# Internet Technology

## 12. Wireless Networking

Paul Krzyzanowski

Rutgers University

Spring 2016

## Some Terms

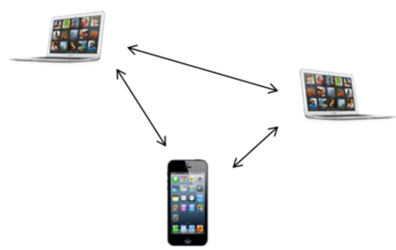
- Base Station
  - Sends & receives data to/from wireless hosts
  - Coordinates transmission among hosts
  - Connects to other, usually wired, networks
  - Examples: cell tower or wireless access point

# Some Terms

- Infrastructure Mode
  - Traditional network services are provided by the network to which the hosts are connected via the base station
  - E.g., DHCP, DNS, routing

# Some Terms

- *Ad hoc* mode (peer-to-peer mode)
  - No back-end infrastructure is present
  - Hosts have to figure out address assignment, name resolution, and routing among themselves
  - Often no base stations: connectivity directly to hosts and routing via forwarding through hosts



# 802.11 LANs

- 802.11 = Wi-Fi
  - Set of standards for wireless local area networking

| Standard | Frequency (GHz) | Data rate (max) |
|---|---|---|
| 802.11 | 2.4 | 1-2 Mbps (obsolete) |
| 802.11b | 2.4 | 11 Mbps |
| 802.11a | 5 | 54 Mbps |
| 802.11g | 2.4 | 54 Mbps |
| 802.11n | 2.4, 5 | 72.2 Mbps |
| 802.11ac | 5 | 1.3 Gbps |
| 802.11ad | 60 | 6.9 Gbps (in-room) |

5 GHz = 5.1-5.8 GHz
2.4 GHz = 2.5-2.485 GHz

*And more…*
*802.11af, 802.11ah, 802.11aj, 802.11ay*

## 802.11 LANs

- Base station = access point (AP)
- Basic Service Set (BSS)
  - One or more wireless stations (devices)
  - and one central access point (AP)
- BSSID = MAC address of the AP

- Devices using an AP operate in infrastructure mode
  - AP interconnects with the wired Ethernet infrastructure
- 802.11 devices can also operate in ad hoc mode
  - Communicate with each other directly

## Access Point Identification

- An access point is assigned
  - A Service Set Identifier (SSID) = textual name for the BSSID
  - A channel number
    - Frequency band is divided into multiple overlapping channels
      - 802.11g/n has 3 non-overlapping channels in the U.S. (1, 6, 11)

## Access Point Discovery & Association

- A wireless host (station) needs to associate with one AP
- **Passive Scanning**
  - AP periodically sends beacon frames, each containing the AP's SSID & MAC address
  - Wireless station scans all channels, searching for beacon frames from any APs
- **Active Scanning**
  - Wireless station may also broadcast a *probe frame* to all APs – iterating through the channels
- **Selection**
  - Wireless station selects one access point (often chosen by the user)
  - Sends association request frame; receives an association response from AP
  - Then send a DHCP discovery message …

## 802.11 MAC Protocol

- Key differences between Ethernet and 802.11
  - Higher bit-error rates in wireless
  - Ethernet can listen while transmitting; 802.11 cannot
    - Received signal is weaker than transmitted signal
    - Receiving station may be receiving signals that the transmitter cannot detect
  - Because Ethernet could listen, it could stop transmission if collision

- What does 802.11 do?
  - Uses Link-layer acknowledgements (ARQ; ack & retransmission)
  - Use CSMA/CA
    - CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance
    - Random access protocol
    - Avoid collisions when possible
      - If two stations sense a busy channel, they both enter random backoff

## 802.11 MAC Protocol: CSMA/CA

### Key idea

- Prevent collisions when they are most likely to occur: when when nodes sense that the channel is clear
- Force nodes to wait a random time, sense, and transmit
- If the channel is busy, the node freezes its timer until it is free
- This reduces the chance that two clients will transmit simultaneously

# 802.11 MAC Protocol: CSMA/CA

1. If the channel is idle
   - Wait a short time (Distributed Inter-frame Space, DIFS)
   - Transmit complete frame
2. Else pick a random backoff value using binary exponential backoff
   - Count down this amount when the channel is sensed idle
   - If the channel is busy, the counter does not change
3. When the counter reaches zero (channel must be idle)
   - Transmit the complete frame
4. Wait for an acknowledgement
   - If a receiver receives the frame & CRC is OK,
     - Waits briefly (Short Inter-frame Spacing, SIFS)
     - Sends back an acknowledgement frame
   - If the transmitter has another frame to send, go to step 2 with new frame
   - If the ACK was not received, *increase the backoff value*; go to step 2

# Hidden Node Problem

A receiver may be receiving signals from another transmitter that cannot be detected by the sender

Hidden node = hidden terminal

# 802.11 MAC: RTS/CTS

- Carrier sensing suffers from the hidden node problem
- RTS/CTS: Additional mechanism for sensing in 802.11 (optional)
  - Before sending a frame, send a Request to Send (RTS) frame to AP
    - Reserves access to the channel
    - RTS indicates the size of the data frame that will be sent
  - AP responds with a broadcast Clear to Send (CTS) frame
    - Gives permission to send the frame
    - Informs other stations not to send anything during that time
  - RTS & CTS frames age generally much shorter than data frames
    - Minimizes collision
  - RTS/CTS has an overhead
    - Used only for large frames > *threshold*

# 802.11 Frame

- Similarities to Ethernet frame
  - Same 6-byte MAC addresses
  - Payload
    2312 bytes vs. Ethernet's 1500 bytes, but normally kept ≤ 1500 bytes
  - 32-bit CRC checksum

- Key difference
  - Ethernet has two address fields: source address & destination address
  - 802.11 has four address fields!
    - Three addresses are always used
    - Four are only used for Ad hoc mode

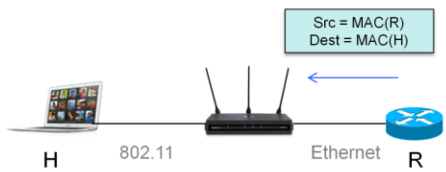
- Also: 802.11n and 802.11ac support optional use of ECC
  (Low-Density Parity Check codes, LDPC)

## 802.11 MAC Addresses

- An AP needs to interconnect between the BSS and a wired LAN
- **Address 1: (wireless destination)**
  - MAC address of the wireless station that will receive the frame
  - If a wireless station transmits, this is the address of the AP
  - If an AP is sending to a wireless station, this is the address of the station
- **Address 2: (wireless source)**
  - MAC address of the wireless station that transmits the frame
  - If a wireless station transmits, this is the address of the station
  - If the AP is sending, this is the MAC address of the AP
- **Address 3 (wired destination/source)**
  - MAC address of the device on the wired network

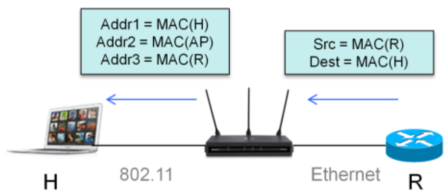
# 802.11 MAC Addresses Example

- Router knows about hosts on a subnet, not APs
- Router R knows address of host H
  To send a datagram to H:
  – Use ARP to find the MAC address of H
  – R creates an Ethernet frame
    - Destination = H's MAC address
    - Source = R's MAC address



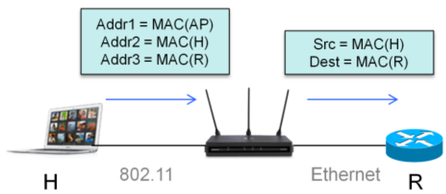
# 802.11 MAC Addresses Example

- AP converts the 802.3 Ethernet frame to an 802.11 frame
  - Address 1 = destination = H's MAC address
  - Address 2 = wireless source = AP's MAC address
  - Address 3 = LAN source = R's MAC address
- H1 can identify the MAC address of the router interface



# 802.11 MAC Addresses Example

- Return datagram from H to R
- H creates an 802.11 frame
  - Address1 = wireless destination = AP's MAC address
  - Address 2 = source = H's MAC address
  - Address 3 = ultimate LAN destination = R's MAC address
- The AP then creates an Ethernet MAC frame for
  - Source address = H's MAC address
  - Destination address = R's MAC address



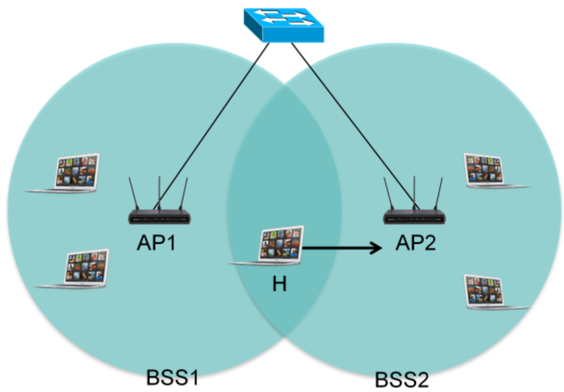
## ARQ Protocol & Retransmissions

ARQ = Automatic Repeat Request

- Unlike Ethernet, 802.11 uses an ARQ protocol
  - We saw that ACKs can get lost, resulting in retransmissions
  - Retransmissions → duplicate packets
- 802.11 has a sequence number in its MAC header
  - Allows a receiver to distinguish duplicate packets from new packets

## Increasing range: multiple APs in a subnet

- Employ multiple BSSs within the same IP subnet
  - But how do you handle mobility of devices?
- A device can keep its IP address & TCP session
  - It's on the same LAN



## Increasing range: multiple APs in a subnet

- Host migration
  - A host detects a weakening signal from its associated AP (AP1)
  - Scans for an AP with a stronger signal
  - Detects an AP with the same SSID but a stronger signal (AP2)
  - Dissociates with AP1 and associates with AP2

# Increasing range: multiple APs in a subnet

- What about the switch?
  - Switches are self-learning
  - Switch has an entry in its forwarding table
    - Associates H'a MAC address with the switch interface to AP1
  - When H associates with BSS2:
    - AP2 will send a broadcast Ethernet frame with H's source address to the switch
    - The switch will update its forwarding table

| MAC | Interface |
|---|---|
| H | AP1 port |

initial forwarding table

→

| MAC | Interface |
|---|---|
| H | AP2 port |

after forged broadcast from AP2

## 802.11 Power Management

- A transceiver on a node can switch between sleep and wake modes
- A node tells its AP that it will go to sleep
  - Sets a power management bit in the 802.11 MAC header
  - Timer in the transceiver is set to wake before the AP is scheduled to send its beacon frame (typically every 100 ms)
- Frame buffering
  - AP knows that a node went to sleep
    - Any frames for the node are stored at the AP
    - Beacon frame contains a list of nodes with buffered frames
  - If no frames to receive, the node goes back to sleep
    - Otherwise, it requests the buffered frames by sending a polling message
- This can achieve 99%+ sleep times

# Bluetooth

- Bluetooth = IEEE 8002.15.1 → designed as cable replacement
- Short-range, low-power, relatively low-speed (up to 4 Mbps), cheap
- Media
  - 2.4 GHz band – 625 μs time slots – TDM network access
  - Sender transmits on one of 79 channels
    - Frequency Hopping Spread Spectrum (FHSS)
- Ad hoc network
  - No access point
  - Up to 8 active devices (255 ”parked” devices)
  - One designated as a master – others are slaves
    - Master can transmit in each odd-numbered slot
    - Slaves transmit only after master granter permission and only to the master

## Wide Area Mobility: Cellular Networking

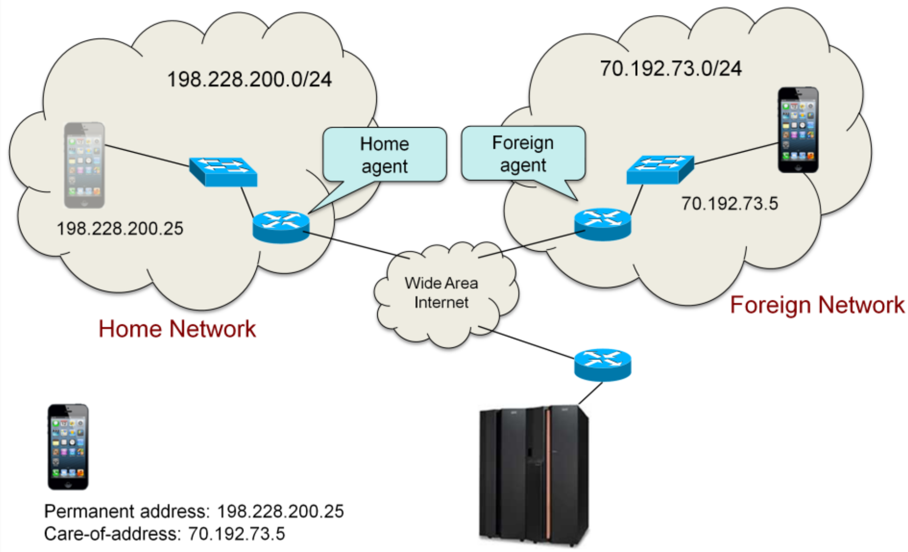
- Home Network
  - Permanent device address
- Foreign Network
  - **Foreign agent** responsible for
    - **Care-of-Address** (**COA**) = foreign address
    - Can be obtained via DHCP on the foreign network
    - Informing Home Agent of the node's current foreign address

## Mobile Routing: Indirect Routing

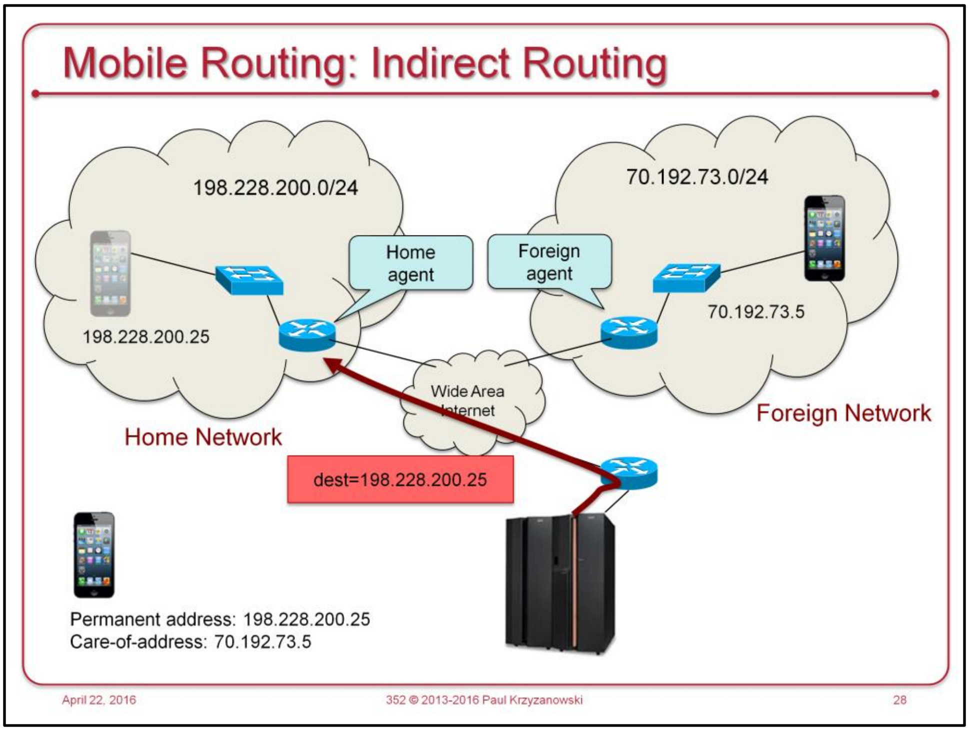
- To the mobile node
  - Address datagrams to mobile node's permanent address
  - Datagrams get routed to the home network
  - **Home agent**
    - Tracks COAs
    - Intercepts datagrams for nodes residing on foreign networks
    - **Encapsulates** datagrams & forwards them to the foreign agent
      - Outer datagram is addressed to the foreign agent
      - Inside datagram is the original datagram
    - **Foreign agent** extracts the encapsulated datagram & forwards to node
- From the mobile node
  - Mobile node can send datagrams directly from its permanent address

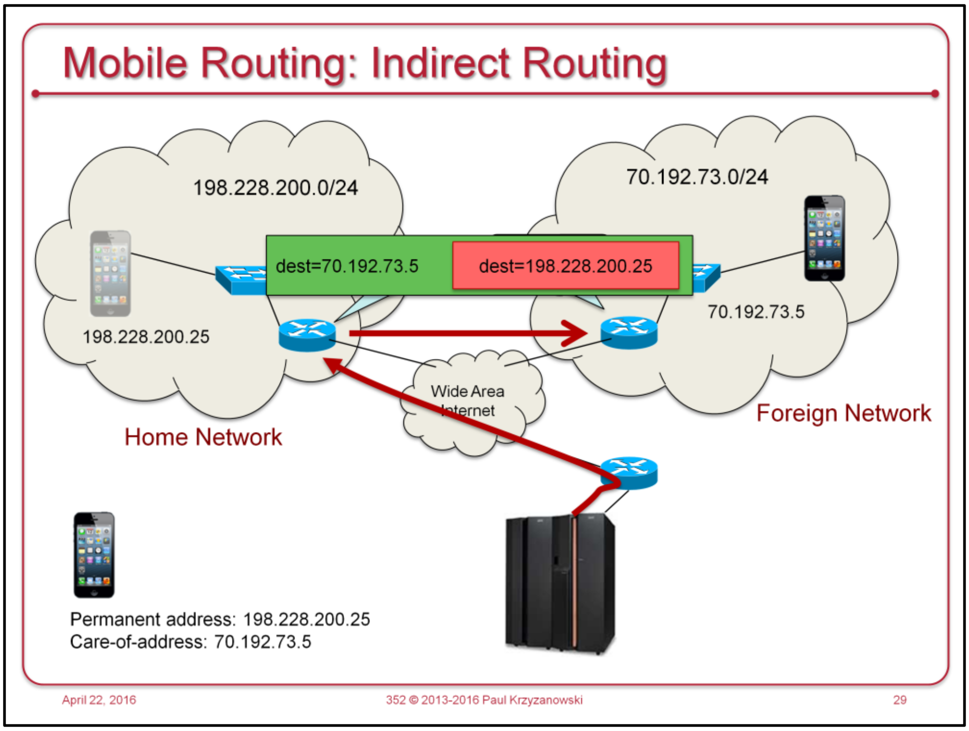
Mobile IP: RFC 5944

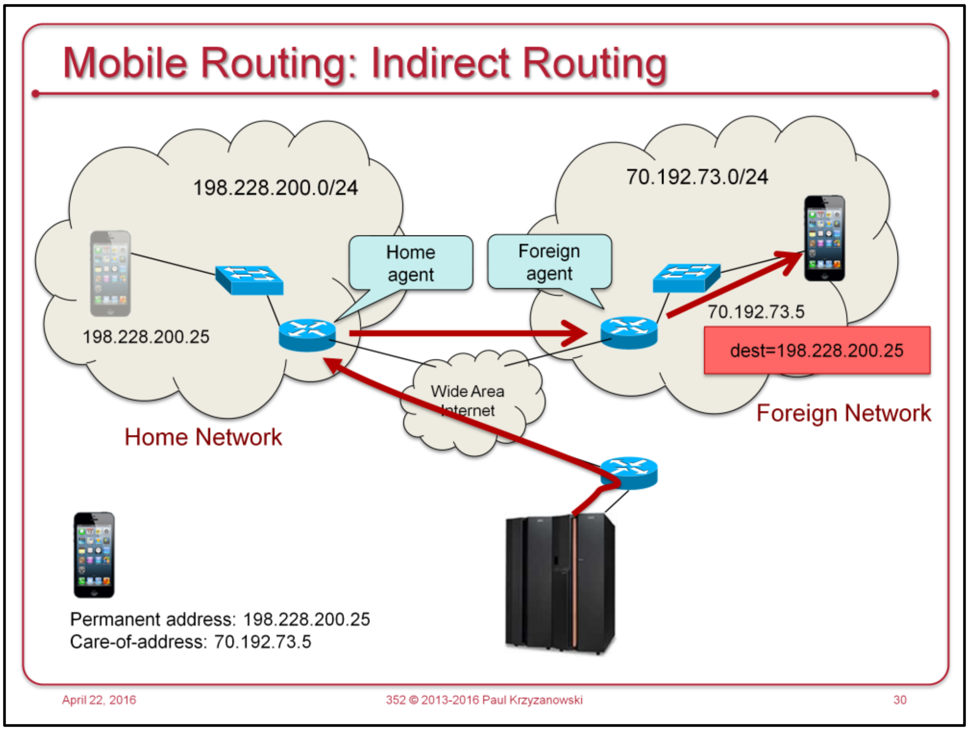
# Mobile Routing: Indirect Routing

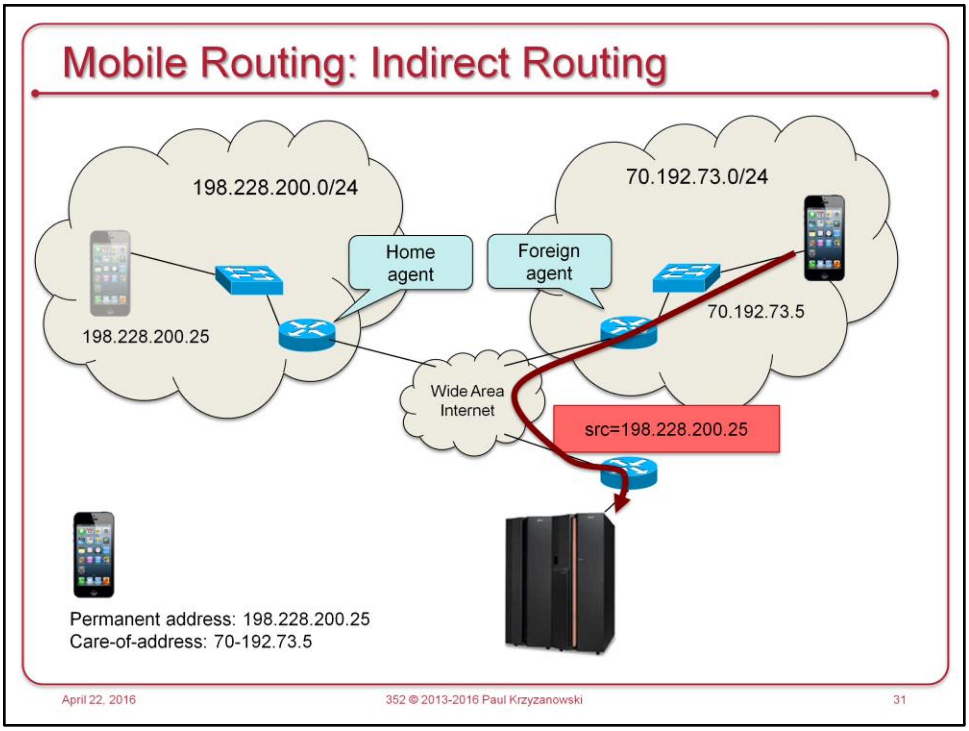



April 22, 2016 352 © 2013-2016 Paul Krzyzanowski 27


Mobile Routing: Indirect Routing
198.228.200.0/24
70.192.73.0/24
Home agent
Foreign agent
198.228.200.25
70.192.73.5
Wide Area Internet
Home Network
Foreign Network
dest=198.228.200.25
Permanent address: 198.228.200.25
Care-of-address: 70.192.73.5
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
28

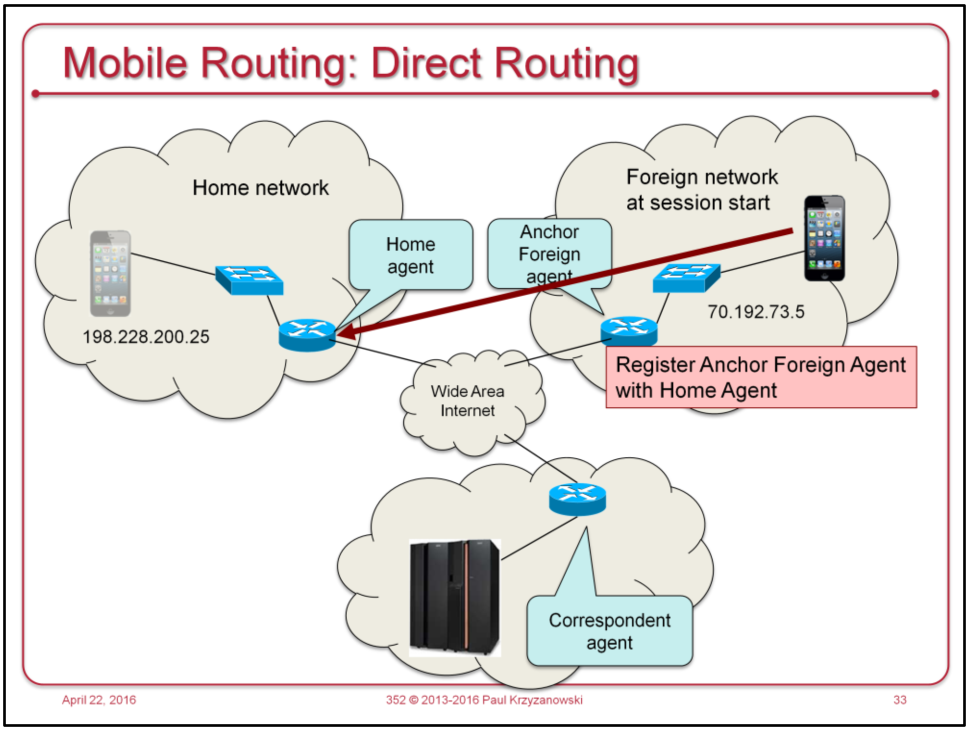

Mobile Routing: Indirect Routing
198.228.200.0/24
70.192.73.0/24
dest=70.192.73.5
dest=198.228.200.25
198.228.200.25
70.192.73.5
Wide Area Internet
Home Network
Foreign Network
Permanent address: 198.228.200.25
Care-of-address: 70.192.73.5
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
29

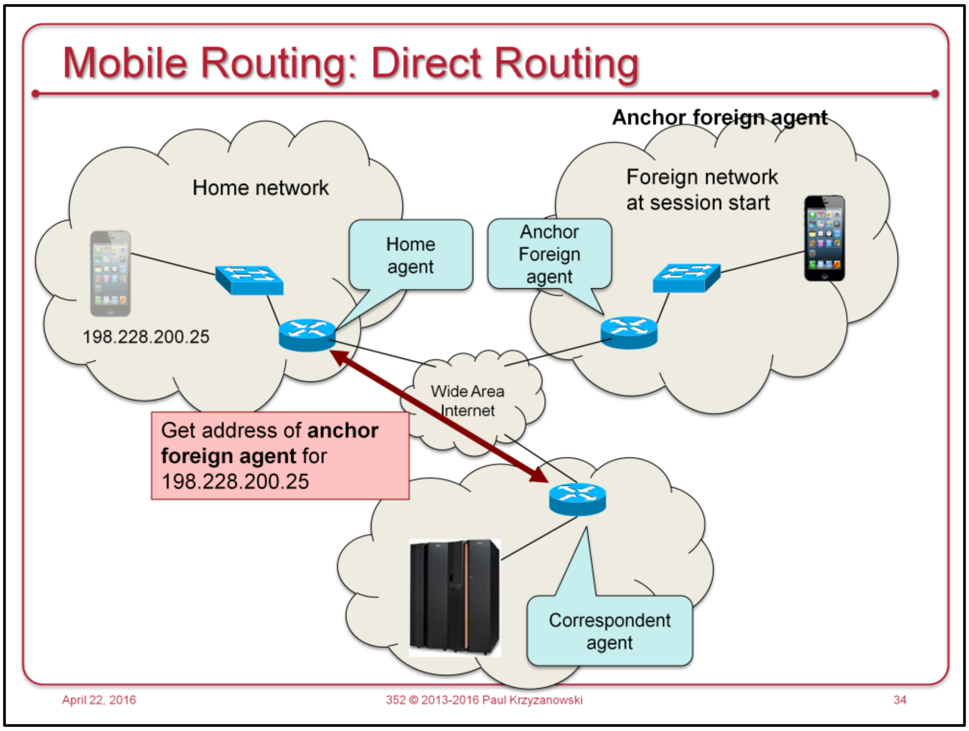

Mobile Routing: Indirect Routing
198.228.200.0/24
70.192.73.0/24
Home agent
Foreign agent
198.228.200.25
70.192.73.5
dest=198.228.200.25
Wide Area Internet
Home Network
Foreign Network
Permanent address: 198.228.200.25
Care-of-address: 70.192.73.5
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
30


Mobile Routing: Indirect Routing
198.228.200.0/24
70.192.73.0/24
Home agent
Foreign agent
198.228.200.25
70.192.73.5
Wide Area Internet
src=198.228.200.25
Permanent address: 198.228.200.25
Care-of-address: 70-192.73.5
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
31

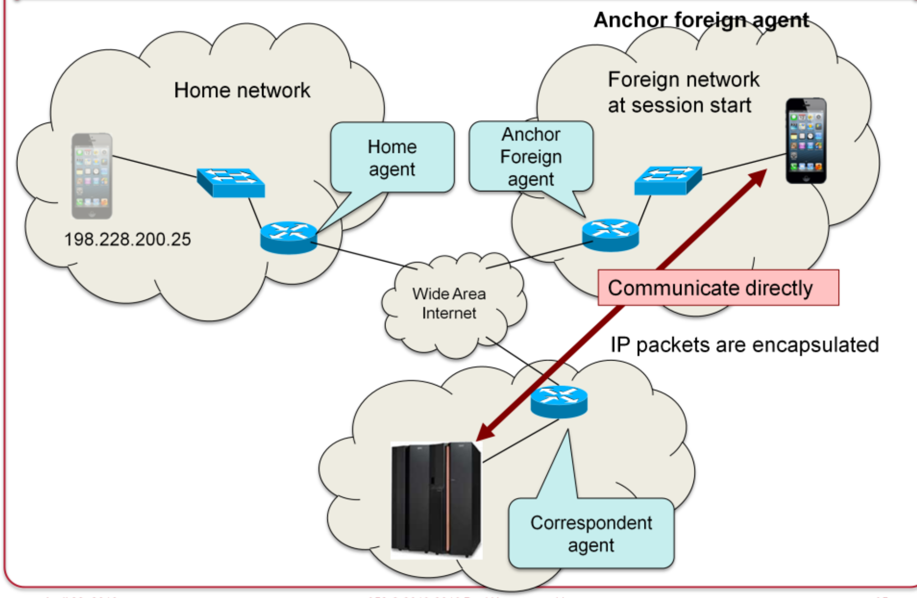
## Mobile Routing: Direct Routing

- Indirect routing suffers from the **triangle routing problem**
  - Datagrams to the mobile node must be routed through the home node
- **Direct Routing**
  - Add a **Corresponding Agent** to the sender's network
  - Learns the care-of-address (COA) of the mobile node
    - Query home agent to find the COA & foreign agent
  - Original foreign agent = **anchor foreign agent**
  - If the mobile node moves to another foreign network
    - Mobile node registers with the new foreign agent
    - New foreign agent tells the anchor foreign agent the new COA
    - Anchor foreign agent encapsulates incoming datagrams and routes them to the new foreign agent (**indirect routing**)

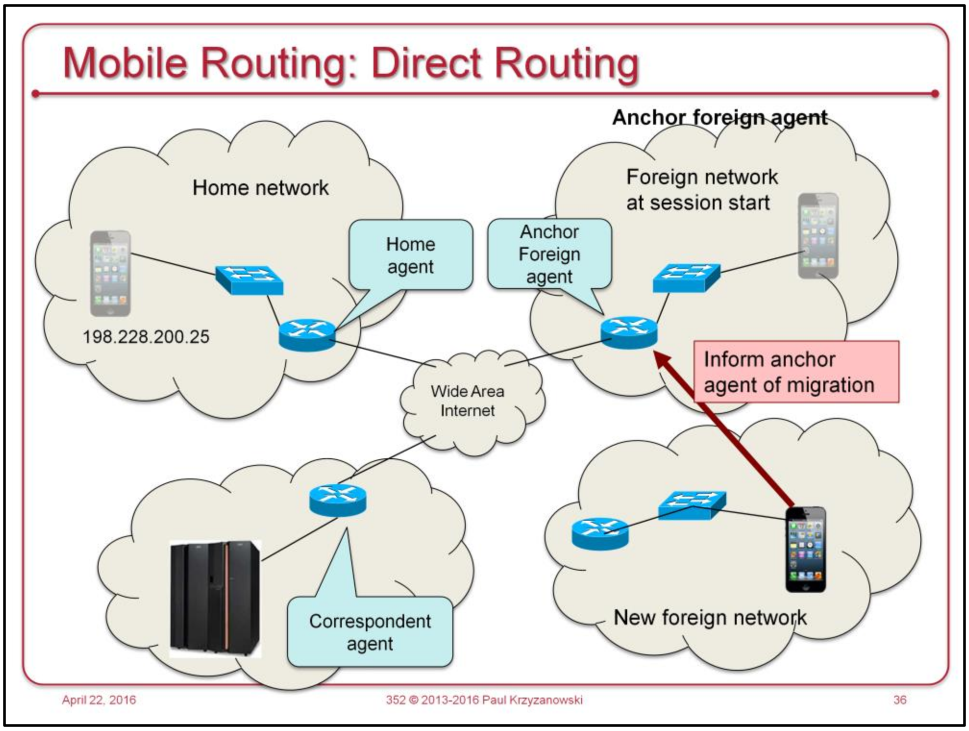

Mobile Routing: Direct Routing
Home network
198.228.200.25
Home agent
Anchor Foreign agent
Foreign network at session start
70.192.73.5
Register Anchor Foreign Agent with Home Agent
Wide Area Internet
Correspondent agent
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
33

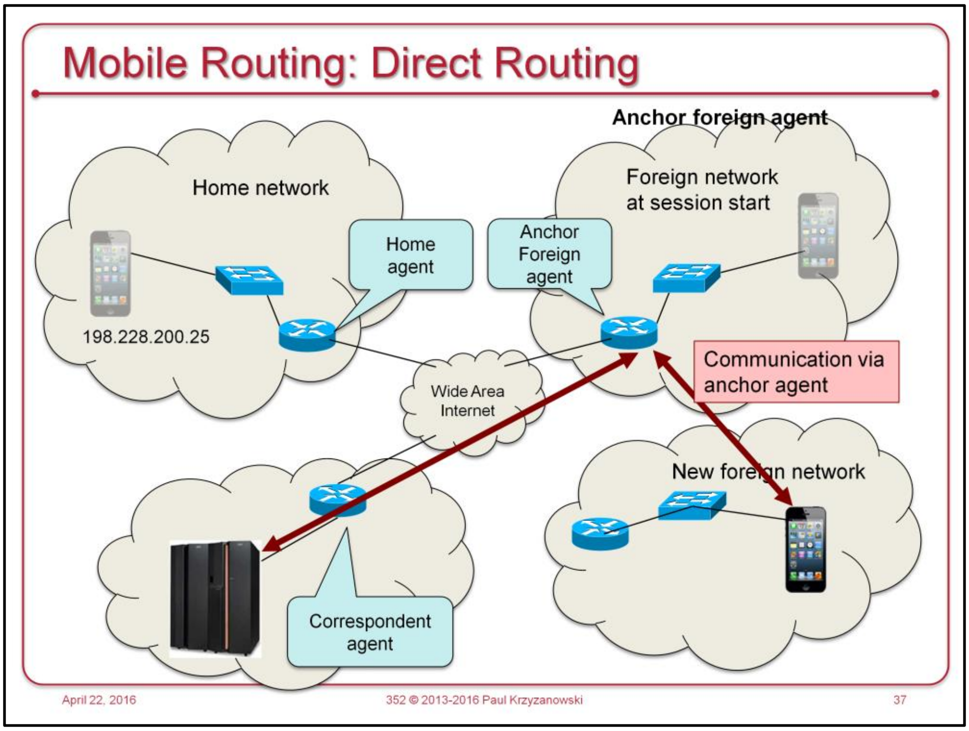

Mobile Routing: Direct Routing
Anchor foreign agent
Home network
Foreign network
at session start
Home
agent
Anchor
Foreign
agent
198.228.200.25
Wide Area
Internet
Get address of anchor foreign agent for 198.228.200.25
Correspondent
agent
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
34

# Mobile Routing: Direct Routing




April 22, 2016 352 © 2013-2016 Paul Krzyzanowski 35


Mobile Routing: Direct Routing
Anchor foreign agent
Home network
198.228.200.25
Home agent
Anchor Foreign agent
Foreign network at session start
Inform anchor agent of migration
Wide Area Internet
Correspondent agent
New foreign network
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
36


Mobile Routing: Direct Routing
Anchor foreign agent
Home network
Home agent
198.228.200.25
Anchor Foreign agent
Foreign network at session start
Communication via anchor agent
Wide Area Internet
New foreign network
Correspondent agent
April 22, 2016
352 © 2013-2016 Paul Krzyzanowski
37

# The end