The information in this guide is to assist students in studying for the final exam. It is not 100% inclusive of material that can be asked on the final exam.

Students are allowed to use both sides of three sheets of 8.5"x11" paper for notes and formulas.

- **No worked examples allowed.**
- **Sheets must be submitted with the exam**
- **Name of the student must be on both sheets**

Possible sources of final exam questions include:

- **Lecture Material**
- **Lab assignments**
- **Homework Assignments – turned in and extra problems**
- **Material from the text book (sections covered by lecture)**

Study Exam 1 and Exam 2
Types of Questions will be similar to the two in class exams.

Chapter 1 material

Figure 1.13 – know the OSI – 7 layer names and what is contained on intermediate hosts
Internet Architecture – fig. 1.15
Bandwidth, latency, propagation delay, transmit times for physical layer.
Bandwidth is in bit per seconds, data sizes are in Bytes and that Kbytes is 1024 Bytes, Mbytes is 1024x1024 Bytes
Delay X Bandwidth product, Throughput, transfer time

Chapter 2 material

NRZ, NRZI, Manchester and 4B/5B encoding.
Framing –
byte oriented: BISYNC, PPP and DDCMP
Bit oriented (HDLC)
– understand basics of these protocols,
Error detection
Two-dimensional parity – how to perform it
CRC – How to create a transmitted message. How to check a message
Transmission methods
ARQ – stop and wait – how this works
SWP – how it works, how to use the SWS and RWS for flow control, how to find the max sequence number necessary to avoid confusion on received packets
Ethernet
Characteristics of an Ethernet channel, Ethernet frame format, how to determine minimum frame size necessary. How the exponential backoff works, what happens with a collision – what is transmitted
CSMA/CD – how it works,
Wireless –
Use of spread spectrum – information in general on this topic
Collision avoidance – how it is obtained in a wireless network – hidden node and exposed node – how these occur

Chapter 3 Material Up to section 3.4

Switching – Forwarding table, Datagrams
Switching – Virtual circuit switching – how to create tables for switches – how it is different from datagrams
Source routing – how it works – what is included in packets
Learning Bridges, Spanning tree algorithm, How bridges configure themselves for a root bridge and designated bridges

IP packet format – standard header length
How to read information from the IP header given in hexadecimal format(the sheet handed out in class will be provided if necessary)
Fragmentation and reassembly

Class A, B and C network addresses – how each start and from this can determine the range
Subnetting, Subnet mask and classless addressing – know how to determine the next hop from a routing table for a particular destination

Tunneling

Distance Vector Routing and RIP
Link State Routing and OSPF
Nothing from section 3.4 to the end of the chapter

Chapter 4 material

EGP and BGP
Multiprotocol label switching (MPLS)
Routing to mobile hosts – process for establishing the foreign agent and care of addresses

Chapter 5 Up to section 5.2.9

UDP
TCP – know three way handshake, how it works, the use of sequence numbering and acks. Do not need to know the state transition diagram
TCP – send and receive buffers, silly window syndrome
TCP – adaptive retransmission – karn/partridge, Jacobson karels, calculation of timeout values
TCP – extensions discussed in the text
RPC – what is it, how it works
Nothing from section 5.2.9 to the end of the chapter

Chapter 6 material

Issues in resource allocation – taxonomy – section 6.1.2
Power of the network
Queuing Disciplines – FIFO, fair queueing, weighted fair queuing, tail drop
TCP congestion control – additive increase, multiplicative decrease
Slow start (congestion window, congestion threshold)
Congestion avoidance – dec bit and RED
Nothing from 6.4.3 to end of chapter

Chapter 7 material

Nothing from chapter 7. We did not talk about this in class – I presented the general topics with very little information

Chapter 8

Symmetric keys – names and how they work
- DES
- AES

Public keys – how they work
Authentication using public keys, digital signature using public keys
Cipher block chaining
Authenticators – cryptographic hash functions, MAC and HMAC
- MD5
- SHA-1

Key predistribuition – symmetric and public
Authentication protocols (see figures 8.7, 8.8, 8.9),