Living with a Small Office Home Office (SOHO) Network

2008 Edition

Tom Schmidt
Schmidt Consulting
Revised 12 January 2008
tom@tschmidtdotcom
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 enables multiple computers to share the connection. Fast Ethernet (100 Mbps) switched LAN provides high-speed internal communication. LAN services include: file backup, network printing, NNTP timeserver, DNS server, Syslog log file server and local private web server.

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 task of securing local network.

After several years of minimal change we have gone through major revamping this year replacing just about everything except wiring.

Table of Contents

1 Overview

In mid 1998 I set up a home network. 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.

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 replaced dialup as the Internet connection. Initially we used Wingate connection sharing software and BlackIce Defender for intrusion detection running on a dedicated laptop to share dialup connection. When we got DSL laptop was replaced with a MultiTech router connected to DSL modem. That has since been replaced with a Netopia (now part of Motorola) 3346 DSL/Router. A recycled desktop serves as a poor mans server. In addition to file sharing it runs: TreeWalk DNS resolver, Tardis network time service, Abyss local web server and Kiwi 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 be shared by workstation and server. Having a KVM make it easy to temporally connect additional systems for setup and testing. A HP 550 ink jet printer is networked and accessible from any PC on the LAN.

Traveling with a Laptop can be a challenge: as network configuration differs at each location. NetSwitcher automates this task providing one click switching between locations.

We use Acronis for automatic on line back up to the server. A CD/DVD 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 quickly becomes 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. Products and services described in this paper represent my choice to deliver the features I need.

Goals for SOHO network:

- Share broadband Internet service
- Share Printer
- Local file sharing
- Local internal web server
- Secure remote access to corporate network
- Access multiple e-mail accounts
- Access to USENET newsgroups
- Fax without a fax machine
- Automatic time synchronization
- Automatic file backups
- Display home weather station data
- Learn networking

This paper discusses Internet access and connection sharing options. Even a small network benefits from having an always-on server. Structured wiring techniques for telephone and Ethernet are covered in detail. Security and Troubleshooting topic helps maintain network and protect it from intruders.

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

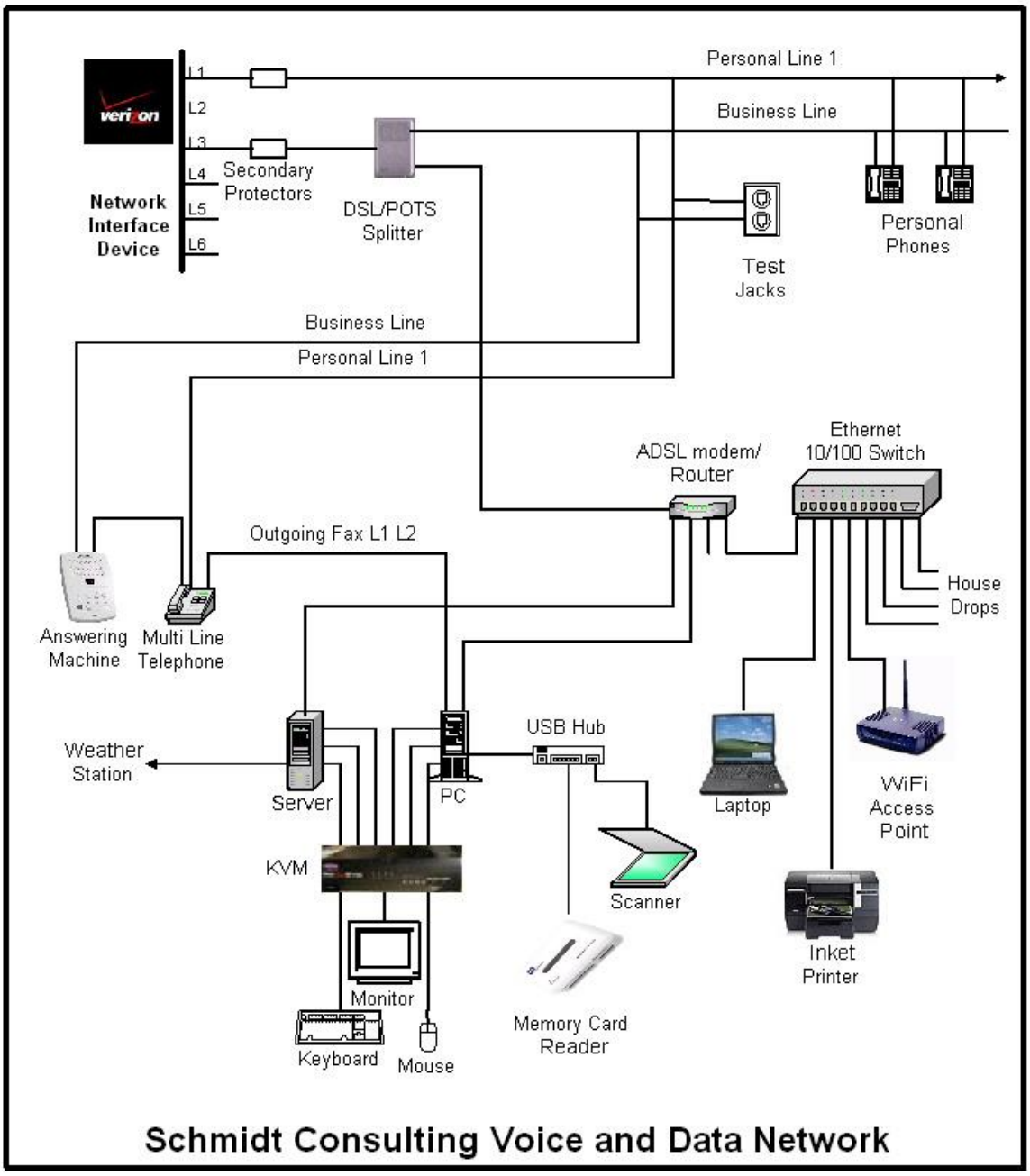


Figure 1 SOHO Data and Voice Block Diagram

2 Internet – Much More Than World Wide Web

The Internet began life 40 years ago as a means for government and academics to share expensive mainframe computers. Today it is the preferred method used to access all sorts of digital media: data, voice and images. Internet is a contraction of Inter Network, literally a network of networks. Creation of the Word Wide Web in the 1990's vastly expanded Internet popularity by providing a Graphical User Interface (GUI) on what 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

Internet Service Providers (ISP) connect end users to the Internet. Internet popularity is driving demand for high-speed low cost service. High-speed Internet access 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 rent copper phone line to deliver DSL. We currently have 1500/384 kbps ADSL service provided by Verizon On Line.

For a more detailed examination of ISPs interested reader it referred "First-Mile Access" paper on the writings page.

2.2 Services

The Internet transports data from one host to another over a common network shared by many other users. New comers often equate the World Wide Web (WWW) with the Internet. WWW is simply one of many Internet services. WWW uses HTTP, Hyper Text Transport Protocol to display web pages.

Other popular services:

DNS - Domain name system acts as an Internet directory service translating host names to IP addresses.

FTP - File Transport Protocol an efficient protocol used to exchange files.

IGMP - Internet group management protocol enables a single server to simultaneously send data to many users, much like over the air transmission.

Instant Messaging - is a popular digital information exchange protocol that allows people to conduct real time chat sessions.

IPTV – is a collection of protocols and services to deliver TV/movies over the Internet. IP radio is already popular. Lack of high-speed first-mile service and concerns over copyright in a digital world are limiting deployment of IPTV. As first-mile access speed increases it will be possible for anyone to deliver "cable TV."

NNTP - Simple Network News transfer protocol is the bases for Usenet

POP - Post Office Protocol and SMTP Simple Mail Transport Protocol provides email services. IMAP, Internet Message Access Protocol is an advanced email format used by some ISPs.

SIP – Session initiation Protocol is used to setup and teardown Internet phone calls. RTP – Real-time transport Protocol is used to deliver packetized voice.

SNTP – Simple Network Time Protocol distributes accurate time information.

VoIP – Voice over IP is an emerging technology that uses packet based Internet transport for telephone calls. This is part of digital convergence using the Internet to carry many different types of traffic as opposed to creating a purpose built network for each service.

2.3 Latency vs Speed

Non technical folks often confuse latency with speed. Latency is how long it takes a packet to get from location A to B. Speed is rate bits are transmitted across the network. A useful analogy is the think of a truck full of DVDs going from Point A to B. From the time the truck begins its journey latency is high – while truck travels to the destination recipient can do nothing. However once it gets there speed is very high due to the tremendous capacity of the DVDs.

Conversely a dialup connection has low latency since data arrives milliseconds after it is requested. Speed on the other hand is low – limited by switched telephone network performance. For a more in-depth explanation see "It's the Latency Stupid."

2.4 Naming Convention

Domain names provide a friendly handle to access a resource rather than using IP addresses directly. Domain names are hierarchal evaluated right to left. The highest-level of the tree called Root is implied. Next is 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.

2.4.1 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. Windows name resolution looks in the Hosts file to see if 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 host is not found the translation request is passed to the DNS Resolver.

Lets trace what happens when we looking up www.google.com. Since the request is not local 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 Resolver is preprogrammed with the IP address of several root nameservers. The request goes to one of the root nameservers that 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 quired for the address of Google nameserver. The server returns the address of the authoritive nameserver for the Google domain. It is important to note root nameserver does not know address of any Google servers other then the Google nameserver. The Google nameserver is then asked for the address of the desired host and 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. This is a very superficial view of how DNS works. For a more in-depth view see DNS Complexity by Paul Vixie.

Obviously going thought this multistep process each time one needs to translate a URL is rather time consuming. To speed up the process DNS resolvers cache recently used information. DNS records have a time to live (TTL) parameter indicating how long cached information may be used before it must be refreshed. Name lookup is normally accomplished in a few milliseconds.

2.5 Routing

Internet is a routed network. This is very different then the broadcast discovery scheme used locally by Ethernet or circuit switching used by the legacy telephone network. When a computer wants to communicate with a resource not available locally it forwards the packet to a gateway router. Routers forward incoming packets to the proper destination or to the next router in the chain. To learn network topology 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.

2.6 Multicast

Most Internet traffic is 1:1 (unicast); a host communicates directly with another host. Multicast emulates traditional broadcast 1:many. This is more efficient way to stream information to many endpoints. Unfortunately even though specifications exist to support it not many ISPs have implemented multicast. In general if you listen to Internet radio or TV it is being done over unicast.

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) metrics 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.

2.8 TCP Slow Start – Receive Window – et al

When a host begins transmission it has no idea how fast the intervening links are between it and remote host. To address this issue transmitter begins sending a few packets waiting for acknowledge. The faster ACK arrive the more packets the transmitter sends per unit of time.

2.9 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 need for a DHCP server. DHCP has been extended to allow automatic configuration if host cannot find a DHCP server. In that case 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 host 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 to 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.

2.9.1 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.

2.9.2 Subnet

IP addresses consist of Network-Prefix and Host address. Subnetting allows IP addresses to be assigned efficiently and simplifies routing. The subnet mask defines boundary between network and host portion of address. Hosts within a subnet communicate directly with one another. Hosts on different subnets use routers to forward packets from one subnet to another.

In our network all computers are on a single 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.

2.9.3 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 a 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 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.

2.9.4 Port Number

Internet 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 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.

2.9.5 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. Internal hosts 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 Internet hosts. This eliminates 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 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.

2.9.6 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 at random 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.

2.9.7 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.

2.9.8 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)

2.9.9 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 a mechanism to learn MAC address associated with a particular IP address. Reverse ARP (RARP) determines if an IP address exists for a particular MAC address.

2.10 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

ARP – Address resolution protocol is used to translate IP address to Ethernet MAC address.

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 root, then 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.

DUN – Dial Up Networking is a suite of tools to allow a computer to access an ISP over low speed dial up link.

FTP – File transport Protocol

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

HTTP – Hyper Text Transport Protocol – used to exchange Web data.

ICMP - Internet Control Message Protocol, handles control function such as PING. PING verifies a remote host is reachable and how long it takes.

IGMP – Internet group management protocol enables a single host to communicate with multiple computers emulating the one-to-many broadcast of over the air transmission.

IM - Instant messaging is a very popular digital information exchange protocol allowing many users to interact in real time chat sessions. Unfortunately IM has evolved outside the IETF standards process with each vendor creating incompatible formats and jealously preventing interoperability.

IMAP – Internet Message Access Protocol

IP – Internet Protocol

IPv4 – Current Internet protocol. A 32-bit address is 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 increases the address space to 128 bits, eliminating the current addressing shortage and opening to door to new applications.

MAC address – 48-bit Ethernet end point address assigned by Ethernet hardware vendor. MAC address is split into two portions, vendor ID (assigned by IEEE) and serial number identifying the specific device.

NAT – Network Address Translation is used to translate one set of IP addresses to another. NAT is used extensively on small residential networks allowing multiple hosts access a single ISP account while using only one public IP address. Network Address Port Translation (NAPT). 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.

NNTP – Network News Transfer protocol.

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

POP – Post Office Protocol

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. Private addresses are not assigned to hosts on the public Internet. This allows the addresses be reused multiple times.

QoS - Quality of Service treats packets differently based on latency requirements.

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

Router – Interconnects two or more networks. Makes forwarding decisions based on destination IP address.

RTP – Real-time transport Protocol is used to deliver packetized voice.

SIP – Session Initiation Protocol is used to set up and tear down Internet phone calls.

Slow Start – TCP control mechanism to address congestion and slow network links.

SMTP – Simple Mail Transport Protocol

Sub Domain – lowest level in 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 receiver has to fake the missing information.

URL - Uniform Resource Locator, human readable host name.

VoIP – Voice over IP Use packet technology to carry voice calls rather then traditional circuit switching.

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.

3 Local Area Network (LAN) – Networking for Everyone

Local Area Network (LAN) allows computers to access shared resources such as printer, files, and the Internet. Ethernet, both wired and wireless, dominates SOHO network market.

3.1 Ethernet

Wired Ethernet IEEE 802.3 is the most common local network technology in use today. It was initially 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 more then one person may start talking at the same time. That is a collision; no one is able to 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 odds 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 operated at 10 Mbps and used fat coax cable with clamp on taps, called vampire taps. Early development focused on improving physical interconnection rather then speed. Specification evolved from Fat coax, to thin coax to twisted pair. Today most common type of Ethernet is unshielded twisted pair (UTP) copper cable consisting of 8 conductors organized as 4 pairs terminated with 8 conductor modular jacks similar to those used for telephone wiring. Since its inception speed has dramatically increased from 10 Mbps (1980) to 100 (1995) to 1G (1,000 Mbps) (1998), 10G (2002) work is under way on 40G and 100G Ethernet. Ethernet Switches have replaced hubs eliminating collision domain permitting full duplex operation.

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

3.1.1 Media Access Controller (MAC) Address

Each Ethernet interface (wired or wireless) 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. MAC vendor ID is assigned by IEEE.

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.

3.1.2 Virtual LAN (VLAN)

Virtual LAN technology allows the same physical LAN to connect multiple computers while isolating one group from another. Typical use is to create separate VLANs based on community of interest for example

payroll, marketing and engineering. A router is used to 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).

3.1.3 Universal Plug and Play

UPNP is an outgrowth of PC plug and play experience designed to automatically configure local network devices. As this paper should make clear configuring a LAN can be a daunting task requiring user to be conversant with network terminology and concepts. UPNP provides automatic discovered and when needed request firewall/router to adjust configuration to allow the particular service Internet access.

Unfortunately UPNP makes no provision for security so one has no knowledge or control of malicious devices attempting to gain unauthorized access to the Internet. If you are unfamiliar with network configuration and confident PCs have not be compromised then UPNP is very convenient. On the other hand if you are comfortable configuring network devices doing so manually improves security.

3.2 Wired Ethernet

Modern digital networks are packet based. Ethernet "packets" are called frames. Data is divided 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. When Gig Ethernet was developed the spec allowed larger frames, 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.

3.2.1 10 – 100 – 1,000 – 10,000 – 100,000 Mbps

Initially UTP Ethernet operated at 10 million bits per second (10 Mbps) over Category 3 UTP wiring. Ethernet development has been in 10X increments. Fast Ethernet increased speed to 100 Mbps over Category 5 wiring. Gigabit Ethernet increased speed another 10 times to 1,000 Mbps. During Gigabit Ethernet development the Cat 5 specification was tightened resulting in Cat5e. The fastest version of Ethernet, 10 Gigabit (10,000 Mbps), has recently been modified to work over Cat 6a. Prior to that 10G required fiber. Work is under way on 100G. Given the high speed it is unlikely to operate over UTP, most likely some form of short distance coax.

3.2.2 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 originally 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 to 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 passes 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 speed improvement will be somewhat less 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 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 prices have come down dramatically making hubs obsolete while dramatically improving LAN performance.

Gig Ethernet NICs and Switches are almost at price parity with Fast Ethernet. 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. Typical PC file transfer speed when used with Gig Ethernet is typically limited to 300-400 Mbps. The limitation is Disk speed, O/S overhead, and PCI throughput.

3.2.3 Managed vs Unmanaged Switches

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

3.2.4 Automatic Link Configuration

To make Ethernet easier to use higher speeds are backward compatible. Transceivers Autonegotiate link characteristics to determine speed and whether connection is half or full duplex. Hubs are half duplex as only one device can be transmitting at a time. When connected to a switch a device is capable of transmitting and receiving at the same time – full duplex.

NIC (computer interface) is configured as uplink port (MDI), Hub or switch as MDI-X. 10 and 100 Mbps Ethernet use one pair for transmit and one for receive, Gig and 10 Gig use all four pair in each direction. Default configuration assumes MDI port is connected to MDI-X port. Having NICs wired as MDI and hub/switch as MDI-X means that in most cases interconnect is a simple 1:1 cable.

Problems occur when like devices are connected, say NIC to NIC or hub/switch to another hub/switch. To make this easier hubs/switches typically have an uplink switch or port. The uplink port reverses normal TX/RX configuration so another like device can be connected. The same effect can be obtained by using a crossover cable. Cross over cable swap TX and RX pair at one connector. Recently vendors have adopted Auto-MDIX to automatically determining remote port type and configure ports automatically. With Autonegotiation (Speed) and Auto-MDIX (gender) Ethernet has become more user friendly. All user need do is connect the cable everything else is automatic.

3.2.5 Topology

For maximum performance a single wide Ethernet switch should be used to serve the entire LAN. Cascading switches is transparent to traffic but limits inter switch speed to that of the link. With a single wide switch throughput is dictated by internal switch backbone performance.

3.2.6 Spanning Tree

Ethernet is designed such that one and only one path exist between any two endpoints. If multiple paths exist switches are unable to determine how to forward frames. Spanning Tree protocol was developed to address problem of multiple paths in complex networks. The protocol detects duplicate paths and turns off redundant paths. Spanning Tree requires managed Switches – low cost unmanaged switches do not implement the protocol. Spanning Tree is typically not an issue in simple SOHO LANs.

3.2.7 Power over Ethernet (PoE)

Until recently wired Ethernet delivered data but not power. Each device needed to provide its own power. For traditional "large" networked devices such as computers this was not a limitation. However as more and more low power Internet appliances such as WiFi Access Points and Voice over IP (VoIP) telephones were deployed benefit of delivering both data and power over the same cable became obvious.

IEEE took on the challenge and in 2005 released PoE specification. PoE provides 13 watts of power per device. The spec injects power two ways. For 10 and 100 Mbps Ethernet PoE uses the two unused pair. Gig uses all four pair so power has to be injected into the active pairs. IEEE 802.3at is currently working on a higher power version of PoE to increase power up to about 30 Watts.

PoE has been a boom for low powered devices. It also facilitates backup power, as UPS only needs to feed PoE Switch (or power injector) rather then every device.

3.3 Wireless Ethernet (WiFi)

Great strides have been made creating high performance low cost wireless LANs. RF technology is at its best where mobility is of paramount importance with bandwidth less so. WiFi radios operate in the unlicensed Industrial Scientific Medical (ISM) band. WiFi popularity has a down side. As more devices attempt to use limited frequency allocation interference problems increase. Government regulators are addressing interference by designating more bandwidth for unlicensed use. Standards bodies are working to facilitate peaceful coexistence between various devices.

IEEE 802.11 radios operate in two modes ad hoc peer-to-peer and managed. Managed mode requires an Access Point to bridge wireless network to wired network. Depending on size and type of construction a site may require multiple Access Points.

The success of various IEEE 802.11 Wireless standards has encouraged many vendors to enter the market. The WiFi Alliance works to insure interoperability between different vendors and promote use of Wireless LANs.

3.3.1 2 – 11 – 54 - 250 Mbps

Initial version of IEEE 802.11 delivered 2 Mbps in 2.4 GHz ISM band. 802.11b increased speed to 11 Mbps, 802.11g increased speed to 54 Mbps. 802.11a operates at 54 Mbps in the 5 GHz band. The much hyped 802.11n operates at 250 Mbps. Due to the way over-the-air transmission operates real world transfer speed is limited to about half raw transmission speed and often significantly lower.

3.3.2 Security

Wireless LANs are inherently less secure then wired. An intruder does not require a physical connection, but can eavesdrop while some distance away. The original 802.11 designers were aware of this risk and incorporated Wireless Equivalent Privacy (WEP) into the 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 enhanced implementations are available. The WiFi Alliance Security WiFi Protected Access (WPA) is current state of the art for wireless security. There are different versions optimized for residential and commercial customers. Netstumbler is a useful tool to help secure WiFi LANS.

3.3.3 Interference

WiFi radios operate in unlicensed bands so interference is a problem, especially in congested urban areas. Interference is the result of other WiFi radios, non WiFi radios operating in the same band such as Bluetooth and wireless phones and unintentional radiators such a microwave ovens.

The WiFi alliance has published numerous whitepapers on the subject. They are working with various standards bodies to make devices more aware of their RF environment by probing for other radios operating in the vicinity. Device use that knowledge to set operating channel and power to minimize mutual interference. Given the tremendous popularity of this technology governments are working to increase frequency allocation for unlicensed radio use. As radios get smarter and frequency allocation increase interference should become less of a problem.

3.4 Alternatives

Ethernet, wired and wireless, is the dominant LAN technology. The cost of installing network wiring is modest if done when 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 typically operate at lower speed than wired Ethernet but have the advantage of not requiring additional wiring.

It is a testament to Ethernet's popularity these alternatives all use modified Ethernet frames, adapted to the physical medium, making it easy to bridge to standard Ethernet.

3.4.1 Phone Line Networking

Home Phoneline Network uses existing phone wiring to create bridged Ethernet LAN operating at a maximum speed of 320 Mbps. This allows computers to connect 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 differences. This allows HomePNA and Ethernet devices to act as if they were connected to the same LAN.

3.4.2 Power line Networking

The HomePlug initiative provides high-speed network device that plug into ordinary AC receptacles at speeds up to 200 Mbps. The HomePlug Powerline Alliance is the clearinghouse for power line networking products.

3.4.3 Ethernet over TV Coax

An interesting new technology utilizes existing TV coax wiring to deliver Ethernet. Coaxsys and Multimedia over Coax Alliance are popularizing this technology. Many homes build in the last few decades have RJ6 coaxial cable feeding multiple TV outlets but are not equipped with Category rated cable suitable for conventional Ethernet. Verizon is using the technology to eliminate need to run both coax and UTP Ethernet when installing FIOS.

3.4.4 Ultra Wideband Radio

There are a number of emerging wireless technologies targeting so-called last-foot problem. One only has to look at the rear of typical residential TV/stereo/home theater installation to understand the problem. The mass of cabling needed to interconnect individual components and the inability of components to talk to one another hinders adoption and is at odds with ease of use. This limitation has dogged consumer electronics industry for years. The goal of Ultra Wideband and WirelessHD technology is to deliver incredibly fast data rates over a few meters eliminating need for interconnect cables.

4 Broadband Router – One Connection So Many Computers

When we first set up our network we used Wingate connections sharing software to share dialup. That was replaced with a MultiTech RF500S router used with Net-to-Net SDSL modem then later with a Westell B90 modem when we got Verizon ADSL. The main consideration was ability to fallback to dialup if DSL failed. At the time it was one of the few broadband routers that included automatic dialup fallback. This came in handy when our first broadband SDSL ISP went bankrupt. Verizon's ADSL service has been very stable so several years ago we dropped dialup account.

Recently purchased a Netopia 3346N that combines ADSL2 modem, NAT router, Firewall, and 4-port Ethernet switch in a single device. This makes access to modem stats more convenient. Before we had to temporally connect DSL modem directly to PC, bypassing router, to access stats. Now stats are a web page accessible from any PC on the LAN.

Figure 2 Netopia ADSL Router

The other reason for purchasing a router/modem combo was to experiment with newer modem that supports ADSL2 and ADSL2+. DSL market is evolving just like dialup market did. ITU has released several enhanced versions of ADSL that deliver higher speed and/or longer range. While Verizon is focused on rolling out Fiber to the Premise (FTTP) I assumed new generation DSLAM cards support ADSL2 and ADSL2+ whether Verizon chooses to market it or not. Had nothing to loose by using a newer modem, as it is backward compatible with previous generation of ADSL.

Using a router creates a clear distinction between LAN and WAN simplifying troubleshooting. The router market is extremely competitive. New routers can be had for less then $50 US and used higher end devices for similar price on eBay, which is where we purchased the Netopia router.

4.1 ADSL modem

The Netopia 3346N router has a built in ADSL and ADSL2+ compatible modem. Turns out our DSLAM only supports ADSL. Given low cost of the unit it was worth a try. Plus we are ready for ADSL2 if Verizon ever swaps out the DSLAM line card.

There are three main ways ADSL modems connect to ISP: Statically, DHCP, and PPPoE. Most business SDSL ISPs use static IP. With static customer manually enters IP setting into the router. Residential accounts typically use DHCP or PPPoE. DHCP works much the same as having a PC on the LAN. When modem powers up it searches for a DHCP server the server in turn automatically loads IP settings. Verizon uses Point-to-Point Protocol over Ethernet in our area. PPPoE works much the same as with dialup only much faster. PPPoE requires customer enter a user name and password.

Behind the scenes most Telcos use Asynchronous Transfer Mode (ATM) to transport IP packets. ATM normally requires configuring virtual circuit parameters. For Verizon VPI/VCI is 0/35 The Netopia modem automatically discovers these setting so all the customer needs to do is enter user name and password.

The modem maintains WAN connection even if it is unused for a long time making the connection instantaneously available.

We have 1500/384 ADSL residential package at about 14,000 feet from the Central Office. Once new router was set up throughput testing showed significantly higher speed. Prior to the upgrade download reported high 1300s low 1400s. After upgrade consistently reported slightly above 1500. Download speed remains the same near 384. Not sure if that was due to modem or router change but it was a nice surprise.

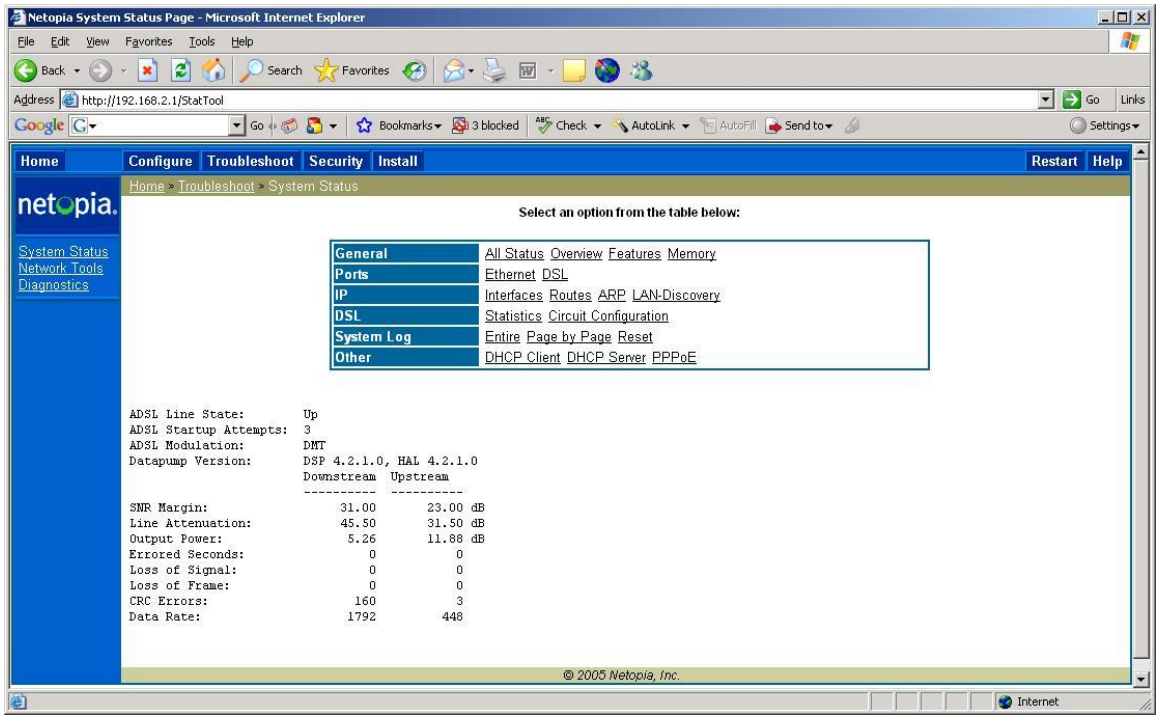


Figure 3 DSL Modem Status Page

Being able to easily see DSL modem stats is a great diagnostic tool.

4.2 PPPoE and MTU

Point-to-Point Protocol over Ethernet (PPPoE) is an encapsulation protocol. PPPoE works much like dialup PPP to connect a computer over a point-to-point link to the ISP. With PPPoE speed is that of Ethernet rather then dialup modem.

Normally Ethernet packets are limited to 1500 bytes. This is also the typical maximum size transmitted over the Internet. PPPoE adds 8 bytes of overhead to each packet reducing maximum payload size to 1492. Internet protocols are designed to fragment and reassemble over large packets presented to it. However: many residential routers do not implement fragmentation. Even when properly implemented fragmentation incurs a significant performance penalty since an over large packet is split into two smaller ones with attendant IP overhead.

A better solution is to limit packet size so fragmentation/reassembly is not required. Windows TCP/IP stack implements path discovery this automatically limits packet size so fragmentation is not required. Typical Windows maximum transmission unit (MTU) size is 1452 bytes.

A good indication of overly large packet problem is if sending a little data <1500 bytes works but larger files do not.

4.3 Network Address Translation (NAT)

Most residential broadband ISPs restrict customer to a single IP address. The limited size of IPv4 address (32-bits) space means addresses are in short supply. ISPs often charge extra if more then one address is needed. This creates a quandary; how to cost effectively connect multiple hosts to the Internet? The most common solution is Network Address Translation (NAT) using private IP addresses. IETF RFC 1918 reserved three blocks of IP addresses guaranteed not used on the Internet. Because these addresses are not used on the public Internet they can be reused multiple times.

Combining NAT and private addresses allow an unlimited number of computers to share a single Internet connection and address. Network Address Translation (NAT) translates addresses on one side to addresses used on the other. NAT offers the advantage of a proxy server while being transparent to most applications. Proxy services were used extensively prior to deployment of NAT.

Internal LAN traffic proceeds normally; NAT is not required for local traffic. When a request cannot be serviced locally it is passed to NAT router, called a gateway. The router converts private address to the public address issued by the ISP and if needed modifies port number to support multiple sessions. The router sends modified packet to remote host as-if-it-originated-from-the-router. When reply is received router converts address and port number back to that of the originating 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 Internet hosts are concerned the entire LAN looks like a single computer.

4.3.1 Performance

NAT requires 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.

Internal NAT translation tables limit the number of simultaneous sessions the router is able to maintain. This limit does not affect normal Internet usage. However when Peer-to-Peer (P2P) is used the very large number of sessions may overwhelm a low-end router.

4.3.2 Security

NAT blocks remotely originated traffic. It functions as a de facto firewall because router does not know where to forward packets that originate outside the LAN unless specifically programmed to do so.

4.3.3 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 session recovery is not possible. It interferes with server functionality and IPsec VPNs.

When NAT was first developed it was assumed private address pool was truly private and no one but the local administrator cared about local address usage. Today in the age of VPNs these internal addresses ARE being exposed to other networks. If a telecommuter's residential LAN and office network both use private addresses they may overlap. In a simple case this is not major problem, the user simply moves the LAN to a different address block. But what happens if home LAN must support multiple telecommuters?

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

4.4 LAN IP Address Assignment

Each device on the network requires a unique 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 router has the flexibility to use static, dynamic address allocation.

4.4.1 Static

When static allocation is used IP parameters: address, subnet mask, gateway address, and DNS address need be manually assigned to the computer. 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.

4.4.2 Dynamic

This is the default Windows IP configuration, at power up PC searches for a DHCP server. The DHCP server in the router assigns each machine's IP parameters. Once PC is configured it is able to communicate. The address is "leased" to the client. Prior to lease expiration client attempts to renew it. Under normal conditions the lease never expires and client IP address remains the same. If client is off network for extended period of time lease will expire. Next time computer is attached will likely receive different IP address.

4.4.3 MAC Reservation

For some devices, such as servers, dynamic addresses are inconvenient. For example binding to HP printer is by IP address, as it does not have a name. If 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 MAC address does not change device is always assigned the same IP address. This is more convenient than setting static addresses manually on each device.

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

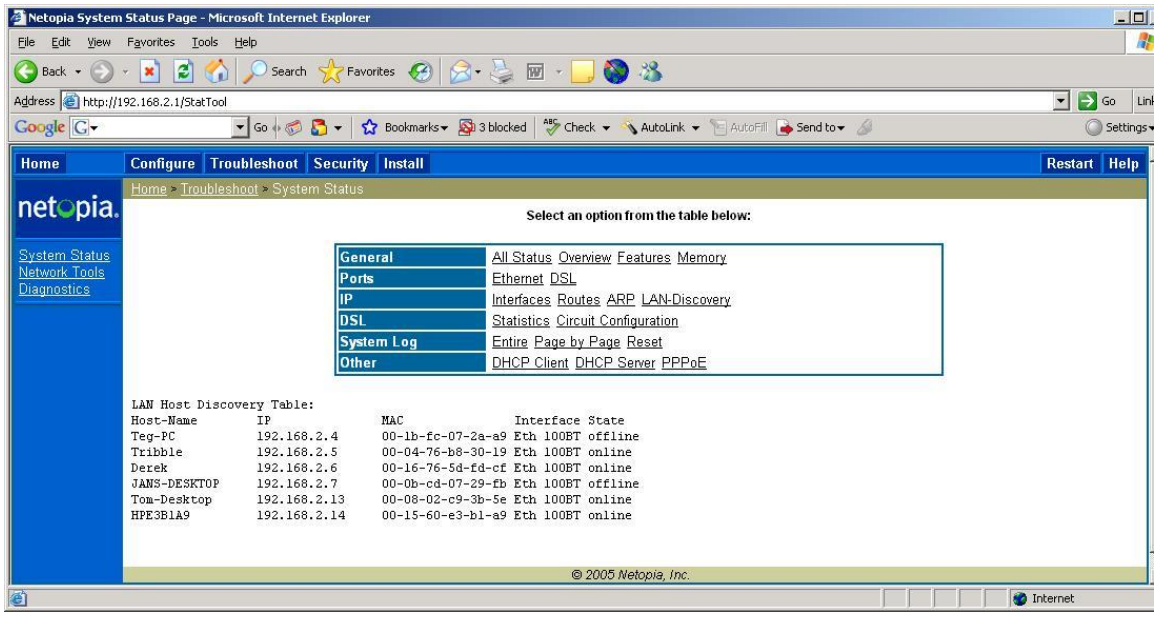


Figure 4 LAN Status Page

Status of PCs and whether or not they are active.

4.5 10/100 Ethernet Switch

The office is wired with 4 Ethernet drops fed by a 16-port 10/100 Ethernet Switch. This turned out to be inadequate so the Router's 4-port Ethernet switch comes in handy. One port feeds the 16-port Ethernet switch. The file server and office desktop connect to the switch everything else goes through the whole house switch. This increased number of office ports to 6 eliminating need to pull more wire.

Most modern Ethernet switches include Auto-MDX. The switch checks link configuration and automatically selects the correct port type depending if switch is connected to a PC or another switch. This eliminates hassle of using crossover cable or up-link ports to interconnect multiple switches.

4.6 DNS

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 run a local DNS nameserver that requires overriding the settings provided by Verizon. Unfortunately the router does not include a mechanism to point to an internal nameserver. The workaround is to manually configure DNS nameserver address in each client's TCP/IP configuration. The primary DNS address is the internal DNS server, secondary points to router in case local server is down.

4.7 Gateway

Each PC forwards 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.

4.8 Firewall

The router includes a stateful inspection firewall. This provides another layer of security by observing inbound and outbound traffic and dropping nonconforming packets.

4.9 QoS

Ethernet and the Internet were designed as egalitarian best effort services. As packets arrive at switch or router they are accepted on a first come first serve basis and either delivered to proper destination or forwarded them to next router. As long as communication paths are fast compared to offered load best effort works well. Packets arrive; they are queued for a short time then sent on their way. The difficulty occurs when packets arrive faster then they can be handled. The Internet has various mechanisms to slowdown packet inflow when nodes become congested. The sender is requested to slow down and in extreme circumstances packets are discarded.

Quality of Service (QoS) mechanisms place different values (Diffserv) on packets so when congestion occurs higher value packets are delivered as quickly as possible. Lower value packets are delayed during minor congestion or discarded during extreme congestion.

As the Internet increasing carries data with varying latency requirements efforts are under way to mark packets with a latency metric. In the event of congestion high value packets are bumped to the head of the line. For example during a Voice over IP (VoIP) phone call round trip latency should be under 150ms. Excessive delay makes carrying on a normal voice conversation difficult and with extreme delay virtually impossible. On the other hand if a print job's packet is delayed even a second other then delaying printout a little no one is likely to even notice.

Residential broadband customers are especially vulnerable to latency issues as a result of asymmetric service. Most residential service had upload as a small fraction of download. This disparity makes it easy to saturated upload path. For example TCP/IP, the protocol used for file transfer, constantly transmits acknowledgements (ACKs) back to the sender letting it know data is arriving correctly. If ACKs are delayed sender will stop sending waiting for the receiver to "catch up" or in extreme cases resend data assuming it was lost.

QoS services allow more graceful congestion degradation by moving high priority packets to the head of the queue. QoS is not a panacea, it does not create more capacity, it simply changes winners and losers.

4.10 Syslog Event Logging

The router logs 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. The router emits SysLog data to the PC server. One of the services running on the server is Kiwi SysLog. The SysLog server stores data from both the Router and Tardis Time server for later review.

4.11 Public Server Behind NAT

Running a public server behind NAT requires router to forward incoming connection requests to the appropriate server. By default incoming connection requests are discarded because router does not know which host on the LAN to forward them. 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.

4.11.1 Local Loopback

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 Hosts file Windows will use that address and not query DNS.

4.11.2 Active vs Passive FTP

The way File Transfer Protocol (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.

4.11.3 Multiple Identical Servers

Most residential broadband ISPs only allocate 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.

4.11.4 Dynamic DNS

In order for a remote user to access a server it needs to know the host name to be able to look ups its IP address. DNS assumes server configuration is static and changes only rarely and then changes are made the system administrator.

This poses a problem for residential customers with dynamic address allocation since server address may change suddenly without notice. Several services have sprung up to address this issue. Dynamic DNS services either run a small application on the router or on the server to detect when public IP address changes. When that happens the Dynamic DNS service database is notified of new address. This is not a perfect solution since there can be significant delay between address changes and when new address is available. However for most casual residential users it works well.

4.11.5 Security

Great care should be taken when running public servers. If an attacker is able to exploit a weakness in the server they gain access to the entire LAN. Once in control of a compromised serve they are free to attempt to attack other machines on the LAN. We use a hosting service to minimize security risk rather then run public server locally.

5 Local Server – Just Like the Big Kids

The server provides several network services: file sharing, DNS nameserver, NIST 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. Most recently the server has been replaced with a 1 GHz Pentium with 320 Gig drive running XP.

5.1 KVM Switch

Figure 5 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 data rate. This is typically 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 user selects a different computer. Mice cause problems because so many proprietary enhancements exist. For compatibility PS/2 mice power up in compatibility mode this allows mouse functionally even if mouse specific driver is not installed. At power up mouse device driver performs a "knock" sequence to determine if a known mouse is attached. If the mouse answers correctly the driver switches on 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 mode. This is only a problem when switching between machines. The KVM transparently passes commands from the active machine to mouse.

This problem only affects PS/2 style mice since they do not support hot plug. The USB KVM resets mice whenever a different computer is selected.

Monitor Plug and Play – modern CRT and LCD monitors communicate with PC using VESA Display Data Channel (DDC). This allows the PC to read monitor characteristics and automatically configuring video subsystem. If KVM does not emulate this feature a PC powered up on an inactive KVM port thinks it is connected to a non Plug and Play monitor reverting to low resolution low refresh mode. A workaround for this is to disable monitor plug and play and set resolution and refresh manually. Or always make sure PC is selected by KVM before booting.

5.2 File Sharing

One of the advantages of having a LAN is to facilitate file sharing between machines. Files can be shared directly between PCs or by using a dedicated file server. My Network Places (Called Network Neighborhood in some version of Windows) are organized by workgroup. In a small LAN all machines

typically belong to a single workgroup, such as HomeLAN. Once configured users are able to browse network shares, as easily as if they were on the local machine.

Getting My Network Places to work reliably in a SOHO peer-to-peer network can be a challenge as there is no Domain controller to coordinate access and provide network browse services. As each PC is turned on it looks to see if there is already a master browser on the LAN. Note this has nothing to do with web browsing. The Master browser collects information about shared network resources, directories, files and printers and makes this information available to other computers on the LAN.

Ad hoc election process can cause problems if PC running master browser gets shutdown. It takes a while for other PCs to notice there is no longer a master browser. Until new election is held it is impossible to browse the network. Depending on power up sequences it is possible to have more then one master browser, in a workgroup at a time. Masters do not exchange information. Having multiple masters will segment the workgroup resulting in non-communicating chunks.

Pchucks'n Network site has a great article about peer-to-peer browsing.

5.2.1 My Network Places

#1 File and Print Sharing Service
Make sure Microsoft "File and Print sharing service" is installed on each machine (Win98/ME). Nothing need be shared but the service must be running for the machine to show up in the Neighborhood.

In XP Simple File sharing is defaulted on except when XP pro is joined to a domain.

#2 Bindings (Win98/ME)
File and print sharing must be bound to a communication protocol typically TCP/IP. Before the popularity of the Internet NetBEUI or IPX were commonly used on the LAN. They are considered obsolete protocols and no longer build into Windows. NetBIOS/SMB is the programming API used by Microsoft to exchange information over the network.

> ***Security Tip*** - If system includes an interface connected directly to the Internet 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.

#3 Workgroup name
My Network Places are 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. The Browse Master is elected at boot time. If the PC running Browse Master is shut down it may take a while for the event to be detected and a new Master elected.

> ***Windows Configuration Tip*** – There is a compatibility problem between Win2000/XP/Vista and older versions of Windows and Win98/ME. We had trouble getting a Win 98 laptop to show up in a corporate network of Win 2000/XP machines. Our workaround was to place laptop in its own workgroup.

#4 Browse Master (Win98/ME)
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. In older versions of Windows is was possible to force a machine to always be the browse master. That is no longer an option with XP/Vista. Browsing performance is much improved in newer versions Windows.

To quickly force, which machine will be the master browser shutdown all PCs on the LAN. Turn on PC chosen as master browser first. As there are no other computers on the LAN it will win browser election. As other computers are turned on they will detect an active master browser and use it.

#5 Login
If network logon (in network properties) is set to Client for Microsoft Networks (Win 98/ME) 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 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
To enable file sharing pick the desired subdirectory to share and check sharing. That directory and all subdirectories will be shared.

> ***Security Tip*** – Files can be shared as read only or read/write. Unless it is necessary to allow others on the LAN to modify file and/or create directories it is better to limit access to read only.

> ***Security Tip*** - 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 system uses a software firewall be sure it does not block NetBIOS and SMB ports used to discover local host names and share files. XP SP2 built in firewall does not interfere with file sharing. Some third party firewalls have to be configured to allow the following ports.

```
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)
```

5.3 Time Service

US National Institute Standards and Test (NIST) and other organizations maintain public timeservers. This eliminates 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 local server in turn is synchronized to Stratum 2 timeservers.

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

> ***Configuration Tip*** -- XP/Visa includes a timeserver that must be disabled when using K9 client.

Configuration Tip -- The load on public timeservers is very high and getting higher, be a good net citizen 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 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 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 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 -- 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.

5.4 Local DNS Resolver

Normally the ISP provides DNS. However, any DNS server can be used to translate URLs to IP addresses. Verizon DSL service has been very reliable, but they have had numerous DNS problems. At first I used the DNS server from my dialup ISP but decided to run my own DNS server. TreeWalk was installed on the server. Running my own DNS server has solved chronic DNS problems. For typical home LAN running local DNS is not very demanding and does not interfere with other programs running on the server.

Running TreeWalk DNS is straightforward. Install the software, and then modify TCP/IP settings. On the PC running TreeWalk set DNS IP address to Loopback address 127.0.0.1. On other PCs DNS address is set to the TreeWalk server.

Running your own DNS resolver is also a convenient way to block ads. More info about ad blocking here.

5.5 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. XP pro includes built in IIS server but not XP home. The server is running XP home so we needed to use a third party web server. We chose Abyss as it is free for personal use. Abyss replaced Xitami server running on the previous server under Win 98.

5.6 Weather Station

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

5.7 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 originating Syslog entries are the router and Tardis Time service.

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

6 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 instances customers could: 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, 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

6.1 Structured Wiring

Figure 6 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 network (LAN) and telephone.

UTP cable is rated by Category; higher numeric designation indicates higher performance. TIA created Category 3, 4, 5, 5e 6, 6a. 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.

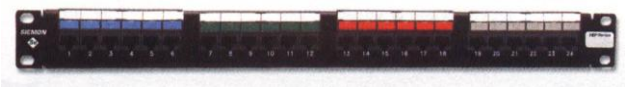


Figure 7 Cat 5 Patch Panel

Cat 5e allows a single wiring scheme for Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps), 10 G Ethernet (10,000 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. The same thing happened during development of 10 G Ethernet, resulting on modified Cat 6 called Augmented Cat 6.

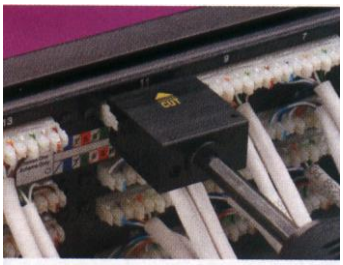


Figure 8 Rear view w/Punchdown Tool

The highest level is Cat 6. Cat 6 doubles bandwidth from 100 MHz for Cat 5e to 250 MHz. IEEE recently released specification for 10G over UTP. As happened with Gig Ethernet during spec development it was found necessary to tweak the cabling spec. Due to the higher frequencies involved at 10 G crosstalk from other nearby cables, called alien crosstalk, is a problem. Cat 6a (augmented) addresses this. Cat 6a cable has a larger outside diameter then Cat 6 to reduce alien crosstalk. As with Cat 5 vs 5e using lower rated cable may work but it does not meet worst-case parameters.

EIA/TIA is a US standards organization. Europe and rest of the world use similar standard defined by ISO/IEC 11801. Performance is grouped by Class rather then category. Class C is equivalent to Cat 3, Class D to Cat 5, and Class E to 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 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.

6.2 Cable Types

The most common type of Category cable is UTP PVC. It can be used in most habitable spaces. The larger diameter of Cat 6a used with 10G Ethernet is increasing interest in screened cable. Screened cable has an outer foil shield. Screened cable is more difficult to work with but its smaller diameter is very attractive when used with high density wiring such as data centers. It will be a long time, if ever, that SOHO networks need 10G Ethernet.

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. It is a common misperception Plenum rated cable is fire proof, which is not correct. Teflon is fire resistant not fire proof. The goal of Plenum cable is to delay 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.

6.3 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 US telephone industry was migrating to modular connectors it was also in early stage of divesture and FCC mandated CPE interconnect. For the first time Customers Premise Equipment (CPE) could 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. The system was called Uniform Service Ordering Code (USOC) Registered Jack (RJ) designation. Most Registered Jacks are only of historical interest today. The RJ nomenclature has passed into popular usage only loosely coupled to its original intent.

4-position connector is used to connect telephone handset to phone. It is 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 for Business Class T-1 carrier.

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

6.3.1 Telco Uniform Service Ordering Code (USOC) Pinout

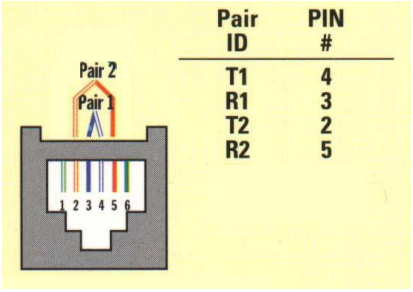


Figure 9 RJ11 & RJ14

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

RJ31 and RJ38 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

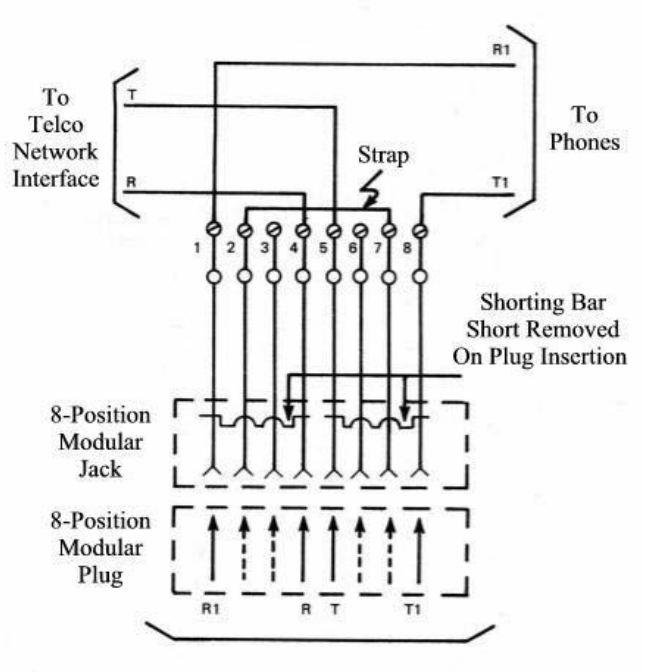


Figure 10 RJ31 and RJ38

within the jack establish continuity when the alarm is not plugged in. Connecting 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 line was previously in use. RJ38 is identical to RJ31 except it has a strap between positions 2 and 7. This allows 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.

6.3.2 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.

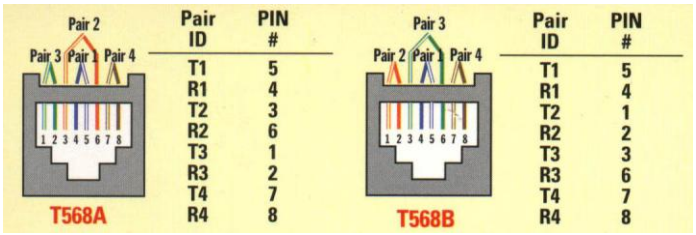


Figure 11 TIA UTP alternate pin outs

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 is the same pinnout used by AT&T key systems prior to development of structured wiring techniques.

6.4 Wiring Color Code

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

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

Standard Telephone practice 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 -	

6.5 Type 66 Punch down Block

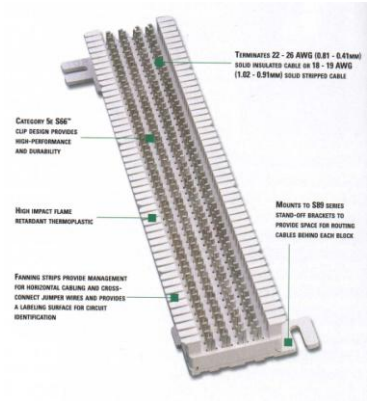


Figure 12 Type 66 Block

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.

6.6 Type 110 Punch down Block

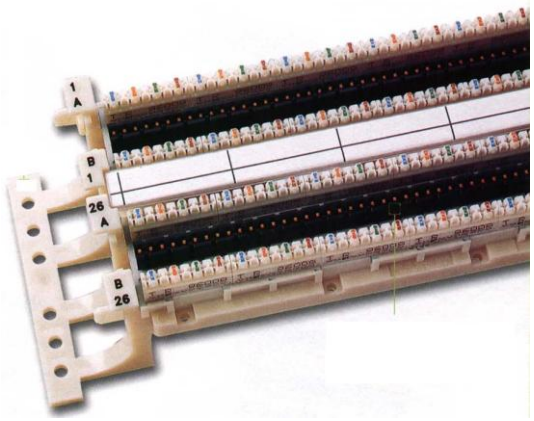


Figure 13 Type 110 Punchdown Block

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.

6.7 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 terminated 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 used. 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 and 10G use all four.

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

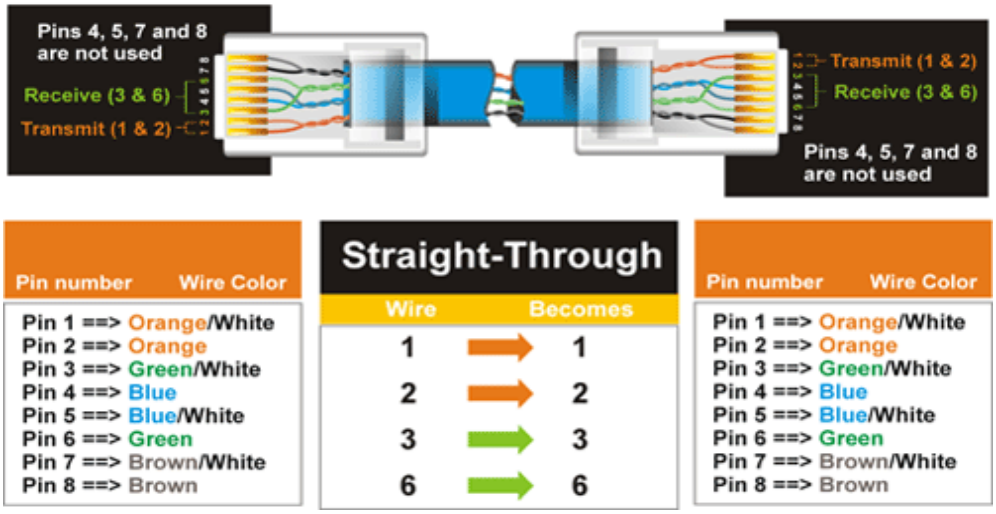


Figure 14 Straight-through Patch Cable

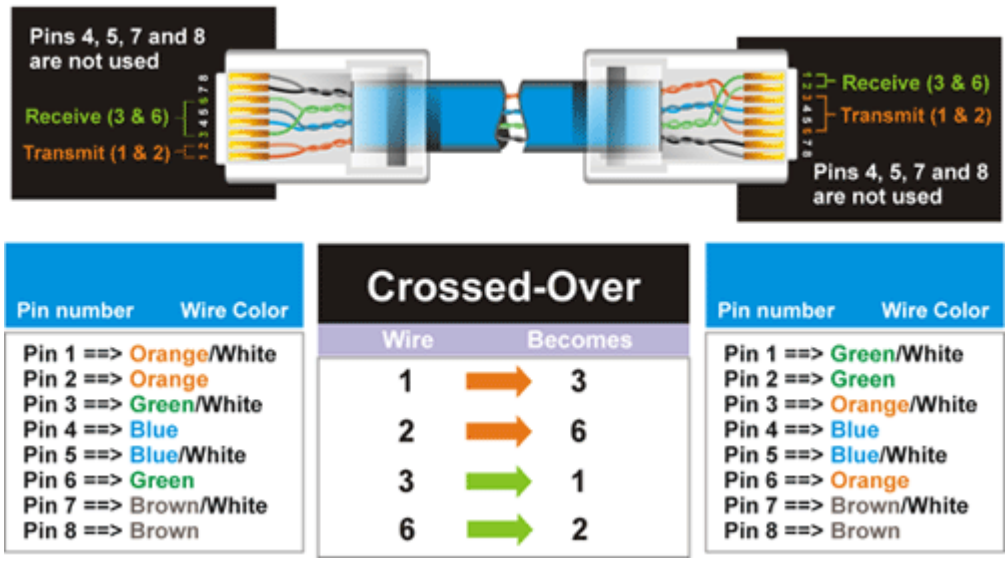


Figure 15 Crossover Patch Cable

6.8 Telephone

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

The 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.

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.

Initially we used dialup as backup if DSL failed. We no longer do so. DSL service has been very reliable. With web sites increasing being optimized for broadband dialup browsing is painful. I designed a custom built device to minimize interference between dialup and phone lines. More information about the Modem Access Adapter (MAA) is available on the writings page.

6.8.1 Telephone Network Interface Device (NID)

Figure 16 Telco NID

In the bad old days before US telecom divestiture (1880 to early 1980's) Phone Company delivered phone service, wired customer's premise and leased all telephone equipment. With divestiture Phone Company's 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 incorporates 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 purpose remains the same: Terminate outside 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 automatically disconnects inside wiring. If phone works when plugged into the test jack problem is due to customer wiring or equipment, if not problem is with Telco.

6.8.2 POTS/DSL Splitter

Figure 17 Splitter

ADSL uses a single phone line to deliver both voice and data service. Filters are required to prevent high frequency signaling used by DSL from interfering with voice. To reduce cost ADSL service uses 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 to isolate 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 allows removal of half-ringer in NID, minimizing DSL signal loading.

Home Alarm Tip – If a phone is connected to splitter "Data" 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 can be installed after the alarm jack and alarm filtered separately.

6.9 Power Distribution

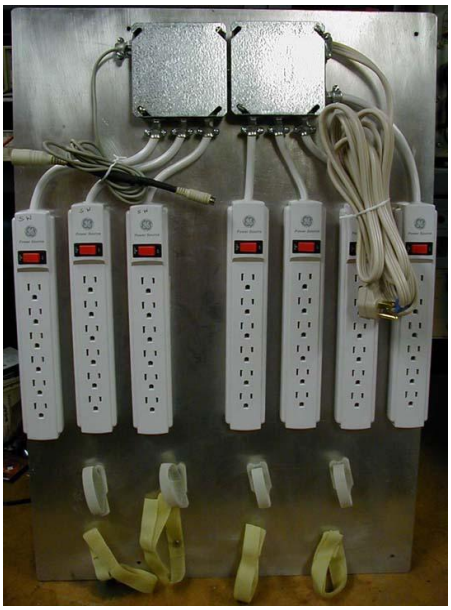


Figure 18 Power Panel

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.

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. 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 keyboard controlled power up. In that case power panel needs to sense power directly from PC main power supply.

6.10 Secondary Lightning Protection

The key to minimizing lightning damage is bonding all services together with a low impedance path to earth ground. All conductors entering the building must be bonded together and equipped with lightning protection. This minimizes difference in potential during transient conditions.

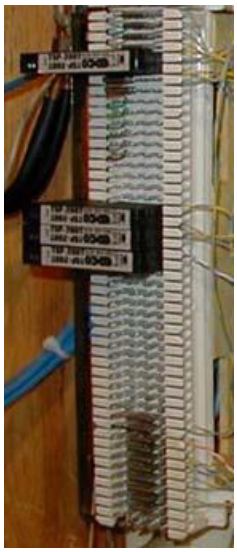
6.10.1 Electrical

Whole house surge protector should be used to protect the electrical system. Remember goal is to direct excessive energy into a low impedance ground and to provide low impedance bonding of all metallic conductors. We use a GE THQLSURGE protector. Installation is easy it plugs into the main breaker panel much like an ordinary two-pole breaker.

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.

Figure 19 AC Mains Protector

6.10.2 Telephone



Telephone Company 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 equipment more susceptible to line surges. Adding secondary protection minimizes risk of equipment damage. The best location for secondary protection is at building entry point. This allows protector to use low impedance power mains earth ground to minimize voltage difference between services.

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

Figure 20 Telephone Surge Protector

6.10.3 CATV

Local Cable Company install a grounding block where coaxial cable enters the building. This insures cable sheath is as at same potential as building safety ground (green wire ground). As with Telephone it is advisable to add secondary CATV protection.

Figure 21 CATV Surge Protector

6.11 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 cable is properly terminated; 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 with higher speed 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 22 Jacket Ripper

Figure 23 RJ11/45 Crimper

Figure 24 66/110 Punch down

6.12 Putting it all Together

The drawing below shows overall connection of phone and DSL wiring. NID, secondary lightning protection, POTS/DSL splitter, 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. “Voice” output terminates at the 66-block to be connected to multiple phones.

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 located wiring closet insures it is available when needed.

Figure 25 Netgear Ethernet Switch

Network wiring was installed after the house was built. Most rooms are equipped with two Ethernet drops, the office with four. UTP Cat 5 cable is home run from each outlet to wiring closet. Location of LAN wiring closet is different from phone wiring closet. A Netgear FS116 16-port unmanaged 10/100BaseT switch interconnects drops. The switch replaced a 16-port 10/100 hub that in turn replaced an 8-port 10 Mbps hub.

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. If I was installing wiring today I'd use Cat 5e cable and patch panel in wiring closet rather then terminate plugs directly to cable.

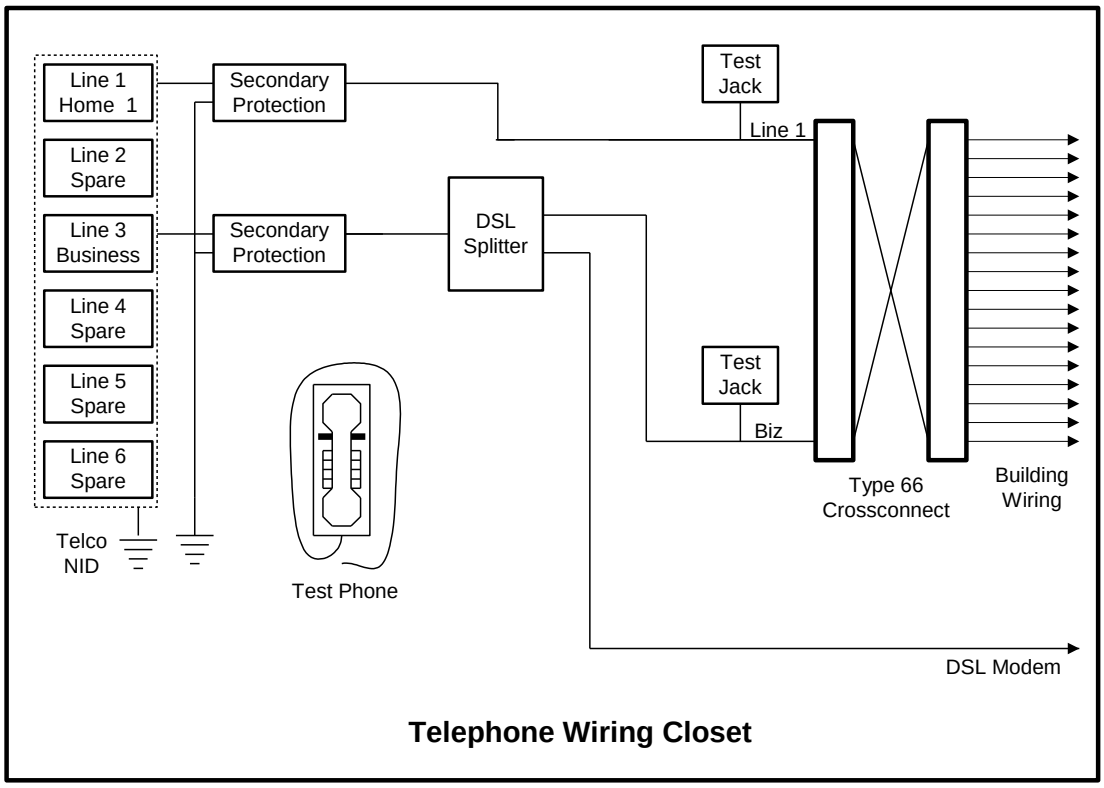


Figure 26 Telephone Closet Wiring

6.12.1 WiFi Access Point

Figure 27 WiFi AP

With implementation of WPA2 we finally felt confidant enough to install WiFi on our SOHO LAN. We chose an EnGenius ECB-3220 Access Point. The AP is located in a second floor utility closet providing coverage throughout the building and limited coverage outdoors.

A feature of this AP is support for Power over Ethernet (PoE). I am not currently using it but it makes providing backup power easy as a single UPS can be used rather then needing AC at every location.

Setup was pretty straightforward. AP defaults to static IP address 192.168.1.1. To configure AP connected it to a spare PC and changed to DHCP client mode. Configured router to use MAC reservation and always issue AP same IP address. Changed configuration to AP. Device supports Bridge and Bridge Router modes.

Debugged connection without security then configured WPA2. We do not have a RADIUS server so selected WPA2 pre-shared key mode. With a shared key each device must be configured with a pre-shared passphase. This eliminates need for RADIUS authentication but requires a passphase entered into each device. This is labor intensive, on a large network but not a big deal for small one. An important downside of shared key is if a device is lost/stolen passphase needs to be charged or intruder will have easy access to LAN.

Ideally passphase should be random and very long to defeat dictionary lookup attack. Good passphases are very difficult to generate manually. Luckily the Internet comes to the rescue with an online passphase generation site. SSID should also be changed to something unique.

Encryption is computer intensive so turning on WPA2 negatively impacts throughput. I find that a small prices to pay for increased security. So far WiFi has worked well – enjoy untethered network access.

6.12.2 Computers and Printers

Most of our PCs were getting rather long in the tooth. Many were still running Windows 98 or ME. Microsoft discontinued support for these Operating Systems in mid 2006. Main driver for replacing these aging computers was inability for run applications that require XP. In addition USB memory sticks are very popular but difficult to use pre XP, as each requires a unique driver.

Interestingly first PC replaced was also the fastest of the old machines. My son was using a Dell Dimension 4100 1 Gigahertz PC running ME. Deemed not adequate for gaming he replaced it with an eMachine W3502. Recycled PC as home server replacing aging IBM 300GL P200 by Installing XP and adding second 320 Gig hard drive for file sharing.

A local computer dealer had a bunch of HP/Compaq Evo 510 towers come off lease. Bought a couple to replace Dell XPS T500 and Toshiba V3100 for my wife and myself. We also purchased a used Dell Latitude C600 laptop locally from another dealer. These are nice solid boxes at very attractive prices. Unless one needs latest and greatest PC hardware buying used PCs off lease is worth looking into.

We did acquire one new PC, a HP M8000e tower. This replaced my daughter's HP Pavillion 6735. This is the first AMD PC I've owned. AMD represents a lot of bang for the buck.

The only computer not affected by this wholesale upgrade is my old trusty DEC Ultra 2000 laptop running Win 98. It is only used to take notes and do simple presentations so cannot justify its replacement - yet.

HP K550 inkjet printer replaced HP 2000. It has a built in print server allowing direct LAN connection.

7 Services – Making Life Worth Living

This section describes the various services running on the LAN.

7.1 World Wide Web (WWW)

All PCs use Microsoft Internet Explorer version 6 and some also use FireFox. It seem seems the browser wars are raging once again. Have multiple browsers is a useful troubleshooting tool. Internet Explorer version 7 seems to break compatibility with some web sites so after trying it for a while reverted back to vers 6.

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

7.2 E-Mail

E-mail accounts fall into three broad categories: ISP accounts, free third party services and business email. ISPs typically provide email service as part of the total package. 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. Google Gmail has become a very popular free email service. I use it as an alternative to business email. Third party email decouples 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.

7.2.1 Browser Based Mail

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

7.2.2 Outlook Mail Client

Outlook mail client is email application designed to optimize email use and storage. Outlook allows access to multiple email account through a single user interface.

Except for web-based mail, e-mail has a sending component, SMTP, and a receiving mailbox, POP. To send mail client connects to an SMTP (Simple Mail Transport Protocol) mail gateway. The SMTP server acts as a relay between e-mail client and POP mail server. The SMTP server verifies each recipient is accessible and returns an error message if not. The SMTP server delivers mail to the appropriate POP server, (Post Office Protocol). It works much as a real post office mailbox. The POP server stores mail temporally. The e-mail program connects to the POP sever and downloads mail.

7.2.3 Corporate Mail

Telecommuters and road warriors need access to corporate mail when out of the office. Depending on where mail server is located this may be easy or difficult. If access is not restricted user is able to log in like any other email account. If the email 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.

7.2.4 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 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.

Reveres Name Lookup
Incoming mail server verifies SMTP server has a valid DNS domain name and associated MX record.

Sender Policy Framework
Sender Policy Framework provides a mechanism receiving email server can use to validate mail is being sent by an authorized rather then spoofed. Much spam is send using forged domain name. SPF provide easy mechanism to detect forged names.

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 user first retrieve mail from the POP account before allowing outgoing mail. Once user is verified ISP assumes that IP address is trustworthy for a short time. This allows customer to send mail regardless of how they connect.

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

7.2.5 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 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.

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.

7.3 Instant Messaging

Instant messaging (IM) is becoming extremely popular both full blown messaging service using a PC and short message service (SMS) via cell phone. IM requires client side software. Unfortunately there is an interoperability battle being waged among the various IM services that see proprietary and incompatible IM formats in their corporate interest. This makes it a challenge to interconnect with users on different systems.

7.4 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. As time goes by fax becomes less and less important. However it is nice to be able to send and receive the occasional fax.

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. 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 a fax we use the Fax software built into XP and an onboard dialup modem salvaged from another PC.

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

7.5 FTP

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

7.6 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. 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.

7.7 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.

7.7.1 Audio and Video

Adding video and audio capabilities to personal computers back in the early '90s profoundly changed usage patterns. No longer primarily perceived as a computing tool personal computers were transformed into gateways to all sorts of digital media.

7.7.2 Digital Rights Management

Audio and video content owners are concerned digital distribution allows uncontrolled lossless duplication of copyrighted works. This is seen as a threat to their business model and over the years have attempted to implement of number of Digital Rights Managements (DRM) schemes to limit customer's ability to use purchased content. The history of DRM has been controversial both at a philosophical level as to the

correct balance between copyright owner rights and user rights and steps copyright owners have taken to implement DRM.

From a practical perspective DRM restrictions may limit ability to make copies of commercial content, store them on a server and access them even over a private LAN.

7.7.3 CD/DVD evolution

Back in the early '90s digital versions of audio CDs were heralded as a tremendous new storage medium. Typical CD stores about 700 Mbytes of data. Compared to only 1.5 Mbytes on 3.5" floppy. This seemed like and infinite amount of space. Back then hard drives were not much larger then a single CD.

Time marches on. DVDs were developed to allow digital movies be distributed in similar format as audio CDs ultimately displacing VHS videotape. Current mass-market DVD technology stores 4.7 Gbytes (single Layer) of data. This is more then enough to store an entire SDTV (standard definition) movie with room for other features.

With increased popularity of HDTV (high definition) a DVD format with even more capacity was needed. Currently there is an contentious market battle over next generation DVD between HD-DVD (15GB (single layer) and Blu-Ray 25 GB (single layer). Current price points of next generation players are high and it is unclear which format will prevail or if both will coexist forcing need for dual mode players.

Video data is encoded and compressed using various MPEG compression schemes. Data within an image is compressed (spatially) and between frames (temporally). Without compression files would be too large even for DVD formats.

Unless being an early adopter is important it is a good time to sit on the sidelines until the smoke clears.

7.7.4 ITunes

Apple's Itunes music service has been a popular complement to the IPOD as a way to purchase and play digital music. That replaced Music Match Jukebox player used previously

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.

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.

7.7.5 Real Audio Player

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

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

7.7.6 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.

7.7.7 QuickTime

Apple QuickTime is a popular movie-encoding format.

7.8 Image Scanning

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 HP ScanJet 5400C. It also functions as a poor mans copying machine allowing scanned images be printed to the network printer.

7.9 Digital Camera

Nothing beats a digital camera to quickly capture images and incorporate them into documents or a web page. Cameras typically use some form a removable Flash memory to provide virtually unlimited image storage. Images are captured and compressed in JPEG format dramatically reducing size with minimal loss in quality.

The popularity of solid-state media cards has spawned a wide assortment of media reader/writers. The HP M8000e PC came with a built in media reader. On other PCs we use a CP Technologies 10-in-1 USB memory card reader/writer.

7.10 Radio/TV

There are many ways to distribute Radio and Television programs. The Internet opens up fascinating opportunities for new sources not constrained by distance or even a local presence.

7.10.1 Internet Radio/TV

Radio and TV programs can be delivered over the air, via Cable or Satellite and more recently over the Internet. Radio programs are already commonly available over the Internet, TV less so due to limited first-mile bandwidth. This will change as bandwidth and data compression techniques improve.

The Internet, unlike other distribution mediums, is one-to-one. A user connects to a media server; server delivers information directly to user. This is both a huge advantage, compared to traditional media, and a disadvantage. An advantage because patron and source are more intimately connected, this is ideal for demand-based programming. It is a disadvantage because emulating one-to-many broadcast model over the Internet is still not a mature technology. As they are overcome cost of "broadcasting" content over the Internet will be drastically reduced.

7.10.2 RF Radio/TV

Hauppauge TV/FM card is installed in the main workstation. I find that combination very useful. 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.

The HP M8000e also came with TV/Radio card; it supports both NTSC analog TV and ATSC digital TV.

7.10.2.1 Over the air (OTA) reception

We live in deep fringe area. With Feb 17 2009 looming as the deadline for end of analog over-the-air (OTA) transmission wanted to see if we could receive OTA digital programming. My worst fears were

realized. Tuner is able to detect station call sign and audio but unable to display video even with large roof mounted rotateable antenna. Time to look into Plan B if we want to be able to watch TV.

7.11 Telephony

Since the telephone was invented over a hundred years ago the same basic technology has been used to connect caller to called party, circuit switching. When a caller initiates a call a semipermanent path through the network is set up for the duration of the call. When the call is over connection is torn down and network components released for use by other customers.

The Internet is causing tremendous change in all aspects of our lives not the least of which is plain old telephone service (POTS). Packet based transport was not designed for real time communication so making telephony work has been a challenge. The payoff is Convergence – the integration of all forms of communication over a single unified transport network.

Currently we use ordinary wired analog POTS telephones and wireless Cell phones. Both live in their own world. In the not to distant future will be able to use a single convergence device that work at home over WiFi, at WiFi hot spots and when not in range the traditional wireless network. The user interface will be varied from the finger cramping cell phone itself to richness of the PC.

7.12 Printing

Computers were once billed as the paperless office. This has not happened. On the other hand the Internet and low cost high quality printers have significantly expanded 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 demand printed as hard copy by recipient.

We had been using a HP 2000 professional Inkjet printer and a HP JetDirect 300X print server for a number of years. It quit working in the middle of my wife finalizing her Masters thesis. It was replaced with and HP K550. The new printer is much faster and cheaper then the 2000 while still retaining individual ink supply. The K550 is network ready, print server is built in rather then external. This results in much richer interaction with printer then before. Curiously one of the reasons for choosing this particular printer was that it still supported Win98. As fate would have it upgrading printer triggered a flurry of system upgrades so we no longer need to support Win98.

7.12.1 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.

7.13 Accounting

Computers are idea bookkeeping machines making them ideal for tracking home and business finances. We have been using various flavors of Quicken over the years for both personal and business. Internet access is nice since it allow importing financial data eliminating need to manually rekey data.

7.14 Secure Remote Access - IPSEC and SSL

VPNs extend corporate network to telecommuters and business partners. There are two approaches to providing remote access: IPsec and SSL.

IPsec developed by the IETF 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 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.

Tunnel mode forces all client traffic through the IPSEC encrypted tunnel to the corporate LAN. This is the most secure and provides the same logging/management functions as if the employee was physically connected locally. The downside it that all traffic has to be encrypted, carried by the tunnel even if it is not directed towards the corporate LAN. An alternative configuration, split-tunnel, addresses that problem.

In split-tunnel mode the tunnel only carries traffic destined for the corporate network. Other traffic flows as if the tunnel did not exist. Split-tunnel creates a potential security concern. The client is able to access 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.

Having employees install IPsec client presents a management challenge. As an alternative some companies are using SSL/TLS to provide a secure connection between remote employees and corporate network. While SSL is not as powerful or secure as IPsec all browsers support SSL, eliminating the need for special client software. This is especially convenient for employees that need to connect to corporate network from multiple computers.

8 Security -- Keeping Bad Guys/Gals 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.

8.1 Virus & Trojans

This is probably what most people think of when discussing Internet security. This attack has been around since the days of standalone PC using floppy disks. The first line of defense is staying away from untrustworthy sites. In the past if I wanted to go to a new site I'd often guess the URL since it is often some variation of company name. This is dangerous practice since attackers often register common misspelling of popular domain names. To prevent this sort of thing I use Google to search for site name. Does not guarantee site is safe but it reduces risk of fat-fingering a dangerous URL.

Anti virus programs have been available for years, two of the most popular are Norton and Mcafee. They check file signatures and monitor downloads. Anti virus programs are powerful but often breed a sense of over confidence. Attackers and anti virus companies are in a constant state of battle. Attackers get more resourceful and constantly introduce new viruses. There is a delay between first time attack is seen "in the wild" and a fix. This creates a window of vulnerability between virus release and antidote.

8.2 Zombies

One of the most insidious form of attack is using compromised computers to attack/spam other computers. Once an attacker is able to install executable code on a machine they not only have gained control of that computer but also potentially able to use that computer to attack others at will. What makes Zombie attacks devastating is often computer owner is not aware PC is compromised. Often the first hint of a problem is a nasty email/letter from their ISP.

8.3 Denial of Service (DoS)

Zombies are often used in Denial of Service attacks (DoS). A DoS attack floods victim with bogus queries. To make attack more powerful many computers are used simultaneously in a Distributed Denial of Service attack. The attack does not corrupt or deface the victim but by overloading victim's network or computers is able to takes service office line or degrade response time during the attack. DDoS attacks are common against popular sites and DNS servers.

8.4 Cookies

Cookies were introduced by Netscape to address stateless nature of the Internet. A cookie is a small block of information a web site asks browser to store on its behalf. Cookies are important because without them sites have no way to know if this is the first or thousandth visit. From this benign beginning advertisers and governments have figured out ways to use Cookies to disclose additional information about browsing activity. This occurs unbeknownst to the typical user.

8.5 Spyware

Companies are finding ever more obnoxious ways to extract information from customers. Spyware collects 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.

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

8.6 Eavesdropping

Radio communication is easy to eavesdrop. An attacker can locate a safe distance away without having to 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 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 tenants are in close proximity.

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

8.7 Social Engineering

Sad to say many security breaches are not the result of compromising technical security barriers. They result from individuals inadvertently giving out privileged information. An attacker typically poses as someone who would normally have legitimate access to the desired information: say a police officer or maintenance technician. If the attacker knows enough background information and lingo they are often able to fool representative into telling them information they are not authorized to access.

8.8 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 secure 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 a Phishing attack is to obtain user account data so attacker is able to masquerade as the user. Phishing is a classic Man-in-the-Middle attack.

8.9 DNS Cache Poisoning

The Internet was designed to be robust in the face of equipment and communication failures. Unfortunately it was not designed to withstand deliberate willful attack. The Domain Name System (DNS) is the vehicle used to convert user-friendly names to computer friendly IP addresses. This is a complex system. One of the ways to minimize unnecessary load on DNS server is to cache recently used information. DNS poisoning exploits a weakness in DNS to plant bogus information. Once corrupt information is loaded computers accessing that DNS server are directed to the incorrect site. That site is controlled by the attacker and like Phishing allows a man-in-the-middle attack.

8.10 Man in the Middle Attack

Man in the middle is a classic cryptographic attack where an intruder intersperses himself between two parties. Once in position intruder is able to intercept traffic from each party and forward it to the other

without either being aware of the attack. The attacker in turn is able to modify messages an observe passwords.

Until recently this sort of attack was rare in the Internet because attacker needed to intercept traffic. Without being located within the ISP or Internet backbone this was not practical. With the advent of Phishing and DNS Poisoning it is becoming common. This attack causes either user or computer to connect to the attacker's site. Often the site is an exact duplicate of the real site. Once the person has been fooled into connecting to the bogus site attacker is free to modify messages and more often capture authentication credentials.

8.11 Data Leaks

Computers work by receiving information, creating copies – either temporary or permanent, modifying the information as needed to accomplish the desired task, making more copies of the modified data and often sending it to a third party. These records are a gold mine for legitimate businesses, law enforcement, and criminals. Digital data is easy and cheap to capture. Once captured lossless replication is easy. Once captured this treasure trove of information often escapes control of those who have created it winding up in the unsavory hands of criminals or out of control government snooping.

8.12 Countermeasures

There is no such thing as perfect security. One must take a cold hard look at how computers are used, how valuable the information contained, how attractive a target you are and the ramification of breach. Security engineering is very different then other forms of engineering. In a typical engineering problem a solution is developed and proper operation verified. Nowhere in the statement of work is there a need to consider deliberate attack on the widget designed to pervert proper operation.

8.12.1 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.

8.12.2 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.

- For example Universal Plug and Play (UPNP) allows PC based applications request router modify firewall rules to allow Internet access. While this is a boon for ease of use it also means a compromised machine is able to modify firewall rules and unless the user is very diligent will never know an unauthorized application has access to the Internet.
- Many devices ship with default passwords. Changing them should be a high priority.

8.12.3 Password Management

No reputable entity will ever ask you for your password. If there is a problem with your password you may be issued a new one but you will never be asked to give someone your password.

- Change passwords and account names, do not use defaults.
- Be weary of any email providing a link and asking you to log in – it may be a Phishing attack.
- 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.

8.12.4 Limit Information Release

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.

8.12.5 Trustworthy Software

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.

Newer versions of Windows make this much easier to limit unauthorized software installation by providing a pop up dialog box asking approval to install software. Much Windows software includes digital signing that verifies it came from the vender it claims to come from. Note: signing says nothing about the quality of the software just who released it.

8.12.6 NAT

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 ignores the request 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.

8.12.7 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 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.

8.12.8 Data Backup

Having duplicate copies of important data is key to recovering from data loss, either accidental or deliberate. With large low cost drives both internal and external backup has never been easier.

8.13 Internet Paranoia

When reading about various threats it is easy to become overwhelmed. 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.

Security is a balance, taking reasonable precautions go a long way to keeping oneself safe in the digital world.

9 Backup – Oops Protection

Having an always-on server makes it possible to use automatic 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 or power anomaly may destroy all copies of the data. If both copies are in the same location they may be destroyed in a fire.

9.1 On Line Backup

One of the purposes of the server it to provide file shares so each person is able to backup data on the server. The upgraded server is not only faster it has much more disk space. The new server has 360 Gbytes compared to only 40 GB before. We chose Acronis True Image as the backup utility. It has the capability to backup data or create a complete disk image that can be used to do a system restore if the disk is corrupted or needs to be replaced.

Backups are scheduled to occur automatically insuring data is safely duplicated. Use of incremental backup allows only file changes to be saved reducing amount of disk space needed to roll back files to any given date.

9.2 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. CDs and DVD are cheap high capacity means to create off line storage. There is some concern about long-term stability of writeable media. It is unclear how long writable media lasts before data is unrecoverable. However it is likely to be at least tens of years so will not to cause problems as off line backup medium.

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

9.3 USB Memory Sticks

USB Memory Sticks have become extremely popular over the last few years. They offer advantage of a large, low cost rewriteable removable storage medium. Once data is copied and stick removed hardware/software problems on the computer have no effect on data.

10 Debug -- When Things Go Wrong

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

10.1 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 as utilization increases. Occasional collisions are nothing to worry about.

> ***Debug tip*** – If cable is not terminated correctly end-to-end continuity may exist but pairs miswired, causing a condition known as a split-pair. A split pair cable will often operate at 10 Mbps but fail at higher speed.
>
> ***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.

10.2 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 3346 Netopia DSL modem/router displays two pages of modem data. 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 by modem. ADSL startup attempts record number of times router had to reinitialize PPPoE sessions since last power up.

```
ADSL Line State:         Up
ADSL Startup Attempts:   101
ADSL Modulation:         DMT
Datapump Version:        DSP 4.2.1.0, HAL 4.2.1.0
                         Downstream  Upstream
                         ----------  ----------
SNR Margin:                   31.00       22.00 dB
Line Attenuation:             44.00       31.00 dB
Output Power:                  5.33       11.88 dB
Errored Seconds:                  0           0
Loss of Signal:                   0           0
Loss of Frame:                    0           0
CRC Errors:                     295           6
Data Rate:                     1792         448
```

```
ATM port status     : Up
Version: CPAAL5: 01.07.2b    SAR: 52

Rx data rate (bps) : 1792
Tx data rate (bps) : 448
ATM Virtual Circuits:

VCC #  Type  VPI   VCI   Encapsulation
-----  ----  ---  -----  -------------------------
  1     PVC    0     35  PPP over Ethernet (LLC/SNAP encapsulation)

ATM Circuit Statistics: VCC-1

  Rx Frames     :    4234906          Tx Frames     :    3082077
  Rx Octets     :  278471116          Tx Octets     :  416823418
  Rx Errors     :          0          Tx Errors     :          0
  Rx Discards   :          0          Tx Discards   :          0
```

10.3 PING

PING is a Windows 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.
```

10.4 Traceroute

Traceroute (Tracert in Windows) determines round trip time to each hop between user and remote host. This information is useful to determine underlying cause of slow Internet response or unavailable hosts. Traceroute uses 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 sender TTL expired. Traceroute uses this information to build a path map and response time list to each hop between source and destination.

Round trip time increases with distance and hop count. A sudden increase typically means that node or previous one is congested. PING is given a low priority so it is not uncommon for a router or server to ignore Ping. In that case Traceroute responds with an "*" indicating nothing was returned in response to the request.

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 <1 ms <1 ms <1 ms  192.168.2.1
 2 24 ms 24 ms 24 ms  10.20.1.1
 3 24 ms 25 ms 25 ms  at-4-2-0-1710.CORE-RTR1.MAN.verizon-gni.net
[130.81.10.65]
 4 27 ms 26 ms 28 ms  130.81.20.116
 5 28 ms 27 ms 26 ms  0.so-5-1-0.XL1.BOS4.ALTER.NET [152.63.16.69]
 6 35 ms 35 ms 35 ms  0.so-6-3-0.XL3.NYC4.ALTER.NET [152.63.0.69]
 7 35 ms 35 ms 35 ms  0.ge-6-1-0.BR3.NYC4.ALTER.NET [152.63.3.166]
 8 35 ms 34 ms 35 ms  192.205.34.49
 9 37 ms 38 ms 39 ms  tbr2.n54ny.ip.att.net [12.122.105.74]
10 36 ms 36 ms 35 ms  gar1.nwrnj.ip.att.net [12.123.0.157]
11 36 ms 35 ms 35 ms  att-gige.esd1.nwr.nac.net [12.119.140.26]
12 36 ms 36 ms 36 ms  3.ge-3-0-0.gbr2.nwr.nac.net [209.123.11.189]
13 37 ms 37 ms 37 ms  0.so-0-3-0.gbr1.oct.nac.net [209.123.11.233]
14 43 ms  *    39 ms  www.dslreports.com [209.123.109.175]

Trace complete.
```

10.5 IPCONFIG

IPconfig is a Windows command line utility to display IP settings for each network adapter. If Point-to-Point Protocol (PPP) adapters are present Ipconfig will also display the virtual adapter entries that emulate physical interfaces.

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 host controller protocol server. At power up client emits a DHCP discovery message to find active DHCP servers. 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. The last two lines show when the lease was obtained and when it expires.

```
C:\DOCUME~1\TSCHMIDT>ipconfig /all
Windows IP Configuration

 Host Name . . . . . . . . . . . .   :Tom-Desktop
 Primary Dns Suffix  . . . . . .   :
 Node Type . . . . . . . . . . . .   :Hybrid
 IP Routing Enabled. . . . . . .   :No
 WINS Proxy Enabled. . . . . . .   :No

Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix  :
 Description . . . . . . . . . . .   :Intel(R)PRO/100 VM Network Connection
 Physical Address. . . . . . . .   :01-0E-02-C9-3B-5E
 Dhcp Enabled. . . . . . . . . .   :Yes
 Autoconfiguration Enabled . . .   :Yes
 IP Address. . . . . . . . . . .   :192.168.2.13
 Subnet Mask . . . . . . . . . .   :255.255.255.0
 Default Gateway . . . . . . . .   :192.168.2.1
 DHCP Server . . . . . . . . . .   :192.168.2.1
 DNS Servers . . . . . . . . . .   :192.168.2.5
                                    :192.168.2.1
 Lease Obtained. . . . . . . . .   :Saturday, November 03, 2007 9:26:44AM
 Lease Expires . . . . . . . . .   :Tuesday, November 06, 2007 9:26:44 AM
```

10.6 Route

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

```
Active Routes:

   Network          Netmask          Gateway       Interface  Metric
   Address                           Address
         0.0.0.0          0.0.0.0      192.168.2.1  192.168.2.13     20
       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    192.168.2.13  192.168.2.13     20
    192.168.2.13  255.255.255.255        127.0.0.1    127.0.0.1     20
   192.168.2.255  255.255.255.255    192.168.2.13  192.168.2.13     20
       224.0.0.0        224.0.0.0    192.168.2.13  192.168.2.13     20
 255.255.255.255  255.255.255.255    192.168.2.13  192.168.2.13      1
```

10.7 NETSTAT

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

```
  -a         Displays all connections and listening ports.
  -b         Displays the executable involved in creating each
             connection or listening port. In some cases well-known
             executables host multiple independent components, and in
             these cases the sequence of components involved in creating
             the connection or listening port is displayed. In this case
             the executable name is in [] at the bottom, on top is the
             component it called, and so forth until TCP/IP was reached.
             Note that this option can be time-consuming and will fail
             unless you have sufficient permissions.
  -e         Displays Ethernet statistics. May be combined with -s.
  -n         Displays addresses and port numbers in numerical form.
  -o         Displays owning process ID associated with each connection.
  -p proto   Shows connections for the protocol specified by proto;
             proto may be any of: TCP, UDP, TCPv6, or UDPv6.  If used
             with the -s option to display per-protocol statistics,
             proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6,
             UDP, or UDPv6.
  -r         Displays the routing table.
  -s         Displays per-protocol statistics. By default, statistics
             shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, UDPv6.
             -p option may be used to specify a subset of the default.
  -v         When used in conjunction with -b, will display sequence of
             components involved in creating the connection or listening
             port for all executables.
  interval   Redisplays selected statistics, pausing interval seconds
             between each display.  Press CTRL+C to stop redisplaying
```

10.8 NBTSTAT

NBTSTAT is a Windows command line utility to display protocol statistics and current TCP/IP connections using NBT(NetBIOS over TCP/IP).

```
-a (adapter status)   Lists remote machine's name table given its name.
-A (Adapter status)   Lists remote machine's name table given its
                      IP address.
-c (cache)            Lists NBT's cache of remote [machine] names and
                      their I addresses.
-n (names)            Lists local NetBIOS names.
-r (resolved)         Lists names resolved by broadcast and via WINS.
-R  (Reload)          Purges and reloads the remote cache name table.
-S (Sessions)         Lists sessions table with the destination IP
                      addresses.
-s (sessions)         Lists sessions table converting destination IP
                      addresses to computer NETBIOS names.
-RR ReleaseRefresh)   Sends Name Release packets to WINS and then,
                      starts Refresh.
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
                      redisplaying statistics.
```

10.9 NETSH

Netsh is a Windows command line scripting utility to modify network setting useful for resetting TCP/IP stack.

10.10 NET

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

10.11 Browstat

Browstat is a Microsoft utility that displays which PC is acting as Master Browser and other stats about network browsing. In a Peer-to-Peer LAN each workgroup elects a machine to act as Browse Master. The Browse Master collects and distributes information about file and printer shares. Browstat does not come bundled with XP it must be downloaded.

This is the status report from our LAN. It was obtained from a client PC. Tribble is a desktop (XP) acting as file server. Because Tribble is running desktop, rather then server O/S, Browstat has limited ability to retrieve information. However in most cases what is important is simply being able to determine which PC is acting as master browser.

```
Status for domain HOMELAN on transport \Device\NetBT_Tcpip_{8927E1F6-
3E61-445B-822F-DF018AC0B1EF}
    Browsing is active on domain.
    Master browser name is: TRIBBLE
Could not connect to registry, error = 53
Unable to determine build of browser master: 53
    \\\\TRIBBLE     .  Version:05.01  Flags: 51003 NT POTENTIAL MASTER
    1 backup servers retrieved from master TRIBBLE
        \\TRIBBLE
    There are 2 servers in domain HOMELAN on transport
\Device\NetBT_Tcpip_{8927E1F6-3E61-445B-822F-DF018AC0B1EF}
    Unable to retrieve server list from TRIBBLE: 64
```

10.12 Ethereal/WireShark

When you need to get down and dirty to see exactly what is going on over the wire nothing bets a packet sniffer. Sniffers observe and display incoming and outgoing packets. If you have a network with managed switches switch can be configured to pass packets of interest to the test PC. When used with unmanaged switch need to run WireShark on the PC of interest. This is one of the downsides of using switches vs hubs since switches limit most traffic to selected endpoints.

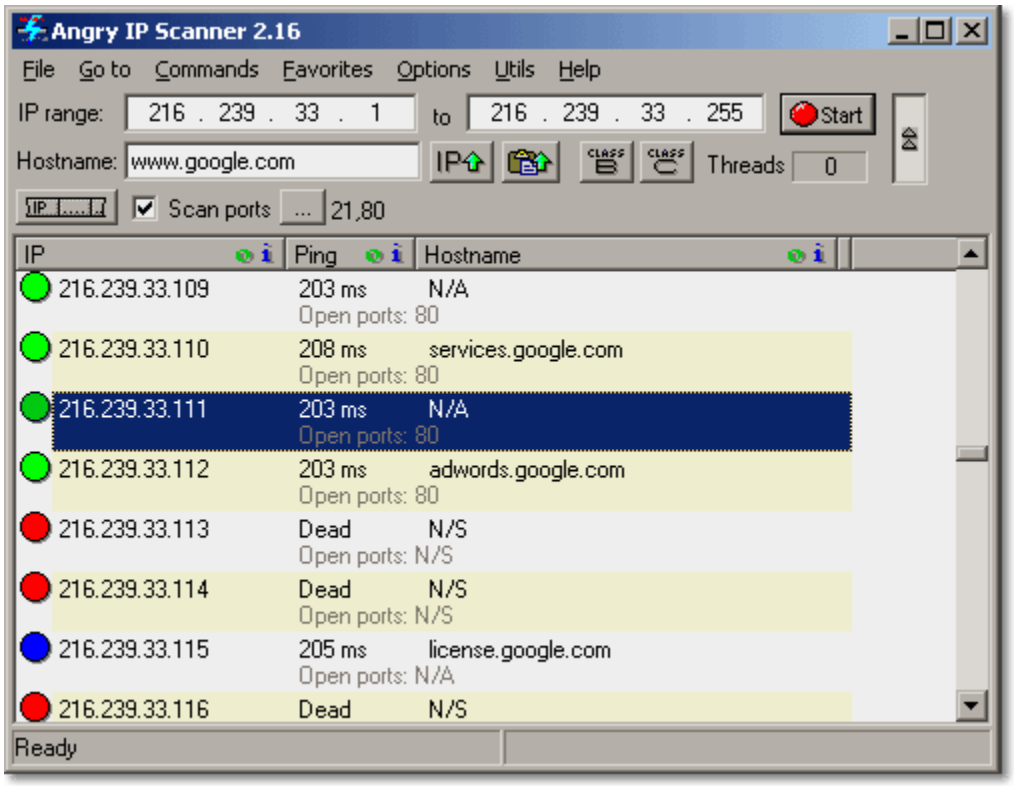
Ethereal is a very popular open source diagnostic program recently renamed WireShark.

10.13 Belarc Advisor

Belarc Advisor is a freeware (for personal use) application that displays hardware and software configuration information.

10.14 Angry IP

AngryIP is a useful utility to view information about which devices are connected to the LAN. Also facilitates finding unauthorized devices connected to the LAN.



10.15 Debugging 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 demarcation point between 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. AutoIP address is in a different subnet than private addresses 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 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 PC's 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 refer to file sharing section.

WAN Debug

- If your DSL or Cable modem has a ready light make sure it is on. This indicates modem is communication properly over the DSL or Cable network.
- If modem is able to report status use that information to verify physical connection is working correctly.
- 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 11/2007 Broadbandreports.com address is: 209.123.109.175. If that works you have identified a DNS problem. If 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.
- If you have DSL or dialup and are experiencing slowness, temporally connect 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.

Internet access problems can be caused by many things: 1) your computer, 2) other computers on LAN, 3) LAN, 4) router or ICS, 5) first-mile WAN connection, 6) internal ISP routing, 7) Internet backbone, 8) ISP used by the remote host, 9) remote LAN and lastly, 10) remote host. The trick is to quickly determine which link in the chain is causing the problem.

11 Laptop – Internet on the Road

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.

12 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 located in-house or operating out of a hosting service. Registering a domain name creates a permanent Internet presence regardless of how business connects to the Internet and where servers are located.

12.1 Registering a Domain Name

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. Registrars coordinate with InterNIC or other registration agencies to insure each registered domain is unique within its TLD.

The registration process provides information on domain name ownership and creates records that point to the nameservers used to tell remote users the IP address of your site. 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.

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.

12.1.1 Email

With a registered domain email is addressed to the domain, not some third party. This personalizes your businesses 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.

12.2 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: Hollis Hosting
Contact: admin@tschmidt.com
Visit: http://HollisHosting.com

Domain name: tschmidt.com

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

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

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

Status: Locked

Name Servers:
ns1.hollishosting.com
ns2.hollishosting.com

Creation date: 04 Nov 1998 05:00:00
Expiration date: 03 Nov 2009 05:00:00

12.2.1 Administrative

Administrative information records data about site ownership and contact.

12.2.2 Technical

Technical information records data about network operation center contact.

12.2.3 Nameservers

Nameservers' listed in the Whois database are the authoritative servers for your domain. These are the servers used by DNS to convert a domain name to IP address. 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 authoritive nameserver become inaccessible.

12.3 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.

12.3.1 Address Records (A)

Address records map host name to IP address.

12.3.2 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.

12.3.3 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.

12.3.4 Pointer Records (PTR)

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

12.3.5 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.

12.3.6 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 Record for Tschmidt.com

Answer records

NAME	CLASS	TYPE	DATA	TTL
tschmidt.com	IN	A	72.37.245.142	14400s (4h)
www.tschmidt.com	IN	CNAME	tschmidt.com	14400s (4h)
tschmidt.com	IN	MX	preference: 10 exchange: tschmidt.com	14400s (4h)
tschmidt.com	IN	NS	ns2.hollishosting.com	86400s (24h)
tschmidt.com	IN	NS	ns1.hollishosting.com	86400s (24h)
tschmidt.com	IN	SOA	server: ns1.hollishosting.com email: hbidad@gmail.com serial: 2007122701 refresh: 86400 retry: 7200 expire: 3600000	86400s (24h)

minimum ttl: 86400

Authority records

NAME	CLASS	TYPE	DATA	TTL
tschmidt.com	IN	NS	ns2.hollishosting.com	86400s (24h)
tschmidt.com	IN	NS	ns1.hollishosting.com	86400s (24h)

Additional records

NAME	CLASS	TYPE	DATA	TTL
tschmidt.com	IN	A	72.37245.142	14400s (4h)

12.4 Public Server

There are many ways to operate a publicly accessible server, using a virtual server as part of a hosting service, collocate your equipment at a data center, or run the server locally.

12.4.1 Hosting Service

The easiest way to set up a web site is with a hosting service. Use of a hosting service maintains 24/7/365 service and keeps site traffic off first-mile Internet connection. Even companies with only dialup Internet access are able to 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. We recently switched to a different local hosting service Hollis Hosting at a cost of $30 per year plus another $10 for domain registration. Most hosting services have business relationships with a domain registrar. This allows one stop shopping for domain registration/renewal and hosting service. Our name is registered with eNom, a popular registrar used by many hosting services. The hosting service also runs virtual SMTP and POP servers to send and receive email.

Normally one has to register a domain name to allow public access to a server. Some hosting services allow customers to set up a web site without a domain name. The virtual site is assigned a name that looks something like http://www.hosting.net/~yourbiz. This uses the domain name of the service as the starting point to access your site. My daughters' web site is an example if this type of service.

12.4.2 Collocation

Most hosting services offer collocation where customer is able install their own equipment in a secure area. Collocation services typically provide redundant high-speed access and emergency backup power.

This allows complete flexibility as to equipment and software used to support the site and limits access to sensitive company data to in-house IT personnel.

12.4.3 On Site Hosting

Large companies often host their own sites since they have the necessary expertise and already run extensive data centers. On site hosting is also an option for casual 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.

Most residential ISPs prohibit customers from operating servers. Some enforce this restriction aggressively other turn a blind eye unless there is a problem. My ISP, Verizon, does not allow servers on residential connections, but not enforce the restriction. They also block incoming access to TCP Port 80, the initial port used to connect to Web server. This restriction requires the use of some other port.

12.5 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 Dreamweaver can be used to good advantage. Numerous companies specialize in web site design if you decide to outsource this task.

12.5.1 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.

12.5.2 Robots File

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.

12.6 Managing site

CPanel is a popular application used by both customers and hosting services to manage web, FTP, and email accounts. It also generates statistics to analyze who visits the site, what pages they view and how long they stay. Prior to the popularization of cPanel separate applications were used to manage customer account, create email accounts and generate usage statistics.

For example creating a new email account is as simple as entering an account name and password for that account.

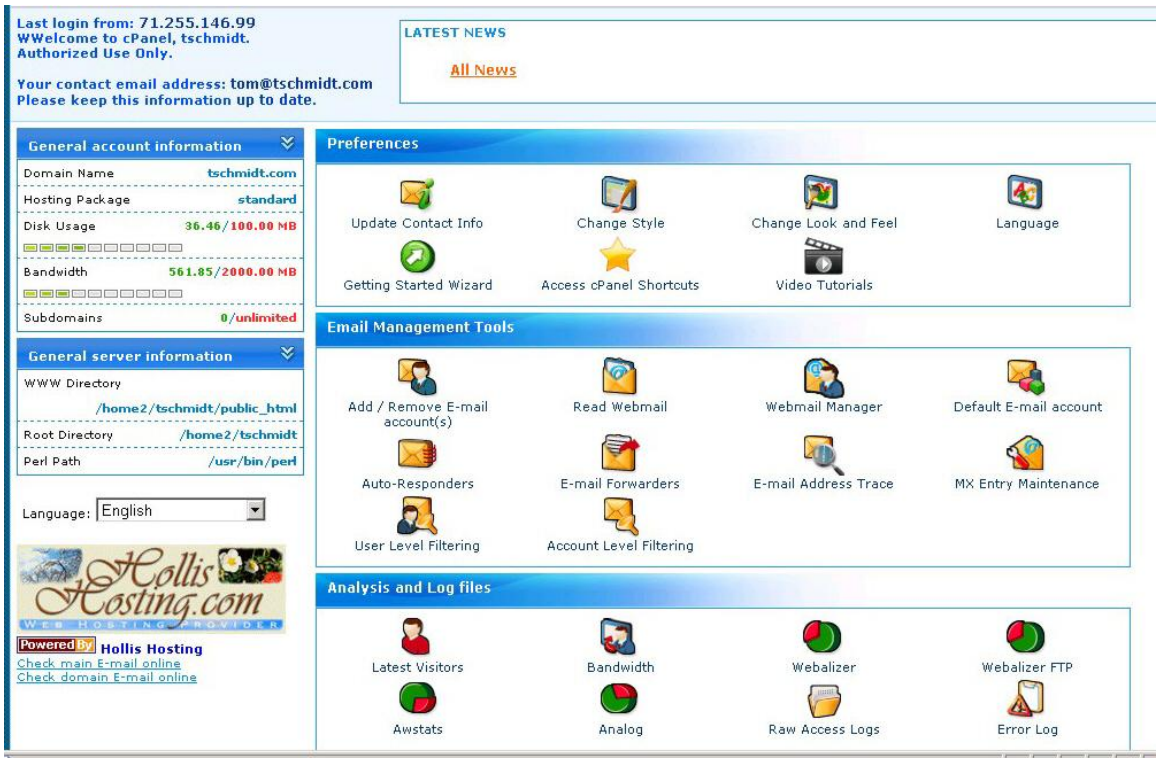


Figure 28 cPanel Welcome Screen

Conclusion

Setting up a SOHO network has been an interesting and rewarding experience. 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 needed 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 to identify and 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