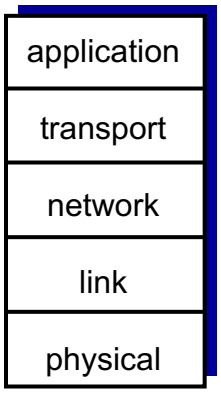
Some Topics for Course Review

CSC 249

MAY 3, 2018

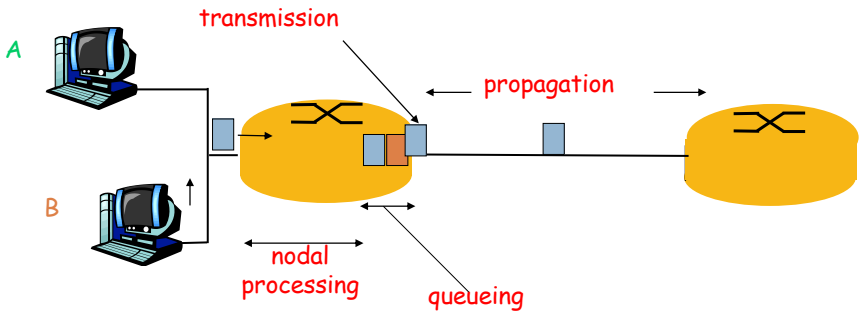
Internet protocol stack (layers)

- *Layer 1 – application:*
  - web browsing, email
- *Layer 2 – transport:* data transfer
- *Layer 3 – network:* routing from source to destination
- *Layer 4 – link:* single hop data transfer
- *Layer 5 – physical:* (electrical signals)



Four sources of packet delay

We will return to these concepts throughout the semester.



3

SMTP, FTP and HTTP

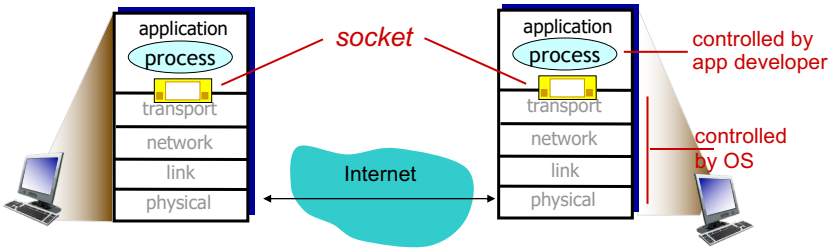
Comparison of basic protocols:

- Push v. pull protocol
- ASCII v. binary data
- Multiple objects in one message or one object per message
- One v. two connections
- Other comparisons?

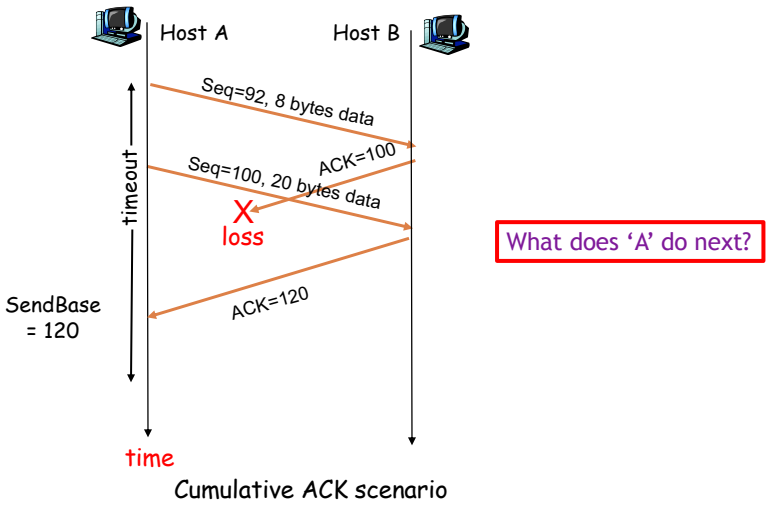
4-4

Sockets

- process sends/receives messages to/from its socket
- socket analogous to door
  - sending process shoves message out door
  - sending process relies on transport infrastructure on other side of door to deliver message to socket at receiving process

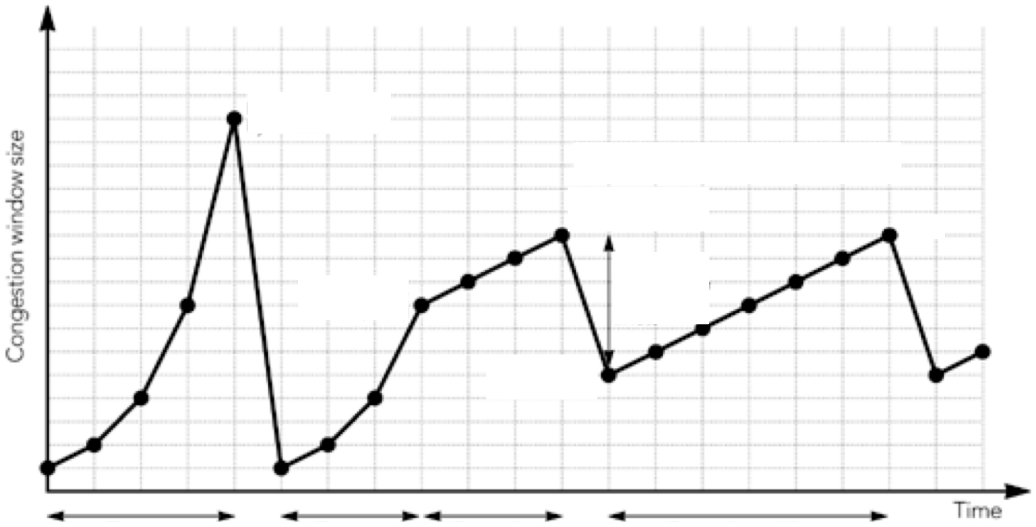


TCP retransmission scenarios (more)



Cumulative ACK scenario

TCP Congestion Control – Identify phases



Transport Layer Review

- The transport layer services are:
  -
  -
  -
  -
- The transport layer **does not** provide:
  -
  -
  -
  -

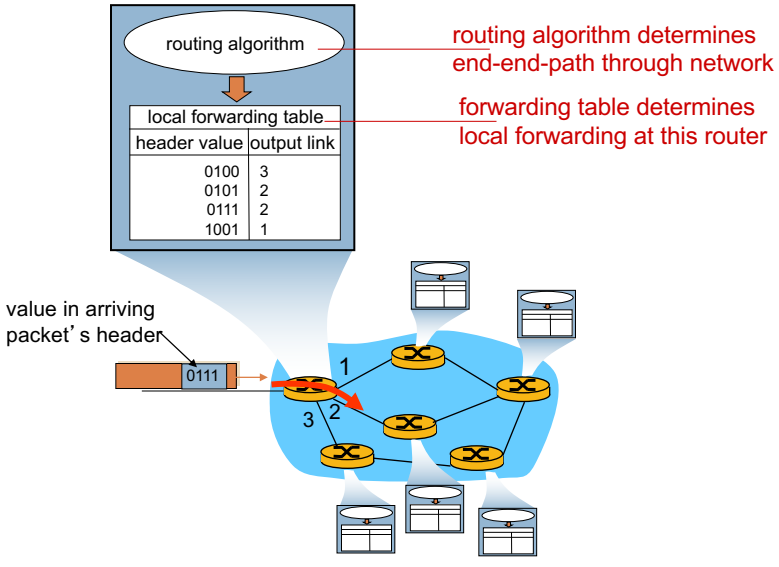
8

Transport Layer Review

- TCP Reliability includes:
  -
  -
  -
  -

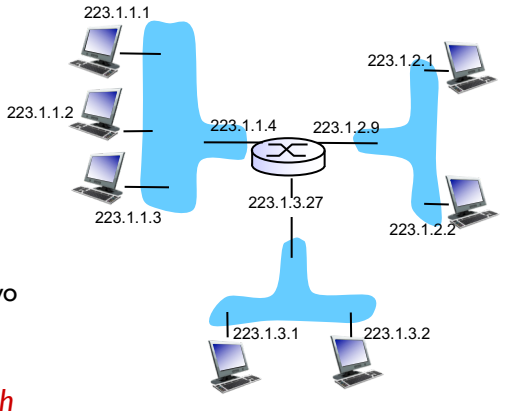
9

Interplay between routing and forwarding



IP addressing: introduction

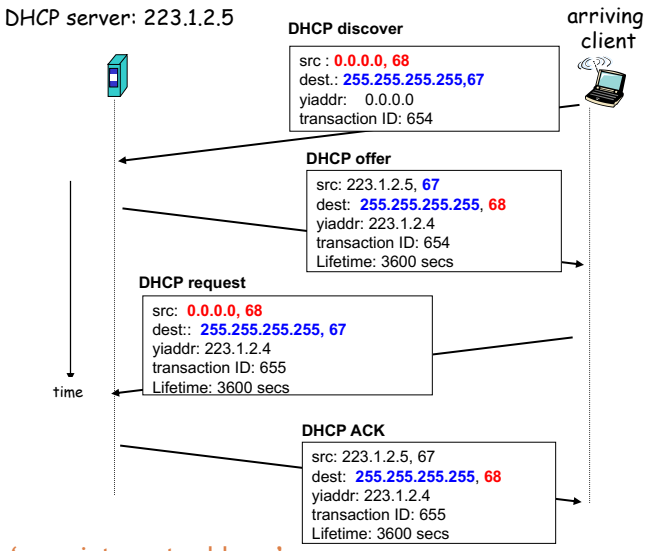
- *IP address:* 32-bit identifier for host, router *interface*
- *interface:* connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)
- *IP addresses associated with each interface*



223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

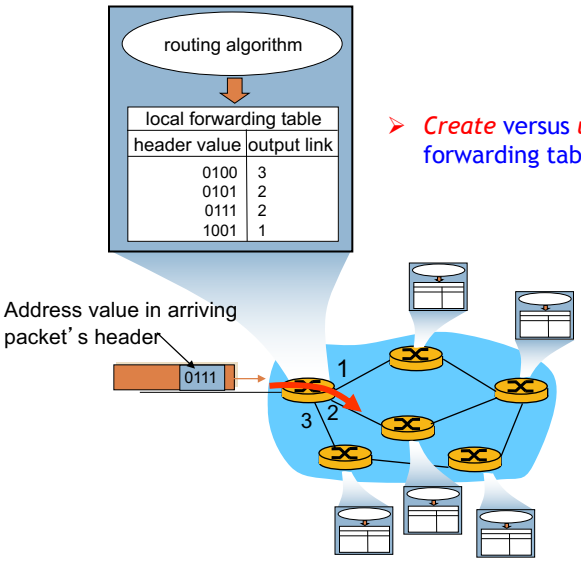
DHCP client-server scenario



yiaddr = 'your internet address'

broadcast address, 255.255.255.255 → sent to every host *in the subnet*

Interplay between routing and forwarding

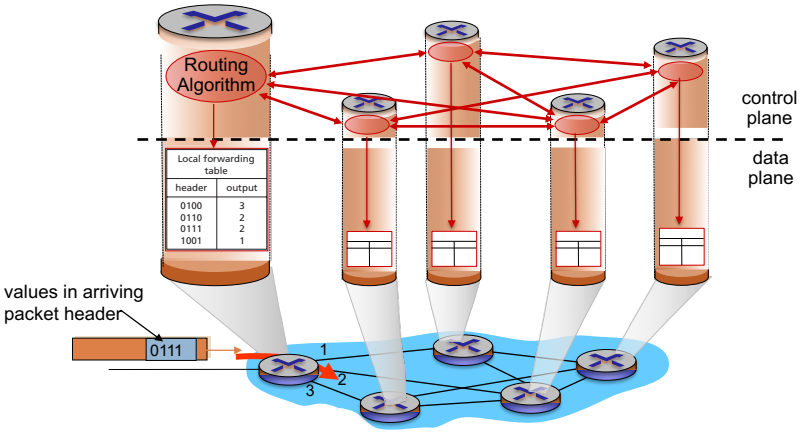


- *Create* versus *use* the forwarding table

13

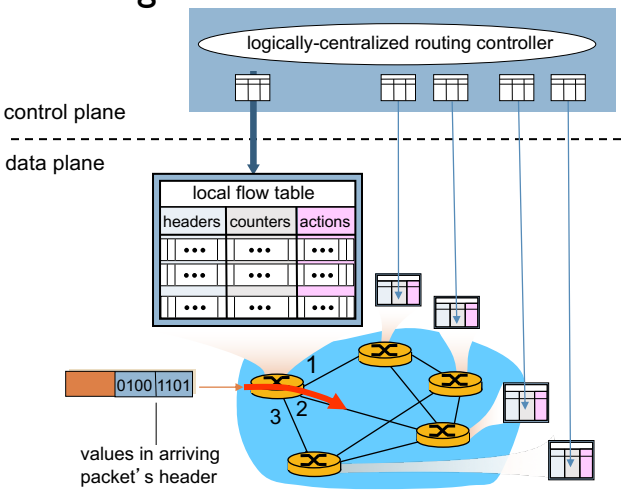
1) Destination-Based Forwarding

- Individual routing algorithm is run *in each and every router.*
- Routers interact with each other in "control plane" to compute forwarding tables
- Traditional approach



3) Generalized Forwarding and SDN

Each router contains a *flow table* that is computed and distributed by a *centralized* routing controller

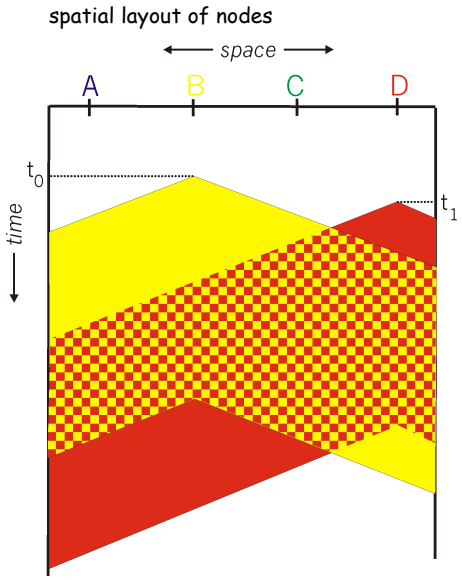


CSMA collisions

collisions *can* still occur:
propagation delay means two nodes may not hear each other's transmission

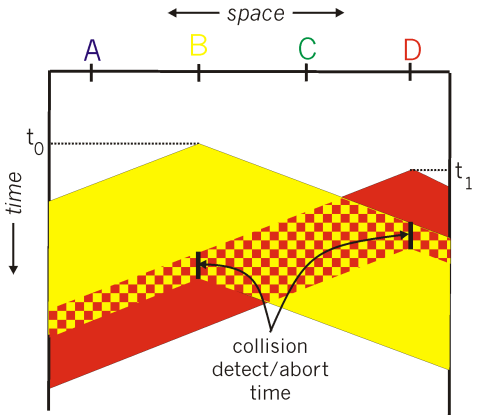
collision:
entire packet transmission time wasted

note:
role of distance & propagation delay in determining collision probability



16

CSMA/CD collision detection



17

Device comparison

- Hub
  -
  -
- Switch
  -
  -
- Router
  -
  -
- SDN Packet Switch
  -
  -

18

Layer	Protocols, and their main features	Happens TO Packet	Action caused BY packet	Action/Event happens on own
Application				
Transport				
Network				
Link				

* Wireless Link Characteristics *

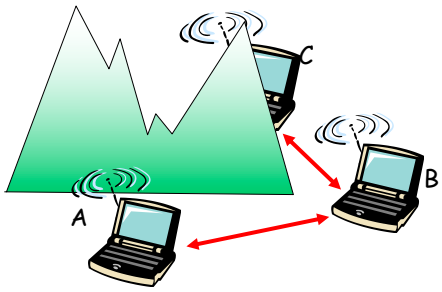
Differences from wired link ….

- decreasing signal strength: EM signal attenuates as it propagates through matter (path loss)
- interference from other sources: wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone, microwave)
- multipath propagation: EM signal reflects off objects, arriving at destination at slightly different times (like echoing)

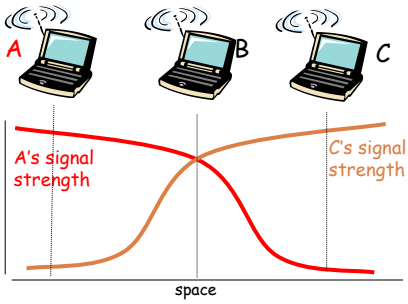
… make communication across (even a point to point) wireless link much more error-prone

Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):

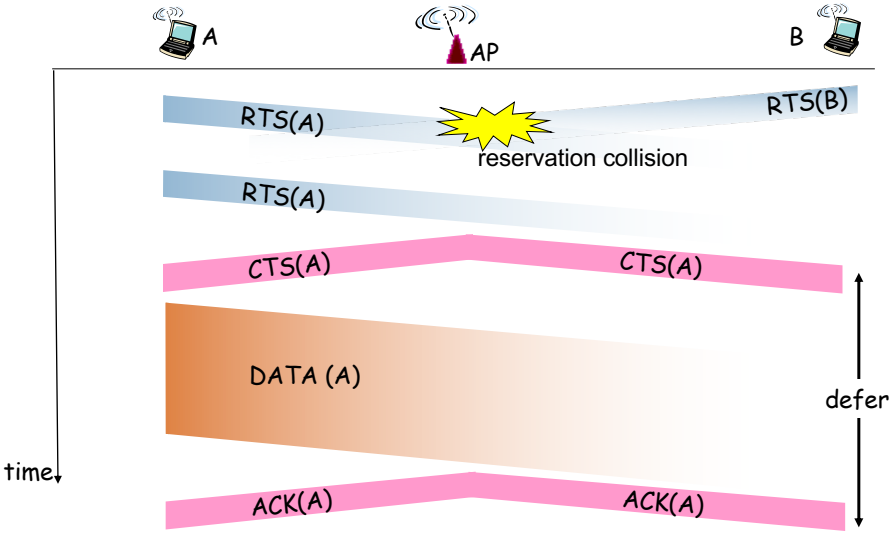


Hidden terminal problem



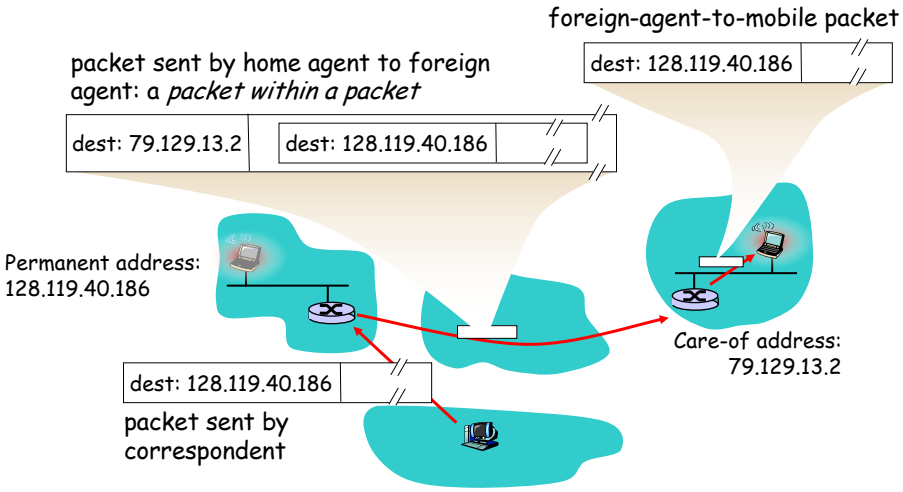
Signal fading

Collision Avoidance: RTS-CTS exchange



22

Mobile IP: indirect routing



23

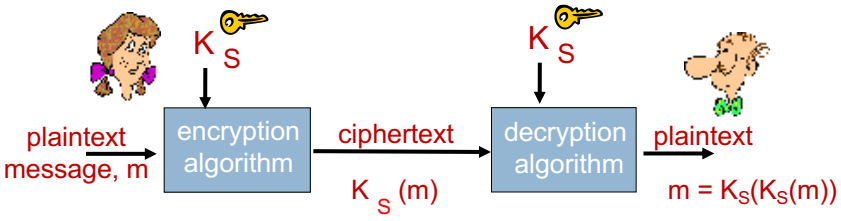
Security Services

1)
2)
3)
4)

Provided via:

1)
2)
3)
4)
5)
6)

Symmetric key cryptography

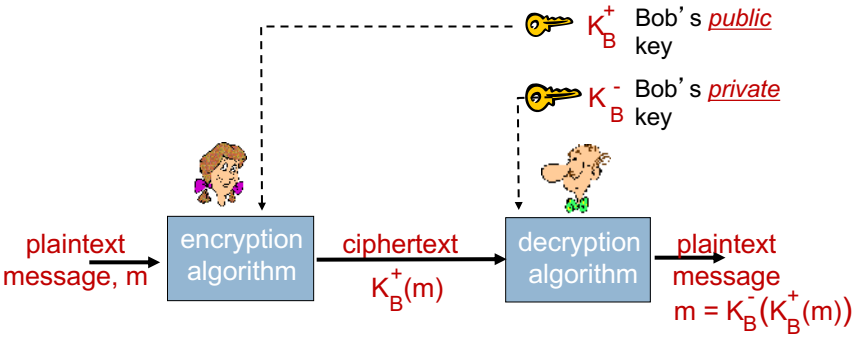


symmetric key crypto: Bob and Alice share same (symmetric) key: K_S

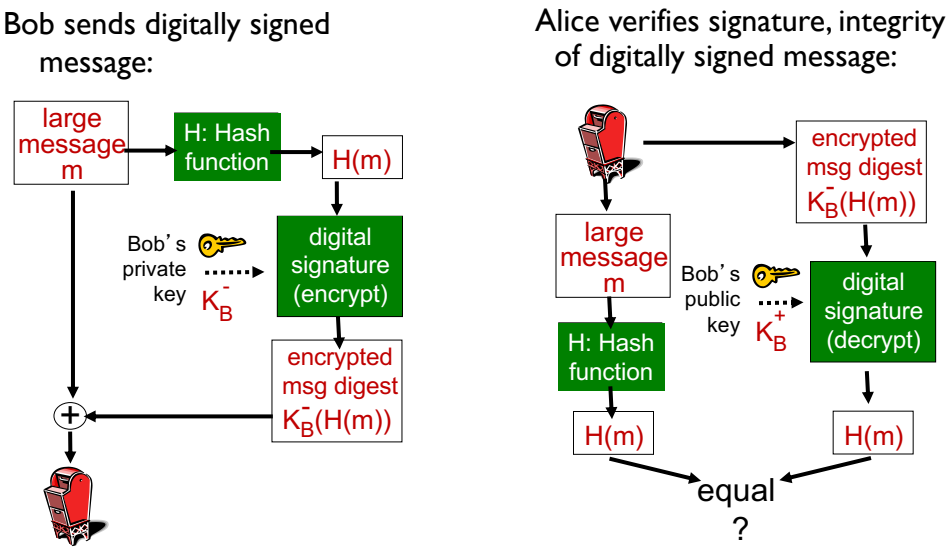
- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

Q: how do Bob and Alice agree on key value?

Public key cryptography

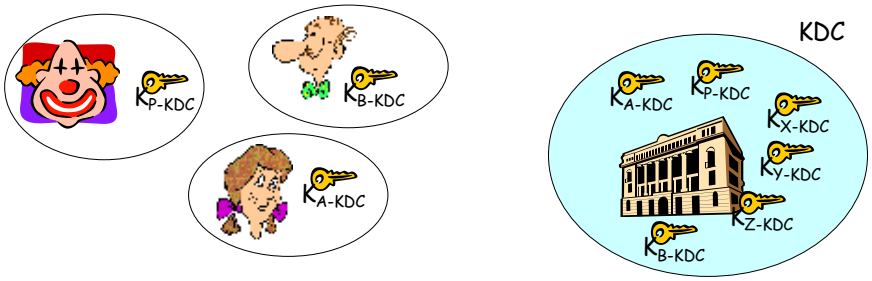


Digital signature = signed message digest



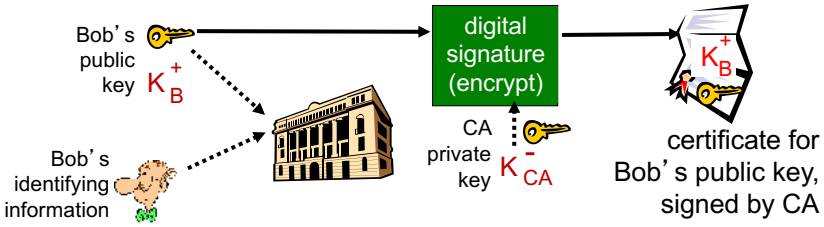
Key Distribution Center (KDC)

- Alice, Bob need shared symmetric key.
- KDC: server shares/knows different secret key for *each* registered user (many users)
  - Alice, Bob know own symmetric keys, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, for communicating with KDC.
  - Permanent / static existence of these 'identity' keys
- KDC creates a unique, single use "session key" for each new communication between Alice and Bob



Certification authorities

- *certification authority (CA):* binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA – CA says "this is E's public key"



Multimedia

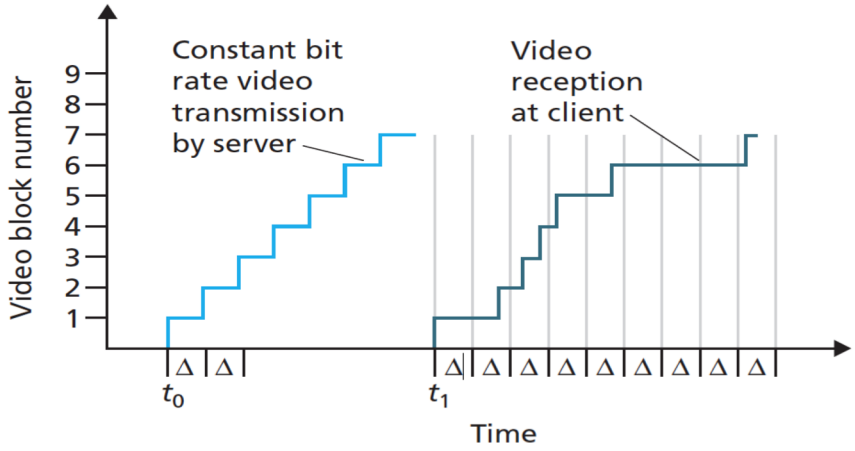
- Multimedia applications can be classified into three categories. Name and describe each category.

- Streaming video systems can be classified into three categories (three stages in protocol evolution). Name and briefly describe each of these categories.

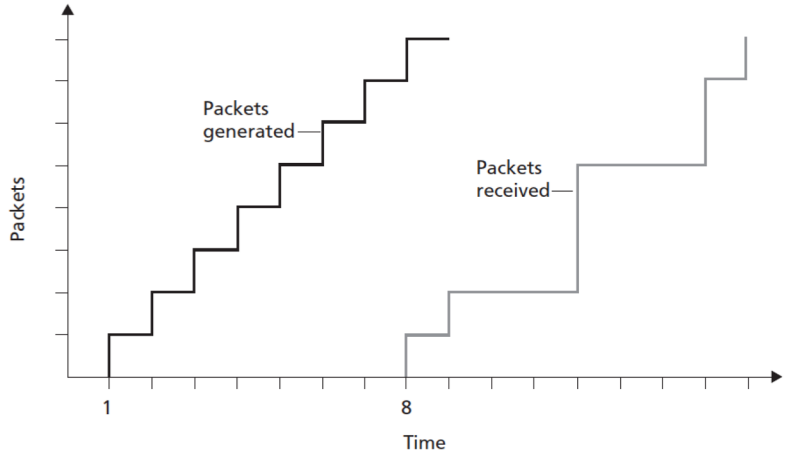
Multimedia: Pre-fetch versus Buffering?

- Client Buffering
  - Streaming: (iii) client begins viewing a few seconds after receiving the first video chunk, at one location in the video, while… (ii) the client also is receiving later portions of the video, while… (iii) the server continues to send the video
    - Avoids the need to download and store the entire video, and so incur a delay in playback if waited to download whole video
- Pre-fetching Data
  - Download/receive the video frames at a **rate** *higher* than the consumption **rate** (frames to be viewed in the future)
  - Prefetched video is stored in the client application buffer
  - Occurs naturally with TCP streaming and congestion avoidance mechanism

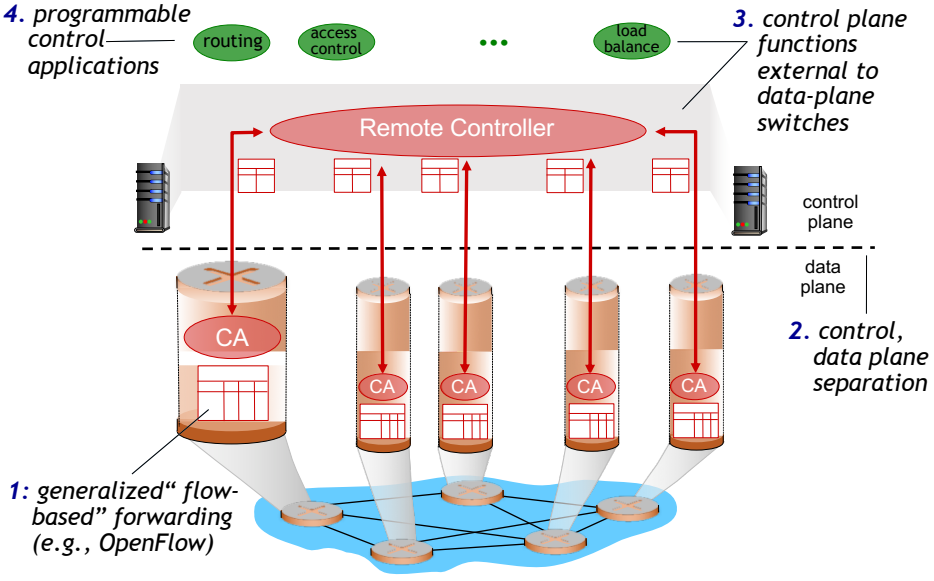
Stored Video Discussion



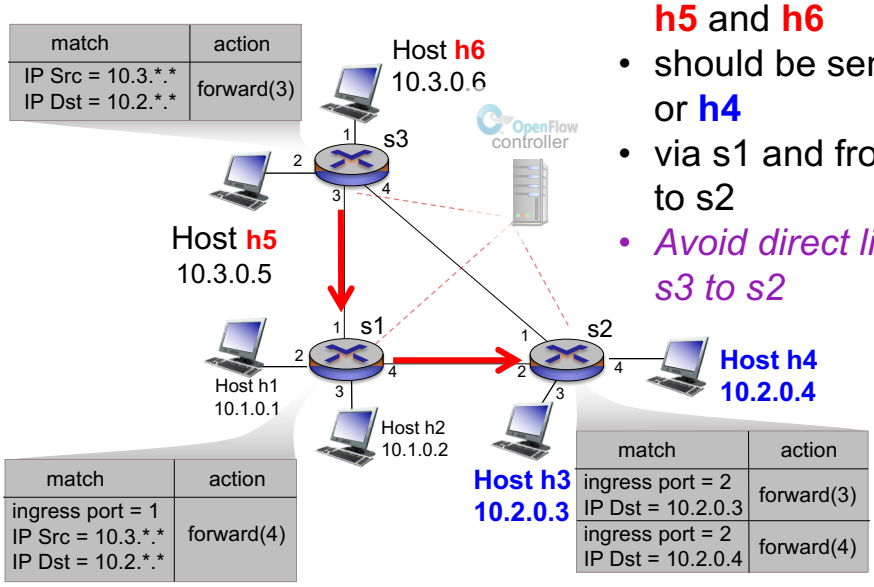
Real-Time Audio Discussion



Software defined networking



OpenFlow example

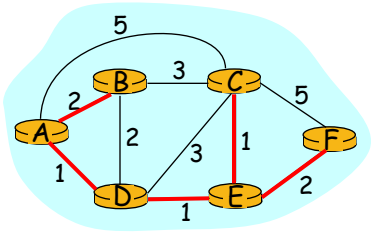


Example:

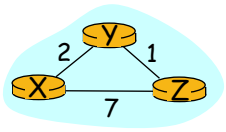
- datagrams from hosts **h5** and **h6**
- should be sent to **h3** or **h4**
- via s1 and from there to s2
- *Avoid direct link from s3 to s2*

Dijkstra's algorithm: example

Step	start N'	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	2,A	5,A	1,A	infinity	infinity
1						
2						
3						
4						
5						



Distance Vector Algorithm: example for *obtaining* complete information



D^X	cost via Y	cost via Z
dest Y		
dest Z		

D^Y	cost via X	cost via Z
dest X		
dest Z		

D^Z	cost via X	cost via Y
dest X		
dest Y		

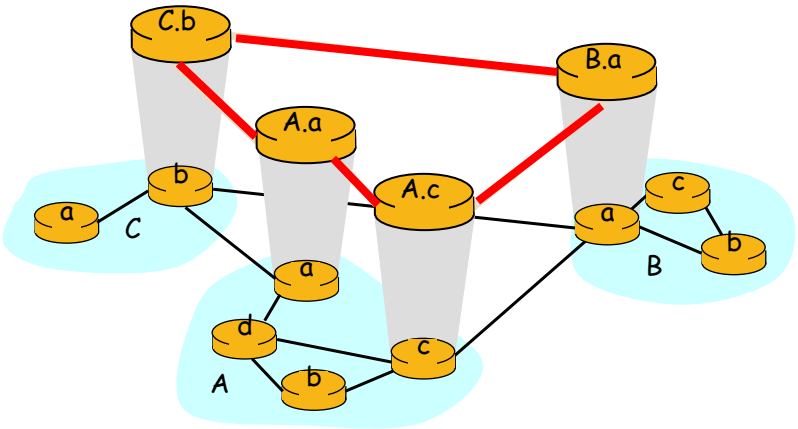
$D^X(Y,Z) = c(X,Z) + \min_w\{D^Z(Y,w)\}$

$= $

$D^X(Z,Y) = c(X,Y) + \min_w\{D^Y(Z,w)\}$

$= $

Inter-AS routing



Discussion Question 2

- What is the difference between a forwarding table for destination-based forwarding and OpenFlow's flow table?
- Each entry in the forwarding table of a destination-based forwarding contains
  1. Only an IP header field value and
  2. The outgoing link interface to which a packet (that matches the IP header field value) is to be forwarded.
- Each entry of the flow table in OpenFlow includes
  1. A set of header field values to which an incoming packet will be matched
  2. A set of counters that are updated as packets are matched to flow table entries (number of packets matched, time since last update…)
  3. A set of actions to be taken when a packet matches a flow table entry, such as forward, duplicate, drop, rewrite header field…

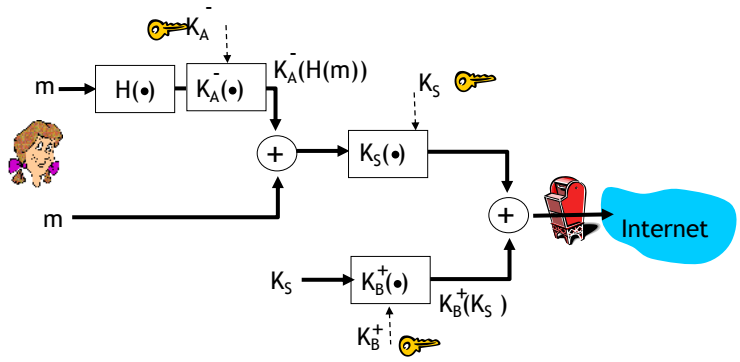
Ethernet CSMA/CD algorithm

1. Adaptor receives datagram from network layer & creates frame
2. If adapter senses channel idle (senses for 96 bit-times), it starts to transmit frame. If it senses channel busy, it waits until channel is idle.
3. If adapter transmits entire frame without detecting another transmission, the adapter is done with frame.
4. If adapter detects another transmission while transmitting, it aborts and sends jam signal
5. After aborting, adapter enters **exponential backoff**:
   1. After the m^{th} collision, adapter chooses a K at random from $\{0,1,2,\ldots,2^m-1\}$.
   2. Adapter waits K·512 bit times and returns to Step 2

48

email: fully secure

- Alice wants to provide secrecy, sender authentication & message integrity.
  …How?



- Alice uses three keys: her private key, Bob's public key, the newly created symmetric key
- What does Bob do to retrieve the msg & be sure it came from Alice?