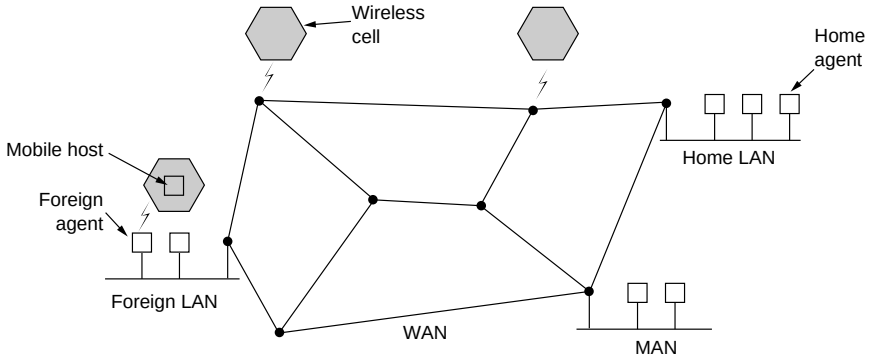
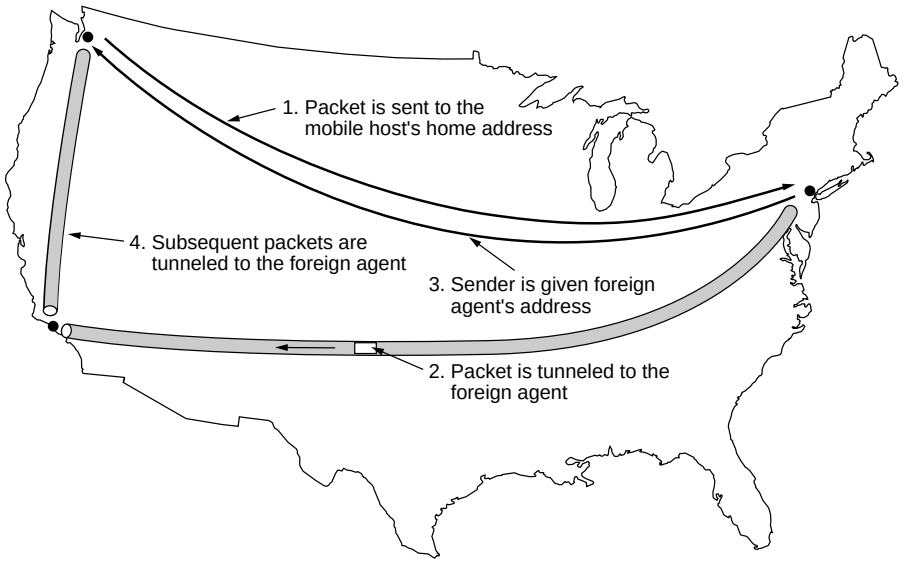
Revision of Lecture Twenty-Three

- Previous lecture focuses on interface between physical layer and network layer, referred to as **medium access control**
- Concepts of **user** and **signalling** (control) channels
- Random access (contention) algorithms
- This lecture we consider higher-layer protocol issues

Networks with Central Access

- In cellular network or WiFi with BSs or access points, establish an **end-to-end** path for two communicating mobiles is easy
  - All packets are routed through the established end-to-end path/connection
- Routing for mobile worldwide
  - Mobile host has a fixed **home** location with a permanent home address
  - When mobile host enters an area, it must register with **foreign** agent in charge of the area
  - Foreign agent then informs mobile's home agent at mobile's home location that the mobile is under its jurisdiction
  - When a packet is sent to mobile, it is routed to mobile's home address
  - Mobile's home agent is then **tunnelling** it to foreign agent where the mobile is currently in
  - Home agent also informs source where mobile is
  - New address sent back by home agent enables source to adapt its routing table
  - Subsequent packets can be sent directly to the foreign agent where the mobile is with

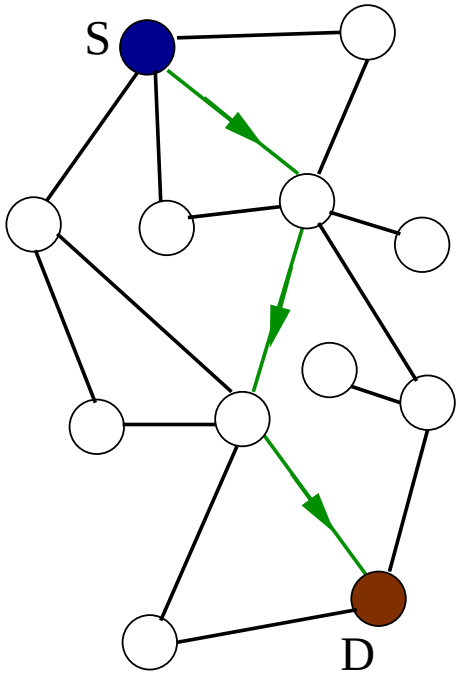




Networks with Distributed Access

- In a network with access points, such as in a cellular network or WiFi, information is transmitted from source to destination via an end-to-end path or connection

- In *ad hoc* networks, however, there are no central access points, and access to network is **distributed**
  1. Mobiles or nodes must periodically perform route discovery, via route discovery packets or beaconing
  2. Based on acquired route information, routing is to establish an end-to-end path from source to destination
  3. Packets are sent via this established end-to-end path



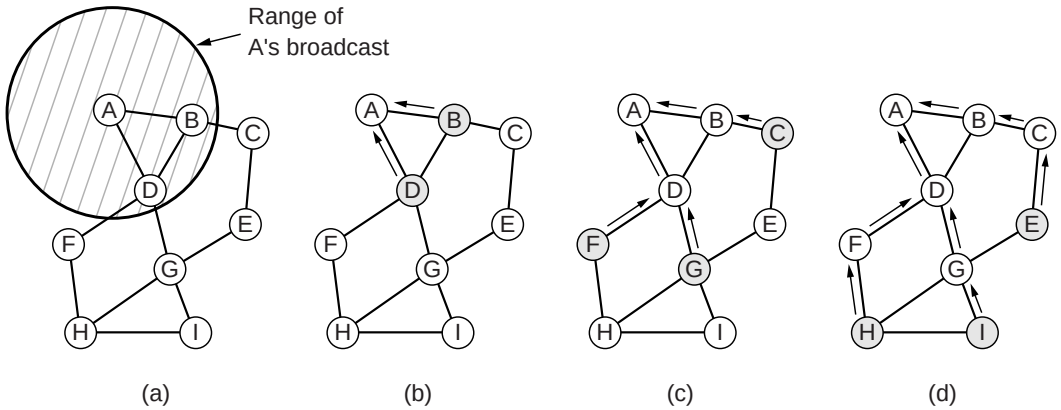
- Clearly, like in networks with central access points, in *ad hoc* networks, communications also rely on
  – Existence of **end-to-end** paths

- There are situations, there exists no end-to-end path most of times

  – before discussing what can be done, we first detail routing in *ad hoc* networks

Routing in Ad Hoc Networks

- Now, like hosts, routers can come and go. We will discuss a routing algorithm for ad hoc networks, called **ad hoc one-dimensional distance vector**, a relative of distance vector routing
- Each node maintains a table, keyed by destination, giving information about that destination, including which neighbour to send packets in order to reach the destination



- **Route discovery**: Consider node A wants to send a packet to node I but it does not know how. A broadcasts a ROUTE REQUEST (RReq) packet
  - When RReq packet arrives a node (B and D in this case as they can receive from A), it is checked to see if it is a duplicate or not. If a duplicate, it is discarded; otherwise do the next

Source address	Request ID	Destination address	Source sequence #	Dest. sequence #	Hop count

ROUTE REQUEST

Source address	Destination address	Destination sequence #	Hop count	Lifetime

ROUTE REPLY

  - If the receiver knows a fresh route to the destination, it sends a ROUTE REPLY (RRep) packet back to sender, basically telling source to "use me" to reach destination; otherwise it rebroadcasts RReq packet

Routing in Ad Hoc Networks (continue)

- **Route discovery**: Eventually, I receives the RReq packet, and it replies with a RRep packet, which is sent back using the route that RReq packet came in and this provides A routing information
- In route discovery, flooding is used, so many measures are employed to keep flood in check, and to make sure the route discovered is a fresh (live) one
- **Route maintenance**: nodes can move or be switched off $\longrightarrow$ network topology can change
  - Periodically, each node broadcasts a Hello message, and each of its neighbours is expected to respond to it
  - If no response is forthcoming, broadcaster knows that the specific neighbour either has moved out of its range or no longer exists
  - Similarly, if a node sends a packet to a neighbour that does not respond, it learns that that neighbour is no longer available
- This information is used to purge routes that no longer work, and also
  - When any of its neighbours becomes unreachable, the node checks its routing table to see which destinations have routes using this now-gone neighbour
  - For each of these routes, the active neighbours are informed that they must do purging too
  - The active neighbours then tell their active neighbours, and so on
- Even in *ad hoc* networks, communication protocols rely on existence of **end-to-end** paths
  - Traditional view of wireless networks: connected graphs over which end-to-end paths have to be established

Delay Tolerance Networks

- Some existing and emerging wireless networks: **no end-to-end paths** most of times, e.g.
  - deep-space interplanetary networks, vehicular ad hoc networks, military networks, wireless mobile sensor networks for environmental sensing and wildlife behavior monitoring
- For these types of applications, traditional protocols relying on end-to-end paths fail to work
  - Root of problem: **mobility** of nodes
  - Solution: also relying on mobility of nodes
- New **store-carry-and forward** paradigm: when next hop not available for nodes to forward message
  - Nodes store the message in their local buffers
  - carry it along their movements
  - and forward it to other appropriate nodes when a transmission opportunity becomes available
- This new "protocol" yields **delay tolerance** networks, also known as **disruption tolerance** networks
  - Called delay tolerance, as this type of applications must be able to tolerate to delay
  - Call disruption tolerance, as this type of applications is resilient to disruptions to network
- Basic "routing" protocol, **epidemic** routing: an extreme flooding based routing strategy
  - Source infects nodes it contacted with massage, and nodes with message infect others they contacted with massage
- Two-hop relaying: source selects some nodes relaying them to forward message to destination

Mobile Data Offloading

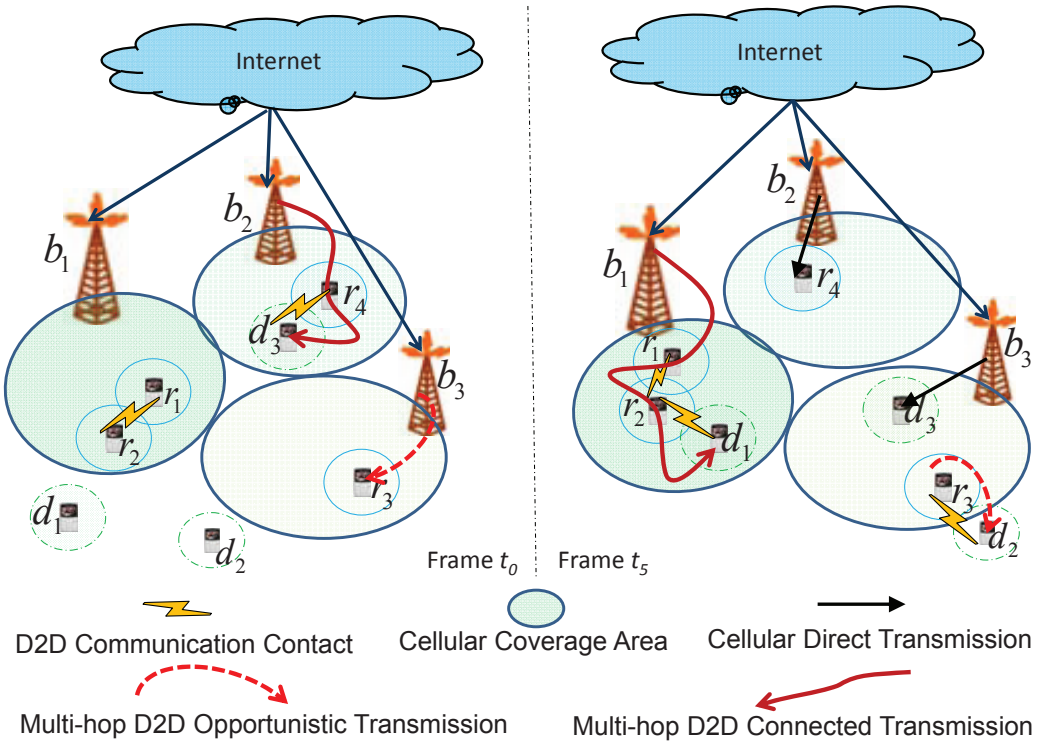
- Cisco Forecast 2017-2022
  - Global mobile data traffic grew 71 percent in 2017
  - Mobile video traffic was 59 percent of traffic in 2017
  - 54 percent of global mobile data traffic was offloaded in 2017
  - Mobile data traffic will increase 7-fold between 2017 and 2022
  - Monthly global mobile data traffic will surpass 77 exabytes by 2022
  - Over 79 percent of the world's mobile data traffic will be video by 2022

1 exabyte$= 10^{18}$ **bytes**

- Popular mobile content downloadings: relying on cellular network mode is extremely costly
  - In fact, cellular networks may not able to cope such large volumes of communications
- You all do it, WiFi offloading, your mobile have two modes, usual cellular mode, and when it comes to contact a WiFi, it can switch to WiFi $\longrightarrow$ Mobile social networks: thanks to this!

Device to Device Communications

- Device to device communications is not new
  - Exploit close proximity of two communicating devices, and local good channel condition, saving energy, etc.
- What new is D2D communication as a vital component of next generation of mobile network
- D2D Communications underlaying cellular network
  1. Cellular direct transmission
  2. D2D connected transmission
  3. D2D opportunistic transmission
- D2D communications share same cellular resources
  - Cellular direct: BS to mobile subscriber, usual communication mode, one-hop
  - D2D connected: BS via some mobile helpers to mobile subscriber, multi-hops This is collaborative communication or relaying, note end-to-end path
  - D2D opportunistic: relying on store-carry-and-forward, do not need end-to-end connection Exploit close proximity of two communicating devices, and local good channel condition



Summary

- This lecture has discussed high-layer protocol issues, in particularly, network routing, with two different communication protocols:
  - Relying on end-to-end connections
  - Do not require end-to-end connections, relaying on store-carry-and-forward
- Mobile networks with access points
- *Ad hoc* networks
- Delay/disruption tolerance networks
- Mobile data offloading
- Device-to-device communication underlaying cellular networks