Dijkstra’s Algorithm

* Don’t need to be in depth about the equations
* Conceptual questions
* Not a memory recall test

Understand bellman-ford (how it works) & distance vector algo

Challenges associated with inside and outside routing domains

OSPF & BGP

* Be aware of them and how they are used
* Differences between the two
* eBGP vs iBGP (edge routers run both protocols)

Link layer services

* What does the link layer need to accomplish
* How it uses the MAC address
* Know MAC addresses quite well
* Difference between MAC address at the link layer and the media layer ? (both use MAC)

Error detection

* Why use it, where is it applicable, \*\*it is NOT 100% reliable – understand why\*\*
* Single and two-dimensional bit parity (be able to calculate for either one, know if an error exists)
* What can two-dimensional bit parity provide for us? \*\*very important\*\* (compared to single bit)

Cyclic redundancy check

* Make sure you know how to calculate a CRC (polynomial calculation), follow example from textbook

Multiple access protocols

* Need to know quite a bit about (how we’re able to share different medias)
* Know what a collision is \*\*important\*\*, understand where they happen, where they don’t happen, how to avoid/detect them

MAC addresses and ARP

* Know different bit lengths for MAC and IP \*\*strong suggestion to know this\*\*
* What ARP means (how to determine IP address, given its MAC address)

Addressing: routing to another LAN

* Pay attention to when we send traffic (look at example closely)
* See what IP address and MAC address are as it goes through its path
* Understand small nuances associated with that

Ethernet frame structure

* Need to know about this
* Be aware of the different components of the header do

Ethernet: unreliable, connectionless

* Understand what it provides and what it doesn’t provide
* RDT
* Binary back-off, random access with CD (CD vs CA)

Ethernet switch

* There will be questions about switches and routers
* Know the difference between the two
* Know what a router brings to the table
* Know when to use router vs ethernet switch

Switch: multiple simultaneous transmissions

* Ethernet protocol used on each incoming link = no collisions (key point to understand)

Switch: frame filtering/forwarding

* Understand this process and how it works

Switches vs. routers

* Know difference between switches and routers (in depth!)

VLANs

* Will be expected to know what we use them for, what their advantages are
* Use them to segregate traffic, for security purposes, efficiency purposes, access control
* How they work, how we can define them in same switch or across different switches (trunk port)

Synthesis: a day in the life of a web request

* Go through entire example
* If you can understand it well, then you have a good understanding of the preceding 6 chapters

Wireless Link Characteristics

* Wireless traffic is much more susceptible to loss/interference
* What multiple access protocols would we use with wireless links
* SNR – understand it and how we change dynamically between the different encoding/modulation tactics in order to deal with the BER

IEEE

* Listen before we transmit, avoid collision
* Have a good understanding of the speeds (don’t need to know the speeds specifically, 802.11a vs g vs n vs b)

802.11: multiple access

- Collision avoidance (different from collision detection!)

What is network security?

* Securing it enough but still accessible by users

AES

* DES replaced by AES

Public Key Cryptography

* If you don’t understand basics, read textbook (if you still don’t get it, google it or email prof)
* You REALLY need to know this concept for every aspect of computing
* Extremely important for building secure applications
* Need to be well informed on this topic

Public key encryption algos

* Compute private key, given public key

RSA: important property

* Make sure you understand this, incredibly important for calculating

Digital signature

* Understand how to sign a large message such as this
* How to use hash functions (take a large message, condense it down)

Certification authorities

* Make sure you understand this concept very well!

Secure e-mail

* Brings it all together
* If you understand core concepts, this should be very straightforward

Key derivation

* Aware of what nonces are, what they are used for
* We don’t just use a single key, we take a key block and slice/dice it in order to get different keys, initialization vectors ?

802.11i

- What does WPA bring and why is it better for majority of users?

Firewalls

* Why do we use them, benefits/negatives to them (not too many negatives)
* Remember it adds a bit of overhead

Multimedia: audio

* Chapter 9 only comes out of slide deck (NOT FROM TEXTBOOK)
* Not going to go in depth on chapter 9, it was a “bonus” chapter
* Information from slides is enough to know for final exam
* Digital vs analog realm signals

Streaming stored video:

* Be aware of the concept of playout
* Actual audio streamed out at a specific rate (variable rate of delay from network, introduces jitter)
* Understand jitter
* Understand playout rate, what we need to accomplish from the other side, in order to get steady playout that the user expects

Streaming stored video: challenges

* Follow slides, not too in depth
* Jitter, what if the user wants to skip forward/back, how does that influence streaming, how do we communicate that

VOIP

* Really basic, not going to ask much about it
* Should know that if you have too much delay, conversation is impossible
* After a certain time, delay makes packets lost

VOIP characteristics

* Just know what is on the slide

Dimensioning best effort networks

* Two approaches: best effort vs multiple classes of service

30% from before midterm, 70% from chapters 5+

Remember a lot of the concepts in ch. 5-9 are built on ch. 1-4