CS3200 Computer Networks **Jul - Nov 2019**

Lecture 20: 23 Sep, 2019

Lecturer: Albert Sunny *Scribe: Rajendra Singh*

Anycast Routing

Anycast DNS is a traffic routing algorithm used for the speedy delivery of website content that advertises individual IP addresses on multiple nodes. User requests are directed to specific nodes based on such factors as the capacity and health of your server, as well as the distance between it and the website visitor.

- In anycast, a packet is delivered to the nearest member of a group. Schemes that find these paths are called anycast routing.
- Sometimes nodes provide a service, such as time of day or content distribution for which it is getting the right information all that matters, not the node that is contacted; any node will do. For example, anycast is used in the Internet as part of DNS.
- Suppose we want to anycast to the members of group 1. They will all be given the address "1," instead of different addresses. Distance vector routing will distribute vectors as usual, and nodes will choose the shortest path to destination 1. This will result in nodes sending to the nearest instance of destination 1.

There several advantages to anycast routing, including:

- Faster connections – Routing users through the nearest intermediary node minimizes round-trip time (RTT), thereby decreasing the number of hops and reducing latency.
- Simplified server configuration – Anycast lets a single DNS server configuration be distributed to all of your network nodes.
- High availability – Advertising an IP address on multiple nodes creates redundancy, thereby providing backup in the event a node becomes overloaded or fails.
- DDoS mitigation – Anycast provides intrinsic DDoS mitigation by offering failover alternatives if a node is attacked or goes down.

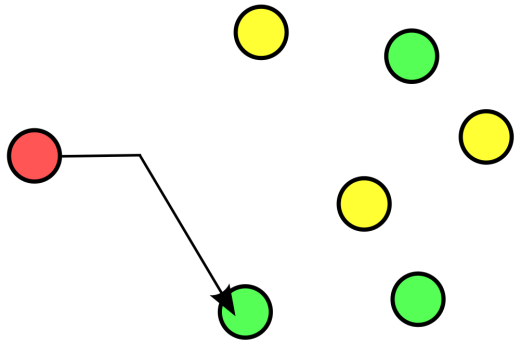

Figure 20.1: Anycast Routing

Routing for Mobile Hosts

Routing to Mobile Hosts (Mobile IP) Mobile IP is the primary mechanism in today's Internet architecture to tackle the problem of routing packets to mobile hosts. It introduces a few new capabilities but does not require any change from non-mobile hosts or most routers—thus making it incrementally deployable.

The mobile host is assumed to have a permanent IP address, called its home address, which has a network prefix equal to that of its home network. This is the address that will be used by other hosts when they initially send packets to the mobile host; because it does not change, it can be used by long-lived applications as the host roams. We can think of this as the long-lived identifier of the host.

When the host moves to a new foreign network away from its home network, it typically acquires a new address on that network using some means such as DHCP. This address is going to change every time the host roams to a new network, so we can think of this as being more like the locator for the host, but it is important to note that the host does not lose its permanent home address when it acquires a new address on the foreign network. This home address is critical to its ability to sustain communications as it moves, as we'll see below.

- Mobile hosts introduce a new complication: to route a packet to a mobile host, the network first has to find it.
- We will assume that all hosts are assumed to have a permanent home location that never changes. Each hosts also has a permanent home address that can be used to determine its home location.
- The routing goal is to make it possible to send packets to mobile hosts using their fixed home addresses and have the packets efficiently reach them wherever they may be.
- A different model would be to recompute routes as the mobile host moves and the topology changes. We could then simply use the routing schemes described earlier in this section. Any issues?
- Another alternative would be to provide mobility above the network layer. When they are moved to new Internet locations, laptops acquire new network addresses. In coming packets would need a higher layer location service. Moreover, connections cannot be maintained while the host is moving.

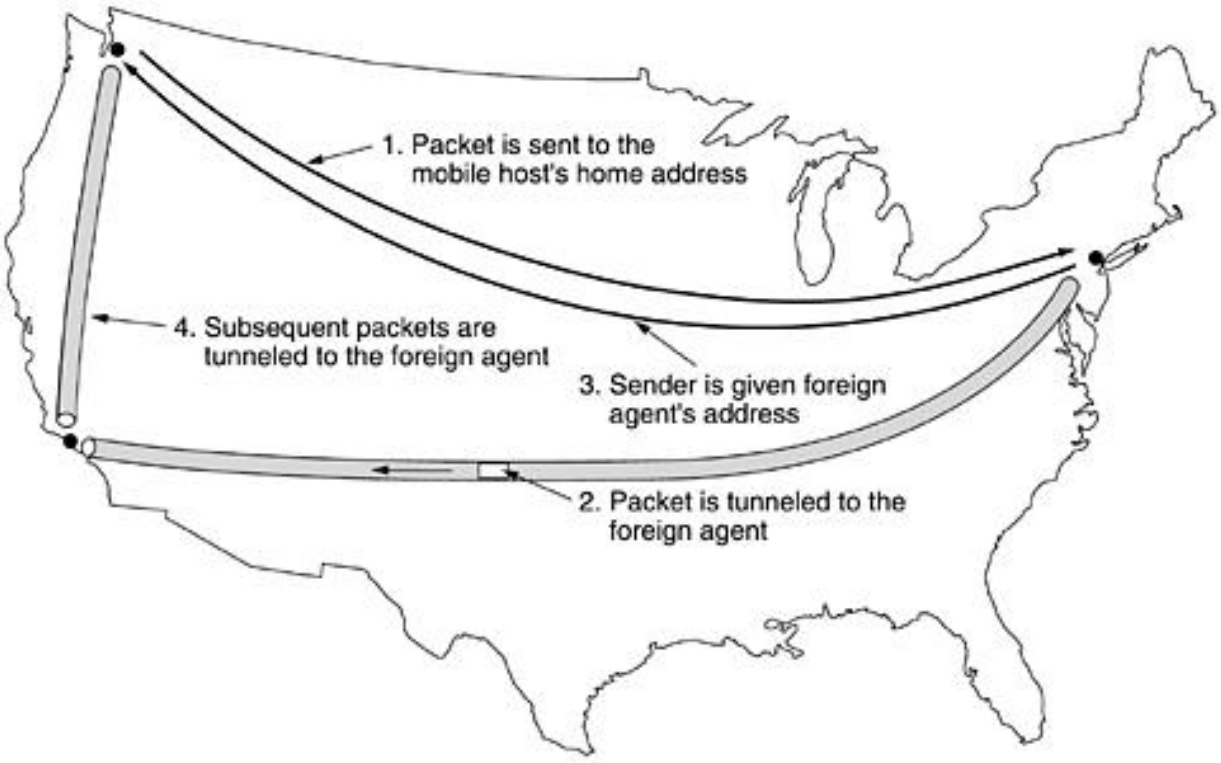

Figure 20.2: Routing for Mobile Hosts

Routing for Adhoc Networks

In adhoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it: typically, a new node announces its presence and listens for announcements broadcast by its neighbors. Each node learns about others nearby and how to reach them, and may announce that it too can reach them. The difficulty of routing may be compounded by the fact that nodes may be mobile, which results in a changing topology.

Adhoc routing protocols fall in two broad categories: proactive and reactive. Proactive or table-driven protocols maintain fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. Reactive or on-demand protocols find a route on demand by flooding the network with Route Request packets.

- We have now seen how to do routing when the hosts are mobile but the routers are fixed.
- Each node communicates wirelessly and acts as both a host and a router. Networks of nodes that just happen to be near each other are called ad hoc networks or MANETs (Mobile Ad hoc NETworks).
- Create multi-hop connectivity among set of wireless, possibly moving, nodes.
- Mobile, wireless hosts act as forwarding nodes as well as end systems
- Need routing protocol to find multi-hop paths

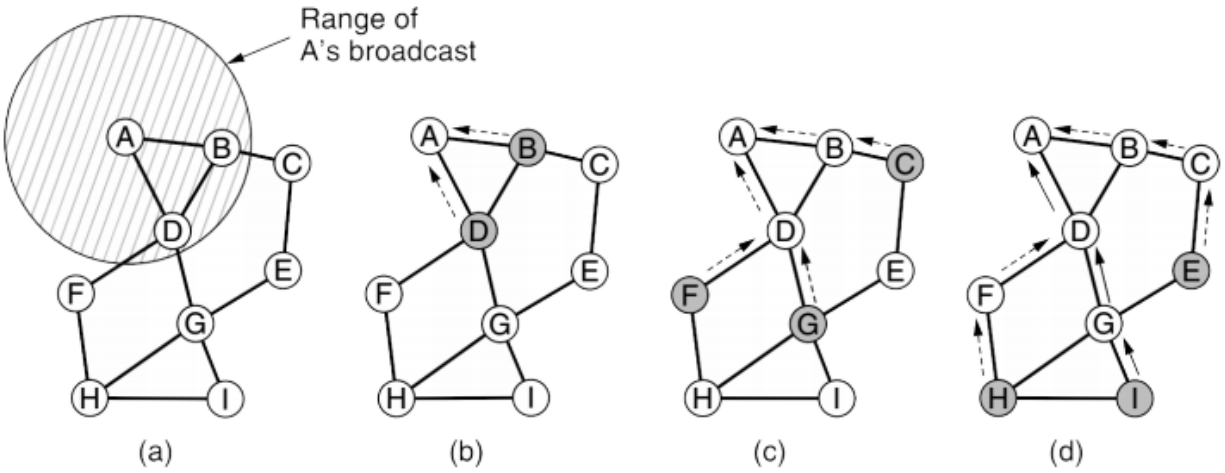

Figure 20.3: Routing for Adhoc Networks

  - Needs to be dynamic to adapt to new routes, movement
  - Interesting challenges related to interference and power limitations
  - Low consumption of memory, bandwidth, power
  - Scalable with numbers of nodes
  - Localized effects of link failure

- AODV(Ad hoc On-demand Distance Vector) (Perkins and Royer, 1999)is a relative of the distance vector algorithm that has been adapted to work in a mobile environment, in which nodes often have limited bandwidth and battery lifetimes.
  Routes to a destination are discovered on demand, that is, only when a somebody wants to send a packet to that destination.

Congestion Control

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network (i.e. the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.). Network congestion occurs in case of traffic overloading.

- Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called congestion. The network and transport layers share the responsibility for handling congestion.

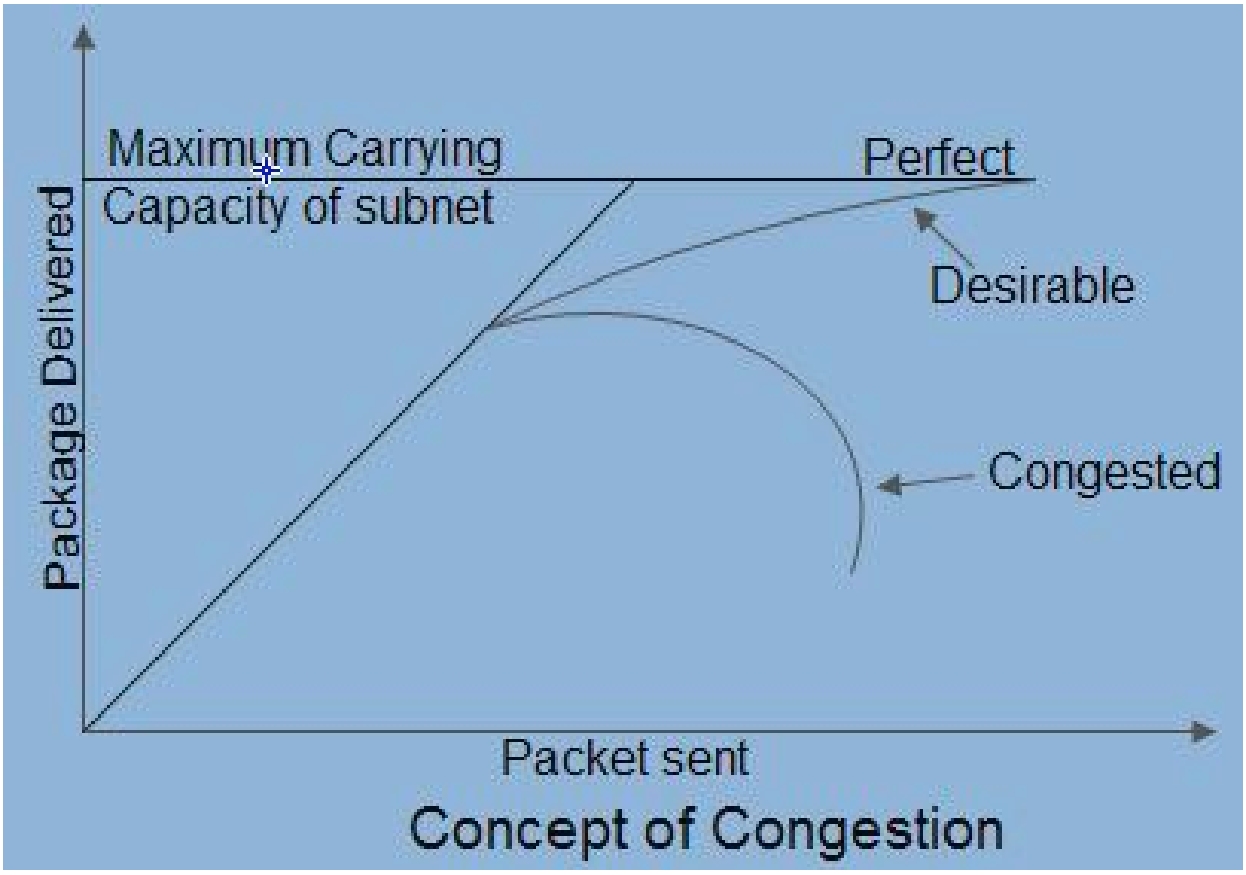

Figure 20.4: Congestion Control

The various causes of congestion in a subnet are:

- The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the problem. This is because, by the time packets reach front of the queue, they have already timed out (as they waited the queue). When timer goes off source transmits duplicate packet that are also added to the queue. Thus same packets are added again and again, increasing the load all the way to the destination.

- The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).

- The routers' buffer is too limited.

- Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.

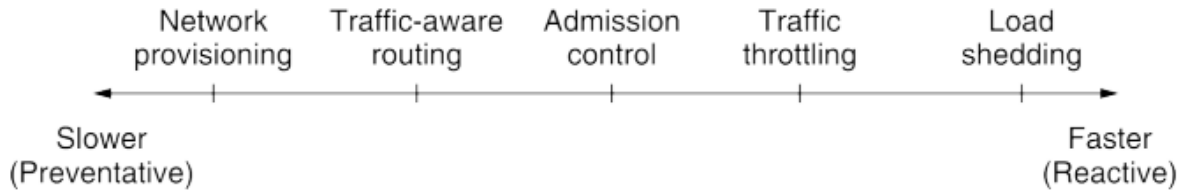

Figure 20.5: Approaches to Congestion Control

Approaches to Congestion Control

- Congestion control has to do with making sure the network is able to carry the offered traffic. It is a global issue, involving the behavior of all the hosts and routers.
- Flow control, in contrast, relates to the traffic between a particular sender and a particular receiver. Its job is to make sure that a fast sender cannot continually transmit data faster than the receiver is able to absorb it.
- End-end congestion control
  - no explicit feedback from network
  - congestion inferred from end-system observed loss, delay
  - approach taken by TCP
- Network-assisted congestion control
  - routers provide feedback to end systems
  - single bit indicating congestion.
  - explicit rate sender should send at

Approaches to Congestion Control: Provisioning

- The most basic way to avoid congestion is to build a network that is well matched to the traffic that it carries.
- If there is a low-bandwidth link on the path along which most traffic is directed, congestion is likely. Sometimes resources can be added dynamically when there is serious congestion, for example, turning on spare routers or enabling lines that are normally used only as backups (to make the system fault tolerant) or purchasing bandwidth on the open market.
- More often, links and routers that are regularly heavily utilized are upgraded at the earliest opportunity. This is called provisioning and happens on a time scale of months, driven by long-term traffic trends.
- It is long term solution to congestion
- It involves :
  - Spare routers
  - Purchase extra bandwidth
  - Allocate resources
- Helps with temporary congestion conditions

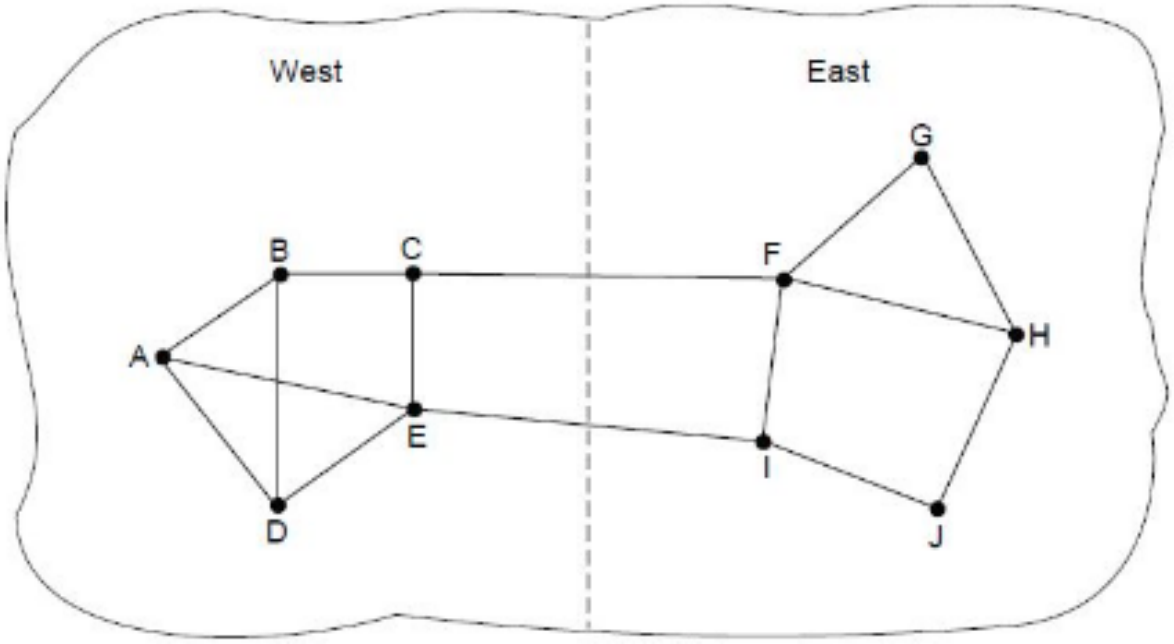

Figure 20.6: Traffic-aware Routing : A Network in which the east and west parts are connected by two links

Approaches to Congestion Control: Traffic-aware Routing

Shifting traffic away from congested regions by setting the link weight to be a function of the link bandwidth and propagation delay plus the (variable) measured load or queuing delay.

- To make the most of the existing network capacity, routes can be tailored to traffic patterns that change during the day as network users wake and sleep in different time zones.
- For example, routes may be changed to shift traffic away from heavily used paths by changing the shortest path weights. This is called traffic-aware routing.
- Splitting traffic across multiple paths is also helpful.
- The goal in taking load into-account when computing routes is to shift traffic away from hotspots.
- Least-weight paths will then favor paths.

References

1. Routing for Mobile Hosts
2. Traffic-aware Routing
3. Ad Hoc Routing
4. Congestion control
5. Approach to Congestion Control
6. Ad Hoc Routing
7. Anycast