Slides for Chapter 3: Networking and Internetworking

From Coulouris, Dollimore and Kindberg
Distributed Systems: Concepts and Design
Edition 4, © Pearson Education 2005

Networking Issues (1)
- Performance:
  - Latency (time between send and start to receive)
  - Data transfer rate (bits per second) [max]
  - Transmission time = latency + length / transfer rate
  - System bandwidth, throughput [actual]: total volume of traffic in a given amount of time
  - Using different channels concurrently can make bandwidth > data transfer rate
  - Traffic load can make bandwidth < data transfer rate
  - Network speed < memory speed (about 1000 times)
  - Access to local disk is usually faster than remote disk
  - Fast (expensive) remote disk + fast network
    - Can beat slow (cheap) local disks

Networking Issues (2)
- Scalability
- Reliability
  - Corruption is rare
  - Mechanisms in higher-layers to recover errors
  - Errors are usually timing failures, the receiver doesn’t have resources to handle the messages
- Security
  - Firewall on gateways (entry point to org’s intranet)
  - Encryption is usually in higher-layers
- Mobility
  - Communication is more challenging: locating, routing,
- Quality of service
- Real-time services
- Multicasting
- One-to-many communication

Types of Networks (1)
- Local Area Networks (LAN)
  - Floor/building-wide
  - Single communication medium
  - No routing, broadcast
  - Segments connected by switches or hubs
  - High bandwidth, low latency
  - Ethernet - 10Mbps, 100Mbps, 1Gbps
  - No latency guarantees (what could be the consequences?)
- Personal area networks (PAN) [ad-hoc networks]:
  - Blue tooth, infra-red for PDAs, cell phones, ...

Types of Networks (2)
- Metropolitan Area Networks (MAN)
  - City-wide, up to 50 km
  - Digital Subscriber Line (DSL): .25 - 8 Mbps, 5.5km from switch
    - BellSouth: .8 to 6 Mbps
  - Cable modem: 1.5 Mbps, longer range than DSL
    - Bright house w/ Road Runner: .5 to 10Mbps

Types of Networks (3)
- Wide Area Networks (WAN)
  - World-wide
  - Different organizations
  - Large distances
  - Routed, latency .1 - .5 seconds
  - 1-10 Mbps (upto 600 Mbps)
Types of Networks (4)

Wireless local area networks (WLAN)
- IEEE 802.11 (WiFi)
  - 10-100 Mbps, 1.5km
- 802.11 (1997): up to 2 Mbps, 2.4 GHz
- 802.11a (1999): up to 54 Mbps, 5 GHz, ~75 feet outdoor
- 802.11b (1999): up to 11 Mbps, 2.4 GHz, ~150 feet [most popular]
- 802.11g (2003): up to 54 Mbps, 2.4 GHz, ~150 feet [backward compatible with 802.11b, becoming more popular]

Wireless metropolitan area networks (WMAN)
- IEEE 802.16 (WiMax)
- 1.5-20 Mbps, 5-50km

Types of Networks (5)

Wireless wide area networks (WWAN)
- Worldwide
- GSM (Global System for Mobile communications)
  - 9.6 – 33 kbps
- 3G (‘third generation’): 128-384 kbps to 2Mbps

Types of Networks (6)

Internetworks
- Connecting different kinds of networks
- Routers, gateways

Network performance

<table>
<thead>
<tr>
<th>Example</th>
<th>Range</th>
<th>Bandwidth/Latency (Mbps/ma)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN Ethernet</td>
<td>1.2 km</td>
<td>10-1000</td>
</tr>
<tr>
<td>MAN ATM</td>
<td>250 km</td>
<td>1.150</td>
</tr>
<tr>
<td>WAN IP routing</td>
<td>worldwide</td>
<td>0.5-600</td>
</tr>
<tr>
<td>Internetwork</td>
<td>worldwide</td>
<td>0.5-600</td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPAN Bluetooth</td>
<td>10 - 30m</td>
<td>0.5-2</td>
</tr>
<tr>
<td>WLAN Wi-Fi (802.11)</td>
<td>0.15-1.5 km 2-54</td>
<td>5-20</td>
</tr>
<tr>
<td>WMAN WiMAX (802.16)</td>
<td>350 km</td>
<td>1.5-20</td>
</tr>
<tr>
<td>WWAN GSM, 3G phone nets</td>
<td>worldwide</td>
<td>0.01-2</td>
</tr>
</tbody>
</table>

Network principles (1)

Packet transmission
- Message: logical unit of information
- Packet: transmission unit
- Restricted length: sufficient buffer storage, reduce hogging

Network principles (2)

Data Streaming
- Audio/video
  - Need 120 Mbps (1.5 Mbps compressed)
  - Play time: the time when a frame needs to be displayed
  - For example, 24 frames per second, frame 48 must be displayed after two seconds
  - IP protocol provides no guarantees
    - IPv6 (new) includes features for real-time streams, stream data are treated separately
    - Resource Reservation Protocol (RSVP), Real-time Transport Protocol (RTP)
Network principles (3)

- Switching schemes (transmission between arbitrary nodes)
  - Broadcast: ethernet, token ring, wireless
  - Circuit switching: wires are connected
  - Packet switching:
    - store-and-forward
    - different routes
    - “store-and-forward” needs to buffer the entire packet before forwarding
  - Frame relay
    - Small packets
    - Looks only at the first few bits
    - Don’t buffer/store the entire frame

Network principles (4)

- Protocols
  - Key components
    - Sequence of messages
    - Format of messages

Network principles (5)

- Protocol layers, why?

Network principles (6)

- Encapsulation in layered protocols

Network principles (7)

- ISO Open Systems Interconnection (OSI) model

Network principles (8)

- Internet layers
  - Application = application + presentation
  - Transport = transport + session

Underlying network
  - Network-specific packets
  - Internetwork packets
  - Internetwork protocols
Network principles (9)

- Packet assembly
  - header and data
  - maximum transfer unit (MTU): 1500 for Ethernet
  - 64K for IP (8K is common because of node storage)
- ports: destination abstraction
  (application/service protocol)
- addressing: transport address = network address + port
  - Well-known ports (below 1023)
  - Registered ports (1024 - 49151)
  - Private (up to 65535)

Network principles (10)

- Packet delivery (at the network layer)
  - Datagram packet
    - one-shot, no initial setup
    - different routes, out of order
  - Virtual circuit packet
    - initial setup for resources
    - virtual circuit # for addressing
    - ATM

Similar but different pairs of protocols at the transport layer (connection-oriented and connectionless)

Network principles (11)

- Routing
  - LAN?
  - Routing Algorithm
    - decide which outgoing link to forward the packet
      - for circuit switching, the route is determined during the circuit setup time
      - for packet switching, each packet is routed independently
      - update state of the outgoing links
  - Routing Table
    - a record for each destination
    - fields: outgoing link, cost (e.g. hop count)

Network principles (12)

- Router example

Network principles (13): Routing tables

<table>
<thead>
<tr>
<th>To</th>
<th>Link</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>local</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>D</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Link</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>local</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>D</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Link</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>local</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>D</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Link</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>local</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>D</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To</th>
<th>Link</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>E</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

Network principles (14)

- Router information protocol (RIP)
  - "Bellman-Ford distance vector" algorithm
  - Sender: send table summary periodically (30s) or changes to neighbors
  - Receiver: Consider A receives a table from B, A updates
    - A -> B -> ... -> X: A updates - B has more up-to-date (authoritative) info
    - A -> not B -> ... -> X: Does routing via B have a lower cost?
    - B -> ... -> X: A does not know X
    - [B -> A -> ... -> X]: A doesn’t update - A has more up-to-date info
    - Faulty link, cost is infinity
  - RIP-1 (RFC 1058)
  - More recent algorithms
    - more information, not just neighbors
    - Link-state algorithms, each node responsible for finding the optimum routes
Network principles (15): Pseudocode for RIP routing algorithm

- \( T_l \) is the table local; \( T_r \) is the received remote table

Send: Each 5 seconds or when \( T_l \) changes, send \( T_l \) on each non-faulty outgoing link.

Receive: Whenever a routing table \( T_r \) is received on link \( n \):

- for all rows \( R_r \) in \( T_r \):
  - if \( (R_r\.link = n) \) // destination not routed via the receiver
    - \( R_r\.cost = R_r\.cost + 1 \); \( R_r\.link = n \).
  - if \( (R_r\.destination \) is not in \( T_l \)) add \( R_r \) to \( T_l \);
  - else for all rows \( R_l \) in \( T_l \):
    - if \( (R_l\.destination = R_r\.destination) \) and \( (R_r\.cost < R_l\.cost \) or \( R_l\.link = n) \) \( R_l = R_r \);
    - if \( R_r\.cost < R_l\.cost \) : remote node has better route
    - if \( R_l\.link = n \) : remote node is more authoritative

Network principles (16)

- Congestion control
  - high traffic load, packets dropped due to limited resources
  - reducing transmission rate: "choke packets" from sender to receiver

Networking principles (17)

- Network connecting devices
  - Hubs: extending a segment of LAN (broadcast)
  - Switches: switching traffic at data-link level (different segments of a LAN), making temporary hardware connections between two ports (or store and forward) [switches do not exchange info with each other]
  - Routers: routing traffic at IP level
  - Bridges: linking networks of different types, could be routers as well

Networking principles (18)

- Tunneling
  - communicate through an "alien" protocol
  - "Hide" in the payload
  - IPv6 traffic using IPv4 protocols

Internet protocols (1)

- IP (Internet Protocol)
  - "network" layer protocol
  - IP addresses
- TCP (Transmission Control Protocol)
  - transport layer
  - connection-oriented
- UDP (User Datagram Protocol)
  - transport layer
  - connection-less

Internet protocols (2): TCP/IP layers

Layers
- Application
- Transport
- Internet
- Network interface
- Underlying network

Messages
- Messages (UDP) or Streams (TCP)
- UDP or TCP packets
- IP datagrams
- Network-specific frames
- Network-specific frames
Internet protocols (3): layer encapsulation

![Layer encapsulation diagram]

Internet protocols (4): Programmer’s view

![Programmer’s view diagram]

Internet protocols (5): Internet address structure

**32-bit**

- **Class A**: 0 Network ID 24 Host ID
- **Class B**: 1 Network ID 16 Host ID
- **Class C**: 1 1 Network ID 8 Host ID
- **Class D (multicast)**: 1 1 1 Multicast address
- **Class E (reserved)**: 1 1 1 0 unused

- **Internet protocols (6): Decimal representation**

**163.118.131.9 (www.fit.edu)**

- **Class A**: Network ID 1 to 127 0 to 255 Host ID 0 to 255
- **Class B**: 128 to 191 0 to 255 0 to 255 0 to 255
- **Class C**: 192 to 223 0 to 255 0 to 255 0 to 255
- **Class D (multicast)**: 224 to 239 0 to 255 0 to 255 0 to 255
- **Class E (reserved)**: 240 to 255 0 to 255 0 to 255 0 to 255

**Internet protocols (7)**

- **Classless interdomain routing (CIDR)**
  - shortage of Class B networks
  - add a mask field to indicate bits for network portion
  - 138.73.59.32/22 [subnet: first 22 bits; host: 10 bits]

**Internet protocols (8)**

- **IP address of source**
- **IP address of destination**
- **Data**
- **Header**
  - up to 64 kilobytes
Internet protocols (9): Network Address Translation

X Sharing one "global" IP address at home
X Routers with NAT
   o Router has a "global" IP address from ISP
   o Each machine has a "local" IP address via DHCP
   o Machine -> router
   o Router stores the local IP addr and source port #
   o Table entry indexed by a virtual port #
   o Router -> outside
   o Put the router IP addr and virtual port # in the packet
   o Outside -> router
   o Reply to the router IP addr and virtual port #
   o Router -> machine
   o Use the virtual port # to find table entry
   o Forward to the local IP address and port #
X What happens if we want the device to be a server, not a client?

Internet protocols (10)

Internet protocols (11)

X Server with NAT
   o Fixed internal addr and port #
   o Fixed entry in the table
   o All packets to the port on the router are forwarded to the internal addr and port # in the entry
   o What if more than one internal machines want to offer the same service (port)?

Internet protocols (12)

X IP Protocol
   o Unreliable or best-effort
   o Lost, duplicated, delayed, out of order
   o Header checksum, no data checksum
   o IP packet longer than MTU of the underlying network, break into fragments
   o Before sending and reassemble after receiving
   o Address resolution (on LANS)
      o Mapping IP address to lower level address
      o ARP: address resolution protocol
   o Ethernet: cache; not in cache, broadcast IP addr, receive Ethernet addr
   o IP spoofing: address can be stolen (not authenticated)

Internet protocols (13)

X RIP-1: discussed previously
X RIP-2: CIDR, better multicast routing, authentication of RIP packets
X Link-state algorithms: e.g., open shortest path first (OSPF)
X Observed: average latency of IP packets peaks at 30-seconds intervals [RIP updates are processed before IP]
   o because 30-second RIP update intervals, locked steps
   o Random interval between 15-45 seconds for RIP update
X Large table size
   o All destinations!
   o Map ip to geographical location
   o Default route: store a subset, default to a single link for unlisted destinations

Internet Protocols (14): IPv6

X IPv6 addresses: 128 bits (16 bytes)
X 3 x 10^23 addresses (7 x 10^23 addresses per square meter!)
X Routing speed
   o No data checksum as before
   o No fragmentation – need to know the smallest MTU in data-link layer
X Real-time and special services
   o Traffic class: priority, time-dependent (expired data are useless)
X Flow label: timing requirements for streams (reserving resources in advance)
X "Next" header field
   o Extension header types for IPv6
   o Routing information, authentication, encryption...
   o Anycast: at least one nodes gets it
   o Security
      o Currently handled above the IP layer
      o Extension header types
      o Migration from IPv4
         o Backward compatibility: IPv6 addresses include IPv4 addresses
         o Islands of IPv6 networks, traffic tunnels through other IPv4 networks
Internet protocols (15):

<table>
<thead>
<tr>
<th>Version (4 bits)</th>
<th>Traffic class (8 bits)</th>
<th>Flow label (20 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload length (16 bits)</td>
<td>Next header (8 bits)</td>
<td>Hop limit (8 bits)</td>
</tr>
</tbody>
</table>

Source address (128 bits)

Destination address (128 bits)

---

Internet Protocols (10): Mobile IP

- Dynamic Host Configuration Protocol (DHCP)
  - assign temporary IP address
  - provide addresses of local resources like DNS
- Routing to maintain continuous access
  - IP routing is subnet-based, fixed relative locations
  - Home agent (HA) and Foreign agent (FA)
  - MA - current location (IP addr) of the mobile host
  - FA - informs the mobile host when it moves
  - proxy for the host after it moves
  - inform local routers to remove cached records of the host
  - responds to ARP requests
  - FA - informs the host when it arrives
  - new temp IP addr
  - contacts HA what the new IP address is
  - HA - receives the new IP address and may tell the sender the new IP addr

Internet protocols (11): MobileIP routing mechanism

Internet protocols (12)

- Transport protocols: TCP and UDP
  - network protocol: host to host
  - transport protocol: process to process
  - Port #’s to indicate processes
- UDP
  - no guarantee of delivery
  - checksum is optional
  - max of 64 bytes, same as IP
  - no setup costs, no segments

Internet protocols (13)

- TCP
  - arbitrarily long sequence
  - connection-oriented
  - sequencing of segments
  - flow control: acknowledgement includes "window size" (amount of data) for sender to send before next ack
  - interactive service: higher frequency of buffer flush, send when deadline reached or buffer reaches MTU
  - retransmission of lost packets
  - buffering of incoming packets to preserve order and flow
  - checksum on header and data

Internet protocols (14)

- Domain names
- DNS
  - distributed data
  - each DNS server keeps track of part of the hierarchy
  - unresolved requests are sent to servers higher in the hierarchy
Internet protocols (15)

- Firewalls
  - monitor and filter communication
  - controlling what services are available to the outside
  - controlling the use of services
  - controlling internal users access to the outside
- Filtering at different protocol levels
  - IP packet filtering: addresses, ports...
  - TCP gateway: check for correctness in TCP connections
  - e.g., are they partially opened and never used (why?)
  - Application-level gateway: proxy for applications
  - no direct communication between the inside and outside
  - e.g., smtp proxy can check addresses, content...

Internet protocols (16)

- Bastion (tcp/ application filter)
- C): two router filters
  - Access to web/ftp server, but not LAN
  - Hide internal IP addresses
  - Bastion has the mapping
  - Second router is the second IP filter (invisible to the outside)

Internet protocols (17)

- Virtual Private Network (VPN)
  - extending a secured internal network to an external unsecured host
  - e.g. IP'Sec tunneling through IP

Network Case Studies (1): Ethernet and WiFi

<table>
<thead>
<tr>
<th>IEEE No.</th>
<th>Name</th>
<th>Title</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.3</td>
<td>Ethernet</td>
<td>CSMA/CD Networks (Ethernet)</td>
<td>[IEEE 1985a]</td>
</tr>
<tr>
<td>802.4</td>
<td>Token Bus Networks</td>
<td></td>
<td>[IEEE 1985b]</td>
</tr>
<tr>
<td>802.5</td>
<td>Token Ring Networks</td>
<td></td>
<td>[IEEE 1985c]</td>
</tr>
<tr>
<td>802.6</td>
<td>Metropolitan Area Networks</td>
<td></td>
<td>[IEEE 1994]</td>
</tr>
<tr>
<td>802.11</td>
<td>WiFi</td>
<td>Wireless Local Area Networks</td>
<td>[IEEE 1999]</td>
</tr>
<tr>
<td>802.15.1</td>
<td>Bluetooth</td>
<td>Wireless Personal Area Networks</td>
<td>[IEEE 2002]</td>
</tr>
<tr>
<td>802.15.4</td>
<td>ZigBee</td>
<td>Wireless Sensor Networks</td>
<td>[IEEE 2003]</td>
</tr>
<tr>
<td>802.16</td>
<td>WiMAX</td>
<td>Wireless Metropolitan Area Network</td>
<td>[IEEE 2004a]</td>
</tr>
</tbody>
</table>

Network Case Studies (2): Ethernet

- Ethernet, CSMA/CD, IEEE 802.3
  - Xerox Palo Alto Research Center (PARC), 1973, 3Mbps
  - 10,100,1000 Mbps
  - extending a segment: hubs and repeaters
  - connecting segments: switches and bridges
  - Contention bus
  - Packet/frame format
    - preamble (7 bytes): hardware timing
    - start frame delimiter (1)
    - dest addr (6)
    - src addr (6)
    - length (2)
    - data: 46 - 1500 bytes: min total becomes 64 bytes, max total is 1518
    - checksum (4): dropped if incorrect

Network Case Studies (3)

- Carrier Sensing Multiple Access / Collision Detection (CSMA/CD)
  - CS: listen before transmitting, transmit only when no traffic
  - MA: more than one can transmit
  - CD: collision detected when signals transmitted are not the same as those received (listen to its own transmission)
  - After detection of a collision
    - send jamming signal
    - wait for a random period before retransmitting
  - T (Tau): time to reach the farthest station
  - When is the collision detected?
    - A and B send at the same time
    - A sends, B sends within T seconds
    - A sends, B sends between T and 2T seconds
    - A sends, B sends after 2T seconds
  - Minimum length of packet for collision detection:
    - packet length > 2T, between T and 2T, and < T?
Network Case Studies (4)

- Physical implementation:
  - \( R \times B \times L \)
  - \( R \): data rate in Mbps
  - \( B \): medium signaling type: baseband [one channel] or broadband [multiple channels]
  - \( L \): max segment length in 100meters or T (twisted pair cable, hierarchy of hubs)

Network Case Studies (5): Ranges and speeds

<table>
<thead>
<tr>
<th></th>
<th>10Base5</th>
<th>10BaseT</th>
<th>100BaseT</th>
<th>1000BaseT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data rate</td>
<td>10 Mbps</td>
<td>10 Mbps</td>
<td>100 Mbps</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td>Max. segment lengths:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twisted wire (UTP)</td>
<td>100 m</td>
<td>100 m</td>
<td>100 m</td>
<td>25 m</td>
</tr>
<tr>
<td>Coaxial cable (STP)</td>
<td>500 m</td>
<td>500 m</td>
<td>500 m</td>
<td>25 m</td>
</tr>
<tr>
<td>Multi-mode fibre</td>
<td>2000 m</td>
<td>2000 m</td>
<td>500 m</td>
<td>500 m</td>
</tr>
<tr>
<td>Mono-mode fibre</td>
<td>25000 m</td>
<td>25000 m</td>
<td>20000 m</td>
<td>2000 m</td>
</tr>
</tbody>
</table>

Network Case Studies (6): WiFi

- IEEE 802.11 wireless LAN
  - up to 150m and 54Mbps
  - access point (base station) to land wires
  - Ad hoc network—no specific access points, "on the fly" network among machines in the neighborhood
  - Radio Frequency (2.4, 5GHz band) or infra-red

Network Case Studies (7): Problems with wireless CSMA/CD

- Hidden station: not able to detect another station is transmitting
  - A can't see D, or vice versa
- Fading: signals weaken, out of range
  - A and C are out of range from each other
- Collision masking: stronger signals could hide others
  - A and C are out of range from each other, both transmit, collide, can't detect collision, Access point gets garbage

Network Case Studies (8)

- Carrier sensing multiple access with collision avoidance (CSMA/CA)
  - reserving slots to transmit
  - if no carrier signal
    - medium is available,
    - out-of-range station requesting a slot, or
    - out-of-range station using a slot

Network Case Studies (9)

- Steps
  1. Request to send (RTS) from sender to receiver, specify duration
  2. Clear to send (CTS) in reply
  3. in-range stations see the RTS and/or CTS and its duration
  4. in-range stations stop transmitting
  5. acknowledgement from the receiver
- Hidden station & Fading: CTS, need permission to transmit
- RTS and CTS are short, don't usually collide; random back off if collision detected
- Should have no collisions, send only when a slot is reserved