\*\*notes for networking final

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

Chapter 4

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

Transport layer

Network layer

Routing protocols

path selection

RIP, OSPF, BGP

Forwarding table

IP protocol

addressing conventions

datagram format

packet handling conventions

ICMP protocol

error reporting

router signaling

link layer

physical layer

IP fragmentation

datagrams seperated into bits, header used to retain fragments

\*\*\*example IP Fragmentation\*\*\*

4000 byte datagram

= 20 (header) + 3980 (data)

MTU = 1500 bytes

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

1040= 20 (header) + 1020 (data)

1020 (data) =3980 – 1480 -1480

\*\*\*end Example

IP address = 32 bit link between pc and router

interface - physical link between host and router

Ip address parts

Subnet part

11001000 00010111 0001000

Host part

0 00000000

CIDR: Classless InterDomain Routing

classful addressing must equate to 32

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

 What is the netmask for /20 ?

❖ 255.255.240.0

What is the netmask for /27 ?

❖ 255.255.255.224

DHCP: Dynamic Host Configuration Protocol

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

IPv6

 Major changes from IPv4:

 Fragmentation: no longer allowed; drop packet if too big;

send an ICMP msg back

 Checksum: removed to reduce processing time; already done

at transport and link layers

tunnel through ipv4 to send ipv6 to other sources = encapsulate ipv6 inside of ipv4

openflow shit

header

action

counters

i.e.

src -> dest

forward

2

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

Chapter 5

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

chapter goals:

routing algorithms and controllers

graph abstractions = costs

Dijkstra’s algorithm:

Each node knows entire net

topology, all link costs

Notation:

 c(x,y): link cost from node

x to y; = ∞ if not direct

neighbors

 D(v): current value of cost

of path from source to

dest. v

 p(v): predecessor node

along path from source to v

 N': set of nodes whose

least cost path definitively

known

use this formula for dispalying answer 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

aggregate routers into regions, “autonomous

systems” (AS)

Interior Gateway Protocols (IGP)

RIP: Routing Information Protocol

❖ OSPF: Open Shortest Path First

IGRP: Interior Gateway Routing Protocol

# OF HOPS NEEDED TO GET FROM NETWORK 1 TO NETWORK 2

OSPF (Open Shortest Path First)

USES Dijkstra’s

Each router constructs a complete topological map

Link costs are set by the administrator

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

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

Link Layer (also known as layer 2)

 nodes = hosts or routers

 links = communication

channels that connect

adjacent nodes

• wired links

• wireless links

 frame = layer-2 packet

transportation analogy

 Trip: OSU to Marseille

❖ Shuttle: OSU to PDX

❖ plane: PDX to Paris

❖ train: Paris to Marseille

 tourist = frame

 travel agent = routing

algorithm

❖ Doesn’t know/care of mode

 transport mode = link layer

protocol

❖ ≠ legs may use ≠ modes

sends packets with data, and dcb (data correction bits)

pariety errors (pariety checking is that thing where odds = 1 at the end, and evens =0 )

CRC = cycle reduncency check

\*\*check lecture 20, i cant figure the redundency cycle yet

MAC ADDRESSES

32 bit ip address

MAC ADDRESS

48 bit mac address

get frame from one interface to another physically connected interface

hexidecimal represention

4 bits for each symbol = 48/4 = 12 symbols

E.g.: 1A-2F-BB-76-09-AD

ARP table holds all mac addresses in the network

to send to another mac address sender encapsulates the other machine's mac into the frame

sender will send the frame into the medium

all nodes hear frame

b is the only one to grab

other nodes discard the frame

we cant just use IP because LAN is designed for all network layer protocols, not just IP

we cant check on the networklayer because overhead, every frame would be processed

MULTIPLE ACCESS LINKS AND Protocols

POINT TO POINT

BROADCAST

need for sharing of medium/channel

 single channel

needs to be used by all nodes

 interference/collision

two or more simultaneous transmissions lead to collided signals

multiple access protocol

 allows multiple, concurrent access

algorithm that nodes use to share channel, i.e., determines when a

node can transmit

 no coordination, no out-of-band channel

agreeing about channel sharing must use channel itself!

MAC Protocols: a taxonomy

Three broad classes:

 Channel Partitioning

❖ divide channel into smaller “pieces” (time slots,

frequency, code)

❖ allocate piece to node for exclusive use

 “Taking turns”

❖ nodes take turns, but nodes with more to send can take

longer turns

 Random Access

❖ channel not divided, allow collisions

❖ need to know how to “recover” from collisions

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

RANDOM ACCESS Protocols

distributed, no cordination among nodes

one node transmits at a time

collisions can occur between two nodes

MAC protocol specifies how to detect and recover from collisions

SLOTTED ALOHA

PROS:

single node can use full power of rate of transmission

simple

only slots nodes need to be sync, decentralized

cons:

collisions = wasted slots

idle slots = wasted

clock syncronization

calculating efficency :

 suppose: N nodes with many frames to send,

each transmits in slot with probability p

 prob that a given node has success in a slot ?

p(1-p)N-1

 prob that any node has a success ?

Np(1-p)N-1

 Efficiency = Np(1-p)N-1

37% transmission time

PURE ALOHA

sends as soon as frame arrives,

really shitty, collision chance rises dramatically

18% transmission time

CSMA (Carrier Sense Multiple Access)/CD (collision detection)

CD = easy in wired, tough in wireless

csmacd - collisions detectable, colliding transmissions aborted, reduce channel waste

bus and star topology

CHAPTER 7

WIRELESS SHIT

Wireless has 2 issues to create:

Wireless - communication over wireless link

Mobility - handle user that changes point of attachment to network

stationary

Wireless =/= mobility

Bridge = connected to network

Relay = the thing responsible for sending packets back and forth from host

Connects = mobiles to base station

Multiple access protocol = coordinated link access

Various data rates = transmission distance

Bridge 2

Handoff to network

\*has limited range

\*computers have to multihop to organize the network

Single or multiple nodes to get started

Insafracture = wireless (1 hop) mesh (multihop)

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

Differences from wired

Decayed strength

Signal intereferance

Multipath propigation

They use:

FDMA = user gets own frequency for whole time

TDMA = user gets whole channel for limited time

CDMA = allows users both frequency, and time, and they can transmit simultaneously

Zi,m= di . cm

CSMA/CD = sense before transmitting, connection free time, connection time

One at a time

No collision detection

Goal is to avoid collisions, but will acknowledgment to recover from one

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

Physical carrier sensing actual sensing of medium to determine whether it is busy or not Virtual carrier sensing provided my MAC via RTS/CTS frames. Predicts future traffic based on information/duration indicated in RTS/CTS frames

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

Wireless is filled with packetloss, network congestion, and bandwidth issues

\*\*CHAPTER 8

Cryptography

Symmetric key - sender/reciever use identical key

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

Mono alphabitic 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