IPv6: An Introduction

Dheeraj Sanghi
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
dheeraj@iitk.ac.in
http://www.cse.iitk.ac.in/users/dheeraj

Outline

- Problems with IPv4
- Basic IPv6 Protocol
- IPv6 features
  - Auto-configuration, QoS, Security, Mobility
- Transition Plans

Internet Protocol

Transports a datagram from source host to destination, possibly via several intermediate nodes ("routers")

Service is:

- *Unreliable:* Losses, duplicates, out-of-order delivery
- *Best effort:* Packets not discarded capriciously, delivery failure not necessarily reported
- *Connectionless:* Each packet is treated independently

IP Datagram Header

0	4	8	16	19	31
VERS	HLEN	TOS	TOTAL LENGTH		
IDENTIFICATION			FLAG	FRAGMENT OFFSET	
TTL		PROTOCOL	CHECKSUM		
SOURCE ADDRESS					
DESTINATION ADDRESS					
OPTIONS (if any) + PADDING					

Problems with IPv4: Limited Address Space

- IPv4 has 32 bit addresses.
- Flat addressing (only netid + hostid with "fixed" boundaries)
- Results in inefficient use of address space.
- Class B addresses are almost over.
- Addresses will exhaust in the next 5 years.
- IPv4 is victim of its own success.

Problems with IPv4: Routing Table Explosion

- IP does not permit route aggregation
  (limited supernetting possible with new routers)
- Mostly only class C addresses remain
- Number of networks is increasing very fast
  (number of routes to be advertised goes up)
- Very high routing overhead
  - lot more memory needed for routing table
  - lot more bandwidth to pass routing information
  - lot more processing needed to compute routes

Problems with IPv4: Header Limitations

- Maximum header length is 60 octets.
  (Restricts options)
- Maximum packet length is 64K octets.
  (Do we need more than that ?)
- ID for fragments is 16 bits. Repeats every 65537th packet.
  (Will two packets in the network have same ID?)
- Variable size header.
  (Slower processing at routers.)
- No ordering of options.
  (All routers need to look at all options.)

Problems with IPv4: Other Limitations

- Lack of quality-of-service support.
  - Only an 8-bit ToS field, which is hardly used.
  - Problem for multimedia services.
- No support for security at IP layer.
- Mobility support is limited.

IP Address Extension

- Strict monitoring of IP address assignment
- Private IP addresses for intranets
  - Only class C or a part of class C to an organization
  - Encourage use of proxy services
    - Application level proxies
    - Network Address Translation (NAT)
- Remaining class A addresses may use CIDR
- Reserved addresses may be assigned

But these will only postpone address exhaustion.
They do not address problems like QoS, mobility, security.

IPng Criteria

- At least 10^9 networks, 10^{12} end-systems
- Datagram service (best effort delivery)
- Independent of physical layer technologies
- Robust (routing) in presence of failures
- Flexible topology (e.g., dual-homed nets)
- Better routing structures (e.g., aggregation)
- High performance (fast switching)
- Support for multicasting

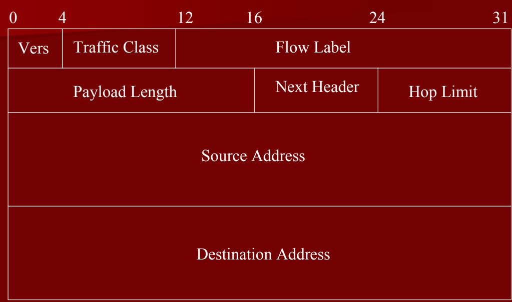
IPng Criteria

- Support for mobile nodes
- Support for quality-of-service
- Provide security at IP layer
- Extensible
- Auto-configuration (plug-and--play)
- Straight-forward transition plan from IPv4
- Minimal changes to upper layer protocols

IPv6: Distinctive Features

- Header format simplification
- Expanded routing and addressing capabilities
- Improved support for extensions and options
- Flow labeling (for QoS) capability
- Auto-configuration and Neighbour discovery
- Authentication and privacy capabilities
- Simple transition from IPv4

IPv6 Header Format



Extension Headers

- Less used functions moved to extension headers.
- Only present when needed.
- Processed only by node identified in IPv6 destination field.
  => much lower overhead than IPv4 options
  Exception: Hop-by-Hop option header
- Eliminated IPv4's 40-byte limit on options
- Currently defined extension headers: Hop-by-hop, Routing, Fragment, Authentication, Privacy, End-to-end.
- Order of extension headers in a packet is defined.
- Headers are aligned on 8-byte boundaries.

Address Types

Unicast Address for a single interface.
Multicast Identifier for a set of interfaces.
Packet is sent to *all* these interfaces.
Anycast Identifier for a set of interfaces.
Packet is sent to the *nearest* one.

IPv6 Addresses

- 128-bit addresses
- Multiple addresses can be assigned to an interface
- Provider-based hierarchy to be used in the beginning
- Addresses should have 64-bit interface IDs in EUI-64 format
- Following special addresses are defined :
  - IPv4-mapped
  - IPv4-compatible
  - link-local
  - site-local

IPv6 Routing

- Hierarchical addresses are to be used.
- Initially only provider-based hierarchy will be used.
- Longest prefix match routing to be used.
  (Same as IPv4 routing under CIDR.)
- OSPF, RIP, IDRP, ISIS, etc., will continue as is
  (except 128-bit addresses).
- Easy renumbering should be possible.
- Provider selection possible with *anycast* groups.

QoS Capabilities

- Protocol aids QoS support, not provide it.
- Flow labels
  - To identify packets needing same quality-of-service
  - 20-bit label decided by source
  - Flow classifier: Flow label + Source/Destination addresses
  - Zero if no special requirement
  - Uniformly distributed between 1 and FFFFFF
- Traffic class
  - 8-bit value
  - Routers allowed to modify this field

IPv6: Security Issues

- Provision for
  - Authentication header
    - Guarantees authenticity and integrity of data
  - Encryption header
    - Ensures confidentiality and privacy
- Encryption modes:
  - Transport mode
  - Tunnel mode
- Independent of key management algorithm.
- Security implementation is mandatory requirement in IPv6.

Mobility Support in IPv6

- Mobile computers are becoming commonplace.
- Mobile IPv6 allows a node to move from one link to another without changing the address.
- Movement can be heterogeneous, i.e., node can move from an Ethernet link to a cellular packet network.
- Mobility support in IPv6 is more efficient than mobility support in IPv4.
- There are also proposals for supporting micro-mobility.

Operation of Mobile IPv6

- Mobile node is always addressable by its **home address**.
- **Home link** is the link to which mobile nodes home address is bound.
- When attached to home link, packets are routed conventionally.
- When the node moves to foreign links, it gets a **care-of address**.
- **Binding** is an association between a home address and a care-of address.

- Care-of address is obtained using auto-configuration mechanisms of neighbour discovery.
- Mobile node, when away, registers its binding with a router on the home link called **home-agent**.
- **Binding update** and **Binding Ack** destination options are used for this purpose.
- Home agent uses **proxy neighbour discovery** to intercept packets destined for the mobile node.
- It then **tunnels** the packet to mobile node's care-of address.
- Mobile node when away uses its care-of address for communication.

- Mobile node uses a **Home Address** option to tell the other nodes its original address.
- Communicating nodes can cache the bindings and communicate with the mobile node directly.
- They use **Binding Request** destination option to learn the current binding.
- A mobile node can send a **Binding Update** to a communicating node which is using its home address as destination address.
- The communicating node should acknowledge it with a **Binding Acknowledgement**.

Neighbour Discovery

- Router Discovery - determines set of routers on the link.
- Prefix Discovery - set of on-link address prefixes.
- Parameter Discovery - to learn link parameters such as link MTU, or internet parameters like hop limit, etc.
- Address Auto-configuration - address prefixes that can be used for automatically configuring interface address.
- Address resolution - IP to link-layer address mapping.
- Duplicate Address Detection.
- Route Redirect - inform of a better first hop node to reach a particular destination.

Neighbour Discovery Operation

- Based on ICMPv6 messages
  - Router Solicitation (RS)
  - Router Advertisement (RA)
  - Neighbour Solicitation (NS)
  - Neighbour Advertisement (NA)
  - Redirect
- Router Solicitation
  - sent when an interface becomes enabled, hosts request routers to send RA immediately.

Neighbour Discovery Operation (contd..)

- Router advertisement
  - Sent by routers periodically or in response to RS.
  - Hosts build a set of default routers based on this information.
  - Provides information for address auto-configuration, set of on-link prefixes etc.
  - Supplies internet/subnet parameters, like MTU, and hop limit.
  - Includes router's link-layer address.

Neighbour Discovery Operation (contd..)

- Neighbour Solicitation
  - To request link-layer address of neighbour
  - Also used for Duplicate Address Detection
- Neighbour Advertisement
  - Sent in response to NS
  - May be sent without solicitation to announce change in link-layer address
- Redirect - used to inform hosts of a better first hop for a destination.

Address Auto-configuration

The problem

- System bootstrap ("plug and play")
- Address renumbering

Addressing Possibilities

Manual	Address configured by hand
Autonomous	Host creates address with no external interaction (e.g., link local)
Semi-autonomous	Host creates address by combining a priori information and some external information.
Stateless Server	Host queries a server, and gets an address. Server does not maintain a state.
Stateful Server	Host queries a server, and gets an address. Server maintains a state.

Auto-configuration in IPv6

- Link-local prefix concatenated with 64-bit MAC address. *(Autonomous mode)*
- Prefix advertised by router concatenated with 64-bit MAC address. *(Semi-autonomous mode.)*
- DHCPng *(for server modes)*
  - Can provide a permanent address *(stateless mode)*
  - Provide an address from a group of addresses, and keep track of this allocation *(stateful mode)*
  - Can provide additional network specific information.
  - Can register nodes in DNS.

Address Renumbering

- To migrate to a new address
  - change of provider
  - change in network architecture
- Methods
  - router adds a new prefix in RA, and informs that the old prefix is no longer valid.
  - When DHCP lease runs out, assign a new address to node.
  - DHCPng can ask nodes to release their addresses.
- Requires DNS update. DHCPng can update DNS for clients.
- Existing conversations may continue if the old address continues to be valid for some time.

Upper Layer Issues

- Minor changes in TCP
  - Maximum segment size should be based on Path MTU.
  - The packet size computation should take into account larger size of IP header(s).
  - Pseudo-header for checksum is different.
- UDP checksum computation is now mandatory.
- Most application protocol specifications are independent of TCP/IP - hence no change.
- FTP protocol exchanges IPv4 addresses - hence needs to be changed.

- The pseudo-header is changed in checksum computation:
  - Address are 128 bits.
  - Payload length is 32 bits.
  - Payload length is not copied from IPv6 header. (Extension headers should not be counted.)
  - Next header field of last extension header is used in place of protocol.
- UDP packets must also have checksum.

  (Since no IP checksum now.)

Changes in Other Protocols

- ICMPv6
  - Rate limiting feature added
    - Timer based
    - Bandwidth based
  - IGMP, ARP merged
  - Larger part of offending packet is included
- DNS
  - AAAA type for IPv6 addresses
  - A6 type: recursive definition of IP address
  - Queries that do additional section processing are redefined to do processing for both 'A' and 'AAAA' type records

Transition to IPv6: Design Goal

- No "flag"day.
- Incremental upgrade and deployment.
- Minimum upgrade dependencies.
- Interoperability of IPv4 and IPv6 nodes.
- Let sites transition at their own pace.
- Basic migration tools
  - Dual stack and tunneling
  - Translation

Transition Mechanisms: Dual Stack

- New nodes support both IPv4 and IPv6.
- Upgrading from IPv4 to v4/v6 does not break anything.
- Same transport layer and application above both.
- Provides complete interoperability with IPv4 nodes.

Transition Mechanism: Tunnels

- Tunnel IPv6 packets across IPv4 topology.
- Configured tunnels:
  - Explicitly configured tunnel endpoints.
  - Router to router, host to router.
- Automatic tunnels:
  - Automatic address resolution using embedded IPv4 address (like IPv4-compatible address).
  - Host to host, router to host

Transition mechanism: Translation

- This will allow communication between IPv6 only hosts and IPv4 only hosts.
- A typical translator consists of two components:
  - translation between IPv4 and IPv6 packets.
  - Address mapping between IPv4 and IPv6
- For translation, three technologies are available:
  - header conversion
  - transport relay
  - application proxy

Transition Plan for Internet

- Maintain complete V4 routing till addresses last.
- Upgrade V4 routers to dual stack.
- Incrementally build up V6 backbone routing system.
  - Use v6-over-v4 tunnels to construct 6bone.
  - Grow like Mbone (multicast backbone).
- De-activate tunnels as soon as underlying path upgraded to V6.

Transition Options for User Sites

- Incrementally upgrade V4 hosts to dual V4/V6
  - Use IPv4-compatible addresses with existing IPv4 address assignments
  - Host-to-host automatic tunneling over IPv4
- Upgrade routers to IPv6.
  - Hosts may require native IPv6 addresses
  - DNS upgrade is needed before hosts get IPv6 addresses
- Connect IPv6 router to an IPv6-enabled ISP.
- Install translators like NAT-PT or SIIT.

Thank You