**------------------------------RDT-----------------------------**

1.0: Reliable transfer, Reliable channel

2.0: channel with bit errors

Question: recover from errors

Solution: 1.error detection. 2. Feedback(ACK, NAK)

2.1: sender, handles grabled ACK/NAK

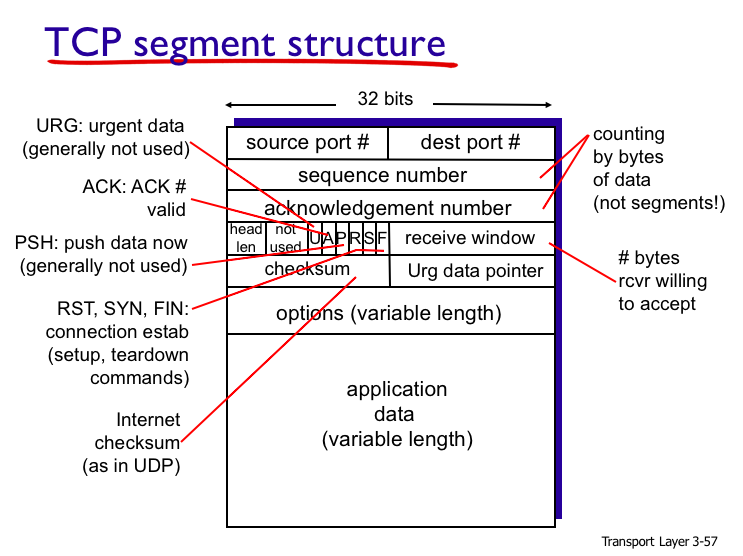
Solution: sequence number

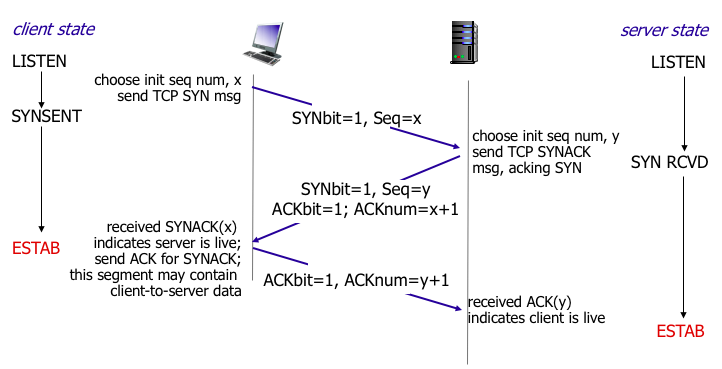
2.2: NAK-free

3.0: channels with errors and loss

Solution: time

**------------------------------TCP-----------------------------**

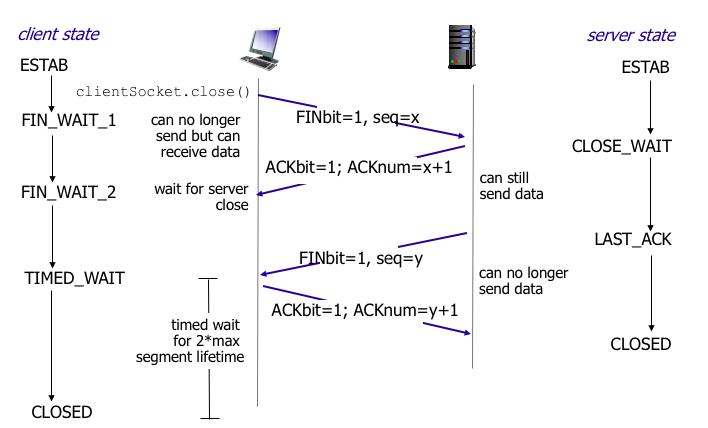


**TCP Congestion Control**:  
**Slow Start**: double cwnd every RTT

**Congestion Avoidance**:

cwnd += (MSS/cwnd)\*MSS upon every incoming non-duplicate ACK

**Time out**: ssthresh = cwnd/2, cwnd=1



**Fast retransmit / fast recovery**:

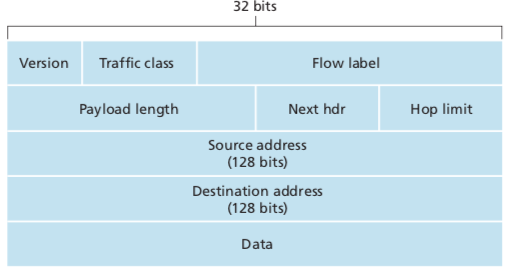
ssthresh = cwnd/2

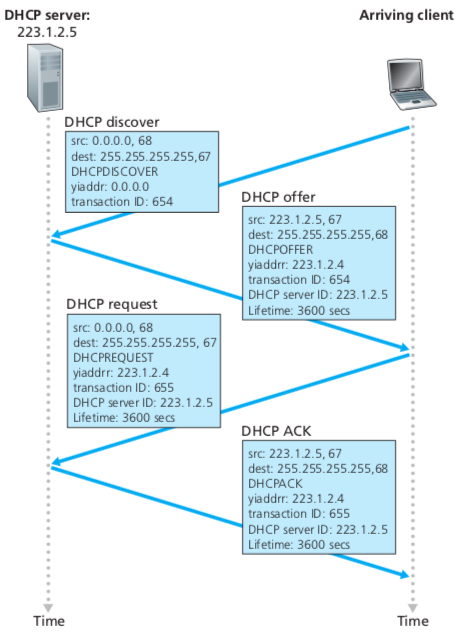
cwnd = ssthresh + 3MSS

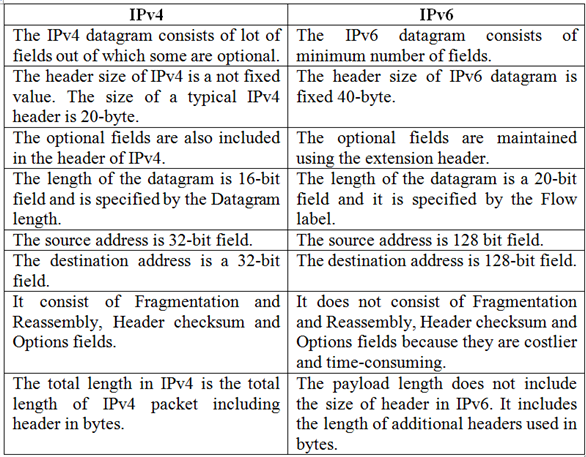
retransmit the lost packet

increase cwnd by 1 MSS upon every duplicate ACK

**------------------------------IPv4 and IPv6-----------------------------**

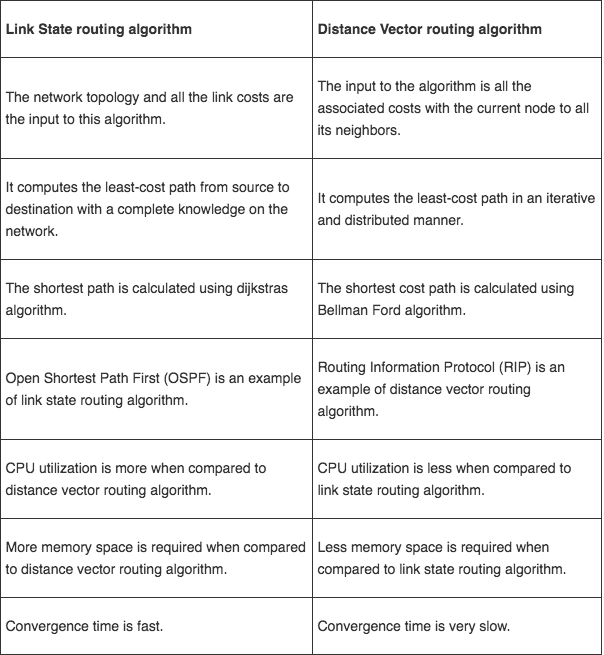
****

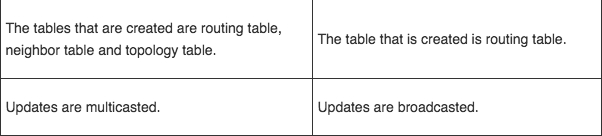
****

****

**------------------------------Link-state vs. distance-vector------------------------------**

****

****

****

**--------------Link-layer---------**

**Services**:

Framing, Link access (MAC), Reliable delivery, Error detection and correction

**Broadcast channel:**

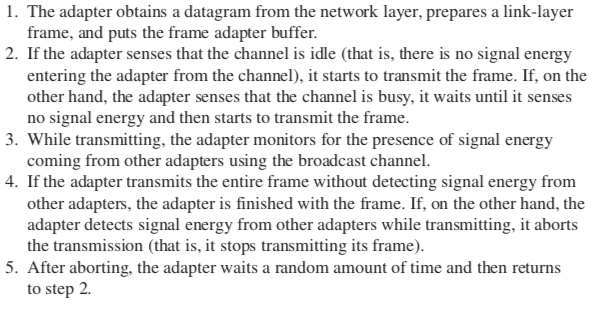
1.One node transfer at full rate 2. Fairness 3. Decentralized

4. Simple and efficient

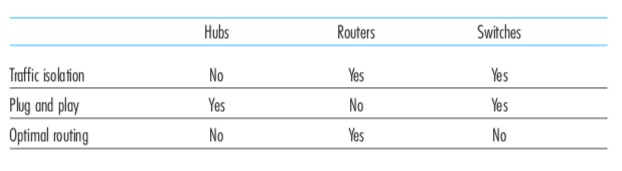
**Category:**

Channel partitioning, random access, taking turns

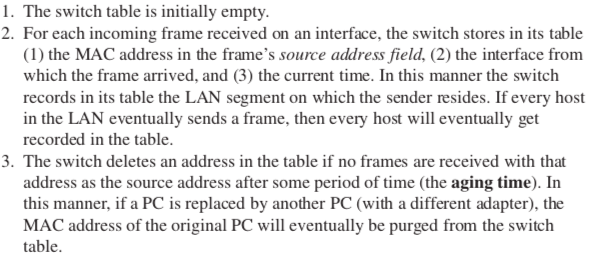
**------------------------------CSMA/CD ------------------------------**

****

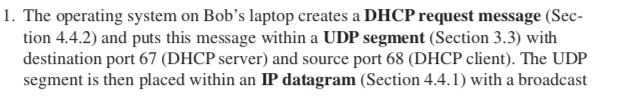
**-------------------------Router vs. Switch-------------------------**

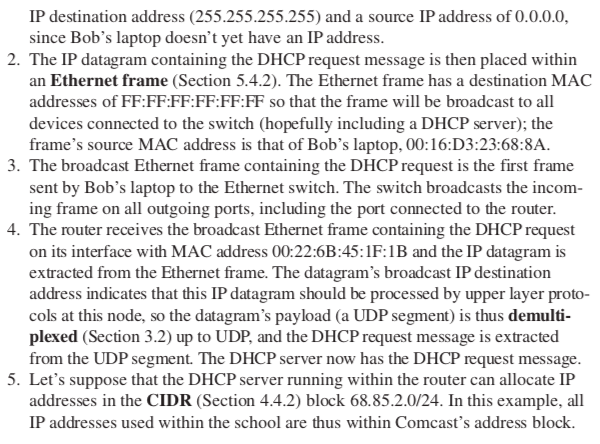
****

**-----------------------Switch self-learning-----------------------**

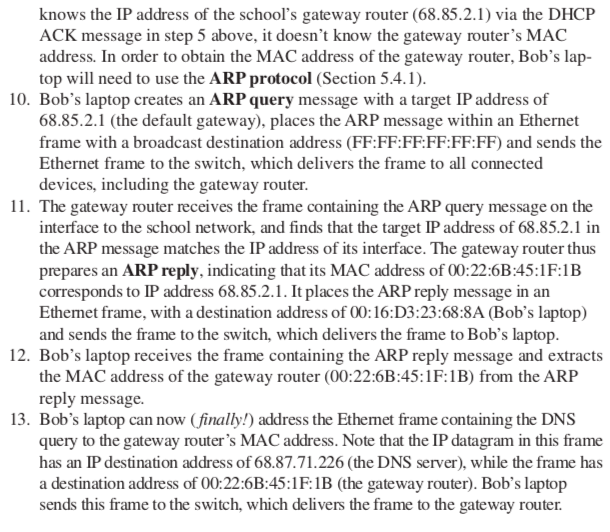
****

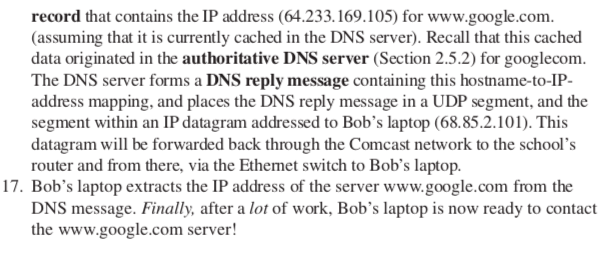
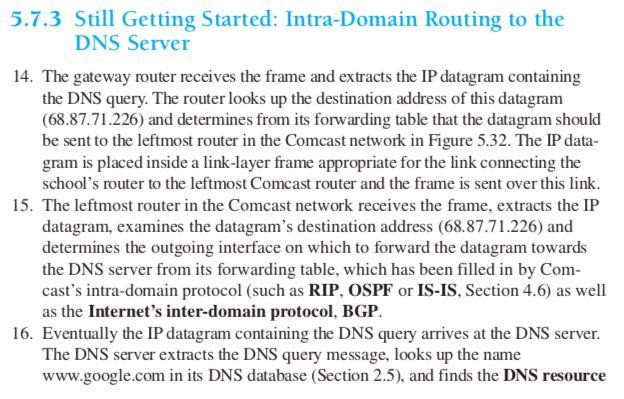
**------------------------------daily life on web------------------------------**

****

****

****

****

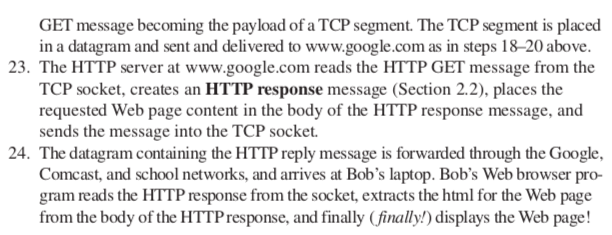
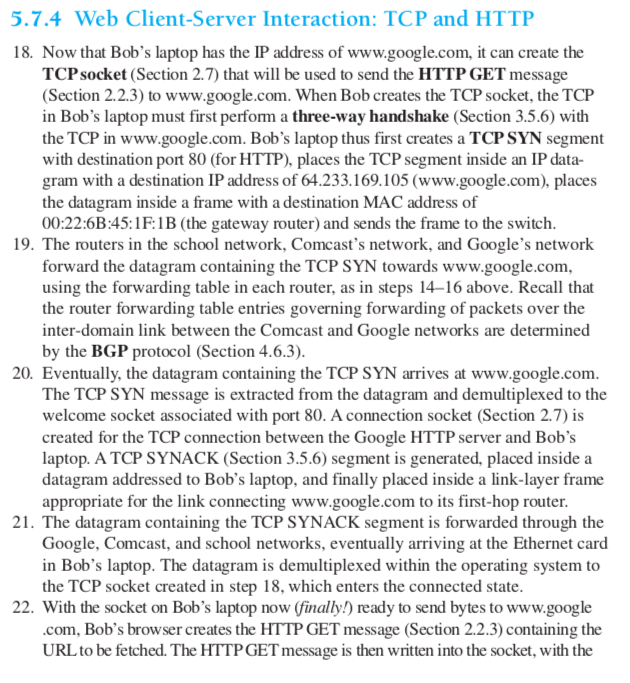
****

**CDMA:**

Channel partitioning

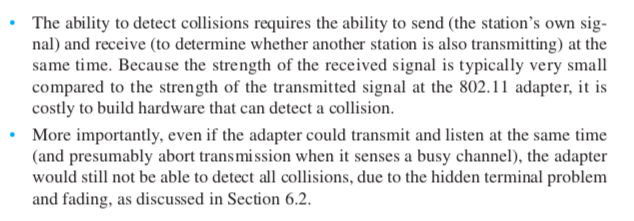
Z = di \* cm

Di=sum(Zi,m\*cm)/M

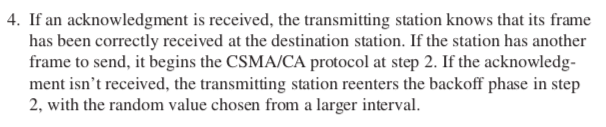
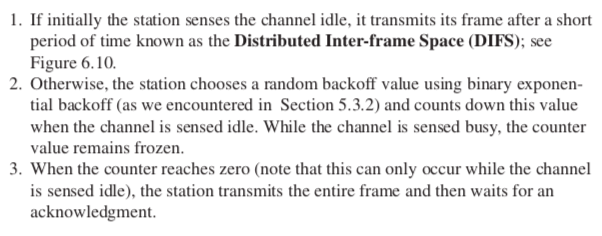
****

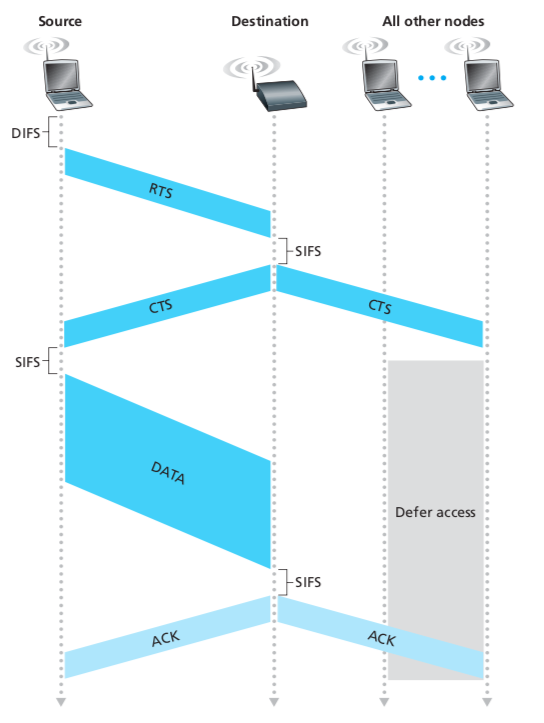
**------------------------------CSMA/CA------------------------------**

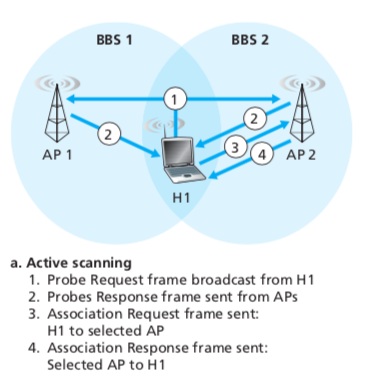
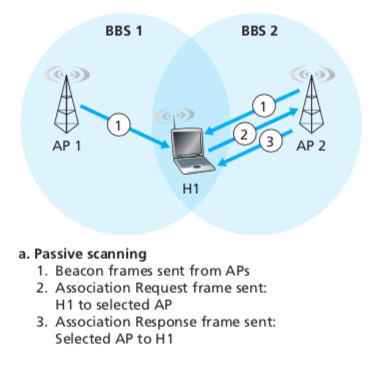
**CA over CD:**

****

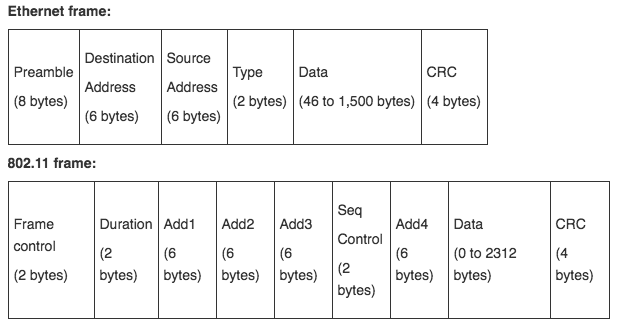
**Details:**

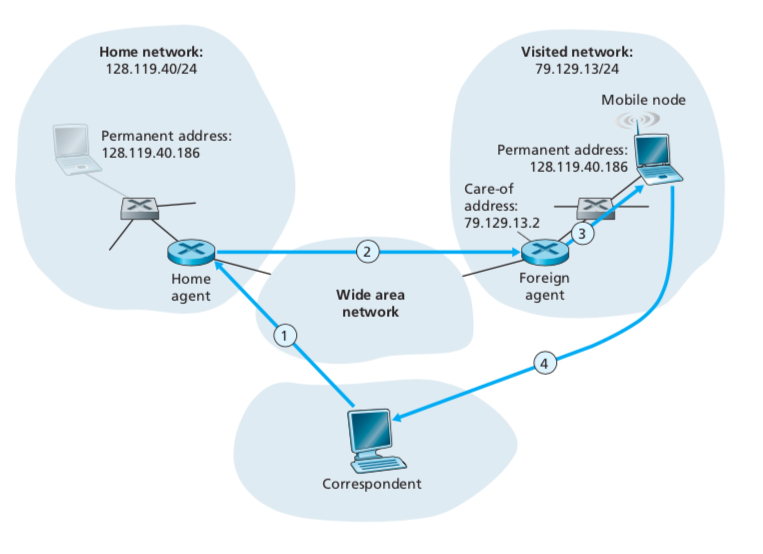
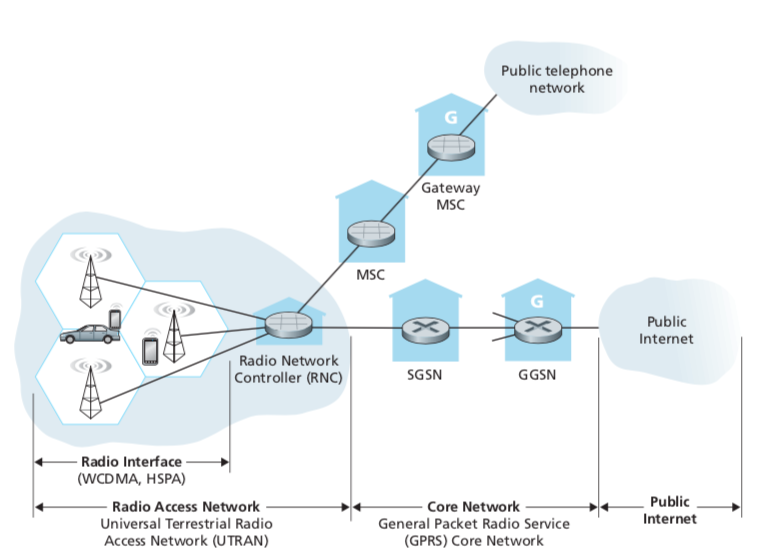
****

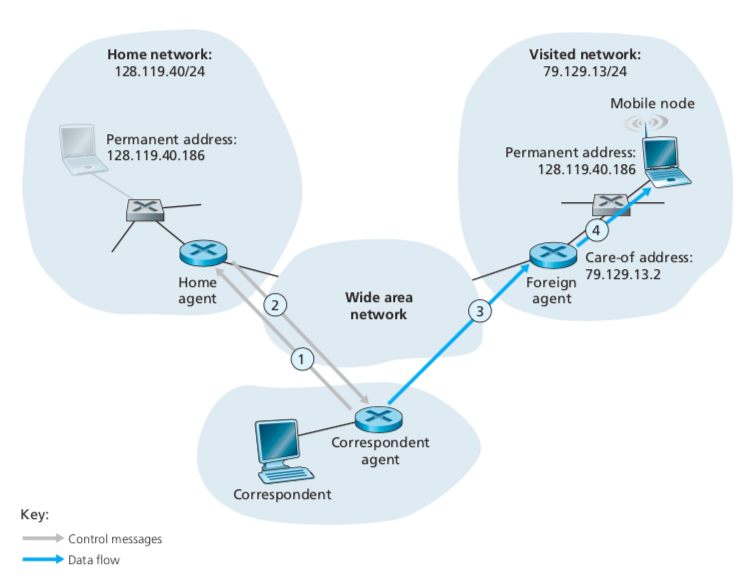
****

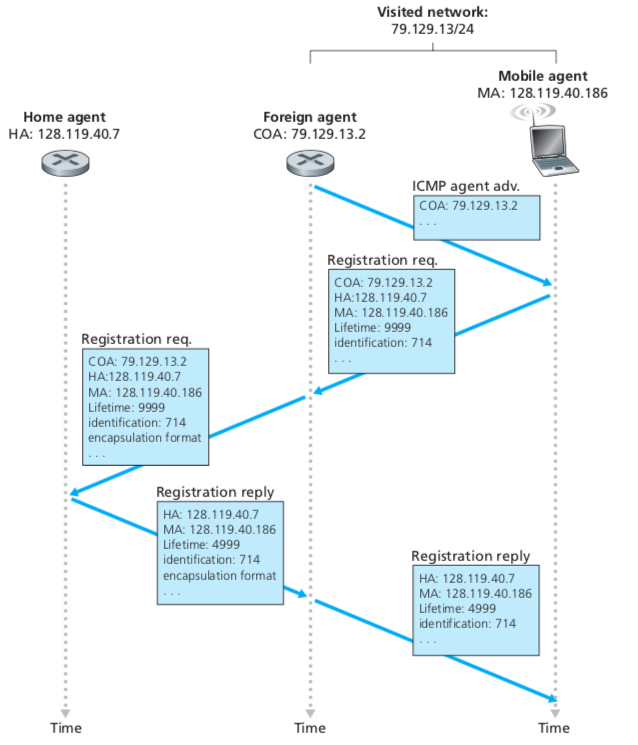
****

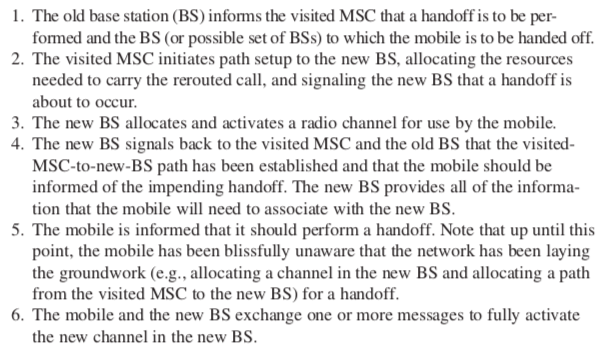
**802.11 frame**

****

**Indirect routing:** 3G

Direct Routing: 

Mobile IP registration: 

Handoff



**Network security**

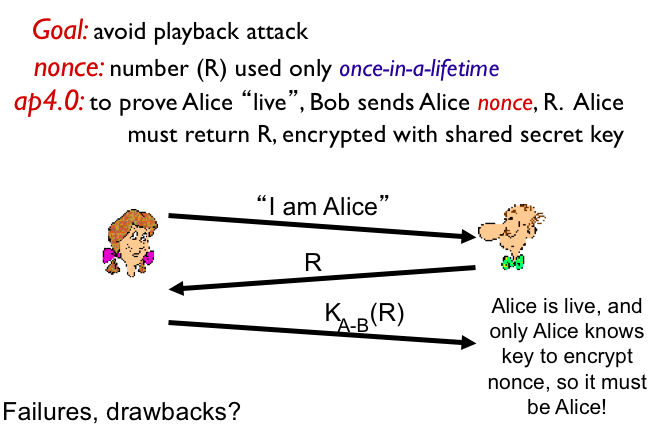
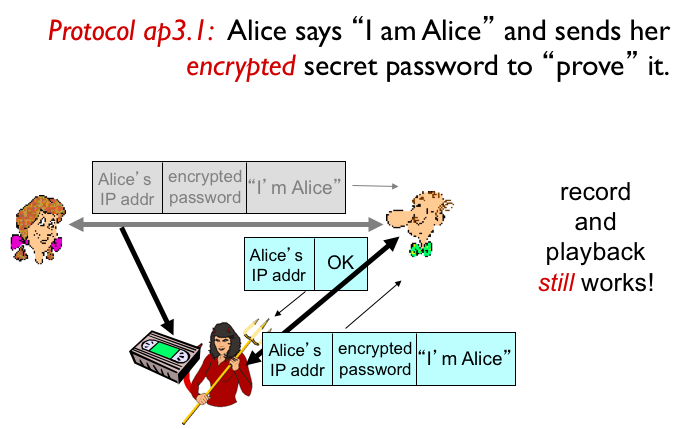
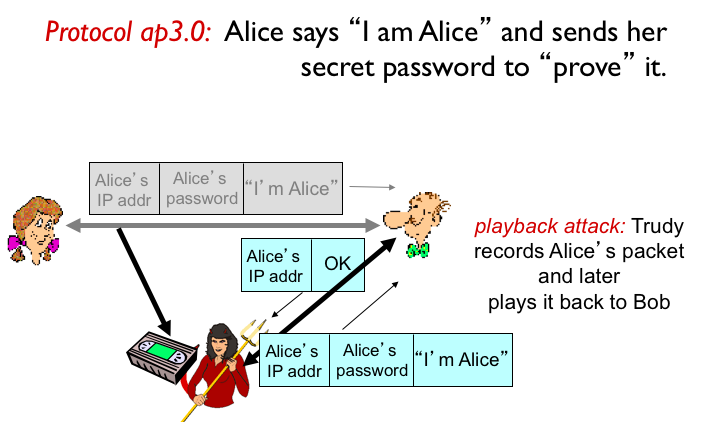
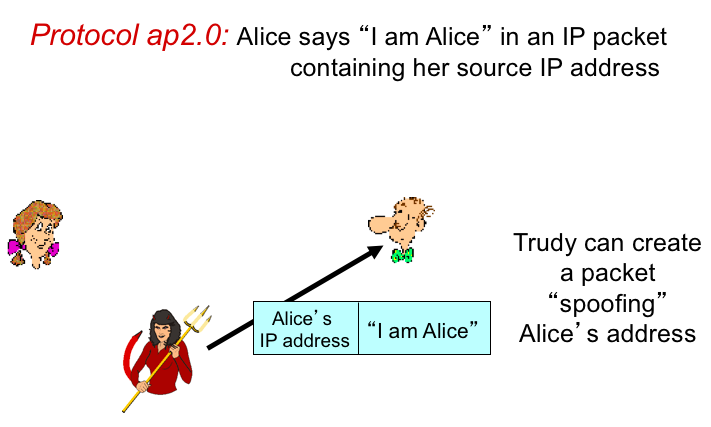
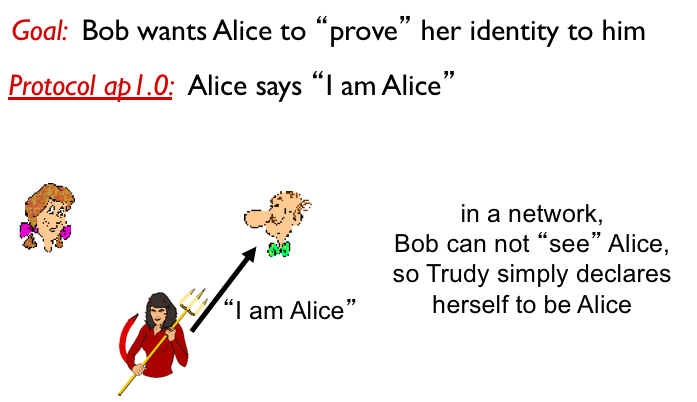
**Confidentiality**: only sender, intended receiver should “understand” message contents

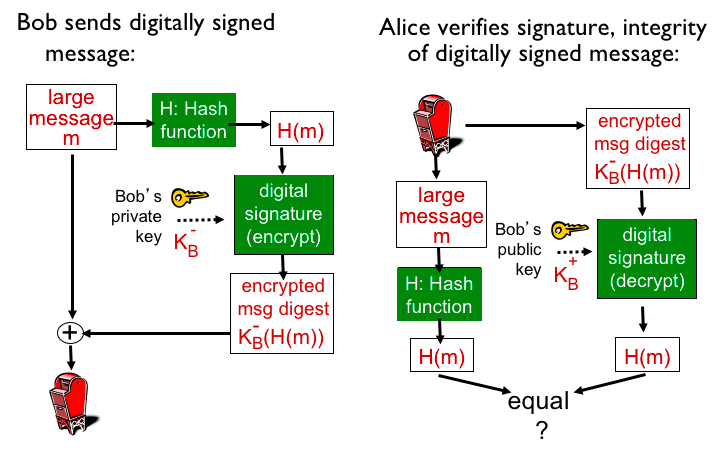
**Authentication**: sender, receiver want to confirm identity of each other

**Message integrity**: sender, receiver want to ensure message not altered without detection

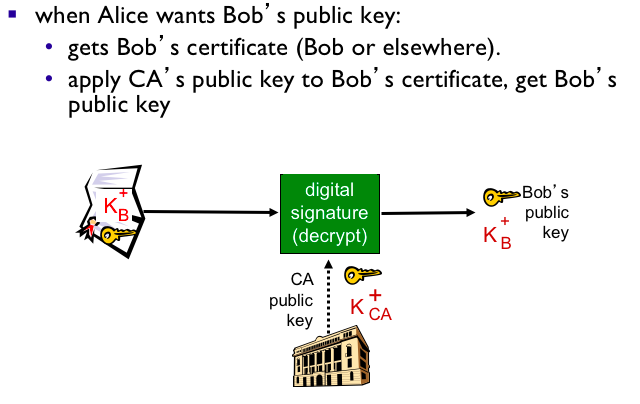
**Access and availability**: service must be accessible and available to users

**Authentication**:



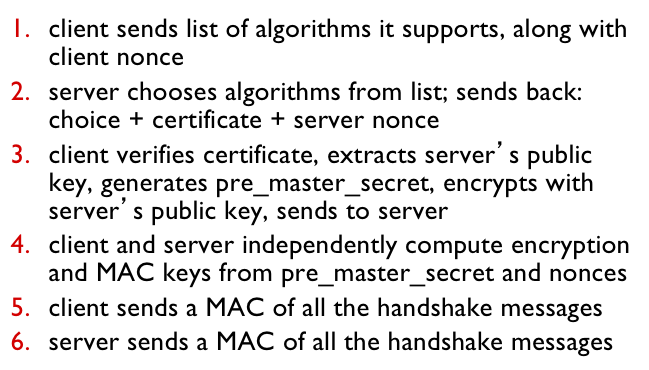
**Digital signature**:

**Certification authority**

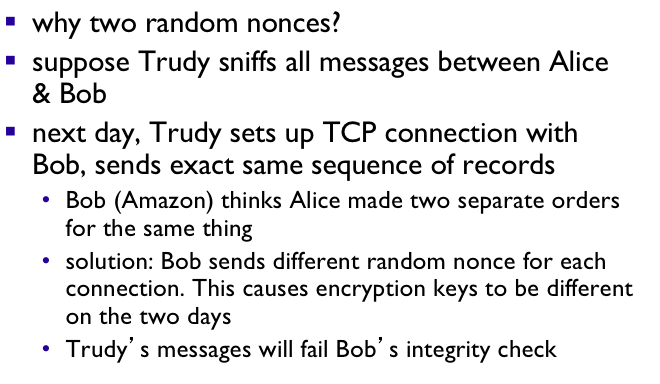


**-------------VPN--------------**

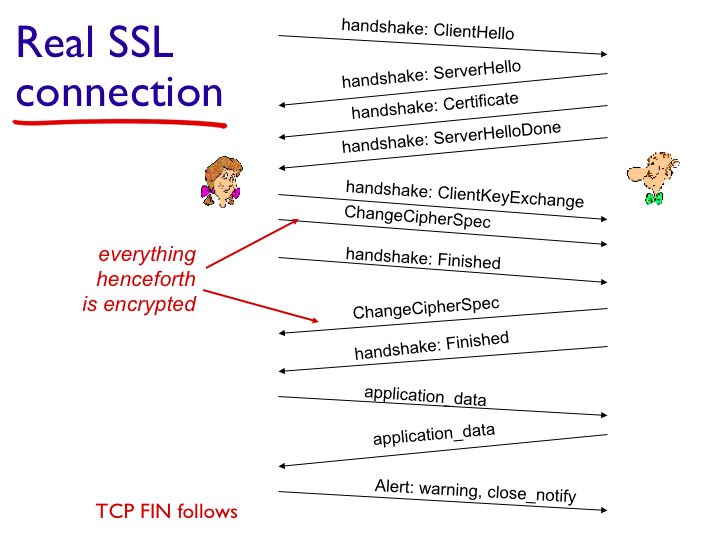
**SSL**



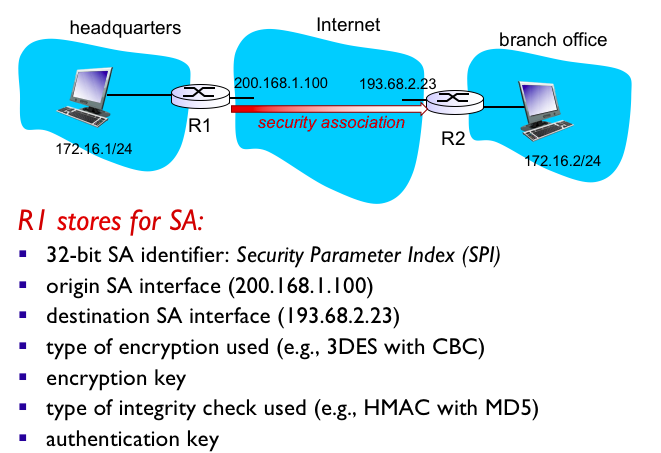
**Why two random nonces?**



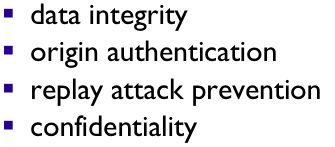
**Real SSL:**



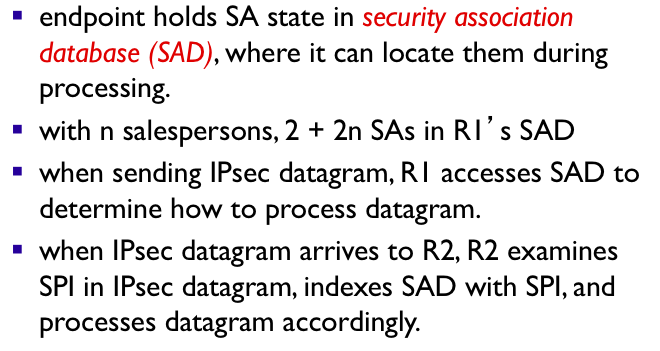
**Example security association:**

****

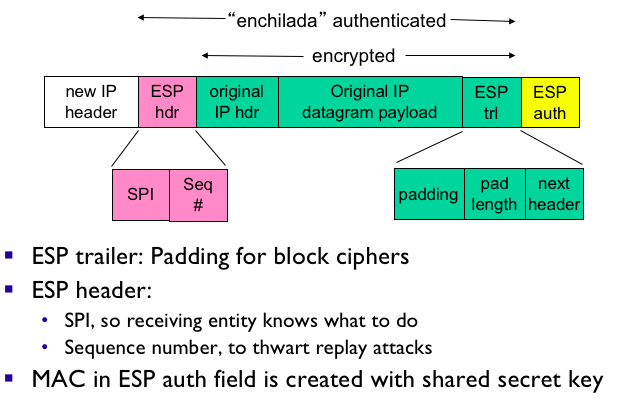
**IPsec Services:**



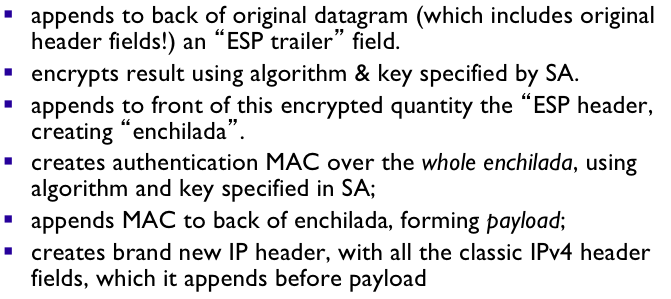
**Security Association database:**

****

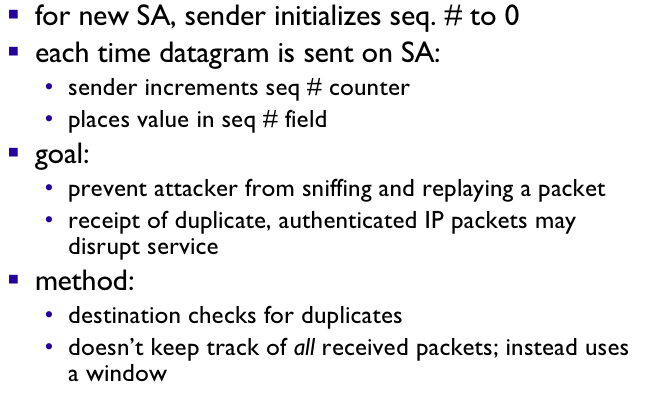
**IPsec datagram:**

****

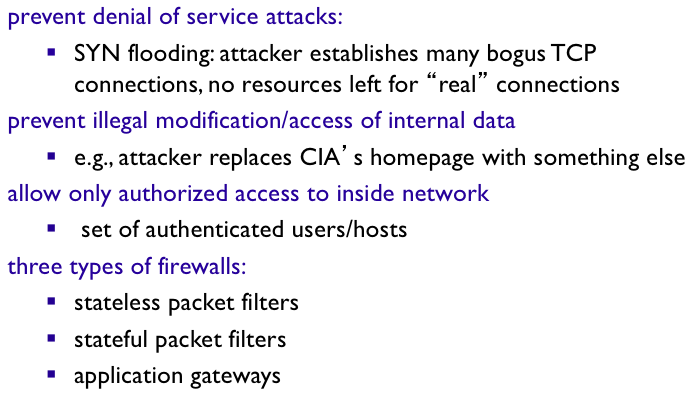
**R1: Convert original datagram to IPsec datagram**

****

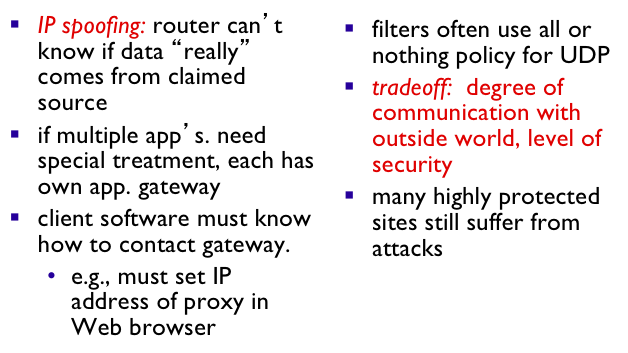
**IPsec seq#:**

****

**Firewalls**

****

**Limitations**

****

**Intrusion detection systems**

****