chapter 4 is the transport layer

acronyms

NAT = network area translation

CIDR = Classless InterDomain Routing

DHCP = Dynamic Host Configuration Protocol

IP fragmentation will break up one massive thing into multiple smaller things

4000 byte datagram

= 20 (header) + 3980 (data)

MTU = 1500 bytes

becomes 3 separate packets of size 1500 or less, this case:

1040= 20 (header) + 1020 (data)

1020 (data) =3980 – 1480 -1480

ip addresses = 32 bit link between pc and router

Interface = physical link between pc and router

subnet information

CIDR: Classless InterDomain Routing

classful addressing must equate to 32

example /8 gives 8 subnets, but 24 hosts per subnet

subnets are determined partially by the /#, for example a /24 would be an ip of 11111111 11111111 11111111 00000000

NAT: Network Address Translation

translates your local to the global

i.e. you send from 10.0.1, to 128.119.40.186, 80

goes to router, your sent converts to 138.76.29.7, 5001

We have to tunnel ipv6 through ipv4 so we encapsulate the ipv6 inside an ipv4 block

Overflow thing

header

action

counters

i.e.

src -> dest

forward

2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

chapter 5 is the routing methodologies

acronyms

AS = autonomous systems

IGP = interior Gateway Protocol

OSPF (Open Shortest Path First)

BGP (Border Gateway Protocol)

Dijkstra’s algorithm:

Each node knows entire net

topology, all link costs

Formula looks like

D(b) = min( D(b), D(c) + c(c,b) )

ALL THINGS KNOW BEST COST ROUTES

DISTANCE VECTOR

NEIGHBORS KNOW COSTS

MUST CONSULT NEIGHBORS FOR INFO OF COSTS OF OTHERS

AS

Neighbors know costs

Must search network for total cost

OSPF (Open Shortest Path First)

USES Dijkstra’s

Admin sets costs

BGP (Border Gateway Protocol) provides each AS a means to:

1. Obtain subnet reachability information from

neighboring ASs.

2. Propagate reachability information to all ASinternal

routers.

3. Determine “good” routes to subnets based on

reachability information and policy.

intra vs inter AS routing

Policy:

Inter-AS: admin wants control over how its traffic

routed, who routes through its net.

Intra-AS: single admin, so no policy decisions needed

Scale:

hierarchical routing saves table size, reduced update

traffic

Performance:

Intra-AS: can focus on performance

Inter-AS: policy may dominate over performance

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

chapter 6 is the link layer

acronyms

CRC = cycle redundancy check

mac address = separate from IP, used to send info to another machine that is physically connected

mac protocols:

partitioning

taking turns

random

TDMA

access channel in 'rounds'

each station gets fixed length

FDMA

each station assigned frequency band

unused transmission time in bands go idle

polling

master invited nodes to transmit in turn, has single point of failure, polling overhead and lots of latency

token passing

token passed around machines, if token, send message, same concerns as polling

\*pariety = shit that is 1 if odd in column/row 0 if even

slotted aloha = on fixed sync clock, sends signals during sync

pure aloha = sends when received

csma/cd and slotted aloha compare like:

csma/cd

1. unsync'd

2. carrier sense - no transmission if others are doing it

3.collision detection

4.random backoff

slotted aloha

1. sync'd

2.no carrier sense

3.no collision detection

4.no random backoff

bit time = time to transmit one bit through

csma/cd algorithm

1. adapter receive datagram, creates frame

2. if channel idle for 96 bit time, start the frame transmission

3. if channel busy, wait until channel idle (plus 96 bit time) to transmit

4. if transmits without detecting another, adapter is done with frame

5. if it finds another transmission while transmitting, send 48 bit jam signal

6. after exiting enters exponential backoff, selects random k, waits k\*512 bit times, then returns to step 2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

chapter 7 is all about wireless transmission

uses

TDMA

FDMA

CDMA

csma/cd

Differences from wired connection

Signal interference

Multipath propagation

Decayed strength

Cons of wireless

Packet loss

Network congestion

Bandwidth issues

Bridge connects to network, relay sends info back and forth

Mac w/ backoff

Lower w = higher collision

Higher w = wasted, and unused slots

Exponential backoff = 2 increases when collision detected, decreases when success

Request-to-send

Clear-to-send

Single or multiple nodes to get started

Insafracture = wireless (1 hop) mesh (multihop)

insafracture -less = blutooth(1 hop) MANET ( multi hop)

Home network

Home agent

Permanant adderess

For routing for mobile, we should ‘let the parent system handle it’, send signals to the parent to get update on child

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

chapter 8 is all about security

Cryptography

Symmetric key - sender/receiver use identical key

public/private - sender a sends w/ b’s public key, b decodes w/ private key

Mono alphabetic cipher = replace letters w/ other letters normally

Poly alphabetic = shifts over x letters

Block cipher = message encrypted in k bits

Chaining cipher blocks double encodes

public/private key effectively means:

K1 (K2 (m)) = m

Certification authorities will ensure that you are decoding a message from one person, and not another to help prevent falsified messages