Cheatography

Operating Systems Cheat Sheet

by calkk via cheatography.com/20194/cs/3033/

Comparisons

Forwarding vs Routing

> **Forwarding**: data plane - Directing a data packet to an outgoing link - individual router using a forwarding table **Routing**: control plane - computing paths the packets will follow - Routers talking amongst themselves - individual router creating a forwarding table.

Link State vs Distance Vector:

> - **DV** error propogates, **LS** only computes its own table. - **DV**: convertence times varies (count-to-infinity problem), **LS**: O(n^2) algo requires O(nE) messages

Flow control vs Congestion control

> **Flow control**: keeping one fast sender from overwhelming a slow receiver **Congestion control** : keep a set of senders from overloading the network

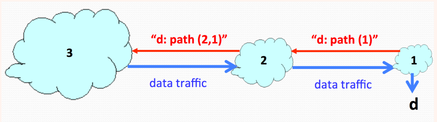
Definitions

Connectionless: No handshaking between sending and recieving adapter.

Unreliable: receiving adapter doesnt send ACKs or NACKs; Packets passed to network later can have gaps; Gaps will be filled if application using TCP

Carrier sense: wait for link to be idle	**Channel idle**: start transmitting; **Channel Busy**: wait until idle
Collision detection: listen while transmitting	**No collision**: transmission is complete; **Collision**: abort transmission and send jam signal

Path-vector Routing

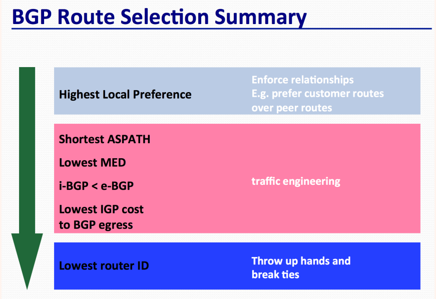


-Advertise entire path

-Distance vector: send distance metric per dest d

-Path vector: send the entire path for each dest d

BGP path selection



BGP Route Selection Summary

Highest Local Preference — Enforce relationships E.g. prefer customer routes over peer routes

Shortest ASPATH
Lowest MED
i-BGP < e-BGP
Lowest IGP cost to BGP egress
— traffic engineering

Lowest router ID — Throw up hands and break ties

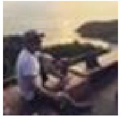
BGP uses both policy and shortest path based routing.

Route learned from customer preferred over route learned from peer, preferred over route learned fromprovider

Congestion Control

Congestion cntrl is preventing a set of senders from overwhelming the network, flow cntrl is preventing one fast sender from overwhelming a slow receiver.

Congestion strategy	Drop one flow, buffer and send after one is gone, reschedule on flow, ask both to reduce flow
Congestion Collapse	Increase in net load results in a decrease of useful work -Causes: False trans, undelivered pckts
Simple Resource Allocation	is FIFO queue, drop tail (incoming) if buf full.
TCP Congestion Control	feedback based, hosted based, congestion window. Send at rate of slowest component, window = min(congestion, receiver wndw) Increase linearly, but half if there is a loss. (w <- w + w/1 or <- w/2) never below 1 MSS though. Congestion window is rep in BYTES because of MSS. #packets per window : CWND/MSS Inc per ACK : MSS*(MSS/CWND) Sending rate = Congestion Window size / RRT. Exponential fast start, because linear is too slow to start and wasteful starting @ 1 MSS/RRT and 1MSS cwnd.
Triple dup ACKs	multiplicative decrease. Timeout – start over @ 1MSS.
Nagel's Algo	buffer small data if less than 1 MSS while waiting for ACK of outgoing packet. Basically sending 1 small packet per RTT. Batching bytes!
Delayed ACK/Piggybacking	send ACK as part of a data packet from B->A if data generated within wait time of 200 – 500 msec.



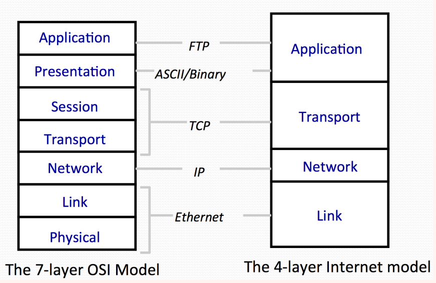
Interconnecting LANs

CSMA/CD	carrier sense multiple access w/ collision detection
Ethernet	is connectionless and unreliable
Spanning Trees	no loops in topology.(no cycles) Select switch with smallest ID as root. Initially each switch thinks its root and sends msg (X,0,X). add1 to distance from neighbor node from root. (Root, dist to root, self)
Cut thru switching	start transmitting as soon as possible. Overlapping transmissions (transmit head of packet while still receiving tail)
Switch over router	PnP, Fast filtering and fwd, cut thru

Interior Routing Protocols (IGP)

RIP	uses distance vector; updates sent every 30 seconds; no authentication; not used much anymore
OSPF	Link-state updates sent (using flooding) as ad when required; Every router runs Dijkstra's algorithm; Authenticated updates; widely used

Network Layer



Different devices switch different things:
physical later: electrical signals (repeaters and hubs)
link layer: frames (bridges and switches)
network layer: packets (routers)

Link Layer / Error Detection / Correction

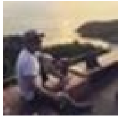
Manchester Coding	Low to high if 0, High to low if 1.
NRZI	invert on every 1, do nothing if 0.

Link Layer / Error Detection / Correction (cont)

4B/5B	more efficient than Manchester, map data bits to code bits 80%
Sentinels	mark start and end of frames from stream of bits. Use a flag 0x7E
Propogation Delay	distance / speed of light, Transm D = message/rate bps
RTT	2 * one way delay (latency)
Latency	Prop + Trans + Queue = Arrival - Departure
Bandwidth-Delay Product	measures data in flight = Bandwidth * latency
Parallel Transmission	latency=M/R + SUM(Prop_i)
Actual end to end latency	SUM(Transp_i + Prop_i + Q_i)
ARQ	detect and retransmit, typically at higher levels (Network +)
FEC (Forward error checking)	correct codes, good for real-time, less retransmissions.
CRC (cyclic redundancy check)	divide n bits of data by C(x), compare to k bits
Hamming Distance	tells us how much error can safely be tolerated. d+1 Detect. 2d+1 correction

Internet Topology and Routing

PoP	physical location access point to internet. Large dense population, part of backbone
Multihoming	>= 2 providers, better performance, extra reliability, financial leverage through competition
AS Prepending	artificially inflate AS path length seen by others to convince some AS's to send traffic another way (Export policy)
Incremental Protocol	Learn multiple routes, pick one with policy



Internet Topology and Routing (cont)

iBGP	distributes BGP info within AS, sessions between routers, maps an egress point to out link. BGP incremental updates, maps dest prefix to egress point
Causes of BGP routing	Topol changes, changes in routing policy, BGP session failure, conflicts in protocols in diff AS's

Software Defined Networking

Vertically integrated Closed, proprietary Slow innovation -> horizontal, open interface, rapid innovation. OS abst.

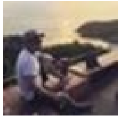
Network OS	has global view of network to make decisions. Control plane is in one place. Distributed sys. Control program operates on top of network OS.
Routing Overlays	IP Tunneling - packet delivery service with new routing strategies
IP multicast	delivering same data to many receivers
RON	resilient overlay network. Increase performance and reliability of routing, more than IP. Adapts to congestion
Overlay Networks	A logical network built on top of a physical network. tunnels between host computers. Hosts implement new protocols and services. Effective way to build networks on top of the internet. P2P
Napster	centralized directory, gnutella –query flooding, kazaa--super nodes, bittorrent- distributed downloading/no free loading BitTorrent prevents free riding: Allow the fastest peers to download from you. Occasionally let some free loaders download

Network Security

Goals:	availability, protection, authenticity, data integrity, privacy
SYN Flooding	Make so many sessions it runs out of memory
DoS aplenty	Attacker guesses TCP seq# for an existing connection. Attacker can send rst to close cnnctn.
Bellovin/Mockapetis attack	make target trust attacker using reverse DNS, take control of DNS server that target talks to and find a trusted connection.
DNS rebinding	send short ttl for dns query, target requests IP of your domain, but feed IP of private server.
IP Spoofing	expose trusted connection, predict Seq # from SYN and predict port => guess state. Now Impersonate one end and send packets.
Stateful Packet Filter	only allow traffic initiated by client. Track all conn.

Queuing Mechanisms

End to End principle	Design principle for the internet that says you should keep functionalities at the end-hosts (Application specific functions)
Random Early Detection (RED)	randomly drop packets to signal congestion before it happens as queue fills up. Probability is prop queue size. If below a threshold, don’t drop anything. Use average queue len to allow short term bursts. -RED is hard to use, must have the right parameters to work. -Desynchronizes senders to have stead aggregate flow, not bursty.



Queuing Mechanisms (cont)

Explicit Congestion Notification (ECN)	router marks packets with ECN bit, 2 bits 1 for ECN enabled and 1 for congestion in IP TOS. Must be supported by end hosts and router to work. But better since it does not drop packets like RED.
NAT soft state	if no packets arrive in time window, then delete mapping.
Firewall	filters packets based on src/dst IP addr, TCP/UDP src/dst port, ICMP type, TCP SYN and ACK bits
Traffic shaping	rate limiting certain traffic like p2p Inspecting every packet is challenging on high speed links. Place complicated firewall rules on edge low speed, and simple in core high speed.
Gateway	users must login, only point that accepts telnet. (central, caching) 1-Detailed policies 2-Avoid rogue machines 3-central logging 4-caching
Middle-boxes	Pros: Fewer IPs, Blocking unwanted traffic, Making fair use of net resources, Improcing web performance. Cons: No longer globally unique, no longer assume simple delivery of packets