ICMP

8강

ICMP

- IP protocol number 1

- Formats: Fig. 8-1, 8-2
  - TLV again: type, code, (checksum), payload
    - Type: big classification
    - Code: small classification
  - Checksum is Internet checksum

ICMP usages

- IP datagram delivery failure notification
  - To source
  - Why: should be something that source can correct (otherwise, what’s the point?)

- Probing network state (“informational”)
  - Ping, tracert
  - Round-trip time, loss rate

ICMP usages

- Table 8-1, 8-2
- Some notable ones
  - 3.3, 3.4, 3.5, 5.1, 8.0, 8.1, 11.0

ICMP processing

- Incoming
  - Informational: OS
  - Error: application or transport (TCP)
    - DF error → TCP
    - Redirect → OS : routing table update

ICMP errors

- Explains to source why delivery failed there
- Not generated for
    - ICMP error
    - Bad header (e.g. checksum error)
    - Multicast/broadcast
    - Invalid source addr (e.g. 0.0.0.0)
    - Fragments other than the first

ICMP error

- Carries a copy of the “offending” packet
  - i.e. the dead one
  - IP—ICMP—deadIP

- Dead IP = IP header + some payload
  - Contains transport port number
    - At least 8 bytes of payload, now more
  - Find the culprit (application)!

ICMP redirect

- When there are more than 2 routers on a subnet
  - One is default, the other’s not
  - What happens your packet went to default but should have gone to the other?
    - Redirect!
    - Packet is normally routed, however

Tracert

- Windows uses ICMP Echo Request (8.0)
  - Linux uses UDP
    - With high port numbers likely unused by normal processes
  - What’s good about using ping instead of UDP datagram?
- Try www.monaco.edu from home
  - Not from KU (firewall …)

ICMP query/information msgs

- Echo Request/Reply
- Router Discovery
  - IPv4: rare, used in Mobile IP
  - IPv6: fundamental!   -- ICMPv6
    - Neighbor Discovery (ND)
    - Multicast Listener Discovery (MLD)
      - later
- All others by DCHP today

ping

- Ping: target OS echoes
  - Sequence number
  - Identifier
    - Process ID in Linux

Neighbor Discovery (ND) in IPv6

- ICMPv6 = ICMP Router Discovery + ICMP Redirect + ARP in v4
  - Supports Mobile IPv6

- Allow nodes on the same link
  - Find each other
  - Determine if they have bidirectional connectivity
  - Determine if a neighbor is unavailable
  - Supports stateless address autoconfig

ND

- Two main parts
  - Neighbor Solicitation/Advertisement (NS/NA)
    - ARP, basically
  - Router Solicitation/Advertisement (RS/RA)
    - Router discovery
    - Mobile agents discovery
    - Redirect
    - Autoconfiguration
- Hop Limit = 255

ICMPv6 RS/RA

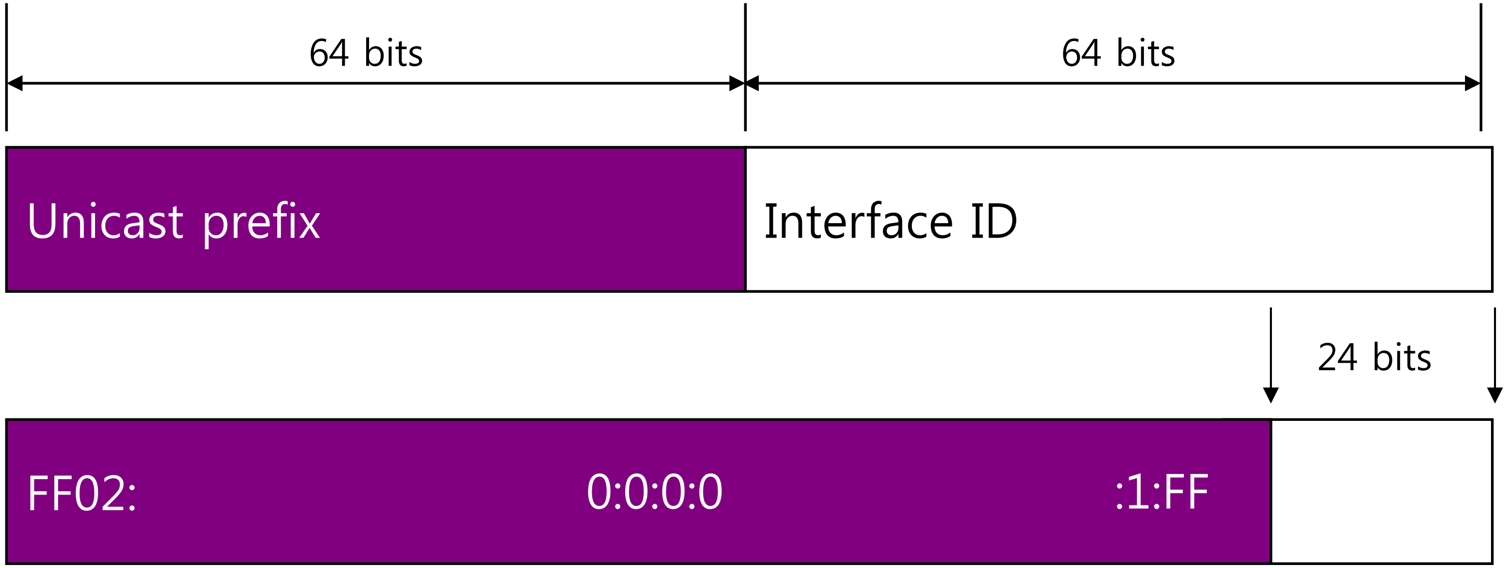
- RA periodically
  - Sent to All Nodes multicast addr = ff02::1
    - Or unicast if in response to RS
- RS induces RA
  - Sent to All Routers multicast addr = ff02::2
  - Flags
    - M: should not use stateless addr autoconfig
    - O: should not use stateless other autoconfig
    - H: willing to act as a HA
    - P: proxy ARP (experimental)

ICMPv6 NS

- Replaces ARP request
  - Sent to Solicited-Node multicast address corresponding to the target IPv6 addr
    - ff02::1:ff/104
- Can also be used for detecting
  - Nearby nodes can be reached
  - If they can be reached bidirectionally
  - Sent to the target unicast address

Solicited-Node multicast

- Acts as a pseudo-unicast address for efficient address resolution
  - Fe80::210:18ff:fe00:100b → ff02::1:ff00:100b



ICMPv6 NA

- Replaces ARP response
  - In response to NS
  - Asynchronously when IPv6 addr changes
    - Not a request!
  - Flags
    - R: I am a router
    - S: in response to a NS → bidirectional connectivity!
    - O: override cache