Introduction to IPv6

PASI (Pan-American Advanced Studies Institute)
Grid Computing and Advanced Networking Technologies for e-Science

Tereza Cristina M. B. Carvalho
ANSP/LARC/PCS/EPUSP
carvalho@larc.usp.br

Agenda

- History
- Comparison between IPv4 x IPv6
- Migration Strategy
- Final Considerations
**History**

- IP (Internet Protocol) was specified in the end of 70’s through the RFC 791.
- 1991 - IETF decided to specify a new version of the IP protocol called IPng (IP next generation) or IPv6 (IP version 6).
- 1994 – the main features of IPv6 were defined.

**IPv6**

- Its development has started in the beginning of 90’s by IETF (Internet Engineering Task Force).
- **Motivation:** Lack of IP address in short-term, since new networks have been connected at an increasing rate to the Internet.
- Based on IPv4 experience, the IPv6 designers take this opportunity for changing and adding new characteristics.
The IP layer is responsible for data forwarding within a TCP/IP network.
  * Defines the network basic transmission unit: **Datagram**.
  * Defines the host addressing scheme: **IP address**.
  * It is responsible for the routing function, selecting the datagram route in the network.

All other protocols (TCP, UDP, ICMP e IGMP) are transmitted in the network as **IP datagrams**.

The IP Layer provides a **non-reliable packet delivery service** without connection (**connectionless** service).
  * Datagrams can be lost, duplicated, delayed or delivered out of order.
  * Defined by RFC 791.
Comparison IPv4 x IPv6

- The main differences between IPv4 e IPv6 include:
  - Addressing.
  - Network address translation.
  - Routing.
  - Security.
  - Administrative workload.
  - Support to mobile devices.

Datagram Format

- IPv4
  - Checksum in the header.
  - Option Field, limited to 40 bytes.
  - No mechanism for the definition of traffic flow.

- IPv6
  - No Checksum in the header.
  - Extension headers with random sizes.
  - Possibility of associating several datagrams to the same traffic flow.
IPv4 Datagram

- The IPv4 datagram header has 24 bytes, 12 of them are used for additional information and 4 for options.
- This information in IPv6 is contained in the extension headers.
The IPv6 datagram has a simpler format. The IPv6 has a basic header with fixed length and zero or more extension headers.

This solution presents great flexibility, because each datagram includes only the necessary headers for the corresponding communication.

![IPv6 Datagram Diagram]

**IPv6 Datagram**

<table>
<thead>
<tr>
<th>Basic Header</th>
<th>Extension Header 1</th>
<th>...</th>
<th>Extension Header N</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>40 bytes</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Extension Headers

- For additional functions, IPv6 uses 6 types of extension headers:
  - Hop-by-Hop Header.
  - Routing Header:
    - Source Demand Routing Protocol (SDRP).
    - It contains the list of IP addresses to be visited.
  - Fragmentation Header:
    - The fragmentation can only be performed by the origin node.
  - Authentication Header.
  - Encrypted Security Payload:
    - Contains the cryptographed payload.
    - The standard algorithm is the DES (Data Encryption Standard).
  - Destination Options Header.

Examples of Extension Headers

<table>
<thead>
<tr>
<th>Basic Header</th>
<th>Routing Header</th>
<th>Segment TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next = TCP</td>
<td>Next = TCP</td>
<td></td>
</tr>
</tbody>
</table>

© Copyright LARC/TMBC 2005
High-Speed Networks - 13

© Copyright LARC/TMBC 2005
High-Speed Networks - 14
### Routing Header Format

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header</td>
<td>Routing Type</td>
<td>Number of Addresses</td>
<td>Next Address</td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Second address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.....</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Addressing

- **IPv4**
  - Maximum Size of the address field is **32** bits.
  - There are five addressing classes: A, B, C, D e E.
  - Each address has two parts: **network address** and **host address**.
  - Multicast support is optional (D Class).
  - Representation of each byte in **decimal** separated by points:
    - 147.100.10.5

- **IPv6**
  - Maximum Size of the address field is **128** bits.
  - There are **3 service classes**:
    - unicast
    - anycast
    - multicast
  - Each address type has a different format.
  - Representation in **hexadecimal** separated by double points:
    - 3ffe:190:4545:3:ff8f:2:de21:67ca
Addressing

- **Unicast Address:**
  - Prefix Format
  - Register Identifier.
  - Provider Identifier.
  - Subscriber Type.
  - Subscriber Identifier.
  - Subnet Identifier.
  - Interface Identifier.

- **Anycast Address:** definition of a group for receiving and sending packets. (e.g., DNS servers).

---

Address Structure – IPv6

- As IPv4, the IP address is assigned to interfaces and not to nodes.
- IPv4 uses an hierarchy of 2 levels (*netid e hostid*). IPv6 allows the usage of a multi-level hierarchy.
**Fragmentation**

- **IPv4**
  - The fragmentation can be performed in every gateway used the subnets interconnection.

- **IPv6**
  - The fragmentation is done by the source node.

**Routing**

- **IPv4**
  - Supports the basic routing protocols.
  - Source routing can be performed by some application from the superior layers.

- **IPv6**
  - Supports the basic routing protocols.
  - Source routing can be implemented using the routing extension header.
Security

- IPv4
  - There are no security mechanisms.
  - Need for the implementation of new protocols to support VPN.

- IPv6
  - Supports security mechanisms used in the implementation of the authentication, non-repudiation, integrity and confidentiality services.
  - Supports security extension headers.
  - Supports a native VPN implementation.

Error Control and Address Resolution

- IPv4
  - Error control performed by ICMP.
  - Translation of logic and physical addresses upon the usage of the ARP e RARP protocols.
  - Multicast Member Control performed by IGMP.

- IPv6
  - Error control.
  - Translation of logic and physical addresses and multicast member control performed by the ICMP.
Two basic questions:

- How 2 IPv6 machines or subnets can communicate between themselves if they are interconnected through IPv4 networks?
- How a IPv4 client application can communicate with an IPv6 server? And a IPv6 client with a IPv4 server?

The main migration strategies are:

- IPv6 Tunelling in IPv4.
- IPv4 Tunelling in IPv4.
- Dual Stack:
  - Two protocol stacks: IPv4 e IPv6 in the same machine.
Migration Strategy

Dual Stack

Not all IPv6 fields can be mapped in IPv4.

Flow = X
Origin: A
Destiny: F
data

Flow = ??
Origin: A
Destiny: F
Data
Migration Strategy

IPv6 Tunelling in IPv4 network

Tunelling

Flow = X
Origin : A
Destiny: F
data

Flow = X
Origin : A
Destiny: F
data

Flow = X
Origin : A
Destiny: F
data

Flow = X
Origin : A
Destiny: F
data
Final Considerations

- **IPv6:**
  - Address limitation.
  - Simplification of routers:
    - Fixed size IP Header.
    - Extension Header: source
    - Usage of traffic flows → Quality of Service.
    - Fragmentation done in the origin.
  - Security:
    - Native security functions.
  - Support of Multimedia applications:
    - Traffic Prioritization
    - Usage of traffic flow.

- **Greater addressing capacity.**
  - 128 bits of address based on hierarchical structure.

- **New type of address - anycast**
  - Facilitate communication between any two group of stations.

- **40 byte-header**
  - Greater processing speed-up.

- **Flow and priority**
  - Transmission with QoS.

- **Support for Mobility.**
Acknowledgments

Thanks to:
Prof. Stephan Kovach and Denis Gabus from the Network and Computer Architecture Laboratory (LARC) from the Department of Computer Engineering - Escola Politécnica - Univ. of Sao Paulo (USP) - Brazil