# 523454

# Computer Network Programming

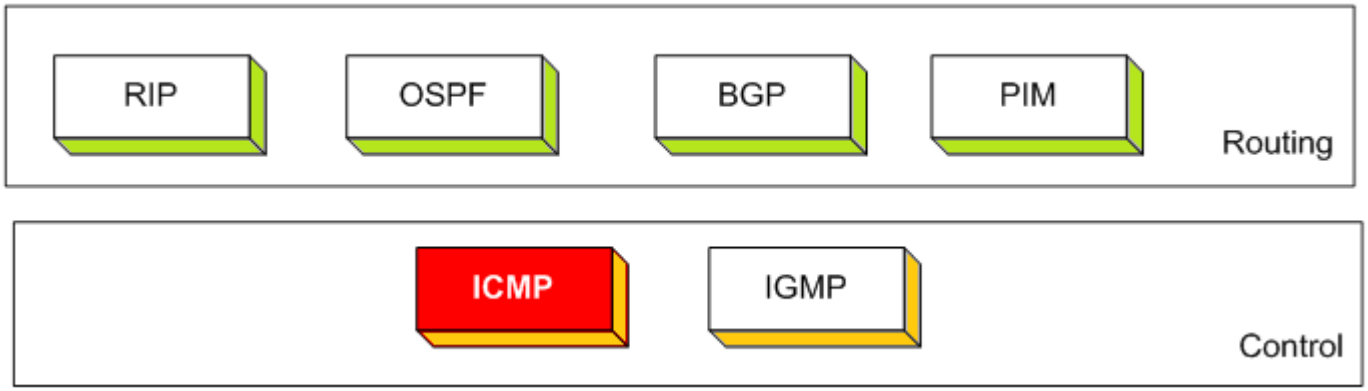
## Lecture 3: ICMPv4 and ICMPv6

Dr. Parin Sornlertlamvanich,

parin.s@sut.ac.th

# Overview

- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
  - Control functions (ICMP)
  - Multicast signaling (IGMP)
  - Setting up routing tables

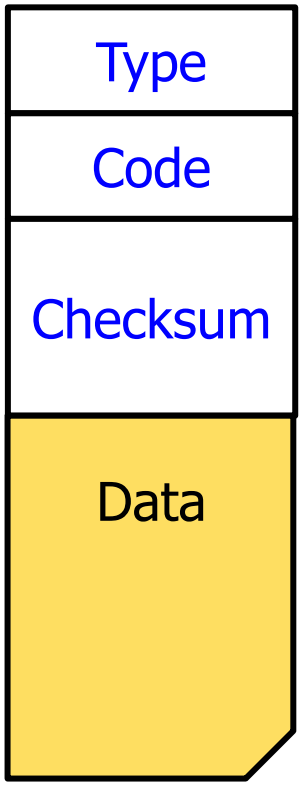


# Internet Control Message Protocol

- ICMP and Internet Protocol (IP)
  - Network layer - There is no TCP or UDP port number associated with ICMP packets
- The Internet Control Message Protocol (ICMP) is a helper protocol that supports IP with facility for
  - Error reporting
  - Simple queries
- 3 ICMP message types
  - Requests
  - Replies
  - Error Reports

# ICMP format

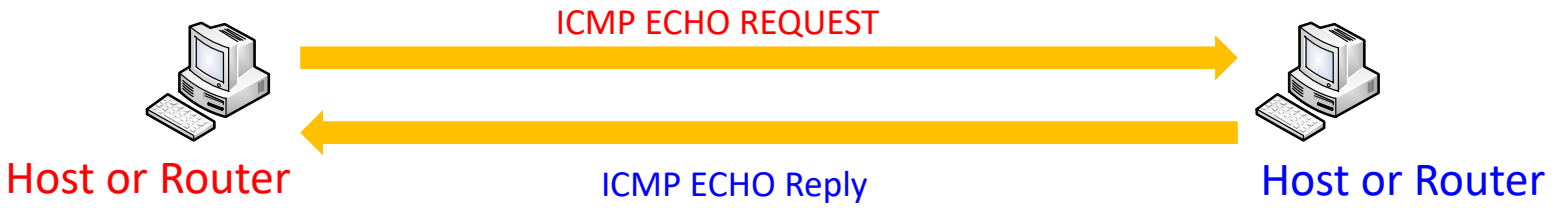
- Type (1 byte)
  - Echo request
    - Request to return data
  - Echo reply
    - Reply to earlier echo
- Code (1 byte)
  - Minor variations of type
- Checksum (2 bytes)
  - Checksum is calculated over entire ICMP message
  - If there is no additional data, there are 4 bytes set to zero
  - at least 8 bytes long




Type 0 = Echo Reply
Type 8 = Echo Request

# Echo Request and Reply

- Ping's are handled directly by the kernel
- Each Ping is translated into an ICMP Echo Request
- The Host responds with an ICMP Echo Reply

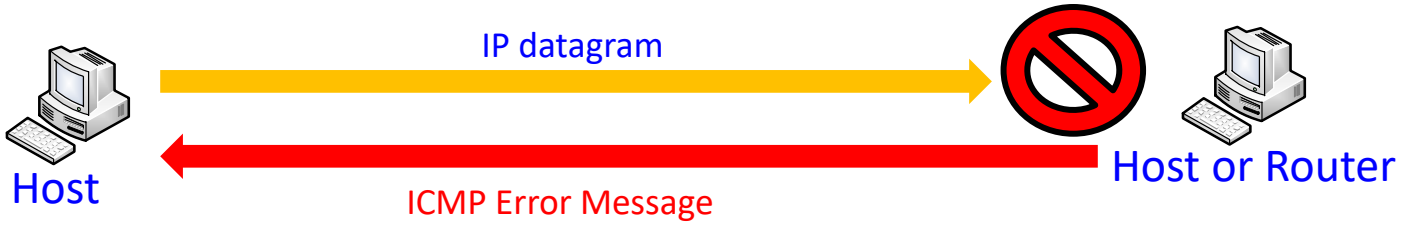


# ICMP Echo

- Data can be anything
- Same Data returned in ICMP Echo Reply

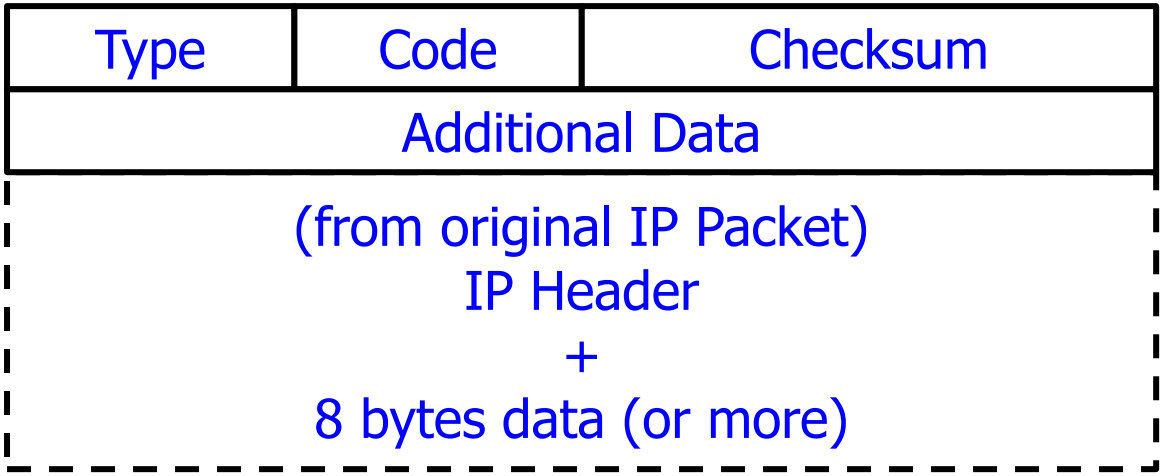
```
02:27:06.105890  192.168.192.23 > 192.168.192.22: icmp: echo request seq 0
        4500 0054 3e8d 0000 ff01 7b9c c0a8 c017
        c0a8 c016 0800 b620 0642 0000 0abe 0d3f
        379d 0100 0809 0a0b 0c0d 0e0f 1011 1213
        1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
        2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
        3435 3637
02:27:06.106051  192.168.192.22 > 192.168.192.23: icmp: echo reply seq 0
        4500 0054 86dc 0000 ff01 334d c0a8 c016
        c0a8 c017 0000 be20 0642 0000 0abe 0d3f
        379d 0100 0809 0a0b 0c0d 0e0f 1011 1213
        1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
        2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
        3435 3637
```

# ICMP Errors



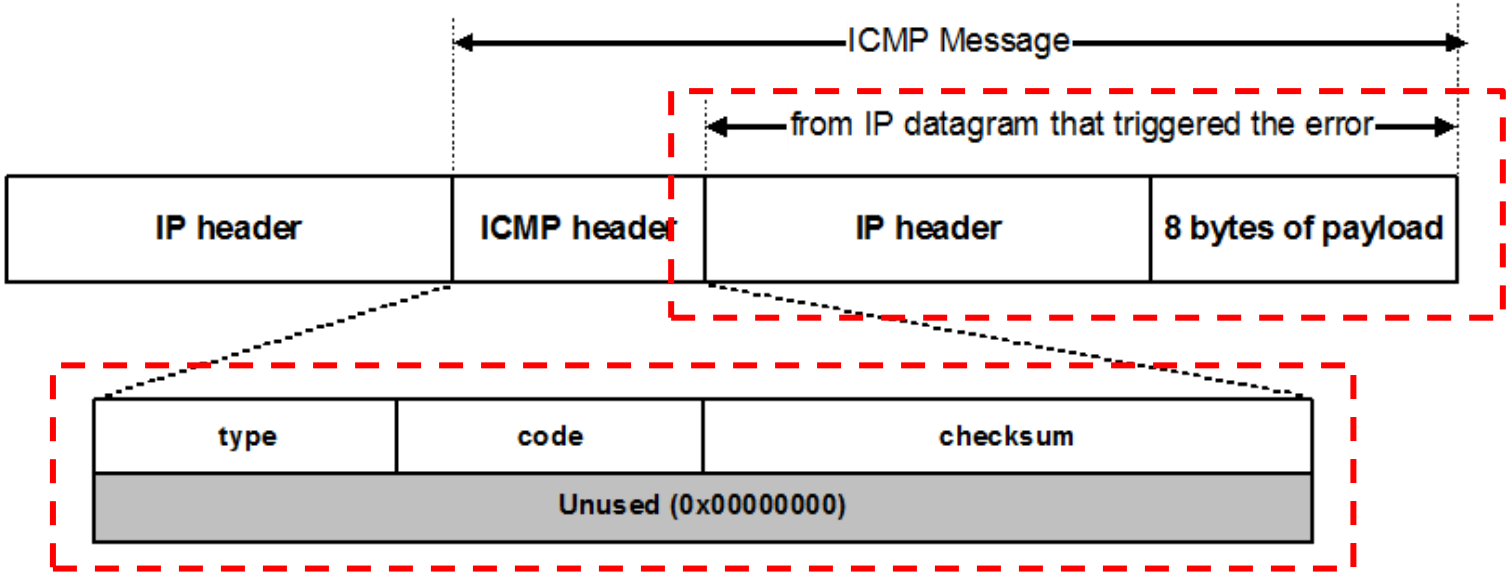

- ICMP error messages report error conditions
- Typically sent when a datagram is discarded
- Error message is often passed from ICMP to the application program

# ICMP Errors




- Additional Data
  - Sometimes indicates where error occurred
- Original Packet
  - Allows source to recognize
    - which packet had problem
  - 8 data bytes (64 bits) is usually transport header
    - or part of it

# ICMP Errors

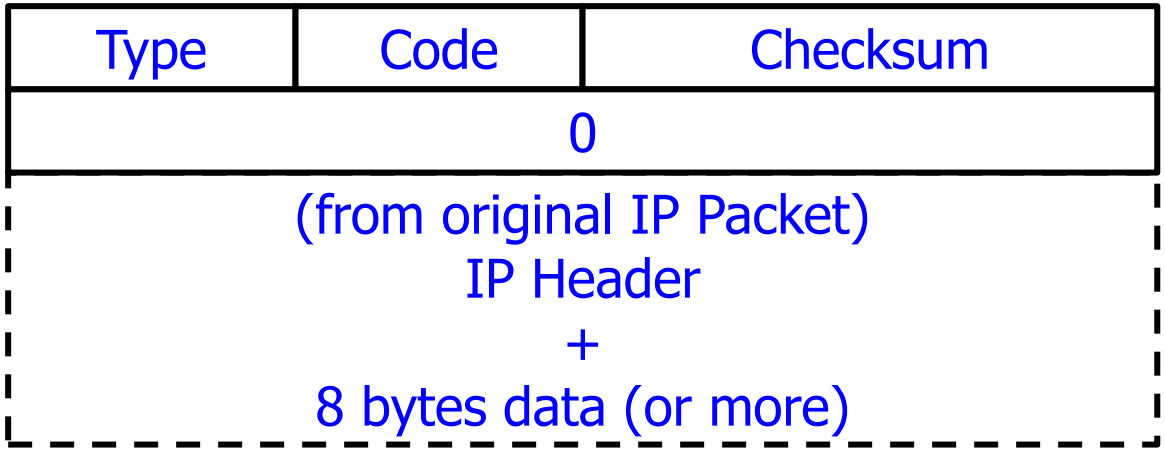



- ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP)

# ICMP Errors

| Type | Code | Description | |
|---|---|---|---|
| 3 | 0–15 | Destination unreachable | Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation. |
| 5 | 0–3 | Redirect | Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change. |
| 11 | 0, 1 | Time exceeded | Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1) |
| 12 | 0, 1 | Parameter problem | Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1) |

# ICMP Unreachable




- Packet could not be delivered
- No additional data
  - Except modern Fragmentation

    Required: MTU
- Code: Why...

| | | |
|---|---|---|
| Network | Host | Protocol |
| Port | Need to Fragment | Source Route Fail |
| Net Unknown | Host Unknown | Source Isolated |
| Net Prohibited | Host Prohibited | Bad TOS (Net) |
| Bad TOS (Host) | Admin Prohibit | |

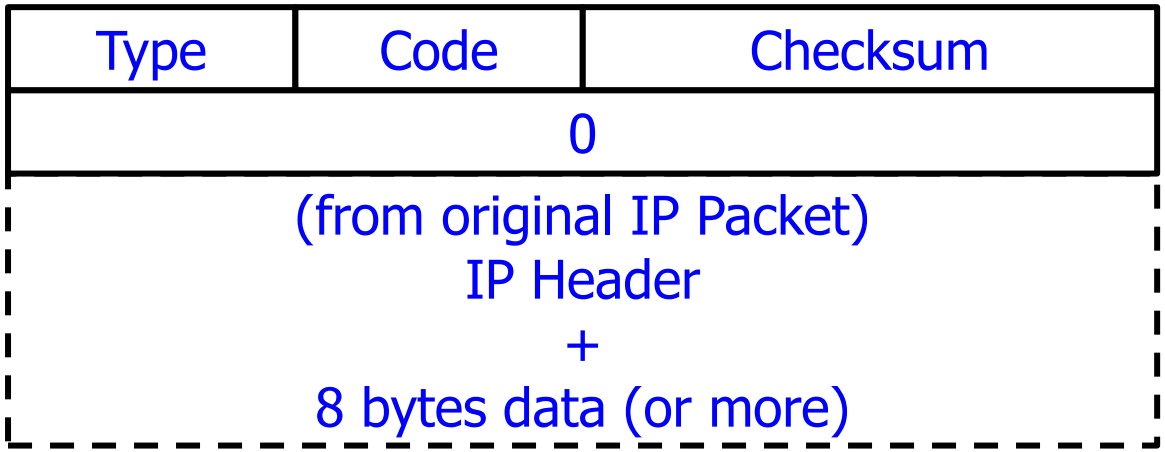
# Codes of the “Destination Unreachable

| Code | Description | Reason for Sending |
|---|---|---|
| 0 | Network Unreachable | No routing table entry is available for the destination network. |
| 1 | Host Unreachable | Destination host should be directly reachable, but does not respond to ARP Requests. |
| 2 | Protocol Unreachable | The protocol in the protocol field of the IP header is not supported at the destination. |
| 3 | Port Unreachable | The transport protocol at the destination host cannot pass the datagram to an application. |
| 4 | Fragmentation Needed and DF Bit Set | IP datagram must be fragmented, but the DF bit in the IP header is set. |

When you try to ping

- Request time out: this error message indicates that your host did not receive the ping message back from the destination device within the designated time period

# ICMP Time Exceeded




- TTL decremented to 0
- Code 0
  - In Transit
    - while being forwarded
- Code 1
  - In reassembly queue
  - waiting for later fragments to arrive

# ICMPv6

- RFC 4443
  - Internet Control Message Protocol v6
  - Implementation required in all IPv6 nodes

- What is it used for?
  - Report errors
  - Report network status
  - Neighbor discovery

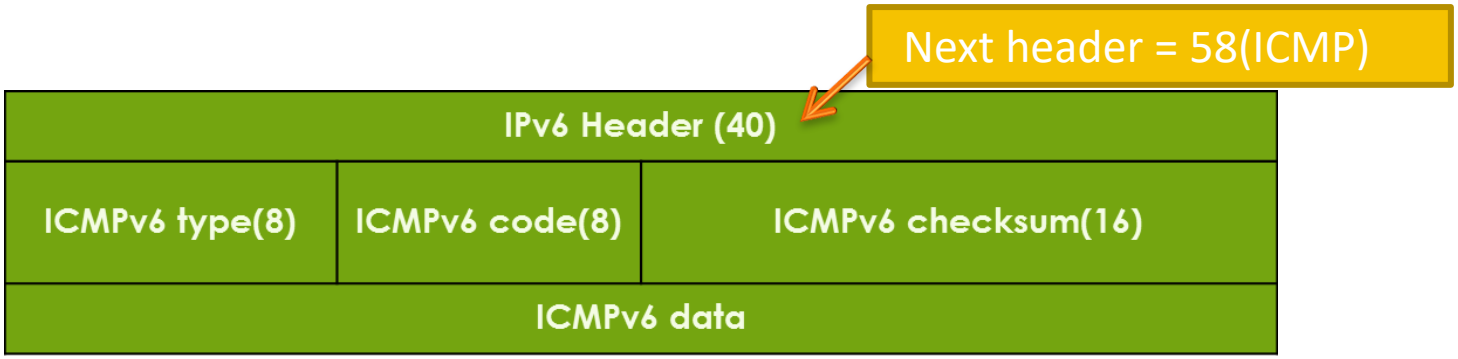
# ICMPv6 (cont.)

- ICMPv6 is more powerful than ICMPv4
  - Can manage multicast group membership (IGMP)
  - Can determine link-layer address of neighbors
  - Can detect neighbor reachability
  - Can find router
  - Support mobile IPv6

# ICMPv6 (cont.)

- Two classes of ICMP messages
  - Error messages
    - Destination unreachable
    - Packet too big
    - Time exceeded (Hop Limit field becomes zero)
    - Parameter problem (Error in IPv6 Header)
  - Informational messages
    - Echo request
    - Echo reply
    - Etc.

# ICMPv6 Packet Format




- Just the same as ICMP (for IPv4)

# ICMPv6 principal types and codes

| | Type | Meaning | Code | Code explanation |
|---|---|---|---|---|
| Errors | 1 | Destination Unreachable | 0 | No route to destination |
| | | | 1 | Administratively prohibited |
| | | | 2 | Out of scope |
| | | | 3 | Address unreachable |
| | | | 4 | Port unreachable |
| | 2 | Packet Too Big | | |
| | 3 | Time Exceeded | 0 | Hop limit exceeded |
| | | | 1 | Fragment reassembly time exceeded |
| | 4 | Parameter Problem | 0 | Erroneous header field |
| | | | 1 | Unrecognized next header type |
| | | | 2 | Unrecognized IPv6 option |
| Informational | 128 | Echo Request | | |
| | 129 | Echo Reply | | |
| | 130 | Multicast Listener Query | | |
| | 131 | Multicast Listener Report | | |
| | 132 | Multicast Listener Done | | |
| Neighbor Discovery | 133 | Router Solicitation | | |
| | 134 | Router Advertisement | | |
| | 135 | Neighbor Solicitation | | |
| | 136 | Neighbor Advertisement | | |
| | 137 | Redirect | | |

# ICMPv6 Error messages

- Destination Unreachable — Type 1
- Packet Too Big — Type 2
- Time Exceeded — Type 3
- Parameter Problem — Type 4

- Deleted
  - Source Quench
- Moved to Informational
  - Redirect

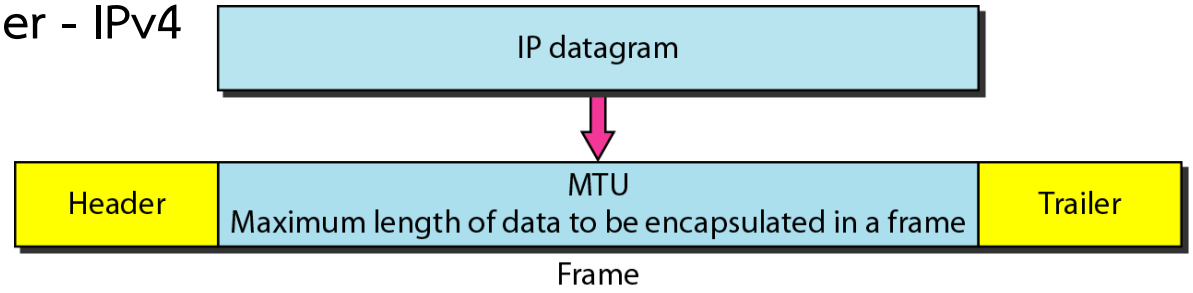
# ICMPv6 Unreachable

- Same format as for IPv4
  - Except more of failed packet expected to be included

- Only 5 codes
  - No Route (0)
  - Communication Admin Prohibited (1)
  - Going Out of Scope (2)
  - Address Unreachable (3)
  - Port Unreachable

# Why Fragmentation

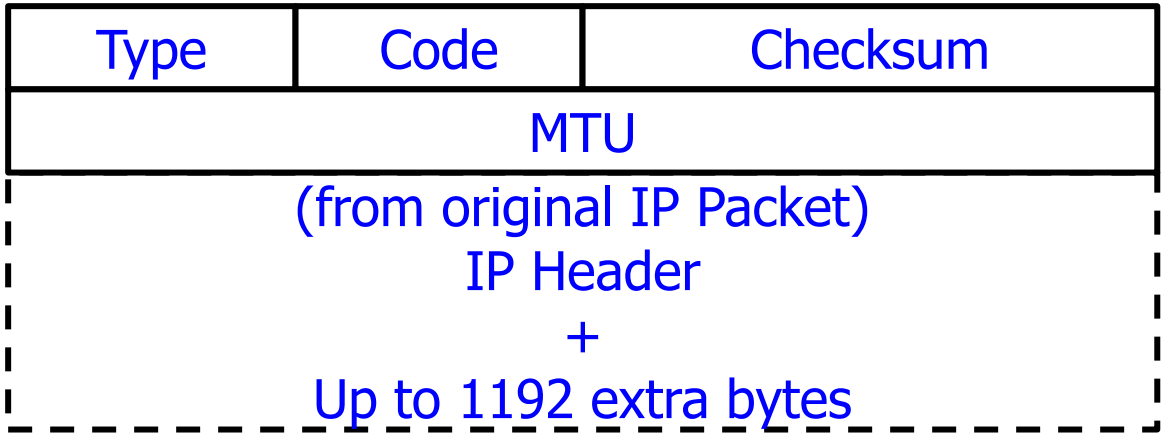
- Packets can be big
  - 65535 bytes
    - including header - IPv4




- Links usually have Maximum Transfer Unit (MTU)
  - Maximum Transmission Unit
  - Limit on maximum packet size
    - Ethernet 1500 (+ Ethernet headers)

- Packet might be bigger than MTU
  - What to do?

# ICMPv6 Packet Too Big



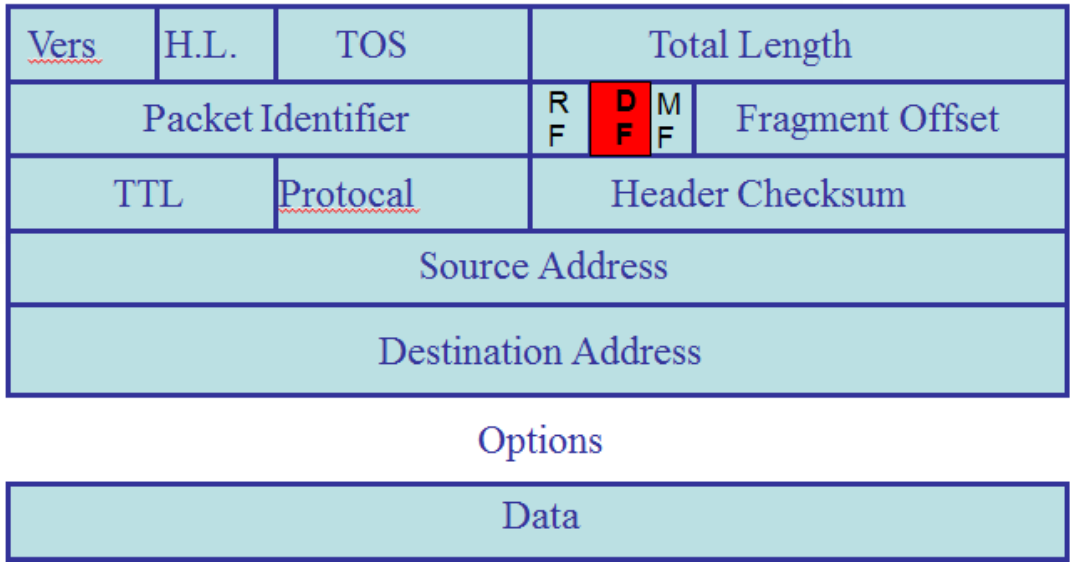

- Replaces IPv4 Unreachable: Need Fragmentation
- MTU specifies the MTU that was too small for packet
  - Allows PMTU Discovery
- Separate code from Unreachable
  - allows unreachable to be blocked
  - still allow "too big" to be received

# Path MTU Discovery (PMTUD)

- Path MTU Discovery
  - Search for the minimum link MTU for all links between source and destination (bottleneck)
  - Used in IPv6 because IPv6 does not allow fragmentation at transit routers
    - Only allow fragmentation at source
  - No path MTU discovery mechanism in IPv4
    - Just fragment packets along the way
  - Not required mechanism
  - Implementation is vendor-specific

# PMTUD (cont.)

- Sending Host discovers the minimum MTU
  - of the Path used
  - and then sends its packets
  - no bigger than that



# PMTUD (cont.)

- If a packet arrives at a router
  - The DF bit is set in the header
  - If fragmentation is required to send the packet

- Router discards the packet
  - Sends ICMP "packet too big and DF set" to source
    - Includes the MTU of the link to be used
    - Source host knows MTU of this link
      - smallest link so far

# ICMPv6 Errors Concluded

- Time Exceeded
  - Identical to IPv4 ICMP (with more data)

- Parameter Problem
  - Similar to IPv4 parameter problem
    - 32 bit pointer
    - code indicates general problem
      - 0 bad header field
      - 1 unrecognized next header
      - 2 unrecognized option

# ICMPv6 Information

- Echo Request/Reply
  - Identical to IPv4 Echo

- No: Address Mask, Timestamp, Info Request

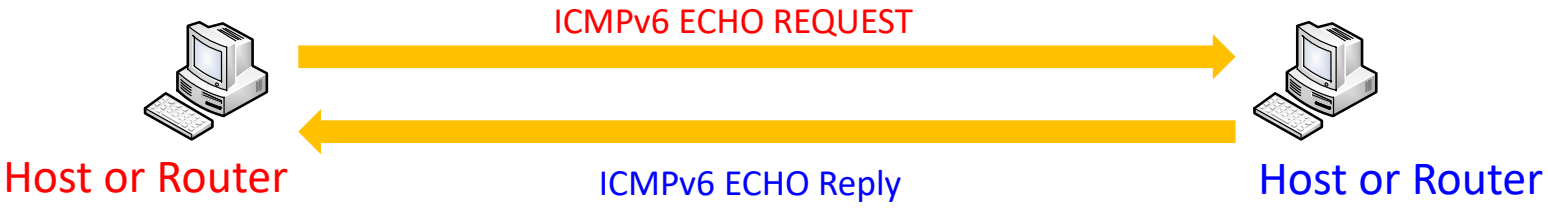
- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement

- Redirect
  - Much more structured messages
- Multicast Listener Discovery (MLD)

# Echo Request and Reply

- ICMPv6 Echo Request = Type: 128
  - Code: 0 (It's not used)

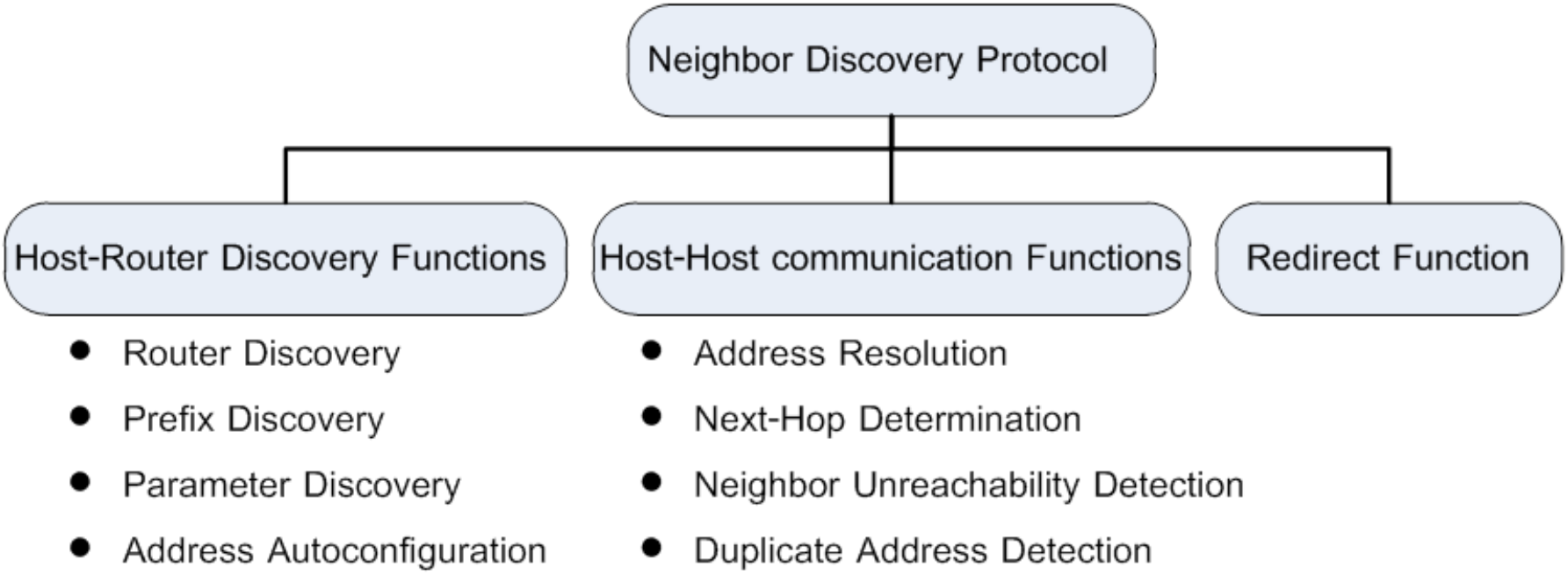
- ICMPv6 Echo Reply = Type: 129
  - Code:0 (It's not used)



# Neighbor Discovery Protocol

- Described in RFC 4861
- Neighbors = nodes on the same link
- ND effectively replaces the ARP found in IPv4
- Multicast instead of Broadcast
  - Multicast group depends upon target address
  - Often only one node will receive request
- Additionally, it combines this with ICMP Router Discovery and Redirect capabilities

# Neighbor Discovery Protocol (cont.)



# Neighbor Discovery Protocol (cont.)

- Neighbor discovery uses 5 ICMPv6 msg.
  - Router solicitation (RS) Type 133
  - Router advertisement (RA) Type 134
  - Neighbor solicitation (NS) Type 135
  - Neighbor advertisement (NA) Type 136
  - Redirect message Type 137

# Neighbor Discovery Protocol (cont.)

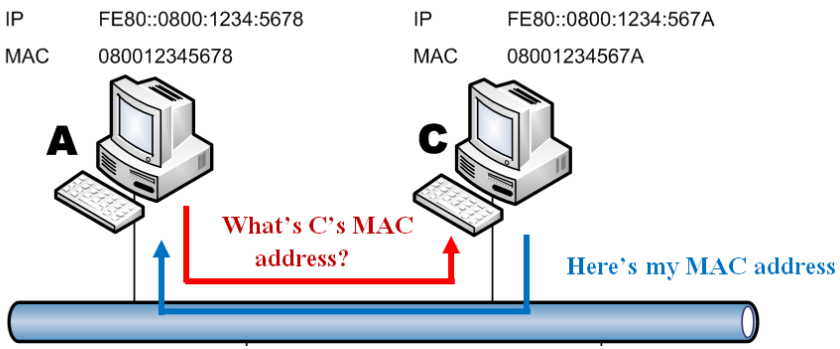
| Mechanism | RS | RA | NS | NA | Redirect |
|---|---|---|---|---|---|
| Address resolution | | | X | X | |
| Router discovery | X | X | | | |
| Prefix discovery | X | X | | | |
| Redirection | | | | | X |
| Neighbor unreachability detection | | | X | X | |
| Duplicate Address Detection | | | X | X | |
| Next-Hop Determination | | | X | X | |
| Address Autoconfiguration | X | X | | | |
| Parameter Discovery | X | X | | | |

# Address resolution

- ARP = convert IP address to MAC address
  - IPv4 ARP works in layer 2
  - IPv4 ARP uses broadcast

- IPv6 uses NS & NA
- Perform MAC address resolution
  - lst address = solicited node multicast address
- Perform neighbor reachability detection
  - Dst address = unicast address

# Address resolution (cont.)

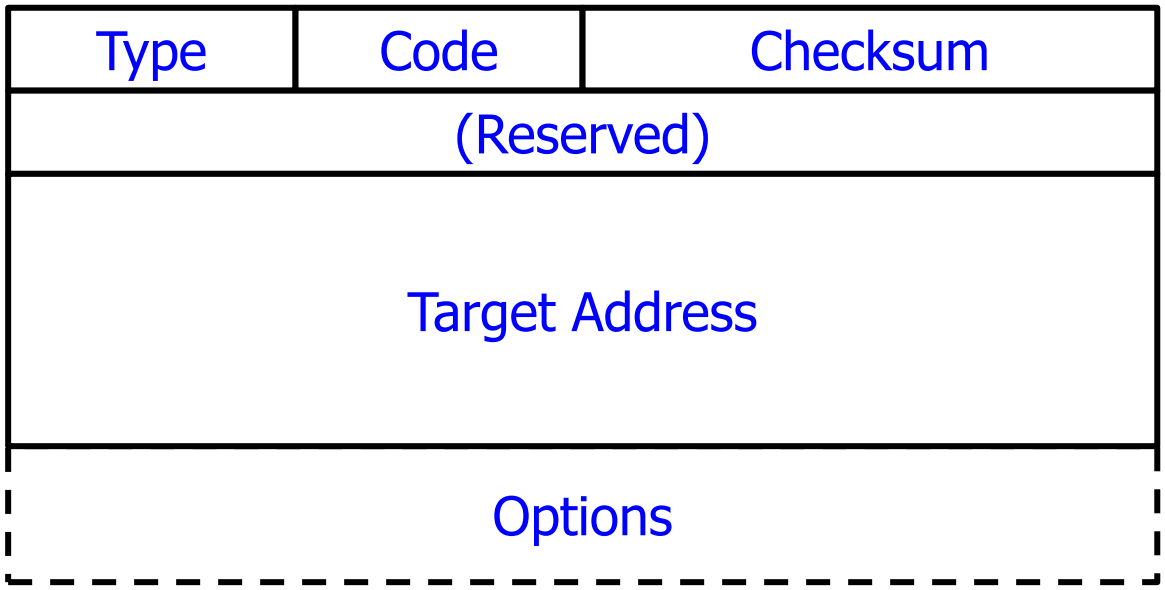



**ICMP type 135 (Neighbor Solicitation)**
**Src: FE80::0800:1234:5678**
**Dst: FF02::1:FF34:567A**
**Data: 08:00:12:34:56:78**
**Src Link-Layer address: 08:00:12:34:56:78**
**Dst Link-Layer address: 08:00:12:34:56:7A**

**Solicited-node multicast**

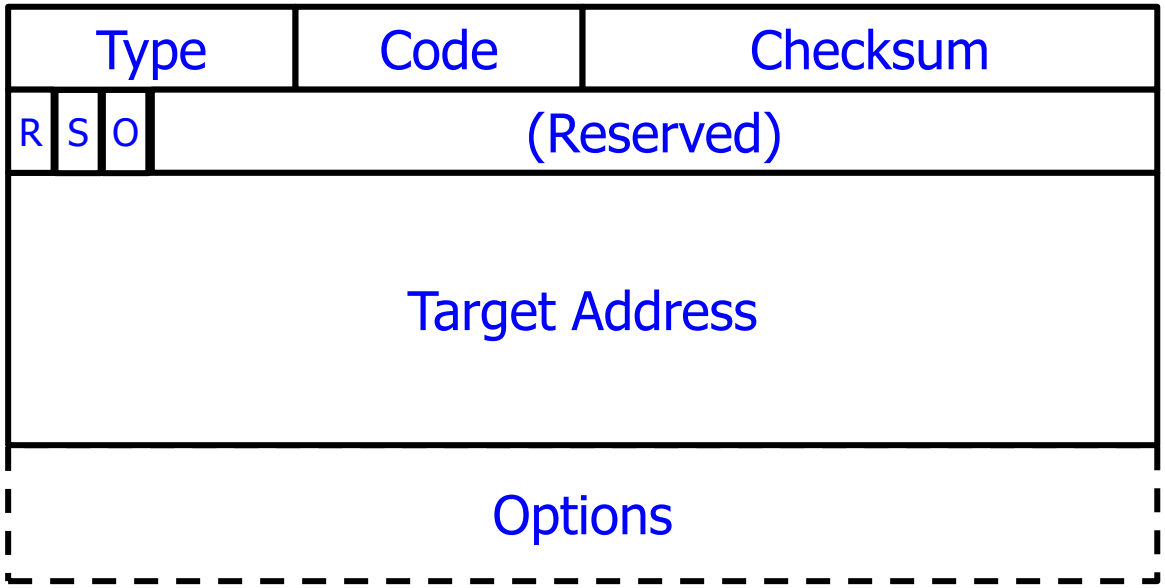
**ICMP type 136 (Neighbor Advertisement)**
**Src: FE80::0800:1234:567A**
**Dst: FE80::0800:1234:5678**
**Data: 08:00:12:34:56:7A**
**Src Link-Layer address: 08:00:12:34:56:7A**
**Dst Link-Layer address: 08:00:12:34:56:78**

# IPv6 Neighbor Solicitation



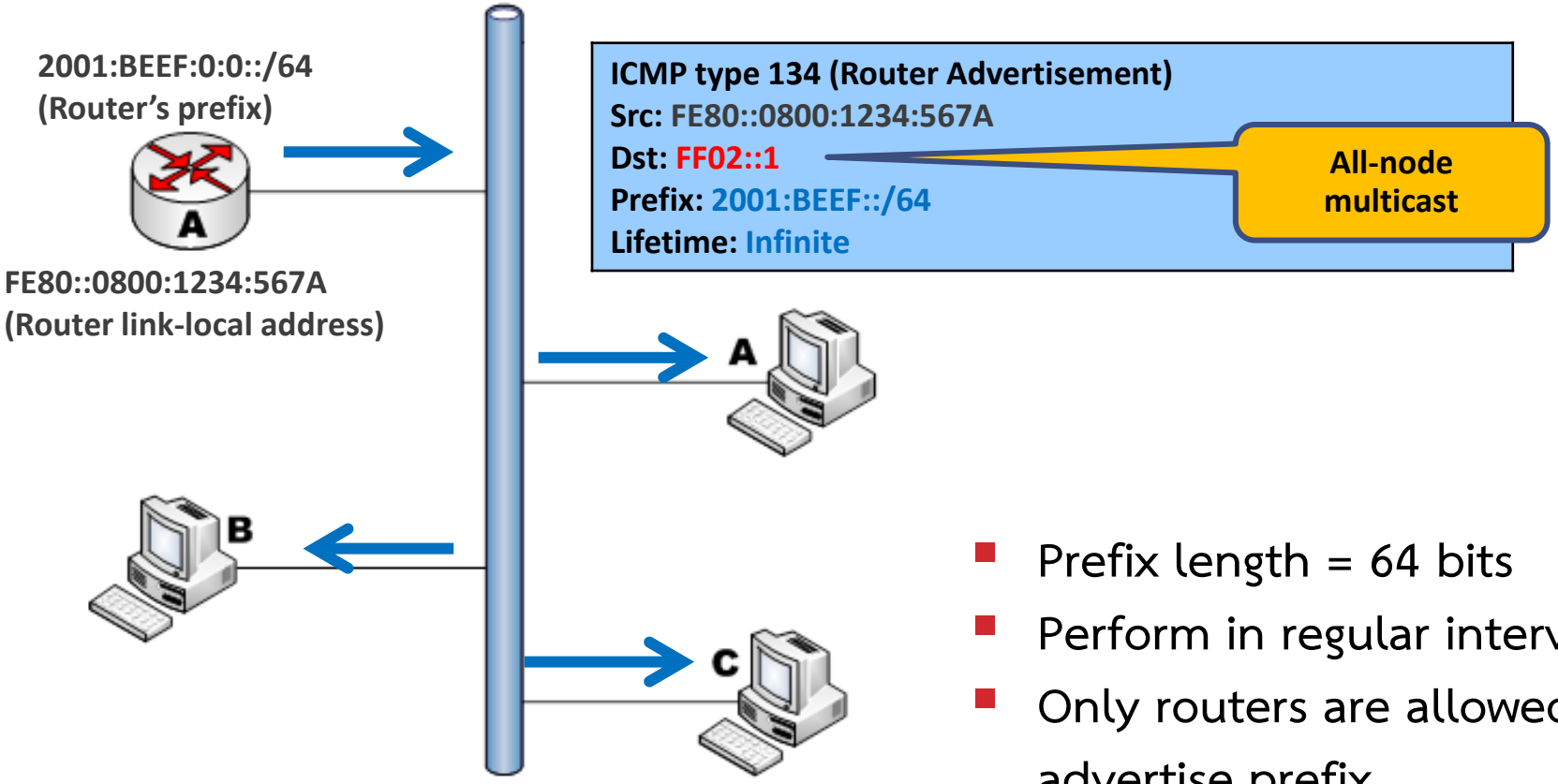

- Target Address
  - The IPv6 address of the host receiving the NS
- Options
  - Source Link Layer Address

# IPv6 Neighbor Advertisement



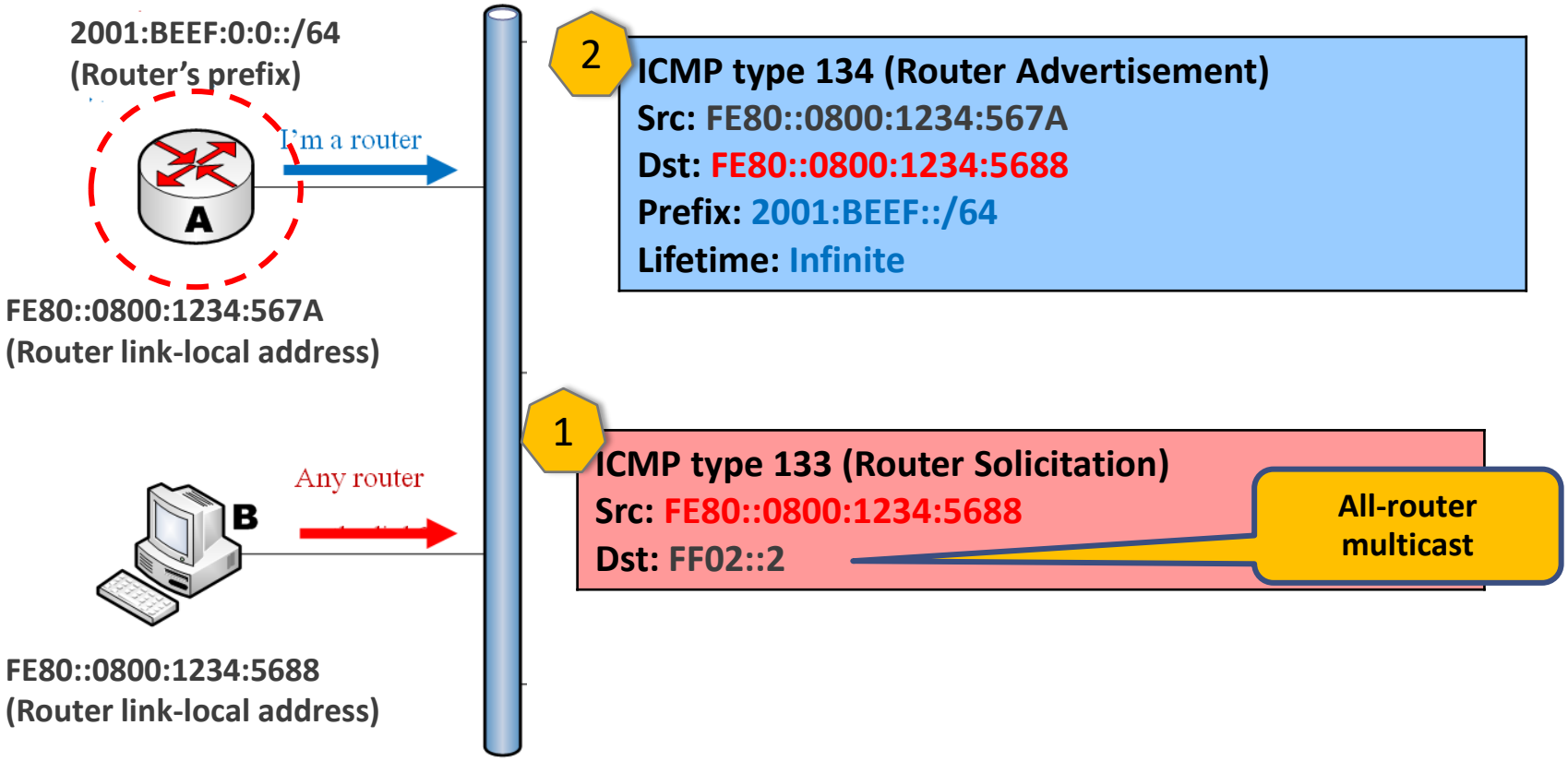

- R Sender is a router
- S Solicited (sent in response to a NS)
- O Override (override any existing cached entry for the link-layer address)
- Options – Target Link Layer address

# Router/Prefix discovery

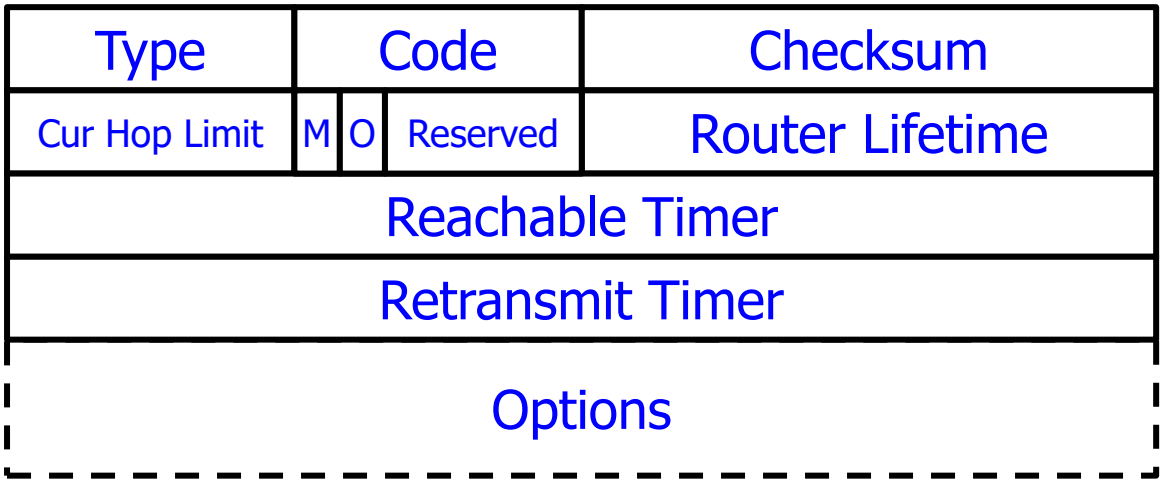



- Prefix length = 64 bits
- Perform in regular intervals
- Only routers are allowed to advertise prefix

# Request Router's prefix



# ICMPv6 Router Advertisement



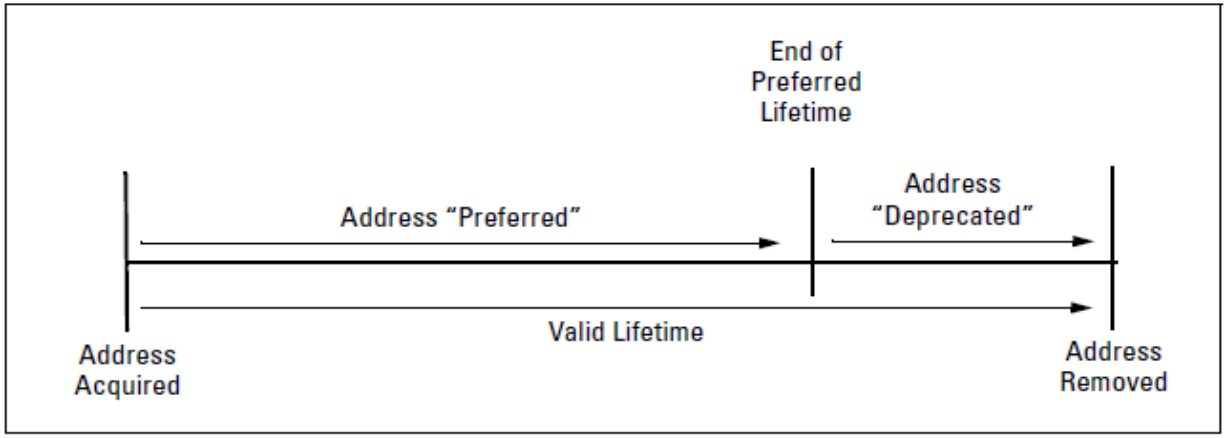

- Announce sender as a router
- Provide information to nodes on link
- Always sent from Link Local Address
  - Hop Limit == 255

# ICMPv6 RA Information

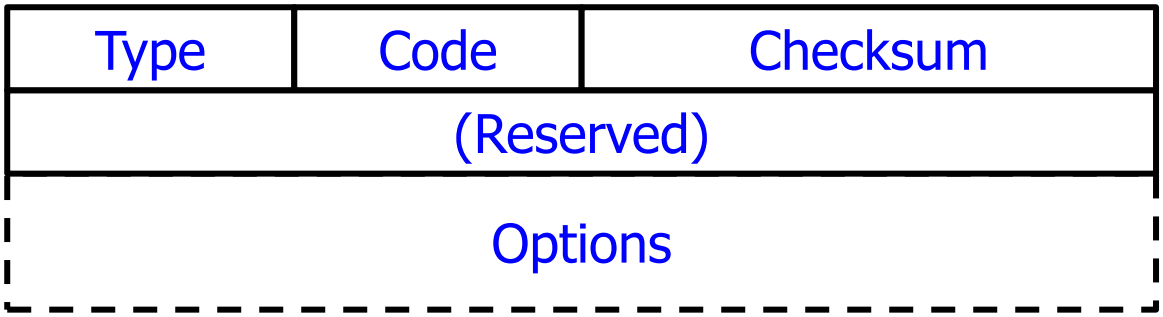
- Option:
  - Source Link Layer Address
  - MTU
  - Prefix Information

| Type | Length | Prefix Length | L | A | Reserved |
|---|---|---|---|---|---|
| Valid Lifetime | | | | | |
| Preferred Lifetime | | | | | |
| (Reserved) | | | | | |
| Prefix | | | | | |

In the deprecated state, an address can continue to be used as a destination for existing communication exchanges but is not used for new exchanges



# ICMPv6 Router Solicitation




- Options:
  - Source Link Layer Address

# Prefix Renumbering

- Can transparently renumber end hosts when the prefix changes
  - Change providers
  - Change subnet ID

- How?
  - Router advertises the old prefix with lifetime = 0
  - Router advertises the new prefix
  - Hosts discard old address when lifetime expires

# Duplicate Address Detection

- Used before assigning an address
  - Tentative address
    - This is an address that has not yet been assigned
  - Check see if any other node has the same address

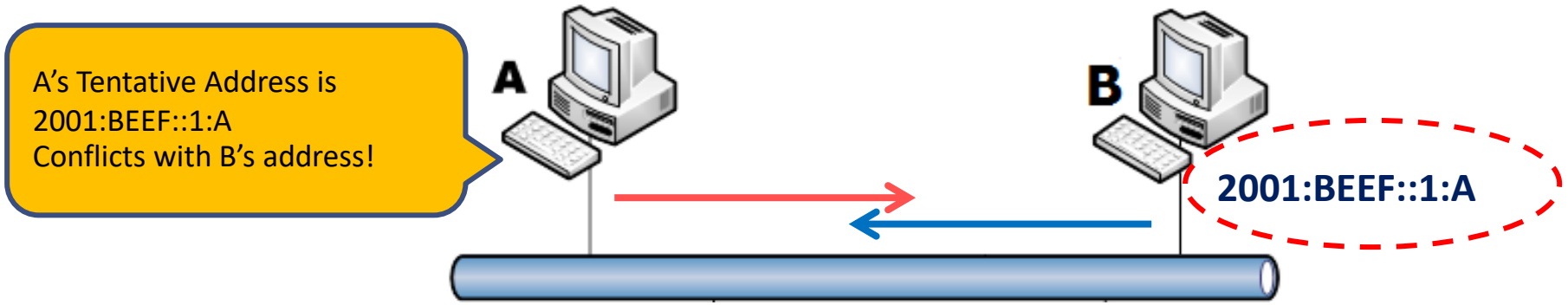
- Send NS for address desired
  - But from what address?
    - node might have none
    - Send from unspecified address 0::0
      - Also allows recognition of DAD

- Reply multicast to all nodes (on link)
  - No link layer address permitted
  - No IPv6 address to send to

# Duplicate Address Detection (cont.)

- Parameters
  - RetransTimer (default = 1000ms)
    - Timer waiting for a reply (NA)
  - DupAddrDetectTransmit (default = 1)
    - Number of DAD requests (NS)

# Duplicate Address Detection (cont.)




**ICMP type 135 (Neighbor Solicitation)**
**Src: :: (Unspecified)**
**Dst: FF02::1:FF01:000A**
**Target address: 2001:BEEF::1:A**

Solicited-node multicast

**ICMP type 136 (Neighbor Advertisement)**
**Src: 2001:BEEF::1:A**
**Dst: FF02::1**
**Target address: 2001:BEEF::1:A**

# Router Renumbering

- Type 138

- Router Renumbering Command messages
  - Code = 0
  - Providing a list of prefixes of routers that are to be renumbered
  - If the addresses on any of their interfaces match the prefixes
    - Change the matched prefixes to the new ones specified in the message

- Each router processing the message will respond with a Router Renumbering Result message
  - Code = 1
  - The renumbering was successful