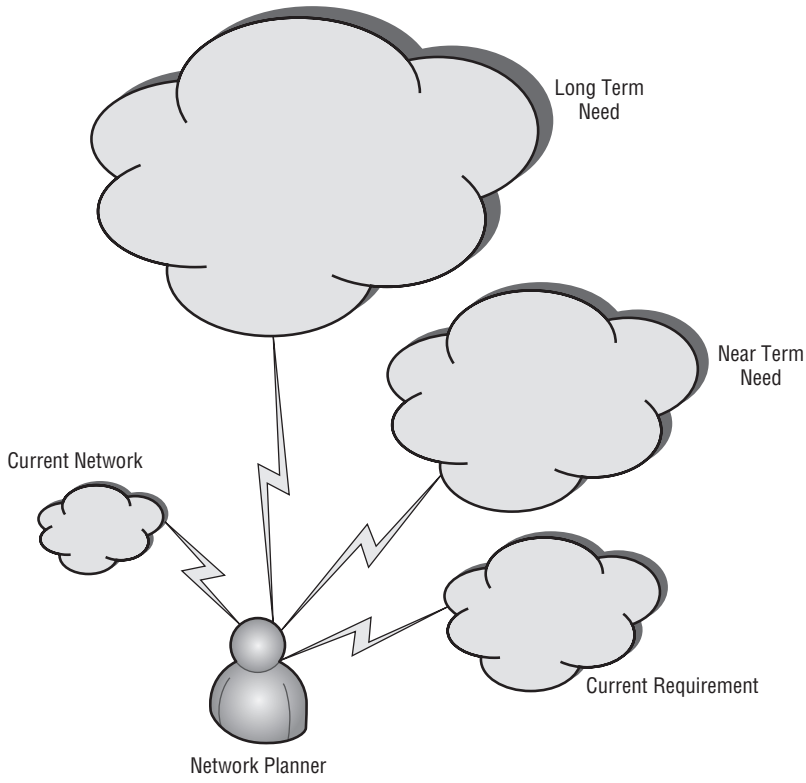


Figure 13-1 The initial planning phase

13.1.1 Totally New Network Planning Phase

As the old saying says, the best-laid plans of mice and men often go awry. The idea is to eliminate as many problems as possible by beginning with a well thought out plan. If you have the opportunity to do a total network design from scratch, there are many variables to consider. The key is to size the network and the network segments so you can meet peak bandwidth requirements without overbuying. Some items involve a recurring cost, whereas others are one-time purchases. Part of the planning entails making appropriate cost estimations. A good place to start is to list both recurring and fixed cost items.

Recurring costs:

- Access fees
- Support contracts (usually billed annually)
- In-house support staff
- Energy needs
- Routine maintenance

One-time costs:

- Hardware
- Cabling
- Initial installation fees

Access fees are the monthly service charges from the telecommunications company for providing access to their network. The rule of thumb is that the more bandwidth required, the higher the cost. Some factors that may help determine which service to use for access are the services offered and the number of telecommunications companies that are located within the area for your new planned network. If there are multiple telecommunications companies within the area, you should request quotes for the types of services they offer. There may be a one-time installation or hookup fee associated with the service plan you are considering.

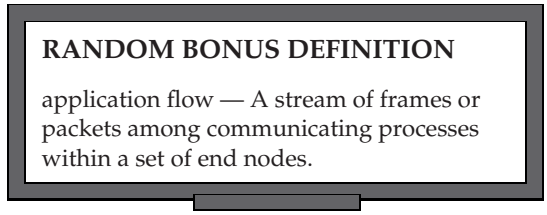
13.1.1.1 Initial Planning

The design approach should be completed using a top-down methodology — that is, start with the big picture. However, each phase should entail a document that details what is needed at that level.

We will begin the initial planning phase using a hypothetical[3] example of the Widget Company, which wants to expand their operations west of the Mississippi River. The corporate planners have researched various areas and determined that Denver best suits their needs for their first expansion out of their Midwest region. The first-level network plan may look something like that illustrated in Figure 13-2.

13.1.1.1.1 Office Interconnection Planning

The plan is for a high-speed network between the new West Region office in Denver and the corporate office in Chicago. This is to be a point-to-point connection to provide for the sharing of services located at the corporate offices. The plan entails using a



[3]What is being discussed is scalable to any size organization. The required numbers depend on the size of the facility and the number of network users located at this facility.

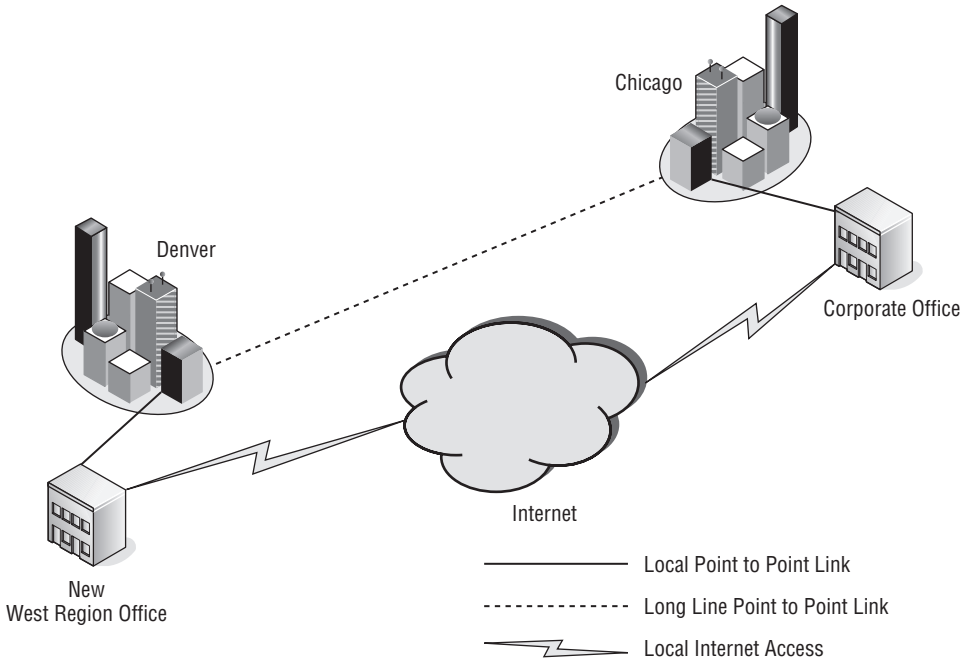


Figure 13-2 The top-level plan for Denver's expansion

carrier to provide those services over its national optical network. However, the plan is to allow the users at the Denver office to also have Internet access locally with a local provider. This Internet access can be used as a redundant path to the corporate office in Chicago, if the need ever arises with a failure in the high-speed optical network. After determining how the offices are to be interconnected, the planning does not end there. Bids will need to be solicited from the optical carriers for services offered and the rate schedule for those services. Also, bids will need to be obtained from local ISPs in the Denver area.

While that bid process is ongoing, other plans can be worked on. You should continue planning both the access to the network from the outside world and the network distribution inside the building. In the Widget Company example, it is determined that a combination server and network services area would also house the access and backbone network distribution equipment. Figure 13-3 illustrates the layout of the combined server and network operations area.

13.1.1.1.2 Network Operations Area

Many companies these days lump computer operations, network operations, and all other telecommunications under the IT (information technology) umbrella. If the company is large enough and the amount of equipment and services offered warrant it, the department could have a number of

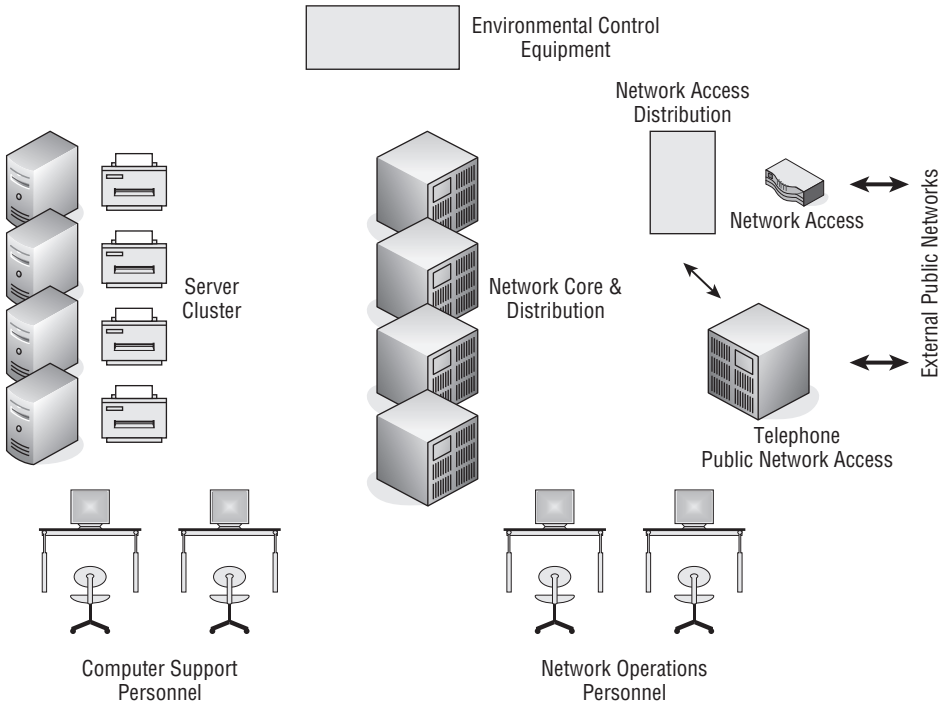


Figure 13-3 The combined server and network operations area

staff to maintain the equipment and support the workforce located at that facility. Sizing and scaling of the support model is proportional; there is no one-size-fits-all approach for each separate installation. Some companies with a corporate office and regional office use a model where much of the IT support is run out of the corporate office, with a smaller staff located at the remote offices performing the hands-on work. Chapter 15 discusses methods of remote network management.

Figure 13-3 shows a single central support area. It is not uncommon to locate core services for IT to save money by not needing more support staff located in different areas of the facility. Once an IT department is set up, the amount of staff required to maintain the on-site equipment and field support calls from the local users for services provided by IT is much lower in the initial implementation phase. If major upgrades to the local network are required, a company can opt to hire contractors or send staff from other locations to assist in the upgrade. Another option is to hire a company to handle the upgrade and pay for the labor that is required directly to that network contractor. Many factors will determine which method would be best, but the overall cost and size are typically the driving forces of the upgrade project. Small upgrades

or addition of added network capacity are usually handled by the on-site IT employees.

NOTE **On-site IT employee numbers have dwindled due to companies "off-shoring" their support functions. It is a situation that appears monetarily lucrative to those that run the budgets of companies but can be a nightmare at times. Being locally based employees for our entire careers may have jaded us, but it is our opinion that this is a poor way to provide IT services support. It has been our experience that the best run network infrastructures are maintained locally by staff who knew their networks well. It can be difficult for an IT support person on a support call to envision what is going on with a network half a world away. Add to it idiom-based language differences and the frustration level rises to the point of exasperation. The key is knowing what you are paying for when you decide how your IT department is to be staffed.**

13.1.1.1.3 Environmental Requirements

There are other considerations to take into account while designing a central area for the computer and network operations for the IT department. One consideration is flooring. There are pros and cons for having a false[4] floor. It can facilitate environmental control of the area by using the space under the false floor as the return duct for the HVAC[5] system, and it can be where the power and network cabling can be placed. The major disadvantage is that adding additional cabling at a later date can be difficult since the tiles would need to be lifted to route the cable. A false or raised floor can be more aesthetically appealing than overhead cabling, but it lends itself to an installation that is fairly static. You do not want to use that type of flooring if you anticipate a dynamic work area with many additions and reconfigurations. It is much easier to use overhead cable racks to distribute the network cabling and power buses for the power drops that may be required. These are easily reconfigurable and facilitate changes much more rapidly than routing cables under a floor.

[4]A false floor is a raised floor made up of individual panels that are normally two-foot squares. They are laid in over a framework that looks like a giant matrix before the tiles are laid in. Usually, the facility is wired under the flooring before the tiles are placed down.

[5]HVAC stands for heating, ventilation, and air conditioning. When there is a high concentration of computer-related equipment is a fixed area, there is a volume of heat that needs to be dealt with. Most facilities install HVAC systems to control the environment not only for temperature but humidity levels, too. High humidity can cause corrosion, and the last thing you want is something growing on your network connections. Contact corrosion can cause problems that are nasty to diagnose and find.

RANDOM BONUS DEFINITION

backoff — The mechanism used in the Ethernet MAC (CSMA/CD) to reschedule a transmission in the event of a collision.

The environmental control system is usually installed and maintained by an HVAC contractor. However, the sizing of the system requires input from the network planners as to the number of BTUs[6] of heat generated within the area. This will include all the equipment within the area as well as the number of human bodies[7] that will be in the area. The HVAC contractor can use that information to right size[8] the equipment needed, with a fudge factor[9] to compensate for minor growth.

13.1.1.1.4 Network Access Requirements

You may have noticed in Figure 13-3 that the public telephone network access and the network access are in the area dedicated for IT services. It has been decided that this site will use VoIP (Voice over IP) and the telephone sets will be IP-enabled phones. The voice communications will run over the network throughout the facility. So the convergence of the voice and data networks will occur in the IT area. Part of the traffic shaping[10] plan may entail that voice communications between the Denver facility and the Chicago corporate office will go directly from the local phone switch as IP data over the directly connected fiber link.

NOTE The term "convergence" is tossed about heavily in the network world. The simple fact of the matter is, it's becoming an IP world. Any form of data that can be digitized can be transmitted over the network within data packets. However, real-time applications such as voice and video require committed bandwidth rates to guarantee a satisfactory level of service. Humans do not take too well to choppy voice reception or flickering video displays. When planning these services, care must be taken to guarantee the required bandwidth to eliminate these types of issues. Traffic profiling and shaping are essential parts of the planning phase.

[6]BTU is the acronym for British Thermal Unit. It is the amount of heat required to heat a pound of water from 60 to 61 degrees while it is sitting at a constant pressure of one atmosphere.
[7]We are talking of live human bodies here. Live bodies generate heat and expel moisture as they breathe. Dead human bodies neither breathe nor generate heat so they need not be counted, but we would not want them around too long either. So although many employers like to work their employees to death, they prefer you to do your dying on your own time.
[8]"Right size" has come to mean many things these days. It usually refers to getting the size right for a particular need. However, it has been hijacked by corporate management as a term to replace "layoff."
[9]"Fudge factor" is a term used to suggest that a number has been tampered with. Here it is used to mean that additional capacity for HVAC equipment is "upped" to compensate for possible future growth.
[10]Traffic shaping is the ability to direct network traffic over segments of a network, depending on bandwidth availability and other policies enforced on the network by the IT staff.

Part of the planning phase is determining levels of access to the network. If it is decided that there will be services available from the Internet, strong consideration needs to go into designing firewalls and DMZ[11] zones. You may want to segment your network to easily facilitate these DMZ areas. There may be other firewalls that police the traffic flow to and from the network at large. Whenever a network ties into the Internet, there should be a firewall between it and the first router on the Internet. This is to prevent unwanted and unsolicited traffic[12] from finding its way into the local network. A preliminary plan may be similar to that illustrated in Figure 13-4.

ACRONYM ALERT

RMON — Remote monitor

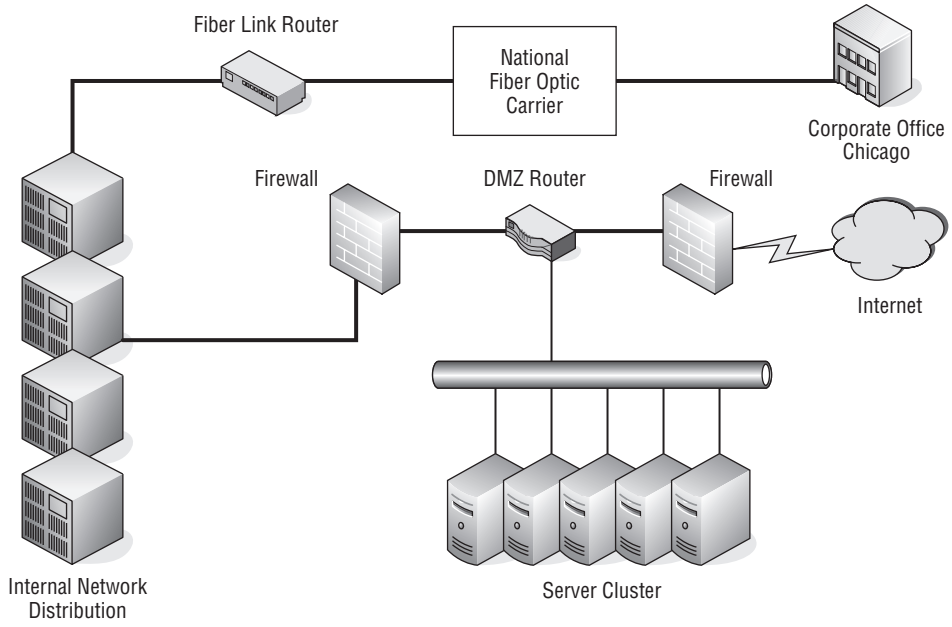


Figure 13-4 A preliminary DMZ plan

[11]DMZ is the acronym for demilitarized zone. It has been adopted by the networking world to mean an area that is not directly connected to any other network segment. It is policed by firewall devices with access policies to prevent a security breach of the network. More on this subject can be found in Chapter 14, ''Network Security.''

[12]Unsolicited network traffic refers to network traffic originated elsewhere over the Internet that has not been asked for. It may be a possible hack attempt. This type of traffic is generally discarded and not allowed into the network. However, if the location is providing services such as web or FTP to the outside world, the unsolicited network traffic must be allowed through to those services. That is the reason they need to be located within the DMZ.

RANDOM BONUS DEFINITION

bridge — A networking node that relays frames among its ports based upon Data Link layer information.

As mentioned previously, the Chicago corporate office is connected to the Denver office via a fiber link by a service provided by a national fiber carrier. There is no need for a firewall because the two connected networks have been secured at both ends of the link. However, since there is another, unsecured path to the Internet, there is a need for a DMZ between the private network and the Internet. You will notice that the DMZ is portioned off with firewalls on both sides that allow for traffic policies to police the traffic flow into and through the DMZ. Policies should be in place to allow users out on the Internet to access services being served by the server cluster in the DMZ. The additional firewall before traffic reaches the internal private network is in place to prevent the possibility of one of the servers being compromised from the Internet and then used for a possible breach of the internal private network. Traffic pattern flow will only allow traffic from the Internet to reach the server cluster and prevent it from accessing the internal private network. Any unsolicited traffic that is originated before the firewall guarding the internal private network will be dropped and not permitted to pass beyond the firewall into the internal private network. Policies have been placed on both firewalls to allow users on the internal private network to access both the server cluster and the Internet since they are originating the network connection.

13.1.1.1.5 Remote User Access

If remote company users need to access the resources on the internal private network, you should consider using a VPN router to allow access through the firewalls. Figure 13-5 shows a typical topology.

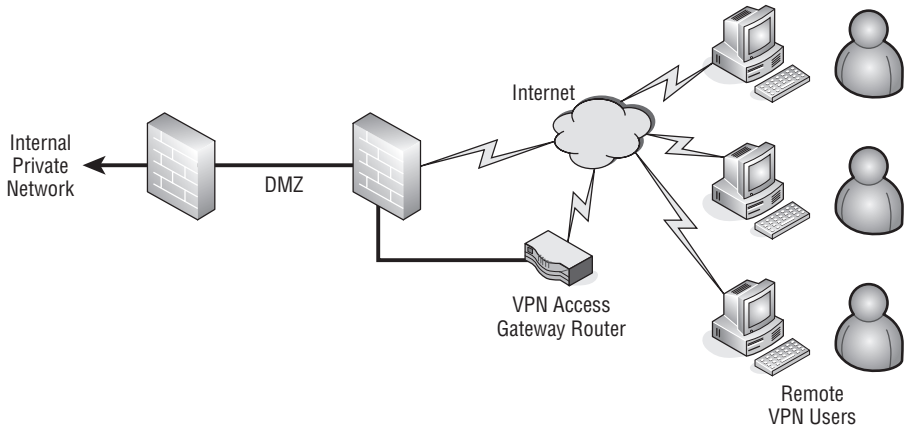


Figure 13-5 A VPN gateway for remote access

The VPN remote users have a VPN client on their PCs that is configured to access the company's VPN access gateway router to permit these users access to the private network and the services that are available to them, as determined by the policies placed on their user IDs. Companies can restrict the services available to these remote users on an individual basis or group basis. Users are authenticated when they access the VPN access gateway router. Chapter 14 discusses authentication and encryption of VPN connections in greater detail. If users are unable to be authenticated due to invalid credentials, they are not able to gain access to the internal private network. Once users are authenticated, their client is assigned an IP address that is routable through the DMZ firewalls into the internal private network. All policies regarding remote user VPN access must be in place to permit traffic from these users to reach the private network.

Now that we have covered the access to the corporate offices and Internet access for the company-based users, as well as remote users able to log in to the facility in Denver, we are ready to discuss the network distribution within the Denver facility. The Denver facility is a new, four-story building. Users have jacks at their desks to accommodate computer access as well jacks for IP-enabled telephones. To ensure worker productivity, provisions are to be made to let them keep working through minor network failures. The idea is to have redundancy for both the IP phone and the computer network access. Each desk position throughout the facility is to have four Ethernet jack outlet boxes next to it. Figure 13-6 illustrates the Ethernet jack outlet, with two network designations assigned to each pair of jacks.

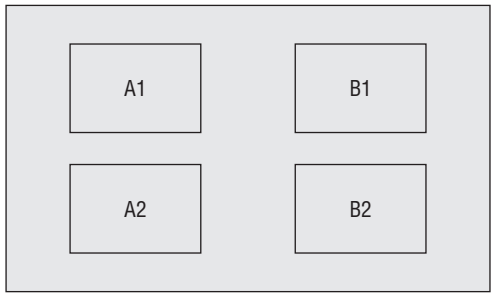


Figure 13-6 The Ethernet jack outlet

13.1.1.1.6 Network Distribution

There are two designations for the networks to be used: A and B. The jacks for each network are labeled 1 and 2. Both the A and B networks are ''live'' at

RANDOM BONUS DEFINITION

browser — An application program that provides a graphical user interface to Internet.

all times and can be used for load balancing within the network. In the event of a network failure, they can provide a means of network redundancy. This will allow users on the failed network to switch to the remaining operational network if needed. The plan is to have users connect one device (such as their PC) to the A network and the other device (such as an IP-enabled telephone) to the B network. This is just an example of a possible scheme to allow for redundancy and network traffic management. There are a variety of methods to accomplish this and the considerations are primarily cost-based. There is a fine line between true redundancy and overkill. Once it is determined how each desk position on each floor is to be wired, we can consider how the distribution is to be made from the network operations area to the wiring closets on each floor. Each wiring closet is to have two switches that are capable of dividing the local network on a particular floor of the building into separate virtual LANs (VLANs) One switch will be assigned to the A network, and the other will be assigned to the B network. This is illustrated in Figure 13-7.

13.1.1.1.7 Network Backbone Distribution

The distribution of the network backbone from the network operations area to each floor is accomplished using a fiber-optic link to provide a high-speed path for the network traffic coming from each floor. Although the fiber-optic link is illustrated as being daisy-chained from a switch on one floor to another switch on another floor, this does not necessarily have to be the case. The switches more than likely do have that capability and daisy-chaining would certainly reduce the number of fiber optic runs in the wiring closets, but a break in any link can potentially affect more than one floor. Another consideration would be to run direct links from each switch in each of the wiring closets to the switched backbone[13] in the network operations area. The wiring to each floor is Category 5 Ethernet cabling. Usually the cabling runs back to the wiring closet, where it is terminated on a patch panel. This permits easy reconfiguration of network jacks to the network node terminating devices in the wiring closet. Figure 13-8 illustrates the distribution of the Ethernet cabling out from the wiring closet to the devices connected to each network node on the floor.

[13]Backbone refers to the distribution of the network out from the core. However, in the day of the multiswitch switched network core, it is difficult to see a ''backbone'' structure per se. The term today refers to the central distribution out from the core, so a network could have a bunch of backbones.

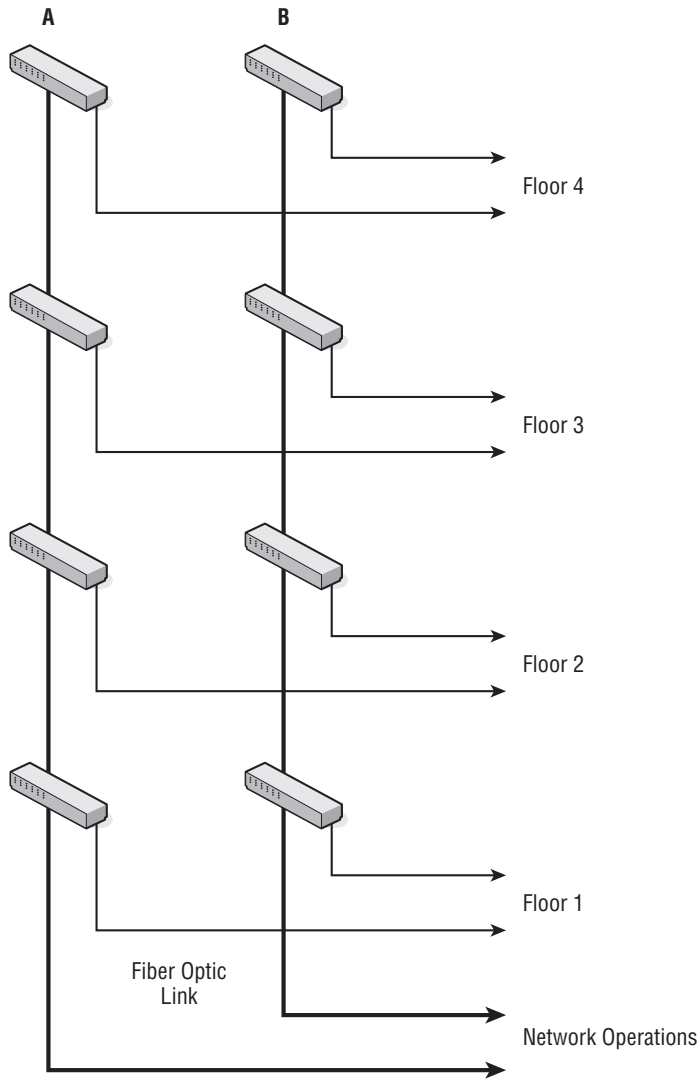


Figure 13-7 The network distribution on separate floors

After being terminated to the patch panel, the network nodes on the floor are connected using patch cables between the RJ-45 Ethernet jacks on the patch panel and the appropriate RJ-45 network jack on one of the network switches located in the wiring closet. Since this is a new installation, it is expected that the wiring closet

ACRONYM ALERT

NOS — Network operating system

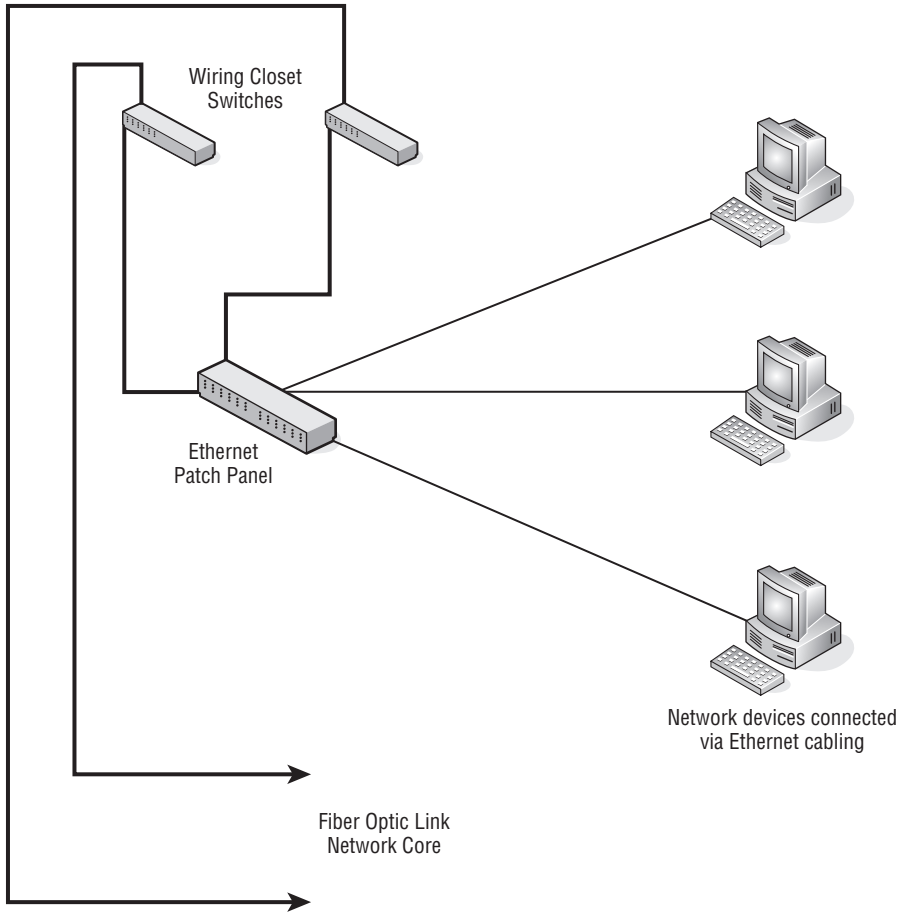


Figure 13-8 Wiring closet network distribution

will be orderly and cables secured and off the floor.[14] Ethernet cables can be bundled and tie-wrapped[15] if needed.

13.1.1.1.8 Wireless Access

So far all the networking that has been discussed is of the wired variety. However, having some wireless network access may be desirable for transient users who may visit the facility and want to use their wireless-enabled laptops.

[14]We have seen wiring closet floors with network cable just strewn all over the place and draped onto the floor. The only way to work on anything was to actually walk on the cables. We highly recommend against this type of wiring system. The chances of intermittent and broken connections are tremendous.

[15]Tie wraps are those plastic straps that are ratcheted when pulled tight. They come in various grades, from very small to fairly thick, and various lengths. They are found in many cabling areas and can be easily cut to reconfigure a cable.

The wireless network is capable of being isolated from the wired network and it may not be desirable to have these users plug into the main network. This will minimize the possibility of a virus-infected laptop spreading a harmful virus to the main network. For this installation, you may want to consider a visitors' area, but only allow visiting users access to the Internet, not to other internal network resources. This can be accomplished as illustrated in Figure 13-9.

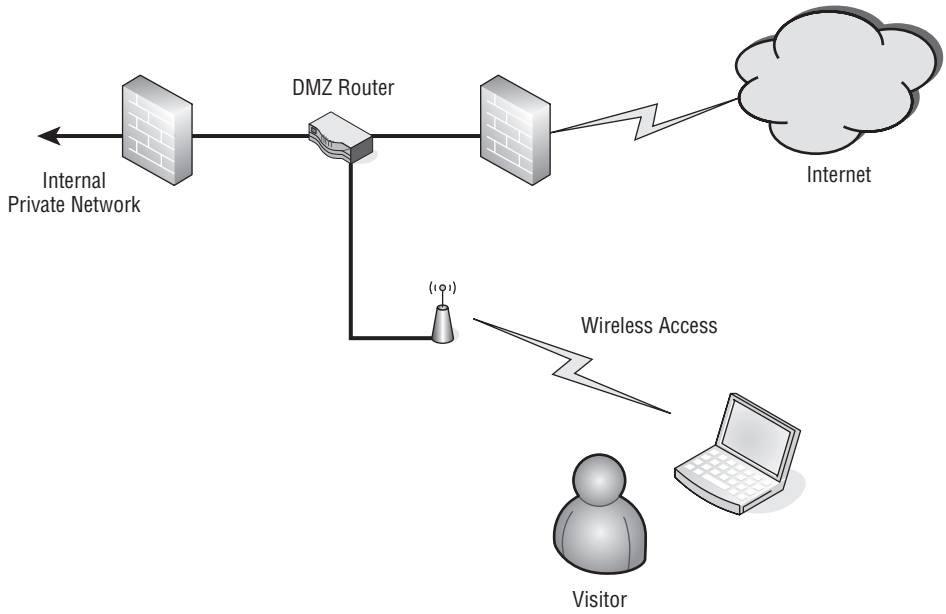


Figure 13-9 Wireless network access

In this figure, the access point from the visitors' area is routed directly to the router located in the DMZ area. Internet access is allowed as a courtesy to visitors to the Denver facility. The reason for the wireless access point being wired into the DMZ and not somewhere on the private network is that it could constitute a breach of the private network's security. With the policies on both firewalls, users in the visitors' area are allowed Internet access but are prevented from penetrating the firewall from the DMZ into the private network. Employees from the corporate office visiting the Denver facility will be allowed to connect their laptops to the network from a secured area. Many companies provide ''drop in'' offices for such visiting employees so that can have access to resources on the private network.

RANDOM BONUS DEFINITION

collision fragment — The portion of an Ethernet frame that results from a collision.

We have now performed the initial planning of the network's design. You have an idea of the overall scope of the project. The project continuously gets refined and developed until the final plan is completed. Each phase through the planning stage must be well documented, and revision control is essential to minimize confusion as the implementation is being rolled out.

13.1.1.2 Finalizing the Plan

The initial planning documentation describes the equipment used and where it should be placed within the facility. Once that has been determined, it is time to lay out the network in regard to addressing and segmentation. We will lay out the VLANs and other subnet segments to be used in various areas of the facility. This is the most critical part of the documentation since it will have major impact on the network's operation and performance.

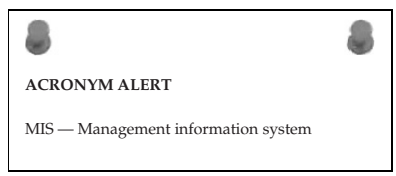
This example uses the network space 192.168.X.X to define the network. The initial plan of the network layout used IP addressing to specify various segments of the network. An addressing scheme has been devised that uses the third octet of the IP address space to indicate a particular routing switch on any particular floor. Table 13-1 illustrates the IP addressing scheme that is to be used in this network.

Table 13-1 IP Addressing Scheme

FLOOR	SWITCH A	SWITCH B
1	192.168.10.X	192.168.11.X
2	192.168.20.X	192.168.21.X
3	192.168.30.X	192.168.31.X
4	192.168.40.X	192.168.41.X

The tens column indicates the floor, 0 indicates the A switch, and 1 indicates the B switch. This is just an example of how with private IP address space addressing you can parse your network where an IP address can be used as an immediate indicator where traffic may be originating from. Can you think of any advantage of doing something like this?

The first thing that should come to mind is the ability to quickly find a problem just by the IP address of the traffic that is being generated. If there is congestion in the network and a flood of packets are coming from a particular network segment, it can be quickly determined by the IP address's third octet. Knowing where the



IP traffic is being originated will aid in rapidly isolating broadcast storms or denial-of-service (DoS) attacks. So careful planning and layout can not only aid with performance, it can also help to troubleshoot network problems.

The final plan should include:

- Complete network diagrams, including IP addresses
- Equipment lists, including their location
- Descriptions of each type of network equipment
- Troubleshooting guides for each type of network equipment
- Lists containing support information for each manufacturer of the network equipment
- A collection location for all warranty statements for all new equipment deployed
- A collection location for all support contracts from the original equipment or other third-party support organizations
- A collection location for all equipment manuals for the network equipment
- Wiring diagrams for each panel deployed about the network
- A collection location for the information dealing with Internet service providers and other telecommunications providers, including data and voice
- A collection location for all license keys that may be required for any of the equipment in the network
- Maintenance/trouble log[16] (used for ongoing support)
- A collection location of all contact information for all staff responsible for the maintenance of the network

The network described in this chapter would have a large amount of documentation associated with it. It may be worthwhile to set aside a portion of the network operations area as a library to collect the hard copy[17] documents as well as files where other information can be kept. The list of finalized documentation is fairly complete, but is not to be construed as everything that needs to be maintained as part of the documentation. Some equipment may come with physical keys, and these too should be collected in an area

[16]A maintenance/trouble log can have various forms. It can be a notebook where trouble events are written or it can be a computerized form. A wide variety of software is available for trouble tracking as part of the IT process.

[17]Hard copy refers to documentation in printed form. Many manufacturers are opting for documentation on CD due to the cost of print media. Whatever form the documentation for the equipment is in, it should be properly stored and filed. An index indicating the documentation that is available and its location is extremely helpful.

where documents are safeguarded, cataloged, and under distribution control, noting where each key is used and what equipment it is used with. The documentation and keys (both software-based and physical) should be kept and cataloged where all network support staff can easily find them.

13.1.2 Network Revision Planning

It was said earlier that planning a network upgrade to an existing network is similar to planning the implementation of a complete brand new network. The major difference is keeping portions of the network running and trouble-free while making changes in order to not affect the operation of the company's business. Usually this is accomplished by building a network segment in parallel and verifying its operation prior to making the cutover to the new network segment. Typically, cutovers are planned during off hours. However, if a company is a 24/7 operation, a maintenance window needs to be scheduled for the cutover.

The following sections review just a few of the possible types of network upgrades or expansions that are typically[18] performed. We will primarily discuss access changes, internal network upgrades, and expansions.

RANDOM BONUS DEFINITION

connection-oriented — A communications model in which stations establish a connection before transmitting data

13.1.2.1 Reworking Network Access

What is involved in a change in network access? Primarily, it is the type of pipe[19] coming from the outside. However, when there is a transition in service, there is also a change in the access equipment to accommodate that type of service. This discussion uses as an example a small company that currently has Internet services coming in on an ISDN service from the local telecommunications company. The company wants to upgrade to accommodate the increase in Internet traffic required to keep the business growing. Just as you would do in the case of a new installation, they will poll their local telecommunications providers to find a service that fits both their needs and their budget. After a thorough

ACRONYM ALERT

FS — Frame status

[18]One could argue that there is no typical network upgrade or expansion and we would have to concur. Many variables are involved, so no two upgrades will be exactly alike. However, the planning will be similar.

[19]A pipe is the type of service that is being provided. It could be DSL, cable, T1, fiber optic, etc. It is the carrier that brings the Internet and other telecommunications services to your doorstep.

investigation, the company's IT department settles on a fiber service from the same telecommunications provider they have their ISDN service with. Figure 13-10 illustrates the setup in preparation for the cutover from an ISDN service to a fiber optic service from the same telecommunications provider.

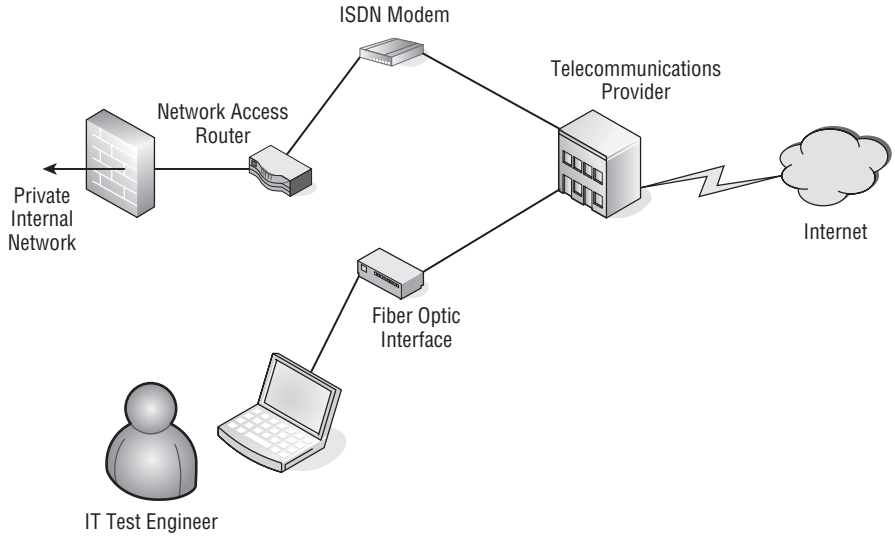


Figure 13-10 Reworking network access

Plans are made to have the telecommunications company bring the fiber cable to the premises of the company while leaving the ISDN service in place. Usually the new service installation includes cabling and the fiber optic interface to convert the fiber signal to Ethernet-compatible signals. Figure 13-10 illustrates that the telecommunications provider has performed its portion of the upgrade of the service. However, instead of cutting over the service on the same day it is delivered and set up, the IT staff wants to first test the reliability of the service provided by the telecommunications provider.

The IT test engineer has connected a crossover cable between his laptop and the Ethernet interface on the fiber optic interface unit. From his laptop, he is able to run a series of tests to verify the operation of the link. He can run burst tests[20] to verify the data throughput of the circuit. Once the IT staff is satisfied that the new access circuit is functioning as expected, they schedule a maintenance window for the circuit cutover. For the scenario of just changing over the service, the cutover is very fast because it only entails removing the Ethernet cable from the network access router to the ISDN modem and connecting it to the fiber optic interface unit.

[20]Burst testing is a method of testing the overall throughput of a network link. It generally refers to the ability to generate enough network traffic to stress the link to its maximum bandwidth capability.

Consider a scenario where the company wants to have a redundant access service to the telecommunications provider in case there is a failure of the fiber optic access link. The plan is to keep the ISDN service as a dial-on-demand service. The ISDN service will only attempt to connect to the telecommunications provider's network if it receives traffic on its Ethernet interface. In this type of upgrade, the network access router may have to be either upgraded for an additional Ethernet interface or replaced with a new router. If the router is being replaced, it could be connected to the fiber optic interface and the IT test engineer could run his tests through the router and out over the fiber optic link. The IT engineer can test the routing through the new network by placing a network device on the interface that is to be used to connect the ISDN modem. With the routing policy set as having the preferred route set to the link with the fiber optic interface, a test can be made to see if the secondary route to the ISDN modem takes over routing traffic when the link to the fiber optic interface is disconnected. A secondary test would be to see if the routing will revert back to the primary link with the fiber optic interface when the link has been restored to operation.

After the operation of the equipment and the new fiber optic link have been tested, a maintenance window should be scheduled for the cutover to the new link and network access router configuration.

RANDOM BONUS DEFINITION

cut-through — A mode of switch operation where frames can be forwarded before they are fully received.

13.1.2.2 Upgrading a Network's Core Routers

Changing over the central core routers of a network is a major undertaking. It requires careful planning and implementation that are as thorough as if these were the initial core routers for the network. The criticality of the situation is that you are taking down a working network for an upgrade.

Planning should include designing the new core, documenting the new installation, obtaining the equipment, installing the equipment and bringing it up as a standalone core routing network, and testing it fully to ensure operation before cutting over from the old routing core to the upgraded one. The timetable for this type of upgrade depends on the complexity of the routing core. The size of the core and the number of network nodes involved will determine the amount of time required for the cutover.

Many times when there is a major change in the core routing network, a company may decide to upgrade the entire network behind it. It may involve not only network node devices but all new cabling as well. Many older installations were wired with older Category 3 cabling. With a major upgrade, the decision may be to upgrade the whole network, including wiring and Ethernet jacks.

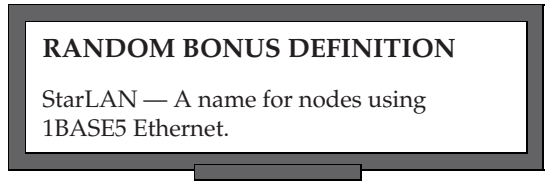
13.1.2.3 Upgrading the Network's Distribution Components

The network distribution system can include older cabling, Ethernet jacks, and network node devices, such as Ethernet switches and hubs. Usually the upgrade of the network distribution components is not a major impact on the current network operations, as a new network distribution fabric[21] can be installed in parallel. This is same process that can be used for an expansion of the network distribution system.

New cabling can be distributed into the areas where the network is either to be expanded or upgraded. With the cabling in place, the Ethernet jacks can be wired in place. Once all the cables are punched down[22] on the patch panel, each run can be tested using Ethernet cable testing tools. With new switches[23] in place in the wiring closet, the patch cables can be placed between them and the patch panel. New cabling, either wire or fiber optic, can be used to terminate each switch back to the network operations area. It, too, will need to be routed over the cable ways between the wiring closet and the network backbone or routing core.

If this process is an upgrade and not a network expansion, it can be done in parallel and users' Ethernet jacks can be moved over to the new network if the IP addressing scheme allows it. To have two parallel networks running and move users from one network to another requires proper routing, as duplicate network addresses would cause routing issues. Planning and documenting the IP addressing scheme is essential to avoid those types of issues.

13.2 Network Supporting Infrastructure



Infrastructure refers to the structural components within a facility in support of the network architecture. Modern buildings make provision for cable ways[24] between floors and from one

[21]The term ''fabric'' usually refers to the threads of the network that are woven to allow network nodes to be connected into the network. It is at times synonymous with the idea of a woven web, especially when full redundancy is employed.

[22]The term ''punched down'' refers to the tool used to push the individual wires of the Ethernet cable.

[23]Many times upgrades include new equipment. New switches can replace hubs or older, less-capable switches. For this example, we are using new switches that have been placed in the wiring closet of the area undergoing the network upgrade.

[24]Cable ways is a generic term used to indicate structural devices connected to the walls, floors, and ceiling of a facility to accommodate the orderly distribution of cabling. The amount of cabling that will be supported by a particular cable way will determine its structural strength.

end of a building to another. Cable ways can be seen passing through walls and can be found above false ceilings. Wiring closets are in areas where there are cable ducts to allow the routing of cabling between floors. A wiring closet may have an overhead cable way that looks like a ladder. Cables are routed over the cable way and can be dropped down between the rungs to various areas in the wiring closet.

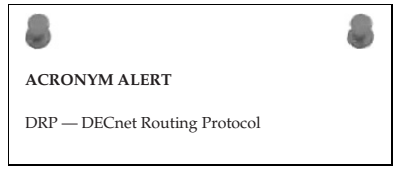
The network operations area is also part of the facility's infrastructure. Adequate space needs to be set aside for the area, as outlined in the initial planning phase. Another consideration for the network operations area within a facility is security on the physical level. Access to the network operations area should be limited to IT staff to prevent inadvertent disruption of network operation by people who are not responsible for keeping the network operational. This limited access should be not only in the networks operation area but throughout the facility, including the wiring closets and other areas used in support of the network, These areas should be secured behind locked doors.

Infrastructure planning is a process that needs to be done in cooperation between the IT staff and the facility's management team. It is not only about floor space but also includes utilities such as electrical and the HVAC support staff. Network planning and implementation requires the cooperation of many departments along with the IT department.

13.3 Budgeting

Budgeting is an important part of the implementation phase. The company must have the financial resources to pay for a new computer network or an upgrade to an existing network. The initial planning phase perhaps does not need to have the financial numbers up front when the initial plan is kicked off. The initial plan takes a directive on what is needed and starts from there. The IT staff can plan the network and list out the equipment required to complete the task. From that they can get cost estimates to feed into the accounting numbers to see if it is possible to fund the project. The idea is to have as precise as a number as possible so that the budgeting is fairly accurate to prevent coming in grossly over budget. Coming under budget is never an issue; however, coming in over budget could cost someone his or her job.

If the project is large and the burden on the budget is excessive, then in cooperation with financial personnel a new budget can be devised to perform the new network implementation in phases. This will spread the load over several budget periods until the full implementation can be completed. This is related more for upgrades, because a company would not undertake the design of a new facility and not budget for completion of the facility. The project



would not be started for a new facility if the company only had the resources to build only the shell of a building. Companies plan new facilities to allow employees to move in and be productive immediately after project completion

However, upgrading older networks in existing facilities can be done on a piecemeal basis. This will allow for budgeting of the upgrade over several accounting periods, thus easing the financial burden. It would take the following considerations, in order: required infrastructure upgrades, improvement of network access to the outside world, core routing on the backbone, and lastly, the network distribution to the devices that are to be connected to the network throughout the facility. Without an allocated budget a network project is unfunded and possibly would only remain in the planning stage.

13.4 Staging

Staging is the period of time between the final planning phase and when the project begins to get under way. The vendor bidding has been completed during the planning stages and the purchase orders begin to flow out to obtain the needed equipment, infrastructure upgrades, and other contracted network services.

If upgrades are required for infrastructure improvements, they must be completed before the project can move along. Having a set timetable and attempting to stick to it allows for each phase of the overall project to meld into the next phase. If one phase falls behind, the timing for the whole project can be jeopardized. Some portions of the project can be worked in parallel, but infrastructure improvement is not one of them (unless there are separate areas requiring infrastructure improvement, which would allow one area to be completed while another area is being upgraded). If an area requiring infrastructure improvement has not been completed, no other network upgrade activity can take place in that area until the infrastructure improvement has been completed.

Most companies do not maintain construction crews for infrastructure upgrades. These types of improvements are usually completed by subcontractors working under the direction of the company's facility management personnel. Electrical wiring, data cabling, and improvements to HVAC in most cases will be bid out to subcontractors. Contractors winning the bids will need to be under signed contract and have their progress monitored to ensure satisfactory completion of the project.

While the improvement of the network's infrastructure is ongoing, equipment that has been ordered will begin to trickle in. It is best to unpack each box and verify that the

RANDOM BONUS DEFINITION

sniffer — Also known as a protocol analyzer.

piece of equipment is exactly what has been ordered and is fully functional. This may require powering the unit and testing it in some manner. The type of device will dictate the type of testing that can be completed without it being placed within a network. At the least, the unit should be able to link to another network device. In many instances it is not likely that full functionality of the device can be tested as part of a bench test. However, bench testing will help eliminate DOA[25] devices or devices that suffer an infant mortality.[26] If the piece of equipment is unable to be placed within its location, then it can be reboxed and placed in storage until the location is clear for its installation. Pre-testing the equipment will minimize the number of surprises you will encounter. Once the network equipment has been received and the infrastructure improvements have been completed, it is time to move on to the next implementation stage: rolling out the network upgrade.

13.5 Rollout

Rollouts are usually synonymous with network upgrades or expansions. They do not apply to a completely new network in a brand new facility. Although some of the stages are similar, no special considerations are required to work around other company personnel with the possibility of causing network outages, as there is with a network upgrade. With an upgrade of a network in an older facility, where there are company personnel who can be affected, some extra planning is required. Such planning should be performed in conjunction with those who would to be affected to minimize the loss of productivity due to the network upgrade. Much of the network upgrade can happen in the background and in areas where other personnel are unaffected. However, in the areas where personnel are affected, it is best to work out a maintenance window to complete the work. If a work area has daily down time after a shift, this work can be completed in the after-hours time periods.

If a whole network is to be upgraded, the network access and core routing areas, along with wiring closet and network distribution equipment, can be upgraded without interfering directly with company personnel. Of course, cutovers of certain network components can and will affect the whole facility, or at least large portions of the network, but do not require the direct interaction with other company personnel. For those types of cutovers, a maintenance window

[25]DOA is dead on arrival. Usually this means the unit did not power on when pulled from the box or perhaps it failed its own self-diagnostic.

[26]Infant mortality is a morbid term and one we prefer not to use. However, it is prevalent in the industry, used to describe a failure of a device shortly after it has been received and powered on.

should be scheduled to be as nonintrusive as possible. Proper notification should be sent out to the whole facility or to those personnel who are to be affected and who will be left without some or all network resources during that period of time.

There are times when a rollout may not go smoothly and either has to delayed and rescheduled or if started, may need to be rolled back due to some impasse that was reached during the maintenance window. Therefore, not only is a careful initial plan required for the rollout but also a contingency plan with a ''what-if''[27] clause to deal with all possible combination of events that could occur while the rollout is going on. Plan for the worst-case scenario and you will be covered. Remember, there are always alligators in the swamp, so be prepared to drain the swamp before proceeding and the alligators will have no place to hide.

13.6 Verification

Whatever can go wrong, will go wrong.
— Murphy's Law[28]

Verification is a kind of nebulous state throughout any network implementation. It is the work done to eliminate as much of Murphy's Law as possible throughout the whole project. As carefully designed as a plan may be, there is always a chance something can go wrong. However, with the proper preparation, these events can be neutralized and dealt with quickly and efficiently.

The verification process should start at the earliest stages of the project. In the early planning stages, you should verify the concepts that are to be implemented into the network design. You should also verify any new products as far as suitability for use within the design. Many times vendors of networking equipment and systems will provide loaners so that their customers can verify a network concept. Part of the evaluation may be a ''bake off'' between vendors to verify which manufacturer's device or system offers better performance and maintainability.[29]

[27] A ''what-if'' is a decision tree element in a flow chart. A rollout plan can be flowcharted to help you see the possibilities that can occur while the rollout phase is ongoing.

[28] Sometimes attributed to Capt. Edward A. Murphy, Jr., an engineer working on the Air Force MX981 project in 1949 who was testing how much deceleration a human can withstand in a crash.

[29] Maintainability is the state of being able to maintain a piece of equipment while it is installed within the network. Things that may be considered include whether the user interface is easy to use and intuitive or if there are things like air filters that need to be replaced at a certain interval. Other considerations include whether the device has built-in redundancy.

Verification should be performed on every aspect that contributes to the overall success of the project. Have the improvements to the infrastructure been completed and done satisfactorily? Usually this is accomplished with a visual inspection and walkthrough with the contractors who performed the work.

RANDOM BONUS DEFINITION

protocol analyzer — Also known as a sniffer, it can perform packet captures, allowing the datagram to be analyzed. Some of the information that can be seen with this device are source and destination addresses, encapsulation, protocol, and data payload, as well if whether it is a whole packet or a fragment of a larger packet.

In the budgeting phase, after a dollar amount has been approved, there is verification that prices quoted in the planning phases are still valid and that billing for received materials and services is correct and within the set budget. Remember, under budget is good and over budget is bad. If price breaks have been given due to a discount for quantity or a new pricing structure from a vendor, then you are good to go. However, if a situation arises when the cost of the project is going to increase, it is best to put on the brakes and verify why there is a cost increase. You may need to get the financial powers-that-be to buy into the cost increase before proceeding any further with the project.

With the design and budget verified, it is time for the materials and services for which purchase orders have been issued to begin to flow in. We already took care of the infrastructure, so the primary concern is that the correct equipment is being received, and if installation services also have been contracted, such as power and data cabling, that the work is being performed on time and as expected. Equipment should be logged in as it is received with the recording of dates, time, model, and serial numbers. Many manufacturers provide warranties for their equipment, but it is up to the customer to provide such information to receive warranty service from them.

ACRONYM ALERT

CAM — Content-addressable memory

During the rollout, there needs to be continued verification of where equipment is to be placed and interconnected with the remainder of the network. It is critical that network addresses are programmed correctly and that the equipment is placed in a subnet address it was planned to be placed in. Once the equipment is in place, performance checks should be made to verify the equipment's operation within the network. Normally verification to the end Ethernet jack in any network segment has been verified by the contractors who performed the data cabling. However, verification for end-user performance is normally performed by the IT staff, either in a proactive manner with a new network rollout or in a passive manner.

NOTE **A "proactive manner" is one where the IT staff actually asks the end user if everything is working satisfactorily. This can include testing the end user applications that require network interaction.**

A "passive manner" is one in which the IT staff performs the rollout of the network project and then sits back and waits for end-user complaints to find the problem areas of the rollout. If there is insufficient staff to perform a full proactive verification of the network, it behooves the IT staff to be selective with whom they verify network operation in a more proactive manner.

RANDOM BONUS DEFINITION

root bridge — The STP bridge with the numerically lowest bridge identifier.

There is constant verification of the documentation every time it is used or reviewed for any reason. If there is something that does not appear correct, mark the document and verify if it is correct and how it was intended during the planning phase. It is not unusual for there to be minor changes that need to be recorded as the network project implementation is being performed. There may be changes in network addressing, configuration changes performed on equipment, and equipment being replaced. Replacement of pieces of equipment that have not failed is rare; however, there may be times when the equipment does not have a capability that is now required within the network. There needs to be a constant update of any changes within the documentation as the project is going on in order to capture the true state of the network in the event that it varies in any manner from the blueprint that was laid out in the planning phases.

13.7 Documentation

ACRONYM ALERT

ASIC — Application-specific integrated circuit

There is nothing more exasperating to any support person than when someone calls seeking help with their network issue but knows squat about it. Okay, perhaps we are being a little harsh here, and you may have inherited a bag of doo-doo from the person who had previously held the position you currently hold, but that excuse still sounds pretty lame to the support person on the other end of the support call. The support person is more than willing to work with you, but please provide them with something they can go on. Just because you have a support contract with the vendor does not mean they know everything about how the device is situated in your network.

There are no excuses whatsoever for inadequate documentation if you were present for the implementation of the network project. Unless the network is very static and did not change, the documentation collected and assembled during the various phases of the network implementation should be complete and include all information necessary to support and maintain the network. This would include any network security passwords used on any of the network equipment requiring administrators to supply passwords to obtain control over their operation. Configuration information for each piece of equipment should be saved in both electronic and hard copy form so they can be reviewed if and when it is necessary. Every piece of information that describes your network's layout and operation should be collected and kept for safekeeping in an orderly manner so it can be easily retrieved when it is needed.

If you are a newly appointed network administrator, your first course of action when taking over the control network operation is to review the documentation for the network and a physical inventory of all devices within the network. This is a long and tedious task, but it is best to perform it while not under the gun when the network is burning down. Systematically collecting and cataloging the network you have been placed in charge of will give you a good understanding of your network and the tools to support and maintain it. If no layout plan is available for the network as it currently stands, attempt to draw one up, including the addressing schemes used. There is no substitute for good and thorough documentation.

POP QUIZ

What are the five major phases of a network's implementation?

13.8 The Final Stretch

Avoid any action with an unacceptable outcome.
— George E. Nichols, Northrop Project Manager

The preceding quote is so true. Proper implementation of a network requires care in planning through each phase of the project. This means not only planning for the obvious but the unexpected as well. If all runs to plan, there is no need for contingency plans. However, when stuff hits the fan

RANDOM BONUS DEFINITION

single-mode fiber — An optical fiber that allows signals in only one transmission mode.

the absence of contingency plans does make for a very unacceptable outcome. Shortsightedness and attempting to take all the shortcuts possible are actions that will ultimately result in an unacceptable outcome. With thoughtful and careful planning, a major network implementation can be completed for both the targeted performance and cost within the time period allocated for the project. Think of it as making a fine stew. Plan out the ingredients, have all the ingredients on hand and ready to go, stage the different cooking phases, and let it all simmer. When you are done, you have an outcome that is rewarding and very satisfying.

AN UNRELATED MOMENT OF PAUSE – MOTHER TURBYNE'S STEW

The thought of stew has me hankering to cook up a pot of some fine stew. It is called Mother Turbyne's Stew because the recipe was obtained from my former cube mate, Jamie Turbyne. We shared some fine cuisine over the years from all the fast food eateries available to us while working the second shift. The recipe made its travels among the staff and everyone seems to like it. You can digress from the recipe as presented here to suit your taste. It is also great to freeze up single-sized portions that microwave well to make for a good and wholesome meal on those late nights at work.

Ingredients:

- **2 bottles of Guinness beer**
- **1 to 1 1/2 pounds of stew meat (beef)**
- **1 medium sized onion**
- **1 pound baby carrots**
- **1 pound frozen peas**
- **2 cloves of garlic**
- **2 tablespoons of butter**
- **Salt and pepper to taste**
- **Water to bring the stew to a consistency that suits your palate**

Preparation:

1. **Peel and dice the onion.**
2. **Add the butter to a four-quart pot and melt over medium heat.**
3. **Add the diced onions. Cook until they appear translucent. (Do not brown them.)**

(continued)

AN UNRELATED MOMENT OF PAUSE – MOTHER TURBYNE'S STEW *(continued)*

4. When the onions are translucent, add the stew meat and brown thoroughly.
5. When meat has been browned, pour in the two bottles of Guinness beer and let the meat and onion simmer in the beer for at least a half hour to make the meat tender. While it is simmering, keep an eye on the pot to make sure it is not rapidly boiling, causing the pan to dry out. Add water if needed to keep the meat covered while it is simmering. Stir from time to time to ensure even cooking.
6. Add the two cloves of garlic sliced into slivers and continue simmering the mixture.
7. When you feel the meat is sufficiently tender, add the package of baby carrots. Continue to simmer the mixture until carrots soften.
8. When carrots have become tender, add the package of frozen peas. The peas can be kept frozen and added to the mixture while frozen. Allow the stew to simmer for about another half hour. You do not want the peas to get mushy.
9. When cooking has been completed, remove from heat and serve with some hearty bread and butter. You have just served up a wonderful meal of Mother Turbyne's Stew.

13.9 Chapter Exercise

This exercise can be done as a class project or as a sole contributor project. If is to be part of a class project, the class should be divided into teams consisting of a project manager and a number of associates. It is the duty of the project manager to divide the planning tasks and the implementation phases between the associates.

The project consists of providing network services to a new facility built next door to an adjacent older building that is to be razed for a parking garage after the move to the new building has been completed. This facility will house approximately 500 employees after the move. Business at this facility is expected to grow by 50 percent in the next year, requiring the workforce to be expanded by 20 percent. The long-term goal of the company is for the facility to house 1,000 employees.

[30]Other brands of beer have been used successfully. Although there is a distinct difference in taste when going to lighter beers, you are encouraged to experiment on your own. However, this is only if you are of legal drinking age for your area. If not, just add beef broth.

Design a network implementation that will accomplish the immediate and future needs of the company for communication, including both data and other services, such as voice and video conferencing.

Draw out initial plans and some detailed plans showing network segmentation for security and traffic patterns. Detailed drawings may include network addresses and the division of the network using subnets and routing between areas. The entire local network is in the private network space, so pick a designated private IP address space and work from there.

If this book is being used in an instructor-led course, the instructor can provide additional information for the requirements he or she is looking for. It is up to the instructor to select the level of detail that is required to submit the project on completion. In a class environment, if time is available, the teams can present their project to the class with their reason for the implementation path they selected.

RANDOM BONUS DEFINITION

Q-compliant — A network node that complies with IEEE 802.1Q.

13.10 Pop Quiz Answer

What are the five major phases of a network's implementation?

1. Planning
2. Budgeting
3. Staging
4. Rollout
5. Verification