PART II

Review: *From November Meeting*

Why Network — to maximize investment by sharing peripherals to all your computers

Who invented Networking — Xerox PARC, 1976 created the Alto computer with a GUI and integrated laser printers to create a LAN

Peer-to-Peer

Client/Server

Wired

Wireless

Assumption: You have a broadband connection and want to share that connection between four to six computers at your house. You elect to use a P-2-P network. Our network will include both wired and wireless network segments (you will probably only need a single segment) so this project of wired and wireless works for all of us.

BUILDING YOUR NETWORK

What hardware is required?

1. **Computers**
2. **Network Interface Cards (NICs) Be aware of rated speed**
3. **Routers (wired or wireless)**
4. **Networking componen ts – Switches and Hubs – again, be aware of speed**

5. Wiring for connectivity

What software is required

6. TCP/IP Protocol for networking – protocol of the Internet

7. IP addresses for each network device

8. DNS address information (supplied by your ISP)

9. DHCP to manage and assign IP addresses (supplied by the router)

CONSIDER A WIRED NETWORK FIRST

The most common network topology in use today is the Star. It also uses the most cost-effective cabling and hardware components currently available so that's the model we'll use for a wired network.

Twisted Pair Cables

10BaseT/100BaseT – Cat 3 and Cat 5 twisted pair cable used for 10 Megabit/second and 100 Megabit/second Networks respectively. RJ-45 connectors on each end. 10BaseT Cat 3 cables and 100BaseT Cat 5 cables are good up to 100 meters (about 108 yards).

Router – a Network Layer (OSI Layer 3) device uses hardware and software to "route" data between destinations. Can be customized by protocol stacks TCP/IP; IPX/SPX; AppleTalk. Routers segment large LANs congested with data traffic. **The Router translates information from one network to another.** Routers select the best path to route a message, based on the destination address and the origin. They know the addresses of all computers and other network devices on the network. They can listen to the activity and redirect data around congested areas until it clears up. Home network

routers contain about four regular ports for connecting either devices or additional ports on switches. Switches may be daisy-chained together to extend a star network.

Switches and Hubs – Switches are replacing hubs because of the high density of connection ports. They operate at the Data Link Layer (OSI Layer 2) and control the flow of data by inspecting the MAC address of each data packet and routing the packet accordingly. **Switches divide networks into Virtual LANs or VLANs**. They memorize addresses of computers and send the information to the correct location directly which reduces traffic and improves performance.

There is a “special” port on a switch or hub that is the “Uplink” port. It is used to connect a switch/hub to another switch/hub. How these ports are used varies by vendor. Some have a switch to select Uplink or not. Other vendors underline the Uplink port and the regular port next to it to indicate that only one of these openings may be used. The Uplink port reverses some wiring internally to enable this port to function properly as an Uplink and not another port. *See Appendix pages 2 and 3*.

Hubs simply broadcast the data to all devices simualtaneously thereby adding to network traffic congestion. *If you have a choice, always use a switch instead of a hub .*

Network Interface Card – NICs provides the physical connection between the network and the computer. Most NICs are internal, with the card fitting into an expansion slot inside the computer. But today, USB adapters are also available. Laptop computers can now be purchased with a network interface card built-in or with network cards that slip into a PCMCIA slot.

NICs provide the PC with a connection to the network as well

as a data conversion function. Data travels in parallel on the PC's bus and the network requires a serial data stream. **The transceiver on the NIC moves the data to and from the PC and converts the data from serial to parallel and vice versa.**

It also supplies the MAC address (Media Access Control) – also known as the hardware address. This ID is burned into a ROM on the NIC and is used to resolve the logical to physical address of the PC.

Bridges – Generally used less today. Were used to chop the network into smaller segments. Bridges are smarter than Hubs and repeaters. Inspects the MAC address to improve segment-to-segment performance.

Repeaters – All network cable types have a maximum length. When the length needs to be extended, a repeater is used. It has no capabilities for directing network traffic or determining a particular route. They simply boost the data signals they receive and pass them along – including noise and signals too weak to use.

NOW CONSIDER A WIRELESS NETWORK

Wireless Standards

802.11a – 5 GHz; Up to 54 Mbps for up to 75 feet. Not compatible with "b" or "g"

802.11b – 2.4 GHz; Up to 11 Mbps for up to 100 to 150 feet in range

802.11g – 2.4 GHz; Up to 54 Mbps. Can be mixed with "b" but limited to 11 Mbps

Wireless Router – similar to the router described previously except it includes the ability to include wireless routing.

Range Extender – Acts like a repeater in a wired network. It receives, amplifies and transmits data packets effectively extending the range of the wireless network. Sometimes special antennas are also utilized.

Wireless NICs – Several models are available for PCs and laptops (PCI and PCMCIA cards)

Wireless Ethernet Bridge – connects a wireless segment to a wired segment

WAP – (Wireless Access Point) connects to a wired network and provides a wireless connection for wireless clients.

Biggest names in wireless components for the home market are: ***Linksys; D-Link; Belkin; and Netgear***. Other brands are also available. Which brand is right for you? You must decide. But purchase all your wireless components from the same vendor, i.e. the same brand

Network Protocols

Ethernet – Most widely used today. Uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) Listen then transmit. Detect packet collisions then waits a random amount of time before attempting to transmit again

LocalTalk – Developed by Apple Computer for Macs. Uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) similar to Ethernet except each computer signals its intent transmit before it actually transmits. ***Speed is only 230 Kbps***.

Token Ring – a single electronic “token” is passed around the ring. If a computer wants to transmit, it must wait for the token to arrive empty. It attaches its data and passes the token along. The receiving computer examines the token packet

and removes the data if the address matches. Data speed is 4 Mbps or 16 Mbps. Low cost of Ethernet equipment and cabling has left Token Ring in the dust.

FDDI – Fiber Distributed Data Interface is a protocol used primarliy to interconnect two or more LANs, often over large distances. Uses token-passing and a dual ring physical topology. Major advantage is speed. Over 100 Mbps over fiber optic cable.

ATM – Asychronous Transfer Mode transmits at 155 Mbps and higher. Transmits all data in small packets of fixed size. Also used primarily to interconnect two or more LANs.

Novell's IPX/SPX — originally derived from the Xerox Network Services (XNS) architecture, A chatty protocol with lots of overhead, Novell licensing proved extremely expensive vs. Microsoft's implementation of TCP/IP which was included in Windows NT.

NetBIOS and NetBEUI — originally developed by IBM for small networks. Microsoft adapted as part of LAN Manager. Do not use. Neither NetBIOS nor NetBEUI are routable.

TCP/IP — is actually two protocols used in concert with one another. IP (Internet Protocol) defines how network data is addressed from a source to a destination. TCP (Transmission Control Protocol) operates at the transport layer and manages connections between computers. ***TCP/IP is the network of the Internet and is the only network protocol you should use at home for Windows and Linux computers.***

Network Addresses

Each device on your network **must** have an address. Network addresses are used much like your home address It provides

a means through which you can be located.

TCP/IP Addressing

TCP/IP requires that addresses be structured in a specific way that is a standard and is used throughout the entire Internet.

IP addresses are 32 bits long broken into four octets as: *xxx.xxx.xxx.xxx* where each *xxx* represents a number between 000 and 255. The numbers 0, 127, and 255 are reserved for special purposes and as such are unavailable for assignment to nodes. ***TCP/IP is the only protocol you should use to build a network*** and each network device is required to have an IP Address.

Addresses on the Internet are guaranteed to be unique through the use of an address registration service, currently administered by the Internet Corporation for Assigned Names and Numbers (ICANN) ICANN works closely through registrars like INTERNIC, Network Solutions, and many others to manage domain registrations and public IP addresses.

There are three major classes of addresses, Class A, B, and C. which are determined by the “size” of the network — that is, the number of devices or “nodes” involved.

Class A: ICANN assignes the first octet and the owner can use all possible combinations in the remaining three octets up to 16.5 Million addresses. Class A example: 57.xxx.xxx.xxx

Class B: ICANN defines the first two octets, leaving the remaining two open for the address’s owner to use. Ex. 123.55. xxx.xxx for 65 thousand combinations.

Class C: Follows the same pattern with the address owner having 255 unique nodes to use.

Since we will never have many nodes on our home networks,

we all fall into the Class C category. However, few if any of us will ever need to register a domain name that will be used publically on the Internet so we won't have a specific IP address for our nework.

We can each register a unique domain name with a registrar to protect our domain name for use as a company web site, but few of us will actually host that domain name on the Internet. If we want to use the domain name publically, then we find a hosting company to host that domain name for us using some of their IP addresses from their Class B or C license.

PRIVATE ADDRESSISNG

There are specific ranges of addresses that are reserved for private use. Meaning they are not allowed out into the public domain.

For your private network in your home it is recommended that you use the following IP address: 192.168.1.xxx which provides you with over 250 addresses to use. 192.168.1.1 thru 192.168.1.255

This is a typical but unique Class C address.

So now we have discussed IP addresses and will use the Class C private address beginning with 192.168.1.1. What else do we need? How about an address for the DNS server?

Domain Name System — using only IP addresses to address computers over the Internet would become ugly. Which is easier to enter into your browser – http://204.71.202.160 or http://www.yahoo.com?

DNS is the protocol used to translate IP addresses into names for us humans.

The DNS runs on servers on the Internet. You submit a request

to visit *Google*. So your request leaves your computer and heads off to the DNS server located at your ISP. That DNS may not know the final IP address of *Google* but it knows of another DNS server that may know the answer so your request is sumbitted to that server. This sequence repeats until the IP address of *Google* is finally determined and your request is routed to the *Google* IP address. This is how DNS operates.

The DNS address you will need will be provided by your ISP. You will enter it into a special screen on your router so your computers may find this local DNS server.

How many “nodes” are on your home network? How many IP addresses do you need? You should “plan” for your network to be flexible. What if you have guests, can your network automatically assign them an IP address so they can use your Internet?

DHCP - Dynamic Host Configuration protocol

This protocol usually runs on a network server or a router and supplies client computers and devices with an appropriate IP address automatically. Most IP addresses are “leased” to a client for a specific period like 24 hours. That IP address is “reserved” for that particular device if it logs back onto the network during the time of the lease. After the lease expires, the client will make another broadcase or request to the DHCP server and another IP address will be assigned.

Using this approach, each and every client computer or device that connects to the network requests and receives an IP address within the specified address range (Class C, private in our case).

Most routers for home networks have this DHCP capability built-in so you won’t struggle setting it up. The details are

included in your user manual.

Network Address Translation – NAT since your private IP address is not allowed outside your private network, how does the Internet know your query came from you? That is a good question. Your router uses a built-in capability called Network Address Translation to convert your private network address into a public address through your ISP. Your router has two connections. The first is the one that is connected to your ISP and is known as a WAN (wide area network) connection. That connection has an IP address that is assigned by your ISP. So everything leaving your network for the Internet has that IP address since it is going "public" to the Internet. The second connection is to your private network. That is where the 192.168.1.1 private address is being used.

So all your private IP addresses stay inside on your private network and as they leave for the public sector, your router translates your private address into a public address for the Internet.

By the way, NAT is a *very* good thing and helps keep your private network "hidden" from the public world. Only the very best and patient hackers are able to detect you behind your NAT - enabled router. Remember the MAC address in the NIC card is used to help resolve addresses inside inbound network packets or datagrams to find their way back to the appropriate or correct computer.

Okay, now we've discussed almost everything you will need to set up you home network.

A Review:

Hardware — for Wired Network

Network Interface Cards (NICs) 10 Mps or 100 Mps or 10/100. One NIC per computer. Most networked printers either have a NIC built-in or require a special (expensive) NIC.

Cables — Cat 3 for 10 Mps; Cat 5 for 100 Mps, 1 cable (patch cord) for each device to be connected.

Switches — as required to connect all the components in a star topology. Switches come in various sizes, 5 ports, 8 ports, 16 ports, and 32 ports. Remember a star topology may be expanded by using the Uplink port to connect to another switch.

And finally, the Router.

Now Hardware for wireless networks

Network Interface Cards (NICS) Remember to purchase all your wireless components from the same vendor (Linksys, D-Link, NetGear, Belkin, etc.) to avoid proprietary issues between vendors. Decide what speed you need and purchase:

• 802.11a – operates at 5GHz; and provides up to 54 Mbps for a range of up to 75 feet.

• 802.11b – operates at 2.4 GHz and provides up to 11Mbps for a range up to 100 ti 150 feet.

• 802.11g – operates at 2.4 GHz and provides up to 54 Mbps. May be mixed with 802.11b devices but is then limited to 802.11b speed of 11 Mbps.

Router Settings

While wireless routers all do basically the same thing, the proprietary features and settings can be very different, so you should plan to follow the guidelines and directions for installing

your router using the directions included with your router.

Usually the preferred method to setup your router is to use the Setup CD-ROM that came with your router. In addition, there is usually a Web-based utility that will allow you to install the router or to modify settings once the router is setup and installed. Again, please check your documention to determine the best way for you to proceed.

The following generic steps are usually okay to use with any wireless router, ***but you should always use the directions from your vendor for your particular wireless router***.

1. Make sure you have the setup information for your specific type of Internet connection. The installation technician from your ISP should have left this information with you after installing your broadband connection. If not, call your ISP and request the settings.
2. Make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.
3. Connect one end of an Ethernet network cable to one of the ports (labeled 1-4) on the back of the Router, and the other end to an Ethernet port on a PC. These ports are for the wired computers that will be part of your LAN. *(See Appendix page 4)*
4. Repeat this step to connect additional PCs or other network devices to the router (e.g. switches).
5. Connect a different Ethernet network cable from your cable or DSL modem to the ***Internet*** port on the back of the Router. (*See Appendix page 4)*
6. Next plug the AC Power Adapter into the Power port and the other end into an electrical outlet.

7. Now Power on the components in the following order waiting at least 30 seconds between components: DSL or Cable modem, the Router, and one PC.
8. Make sure the Power and Internet LEDs on the front panel light up green.
9. The Power LED usually flashes green for a few seconds as the Router goes through its self-test. It will then stay solid green when the test completes.
10. As always, you should follow the directions that came with your Router to setup each PC for proper operation. These instructions will vary according to the version of the installed operating system.

Basically, you need to make sure that TCP/IP is installed under networking. Then check the “properties” for TCP/IP to verify that “Obtain an IP address automatically,” is selected. That insures the DHCP feature of the Router will assign IP addresses to each of your networked devices. Click OK to complete the PC configuration, then restart your computer(s). *(See Appendix page 3)*

Now you finish the Router configuration through your web browser. Launch your web browser and type in the IP address of your Router typically something like: “http:/192.168.1.1” (check the documentation for your Router).

A password request screen appears and you log into the Router as described in your documentation. Then the web-based utility will appear. Again follow the directions that came with your Router to complete the configuration of the Router which includes any unique options you desire.

Be sure you select the option that enables the DHCP to

provide and assign IP addresses to all your network devices. There can only be one DHCP server on a network so discuss this with your system administrator if this as an attachment to a active network that is already operating correctly.

At this point you should check for Internet connectivity using a wired computer. Then return to your wireless router and complete the router setup for the wireless components. At this time I recommend leaving the security disabled. Remember you still have to install the wireless network adapters for your wireless computers. It is easier to get them all working without the security being activated.

Once you have your wireless devices working correctly, then go back and setup your security.

Be sure you follow the directions and instructions of your wireless router and Ethernet card providers (hopefully they are the same vendor).

SECURING YOUR WIRELESS NETWORK

Close your network

When you setup your wireless network, your first choice is whether your network is open or closed. Some vendors call this a “closed network,” others “disable broadcast name.” No matter what you call it, if your network does not broadcase its name, that makes it harder to find. So just say “no.” Name your network what you wish but just don’t tell or broadcast the name. That way, your network does not appear in the list of available networks. This is only step #1.

Other tools

WEP Encryption (Wired Equivalent Privacy) through encryption was a good plan but WEP is not user friendly so most users

simply elect not to use it. However if that's the only option you have then use it. But select the 128-bit version and carefully document the key or the passphrase you enter. You will need to re-enter this key or passphrase on every computer that will connect to the wireless network. Up to four keys may be used with WEP encryption.

Another security tool is *MAC Address Filtering*. Using this tool, you enter the MAC address of each wireless network card that you will allow to connect to your network. Other MAC addresses are excluded or not allowed to connect to your network.

WPA – *Wi-Fi Protected Access* is a new standard and fixes many of the broken parts of WEP while adding support for newer security initiatives.

Given a choice, always use WPA for active encryption since the encrpytion keys automatically change on a regular basis which makes it much more difficult for someont to "*crack*" the encryption and gain access to your network.

Remember, locks were invented to keep honest folks honest. Wireless security has the same goal — it keeps honest folks honest.

When presented with the option, always turn-on the option for a firewall on your router. Almost all current routers today have them so use it!

SHARING FILES, FOLDERS AND DEVICES

After sharing their Internet connection, the second most popular reason for setting up a network is to use that old computer as a storage facility — that is, as a file server. Most folks are also interested in sharing their printers so they have

the ability to print to any printer they own from any computer on their network. This opens the topic of “Shares” in the MS Windows environment. Based on our initial assumption, this is a peer-2-peer network so no domain controller or network server is available so setting up “‘shares” is easier.

Let’s assume for simplicity that, per our assumption, you have several desktop PCs and/or laptop PCs networked together. Remember from the first session that the first line of defense is the local computer. That is, using a logon id and a password to protect the local PC. When you build a peer-2-peer network, no server is involved or accessable to protect the network so how do you go about creating a network “identity” for your peer clients so you may share files, folders, drives and printers?

In the Windows environment, the answer is to define a workgroup and enable Windows File and Printer Sharing.

To create a workgroup for your nework, you need to access the same screen used to assign each a unique name to your computer. You may reach this screen by => Control Panel => System => Computer Name. On the Computer Name screen you have the option to change the computer name and on that screen you may add the name of a computer workgroup (*See Appendix pg 6*). If your computer has a *Windows Key,* a shortcut is avilable. Press the *Windows Key* + *Pause/Break* and the System Properties menu will open.

As with passwords, please choose a name for your workgroup that is meaningful but also secure. Use a combinations of upper and lower case letters as well as numbers to name your workgroup. You will probably windup with a combination of personal and perhaps financial information that you don’t want to become public so be creative with the workgroup name.

You must repeat these steps for every computer in your network so that they all belong to the same workgroup.

Once you have all the computers configured as part of your workgroup, you're almost finished. Now you need to be sure that File and Printer Sharing is turned on.

File and Printer Sharing is a service that is accessed in the computer's networking configuration (*See Appendix page 4).* Again, *Control Panel => Network Connections* for Win XP, Win 2000 and Win Me environments.

If File and printer sharing for Microsoft Windows is visable, be sure the box is checked. If File and printer sharing is not visable, then you need to "Add" that service by clicking on the *Add* button.

Now that the computers belong to a workgroup and File and printer sharing is added, all you need to do is to "share" a folder, printer or an entire drive.

NOTE the dialog at this point will vary depending on the version of Windows.

Starting on the computer that hosts the folder you want to share, use Windows Explorer to navigate to the folder you want to share. Right-click the folder and select Sharing or Properties. The Sharing dialog box will open. To share the folder, click the Share this folder tab and look at the sharing dialog. You may give the "Share" a new name or use the current name. You may also be able to specify a password and access level for the folder such as Read-Only or Full Access (read, write, add and delete).

Note Windows NT, Windows 2000 and Windows XP are more secure than previous versions. In fact using these later

versions of Windows requires that the person wishing to access the shared resource must have an account on the hosting computer. So if Joe wants to access a shared folder on a WinNT, Win2000 or WinXP computer, Joe must have a user account and a password for that host computer.

So you may have to add Joe (and other workgroup members to these computers) — add a user account and password for each workgroup member.

Sharing printers is very similar. Open the printers dialog box (*Start* => *Settings* => *printers*). Select the printer you want to share, Right-click then select share or sharing. The printer's property sheet will open. Click the *Shared As* option and then specify a name for the shared printer. (*See Appendix pg 7*)

Now from the *Network Neighborhood* or *My Network Places* (depending on the Windows version) shared printers will appear along with the shared folders and may quickly be connected to.

Well, if everything has gone well, you now have a wired, or a wireless network up and running. You may even be an adventurous type and tried your hand at a combination that includes both. At any rate, I wish you good luck networking!

The Appendix and Troubleshooting are next which also includes several references for more information and help in solving problems with your network.