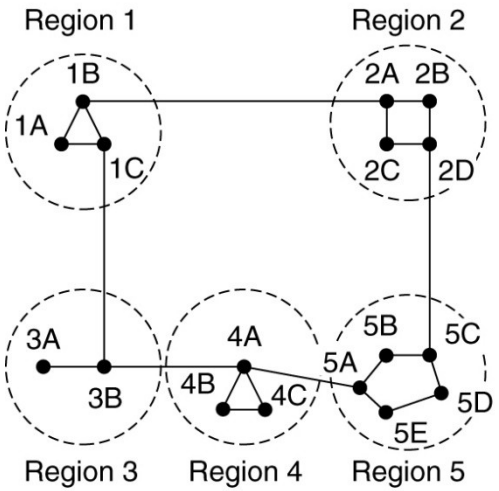
Chapter 5

The Network Layer
Part 3

Hierarchical Routing



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

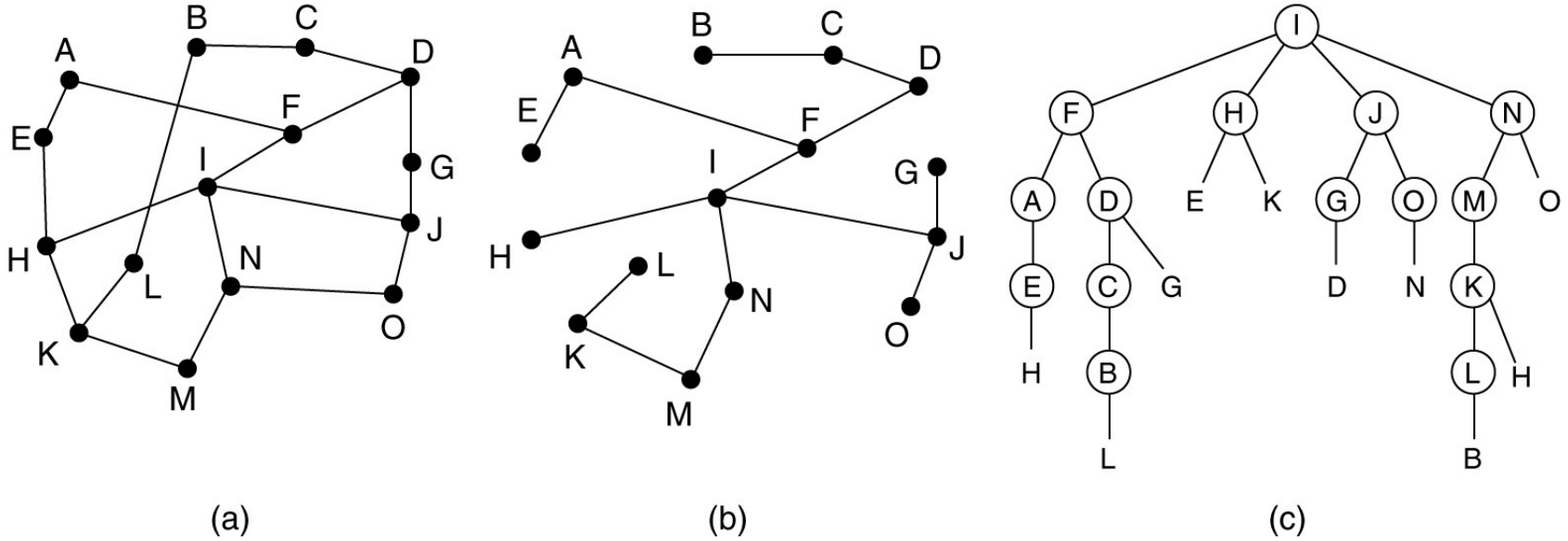
Hierarchical routing.

Broadcast Routing

a) Applications: Weather reports to be sent to all hosts

- To all
- Flooding
- Multi-destination routing
- Using Sink tree (Spanning tree)
- Reverse Path forwarding

Broadcast Routing

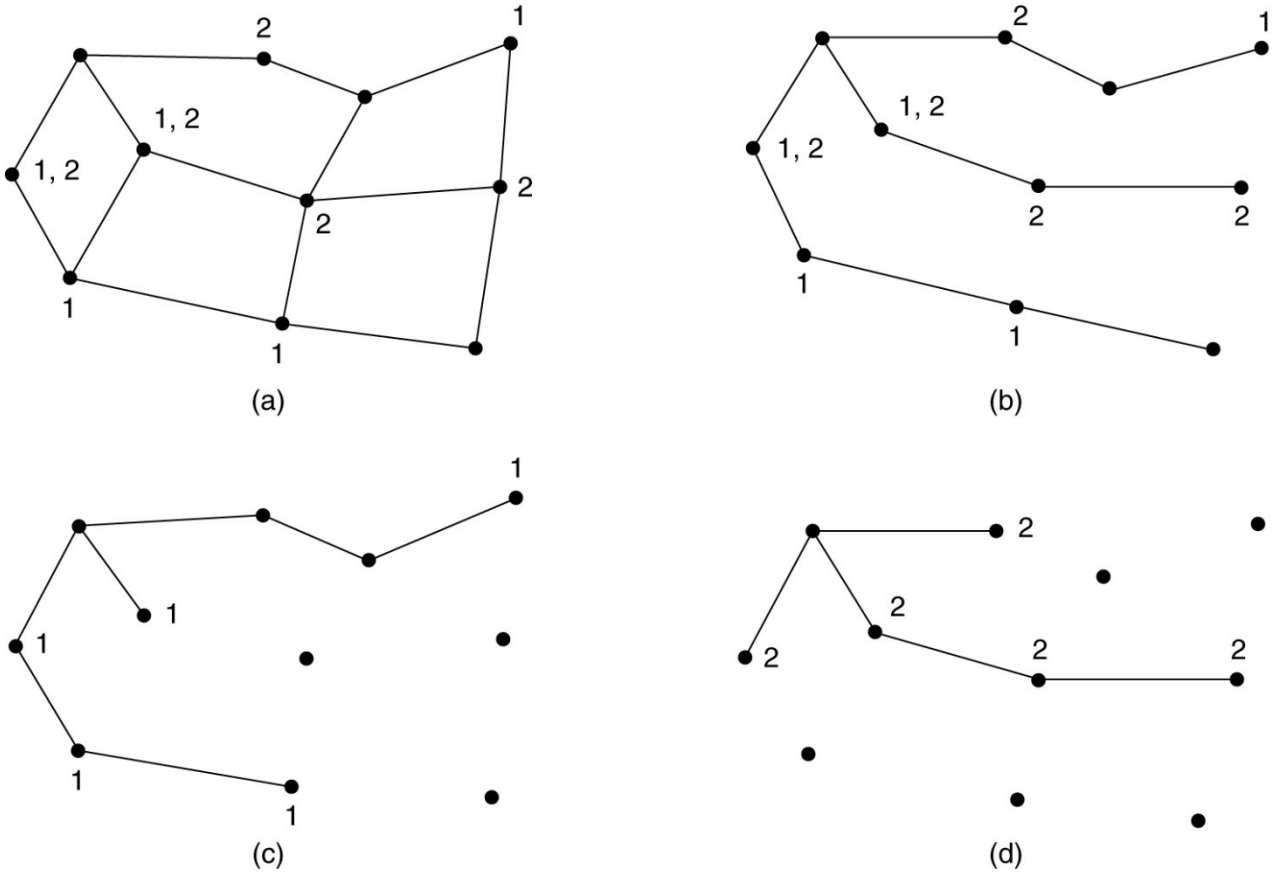


Reverse path forwarding. (a) A subnet. (b) a Sink tree. (c) The tree built by reverse path forwarding.

Reverse Path Forwarding

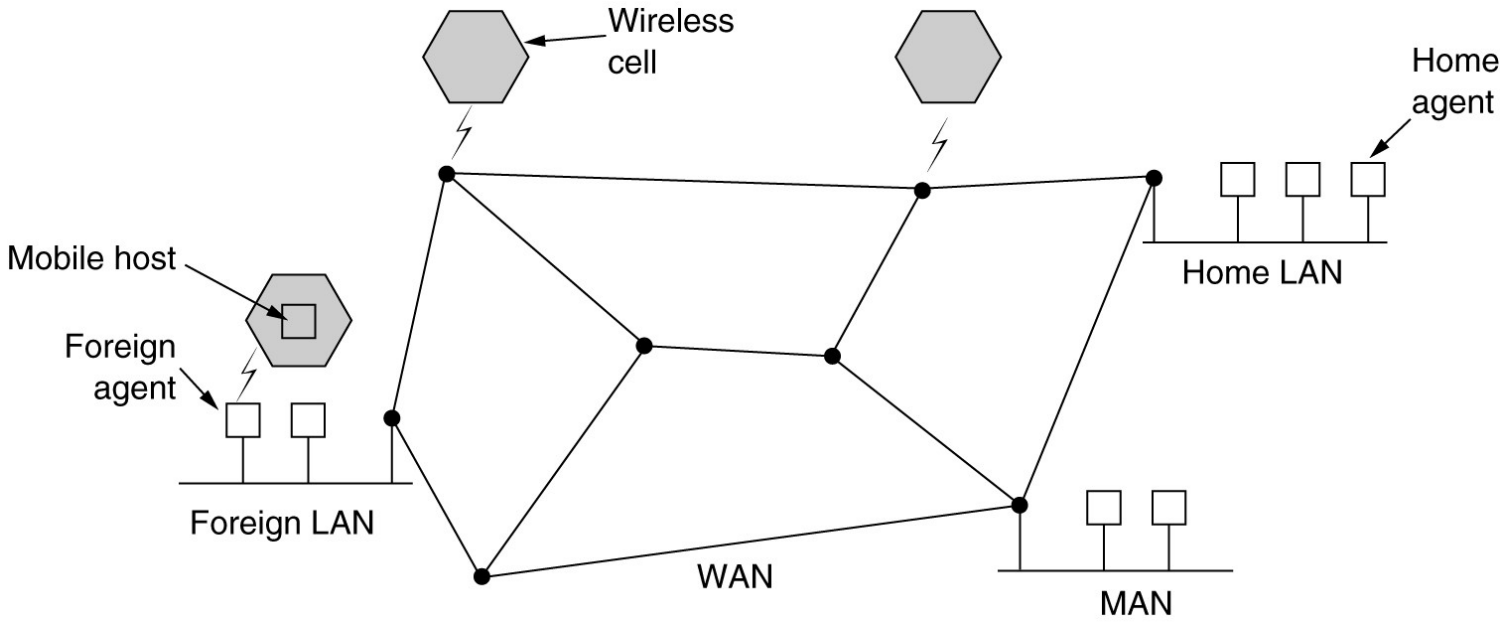
- Ensures loop-free forwarding of multicast packets
- Decision to forward traffic is based upon source address and not on destination address as in unicast routing
- When a multicast packet enters a router's interface, the router looks up the list of networks that are reachable via that interface
- If the router finds a matching routing entry for the source IP address of the multicast packet, the RPF check passes and the packet is forwarded to all other interfaces that are participating in that multicast group
- If the RPF check fails, the packet is dropped.
- By only forwarding packets that come into the interface that also holds the routing entry for the source of the packet, loops are prevented

Multicast Routing



(a) A network. (b) A spanning tree for the leftmost router.
(c) A multicast tree for group 1. (d) A multicast tree for group 2.

Routing for Mobile Hosts



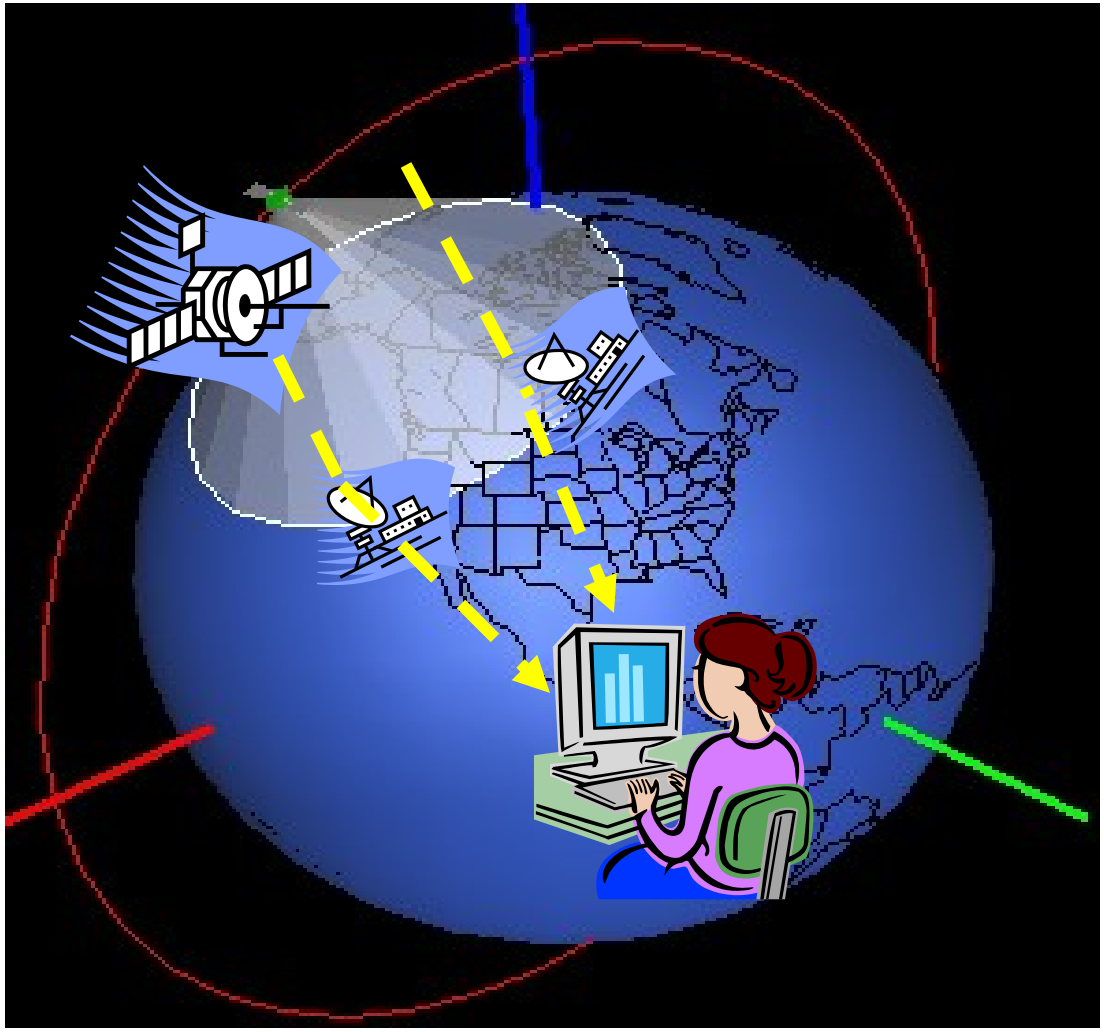
A WAN to which LANs, MANs, and wireless cells are attached.

Why Mobility Protocols

a) Satellites with IP-enabled devices capture videos, images and send them to control centers on earth

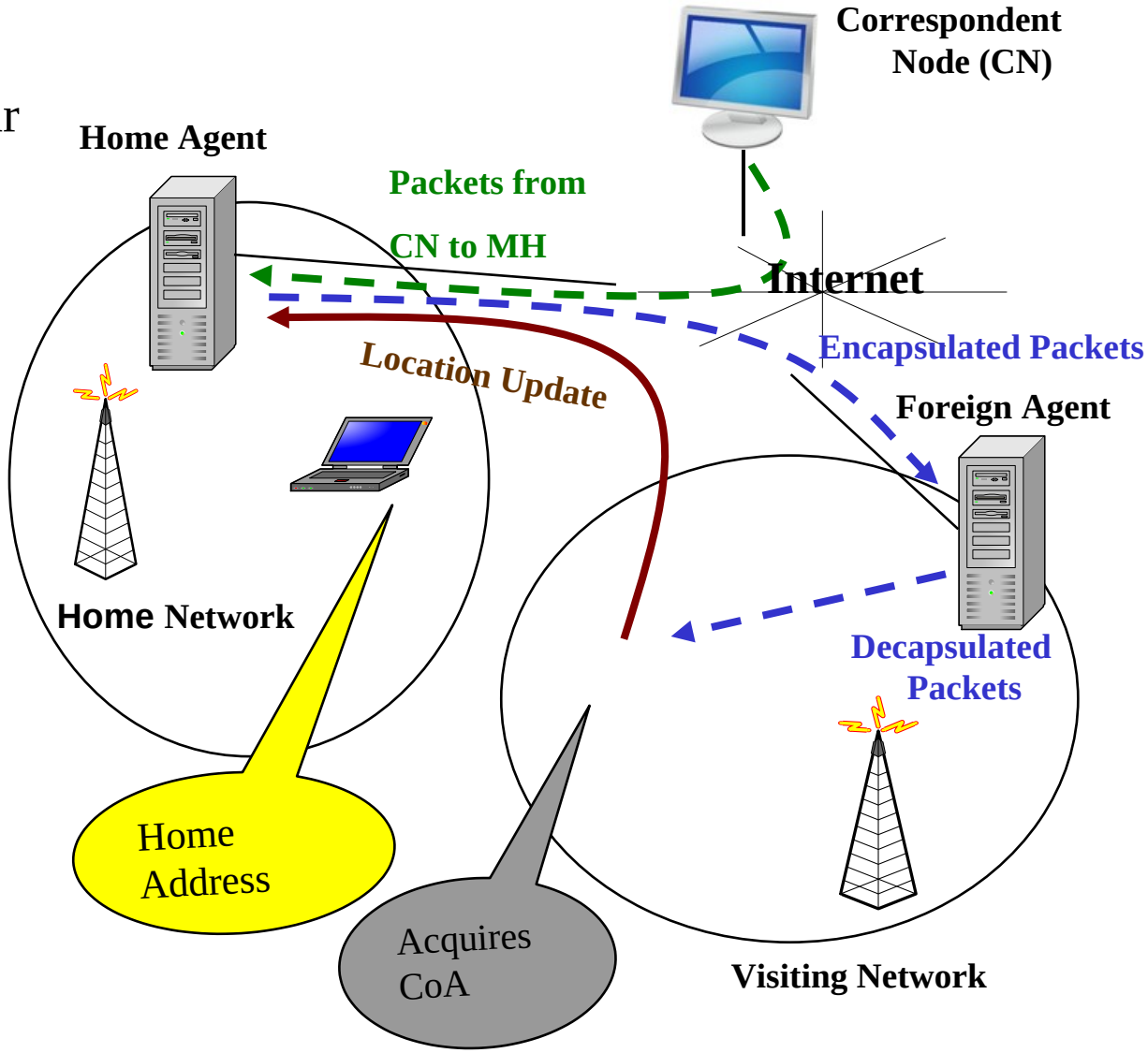
b) Need to maintain continuous connectivity with remote computer

c) Mobility protocols are required to ensure session continuity



IETF Solution to IP Mobility: Mobile IP

- Employs mechanism similar to postal service mail forwarding
- Problems:
  - Inefficient routing
  - High handover latency
  - Packet loss

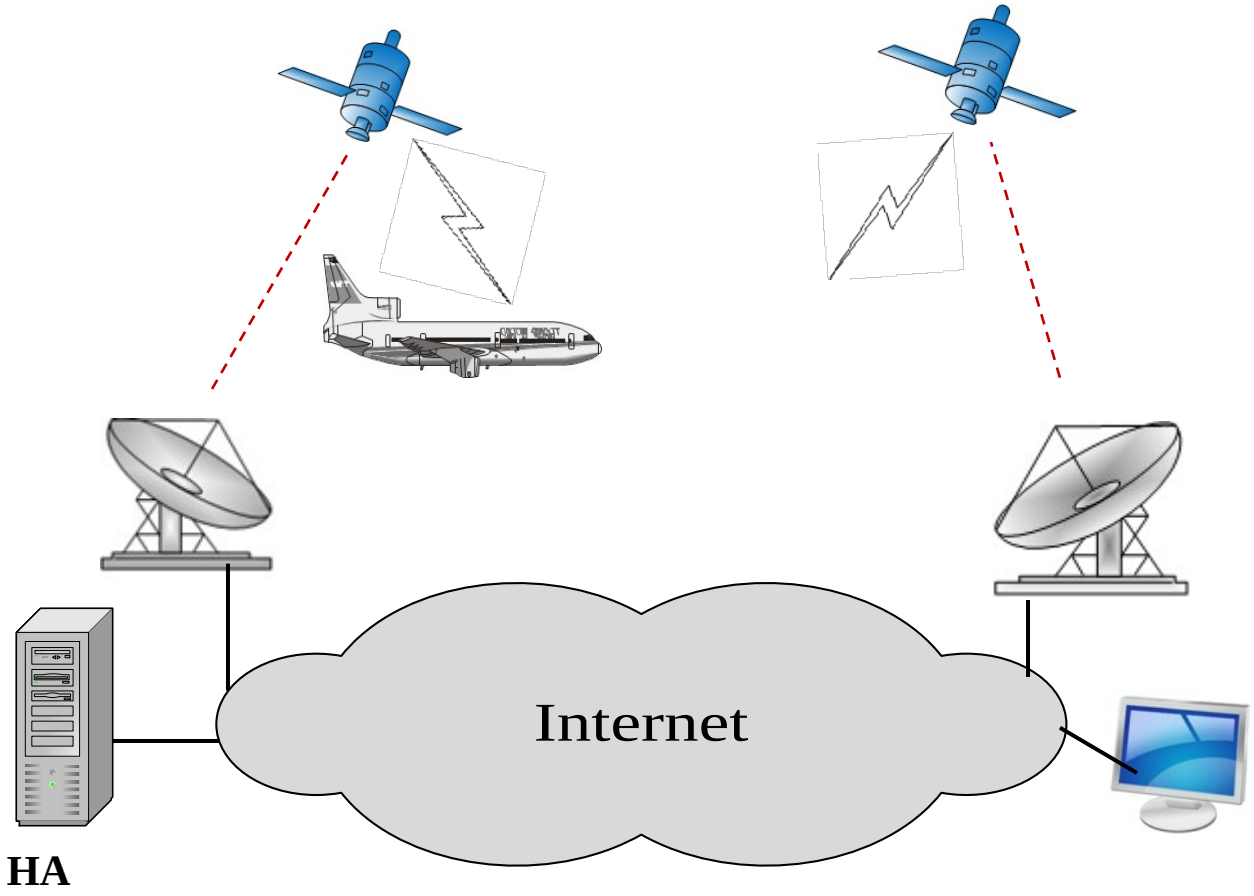


Network Mobility (NEMO)

a) A collection of nodes moving as a unit (Example: airplanes, trains, ships)

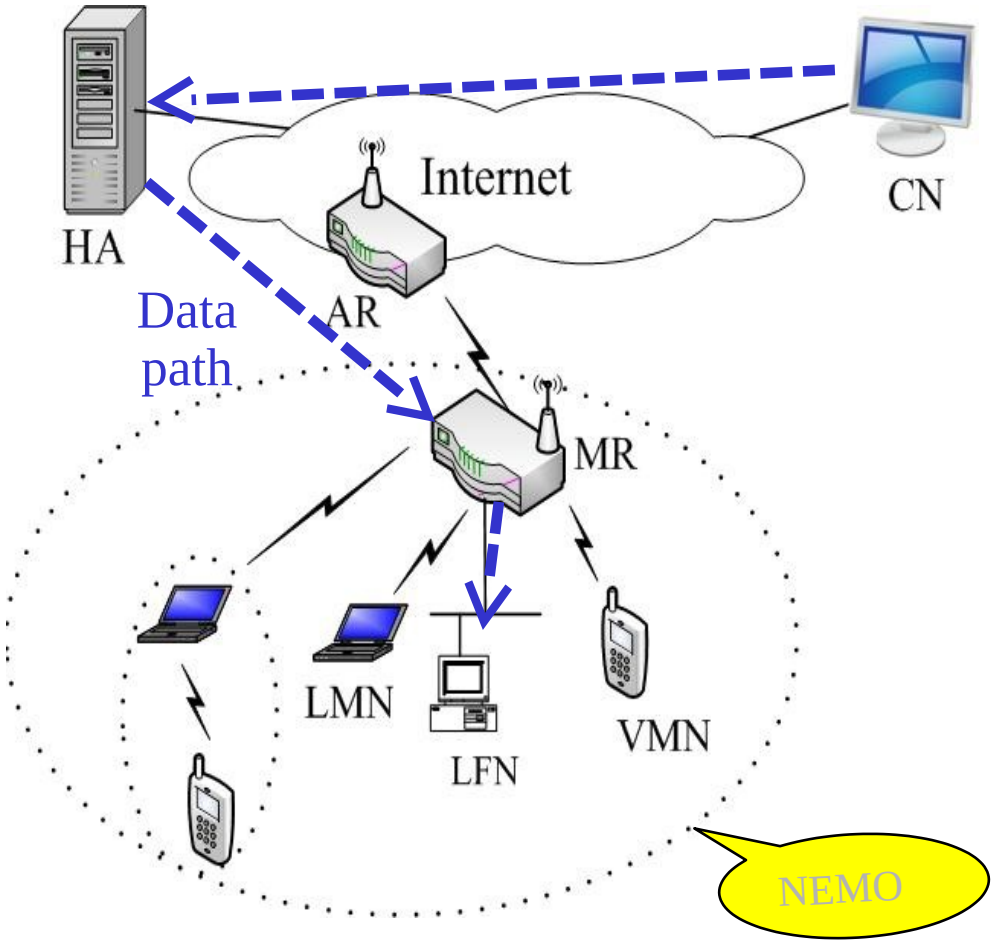
b) Mobility can be managed in an aggregated way in NEMO

c) Mobile Router acts as default gateway and manages mobility on behalf of mobile network nodes

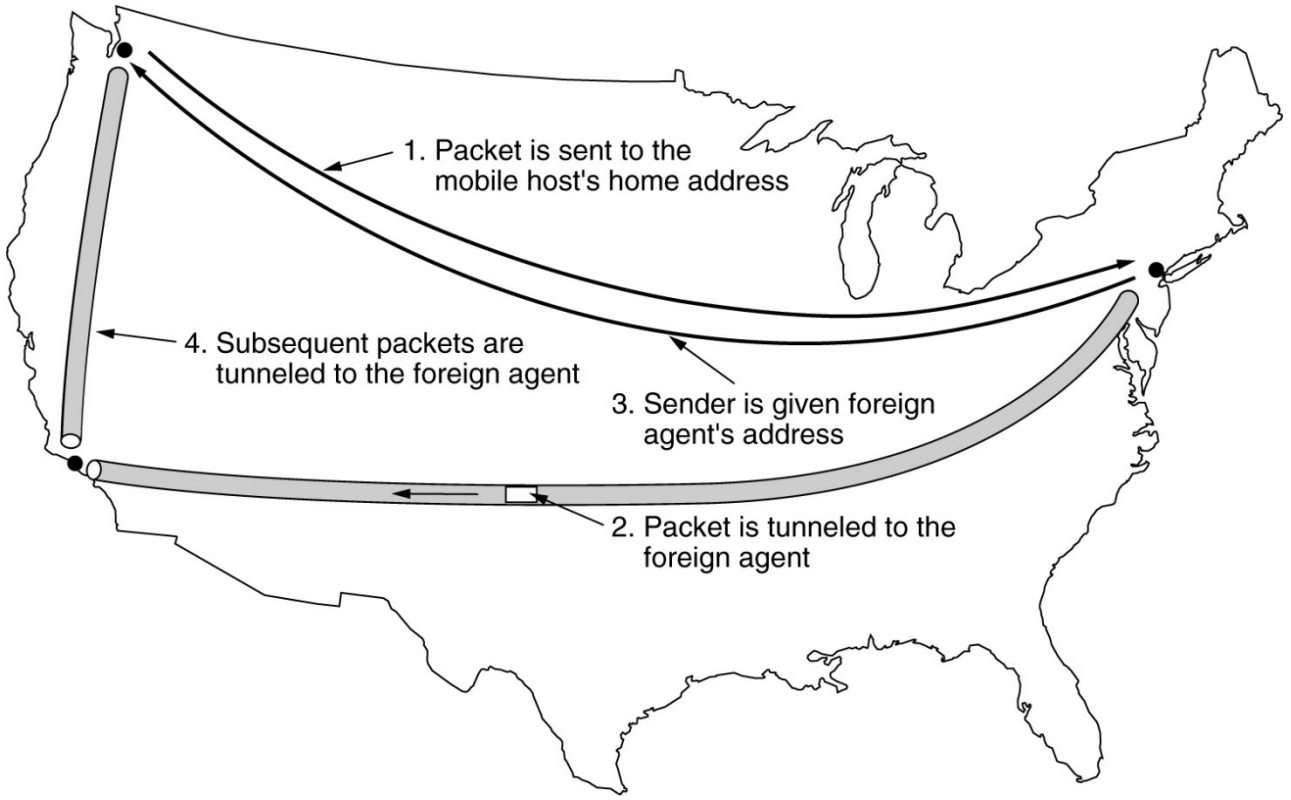


NEMO Architecture

- Inside NEMO
  - MR: Mobile Router
  - LFN: Local Fixed Node
  - LMN: Local Mobile node
  - VMN: Visiting Mobile Node
- Problems:
  - Routing through HA
  - Heavy load on HA
  - Drop in throughput during handover



Routing for Mobile Hosts (2)



Packet routing for mobile users.

Routing in Ad Hoc Networks

Possibilities when the routers are mobile:

1. Military vehicles on battlefield.
   - No infrastructure.
2. A fleet of ships at sea.
   - All moving all the time
3. Emergency works at earthquake .
   - The infrastructure destroyed.
4. A gathering of people with notebook computers.
   - In an area lacking 802.11.

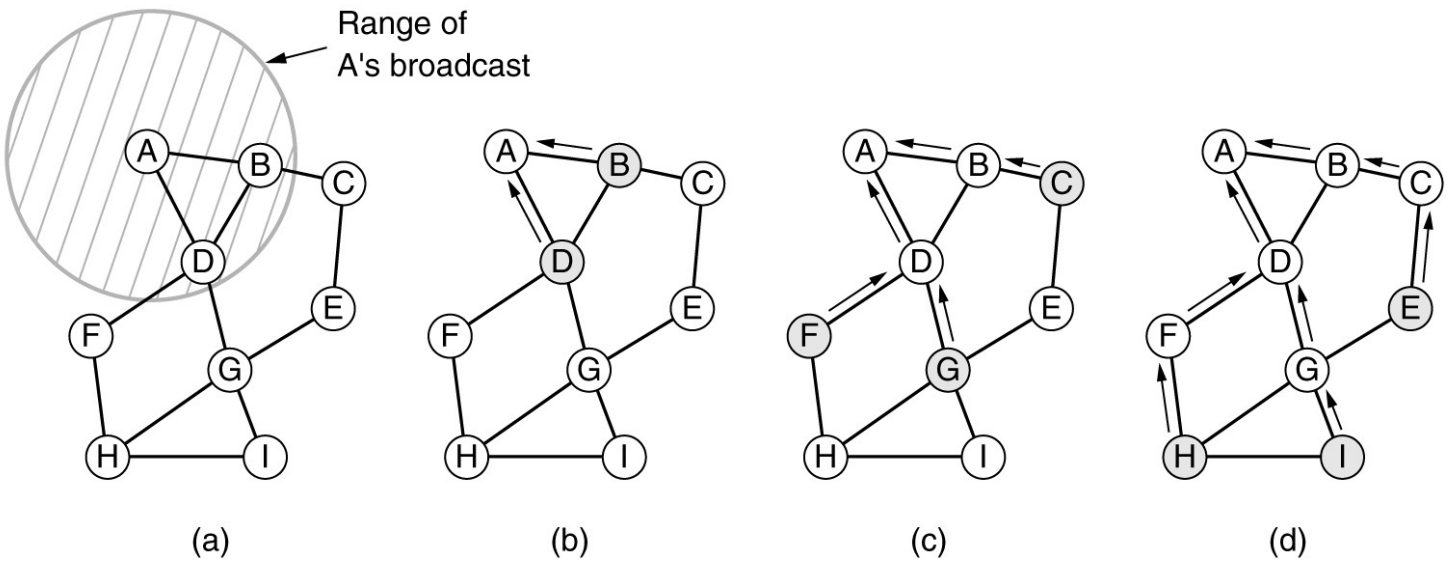
Ad hoc networks

- The topology may be changing all the time
- Hence, routing will also change frequently
- MANET
- VANET
- FANET

AODV

- AODV (Ad hoc On-demand Distance Vector) routing protocol is a classic Ad hoc routing protocol.
  - A route is determined when somebody wants to send packet to that destination
- There are other protocols not discussed here

Route Discovery



a) Range of A's broadcast.

b) After B and D have received A's broadcast.

c) After C, F, and G have received A's broadcast.

d) After E, H, and I have received A's broadcast.

Shaded nodes are new recipients. Arrows show possible reverse routes.

Route Discovery (2)

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

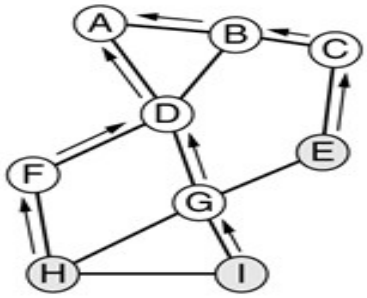
Format of a ROUTE REQUEST packet.

Route Discovery (3)

Source address	Destination address	Destination sequence #	Hop count	Lifetime

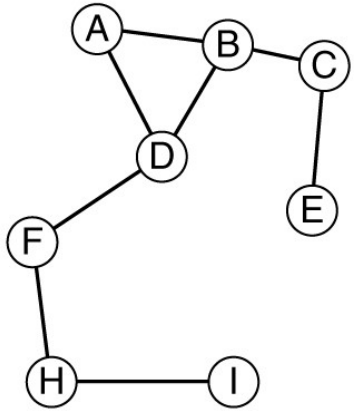
Format of a ROUTE REPLY packet.

Route Maintenance



Dest.	Next hop	Distance	Active neighbors	Other fields
A	A	1	F, G	
B	B	1	F, G	
C	B	2	F	
E	G	2		
F	F	1	A, B	
G	G	1	A, B	
H	F	2	A, B	
I	G	2	A, B	

(a)

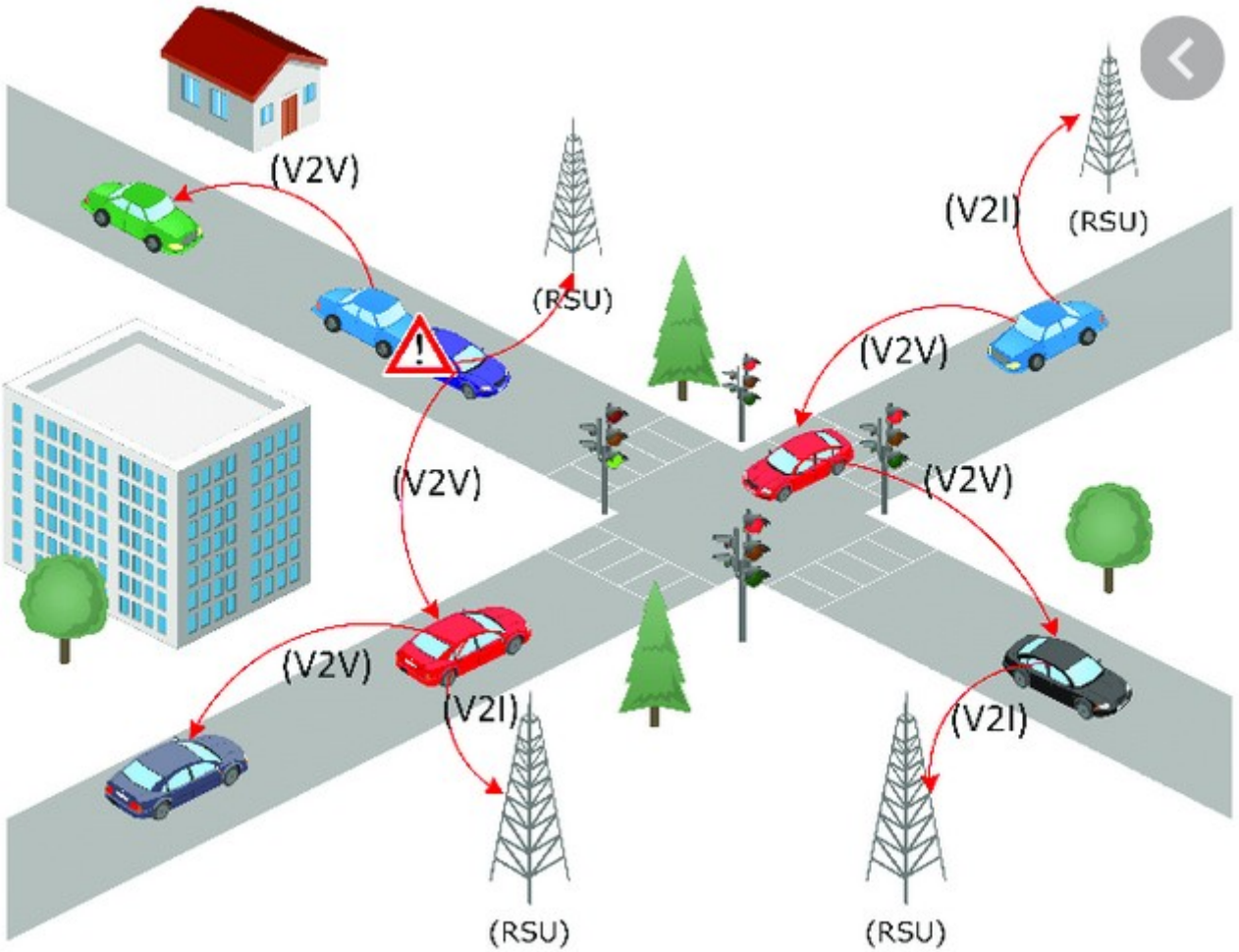


(b)

(a) D's routing table before G goes down.

(b) The graph after G has gone down.

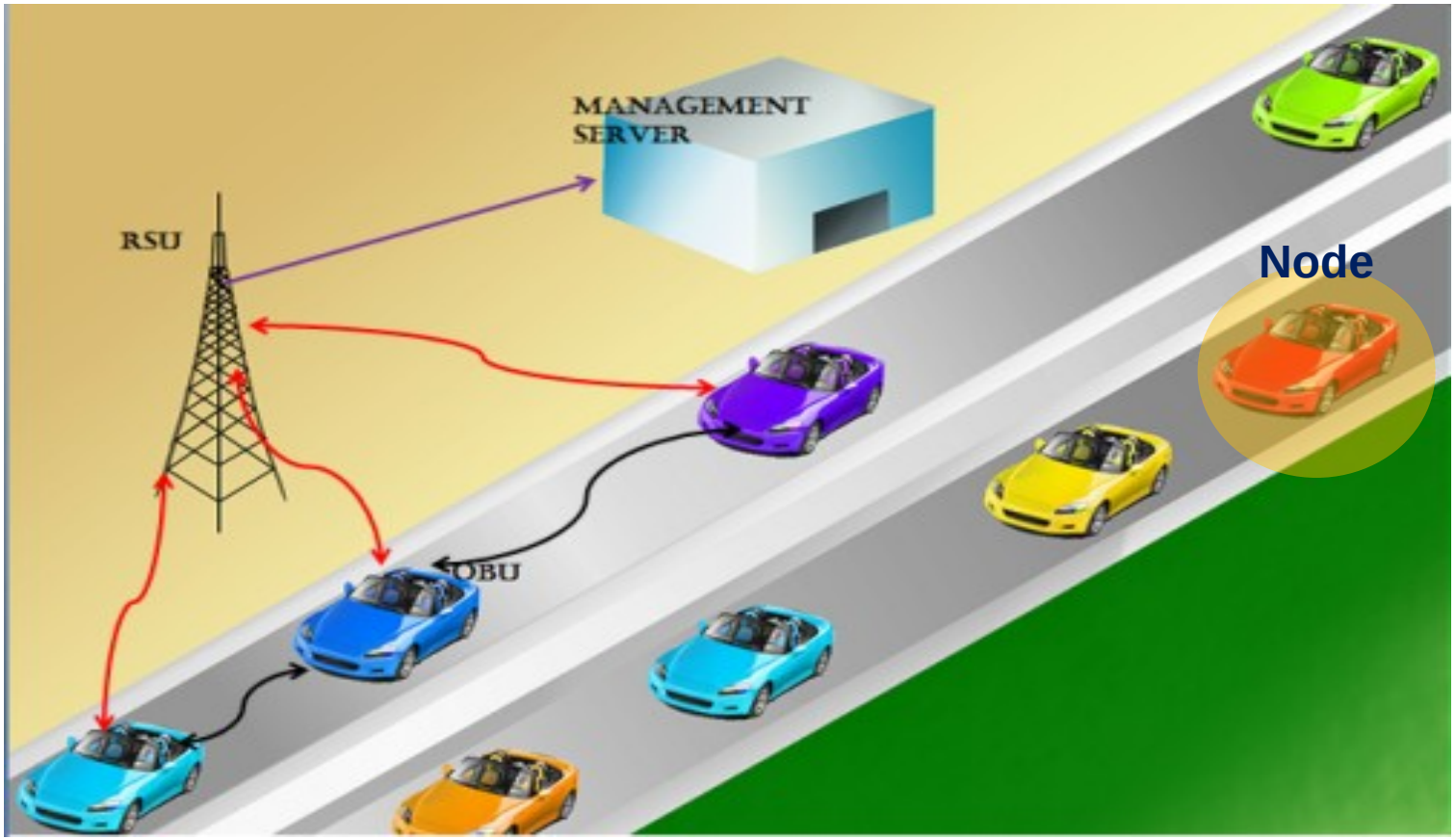
VANET



What is VANET ?

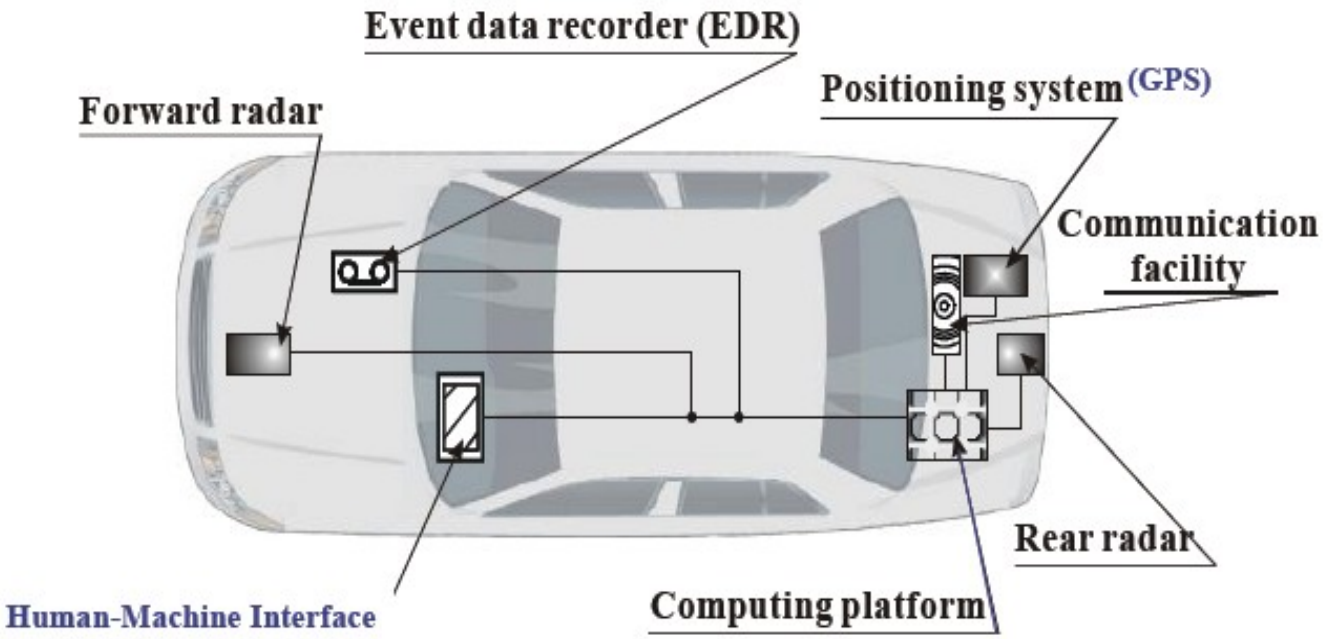
Next generation intelligent vehicular networking technologies

Uses moving car as nodes to create mobile network



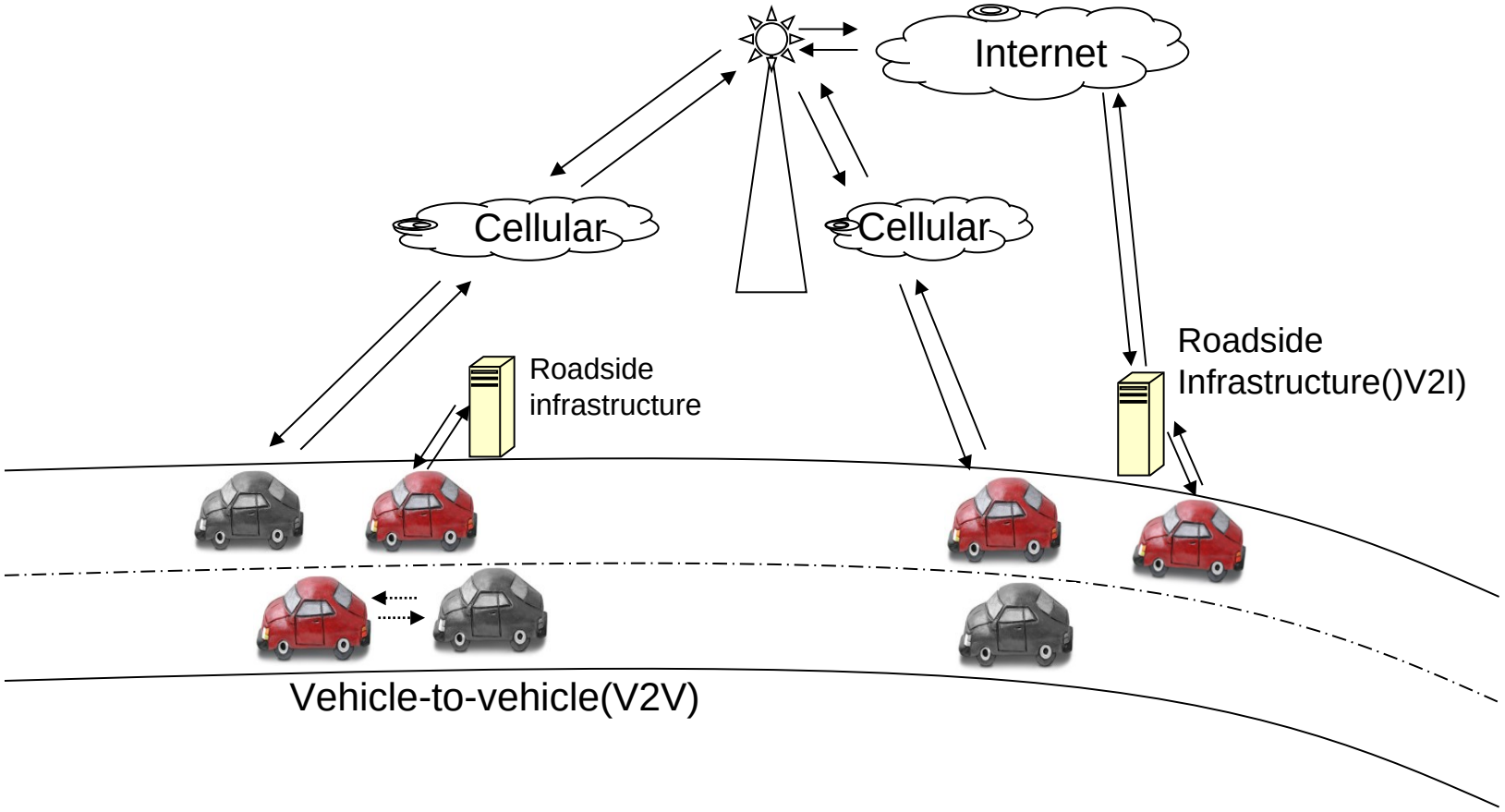
Sensors in Modern car

Equipped with GPS, sensors, computing and comm devices



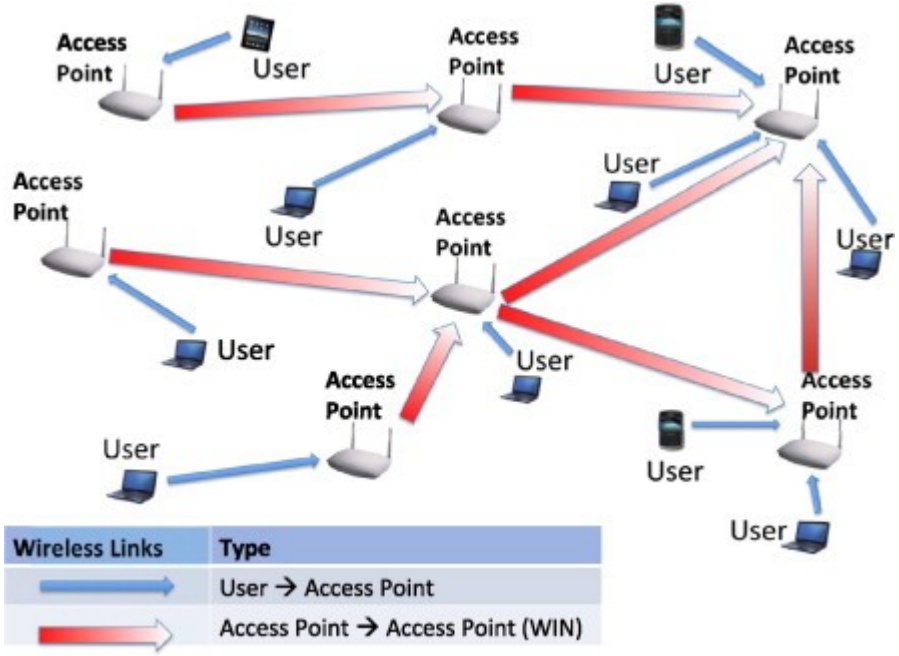
V2V and V2I Communication

Vehicles talk to other vehicles (V2V) and road-side infrastructure(V2I)

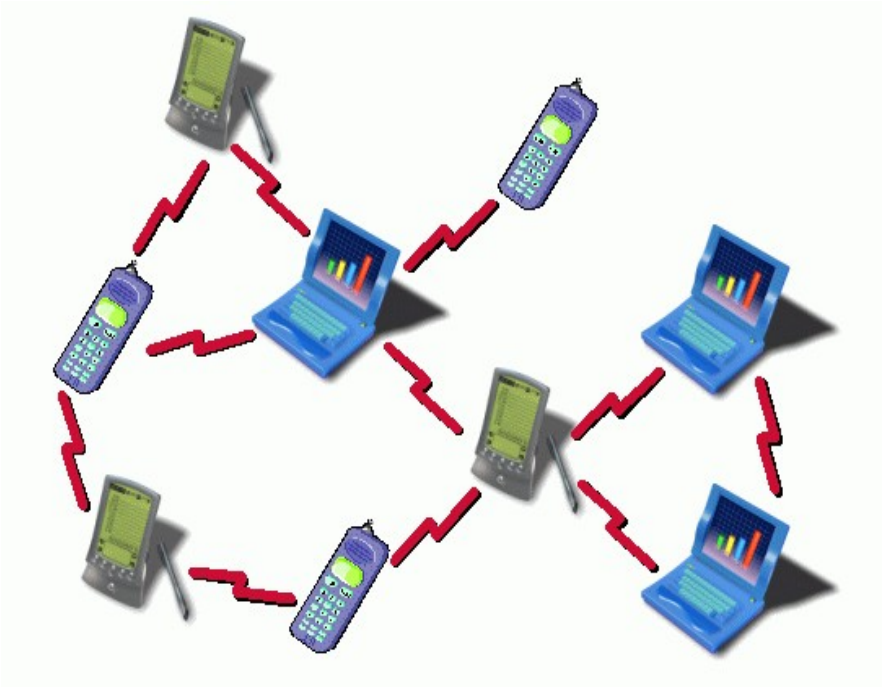


Infrastructure-less

- A wireless ad hoc network is a decentralized type of wireless networl
  - Not rely on a preexisting infrastructure: routers in wired networks or access points

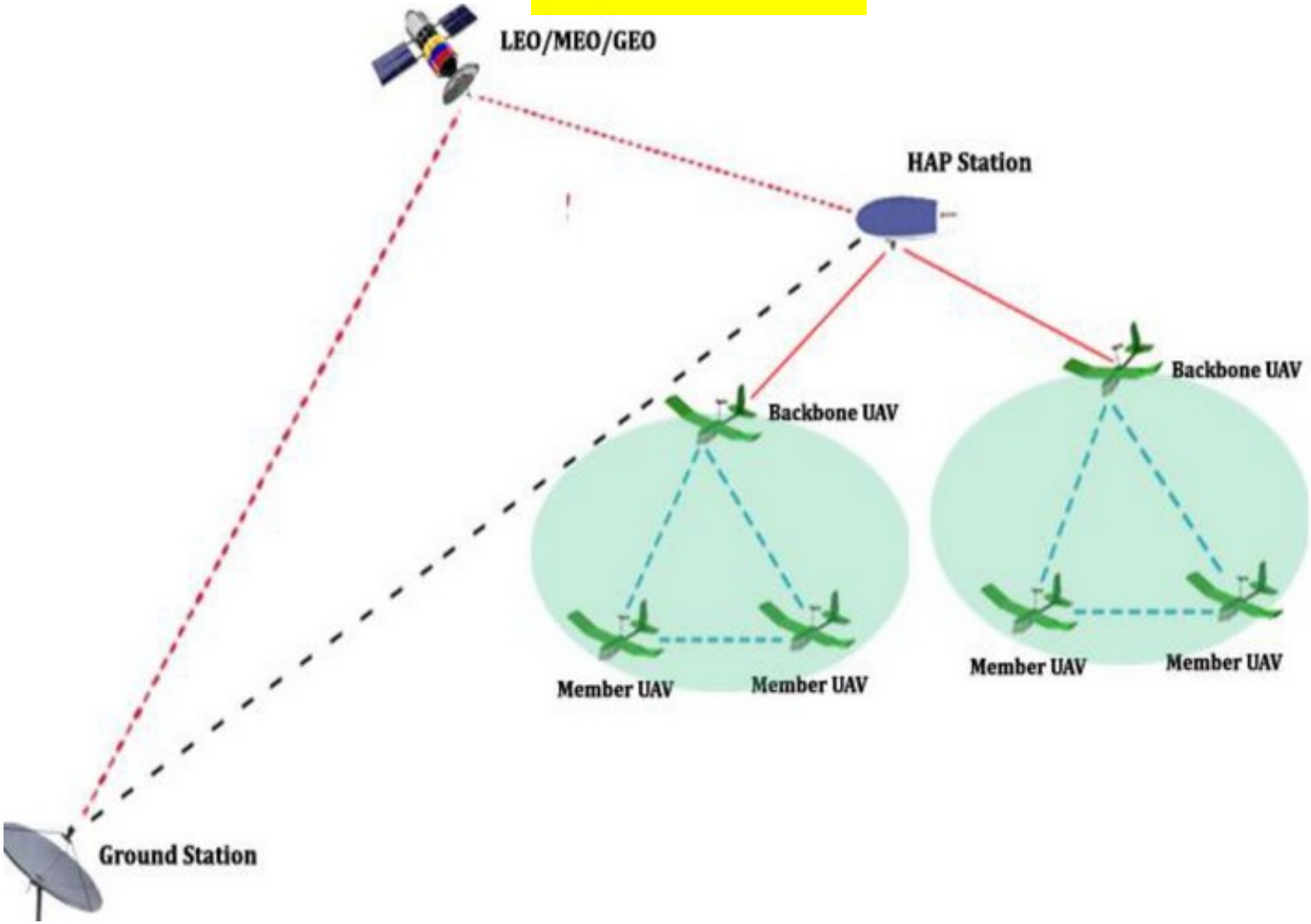


Infrastructure



Infrastructure less/Ad hoc

FANET


LEO/MEO/GEO
HAP Station
Backbone UAV
Backbone UAV
Member UAV
Member UAV
Member UAV
Member UAV
Ground Station

Unmanned Aerial Vehicle (UAV)

- **Unmanned aerial vehicle (UAV), normally known as drone, is an aircraft without a human pilot involved.**
- **UAV is either controlled autonomously by on-board computers or by the remote control of a pilot on the ground**
- **Previously, used for remotely piloted aircraft.**
- **Nowadays, UAV's are used for growing number of civil applications.**

Fanet vs. Vanet vs. Manet

a) FANET can be viewed as a special form of MANET and

b) VANET. But there are some difference

✓ Mobility degree

FANET nodes is much higher than the mobility degree of MANET or VANET nodes. MANET and VANET nodes are walking men and cars respectively, FANET nodes fly in the sky.

✓ **Changing topology**

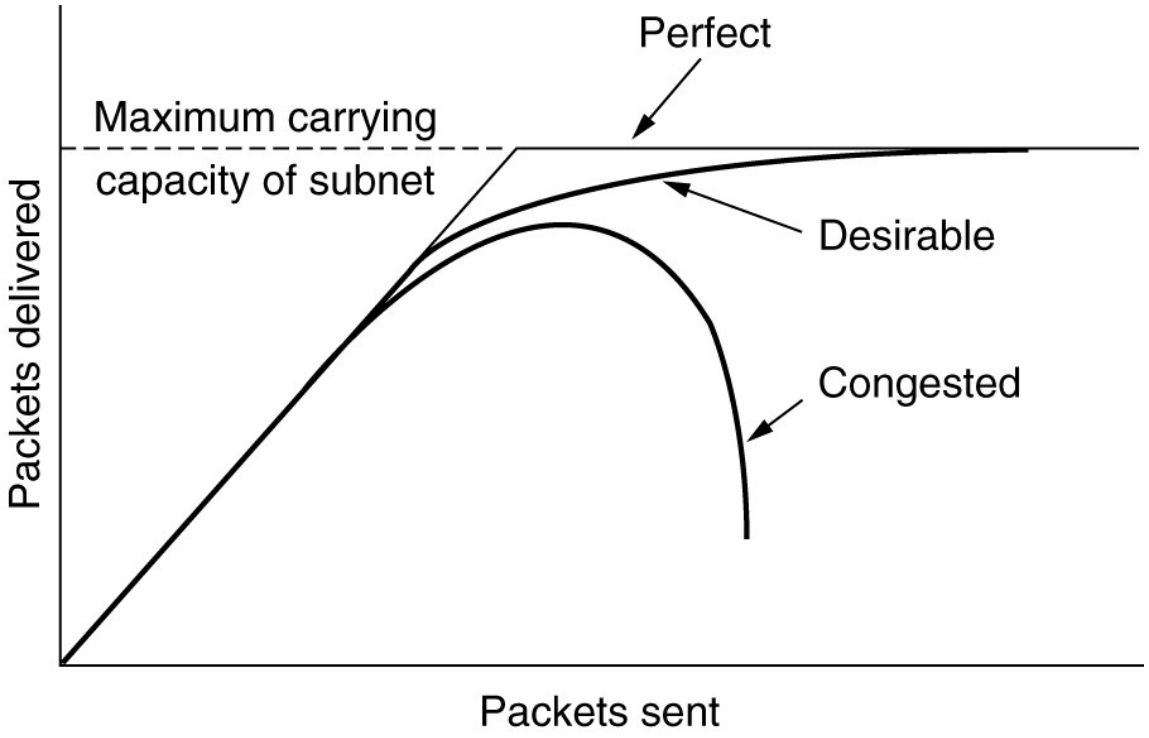
✓ For FANET nodes, the topology changes more frequently than the network topology of a typical MANET or even VANET.

	MANET	VANET	FANET
Node mobility	Low	High	Very high
Mobility model	Random	Regular	Regular for predetermined paths, but special mobility models for autonomous multi-UAV systems
Node density	Low	High	Very low
Topology change	Slow	Fast	Fast
Radio propagation model	Close to ground, LoS is not available for all cases	Close to ground, LoS is not available for all cases	High above the ground, LoS is available for most of the cases
Power consumption and network lifetime	Energy efficient protocols	Not needed	Energy efficiency for mini UAVs, but not needed for small UAVs
Computational power	Limited	High	High
Localization	GPS	GPS, AGPS, DGPS	GPS, AGPS, DGPS, IMU

Congestion Control Algorithms

- General Principles of Congestion Control
- Congestion Prevention Policies
- Congestion Control in Virtual-Circuit Subnets
- Congestion Control in Datagram Subnets
- Load Shedding
- Jitter Control

Congestion



When too much traffic is offered, congestion sets in and performance degrades sharply.

General Principles of Congestion Control

1. Monitor the system .
   - detect when and where congestion occurs.
2. Pass information to where action can be taken.
3. Adjust system operation to correct the problem.

Congestion Prevention Policies

Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Policies that affect congestion.

Data Link layer policies

- GoBack N (heavy load) vs. Selective repeat (less load)
- Out of order caching policy is closely realted
- Ack Policy
  - Ack immediately will generate extra traffic
  - Piggybacked Ack
- Flow control policy
  - Tight window bound reduces data rate and can fight congestion

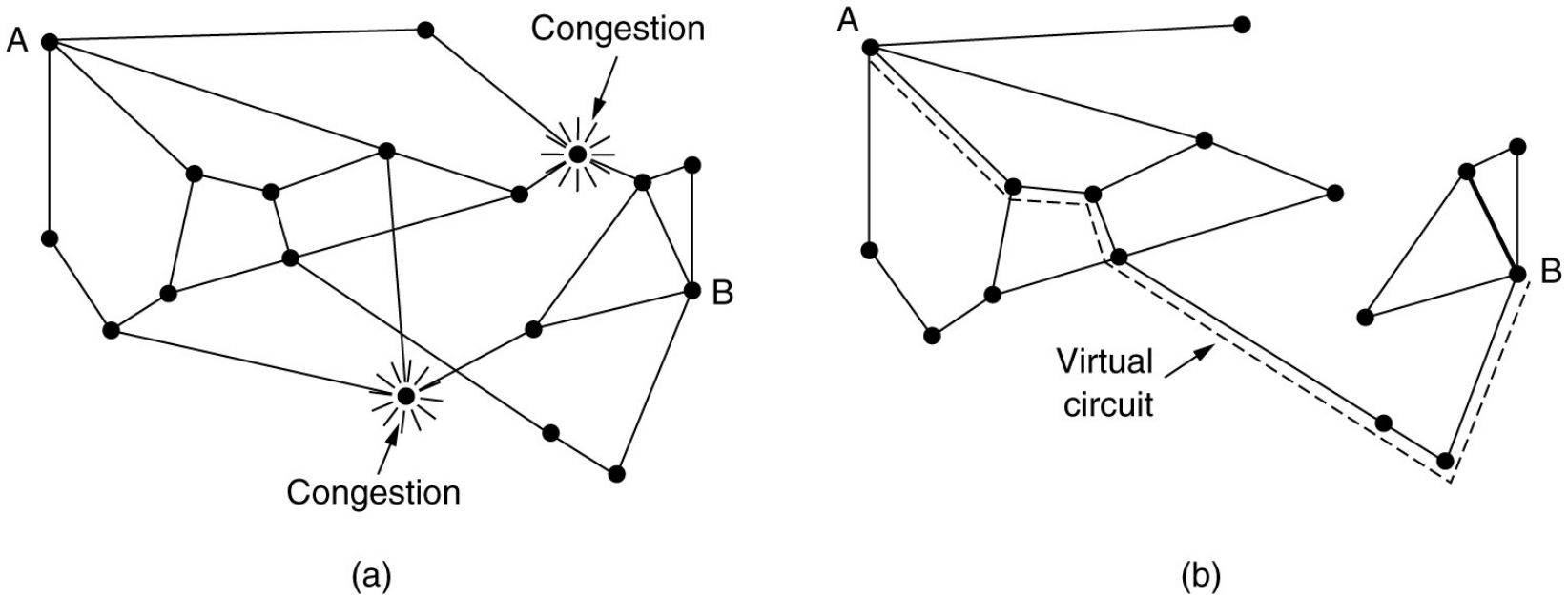
Network layer policies

- VC vs Datagram
- Routers to have one queue per line or shared queue
- Discard policy: Good policy vs bad policy (New / old packet):
  - Milk policy /Wine Policy
- Good routing alg: can spread the traffic

Transport layer policies

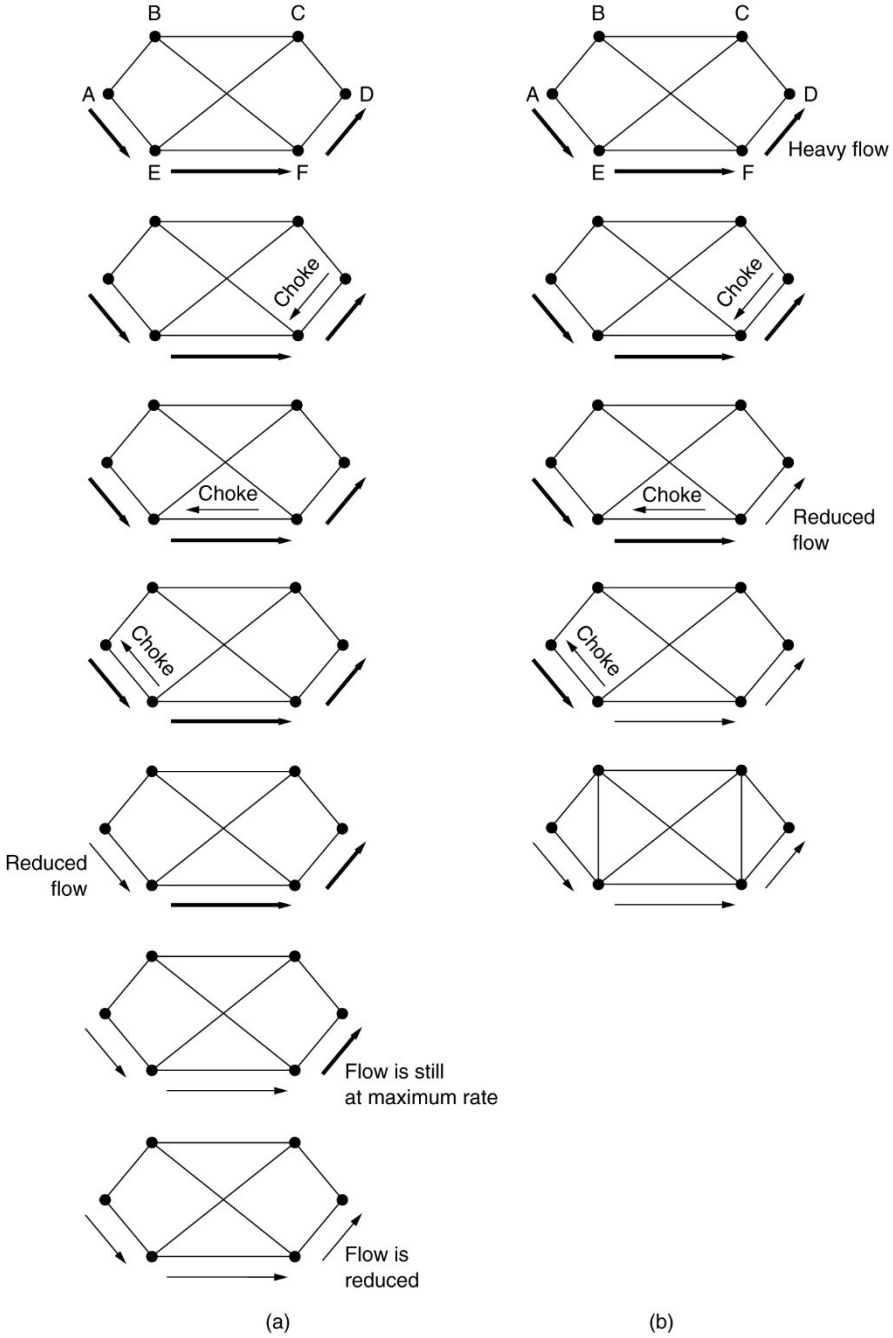
- Similar to DL layer policies => one single link
- However, timeout determination is more complex in Transport layer than DL layer (multi-hop)
- Timeout too short: extra packets are sent
- Timeout too long: slow response in case of lost segment

Congestion Control in Virtual-Circuit Subnets



(a) A congested subnet. (b) A redrawn subnet, eliminates congestion and a virtual circuit from A to B.

Hop-by-Hop Choke Packets



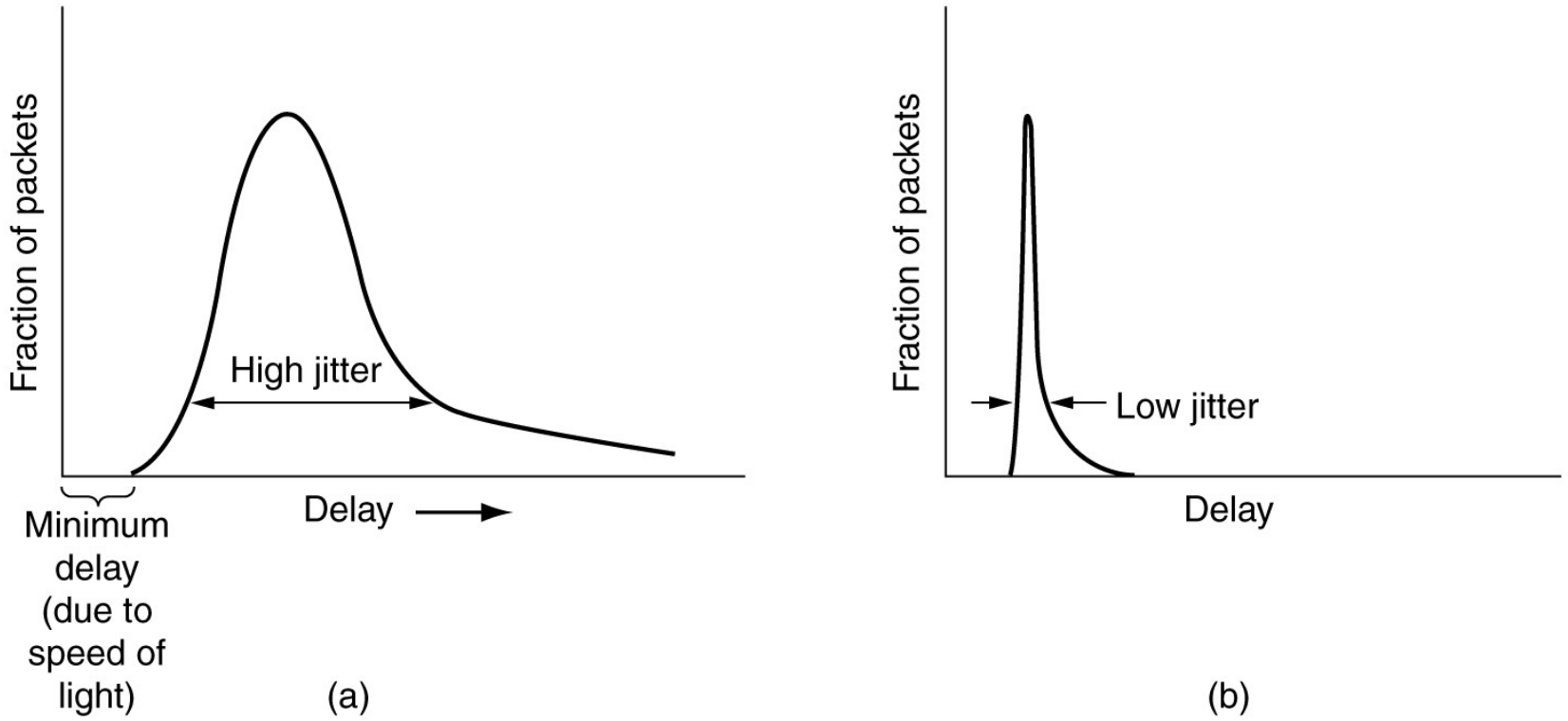
(a) A choke packet that affects only the source.

(b) A choke packet that affects each hop it passes through.

Random Early Detection

- Routers maintain a running average of their queue length
- If the average queue length exceeds some threshold, the line is said to be congested.
- Packets are dropped
- Inform other routers: Choke packets (adds traffic)
- Alternative approach, implicit (not to notify, just drop)

Jitter Control



(a) High jitter. (b) Low jitter.

Quality of Service

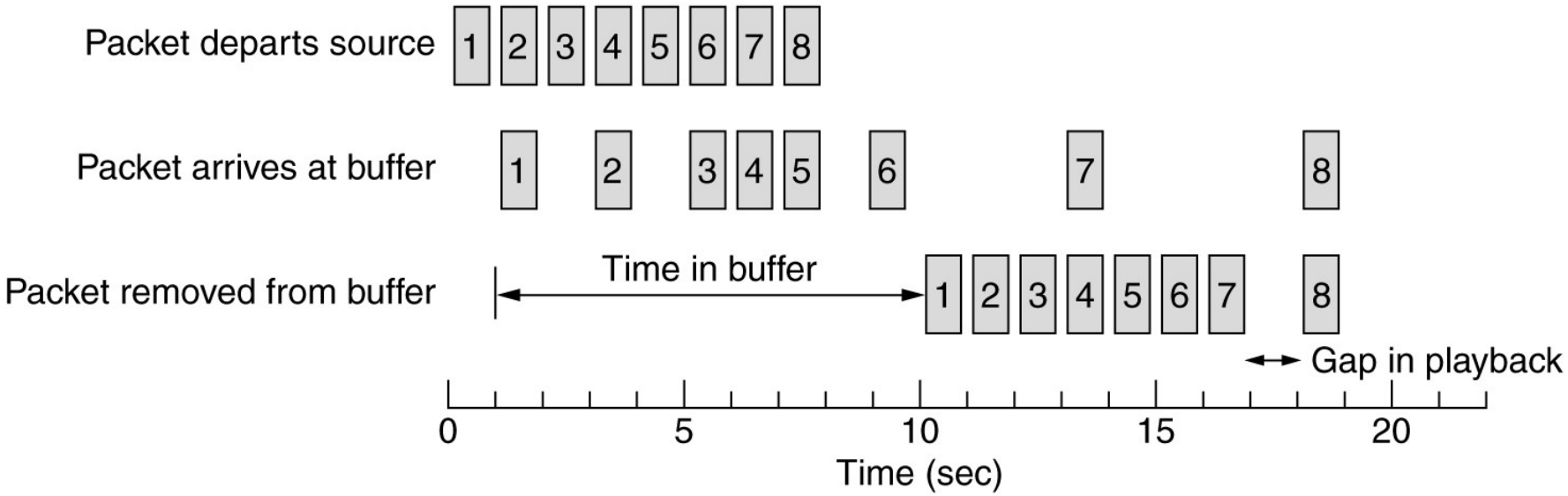
- Requirements
- Techniques for Achieving Good Quality of Service
- Integrated Services
- Differentiated Services
- Label Switching and MPLS

Requirements

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

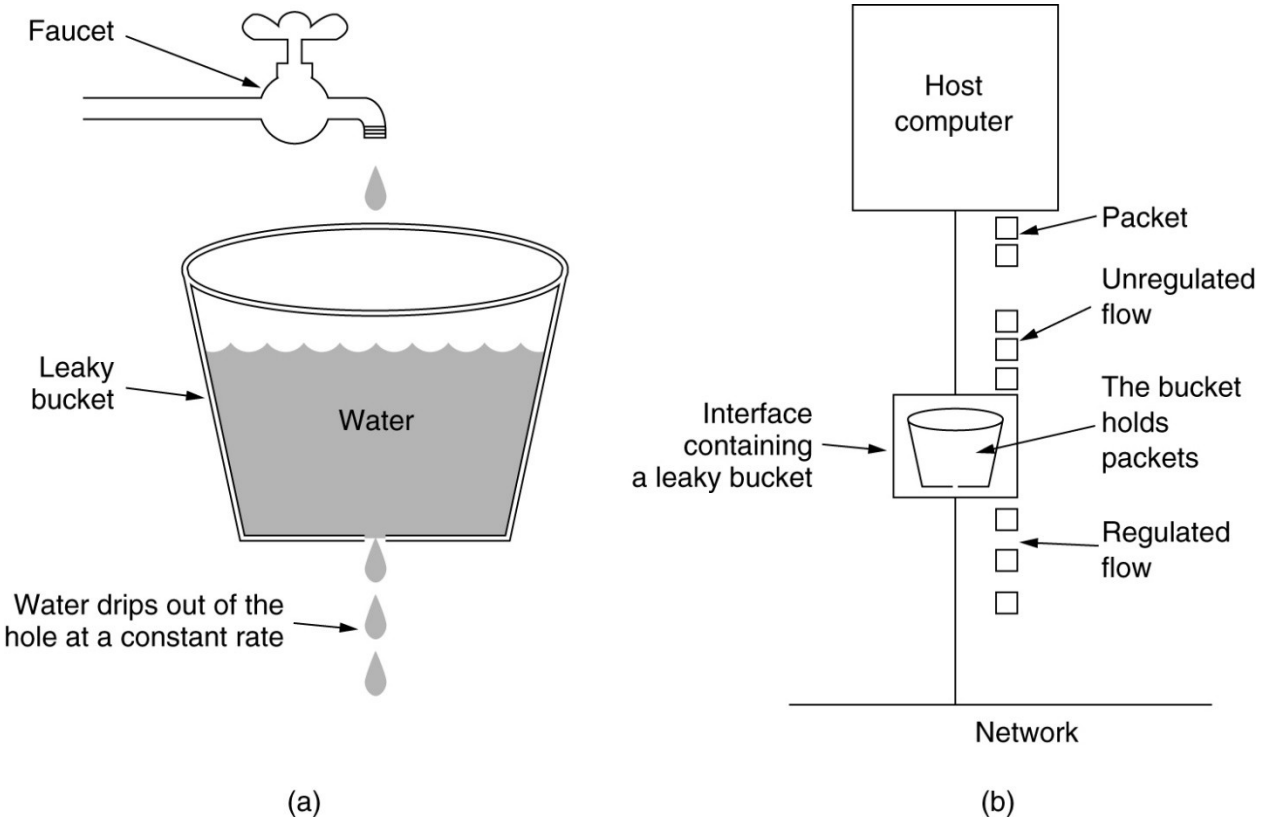
How stringent the quality-of-service requirements are.

Buffering



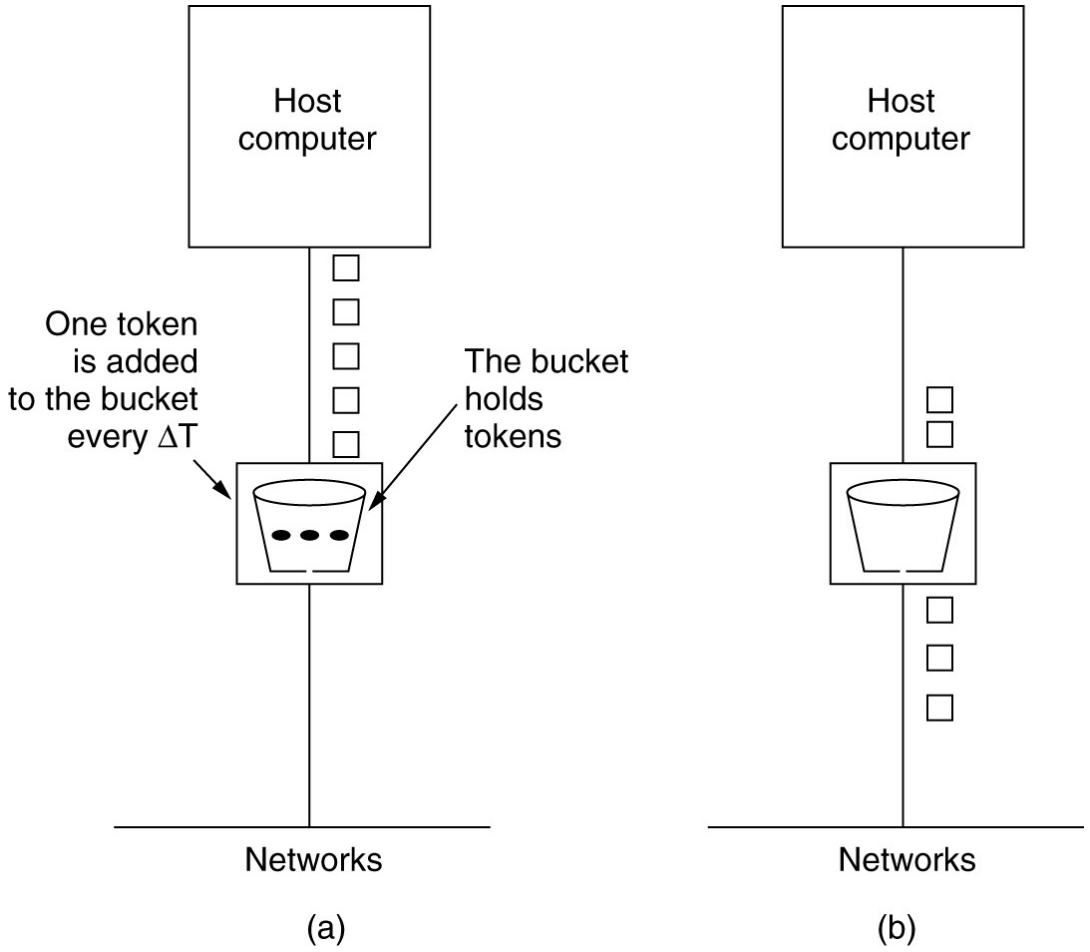
Smoothing the output stream by buffering packets.

The Leaky Bucket Algorithm



(a) A leaky bucket with water. (b) a leaky bucket with packets.

The Token Bucket Algorithm



(a) Before. (b) After.

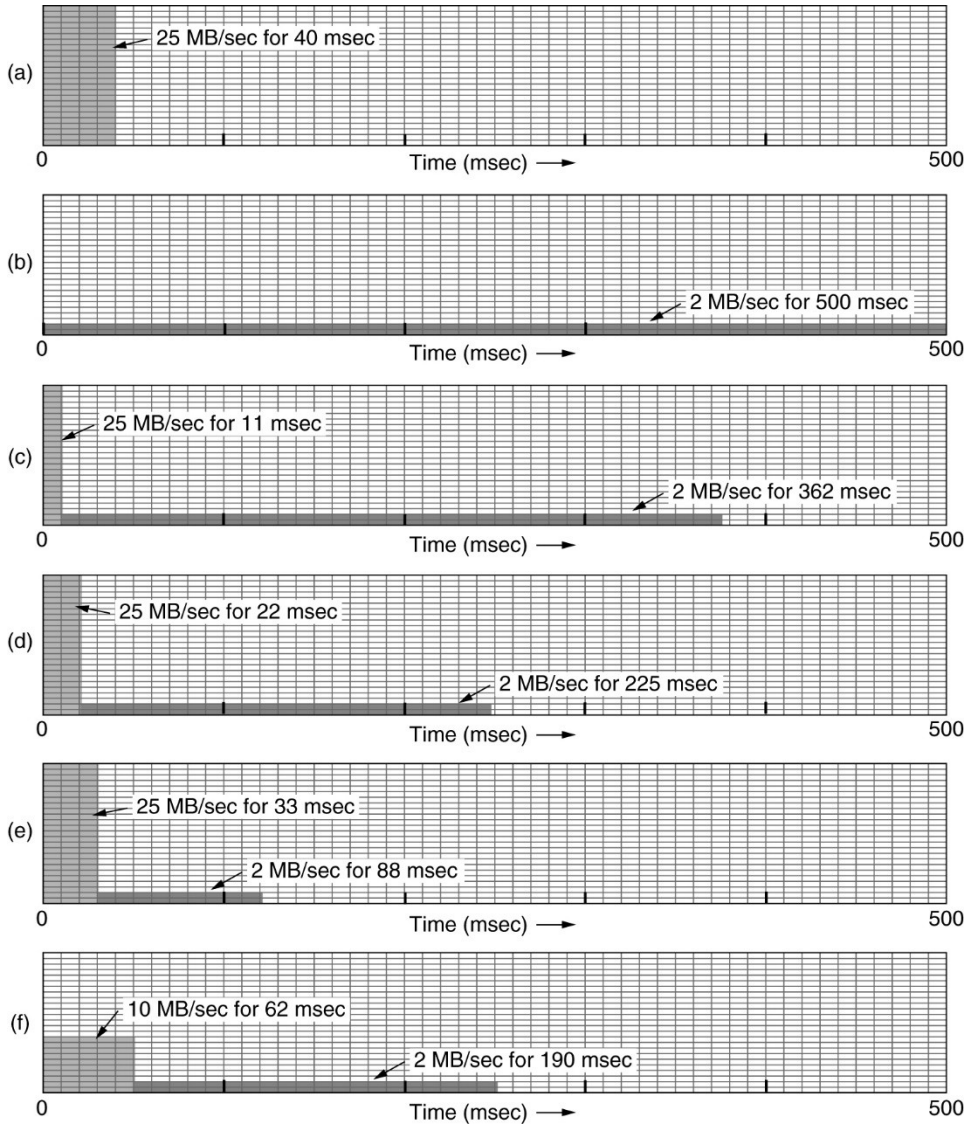
Burst size calculation in token bucket

Calculating the length of the maximum burst (until the bucket empties) is slightly tricky. It is longer than just 9600 KB divided by 125 MB/sec because while the burst is being output, more tokens arrive. If we call the burst length S sec., the maximum output rate M bytes/sec, the token bucket capacity B bytes, and the token arrival rate R bytes/sec, we can see that an output burst contains a maximum of $B + RS$ bytes. We also know that the number of bytes in a maximum-speed burst of length S seconds is MS. Hence, we have

$$B + RS = MS$$

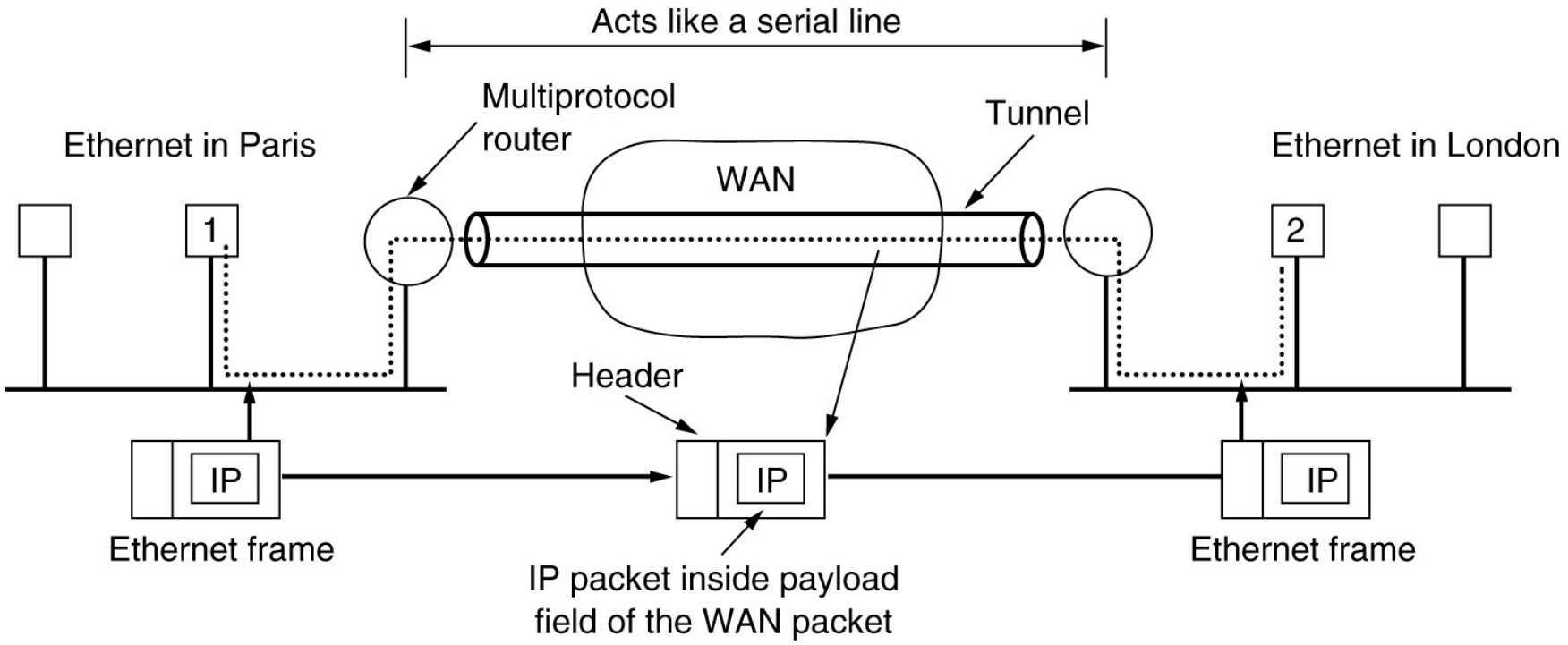
We can solve this equation to get $S = B/(M - R)$. For our parameters of $B = 9600$ KB, $M = 125$ MB/sec, and $R = 25$ MB/sec, we get a burst time of about 94 msec.

The Leaky Bucket Algorithm



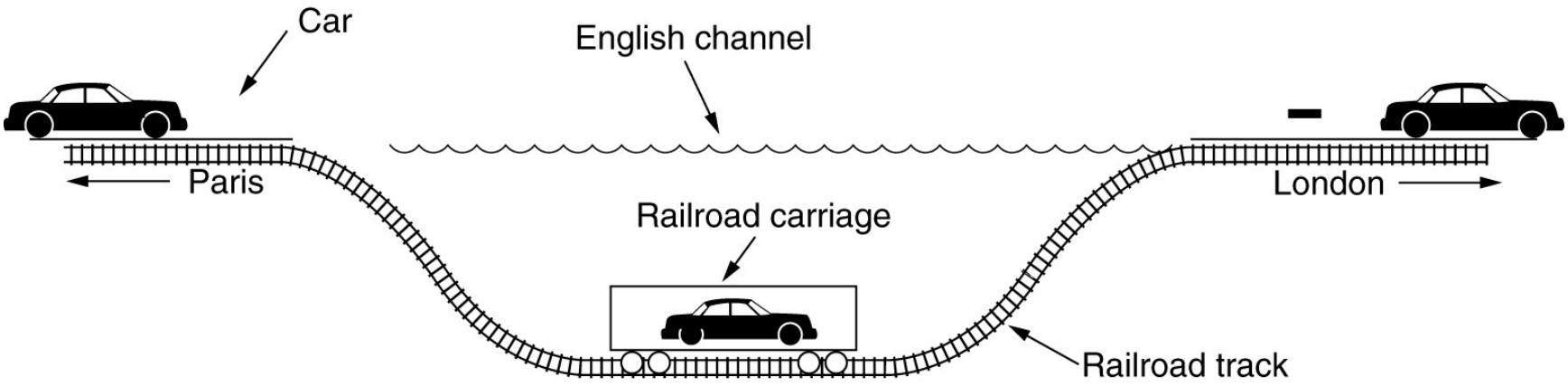
(a) Input to a leaky bucket. (b) Output from a leaky bucket. Output from a token bucket with capacities of (c) 250 KB, (d) 500 KB, (e) 750 KB, (f) Output from a 500KB token bucket feeding a 10-MB/sec leaky bucket.

Tunneling



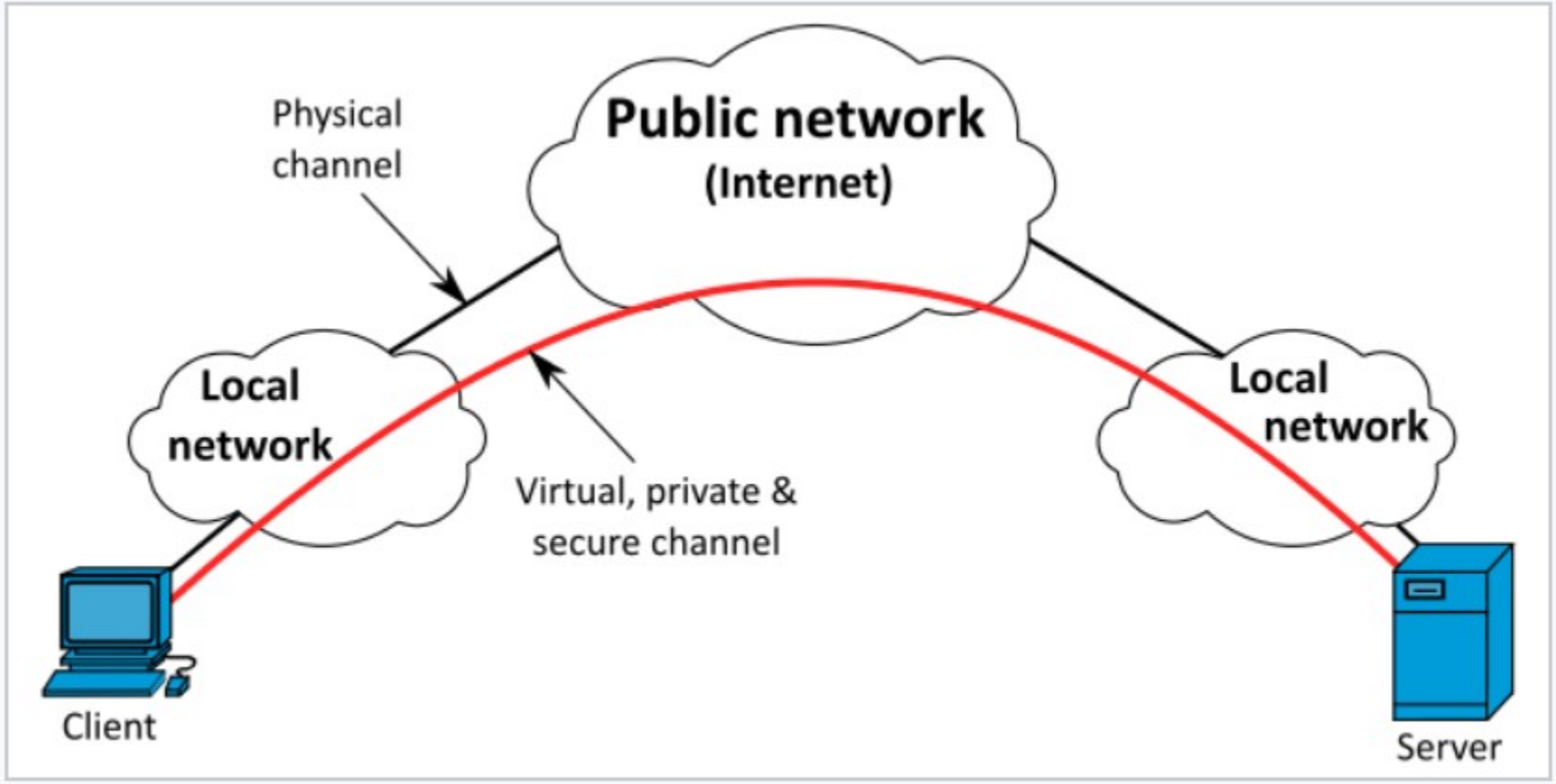
Tunneling a packet from Paris to London.

Tunneling (2)



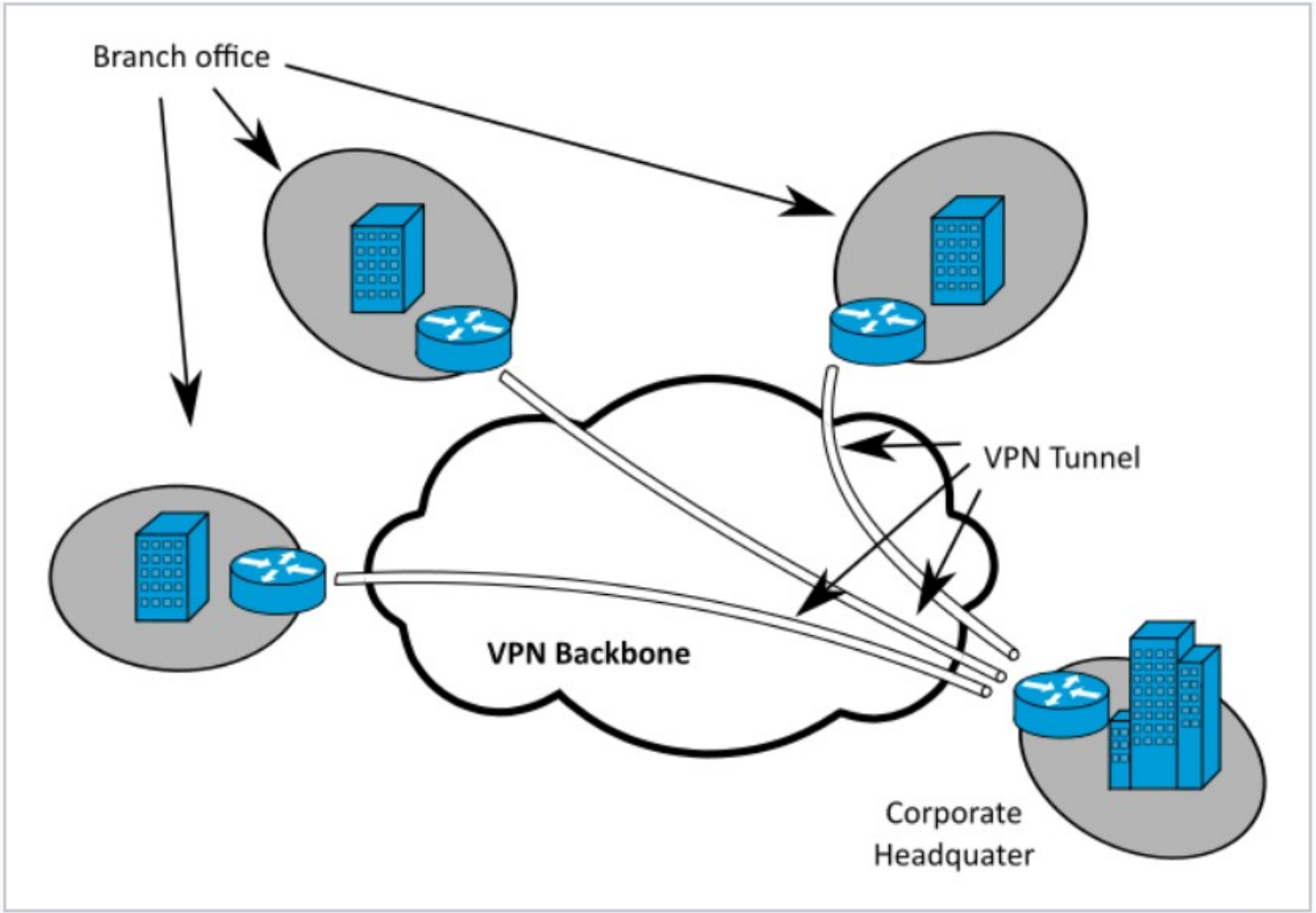
Tunneling a car from France to England.

VPN connectivity



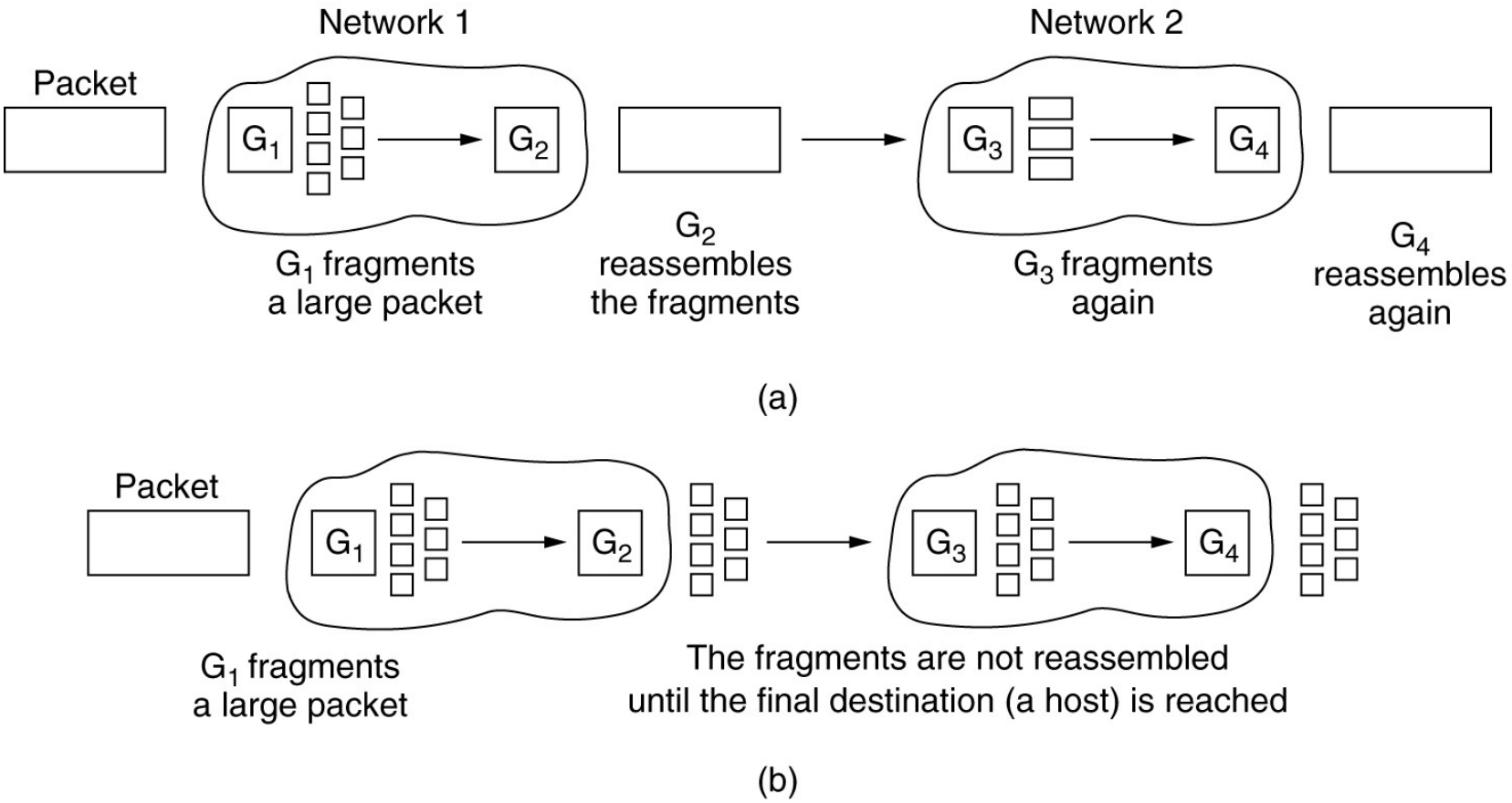
VPN connectivity overview

Site-to-Site VPN



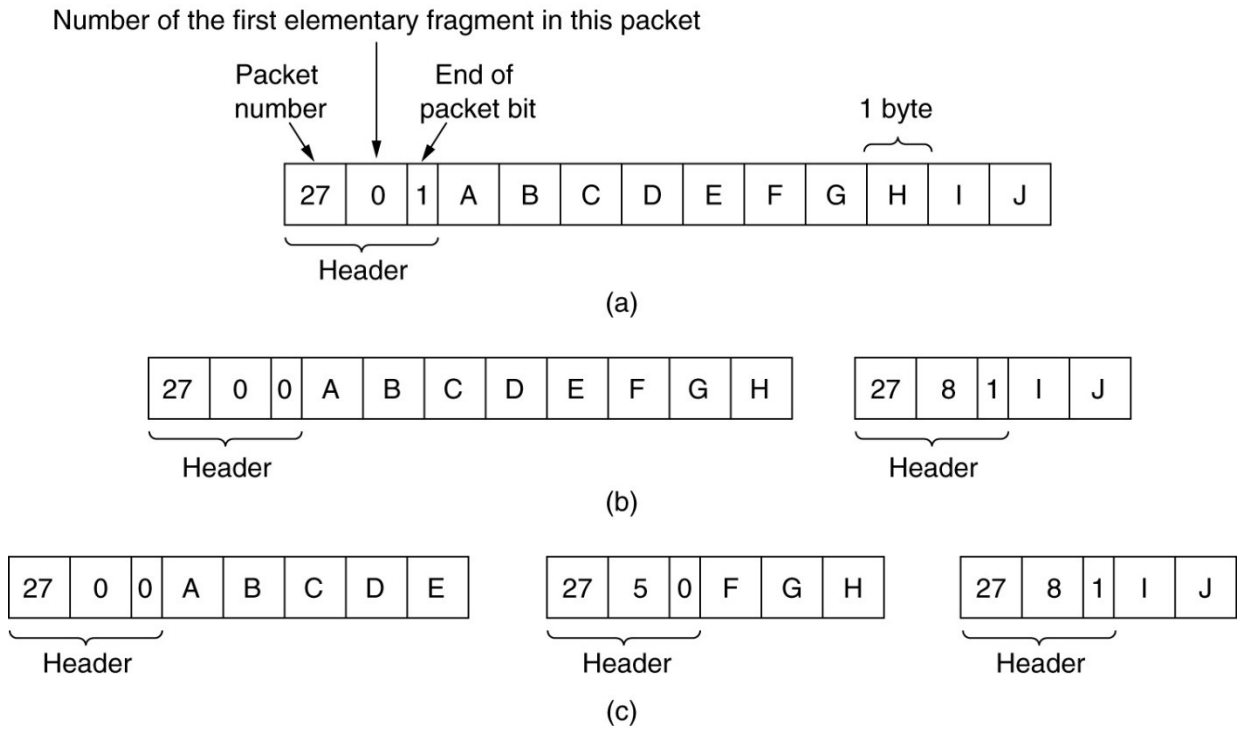
A typical site-to-site VPN.

Fragmentation



(a) Transparent fragmentation. (b) Nontransparent fragmentation.

Fragmentation (2)



Fragmentation when the elementary data size is 1 byte.

(a) Original packet, containing 10 data bytes.

(b) Fragments after passing through a network with maximum packet size of 8 payload bytes plus header.

(c) Fragments after passing through a size 5 gateway.

Internet Control Message Protocol

- Internet Control Message Protocol (ICMP) provides feedback about issues related to the processing of IP packets under certain conditions.
- ICMPv4 is the messaging protocol for IPv4 (supporting it).

- The ICMP messages common to both ICMPv4 and ICMPv6 include:
  - Host reachability
  - Destination or Service Unreachable
  - Time exceeded

ICMP message types

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Ping

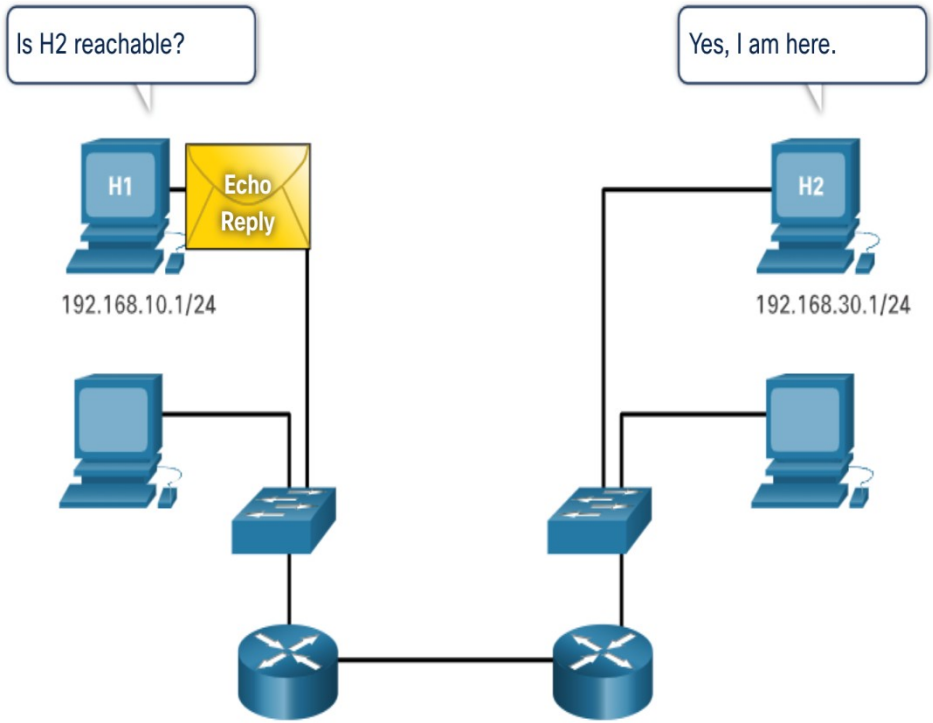
The principal ICMP message types.

Host Reachability

ICMP Echo Message can be used to test the reachability of a host on an IP network.

In the example:

- The local host sends an ICMP Echo Request to a host.
- If the host is available, the destination host responds with an Echo Reply.



Destination or Service Unreachable

- An ICMP Destination Unreachable message can be used to notify the source that a destination or service is unreachable.
- The ICMP message will include a code indicating why the packet could not be delivered.

A few Destination Unreachable codes for ICMPv4 are as follows:

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

Time Exceeded

- When the Time to Live (TTL) field in a packet is decremented to 0, an ICMPv4 Time Exceeded message will be sent to the source host.

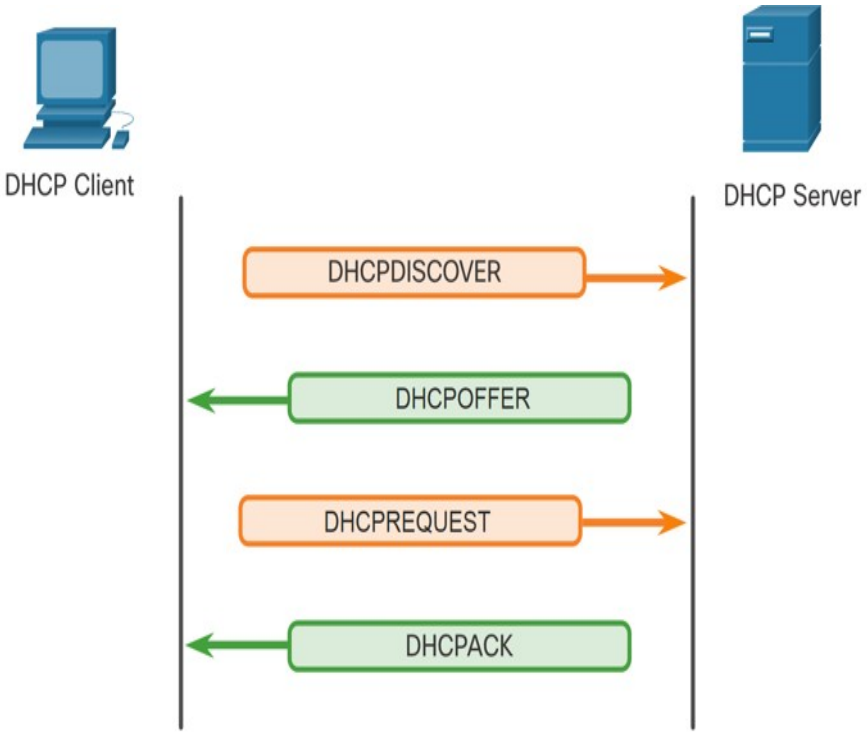
```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

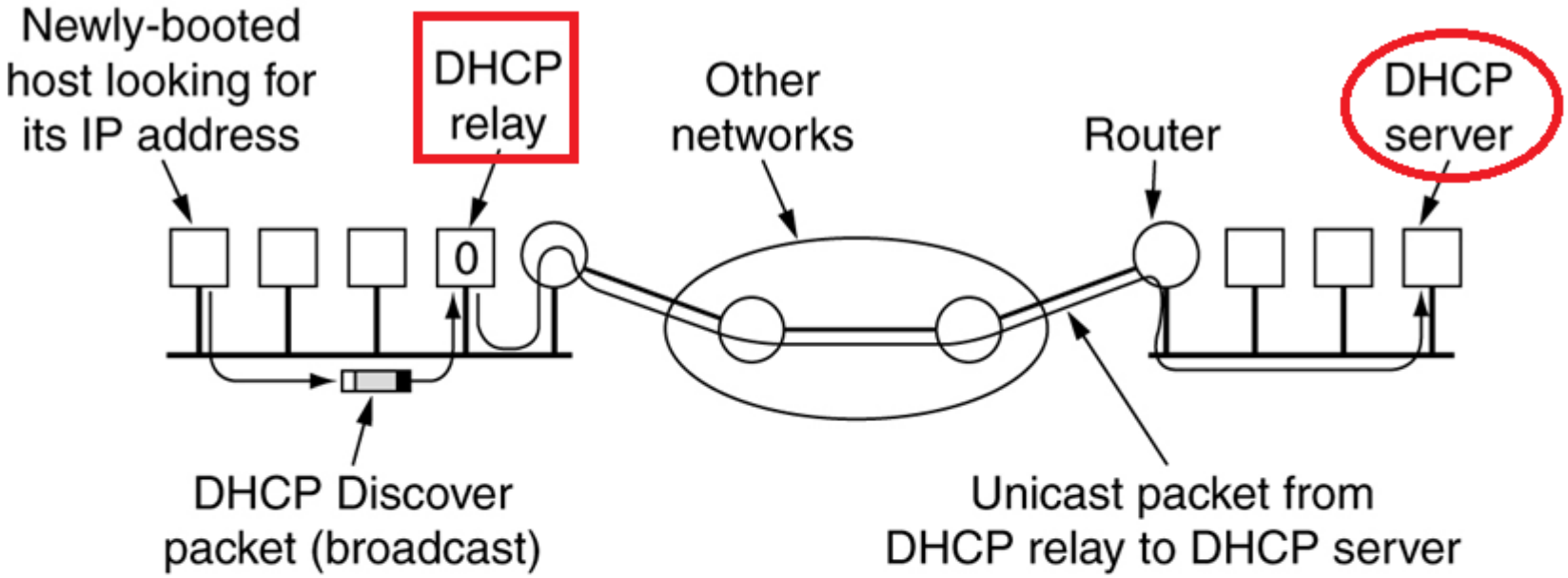
Note: Time Exceeded messages are used by the **traceroute** tool.

DHCP Operation

- When DHCP-configured client boots up, it broadcasts a DHCP discover (DHCPDISCOVER) message to identify any available DHCP servers on the network.
- A DHCP server replies with a DHCP offer (DHCPOFFER) message, which offers a lease to the client. (If a client receives more than one offer due to multiple DHCP servers on the network, it must choose one.)
- The client sends a DHCP request (DHCPREQUEST) message that identifies the explicit server and lease offer that the client is accepting.
- The server then returns a DHCP acknowledgment (DHCPACK) message that acknowledges to the client that the lease has been finalized



DHCP Relay agent



DHCP Relay agent forwards DHCP broadcast msg to DHCP server which is located in another network

DHCP Server reponds with the OFFER msg to the DHCP Relay agent which then forwards it to the DHCP client