Network Layer (II)

Fragmentation Example (cont.)

Fragment	Total bytes	Header bytes	Data bytes	"More fragments" flag	Fragment offset (bytes)
1	2500	20	2480	1	0
2	2040	20	2020	0	310

- Transport layer Packet length 4,500 bytes, MTU 2,500 bytes:
  - 0.
  - 0 + 2480/8 = 310

- Please note that the MTU is not static across the entire network.
- It is possible that the above two fragments reach another router connecting a link with smaller

Fragment	Total bytes	Header bytes	Data bytes	"More fragments" flag	Fragment offset (bytes)
1	1500	20	1480	1	0
2	1020	20	1000	1	185
3	1500	20	1480	1	310
4	560	20	540	0	495

  MTU. Then, the above two fragments will be further fragmented at that router.

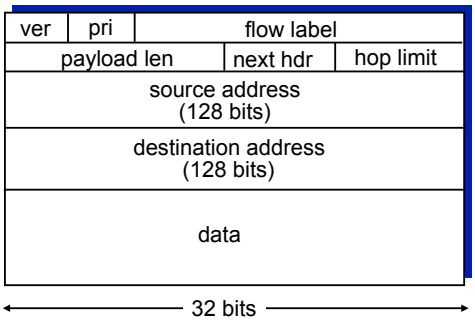
- Suppose the above two fragments reach a router connecting a link with MTU 1,500 bytes. These two fragments will be further fragmented:
  - 0.
  - 0 + 1480/8 = 185
  - 185 + 1000/8 = 310
  - 310 + 1480/8 = 495

IPv6 - Protocol Design

- Keep the good stuff …
  - unreliable datagram service
  - TTL, TOS (for compatibility)
- Eliminate the unnecessary …
  - no fragmentation
    - source hosts can fragment packets using the Fragment extension header; When an IPv6 router encounters a packet larger than the next-hop MTU, it drops the packet and normally sends an ICMPv6 Packet Too Big message.

  - no header checksums
- Address the issues …
  - longer addresses and more

IPv6 Header



- version: 4-bit, 6 indicate v6
- pri: 8-bit traffic class field, like the TOS field in v4, used to give priority to certain datagram
- flow label: 20-bit, identify datagrams in same “flow”
  - concept of “flow” not well defined: audio and video are flow, or file transfer and email are not; it is possible that traffic carried by a high-priority user (someone paying for better service for their traffic) might be also treated as flow.
  - allows packets belonging to a flow to be identified for consistent flow-based handling, such as load balancing.
- payload len: 16-bit integer, number of bytes in the data part (not including the 40-byte header)
- next header: identify upper layer protocol for data (TCP, UDP)
- Discussions
  - Fragmentation: handle by the source and destination, if the router receives a too large packet to be forwarded, it drops the packet, and send a “Packet Too Big” ICMPv6 message.
  - Header checksum: TCP/UDP and link layer protocols have checksum

---

IPv6 Address Representation

- An IPv6 address is represented by 8 groups of 16-bit hexadecimal values separated by colons (:)
- Can be abbreviated:
  - omit leading zeroes in a 16-bit value
  - replace one group of consecutive zeros by a double colon
  - “::” can appear only once in an address
- Example:
  - 2606:4100:38c0:9::5 vs
  - 2606:4100:38c0:0009:0000:0000:0000:0005

- ping IPv6: yingli@davis122-118c8d:~> ping6 fe80::eacf:83ff:fe53:458b%enp128s31f6 (d122-05 pings d122-01)

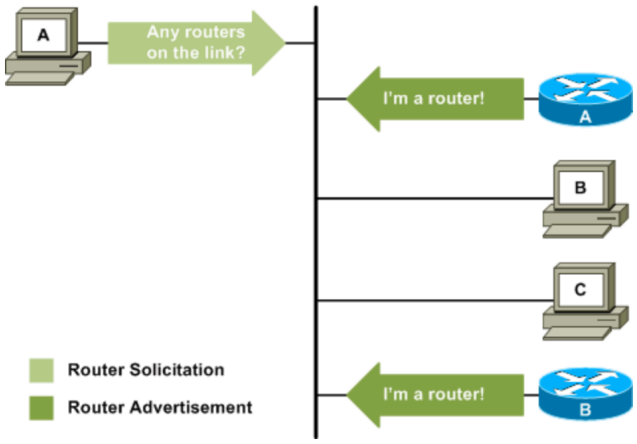
Neighbor Discovery Protocol

- Replaces ARP in IPv6 (multicast vs broadcast): support router discovery, neighbor reachability detection, redirects, and address configuration-related functions.

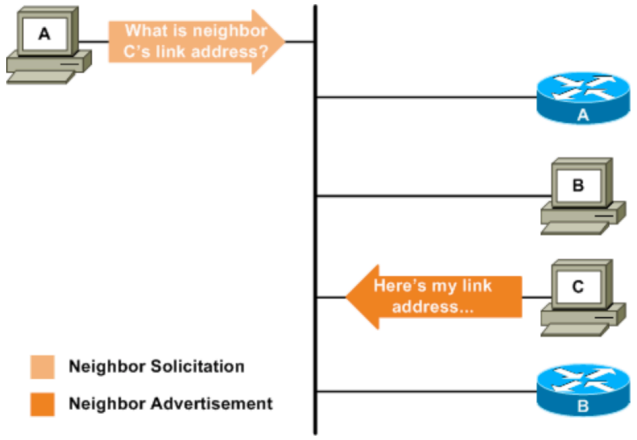
- SLAAC — Stateless Address Auto-configuration: An IPv6 host can use information in Router Advertisements to configure an IPv6 address without necessarily obtaining that address from a DHCP server.
- DAD — Duplicate Address Detection: Before using a newly configured unicast address, a host ordinarily checks whether another device is already using it, using Neighbor Solicitation messages.

- Built into ICMPv6, defines ICMPv6 message
  - Router Solicitation (Type 133)
    - Hosts inquire with Router Solicitation messages to locate routers on an attached link (all routers multicast ff02::2). Routers which forward packets not addressed to them generate Router Advertisements immediately upon receipt of this message rather than at their next scheduled time.
  - Router Advertisement (Type 134)
    - Routers advertise their presence together with various link an Internet parameters either periodically (all nodes multicast ff02::1), or in response to a Router Solicitation message sender. It includes information like available link prefixes, MTU, and etc.
  - Neighbor Solicitation (Type 135)
    - Neighbor solicitations are used by nodes to determine the link layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link layer address.
  - Neighbor Advertisement (Type 136)
    - Neighbor advertisements are used by nodes to respond to a Neighbor Solicitation message.
  - Redirect (Type 137)
    - Router may inform hosts of a better first hop router for a destination.
  - RFC 4861

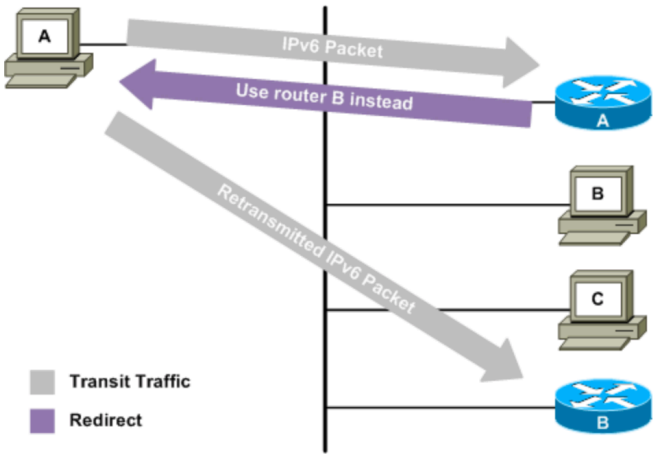
- Router Discovery
  - When first joining a link, an IPv6 host multicasts a router solicitation to the *all routers* multicast group, and each router active on the link responds by sending a router advertisement with its address to the *all nodes* group.



- Address Resolution
  - A host seeking the MAC address of a neighbor multicasts a neighbor solicitation and the neighbor (if online) responds with its link layer address in a neighbor advertisement.



- Redirection
  - Routers uses redirect ICMPv6 message to either point hosts toward a more preferable router, or to indicate that the destination actually resides on link.

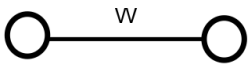


Routing

- Finding a good path from source to destination
  - topology discovery
  - route selection

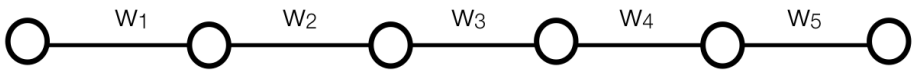
Link Weights

- What is a good measure of “weight” of a link?



  - Link measures:
    - Throughput / bit rate
    - Latency
    - Loss probability

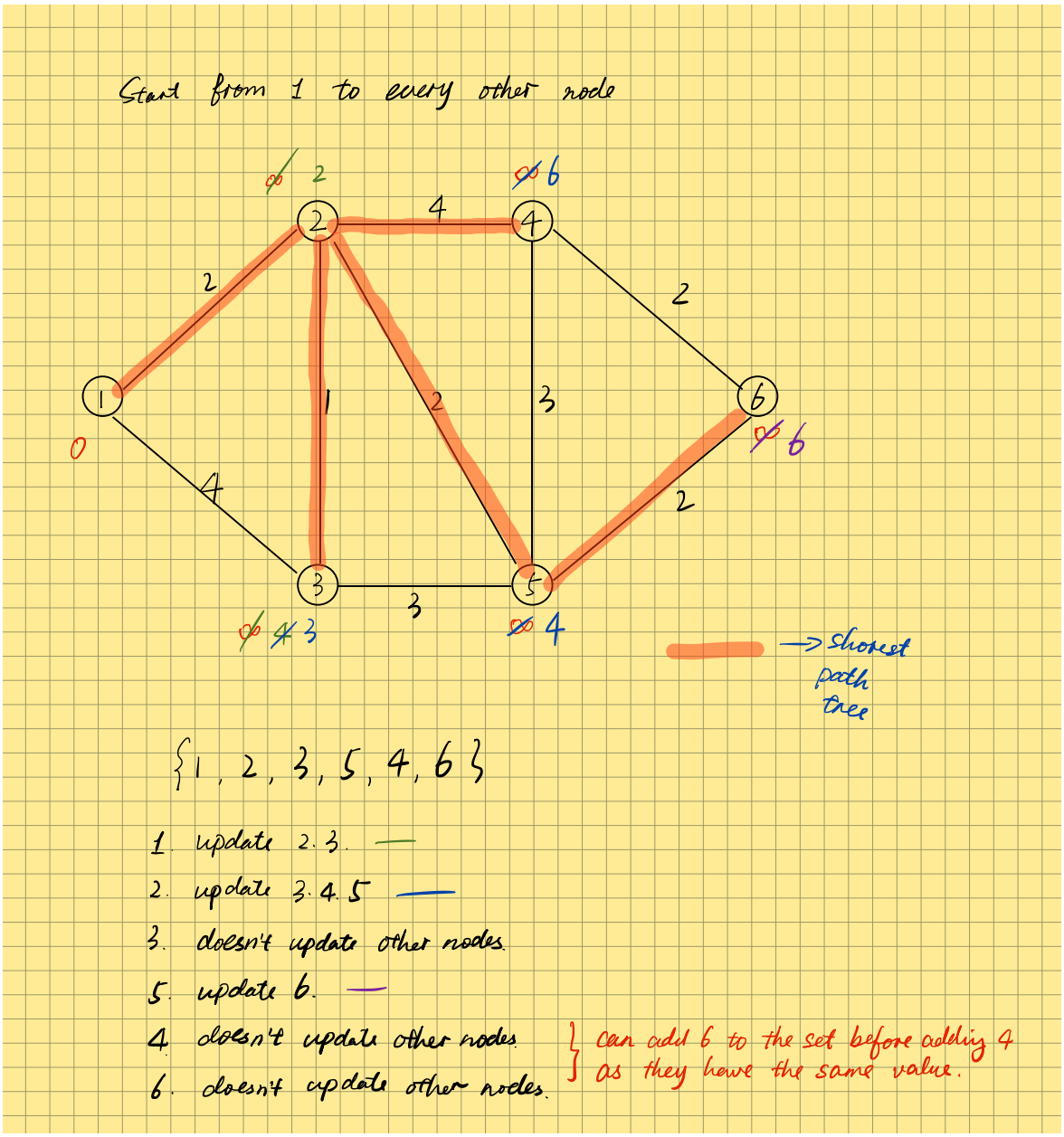
- Weight of a path?



- Path measures:
  - Sum
    - Latency
  - Min/Max
    - Throughput / bit rate
  - Product
    - Loss probability
- The meaning of a link/path cost depends on the routing protocol

Routing Protocols - Categories

- Link State
  - net topology, link costs known to all nodes
  - accomplished via “link state broadcast”
  - all nodes have same info
  - shortest paths calculated and used to populate the routing tables
  - Dijkstra’s algorithm: compute the shortest path from one node to all other nodes
    - It picks the unvisited vertex with the lowest distance, calculates the distance through it to each unlisted neighbor, and updates the neighbor’s distance if smaller.



- Distance Vector: decentralized
  - estimates of distances to all nodes in the network sent to all neighbors
  - estimates are improved based on information from neighbors
  - the process is repeated and routing tables are populated based on the estimates

Disclaimer: Notes adapted from the textbook and online resources.