15-441: Computer Networking

Lecture 24: Wireless Networking

Wireless Challenges

- Force us to rethink many assumptions
- Need to share airwaves rather than wire
  - Don’t know what hosts are involved
  - Host may not be using same link technology
- Mobility
- Other characteristics of wireless
  - Noisy → lots of losses
  - Slow
  - Interaction of multiple transmitters at receiver
    - Collisions, capture, interference
  - Multipath interference

Overview

- Internet mobility
- TCP over noisy links
- Link layer challenges

Routing to Mobile Nodes

- Obvious solution: have mobile nodes advertise route to mobile address/32
  - Should work!!!
- Why is this bad?
  - Consider forwarding tables on backbone routers
    - Would have an entry for each mobile host
    - Not very scalable
- What are some possible solutions?

How to Handle Mobile Nodes? (Addressing)

- Dynamic Host Configuration (DHCP)
  - Host gets new IP address in new locations
  - Problems
    - Host does not have constant name/address → how do others contact host
    - What happens to active transport connections?

How to Handle Mobile Nodes? (Naming)

- Naming
  - Use DHCP and update name-address mapping whenever host changes address
  - Fixes contact problem but not broken transport connections

How to Handle Mobile Nodes? (Transport)

- TCP currently uses 4 tuple to describe connection
  - <Src Addr, Src port, Dst addr, Dst port>
- Modify TCP to allow peer’s address to be changed during connection
- Security issues
  - Can someone easily hijack connection?
- Difficult deployment → both ends must support mobility

How to Handle Mobile Nodes? (Link Layer)

- Link layer mobility
  - Learning bridges can handle mobility → this is how it is handled at CMU
  - Encapsulated PPP (PPTP) → Have mobile host act like he is connected to original LAN
    - Works for IP AND other network protocols

How to Handle Mobile Nodes? (Routing)

- Allow mobile node to keep same address and name
- How do we deliver IP packets when the endpoint moves?
  - Can’t just have nodes advertise route to their address
- What about packets from the mobile host?
  - Routing not a problem
  - What source address on packet? → this can cause problems
- Key design considerations
  - Scale
  - Incremental deployment

Basic Solution to Mobile Routing

- Same as other problems in computer science
  - Add a level of indirection
- Keep some part of the network informed about current location
  - Need technique to route packets through this location (interception)
- Need to forward packets from this location to mobile host (delivery)

Interception

- Somewhere along normal forwarding path
  - At source
  - Any router along path
  - Router to home network
  - Machine on home network (masquerading as mobile host)
- Clever tricks to force packet to particular destination
  - “Mobile subnet” – assign mobiles a special address range and have special node advertise route

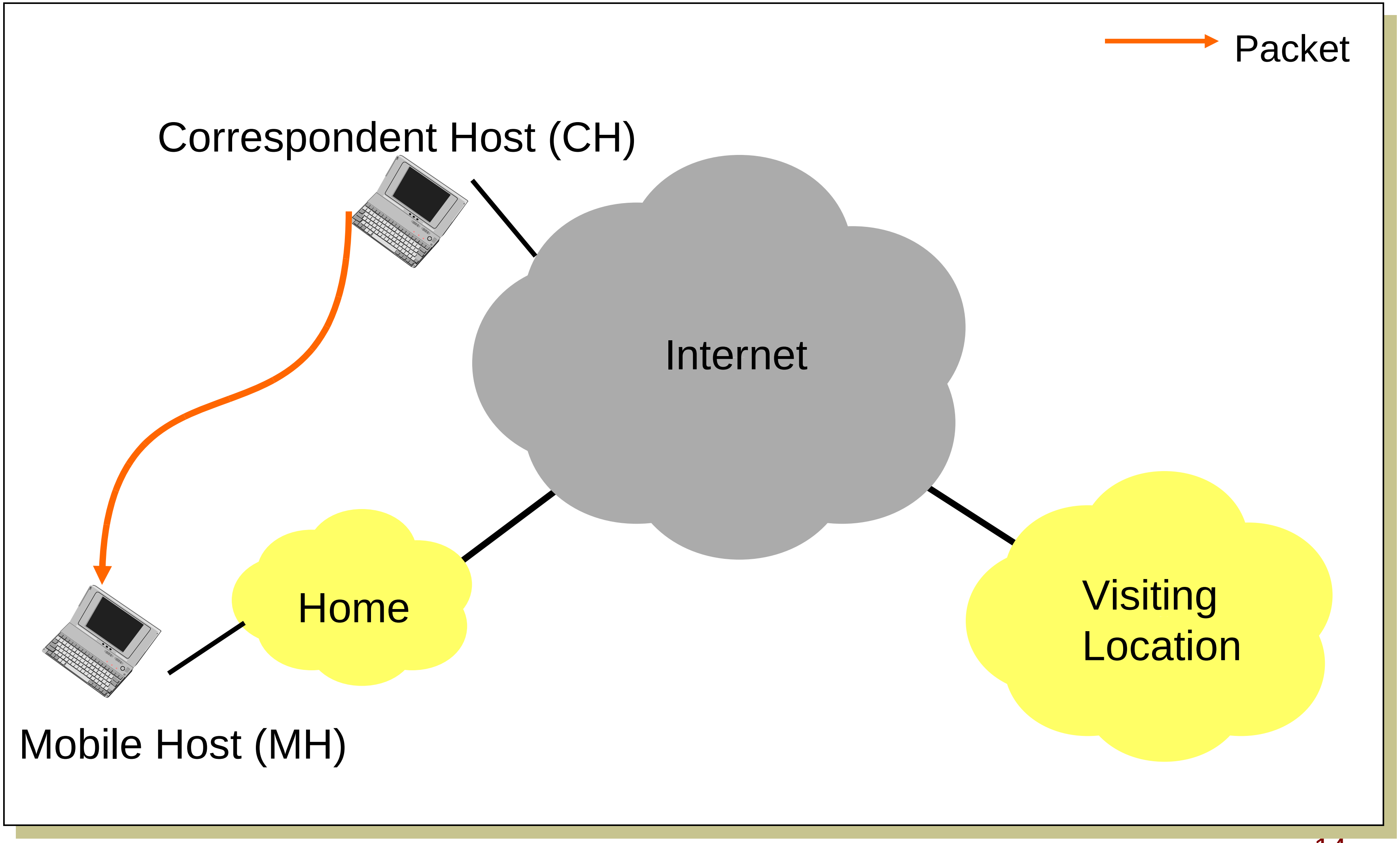
Delivery

- Need to get packet to mobile's current location
- Tunnels
  - Tunnel endpoint = current location
  - Tunnel contents = original packets
- Source routing
  - Loose source route through mobile current location

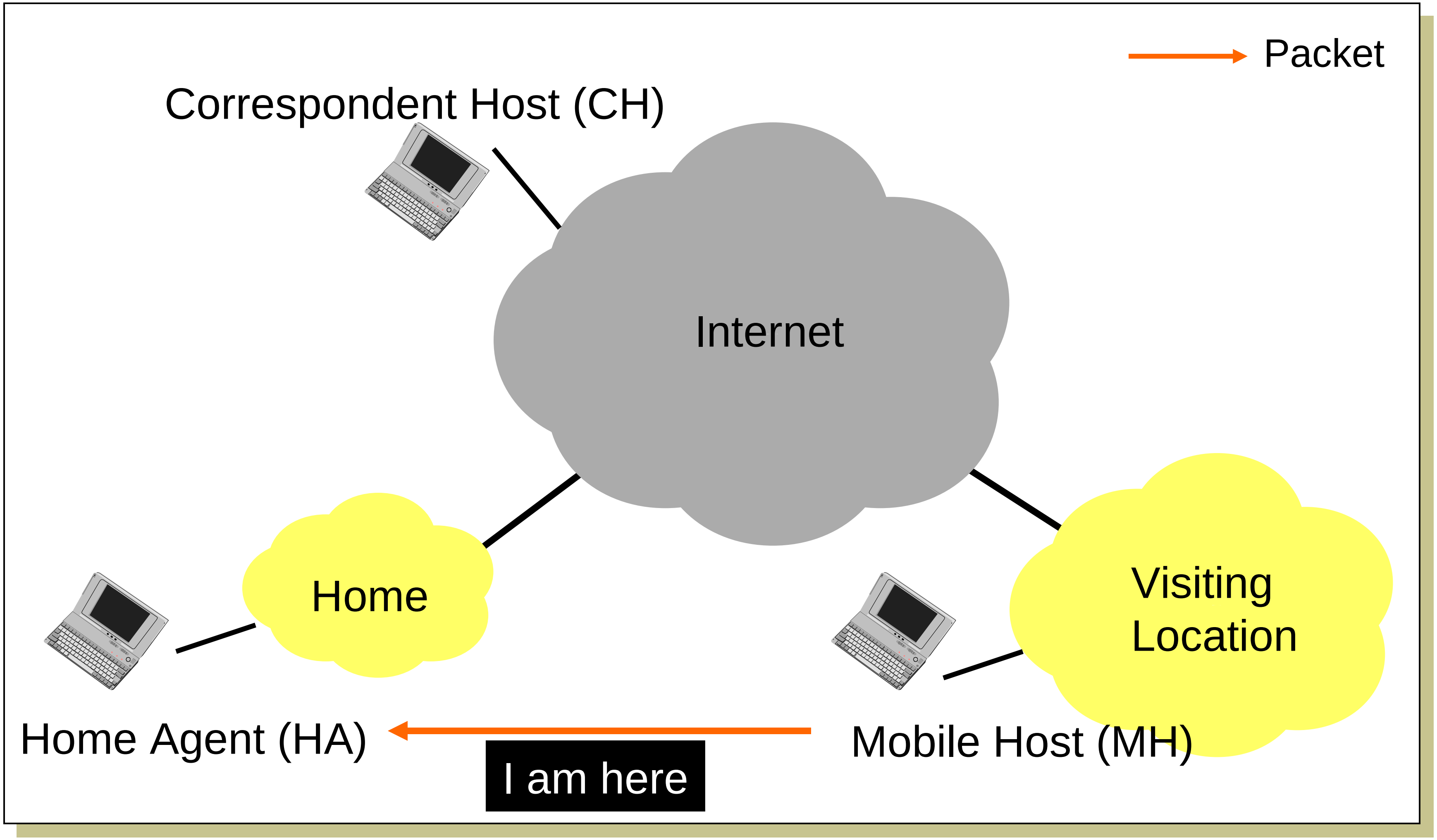
Mobile IP (RFC 2290)

- Interception
  - Typically home agent – a host on home network
- Delivery
  - Typically IP-in-IP tunneling
  - Endpoint – either temporary mobile address or foreign agent
- Terminology
  - Mobile host (MH), correspondent host (CH), home agent (HA), foreign agent (FA)
  - Care-of-address, home address

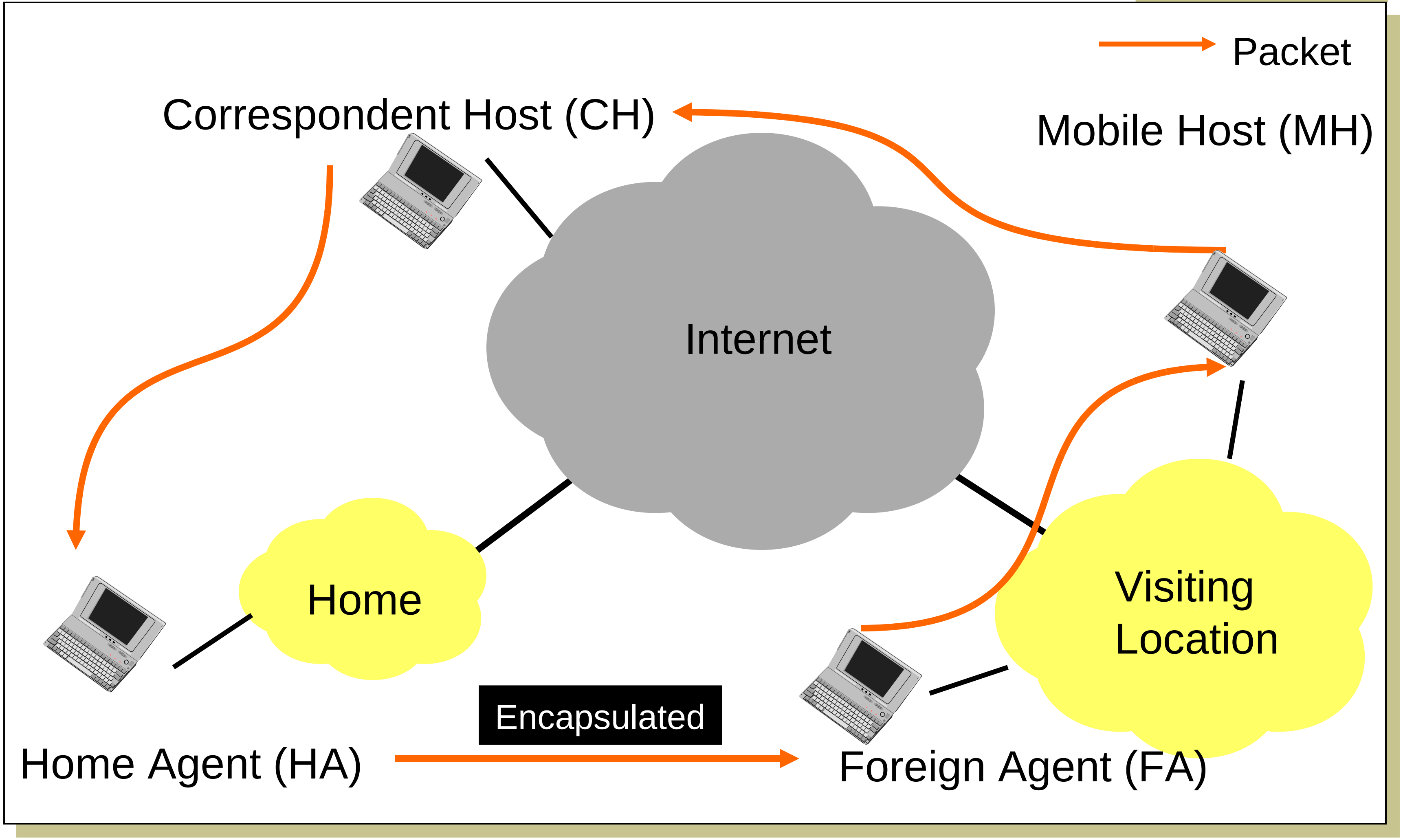
Mobile IP (MH at Home)



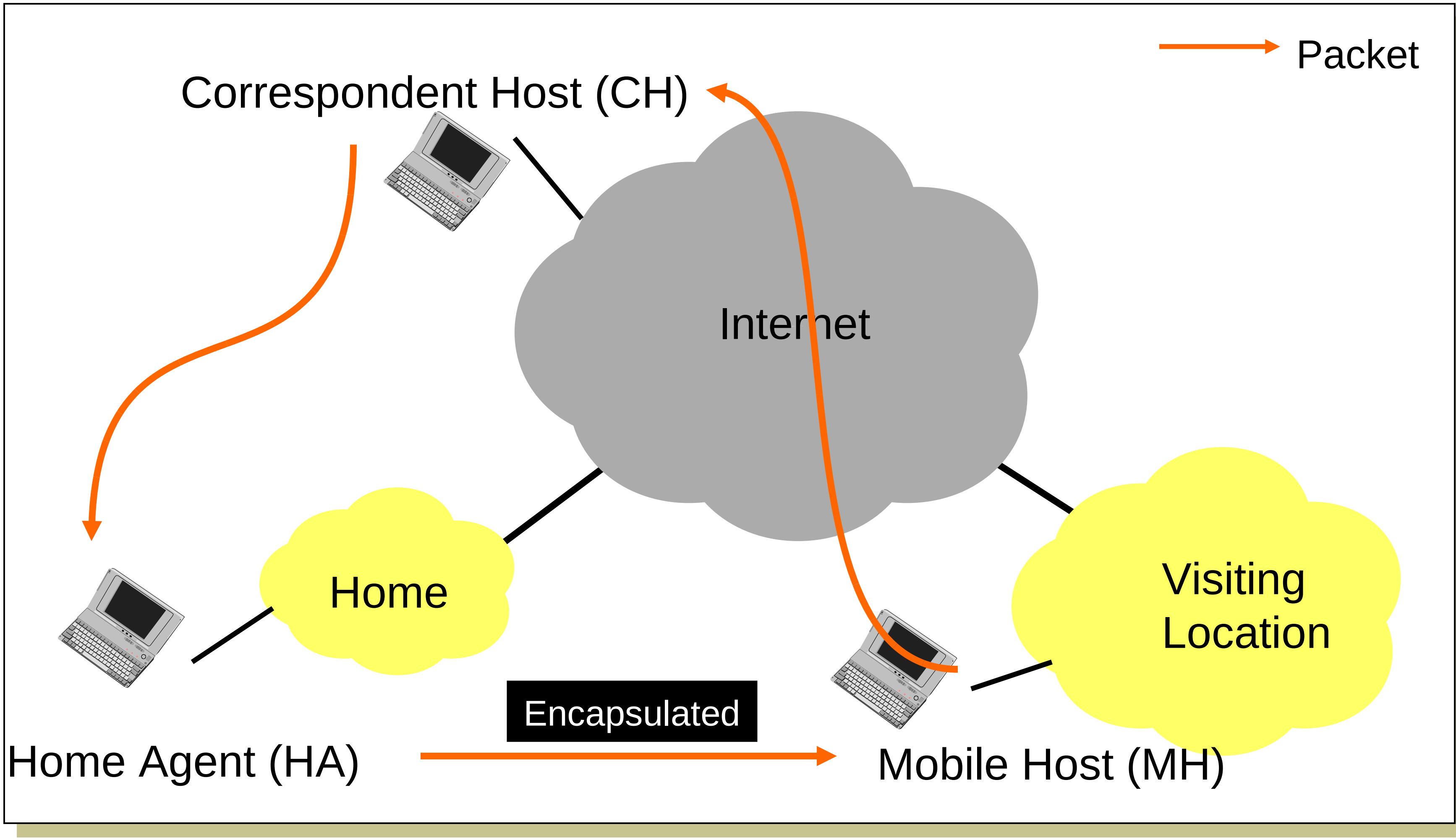
Mobile IP (MH Moving)



Mobile IP (MH Away – FA)



Mobile IP (MH Away - Collocated)



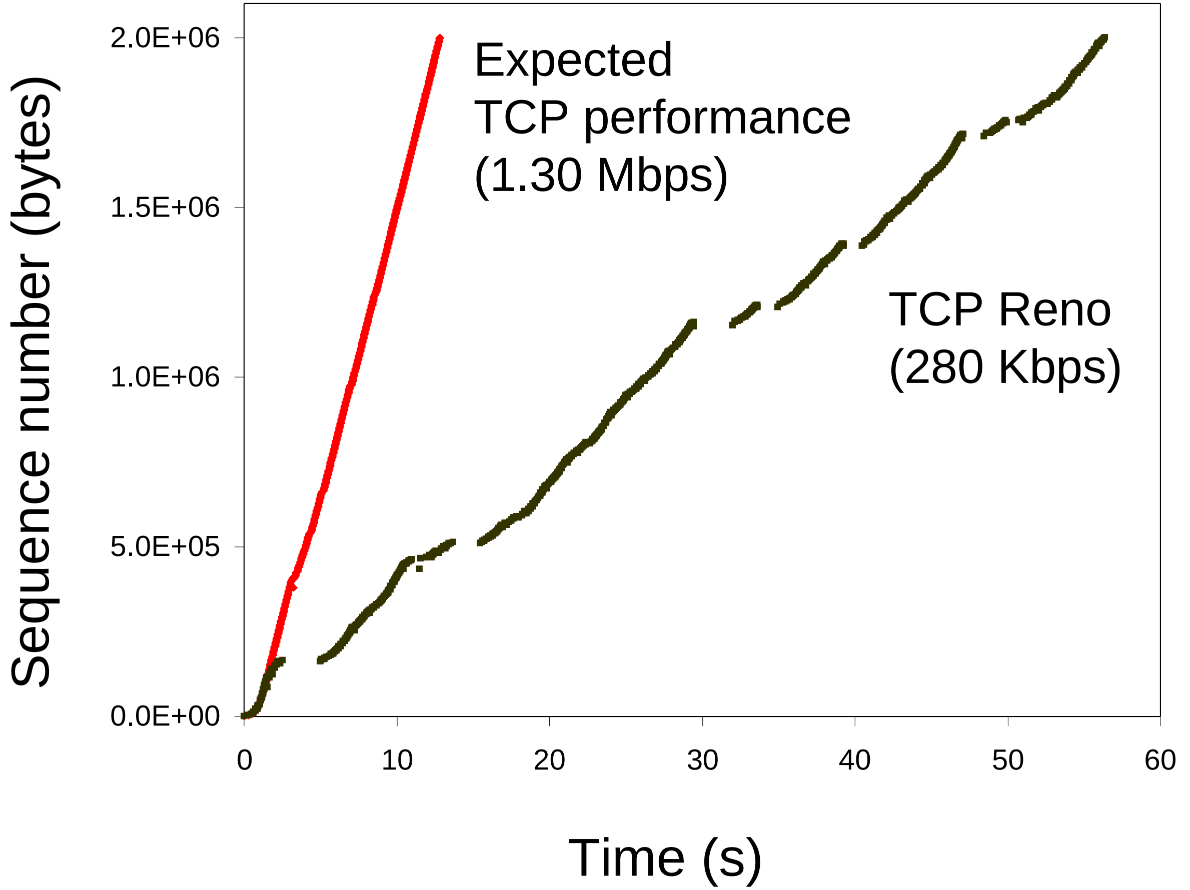
Other Mobile IP Issues

- Route optimality
  - Resulting paths can be sub-optimal
  - Can be improved with route optimization
    - Unsolicited binding cache update to sender
- Authentication
  - Registration messages
  - Binding cache updates
- Must send updates across network
  - Handoffs can be slow
- Problems with basic solution
  - Triangle routing
  - Reverse path check for security

Overview

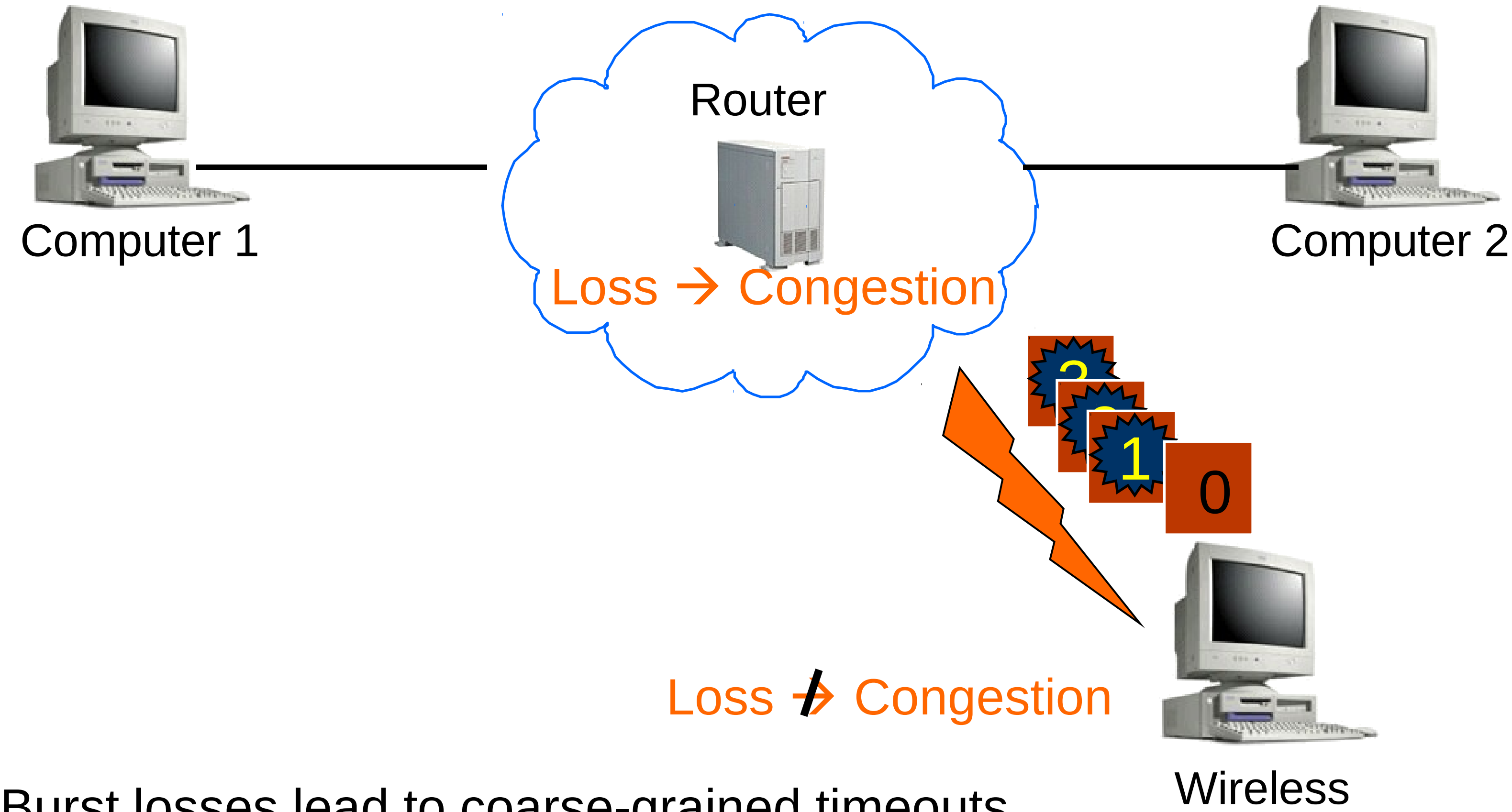
- Internet mobility
- TCP over noisy links
- Link layer challenges

Performance Degradation



2 MB wide-area TCP transfer over 2 Mbps Lucent WaveLAN

Wireless Bit-Errors



Burst losses lead to coarse-grained timeouts

Result: Low throughput

TCP Problems Over Noisy Links

- Wireless links are inherently error-prone
  - Fades, interference, attenuation
  - Errors often happen in bursts
- TCP cannot distinguish between corruption and congestion
  - TCP unnecessarily reduces window, resulting in low throughput and high latency
- Burst losses often result in timeouts
- Sender retransmission is the only option
  - Inefficient use of bandwidth

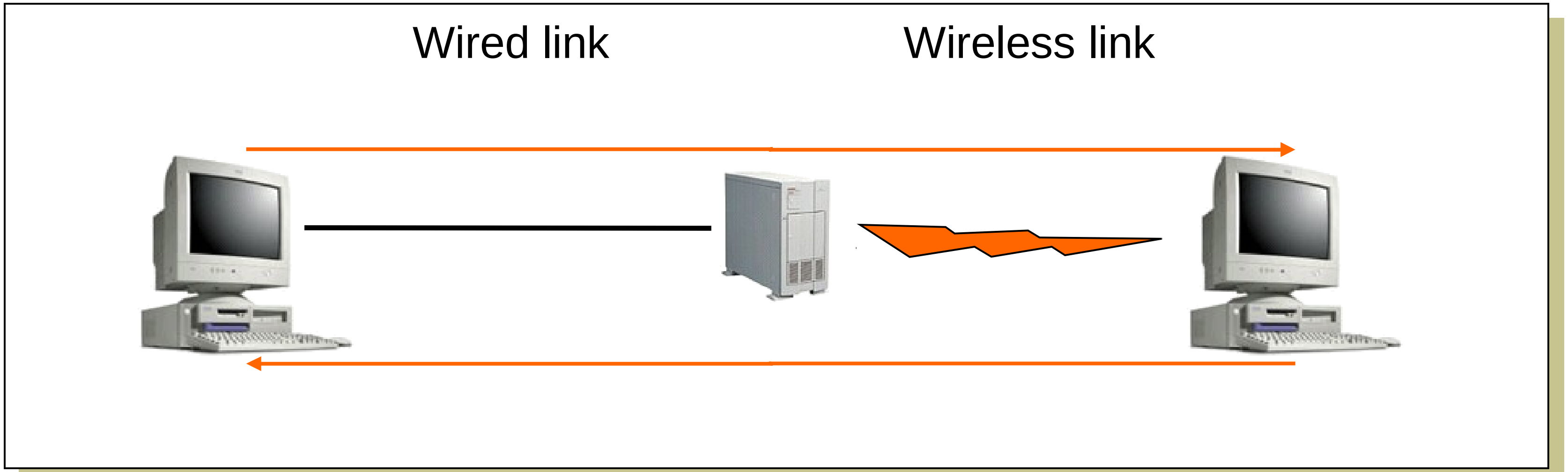
Proposed Solutions

- Incremental deployment
  - Solution should not require modifications to fixed hosts
  - If possible, avoid modifying mobile hosts

- End-to-end protocols
  - Selective ACKs, Explicit loss notification
- Split-connection protocols
  - Separate connections for wired path and wireless hop
- Reliable link-layer protocols
  - Error-correcting codes
  - Local retransmission

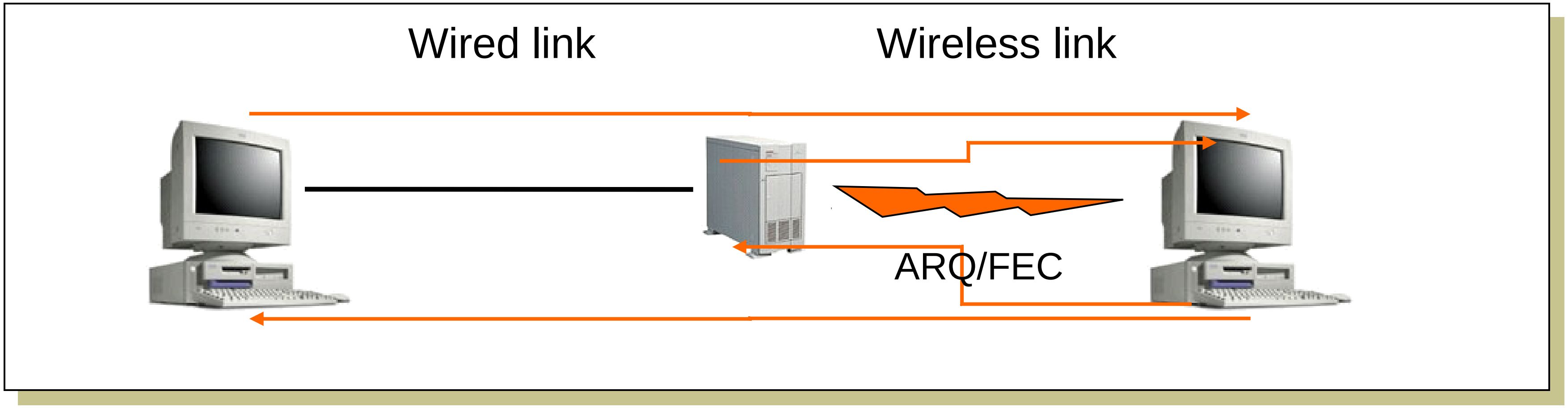
Approach Styles (End-to-End)

- Improve TCP implementations
  - Not incrementally deployable
  - Improve loss recovery (SACK, NewReno)
  - Help it identify congestion (ELN, ECN)
    - ACKs include flag indicating wireless loss
  - Trick TCP into doing right thing → E.g. send extra dupacks



Approach Styles (Link Layer)

- More aggressive local rexmit than TCP
  - Bandwidth not wasted on wired links
- Possible adverse interactions with transport layer
  - Interactions with TCP retransmission
  - Large end-to-end round-trip time variation
- FEC does not work well with burst losses

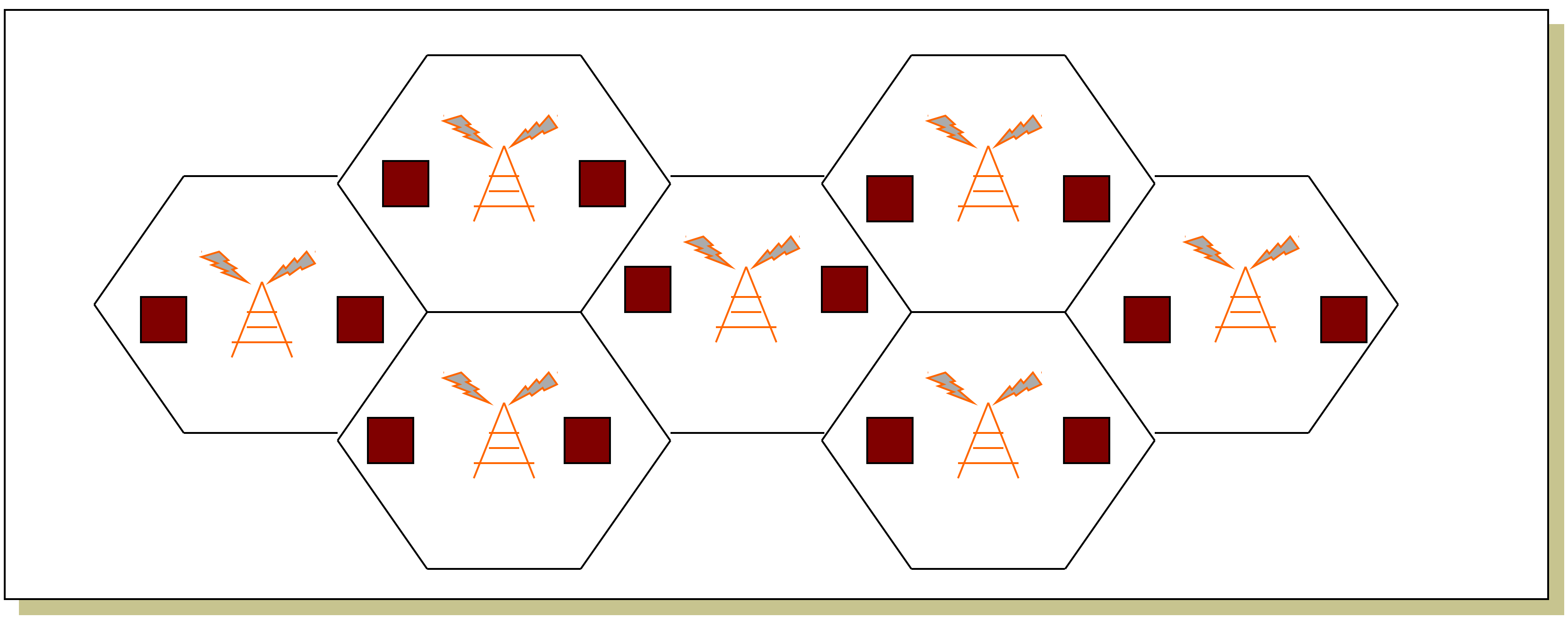


Overview

- Internet mobility
- TCP over noisy links
- Link layer challenges

Cellular Reuse

- Transmissions decay over distance
  - Spectrum can be reused in different areas
  - Different “LANs”
  - Decay is $1/R^2$ in free space, $1/R^4$ in some situations

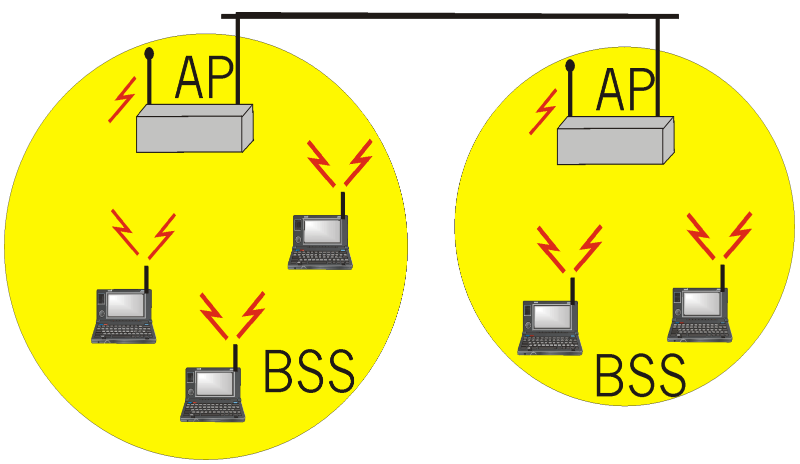


IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-2.5 GHz unlicensed radio spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code
  - widely deployed, using base stations
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-2.5 GHz range
  - up to 54 Mbps
- 802.11n
  - 2.4 or 5Ghz,
  - multiple antennas (MIMO), up to 450Mbps (for 3x3 antenna configuration)
- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions

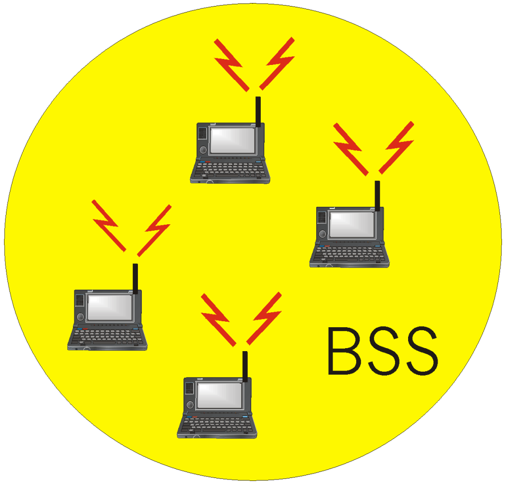
IEEE 802.11 Wireless LAN

- Wireless host communicates with a base station
  - Base station = access point (AP)
- **Basic Service Set (BSS) (a.k.a. "cell") contains:**
  - **Wireless hosts**
  - **Access point (AP): base station**
- **BSS's combined to form distribution system (DS)**



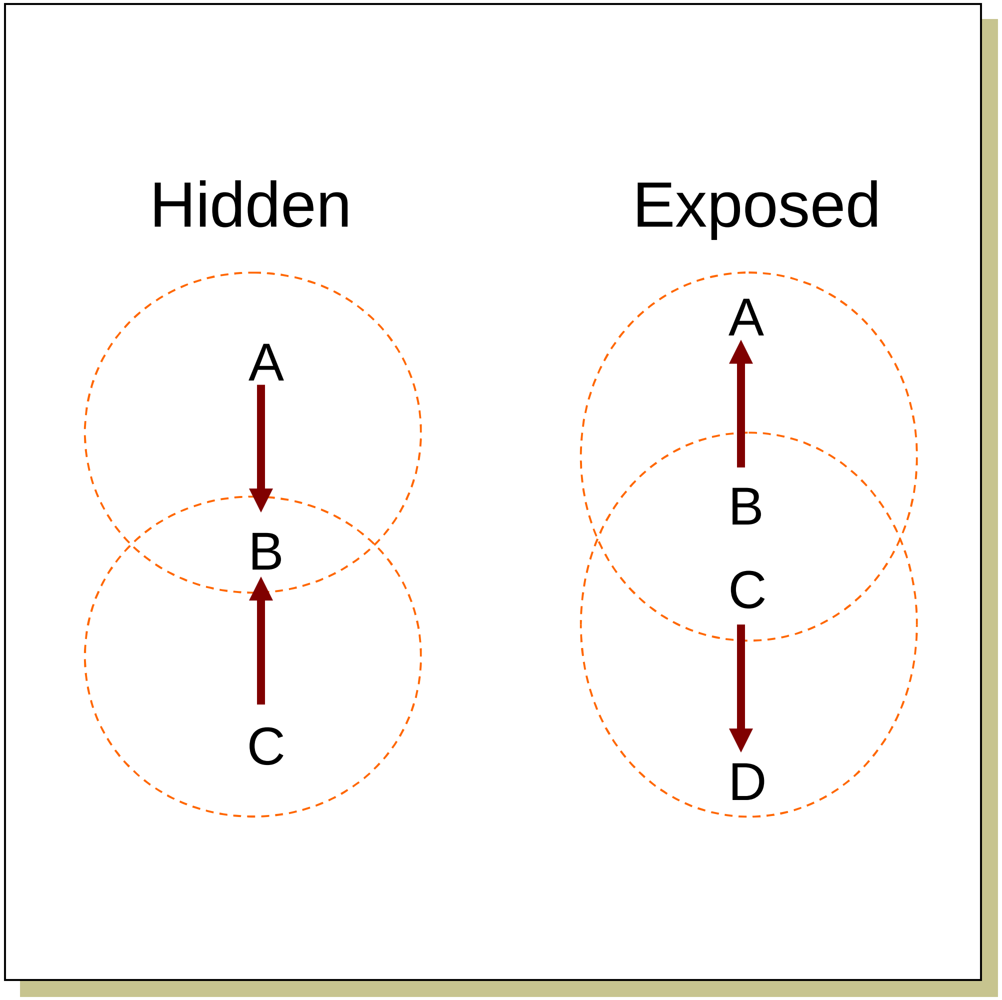
Ad Hoc Networks

- Ad hoc network: IEEE 802.11 stations can dynamically form network *without* AP
- Applications:
  - Laptops meeting in conference room, car
  - Interconnection of “personal” devices



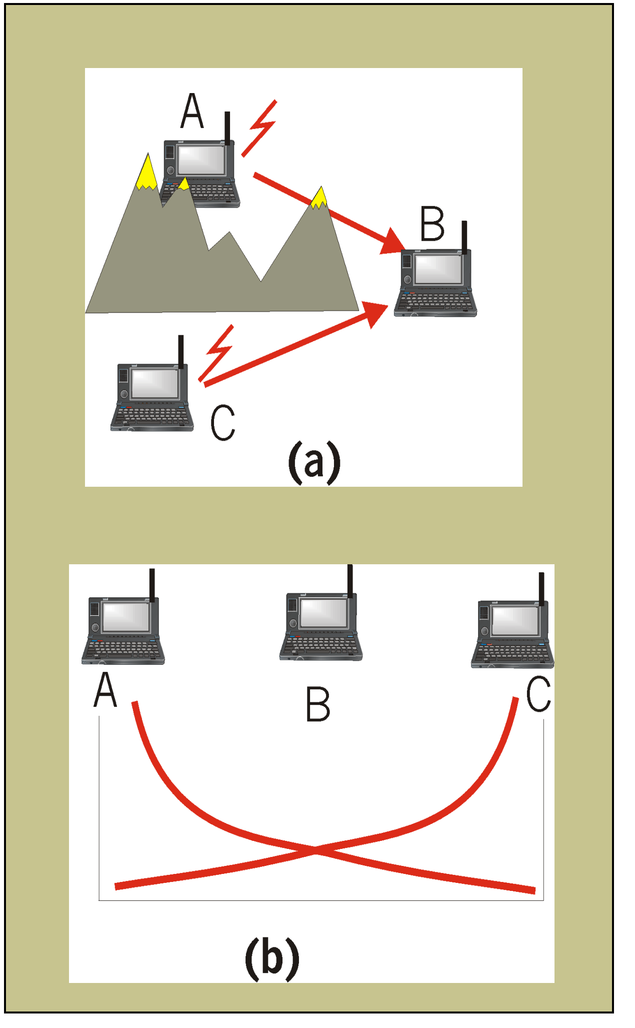
CSMA/CD Does Not Work

- Collision detection problems
  - Relevant contention at the receiver, not sender
    - Hidden terminal
    - Exposed terminal
  - Hard to build a radio that can transmit and receive at same time



Hidden Terminal Effect

- Hidden terminals: A, C cannot hear each other
  - Obstacles, signal attenuation
  - Collisions at B
  - Collision if 2 or more nodes transmit at same time
- CSMA makes sense:
  - Get all the bandwidth if you're the only one transmitting
  - Shouldn't cause a collision if you sense another transmission
- Collision detection doesn't work
- **CSMA/CA: CSMA with C**ollision **A**voidance



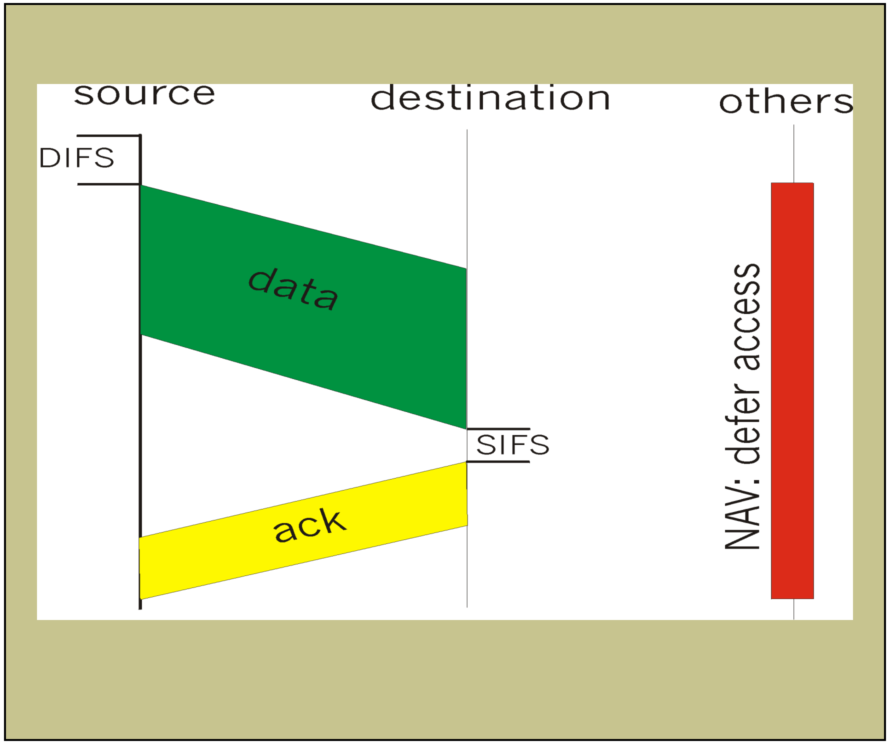
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 CSMA: sender

- If sense channel idle for **DISF (Distributed Inter Frame Space)**
  then transmit entire frame (no collision detection)
- If sense channel busy then binary backoff

802.11 CSMA receiver:

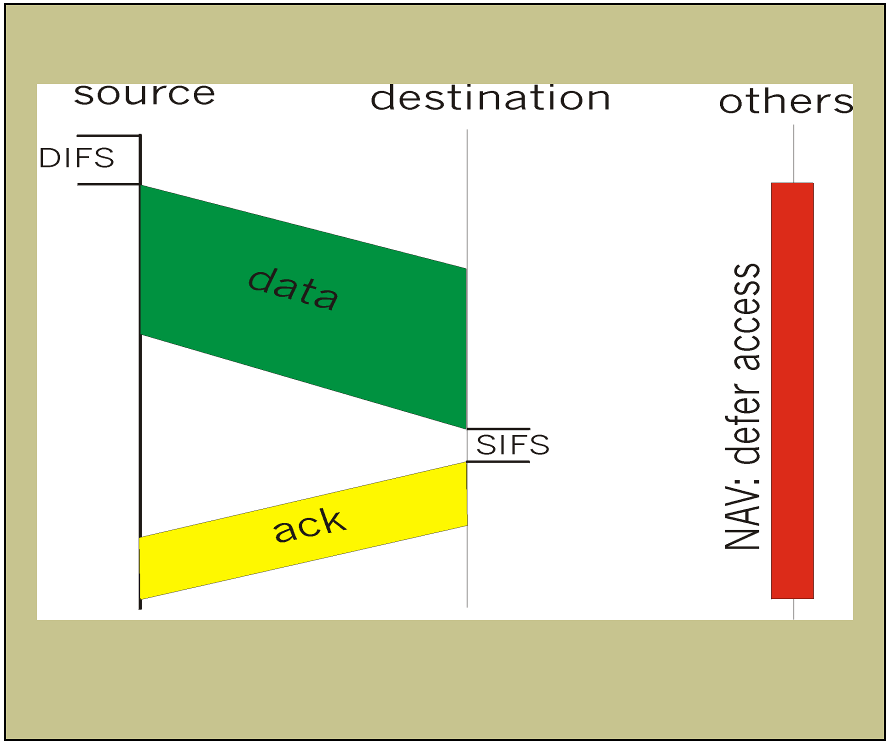
- If received OK
  return ACK after **SIFS (Short IFS)**
  (ACK is needed due to lack of collision detection)



IEEE 802.11 MAC Protocol

802.11 CSMA Protocol: others

- **NAV**: Network Allocation Vector
- 802.11 frame has transmission time field
- Others (hearing data) defer access for NAV time units

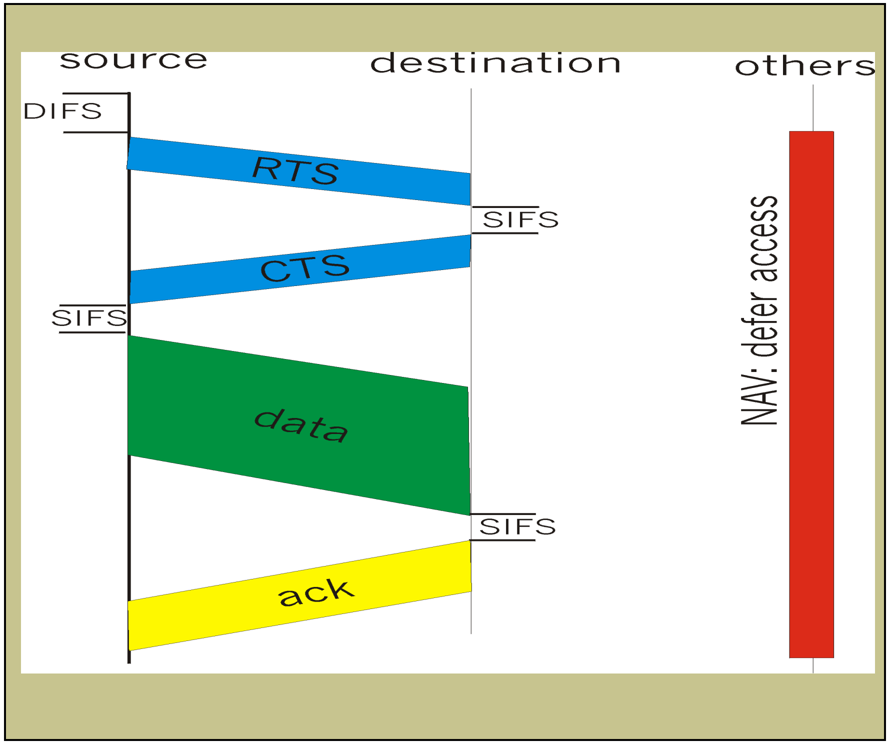


Collision Avoidance Mechanisms

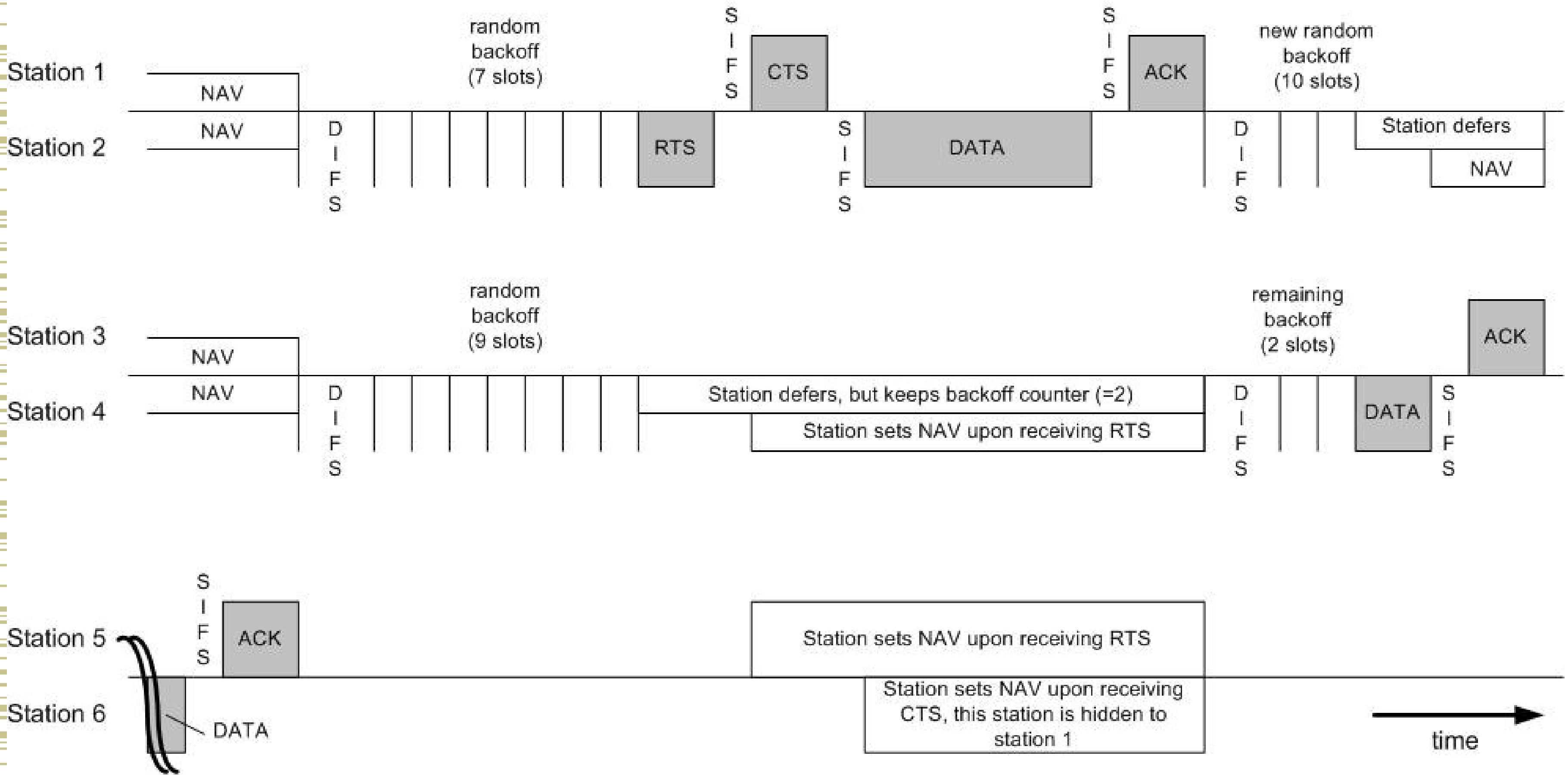
- Problem:
  - Two nodes, hidden from each other, transmit complete frames to base station
  - Wasted bandwidth for long duration !
- Solution:
  - Small reservation packets
  - Nodes track reservation interval with internal “network allocation vector” (NAV)

Collision Avoidance: RTS-CTS Exchange

- Explicit channel reservation
  - Sender: send short RTS: request to send
  - Receiver: reply with short CTS: clear to send
  - CTS reserves channel for sender, notifying (possibly hidden) stations
- RTS and CTS short:
  - collisions less likely, of shorter duration
  - end result similar to collision detection
- Avoid hidden station collisions
- Not widely used/implemented
  - Consider typical traffic patterns



802.11 DCF ([RTS/CTS/]Data/ACK)



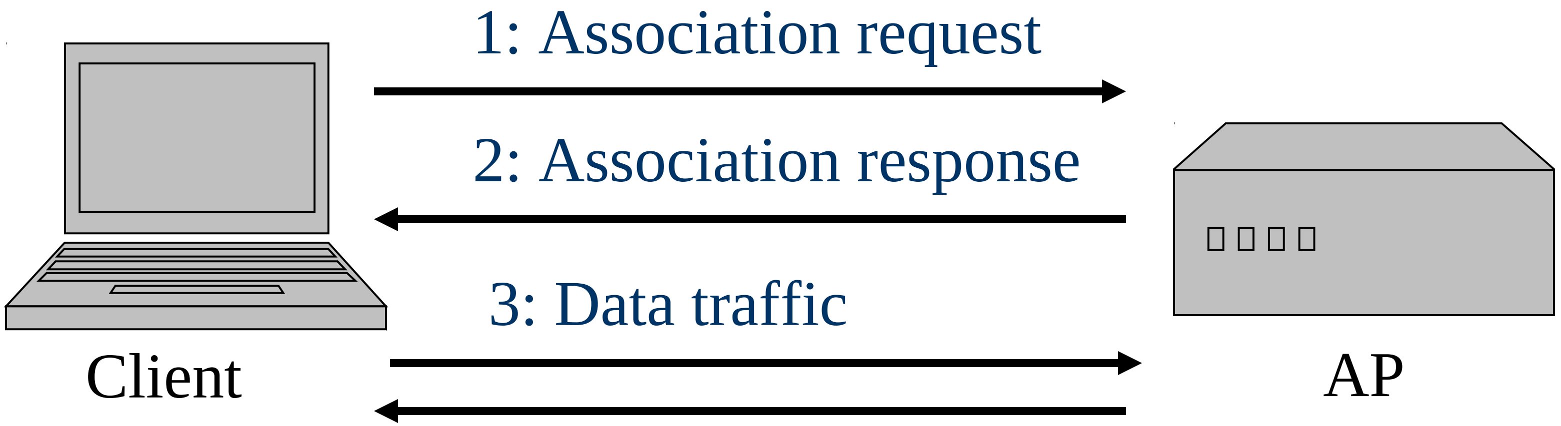
802.11 Management Operations

- Scanning
- Association/Reassociation
- Time synchronization
- Power management

Scanning & Joining

- Goal: find networks in the area
- Passive scanning
  - No require transmission → saves power
  - Move to each channel, and listen for Beacon frames
- Active scanning
  - Requires transmission → saves time
  - Move to each channel, and send Probe Request frames to solicit Probe Responses from a network

Association in 802.11



Time Synchronization in 802.11

- Timing synchronization function (TSF)
  - AP controls timing in infrastructure networks
  - All stations maintain a local timer
  - TSF keeps timer from all stations in sync
- Periodic Beacons convey timing
  - Beacons are sent at well known intervals
  - Timestamp from Beacons used to calibrate local clocks
  - Local TSF timer mitigates loss of Beacons

Power Management in 802.11

- A station is in one of the three states
  - Transmitter on
  - Receiver on
  - Both transmitter and receiver off (dozing)
- AP buffers packets for dozing stations
- AP announces which stations have frames buffered in its Beacon frames
- Dozing stations wake up to listen to the beacons
- If there is data buffered for it, it sends a poll frame to get the buffered data

Important Lessons

- Many assumptions built into Internet design
  - Wireless forces reconsideration of issues
- Link-layer
  - Spatial reuse (cellular) vs wires
  - Hidden/exposed terminal
  - CSMA/CA (why CA?) and RTS/CTS
- Network
  - Mobile endpoints – how to route with fixed identifier?
  - Link layer, naming, addressing and routing solutions
    - What are the +/- of each?
- Transport
  - Losses can occur due to corruption as well as congestion
    - Impact on TCP?
  - How to fix this → hide it from TCP or change TCP

EXTRA SLIDES

The rest of the slides are FYI

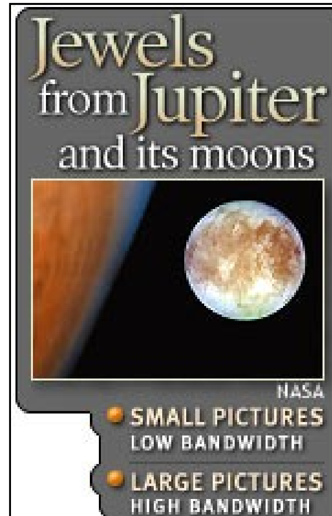
Overview

- Adapting Applications to Slow Links

Adapting Applications

- Applications make key assumptions
  - Hardware variation
    - E.g. how big is screen?
  - Software variation
    - E.g. is there a Flash video decoder?
  - Network variation
    - E.g. how fast is the network?
    - Reason why we are discussing in this class ☺
- Basic idea – adapt quality/format

Source Adaptation



- Can also just have source provide different versions
  - Common solution today
  - No waiting for transcoding
  - Full version not sent across network
  - Can't handle fine grain adaptation

Transcoding Example

- Generate reduced quality variant of Web page at proxy
  - Must predict how much size reduction will result from transcoding
  - How long to transcode?
- Send appropriate reduced-size variant
  - Target response time?

802.11 modes

- Infrastructure mode
  - All packets go through a base station
  - Cards associate with a BSS (basic service set)
  - Multiple BSSs can be linked into an Extended Service Set (ESS)
    - Handoff to new BSS in ESS is pretty quick
      - Wandering around CMU
    - Moving to new ESS is slower, may require re-addressing
      - Wandering from CMU to Pitt
- Ad Hoc mode
  - Cards communicate directly.
  - Perform some, but not all, of the AP functions

Discussion

- RTS/CTS/Data/ACK vs. Data/ACK
  - Why/when is it useful?
  - What is the right choice
  - Why is RTS/CTS not used?

802.11 Rate Adaptation

- 802.11 spec specifies rates not algorithm for choices
  - 802.11b 4 rates, 802.11a 8 rates, 802.11g 12 rates
  - Each rate has different modulation and coding

Transmission Rate ↑ then Loss Ratio ↑

Transmission Rate ↓ then Capacity Utilization ↓

throughput decreases either way – need to get it just right