Living with a SOHO Network
2003 edition

Tom Schmidt
Schmidt Consulting
12 December 2002
tom@tschmidt.com
http://www.tschmidt.com

Abstract

This paper discusses our experience setting up and using a small office home office (SOHO) network over a number of years. It offers guidance on selecting a high-speed Internet Service Provider (ISP), presents Local Area Network (LAN) options, describes Internet sharing methods, and discusses typical network services.

Digital Subscriber Line (DSL) provides high-speed always on Internet access. A router shares the connection with multiple computers. The router automatically falls back to dialup if DSL fails. The LAN is Fast Ethernet providing high-speed internal communication. Network services include file backup, network printing, time server, Syslog log server and local web server. IPsec Virtual Private Network (VPN) client provides secure access to the corporate network. This allows access to corporate resources while telecommuting or on the road.

Change this year was addition of a Syslog server to capture network events.

Table of Contents

1 Overview

In mid 1998 I set up a small network. I started a consulting business and wanted to learn about building and operating a Small Office Home Office (SOHO) network. My prior networking experience was limited to interactions with corporate Information Technology (IT) department.

The LAN has undergone significant evolution. It started with Dialup Internet access and a few 10 BaseT Ethernet drops. It has expanded beyond the office to encompass the entire house and been upgraded to 100 BaseT Fast Ethernet. DSL is the primary Internet connection dialup used for backup. Initially we used Wingate for Internet sharing and BlackIce Defender for intrusion detection running a dedicated laptop. The laptop was replaced with a Multitech Broadband Router. A recycled desktop now serves as a poor mans server. This runs a time server, local web server, Syslog server and file shares. Each PC normally requires its own 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 the workstation and server. The printer is networked and accessible from any PC on the LAN.

A Virtual Private Network (VPN) enables telecommuting between home and corporate network. The VPN encrypts data between home and 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 implemented the VPN has operated flawlessly.

Traveling with a Laptop presents problems, as network configuration differs at each location. A utility called NetSwitcher automates this task providing one click switching between locations.

We finally got serious about file backup. Second Copy 2000 performs automatic back up to the server.

This paper is not intended as a competitive product review. The field is constantly changing; any attempt to do so becomes quickly outdated. Rather, it discusses how specific requirements were addressed and implemented. For up to date product reviews the reader is directed to the many publications and articles on the subject. The products and services described in this paper represent my choice to deliver the features I needed.

Goals for SOHO network:

- Share broadband Internet service
- Automatic fail over to Dialup if broadband 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.

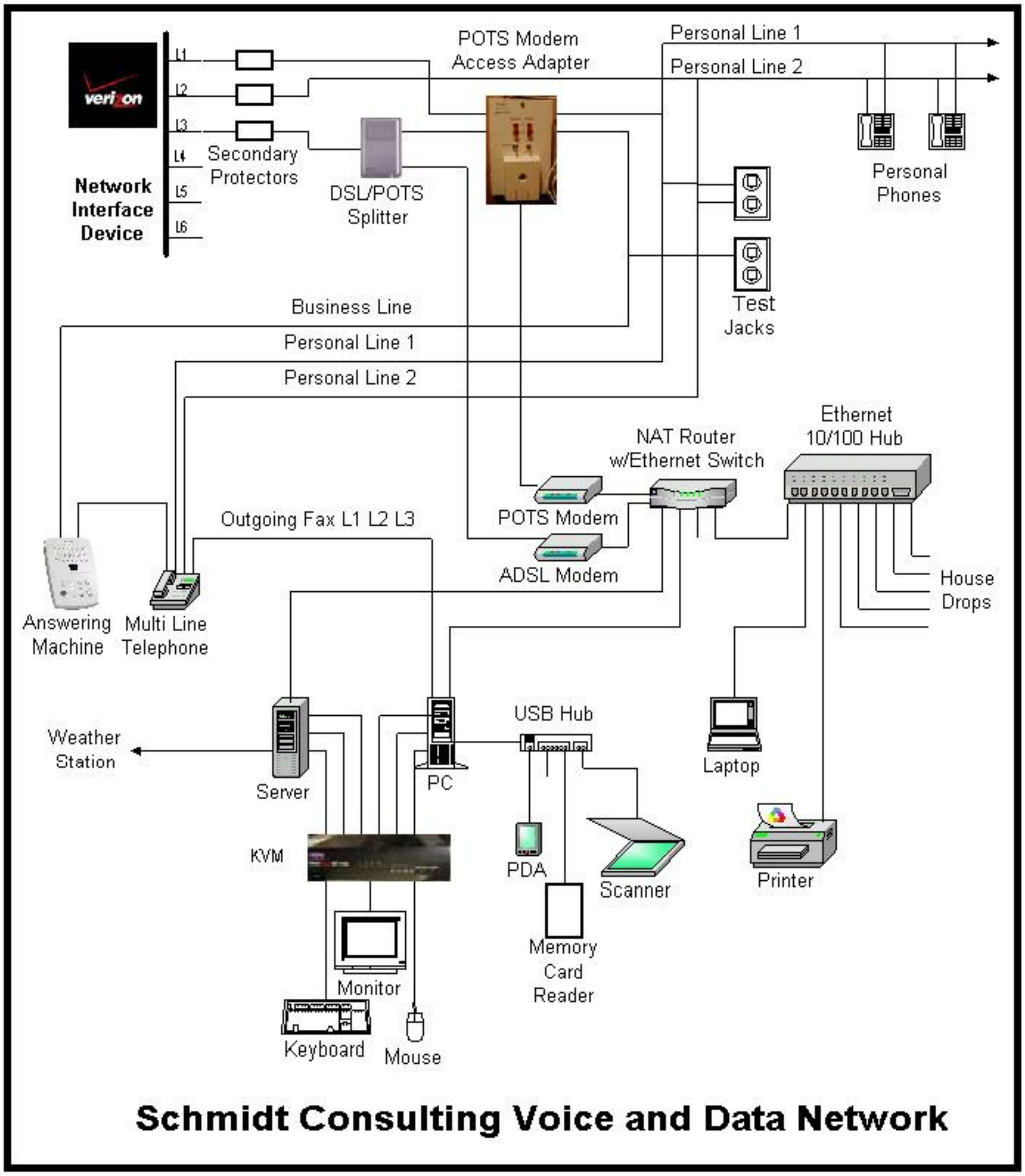


Figure 1 SOHO Data and Voice Block Diagram

2 Internet Access Options – Your Friendly ISP

The most common types of Internet access are: dial-up using ordinary phone service, T-1 data service, Digital Subscriber Line (DSL) high-speed service using telephone wiring, and Cable Modem using the Cable TV facility. An advantage of broadband service; besides high-speed is it is always on. The connection is active 24/7 one does not have to wait while the modem connects to the Internet – it is ready whenever needed.

Typical ISP services:

- Connect customer to ISP network – so called first - mile
- Routing between customer and one or more Internet interexchange carriers
- Customer account authentication and management
- IP address assignment
- DNS name resolution
- E-mail account
- USENET account
- Web hosting
- Billing
- Technical Support

2.1 Plain Old Telephone Service (POTS) Dialup

Dialup Internet access is available to anyone with telephone service. Dialup modems can be used with both wired and cellular phone service. Data rate is significantly slower over cellular and per minute connect charges are the norm so it is not optimal for fixed location use.

Almost all Dialup ISPs support ITU-T V.90 modem standard. The International Telecommunications Union V.90 standard replaced previous generation of proprietary 56Flex and X2 modems. V.90 requires the ISP modem be directly connected to phone company digital trunk. Only a single digital to analog conversion can exist between ISP and user. The ISP modem is synchronized to the digital trunk. This enables it to transmit at up to 56 kbps toward the user. In the US FCC power limitation reduces effective maximum speed to about 53.333 kbps. Transmission from subscriber to ISP uses V.34 mode with a maximum speed of 33.6 kbps. If the modem cannot connect in V.90 mode it automatically falls back to V.34 mode in both directions with a maximum speed of 33.6 kbps. Most phone lines are digitized at the Telco central office at 64 kbps. This means POTS modem technology has reached its theoretical maximum speed. To obtain higher speed requires use of different technology.

ITU recently released V.92 an enhancement to V.90. It increases upload speed slightly to 48 kbps and implements faster auto negotiation to reduce call setup time. V.44 compression improved compression of reference test data 6:1 vs 4:1. Modem on Hold (MOH) allows the modem to park the data session allowing the user to answer a short incoming call. This works in conjunction with Call Waiting and requires support from the ISP. V.92 modems are readily available but ISP’s have been slow to upgrade.

To obtain optimum speed V.90 and V. 92 modems require the phone circuit operate at better than minimum specification. There are many effects that reduce modem speed while not interfering with voice quality. Dialup modem impairments are discussed in a separate paper.

At connect time the modem probes the phone line to determine noise and attenuation characteristics to set initial connect speed. The modem constantly adjusts speed in response to varying line conditions. After the modems synchronize the ISP authenticates the user and assigns an IP address. Once the computer has an IP address it is able to access the Internet. The most common protocol used to traverse the dialup connection is Point-to-Point Protocol (PPP). This allows Internet Protocol (IP) to be carried over the serial telephone link between user and ISP.

2.2 T-1 and E-1 Carrier

T-1 digital carrier was developed by the US Bell System in the early 1960's to reduce interoffice transmission cost. Prior to digital carrier frequency division multiplexing (FDM) was used to carry multiple voice channels over a single facility. T-1 transports 24 voice channels. E1 carrier, used in Europe, is similar carrying 30 voice channels. Each channel is digitized resulting in a 64 kbps data rate. 24 channels require 1.536 Mbps plus an 8 kbps control channel resulting in a data rate of 1.544 Mbps (E1 is 2.048 Mbps). Telephone circuits are full duplex requiring a symmetric connection; T-1 delivers 1.544 Mbps in each direction.

T-1 requires two copper circuits a pair for receive and one for transmit called a 4-wire facility. Internally T-1 may be implemented in a number of ways: 4-wire physical circuit, complex modulation to derive both directions from a single copper pair or SONET optical carrier. Regardless of how it is implemented the customer interface to T-1 service is the 4-wire circuit.

In the early 1980's T-1 was trarrifed and made available to customers. T-1 continues to be extremely popular in commercial service to carry both voice and data. Prices for T-1 have dropped dramatically as technology improves and from competitive pressure by alternative high-speed services.

2.2.1 Converting Voice to Bits

Voice grade phone service occupies the frequency band of 300-3000 Hz. Low frequencies are attenuated to eliminate interference from power line noise. Increasing upper bound beyond 3000 Hz does little to improve intelligibility, at the expense of greater bandwidth consumption. Digital sampling must be performed at least twice as fast as the highest frequency of interest, a sample rate of 8,000 times a second was chosen. It was found sampling to 12-bits resulting in 4096 possible values resulted in excellent voice quality. This required a 96 kbps data stream. To reduce data rate engineers decided to use only 8-bits or 256 values per sample, resulting in a 64,000 bps data stream. To minimize quality degradation, the conversion is performed logarithmically. When sound level is low samples are close together. During loud passages samples are farther apart. This masks quantizing noise generated by the conversion process. The process is called u-LAW (US) A-LAW (Europe) Pulse Code Modulation (PCM).

Twenty-four 64 kbps channels plus the 8 kbps control channel requires 1.544 Mbps. Channels are interleaved in time one after the other using Time Division Multiplexing (TDM). 60's technology allowed T-1 to travel about 6,000 feet before regeneration was required. 6,000 feet was chosen because that is the distance between H88 load coils used to extend voice circuits. This allowed T-1 regenerators to be housed at the same location.

The PCM coding scheme developed for T-1is what makes V.90 and V.92 dialup modems possible. It is also the reason dialup is limited to 56 kbps. Logarithmic sampling minimizes the effect of noise when used for voice but only allows 7 of the 8 bits to be used for data, 8,000 samples per second times 7-bits per sample is 56,000 bits per second. Dialup modems have reached the limit of theoretical performance.

2.2.2 Channelized vs. Unchannelized

When used for Internet access channelization is neither required nor desired. T-1 data circuits are unchannelized this exposes total channel capacity to the IP layer. Multiplexing is performed at the IP rather than physical layer. Some circuits are provisioned to allow flexible control of channelization. This allows an Integrated Access Device (IAD) to dynamically allocate bandwidth between voice and data.

2.2.3 CSU and DSU

The Channel Service Unit (CSU) is connected directly to the 4-wire facility. The CSU regenerates bipolar signals before handing them off to DSU. The CSU provides keep alive and loopback testing enabling the Telco to monitor line quality.

T-1 uses bipolar plus and minus 3-volt pulses, between pulses voltage returns to zero. The Digital Service Unit (DSU) converts bipolar signals to a synchronous interface such as V.35 that both RS232 single ended and RS422 differential signaling to connect to customer equipment.

2.2.4 Smart Jack

When T-1 was developed the interface between CSU and DSU, called DSX-1, was designated the demarcation point between Telco and customer. It still is in the rest of the world. During US deregulation the FCC defined the 4-wire facility as the demarcation point. This caused problems for the Telco as now management and quality assurance functions were no longer under their control but provided by customer premise equipment (CPE). The solution was the Smart Jack. It presents a 4-wire facility interface to the customer but includes loopback provision controlled of the service provider.

2.2.5 Provisioning

T-1 requires repeaters spaced approximately every 6,000 feet. Repeaters regenerate bipolar signals, allowing T-1 to deliver very low error rates compared to analog carrier. Repeaters can be powered from the T-1 line, called a span, eliminating the need for local power.

T-1 bipolar signaling is relatively noisy. This requires care during circuit provisioning to prevent interference between T-1 and other services, including other T-1s on the same cable.

At the customer location the Telco typically installs a Smart Jack. Jack electronics can be powered from the T-1 span eliminating the need for a local power supply. The customer interface to the Smart Jack is an RJ48 8-position data jack. Regardless of how the service provider transports T-1 internally the customer is presented with a 4-wire T-1 facility interface.

T-1 provides end-to-end connectivity. Internet access requires the remote end terminate at an ISP.

Most T-1 compatible routers include CSU and DSU functionality. This allows the router to connect directly to the Smart Jack, eliminating cost and clutter of multiple pieces of equipment.

2.2.6 Beyond T-1

The modern telephone network is almost entirely digital, except for the 2-wire analog connection to POTS equipment. Carrier hierarchy is based on voice channels. The lowest level, called Digital Service 0 (DS-0), is a single PCM digitized voice circuit of 64 kbps. Next in the hierarchy is DS-1 (24 voice circuits over T-1 carrier) operating at 1.544 Mbps, then DS-2 (T-2) operating at 6.312 Mbps equivalent to 4 T-1 circuits. Then DS-3 (T-3) at 44.736 Mbps equivalent to 28 T-1 circuits.

DS level refers to channel speed; T-1 has a DS-1 channel speed of 1.544 Mbps and is carried over a 4-wire copper facility. Popular usage has corrupted this distinction. T-1 is commonly used to mean any 1.544 Mbps service.

Higher speed transmission is optical using Synchronous Optical Network (SONET). Synchronous Transport Signal Level 1 (STS-1) Optical Carrier 1 (OC-1) operates at 51.84 Mbps. Next in the hierarchy is STS-3 (OC-3) 155.52 Mbps. Then STS-12 (OC-12) operating at 622.08 Mbps. Then STS-48 (OC-48) operating at 2.488 Gbps. OC-192 at 10 Gbps is a convergence point. It is the first time Ethernet and SONET speeds match. This opens the door for Ethernet to be carried directly by the SONET network.

2.3 Digital Subscriber Line (DSL)

Digital Subscriber Line (DSL) technology utilizes existing telephone copper wiring between subscriber and phone company central office (CO) to carry high-speed data. This allows the local exchange carrier (LEC) to generate additional revenue by leveraging its massive investment in cabling. Several types of DSL have been developed hence the xDSL moniker. The most common types are Asymmetric DSL (ADSL) G992.1 and Symmetric DSL (SDSL). Telco’s like DSL not only as another revenue source but because it gets long duration data calls off the Public Switched Telephone Network (PSTN). This minimizes the need for expensive upgrades to the circuit switched phone network.

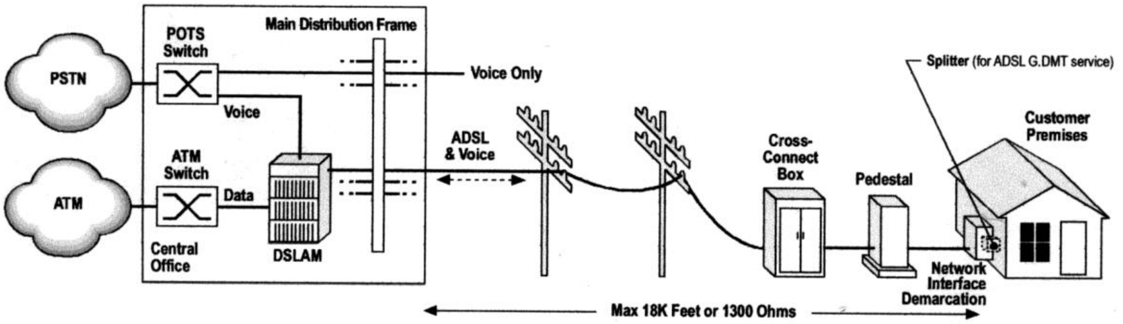


Figure 2 Shared ADSL POTS Service

ADSL was initially developed for video on demand and has been recycled for broadband Internet access. ADSL has higher download speed, toward the subscriber, than upload. It uses frequencies above those used with Plain Old Telephone Service (POTS) allowing it to coexist with voice service. This minimizes cost by allowing a single copper pair to be used for both voice and data service. A single line residence can be equipped with both phone and high-speed data service. Typical ADSL speed is 500 - 1500 kbps downstream and 128 - 512 kbps upstream

At the Telephone central office a Digital Subscriber Line Access Multiplexer (DSLAM) connects to the customer's phone line. The voice portion is passed through a low pass filter and connected to the POTS network. The DSLAM recovers customer data and uses Asynchronous Transfer Mode (ATM) to link customer to ISP. The Telco uses ATM because it facilitates support of 3rd party ISPs. At the customer location a similar filter is used to separate DSL from POTS. This can be either a whole house POTS/DSL splitter or microfilters connected ahead of each non-DSL device.

SDSL is typically marketed as a business service. It requires a dedicated copper pair; it cannot be shared with POTS. Being symmetric makes it suitable for use with servers. A special version of SDSL called IDSL offers symmetric speed of 128 or 144 Kbps over longer distances than either ADSL or SDSL. IDSL uses ISDN signaling allowing it to be used at distances >20K feet.

DSL speed is a function of line length, wire gauge and line quality. ADSL is limited to about 18,000 feet. Providers often limit service to lesser distance to minimize problems. Remote DSLAMs, called Remote Terminals (RT), shorten loop distance by moving the DSLAM closer to the customer. This increases number of potential customers within range and increases average speed.

DSL modems use several interfaces to connect to customer equipment, external Ethernet, external USB, and internal PCI card. Service offerings vary from static IP address (typical for SDSL) to DHCP dynamic IP address and PPPoE or PPPoA that emulates a dialup connection. DHCP and PPP are commonly used for residential service.

DSL is offered by 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). Deployment of DSL may require the coordination of three different entities. The ILEC owns the copper wire between DSLAM and customer. The ILEC, CLEC or DLEC rent the copper circuit and installs the DSLAM and backhaul facilities. The ISP services the customer and connects traffic to the Internet.

2.3.1 Impairments

DSL is an impressive engineering accomplishment that allows high-speed data to be carried by the 100 year-old copper telephone network. Unfortunately not all phone lines are suitable for DSL. Assuming the local central office (CO) or remote terminal (RT) is equipped for DSL it may not be available for a number of reasons. This section discusses common problems and where applicable suggests workarounds.

2.3.1.1 Distance

Typical ADSL maximum distance is 18,000 feet from the DSLAM. Conservative carriers often reduce this to 15,000 feet to minimize potential customer problems. Some ILECs are installing Remote Terminals (RT) to reduce cable distance allowing them to serve more customers. The distance between DSLAM and customer is often substantially longer than shortest driving distance.

2.3.1.2 Loop Carrier

Digital Loop Carrier (DLC), Digital Added Main Line (DAML) et al are techniques that allow multiple customers to share a single phone circuit. This reduces cost of providing phone service. Unfortunately most forms of multiplexing are incompatible with DSL unless designed to support remote DSLAMs. The presence of loop carrier may also limit dialup speed to 33.6 kbps or less. The Phone Company is only required to deliver phone service. If techniques used to deliver phone service interfere with other services the Telco is not obligated to address the situation.

2.3.1.3 Load Coils

Circuit resistance and impedance attenuate signals. This is more pronounced at high frequencies and long circuits. Load coils cancel some of these harmful effects resulting in better voice characteristics over long loops. They are typically installed on loops over 18,000 feet. H88 load coils, the most common type, are spaced every 6,000 feet beginning 3,000 feet from the central office.

Unfortunately load coils are incompatible with DSL. They are effective over the voice frequency range but severely attenuate the high frequencies used by DSL. If Load coils are present they must be removed to use the line for DSL.

2.3.1.4 Bridge Taps

When telephone feeder cable is installed it is not known how many circuits will be needed at each location. The solution is to run a large feeder cable past many customers. As customers order phone service the installer selects an unused cable pair and splices it to the drop cable. The circuit feeding the drop may continue for hundreds or thousands of feet. This creates a bridge tap. It is of no consequence for telephone service but degrades DSL. The DSL signal splits at the tap going down both paths. When it reaches the end of the tap it is reflected back into the line, creating interference. DSL is designed to tolerate some amount of bridge tap, but if circuit is marginal it may cause problems or push line over distance limit. SDSL providers typically pay the Telco to remove bridge taps during circuit install. This tends to be expensive and is not ordinarily done for low cost residential ADSL.

2.3.1.5 Noise and Crosstalk

Telco feeder cable carries many different services: POTS, ISDN and T-1. Phone circuits often closely parallel power lines picking up power line noise. Imperfections cause unintentional coupling from one circuit to another. This raises the noise floor. If noise becomes excessive speed is impacted.

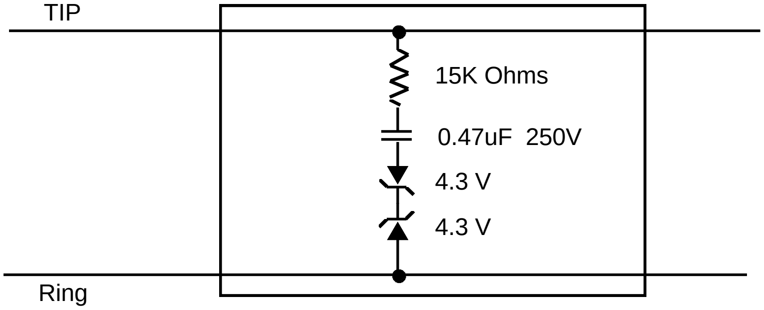
DSL is not typically warranted for minimum speed. It is a best effort service. If you hear noise on your phone you are much more likely to get the Telco to fix the problem than if it only affects DSL or dialup.

2.3.1.6 Half Ringer

Excerpt from DSL 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.



During SDSL installation the Half-Ringer is removed. The Half-Ringer may interfere with ADSL if the signal is marginal. In that case the solution is to install a POTS/DSL splitter. The splitter includes a Half-Ringer behind the low pass POTS filter allowing the one in the NID to be removed.

2.3.1.7 Inside Wiring

DSL was designed to tolerate wiring imperfections. The easiest way to test the quality of inside wiring is to connect the DSL modem directly to the Telco NID test jack. The test jack disconnects inside wiring. If performance improves inside wiring is degrading DSL. A POTS/DSL splitter eliminates the effects of inside wiring and telephone equipment on DSL.

2.3.1.8 Wireless Phones

Wireless phones may interfere with DSL. The RF used by the phones does not overlap DSL however wireless phones tend to inject noise into the phone line. Disconnect all phones and reconnect them one at a time. Sometimes adding an additional microfilter at the offending phone will solve the problem.

2.4 Data Over Cable Service Interface Specification (DOCSIS)

The Cable TV (CATV) industry is aggressively rolling out high-speed Internet service. Historically Cable TV was a one-way medium. TV signals originate at the CATV office, called the Head End (HE), and are broadcast to all subscribers. To accommodate new services the Industry replaced previous generation all coaxial network with Hybrid Fiber Coax (HFC). Fiber is deployed deep into the CATV network. Redundant fiber loops interconnect the Head End to hubs. The hubs in turn connect to local nodes that convert fiber to coax. Coax is only used for a short distance connecting individual subscribers to the HFC network.

Internet access requires two-way transmission, subscribers need to transmit as well as receive. A TV channel (6 MHz wide in the US) is reserved for data service toward the subscribers. The upstream path is more challenging. Distribution amplifiers must be replaced with ones capable of amplifying signals in both directions. The Head End recovers these signals and routes them to Internet exchange carriers.

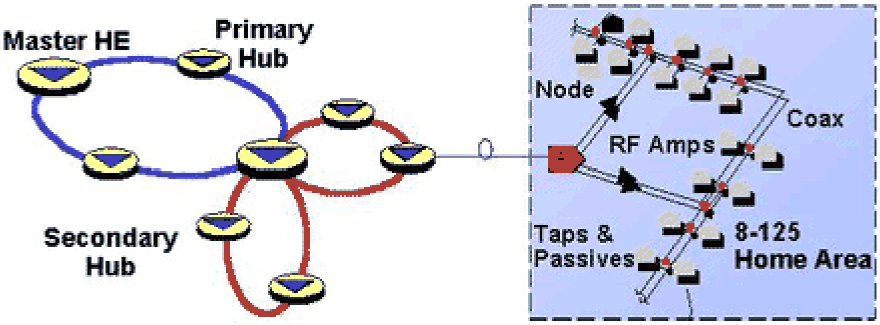


Figure 3 CATV Hybrid Fiber Coax Network

Some early Internet Cable systems were unidirectional. The Cable network was used for downstream transmission and a dialup modem for upstream. This allowed the CATV provider to offer high-speed Internet service without the need to upgrade the cable facility to bi-directional data.

The CATV industry is working to standardize cable modems so they can be purchased retail like dialup modems. The industry is rapidly migrating to DOCSIS Data-Over-Cable Interface Specification created by Cable Labs. DOCSIS 1 deliver per segment bandwidth of up to 40 Mbps toward the customer and 10 Mbps upload. DOCSIS 2 increases upload to about 30 Mbps. This is the total data rate for a particular Cable segment. Individual subscribers are capped at a lower rate to prevent heavy use from degrading service. Typical CATV service offerings are 1-5 Mbps down (toward the customer) with sub megabit rate up.

2.4.1 Impairments

As with DSL high speed Cable Internet access has to overcome a number of challenges to deliver acceptable end user experience.

2.4.1.1 Shared Medium

Cable is a shared medium. Each user competes with others on the same segment. While all Internet access is shared at some point Cable is shared in the first-mile. As more customers subscribe the Cable supplier must reduce the number of subscribers serviced by the segment to deliver acceptable service.

2.4.1.2 Limited Upload

DOCSIS 2 improved upload speed. Cable uses a time slot mechanism, called Time Division Multiplexing, to facilitate equitable upload over the shared cable segment. The Cable industry assumed customers would primarily use download bandwidth. Customers are taking advantage of Internet peer-to-peer capabilities to create and host their own data. This creates a strain on limited Cable upload capability. The Cable industry is waging an aggressive campaign against customers that use a lot of bandwidth. They have taken to calling these customers Bandwidth Hogs.

2.4.1.3 Noise

The frequencies used by the CATV network overlap those used by broadcast services. If these signals penetrate the Cable network they create interference. Keeping these signals out is especially difficult in the 5-42 MHz range used for upstream Internet communication.

2.4.1.4 Privacy

Cable Internet is a shared medium. It is relatively easy for customers eavesdrop on segment traffic.

2.5 Other High Speed Service

Other technologies are capable of delivering high speed Internet. So far they represent a tiny fraction of the broadband market. A significant benefit of most alternatives is they do not require expensive rights-of-way. This dramatically reduces upfront cost to roll out high-speed service.

2.5.1 Satellite

Direct Broadcast Satellite TV is capable of delivering high-speed service. Unfortunately the great distance of geosynchronous orbit adds significant latency making this type of service more appropriate for file transfer than interactive browsing.

Unfortunately Internet service planned for Low Earth Orbit (LEO) satellite has not turned out to be cost effective.

2.5.2 Fixed Wireless

Point-to-Point wireless service uses directional RF transceivers with line of sight connection between ISP and customer. In some cases customer's equipment act as a repeater expanding service footprint. Fixed wireless transceivers operate in both licensed and unlicensed bands.

IEEE 802.11 WiFi Wireless LANs are being deployed in ingenious ways to create radio hot spots that work much as the cellular telephone network. This allows wireless users to roam between multiple WiFi Access Points. Each Access Point has its own means to connect to the Internet.

2.5.3 Cellular Wireless

Cellular carriers invested heavily in 2.5 and 3rd Generation wireless service. Speed has improved but cost remains high. The most popular use of Cellular services continues to be voice and in Europe Short Message Service (SMS). Interest in using mobile devices for Internet browsing or multimedia downloading has not materialized. Looks like optimum use of cellular network is person to person communication.

2.5.4 Integrated Service Digital Network (ISDN)

Basic rate ISDN provides two 64 kbps bearer channels (B channels), and a 16 kbps data control channel (D channel). ISDN is a circuit switched technology with very fast call setup time. Being digital the full 64 kbps is available for data. Multilink combines both channels into a single 128 kbps symmetric connection. The lower speed of ISDN, compared to T-1, increases distance between repeaters to 18,0000 feet, rather than 6,000 feet for T-1. Primary Rate ISDN is basically a T-1 connection.

ISDN was touted as the next big thing by the telephone industry in the 1990s. However deployments missteps and high cost have slowed deployment. ISDN is viable where other forms of high-speed access are not yet unavailable but the window of opportunity for ISDN is passed.

A variation of ISDN, called IDSL, uses ISDN signaling to deliver 128 or 144 kbps data service at greater distance than DSL.

2.5.5 Fiber to the Home (FTTH)

The holy grail of broadband is a fiber optic connection to each customer, called fiber-to-the-home (FTTH). New residential developments are a prime candidate for fiber converged service delivering: broadcast television, telephone service, and high speed Internet access over a single infrastructure. In new developments fiber is cost effective today.

Some municipalities frustrated by the slow roll out of high-speed service are installing their own fiber and renting it to for profit companies that light it and connect customers. Creative solutions make use of nontraditional rights of way such as installing fiber in sewer mains or abandoned water and gas pipes.

2.6 When “Always On” Doesn’t Mean “Always On”

Broadband service is marketed as “always on.” Exactly what this means is subject to interpretation. The most “on” service consists of a bridged or routed connection with a static IP address. Once the service is configured the connection is permanent and always available.

Dynamic Host Configuration Protocol (DHCP) assigns the client IP address for a limited period called a lease. Before the lease expires the client attempts to renew it. DHCP simplifies the task of managing customer addresses. From the customer’s perspective the service is always on, lease renewal is transparent. Some ISPs bind IP address allocation to hardware MAC address. This results in the same address being assigned as long as the customer does not change equipment.

Point-to-Point-Protocol over Ethernet (PPPoE) or ATM (PPPoA) simulates a dialup connection. This type of service is common for ADSL. It leverages ISP investment in RADIUS authentication and billing. After the customer is authenticated they are issued an IP address. If the connection becomes idle the user is disconnected. This allows more customers to be serviced from a given pool of IP addresses. Various methods of generating keep-alive transactions can be used to simulate an always-on connection. Unlike dialup DSL allows 24/7 connection.

2.7 Acceptable Use Policy

ISP controls how the service is used. For example, retail customers are typically prohibited from reselling the service. Some ISPs prohibit use of networks, running servers, and block certain types of traffic. In an attempt to reduce cost some broadband services have imposed usage caps to limit the amount of data that can be transferred. Make sure the ISP does not prohibit using the service in ways that are important to you. Most ISP’s reserve the right to revise policy at any time making for a pretty one-sided contract.

2.8 Privacy Policy

Privacy policy determines how your information is used and protected. It is reasonable for the ISP to collect and use information for diagnostic purposes and to improve service. However, some ISPs sell customer information. 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. That information is potentially marketable. Governments, especially in Europe, are pressuring ISPs to retain customer usage information and make it available to law enforcement.

2.9 Service Level Agreement

Business class service includes a service level agreement (SLA). This defines things like: minimum speed, maximum latency, service reliability and mean time to repair. SLA guarantees are one of the reasons business class service is more expensive the best effort residential. Data communication is the lifeblood of most business. One needs to carefully consider the impact of communication failure.

2.10 E- mail

Consider ISP mail account a throwaway. Each ISP change results in a different email address making it difficult for folks to stay in touch. For a more permanent address use one of the free e-mail services or better yet register a domain name.

2.11 Finding an ISP

Check Find an ISP and Broadband Reports to find service providers. USENET news groups’ comp.dcom.xdsl and comp.dcom.modems.cable are a valuable technical resource. Some states Public Utilities Commissions (PUC) maintain broadband provider information.

3 Dialup Account – The Old Standby

Even though we have DSL we chose to maintain a dialup account. It is used as backup incase DSL fails and while traveling. In our experience the most common cause of DSL failures are internal ISP problems not the DSL circuit itself. To minimize the chance of losing both primary and backup service we use different dialup and DSL providers. Having two of anything, including ISP accounts, is a very useful troubleshooting aid.

Requirements:

- Nationwide point of presence (POP) access numbers
- Unmetered service
- No busy signals
- Decent speed
- LAN not prohibited
- No port blocking
- No proprietary software
- 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 received a single monthly bill and a reasonable rate for Internet Access. Unfortunately the ISP 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 dialup ISP. They are a local dialup ISP that meets our requirements. They have been extremely responsive to e-mail and phone support issues over the years.

3.2 Thoughts on Dial Up

If the ISP requires special connection software make sure it is compatible with the rest of your network environment.

Cost Tip – make sure ISP has access numbers Points of Presence (POP) close enough so calls are unmetered. Failure to do so will result in a rude surprise when the phone bill arrives.

Windows Performance Tip - in dial up networking uncheck "Log on to Network." Most ISP's use RADIUS authentication, eliminating Windows network login speeds up ISP connection process.

Windows Performance Tip - Uncheck NetBEUI and IPX in dialup networking. TCP/IP is the only protocol required.

Security Tip - If the computer is directly connect to the dialup modem unbind file and print sharing from dialup. This prevents folks on the Internet from gaining access to shared files

4 DSL Account – Telco's Brave New World of Data

We had been desperately looking for high-speed Internet service, finally signed up for DSL in late 2000.

Broadband wish list:

- Symmetric speed at least 500 kbps
- LAN not prohibited
- Reasonable price
- Single static IP address
- No port blocking
- No proprietary software
- USENET News account
- Good technical support
- Service Level Agreement

We were looking for near business class service. Outages of more than a few hours are very inconvenient for a consulting business. After hearing horror stories about DSL and Cable we wanted to deal with a stable carrier with a minimum of downtime. We did not want the ISP to perform firewall functions. We had run into problems in the past when the provider blocked outgoing mail. The goal was a transparent connection. We take responsibility for managing our security and network.

We are fortunate to have a wide verity of broadband services available at our location: Cable Internet, SDSL through a DLEC, ADSL through the ILEC, and both T-1 and fractional T-1 through several carriers. The Cable provider prohibits connecting the service to a LAN, eliminating them from contention. T-1 and Fractional T-1 is rather pricey so it was not in contention.

4.1 Distance Determination

Before applying for DSL we wanted to determine distance to the Telco Central Office (CO). The first step is to determine the location of the Central Office. Broadband Reports has a nice CO search utility and ESRI has an online tool that identifies likely cable route between the subscriber and Central Office. We drove several routes to estimate cable distance. Depending on route we estimated our distance between 10,000 and 14,200 feet.

4.2 Selecting a Provider

Our first attempt to get DSL was with Verizon. Our central office is equipped with Verizon ADSL 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. This was lucky because shortly thereafter they got out of the DSL business.

Vitts they indicated we were 10,500 feet from the CO. We signed up for HomeReach 530 service. This is 528 kbps SDSL business service with static IP address and a relaxed service level agreement (SLA). SDSL requires a dedicated line. Vitts coordinated the installation of new service with Verizon. Verizon removed about 1,000 feet of bridge tap and removed the half-ringer in the NID. The service was installed and worked flawlessly until Vitts declared bankruptcy and shutdown in May 2001 forcing us back to dialup.

Through Broadband Reports Verizon Forum learned of Verizon presidential appeals. Did not hold much chance of ever getting DSL but called anyway. A few hours later all lines were qualified and ranked. Ordered Verizon 1500/384 ADSL service in July 2001. Speed was better than Vitts SDSL but the service requires PPPoE and a dynamic rather than static address.

4.3 Splitter vs Microfilter

ADSL uses the same circuit as voice phone service. To reduce cost consumer grade ADSL use microfilters. This allows customer self-install eliminating the expense of a truck roll to dispatch a technician. All non-DSL devices must be behind a Microfilter.

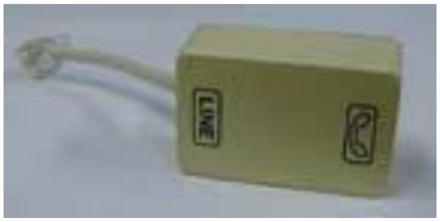


Figure 4 DSL Microfilter

An alternative to microfilters is a POTS/DSL splitter. This allows a single device to service the entire location. Splitters are especially valuable when used with a large number of devices or the service is far from the telephone central office. The splitter has better filter characteristics than microfilters and being installed at the NID isolates inside wiring from DSL. A good way to tell 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.

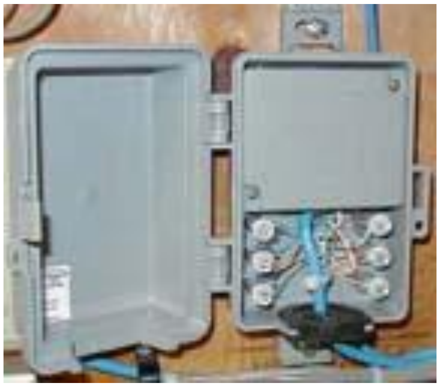


Figure 5 POTS/DSL Splitter

The splitter includes half-ringer test circuit on the phone side of the low pass filter. This allows the half-ringer in the NID to be disconnected reducing unnecessary load on DSL.

Splitter Advantage

- Single device for entire house
- Better electrical characteristics
- Isolates inside wiring from DSL
- Isolates half-ringer from DSL
- Works with home Alarm dialer

Splitter Disadvantage

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

4.4 Installation

Prior to activation date Verizon technicians connect the phone line to DSLAM and create a user account. In Ex Bell Atlantic territory Verizon uses PPPoE. This is very similar to PPP used with dialup modems. PPPoE requires a login to establish the connection. Verizon PPPoE self-install kit includes microfilters, a Westell Ethernet modem and install CD.

When everything is up and running Verizon sends out a welcome email. At that point the modem can be connected. The Westell modem has four indicators, Power, Ready, Link, and Activity. Power is on when the unit is powered up. Ready illuminates after the modem completed is internal self-test. Link is on when the modem is synchronized to the DSLAM. The Activity indicator flashes as data moves over the Ethernet connection. The Link indicator only shows the modem is synchronized to the DSLAM; it does not indicate a complete connection to the Internet exists. This is a source of some confusion.

Figure 6 Westell ADSL Modem

Once the connection is ready the account must be activated using the Verizon install CD. This is required even if you intend to use a router. Verizon PPPoE account activation requires MS PPTP VPN, a customized Netscape browser and WinPoet PPPoE client. I did not intend to use WinPoet as I have a router. I loaded the Verizon install CD on a spare PC. Install was uneventful. Once the connection was up and running transferred settings to Multitech router. It logged in without a hitch.

4.5 Optimization

There are many urban myths about magical tweaks to improve performance. Most of them are snake oil. System tuning is rather difficult because measurements are hard to duplicate since so many effects are outside your direct control.

TCP requires the receiver to periodically send an Acknowledge to let the sender know everything is OK. This is called the receive window. If the transmitter has not received an acknowledgement after it sends a number of packets it stops transmitting and waits. At high speed or if latency is significant the default receive window (RWIN) should to be increased to prevent pauses in transmission.

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

A suite of optimization tools is available at Broadband Reports Tools. Once you know the optimum settings download the DrTCP utility to make the recommended changes.

WinPoet PPPoE has a reputation for being buggy. Windows XP includes a PPPoE client, eliminating the need for third party software. RASPPPoE is available as an alternative to WinPoet. Using a router eliminates the need to run PPPoE at all; the router manages the DSL connection.

4.6 Thoughts on DSL

ADSL has been very reliable with only a few short outages. None of the outages have been problems with the DSL connection itself; the modem has never lost sync. All outages have been ISP routing errors or DNS failures. Verizon was not able to meet all conditions on my wish list but overall I’m very pleased with the service.

DSL wish list and as delivered:

- Symmetric speed at least 500 kbps – **1500/384**
- LAN not prohibited - **OK**
- Reasonable price - **Half the price of previous SDSL service**
- Single static IP address - **Dynamic address via PPPoE**
- No port blocking - **Port 80 blocked, prohibition against running commercial server**
- No proprietary software - **Install only - PPPoE is not proprietary**
- USENET News account – **Good speed and retention**
- Good technical support – **Phone support is mediocre, newsgroup support is excellent**
- Service Level Agreement **- Best effort only**

Security Tip - If the computer is directly connect to the DSL modem unbind file and print sharing from DSL. This prevents folks on the Internet from gaining access to shared files.

5 Wiring Techniques – Cables and Connectors

Many improvements in wiring techniques have been developed by the Telephone industry to deal with the massive number of circuits they install and manage. Of particular significance for our purposes are modular jacks and type 66 and 110 punch down blocks.

Modular jacks were developed by the old Bell Telephone System to reduce cost of installing and maintaining customer equipment. Until the 1970s phones were hardwired. This required a craftsperson to come on site for even the simplest task. Deployment of modular jacks meant that in many cases the customer could now repair, move, or install their own equipment.

About the same time as modular jacks became popular Type 66 punchdown termination was introduced. It is called punchdown because the conductor is terminated with a spring-loaded tool that pushes it into an insulation displacement contact and automatically cuts it to length. 66 style blocks are still widely used for phone systems. LAN wiring uses a second-generation type 110. This allows more circuits to be terminated in a given area. Due to its smaller size 110 provides better high frequency performance than type 66.

Prior to Telecommunication Industry Association EIA/TIA 568 Commercial Building Telecommunications Cabling Standard and EIA/TIA 570 Residential Telecommunication Cabling Standard wiring requirements were developed by various industries or in many cases individual equipment vendors. TIA recognized cable infrastructure has a long life expectancy, typically being used with multiple generations of equipment. They devised a performance based wiring scheme independent of how the wiring was used. This was a breakthrough; almost all communication systems now use structured wiring. TIA Structured wiring centralizes cable termination in a wiring closet. From there dedicated runs fan out to each receptacle. In the wiring closet and at the receptacle a patch cord connects structured wiring to electronic equipment.

When the US telephone network was deregulated the FCC took over responsibility for end user equipment and inside wiring standards, commonly called Customer Premise Equipment (CPE). Phone company practice for the previous 100 years had been to wire phone jacks as a daisy chain. Outside wiring, called the customer drop, terminated at a lightning protector. Inside wire originated at the protector and ran 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 mandated telephone inside wiring be installed using structured wiring techniques compliant with TIA standards. Adoption of TIA structured wiring means the same wiring method is used for voice and data networks.

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.

5.1 Structured Wiring

The key to EIA/TIA 568 & 570 is the notion of structured wiring. A cable from each receptacle runs directly to a central wiring closet. The cable cannot be spliced or connected to other outlets. At the wiring closet each cable is terminated at a patch panel. To provide service a short cable, called a patch cable, is connected between the appropriate patch panel jack and the equipment used to service the room receptacle.

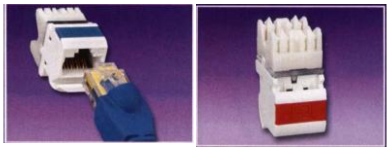


Figure 7 Cat 5 Receptacles

Structured wiring can be unshielded twisted pair (UTP), shielded twisted pair and fiber optic. UTP is the overwhelming choice for home and commercial networks.

UTP cable is rated by Category; higher numeric designation indicates greater bandwidth. TIA created Category 3, 4, 5, 5e and 6. Only Category 5e and 6 are currently recognized, other ratings are obsolete.

Cat 5e allows a single wiring scheme to support Ethernet (10 Mbps), Fast Ethernet (100 Mbps), and Gigabit Ethernet (1000 Mbps) as well as ordinary phone service. When Gigabit Ethernet was being developed it was designed to operate over the installed base of Cat 5. However, real world experience showed that not all installations were up to the task, hence the minor revision to Cat 5e.

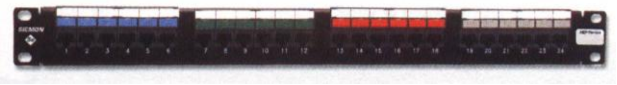


Figure 8 Cat 5 Patch Panel

TIA recently released specifications for Cat 6. Cat 6 doubles performance from 100 MHz for Cat 5e to 200 MHz. Currently no Ethernet version takes advantage of the extra bandwidth provided by Cat 6.

The various UTP category grades are outwardly similar. The differences are in the number of twists per inch and mechanical tolerances. The higher the Category rating the more tightly the pairs are twisted and mechanical specifications are held to tighter tolerances. It is important not to mix components of different Category grades, doing so reduces overall rating to the lowest grade used.

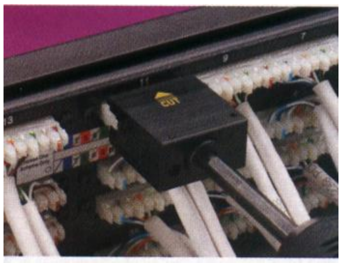


Figure 9 Rear view w/Punchdown Tool

UTP cabling is designed for a maximum end-to-end distance of 100 meters (328 ft). This distance includes a patch cord from device to wall jack, 90 meters of building wiring (in TIA parlance called horizontal wiring), and another patch cord in the wiring closet to connect facility cabling to active electronics.

Receptacles use type 110 terminations. This allows the cable to be quickly terminated with a punch down tool. In the wiring closet each cable is terminated at a patch panel. The patch panel consists of multiple jacks that terminate 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.

5.2 UTP Cable Types

The most common type of UTP Category cable is PVC insulated. It can be used in most habitable spaces.

Where cable is installed in air handling space such as under a raised floor or within a suspended ceiling it must be Plenum rated. Plenum cable is insulated with Teflon rather than PVC. Teflon is fire resistant not fire proof. The goal of Plenum cable is to delay the onset of combustion until the fire is so advanced to make the space incompatible with life.

Outdoor wiring is subject to UV radiation and moisture. Outdoor cable is gel filled to prevent moisture intrusion and has a UV resistant outer jacket, typically black. Direct burial cable includes a corrugated metal rodent shield to protect against burrowing animals.

5.3 Modular Connectors

When the old Bell system moved to connectorized customer premise equipment (CPE) it created a family of modular connectors. Modular connectors come in 4, 6 and 8 position versions. A center locking key prevents the plug from being accidentally ejected from the receptacle.

As the US telephone industry was migrating to modular connectors it was also the early stage of divesture and interconnect requirements. Customers were allowed to attach their own equipment to the telephone network. This required the creation of many tariff offerings that define various interconnect arrangements. Each tariff not only defined the type of jack, but whether it is flush or surface mount and how it is connected to the telephone network. This led to the creation of dozens of Registered Jack (RJ) designations, most of which are only of historical interest today. The RJ nomenclature has passed into popular usage and is only loosely coupled to its original intent.

The 4-position connector is used to connect telephone handset to phone. It was not assigned a RJ designation and need not concern us here.

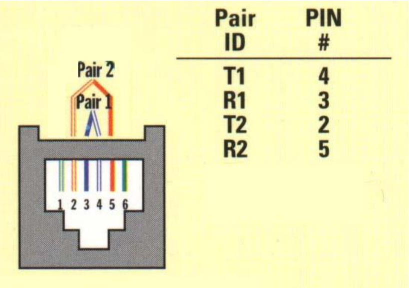
The most popular 6-position jack is referred to as RJ11. It connects single line voice grade telephone equipment to the public switched telephone network (PSTN). A two-line version using the 6-position jack is the RJ14.

8-position RJ31 and RJ38 jacks connect alarm systems to the PSTN. The 8-position RJ48 jack is used to connect to T-1 carrier.

TIA choose the 8-position jack for structured wiring. This jack is often erroneously called RJ45. The USOC RJ45 connects analog data equipment to the PSTN. A resistor in the Jack was used to set acceptable transmit power level.

5.3.1 Telco Uniform Service Ordering Code (USOC) Pinnout

The RJ designation is used to order the particular interconnect arrangement. This is called the Uniform Service Ordering Code (USOC).



Pair ID	PIN #
T1	4
R1	3
T2	2
R2	5

Figure 10 RJ11 and RJ14

RJ11 6-position jack connects a single-line phone to telephone network. RJ14 is used with two-line phone.

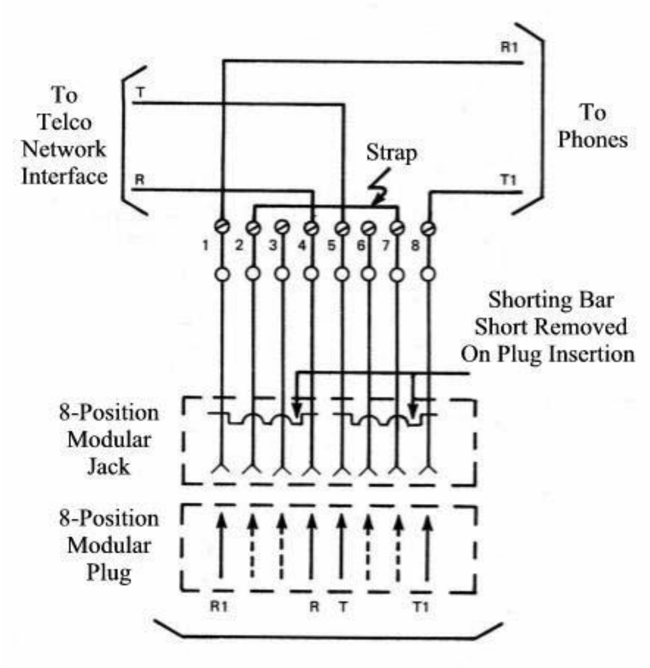


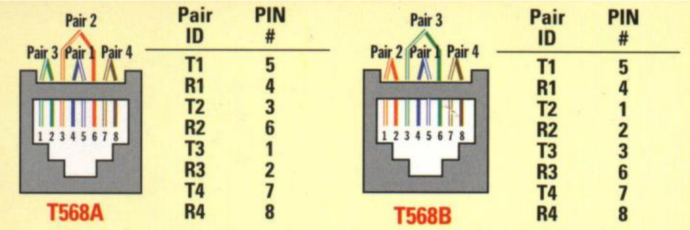
Figure 11 RJ31 and RJ38

RJ31 and RJ 38 are 8-position jacks used with alarm dialers. The jack is placed in series with the phone line close to the Telephone Company Network Interface Device (NID). All phones are wired downstream of the jack. Shorting bars within the jack establish continuity when the alarm is not plugged in. Plugging in the alarm opens the circuit placing it in series with CPE devices. When an alarm event occurs the dialer disconnects CPE devices so it is able to seize the line and dial out even if the line was in use. RJ38 is identical to RJ31 except it has a strap between positions 2 and 7. This allows the dialer to determine if it is plugged into the jack.

RJ48C and RJ48X are 8-position jacks used to terminate T-1 digital service. Receive pair use pins 1-2 transmit 4-5. RJ48X provides automatic loopback when plug is removed. Unlike other 8-position USOC jacks the pairing arrangement is compatible with TIA 568 so LAN patch cables can be used.

5.3.2 TIA T568A and T568B Structured Wiring Pinnout

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.



Pair ID	PIN #
T1	5
R1	4
T2	3
R2	6
T3	1
R3	2
T4	7
R4	8

Pair ID	PIN #
T1	5
R1	4
T2	1
R2	2
T3	3
R3	6
T4	7
R4	8

Figure 12 TIA UTP alternate pin outs

The pairing arrangement of TIA differs from that used on USOC voice jacks. The inner two pair are the same the outer two are different. TIA did this to improve high frequency transmission characteristics. It is important to use the correct type of patch cable. Use of 8-position USOC style patch cable in a Category rated network will cause problems.

The inner two-pair of the TIA-568 8-postion jack mate with inner two pair of the RJ11 and RJ14 USOC 6-position plug. This eliminates the need for adapters when connecting RJ11 and RJ14 equipment to structured cabling.

5.4 Wiring Color Code

Telco USOC RJ11 and RJ14 jacks use Red, Green, Yellow and Black conductors.

TIA Category rated cable consist of 8-conductors, arraigned as 4-pairs. Each pair is a different color, to identify conductors within a pair one wire is solid color the other has a White stripe.

Standard Telephone practice is Tip conductor is positive with respect to Ring. Early touchtone phones were polarity sensitive. Today most telephone equipment includes a diode bridge so polarity is unimportant. However it is considered good practice to maintain proper polarity. Low cost phone line testers are available to quickly determine polarity.

TIA Color Code	T568A Designation	Telco Color Code	Telco Designation
Blue/White	Pair 1	Green	Tip +
Blue	Pair 1	Red	Ring -
Orange/White	Pair 2	Black	Tip +
Orange	Pair 2	Yellow	Ring -
Green/White	Pair 3		Tip +
Green	Pair 3		Ring -
Brown/White	Pair 4		Tip +
Brown	Pair 4		Ring -

5.5 Type 66 Punchdown Block

The first type of insulation displacement terminal was the 66 block. These continue to be used extensively. An advantage of the 66 family is it accepts larger gauge wire than newer 110. Type 66 blocks are typically attached to a standoff bracket that is screwed to the wall. The bracket allows building wiring to be run underneath the block making for a neat installation.

Building wiring is terminated on one set of 66 blocks and equipment on another. Interconnect is accomplished with cross connect wire. This allows a great deal of flexibility in adding and changing equipment over time.

To save space split blocks can be used. In a split block each row of four terminals is divided in half. If needed a device called a bridging clip can be used to connect the left terminals to the right set. Use of bridging clips facilitates troubleshooting allowing circuits to be easily isolated.

To organize cross-connect wire a standoff called a Mushroom is used as a wire guide.

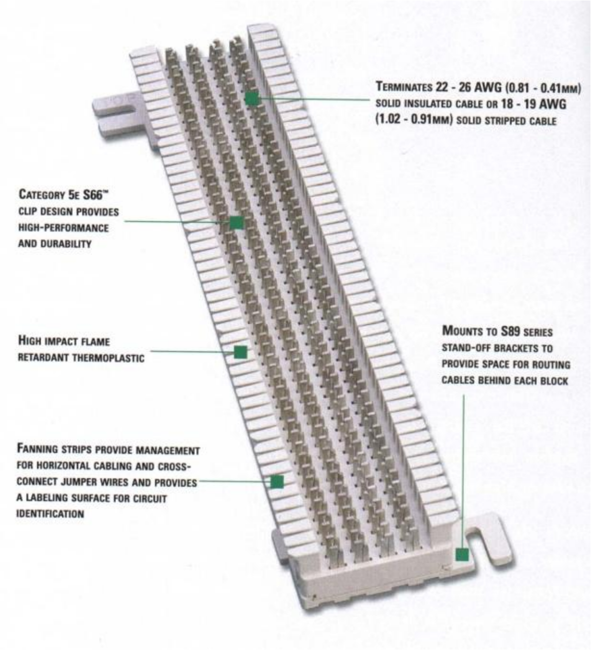

TERMINATES 22 - 26 AWG (0.81 - 0.41MM) SOLID INSULATED CABLE OR 18 - 19 AWG (1.02 - 0.91MM) SOLID STRIPPED CABLE
CATEGORY 5E S66™ CLIP DESIGN PROVIDES HIGH-PERFORMANCE AND DURABILITY
HIGH IMPACT FLAME RETARDANT THERMOPLASTIC
MOUNTS TO S89 SERIES STAND-OFF BRACKETS TO PROVIDE SPACE FOR ROUTING CABLES BEHIND EACH BLOCK
FANNING STRIPS PROVIDE MANAGEMENT FOR HORIZONTAL CABLING AND CROSS-CONNECT JUMPER WIRES AND PROVIDES A LABELING SURFACE FOR CIRCUIT IDENTIFICATION

Figure 13 Type 66 Punchdown Block

5.6 Type 110 Punchdown Block

Type 110 terminals allow higher density wiring than Type 66. 110 termination is preferred for LAN use. Typical 110 module includes a standoff. Building wiring is routed through the standoff and fanned out to the appropriate location. The 110 block is inserted over the base. Cross-connect wire is punched down to the upper terminals of the block.

The same Mushrooms used with Type 66 blocks are used as wire guides.

Cross-connect blocks are mainly used with telephone wiring. When a LAN is installed the cable from each drop is connected to patch panel consisting of a large number of modular jacks. Short cables, called patch cable, are used to connect the drop to network electronics. This results in better transmission characteristics than using punchdown termination.

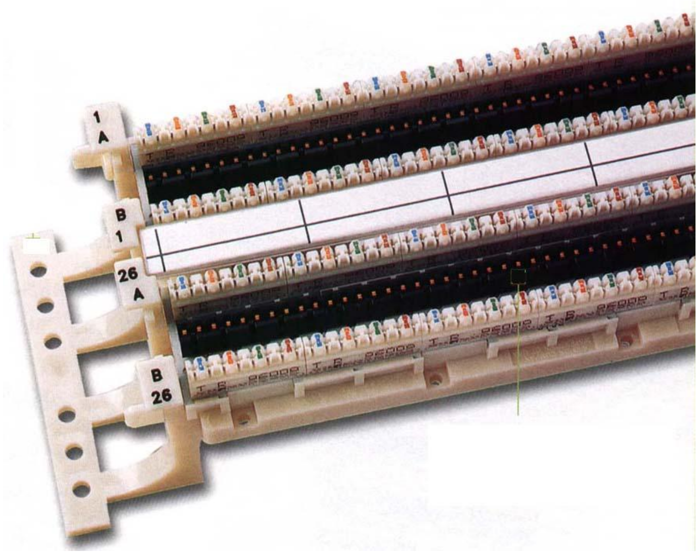
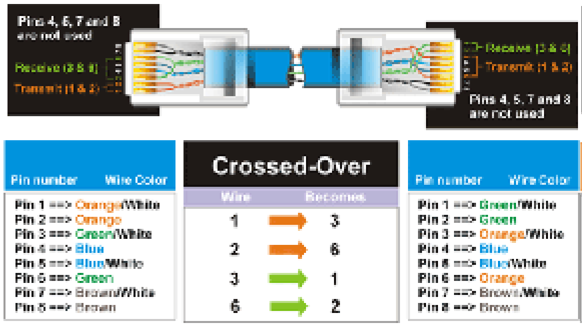


Figure 14 Type 110 Punchdown Block

5.7 Patch Cables

Patch cables connect equipment to wall jack, and patch panel to network electronics. The T568A and T568B pin out options can be ignored since both ends are preterminated by the manufacture.



Pins 4, 5, 7 and 8 are not used
Receive (3 & 6)
Transmit (1 & 2)
Receive (3 & 6)
Transmit (1 & 2)
Pins 4, 5, 7 and 8 are not used

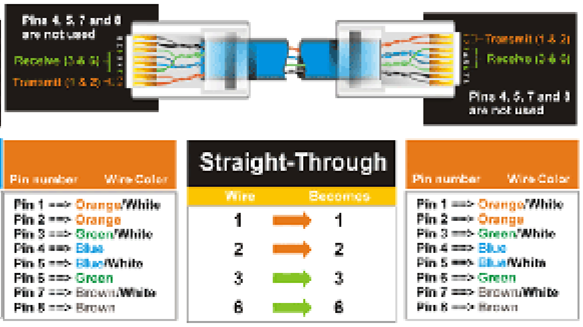
Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Crossed-Over

Wire	Becomes
1	3
2	6
3	1
6	2

Pin number	Wire Color
Pin 1 ==>	Green/White
Pin 2 ==>	Green
Pin 3 ==>	Orange/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Orange
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Figure 15 Crossover Patch Cable



Pins 4, 5, 7 and 8 are not used
Receive (3 & 6)
Transmit (1 & 2)
Transmit (1 & 2)
Receive (3 & 6)
Pins 4, 5, 7 and 8 are not used

Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Straight-Through

Wire	Becomes
1	1
2	2
3	3
6	6

Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Figure 16 Straight-through Patch Cable

Patch cables come in two versions, straight through and crossover. Straight through are used in most circumstances. UTP Ethernet uses a point-to-point wiring scheme. The transmit port of the computer connects to the receive port of the hub/switch and vice versa. If this arrangement cannot be used, for example two computers in direct connection or connecting a switch to another switch a crossover cable is required. Crossover cable swaps transmit and receive pair at one end so like devices can be interconnected. The function of Crossover cable is identical to using an Uplink port.

5.8 Tools

Proper tooling is essential to install a reliable network. Installation should be parametrically tested to insure compliance with TIA standards. Parametric testers cost several hundred dollars US making them rather expensive for a do-it-yourselfer. Testers verify each pair is properly terminated; the cable is not crushed or excessively untwisted. A common problem is called a split pair. Wires have end-to-end continuity but conductors of the pair are terminated to the wrong pins. This type of error may go unnoticed at 10 Mbps Ethernet but not for Fast or Gigabit Ethernet. If a tester is not available an ohmmeter can be used to at least verify continuity.

Tool	Purpose
Wire Cutters	Cut cable to length
Jacket Ripper	Removes outer cable jacket
Punchdown Tool	Terminate Punchdown terminals
110 Blade	Terminate 110 blocks
66 blade	Terminate 66 blocks
Crimper	Crimps wires into modular plug
Fish tape	Snake wire through walls
Phone Circuit Tester	Indicates polarity and loop current of phone circuit
Cable Tester	Verifies proper installation of Category rated wiring

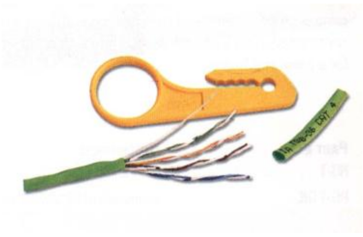


Figure 17 Jacket Ripper

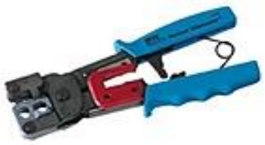


Figure 18 RJ11/45 Crimper

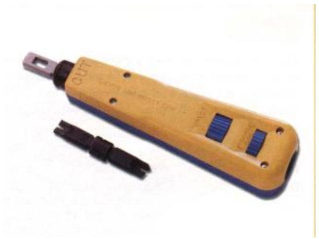


Figure 19 66/110 Punchdown

6 Telephone Network – Not Just Voice Anymore

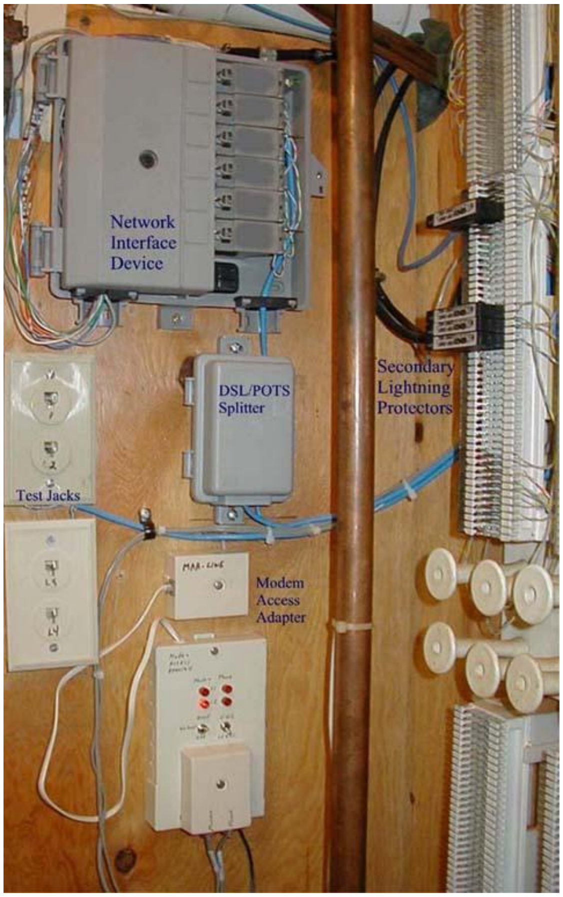


Figure 20 Telephone Wiring Closet

We have three phone lines two for personal use and a third 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 redirected to line 2. Hunting is unidirectional; if someone calls the second line and it is busy the CO 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. Line 2 is optioned with call waiting, so even if both lines are busy the caller does not get a busy signal. The goal was to treat the two personal lines as single main phone number; callers always use the main number. This works well for incoming calls, however outgoing calls are not as simple.

We wanted both lines to return Caller ID of the main phone number. Unfortunately that is not possible, caller ID is bound to each line. The choices for the second line are allow or block Caller ID. Blocking Caller ID hides the phone number from ordinary users, however some people refuse incoming calls with Caller ID blocked. If Caller ID is left on people will learn the second number and may use 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. 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 business use. Unfortunately our local CO 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.

A dedicated modem line seemed overly restrictive. However sharing a line between modem and phone poses a mutual interference problem. Picking up a phone dumps the Internet connection. On the other hand the modem has no way to know if the line is in use, it attempts to dial even if someone is on the phone. I looked for an off the shelf solution but could not find one. So I designed the Modem Access Adapter (MAA). This eliminated the need for a dedicated modem line.

> ***Modem Tip*** – Call waiting can be disabled at the beginning of a call for the duration of the call. The sequence varies by locale, in our area it is *70. Unfortunately sending the disable sequence to a line not equipped with call waiting 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.

6.1 Telco Network Interface Device (NID)

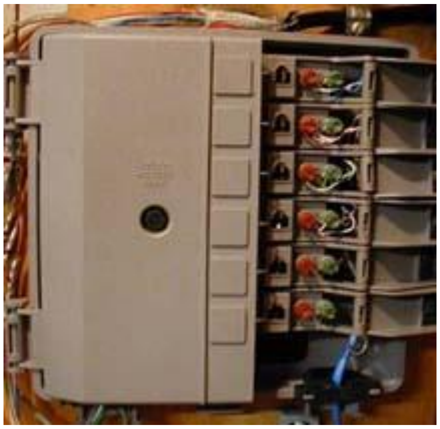


Figure 21 Telco NID

Back in the bad old days when the telephone phone company rented phones and installed inside wiring there was no provision for customers to install their own equipment, commonly called Customer Premise Equipment (CPE). With the advent of telecommunication deregulation the telephone companies were prohibited from being in the equipment business. This caused a dilemma because there is a need to demarcate between customer and Phone Company responsibility. From the demarcation point out is the responsibility of the Telco. Telco responsibility ends at the NID CPE terminals.

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 drop wiring, and provides lightning protection. The customer side has terminals to connect inside wiring and a test connector to quickly isolate inside wiring from the line. Some NIDs include a half-ringer test circuit. The half-ringer creates a unique signature that allows test equipment to determine if the fault is on the Telco or customer side.

Picture at upper 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 CPE wiring and a test jack for each line. Opening the cover exposes a RJ11 test jack. Plugging a phone into the test jack automatically disconnects inside wiring. If the test phone works the problem is with customer wiring or equipment, if not problem is with the Telco.

6.2 Secondary Lightning Protection

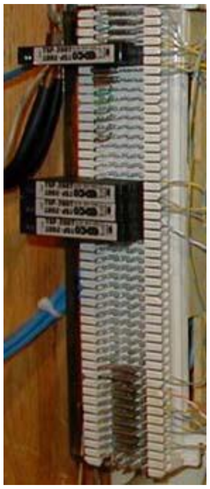


Figure 22 Lightning Protection

The local exchange carrier provides lighting protection as part of the Network Interface Device. Electronic devices are more fragile than 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 equipment damage. The best location for secondary protection is the building entry point. This allows the protector to use the same low impedance earth ground as the power mains minimizing voltage difference between services. Lightning protectors do not absorb energy they divert it. If the diversion path is not low impedance a substantial voltage difference is created. This is what kills electronic gear.

The EDCO TSP-200 series protectors add very little capacitance to the line. This is critical so protectors do not interfere with the high frequencies used by DSL. The protectors clip 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 power mains. When the protector fires fault current is shunted to ground.

One protector should be used on each telephone line. Additional protector should be used on any line that connects to outbuildings.

6.3 POTS/DSL Splitter

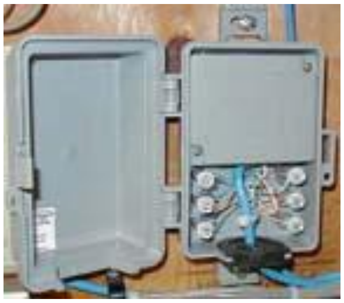


Figure 23 Splitter

Rather than using a microfilter at each non-DSL device I installed a POTS/DSL splitter.

When the business line exits the secondary protector it connects to a Corning/Siecor POTS/DSL splitter. The splitter includes a low pass filter that isolates voice from high frequency DSL signals. The splitter has two outputs; “Data” connected directly to the DSL modem and “Voice” connected to inside phone wiring.

The splitter contains a half-ringer circuit after the low pass POTS filter. This allowed the half-ringer in the NID to be removed, minimizing load on DSL.

> ***Home Alarm Tip*** – Splitter “Data” port delivers dial tone. If a phone is connected to the “DSL Data” jack it is able to make calls. This creates a potential safety hazard with a home alarm system. If a phone is connected to the data port and is in use when the alarm needs to seize the line it will not be able to do so. Care should be taken when using a splitter that only the DSL modem is connected to the “data” jack.

6.4 Modem Access Adapter

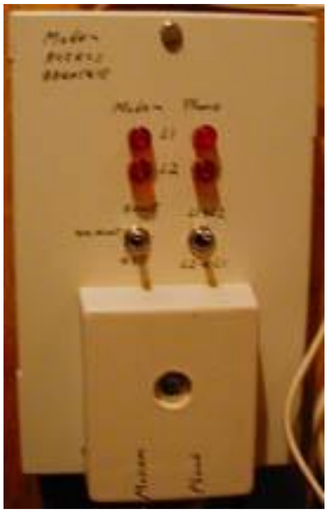


Figure 24 Modem Access Adapter

We wanted a way for the modem to have access to more than one line and to prevent mutual interference between modem and phones. This maximizes the chance of connecting to the dialup ISP while eliminating the need for a dedicated modem phone line.

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 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 is not connected and retries 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 lines are configured as a hunt group when the first line is busy the call is automatically routed to the second. If the personal line is busy the data call is placed on the business line. This is most likely to occur after normal business hours, when personal phone usage is heaviest.

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 searched first. LED indicators identify which phone lines are in use and which line is being used by the modem.

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. The NID, secondary lightning protection, POTS/DSL splitter, Modem Access Adapter, test jacks, test phone and Type 66 punch down blocks are located in the wiring closet.

From the NID each line goes to a secondary protector. POTS/DSL splitter is connected to the business line. Splitter “Data” output runs directly to the DSL modem. Splitter “Voice” and line 1 feed the Modem Access Adapter. Another dedicated line connects the Dialup modem to the MAA.

To make changes easier all building wiring is terminated on punch down blocks. Short twisted pair wire, called cross-connect wire, is used to interconnect the various circuits. 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.

A wall phone is permanently 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.

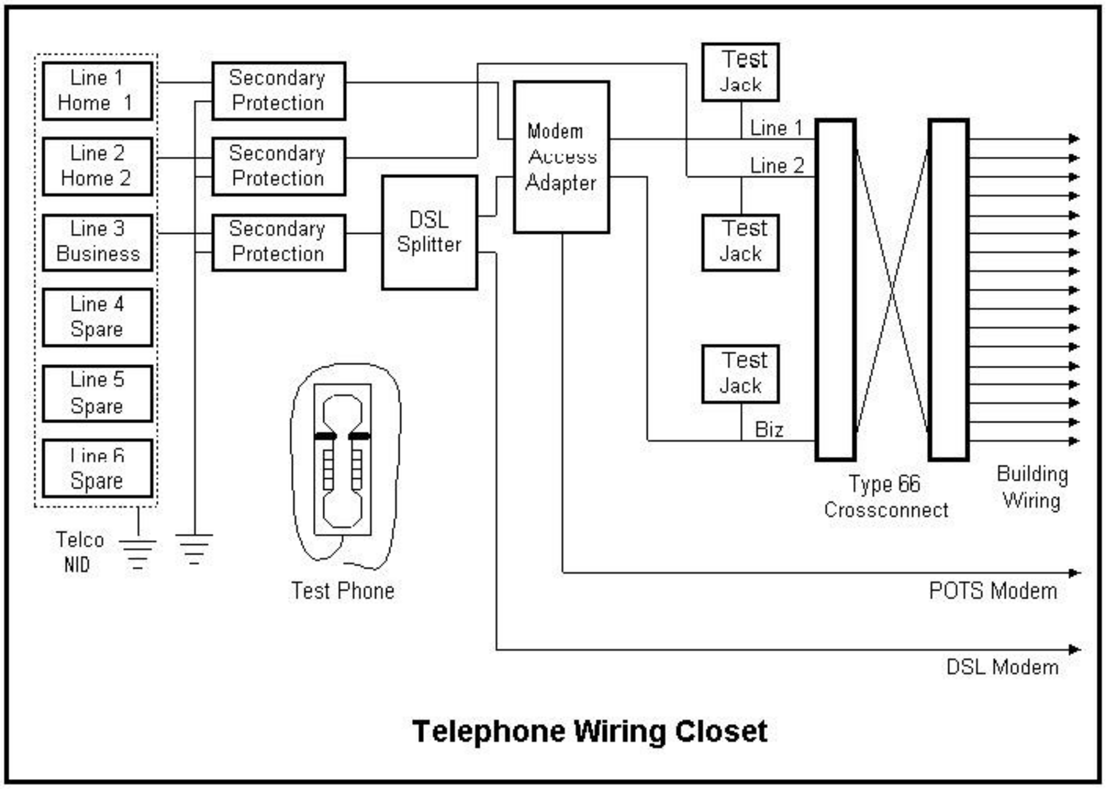


Figure 25 Telephone Wiring

7 Local Area Network (LAN) – Ethernet for Everyone

Local Area Network (LAN) allows computers to access shared resources such as printer, files, and the Internet. The preferred network is wired Ethernet running TCP/IP the same protocol as the Internet.

7.1 Ethernet

Ethernet IEEE 802.3 is the most common local network technology in use today. It is based on CDMA/CA (Collision Detection Multiple Access Collision Avoidance). Think of Ethernet as a telephone party line. Before speaking listen to see if anyone is talking. If no one is talking it is OK to start. It is possible 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 constraints to network design. Minimum packet size must be longer than the end-to-end propagation delay of the network. This insures the transmitter is still transmitting when the collision occurs allowing retries to be done at the data link layer. Power level and end-to-end loss budget must be set to allow reliable collision detection.

When Ethernet was originally developed it used fat coax cable with clamp on taps at prescribed intervals, called vampire taps. Today the most common type of Ethernet is unshielded twisted pair (UTP) copper cable consisting 8 conductors organized as 4 pairs terminated with 8 conductor modular jacks similar to those used for telephone wiring. This dramatically reduced the cost of Ethernet LANs.

7.1.1 10 – 100 – 1,000 – 10,000 Mbps

Initially UTP Ethernet operated at 10 million bits per second (10 Mbps) over Category 3 UTP wiring. Fast Ethernet increased speed to 100 Mbps over Category 5 wiring. Gigabit Ethernet is 10 times faster at 1,000 Mbps. During Gigabit Ethernet development the Cat5 specification was tightened resulting in Cat5e. The fastest version of Ethernet, 10 Gigabit (10,000 Mbps), only operates on fiber.

Most Ethernet devices include provisions for automatic speed sensing. This allows plug and play operation. Both sides of the connection negotiate optimum speed and selection of full or half duplex.

7.1.2 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, which 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.
>
> These addresses are physical station addresses, not multicast nor broadcast, so the second hex digit (reading from the left) will be even, not odd.

7.1.3 Hubs and Switches

Electrically UTP Ethernet is a point-to-point topology. Each Ethernet Interface must be connected to one and only one other Ethernet Interface. Hubs and Switches are used to regenerate Ethernet signals allowing devices to communicate with one another.

CDMA/CA scheme used by Ethernet places a limit on the number of wire segments and how many hubs can be used in a single collision domain. At 10 Mbps the 5-4-3 rule limits maximum of 5 wire segments with 4 hubs between devices, however only 3 of those hubs can have devices attached. For Fast Ethernet the rule is more stringent. A maximum of two Class II hubs, and the distance between hubs must be less than 5 meters. Class I hubs cannot connect directly to another hub. For all intents and purposes Fast Ethernet (100 Mbps) networks are limited to a single hub.

Ethernet switches do not simply repeat data on all ports eliminating the collision domain. The switch examines each incoming packet, reads the destination MAC address and passes it directly to the proper port. Switches allow multiple conversations to occur simultaneously as opposed to being limited to one with a hub. This allows total network bandwidth to be much greater than a hub. A 100 Mbps hub shares 100 Mbps among all devices. A switch segments traffic betweens pairs of ports. A non-blocking 16-port 100 Mbps Ethernet switch has a maximum throughput of 800 Mbps. This assumes 8 pairs of connections evenly divided between the 16 ports each one operating at full 100 Mbps. Port A is able to talk to port D at the same time Port F is talking to Port B. 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 100 Mbps switch to 1.6 Gbps as compared to 100 Mbps for a hub. In actual use the advantage will not be as great but switches offer a tremendous performance advantage compared to hubs.

When a switch does not know which port to use it floods the incoming packet to all ports, much like a hub. When the device responds the switch learns which port it is connected to and associates the MAC address with that port.

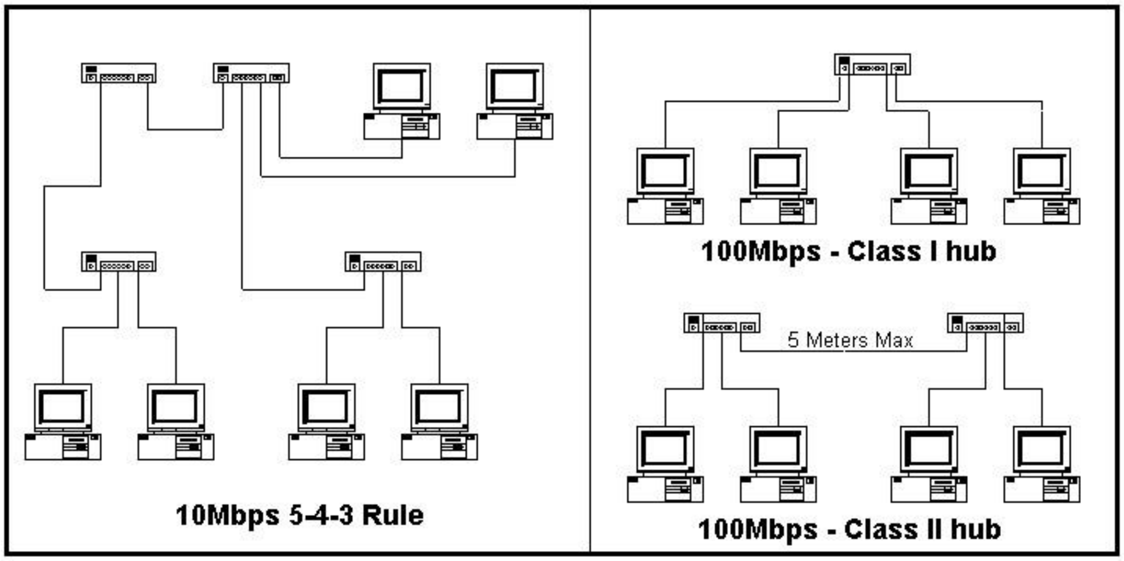


Figure 26 Ethernet and Fast Ethernet Hub Rules

<u>Performance Tip</u> – Gigabit Ethernet transfers 125 MBytes per second, 250 in full duplex mode. This speed exceeds available bandwidth of typical disk drives, PCI, and Card Bus. Desktop PCI delivers about 100 Mbytes per second. Getting optimum performance of Gigabit Ethernet requires high performance hardware/software.

7.1.4 Managed vs Unmanaged Hubs and Switches

Ethernet hubs and switches come in 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 typical home network. Unmanaged devices are considerably less expensive.

7.1.5 Preferred Topology

For maximum performance a single wide Ethernet switch should be used in the wiring closet serving the entire LAN. This maximizes total network bandwidth. Using a central switch allows either a hub or switch to be used in each room if additional drops are required. Ethernet switches used to be rather expensive, but prices have been dramatically reduced, making them 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 structure is being built. The situation is more difficult for existing homes. The cost and disruption to retrofit a LAN is a significant deterrent. Various “no new wire” initiatives minimize impediments to home networking. These initiatives operate at lower speed than wired Ethernet but have the advantage of not requiring installation of new wiring.

7.2.1 WiFi Ethernet Radio

Great strides have been made in creating high performance low cost radio LANs. For the foreseeable future RF technology is at its best where mobility is of paramount importance with bandwidth less so.

The first version of IEEE 802.11 delivered 2 Mbps in the 2.4 GHz ISM band. 802.11b increased data rate to 11 Mbps. Work is in process on 802.11g to increase data rate to 54 Mbps. 802.11a delivers 54 Mbps in the 5 GHz band. 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 wired Ethernet LAN. Depending on size and type of construction a site may require more than one Access Point. The WiFi trade association insures interoperability between different vendors.

7.2.2 Bluetooth

BlueTooth and IEEE802.15 address short-range (<10 meters) wireless personal area network (WPAN) market. The goal is to link multiple portable devices together. A higher power version extends range to 100 meters. BlueTooth operates at a raw data rate of 1 Mbps. Typical BlueTooth usage allows a PC, cell phone and, Palm Pilot to exchange data. BlueTooth devices form a piconet to communicate among a small group of devices. Piconets in turn can form scatternets to cover longer distance. Deployment of BlueTooth has been delayed due to technical issues. The first devices are just now reaching the market.

7.2.3 Phone Line Networking

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

Phone Line LAN uses slightly modified Ethernet packets. This makes HomePNA look like ordinary Ethernet 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.

7.2.4 Power line Networking

Much activity is directed at developing a high-speed power line network standard. X10 devices have been around for years but operate at painfully low data rates. The HomePlug Powerline Alliance has more detail on power line networking. The goal is to deliver megabit data rates over residential power lines.

7.3 Internet Terminology

Internet – Literally Inter network. The Internet is a network of networks.

IPv4 – Current version of the Internet protocol. A 32-bit address assigned to each host. The LAN uses a reserved block of private addresses that can be reused multiple times.

Subnet Mask – Binary mask used to define boundary between network and host portion of the addresses. Within a subnet hosts are directly accessible. Communication to a different subnet requires a router.

DHCP – Dynamic Host Configuration Protocol enables a server to automatically configure network hosts.

TCP - Transmission Control Protocol, TCP is responsible for reordering packets that arrive out of order and requesting retransmission of lost or corrupt packets. When an application creates a TCP/IP connection the receiver sees the same data stream as was transmitted.

UDP - User Datagram Protocol is a connectionless protocol; it is used when end-to-end synchronization is not required. The transmitting station casts 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.

URL - Uniform Resource Locator, human readable host name.

DNS - Domain Name System, translates friendly URL name to IP address.

Gateway – Another name for router used to forward packets between networks.

ICMP - Internet Control Message 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 may be assigned, statically, automatically by DHCP (Dynamic Host Configuration Protocol) or automatically by the client itself, AutoIP. Traditionally the system administrator manually configured each host with a static address. This was laborious and error prone. DHCP simplifies the task by centralizing address allocation responsibility. The down side is the need for a DHCP server. DHCP has been extended to allow automatic configuration if the host cannot find a DHCP server. In that case the device assigns itself an address from the AutoIP address pool. 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.

The current version of IP is 4. Each node is assigned a 32-bit address, resulting in a maximum Internet population of about 4 billion hosts. Due to scarcity of IPv4 addresses it is common practice for ISPs charge for additional addresses. Several techniques have been developed to minimize address consumption. This has been recognized as a serious limitation for some time and a new version, IP version 6, expands address space to 128 bits. This is a truly gigantic number. While IPv6 holds much promise it entails a wholesale 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. The subnet mask defines the boundary between the network and host portion of the address.

For our purposes all computers on the LAN must be on the same subnet. Our network uses subnet mask of 255.255.255.0 allowing up to 254 hosts (computers) also called a /24 subnet because the first 24-bits of the address are fixed. Host addresses are allocated from the last octet (8-bits). The reason for 254 rather than 256 hosts is the lowest address is reserved as the network address and the highest address for multicast.

7.4.3 Port Number

A computer is able to connect to multiple hosts simultaneously. This raises the question how does the computer know how to respond to incoming packets? For example, while writing this paper my mail program is checking e-mail, and I'm listening to a web based 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 a browser to access a World Wide Web site the browser automatically uses port 80. The low port numbers 0-1023 are called well-known port; they are assigned by IANA the Internet Assigned Number Authority when a service is defined. Software uses that port to make initial contact. Once the connection is established high numbered ports are used during the transfer.

7.4.4 Private Address Block

During work on the impending IPv4 address shortage RFC 1918 reserved three blocks of private addresses that are guaranteed not used on the Internet. Private addresses are ideal for our purposes. Devices are assigned an address from the RFC 1918 pool. This eliminates the need and expense to obtain a block of routable addresses from the ISP. To connect the LAN to the Internet the gateway router, or connection sharing software, uses a technique called Network Address Translation (NAT). NAT converts the private IP addresses on the LAN to the public address assigned by the ISP.

Excerpt from IETF RFC 1918 Address Allocation for Private Internets:

```
Internet Assigned Numbers Authority (IANA) 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.
```

7.4.5 AutoIP Address Block

The addressing techniques discussed so far require manual entry of an address or use of a DHCP server. In most situations this works well. But what happens in a simple environment when one just wants to connect a couple of PCs 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 a pool of reserved addresses.

When this happens the machine picks an address from the AutoIP address pool, and tests to see if it is already in use, if not it assigns itself the address. If the address is in use it picks another one and tries again. Refer to IETF Zero Configuration for more information.

AutoIP address block:

169.254.0.0 - 169.254.255.255 (169.254/16 prefix)

7.4.6 LocalHost Address

127.0.0.1 is the loopback address. This is useful for testing to makes sure the network interface is working correctly. Sending data to the loopback address causes it to be received without actually going out over the physical network.

7.4.7 Multicast Address Block

IP sessions are typically one to one, host A communicates with host B. It is also possible for a host to broadcast to multiple hosts. IANA reserved several address blocks for multicast.

Multicast address block

224.000.000.000 – 239.255.255.255 (224/8 – 239/8 prefix)

7.4.8 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 learn the MAC address associated with a particular IP address. Reverse ARP (RARP) determines if an IP address exists for a particular MAC address.

7.5 ISP Interface

The LAN can be bridged or routed to the ISP network. Most residential ISP accounts are limited to a single IP address; this requires either Proxy or NAT translation to convert addresses used on the LAN to the one issued by the ISP.

7.5.1 Bridged

A bridged connection is commonly used when the customer wishes to connect one or at most a few hosts. Most consumer accounts, Dialup, DSL, Cable are bridged. The ISP provides an IP address for every host. The customer's LAN becomes an extension of the ISP's network. This places customer hosts in direct connection to the Internet, and potentially other ISP customers, making implementation of access controls, such as a firewall difficult.

7.5.2 Routed

Large clients commonly use a routed connection. The ISP allocates a block of IP addresses large enough to accommodate all customer hosts. As packets arrive the ISP examines the network portion of the address.

Messages destined for the customer are passed to the customer's router. The router is responsible for packet delivery within the customer's network.

7.5.3 Proxy

Before NAT became popular it was common to use a proxy to isolate LAN from WAN. The proxy runs on the firewall and translates between inside and outside requests. The disadvantage is each application must to be configured to use the proxy. Proxies are also popular to eliminate the need to remap large networks when changing ISPs.

7.5.4 NAT

NAT, or more correctly Network Address and Port Translation (NAPT), is a popular solution for small businesses and individual users where the ISP issues a single IP address. NAT translates addresses used on the LAN to the address issued by the ISP.

7.6 Gateway

Each device on the LAN 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. Large networks quickly saturate with broadcast traffic. The solution is to use multiple smaller networks linked 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 examines the destination IP address and determines how best to deliver the packet. It may deliver it directly to the recipient or forward it to another router. Routers exchange route information among themselves to determine the optimum route. Each routing segment is called a hop.

Each host needs to know the address of its local router, also called a Gateway. When DHCP is used this address is set automatically. In our network router is the Gateway.

7.7 URL Naming Convention

URL names provide a friendly handle to access a resource rather than using IP addresses directly. 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, called registrars. The role of the registrar is to insure each registered 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.

Often an organization creates sub domains such as www.tschmidt.com for web access, mail.tschmidt.com for mail or product.tschmidt.com for product info. Since the domain name is registered and guaranteed to be unique the domain owner is free to add as many sub domains as desired.

7.7.1 Converting Host Name to IP Address

When a domain is registered the registrar database contains the name and address of the nameservers that provide authoritive information about the site. Authoritive nameservers are managed by the site administrator and contain all the information necessary to access the various servers within that domain.

When a Uniform Resource Locator (URL) is entered into the browser, such as http://www.google.com/, the browser first checks to see if this is a local host. Local Windows name resolution uses NetBIOS over IP. This is a broadcast mechanism and works well on small LANs but does not scale well for large networks.

Since the request is not a local host it is passed to the DNS system. The highest level is the root nameservers. The request goes to one of the root nameservers and returns the address of the nameserver for the .COM top-level domain (TLD) since Google is in the COM TLD. Then the COM nameserver is asked for the address of the Google nameserver. The server returns the address of the authoritive nameserver for the Google domain. The Google nameserver is then asked for the address of the desired host. The nameserver returns the address of the desired host. Often sites create sub domains for specific server, the process continues until the address of the desired host is determined. Once the browser has the IP address it is able to communicate with the desired host.

Obviously going thought this multistep process each time one needs to translate a URL is rather inefficient and time consuming. To speed up the process servers cache recently used information. DNS records indicate how long cached information may be used before it must be refreshed. Name lookup is normally accomplished in a few milliseconds.

7.8 Windows Network Neighborhood – My Network Places

Windows network neighborhood allows one to browse local shares. To show up in the neighborhood each machine must be running Microsoft file and print sharing service, even if nothing is being shared. The neighborhood is organized by workgroup, in a small LAN all machines typically belong to a single workgroup, such as HomeLAN. One machine in each workgroup is selected as the Browse Master. Ideally this machine is on all the time. Browse Mastership is negotiated at power up. Network neighborhood becomes unavailable when the Browse Master is turned off, until the remaining machines arbitrate Browse Mastership again. Getting the Neighborhood to work reliably can be a challenge, since so many components interact and sometimes involve large latencies.

7.8.1 8 -Step Program to Share Files in Network Neighborhood

#1 File and Print Sharing Service
Install Microsoft “File and Print sharing service” on each machine. Nothing need be shared but the service must be running for the machine to show up in the Neighborhood.

#2 Bindings
File and print sharing must be bound to a communication protocol. My recommendation is to use TCP/IP for everything. If you want to use NetBEUI for sharing go to Network setting for each adapter and unbind TCP/IP. By default Windows binds each adapter to all protocols.

> ***Security Tip*** - If system includes an interface connected directly to the Internet such as a dialup, Cable, or DSL modem unbind file and print sharing service from that interface. Failure to do so results in sharing system with millions of your best friends over the Internet.

#3 Workgroup name
Network neighborhood is organized by workgroup. You can have as many workgroups as desired. In a small LAN it makes sense to use a single name, such as HomeLAN, because each workgroup requires its own Browse Master.

#4 Browse Master
Browse Master should run from an always-on computer. This is the reason to use the same workgroup name, so only a single Browse Master is required. An election process determines browse Mastership. If you have a PC that is always on go to File and Print sharing properties. Change Browse Master from Automatic to Enabled. This forces the Browse Master to win the election.

If you don't have a machine that is always on it may take a few minutes for the neighborhood to appear after power up. The neighborhood will disappear for a while when the Browse Master is shutdown until lack of a Browse Master is noticed and a new election held.

#5 Login
If network logon (in network properties) is set to Client for Microsoft Networks a password must be entered at boot time for the Neighborhood to be accessible. If the password is bypassed most communication functions operate normally but the neighborhood becomes inaccessible. To eliminate the need to enter a password select Windows Logon. It may be necessary to delete any existing passwords. Search for *.pwd files and delete them.

#6 Enabling Shares
On a machine running file and print sharing service pick the subdirectory to share and check sharing. That directory and all subdirectories will be shared. In a peer-to-peer network shares can be password protected to control access.

> ***Security Tip*** - In general it is a good idea not to share files unless necessary. Some of the most damaging Viruses search for file shares and destroy them.

#7 User Account
Some versions of Windows need user or guest account to share files, this limits shares to authorized users.

#8 Firewall
If the system uses a software firewall be sure it does not block NetBIOS ports used to discover local host names and share files.

```
NetBIOS-ns       TCP/UDP Port 137 NETBIOS Name Service
NetBIOS-dgm      TCP/UDP Port 138 NETBIOS Datagram Service
NetBIOS-ssn      TCP/UDP Port 139 NETBIOS Session Service
```

Windows Configuration Tip – There appears to be a compatibility problem between Win2000 and Win98/ME network neighborhood. 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 for Win 2000 and Win98 machines. The laptop was put in a workgroup by itself and the laptop Browse Master enabled.

7.9 SOHO LAN Implementation

Cat 5 Network wiring was retrofit after the house was built. Most rooms are equipped with two Ethernet drops, the office with four. The location of the LAN wiring closet is different from that used for phone wiring. A SMC 16-port unmanaged 10/100BaseT hub connects all LAN drops. If this were a new installation Cat5e would be used with a 16 port switch. When purchasing a hub or switch get one with more ports than required, networks tend to grow.

I chose to reduce cost by terminating each horizontal LAN cable directly with a modular plug. Modular plugs are somewhat more difficult to install than receptacles so this is not for the faint of heart. By doing so I eliminated the cost and space of the patch panel and patch cable. If you chose this method be sure to specify the correct plug. Contacts used with solid (facility cabling) are different than those used with stranded (patch cords) conductors. Use of incorrect contact will result in intermittent terminations.

8 Broadband Router – One Address So Many Computers

When the LAN was originally set up we used Wingate proxy software running on a laptop sharing a dialup connection. At the time Wingate was the only connection sharing software that included a DHCP server. This was a convenient cost effective solution at the time. However we discovered several shortcomings with this approach.

Software Sharing Limitations:

- Each application must be configured to use the proxy. This makes moving a laptop between networks difficult. We tried an early version that incorporated NAT but had trouble getting it to operate properly.
- Streaming services do not work well behind a proxy.
- Connection-sharing software is effective protecting PCs on the LAN. However the PC directly connected to the Internet is vulnerable. If that machine is compromised the entire network is at risk. To protect the connection-sharing PC we used BlackIce software firewall. This tended to be fragile. Often installing the latest Microsoft patch broke the firewall.
- For optimum security the PC running sharing software should be dedicated to that task. This ties up a PC that could be used for other purposes.
- We were about to get a DSL account. We wanted to use DSL as the primary connection with dialup as backup when DSL was down.

When one factors in cost of using a PC to share the connection: always on PC, second NIC, connection sharing and firewall software a hardware router is very attractive.

Router Wish list:

- Ethernet WAN port for DSL or Cable
- RS232 Serial WAN port for dialup modem
- Automatic fallback to dialup modem if broadband fails
- NAT connection sharing
- 4 port 10/100 Ethernet LAN Switch
- DHCP server for local address allocation
- IPsec pass through for VPN
- Port mapping to run servers
- Event logging
- Good tech support

Figure 27 Multitech Broadband Router

We chose a MultiTech RF500S router. It meets our requirements and Multitech technical support has been outstanding. The router creates a clear distinction between "LAN" and "WAN" simplifying troubleshooting.

8.1 WAN Interface

Service providers offer several types of DSL modems: External Ethernet or USB and Internal PCI card. There are pros and cons to each. An external Ethernet modem is the most flexible because can connect directly to the PC or used with a router to create a LAN. Both Vitts SDSL and Verizon ADSL use external Ethernet modems.

The customer interface of both the Verizon Westell ADSL and Vitts Net-to-Net SDSL modem is 10 BaseT Ethernet. This connects directly to the Wide Area Network (WAN) port of the router. Vitts service was static IP address. This requires IP address, subnet mask, Gateway and DNS address be entered into the router manually. Verizon in Ex Bell Atlantic areas 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 PPPoE PC client. With Verizon PPPoE IP address, subnet mask, Gateway and DNS addresses are configured automatically each time the router logs in.

WAN settings are hidden from the LAN. Devices on the LAN use the router as Gateway and DNS server. The router forwards the request to the ISP provided addresses.

If the DSL connection becomes idle 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 other function of the keep alive is to determine if the router has a good Internet connection. It does this by periodically querying NIST timeservers.

8.2 Automatic Fail over

When a computer on the LAN requests Internet access the router verifies DSL is working. If DSL is unavailable the router automatically connects to dialup ISP. The router includes an idle timer to disconnect dialup modem after a period of inactivity. This prevents the modem from tying up the phone unnecessarily. The router constantly attempts to reestablish the broadband connection. When service is restored dialup session is terminated.

This feature turned out to be very useful. Router was set up before we had DSL. This allowed us to test and debug the LAN on dialup. When our SDSL provider went out of business we were forced to use dialup again full time. When the Verizon ADSL account was activated we simply plugged in the Westell modem and entered PPPoE account information into the router. Once again we were up and running on DSL without changing the LAN.

Setting up the fallback account is similar to using Windows dialup networking (DUN); it requires a Point of Presence (POP) phone number, user name, and password. With dialup PPP the WAN IP address, Gateway address and DNS address are configured automatically each time the router logs in. The router hides the difference between Dialup and DSL from devices on the LAN. Host settings do not change the only difference between Dialup and DSL is speed.

Both Vitts SDSL and Verizon ADSL have been reliable. All outages have been either DNS or ISP routing problems. We have never lost DSLAM sync. Outages typically last a few minutes on rare occasions up to several hours. The fact problems have been with the service provider’s internal network validates our choice to obtain dialup from a different vendor.

8.3 Multiple ISPs

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

> **Sending Mail -** One issue not addresses by the router is sending email. This is only an issue with POP/SMTP not web based mail. Mass mailers have exploited the lack of SMTP security to inundate users with unsolicited junk email called SPAM. SMTP mail server cheerfully accepts all mail sent to it. Spammers love this, all they need is an open SMTP mail server and they are in business. As a counter measure most ISP SMTP servers reject mail unless it originates from within their network. This restricts outgoing mail to users 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 with multiple accounts this restriction is a problem. See section **11.2.4 SMTP SPAM mitigation** for more details.
>
> Our domain hosting service uses SMTP authentication. Neither Verizon DSL nor our dialup ISP block port 25 used by SMTP this allows us to send mail though our SMTP server regardless of how we connect.
>
> **Usenet -** If the ISP auto authenticates, rather than require explicit authentication, use is prohibited if accessed through a different ISP. In some cases even if the server requires authentication access

is blocked. This is typically done to prevent customers from swamping binary news servers by using alternative high-speed connections.

8.4 LAN Address Assignment

Each device on the network requires a private IP address. These addresses are not used on the Internet therefore they do not have to be coordinated by IANA. However they must be coordinated within the LAN. The Multitech router has the flexibility to use static, dynamic or pseudo static addresses.

8.4.1 Static

The network administrator manually assigns address, subnet mask, gateway address, and DNS address to each machine. The router's DHCP server issues addresses in 192.168.2.2 - 192.168.2.100 range with a subnet mask of 255.255.255.0. Static addresses can be assigned in the range 192.168.2.101 – 192.168.2.254. This keeps all addresses in the same subnet without interfering with DHCP operation.

8.4.2 Dynamic

Default Windows TCP/IP configuration is dynamic address allocation. The DHCP server in the router assigns each machine an address. Once the device has an address it is able to use the LAN. The DHCP server assigns other critical numbers, subnet mask, gateway address and DNS address.

8.4.3 Pseudo Static

For some devices, such as servers, dynamic addresses are inconvenient. For example the binding to the HP print server is by IP address, it does not have a name. If the server's address changes each client has to be reconfigured. A solution is to create a pseudo static address. The address issued by the DHCP server is bound to the client's Ethernet MAC address. As long as the MAC address does not change the device receives the same IP address. This is more convenient than setting IP addresses manually and making sure they do not conflict with previously assigned addresses or the DHCP pool.

All machines on the LAN are issued pseudo static addresses. This makes it much easier to interpret SysLog entries that record events based on IP address.

8.5 Gateway

Hosts send packets that cannot be delivered locally to the router's gateway address. The router decides how to deliver packets that travel outside the LAN. Only a single connection exists between our network and the ISP so routing is trivial. The router simply forwards all packets to the gateway address assigned by the ISP.

8.6 DNS Nameserver

Local host name resolution is done within Windows using NetBIOS over IP. If Windows cannot resolve a host name it assumes it is a remote host and forwards the request to the router's DNS address. The router forwards the request to the DNS server specified by the ISP.

8.7 NAT -- Sharing a Single Public IP Address

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 address. Network Address Translation (NAT) provides a mechanism to translate addresses on one side to addresses used on the other. NAT allows multiple hosts to share a single IP address.

Internal LAN communication proceeds normally NAT is not required. When a request cannot be serviced locally it is passed to the NAT router, called the gateway. The router converts the private address to the public address issued by the ISP and in some cases modifies the port number to support multiple sessions. The router then sends the packet to the remote host as-if-it-originated-from-the-router. When the reply returns the router converts the address and port number back to that of the original device and forwards it to the LAN. The NAT router tracks individual sessions so multiple hosts are able to share a single address. As far as the Internet is concerned the entire LAN looks like a single computer.

NAT offers the advantage of a proxy server with the benefit of being transparent to most applications.

8.7.1 Limitations of NAT

As useful as NAT is it is also controversial. It breaks the end-to-end Internet addressing paradigm. NAT maintains state information 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 truly private and no one but the administrator cared about address usage. Today in the age of VPNs these internal addresses ARE being exposed to other networks. If a telecommuter’s LAN and office network both use private address the addresses may overlap. In a simple case this is not major problem, the user simply moves the LAN to a different private address block. But what happens if the home LAN must support multiple telecommuters. This requires the coordination of multiple corporate LANs and the SOHO LAN. In this case it may be impossible to resolve the conflict if corporate networks use identical address blocks.

NAT blocks all remotely originated traffic. It functions as a de facto firewall because it does not know how to route packets that originate outside the LAN. This is often touted as a security benefit but it causes problems running a server. Most NAT routers support port forwarding. This allows the user to specify which incoming packets are forwarded to servers on the LAN. Since only a single public IP address exists, incoming requests can only be mapped to a single device using a specific well-known port. For example the router can be configured to map all TCP port 80 requests to a web server. As far as the remote user is concerned they are accessing the server via the public address. A second server cannot use Port 80 since it has already been mapped. It is trivial to move the server to a different port, however unless remote users are informed of the non-standard usage they will be unable to connect.

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 IPv4 address shortage, not a permanent extension to Internet technology. For more information see RFC 2993 Architectural Implications of NAT.

8.8 Universal Plug and Play

Manually configuring port forwarding can be intimidating for novice users. UPnP allows devices on the LAN to request ports be opened on the NAT router. This is convenient but does pose a security risk since one has not way to know if the device requesting access is trustworthy.

8.9 10/100 Ethernet Switch

The office is wired with 4 Ethernet drops feed by a 16-port 10/100 hub. This turned out to be inadequate so the Router’s 4-port Ethernet switch came in handy. One port on the router is configured as an uplink port. This connects to the 16-port hub feeding the drops. The file server and office desktop connect to the switch taking advantage of switch bandwidth. Everything else goes through the hub. This increased the number of office ports to 6 eliminating the need to pull more wire.

8.10 Event Logging

The router logs all significant events and forwards them to the syslog server. This overcomes one of the main limitations using a dedicated device for Internet sharing – limited storage space.

9 Local Server – Just Like the Big Kids

The server delivers several network services: file sharing, Network Neighborhood browse master, real time clock synchronization, Syslog log server, private web server and weather station. At first we used a laptop as the server. This was convenient because it was self-contained but had limited disk storage capacity. It was replaced with a recycled 200Mz Pentium desktop with a 45GB hard drive. If storage requirements increase it has room for another disk.

9.1 KVM Switch

We did not want to add another set of user I/O when we setup the desktop 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 28 Belkin KVM

Switching between computers is done via a button on the KVM or a keyboard hot key sequence. The KVM creates virtual devices for each computer. When switching computers the KVM reconnects keyboard, mouse and monitor to the active computer and programs physical devices to match stored virtual device configuration.

> ***Video Performance Tip*** -- Workstations tend to use very high video resolution and faster refresh rate than servers. This results in very high video bandwidth. This is usually not a problem for the KVM itself but requires high quality cable. The video cable should use coax for the three video signals. Coax preserves high frequency and minimizes crosstalk between video signals. Failure to use high quality cable will result in poor video quality.
>
> ***Mouse Compatibility Tip*** -- Each computer is fooled 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 active computer. Mice cause problems because so many different enhancements exist. For compatibility PS/2 mice power up in two-button 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 known mouse. If the mouse answers correctly the driver switches it to enhanced mode. This causes problems for KVMs. Unless the KVM has a priori knowledge of the mouse it is unable to configure it properly. Depending on specifics this results in either loss of mouse control or the mouse reverting to default two-button mode.
>
> ***Mouse Compatibility Workaround Tip*** -- 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 thumb button is disabled. To get around this problem the workstation 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 is able to access devices directly. The KVM passes proprietary commands but it does not remember them. The server is connected to port 2 using the default Windows mouse driver. Switching to the server resets the mouse to Microsoft mouse mode. Use of the thumb button is lost but otherwise the mouse functions correctly. Switching back to the main system the mouse is 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 placed the Logitech control panel in 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.

9.2 File Sharing

One of the benefits of having a network is the ability to share files. This requires Windows file and print-sharing service be installed on each machine. The desired subdirectory enabled for sharing. Normally an entire drive is not shared but on occasion this is useful for removable media, such as a CD. Shares can be browsed in the Network Neighborhood or mapped as virtual drives. If they are mapped they are assigned a drive letter just like local drive. The user connects to a remote share as needed or Windows can connect automatically at boot time. In a peer-to-peer environment shares can be password protected to limit access.

We created a share for each user. The main purpose of the share is to backup desktop data on the server.

> ***Security Tip*** -- Some of the most dangerous viruses look for network shares. If they find a shared drive they attempt to delete files. Password protects any shares that contain valuable data.

9.3 Browse Master

Windows use a service called the Browse Master to collect and display machine names and active shares in the Network Neighborhood or My Network Places. Each workgroup requires a browse master. The server is the obvious place to run the browse master since loss of Browse Master causes the neighborhood to disappear. Browse Master in the server is set to enabled not automatic. This forces the server to win the election process.

9.4 Time Service

The US National Institute Standards and Test (NIST) maintains a number of public timeservers. This eliminates the problem of drifting and inaccurate computer clocks. NIST Network Time Service provides multiple stratum-1 timeservers located in: Gaithersburg Maryland, Boulder Colorado and Redmond Washington. We use Tardis 2000 running on the server and K9 on each client for clock synchronization. Tardis is configured with the address of multiple servers. If a server is not accessible Tardis automatically gets time information from the next available server. Timeservers are extremely accurate; however accessing them via the Internet adds potentially several hundred milliseconds of round trip delay. This error is not significant for our purpose and is ignored.

Tardis uses NIST time information to set the 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, running on each client updates the local RTC to synchronize it to the server. This insures all computers are slaved to the local server and the local server in turn is synchronized to NIST.

> ***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 uses the highest subnet address. Assuming a network prefix of 192.168.2/24 the broadcast address becomes 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 may annoy your ISP.

> ***Configuration Tip*** -- We set Tardis to contact NIST every 6 hours. For convenience the LAN broadcast occurs every 64 seconds so client clock is updated as soon as the machine boots. The 6-hour setting limits how often the dialup account is activated in the event broadband is down.

> ***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.

9.5 Log Server

RFC 3164 BSD Syslog protocol provides a standardized method for network devices to output status information to a log server. This creates a central repository for event storage and overcomes storage limitation of most network appliance. Currently the only device on the network originating Syslog entries is the router.

We use Kiwi shareware program for both Syslog server and Log file viewer.

9.6 Private Web Server

The home page of each PC points to a web server running on the server. This allows relevant information to be posted on the web server and shared over the LAN. The server consists of both static information and dynamic weather data. The server is freeware called Xitami from iMatrix.

> ***Security Tip*** -- 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 it.

9.7 Weather Station

Davis Instruments weather station data is posted on the internal web server. Davis software is configured to maintain historical data and create a GIF file of current inside temp, outside temp, wind chill, and wind speed every five minutes. The GIFs are posted to the local web server allowing anyone on the LAN to retrieve weather data.

10 Laptop – Internet Anywhere

We use a laptop at our home office, in the office and while traveling. This means it needs to connect to three different networks. For meeting we often set up an ad hoc isolated network to exchange files among the participants, resulting in a fourth environment. Network settings are sprinkled all over Windows and within various applications. This makes it hard to move a computer between locations.

Even though we minimized differences between locations we still wound up with several site-specific settings. The solution was a program called NetSwitcher to effect location specific changes. NetSwitcher works by modifying settings in the Windows Registry. It is able to change most network settings and to select the default printer. The table shows the various network settings we need. The ones controlled by NetSwitcher are highlighted in yellow.

	@Home	@Office	On the road	Ad Hoc Meeting
IP Address	DHCP	DHCP	Dialup PPP	Static
Interface	10/100 NIC	10/100 NIC	V.90 modem	10/100 NIC
Authentication	Windows Client	NT Domain	Windows Client	Windows Client
Office Shares	VPN	NT permissions	VPN	N/A
SOHO Shares	Peer-to-peer	N/A	N/A	N/A
Default Printer	Local network printer	Local network printer	Directly attached printer	Directly attached printer
Time	K9 client	N/A	N/A	N/A
Email receive	3 POP accounts	3 POP accounts	3 POP accounts	N/A
Email send	Tschmidt.com SMTP	Tschmidt.com SMTP	Tschmidt.com SMTP	N/A
Usenet	Dialup and DSL account	Dialup account	Dialup account	N/A
IE home page	Private web server	Biz home page	Dummy laptop home page	Dummy laptop home page

Netswitcher is able to control everything we needed except default browser home page. A FAQ on the NetSwitcher site describes how to create extensions using the registry editor, REGEDIT, to extract registry entries and to create NetSwitcher scripts. This works well to create custom controls. The only down side is that it is easy to get confused by the hack. If you decide to use the application to change configuration, the change goes into effect and all is well until next time you use NetSwitcher to change location. NetSwitcher overwrites the setting. After a little head scratching you remember what you did and all is well.

During Windows shut down the NetSwitcher dialog box pops up. This allows correct configuration to be selected for the next boot cycle.

11 Services – Making Life Worth Living

This section describes the various services running on the LAN.

11.1 Internet Browsing

All PCs use Microsoft Internet Explorer version 5.5 or 6.

Key to effective use of the Internet is being able to find what one is looking for. Our preferred search engine is Google. They have a nifty IE toolbar add-on. The toolbar allows Google queries be made directly from the toolbar.

11.2 E-Mail

E-mail accounts fall into three broad categories: advertising supported free accounts, ISP accounts and mail via your registered domain. ISPs typically provide email service. This is convenient but ties your e-mail address to current ISP. Change ISP and your e-mail address changes. Free mail services like Yahoo are advertising supported. They decouple your e-mail address from ISP. Free accounts make sense for personal use. For business purposes or to insure long lasting email identity nothing beats registering your own domain name. Once registered mail is addressed to you@yourdomain.TLD. If you change hosting service you simply transfer your domain registration to the new provider, e-mail is unaffected.

11.2.1 Browser Based Mail

The traditional way to access mail has been with a mail client, such as Microsoft Outlook. Most free mail services use a browser interface eliminating the need for a mail client. Web mail is convenient because mail is accessible from any browser equipped PC. The user interface is somewhat less convenient than a mail client but adequate for casual users.

11.2.2 Mail Client

Except for web-based mail, e-mail has a sending component, SMTP, and a receiving mailbox, POP. To send mail the mail client connects to an SMTP (Simple Mail Transport Protocol) mail gateway. The SMTP server acts as a relay between e-mail client and POP mail server. The SMTP server verifies each recipient is accessible and returns an error message if not. The SMTP server delivers mail to the appropriate POP server, (Post Office Protocol). It works much as a real post office mailbox. The POP server stores mail temporally. The e-mail program connects to the POP sever and downloads mail. Normally the mail client requests the server delete mail once it is transferred to the client but this can be overridden so mail remains on the server. This is convenient if you access mail from more than one machine.

11.2.3 Corporate Mail

Telecommuters need access to corporate mail accounts when out of the office. Depending on where the mail server is located this may be easy or difficult. If access is not restricted the user is able to log in like any other mail account. If the mail server is not publicly accessible the employee needs to connect using the corporate VPN.

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 connected all day long. A solution, if it is acceptable to your administrator, is to set up your corporate mail account to automatically forward incoming mail to one of your personal mail accounts. This allows you to access corporate mail without activating the VPN.

11.2.4 SPAM Mitigation

Unlike POP, typical SMTP configuration does not require authentication. This means the SMTP server will cheerfully relay any mail presented to it. This has proven a boon to unscrupulous folks to inundate email users with Spam. ISPs have adopted a number of strategies to minimize the problem. This makes choosing the optimum mail configuration difficult when using multiple mail accounts with multiple ISPs.

Block 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 receive a SPAM complaint they can track down the sender since users are authenticated. The down side of this method is that you must use the SMTP server provided by the ISP or use another SMTP server on a non standard port.

Refuse off network SMTP Access
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 is a common practice with non-authenticated SMTP server to prevent off network access.

Blacklist
The ISP may subscribe to a service that lists domain names and IP addresses of known Spammers. If mail arrives from a forbidden address it is rejected. Lists also exist of address blocks assigned to consumer ISP's, such as dialup accounts. The POP server refuses incoming mail from these addresses on the assumption one should not see dialup customers running SMTP servers.

Name Lookup
Server verifies the SMTP server has a valid domain name and associated MX record.

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. Verizon recently changed this policy and moved to mandatory SMTP authentication.

Rate Filters
Rate filters limit how many messages can be sent from an account over time. This is effective at blocking Spam since Spammers send a huge quantity of mail over a short period of time.

Incoming mail Check
Many services run incoming mail through a Spam filter. The filter evaluates each message to determine if it is Spam. Mail determined to be Spam is either marked as such or deleted.

POP Authenticate Before SMTP Send
To send mail regardless of connection one technique requires the user to retrieve mail from the POP account before allowing outgoing SMTP. Once the user is verified the ISP assumes that IP address is trustworthy for a short time. This allows the customer to send mail regardless of how they connect. Web hosting services commonly use this method since their customers use a variety of ways to access the Internet.

SMTP Authentication
The cleanest method of SMTP access control requires authentication, just like the POP server. This allows the customer to send mail independent of how they connect. This is becoming the preferred method to send mail.

11.2.5 Mail Implementation

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

> ***Mail Configuration Tip*** -- Archiving mail when using multiple clients is difficult. One trick is to have your main computer remove mail from the POP server. The other machines retrieve mail but do not delete messages from the server. When you get back to the main machine it retrieves all intervening messages and removes them from the server.
>
> ***Mail Configuration Tip*** – New mail is sent using the default Outlook account. Replying to mail received on other accounts uses the SMTP server defined for that account. This is the source of some confusion. If Outlook is set up incorrectly sending new mail may work correctly, but replies will be rejected.
>
> ***Security Tip*** -- Be careful opening e-mail attachments. This is a common method used to spread 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 scripts can be embedded in the body of a mail messages. Reading the message activates the virus. Outlook preview has to read the first few lines so it is possible to become infected even it the message has not been read. Outlook has been patched to fix this but one never knows what clever dodge virus writers will come up with.
>
> ***Privacy Warning*** – One obnoxious privacy intrusion is to insert a one-pixel image in HTML mail. When you read the message the browser has to go to the referenced URL to retrieve linked data. This allows the sender to know when and if the mail was read.

11.3 Instant Messaging

Instant messaging (IM) is becoming extremely popular both full blown messaging service using a PC and short message service (SMS) via cell phone – particularly in Europe and Japan. IM requires client side software. There is an interoperability battle being waged among the various IM services that see proprietary and incompatible IM formats in their corporate interest. The most popular universal IM client is Trillian.

11.4 USENET

Most ISPs carry USENET, service is also available from companies specializing in news. USENET provides access to ongoing discussions on a wide verity of topics. There are an incredible number of groups to choose from, both our DSL and Dialup ISPs carry over 40,000 news groups. Many 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. The down side of unmoderated groups is low signal to noise ratio. One needs to wade through a lot of Spam, inane posts, and flames to find the occasional gem.

We use Outlook Express as the newsreader.

News server authentication can occur automatically when connecting to the ISP or require explicit authentication. Explicit authentication allows access to Usenet independent of connection. Verizon recently changed news policy to limit access to users connected through Verizon access network even though the server requires authentication. This was in response to problems with customers using alternative high-speed access to download binary news groups.

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.

11.5 Multimedia

Internet multimedia is hampered by low dialup speed. Broadband eases this chokepoint opening the door to Internet delivery of radio and TV. Currently there are numerous CODECs used to compress and play audio and video. This leads to difficulty in making sure one has the correct CODEC.

Peer-to-peer sharing of electronic works is controversial because content owners are unable to enforce control over how works is used. Direct distribution of content is in its infancy. Broadband distribution obsoletes many existing business models.

11.5.1 Music Match Player

MPEG MP3 compression provides near CD-quality audio at 128 kbps, about a tenth uncompressed CD data rate. MP3 has become the most popular digital music format. We use the Music Match Jukebox player. This is both a player and is able to convert CDs or records to MP3 format.

The file server has enough disk space to store our online music library. We converted all CDs and some records (LP and 78 rpm) to MP3. This enables any computer on the LAN equipped with an MP3 player to access the music library. Near CD quality audio requires 128 kbps, this translates to about a megabyte per minute of music. This results in a large library but well within the reach of a today's cheap hard drives.

11.5.2 Real Audio Player

Real Audio is a popular format for streaming audio and video. The basic client player is free. We use version 8 of Real Player we find it meets our needs better than later versions.

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 and video.

11.5.3 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 using Digital Rights Management (DRM). Paving the way for direct purchase or subscription based music services. So far I have not found that distribution method to be particularly convenient or advantageous.

11.5.4 QuickTime

Apple QuickTime is a popular movie-encoding format.

11.6 Fax

Originally we did not want to use fax, 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 or dedicated fax line.

For incoming fax we use free eFax fax service. A local or 800 number incur a monthly fee. Each customer is assigned a unique phone number in our case 928-223-4815. When a fax arrives at the eFax server it is converted to an image file and e-mailed to the subscriber. Proprietary eFax software is required to view the attachment. The attachment can be saved and imported by other programs.

To send fax we use 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.

11.7 TV and Radio

Hauppauge TV/FM card is installed in the main workstation. It is nice being able to switch between “real” and Internet radio. TV is surprising good on a computer screen. The card has a freeze feature to capture still images. The quality of the image illustrates just how poor NTSC TV is compared to typical computer resolution. NTSC resolution is about 720x480 pixels with less color depth than typical computer display.

11.8 Digital Camera

Nothing beats a digital camera to quickly capture images and incorporate them into documents or a web page. Our camera use SmartMedia memory cards to store images. Images are compressed in JPEG format reducing size dramatically with minimal loss in quality. The camera came with a “slide viewer” called Camedia Master. This works well to organize and title individual images. For image manipulation nothing beats Adobe Photoshop.

A Microtech USB card reader allows the images to be transferred to the workstation.

11.9 Printing

Computers were once billed as the paperless office. This has not happened. On the other hand the Internet and low cost high quality printers have significantly expanded the use of electronic documents. Networked PC are able to access remote printers by using a network ready printer, an external print server, or Windows peer-to-peer print sharing.

We use a 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 than peer-to-peer printing. The print server itself is a little box, the size of a dialup modem. A built in web server manages the print server.

> ***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 pseudo-static address feature comes in handy to fix the server’s address. The router is configured to assign the same IP address based on Ethernet MAC address. This locks down the address of the print server without having to manually configure it.

11.10 Scanning

Flat bed scanners allow documents or photographs to be converted to a digital image. 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. It also functions as a poor mans copying machine allowing scanned images be printed directly.

We wanted to network the scanner. This proved impractical since the scanner needs to know where to put scanned images and without user intervention files are named with only a sequence number. The solution is to connect the scanner to workstation and create a shared image folder on the server. Images are scanned into Adobe Photoshop running on the workstation, named, and then saved on the server. Once on the server any PC is able to retrieve them.

11.11 Virtual Private Network

VPNs extend corporate network to telecommuters and business partners. In our situation a Checkpoint SecureRemote VPN provides secure remote access to corporate network. There are many ways 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 without forcing all remote Internet traffic to flow through the VPN; this is called a split tunnel. Only traffic destined for the corporate LAN flows through the tunnel. Client Internet traffic is not affected. 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 technology is IPsec developed by the IETF. IPsec has two protection mechanisms Authentication Header (AH) and Encapsulating Security Payload (ESP) AH authenticates the client's IP address and cannot be used with NAT because NAT modifies the address. ESP encrypts data to prevent eavesdropping. Authentication is performed using Internet Key Exchange (IKE).

Depending on the type of VPN the broadband router may have to support IPsec pass through. IPsec has a similar problem as FTP. Even though the request originates from the local user, the session appears to originate from the server. NAT needs to be able to learn the active port or the session will fail. This requires the router function as an Application Layer Gateway (ALG). It has to recognize IPsec, just as it needs to recognize FTP.

VPN vendors recognize the popularity of NAT router and typically implement workarounds to allow the VPN to work behind NAT. The most common method is called UDP encapsulation. If the VPN server detects NAT IKE messages are encapsulated in UDP packets. NAT modifies the UDP packets but not the IKE payload within.

Split-tunnel creates a security concern. The client is able to access both Internet and corporate network simultaneously. If an attacker compromises the client he is able to use the client to relay traffic directly into the corporate LAN. 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 is compatible with NAT
- Verify broadband router firmware is compatible with VPN software
- Verify ISP does not block ports used by VPN.
- Make sure VPN is configured to be NAT friendly
- If home and office networks use private IP addresses make sure address ranges are distinct.
- If ISP assigns dynamic IP addresses the VPN client cannot be bound to a specific IP addresses.
- The VPN extend network trust environment to the employee's 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.

12 Security -- Keeping the Bad Guys Out

Internet connectivity is a double edge sword. Being connected gives one access to the vast resources of the Internet but makes your computer vulnerable to attack. Unfortunately a significant number of talented individuals take delight in wreaking havoc on others.

12.1 Eavesdropping

Powerline and Phoneline networks leak data beyond the confines of the network. An attacker can connect to phone line or power line some distance away and gain access to network traffic. This is especially critical in multifamily housing and multioffice buildings where multiple users are in close proximity.

Radio communication is easy to eavesdrop. An attacker can locate a safe distance away without compromising physical building security. The attacker may be able to modify and corrupt computer files traveling over the LAN. If account names and password are sent in the clear they can easily be harvested by monitoring network traffic. This threat was recognized during development of wireless LANs so provisions were made for authentication and encryption to maintain privacy

Security researchers discovered significant shortcomings in the Wireless Equivalent Privacy (WEP) protocol used to protect 802.11 and similar to that used in BlueTooth. Weakness managing the encryption key makes it relatively easy to determine the key thus breaking encryption. The IEEE recently created a revised version of WEP that improves security. At the present time it is best to treat wireless devices as if they were on the Internet and use VPN technology for protection.

Wired Ethernet is less susceptible to eavesdropping because signaling is contained within the wiring. A central Ethernet switch, rather than a hub, makes eavesdropping more difficult because only traffic for the specific port is visible.

12.2 Firewall

The first line of defense is to control data entering and leaving the LAN. Unless you are running a public server on your network incoming security is relatively easy, refuse all incoming connection requests. Our business web and mail server are hosted externally. Access to them originates from the LAN. This means ALL requests that originate outside the SOHO LAN can be refused. One of the benefits of NAT is by default it drops incoming connection requests. 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 NAT discards the packet because it doesn't know which computer on the LAN to forward it to. Only if explicit port forwarding rules are created will NAT know how to handle the request.

The router allows specific IP addresses/ports to be blocked enforcing restrictions on incoming and outgoing traffic.

A firewall imposes a set of rules on data entering and leaving the network. Software firewalls running on the workstation, such as ZoneAlarm are able to control access based on individual application.

12.3 Anti Virus

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.

12.4 Security Patches

Microsoft Windows update is a convenient way to install the latest security patches. As with anti virus software it is important to stay current. Once vulnerability is discovered information about it is rapidly disseminated over the net.

12.5 Spyware

Companies are finding ever more obnoxious ways to extract information from customers. Spyware can be used for multiple purposes. Common usage is to collect information about how the application is used and forward the information back to the company. It is also used to update targeted advertising. Spyware updates the ads and in some cases selectively displays advertising based on usage.

It is possible to configure the firewall to block access to specific sites, but often spyware connects to sites you frequent and cannot easily restrict access. Some personal 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.

Lavasoft Ad-Aware searches for spyware and browser cookies, allowing the user to remove them.

12.6 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.

Window 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 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
- Ban dialup modems in networked machines. They are a potential backdoor to your LAN

12.7 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 Precautions

- 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 just enough information to conduct the transaction. Often times you can use an alias such as in chat rooms and forums.
- The web makes it easy to download and install software. It is hard to tell if a particular program is safe. Using antiviral software is not an absolute 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 and exploit a weakness. All systems have weaknesses.

13 Backup – Oops Protection

One of the benefits of converting to desktop file server was much larger hard disk capacity. This enabled us to use online backup.

13.1 On Line Backup

The server has file shares for each user. We chose Second Copy 2000 as the backup utility. Second Copy allows setting up multiple profiles. Each profile can be run automatically on a scheduled basis or manually. The backup copy can be either a direct data image or compressed to a single backup file.

> ***Security Tip*** -- Password protect network shares. Some viruses search the LAN for shares. Password will not protect shares if the machine with legitimate accesses is infected but it will prevent damage if another computer on the LAN becomes infected.
>
> ***Configuration Tip*** -- Second Copy cannot copy files that are in use. For example the Outlook mail client runs constantly, preventing backup of mail files. The Second Copy profile for mail is set for manual copy. To backup mail, Outlook is shutdown and the profile activated manually.

13.2 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 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. CD-R is the preferred backup media. The disks are large, 660 MB, and cheap. CD-R life expectancy is controversial it is at least 10-20 years more than adequate for our purposes.

Initially I used a Zip Disk for backup. Zip Drives come in 100 Megabyte and 250 Megabyte versions. I grossly underestimated the size of backup data, plus ZIP disks are rather expensive and the transfer rate rather slow. This turned out to be an impractical back up strategy.

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

14 Debug -- When Things Go Wrong

Networks occasionally fail. Good troubleshooting skills are necessary to determine the root cause of the problem. For small SOHO network good use can be made of the diagnostic tools built into Windows and the flashing lights on most devices.

In addition to built-in Window tools Broadband Reports has a number of tuning and diagnostics tests

14.1 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
10/100/1000 Mbps	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 inactive. This is most likely a cable fault or hardware failure of the Ethernet interface.

Ethernet cards automatically select optimum speed. For 100 and 1,000 Mbps operation both sides must be capable of the same speed and wiring must meet at least Cat5 standards. When connected to a hub Ethernet runs in half duplex (HDX). Ethernet switches allow simultaneous send and receive - Full Duplex (FDX).

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

14.2 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 Internet Control Message Protocol (ICMP) to determine round trip time to the remote host. Not all host respond to Ping some administrators disable it.

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 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.

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 broadbandreports.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.cnn.com [64.236.16.84] with 32 bytes of data:
      Request timed out.
      Request timed out.
      Request timed out.
      Request timed out.

      Ping statistics for 64.236.16.84:
          Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
      Approximate round trip times in milli-seconds:
          Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

14.3 Trace Route

Trace Route determines each hop between the user and the remote host, and the round trip time to each hop. This information is useful to determine the underlying cause of slow Internet response or unavailable hosts. Trace Route uses the Time To Live (TTL) field to cause packets to expire at each hop. To reach the next hop TTL is increased. When a router receives a packet with an expired TTL it discards the packet and informs the sender TTL expired. Trace Route uses this information to build a path map and response time list to each hop between the source and destination. Note in some cases a host or router will not respond to being pinged.

Windows includes a command line Trace Route utility, TRACERT. VisualRoute provides a graphical format.

Typical TRACERT report:

```
Tracing route to broadbandreports.com [209.123.109.175] over a maximum
of 30 hops:

1   *     *     *     192.168.2.1 (SOHO 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  broadbandreports.com [209.123.109.175]
```

14.4 NET

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

14.5 NETSTAT

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

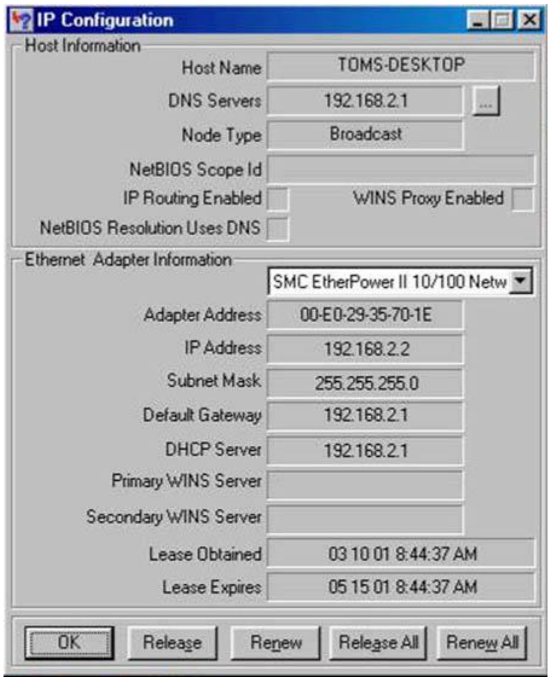
```
NETSTAT –a        Displays all connections and listening ports.
NETSTAT –e        Displays Ethernet statistics.
NETSTAT –help     This list.
NETSTAT –n        Displays addresses and port numbers in numerical
                  form.
NETSTAT -p proto  Shows connections for the protocol specified by
                  proto.
NETSTAT –r        Displays the routing table.
NETSTAT –s        Displays per-protocol statistics.
Interval          Redisplays selected statistics, pausing interval
                  seconds between each display.
NETSTAT ?         This list
```

14.6 IPCONFIG - WINIPCFG

Windows includes a command line utility, IPCONFIG that displays IP settings for all network interfaces. Some versions of Windows include a graphical utility, WINIPCFG that displays the same information. To run either utility go to START menu open the RUN dialog box. To run IPCONFIG enter COMMAMD. This opens a command line Window then enters IPCONFIG/ALL. To run graphical version enter WINIPCFG in the RUN dialog box.

Both utilities display common IP settings then information for each adapter. The first adapter is the Virtual Point to Point Protocol (PPP) adapter for dialup networking.

Adapter Address is the hardware address assigned to the physical network interface. For Ethernet this is a 48-bit Media Access Controller (MAC) address. Dialup PPP assigns a dummy MAC to the adapter. Default Gateway is the address packets are sent to connect to foreign hosts. DHCP server is the address of the dynamic address server. DNS server is the address of the name server. In a simple network DNS, Gateway and DHCP should be the address of the broadband router.



IP Configuration

Host Information

Host Name: TOMS-DESKTOP
DNS Servers: 192.168.2.1
Node Type: Broadcast
NetBIOS Scope Id:
IP Routing Enabled □ WINS Proxy Enabled □
NetBIOS Resolution Uses DNS □

Ethernet Adapter Information

SMC EtherPower II 10/100 Netw

Adapter Address: 00-E0-29-35-70-1E
IP Address: 192.168.2.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1
DHCP Server: 192.168.2.1
Primary WINS Server:
Secondary WINS Server:
Lease Obtained: 03 10 01 8:44:37 AM
Lease Expires: 05 15 01 8:44:37 AM

Figure 29 WINIPCFG

14.7 Route

Route is a command line utility to display and manipulates network routing tables.

ROUTE [-f] [command [destination] [MASK netmask] [gateway] [METRIC metric]]

```
Active Routes:

    Network          Netmask          Gateway      Interface  Metric
    Address                           Address
         0.0.0.0          0.0.0.0      192.168.2.1  192.168.2.2     1
       127.0.0.0        255.0.0.0        127.0.0.1    127.0.0.1     1
     192.168.2.0    255.255.255.0      192.168.2.2  192.168.2.2     1
     192.168.2.2  255.255.255.255        127.0.0.1    127.0.0.1     1
   192.168.2.255  255.255.255.255      192.168.2.2  192.168.2.2     1
       224.0.0.0        224.0.0.0      192.168.2.2  192.168.2.2     1
 255.255.255.255  255.255.255.255      192.168.2.2      0.0.0.0     1
```

14.8 Debug Techniques

The key to effective debugging is to break complex systems into bite size chunks and build on what you know works. One of the nice things about using a router is it provides a clear distinction between the LAN and Internet.

LAN Debug

- Are all PCs actually connected to the LAN?
- Is the Ethernet link indicator on? This mean the physical connection is good.
- Do all machines have the proper IP address? When set for DHCP if the machine cannot find a DHCP server it will self assign an address? This address is different than the private addresses used on the LAN
- Ping machines on the LAN by Network name and IP address. This verifies internal Windows name resolution works and the TCP/IP stack is working correctly.
- If PC does not show up in the neighborhood use the 7-step method to fix browsing.
- Attempt to access the router configuration page.

WAN Debug

- If your DSL or Cable modem has a ready light make sure it is on. This indicates the modem is in communication over the DSL or Cable network.
- If your ISP uses PPPoE make sure it accepted your authentication credentials. If the ISP uses DHCP try to disconnect and renew the address.
- Perform a trace route (tracert in Windows) to stable sites. This will give you an idea if your ISP is experiencing congestion (high ping), or is unable to route to the remote site. It is not uncommon to have sites "disappear" after a major fiber cut as routers try to route around the failure.
- Sites like Broadband Reports have tools to monitor connection quality.
- If you have DSL and are experiencing slow data flow, temporally connect the DSL modem directly to the test jack on the Telco NID. This disconnects inside wiring. If speed improves inside wiring or equipment is interfering with DSL.
- Remember, problems with Internet access may be caused by: your router, your physical connection to the ISP, the ISP, Internet backbone carriers or the remote host.

15 Power Distribution – Untangling The Mess

Electronic devices tend to create a jumble of cables, both data cables and power cords. Low power devices tend to use external power supplies, called wall warts, which take up a fair amount of space. After struggling with the clutter of multiple power strips I decided to try an organize power distribution.

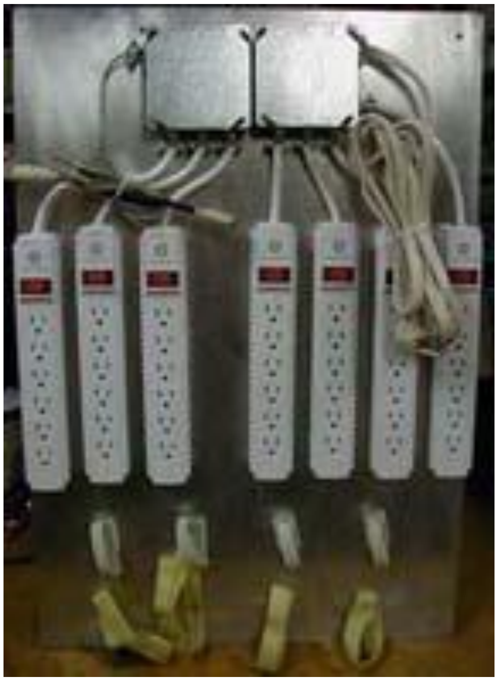


Figure 30 Power Panel

Power Panel requirements

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

To minimize power consumption devices that do not have to be on continuously are automatically switched on/off with the workstation. Power bricks take up a lot of space, so the number of outlets is generous; four strips with six receptacles each are constantly on another three are controlled by the workstation. An adapter cable plugs into the PS/2 keyboard or mouse port sensing 5 Volts. This controls a solid-state relay that feeds the switched power strips.

> ***Power Tip*** -- some power managed PCs leave PS/2 ports powered all the time to allow remote power up. In that case the power panel needs to sense power directly from PC power supply.

Two rows of Velcro are used to organize power wiring. The upper level consists of Cat 5 Velcro cable wraps. This holds excess power cable. The bottom row uses longer pieces of regular Velcro to mount larger inline supplies.

16 Internet Hosting -- Your Presence on the Net

Every business should have at least a minimal Internet presence. Creating a simple web site is neither difficult nor expensive. The web server can be run in-house or by a hosting service.

16.1 Hosting Service

The easiest way to set up a web site is a hosting service to maintain 24/7 presence. The service keeps site traffic off your Internet connection. Even companies with only dialup can have a site.

Virtual hosting is appropriate for low traffic simple site. The hosting service runs multiple virtual web servers on a single physical server. This dramatically reduces the cost of hosting a site. Our site only costs $10 US a month.

For a large site it may be advantageous to use a hosting service but provide your own equipment, called collocation. This uses the high-speed connection of the hosting service combined with the flexibility of managing and owning your own equipment.

Many ISPs allow customers to set up web sites without registering a domain name. The site is assigned a name that looks something like http://www.ISP.net/~yourbiz. This uses the domain name of the ISP as the starting point to access your web site.

In most cases it is advantageous to use the hosting service for DNS services. DNS translates URLs to IP addresses.

16.2 On Site Hosting

On site hosting makes sense for large or complex sites that justify the cost of reliable high-speed access. A business site requires a static IP address. This provides long-term DNS stability. The primary DNS nameservers can be moved on site or remain with the ISP. The secondary nameserver should be located remotely for maximum reliability.

On site hosting is practical for some personal web sites. Most residential broadband services are highly asymmetric; upload speed is much lower than download. This limits web site performance. Heavy site traffic will interfere with other Internet usage. Residential broadband services often use dynamic addresses making it difficult to host a server as the address changes without notice. Dynamic DNS services such as DNS2Go minimizes this problem. The DNS service is updated each time the server's address change. This works well for personal sites but the temporary outage during address update is unacceptable for commercial use.

16.3 Registering a Domain Name

A domain name establishes a business identity and decouples customer access from ISP and hosting service. Changing service providers is transparent to customers.

The first decision is to choose which Top Level Domain (TLD) is most appropriate. The same name can be registered in multiple TLDs this is commonly 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 country specific such as .UK or .US. If you want to identify your company with a specific region they are a good choice.

Many hosting services provide automated tools to register and setup a domain. They coordinate with InterNIC or other registration agencies. You can perform the registration yourself with the appropriate agency and upgrade registration records when you have selected a hosting service. When you submit a domain name the registrar database is examined to insure the request does not conflict with an existing name within the TLD. The new name is assigned provisionally in case another registrar has recently recorded the same name. After a little while the registration is made permanent.

16.3.1 Email

An advantage of registering a domain name is email is addressed to the domain, not the ISP. This personalizes web persona. Normally the hosting service provides one or more e-mail accounts. Email is structured as username@domain.TLD. Most hosting services are able to sort incoming mail to multiple mailboxes, allowing this function to be outsourced. The mail server may be run in-house.

16.4 WHOIS Record

Information for each registered domain is maintained in the WHOIS database. The database maintains administrative and technical information about the site.

WHOIS record for tschmidt.com

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

  Domain Name: TSCHMIDT.COM

  Administrative Contact:
    Administrative Services  (AS935-ORG)              admin@TSCHMIDT.COM
    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
    603.555.5555
    Fax- - 603.880.8783

  Record expires on 04-Nov-2003.
  Record created on 04-Nov-1998.
  Database last updated on 26-Oct-2002 17:42:04 EDT.

  Domain servers in listed order:

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

16.4.1 Administrative

Administrative information maintains data about site ownership and contact information.

16.4.2 Technical

Technical information contains the name of the authoritive nameservers for the site and contact information for technical services. The registrar does not maintain information about the site itself, simply a pointer to the nameserver that does. Registrars require two nameservers, primary and backup. Ideally located the servers are in separate locations and served by different providers. This minimizes the risk the authoritive nameserver becoming inaccessible.

16.5 DNS Record

Once the domain is registered nameserver records must be created. These records provide the translation between friendly URL names and the host IP address. If you use a hosting service they will likely setup the nameserver for you. Still it is a good idea to understand basic concepts. A DNS record lookup utility is available to view DNS records.

The name server maintains a number of different records. These are extensible; DNS functionality can expand over time. Below are commonly used record types.

16.5.1 Address Records (A)

Address records map host name to IP address.

16.5.2 Canonical Name Records (CNAME)

Canonical records allow a specific host to be known by more than one name. For example tschmidt.com and www.tschmidt.com resolve to the same IP address.

16.5.3 Mail Exchange Records (MX)

Mail Exchange records provide the address of mail servers. The preference field allows more than one host to be used to receive incoming mail. This provides backup in case a mail server goes down.

16.5.4 Pointer Records (PTR)

Pointer Record translates host IP address to machine name. This performs reverse lookup based on address rather than name.

16.5.5 Nameserver Records (NS)

The nameserver record provides the name of authoritive nameservers for the domain. Authoritive servers are the primary repositories of domain information. Other servers, called secondary name servers cache this information to speed up access. The information cached on secondary servers must be periodically refreshed.

16.5.6 Start of Authority Records (SOA)

The SOA denotes entry as the official source of information for the domain.

> **Serial number** records revisions to the record. This allows other nameservers to determine if the record has been revised and local copy needs to be updated. Preferred format for the serial number is YYYYMMDDNN. NN is an incrementing number that allows the record to be revised more than once per day.
>
> **Refresh** indicate how often secondary servers should check authoritative server for changes.
>
> **Retry** indicates how long secondary server should wait to reconnect if connection was refused.
>
> **Expire** is how long secondary server should use the current entry if it is unable to contact the authoritive server.
>
> **Minimum** indicates how long secondary servers should cache domain information.

DNS Records for Tschmidt.com

Answer records

NAME	CLASS	TYPE	DATA	TTL
tschmidt.com	IN	A	207.121.124.46	3600s (1h)
www.tschmidt.com	IN	CNAME	tschmidt.com	3600s (1h)
tschmidt.com	IN	MX	preference: 10 exchange: qmx1.tschmidt.com	3600s (1h)
tschmidt.com	IN	MX	preference: 20 exchange: qmx2.tschmidt.com	3600s (1h)
tschmidt.com	IN	NS	ns1.inr.net	3600s (1h)
tschmidt.com	IN	NS	ns2.inr.net	3600s (1h)
tschmidt.com	IN	SOA	server: ns1.inr.net email: hostmaster@inr.net serial: 2002090501 refresh: 10800 retry: 3600 expire: 604800 minimum ttl: 600	3600s (1h)

Authority records

NAME	CLASS	TYPE	DATA	TTL
tschmidt.com	IN	NS	ns1.inr.net	3600s (1h)
tschmidt.com	IN	NS	ns2.inr.net	3600s (1h)

Additional records

NAME	CLASS	TYPE	DATA	TTL
qmx1.tschmidt.com	IN	A	198.77.208.51	3600s (1h)
qmx2.tschmidt.com	IN	A	198.77.208.52	3600s (1h)
ns1.inr.net	IN	A	65.160.136.4	3600s (1h)
ns2.inr.net	IN	A	198.77.208.4	3600s (1h)

16.6 Creating the Web site

Creating a web site requires a combination of graphics and technical skills. Sites range from simple static web pages to complex database driven e-commerce sites able to perform credit card transactions. A word processor can be used to create a simple site, coding HTML manually. 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.

16.7 Uploading Web Pages

Once created the various pages must be uploaded to the web server. The most popular method is File Transfer Protocol (FTP). Files are uploaded and managed used a FTP program such as CuteFTP.

If web server supports Microsoft FrontPage extensions such as Active Server Pages FrontPage uses a proprietary method to upload files to the server.

16.8 Site Logs

The web server typically creates logs of site visitors and pages viewed by each visitor. This data can be analyzed to understand how customers interact with the site.

Conclusion

Setting up a SOHO network and VPN was an interesting and a rewarding experience. The network meets our business and personal requirements. It is a pleasure having high speed Internet access and being able to share network resources.

Significant technical expertise is required to setup the network. The various components are readily available but assembling the knowledge to create and troubleshoot the network can be rather daunting. Each year more residential and SOHO networks are installed. Manufactures are getting better at designing easy to use equipment. In general failures are minor and easy to fix once the root cause is determined. However determining the cause is not always easy. Help is available, manufacturer-sponsored forums and specialized home network interest groups provide insight and help with problem isolation and resolution.

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

Happy Networking