Living with a Home Network

Tom Schmidt
Schmidt Consulting
Revised 1/14/2000
tom@tschmidt.com
http://www.tschmidt.com

Abstract
Long-term experience with a small Internet connected network. Discuss issues involved in setting up the LAN and Internet Gateway, choosing an Internet Service Provider, and setting up the various network services.

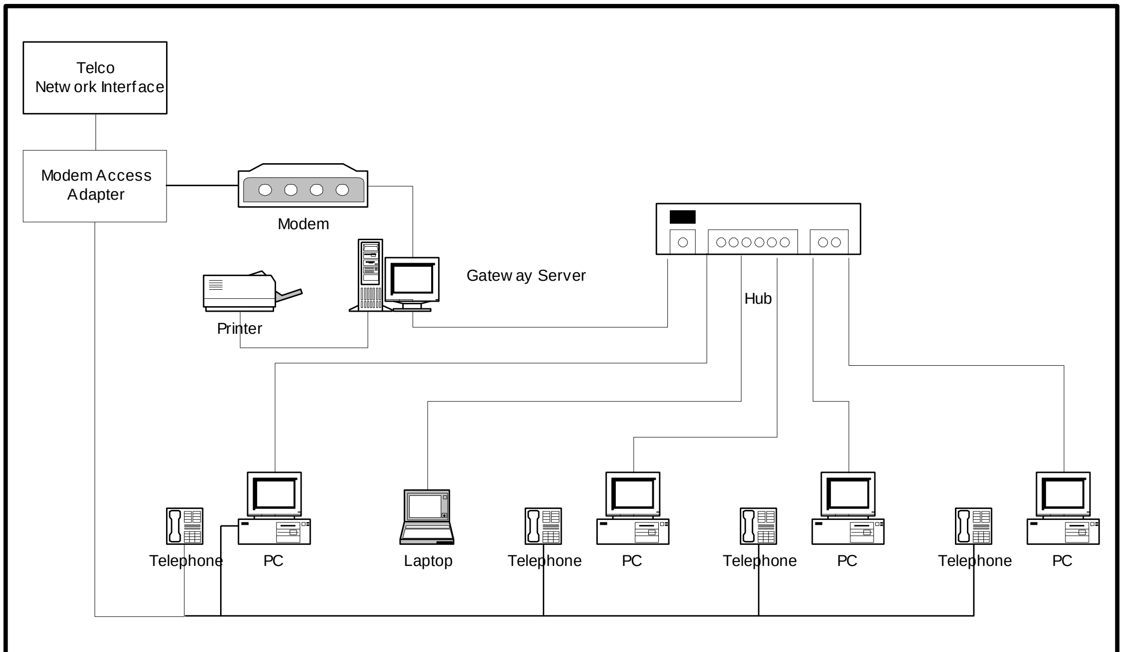
Table of Contents

1 Overview

In mid 1998 I set up a Small LAN. I was starting a consulting business and wanted to learn more about the issues involved in building and operating a small LAN. Until that time my networking experience was limited to interactions with the corporate Information Technology (IT) department.

This paper discusses how to set up a small LAN, use dial-up networking to connect to the Internet, and set up a multitude of useful networking services. It is not intended as a competitive product review. The field is constantly changing so any attempt to do so is rapidly outdated. Rather, it discusses how specific features were implemented. For up to date reviews of networking hardware and software the reader is directed to the many publications and web articles on the subject. The products and services described in this paper represent my choices to deliver the features I needed.

The LAN is Ethernet over Unshielded Twisted Pair (UTP). A permanently connected laptop PC is used as the Gateway server. Having a dedicated machine improves overall reliability because only the software needed to operate the network runs on the server. The Gateway connects to the Internet via a dialup ISP account, runs proxy server to share the account, runs the Firewall to keep the bad guys out, runs a time server to synchronize the PCs and runs a private web server for internal users. The implementation is not static it is constantly changing as needs change and new devices hit the market.



SOHO System Implementation

2 Type of Internet Access - The Wires

The most common reason cited for PC purchase is access to the Internet. Three access methods are available to SOHO customers, traditional dial-up modem, Digital Subscriber Line (DSL), a high-speed service over existing phone wiring, and Cable Modems, a high-speed service over existing Cable TV wiring.

2.1 Dialup

Dialup access is available to anyone with access to a telephone line. Dial-up modems work with cellular phone, however data rates are significantly lower then wired phone line so it is not commonly used at fixed locations.

Most ISPs offer ITU V.90 modem support. The International Telecommunications Union V.90 standard replaced previous generation of proprietary 56Flex and X2 modems. ISPs typically connect directly to phone company digital trunks. This means only a single analog to digital conversion is used, at the subscriber's central office. This allows the ISP modem to synchronize transmission with the digital line, enabling the ISP to transmit at up to 56kbps. Current FCC power regulations limit speed to 53kbps. Transmission from the subscriber to the ISP is limited to 33.6kbps because the subscriber does not have access to digital carrier.

At connect time the modems probe the line to determine noise and attenuation levels. This sets the initial connection speed. During the course of the connection the modems constantly adjust to varying line conditions.

Typical connect speed ranges between 40-48kbs. V.90 is the end of the road for analog modems. The phone company digitizes the subscriber line at the central office. From there the call it is carried as a 64kbps Pulse Code Modulation (PCM) digital signal. This places and upper limit on data of 64kbps, V.90 modems come amazingly close to that limit. Future improvements in "last mile" speed will be based on other technologies, such as Digital Subscriber Line (DSL), Cable Modems and Fiber to the home (FTTH).

2.2 xDSL

DSL uses the existing wiring between the subscriber and the phone company central office to carry high-speed data without interfering with the existing analog phone circuit. Digital data is carried at frequencies above those used for the voice channel. Unlike radio the signals are confined to the wires so signals from one line do not interfere with other subscribers.

Speed varies by supplier; it ranges from approximately 380kbps to 1,500kbs downstream. Depending on the service the upstream rate may be the same or lower. Most service providers assume asymmetric use; more data is returned from a web site then sent to it. DSL is an always-on service, you do not have to “dial” the connection, and it is always live. This makes using the Internet on the spur of the moment practical because the user does not have to wait the minute or so for the modem to connect.

DSL service is offered by traditional phone companies called Incumbent Local Exchange Carriers (ILEC), Completive Local Exchange Carriers (ILEC) and by some ISPs.

Even though DSL operates over existing telephone company copper wire it still requires substantial investment to provide the service. The subscriber needs a DSL modem to convert computer data to DSL signals. At the central office DSL needs to be converted back into a form suitable for networking. Equipment is needed to combine and route the signals from DSL subscribers to the Internet.

Not all phone lines are capable of supporting DSL service. Assuming your phone company local central office is equipped for DSL you will not be eligible for service if you are too far away from the central office or if the phone company uses Digital Loop Carrier (DLC). DLC allows multiple phone lines to share a single copper pair, reducing wiring cost for the Telco. DSL signals are incompatible with existing DLC installation requiring extensive upgrading to DLC to deliver DSL. DSL signals degrade over distance; the exact limit is a function of speed but typical distances ire 12,000-18,000 feet.

For the latest information on DSL go to http://www.dslreports.com/.

2.3 Cable Modem

The cable TV industry is also being very aggressive delivering high-speed data. Cable is a one-way medium. TV signals originate at the CATV office, called the headend, and are delivered to the cable subscribers. The cable is partitioned into a number of channels and each channel carries a TV signal. Internet service is very different. Instead of a one-way connection from the headend to many subscribers each Internet machine connects to a remote server, a many-to-many connection. The cable must support a large number of two-way connections. As is the case with DSL the CATV venders must install much new equipment. Several TV channels are reserved for data services; this accommodates the downstream path to the users. The upstream path is more difficult. The CATV vender must replace the amplifiers used to distribute the signal with ones capable of data transmission in both directions. At the CATV office these signals are converted from the cable format and routed to the backbone data network.

Some early implementations were unidirectional. The cable was used for downstream data and a conventional modem for upstream. This allows the CATV vender to offer high-speed data while it is upgrading its network for bi-directional data.

The CATV is working to standardize the interface so the cable modem can be purchased like a typical dial up modem today DOCIS Data-Over-Cable Interface Specification. Like DSL DOCIS is an always-on connection, it is not necessary to "dial" into the Internet. Typical CATV speeds are 700-10,000kbps.

2.4 Thoughts on Access

DSL and Cable Modems are exciting new high-speed services that provide a high speed always on service. These technologies are in their infancy providers are still learning how to deliver and optimize them. Providers are working hard to expand service but DSL and Cable Modem are still not widely available.

In the short term most of us will be limited to dialup Internet access. This is especially true in rural areas. As DSL and Cable Modems deployment expands they open the door to true high-speed service, Fiber to the Home. Last-mile Fiber optic connection will deliver gigabit data rates enabling data, voice, and telephony to be carried over connection.

3 Internet Service Providers – Let the Mergers Begin

MCI was our first Internet Service Provider (ISP). Two considerations were paramount, nationwide access and a common provider of both long distance telephone service and Internet connectivity. That did not last long the MCI/WorlCom merger required divesture of their Internet service to Cables and Wireless. Cables and Wireless recently sold retail Internet access to Prodigy.

Each of these moves involved a domain name change, which of course changes ones e-mail address. The venders provide forwarding from the old address for a period of time to ease the transition. I did not want to have my clients continually update my e-mail address. Worse, occasional clients may not be able to contact me at all. Changing ISPs also requires changing log in procedures on the gateway server and laptop.

So it was time to choose a different ISP, this time the criterion was: nationwide access, V.90 Modem pool, and unmetered service. Unmetered service was important as we were bumping into the 150-hour limit of the current plan. We chose the same company that was providing our web hosting service INR.Net. They are a local ISP that met our requirements and in addition are extremely responsive to e-mail and phone support issues. They bill directly to a credit card number eliminating paper invoices.

3.1 Acceptable Use Policy

ISPs have written policy that sets limits on how the service may be used. For example, reselling the service is forbidden. Verify your ISP does not specifically prohibit operating a LAN. Even though the ISP does not disallow LANs do not expect technical help from them setting it up either.

3.2 Thoughts about ISPs

Consider ISP mail accounts throwaways, free e-mail accounts or a registered domain name are a better choice if you want a permanent e-mail address. The ISP business is very competitive; assume you will see continuous change and consolidation. If the ISP requires special software make sure it works with the rest of the networking environment.

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

Performance Tip - in dial up networking uncheck "NetBEUI" and "IPX." TCP/IP is the only protocol needed to connect to an ISP.

4 Telco -- Getting Connected

I run a consulting business from a home office, two lines are for non-business and the third reserved for business use.

The two non-business lines are configured as a hunt group. If line 1 is busy incoming calls are automatically sent to line2. Residential service reps may not be familiar with it because it is a "business feature." Line 2 is optioned with call waiting, so even if both lines are busy the caller does not get a busy signal. Caller ID is disabled on the second line. The goal was to treat the two personal use lines as single main number, callers always use the main number. This works well for incoming calls, however outgoing calls are not as simple. Caller ID is bound to each line. We wanted both lines to return the same Caller ID information, that of the main line. Unfortunately that is not possible. The choices for the second line are to allow Caller ID on or disable it. Disabling Caller ID hides the phone number from ordinary users, however some people block incoming calls with Caller ID turned off. If Caller ID is left on people will learn the second number and call it directly, defeating the purpose of the hunt group. Hunting is unidirectional; if someone calls the second line and it is busy the phone company will not ring the first line.

The third line is used solely for business. It is not part of the hunt group used with the other two lines. Since the business only has a single line we wanted to use Telco based answering service. Telco answering is very useful for small single line offices because the caller gets voice mail if the line is busy. I consider call waiting inappropriate for a business connection. Unfortunately our local central office does not support voice mail so we must rely on an answering machine. Another possibility is to use call forwarding to automatically transfer busy or no answer calls to a cell phone.

The LAN uses demand dial Internet access. When any computer on the LAN needs access to the Internet the Gateway automatically dials the modem to connect. This eliminates the need for each user to have a modem and allows all machines to share a single Internet connection.

The modem is not on a dedicated phone line. This leads to problems sharing a phone line with a modem. Picking up a phone disconnects the data connection and if the phone is in use the computer cannot access the Internet. I looked for an off the shelf solution to this problem but could not find one. So the Modem Access Adapter was designed to solve the problem. This eliminated the need for a dedicated modem line and provides optimum use of the three lines.

Usage Tip – Call waiting can be disabled at the beginning of the call, disabling call waiting for the duration of the call. The sequence varies by locale, in our area it is *70. Unfortunately if you send the disable sequence to a line not equipped with call waiting it is interpreted a part of the dialed number, resulting in an incorrect connection. This is a problem if the modem uses multiple lines and not all are equipped with Call Waiting.

Usage Tip -- Call waiting and hunting may be used together. Call waiting can only be optioned on the last number in the hunt group.

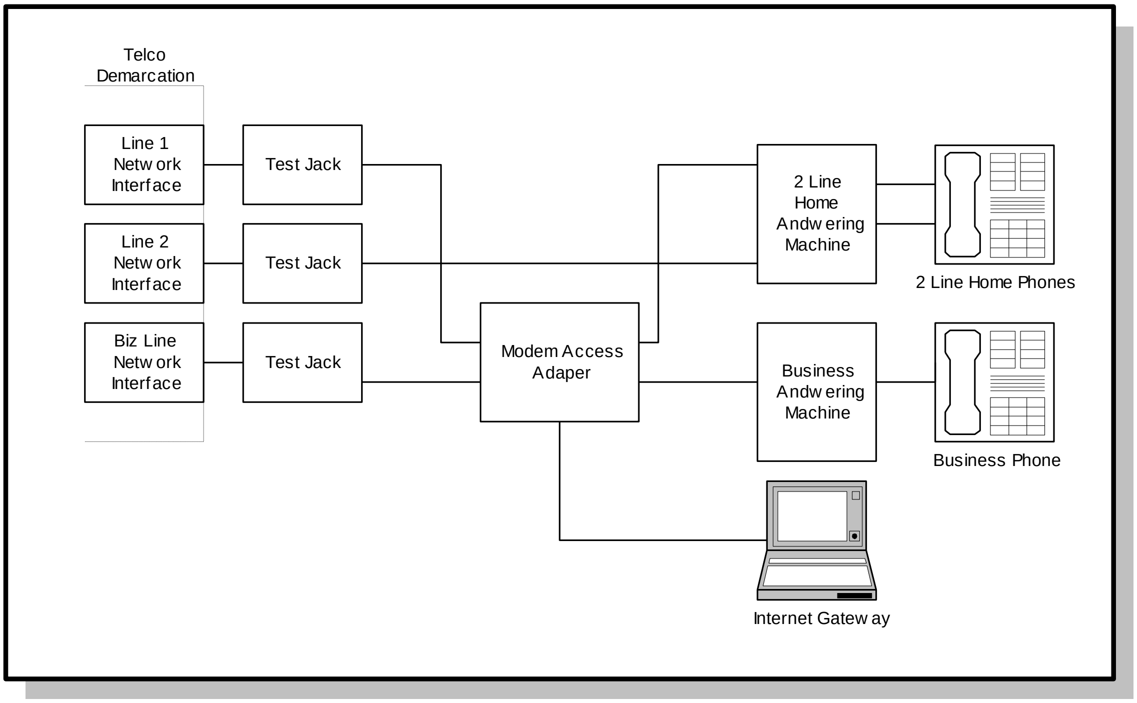
4.1 Modem Access Adapter

The Gateway Server automatically demand dials the ISP. This presents a problem because the modem will not be able to connect if the phone line is in use and conversely someone picking up a phone will disrupt the modem. We wanted a device to search for an idle phone line when the computer needs to access the ISP and to disconnect the phones for the duration of the call. This maximizes the chance of completing the call while reducing overall cost by eliminating the need for a dedicated modem line.

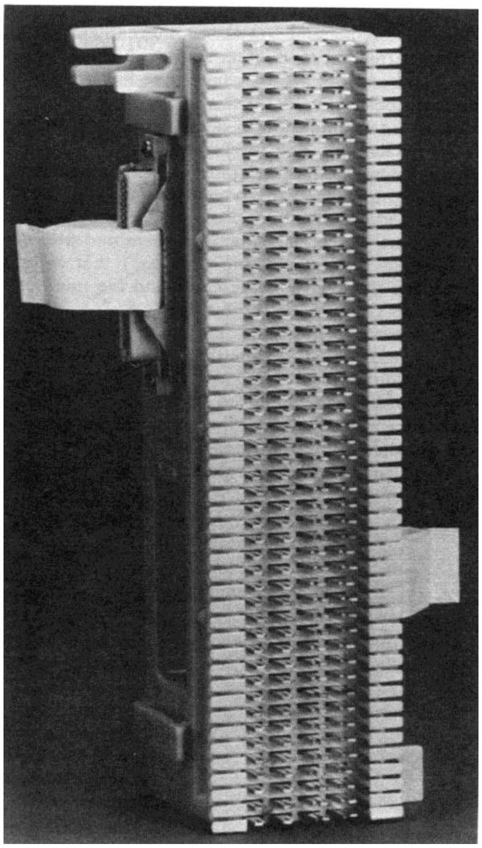
The modem access adapter is a purpose built device that is designed to isolate the data call from the extension phones. When the computer attempts to call the access adapter detects the computer has gone off hook. The adapter searches for an idle line. If it finds an idle line it disconnects the phones and connects the line to the modem. This prevents phones from interfering with the computer. If all lines are busy the modem never receives dial tone and retries the connection attempt later.

The adapter is connected to the primary personal line and the business line. This combination assumes that during the day when the business line is needed the modem uses a home phone line. The two home lines are connected as a hunt group so when the first line is busy the call is automatically routed to the second. If the primary home line is busy the data call is placed on the business line. This is most likely to occur after normal business hours, when home phone usage is heaviest.

Ideally a telephone company based answering service would augment this arrangement. This would guarantee that all business calls are answered. Unfortunately our local phone company does not offer that service. The Modem Access Adapter was published in the July 22, 1999 issue of EDN as a design idea.



4.2 Telco Connection Scheme



The drawing shows how the three phone lines and gateway server are connected. Two lines are used for family, and one line for business. The modem access adapter is placed in series with the primary family line, and business phone line.

To facilitate wiring changes each telephone outlet runs directly to the wiring closet. In the wiring closet each outlet terminates at a type 66 terminal block. Wires are terminated with a special punchdown tool that pushes the wire between contacts and automatically cuts it to length. This speeds up installation because termination does not require cutting, stripping, and tightening the terminal screw. Cross-connect wires connect each phone jack to the proper phone line. To facilitate trouble shooting inside wiring can be completely disconnected from the Telco. This makes it easy to determine if the problem is with the phone company or the inside wiring. In addition each line has a test jack and a spare phone is kept in the closet for troubleshooting.

Wiring supplies can be purchase at electrical supply houses or on line at Mike Sandman... Chicago's Telecom Expert. They have all the supplies needed for networking and telephony wiring.

Wiring Tip -- Clear plastic covers can be used to protect the 66 block terminations.

4.3 Secondary Lightning Protection

The phone company provides lighting protection as part of the Network Interface. This is primarily designed to safeguard the network. Electronic devices are somewhat fragile; this is especially the case with the modem because it has two connections, one to the phone line and one to the computer. This makes modem susceptible to line surges. Adding secondary protection minimizes the risk of damage.

Comm-Omni International manufactures secondary protectors. The protector clips to a 66 style split block. In a split block the four horizontal terminals are split down the middle. The Surge protector clips over a pair of rows providing a path from left side to the right hand side. One side terminates to Telco wiring the other to the inside wiring. The protector must be connected to a good ground. Excessive voltage is shunted to ground protecting the equipment. A protector should be used on each telephone line and on any lines that go to out buildings.

4.4 Thoughts about the Phone Company

All the folks I've worked with have been friendly and accommodating. However, the legacy of 100 years of monopoly service combined with a twisted pair copper physical plant does not come close to meeting the communication requirements of a leading edge family or small business. Cost is too high and bandwidth is inadequate. Hopefully a single high-speed pipe that delivers data, TV, and telephony will be available in the near the future.

5 LAN -- The Connected Home Biz

The goal was to allow a computer to be used anywhere. Once connected the computer has access to other computers, the printer, and the Internet.   Networking consists of the machine-to-machine connection called the Local Area Network (LAN) and software protocols that allow them to talk to each other the TCP/IP stack. The most common local area network technologies are Ethernet, commonly used by companies, Home PhoneLine networking, a modified version of Ethernet that runs over ordinary phone lines, and RF radio LANs.

5.1 Ethernet

Ethernet IEEE 802.3 is the most common local network used today it is based on a CDMA/CA (Collision Detection Multiple Access Collision Avoidance) scheme. Think of Ethernet as a telephone party line. Before speaking you listen to see if anyone else is talking. If no one is talking then you start. It is possible that several people will start talking at the same time. This is a collision; no one can understand what is being said. Each sender notices this and stops talking for a while. When the line is idle they try again. Each party waits a different amount of time to minimize the chance of colliding again. CDMA/CD imposes a number of design considerations on the network. The minimum packet size must be longer then the end-to-end propagation delay of the system. This insures the transmitter is still transmitting when the collision occurs allowing retries to be done by the network layer. Power levels must be set to allow collision detection.

When Ethernet was fist developed is used a fat coax cable with taps clamped to the cable at prescribed intervals. Today the most common type of Ethernet uses twisted pair cable, similar to phone wire. This dramatically reduced the cost of implementing a LAN.

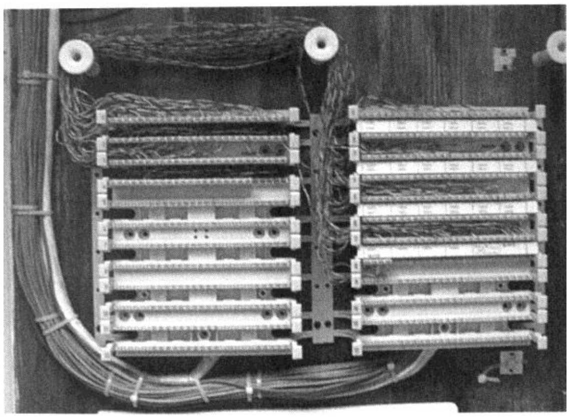
5.1.1 UTP Unshielded Twisted Pair

As LANs became pervasive it was discovered that one of the major costs of networking was wiring, regardless of the actual network deployed. Wiring has a relatively long life time, 5-10 years in an office building. This means that several generations of computers will use the same wiring. The Telecommunications Industry Association set about developing a wiring scheme that was independent of LAN technology. They created five categories based on the maximum frequency the wiring needed to carry. Only two are in widespread use Cat 3 and 5. Category 3 is typically used for phone wiring and Category 5 for 100Mbps Ethernet.

5.1.2 Structured Wiring

EIA/TIA 568 Category 5 unshielded twisted pair is used for LAN wiring. Phone wiring normally uses Category 3 because the wire and connectors are cheaper. Wiring is “home run,” each outlet is a separate cable run back to a central wiring closet

UTP is designed for a maximum of 100meters of length, this includes a patch cord from the computer to the wall jack, 90 meters of wiring (in TIA parlance call horizontal wiring), and another patch cord in the wiring closet to connect facility wiring to the hub. Horizontal wiring is terminated to terminal blocks in the wiring closet. 66 style blocks can be used however 110 style blocks are more common because they are denser, allowing more terminations for a given amount of wall space. Special patch cords are used to connect the terminal block to the hub.



Terminating horizontal wiring at a punchdown block and then connecting selected outlets to the hub with a patch cord makes sense in a commercial installation that has a large number of outlets that are constantly being rearranged. In a small office or home the situation is different, the number of outlets is rather small and one can purchase a low cost hub with enough ports for all outlets. Hubs are available with 16 and 24 ports. Some hubs can be connected to each other (stacked) to increase the number of ports. In a home installation wiring can be terminated directly to UTP plugs in the wiring closet. Plugs are somewhat more difficult install then receptacles so it is not for the faint of heart but doing so eliminates the cost and space of the 110 blocks.

5.1.3 Special Tools

Proper tooling is absolutely essential to produce a reliable network.

Tool	Purpose
Wire Cutters	Cut Cable to length
Cable Stripper	Special Stripper to remove the outer cable jacket
Punch Tool	Terminate 66 and 110 blocks
110 Blade	Terminate 110 blocks
66 blade	Terminate 66 blocks
Crimper	Crimps wires into Plug
Fish tape	Used to snake wire through walls

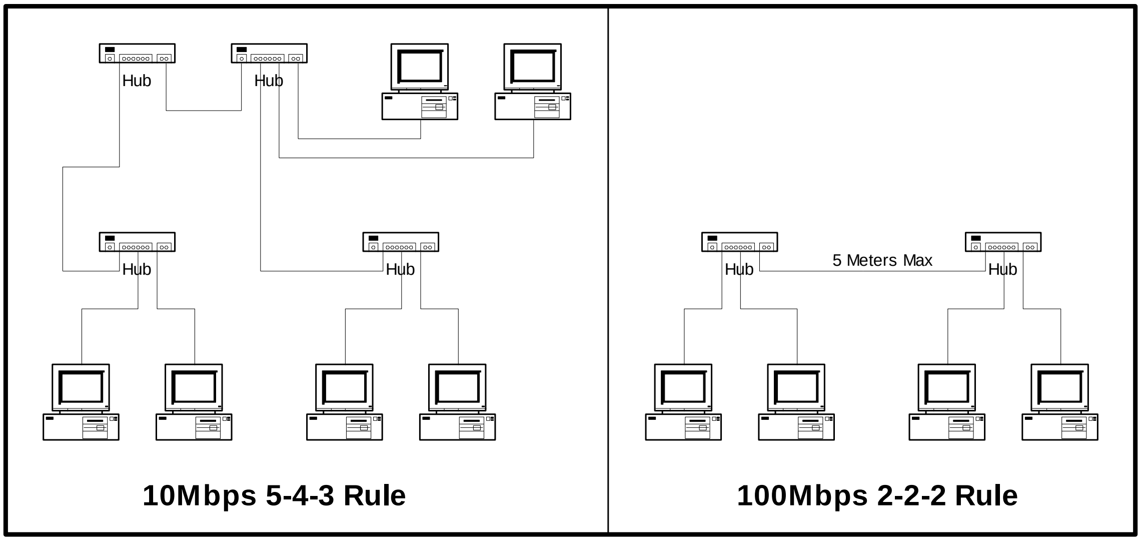
A good wiring guide is the “Technician’s Handbook -- Communications Cabling” by James Abruzzino ISBN 0-9671630-0-5.

Cabling should be tested after installation; simple testers are in the $100 range making them somewhat expensive for small installation. Using an ohmmeter will verify end-to-end continuity. This finds many common errors however it will not find split pairs. This is where end-to-end continuity exists but the pairing is incorrect. This type of mistake may work with 10Mbps but will fail at 100. The other concern is excessive untwisted length. When terminating the wire it is important to untwist only enough wire to make the connection and no more.

5.1.4 10Mbps vs. 100Mbps vs. 1Gbps

Initially UTP Ethernet ran at 10 million bits per second. Fast Ethernet increased speed to 100 million bits per second over Category 5 wiring. Today most new installations use 100Mbs because there is very little cost difference between 10 and 100. The newest version, Gigabit Ethernet is 10 time faster then Fast Ethernet, 1,000Mbps. Work is ongoing to increase speed by another factor of 10. Gigabit Ethernet is mainly used for corporate backbone networks but as costs fall it will be deployed all the way to the desktop.

UTP Ethernet is a point-to-point topology. Each Ethernet outlet must be connected to a hub. The hub allows devices to talk to each other, remember the party line analogy. CDMA/CD used by Ethernet places a limit on how may wire segments and hubs can be used between devices. 10Mbps Ethernet uses the 5-4-3 rule, Maximum of 5 wire segments and 4 hubs between devices, however only 3 of those hubs can have devices attached. Because 100Mbps Ethernet is so much faster the rules are more stringent, maximum of two wire segments and two hubs betweens devices, and the distance between hubs is limited to 5 meters. For all intents and purposes 100Mbps systems are limited to a single hub.



Fast Ethernet runs into a problem if the user needs to increase the number of ports in a room. If another hub is used the topology rules are violated. The solution is to use a switching hub as the main hub. Switching hubs isolate each port. A port can start transmitting even if others are using the LAN. Switching hub connect data coming in on a port to a single outgoing port. This allows multiple connections to exist at a time increasing overall bandwidth. If a switching hub is used as the main hub conventional hubs can be used at each computer location to increase the number of ports without violating topology.

5.2 PhoneLine Networking

The Home Phoneline Network Alliance has developed a method using existing phone wiring to create a 1Mbps Ethernet type LAN. This allows computers to be interconnected wherever a phone jack exists. They are working on a second-generation specification to increase speed to 10Mbps.

Home PhoneLine LAN use Ethernet packets with minor changes to the header. The physical layer hardware adds the unique header information for transmission and removes it on reception. This make HomePNA look like any other Ethernet LAN to the software drivers.

HomePNA equipped computers cannot connect to UTP Ethernet directly, a device called a bridge is needed to rate match between the two networks and deal with signaling difference. Adapters such as the Linksys Network Bridge can be used to connect a HomePNA LAN to Ethernet

5.3 RF Wireless LANs

Traditionally, RF has been expensive and provided relatively low bandwidth. RF LAN makes sense where mobility is more important then speed.

IEEE 802.11 is an industry standard 2Mbps Radio LAN designed for use within a large building. The LAN can be configured with multiple micro cells to increase total bandwidth. IEEE is working on a second generation of the standard, which will increase data rates to 11Mbps. This makes Wireless LAN much more attractive.

HomeRF is an Intel led initiative to standardize on a low cost RF solution for home use. It will provide a low cost mechanism to communicate with relatively low bandwidth devices (1mbps). The initial target is a wireless phone with data capability.

BlueTooth is addressing shortrange (<10meters) personal area network market. The goal is to link multiple portable devices together. A higher power version extends the range to 100meters. Typical uses of Bluetooth are to allows a PC, cell phone, and, Palm Pilot to exchange data.

Significant overlap exists between the three competing RF LAN technologies. For the foreseeable future RF technology is be best where mobility is of paramount importance and wired LANs with large bandwidth requirements.

5.4 TCP/IP

The LAN uses the Internet Protocol (IP) to connect local devices. Using the same communication protocol for the LAN and the Internet simplifies configuration and management of the LAN. IP is the mechanism used to deliver a packet of data from one computer to another. TCP stands for Transmission Control Protocol. IP is an unreliable delivery mechanism it launches packets to the Internet; they may arrive out of order and not at all. TCP orders the incoming packets and requests retransmission of any that are missing. When applications make a TCP/IP connection the receiver sees the same data stream that was transmitted.

A simpler protocol UDP/IP User Datagram Protocol is used when end-to-end synchronization is not required. UPP is a connectionless protocol. The transmitting station simply casts the packets out to the Internet. Each packet is dealt with individually. UDP is often used with multimedia. If a packet is lost it cannot be retransmitted in time so the receiver has to fake the missing information.

5.5 IP Addresses and Names

Each device (node) must have a unique address. Addresses can be assigned, statically, automatically by DHCP (Dynamic Host Control Protocol) or automatically by the client when DHCP is not present. Traditionally the system administrator configured each device with an address. This was labor intensive and error prone. DHCP simplified the task by centralizing address assignment. The down side is a DHCP is required to allocate addresses. Recently DHCP has been extended to allow automatic configuration if the host cannot find a DHCP server. In that case the device assigns itself an address after failing to find a DHCP server and determining the address is not in use. This is convenient for small LANs that use IP and do not have access to DHCP.

The Internet Assigned Number Authority assigns Internet addresses. That is who assigned the addresses used by your ISP. IANA allocated three blocks of private addresses that are guaranteed not to be used on the Internet. The private addresses are ideal for a small LAN. Devices on the LAN are assigned from the pool of private addresses. When the LAN is connected to the Internet the gateway uses a technique called Network Address Translation (NAT) to convert the private IP addresses to the single IP address assigned by the ISP.

In our implementation DHCP is built into the Wingate proxy server. We use Class C private addresses in the range of 192.168.0.x this allows up to 254 hosts on the LAN. The IP address of the Gateway LAN adapter is statically assigned as 192.168.0.1. The DHCP server then assigns an IP address to each client from the pool of remaining addresses.

5.6 Dotted-Decimal Notation

Internet addresses often expressed as four decimal numbers separated by a period. The 32-bit address is divided into four 8-bit fields. Each field has a range of 0-255.

5.7 Subnetting

IP addresses consist of three parts, the Network-Prefix, Subnet-Number and the Host Number. The purpose of Subnetting is to allow IP addresses to be assigned efficiently and simplify the task of routing packets through the internetwork.

For our purposes all the computers on the network must be on the same subnet. For example our network allows up to 254 hosts (computers) the subnet is 255.255.255.0.

5.8 Port Numbers

A single computer may be connected to multiple hosts over the Internet. How does the computer know how to deliver each packet? For example, while writing this paper my mail program is checking e-mail, and I'm listening to a Real Audio radio program. Each IP packet includes a port number. Port numbers are 16 bit values that range from 0-65,535. For example when you enter a URL into you web browser to access a World Wide Web site the browser automatically uses port 80. The low port numbers 0-1023 are called the well-known ports; they are assigned by IANA when a particular service is defined. Software uses that port to make initial contact. After the connection is established the high numbered ports are used.

5.9 Winipcfg

In Windows systems Winipcfg.exe displays the current configuration for each adapter. Each computer has a Network card and some have a modem. In addition to address and subnet two other important fields are Adapter address and Default Gateway. The adapter address is the hardware address assigned to the physical network interface. For Ethernet this is a 48-bit Media Access Controller (MAC) address. The Default Gateway tells IP software where to send packets that are not on the local LAN.

5.10 Nameserver - Domain Name Service

Entering long strings of numbers such as 192.168.0.3 is not very convenient. The Domain Name Service (DNS) allows a name to be used instead of a number. When you enter a name into your web browser such as http://www.yahoo.com the browser asks DNS to look up the IP number. If local DNS does not know it asks other DNS severs until the number is found. Once the system obtains the IP address it uses the address to connect to the remote host. DNS names are intended as a convenience for humans they are not used by the computers on the Internet. DNS acts as a giant Internet "White Pages."

The LAN needs a simple DNS server. Basically all it has to do is accept requests from the LAN and if the name is not one of the machines on the LAN pass the request to the DNS server operated by the ISP. In our implementation DNS is built into the Wingate proxy server.

5.11 Network Neighborhood

Windows network neighborhood allows one to browse networked computers. To show up in the neighborhood each machine must be configured for file and print sharing, even if devices are not being actively shared. The neighborhood is grouped by workgroup names, in a small LAN all machines typically belong to a single workgroup, like HomeLAN. At least one machine in each workgroup must be configured as the Browse Master. Ideally this is a machine that is left on all the time. Browse Mastership is negotiated at power up; in general it is a good idea to disable the Brows Master on the client machines. If the browsmaster is running on a client, the network neighborhood becomes temporally unavailable when the client is turned off, until the remaining machines rearbitrate browsmaster ownership.

Security Tip – File and print sharing is a much-debated topic. By default file and print sharing is configured to be accessible to all interfaces. Sharing should be disabled on the interface used to connect to the Internet, if this is a modem go to Networking on the Windows control panel find the entry that starts TCP/IP -

>Dialup Adapter, go to Bindings and uncheck “File and Printer sharing for Microsoft Networks.” Unchecking this feature prevents access to shares by anyone on the Internet while still allowing access from the LAN.

Configuration Tip – Force the Gateway server to always be the Brows Master. This guarantees Network Neighbor is always available. Go to File and Print sharing in Network control panel. Open the Advanced tab, highlight Browse Master and change the Value to Enabled. Set it to disable on each client.

5.12 Implementation

The LAN was wired using Category 5 wiring. Currently the hub is 10BaseT. At the time of installation there was a significant cost difference between 10 and 100Mbps hubs. Costs are falling rapidly. For new installations a 10/100 hub is preferred, with clients using 10/100TX network cards. This allows both 10 and 100Mbps computers use the LAN. The hub does rate matching when different speed hosts exchange data.

6 Sharing a Single Internet Connection

The LAN cannot simply be “plugged in” to the Internet. On a small LAN all hosts communicate by broadcasting information to all other hosts. This works well on small systems but will overwhelm large systems. Routers are used to keep traffic on different network segments separate. They monitor packet traffic and only transfer packets bound between segments. This allows multiple segments to communicate while keeping local traffic local.

The LAN private addresses must be converted to the single IP address assigned by the ISP. This is called Network Address Translation (NAT). This allows multiple computers to use a single ISP account.

Hardware appliances or software running on a PC can perform web access. We use a dedicated Pentium laptop PC, running Windows 98 Second Edition as the gateway. A laptop was chosen for its low power consumption and small size. Wingate was chosen to perform Internet Gateway functions and other low level IP (DHCP and DNS).

6.1 NAT and Proxy service

Wingate is a proxy server, acting on behalf of the user. When a proxy is used applications do not access the Internet directly, instead they pass the request to the proxy, the proxy in turn examines the packet to determine if it should be allowed to pass. If the packet is acceptable it is modified with the proxy as the source address. When a response is returned it is examined, and if allowed, the address is changed back to the original address and forwarded to the requesting device. Proxies are valuable because they completely hide the LAN from the Internet. Internet hosts only see the proxy; all requests appear to originate from the single proxy computer. Because all requests go through the proxy multiple PCs can share a single Internet connection. The proxy maintains the bookkeeping to keep track of where each packet originated from so responses can be returned to the proper computer. The downside is that Internet applications must be proxy aware. Each application Browser, Real Audio, etcetera must be setup so it knows how to access the proxy; this involves setting the proxy server name and port number for each service.

Configuration Tip: -- Use the Computer Name from network setup as the name of the proxy server. In Control Panel go to Network, and then click the Identification tab to get the computer name. In the past I used the name Wingate, since the Proxy is also a DNS server it knows how to resolve the name Wingate. However, Windows 98 changed name resolution so that not longer works.

To simplify client configuration Wingate version 3 includes Windsock Redirector Protocol (WRD). This eliminates the need for Proxy aware application. This is especially important for games that tend to assume direct dialup access. WRP runs on each computer and automatically redirects TCP/IP requests to the Wingate Server.

6.2 Demand Dialer

When any computer on the LAN requests a resource that is not local the demand dialer automatically connects to the ISP. When the connection has been idle for a while it is automatically terminated.

7 Firewall and Intrusion Detection -- Keep the Bad Guys Out

Being connected to the Internet is a double edge sword. Your computer can communicate with millions of other hosts. At the same time a small percentage of those millions of hosts are interested in doing mischief on your system. The problem is most serious with permanent connections such as DSL and Cable Modems, but even dialup users are exposed to attack. The Proxy (Wingate) effectively hides the computers on your network, except the one directly connected to the Internet. The security of your entire network is determined by how well protected this machine is.

File and print sharing should be disabled on the interface used to connect to the Internet. You should not access unknown web sites or run a mail client on the Gateway machine. This minimizes the risks a Trojan virus being secretly installed on the Gateway. Hacking exploits often involve searches for machines compromised by Trojan software. The latest security fixes should be installed on all machines. One Windows platforms the Windows Update feature is very convenient. Clicking on Update take you to the Microsoft site, it checks machine configuration and displays a list of recommends updates. These are downloaded and installed with a few mouse clicks.

A dialup user can expect to be port scanned every couple of days. For DSL or Cable modem users this happens multiple times per day. The port scan is like a thief checking to see if your doors are locked. In general the person scanning your computer is not looking at you specifically. They want to find a machine to compromise to hide their identify while attacking another computer. If your computer is used in this manner it looks as if the attach came from your machine.

To increase security a Firewall is inserted between the Internet and your computer. The firewall looks at each packet to determine if it should be allowed to pass. A firewall can be a physical device or software running on the gateway machine. A SOHO site is pretty easy to secure since all traffic originates from inside, any traffic originating from an external host is rejected. This assumes you are not running a public web server on your network. In most cases using a web-hosting service is a better choice then running your own public web server.

Firewalls provide Intrusion Detection. For better or worse you get to see all the access attempts. I chose a new product BlackICE Defender. This is billed as a personal firewall. Normally configuring a Firewall involves setting up a number of rules. This is done automatically in BlackICE by selecting the level of paranoia. In addition to the security setting it looks for attack signatures. This is analogous to a Virus scanner; it looks for suspicious activity and blocks access from that host.

Several sites offer free services that perform port scans to determine vulnerability. Secure-Me at DSLReport Demo Scan at HackerWacker and Shields Up at Gibson Research run a series of tests to see which ports are open.

No security measure is able to guarantee that you will not be compromised but these steps go a long way to hardening your site, reducing the odds.

Installation Tip: -- The default configuration for BlackICE Defender is to monitor all network ports. It needs to be configured to ignore your LAN interface. The BlackICE knowledge base article describes how to set this up `KB:q000023`.

Usage Tip: -- The current version of BlackICE misinterprets some normal activity as an attack. The most common cause is Tracert or other Internet Trace Route programs. These attacks will appear to be coming from your LAN so they are easy to identify.

8 Debug -- When Things Go Wrong

Unfortunately networks occasionally fail. When a system failure occurs it is often difficult to determine the underlying cause. Luckily, Windows includes a number of built in diagnostic tools.

Test	Result
Ping by IP address	Two machines can successfully connect
Ping by Name	DNS is working, Two machines can connect
WinIPcfg	Network adapter settings
Net View	DOS version of Network Neighborhood
Netstat -a	Active Ports
Tracert or Visual Route	Host to host path
Modem Test	Modem venders self test

8.1 PING

Ping is a command line utility to determine if a remote machine is reachable. The host is specified by either IP address or domain name. Ping uses the Internet Control Message Protocol (ICMP) to determine round trip time to the remote host. In the first example we Ping the gateway on the local LAN by its IP address. In the second case we Ping a public web server on the Internet by its domain name. Notice that domain lookup functions correctly, the name is translated to the server IP address, but Ping itself failed. This is because ICMP is not propagated through the firewall. Performing Ping from the gateway returns correct round trip times because it does not go through the proxy.

Example 1: Ping to local host by IP address.

```
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum =  2ms, Average =  1ms
```

Example 2: Ping to remote host by DNS Name.

```
Pinging tschmidt.com [198.77.209.186] with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 198.77.209.186:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
```

```
          Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

8.2 Net

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

```
NET CONFIG     Displays your current workgroup settings.
NET DIAG       Runs the Microsoft Network Diagnostics program to display
               diagnostic information about your network.
NET HELP       This list
NET INIT       Loads protocol and network-adapter drivers without
               binding them to Protocol Manager.
NET LOGOFF     Breaks the connection between your computer and the
               shared resources to which it is connected.
NET LOGON      Identifies you as a member of a workgroup.
NET PASSWORD   Changes your logon password.
NET PRINT      Displays information about print queues and controls
               print jobs.
NET START      Starts services.
NET STOP       Stops services.
NET TIME       Displays the time on or synchronizes your computer's
               clock with the clock on a Microsoft WfW, Windows NT,
               Windows 95, or NetWare time server.
NET USE        Connects to or disconnects from a shared resource or
               displays information about connections.
NET VER        Displays the type and version number of the workgroup
               redirector you are using.
NET VIEW       Displays a list of computers that share resources or a
               list of shared resources on a specific computer.
NET ?          This list
```

8.3 Netstat

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

```
NETSTAT -a         Displays all connections and listening ports.
NETSTAT -e         Displays Ethernet statistics. This may be combined
                   with the -s option.
NETSTAT -help      This list.
NETSTAT -n         Displays addresses and port numbers in numerical
                   form.
NETSTAT -p proto   Shows connections for the protocol specified by
                   proto; proto may be TCP or UDP.  If used with the -s
                   option to display per-protocol statistics, proto may
                   be TCP, UDP, or IP.
NETSTAT -r         Displays the routing table.
NETSTAT -s         Displays per-protocol statistics.  By default,
                   statistics are shown for TCP, UDP and IP; the -p
                   option may be used to specify a subset of the
                   default.
interval           Redisplays selected statistics, pausing interval
                   seconds between each display.  Press CTRL+C to stop
                   redisplaying statistics.  If omitted, netstat will
                   print the current configuration information once.
NETSTAT ?          This list
```

8.4 WinIPcfg

WinIPcfg is a Windows utility that displays how each communication adapter is configured. The most important fields are the IP addresses and subnet mask. The subnet mask must be the same for all hosts on the LAN.

8.5 Trace Route

Trace Route uses Internet Control Message Protocol (ICMP) to find each hop between the user and the remote host, and the delay to each hop. This is very useful to determine the underlying cause of slow or unavailable hosts. Trace Route uses the Time To Live (TTL) field to cause the ICMP packet to be rejected because it has gone through too many hops. When this occurs the host informs the sender that the packet has expired. Trace route uses this information to built a path map and list response time to each hop between the source and destination.

The Windows version of Trace Route is TRACERT.EXE a command line utility. VisualRoute provides the same information as tracert in a graphical format. In addition it performs a WHOIS lookup to determine where the site is located and who owns it. This information is then displayed on a map to show overall routing.

9 Browsing -- Wild Wild Web

All PCs use Microsoft IE5. The browsers are equipped with 128-bit encryption for added security.

10 E-Mail -- Mail at the Speed of Light

E-mail services fall into three broad categories; ISP account, browser based free mail, and your own mail server. ISPs typically offer one or more mail accounts. This is convenient but ties your e-mail address to your ISP. Change ISP and your e-mail addresses changes. Free mail services like Yahoo and HotMail are advertising supported. They decouple your e-mail account from your ISP. Free accounts make sense for personal use. Even though they are advertising supported the advertising is not overly intrusive. If you have registered a domain name your mail is addressed to you@yourdomain.com. If you change the hosting service you simply transfer you domain to the new provider. They change DNS lookup and no one will notice the change.

Initially we intended to setup an internal mail server. The web hosting service dumps all mail for the domain into a single account. The mail server retrieves incoming mail, examines the name and sorts it into the proper mailbox. This eliminates the hassle and cost of having the ISP manage account adds and deletes. We have not set this up yet because the personal free mail service is working well for family members. It has the advantage that any computer can be used to check mail it does not require a mail client or that the computer even be on the LAN, just that is has Internet access. The domain mail account is reserved for business purposes.

10.1 ABC’s of Internet Mail

Free E-mail accounts use the browser eliminating the need to install special software. Heavy e-mail users typically use and E-mail program, such as Microsoft Outlook.

Internet mail has a sending component, SMTP, and incoming part called POP. When you compose and send e-mail your mail program connects to the SMTP (Simple Mail Transport Protocol) mail server. The SMTP server acts as a relay between your e-mail reader and the Internet. Incoming mail is delivered to the POP server, (Post Office Protocol) maintained by the ISP. It works much as a post office box. As mail is received it is temporally stored in your mailbox until you have a chance to retrieve it. The e-mail program connects to the POP sever and downloads the mail. Normally it automatically deletes mail once it is transferred but this can be overridden so mail remains on the server.

Security Tip: -- Hackers use e-mail to spread viruses and worms. A good precaution to not open mail attachments unless you know the sender.

Security Tip: -- The aforementioned warning has been issued many times. What is less well known is that simply reading e-mail can infect your system. ActiveX controls or VB scripting can be embedded in the body of a mail messages. Reading the message activates the virus.

Security Tip: -- Spam is a big problem. Many ISP's restrict SMTP access to customers only. This means if you have multiple ISPs or a domain hosting service you may not be able to use a particular SMTP server. This is a minor inconvenience since any SMTP server can be used to relay outbound mail.

11 Fax – E-mail on Paper

Originally we did not want to use fax, preferring to interact with clients via e-mail. We found it is very difficult to get away from fax completely so we sought a solution that did not require a "real" Fax machine.

For incoming fax we use the eFax.com fax service. Basic service is free, if you want a local or 800 number they charge a monthly fee. Each customer is assigned a unique phone number; in our case 520-223-4815. When a fax comes in it is converted to a file and e-mailed to the subscriber. On the subscriber's machine special eFax software reads the attachment. The attachment can be saved and imported by other programs.

To send a fax we use Phone Tools that Dell bundles with its PCs. This allows direct faxing of electronic documents or scanned hard copy.

This works well for the limited number of faxes we use.

12 Newsgroups -- All the News Ready or Not

Most ISPs carry USENET news groups. USENET gives you access to ongoing discussions on a wide verity of topics. There are an incredible number of groups to choose from, our ISP carries 44,000 news groups. Most groups have a FAQ that describes what the group is about to limit off topic posts. Each group is interested in a specific topic; members are usually very vocal in discouraging off topic posts. Newsgroups are a valuable source of information. Given the incredible number of users it is likely that someone will be able to provide an answer to your question.

We use Outlet Express as the newsreader. Outlook must be configured to use the Wingate proxy or the Wingate WRP to access the news server.

13 Audio -- Tunes from Around the world

Using the Internet to deliver streaming audio or video is hampered by the low data rates available to dial up user. To overcome this limitation multimedia is heavily compressed. Two compressed audio format are commonly used on the Internet Real Audio and MP3.

13.1 Real Audio

Real Audio is the most popular format for streaming audio and video. The basic client player is free. The player must be configured to use the proxy or Wingate WRP software must be loaded on the client.

Real Audio multimedia compresses the stream so that is can be delivered in real time over a dialup connection. Many web sites use real audio to deliver multimedia and many radio stations provide live feeds over the Internet. Broadcast.com and BroadcastMusic.com are two sites that serve as portals to music sources.

13.2 MP3

Higher quality audio is available using the MPEG MP3 compression format. This provides near CD-quality sound at approximately 1/10 the data rate. Typical MP3 content is delivers at 110-125kbps. That is 2-3 times faster then V.90 modem so it cannot be delivered in real time. The real audio G2 player includes MP3 playback support but web audio aficionados prefer the WinAmp player.

14 Atomic Time -- Setting Your Watch on the Internet

The Internet allows access to accurate time standards. This eliminates the problem of drifting and inaccurate computer clocks. We use a program called Tardis 2000. The software runs on the server and monitors for active dialup. When the server is online Tardis periodically polls one of several timeservers. In the US the National Institute Standards and Test (NIST) maintain a number of public timeservers. It uses this information to set the Real Time Clock (RTC) on the gateway server. Included in Tardis is a Network Time Protocol (NTP) timeserver that periodically broadcasts time over the LAN. A companion program, K9, runs on each client. It updates the local RTC to match the time on the server. This insures all computers are slaved to the server and the server is synchronized to official time when the system is on line.

NIST Network Time Service use multiple stratum-1 timeservers located in Boulder Colorado, Gaithersburg, Maryland (Washington, D.C. area) and Redmond Washington. Tardis should be configured for each of the addresses. If a server is not working Tardis automatically gets time information from the next server in the list.

The timeservers are extremely accurate, however accessing the server via the Internet adds several hundred milliseconds of round trip delay. That is not a problem for our purposes.

Security Note: Tardis 2000 defaults to time broadcasts on all available interfaces. This should be changed to use just the LAN connection, typically 192.168.0.255. 255 is the broadcast address. If this is not done each time broadcast is sent out over all ports including the one connected to the Internet. This will prevent the dialup connection from timing out and probably annoy your ISP.

Configuration Tip: Limit how often Tardis connects to the Internet Time server, this reduces unnecessary load on the public timeservers. We set Tardis to poll once every 2 hours when online.

15 Printing – Data to Paper

Network printing allows any computer on the network to access the printer. Printers can be shared by using a network ready printer, an external print server, or Windows print sharing.

The printer is setup to use Microsoft peer-to-peer printer sharing. This allows a printer to be shared by all Windows machines. The printer is connected to the Gateway server parallel port. Each client machine is configured for network printing. In general this has been acceptable but a number of shortcomings have come to light.

- Not able to observe print status on clients
- Cannot abort in process print job
- Sending simultaneous jobs from different PCs occasionally cause print failure
- Activating the dialer occasionally aborts print jobs

We sought to overcome these limitations with an external print server. The print server was connected between the printer and the LAN, eliminating dependences on the gateway server. Print server configuration was done with a PC browser. Any PC could look at the print queue and paper status. However, we could not make the server work. It turns out many low cost printers use GDI (Graphics Data Interface). A GDI printer offloads print rendering to the PC, unfortunately this precludes the use of a print server.

For the short term the printer stays connected to the Gateway. When it is replaced it will be by a network printer.

16 Scanning -- Paper to Data

A flat bed scanner was added recently. This allows any document or photograph to be converted to an image file. These files can be faxed or incorporated into other documents. Text documents can be processed by Optical Character Recognition (OCR) software to convert the graphics images to text that can be understood by text editors. The scanner is an Umax 2200 it uses USB to connect to the computer.

The scanner also functions as a poor mans copying machine. Scanned images can be sent directly to the printer.

17 File Sharing --Sharing Your Stuff

One of the benefits of having a network is the ease with which files can be transferred between machines. The Gateway is used as a software repository. Applications, patches and drivers are in a shared directory. This makes it convenient to access these file when building a new system or performing an upgrade.

Windows makes connecting to remote drives easy. The user can connect to a remote drive as needed or Windows can automatically connect at boot time. Mapped drives show up as additional drive letters.

Security Tip: having machines automatically connect to the shared drive is a potential security risk. Some of the most dangerous viruses look for shared drives. If they find a shared drive they can wreak havoc on it not just the machine the virus is on.

18 Off Line Backup – Preventing Murphy’s Law

There is nor substitute for off line backup. If your data consists of a few e-mails and self created documents a few floppies will suffice. To backup more data requires tape or a Zip Disk.

I chose Zip Disk because it functions as either a backup medium or as a large floppy. Zip Drives come in 100Megabyte and 250Megabyte versions. I chose the 100MB because it is the most common. I underestimated the size of backup data. User data on the office machine is approximately 1Gigibyte requiring 10 Zip disks. Next time I’ll pick a larger backup device.

19 Virus Protection -- More Keeping the Bad Guys Out

A sad fact of life is that a significant number of talented individuals take delight in wreaking havoc on the systems of people they do not know. Running an anti virus program goes a long way to reducing that risk.

We use Mcafee VirusScan. This is configured to verify e-mail and downloads in addition to files on the hard disk. Automatic update is not proxy aware preventing its use on the LAN. The workaround requires we periodically check the Mcafee download page.

It is unnecessary to run the anti virus program on the gateway since unknown software is never downloaded and it is not running a mail client.

20 Telecommuting -- Staying Connected on the Road

Windows networking makes it difficult to use a PC in different locations. Much network configuration is static, non-discoverable, and sprinkled through out the system. Initially we used a program called NetSwitcher to change configurations between LAN and dialup use. NetSwitcher works by editing network setting in the Windows Registry. It works well enough within its design scope but does not provide a mechanism to modify Outlook Mail, Real Audio, PointCast, or other Internet based application. This is a problem because these applications require unique configuration to work through a proxy. When used on the road the proxy is not available requiring changes to these applications before they can be used.

Wingate version 3 includes a Windsock Redirector Protocol (WRP) called the Wingate Internet Client. This solves the problem when transitioning between a Wingate proxy LAN and a dialup connection. Applications do not have to be configured to use the proxy. When WRP is turned on it automatically routes all external requests through the proxy. To move between locations WRP is turned on or off.

This does not address the requirement of corporate users that want to use the same machine for dialup on the road, at home on a LAN, and at work on the corporate LAN. Corporate LANs requires different settings then the home LAN. NetSwitcher could be used but it is not a complete solution because it cannot reconfigure all network applications. Some corporate networks use a script to configure the browser. The browser points to a URL where the script is stored this automatically configure the browser but it does help with other programs.

What is needed is a discovery mechanism so the computer can set network parameters automatically. As small networks become more prevalent this issue will be resolved. In the future systems will be much easier to use in multiple locations.

Mail Tip – If you use a desktop and a laptop computer configure the mail reader on the laptop to leave mail on the POP server. This allows it to be read by both the laptop and desktop system.

21 Private Web Server – Your own miniWeb

The home page of each browser points to the web server running on the gateway machine. This allows relevant information to be posted on the web server and shared with all systems on the LAN. The goal is to use the server to distribute live information, weather data, security status, etcetera. Currently the server is limited to static pages. The server is freeware called Xitami from iMatrix. Originally we used Microsoft PWS but ran into a problem because it binds itself to all network interfaces, this means it is accessible from the local network AND the Internet. Xitami is configured to only use the LAN adapter, preventing access from the Internet

Shared software is placed on the web server to simplify distribution. This has not turned out to be as useful as expected. It is more convenient to access software as shared files then via the browser. Programs can be installed directly from a shared file whereas when using the browser they must downloaded to the local system. The solution was simple files are placed in a shared subdirectory on the web server. This allows files to be accessed by the browser or as a remote drive.

HTML pages can be created at a low level using a text editor or with software specifically designed for web creation such as Microsoft FrontPage.

Security Note: Make sure the web server can only be accessed from the LAN to prevent unauthorized access from the Internet.

22 Web Hosting -- Your Presence on the Web

Using a web hosting service allows a small business to maintain a 24/7web presence regardless of how the office is connected to the Internet. The service provider maintains the servers and provides high-speed Internet access. We use the same company for both web hosting and dial up access http://www.inr.net. A secondary benefit of outsourcing the public server is the LAN does not have to allow access from Internet hosts, dramatically easing the task of securing the LAN.

Many ISPs allow customers to set up public web servers. You are assigned a name that looks something like http://www.ISP.net/~yourbiz. This uses the domain name of the ISP as the starting point for your web site.

HTML pages can be created at a low level using a text editor or with software specifically designed for web creation such as Microsoft FrontPage. The pages are created off line on a development server then uploaded to the production site.

23 YourDomain.com – Your Name on the Web

Registering a domain name helps to identify your business and prevents changes in ISP or hosting service providers from affecting your customers. Once you have a registered domain name it can be transfered to a different service provider without impacting your public persona.

23.1 Naming Convention

In the DNS section we discussed how domain names map to IP addresses. They provide a friendly handle to access a particular site. Domain names are hierarchal, the highest level is called the top-level domain (TLD) these are the .COM, .EDU, ORG. .MIL and .GOV of the world. As the Internet expanded each country was assigned a unique domain. For example the TLD for the United Kingdom is .UK. Within each domain various agencies are responsible for name assignment. This has been the source of much controversy in recent years but need not concern us here. The role of the agency is to insure each domain name is unique within a top-level domain. For example in our case the "schmidt" domain was already assigned so we picked tschmidt.com. Sometimes a company adds additional sub domains such as www.tschmidt.com for web access, mail.tschmidt.com for mail etc. The hierarchy is evaluated from right to left. The right most name is the TLD.

23.2 Registering Your Domain Name

The first choice is to decide which TLD is most appropriate for your business. You can register the same name in multiple TLDs this is typically done when a company has a valuable tradename.

Hosting companies typically provide automated tools to register and setup a domain. They coordinate with InterNIC or other registration agencies. The registrar database is examined to insure the new name is unique within the TLD. The new name is assigned provisionally in case it has recently been allocated from another registrar. The ISP updates their DNS name server database to translate the domain name to the IP address of your web server. This can be a server shared with other businesses or you can collocate your own equipment at the ISP site. This is a business decision that depends traffic volume and the type of site you intent to set up. Obviously an e-commerce site driven by a catalog database with credit card authorization is much more demanding then a simple static web presence.

InterNIC has a two-year initial registration, after that it must be renewed every year or the name lapses.

Once the registration process is complete you need to create the web site itself. Sites range from simple ones that provide static information to complex database driven e-commerce. The hosting service provides a log file of everyone that visited the site and what pages that look at. This data can be analyzed off line to understand how customers navigate your site.

The hosting service will also provide e-mail service. E-mail is structured as username@domain.TLD.

23.3 WHOIS record for Tschmidt.com

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

   Domain Name: TSCHMIDT.COM

   Administrative Contact:
      Administrative Services  (AS935-ORG)  admin@TSCHMIDT.COM
      (603) 673-5804
   Technical Contact, Zone Contact:
      Network Operations Center  (NO153-ORG)  noc@INR.NET
      603. 880.8120
      Fax- 603.880.8783
   Billing Contact:
      Administrative Services  (AS935-ORG)  admin@TSCHMIDT.COM
      (603) 673-5804

   Record last updated on 04-Nov-1998.
   Record created on 04-Nov-1998.
   Database last updated on 5-Jan-2000 13:08:31 EST.

   Domain servers in listed order:

   NS1.INR.NET                  198.77.208.2
   NS2.INR.NET                  216.64.64.2
```

This is a good example of an outsourced web host. Administrative and Billing contacts refer to the company registering the name. The Technical Contact is the hosting service that own responsibility for translating host names to IP addresses. Notice there are two name servers, InterNIC requires a primary and alternate name server. The IP address for your site is allocated from the pool of addresses previously assigned to your service provider.

24 Conclusions

Setting up the network has been extremely successful and a great learning experience. The down side is a significant amount of technical expertise is required to set it up and failures occur fairly often.

Networking today is like to having an early horseless carriage (or a British sports car), when it worked it was exhilarating, but one needed a riding mechanic to keep the machine running. As networking expands beyond the province of corporate IT departments it will become easier to use until the point is reached where a non-networked device is unthinkable – bring on the Internet toasters.

Happy networking.

Last Page
Intentionally Blank