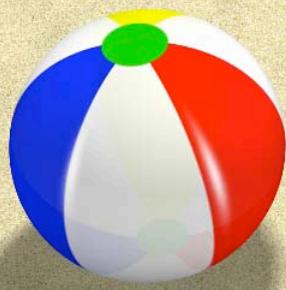


Building a Home Network

Kent Reuber

reuber@stanford.edu

736-7650



Stanford Networking Systems supports Stanford DSL, Stanford West/Welch Rd. cable modems, and Ethernet services, thus acting as the ISP. We at Networking don't directly support home networks (e.g., we won't come to your house), but we do want to share our recommendations and guidelines which will hopefully make your home network usage safer, easier to maintain, and more robust.

Outline

- ✳ Vocabulary and other basics.
- ✳ Network devices (routers, switches, access points, ...)
- ✳ Example network layouts.
- ✳ Example home network components.



This class will give you the basics of setting up a home network. It's very difficult to be too specific--there are a lot of different devices from numerous vendors, so it's almost impossible to give you too many details. What we *can* do is to tell you how we'd recommend that you set things up. Then you can consult the documentation with your particular hardware for specific instructions.

Network vocabulary

- IP (or TCP/IP): The communication protocol of the Internet.
- IP address: A 32 bit number used for network identity. It is usually expressed a series of four decimal numbers (e.g., 171.64.20.120). Used to communicate between networks.
- MAC (or hardware) address: a 48 bit number, usually expressed as 12 hexadecimal (0-9,a-f) numbers. Used to communicate within a network.
- Subnet mask: A 32 bit number describing the size of the local network. Usually expressed as four “octet” decimal numbers. Only certain digits are available in each octet: 0, 128, 192, 224, 240, 248, 252, 254, 255.
- Default gateway: The IP address of the router that provides the exit point of the local net.



In the past, there were a wide variety of networking protocols: AppleTalk, NetBEUI, Novell NetWare, etc. Most of these have been replaced by TCP/IP, since TCP/IP is required for Internet access, and that's what everyone wants to do. There's nothing to prevent you from running these older network protocols on your local network, but they won't be routed outside of your local net. And, if desired, you can run multiple network protocols. For example, if you have an older AppleTalk printer, there's no reason you can't continue to run both AppleTalk locally for printer access and use TCP/IP for Internet access. But, in most cases, people are reverting to pure-TCP/IP networks.

Devices on the local net communicate using MAC addresses not IP addresses. MAC addresses are burned into every device and there should never be any duplicates. The first 6 hexadecimal digits (known as the Organizationally Unique Identifiers or OUI) will tell you the maker of the device. There are OUI lookup tables on the Internet. The one I use is:
http://coffer.com/mac_find/

Subnet masks describe the size of your local network. The larger the mask, the smaller the network. (For example, a mask of 255.255.255.128 is a smaller network than 255.255.255.0). Since a device knows its own address and the default gateway, it can calculate whether the any given address it wants to communicate with is local or not. You may occasionally encounter CIDR notation such as “/24”, which describes the size of a local network. These are equivalent to the decimal form of subnet masks; they're just a different notation (for example, /16 is equivalent to 255.255.0.0, /22 to 255.255.252.0,

IP addressing rules



"All I did was to ask for her IP address." (IT Guy comic)

- All IP addresses within the local network must be unique.
- All Subnet masks (network size) and all gateways (exit points) of devices on one side of a router should be the same.
- Most broadband routers provide DHCP servers (automatic IP addressing), so you don't have to manage addresses manually.



All IP addresses on your local network must be unique. Note: 192.168.*.* , 172.16-31.*.* and 10.*.*.* address ranges are not routed anywhere on the Internet, and can be used by anyone, including you. However, many of these addresses are routed within Stanford. Stanford reserves the 192.168.1.* range, so if you use IP addresses in this range, you're guaranteed not to have a conflict with another Stanford address.

All subnet masks and gateways within your local net must be the same. (Note: they can be different on opposite sides of a router.)

Most broadband routers will provide DHCP (dynamic IP addressing) over a limited range (e.g., 192.168.1.100-250), leaving other addresses (2-100) for use by devices with static addresses. For the most part, only those devices running services (e.g., print servers, file servers) need fixed addresses. Almost all other clients, especially laptops, should probably use DHCP.

Recommendations

★ Buying things:

- Ask questions (e.g., Expert Partners list) before you buy. Have a goal...
- Check online to see if manuals are available.
- Buy stuff that you can return, if possible.

★ Use dedicated hardware (e.g., print servers, broadband routers) rather than software

- Dedicated hardware is more robust and simpler to operate (usually via Web browser).
- No need to worry about the computer hosting the service to be up.



It's always best to figure out what you want to do first, then ask others (e.g., Expert Partners or your department computer support person) before you buy. Getting the straight story from salespeople doesn't always happen. It's better to ask and know that you'll have problems ahead of time rather than having to return products that don't work. Still, it's best to buy products that you can return if things don't work out. Products can be defective, so a good return policy is worth it.

These days, you can get software for routing and print serving functions. My suggestion is not to use software if possible. If you have to depend on a certain computer to be turned on and be working correctly, it makes your network more complex. For example, if the computer in the study has to be on to print, I may have to get up from the living room to turn the computer on, wait for it to boot, etc. Also, this may be tough to explain to your spouse and children. Also, what if your computer that's sharing your printer crashes or gets hacked, etc. Dedicated print servers and routers have very robust operating systems and user friendly interfaces (usually accessed via Web browsers).

Networking shopping list

★ Necessary or highly recommended:

- Internet Service Provider (ISP).
- Broadband (NAT) router.
- Print server or network printer.
- Cables.

★ Optional:

- Wireless access point.
- Wireless repeater.
- Small hubs/switches.
- Web cams, ...



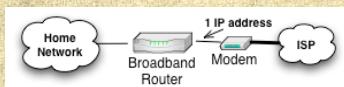
Obviously, you need an ISP who will provide you with a connection to the Internet. This could be AT&T DSL, Stanford DSL, Comcast cable modem, etc.

Even in cases where your ISP can provide you with more than one IP address (such as provided by Stanford DSL), I recommend you use a broadband (NAT) router. The Network Address Translation used in these routers hides your network from the Internet while still allowing you reach the world. Your home network is likely to have important financial data and you simply don't want this to be exposed to the outside world.

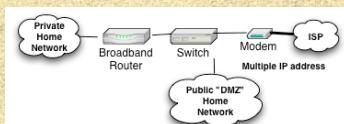
You'll also want some way of sharing a printer. Many printers now come with network connections built in, but many personal printers (e.g., inkjets) don't. For those that don't, you'll need a print server.

There are also any number of additional pieces of hardware that may be useful which we'll describe later.

Home network layouts



- If your ISP provides you with only 1 address, you need a broadband router to create a home network.



- Even if your ISP provides multiple IP addresses (e.g., Stanford DSL), it's still a good idea to use a broadband router to provide firewalling and allow you to grow your network as large as you need.

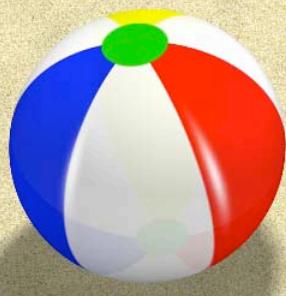


Here are the two scenarios for setting up a home network. Remember that each device in use must have its own unique IP address.

If your ISP provides you with only a single IP address (typical of most non-Stanford DSL and cable modem providers), you'll need a broadband router. The IP address they assign you gets assigned to the "WAN" jack on the broadband router. The router creates a network on the "LAN" jacks and, if present, the wireless which you can use for your devices.

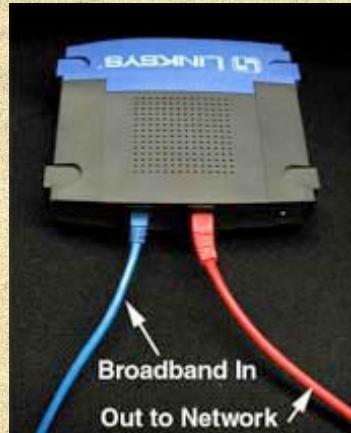
If you have an ISP that provides you with multiple IP addresses (such as Stanford DSL, which provides 5 IP addresses), you technically don't need a broadband router if you have enough addresses for every device. However, because broadband routers provide firewalling from the Internet (that is, outside uses can't reach your private devices directly), it's still a good idea. And, in these days of laptops, iPhones, TiVo, etc., it's easy to exceed 5 addresses. You can put some devices that you want to be reachable via the Internet outside of the broadband router. This area of corporate networks is often referred to as a "DMZ". Note that most DSL and cable modem service is highly asymmetric in bandwidth: while you may get multiple megabit speed "downstream" to your network, you may only get a fraction of a megabit for "upstream" communication. So, don't expect high-speed access for any servers that you run on your home network.

Network Devices: Broadband routers



A broadband router running Network Address Translation (NAT) is the most important device on your network, providing the access between your local network and the Internet. In many cases, it will also provide you with wireless services.

Broadband (NAT) router



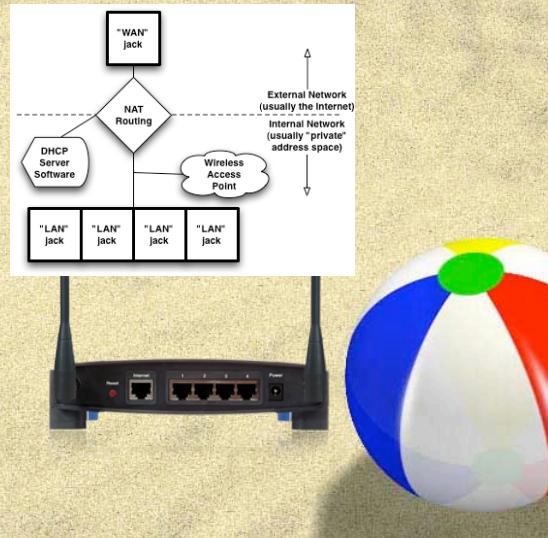
- Hides network from the outside world using NAT.
- Connections:
 - "WAN" Ethernet jack connects to ISP equipment.
 - Ethernet "LAN" jack(s) connect to the local network.
 - Usually also has wireless.



Whoever or whatever your ISP is, they will eventually terminate in one or (rarely) more RJ45 Ethernet jacks (sometimes referred to as “interfaces”). Broadband NAT routers have a “WAN” (Wide-Area Network) jack which connects to the ISP’s jack via an ordinary Ethernet cable. A broadband router will also have a small number (usually 1-4) of Ethernet jacks to connect to equipment on your local network. This may not be enough jacks for all your equipment and you may need to use a hub or switch for additional ports. Most broadband routers these days also have wireless antennas which give you a router and wireless solution in one device.

Inside a Broadband Router

- ★ Broadband routers include several software and hardware components.
- ★ In many cases, you can disable components that you don't need.



Routing software takes care of receiving and forwarding packets between your local network and the Internet.

DHCP servers provide IP addresses to machines on your local network. Many can also supply addresses to the network connected to the WAN jack; you almost never want to do this, because it can disrupt connectivity on the upstream network.

Broadband routers have a built in access point allowing you send your local network into the air for wireless devices.

What is NAT?

- NAT = “Net Address Translation”
- Several different methods. For the gory details, see RFC 1613.
- Most frequently encountered method is the one used in home broadband routers which proxy an entire non-routable network range behind a single routable “public” IP address.
- NAT router acts as a proxy: it forwards traffic from your local net and relays the reply back to the originating device.



The most common form of NAT used to be called “IP masquerading”, because an entire network was hidden behind a single IP address. In the past, many ISP’s didn’t allow this sort of thing, so you had to hide it. These days, most ISP’s *expect* you to use broadband routers.

If you want to find out more things NAT can be used for (or if you have trouble sleeping at night), you may be interested in RFC 1613. Another reference: Bill Dutcher, “The NAT Handbook” (Wiley)

Why would you want to use NAT?

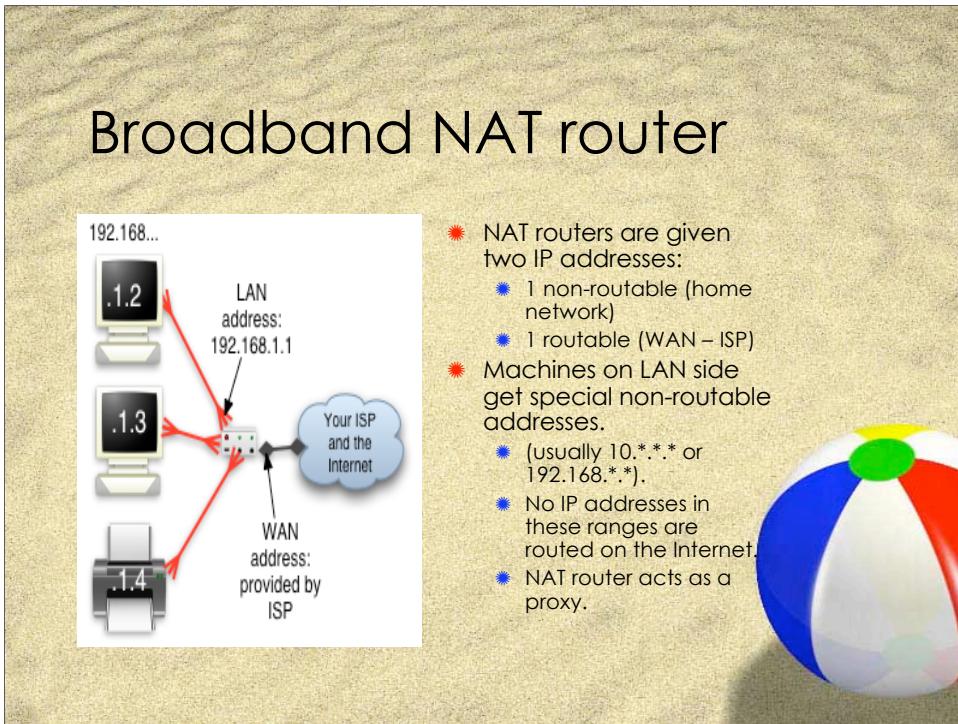
- Allows you to buy a single IP address from your ISP and share that address among a large number of devices. (May save \$\$)
- All devices on the local network can access the Internet at the same time, though the bandwidth is shared.
- NAT provides a firewall function:
 - Outside hosts can *reply* to hosts behind the NAT router, but can't initiate connections.
 - Inside hosts have to initiate the connection.
 - Note: there are some ways around this.



The reason most people use NAT routers is that their home network size is larger than the number of public addresses provided by their ISP's. Most ISP's give you just one address, which means you must use NAT to create a network. Of course, they'll happily sell you a business account with multiple IP addresses for more money...

The other reason is that NAT routers create a simple firewall without having to do much configuration on the user's part. In most cases, you don't want to expose any machines on your home network (especially those that may contain sensitive data) to the Internet. Hackers are always scanning for machines to use for their own purposes, and you don't want them to select yours. The only machine that you want exposed to the Internet is a machine that's running some services, such as a home Web or file server. Ideally, any of these public machines should be separated from your private machines with some kind of firewall such as a broadband router.

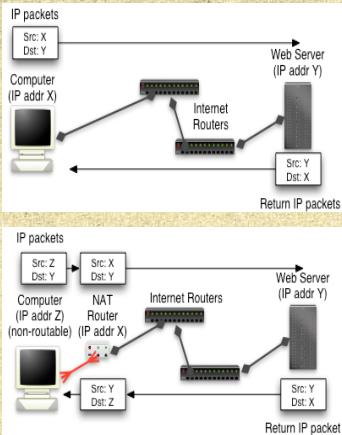
Broadband NAT router



Here's an example of a home network. The NAT router (the white box) has an address provided by the ISP on the WAN interface, and creates an non-routable network 192.168.1.*. The LAN interface of the router has an address of 192.168.1.1, which is the default gateway for your local net. The subnet mask for broadband routers is almost always a "class C" network, or 255.255.255.0.

In this example, there are three devices: two computers and a printer. Note that each one has a *different* IP address, but all will have the same subnet mask (255.255.255.0) and gateway (192.168.1.1).

How NAT works



- Normal routers maintain source and destination IP addresses from end-to-end.

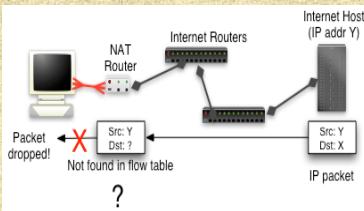
- NAT routers change IP addresses and port.
 - Outgoing packets appear to come from the NAT router's public address.
 - NAT routers keep track of each "flow" so that replies can be returned.



A NAT router acts as a middle-men. It receives packets from devices on unrouteable network and forwards them on using its routable public IP address. When replies are received, a NAT router forwards the packets to the original host. A router maintains “flow tables” of currently open connections so that it knows which machine on the local network should receive each reply.

Although it's not shown in this diagram, most NAT routers will also change the source TCP or UDP port numbers.

How NAT firewalling works



- ★ Suppose a host (either friendly or malicious) sends a packet to the NAT router without the connection being initiated from the inside.
 - Outside hosts can't send directly to the hosts on the local network side -- they have non-routable addresses!
 - Since there is no entry in the flow table, the NAT router has no idea where to forward it and drops the packet. Instant firewall!



Without an entry in the flow tables, a router has no way of forwarding packets to the local network. Thus, the local net is isolated from the Internet, which is usually a good thing. There is a way to override this using a technique called port forwarding.

Circumventing the NAT firewall (if you must)

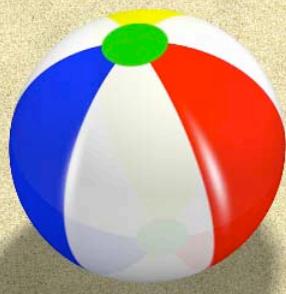
- You may want to run a server behind your NAT router. How do you let the traffic you want?
- NAT routers have a limited ability to “port forward”, sending all traffic to a given computer on the internal net and bypassing the flow table.
- For example:
 - Send all Web traffic (port 80) to 192.168.1.3
 - Send all mail traffic (port 25) to 192.168.1.5
- You can get hacked if forwarded port is running a vulnerable service! For example, if your IIS Web server isn't patched, your firewall won't help you. Always keep services with patched, especially those that are open to the Internet.



Port forwarding allows you to create a permanently open path through the NAT router. You can tell the router that any inbound connection destined for a given TCP or UDP port is forwarded to a specific host (e.g., a Web server, an FTP server, etc.). However, just because you have a firewall doesn't mean these systems are secured. If there are vulnerabilities in any Internet facing servers, you must keep them patched or you risk the servers being compromised. Expose hosts to the Internet with caution.

Look at the logs on your hosts that are open to the Internet. In many cases, you'll find people from all over the world trying to guess passwords, and using other nasty tricks. Do you know where your logs are?

Network Devices: Wireless



These days, more and more devices are using wireless. Once a home network expands beyond a single room, wireless becomes very attractive, because you don't have to run cabling. Still, wireless is more prone to interference, so any time-sensitive applications (e.g., video streaming) may be better over wired connections.

Wireless frequency choices

- Usually you'll want at least wireless 802.11b/g (2.4 GHz). 802.11n (2.4 GHz and 5.5 GHz) is OK if your computers support it.
- Internet access speed is limited by the ISP.
 - Most DSL is only 1 Mbps. Even 802.11b (~3 Mbps real world) won't be a bottleneck. P.S., don't believe the "theoretical" wireless bandwidths.
 - Faster 802.11g and 802.11n usually only matters for transfers within your network.
- Note: wireless access points/routers act like hubs, so only one wireless device can send/receive at any instant.



The most popular wireless standards are 802.11b and 802.11g which use the 2.4 GHz frequency range. (There is also an 802.11a standard that uses the 5.5 GHz range, but it is rarely used.) 802.11n uses the 2.4 GHz range, and sometimes but not always the 5.5 GHz range as well.

Even 802.11b is much faster than typical DSL speeds, so wireless speed isn't usually a bottleneck when accessing the Internet. Don't let salesmen sell you more than you really need. Of course, having faster wireless will speed up access within your network if all your systems are compatible.

Wireless speeds

- 802.11b: rated at 11 Mbps
 - Real world typical: 3 Mbps
 - Best: ~ 5 Mbps
- 802.11g: rated at 54 Mbps
 - Real world typical: 12 Mbps
 - Best: ~ 22 Mbps.
- 802.11n: rated at 300 Mbps
 - Real world typical: ~45 Mbps
 - Best: ~ 80 Mbps
- Note: wireless speeds dependencies:
 - Distance between client and access point.
 - Types of materials in house walls.



Most of the bandwidths given in sales brochures are very exaggerated. Usually, they cheat, counting both download and upload speeds together. (In 802.11n which has both 2.4 GHz and 5.5 GHz frequencies, often the bandwidths for both frequencies will be added together.) This chart shows typical speeds that I've actually encountered with wireless devices.

Most wireless access points can send reliable signals around 40 feet, though this may vary by the construction of any intervening walls. The only way to find out what you need is to try it.

Routers vs. Access Points

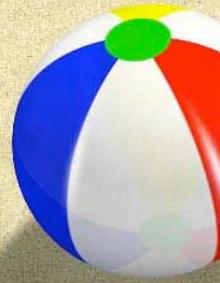
- Routers create a network, and include multiple jacks for connecting your net to your ISP.
- Access points are network endpoints, so they usually have only one jack. They extend your wired network “into the air”.



Many people confuse access points and routers. In general, you will use only one router on your home network. You might need multiple access points if you need to provide wireless to a wide area.

Wireless network name

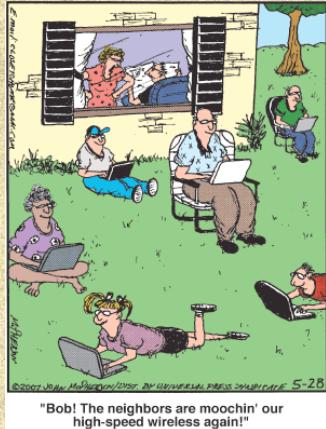
- A computer will be able to roam freely between access points with the same network name (also called SSID).
 - In most cases, all of your access points should broadcast the same SSID, but they should use different channels to minimize interference. The usual 802.11b/g channels are 1, 6, and 11.
 - Any of your access points should have a different SSID than those of your neighbors.
- If you put up your own wireless on access point on campus, it should not use the SSID "Stanford" or any other reserved name. Use a name that indicates that it belongs to you.



This slide only applies if you have multiple access points in your house. Laptops will freely roam between access points with the same SSID's. In most cases, all of your access points should broadcast the same SSID.

To prevent this roaming, the SSID's on your network should be different than those of your neighbors.

Wireless protection



- ★ Use MAC address filters, WEP or WPA to prevent neighbors from using your wireless.
- ★ May want to use hidden SSID (network name).
- ★ Use encrypted protocols (https, SSH, Kerberos, SSL) especially in public wireless areas.



Wireless signals are repeated everywhere in range. Anyone in the area can see all your traffic unless you take precautions.

WEP and WPA are protocols that encrypt signals between access points and clients and also prevent others from using your wireless unless they know the proper passwords. While WEP is somewhat simpler to implement, it can be cracked if someone is capable of capturing enough data. WPA is the newest encryption method.

Another thing you can do is to not broadcast your network name. To join these hidden networks, you have to know the name of your network, which may limit who attempts to join it.

I personally don't use either WEP or WPA. I simply use MAC address filters which limit what specific devices can associate to my access points. Instead of relying on the encryption protocols in the access points, I use encrypted transport protocols such as Kerberos, SSL, SSH, etc. In most cases, public access wireless (e.g., airports, Starbucks, etc.) will be completely open and unencrypted, so it's better to set up your computer with software that doesn't rely on access points for encryption.

Network Devices: Printing and cabling



Print server

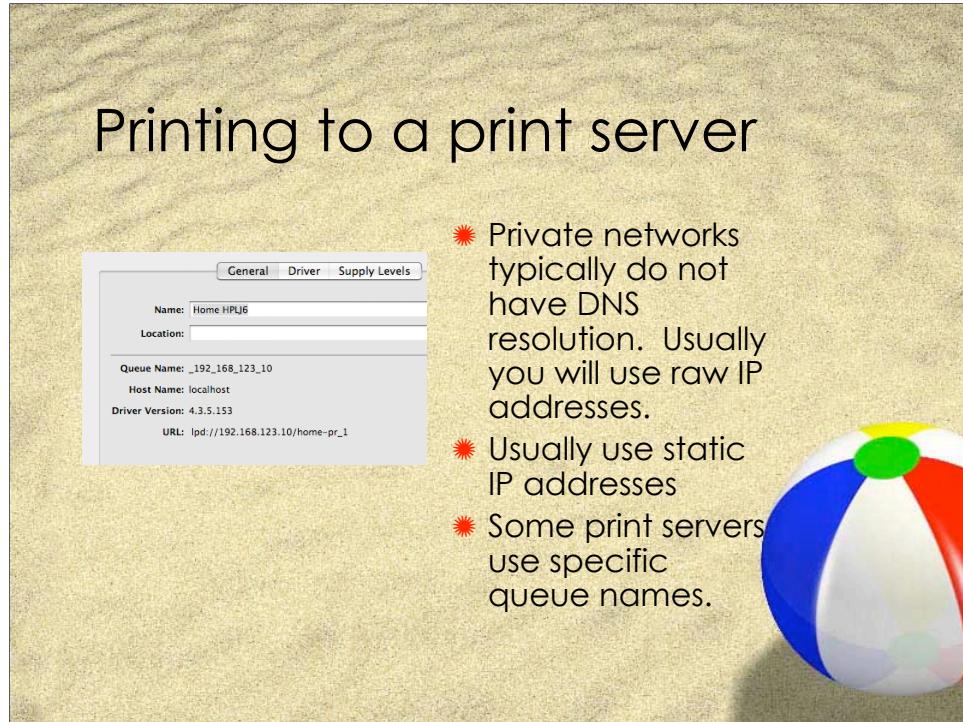


- Used to network a printer that doesn't have a network jack.
- Usually has one Ethernet and one or more parallel or USB jacks.
- Many print servers include wireless.



These print servers will usually use the LPR or IPP printing protocols. If the printers and computers all support it, there's no reason that you have to use TCP/IP. If all your devices support Novell or AppleTalk, for example, there's no problem using it on your home network for printing. But support for non-TCP/IP protocols is fading.

Printing to a print server



For devices on your local network to be able to print, they usually need 3 pieces of information: the printer name or IP address, the print queue name, and the printing protocol. The screen capture shows the setup of my black and white HP printer which uses a Netgear print server.

Most home private networks won't have DNS, so you will probably need to set up printing to a raw IP address. I usually recommend using static addresses for printers even though many devices use Bonjour to browse the network.

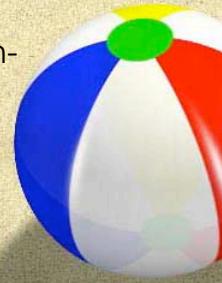
Some print servers need for you to specify a print queue. Check your documentation.

Typical printing protocols are LPR/LPD (Unix printing) or IPP. Again, check your documentation.

Cables

✿ Ethernet cables

- ✿ Category 5 or 5e is sufficient. No need for Category 6.
- ✿ Only 4-wire cables are necessary for 10/100 Mbps speed. Gigabit needs 8 wires.
- ✿ May need crossover cables for switch-switch connections though most switches have a selector switch.
- ✿ May also need USB or parallel cables.



Typically you will buy 8 conductor category 5e cables for your network.

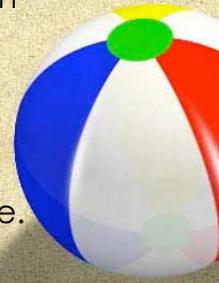
Crossover cables have reversed receive and transmit wires.

Other devices



Hubs and switches

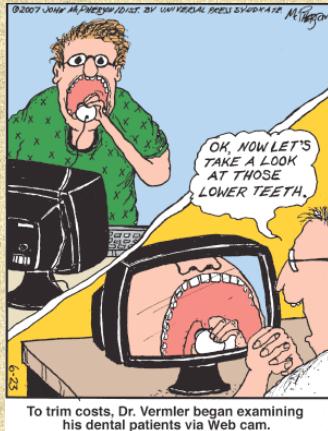
- ✿ Probably doesn't matter which you use, though hubs are becoming harder to find. It's unlikely that your net is so congested that a switch would add performance over a hub.
- ✿ Switch speed is almost always faster than your ISP, so switch speed will not be a bottleneck to accessing the Internet, though it will speed up your internal traffic.
- ✿ Always remember not to create loops in cabling -- you must wire in a "star" shape.



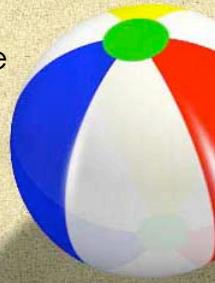
While switches are more efficient at moving traffic than hubs, it's unlikely to affect the performance of your local network. The speed of your local network is usually faster than your connection to the Internet by a factor of 10 or more, so it's the Internet connection speed that's the bottleneck, not the speed of your local net. The same goes for 802.11b vs. 802.11g wireless. The speed of the wireless is much faster than the speed of your Internet connection, so the wireless speed won't affect the speed at which access external Internet sites. A faster hub/switch will speed up file sharing on your local network though.

When creating a wired network, never create a loop. Loops can be created using wireless as well. If your computer has both a wired and a wireless card, you can use them at the same time. However, if you then turn on "bridging" on your computer between the wired and wireless network, you can create a loop which will bring your network down.

Web cams



- ★ Many of the new Internet cameras have built-in Web servers so that you don't need a computer.
- ★ Some people use cams for security or just to watch their kittens...



Many devices call “web cams” are simply video cameras designed to plug into computer USB ports. If you want a stand-alone device, you may want to look for a “web cam server” with an integrated Web server software and an Ethernet jack and/or a wireless antennas.

Voice over IP (VoIP)

- ★ Many companies are starting to sell equipment that can place calls over Internet connections.
- Lower cost, but may have voice quality or latency issues.
- Important: VoIP won't work during power outage.



Lots of companies are jumping on the VoIP bandwagon. By sending voice signals through your “always on” Internet connection, you can sometimes save a lot of money on toll calls, especially overseas. Skype, for example, allows you to call Skype-to-Skype for free anywhere in the world, which is great if you want to save money on international calls. I’ve found though that voice quality on consumer level VoIP phones is often not the best. There can be quite a bit of latency and jitter. Still, if you’re trying to do something on the cheap, VoIP may work for you.

Also, be sure to determine if your VoIP equipment supports E-911. For conventional “land line” calls to 911, your address will be automatically routed to emergency service providers. For some VoIP carriers, they may not be able to relay this information because they have no way of relating your IP address to your house address.

Stanford-run networks



Stanford DSL

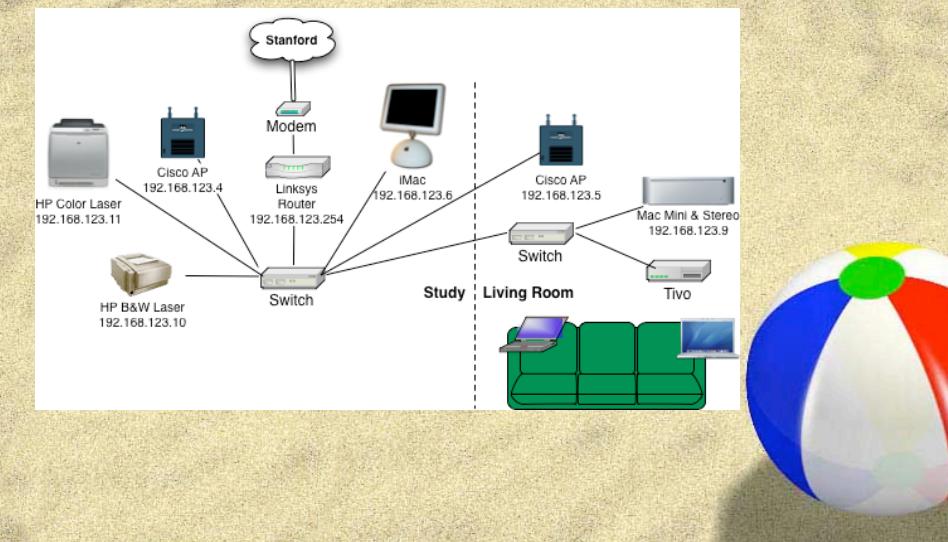
- Customers receive 5 Stanford IP addresses.
 - Can access IP-limited resources (e.g., journals).
 - Don't need a broadband router, but it's still a good idea.
- Netopia router (provided):
 - Provides DHCP. No need to register these devices in Netdb.
 - Has 4 10/100 ports for devices.
 - Only routes IP.
- DNS is provided by campus servers.
 - You can connect to your computer by specifying its hostname (xxx.stanford.edu).



Stanford DSL is different from most “residential” DSL/cable modem services. First, most “residential” DSL/cable services give you only 1 address for your computer, which forces you to use a broadband NAT router if you want to have multiple systems connected to the Internet simultaneously. Stanford DSL actually has an entire network preconfigured. Just plug your devices into the DSL modem that we provide, enter (unique!) address information into each system, and you have an instant network.

Also, Stanford DSL will give all your computers Stanford addresses. So, looking up electronic journals that are restricted to computers on the Stanford campus isn’t a problem.

Kent's Stanford DSL Network



Here's my home network. My DSL service from Stanford enters the house in the study. Even though Stanford provides 5 public IP's, I only use a single public address. My NAT router creates a private net 192.168.123.X. The router has my static address from Stanford on one interface and the address 192.168.123.254 on the other. This second interface is the "default gateway" for all of the systems on my local network. My DSL router creates a subnet mask with 255.255.255.0. The router also holds the address of Stanford's DNS servers, which will be passed to local machines via the built-in DHCP server. I have two category 5 Ethernet cables running between my living room and study. I find I need a separate wireless for the living room. The wireless penetrates the house well enough that I can get reliable signals on either the front or back patios.

I found that my Internet radio and video streams would sometimes cut out when I was surfing the Web. Because I'm picky about my music/video quality, I moved to wired connections for Tivo and Internet radio.

Stanford West/Welch Rd.

- Service is transitioning to 10 Mbps cable modem to isolate disruptive user traffic.
- With cable modem, up to 5 addresses per account can be allocated.
- DHCP & DNS is provided by campus servers. Computers are registered in Netdb (check DHCP and roaming flags).
- Because some residents are not Stanford affiliated, the IP address are not considered part of Stanford for purposes of library journals and Departmental Firewalls.
 - Users needing access to campus firewalled hosts should log into the public VPN.
 - Users wishing library journal access will need to use the Library proxy service.
- More info: <http://www.stanford.edu/services/stanfordwest/>



In the past, Stanford West and Welch Road users have configured devices that interfered with those of their neighbors, or worse, brought the entire network down. To isolate users from one another, we're installing cable modems. The download speed is comparable to the previous Ethernet service, but upstream speed is not.

Because there are a number of non-Stanford affiliated residents, the Stanford West and Welch Rd. will now be considered as external to Stanford.

-Stanford-affiliated users needing access to library journals should use the library proxy service, see: <http://www-sul.stanford.edu/apcproxy/>

-Stanford-affiliated users needing access to firewalled system may need to access the Stanford public VPN: <http://vpn.stanford.edu/>

Books

- ★ “*Linksys Networks, the Official Guide*”, Kathy Ivens, Larry Seltzer, Osborne
- ★ “*Home Networking Bible*”, Sue Plumley, Wiley
- ★ Check amazon.com and other online bookstores. More literature is being published all the time.

