

Occasionally I have students who take a security course who either have inadequate networking experience, or who are a bit rusty and need a refresher. This document is just the bare bones basics. These are rudimentary concepts that frankly everyone in any computer related profession should know.

## **Network Basics**

Getting two or more computers to communicate and transmit data is a process that is simple in concept, but complex in application. Consider all the factors involved. First, you will need to physically connect the computers. This connection (although sometimes accomplished by infrared light) usually requires either a cable that plugs into your computer. This cable then is plugged either directly to the other computer, or is plugged into a device that will in turn connect to several other computers.

Of course wireless communication is being used with more frequency, and wireless connecting doesn't require a cable. However, even wireless communication relies on a physical device to transmit the data. There is a card in most modern computers called a **Network Interface Card**, or simply a **NIC**. Its outer edge has a connection slot that looks like a telephone jack, only slightly bigger. Wireless networks also use a NIC; but rather than having a slot for a cable to connect to, the wireless network simply transmits to a nearby wireless router or hub.

### ***The Physical Connection***

As mentioned, cables are one of the ways that computers communicate to each other. The cable connection used with traditional NIC's (meaning not wireless) is an RJ 45 connection. (*RJ* is short for "Registered Jack.") In contrast to the computer's RJ 45 jacks, standard telephone lines use RJ 11 jacks. The biggest difference between jacks involves the number of wires in the terminator. Phone lines have four wires, whereas RJ 45 connectors have eight.

This connector jack must be on the end of the cable. The cable used in most networks today is a category 5 cable, or abbreviated as a “cat-5” cable. (Note that cat-6 cable is becoming more prevalent with high-speed networks.)

If you look on the back of most computers, you will probably find two ports that look like phone jacks. The first port is probably a traditional modem and has a standard RJ 11 jack. The second port is larger, and this is an RJ 45 jack. Not all computers come with a NIC, but most modern computers do. Table 2-1 summarizes the various categories of cable and their uses.

Table 2-1  
Cable Types and Uses

Category	Specifications	Uses
1	Low-speed analog (less than 1 MHz)	Telephone, door bell
2	Analog line (less than 10 MHz)	Telephone
3	Up to 16 MHz or 100 Mbps (mega bits per second)	Voice transmissions
4	Up to 20 MHz/ 100 Mbps	Used in data lines, Ethernet networks
5	100 MHz / 100 Mbps	The most common type of network cable
6	1,000 Mbps	Used in very high-speed networks

This type of cable is also often referred to as unshielded twisted pair cable (UTP). In UTP, the wires in the cable are in pairs, twisted together without any additional shielded. As you

can see in Table 2-1, each subsequent category of cable is somewhat faster and more robust than that last. It should be noted that although cat-4 can be used for networks, it almost never is used for that purpose. You will usually see cat-5 cable, and increasingly cat-6.

Category 6 cable is for the gigabit Ethernet. Cat 5 cable works at speeds of up to 100 mega bits per second (mbps), whereas Cat 6 works at 1000 mbps. It is widely available now, and has been for several years. However for it to truly function properly you need hubs/switches, and NIC's that also transmit at gigabit speeds. For this reason the spread of gigabit Ethernet has been much slower than many analysts expected.

Notice the speeds listed in Table 2-1 (such as MBPS); this speed stands for mega bits per second. Many readers are probably already aware that ultimately everything in the computer is stored in a binary format, a 1 or a 0. These units are called bits. It follows, then, that a category 5 (cat-5) cable can transmit up to 100 million bits per second. It takes 8 bits, or one byte, to represent a single character such as a letter, number, or carriage return. Remember that this is the maximum that the cable can handle. If multiple users are on a network, all sending data, that traffic uses up bandwidth rather quickly. And pictures being sent use a lot of bandwidth. Simple scanned-in photos can easily reach 2 megabytes (2 million bytes) or 16 million bits, or much more. Streaming media such as video is perhaps the most demanding on bandwidth.

If you simply want to connect to computers to each other, you might have the cable go directly from one computer to the other. But what do you do if you wish to connect more than one computer? What if you have 100 computers you need to connect on a network? There are three devices that can help you to accomplish this task: the hub, switch, and router. These use cat-5 or cat-6 cable, with RJ 45 connectors.

## The Hub

The simplest connection device is the **hub**. A hub is a small box-shaped electronic device, into which you can plug-in network cables. It will have four or more (commonly up to 24) RJ 45 jacks, each called a port. A hub can connect as many computers as it has ports (for example, an 8-port hub can connect 8 computers). You can also connect one hub to another; this strategy is referred to as “stacking” hubs. Hubs are quite inexpensive and simple; just plug the cable in. However, hubs have a downside. If you send a packet from one computer to another, a copy of that packet is actually sent out from every port on the hub. These copies can lead to a lot of unnecessary network traffic. This situation is due to the fact that the hub, being a very simple device, has no way of knowing where a packet is supposed to go. Therefore it simply sends copies of the packet out all of its ports.

## The Switch

The next device to consider is the **switch**. A switch is basically an intelligent hub. A switch works and looks exactly like a hub, with one significant difference. When it receives a packet, it will send that packet only out the port it needs to go out. A switch is essentially a hub that is able to determine where a packet is being sent.

## The Router

Finally, if you wish to connect two or more networks together, you use a **router**. A router is similar in concept to a hub or switch, as it does relay packets; but it is far more sophisticated. You can program most routers and control how they relay packets. Also, unlike using a hub or switch, the two networks connected by a router are still separate networks. So the three basic connection devices are the hub, switch, and router. All of which connect category 5 or category 6 cable, using RJ 45 connectors.

## Connection Speeds

This explains the connections between computers on a local network, but surely there are faster connection methods? Well there are. In fact your internet service provider, or your company probably has a much faster connection to the internet. Table 2-2 summarizes the most common connection types and their speeds.

Table 2-2

Connection Types

Connection Type	Speed	Details
DS0	64 kilobits per second	Standard phone line.
ISDN	128 kilobits per second	2 DS0 lines working together to provide a high-speed data connection.
T1	1.54 megabits per second	24 DS0 lines working as one. Whereas 23 carry data, one carries information about the other lines. This type of connection is becoming common for schools and businesses.
T3	43.2 megabits per second	672 DS0 lines working together. This method is the equivalent of 28 T1 lines.
OC3	155 megabits per second	All OC lines are optical and do not use traditional phone lines. OC3 lines are quite fast and very expensive. They are often found at telecommunications companies.
OC12	622 megabits per second	The equivalent of 336 T1 lines, or 8064

		phone lines.
OC48	2.5 gigabits per second	The equivalent of 4 OC12 lines.

It is common to find speeds up to T1 lines in many locations. A cable modem can sometimes achieve speeds comparable to a T1 line. You are not likely to encounter the OC lines unless you work in telecommunications.

### ***Data Transmission***

We've seen, briefly, the physical connection methods; but how is data actually transmitted? To transmit data, a **packet** is sent. The basic purpose of cable is to transmit packets from one machine to another. It does not matter whether that packet is a part of a document, video, an image, or just some internal signal from one computer to another. This fact begs the question: What, exactly, is a packet? As you probably know, everything in a computer is ultimately stored as one's and zeros, called bits. These ones and zeros are grouped into groups of 8 bits, called a byte. A packet is a certain number of bytes divided into a header and a body. The header is a twenty bytes at the beginning that explain the packet. The header tells you where the packet is coming from, where it is going, what type of packet it is and more. The body contains the actual data, in binary format, that you wish to send. The aforementioned routers and switches work by reading the header portion of any packets that come to them. This process is how they can determine where the packet should be sent to.

### **Protocols**

There are different types of communications, for different purposes. The different types of network communications are called **protocols**. A protocol is, essentially, an agreed-upon method of communications. In fact, this definition is exactly how the word "protocol" is used in

standard, non-computer usage. Each protocol has a specific purpose and normally operates on a certain port (more on ports in a bit). Some of the most important protocols are listed in Table 2-3.

Table 2-3

Protocols

<b>Protocol</b>	<b>Purpose</b>	<b>Port</b>
FTP (File Transfer Protocol)	For transferring files between computers.	20 & 21
SSH	Secure Shell. A secure/encrypted way to transfer files	22
Telnet	Used to remotely log-on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators.	23
SMTP (Simple Mail Transfer Protocol)	Sends email.	25
WhoIS	A command that queries a target IP address for information.	43
DNS (Domain Name Service)	Translates URL's into web addresses.	53
tFTP (Trivial File Transfer Protocol)	A quicker, but less reliable, form of FTP.	69
HTTP (Hypertext Transfer Protocol)	Displays web pages.	80
POP3 (Post Office Protocol Version 3)	Retrieves email.	110

NNTP (Network News Transfer Protocol)	Used for network news groups (usenet newsgroups). You can access these groups over the web via <a href="http://www.google.com">www.google.com</a> by selecting the “groups” tab.	119
NetBIOS	An older Microsoft protocol that is for naming systems on a local network.	137, 138, 139
IRC (Internet Relay Chat)	Chat Rooms.	194
HTTPS (Hyper Text Transfer Protocol Secure)	HTTP encrypted with SSL or TLS	443
SMB (Server Message Block)	This is used by Microsoft Active Directory	445
ICMP (Internet Control Message Protocol)	These are simply packets that contain error messages, informational messages, and control messages.	no specific port

You should note that this list is not complete. There are dozens of other protocols; but for now these will suffice. All of these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol). The most important thing for you to realize is that the communication on networks takes place via packets, and those packets are transmitted according to certain protocols, depending on the type of communication that is occurring. You may be wondering what a port is. Don't confuse this type of port with the connections on the back of your computer, such as a serial port or parallel port. A port in networking terms is a handle, a connection point. It is a numeric designation for a particular pathway of communications. All network communication, regardless of the port used, comes into your

computer via the connection on your Network Interface Card (NIC). You might think of a port as a channel on your TV. You probably have one cable coming into your TV but you can view many channels. You have one cable coming into your computer, but you can communicate on many different ports.

So the picture we've drawn so far of networks is one of machines connected to each other via cables, and perhaps to hubs/switches/or routers. Networks transmit binary information in packets using certain protocols and ports. So that is an accurate picture of network communications, albeit a simple one.

## **How the Internet Works**

Now that you have a basic idea of how computers communicate with each other over a network, it is time to discuss how the internet works. The internet is essentially just a large number of networks that are connected to each other. Therefore the internet works exactly the same way as your local network. It sends the same sort of data packets, using the same protocols. These various networks are simply connected into main transmission lines called backbones. The points where the backbones connect to each other are called **Network Access Points** (NAP). When you log-on to the internet, you probably use an **Internet Service Provider** (ISP). That ISP has a connection either to the internet backbone, or to yet another provider who has a backbone. So basically, logging on to the internet is a process of connecting your computer to your ISP's network, which is, in turn, connected to one of the backbones on the internet.

## ***IP Addresses***

With tens of thousands of networks and millions of individual computers communicating and sending data, a predictable problem arises. That problem is ensuring that the data packets go to the correct computer. This task is accomplished in much the same way as traditional "snail"

letter mail service is delivered to the right person: via an address. With network communications, this address is a special one, referred to as an “IP” address. For now we will only discuss the most common type of IP address in use today, that is IPv4. We won’t be discussing IPv6.

An IP address is a series of four, three-digit numbers, separated by periods. (An example would be 107.22.98.198.) Each of the three-digit numbers must be between 0 and 255. So you can see that an address of 107.22.98.466 would not be a valid one. The reason for this rule is that these addresses are actually four binary numbers; you just see them in decimal format. Recall that a byte is 8 bits (1’s and 0’s), and an 8-bit binary number converted to decimal format will be between 0 and 255. So you don’t have to do the math yourself; I will tell you that this rule means there are a total of over 4.2 billion possible IP addresses.

You should not be concerned that we are likely to run out of new IP addresses soon. There are methods in place already to extend the use of addresses. The IP addresses come in two groups: public and private. The public IP addresses are for computers connected to the internet. No two public IP address can be the same. However, a private IP address, such as one on a private company network, only has to be unique in that network. It does not matter if other computers in the world have the same IP address, because this computer is never connected to those other worldwide computers. Often network administrators use private IP addresses that begin with a 10, such as 10.102.230.17. The other private IP addresses are 172.16.0.0 - 172.31.255.255 and 192.168.0.0 - 192.168.255.255.

It should also be pointed out that often an ISP will buy a pool of public IP addresses and assign them to you when you log on. So, an ISP might own 1000 public IP address, and have 10,000 customers. Because all 10,000 customers will not be online at the same time, the ISP

simply assigns an IP address to a customer when he or she logs on, and the ISP un-assigns the IP address when the customer logs off.

The address of a computer tells you a lot about that computer. The first byte (or the first decimal number) in an address tells you to what class of network that machine belongs. Table 2-4 summarizes the five network classes.

Table 2-4

Network Classes

<b>Class</b>	<b>IP Range for the First Byte</b>	<b>Use</b>
A	0-126	Extremely large networks. No class A network IP addresses are left. All have been used.
B	128-191	Large corporate and government networks. All class B IP addresses have been used.
C	192-223	The most common group of IP addresses. Your ISP probably has a class C address.
D	224-247	These are reserved for multicasting.
E	248-255	Reserved for experimental use.

These five classes of networks will become more important should you decide to study networking on a deeper level. Observe the Table 2-4 carefully, and you probably will discover that the IP range of 127 was not listed. This omission is because that range is reserved for testing. The IP address of 127.0.0.1 designates the machine you are on, regardless of that machine's assigned IP address. This address is often referred to as the *loop back address*. That

address will be used often in testing your machine and your NIC. We will examine its use a bit later in this document, in the section on network utilities.

This discussion of IP addresses is based on IP V4, the current standard. However it should be noted that IP V6 is likely to be implemented in the future. Rather than 32-bit addresses (4 8-bit numbers), the IP V6 uses 128-bit addresses. IP V6 is configured for backward compatibility. That phrase means that to use the new IP version 6.0, there fortunately will not be a need to change every IP address in the world. Keep in mind that when we discuss the packet structure of an IP packet, we are talking about both the IP V4 and the IP V6 packets. In comparison to IP V4 packets, IP V6 packets have longer header segments, and the IP V6 header is structured a little differently.

### ***Uniform Resource Locators***

After you connect to your ISP, you will of course want to visit some websites. You probably type names into your browser's address bar, rather than IP addresses. For example, you might type in `www.chuckeasttom.com` to go my website. Your computer, or your ISP, must translate the name you typed in [called a **Uniform Resource Locator (URL)**], into an IP address. The DNS protocol, mentioned in the Table 2-3, handles this translation process. So you are typing in a name that makes sense to humans, but your computer is using a corresponding IP address to connect. If that address is found, your browser sends a packet (using the HTTP protocol) to port 80. If that target computer has software that listens and responds to such requests (like a web-server software such as Apache or Microsoft Internet Information Server), then the target computer will respond to your browser's request and communication will be established. This method is how web pages are viewed. If you have ever received an Error 404: File Not Found, what you're seeing is that your browser received back a packet (from the web server) with error

code 404, denoting that the web page you requested could not be found. There are a series of error messages that the web server can send back to your web browser, indicating different situations. Many of these problems the browser handles itself, and you never see the error message. All error messages in the 400 series are client errors. That term means something is wrong on your side, not the web server. Messages in the 500 series are server errors; that term means there is a problem on the web server. The 100-series messages are simply informational; 200-series messages indicate success (you usually do not see these, the browser simply processes them); and 300-series messages are re-directional, meaning the web page you are seeking has moved and your browser is then directed to the new location.

Email works the same way as visiting websites. Your email client will seek out the address of your email server. Then your email client will use either POP3 to retrieve your incoming email, or SMTP to send your outgoing email. Your email server (probably at your ISP or your company) will then try to resolve the address you are sending to. If you send something to `chuckeasttom@yahoo.com`, your email server will translate that email address that into an IP address for the email server at yahoo.com; and then your server will send your email there. Note that there are newer email protocols out; however, POP3 is still the most commonly used.

Many readers are probably familiar with chat rooms. A chat room works with packets. You first find the address of the chat room, then you connect. Your computer's chat software is sending packets back and forth. Remember that a packet has a header section, and that header section contains your IP address and the destination IP address that you are going to, as well as other information. Obviously there are more details to packet structure, but this is the basic overview.

## **History of the Internet**

At this point, you should have a basic understanding of how networks and the internet work. You should have some idea about IP addresses, protocols, and packets. With your current knowledge, it would be a good time to give you a brief tour of the history of the internet. Many readers will find this overview will help them put all of the material learned thus far into historical perspective.

The internet traces its roots to the Cold War. One positive thing that can be said about the Cold War, was that it was a time of significant investment in science and technology. In 1957, after the Soviet Union launched the Sputnik satellite, the U.S. government formed the Advanced Research Projects Agency (ARPA) within the Defense Department. ARPA's sole purpose was to fund and facilitate research into technology. Obviously this aim would include weapons technology, but the total focus would also include communications technology.

In 1962 a study by the Rand Corporation proposed devising a communication method wherein data was sent in packets between locations. If a packet was lost, the originator of the message would automatically resend the message. This idea was a precursor to the internet communication methodologies that would eventually arise.

In 1968 ARPA commissioned the construction of ARPANET, a simple internet web of four points (called nodes): UCLA, Stanford, UC Berkley, and the University of Utah. Although no one knew it at the time, this small web was the birth of what would become the internet. At this point, ARPANET had only these four nodes connected.

The year 1972 was a milestone for the development of the internet, in more than one sense. That year ARPA was renamed "DARPA," the Defense Advanced Research Projects Agency. Also that year, Ray Tomlinson invented the first email program. At this point, four years after the birth of ARPANET, only 23 hosts were on the network. (A "host" is a machine

with data on it, that you can connect to. For example, a web server, or email server, is a host) The following year, 1973, would mark the birth of the TCP/IP protocol, which allowed the various computers to communicate in a uniform fashion, regardless of their hardware or operating system.

In 1974, a man named Vince Cerf published a paper on the TCP protocol and, for the first time in computer history, used the term *internet*. In 1976 Ethernet cable was developed (the same cabling we use today) and DARPA began to require the use of TCP/IP protocol on its network. This year also marked the beginning of widespread distribution of the Unix operating system. The development of Unix and the internet would go hand-in-hand for many years to come. By this time, eight years after the birth of ARPANET, there were only 111 hosts on the network.

In 1979 a major development occurred: the birth of USENET newsgroups. These groups are essentially bulletin boards open to the entire world. Today you can access these groups via newsgroup reader software, or via the web through [www.google.com](http://www.google.com) (and then by selecting “groups”). There are thousands of newsgroups devoted to every topic imaginable. Just two years later the National Science Foundation (NSF) created CSNET for universities and research centers that were not part of ARPANET. That same year Cerf proposed connecting CSNET and ARPANET. By 1981, the University of Wisconsin had created DNS (Domain Name System) so that people could find nodes on the network via a name rather than the actual IP address. At this point there were 562 hosts on the network.

The early 1980s saw enormous growth in the early internet. DARPA divided its ARPANET into military and non-military segments, thus allowing more people to use the non-military segment. The National Science Foundation introduced the T1 line (a very fast connection). In 1986 the Internet Engineering Task Force (IETF) was formed to oversee the

creation of standards for the internet and internet protocols. By this time, the internet consisted of 2,308 hosts.

A pivotal year for internet development turned out to be 1990. That year Tim Berners-Lee, working at CERN laboratories in Europe, developed the hypertext transfer protocol and gave the world its very first web pages. Via the http protocol and the hypertext markup language (HTML), people could publish ideas on the internet for anyone (with a connection) to view. By 1990 there were over 300,000 hosts on the internet. (Fast-forward to 2004; Tim Berners-Lee receives the first Millennium Prize for contributions to technology. He is widely regarded as the father of the world-wide web.)

Internet growth and activity exploded in the 1990s. In 1992, CERN released the invention of web pages to the world at-large. In 1993, the first graphical web browser, named “Mosaic,” was invented. By 1994, Pizza Hut began taking orders via web pages. The internet has continued to grow; today there are millions of web pages around the world. Everyone has a web page, from university departments, government agencies, corporations, schools, religions, and virtually any group you can imagine. Many of you will use web pages for banking, shopping, information, and entertainment. You likely will use email (by the way, I primarily use email for communication, so that is the best way to contact me if you wish: [chuckeasttom@yahoo.com](mailto:chuckeasttom@yahoo.com)). The internet has become a virtual “living level” of interaction in our society. What company does not have a website? What movie release does not have a website? What political candidate does not have a website? In just over three decades the internet has become an integral part of our society.

## **Basic Network Utilities**

There are network utilities that you can execute from a command prompt (Windows) or from a shell (Unix/Linux). Many readers are already familiar with Windows, so the text's discussion will execute the commands and discuss them from the Windows command-prompt perspective. However, it must be stressed that these utilities are available in all operating systems. In this section, you will read about IPConfig, ping, and tracert utilities.

## ***IPConfig***

The first thing you will want to do is to get information about your own system. To accomplish this fact-finding mission, you will need to get a command prompt. In Windows XP, you do this by going to the start menu, selecting "all programs," then choosing "accessories." You will then see an option called "command prompt." (For Windows 2000 users the process is identical, except the first option is simply called "programs" rather than "all programs.") Now you can type in ipconfig. (You could input the same command in Unix or Linux by typing in ifconfig from the shell.) After typing in ipconfig (ifconfig in Linux), you should see something much like what is shown here:

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\chuck>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Wireless LAN adapter Wireless Network Connection:
    Connection-specific DNS Suffix  . : gateway.2wire.net
    Link-local IPv6 Address . . . . . : fe80::2dff:c9b4:92ca:9b43%11
    IPv4 Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Ethernet adapter VirtualBox Host-Only Network:
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::851e:deca:6578:af54%49
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Tunnel adapter isatap.gateway.2wire.net:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Tunnel adapter Reusable ISATAP Interface {15831C80-8547-4DBC-A5E7-160479674F9B}:
    Media State . . . . . : Media disconnected
```

This command gives you some information about your connection to a network (or to the internet). Most importantly you find out your own IP address. The command also has the IP address for your default gateway, which is your connection to the outside world. Running the IPConfig command is a first step in determining your system's network configuration. Most commands this text will mention, including IPConfig, have a number of parameters, or flags, that can be passed to the commands to make the computer behave in a certain way. You can find out what these commands are by typing in the command, followed by a space, and then typing in hyphen question mark, `-?`. That is shown here:

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\chuck>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:
    Connection-specific DNS Suffix  . : gateway.2wire.net
    Link-local IPv6 Address . . . . . : fe80::2dff:c9b4:92ca:9b43%11
    IPv4 Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::851e:deca:6578:af54%49
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Tunnel adapter isatap.gateway.2wire.net:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter Reusable ISATAP Interface {15831C80-8547-4DBC-A5E7-160479674F9B}:
    Media State . . . . . : Media disconnected
```

As you can see, there a number of options you might use to find out different details about your computer's configuration. The most commonly used method would probably be the IPConfig/all, shown here:

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\chuck>ipconfig /all

Windows IP Configuration

Host Name . . . . . : ChucksPC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : gateway.2wire.net

Wireless LAN adapter Wireless Network Connection 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Virtual WiFi Miniport Adapter
Physical Address. . . . . : 00-21-5D-69-2B-79
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . . . . . : gateway.2wire.net
Description . . . . . : Intel(R) WiFi Link 5100 AGN
Physical Address. . . . . : 00-21-5D-69-2B-78
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2dff:c9b4:92ca:9b43%11(Preferred)
IPv4 Address. . . . . : 192.168.1.101(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 22, 2010 7:51:22 AM
Lease Expires . . . . . : Tuesday, November 23, 2010 7:51:22 AM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 268441322
DHCPv6 Client DUID. . . . . : 00-01-00-01-10-81-97-A6-00-E0-B8-FD-A5-8F
DNS Servers . . . . . : 192.168.1.254
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Local Area Connection:

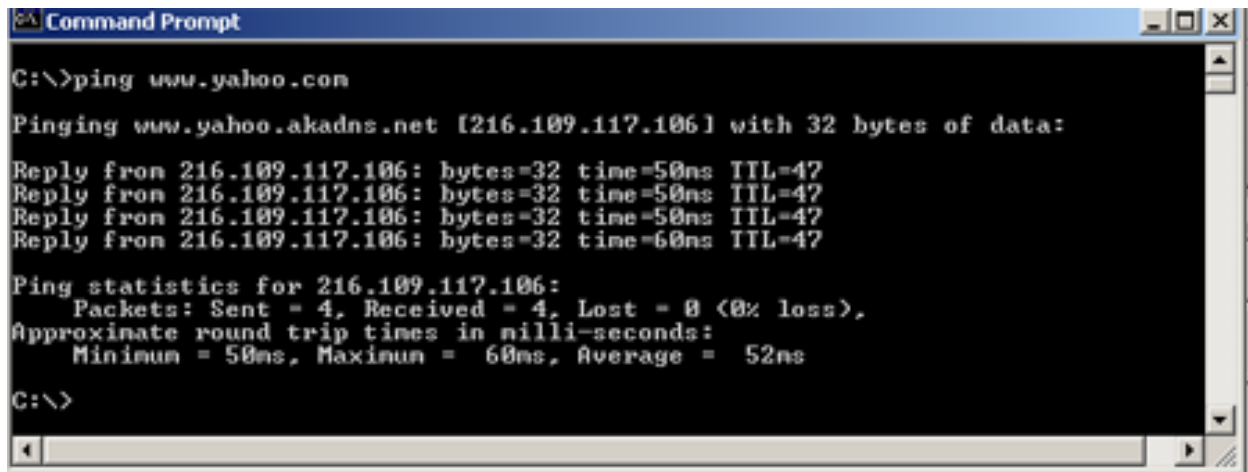
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Marvell Yukon 88E8057 PCI-E Gigabit Ether
Physical Address. . . . . : 00-E0-B8-FD-A5-8F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:
```

You can see that this option gives you much more information. For example, IPConfig/all gives the name of your computer, when your computer obtained its IP address, and more.

## **Ping**

Another commonly used command is ping. Ping is used to send a test packet, or echo packet, to a machine to find out if the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be employed in elementary hacking techniques. The command is shown here:

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The command prompt shows the following text:

```
C:\>ping www.yahoo.com
Pinging www.yahoo.akadns.net [216.109.117.106] with 32 bytes of data:
Reply from 216.109.117.106: bytes=32 time=50ms TTL=47
Reply from 216.109.117.106: bytes=32 time=50ms TTL=47
Reply from 216.109.117.106: bytes=32 time=50ms TTL=47
Reply from 216.109.117.106: bytes=32 time=60ms TTL=47

Ping statistics for 216.109.117.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 60ms, Average = 52ms

C:\>
```

This figure tells you that a 32-byte echo packet was sent to the destination and returned. The ttl item means “time to live.” That time unit is how many intermediary steps, or hops, the packet should take to the destination before giving up. Remember that the internet is a vast conglomerate of interconnected networks. Your packet probably won’t go straight to its destination. It will have to take several hops to get there. As with IPConfig, you can type in ping -? to find out various ways you can refine your ping.

## ***Tracert***

The final command we will examine in this document is the tracert. This command is a sort-of ping “deluxe.” Tracert not only tells you if the packet got there and how long it took, but also it tells you all the intermediate hops it took to get there. This same command can be executed in Linux or Unix, but there it is called “traceroute” rather than “tracert.”) You can see this utility [here](#):

```
Command Prompt
4    50 ns    60 ns    40 ns    172.24.217.1
5    60 ns    60 ns    70 ns    10.238.254.6
6    40 ns    50 ns    41 ns    ndf16-gsr12-1-gig-7-0.nyc2.attens.net [63.240.0.
237]
7    40 ns    40 ns    40 ns    ndf16-gsr12-1-gig-7-0.nyc2.attens.net [63.240.0.
237]
8    50 ns    40 ns    70 ns    gar3-p320.n54ny.ip.att.net [12.122.255.209]
9    40 ns    51 ns    50 ns    gbr6-p90.n54ny.ip.att.net [12.123.1.190]
10   60 ns    40 ns    60 ns    tbr1-p012401.n54ny.ip.att.net [12.122.11.13]
11   40 ns    50 ns    50 ns    ggr2-p300.n54ny.ip.att.net [12.123.3.58]
12   40 ns    50 ns    40 ns    att-gv.ny.cv.net [192.205.32.198]
13   50 ns    50 ns    81 ns    dcr1-loopback.Washington.cv.net [206.24.226.99]

14   50 ns    50 ns    50 ns    bhr1-pos-10-0.Sterling2dc3.cv.net [206.24.238.38
]
15   50 ns    50 ns    60 ns    csr11-ve242.Sterling2dc3.cv.net [216.109.66.99]

16   50 ns    50 ns    50 ns    216.109.84.162
17   50 ns    60 ns    50 ns    v131.bas2-m.dcn.yahoo.com [216.109.120.146]
18   50 ns    60 ns    50 ns    p20.www.dcn.yahoo.com [216.109.117.207]

Trace complete.
C:\>
```

With `tracert`, you can see (in milliseconds) the IP addresses of each intermediate step listed, and how long it took to get to that step. Knowing the steps required to reach a destination can be very important.

Certainly there are other utilities that can be of use to you when working with network communications. However the three we just examined are the core utilities. These three (`IPConfig`, `ping`, and `tracert`) are absolutely essential to any network administrator, and you can commit them to memory.

## Other Network Devices

There are other devices that work to protect your computer from the outside world. The two most common devices in this category are the firewall and the proxy server. A firewall is essentially a barrier between your network and the rest of the internet. A personal computer (pc) can be used as a firewall; or in many cases, a special router can function as a firewall. Firewalls use different techniques to protect your network, but the most common strategy is packet filtering. In a packet-filtering firewall, each incoming packet is examined. Only those packets that match the

criteria you set are allowed through. (Commonly only packets using certain types of protocols are allowed through.) Many operating systems, such as Windows XP and many Linux distributions, include basic packet-filtering software with the operating system.

The second very common type of defensive device is a proxy server. A proxy server will almost always be another computer. You might see the same machine used as both a proxy server and a firewall. A proxy server's purpose is quite simple: it hides all of your network from the outside world. People trying to investigate your network from the outside will see only the proxy server. They will not see the actual machines on your network. When packets go out of your network, their headers are changed so that the packets have the return address of the proxy server. Conversely, the only way you can access the outside world is via the proxy server. A proxy server combined with a firewall is basic network security. It would frankly be negligent to ever run a network that did not have a firewall.

There are many other security devices such as Intrusion Detection Systems and Honeypots, but you will learn about those in any of my security courses.

## **Advanced Topics**

Time for some advanced topics—So make sure you fully understand the preceding material before you proceed into this section. The information presented in this section will give you a broader understanding of networks in general. If you have any intention of delving into network security on a professional level then you will need this information, and probably much more.

### ***The OSI Model***

Let's begin with the OSI model, or **Open Systems Interconnect** model (Table 2-5). This model describes how networks communicate. It describes the various protocols and activities, and it tells how the protocols and activities relate to each other. This model is divided into seven

layers. It was originally developed by the International Standards Organization (ISO) in the 1980s.

Table 2-5 The OSI Model

Layer	Description	Protocols
Application	This layer interfaces directly to and performs common application services for the application processes.	
Presentation	The presentation layer relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems.	POP, SMTP, DNS, FTP, Telnet
Session	The session layer provides the mechanism for managing the dialogue between end-user application processes.	NetBIOS
Transport	This layer provides end-to-end communication control.	TCP
Network	This layer routes the information in the network.	IP, ARP, ICMP
Data Link	This layer describes the logical organization of data bits transmitted on a particular medium. Data Link is divided into two sublayers: the Media Access Control layer (MAC) and the Logical Link Control layer (LLC).	SLIP, PPP
Physical	This layer describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals. In other words, the physical layer is the actual NIC, Ethernet cable, and so forth.	None

Many networking students memorize this model. It's good to at least memorize the names of the seven layers and to understand basically what they each do. From a security perspective, the more you understand about network communications, the more sophisticated your defense can be. The most important thing for you to understand is that this model describes a hierarchy of communication. One layer will only communicate with the layer directly above it, or below it.

## **MAC Addresses**

**MAC addresses** are an interesting topic. (You might notice that MAC is also a sublayer of the data link layer of the OSI model.) A MAC address is a unique address for an NIC. Every NIC in the world has a unique address that is represented by a six-byte hexadecimal number. There is a protocol that is used to convert IP addresses to MAC addresses. This protocol is the Address Resolution Protocol, or ARP. So when you type in a web address, the DNS protocol is used to translate that into an IP address. Then the ARP protocol will translate that IP address into a specific MAC address of an individual NIC.

This brings us to how DNS is accomplished; or rather, how does a URL get translated into an IP address? How does the computer know what IP goes with what URL? There are servers set up just to do this task. They are called DNS servers. If you are on a corporate network you probably have a DNS server on your network. If not, then your ISP has one. These servers maintain a table of IP-to-URL entries. From time to time there are transfers of DNS data, called Zone Transfers, that allow one DNS server to send its changes to another. Across the internet there are root DNS servers that are maintained with centralized data for all registered URL/IP addresses.