Living with a
Small Office Home Office Network (SOHO)
2006 Edition

Tom Schmidt
Schmidt Consulting
2 March 2006
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.

Internet access is via 1500/384 Digital Subscriber Line (DSL), provided by the local Telephone Company. A NAT router allows multiple computers to share the connection. The router automatically falls back to dialup if DSL fails. The LAN uses Fast Ethernet (100 Mbps) providing high-speed internal communication for file sharing. LAN services include: file backup, network printing, NNTP timeserver, DNS server, Syslog log file 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.

A local hosting service hosts our business web server and e-mail. Use of a Hosting service moves web site traffic off the broadband connection. It also significantly eases the task of securing the local network.

Table of Contents

1 Overview

In mid 1998 I set up a small network. I was starting 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 over the years. It started with Dialup Internet access and a few 10 BaseT Ethernet drops. Over the years it expanded beyond my home office to encompass the entire house and upgraded to 100 BaseT Fast Ethernet. 1500/384 DSL is the primary Internet connection with dialup as backup. Initially we used Wingate connection sharing software 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. In addition to file sharing it runs: DNS, network timer, local web server and Syslog log server. Each PC normally requires its own monitor, keyboard, and mouse. Rather then use separate I/O devices for server and desktop we opted to use a Belkin KVM (Keyboard Video Mouse) switchbox. This allows a single keyboard, mouse and monitor to be shared by 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 can be a challenge: as network configuration differs at each location. A utility called NetSwitcher automates this task providing one click switching between locations.

For backup we use Second Copy 2000 to perform automatic on line back up to the server. A CD burner provides off line backup.

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. For up to date product reviews the interested 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
- Local 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

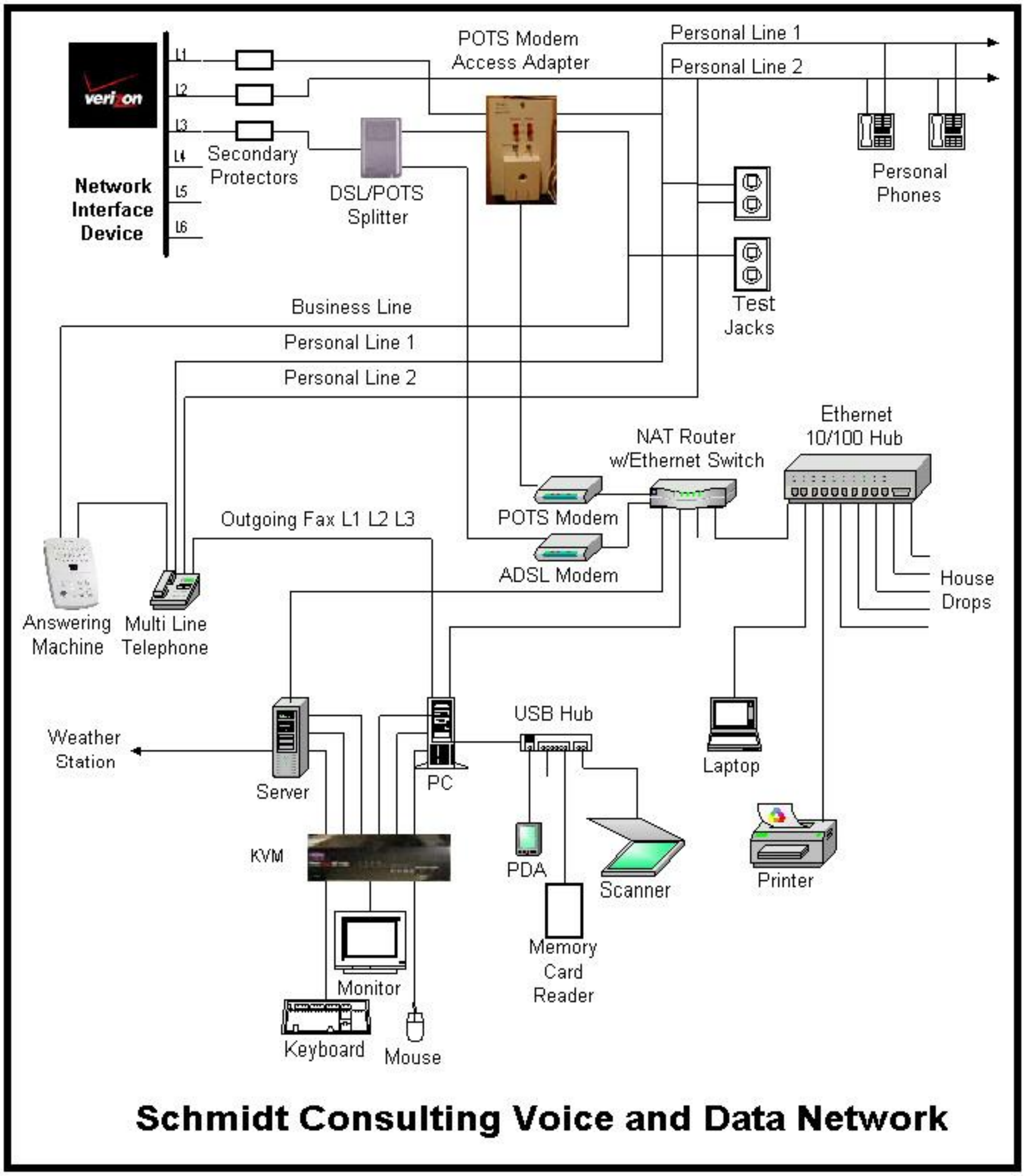


Figure 1 SOHO Data and Voice Block Diagram

The paper discusses Internet access and connection sharing options. Then covers structured wiring and details of both telephone and Ethernet networks. Even a small network benefits from having an always-on server. Security and Troubleshooting topics help to maintain the network and protect it from intruders.

Last topic discusses registering a domain name and running a public server. Every business ought to have a least limited Internet presence. It does not take much effort to set up a simple web site and cost is low.

2 Internet – Much More Than World Wide Web

The Internet began life 35 years ago as a means for academics to share expensive mainframe computers. Today it is the preferred way to interconnect all sorts of digital media: data, voice and images of all types. Internet is a contraction of Inter Network, literally a network of networks. Creation of the Word Wide Web in the 1990's vastly increased Internet popularity by providing a Graphical User Interface (GUI) on what had been until then been a text based communication network. Some equate World Wide Web with the Internet. The two are not synonymous. The web is simply one, admittedly a very popular, application supported by the Internet.

2.1 ISP

An Internet Service Provider (ISP) delivers the link between end user and Internet. Internet popularity is driving demand for high-speed low cost service. High-speed Internet access, incorrectly called broadband, is becoming widely available. Even though we are in a fairly rural area broadband is available from three sources 1) Cable company 2) Telco 3) Competitive Local Exchange Carrier (CLEC) that rents copper phone line to deliver DSL For a more detailed examination of ISPs the interested reader it referred "First-Mile Access" paper on the writings page.

2.2 Routing

Internet is a routed network. This is very different then the broadcast discovery scheme used by Ethernet. When a computer wants to communicate with a resource not available locally it forwards the packet to a gateway router. Routers know how to forward incoming packets to the proper destination or to the next router in the chain. Routers use a variety of techniques to communicate among themselves such as RIP and OSPF. ISP routers know how to forward incoming packets to customers and customer originated packets to the Internet backbone. Each router in the chain forwards packets closer to the destination until the packet ultimately arrives at its destination. It is not uncommon to have ten to twenty hops between sender and destination.

2.3 Internet Terminology

As with any specialty the Internet has its share of technical terms and acronyms. Here are some of the most important.

Address – 32 bit (IPv4) or 128 bit (IPv6) host address. Except for certain exceptions (private addresses) each address on the Internet must be unique. Example of an IPv4 address: 198.245.39.4, IPv6 address: FEDC:BA87:200C:4267:FFFE:1080:0003:0016

AutoIP – Enhancement to DHCP allowing a host to self-assign an IP address if it cannot find a DHCP server.

DHCP – Dynamic Host Configuration Protocol automatically configure network hosts with IP settings.

DNS - Domain Name System translates host name: such as www.tschmidt.com to IP address 207.121.124.46.

Domain Name – Hierarchical naming structure used on the Internet. The highest level is the top-level domain such as .COM, .EDU, .NET .UK etc, next the registered domain name, such as Google. Then sub domains such as mail or www as in mail.google.com or www.google.com.

Dotted Decimal Notation - for ease of representation 32 bit IPv4 addresses are broken down into four groups of 8-bits. 8-bits can represent any value from 0-255. 192.168.1.5 is a typical IPv4 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.

IP – Internet Protocol

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. IPv4 provides about 4 billion IP addresses.

IPv6 – Next generation IP. The most notable change is address increase to 128 bits, eliminating the current addressing shortage and opening to door to new applications.

NAT – Network Address Translation is used to translate one set of IP addresses to another. This is used extensively with small residential network allowing multiple hosts access a single ISP account while using only one public IP address.

NAPT – Network Address Port Translation. A more accurate term for translation technique used with small routers. In order to share a single public address with many local private addresses NAT translation needs to include port translation.

OSPF - Open Shortest Path First Router communication protocol allowing routers to exchange network topology information.

Port – 16-bit value used to distinguish amount multiple simultaneous connections to a single host.

Private IP address – Blocks of IP addresses reserved by IANA for private use. Not used on public Internet. This allows Private LANs to reuse the addresses multiple times.

Registered Domain – Next level in the domain hierarchy, such as Google, under the TLD.

RIP – Routing Information Protocol. Early router communication protocol: see OSPF.

Router – Provides an interface between two or more networks. Makes forwarding decisions based on the destination IP address.

Sub Domain – lowest level in the domain hierarchy, such as: www. The domain owner can create as many sub domains at they want.

Subnet Mask – Binary mask used to define boundary between network and host portion of addresses. Within a subnet hosts are directly accessible, communication does not require a router. Communication to a different subnet requires a router. For example a Subnet mast of 255.255.255.0, also called a /24 address, has 24-bits allocated to the network portion and 8 –bits reserved for hosts.

TCP - Transmission Control Protocol, TCP is an end-to-end transfer protocol that recovers from transmission errors and is responsible for reordering packets that arrive out of order. When an application creates a TCP/IP connection the receiver sees the same data stream as was transmitted.

TLD – Top Level Domain – highest level of the domain naming hierarchy such as: .COM, .EDU, .NET, .UK etc

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.

Well Known Port – used to establish initial connection. For example: the well-known port for web servers is TCP port 80.

WWW – World Wide Web Graphical information system based on hypertext.

2.4 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 a system administrator manually configured each host with a static address. This was laborious and error prone. DHCP simplifies the task by automating address allocation. 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 Internet protocol is version 4. Each node is assigned a 32-bit address, resulting in a maximum Internet population of about 4 billion hosts. Due to IPv4 address scarcity it is common practice for ISPs charge for additional addresses. Address exhaustion has been a concern for a long time. Several techniques have been developed to minimize address consumption. Next generation IP, version 6, expands address space to 128 bits. This is a truly gigantic number. While IPv6 holds much promise it entails wholesale overhaul of the Internet. Such change is always resisted until one has no choice to go through the pain of conversion.

2.4.1 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.

2.4.2 Subnet

IP addresses consist of Network-Prefix and Host address. The purpose of Subnetting is to allow IP addresses be assigned efficiently and simplify routing. The subnet mask defines the boundary between the network and host portion of the address. Hosts on the same subnet are able to communicate directly with one another. Hosts on different subnets must go through a router.

For our purposes all computers on the LAN are 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.

2.4.3 Class vs Classless Inter-Domain Routing (CIDR)

When the Internet was initially developed the divide between network prefix and host address was embedded within the address itself, rather then set by the subnet mask. These were called address classes, lettered A – E.

Class A – first octet is in the range 1 – 126 (0XXXXXXXb). 8-bits reserved for network portion leaving 24 for host addresses. 24-bits provides 16,777,213 host addresses. The lowest address is reserved as the network address, highest for broadcast. NOTE: first octet of 127 is reserved for test purposes.

Class B – first octet is in the range 128 – 191 (10XXXXXXb). 16-bits reserved for network portion leaving 16 for host addresses. 16-bits provides 65,533 host addresses.

Class C – first octet is in the range 224 – 249 (110XXXXXb). 24-bits reserved for network portion leaving 8 for host addresses. 8-bits provides 254 host addresses.

Class D - first octet is in the range 224 – 239 (1110XXXXb). Class D networks reserved for multicasting.

Class E - first octet is in the range 240 – 255 (1111XXXXb). Class E networks reserved for experimental use.

It became clear very early that allocating addresses this way was very inefficient. Class C was too small for many organizations and Class A too large. Classless Inter-Domain Routing (CIDR) was developed to allow the network prefix be fixed at any bit boundary. CIDR using variable submask is now universal and Class based routing of historic interest, although one still hears reference to Class A, B, and C networks.

2.4.4 Port Number

Internets host are able to carry on multiple simultaneous communications sessions. This raises the question how does the computer know how to respond to incoming packets? While writing this paper my mail program is checking e-mail every few minutes, I'm listening to a web based radio program and from time to time getting information from a multitude of web sites. Each TCP or UDP packet includes a port number. Port numbers are 16-bit unsigned values that range from 0-65,535. The low port numbers 0-1023 are called well-known ports; they are assigned by IANA the Internet Assigned Number Authority when a service is defined. Software uses the well-known port to make initial contact. Once the connection is established high numbered ports are used during the transfer. For example: when you enter a URL to access a web site the browser automatically uses port 80. This is the well know port for web servers.

2.4.5 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. Private addresses are not used on the Internet. This allows them to be used and reused without risk of colliding with an Internet host. This eliminates the need and expense to obtain a block of routable addresses from the ISP. To connect LAN to Internet the router, or connection sharing software, uses a technique called Network Address Translation (NAT). NAT converts the private LAN 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.

2.4.6 AutoIP Address Block

A fourth block of private IP addresses is reserved for AutoIP. If a host is configured to obtain a dynamic address and a DHCP server cannot be found the host assigns an address to itself from this pool of reserved addresses. The host picks an address from the AutoIP address pool, and tests to see if it is already in use by trying to contact that IP address. If the address is not in use it assigns itself the address. If the address is in use it picks another one and tries again.

AutoIP address block:
169.254.0.0   - 169.254.255.255 (169.254/16 prefix)

AutoIP is extremely useful for tiny networks that do not have a DHCP server. Before AutoIP the user had to manually configure IP addresses to set up a simple network.

2.4.7 Local Host Address

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

2.4.8 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)

2.4.9 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.

2.5 Naming Convention

Domain 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.

2.5.1 Domain Name Service (DNS)

When a domain is registered the registrar database contains 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 looks in the Hosts file to see is an address has been entered manually then it uses NetBIOS over IP to search local machines on the LAN. This is a broadcast mechanism and works well on small LANs but does not scale well. If the host is not found the translation request is passed to the DNS server.

Lets trace what happens when we looking up www.google.com. Since the request is not a local host it is passed to the DNS system. The highest level is root. The naming hierarchy includes an implied dot (.) to the right of the TLD this is called the root. The DNS server is preprogrammed with the physical address of several 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. It is important to note the root nameserver does not know the address of the Google web server, it only knows the address of the Google nameserver. The Google nameserver is then asked for the address of the desired host. The nameserver returns the address. 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 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.

3 Wiring Techniques – Cables and Connectors

Many improvements in wiring technology 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 US 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 punch down termination was introduced. It is called punch down because each 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 second-generation termination Type 110. 110 terminals are smaller allowing 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 electronic equipment. They devised a performance based wiring scheme independent of usage and equipment. This was a breakthrough; almost all communication systems now use structured wiring. TIA Structured wiring centralizes cable termination in a wiring closet. Point-to-point cable runs fan out to each receptacle. At the wiring closet and 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 confirm to TIA structured wiring guidelines. 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

3.1 Structured Wiring

Figure 2 Cat 5 Receptacles

The key to EIA/TIA 568 & 570 is the notion of structured point-to-point 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.

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

UTP cable is rated by Category; higher numeric designation indicates higher performance. TIA created Category 3, 4, 5, 5e and 6. Only Category 5e and 6 are current, other ratings are obsolete. UTP structured 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 network electronics.

Receptacles use type 110 punch down termination. This allows rapid termination with a punch down tool. In the wiring closet each cable is terminated at a patch panel.

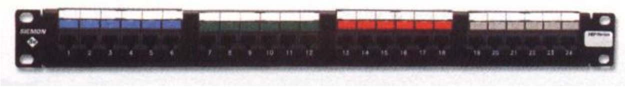


Figure 3 Cat 5 Patch Panel

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

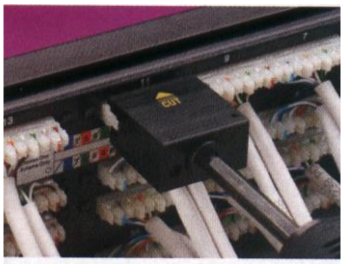


Figure 4 Rear view w/Punchdown Tool

The highest level is Cat 6. Cat 6 doubles bandwidth from 100 MHz for Cat 5e to 250 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.

Companies such as Hubbell offer residential wiring cabinets. A single cabinet is used for Coaxial TV, Telephone, and networking.

3.2 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, usually black. Direct burial cable includes a corrugated metal rodent shield to protect against burrowing animals.

3.3 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 in the early stage of divesture and FCC mandated interconnect. For the first time Customers Provided Equipment (CPE) could be connect directly to the telephone network. This resulted of many tariff offerings defining various interconnect arrangements. Each tariff not only defined the type of jack, but whether it was flush or surface mount and how it connected to the telephone network. This was called the Uniform Service Ordering Code (USOC) Registered Jack (RJ) designation. Most Registered Jacks designations are only of historical interest today. The RJ nomenclature has passed into popular usage only loosely coupled to its original intent.

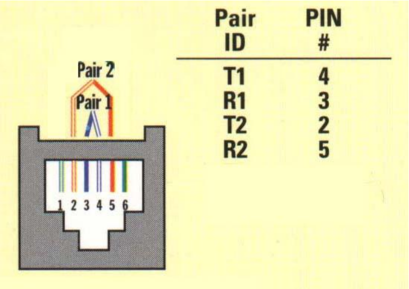
The 4-position connector is used to connect telephone handset to phone. It was not assigned a RJ designation and need not concern us here.

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 RJ48C and RJ48X jacks are 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.

3.3.1 Telco Uniform Service Ordering Code (USOC) Pinout



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

Figure 5 RJ11 & RJ14

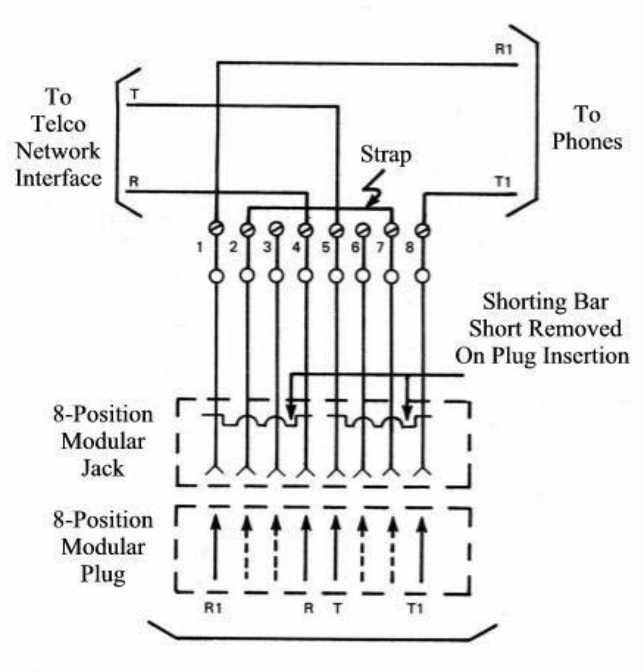


Figure 6 RJ31 and RJ38

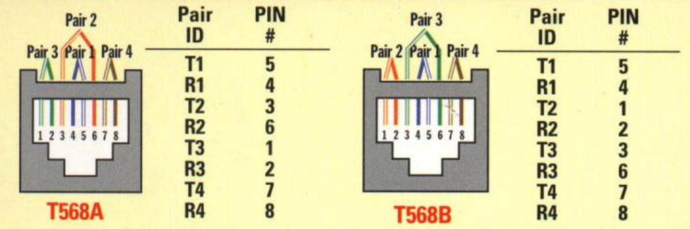
RJ11 6-position jack connects a single-line phone to telephone network. RJ14, also 6-position, is used with two-line phone.

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). 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 the alarm in series with CPE devices. When an event occurs the alarm dialer disconnects downstream CPE devices so it is able to seize the line and dial out even if the line was previously 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.

3.3.2 TIA T568A and T568B Structured Wiring Pin out

A cause of much confusion when implementing EIA/TIA 568 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.



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 7 TIA UTP alternate pin outs

The pairing arrangement of TIA differs from that used on USOC voice jacks. The inner two pairs are the same but the outer two differ. 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 RJ11 and RJ14 USOC 6-position plug. This eliminates the need for adapters when connecting RJ11 and RJ14 equipment to structured cabling. T568A is the preferred pin out because the inner two pair map directly to pair 1 and 2 on USOC punch down blocks, making cross connection easier. The most recent version of EIA/TIA 568 commercial wiring specification requires use of T568A for new installations, as does EIA/TIA 570 residential structured wiring. T568B is popular in the United States because it was used by AT&T key systems prior to the development of structured wiring techniques.

3.4 Type 66 Punch down Block

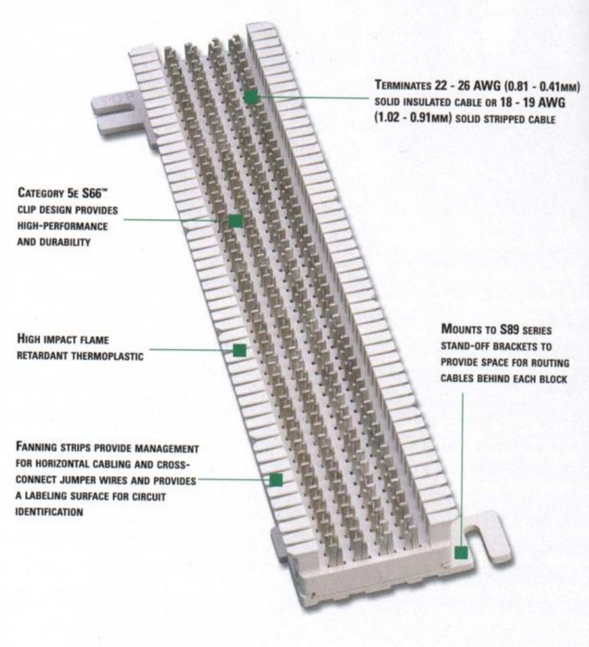

Terminates 22 - 26 AWG (0.81 - 0.41mm) solid insulated cable or 18 - 19 AWG (1.02 - 0.91mm) solid stripped cable
Category 5e S66™ clip design provides high-performance and durability
High impact flame retardant thermoplastic
Mounts to S89 series stand-off brackets to provide space for routing cables behind each block
Fanning strips provide management for horizontal cabling and cross-connect jumper wires and provides a labeling surface for circuit identification

Figure 8 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 screwed to the wall or backer board. 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.

3.5 Type 110 Punch down Block

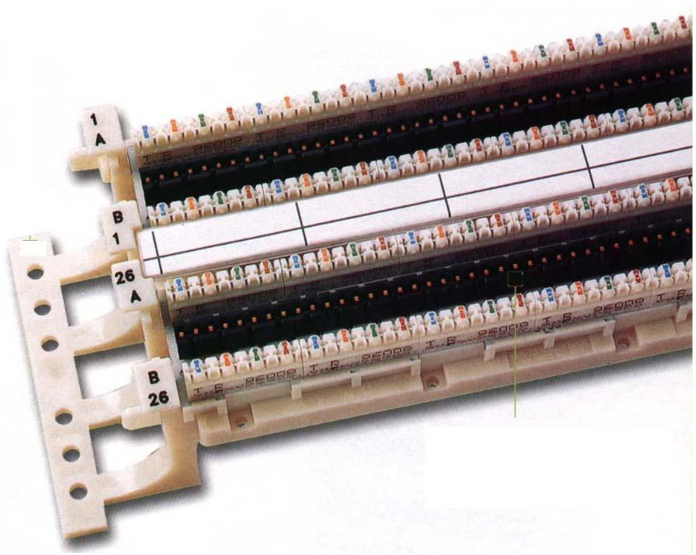


Figure 9 Type 110 Punchdown Block

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.

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 8-position modular jacks. Short cables, called patch cable, are used to connect the drop to network electronics. This results in better transmission characteristics than using punch down termination.

3.6 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 has Tip conductor 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.

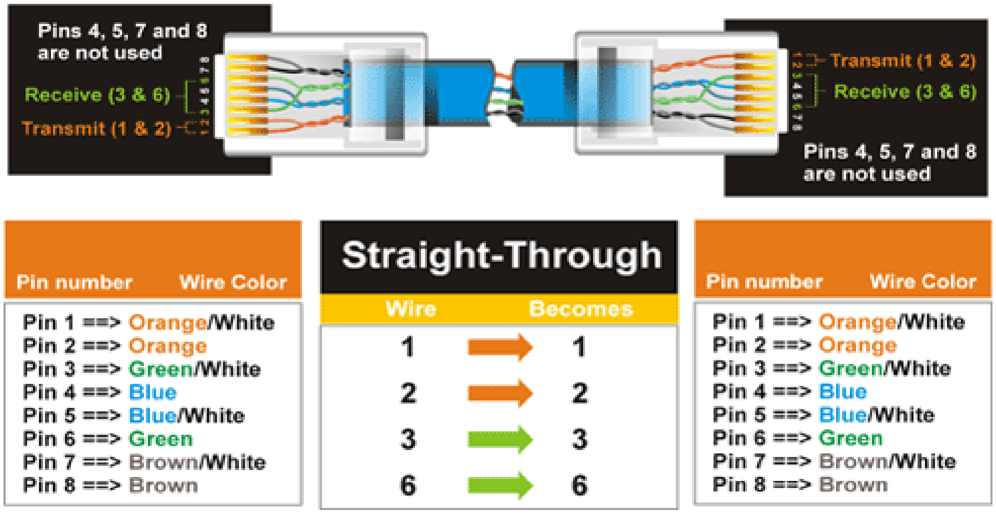
TIA Color Code	T568A 8-pos Pinout (Preferred)	T568B 8-pos Pinout	Telco Color Code	Telco Designation	RJ11/14 6-pos Pinout
Blue/White	Pair 1 pin 5	Pair 1 pin 5	Green	Tip + Line 1	Pair 1 pin 4
Blue	Pair 1 pin 4	Pair 1 pin 4	Red	Ring -	Pair 1 pin 3
Orange/White	Pair 2 pin 3	Pair 2 pin 1	Black	Tip + Line 2	Pair 2 pin 2
Orange	Pair 2 pin 6	Pair 2 pin 2	Yellow	Ring -	Pair 2 pin 5
Green/White	Pair 3 pin 1	Pair 3 pin 3		Tip +	
Green	Pair 3 pin 2	Pair 3 pin 6		Ring -	
Brown/White	Pair 4 pin 7	Pair 4 pin 7		Tip +	
Brown	Pair 4 pin 8	Pair 4 pin 8		Ring -	

3.7 Patch Cables

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

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 on an Ethernet Hub or Switch. 10 and 100 Mbps Ethernet use two of the four pair, Gig uses all four.

Newer Ethernet devices implement autosensing that automatically determines which pair is used for transmit and receive. Autosensing eliminates the need for crossover cables and uplink ports.



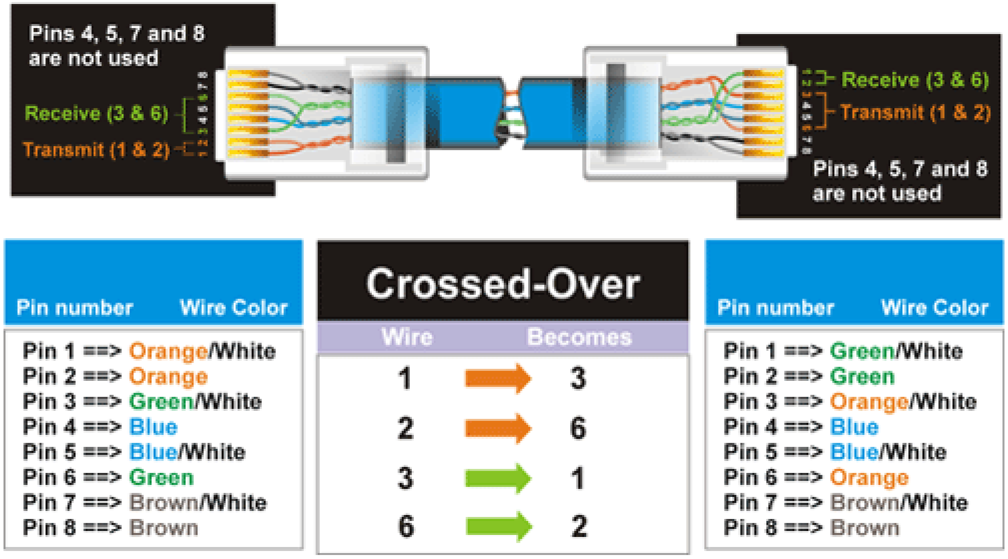
Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

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 10 Straight-through Patch Cable



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 11 Crossover Patch Cable

3.8 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. Testing verifies the cable is properly terminated; the cable is not crushed or excessively untwisted. A common problem is split pair. A cable with split-pair has end-to-end continuity but correct pairing is not maintained. This type of error may go unnoticed at 10 Mbps Ethernet but will fail when used for Fast or Gigabit Ethernet. A parametric cable tester is needed to detect split-pair. An ohmmeter only verifies continuity.

Tool	Purpose
Wire Cutters	Cut cable to length
Jacket Ripper	Removes outer cable jacket
Punch down Tool	Terminate Punch down terminals
110 Blade	Terminate 110 blocks
66 blade	Terminate 66 blocks
Crimper	Crimps cable 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

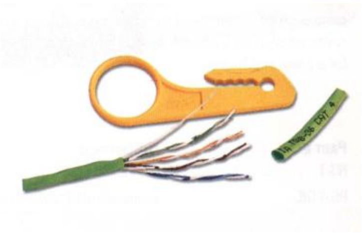


Figure 12 Jacket Ripper

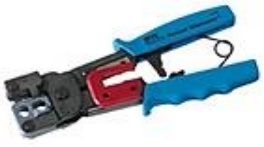


Figure 13 RJ11/45 Crimper

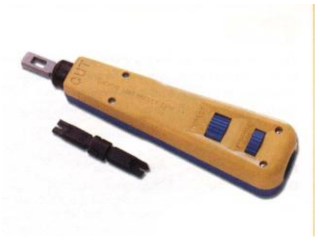


Figure 14 66/110 Punch down

4 Local Area Network (LAN) – Ethernet for Everyone

Local Area Network (LAN) allows computers to access shared resources such as printer, files, and the Internet.

4.1 Ethernet

Wired 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, 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. As electronics costs have come down speed has been dramatically increased from 10 Mbps to 100 and even to 1,000. Ethernet Switches have largely replaced hubs eliminating the collision domain mentioned above and permitting full duplex operation.

As speed increases fiber becomes the preferred choice. The difficulty with fiber is not so much the cost of horizontal wiring but the high cost of opto-electrical converters needed to connect NICs to fiber cable.

4.2 Packet Network Basics

Modern digital networks are packet based. Ethernet “packets” are called frames. Data is split into chunks called frames. Ethernet frames can be up to 1518 bytes long of which 1500 bytes are available for payload. 18 bytes are used for Ethernet addressing and frame management. Gig Ethernet is able to send data in larger chunks, called Jumbo Frames but that need not concern us here. Each packet includes network specific information providing necessary information to deliver the packet. In the case of Ethernet this consists of sender and destination address, length of the packet, and error detection to verify errors did not corrupt the packet in transit.

4.2.1 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 over fiber. However development work is underway to develop a short distance copper version to reduced interconnect cost compared to optical interconnect.

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.

UTP Ethernet requires a point-to-point connection between Network Interface Controller (NIC) and Hub or Switch, lending itself to structured wiring.

4.2.2 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 was already discussed.

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.
```

4.2.3 Hubs vs 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 work very differently then hubs. The Switch examines each arriving packet, reads the destination MAC address and pass it directly to the proper output port. Switches eliminate the collision domain allowing multiple conversations to occur simultaneously as opposed to being limited to only one with a hub. This dramatically increases network performance. 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 1600 Mbps. This assumes 8 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. Switches enables full duplex communication. This means individual computers can be transmitting at the same time they are receiving. 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 the port and associates the MAC address with that port. The switch also floods all ports with broadcast frames. Switches are transparent. Ethernet applications have no knowledge switches are being used instead of hubs.

Switches used to be much more expensive then hubs. In recent years switches have come down dramatically in price obsolescing hubs while speed has been dramatically increased. New installations should be Gig switch based. Gigabit Ethernet prices are rapidly declining. Gig Ethernet LANs are an interesting inflection point. Historically computer performance has been limited by network speed. Gig Ethernet reverses that. When connected to Gig Ethernet typical PCs are only able to utilize a fraction of rated speed due to internal bottlenecks.

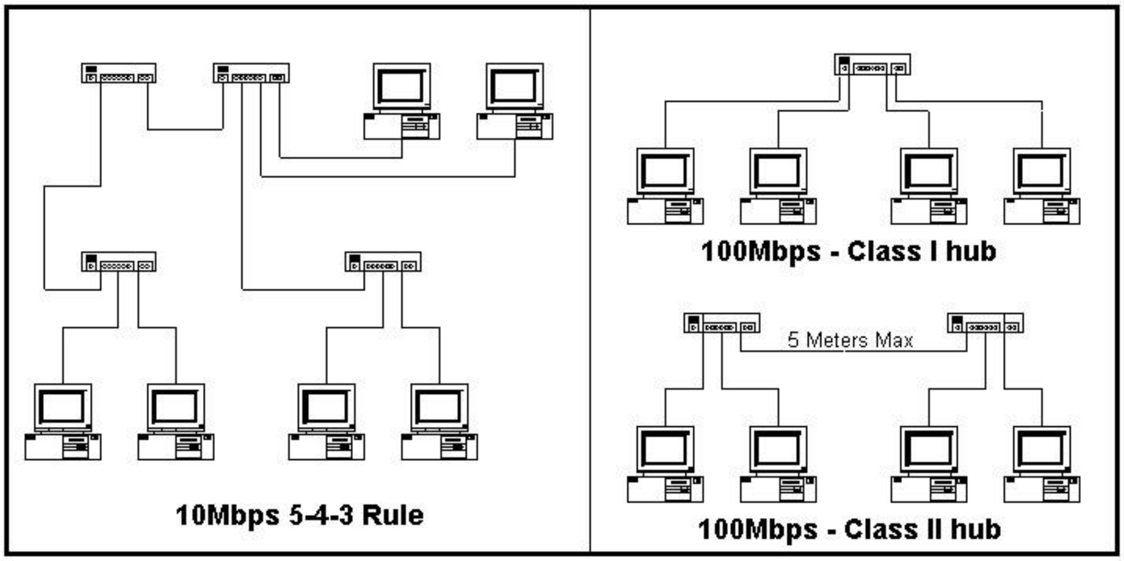


Figure 15 Ethernet and Fast Ethernet Hub Rules

> ***Performance Tip*** – Gigabit Ethernet transfers 125 MBytes per second, 250 in full duplex mode. This speed exceeds sustained throughput of typical PC memory, disk drives, PCI, and Card Bus. Getting optimum performance of Gigabit Ethernet requires high performance hardware/software.

4.2.4 Managed vs Unmanaged Hubs and Switches

Ethernet hubs and switches come in managed or unmanaged versions. Managed devices allow the administrator control of various parameters and observe traffic. These features are likely overkill in a typical SOHO network. Unmanaged devices are considerably less expensive.

4.2.5 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. If switches are cascaded traffic between switches is limited to the speed of the link whereas traffic on a single switch is limited by the speed of the switch backplane.

4.2.6 Virtual LAN (VLAN)

Virtual LAN technology allows the same physical LAN to connected multiple computers while isolating one group from another. Typical use is to set up separate VLANs for say payroll, marketing and engineering. A router is used to logically interconnect the domains providing a great deal of control over how data flows across VLAN boundaries.

VLANs are not yet common for home LANs but may become so if Internet services are delivered by multiple service providers, perhaps one for data, another for IP based TV (IPTV), and yet another offering Voice over IP (VoIP).

4.2.7 Quality of Service (QoS)

Packet based networks are egalitarian best effort networks. This works amazing well for transferring large chunks of data from point A to point B. The network functions in the presence of all sorts of impairments and failures. However: best effort does not work as well with latency critical applications such as telephony and streaming media. When a switch or router encounters congestion it buffers incoming packets until it is able to forward them. Quality of Service (QoS) allows latency critical data to go to the head of the line. This simple strategy works well if latency critical traffic is a small percent of the total so bumping its priority has little negative effect on other traffic.

Given the low cost and high speed of consumer Ethernet equipment few QoS problems occur on wired Ethernet LAN. Wireless LANs are slower and subject to radio interference benefit from QoS. Where QoS is most important is uploading to the Internet. Most consumer broadband links have relatively little upload capability. QoS is a great help in managing this limited resource.

4.3 WiFi Ethernet Radio (WLAN)

Great strides have been made in creating high performance low cost wireless LANs. 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 speed to 11 Mbps, 802.11g increased speed to 54 Mbps. 802.11a delivers 54 Mbps in the 5 GHz band. 802.11 radios 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 multiple Access Points. The WiFi Alliance insures interoperability between different vendors. Development work is under way to increase speed to 100 Mbps.

The nature of radio means WiFi speed is not directly comparable to wired Ethernet. WiFi is half duplex and collision avoidance/detection issues means a given WiFi speed is equivalent to about half that of wired Ethernet. For example 802.11a at 54Mbps delivers about the same thru put as a 27 Mbps wired Ethernet LAN.

Wireless LAN security and privacy is much more difficult then wired because an intruder does not require a physical connection to compromise the network. The original 802.11 designers were aware of this risk and incorporated Wireless Equivalent Privacy (WEP) in the original specification. Unfortunately almost immediately security researchers found critical weakness with WEP and shortly thereafter hacking tools became readily available making WEP virtually worthless. IEEE developed a comprehensive security standard and several interim implementations are currently available. The WiFi Alliance Security WiFi Protected Access (WPA) is current state of the art for security. Netstumbler is a useful tool to help secure WiFi LANS.

4.4 Alternatives

Ethernet, wired and wireless, is the dominant LAN technology. The cost of installing network wiring is modest 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.

It is an interesting testament to Ethernet's popularity these alternatives all use modified Ethernet frames adapted to the specific requirement of the physical medium while making it easy to bridge to standard Ethernet.

4.4.1 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. This allows HomePNA and Ethernet devices to communicate as if they were physically connected to the same LAN.

4.4.2 Power line Networking

The HomePlug initiative provides high-speed network device that plug into ordinary AC receptacles. The HomePlug Powerline Alliance is the clearinghouse for power line networking products.

4.4.3 Ethernet over Coax

An interesting technology is to utilize TV coax wiring to deliver Ethernet. Coaxsys and Multimedia over Coax Alliance are popularizing this technology. Many homes build in the last couple of decades have multiple TV outlets but are not wired with Category rated cable suitable for conventional Ethernet.

4.5 SOHO LAN Implementation

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

I chose to reduce wiring cost by terminating each horizontal LAN cable directly with a modular plug. Modular plugs are 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.

5 Telephone – Not Just for Voice Anymore

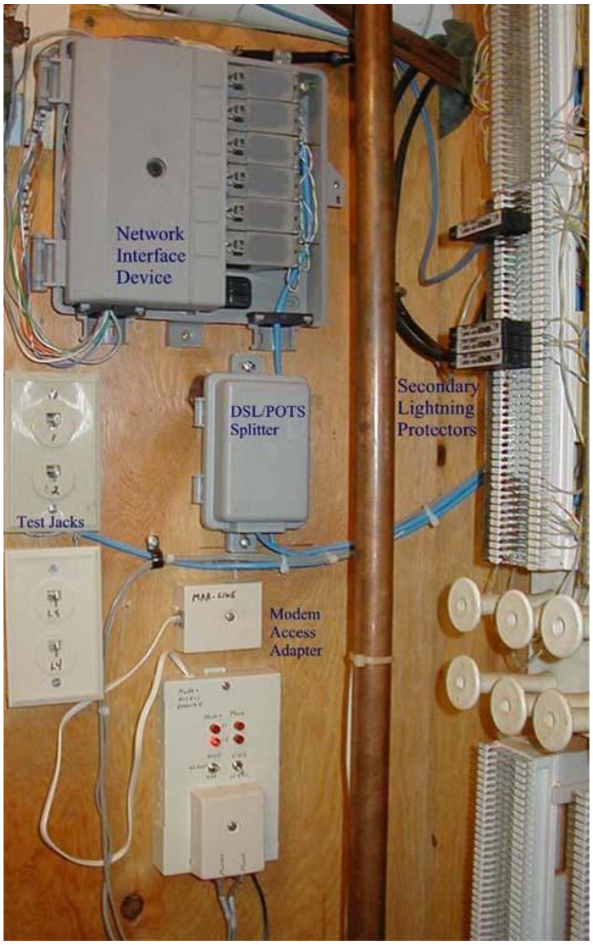


Figure 16 Telephone Wiring Closet

We have three phone lines, two for personal use and a third for business. 1500/384 ADSL service provides high speed Internet access. ADSL is installed on the business line.

The two non-business lines are configured as a hunt group, also called transfer on busy. 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 telephone service reps may not be familiar with Hunting 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 we learned that is not possible, caller ID is bound to physical 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 use. It is not part of the hunt group. Since the business has only a single line we wanted to use Telco based answering service. Telco answering service is a good match for single line offices because the caller gets voice mail if the line is busy instead of a busy signal. I consider call waiting inappropriate for business use. Unfortunately our local telephone central office (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.

Even though we have ADSL we maintain a backup dialup ISP account. Using a dedicated modem phone line seemed needlessly expensive. 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 cannot detect if the line is in use. 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. Operation of the MAA is described below.

5.1 Telco Network Interface Device (NID)

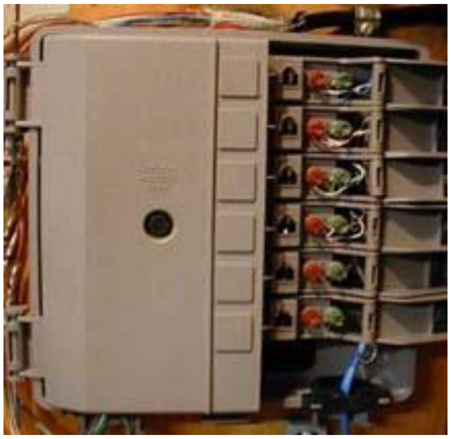


Figure 17 Telco NID

In the bad old days before US telecom divestiture (1880 to early 1980's) Phone Company supplied service, wired customer's home and business and leased all telephone equipment. With divestiture Phone Company regulated responsibility was limited to delivering service to premise. Inside wiring and equipment became customer's responsibility. This created a dilemma for the Phone Company, how to determine if a problem was their responsibility or that of the customer?

Enter the Network Interface Device (NID). NID is the demarcation point, between Phone Company and customer. It incorporated lightning protection and a method to easily disconnect customer premise equipment (CPE) from the telephone network. Early NIDs used modular jack connected to old style carbon block lightning protector. Over time NIDs evolved into a single integrated package. The specific embodiment of the Network Interface Device (NID) has changed over the years but the purpose remains the same: Terminate outside drop wiring; provide lightning protection and means to disconnect inside wiring. Some NIDs include a half-ringer test circuit. The half-ringer creates a unique signature to allow test equipment to determine if fault is on Telco or customer side.

Picture above shows a typical multiline NID installed indoors, as opposed to more common location outside. 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 disconnects inside wiring. If the test phone works the problem is with customer wiring or equipment, if not problem is with the Telco.

5.2 Secondary Lightning Protection

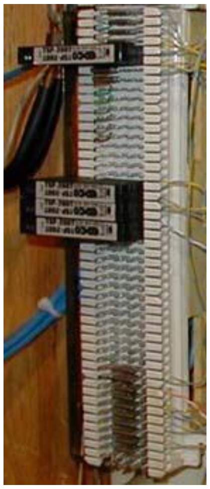


Figure 18 Lightning Protection

Local exchange carrier provides lighting protection as part of the NID. 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 risk of equipment damage. The best location for secondary protection is the building entry point. This allows protector to use power mains low impedance earth ground to minimize 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 the protector does not interfere with the high frequency DSL signal. The protectors clip to 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 is used for each incoming telephone line. Additional protectors should be used on any lines connected outbuildings.

5.3 POTS/DSL Splitter

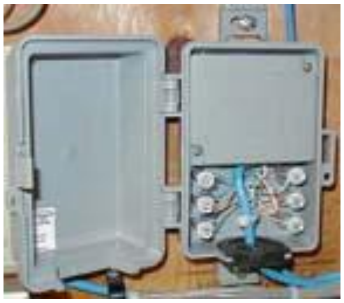


Figure 19 Splitter

ADSL uses a single phone line to deliver both voice and data service. Filters are required to prevent the high frequencies used by DSL from interfering with voice. To reduce cost ADSL service used customer-installed filters. All non-DSL equipment must be behind a filter.

Rather than using a microfilter at each non-DSL device I installed a POTS/DSL splitter. The business line is connected to a Corning/Siecor POTS/DSL splitter. The splitter provides 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 test circuit after the low pass POTS filter. This allowed the half-ringer in the NID to be removed, minimizing DSL signal loading.

Home Alarm Tip – If a phone is connected to the splitter "Data" jack it works normally. This creates a potential safety hazard with a home alarm system. If a phone is inadvertently 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 so only the DSL modem is connected to the "data" jack. Or the splitter installed can be installed after the alarm jack and the alarm filtered separately.

5.4 Modem Access Adapter

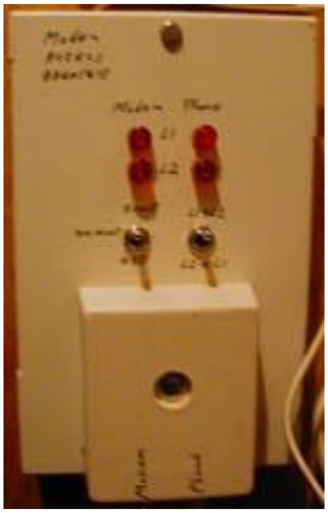


Figure 20 Modem Access Adapter

We wanted dialup modem to have access to multiple phone lines while preventing 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 modem going off hook and searches for an idle line. If it finds an idle line it disconnects phones before connecting the modem. While modem is in use phones are disconnected preventing them from interfering with modem. If all lines are busy modem cannot connect and retries later. This prevents modem from barging into an active phone call.

The adapter is connected to the primary personal line and business line. When the modem attempts to connect adapter tests primary personal line first, if it is busy business line is checked. The search order assumes that during the day, when business line is needed, modem uses 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 data call is placed on 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 sets 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.

5.5 Putting it all Together

The drawing below shows overall connection of phone and DSL wiring. 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. A POTS/DSL splitter is connected to business line. Splitter "Data" output runs directly to DSL modem. Splitter "Voice" and line 1 feed the Modem Access Adapter. A dedicated drop connects Dialup modem to MAA.

To make changeover 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. 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 corded plug. This allows test phone to be plugged into the CPE test jacks or directly into the NID. Having the phone permanently mounted in the wiring closet insures it is available when needed.

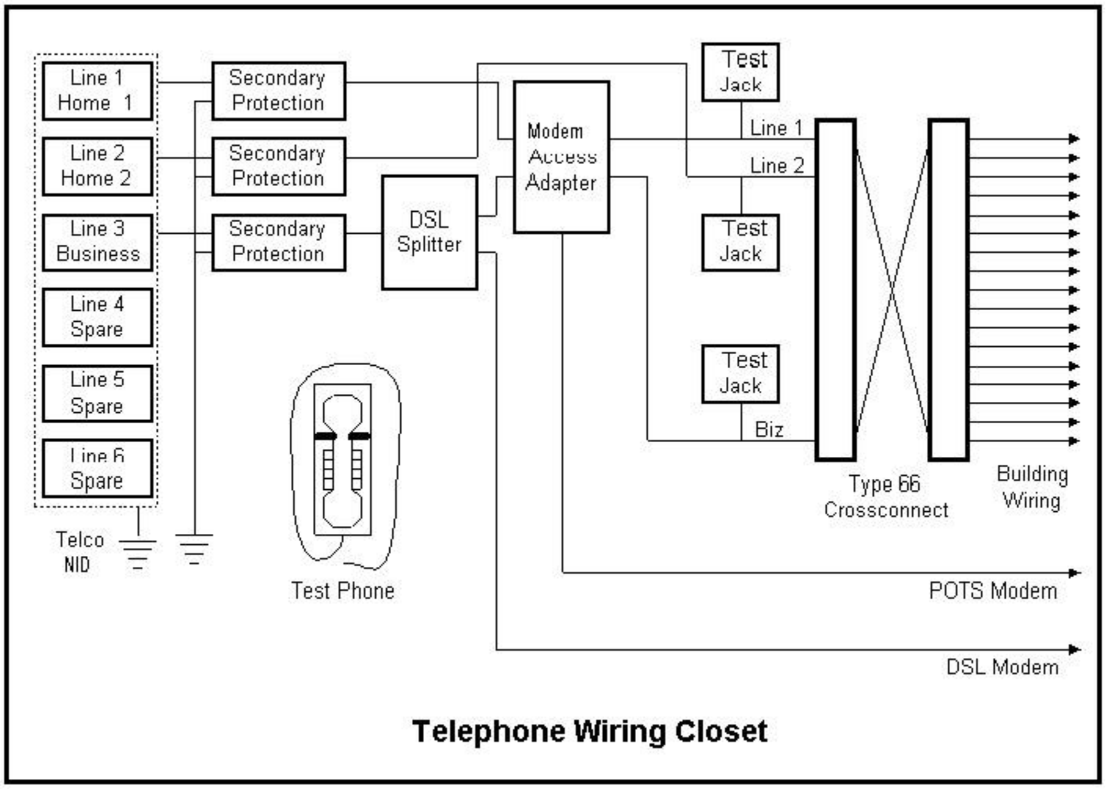


Figure 21 Telephone Wiring

6 Broadband Router – One Connection So Many Computers

When the LAN was first set up we used Wingate software running on a laptop sharing a dialup connection. At the time (1998) 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:

- 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.
- At the time Wingate provided a proxy service rather than NAT. This required each application be configured to use the proxy in order to access the Internet.
- 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.

Figure 22 Multitech Broadband Router

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

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. The router market is extremely competitive. Routers can be had for less then $50 US.

6.1 Network Address Translation (NAT)

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 public Internet 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. NAT offers the advantage of a proxy server with the benefit of being transparent to most applications. Proxy services were used extensively prior to the deployment of NAT.

Internal LAN intercommunication proceeds normally NAT is not required. When a request cannot be serviced locally it is passed to the NAT router, called a gateway. The router converts private address to the public address issued by the ISP and in some cases modifies port numbers to support multiple sessions. The router sends the modified packet to the remote host as-if-it-originated-from-the-router. When reply is received router converts 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 blocks remotely originated traffic. It functions as a de facto firewall because it does not know how to route packets that originate outside the LAN to host on the LAN unless specifically programmed to do so.

6.1.1 Performance

NAT requires router do a lot of bookkeeping, changing IP and port addresses, then computing new packet checksum. Routers have no trouble keeping up with WAN connections of a few megabits per second. If you are blessed with really fast broadband connection say 5 or 10 or even 100 Mbps make sure router is up to the task. Our DSL connection is 1500/384 kbps. The router does not degrade network performance.

6.1.2 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, the session is lost. It interferes with server functionality and IPsec VPNs.

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 SOHO LAN. In this case it may be impossible to resolve address collisions if multiple networks use identical address blocks.

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.

6.2 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 it connects directly to PC or router. The WAN port on most routers offer a variety of WAN configuration options simplifying the task of switching from one broadband ISP to another.

The Verizon Westell ADSL modem has a 10 Base-T Ethernet port that connects directly to the Wide Area Network (WAN) port of the router. 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 software. Verizon PPPoE sets IP address; subnet mask, Gateway and DNS addresses 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 connection from being dropped. This simulates a true always on connection. The other function of the keep alive is to determine if router has a good Internet connection. It does this by periodically querying NIST timeservers.

6.2.1 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 activates dialup connection. The router includes an idle timer to disconnect dialup modem after a period of inactivity. This prevents modem from tying up the phone unnecessarily. Router constantly attempts to reestablish the broadband connection. When broadband service is restored dialup session is terminated.

Dialup 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 back to dialup. 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 having to modify the LAN.

Setting up 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 difference between Dialup and DSL from devices on the LAN. Host settings do not change the only difference between Dialup and DSL is speed.

Verizon ADSL has been reliable. 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.

6.2.2 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. Unfortunately there are a few things the router cannot hide.

Sending Mail - 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 servers cheerfully accept 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 8.3.4 Spam Mitigation** for more details.

Our domain hosting service uses SMTP authentication. Neither Verizon DSL nor our dialup ISP block outgoing port 25 used by SMTP this allows us to send mail though our domain 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 uses authentication access is blocked. For example Verizon limits Usenet access to Verizon IP address blocks. This is done to prevent customers from swamping binary news servers by using alternative high-speed connections.

Speed – obviously the router can do nothing about the speed difference between DSL and dialup.

6.3 LAN Address Assignment

Each device on the network requires a private IP address. These addresses are not used on the Internet therefore they are not 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.

6.3.1 Static

IP parameters: address, subnet mask, gateway address, and DNS address need be manually assigned 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.

6.3.2 Dynamic

Default Windows IP configuration is dynamic address allocation. At power up the PC looks for a DHCP server on the LAN. The DHCP server in the router assigns each machine IP parameters. Once the PC is configured it is able to use the LAN and Internet.

6.3.3 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 static addresses manually.

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.

6.4 Gateway

The host sends packets that cannot be delivered locally to the gateway. The gateway 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.

Broadband NAT routers are not true routers in the conventional sense. The do not share routing information with other routers and typically have only a single port.

6.5 DNS Nameserver

Host name resolution for local devices is performed by 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 IP address. The router then forwards request to Verizon DNS nameserver. To devices on the LAN the router looks like a DNS server. We are running a local DNS nameserver that requires overriding the setting provided by the router. Unfortunately the router does not include a mechanism to point to an internal private nameserver. The workaround is to manually configure DNS nameserver address on each client, another reason to use pseudo-static addresses.

6.6 10/100 Ethernet Switch

The office is wired with 4 Ethernet drops fed 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.

6.7 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 data storage space.

6.8 Public Server Behind NAT

Running a server behind NAT requires router forwarding incoming connection requests. By default incoming connection requests are discarded because the router does not know which host on the LAN to direct it to. The router acts as an inbound firewall. Port forwarding configures the router to accept an inbound connection request, to say port 80, and forward to the web server. To the remote host the server looks like it is using the public IP address, when in fact it is on a private address block. Each service needs to be forwarded to the host running the appropriate service.

6.8.1 LAN Access to Local Public Server

Most Residential NAT routers do not perform WAN loopback. This prevents access to local public server by its domain name or public IP address from within the LAN. The server must be accessed by its LAN machine name or LAN IP address. When the server is accessed by public IP address the router forwards the request to the Internet. It does not realize the host is local. The packet never reaches the server.

If local access by DNS name or public address is important add the name/address information to Windows Host file. The Host file performs static name translation service invoked prior to DNS. If the requested host name is found in the Hosts file Windows will use that address and not query DNS.

6.8.2 Active vs Passive FTP

The way FTP allocates ports causes problems with NAT. To NAT the connection appears to originate from the server, rather then user. This causes NAT to prevent the transfer. This can be a problem if your change FTP ports from default 20/21 to some other value. NAT routers only know how to handle FTP on the default port.

To learn more read: Active FTP vs. Passive FTP, a Definitive Explanation.

6.8.3 Multiple Identical Servers

Most residential broadband ISPs only allocated a single IP address per customer. This causes problems running multiple servers of the same type. For example when running a web server, all incoming requests to port 80 are redirected to that server, this makes it impossible to run two web servers on a single IP address using the well-known port. The work around is to use a different port for one of the web servers. This can cause problems since the remote user has no way to know the server is using a non standard port. Many DynamicDNS sites have provisions to redirect the request to the alternate port.

6.8.4 Security

Great care need be taken running public servers. If an attacker is able to exploit a weakness in the server they gain free run of the local LAN as if the were locally connected.

6.9 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 no way to know if the device requesting access is trustworthy.

7 Local Server – Just Like the Big Kids

The server provides several network services: file sharing, DNS nameserver, Network Neighborhood browse master, real time clock synchronization, Syslog log server, private web server and local 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.

7.1 KVM Switch

Figure 23 Belkin KVM

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.

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 real devices to match stored virtual device configuration.

> ***Video Performance Tip*** -- Workstations use higher video resolution and faster refresh rate than servers resulting in very high video rate. This is 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.
>
> ***Mouse Compatibility Tip*** -- Each computer thinks it is directly 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 device 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. This is only a problem when switching between machines. The KVM transparently passes commands from the active machine.
>
> The Belkin KVM does not support my favorite mouse, the Logitech Wheel mouse. Switching between systems revert the mouse to default mode, use of scroll wheel and thumb button is disabled. To get around this problem the workstation runs the Logitech mouse driver and is connected to KVM port 1 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. Switching to server resets mouse to Microsoft mouse mode. Enhanced functions are lost. The mouse still works but neither the thumbwheel or thumb button is functional. I placed the Logitech control panel in the workstation 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.
>
> ***Monitor Plug and Play*** – modern CRT and LCD monitors communicate using VESA Display Data Channel (DDC). This allows the PC to read monitor characteristics and automatically configuring the video subsystem. If the KVM does not emulate this feature when the PC is powered up on an inactive KVM port it thinks it is connected to a non Plug and Play monitor

reverting to low resolution low refresh mode. When the desktop is turned on connected to an inactive KVM port it thinks it is connected to a non plug and play monitor and reverts to VGA mode. A workaround for this is to disable monitor plug and play and set resolution and refresh manually. Or always make sure the KVM is set for the desktop before turning it on.

7.2 Local DNS Server

Normally the ISP provides DNS. However, any DNS server can be use to translate names to IP addresses. Verizon DSL service has been very reliable, but they have had numerous DNS problems. I used the DNS server from my dialup ISP for a while but finally decided run my own. Bind-LE was installed on the server. Running your own DNS server puts you in charge of DNS issues.

Installing and running Bind-LE (Win 98) or TreeWalk DNS (XP, W2K) is straightforward. Install the software. Then modify TCP/IP settings. On the PC running Bind use IP loopback address 127.0.0.1 for DNS, on other PCs DNS points to the Bind server. Running my own DNS server has solved the problem.

7.3 File Sharing

One of the advantages of having a LAN is easy file sharing between machines. The server in out network is set up with shares for each family member. Manual and automatic backup is used to protect data.

Windows network neighborhood allows one to browse network shares, as easily as if they were on the local machine. To show up in My Network Places each machine must be running Microsoft file and print sharing service, even if nothing is being shared. The network 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 constantly on. Browse Mastership is negotiated at power up. Network neighborhood becomes unavailable when the Browse Master is turned off, until the remaining machines negotiate Browse Mastership again. Getting the Neighborhood to work reliably can be a challenge, since many components interact and involve large latencies.

The alternative to using peer-to-peer file sharing is to set up a Windows Domain controller. In general that is overkill for most small home and office networks.

7.3.1 Share Files in My Network Places

#1 File and Print Sharing Service

Make sure Microsoft "File and Print sharing service" is installed 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 or IPX for sharing go to Network setting for each adapter and unbind TCP/IP. By default Windows binds each adapter to all protocols. NetBIOS over TCP/IP should be checked. NetBIOS is the programming API used by application to exchange information over the network.

> ***Security Tip*** - If system includes an interface connected directly to the Internet such as when using Internet connection sharing software like MS ICS or Wingate unbind file and print sharing service from that interface. Failure to do so results in sharing the computer with millions of your "best friends" on the Internet. See item #8 for Ports used in file and print sharing.

#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
Ideally the 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. Even if no directories are shared the PC will still show up in My Network Places.

> ***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 and SMB ports used to discover local host names and share files.

```
TCP/UDP Port 137 NETBIOS Name Service
TCP/UDP Port 138 NETBIOS Datagram Service
TCP/UDP Port 139 NETBIOS Session Service
TCP/UDP Port 445 SMB (Server Message Block)
```

> ***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.

7.4 Time Service

US National Institute Standards and Test (NIST) and other organizations maintain public timeservers. This eliminates the problem of drifting and inaccurate computer real time clocks. For personal use NIST recommends using NTP Pool Time Servers. 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.

We use Tardis 2000 running on the server and K9 on each client for clock synchronization. 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 local Real Time Clock (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 a pool Stratum 2 timeservers.

Tardis support Syslog. This allows the Syslog server to capture Tardis2000 events.

> ***Configuration Tip*** --Tardis 2000 defaults NTP time broadcasts to all available interfaces. If Tardis is run on a computer with direct Internet access 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 dialup connection from timing out and may annoy your ISP.
>
> ***Configuration Tip*** -- The load on public timeservers is very high and getting higher, be a good net citizen on set Tardis to only update every few hours. We set this parameter to once every 2 hours. For convenience the LAN broadcast occurs every 64 seconds so client clock is updated as soon as the machine boots.
>
> ***Configuration Tip*** -- Tardis monitors dialup status. This is convenient if the PC running Tardis is directly attached to the Internet running DUN. Tardis will update Internet time only if the connection is active; this prevents Tardis from activating an auto dialer.

7.5 Private Web Server

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

> ***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.

7.6 Weather Station

Davis Instruments weather station data is posted on the internal web server. Davis software is configured to update a historical data file and create GIF images. The GIFs are posted to the local web server allowing anyone on the LAN to retrieve weather data.

7.7 SysLog Server

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 overcoming storage limitation of most network appliances. Currently the only devices on the network originating Syslog entries are the Routefinder router and Tardis Time service.

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

8 Services – Making Life Worth Living

This section describes the various services running on the LAN.

8.1 *Internet Browsing*

All PCs use Microsoft Internet Explorer version 6. Web browsing uses Hyper Text Transfer Protocol (HTTP). I played around with FireFox as an alternative to IE. It worked well but I was too lazy to migrate all the shortcuts from IE to FireFox. It seem seems the browser wars are raging once again. I'll seriously consider it on the next PC upgrade.

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 Search toolbar add-on. The toolbar allows Google queries be made directly from the toolbar.

8.2 *FTP*

File Transfer Protocol (FTP) is a very effective way to transfer large files over the Internet. FTP predates HTTP.

8.3 *E-Mail*

E-mail accounts fall into three broad categories: advertising supported free accounts, ISP accounts and business accounts. 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 e-mail address from ISP. Free accounts make sense for personal use and as throwaways if they attract too much spam. For business purposes or to insure long lasting email identity nothing beats registering your own domain name. Once registered e-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.

8.3.1 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 handy than a mail client but adequate for casual users.

8.3.2 Mail Client

Except for web-based mail, e-mail has a sending component, SMTP, and a receiving mailbox, POP. To send mail the 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.

8.3.3 Corporate Mail

Telecommuters and road warriors need access to corporate mail 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. Some companies are implementing web-based email making life easier for road warriors and telecommuters. Corporate web based e-mail is convenient because it does not require a specialized email client – any machine with a web browser is able to access mail.

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 a personal mail account. This allows you to access corporate mail without activating the VPN.

8.3.4 SPAM Mitigation

Unlike retrieving mail from a POP server sending mail through a SMTP server does not normally require authentication. This means the SMTP server will cheerfully relay any mail presented to it. This has proven a boon to unscrupulous folks inundating the Internet with Spam. ISPs have adopted a number of strategies to minimize the problem. This presents a challenge choosing optimum mail configuration when using multiple mail accounts and multiple ISPs.

Block Port 25
SMTP uses TCP port 25. Some ISP's block this port at the edge of their network. If the ISP blocks outgoing use it effectively prevents customers from using a 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. If the ISP bocks incoming Port 25 (more common) it prevents you from running a SMTP server and accessing it while off network.

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 so called Blacklist service listing domain names and IP addresses of known Spammers. If mail arrives from a forbidden address it is rejected. Blacklists 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 or residential broadband customers running SMTP servers.

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

Rate Filter
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.

Mailing List Filter
Mailing list filters limit number of recipients in a single message. This is less effective then rate filtering and becomes a real nuisance when sending a message to a large number of recipients.

Incoming SPAM 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

This method allows clients connected to a different access network the ability to send mail thorough a non-authenticated SMTP server with a reasonable amount of security. The technique requires the user first retrieve mail from the POP account before 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.

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.

8.3.5 Mail Implementation

None of the ISP's we use block outgoing port 25. The hosting service uses SMTP authentication. This allowed me to configure all mail accounts on 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.

Outlook Configuration Tip – New mail is sent using the SMTP server defined for the default account. Reply uses the SMTP server defined for that account. This is the source of some confusion. Depending on how Outlook is set up mail will be sent on some account while others will fail. Any SMTP server can be used to send mail, not just the one provided with the particular mail account.

Multiple SMTP servers – If you have to switch between multiple SMTP mail servers based on location the registry hack built into NetSwitcher (see **Laptop – Internet Anywhere**) is a life savor. This allows different SMTP servers be used depending on location.

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 – An obnoxious privacy intrusion is the insertion a one-pixel image in HTML mail. When you read the message the browser has to go to the referenced URL to retrieve it. This allows the sender to monitor when and if mail is read.

8.4 USENET

Most ISPs provide access to USENET news. News 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 or in Verizon's case they require both.

> ***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.

8.5 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.

8.6 Multimedia

Internet multimedia was 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 their work is used. Online distribution of content is in its infancy. Broadband distribution obsoletes many existing business models.

8.6.1 ITunes

Apple's Itunes music service has been a popular complement to the IPOD as a way to purchase and play digital music.

8.6.2 Music Match Player

MPEG MP3 compression provides near CD-quality audio at 128 kbps, about a tenth uncompressed data rate. MP3 has become a 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 and burn music CDs.

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.

8.6.3 Real Audio Player

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

Streaming is different then downloading in that information is used before it is entirely transferred. Streaming players use a several second elastic buffer. When play is started playback is delayed a short time allowing the buffer to fill. The buffer isolates playback from temporary differences in transfer speed. If data slows down, the buffer is able to feed the player. If data arrives faster then it is being used the buffer expands to store it.

8.6.4 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.

8.6.5 QuickTime

Apple QuickTime is a popular movie-encoding format.

8.7 Printer

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 document distribution. This White Paper is a perfect example. It was composed on a computer, uploaded to a web server and is directly viewable on the web or printed as hard copy.

We use a HP 2000 professional Inkjet printer and a HP JetDirect 300X print server. This allows any PC on the LAN to use the printer. Many print servers are on the market. We chose the HP print server mainly to minimize potential compatibility problems. The printer driver runs locally on each PC. 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 lock down the server’s address. The router allocates the same IP address based on Ethernet MAC address. This locks down the address of the print server without having to manually configure it with static IP address.

8.7.1 Portable Document Format (PDF)

Printing documents on different printers can be a challenge since margins and fonts differ. The Adobe PDF format has become the industry standard for print document formatting. I use CutePDF Writer to convert MS Word documents to PDF format.

8.8 Scanner

A flat bed scanner converts documents and photographs to digital images. These files can be faxed or incorporated into documents. Optical Character Recognition (OCR) software converts text images to format understood by work processors.

The scanner is an Umax 2200 using USB to connect to the computer. It also functions as a poor mans copying machine allowing scanned images be printed to the network printer.

We wanted to network the scanner. This proved impractical since the scanner needs to know where to put scanned images. Without user intervention files are named with a sequence number. The solution was to connect 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.

8.9 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 dramatically reducing size 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.

8.10 Fax

Originally we did not want to use fax at all, preferring to interact with clients via e-mail or telephone. We found it very difficult to get away from fax entirely so we sought a solution that did not require a "real" fax machine or dedicated fax phone line.

For incoming fax we use free eFax fax service. Paid accounts are able to specify local phone number and send as well as receive faxes. Free accounts are assigned a random 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.

8.11 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.

8.12 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 to main office. 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, used by some broadband providers adds 8 bytes of overhead, this reduces max packet (MTU) to 1492 bytes rather then 1500. Make sure the VPN handles this correctly.

8.12.1 IPsec vs SSL

IPsec is a very robust way to provide telecommuters remote access to corporate LAN. With IPsec it is as if the employee was sitting in the office. The down side is IPsec requires a dedicated client on the user’s machine. For less demanding use many companies are opting to use Secure Sockets Layer (SSL) to provide limited remote access. SSL is the same security scheme used to access secure e-commerce web sites. While SSL is not as powerful as IPsec all browsers support SSL, eliminating the need for special client software.

9 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.

9.1 Security Patches

For Machines running Windows the Microsoft Windows update tool 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.

9.2 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.
- If possible don't run public servers on your LAN, let the hosting service do it
- Ban dialup modems on networked PCs. They are a potential backdoor to your LAN

9.3 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. See **Section 9.4 Phishing**.
- 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 helpful but it 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.

9.4 Phishing

Phishing is a relatively new term in the ongoing battle against viruses and scams. Phish email looks like it originated from a legitimate company. The email typically states the recipient needs to "log in" to the corporate web site and review and update account information. Everything looks legitimate except, using various subterfuges, the site is bogus. It looks like the real one but it is actually controlled by the attacker. The goal of Phish attack is to obtain user account data so the attacker is able to masquerade as the user.

9.5 Eavesdropping

Radio communication is easy to eavesdrop. An attacker can locate a safe distance without compromising physical building security. An attacker can cause a Denial of Service DoS) attack and if account names and password are sent in the clear they can be harvested by monitoring network traffic. This threat was recognized during development of WiFi wireless LANs. Provisions were made for authentication and encryption to maintain privacy called Wireless Equivalent Privacy (WEP)

Unfortunately security researchers quickly discovered serious shortcomings in WEP. Weakness managing the encryption key makes it relatively easy to determine the key thus breaking encryption. Current state of the art for WiFi security is WiFi Protected Access (WPA). There are versions optimized for some home networks and large corporate sites.

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 office buildings where multiple tenets are in close proximity.

Wired Ethernet is less susceptible to eavesdropping then the other technologies mentioned because signaling is contained within the wiring and wiring carrying Ethernet signals does not typically exit the building. Using Ethernet switches, rather than hubs, makes eavesdropping more difficult because only traffic destined for the specific port is visible at the machine.

9.6 NAT

NAT is often considered a firewall when in fact it is not. One of the security 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. This is what gives NAT its firewall like characteristics.

9.7 Firewall

The first line of defense is to control data entering and leaving the LAN. Unless you are running a public server incoming security is easy, refuse all incoming connection requests. Our business web and mail server are hosted externally. This means ALL requests that originate outside the SOHO LAN can be refused

A firewall imposes policy 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. Many low cost Broadband routers include some form or firewall.

In some respects firewalls are overrated. A machine without active listening services is impossible to attack directly. If the host is running one or more services the firewall needs to allow incoming connection to the server. When that happens the firewall is no longer part of the security scheme. The server itself must be hardened to thwart malicious attack. Firewalls are great for keeping unnecessary traffic off the LAN and providing a secondary line of defense against incorrectly configured machines – but firewalls are not the magic bullet many people think they are.

The other common avenue of compromise is to download software. The may occur through normal download or more commonly through an email attachment. Firewalls are ineffective in this form of attack unless they respond to traffic between the malware and Internet.

9.7.1 Internet Paranoia

Assuming you are using either a NAT router or firewall the first thing you notice when examining security logs is a tremendous number of “bad” packets. Very little of this traffic is actually an attack. Most is the result of incomplete sessions and mistyped or misprogrammed addresses. Before sending off an irate e-mail to your ISP complaining about being attacked may want to take a gander at this tongue in cheek posting called: You pinged me you dog, Internet Paranoia.

9.8 Virus & Trojans

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.

9.9 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 application usage information and forward it 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.

Firewalls can be configured to block access to specific sites but that is a never-ending chore. 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. The down side is constant alerts asking whether or not to allow particular access.

Ad-Aware SE and SpyBot are two very popular freeware program used to remove various forms of spyware. They are updated periodically to detect and removes various forms of spyware.

10 Backup – Oops Protection

Having an always-on server makes it possible to use automatic online backup. On line backup is convenient so backups actually occurs. However it is not as secure as offline offsite backup. With online backup a software attack may succeed in destroying all copies of the data. If both copies are in the same location they may be destroyed in a fire.

10.1 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.

10.2 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 fire. 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, 700 MB, and cheap. CD-R life expectancy is controversial it is at least 10-20 years. That is more than adequate for our purposes but not long enough for true archival storage. If even more space is needed recordable DVDs are available.

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 is low. This turned out to be an impractical back up strategy.

For maximum safety the backup copies should not be stored at the same physical location as the computer.

11 Debug -- When Things Go Wrong

Networks occasionally fail. Good troubleshooting skills are necessary to determine the root cause of the problem. For a small SOHO network good use can be made of the diagnostic tools built into Windows and the indicators on most Ethernet devices. Hardware, software, and service vendors are also a good source depending on the root cause of the problem. Consumer items are very competitively priced, that limits how much one-on-one support the vendor is willing to provide. There are many Internet resources to help resolving issues my favorite is Broadband Reports.

Windows includes a number of command line utilities to help debug network issues. To run the desired utility go to START menu open the RUN dialog box, enter “command,” press OK. This opens the command prompt, also called the DOS box. The run the command type the command and any command line switches at the prompt then press return.

11.1 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 off 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 Cat5e or Cat 6. 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.

> ***Debug tip*** – If cabling is not terminated correctly end-to-end continuity may exist but pairs miswired, causing a split-pair. Often a cable with split pair will operate at 10 Mbps but will fail at 100 Mbps.

> ***Debug tip*** – Normally a computer is connected to a Hub or Switch using a straight through patch cable. When connecting like devices say PC-to-PC or Switch-to-Switch a crossover cable or uplink port is used. Some newer devices include auto-sensing ports eliminating the need for crossover cables. If ports are mismatched the link will not work.

11.2 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
```

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.
```

11.3 Traceroute

Traceroute determines round trip time to each hop between the user and the remote host. This information is useful to determine the underlying cause of slow Internet response or unavailable hosts. Traceroute uses the Time To Live (TTL) field causing 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. Traceroute 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, in that case Traceroute or Ping return a timeout for that hop.

Windows includes a command line Traceroute 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]
```

11.4 NET

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

11.5 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
```

11.6 NBTSTAT

NBTSTAT displays protocol statistics and current TCP/IP connections using NBT(NetBIOS over TCP/IP).

```
NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-s] [S] [interval] ]

 NBTSTAT -a   Lists the remote machine's name table given its name.
 NBTSTAT -A   Lists the remote machine's name table given its IP
              address.
 NBTSTAT -c   Lists the remote name cache including the IP addresses.
 NBTSTAT -n   Lists local NetBIOS names.
 NBTSTAT -r   Lists names resolved by broadcast and via WINS.
 NBTSTAT -R   Purges and reloads the remote cache name table.
 NBTSTAT –S   Lists session table with the destination IP addresses.
 NBTSTAT -s   Lists sessions table converting destination IP address
              to host names via the hosts file.

 RemoteName   Remote host machine name.
 IP address   Dotted decimal representation of the IP address.
 interval     Redisplays selected statistics, pausing interval seconds
              between each display. Press Ctrl+C to stop.
```

11.7 IPCONFIG

IPconfig displays IP settings for each adapter. The first adapter (0) is the Virtual Point to Point Protocol (PPP) adapter for dialup networking. The second adapter (1) is the Ethernet NIC

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. Interface 1 is set up for DHCP allowing automatic allocation of IP parameters. The last two lines show when the lease was obtained and when it expires.

```
C:\WINDOWS\Desktop>ipconfig /all

Windows 98 IP Configuration

        Host Name . . . . . . . . . : Tom-Desktop
        DNS Servers . . . . . . . . : 192.168.2.3
        Node Type . . . . . . . . . : Broadcast
        NetBIOS Scope ID. . . . . . :
        IP Routing Enabled. . . . . : No
        WINS Proxy Enabled. . . . . : No
        NetBIOS Resolution Uses DNS : Yes

0 Ethernet adapter :

        Description . . . . . . . . : PPP Adapter.
        Physical Address. . . . . . : 44-45-53-54-00-00
        DHCP Enabled. . . . . . . . : Yes
        IP Address. . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . :
        DHCP Server . . . . . . . . : 255.255.255.255
        Primary WINS Server . . . . :
        Secondary WINS Server . . . :
        Lease Obtained. . . . . . . :
        Lease Expires . . . . . . . :

1 Ethernet adapter :

        Description . . . . . . . . : SMC EtherPower II 10/100 Network
Driver
        Physical Address. . . . . . : 00-E0-29-35-70-1E
        DHCP Enabled. . . . . . . . : Yes
        IP Address. . . . . . . . . : 192.168.2.4
        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. . . . . . . :  2 07 06 7:28:44 AM
        Lease Expires . . . . . . . :  2 10 06 7:28:44 AM
```

11.8 Route

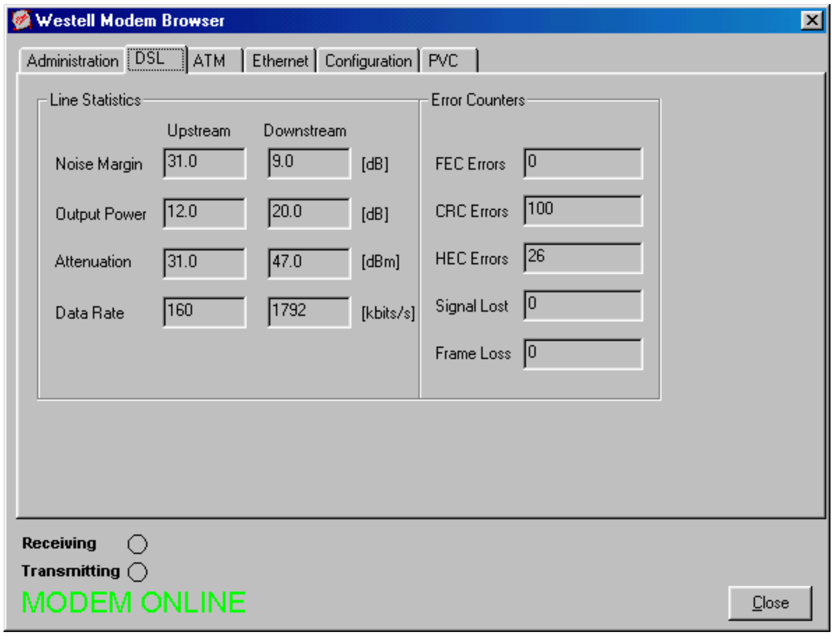
Route is a command line utility to display and manipulates network routing tables.

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
```

11.9 Modem Statistics



Line Statistics

	Upstream	Downstream	
Noise Margin	31.0	9.0	[dB]
Output Power	12.0	20.0	[dB]
Attenuation	31.0	47.0	[dBm]
Data Rate	160	1792	[kbits/s]

Error Counters

FEC Errors	0
CRC Errors	100
HEC Errors	26
Signal Lost	0
Frame Loss	0

Receiving ○
Transmitting ○
MODEM ONLINE

Figure 24 Westell ADSL Modem Statistics

The device directly connected to the first-mile network often has to ability to report low-level connection statistics. This is a powerful diagnostic aid since it measures the condition of the physical interface not just end-to-end performance.

The Westell Verizon ADSL diagnostic utility must connect directly to the ADSL modem, it does not work through a router. That is a simple matter of temporally swapping Ethernet cables to run the test.

The display shows sync speed matching the marketed ADSL rate of 1500/128 and adequate noise margin. 6 dB is the minimum acceptable ADSL noise margin. The error counters show minimal errors for the number of packets logged (different screen) by the modem.

11.10 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. First step is determining if the problem is the LAN or Internet.

LAN Debug

- Are all PCs 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 AutoIP address. This address is different than private addresses used on the LAN preventing intercommunication.
- Ping machines on the LAN by Network name and IP address. This verifies internal Windows name resolution and the TCP/IP stack is working correctly.
- Attempt to access the router configuration page or the PC running connection sharing. If it does not respond but other machines do the problem is likely the router.
- If networking looks really broken try pinging local loopback address 127.0.0.1. This tests the local IP stack, and works even it the machine is not connected to a LAN. If this does not work make sure the NIC is bound to TCP/IP. If configuration is correct try deleting and reloading TCP/IP stack.
- If some PCs do not show up in Network Neighborhood see**:**
- **Share Files** in My Network Places

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.
- Ping a stable site like Broadbandreports.com that does not block ICMP Echo (Ping). If Ping cannot resolve the host name you may be experiencing a temporary DNS problem. Try Pinging the site by IP address. As of 12/2004 Broadbandreports.com address is: 209.123.109.175. If that works you have identified a DNS problem. If the site is not accessible by address there is a bigger problem.
- Perform a Traceroute (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.
- Access the modem log to see it the problem exists with the first mile connection itself.
- If you have DSL or dialup and are experiencing slowness, 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 or dialup.
- Sites like Broadband Reports have tools to continuously monitor connection quality.

Remember Internet access problems may be caused by: your computer, your LAN, your router or ICS, your first-mile connection, internal ISP routing, Internet backbone, the ISP connected to the remote host, the remote host LAN and lastly the remote host itself. The trick its to quickly determine which link in the chain is the cause of the problem.

12 Power Distribution – Untangling the Mess

Electronic devices 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.

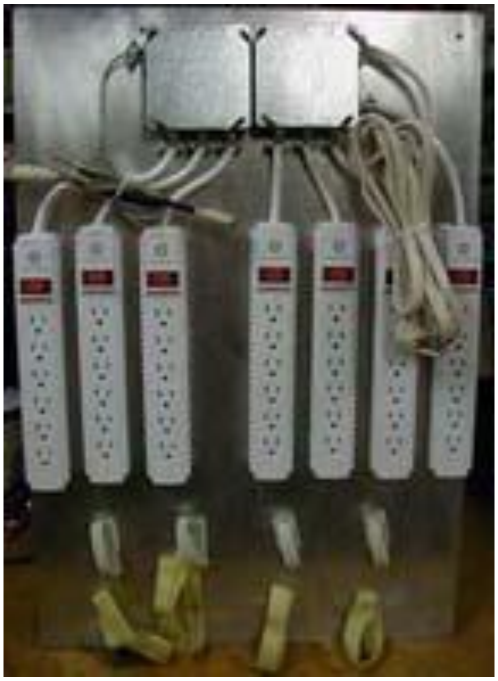


Figure 25 Power Panel

Power Panel requirements

- Multiple always on receptacles
- Multiple switched receptacles controlled by workstation
- Wire routing provisions
- Mounting provisions for “wall wart” 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.

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.

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

13 Laptop – Internet Anywhere

We use a laptop at our home office, in the office and while traveling. This means it needs to connect to multiple networks. For meeting we often set up an ad hoc isolated network to exchange files among the participants. 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 is a program called NetSwitcher. 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	SOHO network printer	Office 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 NetSwitcher FAQ describes how to create customer controls using the registry editor: REGEDIT, to extract registry entries and create scripts. This works well to create custom controls. The 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.

14 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.

14.1 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 first-mile Internet connection. Even companies with only dialup Internet access can have a web 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 cost. Our site only costs $10 US a month. We use a local hosting service INR.NET to host our site.

For a large site it may be advantageous to use a hosting service but provide your own equipment. This is 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 virtual 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. My daughters' site is an example if this type of site.

14.2 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 also an option for personal sites. Most residential broadband services are asymmetric; upload is much slower than download. This limits 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 DynDNS minimizes this problem. The DNS service is updated each time the server's address change. This works well for personal sites but the site will be temporally inaccessible during address update making it inappropriate for serious commercial use.

14.3 Registering a Domain Name

A domain name establishes a business identity and decouples your business from ISP and hosting service. With a registered domain changing service providers or hosting service is transparent to customers.

The first decision is 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 proposed 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.

14.3.1 Email

With a registered domain email is addressed to the domain, not the ISP. This personalizes your businesses web persona. Hosting services typically provide 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. This enables employees' access individual accounts without the need to run an internal mail server.

14.4 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

```
Registration Service Provided By: ITZA Company, LLC

Domain name: tschmidt.com

Registrant Contact:
   Schmidt Consulting
   Tom Schmidt ******@tschmidt.com)
   +1.6036732463
   Fax: +1.9282234815
   95 Melendy Rd
   Milford, NH 03055-3417
   US

Administrative Contact:
   Schmidt Consulting
   Tom Schmidt ******@tschmidt.com)
   +1.6036732463
   Fax: +1.9282234815
   95 Melendy Rd
   Milford, NH 03055-3417
   US

Technical Contact:
   NA
   LLC InterNet Resource NETworks ****@INR.NET)
   +1.6038808120
   Fax: +1.6038808783
   443 AMHERST ST STE 122
   NASHUA, NH 03063-1223
   US

Status: Locked

Name Servers:
   NS1.INR.NET
   NS1.ITZA.NET
   NS2.INR.NET
   NS2.ITZA.NET

Creation date: 04 Nov 1998 00:00:00
Expiration date: 03 Nov 2006 00:00:00
```

14.4.1 Administrative

Administrative information records data about site ownership and contact.

14.4.2 Technical

Technical information records data about network operation center contact.

14.4.3 Nameservers

Nameservers' listed in the Whois database are the authoritative servers for your domain. These are the servers used by DNS to a domain name to IP. The registrar does not maintain information about the site itself, simply an address pointer to the nameserver that does. Registrars require two nameservers, primary and backup. Ideally servers are in separate locations served by different providers. This minimizes risk the site authoritive nameserver become inaccessible.

14.5 DNS Record

Once the domain is registered nameserver records must be created. These records provide the translation between friendly 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. Below are commonly used record types. The DNS Stuff web site has a number of useful utilities to verify DNS is set up correctly.

14.5.1 Address Records (A)

Address records map host name to IP address.

14.5.2 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.

14.5.3 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.

14.5.4 Pointer Records (PTR)

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

14.5.5 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.

14.5.6 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)

14.6 Creating a Web Site

Creating a web site requires a combination of artistic 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 more complex sites 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.

14.7 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.

14.8 Robots

Search engines make it easy to find information on the Internet by indexing and cataloging information. Search engines perform this task by using search bots, called spiders, to traverse Web hypertext structure. Spiders periodically visit millions of sites to maintain an up to date index of billions of web pages.

An informal Internet standard has been developed to control the actions of these search engine spiders. When the spider first connects to a site it looks in the root directory for the file robots.txt. The purpose of robots.txt it to tell well behaved spiders, which web pages they are not supposed to index. Even if the site does not intend to prevent spiders from indexing pages it is a good idea to place a null robots.txt file in the root directory. This eliminates numerous entries in the server's error log about access to a non-existent file.

14.9 Server 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 has been 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 necessary components are readily available but assembling the knowledge to create and troubleshoot it 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 pretty straightforward and easy to fix once the root cause is determined. However, determining cause is not always easy. Help is available from many sources. Manufacturer-sponsored forums and specialized home network interest groups provide problem isolation and resolution help.

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