Living with a SOHO Network
2001 edition
The Joys of DSL and VPN

Tom Schmidt
Schmidt Consulting
Revised 3/25/2001
tom@tschmidt.com
http://www.tschmidt.com

Abstract
This paper discusses our experience setting up a small office home office (SOHO) network. It examines technical requirements of a Local Area Network (LAN), choosing an Internet service provider (ISP), Internet sharing methods, and how to setup network-based services. Internet access is via DSL this provides a high-speed always on connection. DSL and Cable modem services enable individuals and small businesses to access telecommunication services once the province of large corporations and governments. Virtual Private Network (VPN) encryption software provides secure remote access to the corporate network. This allows access to corporate resources without leaving home.

Table of Contents

1 Overview

In mid 1998 I set up a home LAN. I was starting a consulting business and wanted to learn more about the issues involved in building and operating a Small Office Home Office (SOHO) LAN. Until that time my networking experience was limited to interactions with the corporate Information Technology (IT) department. This is the third installment of that paper. The LAN has undergone significant evolution over time. DSL is now the primary Internet connection; dialup is used as a backup if DSL fails. Initially we used PC based software for Internet sharing and firewall. That gave way to a Broadband Router, as did peer-to-peer printing that is now performed by a network print server. The laptop originally used for Internet sharing, local web server, timeserver, and file server died. The new server, a recycled desktop, runs the timeserver, local web server, and a much larger file server. Replacing the laptop with a desktop normally requires another monitor, keyboard, and mouse. Instead we opted to use a KVM (Keyboard Video Mouse) switchbox. This allows a single keyboard, mouse and monitor to be used with multiple computers.

An added complexity this year was the need secure access to corporate information as a telecommuter. Setting up a Virtual Private Network (VPN) between the SOHO and the corporate network provides secure access when telecommuting. The VPN encrypts data between the home LAN and the corporate network. As is typical with all things networking the installation and debugging was accomplished with some difficulty. However, once properly implemented the VPN has operated flawlessly.

The laptop is much more active this year. Using a laptop in different networks requires a unique configuration for each location, corporate office, SOHO office, and on the road. Luckily a utility exists called NetSwitcher that simplifies this task.

This paper discusses how to set up a small Internet connected LAN. The LAN does much more the simply allow multiple computers to share a single Internet connection. It is the glue that allows devices to interact with one another. This paper is not intended as a competitive product review. The field is constantly changing; any attempt to do so is rapidly outdated. Rather, it discusses how specific requirements were addressed and implemented. For up to date reviews of networking hardware and software the reader is directed to the many publications and web articles on the subject. The products and services described in this paper represent my choices to deliver the features I needed.

Goals for the network:

- Share single Internet DSL connection
- Automatic Dialup if DSL fails
- Printer sharing
- File sharing
- Local private web server
- VPN access to corporate network
- A access to multiple e-mail accounts
- Fax without a fax machine
- Automatic time synchronization
- Minimize telephone busy signal
- Learn about SOHO networking

The drawing on the next page shows the entire environment; phone service and networking for both business and personal use.

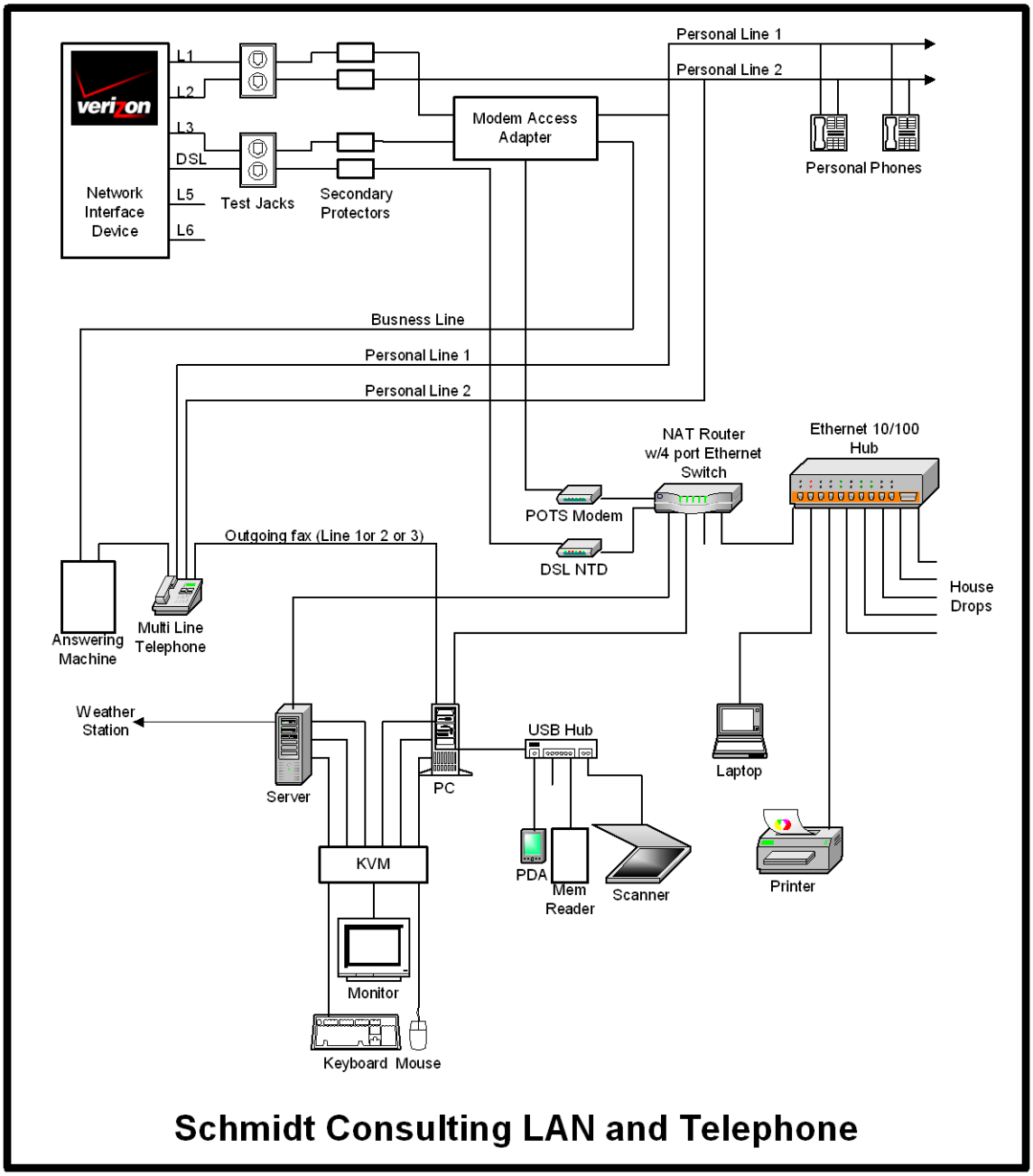


Figure 1 SOHO data and voice block diagram

2 Internet Access – Your Friendly Internet Service Provider

The reason most often cited to purchase a PC is for Internet access. The PC has progressed from a hobbyist plaything to an important item of telecommunication equipment. The most common access method for residential customers are: dial-up over a regular phone line, Digital Subscriber Line (DSL) a high-speed service using existing telephone wiring, and Cable Modem over Cable TV distribution facilities.

The ISP provides the following services:

- Connection between the end user and ISP network – so called last mile
- Routing between customers and one or more Internet backbone(s)
- User authentication
- User IP address assignment
- DNS name resolution – translate host name to IP address
- E-mail account(s)
- USENET Newsgroup
- Web hosting
- Billing
- Technical Support

The service provider is the bridge between the retail customer, and the interexchange carriers that operate the Internet backbone.

2.1 Dialup

Dialup access is available to anyone with an analog telephone line. Modems can also be used with cellular phones, however data rates are significantly lower then wired phones so it is not commonly used at fixed locations.

Most ISPs support the ITU V.90 modem standard. The International Telecommunications Union V.90 standard replaced previous generation of proprietary 56Flex and X2 modems. ISPs typically connect directly to phone company digital trunks. This means only a single analog to digital conversion exists, at the subscriber's connection in the Telco central office. The ISP's modem is synchronized to the digital trunk. This enables the ISP to transmit at up to 56kbps. Current FCC power regulations restrict maximum speed to 54kbps. Transmission from the subscriber to the ISP is limited to 33.6kbps because the subscriber does not have access to digital carrier. The ITU recently released the V.92 standard. It increased upload speed slightly to 44Kbps and implements faster auto negotiation to reduce connection setup time. V.92 also supports improved data compression. Check with your ISP to see if and when they plan to roll out V.92.

At connect time the modems probe the line to determine noise and attenuation levels. This sets the initial connection speed. During the course of the connection the modems constantly adjust to varying line conditions. After the modems synchronize the user is authenticated and an IP address issued. As soon as the computer has an IP address it is able to access the Internet.

2.2 DSL

Digital Subscriber Line (DSL) technology uses the existing twisted pair telephone copper wiring between the subscriber and the phone company central office to carry high-speed data. This allows the local exchange carriers to generate additional revenue by leveraging their massive investment. Several types of DSL have been developed hence the xDSL moniker. The most common types of DSL are Asymmetric DSL (ADSL) and Symmetric DSL (SDSL).

ADSL offers higher download speed, toward the subscriber, and then upload. It has the advantage that it coexists with POTS voice service. This reduces cost by allowing a single copper pair to be used for both voice and data service. A residence with a single phone line can be equipped with both a standard analog

POTS (Plain Old Telephone Service) phone and high-speed data service. Filters split the signals inside the residence. Low frequencies are delivered to the phones; high frequencies to the DSL modem.

SDSL is typically marketed as a business service. It requires a separate copper pair; it does not coexist with POTS. Being symmetric makes it suitable for servers. SDSL is also typically offered with a static IP address. A static address allows external hosts to connect to the server. A special case of SDSL is IDSL that offers symmetric speed of 144Kbp/s over longer distances then either ADSL or SDSL. IDSL uses ISDN signaling allowing it to be used at >20K feet.

Speed varies by supplier; it ranges from a low of 144Kbp/s for IDSL up to several megabits per second for subscribers close to the central office. In our area Verizon ADSL is available at 640/90, 1600/90 and 7100/680. Vitts SDSL services range from 270/270 to 2320/2320. Speed decreases with distance between the subscriber and the Digital Subscriber Line Access Multiplexer. (DSLAM). The DSLAM combines data from multiple customers into a single high-speed connection. It can be located at the Telco central office or in a remote cabinet.

DSL service is offered by traditional phone companies called Incumbent Local Exchange Carriers (ILEC), Competitive Local Exchange Carriers (CLEC) and by companies specializing in data services called Data Local Exchange Carriers (DLEC).

Even though DSL operates over existing t copper wire it requires substantial investment to provide the service. The subscriber needs a DSL modem to convert computer data to DSL signals. At the central office a DSLAM multiplexes individual subscriber lines that are backhauled to the ISP. The ISP routes them to the interexchange carriers that operate the Internet backbone. Equipment is needed to combine and route the signals from DSL subscribers to the Internet, provide domain name service (DNS), mail and news server.

Not all phone lines can be used for DSL. Assuming your local telephone company local central office is equipped for DSL you will not be eligible for service if you are too far away from the central office, if your line has load coils, or if you line is supplied by Digital Loop Carrier (DLC). DLC allows multiple phone lines to share a single copper pair, reducing wiring cost for the Telco. DSL signals are incompatible with existing DLC installation requiring extensive upgrading to DLC to deliver DSL. DSL signals degrade over distance; the exact limit is a function of speed but typical ADSL distances are 12,000-18,000 feet.

Common telephony practices can interfere with DSL. Load coils are inductors that compensate for high frequency loss. They do a good job over the range of voice frequencies but interfere with the high frequencies used by DSL. Loading coils must be removed from DSL lines. Another problem is bridge taps. When cable is installed future use is uncertain. The phone company does not know how many phone lines will be needed at each location served by the cable. To address this uncertainly groups of wires are run past multiple homes. When the installer needs to add a new phone circuit they find an unused pair and connect the house to it. The wire may continue down the road thousands of feet. This is of no consequence for voice but interferes with DSL because the signal bounces off the far end interfering with signaling. This situation is called a bridge tap. Ideally when the DSL line is installed the Telco should remove any bridge taps to improve signal quality.

Deployment of DSL may require the coordination of three different companies. The ILEC owns the copper wire. The CLEC or DLEC in turn rents the line and installs the DSLAM at the Telco and the modem at the subscriber premises. The ISP is the retailer that sells the service to the customer and acts as first line technical support. Needless to say getting DSL properly installed is sometimes a challenge.

For the latest information on DSL service visit to DSL Reports and the DSL Forum.

The USENET news group comp.dcom.xdsl is another good source of information.

2.3 Cable Modem

The cable TV industry is being very aggressive delivering high-speed data. Historically Cable TV was a one-way medium. TV signals originate at the CATV office, called the headend, and are delivered to the cable subscribers. The cable is partitioned into a number of channels and each channel carries a TV signal. Internet service is very different. Instead of a one-way connection from the headend to many subscribers each PC is able to connect to multiple computers and traffic is bi-directional. The cable must support a large number of two-way connections. As is the case with DSL the CATV vendors must install much new equipment. Several TV channels are reserved for data services; this accommodates the downstream path to the users. The upstream path is more difficult. The CATV vendor must replace the amplifiers used to distribute the signal with ones capable of data transmission in both directions. At the CATV office these signals are converted from the cable format and routed to the backbone data network. The network needs to be divided into smaller groups to minimize how many customers share the available bandwidth.

Some early cable implementations were unidirectional. The cable was used for downstream data and a conventional modem for upstream. This allows the CATV vendor to offer high-speed data while it is upgrading its network for bi-directional data.

The CATV industry is working to standardize the interface so cable modems can be purchased in retail stores like analog modem. The industry is rapidly migrating to the DOCIS Data-Over-Cable Interface Specification. Like DSL DOCIS is an always-on connection, it is not necessary to "dial" into the Internet. Typical CATV speeds are 700-10,000kbps.

The USENET news group comp.dcom.modems.cable is a good source of information.

My experience with cable is very limited is has only just arrived in our area.

2.4 Other High Speed Services

The demand for high speed Internet access is driving network innovation. In addition to DSL and Cable fixed wireless services that do not require access to expensive right of way are being deployed on a trial basis. Satellite service is competing with wired service in some areas. The long distance up and back from geosynchronous orbit add significant latency making this type of service more appropriate for file downloading then interactive browsing. The holy grail of broadband is fiber optics. It promises virtually unlimited speed. It is being rolled out in several greenfield areas. New residential development is a prime candidate for fiber converged service; fiber provides broadcast television, telephone service, and broadband Internet access. In a new development fiber is cost effective today. As prices fall more and more homes and small businesses will have direct access to high-speed fiber.

2.5 When "Always On" doesn't mean "Always On"

DSL and Cable modem are marketed as an "always on service." Exactly what always on means depends on how the service is implemented. The most "on" service consists of a static IP address. The DSL connection looks like a LAN. One simply sends bits down the wire. Some DSL providers use a server to allocate IP addresses. This is called Dynamic Host Controller Protocol (DHCP). When a device connects for the first time it asks for an IP address. DHCP issues the address for a period of time called a lease. When the lease is about to expire it is automatically renewed. The benefits of DHCP are that it is much easier to manage then manually assigning static addresses. From the customers point of view it to is always on even during the time the address lease is being updated.

Some DSL and Cable modem suppliers have implemented a technique call Point-to-Point-Protocol over Ethernet (PPPoE) or Point-to-Point-Protocol over ATM (PPPoA). This simulates a dialup connection. This type of service is typically offered to residential customers. It leverages existing ISP investment in dialup authentication and billing. Service contracts stipulate how many hours of continuous use are allowed.

When the time is up the user is unceremoniously disconnected just like a dialup user. This allows more customers to be serviced from the same size pool of IP addresses.

3 Dial Up – The Old Standby

The dialup account is used as a backup incase DSL fails and by the laptop while traveling. Minimizing the number of Internet providers simplifies computer configuration when moving between different connections.

We have been using a local ISP for the past three years.

Our requirements were:

- Nationwide point of presence (POP) access
- Unmetered service
- Reasonable price
- Email account
- USENET News server
- No prohibition against using a LAN
- Does not require special software
- Good technical support

3.1 Selecting a Provider

Initially we use a nationwide ISP that also provided long distance telephone service. We got a single monthly bill and a reasonable rate for Internet Access. Unfortunately the DSL business proved to be very unstable. Carriers merged or sold off consumer accounts every few months. After having our account sold several times we chose the same company that was providing our web hosting service INR.Net. They are a local ISP that met our requirements and have been extremely responsive to e-mail and phone support issues. They bill directly to a credit card eliminating paper invoices.

3.2 Acceptable Use Policy

ISPs have written policy that sets limits on how the service may be used. For example, reselling the service is forbidden. Verify your ISP does not specifically prohibit operating a LAN. Even though the ISP does not disallow a LAN it is unreasonable to expect technical help from them in setting it up.

3.3 Privacy Policy

Examine the privacy policy to determine how your information will be treated. It is reasonable for the ISP to collect and use information for diagnostic purposes and to improve service. However, many ISPs sell customer information to 3rd parties. Your ISP knows every web page you access, every file you download or upload and every mail, USENET and IM message that flows over their network. All of that information can be sold to others depending on the privacy policy.

Most ISP's reserve the right to change policy at any time so the current policy is not an ironclad guarantee.

3.4 Thoughts about Dial Up

Consider ISP mail accounts throwaways, free e-mail accounts or a registered domain name are a better choice if you want a permanent e-mail address. The ISP business is very competitive; assume you will see continuous change and consolidation. If the ISP requires special software make sure it works with the rest of your network environment.

Windows performance Tip - in dial up networking uncheck "Log on to Network." Most ISP use RADIUS authentication, eliminating Windows network login speeds up the initial connection to the ISP.

Windows performance Tip: - Uncheck NetBEUI and IPX in dialup networking. TCP/IP is the only protocol needed to connect to an ISP.

Security Tip: - If file and print sharing is installed unbind it from the dialup adapter. This prevents folks on the Internet from gaining access to shared files.

4 DSL – Telco's Enter the Brave New World of Data

We had been looking at DSL service for several years. Our quest for DSL was driven as much for the extra speed as to learn more about it.

Our requirements were:

- Symmetric speed at least 500kbp/s
- Service Level Agreement
- True always on service
- Single IP address
- No content filtering
- Does not require special software
- Good technical support
- Reasonable price
- No prohibition against using a LAN

We were looking for a near business class service provider. DSL is not mission critical but outages of more then a few hours are very inconvenient. After hearing the horror stories about DSL and Cable modems we wanted to deal with a stable carrier with minimum downtime.

We did not want the provider to perform any firewall functions. We had run into problems in the past with the provider blocking out going mail etc. The goal was a transparent connection. We take responsibility for our security.

In our area Verizon offers various ADSL plans. Verizon offers a total solution they own the wires, provide the network infrastructure and maintain retail sales force. In addition to the Incumbent Local Exchange Carrier (ILEC) other companies called Data Local Exchange Carriers (DLEC) collocate equipment in telephone central offices to offer DSL service. They rent Telco copper pair between the central offices to the subscriber and space in the central office for the Digital Subscriber Line Access Module (DSLAM) equipment. The DSL market is evolving to a three-tiered model. The Telco rents copper pair to a wholesale DSL provider. The wholesaler sells this service to a retail ISP that in turn sells DSL service to end users. This is attractive to carriers because they do not have to staff up to support end users. It creates a rather cumbersome supply chain that makes installation coordination and problem resolution a challenge.

4.1 Distance to the Central Office

Before applying for DSL we attempted to determine our distance from the telephone company central office (CO) Telephone cable does not necessarily follow roads so this is only an approximation. The first step is to determine the location of the central office. DSL Reports has a nice CO search utility. We drove several likely routes to determine the distance. Depending on route our distance was between 9,500 and 14,700 feet.

4.2 Selecting a Provider

Our first attempt was Verizon. Our central office is equipped with Verizon DSL but we did not qualify. No reason was given but it was probably excessive distance. When I plugged in phone numbers closer to the CO they qualified. Next we tried to sign up with a business class DSL supplier. We were turned down due to distance. They estimated we were 20.9K feet from the CO. In retrospect this was lucky because shortly thereafter they got out of the DSL business.

Next we tried Vitts. According to Vitts we were only 10K feet from the CO. As others have also found out DSL prequalification distance estimates are all over the place. The only way to get an accurate measurement is to actually have the line installed. We were concerned the estimate might be too low, but at least it gave us a chance to get the circuit installed. At worst we would have to settle for a lower speed. We signed up for HomeReach 530 service. This is their standard business SDSL 528kbp/s business service with a relaxed service level agreement (SLA). Vitts is interesting because they run a native IP network. They use Net To Net Technology DSL equipment that runs IP over DSL. IP packets are not converted to ATM for DSL transmission eliminating overhead. Vitts also acts as the ISP so the supply chain is reduced to Vitts and Verizon.

4.3 Getting the Circuit Installed

SDSL requires a dedicated line. Vitts handled the coordination with Verizon our Incumbent Local Exchange Carrier (ILEC). Our outside wiring is 20 years old and has been modified several times. I wanted Verizon to reduce wiring clutter and rework the Network Interface (NI). I called the local business office and got a rather quizzical response. They don't have customers calling to discuss how to install telephone company wiring. Fortunately I was transferred to the engineering department and discussed my wishes with a helpful engineer. They agreed what I wanted was reasonable and promised to inform the craftsman when they were dispatched to install the DSL circuit.

Verizon showed up as scheduled and did a great job updating and cleaning up the wiring. Turns out the folks that install data circuits are separate from the normal phone installers. Verizon removed about a 1,500 feet of bridge tap. Removing bridge taps improves DSL performance. This is not done for free, it is up to the DSL provider to request and pay for this service. Bridge taps occur because your phone line is spliced to the cable running down the road. That circuit may continue for hundreds or thousands of feet down the road beyond your residence. This extra cable degrades DSL performance. They installed a new six-line Network Interface device (NID) to replacing a jumble of old lightning protectors and network interface disconnects.

Vitts showed up a few days later and installed the DSL modem, which I was admonished to call a Network Termination Device (NTD). The Vitts Technician connected his laptop to the NTD and got a solid connection at 528kbps. I was elated. I finally had DSL. The next morning the line was dead. The NTD indicated it was unable to sync to the line. Vitts dispatched a tech the following day to replace the NTD. The line has been flawless ever since.

The NTD converts the DSL line to 10Mbp/s Ethernet. It is connected to the WAN port of a Multitech RF500 broadband router that interfaces the LAN to DSL. Vitts uses static IP addresses. This provides a permanent address for as long as I use the service.

Over the last four months I've experienced three short outages. They were always internal routing screw ups within the Vitts network never problems with the local loop.

Total time to get DSL was approximately two months from order entry to going live.

4.4 Optimization

Did the speed tweaks on DSL Reports. Depending on overall network conditions the Speed Test Center indicate 488kbp/s down and 490kbp/s up transfer speed. Trace Route indicate typical 8ms ping times within the Vitts Network and coast-to-coast ping times in the 45-55ms range.

> ***Windows performance Tip*** – Optimizing the TCP/IP stack can significantly improve performance. The speed tweak adjusts the receive window to accommodate fast transfer rate with substantial latency.

4.5 Acceptable Use Policy

Same caution as applies to dialup ISPs be sure to review the acceptable use policy. Make sure the provider does not prohibit operating a home LAN.

Some services place monthly quotas on maximum download or upload quantity. Make sure you fit in any restrictions.

4.6 Privacy Policy

Examine the privacy policy to determine how your information will be treated. It is reasonable for the ISP to collect and use information for diagnostic purposes and to improve service. However, many ISPs sell customer information to 3rd parties. Your ISP knows every web page you access, every file you download or upload and every mail, USENET and IM message that flows over their network. All of that information can be sold to others depending on the privacy policy.

Most ISP's reserve the right to change policy at any time so the current policy is not an ironclad guarantee.

4.7 Service Level Agreement

Business class DSL typically includes a service level agreement. This defines minimum speed, maximum latency, and time to repair if when something goes wrong, etc. These guarantees are one of the reasons business class service is more expensive then consumer. The upside is a guaranteed minimum level of service rather then a best effort promise that make it hard to determine if the provider is delivering the service or not. Data communication is the lifeblood of most businesses one needs to carefully consider the impact of communication failure.

4.8 Turmoil in DSL Land

Making money delivering DSL service turned out to be more difficult then expected. The decline in stock market valuation makes it much harder for companies to obtain financing. This has caused severe problems for many companies. In our case our first choice discontinued DSL service early in 2001. Luckily we were unable to obtain service from them. Our current provider, Vitts is in Chapter 11 bankruptcy. It does not appear they will survive. So we will soon be faced with selecting another DSL provider.

Select your provider with caution and have a backup plan if they run into trouble.

5 Telco Wiring -- Getting Connected

All our communication services are delivered via Telco twisted pair wiring. Verizon provides three phone lines and the DSL provider rents a fourth Verizon line for data. Two of the phone lines are for family use and the third reserved for business.

The two non-business lines are configured as a hunt group. If line 1 is busy incoming calls are automatically sent to line 2. Hunting is unidirectional; if someone calls the second line and it is busy the phone company will not ring the first line if it is idle. Residential service reps may not be familiar with it because it is a "business feature." You may have to press the rep a little to get it. It is especially nice because it is free; the Telco does not nickel and dime you with charges. Line 2 is optioned with call waiting, so even if both lines are busy the caller will not get a busy signal. The goal was to treat the two personal use lines as single main phone number; callers always use the main number. This works well for incoming calls, however outgoing calls are not as simple.

We wanted both lines to return Caller ID information, of the main phone number. Unfortunately that is not possible, caller ID is bound to the specific line. The choices for the second line are to allow Caller ID or disable it. Disabling Caller ID hides the phone number from ordinary users, however some people block incoming calls with Caller ID turned off. If Caller ID is left on people will learn the second number and call it directly, defeating the purpose of the hunt group. We opted to leave Caller ID enabled and remind family and friends to use the main number.

The third line is reserved for business. It is not part of the hunt group. Since the business has only a single line we wanted to use Telco based answering service. Telco answering service is a good match for single line offices because the caller gets voice mail if the line is busy instead of a busy signal. I consider call waiting inappropriate for a business connection. Unfortunately our local central office does not support voice mail so we must rely on an answering machine. Another possibility is to use call forwarding to automatically transfer busy or no answer calls to a cell phone.

The fourth line is used for SDSL. SDSL requires a dedicated line; it cannot coexist with POTS service. DSL is our primary connection to the Internet. If the DSL line fails the router automatically switches to the dialup analog modem.

We did not want to dedicate a line solely for the dialup modem. This leads to sharing problems. Picking up a phone disconnects the data connection and if the phone is in use the computer cannot access the Internet. I looked for an off the shelf solution to this problem but could not find one. So the Modem Access Adapter (MAA) was designed to solve the problem. This eliminated the need for a dedicated modem line and provides optimum use of all three lines. The MAA is located in the main wiring closet by the Network Interface Device.

> ***Usage Tip*** – Call waiting can be disabled at the beginning of the call, disabling call waiting for the duration of the call. The sequence varies by locale, in our area it is *70. Unfortunately if you send the disable sequence to a line not equipped with call waiting it is interpreted as part of the dialed number, resulting in an incorrect connection. This is a problem if the modem uses multiple lines and not all are equipped with Call Waiting. The V.92 standard allows the modem to automatically disconnect/reconnect when it detects call-waiting tones. This can be convenient if one only has a single phone line.
>
> ***Usage Tip*** -- Call waiting and hunting may be used together. Call waiting can only be optioned on the last number in the hunt group.

5.1 Network Interface Device

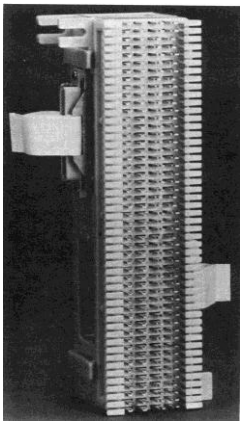
Back in the dark old days when the phone company rented you a phone and did all the inside wiring they made no provision to install customer supplied equipment, commonly called Customer Premise Equipment (CPE). With the advent of telecommunication deregulation the local telephone companies were prohibited from being in the equipment business. This caused a dilemma because there is a need for a demarcation point between the customer and phone company. Everything outside the demarcation point is the responsibility of the Telco; anything inside is the customer's.

The specific embodiment of the Network Interface Device (NID) has changed over the years but the basic purpose remains the same. The Telco installs a device that terminates outside wiring, and provides lightning protection. The customer side has terminals to connect the inside wiring and a method to quickly disconnect inside wiring from the telco for test purposes.

The picture at right shows a typical multiline NID. Telephone company wiring terminates on the left. A cover protects the Telco side. The Telco side contains protection circuits that divert lightning surges to ground. The right hand side has provisions to connect inside CPE wiring and a test disconnect. Opening the cover exposes a RJ11 single line phone test jack. Plugging a phone into the test jack, automatically disconnects the inside wiring. If the test phone works the problem is the inside wiring, if it does not the problem is with the Telco.

5.2 Telephone Wiring Methods

Telephone wiring used to be installed as a daisy chain. Wire originated at the NID and ran to the fist outlet from there to the next, and so on. The FCC recently mandated new telephone wiring be installed using the homerun method wired with at least Cat3 twisted pair cable. Homerun wiring requires each outlet have a separate cable that runs all the way back to the NID. This provides a great deal of flexibility for later changes.



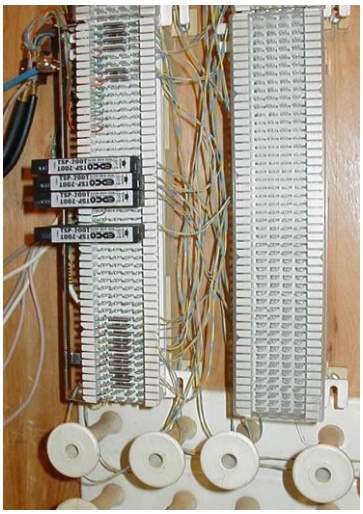
We have taken the homerun method a step farther. In the wiring closet each outlet terminates at a type 66 terminal block. Wires are terminated with a punchdown tool that pushes the wire between contacts and automatically cuts it to length. This speeds up installation because termination does not require cutting, stripping, and tightening the terminal screw. Cross-connect wires connect each phone jack to the proper phone line.

Each phone line has a second test jack. This allows a test phone to be connected to the jack without interfering with other phones on the line. The test phone can also be connected to the NID test jack. This automatically disconnects the internal wiring to determine if the problem is the responsibility of the Telco or us. For convenience a spare phone is kept in the wiring closet for troubleshooting.

Telephone wiring supplies can be purchase at electrical supply houses or on line at Mike Sandman... Chicago's Telecom Expert. They have all the supplies needed for networking and telephony wiring.

> ***Wiring Tip*** -- Clear plastic covers can be used to protect the 66 block terminations.

5.3 Secondary Lightning Protection



The phone company provides lighting protection as part of the Network Interface Device. This is primarily designed to safeguard the network. Electronic devices are somewhat fragile; this is especially the case with computer equipment because they have multiple connections, power, phone, DSL and Ethernet. This makes the equipment susceptible to line surges. Adding secondary protection minimizes the risk of damage. The best place for lightning protection is the building entry point. That allows everything to be bonded together with a low impedance connection. This minimizes voltage difference between different conductors. Lightning protectors do not absorb energy they divert it somewhere else. If the diversion path does not have low impedance a substantial voltage difference is created. This is what kills electronic gear.

These protectors add very little capacitance to the line. The high frequencies used by DSL place special demands on protector to not degrade the signal

Comm-Omni International manufactures secondary protectors. The protector clips to a 66 style split block. In a split block the four horizontal terminals are split down the middle. The Surge protector clips over a pair of rows providing a path from left to the right hand side. The left side connects to the Telco wiring. The right side to internal wiring connects. With the protector remove inside wiring is completely disconnected from the external conductors. A grounding bar runs down the left side of the block. This is connected to a high quality earth ground. Excessive voltage is shunted to ground protecting the equipment. One protector should be used on each telephone line and on any lines that connect to out buildings.

5.4 Modem Access Adapter

If the DSL line fails the router automatically uses the dial the ISP. We wanted a way for the modem to have access to more then one line and to prevent interference between the modem and phones. This maximizes the chance of completing the call while reducing overall cost by eliminating the need for a dedicated modem line.

The modem access adapter is a purpose built device that is designed to isolate the data call from the extension phones. When the modem initiates a call the access adapter detects the off hook condition. The adapter searches for an idle line. If it finds an idle line it disconnects the phones and connects that line to the modem. This prevents the phones from interfering with the computer. If all lines are busy the modem never receives dial tone and retries the connection attempt later. This prevents the modem from trying to dial when all lines are in use.

The adapter is connected to the primary personal line and the business line. When the modem attempts to connect the adapter tests the primary personal line first, if it is busy the business line is checked. The search order assumes that during the day, when the business line is needed, the modem uses a personal phone line. Since the two personal use lines are configured as a hunt group when the first line is busy the call is automatically routed to the second. If the primary home line is busy the data call is placed on the business line. This is most likely to occur after normal business hours, when home phone usage is heaviest.

Two toggle switches control operation. The left hand switch enables or disables the device. It also controls whether or not it searches both lines. The switch on the right selects search order; either line can be selected to search first. The red indicators show which phone lines are in use and which line the modem is connected to.

The Modem Access Adapter was published as a Design Idea in the July 22, 1999 issue of EDN. A theory of operation, schematic diagram, parts list and software listings were published.

5.5 Putting it all together

The drawing shows the overall connection of phone and DSL wiring. Two phone lines are used for personal use and one for business. The modem access adapter is located in the wiring closet and placed in series with the primary family line, and business phone line.

The Telco network interface includes a test jack. Inserting a plug disconnects all house wiring making it easy to isolate problems, to inside or outside. From the NID each line goes to a modular test jack. From there it goes to a secondary lightning protector. The outputs of the protector connect to the various phones. To make changes easier building wiring is terminated to punchdown blocks. Short wires, call cross connect wire, is used to interconnect the various phones. This makes it easy to rearrange wiring by adding and removing cross connect wires without affecting building wiring.

Each telephone jack is wired with two lines, in an RJ14 configuration. Additional lines are run to the home office for the business line, DSL and the analog modem.

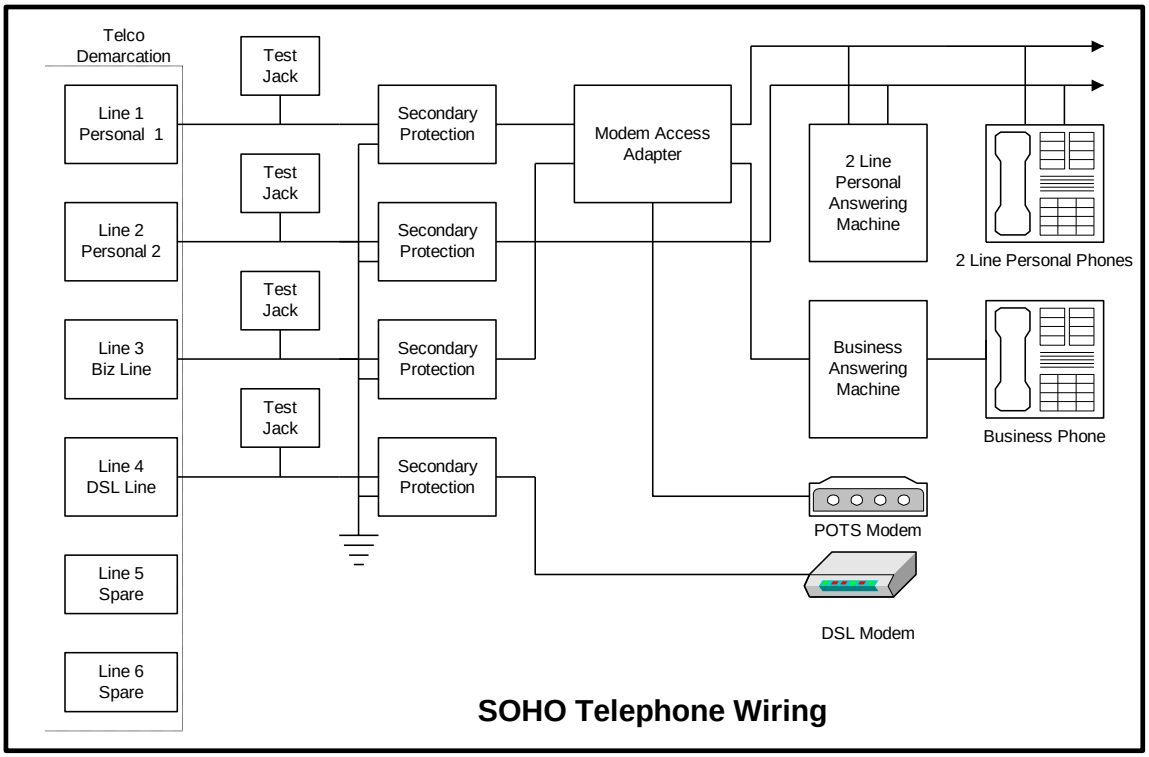


Figure 2 Telephone wiring

6 LAN -- The Networked Home

The Local Area Network (LAN) allows computers to be used anywhere in the house. Each computer has access to shared resources such as printer, files, and the Internet.

The LAN is 100 megabit per second Ethernet over Cat5 unshielded twisted pair wire. Most rooms have two data outlets. The cable from each outlet is run to a central wiring closet. A 16-port hub connects everything together. Ethernet and Cat 5 wiring is the most prevalent LAN technology by far. It is well suited for residential use, components are readily available and easy to install.

The only protocol used on the LAN is TCP/IP. This is the same protocol used on the global Internet

6.1 Ethernet

Ethernet IEEE 802.3 is the most common local network technology used today. It is based on CDMA/CA (Collision Detection Multiple Access Collision Avoidance) scheme. Think of Ethernet as a telephone party line. Before speaking you listen to see if anyone else is talking. If no one is talking then you start. It is possible that several people may start talking at the same time. This is a collision; no one can understand what is being said. When this occurs everyone stops talking for a while. When the line is idle they try again. Each party waits a different length of time to minimize the chance of colliding again. CDMA/CD imposes a number of design considerations on the network. The minimum packet size must be longer then the end-to-end propagation delay of the system. This insures the transmitter is still transmitting when the collision occurs allowing retries to be done by the network layer. Power levels must be set to allow collision detection.

When Ethernet was developed it used a fat coax cable with taps clamped on at prescribed intervals. Today the most common type of Ethernet is unshielded twisted pair (UTP) copper cable, similar to phone wire. This has dramatically reduced the cost of implementing a LAN.

6.1.1 Media Access Controller (MAC) Address

Excerpt from Assigned Ethernet numbers:

> Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits which specify the interface serial number for that interface vendor.
>
> These high-order 3 octets (6 hex digits) are also known as the Organizationally Unique Identifier or OUI.
>
> Ethernet addresses might be written unhyphenated (e.g., 123456789ABC), or with one hyphen (e.g., 123456-789ABC), but should be written hyphenated by octets (e.g., 12-34-56-78-9A-BC).
>
> These addresses are physical station addresses, not multicast nor broadcast, so the second hex digit (reading from the left) will be even, not odd.

6.1.2 10Mbps - 100Mbps - 1Gbps - 10Gbps

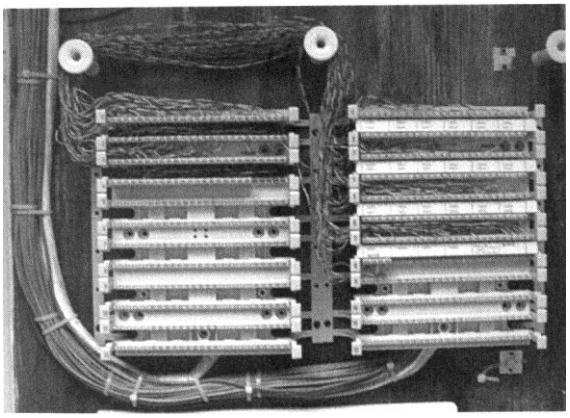
Initially UTP Ethernet ran at 10 million bits per second. Fast Ethernet increased speed to 100 million bits per second over Category 5 wiring. Gigabit Ethernet is 10 time faster then Fast Ethernet, 1,000Mbps. Work is ongoing to increase speed by another factor of 10 to 10 Gigabits per second. Gigabit Ethernet is mainly used for corporate backbone networks but as costs fall it will be deployed all the way to the desktop.

6.1.3 UTP Unshielded Twisted Pair

A significant cost cabling, regardless of the type of network. Wiring has a relatively long life time, 5-10 years in an office building. This means that several generations of computers use the same wiring. The Telecommunications Industry Association set about developing a wiring scheme that was independent of LAN technology. They created five categories based on the maximum frequency the wiring needed to carry. Only two are in widespread use Cat 3 and 5e. Category 3 is typically used for phone wiring and Category 5e for 100Mbps Ethernet. Category 5e is a minor enhancement of Category 5. Gigabit Ethernet was designed to operate over Cat5 copper or fiber optic cable. As Gigabit Ethernet was deployed it was discovered that not all Cat5 installation were up to the task. This resulted in the Cat5e specification. It tightened critical parameters. It is the preferred method of wiring today. There is very little cost difference between Cat3 and Cat5e, most of the cost is pulling, and terminating the wires. It is false economy to limit the installation to only 10Mbp/s.

6.1.4 Structured Wiring

EIA/TIA 568 Category 5e unshielded twisted pair is the preferred standard LANs. Phone wiring typically uses Category 3 because the wire and connectors are a little cheaper. The FCC recently changed rules to require phone wiring to use Cat 3 as a minimum and be run home run fashion like other structured wiring. In “Home Run” wiring each outlet is connect to a separate cable and the cable is run directly back to a wiring closet Splicing or daisy chaining is no allowed.

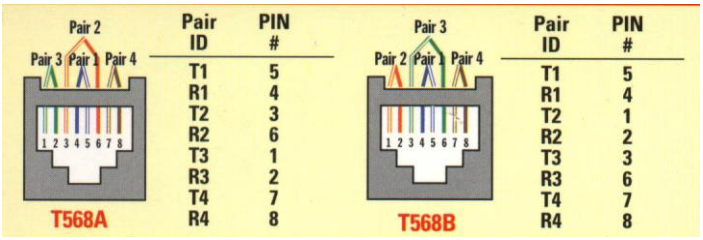


UTP is designed for a maximum of 100meters of length, this includes a patch cord from the computer to the wall jack, 90 meters of wiring (in TIA parlance call horizontal wiring), and another patch cord in the wiring closet to connect facility wiring to the hub. Horizontal wiring is terminated to terminal blocks in the wiring closet. 66 style blocks can be used however 110 style blocks are more common because they are denser, allowing more terminations for a given amount of wall space. The picture shows typical 110 blocks. Network installations use 110 blocks preassembled to modular jacks. The inside wire is terminated to the 110 block on the back of the jack panel. The front of the panel consist of a series of modular jacks. Patch cords connect the terminal block to the hub.

Terminating horizontal wiring at a punchdown block and then connecting selected outlets to the hub with a patch cord makes for a very flexible installation. This is ideal when used with a large number of outlets that are constantly being rearranged. In a small office or home the situation is different, the number of outlets is small and one can purchase a low cost hub with enough ports for all outlets. In a home installation wiring can be terminated directly to UTP plugs in the wiring closet. Plugs are somewhat more difficult install then receptacles so it is not for the faint of heart but doing so eliminates the cost and space of the 110 blocks, and patch cable. The horizontal wiring is terminated with a UTP plug and connected directly to the hub.

6.1.5 568A and 568B Pinout

A cause of much confusion when implementing structured wiring is the fact that two different connector pinnouts were defined T568A and T568B.



They are nearly identical except pair 2 and 3 are swapped. Electrically this is of no consequence as long as both ends use the same pinnout. When wiring a premise pick one version and use it through.

6.1.6 Patch Cables

Patch cable are used to connect devices to wall jack. Normally patch cables are purchased ready made. The pinnout version of patch cables can be ignored since the vendor terminated both ends the choice of pair color does not matter.

Patch cables come in two versions, straight through and crossover. Straight through cables are used in almost all circumstances. Connecting computer to wall jack and to computer to hubs. UTP Ethernet uses a point-to-point wiring scheme. The transmit port of the computer connects to the receive port of the hub, and vice versa. If this default arrangement cannot be used, for example connecting two computers directly together you need to use a crossover cable. This type of cable swaps the transmit and receive pair at one end of the cable so like devices can be directly connected.

6.1.7 Special Tools

Proper tooling is absolutely essential to produce a reliable network. Do not attempt to install and terminate network wiring without proper tools

Tool	**Purpose**
Wire Cutters	Cut Cable to length
Cable Stripper	Special Stripper to remove the outer cable jacket
Punchdown Tool	Terminate 66 and 110 blocks
110 Blade	Terminate 110 blocks
66 blade	Terminate 66 blocks
Crimper	Crimps wires into Plug
Fish tape	Used to snake wire through walls

A good wiring guide is the “Technician’s Handbook -- Communications Cabling” by James Abruzzino ISBN 0-9671630-0-5.

Cabling should be tested after installation; simple testers are in the $100 range making them somewhat expensive for small installation. An ohmmeter will verify end-to-end continuity. This finds many common errors however it will not find split pairs. This is where end-to-end continuity exists but the pairing is incorrect. This type of mistake may work with 10Mbps but will fail at 100. The other concern is excessive untwisted length. When terminating the wire it is important to untwist only enough wire to make the connection and no more.

6.1.8 Wiring Topology

UTP Ethernet uses a point-to-point topology. Each Ethernet outlet must be directly connected to a hub port. The hub regenerates the signals and allows devices to talk to each other, remember the party line analogy. Cable must run directly between the outlet and the hub it cannot be spliced. CDMA/CA scheme used by Ethernet places a limit on how may wire segments and hubs can be between devices. For 10Mbps Ethernet use the 5-4-3 rule, maximum of 5 wire segments and 4 hubs between devices, however only 3 of those hubs can have devices attached. Because 100Mbps Ethernet is faster the rules are more stringent. A maximum of two Class II hubs, and the distance between hubs is limited to less then 5 meters. Class I hubs cannot connect directly to another hub. For all intents and purposes 100Mbps systems are limited to a single hub.

Where hubs need to be cascaded the solution is to use an Ethernet switch. Switches do not simply repeat incoming packets on all ports. A switch examines each incoming packet, reads the destination address and passes it directly to the proper port. Multiple conversations can occur simultaneously as opposed to only one in a hub. Total switch bandwidth is greater then in a hub. A 100Mbp/s hub shares 100Mbp/s among all devices. A switch segments traffic betweens pairs of ports. A non-blocking 16-port 100Mbp/s Ethernet switch has a maximum throughput of 800Mbp/s. This assumes 8 pairs of connections evenly divided between the 16 ports, even though each port is limited to 100Mbps. Switches have another advantage because collisions no longer occur switches support full duplex communication. This means individual computers can be transmitting at the same time they are receiving. This doubles throughput of our hypothetical 16-port switch to 1.6Gbp/s. In actual use the advantage will not be as great but switches offer tremendous advantage over hubs. A typical installation may use a switch in the main wiring closet. Since a switch feeds each drop if more Ethernet ports are needed a hub can be added.

The switch determines connections based on MAC address. Every Ethernet controller has an address. The switch monitors packets as they arrive and associates a port with a specific MAC address. When the switch does not know which port to use it broadcasts the incoming packet to all ports, much like a hub. When the device responds the switch knows which port it is connected to.

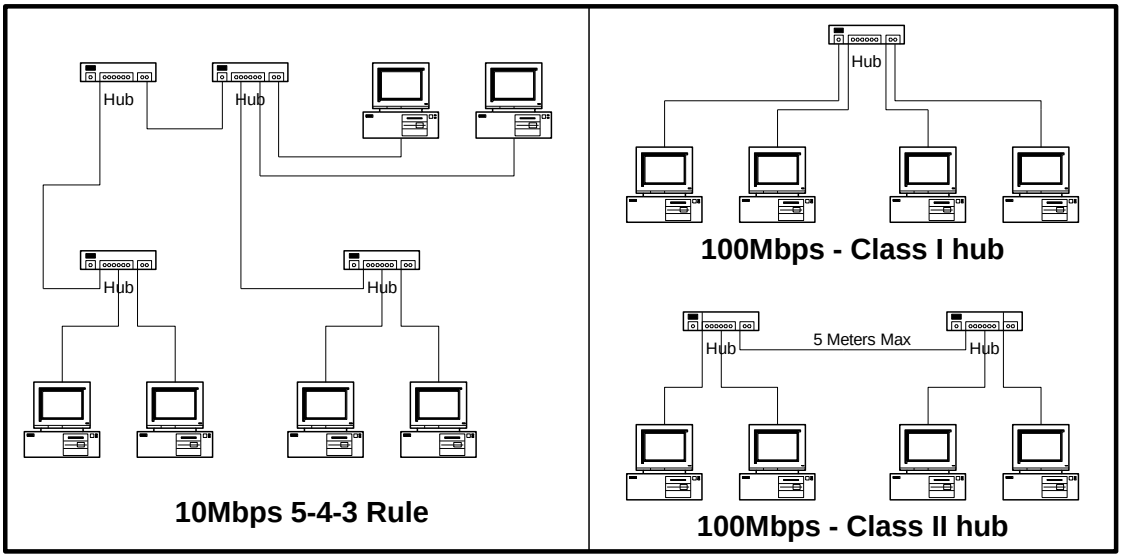


Figure 3 Connectivity rules for Ethernet and Fast Ethernet

6.2 Alternatives to Wired Ethernet

Wired Ethernet is the predominant commercial LAN. It is also popular in new home construction. The cost of installing additional network wiring is low if done when the house is being built.

The situation is more difficult for existing homes without network wiring. Most folks want to share a single Internet connection, and perhaps a printer. Bandwidth requirement are modest. The need is a simple method to network a few computers blazing speed is not required. The cost and disruption of running wiring through the wall discourage folks from installing a home network.

This section examines several technologies that do not require new wiring.

6.2.1 PhoneLine Networking

The Home Phoneline Network Alliance uses phone wiring to create a 1Mbps Ethernet type LAN. This allows computers to be interconnected wherever a phone jack exists. Recent revision to the specification increases speed to 10Mbps. The specification allows analog telephone, DSL, and LAN to coexist on a single pair of telephone wire.

Home PhoneLine LAN use Ethernet packets with minor changes to the header. The physical layer hardware adds the unique header information for transmission and removes it on reception. This make HomePNA look like any other Ethernet LAN to the software drivers.

HomePNA equipped computers cannot connect to UTP Ethernet directly, a bridge is needed to rate match between the two networks and deal with minor signaling difference. Adapters such as the Linksys Network Bridge can be used to connect a HomePNA LAN to Ethernet. This allows HomePNA and Ethernet devices to communicate as if they were all physically connected to the same LAN.

6.2.2 RF Wireless

Traditionally, RF has been expensive and provided relatively low bandwidth. A RF LAN makes sense where mobility is more important then speed.

Radio based communication is relatively easy to eavesdrop. This threat was recognized so wireless LANs provide encryption to maintain privacy. This is especially important in a LAN because an attacker is able to not only eavesdrop but may be able to modify and corrupt computer files.

Most of these devices operate in the 2.4Ghz ISM band. This allows the same radio to be used throughout the world.

IEEE 802.11 is an industry standard Wireless LAN. The LAN can be configured with multiple micro cells to increase total bandwidth. The original version of the spec supported 2Mbp/s, the latest version runs at 11Mbp/s. Work in progress aims to increase this to 22Mbp/s and create a new standard that operates at 54Mbp/s in the 5Ghz band. The WiFi trade association insures interoperability.

802.11 operate in two modes ad hoc peer-to-peer and managed. Managed mode requires an Access Point to bridge the wireless network to the LAN.

HomeRF is an Intel led initiative to standardize on a low cost RF solution for home use. Data rate is 1.6mbps. The initial target is a wireless phone with data capability.

BlueTooth is addressing short-range (<10meters) personal area network market. The goal is to link multiple personal portable devices together. A higher power version extends the range to 100meters. BlueTooth operates at a raw data rate of 1Mbp/s. Typical BlueTooth usage allows a PC, cell phone, and, Palm Pilot to exchange data.

Significant overlap exists between the three competing RF LAN technologies. For the foreseeable future RF technology is at its best where mobility is of paramount importance, and bandwidth of lesser importance.

6.3 TCP/IP

The LAN uses the Internet Protocol (IP) to connect local devices. Using the same communication protocol for the LAN and the Internet simplifies configuration and management of the LAN. IP is the mechanism used to deliver a packet of data from one computer to another. TCP stands for Transmission Control Protocol. IP is an unreliable delivery mechanism it launches packets to the Internet; they may arrive out of order and not at all. TCP orders the incoming packets and requests retransmission of any that are missing. When an application creates a TCP/IP connection the receiver sees the same data stream that was transmitted.

A simpler mechanism, UDP/IP User Datagram Protocol, is used when end-to-end synchronization is not required. UDP is a connectionless protocol. The transmitting station simply casts the packets out to the Internet. Each packet is dealt with individually. UDP is often used with multimedia. If a packet is lost it cannot be retransmitted in time so the receiver has to fake the missing information.

ICMP Internet Control Message Control Protocol handles control function.

6.4 IP Address

Each IP device (node) must have an address. Addresses can be assigned, statically, automatically by DHCP (Dynamic Host Control Protocol) or automatically by the client when DHCP is not present, AutoIP. Traditionally the system administrator manually configured each device with an address. This was labor intensive and error prone. DHCP simplified the task by centralizing address assignment. The down side is a DHCP server is required to allocate addresses. Recently the DHCP protocol has been extended to allow automatic configuration if the host cannot find a DHCP server. In that case the device assigns itself an address after failing to find a DHCP server and automatically determining the address is not in use. This is convenient for small LANs that use IP and do not have access to a DHCP server. This occurs most commonly when two PC's are directly connected. Most Internet sharing packages and hardware access devices implement a DHCP server.

The current version of IP is version 4 each node is assigned a 32-bit address, so the maximum population of the Internet is 4 billion devices. This has been recognized as a serious limitation for some time and a new version of IP version 6 expands the address space to 128 bits. This is a truly gigantic number. If IPv6 addresses were uniformly distributed over the Earth it would result in thousands of addresses per square foot. Several techniques are discussed to conserve the limited IPv4 address space.

6.4.1 Dotted-Decimal Notation

Internet addresses are expressed in dotted decimal notation, four decimal numbers separated by periods, nnn.nnn.nnn.nnn. The 32-bit address is divided into four 8-bit fields called octets. Each field has a range of 0-255. The smallest address is 0.0.0.0 and the largest 255.255.255.255.

6.4.2 Subnet

IP addresses consist of three components, the Network-Prefix, Subnet-Number and the Host Number. The purpose of Subnetting is to allow IP addresses to be assigned efficiently and simplify routing.

For our purposes all the computers on the network must be on the same subnet. For example our network allows up to 254 hosts (computers) the subnet is 255.255.255.0, also called a /24 subnet because the first 24 bits are fixed.

6.4.3 Port Number

A single computer may be connected to multiple hosts over the Internet. How does the computer know how to deliver each packet? For example, while writing this paper my mail program is checking e-mail, and I'm listening to a Real Audio radio program. Each IP packet includes a port number. Port numbers are 16 bit values that range from 0-65,535. For example when you enter a URL into you web browser to access a World Wide Web site the browser automatically uses port 80. The low port numbers 0-1023 are called the well-known ports; they are assigned by IANA the Internet Assigned Number Authority when a particular service is defined. Software uses that port to make initial contact. After the connection is established the high numbered ports are used.

6.5 Private Addresses

The Internet Assigned Number Authority assigns Internet addresses. This is the entity that assigned the addresses used by your ISP. IANA allocated three blocks of private addresses that are guaranteed not to be used on the Internet RFC 1918. The private addresses are ideal for a small LAN. Devices on the LAN are assigned from the pool of private addresses. This eliminates the need for coordination of the IP addresses used on the LAN with those used on the Internet at large. When a computer on the LAN needs to access the Internet the gateway router uses a technique called Network Address Translation (NAT) to convert the private IP addresses to the public address assigned by the ISP.

Excerpt from IETF RFC 1918 Address Allocation for Private Internets

> The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets:
>
> | | | | |
> |---|---|---|---|
> | 10.0.0.0 | - | 10.255.255.255 | (10/8 prefix) |
> | 172.16.0.0 | - | 172.31.255.255 | (172.16/12 prefix) |
> | 192.168.0.0 | - | 192.168.255.255 | (192.168/16 prefix) |
>
> We will refer to the first block as "24-bit block", the second as "20-bit block", and to the third as "16-bit" block. Note that (in pre-CIDR notation) the first block is nothing but a single class A network number, while the second block is a set of 16 contiguous class B network numbers, and third block is a set of 256 contiguous class C network numbers.
>
> An enterprise that decides to use IP addresses out of the address space defined in this document can do so without any coordination with IANA or an Internet registry. The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the enterprise, or the set of enterprises, which choose to cooperate over this space so they may communicate with each other in their own private Internet.

In our implementation DHCP is built into the Multitech broadband router. We use Class C private addresses in the range of 192.168.2.x this allows up to 254 hosts on the LAN. The IP address of the NAT router is statically assigned as 192.168.2.1. The DHCP server in the router then assigns an IP address to each client from the pool of remaining addresses.

Some devices work better with a static address. Our local web and print server are assigned static address so the address is constant. An option in the router forces the router to always issue the same address to a given device.

6.6 LocalHost Address

127.0.0.1 is a reserved loopback address. This is useful for testing to makes sure everything in the computer is working correctly. This allows you to sent packet to the machine you are running on.

6.7 Gateway

Ethernet is local network. This means each device is in direct communication with all the other devices. When devices need to discover information on the LAN they broadcast the request to everyone. This works well on a small network but does not scale very well; the network quickly becomes overloaded with broadcast messages. The solution to this problem is to interconnect individual LANs with a router. Routers have the intelligence to connect multiple networks together. This confines the broadcast discovery mechanism to a small group.

Routers have IP addresses like any other device. When a computer is unable to connect directly it forwards the packet to the router. The router in turn sends it to the correct host or to another router in complex networks.

Routers are also called Gateways, since they link multiple networks together. This is one of the parameters that each device on the LAN needs to know. When a DHCP server is used it sets this address automatically. In our network the Gateway address is the broadband router. This is the gateway to other networks.

The name Internet is a contraction of Internetwork. The Internet is a network of networks.

6.8 Name Resolution

Entering long strings of numbers such as 192.168.0.3 is not very convenient. The Domain Name Service (DNS) allows a name to be used instead of a number. When you enter a name into your web browser such as http://www.yahoo.com the browser first checks to see if this is a name of a device on the LAN. If it is not local the request is forwarded to a DNS server. Your ISP provides the first server in the chain. If it doesn't know the address the request is passed to other DNS servers until the number is found. Once the system obtains the IP address it uses the address to connect to the remote host. DNS names are intended as a convenience for humans, computer use IP addresses to communicate. DNS acts as a giant Internet "White Pages."

Computers on the LAN use a different name resolution mechanism. Names are broadcast using NetBIOS over IP. This works well when on small LANs, it eliminates the need to use a local DNS server or other name resolution technique.

6.9 Whois

Some times it is useful to look up the owner of a domain. The WHOIS database stores contact information for each registered domain name.

6.10 Network Neighborhood – My Network Places

Windows network neighborhood allows one to browse networked computers. To show up in the neighborhood each machine must be configured for file and print sharing, even if nothing is being shared. The neighborhood is organized by workgroup name, in a small LAN all machines typically belong to a single workgroup, like HomeLAN. At least one machine in each workgroup must be configured as the Browse Master. Ideally this is a machine that is left on all the time. Browse Mastership is negotiated at power up; in general it is a good idea to disable the Brows Master on the clients. If the Browse Master is running on a client, the network neighborhood becomes unavailable when the client is turned off, until the remaining machines arbitrate Browse Master ownership again.

Windows Security Tip – File and print sharing is a much-debated topic. By default file and print sharing is configured to be accessible to all interfaces. Sharing should be disabled on any interface that has direct access to the Internet, such as dialup modem. Go to Networking on the Windows control panel find the entry that starts TCP/IP ->Dialup Adapter, go to Bindings and uncheck "File and Printer sharing for Microsoft Networks." Unchecking this feature prevents access to shares by anyone on the Internet while still allowing LAN access.

Windows Configuration Tip – If one machine is always on force it to become the Brows Master. This guarantees the Network Neighborhood is always available. Go to File and Print sharing in Network control panel. Open the Advanced tab, highlight Browse Master and change the Value to Enabled. Set it to disable on each client.

Windows Configuration Tip – a computer must have the file and print sharing service running to be visible in network neighborhood. Sharing must be installed even if nothing is shared.

Windows Configuration Tip – There appears to be a compatibility problem between Win2000 and Win98/ME browsing. We had trouble getting a Win 98 machine to show up in a network of Win 2000 machines. The solution to was to create separate workgroup names for the Win 2000 and Win98 machines. All machines have file and print shared enabled.

Windows Configuration Tip – If Windows is configured for user authentication and you do not enter a password access to Network Neighborhood is denied, even though other IP based communication is allowed.

6.11 Implementation

The LAN wired with Category 5 cable connected to a SMC 16-port 10/100BaseT hub. Except for one laptop all network Ethernet adapters operate at 100Mbp/s. The cost difference between 10 and 100Mbp/s Ethernet is negligible. In a mixed environment use a 10/100-hub autosensing hub to automatically convert between 10 and 100Mbp/s Ethernet ports. This provides seamless upgrade to 100Mbp/s. When purchasing a hub get one with more ports then you think you will need, networks tend to expand over time.

Rather then terminating the cables at a patch panel they were directly terminated with CAT5 plugs. Terminating plugs is harder then receptacles but it eliminated the need and cost of a patch panel and patch cables.

Computers run Windows 98. The only communication protocol is TCP/IP. IPX and NetBEUI are not installed. TCP is used Internet access and file and print sharing. Most machines are assigned a dynamic IP address, except for servers, which get a permanent address bound to the MAC address.

One PC is dedicated for use as a server. It has the Browse Master enabled, and runs local web server, time, and file server. A printer server is used for network printing.

Ethernet Tip – The most flexible hub is 10/100 autosensing. This allows a mix of 10 and 100Mbp/s computers. Internally the hub combines all low-speed ports together and all high-speed ports. If a packet goes between different speed ports the hub does a store and forward. The packet is completely assembled at the incoming speed then sent out at the outgoing speed.

7 Broadband Router – One Address So Many Computers

When the LAN was first set up we used proxy software running on a laptop. This allowed multiple computers to share a single ISP account. The software included a DHCP server to automatically allocate IP addresses. This was convenient and at the time a cost effective solution, assuming one has a spare computer available.

Over time several shortcomings became apparent:

- Each application must be configured to use the proxy. This makes moving a laptop between LANs difficult. We wanted to replace Proxy with NAT.
- Streaming services such as Windows Media Player and Real Audio player do not work well behind a proxy. NAT solves this problem.
- Even though sharing software does a good job protecting PCs on the LAN the machine connected to the Internet is vulnerable. If that machine is compromised the attacker has access to everything on the LAN. To protect this PC I was running both the sharing software and a firewall. This was fragile installing the latest Microsoft patches often broke the firewall.
- When one factors in the total cost for software solution, extra NIC card, sharing software, firewall very little difference exists between software and hardware solutions.

I wanted to be able to take advantage of high speed Internet connection and share it among all computers just as we were doing with dialup. However, I was also aware of the DSL horror stories so I wanted to set up a system that could do automatic fallback to dialup. This minimizes the chance of losing all Internet connectivity.

Router requirements:

- Ethernet port for DSL
- RS232 Serial port for dialup modem
- Automatic fallback to analog modem if broadband fails
- NAT support using single public IP address
- 4 port 10/100 Ethernet Switch
- DHCP server for LAN addresses
- Dynamic and static IP address assignment on LAN
- IPsec pass through for VPN (that came later)
- Good tech support

The device I finally purchased was the MultiTech RF500S. I've been very pleased with the choice. It meets our entire technical requirement and technical support has been outstanding.

7.1 DSL Interface

DSL providers offer three types of modem, External Ethernet, External USB, Internal PCI. There are pros and cons to each. External Ethernet is the most flexible because it can be use with a single computer or a router. PCI and USB must be directly connected to a PC.

The computer interface of the NetToNet network termination device is Ethernet. This connects directly to the Wide Area Network (WAN) port of the router. My DSL service uses static IP addresses so configuration was simple, entered DSL IP address, Subnet mask, and Gateway address. In the DNS section I entered the addresses of the two DSL DNS server. Once those setting were entered and saved we were up and running.

7.2 Automatic Fail over

When a client on the LAN requests Internet access the router verifies the DSL connection is working. If it is bad the router automatically uses the analog modem to connect to the dialup ISP. The router includes an idle timer to disconnect the modem after a period of inactivity. When DSL service is restored the dialup connection is automatically terminated.

This feature has turned out to be very useful. The router was set up before we had DSL. This allowed us to test and debug the configuration to prior to getting DSL After several months of use DSL has only gone down three times and each time only for a short interval. The causes of the failures were a surprise. Except for the first time when the DSL modem failed we have not had a link failure. All the problems have been short-term router screw-ups within the ISP.

Setting the dialup modem was similar to Windows dialup networking. Had to enter a phone number, user name, and password. The dialup IP is set automatically by the ISP. The DNS servers provided by the dialup ISP were of course different then the one from the DSL ISP. These are entered as the third and fourth DNS addresses. This allows the network to use two entirely different sets of DNS servers in case of a malfunction.

7.2.1 Using multiple ISPs

The fallback feature is great but it adds some complexity in setting up the network. Normally you use the DNS servers provided by your ISP to translate domain names to IP addresses. If your DSL ISP is down so might their DNS servers. The solution is to include entries for DNS servers from both DSL and dialup ISPs. Luckily the router has entries for four DNS servers; this is enough for primary and alternate DNS servers from both ISPs.

The other problem concerns outgoing mail. This is not an issue if you use one of the free Internet mail services. If you use a POP/SMTP mail client connecting through different ISPs will interfere with sending mail.

As the Internet has become more popular some of the assumption made in the initial design have come up short. One of the worst is an almost complete lack of security and authentication. Mass mailers have exploited this weakness to inundate users with unsolicited email called SPAM. The SMTP outgoing mail relay cheerfully accepts all outgoing mail sent to it and delivers it to everyone on the address list. Stammers love this, all they need to do is find an open SMTP mail server and they are in business. As a counter measure most ISP's require the mail be sent from inside the network. This restricts outgoing mail to users that are currently logged in giving the ISP some control. Normally this is not an issue dialup customers are authenticated at connect time and DSL or Cable customers are hardwired to the network. The problem during failover is that we are no longer using the DSL account we are using dialup. Different companies supply these accounts so authentication is not shared. The DSL SMTP mail server will reject mail received from foreigners.

An added complication is that some ISPs will not even allow you to send mail to a foreign SMTP mail gateway. If that is the case no need to read the rest of this section because you are dead in the water.

We need a mechanism that allows us to send mail regardless of how we connect to the Internet. We want this to occur without manual intervention. Later in this paper we discuss a program called NetSwitcher that we use to move a laptop between multiple LAN.

We discussed this problem with our dialup ISP. Our dialup ISP also host our web site and provides email service. The most secure solution is to be authenticated by the SMTP server. This way outgoing mail is just like access to incoming POP mail. If your ISP supports this feature you can use the same SMTP relay regardless of how you connect. The other fix works if your DSL address is static. In that case your dialup ISP accepts SMTP mail if you are log in directly or if it comes from a specific IP address. This isn't

foolproof since IP addresses can be spoofed, so caution is still advised. Both solutions eliminate the need to reconfigure anything during fail over.

7.3 LAN Address Assignment

Each device on the network requires an address. The LAN uses private addresses. These addresses are not used on the Internet therefore they do not need to be coordinated with other Internet users. They still must be coordinated within your network since addresses cannot overlap.

7.3.1 Dynamic

In most cases dynamic address assignment is convenient. When a new machine is plugged in the DHCP server, built into the router, assigns it an address. Once the device has an address is can use the LAN. The DHCP server assigns several other critical numbers, a subnet mask and a gateway address. As discussed previously the subnet mask defines how the address should be interpreted. Only machines on the same subnet can directly communicate. The gateway address is where the computer sends any packets that cannot be delivered locally. The gateway is the router. It is up to the router to determine how to deliver the packet. In our case this is very simple, any message not addressed to a host on the LAN is forwarded to the ISP. The router also tells the computer on the LAN what address to use for DNS lookup.

7.3.2 Static

For some devices, such as servers, dynamic addresses are a problem. The MultiTech router does not implement DNS for LAN based devices. That means local servers need to be accessed by IP address rather then name. We need the ability to permanently assign an address to a specific device. The router has a neat solution for this problem. All addresses are dynamically assigned. However once an address is issued it can be locked so it never changes. This is ideal each device thinks it is getting a dynamic address while the administrator is able to freeze specific address.

The router performs this bit of magic by binding an IP address to the Ethernet MAC address. Each Ethernet device has a unique 48-bit Media Access Controller address. This is how Ethernet devices communicate with one another. This is much more convenient then setting IP addresses manually and making sure they do not conflict with previously assigned addresses or the DHCP pool.

7.4 NAT -- Sharing a Single Internet Connection

The LAN cannot simply be “plugged in” to the Internet. Because the addresses used on the LAN cannot be used on the Internet and because the ISP only provides a single address we need a translation mechanism between the two networks. Network Address Translation (NAT) provides a mechanism to translate addresses on one side to addresses on the other. When NAT is combined with private IP addresses we have the ability to create a LAN with an unlimited number of local addresses and map them to a single public address.

The way NAT works is that all addresses used on the LAN come from the private address pool. IntraLAN communication proceeds normally NAT is not required. When a request cannot be serviced locally it is passed to the NAT router. The router modifies the address and port number to match the public address issued by the ISP and sends it on it way. When the reply comes back the router converts the address to that of the original device and forwards it to the LAN. The NAT router can keep track of a large number of sessions so multiple devices can use the same address.

For more information see RFC1631 The IP Network Address Translator (NAT).

7.4.1 Limitations of NAT

As useful as NAT is it is also controversial. It breaks the end-to-end paradigm of the Internet. The NAT device is required to maintain state information and if it fails recovery is not possible. It also interferes with server functions and most types of VPN.

When NAT was first developed it was assumed that the private address pool was private and no one but the administrator cared about the assignment. Today in the age of VPNs these internal addresses ARE being exposed. If a telecommuter's LAN and the office are both using private address they may overlap. In a simple case this is not a problem, the home user simply moves their LAN to a different group of private addresses. But what happens if the home LAN must support two telecommuters. This requires the coordination of two corporate LANs and the SOHO LAN. In this case the conflict may not be resolvable.

By design NAT blocks all remotely originated traffic. It acts as a firewall because it does not know how to route traffic that originates outside the LAN. This is often touted as a major security benefit but it causes tremendous problems if one wants to run a server. NAT makes it very difficult to run multiple servers such as used for telephony and gaming. Since only a single external IP address exists, incoming requests can at most be mapped to a single physical device.

This is not to discourage use of NAT it is very powerful technique. But NAT should be seen for what it is, a short-term workaround to minimize the impact the IP address shortage, not a permanent extension to Internet technology.

For more information see RFC 2993 Architectural Implications of NAT.

7.5 10/100 Ethernet switch

The office is wired with 4 Ethernet drops feed by the whole house 10/100 hub. This turned out to be inadequate so the built in 4-port Ethernet switch was very handy. This must be an Ethernet switch because a hub is used in the wiring closet, and two hubs cannot be cascaded at 100Mbp/s. One port on the switch is configured as the uplink port. This connects to the existing 16-port hub. The file server and office desktop connect to the switch to take advantage of switch bandwidth. Everything else goes through the hub. This increased the number of SOHO office ports to 6 eliminating the need to pull more wire.

> ***Configuration Tip*** -- many residential broadband routers include multiple Ethernet ports. Check the fine print, as to speed and whether it is a hub or a switch.

7.6 Virtual Private Network

Companies are using VPNs to extend the corporate network to telecommuters and business partners. In our situation a Checkpoint firewall/VPN is used to secure the corporate network. I wanted to be able to access this network from home and on the road as a telecommuter.

There are many was to configure a VPN. It can be setup to tunnel everything from the remote site to the corporate LAN. This is typically used to connect remote offices. We wanted to provide employees with secure access to the corporate network but not force all remote traffic through it. In addition some users, such as yours truly, run networks behind NAT routers. This added a level of complexity to the setup.

The preferred VPN is IPsec, as defined by the Internet Engineering Task Force IETF. IPsec has options to encrypt the entire packet, including IP address and port number; address information is also embedded in user authentication. This is the most secure way to configure the VPN and is commonly used to create a tunnel between two offices. Unfortunately it is incompatible with NAT, because NAT needs change the host address to convert from the local private address space to the public Internet. Most VPN's have options to work around this by not encrypting the host's physical address. We were able to pick authentication and encryption options that work with NAT. In operation when the user requests access to a

host on the corporate network the VPN authentication box pops up, once authenticated the VPN encrypts data flowing between the user's computer and the corporate firewall. The VPN client is selective, it knows which IP addresses reside on the corporate LAN it ignores other addresses so they operate normally

Getting this to work required updating the firmware in the SOHO router. Installing later VPN software at the office and client. User authentication was changed to a NAT friendly version. Now that the VPN is up and running it works without a hitch. The only minor inconvenience is on machines configured for dialup networking. When the VPN is activate it also pops up the dialer even when connected to a LAN.

For more information refer to RFC 2709 Security model with tunnel-mode IPsec for NAT domains.

VPN Installation tips:

- Verify VPN software is compatible with NAT
- Verify broadband router firmware is compatible with your VPN software
- Make sure your IT department has configured the VPN to be NAT friendly
- If both the home network and work network use private IP addresses make sure no conflicts exist. The same addresses cannot be used in both locations.
- It is possible to bind VPN clients to a specific remote IP address. If your DSL provider offers a static IP address this is not a problem, inform your VPN administer of your address. If not your administrator will not be able to bind your account to a specific address.
- VPN's extend the trust environment to the employees PC. If this computer is compromised so is the corporate LAN. Employees and family members need to understand safe computing practices.

7.7 Logging

The router creates several logs. It maintains statistics on the amount of traffic generated and received by each device, logs sites accessed by each PC, and logs intrusion attempts. This information can be copied to a file for additional analysis.

8 Debug -- When Things Go Wrong

Unfortunately networks occasionally fail. When a failure occurs it is often difficult to determine the underlying cause. Luckily, Windows includes a number of built in diagnostic tools.

Test	Result
Ping by IP address	Two machines can successfully connect
Ping by Name	DNS is working, Two machines can connect
WinIPcfg	Network adapter settings
Net View	DOS version of Network Neighborhood
Netstat -a	Active Ports
Trace Route	Host to host path
Modem Test	Modem vendors self test

In addition to the built in Windows tools DSL Reports has a number of tuning and diagnostics test on the tool page http://www.dslreports.com/tools.

8.1 PING

PING is a command line utility to determine if a remote machine is reachable. The host is specified by either IP address or domain name. PING uses the Internet Control Message Protocol (ICMP) to determine round trip time to the remote host. In the first example we pinged the gateway on the local LAN by its IP address. In the second case we ping a public web server on the Internet by its domain name. The third example shows a typical report when the host ignores ping requests.

Ping is very useful to verify the various computers can access the LAN. If the computer cannot ping or be pinged low-level communication is broken and needs to be fixed.

Not all computers respond to ping requests. Some administrators disable the response. In that case you get a timeout.

Example 1: Ping local computer IP address.

```
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum =  2ms, Average =  1ms
```

Example 2: Ping remote host by DNS Name.

```
Pinging dslreports.com [209.123.109.175] with 32 bytes of data:

Reply from 209.123.109.175: bytes=32 time=26ms TTL=242
Reply from 209.123.109.175: bytes=32 time=21ms TTL=242
Reply from 209.123.109.175: bytes=32 time=23ms TTL=242
Reply from 209.123.109.175: bytes=32 time=20ms TTL=242

Ping statistics for 209.123.109.175:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum =  26ms, Average =  22ms
```

Example 2: Ping remote host by DNS Name, ICMP response disabled.

```
Pinging www.compaq.com [161.114.19.252] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 161.114.19.252:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

8.2 NET

NET is a command line utility to display information about Windows networking and workgroup

```
NET CONFIG     Displays your current workgroup settings.
NET DIAG       Runs the Microsoft Network Diagnostics program to display
               diagnostic information about your network.
NET HELP       This list
NET INIT       Loads protocol and network-adapter drivers without
               binding them to Protocol Manager.
NET LOGOFF     Breaks the connection between your computer and the
               shared resources to which it is connected.
NET LOGON      Identifies you as a member of a workgroup.
NET PASSWORD   Changes your logon password.
NET PRINT      Displays information about print queues and controls
               print jobs.
NET START      Starts services.
NET STOP       Stops services.
NET TIME       Displays the time on or synchronizes your computer's
               clock with the clock on a Microsoft WfW, Windows NT,
               Windows 95, or NetWare time server.
NET USE        Connects to or disconnects from a shared resource or
               displays information about connections.
NET VER        Displays the type and version number of the workgroup
               redirector you are using.
NET VIEW       Displays a list of computers that share resources or a
               list of shared resources on a specific computer.
NET ?          This list
```

8.3 NETSTAT

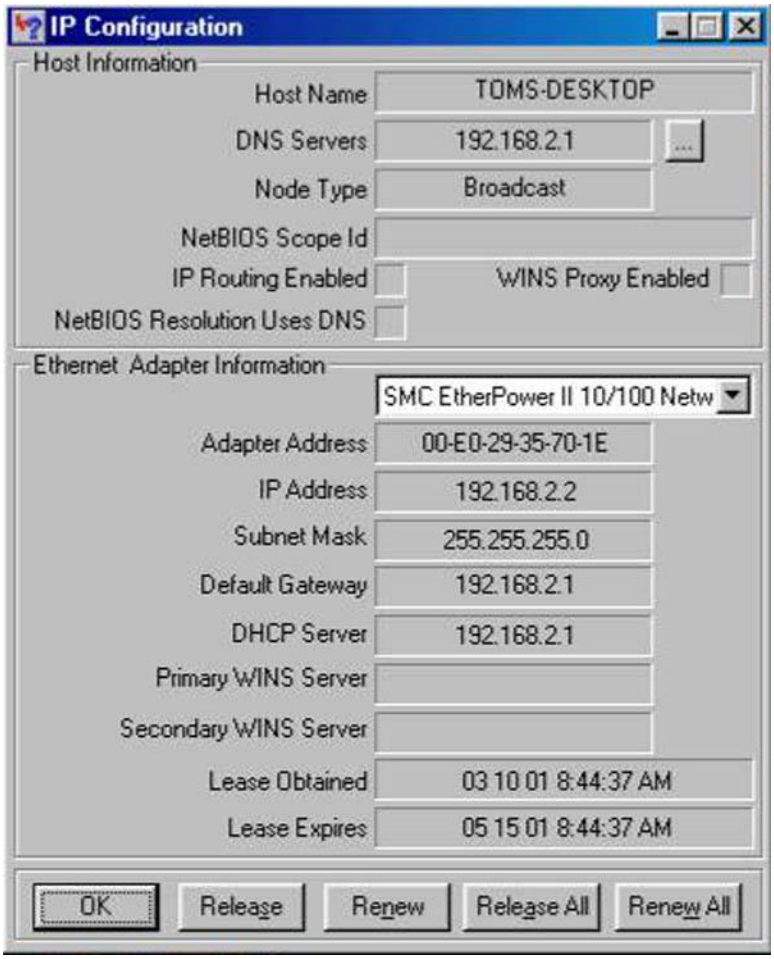
NETSTAT is a command line utility to display protocol statistics and current TCP/IP network connections.

```
NETSTAT –a          Displays all connections and listening ports.
NETSTAT –e          Displays Ethernet statistics. This may be combined
                    with the -s option.
NETSTAT –help       This list.
NETSTAT –n          Displays addresses and port numbers in numerical
                    form.
NETSTAT -p proto    Shows connections for the protocol specified by
                    proto; proto may be TCP or UDP.  If used with the -s
                    option to display per-protocol statistics, proto may
                    be TCP, UDP, or IP.
NETSTAT –r          Displays the routing table.
NETSTAT –s          Displays per-protocol statistics.  By default,
                    statistics are shown for TCP, UDP and IP; the -p
                    option may be used to specify a subset of the
                    default.
Interval            Redisplays selected statistics, pausing interval
                    seconds between each display.  Press CTRL+C to stop
                    redisplaying statistics.  If omitted, netstat will
                    print the current configuration information once.
NETSTAT ?           This list
```

8.4 WINIPCFG

In versions of Windows versions WINIPCFG displays the current configuration for each network adapter. In Windows 2000 use the IPCONFIG command in a DOS box. WINIPCFG lets you look at each network adapter in the computer. The first is the virtual adapter for dialup, and then each network adapter is shown.

The first thing to check is that the computer has the correct IP address. In addition to address and subnet two other important fields are Adapter address and Default Gateway. The adapter address is the hardware address assigned to the physical network interface. For Ethernet this is a 48-bit Media Access Controller (MAC) address. The Default Gateway tells IP software where to send packets that are not on the local LAN.



8.5 Trace Route

Trace Route uses Internet Control Message Protocol (ICMP) to find each hop between the user and the remote host, and the delay to each hop. This is very useful to determine the underlying cause of slow or unavailable hosts. Trace Route uses the Time To Live (TTL) field to cause the ICMP packet to be rejected because it has gone through too many hops. When this occurs the host informs the sender that the packet has expired. Trace Route uses this information to build a path map and response time list to each hop between the source and destination. Note in some cases hosts do not respond to being pinged, Trace Route still works but it will timeout to those hosts.

The Windows version of Trace Route is TRACERT a command line utility. VisualRoute provides the same information as TRACERT in a graphical format. In addition it performs a WHOIS lookup to determine

where the site is located and who owns it. This information is then displayed on a map to show overall routing.

Typical TRACERT report:

```
Tracing route to dslreports.com [209.123.109.175]
Over a maximum of 30 hops:

  1  1ms   1ms   1ms 192.168.0.1 (Note: Broadband router address)
  2 10ms   9ms  11ms 064-031-085-129.inaddr.vitts.com [64.31.85.129]
  3  9ms  11ms  10ms 064-184-151-021.inaddr.vitts.com [64.184.151.21]
  4 15ms  13ms  13ms 216-064-088-006.inaddr.vitts.com [216.64.88.6]
  5 16ms  14ms  16ms 216.35.204.130
  6 14ms  15ms  17ms 216.34.127.126
  7 14ms  16ms  17ms bbr01-g2-0.wlhm01.exodus.net [64.14.70.67]
  8 21ms  19ms  19ms bbr01-p4-0.whkn01.exodus.net [209.185.249.37]
  9 19ms  20ms  20ms bbr01-p1-0.jrcy01.exodus.net [209.1.169.54]
 10 22ms  24ms  22ms dcr03-g4-0.jrcy01.exodus.net [216.32.223.99]
 11 20ms  21ms  22ms acr01-p4-1-0.jrcy01.exodus.net [216.32.222.218]
 12 20ms  21ms  23ms 209.67.40.14
 13 47ms  25ms  25ms s4-0-1.core2.oct.nac.net [209.123.11.25]
 14 40ms  39ms  38ms f0-0.colo1.oct.nac.net [209.123.168.226]
 15 42ms  25ms  33ms dslreports.com [209.123.109.175]

Trace complete.
```

This indicates how long it took to get a response from each hop, and the IP address and name of each hop.

9 Browsing -- Wild Wild Web

All PCs use Microsoft IE5.5 the browser is equipped with 128-bit encryption for added security.

10 E-Mail -- Mail at the Speed of Light

E-mail accounts fall into three broad categories; ISP account, browser based free mail and having your own domain name. ISPs typically offer one or more mail accounts. This is convenient but ties your e-mail address to your ISP. Change ISP and your e-mail addresses changes. Free mail services like Yahoo and HotMail are advertising supported. They decouple your e-mail account from your ISP. Free accounts make sense for personal use. Even though they are advertising supported the advertising is not overly intrusive. Because these accounts use standard web browser they have the advantage that you can access mail from any computer. If you have a domain name your mail is addressed to you@yourdomain.com. If you change the hosting service you simply transfer you domain to the new provider, your mail address stays the same. This is the best solution for a long-lived e-mail address.

Another benefit of using your own domain name is that you can create as many user names as you want. This comes in handy for sites that force you to register. You can create a unique name for each site so you can track how they use and abuse the information you released.

10.1 Web Mail

Web based mail eliminates the need for specialized mail clients. Sending and receiving mail uses a web browser. This allows to mail from any computer with Internet access. The user interface is less convenient then a mail client but is useful for casual use.

10.2 POP Mail

E-mail has a sending component, SMTP, and a mailbox part POP. When you compose and send e-mail your mail program connects to the SMTP (Simple Mail Transport Protocol) mail server. The SMTP server acts as a relay between your e-mail client and the Internet. The SMTP server verifies that each recipient is accessible and returns an error message if not. Incoming mail is delivered to the POP server, (Post Office Protocol) maintained by the ISP. It works much as a post office box. Mail is stored temporally until you have a chance to retrieve it. The e-mail program connects to the POP sever and downloads the mail. Normally the client tells the server to deletes mail once it is transferred but this can be overridden so mail remains on the server. This is convenient if you access mail from more then one machine.

> ***Security Tip*** -- Be careful opening e-mail attachments. This is the most common method of spreading viruses and trojans.
>
> ***Security Tip*** -- The aforementioned warning has been issued many times. What is less well known is that simply reading e-mail can infect your system. ActiveX controls or VB scripting can be embedded in the body of a mail messages. Reading the message activates the virus.
>
> ***Security Tip*** -- Spam is a big problem. Many ISP's restrict SMTP access to customers logged into the service. This means if you have multiple ISPs or a domain hosting service you may not be able to use a particular SMTP server. This causes trouble if you use difference ISP's for example DSL and dialup. This is discussed in the laptop and router automatic fail over section.

10.3 Corporate Mail

Telecommuters need to be able to access corporate mail from the SOHO LAN. Depending on where the mail server is located this may prove to be difficult. If access to the mail server is not restricted the user logs in like any other POP account.

If the mail server is not publicly accessible then you need to connect using the VPN client. In our case connecting to the VPN requires additional authentication and is expired periodically to increase security protection. This is not a problem when traveling and connecting for a short time but it gets tedious as a telecommuter. Another option, if it is acceptable to your administrator, is to set up your corporate mail account to automatically forward all incoming mail to a personal mail account. This allows you to access your corporate mail without activating the VPN.

> ***Mail Configuration Tip*** -- Archiving mail when using multiple clients gets pretty difficult. One of the things I've found useful is to have your main computer remove mail from the POP server. The rest of the machines retrieve a copy but do not delete the message. Then when you get back to the main machine you can archive the received mail.

11 Fax – E-mail on Paper

Originally we did not want to use fax, preferring to interact with clients via e-mail or the telephone. We found it is very difficult to get away from fax completely so we sought a solution that did not require a "real" Fax machine.

For incoming fax we use the eFax.com fax service. Basic service is free; if you want a local or 800 number they charge a monthly fee. Each customer is assigned a unique phone number in our case 520-223-4815. When a fax comes in it is converted to a file and e-mailed to the subscriber. On the subscriber's machine special eFax software reads the attachment. The attachment can be saved and imported by other programs.

To send a fax we use Phone Tools that Dell bundles with its PCs. This allows direct faxing of electronic documents or scanned hard copy.

This works well for the limited number of faxes we use.

12 USENET News – Unfiltered Opinion

Most ISPs carry USENET news groups. USENET gives you access to ongoing discussions on a wide verity of topics. There are an incredible number of groups to choose from, our ISP carries more then 44,000 news groups. Most groups have a FAQ that describes what the group is about to limit off topic posts. Each group is interested in a specific topic; members are usually very vocal in discouraging off topic posts. Newsgroups are a valuable source of information. Given the incredible number of users it is likely that someone will be able to provide an answer to your question.

We use Outlook Express as the newsreader.

News server authentication can occur automatically when you connect to the ISP or require explicit authentication. Requiring explicit authentication allows access news regardless of how you connect to the Internet.

13 Audio -- Tunes From Around the World

Using the Internet to deliver audio and video has been hampered by the limited speed available using dialup. Broadband eases this chokepoint opening the door to Internet delivery of radio and TV.

13.1 Real Audio

Real Audio is the most popular format for streaming audio and video. The basic client player is free.

Real Audio implements both a player and compression mechanism. Since most users are still limited to dialup the service is optimized for that. Some programs are encoded multiple data rates so broadband user have access to higher quality programs.

13.2 MP3

The MPEG MP3 compression format provides CD-quality sound at a data rate of 128kbp/s. This represents a ten fold data reduction compared to music CDs. MP3 has become the most popular digital music format. We use the Music Match Jukebox player. This is a MP3 player, and converts CDs to MP3 files.

The new file server has is enough disk space to create an online CD library. We converted all our CDs and some records to MP3 format. This enables any computer with an MP3 player to access the entire library. CD quality audio requires 128Kbp/s, this translates into a megabyte per minute of playing time so large libraries consume 10s of gigabytes. This is large but well within the reach of cheap hard drives.

13.3 WMA

Microsoft developed a different compression format. Windows Media Player is capable of decompressing either MP3 or WMA format.

14 Printing – Information to Paper

Network printing allows any computer on the network to access the printer. Printers can be shared by using a network ready printer, an external print server, or Windows peer-to-peer print sharing.

The printer is a HP 2000 using a HP JetDirect 300X print server. Many different print servers are on the market. The print driver runs on the machine requesting the print job. The output of the driver is sent to the printer over the network. This works much better then peer-to-peer printing used previously. The print server itself is a little box, the sizes of an analog modem. It has a built in web server to manage the print server.

Not all printers can be connected to a print server. Our original printer used the Windows Graphic Device Interface (GDI) that is incompatible with print servers.

> ***Configuration Tip*** -- The LAN is not able to resolve the print server name. The server must be accessed by IP address. This is inconvenient if the address keeps changing. The router's quasi-static address feature comes in handy. Once the router assigns the server an address it frozen. This locks the address to the specific Ethernet MAC address. The MAC address is a unique address assigned by the manufacture to each device.

15 Scanning -- Paper to Information

Flat bed scanners allow documents or photographs to be converted to an image file. These files can be faxed or incorporated into other documents. Text documents can be processed by Optical Character Recognition (OCR) software to convert the graphics images to text that can be understood by text editors. The scanner is an Umax 2200 it uses USB to connect to the computer.

The scanner also functions as a poor mans copying machine. Scanned images can be sent directly to the printer.

16 Local Server – Just Like the Big Kids

The server performs several tasks, file sharing, real time clock synchronization, and private web server. At first we used a laptop as a server. This was convenient because it was self-contained but it had limited disk storage capacity. When the laptop died it was replaced with a recycled 200Mz Pentium desktop with a 45GB hard drive. If storage requirements grow it has room for another disk.

16.1 File Sharing

One of the benefits of having a network is the ease with which files can be transferred between machines. This allows online backup of important files.

File sharing makes bringing up a new computer easier since drivers and applications are all located in one convenient place.

Windows makes connecting to remote drives easy. The user can connect to a remote drive as needed or Windows can automatically connect at boot time. Mapped drives show up as additional drive letters. In a peer-to-peer environment shares can be password protected to limit access.

> ***Security Tip*** -- Some of the most dangerous viruses look for shared drives. If they find a shared drive they can wreak havoc on it not just the machine the virus is on. Password protects any shares that contain valuable data.

16.2 Atomic Time

The Internet allows access to extremely accurate time. This eliminates the problem of drifting and inaccurate computer clocks. We use a program called Tardis 2000. The software runs on the local server and periodically polls a public timeserver. In the US the National Institute Standards and Test (NIST)

maintain a number of public timeservers. Tardis uses this information to set the local server's Real Time Clock (RTC). Tardis includes a Network Time Protocol (NTP) timeserver that periodically broadcasts time info over the LAN. A companion program, K9, runs on each client. It updates the local RTC to match the time on the server. This insures all computers are slaved to the local server and the local server in turn is synchronized to NIST time.

NIST Network Time Service use multiple stratum-1 timeservers located in Boulder Colorado, Gaithersburg, Maryland (Washington, D.C. area) and Redmond Washington. Tardis is configured for each of the addresses. If a server is not accessible Tardis automatically gets time information from the next server in the list.

The timeservers are extremely accurate, however accessing the server via the Internet adds up to several hundred milliseconds of round trip delay. That is not a problem for our purposes.

> ***Configuration Tip*** --Tardis 2000 defaults to time broadcasts on all available interfaces. If Tardis is run on a computer with direct access to the Internet the configuration should be changed to limit broadcasts to the LAN. IP broadcast is a reserved address x.x.x.255, so typical broadcast address may be 192.168.0.255. If this is not done the broadcast is sent out over all ports, including the one connected to the Internet. This may prevent the dialup connection from timing out and will probably annoy your ISP.
>
> ***Configuration Tip*** -- Limit how often Tardis requests time from Internet Time servers. This reduces unnecessary load on the public timeservers. We set Tardis to poll once every 12 hours. For convenience the LAN broadcast occurs every minute so the client clock is updated as soon as the machine boots.

16.3 Private Web Server

The home page of each PC points to the web server running on the local server. This allows relevant information to be posted on the web server and shared with all systems on the LAN. The goal is to use the server to distribute live information, weather data, security status, and etcetera. Currently the server is limited to static pages. Dynamic pages are another item on the to-do list. The server is freeware called Xitami from iMatrix.

HTML pages can be created at a low level using a text editor or with software specifically designed for web creation such as Microsoft FrontPage.

> ***Security Note*** -- If the web server is running on a computer with direct access to the Internet make sure the server is only bound to the LAN interface. Otherwise anyone on the Internet will be able to access your private web pages.

16.4 Local Weather Station

Once of the reasons to run a local web server was to present live data. Davis Instruments has a line of personal weather stations and software that can be use to post weather data to a web server. The weather station is installed but the web software is still a work in progress.

17 So Many Computers So Little Space – KVM to the Rescue

Replacing the laptop server with a desktop PC required another set of user I/O devices. We did not want to use a second set of devices. The solution is to use a KVM (keyboard, video, mouse) switch. KVM's have been used in server farms for years to allow single point of control for multiple servers. We purchased a 4 port Belkin Omni View SE KVM.

This is a 4-port device. Currently port 1 is connected to a desktop and port 2 to the server. The other two ports are for future expansion.

Switching between computers is done via a button on the KVM or with a hot key sequence. When changing computers the KVM reconnects the keyboard, mouse and monitor to the selected computer. The KVM creates virtual devices for each computer. When the user switches to a particular computer the KVM programs the devices so they match the configuration of the virtual device.

> ***Video Performance Tip*** -- Servers normally run video at fairly low resolution and refresh rate. Desktops on the other hand use much higher resolution and faster refresh rate to reduce flicker on large displays. This results in very high video data rates. This is usually not a problem for the KVM itself but requires high quality video cables. The video cable should use coax for each of the three video signals. Use of coax preserves the high frequency component of the signal and minimized cross talk between the three colors. Failure to use high quality cable results in poor video quality.
>
> ***Mouse compatibility Tip*** -- The KVM works by fooling each computer into thinking it is connected to a keyboard, mouse and monitor. The KVM must memorize commands sent to each device and reconfigure the device each time the user selects a different computer. Mice cause problems because so many different enhancements exist. For compatibility PS/2 mice power up in two button mouse mode. This enables mouse functionally even if the correct driver is not installed. At power up the driver performs a knock sequence to determine if it is a mouse it knows. If the mouse answers correctly the driver switches it to an enhanced mode. This causes problems for KVMs. Unless the KVM has a priori knowledge about the mouse it will be unable to configure it properly. Depending on specifics this results in either loss of mouse control or the mouse reverts to default two-button mode.
>
> ***Mouse Workaround tip*** -- Turns out the Belkin KVM does not support my favorite mouse the Logitech Wheel mouse. Switching between systems causes the mouse to revert to default mode, use of the wheel and left thumb button is disabled. To get around this problem the desktop is connected to port 1 on the KVM. The Logitech driver is installed. When the system boots everything is fine. The KVM passes proprietary commands but it does not remember them. The server is connected to port 2 it is running the default Windows mouse driver. Switching to the server resets the mouse to Microsoft mouse mode. Use of the left thumb button is lost but otherwise the mouse functions correctly. Switching back the main system the mouse is once again reset this time as a default IBM PS/2 two-button mouse. The mouse still works but neither the thumbwheel or thumb button is functional. I put the mouse control panel on the tool tray. Forcing the driver to search for new devices resets the mouse back to full functionality. Not very elegant but it solves the problem.

18 Backup – Oops Protection

One of the benefits of switching from a laptop to a desktop file server was much larger hard disk. This enables us to use online backup. Online backup is convenient but it is vulnerable to virus attack. If one of the machines on the network is compromised the virus is able to explore the network for shares. If it finds any it may be able to delete or modify files.

18.1 On Line Backup

The server has shares allocated for each person. Currently it is running with a 45GB drive so that is more then adequate, if we need more space there is room for an additional drive. Online backup provides redundancy for most hardware and software problems. It is unlikely that both copies of the data will be damages by the same failure. Online backup is also fast; access speed is limited by the speed of the network. This makes it convenient to backup massive amount of data.

We are still experimenting with backup software, one of the things we want to do is to backup and synchronize a desktop and laptop. One of the problems of using a laptop is not having the right stuff in the right place at the right time.

> ***Security Tip*** -- Password protect network shares. Some viruses are able to search the network and do damage to shares. This will not protect shares if the machine that accesses then is infected. But it will prevent damage if another computer on the network gets infected.

18.2 Off Line Backup

There is nor substitute for off line backup. If your data consists of a few e-mails and self created documents a few floppies will suffice. To backup more data requires tape or a Zip Disk. Offline backup is the best way to recovery from a virus.

I chose Zip Disk because it functions as either a backup medium or as a large floppy. Zip Drives come in 100Megabyte and 250Megabyte versions. I chose the 100MB because it is the most common. I underestimated the size of backup data. Next time I'll pick a larger backup device.

19 Safe Computing -- Keeping the Bad Guys Out

It is easy to forget that Internet connectivity is a double edge sword, being connected gives one access to the richness if the Internet it also allows attacks from anywhere on the planet. A sad fact of life is that a significant number of talented individuals take delight in wreaking havoc on others.

19.1 Firewall

The first line of defense is to control data entering and leaving the LAN. A firewall imposes a set of rules on data entering the local network. Some, such as ZoneAlarm also control what leaves the network.

Unless you are running some form of public server on your network incoming security is relatively easy, refuse all incoming connection requests. Our business web and mail server are hosted eternally. Access to them is polled. What this means is ALL requests that originate outside the LAN are refused. One of the benefits of using NAT is that it prevents connection attempts from remote computers. Only the IP address of the NAT router is visible to the attacker. If a remote host attempts to connect to public IP address the NAT router prevents the connection because it doesn't know which computer to send the packet to.

The router allows specific IP addresses/ports can be blocked. This can be used to enforce additional restrictions on incoming and outgoing traffic. This is especially useful if you have configured the router to support a public server on the LAN.

19.2 Anti Virus Software

We use Mcafee VirusScan. It verifies files stored on the system and verifies e-mail and downloads. New attacks are constantly being developed, it is important to keep the anti virus program up to date.

19.3 Software Security Patches

Microsoft provides a convenient way to install the latest security patches with Windows Update. As with anti virus software it is important to get the latest updates. Once a vulnerability is discovered information is quickly distributed on the web. The best insurance is the install the latest patches.

19.4 Spyware

Companies find every more clever ways to obtain customer information. This has led to a technique called spyware. Software you install sends information about your usage back to the company. A common method is HTML email. By embedding a remote link the company can determine the time and date you read the mail. More worrisome are programs such as Real Jukebox that reports what songs you played.

A typical firewall is ineffective; it is designed to control remote access, not from within. It is possible to configure the firewall to block access to specific sites. Some personal firewalls, Zone Alarm, being the most popular example monitors both incoming and outgoing traffic. This allows the user to specify what to allow and disallow.

Gibson Research created a spyware removal tool called OptOut. That is no longer supported and has been taken over by Lavasoft Ad-Aware.

19.5 Configuration

To make configuration easier most programs and operating systems use default settings. Check these carefully to make sure they do not compromise system integrity.

Windows Configuration Tips:

- Disable VB scripting
- By default each network interface is bound to all services. Make sure any machine that has direct access to the Internet does not have File and Print Sharing" bound to the interface used to access the Internet
- Change passwords and account names, do not used the defaults.
- Write down user names and passwords and store them in a safe and secure location away from the computer so you have access when you forget them. Don't worry you will forget them.
- Don't run public servers on your LAN, let the hosting service do it
- Don't allow modems in networked machines. They are a backdoor into your LAN

19.6 Social Engineering

Sad to say many security breaches are not the result of compromising the technical security barriers. They result from individuals inadvertently giving out privileged information.

Security Tips

- No reputable entity will ever ask you for your password. If there is a problem with the password you may be issued a new one but they will never never never ask you for yours.
- Limit the amount of personal information you divulge. You need to disclose enough to conduct the transaction that is all. Often times you can operate under an alias such as in chat rooms and forums.
- The web makes it easy to download and install software. You have no way of knowing if it is safe. Just because you are running antivirus software is no guarantee. If this is a new virus or trojan you may be infected before it is antivirus program is updated.
- Don't advertise what you have. The more the attacker knows about your installation the easier it is to find a weakness. All systems have weaknesses.

20 Laptop – Computing Anywhere

We use a laptop in our home office, in the office and while traveling. This means it needs to connect in three different environments.

One of the reasons to convert from proxy based Internet sharing to NAT was to eliminate the need to configure applications for each location. NAT is largely transparent to applications. The next three sections describe the unique configuration required at each location. The forth section describes Netswitcher, the program we use to switch between locations.

20.1 At the Office

The corporate network is an NT domain, running Windows 2000 on most of the systems. A few system like my laptop run Windows 98.

Address Assignment
Mobile computers are assigned dynamic addresses from a DHCP server. All network parameters are assigned automatically.

The Corporate network uses private IP addresses behind a Checkpoint firewall VPN server.

User Authentication
User authentication is by a NT domain server.

File Sharing
Network browsing was difficult to configure. None of the Win98 machines could browse the network. The solution was to create a workgroup of one on the laptop and enable the browse master. Now the laptop can see everything on the network and the laptop shows up in its own workgroup.

Commonly used shares are mapped as desktop shortcuts. The NT domain controller manages share access.

Printing
Print driver is installed for corporate network printers.

Time
Corporate clients determine current time by polling a local time server. Each client runs a daemon that periodically polls the timeserver. This is a different method then used by the SOHO LAN. The daemon is not installed. When on the corporate network the laptop free runs.

K9 is the companion client application to Tardis running on the SOHO LAN. It runs when the laptop is connected to the corporate LAN but does not hear any NTP broadcasts.

E-mail
The Outlook mail client is configured with three accounts, account #1 is the ISP account for forwarded corporate mail, account #2 is the Schmidt Consulting business account, and account #3 is another ISP account. Since the laptop is a secondary mail reader, Outlook is configured to leave incoming mail on the server. This allows the laptop to read mail without removing it from the mail server. When the primary client accesses the mail server the message is removed. This is a little cumbersome if you have not accessed mail from the primarily client for a while but it eliminates having to move mail between machines for archival purposes.

Outgoing mail for all account configured to use the corporate SMTP mail server.

USENET News
The laptop uses the dialup ISP news server. Access from multiple service providers is not a problem because the ISP requires user authentication to access news. This eliminates any restriction on how one connects to the server.

Home Web page
Browser home page set to corporate public home page

20.2 At the Home Office

At home when the laptop is connected to the SOHO LAN it is primarily used to copy files to and from the laptop.

Address Assignment
Address assigned from a DHCP server. All network parameters are assigned automatically.

Same configuration as the corporate LAN.

User Authentication
Windows authentication, Client for Microsoft networks. This provides limited security of network resources if the correct password is not entered.

File Sharing
VPN provides secure remote access to corporate shares. Commonly used shares are mapped as desktop shortcuts. Opening a share automatically activates the VPN client. The VPN client requests a user name and password. Once the user is authenticated the share is accessible. The VPN is only used to connect to shares it is not a tunnel to corporate network. The ISP carries other traffic.

The laptop also has access to shares on the SOHO LAN. They are protected with user level passwords.

Printing
A different print driver is installed for the SOHO network printer.

Time
K9 client is running on all SOHO PCs. K9 is placed in startup folder so it starts automatically. K9 listens for NTP broadcasts to automatically set the client RTC.

E- mail
The three mail accounts are the same as in the office.

Outgoing mail for all account configured to use the SOHO business domain SMTP mail server.

USENET News
News account same as in the office.

Home Web page
Browser home page set to family private home page.

20.3 On the Road

When traveling I use my own dial up ISP. Personal accounts are cheaper then corporate ones. But the main reason is it simplifies networking while on the road. The Dialup ISP is also the hosting service for my domain so it eliminates a lot of special configuration when I'm on the road.

Address Assignment
Dynamic address supplied by dialup networking after successful connection to ISP.

User Authentication
Windows authentication, Client for Microsoft networks. This is a don't care when used with dialup networking.

File Sharing

VPN provides secure remote access to corporate shares. Commonly used shares are mapped as desktop shortcuts. Opening a share automatically activates the VPN client. The client requests a user name and password. Once the user is authenticated the share is opened. The VPN is only used to connect to shares it is not a tunnel to corporate network. The ISP carries other traffic.

Unable to shared files on SOHO LAN.

Printing
Yet another print driver is installed for a locally attached portable printer.

Time
K9 time client started automatically at boot. K9 is inoperative in dialup since it does not receive NTP broadcasts.

E-mail
Three mail accounts are the same as in the office.

Outgoing mail for all account configured to use the SOHO business domain SMTP mail server.

USENET News
News server account same as in the office.

Home Web page
This is a don't care on the road.

20.4 Switching Between Locations

Each location requires somewhat different network configuration. Doing this manually is inconvenient. Luckily a program, NetSwitcher, exists that addresses most of the issues.

NetSwitcher works by modifying settings in the Windows Registry. It can control most network settings can select the default printer.

This left us with the need to change outgoing mail servers on the three mail accounts and the default home page in the browser. A FAQ on the NetSwitcher web page describes how to create extension by using the registry editor, REGEDIT, to extract registry entries and creating scripts that NetSwitcher executes. This has worked extremely well. The only down side is that it is easy to get confused by the hack. If you go in and make a change to Outlook, the change goes into effect and all is well. The next time you change location NetSwitcher overwrites the change. After a little head scratching you remember what you did and all is well, but this is not something to roll out on a large scale.

When Windows shuts down the NetSwitcher dialog box pops up. This allows the correct configuration to be selected for the next boot.

21 Web Hosting -- Your Presence on the Web

Every business needs at least a minimal web presence. The easiest was to set up a web server it to have it hosted. Using a hosting service allows a small business to maintain a 24/7web presence regardless of how the office is connected to the Internet. The hosting service maintains the server and provides high-speed Internet access. This reduces traffic on relatively expensive and slow DSL connection. A single server is capable of hosting many web sites resulting in very low monthly cost. The fee is based on web size and the amount of traffic it generates. We use the same company for both web hosting and dial up access http://www.inr.net.

Using a hosting service means web traffic does not have to be granted access to your network. Internet traffic that originates within the LAN is allowed out but access attempts from the outside in are rejected. This dramatically eases the security task of a small network.

Many ISPs allow customers to set up public web servers. You are assigned a name that looks something like http://www.ISP.net/~yourbiz. This uses the domain name of the ISP as the starting point for your web site.

HTML pages can be created at a low level using a text editor or with software specifically designed for web creation such as Microsoft FrontPage. The pages are created off line on a development server then uploaded to the production site.

22 YourBiz.com – Your Web Name

Instead of having potential customers' access you site indirectly through the name of the hosting service a much better approach is to register your own domain name. Registering a domain name helps to identify your business and prevents changes in ISP or hosting service providers from affecting your customers. Once you have a registered domain name it can be transferred to a different service provider without impacting your public persona. This lets your customers access your site by entering http://www.yourbiz.com.

22.1 Naming Convention

In the DNS section we discussed how domain names map to IP addresses. Names provide a friendly handle to access a particular site. Domain names are hierarchal, the highest level is called the top-level domain (TLD) these are the .COM, .EDU, ORG. .MIL and .GOV of the world. As the Internet expanded each country was assigned a unique domain. For example the TLD for the United Kingdom is .UK. Within each domain various agencies are responsible for name assignment. This has been the source of much controversy in recent years but need not concern us here. The role of the agency is to insure each registered domain name is unique within a top-level domain. For example in our case the "Schmidt" domain was already assigned so we picked tschmidt.com. Sometimes a company adds additional sub domains such as www.tschmidt.com for web access, mail.tschmidt.com for mail or product.tschmidt.com. The hierarchy is evaluated from right to left. The right most name is the TLD.

22.2 Registering Your Domain Name

The first choice is to decide which TLD is most appropriate for your business. You can register the same name in multiple TLDs this is typically done when a company has a valuable trade name.

Hosting companies typically provide automated tools to register and setup a domain. They coordinate with InterNIC or other registration agencies. The registrar database is examined to insure the new name is unique within the TLD. The new name is assigned provisionally in case another registrar has recently allocated it. The ISP updates their DNS name server database to translate the domain name to the IP address of your web server. The web server can be either a physical server collocated at the hosting service or a virtual server provided by the hosting service. Virtual servers allow multiple web sites to be run using a single server. Choice of the optimum method is a business decision that depends traffic volume and the type of site you intent to set up. Obviously an e-commerce site driven by a catalog database with credit card authorization is much more demanding then a simple static web presence.

It takes 24-48 hours for your domain name to propagate throughout the Internet.

22.3 WHOIS record for Tschmidt.com

```
Registrant:
Schmidt Consulting (TSCHMIDT-DOM)
   95 Melendy Road
   Milford, NH 03055
   US

   Domain Name: TSCHMIDT.COM

   Administrative Contact:
      Administrative Services  (AS935-ORG)  admin@TSCHMIDT.COM
      (603) 673-5804
   Technical Contact, Zone Contact:
      Network Operations Center  (NO153-ORG)  noc@INR.NET
      603. 880.8120
      Fax- 603.880.8783
   Billing Contact:
      Administrative Services  (AS935-ORG)  admin@TSCHMIDT.COM
      (603) 673-5804

   Record last updated on 04-Nov-1998.
   Record created on 04-Nov-1998.
   Database last updated on 5-Jan-2000 13:08:31 EST.

   Domain servers in listed order:

   NS1.INR.NET                198.77.208.2
   NS2.INR.NET                216.64.64.2
```

This is an example of a hosted web site. Administrative and Billing contacts refer to the company registering the name. The Technical Contact is the hosting service that own responsibility for translating host names to IP addresses. Notice there are two name servers, InterNIC requires a primary and alternate name server. The IP address for your site is allocated from the pool of addresses previously assigned to your service provider.

22.4 Creating Your Web Site

When the registration process is complete you need to create the web site itself. Sites range from simple ones that provide static information to complex database driven e-commerce. A word processor can be used to create a simple site. For more complex site specialized tools such as Microsoft FrontPage can be used to good advantage. Numerous companies specialize in web site design if you decide to out source this task.

22.5 Site Logs

The hosting service typically provides logs of everyone that visited the site and what pages they looked at. This data can be analyzed to understand how customers navigate your site.

22.6 E-mail

An advantage of having your own domain name is that email is addressed to your domain not your ISP. This personalizes your web presence. Normally the hosting service provides one or more e-mail accounts. E-mail is structured as username@domain.TLD. The hosting service can sort incoming mail by user name if you need multiple mail accounts. You can also run your own mail server to create multiple accounts. Regardless of how many accounts you create one account is an alias. This is where anything not sorted to another account is sent. I did not realize how useful that is until I started creating unique username every time a site asks me to register. That way it is easy to determine who sold your email address when you start getting SPAM.

23 Conclusions

Setting up a SOHO network and VPN has been extremely successful and a rewarding experience. The LAN meets our business and personal networking needs. It is a pleasure to have high speed Internet access.

The down side is that a significant amount of technical expertise is required. The building blocks are all readily available but the detailed knowledge to create and troubleshoot can be hard to come by. If you hunt a little the resources are out there. Every year more small networks are created and the manufactures get better at making equipment that is easy to use. In general failures are minor and easy to fix, if one knows the root cause. It is determining the cause that is difficult. Help is available, manufacturer sponsored forums and specialized news and interest groups can often provide insight and help in your specific problem.

Networking today is like to having an early horseless carriage (or a British sports car), when it worked it is exhilarating, but one needed a riding mechanic to keep it running. As networking expands beyond the province of corporate IT departments it will become easier to use until a non-networked device is unthinkable.

Start now and become a pioneer.

Happy networking.

Last Page
Intentionally Blank