Networking 101

Data Communications Systems
Final Exam Study Guide

Professor Don Colton

IT 280 - Winter 2011
Brigham Young University Hawaii

Contents

Chapter 1

Introduction

Networking 101 is a college-level introduction to data communications and networking. It covers the information appropriate to an introductory one-semester (forty class hour) course in networking.

We focus on target skills, concepts, and topics that are normally expected of students who have passed such a course. We also cover the basic skills and concepts that support these target objectives.

This is a substantial departure from approaches that work from a historical aggregation of things that were taught since the early days of networking. It is, instead, a re-inventing of the subject matter, giving up some less useful topics in favor of things that are more relevant at the introductory level.

Please note that this booklet is currently (Feb 2011) under development, so new sections may appear and existing sections may be revised. Suggestions are welcome: email `doncolton2@gmail.com`

1.1 Target Skills

So, what **is** typically expected of students who have passed an introductory course in networking? What would your parents and friends expect you to know?

(a) Can you help me set up my home network? I don't understand all these settings.

(b) Can you help me set up my wireless home network? Does it matter if I

let my neighbors share it?

(c) Can you help me with all these firewalls and things? It sounds like a good thing, but it just seems to get in the way, especially when I am gaming.

(d) Can you help me share a printer with my roommates?

(e) Can you help me share documents and files with my family?

These target skills, sometimes called exit skills, are the skills that enable students overcome their own networking problems and to solve networking problems for others.

Skill: Home Router: Students should be able to properly set up a home router. This is covered in chapter 5 (page 32).

Skill: WiFi: Students should be able to properly set up wireless networking. This includes channel selection, wep/wpa, ssid, and antenna considerations. This is covered in chapter 6 (page 35).

Skill: Security: Students should know what security they have and whether they need more. Includes password selection, firewalls, and issues with opening up ports for gaming or whatever. Does sharing your WiFi put you in any danger? This is covered in chapter 7 (page 37).

Skill: Be The Server: Networks often involve the sharing of printer and files. This can be done by adding network-ready printer or storage. But often it is done by sharing parts of existing computer systems, such as their printer or hard drive. How this is done depends a lot on the operating system of the computer that will be doing the sharing.

We will address a few of these tasks in the context of Microsoft Windows. Specifically we will look at printer sharing, file sharing, and configuring ad hoc wireless networks. This is covered in chapter 8 (page 42).

1.2 Basic Skills

The target skills are things you **already know** you don't know. You want to learn them.

Most of the target skills cannot simply be memorized. Instead, they must be understood. Almost immediately basic concepts come up like domain names, WiFi network IDs, IP addresses, network masks, and ports.

The basic skills and concepts are those other things you have to learn first before you can be truly proficient in the target skills.

The basic skills are things you **didn't know** you would need to know. You may not know they even exist.

Skill: Networks: Students should understand the following concepts: IPv4 address, subnet mask, port, address classes ABC, MAC address, collision domains, what's a LAN, broadcast addresses. This is covered in chapter 2 (page 7).

Skill: Basic Concepts: Understand the following concepts: OSI 7-layer model, packets, frames, udp, tcp, arp, ports (21, 22, 25, 80, 443). I could have included this with Networks but I wanted the groupings to be of similar size and it was getting kind of big. This is covered in chapter 3 (page 26).

Skill: Power Tools: Students should be able to properly use these tools: speedtest.net, ping, traceroute, ipconfig, nmap, ssh, telnet, ftp, and wireshark. These are the tools of the trade and students should be either skilled or familiar with them. This is covered in chapter 4 (page 28).

1.3 Notation

The following notation is used freqently in this book to quickly identify important types of content.

Skill: This is a skill that should be acquired.
FYI: This is something that would be interesting or helpful to know, but you are not expected to memorize it.
Mem: This is something that should be memorized.

Q: This is a typical question that uses the skill.
A: This is a correct answer for the question just given
A? This is an explanation of how the answer could be derived.

Chapter 2

IPv4

For most people, the first exposure to the Internet comes in the form of a web browser. It is a living newspaper. It is a window into the library of the world. And it has its own cryptic way of finding content. It is called a URL.

The information itself lives on a server. A server is another computer, somewhere else in the world, that provides services to people like yourself. The URL is the browser's way of finding that server and requesting the content that you desire.

The **web** is a common name for the Internet. It refers specifically to that part of the Internet where web pages and web sites live.

The **Internet** includes the whole collection of all web sites and other services (of which there are many) that are connected together in a world-wide network of resources and components. It is much bigger than the web, but the web is its most familiar face.

2.1 The URL

URL, pronounced as three separate letters, like "you are ell," stands for Universal Resource Locator. Another common term is **URI**, for Universal Resource Identifier. URI is actually more technically correct, but somehow URL seems to roll off the lips easier and has become the defacto name for web addresses.

A URL consists of several parts. Let's look at one.

`http://doncolton.com/inet/book.pdf`

This URL is pretty standard. We will look at a more complicated one shortly.

`http:` is the protocol.

`doncolton.com` is the domain name.

`/inet/book.pdf` is the complete path.

2.1.1 Protocols

http is the protocol.

It is the language with which the browser will talk to the server. HTTP stands for Hyper Text Transport Protocol.

Other popular protocols you may see include these:

https: hyper text transport protocol with security.

mailto: email address (and possibly more).

ftp: file transport protocol.

2.1.2 Domain Names

`doncolton.com` is the domain name. It is intended to identify a specific computer that contains or has access to the resources you want.

There is a whole system of domain names. The most popular set is called the **dot com** domain names. These are used by nearly every business that has a presence on the Web.

Often domain names start with **www**, which stands for World Wide Web. It is not a requirement, but it is probably the most familiar way to introduce a URL, instead of saying "http://".

The actual way that computers are identified on the Internet is by way of something called an **IP address**. These are typically written as four numbers connected by dots. For example, `216.228.254.20` is the IP address of the computer that sits on my desk at the university where I teach.

We will talk much more about IP addresses, starting in section 2.2 (page 10) below.

Numbers are a fine way for computers to find each other, but humans like words instead. We see that in the numerous clever attempts to convert telephone numbers into words. Imagine 1-555-SAVE-NOW. Compare that to 1-555-728-3669. Which one do you think is easier to remember? For me it is easier to dial the digits, but easier to remember the words.

A whole industry has grown up around the providing of domain names. They are big business. And it makes it pretty easy to identify the business or organization that you are visiting on the web.

See section **??** (page **??**) for more on the domain name system.

Capitalization does not matter with domain names. You can say "doncolton.com" or "DonColton.COM" and it's all the same to the network.

2.1.3 Paths

`/inet/book.pdf` is an example of a path.

Strictly speaking, the path is not required to have any special meaning. It is just the name of the object you wish to retrieve. But practically speaking, it is usually the case that the path can be deconstructed into smaller pieces.

`/inet/` is the directory or folder on the server.

`book.pdf` is the filename on the server. If you decide to save a copy of it on your local computer, this is probably what it will be called.

`.pdf` is the type of file at that location.

Capitalization DOES matter with the path. "book.pdf" is usually not the same as "Book.pdf" or "Book.PDF". It could be, but often it is not. This can be confusing. Sorry.

Because path names often are built out of folder names and file names, you can sometimes trim off the last piece and retrieve again. This can often get you additional information. For example, if "/inet/book.pdf" is the path you are given, you could try to retrieve just "/inet/". You might find a directory of several items, including "book.pdf" as well as "answerkey.pdf" and "quiz1.pdf". Or maybe not. But it may not hurt to look.

2.2 IPv4 Addresses

The main thrust of this chapter is an exploration of the IP address, more properly called the IPv4 address. "v4" means version 4. There is a new standard emerging, IPv6. It will eventually replace IPv4, but people are slow to change, and IPv4 is still the dominant way to provide addresses on the Internet.

As a basic skill, students must be able to manipulate IPv4 addresses to answer various questions about them. Let's dive right in.

2.2.1 Vocabulary

Skill: Know the names of various notations used in IPv4 addressing.
Mem: dotted quad notation looks like 123.123.123.123. It consists of four numbers. Each number is a base-10 number between 0 and 255. A dot is written between each of the four numbers.
Mem: a quad is one fourth of an IPv4 address.
Mem: CIDR (slash) notation looks like /21

2.2.2 Number Bases

Normally we use base 10 when we do numeric calculations. Base 10 is the system of numbering that uses ten digits (zero through nine) to form numbers.

It's not the only number system we commonly use. The second most common system is base 60. We use it for keeping time. The minute after 10:59 is 11:00. The second after 2:59:59 is 3:00:00. We commonly divide time into hours, minutes, and seconds. Minutes run from zero to 59, and then they roll over, starting a new hour, with minutes returning to zero.

Computers use base 2 for engineering reasons. It makes a lot of things easier. But numbers in base 2 can get long. They have three times as many digits as the same number would have in base 10.

To get around that wordiness, base 2 is often converted into some other power of two for convenience.

This is similar to what we do with numbers in base 10. We group the 10s in groups of three, and separate them by commas. For example, the number

after 999 is 1,000. The number after 999,999 is 1,000,000. It's even more obvious when we try to say the numbers. We say 999 thousand, 999. Or 999 million, 999 thousand, 999.

(Interestingly, some asian countries group their powers of 10 in groups of 4. 10000 ("mahn") is the base for large numbers, instead of the 1000 that is commonly used in western countries. And some years ago the British usage was to group large numbers by six digits. A million was a one followed by six zeroes. A billion had 12 zeroes. A trillion had 18 zeroes. Current usage has a million at 6, a billion at 9, and a trillion at 12. It makes less sense, but it's still the current usage.)

Each digit in a base 2 number is called a bit, which is short for binary digit.

Starting with numbers in base 2, we can group by threes to get base 8 (2x2x2, octal). We can group by fours to get base 16 (2x2x2x2, hex). And we can group by eights to get base 256.

Octal lets us express numbers in a computer-friendly way with roughly the same number of digits as we would use in base 10. The down side is that grouping by three is awkward.

Hex (hexadecimal) lets us express numbers in a computer-friendly way with fewer digits than base 10. Grouping by four is wonderful. The down side is you need 16 digits, so beyond 9 we use the letters A through F, which is awkward.

Base 256 is a cross between base 10 and base 2. We group bits into groups of eight, also called octets. Then we translate each octet into base 10. (This is exactly what we do with minutes and seconds, except they are base 60.) Base 256, also called dotted quad, is the notation used for IP addresses, net masks, and many related concepts in networking.

Skill: Be familiar with the notation for powers, especially powers of two.
Mem: 2^5 means 2 to the fifth power, and means you multiply 2 by itself 5 times. 2x2x2x2x2 = 32. It is also written as `2^5`.
Mem: 2^n means 2 to the nth power, and means you multiply 2 by itself n times. It is also written as `2^n`.
Mem: 10^n means 10 to the nth power, and means you multiply 10 by itself n times. It is also written as `10^n`.

Skill: Be familiar with the number bases used in networking.
Mem: **base 2** notation consists of ones and zeroes.

Mem: **binary** means base 2.
Mem: dotted binary looks like 10110101.10001001.11010010.01101001. It simply translates each part of dotted quad into base 2.
Mem: **base 8** notation consists of digits from 0 to 7. Each digit corresponds to exactly three bits.
Mem: **octal** means **base 8**.
Mem: **base 16** notation consists of digits from 0 to 9 and letters from A to F (for the values 10 to 15). Each digit corresponds to exactly four bits.
Mem: **hex** or **hexadecimal** means **base 16**.
Mem: **base 256** notation is another name for dotted quad notation. It highlights the fact that each part of the address is a number between 0 and 255. Each portion corresponds to exactly eight bits.
Mem: **octet** means eight bits.

Skill: Be familiar with units of measure for information quantity.
Mem: **bit** means one binary digit, either a zero or a one.
Mem: **nybble** means four bits.
Mem: **byte** normally means eight bits.
Mem: **kilo** means $2^{10} = 1024$ for engineers and 1000 for marketing.
Mem: **mega** means $2^{20} = 1024^2$ for engineers and 1000^2 for marketing.
Mem: **giga** means $2^{30} = 1024^3$ for engineers and 1000^3 for marketing.
Mem: **tera** means $2^{40} = 1024^4$ for engineers and 1000^4 for marketing.
Mem: **KB** means kilobyte, one thousand bytes.
Mem: **Kb** means kilobit, one thousand bits.
Mem: **Kbps** means kilobits per second.
Mem: **MB** means megabyte.
Mem: **Mb** means megabit.
Mem: **Mbps** means megabits per second.
Mem: **GB** means gigabyte, one "gig".
Mem: **Gb** means gigabit.
Mem: **Gbps** means gigabits per second.

Marketing v Engineering: Marketing wants things to sound as good as possible. Therefore, they normally use 1000 as their number base in describing things. I bought a 2T external hard drive recently. By that, marketing means 2,000,000,000,000 bytes. Engineering would have meant 2x1024x1024x1024x1024. So in engineering terms, my 2T drive is really only 1862 Gig instead of 2000 Gig (or 2048 Gig). But hey, I'm happy. It's a lot of storage. Just be aware that they are not talking the same language.

2.2.3 Popular Numbers

Not all numbers are equally popular. In day-to-day living, the number 100 comes up a lot more often than the number 97. Similarly, 5 is more popular than 3 or 4 or 6 or 7.

Numbers like 10, 100, and 1000 are popular because they are "round," meaning that they end in a lot of zeroes.

In networking as well some numbers are much more popular than others. And it is because they are round in some sense. For networking, round means how they look in base 2, binary.

Skill: Quickly recognize and use the common IPv4 numbers: Powers of 2. These are the only numbers that appear in (dotted quad) subnet block sizes. (Spaces have been added for clarity, but normally they are left out.)
Mem: binary 00000000 is 0
Mem: binary 0000000 1 is $2^0 = 1$ (multiply no 2s)
Mem: binary 000000 1 0 is $2^1 = 2$ (multiply one 2)
Mem: binary 00000 1 00 is $2^2 = 4$ (multiply two 2s)
Mem: binary 0000 1 000 is $2^3 = 8$ (multiply three 2s)
Mem: binary 000 1 0000 is $2^4 = 16$ (multiply four 2s)
Mem: binary 00 1 00000 is $2^5 = 32$ (multiply five 2s)
Mem: binary 0 1 000000 is $2^6 = 64$ (multiply six 2s)
Mem: binary 1 0000000 is $2^7 = 128$ (multiply seven 2s)

Skill: Quickly recognize and use the common IPv4 numbers: Negative Powers of 2. These are the only numbers that appear in (dotted quad) net masks. They are also the boundaries between the address classes. (Spaces have been added for clarity, but normally they are left out.)
Mem: binary 11111111 is 256 - $2^0 = 255$
Mem: binary 1111111 0 is 256 - $2^1 = 254$
Mem: binary 111111 00 is 256 - $2^2 = 252$
Mem: binary 11111 000 is 256 - $2^3 = 248$
Mem: binary 1111 0000 is 256 - $2^4 = 240$ (also start of class E)
Mem: binary 111 00000 is 256 - $2^5 = 224$ (also start of class D)
Mem: binary 11 000000 is 256 - $2^6 = 192$ (also start of class C)
Mem: binary 1 0000000 is 256 - $2^7 = 128$ (also start of class B)
Mem: binary 00000000 is 256 - $2^8 = 0$ (also start of class A)

We will talk about classes and network masks shortly.

2.3 Network.Host Addressing

Before 1981, the Internet, then called the ARPANet, used 8-bit network addresses and 24-bit host addresses. This is before the introduction of classes A, B, and C.

IP addresses were originally conceived in a network.host naming format. A **host** is an individual computer.

The idea was that within a network, hosts could communicate directly to one another. Whatever happens in Las Vegas, stays in Las Vegas, so to speak. The Internet did not want to know or be bothered by the details of how each network was organized. The Internet only cared about communication between networks.

If computer 20.1234 wanted to talk to computer 20.5678, they could do so without involving the Internet. Both were on network 20. They could just talk by whatever rules were used on network 20.

If computer 20.1234 wanted to talk to computer 30.5678, they would need to involve the Internet. In the simple case, there would be one machine that had two wires. One wire would connect it to network 20 and the other wire would connect it to network 30. That machine would act as a gateway, or go-between, for networks 20 and 30. Often the gateway got a special number, like .1. It could be 20.1 on the 20 network, and 30.1 on the 30 network.

Typically the connecting wires were telephone lines.

Of course, for 256 networks to communicate, it is not necessary for each to have a private line to the other 255. If six degrees of separation works for humans, why not computer networks as well?

http://en.wikipedia.org/wiki/Six_degrees_of_separation has more on this six degrees concept. It makes for interesting reading. They even made a movie.

Long story short, by careful programming we could have a message from 20.1234 go to machine 99.1111 through a number of intermediaries. It might go first to 20.1, alias 30.1, which could pass it along to 30.77, alias 77.1, and so on until it reached the 99 network for final delivery.

Routing involves having a small number of core machines that know where everything is. Pass a message to one of these core machines and they can pass it on to the proper branch of the network. The core routers were

operating based on hand-crafted routing tables. Each time a new network came online, the tables would be adjusted. This did not happen often at first, so it was no big problem.

2.4 Classful Addressing

http://en.wikipedia.org/wiki/Classful_network gives good background on the origin of classful networks.

There were to be 256 networks, and each network could have like 16 million hosts. But that's not how things turned out. As prices for computers came down, it turned out that there was a large demand for many more networks, and the networks were much smaller than 16 million hosts. So the numbering got rearranged.

Classful addressing started about 1981.

The original networks 1 through 126 remained as before. They are called Class A networks. Each one has 16 million hosts.

The 64 networks from 128 to 191 became Class B. Instead of just being those 64 networks, each was divided 256 ways, creating 16 thousand smaller networks. You don't get something for nothing though. Each network had only 1/256 as many hosts, which is $2^{16} = 65536$ hosts. (We are being a bit sloppy here. It's actually only 65534. We will clean up our sloppiness later.)

The 32 networks from 192 to 223 became Class C. Instead of just being those 32 networks, each was divided 256 ways, and then 256 ways again, creating around 2 million networks, each having $2^8 = 256$ (really 254) hosts.

And life was good for a while. This way of dividing things became known as **classful addressing** and it prevailed for many years. Eventually the addresses started to run out. Then these address classes were further divided, not by the powers that be, but by the end users, the companies that were using them.

They started to create sub-networks, called subnets, and the addressing was called **classless addressing**. We will get to that in 2.5 (page 19), but first we need to concentrate on the world of Classful Addressing.

Skill: Given an IPv4 address, tell what the class is.
Mem: 1-126.0.0.0 is class A. (starts with 0xxxxxxx)
Mem: 128-191.0.0.0 is class B. (starts with 10xxxxxx)

Mem: 192-223.0.0.0 is class C. (starts with 110xxxxx)
Mem: 224-239.0.0.0 is class D. Multi Cast. (1110xxxx)
Mem: 240-255.0.0.0 is class E. Experimental. (1111xxxx)

Q: For 19.19.19.19, what class is it?
A: A.

Q: For 199.199.199.199, what class is it?
A: C.

2.4.1 Network Masks

Since the network.host split had become variable, instead of always being an 8.24 split, programs had to be updated. Programmers are lazy and hate to update anything twice if the can spend the extra time to get it updated correctly the first time.

To handle this variation in splits, a lot of programming was done using the knowledge that class A was always an 8.24 split, and class B was always a 16.16 split, and class C was always a 24.8 split.

net mask: Given a computer address, like 20.1234, programmers needed to separate that address into its two parts. They did this mathematically by using something called a mask. The mask consisted of ones for the things they wanted to keep and zeroes for the things they wanted to get rid of. The logic behind this relates to AND and OR, with 1 standing for TRUE and 0 standing for FALSE. Computers can do this calculation really fast.

For class A, the net mask is 11111111.00000000000000000000000. It consists of eight 1s followed by 24 0s.

For class B, the net mask is 1111111111111111.0000000000000000. It consists of 16 1s followed by 16 0s.

For class C, the net mask is 11111111111111111111111.00000000. It consists of 24 1s followed by eight 0s.

Programmers, being human and not machines (a statement that some might dispute), found two improvements to this notation. The first was to separate the 32 bits into four groups of 8. Thus:

For class A, the net mask is 11111111.00000000.00000000.00000000.

For class B, the net mask is 11111111.11111111.00000000.00000000.

For class C, the net mask is 11111111.11111111.11111111.00000000.

The second was to convert each set of 8 into base 10 numbering. Maybe this was for the sake of their managers. In any case, the result was shorter.

For class A, the net mask is 255.0.0.0.

For class B, the net mask is 255.255.0.0.

For class C, the net mask is 255.255.255.0.

That is because 11111111 (eight 1s) is the base 2 (binary) number that is equivalent to 255 in base 10 (decimal). And 00000000 in any base is always the same: 0.

Skill: Understand net masks.

Q: Explain net mask.
A: A net mask consists of some number of binary 1s followed by some number of binary 0s. For IPv4, the total is 32 bits. It is normally written in base 10 notation, consisting of four numbers, each of which represents 8 bits.

Q: What do the 1s mean?
A: The 1s indicate the part of the address that is the network number.

Q: What do the 0s mean?
A: The 0s indicate the part of the address that is the host number.

2.4.2 CIDR Routing

Instead of having 256 networks, Classful Addressing gave us millions. This had an impact on the routing tables in those core routers. Nobody wants millions of lines of routing information, especially when 256 lines was working just fine, thank you very much.

CIDR started about 1993, and opened the door to classless addressing.

CIDR was invented as a way to consolidate groups of networks into a single entry in the routing table.

CIDR stands for Classless Inter-Domain Routing. Its original purpose is to bundle together several class B or C networks in a single expression. It is also used as a shorthand notation to express network and subnet masks, which we will discuss soon.

CIDR is also called **slash notation**. It uses a /16 to indicate that the first 16 bits of the IP address are the network bits. If we are consolidating 4 class B addresses, and they each have the same first 14 bits in their network number, we can call it a /14 super-net.

Skill: Explain CIDR "slash" notation.
Mem: /8 = 11111111.00000000.00000000.00000000 = 255.0.0.0
Mem: /16 = 11111111.11111111.00000000.00000000 = 255.255.0.0
Mem: /24 = 11111111.11111111.11111111.00000000 = 255.255.255.0
Mem: /xx means the first xx bits of the net mask are 1s. The rest are 0s. There are 32 total bits.

Skill: Given an IPv4 address, tell the CIDR and the default Net Mask in dotted quad notation.
Mem: For class A, CIDR is /8, net mask is 255.0.0.0
Mem: For class B, CIDR is /16, net mask is 255.255.0.0
Mem: For class C, CIDR is /24, net mask is 255.255.255.0

Q: For 199.199.199.199, what is the CIDR and default Net Mask?
A: /24 and 255.255.255.0.

2.4.3 Special Addresses

Some IPv4 addresses were given special significance. They were not just any old address. Here is the list.

Skill: Tell the IPv4 special address ranges.
Mem: 0.0.0.0/8 is the local network.
Mem: 10.0.0.0/8 is the class A private address range.
Mem: 127.0.0.0/8 is the localhost address range.
Mem: 127.0.0.1 is the local host.
Mem: 169.254.0.0/16 is the **link local** self-assigned address range.
Mem: link local is also called **APIPA**.
Mem: 172.16.0.0/12 is the class B private address range.
Mem: 192.168.0.0/16 is the class C private address range.
Mem: 255.255.255.255 is the IPv4 global broadcast address.

http://datatracker.ietf.org/doc/rfc1918/ covers 10, 172, 192.

http://datatracker.ietf.org/doc/rfc3927/ covers APIPA.

2.5 Classless Addressing

As mentioned above, organizations started to create sub-networks, called subnets, and the addressing was called **classless addressing**. We are now ready to talk about it.

Making some original addresses into class B and class C addresses was simple and elegant. 16 million hosts per network was a bit much. As computer prices came down and networking prices came down, there was great pressure to further subdivide the B and C addresses (and the A addresses too).

It was too late to redesign the overall plan for Classful Addressing. Too many people were using it. Too many programs depended on it.

But CIDR and the net mask concept provided an opportunity to go the other way. Instead of aggregating things into super-nets, they could be further divided into subnets.

To keep clear the division between network bits and host bits, it would be necessary to utilize an explicit subnet mask telling exactly how many bits were network. There was already an implicit mask based on the first number in the IP address. Now things were going to be expressed and not just assumed.

2.5.1 Subnet Block Size

Subnetting is the process of dividing a class A, B, or C address block into smaller blocks, and associating those blocks as separate networks.

Since base 2 is very convenient for networking, things are most efficient when done by doubling or splitting in half. That keeps it simple for the network programmers and fast for the networking equipment.

The cost of this subnetting was that net masks got more complicated. Instead of just consisting of 255s and 0s, we got a bunch of other numbers that you met back in section 2.2.3 (page 13).

Skill: Given a CIDR subnet, tell what the subnet mask is in dotted quad notation. (Be able to do this for /8 through /30.)

Q: For /21, what is the subnet mask?
A: /20 = 11111111.11111111.11110000.00000000 = 255.255.240.0.
A: /21 = 11111111.11111111.11111000.00000000 = 255.255.248.0.

A: /22 = 11111111.11111111.11111100.00000000 = 255.255.252.0.
A: /23 = 11111111.11111111.11111110.00000000 = 255.255.254.0.
A: /24 = 11111111.11111111.11111111.00000000 = 255.255.255.0.
A: /25 = 11111111.11111111.11111111.10000000 = 255.255.255.128.
A: /26 = 11111111.11111111.11111111.11000000 = 255.255.255.192.
A: /27 = 11111111.11111111.11111111.11100000 = 255.255.255.224.
A: /28 = 11111111.11111111.11111111.11110000 = 255.255.255.240.
A: /29 = 11111111.11111111.11111111.11111000 = 255.255.255.248.

Subnet block size is a key number in calculating a bunch of other important numbers.

There are several ways to calculate the subnet block size.

Powers of Two Method: The block size is just 2 raised to the power of however many bits are available for the host address. Remove as many 8s as you can before converting to base 10. Then add a .0 for each 8 you removed.

Skill: Given a CIDR subnet, tell what the subnet block size is in dotted quad notation.

Q: For /10, what is the subnet block size?
A: 0.64.0.0.
A? 32 - 10 = 22 host bits. $2^{22} = 2^6$ x 2^8 x 2^8 = 0.64.0.0.

Q: For /23, what is the subnet block size?
A: 0.0.2.0.
A? 32 - 23 = 9 host bits. $2^9 = 2^1$ x 2^8 = 0.0.2.0.

Q: For /28, what is the subnet block size?
A: 0.0.0.16.
A? 32 - 28 = 4 host bits. 2^4 = 0.0.0.16.

Split Block Method: Figure out which quad has the split within it. For /8, /16, and /24, the split falls between quads which makes everything very easy. For the rest, /9-15 are in quad 2, /17-23 are in quad 3, and /25-30 are in quad 4.

Within that quad, determine how many host bits there are, and take 2 raised to that power.

Skill: Given a CIDR subnet, tell what the subnet block size is in dotted quad notation.

Q: For /10, what is the subnet block size?

A: 0.64.0.0.
A? 10 is in quad 2, with a 2/6 split. $2^6 = 64$. Put 64 in quad 2.

Q: For /23, what is the subnet block size?
A: 0.0.2.0.
A? 23 is in quad 3 with a 7/1 split. $2^1 = 2$. Put 2 in quad 3.

Q: For /28, what is the subnet block size?
A: 0.0.0.16.
A? 28 is in quad 4 with a 4/4 split. 2^4 16. Put 16 in quad 4.

Subtraction Method: As a happy coincidence, the subnet mask plus the block size always equals zero. So if you know the net mask, you can subtract it from zero to get the block size. It is very convenient to do this in base 256.

Skill: Given a CIDR subnet, tell what the subnet block size is in dotted quad notation.

Q: For /10, what is the subnet block size?
A: 0.64.0.0.
A? 0.0.0.0 minus 255.192.0.0 (/10 net mask) = 0.64.0.0.

Q: For /23, what is the subnet block size?
A: 0.0.2.0.
A? 0.0.0.0 minus 255.255.254.0 (/23 net mask) = 0.0.2.0.

Q: For /28, what is the subnet block size?
A: 0.0.0.16.
A? 0.0.0.0 minus 255.255.255.240 (/28 net mask) = 0.0.0.16.

Skill: Given an IPv4 subnet mask, tell what the subnet block size is in dotted quad notation.

Q: For 255.255.248.0, what is the subnet block size?
A: 0.0.8.0.
A? 255.255.248.0 + 0.0.8.0 = 0.0.0.0

2.5.2 Subnet Count

There are two ways to count subnets. The old way, in effect until about 2005, is called **no subnet-zero**. The new way, in effect since 2005, is called **subnet-zero** or "with" subnet-zero.

The subnet-zero issue is what to do with the first and last subnets in the network. The old-school idea was that no subnet should use those slots. Any exam questions you might find online from that era probably assume this old-school approach.

The current idea is that every subnet slot can be used. Under this method, which is widely accepted, the number of subnets is just the power of two that matches the number of bits available for the subnet portion of the address.

With no subnet-zero, just take the subnet-zero count and subtract two from it.

Skill: Given an IPv4 address and a CIDR subnet, tell how many subnets there are, assuming subnet-zero.

Q: For 150.150.150.150/21, how many subnets are there (with subnet-zero)?
A: $2^5 = 32$.
A? 21-16 (class B) = 5 bits.

Skill: Given an IPv4 address and a CIDR subnet, tell how many subnets there are, assuming no subnet-zero.

Q: For 150.150.150.150/21, how many subnets are there (no subnet-zero)?
A: $2^5 - 2 = 30$.

2.5.3 First Subnet

You need to know the subnet block size and the (classful) network address.

With subnet-zero, the first subnet address **is** the network address.

With no subnet-zero, the first subnet address is the network address plus the block size.

Skill: Given an IPv4 address and a CIDR subnet, tell what the first subnet address is in dotted quad notation, assuming subnet-zero.

Q: For 150.150.150.150/21, what is the first subnet address (with subnet-zero)?
A: 150.150.0.0.
A? With subnet-zero, the first subnet is always the same as the network address.

Skill: Given an IPv4 address and a CIDR subnet, tell what the first subnet address is in dotted quad notation, assuming no subnet-zero.

Q: For 150.150.150.150/21, what is the first subnet address (no subnet-zero)?
A: 150.150.8.0.
A? With no subnet-zero, the first subnet is always the network address plus the block size. 150.150.0.0 + 0.0.8.0 = 150.150.8.0.

2.5.4 Last Subnet

You need to know the subnet block size and the (classful) network address of the NEXT network.

With subnet-zero, the last subnet address **is** the next network address minus the block size.

With no subnet-zero, the last subnet address is the next network address minus two block sizes.

In calculating the next network address, be careful to remember whether the network is class A, B, or C.

Skill: Given an IPv4 address and a CIDR subnet, tell what the last subnet address is in dotted quad notation, assuming subnet-zero.

Q: For 150.150.150.150/21, what is the last subnet address (with subnet-zero)?
A: 150.150.248.0.
A? It is always the next network address minus the block size. 150.151.0.0 - 0.0.8.0 = 150.150.248.0.

Skill: Given an IPv4 address and a CIDR subnet, tell what the last subnet address is in dotted quad notation, assuming no subnet-zero.

Q: For 150.150.150.150/21, what is the last subnet address (no subnet-zero)?
A: 150.150.240.0.
A? It is always the next network address minus the block size x2. 150.151.0.0 - 0.0.8.0 x2 = 150.150.240.0.

2.5.5 Current Subnet

There are four questions you should be able to answer about the current subnet. What is the subnet address, the first host address, the last host address, and the broadcast address.

To solve this, you need to know the subnet block size. You need to be able to count in multiples of that number.

For 16, the multiples would be 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240.

You don't actually need all of those numbers. You just need the one that is before and the one that is after the current IP address.

If the current IP address is 1.2.3.150/28, then quad 4 is where the split occurs and we should look for the numbers that surround 150. Those would be 144 and 160.

The **subnet address** is 144 because that is the multiple of 16 that comes at or before 150.

The **first host** is always just one beyond the subnet address.

The **next subnet address** is 160 because that is the multiple of 16 that comes after 150.

The **last host** is always just two before the next subnet address.

The **broadcast address** is always just one before the next subnet address.

Skill: Given an IPv4 address and a CIDR subnet, tell what the current subnet address is, meaning the subnet in which that IPv4 address occurs.

Q: For 150.150.150.150/21, what is the current subnet address?
A: 150.150.144.0.

Skill: Given an IPv4 address and a CIDR subnet, tell what the first host address is in dotted quad notation.

Q: For 150.150.150.150/21, what is the first host address?
A: 150.150.144.1.

Skill: Given an IPv4 address and a CIDR subnet, tell what the last host address is in dotted quad notation.

Q: For 150.150.150.150/21, what is the last host address?

A: 150.150.151.254.

Skill: Given an IPv4 address and a CIDR subnet, tell what the broadcast address is in dotted quad notation.

Q: For 150.150.150.150/21, what is the broadcast address?
A: 150.150.151.255.

Another question that could be asked is whether two IP addresses are in the same subnet or not.

Skill: Given an IPv4 address and a CIDR subnet, tell whether another specified IPv4 address is in the same LAN.

Q: For 150.150.150.150/21, is 150.150.149.149 in the same LAN?
A: Yes.

Q: For 150.150.150.150/21, is 150.150.155.155 in the same LAN?
A: No.

Chapter 3

OSI 7-layer Model

Students should be able to apply the OSI model to networking hardware and software. Mostly we are concerned with the bottom four layers.

See also: http://en.wikipedia.org/wiki/OSI_model

Skill: Tell the numbers and names of the layers in the OSI model?
Mem: 7 **application layer** (the highest layer)
Mem: 6 **presentation layer**
Mem: 5 **session layer**
Mem: 4 **transport layer**
Mem: 3 **network layer**
Mem: 2 **data link layer**
Mem: 1 **physical layer** (the lowest layer)

Skill: Know which common networking items match layer 1: Physical.
Mem: Bit (protocol data unit)
Mem: Repeater (device, two-port hub)
Mem: Hub (device, multi-port repeater)
Mem: Media: wire, coax, fiber, rj45, cat5e

Skill: Know which common networking items match layer 2: Data Link.
Mem: Frame (protocol data unit)
Mem: Switch (device, multi-port bridge)
Mem: Bridge (device, two-port switch)
Mem: Physical Addressing, MAC Address
Mem: LAN (local area network)

Skill: Know which common networking items match layer 3: Network.
Mem: Packet (protocol data unit)
Mem: Router (device)
Mem: Gateway (device)
Mem: Logical Addressing, IP Address
Mem: WAN (wide area network)
Mem: DHCP (dynamic host configuration protocol)
Mem: NAT (network address translation, aka PAT)

Skill: Know which common networking items match layer 4: Transport.
Mem: Segment (protocol data unit)
Mem: Port
Mem: Flow Control
Mem: TCP (reliable)
Mem: UDP (fast)

Skill: Know which common networking items match other layers.
Mem: Encryption :: 6 Presentation
Mem: User :: 7 Application

Chapter 4

Power Tools

Skill: Given a network diagram, tell the route that data would take from point of origin to destination, and the transformations that would occur. This includes NAT, and traversal from one LAN to another.

4.1 speedtest.net

There are really three different numbers that are commonly associated with speed.

Latency measures the time it takes to transmit a small amount of information from your computer to another computer, and to receive a response. Gamers often refer to this as lag.

Download Speed measures the time it takes to download a large file from the Internet to your local computer.

Upload Speed measures the time it takes to upload a large file from your local computer to the Internet.

Telephone lines provide fast latency but small upload and download volume. A satellite link provides slow latency but huge upload and download volume.

Skill: Critically compare the bandwidth characteristics of several types of physical communication media.

Skill: Explain how bandwidth and latency impact throughput in a data

communications channel.

http://speedtest.net/ provides a combined measure of network speed, including download speed, upload speed, and latency.

http://www.pingtest.net/ provides a more carefully calculated average ping time (latency) for your network connection.

http://en.wikipedia.org/wiki/Latency_(engineering) provides additional discussion of latency.

http://en.wikipedia.org/wiki/Lag provides additional discussion of lag.

4.2 ping

The **ping** command measures **latency**. It is also used very simply to discover if the local computer can reach the remote computer.

http://en.wikipedia.org/wiki/Ping provides an overview of **ping**.

4.3 traceroute

The **traceroute** command measures latency and also gives a list of the intermediate routers through which packets will travel between the local computer and the remote computer. It is used to discover where the bottlenecks might be occurring.

http://en.wikipedia.org/wiki/Traceroute provides an overview of **traceroute** (Unix) and **tracert** (Windows).

4.4 ipconfig

The **ipconfig** command (Windows), also known as the **ifconfig** command (Mac and Linux), displays the configuration details relating to IP addressing on the local computer.

http://en.wikipedia.org/wiki/Ipconfig provides an overview of **ipconfig** (Windows).

http://en.wikipedia.org/wiki/Ifconfig provides an overview of **ifconfig** (Unix).

4.5 nmap

The **nmap** command explores (maps) the network to discover what other resources are available, including other computers.

http://en.wikipedia.org/wiki/Nmap provides an overview of **nmap**.

Free downloads are available for Windows, Mac, and Linux at http://nmap.org/download.html

4.6 ssh

The **ssh** command makes a secure shell (command line) connection with another computer. All data between the two computers is encrypted if it goes through the ssh connection.

http://en.wikipedia.org/wiki/Secure_Shell provides an overview of **ssh**.

4.7 telnet

The **telnet** command makes an insecure shell (command line) connection with another computer. It has been mostly replaced by **ssh** because of the security issues. However, it is almost universally available.

http://en.wikipedia.org/wiki/Telnet provides an overview of **telnet**.

4.8 ftp

The ftp command provides for file transfer with another computer.

http://en.wikipedia.org/wiki/Ftp provides an overview of **ftp**.

4.9 wireshark

The **wireshark** tool allows you to examine packets that are visible to the computer you are using. It can be a great aid in finding out how much traffic is taking place, in case some of it can be eliminated.

http://en.wikipedia.org/wiki/Wireshark provides an overview of **Wireshark**. Wireshark was formerly called **Ethereal**.

http://www.wireshark.org/ is the official website for this open source tool.

Free downloads are available for Windows and Mac at http://www.wireshark.org/download.html

Chapter 5

Home Router

Students should be able to explain and properly set the parameters of a modern Wireless Home Router.

Skill: Distinguish between LANs and WANs.

A **LAN** is a local area network. It comprises the computers and equipment that can talk to each other without involving the Internet. Normally one of the devices does have access to the wide area network (Internet) and serves as a gateway for the other devices.

Communication on a LAN is normally done by way of MAC addresses.

A **WAN** is a wide area network. Historically the term had meaning, but currently it is mostly just another way to say Internet.

Communication on the Internet is done by way of IP addresses.

Skill: MAC cloning: What, Why, How?
A: The router will take over the WAN connection from a computer. The router uses the MAC address of that computer instead of its own. This avoids port security problems upstream.

Skill: Interior **DHCP** server: settings?
A: Net Mask, Local IP address of the router.
A: First IP address to be given. Number of IP addresses to be given. Client Lease Time.
A: additional IP addresses can be statically assigned. This could be handy for print servers, file servers, and video feeds.

Skill: MAC Filter: What, How, Issues?
A: It allows you to restrict service based on MAC address. Because of MAC cloning, it is not 100% reliable.

Skill: Home Router as **Firewall**: How, Issues.
A: When interior computers are assigned IPv4 addresses by **NAT**, sometimes called **PAT**, exterior computer cannot reach them directly by IP address. Messages come to the router which determines ultimate destination based on port number. Port numbers are difficult to predict except (a) when responding to a request that originated inside the LAN (b) when accessing a service for which **port-forwarding** has been established (c) when a machine has been designated as the **DMZ** Host (de-militarized zone)

Skill: Home Router as Policeman: How, Issues. What WAN Access Policy options are commonly available?
A: Block for specified interior machines by time of day, day of week.
A: Block for specified services, such as multi-player games.
A: Block for specified exterior domain names.
A: Block for specified words that appear on exterior websites.

Skill: QoS: What, How.
A: **QoS** stands for **Quality of Service**. It is a way of prioritizing bandwidth among interior machines. Allocation is commonly based on Hardware Port, MAC address, IP address, and service (layer 4 port).

Skill: Passwords: What, Issues.
A: The router itself has a master password. Defaults are well known. The password should be changed before the router is placed in use. If the password is lost, the router can be reset to restore the default password. To do this, you must have physical control of the router. The procedure is well known. You can also restore the router to its factory defaults if tampering may have occurred. You may also be able to back up all settings in case you want to restore them later.
A: The WiFi service set should normally have a password. Defaults are well known.
A: The SSID, if hidden, can act as a rudimentary password, but it can often be sniffed.

Skill: File Server: What. Some home routers can act as local file servers. Normally the protocol is SMB (Server Message Block). This provides file-

sharing capability between interior computers (and possibly exterior).

Skill: Print Server: What. Some home routers can act as local print servers. Print servers are also commonly done as separate interior computers.

Chapter 6

WiFi (802.11)

Students should be able to answer questions about WiFi, including estimating the range of a WiFi signal given the distance and obstructions between the base station and the receiver.

What is an **SSID**?
A: Service Set Identifier. 32 characters. Broadcast or hidden. It is the "name" of the wireless access point.

What security methods are commonly used?
A: none, WEP, WPA, **WPA2**

What **channels** exist (in the USA)?
Mem: 1-11

What channels are commonly usable (in the USA) and why so few?
Mem: 1,6,11 because of signal bleed between adjacent channels.
Mem: 1,4,8,11 gets lower throughput than 1,6,11. (CISCO study.)

Skill: Given a floor plan, tell how much signal will be present at various places.

Skill: Know a bit about wireless transmission power measurement.
FYI: **dBm** = **decibel**s based on a 1-milliwatt scale.
FYI: 20 dBm = 100 mW = 100 milliwatt of transmission power.
FYI: 10 dBm = 10 mW = 10 milliwatt of transmission power.
FYI: 0 dBm = 1.0 mW = 1 milliwatt of transmission power.
FYI: -10 dBm = 0.1 mW = 1/10 milliwatt of transmission power.
FYI: -20 dBm = 0.01 mW = 1/100 milliwatt of transmission power.

FYI: See also: http://en.wikipedia.org/wiki/DBm
FYI: 30 dBm: microwave oven leakage (noise when operating).
FYI: 20 dBm: strongest legal (outdoor) WiFi signal strength (USA)
FYI: 15 dBm: typical laptop WiFi signal strength.
FYI: -70 dBm: Weakest WiFi signal that can be usefully received.

Skill: For typical WiFi, how much signal exists and how is it affected by obstacles?
FYI: dB is a ratio of two dBm measurements. It is calculated by subtracting because dB is logarithmically scaled.
Mem: 50 dB: typical **SNR** (**signal to noise ratio**), maximum 100 dB.
Mem: .5 dB: loss in open air, per meter.
Mem: 5 dB: loss through interior plaster-board wall, wooden studs.
Mem: 10 dB: loss through exterior wall, e.g., cement, re-bar, metal studs.
Mem: 15 dB: loss through floor, thick plywood, support beams.

Skill: Tell what else commonly affects signal strength.
A: indoors: people, furniture, cupboards, appliances.
A: outdoors: people, trees, rain.
A: interference: **microwave ovens**, wireless telephones.
A: the orientation of directional antennas.

Chapter 7

Security

By security, we mean keeping out the bad guys. Specifically we want to prevent the bad guys from seeing or changing anything that you want to protect. This may include where the gold is buried in your back yard. Or what the key looks like to your safe. Or what secrets are written in your diary.

The easy solution is to just burn everything. Then nobody can get to it. But you cannot get to it either.

Normally then, your goal is to maintain easy access for yourself, and at the same time make it difficult or impossible for unauthorized persons to have any access at all.

In this chapter will consider secure connections, firewalls, and passwords.

To achieve security, you need to understand where your **threats** are coming from.

Inside Threats: These are threats posed by machines that are inside your local area network.

Outside Threats: These are threats posed by machines across the world that may be trying to hack into your system.

7.1 Well Known Ports

Security is often done on a port-by-port basis. Each well-known port is connected to a service. These are the "vectors" through which bad guys can

try to attack you.

Skill: Tell the common well-known ports and their usages.
Mem: 21 FTP, File Transfer Protocol.
Mem: 22 SSH, Secure Shell.
Mem: 25 SMTP, Simple Mail Transfer Protocol.
Mem: 80 HTTP, Hyper Text Transfer Protocol.
Mem: 443 HTTPS, Hyper Text Transfer Protocol Secure.

7.2 Secure Connections

By using a network, you are necessarily moving information around. You may want that information to remain private between yourself and the person to whom you send it. Does the net have the ability to keep a secret?

As your first order of business when communicating, you can choose some keys by which your data will be encrypted. There is a clever way by which this is often done, but you don't really need to understand it. The important thing is that ALL communications can be observed and copied, but encrypted ones will remain obscure and secret.

When using web pages, HTTPS is the secure protocol. It utilizes SSL, the Secure Sockets Layer, to provide encryption.

When using WiFi, **WEP** was the first major security protocol, but it was found to be very insecure. WPA and later **WPA2** have replaced WEP as the standard for security in wireless communication.

When using a shell (command line terminal window), **ssh** is the standard security protocol. It has almost entirely replaced **telnet** which was used for command line access.

7.3 Firewalls

Skill: Explain how firewalls mitigate some network attack scenarios.

Firewalls provide a defense between yourself and the threats you are protecting against.

Inside Threats: Your operating system typically provides the best defense against inside threats. The protection varies from system to system, and

specific observations are beyond the scope of this document and this course. However, it is common to allow files or printers to be shared within your LAN. This sharing often requires special steps by the owner of the resource (the files or the printer).

Outside Threats: Your home router probably provides the best overall defense against outside threats. Typically the router does network address translation (NAT) as part of sharing your Internet connection among several computers at the same time. This makes each of those computers effectively invisible to everyone outside of your local area network. However, your home router has no capability to protect you against inside threats.

DMZ and Port Forwarding are settings in your router. They can open up one machine, or parts of several machines, to abuse from outside your local area network. However, they are necessary if you want your machines to act as servers. This typically happens (a) for gaming, if you want to host a game, (b) for running a personal website, and (c) for serving video, such as making surveillance cameras at home visible to you at work.

Providing wireless access to strangers can easily give them access to the inside of your network. At that point, your router is no longer providing a firewall between the stranger and your equipment and data. Generally it is a good idea to have WPA2 or better security on your wireless connections.

7.4 Password Selection

Skill: Explain why weak passwords are a significant problem in networks.
A: Because hackers get in and cause trouble.

There are a few rules for picking a good password. (a) Make it easy for you to remember. (b) Make it difficult for anyone else to guess. (c) Make it difficult for anyone else to remember, should they happen to see it.

The first real question is whether you need to remember it or not.

The best strategy for passwords that you do not need to remember is simply to use a random password generator. This satisfies (b) and (c) but not (a). However, if you have an automated way to store the password, then (a) may not be an issue.

For the rest of this section, we will focus on passwords you must remember.

Hackers and others that wish go guess your password have several typical

approaches. (a) If they know you, they can try combinations of personal information such as your telephone number or the name of your spouse or significant other or pet. (b) Whether they know you or not, they can try lists of common passwords.

Here is a list of the 13 most common passwords found on **Gawker** when hackers broke in during December of 2010: 123456, password, 12345678, lifehack, qwerty, abc123, 111111, monkey, consumer, 12345, 0, letmein, trustno1.

Would you use any of those? Apparently many did. We can attribute it to not thinking, or maybe to not caring. After all, if I have an account on Gawker, do I *really* care if someone else knows it?

It would be much more interesting to look at a collection of passwords for online banking.

But why stop at 13? Hackers have lists of thousands of common passwords. They can try each of those in an attempt to break into your account. If you care, you need to pick something they will not find.

And stay away from short passwords. Hackers will also try a brute force attack with all passwords, starting with the blank password, then going through the 26 letters one by one, then the digits and special characters. Then all possible two-character passwords. Then all possible three-character passwords. Depending on their connection, they can get up to five or six characters pretty fast.

The best strategy that I have found for passwords you must remember is to select a familiar phrase and reduce it to the first letters of each word. For example, **Lincoln**'s **Gettysburg Address** starts with the words: "Four score and seven years ago our fathers brought forth on this continent a new nation, ..."

These words are very familiar to the typical school child in the USA. By themselves, they may satisfy (a) and (b), but not (c) because they would be immediately recognized if seen. Plus they take a long time to type.

Going with the initials, we have "Fsasyaofbfotcann". It now satisfies (a), (b), and (c). Beyond this, it could be further modified by replacing the "F" with a "4" and maybe the "s" with a "7". Many other replacements might be considered, such as using digits or special characters that are shaped similarly to the letters they replace. "A" might be replaced with "4". "s" might be replaced with "5". "O" (oh) might be replaced with "0" (zero).

The password is reduced to gibberish that nobody would guess or remember if seen, but still you could create it as needed.

Chapter 8

Be The Server

Networks often involve the sharing of printer and files. In this chapter we show how this can be done by sharing parts of existing computer systems.

The exact how-to depends a lot on the operating system of the host computer. We have chosen to address these tasks in the context of Microsoft Windows. We will look at printer sharing, file sharing, and configuring ad hoc wireless networks.

8.1 Printer Sharing

Skill: Print Server: MS Windows provides the ability for your computer to act as a local print server. (Print servers are also commonly done as separate interior computers.)

todo: add more

8.2 File Sharing

Skill: File Server: MS Windows provides the ability for your computer to as a local file server. Normally the protocol is SMB (Server Message Block). This provides file-sharing capability between interior computers (and possibly exterior).

todo: add more

8.3 Ad Hoc Wireless Networking

todo: add more

Chapter 9

Lab Activities

Skill: Build a straight-through cable using RJ45 connectors.

Skill: Build a cross-over cable using RJ45 connectors.

Skill: Perform and report a Wireless Site Survey.

Skill: Deploy a basic Ethernet LAN

Skill: Demonstrate the ability to solve basic problems and perform basic troubleshooting operations on LANs and connected devices.

Skill: set up an ad hoc wireless network between two laptops

Skill: set up a file sharing network either on ad hoc network or sandboxed network

Skill: Given a wireless home router and a set of configurations to achieve, set the router to the requested configuration.

Index