Sun City Summerlin Computer Club Seminar

Advanced Networking

Tom Burt
September 22, 2004

This 2 1/2 hour seminar is the third of a three part series on computer networking. This seminar will explore more advanced networking concepts. We'll also keep some time open to answer your networking questions.

This seminar's target audience is users who are pretty comfortable with their PC and Windows and want to move up to taking better advantage of having multiple PCs.

Tom Burt (tnburt@ieee.org)

Where to Find the Materials

Sun City Summer Computer Club Website:

http://www.scscc.com/smnr

- **Acrobat file of these slides and Notes**

Go to the "smnr" page on the Club web site using the link above.

Find the link to this "Advanced Networking" presentation, which is saved as an Adobe Acrobat PDF file. Also look for link to the "Advanced Networking" presentation, which is also saved as an Adobe Acrobat PDF file.

Click the link to open the PDF document.

From there, you can print the document by clicking on the printer icon or you can save it to your hard disk by clicking the diskette icon.

Seminar Agenda

- **Brief Networking Refresher**
- **Helpful Web Site Links**
- **Global Structure Of The Internet**
- **TCP/IP – Nuts and Bolts**
- **File and Print Sharing Via TCP/IP (No IPX/SPX)**
- ***-- Bio Break (~10 min)***
- **Mixed-OS Home Networks (WinXP, Win9x, Mac)**
- **Tuning Your Router / Firewall**
- **Setting Up Your Own Home Web Server**

- **Open Questions and Answers**

The Agenda above is for the Advanced Networking seminar.

Our goal in this presentation is to refresh some of the concepts from the earlier Networking seminars and then to get to the Advanced Networking topics.

We'll take a quick look at some helpful web links where you can find more information.

We'll look at how information moves around a TCP/IP network, whether in-house or on the Internet.

We'll look briefly at setting up home networks that integrate Macintosh and Windows 9x PCs with Windows XP PCs.

We'll look at how to share files and printers using only TCP/IP without including the IPX/SPX protocols.

We'll spend some time looking at the settings of your home hardware firewall / router to see what can be done to enhance security.

Refresher

- **Networks allow computers to communicate.**
- **Why Have a Home Network?**
  - **PCs can share: files, printers, Internet connection.**
  - **Each PC can back up the other's data.**
- **Simple Home Networks are easy to set up.**
  - **Network cables, router or switch.**
  - **Enable client / server software configuration.**
- **Wireless networking uses 2.4 GHz radio spectrum.**
  - **11 Mbits (802.11b) per second or 54 Mbits per second (802.11g) standards.**

TNB Sept 22, 2004 **Advanced Networking**

Networking is the process of connecting two or more computers together so that they can communicate with one another. Networks can also communicate with other networks, making possible vast interlinked sets of computers.

Our focus in Beginning Networking was on very simple home networks of two or a few PCs, connected to each other using Ethernet cables. Using a simple network of this type allows the connected PCs to share printers and files and also, if you have a wide-band Internet connection, such as DSL or Cox cable, to share that connection as well, so that all PCs on the net can concurrently access the Internet via the high-speed connection.

Simple mixed (wired and wireless) home networks are easy to set up. You do need some equipment and you need to configure some software to get it all to work, but generally, once a network is set up, it needs little if any additional tinkering, at least until you add another PC or change some other aspect of the configuration.

In Intermediate Networking, we looked at Wireless Networking, which uses a "hub and spoke" topology. There is a central switching point, the Wireless Access Point (WAP) that all the other remote nodes communicate with. Each remote node sends and receives via its own attached or built-in Wireless Network Adapter (WNA).

Advanced Networking Web Links

- http://www.cybergeography.org/atlas/topology.html
- http://www.freeprogrammingresources.com/tcp.html
- http://www.tcpipguide.com/free/
- http://www.protocols.com/pbook/tcpip2.htm
- http://www.linksys.com
- http://www.netgear.com/
- http://www.dlink.com/
- http://www.belkin.com
- http://www.networksorcery.com/enp/protocol/ip/ports00000.htm
- http://www.grc.com/
- http://www.whois.sc/
- http://www.microsoft.com/windowsxp/using/networking/default.mspx
- http://support.microsoft.com/default.aspx?kbid=314067
- http://www.asp.net/webmatrix/

- **Win XP Help and Support (Networking and the Web)**

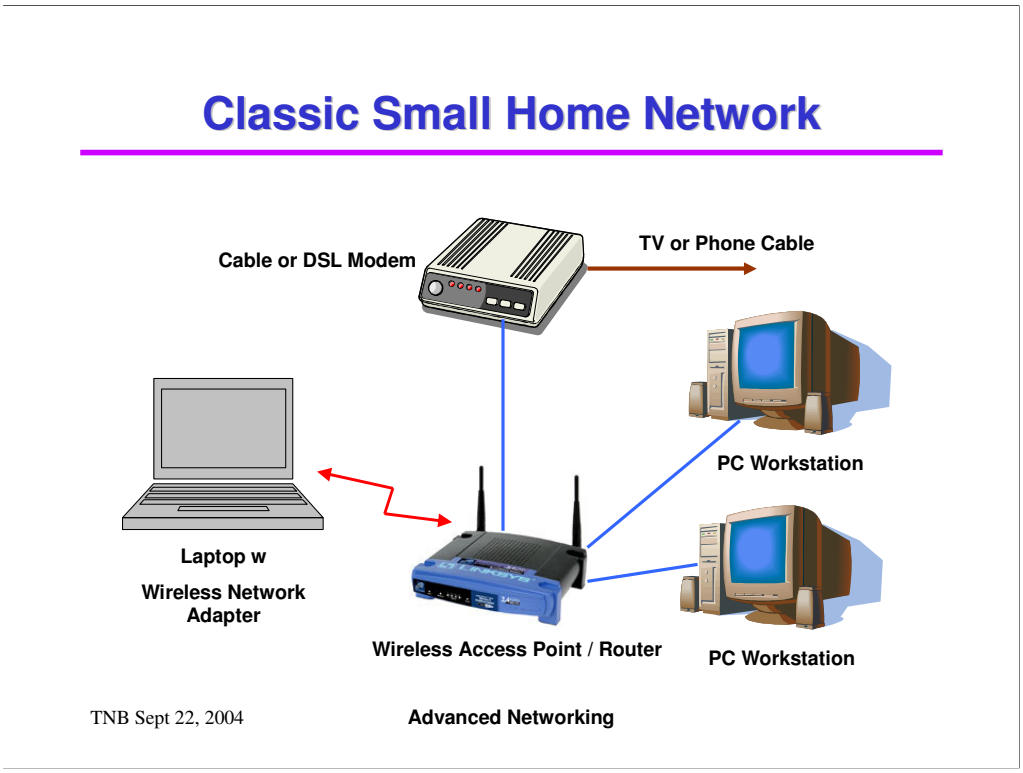
TNB Sept 22, 2004 **Advanced Networking**

The above hyperlinks go to some interesting general information sites about TCCP/IP and the Internet as well as to the major home networking equipment vendors' web sites. All these vendors provide a wealth of technical information.

There is also a link to the Microsoft home networking site, which again has much useful information.

I've also included a link to the Web Matrix authoring tools.

Finally, the Windows XP Help system has extensive information on networking which is worth reading for more information.



Above is the archetypical simple mixed wired and wireless network configuration diagram.

We have one or more PC workstations, connected by Ethernet cables to an integrated WAP / router. The switch provides high speed connections between each of the other Ethernet "wired" devices connected to it. The "wired" links run at 100 million bits per second.

We also have a laptop computer connected by a wireless link to the same WAP / router. The wireless link may run at (up to) either 11 million bits per second or 54 million bits per second. Due to distance, obstacles and interference, it may run much slower.

In addition to its routing firmware, the router may also contain Internet firewall firmware

The router is connected by Ethernet cable to a cable or DSL modem.

The Cable or DSL modem is connected to the TV coaxial cable or to the DSL telephone jack, which provides the connection to the external Internet.

Wired Networking Hardware

- **Network Interface Card / Chip (NIC)**
  - Every NIC has a unique 6 byte (48 bit) physical address.
  - Try IPCONFIG /ALL to see yours.
- **Ethernet Cable (Category 5 or 6)**
  - Costs about $1 per foot retail for short cables.
- **Hub / Switch**
  - Usually 4 Ethernet ports + a WAN port and Uplink port.
  - Also comes in 8 or 16 ports.
  - One hub or switch can connect to another switch.
  - May also be a Router or Wireless Access Point (WAP).

Network Interface Cards mount inside a PC or may be integrated onto the PC motherboard. They provide the hardware send / receive / control interfaces to an Ethernet cable. Almost all NICs now support dual speeds of 10 and 100 million bits per second. The NIC automatically senses what speed the rest of the network is running and chooses the corresponding speed. The newest generation of NICs can run at 1000 million bits per second (gigabit Ethernet), but such speeds are overkill for home networks today unless you want to stream video to your TV.

Ethernet cables come in two speed ratings: Category 5 for 10/100 Megabit, Category 6 for Gigabit. The are shielded with 4 twisted pairs inside and have 8-pin RJ 45 snap-in jacks at each end. Ethernet cables can be up to 100 feet long.

A hub or switch is a simple interconnection device that has sockets for RJ 45 connectors from Ethernet cables. A hub is an older, “dumb” device that takes every message it receives and sends it to every other device connected to it. A switch looks at the target address in each message and only sends the message out the Ethernet port that target address is plugged into. A hub or switch also acts as an amplifier, so that two PCs can effectively be 200 feet apart if the hub / switch is centered between two long cables.

Wireless Networking Hardware

Wireless Access Point / Router (WAP)

- Provides basic switch functionality.
- Provides dynamic IP address services.
- Provides Network Address Translation (Isolates internal LAN net from Internet).
- Handles 802.11 wireless protocols.

PC Card Wireless Network Adapter

- Remote wireless connection.

USB /wireless Network Adapter

- Remote wireless connection.

TNB Sept 22, 2004 **Advanced Networking**

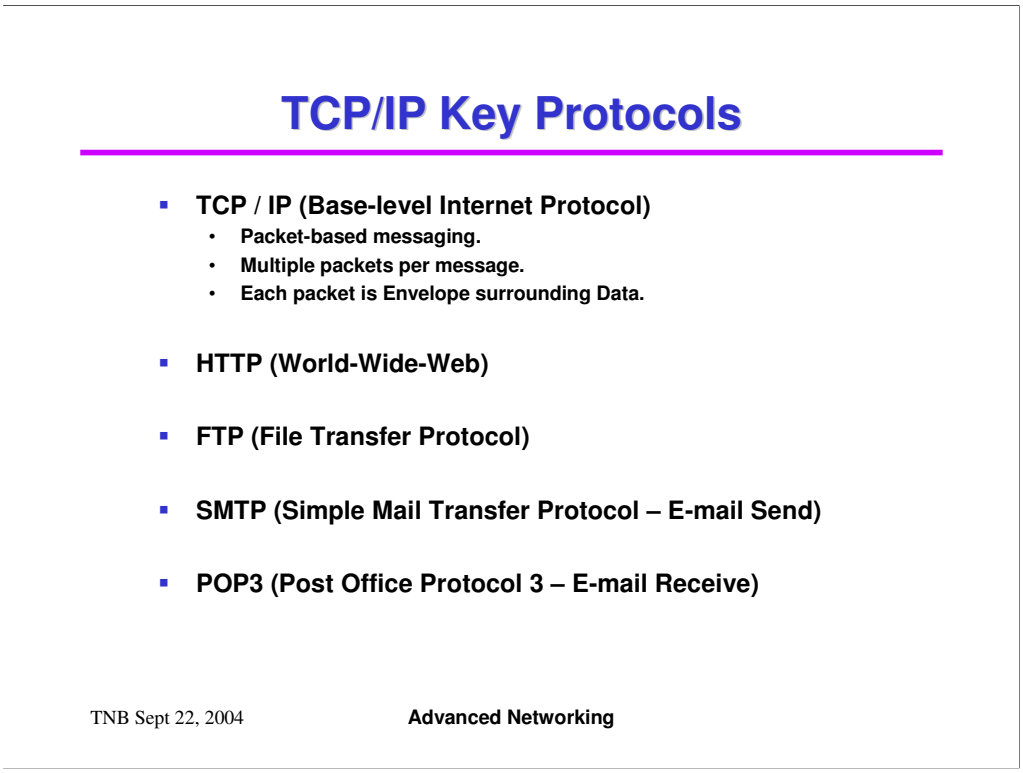
Routers are switches with a much higher level of intelligence. Routers have built in functions to dynamically assign “private” IP addresses from a specified range (DHCP). The router also performs transparent mapping (IP masquerading) of these private IP addresses into a single “public” IP address assigned by the cable or DSL Internet Service Provider. This makes your entire in-house network look like a single PC to the outside world. Routers often also include firewall functionality. Firewalls effectively block incoming TCP/IP connections from all but a handful of standard, “safe” ports. This keeps out hackers.

A Wireless Access Point / Router combines the features of the router and the central 802.11b or 802.11g wireless transmitter receiver.

With either Cox cable or Sprint / Earthlink DSL, whether running a wired, wireless or mixed network, you must have a router in place to allow more than one PC to simultaneously access the Internet. These ISPs only allow one physical connection, i.e. a single IP address, to their network from a given connection point.

A cable or DSL modem converts Ethernet messaging signals to signals compatible with either your cable TV wiring or your special DSL telephone wiring. Cox cable uses two reserved digital channels for the incoming and outgoing message signals. DSL uses specially tuned phone wiring to allow the high speed signals.

Both cable and DSL are asymmetric. Commonly, incoming messages travel at 1.5 Megabits per second; outgoing messages travel at 128 Kilobits per second.



TCP/IP is the core messaging protocol used by computers to communicate over the Internet.

HTTP (Hyper Text Transfer Protocol) uses TCP/IP to send and receive information specifically structured as web pages. A web browser such as Internet Explorer sends requests for web-page content to a web server at some specified address. The web server responds by sending back the requested web page content.

FTP (File Transfer Protocol) uses TCP/IP to support uploading and downloading files between your PC and a remote FTP server.

SMTP and POP3 use TCP/IP to send and receive e-mail address between your PC and a remote e-mail server.

TCP/IP Message Structures

- **Messages are broken into small units called packets.**
- **Each packet has layers of envelope surrounding data.**
- **Each packet has error detection.**
- **Various types of packets.**
- **Demo of Ethereal "packet sniffer" tool.**
  - http://www.ethereal.com/

Message streams are broken up into one or more small "packets" (size varies) by the sender. While the theoretical length of a packet could be a bit over 64000 bytes, in practice, about 1500 bytes is the agreed-upon maximum.

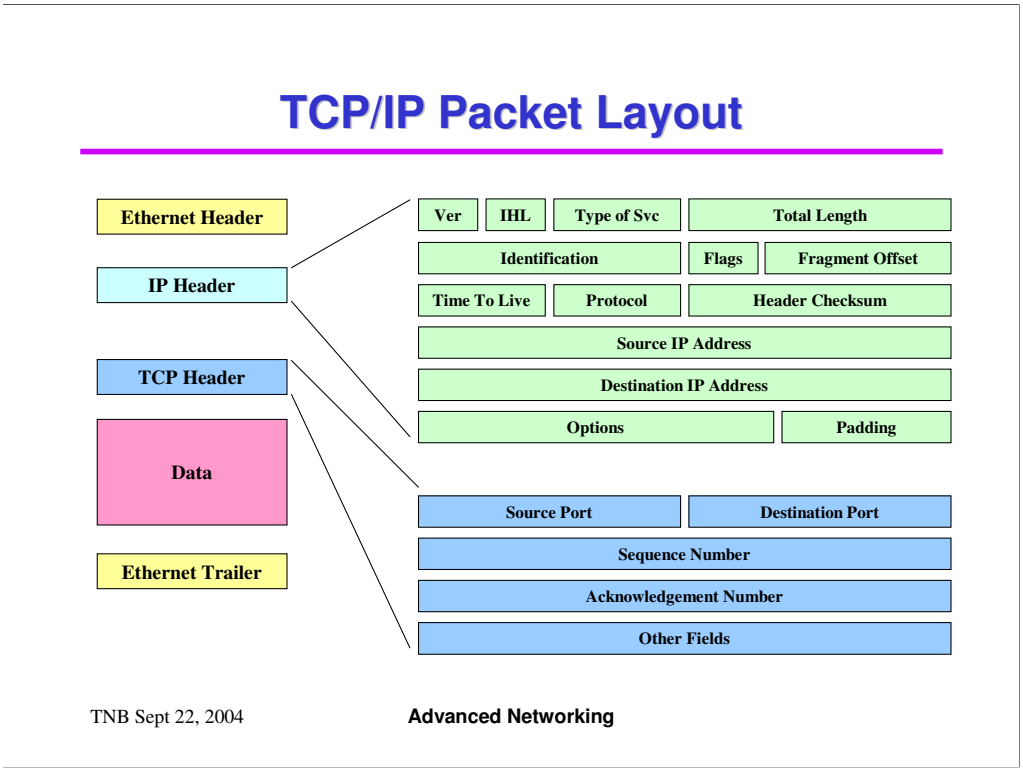
Each packet has headers and trailers that act as an envelope and also provide error detection, so that garbled packets can be detected by the receiver and, on request, retransmitted by the sender.

The envelope includes the address of the sender, the address of the receiver, a sequence number, an error detection and correction check-sum and other useful bits of information to help the Internet get the packet to its destination. The receiver collects the incoming packets, checks them for errors and reassembles them into the correct sequence. If a packet is lost or has an unrecoverable error, the receiver will send a small message to the sender asking for a re-transmit.

To see examples of packets, we will have a short demo of Ethereal, a freeware network monitor (packet sniffer) tool. Once installed, Ethereal's monitoring can be turned on for an interval of time and the captured results can be displayed and saved.

One point of note …

Ethereal can be used by anyone, so it can in theory be used to capture passwords and other sensitive information as it passes by.



The above diagram shows the block layout of a packet.

The IP Header is an envelope for the entire packet. Key fields include:

Ver: The IP version (e.g. 4 or 6)

IHL: Internet Header length (varies with version).

Total Length: Length of packet, including the IP Header

Time To Live: How many seconds (maximum) before the packet is discarded

Source IP Address: IP address of the packet's sender

Target IP Address: IP address of the packet's intended recipient

The TCP/IP Header is an inner envelope for the application and data. Key fields:

Source Port: The TCP port from which the packet originates

Destination Port: The TCP port to which the packet is to be sent

Ports (or sockets) are related to specific TCP applications, such as web browsing or e-mail or file and print sharing.

Common TCP/IP Ports

- http://www.networksorcery.com/enp/protocol/ip/ports00000.htm

FTP:	20, 21	File Transfer
Telnet	23	Remote console
SMTP	25	Outbound e-mail
Gopher	70	Archive searching
HTTP	80	World Wide Web
HTTPS	443	Secure WWW
POP3	110	Inbound e-mail
SFTP	115	Simple FTP
NTP	123	Network Time protocol
NetBIOS	137, 138, 139	File & Print sharing
Site-Defined :	> 49151 (48K)	

Above is a list of some of the common TCP ports used for various application processes.

Network Address Port Translation

- **Router keeps a table of all connected PCs on internal LAN.**
- **Outbound requests from PCs on internal LAN:**
  - **Saved in NAT table**
  - **IP address converted to that of the router.**
  - **TCP requesting port number in header is remapped.**
  - **Modified packet is sent.**
- **Inbound responses to the router:**
  - **Destination port number is looked up in NAT table.**
  - **IP address converted to that of the requesting PC.**
  - **Destination port is converted back to the original port.**
  - **Modified packet is passed on to the actual PC.**

TNB Sept 22, 2004 **Advanced Networking**

Network Address Port Translation, or IP masquerading, is a specialized case of Network Address Translation. A single "real" IP address belonging to the router is used to support multiple IP addresses for PCs connected to it.

For outbound requests, this is done by remapping the "source port" field of the TCP/IP header and substituting the router's IP address for that of the requesting PC. A typical remap might add the number 51000 to the original port number (e.g. port 80 becomes port 51080). The responder to the message will always specify the target port in its response to be the source port of the requestor. The internal PC's original request is remembered in a table.

When the reply comes back to the router from the target of the request, the router looks at the "destination port" field of the incoming TCP header and looks up that port (as the source port) and the sender's IP address in the saved request table. This determines the correct internal IP address to send the response to. The router then adjusts the destination port number (subtract 51000) and IP address in the response's TCP header and forwards the packet to the original requesting PC. Finally, it clears the entry out of the table.

TCP/IP Name / Address Services

- **Dynamic Host Configuration Protocol (DHCP)**
  - **Address server automatically assigns a dynamic IP address to requesting PCs.**
  - **IP address is "leased" to the PC for a set length of time (e.g. 12 or 24 hours). PC can "renew" the lease.**
- **Domain Name Services (DNS)**
  - **Resolves host names like AOL.COM to IP addresses (e.g. 172.20.148.50)**
  - **Experiment with PING command.**
  - **Cox.net DNS servers at: 68.111.16.30 and 68.111.16.25.**

TNB Sept 22, 2004 **Advanced Networking**

Dynamic Host Configuration Protocol (DHCP) is a service that dynamically assigns IP addresses to network computers (PCs, routers, printers, other devices). Each such IP address is "leased" to the requesting PC for a set length of time, such as 12 or 24 hours. A computer can renew or release its lease. Windows XP requests a new lease each time it boots up. The DHCP server has a defined "pool" of address it can lease out. For your local local WAP / router, typical IP addresses in the pool will range from: 192.168.1.100 to 192.168.1.199 – i.e. 100 addresses out of a possible 255. The others are reserved for permanent static assignment to devices like print or database servers. Note that IP address series starting with 192.168.x.y are "special". Those addresses cannot be directly accessed from computers outside your private LAN. The router uses Network Address Translation (NAT) to transparently route traffic between computers on your private LAN and external computers on the public Internet.

Domain Name Services (DNS) servers are special computers on the public Internet that convert human-readable domain names to IP addresses. ISPs like Cox.net, Earthlink.net, AT&T.net all have their own DNS servers. These DNS servers themselves form a network along with the main domain name registration services, such as Network Solutions. These DNS servers regularly synchronize with each other so that most requests to resolve a domain name can be processed by a nearby DNS server. Normally on Windows, you can just let Windows TCP/IP automatically find the nearest DNS server.

Key Local Networking Services

- **Client For Microsoft Networks**
  - Allows a PC to connect to shared files and printers on another networked PC in the same Work Group or Domain.
- **File and Printer Sharing for Microsoft Networks**
  - Allows a PC to share its printers and files with other networked PCs in the same Work Group or Domain.
- **Internet Information Server (IIS) - Optional**
  - Full featured web server that runs on a client PC.
  - Same as web server that runs on MS Windows Servers.
  - Optional install on Win XP.
  - Configure via IIS Administration Tool.

TNB Sept 22, 2004 **Advanced Networking**

The Client for Microsoft Networks service is the core service that allows a Windows PC to access shared files and printers on other PCs on the same Workgroup on a LAN. Originally know as MS-Net or NetBIOS, this service allows a PC to "map" a logical drive to a shared folder on another PC. It also allows a PC to "add" a logical printer that physically resides on another PC. This service is normally installed and set up automatically when Windows is installed. However, it can added or removed later using the Control Panel's Network Connections applet.

File and Printer Sharing for Microsoft Networks is the core service that allows a Windows PC to share its printers and file folders with other PCs on the same Workgroup on a LAN. Printer shares are defined in the Control panel / Printer applet. File folder shares are defined using the Windows Explorer's "Share As" function. Each shared folder is given a "Share Name" and other properties of the share are set. Important Note … the underlying file folder's access control properties must be consistent with those of the share. Otherwise remote users will not be able to access the folder, even though they can connect to the share. This service is not automatically installed. It must be added using the Control Panel's Network Connections applet.

A particular PC may be set up as just a client, just a file and print server, or as both. For a small network, it's generally most effective to have each PC operate as both a client and a server. Each PC can then function as a backup server for the other.

Bio-Break
10 Minutes

NetBIOS Over TCP/IP

- **How do PC's on your home LAN "see" each other?**
  - **Network Neighborhood**
  - **How are local PC names resolved**
- **Demo - Review Windows XP TCP/IP Settings Dialog**
  - **Basic settings**
  - **Advanced settings**
  - **Bindings**
- **Can use the LMHosts File to map names to IP addresses**
  - **Show LMHosts**

Home LANs do not have a private DNS server. Usually they also lack a WINS server. So other means are needed to allow the various devices on the LAN to know each other by name. This allows accesses to shared resources via the UNC syntax: \\<device name>\<share name>.

If all local LAN IP address are static (don't change across boot-ups) you could use an IP address directly in accesses: \\<IP address>\<share name>. This avoids the naming issue, but forces remembering each PC's internal IP address.

One easy solution is to run the IPX / SPX protocol, which automatically broadcasts machine names, on all network PCs. However, this doesn't work well for some shared devices like stand-alone print servers. It also adds more network traffic because IPX / SPX is running in parallel with TCP/IP.

Some routers support NetBIOS over TCP/IP automatically. If not, you can set the flag to explicitly enable NetBIOS over TCP/IP in the LAN Properties > TCP/IP > Advanced dialog. This enables broadcasting of machine names over TCP/IP.

You can also explicitly specify machine names and IP addresses in the "LMHosts" or "hosts" text files. This can also be handy for frequently visited external sites. These files are located at folder: C:\Windows\System32\drivers\etc .

Tuning Up Your Router / Firewall

- **Read the router vendor's instructions – TWICE!**
- **Typically connect using web browser.**
  - **Linksys: 192.168.1.1**
  - **Belkin: 192.168.2.1**
- **Demo of exploring SCSCC's Belkin WAP / router**
  - **Set admin password (record it somewhere safe).**
  - **Cloning the MAC address from your PC.**
  - **May want to set some port redirection (DMZ).**
  - **For wireless, security settings.**
  - **For wireless, allowed Mac addresses.**

TNB Sept 22, 2004 **Advanced Networking**

There's not much to comment on here. Just follow the steps.

Depending on your ISP, you may want to "clone" the MAC address from the primary PC on the local LAN onto the router. The router will send that MAC address in the Ethernet header of all outbound packets.

For wireless, if you want to be secure, it's critical to change the default SSID and the Administrator password. You should also turn off broadcasting. I recommend also turning on WEP encryption so your packets can't be monitored by an external user with a wireless network adapter.

It's important to power cycle both the Cable/DSL modem and the WAP/Router so they will discover each other correctly. Power on the modem first, then the WAP/Router.

Normally, home routers block incoming requests (as opposed to responses) to just about all TCP ports. Port forwarding is a way to permit inbound traffic directed to a specific port, such as port 80 (HTTP) or port 23 (FTP), to be routed to a specific PC, such as a web server or FTP server, on the network. The idea is that this special PC can better limit access to other PCs and files on the internal LAN.

Cautionary note – Cox's High Speed Internet service agreement may not permit running a personal web or FTP site. I looked all over the site and couldn't find an on-line copy of the service agreement.

LAN and WAN Trouble Shooting

- See MS Troubleshooting Guide
- LAN Connection Properties Dialog
- IPCONFIG /ALL
- Ping Tool
- Whois Tool
- TraceRt tool
- Monitor LAN Traffic With Ethereal

TNB Sept 22, 2004 **Advanced Networking**

This part of the presentation is all demonstrations of the various tools and documents listed above.

Ethereal was demonstrated earlier in the presentation.

The Piing and TreaceRt tools run under the command prompt.

The “Whois tool” is at a web site: www.whois.rc .

Your Own Web Server

- **Server Software:**
  - MS IIS included with Windows XP and Windows 2000.
  - Apache (freeware): http://httpd.apache.org/ .
  - Both can support server-side scripting (.ASP, .JSP, PHP).
  - Complete control over content.
  - No ads.
  - No disk space limits.
  - Or use it to test your web content before publishing to a host.
- **Demo: Installing and Setting up the IIS Web Server.**
- **How to enable traffic from external Internet.**
  - Need to configure your firewall to route port 80 traffic.

TNB Sept 22, 2004 **Advanced Networking**

This material will only be covered if there is interest.

Internet Information Server (IIS) is an optional service installed via the Control Panel. You may need to provide your Windows XP setup CD to the installer.

Even if you don't choose to allow outside connections to your web server, you may wish to set up an internal site as a way to test more complex web site structures and pages that feature "dynamic content" before publishing them to a commercial hosting service.

To allow inbound traffic to your web server from the external Internet, see the earlier discussion on IP port forwarding within the hardware router.

By default, the various web sites are kept in folder: C:\InetPub\wwwroot. However, these settings can be changed via the IIS Administrator.

Other Software Configuration

- **Internet Explorer Configuration.**
  - Privacy, Security, Cache size, History, Programs
- **E-mail configuration.**
  - Accounts, security, other options
- **Security for Shared Folders and Files.**
  - Adding authorized users, permissions
- **Activating an Advanced Software Firewall.**
  - Firewall blocks undesired external connections.
  - Win XP Internet Connection Firewall – Basic.
  - Zone Alarm (Free or Pro) – Better than ICF.
  - Norton Internet Firewall (not free) – Better than ICF.

This material will only be covered if there is interest.

The demo steps through these activities briefly. Internet Explorer and E-mail configuration have been documented in depth in other seminars and SIGS.

Security varies depending on which version of Windows is being run. For Windows XP, each file and folder has an established list of Users or Groups allowed to access the folder or file. For each such User or Group, the allowed mode of access (Read, Change, Full Control) is then specified. For a home LAN, the easiest thing is to add the "Everyone" Group and specify "Change" or "Full Control" as the access level. This is less secure, but vastly more convenient.

Free Zone Alarm (www.zonealarm.com) is recommend as a much more capable replacement for the Windows Internet Connection Firewall. Once Zone Alarm is downloaded and installed, you should go back to the Control Panel's LAN Connection settings applet and disable ICF. There's no advantage to running two software firewalls.

Alternatively you can buy Norton's high quality Internet Firewall, install it and then disable ICF.

Open Workshop / Q and A

Your Networking
Problems and Questions