Schmidt Consulting

Living with a Small Office Home Office (SOHO) Network

2016 Edition

12/8/2015

Tom Schmidt
tom@tschmidt.com
http://www.tschmidt.com

Abstract

This paper documents our experience setting up and using a small office home office (SOHO) network over more than fifteen years. It offers guidance on selecting a broadband Internet Service Provider (ISP), presents wired and wireless Local Area Network (LAN) options, describes Internet sharing method, and discusses numerous network services.

Our Internet access is DSL provided by a competitive local exchange carrier (CLEC). An ADSL2+ router is connected to a 16-port Gig Ethernet switch allowing multiple devices to share the connection. An 802.11n Access Point provides Wi-Fi connectivity throughout the house. LAN services include: file sharing, media server, automatic system backup, printing, NTP timeserver, Syslog server, private internal website, personal weather station, multiple home automation controllers and cell phone Wi-Fi offload.

We use a hosting service for our business web server and e-mail. Hosting moves web site traffic off the broadband connection. It also significantly eases the task of securing the local network. A registered domain provides a persistent email address reducing risk of losing contact with colleagues and friends.

A Gig Ethernet switch replaced the Fast Ethernet switch resulting in faster internal LAN transfers. We switched to a mobile virtual network operator (MVNO) for cell phone service with an interesting technology wrinkle; they default to Wi-Fi whenever possible to minimize cellular usage.

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 network experience was limited to interactions with corporate Information Technology (IT) department. Back then home networks were pretty rare and some residential ISPs even prohibited them. Today home networks are ubiquitous and the proliferation of handheld devices means residential customers often use a combination of wired and wireless devices. It has been fun documenting the network's evolution over the years.

We began with a V.90 dialup connection, Wingate connection sharing software running on a Win98 laptop and a small 10 Mbps Ethernet hub. Over the years LAN has expanded beyond my home office to encompass the entire house with a total of 24 Ethernet ports serviced by a Netgear Prosafe Plus GS116Ev2 16-port Gig Ethernet switch. A Netgear WN802Tv2 802.11N Access Point provides Wi-Fi connectivity. Current Internet access is 7Mbps/1Mbps ADSL provided by a CLEC FirstLight Fiber. A ZyXel P660R-D1 ADSL2+ router provides Internet sharing. Internet speed is relatively low by current standards but adequate for our needs.

Each time I upgrade my office workstation the old PC gets recycled as a low end server. In addition to file sharing it runs: Tardis network time service, Abyss web server Kiwi Syslog log server and a Davis weather station with Ambient virtual weather station application. To reduce clutter I use a Belkin 4-port keyboard, video and mouse (KVM) switchbox to switch between: 1) main PC, 2) server and 3) dual boot PC (XP/Ubuntu). The fourth port on the KVM is cabled along with Ethernet and power making it easy to temporally connect additional systems for setup and testing.

WD TV Live Hub allows us to watch Netflix and other Internet content on our living room TV and acts as a media server. A Hauppage TV PCI tuner card in my office PC delivers RF TV and FM radio.

Over the last few years I've built several home automation systems for various parts of the house: greenhouse, wood heat, window ventilator and most recently our aquarium. Each of these controllers has a web interface requiring an Ethernet connection. I've posted details about these and other home automation projects on the writings page of my website.

Printer is a HP Officejet Pro 8100. It replaced a couple of earlier HP printers that died. An Epson V550 flatbed scanner turns paper into electronic documents. It replaced an older HP scanner when I updated to Win7.

Acronis True Image provides automatic online backup of PC data to the server. For offline backup we use several different flavors of external USB drives.

1.1 Goals for SOHO network:

- High speed Internet access
- Share Internet connection
- Wired and Wireless LAN
- Printer sharing
- File sharing
- Internal private web server
- Time synchronization
- Automatic PC backup
- Offline file backup
- Home weather station
- Home automation
- Internet TV

1.2 Organization

This paper discusses Internet access and local area network (LAN) components. A separate paper goes into more detail about ISPs and the tradeoffs among different type of access. Structured wiring for telephone and Ethernet is covered in detail. The security and troubleshooting topics provides information to maintain the network and protect it from intruders.

Lastly I discuss registering a domain name and running a public Internet web 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. Even if you do not run a business registering a domain provides a consistent email address and having a web site gives you flexibility over your Internet presence. For a few dollars per month it is a lot of bang for the buck.

This report is not intended as a competitive product review. The market 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 reader is directed to the many publications and articles on the subject.

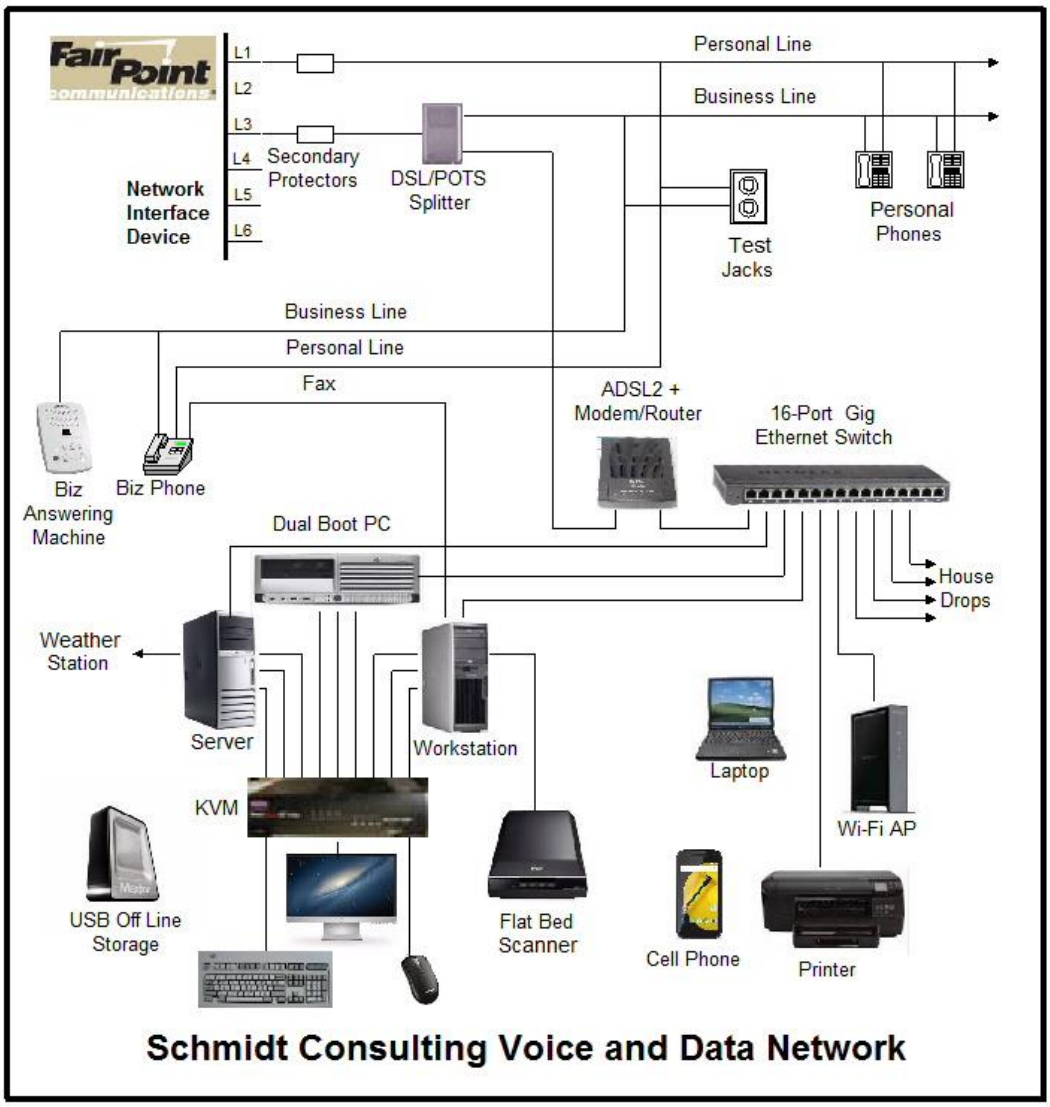


Figure 1 Schmidt Consulting Network

2 Internet Technology – Geek Stuff

This section discusses some of the important technology involved in setting up a SOHO network. While not essential reading it is helpful to know what is going on under the hood.

The Internet was created almost 50 years ago as a means for government and academics to share expensive mainframe computers. Today it is the preferred method to access all sorts of digital information: data, voice and video. Internet is a contraction of Inter Networking, literally a network of networks. Creation of the Word Wide Web (WWW) in the 1990's vastly expanded Internet popularity by providing a Graphical User Interface (GUI) on what until then had been text based. 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.

The Internet is a packet network that transports data from one host to another over a network shared by many users. Internet is fundamentally different than the legacy public switched telephone network (PSTN). The telephone network establishes a dedicated path for the duration of the call. This reservation exists whether it is needed or not. The Internet on the other hand works on chunks of data called packets. Packets are presented to the Internet on an as required basis. At each hop a router examines the packet's address field and determine how best to forward it toward the destination.

2.1 ISP

Internet Service Providers (ISP) connects end users to the Internet. The incredible popularity of the Internet is driving demand for higher speed and lower cost. Connection between ISP and customer is often called the last-mile. I prefer the term first-mile, because it elevates end user's importance. Internet's value proposition is its ability to connect end points. Without end points the network is useless.

Even though we are in a fairly rural area wired residential broadband is available from multiple sources:

1) Comcast DOCSIS, multiple system operator (MSO)
2) FairPoint Communication ADSL, incumbent local exchange carrier (ILEC)
3) FirstLight Fiber ADSL, competitive local exchange carrier (CLEC)

We have FirstLight ADSL bundled with phone service. Typical sync speed is 7Mbs down/996kbps up. This is a significant improvement from the 3360/864 kbps speed provided by FairPoint and previously Verizon ADSL of 1792/448. Unlike FairPoint the CLEC does not cap the speed. Sync speed is the result of circuit characteristics. If phone loop is very short maximum speed is 24/1 Mbps. In our case we are pretty far away so speed is lower but still a very significant improvement over what we had before. Over the year download speed varies from a low of 6.5Mbps to high of 7.4, upload is a stable 996kbps.

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

2.2 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. If you are downloading a large file speed is important, latency less so. If on the other hand you are conducting a Voice over IP (VoIP) phone call latency is critical to maintaining good communication.

A useful analogy is to think of a truck full of DVDs going from Point A to B. From the time truck begins its journey latency is high – while the truck travels to destination recipient can do nothing. However once it arrives communication speed is very high due to the tremendous capacity of the DVDs. Conversely a dialup connection has low latency since it only takes a few milliseconds for data to arrive at its destination but speed is very low – limited by telephone network performance. For a more in-depth explanation see "It's the Latency Stupid."

2.3 Naming Convention

The Uniform Resource Locator (URL) is a human friendly handle rather than the numeric IP addresses. Translation of URL to IP address is performed by the domain name system (DNS). 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, GOV, UK, TV domains 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. 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 when we were registering our domain name the preferred name schmidt.com was already assigned so we choose tschmidt.com.

Often an organization needs to create sub domains such as www.tschmidt.com for web access, mail.tschmidt.com for email or product.tschmidt.com for product info. Once the domain name is registered it is guaranteed to be unique so the owner is free to add as many sub domains as desired.

2.3.1 Domain Name System (DNS)

When a domain is registered the registrar database contains a list of 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 URL is entered into the browser, such as http://www.google.com/, browser first checks to see if host is on the LAN. 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. This is a broadcast mechanism and works well on small LANs but does not scale well. If host name is not found locally translation request is passed to the DNS Resolver.

Let's trace what happens when we look up http://www.google.com. Since the Google URL is not located on the LAN 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 queried for the address of the Google Nameserver. The server returns the address of the authoritive Nameserver for the Google domain. It is important to note root Nameserver does not know the address of the Google servers other than the Google Nameserver. Google Nameserver is then asked for the address of the desired host. Often sites create sub domains for specific servers, the process continues until the address of the desired host is determined. Once browser learns host's IP address it is able to communicate. 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. URL name lookup is normally accomplished in a few milliseconds.

2.3.2 DNS Security Extensions (DNSSE)

As the Internet becomes ever more pervasive attention has been drawn to lack of DNS security. Hackers are able to easily poison cached DNS information. Doing so allows an attacker to redirect browsers to compromised site for nefarious purposes. A high priority initiative is to implement Domain Name System Security Extensions (DNSSEC) to counteract this sort of attack and increase level of confidence in DNS.

2.4 Routing

Internet is a routed network. This is very different then broadcast discovery scheme used locally by Ethernet or circuit switching used by telephone network. When a computer wants to communicate with a resource not available locally it forwards the packet to gateway router. The gateway router is the interface

between the local network (LAN) and the Internet. The router forwards packets to the proper destination or to next router in the chain. In order to learn network topology routers use a variety of techniques to communicate among themselves such as RIP and OSPF. ISP routers 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.

The routing task for typical residential router is trivial as there is usually only one connection to the Internet. The router simply forwards all packets to the ISP's edge router.

Doing a trace route to an Internet host provides a graphic indication of how routing works. Here is a trace route from my east coast home office to my web site hosted on the west coast.

Tracing route to tschmidt.com [67.220.209.110]over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.2.1
2	28 ms	28 ms	28 ms	xx.milford1-1.nh.g4.net [66.211.144.97]
3	29 ms	28 ms	28 ms	gi-3-1.nashua1-1.nh.G4.net [216.177.5.178]
4	30 ms	29 ms	29 ms	ge-24-v108.merrimack3-1.nh.G4.net [216.177.5.150]
5	35 ms	35 ms	34 ms	gi-21-v358.manchester3-1.nh.G4.net [216.177.30.153]
6	29 ms	29 ms	29 ms	ge-0-0-3.manchester1-9.nh.G4.net [216.177.5.45]
7	193 ms	199 ms	204 ms	s5-0-24-0.cr01.4-2.mnchnhcohba.seg.NET [216.107.229.209]
8	30 ms	30 ms	30 ms	66-109-52-73.tvc-ip.com [66.109.52.73]
9	35 ms	34 ms	34 ms	66-109-52-21.tvc-ip.com [66.109.52.21]
10	35 ms	34 ms	34 ms	66-109-52-86.tvc-ip.com [66.109.52.86]
11	39 ms	47 ms	49 ms	v204.core1.ymq1.he.net [209.51.163.105]
12	61 ms	45 ms	45 ms	10ge14-4.core1.nyc4.he.net [184.105.222.97]
13	106 ms	113 ms	105 ms	10ge10-3.core1.lax1.he.net [72.52.92.226]
14	105 ms	106 ms	115 ms	10ge1-3.core1.lax2.he.net [72.52.92.122]
15	106 ms	106 ms	106 ms	webnx.com.any2ix.coresite.com [206.223.143.172]
16	107 ms	106 ms	106 ms	100-42-223-146.static.webnx.com [100.42.223.146]
17	105 ms	105 ms	105 ms	100-42-223-174.static.webnx.com [100.42.223.174]
18	106 ms	106 ms	106 ms	110-209-220-67.verygoodserver.com [67.220.209.110]

Trace complete.

2.5 Unicast vs Multicast

Most Internet traffic is between one sender and one receiver (unicast). Multicast emulates traditional broadcast one-to-many model. This is a more efficient way to stream identical information to many endpoints. Unfortunately even though specification is mature not many ISPs have implemented multicast. In general if you listen to Internet radio or TV it is being transmitted as unicast.

2.6 TCP vs UDP

There are two principle ways to transmit information over the Internet; Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP creates a session where receiver acknowledges each packet and lost or damaged packets are resent. This is ideal for file transfer type communication. Recovery from missing or corrupt packets is more important than latency. With UDP transmitter sends data without expecting feedback from receiver. UDP is commonly used with streaming audio and video transmission where latency is more important than accuracy and insufficient time exists to recover from transmission errors. If an error occurs it is up to the receiver to fake the missing data.

2.7 Quality of Service (QoS)

Internet is an egalitarian best effort network. This works amazing well for transferring large chunks of data from point A to point B. The network continues to operate in the presence of all sorts of impairments and

failures. However: best effort does not work as well with latency sensitive applications such as telephony and streaming media. For example during a Voice over IP (VoIP) phone call round trip latency should be under 150ms, in each direction. Excessive delay makes carrying on a conversation difficult and with extreme delay virtually impossible. Streaming media is less sensitive to latency as long as average data rate exceeds playback rate. When a stream is first started an elastic buffer is filled prior to beginning playback. The buffer fills and empties dynamically. As long as latency does not allow the buffer to completely empty the effect is hidden from the user.

QoS problems typically do not occur on the LAN where bandwidth is plentiful. The most common chokepoint is first-mile access, the ISP's edge network. Most residential broadband links are relatively slow, especially upload capacity, and they are often heavily oversubscribed to minimize capital cost. 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 packets go to the head of the queue. This simple strategy works well if latency critical traffic is a small percent of total so bumping its priority has little effect on other traffic. QoS marks packets with a (Diffserv) priority level. When congestion occurs higher value packets are delivered as quickly as possible. Lower value packets are delayed or discarded. QoS services allow more graceful degradation by moving high priority packets to the head of the queue. QoS is not a panacea, it does not create more capacity, and it simply redefines winners and losers.

2.8 Flow Control - Back Pressure, TCP Slow Start, Receive Window

When a host begins transmission it has no idea how fast the intervening links are between it and the remote host. Switched Ethernet uses back pressure to prevent overwhelming slower links. An Ethernet receiver asks the transmitter to stop sending data by sending it a pause frame. This occurs if the outgoing switch port becomes congested.

At the IP level transmitter uses a technique called slow-start by sending a few packets then waiting for acknowledge. The faster ACKs are received the more packets transmitter sends per unit of time. TCP Receive Window (RWIN) parameter determines how many unacknowledged packets can be outstanding before transmitter must stop transmitting and wait.

2.9 IP Address Configuration

Each IP device (host) must have an address. Addresses may be assigned: manually, automatically by Dynamic Host Configuration Protocol (DHCP) server or by the client itself using Automatic Private IP addressing (APIPA). Historically a system administrator manually configured each host with a static address and other IP parameters. This was laborious and error prone. DHCP simplifies the task by automating address allocation. When a host detects it has a network connection it transmits a DHCP discovery message. If the LAN contains a DHCP server the server responds with all the information the client needs to utilize the network. DHCP has been extended to allow automatic configuration if the client cannot find a DHCP server. In that case client 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.

IPv4 assigns each host 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. Classless inter-domain routing (CIDR) and Network Address translation (NAT) are two techniques used to delay the day of reckoning. 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 but to go through the pain of conversion. My ISP does not currently support IPv6 so I have limited experience with it.

2.9.1 IPv4 Dotted-Decimal Notation

IPv4 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 largest 255.255.255.255.

2.9.2 Subnet

IP addresses consist of two parts a Network-Prefix and Host address. Subnetting allows IP addresses to be assigned efficiently and simplifies routing. The subnet mask defines the boundary between network and host portions of the 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: 255.255.255.0 allowing up to 254 hosts (computers) also called a /24 (pronounced slash 24) subnet because the first 24-bits of address are fixed. Host addresses are allocated from the last octet (8-bits). The reason for 254 rather than 256 hosts is lowest address is reserved as the network address and highest address is used for multicast.

2.9.3 Class vs Classless Inter-Domain Routing (CIDR)

When Internet was initially developed divide between network prefix and host address was embedded within the address itself, rather than 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 provide 16,777,213 host addresses. The lowest address is reserved as the network address, highest for broadcast. The 127 octet 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 provide 65,533 host addresses.

Class C – first octet is in the range 192 – 223 (110XXXXXb). 24-bits reserved for network portion leaving 8 for host addresses. 8-bits provide 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 subnet mask 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 Local host Address

127.0.0.1 is the Loopback local host address. This is useful for testing to makes sure the network stack. Sending data to the Loopback address causes it to be received without actually going out over the physical network. The entire /8 block is reserved for local loopback but by convention 127.0.0.1 is used as the loopback address...

2.9.5 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)

2.9.6 Private Address Block

During work on impending IPv4 address shortage RFC 1918 reserved three blocks of private addresses. Private addresses are ideal for our purposes because they are not used on public Internet. This allows them to be used and reused without risk of colliding with Internet hosts. This eliminates the need to obtain a block of routable addresses from the ISP. Internal hosts are assigned an address from RFC 1918 private address pool.

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.*

2.9.7 APIPA Address Block

A fourth block of private IP addresses is reserved for APIPA, automatic private IP addressing. If a host is configured to obtain a dynamic address and a DHCP server cannot be found host assigns an address to itself from this pool of reserved addresses. Host picks an address from the APIPA 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)

APIPA is useful for tiny networks that do not include a DHCP server. Before AutoIP user had to manually configure address and subnet mask to set up a simple IP network.

2.9.8 Network Address and Port Translation

Residential ISP accounts are typically assigned a single IP address. This limits customer to connecting a single computer to the Internet. Network Address Translation (NAT) is used to convert multiple private LAN IP addresses to/from the single public IP address assigned by the ISP. To enable multiple sessions of the same type to operate simultaneously Port numbers also need to be changed. NAT allows a virtually unlimited number of devices, assigned private IP addresses, to share an ISP account even if the ISP only provides a one IP address.

NAT is widely used on residential networks to share a connection among multiple computers.

2.9.9 Address Resolution Protocol (ARP)

IP addresses represent Internet global numbering scheme. Addresses used by local network are 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.

2.9.10 Ports

Internet host is able to carry on multiple simultaneous communications sessions. This raises the question how does the computer know how to respond to specific 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. Once the connection is established client and server agree on high number ports to use to actually transfer data.

2.10 IPv4 vs IPv6

IPv4 is the predominant protocol used on the Internet today. A defining characteristic is its 32-bit address space. Each host on the Internet needs a unique address. The IPv4 address field is 32-bits wide able to address a maximum of 4,292,967,295 hosts. 4 billion is a pretty large number and it certainly was back in the 1980's when the Internet was limited to a few educational intuitions and the federal government.

To put 4 billion into perspective present worldwide population is a little over 7 billion. It is true that not everyone has Internet access but many do and those who have access often have multiple devices. At any given time in our home there are typically a dozen devices connected to the Internet.

The address limitation of IPv4 was recognized long ago. While mechanisms such as private addresses and NAT have extended the life of IPv4 it is clear the address range needs to be expanded. A watershed event occurred February 2011 when the last IPv4 address blocks were handed out to regional registrars.

The successor to IPv4 is IPv6 with a massively expanded address range of 128-bits. IPv6 brings a host of improvements to the Internet but because it is not directly backward compatible with IPv4 adoption has been very slow. Companies and service providers are faced with a typical chicken and egg problem. There is no first mover advantage. Being the only one able to support IPv6 has no advantage.

3 ISP Modem – High Speed for (Almost) Everyone

A modem is usually required to convert the local connection, typically Ethernet, to the signaling and physical interface used to connect customers to the ISP network. In the case of DSL it is an ADSL or VDSL (very high speed DSL) modem, Cable uses some flavor of DOCSIS and the holy grail of first-mile broadband, fiber optic, is typically a version of passive optical network (PON). The granddaddy of modems uses the voice grade telephone network but the upper limit of V.92 dialup modems is low, only 56kbps. That can be useful for some specialized remote access applications and even slower dialup modems are used for alarm dialers where connect time is more important than transfer speed. But for general purpose Internet access dialup it is almost unusable since most web sites today are optimized for multimegabit per second access.

When we first set up our SOHO network back in 1998 used Wingate connections sharing software running on a laptop to share a v.90 dialup connection. Over time we have used several different modems and routers as our ISP and connection speed changed. Our current connection is ADSL2+. My preference is a combo ADSL modem/router because it makes access to low level modem info easy. Having access to modem status is handy for troubleshooting. Our current ADSL modem/router is a ZyXEL P660R-D1 single port router. We have ADSL through a competitive local exchange carrier (CLEC) so the rest of the modem discussion will be about DSL.

3.1 ADSL Overview

ADSL takes advantage of the fact the subscriber copper circuit has unused capacity. Analog voice uses only a tiny fraction of available capacity. With clever engineering that unused capacity can be used to send and receive data. A tremendous amount of engineering has gone into DSL to allow 100 year old telephone copper loop deliver multimegabit Internet service. ADSL modems use a technique called discrete multi-tone (DMT) to divide available capacity into small chunks and send a few bits over each separate tone. DMT has the advantage of being able to work around impairments by changing the number of bit bits sent in each tone.

DSL is a distance limited technology. The signal weakens as it travels down the wire and picks up noise limiting connection speed. The higher the frequency the faster it degrades with length. One does not know in advance how fast the connection will be until it is turned up. ISPs often market DSL as “up to xx Mbps” causing customer frustration when actual speed is less than marketing representation. Customer must be within 18,000 feet (3.5 miles) of the central office or remote terminal to qualify at all. The closer you are the more likely to obtain high speed.

ITU ADSL specification has gone through several enhancements. ADSL2 and ADSL2+ delivers higher speed and longer range then first generation equipment. ADSL delivered up to 8 Mbps down (toward customer and 1 Mbps up. ADSL2 increased download speed to 12 Mbps, upload is unchanged. ADSL2+ doubles maximum download speed to 24 Mbps over relatively short distances. Another standard, VDSL2 is able to deliver even higher speed but only over a few thousand feet of cable.

DSL is a complex and fascinating technology. The interested reader is invited to research the topic in depth. Allied Telesis has a White Paper that goes into much greater technical detail.

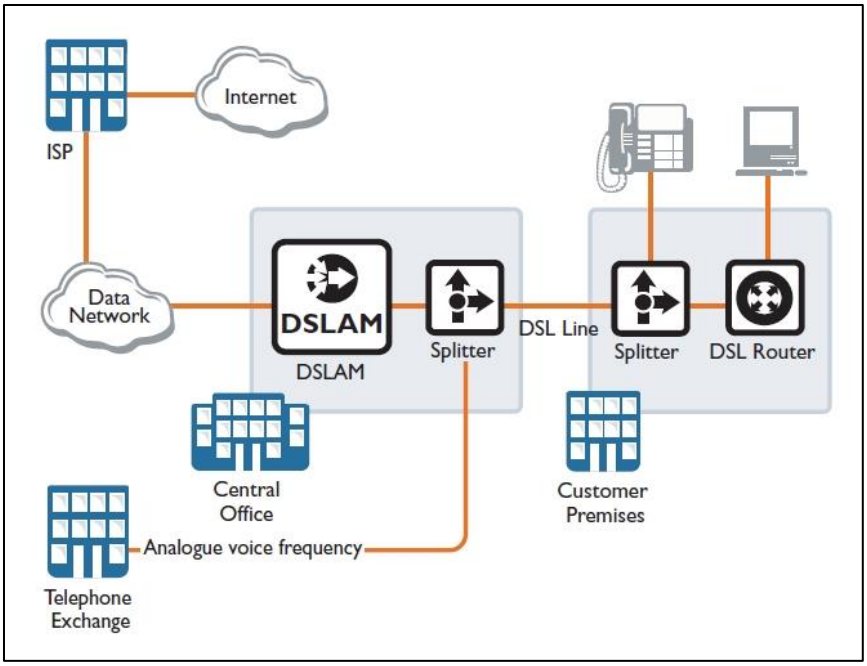


Figure 2 DSL End to End

3.1.1 Inline Filters vs Whole House POTS/DSL Splitter

Because DSL shares the same circuit as plain old telephone system (POTS) filters are required at both ends to prevent high frequency DSL signals from interfering with telephone operation and voice grade equipment from degrading DSL. Customer has the option to use an in-line filter at each non-DSL device or installing a whole house POTS/DSL splitter. To reduce deployment cost rather than sending a tech out to install a whole house splitter ISPs typically provide a self-install kit including inline filters for the customer to self-install. I'll talk more about wiring in a later section.

3.1.2 Fastpath vs Interleave

Because DSL uses copper phone lines it is sensitive to electrical impulse noise. To make the signal more resistant ADSL adds redundant bits to each frame called forward error correction (FEC). If noise corrupts some of the bits the receiver is able to correct the corrupt data as long as it is not too extensive. If too many bits are corrupt the frame cannot be recovered. To increase noise tolerance DSL interleaves multiple frames. When the receiver deinterleaves the data noise damage is now spread over multiple frames increasing the odds receiver will be able to recover the data.

As with any engineering tradeoff there is no free lunch. Interleave increases latency because multiple frames must be queued up prior to transmission. The improved effective signal to noise ratio (SNR) is advantageous for file transfer and streaming media. Correcting corrupt data on the fly eliminates the need for retransmission. With streaming media there is not enough time to request retransmission so receiver needs to fake the missing data, resulting in audible or visual anomalies. How annoying that is depends on how much data has gone missing.

On the other hand latency sensitive applications benefit from fastpath, because it reduces latency at the expense of signal integrity. Fastpath reduces DSL latency by about 10ms. In most cases this savings is swamped out by other end-to-end Internet latencies. But if you are a gamer and your line stats are good may be worthwhile experimenting with fastpath.

3.2 ADSL Modem

Several years ago we switched to a competitive local exchange carrier (CLEC). They rent copper subscriber circuits from FairPoint, our incumbent local exchange carrier (ILEC), and co-locate their equipment in FairPoint central offices. FirstLight markets ADSL differently as it does not impose a speed cap. Speed is based solely on what the circuit is able to handle. We were pleasantly surprised to see sync speed increase to 7 Mbps down and almost 1 Mbps up. Download is now about twice the speed as when we were using FairPoint DSL.

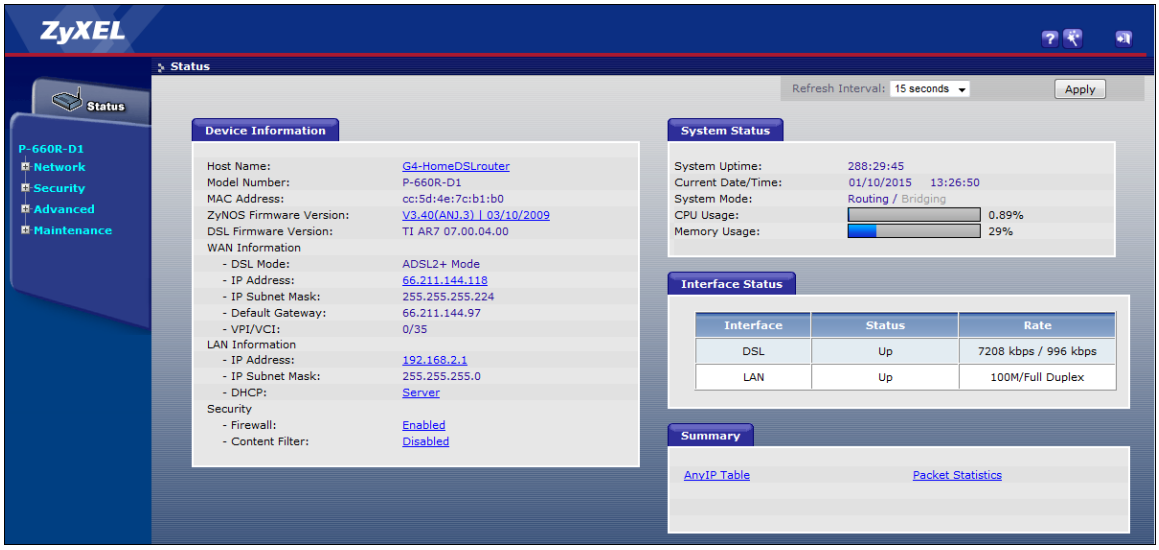


Figure 3 DSL Router Status Page

The ZyXEL router has a nice feature that if you do not enter a password to log in the main status screen is displayed in read only mode. This lets anyone view connection status but restricts being able to make changes. Because speed is not capped it floats based on line conditions. Download speed varies by a few hundred kilobits per second; upload does not vary at all.

3.3 Modem WAN Interface

The Wide Area Network (WAN) side of the modem is responsible for encoding and recovering bits over the phone line and extending the ISP's network to the customer. Often times the ADSL modem is combined with a residential NAT router, Ethernet switch and in some cases a Wi-Fi Access Point to deliver multiple services in one inexpensive combo device. However the modem function remains the same, to interface to the phone line and connect to the ISP equipment.

The main functions of the ADSL modem are:

- Physically connect to phone line
- Create and recover ADSL signals
- Data encapsulation typically using ATM between customer and ISP
- Allow ISP to automatic configure WAN side IP settings

3.3.1 ATM

Most DSL connections use Asynchronous Transfer Mode to transport data over the DSL link. ATM is designed to transport low latency digital telephone traffic. Data is transported in 53-byte cells of which 48 carry data the other 5 are overhead. ATM is a legacy of circuit switched telephone network and uses virtual circuits. When setting up the modem need to specify the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). Unfortunately when used for data ATM adds significant overhead, the so called ATM cell tax.

There are various methods of transporting IP packets over ATM, called adaption layers. You need to use the method specified by your ISP.

3.3.2 IP Settings

Once the modem is able to successfully transport data over the DSL link the next step in the process is to configure Internet Protocol (IP) parameters so the computer or router is able to access the Internet. Each device requires an IP address and a subnet mask that identifies the network and host portion of the address. To communicate with other devices on the Internet it needs to know the default gateway server address. This is the address the computer uses to hand off packets when the destination host is not on the LAN. Lastly devices need the address of the DNS server to translate URL name to the IP address of the distant server.

The modem is transparent to IP. What is being configured is the wide area network (WAN) interface which is either the outward facing router interface or if only a single PC is being used the computer itself.

There are three methods ISPs use to configure customer equipment:

- Statically
- DHCP
- PPPoE (or PPPoA)

Most business accounts are configured statically to facilitate running servers. With a static assignment the IP address never changes. The ISP sends customer configuration information and customer in turn manually configures equipment.

Residential accounts typically use DHCP or PPPoE. DHCP works much the same as having a PC connected to a LAN. When modem powers up its first synchronizes to the DSL line then searches for a DHCP server. The DHCP server communicates IP settings to the router. FairPoint and most other ILEC's use Point-to-Point Protocol over Ethernet. PPPoE works much the same as with dialup only much faster. PPPoE requires customer enter a user name and password. The downside of PPPoE is slightly higher overhead and the need to log in and maintain a persistent user session.

FirstLight uses DHCP rather than PPPoE for residential accounts. In the past we would often lose Internet access due to inability to maintain a PPPoE session even though DSL itself was working correctly. DHCP has proven to be much more reliable and has slightly less overhead then PPPoE.

3.3.3 PPPoE and MTU

The downside of PPPoE is that customer needs to login and ISP maintain an active session. Being an encapsulation protocol PPPoE reserves 8 bytes of each 1500 byte packet reducing maxim transmission unit (MTU) to 1492.

Internet packets are limited to 1500 bytes. PPPoE adds 8 bytes of overhead to each packet reducing maximum payload size to 1492. Internet packets can be fragmented and reassembled. 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 protocol stack implements path discovery to automatically limit packet size so fragmentation is not needed. When PPPoE is used maximum transmission unit (MTU) is 1452 bytes: 1452 bytes data + 40 bytes TCP/IP overhead + 8 bytes PPPoE = 1500 bytes. A good indication of packet fragmentation is if sending a little data <1452 bytes works but larger files do not.

The main downside of PPPoE is not the slight extra overhead of the 8 bytes (.6%) but the difficulty maintaining the session. If the session terminates connection is lost until the user logs in again. With a modem this happens automatically so normally hidden from the user. With both Verizon and FairPoint we would normally go days with the same PPPoE session so did not notice the momentary interruption. However on numerous occasions with both ISPs had multiple episodes where modem would log back in and almost immediately be dropped or account was not recognized at all for hours on end. I'm happy to be rid of PPPoE.

3.3.4 Bridged vs Routed

Residential accounts are typically bridged. This means each customer is connected to the ISP's LAN, much like connecting multiple devices to your home LAN. For privacy ISP gear prevents customers from seeing each other.

Business customers with multiple IP addresses and static settings are typically routed. The ISP's router and customer's router talk to one another. If the company uses multiple ISP their router is also responsible for controlling traffic flow.

4 Broadband Router – One Connection Many Computers

In order to share the Internet connection a router is needed to manage the LAN and transfer data between the LAN and the ISP's Network. In some instances the router includes' a modem allowing the router to be connected directly to the ISPs network. In other cases the router's WAN interface is Ethernet to allow it to connect to a separate modem. I prefer using a modem/router combo. This makes accessing modem stats easier than using separate devices and also typically lower power consumption.

If you only need to connect a single device simply plug it into the modem. If you want to use multiple devices you need a router to share the ISP connection. Using a router creates a clear demarcation between LAN and WAN simplifying troubleshooting. LAN services continue to operate even if the WAN connection is lost. The router market is extremely competitive. New routers can be had for less than $50 US and used high end devices go for short money on eBay.

Figure 4 ADSL2+ Broadband Router

4.1 LAN Side Address Management

The goal of using a router is to share your ISP connection with multiple computers. Each device needs an IP address. These address can be either manually assigned by the user or automatically by the router.

4.1.1 LAN IP Address Assignment

The choice for most residential networks is to configure the LAN using RFC 1918 private addresses. By using private addresses and network address translation (NAT) a virtually unlimited number of computers are able to share a single ISP IP connection. Being private the address pool can be used and reused multiple times conserving IPv4 Address space and eliminate need to request and pay for additional public addresses.

There are two ways to configure IP setting on LAN devices, statically and dynamically. Each has benefits and limitations.

4.1.2 Static

The pros and cons of static allocation on the LAN are much the same as on the WAN. Static assignment requires IP parameters: address, subnet mask, gateway address, and DNS address be manually configured on the device. If the LAN is using a mix of static and dynamic addresses it is important to pick a static address outside the range used by DHCP but within the subnet. If a computer is configured statically it is possible the DHCP server will assign the same address to another device. This results in an address collision which will prevent both devices from communicating. We configured the router's DHCP server

to issue addresses in 192.168.2.2 - 192.168.2.100 range with a subnet mask of 255.255.255.0. Static addresses are assigned in the range 192.168.2.101 – 192.168.2.254. This keeps all addresses within the subnet without interfering with each other.

4.1.3 Dynamic

This is the default behavior of most operating systems. When the computer detects it is connected to a network, either wired or wireless, it searches for a DHCP server. The DHCP server in the router responds to the request and assigns each machine an appropriate IP address and other settings. Once the PC is configured it is able to communicate. The address is "leased" to the client. Prior to lease expiration the client attempts to renew it. Under normal conditions this is successful and the lease never expires and the IP address remains the same. If client is off network for extended period of time lease will expire. Next time the computer connects it may receive different IP address.

4.1.4 MAC Reservation

For some devices, such as servers, dynamic addressing is inconvenient. For example the binding to our HP printer is by IP address. If the address changes each PCs needs 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 MAC address. As long as MAC address does not change the device is always assigned the same IP address. This is more convenient than setting addresses manually on each device but achieves the same effect.

A down site of MAC reservation is if you change the router LAN addresses will be once again be randomly assigned. For our LAN I statically assign the address for "servers" and the home automation gear. I let the router dynamically assign addresses to "client" devices such as: PCs, laptops, and cell phones.

4.1.5 Media Access Controller (MAC) Address

Each interface (wired or wireless) has a unique 48-bit MAC address built into hardware. This allows the device to be uniquely addressed. This address is not the same as the IP address.

Excerpt from Assigned Ethernet numbers:

> Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits which specify the interface serial number for that interface vendor.
>
> These high-order 3 octets (6 hex digits) are also known as the Organizationally Unique Identifier or OUI.
>
> These addresses are physical station addresses, not multicast nor broadcast, so the second hex digit (reading from the left) will be even, not odd.

Device manufactures obtain OUIs from IEEE. Each chip is assigned a unique value consisting of the OUI and a serial number allocated from the last three octets. Three octets yield: 16,777,215 values, so the OUI lasts a long time. When the manufacturer exhausts the allocation they need to go back to IEEE for another OUI. Since the first three octets are assigned to the chip manufacturer it is possible to verify who made the chip by looking up the OUI on the IEEE's web site.

4.2 Network Address Translation (NAT)

Most residential ISPs restrict customer to a single IP address. Small size of the IPv4 address (32-bits) space means addresses are in short supply. ISPs often charge extra if more than one address is needed. This creates a quandary; how to cost effectively connect multiple hosts to the Internet? The most common

workaround is Network Address Translation (NAT) using private IP addresses. IETF RFC 1918 reserves 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, more properly Network Address Port Translation since both address and port number are modified, and RFC 1918 private addresses allow a virtually unlimited number of computers to share an Internet connection even though the ISP only provided a single IP address. NAT provides translation between private addresses on LAN side and the single public address issued by the ISP.

Internal LAN traffic proceeds normally; NAT is not required for local traffic between computers on the LAN. When a request cannot be serviced locally it is passed to the NAT router, called a gateway. Router modifies the packet by replacing private address with public address issued by the ISP and if needed changes the port number to support multiple sessions and calculates a new checksum. 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 calculates the new checksum and forwards it to the LAN. 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.

4.2.1 Performance

NAT requires a fair amount of bookkeeping, changing IP and port addresses, and 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 100 Mbps make sure router is up to the task.

NAT translation table size limits the maximum number of simultaneous sessions router is able to maintain. This limit does not affect normal Internet usage. However when Peer-to-Peer (P2P) protocols are used the large number of simultaneous sessions may overwhelm a low-end router.

4.2.2 Security

NAT blocks remotely originated traffic. It functions as a de facto incoming firewall because the router does not know where to forward packets that originates outside the LAN unless specifically programmed with port forwarding rules.

4.2.3 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.

This is not to discourage use of NAT as 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.

4.3 Default Gateway

Local devices on the LAN are able to communicate directly with one another, a router is not required. If a PC has a packet destined for an off LAN device it forwards the packet to the gateway. The gateway router decides how to deliver packets that travel outside the LAN. Since only a single connection exists between our network and the ISP routing is trivial. The router simply forwards all non-local packets to the ISP's edge router.

4.4 DNS

The Domain Name System (DNS) allows access to Internet hosts by name rather than IP address. Name resolution for local devices is performed by NetBIOS over IP. Windows maintains a list of local computer names. It is also possible to manually define names by placing entries in the Hosts file on the computer to

override other name resolution. If Windows cannot resolve a host name locally it assumes it is a remote host and makes a DNS request of the router. Residential routers typically do not actually implement a DNS resolver; rather it simply passes the request to the ISP's DNS nameserver.

When a PC connects to the LAN one of the pieces of information configured by DHCP is the DNS server address. When a PC needs to look up a host address it sends the request to the router. The router in turn figures out which DNS server to use. ISPs typically implement multiple DNS server for redundancy. If the primary DNS resolver goes down the router will attempt to use the secondary server.

Normally DNS is provided by your ISP. However, any DNS server can be used to translate URLs to IP addresses. If you chose not to use the DNS provided by your ISP you have two option use a public DNS server or run your own. There are a number public DNS servers of which Google is probably the most widely known. The other option is to run your own DNS resolver. I've used TreeWalk for many years but it appears the site no longer exists.

There is a downside of using DNS other than provided by your ISP. Many larger ISPs have special arrangements with Content Delivery Network (CDN) providers. The role of CDN is to improve streaming performance by locating caching media servers near the respective ISP. If you are not using DNS provided by your ISP may take a hit on multimedia performance since your DNS server is not privy to those special arrangements.

4.5 Firewall

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

4.5.1 Universal Plug and Play

UPNP is an outgrowth of PC plug and play experience. UPNP is designed to automatically configure local network devices and firewall rules. 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 discovery and when needed requests firewall/router configuration changes.

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

4.6 QoS

The router implements multiple QoS functions to make optimum use of limited WAN bandwidth. If packets arrive faster than they are able to be delivered QoS places high priority packets at the head of the list. It is important to keep in mind QoS does not improve capacity it simply determines winners and losers. In a bandwidth limited environment that can often improve the user experience but it does not magically create more capacity.

4.7 Syslog Event Logging

Router logs significant events and forwards them to Syslog server. This overcomes one of the main limitations of using a dedicated appliance for Internet sharing – limited data storage. Router emits Syslog data to the PC server. One of the services running on the server is Kiwi Syslog. Running a syslog server is convenient because it is able to aggregate logs from multiple devices – one stop shopping

Curiously I had to use Telnet to access the command line interface to set up Syslog, as there was no GUI for this feature. Syslog feature was not even mentioned in the user manual. If you are comfortable poking

around with the command line interface (CLI) it makes sense to Telnet into your router to see what surprises are available.

4.8 Management

Routers typically include a number of remote management features. They assist in troubleshooting but do impact security. Below are the most common management functions.

4.8.1 ICMP

Internet control management protocol (ICMP) is a suite of tools used to trouble network problems. For our purposes the most useful is Ping. Ping sends a small packet to the remote host and waits for a response. This is an easy way to verify remote host is up and running. It is a good idea to enable router to respond to ICMP. In addition may need to contact your ISP to have them enable ICMP within their network. Some ISPs disable support for ICMP making troubleshooting more difficult.

4.8.2 SNMP

Simple Network Management Protocol (SNMP) is a widely used management scheme for large networks. SNMP can be configured to provide read only access to configuration data or read/write enabling remote management. SNMP uses management information block (MIB) to interpret status and remotely manage a device. SNMP is not typically used on small networks. If SNMP is not being used disable the feature, or if device does not allow SNMP to be disabled, at least change the default read-only and read-write community strings. The community string acts as a password so device only responds to authorized queries. The default community strings are often public/private.

4.8.3 Broadband Forum TR-069

TR-069 CPE WAN Management Protocol is a Broadband Forum spec to facilitate ISP management of end user devices. If the router is supplied or configured by your ISP this feature is probably enabled and you will not be able to turn it off. If you are managing the router yourself turn off this feature unless you have shared access password with your ISP.

4.9 Internet Server Behind NAT

Running a public server behind NAT requires the router 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 de facto 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 supplied by the ISP, when in fact web server is on a private address hidden from the Internet.

> **Operational tip** - Most Residential NAT routers do not perform WAN Loopback. This prevents access to local public server by its URL or public IP address from within the LAN. Server must be accessed by its LAN machine name or LAN IP address. When a server is accessed by its public IP address within the LAN the router forwards the request to the Internet. It does not realize host is local. End result is 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.

4.9.1 Dynamic DNS

Remote hosts use DNS to map URL to server's IP address. DNS assumes server configuration is static and changes only rarely. 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 server to detect IP address change.

When that occurs Dynamic DNS service is notified of address change. This is not a perfect solution since there can be significant delay between address changes and when new address is available. However for casual residential users it works well enough.

4.9.2 Multiple Identical Servers

Most residential broadband ISPs allocate a single IP address per account. This causes problems running multiple servers of the same type. For example when running a web server, by default incoming requests are directed to port 80, making it impossible to run two web servers on a single IP address using the well-known port number. A workaround is to use a different port number for one of the web servers. If you are the only one accessing the server this is not a concern since you are aware of the non-standard port and can easily specify it in the browser.

http://mysite.com:8080

Where this becomes a problems is with a public server. In that case users have no way to know they need to use a nonstandard port to access the server. Many DynamicDNS services have provisions to redirect requests to the alternate port.

4.9.3 Active vs Passive FTP

The way File Transfer Protocol (FTP) allocates ports causes problems with NAT. To NAT an outbound FTP session appears to originate from the remote server, rather than internal on the LAN. As a result NAT prevents the transfer. Routers know about this behavior so use of default FTP ports is not a problem. It becomes an issue if you change FTP ports from default 20/21 to some other value.

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

4.9.4 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 server they are free to attack other machines on the LAN. We use a hosting service to minimize security risk rather than run a public server locally.

4.10 Bonding vs Load balancing

If a single Internet connection is not adequate one option is obtain addition connections and use bonding or a load balancing router. As with all engineering decisions there are tradeoffs.

4.10.1 Bonding

Bonding combines multiple ISP connections into a single pipe with the effective speed of the sum of each pipe and a single IP address. Bonding requires the cooperation of the ISP. While the effective speed is doubled (assuming two equal speed links) it does not have much effect on latency since data is split between each connection

4.10.2 Load Balancing

Load balancing is performed by a router with multiple WAN connections. As each outbound LAN request hits the router it picks the least used connection. From the Internet perspective each connection has its own IP address so it simply looks like two independent links. The advantage of load balancing is it does not require the ISP to do anything. Even though each individual session is limited to the speed of whichever link it is assigned traffic is spread evenly over all links so effective Internet speed is increased.

4.11 Measuring Internet Speed

In a SOHO network LAN performance is rarely a speed determinate. Speed is typically limited by first-mile WAN connection. It can be a challenge teasing out various components of end-to-end performance to

see if ISP link is working as advertised. The first step is to determine the bit rate being delivered by the ISP. In the case of ADSL this is a matter of looking at modem status and determining download and upload bit rate.

IP transmission splits data into 1500 byte chunks called packets (1-byte = 8-bits). Some of the 1500 bytes are used for network control so are not available for user data. TCP/IP uses 40 of the 1500 bytes for control. NOTE: this analysis assumes use of maximum size packets. Since overhead is fixed using smaller packet size incurs a higher percentage overhead. With 40-bytes reserved for control out of every 1500-bytes sent only 1460 are available for data. This represents 2.6% overhead.

Some ISPs, typically phone companies, use an additional protocol called Peer to Peer Protocol over Ethernet (PPPoE) to transport DSL data. This is an adaptation of PPP used by dialup ISPs. Telco's like PPPoE because it facilitates support of third party ISPs as mandated by FCC. PPPoE appends 8-bytes to each packet increasing overhead to 48-bytes reducing payload to 1452. Where PPPoE is used overhead is increased to 3.2%.

Most DSL ISPs use IP over Asynchronous Transfer Mode (ATM) (AAL5). ATM was designed for low latency voice telephony. When used for data it adds significant overhead. ATM transports data in 53-byte Cells of which only 48 are data the other 5 used for ATM control. Each 1500-byte packet is split into multiple ATM cells. A 1500-byte packet requires 32 cells (32 x 48 = 1,536 bytes). The extra 36=bytes are padded, further reducing ATM efficiency. 32 ATM cells require modem transmit 1,696 bytes of which only 1452 carry payload. Where ATM/PPPoE is used overhead is increased to 14.4%.

TCP/IP overhead 2.6% efficiency 97.4%
TCP/IP/PPPoE overhead 3.2% efficiency 96.8%
TCP/IP/PPPoE over ATM overhead 14.4%, efficiency 85.6%

As an example our old FairPoint 3000/768 ADSL service had a sync rate of 3360/864, 3360 kbps toward customer, 864 kbps toward Internet. FairPoint uses PPPoE and ATM yielding an overhead of 14.4%. Best-case transfer rate is 85.6% of sync rate, resulting in 2,876 kbps down 740 kbps up.

FirstLight DSL does not use PPPoE saving that overhead. Because speed is not capped like FairPoint sync speed varies a little. Current sync speed is about 7 Mbps down and 1 Mbps up yielding best case transfer of 6.19Mbps down and .884Mbps up.

File transfer speed reported by Broadband Reports or Speedtest.net is shown below.

NOTE: This is best-case speed based on packet overhead only. Errors, transmission delays, etc. will reduce speed from this value. The higher the speed the more impact even modest impairments have on throughput.

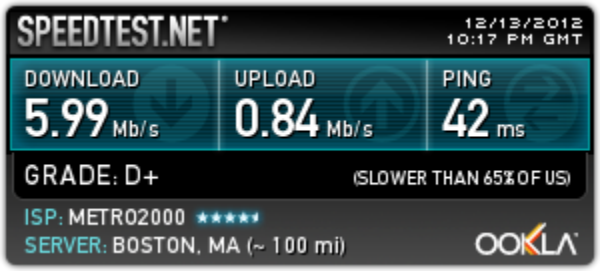


Figure 5 DSL Speed Test Results

5 Wi-Fi Access Point – Networking Without Wires

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. Wi-Fi radios operate in the unlicensed Industrial Scientific Medical (ISM) band. Wi-Fi popularity has a down side. As more devices attempt to use the limited frequency allocation interference problems increase. Government regulators are addressing interference by designating more bandwidth for unlicensed use. Standards bodies are working to facilitate graceful coexistence between various devices.

IEEE 802.11 radios operate in two modes ad hoc peer-to-peer and infrastructure. Infrastructure mode requires one or more Access Points to bridge wireless network to wired network. Depending on size and type of building construction a site may require multiple Access Points. Ah-hoc mode allows two or more Wi-Fi devices to communicate directly without needing an Access Point. Most Wi-Fi communication makes use of Access Points.

Many residential routers include a Wi-Fi Access Point. Ours does not and even if it did the location of the router is not ideal for Wi-Fi use. We use a standalone Netgear WN802Tv2 Access Point. It is an 802.11n 2.4 GHz Access Point connected to a port on the Ethernet switch. This was an upgrade we made several years ago and coverage throughout the house is much better.

5.1 Wi-Fi Overview

The success of various IEEE 802.11 wireless standards has encouraged many vendors to enter the market. The Wi-Fi Alliance works to insure interoperability between different vendors and promote use of Wireless LANs. The result is that wireless IEEE 802.11 networks are often referred to as Wi-Fi.

5.2 WLAN Speed

As is the case with Ethernet IEEE 802.11 Wireless Local Area Network (WLAN) performance has dramatically improved over the years.

- 2 Mbps 2.4 GHz 802.11 (1997)
- 54 Mbps 5GHz 802.11a (1999)
- 11 Mbps 2.4 GHz 802.11b (1999)
- 54 Mbps 2.4 GHz 802.11g (2003)
- 150 Mbps 2.4/5 GHz 802.11n (2009)
- 500 Mbps 5 GHz 802.11ac (2013)
- 7000 Mbps 60GHz 801.11ad (2012) (very short range)

Due to the way over-the-air transmission operates real world transfer speed is limited to less than half the raw transmission speed and often significantly lower. However advances in wireless technology make it the network technology of choice in many instances.

5.3 Security and Authentication

Wireless LANs are inherently less secure then wired. An intruder does not require a physical connection, but can eavesdrop some distance away. The original 802.11 designers were aware of this 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 useless. As an interim measure the Wi-Fi alliance developed WPA that could be retrofit to existing hardware. IEEE developed a comprehensive security standard Wi-Fi Protected Access 2 (WPA2). WPA2 using AES-CCMP is the preferred privacy implementation. Only use WPA or WPA2-TKIP if equipment does not support WPA2 AES-CCMP. WEP should never be used.

In a commercial setting WPA2 if often used with RADIUS to uniquely identify each user. That is typically not an option for home users. A simpler method uses a preshared key (PSK). With PSK the Access Point and each client have a secret password installed for mutual authentication.

There are many key generation utilities available to simplify creating long security keys. Wireless keys need to be significantly stronger than a typical end user password. An attacker is able to capture wireless traffic at their leisure and then use dictionary attack or brute force methods to discover the key. This is very different than trying to login to your account online since in most implementations lockout the account after a few invalid attempts.

To improve security do not used the default network name (SSID), create your own. This prevents an attacker from quickly running through a list of previously cracked passwords/SSID combinations.

5.4 Wi-Fi Protected Setup (WPS)

WPS was designed to make it easier for home users to configure multiple Wi-Fi devices using a preshared key. Creating a long key and configuring Wi-Fi parameters can be a daunting task for the typical user. Unfortunately, as was the case with WEP, security flaws have been discovered in WPS implementation. The Wi-Fi alliance has tightened testing of WPS but to be on the safe side it is best to disable this feature and manually configure devices.

5.5 Interference

Wi-Fi radios operate in unlicensed bands so interference can be a problem, especially in congested urban areas. The radios must be certified as compliant with the specification but users do not need an FCC license to operate the equipment. Interference is the result of other Wi-Fi radios, non-Wi-Fi radios operating in the same band such as Bluetooth or wireless phones and unintentional radiators such as microwave ovens. Wi-Fi operates in three bands 2.4GHz and 5GHz are the most common and the new 801.11ac operates in the 60 GHz band for extremely high speed but short range communication. The 2.4GHz band is by far the most popular but it is also the most crowded. While there are many 2.4 GHz channels defined Wi-Fi uses a much wider channel there are only three non-overlapping channels. In general when operating in the 2.4 GHz band it is best to use channels 1, 6, or 11 for optimum performance.

Wi-Fi 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. That knowledge is used to set operating channel and transmit power to minimize 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.

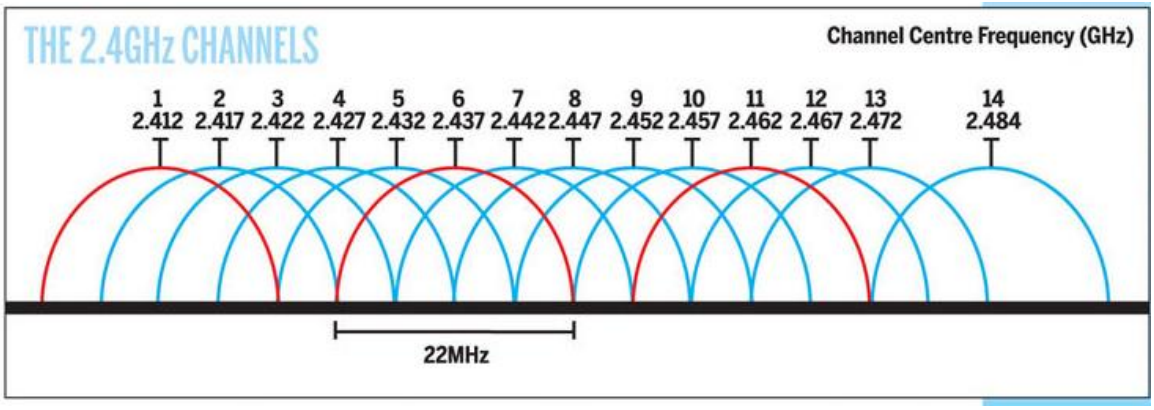


Figure 6 2.4GHz Wi-Fi Channels

6 Ethernet Switch – Ethernet Conquers All

If you want to connect more than one computer to the Internet you need a Local Area Network (LAN). LANs are useful for much more than just sharing your Internet access. Having a LAN allows computers to access shared resources such as a printer and files. Local resources are still available even if you lose Internet access. Wi-Fi and Unshielded Twisted Pair (UTP) Ethernet technology is ubiquitous and dominates the SOHO market.

Creating a LAN can be as simple as enabling Wi-Fi on your router or as complex as installing hundreds of feet of Ethernet cable and dozens of jacks. Our LAN consists of an Access Point located on the second floor and 24 Ethernet jacks sprinkled throughout the house and office. The DSL router and Ethernet switch connect to an Ethernet patch panel located in the basement near my office.

Residential routers include at least one Ethernet port. Some incorporate a built in Ethernet switch to provide multiple ports. The router provided by our ISP is a single port router. This is not an issue for us as we need a large number of Ethernet ports so we use a 16-port Gig Ethernet switch.

> **Performance tip** – Using a single wide switch is advantageous from a performance standpoint rather than cascading multiple switches. While cascaded switches are transparent doing so limits speed between switches to that of the intervening link. In a wide switch traffic between ports travels over the much faster internal switch fabric.

6.1 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. Due to their tremendous performance advantage switches have entirely replaced hubs.

The carrier sense multiple access – collision avoidance (CSMA/CA) scheme originally used by Ethernet places a limit on the number of wire segments and how many hubs can be used within a single collision domain. Each device listens for the bus to be idle before it begins to transmit. It is possible multiple devices will transmit at the same time, causing a collision. When that occurs data is corrupted. Transmission is halted and each device waits a random amount of time before attempting to transmit again. Original Ethernet was half duplex, only one device on the network is able to talk at a time, all others are listening.

Ethernet switches operate very differently. 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. This dramatically increases network performance. A 100 Mbps hub shares 100 Mbps among all devices. With a switch traffic flows between port pairs. A non-blocking 16-port 100 Mbps Ethernet switch has a maximum throughput of 1600 Mbps. This assumes connections are evenly used among the 16 ports each one operating at 100 Mbps. Port A is able to talk to port D at the same time Port F is talking to Port B and so forth. Switches enable full duplex communication, computers are able to transmit and receive at the same time. Switches offer a tremendous performance advantage compared to hubs. In a home network switches represent a less dramatic improvement if almost all traffic is to and from the Internet. In that case the Internet connection, normally much slower than the LAN, determines speed. However if there are local resources such as files and printers on the LAN the Ethernet switching advantage come into play even on small home networks.

When a switch does not know which port to use it floods the incoming frame to all ports, much like a hub. When the device responds the switch learns MAC address associated with the port. Once it knows which MAC addresses are associated with each port it only needs to forward frames to that port. The switch also floods all ports with broadcast frames. Switches are transparent to Ethernet traffic, replacing a hub with a switch is simply a matter of swapping out the device.

Gig Ethernet interfaces are at price parity with Fast Ethernet. New gear delivers Gig as a baseline. Gig Ethernet is an interesting inflection point. Historically computer performance was limited by network

speed. 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 limited to 300-400 Mbps due to disk speed, O/S overhead, and PCI throughput. Bottleneck is no longer communication but has shifted to computing elements.

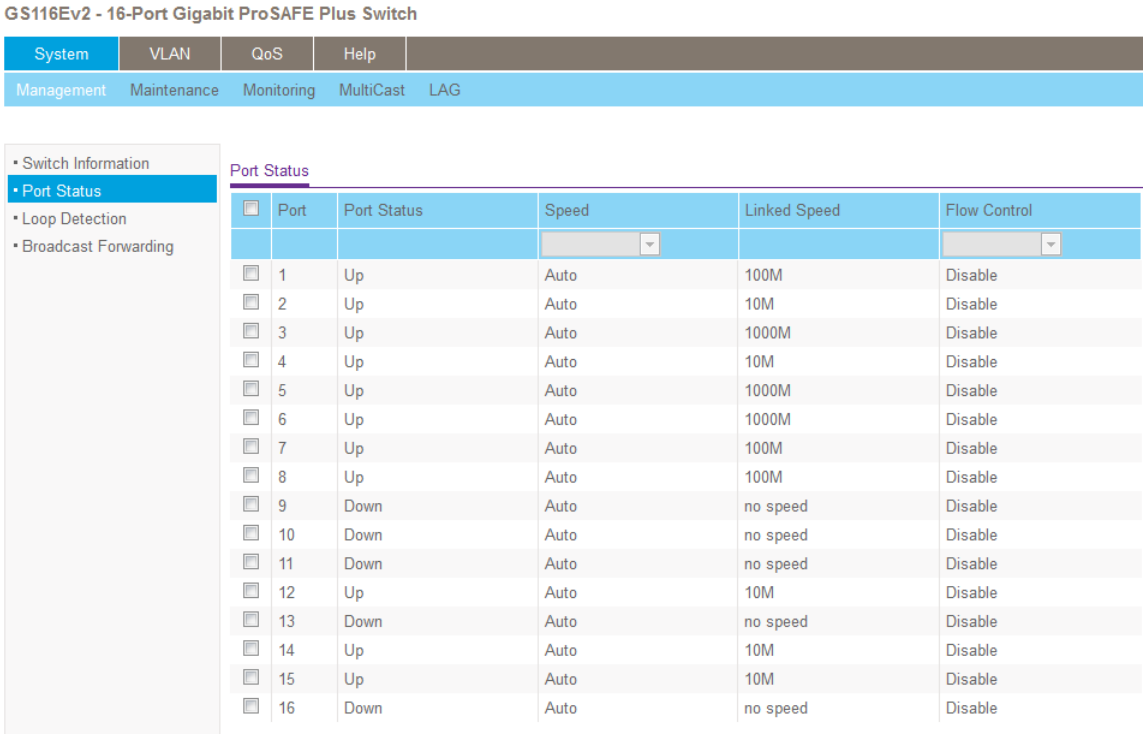
6.2 Managed vs Unmanaged Switches

Ethernet switches come in managed and unmanaged flavors. Managed devices allow the administrator complete control of various parameters, define VLANs and observe traffic etc. An unmanaged switch has no user interface and is simply plugged into the network. Managed switches are overkill in a typical SOHO network. Unmanaged devices are considerably less expensive and operate at lower power reducing energy cost.

Our switch is an interesting hybrid between managed and unmanaged. We use a Netgear ProSafe Plus 16-port Gig switch. It is like an unmanaged switch in that you just connect it to your LAN and it works. The Web Interface allows you to do many of the features of a managed switch while still being priced near that of an unmanaged dumb switch and important for our situation it is the same size. This was critical as I have very limited space to locate the switch.

The features that are of particular value to me are: Port Status, Port Statistics, Mirroring and Cable tester. The switch supports other useful features such as VLANs and QoS that we are currently not using.

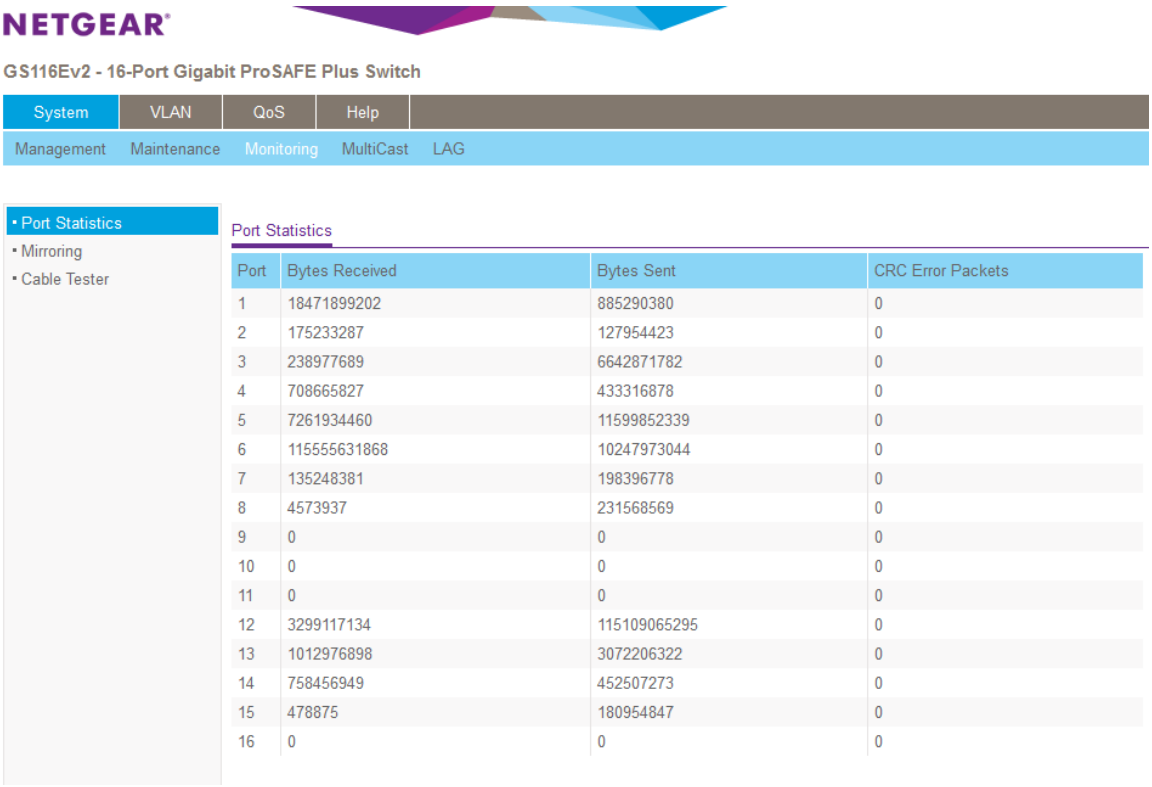
Mirroring is handy for troubleshooting as it copies traffic to another port. This allows that port to be used as a monitor to analyze traffic. There is also a built in cable tester, it is supposed to be able to detect bad cables and estimate distance to the fault. So far I have not had any bad connections to try it on.



Port	Port Status	Speed	Linked Speed	Flow Control
1	Up	Auto	100M	Disable
2	Up	Auto	10M	Disable
3	Up	Auto	1000M	Disable
4	Up	Auto	10M	Disable
5	Up	Auto	1000M	Disable
6	Up	Auto	1000M	Disable
7	Up	Auto	100M	Disable
8	Up	Auto	100M	Disable
9	Down	Auto	no speed	Disable
10	Down	Auto	no speed	Disable
11	Down	Auto	no speed	Disable
12	Up	Auto	10M	Disable
13	Down	Auto	no speed	Disable
14	Up	Auto	10M	Disable
15	Up	Auto	10M	Disable
16	Down	Auto	no speed	Disable

Figure 7 Ethernet Switch Port Status

This page shows the connect speed of each device. As you can see we have a mix of speeds. Most of the 10 Mbps devices are the home automation controllers; however some are hosts that drop down to 10 Mbps when idle to conserve power.



Port	Bytes Received	Bytes Sent	CRC Error Packets
1	18471899202	885290380	0
2	175233287	127954423	0
3	238977689	6642871782	0
4	708665827	433316878	0
5	7261934460	11599852339	0
6	115555631868	10247973044	0
7	135248381	198396778	0
8	4573937	231568569	0
9	0	0	0
10	0	0	0
11	0	0	0
12	3299117134	115109065295	0
13	1012976898	3072206322	0
14	758456949	452507273	0
15	478875	180954847	0
16	0	0	0

Figure 8 Ethernet Switch Port Statistics

We have a mix of Cat 5 and Cat5e cabling. The runs are all fairly short but I wanted to make sure the links are working without errors. Much to my relief the switch is reporting zero errors over long period of time.

6.3 Automatic Link Configuration

To make Ethernet easier to use higher speeds are backward compatible. Transceivers Auto negotiate link characteristics to determine speed and whether connection is half or full duplex. Hubs are limited to half duplex as only one device is able to transmit at a time. Switches are full duplex capable of transmitting and receiving at the same time.

NIC (computer interface) is configured as uplink port (MDI), Hub or switch as MDI-X. Default configuration assumes MDI port is connected to MDI-X port. Under normal circumstances devices connect using a 1:1 cable. A mismatch occurs when like devices are connected, say PC to PC or switch to switch. To make this easier hubs/switches have historically had an uplink switch or dedicated uplink 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. Crossover cable swaps TX and RX pair at one connector. Recently vendors have adopted Auto-MDI-X to automatically determining remote port type and configure ports automatically eliminating the need for crossover cables, and uplink ports/switch on Ethernet switches.

With Auto negotiation (Speed/duplex) and Auto-MDI-X (gender) Ethernet has become much more user friendly. All a user needs to do is connect the cable, everything else is automatic.

6.4 Power over Ethernet (PoE)

Until recently 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 an issue. However as more and more low power appliances such as Wi-Fi Access Points and Voice over IP (VoIP) telephones are deployed the benefit of delivering both data and power over Ethernet cabling became obvious.

IEEE took on the challenge and in 2003 released PoE specification. PoE provides 13 watts of power per device. For 10 and 100 Mbps Ethernet PoE uses the two unused pair. Gig and higher speed uses all four pair so power has to be injected into the active pairs. Second generation PoE, called PoE plus, increased maximum device power to 25 watts

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

6.5 Topology

UTP is a point to point technology. Cable runs from an outlet located near the device to a port on the Ethernet switch. For maximum performance a single wide Ethernet switch should be used to serve the entire LAN rather than cascading switches. Cascading is transparent to traffic but limits inter switch speed to that of the link connecting the switches. With a single wide switch intra-LAN throughput is dictated by the much higher performance of the internal switch backbone.

6.6 Unshielded Twisted Pair

Ethernet IEEE 802.3 using unshielded twisted pair (UTP) copper cable is by far the most common networking technology in use today. UTP consisting of 8 conductors organized as 4 twisted pairs terminated with 8 conductor modular (8P8C) jacks similar to those used for telephone wiring. The jack is commonly, but incorrectly, referred as an RJ-45 jack. As speed has increased the cable specifications have become more stringent. EIA/TIA 568-C structured wiring speciation applies to commercial locations and EIA/TIA 570-C is the variant for residential.

Ethernet also supports various flavors of optical fiber but due to higher cost fiber is more appropriate where the strengths of fiber can be used to an advantage: extremely small size, incredible speed and being non-metallic fiber is immune to lightning.

6.6.1 UTP Speed

Since its inception UTP speed has increased dramatically. Category 8 UTP cable is being specified for use with 40G Ethernet and IEEE is working on 2.5 and 5G Ethernet versions that will operate over existing Cat5e and 6 cabling.

- 10 Mbp/s Cat 3 10 Base-T (1990)
- 100 Mbp/s Cat 5 100 Base-TX (1995)
- 1,000 Mbp/s Cat 5e 1000 Base-T (1999)
- 2,500 Mbp/s Cat 5e 2500 Base-T (P802.3bz 2017 estimate)
- 5,000 Mbp/s Cat 5e 5GBase-T (P802.3bz 2017 estimate)
- 10,000 Mbp/s Cat 6A 10GBase-T (2006) (Cat 6 up to 55 meters)
- 40,000 Mbp/s Cat 8 40Gbase-T (P802.3bq early 2016 estimate)

In general Ethernet UTP cable distance is limited to 100 meters (328 feet). Range extenders can be used for longer distance. Cable distance is typically not a concern for residential users.

As speed and distance increases fiber becomes attractive compared to copper cable. The difficulty with fiber is not so much the cost of fiber itself but termination and the cost of opto-electrical converters needed to connect NICs to fiber. That being said fiber is an ideal way to link buildings as it is immune to lightning and able to transport high speed data much further than copper.

6.7 Virtual LAN (VLAN)

Virtual LANs allow a single physical LAN to interconnect multiple computers while isolating one group from another. Typical use is to create VLAN based on community of interest for example payroll,

marketing and engineering. A router is used to interconnect separate groups providing a great deal of control over how data flows across VLAN boundaries.

VLANs are not common for home LANs but may become more 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).

6.8 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 the problem of multiple paths in complex networks. The protocol detects duplicate paths and turns off redundant ports. 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.

7 Alternative LAN Technologies

Ethernet and Wi-Fi are the dominant LAN technologies. The cost of installing network wiring is modest if done when structure is being built. The situation is more difficult for existing structures. 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 equipment.

7.1 Personal Area Network (PAN)

Bluetooth is optimized for low power short range peripheral connection such as wireless headsets. Since Bluetooth operates in the crowded 2.4GHz band care needs to be taken so Bluetooth and Wi-Fi do not degrade one another.

7.2 Phone Line Networking

Home Phoneline Network (HomePNA) uses telephone 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. Like DSL HomePNA take advantage of unused capacity of copper wire to create a network.

PNA uses a slightly modified Ethernet packet. 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.

HomePNA never really took off so finding gear can be difficult. There are numerous Ethernet extenders that are able to use existing voice grade telephone twisted pair. Many of these use off the shelf VDSL chipsets allowing point to point Ethernet connections several thousand feet apart.

7.3 Power line Networking

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

7.4 Ethernet over TV Coax

Multimedia over Coax Alliance (MoCA) is popularizing an interesting technology that utilizes TV coax wiring to deliver Ethernet at up to 800 Mbps. A competing ITU-T standard G.hn is getting international traction also hits the 800 Mbps range.

Many homes built in the last few decades have RG6 coaxial cable feeding multiple TV outlets but are not equipped with Category rated UTP cable suitable for conventional Ethernet. Verizon is using the technology extensively to eliminate need to run both coax and UTP Ethernet to set top boxes when installing FIOS.

8 Local Server – Just Like the Big Kids

There are many advantages of running your own server. Having an always on computer on your LAN makes it easy to back up PCs and provide a number of other network services.

We use a server for the following:

1) Stable Windows Master Browser (peer to peer files sharing)
2) File sharing
3) Automatic online PC backup
4) USB printer sharing
5) NTP clock synchronization
6) Private web server
7) Syslog server
8) Personal weather station

Current server is a recycled HP/Compaq DC7600 tower upgraded to Win 7 and a 2TB HDD. Using an old PC as a poor man's server is a great way to extend the life of outdated PC hardware as running a server on a small network is not very demanding. I was debating between purchasing a 2 and 3TB drive. Older PCs are limited to 2TB HDD. Could have partitioned the drive but as a 2TB HDD was more than enough capacity decided to go with that size drive.

8.1 KVM Switch

Figure 9 KVM

I did not want to add another set of user I/O when we setup the server. The solution was to use a KVM (keyboard, video, and mouse) switch. KVM's have been used in server farms for years to allow single point of control for multiple computers. KVMs are pretty brute force doing hardware switching of peripherals so it don't interact or care about the O/S. I purchased a 4-port Belkin Omni View SE KVM. Port 1 is the main workstation, port 2 the server, port 3 is a WinXP/Ubuntu computer and port 4 is used for temporary connection to PCs I'm working on. I wired up a set of I/O, network, and power cables to make it easy to temporally connect another PC for test or configuration. That has turned out to be a very handy benefit of using the KVM.

Switching between computers is done via a button on the KVM or a keyboard hot-key sequence. When switching computers the KVM reconnects keyboard, mouse and monitor to the active computer and reconfigures the keyboard and mouse to match their condition prior to being switched away from that computer.

> ***System Boot*** – The KVM does not emulate the attached device. It simply passes any commands to the devices and remembers recent commands so the device can be reconfigured when switching computers. This causes problems at boot time if the KVM is not switched to that computer. Video defaults to low resolution VGA and the mouse to basic PS/2 mouse. Normally this only occurs after a power failure when PCs are powered up and the KVM set to a different computer.
>
> ***Video Performance Tip*** -- Workstations use higher resolution than servers resulting in very high video data rate. This is typically not a problem for KVM itself but requires high quality video cable when used with analog monitor interface. Coax preserves high frequency and minimizes crosstalk between the red, green, blue video signals.
>
> ***Mouse Compatibility Tip*** -- Each computer thinks it is directly connected to a keyboard, mouse and monitor. The KVM memorizes commands sent to each device and restores device configuration when user selects a different computer. PS/2 Mice cause problems because there are so many proprietary enhancements. PS/2 mice power up in compatibility mode in order to support

basic mouse functionally, even if proprietary mouse driver is not installed. At O/S boot time mouse driver performs a "knock" sequence to determine if a known mouse is attached. If mouse answers correctly driver switches on enhanced mode. This causes problems for KVMs. Unless the KVM has a-priori knowledge of a specific mouse it does not know which commands it needs to store to configure the mouse correctly. This may result in either loss of mouse control or mouse reverting to default mode. This is only a problem when switching between machines. The KVM transparently passes commands from active machine to mouse so in that case the mouse is always be correctly configured.

This problem only affects PS/2 style mice since they do not support hot plug. A USB enabled KVM resets mouse whenever a different computer is selected. The downside if USB enabled KVMs is that it often takes a long time to reconfigure a USB device.

PS/2 Mice – PCs have supported USB mice and keyboards for years. Our KVM only supports PS/2 devices. It is becoming increasingly difficult finding PS/2 compatible mice so I keep a spare on hand just in case.

Monitor Plug and Play – modern CRT and LCD monitors communicate with PC using VESA Display Data Channel (DDC). This allows PC to read monitor characteristics and automatically configure video subsystem. My KVM passes DDC commands but does not emulate the monitor itself. If a PC powers up on an inactive KVM port it thinks it is connected to a non-Plug and Play monitor reverting to low resolution low refresh mode. 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.

8.2 Remote Server Management

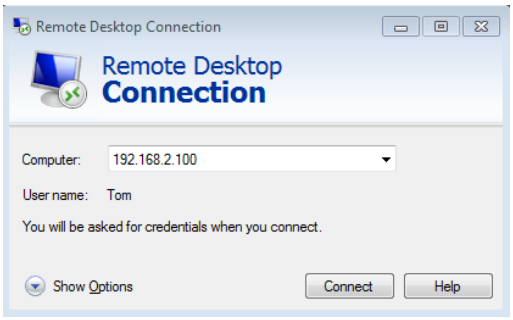


Figure 10 RDP

KVM is a brute force method of server management by simply switching physical I/O devices. Its advantage is it provides access even before O/S is in control. A more elegant method is remote desktop protocol (RDP). Depending on your flavor of Windows this management tool may be built in. If not there are numerous third-party applications such as Teamviewer.

To use RDP, once server is up and running, open the Windows Remote Desktop Connection feature on the client. Enter the IP address and user name to log in, a later screen will ask for the password. Windows will complain about the lack of the security certificate. Check the box to whitelist the server. Once connected you have access to the remote desktop services based on the permission of your account. To terminate the session click the X in the upper right hand corner.

Figure 11 Remote Desktop to Tribble Server

8.3 NetBIOS Master Browser

In a SOHO peer to peer network, i/e. not part of the Windows Domain, computers need a way to advertise and collect information about each other. That is the job of the master browser. The difficulty is deciding which PC should assume that role. When a Windows PC detects there is not a Master Browser on the LAN it initiates an ad hoc election process. The result is that any PC may win the election. If that PC is then turned off other PCs will not be able to locate local resources until the completion of another master browser election which can take several minutes. In a home network having an always on server means the server will always become the master browser eliminating the confusing situation of being unable to see other PCs on the LAN.

TechNet Browser election FAQ

8.4 File Sharing

One of the advantages of having a LAN is to facilitate file sharing. Files can be shared directly between PCs or by using a dedicated file server. Access is organized by workgroup. In a small LAN all machines typically belong to a single workgroup, such as HomeLAN. Once properly configured users are able to browse network shares, as easily as if they were physically at the local machine.

We mainly use server shares for automated backup. Software running on the workstation periodically backs up files to the server. That way if one of the workstations fail or become infected the system can be rebuilt with minimal loss of data.

Windows 7 has a feature called Homegroup that is supposed to make sharing easier and more secure because it requires a password. I was never able to get it working reliable so reverted to traditional sharing methods. The security feature is nice but if any of the PCs granted access becomes compromised the shares are vulnerable.

8.5 System Backup

Client PCs are automatically backed up to the server using Acronis True Image Home. Backup is set on a weekly schedule so at worst a week's worth of work is lost. This has come in handy when we had a disk crash. Backup is covered in more detail later.

8.6 Printer Sharing

Our HP inkjet printer has a built in print server and is directly connected to the LAN. A Brother P-touch label printer is connected via USB. Windows has built in support for printer sharing allowing a USB enabled printer to be accessed from any device on the LAN. This has the downside of requiring the PC to be turned on but is a nice feature if the printer does not have network support.

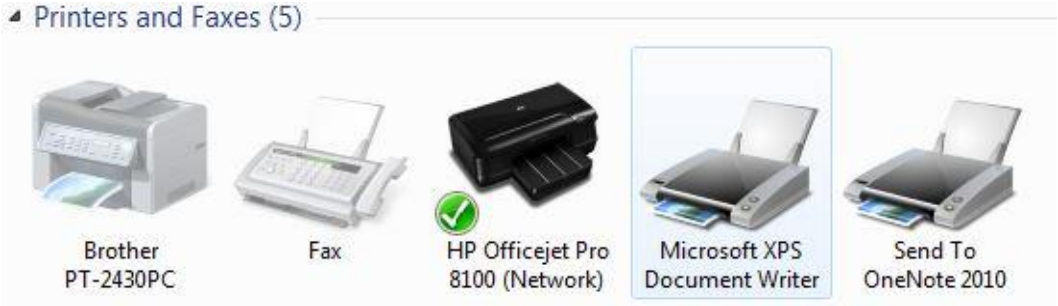


Figure 12 Printers

8.7 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.

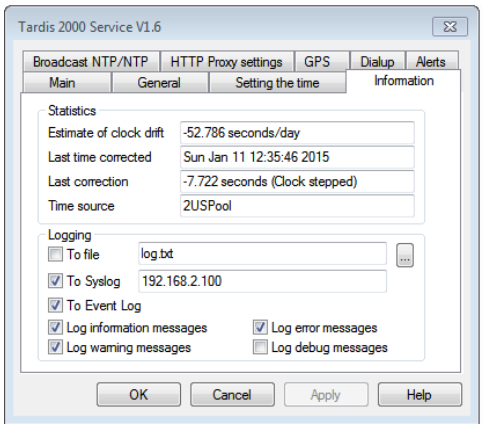


Figure 13 TARDIS Status Page

Current generation of Windows PCs have a built in NTP client that is used by default to synchronize the real time clock. This means each PC independently accesses a NTP server somewhere out in the cloud. A more elegant method is to use a time server, running on the local server, and have it in turn synchronize the LAN PCs. We use Tardis 2000 running on the server and point each LAN PC to it. This way we are only making a single access of the NTP Internet pool and even if we lose Internet connectivity devices remain synchronized to one another, with more drift due to the server RTC. This is most important for the home automation PLCs as they do not have a built in battery backed RTC. If power is restored they default to junk date/time. From a privacy perspective another benefit of running your own NTP server it that only one access is being made to NTP time severs as opposed to individual accesses from each device.

Previously I had been using the lightweight K9 service to listen for NTP broadcasts. Currently dispensed with that and simply point each PC to the server running Tardis time service.

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

8.8 Private Web Server

The browser home page of each desktop PC points to a personal web server running on the server. This allows relevant information be posted. Server main page consist of links to internal devices such as the home automation servers, weather station and network devices as well as useful external links. I chose Abyss as it is free for personal use.

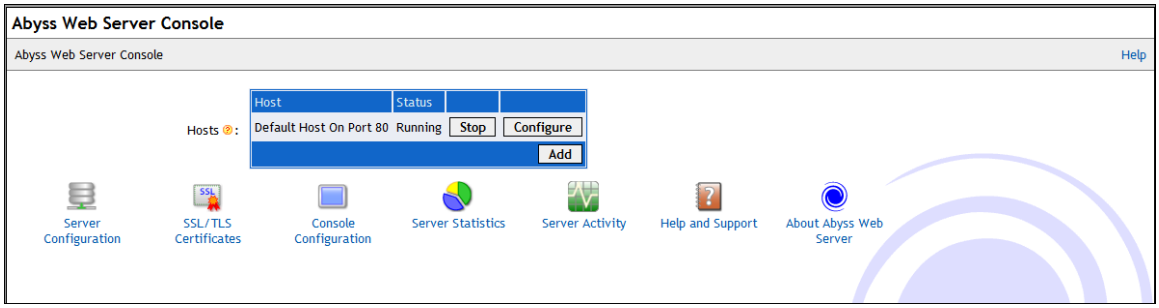


Figure 14 Abyss Server Console

8.9 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. We use Kiwi free shareware program for both Syslog server and Log file viewer. The Syslog server runs as a service on the server and the data is accessible from any device on the LAN.

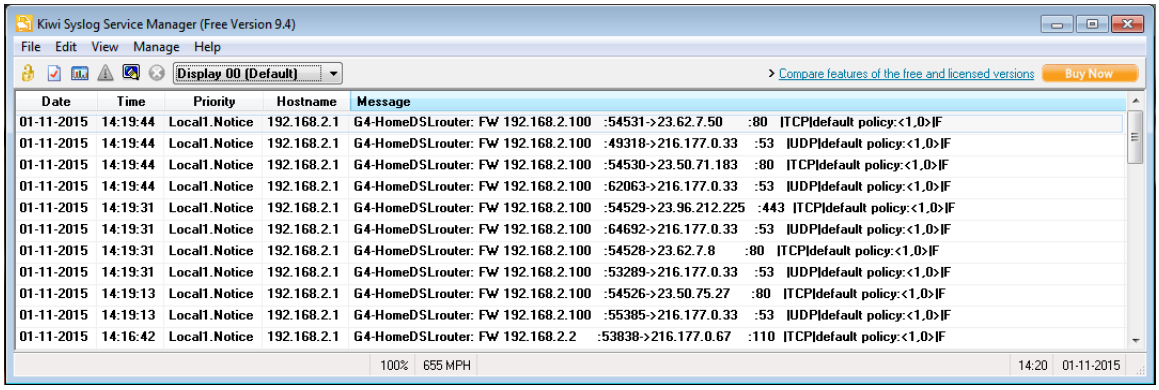


Figure 15 Syslog Server Viewer

8.10 Weather Station

A Davis Instruments Monitor II weather station data is posted on the internal web server. Weather station data is downloaded over a RS232 serial port to the server. Ambient virtual weather station software running on the server processes the data and displays it as a web page.

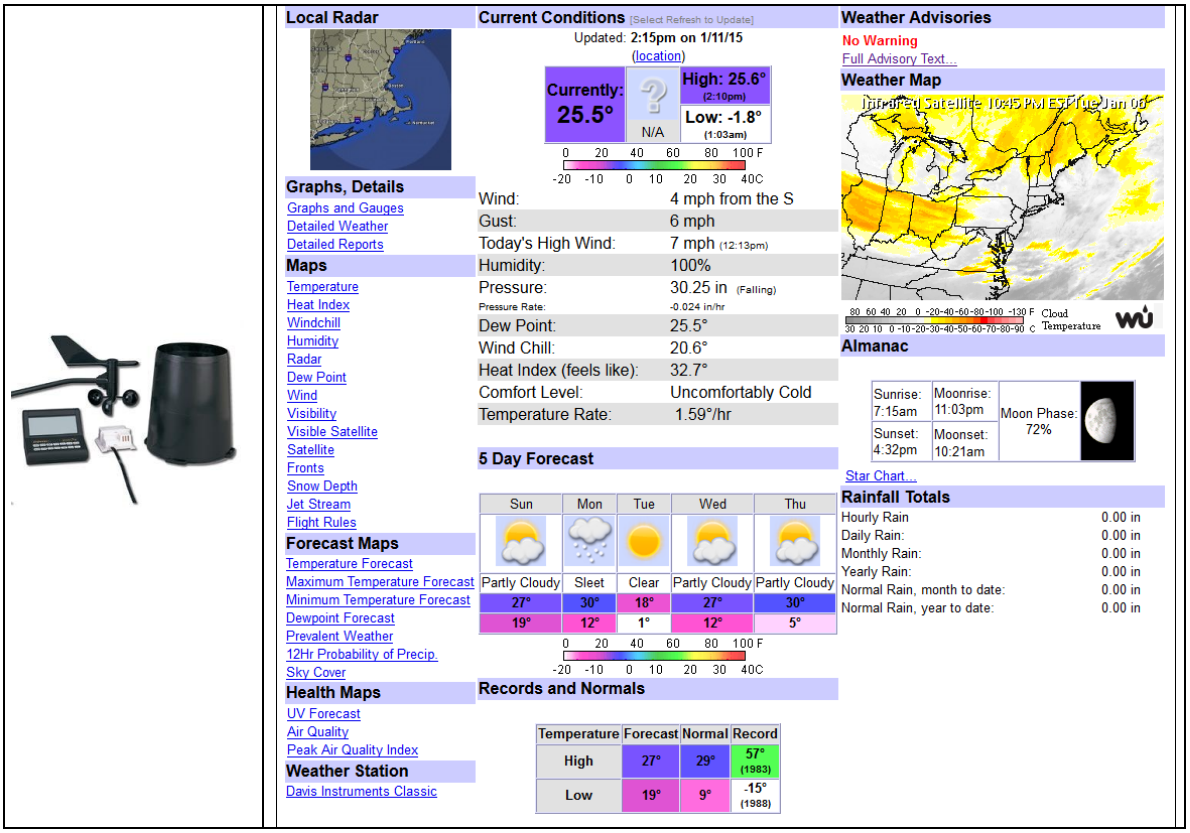


Figure 16 Home Weather Station

9 Widgets & Services – Making Life Worth Living

This section describes the various programs we use to access Internet services.

9.1 Computers

We have a collection of Win 7 desktop PCs. These are off-lease PCs purchased on eBay. If you do not need the latest and greatest hardware acquiring an off-lease few year old commercial PC delivers a lot of bang for the buck. Each time I upgrade my workstation I repurpose the old one as a poor-man's server. I've also setup a SFF HP/Compaq DC7600 with XP and Ubuntu. It provides a platform for compatibility testing, nice having more than one computer and/or browser for testing.

My laptop is a Lenovo T61 ThinkPad running Win7 that was also acquired off lease from an eBay vender.

9.2 World Wide Web

Having multiple browsers is a useful troubleshooting tool. Microsoft Win7 PCs automatically get the latest and greatest version of Internet Explorer, at time of this writing it is version 11. I use Firefox as my main desktop browser and just to keep life interesting run Chrome on my laptop. The dual boot PC runs a down rev version of IE on XP and Firefox on Ubuntu.

It is interesting having my own web site to see the ebb and flow of browser popularity. Below is a recent report of browser preferences at my site.

Browsers (Top 10) - Full list/Versions - Unknown

Browsers	Grabber	Pages	Percent	Hits	Percent
MS Internet Explorer	No	570	27 %	3,539	15.8 %
Google Chrome	No	500	23.6 %	9,697	43.5 %
Firefox	No	476	22.5 %	3,764	16.8 %
Unknown	?	162	7.6 %	286	1.2 %
Opera	No	131	6.2 %	543	2.4 %
Safari	No	128	6 %	2,659	11.9 %
Mozilla	No	103	4.8 %	1,234	5.5 %
Android browser (PDA/Phone browser)	No	20	0.9 %	408	1.8 %
Netscape	No	9	0.4 %	11	0 %
Lynx	No	4	0.1 %	4	0 %
Others		8	0.3 %	143	0.6 %

Figure 17 Web Site Browser Preference

9.2.1 Search Engine

Key to effective use of the Internet is being able to find what one is looking for. Our preferred search engine is Google.

9.3 Secure Remote Access - IPSEC and SSL/TLS

VPNs provide secure access to web sites and extend the corporate network to telecommuters and business partners. There are two approaches to providing secure 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. ESP encrypts data to prevent eavesdropping. Authentication is performed using Internet Key Exchange (IKE).

NAT is very hostile to VPN security because it modifies packet address and checksum. Because NAT is so ubiquitous VPN software has implemented workarounds that are compatible with NAT.

Tunnel mode forces all client traffic through 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 is split-tunnel. In split-tunnel mode tunnel only carries traffic destined for corporate network. Other traffic flows normally as if tunnel did not exist.

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. All browsers support SSL as a way to securely log into web sites. While SSL is not as powerful or secure as IPsec it eliminates the need for special client software. This is especially convenient for employees that need to connect to corporate network from multiple computers.

9.4 E-Mail

E-mail accounts fall into three broad categories: ISP, free third party and corporate. ISPs typically provide an email account as part of the package. This is convenient but ties your e-mail address to your current ISP. Change ISP or if the ISP gets bought out and changes their name your e-mail address changes. Free email services like Google Gmail have become extremely popular. Corporate email accounts, tied to the company domain are the third type of email.

For business purposes or to insure long lasting email identity nothing beats registering your own domain. Once registered e-mail is addressed to you@yourdomain.TLD. Even if you change hosting services you simply transfer the domain to the new provider, e-mail address is unaffected.

Even though I have an Internet domain and ISP email accounts I use my Gmail account as an alternative account. To eliminate the need to log into Gmail I have incoming Gmail forwarded to my domain account. My cell phone is Android based and Google wants to tie everything to your Gmail account.

Having multiple email accounts is a useful troubleshooting tool. If one does not work, try the other and then try to determine the difference between the one that works and the one that does not.

The greenhouse controller sends out a morning and evening status email, documenting the previous 12 hours. It logs into the ISP SMTP server to send email to my domain email address. The recurring nature of these emails is a great troubleshooting tool. Missing a report becomes the trigger to investigate root cause. It has flagged several problems over the years with my ISP email system and with the DSL router refusing to forward DNS requests. All in all a handy side effect of these periodic emails.

9.4.1 Email Access

Traditionally email uses an email client, such as Microsoft Outlook or Windows Live Mail. Most free mail services use a browser interface eliminating need for a dedicated email client. Web mail is convenient because email is accessible from any browser equipped PC. I find the web based email user interface is somewhat clunky but adequate for casual use.

Except for web-based mail, e-mail has a sending component, SMTP, and a receiving mailbox, POP. To send mail the client connects to a Simple Mail Transport Protocol (SMTP) mail gateway. 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. SMTP server delivers mail to the appropriate Post Office Protocol (POP) server. It works much as a physical post office mailbox. POP server stores mail temporally. When the e-mail client connects to the POP server it downloads mail and typically removes it from the server. A more sophisticated alternative to SMTP/POP email is Internet Message Access Protocol (IMAP).

For cell phone access to my domain based email I played around with the Android email client vs using browser based access. Unless I missed the setting you cannot set up Android to only log into an email account manually on demand. It can only be set up to constantly poll the server or be disabled. Given this limitation I opted to access my domain email using the Android browser rather than the email client.

9.4.2 Email Implementation

I use Windows Live to replaced Outlook Express I had been using on the Win XP boxes. I did not want to lose years of archived email so faced the daunting task of exporting old Outlook mail and importing it into

Windows Live. After much trial and tribulation I was able to do it but it was not a pleasant experience. Personally I find the Live Mail user experience less satisfying than the old Outlook but mail is mail.

I configured the email client to use SSL/TLS to access SMTP/POP servers. This has the advantage of providing end to end privacy between the email client and mail server. Without using SSL email credentials are sent in the clear making them vulnerable.

> ***Mail Configuration Tip*** -- Accessing 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.
>
> ***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*** – Be aware of Phishing attacks. Sender fakes an email and asks you to log in to update or correct your account. Luckily most attacks are worded so poorly as to make them obvious but hover over the link before clicking and see if it is pointing to the real web site. If in doubt close the email and log into to the site normally rather than use the email link.
>
> ***Security Tip*** -- What is not 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.
>
> ***Privacy Warning*** – An obnoxious privacy intrusion is the insertion a one-pixel image in HTML mail. When message is read browser has to go to the referenced URL to retrieve it. This allows the sender to monitor when and if mail is read.

9.4.3 Email Privacy on the Road

When logging into traditional SMTP/POP servers unless they are set up for SSL the user's credentials are sent in the clear. With a wired connection this is not a huge security issue but it is when using popular Wi-Fi hotspots because traffic is not encrypted so anyone nearby is able to eavesdrop on your email credentials. Because of this and other security considerations most email accounts now require the use SSL to encrypt the session protecting it from eavesdropping. If this is an option be sure to take advantage of it, especially on mobile devices.

9.4.4 SPAM Mitigation

Unwanted email (SPAM) is a tremendous problem. Something like 70% of all email messages are SPAM. ISPs and third parties have been waging an antispam battle of years. ISPs have adopted a number of strategies to minimize the problem.

9.4.4.1 Messaging Malware Mobile Anti-abuse Working Group (M^3AAWG)

M3AAWG is an industry group promulgating best-practices to reduce spam. Historically SMTP servers accepted anonymous email creating a haven for spammers. ISPs have developed a number of proprietary workarounds over the years to limit spam. Recommendation is to use SSL/TLS to securely access SMTP and POP mail server. Where SSL is not feasible use Port 587 to send email instead of Port 25. Port 587 requires authentication therefor ISPs will not block the port allowing off network access.

9.4.4.2 Blacklist

Many mail services subscribe Blacklist services such as Spamhaus. Blacklists are databases of Spammers and IP address blocks of residential ISPs. If mail arrives from a blacklisted address it is rejected. MXtoolbox has a handy tool to check if the IP address of your mail server has been blacklisted. It also checks MX records to verify domain DNS records are configured correctly.

9.4.4.3 Sender Policy Framework

Sender Policy Framework (SPF) creates a mechanism to validate email return address is not forged. SPF adds DNS records indicating which servers are authorized to send email from a specific domain. Before email is accepted email server verifies it originated from an authorized server.

9.4.4.4 Email Client Filter

For SPAM that makes it all the way through to email client one can set rules for handling incoming mail by the email client. This can drastically reduce the number of unwanted messages in your in box.

9.5 Wired and Cellular Telephony

Since the invention of the telephone, over a hundred years ago, the public switched telephone network (PSTN) has used the same switching method to connect caller to called party. When a call is initiated a temporary path through the network is established for the duration of call. When the call is terminated the connection is torn down and network components released for use by other customers. The path is in place for the duration of the call regardless of whether or not either party is talking.

The Internet is causing tremendous change in all aspects of our lives not the least of which is plain old telephone service (POTS). Voice over IP (VoIP) uses the packet network to transport phone calls reducing cost and increasing functionality. Packet based networks were not designed for real time communication so making telephony work has been a challenge. As first-mile speed increases VoIP becomes more practical. The payoff is convergence – integration of all forms of communication over a single unified transport network.

9.5.1 POTS

We use ADSL for Internet access and a wired POTS line is part of the package. While POTS is ancient technology it is incredibly reliable here in snowy NH. We have lost power multiple times over the years, sometimes for days at a stretch, but we have never lost telephone service. When we switched to a CLEC for DSL got several advanced calling features and unmetered US and Canadian calling as part of the package, all for less than we were paying previously. Even though they were free there were two advanced features I had the CLEC turn off, voice mail and call waiting. We have our own answering machine; it is easier pressing a button on the machine to retrieve messages than dialing into the CLEC VM system. I also had them turn off Call Waiting; if the phone is busy the person can call back later rather than interrupt an ongoing conservation.

9.5.2 Cell Phone

Our cell phone provider Republic Wireless has an interesting wrinkle on mobile telephony. They are a mobile virtual network operator (MVNO). Whenever the phone is connected to Wi-Fi all traffic: voice, text and Internet are transported over Wi-Fi eliminating cellular network usage charges. When not connected to Wi-Fi the phone uses the Sprint 3G/4G-LTE network and roams to Verizon if out of range. Voice and text is unlimited regardless of how the phone connects. Any unused cellular data results in a credit on the next month's bill. The Wi-Fi first feature requires custom Android firmware so phone selection is limited to a few Motorola Android phones customized by Republic but so far the service has worked out well for us. Since most of the places we frequent have Wi-Fi our cellular data usage is very low resulting in very modest monthly cost.

Battery life of these spiffy smart phones is significantly shorter than flip phones. In the office I keep a USB cable plugged into the server at my desk. This is convenient and eliminates the need to keep the USB AC charger plugged in. I keep the charger in my laptop bag for travel. In the car we use a couple of car adapters to keep the phone charged while driving. A down side of using the car charger is the cigarette lighter (accessory) socket is turned off when the car is not running. When camping this can be a problem as the phones need to be charged every day unless they are put into airplane mode. I wired up a cigarette lighter socket to a couple of large alligator clips and a fuse. The adapter can be clipped directly to the car battery

to recharge the phones. We also have a rechargeable USB battery pack that provides several days of power to keep the phones charged.

9.6 FTP

File Transfer Protocol (FTP) is an effective way to transfer large files over the Internet. FTP predates HTTP so has kind of lost favor but is still very much alive. My main use of FTP is to make changes to my site. This paper will be uploaded to my web server using FTP.

9.7 Telnet, SSH, and Terminal Emulation

While GUIs are all the rage there is a lot to be said for command line interfaces (CLI) and heaven forbid I still need to occasionally work on RS232 gear and need a terminal emulator. PuTTY is my preferred application. Being able to Telnet into the ZyXEL router came in handy as that was the only way I could find to set the Syslog log server feature.

9.8 USENET

Usenet Newsgroups can be 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. Many groups have an online FAQ that describes what the group is about to limit off topic posts.

Most ISPs used to include USENET access as part of the service. Due to declining interest in Usenet and legal attacks related to pornography many ISPs are taking easy way out and eliminating or scaling back support of Usenet. If your ISP does not provide Usenet access there are a number of 3rd party services.

Our ISP dropped Usenet years ago, I thought about signing up with a third party provider but no longer use it enough to justify the cost.

9.9 Multimedia

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

Internet multimedia was hampered by low dialup speed. Broadband eases this chokepoint opening the door to Internet delivery of telephone, radio, TV and movies. 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.

Internet delivery is bringing dramatic change to long-standing business models. Prior to the Internet media distribution was an expensive proposition that had been mastered by only a few companies. The Internet undermines traditional business model by reducing distribution cost nearly to zero. Legacy media players have had a difficult time adapting to change wrought by technology and have been primarily focused on crippling digital delivery. Over time both artists and patrons will learn how to utilize this new distribution model.

9.9.1 Digital Rights Management

Audio and video content owners fear lossless digital duplication of copyrighted works will undermine their business rather than open up new distribution models. Digital Rights Management (DRM) has been controversial for both philosophical and technical reasons. What is the proper balance between rights of copyright holders and patrons desire for unfettered access? Technically DRM implementations have been a disaster. DRM is easily circumvented, caused ill will on the part of consumers, broken backward compatibility, rendered investment in content library worthless and been a PR nightmare due to DRM implementation run amuck.

9.9.2 CD/DVD/Blu-ray evolution

Back in the early '90s digital versions of audio CDs were heralded as a tremendous new storage medium. A CD holds about 700 Mbytes of data, compared to only 1.5 Mbytes for a 3.5" floppy. At the time that seemed like an almost infinite amount of space.

Time marches on. DVDs were developed to allow digital movies be distributed in similar format as audio CDs ultimately displacing VHS videotape. DVDs store 4.7 Gbytes (single layer) of data. This is more than enough to store an entire SDTV (standard definition) movie with room for extra features.

With increased popularity of high definition Television HDTV a media format with more capacity was needed. Blu-Ray 25 GB (single layer) won the battle. HDTV dramatically improves image quality compared to NTSC standard definition TV. That being said standard definition DVDs using component video or HDMI interconnect looks pretty good on HDTV TVs and computer monitors.

Video data is encoded and compressed using MPEG compression. Image is compressed (spatially) and between frames (temporally). Audio is also compressed. Without compression files would be uneconomically large.

An annoying aspect of commercial video content is region coding. Typical DVD player will refuse to play the media unless the region code of the player and DVD agree.

9.9.3 Netflix

Netflix pioneered snail mail DVD rental. They are moving away from physical media by expanding online library. Netflix customers can use their PC to access a growing library of on-line titles or use Roku player to watch streaming media on their TV. Image quality is automatically adjusted based of broadband speed. We opted for a WD TV live hub to stream Netflix to our TV. It provides access to other streaming services and is a media server to boot. Files uploaded to the server can be watched on an ordinary TV.

9.9.4 ITunes

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

MPEG MP3 compression provides near CD-quality audio at 128 kbps, about a tenth the uncompressed data rate. MP3 has become a popular digital music format. We converted all CDs and some records (LP and 78 rpm) to MP3 and store music on file server. This enables any computer on the LAN equipped with an MP3 player to access 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.

9.9.5 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.

9.9.6 QuickTime

Apple QuickTime is a popular movie-encoding format.

9.9.7 VLC Media Player

The Video LAN media player is a popular free multimedia player.

9.10 Fax

The Pro version of Windows 7 includes a fax capability. Being able to send and receive fax is becoming less and less important but it is nice to have the ability to send the occasional fax. This requires having a dialup modem connected to a phone line. I purchased a USB V.92/Fax modem just in case I ever need dialup/fax. I've installed the modem and tested it but so far have not had the need to actually send a fax.

If faxing is important may want to check out eFax rather than purchasing a fax machine or one of an all-in-one printer/scanner/fax machines.

9.11 Radio/TV

There are many ways to distribute Radio and Television programs. Internet over the top (OTT) delivery opens up fascinating opportunities for new sources not constrained by distance or even a local presence.

9.11.1 RF Radio/TV

I use a Hauppauge TV/FM card is installed in the main workstation. It supports NTSC analog and ATSC digital TV and analog FM. I find the card very useful. ATSC standard definition TV looks surprising good on a computer screen, not as good as HD but much better than analog NTSC. NTSC resolution is about 720x480 pixels with less color depth than typical computer display. HDTV resolution is 1366x768 and 1910x1080. The card has a freeze feature to capture still images.

Titan TV is a popular on line TV program guide.

It is also possible to implement a TV server and then distribute programs over your LAN. The Silicon Dust HDHomeRun is probably the most well-known system. So far we have not opted to go that route.

9.11.2 Internet Radio/TV

Historically radio and TV programs were broadcast to many people simultaneously. This was due to technical constraints of the medium. Internet, unlike broadcast, 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 immature. Multicasting allows a single media stream be delivered to multiple subscribers. Multicast reduces server and bandwidth cost.

We are a Netflix subscriber and use a WD TV live Hub to watch TV. Besides Netflix it allows TV to access other Internet based content and an internal hard drives acts as a media server.

9.12 Printing

Computers were once billed as the paperless office. This has not happened. On the other hand 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 needed.

9.12.1 Document Printing

Our printer is an HP Officejet Pro 8100. The 8100 includes a built in print server allowing it to be directly connected to the network. Being a higher end inkjet printer the print heads and ink are separate and it has separate ink cartridges for each color. This dramatically reduces the cost per page.

Printing documents on different printers can be a challenge since margins and fonts differ. The Adobe PDF format has become the de facto industry standard for print document formatting.

9.12.2 Photo Printing

We had a HP inkjet photo printer for a while but never used it much so when it died did not bother to replace it. To print photos we use the Shutterfly service, much easier to use then messing around with the printer. The only down side is the lengthy upload time due to limited DSL upload speed.

9.12.3 Label Printing

A Brother P-touch PT-2430PC USB printer is used to print various labels.

9.13 Document Scanning

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

I prefer using a separate scanner rather than an all in one printer/fax/scanner because the printer is behind my desk and the flatbed scanner is conveniently located on my desk. The upgrade to Win7 relegated my old HP Scanjet 5400C flatbed scanner to the scrap heap. Replaced it with a LED based Epson V550 Photo scanner. It also functions as a poor man's copying machine allowing scanned images to be directly printed.

9.14 Digital Photography

Digital cameras are fantastic to quickly capture images and incorporate them into documents or a web page. Cameras typically use some form of 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. Cameras typically support USB file access eliminating the need to pop out the memory card to access pictures.

Being lazy, now that I have a smart phone noticed I rarely use my digital camera. The Phone USB charging cable does double duty allowing easy access to pictures and even the occasional screen shot for troubleshooting. I typically transfer pictures to internal server for safe long term storage and editing shortly after then are taken.

9.15 Office Suite

I work from home so have used one flavor or another of Microsoft Office for years, currently using Office 2010 for documenting editing, spreadsheet, and PowerPoint presentations. I've played around with Open Office a little and find it is OK for casual use but it has a number of compatibility issues with MS Office.

9.16 Home Automation

Most of the recent changes to our network have been adding Ethernet drops to support home automation projects. Over the last several years I've designed a: greenhouse controller, wood heat controller, window ventilation controller and most recently an aquarium controller. They are all built around a CAI networks WebControl web based programmable logic controller (PLC).

The interested reader is referred to the Writings page for more information about these projects.

9.17 Bookkeeping and Taxes

Computers are great 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.

For annual income tax preparation we use Tax Act software.

10 Backup – Oops Protection

Having an always-on server makes it possible to use automatic backup. On line backup is convenient insuring backup actually happens. 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. Even with off line backup if all copies are in the same location they may be destroyed in case of fire or flood. Optimum backup strategy consists of on line and off line backup with off line data stored at a different location. It all depends on how valuable is the data and what is the impact of its loss.

10.1 On Line Backup

One of the benefits of having a server is to provide automatic backup. We use Acronis True Image backup utility. It has the capability to backup only user data or create a complete disk image that can be used to do a system restore the system if the HDD crashes.

Backups are scheduled automatically insuring data is safely duplicated. Use of incremental backup saves only data that has changed since the last backup reducing amount of disk space needed. Even so with modern huge drives the amount of data being backed up can be significant. The main reason to upgrade to a Gig Ethernet switch was to speed up backups.

10.2 Off Line Backup

Figure 18 External USB Drive

External USB hard drives are an ideal way of providing off line backup. They can be disconnected when not in use protecting them from lightning strikes and hardware failures.

Our current off line backup is a WD My Book 4TB USB drive. This is twice the capacity of the server drive so should be good for several years. I set up the drive to back up the server an also each desktop. This necessitates physically connecting the drive to each system's USB port. I try to be religious doing this to minimize risk of data loss in the event of a hardware failure. The server has a complete system image of each desktop allowing a crashed system to be recovered. When the drive is connected to individual computers it only backs up user data not the entire drive. User data backup provides a more convenient way to access specific files then the incremental disk image.

In an ideal word off line file backups are stored in a separate location in case the building is destroyed. So far I have not gone to that extreme.

10.3 As Purchased System Image

One of the things I try to do is create an as-purchased image backup of each computer. This makes it easy to restore the computer to as purchased condition in case of problems or when repurposing the machine, say from a workstation to server or if I need to give the PC away and want to make sure it does not contain any personal data. The Maxtor One Touch USB 500 GB we had been using for several years reached capacity. I repurposed that drive to store the initial disk image of each PC as they were placed them into service. Previously I had stored the initial system backup image as part of other back up data. But on more than one occasion I inadvertently deleted the initial image because I forgot what it was. Keeping the initial image on a separate USB drive dedicated to that purpose prevents this Murphy from occurring and allows each system to be brought back to pristine condition.

10.4 CD/DVD/Blu-ray

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 should not to cause problems as off line backup medium.

10.5 USB Flash Drive

Figure 19 USB Flash Drive

Multi Gigabyte USB Flash Drives have become extremely popular over the last few years. They offer the advantage of large, low cost rewriteable removable storage. Removing the drives makes it immune to lightning and power lines surges. I like the Cruzer Flash drives because they have a retractable USB plug rather than an end cap.

I've been in this game for a long time and the idea of a 32GB Flash drive or 32GB micro SD card (for our cell phones) for under $10US just blows me away.

11 Security -- Keeping Bad Guys Out

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

11.1 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.

11.2 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 a 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. They check file signatures and monitor downloads. Microsoft Security Essentials is a no cost way to add anti-virus protection to Windows PCs. 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.

11.3 Phishing

Phishing email looks like it originated from a legitimate company. The email typically states recipient needs to "log in" to secure web site and review and update account information. The site looks real but is actually controlled by the attacker. Goal of 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. I hate to admit it but I fell for a Paypal Phishing attack years ago. Hurried up and went back to the real site and changed account credentials. Hover over the link in the email to see the URL, if I doubt ignore the email and log into your account directly.

11.4 Zombies

One of the most insidious forms 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 even aware PC is compromised. Often the first hint of a problem is a nasty email/letter from their ISP.

11.5 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 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.

11.6 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.

11.7 DNS Cache Poisoning

Internet was designed to be robust in the face of equipment and communication failures. Unfortunately it was not designed to withstand deliberate willful attack. Domain Name System (DNS) is the vehicle used to convert user-friendly names to computer friendly IP addresses. 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 cached information. Once cache is corrupted computers accessing that DNS server are directed to incorrect site controlled by the attacker. A high priority initiative is to implement Domain Name System Security Extensions (DNSSEC) to counteract this sort of attack and increase level of confidence in DNS.

11.8 Eavesdropping

Radio communication is easy to eavesdrop. An attacker can locate a distance away without having to compromise physical site 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. During development of IEEE 802.11 Wireless Local Area Network (WLAN) this threat was recognized and provisions made for authentication and encryption called Wireless Equivalent Privacy (WEP). Unfortunately security researchers quickly discovered serious shortcomings in WEP. Weakness managing encryption key makes it relatively easy to determine the key thus breaking encryption. Current state of the art for Wi-Fi security is Wi-Fi Protected Access (WPA2) using AES encryption. There are options optimized for home networks using a preshared key and for large organization using RADIUS authentication.

> **Security Tip** –POP/SMTP email send user credential in the clear. This is not a huge concern on wired or security protected Wi-Fi networks. It is a serious when using public hotspots as over the air is sent in the clear allowing anyone with a sniffer to grab your email passwords. If at all possible use SSL/TLS to log into email to protect username and password.

Powerline, Phoneline and Coax networks leak data beyond the confines of the network. An attacker can connect to phone, power or Cable 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 wiring and LAN wiring does not typically exit the building.

11.9 Man in the Middle Attack

Man in the middle is a 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 because attacker needed to intercept traffic by being located within ISP or Internet backbone. With widespread use of public Wi-Fi hot spots and even recently Cell sites this type of attack is becoming more common. Some ruse is used to cause user to connect to attacker's site. Site is often an exact replica of a real site. Once user has been fooled into connecting to bogus site attacker is free to spoof site information and capture user's authentication credentials.

11.10 Passphrase storage

For a computer to recognize authorized user it needs a method to establish entered credentials are valid. This means computer must store the passphrase, or more correctly a hash of the passphrase. As long as

computer remains under control of authorized user everything works fine. However if machine is stolen or lost an attacker is able to retrieve hard disk contents and run dictionary attack at his leisure. Security researchers have even found it is possible to obtain valid data from dynamic memory even after it has been powered down for a relatively long period of time. Fogo the convenience of having your computer remember passwords and enter then each time you need to log in.

11.11 Data Leaks

Computers work by receiving information, creating copies – either temporary or permanent, modifying the information as needed to accomplish desired task, make more copies of 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 and transmit. Once captured this treasure trove of information often escapes control of those who have created it winding up in unsavory hands.

11.12 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 those 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.

The biggest problem with cookies it when sites use then to correlate user activity across multiple web locations.

11.13 Social Media Sites

The explosion of social media creates another avenue where personal information can be unwittingly released into the wild or harvested for nefarious purposes. Members offer unwittingly post sensitive personal information that winds up being widely distributed.

11.14 Add Blockers

A less obvious vector for malware is web page ad insertion. Many web sites depend on advertising revenue to survive. Add insertion is contracted out to a third-party resulting in not only the annoyance of inane ads but also the possibility of advertising malware. To deal with this we recently started running Adblock Plus.

11.15 Countermeasures

There is no such thing as perfect security. One must take a cold hard look at how computers are used, how valuable is the information, how attractive a target and ramification of a breach. Security engineering is very different than other forms of engineering. In a typical engineering problem a solution is developed and proper operation verified. Various failure modes are analyzed but there is no need to consider deliberate attack designed to pervert operation.

11.15.1 Security Patches

For machines running Windows the 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. Many software applications also offer automatic monitoring of new releases and prompt the user to upgrade. However I've have noticed a trend to incessant updates and there is always the risk an update will break backward compatibility.

IMHO Microsoft violated that trust by using the Windows Update feature to install Windows 10 upgrade nagware and download, but not install, Win 10 itself even if the user did not specifically request the upgrade. If they want to promote the benefits of their latest and greatest O/S all well and good but don't make it a critical automatic update. There are several ways to remove this nagware both manually and automatically. I went the manual route but then it came back. Recently I ran GWX Control Panel to remove the Win10 nag ware and remove the Gigabytes of downloaded upgrade software.

11.15.2 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.

- UPNP allows PC based application 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. Unless 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.
- Wi-Fi predefined password management for home systems can be a challenge. Wi-Fi Protected Setup (WPS) was intended to simplify this process. However as with WEP it has been shown to have serious security vulnerability and should be disabled.
- Change the default Wi-Fi SSID. This makes it harder for an attacker to crack the security. With the default SSID an attacker is able to precompute SSID/Password combinations.

11.15.3 Passphrase Management

No reputable entity will 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. On line passwords are reasonable secure because most accounts will be locked out if more than a few incorrect passphrases are entered. The more significant risks are encrypted transmission and devices that can be attacked offline. In that case attacker is able to perform dictionary attack running through millions of possible passphrase until they find the right one.

- Change passwords, do not use defaults.
- Do not use a single favorite password on multiple sites. Since Internet access often use you email address for the username if you use the same password at multiple sites and it is compromised the other accounts are at risk.
- Use long passphrases of both letters and numbers and if possible punctuation characters.
- The most common passphrases have numbers at the beginning or end. To make dictionary attack harder use passphrases with number within the password rather than at the beginning or end.
- Be wary 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.
- On your Wi-Fi network changes default SSID. Using the default SSID allows the attacker to precrack possible passwords. Using a unique SSID at least forces the attacker to run through the list again.
- In general periodic password changes are a waste of time and tend to result in selection of trivial passwords that user is able to remember. Wherever possible forgo mandatory password change interval but pick a robust password and one that is unique for that account.

11.15.4 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. Companies want to harvest your information to sell you stuff. It is surprising, and scary, how much information can be gathered about someone by simply following them to different sites.

11.15.5 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.

Windows make it easier to limit unauthorized software installation by providing a pop up dialog box asking to approve installation. Much Windows software is digitally signed verifying it came from the vender it claims to come from. Note: signing says nothing about quality of the software just verifies who released it.

11.15.6 NAT

A security side effect NAT is by default it drops incoming connection requests. If a remote host attempts to connect to public IP address NAT ignores request because it doesn't know which computer on LAN to forward it to. Only if explicit port forwarding rules are created will NAT know how to handle request. This is what gives NAT its firewall like characteristics for inbound connections.

11.15.7 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 firewall running on workstation, such as Windows built in firewall is able to control access based on individual application. Many low cost Broadband routers include some form or firewall.

In some respects firewall security is 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. In that case the firewall is no longer part of the security scheme since it must allow data to pass. The server 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.

11.15.8 Data Backup

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

11.16 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.

12 Troubleshooting -- 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 product vendor, able to help resolve end user issues. My favorite is DSL Reports.

Windows includes a number of command line utilities to help debug network issues. To run the desired utility press the Windows key and the R key simultaneously. Type "cmd," press OK. This opens the command prompt, also called the DOS box.

There are lots of ways to troubleshoot problems. The most comprehensive is to start at the bottom and work your way up.

1. Does device think it is connected to a wired or wireless network?
2. Does the PC have the appropriate IP address for the specific network?
3. Can you access the router's web GUI or Ping it?
4. Is Router able to establish an ISP link?
5. Are you able to Ping the remote host by IP address?
6. Are you able to Ping the remote host by URL?

12.1 Documentation

Even with a small home network documentation is important and will save time later. No matter how obvious something seems now a couple of years down the road it can be a head scratcher. I created an Excel spreadsheet listing: device description, purchase date, MAC address and IP address if set statically. Used MS Word to document patch panel and switch connections. Did the same for 66-blocks used for telephone wiring.

The trick is to be disciplined enough to keep documentation up to date. It is interesting going back through early revisions to see how things have evolved over time.

12.2 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 Link indicator is off link is inactive. This is most likely a cable fault or Ethernet hardware failure.

Ethernet cards automatically select optimum speed. For 100 and 1,000 Mbps operation both sides must be capable of the same speed and wiring meet Cat5e or Cat 6 requirements. 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 network utilization increases. Occasional collisions are nothing to worry about. Hubs have been obsolete for years so rarely seen on a residential network.

In Windows go to the Network Connections page and click on the interface you are using. Either use the GUI or type NCPA.CPL. If the word Status is not in bold the PC does not think that interface is connected

to a network. If you prefer command line troubleshooting type the command: GETMAC –v. It will display each interface and whether or not Windows thinks it has an active connection.

If the desired device does not show up at all that means Windows does not think it exists. Sometimes an interface may lock up. Unplug the PC from power; do not just turn it off. This makes sure power is removed from everything except the RTC. Leave it off for a few seconds and try to reboot.

One of the advantages of using the ProSAFE Plus switch is I'm able to log into the switch and see the status of each port.

> ***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 PC-to-PC or Switch-to-Switch a crossover cable or uplink port is required. Newer devices implement Auto-MDIX eliminating the need for crossover cables. If ports are mismatched the link will not work.

12.3 Modem Statistics

The modem connects to the ISP network: ADSL, Cable, satellite, or if you are very unlucky dialup. Modem stats provide a powerful diagnostic aid since reports condition of the physical interface rather than end-to-end performance.

The Status page of our ADSL2 router shows DSL link speed and IP settings. There is a diagnostic submenu to display low level ATM and ADSL stats. If you can get to the modem the good news is at least your LAN is working correctly even if you cannot access the Internet.

12.4 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 hosts respond to Ping some administrators disable it. It is a good ideal prior to troubleshooting to have a host in mind. I like using DSL Reports because I use the site a lot and it responds to Ping.

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 Pinging by name first step is to translate host name to IP address. If you are able to Ping an Internet host by IP address but not by URP there is a problem with DNS resolver. Try configuring one of the PCs with public DNS resolver. I use Google's 8.8.8.8 just because it is easy to remember. This quickly determines if DNS is working correctly. The third example shows a typical report when the host ignores ping requests.

> **Tip** – Ping is extremely useful but not all routers and hosts respond. If a device does not respond need to determine if that is because of a problem or it is configured to ignore Ping.

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 DSLreports.com [64.91.255.98] with 32 bytes of data:
Reply from 64.91.255.98: bytes=32 time=63ms TTL=47

Reply from 64.91.255.98: bytes=32 time=62ms TTL=47
Reply from 64.91.255.98: bytes=32 time=62ms TTL=47
Reply from 64.91.255.98: bytes=32 time=62ms TTL=47

Ping statistics for 64.91.255.98:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 62ms, Maximum = 63ms, Average = 62ms

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.

12.5 Trace Route

Trace route (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. Trace route uses Time to Live (TTL) parameter to control at which hop the packet expires. When a router receives a packet with an expired TTL it discards the packet and informs sender TTL expired. Trace route 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 unexplained increase typically means that hop or previous one is congested. PING is given a low priority so it is not uncommon for a router or server to ignore it. In that case Trace route responds with an "*" indicating nothing was returned.

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

Typical TRACERT report:
Tracing route to DSLreports.com [64.91.255.98] over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.2.1
2	29 ms	28 ms	28 ms	xx.milford1-1.nh.g4.net [66.211.144.97]
3	29 ms	29 ms	29 ms	gi-3-1.nashua1-1.nh.G4.net [216.177.5.178]
4	59 ms	62 ms	66 ms	ge-24-v108.merrimack3-1.nh.G4.net [216.177.5.150]
5	105 ms	115 ms	117 ms	gi-21-v358.manchester3-1.nh.G4.net [216.177.30.153]
6	176 ms	180 ms	192 ms	ge-0-0-3.manchester1-9.nh.G4.net [216.177.5.45]
7	255 ms	267 ms	275 ms	s5-0-24-0.cr01.4-2.mnchnhcohba.seg.NET [216.107.229.209]
8	345 ms	362 ms	377 ms	66-109-52-73.tvc-ip.com [66.109.52.73]
9	454 ms	493 ms	429 ms	66-109-52-21.tvc-ip.com [66.109.52.21]
10	35 ms	34 ms	35 ms	66-109-52-86.tvc-ip.com [66.109.52.86]
11	39 ms	38 ms	48 ms	v204.core1.ymq1.he.net [209.51.163.105]
12	46 ms	45 ms	45 ms	10ge2-3.core2.tor1.he.net [184.105.222.93]
13	56 ms	67 ms	56 ms	10ge15-1.core1.chi1.he.net [184.105.213.150]
14	56 ms	56 ms	56 ms	equinix-chi.liquidweb.com [206.223.119.138]
15	62 ms	62 ms	62 ms	lw-dc3-core2-vlan66.rtr.liquidweb.com [209.59.157.226]
16	81 ms	63 ms	63 ms	69.167.128.122
17	63 ms	62 ms	63 ms	lw-dc3-dist15-po5.rtr.liquidweb.com [69.167.128.201]
18	63 ms	63 ms	63 ms	www.dslreports.com [64.91.255.98]

Trace complete.

12.6 IPCONFIG

Ipconfig is a Windows command line utility that displays IP settings for each network interface. If Point-to-Point Protocol (PPP) or VPN is used they are also shown. With the advent of IPv6 the IPCONFIG /ALL command gets pretty verbose with all the tunnel adapters. Tunnel adapters are software that allows data to move between IPv4 and IPv6 networks.

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 address will typically be that of the broadband router.

```
Windows IP Configuration
   Host Name . . . . . . . . . . . : TomWorkstation
   Primary Dns Suffix  . . . . . :
   Node Type . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . : No
   WINS Proxy Enabled. . . . . . : No

Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix:
   Description . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
   Physical Address. . . . . . . : 00-22-64-B0-85-A9
   DHCP Enabled. . . . . . . . . . : Yes
   Autoconfiguration Enabled . . : Yes
   Link-local IPv6 Address . . . : fe80::6597:3021:9e56:2fd2%11(Preferred)
   IPv4 Address. . . . . . . . . . : 192.168.2.4(Preferred)
   Subnet Mask . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . : Sunday, December 06, 2015 7:54:08 AM
   Lease Expires . . . . . . . . . : Wednesday, December 09, 2015 7:54:08 AM
   Default Gateway . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . : 234889828
   DHCPv6 Client DUID. . . . . . : 00-01-00-01-1B-09-A4-E3-00-22-64-B0-85-A9
   DNS Servers . . . . . . . . . . : 192.168.2.1
   NetBIOS over Tcpip. . . . . . : Enabled

Tunnel adapter isatap.{BF74DEC9-92D1-4BC5-8E60-A306F00D82B5}:
   Media State . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix:
   Description . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . : No
   Autoconfiguration Enabled . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:
   Media State . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix:
   Description . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . : No
   Autoconfiguration Enabled . . : Yes
```

Useful IPCONFIG options are:

/all – verbose report
/flushdns – clears DNS cache
/release – releases DHCP lease
/renew – attempts to obtain new DHCP lease (Note) if computer has more than one adapter will get error message cannot renew lease on disconnected interfaces.

12.7 NETSH

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

In Vista and later operating systems it is a handy way to troubleshoot wireless issues. Typing the command: "netsh wlan show interfaces" displays the wireless network name (SSID), the MAC address of the access point as well as the MAC address of the computer.

12.8 Windows Master Browser

LANscan is a small utility that displays the name of each computer (assuming it supports NetBIOS) on the LAN and which one is the Master Browser.

12.9 HDD Management

The Acronis tools also come in handy for managing hard disk partitions and cloning new drives to upgrade systems.

12.10 DNS Performance Testing

DNS servers operate behind the scene largely unnoticed until something goes wrong. Normally an ISP provides the address of two DNS server so if the primary goes down the backup is able to resolve queries. When that occur will likely notice browsing problem that looks like slow Internet access. Most web pages consist of many parts each with a unique URL. If the primary DNS server fails system waits for a response when it times out it tries the backup server. This is manifest as very slow browsing.

Gibson Research has a handy DNS benchmarking tool to evaluate DNS performance.

12.11 Angry IP

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

> **Security tip** – Microsoft Security Essential flags Angry IP as a potential threat. Need to click "Allow" so it does not complain.

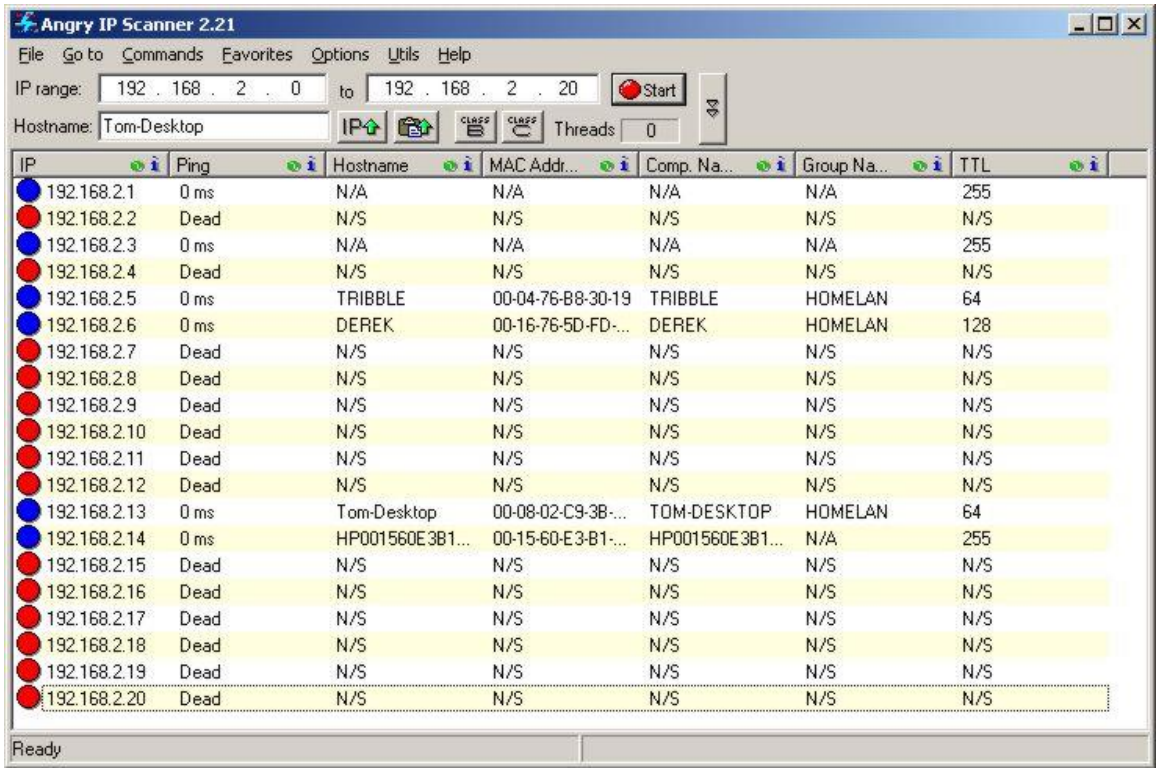


Figure 20 Angry IP LAN scan

12.12 WireShark

When you need to get down and dirty to see exactly what is going on over the wire nothing beats 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.

12.13 inSSIDer

inSSIDER is a handy troubleshooting tool for wireless problems. It scans all 2.4 and 5 GHz channels (assuming radio supports both) and display signal level, network name and encryption type. If you are in an urban area it is truly amazing how many wireless networks there are. Even though there is often more than one network on a given channel Wi-Fi radios are able to cut through the clutter and deliver fast Internet access. This utility used to be shareware now it if paid, may be able to find old shareware version still available.

12.14 Belarc Advisor

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

12.15 Internet Speed Testing

Speed testing measures end-to-end file transfer speed. For most SOHO networks ISP first-mile link will be the principal determinate of speed. However it is possible congestion elsewhere in network is degrading performance. There are numerous speed test utilities. The two I use the most often are DSL Reports and Speedtest.net.

12.16 LAN Speed Testing

If you need to test file transfer performance between PCs on your LAN use IPERF

12.17 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? LAN transfers should work even if Internet access is down. If you can get to your router's web configuration/status screen that is a good indication locally everything is working correctly.
- Is the Ethernet link indicator on? If so it means 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 APIPA address. If PC has an APIPA address 169.254.x.x there is probably something wrong with your gateway's DHCP server.
- Ping the default gateway address. This is the address of your router.
- Ping machines on the LAN by Network name and IP address. This verifies internal Windows NetBIOS name resolution is working correctly.
- If networking looks really broken try pinging local Loopback address 127.0.0.1. This tests PC's IP stack, and works even if the machine is not connected to a LAN. If this does not work try deleting and reloading TCP/IP stack. If you are using Windows here is a link to the procedure.
- If you use Ethernet and Wi-Fi on your LAN begin troubleshooting the wired connection. There is less to go wrong with Ethernet then Wi-Fi, especially if you are troubleshooting speed related issues.
- Brute force if all else fails try removing power. With power management sometimes hardware hangs, you have nothing to lose by pulling the plug rather than just rebooting.

WAN Debug

- If your DSL or Cable modem has a ready light make sure it is on. This indicates modem is communication properly over 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 (typically DSL) make sure it accepted your authentication credentials. If account uses DHCP try to disconnect and renew the address.
- If you need to change modems many ISPs bind account to modem MAC address. Either clone the old MAC on the new modem or contact the ISP to reset the line.
- Ping a stable site like Broadbandreports.com that does not block ICMP Echo (Ping). If Ping cannot resolve host name you may be experiencing a temporary DNS problem. Try Pinging the site by IP address. As of December 2015 DSLreports.com address is: 64.91.255.98. If you can ping site by IP address but not URL you have identified a DNS problem. If site is not accessible by address there is a bigger problem.
- If you suspect a problem with your ISP's DNS resolver trying using one of the free DNS services and plug it into your computer. I use Google's 8.8.8.8 just because it is easy to remember.
- Perform a Trace route (tracert in Windows) to stable sites. This will give you an idea if your ISP is experiencing congestion (high ping), or is unable to route to the remote host. It is not uncommon to have sites "disappear" after a major fiber cut as routers try to route around failure.
- If you have DSL or dialup and are experiencing slowness, temporally connect modem directly to Telephone Company NID test jack. 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.

13 Wiring – Cables and Connectors

Many improvements in wiring technology were developed by the Telephone industry to deal with 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. Within the old Bell system they were known as registered jacks. A uniform service ordering code (USOC) defined the physical jack, type of mounting, and how the jack was connected to the telephone network.

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 a wire 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. There are other types of insulation displacement technology but these two are the most relevant for our purposes.

Prior to Telecommunication Industry Association EIA/TIA 568C Commercial Building Telecommunications Cabling Standard and EIA/TIA 570C Residential Telecommunication Cabling Standard wiring requirements were developed by various industry groups or in many cases equipment vendors themselves. TIA recognized cable infrastructure has a long life expectancy. It is typically used with multiple generations of electronic equipment. TIA 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 implements a home-run wiring method between a centralized wiring closet and terminal devices. Horizontal wiring originates at a patch panel in an equipment room and runs to jacks near the network device. Short patch cables connect devices to jacks and patch panel jacks to network infrastructure equipment.

When US telephone network was deregulated 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 was to wire phone jacks as a daisy chain. Outside wiring, called 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 limitation of this method became apparent. FCC mandated telephone inside wiring confirm to TIA structured wiring guidelines. Adoption of TIA structured wiring means identical wiring methods are used for both voice and data.

13.1 Modular Connectors – Registered Jack

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 directly connect 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. Today most Registered Jack designations are only of historical interest. The RJ nomenclature has passed into popular usage only loosely coupled to its original intent. The more precise way to refer to modular jacks is in term of positions and contacts. For example the single line phone jack commonly referred to as RJ11 is a 6P2C; it is a 6-position modular connector of which only 2 contacts are used. The so called RJ45 jack used in networking is more properly called an 8P8C.

The 4-position connector is used to connect telephone handset to phone. It is not assigned a RJ designation as it was never intended as an interface point for customer equipment.

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. Analog phones are often called POTS for Plain Old Telephone Service.

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 8P8C 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.

13.2 Telco Uniform Service Ordering Code (USOC) Pin out

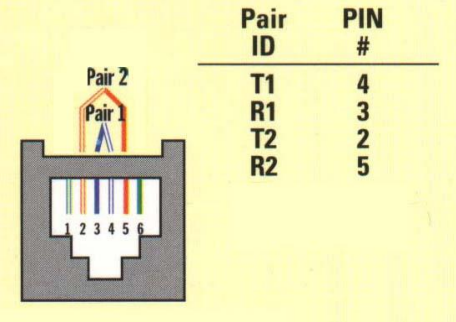


Figure 21 RJ11 & RJ14 Voice Jack

RJ11 6-position jack connects a single-line phone to the telephone network using pins 3 and 4. RJ14, also 6-position, is used with two-line phone using pins 3 and 4 for line 1, and pins 2 and 5 for line 2. An infrequently used three line version RJ25 uses pins 1 and 6 for the third line.

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 within the jack establish continuity when the alarm is not plugged in. Inserting the alarm plug opens the circuit placing the alarm in series with CPE devices. This allows the alarm dialer to disconnect downstream CPE devices so it is able to seize line and dial out even if line was being used. 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 a jack.

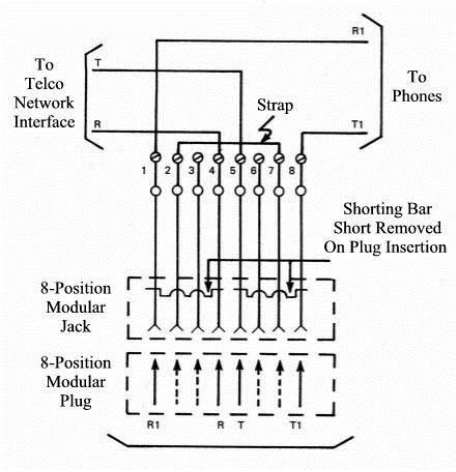


Figure 22 RJ38 Alarm Jack

Uncommon in residential use RJ48C and RJ48X are 8-position jacks used to terminate 1.544 Mbps 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 pairing arrangement is compatible with TIA 568 so LAN patch cables can be used.

13.3 Type 66 Punch Down Block

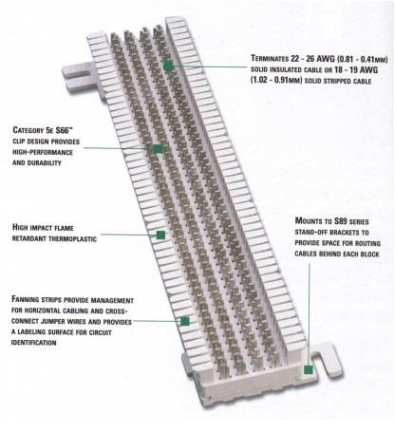


Figure 23 Type 66 Punch Down Block

The first type of insulation displacement terminal was the 66 block. These continue to be used extensively. 66-block terminates 25 cable pairs. The four terminals are bussed together allowing multiple terminations. 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 bridging clip can be used to connect the terminal on left to the right side. Use of bridging clips facilitates troubleshooting allowing circuits to be easily isolated.

13.4 Type 110 Punch Down Block

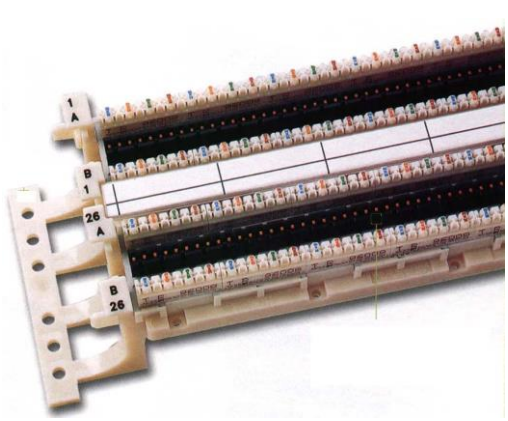


Figure 24 Type 110 Punch Down Block

Type 110 terminals allow higher density wiring than Type 66. 110 termination is preferred for LAN use. Typical 110 modules include a standoff. Building wiring is routed under the bracket through the standoff and fanned out to the appropriate location. Multiple position 110 blocks are then inserted over the base. 4-pair block are used for LANs and 5-paur for telephone wiring. Cross-connect wire is then punched down to the upper terminals of the block. Cross-connect blocks are mainly used with telephone wiring.

The 110 style terminal is used on Structured wiring jacks allowing the same punchdown tool to be used for both.

13.5 Structured Wiring

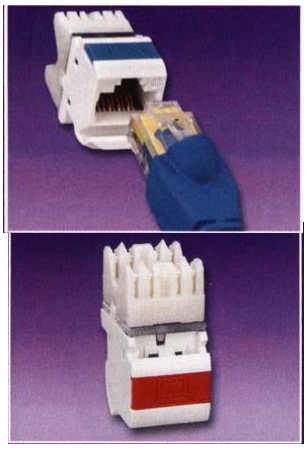


Figure 25 8P8C Data Jack aka RJ45

The key to EIA/TIA 568 & 570 is notion of structured point-to-point wiring. A cable from each receptacle runs directly to a central wiring closet. 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 patch panel and equipment used to service the room receptacle. At the other end another patch cable connects receptacle to network device.

Structured wiring specification defines multiple wiring types: 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. 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.

13.5.1 Patch Panel

Receptacles use type 110 punchdown termination. This allows rapid termination with a punch down tool. In the wiring closet each cable is terminated at a jack on a patch panel. Using a patch panel allows short jumpers called a patch cable to connect individual drop to network gear. Patch panels are designed to mount on equipment racks. It is also possible to mount then directly on a will using a hinged bracket. Panel projects several inches from the wall in normal use but by unscrewing one side of the panel it swings out providing access to rear terminations.

Figure 26 Patch Panel

Figure 27 Residential Wiring Cabinet

In office environments patch panels and active electronics are usually mounted on 19" racks. For residential use special wiring cabinets are often used to terminate phone, TV and LAN wiring and provide power for network devices.

The downside of residential wiring cabinets is space and power dissipation. My preference is to mount patch panel, punch down blocks and active equipment to a plywood backboard. This provides maximum flexibility.

13.5.2 Category Rating

Cat 5e supports Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps) over a distance of 100 meters, as well as use for ordinary phone service. Cat 3 can be used for phone service but cost is comparable to Cat 5e which provides greater flexibility. Cat 4 is obsolete. When Gigabit Ethernet was developed it was intended to use 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 (enhanced) to guarantee worst case compliance with Gig Ethernet. In reality well installed Cat 5 installation will probably work just fine with Gig Ethernet, especially the relatively short runs and low cable density typical of the home. Much of our early LAN wiring was done with Cat5 and it runs Gig Ethernet without error.

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. If Cat6 rather than Cat6A is used maximum 10G distance is reduced from 100 to 55M, still more than adequate for most residential use.

EIA/TIA is working on the Category 8 to support 25 and 40 G Ethernet. This is pushing twisted pair copper cabling to the limit. EIA is working closely with the IEEE 801.3 Ethernet committee so Ethernet Phys and cabling work well with one another. Both specs should be approved sometime in 2016. For residential use

this is pretty much a moot point, it will be a long time if ever before residential networks come anywhere near requiring that speed. Cat 8 is primarily targeted at data centers with huge bandwidth requirements.

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 than category. Class C is equivalent to Cat 3, Class D to Cat 5, and Class E to Cat 6.

Category rating is end to end. In order to meet the spec: wire, connectors, and installation practice must meet the appropriate grade. 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.

13.5.3 Cable Types

The most common type of Category rated 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 attractive when used with high density wiring such as data centers.

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 degradation. Outdoor cable is gel filled (icky-pic) 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.

For long runs especially between buildings fiber is ideal. Being nonmetallic it is not susceptible to lightning damage. The downside of fiber is termination cost and cost of electro/optical converters.

13.5.4 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 cables are used with 10 and 100Mbps Ethernet to transpose 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.

Crossover cables are pretty much obsolete. Newer devices implement Auto-MDIX that automatically determines transmitter and receiver. Gig and higher speed Ethernet use all four pair in a hybrid arrangement. Auto sensing eliminates need for crossover cables and uplink ports.

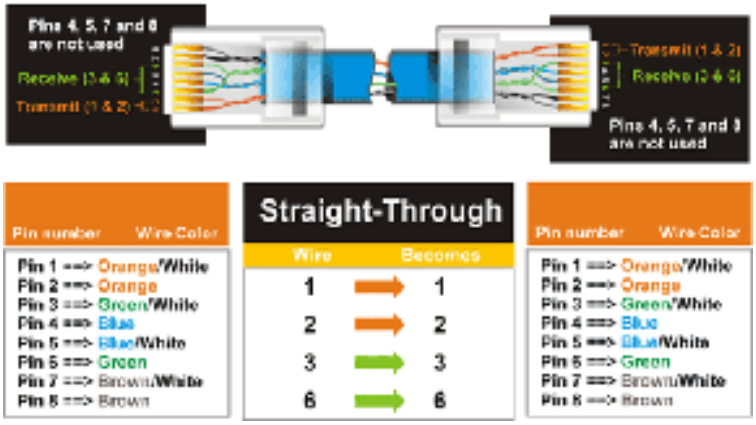


Figure 28 Patch Cable

13.5.5 TIA T568A and T568B Structured Wiring Pin out

A cause of much confusion when implementing EIA/TIA 568 structured wiring is the fact two different connector pin outs are 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.

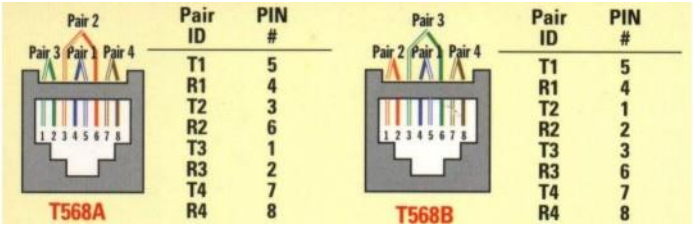


Figure 29 8P8C Structured Wiring Jacks

Pairing arrangement of TIA differs from that used on USOC voice jacks. The Inner two pairs are the same but outer two differ. This was done 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 due to split-pair.

The inner two-pair of TIA-568 8-postion jack mates with inner two pair of RJ11 and RJ14 USOC 6-position plug. This eliminates need for adapters when connecting RJ11 and RJ14 equipment to 8-pos structured wiring. EIA/TIA 568 commercial and EIA/TIA 570 residential structured wiring specifications require use of T568A pinnout unless building is already wired with B. T568A is preferred because inner two pair map directly to pair 1 and 2 on USOC punch down blocks, making cross connection easier. T568B is popular in the United States because it uses the same pin out as AT&T key systems in widespread use prior to the development of structured wiring standard.

13.6 Color Code

Legacy Telco USOC RJ11 and RJ14 jacks use green, red, black and yellow conductors. TIA Category rated cable consist of 8-conductors, arraigned as 4-twisted pairs. Each pair is a different color, to identify conductors within each pair one wire is solid color (Ring) the other has a White stripe (Tip). The term Tip and Ring refer to old style manual switch boards where operator had to physically insert a phone jack to make the connection.

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 good practice to maintain proper polarity. Low cost phone line testers are available to quickly determine polarity.

TIA Color Code	T568A 8-pos (preferred)	T568B 8-pos	Telco Color Code	Telco Designation	RJ11/14 6-pos
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			
Green	Pair 3 pin 2	Pair 3 pin 6			
Brown/White	Pair 4 pin 7	Pair 4 pin 7			
Brown	Pair 4 pin 8	Pair 4 pin 8			

13.7 Telephone

Traditional wired telephones are often called POTS, plain old telephone service. We have two wired phone lines, one for personal use and one for business. Lines are configured as a hunt group, also called transfer on busy. If line 1 is busy incoming calls are redirected to line 2. Hunting is unidirectional; if someone calls the second line and it is busy switch 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. Surprisingly there was no extra charge for this feature, probably because it results in more completed calls.

Before the advent of broadband Internet we made extensive use of dialup. Dialup uses the public telephone network to provide Internet access. Unlike ADSL a dialup connection actually places a phone call to the ISP and ties up the line for the duration of the session. If someone picks up a phone it will disconnect the session and if the phone is in use when the modem attempts to initiate the call it will interfere with the voice call. For readers still stuck on dialup I designed a device to minimize interference between dialup and phone lines. More information about the Modem Access Adapter (MAA) is available on the writings page.

For some years I after we were able to get ADSL maintained dialup as a backup. We no longer do so. DSL service has been very reliable. With web sites increasing being optimized for broadband dialup browsing is painfully slow.

13.8 Telephone Network Interface Device (NID)

Figure 30 Typical Telco Demarc

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 customer's premise. Inside wiring and equipment became the customer's responsibility. This created a dilemma for the Phone Company, how to determine if a problem was their responsibility or 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. 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 disconnect inside wiring for testing. 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. Modern NIDs use gas tube protectors rather than old style carbon block. Gas tube provides tighter control of overvoltage and being hermetically sealed minimizes added noise.

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 line module 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.

13.8.1 POTS/DSL Splitter

Figure 31 Whole House POTS/DSL Splitter

ADSL shares the same phone line used to deliver POTS. Filters are required to prevent high frequency DSL signaling from interfering with voice. To reduce cost ISPs often send customer a self-install kit. The kit includes in-line filters that must be used by each non-DSL device connected to phone line.

Rather than using a microfilter at each non-DSL device I installed a POTS/DSL splitter. Splitter provides a low pass filter isolating voice from high frequency DSL. 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 allowing the one in the NID to be removed. ADSL was designed to operate in the presence of half-ringer but it represents a small additional load.

In some cases the local phone company will install a splitter directly in the NID eliminating the need for customer installed external splitter or in-line filters.

> ***Home Alarm Tip*** – If a phone is connected to splitter "Data" port it will work normally. This creates a potential safety hazard with a home alarm system. If a phone is inadvertently connected to data port and is in use when alarm needs to seize phone line it will be unable to do so. Care should be taken when using a splitter so only DSL modem is connected to "data" jack. The other option is to install splitter after alarm jack and filter alarm separately.

13.9 Coaxial Cable

Historically 75 ohm coaxial was limited to RF TV distribution of: Over the air, Cable and Satellite. It is possible to use this cable to also carry digital data. A number of fiber ISPs are using MoCA technology to eliminate the need to run Category rated cable to set top boxes. If you need to provide wired Internet and have coax cabling at the location this may be an option. As with UTP cabling special tooling is needed to strip, prep and install F style connectors.

13.10 Transient Surge Protection

The key to minimizing lightning and transient voltage damage is bonding all services together with a low impedance path to each other and to Earth. All conductors entering the building must be bonded together. Bonding minimizes the voltage difference between conductors during transient events. IEEE has a nice white paper about lightning and surge protection. A good analogy is to think of your home as a bank vault. The goal is to prevent dangerous voltages from passing through the perimeter and to insure everything metallic is at the same potential.

Recent versions of the National Electrical Code (NEC) require the installation of an intersystem bonding bridge. This insures all conductors are connected to an equipotential point to minimize differences in potential during transient events. Transient protectors are used to clamp overvoltage of ungrounded conductors by connecting to this bonding point.

13.10.1 Power

Figure 32 Power Surge Protector

A whole house surge protector should be used to protect electrical system. Goal is to direct transient energy into low impedance ground and to provide low impedance bonding of all metallic conductors. We use a GE THQLSURGE protector. Installation is easy. Device plugs into breaker panel much like an ordinary two-pole breaker. A small neon light indicates the protector is working correctly.

Surge protectors do not absorb energy they divert it. If diversion path is not low impedance a substantial voltage difference is created. This is what kills electronic gear.

13.10.2 Telephone

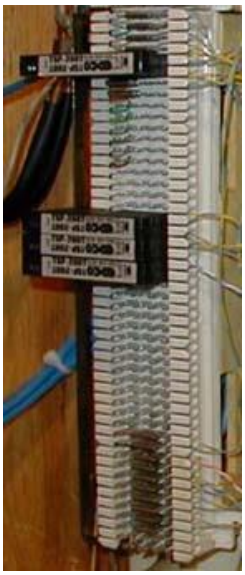


Figure 33 Telco Surge Protector

Telephone Company provides lighting protection as part of the NID. NID is connected to building ground system. Electronic devices are more fragile than electromechanical phones. This is especially the case with computer equipment because it has multiple connections: power, phone, DSL and Ethernet. This makes equipment susceptible to transient surges. Adding secondary protection minimizes risk of equipment damage. This is especially the case if you have an old style carbon block protector rather than new gas-tube NID. Best location for secondary protection is at building entry point. This allows protector to use same Earth ground as AC mains to minimize voltage difference between services.

EDCO TSP-200 series protectors add very little capacitance to phone line. This is critical so protector does not interfere with high frequency DSL. Protector clips 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.

13.10.3 Coaxial TV

Figure 34 Coax Surge Protector

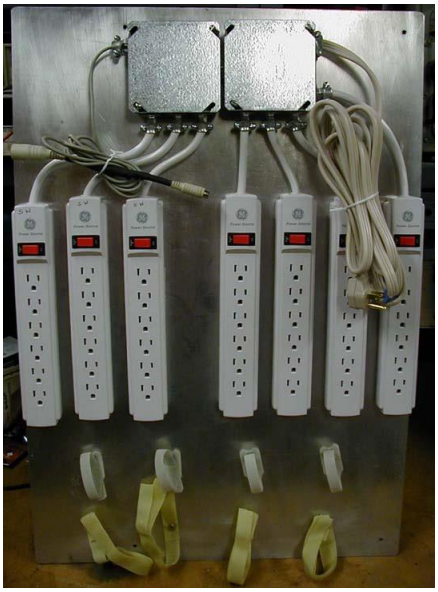
Cable and Satellite providers bond the coaxial cable sheath, where it enters residence, to the building ground system. This insures sheath is as at same potential as building Earth ground. As with Telephone it is advisable to add secondary coaxial protection to limit transient voltage on the inner conductor.

We have an Over the Air (OTA) TV and FM antennas. They are grounded and bonded to the building ground system. A coaxial surge protector is used on each cable where it enters the building.

13.10.4 Point of Use Protection

Once perimeter protection is in place installing point-of-use surge protectors offer additional transient protection. Since damage is caused by differences in potential between conductors ideally all conductors should pass through the surge protector for maximum effectiveness.

13.11 Power Distribution



Electronic devices create a jumble of cables, both data cables and power cords. Low power devices tend to use external power supplies, despairingly 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 switched by the workstation. Power bricks take up a lot of space, so the number of outlets is generous. Panel has four always on strips with six receptacles each and three strips controlled by workstation. A cable plugs into PS/2 keyboard or mouse port sensing 5 Volts. That signal is used to control a solid-state relay to turn power on/off.

Figure 35 Power Distribution

> ***Power Tip*** -- some PCs leave PS/2 ports powered all the time to allow keyboard controlled wake-up. In that case power panel needs to sense power directly from PC main power supply. Many newer PCs no longer have PS/2 ports. Assuming USB 5 volt power is turned on/off that can also be used to switch external power.

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

13.12 Tools

Proper tooling is essential to install a reliable network. Jacket ripper uses a sharp blade to cut through outer jacked without deforming twisted pair or cutting through insulation. Punch down tool with interchangeable blades for 66 and 110 termination is needed for both LAN and telephone work. I found a handy palm rest at a local big box home center to hold Jack during termination. This makes terminating jack easier. I use Rino hand labeler to mark cable ends. This is a handy little device that dispenses and cuts cable labels.

Once cabling is installed commercial installations perform full parametric testing to verify system meets applicable performance standards. That test equipment is very expensive and not practical for the casual installer. There are numerous continuity testers in to $20-$50 range. These low cost tester are only able to verify continuity and shorts, will not detect excessive untwist, split-pair etc. Still for the price is a great time saver to verify cable is property terminated.

Phone line tester is handy for checking active telephone lines. It verifies line polarity, voltage, loop current and ringing voltage. If you do a lot of telephone work a buttset is handy to have. A buttset is special purpose telephone used for testing.

If you are faced with the task of identifying unknown cables a toner is invaluable. Toner consists of two parts a tone generator and sensor. The generator places a signal on the wire. When the sensor is brought near it emits a tone due to capacitive coupling.

Lastly I found cable breakout tester, typically called a banjo, to come in handy doing nonstandard wiring. Breakout provided access to individual conductors to verify wiring.

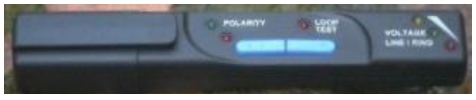
Tool	Purpose
Wire Cutters	Cut cable to length
Jacket Ripper	Removes outer cable jacket
Punch down Tool	Terminate Punch down terminals
110 Blade	Terminate 110 blocks
66 blade	Terminate 66 blocks
Palm Rest	Holds Jacks being terminated
Crimper	Crimps cable into modular plug
Fish tape	Snake wire through walls
Labeler	Identifies Cable ends
Phone line Tester	Indicates polarity and loop current of phone circuit
Cable Tester	Verifies proper installation of Category rated wiring
Toner	Identifies cable ends
Buttset	Portable Telephone to test phone line
Breakout adapter	Electrical access to each wire

Cable Ripper

RJ11/45 Crimper

66/110 Punchdown

Wiring Tester



POTS Telephone Tester

Breakout Adapter

Figure 36 LAN & Telephone Tools

13.13 Putting it all Together

The drawing on the next page 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. House was built well before the days of home networks. Wiring terminates in two different locations, one for phone and alarm wiring another for networking.

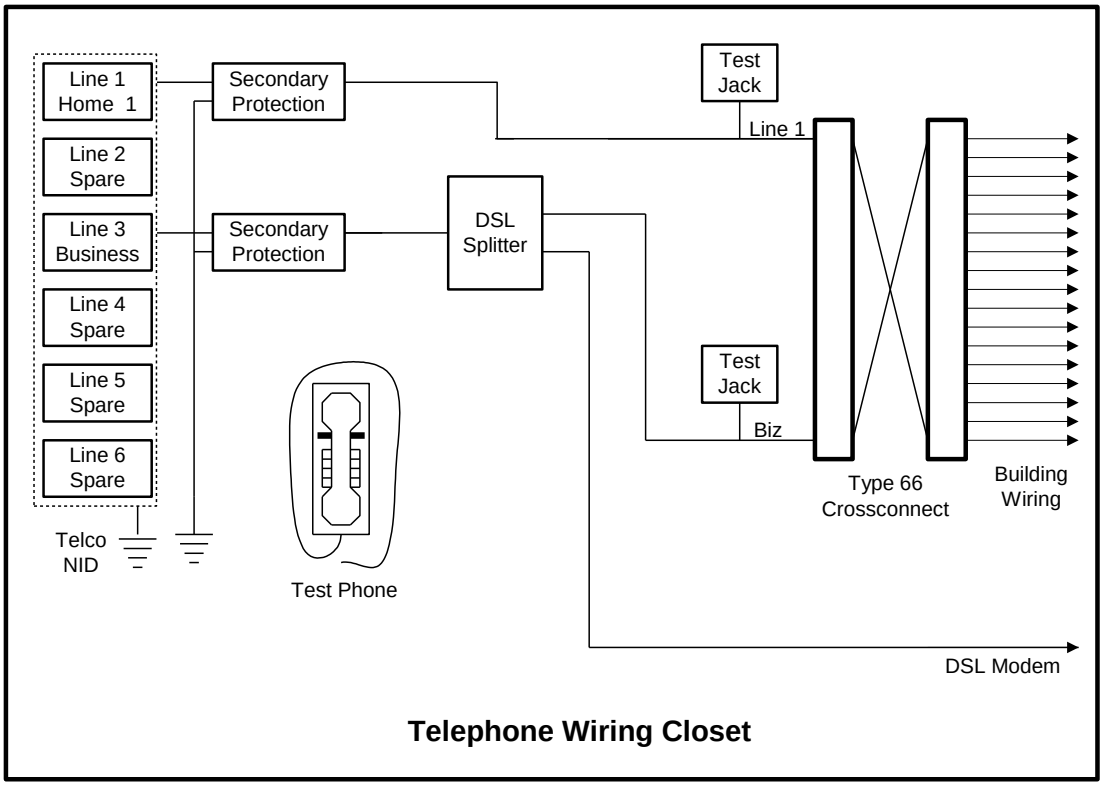


Figure 37 SOHO Telephone Wiring

13.13.1 Telephone wiring

Telco NID is located in basement. From NID each line goes to a secondary protector. A POTS/DSL splitter is connected to business line. Splitter "Data" port runs directly to DSL modem. "Voice" port terminates at 66-block to be connected to multiple phones.

To make changes easier all building wiring is terminated on 66 style punch down blocks. Cross-connect wire is a single twisted pair used to interconnect building wiring. This makes it easy to rearrange wiring by adding and removing cross-connects. Test jacks connected to each line allow a test phone to be conveniently plugged in during troubleshooting. The test jacks are different than the ones in the NID in that connecting a phone does not disconnect downstream wiring.

An old style Western Electric wall phone is permanently mounted in 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 phone permanently located in wiring closet insures it is available when needed.

13.13.2 LAN Wiring

House was built in 1982 predating SOHO networking. LAN wiring closet is in center of basement rather than at outer edge with phone wiring to optimize cable runs. LAN wiring has been expanded over the years. When first installed wired a few drops in the basement. Several years later added drops in bedrooms. Recent additions have been to add several home automation controllers.

When I initially installed LAN did not use patch panel. Instead terminated each cable with a modular plug and plugged cable directly into a small Ethernet hub (home network predates widespread use of switches). Modular plugs are more difficult to install than receptacles so this is not for the faint of heart. Over time some of the drops failed due to connector problems. Rewired the system using a 24-port 1U rack mounted Patch Panel. Like most other networking items Patch Panels have gotten dramatically cheaper over the

years. I used a 1U hinged bracket to mount panel to the wall. With the addition of multiple home automation controllers all 24 ports are wired, even thou not all are currently being used.

> **Tip** – if you decide to terminate cable with modular plugs make sure the plug is compatible with the type of wire you are using. Plugs are normally used on patch cords with stranded conductors. The internal contact for stranded and solid conductor wires is different.

13.14 DSL Router

The ISP supplied ZyXEL P-660R-D1 DSL router lives in the same closet as the patch panel and Ethernet switch. One of the patch panel drops terminates in the Telephone wiring closet. The "data" port of the whole house POTS/DSL splitter is connected at that end and a RJ11 patch cable connects the patch panel port to the modem. An Ethernet patch cord connects the router LAN port to the switch.

13.15 Ethernet Switch

I wanted to locate the Ethernet switch directly above the patch panel but the switch is not rack mountable. I bent a piece of thin gauge aluminum stock to act as a shelf above patch panel. This provides a convenient place for the Ethernet switch. Switch connects to patch panel with 1-foot patch cables.

Figure 38 16-port Ethernet Switch

Switch is a Netgear Prosafe Plus GS116Ev2 16-port fanless Gig switch. The switch is an interesting hybrid between dumb unmanaged and full blown manage switch. It can simply be plugged in and it works as a dumb switch. A built in web server provides access to advanced features. So far I have been very happy with my decision to upgrade.

13.16 Wi-Fi Access Point

The IEEE 802.11n standard represents a significant advantage over previous b and g generations. I replaced our preN AP with a Netgear wn802tv2.

Figure 39 AP

Setup was pretty straightforward. AP defaults to static IP address 192.168.0.233. To configure AP connected it to wired port on my laptop and configured the laptop statically to match the settings of the AP. Logged into the AP and changed AP network settings to match our LAN. I set network resources statically above the range used by DHCP

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

Ideally passphrase should be random and very long to defeat dictionary lookup attack. Good passphrases are difficult to generate manually. Luckily Internet once again comes to the rescue with an online passphrase generation site.

WPA2 has several encryption options, for maxim security and performance use AES not TKIP. Temporal Key Integrity Protocol was developed as an intern improvement to address serious weaknesses discovered in the original encryption scheme Wireless Equivalent Privacy (WEP). TKIP is in essence a wrapper around the flawed WEP, as such is it more computationally intensive and not quite as secure as AES. Unless you need backward compatibility with old Wi-Fi clients use AES.

13.17 Future Proofing

During any discussion about wiring the topic of future proofing is bound to come up. The problem is wiring and buildings have very long life expectancies. It is difficult to anticipate network requirement 10 – 50 years down the road. Some folks are proponents of the "kitchen sink" approach, wire up every possible location with every sort of physical connection that may be needed. The down side is excessive upfront cost and it is rather brittle in the face of changing needs and technology.

Try to anticipate near term needs but don't go overboard. No matter how carefully you plan down the road you will find yourself in a situation where you need to add wiring for something completely unanticipated. My most recent Ethernet addition was adding a drop near our aquarium to support the PLC controller I designed. If you told me I needed an Ethernet drop by the aquarium when I first installed the LAN in 1998 I would have said you were crazy. To deal with the unanticipated try to include pathways that makes it easy to add wiring. Install empty conduits; build wiring chases etcetera to make modifications as easy as possible. I've been lucky. When we built the house there is ventilation duct used to blow air from the cathedral ceiling on the second floor down into the basement. That has turned out to be a lifesaving cable chase when I've needed to add wiring.

My Top 10 Home Networking Predictions

1. POTS phone service will be replaced by VoIP and network convergence, eliminating the need for analog POTS wiring but increasing the need for Ethernet ports that supply power (PoE) to make deploying wired phones easy. Not everyone wants a wireless phone on their desk.

2. Copper twisted pair will remain the technology of choice for residential fixed location network devices. Fiber is great but costly. Where fiber shines is wiring outbuildings because it is immune to lightning.

3. 1 Gbp/s data rate per device will be more than adequate for years to come. Yes there are faster Ethernet standards but we are approaching the "good enough" speed for home LANs.

4. Improvements in Wi-Fi and increased use of hand held devices will place a premium on wireless access.

5. There is a long term trend to Video over IP (VoIP) but it will be a long time before RF based coaxial TV distribution fades to insignificant. MoCa is a good way to bridge the two technologies allowing IP based devices to utilize coax for both RF and Internet.

6. Smart white good evolving in concert with the smart power grid allowing network management via web protocols. ZigBee or something similar is likely to dominate that space. Our new washer has near field communications (NFC) built in allowing it to talk to a smart phone, but only if it is right next to the machine.

7. Security systems are migrating to wireless with ultra-low power devices that harvest energy eliminating the need for batteries.

8. Deployment of 60 GHz wireless should be a boon to eliminate the rat's nest of wires needed in a typical home theater system. This is a short range wireless network limited to a few feet but blazing speed is ideal to for A/V equipment.

9. Converged cellular and Wi-Fi networks. As demand for wireless bandwidth explodes carriers will look at offloading traffic to Wi-Fi networks. This prediction has already come true. Our cellular vender Republic Wireless has a Wi-Fi first strategy.

10. US residential customer will continue to have limited choice of broadband ISPs and prices will remain high by worldwide standards.

14 Laptops, Cell Phones & Tablets – Internet on the Road

My current laptop is a Lenovo T61 widescreen running Win7. It has both Ethernet and 801.11n Wi-Fi built in. Both my wife and I have used it for presentations and being on several volunteer committees it is nice being able to work on documents in real time rather than trading emails. I've also used it on the bench with a USB logic analyzer to troubleshoot equipment.

For convenience I always purchase a second power adapter. One stays in the laptop travel bag the other is near my desk so I can plug in the laptop and charge it without having to hunt for the charger.

14.1 Security

A large number of laptops/phones/tablets are lost or stolen daily. Once you have lost possession of your computer an attacker has unlimited time to crack whatever security you have used. If the laptop has sensitive information consider using encryption to protect files, or better yet leave the sensitive files in the office and use remote desktop or Citrix to provide access without the need to save the data locally.

Wi-Fi hotspots normally do not provide over the air security like WPA2. This means non-encrypted traffic is easy to eavesdrop. The worst offender is SMTP/POP protocols since they send login credentials in the clear. If your ISP supports using SSL access to email use that to protect you privacy when accessing email. If not consider restricting access to over a VPN to protect privacy.

Windows finds other network resources locally by broadcasting info over the LAN. Normally when connecting to public networks these broadcasts are blocked (port isolation). However if the public network is not configured correctly others may be able to see shared directories/files/printers. It is good practice to disable sharing on mobile devices. This does not impact being able to access shares on other computers just does not share files on this particular PC. Windows 7 concept of a password protected Homegroup improves the security while traveling but I was never able to get it to work reliability.

Flash drives are often used to move files around between PCs at meetings. There is always a risk of plugging in an infected drive. Maintain up to date anti-virus software and make sure it is configured to verify removable media.

15 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 operated by a hosting service. Registering a domain name creates a permanent Internet presence regardless of how the business connects to the Internet or where the servers are located.

Even if you are not a business having your own domain is still advantageous. It gives you a personalized email address for as long as you want it. That makes it easy for folks to stay in touch. Having your own site gives you a great deal of freedom to use it as you please. This paper is a good example. I enjoy writing about what I am doing and the solutions to various problems I've worked out. My site provides a vehicle to publically post those articles. Lastly if you are in a technical field it can't hurt your resume that you have your own site.

For most small to midsized businesses using a virtual server managed by a hosting service is the optimum strategy. Server is located in a data center with virtually unlimited access to bandwidth. A single server is able to host many web sites resulting in very low cost. The server used for my site hosts several hundred other web sites in addition to mine.

The hosting service takes care of most of the technical details: setting up the various servers, registering a domain name and creating DNS records. This allows the customer to focus on the creative aspects of building a web site.

Creating the site itself requires a combination of artistic and technical skills. There are many software packages available to help create a web site. In some cases site development tools are provided by the hosting service as part of your contract. If you don't want to develop the site yourself there are many companies that specialize in web site development.

15.1 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's name is trademarked. Large companies often register variations on their name to prevent cyber squatters from registering confusing or derogatory domains. The COM and BIZ TLDs are for commercial use. 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 ICANN or other registration agencies to insure each domain name is unique within its respective TLD.

The registration process involves providing information on domain name ownership and creating 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 or if name is already in use will need to choose a different name. If you really want a name that is already registered all is not lost. You can try to purchase it from the owner. When I registered my domain wanted schmidt.com but that was already registered by a printer in Minnesota so I picked tschmidt.com

15.1.1 Email

With a registered domain name email is addressed to the domain, not a third party. This personalizes your businesses persona. Email is structured as username@yourdomain.TLD. Most hosting services allow multiple mailboxes. This enables employees or family members to have individual accounts without the need to run an internal mail server.

15.2 Web Server

There are many ways to operate a public web server: hosting service virtual server, locate your equipment at a data center, or run the server locally.

15.2.1 Virtual Server

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 can have a web site. Virtual hosting is appropriate for low traffic sites. The hosting service runs multiple virtual web servers on a single physical server. We use a local hosting service Hollis Hosting at a cost of $40 per year plus another $15 for annual domain registration. Most hosting services have business relationships with a domain registrar. This allows one stop shopping for domain registration/renewal and Internet hosting. Our domain 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.

Transferring account from one hosting service to another is pretty easy. DNS registrar needs to be notified of new Nameservers and web site contents transferred from old to new server.

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.

15.2.2 Dedicated Server 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 restricts access to sensitive company data to in-house IT personnel.

15.2.3 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. To accomplish this one needs to set up a web server. Running the server on a dedicated PC is more secure than sharing the PC between web server and other functions because it is easier to constrain what the attacker is able to access if they compromise the computer. Abyss web server is free for personal use and runs on Windows PCs. I use it for an internal non-public web server on our network.

Residential broadband is typically asymmetric; upload is much slower than download. This limits site performance. Heavy site traffic will interfere with other Internet usage.

Most residential broadband uses dynamic address assignment making it difficult to host a server as the address can change unpredictably. Dynamic DNS is a workaround. The DNS service is updated each time the server's address changes. This works well for personal sites but be aware the site becomes temporarily inaccessible during the address update making it inappropriate for serious commercial use. Software running on the customer side detects when the IP address is changed and updates the dynamic DNS service.

Residential ISPs commonly prohibit customers from operating servers. Some enforce this restriction aggressively other turn a blind eye unless there is a problem. Some ISPs block access to Port 80 used to access web sites forcing the use of a nonstandard port. This is not an issue if you are using the site it for personal access simply append the port number to the URL so the web browser knows which port to use. For example: http://mysite.com:8080

Residential accounts are normally limited to a single IP address. This is a problem if more than one web server is needed. A workaround is to use a non-standard port, such as 8080, for one of the servers.

15.3 WHOIS Record

Information for each registered domain is located in the WHOIS databases maintained by Regional Internet Registries (RIR). The database maintains administrative and technical contact information about the site. The Whois database does not maintain information about the site itself. To find the IP address of a site one needs to query one of the nameservers associated with the site.

15.3.1 Administrative

Administrative information records data about site ownership and contact.

15.3.2 Technical

Technical information records data about network operation center contact.

15.3.3 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 DNS servers are in widely separate locations served by different providers. This minimizes risk the authoritive Nameserver ever becoming inaccessible.

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:
95 Melendy Rd
Milford, NH 03055-3417
US

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

Technical Contact:
Schmidt Consulting
Tom Schmidt admin@tschmidt.com
+1.6036732463
Fax:
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 2016 05:00:00

15.4 DNS Record

Once domain is registered Nameserver records must be created. These records provide translation between URL and IP address. If you use a hosting service they will most 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 site View DNS has a nice tool to check DNS entries for errors.

The name server maintains a number of different records. Below are commonly used record types.

15.4.1 Address Records (A)

Address records map host name to IP address.

15.4.2 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 resolves to the same IP address.

15.4.3 Mail Exchange Records (MX)

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

15.4.4 Pointer Records (PTR)

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

15.4.5 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.

15.4.6 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.

15.4.7 Sender Policy Framework (SPF)

Sender Policy Framework (SPF) adds DNS record to allow mail servers to verify incoming email was sent from domain and not spoofed by spammer.

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 minimum ttl: 86400	86400s (24h)

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	72.37.245.142	14400s (4h)

15.5 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. Often the hosting service provides a development toolkit to assist customers designing a web site. For more complex sites specialized design tools such as WordPress can be used to good advantage. If you want to outsource the design there are numerous companies that specialize in web site development.

15.5.1 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 FileZilla.

15.6 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.

```
# www.tschmidt.com
# Created 2/25/2006

# All robots can spider domain
User-agent: *
Disallow:
```

15.7 Site Management

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.

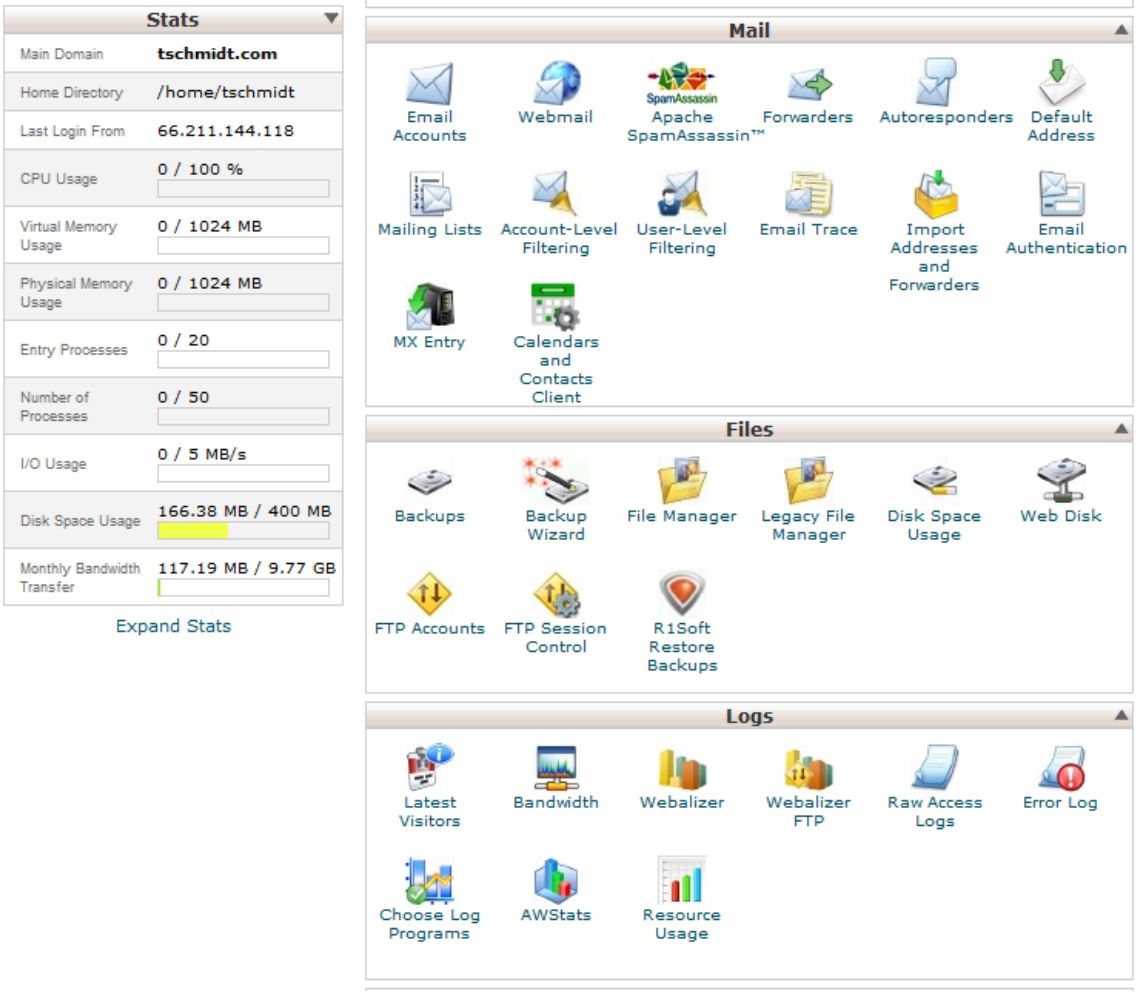


Figure 40 Hosting Service cPanel Home Page

Conclusion

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

Significant technical expertise is required to setup a network. The necessary components are readily available but amassing the knowledge needed to create and troubleshoot can be rather intimating. Each year more residential and SOHO networks are installed. Manufactures are getting better at designing customer friendly equipment. But one needs to be careful, sometimes ease of use brings with is security issues. In general failures are pretty straightforward to identify and fix once 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.

Happy Networking