Internet Protocol version 6

Comer's
chapter 33 (4th ed.)
chapter 29 (3rd ed.)

Content of this lecture

- Internet Protocol (IPv6)
  - Addresses
  - Base Header and Extension Headers
- Internet Control Message Protocol (ICMPv6)
- IPv4/IPv6 Interoperability

Change

According to Comer:

- Larger Addresses
- Extended Address Hierarchy
- Flexible Header Format
- Improved Options
- Provision for Protocol Extension
- Support for Autoconfiguration and Renumbering
- Support for Resource Allocation

IPv6 Addresses

- 128 bits long
- Colon hexadecimal notation
  - 68E6:8C64:FFFF:FFFF:0:1180:95A:FFFF
  - (104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255 in dot ted decimal)
- 15% of address space is assigned
  - 0000 0000 prefix reserved for IPv4 compatibility

Address Types

- Unicast
  - Destination is a single network connection (host or router)
- Anycast
  - Destination is a set of computers
  - Datagram is routed to “nearest” member of a group
- Multicast
  - Destination is a set of computers

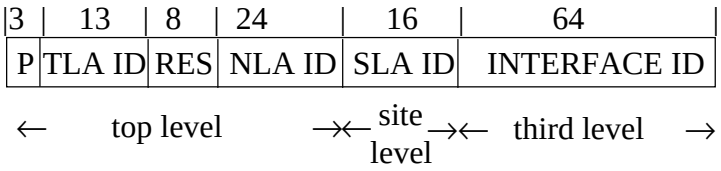
Special Addresses

- Unspecified address
  - 0:0:0:0:0:0:0:0
  - can be used as a source address when own address is unknown
- Loopback address
  - 0:0:0:0:0:0:0:1
  - For testing, do not use in network
  - Datagram is delivered to the local machine

Unicast Address Hierarchy

- Individual network interface
  - Single connection between computer and network
- Individual site
  - Set of computers in a single organization
- Globally-known public topology
  - Publicly available “section’’ of the Internet
  - Two types: ISPs and exchange

Aggregatable Global Unicast Address



- TLA ID = Top-Level Aggregation
- NLA ID = Next-Level Aggregation
- SLA ID = Site-Level Aggregation
- Interface ID

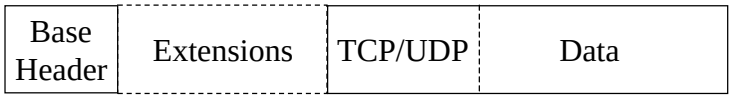
Local Addresses

- Unicast address with local scope
- Link-local address
  - Datagrams are not delivered outside the physical network
  - Prefix: 1111 1110 10
- Site-local address
  - Datagrams are not delivered outside the site
  - Prefix: 1111 1110 11

Autoconfiguration

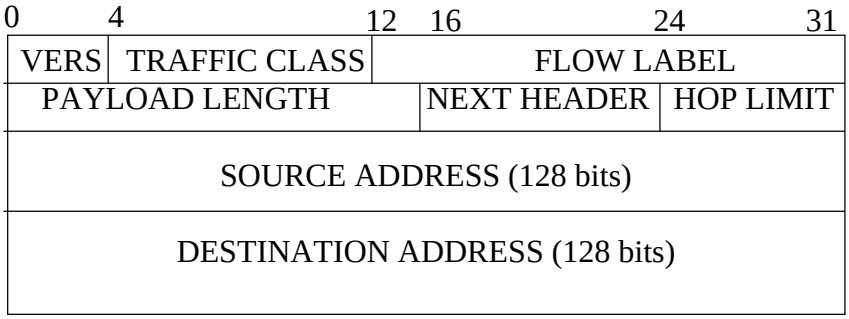
- No address assignment server
- Uses link-local addresses with interface identifier
  - router solicitation - router advertisement
- Router informs the host if autoconfiguration is used or not
- Timers tell how long the prefix is valid

Structure of IPv6 Datagram



- Base header is fixed
  - 40 octets long
  - Options are in an extension header
- Several extension headers

Base Header



- Every IPv6 datagram begins with the base header

Extension Headers

- Base header does not offer
  - fragmentation
  - source routing
  - options
  - authentication and confidentiality
- Efficient and easy to change
- Next header field help to parse the information in the datagram

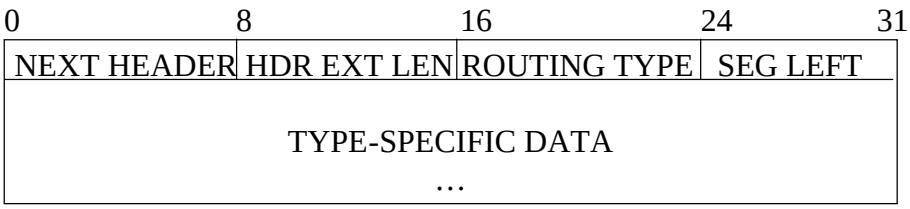
Fragmentation

0 31

NEXT HEADER	RESERVED	FRAG. OFFSET	RS	M
DATAGRAM IDENTIFICATION				

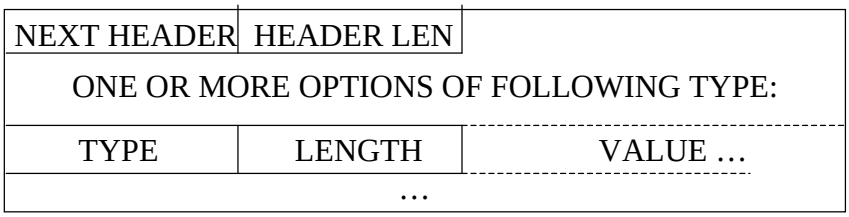
- End-to-End Fragmentation
  - Guaranteed minimum MTU (1280 octets)
  - Path MTU Discovery
- When fragmentation is needed, fragment extension header follows the base header

Source Routing



- IPv6 offers loose source routing

Options



- Hop By Hop Extension Header and End To End Extension Header both uses this format
- Next Header of previous Header tell the type of this header

Pseudo Header

SOURCE ADDRESS	
DESTINATION ADDRESS	
LENGT OF THE DATA FIELD	
ZERO	NEXT HDR

- TCP and UDP use pseudo-header in checksum calculation
  - Same information as in the IPv4 pseudo-header

Summary

- IPv6 provides connectionless, best-effort delivery service
- Datagram consists of base header, extension headers and (upper layer) data
- Unicast, anycast and multicast addresses
- Requires also changes to other protocols

References

- Comer chapter 33
- RFC 2373 - IP Version 6 Addressing Architecture, 1998
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, 1998

Internet Control Message Protocol version 6 (ICMPv6)

ICMP for IPv6

- Like IPv4, IPv6 has its own ICMP that is mandatory
  - Error messages
  - Informational messages
- General structure of message same than previous ICMP
- More use in the IPv6 network

Destination Unreachable

- Error codes:
  - No route to destination
  - Administratively prohibited
  - Address unreachable
  - Port unreachable
- As much data from the original packet as possible so that the ICMP message fits in the minimum MTU

Other Error Messages

- Packet too big
  - Packet is larger than MTU
- Time exceeded
  - Hop Limit is zero
- Parameter problem
  - Erroneous header field
  - Unrecognized Next Header / IPv6 option
- Echo request and reply

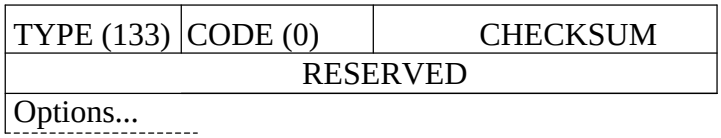
Neighbor Discovery Protocol

- IPv6 does not use ARP
- Neighbor Discovery protocol is used for finding link layer addresses and routers
- Uses ICMP message format (extension to ICMP)

Neighbor Discovery Messages

- Router Solicitation and Advertisement
  - various link and Internet parameters
  - periodically or just booted machine can ask
- Neighbor Solicitation and Advertisement
  - link level address resolution and reachability
- Redirect
  - better first hop for destination

Router Solicitation Message



- Contains source link layer address, if known
- Used when a network interface become enabled
- Request for Router Advertisement message

Router Advertisement Message

TYPE (134)	CODE (0)	CHECKSUM
CUR Hop L	M O RES.	ROUTER LIFETIME
REACHABLE TIME		
RETRANS TIME		
Options...		

- Information about network parameters and router parameters (e.g. is this the default router and use of address configuration method)
- Options: Link layer address, MTU, prefix info

Neighbor Socilitation Message

TYPE (135)	CODE (0)	CHECKSUM
RESERVED		
TARGET ADDRESS (128 bits)		
Options...		

- Request for link-layer address of the target
  - Uses multicast if the receiver is unknown
  - Uses unicast if reachability is checked
- Options contains source address if it is known

Neighbor Advertisement Message

TYPE (136)	CODE (0)	CHECKSUM
R S O	RESERVED	
TARGET ADDRESS (128 bits)		
Options...		

- Flags: router, response and overwrite
- Target's IP address
- Target's link-layer address is in the options field

Redirect Message

TYPE (137)	CODE (0)	CHECKSUM
RESERVED		
TARGET ADDRESS (128 bits)		
DESTINATION ADDRESS (128 bits)		
Options...		

- Informs better route (next hop address) or that the target is the neighbor (addresses are same)
- Options: link-layer address, original message

Neighbor Unreachability Detection Algorithm

- Hosts maintain a cache for neighbors
  - IPv6 and link-level addresses
  - Is the neighbor a router
  - Information about state of neighbors
- Information in the cache is maintained by Neighbor unreachability detection algorithm

Path MTU Discovery

- IPv6 uses end-to-end fragmentation
- Sender needs to know the smallest MTU
  - First use the MTU of the first hop in the path
  - If it is too big, ICMP Packet Too Big message received
  - Reduce Path MTU until ok
- Other solution: send only minimal length packets

Path MTU (continue)

- Path MTU may change
  - increasing and decreasing of path MTU must be done sometimes
  - test unfrequently by sending a new large message
- In Multicasting
  - choose the smallest path MTU

Summary

- Also the Internet Control Message Protocol changes
- More data from the original message included in error message
- ICMP is used instead of ARP
- ICMP is used for detecting the need for fragmentation in IPv6

References

- RFC 2463 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, 1998
- RFC 2461 - Neighbor Discovery for IP Version 6 (IPv6), 1998
- RFC 1981 - Path MTU Discovery for IP Version 6, 1996

IPv4/IPv6 Interoperability

Motivation

- Majority of hosts in the Internet will continue to use IPv4
  - NAT
  - Somebody needs to be the first
  - Interoperability must be guaranteed
- IPv6 offers number of advantages compared to IPv4

Dual Stack (RFC 1933)

- Two kinds of network nodes
  - Implement only IPv4
  - IPv6 nodes providing compatibility with IPv4
- IPv6 over IPv4 tunneling
  - router-to-router, host-to-router, host-to-host
  - ICMP error message handling
- Needs to change DNS also

SIIT (RFC 2765)

- Stateless IP/ICMP Translation Algorithm (SIIT)
- Network that consists of IPv6-only and IPv4-only nodes (and IPv4 address pool)
- Two-way translation of IP and ICMP messages
  - Not for options and routing extension headers

NAT-PT (RFC 2766)

- Network Address Translation – Protocol Translation (NAT-PT)
- ”Combination” of SIIT and NAT
  - Several IPv6 nodes uses one IPv4 address (translation is done with NAT)
  - SIIT is used for protocol translation with minor modifications

Summary

- Interoperability research is still ongoing
- Two kind of methods
  - Dual stack
  - Interoperability protocols
- Requires changes to other network parts like DNS etc.

References

- RFC 1933 - Transition Mechanisms for IPv6 Hosts and Routers, 1996
- RFC 2765 – Stateless IP/ICMP Translation Algorithm (SIIT), 2000
- RFC 2766 - Network Address Translation – Protocol Translation (NAT-PT), 2000
- IETF Next Generation Translation workgroup http://www.ietf.org/html.charters/ngtrans-charter.html