White Paper

Deploying
Internet connected
Small Business and Home LANs

This paper discusses the issues involved in connecting a small group of PCs to the Internet via a local area network. PCs are being used as the on ramp to the Internet. Communication has become more importance then their original compute role. All aspects of getting connected are examined, selecting and connecting to an ISP, LAN selection tradeoffs, security, and the special needs of laptop users.

Tom Schmidt
Schmidt Consulting
tom@tschmidt.com

August 9 1998
Revised January 28, 1999

Contributors:

Skip Gaede of Compaq Computer
I turn to Skip whenever I have Windows TCP/IP configuration questions.

Larry Huppert of Compaq Computer
Larry helped flesh out the user model.

Bill Laing of Compaq Computer
Bill's Secure Home (Inter) networking paper of April 1998 describes a similar home networking implementation. He provided generous help at the beginning of this project. His paper convinced me this topic was worth pursuing.

Jeff Schreriesheim of Compaq Computer
Jeff put me in contact with various folks working on Internet networking.

Table Of Contents

1   Introduction

This paper discusses the issues involved in connecting a small group of PCs to the Internet via a local area network. PCs are becoming the onramp to the Internet. As PC prices fall more and more locations need to resolve how to provide access to multiple computers and facilitate data sharing. The benefits of computing now depend on being well connected.

Connecting a single PC to the Internet is pretty easy. Consumer PCs are sold dialup network ready. ISP's typically offer software that automates browser and dial up networking configuration. At the other end of the spectrum large corporations have in-house Information Technology (IT) groups that have the expertise to manage hundreds or thousands of users. The difficulty occurs when the need is to connect a few PCs. The hardware and software components are readily available but they require a great deal of expertise to assemble and configure. This puts networking out of range for residential and small businesses.

PC penetration in the US home market is approximately 40%. Approximately 60% of US PC households have more then one. Once a site has more then one PC the opportunity exists to link them together. Interest in the Internet increases the importance of having a LAN. Without a LAN each computer is an island. When a computer is on-line none of the other computers are able to use the Internet. Implementing an Internet connected LAN allows multiple PCs to have simultaneous Internet access in addition to the benefits of file and print sharing.

The connectivity problem for small business is much the same as for home users. Businesses are eager to explore the benefits of network computing. They want Internet access to deploy virtual storefronts, online ordering, information exchange, electronic billing, etc. However, they lack the expertise to deal with complex networking issues. They must pay for expensive consulting services to get connected. A shrink-wrapped networking solution will be a boon for small business.

Another difficult problem is moving PCs between locations. As the numbers of intelligent devices grow users want to take them wherever they go. This is difficult today, because location specific information is sprinkled throughout the operating system, drivers, and applications. Lack of convenient connectivity limits the growth of these devices. A user should be able to simply plug the device into an information outlet, no fuss no muss.

Connected systems are vulnerable to attack from both the inside and outside. The implementation must facilitate easy access to the Internet while providing protection from malicious use.

Currently, much of the small network emphasis is focused on the physical connection; the wires and adapters needed to connect the computers. This is important, the simpler it is to connect computers together the more it will be done. However, another significant issue is the software that ties the devices together. Today it is fairly easy to use Category 5 unshielded twisted pair to connect multiple machines; large corporations do this all the time. The problem for small sites is that just connecting the devices together is not enough. One must have a great deal of specialized knowledge to configure the hardware and software. Ideally, a user simply plugs a new computer into the network, responds to a few simple questions, such as: "What do you want to call this computer?" and is up and running.

To gain experience, and understand the issues involved, I implemented a small Internet connected LAN. I tried to approach the problem from the perspective of the end user. I determined what I wanted it to do, and then tried to find products that worked. This White Paper is the result of that experience.

The Call to Action section discusses the technical innovation needed to simplify deployment of small Internet a LAN.

2 Requirements

This section describes the requirements for an Internet connected home LAN. It reflects the way my family and I use the Internet and our PCs. This is provides a base level feature set, once a network is deployed it is easy to add enhancements.

The features set described is also applicable to the needs of small business with 5-10 PCs.

2.1 LAN

The network provides a high-speed PC to PC connection. The LAN Alternative section describes the pros and cons of the various schemes. The LAN is Internet Protocol (IP) centric, no other transport protocols are implemented. Dynamic Host Control Protocol (DHCP) is used to automatically assign unique addresses to each device. Domain Name Service (DNS) is used to automatically translate the user-friendly NetBIOS system names to numeric IP addresses. All machines on the LAN show up in the Windows Network Neighborhood.

2.2 File Sharing

Files can be shared between computers. Sensitive files require password authentication.

2.3 Remote Printing

A common printer is accessible from any computer on the LAN.

2.4 ISP Access

Small sites typically use dialup Internet Service Providers (ISP) to connect to the Internet. The user places a phone call to a local ISP Point of Presence (POP). The connection typically uses Microsoft Remote Access Service (RAS) to authenticate the user. The Point to Point Protocol (PPP) is used to encapsulate IP traffic so it can travel over the phone link between the user's computer and the ISP.

The ISP uses Dynamic Host Control Protocol (DHCP) to assign an IP address when the connection is established. These addresses are "leased" for the duration of the connection. When the user disconnects the address is reclaimed and can then be assigned to different user. Due to the exponential growth of the Internet and the way address are assigned a critical address shortage exists. Assigning addresses dynamically means the ISP address pool need be only large enough to cover the actively connected users. If the ISP uses static addressing they must assign at least one address to each customer even it they are not connected. The ISP provides Domain Name Service (DNS) to translate numeric IP addresses to friendly names.

Ideally the POP is located near the user so the call is local. This is not a significant problem when using an ISP with a national or worldwide presence, such as AT&T WorldNet or Cables and Wireless. However, regional and local ISP's are at a significant disadvantage. The ISP industry has come up with an interesting solution to the problem called IPASS. It allows a user to access their home ISP from any participating ISP. The ISP recognizes them as a "foreign" user. The login information is passed to the user's home ISP for authentication. If the login is accepted the user has the same access as if they dialed the local ISP. There is a modest additional monthly fee for this service. This requires minor changes to the dialer when accessing a "foreign" ISP.

2.5 Internet Gateway

The gateway is responsible for linking the LAN and the ISP together. The Gateway is also responsible for providing LAN services. Each computer on the LAN needs its own IP address. The Gateway provides local DHCP (Dynamic Host Control Protocol) services that assign IP addresses to each client computer. The Gateway also provides local DNS to resolve computer names on the LAN. All machines on the LAN access the local DNS to resolve computer names to IP addresses. It knows the name and address of all the local machines because it used DHCP to assign their addresses. DNS automatically forwards request for

computers not on the LAN to the DNS provide by the ISP. The ability of DNS to be cascaded is what makes it so powerful. If a name cannot be resolved the request is passed up the DNS chain.

The Gateway must convert the IP addresses of the machines on the LAN to the IP address issued by the ISP. The Gateway uses NAT (Network Address Translation) to map the unique private IP address of each LAN client to the single IP address issues by the ISP.

The gateway automatically dials into the ISP whenever clients access a non-local resource. This requires an intelligent interface between the modem and the telephone line. Otherwise, the modem may attempt to dial out when the line is in use. In a two-line installation the modem should automatically search for an idle line. These are the tasks performed by the Modem Access Adapter (see Appendix). It automatically searches for an idle line when the modem attempts to place a call. If it finds one it disconnects the attached telephones to prevent them from interfering with the data call.

2.6   FireWall

Connecting a LAN to the Internet means THE LAN IS CONNECTED TO THE INTERNET. Without a firewall all PCs on the LAN are visible on the Internet, clearly not a desirable state of affairs. The job of the firewall is to control the flow of information between the LAN and the Internet. A proxy server implements the firewall function. Client requests are passed to the proxy server. The proxy examines the request, if it is allowed it is forwarded to the proper computer, if not the request is discarded. Incoming Internet traffic is examined to determine whether it is a response to a LAN generated request or it originated from outside the firewall. If the firewall accepts the data it is forwarded to the proper client. Requests that originate outside of the firewall are rejected.

2.7   Web Browsing

The gateway and clients are all equipped with web browsers. All users have access to the web

2.8   Private Web Site

A local web site is used to share information. It has a wide range of uses such as information sharing, video feeds, and home automation like X10 or CEBus Devices, and security systems. The web site is inside the firewall only members of the LAN have access.

In a dialup environment remote access is not practical. However, when DSL and cable modems are deployed it will be possible to utilize Virtual Private Network (VPN) techniques to securely access the private server from anywhere on the Internet. This allows authenticated user to access the private web site.

2.9   Public Web Site

It is assumed the public web site will be hosted by the ISP. This eliminates the slow last mile bottleneck and greatly simplified the security of the site. Web creation is performed locally, when it is debugged the files are uploaded to the ISP web server.

2.10 Time Synchronization

It is important to maintain accurate time and date with connected PCs. Updating and file sharing experience problems if the machines do not have an accurate time reference. PC real time clock accuracy is rather poor. The real time clock may vary by as much as a minute a month.

Once again the Internet comes to the rescue. The IETF defined several protocols that transmit time signals across the web. This allows the PC clock to be slaved to the atomic clock time standard maintained by the National Institute of Standards and Test (NIST).

2.11 Remote Corporate Access

Telecommuting and satellite offices require remote access to the corporate network. This allows remote access to the same resource local users have.

2.11.1 RAS

Corporations typically provide dial up remote access for mobile workers. For PCs using Microsoft Windows the Point to Point Protocol is used over a dialup line to connect to a Remote Access Server (RAS). This enables a user to place a phone call to a company access point. The RAS server authenticates the user, once the user is authenticated LAN access is extended out to the remote location.

Security is primarily concerned with user authentication, the connection itself is assumed to be secure because it uses circuit switched telephone company facilities. The remote user is assumed to be an isolated PC, not a PC on a LAN. Little concern is shown for accidental sharing of sensitive data at the remote site.

RAS access causes difficulty with networked computers. Connecting via RAS and LAN access is not feasible; Windows 9x does not provide a mechanism to selectively route traffic. If a network connected user activates a RAS connection the RAS connection becomes very slow. Windows NT is more flexible it supports multihomed systems. Another disadvantage of this approach is that two-phone lines are required, one for the Internet connection and one for RAS.

Luckily we have an emerging technique that allows remote users to securely access the corporate network using their existing ISP accounts.

2.11.2 VPN

Companies are beginning to utilize VPN's to improve remote services and reduce the cost of linking remote offices and telecommuters to corporate headquarters. VPN's allow the Internet to be used to connect geographically dispersed sites at low cost. The remote user establishes an Internet connection, through an ISP then connects to the VPN access point on the corporate network. Both ends of the connection negotiate on how to encrypt the information between the two machines. From then on all communication between the two locations is encrypted, preventing it from being compromised. This technique is commonly called tunneling. It can be though of as a private tunnel between the remote user and the corporate site, no one else can access the traffic flowing between the sites.

VPN's are not only a great convenience for remote users; they reduce the cost of providing remote access. The company no longer needs to maintain multiple RAS locations with the associated modems and telephone lines. VPN is simply another form of IP traffic routed over the corporate backbone.

Telecommuter and remote office services require different VPN implementations. In the remote office case all members of the LAN are corporate employees. They typically have the same security privileges. IT has minimal concern that members of the LAN community will misappropriate each other's data. In a telecommuting environment household members may work for different companies. Each member needs secure access to corporate information without exposing it to other machines on the SOHO LAN.

This drives different implementation models. Remote office implementations use Gateway to Gateway tunneling. Data on each side of the gateway is unencrypted. The gateways provide a virtual point to point network that links the remote site to the corporate backbone. In the case of SOHO LANs the VPN tunneling software should located at the client. This allows sensitive corporate information to transverse the home LAN in an encrypted state. This minimizes the likelihood the data will be compromised. It also solves the problem of inadvertently connecting multiple corporate networks together at the telecommuter's site.

The IETF VPN standard is called IPsec. Currently the VPN market is dominated by proprietary implementations so it is important to install the same software at both ends of the link.

VPN's may also be used to remotely access the SOHO LAN. SOHO LANs that have a permanent Internet connection such as an xDSL, or Cable Modem can use VPN to allow secure remote access into the private LAN. Turning on your coffeepot from work is now within the realm of possibility.

2.12 E-mail

One of the benefits of Internet access is the ability to send and receive e-mail. Each person on the SOHO LAN should have a private personal mail account.

Some users will have multiple E-mail accounts. This is typically the case of personal and corporate E-mail accounts. The E-mail client must allow access to each account while maintaining security separation between them.

2.13 News Groups

Most ISP's provide access to Internet news groups. The discussion groups provide a good source of information on a wide range of topics. There are thousands of active news groups.

2.14 Chat

Chat rooms are the web equivalent of news groups. They have the benefit of operating in real time whereas there is a significant delay in transmission of new group posting. This are typically free services hosted by the various Internet portal sites.

2.15 Telephony

The near term implementation allows PC to PC Voice over IP phone calls. This uses standard third party software and the PC multimedia sound system.

2.16 Mobile Clients

As a laptop user I need to be able to use my notebook it at work, at home, and on the road. It is my primary interface to electronic communication. Unfortunately, a PC configured to use one LAN cannot simply be plugged into different one. This lack of connectivity reduces the value of mobile computing.

When traveling I want access to both business and personal information, while maintaining professional separation between them. Personal use of E-mail and remote access to a home LAN will become as commonplace as using a phone to call home. ISP roaming gives roadwarriors access to a common bitpipe (the Internet) to access both business and personal data without incurring corporate telecommunication charges.

When more then one PC is used to access the same information synchronization become a problem. Microsoft Exchange mail is an example of a mobile friendly application. The exchange server is the primary repository of mail messages. When a client connects to the mail server it may choose to view mail, download copies, or transfer mail from the server to the client. If the client views mail it must stay connected to read and compose messages. Downloading copies of e-mail maintains master copies on the server, and allows the client to compose mail offline, then reconnect to the server to resynchronize. Lastly the client can simply download all mail from the server. This makes the client the primary repository for mail. Only one PC can be used to access mail in this mode.

Roadwarrior wish list:

- Secure corporate access from anywhere
- Personal information access
- Easy roaming between different networks
- Strong Authentication
- Ability to use different computers to access information sources

- Maintain isolation between security domains

This requires the laptop reconfigure itself when it is moved to a different environment. When the unit is remote from the corporate campus it uses virtual private network (VPN) to maintain privacy.

2.17 Authentication

SOHO and remote offices require strong user authentication when connecting to the corporate network. This is necessary to insure the remote user is whom they claim to be.

In a home environment users may not require any authentication. Any PC connected to the LAN is assumed to be trustworthy and allowed full network privileges.

Wherever possible a single authentication scheme should be used so users do not have to memorize multiple passwords.

Authentication for laptop computers is extremely important since not only do they store sensitive information they allow remote access to corporate networks.

2.18 Manageability

Ideally all aspects of the SOHO environment should be configurable from a central location. Once the initial system is setup the system administrator can go to any client and log in. This relaxes placement issues of the various components and eliminates the need for keyboard and display on the gateway server.

Network distribution of software dramatically reduces the time it takes to configure the client machine. This allows a singe copy of software to be located on a central server to update all clients.

SOHO LAN is a good candidate for outsource network and computer administration. With proper authentication it should be possible to grant a third party access to the SOHO LAN. This requires that minimum functionality is always available to allow the remote help desk to take control of the network.

3 WAN Access Discussion

This paper is agnostic on the topic of WAN access. Obviously, a fast cheap interface is desirable. However, the physical WAN connection does not affect the basic design of the LAN. All that is needed is some form of Internet access the details are of secondary importance.

The first question to ask is -- how much bandwidth do we need? Lets look at the types of information flows between a typical home and the world at large. Digital TV requires approximately 20Mbps per channel. If we assume a four-person household each watching a different channel and one channel dedicated to thumbnails we need 100Mbps. Lets assume these folks have the radio going at the same time. CD quality audio is approximately 1.5Mbps. For a family of 4 we need another 6Mbps. Each person has a dedicated telephone line at 64kbps that requires another .25Mbps. Let's assume multimedia becomes popular and a lot of amateur photography is flowing across the web. A 5x7 photograph digitized at 1000 pixels per inch and 24 bits per pixel needs about 850Mbits to encode the picture. If we assume an acceptable transmission time is 10 seconds per picture we need another 85Mbps. Since it is unlikely each family member will do this at the same time lets assume 85Mbps is shared among all four members.

Other forms are electronic data are tiny in comparison. Let's say we decide to deliver newspapers and magazines electronically. A 200-page magazine has about a million and half characters, or 15Mbits, adding a small picture on each page at 1Mbit per picture costs another 200Mbits or approximately 215Mbits per magazine. This only requires a second to deliver to our theoretical home served via a 200Mbps connection.

In summary for a family of four we need:

Service	Bandwidth
Broadcast TV	100.00Mbps
Broadcast Radio	6.00Mbps
Telephone	.25Mbps
Interactive Data	85.00Mbps

Total	191.25Mbps

We may argue with the exact numbers but something on the order of 100-200Mbps is extremely interesting. The TV and radio bandwidth numbers assume some mechanism exists to select the channels of interest from those carried on the provider's backbone. Purely by coincidence the bandwidth is evenly split between multicast (broadcast) at 106Mbps and unicast at 85.25Mbps. It is interesting to note that voice telephony consumes about a .1% of total bandwidth, this is why the Telephone Companies are nervous about digital convergence.

3.1 POTS – Plain Old Telephone Service

This is the acronym for Plain Old Telephone Service. With the deployment of V.90 modems ISP's provide 56kpbs downloads and 33kbps uploads. This is the upper bound on analog transmission based on information theory. The bandwidth of the copper wire is large, however each voice channel is digitized at a 64kbps rate. This limits data transmission to no more then 64kpbs in each direction. Due to the way voice is encoded and FCC limits on transmit power real life data rates are somewhat less.

The latest generation of modems provide asymmetrical data rates. The stream that originates at the ISP is synchronized to the Digital T1 line. This eliminates sampling errors, increasing the data from the ISP to close to 56Kbps. The modem at the user site does not have access to the T1 clock so the data rate is limited by sampling theory to 33Kbps. This is no small feat, consider the analog bandwidth of the telephone voice channel is 300-3000hz.

In addition to relatively low bandwidth POTS connections incur lengthy connect times. The modem must seize the line, wait for dial tone, dial the number, wait for remote answer, trains the modems to line characteristics, and then authenticate the user. This typically takes tens of seconds. This makes dialup access unacceptable for spur of the moment use. Looking up a phone number, checking movie times on the web need faster connect time before they will be widely used.

The benefit of POTS is worldwide availability. It is the least common denominator of connectivity. Almost anywhere in the world a telephone is close by.

In addition to basic POTS the phone companies provide a number of value add services that affect data communications.

Call Waiting informs the user that another party is attempting to call while the line is in use. It disconnects the audio path to the remote phone and signals the local phone that another call is waiting by transmitting a series of tones. During this time the new caller hears normal ringback, the phone appears to be ringing. Temporally disconnecting the "talk path" causes the modem to hang-up. This disconnects the data call and allows the phone to ring. In a SOHO environment this "problem" may actually be a benefit. Customers pay for Call Waiting so they will not miss important calls. Disconnecting the modem allows the voice call to be completed, as soon as the line is idle the ISP connection is automatically reestablished by the LAN gateway server. Except for the delay in transmission this interruption is transparent. If file a transfer was in progress when the modem disconnected it can usually be restarted when connection is reestablished. Call Waiting can be disabled on a call by call basis by prefixing the call with additional touch-tone numbers. This dialing prefix can only be used on Call Waiting enabled lines, sending the prefix on normal lines causes the wrong number to be dialed. This is a significant problem for multi-line systems because the Call Waiting disable sequence cannot simply be included in the modem dialing commands.

Users of SOHO networking will likely require more then one telephone line. The Telephone Company can provision these as completely separate entities, or as a Hunt group. With Hunting when the called number is busy the Phone Company will automatically connect the call to the first idle phone line in the hunt sequence. This minimizes the likelihood callers will reach a busy phone. The Hunt order is unidirectional and is specified at the time of ordering. For example, if a caller dials the last number of a hunt group they will get a busy signal if that line is in use, even if other numbers in the hunt group are idle. Call Waiting can be used in conjunction with hunting but it must be on the last number of the hunt sequence

Another value add service is Caller ID. During ringing caller information is transmitted to the called phone. This uses the Bell 202 1200-baud half-duplex modem standard. On outgoing calls Caller ID can be turned off for all calls by the phone company or selectively, like Call Waiting, on a call by call basis. Disabling Caller ID does not disable Caller ID information to 800 or 911 numbers. Caller ID is hardwired to the telephone line. This is inconvenient where hunting is used. With hunting only the main directory number is "published," callers are discouraged from dialing the "hidden" numbers. It would be nice if Caller ID reported the main line number regardless of the actual line used.

3.2   ISDN – Integrated Services Digital Network

Integrated Services Digital Network provides digital subscriber services. Basic rate ISDN provides two full duplex 64kbps-bearer channels, and a 16kbs-control channel. ISDN is a circuit switched technology. It provides a value add subscriber service that maps directly to the long distance carrier infrastructure. POTS and ISDN both utilize the same 64Kbps digital voice channel.

One of the benefits of ISDN is very fast connection time. ISDN users consistently praise this as more important then the additional bandwidth. On the down side, ISDN deployment is spotty and getting it up and running can hardly be called plug and play. It is also rather expensive, With the mass deployment of V.90 analog modems ISDN does not look nearly as attractive as it did in years past.

ISDN calls are typically billed by the minute. This may make ISDN ISP access significantly more expensive then POTS calls with unlimited usage.

3.3   DSL -- Digital Subscriber Line

Digital Subscriber Line technology uses existing telephone company twisted pair copper wiring to provide high speed subscriber digital access. Depending on the implementation download rates are 600kbps-6mbps and upload rates are between 128kbps-1.5mbps. One of the advantages of DSL is that the data is not carried on the telephone company circuit switched network. DSL data shares the subscriber local loop used for POTS voice traffic, at the subscriber termination point the DSL data is stripped off and routed through an IP network. This means IP packet traffic is not carried over expensive telco circuit switched facilities, as is the case of ISDN.

DSL can occupy from 0.1 MHz (100 kHz) to over 5 MHz.
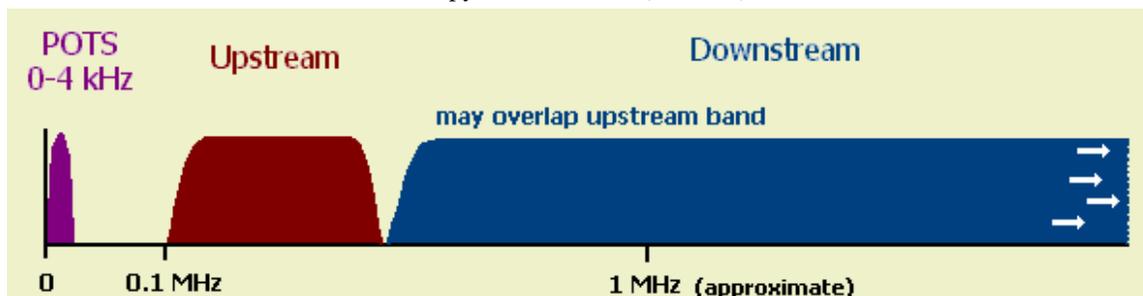
Going this fast over existing copper wires that were originally designed for analog voice service taxes the wiring infrastructure. Interference between DSL and other telephone services is a problem. Telco twisted pair wiring is lossy at these frequencies; this limits the distance between the telephone central office (CO)

and the user to 15,000-20,000 feet. Telephone companies use loading coils to improve voice transmission on long subscriber lines. Loading coils flatten the passband in the voice range (30-3000hz) but introduce significant attenuation at high frequencies. For DSL the loading coils must be removed. Another potential problem is bridging. When the Phone Company installs wiring they do not know exactly where it will ultimately be terminated. It is installed in such a way that a single pair can be terminated at more then one location. This makes it easy for the installer to find an idle pair when a customer orders telephone service. This increases loss and reflection for xDSL because the connection between the telephone company central office and the subscriber is not point to point but rather a tree structure with the trunk at the central office.

Another issue is Digital Loop Carrier (DLC). In order to minimize copper subscriber lines are frequently digitized remotely. When DLC is used multiple subscriber lines terminate at a remote DLC. The DLC equipment digitizes the subscriber line and multiplexes multiple lines on a single digital link that runs back to the central office. To support DSL the DLC equipment must be modified to split out digital data. The data is then sent to a hub and the hub is connected to new carrier facilities that route the IP traffic back to the central office.

DSL is a major capital investment even though it reuses the huge installed base of copper twisted pair it requires substantial investment in new facilities. The Telephone Companies are concerned DSL will erode T1 revenue. Today, a T1 line that delivers 1.5Mbps cost about $2000 a month. The same speed DSL line is likely to be priced at less then 10% of that. T1 is more robust but at ten times the price many user will opt for DSL. An additional consideration is that as Voice over IP matures DSL will eliminate the need for multiple phone lines. DSL has enough bandwidth to carry multiple telephone conversations without requiring a dedicated copper pair for each number.

3.4   Cable Modems

This technology steals one or more video TV channels to transport data. Cable TV transmission systems are broadband. The COAX cable that delivers broadcast TV has between 400-1000Mhz of bandwidth. This bandwidth is divided into multiple TV channels. Each channel occupies 6Mhz and uses the same modulation scheme as over the air broadcasts. Cable modems utilize one or more forward channels (originated by cable TV company) to deliver high bandwidth data to subscribers. User transmission utilizes the back channel (toward the cable TV Company). The back channel is positioned below channel 2 at 54Mhz.

Cable modems require substantial investment on the part of the cable TV industry. These systems were designed to deliver broadcast TV. They do not support two way transmissions. This requires the distribution amplifiers to be upgraded and safeguards added to prevent the analog TV channels from interfering with the data channels. CATV venders are also under pressure to deploy Digital TV, which consume more bandwidth then conventional analog TV this places tremendous pressure on unused cable bandwidth.

All subscribers share CATV bandwidth. This isn't a problem for broadcast since the same data is delivered to all users. Bandwidth used by one subscriber reduces the bandwidth available to the others. This is identical to the problem faced by LANs. In order to guarantee reasonable data rates the CATV venders must split the cable network into subnets with separate links back to the head end.

Cable TV venders are planning to deliver telephone service. From a bandwidth perspective this is fairly easy to do. However, they have no experience delivering telephone service and must overcome regulatory hurdles. Telephony over CATV requires active electronics so protection from power failure is more difficult.

A related issue is the FCC must carry HDTV rule. Digital TV is not compatible with the analog NTSC format. The FCC gave broadcasters additional UHF channels to simulcast analog and digital TV. For CATV providers this means they need to carry more channels, putting pressure on available cable bandwidth.

3.5   Cell Phone

The current cellular phone system is based on low bandwidth channels optimized for voice. Both analog and digital transmission schemes are used. This is a circuit switched network with high cost when used for data transmission. RF systems suffer from the same problem all shared services have, users must share the available bandwidth.

RF technology complements wired technology. In urban areas where customers are close together wired connections are more cost effective, in rural areas the situation is reversed.

RF will always excel is when mobility is important, either as a pedestrian or in a vehicle. For that class of user not other technology will do.

3.6   Geosynchronous Satellites

Geosynchronous satellites provide cost effective solutions to broadcast TV and Radio. They occupy stationary orbital locations so the antenna does not have to track the satellite or implement handoff from one satellite to another. However, because the satellites are far above earth the time it takes the signal to reach the destination is unacceptable for interactive data and voice use. It takes approximately ¼ of a second for the transmitted signal to reach the user and another ¼ second to return.

3.7   DirectPC

Hughes operates the DirectPC satellite network in low earth orbit (LEO). It provides a unidirectional 300kbps downlink in conjunction with a standard telephone modem. To use the system the user places a call to a Hughes ISP. The ISP processes requests but instead of sending the response via the modem it uses the high-speed satellite circuit. This requires the use of a small dish antenna.

This system works well for large file transfers or multimedia streams because once the connection is set up via the modem all the traffic flows through the satellite link. However, does not work as well viewing web pages. This tends to be very interactive and is limited by modem speed and the additional transmission latency through the satellite link. The system has the option to allow some traffic to be handled totally by the modem. This is advantageous where very small transfers are involved.

The basic contract limits use to a single computer. Hughes offers the service to sites with multiple computers, however it is much more expensive.

3.8   Internet in the Sky – Teledesic

This system is designed to deliver 500Mbps in a 100Km circle. This makes it attractive for rural areas and over water. These satellites are in orbit only a few hundred miles above the earth (LEO). This dramatically reduces travel time to less then 100ms. These satellites are not fixed over a single location, so many are needed to cover the globe. This is likely to be a premium service but may compete with wired access in rural areas. It will also put pressure on the other carriers to deliver high bandwidth service.

3.9   Fiber and Hybrid Fiber/Copper

This is the Holy Grail of connectivity – bandwidth too cheap to meter. In the long term the other wired schemes do not provide enough bandwidth. Broadcast video, interactive video and fast data transfer needs data rates in the hundred of megabits per second range. Using a single transport medium allows a service provider to collapse the physical network into a single high-speed connection to each user.

The question is who will implement this new network. The Telco's and CATV venders have an installed base to protect. Upgrades to the existing network are a very attractive option during early phases of the rollout. At that time the "take rate," the number of customers for the new technology is very low. At this stage the market opportunity does not justify the huge investment need to rewire the planet. However, once

the technology becomes mainstream enough customers exist to justify the deployment of more appropriate new technology.

The electric power utilities are and interesting wild card in this equation. They have no installed base, own the right away, have people with trucks, and know how to send out bills.

3.10 Conclusions

It is too soon to predict the winners and losers. From a historical perspective the established players rarely succeed in making the change to new technology. The cost of stringing new wire is astronomical but so is the cost of upgrading existing systems. During the transition phase different technologies may become dominate regionally. The economics of the situation is strongly affected by the take rate, the percent of users passed by the carrier that signup for the service. The problem facing all the players today is that the take rate will be very low at first. Only 40% of US homes have PC. Only a few are interested in high-speed web access. The small size of the early market makes it hard to justify the massive investment required to provide high-speed services. However, early investments are likely to capture much of the market once the demand for high-speed bandwidth takes off.

The SOHO LAN must be designed to work with all these technologies. The basic premise of this paper is that wide area communication will be based on IP (Internet Protocol). The SOHO LAN is what the Telephone Company terms Customer Provide Equipment (CPE). It must be designed to connect to a diversity of wide area networks (WAN). A given site may require access to more then one WAN to obtain all desired services. It provides the interface between the external common carrier transmission facilities and the various local networks used in the home and small business.

4   Selecting an ISP

This turned out to be surprisingly difficult. I wanted to approach this as a typical user. This wasn't completely realistic because I already had Internet access. The selection problem will be much harder for someone who cannot use the Internet to find out about the Internet.

The first thing I did was look in the local phone book. The only ISP's listed were small mom and pop operations. I looked at their sites but was not impressed.

Through our IT department I found a referral to a local mid size ISP. Looked at their web site and sent an e-mail with several questions. Got a very timely response to my questions. They would have been viable but they did not offer all the features I was looking for.

Then I tried AT&T and MCI (now sold to Cables and Wireless) to see what national services looked like. I was totally baffled by the AT&T web site; MCI's was somewhat better. Sent E-mail requesting additional information from both venders. Received an immediate answer from AT&T, however they didn't answer many of my questions. It took MCI a week to respond. It was a little more informative then the AT&T response. They answered a few of my question and stated the other questions were being "forwarded to our Internet support team … will be answered as soon as they have a chance to review." That was months ago, I still haven't received a reply. Interesting, they told me I could call the technical support department, however I shouldn't call between 5-10PM due to lengthy waits. What a fantastic marketing ploy tell people before they sign up that if they have a problems not to expect timely help.

Then I tried another ISP based on a referral from a friend; they had a nice web presence. I sent them E-mail asking several questions. Unfortunately they didn't answer repeated E-mail requests.

I found this experience extremely frustrating. Here I was a hot prospect that wanted to become a subscriber and I could not get answers to basic questions. This certainly does not instill customer confidence. I finally selected MCI so I could combine long distance telephone and Internet on one account. After an initial ordering mistake the setup CD arrived. The MCI supplied software configured the browser and dialup networking. Even though MCI offers E-mail the setup utility does not configure the mail client. When I

called the help desk and told them I was using Windows 98 (June 1998) they said sorry "we don't support that yet."

After configuration the dialer would activate on every boot cycle and whenever the Browser was opened. MCI had set Internet Explorer up to use a dialup connection rather then LAN access. This is really somewhat of a misnomer. The only difference is in dialup mode each boot cycle queries if you want to log into the Internet. Selecting LAN mode solves this problem. This requires that the user activate the dialer manually to connect.

I asked about V.90 support, MCI adopted X2 modems so many of the POP (Point of Presence) sites have X2 modems. My local POP was planned to be upgraded in the fall of 1998, this has still not occurred and Cable and Wireless the new owners, have not committed to a date (as of January 1999).

The MCI account information did not include information on access to a news server. E-mail brought a timely response on the server's name and how to configure it.

5   Domain Hosting

Every computer on the Internet has an address; this is a 32bit number that by convention is written as nnn.nnn.nnn.nnn. This is the format machines use to communicate with one another. Every message on Internet includes the address of the source and destination. These numbers are not very convenient for humans so the Internet includes provisions to use a name rather then numeric address. For example my web server can be accesses as http://www.tschmidt.com. DNS provide a service to look up registered names and translate them to numeric addresses.

Dot COM is the top-level domain. These are the domains such as .GOV, .EDU, .ORG, .NET, .MIL or the two character country code domains such as .UK. The text to the left of the .com is the user's domain name. Each domain name must be unique within a top-level domain. If this were not true it would be impossible to route messages to the proper location. Note that the Internet is only concerned with the top-level domain and the domain name. Once the Internet has forwarded the packet to the proper domain name, in my case tschmidt.com, its job is done. Further subdomain routing is the responsibility of the domain owner.

In the US the .com and .net top level domain names are administered by Network Solutions. When you sign up for ISP services your Internet address will be contained within the domain name they registered. E-mail is typically yourname@ispname.com and if you use your ISP to provide a web server its address is typically http//www.ispname.com/~yourname. This locks your Internet address into the name of the local service provider.

Another solution is to register your own domain name. Instead of being addressed using the name of your ISP your address becomes yourname@yourdomain.com and your web site becomes http://www.yourdomain.com.

Your ISP or another company that specializes in web hosting can do web hosting. Most companies offer the ability to search for available domain names. Once you select a name the provider will do the paperwork to register it with InterNIC. Once InterNIC approves the name your provider configures their routers and nameserver to allow people to connect to your web server and send E-mail. This process is highly automated so is only takes a day or so. Once you register a domain name you can move it to a different hosting service. This is transparent to anyone access your web site and sending E-mail.

The web hosting service will bill you for a setup charge and a monthly fee for web and E-mail hosting. InterNIC will send you a bill to register your domain name. The fee is currently $70.00 US for the first two years and then $35.00 a year thereafter.

A separate group is responsible for allocating the limited number of physical IP addresses. IANA the Internet Assigned Numbers Authority is charge with assigning blocks of IP addresses. This normally does

not impact end users. The ISP or web hosting service issues IP addresses from the quota it has already been assigned. IP address assignment and domain name registration is in a period of transition. The US government is relinquishing control of these services. Debate is ongoing about how this should be handled in the future and way to protect company trademarks in the domain name scheme.

6   LAN Discussion

Much of the discussion of SOHO connectivity focuses on the problem of physically connecting multiple computers. This is an important consideration, but it is not the major impediment to SOHO LANs. Consumers don't seem to have problems wiring telephones, cable TV, or alarm systems. We have a reasonable solution today, Category 5 10/100Mbps Ethernet wiring. Material cost of wiring a new home with RJ45 Ethernet jacks is approximately $400 for components (16 combination LAN and telephone outlets). The labor is similar to installing conventional telephone wiring in the range of $500-1000 per home. To this must be added NIC cards in each PC. Current 10/100 NIC's are less then $30. A 10/100Mbs speed sensing 16 port hub goes for $500.

The unsolved problem is that when you plug in your shinny new computer into the RJ45 network jack nothing happens. The task of obtaining the right software and configuring it is truly daunting. We need to extend plug and play from the system to the entire network. The consumer should be able to purchase a preconfigured gateway server and various client devices. The gateway automatically configures itself to the ISP and the clients configure themselves to the gateway. The only questions that are asked are non-technical ones such as what do you want to name your computer and what is your user name and password.

6.1   TUT – IP over Telephone Wiring

Tut Systems implements a medium speed LAN that uses standard telephone wiring. This is a tremendous advantage because it allows the creation of small LANs without investing in facility wiring. Tut is the same paradigm as Video for Windows, it lets users experiment with a new feature for free. Most implementations use a modified Ethernet controller to deliver 1Mbps data rates. IP is used as the transport protocol this makes it easy to route data between Tut and standard Ethernet.

QOS support will be important because of Tut's modest data rates. File transfer and print jobs will saturate the Tut LAN interfering with multimedia presentations.

Another consideration is security. TUT signals are carried on telephone wires so they propagate beyond the perimeter of the house. This allows someone with physical access to the telephone line to tap the signals. The nature of the RF signals makes non-invasive eavesdropping possible.

6.2   IEEE 802.3 Ethernet

10Mbps Ethernet has been around since the early 1980's. 100Mbps was introduced a few years ago, and is rapidly gaining market share as prices fall. 100Mbps provide a 10-fold increase in speed at a very modest increase in cost. Both speeds can be carried over unshielded twisted pair wiring. This is the most common form of premise wiring used today. It has completely replacing coax in new installations.

When implementing Ethernet one needs to keep in mind that UTP Ethernet is effectively a point to point link. Each computer needs it own link to the hub. The hub acts as a central connection point to each of all the wires. The UTP specification limit wire length to 100 meters. Typically 90 meters is allocated to the building wiring and 10 to patch cables.

6.2.1   Hubs 10/100 Hubs Switching Hubs

Ethernet uses a technique called CSMA/CD, Carrier Sense Multiple Access Collision Detection. Ethernet is a computer version of the old-fashioned telephone party line. When a station wants to transmit it first listens to see if the line is idle, if it is it sends the message. Under some circumstances more them one

station will transmit at the same time, this causes a collision. Collisions corrupt the data; stations detect this condition and retry the transmission after waiting a random interval. When you connect your computer to a hub all transmissions are repeated on all other hub ports. Collisions my occur on any of the hubs ports which result in all stations seeing a collision. Since electricity travels at a finite speed the time it takes a signal propagate end to end limits the electrical length of the LAN and places a lower limit on how short a message can be. The minimum message length must be long enough so the transmitter can detect a collision while it is still transmitting

This requirement gives rise to the 5-4-3 rule for 10Mbps Ethernet. The number is segments are limited to 5. Each wire is a segment, Since each computer consumes a segment three are left. The three unused segments mean that there can be up to 4 hubs between any two systems, hence the 4 of the 5-4-3 rule. The last number, 3 limits the number of segments that can be populated. Only three of the segments can be populated.

Increasing the speed to 100Mbs tighten these restrictions. 100TX defines two types of repeaters Class II is relevant for our homogeneous network. With Class II hubs 100TX is limited to 2-2-2. The maximum distance between any two systems is limited to two segments and two hubs. A further restriction limits the distance of the hub to hub connection to 5 meters. Due to the very tight timing requirements it is recommended that both hubs be from the same manufacturer.

10Mbps 5-4-3 Rule   **100Mbps 2-2-2 Rule**
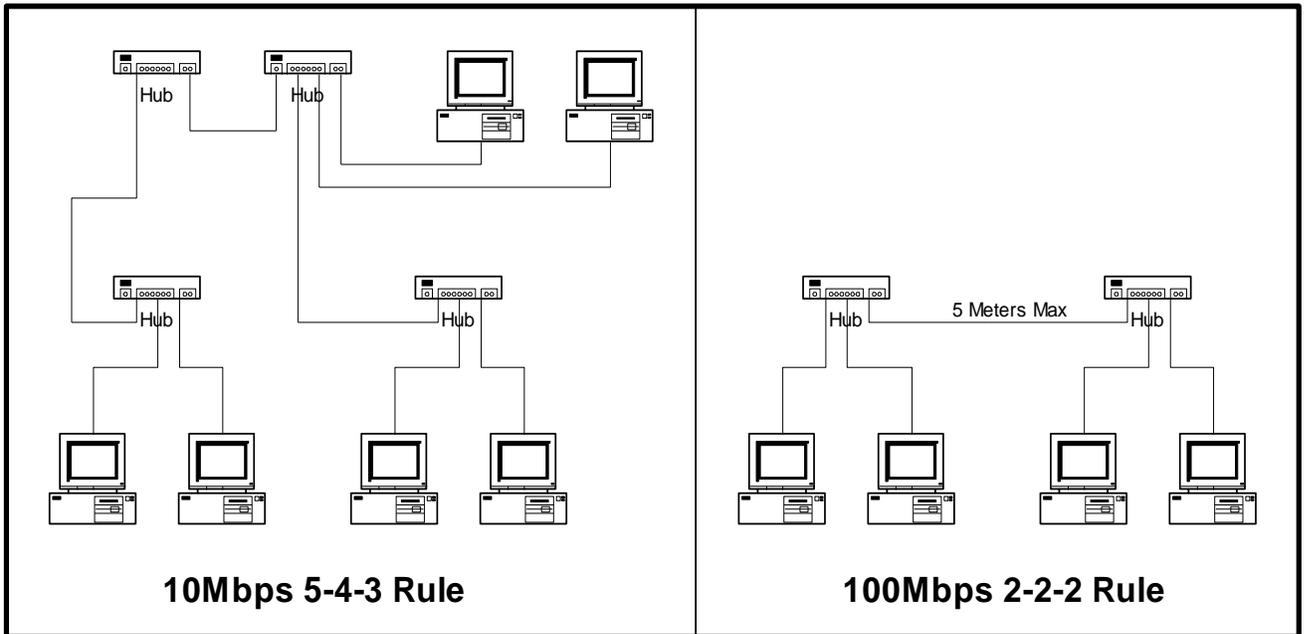
10/100 autospeed-sensing hubs include additional intelligence on each port. The hub automatically connects all the ports that are running at 10Mbs to an internal 10Mbps backplane, and the ports operating at 100Mbs to a 100 Mbps backplane. Traffic that flows between the 10 and 100 backbone are speed shifted to the appropriate speed. This allows all devices to communicate will all other devices. 10/100 hubs are a great convenience providing transparent interoperability in mixed speed environments.

So far the hubs we have discussed simply repeat what they see on each segment to all other segments. This means the total amount of traffic on the LAN is limited to 10 or 100Mbps. Switching hubs have an internal switch matrix that runs at a faster rate then the individual segments. The switch does not simply repeat all packets to all other ports. It examines the packet address header and determines where to send it. Lets assume we have six systems connected to a six port switching hub. When the computer on port 2 wants to send a message to port 5. Internally the hub passes the packet from port 2 to port 5 without sending it to any

other ports. If the computer on port 6 decides it wants to send a message to port 3 it does so without slowing down the other connections. If port 1 and 4 are also in use then up to 300Mbps of data may be flowing through the hub.

The other advantage of a switching hub it that it isolates each segment. This allows the LAN to be extended beyond the limits of the 4-5-2 rule for 10Mbs and the 2-2-2 rule for 100 Mbps.

100Mbps with Switching Hub
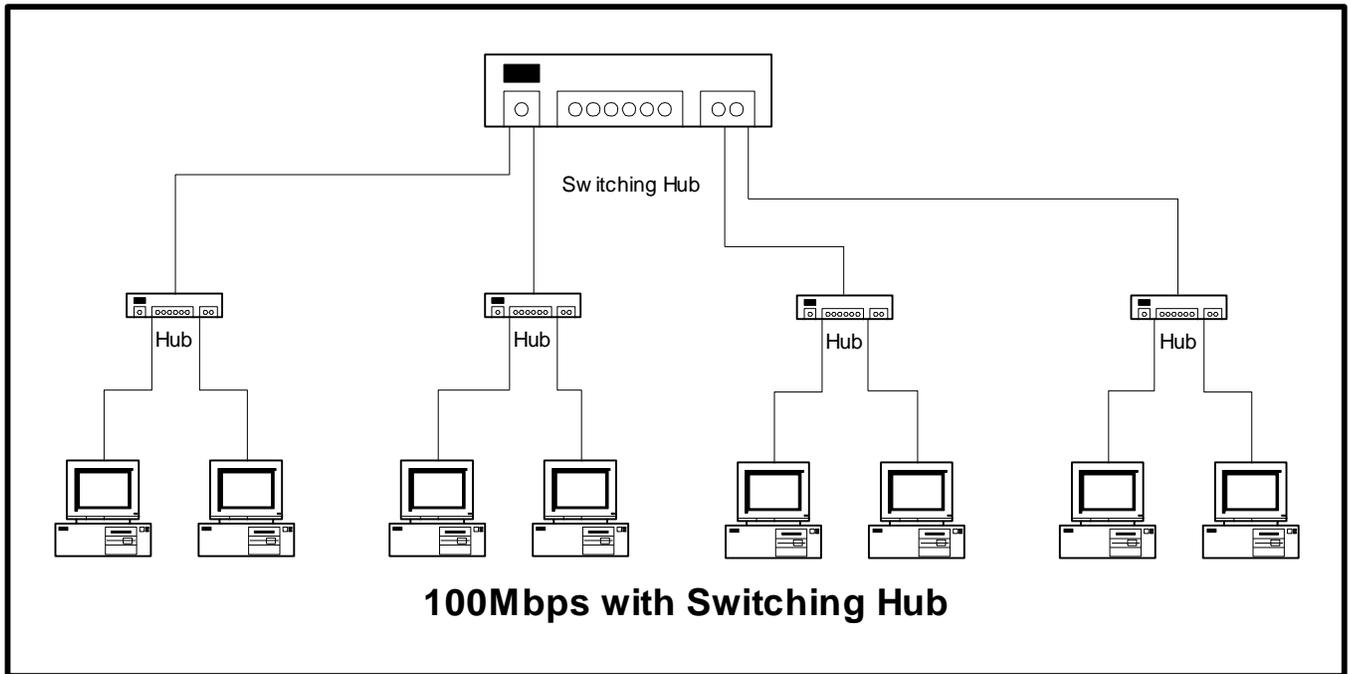
When deciding how to configure the system if a single hub will be used to connect all computers on the LAN and it is unlikely that another hub will be needed to provide additional ports chose a 10/100 auto speed sensing hub.

If it is likely that additional hubs will be added the "root" or top level hub should be a switching hub. This allows another non-switching hub to be added at each outlet to expand the number of port without violating topology rules.

This has been a very abbreviated discussion of Ethernet, for an in-depth treatment read "Ethernet Networks" From 10Base-T to Gigabit 3rd edition by Gilbert Held ISBN 0-471-25310-3.

The IEEE 802 family of LAN standards:
- IEEE Standard 802-1990 Local and Metropolitan Area Networks. Overview and Architecture 20 Nov 1990.

The IETF defined the method to use IEEE802.3 physical layer for IP.
- rfc1042.txt -- Standard for the transmission of IP datagrams over IEEE 802 networks. J. Postel, J.K. Reynolds. Feb-01-1988. (Status: STANDARD)

6.3 Long Distance IEEE P1394B

The IEEE P1394B working group is developing Gigabit 1394 (800, 1600, and 2300Mbps). They have also accepted a request from the VESA Home Networking group to develop a long distance version of 1394.

1394 was originally developed to connect high-speed computer peripherals, cable length is limited to 4.5 meters. The Home Networking group wants to expand the use of 1394 to include LAN functionality. This eliminates the need for Ethernet in the SOHO environment. The minimum goal is 100Mbps @100meters. 100Mbps transmission is less then the preferred speed for video distribution. If the long distance speed is only 100mbps some form of switching will be required to increase total system bandwidth. Support for 1394B should begin to show up in 2000.

The working group will create a standard for both fiber optic and copper cable. The copper cable standard will utilize the EIA/TIA Category 5 100Mbps premise-wiring standard. The fiber standard is still in the early stages of development.

One of the benefits of using 1394 is that a single wall jack can service an "unlimited" number of nodes. The adapter between the short and long distance 1394 connects everything to a single long distance segment. Since 1394 is an arbitrated bus total throughput is limited by arbitration delays.

An IETF working group is developing a specification for using the 1394 physical layer for IP.
- Draft IPv4 over IEEE 1394

6.4   CEBus

CEBus is an EIA standard that attempts to standardize "Home Plug & Play " communication. It addresses everything from low bandwidth command and control to fast fiber optic networks. This has been met with limited success. Most home electronic devices are analog, and do not include communications. TV, Radio, Audio, X10 remote control, etc have all implemented function specific interfaces. This makes it very difficult to integrate them.

An interesting possibility is that once a SOHO communication infrastructure is in place. CEBus will be used to perform home command and control functions. CEBus is not limited to physical interconnect the CEBus Industry Council developed the Common Application Language (CAL) to facilitate device interoperability

The CEBus specification:
- EIA/IS-60 EIA Home Automation System (CEBus®) (Oct., 1992)

6.5   Lon-Works

A CEBus competitor is Lon-Works. It provides low cost command and control functions over the power line. This EIA has also standardized this.

- EIA-709

6.6   Wireless LAN IEEE 803.11, HomeRF, WPAN, BlueTooth

These standards and initiatives aim at deploying wireless RF LANs. Traditionally, RF has been expensive and provided relatively low bandwidth.

With the Adoption of IEEE 802.11 an industry standard exists to provide 2Mbps within a single site. Work is well along within 802.11 to increase data rates to 10Mbps. This makes Wireless LAN much more attractive.

 The Wireless Personal Area Network (WPAN) group is an IEEE 802.11 study group that is tasked to develop a short range (10 meter), low speed (1Mbps), low power RF LAN. This allows small low powered devices to exchange information. Today devices must be cabled together to communicate.. WPAN also supports ad hoc networking. This allows people to come together casually and exchange information. Another exciting prospect is smart buildings that provide electronic signage. Information about conference

rooms, directory information, floor plans, etc will be transmitted via WPAN. As you walk around the building this information is transmitted to your wearable computer.

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 working on similar problems as WPAN. They are an Ad Hoc group, where WPAN is under the auspices of IEEE802.11.

Security is a major consideration for RF devices; transmitted signals do not obey at property lines. Spread spectrum techniques makes the transmitted signal look like random noise to an unsynchronized receiver. This is touted as a significant security feature. However, to establish communication all parties must agree on a common key. Only a few keys are used so it feasible to cycle through all combination in a reasonable amount of time. Once the key is obtained transmission can be recorded for subsequent analysis. As in other communication networks the data can be encrypted but this requires substantial processing power.

The level of activity underscores the value of wireless connectivity. Devices that place a premium on mobility and require limited bandwidth will benefit from these emerging standards.

6.7 Power Line

Intel is promoting this technology, as part of the no-new-wires initiative. This has the advantage that wherever a device is needed an AC receptacle is likely to be close by. The disadvantage is that the power line is an extremely hostile environment. The complexity and cost of the transceivers will be similar to 802.11

6.8 Conclusions and Predictions

TUT based systems are likely to prove popular because they do not require new wiring. However, over time the limitation of low bandwidth will cause TUT implementation to migrate to faster forms of communication.

Early adopters will likely use Fast-Ethernet over Category 5 unshielded twisted pair. Ethernet components are fast, reliable and cheap. When long distance 1394B is deployed we may see a shift away from Ethernet to 1394. Ideally this will move directly to fiber, bypassing copper interconnect. This is probable 2-4 years away.

RF links will be attractive to users that require mobility and have modest bandwidth requirements. The various RF initiatives aim to reduce the cost of RF. If they are successful wireless links should become popular.

The appeal of AC wiring as a general purpose LAN is unclear. It has almost the same complexity as RF, hence similar costs without the benefit of mobility. For low speed command and control where the device needs to be connected to the power line anyway this is a good solution.

These implementations will need to coexist. The details of the physical network are not a critical concern to the concept of SOHO networking. The SOHO network needs to work with common network topologies. A SOHO installation may comprise multiple physical networks, high speed wired LAN for computer and entertainment, RF LAN for mobility devices, and CEBus for fixed location command and control. A client computer may be connected to more then one LAN. Software in the client needs to determine which link is the best and disable the others. Routing between the different LANs can either be hard coded in the gateway server or the router elected dynamically.

7   Implementation

This describes an actual implementation in daily use. The PCs uses a combination of Windows 95 and 98.

7.1   LAN

The LAN uses a combination of 10 Base T and 10/100TX Ethernet adapters. Wiring is EIA/TIA 568A Category 5 terminated at an 8 port 10 Base T unmanaged hub. TCP/IP is the only protocol used.

7.2   File and Print Sharing

Microsoft peer to peer file and print sharing is used.

The gateway server is collocated with the printer. This allows the standard Centronics parallel port on the gateway to service the printer.

Another option is to use a network ready printer. Commercial duty printers commonly employ direct Ethernet connection. The other option is to use a standalone print server. This device provides a low cost interface that allows any printer to be placed on the LAN.

7.3   POTS ISP Access

Internet access is via a dialup connection to Cables & Wireless. Two telephone lines provide WAN connection; they are shared for voice and data. The main number is configured to hunt to the second number if the first is busy; Call waiting is used on the second number. The modem is connected to the modem access adapter (describe in the appendix). The adapter senses when the modem is attempting to dial and searches for and idle phone line. If it finds an idle line it disconnects all extension phones and connects the modem. This prevents interference between phones and modem.

The telephone wiring uses the existing two pair house wiring, the only modification was to disconnect it from the TELCO Network Interface (NI) and reconnect it to the modem access adapter. Telephones consist of a combination of single line and two line units. The modem access adapter is installed in close proximity the Telephone Company Network Interface (NI). This required running a single telephone pair to the server location.

Cables & Wireless Internet provides nationwide points of presence (POP). This allows access to the Internet via a local call from most locations in the United States. Where local access is not available 800 number service can be used at extra cost.
They implemented X2 high speed modem capability and are in the process of upgrading to V.90.

7.4   Domain Hosting

A local company InterNET Resource NETworks was chosen to host the tschmidt.com domain. This service provides a 10Mbyte of web space and 3 email accounts. They handled all the domain registration paperwork.

7.5   Internet Gateway and Firewall

The gateway is running WinGate version 2.1d software which manages the LAN and provides Internet access. There are many products on the market that connect a LAN to the Internet. WinGate is one of the more popular packages and the only product I found that implemented DHCP. This allows automatic assignment of client IP addresses.

The server runs Windows 98 it provides typical LAN functionality and links the LAN to the Internet via dial up networking.

The gateway is used to provide automatic demand dialing. When an attempt is made to access an off LAN resource the dialer automatically connects to the ISP. When the line is idle it automatically disconnects after 10 minutes.

7.6   Web Browsing

Internet Explorer is installed on the gateway server and the clients.

7.7   Private Web Server

Microsoft Personal Web Server (PWS) was installed on the gateway server. The free copy of FrontPage Express, included in Windows 98, was used to create a simple internal home web site.

Running PWS on the gateway platform compromises overall system security. Both the LAN and the dial up adapter can access PWS. PWS does not provide a mechanism to bind to a specific interface. Any port configured for TCP/IP can access PWS. In a dialup environment this is not too serious since ISP's typically dynamically assign IP address for dialup users. This makes it hard for a hacker to attack a specific site.

I've removed PWS and used the web server built into WinGate, this has limited functionality but it is more then adequate for serving a few static web pages.

7.8   Public Web Server

The public web server is not run locally. The main reason is because this is a dialup site it does not have a permanent Internet connection. If a permanent connection with a static IP address exist it is possible to operate a public web site locally. However this requires a more complex fire wall structure because the web server must live "outside" the protected corporate LAN. This is typically called the DMZ, for DeMilitarized Zone. The other factor that must be taken into account is the amount of site traffic, the links muse be sized accordingly. In general residential and small business users are better served by outsourcing the public web server.

Currently InterNet Resources NETworks is hosting the public web server. They handled the domain registration and are hosting the tschmidt.com domain.

Files are uploaded using FTP. Once pages are debugged locally they are transferred to the public web server, tschmidt.com. The web hosting service compiles statistics and access logs to analyze web usage.

For those who chose not to register a domain name ISP's typically provide web-hosting services to their customers. These are the sites you see with names like http:// foobar1.com/~myhomepage. This provides public access without the need to register your own domain name.

7.9   Time Synchronization

A timeserver (Tardis) runs on the server. This obtains accurate time information from web based NIST timeservers. This is used to synchronize the server. The server in tern broadcasts current time information to all the clients on the LAN.

7.10 Remote Corporate Access

A notebook PC used at work, on the road, and on the Home LAN. It is equipped with an Ethernet port and a modem. The LAN is used to access the corporate network locally. The modem is used for dialup networking from remote locations. The notebook Ethernet port can also be used to connect to the SOHO LAN. However when it is connected the RAS connection cannot be used. This is on due to Windows 98 limitations. RAS and LAN connections are mutually exclusive. Windows 98 it does not have a mechanism to route traffic through different network connections.

Corporate VPN would solve this problem but it is not currently available.

7.11 E-mail

ISP's typically provide one or more E-mail accounts as part of the service. Your E-mail address will look something like myname@myisp.com. A disadvantage is your E-mail address is coupled to your ISP. Changing ISP's requires a change in E-mail address. Registering a domain name eliminates the

dependency of you mail address on your ISP. With your own domain your mail address becomes myname@mydomain.com.

A solution for casual users is to sign up for one of the free advertising supported E-mail services such as Excite or yahoo.

Users that have their own domain name can use products like Mdaemon that allow an unlimited number of mail accounts. The web hosting service simply dumps all incoming mail into a single mailbox. The mail server retrieves the messages and sorts then by user name, the portion of the address left of the @ sign. This creates a number of user mail accounts on the local server. Each users mail client points to the local mail server.

It is not uncommon for users to have more then one mail account. Most mail program provides a mechanism to access more then one mail account. Internet mail consists of two portions, POP and SMTP. POP stands for Post Office Protocol, the mail client goes to the POP server to retrieve mail. SMTP stands for Simple Mail Transport Protocol. When your mail program sends mail from your outbox it connects to the SMTP server. The server then forwards the mail across the Internet.

Any valid SMTP service can be used to send mail. This greatly eases the problem of accessing mail from more then one account because you can use the same SMTP server for all accounts. The preferred SMTP server is the one provided by your ISP. Many ISP prohibit access to other SMTP servers in an effort to limit SPAM.

Currently we are using a combination mail. One system is running Outlook 98 with access to mail accounts on both the ISP and the account provided by the web hosting company. The rest of the family uses the free mail service provided by Yahoo. The system currently does not have a local mail server. Outlook is configured to point to WinGate for both incoming and outgoing mail.

7.12 News

Microsoft Outlook 98 uses Outlook Express for news. Initially this information was not provided by MCI. An E-mail request produced the name of the news server. Outlook Express is configured to use WinGate as the news server. WinGate in turn is programmed to pass all news requests to the newsreader provided by the ISP.

7.13 Chat

Chat room support did not required and specific configuration. This uses the web browser .

7.14 Voice over IP

The current installation does not support Voice over IP. NetMeeting requires the ability to dynamically assign a large of ports through the firewall. This is not supported in this version but is in the later version of the proxy.

This is also a problem with many of the Internet games. The later version of the proxy supports this capability.

7.15 Mobile Client

NetSwitcher is installed on the laptop. This utility captures location specific information and simplifies switching between locations. When the machine is moved NetSwitcher is invoked to change network settings, proxy, and printer selection.

This is far from ideal but it is the best off the shelf solution I could find.

The mobile mail client is configured to leave mail on the POP server. This allows the mobile PC to read mail and still have it available on the main machine. Once mail is downloaded it is only available on the machine that downloaded it

7.16 Authentication

The laptop uses corporate NT domain authentication. SOHO LAN clients are not authenticated, they are assumed to be trustworthy. Since the SOHO LAN does not require domain authentication moving the notebook between environments does not cause problems.

7.17 Regulatory Issues

The SOHO LAN must meet a variety of regulatory requirements that address safety and limit interference. The paper is US centric; other geographies have similar regulations promulgated by local standards organizations.

Building wiring must meet safety standards dictated by the National Electrical Code 1999 (NEC) Article 800 Communication Systems. This addresses flammability and sets limits on voltage and short circuit current. The NEC is published National Fire Protection Association (NFPA).

The NEC limits permanently connected devices to 80% of branch power. This means a computer can only draw 12 Amps on a 15 Amp branch circuit. Given the low power consumption of typical PCs this is normally not an issue.

Devices that connect directly to the telephone network must meet FCC CFR 47, Part 68. This affects the modem access adapter and modem. This standard is concerned with harm to the telephone network.

Electronic devices used in a residence must meet FCC CFR 47 Part 15 Class B. This FCC standard limits unintended radiation. Network components are not commonly used in residences, so some are only certified to Class A.

All computing devices must meet UL1950. This addresses overall safety issues.

A schematic representation of the entire implementation is shown on the next page.
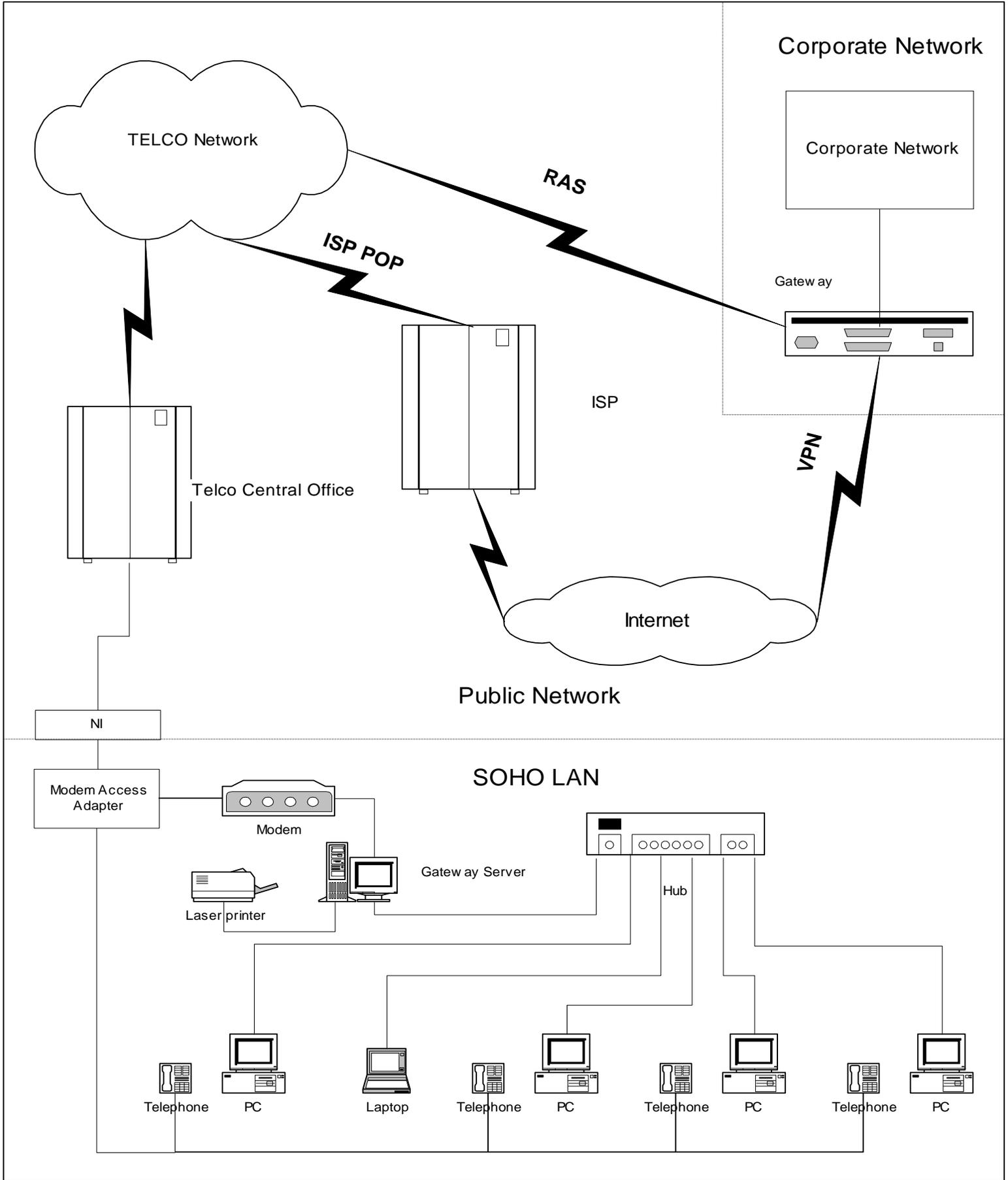
System Implementation

8 Concepts for Future Enhancement

The deployment of SOHO LANs should be viewed as an enabling technology that opens the floodgates of new opportunity. It is akin to the change that happened when hardware design went from hardwired logic to microprocessor. In a hardwired design each feature adds incremental cost. In a microprocessor design once the base hardware is acquired incremental feature cost is almost zero.

8.1   Integrated Messaging

Better integration of voice and data messaging increases the value of SOHO LANs. Once a local mail server is in place expanding it to universal messaging is the logical next step. The telephone answering machine is integrated into the mail server.

Each person has a mail account. This works well for E-mail, and in businesses where each person has a unique phone number. In a home setting and companies that do not provide dedicated phone numbers some form of automated attendant is needed to ask the caller's name and who the caller want to talk to. Using this information the answering machine routes the call to the correct mailbox.

Messages may be retrieved from PCs or the telephone. For convenience telephones can be equipped with a message waiting light, the answering machine turns on the light when a message is received. To retrieve a message the user pickup the phone and dials an access code. This allows messages to be retrieved in a familiar manner.

The answering machine can also be used in a do-not-disturb-mode. Do not disturb screens calls and automatically dumps them into mail. This feature should be a boon for interruption free diners and enforcing "no calls after 10:00PM" rule.

8.2   Local loop Bypass – VoIP

Each telephone number requires a dedicated pair of wires between the user and the Telephone Company. This becomes expensive if multiple phone numbers are desired.

Packet based digital connections can carry an unlimited number of simultaneous conversations, limited only by available bandwidth. Typical Internet telephone calls transmit voice at 8Kbps in each direction. As ISP's roll out Voice over IP telephony services we will be able to utilize the LAN and ISP connection to create virtual telephone lines. When a user picks up a phone, or uses a PC to place a call the gateway server determines if the call can be placed by the ISP. The call is routed over the ISP connection leaving the expensive dedicated telephone line free for additional calls.

This feature is ideal when fast permanent ISP connection are available. However, even a V.90 modem has enough bandwidth to create a virtual telephone line without unduly impacting data throughput. In the case of DSL and cable modem this all but eliminates the need for multiple telephone lines. This is another reason the Telco's are treading carefully into the world of IP based digital communication.

8.3   PBX functionality using USB or Ethernet Telephones

A network centric approach to telephony allows us to dispense with the traditional PBX and leverage the existing LAN. This eliminates the need for separate voice and data infrastructures. PBX functionality is provided by a software application running on a network server. Combining LAN based telephony with Internet telephony results in a very low cost Digital PBX that is easy to upgrade. Need another phone, just plug it in, need another line, just create another user name in your domain.

USB telephones require a local PC to route voice traffic over the LAN. Ethernet telephones plug directly into LAN. All PBX functions are implemented in a server. Since the analog to digital conversion is

performed in the telephone special line cards are not required in the server. Voice over IP is used to transmit telephone calls over the SOHO LAN and out to the Internet.

LAN based telephony requires substantial active electronics. Telephones, PCs, Servers, DSL or Cable modems. If anything fails phone service is lost. It may make sense to design a combo phone that combines the network features with traditional POTS. This provides a POTS fallback, if the network fails or power is lost.

8.4 Telecommuter Features

The goal of telecommuting is to have the full suite of corporate voice and data network services extended to a remote site.

Today RAS and to a lesser extend VPN are used to extend the corporate network to remote users. Little is being done to provide remote voice service. Voice mail systems allow remote access and PBX add-ons provide follow me service. As PBX venders implement Voice over IP forwarding it becomes a simple matter to have the PBX route voice calls to the remote site. When an incoming call is detected the PBX notes that the employee is connected remotely, the call is routed to the remote site using the VPN. When the SOHO network receives the call it is routed to a network telephone. For outgoing calls the network telephone passes the connection request to the SOHO LAN gateway that encrypts and routes it to the corporate gateway. From here it is unencrypted and passed to the PBX.

8.5 Automatic Inbound Call Routing

When a one to one relationship does not exist between telephone numbers and a user location the system has to determine who the call is for and where they are located

Determining whom the caller wants to speak with can be accomplished by assigning unique phone numbers to each caller or by using an automated attendant. In an office environment where each person has a unique location the call is then simply routed to that location. If that is not the case routing can be tied to computer login. The person is assumed to be wherever they are logged in.

8.6 Integrating TV and Settop boxes

Settop box and cable TV converters provide an interface between a TV and the wide area broadcast network. This represents diverse combinations of source material, Broadcast TV, Cable TV, Satellite TV, and WebTV. The situation of CATV venders is unique in that they own the premise equipment coax and cable converter boxes. This is changing as the cable industry moves to a model where customer premise equipment is purchased retail, as is the case for telephones and modems today.

Combining video from different sources is very cumbersome. The various video feeds must be decoded and then passed through a RF modulator to create a personal TV channel. The IR system used for remote control uses proprietary protocols from each vender. IR does not pass through walls so to allow remote control from another location requires an IR sensor in the viewing location that transmits the signals to the device being controlled.

Current practice connects the converter box input to the broadcast source and the output directly to a TV. This forces a 1:1 relationship of settop boxes and TVs. Since the settop box is the enforcement agent of the licensing agreement it limits viewing to a single location this needs to be decoupled. In the SOHO LAN view the end user purchases the service they desire. This typically determines which channels are available and may place limitation on simultaneous viewing. The CATV provider does not care which device is used to view the program. This allows a combination of PCs and TVs to be used, contingent on licensing restrictions.

To do this we need to split settop box functionality into two parts, the CATV interface and the authentication component. The CATV interface connects to the providers network, selects the channels of interest, and converts them to a format suitable for the SOHO LAN. Due to security and bandwidth

considerations only those channels currently being viewed are passed to the LAN. Free channels are directly viewable. Pay per view is locally decrypted to enforce the provider's proscribed security policy.

This enables the SOHO LAN to deliver a mix of broadcast channels without the need to provide complex switching systems RF modulators.

8.7 Authentication

One of the pet peeves of most people is that large number of passwords and PINs they are required to use. This proliferation almost guarantees people will utilize easy to guess passwords and PINs and change then minimally when forced to do so.

This problem has two major components, identifying the user and sharing this information with other applications.

User identity can be verified with password (what you know), biometrics scans (what you are), and smart cards (what you have). The hardware industry is making great strides in this area. Once a user has been authenticated the users identity needs to be shared with other applications. This requires some form of non-forgeable document so the application is able to trust the user is who they claim to be. Digital Certificates are difficult to forge electronic documents.

A related problem is verifying documents authenticity. Digital IDs, like VeriSign allow users to append an unforgeable digital signature.

8.8 Thin Clients

The SOHO LAN makes it easy to connect to the Internet. As the market expands many of these devices will not be general purposes computers like today's PC but more appliance like, tailored to a specific function. As RF technology matures many of these devices will be wearables that people carry with them all the time.

The SOHO LAN needs to be client device agnostic. As long at the device meets the physical interface requirements and supports IP it works.

8.9 Home Automation

This has languished for years. An interesting assortment of home automation devices exists but they appeal mostly to hobbyists. One of the problems is the lack of device infrastructure. It is possible to purchase X10 devices, alarm systems, CEBus, etc to control lights and appliances. This requires the user perform a substantial amount of configuration and when the system is finally up and running access is limited to a single location.

The SOHO LAN creates the infrastructure to share these devices. A central web server allows the devices to be viewed and controlled from any computer in the house. This may be what finally pushes home automation into the mass market.

8.10 Meter Reading and Load Management

The benefit of automated meter reading has been obvious for years. But the cost of deploying a dedicated meter reading device has proved too expensive. Where the SOHO LAN is deployed the utilities do not have to provide end to end connectivity. Utility cost is limited to the cost of a smart meter and the need to provide a secure communication between the meter and the billing site on the web.

Load management is a mechanism utilities use to minimize demand at critical times. This is currently limited to industrial users due to the high implementation cost. The combination of SOHO LAN and smart appliances dramatically reduces this cost. In this model the utility broadcast demand based pricing. End users adjust consumption to balance need with cost.

8.11 Home VPN

VPN's are typically thought of as mechanisms to allow employees gain remote access to work. VPN can also be used to allow individuals to remotely access their own LAN. This allows remote access from anywhere the Internet is accessible. Once connected the remote user performs any task that someone physically there could do. The 1950's vision of turning on the coffeepot from work is possible. On a more practical side this provides access to security cameras, and home automation controls.

8.12 Home RF Communications

The popularity of wireless and cellular phones underscores the demand for unteathered communication. It is easy to add wireless access point to the SOHO LAN. While it is unlikely low cost RF will ever provide blazing speed, for many application being unteathered is more important then multi megabit per second transfer rate.

Wireless poses some unique challenges. The most important is that radio is not a wire. This means anyone in the vicinity can hear what is transmitted. In a cabled communication implementation an intruder must physically connect to your wires. Wireless data can be secured by encryption at the application level or by controlling the spectrum spreading sequence. This needs to be developed further. In the rush to deploy low cost short range communication security is not receiving adequate attention.

8.13 Internet Conferencing

Audio and video conferencing will become important forms of collaborative computing in the near future. As connect speed increase overall quality will increase.

9 Call to Action

Based on my experience setting up a SOHO LAN it became obvious that much needs to happen before they become commonplace. This is not so much due to a lack of technological solutions but rather the complexity of setting up the systems.

9.1 Facilities Cabling

The long-term residential solution is likely to be optical Gigabit Ethernet or 1394B. Businesses it will probably use Fast-Ethernet to the desktop and Gigabit Ethernet as a backbone. To be successful we need to address two types of customers, do it yourselfer and those requiring professional installation? A referral service will help users select a vender to install and configure the system. For do it yourselfers, we need to provide a training video, and either cheap limited use tools or provide a tool rental service.

EIA/TIA-570 is specific to residential but this specification has not been widely accepted. TIA is in the process of updating specification. One of the problems with previous attempts to standardize home wiring is that the standard allowed too many types of interconnects. The home specification includes requirements for POTS, LANs, CATV, and fiber optic. This results in a costly wiring infrastructure that is not well integrated.

To be successful we need a unified wiring scheme. Simply having al lot of wires in the walls is not beneficial. Ideally, system requirements will be met by a single type of interconnect. If that is not feasible it must be possible to bridge the different standards to a single logical network.

9.2 Hub

Need to develop a cheap hub optimized for SOHO use. Rather then spend money on patch facilities build a wide hub. The hub needs to be wide enough to terminate all data outlets, even though only a small number of drops will be active. The power supply should have enough ride through to survive momentary power outage. Power consumption should be very low. Provide enough local intelligence to help troubleshoot LAN problems.

9.3 Server

The server should be a low cost medium performance PC with very aggressive power management to get idle power consumption under 5w.

The server should be remotely configurable but a built-in low cost DSTN display and keyboard may be more convenient for users. Another option is to integrate the video and keyboard switch box to allow the server to be collocated with one of the desktops allowing use of a single set of peripherals.

The HDD should be a low cost RAID array that allows a user to replace a failed drive without data loss.

A multiple line V.90 modem maximizes the benefits of dial on demand. The adapter should have provision to make it easy to add a xDSL modem. Probably filters and RJ14 jack.

NIC supports both fast Ethernet and Tut. The NIC must support suspend power management to allow the CPU to be suspended. The hardware must be capable of simultaneous connection to both LANs. Ideally the NIC, TUT interface and modem are all built into a single adapter.

Power supply should have built in mini UPS to provide a few of minutes ride through to do an orderly shutdown. Suspend controls an AC receptacle. This allows the printer and other peripherals be turned off during suspend. Redundant power supply is nice, probably needs to be an option.

9.4 Clients

Clients are standard PCs with a network adapter that supports either 100TX or Tut.

9.5 Software Package

The server uses Windows NT or Linux., LAN support, firewall, web server, and timeserver. Router software logically connects the Fast Ethernet network to the Tut network.

The client operating system is Windows 98, timeserver client, WinZip, Real Audio, Adobe Reader.

To support mobile user we need an application like NetSwitcher that reconfigures the machine whenever it is moved to a different location.

9.6 Configuration

We need to understand what are the typical applications customers use and develop default configuration that work out of the box. During configuration the only questions the user is asked are ones that directly relate to how the user perceives the system. These are questions like "What do you want to name this computer," "What is your name," and "Please choose a password." Fore more experienced user we need to provide enough information to allow them to add additional hardware and software components.

Both Microsoft and Sun recognize the need to simplify networking. Sun is developing Jini, a specification for self-describing devices. This allows devices to negotiate for how they interoperate. Microsoft is proposing Universal Plug and Play. This extends plug and play from the PC to the network at large. These are critical initiatives because far too much technical expertise is required to set up networks, and move devices from one network to another.

Once the Server is up adding new clients should be as simple as doing a first time network boot. This takes care of low level configuration details and installs the various software packages. This is a great way to leverage the BIOS network boot mode.

User level test programs that verify common network and modem problems need to be developed. Customers should not have to run Winipcfg, ping, and Regedit to debug simple problems.

9.7 Manageability and Service

A critical part of this installation is the Internet firewall to keep the bad guys out. One of the service offerings could be security testing, make sure that the firewall is correctly configured. Another ongoing problem is upgrades and patches, I assume most small sites want to outsource this. This is an opportunity to offer some form of subscription service to automatically distribute and install the latest version of software and install bug fixes and security patches.

The servers and clients should be equipped with remote access software so the helpdesk can remotely configure the network. This must be done securely and only with the consent of the user.

Appendix A   Facilities Cabling

Facility wiring is based on the EIA/TIA-568A Commercial Building Telecommunications Cabling Standard. This uses 4 pair unshielded twisted pair cable terminated at modified Telco RJ45 8 conductor connector. This was routed to a central wiring closet where the hub was installed. Some of the NICs are 10Meg so I installed a 10 Mbps hub.

EIA/TIA 568A practice is to terminate the cable to punchdown blocks in a wiring closet. The punchdown blocks are prewired with RJ45 receptacles. A short RJ45 patch cord is used to connect the punchdown block to the hub. This allows easy reconfiguration of wire termination. This is very useful in a large commercial site but is overkill in a SOHO environment. I simply left slack in the wiring closet cables and terminated them directly to RJ45 plugs. The appropriate cables are simply plugged into the hub.

Telephone wiring was not changed except for the addition of a run from the wiring closet, where the modem access adapter is located, to the computer room, to connect the server modem.

The IEEE1394B working group is working on long distance version that utilizes either Category 5 UTP or fiber. As that standard evolves the facility cabling requirements will be integrated into the EIA/TIA specifications.

- EIA/TIA-568A Commercial Building Telecommunications Wiring Standard (ANSI/EIA/TIA-568-A-95) (Oct, 1995)
- EIA/TIA-570 Residential and Light Commercial Telecommunication Wiring Standard (ANSI/EIA/TIA-570-91) (June, 1991)
- TIA/EIA-606 Administration Standard for the Telecommunications Infrastructure of Commercial Buildings (ANSI/TIA/EIA-606-93) (Feb., 1993)
- TSB-67 Transmission Performance Specification for Field Testing of Unshielded Twisted-Pair Cabling Systems (TIA-TSB-67) (Oct 1995)

Lessons learned

- It was hard to find technical information on Category 5 wiring. These components are normally used in large commercial sites and are not typically sold to individuals. The web was very helpful in tracking down information and venders.

- Within the EIA/TIA–568Aspecification there are two connector terminations T568A and T568B. These differ only in the nomenclature of the various pairs. Attempting to find the preferred version was an exercise in frustration, with much misinformation. Turns out, T568A is the preferred implementation, T568B is an optional pinout to provide backward compatibility with AT&T Merlin telephone systems. To add to the confusion EIA/TIA is working on a revision to the EIA/TIA568A spec called EIA/TIA568B.

- Tooling is expensive and it is hard to determine what is needed. Three tools are required

  1. 110 punchdown tool for the receptacles. The connectors use an insulation displacement connector system. This is based on the 110 series telephone punchdown blocks originally used to interconnect voice telephone systems.

  2. Cable stripper. Even though the wire termination use insulation displacement termination the outer cable conductor needs to be stripped first. Since Category 5 wire use a loose fill construction a special jacket stripper is required that indexes on the outside of the jacket, this is the opposite of most cable strippers.

3. Crimp tool for the Category 5 RJ45 plugs. A typical large-scale installation uses a 110 tool to punchdown the connection the receptacle and to a punchdown patch panel in the wiring closet. Patch cables connect the hub to the appropriate facility cable. Normally the patch cables are purchased preassembled. Since I chose not to use punchdown blocks I had to terminate each facility cable in the wiring closet with a RJ45 plug. The crimping tool used for Category 5 "RJ45" plugs is not the same as used for telephone plugs. It is incorrect to call this a RJ45 it is a T568A or T568B. The mating interface is the same as the Telephone Company RJ45 but I believe the cable retention mechanism and internal details are different.

•   Proper tooling is absolute essential; the plugs and jacks cannot be terminated properly by using commonly available hand tools.

•   The wire is more fragile then other wire used in residential construction, it must be feed correctly to keep it from kinking and stables or aggressive use of tie-wraps easily crushes it.

Having said all that, the actually wiring process went well. I installed 8 outlets in three locations in about five hours. They all tested correct the first time.

Appendix B   Modem Access Adapter

The modem is located in the gateway server and automatically dials the ISP whenever one of the clients attempts to access a non-local resource. This is a great feature because to the clients it looks as if they are permanently connected. Establishing the initial connection incurs the typical dialup delay, this result in a short additional delay loading the first web page. When the connection is idle for more then 10 minutes the gateway automatically disconnects.

If the telephone line is not dedicated to the gateway server telephones and modem will interfere with each other. The modem cannot tell if the phone is in use and the phone cannot tell if the modem is being used. Another consideration is that sites implementing an Internet connect LAN are likely to have more then one telephone line. To make the implementation as flexible as possible we need to insure that the modem does not interfere with telephone calls, telephone calls do not interfere with the modem, and where more then one telephone line is available the modem searches for an idle line.

There are devices on the market that monitor phone usage by sensing the voltage on the telephone line. These are sold as data protection and privacy devices. When the line is not in use the voltage on the telephone line is approximately 48 volts. When the phone is picked up the voltage drops to around 7 volts. The device monitors line voltage and disconnects the extension whenever the line voltage drops below threshold. There are several problems with this type of device. One is needed for each line at each phone. Multi line phones typically implement line usage indicators that work on the same voltage sensing principle. Unfortunately the voltage drop across the protection device is so high that the line indicators fail to detect other phones. Lastly, since the devices are designed to prevent phones from interfering with each other, they also prevent using several extensions to talk to the same person.

The Modem Access Adapter is designed to address these shortcomings. When it detects the modem attempting to place a call it searches the telephone lines to see if they are in use. If it finds an idle line it disconnects that line from the extension phones and connects it to the modem. This prevents extensions from interfering with the data call. Disconnecting the extensions from the phone line cause the busy light to turn on indicating the phone is in use. If all the telephone lines are in use the modem aborts the attempt when is detects no dial tone.

To disconnect the extension phones requires that the adapter is placed between the extension phones and the Telephone Company supplied network Interface. A single telephone line connects the adapter to the gateway server modem.

The adapter does not address call-waiting issues. It does not have a mechanism to inform the modem which line it is connected to. If that feature was added and the Dial Up Networking software driver modified the computer could selectively disable Call Waiting. In the current setup when call waiting happens the modem automatically disconnects. This allows the phone to ring normally. The server redials the modem to reestablish connection with the ISP.

Appendix C   NIC's and Hubs

The price points for 100TX Ethernet are falling. New systems should be 100 Mbps only. If a combination of 10Mbps and 100Mbps NICs are used a switching hub must be used. A switching hub cost more per port then simply replacing the PCI NIC.

One of the PCs is and an old 486 ISA machine. I looked into the alternatives, using a 10/100 ISA NIC's or a switching hub. Both of these solutions are very expensive PCI 10/100 NIC's cost approximately $30, the ISA version is $150. Using different speed NIC's requires a switching hub. These are also very expensive since they require a FIFO behind each drop. Also, hub power consumption is relatively high, which increases operating cost.

I chose to stay with 10baseT. Wherever possible I purchased 10/100 NIC's to simplify future upgrade to full 100Mbps. The hub is a simple 8 port unmanaged 10BT device that costs approximately $50. Power consumption is under 5 watts.

At first look there is little reason to implement a 100Mbps LAN. The ISP link is limited to less then 56Kbps down and 33kbps up. This means WAN traffic consumes less then 1% of a 10mbps LAN. As an experiment I stated a large PC to PC file transfer while listening to a real audio broadcast. The LAN was running at 70% utilization, which caused to broadcast to become unusable. This is not an unrealistic scenario considering the printer is a shared resource and the LAN has access to a local web server. Emerging Quality of Service (QOS) protocols will improve the situation. Overprovisioning is another solution. The greater the bandwidth the less important it is to closely manage bandwidth consumption.

Appendix D   Gateway Server Hardware

The gateway server performs a complex suite of services. It manages the local IP network (DHCP & DNS), provides file and print services, is a Web server, implements an Internet firewall and translates the private IP addresses on the LAN to the single IP address issued by the ISP (NAT).

The gateway is a x86 notebook with a NIC and modem, running Windows 98. The reasons I choose a notebook are the same Bill Laing stated in his memo Secure Home (Inter) networking, "it is quiet, low power, has built in battery backup (it doesn't need to reboot after a power failure, is small, and I had one."

Power consumption is a critical concern, when the unit is placed in standby with the display off and the HDD spun down, it draws about 12 watts AC. In standby mode the CPU is still running so it responds to normal network traffic. Next generation PCs with ONnow improve the way NIC's respond to network traffic during suspend. Prior to entering suspend wakeup templates are loaded in the NIC. The NIC evaluates all incoming packets against this template. If the data matches the templates system is restarted. This reduces power consumption to the 3-5 watt level, at the expense of somewhat increased latency.

Appendix E   Gateway Server Software

The server uses Windows 98 and a number of add-on software packages.

Operating System -- Windows 98

TCP/IP stack

This is the only network stack in the server. It is the standard TCP/IP stack supplied by Microsoft. This requires deleting NPX and NetBEUI. I wanted to run a pure IP network. The details are listed below:

- Server IP STATIC address set to 192.168.0.1. This is an IETF defined private address. These addresses are only valid on the LAN.

- Subnet mask set to 255.255.255.0 SOHO Network is limited to 254 devices.

- DNS entries point to the DNS server provided by the ISP. WinGate provides DNS for the local LAN

- File and print sharing turned on.

- The Server is configured as THE Browsemaster. This allows browsing the local network. If this is not enabled clients can connect to other machines but they cannot brows them.

- Computer name and workgroup entered.

- No LMHOST or other hardcoded name or address info.

- No Login Password

File sharing

Ideally file sharing should be FTP; this allows the web browser to provide a common interface to internal and external files. The Personal Web Server (PWS) does not support FTP in Windows 98. File transfer is done through traditional network means.

File sharing requires enabling sharing in the TCP/IP stack as described above and sharing enabled in the properties of each shared device. I've enabled read only sharing of the server's hard disk and CD. Optionally this can be configured to force the user to supply a password.

Print sharing

The printer is a HP 722 inkjet color printer; it is directly attached to the parallel port of the gateway server. This dictates the placement of the server. Locating the server close to the printer requires a dedicated telephone line to connect the modem in the server to the modem access adapter.

Configuring the printer required enabling print sharing in the Windows network configuration and loading the network printer driver.

Web Server

Microsoft includes Personal Web Server and Front Page Express with Windows 98. PWS is used to setup a local web server inside the firewall. This provides a central access point for common data. PWS has a web wizard that allows the creation of simple web pages.

The web server can also be used to create and debug public web pages hosted by the ISP. Microsoft provides a mechanism to automatically upload this information to the ISP.

Proxy Server – WinGate

WinGate is a third party application that provides a firewall between the SOHO LAN and the Internet. The firewall insures that only authorized communication takes place. It hides the details of the local LAN using a technique called Network Address Translation (NAT) to allow all the PCs on the LAN to use a single ISP assigned IP address.

WinGate provides basic network support features. Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses to the client machines. Domain Name Service (DNS) maps the numeric IP address to a human friendly name.

The current implementation does not allow connections to originate from the Internet. All traffic originates from the SOHO LAN or the gateway server. Preventing access from the Internet dramatically simplifies the task of protecting the LAN. WinGate can be configured to allow access to a public web site. However, I think that even when DSL services roll out most SOHO sites will not host their own web site. Rather they will use the ISP to provide hosting services. This leverages the high-speed connection of the ISP. With remote hosting web pages are created and debugged on the local private web server, then uploaded to the public web server hosted by the ISP.

DHCP - Dynamic Host Configuration Protocol

The Internet Protocol (IP) requires that each device have a unique identifier. For IPv4 this is a 32-bit address. Each device on the Internet must have a unique address.

Traditionally the address of each Internet device was manual assigned to the device. This became increasing cumbersome as network size grew. To solve this problem the IETF created Dynamic Host Control Protocol (DHCP) which allows a client to obtain its IP address automatically from a DHCP server.

- rfc2131.txt -- Dynamic Host Configuration Protocol. R. Droms. March 1997. (Status: DRAFT STANDARD)
- rfc2132.txt -- DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997. (Status: DRAFT STANDARD)
- rfc1534.txt -- Interoperation Between DHCP and BOOTP. R. Droms. October 1993. (Status: DRAFT STANDARD)
- rfc1533.txt -- DHCP Options and BOOTP Vendor Extensions. S. Alexander & R. Droms. October 1993. (Status: PROPOSED STANDARD)

WinGate includes a DHCP server; this eliminates the need to configure individual machines.

DHCP is enabled by default, no configuration is needed.

Windows 98 implements a new feature that automatically picks an IP address if it cannot find a DHCP server. This was done to allow enable applications that require an IP address. This causes some problems when initially configuring the network. The address Microsoft picks may be beyond the range of the 255.255.255.0 subnet mask used by WinGate. This causes pings between machines to fail. Once the WinGate DHCP server is up and running this is not a problem.

DNS – Domain Name Service

The 32 bit IP address is displayed as four three-digit values in the form "nnn.nnn.nnn.nnn." This format is inconvenient for humans to use. DNS provides the translation of these numeric values to the more familiar URLs such as compaq.com.

- [rfc1035.txt](rfc1035.txt) -- Domain names - implementation and specification. P.V. Mockapetris. Nov-01-1987. (Status: STANDARD)

- [rfc1034.txt](rfc1034.txt) -- Domain names - concepts and facilities. P.V. Mockapetris. Nov-01-1987. (Status: STANDARD)

WinGate provides DNS for DHCP addresses it assigns on the local LAN. When the link with the ISP is active the local DNS server is cascaded with the DNS servers of the ISP. This part of the configuration is somewhat confusing since the DNS entries for the network adapter point to the ISP not WinGate.

As of this writing I'm still debugging the cause of slow DNS translation. It takes DNS several seconds to resolve the server name the first time the server is accessed.

NAT – Network Address Translation

ISP's typically issue a single dynamic IP address during user login. To communicate each device requires a unique 32-bit address. The IP address of each client must be mapped to the single IP address issued by the ISP. Network Address Translation solves this mapping problem. Each machine is issued an IP address from the pool of addresses reserved for private networks (RFC1918). These addresses are unique within the LAN, and they are guaranteed to be unused on the Internet. The DHCP server on the LAN allocates addresses from this pool. When a request cannot be fulfilled on the LAN NAT translates the private IP address to the IP address issued by the ISP. NAT allows multiple clients to share a single IP address in real time.

- [rfc1631.txt](rfc1631.txt) -- The IP Network Address Translator (NAT). K. Egevang & P. Francis. May 1994. (Status: INFORMATIONAL)
- [rfc1918.txt](rfc1918.txt) -- Address Allocation for Private Internets. Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot & E. Lear. February 1996. (Status: BEST CURRENT PRACTICE)

The Internet Assigned Numbers Authority (IANA) reserved the following three blocks of IP addresses for private internets:

Start Address	End Address	
10.0.0.0	10.255.255.255	1 Class A (16M)
172.16.0.0	172.31.255.255	16 Class B (1M)
192.168.0.0	192.168.255.255	256 Class C (64K)

The SOHO LAN DHCP server is configured to assign addresses in the 192.168.0.x range. The server utilizes a static address of 192.168.0.1. The DHCP server assigns addresses from this pool of 252 addresses.

Proxies and Mappers

Proxies provide isolation between the LAN and outside world. Requests generated from within the LAN are examined, and if approved, forwarded out to the Internet. The local devices are never directly connected to the external world. Requests that originate from the Internet are rejected.

Mappers function like patch cords. They connect a request coming in on one port to a predefined service.

WWW -- World Wide Web

- [rfc2068.txt](rfc2068.txt) -- Hypertext Transfer Protocol -- HTTP/1.1. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners-Lee. January 1997. (Status: PROPOSED STANDARD)

- rfc1945.txt -- Hypertext Transfer Protocol -- HTTP/1.0. T. Berners-Lee, R. Fielding & H. Frystyk. May 1996. (Status: INFORMATIONAL)

WinGate is configured to proxy HTTP on port 8080. HTTP requests that come in on port 8080 are forwarded to the ISP to connect to the appropriate web server. To support the PWS server running on the same machine, the address of the proxy must be different then that of the web server. The well known default port for http is 80. So this does not conflict with proxy access. Browsers use port 80 by default when they bypass the proxy to access the PWS. This allows the browser to bypass the proxy when accessing the local web server.

FTP – File Transfer Protocol

- rfc2228.txt -- FTP Security Extensions. M. Horowitz, S. Lunt. October 1997. (Status: PROPOSED STANDARD)
- rfc959.txt -- File Transfer Protocol. J. Postel, J.K. Reynolds. Oct-01-1985. (Status: STANDARD)

This proxy is used to support username.password@server.domain method of firewall transversal. Neither Microsoft Explorer nor Netscape use this method. The browser uses the HTTP proxy for FTP transfers.

This proxy is not used

Telnet

- rfc855.txt -- Telnet Option Specifications. J. Postel, J.K. Reynolds. May-01-1983. (Status: STANDARD)
- rfc854.txt -- Telnet Protocol Specification. J. Postel, J.K. Reynolds. May-01-1983. (Status: STANDARD)

Telnet is a terminal-remote host protocol.

This proxy is not used.

NNTP – Network News Transfer Protocol

- rfc977.txt – Network News Transfer Protocol. B. Kantor, P. Lapsley. Feb-01-1986. (Status: PROPOSED STANDARD)

This proxy is used to access Internet news groups. WinGate is configured to map NNTP requests on port 119 directly to the ISP news server.

SMTP – Simple Mail Transport Protocol

- rfc821.txt -- Simple Mail Transfer Protocol. J. Postel. Aug-01-1982. (Status: STANDARD)

SMTP is used by the mail client to send Internet mail. WinGate is configured to map SMTP requests on port 25 directly to the MCI Mailrelay.

POP3 – Post Office Protocol

- rfc1957.txt -- Some Observations on Implementations of the Post Office Protocol (POP3). R. Nelson. June 1996. (Status: INFORMATIONAL)

- [rfc1939.txt](rfc1939.txt) -- Post Office Protocol - Version 3. J. Myers & M. Rose. May 1996. (Status: STANDARD)

The mail client to retrieve mail from the Internet mail server uses the POP3 proxy. It listens on port 110.

IMAP4 – Internet Mail Access Protocol

- [rfc2060.txt](rfc2060.txt) -- INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1. M. Crispin. December 1996. (Status: PROPOSED STANDARD)

This is another mail standard. It is not used in this implementation.

Real Audio

The proxy supports streaming audio from Real Audio.

Real Audio proxy listens on Port 1090. It is used to deliver audio streams over the web.

VDOLive
This is another multimedia proxy, listens on Port 7000.

Xing Streamworks
Yet another streaming audio format Listens on port 8000.

Socks 5

- [rfc1961.txt](rfc1961.txt) -- GSS-API Authentication Method for SOCKS Version 5. P. McMahon. June 1996. (Status: PROPOSED STANDARD)
- [rfc1929.txt](rfc1929.txt) -- Username/Password Authentication for SOCKS V5. M. Leech. April 1996. (Status: PROPOSED STANDARD)
- [rfc1928.txt](rfc1928.txt) -- SOCKS Protocol Version 5. M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas & L. Jones. April 1996. (Status: PROPOSED STANDARD)

Socks implements strong authentication in finer manner then traditional transport level firewalls. This provides better security in client server relationships.

The SOCKS proxy listens on port 1080.

Demand Dialing
When a client machine requests a resource that is not on the LAN WinGate automatically establishes a connection to the ISP. It uses Microsoft Dial Up Networking (DUN) to connect to the ISP. It also monitors ISP traffic and disconnects after a predetermined idle period. To the user it appears as if the client machines were permanently connected.

- [rfc1661.txt](rfc1661.txt) -- The Point-to-Point Protocol (PPP). W. Simpson, Editor. July 1994. (Status: STANDARD)

WinGate is configured to make three dial attempts to the local MCI POP. It automatically disconnects when the link is idle for 10 minutes.

The dial up adapter is bound to the TCP/IP stack. The standard Microsoft TCP/IP dial up defaults of, Client for Microsoft Network, Microsoft Family Login, and File and print sharing not bound.

This combined with the System Policy setting minimizes the chance of penetration from the Internet.

Bonding

Bonding allows multiple ISP connections to be used to increase total throughput. Two modems or ISDN lines can be bonded together to double the data rate between the LAN and ISP. Each device carries half the total traffic.

This feature is not used.

System Policies

WinGate is configured to only accept connections that originate from the LAN or the local host. This effectively prevents connections being initiated from outside the local network.

GateKeeper

GateKeeper is WinGate's user interface. GateKeeper is available locally on the server and in the WinGate Pro version it can be run remotely from the clients.

GateKeeper requires a system administrator to enter a password. After authentication the administrator has access to all Gatekeeper functions.

Time Synchronization -- Tardis

The IETF developed protocols to synchronize multiple computers to master atomic clocks. This automates setting the RTC clocks on the SOHO networks. Clock accuracy is vastly improved from the standard PC RTC error of one minute a month.

Two IETF RFCs concerning time:

- rfc1305.txt -- Network Time Protocol (Version 3) Specification, Implementation. David L. Mills. March 1992. (Status: DRAFT STANDARD)
- rfc1361.txt -- Simple Network Time Protocol (SNTP). D. Mills. August 1992. (Status: INFORMATIONAL)

In the US the NIST maintains public NTP and SNTP servers. These are very accurate atomic clocks. Other governments provide similar services. This allows anyone with Internet access to obtain atomic clock accuracy. The NIST servers listen for a NTP request on port 123, and respond by sending a UDP/IP data packet in the NTP format. The data packet includes a 64-bit timestamp containing the time in UTC seconds since January 1, 1900 with a resolution of 200 picoseconds.

I found a Shareware program called Tardis that uses SNTP to access public Internet timeservers. It monitors the dialup connection and queries NIST timeserver every 10 minutes. This synchronizes the server real time clock to the NIST timeserver. Tardis is also used as the timeserver on the LAN. It uses the NTP protocol to broadcast this information to all LAN clients. This allows simple software on the client to listen to the NTP broadcast and synchronize the local RTC. The software uses the Windows Time Zone setting to convert UTC to local time. This guarantees all PCs on the LAN have the same time and that it is in close agreement with the primary time standard.

Server Addresses

The NIST Network Time Service uses seven stratum-1 timeservers located in Boulder, Colorado, Gaithersburg, Maryland (Washington, D.C. area) and Redmond, Washington. Additional servers are planned. The servers are:
- time-a.timefreq.bldrdoc.gov (132.163.135.130)
- time-b.timefreq.bldrdoc.gov (132.163.135.131)

- time-a.nist.gov (129.6.16.35)
- time-b.nist.gov (129.6.16.36)
- time.nist.gov (192.43.244.18)
- time-nw.nist.gov (131.107.1.10)
- utcnist.colorado.edu (128.138.140.44)

NTP and SNTP Format

NTP and SNTP use the same timestamp. The integer part is in the first 32 bits and the fraction part is in the last 32 bits. The precision of this representation is about 200ps. Internet latencies reduce this to typical accuracy of +/- 100ms. This is more then adequate for our purposes.

The 32-bit integer will overflow on February 6 2036. Corrective action must be taken before that time to address the rollover problem.

Occasional leap seconds are introduced into the UTC time system by international agreement for keeping the atomic-based time scale in approximate agreement with the astronomical time scale, UT1, which is based on the rotation of the earth. Even though the atomic UTC time scale is much more uniform than the UT1 scale, some users must work with earth-based time. Since time-and-frequency radio stations such as WWV normally broadcast only UTC time, the broadcasters agreed to occasionally adjust UTC time in steps of exactly 1 second so that the difference between UTC and UT1 would never exceed 0.9 seconds. Leap seconds have been inserted as needed into the UTC time scale since 1972 at average intervals slightly longer than one year.

Appendix F Client Hardware

Clients consist of desktop and laptop PCs. All but one is Pentium based, the orphan is a 468DX2-66.

Any device equipped with an UTP Ethernet connection can be connected to the SOHO LAN.

Appendix G   Client Software

Windows 9x

The 486 client runs Windows 95 all other clients use Windows 98. Network protocol is TCP/IP. This is the only protocol running.

Clients are configured for dynamic IP address assignment, except for the notebook they all have the same work group "Home LAN", and browsmaster is turned off. This insures that only the server will be elected as browsmaster.

Browser

The Browser is Microsoft Internet Explorer version 4.

The browser is configured to use the WinGate proxy for HTTP, Secure HTTP, FTP, and SOCKS for everything else. The http port is 8080 and the SOCKS port is 1080. Access to local web server bypasses the proxy.

Mail

Most ISP's offer mail service as part of the monthly service cost. At first glance this looks the optimum solution. The problem with using the ISP mail is threefold.

- The mail account login is tied to the ISP login. So even in the case where an ISP offers separate e-mail accounts only a single e-mail account can be open at a time. This is obviously a problem for a SOHO LAN.

- Additional e-mail accounts are not free. Typical cost is $5.00 per month per account. While this isn't a large amount of money, for heavy e-mail users, it does seem excessive for occasional use.

- Since the email account is issued by the ISP changing ISP's require obtaining a new e-mail address.

The solution is to use one of the free advertising supported e-mail accounts. The down side is that one has to put up with advertising banners. The two most popular are RocketMail and Yahoo. These do not require e-mail client software as they use standard web browser.

Each account is password protected and has the ability to include attachments.

Time Synchronization -- K9

This is a companion to the Tardis software used on the server. It listens for NTP broadcasts from the LAN to continually set the local RTC.

This allows the client real time clock to be maintained to within one second of the NIST timeservers. K9 is started automatically at boot time from the startup menu. It runs in the background to automatically update the client clock.

Point Cast

Point Cast provides a subscription to news and stock quotes. The client machines access a Point Cast server to download the latest news.

PointCast offers a free caching server to minimize Internet traffic. It only runs on NT so I could not try it. This would be a very useful addition for business users.

PointCast version 2.5 is configured to use the HTTP proxy at port 8080 and SOCKS on port 1080.

Real Audio

Real Audio allows the transfer of audio and video streams at relatively low data rates.

RealPlayer version 5 uses the Real Audio proxy at port 1090.

Acrobat Reader

The Adobe Acrobat Reader is used to view Portable Data Format (PDF) files. This is commonly used to transmit electronic documents on the web. It is optimized for printing typeset documents and is primarily a read only format.

This is a browser plugin.

WinZip

The WinZip utility from Nico Mak Computing is commonly used to compress files. The reduced size significantly speeds up Internet transfer.

This is a browser plugin.

NetSwitcher

NetSwitcher allows the user to quickly change network settings when the notebook is moved to different LANs. The PC is manually configured at each site, then NetSwitcher takes a snapshot of the configuration. This allows the user to quickly switch between network settings. Even though this is a rather brut force mechanism it works surprising well. NetSwitcher is not a perfect solution it requires rebooting if some setting are changed, and the only application it supports is Internet Explorer.

This could easily be automated by extending DHCP. During the boot process the client obtains site specific configuration settings in addition its IP address from the DHCP server. For a short-term solution this can be done using vender specific DHCP extensions and reverse engineering the Windows registry keys used by various applications.

The long-term solution needs to be driven by the IETF to modify the DHCP specification and by Microsoft to standardize the APIs applications use to obtain network information.

Appendix H   Equipment Cost

This section is intended to provide a feel for typical SOHO LAN costs.

Facilities Cabling

The table below itemizes the components needed to wire a home or small office with 16-combination telephone and LAN outlets. For a do it yourself solution add the cost of tooling, 110 punchdown tool ($60), RJ45 crimper ($50), and cable striper ($7) this bring the total cost for wiring to $500.

Quantity	Component	Usage	Price	Total
16	Single gang electrical box	Dual	$.50	$8.00
16	Category 5 T568A receptacle	LAN	$5.50	$88.00
16	Category 3 RJ11 receptacle	Tel	$4.00	$64.00
16	Single gang two hole faceplate	Dual	$2.50	$40.00
16	Category 5 plug	LAN	$1.00	$16.00
1	2 pair terminal block	Tel	$2.00	$2.00
1000 ft	Category 5 4 pair PVC wire	LAN	$120.00	$120.00
1000 ft	Category 3 2 pair PVC wire	Tel	$55.00	$55.00
			Total	$393.00

Having the system professionally installed in an existing house is probably 1-2 man-days, less for new construction. Estimated labor rates are $50-$75 per hour. This brings total cost to $800- $1,600.

Modem Access Adapter

The bill of materials for this device is approximately $25.

NIC's and Hubs

10 BT ISA NIC is $20; PCI 10/100TX NIC is $40
10BT 16 port unmanaged hub is $100. 16 port 100TX only unmanaged hubs is $500.
Category 5 patch cables are $3, use one to connect each computer to wall jack

Server

The ideal candidate middle of the road desktop PC optimized as a server.

WinGate come in flavors licensed by the number of client machines. The deluxe version called WinGate Pro allows remote administration and user authentication . Gatekeeper can be run on any client. The Pro version is more appropriate for the small business while the cheaper Lite is fine for home users. For a 5 usr license Lite retails for $110, while Pro is $250. The license is based on the number of simultaneous Internet accesses, not the number of physical clients.

This software can be upgraded by obtaining a new key. All WinGate packages are the same; the key simply enables different features.

The Tardis timeserver software is $20.

Client

License for 5 K9 time setting clients is $30.

NetSwitcher is $8 per copy.

Appendix I Monthly Operating Cost

PC users do not concern themselves with the ongoing computer costs, Once the machine is purchased incremental use is free. As these devices become more "connected" monthly service cost need to be factored in.

Telephone Line

Bell Atlantic offers unlimited local calling for approximately $20 per month. The exact amount varies depending on the size of the local calling area. The calling area needs to be large enough so the ISP is a local call. Optional features, Call waiting $4.00 month, Caller ID $5.00-6.00 month, Hunting feature is free.

ISP

Cables and Wireless dialup service costs $15 a month for 150 hours of Internet access. Includes is a single mail account and non-commercial web hosting.

Domain Hosting

InterNET Resources NETworks changes $10 a month to host a light duty web server and provide E-mail service, large sites and ones generating a lot of traffic cost more. Domain registration through InterNIC is an additional $35.00 per year

Electricity

New England electric rates are among the highest in the country at $.15 a kilowatt-hour. Minimizing idle power consumption is critical.

Device	Power
Gateway Server	15W
Printer	3W
10BT Hub	3W
Modem Adapter	2W
Total	23W

This is approximately 17Kwh per month. It increases monthly electric cost by $2.50. This doesn't sound like much but it represents approximately 1.5% of our monthly electric bill. Clearly, increasing residential electric consumption by 1.5% is undesirable. Hopefully this will be offset by lower PC power consumption.