

# Networking Basics

## Table of Contents

Networking Basics.....	1
Overview/Who Should Read This Manual .....	2
Budgeting/Planning .....	2
Terminology and Concepts You Need to Know .....	3
Your #1 Source for Windows Networking Assistance .....	6
Network Designs .....	7
Peer-to-peer network physical layout.....	7
Dedicated server-client network physical layout .....	8
Things that Hamper or Prevent Reliable Networking.....	9
Appendix 1 – Real-life Network Example.....	12
Equipment Notes: .....	13
Communication basics.....	14
Barriers to Computer Communication.....	16
Appendix 2 – Making Computer Administration Easier .....	18
Changing the Start Menu.....	18
Changing the Way Windows Displays Folders and Files .....	18
Comment.....	19
Appendix 3 – It Looks Different <i>but the Concept is the Same</i> .....	20
Appendix 4 – Computers as Network Servers .....	21
Creating a Shared Resource.....	21
Windows Server Permission Settings.....	22
Sharing and Windows Vista/Windows 7.....	22
Appendix 5 - Connecting a Workstation to the Network .....	23
Appendix 6 – Making Network Connection Icons Permanent .....	24
Appendix 7 – Bringing It All Together.....	25
Be Consistent .....	27
SQLPos Point of Sale and Employee TimeClock Software .....	28
Installing Club Data Software Updates .....	28
Appendix 8 – Obtaining Technical Support .....	29
Appendix 9 – Tricks of the Trade.....	30
AutoDisconnect.....	30
Windows Power Saving Features .....	31
HOSTS File.....	32
How it works .....	32
Dedicated IP Addressing .....	33
Where Dedicated IP addressing is done.....	34

## Overview/Who Should Read This Manual

This manual can help the reader understand some of the basic elements to implementing a Windows-based network. The manual is not intended to be the definitive treatise on this subject as scores of books have already been written on the subject. However, this is intended to be a more friendly approach to the concept as it relates to a typical club environment. The examples used in the manual are related to common setups encountered in the club industry and therefore, the reader may be able to relate to them without dipping too deeply into the “geek” mentality, although few computer topics are more “geeky” than networking!

As it concerns the implementation of multiple computers in an office, there are primarily three general courses of action one may take. The first one of the three is the fastest; the other two both require significant personal involvement:

1. **Hire the expertise.** This is the simplest, probably the fastest and likely most expensive solution. An important caveat is that this method could leave your business crippled if you encounter a problem and can't get to the right person who initially set up the system. If this is the direction you want to take, instead of reading this manual, set it aside and go check your bank balance.
2. **Do it yourself.** This is the most time-consuming, usually requires a good amount of reading and a willingness to dig into the Windows operating system at a technical level.
3. **Hire expertise and learn it yourself.** This is the most successful way to implement a system that doesn't have to be horribly expensive but still requires an investment of personal time. It's a blend of hiring trained personnel to install and get things working in the least amount of time, spending the time to learn how the system works yourself so you can fix it if need be, and also retaining hired expertise for those situations that you can't solve yourself.

## Budgeting/Planning

There are other considerations you should take before you actually get started, such as:

- **“Do I want it fast or do I want it right?”** Fast implementations often breed oversights and mistakes with repairs and cost overruns later on.
- **“Do I want cheap or do I want quality?”** Quality doesn't necessarily mean expensive but it does mean you'll have to open your wallet. Often a member or friend may say “I know a guy...” or “I've got a grandson who's pretty good at this sort of thing...” Stay away from those situations unless you enjoy frustration and are willing to put up with spending a lot of money and time for not a lot of value. When somebody offers to give you “an old computer I don't use anymore,” he/she is not doing you any favors -- there's a reason why the computer was mothballed. After all, nothing is ever really “free.” However, buying used equipment can be an excellent solution to help curtail cost, but only if you buy brand-name, fairly current equipment from a reputable vendor who will give you some sort of warranty.
- **“Do I want to walk the tightrope without a net or do I want some security?”** Computers have become the backbone of today's business operations. A solid, reliable system can help you be more efficient and save money but a poorly-implemented system will make you inefficient and could cost you a lot of money – or even your job. Just installing it and getting it working is only part of the equation. You also need to plan for ongoing maintenance as your system ages. Remember, a computer is just another *machine*, and machines periodically need maintenance and/or *replacement*.

## Terminology and Concepts You Need to Know

To be able to navigate the world of networking, one needs to know some terms:

- **Network interface cards (NIC).** These are electronic parts that are required to connect a device to the physical network. Most computers today have these designed right into the product, but in some cases such as some printers, they're additional components that you need to purchase, install and configure before the device can be plugged into the network.
- **Network cabling.** This is electrical wiring that physically connects the device to the network, not unlike the cable that connects a toaster to the wall socket. Network cabling comes in several configurations, but generally Category 5 (called cat-5) is the industry standard. You might see cat-5e (enhanced) or even cat-6, and these denote higher quality and insulated wire that helps the electrons flow through the wire faster and with less interference from outside influences such as televisions, fluorescent lights, microwave ovens, refrigerators and air conditioning systems. It's best to have network cabling professionally installed.
- **Network Switch/Hub.** This is a device that allows multiple network devices to be plugged into the same network. It's a lot like a multi-outlet power strip that you might plug into a wall outlet so you can plug more things in. A "switch" is generally electrically more efficient and works faster than a network "hub" but both provide similar functionality.
- **Network Router.** This device helps keep multiple devices on the network unique and distinct from one another, much like your house number is unique on your street. Each computing device on the network must have its own "address" and the router can assign such addresses to the devices on the network when set to be a "DHCP" server. DHCP represents "dynamic host communication protocol" and it's an industry standard method for assigning addresses to network devices. For networks that are also connected to the Internet, it provides a "route" for the electrons to flow between the computers on your internal network and the computers on the external network, e.g. the Internet. There should be *only one* DHCP router on your internal network.
- **Wireless (Wi-Fi) networking** is increasingly popular and is found in coffee shops, hotels and motels, restaurants and even entire communities. Wireless networking is used in place of wired cat-5 networking and it carries with it additional issues that are beyond the scope of this manual. Generally speaking, wireless is not as fast, is less secure and reliable, and is harder to support and maintain than wired networking is. It *can* work very well, but if your goal is to create a rock-solid network for your mission-critical operations, Wi-Fi is probably not in the plan. For your customers and to provide them with convenient access to the Internet, it's fine. But for your day-to-day business operations, it's not the best solution unless the preferred cat-5 wired solution is simply not possible.
- **TCP/IP.** This is akin to the "language" that computers around the world use to talk to one another. It requires that every device have its own unique "address" much like the address for your home is unique in the entire world. The IP address (short for TCP/IP address) is listed as a series of numbers and may range between 1.0.0.2 and 255.255.255.254. Certain ranges of numbers are reserved for specific purposes by the organization that operates the Internet, and IP addresses are typically defined as "external" addresses (those on the Internet) or "internal" addresses which are for local use, inside your office. A typical "internal" address on a network might be: 192.168.1.101 or 10.0.0.22 while an "external" address might be 67.135.106.53. Your router allows internal addresses on a local network to communicate with external addresses on the Internet. There's also a thing called a "subnet mask" that also affects

this addressing concept. Think of a subnet mask as being like an apartment building inside a large apartment complex that has the same street address. A subnet mask is also numerical and follows the same structure as the IP address. Two commonly used subnet masks are 255.255.0.0 and 255.255.255.0.

- **CRITICALLY IMPORTANT CONCEPT:** For network devices on the same local “internal” network to communicate with one another, the IP addresses and subnet masks must be compatible with one another. For example, a computer with an IP address of 192.168.1.1 will not talk to a computer with an IP address of 10.0.0.5. However, a computer with an IP of 192.168.1.6 will talk to another computer whose IP address is 192.168.1.205 as long as the subnet mask is the same for both. But if the IP addresses used are compatible but the subnet mask is not, then communication can be blocked again. In other words, 192.168.1.6 will communicate with 192.168.1.205 if both subnet masks are 255.255.255.0 but if one of the units has a subnet of 255.252.206.0 instead, they won’t connect because the subnet masks are not compatible.
- **TIMESAVER:** If your router is configured to provide DHCP services (most are right out of the box) and your computers are set to use DHCP services (usually the default), then the router will take care of all the addresses automatically. Problem solved. Note however that you cannot have two DHCP routers on the same network because your computers won’t know which one to use. So be sure you have only one router that’s set to be a DHCP router.
- **If you choose to set the addresses manually, do this:** set the subnet mask on every computer in your network to exactly the same number. 255.255.255.0 is probably the most common subnet mask for a local, “internal” network. If the subnet mask is the same for all units, then the only other changes you’ll likely need to make are to the last 3 digits of the IP address.
- **DNS.** This means “dynamic name service” and works as a sort of IP number to name translator. In other words, it’s not so easy to remember that 192.168.1.108 is the computer register at the grill bar but naming it “GRILL-BAR” makes it a lot easier to remember. Using names is often easier for humans to identify the various machines on the network. Just as no two devices on the same network can have the same IP address, no two can have the same name, either. Sometimes users will install a computer server that provides DNS services inside a “domain.” This is outside the scope of this document and is best left to computer tech people.
- **Routable vs. Non-routable IP addresses.** While the IP numbering system provides for a great many unique addresses, the inventors of the IP system recognized the need to make a group of computers private, so they reserved certain number ranges to provide internal private networking without affecting the Internet as a whole. These are called “non-routable” IP addresses and should be used for your internal network. The most common are:
  - 10.0.0.0 to 10.255.255.255
  - 192.168.0.0 to 192.168.255.255
  - A third, lesser-used range is 172.16.0.0 to 172.31.255.255

Non-routable means that computers that are not physically connected to internal networks using one of these number ranges cannot see or access them. This is a security measure that keeps an internal network safe from the outside.

There is also a special “loopback” range of addresses that is set aside for testing only that won’t work at all for your network: 127.0.0.0 to 127.255.255.255. It’s sort of a “short-circuit” and is sometimes used by a computer to connect to itself, such as for testing a computer that was also an intranet web server. For example, pinging 127.0.0.1 will connect a computer to itself to tell whether the network card is working.

- Gateway.** This is usually your router's IP address. The router actually has the electronics for two NIC cards inside it so that it can have two IP addresses – one for the “outside” network (e.g. the Internet) and the other for the “inside” network (e.g. your office). You assign your computer's “internet gateway” setting to be the router's internal IP address so that when your computer tries to connect to something on the Internet, it sends the command to the gateway (e.g. the router). Because the router knows which computer (by the internal IP address) is making the request, it automatically “routes” the electrical communication between the external Internet and the internal computer making the request.

- PING.** This is a common diagnostic tool that is built into Windows. It can be used to tell whether the computer can connect to a specific destination computer. It can be run at the Windows command prompt. For example, typing: **ping clubdata.com** will cause the computer to attempt to connect to Club Data's web site. It will try four times to send a small 32-byte packet of data and report the time (in milliseconds or 1/1000<sup>th</sup> of a second) it takes to make each connection. Using ping can help diagnose network performance or even basic connectivity. You can ping another computer by either its name (see how handy DNS can be?) or by its IP address such as **ping 67.222.32.240**. The lower the number, the faster the connection. In the above example, the average round-trip communication between the computer and Club Data's web site was 100ms, or 1/10<sup>th</sup> of a second.

```

C:\WINDOWS\system32\cmd.exe
C:\>ping clubdata.com

Pinging clubdata.com [67.222.32.240] with 32 bytes of data:

Reply from 67.222.32.240: bytes=32 time=101ms TTL=50
Reply from 67.222.32.240: bytes=32 time=100ms TTL=50
Reply from 67.222.32.240: bytes=32 time=101ms TTL=50
Reply from 67.222.32.240: bytes=32 time=101ms TTL=50

Ping statistics for 67.222.32.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 100ms, Maximum = 101ms, Average = 100ms

C:\>
  
```

- IPCONFIG.** This is another diagnostic tool built into Windows that is very helpful in diagnosing the computer's networking settings. Type the command at a Windows command prompt.

A particularly helpful ipconfig feature is to type: **ipconfig /all** which shows not only the IP information but information about your network card and if DHCP is in use, what the address of the DHCP server is and more. In this case, the gateway and DHCP server are one in the same. It also shows that the “lease” on this IP address was obtained on February 12, 2009 and unless the computer is powered off, will remain for a complete year. A “lease” is the time period the computer is allowed to use that IP address until a new address may (or may not) be assigned. Restarting the computer will automatically renew the lease in a DHCP-based network.

```

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 10.0.0.47
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.2

C:\>
  
```

```

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : dphxp
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

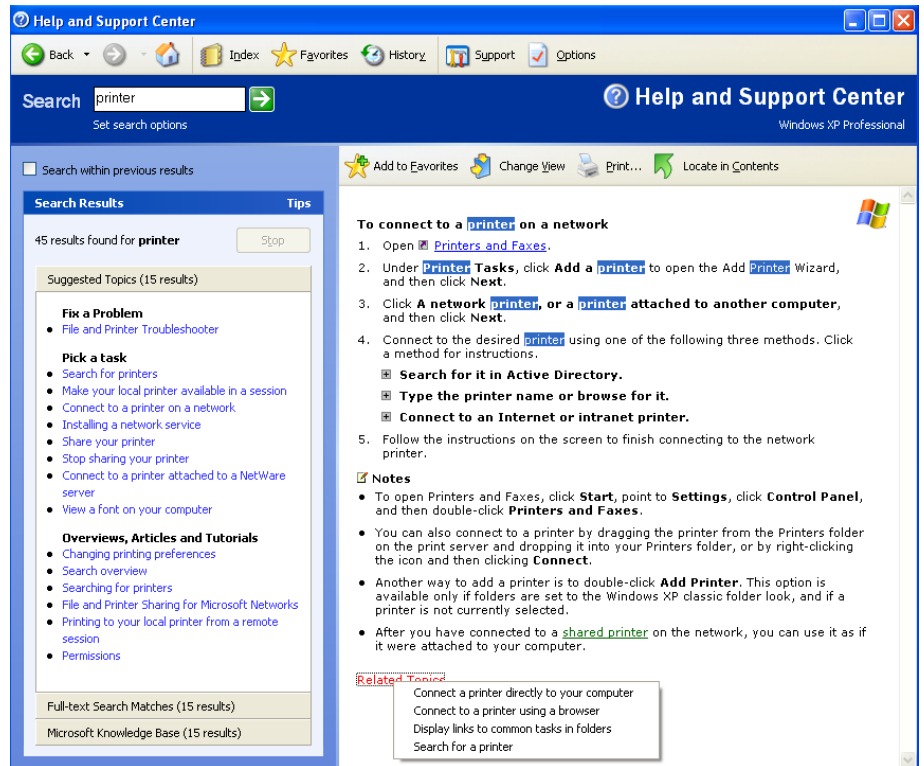
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC
    Physical Address . . . . . : 00-1A-4D-50-A8-E9
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address . . . . . : 10.0.0.47
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.2
    DHCP Server . . . . . : 10.0.0.2
    DNS Servers . . . . . : 10.0.0.2
    Lease Obtained. . . . . : Thursday, February 12, 2009 3:11:06 AM
    Lease Expires . . . . . : Friday, February 12, 2010 3:11:06 AM

C:\>
  
```

## Your #1 Source for Windows Networking Assistance

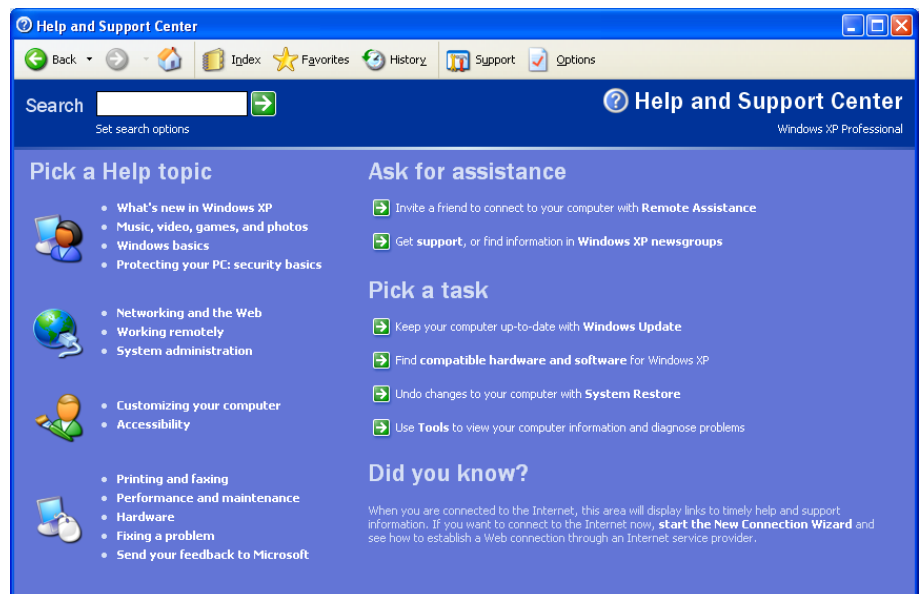
- Click **START – HELP**
- In the Search box, type the key word you want to learn about
- Click the “GO” arrow (or press the ENTER key on your keyboard)
- In the example to the right, the user needed help connecting to a network printer. Typing PRINTER into the search box yielded plenty of choices; “connect to a printer on a network” was one of them. Clicking on that topic displayed step-by-step information.
- Clicking on the Related Topics option at the bottom of the screen provided even more help.



Microsoft has built an incredibly powerful manual into Windows that you can browse through in the help browser. Click the “HOME” icon at the top (the little house) to return to the list of main topic areas and branch out from there.

Hint: because of the way search tools work, typing one or two key words into the search box works much better than typing a whole sentence. For instance, typing **network printer** into the box will yield the information you want but typing **how do I connect to a network printer** will likely not because it will focus on the words “how do I” instead of “network printer.”

Over the years, many customers have asked us, “How did you learn all this stuff?” Well, now you know.



## Network Designs

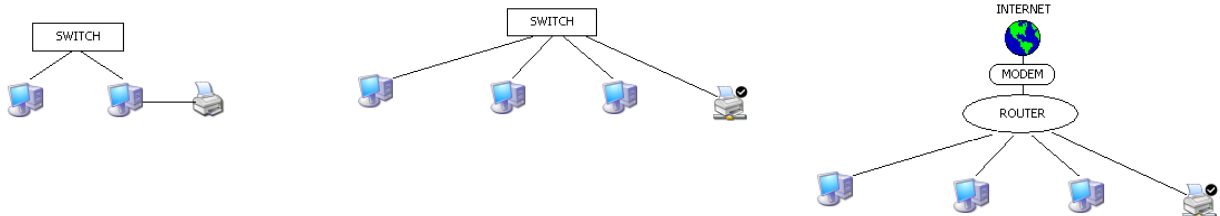
The way you design your network should match the way you operate your business. In general, there are two general “topologies” that are used, either peer-to-peer or client-server. Implementing and maintaining either of them successfully requires basic networking skills.

**Appendix 1 covers a typical network setup at a medium-sized facility. It’s an attempt to explain a real-life example of one club’s solution.**

- **Peer-to-Peer.** The purest example of peer-to-peer is a home network where you might have two or three computers, and maybe one of them has a printer connected to it as a “shared” printer so that everybody in the family can print to it. Peer-to-peer can be useful in small offices.
  - Advantages: lower cost, ease of use.
  - Disadvantages: lower performance and reliability for mission-critical applications such as accounting and POS that run over a network where multiple users are needed. Is usually limited to a small number of computers that can be connected simultaneously.
- **Dedicated server – client.** This is similar to a peer-to-peer network except that one of the computers is used for data or printer sharing only and is never used to do actual work such as word processing, accounting, etc. In fact, in most cases, a dedicated server has a monitor, mouse and keyboard like any other computer, but the monitor is powered off and the unit is safely stored in a protected area. All the work is done at the client workstations while the dedicated server only stores the programs and data that the workstations use. Server operating system software (e.g. Windows Server) is often preferred over workstation operation systems such as Windows XP because they are designed to provide the utmost in high performance for multi-user situations.
  - Advantages: higher performance and reliability for mission-critical applications, especially for POS and accounting systems with multiple users. Can expand as the business needs grow without the limitation to the number of simultaneous computers that peer-to-peer networks have.
  - Disadvantages: more expensive. Server software has many server options and can be implemented very simply or become extremely complicated as more options are selected.

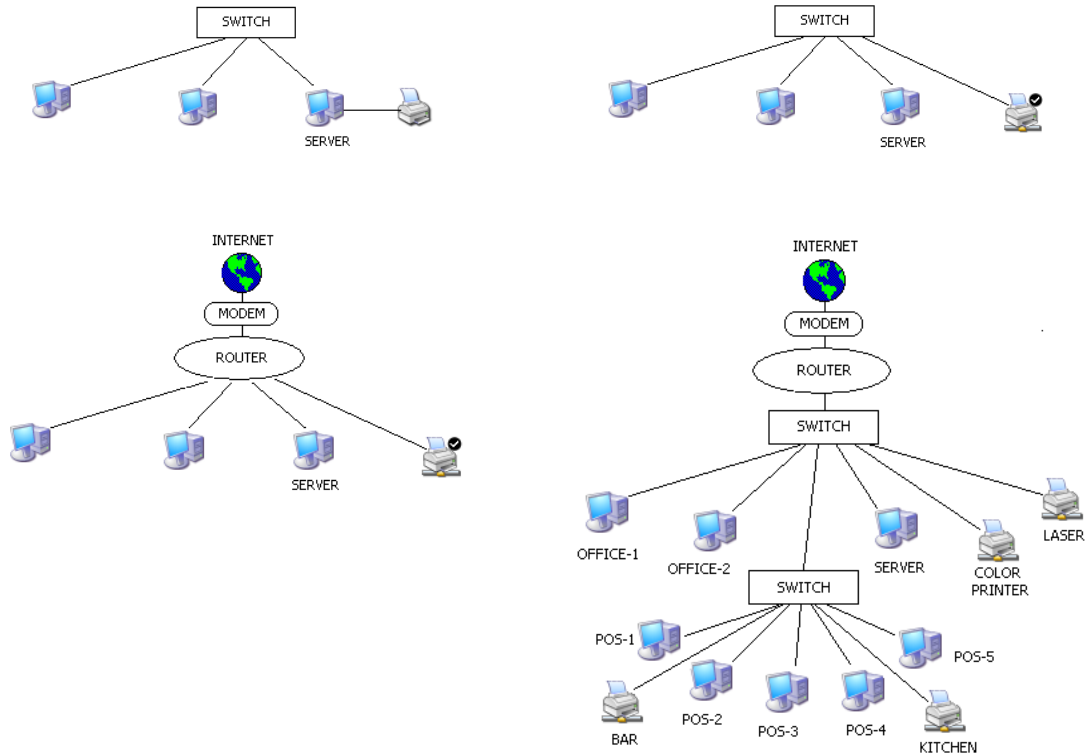
### Peer-to-peer network physical layout

There are many options with peer-to-peer, although the number of network devices that can be connected together is usually limited to five with Windows XP-Home installations and ten with Windows XP-Professional. Peer-to-peer can be set up as simply using an inexpensive network switch to connect two computers and a shared printer, three computers and a network printer or three computers and network printer to a 4-port router that connects to the Internet through a cable or DSL modem:



### Dedicated server-client network physical layout

This affords the most flexibility, performance and reliability even for small networks. DS-C can be configured similarly to peer-to-peer using an inexpensive network switch to connect two computers, a server and either a shared printer or a network printer, or two computers, a server and network printer to a 4-port router that connects to the Internet through a cable or DSL modem, or a large internal network with a couple office workstations, networked laser and color printers, multiple switches, plus a POS system with remote station printers in the kitchen and at the bar. If your vision is that your computing needs will expand, installing a dedicated server-client system will be the most efficient for you overall because you can expand it as your needs grow.





## Things that Hamper or Prevent Reliable Networking

Any one of the following or any combination of the following can cause a network connection to fail either completely or partially. A partial, intermittent connection is the most confusing and most dangerous to your operation because it can contribute to database integrity problems, invalid or missing data, lost work and lost time, causing staff to do the work all over again.

- **Poor network wiring installation.** Poor quality or old cable or cable that's been compromised by stapling, pinching, stretching, placement near high-electrical demand electrical devices such as coffee makers, refrigerators, air conditioners, microwave ovens, fluorescent lights, or any electrical appliance that generates a magnetic field.
- **Exposed wiring.** If your network wire is strung loosely on the floor, around the edge of the room where someone could get at it with a vacuum cleaner or mop, beneath a carpet, or placed in locations that are easy to trip over, you're just asking for trouble. There are eight thin wires inside a network cable, and when one of them breaks, it breaks internally – you can't see it. But suddenly, the computer isn't working and you'll tear your hair out trying to find the problem. It might reconnect after "jiggling the wire" a little but if that fixes the problem, you need to understand that "jiggling the wire" is not the fix you think it is: all you've done is create an intermittent connection. Most computer professionals would rather have *no* connection than an intermittent one because at least with no connection, you know your data is stored locally on your computer. With an intermittent connection, you can't predict what data gets through and what doesn't.
- **Electrical power fluctuations.** If your lights periodically dim, you have frequent electrical storms or man-made static electricity (low humidity/carpet shocks, etc.), your network will almost certainly encounter problems. Those little bits and bytes flowing through your network from computer to computer are electrical impulses and such power problems inject unexpected electrical "noise" into the mix. Having all that extra electrical noise on the network will slow things down at best, probably result in corrupted data and can literally burn out a computer so it won't even power on.

Solution: Purchase a suitable uninterruptured power supply (UPS) for each device on your network. These battery-backup units moderate the electrical power and provide a wonderful measure of protection, including powering the computer for typically 10-20 minutes if the power goes out completely, giving the user a chance to save data and power the computer down safely. However, a UPS can still fail in three scenarios:

1. **Electrical storms.** If your building is struck with a multi-million volt lightning strike, it's hard to expect a shoebox-sized device to guarantee 100% protection. After all, the lightning travelled several thousand feet through open space to get to you; it's not likely to stop inside that little UPS.
2. **Inattention to the age of the UPSs' batteries.** The batteries inside a really good, name brand UPS have only a two or three-year lifetime at best. You should expect to periodically replace either the batteries or the UPS itself. At \$50-\$75 each, on a large network, this should be a recurring budget item. A five-year old UPS might provide some help from small voltage spikes or static electricity, but if the power goes out, it might not power the computer for more than a few seconds – probably not enough to save what you were doing or power the computer down safely. The result is often corrupted data or worse yet, Windows becomes corrupted and the computer won't start up again when the power comes back on.

3. **Inattention to how long the computer's been on UPS battery backup power during a power outage.** Remember, you only get 10-20 minutes' grace period with a typical workstation UPS. That time is intended to get you past saving your work and powering the computer down safely. If you let it run and the battery finally gives out, you've essentially recreated scenario #2 above.
- **Firewalls.** Think about it: a computer firewall is put in place to prevent potentially damaging information from getting to the computer. But unless the user configures the firewall so that it knows the difference between what's "acceptable" and "damaging" it has no way to know and therefore, to be safe, it just blocks everything. This often happens after the firewall software has been installed or updated, which is either a manual or automatic process depending on the computer's settings and the end user's preferences. Here's what you need to know about firewalls:
    1. Not all firewall software works the same way. Some firewall software is more tenacious than others; some is more configurable than others. They all have the same goal (to protect the computer) but they look, act and are usually configured differently.
    2. Installing multiple firewalls on a computer is like putting multiple locks on a door. Multiple firewalls can interact with one another so that if you unlock a feature on one, that feature may become activated on the other one.
    3. Firewall software runs at the system operating system level, which means that it starts up well before you see anything on the screen as the computer starts up. Sometimes, the only way to turn it completely off is to uninstall it.
    4. **It is the solely and completely the end-user's responsibility to know how to activate, deactivate or configure the firewall software on his/her computers and network.** There are too many firewall software manufacturers and related options for Club Data to help you troubleshoot or configure these issues over the telephone.
  - **Antivirus Software.** While the goals of antivirus software are similar in some ways to those of a firewall, it functions quite differently. Instead of just "blocking" a connection altogether, it actually scans the contents of the actual file itself to see if it contains various key elements that the antivirus software company has identified as being related to a known computer virus. If one of these key "signatures" doesn't exist, it lets the file pass through. Most virus signatures are well known to antivirus software manufacturers, but the malicious people who create viruses are constantly looking for ways to disguise an existing signature or even develop a new one the world has never seen. Why these people create the viruses in the first place is curious, but that's another matter entirely. What's primarily important to know is that antivirus software uses up some of your computer's power and effectively makes the computer seem to run slower. Because the antivirus software must process network traffic, it may appear that the network has "slowed down." Other things to know :
    - Computer viruses don't exist to help you compute better. They're almost always designed to be destructive in some fashion, or at the very least, a nuisance. You don't want to get them.
    - If your computer is connected to the Internet, acquiring a computer virus is much more likely than if your computer is on an internal network only. However, even private internal networks can acquire viruses as employees bring CDs or memory sticks from home to view on their computers at work; if those items were infected at home, bringing them to the office can infect the office.

- Antivirus software requires frequent updating for it to be valuable. Because new viruses are being created almost every day, the antivirus software companies try to keep up by identifying the newest ones and updating their software to catch them. You need to keep your antivirus software up-to-date.
- Adding RAM memory to your computer can usually help improve the computer's speed.
- **Like firewall software, it is the solely and completely the end-user's responsibility to know how to activate, deactivate, configure and update the antivirus software on his/her computers and network.** There are too many antivirus software manufacturers for Club Data to help you troubleshoot or configure these issues over the telephone.
- **Multi-tasking.** If you're the kind of person who likes to have a lot of office software running simultaneously (word processing, a spreadsheet, email, perhaps a CD is playing in the background, etc.), your network experience will likely suffer when you use your computer. In short, the more things you ask your computer to do simultaneously, the less time it can devote to each of them – the computer's power has to be divided by all the applications that you have open. Well, sending and receiving data over the network is one of those tasks. If you're the main computer and also the file server for your POS system, think about the effect that has on all your POS system users!

Comment: Let's be honest about multi-tasking -- how many of us *really* can do more than one thing simultaneously? You have only one keyboard, only one mouse, and your eyes can focus on only one object at a time, right? So is it *really* necessary that all those applications be kept running all the time and slowing down your computer?

- **Your network design can make a difference!** If your network uses the peer-to-peer design but your computer is also the "main" computer for, say, your POS system, consider that each of those POS terminals is also using resources on your computer and what you do affects them, too. For example, if you start a major billing or data updating function that requires heavy use of the computer to do a lot of data reading, calculation and then data storing, there may not be much computer power left for the POS terminals to use and to your restaurant servers, the network may look like it's stopped working altogether -- it may seem like it takes *forever* to save or recall a hold sale in the restaurant! There are some kinds of computing actions that are more intense than others and when you're also the "main" computer for other networked users, your peer-to-peer workstation computer may not have enough horsepower to even give them the time of day.

Workstation operating systems like Windows XP, Vista and Windows 7 are designed differently than server operation systems like Windows Server. Workstation software is designed to give the most performance to the single user who's currently at the computer's keyboard. Server software is designed to provide high quantities of data to multiple network users at multiple remote computers simultaneously while putting much less emphasis on a user who might be at the server's keyboard.

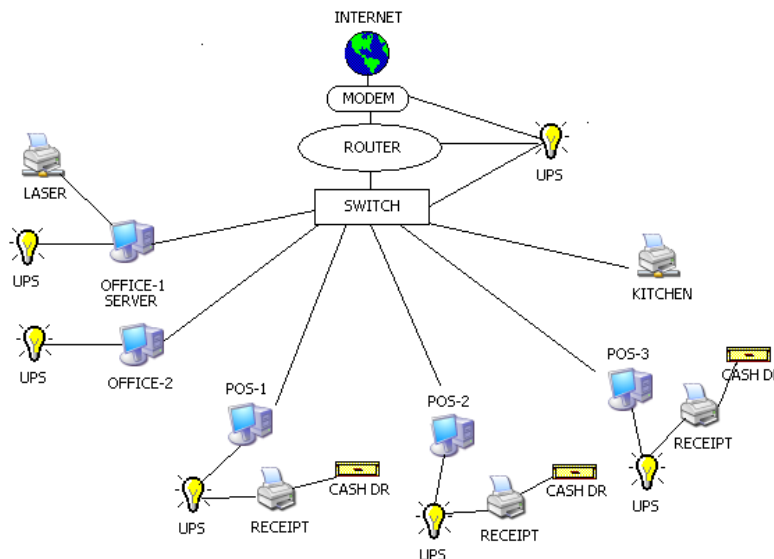
## Appendix 1 – Real-life Network Example

Most club office users have more than one PC that they want to use. This illustration attempts to capture the essential functions of a typical club where all of the equipment resides within a single building, the clubhouse.

The illustration includes one back office file server PC, one PC in the back office for doing accounting, three POS register PCs on the sales floor which are also used to finish/tender tickets, a remote printer in the kitchen for food orders, and all the PCs must be able to access the Internet. The primary uses of the network are for recording sales and financial activity into a single Club Office accounting system. Other typical uses (word processing, producing a newsletter, sending/retrieving email, etc.) are not addressed in this document.

### Equipment Inventory

- POS System
  - 3 Dell PCs (a standard model, Windows XP Home or Professional installed)
  - 3 touch screen monitors
  - 3 cash drawers
  - 3 thermal receipt printers for customer receipts
  - 1 dot-matrix impact printer for kitchen remote
- Office
  - 2 Dell PCs (better equipped than POS system, more memory, etc.)
    - Both with Windows XP Professional installed
    - One of the PCs is used as a simple file & print server
    - One of the PCs is used as a normal user workstation
    - LCD flat panel monitor, keyboard, mouse on each
  - 1 laser printer (as a shared printer on the file server)
- Other
  - 8-port network switch
  - Cable modem
  - Router (set in DHCP mode, usually the default)
  - Category-5 wiring throughout
  - 6 uninterruptable power supplies
    - 5 UPSs – one for each PC
    - 1 UPS – for cable modem, router & switch



## Equipment Notes:

- **Modem:** connects the office to the Internet via the club's ISP (Internet Service Provider). The connection may be via cable, telephone line or satellite. The modem type must match the connection type and is normally provided with the ISP's high speed Internet access subscription. For example, a cable modem is for connecting to a cable-tv provider while a DSL modem is for connecting to a DSL telephone line.
- **Router:** assigns all internal IP addresses to all the computers; serves as the gateway to the Internet through the modem. A typical router has a single, designated port to connect to the modem and often four other ports to connect to the internal network.
- **Switch:** the main connection point for all computers on the network. A switch is sort of a smart multi-outlet strip that affords more connections than the router. Switches come in multiple configurations – 5 ports, 8 ports, 12, 16, 32, etc. depending on how many connections you need.
- **UPS:** provide electrical protection to the computers and emergency short-term power during brownouts or power outs. A typical UPS has multiple outlets; some of which are for battery-backup power and others just for protection and filtering from voltage spikes and lightning but no emergency battery power. Be sure to use the right outlets.
- **Cat-5** cable is the communication wiring that physically connects the computers and other network devices so that they can talk to one another. Plugging the computers into the wall power outlet isn't enough: the computers need the communication connection, too.
- **PCs:** computers can be configured in many ways. For POS registers, the computers need not be as fast, have as much memory or hard disk space as PCs that might be installed in the office. This illustration uses Windows XP on every computer, even the file/print server. While XP home may be okay for a POS register, XP Professional is suggested for the office computer or file server because the Home version can only accept 5 simultaneous connections while the Professional version can accept up to 10. Office users typically install and use more applications than might be at a POS unit, which is normally running only the POS software or TimeClock for employees to punch in/out. However, the office might use Microsoft Office, Outlook for email, possibly a special graphics application for creating the club's newsletter, etc. so the office computers need more memory, bigger hard disks and faster processors because they're doing more things. A computer that is used as a file server should be the fastest of all the computers, have the most memory and the largest hard disk for storage.
- **Laser printer:** a fast laser printer can be a tremendous time saver and is generally more economical than ink jet printers are. Ink jets and ink stick (dye sublimation) printers may produce better color photos and be less expensive at the initial purchase, but their overall ink cost is much greater on a per-page basis than laser toner. When choosing a centrally shared printer for printing reports, checks and statements, a brand name laser is the best choice. Laser printers typically use 8½ x 11 or 8½ x 14 inch single sheet paper, but some can use 11x14 or 11x17.
- **Receipt printer:** Most clubs use fast, thermal printers such as the Star TSP-100 for printing receipts. Thermal printers are reliable, quiet, fast, easy to reload with paper, and print an excellent, crisp customer receipt.
- **Kitchen printer:** impact (e.g. dot matrix) printers are recommended for environments where heat can be a factor. The Star SP700 series is an excellent, fast and durable unit that takes little space. Thermal printers are not a good choice for kitchens because heat can easily blacken the thermal paper and make it unreadable. Because a kitchen printer is often located a distance away from the nearest PC, the type of printer cable necessary to print to the printer can dictate whether the printer communicates to the

computer using a USB, parallel, serial or network mode. When deciding the kind of kitchen printer and its physical location, consider the following cabling limitations:

- **USB:** typically limited to 6-10 feet max. An advantage of USB is its ease of use and “plug-n-play” capability; most modern computers have multiple USB ports built in. Not all printers can use a USB connection; be sure to check before you buy.
- **Parallel:** this cable type is limited to less than 25 feet. Also very easy to configure although the computer must have a parallel port, a parallel cable itself is rather thick and stiff and the physical connectors on each end are the largest of all printer types.
- **Serial:** typically works up to 200 feet. The cable and connectors are similar to the parallel type. Hardest to configure because of the many serial port settings that must be just right or the printer won't print readable receipts. A bigger problem is that many modern computers do not include a serial port as an option and it must be added as a separate piece of hardware inside the computer.
- **Cat-5:** limited to about 300 feet per single cable segment; if greater than 300 feet, it must be connected to a “repeater” to reamplify the signal for the next cable segment. The wiring is flexible and fairly small, and these printers incorporate their own network electronics so that they plug directly into the network switch instead of to a computer. They use the TCP/IP protocol and must be configured to use a fixed IP address on a DHCP network instead of letting the network router assign an address. This is a bit harder to set up than USB or Parallel, but once configured, is highly reliable and convenient.
- **Cash drawer:** these typically plug directly into the receipt printers using a telephone-type connector and cable. As the receipt prints, the printer sends a small electrical pulse to the cash drawer that opens a latch and the drawer pops open. The cash drawer cable must be pinned to match the receipt printer type, i.e. a cash drawer set to work for an Epson receipt printer will not work with a Star printer because the Epson and Star printers use different electrical plug connections for the cash drawer.

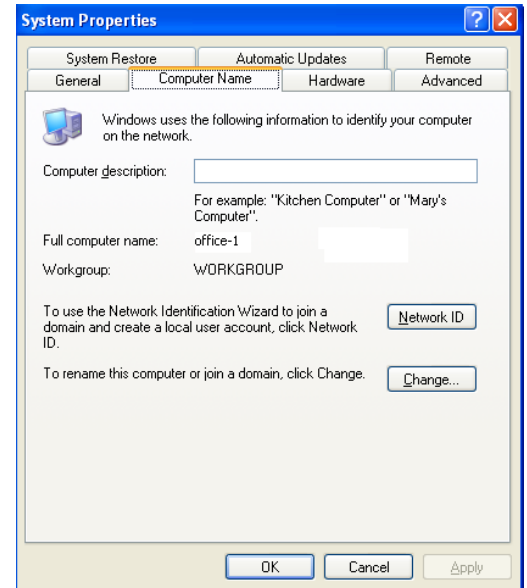
### Communication basics

Just as two people must share a common language to be able to communicate effectively, for PCs and other network devices to actually communicate with one another, they must also have some level of compatibility. Additionally, there must be a minimum of barriers put in place between the communicating parties. In this illustration, the compatibility factors include the computer names, the workgroup name and the IP address. The most common barriers that prevent computer communication are firewalls and over aggressive antivirus software.

**Workgroup or Domain?** Think of a domain in terms of a large corporation where there are hundreds or even thousands of workers in various departments such as accounting, sales, public relations, advertising, design support, legal, customer service, research & development, systems, investor relations, etc. In the context of a large corporation, each department may be large enough to be a workgroup unto its own (and possibly even have its own server!) and the domain architecture concept seems like a pretty good idea – the domain is the umbrella that covers all the departmental workgroups. But a corporation has a complete MIS systems department staff to manage the domain and all the things related to it; club operations don't quite match that scope, nor do they have budgets to have full time MIS staff.

A club may have the very same functions as the large corporation, but club staffers generally wear a lot of hats, and they generally do their work using one (or sometimes two) computers. Creating a domain in this 5-computer illustration is overkill; it's “make-work.” One isn't necessarily “better” than the other, but a Workgroup is simpler to configure and a lot less expensive to maintain than hiring a full-time staff to manage it.

- Primary network configuration settings are established in the Windows Control Panel, in the section entitled SYSTEM, under the COMPUTER NAME tab, as in this example:
- Workgroup name: this helps identify groups of computers that are intended to work together. Windows' default setting is usually MS-HOME or WORKGROUP, but you can use any name you like. Many clubs use their club name or club abbreviation as the workgroup name while others add the word OFFICE to their club abbreviation so it becomes ABCOFFICE. Generally speaking, keep it simple and don't add to the complexity by inserting punctuation characters, either.
- In our illustration, the computer names are also simple: OFFICE-1, OFFICE-2, POS-1, POS-2, POS-3. Their names denote their tasks and even suggest their locations. Whatever names you choose, remember that they must be unique (no two computers on the network can have the same name) and short and simple names will lessen the complexity.
- To communicate, the computers must be using the same "language." TCP/IP is the most common "protocol" (e.g. language) that computers use to talk to one another, and TCP/IP uses unique numerical computer "addresses" for each computer to keep them apart. Each PC has its own unique "TCP/IP address" on the network, just as houses on Maple Street have their own house numbers. A TCP/IP address has four segments separated by a decimal, such as 192.168.1.103. While not absolutely correct, think of the first three segments (192.168.1 in this example) as Maple Street while the last segment (103 in this example) is the house number. If you think of your network as a "street," TCP/IP addressing gets a lot easier because you only have to change the last segment – e.g. the "house" number.
  - For true convenience, your router is likely configured (right out of the box) as a "DHCP server" which means that it automatically controls and assigns all the TCP/IP addresses on your network for all devices that are also set to use DHCP automatic addressing. Talk about easy!
  - However, you should also understand that the order in which devices are powered on determines which device gets which IP address. In other words, the first device powered up gets the first available numerical IP address while the next device gets the next address, etc. This generally doesn't mean a hill of beans on a daily basis, unless you have a kitchen printer plugged directly into the network switch.
    - While automatic addressing works fine for the computers, it doesn't work in cases where a device's address can never change because of being powered off and then on again. A kitchen printer is one of these devices because every POS computer that will print orders to it must be configured to print to the kitchen printer's specific TCP/IP address. Can you guess what problem occurs if the kitchen printer's IP address is subject to change because it was accidentally unplugged or the building's power flickered off and back on again? That's right: *suddenly none of the orders sent to the kitchen will print because the kitchen printer doesn't have the same address it had before – it has a new IP address!*



- The solution is to define the kitchen printer with a fixed IP address. You already know that no two devices can have the same address, but what address should you use? It's easy to figure out. In our example, there are 5 computers on the network. That means that there are only five consecutive IP numbers that will be used. Simply find out the IP address of any one of the computers powered and add 10 to the last segment of the number. Therefore, if the OFFICE-1 computer's address was 192.168.1.105, adding ten would yield 192.168.1.115, a compatible address that will never be in conflict with the other computers. (Note: the last number in an IP address segment cannot exceed 254. If adding 10 results in a number greater than 254, then subtract 10 instead. The idea is to add or subtract a number that is larger than the total number of computers on your network and the resulting address is likely one that you can use for your fixed IP address remote printer.)
- Most printer manuals include information on how to set the IP address for printers that have that capability, but the actual steps involved are beyond the scope of this document.

### Barriers to Computer Communication

Reliable communication between the various devices on your network is essential. Club Office accounting and SQLPos POS rely on a sound functional network to allow the system to complete operations such as placing food orders on hold from one POS unit and recalling them from another unit a few moments later, closing tickets and allowing the completed tickets to flow into the Club Office accounts receivable system. Or allowing employees to punch in/out with TimeClock so that payroll time records can be correct and payroll properly calculated. In an otherwise physically sound, working network, four primary barriers exist that can cause the communication between the devices to fail:

1. **Misconfigured network shares.** The main central repository of programs and data must be "shared" to networked users so they may create, modify and delete files as are required by the software. Allowing only "read" access isn't good enough.
2. **Misconfigured firewalls.** A firewall is usually a piece of software running on either the computer being used or the computer you're trying to connect to, *or both*. The firewall's purpose is protecting against outside things from getting in. Think of a firewall like a door. If the door can't be opened, you can't get to the room on the other side.
3. **User permission settings.** This refers to whether the person using the computer has sufficient privileges to the computer and/or to the software involved. Computer user privileges aren't the same as giving a verbal okay: they're actually configuration settings made in the user accounts that are defined on the computer(s) involved. User permissions are like a key that can unlock the lock on the door.
4. **Overly aggressive antivirus software.** This is software that in real-time, scans the actual *content* of the programs and data traveling in and out of the computer. While the firewall is the door and user permission the key to the door's lock, antivirus software is like a traffic cop's radar – always scanning the moving cars and raising an alert when something's not right. Antivirus software can behave almost like a firewall if it's set to the very highest protections. Because it's running in real-time, it has the propensity to slow down the computer enough so that the network may seem as if it's not working when in actuality, it's just the antivirus software being super-busy and working overtime scanning and double-scanning everything going in and out of the computer.

As an observation, most users lack the knowledge to configure a firewall or antivirus product to allow computers to communicate on a network. In addition, those same users usually won't take the time to learn how to do it. It's not rocket science but it does take a little time and patience before one is comfortable with it. To that end, here are a few ideas:



1. Shut the firewall and antivirus software completely off. If you don't know how to do that, uninstall the respective software (if you can). Obviously this choice means that you are operating without the benefit of the protection afforded by these products, but if given the choice between being able to get work done vs. not being able to do anything, most people would lean in the direction of getting the work done. If this is a choice you decide to take, we recommend that those computers not be allowed to access the Internet.
2. Select an antivirus product that does not bundle-in additional firewalls as parts of its basic security package. Products such as Avast and AVG have easy configuration options that simply by checking a box enable or disable the installation of certain functions and using such products can make your life a lot easier. Before you buy antivirus software, read something about it – the manufacturers' web sites usually have plenty of helpful information and sometimes, a try-before-you-buy policy.
3. Take the time to learn how to set up allowable activities and exceptions for the firewall and/or antivirus software you are using. Read the built-in help files, contact the technical support people who wrote the software or, believe it or not, try reading the operation manual. If you purchased a commercial package, chances are there's at least a small printed manual that came with the product, or at least an Adobe Acrobat PDF version of it is available on the software CD. For example, the default setting for the firewall built into Windows XP does not allow file and printer sharing. If this is the main computer that's functioning as the Club Office server and these features are not enabled, nobody will be able to use Club Office from any computer on the network, SQLPos will not be able to transfer its sales to the A/R system and employees will not be able to use TimeClock to punch in or out. So just that one, single checkbox on the Windows firewall configuration screen can have an *incredible* effect on your network.
4. Antivirus software is necessary in today's computing experience. Antivirus software generally works on certain types of files (called "executable" files) that virus creators like to attack. These are generally operating system files that are of the EXE or COM file type – essentially program files that the user "executes" on the computer by double-clicking on them as opposed to data files or help files that generally just sit around and take up space. An executable program is one that *executes* – *it does something*. By sneakily attaching a virus to a common executable file and then putting it on your computer, the virus creator hopes that when you execute that file, the virus is activated at the same time. What the virus subsequently does can be disastrous to your business and there's no way to know what or the scope of the damage that could result. Some viruses simply may display an annoying message on your screen while others can completely erase your hard drive – as well as all the other hard drives on all the computers on your network, which could take your business weeks or months to recover from!


This is why antivirus protection is a necessary evil and it's also why antivirus software focuses on protecting those executable files from being changed; if it can keep them from being changed, it can prevent them from becoming infected at the same time.

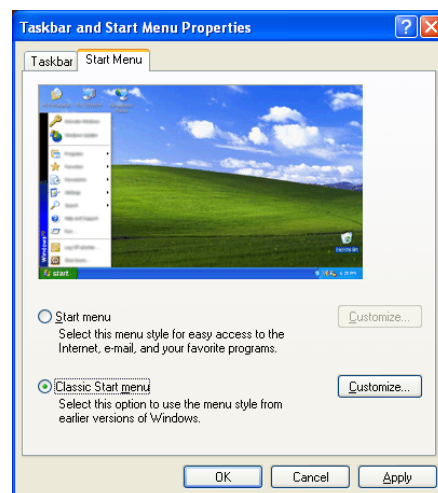
However, consider that a software program update is, by design, a change in the executable files on your computer – a replacement in many cases of the very files that your antivirus software is working so hard to protect. Consequently, antivirus software can actually prevent a software update from being successful. Therefore, the only really secure way to update your computer's software with new programs usually involves reducing or temporarily shutting off the antivirus software while the software update takes place and then turning it on again after the update is complete.

## Appendix 2 – Making Computer Administration Easier


Windows provides multiple ways to display its screens on the monitor. The default way is intended to be “friendlier” and easier to use, but this method “hides” things from the desktop. Unfortunately, those are the very things that can make Windows administration easier. To show them, use the “Classic” view. This is set in two places: at the **start** menu and again inside Windows’ File **Explore** that changes the way file folders and folder contents are displayed. And if you don’t think this is important, be sure to review Appendix 3 later on...

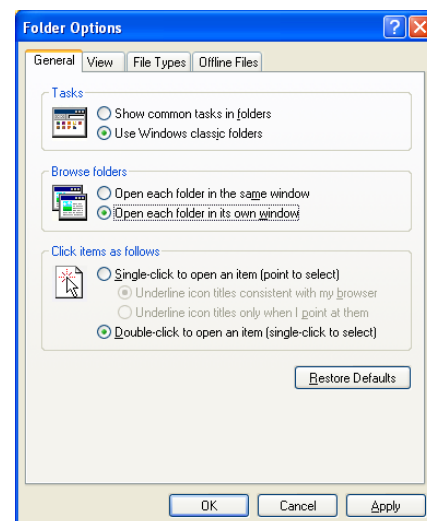
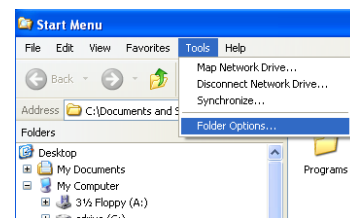
### Changing the Start Menu

1. Changing the start menu setting also changes the Windows Desktop so it includes more system-related information.
2. Right-click on 
3. Choose the properties option that appears. This will display the Taskbar and Start Menu Properties box.
4. Select the Classic Start menu option.
5. Click Apply to make the change, then click OK.
6. Immediately, you’ll see icons on your desktop that weren’t there before: “My Computer” and “My Network Places” are two options that will save you time and aggravation and what’s more, will make it easier for technical support people to help you when you call them for assistance.

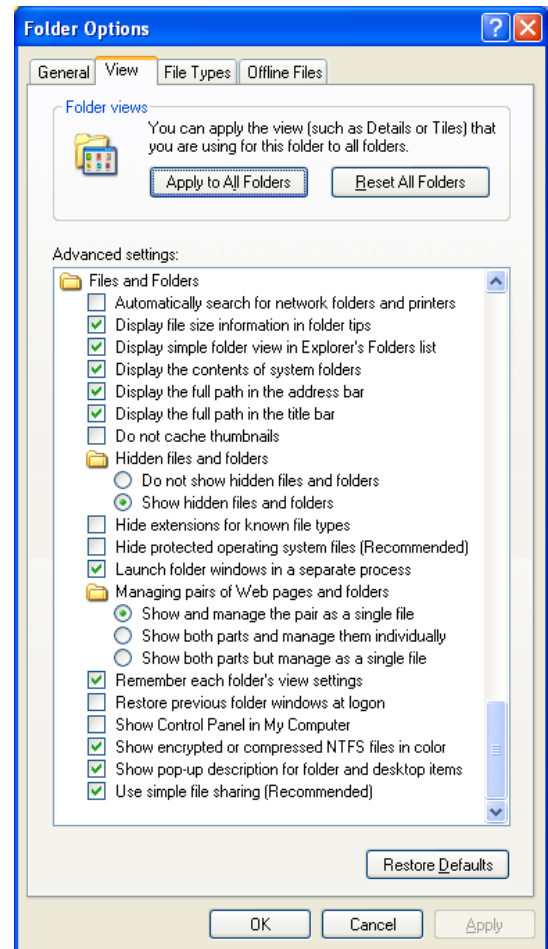


### Changing the Way Windows Displays Folders and Files

1. Changing the way contents of folders and files are displayed on your computer is the next important step to making your computing life easier.
2. Right-click on 
3. Choose the **Explore** option that appears. Don’t confuse the Windows file/folder **Explore** feature with **Internet Explorer browser** – they’re two different yet very similar functions built into Windows. Thinking of **Explore for files** and the **Explorer browser for web sites** may help you keep them apart.
4. Choose the Tools menu option; then choose Folder Options:
5. At the Folder Options panel, choose **Use Windows classic folders**.
6. Many users prefer to **Open each folder in its own window** because this setting allows “parking” a folder and leaving it on the screen already open to a certain place. This is very handy when you need to copy a file from one place to another. Having the destination folder “parked” on the screen is more convenient than having to look for it all over again.
7. Click Apply to lock the setting.
8. Click the **View** tab at the top of the screen.



9. Inside the **View** tab, change the settings to read like the example to the right (your view tab may not be as tall as this example – use the scroll bar on the right side to move up/down):
  - a. Uncheck the **automatically search** option to turn it off. This is *especially* important for POS computers that are configured to use specific printer assignments for kitchen or other remote printers.
  - b. Check to **show hidden files and folders** so that you can navigate through the whole computer.
  - c. Uncheck the **hide extensions** option so you can see all the files. This will give you the ability to tell one file type from another.
  - d. Scroll down the screen so that you can see the option to **hide protected operating system files** and uncheck it. You'll get a warning message, but click YES to confirm that you want to do this.
  - e. Check the box to **use simple file sharing** if it isn't already checked. This will make it easier later on.
  - f. Click Apply to lock the settings.
  - g. At the top of the screen, click **Apply to All Folders** to have the settings apply throughout your computer; another informational message will appear, click OK to close it.
  - h. Then click OK to close the Folder Options screen.



### Comment

You won't gain a true appreciation for how important consistent screen displays are until you've just driven into your driveway at home late at night after a 25-minute ride from the club when your cell phone rings and it's your bar manager who's in crisis mode trying to reconnect the network after the power went out for a few seconds while there's a large wedding party still in progress at the club.

If you know what the screens look like, you can quickly walk the bar manager through a fairly complex operation that's been made a great deal simpler by having consistent screen displays throughout your operation.

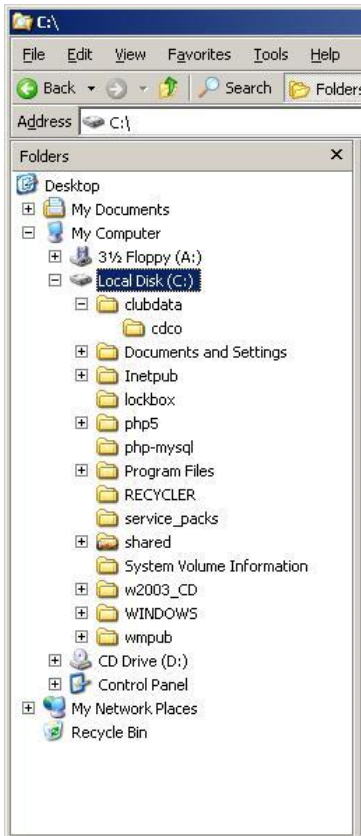
Or, you could turn around, drive back to the club, fix the problem on your own in 5 minutes and then drive back home again – wasting nearly an hour of unexpected drive time as well as additional gasoline expense.

It's your time and money.

## Appendix 3 – It Looks Different *but the Concept is the Same*

Windows comes in many versions and while the screen displays in each may be different from one another, it's important to know that the general appearance and functionality is generally very similar across versions *when the file/folder settings are consistent*. Here's what Windows Explore looks like on three different systems where the user has chosen to view the local C: drive:

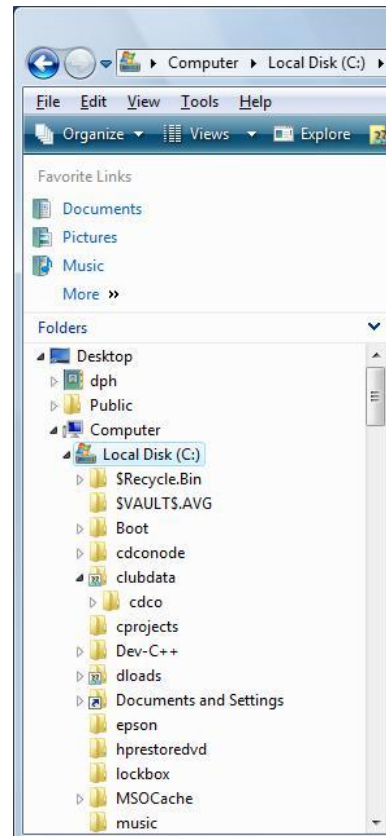
Windows 2003 Server



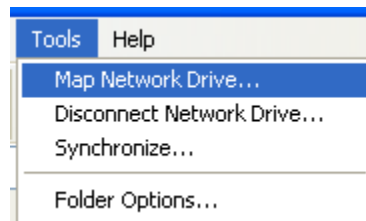
Windows XP



Windows Vista/Windows 7



Notice that the menus at the top of each screen are nearly identical. More importantly, the TOOLS menu option is roughly in the same place – just to the left of HELP. That's important because the tools menu includes an extremely valuable networking option:



**Map Network Drive** is the launch point for connecting and reconnecting the computer to a server, or to another computer's shared data area. Take the time to become best friends with it. We won't cover it here because you can just as easily click **Help** and type the word **CONNECT** into the Windows Help search box to find out all you need to know.

## Appendix 4 – Computers as Network Servers

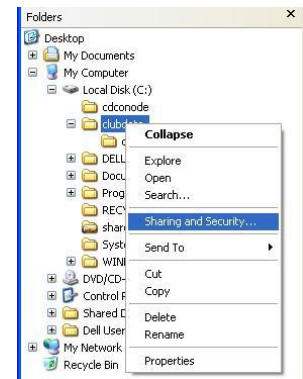
There are a few things that you need to know when setting up a server. These apply whether you're actually using the Windows Server operating system or any other flavor of Windows that will function in a either a central file or print server role on your network. Essentially, two things need to happen:

1. **A resource on the computer must be shared** so that other computers can see it and therefore possibly connect to it. Sharing makes a resource visible on the network – if it's not shared, it's only accessible from the server computer's own console. Sharing is like putting a picture window in the kitchen wall so that a neighbor can look in and see the cherry pie you just baked sitting on the counter.
2. **Appropriate permissions must be provided** so that others can actually use it. Being able to "see" a shared resource doesn't automatically mean that others can access it. Permissions are like opening a window so that a neighbor can reach inside and grab a piece of that cherry pie!

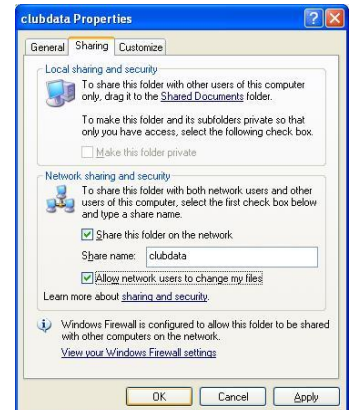
### Creating a Shared Resource

The procedures for sharing a folder or printer are virtually identical, even from one version of Windows to another. Using Windows XP as the example here, the basic procedure is:

1. Right-click on the folder or printer to be shared.
2. Choose **Sharing and Security** from the menu that appears.

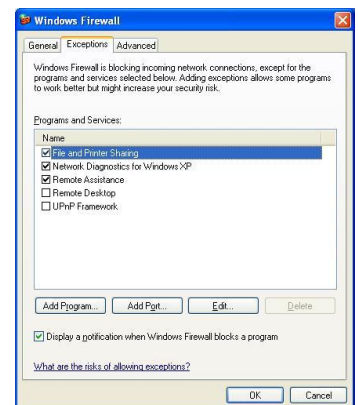
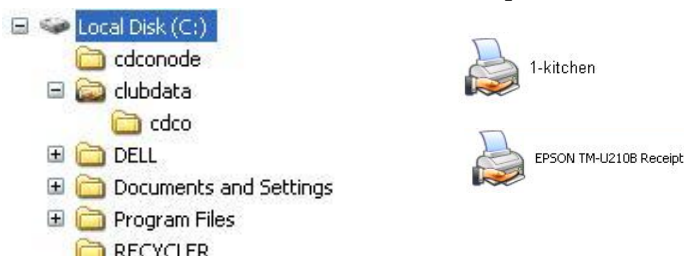


3. Select the option that enables sharing the item.
4. Give the item a share name (this is what becomes visible to the network). Suggestion: keep the share name short.
5. Set permissions for users who can access the shared item.



6. Make certain that File and Print sharing is enabled on the computer's firewall so that the firewall doesn't keep users out, too. The sharing screen normally includes a handy link to view the Windows Firewall Settings – check it to make sure.

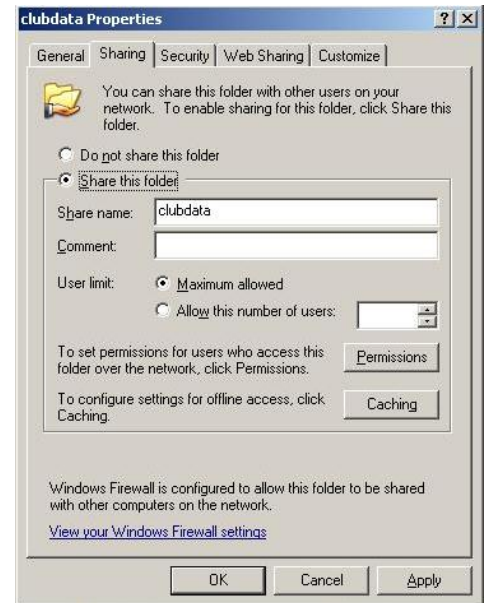
7. Click Apply and OK where those options are visible. When done, the item just shared will have a small "hand" beneath it that indicates a share exists, like the folder and printers below:



### Windows Server Permission Settings

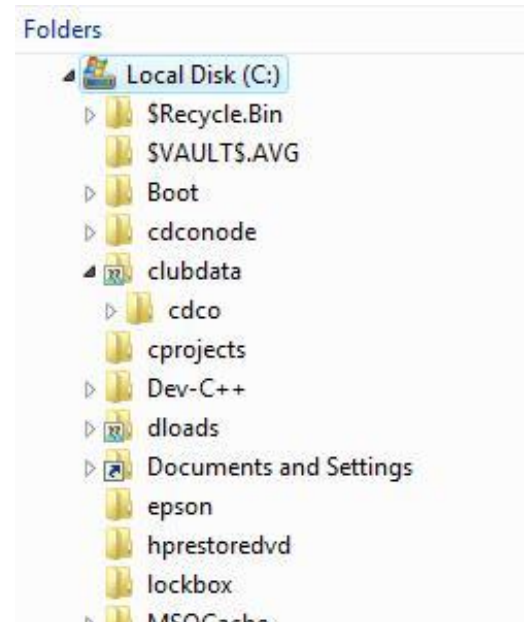
With Windows Server 2003, you'll encounter a vastly different and broader permissions issue in that "groups" and "users" are involved. The scope of this document does not permit covering this topic fully but the general procedure for creating a shared resource still holds true.

If you use a Windows Server at your facility, learn the basics for managing it. It's an extremely powerful and capable server operating system that's perfectly at home in a small 5-computer network or in a large, multi-national corporation with thousands of computers. Because of its flexibility and the numerous ways that Windows Server can be configured, *it can quickly become quite a bit more complicated than XP, Vista and Windows 7.*



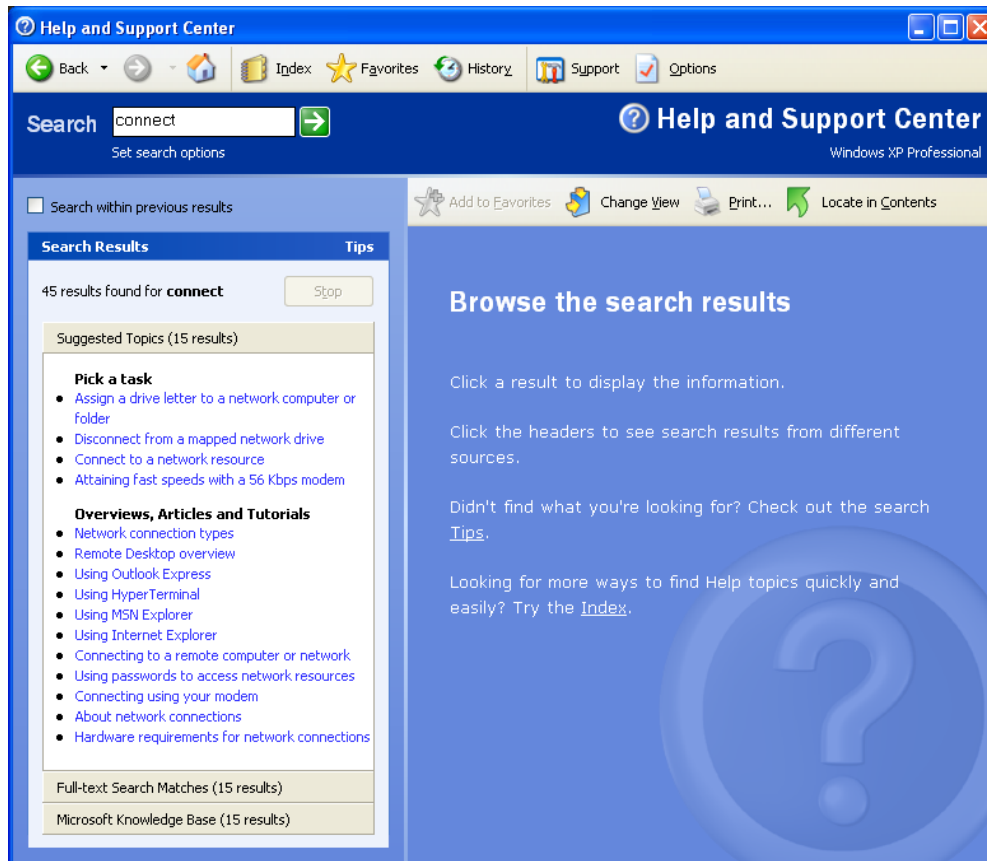
### Sharing and Windows Vista/Windows 7

Windows 7 and Vista's sharing method is different still yet it follows the same general procedure outlined earlier. After the share has been created, the display indicates a departure from using the small hand to mark that a folder is shared: a small box with question marks appears on the folder in place of the hand. In the enlarged example to the right, both the **clubdata** and **dloads** folders are shared:



## Appendix 5 - Connecting a Workstation to the Network

1. Click Start, then Help.
2. Into the help search window, type the word CONNECT and click the GO arrow. You'll soon see a screen like the one below where you can find out all you need to know:



## Appendix 6 – Making Network Connection Icons Permanent

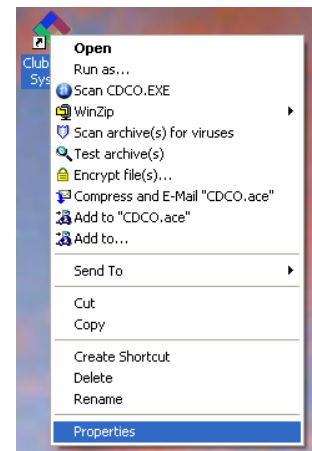
Windows includes internal “*Intellisense*” (Microsoft’s word for “intelligent” and “sensible”) that tries to recreate your computing environment on its own when things go awry. The goal is to help you, and as admirable as this is, it doesn’t always work out the way one might hope.

Sometimes, a network connection that you’ve created to run a certain application on a specific network drive is lost. There are many possible reasons why this can happen, but one way is if you start your computer before the main server computer is started up: when your computer tries to establish a connection to the server, it can’t find it because it isn’t turned on, and so Windows “intellisense” takes over. Here’s how it works:

1. The computer can’t establish network drive P: because the destination server computer isn’t powered on at the time your computer is trying to make the connection.
2. Windows knows that the name of the server computer where drive P: is supposed to be connected is called “ABCSEVER” and the shared resource name is “**clubdata.**”
3. But because drive P: can’t be established, “Intellisense” kicks in and substitutes the words instead of the drive letter and it decides to change the shortcut for you to read **\\ABCSEVER\CLUBDATA\CDCO** instead of **P:\CDCO**.

You don’t want this scenario to happen and preventing it is quite simple:

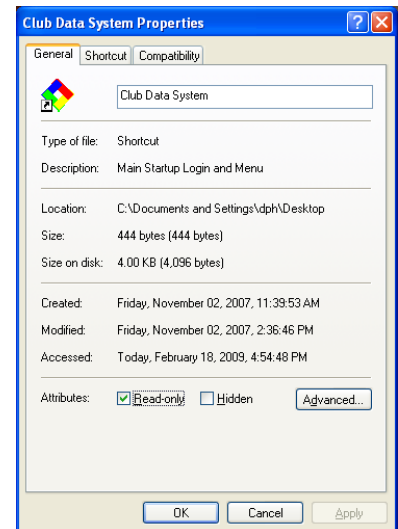
1. Right-click on the desktop shortcut and choose the Properties:



2. Select the GENERAL tab in the properties panel.


3. Click the Read-only box.

4. Click Apply and OK.





## Appendix 7 – Bringing It All Together

Okay, now it's time to put all this into the context of how Club Office accounting, SQLPos POS and TimeClock operate. To start, it might be helpful to look at a map analogy. It's a map of what we here in the Twin Cities call the I-494/I-694 Loop – it's the main highway system that circles the Minneapolis-St. Paul area. Our office is in the lower left corner of the loop – the  in the map is almost directly above our office building.



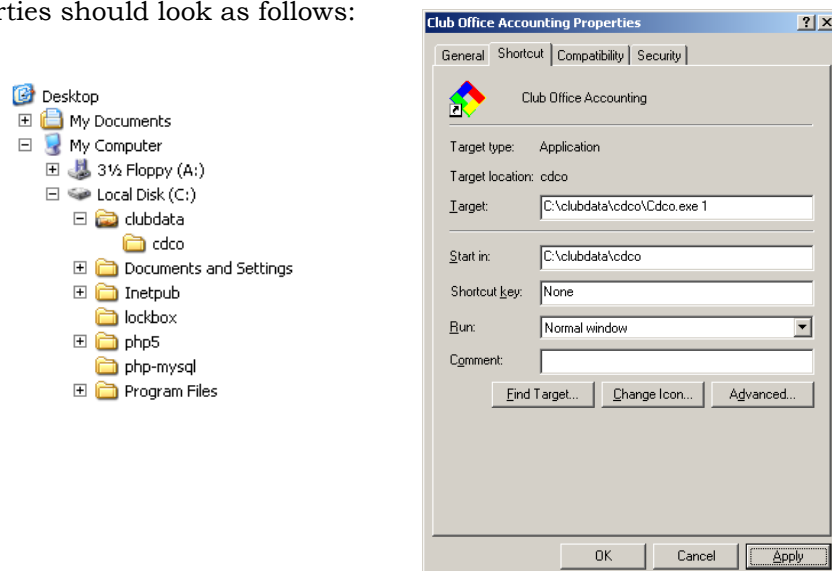
The point of the map analogy is to show that while there are many ways to get to our office, the route you take depends on where you are *relative to where you want to go*. Networking is the same thing – the path to the centralized data is *relative to the computer you're currently using*. In networking, you establish this path by “*mapping a network drive*.”

Your computer likely has a hard disk inside it. By default, this is usually called the “C:” drive by an alphabetical naming convention that was invented a few decades ago. If a CD-ROM or other drive is also installed in the computer, it would likely become the “D:” drive, and so forth down the alphabet as more hardware drives are physically installed inside the computer's case. Letters toward the front of the alphabet generally refer to pieces of physical hardware that are installed inside the computer itself, so relative to the computer, it has a drive “C:” and probably a “D:” drive physically built right in, e.g. “*hardware drives*” that the user on that computer has immediate access to. But what about data that's located on a different computer's drive?

This is where *network drive mapping* comes in. Because drive letters can go all the way to “Z,” the unused letters can be used to represent “software assigned drives.” A network drive is simply a relative location on the network that has been assigned a drive letter by the Windows software so that *relative to the local computer*, it appears as if it's actually installed inside the local computer's case even though it physically resides inside a different computer's case.

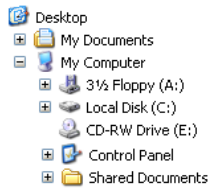
But here's where it gets a little tricky: when two computers are pointed to the same relative place, they may not be using the same drive letter to do so because *it depends on which computer you're using*.

At the main server computer, a typically Club Office system is installed to the C: drive into a folder named **clubdata** and the folder is shared with full read/write/create/delete privileges given to all users. If the software will also be used periodically on the server, then there's a desktop shortcut on the server to start Club Office. The server's Explore screen and desktop shortcut properties should look as follows:

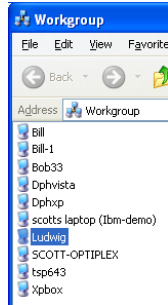


Because we're connecting a second computer to the Club Office accounting system, we'll map a drive from it to the **clubdata** share on the server. First, let's open up Explore to view the local computer's drives. Then we'll open up the Network Workgroup to view the computers on the network. In this example, the Club Office software has been installed on the server named **LUDWIG** so we select that computer and open it to view the resources that it's sharing. Then by right-clicking on the **clubdata** share, Map Network Drive appears as an option:

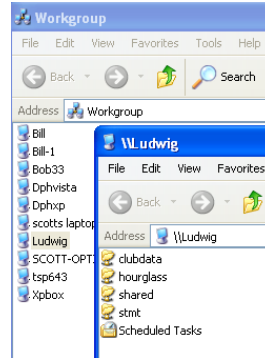
Windows Explore



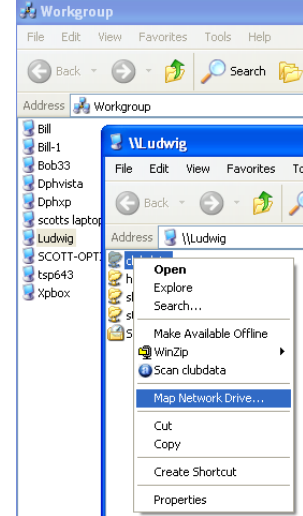
Computers



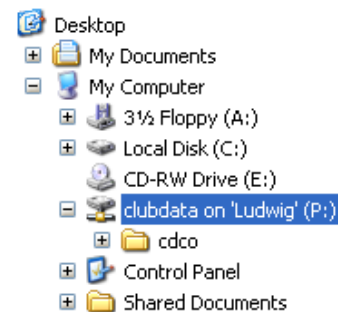
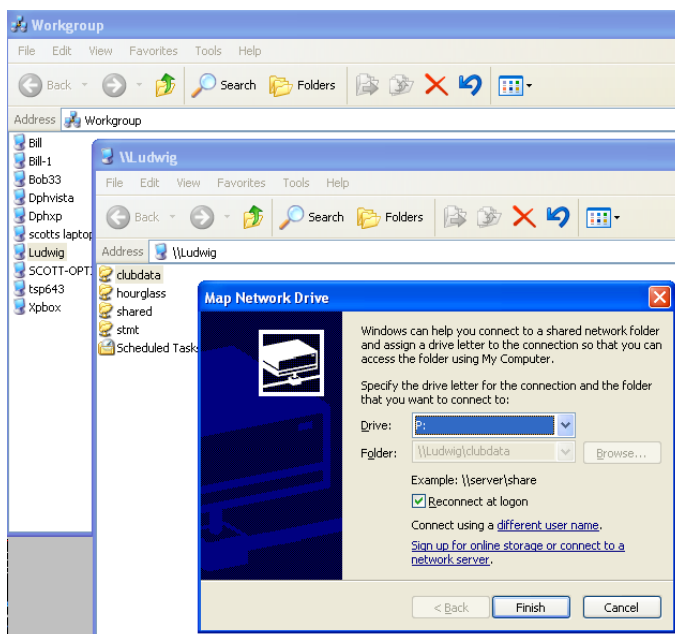
Ludwig's shared resources



Starting the map process

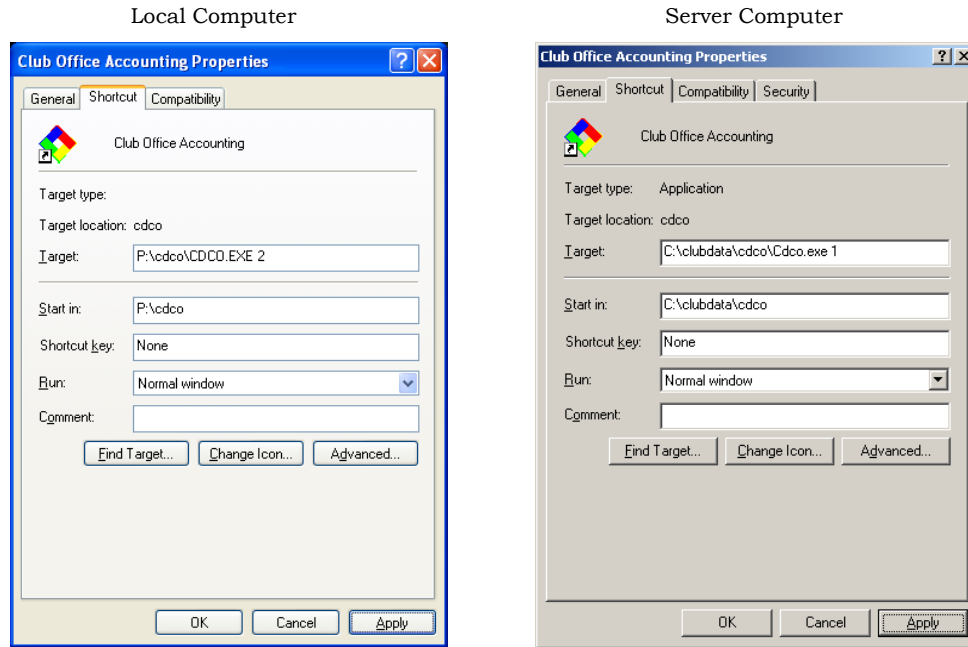


The Windows Map Network Drive wizard appears, we select drive P from the list of drives that are available, check the box to "Reconnect at logon" so that the computer will try to automatically connect drive **P:** to the **clubdata** share on the **Ludwig** server when the computer is restarted at a later date, and then click the Finish button. When done, Windows Explore shows that in addition to the local drives on the computer, now there's a (**P:**) network drive. The icon for the new network drive is similar yet slightly different than the icon for the local C: drive and it displays both the name of the share and the name of the computer to which the network drive is connected:



Now that the network drive has been mapped to the server, we can create a desktop shortcut to point the local computer to the accounting system located on the server. In this example, since we're adding the second computer to the network, this computer workstation will be the 2<sup>nd</sup> one connected to Club Office accounting.

For comparison, the desktop shortcut that was made earlier on the server itself is also shown below:



What's important to understand is that the remote computer and server are pointed to *exactly the same CDCCO.EXE* startup program but in *relative* terms:

- The local computer's startup is looking at the *networked* drive mapped to the server computer because that's where the accounting system is. The path to the startup program is **p:\cdco\cdco.exe**
- The server computer's startup is looking at its own internal *local* drive so it's startup path is **c:\clubdata\cdco\cdco.exe**
- The numbers at the end of the target line above is a Club Office requirement that allows the software to know which computer is doing what inside the accounting system. No two computers can use the same startup number.

### Be Consistent

While it's true that you can use any available network drive letter to map to a centrally located resource on a server, you should be consistent across your network when making these mapped drive assignments. Don't use drive P: from one computer, drive X: from another and drive M: from a third to map to the same location on a server.

Club Office accounting users typically use drive **P:** as their networked drive and you'll find that supporting your own network and fixing your own network connection problems will be a lot simpler if you're consistent.

## SQLPos Point of Sale and Employee TimeClock Software

These products are designed to run on remote computers and connect to the Club Office accounting system via mapped network drives (although both of these products also allow completely disconnected operation, too). Most users select drive P: as the networked drive of choice but as long as you are consistent throughout your network, you'll find that maintaining your network and securing support from Club Data will be a lot easier.

Because both SQLPos and TimeClock have their own installers and installation instructions, you can find more information in their respective installation/operation manuals.

## Installing Club Data Software Updates

When you install a Club Office, SQLPos or TimeClock update, the contents of the update need to go to a specific location either onto the computer's local C: hard disk or to a networked drive. Remember though, that these locations are *relative to the computer you're using at the time!* You'll understand why it's important to know the network relationship of the computer you're using to the network when you install software updates by pondering the following:

- If you are installing an update to the Club Office accounting software on the server itself, this is likely to the **c:\clubdata\cdco** folder.
- If you're installing the Club Office software update from a remote workstation that's connected to Club Office via a networked drive, the same location is likely **p:\cdco** instead.
- Our Club Office accounting software updates are preset to install to the **p:\cdco** folder. If you use a different networked drive from your remote workstations, or if you're installing the update on the main server itself, then you need to change the destination setting at the installer screen to point to the correct location where your Club Office system resides.
- SQLPos POS software updates are unique in that usually more than one computer is involved: the workstation as well as Club Office accounting. The SQLPos workstation update is present to install to the **c:\cdconode** folder because the point of sale software actually resides on the workstation itself and connects to the main server via a mapped network drive. However, the Club Office accounting system has its own SQLPos update (up-add-sqlpos) that is preset to install to the **p:\cdco** folder, where the accounting system resides. (Note: as a convenience to our users who have SQLPos POS, we also publish a special Club Office accounting software update called updatecdcoplus that includes *both* the Club Office accounting and SQLPos updates, eliminating the need to install the up-add-sqlpos update altogether.)
- TimeClock software updates are preset to install to the **p:\cdco** folder, just like the Club Office accounting system. This is because TimeClock needs to use the employee database, which is part of the accounting system. Therefore, if you're installing a TimeClock software update from a remote TimeClock computer, the default **p:\cdco** folder should work fine (provided you use drive P: as your mapped drive, that is), but if you are installing the update on the main server itself, then this is likely to the **c:\clubdata\cdco** folder instead because that's where Club Office resides when you're working on the server itself.
- ***If a software update is not installed to the right location, the software update will not be successful.*** Software updates should only be performed by staff members who have a working understanding of where their Club Office system software resides and who have the necessary computing skills to locate it properly from the computer being used at the time the update is performed.

## Appendix 8 – Obtaining Technical Support

If you've gotten this far, you hopefully understand that successfully connecting computers together in a Windows network is quite a *visual* process – one actually has to “see” what's on the screen *and know where to look* to be efficient and accurate at accomplishing the tasks.

Because all this happens in such a visual medium, solving network problems over the telephone is extremely challenging. It's frustrating for the caller because more often than not, the caller doesn't know where or what to look for and is in a hurry at the same time. But it's *even more frustrating* for the tech support person on the other end of the conversation because he or she can't see the computer's screen at all.

The tech has to try to envision the screen *through the caller's eyes and words* to get the lay of the land:

Is the person at the main server or are they at a remote workstation? Is the server powered on? Is the network even working? Does the caller know what a computer server is? Is there a firewall or antivirus software involved? Has Windows on this computer or the server or both recently been updated? Is the computer plugged in? Is the network cable plugged in? What kind of a server is it (Windows Server has special permissions settings while XP has far fewer) and are user access permissions involved? What's the skill level of the caller and does he/she have the basic computing skills or time needed to fix this? Does what the caller is describing make logical sense in the context of networking or something else? What's the IP address (you can often tell whether there's a working router on the network or not)? Did somebody unplug the network switch? Is this a hardwired or wireless network problem?

Okay, enough already! But perhaps now you have an appreciation why your customer support agreement with Club Data does not include answering network issues. It also may help you understand why there may periodically be an extra charge for “network support” on your Club Data statement when your staff calls for help reconnecting a remote kitchen printer, remapping a network drive to a server, or trying to diagnose all manner of possible network problems.

## Appendix 9 – Tricks of the Trade

There are some specific tricks that one can use to “make” a computer behave the way you want it to, as far as networking is concerned anyway. However, this involves a little manual maintenance at the front end and sometimes subsequent maintenance later on should you replace a router, server, or should a computer’s network name be changed.

### AutoDisconnect

All versions of Windows include an “automatic disconnect” feature as it relates to staying connected to a remote, network resource. The feature is intended to have some intelligence and is designed to reduce unnecessary network traffic. The feature essentially “disconnects” from the resource after a period of user inactivity, usually 10 to 15 minutes. An example of a common, everyday situation might be opening the membership screen to view an account, then taking a phone call and going into another person’s office for a quick chat, all the while leaving the screen untouched and open at that member’s account. Sound familiar? An autodisconnect feature may be important in a large business setting where there may be hundreds or thousands of computers, but in a small office setting it’s the source of a headache. Why? Well, when Windows shuts off the connection, other parts of the system that definitely should not be disconnected (such as the Access database engine) are affected, yet they can’t do anything about it. So when Windows disconnects, Access can’t override Windows and when you go back to the membership screen to do something, Windows tries to reactivate itself but Access can no longer find what it was connected to and now Windows and Access are fighting with one another. The result can be a database that is left in an unsettled status: it’s open, kind of, but not really, but it’s closed, but not really... it’s... unsettled. Microsoft Access doesn’t like that.

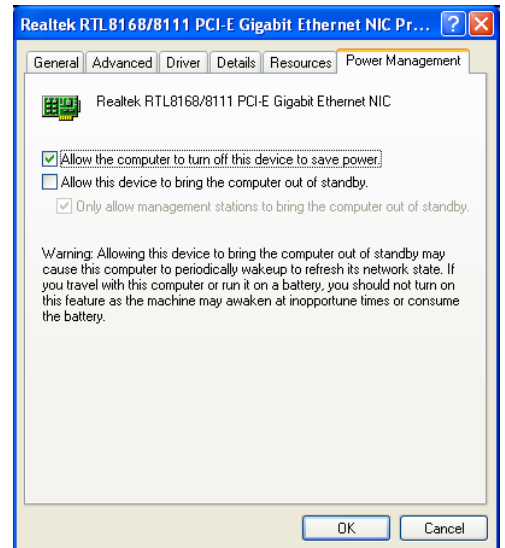
So what to do? One solution is never to leave your screen open on a record unless you’re actively using it. This will help a lot and frankly, is just plain sound computing practice. Another solution is to tell Windows not to disconnect after 10 or 15 minutes. How do you do that? Rather easily, really. However, you cannot turn the feature completely off. What you can do is set the autodisconnect time to a very large time period, on the order of 136 years instead of only a few minutes, and by so doing it will have the same effect. Here’s how to do that:

1. Get to a command prompt on your screen.
2. Type this into the command window: **NET CONFIG SERVER /AUTODISCONNECT:-1**
3. Then press the ENTER key on your keyboard. You should get a message that the command completed successfully.
4. This has changed the autodisconnect time in the Windows Registry to 4,294,967,295 seconds, which is slightly more than 136 years, the maximum value allowed.

While changing autodisconnect will help, you also need to make a companion change to the way Windows looks at “saving electricity.” That’s next.

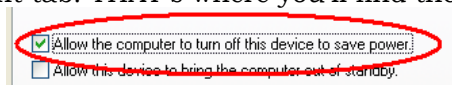
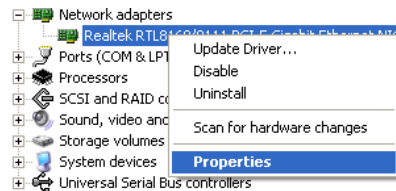
## Windows Power Saving Features

It makes perfect sense for laptop computers to conserve as much electrical power as possible because it makes the laptop's battery run longer. But the same logic makes no sense for a desktop office computer that's plugged into the wall because it's not running on a battery. However, a default Windows installation is preconfigured to settings that are more in line with a laptop than a desktop, and many things are set to "power down" after a period of inactivity. This is all well and good, and it's nice being "green," but in a network setting where you expect to be connected to other equipment, it contributes to network disconnects because one of the things that can be powered down is the network interface card itself – the piece of electronics that physically connects the computer to the network. Believe it or not, the default Windows setting is "allow the computer to turn off this device to save power." You will most likely find a checkmark in the box next to this setting:

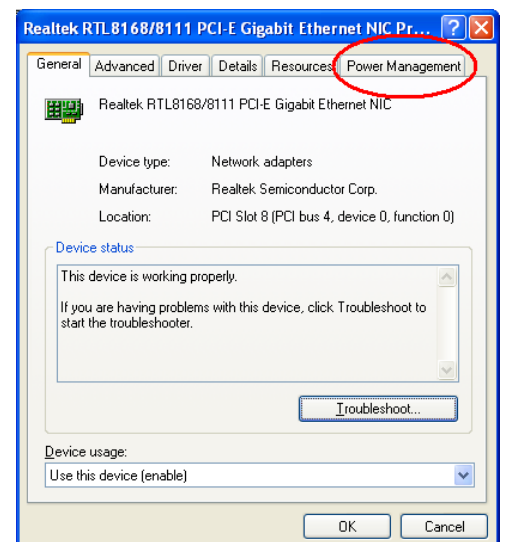
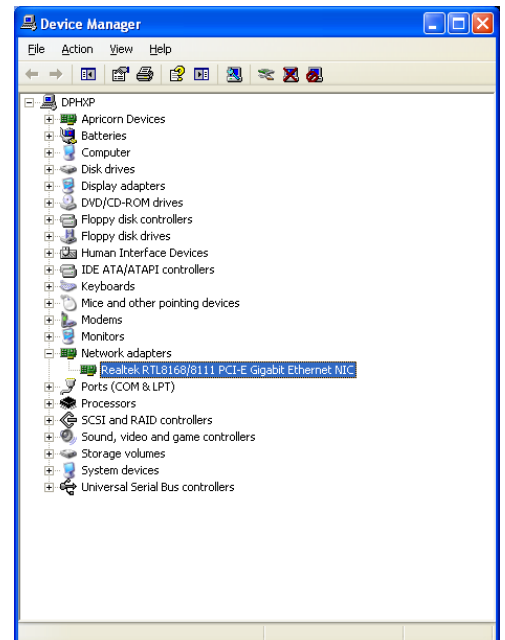


To turn it off, first you need to find where the setting is. It's in the Hardware Device Manager. Here's how:

1. Open the Windows Control Panel
2. Find the option for SYSTEM and open it. Look for a tab or link that says "Hardware" or "Device Manager." Different versions of Windows look differently, but they're one-in-the-same, and after it opens it may look something like the one to the right:
3. Click on the + next to Network Adapters and it will open a new line showing the adapter in your computer.
4. RIGHT-click on the adapter and choose the properties option, like this:
5. The properties panel will display something similar to this example on the right: Choose the Power Management tab. THAT'S where you'll find the setting:



6. Uncheck the box and click OK.
7. **Important:** close all the boxes on the screen and restart your computer for the change to take effect; if you don't restart the computer, it won't work.

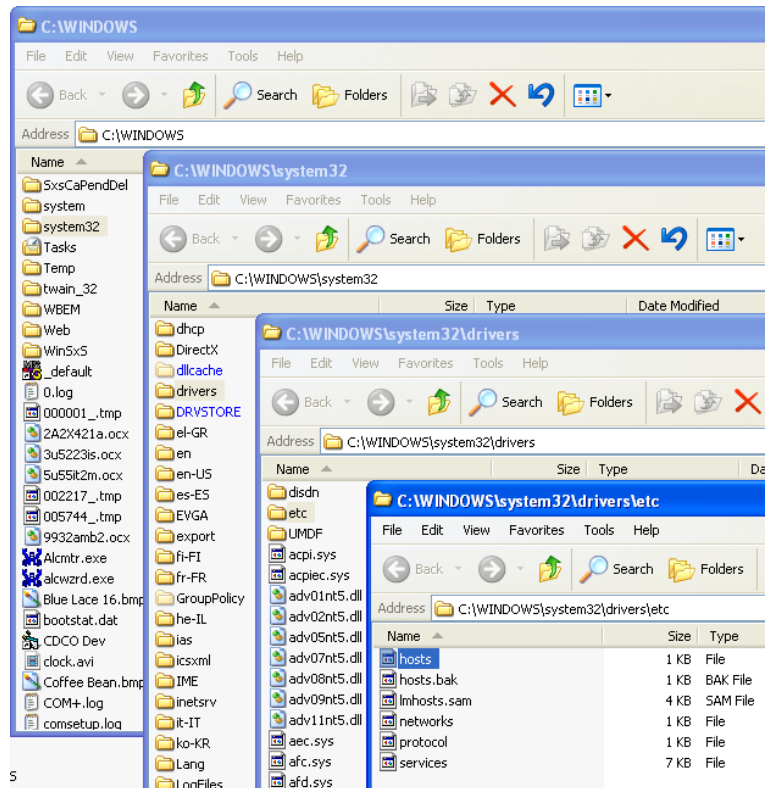


## HOSTS File

Here's a trick that hardly any tech people use but which forces your computer to "see" other things on the network. It can be particularly helpful in staying connected to file servers. When this is set, it eliminates most of the time that Windows takes for "network discovery" – the time it takes to search for devices on the network that it's supposed to connect to.

The HOSTS file is a static text file that you can edit using Windows Notepad. However, first you have to find it, and Microsoft buried it deep into an obscure place in the Windows folder:

1. Open the C: drive
2. Open the WINDOWS folder
3. Open the SYSTEM32 folder
4. Open the DRIVERS folder
5. Open the ETC folder
6. Now you'll see the hosts file!
7. Use Windows Notepad to open it.

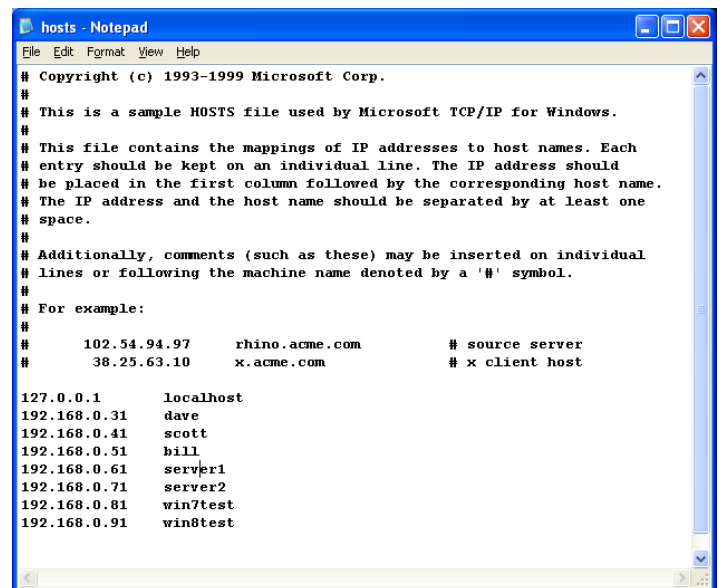


It's quite a cryptic text file but will most likely have only one entry in it:

```
127.0.0.1    localhost
```

127.0.0.1 is your computer. It's the same on every Windows computer and it points to itself. This is there so that the computer can "find itself" on the network.

In the example to the right, you can see some additions that have been made to the list. These are some of the computers in our office. Note that the IP address of the computer is on the left and the computer's network name is on the right, separated by a space.



## How it works

When the computer powers up, Windows preloads this file into its network memory and immediately knows the IP addresses of the other important computers on the network that this computer frequently connects to. It no longer has to "look" for them and it can connect right away. And it does. It's very fast and coupled with the autodisconnect feature, goes a long way to keeping the computers connected. BUT – there are serious caveats to using a HOSTS file:



- The HOSTS file must be edited/maintained on EACH computer; there isn't a single central one for the whole network. (Well, there can be, but that would be for a main DNS server and we won't get into the complexity of that...)
- If the network IP address of a computer listed in the host file ever changes, you won't connect to it anymore.
- If another computer's network name changes, you won't connect to it anymore, either.
- If you replace a router and the entire network addressing system changes to something else, you likely won't connect to anything at all.
- You must use dedicated IP addressing on your network instead of DHCP. If you use DHCP addressing, the HOSTS file is not a workable solution because the IP addresses are not permanent – they may change from one day to the next.

There's a pretty healthy tradeoff to using the HOSTS configuration file. On the one hand, it truly aids network connections but on the other hand, should your network setup ever change, you need to edit the HOSTS file to reflect the new network setups or you will not be able to connect to them at all. It's kind of an "all or nothing" setup that may require periodic maintenance as computers are added/removed/replaced at your facility. But if you want absolutely the most network reliability you can possibly have, it's part of a great solution. The last part is next.

### Dedicated IP Addressing

This is the last item on the list for making a network really and truly solid. While it's at the heart of using the HOSTS file, one can use dedicated IP addressing without using the HOSTS file and still benefit from the added connectivity the dedicated addressing can provide. DHCP stands for "dynamic host configuration protocol" – and notice that word "host" in there... Every computer on a network is considered a "host" of some type and the dynamic part of this works because a piece of equipment on your network (a router) has been configured to provide a few dozen other computers that connect to it with compatible addresses so that they can use the network. The "dynamic" part is that on its own, the router automatically assigns addresses as they're requested and "releases" those addresses when they're either no longer needed or the router's "time-out" is reached, whichever comes first.

Most people use DHCP. If you have a wireless network it's a virtual certainty that you use DHCP because it's design is for ease-of-use: turn on the laptop, after a few moments the laptop's wireless radio finds and locks onto one of eleven channel frequencies that are typically reserved for Wi-Fi use, the wireless router "sees" the laptop and automatically issues an unused IP address from within its list of available addresses, and bingo, you're connected. The computer can use that IP address as long as it maintains an active connection – the address is "leased" to the computer by the router for as long as it needs it or until the router's lease time limit is reached, whichever comes first. The "dynamic" part of all this is that the router issues and releases and reissues addresses on its own, automatically.

However, the address your computer gets is usually related to *when* you turn it on and what other network devices are already on when you connect to the network. If you're the first computer to fire up, the router usually leases the first available address from the address pool to your computer. If you're the second computer, you'll get the second address and so forth until all the addresses in the address pool are used up with active connections. As a computer drops a connection, the router senses that the address is no longer actively being used and it puts the address back in the available pool. The next computer to log onto the network will probably get the recently released address. That's the "dynamic" part of DHCP. Addresses are leased, released and reissued and it happens automatically and without any user intervention. The intention is that it's very close to "plug-n-play." It works pretty well, really. But because the

addresses can and frequently do change, it can also create some connectivity problems, too, because a computer that you connected to last week suddenly has a new address and now your computer has to try to reconnect to it using new parameters. It often takes time to “find” it again, and sometimes it doesn’t work at all because firewalls and antivirus tools may link a computer’s IP address to a specific computer name. If that computer comes alive with a new address, the firewall may reject the connection thinking it could be dangerous – the address and the name that it had in memory don’t match. *Oops!* Suddenly something that worked last week doesn’t work this week. Hmm... doesn’t that sound familiar?

Enter **dedicated IP addressing**. When an IP address is assigned to the computer, it retains that address until someone changes it. But there are some caveats to using dedicated addresses, too...

- The dedicated address should be outside of the range of DHCP addresses that a router on the network might issue. Assuming that the router might be set to provide 50 addresses starting at 192.168.0.100 this means you should use an address of 192.168.0.99 or below or 192.168.0.151 or above, leaving the 100-150 range for the router. You want to leave these alone because if the dedicated-IP computer is powered off, it opens the door for the router to issue the same address; then later when the dedicated-IP computer is powered up, there will be two computers on the network that have the same address. An error message will likely occur at that point and *both* computers will cease network communications. Sound like a bad thing? It is.
- You must maintain a list of which computers have what addresses so that you accidentally don’t reuse one. All it takes is a moment on the network with the same IP address as another computer to knock both computers off their connections.
- If a router is replaced, you may have to manually change the addresses of every dedicated-IP device on your network for them all to be compatible again. This includes network printers, possibly kitchen slip printers, and file and print servers. It usually means remapping connections to printers and sometimes even reinstalling printer drivers, not to mention reconfiguring the applications that use those printers. This can be a time-consuming task if you have a great many computers to manage.
- Adding an IP-based printer (such as a kitchen remote) to the network can be a cumbersome experience involving multiple manual changes of one PC to first be compatible with the printer and after configuring it to match the network, changing the PC back so it can talk to it again afterward.
- If using a HOSTS file, each computer’s file must be edited to match the new IP addresses and computer names and then rebooted for the changes to take effect.
- If you use the Internet, you must know the IP address of your Internet gateway and DNS servers so that appropriate DNS operations can be performed. In dedicated-IP mode, you must periodically monitor this to make sure your ISP hasn’t changed your gateway address or you’ll experience Internet connectivity problems, too. Internet service providers (ISPs) typically don’t notify their customers of such changes because they assume you’re using DHCP, which reconfigures itself more-or-less automatically. And of course, this applies to each computer, not just one.
- If you use a local DNS server, changing the server computer’s name and/or IP address can make that computer’s indexing system completely invalid and it’s entirely possible that you may not be able to get it working again, even from the server’s keyboard console. Managing a DNS server is outside the scope of this document and, in fact, is outside the scope of most computer users’ technical expertise.

### **Where Dedicated IP addressing is done**

The IP address is a property of the network interface card and can be accessed via the Windows Device Manager. It is highly suggested that before diving into this project, you secure some technical support assistance. It’s not a project that’s to be taken lightly.