Finals Summary

50.012 Networks, Elective 2019

Tey Siew Wen

06 Feb 2020

Topic	Specific Sections
TCP Congestion Error	Lecture 10: Congestion Control, Lecture 11: TCP Wrapup
Network Layer	Lecture 13: Network Layer Overview, Lecture 14: IP Addressing, Lecture 15: Routing Algorithms, Lecture 16: Routing
Link Layer & Synthesis	Lecture 19: Link Layer
Wireless and Mobile Networks	Lecture 21: Wireless Networks

1 Lecture 10: Congestion Control

1.1 Principles of Flow Control

- Receiver controls sender so the sender won't overflow receiver's buffer by transmitting too much/-too fast
    - Application may remove data from TCP socket buffers
- Receiver includes a `rwnd` (receiver window) value in TCP header of receiver-to-sender segments
    - `RcvBuffer`

1.2 Principles of Congestion Control

- Congestion Control ≠ Flow Control!
- Mainfestations
    - Buffer Overflow at Routers: Lost Packets
    - Queueing in Router buffers: Long Delay

When packets are lost, any upstream transmission capacity used for that packet is wasted.

1.2.1 Scenario 1: One Router w/ Infinite Buffers

- Assuming no retransmission

1.2.2 One Router w/ Finite Buffers

Assumptions for idealized case

- Sender knows when router buffers available
- Sender sends only when router buffers available

Transfer rates

- $\lambda_{\text{in}} = \lambda_{\text{out}}$: Application-layer input = output
- $\lambda'_{\text{in}} \geq \lambda_{\text{in}}$: Transport-layer input includes retransmissions

1.2.3 TCP Congestion Controls

Increase sender's transmission rate until loss occurs

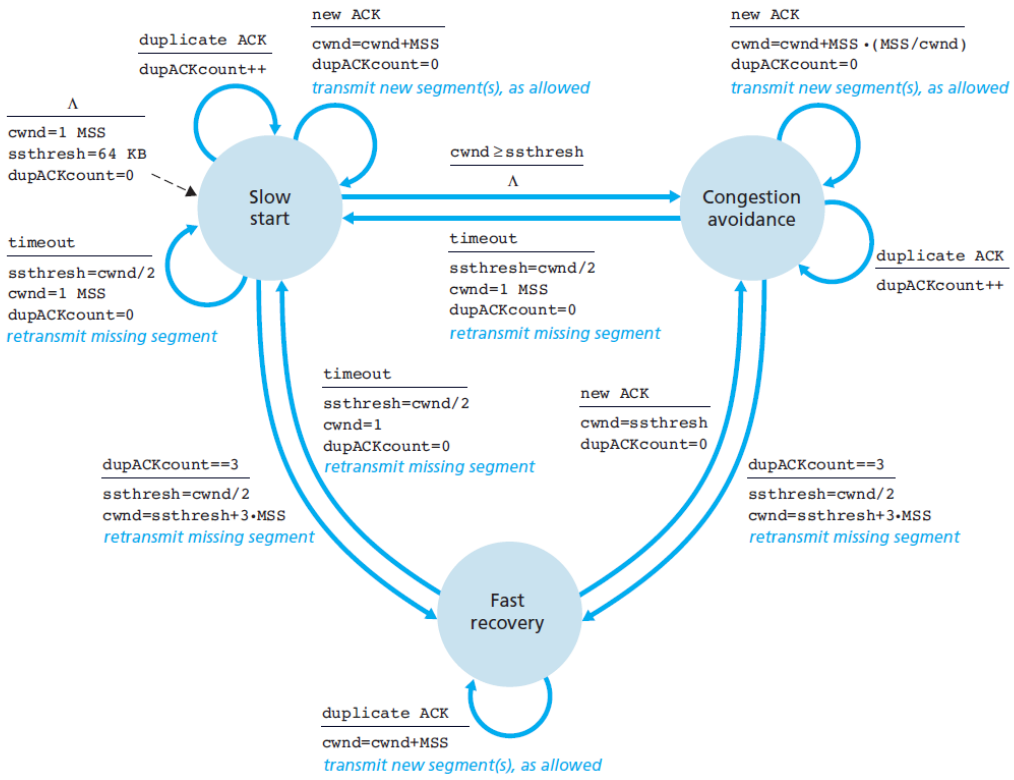
- Additive Increase: Increase cwnd (congestion window) by 1 MSS every RTT until loss detected
- Multiplicate Increase: Reduce cwnd in half after loss

2 Lecture 11: TCP Wrapup

2.1 TCP Congestion Control

A summary code for the sections discussed below:

```
cwnd = MSS
while connected:
if time < slow_start_duration:
    cwnd *= 2
    if receive_ACK:
    cwnd += MSS
else: # congestion-avoidance state
    if receive_ACK:
    cwnd += MSS*(MSS/cwnd)
```



2.1.1 Start Connection: Slow Start

When connection begins, increase rate exponentially until first loss event. (Initial rate is slow but ramps up very fast)

1. Initial cwnd: 1 MSS (maximum segment size)
2. Double cwnd every RTT
    - It is doubled with the formula: $cwnd = cwnd + MSS * \frac{cwnd}{mss}$
3. Increment cwnd for every ACK received

2.1.2 Congestion-avoidance state

Window grows exponentially in **slow start** to threshold, then grows linearly during the congestion-avoidance (CA) state.

- The inexponential increase is switched to linear when `cwnd` gets to half of its value before timeout.
- On loss event, `ssthresh`=0.5∗`cwnd` before loss event.

In the CA state, the congestion window is increased by $\frac{1}{k}$.

- where $k = \frac{cwnd}{mss}$

2.1.3 Explicit Congestion Notification (ECN)

Network-assisted congestion control

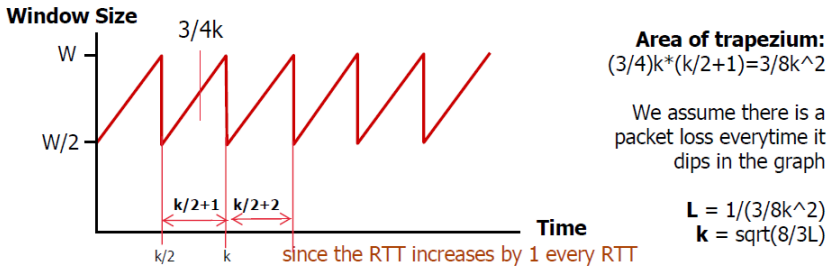
- 2 bits in IP header (ToS field) marked by network router to indicate congestion
- Receiver sets ECE bit on ACK to notify sender of congestion

2.1.4 Calculating TCP Throughput

Ignoring slow start and assuming there is always data to send,

$$\text{TCP Throughput} = \frac{3}{4} * \frac{W}{RTT}$$

- where W: window size in bytes where loss occurs



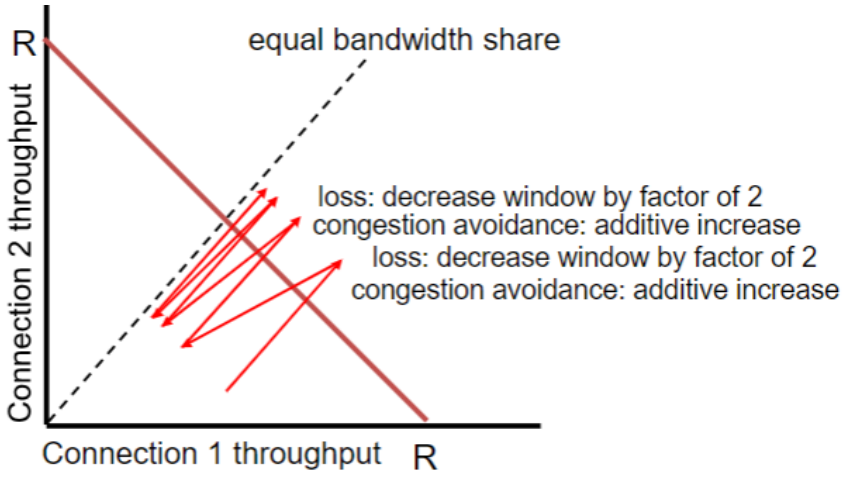
Calculating Segment Loss Probability, L

e.g. given 1500 byte segments, 100ms RTT, 10Gbps throughput, requires average 83,333 in-flight segments

$$10^7 = \frac{1.22 \times 1500}{100 \times 10^{-3} * \sqrt{L}}$$
$$L = 2 \times 10^{-10}$$

2.1.5 TCP Fairness

- Goal: For n TCP sessions sharing same bottleneck link of bandwidth R, each should have $\frac{R}{K}$ rate.
- Implementation via Additive Increase and Multiplicate Decrease



3 Lecture 13: Network Layer Overview

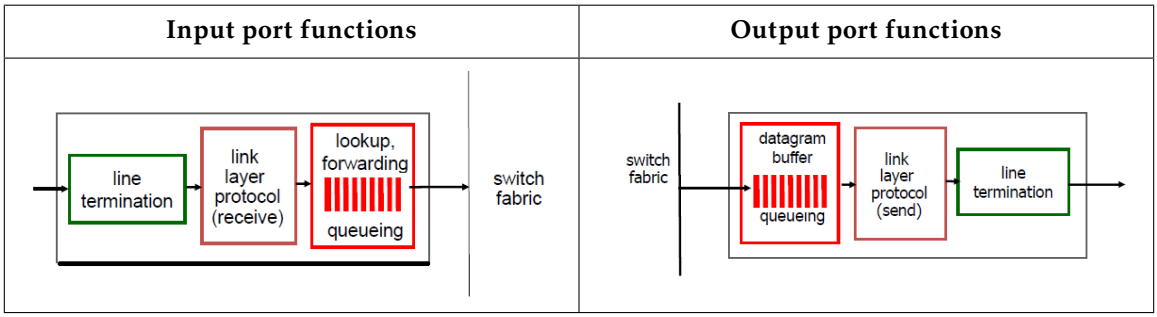
3.1 Two Key Network-Layer Functions

1. *Forwarding*: Router-local action of transferring a packet from an input link interface to the appropriate output link interface. (Data Plane)
2. *Routing*: Network-wide process that determines the end-to-end paths that packets take from source to destination. (Control Plane)

Control Plane Approaches:

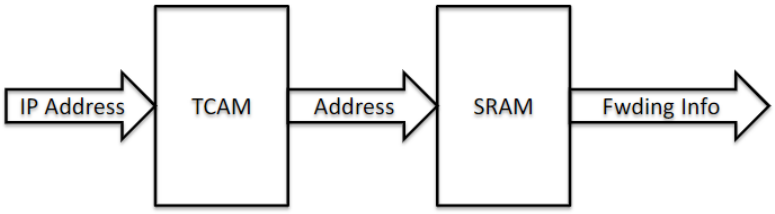
1. Traditional Routing Algorithms: Implemented in Routers
    - Per-router control plane: Individual routing algorithm components in each and every router interact in the control plane
2. Software-defined Networking (SDN): Implemented in remote servers
    - A distinct controller interacts with local control agents

Overview



3.2 Input Processing

Typical Forwarding Process:



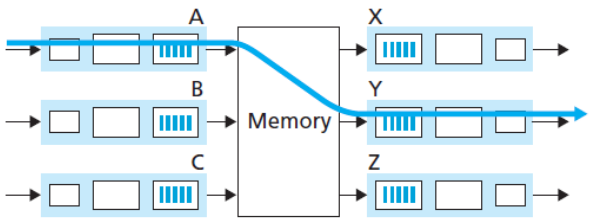
1. Every router has a **forwarding table**, which is computed and updated by its routing processor, and **stored at the input port**.
    - A router forwards a packet by examining the value of a field in the arriving packets header, and then using this header value to index into the routers forwarding table.
    - The value stored in the forwarding table entry for that header indicates the routers outgoing link interface to which that packet is to be forwarded.
    - The value to be examined in the packet's header is determined by the routing algorithm.

2. The routing processor also stores a **shadow copy**, typically stored at each input port.
    - With a shadow copy, forwarding decisions can be made locally, at each input port, without invoking the centralized routing processor on a per-packet basis
    - This helps to avoid a centralized processing bottleneck.
3. After determining the outgoing link interface, the packet is forwarded from the the router's input ports to its output ports via **switching fabrics**.

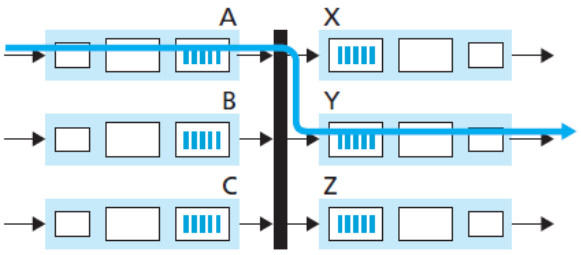
3.2.1 Switching Fabrics

There are 3 types.

1. Memory
    - An input port with an arriving packet first signaled the routing processor via an interrupt. The packet was then copied from the input port into processor memory.
    - The routing processor then extract the destination addr from the header, looked up the appropriate output port in the forwarding table, and copied the packet to the output ports buffers.
    - If the memory bandwidth is such that B packets per second can be written into, or read from, memory, then the **overall forwarding throughput** (the total rate at which packets are transferred from input ports to output ports) **must be less than** $\frac{B}{2}$.
    - Two packets cannot be forwarded at the same time, even if they have different destination ports, since only one memory read/write over the shared system bus can be done at a time.

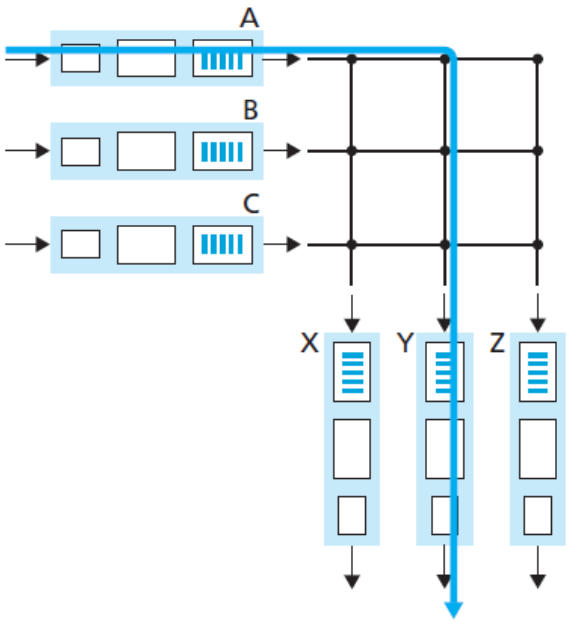


2. Bus
    - The packet is transferred directly from the input port to the output port over a shared bus, without intervention by the routing processor
    - The input port pre-pend a switch-internal label (header) to the packet to indicate the local output port for the packet
    - The packet is received by all output ports, but only the port that matches the label will keep the packet. The label is then removed at the output port.
    - **Bus Contention**: Only one packet can board the bus at a time. Hence, the switching speed of the router is limited to the bus speed and transmitting the packet onto the bus



3. Crossbar

- An interconnection network consisting of $2N$ buses that connect N input ports to N output ports
- There is a switch fabric controller to open/close cross points of the horizontal and vertical bus
- Capable of forwarding multiple packets in parallel.
- Initially developed to connect processors in multiprocessor.

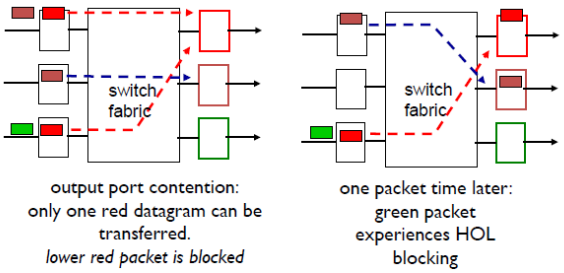


3.2.2 Input Port Queueing

Since the switching fabric operates slower than the input ports, queueing at input queues may cause the input buffer to overflow. Packet loss will then occur when no memory is available to store arriving packets.

Head of the Line (HOL) Blocking

Queued datagram at front of queue prevents others in queue from moving forward



3.2.3 Output Processing

Output port processing takes packets that have been stored in the output ports memory and transmits them over the output link. This includes selecting and de-queueing packets for transmission, and performing the needed linklayer and physical-layer transmission functions.

If the datagrams arrive from fabric faster than the transmission rate, buffering will be required. **Packet loss may occur** due to congestion and lack of buffers.

3.3 Routing Algorithms

- *Destination-based forwarding*
  - Destination address range is the index for a particular link interface
  - However there are times ranges don't divide up nicely
- *Longest Prefix Matching*
  - Longest address prefix is the index for matching destination addr
  - Performed using Ternary Content Addressable Memories (TCAMs)

e.g of longest prefix matching. given

Destination Address Range	Link Interface
1100 1000 0001 0111 0010*** **** ****	0
1100 1000 0001 0111 0011*** **** ****	1
1100 1000 0001 0111 0011000 **** ****	2
otherwise	3

a) **1100 1000 00010111 0010**110 1011 0110: 0

b) **1100 1000 00010111 0011000** 1011 0110: 2

c) **1100 1000 00010111 0011**001 1011 0110: 1

3.3.1 Ternary Content-addressable memory (TCAMs)

- A specialized type of high-speed memory that searches its entire contents in a single clock cycle.
  - More power, more area and higher latency than SRAM
  - To retrieve data on RAM, the operating system (OS) must provide the memory address where the data is stored.

    - Data stored on CAM can be accessed by performing a query for the content itself, and the memory retrieves the addresses where that data can be found.
    - Performs parallel processing
- Able to store and query data using three different inputs: 0, 1 and X (Ternary).

4 Lecture 14: IPv4 Addressing

Hosts/Routers typically has interfaces such as wired Ethernet, wireless 802.11. Interfaces are connections between the host/router and the physical link.

Since every host and router is capable of sending and receiving IP datagrams, IP requires each host and router interface to have its own IP address. Thus, an IP address is technically associated with an interface, rather than with the host or router containing that interface.

- Each IP is 32 bits long (4 bytes)
  - Each byte of the address is written in its decimal form, separated by a period from other bytes in the address. Example: 193.32.216.9
  - Total of 2^{32} possible IP addresses.
- Each IP address can be assigned to a **subnet**. Example 223.1.1.0 /24
  - The leftmost 24 bits of the 32-bit quantity define the subnet address
  - So any host that has an IP address of 223.1.1.x can be identified to be under the same subnet. Any additional hosts will also be required to have the address of this format.

To determine the subnets, detach each interface from its host/router, creating islands of isolated networks. An example is shown below.

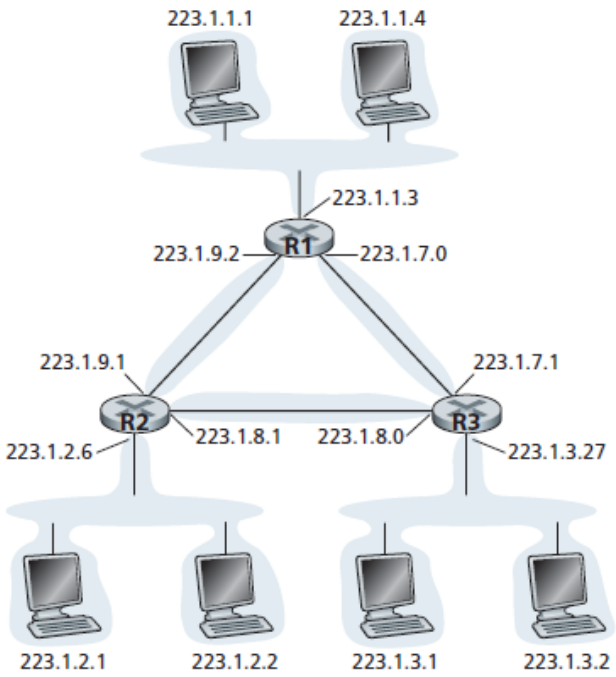


Figure 4.17 ♦ Three routers interconnecting six subnets

> Core routers in Singapore are running on IPv4. Singtel currently has Singtel has OLT vendors which operate on IPv6, and most of their services are IPv6 ready. They have a tunneling protocol for translating IPv6 internally within the Singtel network to IPv4 to these core routers.

4.1 Classless InterDomain Routing (CIDR)

- Address format: `a.b.c.d/x`
    - x most significant bits in the address (the prefix) constitute the network portion of the IP address.
        - Organizations usually use a range of addresses with a common prefix.
        - Hence, when a router outside the organization forwards a datagram whose destination address is inside this organization, they only care about the prefix.
        - This **reduces the size of the forwarding table** in the routers, since a single entry of the form `a.b.c.d/x` will be sufficient to forward packets to any destination within organization.
        - Sometimes organizations may come together under a subnet for **route aggregation/ route summarization**.
    - The remaining $(32-x)$ bits are used to distinguish among the devices within the organization.

> Currently there is around 800k prefixes! 60k networks around the world. Singapore comprise of about 1k networks.

4.2 Dynamic Host Configuration Protocol (DHCP)

DHCP allows host to dynamically obtain its IP address from a network server when it join its network.

How it works - DORA

1. Host broadcast "DHCP **D**iscover" msg [optional]
2. DHCP server hears the broadcast and responds with "DHCP **O**ffer" msg [optional]
3. Host requests IP address: "DHCP **R**equest" msg
4. DHCP server sends address: "DHCP **A**ck" msg

Example

1. New connecting host sends a DHCP *request* encapsulated in UDP, IP and Ethernet.
2. The Ethernet frame *broadcast* on LAN, received at router running DHCP server
3. Ethernet demuxed to IP demuxed, UDP demuxed to DHCP
4. DHCP server formulates an ACK containing
    - client's IP address
    - First-hop router for client (if requested)
    - Name & IP Address of DNS Server (if requested)
    - MASK to determine which portion is the network/host (if requested)
5. Encapsulation of DHCP server, frame forwarded to client, demuxing up to DHCP at client
6. Client obtains the info inside ACK.

4.3 Network Address Translation (NAT)

- All datagrams leaving local network must have the same single source NAT IP address, but with different src port numbers
  - Replace (`src IP addr, port#`) of every outgoing datagram to (`NAT IP addr, new port#`)
  - Record every (`src IP addr, port#`) to (`NAT IP addr, new port#`) translation pair in NAT translation table.
- Allows local network to use just 1 IP for all devices in the network
  - The local network can change address of devices in local network without notifying outside world.
  - Security: Devices inside local net not explicitly addressable & visible by outside world.
- Allow local network to change ISP without changing addresses of devices in local network

5 Lecture 15: Routing Algorithms

5.1 Link-state Broadcast Algorithm (LS Algorithm)

5.1.1 Properties of the Algorithm

- Centralized: Use global information. Requires each node to first obtain a complete map of the network before running the Dijkstra algorithm.

5.1.2 How it works

Watch this for explanation of how it the algorithm works: https://www.youtube.com/watch?v=ue-BDS-7Ikw.

5.1.3 Time Complexity

- Total number of nodes we need to search through over all the iterations is $\frac{n(n+1)}{2}$
  - First iteration n, 2nd iteration $n-1$ and so on.
  - $n + n - 1 + ... + 1 = \frac{n(n+1)}{2}$
  - Hence, **worst case time complexity** = $O(n^2)$
  - If we implement the data structure as a heap, can reduce to logarithmic complexity.

5.1.4 Possible Pitfall Scenario - Unequal link costs

$$c(u,v) \neq c(v,y)$$

For most algorithms, it is assumed that the link costs depend on the traffic carried. And here, the load carried on both directions are not equal.

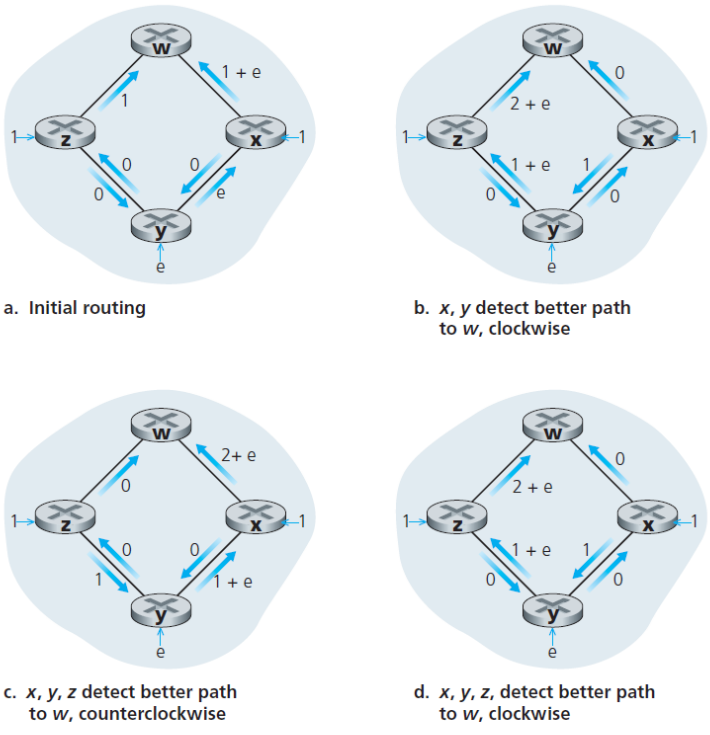


Figure 4.29 ♦ Oscillations with congestion-sensitive routing

- Initialization
  - Both x and z originates a unit of traffic destined for w,
  - y injects an amount of traffic equal to e, also destined for w.
- 1st run
  - y
    - determines that the clockwise path to w has a cost of 1, while the counterclockwise path to w (which it had been using) has a cost of $1 + e$.
    - So the least-cost path for y is now clockwise.
  - x
    - determines that the least-cost path is also clockwise.
- 2nd run
  - x, y, and z all detect a zero-cost path to w in the counterclockwise direction, and all route their traffic to the counterclockwise routes.
- 3rd run
  - x, y, and z all detect a zero-cost path to w in the clockwise direction, and all route their traffic to the clockwise routes.

Solutions

1. Mandate that link costs do not depend on the amount of traffic carried
2. Not all routers run the LS algorithm at the same time
   - Even though they initially execute the algorithm with the same period but at different instants of time, the algorithm execution instance can eventually become, and remain, synchronized at the routers. To avoid this, randomize the time it sends out a link advertisement.

5.2 Distance Vector (DV)

5.2.1 Properties of the algorithm

- Iterative
  - this process continues on until no more information is exchanged between neighbors
  - requires no signal to ask it to stop
- Asynchronous
  - does not require all of the nodes to operate in lockstep with each other
- Distributed
  - each node receives some information from one or more of its directly attached neighbors, performs a calculation, and then distributes the results of its calculation back to its neighbors.

5.2.2 Bellman-Ford equation for Least Cost

$$d_{x,y} = \min_{v} [c(x, v) + d_v(y)]$$

5.2.3 How it works

Watch this: https://www.youtube.com/watch?v=x9WIQbaVPzY

- A node x updates its distance-vector estimate when it either sees a cost change in one of its directly attached links or receives a distancevector update from some neighbor.
- To update its own forwarding table for a given destination y
    - what node x really needs to know is not the shortest-path distance to y but instead the neighboring node $v*(y)$ that is the next-hop router along the shortest path to y.

5.2.4 Pitfall - Count to infinity problem when a link cost increases

Good news travel fast (Lower cost), Bad news travel slow (Higher cost)

Solution

- Poisoned Reverse: if z routes through y to get to destination x, then z will advertise to y that its distance to x is infinity. z will continue telling this little white lie to y as long as it routes to x via y.
    - However, does not work for loops involving three or more nodes (rather than simply two immediately neighboring nodes)

6 Lecture 16: Scalable Routing

Routers are usually aggregated into domains known as *autonomous systems* (AS).

Intra-AS Routing	Inter-AS Routing
Gateway has links to other routers in other AS	Gateway performs inter-domain routing and intra-domain routing
All routers in AS must run same intra-domain protocol	Routers in different AS can run different intra-domain routing, but all routers would need to run the same inter-domain protocol
Single admin, so no policy decisions needed	Admin wants to control over how its traffic is routed, who routes through its net
Scalablity less of an issue, can always use hierarchical routing to reduce scale	Scalability is critical
Focus on performance	Policy may dominate over performance

6.1 Inter-AS: Border Gateway Protocol (BGP)

- It is a **path-vector** protocol
  - Link cost is not the priority; **the routing policy is the most important** for BGP Routing.
  - `CIDRized Prefix + AS-path + Next-hop`
    - Next-hop: IP addr of gateway router to enter the path (You cannot route AS, only route routers.)
    - AS-path: Enforce import-policy for paths, avoid looping
- Provides each AS a means to
  - **eBGP**: Obtain subnet reachability information from neighbor AS
  - **iBGP**: Propagate reachability information to all AS-internal routers
- BGP messages are exchanged between peers over semi-permanent TCP connection to advertise paths to different destination network prefixes
  - OPEN: *open TCP connection* to remote BGPpeer and authenticate sending BGP peer
  - UPDATE: Advertises new path / withdraw old path
  - KEEPALIVE: Keeps connection alive *in absence of UPDATES*. ACKs OPEN request
  - NOTIFICATION: Report errors in previous msg / Close Connection.

6.1.1 BGP Route Selection

- BGP *sequentially* invokes these rules to select a route
  1. Local Preference value attribute: Policy Decision
  2. Shortest AS-Path
  3. Closest Next-Hop router: Hot Potato Routing
  4. Additional Criteria

- **Hot Potato Routing**: Choose local gateway that has the **least intra-domain cost**, without caring about inter-domain cost.
- *Habit of Keeping quiet*: If a network X does not want to route from B to C via X, X will not advertise to B a route to C.

6.2 Intra-AS: Interior Gateway Protocols (IGP)

Routing with Interior Gateway Protocols (IGP).

- RIP: Routing Information Protocol
- OSPF: **Open Shortest Path First**
  - Area Border: Summarize distances to nets in own area then advertise to other Area Border routers
  - Backbone: run OSPF routing limited tobackbone
  - Boundary: Connect to other AS
- IGRP: Interior Gateway Routing Protocol

7 Lecture 19: Link Layer

7.1 Introduction

- **Main Responsiblity of the Link Layer**
  - Transfer datagram from one node to *physically adjacent* node over a link.
  - Over different links, the datagram is transferred by different link protocols
    - e.g. First Link 802.11, Second Link PPP, ... Last link Ethernet
  - Each link protocol provide different service.
    - e.g. may or may not provide RDT over link
- **Whether the Link Layer is implemented**
  - Implemented via the combination of hardware, software and firmware in *every host*
  - Particularly in the *network interface card (NIC)* such as the Ethernet card/802.11 card or a Ethernet chipset. It has a physical interface (physical layer) and a controller (link layer)
  - Attaches to the host's system buses to connect to the CPU of the host (application, transport, network and link layers), so that it is easier manage the link layer.

7.1.1 Two types of links

1. Point-to-point (PPP)
   - Dial-up Access
   - Link between Ethernet switch and host
2. Broadcast
   - Ethernet
   - upstream HFC
   - 802.11 wireless LAN

7.2 Link Layer Services

- **Framing, link access**
  - Encapsulate datagram into frame, add header and trailer
  - Channel access if *shared medium* [optional]
  - "MAC" Address used in frame headers to identify `src, dest`.
- **Reliable delivery** between adjacent nodes
  - Usually used on wireless links that would have *high error rates*. Seldomly used on low bit-error links incude Fiber, Twisted pair, Coaxial Cables.
- **Duplexing**
  - Half-duplex: Nodes at both ends of link can transmit *but not at the same time*.
    - There may be collision if the node receive ≥ 2 signals at the same time, due to simultaneous transmissions (interference).

- Duplex: Nodes at both ends of link can transmit at the same time. There will be 1 wire for 1 direction.
  - Utilize Multiple Access Protocol.

7.3 Addressing: IP vs MAC

IP address	MAC address
32-bit	48-bit
Organizations reserve certain IP address ranges	MAC address allocation administered by IEEE, manufacturer buys a portion of MAC address space, so first 24 bits configured by manufacturer
Dynamically assigned by the network	MAC address burned in the NIC ROM. But some are also software configurable.
Uses Decimal Notation e.g. 224.12.13.2/24	Uses Hexadecimal Notation e.g. IA-2F-BB-76-09-AD
Network layer forwarding	To get frame from one interface to another physically connected interface
Not portable, as address depends on IP subnet to which the node is attached.	Portable, as LAN card containing fixed MAC flat address can be moved from one LAN to another.

7.4 Address Resolution Protocol (ARP)

IP address: Each IP node (host/router) on LAN has a ARP Table that contains IP/MAC address mappings for some LAN nodes, and the TTL time after which address mapping will be forgotten. These ARP tables are created by nodes without intervention from net adminstrator.

So if we know an interface's IP address, we can determine an interface's MAC Address.

7.4.1 Within the same Local Access Network (LAN)

1. A wants to send datagram to B, but A's ARP table does not have B's MAC Address
2. A broadcast ARP query packet, containing B's IP Address. All nodes on same LAN will receive this query.
3. B receives this packet and replies to A with its MAC Address as a frame.
4. A Caches the IP-to-MAC Address pair in its ARP table until timeout.

7.4.2 Across LANs

1. All the nodes in the same LAN as A will not know the MAC address of B, who is inside another LAN. But there is a router R between the 2 LANs
2. A create IP datagram with `IP src A, dest B`, and put it inside a link-layer frame with `dest R`. This frame is thus sent from A to R.
3. R receives this datagram, take it out of the frame and pass it to IP.
4. R can now create a link-layer frame with `dest B`, containing the A-to-B IP datagram.

7.5 Multiple Access Protocol (MAP)

- MAP is a distributed algorithm that determines how nodes share channel (when the node can transmit).

- Communication about channel sharing uses the channel itself.
- No out-of-band channel for coordinated.

7.6 Ethernet

The sending adaptor encapsulates IP datagram in an **Ethernet Frame structure** as such:

Preamble	Destination Address	Source Address	Type	Payload	CRC

- Preamble: 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- Address: 6 byte source, destination MAC Address
- Type: Indicates higher layer protocol (Mostly IP but others possible, e.g. Novell IPX, AppleTalk)
- CRC: Cyclic Redundancy Check at receiver

7.7 Switches

Switches and Routers are rather similar:

- Both are store-and-forward
- Both have forwarding tables

Switches	Routers
Link-layer devices	Network-layer devices
Learn forwarding table using flooding, learning, MAC addresses	Compute table using routing algorithms, IP addresses

7.7.1 Self-learning

- When the switch receives a frame, it will record sender/location pair in switch table and learn of the location of the sender.

7.8 Virtual Local Area Network (VLANs)

- Made up of switch(es) supporting VLAN capabilities to define multiple virtual LANs over single physical LAN infrastructure
- **Port-based VLANs**
    i. *Single physical switch can operate as multiple virtual switches:* Switch ports are grouped by switch management software
    ii. *Traffic Isolation:* Frames to/from ports 1-8 can only reach ports 1-8
    iii. *Dynamic Membership:* Ports can be dynamically assigned among VLANs
    iv. *Trunk port:* Carries frames between VLANs defined over multiple physical switches

802. IQ VLAN frame format

Preamble	Destination	Source	NEW	Type	Data (Payload)	CRC

NEW:

- 2-byte Tag Protocol Identifier
- Tag Control Information
  - 3-bit priority field like IP TOS
  - 1 bit drop eligible indicator
  - 12 bit VLAN ID field

7.9 Example of all layers together!

A typical scenario:

1. Laptop tries to connect to the Internet and requires the following:
   i. its IP address
   ii. First-hop router address
   iii. DNS server address
2. Make a DHCP request encapsulated in IP & 802.3 Ethernet
3. Broadcast Ethernet frame on LAN, and the router running the DHCP router receives it.
   i. This frame is demuxed to IP, UDP demuxed to DHCP
   ii. DHCP Server formulate DHCP ACK containing what the client wants
   iii. Encapsulate frame at DHCP server and forward (Switch Learning) through LAN
4. Client demultiplexes the DHCP frame and receive the ACK reply

8 Lecture 21: Wireless Networks

Examples:

	Single hop	**Multiple hop**
Infrastructure	*WiFi*, *cellular* Host connect to base station which connects to larger internet	*Mesh Net* Host have to relay through several wireless nodes to connect to larger internet
No infrastructure (**No base station + no connection to larger internet**)	*Bluetooth*	*MANET*, *VANET*

8.1 802.11 Wireless LAN

- Basic Service Set (BSS) in infrastructure mode consists of wireless hosts and access point
- Host communicates with a base station, known as an access point (AP).
- 802.11b spectrum divided into 11 channels at different frequency
  - Admin choose frequency for AP
- Channel can be same as that chosen by neighboring AP, which may result in **interference**
  - Under **Carrier Sense Multiple Access** (CSMA)
    - *Collision Detection*: Collisions are detected within short time to reduce channel wastage
      - Easy in wired LANs: can measure signal strength, and compare transmitted, received signals
      - Difficult in wireless LANs: Received signal strength overwhelmed by local transmission strength
    - *Collision Avoidance:*
      - Sender Channel sensed idle → transmit entire frame
      - Sender Channel sensed busy → defer transmission by starting random *backoff time* and transmit when timer expires. *This interval increases exponentially if no ACK.*
- Host associates with an AP by scanning channels, listening for **beacon frames** containing AP's name (SSID) and MAC address and selecting one to associate with
  - There are 2 types of scanning: Passive, Active
    - Passive: APs will send beacon frames
    - Active: Host broadcast Probe Reuqest Frame + AP will send Probe Response Frames
  - Then, the host will send Association Request Frame to the selected AP and the selected AP will send Association Response Frame back.
  - Typically run DHCP to get IP address in the selected AP's subnet

8.1.1 Mobility within same subnet

- When hosts are **moving between diff APs in the same subnet**, then the self-learning switch will see frame from the host and remember which switch port can be used to reach the hosts.
    - If diff subnets, then the host will probably lose connection.
    - Otherwise, OUT OF SYLLABUS

8.1.2 Rate Adaptation

Rate adaptation allows transmission to be done at different rates within the wireless network, depending upon the network conditions.

- Adaptor can detect channel condition in real-time
- Plotted in a Signal Noise Ratio (SNR) vs Bit Error Rate (BER) graph
- As the mobile moves away from base station
    - BER ↑, SNR ↓
    - When BER becomes too high, switch to a lower transmission rate but with lower BER.

8.1.3 Power Management

Beacon Frame: Contains list of mobiles with AP-to-mobile frames waiting to be sent

1. Node stays awake if AP-to-mobile frames are to be sent.
2. Otherwise node tells AP "I am going to zzz until next **beacon frame**"
3. AP say "ok then i don't transmit frames to you"
4. Node autowakes up before next beacon frame.

8.2 Mobile Networks

8.2.1 Cellular Network Architecture

Components of the architecture

2G:

- BTS: Base Transceiver Station
- BSC: Base Station Controller
- MSC: Mobile Switching Center

3G:

- SGSN: Serving GPRS Support Node
- GGSN: Gateway GPRS Support Node

4G:

- UE: User Element
- MME: Mobility Management Entity
- HSS: Home Subscriber Server
- S-GW: Serving Gateway
- P-GW: Packet data network Gateway
- EPC: Evolved Packet Core

Network	What changed	Components
3G	New Cellular Data Network operates in parallel with existing cellular voice network. Voice network is unchanged in core.	SGSN, GGSN
4G	No more separation between voice and data. All traffic is carried over IP core to gateway.	UE, MME, HSS, S-GW, P-GW, EPC

8.2.2 Handling Mobility

Handoff with common MSC

1. Old BSS: "Oi MSC, i want to HOTO, this is the list of new BSSs"
2. MSC: "Ok i set up new path and allocate resources for these new BSS"
3. New BSS tries to prepare to take over and allocates radio channel for use by mobile
4. After finishing, the New BSS signals MSC and old BSS "I am ready"
5. Old BSS tells new BSS: "ok now i really HOTO to you"
6. New BSS signal to activate new channel
7. Mobile signals via new BSS to MSC: "Handoff complete"

✓ Allows stronger signal to/from new BSS: Continuing connectivity and less battery drain

✓ Load Balancing: Free up channel in current BSS

Handoff Between MSCs

Distinguishing networks beyond a single MSC

1. Home Network
    - Network of cellular provider that a mobile is subscribed to
    - Network to which the mobile user's permanent phone number belongs
    - Data Stored in **Home Location Register** (HLR): The database containing permanent cell phone #, profile info, info of current location (even outside the home network)

2. Visited Network
    - Network in which mobile currently resides
    - Data is stored in **Visitor Location Register** (VLR): Database with entry for each user currently in network.
    - A visited network can also be home network

Multi-MSC Chain
Made up by the Anchor MSC (1st MSC visited during call) + other MSCs that are added onto the end of the chain as the mobile moves to new MSC.

- Optional path minimization step to shorten multi-MSC Chain

Consequences of mobility

- Performance
    - There may be packet loss/delay due to handoff / link-layer retransmissions
    - TCP may interpret this loss as congestion, and *decrease cwnd unnecessarily*
    - *Limited bandwidth* of wireless links; wireless behind wired networks by 1-2 orders in terms of speed
- Aside from Performance, there should be minimal impact
    - Best Effort Service Model remained unchanged.
    - TCP and UDP can run over wireless mobile