BUS 175 Networking Basics Course Guide

Hi everyone. I have decided to make a tutorial for the students in BUS 175 with Professor Satpathy to offer supplemental information to the terms and concepts you may not understand immediately in class. This course is very technical, and you may have trouble understanding the material. I hope this guide will offer you a basic and simple understanding of the topic. I'll try to explain it the best I can in layman terms but please do understand that I am not an expert in this field.

Let's get started.

Table of Contents

1. The Fundamentals
2. Client/Server Relationship
3. Database Servers
4. Data Centers
5. Different Types of Networks (Infrastructure)
6. Types of Connectors
7. IP (Internet Protocol)
8. Client/Server IP Addressing
9. Domain Name System (DNS)
10. Data Center Computing
11. Methods of Database Processing
12. Virtualization
13. Internet
14. Intranet
15. Extranet
16. Storage Area Networks (SAN's)
17. Open Systems Interconnection Model (OSI Models)
18. Protocol Data Units (PDU's)
19. User Datagram Protocol (UDP)
20. Transfer Control Protocol / Internet Protocol (TCP/IP)
21. Connectionless
22. Connection Oriented
23. Wireshark Legacy / Wireshark Packet Analyzer
24. End

The Fundamentals

In networking, there are a few things you need to absolutely know before we continue.

1. All networks deal with computers. It doesn't matter if it's Mac, Windows, Linux, iPhone, etc. It needs computers.

2. Networks are created through connecting one computer to another. This can be done with and without internet or Wi-Fi or just by connecting a cable from one computer to another.
3. The internet is not just Google Chrome and the webpages it loads. If you think that is the case, please consider taking a remedial course on information systems and technology.

If you understand this so far, read on.

Client / Server Relationship

There are two types of computers that are in networks. There are clients (that's you) and there are servers (the webpage). Your computer and the webpage talk to each when requested. The talk is exchanged by ***packets***. Packets are packaged ***bits*** of information that are encoded to transport over a network. They can't be sent all at once so the information on the webpages are sent bit by bit. Same concept goes for the return of information requested from the webpage (the server).

Database Servers

Most of the time servers are going to be computers where databases are held. You can access the databases with a DBMS – database management systems. You can create, modify, and delete information, also known as records, in the system. Some DBMS's are MySQL, Microsoft Access, & Oracle. There are more but those are the more popular ones.

Data Center

A center where databases and/or servers are held. It can be on-site, offsite, in any size room across multiple floors or buildings.

Different Types of Networks (Infrastructure)

1. Personal Area Network (PAN)
    a. Your iWatch to your iPhone to your iMac to you.
2. Small Office Home Office Network (SOHO)
    a. This is pretty much a LAN but generally with fewer than 10 computers connected.
3. Local Area Network (LAN)

   a. This network is local. This can include your computer, wired & Wi-Fi devices across many floors if need be. Typically connected through 1 router. If not part of a WAN, the LAN connects directly to Internet Service Provider (ISP).
4. Metropolitan Area Network (MAN)
   a. This practically encompasses a city or a specific geographic region. Usually corresponds with one area which is why when Charter, or your ISP, has an outage at the apartments at UCR, everyone's mad…though it doesn't always have to be Charter.
5. Wide Area Network (WAN)
   a. This network covers more than one LAN. This network can span across many buildings at UCR and is usually the direct contact to the MAN which is generally the ISP.
   b. Normally used with sharing information between departments. Ex – Info between FBI, CIA, NSA, Donald Trump…Russians……etc.

Types of Connectors

1. HUB
   a. Common connector between computer to computer. It usually copies the information (bits & packets) so it can be accessible to other computers on the same network. This is considered ancient hardware since there are newer connectors that do the job better.
2. Switch
   a. A switch is an upgraded hub where rather than just copies and makes info available, it also can forward information to a specific computer on a network. Think of the old days when telephone operators used to be the intermediary for phone calls. They would use a 'switchboard'. Same concept.
3. Router
   a. The big one for all connectors. A router is also known as an access point / gateway and this device connects to or more networks together. Ex: your LAN to your ISP (located in the MAN). This thing also sends, receives, and forwards information across networks. The difference between this and a switch and hub is that a router will use the TCP/IP protocol and encode the information and send it to its location. A router finds the best 'route' to take to get your information to you quickly. More advanced topic for later.

Internet Protocol

1. IP (Internet Protocol)
   a. Literally stands for Internet Protocol.
   b. Every computing device that can be connected to a network has an IP address. This address serves as the identity of your computer. Each IP address is unique and cannot be the same as another computer's. If you don't understand this,

think of how every citizen in the U.S. has a social security number and it can't be the same as another person's. The IP address can also be used by servers to send the appropriate information to your computer and not someone else's.

2. IPv4 (Internet Protocol version 4)
    a. Internet Protocol version 4
    b. IPv4 gets its name by having 4 bytes of 8 bits. (1 byte = 8 bits). Add it all up, its 32 bits.
        i. Decimal notation goes 00000000.00000000.00000000.00000000 ← that's 32 0's for those that don't want to count them all.
        ii. The bytes are measured in 1's and 0's. You can calculate your IP address given the bytes.
        iii. You can have an example like 10101100.11000101.11111111.00000001.
            1. You can calculate what your IP is by knowing your times table. Starting from the last number all the way to the right (8^{th} place from left), you multiple it by 1. The next number (7^{th} place from the left), multiple that by 2. The next, (6^{th} place), multiple that by 4. Then (5^{th} place), x 8. And so on. Here's a chart.
            2.

N^{th} decimal from the left	Multiply that by
8^{th}	x 1
7^{th}	X 2
6^{th}	X 4
5^{th}	X 8
4^{th}	X 16
3^{rd}	X 32
2^{nd}	X 64
1^{st}	X 128

            3. After you multiply those 1's and 0's, add them all up (the non-zero numbers) to get your IP address.
            4. 10101100.11000101.11111111.00000001 = 172.197.255.1
                a. ^^ Currently that IP address traces to someplace in Sydney, Australia.
    c. This is the standard IP address that is used today, however there is more devices connected to the internet now than ever before. They're running out of permutations so they created IPv6. More on that later.

3. IPv6 (Internet Protocol version 6)

a. Similar to IPv4 in the way they are used to identify computers but because there are more and more computers, they're running out of permutations for the 32-bit IP addresses.
b. IPv6 instead is almost entirely different where it uses hexadecimal inputs rather than just numerals like in IPv4.
    i. Aka – They have letters in them too.
c. Not all systems support IPv6 yet but a lot of companies are making ipv4 and ipv6 in the same computers as a default.
d. For what we're required of for BUS 175, just know that IPv6 is different than IPv4.

Client/Server IP Addressing

As previous mentioned, every computing device has a unique IP address. Clients (you) have a different IP address than with servers (the webpage/database/cloud/Russian military). However, because we're human and not robots, we tend to remember cnn.com rather than 151.101.0.73. ←Actually, points to CNN's server…lol. When working locally though, your router will assign your IP address a different IP address to help protect your computer from the outside world.

This concept is through DHCP.

1. DHCP (Dynamic Host Configuration Protocol)
    a. The protocol that pre-configures dynamic IP addresses for a router through a scope. Think of this as the rental car agency. You go in and say you need a car. That is a DHCP request. They respond back to you and say, OK, this is what we have (DHCP offer). In that offer, you get your car (dynamic IP), the information where the car is from (subnet mask), and how long you can lease it for before having to rent it again (lease time).

2. Dynamic IP Address
    a. When working locally, your router wants to protect you and it will assign you a short-term IP address that changes. This is called a dynamic IP address. I guess an example of this will be renting a car. You'd be able to hold on to the car for a day, week, month, etc. until your lease is up. Then you'd have to return it. Dynamic IP addresses can be assigned to more than one computer, but only once at a time.

3. Subnet

   a. A sub network (smaller network) within a larger network. Concept only used in IPv4. Primarily used for network management and origination within a closed campus. Aka, UCR and its different departments.
4. Subnetting
   a. Subnetting is where you take many IP addresses in a LAN through a gateway to look for the real website you're trying to get to. To explain further, think about each one of us (students) is/are an IP address. To get to SoBA from OLMS 421, we all would need to go through the door (gateway) to find where SoBA (the real website) is. That's my best explanation. Ask Satpathy for further clarification or learn from YouTube.

5. Subnet Masking
   a. Subnet masking is a tricky concept that even the most well versed technical guys have difficulty with. In the 'real world' outside of textbook, subnet masking is determined by which network pathways can be used in accordance to the hosts and records. I don't even really understand it tbh. Still learning ~

6. Network Address Translation (NAT):
   a. Normally found and used in routers, NAT converts your computer's public IP address (your 10.23.45.1234) to a 192.162.2.38 number to a private IP address. Translates local IP to global IP.

Domain Name Servers (DNS)

To understand Domain name server, first you need to know what a domain is. Google.com is a domain. Facebook.com is a domain. Jonathanng.xyz is a domain. Ok, you get the point.

1. DNS – Domain Name System
   a. The internet equivalent to a phone book. The DNS server is pretty much a lookup table of the domain names and associates the domains to IP addresses. For instance, the domain CNN.com is 71.53.22.2222 (or something like that).
   b. **From lecture notes**
      i. DNS gives us IP mapping
      ii. Provides aliasing
2. Name servers
   a. DNS points to name servers which in turn forwards you to the domain's IP address you wanted to go to.
      i. Ex – I want to go to www.target.com. First, it would go from browser → dns servers → name servers → real target.com.
3. Cache Files

a. "Catch files" 'caught files'. Automatically catches your web browsing history and stores little bits of cookies there so that the hungry web browsers will find it faster. This is all done on your personal computer.

Data Center Computing

If you've read up to this far, congrats. I don't even know how I did it. I just want to watch Netflix.

Ok, data center computing.

1. Data Center Computing
    a. Essentially, a data center is the brain of the company where most of the computing needs of the corporation is being processed. It normally is the center of the most important things in a corporation because all business typically run through a data center nowadays.
2. Tiers of Data Center Computing
    a. The data center tiers are measured from Tier 1 – Tier 4.
    b. Classified by how probable the server is to failure or downtime and the amount of backup computers they have to handle the failure.
        i. Tier 1 has the highest rate of failure because they only have 1 computer running the server = 99.671% uptime
        ii. Tier 2 has 2nd highest failure rate since they have the server and 1 backup = 99.741% uptime
        iii. Tier 3 has 1 server and 2 backups. = 99.982% uptime
        iv. Tier 4 has 1 server and 3 backups leading to a 99.995% uptime guarantee.

3. Datacenter: Horizontal Partitioning
    a. Splitting the database records / ***rows*** to make it easier and more efficient to find.
    b. This can be conceptualized through taking a set of 50,000 addresses and dividing them into 2 or more tables by zip codes.
    c. This way the information is the same but just organized differently.

4. Datacenter: Vertical Partitioning
    a. Splitting the database records / columns to make the tables more organized; efficient.
    b. Conceptualized through 'normalization' and 'row splitting'
        i. Normalization

1. Making the table 'normal' by cleaning up unnecessary and redundant information and putting them into another table where it belongs.

ii. Row Splitting
    1. If you're taking 173, this applies. This concept is when the columns are organized, it can take the organized rows and match them with another data set from another database using unique keys. In a way, this is the concept of a password.

Methods of Database Processing

There is more than one method for data processing. Data servers can be in one location and locked up like a jail cell onsite in a closet somewhere or they can be dispersed across many places. These include centralized data processing, decentralized data processing, and distributed data processing.

1. Centralized Data Processing
    a. It is exactly as what it's titled as. Centralized. This method is where all processes happen onsite. There can be pros and cons for this but that's up for debate. Consider this concept a consolidation of tech resources. Typically, this is based around mainframes. (large supercomputers)
2. Decentralized Data Processing
    a. Not in one location. (Thanks Sherlock). Is dispersed across many servers and/or locations and departments. Data servers can benefit from decentralized datacenters since it would allow the businesses to choose hardware and software based on their needs. Ex – you wouldn't want accounting software on a datacenter dedicated to rocket science.
3. Distributed Data Processing (DDP)
    a. Computers & servers are dispersed across an organization where information is copied on all computers once something is changed.
    b. It is scalable meaning that the company can increase the size or decrease the size of what they need.
    c. Goal is to process the information that is most effective use of their resources.
    d. Usually done with smaller computers and not mainframes.
    e. All connected to each other with access to each other's data. (I still need a bit more clarification on this too).
    f. Hadoop clusters are part of a DDP but only exist to decrease the time it takes for information to pass through. Apparently, they're also called 'shared nothing' systems since if it fails, no information is lost because changes are copied to all servers.

BUS 175 Networking Basics Course Guide

Virtualization

1. Setting up a computer for it to host multiple virtual (cloud) servers on a single physical server at once.
    a. Satpathy said that this can be done by 'slicing' the physical server into one with Windows, one with Linux, one with Apple. ← This one Is operating system virtualization. It can be done with servers, client, software, etc.
    b. If you don't understand, think of it as a multi-use server. You can do a lot with it.
2. Every time something is installed on it, the software is called 'instances'.
3. There is more than one type of virtualization.
    a. Operating System Virtualization
        i. Running Windows/Mac in the cloud.
    b. Server Systems Virtualization
        i. Running Linux / Windows servers in the cloud.
        ii. Don't know if Mac's are generally used as servers….
    c. Storage System Virtualization
        i. Meaning a place to keep all your files and stuff…but this can also be accomplished by the first two listed.

Internet

- To get onto the internet, your computer must go through an Internet Service Provider (ISP) that connects you to another ISP. They are the middle man between you and the website you're trying to get to.
- Internet is when computers are connected to each other OUTSIDE of the internal network.

Intranet

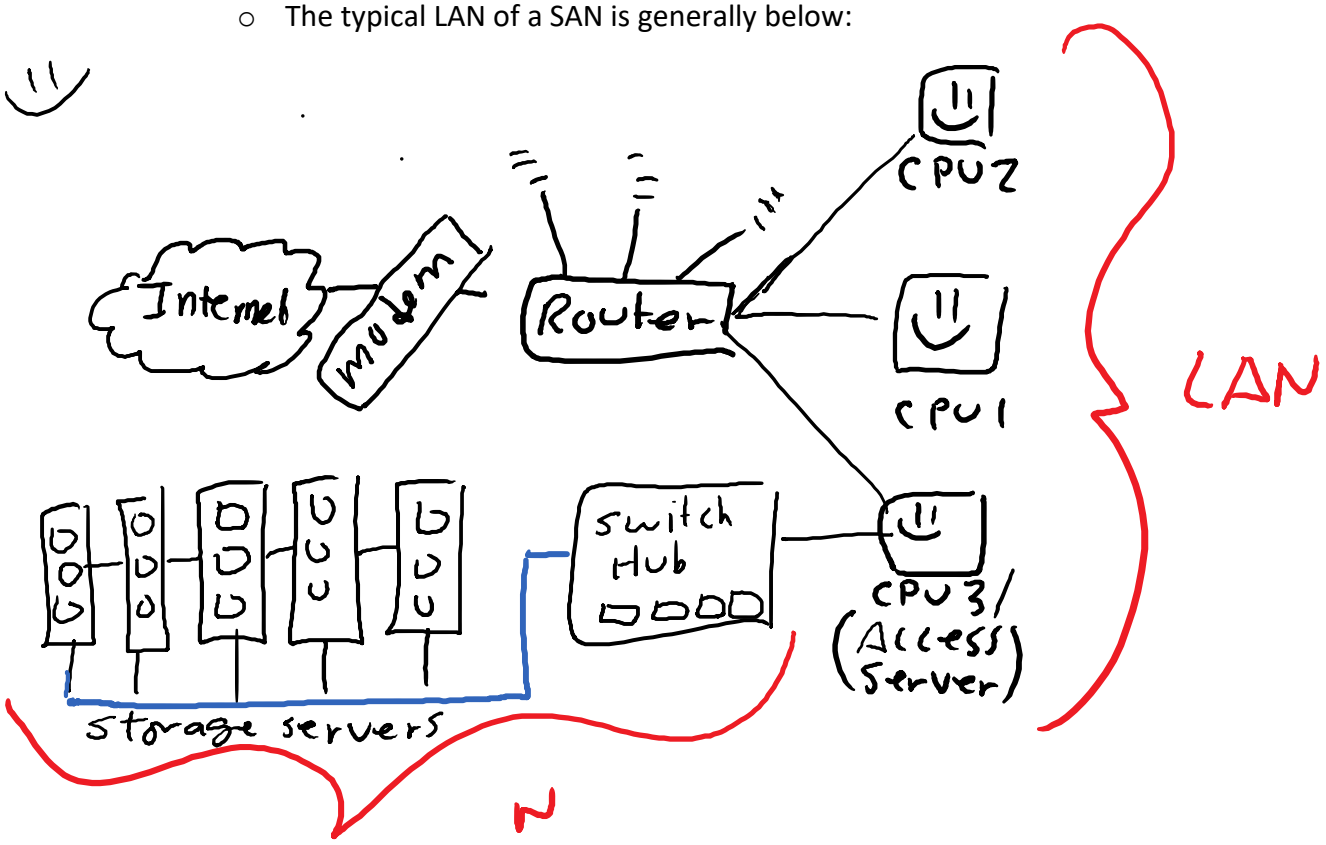
- An intranet is different than an internet. Be very careful not to get these two mixed up.
- Intranets are generally computers that are connected to other computers WITHIN a network or general area/vicinity.
    - Think Internal safeguards. That's what an intranet is.
        - Example: If you're not a UCR student/ on campus, you can't access those Mergent database that UCR library offers. That database is part of an intranet.
- Intranets, although connected to other computers within a network, they also use Internet based protocols – TCP/IP for local networking and Wide area networking (WAN) and sometimes even MAN's. Sometimes bigger.
- Intranets, like subnet masking, can easily be managed within a network but once you go out to the internet…it's like going into the ocean. Good luck with that.

Extranet

- Extranet's are similar to Intranets but they do have differences in the way that they are designed.
    1. Despite intranets being internalized, extranets provide side doors to let other people / vendors access the network as well.
    2. This can be for many reasons including, but not limited to,
        a. Financial audits
        b. Security
            i. Aka – police sharing their files with the FBI.
        c. Accounting
        d. Etc.

Storage Area Networks (SAN's)

- Storage Area Networks are networks that are dedicated to, well… storage.
- It is considered to be a separate network to handle storage needs.
    - Its also important to note that a SAN, although is its own network, is still connected locally to a LAN.
- SAN's can also be compared to data centers in the sense that SAN's have lots of servers there. Not for processing like data centers, but just for storage.
    - The typical LAN of a SAN is generally below:



SA

- Please forgive my drawings. I know, its ugly.):

OSI Model (Open Systems Interconnection)

- According to the book, the OSI model is a model of communications between cooperating devices. ← that sounds pretty boring.
    - In my terms, the OSI model is the model that highlights the entire process of data travel. I think my definition sounds better.
    - Note that the OSI model is only a concept and is not really used in practice.
        - The ones that are used in practice today is the TCP/IP model. It's similar but it has its differences.
    - To better understand this, you'd need to know that there are 7 Layers (aka steps) to the OSI model.

        - Starting from the very first layer (the origin layer) is the Application layer, then it goes to Presentation, Session, Transport, Network, Data Link, Physical link.
        - You may find the mnemonic device "Please Do Not Teach Students Pointless Acronyms" useful if you think of it from Layer 1 to Layer 7.
    - **Layer 7 (Application Layer) – Open envelop**
        - This is where you interact with the data whenever you request/receive webpages or whatever. Think of it as being named application because you're using an Application (your web browser) to see the data.
    - **Layer 6 (Presentation Layer) – The pretty envelop in your hand**
        - This layer is when your computer wants to present itself and the data in the best way possible. In this layer the webpages will make itself pretty for you to look at before you interact with it.
    - **Layer 5 (Session Layer) – When mailman is handing you the mail / you giving mailman mail.**
        - In this layer, the data packets talk with your computer to let that data in. Once its in, it's in session. Like at an airport when the air traffic controller tells the planes that they can land. Once those pilots land the plane, the session is on to get passengers on/off board.
    - **Layer 4 (Transport Layer) – In the truck to be delivered to/from post office.**
        - When the data packets are en route to your computer.
    - **Layer 3 (Network / Internet Layer) – Post office**

        - This is where most of the behind the scenes networking concepts are. In this layer, data packets are being routed in the right direction before its en route to you.
    - **Layer 2 (Data Link) – Mailman's collection bag /delivery bag**
        - An example of this is when data is ready to be on its way. Similar to your snail mail is in the truck and almost out for delivery.
    - **Layer 1 (Physical Link) – Your mailbox**
        - This is where the requests are made / received.

The OSI model is pretty easy to understand assuming you can follow the steps on how a post office system works...conceptually speaking.

Protocol Data Unit (PDU)

- There is not a good definition of what a PDU is anywhere so here's my best shot at explaining it.
- A PDU is a name for the data at each layer of the OSI model.
    - In Layer 4 Transport, the data is called "Segments". The PDU for layer 4 is "Segments.
    - In Layer 3 the data is defined as packets. The PDU for Layer 3 is "Packets".
    - Layer 2, Frame. Layer 1, Bits. Layer 5 and above, it's just called data.

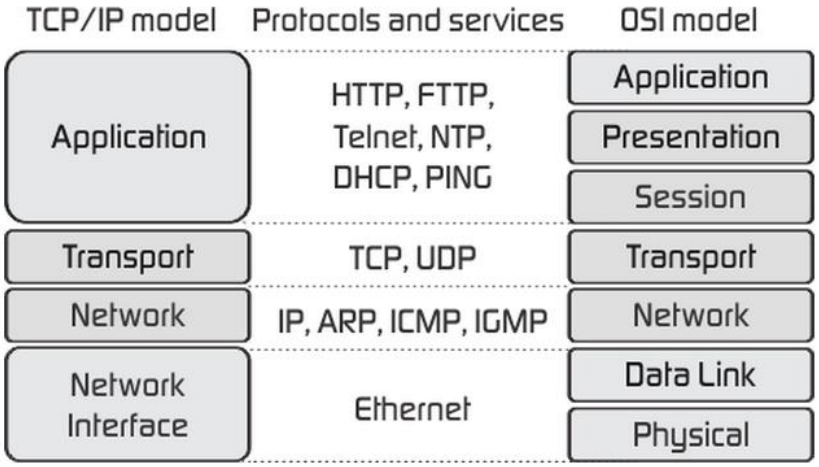
User Datagram Protocol (UDP)

- The OSI model offers two different networking protocols in Layer 3 – TCP and UDP.
- With UDP, the protocol was established before TCP/IP and it boasted a lot of problems.
    - For starters,
        - UDP does not guarantee delivery, does not preserve sequence order, or protects against duplication.
- UDP is not common but there are applications that do actually use it…still. The book states that one application Simple Network Management Protocol (SNMP) uses it but other than that, it is archaic and is not efficient.

TCP/IP (Transmission Control Protocol / Internet Protocol)

- TCP/IP was developed after UDP has failed to do what those CS guys back in the day wanted it to do. Although UDP has some pretty good functions, TCP included UDP features while developing TCP/IP.
- TCP/IP is similar to the OSI model but in this model, it consolidates the OSI layers into 4 layers…that and it renames it too.

- One thing to note is that TCP/IP model works almost entirely in Layer 3, Network/Internet layer.



- Be careful to also note that TCP / IP model uses a 3 tier/ 3 layer model.
    - Networks
        - This includes the Network Access layer where all information goes in/out of computers
    - Computers:
        - We need computers to even host this scenario.
        - This layer would also play hosts in transporting data packets from one computer to another.
    - Applications
        - Similar to the OSI model, applications are specific software that are used to access the network / programs you are running.

Connectionless

- According to technopedia, connectionless is when there is no structure in the data when computers are exchanging information with each other. On top of that, connectionless data transfers are when computers would be receiving data whether they like it or not. This is generally practiced in UDP and IP transmissions but because it is unorganized and unstructured It is not commonly used anymore without the presence of TCP.

Connection-Oriented

- Like connectionless and my research on technopedia, connection-oriented means that prior to any data being sent or received, a connection must be established. Additionally, Connection-oriented practices follow a structure (similar to the OSI / 3 layer concept) when establishing communications between computers. With connection, oriented methods, data packets can be traced within each layer of data transmission/receipt. It is important to know that in connection oriented concept, both computers / hosts/ clients

would have to be able to send and receive data transmissions. If they can't, the practice would be connectionless.

Wireshark Legacy / Wireshark Network Analyzer

- In lecture, Professor Satpathy introduced Wireshark to us to analyze packets and data.
- In the event that he asks us what Wireshark is/was used for, it is to analyze packet data that we can use to monitor bandwidth, detect network intrusions, and diagnose problems at the network level (Layer 3 – Internet / Network).

From here on out, everything covered below is catered specifically towards the FINAL EXAM.

A few definite things we know about the final.

- It will be 50 question Multiple Choice.
- Covers Ch10, Ch12, Ch13, Ch18, Ch19.
- It will be in our regular room on March 20, 2017 from 8:00 AM to 9:30 AM.

Here we go.

Chapter 10

- Chapter 10 covers all internet based "Applications". These applications can be anything from your web browser to the e-mail protocols you use. Everything that is covered in this chapter is focused around the Application Layer of the OSI/TCP/IP model.

  Beginning with what we all know as E-Mail, there are different protocols for e-mail.

  - Should a question arise on which request for comment (RFC) it came from, it came from RFC 5598 – though I highly doubt there'll be a question like that.
    - E-Mail is structured through
      - Message User Agents (MUA) – Also known as User Agents.
      - Message Handling Service (MHS)
      - Message Transfer Agents (MTA)
  - Message User Agents
    - A program that allows to send and receive e-mail messages.
    - Layman terms – E-mail Program
      - Aka Outlook, or the Gmail App on your iPhone.
  - Message Handling Service (MHS)
    - Has no significant meaning besides being a middle man between the two e-mail servers / programs.
    - These are the servers that messages bounce off of.
  - Message Submission Agent (MSA)
    - GMAIL servers & Hosting Servers where they messages are first sent over.

- Message Transfer Agent
  - These are all the computers in which the path of data flows closer and closer to the recipient data.

- Mail Delivery Agent (MDA)
  - Delivers the contents of the packet to the store

IMPORTANT TO KNOW:

Each step is transferred through SMTP until it gets to the message store. That is where IMAP and POP3 happen.

- Message Store
  - Where all the e-mails are stored until they're taken and opened through IMAP or POP3.

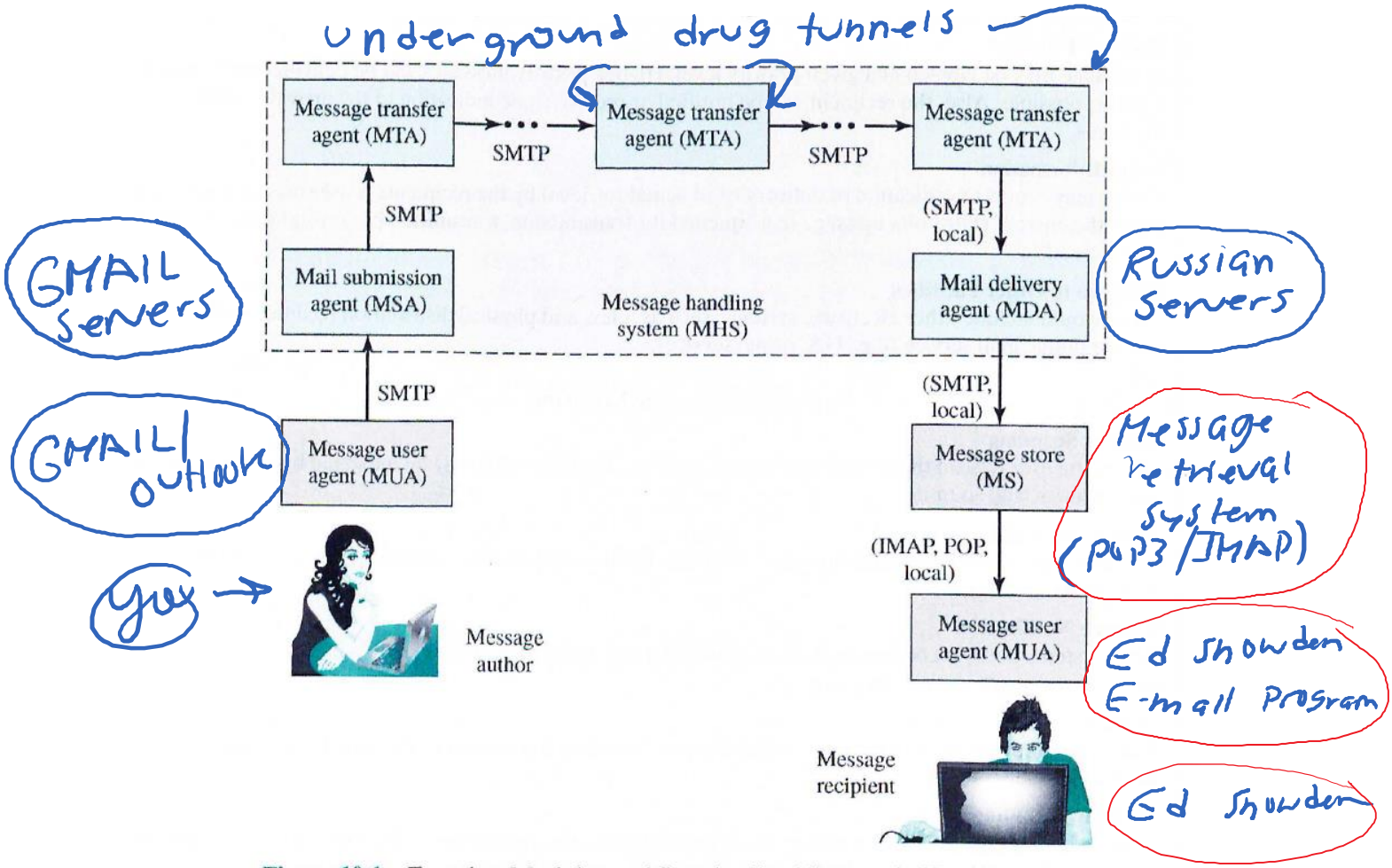


Figure 10.1 Function Modules and Standardized Protocols Used Between Them in the Internet Mail Architecture

I know, I know, the concept of it is difficult to grasp. Let me try and explain it a little bit further. Think of it this way. You need to send a package of pasta sauce to Satpathy. You would package it up (You), then you would get into (Your Car) to go to the (Riverside Post Office). From there, the post office takes it and gives it to the Riverside mail man which then gives it to the Pasadena Mailman, and then gives it to the Arcadia mailman (MTA) and then it gets delivered to the Arcadia post office (MDA). Because Satpathy is super cheap he shops at KMART and Kmart unpackages the items sent to Satpathy and when Satpathy goes to the store, he has to read every single label to make sure it fits his dietary needs (MS). Then he gets in his car (MUA) and then finally makes the pasta sauce for dinner (Message Recipient).

Message Author	You
Message User Agent (MUA)	Your Car
Mail Submission Agent (MSA)	Riverside Post Office
Mail transfer Agent (MTA)	Riverside Mailman
Mail Transfer Agent (MTA)	Pasadena Mailman
Mail Transfer Agent (MTA)	Arcadia Mailman
Mail Delivery Agent (MDA)	Arcadia Post Office
Message Store	Shelf of Items at K-Mart in Arcadia
Message User Agent	Satpathy's Car
Message Recipient	Satpathy

Important things to note/understand:

All internet traffic, whether it's the email architecture or basic Facebook browsing, uses ports to let information in and out of your computer.

PORT

- An internet port is pretty much windows in a house. You can let air in through all your windows or you can specify which window you want air coming in/out of.
- Ports can usually be configured through your Mac/Windows operating system and/or router interface and/or Wireshark for that matter.

Post Office Protocol (POP3) (Port 110)

- The Post Office Protocol is a protocol that allows users to download messages directly from the e-mail server.
    - After the download to your phone or computer, the message gets deleted from the e-mail servers.
- The protocol is connected through **TCP/IP Port 110.**
- The 3 in Pop3 is Version 3.
-

Internet Mail Access Protocol (IMAP) (Port 143)

- Unlike POP3, IMAP is downloads a copy of the e-mails to your client and allows you to access mail on e-mail server.
- IMAP has stronger security measures
- Protocol is connected through **TCP/IP Port 143**
- Defined by RFC 3501.
-

Difference between POP3 and IMAP:

- The difference is pretty much POP gets downloaded to the device and then immediately deleted.
- IMAP gets downloaded on the device and a copy is left on the original mail server.

Simple Mail Transfer Protocol (SMTP)

- Only used when transferring mail from one user agent to the Mail Transport Agent (MTA) to another (MTA) and so forth.
    - Important Note: It does NOT include the Message Store to the Message User Agent.
- Almost entirely encoded in ASCII and binary.
- Defined by RFC 882 (dunno if we need to remember that).
- Can trace SMTP at each step since it keeps a log of where that message has gone through.
- E-Mails are sent through SMTP.
- Has certain restrictions since it can't transport large files (that's where you use FTP).

Multipurpose Internet Mail Extensions (MIME)

- According to the book, it supplements SMTP so essentially it doesn't have a port number. (I think). Apparently it also allows for more encapsulation of multimedia.
- Cannot transport text data of foreign non English symbols or letters since they're not represented by 8 bit, 128 decimal encoding.
- Defined in RFC 822.
- Must be encoded by 1, or 0. ← Parameter values.

The above protocols are just some protocols that use ports. There are other ones that you should know and I have a feeling that Satpathy might include these on the exam as well.

File Transfer Protocol (FTP) (Port 21)

- This protocol is commonly used when uploading or downloading large files. The book didn't really talk about it but Satpathy did mention it quite often in class. I have a strong feeling this is going to be on the exam. Remember, port 21! If theres a question about Secure FTP (SFTP), it's port 22. It just adds a secure layer to it.

Hypertext Transfer Protocol (HTTP) (Port 80)

- This is what we use to browse the web and everything.
- HTTP is considered a transaction oriented client/server protocol.
- Makes use of TCP to initiate the transfers and provides reliability among the transfer.
- HTTP is also considered a stateless protocol.
    - According to lecture, stateless pretty much means that the server does not remember the previous history. When you browse incognito on Chrome or in Private mode, you are operating on a stateless connection. Cookies on the other hand are NONSTATELESS since they track everything you do.
- Stateless is treated independently.
- HTTP is also considered to be all ASCII and NON-binary
    - Meaning that it's not encoded in 1's and 0's.

Proxy

- A proxy is an IP address that is not your own.
- Think of it this way – When we were in high school and tried to go on Myspace back in the day, the computer lab computers blocked us. What we could have done is google "proxy server" and it would pretty much masks your IP and the server on the other end would see that its coming from an IP other than your own.
    - On another note, a VPN is similar to a proxy in that it uses a different IP than yours.
    - Although, ***DO NOT THINK THAT A VPN IS A PROXY. Its completely different.***
        - *It's just similar in that regard.*

Secure Socket Layer (SSL)

- SSL's are secure layers that run on the application layer of the TCP/IP model.
- The SSL directs data to specific ports that have a Secure header on it only to be read by those secure servers on it.
- SSL's can run on FTP and on HTTP, indicating that the sockets (ports) that the information is talking to only runs on SFTP and HTTPS. (The S's stand for secure).

SSL Categories

Pretty sure he's going to ask us this question. "Which of the following is NOT …blah blah."

- **Confidentiality**
    - Encrypted data between two applications.
- **Integrity**
    - Assures that the data is not altered or substituted on its way to you.

- **Authentication**
    - Validates identity on both partners of the exchange.

Three Forms of Intermedia System defined in HTTP

- **Proxy**
    - Stated above. Look up ^^.
- **Gateway**
    - The "gateway" to the internet. Aka your router.
    - It acts as an intermediary and gives your computer a 'public' IP address and instead of 71.123.222.1, it will show other networks or something 192.121.0.73.
    - A gateway is also a NON-HTTP server.
- **Tunnel**
    - Remember when I talked about a VPN? A VPN is practically a virtual tunnel. A tunnel is pretty much what it is. Practically a shortcut / direct route to the other computer you're trying to get to.
- **Cache**
    - Catched' files. Cache files = catched files. Like it stores information in your browser so it loads faster when you return to that page again. Not necessarily an intermediary, but I guess if you really want it to, it could be since you're going to the cached' files first before the actual URL.

Ok, now that I've practically defined what all those protocols and HTTP stuff, we're going to go into bandwidth. Professor Satpathy stated in class that we're expected to know what bandwidth is and the different frequencies it travels in. But first, let's define bandwidth.

Bandwidth:

- Bandwidth is pretty much the amount of data/frequencies that can be transmitted through a datalink.
- It can be measured in either the analog state (cables) or through Wi-Fi.
- Bandwidth is highly scalable and can be increased by adding more peer to peer computers to lessen the load of utilization.

Internet Service Provider (ISP)

- Exactly what you think it means.
- They're the ones that supply you how much bandwidth you get.

Peer to Peer (P2P)

- BitTorrent
- Skype

BUS 175 Networking Basics Course Guide

CHAPTER 12: LAN Architecture and Infrastructure

Chapter 12: LAN Architecture: focuses the physical aspect of internet/network connections. (Ex: cables, router, switches, etc.).

LAN: Local Area Network

- The network in which all computers are connected to.
- There are different LAN's. Not just a LAN.
    - There's WLAN and more. (W = Wide LAN).
- There are also many characteristics of a LAN.
    - From Satpathy's slides:
        - High data rate, high-speed interface, distributed access, limited distance, limited number of devices.

In order to even have a LAN, there needs to be the physical layers to it all.

In this case, Ethernet cables (not to be confused with internet cables) transfer information through the wires inside the cables.

In lecture, we learned about UTP (untwisted pair) and STP (shielded twisted pair). However, there are a few more cables out there.

Transmission Medium

- Quite literally the physical layers connecting to your PC/Mac to the routers. Or if you're on Wi-fi, the cable connecting the modem to the wireless router. The transmission is in the form of **electromagnetic waves.** (aka Microwaves)

These physical cables/connections include:

- Guided transmission media
- Unguided transmission media.

Guided Media transmission

- The waves (information) are guided along a solid, physical cable usually made up of copper.
    - Can be in twisted pair, copper coaxial cable, or through optical cables.
        - Fun fact about twisted pairs
            - They are twisted because each cable has about 2-3 wires in them, each with a positive and negative electromagnetic field. It is twisted so that the cables together cancel out the magnetic field and has a higher rate of successful data transfer (throughput)
- **Throughput:**
    - Synonymous with transfer rate. Normally reflects the successful transfer rate.
- The cables/medium are more important in determining how fast the speeds of data transfer can go.
    - **Different Cables offers different Speeds**

- UTP = Unshielded Twisted Pair
  - Is generally a telephone wire or internet (voice) wire.
- CAT3 UTP = Transmission Speeds up to 16 Mhz. ← This sucks. No one uses this unless they're in 1960's or so.
- CAT4 UTP = Transmission speeds up to 20 MHz
- Cat5 UTP = Most commonly used today at 100 Mhz.
- CAT5e UTP = Implements new LAN capabilities
- CAT6 UTP = Supports performance up to 250 MHz
  - Tbh, I don't think he's going to ask us the speeds of these.

Although you might not need to know the MHz it runs on, you DO NEED TO KNOW what the BASE-T and BASE-TX means.

- **T & TX = Twisted Pair**

Data Collision & Data Loss

- This occurs when multiple clients are sending data all at once.
- Think about yourself at a Rave seeing Martin Garrix or someone. You try and make a phone call or send a text. You can't. This is a result of data collision and thus, becomes data loss.

Time Division Multiplexing

- Gives clients a certain time window to send data
- Establish connection on a clock for when certain times run out

Frequency Division Multiplexing

- Sharing by dividing the frequency.
  - Sending the signal (tuning in the radio station) to receive certain types of data.

Collision Detection

- A program / hub that is always listening to determine if there is any collision of packets.
- ^^ this is a bad definition but please, its 1:35 AM rn and I've been working in this since 7 PM. My god.

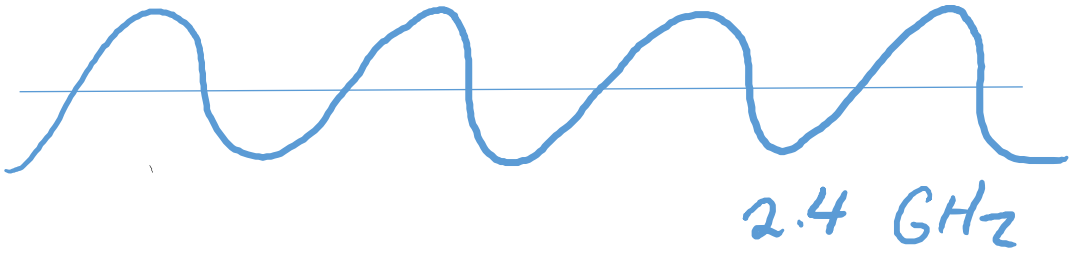
- CSMA = Carrier Sense Multiple Action with Collision Detection
  - Can be also referenced as Collision Detection

Unguided Media Transmission

- Wireless (Wi-Fi)

Bandwidth is more important in unguided media transmission.

- Usually measured in Gigahertz (Ghz) bands.
  - 2.4 GHz or 5 GHz bands.
    - The 2.4 Ghz is wider wavelength and can reach a further range (distance), though it is often congested and you might experience slow speeds.
    - It also has a higher penetration.



- 5 GHz band is a narrower baseband where it doesn't have as much penetration distance as 2.4 GHz but at the same time, it's also a lot less congested – meaning speeds (at this current time) are probably faster on a 5 Ghz band.

Attenuation

- When Wi-Fi signal gets weaker the further you go and if gets weaker if there is interference between you and the signal.

LAN Protocol Architecture

IEEE 802 from the institute of electrical engineers in clause 802 deals specifically with data links.

Insider the mediums of guided transmission mediums comes the LLC and MAC.

Media Access Control

- The MAC resides in Layer 2 of the OSI model (Data Link layer).
- The MAC serves to assemble data into frames with addresses with error detection fields and disassembles the frames when it is received. The MAC also governs the LAN transmission medium.

Logical Link Control

- Provides an interface to high layers and perform flow and error control.
- Specifies network layer and media access control sublayer of the data link layer.
- Enables LAN's with different MAC protocols.

BUS 175 Networking Basics Course Guide

CHAPTER 13 (goddamm. Finally,)

1. **Physical Topology**
    a. Essentially this is called a broadcast domain.
        i. **Bus topology**
            1. Only one conversation can happen at a time
            2. Transmission from one system travels an entire medium.
            3. Every node / end receives messages but ignores it if the MAC is unmatched.
        ii. **STAR topology**
            1. They are simple and maintainable.
                a. It is easy to maintain.
                    i. IF the central node is down, the entire network would be down.
                    ii. IF the control node fails, the entire network is dead.
                b. Under what circumstances would you use a STAR topology?
        iii. **Ring Topology**
            1. Last node is connected back the first node (any computer can be first or last) to form a closed ring
            2. The way this works -- the packets -- travel on the loop from node to node until the design node is reached.

Power over Ethernet

- The power over Ethernet concept is actually pretty fascinating. Rather than just sending electrical data pulses through Ethernet, the cables now can actually power a phone or anything by using TWO or MORE TWISTED PAIRS in the Ethernet cable to distribute the power.
- Other pairs in the Ethernet cable would be used to transmit data.
- Switches and arrays primarily power the supplies in PoE networks.

Advantages in having power over Ethernet.

- Cheaper to use where AC power is expensive or inconvenient to power network devices.
- Can be deployed using CAT5 UTP cables – way less expensive than using AC wires.
- Superfast Gigabit internet connections are possible
- Can be deployed in buildings and don't have to worry about the electrical codes
- Can work internationally

CHAPTER 18: **Network Security**

Objectives of Computer Security (CIA Triad)

- **Confidentiality**
    - Pretty much self-explanatory. People don't want their secrets exposed. Remember the AshleyMadison hack? Aka Privacy.
- **Integrity**

- Involves that every data bit is consistent with each other and that the accuracy and trustworthiness of the data is legit. Data cannot be changed in transit or what not. SSL/SSH ensures that this does not happen by directing them to very specific ports.

- **Availability**
  - Making sure that absolutely nothing goes wrong. Performing hardware repairs immediately so that there isn't any conflicts with system software. By doing this it can prevent any bandwidth bottlenecks and can prevent a DOS or DDOS attack.

Malware: A malicious software that has 2 components.

1. **Propagation mechanism**
   a. The way the malware object spreads.
      i. What are the way it spreads from point A to point B?
2. **Payload**
   a. The malicious action that the malware performs.
   b. What takes place after the propagation is done.

Propagation Techniques

- Viruses (spreads from system to system based on some kind of user action).
  - We can only get the virus propagated from point A to point B provided the user is taking action.
    - Only happens when users perform certain things:
      - Clicking something,
- **Worms**
  - Spreads from system to system without any human intervention.
    - Example of a worm: Stuxnet
    - In order for worms to work, you have to have vulnerable systems.
    - Most of the time, the possible solution is to update your system regularly with the most recent OS.
- **Trojan Horses**
  - Disguise themselves as a beneficial program.
  - Deliver malicious payload behind the scene.
  - Act as advertised when they run.
    - Application control is important. Restrict the right version number.

Malware Payload:

- **Adware**
  - Displays ads for malware authors.
  - Pop ups
  - Pop windows
  - Replaces legit ad with author's ad.
- **Spyware**
  - Gathers info without user's knowledge.
  - Sends back info to the malware author.
  - Key loggers
  - Monitors users web browsing.
  - Search your hard drives and cloud space.
- **Ransomware**
  - Blocks access to user's files until the author gets paid.

        - Ex: Crypto locker
            - **Comes via e-mail.**
    - **Preventing Malware**
        - Firewall
        - Encryption
        - User Education
        - Security Patches
        - Anti-Malware software

    - **Logic Bombs**
        - Targeted payload
        - Works when a certain condition is met.
        - Date/Time reached.
- **Botnets**
    - Collection of zombie computers used for malicious purposes.
        - Renting out computer power
        - Delivers spam
        - Engages in DDOS Attacks
        - Performs brute force attacks against passwords.

DOS Attacks:

- Makes resources unavailable to legitimate users.
- Send a huge number of request to servers.
- Difficult to distinguish from legit request.

Limitations of DOS Attacks:

- Requires massive network bandwidth
- Easy to block IP addresses

Distributed Denial of Service Attack [DDOS]

- Botnet
    - We start with a bot
    - Bot sends an echo request to a server.
    - Servers will give an echo replay.
- Preventing DDOS attacks:
    - Security Layer from ISP will always give your IP address out.

Eavesdropping Attack

- Relies on communication between client and server.
- Network Device Tapping
- DNS poisoning
- ARP Positions

- Most dangerous attacks are the insider attacks.

  Data that shared with you:

  51% of org of security breach was done by insider attack.

CHAPTER 19:

BUS 175 Networking Basics Course Guide

Social Engineering

- Authority Trust
- Intimidation
    - Basically, go in and scare people.
    - Boss in trouble, will lose job if he won't do it now. Wife's case.
    - Essentially forcing someone to do something stupid.
- Consensus
    - (Social Proof)
- Scarcity
- Urgency
    - Time is running out
- Familiarity / Liking
    - When you're trying to do some social engineering act, you must be likeable.
    - That way it is easy for that person to say yes.
- Shoulder surfing
- Dumpster Diving
- Tailgating

Impersonation Attack:

- Spam (unsolicited Attack)
- Phishing (Stealing credentials)
- SpeakPhishing (Targeted phishing)
- Pharming (Using fake sites)
- Whaling (targeted attacked on executives)
- Vishing (voice phishing)
- Spim (spam on Instant message)
- Spoofing (Fake IM identity)

Different Types of Wireless Attacks:

Wireless Attack

- Compromise a wireless network
    1. Wi-Fi Password Protected
        i. Ex: Starbucks -- LAN not safe.
- Offer free Wi-Fi to create a persona to that profile and start marketing.
    - Encryption is the key.
- Option 1: You can opt to use no encryption
- Option 2: Wire equivalent privacy (WEP) <-- uses static key.
- Option 3: Wi-Fi Protected Access (WPA)
    - Uses Temporary keys
    - Changes keys for every transaction
- Option 4: WPA2 - Very advanced encryption standards.

Jamming / Interference

- War-driving
    - Drive around neighborhood and find open access points.
- Wigle.net (example site)

Application Attacks

- Webgoad
- Cross site scripting attacks (XSS)
- An attacker tricks a user's browser into downloading a script from one site and executing it on another site.

Am I missing anything?

- Let me know if there's something that I may have missed or if you need clarification on my writing. Thanks, guys!

The End

This is how much we've covered in class. It has been a long journey updating this guide for you all to benefit from. Hopefully I helped you understand this a little bit better and may earn you a point or two more on the exams. If you need extra help, feel free to shoot me an e-mail at jonathanngw@gmail.com or FB messenger me. FB messenger would probably be the fastest way to get a hold of me. Study hard everyone!

-Jonathan