Living with a SOHO Network
2002 edition

Tom Schmidt
Schmidt Consulting
Revised 1/14/2002
tom@tschmidt.com
http://www.tschmidt.com

Abstract
This paper discusses our experience setting up a small office home office (SOHO) network. It offers guidance on selecting an Internet Service Provider (ISP), presents Local Area Network (LAN) options, describes Internet sharing methods, and discusses implementation of multiple LAN based services.

DSL provides a high-speed always on Internet connection. A broadband router connects the LAN to the Internet with automatic fallback to dialup in the event DSL fails. The LAN is 10/100 BaseT Ethernet. Network services include file and print sharing, time service, and a local web server. IPsec Virtual Private Network (VPN) software provides secure remote access to corporate network. This allows access to corporate resources while telecommuting.

Major changes this year were transition from SDSL to ADSL and implementing automatic file backup.

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.

The LAN has undergone significant evolution over time. It started out with a few 10 BaseT Ethernet drops. It has expanded to encompass the entire house and home office and been upgraded to 100 BaseT. DSL is the primary Internet connection dialup being reserved for backup. Initially we used Wingate for Internet sharing and BlackIce Defender for intrusion detection running a dedicated laptop. The laptop has been replaced with a Multitech Broadband Router. A recycled desktop now serves as a poor mans server. This runs the timeserver, local web server, and file shares. Network printing is done with a dedicated HP print server. Desktop PCs normally require a dedicated monitor, keyboard, and mouse. Instead we opted to use a Belkin KVM (Keyboard Video Mouse) switchbox. This allows a single keyboard, mouse and monitor to be shared by multiple computers.

A Virtual Private Network (VPN) enables telecommuting between home and corporate network. The VPN encrypts data between the home and the corporate network providing a secure channel over the public Internet. As is typical with all things networking installation and debug was accomplished with some difficulty. However, once properly implemented the VPN has operated flawlessly.

Traveling with a PC laptop presents problems, as network configuration differs at each location. Luckily a utility called NetSwitcher simplifies this task providing one click switching between locations.

File backup was finally addressed. We chose Second Copy 2000. It is configured to automatically backup several client profiles to the file server.

This paper is not intended as a competitive product review. The field is constantly changing; any attempt to do so is quickly 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 SOHO network:

- Share single Internet DSL connection
- Automatic fail over to Dialup if DSL fails
- Printer and scanner sharing
- File sharing
- Local private web server
- VPN access to corporate network
- Access to multiple e-mail accounts
- Access to USENET newsgroups
- Fax without a fax machine
- Automatic time synchronization
- Automatic file backups
- Learn networking

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

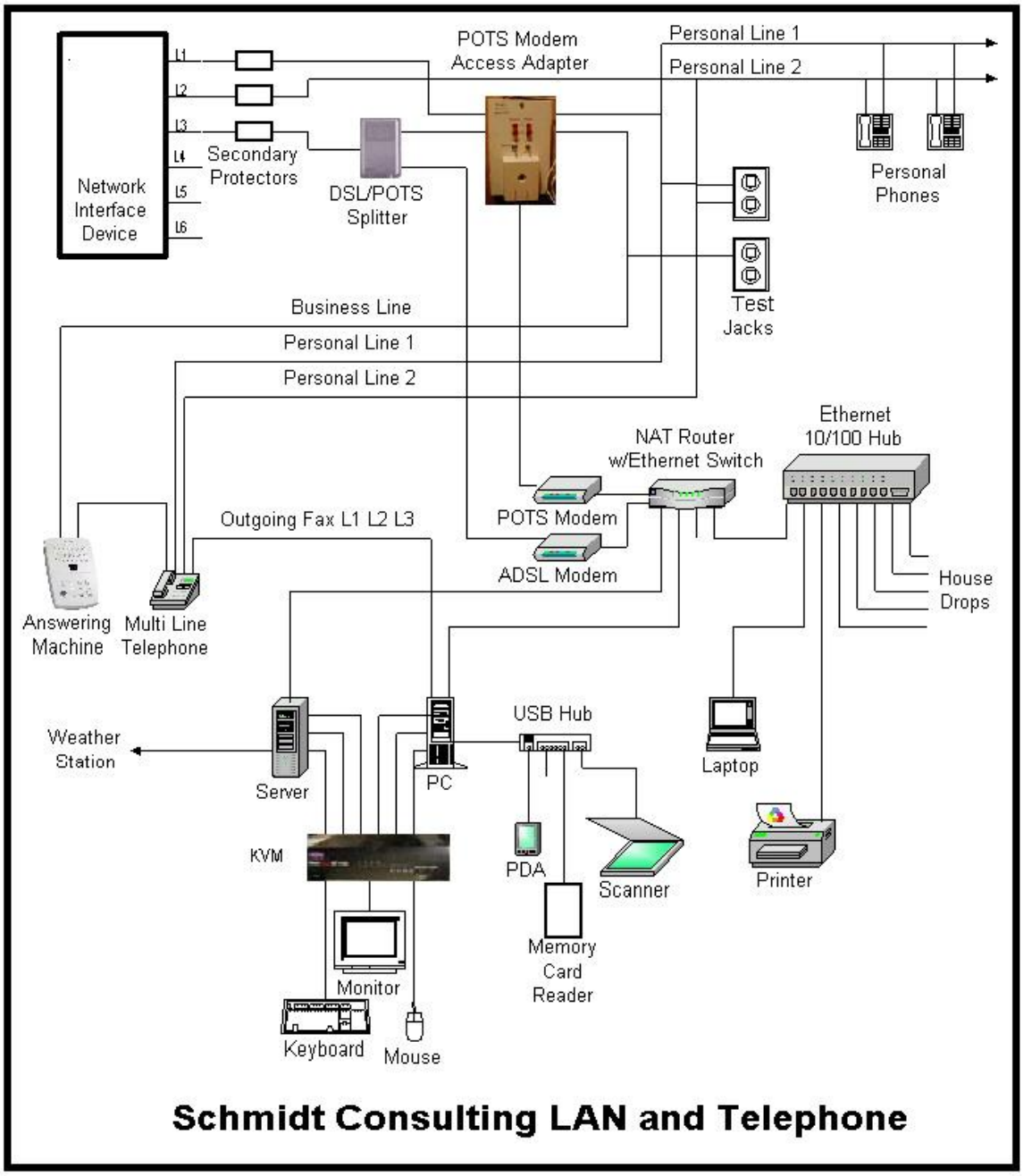


Figure 1 SOHO data and voice block diagram

2 Types of Internet Access – Your Friendly ISP

The PC has progressed from hobbyist plaything to an indispensable telecommunication device. Almost all PCs are purchased with the intent to connect to the Internet. The most common access methods 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 using the Cable TV distribution facilities. In each case the ISP is the link between the end user and the Internet backbone.

Typical ISP services:

- Connection between the end user and ISP network – so called first mile
- Routing between customer and one or more Internet interexchange carrier
- User authentication
- IP address assignment
- 1st level DNS name resolution – translate host name to IP address
- E-mail account
- USENET account
- Web hosting
- Billing
- Technical Support

2.1 Dialup

Dialup access is available to anyone with telephone service. Modems are normally used with wired phone service but can also be used with wireless cellular phones. However the data rate is significantly lower over cellular and cellular service typically change for connection time so it is not optimal for fixed location use.

Almost all ISPs support the ITU V.90 modem standard. The International Telecommunications Union V.90 standard replaced previous generation of proprietary 56Flex and X2 modems. V.90 takes advantage that the ISP modem pool is directly connected to phone company digital trunk. This means only one analog to digital conversion exists between the user and the ISP. The ISP modem is synchronized to the digital trunk. This enables it to transmit at up to 56kbps toward the user. 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 V.92 a minor enhancement to V.90. It increased upload speed slightly to 44Kbps and implements faster auto negotiation to reduce connection setup time. The standard also includes V.44 improved data compression. V.92 includes a mechanism to ignore call-waiting tones to allow the user to answer a second call without dropping the modem connection. V.92 modems are available but ISP's have not been rushing to upgrade.

At connect time the modem probes the line to determine noise and attenuation levels. This sets the initial connect speed, during the session the modem 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. The most common protocol between the end user and ISP is the Point-to-Point Protocol (PPP) defined by the IETF, the same folks that write the Internet specifications. This allows the Internet protocol to be carried over the serial telephone link between the user and ISP.

Phone lines are digitized at the Telco central office at 64kbps. This means analog modem has reached its theoretical maximum speed. To obtain higher speed requires use of different technology.

2.2 DSL

Digital Subscriber Line (DSL) technology utilizes the existing telephone copper wiring between the subscriber and the phone company central office (CO) to carry high-speed data. This allows the local exchange carrier to generate additional revenue by leveraging the massive investment in cabling. Modems

at the user and CO side use frequencies above those used for voice telephony to deliver high-speed data. Several types of DSL have been developed hence the xDSL moniker. The most common types are Asymmetric DSL (ADSL) and Symmetric DSL (SDSL). Another benefit of DSL to the Telcos is that it gets long duration data calls off the Public Switched Telephone Network (PSTN). This minimizes the need to upgrade the expensive circuit switched phone system.

ADSL offers a higher download speed, toward the subscriber, then upload. It has the advantage that it coexists with Plain Old Telephone Service (POTS). 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 analog POTS line and high-speed data service. Filters split the signals at the CO and inside the residence low frequencies are delivered to the telephone; high frequencies to the DSL modem.

SDSL is typically marketed as a business service. It requires a separate dedicated copper pair; it does not coexist with POTS. Being symmetric makes it suitable for use with servers. SDSL is also typically offered with a static IP address. A static address allows external hosts to more easily connect to servers. A special case of SDSL is IDSL it offers symmetric speed of 144Kbp/s over longer distances then either ADSL or SDSL. IDSL uses ISDN signaling allowing it to be used at distances >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 consumer ADSL is available at 768/128, 1500/128 and 1500/384 plans. Speed decreases with distance. Subscribers far from the CO are not able to sign up for maximum speed. At the CO or remote terminal (RT) the Digital Subscriber Line Access Multiplexer (DSLAM) combines data from multiple customers into a single high-speed connection. Traffic from multiple DSLAMs is combined together, along with traffic from other COs on the ISP's internal network. From there interexchange carriers, that provide the Internet backbone, carry it.

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. 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.

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.

2.2.1 Impairments

DSL is an impressive engineering accomplishment that enables broadband data to be carried on 100-year-old copper telephone circuits. Not all phone lines are suitable for DSL. Assuming your local central office is equipped for DSL you may not be able to obtain it for a number of reasons. This section discusses common problem and where applicable workarounds.

2.2.1.1 Distance

DSL signals decrease as they travel down the wire. Typical practice limits DSL to between 15,000 – 18,000 feet from the CO or remote DSLAM. This is actual cable distance. The route the phone line takes may not

be the shortest distance between the CO and subscriber. Some ILECs are installing remote Terminals (RT) to reduce cable distance allowing them to serve more customers.

2.2.1.2 Digital Loop Carrier

DLC is a technique that allows the phone company to use a single circuit to deliver more then one phone line. This reduces the cost of delivering telephone service. Unfortunately it is incompatible with DSL.

If your phone is on DLC you will not be able to get DSL. Depending on the type of DLC it may also limit analog modem speed to 33kbps or less. Newer versions of DLC called Remote Terminals eliminate the limitation allowing more customers to obtain DSL.

2.2.1.3 Load Coils

As phone signals travel down the wire they become attenuated due to resistance and impedance effects. This is more pronounced at high frequencies then low. The phone company extends the range of phone circuits by placing loading coils periodically along the line. This cancels out some of the harmful effects and result in a stronger voice signal over long circuits.

Unfortunately load coils are incompatible with DSL. Load coils are effective over the range used by human voice at the expense of higher frequencies. This did not matter as long as the circuit was used solely for voice but it severely attenuates DSL. The only solution is to have them removed. SDSL providers normally pay the ILEC to do this as part of the circuit install. If you line is loaded you will not qualify for ADSL.

2.2.1.4 Bridge Taps

When telephone cable is installed the phone company does not know exactly how many circuits will be needed at every location. The solution is to run a large cable down the road. As customers order phone service the installer selects an unused pair in the cable and splices the local drop. This means the circuit feeding your phone may continue past your house for hundreds or thousands of feet. This is called a bridge tap. It is of no consequence for telephone service. DSL is designed to tolerate some amount of bridge tap, but if your circuit is marginal it may cause problems or push you line over the distance limit. SDSL providers normally pay the local Telco to remove bridge taps when the circuit is installed. This tends to be expensive and is not done for low cost residential ADSL.

2.2.1.5 Noise and Crosstalk

The cable that carries your phone circuit also carries many other phone lines. These may be ordinary POTS service, ISDN or T1. Imperfections cause some unintentional coupling from one circuit to another. This raises the noise floor on the connection. If it gets excessive your speed is reduced or you see lots of retransmissions to recover from data errors.

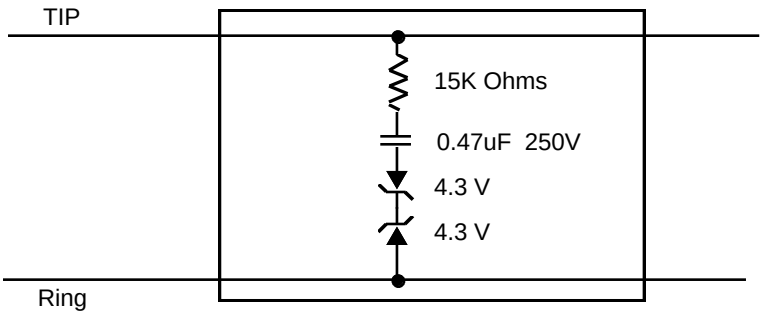
If you can hear noise on your phone you are much more likely to get the Telco to fix the problem. If it only affects DSL it will be hard getting them to fix it, since in general consumer grade DSL is not warranted for minimum speed. It is simply a best effort on the part of the Telco.

2.2.1.6 Half Ringer

Excerpted from ADSL Forum Technical Report 013.

> It has been standard practice in many areas of the United States to install, at the Network Interface Device (NID), a network termination device that is called a half ringer. It is an example of an AC type termination device since it is detected using AC techniques.
>
> A normal POTS mechanical ringer, in a residential telephone, is made up of an inductor and a capacitor in series that is bridged

between Tip and Ring of the line in the phone. The 'half' ringer is just the capacitor part of the ringer. The half ringer is actually a capacitor in series with a zener diode and a resistor that resembles one half of a 'normal' mechanical ringer. This, in the U.S., is a 0.47 micro Farad capacitor without the addition of the inductor part of the circuit, hence the name 'half' ringer.



Half-ringers represent a load to DSL if you are at maximum distance the additional load may interfere with DSL. Common practice for SDSL installation is to disable the half ringer in the NID. If the phone company installs a POTS/DSL splitter for ADSL the half-ringer is built into the splitter after the POTS filter so the effect is minimized.

This is only a concern if your signal is marginal. If you think the half-ringer is interfering with DSL try to get the Telco to install a POTS/DSL splitter rather then use the self-install microfilters. When the splitter is installed the half-ringer in the NID is disabled.

2.2.1.7 Inside Wiring

Inside wiring is the cause of many DSL problems. The FCC recently mandated telephone inside wiring be installed using the homerun method with at least Cat3 twisted pair cable. This means in new construction each phone outlet is run directly to a central wiring closet, usually in close proximity to the NID. The cable itself is of higher quality then the 4-conductor IW (inside wire) historically used for phone wiring. Each pair is twisted to minimize noise pickup.

DSL was designed to tolerate poor inside wiring. The easiest way to test inside wiring is to connect the DSL modem directly to the NID. The test jack on the NID automatically disconnects inside wiring. If your speed improves inside wiring is interfering with DSL. The simplest way to isolate the effect of bad inside wiring is to use a POTS/DSL splitter instead of multiple microfilters.

2.2.1.8 Wireless Phones

Wireless phones may interfere with DSL. The frequencies used by the phones do not overlap however they inject a substantial amount of noise into the phone line.

If you are experiencing problems disconnect all the phones and reconnect one at a time. Sometimes adding additional microfilters at the offending phone will solve the problem.

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 all cable subscribers. Cable bandwidth is divided into channels. Each channel carries one TV station. Internet service is very different. Instead of a one-way connection from the headend to many subscribers each PC needs a point-to-point connection so it can both send and receive. As is the case with DSL the CATV

vendors must install much new equipment. One or more 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 TV signal with ones capable of carrying signals in both directions. At the CATV office these signals are converted from the cable format and routed to the backbone data network. The cable network that feeds the subscriber must be divided into small groups to minimize the number of customers sharing cable bandwidth.

Some early cable Internet systems were unidirectional. The cable was used for downstream data and a conventional modem for upstream. This allowed the CATV vendor to offer high-speed data while it upgraded the network for bi-directional data.

The CATV industry is working to standardize the interface so cable modems can be purchased in retail stores like dialup modems. The industry is rapidly migrating to the DOCSIS Data-Over-Cable Interface Specification created by CableLabs. Like DSL DOCSIS is an always-on connection, it is not necessary to "dial" into the Internet. Typical CATV data rates are 700-10,000kbps down (toward the customer) with sub megabit rate up.

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 and we are not a subscriber.

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 service that do not require access to expensive right of way is being deployed on a trial basis. Satellite service is competing with wired service in some areas. The distance to and from geosynchronous orbit adds 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 over a single infrastructure. In new developments 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 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 limited period called a lease. When the lease is about to expire it is automatically renewed. DHCP makes it much easier to manage the IP address pool then manually assign static addresses. From the customers point of view it is an always-on service, lease renewal is transparent to the user.

Some broadband carriers 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. In typical usage once the customer is authenticated they are issued a dynamic IP address. This has to be renewed periodically like DHCP. When the connection has been idle for a predetermined time the user is disconnected. This allows more customers to be serviced from a given pool of IP addresses. PPP is an encapsulation protocol, as such it add 8 bytes of overhead to every packet. Internet Packets can be up to 1500 bytes long so in most cases this is not significant.

3 Dialup Account – The Old Standby

Even though we have DSL we chose to maintain a dialup account. It is used as a backup incase DSL fails and while traveling. Having two different ISP accounts is also a very useful troubleshooting tool.

In our experience the most common cause of DSL failure is internal problems within the ISP not with the DSL circuit itself. To maximize the chance of dialup working in the event of DSL failure our dialup ISP is completely separate from our DSL supplier.

Our requirements were:

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

3.1 Selecting a Provider

Initially we used 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 provides our web hosting service INR.Net as our ISP. They are a local ISP that met our requirements. They have been extremely responsive to e-mail and phone support issues.

3.2 Acceptable Use Policy

ISPs have a 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 prohibit using a LAN it is unreasonable to expect technical help from them in setting it up.

Most ISP's reserve the right to revise the policy at any time making for a pretty one-sided contract.

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, some 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 that information is potentially marketable depending on the privacy policy.

3.4 Thoughts about Dial Up

Consider your ISP mail account a throwaway. Free e-mail or a registered domain name is 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. When this occurs you email address changes making it difficult for people to stay in touch.

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 Account – Telco's Enter the Brave New World of Data

We had been looking for broadband service for several years for both personal and business purposes. Cable service was not available in or town, Satellite has too much latency and charge extra for home network. DSL was the only broadband service that met our needs.

DSL wish list:

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

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 own security.

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 we estimated our distance between 9,500 and 14,700 feet.

4.2 Selecting a Provider

Our first attempt was Verizon. Our central office is equipped for Verizon DSL but we did not qualify. No reason was given. When I plugged in phone numbers closer to the CO they qualified so I assume the reason was excessive distance.

Next we tried to sign up with HarvardNet. 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 10.5K feet from the CO. As others have found out DSL prequalification distance estimates are all over the place. The only way to get an accurate measurement is to actually have the service 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 standard business SDSL 528kbp/s business service with a relaxed service level agreement (SLA). SDSL requires a dedicated line. Vitts coordinated the installation of a new line with Verizon. The service was installed and worked flawlessly until Vitts declared bankruptcy and shutdown in May 2001 leaving us without high-speed access. Once again we were forced to use dialup. Several other DSL providers service our area but deteriorating financial conditions made the future look bleak.

Through DSL Reports I learned of Verizon presidential appeals, +1 888.216.1443. Did not hold out much chance of ever getting DSL but called anyway. Less then four hours later all three phone lines were qualified and ranked. I held off ordering for a while. At that time Verizon DSL had a pretty bad reputation and they were changing acceptable use policy to restrict sending email. But I was getting desperate for high-speed connectivity. Used DSL Reports to check local Verizon customers, got pretty good feedback about the overall quality of service.

Ordered Verizon 1500/384 DSL in July 2001 with an activation date of early August. ADSL is different then SDSL because it coexists with existing phone service. This reduces cost but requires a method of separating DSL from phone signals. Verizon sends out a self-install kit that consists of special account activation software, DSL modem and microfilters.

4.3 POTS/DSL Splitter vs Microfilters

ADSL requires a filter to isolate DSL from phone voice signals. To reduce cost consumer grade DSL service typically use Microfilters. This allows the customer to self-install DSL eliminating the expense of a truck roll to dispatch a technician. Microfilters must be installed on every non-DSL device.

Figure 2 DSL Microfilter

An alternative to the microfilter is a single whole house POTS/DSL splitter. This allows a single device to serve the entire house. Splitters are especially valuable if you have a large number of telephone devices or you are far from the telephone central office. The splitter has better filter characteristics and being installed at the NID does a very good job isolating inside telephone wiring from DSL. A good way to see if a splitter will improve DSL performance is to connect the DSL modem directly to the Telco NID. This disconnects inside wiring. If performance improves use a splitter.

Figure 3 POTS/DSL Splitter

The splitter includes half-ringer test circuit on the phone side of the splitter. This allows the half-ringer in the NID to be disconnected, further reducing unnecessary loads on DSL.

A single microfilter can be used to supply the entire house but a purpose built POTS/DSP splitter has better filtering capabilities.

Advantage of Splitter

- Single device for entire house
- Better electrical characteristics
- Isolates inside wiring from DSL
- Isolates half-ringer test circuit from DSL
- Works with Alarm installation

Disadvantage of Splitter

- Installation required
- Dedicated run from splitter to DSL modem
- Have to purchase separately

4.4 Installation

The Verizon self-install kit included a Westell "white" modem and install CD. The type of modem varies depending on your location.

Prior to the activation date Verizon technicians connect your phone line to the DSLAM at the central office and create a user account. Verizon uses PPPoE for log on. This is very similar the way PPP used with dialup modems. PPPoE requires login to establish a connection.

Figure 4 Westell ADSL Ethernet modem

When everything is up and running in the central office Verizon sends out a welcome email. At that point the modem can be connected to the phone line. The Westell modem has four indicators, power, ready, link, and activity. The power light is on when the unit is powered up. Ready is on after the modem completes is internal self-test. Link is on when the modem is synchronized to the DSLAM in the CO. The activity indicator flashes as data moves over the Ethernet connection between the modem and the user's equipment. The link indicator indicates the modem is synchronized to the DSLAM; it does not indicate a connection to the Internet exists. This is a source of some confusion.

Once the connection is activated you need to run the Verizon install CD, even if you intend to use a router. Verizon requires use of MS PPTP VPN and a customized Netscape browser for initial configuration and WinPoet for PPPoE, to simulate a dialup connection. I did not intend to use WinPoet as I have a router. I loaded the Verizon install CD on a spare PC. Install was pretty uneventful. The only annoyance is Netscape runs in a small window, that cannot be expanded and the Verizon stuff has to be scrolled horizontally and vertically. When activation is complete a screen with all your account info is displayed, this cannot be copied or printed directly from the browser. Once the connection was up and running I transferred the PPPoE setting to my Multitech RF500S router. It logged on without a hitch.

Verizon ADSL has been very reliable with only a few short outages. None of the outages have been problems with the phone line itself; I've never lost the link light. The problems have been Verizon routing errors or DNS failures. Overall I'm pleased with the Verizon service. My only complaint is the ever-changing acceptable use policy. Since I signed up Verizon added restrictions on outgoing mail and has banned use of servers.

4.5 Optimization

There are many urban myths about magical tweaks you can make to improve performance. In general most of them are nonsense. One thing that makes optimization difficult is that measurements are hard to duplicate since so many things can change between tests.

The only useful tweaks I've found is to adjust the TCP receive window and in some cases to force a specific maximum packet size. A TCP connection requires the receiver to periodically let the sender know that everything is OK. This is called the receive window. If the transmitter has not received an acknowledgement after it has sent a number of packets it stops transmitting and waits. At fast connection speed, and if the connection adds latency the receive window (RWIN) needs to be increased to prevent pauses in transmission.

The other useful tweak affects the maximum chunk of data that can be transmitted; this is called the maximum transmission unit (MTU). In an Ethernet network the maximum packet size is 1500 bytes. Normally this setting is fine. However PPPoE encapsulation adds 8 bytes to each packet. This reduces the maximum packet size to 1492 bytes. If the source attempts to send larger packet it will either be rejected or fragmented into two parts, with attendant degradation in performance.

A good way to optimize your setting is to go the DSLR Tools page and run the tweak test. Once you know the optimum settings download the DrTCP utility to make the changes.

4.6 Acceptable Use Policy

ISPs have a 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 prohibit using a LAN it is unreasonable to expect technical help from them in setting it up. Some services place monthly quotas on maximum download or upload. Make sure you fit in any restrictions.

Most ISP's reserve the right to revise the policy at any time making for a pretty one-sided contract.

4.7 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, some 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 that information is potentially marketable depending on the privacy policy.

4.8 Service Level Agreement

Business class DSL includes a service level agreement (SLA). This defines minimum speed, maximum latency, and time to repair if 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 business. One needs to carefully consider the impact of communication failure.

4.9 Thoughts about DSL

Successfully delivering DSL service has turned out to be more difficult then expected. The decline in stock market valuation makes it much harder to obtain financing. This has caused severe problems for many companies. In our case our first and second choice for DSL supplier no longer exist. It is unlikely Verizon will go under but it means almost no competition exists in the local DSL market. As a result we had to scale back our DSL wish list.

DSL as delivered:

- Symmetric speed at least 500kbp/s (1500/384)
- No prohibition against using a LAN (OK)
- Reasonable price (Half the price of Vitts SDSL service)
- Single static IP address (Dynamic address via PPPoE))
- Service Level Agreement (Not offered – best effort only)
- True always on service (No – PPPoE emulates dialup)
- No content filtering (Port 80 and SMTP filters, new prohibition on any kind of server)
- Does not require special software (Install only. PPPoE is not proprietary)
- Good technical support (Nonexistent)

5 Wiring Techniques – The Nuts & Bolts

Many of the advances in termination technology were developed by the Telephone industry to deal with the massive number of circuits they install and manage. Of particular note for our purposes are Modular jacks and type 66 and 110 punch down blocks.

Modular jacks were developed by the old Bell System to reduce the cost of installing and maintaining customer equipment. Until the mid 1970s phone cords were hardwired. This required a craftsperson to come on site for even the simplest of jobs. The deployment of modular jacks meant that in many cases the customer could repair and move their own equipment. The six-position version of the modular jack is used to connect single and two line phones to facility wiring. A smaller four-position version is used at both ends of the handset cable. TIA568 adopted the 8-position modular connector for use with structured network wiring.

The jacks are commonly called RJxx for registered jack. This stems from the pre divesture days when each use of the jack had to be documented in the telephone tariff.

About the same time as modular jacks became popular Type 66 punch down termination was introduced. It is called punch down because the wire is terminated with a spring-loaded tool that pushes it between insulation displacement contacts and automatically cuts the wire to length. The type 66 block is still widely used in phone systems. LAN wiring adopted second generation, type 110, termination. This allows more circuits to be terminated in a given area. Due to smaller size the 110 contact provides better high frequency performance.

A significant portion of overall phone system or LAN cost is in the cabling. Until EIA/TIA568 each equipment vendor created unique cabling and connector requirements. The TIA recognized cable infrastructure has a long life expectancy, typically being used with multiple generations of electronic equipment. They developed a performance based wiring scheme independent of the specific equipment used. This was a breakthrough, all new telephone premise and LAN wiring is based on the standards developed by TIA568. A companion document EIA570 addresses unique aspects of residential wiring.

When the telephone network was deregulated the FCC took over responsibility for setting customer equipment and inside wiring standards, commonly called Customer Premise Equipment. Phone company practice for the last 100 years has been to wire phone jacks as a daisy chain. Wire originates at the NID and runs to the first outlet, from there to the next, and so on. As customers began using more sophisticated services the limitation of this method became apparent. The FCC recently mandated telephone inside wiring be installed using homerun method with at least EIA568 Cat3 twisted pair cable. Homerun wiring requires each outlet have a separate cable that runs all the way back to a central wiring closet. This provides a great deal of flexibility for change and reconfiguration.

A useful wiring guide is the “Technician’s Handbook -- Communications Cabling” by James Abruzzino ISBN 0-9671630-0-5. A free online guide is available from Levitron.

Wiring supplies can be purchase at electrical supply houses or on line from Mike Sandman.

5.1 Structured Wiring

The key to the EIA 568 standard is the notion of structured wiring. Cable from each data or phone outlet is run back to a central wiring closet. The wire cannot be spliced or connected to other outlets. At the wiring closet each cable is terminated at a patch panel. To configure a specific service a short cable, called a patch cable is connected between the appropriate patch panel jack and the device that services that outlet.

EIA/TIA 568 created different performance grades. Category 3, also called Cat3 is rated for 10Mbp/s. This is the minimum acceptable standard for telephone and digital networks. Cat5e is required for 100Mbp/s networks, and is the minimum recommended for new LANs. Cat5e allows the LAN to operate at up to 1000BaseT Ethernet. This allows a single wiring scheme to support Ethernet (10Mbp/s), Fast Ethernet

(100Mbp/s), and Gigabit Ethernet (1000Mbp/s). When Gigabit Ethernet was being developed it was designed to operate over the installed base of Cat5. However, real world experience showed that not all installations were up to the task, hence the revision to Cat5e.

Figure 5 Cat 5 Jack

Cat5e is the sweet spot for any new LAN installation. Cat6 and Cat7 extend the frequency range even higher, but at additional cost. At some point copper wiring runs out of steam and must be replaced with fiber optic cabling.

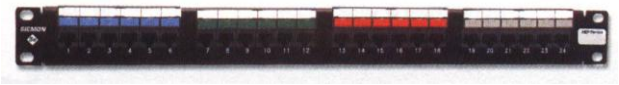


Figure 6 Cat 5 Patch Panel

Unshielded Twisted Pair (UTP) Category 3 and Category 5e cabling is designed for a maximum end-to-end distance of 100meters. This includes a patch cord from the computer to the wall jack, 90 meters of wiring (in TIA parlance called horizontal wiring), and another patch cord in the wiring closet to connect facility cabling to the hub or switch. Receptacles use type 110 terminations. This allows the cable to be quickly terminated with a punch down tool. In the wiring closet it is common practice to connect multiple cables to a patch panel. A patch panel consists of multiple jacks to facilitate terminating a large number of cables. From the patch panel a short patch cable is used to connect each run to an Ethernet hub or switch.

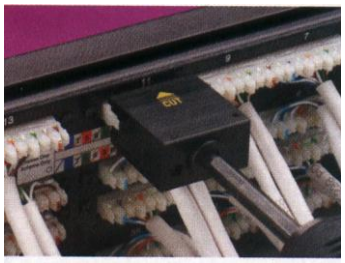


Figure 7 Rear view

Terminating horizontal wiring to a patch panel makes for a very flexible installation. This is ideal when used with a large number of outlets that are constantly being rearranged. I chose to reduce cost by terminating each building cable directly with a Cat5 plug. Plugs are somewhat more difficult to install then receptacles so it is not for the faint of heart. By doing so I eliminated the cost and space of the patch panel and patch cable. Each building cable is directly connected to the central Ethernet hub.

The various category grades are very similar. The differences are the number of twists per inch of the cable. Each pair of wires in the cable has a different number of twists per inch. The higher the Category number the tighter the mechanical tolerances necessary to operate at the higher frequency. It is important not to mix Category grades, doing so reduces the rating to the lowest grade used.

5.2 UTP Unshielded Twisted Pair

Use of unshielded twisted pair wiring reduces the cost of network infrastructure compared to older technology that utilized coax cable. Standard cable consists of 8 separate conductors with each pair twisted together. To make identification easy the performance grade is printed on the cable jacket. Building wiring uses solid wire cable. Patch cables use stranded cable to provide long flex life. Be sure plugs and receptacles are compatible with the type of cable.

5.3 Patch Cables

Patch cables connect computer to wall jack, and the patch panel to a hub or switch. Patch cables are available in different length and colors. The T569A or T568B pin out option can be ignored since the vendor terminates both ends, the choice of pair color does not matter.

Patch cables come in two versions, straight through and cross over. Straight through cables are used in almost all circumstances. 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 cross over cable. Crossover cable swaps transmit and receive pair at one end so like devices can be directly connected.

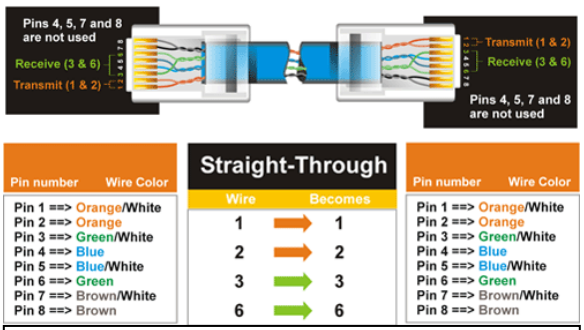


Figure 9 Straight-through Patch Cable

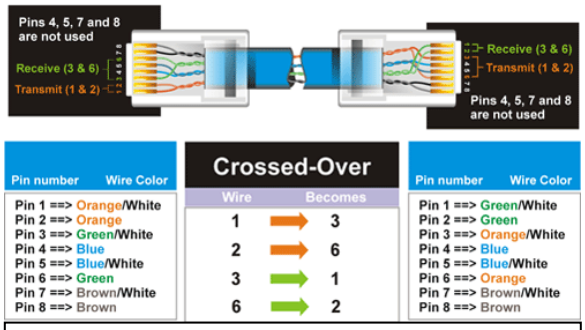


Figure 8 Cross-over Patch Cable

5.4 TIA 568A and 568B Pin out

A cause of much confusion when implementing structured wiring is the fact that two different connector pin outs were defined T568A and T568B. They are nearly identical except pairs 2 and 3 are swapped. Electrically this is of no consequence as long as both ends use the same pin out. TIA 570 Residential wiring standard requires use of the T568A pin out.

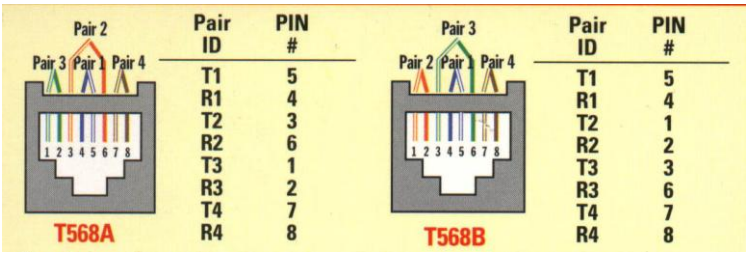


Figure 10 UTP alternate pin outs

5.5 Uniform Service Ordering Code (USOC) Pin out

The RJ11 and RJ14 connectors are the two most common jacks used for residential phone systems. RJ11 (Registered Jack 11) is a 6 position modular connector terminating a single pair. RJ14 is also a 6-position connector but it terminates two pairs, allowing a single jack to support two phone lines. RJ14 is by far the most common configuration in new construction

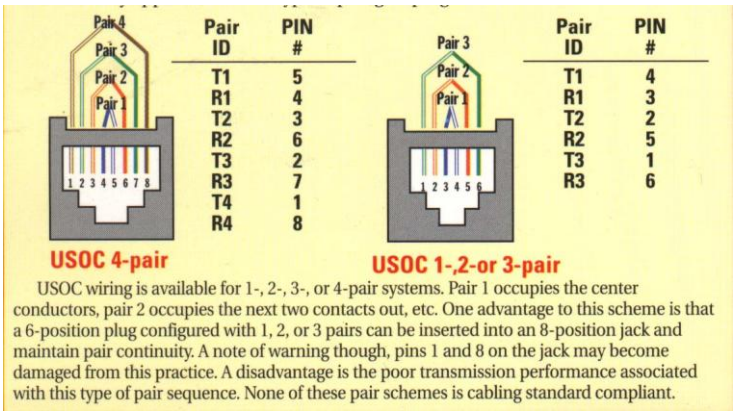


Figure 11 Telephone RJxx Jacks

A third common telephone jack is RJ31X used with alarm circuits. This is an 8-position connector. The jack is placed in series with one phone line close to the NID so extension phones are downstream of the jack. When the alarm system is plugged in the jack opens the phone circuit. This places the alarm in series with the phones. When the alarm is activated it disconnects the phones so it is able to dial out even if the line was in use.

5.6 Type 66 Terminals

The first type of insulation displacement terminal developed by the telecom industry was the Type 66 block. These continue to be extensively used. Types 66 blocks accept large number of accessories. For telephone wiring one advantage of the 66 family is that it accepts larger gauge wire then the 110 system.

Type 66 blocks are typically clipped to a standoff bracket that is screwed to the wall. The bracket allows cables to be run underneath the blocks.

Building wiring is terminated on one set of terminal blocks and equipment on a different set. To interconnect equipment to the specific jack single pair cross connect wire is used. This allows a great deal of flexibility in adding and changing equipment over time.

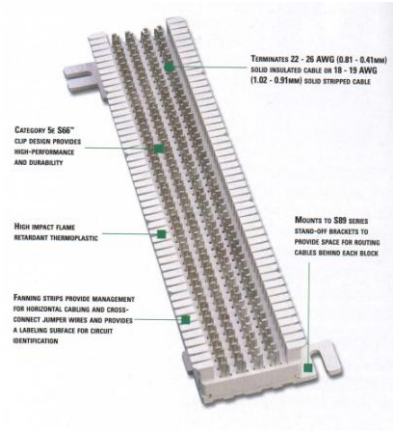


Figure 12 Type 66 terminal block

5.6.1 Type 66 Accessories

The Type 66 family includes a number of accessories and options.

- **Standoff:** Type 66 block clips to standoff. This allows building wire to be routed through the standoff under the block.
- **Bridging clips:** Blocks normally consist of 25 terminal pairs vertically and 4 terminals across. A common variant is the split block. This divides each horizontal row in half doubling the number of circuits. A bridging clip connects all four horizontal terminals. Bridging clips make troubling shooting easier since simply removing the clip opens the circuit.
- **Test clips:** come in several flavors that facilitate connecting test equipment to the block
- **Cover:** Protects the 66 block terminations from foreign objects.
- **Mushrooms:** Cross-connect wire can become unsightly if not managed properly. Mushrooms screw to the wall to create wire routing channels.
- **Line use Indicator:** LED indicator that show when a phone line is in use.

5.7 Type 110 Terminals

Type 110 terminals allow wiring to be packed more densely then Type 66. The smaller terminal causes less disruption to high frequency signals, making 110 termination the preferred connection for LAN use. A typical 110 module includes a standoff. Building wiring is routed in these channels. It is brought out from the standoff and punched down to a terminal. Then another 110 block is inserted over the base. Cross-connect wire is punched down to the upper block.

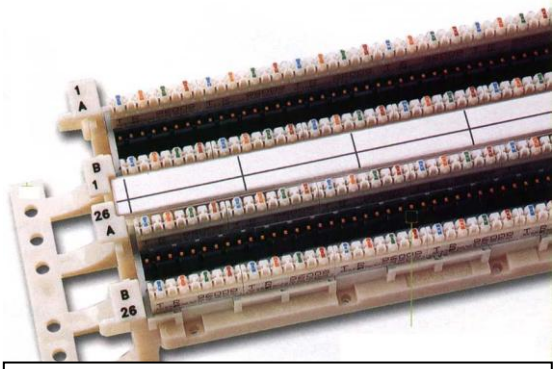


Figure 13 Type 110 Punchdown block

The same insulation displacement terminal used on Type 110 blocks is also use on receptacles designed for Cat3 and Cat5e. LAN wiring is not cross connected as in telephone practice. When a LAN is installed the cable from each receptacle is connected to patch panel consisting of a large number of modular jacks. Patch cable, terminated with modular plugs, is used to interconnect the patch panel to LAN electronics.

5.8 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
Jacket 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 modular Plug
Fish tape	Used to snake wire through walls
Circuit Tester	Indicates polarity and loop current of phone circuit
LAN Tester	Verifies correct wiring of Cat3 and Cat5e LAN

Figure 16 Jacket stripper

Figure 15 66/110 Punchdown

Figure 14 RJ11/45 Crimper

Cabling should be tested after installation; simple testers are in the $100 US range making them expensive for do-it-yourself installation. An ohmmeter will verify end-to-end continuity uncovering many common wiring errors however it will not find split-pairs. Wiring is paired to reduce noise susceptibility; signals traveling on one wire are almost exactly balanced out by signals of opposite polarity on the other wire in the pair. If the pairs are incorrectly terminated this cancellation does not occur. Testers verify each pair is properly terminated; the cable is not crushed or excessively untwisted. These types of installation errors may work with 10Mbps Ethernet but will break Fast and Gigabit Ethernet.

6 Telephone – Connection to the World

We have three phone lines. Two lines are for family use and the third reserved for business. ADSL is installed on the business line.

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. Residential service reps may not be familiar with setting up a Hunt group 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 feature 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.

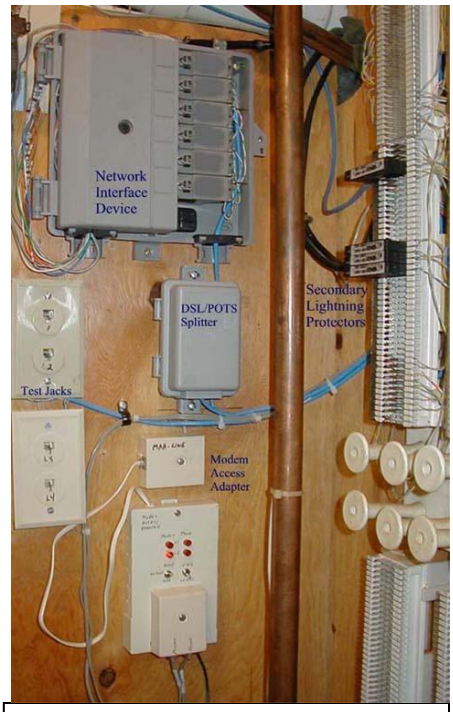


Figure 17 Telephone wiring closet

We wanted both lines to return Caller ID 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 may call it directly, defeating the purpose of the hunt group. We opted to enable Caller ID and remind family and friends to use the main number.

The third line is reserved for business use. 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 the call on busy or no answer to a cell phone.

We did not want to dedicate a line solely for dialup modem use, as this seemed overly restrictive. However sharing one line for both modem and phone poses a mutual interference problem. Picking up a phone dumps the modem. On the other hand computer has no way to know the phone is already in use, causing it to attempt to dial even if the phone is in use. I looked for an off the shelf solution to this problem but could not find one. So the Modem Access Adapter (MAA) was designed. This eliminated the need for a dedicated modem line and provides optimum use of the phone lines.

> ***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 hold the connection when it detects call-waiting tones. This allows the new call to be answered without dropping the Internet connection.

6.1 Network Interface Device

Back in the bad old days when the phone company rented you a phone and did 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 to demarcate between the customer and Phone Company responsibility. Everything outside the demarcation point is the responsibility of the Telco; anything inside is the customer's.

Figure 18 Telco NID

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 inside wiring and a test connector to quickly disconnect inside wiring from the Telco. Some NIDs include half-ringer test circuit. The half-ringer creates a unique test signature to allow test equipment to determine if faults exist on the Telco or customer side of the demarcation point.

The picture at right shows a typical multiline NID. Telephone company wiring terminates under the protective cover on the left. The Telco side contains protection circuits that divert lightning surges to earth 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.

6.2 Secondary Lightning Protection

The phone company provides lighting protection as part of the Network Interface Device. Electronic devices are more fragile then electromechanical phones; 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 location for lightning protection is the building entry point. That allows all equipment to be bonded to the same low impedance ground connection minimizing voltage difference between different conductors. Lightning protectors do not absorb energy they divert it somewhere else. If the diversion path is not low impedance a substantial voltage difference is created. This is what kills electronic gear.

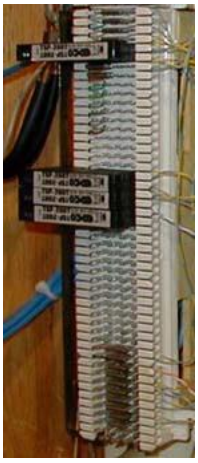


Figure 19 Lightning Protection

The EDCO TSP-200 series protectors add very little capacitance to the line. This is critical so the protectors do not interfere with the high frequencies used by DSL. The protector clips to a 66 style split block. The Surge protector acts like a bridging clip between the left side (Telco) and right side (Phone). With the protector removed inside wiring is completely isolated from the external conductors. A grounding bar runs down the left side of the block. This is connected to a high quality earth ground, the same used by the NID and the power service entrance. When the protector fires damaging voltage is shunted to ground.

One protector should be used on each telephone line. Additional protectors should be used on any lines that connect to outbuildings.

6.3 POTS/DSL Splitter

Rather then using the microfilters at each non DSL device I installed a POTS/DSL splitter.

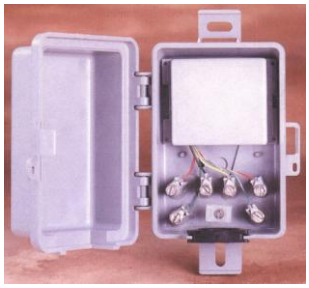


Figure 20 Splitter

When the business line exits the secondary lightning protector it runs to a Siecor (now Corning) POTS/DSL splitter. The splitter includes a low pass filter that isolates the voice phone line from the high frequency DSL signals. The splitter has two outputs; DSL is connected directly to the DSL modem the phone output connects to inside phone wiring.

The splitter contains a half-ringer test circuit connected to thee phone side of the splitter. The half-ringer in the splitter allows the one in the NID to be removed.

6.4 Modem Access Adapter

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

Figure 21 Modem Access Adapters

When the modem initiates a call the adapter detects the off hook condition and searches for an idle line. If it finds an idle line it disconnects the phones before connecting the modem. As long as the modem is in use the phones are disconnected preventing them from interfering with the modem. 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 adapter features. The left hand switch enables or disables the device. It also controls whether or not to search both lines. The right hand switch 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.

6.5 Putting it all together

The drawing below shows the overall connection of phone and DSL wiring. Two phone lines are used for personal use and one for business. The NID, secondary lightning protection, POTS/DSL splitter, Modem Access Adapter, and Type 66 punch down blocks are all located in the wiring closet.

From the NID each line goes to a secondary lightning protector. The POTS/DSL splitter is connected to the business line. The DSL output is run directly to the DSL modem. The voice output of the splitter and line 1 feed the Modem Access Adapter. Another dedicated line connects the analog POTS modem to the MAA. To make changes easier all building wiring is terminated to punch down blocks. A short wire, called cross-connect wire, is used to interconnect the various phones. This makes it easy to rearrange wiring by adding and removing cross-connects without affecting building wiring. Test jacks for each line allow a test phone to be conveniently plugged in during troubleshooting.

An old wall phone is mounted in the wiring closet, with a RJ11 cord. This allows the test phone to be plugged into the test jacks on the CPE wiring side or directly into the NID. Having the phone permanently mounted in the wiring closet insures it is available when needed.

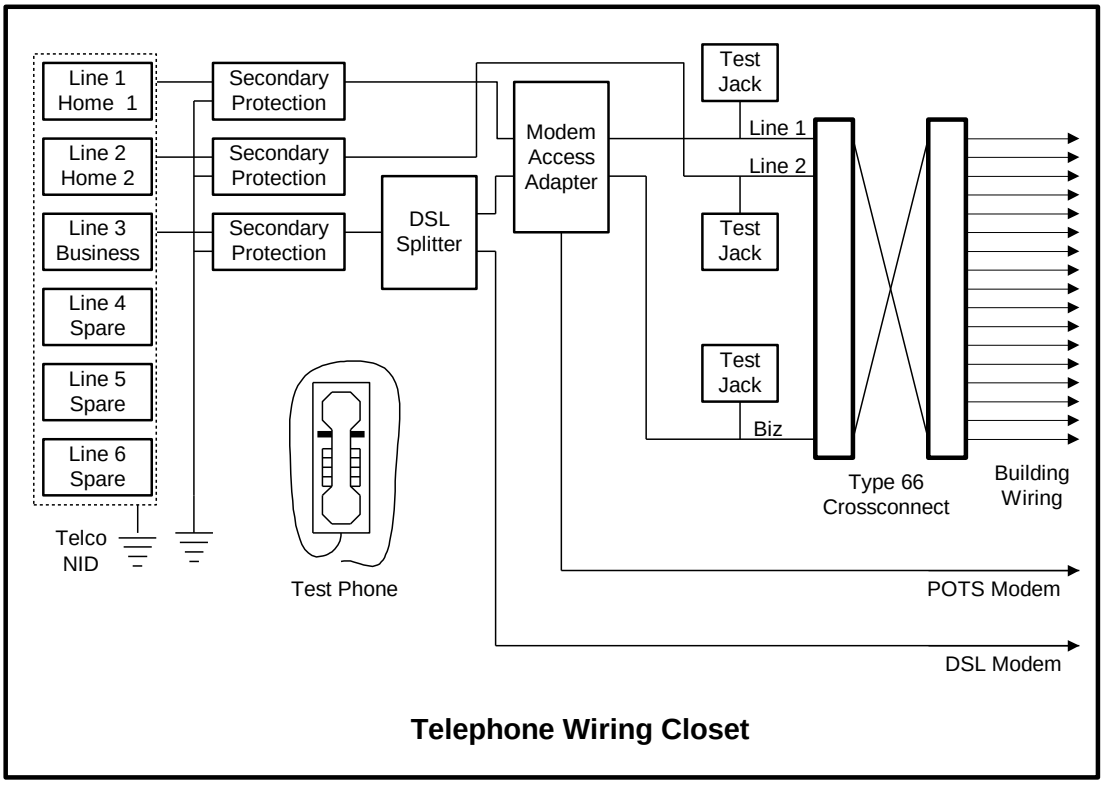


Figure 22 Telephone wiring

7 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 are wired with two network outlets. Cable from each receptacle is run to a central wiring closet. In the wiring closet a 16-port hub connects everything together. Ethernet over Cat 5 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

7.1 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. That 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 constraints 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 wiring is unshielded twisted pair (UTP) copper cable consisting of 4 pairs of wire terminated with 8 conductor jacks similar to those used for telephone wiring. This has dramatically reduced the cost of implementing a LAN.

7.1.1 Media Access Controller (MAC) Address

Each Ethernet interface has a unique address called the MAC address. This allows each interface to be uniquely addressed. This is not the same as the IP address that will be discussed later.

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.

7.1.2 10Mbps - 100Mbps - 1Gbps - 10Gbps

Initially UTP Ethernet operated at 10 million bits per second (10Mbp/s). Fast Ethernet increased speed to 100 million bits per second over Category 5 wiring 100Mbp/s). Gigabit Ethernet is 10 times faster then Fast Ethernet (1,000Mbp/s). During Gigabit Ethernet development the Cat5 specification was tightened resulting in Cat5e. Work is in progress to increase Ethernet speed by another factor of 10 to 10 Gigabits per second.

7.1.3 Ethernet Hubs and Switches

UTP Ethernet is a point-to-point topology electrically even though logically it is a party line. Each Ethernet interface must be directly connected to another Ethernet Interface. Hubs regenerate Ethernet signals and allow 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 or daisy chained. CDMA/CA scheme used by Ethernet places a limit on the number of wire segments and how many hubs can be used. 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 Ethernet networks 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. A switch allows multiple conversations to occur simultaneously as opposed to being limited to only one with a hub. This allows total switch bandwidth to be greater then 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 capacity of 800Mbp/s. This assumes 8 pairs of connections evenly divided between the 16 ports; each one operating at full 100Mbps. A switch has another advantage it eliminates collisions allowing 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 100Mbp/s switch to 1.6Gbp/s as compared to 100Mbp/s for a hub. In actual use the advantage will not be as great but switches offer tremendous performance advantage

The switch selects the proper port based on MAC address. Every Ethernet controller has a MAC address. The switch reads 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.

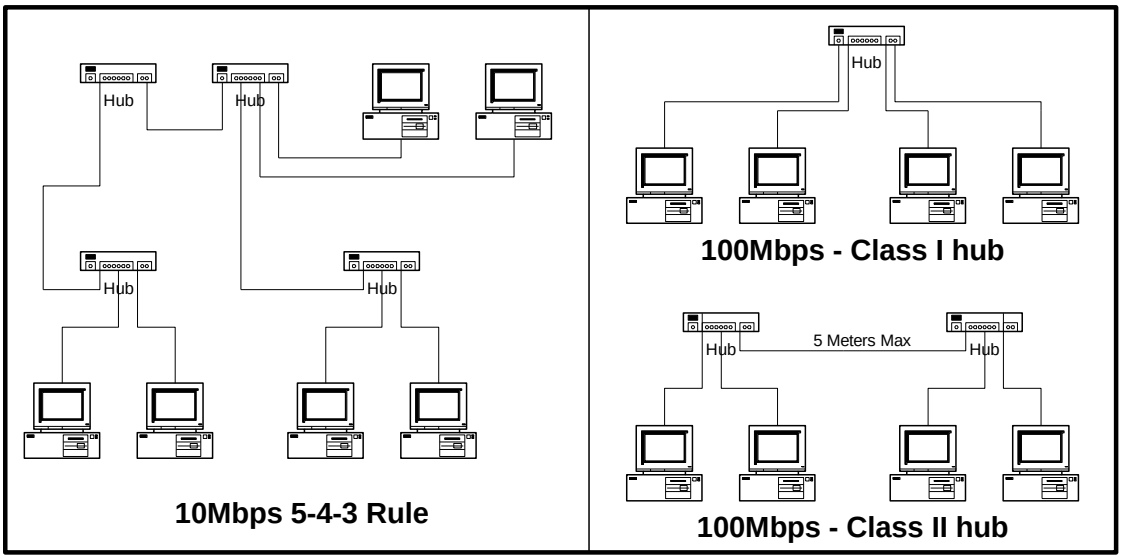


Figure 23 Hub rules for Ethernet and Fast Ethernet

Ethernet Tip – Use 10/100 autosensing hub or switch. 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.

7.1.4 Managed vs Unmanaged Hubs and Switches

Ethernet hubs and switches come in both managed or unmanaged versions. Managed devices allow the administrator to control various parameters and observe traffic. These features are valuable in a corporate network but are overkill in a home network. Unmanaged devices are considerable less expensive.

7.1.5 Preferred Topology

For maximum flexibility a switch should be used in the wiring closet. This maximizes total network bandwidth. Using a central switch allows hubs to be used in each room if additional Ethernet drops are needed. Switches used to be very expensive, but recently switch prices have been dramatically reduced, making a switch the preferred choice.

7.2 Alternatives to Wired Ethernet

Wired Ethernet is the dominant commercial LAN. It is also popular in new home construction. The cost of installing network wiring is low if done when the house is being built. The situation is more difficult for existing homes. The cost and disruption of installing new wiring discourage folks from installing a home network. Various "no new wire" initiatives attempt to minimize impediments to home networking. These initiatives operate at lower speed then Wired Ethernet but have the advantage on not requiring dedicated wiring.

7.2.1 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 increased speed to 10Mbps. The specification allows analog telephone, DSL, and LAN to coexist on a single pair of ordinary 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 software.

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 physically connected to the same LAN.

7.2.2 RF Wireless

Great strides have been made in creating high performance low cost radio LANs. 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.

IEEE 802.11 The original version of the spec supported 2Mbp/s, 802.11b runs at 11Mbp/s in the 2.4Ghz ISM band. 802.11a delivers 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. Depending on the type of building a single site may need more then one Access Point.

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 (PAN) 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. BlueTooth devices form a piconet to communicate amount a small group of devices. Piconets in turn can form scatternets to cover a longer distance. Deployment of BlueTooth has been delayed due to technical issues. The first devices are just now reaching the market.

7.2.2.1 Wireless Security

Radio based communication is relatively easy to eavesdrop. This threat was recognized so wirelesses 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. Security researchers have discovered significant shortcomings to Wireless Equivalent Protocols (WEP) used in 802.11 and similar to that used in BlueTooth. This weakness makes it relatively easy to break wireless encryption if significant traffic exists. The IEEE recently created a revised version of WEP that improves security.

7.3 TCP/IP

The LAN uses the Internet Protocol (IP) to connect local devices. Using the same communication protocol for both LAN and Internet simplifies configuration and management. 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 such as PING. PING verifies a remote host is reachable and how long it takes.

7.4 IP Address

Each IP device (host) must have an address. Addresses can be assigned, statically, automatically by DHCP (Dynamic Host Control Protocol) or automatically by the client itself, AutoIP. Traditionally the system administrator manually configured each device with a static 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. AutoIP 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. Due to the scarcity of IPv4 addresses ISPs change extra for multiple addresses. Several techniques have been developed to minimize the consumption of addresses.
IPv6 also promises to minimize the size of routing tables each router must maintain. While IPv6 holds much promise it entails a complete overhaul of the Internet. Such change is always resisted until one has no choice to go through the pain of conversion.

7.4.1 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.

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

7.4.3 Port Number

A single computer may connect to multiple hosts. How does the computer know how to interpret 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 TCP or UDP 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.

7.4.4 Private Addresses

The Internet Assigned Number Authority allocates Internet addresses. This is the entity that assigned the addresses used by your ISP. RFC 1918 allocated three blocks of private addresses that are not used on the Internet. The private addresses are ideal for use on a LAN. Devices on the LAN are assigned an address from the pool of private addresses. This eliminates the need for coordination and the expense of obtaining addresses from the ISP. 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 pseudostatic addresses so the address never changes. An option in the router forces the router to always issue the same address based on its Ethernet MAC address.

7.4.5 AutoIP

The addressing techniques discussed so far require manual entry of an address or that a DHCP server exist on the network. In most situations this works well. But what happens in a simple environment when one just wants to connect a couple of PC and not implement any network infrastructure. AutoIP was developed to solve this problem. If the host is configured to obtain a dynamic address and a DHCP server cannot be found the host assigns an address to itself from another pool of reserved addresses.

When this happens the machines picks a random address from the AutoIP address pool, and tests to see if any device on the LAN is already using it, if not it assigns itself the address. If the address is in use it picks another one and tries again.

AutoIP address block:

169.254.0.0 - 169.254.255.255 (169.254/16 prefix)

Refer to IPv4 Link Local spec for more information about AutoIP.

7.4.6 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.

7.4.7 Address Resolution Protocol (ARP)

IP addresses represent the global numbering scheme of the Internet. The addressing scheme used by the physical network is different. For example Ethernet uses a 48-bit MAC address. ARP provides the mechanism to determine the IP address if the MAC address is known and vice versa.

7.5 Gateway

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

When a host is unable to connect directly to another host it forwards the packet to the router. The router determines how best to deliver the packet. It may deliver it directly to the recipient or have to forward it to another router. Routers exchange route messages among themselves to determine the best route. Each router segment is called a hop.

One of the parameters each host needs to know is the address of its local router, also called a Gateway. When a DHCP server is used it sets this address automatically. In our network the Gateway address is the broadband router.

The name Internet is a contraction of Inter-network. The Internet is a network of networks.

7.6 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 Uniform Resource Locator (URL) into your web browser, such as http://www.yahoo.com, the browser first checks to see if this is a name of a local device on the LAN. If it is not local the name resolution request is forwarded to a DNS name server. Your ISP provides the first name server in the chain. If it doesn't know the address the request is passed to other DNS servers until the targets IP address is found. Once the system obtains the IP address it uses the address to connect to the remote host. DNS names are 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.

7.6.1 Naming Convention

URL 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 two letter top level domain. For example the TLD for the United Kingdom is UK. Within each domain various agencies are responsible for name registration. 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.com" 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 for product info. The name hierarchy is evaluated from right to left starting with the TLD.

7.7 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.

7.8 Network Neighborhood – My Network Places

Windows network neighborhood allows one to browse local computers. To show up in the neighborhood each machine must be running the Microsoft file and print sharing service, 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 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 – 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 permanently on force it to win Brows Master election. This guarantees the Network Neighborhood is always available. On the always on PC go to File and Print sharing in Network control panel open Advanced tab, highlight Browse Master and change the Value to Enabled. Set Browse Master to disable on the other PCs.

Windows Configuration Tip – a computer must have 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 laptop 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. The laptop was put in a workgroup of one and the Browse Master for forced on.

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.

Windows Configuration Tip – If you are running a person firewall be sure it does not block the NetBIOS ports used to discover local host names and share files.

From IANA.ORG registered Port numbers:

```
netbios-ns      137/tcp    NETBIOS Name Service
netbios-ns      137/udp    NETBIOS Name Service
netbios-dgm     138/tcp    NETBIOS Datagram Service
netbios-dgm     138/udp    NETBIOS Datagram Service
netbios-ssn     139/tcp    NETBIOS Session Service
netbios-ssn     139/udp    NETBIOS Session Service
```

7.9 Implementation

The LAN wired with Category 5 cable connected to a SMC 16-port 10/100BaseT hub. If this were a new installation I'd opt for a switch rather then a hub. Most rooms are wired with two Ethernet drops.

Except for one laptop all Ethernet adapters operate at 100Mbp/s. The cost difference between 10 and 100Mbp/s Ethernet is negligible making 100Mbp/s devices the preferred choice. The 10/100 autosensing hub automatically rates matches between 10 and 100Mbp/s 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 grow over time.

Rather then terminating building cables at a patch panel they were directly terminated with CAT5 plugs. Terminating plugs is somewhat harder then receptacles but it eliminated the need and cost of a patch panel and patch cables. Building wire is plugged directly into the central hub.

PCs run Microsoft Windows 98SE or Millennium operating system. The only communication protocol used is TCP/IP. Using the same protocol for local access and Internet simplifies configuration. Most machines are assigned a dynamic IP address. This minimizes problems adding and removing computers from the network. Servers need static address so the can be referenced by IP address. The router has a provision to bind the IP address to Ethernet MAC address. This is convenient because the router always assigns the same address even though the device is configured for dynamic addressing.

One PC is dedicated for use as a server. It runs file sharing, web server, and a timeserver. It has Browse Master enabled so it is always the Network Neighborhood Browse Master. This insures Network Neighborhood is always visible. A dedicated print server is used for network printing.

8 Broadband Router – One Address So Many Computers

This section describes how to connect a LAN to a single Internet account.

Figure 24 Broadband Router

When the LAN was first set up we used Wingate proxy software running on a laptop. This allowed multiple computers to share a single dialup ISP account. At the time Wingate was the only connection sharing software that included a DHCP server. This was a convenient cost effective solution. However over time shortcomings of this approach became apparent.

Software Proxy Limitations:

- Each application must be configured to use the proxy. This makes moving a laptop between LANs difficult. We wanted to replace the Proxy with NAT. Wingate had a NAT version of the software but we had trouble getting an early version to work with our hardware.
- Streaming services such as Windows Media Player and Real Audio player do not work well behind a proxy.
- Even though connection sharing software does a good job protecting PCs on the LAN the machine connected to the Internet is still vulnerable. If that machine is compromised the attacker has access to everything on the LAN. To protect the directly connected PC I ran a software firewall. This tended to be fragile. Often installing the latest Microsoft patch broke the firewall.
- When one factors in the total cost for the software solution, second NIC card, sharing software and firewall very little difference exists between software and hardware solutions.

Our router requirements:

- Ethernet port for DSL
- RS232 Serial port for dialup modem
- Automatic fallback to analog modem if broadband fails
- NAT 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
- Port mapping to run servers
- Good tech support

The router we chose was a MultiTech RF500S. It meets our requirements and technical support from Multitech has been outstanding.

8.1 WAN Interface

DSL service providers offer three types of modems, External with an Ethernet port, External with USB port and Internal PCI. There are pros and cons to each. An external Ethernet modem is the most flexible because it can be connected directly to a computer or used with a router to create a LAN. We used an external DSL modem for both Vitts and Verizon DSL.

The customer interface of the Verizon Westell ADSL modem is 10baseT Ethernet. This connects directly to the Wide Area Network (WAN) port of the router. Verizon uses PPPoE encapsulation. This requires the user to log in, much the same as with a dialup account. The router implements PPPoE eliminating the need to run special software on the PCs. With PPPoE the WAN IP address, Gateway address and DNS address are configured automatically each time the router logs in.

If the DSL connection is idle for a while Verizon will automatically disconnect. The router maintains a keep alive that prevents the connection from being dropped. This simulates a true always on connection. The router uses the keep alive to verify the Internet is accessible. If the connection is lost the router automatically attempts to reconnect. If the connection is down for more then a three minutes and one of the devices on the LAN is requesting Internet access the router activates the back POTS dialup modem. The router continuously attempts to reestablish the DSL connection. When that occurs it disconnects the POTS modem and routes traffic though the high-speed connection. Except for momentary outages and difference in speed this is invisible to the user.

8.2 Automatic Fail over

When a client on the LAN requests Internet access the router verifies the DSL connection is working. This is the preferred Internet connection. If DSL is down the router automatically uses the analog modem to connect to the dialup ISP. The router includes an idle timer to disconnect the analog modem after a period of inactivity. This prevents the modem from tying up the dialup connection unnecessarily. The router continuously attempts to reestablish the broadband connection. When DSL service is restored dialup is automatically terminated.

This feature turned out to be very useful. The router was set up before we had DSL. This allowed us to test and debug the dialup configuration prior to getting DSL After our first DSL provider went out of business we were forced to use dialup full time. When the Verizon account was activated we simply plugged in the Westell modem and entered our PPPoE account information into the router. Once again we were up and running on DSL.

Setting up the dialup account is similar to Windows dialup networking; it requires POP phone number, user name, and password. With PPP the WAN IP address, Gateway address and DNS address are configured automatically each time the router logs in. These setting are different depending on if the connection is dialup or DSL. The router hides the difference from network clients.

Both Vitts and Verizon service has been reliable. We have never lost DSLAM sync. All outages have been either DNS or ISP internal routing problems. The few outages that occur last a few minutes to at most several hours. That fact that problems have been with the service provider's internal network operation validates our choice to obtain backup dialup from a different vendor.

8.2.1 Using multiple ISPs

The fallback feature is great but it adds some complexity in setting up the network. Each provider issues a different IP address and uses different DNS and gateway servers. The router hides these differences from the local machines. As far as they are concerned the router is the gateway and DNS sever.

Another problem concerns sending email. This is not an issue if you use web-based email. If you use a POP/SMTP mail client connecting through different ISPs may prevent you from sending mail. As the Internet has become more popular some of the assumption made in the initial design have come up short. Mass mailers have exploited the lack of SMTP security to inundate users with unsolicited email called SPAM. The SMTP mail server cheerfully accepts all outgoing mail sent to it and delivers it to everyone on the address list. Spammers love this, all they need is an open SMTP mail server and they are in business. As a counter measure most ISP's reject mail unless it is sent from within their network. This restricts outgoing mail to users that are currently logged in giving the ISP some control over Spam. This is not a problem if one has a single email account provided by the ISP. However if you use multiple email accounts sending mail independent of the connection can be a problem. See section **11.4 SMTP SPAM mitigation** for more details.

Our hosting service uses SMTP authentication. Neither Verizon DSL nor our dialup ISP block SMTP port 25 this allows us to send mail securely regardless of how we connect.

Usenet may also be a problem of the ISP auto authenticates. In that case you will not be able to access news when you use an alternative ISP.

8.3 LAN Address Assignment

Each device on the network requires an IP address. The LAN uses reserved private addresses. These addresses are not used on the Internet therefore they do not need to be coordinated with other Internet users. However they still must be coordinated within your own network since local addresses cannot overlap. The Multitech router has the flexibility to use dynamic, pseudo static, or static addresses.

8.3.1 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 it is able to use the LAN. The DHCP server assigns several other critical numbers, subnet mask gateway address and DNS 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 packets that cannot be delivered locally are sent. In our case the gateway is the Multitech router. The router decides how to deliver the packet. Since only a single connection exists between our network and the ISP routing is trivial. The router simply forwards all packets to the gateway address assigned by the ISP. Local host name resolution is done within Windows. If Windows cannot resolve a host name it forwards the request to the router. The router in turn forwards the request to the DNS address specified by the ISP.

8.3.2 Pseudo Static

For some devices, such as servers, dynamic addresses are a problem. For example the binding to the print server is by its IP address, it does not have a name. That means if the address changes each client has to be reconfigured. A solution is to create a pseudo static address. The address is issued by the DHCP server but bound to the client's Ethernet MAC address. This is more convenient then setting IP addresses manually and making sure they do not conflict with previously assigned addresses or the DHCP pool.

This is especially useful for network appliances that do not include user interface.

8.3.3 Static

It is also possible to manually assign the IP address. The Multitech DHCP server is configured to issue addresses from the 192.168.2.2-100 range with an subnet mask set to 255.255.255.0 Since all the addresses must be in the same subnet static addresses can be assigned in the range of 192.168.2.101-254 without interfering with DHCP while still residing in the same subnet.

8.4 NAT -- Sharing a Single Internet Connection

The LAN cannot simply be "plugged in" to the Internet. The IP addresses used on the LAN are forbidden on the Internet and the ISP only provides a single IP address. 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.

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 and port number 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.

NAT offers many of the advantages of using a proxy with the benefit that it is transparent to most applications. For more information see RFC1631 The IP Network Address Translator (NAT).

8.4.1 Limitations of NAT

As useful as NAT is it is also controversial. It breaks the end-to-end addressing 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 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 office network both using private address the addresses 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 if both corporate networks use the same address block.

By design NAT blocks all remotely originated traffic. It functions as a de facto firewall because NAT does not know how to route traffic that originates outside the LAN. This is often touted as a major security benefit but it causes problems if one wants to run a server. Single IP NAT makes it impossible to run multiple servers that use the same well-known port. NAT routers provide a mechanism to map local servers to the public IP address. However since only a single external IP address exists, incoming requests can at most be mapped to a single physical device using the well-known port. For example the router can be configured to map all TCP port 80 requests to a server. As far as the remote user is concerned they are accessing the server via the public address of the network. The problem occurs if a second server needs to be used. Since port 80 is already being mapped it cannot be used. It is trivial to select a different port, however unless remote users are informed of the non-standard usage they will be unable to access the second server.

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.

8.5 10/100 Ethernet switch

The home office is wired with 4 Ethernet drops feed by the whole house 10/100 hub. This turned out to be inadequate so the Router's built in 4-port Ethernet switch is very handy. Since a simple hub feeds the house the router has to have a switch, since two hubs cannot be cascaded at 100Mbp/s. One port on the switch is configured as the uplink port. This connects to the 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.

8.6 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 provide secure remote access to the corporate network.

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 the VPN, this is called split tunnel mode. In addition, some users such as yours truly, run home networks behind a NAT router. 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 two security modes Authentication Header (AH) and Encapsulating Security Payload (ESP) AH authenticates the IP address and cannot be used with NAT since the NAT router modifies the client's address. Mutual authentication is performed using Internet Key Exchange (IKE).

Getting this to work required updating the firmware in the SOHO router. Installing newer VPN software at the office and client. 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.

Depending on the type of VPN you use the router may have to support IPsec pass through. IPsec has a similar problem as FTP. Even though the request originated from the local user, the server determines which port to use for the actual session. The NAT router needs to be able to learn the association or the session will fail. This requires the router function as an Application Level Gateway (ALG). It has to understand IPsec, just like it needs to understand FTP.

Split-tunnel VPN creates a security concern. The client is able to access the Internet and corporate network at the same time. An attacker can relay traffic directly into the corporate LAN from a compromised client. As a minimum each client should be running the latest antiviral software. User training should stress safe computing practices.

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
- Verify ISP does not block VPN traffic because it is considered biz use
- 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 IP address range cannot be used in both locations.
- If your ISP assigns dynamic IP addresses the network administrator cannot bind the remote VPN client to a specific IP addresses.

- 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.
- PPPoE adds 8 bytes of overhead, this reduces max packet (MTU) to 1492 bytes rather then 1500. Make sure the VPN handles this correctly.

8.7 Logging

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

9 Debug -- When Things Go Wrong

Unfortunately networks occasionally fail. When a failure occurs it is often difficult to determine the underlying cause. 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	Observe host to host path
Ethernet Indicators	Verify physical link operation

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

9.1 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 ping a local PC its IP address. In the second case we ping a public web server on the Internet by its domain name. When using PING by name the first thing PING does is translate the host name to IP address. This quickly determines if DNS is working correctly. The third example shows a typical report when the host ignores ping requests.

PING is very useful to verify if the remote host is accessible and how long it takes to reach it. If the host cannot 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 the ping command times out as shown in example 3.

Example 1: Ping local computer IP address.

```
Pinging 192.168.2.2 with 32 bytes of data:
      Reply from 192.168.2.2: bytes=32 time=2ms TTL=128
      Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
      Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
      Reply from 192.168.2.2: bytes=32 time=1ms TTL=128

      Ping statistics for 192.168.2.2:
          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
```

9.2 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 packet to be rejected at each hop. To reach the next hop TTL is increased by one. When a router receives a packet with an expired TTL it discards the packet and informs the sender the packet exceeded the TTL limit. 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 a host will not respond to being pinged, Trace Route still works to identify the route but ping will timeout.

Windows includes a command line Trace Route utility, TRACERT. VisualRoute provides more information then 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 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   *     *     *     192.168.2.1 (Broadband Router)
2  21 ms 68 ms 28 ms  10.20.1.1
3  20 ms 20 ms 22 ms  F0-1-0.G-RTR1.MAN.verizon-gni.net [64.223.132.66]
4  24 ms 23 ms 22 ms  s3-0-2.bstnma1-cr7.bbnplanet.net [4.24.92.5]
5  24 ms 24 ms 23 ms  so-3-1-0.bstnma1-nbr1.bbnplanet.net [4.24.4.225]
6  27 ms 24 ms 23 ms  so-7-0-0.bstnma1-nbr2.bbnplanet.net [4.24.10.218]
7  31 ms 31 ms 30 ms  p9-0.nycmny1-nbr2.bbnplanet.net [4.24.6.50]
8  29 ms 32 ms 32 ms  p1-0.nycmny1-cr2.bbnplanet.net [4.24.7.6]
9  33 ms 36 ms 34 ms  h0.netaccess.bbnplanet.net [4.24.153.130]
10 36 ms 36 ms 36 ms  a9-0-0-8.msfc1.oct.nac.net [209.123.11.85]
11 36 ms 33 ms 39 ms  dslreports.com [209.123.109.175]

Trace complete.
```

9.3 NET

NET is a Windows 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 a service.
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
```

9.4 NETSTAT

NETSTAT is a Windows 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
```

9.5 WINIPCFG

Windows WINIPCFG utility displays the current configuration for each network adapter. From the start menu open run dialog box. Type WINIPCFG. In Windows 2000 enter the IPCONFIG command in a DOS box.

WINIPCFG lets you examine 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 if the computer has the correct IP address. If the PC is supposed to obtain a dynamic address from a DHCP server and instead it self-assigned an AutoIP address you know the PC was unable to find the DHCP server.

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. The DHCP server is the address of the dynamic address server. DNS server address is the address of the name server. In a simple network DNS, Gateway and DHCP should all be the address of the broadband router.

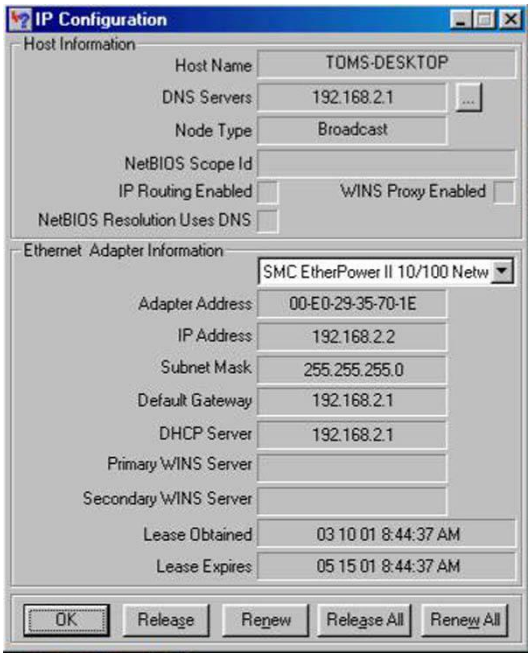


Figure 25 WINIPCFG

9.6 Ethernet Indicators

Ethernet cards, hubs and switches typically include a number of indicators that are very helpful troubleshooting aids.

Indicator	Purpose
Link	Active connection between card and hub/switch
10/100Mbp/s	Indicates link speed
Full Duplex/Half duplex	Half duplex when used with a hub and full duplex with switch
Activity	Flashes during transmission or reception
Collision	Flashes when hub detects collision

If the Link indicator is not on the link is not working. This is most likely a cable fault or hardware failure of the Ethernet adapter or hub.

Ethernet cards automatically determine if they should operate at 10 or 100Mbp/s. For 100Mbp/s operation both sides must be capable of Fast Ethernet and wiring must meet Cat5 standards.

When using a hub collisions get worse at utilization grows. Occasional collisions are nothing to worry about.

10 Browsing -- Wild Wild Web

All PCs use Microsoft IE5.5 or 6.

Key to effective use of the Internet is being able to find what you want. Our preferred search engine is Google. They recently created a toolbar add on to IE. This allows search requests to be made directly from IE.

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

E-mail accounts fall into three broad categories; ISP account, browser based free mail and accounts on your own domain. ISPs typically offer one or more email accounts to subscribers. This is convenient but ties your e-mail address to your current ISP. Change ISP and your e-mail addresses changes. Free mail services like Yahoo are advertising supported. They decouple your e-mail address from your ISP. Free accounts make sense for personal use. Even though they are advertising supported the advertising is not overly intrusive. These accounts use a web browser interface. They have the advantage of being accessible from any computer. For business purposes or to insure long lasting email address nothing beats registering your own domain name. Once you have a domain name mail is addressed to you@yourdomain.com. If you change the hosting service you simply transfer your domain to the new provider, your mail address stays the same.

> ***Antispam tip:*** With your own domain 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.

11.1 Browser based Mail

Web based mail eliminates the need for specialized mail clients. You can access mail from any browser equipped PC. The user interface is less convenient then a mail client but is very useful for casual use.

11.2 Mail Client

Except for browser-based mail, e-mail has a sending component, SMTP, and a mailbox part POP. When you 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 mail. Normally the mail client requests the server to delete 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.

11.3 Corporate Mail

Telecommuters need to be able to access corporate mail when out of the office. 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 a VPN client.

In our case connecting to the VPN required additional authentication and the connection was expired periodically to increase security. This is not a problem when traveling and connecting for a short time but it gets tedious as a telecommuter. A solution to this problem, if it is acceptable to your administrator, is to set up your corporate mail account to automatically forward all incoming business mail to one of your personal mail accounts. This allows you to access your corporate mail without activating the VPN.

11.4 SPAM Mitigation

The lack of SMTP security is the cause of many problems. Unlike POP, typical SMTP configuration does not require authentication. This means it will cheerfully forward any mail presented to it. This has proven a boon to mass mailers to inundate users with Spam. ISPs have adopted a number of strategies to minimize the problem. This makes choosing the optimum mail configuration difficult, especially when using a laptop that connects via different ISPs or to manage multiple mail accounts.

11.4.1 Block Outgoing Port 25

SMTP uses TCP port 25. Some ISP's block this port at the edge of their network. This effectively prevents customers from using any SMTP server not under control of the ISP. ISPs like this approach because if they get a SPAM complaint they can track down the sender since each user is authenticated.

The down side of this method is that you have to use the SMTP server provided by the ISP or use a SMTP server on a non standard port.

11.4.2 Prevent Relaying

In this case the ISP blocks SMTP access from clients outside its network. This prevents anyone not logged into the ISP's network from using the ISP's server to send mail.

This prevents the user from using the same SMTP server if they use multiple ISPs.

11.4.3 Blacklist

The ISP can subscribe to a service that lists the domain names of known Spammers. If mail arrives from a forbidden address it is refused. Lists also exist of address blocks assigned to consumer ISP's. Mail can be blocked if it arrives from one of these addresses on the assumption that one should not see a SMTP on these address ranges.

11.4.4 Reverse Name Lookup

Before accepting mail the ISP can verify the mail is from a valid domain. They can also verify the forwarding SMTP server IP address resolves to a domain name.

11.4.5 Account Verification

Verizon has a controversial policy of only accepting outgoing mail if the email from address is a Verizon mail account, such as username@verizon.com.

The downside of this policy is you cannot use Verizon outgoing SMTP server to send mail from non-Verizon mail accounts.

11.4.6 Quantity Limits

The ISP may implement rate filters, limiting how much mail can be sent over a given period of time. This is effective at blocking Span since they need to send a huge quantity of mail.

11.4.7 POP Authenticate Before SMTP Send

To allow customer SMTP access regardless of how they connect one technique is to force the user to retrieve mail from the POP account before allowing SMTP access. Once the user is verified the ISP assumes the IP address is trustworthy for a short time. This allows the customer to send mail regardless of how they connect, unless the ISP blocks access to port 25. Web hosting services commonly allow this type of connection since their customers use other providers to access the Internet.

11.4.8 SMTP Authentication

A cleaner method of SMTP access control is to require authentication, just like the POP server. This allows the customer to send mail independent of how they connect, unless the connecting ISP blocks access to port 25. This is becoming the preferred method of foreign mail access.

11.4.9 My Implementation

None of the ISP's I use block port 25 and my domain hosting service just implemented SMTP authentication. This allowed me to configure all mail accounts on both the workstation and laptop to send mail using my domain SMTP server. This eliminates the need to modify SMTP based on how I connect.

Mail Configuration Tip -- Archiving mail when using multiple clients is difficult. One trick I've found useful is to have your main computer remove mail from the POP server. The rest of the machines retrieve mail but do not delete the message from the server. Then when you get back to the main machine it retrieves all the intervening messages and removes them from the server.

Mail Configuration Tip – I use Microsoft Outlook mail client configured with multiple mail accounts. One account is set as the default. New mail is sent using the SMTP server configured for that account. However if you reply to mail received from a different account Outlook uses the SMTP server defined for that account. This is the source of some confusion. If you set Outlook up incorrectly sending new mail will work fine, but you will be unable to send replies.

Security Tip -- Be careful opening e-mail attachments. This is a common method of spreading viruses and Trojans. Configure your anti-virus program to scan email and attachments prior to opening them and quarantine infected mail.

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.

12 Fax – E-mail on Paper

Originally we did not want to use fax at all, preferring to interact with clients via e-mail or telephone. We found it 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 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 928-223-4815. When a fax comes in it is converted to a file and e-mailed to the subscriber. Special eFax software is used to read the attachment. The attachment can be saved and imported by other programs.

To send a fax we use the Phone Tools utility Dell bundled with the PC. This allows direct faxing of electronic documents or scanned hard copy. The multiline office phone includes a data jack that allows the fax modem to be switched to any phone line.

This works well for the limited number of faxes we send and receive.

13 USENET – 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 40,000 news groups. Most groups have an online FAQ that describes what the group is about to limit off topic posts. Newsgroups are a valuable source of up to date 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 to Usenet regardless of how you connect.

Security Tip -- Spammers commonly harvest email addresses from Usenet posts. It is common practice to use a fake mail address on Usenet. Do no simply make up an email address – it may turn out to be someone else's real address, instead use an invalid Top Level Domain. My Usenet mail address is tomnews@tschmidt.invalid.

14 Multimedia – Sound and Images from Around the World

Using the Internet to deliver audio and video is hampered by the limited speed available using dialup. Broadband eases this chokepoint opening the door to Internet delivery of radio and TV. Peer-to-peer sharing of music and video is controversial because it makes it difficult for content owners to charge usage fees. Direct distribution of content is in its infancy. Deployment of broadband opens the door to new methods of distributing content.

14.1 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 limited to dialup the service is optimized for slow connections. Some programs are encoded in multiple data rates so broadband user have access higher quality audio.

14.2 MP3

MPEG MP3 compression format provides near CD-quality audio at 128Kbp/s about a tenth the raw music data rate. 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 to a megabyte per minute of playing time so large libraries consume tens of gigabytes. This is large but well within the reach of a cheap hard drive.

14.3 Windows Media Player

Microsoft developed proprietary audio and video compression formats that can only be viewed with Windows Media Player. They are also beginning to deploy provisions for secure distribution of music. Paving the way for direct purchase or subscription based music services.

15 Printing – Data to Paper

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

Initially we used Windows peer-to-peer print sharing. The printer was connected to the laptop used to share the Internet connection. It worked okay for occasional use but we ran into problems of lost and aborted print jobs. This typically occurred if the connection sharing software needed to establish an Internet connection or if simultaneous print jobs were started from multiple computers. We attempted to use a print server to address this problem. However we found that the HP 720 Inkjet printer used Windows Graphic Device Interface (GDI) that is incompatible with print servers.

We acquired a new HP 2000 professional Inkjet printer and a HP JetDirect 300X print server. Many different print servers are on the market. We chose the HP print server mainly to minimize potential compatibility problems. The print driver runs locally on the machine requesting the print job. The output of the driver is sent to a virtual printer port, which is the print server. The print server in turn delivers the print job to the printer. This works much better then peer-to-peer printing. The print server itself is a little box, the size of an analog modem. It has a built in web server to manage the print server remotely.

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

16 Scanning -- Paper to Data

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.

We investigated networking the scanner. This proved difficult since the scanner needs to know where to put scanned images and without user intervention each file is named with a sequence number. The solution we came up with it to connect the scanner to a PC workstation and create a shared image folder on the server. Images are scanned using Adobe Photoshop running on the workstation, named, and then saved on the server. Once on the server any PC on the LAN can retrieve the files.

We ran into a problem with the Umax tool bar application that supports the scanner buttons. It often caused Windows to hang on shutdown. We finally gave up and removed the application.

17 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 the server. This was convenient because it was self-contained but had limited disk storage capacity. When the laptop died it was replaced with a recycled 200Mz Pentium desktop with a new 45GB hard drive. If storage requirements increase it has room for another disk.

17.1 File Sharing

One of the benefits of having a network is the ease files can be transferred between machines. This allows online backup of important files. File sharing makes bringing up a new computer easier since device drivers and application software 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. We created a share on the server for each network user.

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.

17.2 Time Service

The Internet allows access to extremely accurate time standard. 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 the time information from the NIST server 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 the computers on the LAN are slaved to the local server and the local server in turn is synchronized to NIST.

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 them via the Internet adds up to several hundred milliseconds of round trip delay. This source of error is not a problem for our purpose.

> ***Configuration Tip*** --Tardis 2000 defaults the NTP time broadcasts to all available interfaces. If Tardis is run on a computer with direct access to the Internet the configuration should be changed to limit broadcast to the LAN. IP broadcast is a reserved address x.x.x.255, so typical broadcast address might be 192.168.2.255. If this is not done the time 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 likely 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 64 seconds so the client clock is updated as soon as the machine boots.
>
> ***Configuration Tip*** -- Tardis includes a provision to monitor for active dialup connection. This is convenient if the PC running Tardis is directly attached to the Internet. In our case Tardis is behind a router so it cannot determine if an Internet connection exists. On DSL this is of no import since it is an always-on connection. However, in the event of fallback to dialup we do not want Tardis to force dialup to be active for long periods. Tardis is set to access the NIST timeserver every 12 hours. So at most it will activate dialup twice a day. The router is set to timeout dialup after 30 minutes of idle, so Tardis will cause dialup to be active for an hour a day.

17.3 Private Web Server

The home page of IE on 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, 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 web server is only bound to the LAN interface. Otherwise anyone on the Internet will be able to access your private web pages.

17.4 Local Weather Station

One of the reasons to run a local web server is 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. We configured the Davis software to maintain history data and to create a GIF file of inside temp, outside temp, wind chill, and wind speed every five minutes. These GIFs are displayed on the local web page.

18 KVM -- So Many Computers So Little Space

We did not want to use another set of user I/O when we setup the server. The solution was 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 computers. We purchased a 4 port Belkin Omni View SE KVM. Port 1 is the workstation port 2 the server leaving 2 ports for future use.

Figure 26 KVM

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 -- Workstations tend to use much higher resolution and faster refresh rate then servers. This results in a very high video data rate. This is usually not a problem for the KVM itself but requires high quality video cable. The video cable should use coax for each of the three video signals. Coax preserves the high frequency component of the signal and minimized cross talk between the three video signals. Failure to use high quality cable will result 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 cause the mouse to revert to default mode, use of the wheel and left thumb button is disabled. To get around this problem the desktop runs the Logitech mouse driver and is connected to port 1 on the KVM. When the system boots everything is fine. Port 1 is the default port so at power up the host can access these devices directly. 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 to 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 solved the problem.

19 Backup – Oops Protection

One of the benefits of switching from a laptop to a desktop file server was much larger hard disk. This enabled us to use online backup.

19.1 On Line Backup

The server has shares allocated for each person. Currently it is equipped with a 45GB drive, if we need more space there is room for an additional drive. We chose Second Copy 2000 as the backup utility. Second Copy allows setting up multiple profiles. Each profile can be run automatically or manually. The backup copy can be either a direct copy of the data or it can be a compressed image.

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.

Configuration Tip -- Second Copy cannot copy files that are in use. For example the Outlook mail client is always running, preventing backup of mail files. The Second Copy profile for mail is setup for manual copy. To backup mail, Outlook is shutdown and the profile activated manually.

19.2 Off Line Backup

There is no substitute for off line backup. It is the best way to recover from virus or physical damage, such as a fire. If your data consists of a few e-mails or text documents a floppy will suffice. Zip Drives, CD-R, or tape can be used to create large off line backup.

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 grossly underestimated the size of backup data. Next time I'll select a larger backup device.

Occasional backup to off line storage allows recovery if the worst happens. For maximum safety the backup copies should not be stored in the same location at the computer.

20 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 vast resources of the Internet but at the same time makes your computer vulnerable to attack. Unfortunately a significant number of talented individuals take delight in wreaking havoc on others.

20.1 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. This means ALL connection requests that originate outside the SOHO LAN are refused. One of the benefits of NAT is that by default 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 the public IP address the NAT router prevents the connection because it doesn't know which computer to send the packet to. Only if explicit mapping rules are created will NAT know how to route the request.

The router allows specific IP addresses/ports to 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.

20.2 Anti Virus Software

We use Mcafee VirusScan. It checks 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.

20.3 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 vulnerability is discovered information is quickly distributed on the web. The best insurance is the latest patch.

20.4 Spyware

Companies find every more clever ways to obtain information about customers. This has led to a technique called spyware. Spyware gets installed with many applications and sends information about usage back to the company. The application periodically contacts the company to send information about user activity. Another method is a 1-pixel tag in HTML To render the tag the browser must connect to the link, depending on the ID of the tag the company is able to learn if and when you access the page. More worrisome are programs such as Real Jukebox that reports which songs were played.

It is possible to configure the firewall to block access to specific sites, but often time's spyware connects to sites that you frequent and cannot restrict access. Some personal software firewalls such as Zone Alarm monitor both incoming and outgoing traffic by application. This allows the user to specify what to allow into and out of the PC.

Gibson Research created a spyware removal tool called OptOut. That is no longer supported and has been taken over by Lavasoft Ad-Aware. This program searches for know spyware programs and browser cookies, allowing the user to remove them.

20.5 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 use 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 use of modems in networked machines. They are a potential backdoor to your LAN

20.6 Social Engineering

Sad to say many security breaches are not the result of compromising 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 you will never be asked to give someone your password.
- Limit the amount of personal information you divulge. You need to disclose enough information 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 antiviral software is no guarantee. It is possible to get infected before the antiviral 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.

21 Laptop – Connecting from Anywhere

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

Location specific network settings are sprinkled all over Windows and within various applications. This makes it hard to move a computer between locations. One of the reasons we converted from proxy to NAT was to eliminate configuring applications to use location specific proxy. NAT is largely transparent to applications.

Even though we attempted to minimize the differences between locations we still wound up with several site-specific settings. The solution was to use NetSwitcher to effect location specific changes. The table below shows the various network setting and which ones need to be changed by NetSwitcher.

	@Home	@Office	On the road
IP Address	DHCP	DHCP	Dialup PPP DHCP
User Authentication	Windows Client	NT Domain	Windows Client
Office File Shares	VPN	NT permissions	VPN
SOHO File Shares	Peer-to-peer	N/A	N/A
Default Printer	Local network printer	Local network printer	Directly attached printer
Time	K9 client	N/A	N/A
Email receive	3 POP accounts	3 POP accounts	3 POP accounts
Email send	Authenticated SMTP	Authenticated SMTP	Authenticated SMTP
Usenet	Authenticated dialup account DSL account	Authenticated dialup account	Authenticated dialup account
IE home page	Private web server	Biz home page	Dummy home page on laptop

Note: Netswitcher modifies entries highlighted in yellow.

Figure 27 Laptop configuration table

21.1 Netswitcher

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

This left us with the need to change 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 create 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, the change goes into effect and all is well. The next time you change location then 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.

22 Web Hosting -- Your Presence on the Web

Every business needs at least a minimal web presence. The easiest way to set up a site is to use a hosting service 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 first mile connection to your business. Many ISPs allow customers to set up public web servers for free. 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.

Using a hosting service means web site traffic need not 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 managing a small network.

23 YourDomain.com – Your Name on the Internet

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

There are many ways to implement a business web server. It can be a virtual server provided by the hosting service, a physical server collocated at the hosting service, or a server physically located at your place of business. A virtual server allows a single physical machine to run multiple web sites resulting in very low cost. This is cost effective for low traffic sites. Choice of the optimum server implementation 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.

A registered domain allows email to be moved completely in house rather then use the services of the hosting service. To do this one must set up a POP and SMTP server and have the hosting service create DNS records that point to the IP address of the servers. This requires your network be assigned static IP address.

The hosting service fee is based on the size of the web site and the amount of traffic it generates. We use the same company for both web hosting and dial up access http://www.inr.net.

23.1 Registering Your Domain Name

The first choice is to decide which Top Level Domain (TLD) is most appropriate for your business. You can register the same name in multiple TLDs this is typically done when the company name is trademarked. The COM TLD is for commercial use, so is the new BIZ TLD. Networking companies commonly use the NET TLD. Some TLDs are geographically specific. If you want to identify your company with a specific region they are a good choice.

Hosting services typically provide automated tools to register and setup a domain. They coordinate with InterNIC or other registration agencies. To register a name the registrar database is examined to insure the request does not conflict with an existing name in the TLD. The new name is assigned provisionally in case another registrar has recently recorded the same name. The hosting service updates their DNS name server database to translate the domain name to the IP address of your web server. Once registered it takes 24-48 hours for your domain name to propagate throughout the DNS system on the Internet.

23.2 WHOIS record for Tschmidt.com

Information for each registered domain is maintained in the WHOIS database. Below is the WHOIS record for the Tschmidt.com domain.

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

   Domain Name: TSCHMIDT.COM

   Administrative Contact, Billing Contact:
      Administrative Services  (AS935-ORG)  admin@TSCHMIDT.COM
      Schmidt Consulting
      95 Melendy Road
      Milford , NH 03055
      US
      (603) 673-5804
   Technical Contact:
      Network Operations Center  (NO153-ORG)  noc@INR.NET
      Internet Resource Networks
      20A Northwest Blvd. #131
      Nashua, NH 03063
      US
      603.880.8120
      Fax- - 603.880.8783

   Record last updated on 11-Oct-2001.
   Record expires on 04-Nov-2003.
   Record created on 04-Nov-1998.
   Database last updated on 23-Dec-2001 22:29:00 EST.

   Domain servers in listed order:

   NS1.INR.NET                65.160.136.4
   NS2.INR.NET                198.77.208.4
```

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 owns 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.

23.3 Creating Your Web Site

Creating a web site requires a combination of graphics and technical design elements. Sites range from simple ones that provide static information to complex database driven e-commerce sites. A word processor can be used to create a simple site. For a 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 outsource this task.

23.4 Site Logs

The hosting service typically provides a log of everyone that visits your site and what pages they looked at. This data can be analyzed to understand how customers use the site.

23.5 Email

An advantage of having your own domain name is that email is addressed to your domain not the ISP. This personalizes your web presence. Normally the hosting service provides one or more e-mail accounts. Email 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 mail not sorted to another account is deposited. I did not realize how useful that is until I started creating a 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.

24 Power Distribution – Wires and More Wires

Creating a home network tends to create a jumble of cabling, both data and power to feed the computers and large number of wall warts used by small devices. After struggling with multiple power strips I decided to try an organize power distribution.

Figure 28 Power Panel

Power Panel requirements

- Multiple always on receptacles
- Multiple switched receptacles
- Wire routing provisions
- Mounting provisions for larger power supplies.

I wanted a large number of always on outlets. Power bricks tend to take up a lot of space, so the number of power strips is generous, four strips with six receptacles each. To minimize power consumption devices that do not have to be on continuously are automatically switched on/off with the workstation. An adapter cable plugs into the PS/2 keyboard or mouse port to pickup 5 Volts. This controls a solid-state relay that feeds the switched power strips. One note of caution; some power managed PCs leave PS/2 ports on all the time to allow remote power up. If that is the case the power panel needs to sense power directly from the main power supply.

Two rows of Velcro are used to organize the wiring. The upper level consists of Cat5 Velcro cable wraps. This holds surplus cable. The bottom row uses longer pieces of regular Velcro to hold inline power supplies.

The power panel has been used for several years and goes a long way to providing a safe environment and reducing clutter.

25 Conclusions

Setting up a SOHO network and VPN has been an extremely successful and a rewarding experience. The network meets our business and personal requirements. It is a pleasure to have high speed Internet access from every computer.

The down side is that a significant amount of technical expertise is required to setup the network. The building blocks are all readily available but the detailed knowledge to create and troubleshoot the network can be hard to come by. If you hunt a little the resources are out there. Every year more small networks are created and manufactures get better at designing easy to use equipment. In general failures are minor and easy to fix once one determines the underlying cause. It is determining the root cause that is difficult. Help is available, manufacturer-sponsored forums and specialized home networking interest groups provide insight and ready help with problem solving.

Networking today is similar to the early days of the automobile industry. When it worked it was exhilarating, but one needed a riding mechanic to keep the car going. As networking expands beyond the province of corporate IT departments it will become ever easier to install and use.

Start now - become a pioneer.

Happy networking.

Last Page
Intentionally Blank