Small Company Network

Section Six

“Balancing the load”

Introduction

DISTRIBUTED NETWORKING

Our next scenario incorporates multiple servers and workstations in several locations as a single company network infrastructure (a distributed networking environment). This environment will be based on extending our office network, adding resources and remote locations in order to support up to three hundred employees. In such an environment balancing control and administrative functions over a team of IT professionals becomes important. Prior to this section, each network environment could easily be maintained by a single IT person. The need for multiple IT personnel in this scenario stems more from having multiple locations then multiple servers. The size of an IT department depends mostly on the distribution of resources, complexity of services and the want of a company to provide quality support.

There is a set of standards and initiatives for distributed networking that can be found on the Distributed Management Task Force Inc. (DMTF) website:

http://www.dmtf.org/standards/index.php

These standards cover:

1. Common Information Model (CIM)
2. Desktop Management Interface (DMI)
3. Directory Enabled Network (DEN)
4. Web Based Enterprise Management (WBEN)
5. Alert Standards Format (ASF)
6. System Management BIOS (SMBIOS)

We will be applying many of these standards and initiatives in this section to deploy our small company network in order to maintain a structured and manageable infrastructure.

ITS

Information Technology Services (ITS) is a modern term applied to the department responsible for managing a companies computing services and its' infrastructure. As complexity and size increases, so does the need to provide specialized personnel to support those resources.

There is a direct need to organize the ITS department so that it can perform parallel tasks in union with each other to maintain stability and quickly resolve issues that can hinder the performance of computing services and the personnel that use it to do their job. There is also the obvious need to organize ITS activities in such a way as to gain metrics from services rendered so that management can provision personnel adequately for each task. The overriding vision of each ITS department is to build a network that minimizes user complexity and maximizes productivity.

ITS is commonly broken down into three main groups:

1. Infrastructure/Communications Management
2. Server Management
3. Desktop Management

A network manager usually drives the vision of how a network operates. That person governs the interaction of each group so that they compliment each other and work as a team to provide services. It should be noted that no one group is more important then another -- each group needs to have a balanced and cooperative relationship with each other. This may sound simple but it is common to find groups in ITS that are constantly fighting with each other for the limited funding of projects -- which in turn makes the team look and react in a dysfunctional way.

The network manager must constantly deal with each group in an even manner using the metrics gained by services rendered to legitimize each project and keep all personnel focused on overall operations. Cross training and inter-group coordination will help to provide a basis for a cooperative environment. Maintaining a constant flow of information so that all ITS members are aware of each others duties and current projects also added to teamwork. Believe it or not, these are the most overlooked areas of network management.

SUMMARY

This section focuses on fine tuning both IT staff and distributed network resources so that stability and service can be maximized. While this is no easy task basic standards and initiatives can be applied to make this goal achievable. In building an IT department, keeping everyone on an even playing field will reduce internal struggles for the limited resources that team members must learn to share.

Network Infrastructure

GENERAL

In previous sections, we worked our way up to a single server environment with broadband Internet technology. We connected remote computers using VPN technology and outsourced both e-mail with our web presence. This section moves us into an environment with specialized servers and more robust internetworking communications. While this infrastructure is expensive, it is also more robust and secure allowing for greater control over all of the companies distributed computing resources.

FIGURE 6 - 1. Distributed Locations

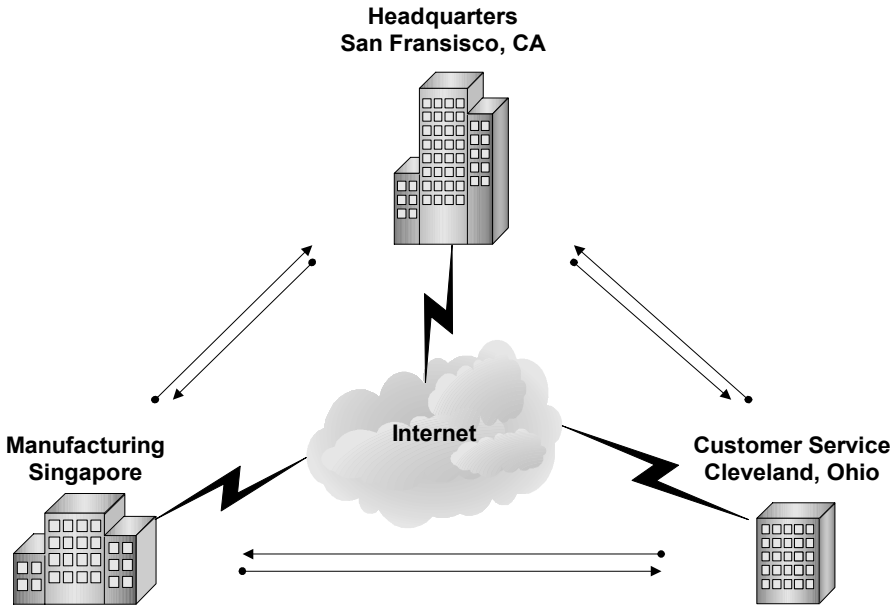


Figure 6-1 represents a high-level "site" topology. Three locations incorporating unique services with the company connecting network resources through Internet technology. There does not need to be large groups of personnel in each location. In our scenario, headquarters can be just a couple of floors in a given building. Customer service can be a single floor in a given building. Manufacturing can be a small building with contracted workers. This site topology can reflect both small and large company assets. We will describe our next level site by site to give you a closer look at how this topology works.

NETWORK STRATEGY

Each site requires at least one server to act as the account database repository - this enables quick logons and local account authentication. Each site must be built to act independently but also be able to interact with their sister sites. Services that are common to all three sites should be located in a secure site (also known as a collocation[122]) so that when any one site losses communication the other three sites can continue unhampered. The basic concept is to localize high-bandwidth resources at the site level while placing low-bandwidth shared resources in a place that is both secure and independent of any one site.

There is no rule of thumb that can be used for every business profile but I will offer the following as a guideline to building your companies strategy:

- **Local Servers**
  - Domain Controllers
  - Site E-Mail
  - Special resources (servers that provide a unique function per site)
  - Database Servers
  - Local User Storage
- **Collocation Servers**
  - Schema Managers
  - Common Database Servers
  - Web Farms
  - Master E-Mail servers
  - Backup User Storage
  - Disaster Recovery
  - High Security Services

Lets look first at common servers located at each site:

FIGURE 6 - 2. Common Site Resources

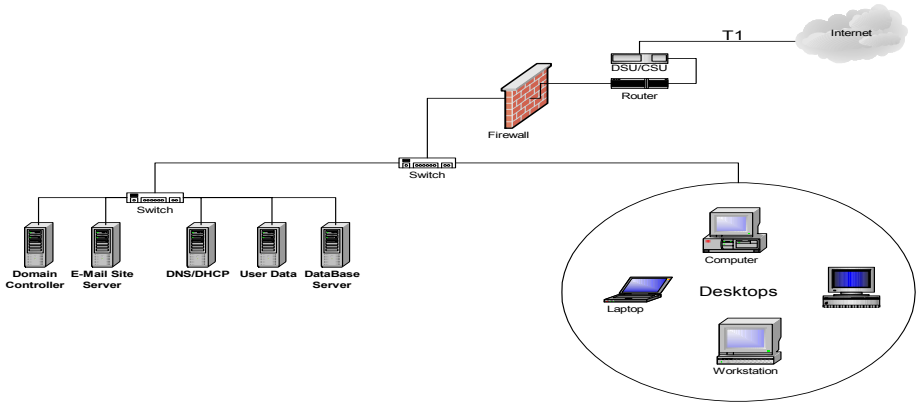


Figure 6-2 is a simplified topography diagram depicting the basic network structure that could be found in each site. You can begin to see the logical separation of the three IT groups (infrastructure management, server management and desktop management). The Infrastructure management group is responsible for maintaining the Internet connection

122.In general, collocation is moving or placing things together, sometimes implying a proper order. On the Internet, this term (often spelled “collocation” or “co-location”) is used to mean the provision of space for a customer's telecommunications equipment on the service provider's premises. For example, a Web site owner could place the site's own computer servers on the premises of the Internet service provider (ISP).

(T1 hardware and firewall hardware/software), switches and cables. The server group is responsible for maintaining all common network services (DNS, DHCP, user data, account management-mail services, and database management). The desktop management group is responsible for each workstation (software and hardware), configuration with network services, printing services, and basic software training.

You will notice a few changes to our previous network resources. We have put in place a Firewall (special software and hardware) to protect our network resources. We have also put in place a T1 circuit for Internet (and possibly telephone) resources. We have also provisioned server hardware to provide DNS and DHCP services. Of course we have included additional servers to provide local E-mail, user data and database resources -- these are dependant mostly on the needs of the business and the availability for provisioning the hardware and software.

DIRECTORY SERVICES

Using a directory schema as the technology that binds our three remote sites, it is important to standardize network services with one common vender. Microsoft (AD), Oracle (OiD), and Novell (NDS) are leading contenders in directory technology[123]. Each provides LDAP[124] compliant directory databases that promote a seamless integration of accounts and asset management. While they can be integrated with each other, each works best when it is independent of any third party directory software. Unlike previous domain or zone technologies (such as NT or Apple), a directory is a hiarchial *object oriented* depiction of network resources that can be designed to closely reflect that organizational structure of a company. Using such a hiarchial object oriented format simplifies administration and improves structural integrity of the network's resources. For medium to large scale network installations the use of a directory technology can enhance the management and maintenance of computing assets across the board.

While the long term gains in using a directory schema is great, the up-front cost is high. In designing and building the directory schema, there is the definite need to experiment and test your schema prior to implementation. There is also a need to have some parallel testing environment in place so that each adjustment made to the production schema is fully understood. Since the directory schema can have great effect on the companies computing infrastructure, each implementation of a policy or object should be tested so that negative effects can be minimized. Down the road, libraries of policies and documentation supporting potential changes will help to reduce the administrative overhead

123.**AD** - Active Directory is Microsoft's trademarked directory service, an integral part of the Windows 2000 architecture. **OiD** - Oracle Internet Directory is a standards-based LDAP directory which leverages the scalability, high availability and security features of the Oracle database. **NDS** - Novell Directory Services is a popular software product for managing access to computer resources and keeping track of the users of a network, such as a company's intranet, from a single point of administration.

124.**LDAP** (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.

and automate much of the IT workload (including OS and application installations along with pushing self-healing[125] applications to the desktop).

Finally, in building a directory-based networking schema, we are able to minimize the need for multiple domains in our network. We gain greater security and centralize authority so that departments and individuals are required to go through ITS to utilize network bandwidth. For all of the resources to work well together, there must be a centralized authority to oversee the use of limited network resources so that everyone benefits equally - a directory technology can provide such an environment.

SOFTWARE LICENSING

Managing software and applications in a distributed network environment can be difficult. There are limitations on what software versions are legal in foreign countries as well as language issues and intellectual property restrictions that need to be assessed. Further there is the need to limit access to distribution media so that unlawful copies of software is not permitted.

Distributing software by pushing the applications across the network from a central location and not allowing users to handle distribution media has become very popular. There are packaging and distribution applications independent from directory software and each application has its merit. It is important to balance cost with value -- directory enabled distribution software is less costly then specialized packages but may tend to add unforeseen complications to network administration.

Benefits of pushing applications using distribution software does help to minimize the personnel needed to maintain physical application libraries and can help to prove *due diligence* when confronted with software license auditing as well. In fact, a well conceived process can greatly reduce operating costs and promote greater uptime for users. Distributed packages can also help to ensure freshening and facilitate an automated process for applying hotfixes and service packs.

SUMMARY

Network infrastructure supports much more then just communications and collective use of peripherals. It must support processes that ensure complicity of software distribution and freshening as well as versatility in the movement of user accounts and resources. A small business can grow quickly and so should its computer resources. Growth should be an extension of the automated distribution methodology as well as the consolidation of organized processes. A well conceived network strategy includes a vision of how the network should be in a larger environment. Of course cost and value must be balanced to ensure that the company does not over extend its assets and keep it from being able to change direction if the business model so designates.

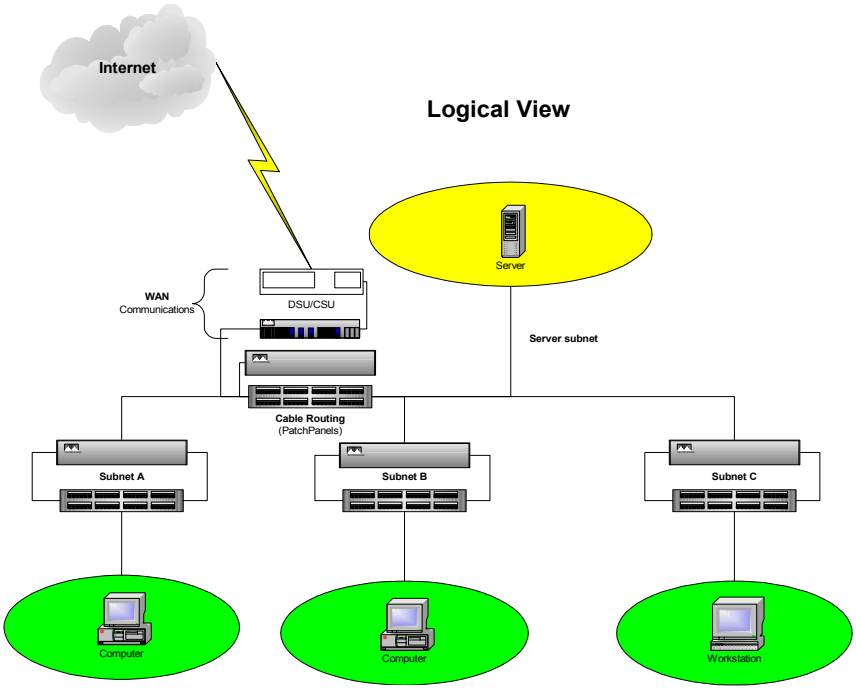
125.In information technology, self-healing describes any device or system that has the ability to perceive that it is not operating correctly and, without human intervention, make the necessary adjustments to restore itself to normal operation. Because users of a product may find the cost of servicing it too expensive (in some cases, far more than the cost of the product itself), some product developers are trying to build products that fix themselves.

Infrastructure/Communications Management

Primary to the coordination of communications management is the need to establish an infrastructure that promotes collaboration between our three locations. Uniformity in all three sites can promote quick and standard solutions to common networking problems. Basically, the goal is to keep all local infrastructure for each site as much the same as possible. There will always be some significant differences (specialized services and unique hardware) in operations but the skeleton infrastructure should mirror each of the other sites.

There should be a person or group dedicated to the maintenance of *infrastructure*. Depending on the size of the network whoever is responsible for infrastructure should manage any/all outsourcing of services (cable installations, router installations and so on) as well as coordinate local connectivity with all other sites.

FIGURE 6 - 3. MAC Group



MAC GROUP

Sometimes referred to as the MAC[126] group, personnel assigned to the communications department (or group) are responsible for maintaining all connectivity devices (usually referred to as network appliances). Routers, CSU/DSU[127], firewalls, switches and patch

126.Media Access Control

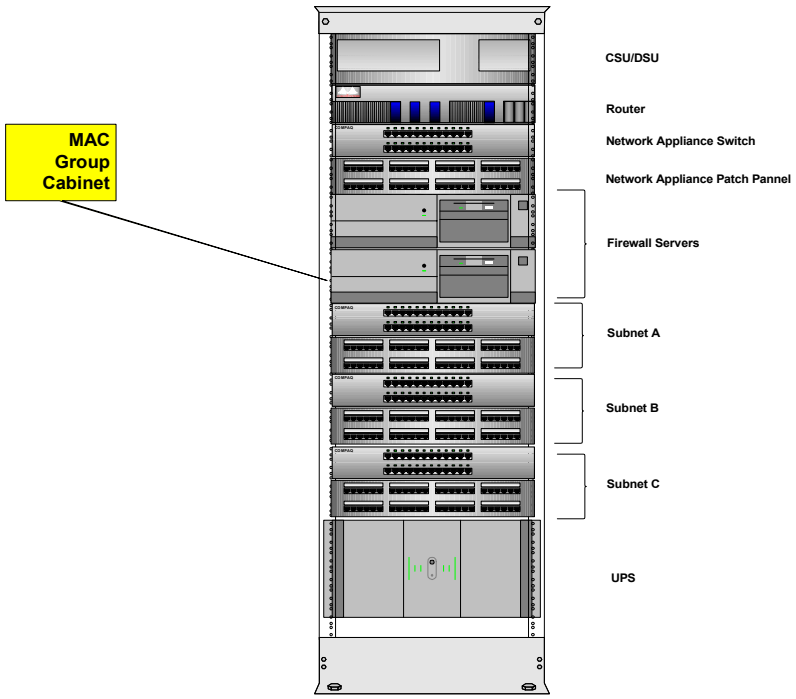
127.A CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device about the size of an external modem that converts a digital data frame from the communications technology used on a local area network (LAN) into a frame appropriate to a wide-area network (WAN) and vice versa.

panel connections (including wall plates and cables) make up a good portion of the responsibilities associated with this group. Topology issues, general network strategy, maintenance and upgrading resources are a never ending battle. The only time other departments notice this group is when problems arise -- basically it's a thankless job.

Coordination of upgrades and modifications should be done so that all three sites maintain the mirrored technology. This requires a central authority that should monitor local topologies and keep an intimate knowledge of personnel and resources for each of the sites so that there is no surprise down the road.

CABINETS

FIGURE 6 - 4. Cabinet (a.k.a. Rack) View



The physical layout of equipment can be positioned in a logical format. By doing so you help to simplify the troubleshooting process and improve uptime[128]. Most cabinets (also know as racks) evolve through time and get fairly messy over the years. If you plan well and leave open space for growth you can maintain organization and uptime. This is yet another battle that must be fought. People who don't visualize growth have little concern for allowing for empty space to be there -- especially when cabinet space is expensive to buy and maintain. There needs to be some project planning that takes into consideration the cost of maintenance and downtime related to modifying cabinet space

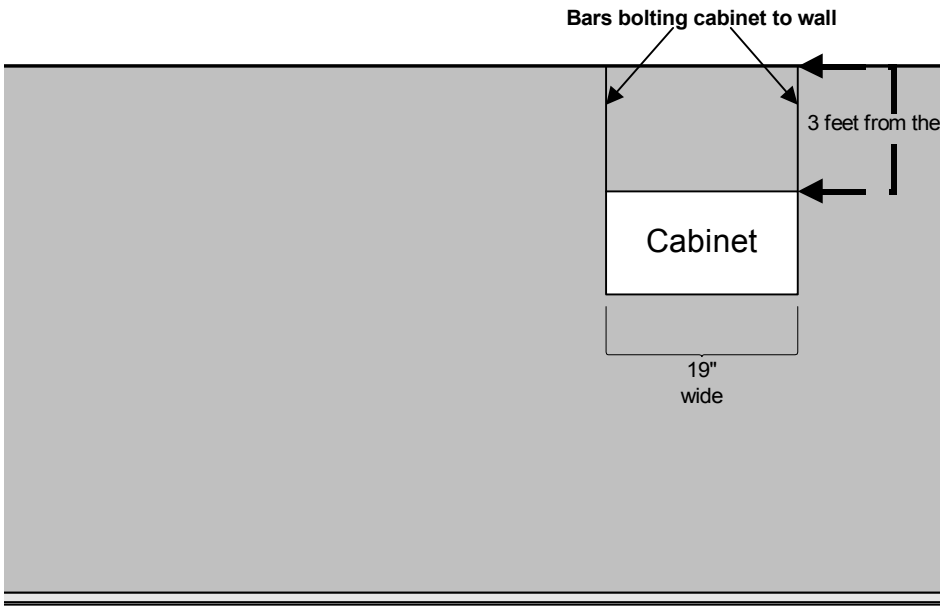
128.Uptime is a computer industry term for the time during which a computer is operational. Downtime is the time when it isn't operational. Uptime is sometimes measured in terms of a percentile. For example, one standard for uptime that is sometimes discussed is a goal called five 9s - that is, a computer that is operational 99.999 percent of the time.

(which also must allow for hardware upgrades and equipment replacements as well) so that a balance can be struck between over planning and cost cutting. It is the balance between both that will help to develop the best plan for growth incorporating cost savings.

In our small company, one Infrastructure cabinet is usually enough for each site allowing for up to 192 devices overall. This incorporates a 48 U cabinet with four 48 port subnets, two firewall servers, a high end rack mountable UPS, router and csu/dsu. Common devices share the first subnet (also know as network appliances -- servers, routers, backbone to switches, etc.) and each additional subnet is broken down into various physical locations (either buildings or rooms) so that network traffic is localized. Having a spare switch in case of hardware failure is a great idea.

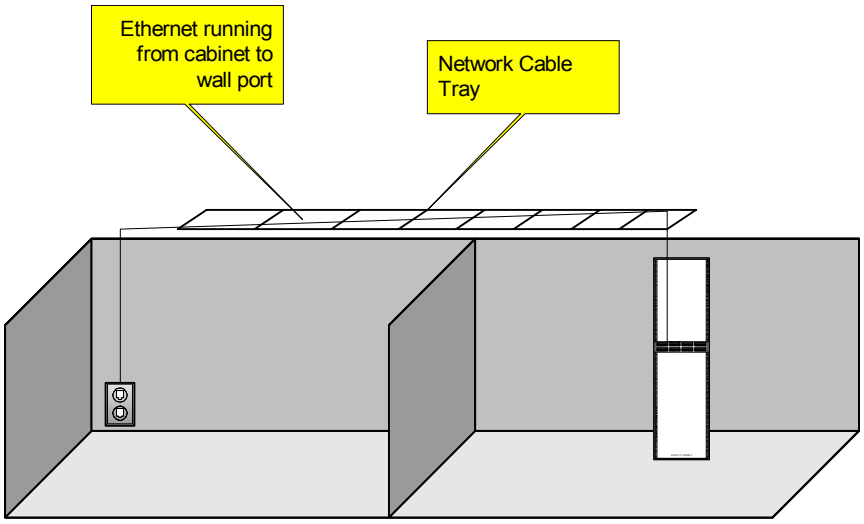
Cabinets should be fastened to the wall so that it can not move during natural disasters and all components should be bolted to the cabinet.

FIGURE 6 - 5. Cabinet Position to Wall



The mounting bars (connecting the cabinet to the wall) should be at the top of the cabinet to provide the greatest stability with the base of the cabinet securely bolted to the floor. There should be 3 feet behind the cabinet so that maintenance can be easily performed if hardware needs to be replaced or repaired. There should also be three feet in front of the cabinet as well. Proper ventilation is important so that the hardware can breathe and the temperature can be maintained at a safe 70 degrees Fahrenheit.

FIGURE 6 - 6. Cable Run



Above the ceiling, cable trays are placed so that the ethernet cable can be safely ran. By safely, I mean that there can be no bending, crimping or cutting of the cable which would lead to poor (or no) communications. Usually cable trays have less then 13” of free space between each cross bar so that the cable does not sag. Wire tires are usually applied periodically throughout the cable tray so that cables are not pulled to tightly or get twisted when the cable is drawn during installation. Ethernet is usually pulled down inside the wall and then brought our through the wall plate and connected to female ports on the wall plate.

CABLE COLOR CODES

Ethernet (cat5) cabling usually comes in two flavors:

- T-568A
- T-568B

T-568A (see figure 6-7) is supposed to be the standard for new installations, and T-568B is the alternative. However, most off-the-shelf data equipment and cables seem to be wired to T568B (see figure 6-8). It is important to make sure you follow one (and only one) of these standards when installing ethernet.

FIGURE 6 - 7. Wire color coding (type A)

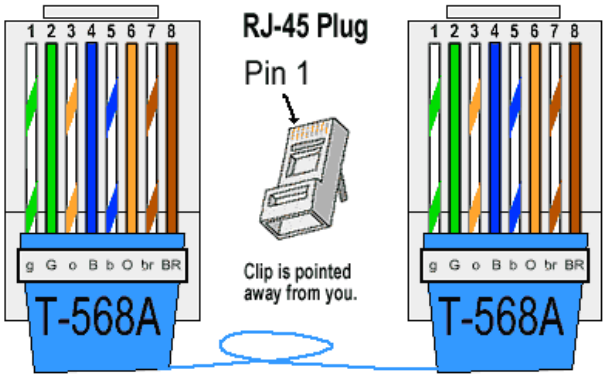
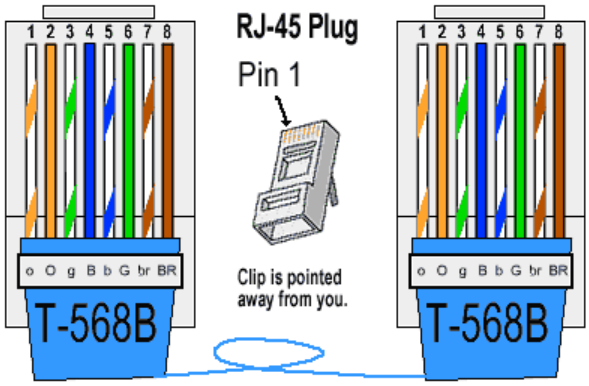


FIGURE 6 - 8. Wire color coding (type B)



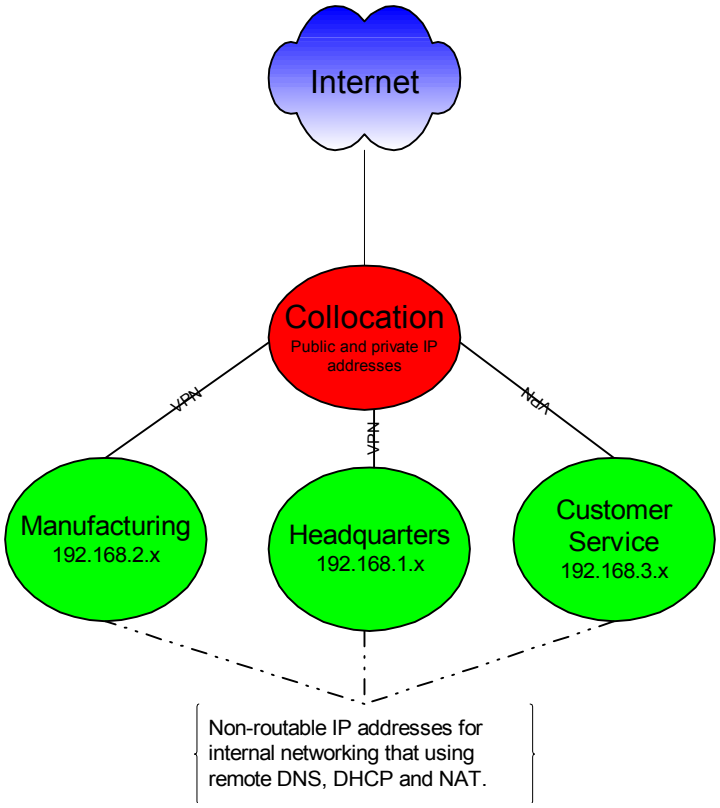
SUBNETS

Each site maintains a class C subnet (with up to 254 IP addresses). If the site needs to expand then each site could either supernet[129] or expand to a class B subnet. Either way, the network subnet can grow with the site and expand to a much larger size. The goal is not to make the network too large or too small, but just right (as covered in previous sec-

129.Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class. The original Internet Protocol (IP) defines IP addresses in four major classes of address structure, Classes A through D. Each class allocates one portion of the 32-bit Internet address format to a network address and the remaining portion to the specific host machines within the network. Using supernetting, the network address 192.168.2.0/24 and an adjacent address 192.168.3.0/24 can be merged into 192.168.2.0/23. The “23” at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses. Supernetting is most often used to combine Class C network addresses and is the basis for most routing protocols currently used on the Internet.

tions of this book). Again DHCP is the key to flexibility and organizational management. Routable addresses should be managed from the central collocation and all external DNS records are best defined there. In this way you limit the vulnerability of your local assets and localize potential damage that outsiders can inflict. Each site is given servers on the collocation to post their web pages and sharable information while internal resources (those local to each site) are masked by non routable resources. The local firewall acts as a gateway to the collocation and the collocation uses yet another firewall to both combine all site gateways (also to be referred to as bridgehead servers) and the outside world. The end result is a two tiered firewall security system with the added advantage of using NAT to further mask local IP addressing schemes.

FIGURE 6 - 9. IP Addressing



As you can see in Figure 6-9, the collocation acts as the binder to each of the local sites. The local firewalls link each site to the collocation and the collocation firewall to the outside world. If someone tried to break into the companies network they must first get past the collocation firewall and then the local network firewall. This security strategy applies to company subnets that are well hidden from the outside world. If a hacker gets the IP addresses of the local firewall (or gateway) they can work their way in from that point as well. It is therefore imperative to limit access to each local site using routing pools that restrict access to only those addresses verified by the collocation firewall. There must also be someone who is constantly monitoring collocation activity to verify that no one has hacked into any resources.

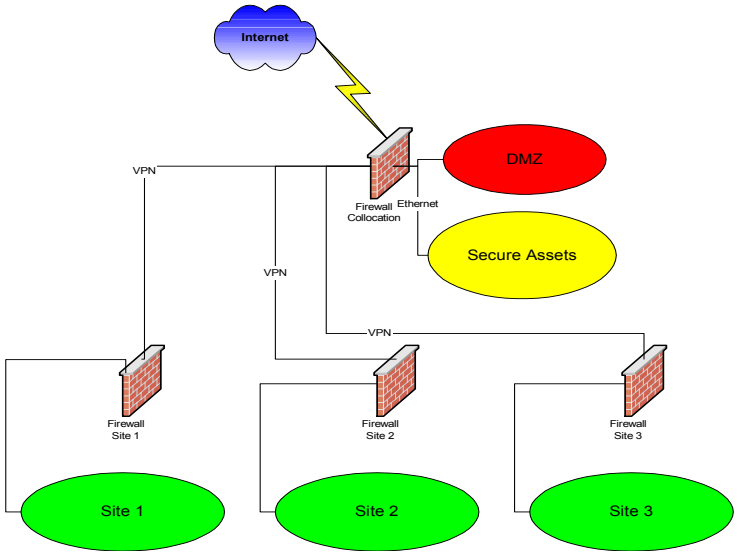
CENTRALIZED DNS

Each site maintains a remote DNS server that acts as a backup DNS table and local DNS resolver. All sites focus on one primary DNS server found at the collocation. This DNS server also pushes DHCP to remote DHCP servers. Each site can continue to provide local network services even when the central DNS (found in the collocation) is unavailable. Synchronization will occur when communication is reestablished. This strategy allows for the company to be flexible in expanding sites and services. It also allows the company great flexibility in severing ties (selling off parts of the company) without causing any real network downtime due to re-configuration.

SECURITY

As you can see security is managed locally and centrally. Firewalls can be operated through the corporate headquarters via the collocation and site firewalls. Intellectual property can be maintained locally and synchronized with the collocation in secure servers. Data to be shared with the outside world can be posted in the DMZ at the collocation. If someone hacks the web farm in the DMSZ, the system can be reloaded from secure servers quickly and headquarters can update firewall security to protect against further encroachment of hackers. Using more then one vender for your firewall resources (say a CISCO PIX[130] for the collocation and Checkpoint Firewall 1[131] for the site firewalls) will increase security by making each layer of security unique and require that the hacker break more then one firewall technology to gain full access.

FIGURE 6 - 10. Multi-Tiered Firewall Security



130.The Cisco PIX Firewall Series delivers strong security in an easy-to-install, integrated hardware/software firewall appliance that offers outstanding performance. Cisco`s world-leading PIX Firewall family spans the entire user application spectrum, from compact, plug-n-play desktop firewalls for small/home offices to carrier-class gigabit firewalls for the most demanding enterprise and service provider environments.

131.Checkpoint FW-1 has been the firewall market leader since shortly after its introduction in 1994/95. Its well designed GUI interface was, and still is, the best visual interface to any firewall product.

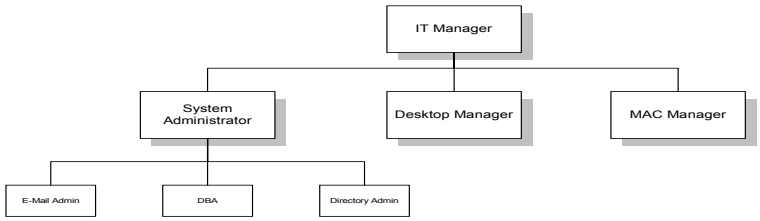
Server Based Central Solutions

THE SERVER GROUP

The site server group provide local support for *common use* computers and peripherals and share in the operations and management of the collocation resources. This ensures consistency and 24 hour staffing (for the collocation resources) with a minimum of cost. The server group maintain file servers, NAS[132], print services and disaster recovery procedures. Members of the server group are also deeply threaded with desktop support personnel in providing remote installation services, directory policies and overall management of networking services.

Each member of the server group usually has a strong understanding of TCP/IP[133], computer networking and operating systems deployed at the site. Individual members also maintain specialized skills (such as E-Mail administration, database administration (DBA), Directory administration AD, NDS, DiA, etc.). An SysAdmin usually heads this group and acts as liaison for the server group with other departments and groups on and off site.

FIGURE 6 - 11. IT Server Group Organization Chart



While each organization may differ on the way they set up groups and responsibilities, Figure 6-11 gives you a general approach to how most companies organize their IT department. The larger the company -- the more personnel fit into each box. The MAC

132.Network-attached storage (NAS) is hard disk storage that is set up with its own network address rather than being attached to the department computer that is serving applications to a network's workstation users. By removing storage access and its management from the department server, both application programming and files can be served faster because they are not competing for the same processor resources. The network-attached storage device is attached to a local area network (typically, an Ethernet network) and assigned an IP address. File requests are mapped by the main server to the NAS file server.

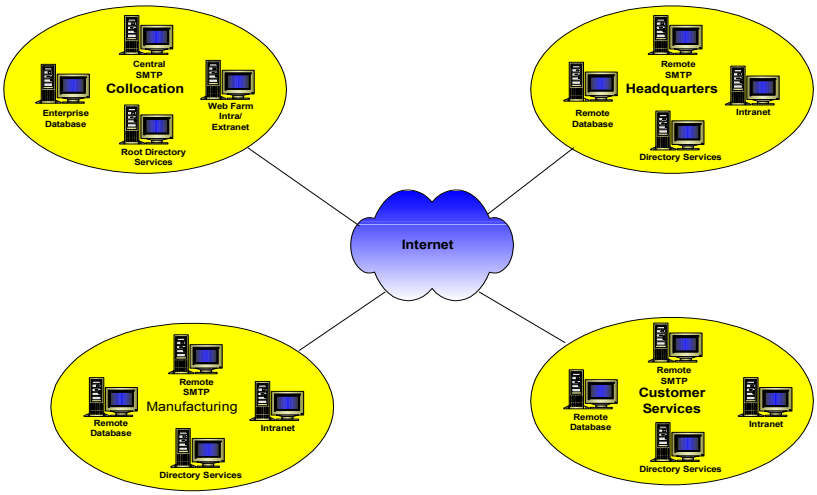
133.TCP and IP were developed by a Department of Defense (DOD) research project to connect a number different networks designed by different vendors into a network of networks (the "Internet"). It was initially successful because it delivered a few basic services that everyone needs (file transfer, electronic mail, remote logon) across a very large number of client and server systems. Several computers in a small department can use TCP/IP (along with other protocols) on a single LAN. The IP component provides routing from the department to the enterprise network, then to regional networks, and finally to the global Internet.

and Desktop Management groups have also been added to Figure 6-11 to show their relationship with the Server Group. There is a need to maintain strong communication ties between each of these groups so that there is a consistent and structured approach to maintaining network continuity. Often cross training occurs between group members so that personal relationships can develop and expand intergroup cooperation.

SERVER RESOURCES

It is important for each site to share resources with other sites in the company as well as operate independently. A site should be part of the collective (the company network) but be able to continue operating when the corporate network is down (or even transition to another company seamlessly if the site is sold off). By maintaining a common "enterprise" site (such as the collocation), each local site can maintain remote server based resources that synchronize with the common site. This brings up the need to emulate common resources found at the collocation at each site. Most enterprise solutions (E-Mail, database and Directory services) can be deployed in a hiarchial configuration allowing for a variety of connection schemes to anchor remote sites to a common location.

FIGURE 6 - 12. Server Interdependencies



SMTP[134] services are directed from a central point (the collocation) and redirected to each local SMTP server (E-Mail Server). As long as there is communication between the Collocation and each site mail in transferred appropriately. If a site is down for any reason, e-mail is collected at the collocation and then synchronized with the local SMTP server once communication is re-established. This ensures that company communications is maintained with the highest level of security and system failover with added support from the collocation provider NOC[135] personnel to assist.

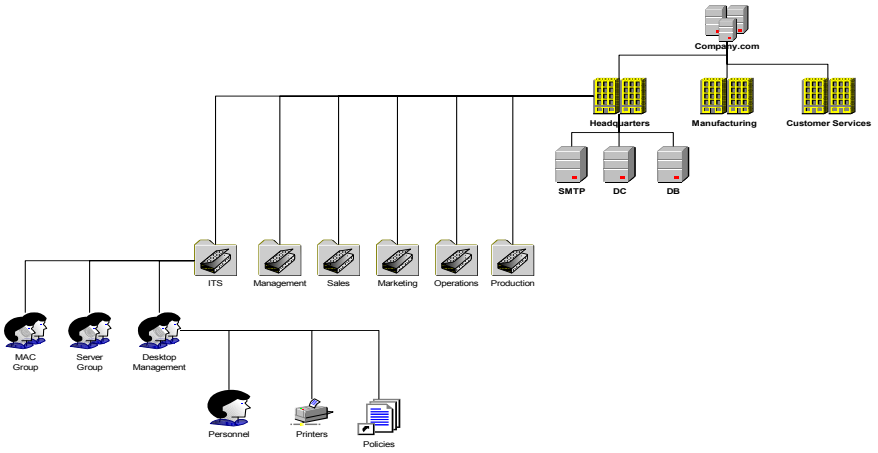
Each remote site maintains data and services that are independent of other sites and synchronize the data with the collocation resources. In other words, remote database tables

are synchronized with the enterprise database, Intranet information is synchronized with the collocation web farm (as either departmental or site sections of the company Intranet schema) and Directory services are replicated across the company.

DIRECTORY ARCHITECTURE

Managing resources through a “Directory Schema” (such as Microsoft’s Active Directory or Novell’s NDS) assets become objects and are managed through “policies”.

FIGURE 6 - 13. Directory Tree (schema)



In Figure 6-13, headquarter’s ITS groups are mapped out to show the relationship within the global organization. First you have the root of the forest (the Company.com domain). Under the domain object are three site objects (headquarters, manufacturing, and customer services). These sites can either be sub-domains or simply organizational units within the root domain (normally subdomains would be applied here). Server resources would be shared throughout the site. Organizational units would be formed

134.SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server. Most mail programs such as Eudora let you specify both an SMTP server and a POP server. On Unix-based systems, sendmail is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server and also comes in a version for Windows NT.

135.A network operations center (NOC) is a place from which a telecommunications network is supervised, monitored, and maintained. Large enterprises with large networks as well as large network service providers typically have a network operations center, a room containing visualizations of the network or networks that are being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the networks. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and domain name management, performance monitoring, and coordination with affiliated networks.

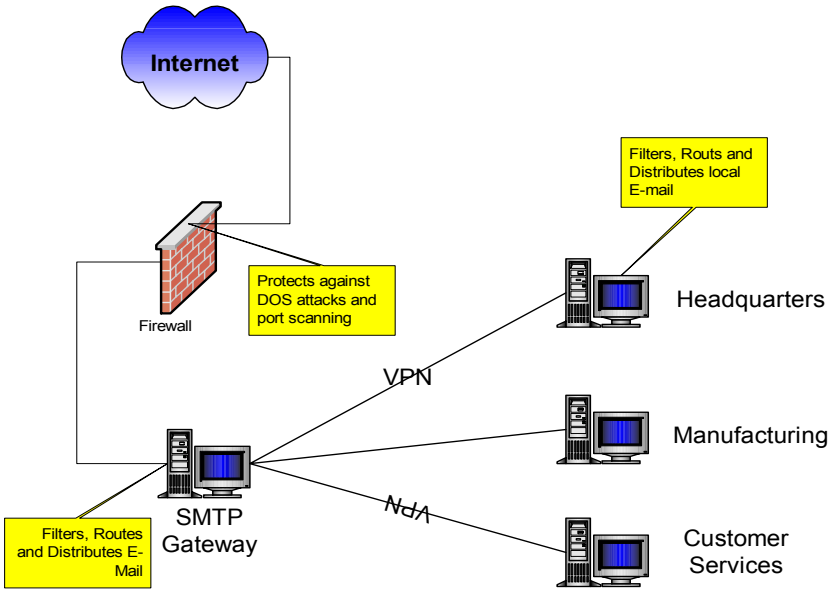
for each of the departments at the site (these may change due to the functionality of the site). Within each organizational unit is the groups that can be found there (such as MAC, server, and desktop management groups). associated with each group is their network policies (what rights they have to network resources), shared devices (such as printers) and members of that group (user profiles).

Software licensing, remote installation services and many other remote management services can be administered through the directory service. This greatly enhances remote administration and allows for the control of application licensing, desktop environment testing and versioning of OS and software (service packs, hotfixes, etc.). In a directory domain, all computers can be conditioned and updated by the system administrator (either per site or from headquarters). This helps to ensure security and prevent software theft. Since software is distributed across the network no physical media is available for people to copy and take off site.

E-MAIL (SMTP)

E-mail (as stated previously) is distributed from the SMTP gateway located in the collocation. Here is where you would also filter spam and e-mail viruses. By forcing all e-mail to come through one central point you have greater uptime and availability. A SMTP gateway also minimizes disaster recovery procedures.

FIGURE 6 - 14. SMTP Routing



DNS manages SMTP servers through "MX[136]" records. The MX record would point to the SMTP gateway. Each of the site E-mail servers would set up their routing tables to

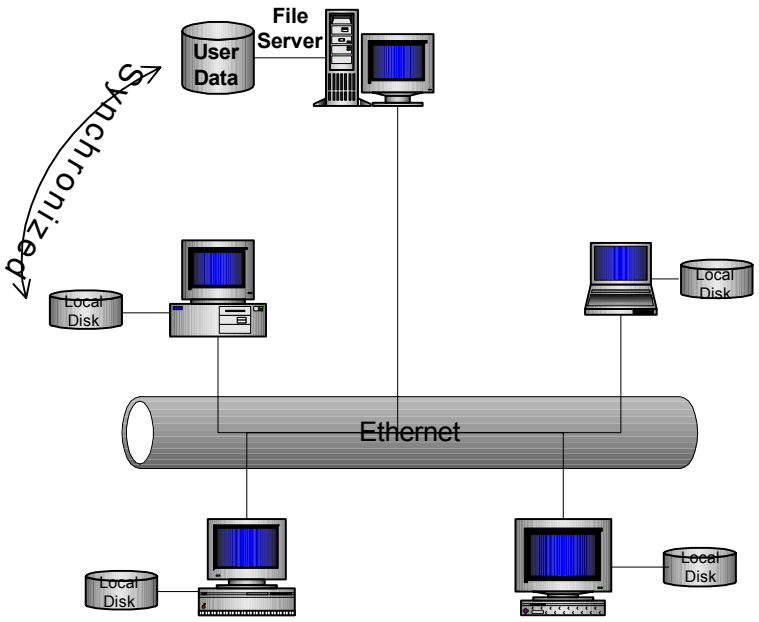
136.An MX record is the Mail Exchanger record. This tells the world what your mail server IP address and name is so that you can receive SMTP e-mail.

point toward the gateway for E-mail traffic. Internal e-mail can be routed either through the gateway server (which would allow for a single antivirus scanning point) or directly from one site server to the other. In our small network it would not be much difference in speed to go either way. If this were a larger network you might consider installing E-mail antivirus software on site servers as well.

FILE SHARING

Using File Server technology (either dedicated network appliances (NAS) or traditional file servers), user data can be managed and backed up from select locations on the network. This reduces backup costs and the chance for data loss due to workstation hardware failures.

FIGURE 6 - 15. Local and Server File Sharing and Synchronization

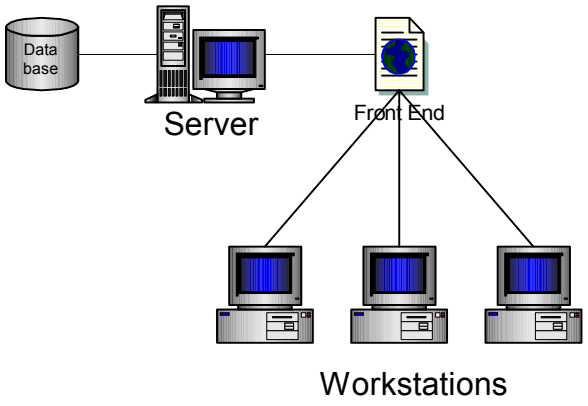


Folders on each workstation are sychronized with folders on the server so that data is up to date in both locations. If the server becomes unavailable then the data on the local workstation hard drive can continue to be modified and sychronize any changes once the server is back on-line. It is important to ensure that the file server can support multiple operating systems (Apple, UNIX, Linux, and Microsoft) so that there is the greatest flexibility for expansion. The downside to network attached storage is that it takes up network bandwidth and relies on network stability to provide access. The upside is that it is fairly inexpensive and easy to put in place. There are many variations on network attached storage and we will see that cost can go up fast as the need for uptime becomes more and more important. As for now, this configuration allows for redundancy without thigh cost and works well in small to medium size companies.

DATABASE MANAGEMENT

Database management is often riddled with compromise. Most often based on what works instead of best practices, database creation, management and growth usually reflects vender specific practices and can very depending on how many venders are in play for each application that each database supports. It is often best practice to focus on a single vender for the database engine and mold vender specific requirements into general practices used for all database conventions.

FIGURE 6 - 16. Database Server User Access



User access to database records and tables is usually granted through a front end application (figure 6-16 shows a web page interface). Various front end applications can be used depending on the limitations defined by each software vendor. Peoplesoft[137] can access Oracle records and tables while Deibold[138] accesses separate tables and records hosted by the same database server. While both applications have little in common they do share the same database engine and can also share the same server platform. Ultimately, defining both logical and physical sharing characteristics can reduce overall cost in assets and their management.

While non-DBA personnel can manage front end resources, ITS DBA personnel can maintain database assets and control the *back-end*[139] resources. Since the average person on the network does not see back-end applications (such as Oracle in our example),

137.PeopleSoft is a leading provider of e-business application software and claims to be the only software company to provide e-business solutions purely over the Internet for Fortune 1000 corporations. The company was founded in 1987 by Dave Duffield and Ken Morris, whose goal was to build client/server applications that empower the user, are easily adaptable in a changing marketplace.

138.Diebold is a services company providing integrated technology solutions that enable our customers to maximize their self-service capabilities.

139.A “back-end” application or program serves indirectly in support of the front-end services, usually by being closer to the required resource or having the capability to communicate with the required resource. The back-end application may interact directly with the front-end or, perhaps more typically, is a program called from an intermediate program that mediates front-end and back-end activities.

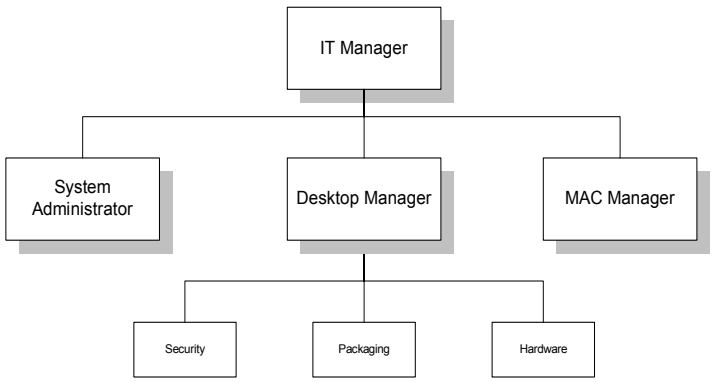
users generally refer to database resources in terms of the front-end application. It should be noted that front-end applications usually are not located on the same server as the back-end resources -- this helps to improve performance and scalability for more powerful applications while making resources more modular.

Desktop Management Team

GENERAL

Once thought of as the *grunts* of IT, desktop management has come to the forefront as more then just changing out broken hardware or upgrading software. Desktop management is tightly threaded with the server management group to test, develop and deploy new hardware and software (both individually and in mass). Applications can be *pushed* to the desktop or made available (on the intranet) to be *pulled* by the user. Any software that is mandatory (such as antivirus software) would be *pushed* to the desktop while any software that is optional (such as a desktop publishing package) would be made available for download via a *pull*. Packaging software for either push or pull technology also gives the desktop management team the ability to make *self-healing*[140] programs.

FIGURE 6 - 17. Desktop Management Team



While there are many variants on this theme, a desktop management team consists mainly of personnel who manage:

1. Antivirus and security (**Security**)
2. Create Images or software packages (**Packaging**)
3. Repair and install hardware (**Hardware**)

140.In information technology, self-healing describes any device or system that has the ability to perceive that it is not operating correctly and, without human intervention, make the necessary adjustments to restore itself to normal operation. Because users of a product may find the cost of servicing it too expensive (in some cases, far more than the cost of the product itself), some product developers are trying to build products that fix themselves.

THE DESKTOP MANAGER

The Desktop Manager (or *lead* desktop management technician), manages the desktop management team. They are usually responsible for maintaining hardware standards and software licensing inventory. They report directly to the IT Manager and act as liaison between other department managers and their teammates. Usually, this person has a global knowledge of all aspects of their team responsibilities and can act as backup for any person who is out sick or on vacation. The desktop manager is also responsible for providing a vision of what new technologies are available to improve services and provides metrics regarding hardware/software cost and usage as well as a host of other variables concerning user support. The primary objective of the Desktop Manager is user satisfaction and desktop stability.

SECURITY

The security specialist (or *team* depending on the size of the company), manages desktop antivirus software, the testing and deployment of hot fixes, security patches and software upgrades to insure that all precautions are met in protecting desktop company assets from attacks (both outside and inside). Their duties also include research and evaluation of potential trends and application holes that could pose a threat to the security of the network. They are the ones who communicate to infected users, and provide global security updates to the network community. They work hand in hand with server security personnel (e-mail, file sharing) as well as with the Infrastructure/Communications Management team to ensure that any potential threat is well documented and protected against on all levels.

PACKAGING

The Packaging/Imaging person is responsible for building disk images and pre-packaged software for desktops. Using special software, programs and operating systems can be customized so that the user does not have to answer one question concerning how or where the software is to be installed. Further, the person responsible for packaging tests all of the variables (OS, other applications, network settings and user profiles) to insure that the package does not break anything when installed onto a workstation (a.k.a. QA[141]).

Packages

Packages are *branded* for licensing and prevention of piracy. In other words, software media is configured so that the company name and ownership is automatically placed into the installation so that users can not take the software home and install it under their personal name. This also helps at work to maintain standards (when someone leaves the company the software does not retain their name and can be reused for the next employee).

141.In developing products and services, quality assurance is any systematic process of checking to see whether a product or service being developed is meeting specified requirements. Many companies have a separate department devoted to quality assurance. A quality assurance system is said to increase customer confidence and a company's credibility, to improve work processes and efficiency, and to enable a company to better compete with others. Quality assurance was initially introduced in World War II when munitions were inspected and tested for defects after they were made. Today's quality assurance systems emphasize catching defects before they get into the final product.

Push/Pull

Using Push and Pull technology, these packages are installed onto workstation with automated auditing of distribution to maintain licensing limitations and requirements:

- **Push** technology can either be done via Directory policies (which automates the distribution of software and applications), or by third party software (packaging and deployment tools).
- **Pull** technologies include posting links onto internal websites giving access to pre-configured software and alternative Directory policies that pre-stage software for installation when a person clicks on the menu item the first time.

Images

The term “images” usually refers to programs that take a snapshot of pre-installed hard drive contents and compress it into a file that can be used to mass produce the same hard drive configuration. While this has been a reliable method for pushing standard desktop contents out to the user’s workstations it is not a “living” image and is outdated when new service packs or software is released. This technology is still widely used throughout the industry but it‘s slowly being replaced by package deployment and directory policies to create a “living” image for each desktop.

FIGURE 6 - 18. Package Deployment

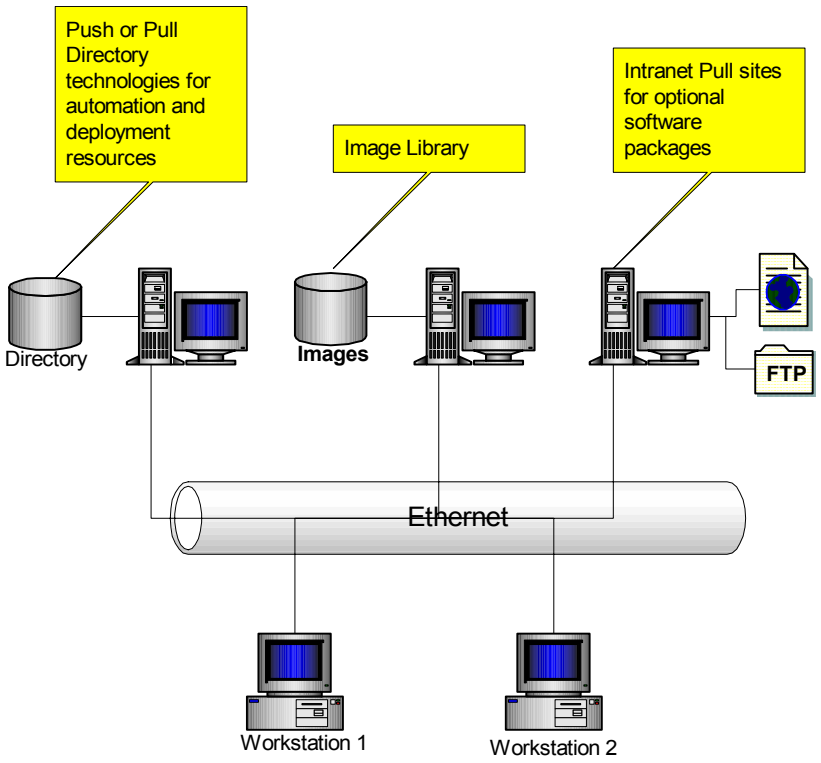


Figure 6-18 represents a topology that supports all three deployment models:

1. **Directory Policies** (using Active Directory, Novell Zenworks or Apple Directory)
2. **Third party Packaging** and Deployment
3. **Web based** installation links (either through HTTP or FTP)

It should be noted that third party packaging tools are generally a must for Active Directory while Novell provides an excellent packager in Zenworks and Apple provides their own packager in OS X Server software. Usually, a blend of all these resources works best for small to medium size companies.

There should always be an evaluation process prior to pushing any packages across the network -- if there is a bad image you'll be pushing it out to a lot of people who will not like the end result. You should build a test environment that emulates your customer base and deploy there first. Once deployed, you should test to see if the package works like you expected. Generally you build a testing checkoff sheet to verify operability. When you do decide to push packages out to your user base, you should do so in groups so that if anything goes wrong you only have to deal with a small subset of your network community. Never push packages across weak network links (56 KB modems, etc.).

HARDWARE

Your hardware person (or team) should be certified by the manufacturer for the equipment you have on the network. This should include:

- Workstations
- Servers
- Printers

Having your hardware person certified makes it easier and quicker to resolve RMA[142] issues by not requiring technicians to go through the detailed questioning over the phone regarding the validity of the hardware failure -- if your person is certified then there is no questioning process and the part can be shipped immediately.

The hardware person should have good people skills and work interactively with all team members. If the job is being done right then the hardware technician shouldn't look overly occupied (equipment should be up and running with very little downtime).

New technology has grown from the need to limit downtime. Many manufacturers have implemented early warning firmware in their products which warn of impending hardware failures. It is clearly an advantage to put a early warning network in place.

142. An RMA (return merchandise authorization) is a numbered authorization provided by a mail-order merchant to permit the return of a product. Most mail-order businesses have a policy concerning returns. Some companies allow only defective products to be returned; others allow any software to be returned if it is unopened. RMA numbers are important to both the merchant and customer. An RMA number tells the merchant that a return is being made and offers protection against fraudulent returns. The customer can use the RMA number to inquire on the progress of a return. For example, if the customer hasn't received any information about the return, the customer can call the merchant and use the RMA number as a reference.

SUMMARY

Our definition of a small company incorporated a disbursed multi-site enterprise so that we could should how such an organization could work together. We showed how a centralized location could work as the hub for all communication activities and minimize hacking dangers. We further offered a structural model that made it fairly easy to keep services going even when parts of the company were disconnected or sold off. We showed that automation could minimize the need for extensive personnel to maintain services and that sites could work together to further minimize downtime and provide 24 hour support. Security, automation and modularity all work together to produce stability and flexibility -- the basics for any growing network. The Internet has made it possible to take advantage of remote networking to optimize business operations and make remote sites work as one integrated computer network sharing ideas and resources.