

The Home Business Network

Section Three

Building a small business at home...

Introduction

GENERAL

The main difference between the home network and a home *business* network is purpose. You can take the content of this section and use it to build a home network, but at a greater cost (both up front and long term). The price of cable modems, DSL and satellite Internet connections have dropped dramatically -- making their technology quite available for the average home owner. But the cost of server software, specialized hardware and administration make it more than just a hobby.

This section will take the concepts learned in section two and further develop them into a business system. We will look at an expanded peer-to-peer workgroup and then a server-client domain. We will also take the home network from its slow 56Kb modem Internet on to DSL, cable modem, and satellite. We will look at expanding networked computers up to five machines.

The main objective of this section is to show the modular expendability of our little network and how you can best plan for upgrades and improvements while not having to start over each and every time you make a major change. Consistent with what was discussed in section one, we will emphasize "standards". In section two we did not have to follow too many standards mainly because there was little need -- both the laptop and desktop acted independently except for Internet access and the use of the printer. In a business environment, this changes -- everyone must act as a team of computers to perform all of the business functions.

Finally, we will look at inexpensive methods to provide a "presence" on the web for your business. This can be thought of as putting up your shingle.

Planning

DOCUMENTATION

When someone tells you to document everything, most people think of some long difficult process requiring hours of structured writing with detailed diagrams. While you would always gain from a structured, methodical writing process, most people are not prepared (nor have the time) to do it. What I have found very useful is for you to keep receipts of things you bought, scratch notes of what you wanted to do, and drawings that you made on the fly - everything associated to your network. Put them in some order so that you can sort through them when needed. These documents will prove more important than you may first think.

Before you build, take the time to make a note of what it is you want. Too many times networks are built because someone decides there should be a network. While it is true that networks are basically the same, you can benefit by reducing the cost of items based on the needs of the business.

List the things you want your network to support (purpose, then software/hardware).

Business Needs

- Writing letters, memos and other correspondence - Word Processing
- Communication - E-Mail
- Bookkeeping - Accounting software or Spreadsheets
- Designs - Graphics, Computer Aided Design
- Research - Web Browsers
- Other

CENTRALIZE ASSETS

Think big but start small. Pick technology that will simplify your administrative overhead but not break the bank. Build your network around devices that provide local DHCP and NAT⁷⁶ (both generally thought of for larger networks but made affordable using low-end routers). Keep what you have in place (in our case the home network from section two) and build on it. Convert all manually configured IP addresses to dynamic as soon as possible -- you'll be glad you did this before your network gets too big. Realize that most small networks grow quickly -- what you put in place should be scalable and centrally managed when possible.

PROCUREMENT

When you buy, always buy in bundles to help cut costs. Stay with one vendor as much as possible so that computer parts are interchangeable. Make sure the company has a good record of supporting small businesses (technical support, returns policy, etc.). Never lease anything if possible (I like to call it *fleeing*).

76. NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses.

Helpful suggestions

- Decide what software should be common to more than one machine (usually computers bought from Compaq, Dell, Gateway or other nationally sold brands have most of the applications you want already installed).
- Take the time to look for bargains as well (refurbished systems can work out as well as new ones).
- Never buy cutting edge technology.
- Build a rapport with your sales manager.
- Always get surge suppressors for every device.
- Never let yourself get caught up in the sales hype -- keep your eye on the ball.

The bottom line is just that -- the bottom line. Don't buy more than you have to but don't get caught without the resources you need.

SUMMARY

Planning your network (or upgrade) should be done carefully and deliberately. You should look at your network components as business assets and deploy them as such. Keep the costs low by purchasing computers bundled with general business software. Centralize your network configuration by using inexpensive network appliances (such as routers with DHCP and NAT installed).

The Basic Home Business Network

DSL

FIGURE 3 - 1. DSL Topology

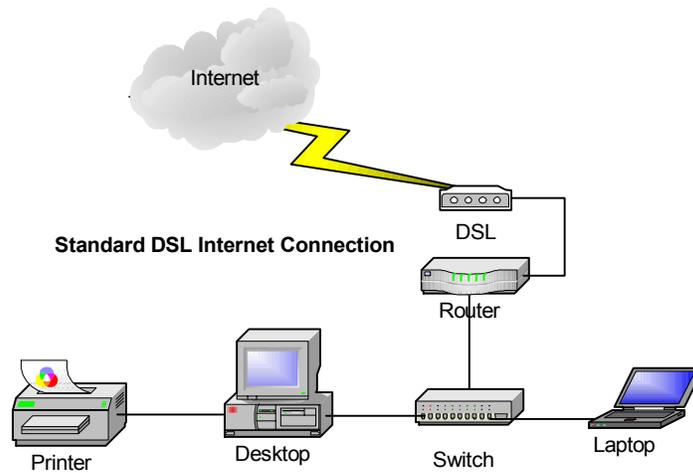


Figure 3-1 represents a standard topology for a home business network. There are three layers:

1. **Internet Access** represented by the DSL⁷⁷ modem
2. **Network Applications** represented by the Router
3. **Local Area Network** represented by the Ethernet switch, computers and printer.

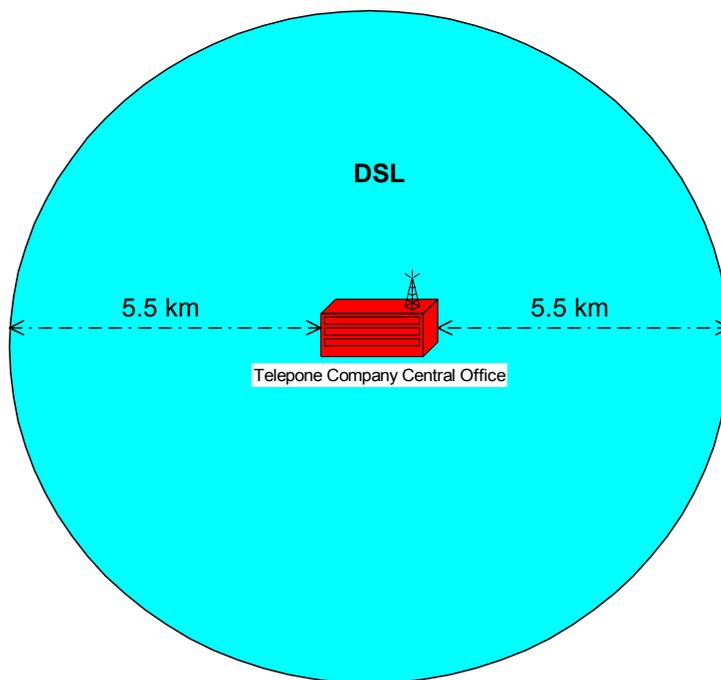
If we view our network in levels, we can start to see an organization of resources that helps to make administration and troubleshooting easier.

- **Level 1** - Internet Access level provides Internet Access, and DNS services.
- If you could not resolve a host name outside of your LAN you would look at the DSL modem to make sure it was working properly.
- **Level 2** - Network Applications level provides DHCP and NAT services.
- If your host IP was 169.254.x.x, you would look at the router to find out what was wrong.
- **Level 3** - LAN level provided local network services.
- If the printer failed to print you would look within layer 3 to resolve your printing problems.

77. DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL.

Digital Subscriber Line technology has significantly reduced the cost of high bandwidth. DSL started rolling out to customers in 1998 and has grown rapidly. Performance is gauged by your proximity to your telephone companies central office. Fairly inexpensive and available in most residential areas, DSL moves data at rates up to 6.1 megabits (millions of bits) per second (of a theoretical 8.448 megabits per second), far exceeding that of the standard T1 line used in most medium size businesses. In general, the maximum range for DSL without a repeater⁷⁸ is 5.5 km (18,000 feet). As distance between your home business and the telephone companies central office decreases the rate of performance increases.

FIGURE 3 - 2. Primary DSL Area of Coverage



Another factor for performance is the gauge of copper wire used. Heavier 24 gauge wire can carry the same data rate farther than 26 gauge wire. Also, if your phone company has upgraded their local loop⁷⁹ to optical fiber, DSL service can be extended far beyond the 5.5 km barrier.

There are various levels of service (usually referred to as SLA⁸⁰s or Service Level Agreements) depending on what you are willing to pay for. The bottom line DSL con-

78. In digital communication systems, a repeater is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal along the next leg of the medium. In electromagnetic media, repeaters overcome the attenuation caused by free-space electromagnetic-field divergence or cable loss.

79. In telephony, a local loop is the wired connection from a telephone company's central office in a locality to its customers' telephones at homes and businesses.

nection is usually packaged as a medium bandwidth access port which includes one dynamic IP address and little more. You usually are on the bottom of the totem pole when it comes to service. Each telephone company has defined SLAs they offer to their customers but here are some general SLA levels:

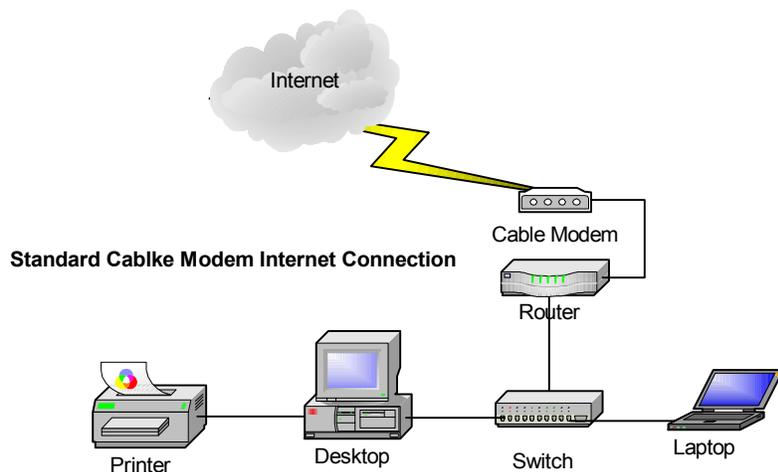
- **Basic** - Single *dynamic* IP address, no guarantee of performance, no priority for technical assistance, single e-mail address with minimal storage.
- **Upgraded Basic** - Single *static* IP address, guarantee of performance, low priority for technical assistance, single e-mail with minimal storage.
- **Small Business Package** - Up to five *static* IP addresses, guarantee of performance, high priority of technical assistance, five e-mail accounts with up to five MB storage, small web presence.

While there are probably more levels of SLAs available from your telephone company these three should give you a basic idea of what is out there. It should be noted that most telephone companies dedicate a support engineer to any small business package so that they can build a relationship that should improve your technical support.

NOTE: You can always start out with a basic package if your strapped for money and upgrade as your capital allows. You must have your phone line tested to make sure you can receive DSL.

CABLE MODEM

FIGURE 3 - 3. Cable Modem Topology



Cable Modem⁸¹ Technology does not offer the bandwidth that many DSL subscribers get but it remains a valid option that you may find advantageous. It is called a “cable modem” because the bandwidth is provided through the same cable your TV uses. Your

80. A Service Level Agreement (SLA) is a contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish.

Cable TV provider sells access to you as an upgrade option to your TV cable contract. It should be noted that cable modem technology is capable of providing greater data rates than the 1.5 MB earlier stated but is limited by the T-Carrier system⁸² your local provider uses to deploy their service. All cable modems attached to cable TV coaxial cable lines communicate using a Cable Modem Termination System (CMTS) provided by your local cable TV company office.

FIGURE 3 - 4. Cable Modem Configuration

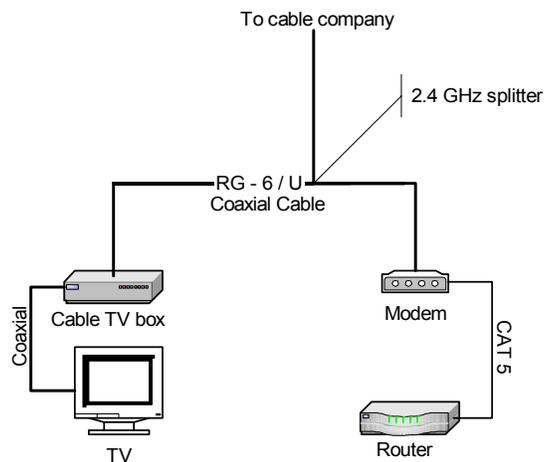


Figure 3-4 displays the basic topology applied to a cable modem configuration. The cable is split using a 2.4 GHz splitter device that has three or more coaxial cable connectors. One (or more) cables are attached to TV(s) in the home while another connection goes directly to the cable modem. You can not have more than one cable modem on the same internal cable. Cable modems can also be used directly with the TV making the TV an Internet terminal. This is an either or situation - either using the TV or the LAN for Internet communication. In a small business environment using the TV as an Internet terminal is not the appropriate option.

The cable modem has two connections:

- Coaxial cable connector - connects to the TV cable.
- RJ45 - connects to the network router.

If you only have a single computer in your LAN you could connect the cable modem directly to the computer's NIC, but this would limit LAN scalability and open the computer to unnecessary security holes.

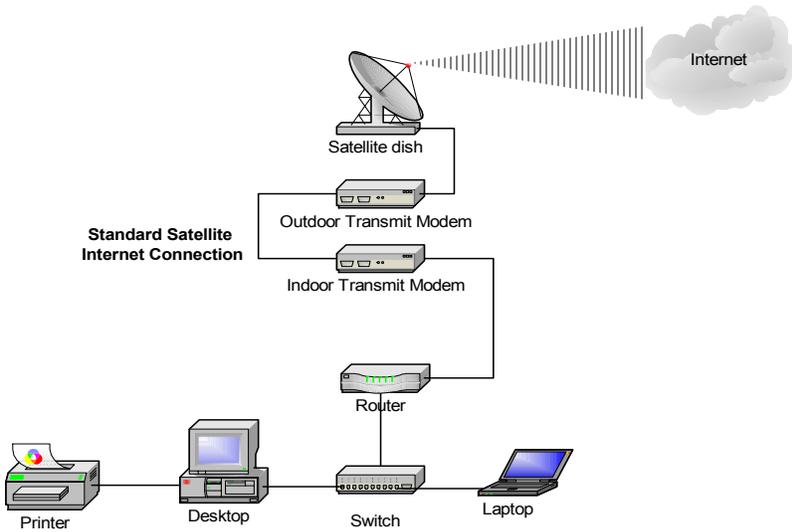
81. A cable modem is a device that enables you to hook up your PC to a local cable TV line and receive data at about 1.5 Mbps.

82. The T-carrier system, introduced by the Bell System in the U.S. in the 1960s, was the first successful system that supported digitized voice transmission.

SATELLITE

Broadband satellite Internet access is offered in locations that DSL and cable modem can not reach. Satellite is expensive to install but around the same monthly fee as DSL and cable.

FIGURE 3 - 5. Satellite Access Topology



Satellite Internet access is affected by weather which can be a problem for areas of high fog or fowl conditions. Most satellite service providers offer a variety of data rates and encryption to secure your data connection from dish to ISP.

Some of the drawbacks of Satellite are:

- Many satellite access providers only support USB connections which may disallow use of a router between the access port and LAN.
- Latency⁸³ is an issue in that there is a time lag from send to receive.
- The FCC requires that only licensed professionals install two way satellite communications.
- Only dynamic IP addressing is usually available.
- Most satellite providers do not support hosting business web sites.
- Many satellite providers do not support Macintosh systems.

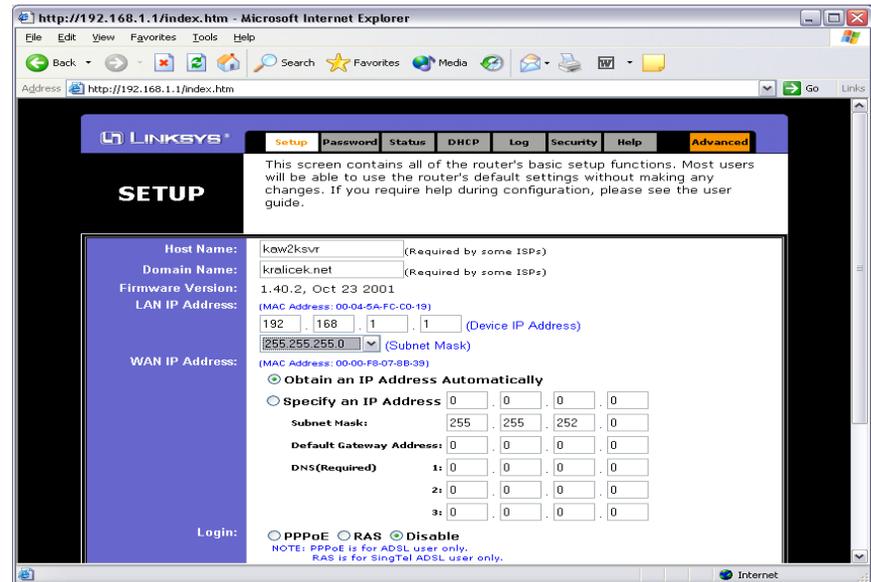
Generally speaking, satellite technology should only be used as a option of last choice, when DSL and cable modems are unavailable. With a lot of equipment that must be maintained, expensive installations and problems with weather, satellite broadband access can be more hassle then it's worth.

83. In a network, latency, a synonym for *delay*, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.

CABLE/DSL ROUTER

Router technology, once an expensive proposition for small and large businesses has been repackaged for the home business community.

FIGURE 3 - 6. LinkSys Router Menu



Inexpensive and packed with useful features like DHCP⁸⁴, NAT⁸⁵, a firewall and more, no home network should be without it. The key benefit lies in the ability for the router to protect your assets while providing an automatic network configuration that makes add-

84. Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

85. NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

ing additional computers to the network as simple as plugging the network cable in and turning the computer on. Some more advanced features are:

- **Filtering** (Filters enable you to prevent certain PCs on your network from accessing your Internet connection.)
- **Forwarding** (Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your router, they will be redirected to the specified IP).
- **Dynamic Routing** (The dynamic routing setup allows your network to dynamically adjust to layout changes).
- **Static Routing** (This feature sets a fixed path for data to follow on the network).
- **DMZ Host** (This feature sets a local user to be exposed to the Internet. Any user on the Internet can access in/out data from the DMZ host).
- **Mac Address Clone** (this allows you to change the WAN MAC address of this router).

You can also review incoming and outgoing access logs to monitor use of Internet resources.

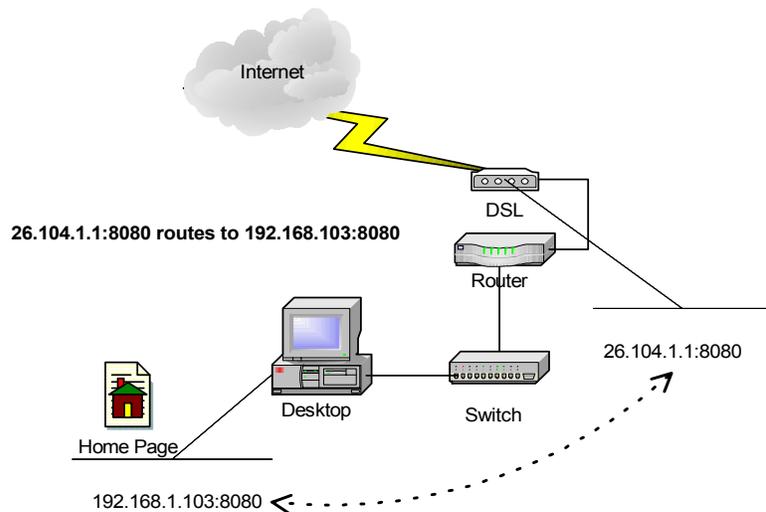
FIGURE 3 - 7. Outgoing Access Log

LAN IP	Destination URL/IP	Service/Port Number
192.168.1.103	oasis.mandrakesoft.com	HTTP
192.168.1.103	www.mandrakesecure.net	HTTP
192.168.1.103	images.mandrakesoft.com	HTTP
192.168.1.103	www.mandrakesoft.com	HTTP
192.168.1.103	oasis.mandrakesoft.com	HTTP
192.168.1.103	www.mandrakesoft.com	HTTP
192.168.1.103	www.mandrakeonline.com	HTTP
192.168.1.103	www.mandrakesoft.com	HTTP
192.168.1.103	www.mandrakesoft.com	HTTP
192.168.1.103	www.yahoo.com	HTTP
192.168.1.103	srd.yahoo.com	HTTP
192.168.1.103	login.yahoo.com	HTTP
192.168.1.103	www.yahoo.com	HTTP
192.168.1.103	www.yahoo.com	HTTP
192.168.1.103	ordering.yahoo.com	443
192.168.1.103	sec.yimg.com	443
192.168.1.103	ordering.yahoo.com	443
192.168.1.103	sec.yimg.com	443
192.168.1.103	ordering.yahoo.com	443
192.168.1.103	us.fl.yahoofs.com	HTTP
192.168.1.103	search.personals.yahoo.com	HTTP
192.168.1.103	personals.yahoo.com	HTTP
192.168.1.103	us.il.yimg.com	HTTP
192.168.1.103	us.il.yimg.com	HTTP

For the price of a fine dinner, a router becomes an indispensable tool that centralizes administration, simplifies installations, and provides security. From the outside of your network, your LAN looks like one system - the router. If anything can get hacked it would end up being your router. If you monitor your logs often, you should be able to see people trying to get in and stop them. With additional software, your router can become a fairly sophisticated firewall⁸⁶ that shields your data from intruders while making the Internet a more safe place to be. If there are sites on the Internet you don't want your users to be, you can block their access to those sites.

The router, using dynamic (or static routing) can distribute port access from a single IP address to individual IP addresses within your LAN. For instance, if you have a secure web service hosted on a non-routable IP address (say 192.168.1.103) and you wish select others to have access to that web site, you might define a port 8080 for an outsider to connect to. You would not have them connect directly to 192.168.1.103:8080 because that is a non-routable connection. Instead you would set up a dynamic route between the router address (which is a routable address) to the non-routable address (192.168.1.103) using port 8080.

FIGURE 3 - 8. Dynamic Routing



In figure 3-8, an outsider (on the Internet) would type into their Internet Browser **http://26.104.1.1:8080** and the router would translate the request to **http://192.168.103:8080**. You can have as many computers as you like given special routes so that from the outside there is only one computer shown while in truth you are allowing access to several

86. Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

computers through the modems IP address. When choosing ports for routing you should refer to a updated list of designated port settings:

<http://www.iana.org/assignments/port-numbers>

There are many commonly used ports for TCP, the more you become familiar with the better. It would benefit you to make a print out of the web site listed above so that you have a ready list for when you decide to create your routing table. If all of this seems complicated right now, don't worry, if you are not sharing information from inside your LAN to someone on the internet (say a web page), then the default configuration for your router is all you need.

DMZ HOST

The DMZ host is used for computers that you are willing to allow greater access from the outside (through the Internet). By assigning a DMZ host you are opening up that computer to share special resources with the clients or other workers on the Internet. Some of these special resources may be:

- SQL⁸⁷ or Oracle Databases
- IIS⁸⁸ or Apache Web Server
- E-Mail Server front-ends

While there are more possibilities, the three above cover a large percentage of DMZ deployments. The purpose is to put a visible access point for all to see but only those who should have access to gain that access through. This can also be understood as a "front end" to protected computers. We have not really discussed servers much up to this point and we will avoid doing so until they become cost effective. Up to this point server software is cost-prohibitive and doesn't really provide enough benefits for that investment to be made. Workstation software can allow up to ten concurrent connections and will also facilitate applications that would provide the same services as the SQL/Oracle, IIS/Apache, or E-mail front-end. As our network grows we will see the introduction to server software and their value to a business.

MAC ADDRESS CLONE

This option allows you the ability to disguise your router so that Internet users can not determine what manufacturer it belongs to. This is a useful option if you are really serious about security. Since each home router manufacturer has default accounts and passwords for their product, crackers can use that default information to break into your system. By changing the router's mac address you are hiding it's identity. The real

87. SQL (Structured Query Language) is a standard interactive and programming language for getting information from and updating a database. Queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth. There is also a programming interface.

88. (Internet Information Server) is a group of Internet servers (including a Web or Hypertext Transfer Protocol server and a File Transfer Protocol server) with additional capabilities for Microsoft's Windows NT and Windows 2000 Server operating systems. IIS is Microsoft's entry to compete in the Internet server market that is also addressed by Apache, Sun Microsystems, O'Reilly, and others.

answer to protecting your router access is to set an account with a strong password and make sure that the default is not available.

ETHERNET SWITCH

Using an Ethernet switch instead of a hub⁸⁹ is essential to providing optimal network performance. The main difference between a hub and a switch is port speed.

HUB technology

If we look at a 100BaseT hub, the speed for the device may be 100 bits per second (bps) but that is divided by the number of connections currently being used. Say you have five computers connected to a hub you divide one hundred by five ending in a guaranteed port speed of twenty-five bps. If you hub has more connections the port speed is reduced even more. Hub technology does not ensure one steady port rate. The fewer people using the network the faster it performs.

SWITCH technology

A switch on the other hand guarantees that every port provides 100 bps no matter how many devices are attached to it. Most modern switches also include a duplexed port rate which guarantees 100 bps both ways (in and out). There is this thing manufacturers call a “switching fabric⁹⁰” which is the logic that ensures the port rate. A “hub” usually contains no “logic” or intelligence built into the device.

Shared Technologies

Both switch and hub technology generally employ an uplink port which allows you the ability to “stack” devices. Stacking does not generally refer to the physical placement of devices but focuses primarily on the ability to build a backbone⁹¹ between them (as in figure 3-9). By using a backbone, each switch added to the network acts as a network *segment*, reducing packet collisions and optimizing performance. As important, is the physical extension a backbone permits for your network to scale as you grow.

Uplink ports usually require a crossover cable, BNC or Thinnet connector to bind network devices. Usually, when using an uplink port one of the standard ports must remain empty otherwise all segment connectivity fails. You should read your switch user information completely before either purchasing or deploying a device. You should also stick to one vendor for your switch technology to avoid problems of incompatibility. Keeping a spare switch on site is also a good idea. If possible, label all cables connecting to each

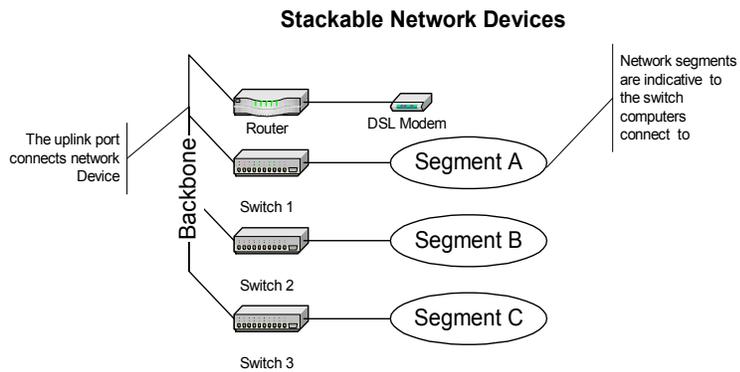
89. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions.

90. Switching fabric is the combination of hardware and software that moves data coming in to a network node out by the correct port (door) to the next node in the network. The term suggests that the near synonym, switch, tends to make switching seem like a simple hardware function. Switching fabric includes the switching units (individual boxes) in a node, the integrated circuits that they contain, and the programming that allows switching paths to be controlled.

91. A backbone is a larger transmission line that carries data gathered from smaller lines that interconnect with it.

device so that you can troubleshoot problems (the host name of each computer on both ends of the cable will help to centralize failed hardware and resolve the problem more quickly).

FIGURE 3 - 9. Backbone

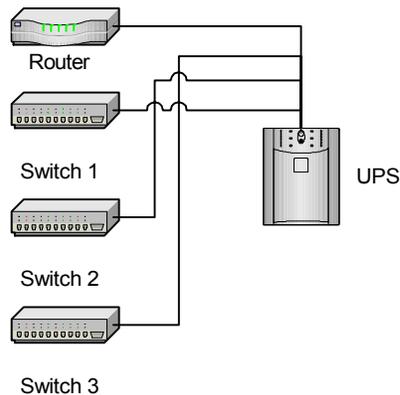


UPS

Something we have not talked about yet is Uninterrupted Power Supplies (or UPS⁹²).

FIGURE 3 - 10. Network Power Support

Power Protection for Network Appliances



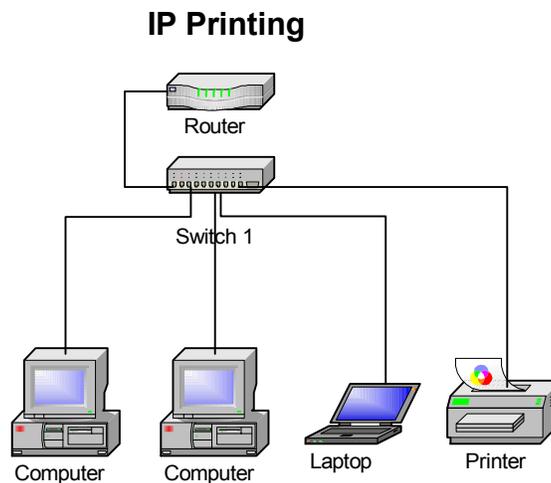
92. An uninterruptible power supply (UPS) is a device that allows your computer to keep running for at least a short time when the primary power source is lost. It also provides protection from power surges. A UPS contains a battery that “kicks in” when the device senses a loss of power from the primary source. If you are using the computer when the UPS notifies you of the power loss, you have time to save any data you are working on and exit gracefully before the secondary power source (the battery) runs out.

Providing power protection for your network devices is vital to the stability of your network. While it is also important to attach a UPS to each and every desktop computer, too many people fail to protect their switches and routers. The UPS does not only provide battery life for your device to be shut off properly, it also offers line conditioning, spike, and surge suppression. While adding a surge suppressor would be a nice try, surge suppressors don't usually provide line conditioning - which ensures the quality of electricity. Since personal UPS devices are very reasonably priced, it would be a big mistake to not have all of your hardware protected.

IP PRINTING

Since we are talking about a business, we have to look at resources differently than a hobby network would be set up. In a hobby network, having the printer connected to a desktop is fine since you don't have to worry about sharing it with too many other users. In a business network, you are going to see a lot of printing which will effect the person having to use the computer that the printer is attached to. This can become a problem on many levels.

FIGURE 3 - 11. Local Printing



The printer has its' own NIC (and IP address) that connects to the switch. Each workstation (desktop and laptop) maintains their own print queue -- no longer requiring accounts and passwords to be the same on all machines in order to print - this is both good and bad. It is a good idea to set a static IP before installing the printer driver on each computer. There are two low cost IP printer options available for printers:

1. **Print Server** (a device that transfers standard printer ports to an Ethernet connector with IP address).
2. **Internal NIC device** (a add-on card option offered for specific types of printers on the market (such as HP's LaserJet printer series)).

With either option, the printer is transposed from a printing divide dependant on a workstation to share printing services, to an Ethernet node owning it's own IP address and device name on the network (if fact a network appliance).

You should consider the following before you decide to add an IP printer to your network:

The Good...

- No special computer must be on for all others to print.
- User accounts do not have to be the same on all computers.
- Anyone can print without affecting the performance of another computer.

The Bad...

- No central management of printing resources.
- Uses up an Ethernet port on the switch.
- Costs more than a standard printer.

Ultimately, as your business grows you will turn to an IP printing solution. Later on in this book we will describe alternative you can apply in providing IP printing which will resolve most (if not all) of the bad in IP printing.

STORAGE

Three facts of life:

- There is nothing more important than your data.
- There is nothing more damaging than a hardware failure that destroys your data.
- There is nothing more you can do if you don't have a disaster recovery plan and your data is lost.

Mechanical devices have a higher rate of failure than solid state devices. Let's face it, newer hard drive technology spins at 10,000 to 15,000 RPM on an average. At that rate it's natural to see more failures occur more often. While hard drive failures are not as common an occurrence as they could be, when they happen, it is usually devastating to your data. There are several ways in which you can protect against data loss while not expending large amounts of cash or time.

You should backup your *important* data to one of the following devices:

- Second Hard drive
- CD-R or CD-RW⁹³
- Tape
- ZIP

It is useful to know which data is important and which isn't. Applications and the operating system can be re-installed using the CDs that came with your computer (for your bundled software) or other applications purchased afterwards. What can not be easily replaced is the data that you generate from your applications (spreadsheets, word processing, graphics, etc.). Knowing where this data is and making backups of that data is essential to your recovering from disaster. If you can automate the backup process you

93. CD-R and CD-RW are writable compact disk drives.

can improve your chances of maintaining all of your data. The one thing you must do manually is test your backups occasionally so that you are sure that the process is working effectively. Even the best system administrators fail to assure that their backups are properly tested -- this is usually the result of forgetting to test or becoming too self assured that the backup process is working. Never become complacent with your backup process -- test your data recovery process (this will help to not only assure the process is working but also keep yourself trained for when a disaster does occur).

A good backup strategy consists of the following:

- Perform a full backup of all data once a week.
- Perform incremental⁹⁴ or differential⁹⁵ backups every workday that a full backup is not being performed.
- Backup data when all users are off-line and not using their computers.
- If possible, store all backups off-site in case of natural disasters.

RAID

RAID⁹⁶ is a technology once too expensive for the home business. This technology allows you the ability to either Mirror, stripe or stripe with parity, creating disk sets that act as one volume (i.e.; two or more drives combined to create drive C: in an IBM format). With the introduction of ULTRA ATA RAID cards (such as the ones Promise Incorporated offers) the average person can create reliable RAID volumes using low cost drives (like the ones generally offered by PC and Apple manufactures).

Most operating systems offer software RAID. Using hardware (such as the Ultra ATA RAID card) to create RAID volumes is always the best practice -- you are not dependant on the operating system to restore a drive set. Hardware RAID sets also perform better and are more reliable.

Lets look at some RAID options:

- **Mirror**⁹⁷ In using a mirror drive set, you are actually writing data to two disks simultaneously. This provides a "hot" backup of your information. If one of the drives fail the information can be accessed on the second drive. Once set up, mir-

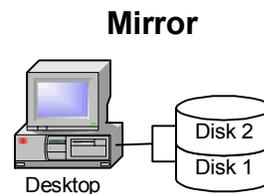
94. An incremental backup backs up only those files created or changed since the last normal or incremental backup. It marks files as having been backed up (in other words, the archive attribute is cleared). If you use a combination of normal and incremental backups, you will need to have the last normal backup set as well as all incremental backup sets in order to restore your data.

95. A differential backup copies files created or changed since the last normal or incremental backup. It does not mark files as having been backed up (in other words, the archive attribute is not cleared). If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.

96. RAID (redundant array of independent disks; originally *redundant array of inexpensive disks*) is a way of storing the same data in different places (thus, redundantly) on multiple hard disks. By placing data on multiple disks, I/O operations can overlap in a balanced way, improving performance. Since multiple disks increases the mean time between failure (MTBF), storing data redundantly also increases fault-tolerance.

rored drive sets offer excellent protection against data loss with little down time -- replace the broken drive with another drive, recreate the mirror set and your back in business with a fault tolerant solution.

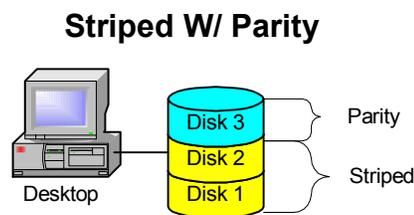
FIGURE 3 - 12. RAID 1 (Mirroring)



The down side to mirroring drives is that it takes a bit longer to copy data to both drives at a time. While most people would not notice this decrease in performance, there are some cases where speed can be an issue (such as playing movies or audio clips). The second downside to this is that your paying for two drives but getting the disk space of one drive. Say you have two 20 BG hard drives, you will only get 20 GBs worth of disk space. Since hard drives are fairly inexpensive this is a viable option to more costly tape backup schemes. NOW I must say that if you ask the professionals about this they would argue the point that RAID is not a alternative to tapes or a well thought out backup strategy but I would contend that it is surely betting then no fault tolerance.

- **Striping with Parity** (a.k.a. RAID 5) requires three or more drives connected to the RAID card and helps you retrieve some of your lost diskspace.

FIGURE 3 - 13. RAID 5 (Striped w/Parity)



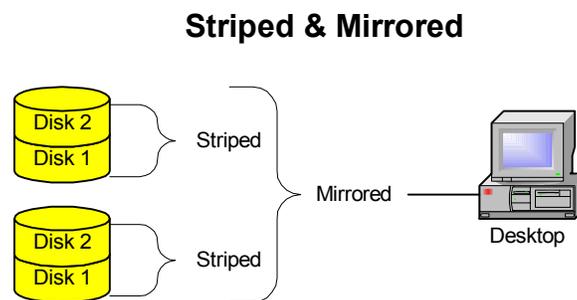
In RAID 5 you get the majority of diskspace minus parity to write data to. In Figure 3-13 you loose disk 3 but can freely write to disk 1 and 2. The up side is that you can loose any one of the drives in the RAID 5 set and replace the broken drive salvaging all of the potentially lost data. This implies that no specific drive is dedicated as the parity drive - - and that is true. The above diagram is used to represent the disk space lost and not the physical allocation of disks in the RAID set.

97. A mirrored volume is a fault-tolerant volume that provides data redundancy by using two copies, or mirrors, of the volume to duplicate the data stored on the volume. All data written to the mirrored volume is written to both mirrors, which are located on separate physical disks.

Additionally you can add a hot spare to the RAID set so that when one drive dies another takes its' place automatically allowing you the convenience of replacing the bad drive during a lull in system usage. This hot spare would not be available for use until a disaster occurs.

- **Stripe Mirrored Sets (RAID 0+1)** are the most costly but offer the ability for up to two drives to fail without losing any data. You create two striped sets (RAID 0) and then mirror them both together. This RAID configuration is for the person who really wants to protect their data...most people do not need this level of fault tolerance.

FIGURE 3 - 14. RAID 0+1 (Stripped & Mirrored)



The downside to this is cost and complexity. You should know what your doing before building this configuration and you should have enough money in hand to build it. You should also have a machine large enough to handle four drives (power and physical placement).

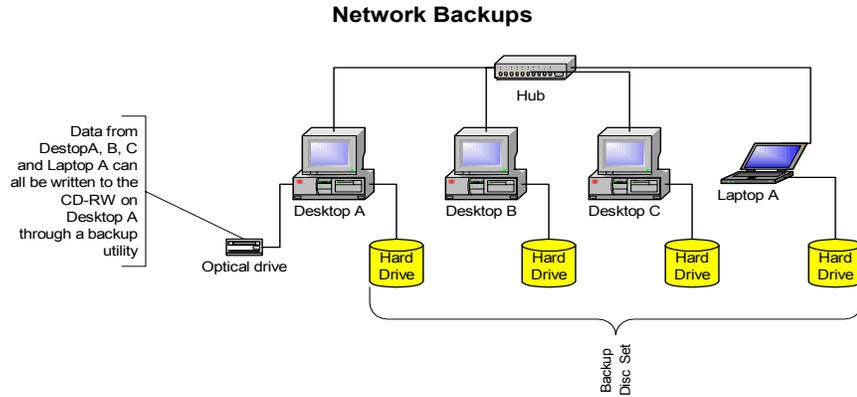
While there are more versions of RAID configurations out there, the three mentioned are the most affordable and easily installable for small businesses.

CD-R AND CD-RW

Windows 2000, Apple OS X and Linux all offer the ability to write to CD-R and CD-RW drives. By using the CD-RW, you can leave a CD in the CD-RW drive and configure your backup software to write there. You would link the folders containing data on each of the desktops and laptop computers to a backup set to be recorded on the CD-RW drive. If you want multiple backup sets you would change out the CD-RW media with new formatted media. This works well as long as your backing up relatively small amounts of data (256 MB or less).

A downside to this process is the workload you place on both the computer recording the data and network bandwidth. While the backup is running there will be a large load placed on the network moving data from each of the workstations to the recording media. The computer recording data from other systems will also require an account that can access and copy data. All users must be off their machine in order to copy file contents. If a file is left open while by another user while the backup process is running the backup software will ignore that file and not complete the backup of that data. It is always a good idea to monitor backup logs to see if all data has been backed up completely.

FIGURE 3 - 15. CD-RW Backups Across the Network

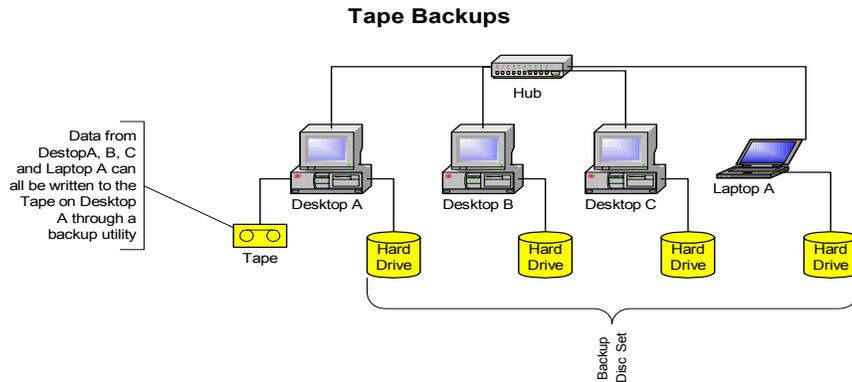


CD-RW backups across the network can be a cost effective means to backing up data but it does require time and dedication to keep it current. If you do decide to go this route, make a schedule, automate as much as you can and remember to replace CD media when required and monitor your log files. This would work well as a secondary function in conjunction with a good RAID set on each machine.

TAPES

Tape backups can be a great way to backup all of your data -- there are 100-350 GB drives out there just waiting for you.

FIGURE 3 - 16. Network Tape Backups



It works much the same way on the network as the CD-RW example previously explored, except that your using a tape device instead of a CD-RW. The downside to this option is significant - the tape drive is slower to backup and restore data, much more costly to purchase and maintain, and it will take up a lot of your time to keep current. Since you are backing up larger amounts of data the bandwidth to accomplish this will be much greater. Tape devices use streaming data so it takes time to mount a tape and locate your data. The larger the tape the longer the mounting process. If you are in a

crunch to get back up -- tape devices will test your patience. If you do not test your restore process often, you will come in contact with data you can't restore - and that will be the time you need it most.

ZIP DRIVES

Zip drives offer a personal level of backups that you can depend on for small jobs. Do not use ZIP drives for your network backup strategy -- much like the CD-RW backup option, ZIP drives are limited in capacity and must be maintained the same as CR-RWs. Unlike CD-RWs, the media is expensive and specific to the type of ZIP drive you use. There are many different models with different capacities and they usually are downward compatible.

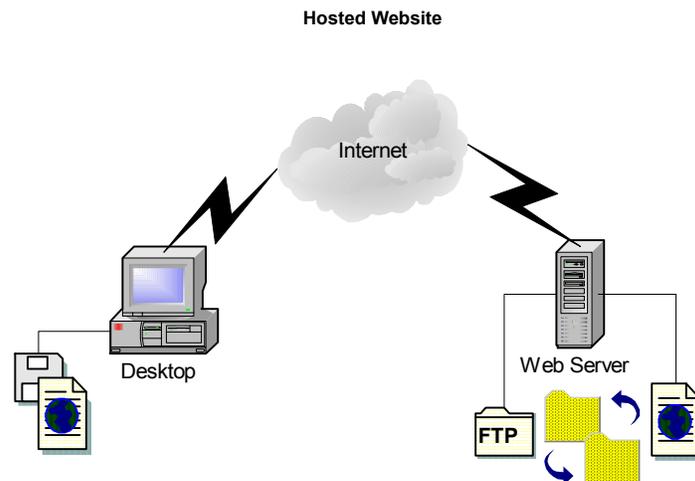
ADMINISTRATION

In all of this you are noticing a trend - that the larger the network, the more administration that must take place. To cut costs we have limited our network to a peer-to-peer configuration and that is a configuration requiring greater administration. There will come a time when the cost of administration forces you to invest in a server-client environment to help cut the cost of administration -- and that is a double-edged sword as well. We will look at that aspect of networking in the following sections.

INTERNET PRESENCE

If you are limited on personnel and resources the last thing you want to do is manage your own web server. It is cost effective for small companies to have their web pages hosted outside the business -- let someone else have the security headaches and responsibility for maintaining content.

FIGURE 3 - 17. Hosted Internet Presence



You build your web pages on a personal web server (locally) and then FTP⁹⁸ the files to your hosting ISP on an external server. You keep the original data and post the duplicate. If someone damages the hosted data you can restore from the data on your local computer. You also gain by the ability to backup local data to CD-RW or tape and have

an archive as well. This is a win-win situation for small businesses. The key is to have an ISP that supports the web development tools that you use to make your presence known.

What I have found in web pages that have annoyed me over the years are that they tend to get more complicated as they mature (age). I find that simplicity is the mark of excellence. If people can find what their looking for quickly that's a good thing. Too many web pages take forever to find what your looking for and lead you into paths that have no relationship with what your looking for -- I never visit those web sites again.

SUMMARY

If you have a home network with less then five computers -- don't waste money, stick to bundled software and don't get hooked on server solutions -- the benefits will not (on the average) be enough to recoup the investment. Keep things simple, first establish a sound foundation with computers that connect to each other quickly and efficiently. Link to a central inexpensive device that supports DHCP and NAT. Obtain the best bandwidth technology at the lowest cost (DSL, Cable Modem then satellite). Only allow your router to speak directly with the internet and use safe computing -- a solid antivirus package that updates regularly.

Backup data - I mean backup data! Test your backups regularly, and automate the process if possible. The worst case scenario always includes data that has not been backed up. Use RAID technology when possible but ALWAYS include a secondary backup process. Whenever possible keep backups off site in safe place - when the twin towers fell so did their data.

Unless you have the personnel, host your web presence through an ISP. It is never cost effective to have your customer enter your local network without safeguards. Depend on keeping your home network secluded until you are big enough to pay for serious security - a quiet presence is a safer bet.

98. File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols.