Schmidt Consulting

Living with a Small Office Home Office Network

2025 Edition

12/1/2024

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

Abstract
This paper documents our experience setting up and using a SOHO (small office home office) network over many years. It offers guidance selecting an ISP, internet connection sharing, presents wired and wireless LAN options and discusses numerous network services. We have a poor man's server running on a laptop for: file sharing, automatic PC backup, NTP timeserver and a private internal website. In addition the LAN supports multiple DIY home automation controllers and cell phone WiFi offload.

In late 2021 we were finally able to upgrade from DSL to PON (passive optical network) internet provided by the local Telco Consolidated Communication. We also moved our landline phone service to them using VoIP over the same fiber.

I use a hosting service, Dream Host, for public web server and e-mail. Using a hosting service moves web site traffic off the local broadband connection and significantly eases the task of securing the local network. Having a registered domain name provides a persistent email address reducing risk of losing contact with colleagues and friends. This was more important before the advent of third party email services. Having your own web presence gives you a great deal of flexibility even if not running a business.

We use Boost Mobile a MVNO (mobile virtual network operator) for cell phone service. Our phones support WiFi calling, a useful feature here in terrain challenged NH.

Table of Contents

1 Overview

In 1998 I set up a home network as part of starting a consulting service and wanted to learn about the design and operation of a SOHO (small office home office) network. Back then residential networks were fairly rare and some ISPs even prohibited them. Today residential networks are ubiquitous and the proliferation of portable devices means customers often use a combination of wired and wireless connectivity. It has been fun documenting how our home network has changed over the decades. We began with a V.90 dialup connection, Wingate connection sharing software running on a Win98 laptop and a small 10 Mbps Ethernet hub. After that we had DSL for a couple of decades from various providers. Finally in 2021 we were able to get fiber internet.

Our current internet connection is 100/100 Mbps PON (passive optical network) provided by the local Telco Consolidated Communication under the Fidium brand The ONT (optical network terminal) (Adtran 411) also supports landline phone via a RJ11 jack. It uses VoIP over the same fiber as internet access. The Ethernet port of the ONT feeds a Netgear AX1800 RAX10 WiFi router. Over the years the LAN has expanded beyond my home office to encompass the entire house with a total of 24 Ethernet drops serviced by a Netgear Prosafe Plus GS116Ev2 16-port Gig Ethernet switch and a smaller Netgear GS108Ev3 8-port switch dedicated to home automation widgets. We have a portable gas generator to manage utility power outages. To augment the generator I built a DC UPS to operate critical LAN equipment during a power outage when the generator isn't running.

My wife and I use a couple off lease HP Z230 SFF desktops and Lenovo ThinkPad T520 laptops running Win 10. In the past I've recycled the previous generation desktop as a poor man's server. This time I purchased an off lease Lenovo ThinkPad T420 laptop. That reduced previous server power consumption from 80 watts to 20. For storage I stuck a large HDD in the DVD bay. For the server I found a nifty software application called Input Director to share the main workstation keyboard and mouse instead of using a KVM. To round out my office I recycled one of the old SFF desktops as a test PC continuing to run Win 7 and dual boot Ubuntu. Acronis True Image provides automatic backup of PC data to the server. For offline backup we use an external USB drive.

I use a Belkin 4-port KVM (keyboard, video and mouse) to switch between: 1) main PC, 2) dual boot PC and 3) unused spare. The 4th KVM port is used for testing. I cabled it along with Ethernet and power making it easy to temporally connect a computer for setup and testing.

We use a Roku Express connected to our main TV for streaming. At some point we will upgrade our TV to ATSC 3.0 as we use an antenna for live TV reception.

Over the years I've built several home automation devices for various functions: greenhouse, wood heat, window ventilator, aquarium, an outdoor temperature logger and most recently for notification when snail mail arrives. 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.

Our printer is a networked HP Officejet Pro 8100. I use a Brother P-touch PT-2430PC printer for labels. An Epson V550 flatbed scanner turns paper into electronic documents.

1.1 *Organization*

This paper discusses internet access and LAN (local area network) components we use to support our communication requirements. A separate paper on my web site goes into detail about the various methods and tradeoffs of internet 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 site. 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 tremendous flexibility about your internet presence. For a few dollars per month it represents 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 we implemented specific requirements to meet our needs. For up to date product reviews the reader is directed to the many publications and articles on the subject.

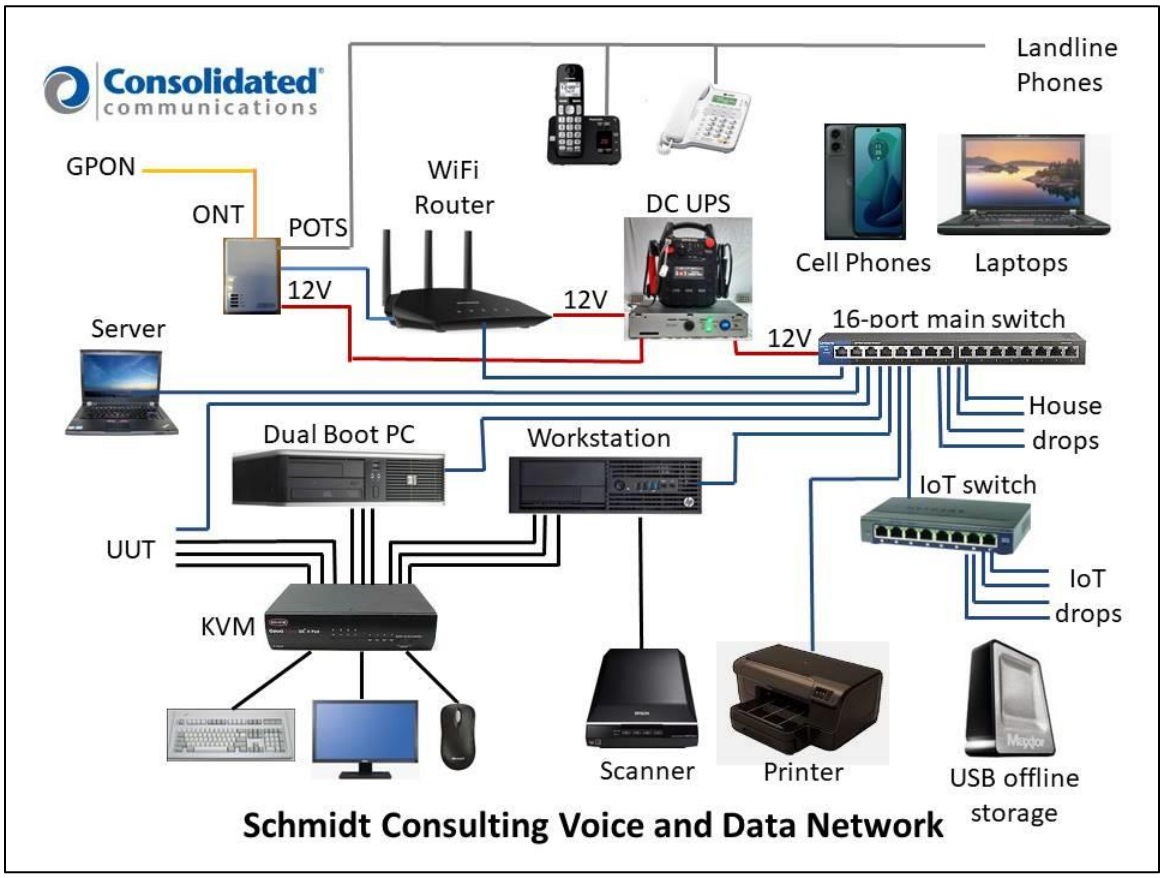


Figure 1 Schmidt Consulting Network

1.2 Goals for SOHO network

- Share internet connection
- Wired and Wireless LAN
- File sharing
- Printer sharing
- Internal private web server
- NTP computer time synchronization
- Automatic PC backup
- Offline file backup
- Home automation
- Internet TV

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 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. The internet is fundamentally different than the legacy PSTN (public switched telephone network). 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 destination address field to determine how best to forward it toward the destination.

2.1 *ISP (Internet Service Provider)*

ISPs (internet service provider) connects end users to the internet. The incredible popularity of the internet is driving demand for higher speed at 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. The 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 and wireless broadband is available from multiple sources:

1) Comcast DOCSIS, MSO (multiple system operator)
2) Consolidated Communication PON, ILEC (incumbent local exchange carrier)
3) FirstLight Fiber CLEC (competitive local exchange carrier)
4) There are numerous wireless carriers offering data plans

Consolidated Communication is aggressively deploying fiber PON (passive optical network) throughout New England. They offer four residential speed tiers of symmetrical access under Fidium branding: 100 Mbps, 300 Mbps, 1 Gog and 2 Gig. If the customer has fiber internet they offer a much reduced rate for traditional telephone service. This is via VoIP over the fiber but the ONT emulates the analog phone line.

For a more detailed examination of ISPs the interested reader is referred to the First-Mile Access paper on 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 point A to B. Speed is the 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 on a

Voice over IP (VoIP) phone call latency is critical to maintaining good two way 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*

Computers use IP addresses to communicate with one another. However these are not very human friendly. The URL (uniform resource locator) is a human friendly handle rather than the numeric IP addresses. Translation of URL to IP address is performed by DNS (domain name system). Domain names are hierarchal, evaluated right to left. The highest-level of the tree called Root name server is implied. Next is the TLD (top-level domain) 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 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 DNS (Domain Name System)

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 the 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 DNSSSE (DNS Security Extensions)

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

The 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 the DSLreports web site

```
Tracing route to dslreports.com [64.91.255.98] over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  home [192.168.2.1]
  2     7 ms     8 ms     7 ms  10.10.10.14
  3     6 ms     8 ms     6 ms  20.l.burlvtma96w.vt.consolidated.net [70.109.168.167]
  4     7 ms     7 ms     7 ms  burl-lnk-70-109-168-28.ngn.east.myfairpoint.net [70.109.168.28]
  5    14 ms    17 ms    17 ms  et-0-3-0.mpr1.yul1.ca.zip.zayo.com [64.124.142.45]
  6    31 ms    37 ms    34 ms  ae2.cs1.lga5.us.zip.zayo.com [64.125.27.164]
  7     *       33 ms     *     64.125.28.191
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    43 ms    43 ms    43 ms  lw-dc3-core1.rtr.liquidweb.com [209.59.157.16]
 11    43 ms    42 ms    42 ms  lw-dc3-storm1.rtr.liquidweb.com [69.167.128.89]
 12    44 ms    43 ms    43 ms  www.dslreports.com [64.91.255.98]
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 basic ways information is conveyed over the internet; TCP (transmission control protocol) and UDP (user datagram protocol). TCP creates a session where the 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 deal with the missing data as best it can.

2.7 *QoS (Quality of Service)*

The 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 latency should be under 150ms. Excessive delay makes carrying on a conversation difficult and with extreme delay virtually impossible. Streaming media is less sensitive to latency as long as the average data rate exceeds playback rate. When a stream is 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 upload speed since most residential internet connections are highly asymmetric and often much slower than a LAN. Download speed is many times that of upload. When a switch or router encounters congestion it buffers incoming packets until it is able to forward them. QoS (Quality of Service) 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 the transmitter sends per unit of time. TCP RWIN (receive window) parameter determines how many unacknowledged packets can be outstanding before the transmitter must stop transmitting and waits for an acknowledgement.

2.9 *IP Address Configuration*

Each IP device (host) must have an address. Addresses may be assigned: manually, automatically by a DHCP (dynamic host configuration protocol) server or by the client itself using APIPA (automatic private IP addressing). 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. IPV6 adds several additional ways to automatically configure hosts.

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. CIDR (classless inter-domain routing) and NAT (network address translation) are two techniques used to delay the day of reckoning. IPv6 expands the address space to a mind boggling 128 bits. 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 CIDR (Classless Inter-Domain Routing)

When internet was initially developed the 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 wastefully large. 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. There has been an effort to reduce this size of this block to help alleviate the IPv4 address shortage however concern is that much software assumes the entire /8 is dedicated for loopback.

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 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 the host assigns itself an address 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 APIPA a 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 customers are typically assigned a single IP address. This limits customer to connecting a single computer to the internet. NAT (network address translation) is used to convert multiple private LAN IP addresses to/from the single 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 single IP address. NAT is one of the services built into residential routers.

2.9.9 CGNAT (Carrier Grade NAT)

Normally the ISP hands out one or more public IPV4 address to each customer. This allows the customer to connect to any other IPv4 address on the internet and conversely allows the customer to run a server accessible to anyone on the internet. Due to the extreme shortage of IPv4 addresses some ISPs do not have enough IP addresses to provide each customer with their own address so the notion of CGNAT was born as a workaround. CGNAT works much the same as NAT (network address translation) on a person's home network. For outgoing connections CGNAT is largely transparent but it prevents customer from hosting their own servers because multiple customers share a single public IPv4 address.

2.9.10 Ports

An 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 the connection is established high numbered ports are used during the transfer. For example: when you enter a URL to access a web site the browser automatically uses port 80. This is the well know port for web servers. Once the connection is established client and server agree on high numbered 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 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 but it is painfully small today.

To put 4 billion into perspective present human population is about 8 billion people. It is true that not everyone has internet access but many do and those who have access often have multiple connected devices. Interesting statistic: there are already more cell phones than humans on the planet. In our home at any given time there are dozens of 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 backward compatible with IPv4 adoption has been painfully 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 offers no advantage.

3 ISP – The World at Your Fingertips

The role of an ISP is to allow users to access the internet. Wired ISP's require some type of device to convert the ISP's physical medium (copper pair, coaxial or fiber optic cable) to Ethernet for use by the customer. Wireless ISPs require radios that operate at certain frequencies assigned to the ISP. People are probably most familiar with the cellular telephone network but fixed wireless is also available, typically in rural areas where the cost of deploying a physical connection to each customer is not cost effective.

It is common to call the customer connection the last-mile, implying internet goodness occurs somewhere else and customers are simply information consumers. I prefer the term first-mile to denote the transparent end-to-end nature of the internet.

3.1 *Fiber Optic Connectivity*

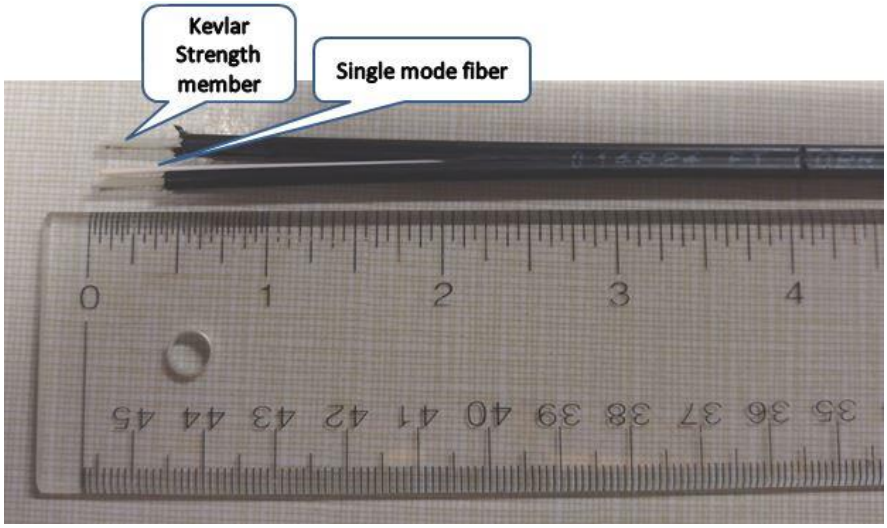


Figure 2 PON Drop Cable

Our internet access is PON (passive optical network) fiber provided by Consolidated Communication using the Fidium brand. We are about 600 feet off the road with a combination of 400 aerial and 200 feet underground in conduit. During the install the tech measured the distance from our house to the fiber terminal on the road and came up with a measure of 1,000 feet. He had a 900 and 1100 foot spool in his truck. The fiber is preterminated so he used the 1100 spool and coiled up the excess at the transition from aerial to underground. Installation was surprising fast: installing the fiber, getting internet up and running and transferring our landline phone.

An advantage of PON is it does not require active electronics in the field. Customer drops are a single optical fiber run to a passive optical splitter. Traffic from multiple customers is carried over a single fiber from the splitter to/from the central office. Typical split ratio is 32 customers but ultimately engineering determines optimum split. Fiber is much less distance sensitive then copper allowing long runs up to 20 Km, and even longer in some circumstances. The ONT (optical network terminal) at the customer location coverts the fiber to Gig UTP Ethernet and optionally analog telephone while restricting access to only the specific customer's data. Our ONT is GPON 2.488 Gbps toward the customer and 1.244 up both over a single fiber using different "colors" (optical wavelengths).

We also took advantage of FCC telephone number portability to switch our landline phone service from the DSL CLEC to Consolidated. This is implemented as VoIP handled entirely within the ONT. As far as the customer is concerned it is just a regular RJ11 analog phone interface. A down side of fiber is if the ONT loses power internet and telephone service is lost. This is an important consideration during emergencies. On the plus side PON does not require power in the field so as long as the customer and central office have some form of backup power communication remains active.

3.2 *Web Based Fidium Account Management*

Fidium has a web site to manage the account and make payment. Like many companies they offer discount for paperless billing and electronic payment. Since we also subscribe to landline phone there is a section to manage phone options. They offer a 1-year reduced teaser rate and discount for paperless billing and autopay.

Fidium has a line item for router and fiber maintenance of $10US per month. Since I'm using my own router the charge for that line item is zeroed out.

3.3 *IP Settings*

Once the ONT is able to successfully transport data 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 network device requires an IP address and a subnet mask that signifies the network and host portions 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 local to the LAN. Lastly devices need the address of a DNS server to translate URL name to the IP address of the distant server.

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 the customer in turn manually configures equipment. Changes require manual intervention by the ISP and customer.

Residential accounts typically use DHCP or PPPoE. DHCP works much the same as having a PC connected to a LAN. PPPoE (point-to-point protocol over Ethernet) works much the same as with dialup only much faster. PPPoE requires the use of a customer user name and password. PPPoE has slightly higher overhead then DHCP and is session based.

Fidium uses DHCP so customer device works just like connecting a computer to a LAN. Fidium binds the customer account to the MAC address of the connected device. So if you change your router will either need to contact Fidium to have them update the MAC address or use the clone WAN MAC address feature built into many routers to change the router's MAC address to that of the old one.

3.3.1 PPPoE and MTU

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

Overly large packets can be fragmented and reassembled however this adds a lot of overhead and is not allowed with IPv6. 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 MTU discovery to automatically limit packet size so fragmentation is not needed. When PPPoE is used MTU (maximum transmission unit) 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 DSL 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. So far in the few months we have had Consolidated fiber have not had any problems with PPPoE.

3.3.2 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.

3.4 *Cell Phone Connectivity*

Cell carriers are moving to an IP centric network. Much like wired ISPs in modern cellular networks all traffic is carrier via IP. The phone connects to a local cell tower and as with a wired ISP customer IP settings are automatically configured. However since cell phone is moving an additional level of complexity is the seamless handoff from one cell tower to another.

Our current Cell phone service is provided by a MVNO (Mobile Virtual Network Operator) Boost Mobile. Here in terrain challenged NH cell site signal can be spotty so convenient they support WiFi calling built into Android phones.

3.5 *Web Based Boost Mobile Account Management*

Like wired ISP Boost has a web portal to pay bills, look at current phone usage stats and make changes to service plans.

3.6 *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.

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 DSL use PPPoE to transport 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 also use IP over ATM (asynchronous transfer mode) (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%

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.

Fidium fiber provided by Consolidated uses DHCP and overprovisions network so speed test results reports the marketing speed minimizing customer confusion. File transfer speed reported by Speedtest.net for our 100/100 Mbps PON is shown below.

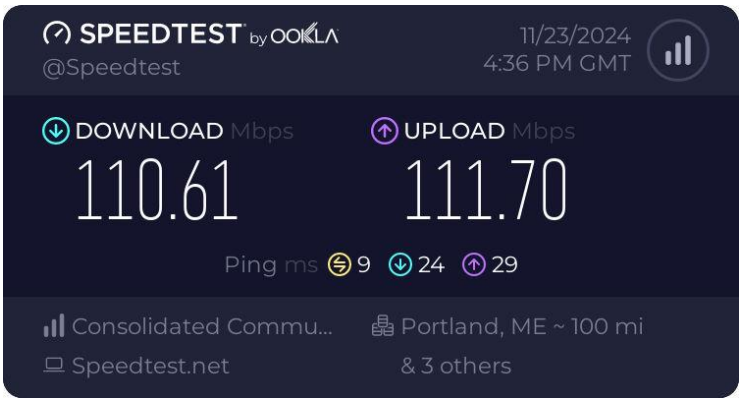


Figure 3 Speed Test Results

4 Broadband Router – One Connection Many Computers

In order to share a residential ISP internet connection a router is needed to manage the LAN and transfer data between the LAN and ISP Network. Residential ISP accounts are typically limited to a single IP address so in order to connect multiple devices a router with NAT is required. Consumer routers provide numerous network services in one convenient box: DHCP (issues IP addresses to LAN devices), NAT (Shares single ISP address among multiple LAN devices), firewall and logging capability. Often residential routers include WiFi allowing the option of using wired or wireless connection. I replaced the Consolidated provided router with a Netgear RAX 10 to maximize configuration flexibility.

Figure 4 Netgear AX 1800 RAX10 Dual band WiFi 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 addresses can be manually configured by the user or automatically by the router. There are two addresses used on the LAN. The MAC address is hard coded into the Ethernet or WiFi interface and the IP address is used for upper level communication.

4.1.1 MAC (Media Access Controller) Address

Each Ethernet device (wired or wireless) has a unique 48-bit MAC address built into hardware. This allows the device to be uniquely addressed. This address is different than 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 and purchase 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.

4.1.2 ARP and Reverse ARP

ARP (address resolution protocol) is used to discover which MAC address is associated with a specific IP address. Reverse ARP is used to determine the IP address assigned to a specific MAC address.

4.1.3 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 NAT (network address translation) a virtually unlimited number of computers are able to share a single ISP IP address. Being private the address pool can be used and reused multiple times conserving scarce IPv4 Addresses and eliminates the need to pay for multiple public addresses.

The IP address is bound to the physical MAC address. This allows higher level protocols to utilize the IP address while lower level networking uses the MAC address.

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

4.1.4 Static Configuration

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 addresses 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 not a computer configured statically may use the same address as another computer configured via DHCP. This results in an address collision which will prevent both devices from communicating.

Our router's LAN base address is 192.168.2.1. I configured the DHCP server pool to issue a maximum of 32 addresses beginning with 192.168.2.2 with a subnet mask of 255.255.255.0. Static addresses are assigned beginning at 192.168.2.100 and up with the same subnet mask. This keeps all addresses within the subnet without interfering with each other.

In most operating systems the default is automatic network address configuration. This can be changed to a static manual configuration if desired. In Windows DNS may be set statically even if the IP address is configured dynamically. This can be a handy troubleshooting tool when debugging DNS issues.

4.1.5 DHCP (Dynamic Host Configuration Protocol)

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 for a fixed period of time. 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 an period of time the lease will expire. Next time the computer connects it may receive different IP address. This behavior depends on whether or not the DHCP server remembers which MAC addresses have been seen recently.

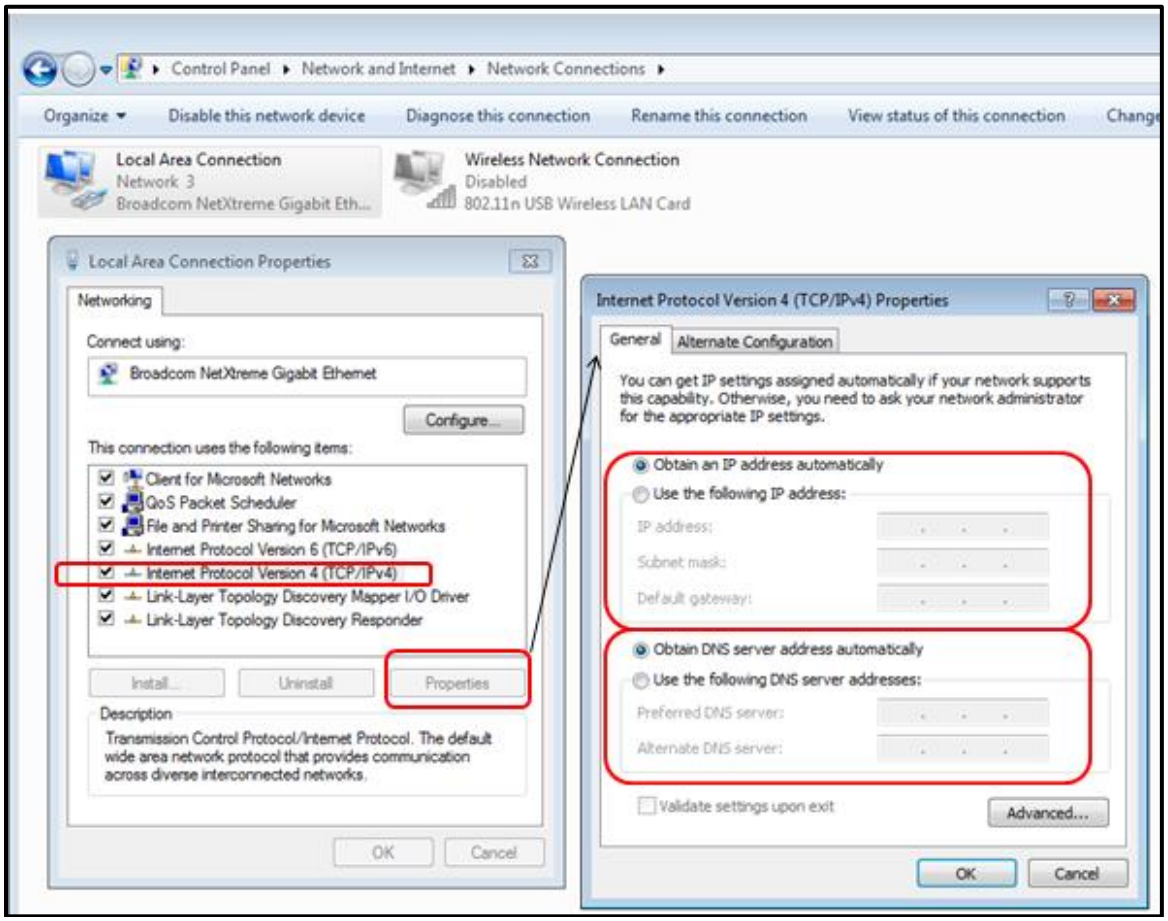


Figure 5 Windows IP Configuration

4.1.6 DHCP MAC Reservation

For some devices, such as servers, dynamic addressing is inconvenient. There are two ways to maintain a persistent IP address. We have already discussed static assignment, another technique is MAC reservation. The specifics vary by router but what you are doing is using the DHCP server to bind the device IP address to its 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 replace the router LAN addresses will be once again be randomly assigned. For our LAN I statically assign the address for "servers" and home automation gear. I let the router dynamically assign addresses to "client" devices such as: PCs, laptops, and cell phones. To work around a Win 10 bug on our home server I use MAC reservation so it always gets the same IP address.

4.2 NAT (Network Address Translation)

Most residential ISPs restrict customer to a single IP address. The limited 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 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. The 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 the 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 fast broadband connection say 100 Mbps or faster make sure the router is up to the task.

NAT translation table size limits the maximum number of simultaneous sessions a 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 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.

4.2.4 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. However if a device 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. The ISP router in turn determines how best to forward the packet.

4.4 *DNS (Domain Name System)*

The DNS (domain name system) 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. Currently I'm using the DNS server provided by our ISP.

There is a downside of using a different DNS server. Many larger ISPs have special arrangements with CDN (content delivery network) 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 UPNP (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 (*Quality of Service*)

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*

I had been using the free version of the Kiwi Syslog server to store and display router and time server stats. The new router has fairly large storage capacity so it is more convenient to simply access the router logs.

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 Message Protocol)

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 (simple network management protocol) 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 a MIB (management information base) 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 the device will only responds to authorized queries. 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 the address changes the Dynamic DNS service is notified. 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 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.

5 WiFi – 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. WiFi radios operate in the unlicensed Industrial Scientific Medical (ISM) band. WiFi 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 WiFi devices to communicate directly without needing an Access Point. Most WiFi communication makes use of Access Points.

Many residential routers, such as ours, include a WiFi Access Point. The optimum location for good WiFi is typically high in the residence. Since WiFi is built into our broadband router that means locating the router in an upstairs utility closet. This makes physical access difficult but anything we need to do can be done remotely.

5.1 *IEEE 802.11 vs WiFi*

There is some confusion as to these two entities. The Institute of Electrical and Electronic Engineers (IEEE) develops multiple standards. The two most relevant for this paper are 802.3 Ethernet and 802.11 Wireless LAN. Interested parties submit a PAR (project authorization request) if approved the activity is assigned a project code. The first Wireless LAN was denoted as 802.11, the second as 802.11a and so forth. When the end of the alphabet is reach the sequence restarts with a two letter code aa, then ab, ac etc. This works well internally for project tracking but as a marketing name leaves much to be desired.

The success of various IEEE 802.11 wireless standards has encouraged many vendors to enter the market. The WiFi Alliance works to insure interoperability between different vendors and promote use of Wireless LANs. The result is that wireless IEEE 802.11 networks are often referred to as WiFi. Recently the alliance has begun branding various version of the wireless specification with a single increasing number. This is less confusing for the average consumer then multiple noncontiguous letter designations.

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	WiFi 4	802.11n (2009)
• 500 Mbps	5 GHz	WiFi 5	802.11ac (2013)
• 10 Gbps	2.4/5/6 GHz	WiFi 6	802.11ax (2019)
• 46 Gbps	2.4/5/6 GHz	WiFi 7	803.11be (2024)

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 WiFi alliance developed WPA that could be retrofit to existing hardware. IEEE developed a comprehensive security standard WiFi 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 2016 security researchers found a weakness in WPA2 nicknamed: KRACK (Key Reinstallation Attack). There are some software patches that reduce the severity of this attack. The WiFi Alliance has announced a new encryption protocol WPA3.

In a commercial setting WPA2 if often used with RADIUS (remote authentication dial-in user service) to uniquely identify each user. That is typically not an option for home users. A simpler method uses a PSK (preshared key). With PSK the Access Point and each client have a secret password installed for mutual authentication. WPA3 implements SAE (Simultaneous Authentication of Equals) that is more robust then the preshared key mechanism used with WPA2.

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 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 *WPS (WiFi Protected Setup)*

WPS was designed to make it easier for home users to configure multiple WiFi devices using a preshared key. Creating a long key and configuring WiFi 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 WiFi 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 *SSID (Service Set Identifier)*

Under normal conditions each AP will broadcast its name, called the SSID. This broadcast is what is used to display available networks on your computer or phone. The client in turn selects one of the available networks and uses its SSID to request it be associated with that network. It is possible to turn off SSID broadcast and some folks argue it improves security however that is not true. If SSID broadcast is disabled the SSID must be added to the client

manually to allow it to connect. The client in turn has to broadcast the SSID in effect asking - hey is there an Access Point nearby with this name? All an attacker needs to do is wait for someone to connect in order to learn the SSID of the Access Point.

5.6 *Multiple APs (Access Points)*

If a single AP does not cover the intended location you can install multiple AP and set them to the same SSID. As the client moves around it will track the signal strength of the various Aps and automatically switch to the strongest.

5.7 *Interference*

WiFi 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 WiFi radios, non-WiFi radios operating in the same band such as Bluetooth or wireless phones and unintentional radiators such as microwave ovens. WiFi operates in three bands 2.4GHz and 5GHz are the most common 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 WiFi uses a much wider channel so there are only three non-overlapping WiFi channels. In general when operating at 2.4 GHz it is best to use channels 1, 6, or 11 for optimum performance.

WiFi alliance has published numerous whitepapers on the subject. They are working with various standards bodies to make devices more aware of their RF environment by probing for other radios operating in the vicinity. 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.

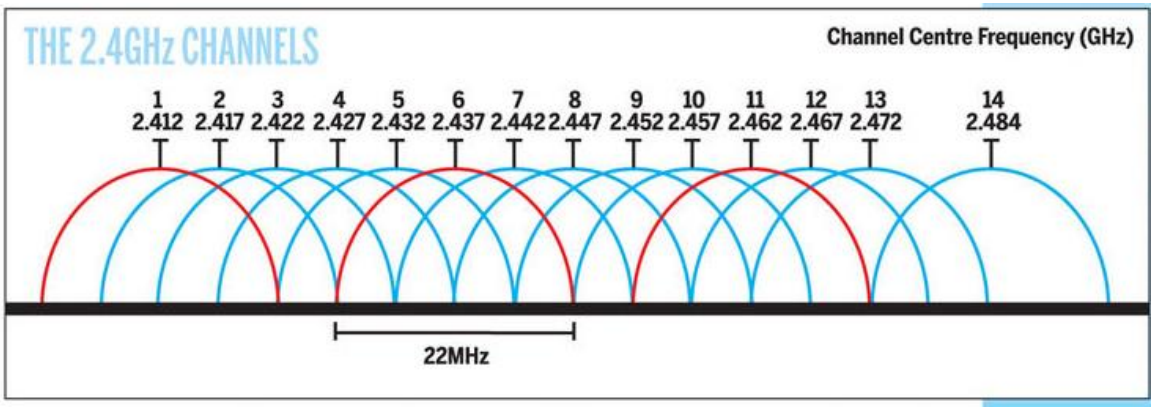


Figure 6 2.4GHz WiFi Channels

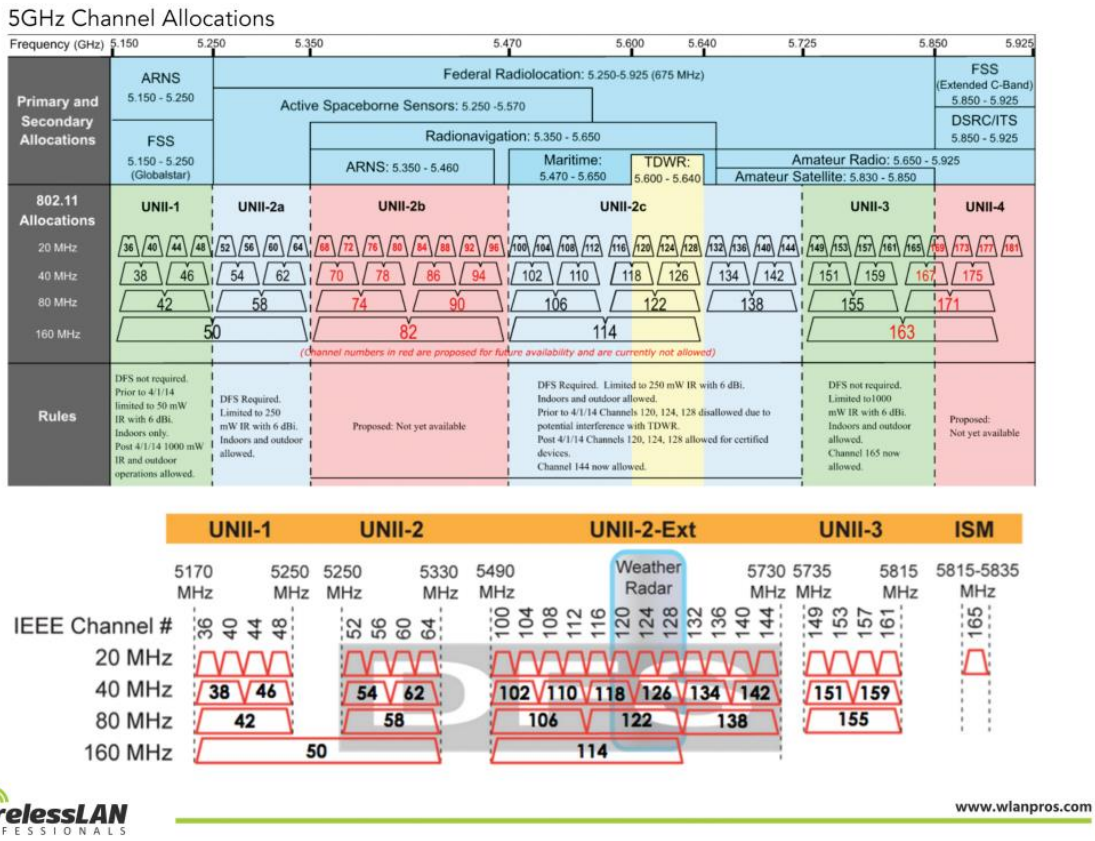


Figure 7 5GHz WiFi Channels

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 connection. Having a LAN allows computers to access shared resources such as a printer and files. Local resources remain accessible even if you lose internet access. WiFi and Unshielded Twisted Pair (UTP) Ethernet dominate the SOHO market.

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

> **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 1Gbps Ethernet switch has a maximum throughput of 16Gbps. This assumes connections are evenly used among the 16 ports each one operating at 1Gbps. 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 rather than between devices on the LAN. In that case the internet connection, normally much slower than the LAN, constrains speed. However if there are local resources such as files and printers on the LAN the Ethernet switch 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 the MAC address or addresses 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.

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 able to detect bad cables and estimate distance to the fault.

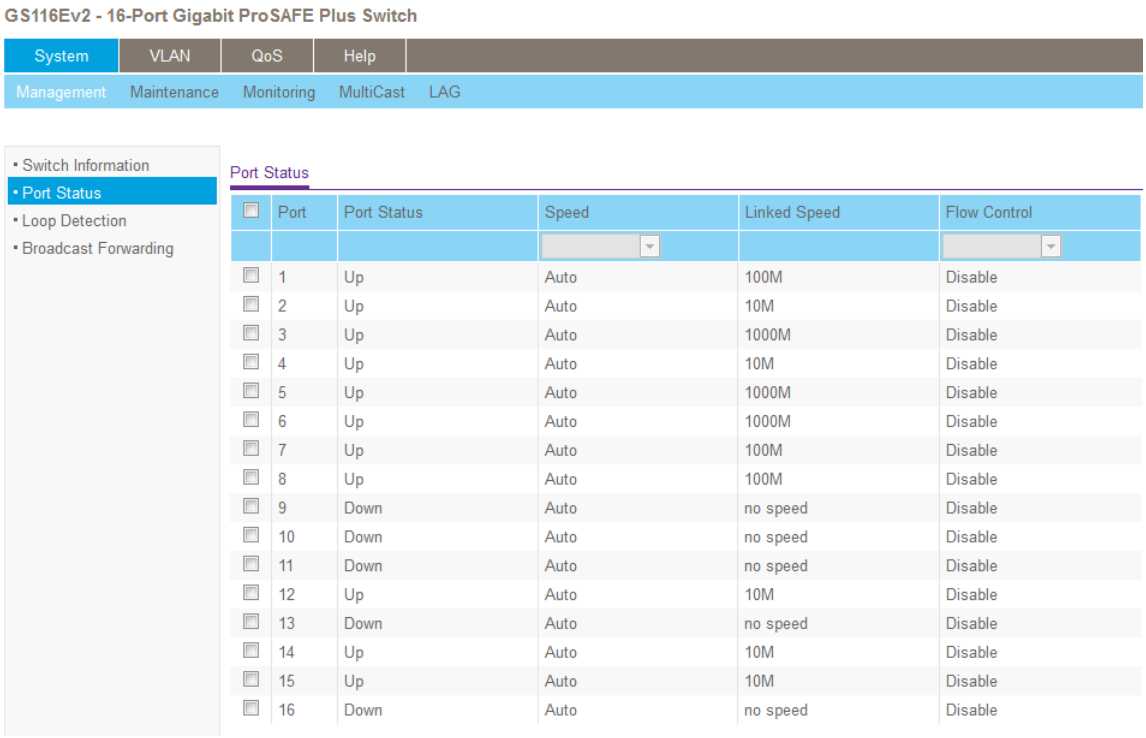
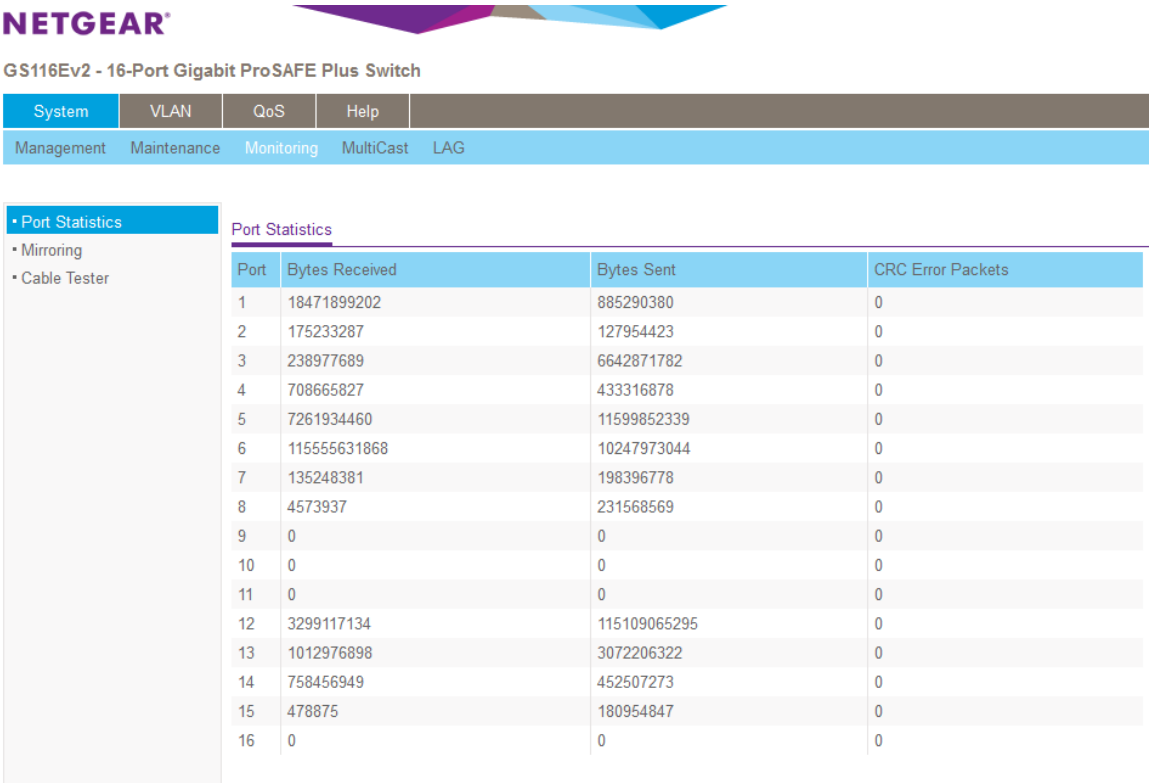


Figure 8 Ethernet Switch Port Status

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 9 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 even at 1 Gbps. 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.

Ethernet and Fast Ethernet 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. One pair of the cable is used for transmit the other for receive. 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. Gig UTP Ethernet and faster uses all four pairs simultaneously for transmit and receive.

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 *PoE (Power over Ethernet)*

Until recently Ethernet delivered data but not power. Each device had 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 WiFi Access Points and Voice over IP (VoIP) telephones and IoT (internet of things) are deployed the benefit of delivering both data and power over Ethernet cabling became obvious.

IEEE took on the challenge and in 2003 released the 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. Third generation 4PPoE increased power to 51 watts and most recently Type 4 to 71 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 *UTP (Unshielded Twisted Pair)*

Ethernet IEEE 802.3 using UTP (unshielded twisted pair) copper cable is by far the most common LAN technology in use today in the US. In Europe (STP) shielded twisted pair is often used but it much more difficult to terminate. 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 structured wiring speciation applies to commercial locations and EIA/TIA 570 is the variant for residential.

6.6.1 UTP Ethernet Speed

Since its inception UTP speed has increased dramatically. Today data centers are using 40G Ethernet. For residential use there are new 2.5 and 5G speed version that operate over existing Cat5e and 6 cabling but by far Gig Ethernet is the most common and cost effective speed for residential use. Ethernet has become so ubiquitous special single pair is being used for industrial automation and real time Ethernet is used for time critical applications.

- 10 Mbps Cat 3 10Base-T (1990)
- 100 Mbps Cat 5 100Base-TX (1995)
- 1,000 Mbps Cat 5e 1000Base-T (1999)
- 2,500 Mbps Cat 5e 2.5GBase-T (2016)
- 5,000 Mbps Cat 6 5GBase-T (2016)
- 10,000 Mbps Cat 6A 10GBase-T (2006) (Cat 6 up to 55 meters)

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 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 VLAN (*Virtual* LAN)

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 WiFi are the dominant LAN technologies. The cost of installing network wiring is modest if done when the structure is being built. The situation is more difficult for existing structures. 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 all these alternatives use modified Ethernet frames, adapted to the physical medium, making it easy to bridge to standard Ethernet equipment.

7.1 *PAN (Personal Area Network)*

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 WiFi do not degrade one another. While Bluetooth can be used to create a network, it is more commonly used to attach peripherals wirelessly.

7.2 *MoCA (Multimedia over Coax Alliance)*

MoCA is popularizing an interesting technology that utilizes TV coax wiring to deliver Ethernet at up to 2.5 Gbps. A competing ITU-T standard G.hn is getting international traction and hits the2 Gbps speed 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.

7.3 *Home PNA (Phone Line Network)*

Home Phone line Network 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.

7.4 *Ethernet Range Extenders*

HomePNA never 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 VDSL2 chipsets allowing point to point Ethernet connections over several thousand feet. I used a pair of StarTech VDSL2 Ethernet range extenders to enable a friend to extend their LAN out to a barn a few hundred feet from the house.

8 Desktop PCs – Computing at Home

I had resisted migrating from Win 7 to Win 10. However in 2019 with Win 7 end of support near I decided to bite the bullet and replace or upgrade all our PCs.

8.1 *Desktop Workstation*

I purchased a couple of off-lease HP Z230 SFF computers (2014 vintage) for myself and my wife. These were originally Win 7 boxes but the refurbishing service upgraded them to Win 10 Pro. Over the years we have been happy purchasing off-lease commercial computers.

I'm not a fan of the Win 10 touch pad interface so installed Open Shell to deliver a Win 7 type interface.

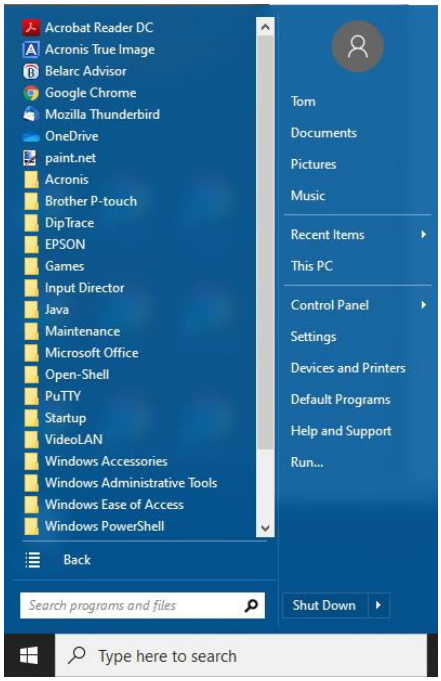


Figure 10 Open Shell Start Menu

Win 10 is working well enough, but then I had no problem with Win 7 and only switched because security updates ended in 2020. One annoying thing I've noticed is it now takes many more Mouse clicks to do semi low level stuff.

I turned off as much of the Windows 10 telemetry tracking as possible.

8.2 *Dual Boot Test Computer*

In addition to a regular Windows 10 desktop machine I maintain a dual boot PC: Windows 7 and Ubuntu for software testing. I reinstalled Win 7 on an old HP DC7900 SFF (2008 vintage) PC. Once I had that running and up to date installed Ubuntu in a dual boot configuration. I am currently running the latest and greatest Ubuntu LTS version 24.04.

8.3 *Windows 10 end of support*

Microsoft has announced Windows 10 end of support as on October 14th 2025. They have been aggressively pushing folks to migrate to Windows 11 however they have set hardware requirement very high so many computers able to run Win 10 do not qualify. None of our desktop or laptop PCs meets the new hardware requirements and even if they did Win 11 does not offer any advantage for us.

Not sure what we will do when the time comes but a third-party security patching company 0patch looks interesting and we are thinking about giving it a try when Microsoft support ends.

9 Laptop – Mobile Computing

My laptop is another off lease computer, a Lenovo ThinkPad T520 (2011 vintage) I purchased several years ago running Win 7 Pro. Since the desktops are all running Win 10 I decided to upgrade my laptop. I had resisted the MS free upgrade but now that Win 7 has reached end of life Microsoft will no longer be fixing security bugs.

9.1 *Laptop Upgrade to Win 10*

I purchased a 240GB SSD and cloned the old drive. That way if the upgrade failed I had a backup, swapped the drives – so far so good. I ran across several YouTube videos indicating even though the Microsoft Win 10 free upgrade offer was long gone it will still possible to upgrade. Note: this was back in 2019; this is no longer an option AFAIK.

I downloaded Win 10 from the Microsoft site. You have to option to do an in situ upgrade or create boot media. Since I had just cloned the hard drive I chose in situ. At the time we had a relatively slow DSL connection (6.5 Mbps) but everything went fine, took a few reboots but as far as I can tell did not lose anything.

For convenience I always purchase a second laptop 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.

My wife was using my ancient T61 ThinkPad so during the upgrade process picked up an upgraded T520 ThinkPad for her. This has worked out well during the COVID pandemic allowing us to each conduct remote Zoom meetings. Both are running Win 10 pro.

9.2 *Remote Control/Laser Pointer*

For presentations I use a Logitech R400. Great remote control and has a built in laser pointer. However it is time to get another as the plastic has degraded and become sticky that cannot be cleaned off.

9.3 *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.

WiFi hotspots normally do not provide over the air security like WPA2. This means non-encrypted traffic is easy to eavesdrop. However even if they do you have no way to determine if you are susceptible to a man in the middle attack.

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.

10 Local Server – IT Just Like the Big Kids

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

We use a server for the following services:

1) Windows peer to peer files sharing
2) Destination for automatic PC backup
3) NTP clock synchronization
4) Private web server
5) Web based access to home IoT devices

10.1 *Server PC*

I bought an off lease ThinkPad T420 laptop upgraded to Win 10 Pro on eBay. First thing I did was clone the HDD to an SSD to replace the rotating media. I ordered a drive adapter to use a 2TB 2.5" hard drive in the DVD slot as a data drive. I've been working with computers for decades and the ability to have 2TB in such a small form factor blows me away. I copied the data from the old server and enabled sharing of specific directories.

As with the other Win 10 systems I turned off as many of the tracking options as possible and used Open-Shell to replace the tablet style start menu with a Win 7 look alike.

10.1.1 Power Consumption

In the past when I've upgraded our desktop PCs would recycle one as a poor man's server. The downside of using a desktop as a server is it draws about 80 watts. I've been happy with the various ThinkPad's I've owned over the years so decided to use a laptop as the server. This reduced AC power consumption to about 20 watts.

New Hampshire has relatively expensive electrical power about $0.22 per kWh (2024). An 80 watt load running 24/7 consumes about 2 kWh per day or 57.6 kWh a month. At $0.22 a kWh the server costs $12.67 a month, using a laptop reduced cost to $3.16 per month.

10.2 *Virtual Input Devices*

I found a nifty utility called Input Director that enables keyboard and mouse sharing. You configure Input Director to specify where, relative to your main display, the slave device resides. I only have one slave located to the left of the main LCD. Moving the mouse to the left side of the screen switches peripheral input control to the laptop. I find this much more convenient than using the KVM. Being a laptop when the screen is blanked wakeup is virtually instantaneous.

The only downside I've noticed is making sure the mouse is back on the main screen if you reboot the slave device. If not during the boot process you lose the ability to control the main computer until it finishes.

10.3 *Peer to Peer Network Discovery*

Prior to Win 10 Microsoft used an election process to select the master browser. The master browser collects information about machines on the LAN. PCs on the LAN hold an election

process to select which machine will be the master browser. If that machine is shut down the lack of a master browser is detected and anther election is held. This software was built on SMBv1 (server message block) which has security vulnerabilities. SMVv1 has been depreciated and the master browser has been replaced with WS-Discovery.

10.4 *Win 10 File Sharing Problems*

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 sharing is configured users are able to browse network shares, as easily as if they were physically on the local machine. Commonly used shares can be mapped as a virtual drive providing seamless integration.

We mainly use server shares for automated backup. Software running on each 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.

I had a terrible time getting file sharing to work reliability with Win 10. Randomly share discovery would fail. If I typed the server's address into network in File Explorer shares were not visible. Regardless of whether or not shares were accessible media files were always visible, so network discovery was working. Tried all the tips I ran across on the internet to no avail.

A workaround I discovered is to do a Network Reset on the server after each MS upgrade. That fixes the sharing problem but also resets the server network stack to DHCP so the address of the server may change. Initially I configured the server back to static IP addresses after the network reset but that was pretty inconvenient. My solution was to configure MAC reservation in the router for the server. That way when I reset the server network stack to fix the sharing problem, it obtains the same dynamic IP address from the router. This works but I find it frustrating that Microsoft broke something as basic as peer-to-peer file sharing that had been working just fine in previous versions of the OS.

10.5 *Desktop 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. Offline backup is covered in more detail later.

10.6 *Internet Time Service*

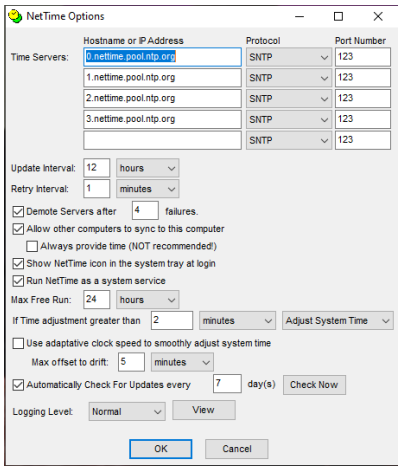


Figure 11 NetTime Config Page

NIST the US National Institute of Standards and Technology 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.

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 a local server, and have it in turn synchronize local devices. We use NetTime running on the server and point each non-mobile device to it. This way we are only making a single access to the NTP internet pool and even if we lose internet connectivity devices remain synchronized to one another, abet 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 date/time if they cannot access NTP server. 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 access from each device.

10.7 *Private Web Server*

The browser home page of each desktop PC points to the 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. So far the web interface consists of static data but on my TO-DO list is to present some of the home automation data using pretty graphs.

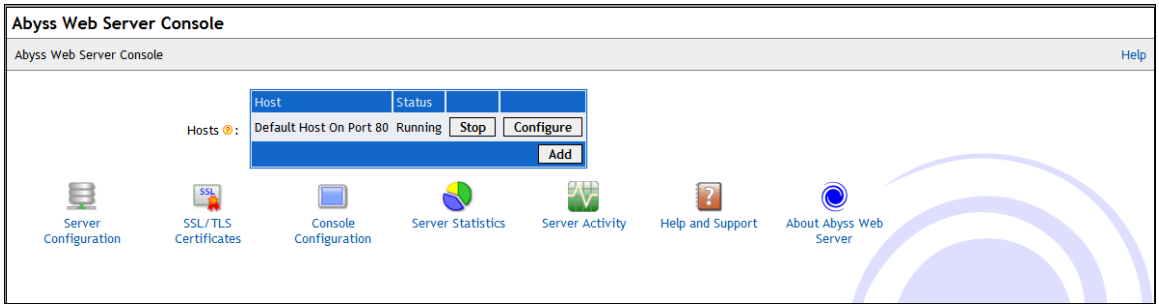


Figure 12 Abyss Server Console

11 Telephony – Reach Out and Talk to Someone

11.1 *POTS (Plain Old Telephone Service)*

While POTS is ancient technology I prefer using traditional landline telephone vs a cell phone. The ONT uses the fiber ISP connection for both internet and phone. Telephony is supported via VoIP and the ONT emulates the analog phone interface so it is a simple matter to connect existing landline phones to the ONT. The only down side is the ONT needs power for the phone to work, unlike traditional copper landline service where the phone company central office supplied power.

11.1.1 ONT REN Limitation

The ONT we use has a REN (ringer equivalency number) of 3. This limits how many telephone ringers is it able to support. The REN should be listed on each phone. If the total REN exceeds the capability of the ONT you will need to turn off some of the ringers.

11.1.2 ONT Battery Backup

One of the downsides of fiber is the customer must provide local power to remain active. Fidium provides options to use a battery power pack to maintain telephone voice service during a power outage. I opted to use a DIY UPS to keep the entire LAN alive during an outage described later in this paper.

11.1.3 Web Based Landline Feature Management

Consolidated/Fidium has an online page to manage telephone features. We have our own answering machine; it is easier pressing a button on the machine to retrieve messages than dialing into the online VM system so I disabled that feature. The other feature I disabled was Call Waiting; if the phone is busy the person can call back later rather than interrupt an ongoing conversation.

11.2 *Cell Phone*

We had been using Republic Wireless a MVNO (mobile virtual network operator) they made a name for themselves by being a WiFi first provider. Initially by customizing Android firmware and later running an app on Android phones. When the phone is connected to WiFi all traffic: voice, text and internet are transported over WiFi eliminating cellular network coverage issues and possible usage charges. This was a great feature here in terrain challenged NH where cell phone service can be spotty.

They were acquired and now we are serviced by Boost Mobile. The Republic app was discontinued and we lost access to WiFi calling. We recently purchased Motorola G 5G (2024) phones that support WiFi calling built into the Android O/S. Not sure about other OEMs but Moto has a convenient way to transfer everything from the old phone to new using USB on-the-go. . When not connected to WiFi the phone uses the (T-Mobile) 4G-LTE/5G network and roams to Verizon if out of range. Voice and text is unlimited regardless of how the phone connects. As someone who has been in the computer biz for decades is it amazing how much functionally can be crammed into such a small package.

11.2.1 Emergency Cell Phones Use

During a power outage each Cell site needs to provide emergency power. So depending on the situation you may lose the ability to make or receive calls. One of the advantages of PON

(passive optical network) is it does not require outside plant power. As long as the fiber is not damaged and the customer and Central Office have power the system should be functional.

11.2.2 5G Hype and Reality

The next generation of cell phone technology called 5G is following other communication networks in fully embracing the internet and carrying all services as packet switched data. This is a positive development as it makes the most of over the air RF capacity. The other much ballyhooed feature is a massive increase in data capacity. This is mainly limited to millimeter wave bands, that while delivering eye popping bandwidth have very short range and do not penetrate buildings very well. 5G does offer improvements when used on the lower bands and being IP centric blurs the distinction between: voice, data and text.

11.2.3 Charging and Battery Life

Battery life of these spiffy new smart phones is significantly better than earlier phones; it is easy to go all day on a charge. 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 phone charger in my laptop bag for travel. In the car we use a USB car adapter to keep the phone charged while driving. The cigarette lighter (accessory) socket is turned off when the car is not running but that is not a problem as we don't leave the phones in the car when we are not there. When camping needing to run the car's engine to activate the socket is be a problem as the phones need to be charged every day or so 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's battery to recharge the phones. We also carry a rechargeable USB power pack that provides several days of phone power.

11.2.4 USB Car Charger Issues

Initially I tried purchasing USB cigarette lighter chargers on eBay. I loaded tested the chargers and they failed miserably. None of them delivered the rated current and worse became very hot so I gave up on no-name Chinese charger and purchased a bunch of Anker chargers for myself and family. The USB cable also figures into this. Having a phone with a high current requirement plugged into a small gauge USB cable will substantially increase charge time.

12 Miscellaneous Devices

12.1 *E-readers and Tablets – Nontraditional Computing Devices*

These devices are becoming more common. Be ing wireless they place additional demands on WiFi.

12.2 *TV Streaming – TV on the Interwebs*

There are many ways to distribute Radio and Television programs. OTT (internet over the top) delivery opens up fascinating opportunities for new sources not constrained by distance or even a local presence. It is interesting Consolidated is not delivering transitional "Cable TV" over its fiber network. Instead they have chosen to partner with several OTT providers. We use a Roku Express media player. It worked fine on DSL but much better new that we have a faster internet connection.

12.2.1 LAN Based TV Distribution

It is possible to implement a TV server and then distribute programs over your LAN. The Silicon Dust HDHomeRun is probably the best known system. We are OTA (over the air) TV viewers and waiting for the dust to settle on the rollout of ATSC 3.0. This is an enhanced version of digital TV but is not backward compatible with the current standard ATSC 1.0. This means TVs need to implement both ATSC 1.0 and ATSC 3.0 tuners. In addition the ATSC 3.0 spec provides internet integration so lots of complex software on the part of the receiver. The rollout and customer acceptance of ATSC 3.0 has been slowed due to broadcasters implementing DRM (digital rights management) encryption.

Titan TV is a popular on line TV program guide. You select your location of if you are using over the air or subscribe to cable.

12.3 *Printing – Turn Data into Dead Tree Sheets*

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.

12.3.1 Document Printing

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

12.3.2 Label Printing

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

12.4 *Document Scanning – Turn Dead Tree Sheets into Data*

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. We are currently using an Epson V550 Photo scanner. It also functions as a poor man's copying machine allowing scanned images to be directly printed.

13 KVM Switch – Sharing Peripherals among Multiple Computers

Figure 13 KVM

My office has a main workstation, test PC running Win 7 and Ubuntu and ability to temporally connect another computer for configuration and test purposes. I did not want to use dedicated I/O for each computer. 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; it doesn'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 is the Win7/Ubuntu test computer, Port 3 is not used and port 4 is 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 keyboard hot-keys. 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. 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.

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 to preserve high frequency and minimizes color crosstalk.

Mouse Compatibility Tip -- 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.

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.

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.

14 Backup Power – Computing When the Lights Go Out

Several years ago I set up a portable generator to supply power in the event of a utility outage. These occur every few years here in NH due to massive ice or snow storms. These tend to be statewide outages and we can be without power for a week or more. Our goal is to use the generator a few hours in the morning and again in the evening. This intermittent use means we lose internet and phone service when the generator is off.

Figure 14 DIY DC UPS

The fiber ONT needs to be powered for the internet and landline telephones to work and router for WiFi. We are in a dead spot here in terrain challenged NH so having our cell phones use WiFi is great. I also wanted to keep the main Ethernet switch powered. That way we are able to access our poor man's server because it is a laptop with its own battery.

All of our network devices are powered by small DC wall warts. It seemed ridiculous to convert UPS battery power to AC then back to DC to power the devices. So I built a simple DC UPS that replaces the wall warts and powers critical network gear directly from 12 volt DC.

An important consideration is rapid battery recharge time and long run time since the generator will only be operated for short periods of time each day. The UPS includes a 5A battery charger. This is pretty much the maxim charge rate for a small SLA battery. A novel feature of my design is rather than building the battery into the UPS I used a car jump pack. That gives us the best of both worlds. The UPS gets a "free" battery and the jump pack is kept fully charged by the battery maintainer in the UPS.

I've posted details on my site: DC UPS.

15 Widgets & Services – Making Life worth Living

15.1 WWW (*World Wide Web*)

Having multiple browsers is a useful troubleshooting tool. I use a combination of Firefox and Chrome. The dual boot PC runs Firefox on Win 7 and Ubuntu.

Due to the obnoxious over use of web site ads I use the Adblock Plus ad blocker.

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

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

Browsers	Grabber	Pages	Percent	Hits	Percent
Google Chrome	No	581	63.2 %	2,749	62.9 %
Safari	No	115	12.5 %	982	22.4 %
Unknown	?	106	11.5 %	153	3.5 %
Firefox	No	81	8.8 %	349	7.9 %
Opera	No	18	1.9 %	89	2 %
Mozilla	No	15	1.6 %	22	0.5 %
Netscape	No	2	0.2 %	3	0 %
IPhone (PDA/Phone browser)	No	1	0.1 %	1	0 %
Edge	No	0	0 %	1	0 %
MS Internet Explorer	No	0	0 %	17	0.3 %
Others		0	0 %	1	0 %

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

Browsers	Grabber	Pages	Percent	Hits	Percent
Google Chrome	No	1,877	73.3 %	2,244	52.7 %
Firefox	No	243	9.4 %	473	11.1 %
Unknown	?	122	4.7 %	163	3.8 %
Mozilla	No	104	4 %	1,009	23.7 %
MS Internet Explorer	No	76	2.9 %	100	2.3 %
Opera	No	69	2.6 %	86	2 %
Safari	No	62	2.4 %	175	4.1 %
Netscape	No	4	0.1 %	4	0 %
Lynx	No	1	0 %	1	0 %
Android browser (PDA/Phone browser)	No	1	0 %	1	0 %
Others		1	0 %	1	0 %

Figure 15 2021 SSL & non SSL Browser Preference

15.1.1 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. But it is disconcerting how much information Google has amassed about me by using their products. If you are worried about Google's dominance there are other search engines available.

15.2 *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. Most modern browsers will throw a security nag screen if the site you are trying to access does not support TLS.

15.3 *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. However with the proliferation of free email accounts like Gmail, some ISPs are eliminating this feature. ISP email ties your e-mail address to your current ISP. Change ISP or if the ISP gets bought out and changes their domain name your e-mail address changes. Free email services like Google Gmail and Yahoo 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 I use Gmail as an alternative email account. To eliminate the need to log into Gmail I have incoming Gmail forwarded to my domain email. My cell phone is Android based and Google wants to tie everything to your Gmail account. To improve security Google is moving to two factor authentication. This involves sending a short security code to a previously specified device, most often a text message to your cell phone.

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.

I've built multiple home automation devices and most have a web interface and the ability to send email. For example the greenhouse controller sends out a morning and evening status email, documenting the previous 12 hours. It sends 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 network problems over the years. All in all a handy side effect of these periodic emails.

15.3.1 Email Access

Traditionally email uses an email client, such as Microsoft Outlook or Thunderbird. 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 SMTP (simple mail transfer protocol) mail gateway. SMTP server acts as a relay between e-mail client and POP (post office protocol) mail server. The SMTP server verifies each recipient is accessible and returns an error message if not. SMTP server delivers mail to the appropriate POP server. It works much as a physical post office mailbox. The 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 IMAP (internet message access protocol).

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.

15.3.2 Email Client

When upgrading to Windows 10 took the opportunity to switch email client. We had been using Windows Live, I switched to Thunderbird. Migrating to Thunderbird was surprising easy. I needed to export Windows Live address book and messages. Importing the address book was pretty easy. To import messages I needed to download a third party app.

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 POP 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.

15.3.3 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 WiFi 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.

15.3.4 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.

15.3.4.1 Messaging Malware Mobile Anti-abuse Working Group

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.

15.3.4.2 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.

15.3.4.3 Sender Policy Framework

Sender Policy Framework (SPF) creates a mechanism to validate the 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.

15.3.4.4 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.

15.4 *FTP (File Transfer Protocol)*

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 web site. This paper will be uploaded to my web server using FTP. I use WinSCP for FTP.

15.5 *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.

15.6 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 concerns related to pornography most ISPs are eliminating support for Usenet. If your ISP does not provide Usenet access there are a number of 3rd party services.

15.7 *Large File Transfer*

Most email services set a maximum file size for email. To send large files I use WeTransfer. It is a free service that lets you send files to one or more recipient. When each recipient downloads the file the sender gets a confirming email.

15.8 *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 are having 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.

15.8.1 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. DRM (digital rights management) 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.

15.8.2 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. Digital HDTV dramatically improves image quality compared to analog 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.

15.8.3 Netflix

Netflix pioneered snail mail DVD rental. Today they are a major streaming service. Netflix customers can use their PC to access a growing library of on-line titles or use a Roku player to watch streaming media on their TV. Image quality is automatically adjusted based of broadband speed.

15.8.4 Pluto TV

Pluto TV is another up and coming streaming service. It is free with content supported by advertising.

15.8.5 Cord Cutter News

As Cable TV rates have increased many folks are looking to reduce cost called cord cutting. We have always used a TV antenna for traditional TV and so have never had a cord to cut. There is an interesting YouTube channel called Cord Cutter News providing the latest information about alternatives to traditional Cable TV services.

15.8.6 VLC Media Player

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

15.9 *Digital Photography*

Digital cameras are a fantastic way 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 our internal server for safe long term storage and editing shortly after then are taken.

15.10 *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, spreadsheets, and PowerPoint presentations. I've played around with OpenOffice and LibreOffice a little but as long as I can run my copy of MS Office 2010 I'll just continue to use it. Not looking to rent an office application or need any of the cloud stuff.

15.11 *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, aquarium controller and most recently an outdoor temperature/humidity logger. They are all built around a CAI networks WebControl web based programmable logic controller (PLC). I also designed a control system for our outdoor lights but it is dumb hardware and does not live on the LAN.

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

15.12 *Bookkeeping and Taxes*

Computers are great bookkeeping machines making them ideal for tracking home and business finances.

For annual income tax preparation we use Tax Act software.

16 Data Backup – Oops Protection

Having an always-on server makes it possible to schedule automatic backup 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. I prefer managing my own data so I am not a fan of cloud storage.

16.1 *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.

A downside to keep in mind is if one of the machines on the LAN becomes compromised it is possible the backup shares will be attacked.

16.2 *Off Line Backup*

Figure 16 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.

16.3 *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 are placed in 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.

16.4 *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.

16.5 *USB Flash Drive*

Figure 17 32 GB 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.

17 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.

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.

17.1 *Strong Passphrase*

Having to maintain multiple passphrases is a bugaboo of modern life. Strong passphrases should be long enough to thwart brute force attacks, have a mix of words and numbers. For extra points throw in a few punctuation characters.

Interesting YouTube video about choosing strong passwords.

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 record the transaction and perform dictionary attack running through millions of possible passphrase until they find the right one. This type of attack is also a risk if a site is compromised. The attack will often yield user password and the attacker can use them to gain access to the compromised site and if you use the same credential other accounts.

- Change passwords, do not use defaults.
- Do not use trivial password such as: password, 1234, etc.
- Do not use a favorite password on multiple sites. Since internet access often uses your email address for the username if you use the same password at multiple sites and one is compromised the other accounts are at risk.
- Use long passphrases, at least 8 characters, of both letters and numbers and if possible punctuation characters.
- 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. Use other means to access your account.
- 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.
- In general periodic password changes are a waste of time and tend to result in selection of trivial passwords that user is able to easily remember. Wherever possible forgo mandatory password change interval but pick a robust password and one that is unique for each account.
-

17.2 *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.

17.3 *Password Managers*

I'm not a fan of password managers; to me this looks like a single point of failure. If the service is ever compromised so are all your passwords.

17.4 *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.

17.5 *Virus & Trojans*

This is probably what most people think of when discussing security. This attack has been around since the days of standalone PCs using floppy disks. The first line of defense is staying away from untrustworthy sites and do not connect your system to unknown devices. 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 a search engine to learn the site name. This does not guarantee site is safe but it reduces risk of fat-fingering a dangerous URL. The other vector that is becoming more common is to embed Virus software in online advertising. Since you have no way to know where that is coming from it is very difficult to protect against. One helpful technique is to use an ad blocker. However sites are increasingly refusing to serve content if they detect use of an ad blocker.

Anti-virus programs have been available for years. They check file signatures and monitor downloads. Windows comes with security software. 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.

When traveling do not plug your USB devices into public charging ports, use your own AC adapter. Beside power USB supports data transfers so a malicious charger is able to infect your system. The same caution applies to USB flash drives, it you don't know the source of the drive do not plug it into your system.

17.6 *Phishing Email*

Phishing email looks like it originated from a legitimate company. The email typically states recipient needs to "log in" to a 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. I quickly realized my mistake and went to the real site and changed account credentials. Hover over the link in the email to see the URL looks authentic for the site. Be sure to start all the way from the top level domain. One Phishing trick is to create a very long URL that looks OK if you only examine the first few subdomains. As a safeguard never login to an account from an email link, go directly to the site in question.

17.7 *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.

17.8 *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.

17.9 *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 programs used to remove various forms of spyware. They are updated periodically to detect and removes various forms of spyware.

17.10 DoS (*Denial of Service*)

Zombies are often used in DoS (denial of service attack). A DoS attack floods the 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.

17.11 *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. This prompted development of a stronger encryption scheme WiFi Protected Access (WPA2) using AES encryption. There are options optimized for home networks using a preshared key and for large organization using RADIUS authentication. There is a newer version called WPA3 but it is not yet commonly deployed.

> **Security Tip** –POP/SMTP email send user credential in the clear. This is not a huge concern on wired or security protected WiFi networks. It is a serious risk 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.

17.12 *DNS Cache Poisoning*

Internet was designed to be robust in the face of equipment and communication failures. Unfortunately it is not designed to withstand deliberate willful attack to network components. 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.

17.13 *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 WiFi 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.

17.14 *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.

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.

17.15 *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.

17.16 *Ad Malware*

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 have been using an ad blocker Adblock Plus.

17.17 *Software Patch Management*

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.

17.18 *Device/Software 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.
- WiFi predefined password management for home systems can be a challenge. WiFi 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 and security configured manually.
- Change the default WiFi 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.
-

17.19 *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.

17.20 NAT

A security side effect of NAT is by default it drops incoming connection requests. If a remote host attempts to connect to the 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.

17.21 *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 remotely. 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.

17.22 *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.

17.23 *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.

18 Troubleshooting Tips -- 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 can be a good diagnostic source. However consumer products are very competitively priced, that limits how much one-on-one support a vendor is willing to provide. There are many internet resources, besides the product vendor, able to help resolve end user issues. My favorite is DSLReports.

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, or use the Windows search feature and type cmd. This opens the command prompt, commonly called the DOS box.

There are many ways to troubleshoot problems. The most comprehensive is to start at the bottom and work your way up. This insures you do not miss anything but can be time consuming. Another option is to start in the middle, if that works you know the problem is after that level. When troubleshooting wireless problems a good first step is to see if the wired connection is working. No sense trying to fix a WiFi problem if the network itself is not working properly.

Troubleshooting questions:

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? This is the default gateway in network settings.
4. Is Router able to establish a connection to the ISP?
5. Are you able to Ping the remote host by URL?
6. If not, are you able to Ping the remote host by its IP address? If so have a DNS problem.
7. If steps 5 and 6 both fail traceroute to the remote site. This will indicate where things are failing. If the first few hops work but later ones fail the connection to your ISP is working but something is wrong either within the ISP or the internet in general.
8.

18.1 *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. I used MS Word to document the patch panel and Ethernet switch port utilization. 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 fun going back through early revisions of the network to see how things have evolved over time.

18.2 *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 the 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 Cat5 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 collision frequency gets worse as utilization increases. Occasional collisions are nothing to worry about. Hubs have been obsolete for many 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. All network interfaces will be displayed. Hover over the desired interface and right mouse click. 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.

> ***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.

18.3 *Router and Ethernet Switch Statistics*

Both the router and Ethernet switch provide information as to the heath of the internet and LAN. The switches logs frames sent on each port and any errors that occur.

18.4 *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 DSLReports 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 the 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 the 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

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.

18.5 *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:

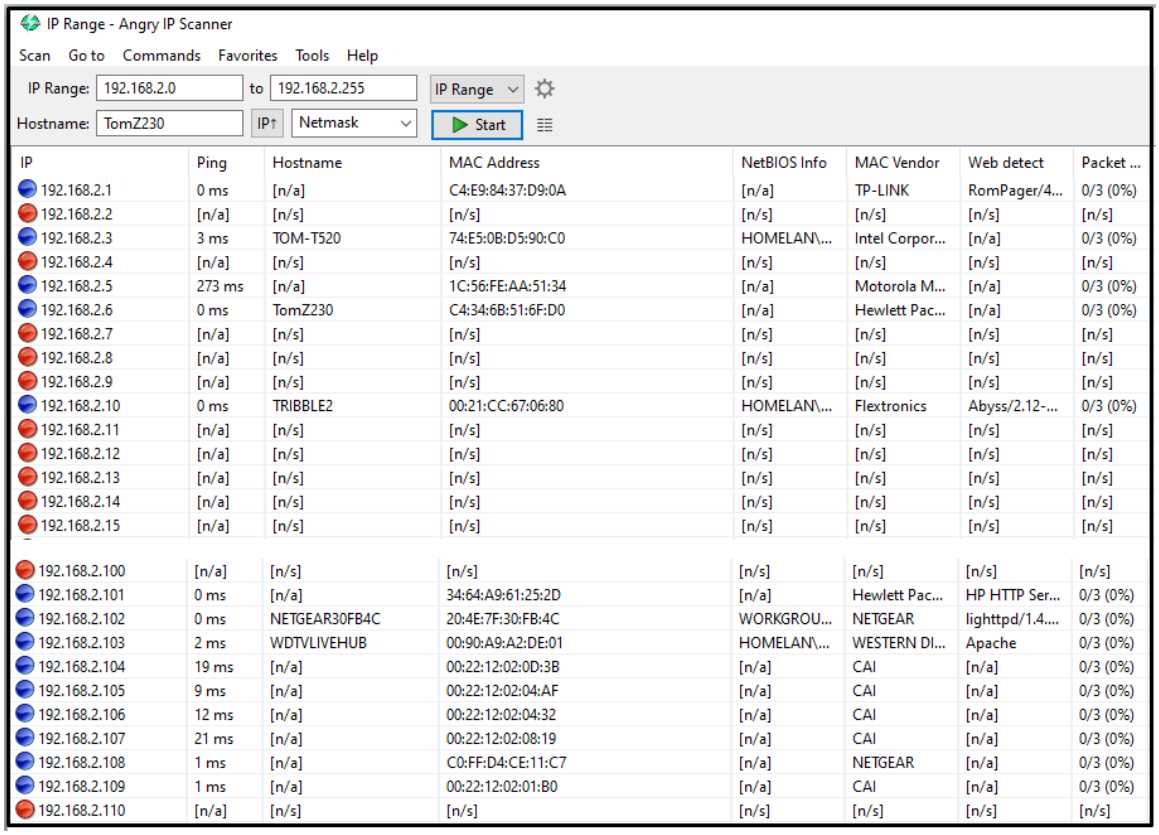
1 <1 ms <1 ms <1 ms 192.168.2.1
2 34 ms 33 ms 33 ms xx.milford1-1.nh.g4.net [66.211.144.97]

```
 3    35 ms    35 ms    35 ms  66.211.128.221
 4    35 ms    34 ms    34 ms  manchester0-8.nh.G4.net [66.211.128.133]
 5    37 ms    37 ms    36 ms  216-107-229-217.static.firstlight.net [216.107.229.217]
 6    37 ms    37 ms    37 ms  66-109-52-101.tvc-ip.com [66.109.52.101]
 7    39 ms    39 ms    39 ms  be13.albnypscr1.ip.firstlight.net [66.152.98.13]
 8    40 ms    40 ms    39 ms  be23.albynypsbr1.ip.firstlight.net [66.109.53.38]
 9    65 ms    64 ms    65 ms  equinix-chi.liquidweb.com [208.115.136.138]
10    72 ms    71 ms    71 ms  lw-dc3-core1.rtr.liquidweb.com [209.59.157.156]
11    71 ms    71 ms    70 ms  lw-dc3-storm1.rtr.liquidweb.com [69.167.128.89]
12    71 ms    71 ms    71 ms  www.dslreports.com [64.91.255.98]
```

Trace complete

18.6 *Angry IP*

AngryIP is a useful utility to view information about which devices are connected to the LAN. Also facilitates finding unauthorized devices. In our case the lower addresses are dynamic and those above 100 statically assigned to servers.



IP	Ping	Hostname	MAC Address	NetBIOS Info	MAC Vendor	Web detect	Packet ...
192.168.2.1	0 ms	[n/a]	C4:E9:84:37:D9:0A	[n/a]	TP-LINK	RomPager/4...	0/3 (0%)
192.168.2.2	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.3	3 ms	TOM-T520	74:E5:0B:D5:90:C0	HOMELAN\...	Intel Corpor...	[n/a]	0/3 (0%)
192.168.2.4	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.5	273 ms	[n/a]	1C:56:FE:AA:51:34	[n/a]	Motorola M...	[n/a]	0/3 (0%)
192.168.2.6	0 ms	TomZ230	C4:34:6B:51:6F:D0	[n/a]	Hewlett Pac...	[n/a]	0/3 (0%)
192.168.2.7	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.8	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.9	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.10	0 ms	TRIBBLE2	00:21:CC:67:06:80	HOMELAN\...	Flextronics	Abyss/2.12-...	0/3 (0%)
192.168.2.11	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.12	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.13	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.14	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.15	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.100	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
192.168.2.101	0 ms	[n/a]	34:64:A9:61:25:2D	[n/a]	Hewlett Pac...	HP HTTP Ser...	0/3 (0%)
192.168.2.102	0 ms	NETGEAR30FB4C	20:4E:7F:30:FB:4C	WORKGROU...	NETGEAR	lighttpd/1.4....	0/3 (0%)
192.168.2.103	2 ms	WDTVLIVEHUB	00:90:A9:A2:DE:01	HOMELAN\...	WESTERN DI...	Apache	0/3 (0%)
192.168.2.104	19 ms	[n/a]	00:22:12:02:0D:3B	[n/a]	CAI	[n/a]	0/3 (0%)
192.168.2.105	9 ms	[n/a]	00:22:12:02:04:AF	[n/a]	CAI	[n/a]	0/3 (0%)
192.168.2.106	12 ms	[n/a]	00:22:12:02:04:32	[n/a]	CAI	[n/a]	0/3 (0%)
192.168.2.107	21 ms	[n/a]	00:22:12:02:08:19	[n/a]	CAI	[n/a]	0/3 (0%)
192.168.2.108	1 ms	[n/a]	C0:FF:D4:CE:11:C7	[n/a]	NETGEAR	[n/a]	0/3 (0%)
192.168.2.109	1 ms	[n/a]	00:22:12:02:01:B0	[n/a]	CAI	[n/a]	0/3 (0%)
192.168.2.110	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]

Figure 18 Angry IP LAN Scanner

18.7 *Belarc Advisor*

Belarc Advisor is a freeware (for personal use) application that displays Windows hardware and software configuration information and whether or not security patches are up to date.

18.8 *WiFi tools*

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 WiFi radios are able to cut through the clutter and deliver fast internet access. This utility used to be shareware now it is paid, may be able to find old shareware version still available.

On my Android phone I use WiFi Analyzer by Vrem.

18.9 *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 . . . . . . . . . . . . : TomZ230
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
```

Ethernet adapter Ethernet:

```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection I217-LM
   Physical Address. . . . . . . . . : C4-34-6B-51-6F-D0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.2.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, December 6, 2019 7:20:38 AM
   Lease Expires . . . . . . . . . . : Monday, December 9, 2019 2:02:01 PM
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DNS Servers . . . . . . . . . . . : 192.168.2.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

18.10 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.

18.11 NETSTAT

Netstat is another handy command line utility. The –a option displays connections and listening ports. Using the -e option displays Ethernet stats including errors.

```
C:\Users\TSchmidt>netstat -e
Interface Statistics
                           Received            Sent

Bytes                      1755562572      217462740
Unicast packets               2768763             1839936
Non-unicast packets        86562               85233
Discards                          0                   0
Errors                     0                   0
Unknown protocols          0
```

18.12 Network Discovery

Network discovery is used in small LAN to allow computers to see each other and access shares.

LANscan is a utility that displays the name of each computer (assuming it supports NetBIOS) on the LAN and which one is the Master Browser. The Master Browser works with SMBv1. Microsoft has depreciated SMBv1 in Windows 10 due to security issues. Win 10 now uses WS-Discovery. This should be turned on automatically when enabling file sharing. Below is a typical LANscan output in a Windows 10 network. Note none of the computers are flagged as MASTER because SNBv1 is not enabled.

```
LANscanner v2.02 - ScottiesTech.Info
Scanning LAN...
--                         192.168.2.109    00-22-12-02-01-b0
--                         192.168.2.5      1c-56-fe-aa-51-34
--                         192.168.2.108    c0-ff-d4-ce-11-c7
--                         192.168.2.101    34-64-a9-61-25-2d
--                         192.168.2.107    00-22-12-02-08-19
--                         192.168.2.106    00-22-12-02-04-32
--                         192.168.2.105    00-22-12-02-04-af
--                         192.168.2.104    00-22-12-02-0d-3b
NETGEAR30FB4C              192.168.2.102    20-4e-7f-30-fb-4c     WORKGROUP
TOM-T520                          192.168.2.3       74-e5-0b-d5-90-c0    HOMELAN
TOMZ230                           192.168.2.6       C4-34-6B-51-6F-D0  HOMELAN
TRIBBLE2                          192.168.2.10      00-21-cc-67-06-80    HOMELAN
```

18.13 HDD Management

The Acronis system backup tool also comes in handy for managing hard disk partitions and cloning new drives in order to upgrade a system. If you just need to clone a drive, say to install and SSD I've used Macrium Reflect

18.14 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.

If your ISP is having trouble with their DNS Windows networking has a nifty feature that even though the computer is set for dynamic IP addressing you are able to set DNS statically. To do this go to properties on the desired network interface and select IPv4 properties. The lower portion of the dialog box has entries for DNS. I typically use the Google public DNS server address of 8.8.8.8 because it is easy to remember. Wikipedia has a short list of public DNS servers or do an internet search for public DNS.

18.15 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.

18.16 Is Website Up

If you are having problem reaching a specific web site I find Uptrends useful. It tests access from multiple locations worldwide. This lets you know if the problem is the website itself or just your connection.

18.17 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, mainly use Speedtest.net.

18.18 LAN Speed Testing

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

18.19 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. I typically use the most likely and easiest technique first. Do the easy stuff first even it is not the most likely. If that does not resolve the problem work your way through the list in a methodical fashion.

LAN Debug

- Are all PCs connected to the LAN? LAN transfers should work even if you lose internet access. If you can get to your router's web configuration/status screen that is a good indication that locally things are working correctly.
- Is the Ethernet link indicator on? If so it means the physical connection is good.
- Make sure the computer's network interface is on. In Windows and smart phones this can be set in software. On laptops there is often a physical switch to turn WiFi off.
- 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. If you are using a wired connection try unplugging/reconnecting the LAN cable. You can also use Windows IPCONFIG command to release/renew the DHCP lease. Use "IPCONFIG /release" (without the quotes) to terminate the lease then use the command again with /renew to request a new DHCP lease. If everything is working at this point should have the proper IP address.
- Ping the default gateway IP address. This is the address of your router. If this works is means your router is working.
- Try logging into your router.
- Ping machines on the LAN by name and IP address. This verifies Windows 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 resetting the network stack. In Win 10 towards the bottom of the network setting status page is the option to perform a network reset. .
- If you use Ethernet and WiFi on your LAN begin troubleshooting the wired connection. There is less to go wrong with Ethernet then WiFi, especially if you are troubleshooting speed related issues.
- When troubleshooting WiFi make sure the security method and password are set correctly. You can temporally disable security and try to connect. Just keep in mind that leaves your network wide open.
- If all else fails try brute force by removing power. Sometimes hardware hangs; you have nothing to lose by disconnecting power rather than just rebooting. Physically unplug the machine as some PC subsystems remain powered even if the computer is turned off.

WAN Debug

- If your DSL modem, Cable modem or fiber ONT 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 the physical connection to the ISP 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 the account to modem's MAC address or limit customer to a single DHCP lease. If connection is bound to DHCP turn off the modem long enough the DHCP lease to expire. If the service is bound to the MAC either clone the old MAC on the new modem or contact the ISP to reset the line.
- Ping a stable site like DSLRreports.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 2019 DSLreports.com IPv4 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.
- If you are able to reach some web sites but not others it may be a problem with the site itself. The Uptrends is a handy way to test web site availability.
- Perform a Trace route (tracert) in Windows) a stable site. 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 temporally "disappear" after a major fiber cut as routers try to route around failure. Ping time should gradually increase with hop count and distance. Sudden unexplained increase typically means there is congestion at that or the previous hop.
- If you are experiencing slow internet access doesn't hurt to try rebooting your modem.
- 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 your internet access.

19 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 568D Commercial Building Telecommunications Cabling Standard and EIA/TIA 570 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 the FCC took on 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.

Today much internet LAN traffic is carried wirelessly using WiFi. However even though the connection to the end device is wireless the Access Point most often needs an Ethernet link back to the LAN.

19.1 *Registered Jack Modular Connectors*

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

As US telephone industry was migrating to modular connectors it was also in early stage of divesture and FCC mandated CPE interconnect. For the first time Customers Premise Equipment (CPE) could 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 two line version the RJ14 is a 6P4C. The connector used for Ethernet referred as the RJ45 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.

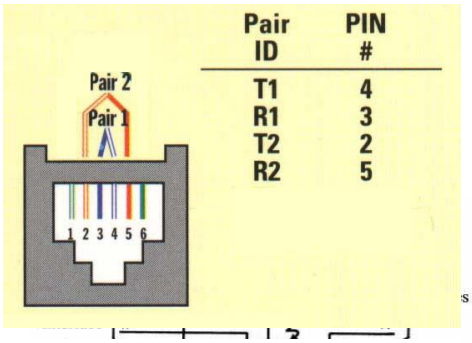


Figure 19 RJ11 & RJ14 Voice Jack

19.2 *USOC (Uniform Service Ordering Code) Pin out*

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

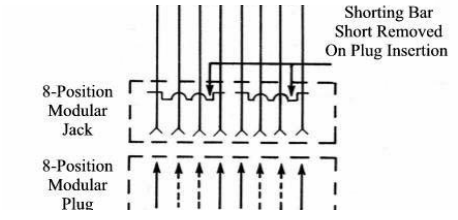


Figure 20 RJ38 Alarm Jack

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.

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.

19.3 *Type 66 Punch Down Block*

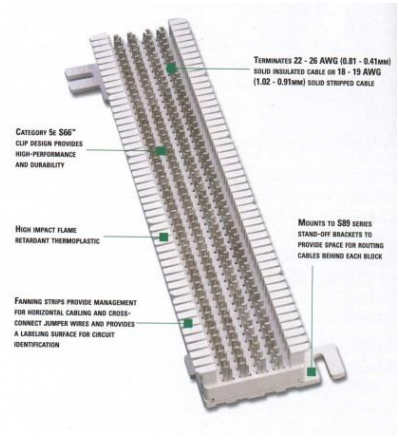


Figure 21 Type 66 Punch Down Block

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.

19.4 *Type 110 Punch Down Block*

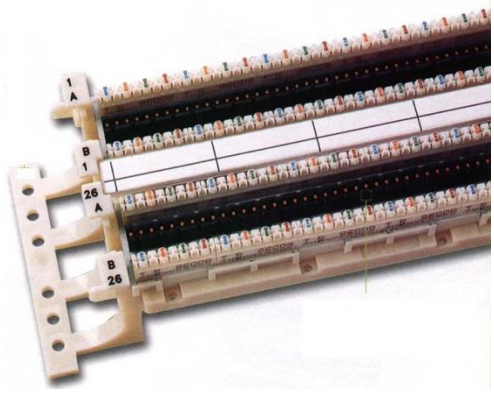


Figure 22 Type 110 Punch Down Block

Type 110 terminals allow higher density wiring than Type 66. Typical 110 modules include a standoff. Building wiring is routed under the bracket through the standoff and fanned out to the appropriate location. Multiple positions 110 blocks are then inserted over the base. 4-pair block are used for LANs and 5-pair 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 also used on Structured wiring jacks allowing the same punchdown tool to be used for both.

19.5 *Structured Wiring*

Figure 23 8P8C Data Jack

The key to EIA/TIA 568 & 570 is the use 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 the 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.

19.5.1 Patch Panel

Receptacles use type 110 punchdown terminations. 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 24 Patch Panel

Figure 25 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.

19.5.2 Category Rating

Cat 5e supports Ethernet up to Gigabit (1000 Mbps) over a distance of 100 meters (328 feet), as well as 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.

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 used in 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.

Category 8 is pushing the limits of copper and is primarily intended for relatively short runs in data centers.

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.

19.5.3 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 typically gel filled (icky-pick) 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.

19.5.4 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 network 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.

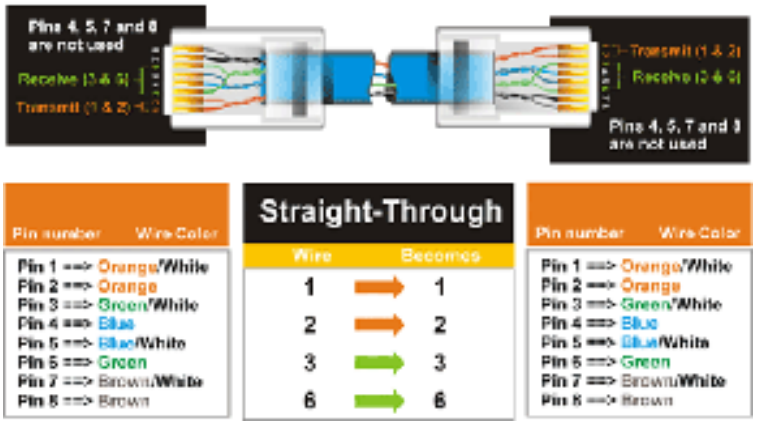


Figure 28 Patch Cable

19.5.5 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.

The connector pinout version should not be confused with the revision level of the 568 specification itself. The latest version of the TIA 568 specification is D.

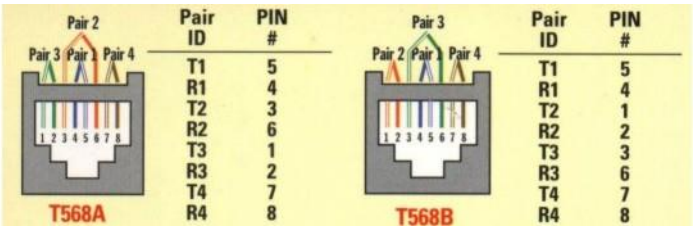


Figure 29 8P8C Structured Wiring Jacks

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.

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 pinout 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 Merlin key systems in widespread use when the structured wiring standard was being developed.

19.6 *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			

19.7 Landline Telephone

Traditional wired analog telephones are often called POTS (plain old telephone service). Before the advent of broadband internet we made extensive use of dialup. Dialup uses the public switched 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.

19.8 NID (Network Interface Device)

Figure 26 Typical Telco Demarc

In the bad old days before US telecom divestiture early 1980's the 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 NID (network interface device). 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 surge 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.

Now that our landline phone service is provided by the ONT we no longer have a NID. Inside phone wiring simply plugs into the ONT. We did need to turn off the ringers on several

phones (we have 5) because the ONT has a REN (ringer equivalence number) of only 3. Old style Western Electric phones had a REN of 1, modern electronic phones are often much lower. If the REN is exceeded the phone may not ring correctly of the ONT damaged.

19.9 *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.

19.10 *Power distribution*

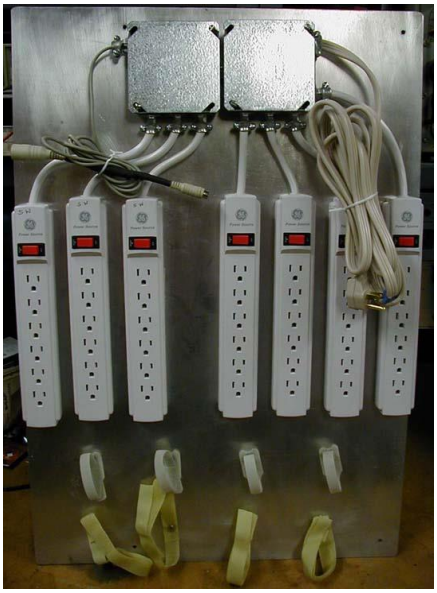


Figure 27 Power Distribution

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

Power Panel requirements

- Multiple always on receptacles
- Multiple switched receptacles controlled by workstation
- Wire routing provisions
- Space for "wall wart" power supplies.

To minimize power consumption devices that do not have to be on continuously are controlled automatically 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.

During the upgrade to Win 10 I replaced PS/2 power sensing with a USB connection. When the workstation is turned on 5 volts from the USB connection activates a SSR (solid state relay) powering up peripherals.

19.11 *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.

19.11.1 Power

Figure 28 Power Surge Protector

A whole house surge protector should be used to protect electronic devices system. The goal of the protector is to limit voltage extremes between phase conductors and phase conductors and ground. We use a GE THQLSURGE protector on the main service entrance and an Eaton CHSPT2ULTRA on the water heater service entrance. Installation of the GE device is easy it plugs into breaker panel much like an ordinary two-pole breaker and connects to the ground bar. A small neon light indicates the protector is working correctly. The Eaton protector mounts through a ½" knockout and also has status indicators.

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

19.11.2 Telephone

The gas tube surge suppressor in the NID does a good job shunting surges to ground. For added protection use a semiconductor secondary surge suppressor.

If you are running telephone wiring to an out building it is good practice to use surge suppressors where cable exits and enters each building.

19.11.3 Coaxial TV

Figure 29 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.

19.11.4 Point of Use

Once perimeter surge protection is in place installing point-of-use surge protectors' offers 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.

Figure 30 Surge Protector

I found a nice commercial surge protector on eBay designed to be used with high power printers.
The Ametex ESP XG-PCS-15D surge protector does all the things expected plus if voltage remains too high or too low it disconnects the load. The built in LCD screen cycles through: Under-volt count, over volt count, power outage count, surge count, current voltage.

There is a cable you can use to connect them to a PC USB port for detailed logging. This is a hand way to see a history of power line problems.

19.12 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 the Jack during termination. This makes termination easier. I use a Rino hand labeler to mark cable ends. This is a handy little device that dispenses and cuts cable labels.

When I initially installed our LAN crimped modular jacks directly to building cable. Since then I have switched to using a patch panel and factory made patch cables. Still, being able to fabricate custom cables is occasionally useful. When attaching modular plugs be sure to get ones designed for the type of cable you are using: solid or stranded because the contacts are different.

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 a special purpose telephone designed 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.

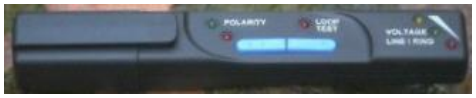
Lastly I found cable breakout tester, typically called a banjo, to come in handy doing nonstandard wiring. It provides access to individual conductors to verify wiring.

Cable Ripper

RJ11/45 Crimper

66/110 Punchdown

Wiring Tester



POTS Telephone Tester

Breakout Adapter

Figure 31 LAN & Telephone Tools

20 Putting it all Together

Telephone and LAN wiring terminates at different locations. Inside LV wiring is located in a small utility close near where underground wiring enters the building. I installed multiple 66 blocks to allow easy patching of telephone and other widgets. The LAN patch panel is in another closet adjacent to my basement office.

20.1 *Telephone Wiring*

The PON ONT is located in the LV wiring closet. Phone wiring is pretty simple, the multiple inside telephone jacks are paralleled using the 66 blocks and a short pigtail terminated with an RJ11 plug connects to the phone jack on the ONT.

An old style Western Electric wall phone is permanently mounted in the wiring closet, with a RJ11 corded plug. This allows the test phone to be plugged into the ONT disconnecting inside phone wiring. Having the phone permanently mounted insures it is available when needed.

20.2 *LAN Wiring*

We built the house in 1982 predating SOHO networking. The water heater is in a closet adjacent to my basement office so that does double duty as the LAN wiring closet. Our LAN wiring has been expanded over the years. When first installed I wired a few drops in the basement. Several years later added drops in bedrooms as our kids got older. The most 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. I did the LAN 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 terminated, even thou not all are currently being used.

20.3 *DSL Router*

The ISP supplied WiFi router is located in a cubby hole above 2nd floor bedroom closet. An Ethernet cable connects to the LAN port on the ONT and goes to the patch panel. A short patch cord connects it the drop in the closet. This in turn is connected to the WAN port on the router. The WiFi the router has 4 Gig Ethernet LAN ports. Another drop connects one of the router LAN ports to the basement patch panel where it connects to the main Ethernet switch.

20.4 *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.

With the addition of DIY home automation widgets I ran out of ports on the main switch so I added an 8-port switch dedicated to IoT devices.

20.5 LAN UPS

I built a DIY UPS to power the LAN in the event of utility failure. The UPS is plugged into a surge protector. The UPS powers the ONT, WiFi router and Ethernet switch. The battery is sized for multiple hours of operation so we do not loose internet access when we are not running the backup generator. Rather than using an inverter to create AC only to have the wall warts convert it back to DC Networking gear is powered by a 12V power supply when mains power is available or directly from the battery when it is not.

The UPS uses an automotive jump pack as the battery. This is handy as the battery charger/maintainer keeps the battery fully charged and the jump pack provides a "free" battery for the UPS. As long as mains power is available unplugging the jump pack has no effect on the network. The jump pack came with a 12V 17 AH battery. I found a 22 AH battery that is the same size so plan to install it when the original battery needs to be replaced.

20.6 *LAN Device Addressing*

I configured the servers and home automation devices with static IP addresses. The odd man out is the file server. I initially set it statically but due to Windows 10 problem had to set it dynamically and use the router's MAC reservation feature to maintain a stable IP address.

The remaining devices are set for DHCP, including our children's WiFi gadgets. That way they are able to use our WiFi when visiting rather than using expensive cell data.

All the non-portable devices use the NTP time service running on the server to obtain network time. The server in turn is pointed to pool time servers.

20.7 *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.

21 Internet Hosting -- Your Presence on the Net

Every business should have at least a minimal internet presence. Creating a simple web site is neither difficult nor expensive. The web server can be located in-house or 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 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. Your server is located in a data center with virtually unlimited access to bandwidth. A single server is used to host many web sites resulting in very low cost.

The hosting service takes care of most of the technical details: setting up the various servers, registering a domain name, creating DNS records and obtaining an SSL security certificate. 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.

21.1 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 you 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 it was already registered so I picked tschmidt.com

21.1.1 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.

21.2 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.

21.2.1 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 your internet connection. Virtual hosting is appropriate for low traffic sites. The hosting service runs multiple virtual web servers on a single physical server. Our hosting service announced they were shutting down in early 2024. We looked at various services and on the advice of a friend chose DreamHost. 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 was 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 your 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. If you have locked your name the current hosting service needs to contact the registrar to unlock it. This is a security measure to prevent unauthorized transfers.

Normally one registers a domain name to create a public 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 name of the service as the starting point of your site.

21.2.2 Dedicated Server Collocation

Most hosting services offer collocation where customers are 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.

21.2.3 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 our internal non-public web server.

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 ISPs assign dynamic IP 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. Software running on the customer side detects IP address changes and updates the dynamic DNS service. 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.

ISPs typically prohibit residential 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.

21.3 *WHOIS Record*

Information for each registered domain is located in the WHOIS databases maintained by RIR (regional internet registries. The database maintains administrative and technical contact information about the site. The Whois database does not maintain information about the site itself; it contains a list of authoritive nameservers. To find the IP address of a site one needs to query one of the nameservers associated with the site.

```
Domain Name: tschmidt.com
Registry Domain ID: 2338933_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.DREAMHOST.COM
Registrar URL: WWW.DREAMHOST.COM
Updated Date: 2024-10-10T21:17:56.00Z
Creation Date: 1998-11-04T05:00:00.00Z
Registrar Registration Expiration Date: 2025-11-03T05:00:00.00Z
Registrar: DREAMHOST
Registrar IANA ID: 431
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant Name: Proxy Protection LLC
Registrant Organization: Proxy Protection LLC
Registrant Street: 417 Associated Rd #327
Registrant Street: C/O tschmidt.com
Registrant City: Brea
Registrant State/Province: CA
Registrant Postal Code: 92821
Registrant Country: US
Registrant Phone: +1.7147064182
Registrant Phone Ext:
Registrant Fax:
Registrant Email: vjlxeu43v6eqnhs@proxy.dreamhost.com
Admin Name: Proxy Protection LLC
Admin Organization: Proxy Protection LLC
Admin Street: 417 Associated Rd #327
Admin Street: C/O tschmidt.com
Admin City: Brea
Admin State/Province: CA
Admin Postal Code: 92821
```

Admin Country: US
Admin Phone: +1.7147064182
Admin Phone Ext:
Admin Fax:
Admin Email: hzfkv8s4ftyetpl@proxy.dreamhost.com
Tech Name: Proxy Protection LLC
Tech Organization: Proxy Protection LLC
Tech Street: 417 Associated Rd #327
Tech Street: C/O tschmidt.com
Tech City: Brea
Tech State/Province: CA
Tech Postal Code: 92821
Tech Country: US
Tech Phone: +1.7147064182
Tech Phone Ext:
Tech Fax:
Tech Email: k3u83q246wyvn2f @proxy.dreamhost.com
Name Server: NS1.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS3.DREAMHOST.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: DOMAIN-ABUSE@DREAMHOST.COM
Registrar Abuse Contact Phone: +1.2132719359
URL of the ICANN WHOIS Data Problem Reporting System: HTTPS://ICANN.ORG/WICF
>>> Last update of WHOIS database: 2024-11-23T21:05:12.00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

DreamHost whois server terms of service: http://whois.dreamhost.com/

DreamHost is a global Web hosting and cloud services provider with over 375,000 customers and 1.2 million blogs, websites and apps hosted. The company offers a wide spectrum of Web hosting and cloud services including Shared Hosting, Virtual Private Servers (VPS), Dedicated Server Hosting, Domain Name Registration, the cloud storage service, DreamObjects, and the cloud computing service DreamCompute. Please visit http://DreamHost.com for more information.

Figure 32 WHOIS Domain Record

21.3.1 Administrative

Administrative information records data about site ownership and contact.

21.3.2 Technical

Technical information records data about network operation center contact.

21.3.3 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.

21.4 *DNS Record*

Once a 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.

21.4.1 Address Records (A)

Address records map host name to IP address.

21.4.2 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.

21.4.3 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.

21.4.4 Pointer Records (PTR)

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

21.4.5 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.

21.4.6 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.

21.4.7 SPF - Sender Policy Framework

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

A records

	Name	Address	Type	Class	TTL
#1	tschmidt.com	104.152.168.18	A	IN	14400 (4 hrs)

MX records

	Preference	Exchange	Name	Type	Class	TTL
#1	0	tschmidt.com	tschmidt.com	MX	IN	14400 (4 hrs)

NS records

	Nsd name	Name	Type	Class	TTL
#1	ns2.hollishosting.com	tschmidt.com	NS	IN	86400 (1 day)
#2	ns1.hollishosting.com	tschmidt.com	NS	IN	86400 (1 day)

SOA records

Mname	ns1.hollishosting.com
Rname	server18.hostwhitelabel.com
Serial	2015082000
Refresh	86400
Retry	7200
Expire	3600000
Minimum	86400
Name	tschmidt.com
Type	SOA
Class	IN
TTL	86400 (1 day)

TXT records

Text	0	v=spf1 ip4:67.220.209.110 ip4:67.220.209.136 ip4:67.220.209.137 a mx ip4:72.37.245.130 ?all
Name	tschmidt.com	
Type	TXT	
Class	IN	
TTL	14400 (4 hrs)	

Figure 33 DNS Record

21.5 *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.

21.5.1 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 WinSCP. My hosting service supports web based file uploads/deletion so I no longer need to use FTP

21.6 *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:
```

21.7 *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.

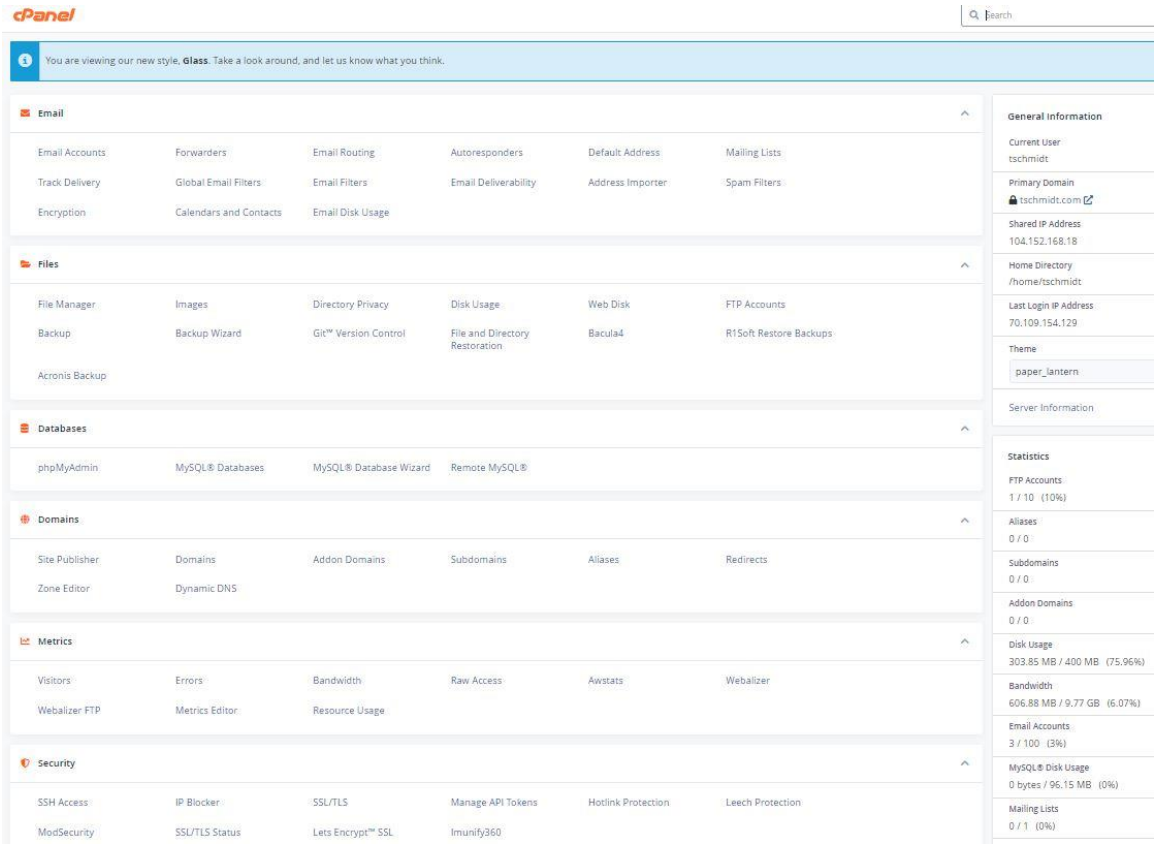


Figure 34 Hosting Service cPanel Home Page

21.8 *Troubleshooting*

On occasion I've had instances where the site was inaccessible from some ISPs but not others. Uptrends has a nifty tool that accesses the site from multiple locations around the world and reports success/failure and latency.

Conclusion

Setting up a SOHO network has been an interesting and rewarding experience. The network meets our business and personal requirements. It has been great to finally be able to sign up for fiber internet. Unlike DSL if we need faster speed it is just a matter of paying the additional cost and having the ISP change PON settings. An unanticipated advantage of fiber internet is traditional landline telephone service costs less. Currently we are paying about the same for 100/100 internet and phone as we were paying for DSL and phone. Even when the Consolidated/Fidium teaser rate expires our cost will only go up by $20 a month.

Unless you are planning a very complex network the necessary components are readily available however amassing the technical knowledge to create and troubleshoot can be rather intimidating. Every 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 it security issues. In general failures are pretty straightforward to identify and fix once root cause is determined. However, determining root 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