

Staying Safe on the Internet

John Lortz (jlortz@shf.org) and Susan Leavitt (sleavitt@shf.org)
Senior Health Foundation (www.shf.org)

Introduction

Without a doubt, the Internet is vast and fascinating place that provides information and resources on every imaginable topic and lets you quickly and easily communicate with family and friends. For many, it's hard to imagine life without the Internet. But as you come to understand the more you use it, the Internet does have a dark side. Yes, there are undesirable places you probably don't want to visit, but the dark side we're referring to here come in the form of outside intrusion, loss of privacy, and just plain nuisances we could certainly do without.

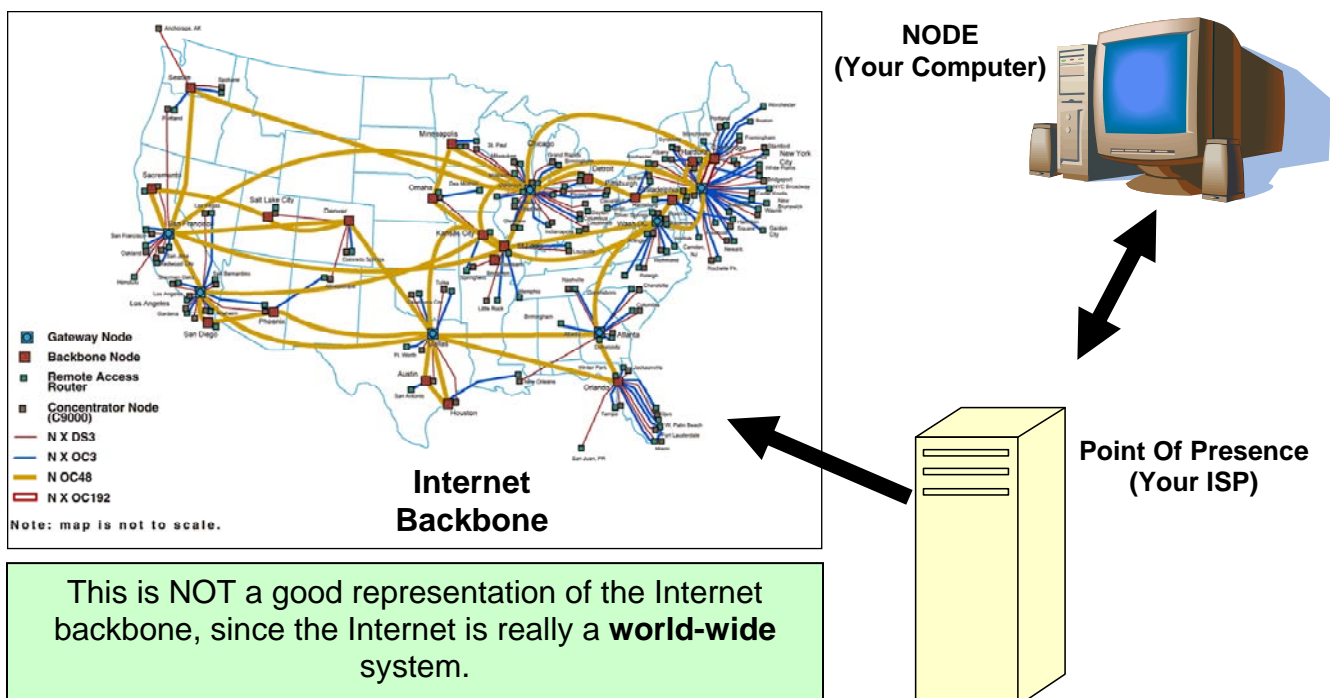
In this booklet we'll help you understand the threats you encounter on the Internet, where they might come from, and what you can do to protect your computer from them. Along the way, you'll also learn a bit more about how the Internet works, so that you can fully understand why protecting yourself is important.

Understanding How the Internet Works

When you log your computer onto the Internet, your computer suddenly becomes connected to a vast web of interconnected computers that spans the world. To help you understand how your computer is vulnerable to attack while on this web, there are some basic facts you must first learn about your Internet Connection and how the Internet works.

The Physical Connection (Communication lines and hardware)

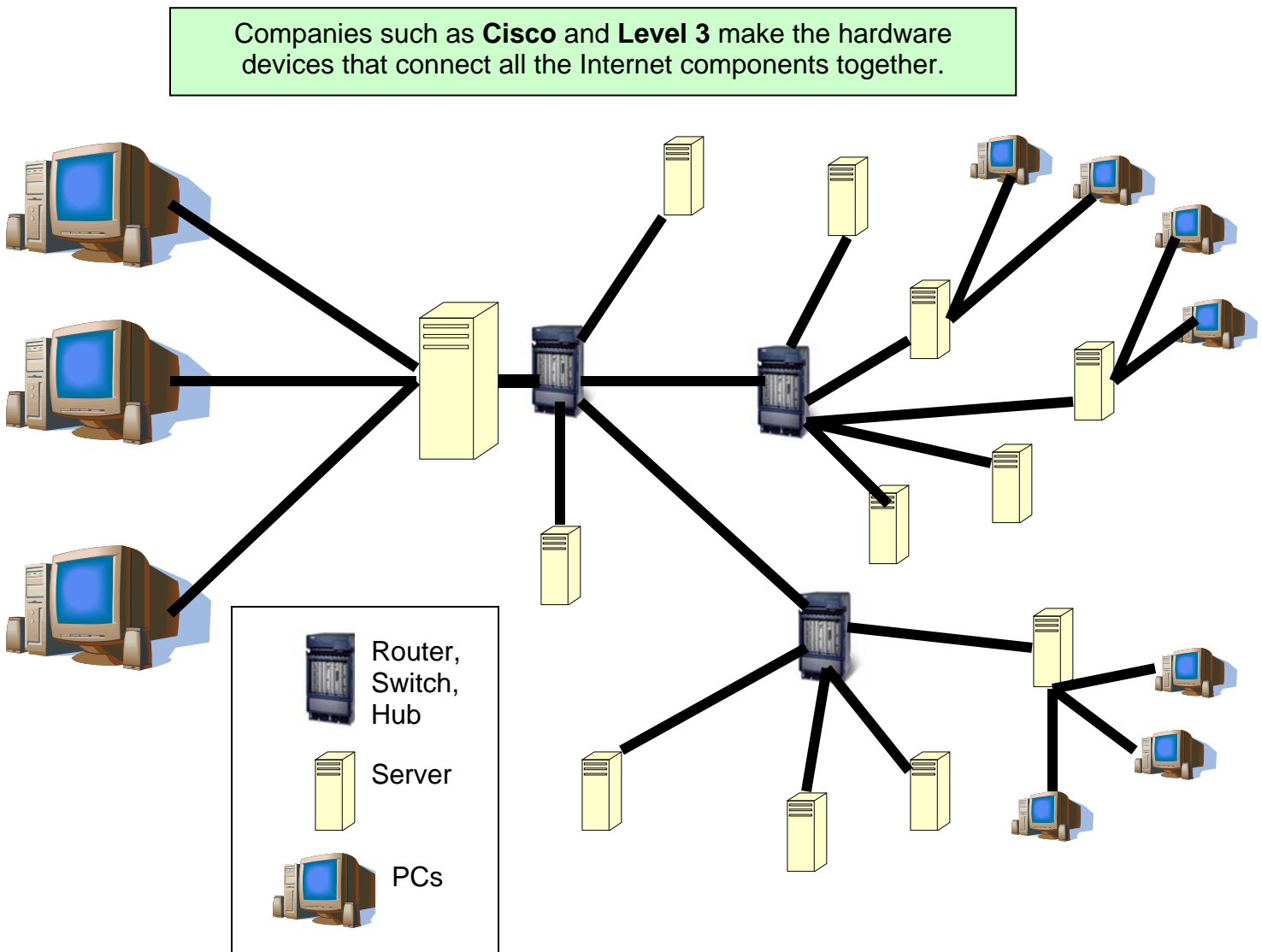
The Internet has a **Backbone** that consists of high-speed communication channels running across the country and around the world. The backbone is operated by private companies such as AT&T, Qwest, and @Home, and consists of underground lines, microwave transmissions, and satellites.



Where different Backbone channels meet, you have an Internet Exchange Point, or **Network Access Point (NAP)**. Some of these points are also called Metropolitan Area Exchanges (**MAE**). These points are owned and managed by private companies such as MCI WorldCom and Ameritech, and are what allows the various communication companies to share lines so that the network can cover the entire country and globe.

Individuals connect their computers to the Internet at **Points of Presence (PoPs)** which are maintained by **Internet Service Providers (ISP)**. We often call the individual computers, **nodes**.

Hardware and software devices such as **hubs**, **switches**, and **routers** are at the connecting points of all the various Internet communication lines. They allow a smooth and organized flow of information between all the smaller networks of computers on the Internet.



When you connect to the Internet, your computer becomes part of this vast network. However, unlike the computers that actually make up the Internet (called **servers** or **hosts**), your computer can NOT be accessed by others who are connected. In this way, **your connection is really a one-way street** where you can go out to the servers and get information, but nothing can come back to your computer unless you ask for it. **At least, this is the way it's SUPPOSE to work.**

The Software that Makes the Hardware Connection Work

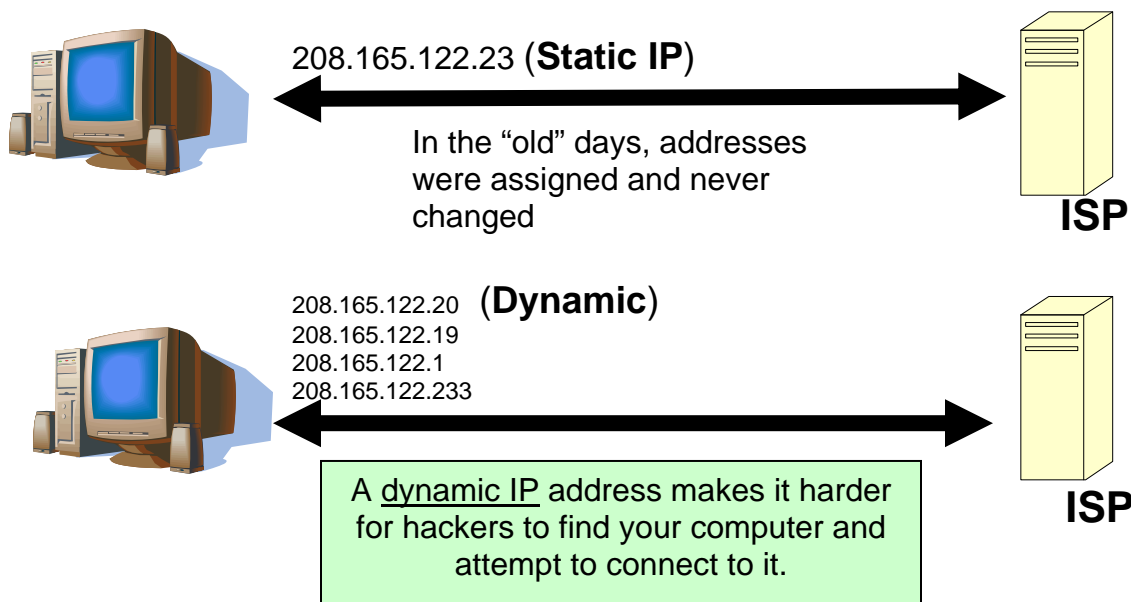
Now that you've seen how all these computers are connected, let's talk about what really makes the connection work. As part of Microsoft Windows on your computer, and as part of the operating system on the Internet servers, there is special **software that let's one computer talk to another**. We sometimes refer to these programs as "**protocols**", which simply means they are rules that each computer must follow so they can communicate with each other.

The Internet Protocol - The main protocol of the Internet is called **TCP / IP** (Transmission Control Protocol / Internet Protocol). TCP/IP is really two protocols that work together to let Internet communication take place.

Addresses on the Internet - So that all the computers on the Internet can communicate with each other, each computer that is connected to the Internet has an **IP Address**, which is a series of numbers that looks like this: 208.164.129.115

Your computer's IP address is assigned by your Internet provider, who has a large block of addresses it can give out. Most Internet providers assign your address **dynamically**, meaning that it's automatically assigned each time you connect through a dial-up connection, or for broadband (cable and DSL), assigned and re-assigned at various times throughout the day or week.

A big reason that your provider assigns addresses dynamically (which also means you get a different address each time one is assigned), is for your protection. With a constantly changing address, there is a reduced chance for Internet intruders to find your computer and attempt to access it.



Try This: Choose Start / Run, type in **command**, and click OK. This opens a command window. At the flashing prompt, type **IPCONFIG** (for Windows XP) or **WINIPCFG** (for Windows 98/ME) and press ENTER. You should see your current IP address displayed.

Also Try This: At the same prompt, type **ping www.yahoo.com** and press ENTER. This causes your computer to send out 4 short signals to Yahoo, which should answer. If you get no answer, your are not connected to the Internet. Pinging is a way to test Internet connections, or test to see if an Internet server is up and running. Also notice that Yahoo has an IP address, just like all other computers on the Internet. When you are finished, type **exit** and press ENTER.

```
C:\WINDOWS\system32\command.com
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Network Bridge <Network Bridge> 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 192.168.10.18
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.10.1

C:\>
```

```
C:\WINDOWS\system32\command.com
C:\>ping www.yahoo.com

Pinging www.yahoo.akadns.net [68.142.197.67] with 32 bytes:

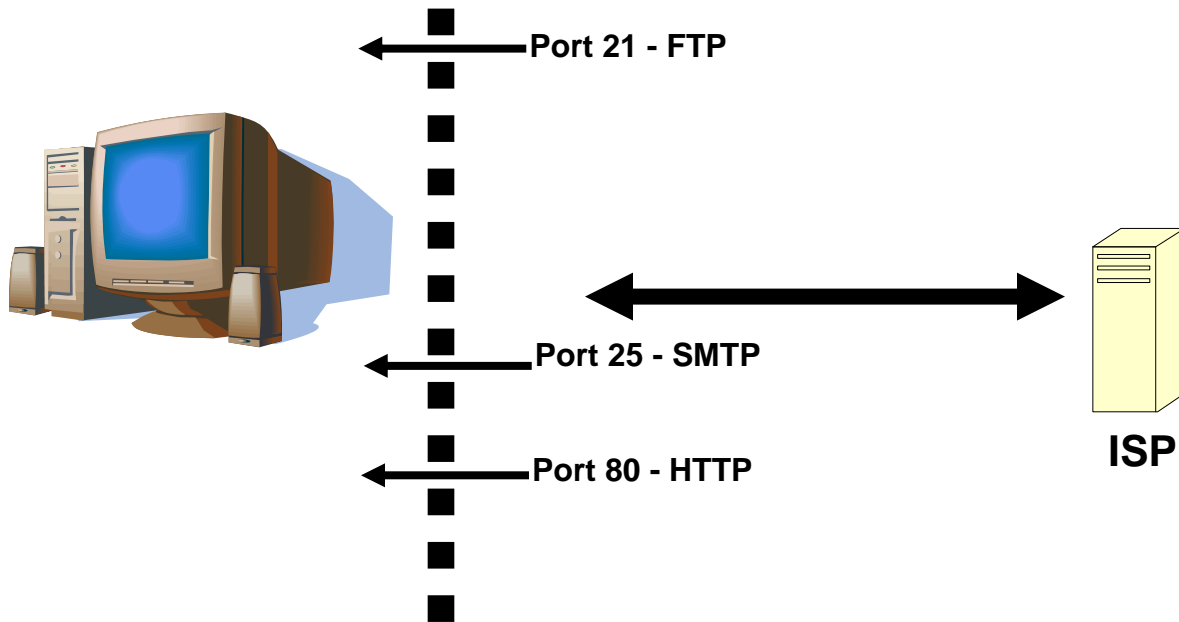
Reply from 68.142.197.67: bytes=32 time=44ms TTL=51
Reply from 68.142.197.67: bytes=32 time=43ms TTL=51
Reply from 68.142.197.67: bytes=32 time=50ms TTL=51
Reply from 68.142.197.67: bytes=32 time=43ms TTL=52

Ping statistics for 68.142.197.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 50ms, Average = 45ms

C:\>
```

The Ports on Your Computer – In addition to TCP / IP and your IP address, there's one more software component we need to discuss with regards to your Internet connection. Each time you connect to the Internet and perform a specific task, such as browse to a Web page, send an E-mail, or download a file, your communication with the Internet takes place through one of thousands of different **ports**, which are assigned a number from 1 to 65535.

The ports we are referring to here are NOT the plugs on the back of your computer (although these also are called ports), instead, these ports are small communication opens in the Windows software that let signals pass back and forth. Each port has a very specific type of communication it lets through and no other. For example, **port 21** is only used for download files (File Transfer Protocol), **port 25** is only used for sending e-mail (Simple Mail Transfer Protocol), and **port 80** is used for Web pages (HyperText Transfer Protocol).



There are lots of places you can visit on the Internet, to see a list of the common port numbers and what they are for. Here are a few we especially like:

- www.portsdb.org/PortsDB/services
- www.neohapsis.com/neolabs/neo-ports/

Try This: Choose Start / Run, type in **command**, and click OK. This opens a command window. At the flashing prompt, type **netstat -an**. You should see a list of TCP ports that are open and listening for communications.

```

C:\WINDOWS\system32\command.com
C:\>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING
TCP   0.0.0.0:445             0.0.0.0:0               LISTENING
TCP   0.0.0.0:2967            0.0.0.0:0               LISTENING
TCP   127.0.0.1:1074          0.0.0.0:0               LISTENING
TCP   127.0.0.1:1476          127.0.0.1:1476          ESTABLISHED
TCP   127.0.0.1:1477          127.0.0.1:1476          ESTABLISHED
TCP   192.168.10.18:139       0.0.0.0:0               LISTENING
TCP   192.168.10.18:445       192.168.10.55:4042      ESTABLISHED
UDP   0.0.0.0:445             *:*:
UDP   0.0.0.0:500             *:*:
UDP   0.0.0.0:1025            *:*:
UDP   0.0.0.0:1026            *:*:
UDP   0.0.0.0:4500            *:*:

```