Acronyms/Abbreviations

- DOCSIS = Data-Over-Cable Service Interface Specification
- CMTS = Cable Modem Termination System
- DS = Downstream
- US = Upstream
- CM = Cable Modem
- IPv6 = Internet Protocol version 6
- ICMPv6 = Internet Control Message Protocol version 6
- DHCPv6 = Dynamic Host Configuration Protocol for IPv6
- MSO = Multiple Services Operator
- SMB = Small Business
- PDA = Personal Digital Assistant
- NAT = Network Address Translation
- CIDR = Classless Interdomain Routing
- DAD = Duplicate Address Detection
- SLA = Subnet Level Address
- VPN = Virtual Private Network
- ARP = Address Resolution Protocol
- eSAFE = Embedded Service/Application Functional Entity
- RS = Router Solicitation
- RA = Router Advertisement
- DUID = DHCP Unique Identifier
- DNS = Domain Name System
- CPE = Customer Premises Equipment
- ND = Neighbor Discovery
- NS = Neighbor Solicitation
- HFC = Hybrid Fiber Coaxial
- EUI = Extended Unique Identifier
- TFTP = Trivial File Transfer Protocol
- ToD = Time of Day
- MDD = Mac Domain Descriptor
- APM = Alternative Provisioning Mode
- ASM = Anysource Multicast
- SSM = Source Specific Multicast
- SLAAC = Stateless Address Autoconfiguration
- MLD = Multicast Listener Discovery
Tutorial-1: Agenda

- **Structure of IPv6 Protocol**
  - IPv4 and IPv6 Header Comparison
  - IPv6 Extension Headers

- **IPv6 Addressing**
  - Addressing Format
  - Types of IPv6 addresses

- **ICMPv6 and Neighbor Discovery**
  - Router Solicitation & Advertisement
  - Neighbor Solicitation & Advertisement
  - Duplicate Address Detection

- **Multicast in IPv6**

- **DHCP & DNS for IPv6**
  - DNS with IPv6
  - DHCPv6 Overview
Tutorial-2: Agenda

- Routing in IPv6
  - RIPng
  - OSPFv3
  - BGP-4 Extensions for IPv6
  - Multi-Topology IS-IS

- Tunneling
  - Automatic 6 to 4 Tunnels
  - ISATAP

- IPv6 for DOCSIS Overview
  - IPv6 Drivers in Broadband Access Networks
  - CMTS & CM Requirements for IPv6
  - MSO CPE Address Assignment Strategies
IPv6 Routing
Routing in IPv6

- As in IPv4, IPv6 has 2 families of routing protocols: IGP and EGP, and still uses the longest-prefix match routing algorithm

- IGP
  - RIPng
  - Integrated IS-IS for IPv6
  - OSPFv3 (RFC 2740)

- EGP:
  - MP-BGP4
RIPng (RFC 2080)
Similar characteristics as IPv4
- Distance-vector, hop limit of 15, split-horizon, multicast based (FF02::9), UDP port (521) etc.

Updated features for IPv6
- IPv6 prefix & prefix length

Special Handling for the NH
- Route tag and prefix length for NH is all 0. Metric will have 0xFF; NH must be link local
OSPFv3 (RFC 2740)
OSPFv3 and OSPFv2 Differences

- Protocol processing per-link, not per-subnet
- Addition of Flooding scope
  - Three flooding scopes have been introduced: link-local, area, and AS
- Explicit support for multiple instances per link
  - This allows for separate ASes, each running OSPF, to use a common link
  - Single link can belong to multiple areas
- Use of IPv6 link-local addresses
- Authentication method changes
  - The authentication of OSPF for IPv4 has been removed.
- Handling of unknown LSA types
  - A new LSA handling bit has been added to the LS Type field to allow flooding of unknown LSA types
## OSPFv3 and OSPFv2 Similarities

<table>
<thead>
<tr>
<th>packet type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hello</td>
</tr>
<tr>
<td>2</td>
<td>Database Description</td>
</tr>
<tr>
<td>3</td>
<td>Link State Request</td>
</tr>
<tr>
<td>4</td>
<td>Link State Update</td>
</tr>
<tr>
<td>5</td>
<td>Link State Acknowledgment</td>
</tr>
</tbody>
</table>

- OSPFv3 has the same 5 packet type but some fields have been changed.
- Mechanisms for neighbor discovery and adjacency formation
- Interface types
  - P2P, P2MP, Broadcast, NBMA, Virtual
- LSA flooding and aging
- Nearly identical LSA types
# OSPFv3 and OSPFv2 header comparison

<table>
<thead>
<tr>
<th>Version</th>
<th>Type</th>
<th>Packet Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Router ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Area ID</td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td>Autype</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Type</th>
<th>Packet Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Router ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Area ID</td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td>Instance ID</td>
<td>0</td>
</tr>
</tbody>
</table>

- Size of the header is reduced from 24 bytes to 16
- Router ID & Area ID are still a 32 bit numbers
- Instance ID is a new field that is used to have multiple OSPF process' instance per link. In order for 2 instances talk to each other they need to have the same instance ID. By default it is 0 and for any additional instance it is increased, Instance ID has local link significance only
- Authentication fields have been suppressed – RFC 4552 talks about the authentication implementation in OSPFv3
BGP-4 Extensions for IPv6 (RFC 2545)
BGP-4 Extensions for IPv6

- The IPv6 support derives from the capability of BGP-4 to exchange information about network layer protocols other than IPv4.

- To make BGP-4 available for other network layer protocols, RFC 2858 (obsoletes RFC 2283) defines multi-protocol extensions for BGP-4:
  - Enables BGP-4 to carry information of other protocols e.g. MPLS, IPv6
  - New BGP-4 optional and non-transitive attributes:
    - MP_REACH_NLRI
    - MP_UNREACH_NLRI

- To establish a BGP connection exchanging IPv6 prefixes, the peering routers need to advertise the optional parameter BGP capability to indicate IPv6 support.
BGP-4 Extensions for IPv6

- New optional and non-transitive BGP attributes:
  - MP_REACH_NLRI (Attribute code: 14)
    “Carry the set of reachable destinations together with the next-hop information to be used for forwarding to these destinations” (RFC2858)
  - MP_UNREACH_NLRI (Attribute code: 15)
    Carry the set of unreachable destinations

- Attribute 14 and 15 contains one or more Triples:
  - Address Family Information (AFI)
  - Next-Hop Information (must be of the same address family)
  - NLRI
BGP-4 Extensions for IPv6

- Address Family Identifier (AFI) for IPv6
  - AFI = 2 (RFC 1700)
  - Sub-AFI = 1 Unicast
  - Sub-AFI = 2 (Multicast for RPF check)
  - Sub-AFI = 3 for both Unicast and Multicast
  - Sub-AFI = 4 Label
  - Sub-AFI = 128 VPN
BGP-4 Extensions for IPv6

- **TCP Interaction**
  - BGP-4 runs on top of TCP
  - This connection could be setup either over IPv4 or IPv6

- **Router ID**
  - When no IPv4 is configured, an explicit bgp router-id needs to be configured
  - This is needed as a BGP Identifier, this is used as a tie breaker, and is send within the OPEN message
ISIS for IPv6
IS-IS for IPv6

- 2 Type/Length/Values added to introduce IPv6 routing
- IPv6 Reachability TLV (0xEC)
  - External bit
  - Equivalent to IP Internal/External Reachability TLV’s
- IPv6 Interface Address TLV (0xE8)
  - For Hello PDUs, must contain the Link-Local address
  - For LSP, must only contain the non-Link Local address
- IPv6 NLPID (0x8E) is advertised by IPv6 enabled routers
Multi-Topology IS-IS Extensions

- Mechanism that allows IS-IS, used within a single domain, to maintain a set of independent IP topologies
- Multi-Topologies extension can be used to maintain separate topologies for:
  - IPv4
  - IPv6
  - Multicast
- Topologies need not be congruent (of course)
Maintaining MT Adjacencies

- Each adjacency formed MUST be classified as belonging to a set of MTs on the interface.
- MT membership advertised in IIH packets
- Boundaries between levels will be the same for all MTs.
The Multi-Topology software will create two topologies inside Area for IPv4 and IPv6. IPv4-only routers will be excluded from the IPv6 topology.
Tunneling
Tunneling

- There are two general types of tunneling
  - Manually configured tunneling of IPv6 over IPv4
    - IPv6 packets are encapsulated in IPv4 packets to be carried over IPv4 routing infrastructures.
    - These are point-to-point tunnels that need to be configured manually
  - Automatic tunneling of IPv6 over IPv4
    - IPv6 nodes can use different types of addresses, such as 6 to 4 or ISATAP addresses, to dynamically tunnel IPv6 packets over an IPv4 routing infrastructure.
    - These special IPv6 unicast addresses carry an IPv4 address in some parts of the IPv6 address fields.
6 to 4 Tunneling
Automatic 6 to 4 Tunnels

- Automatic 6to4 tunnel allows isolated IPv6 domains to connect over an IPv4 network
- Unlike the manual 6to4 the tunnels are not point-to-point, they are multipoint tunnels
- IPv4 is embedded in the IPv6 address is used to find the other end of the tunnel
- Address format is 2002:<IPv4 address>::
IPv4 Host B
IPv6 Host A
IPv4 Network
IPv6 Network
IPv4
IPv6
Network Prefix: 2002:c0a8:6301::/48
Network Prefix: 2002:c0a8:1e01::/48

Automatic 6to4 Tunnel (RFC 3056)

6to4:
- Is an automatic tunnel method
- Gives a prefix to the attached IPv6 network

<table>
<thead>
<tr>
<th>2002</th>
<th>Public IPv4 Address</th>
<th>SLA</th>
<th>Interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>/16</td>
<td>/48</td>
<td>/64</td>
<td></td>
</tr>
</tbody>
</table>
Automatic 6to4 Tunnel (RFC 3056)

IPv6 Host A
IPv6 Network
2002:c0a8:6301::1

6to4 Router
192.168.99.1

Tunnel: IPv6 in IPv4 Packet

IPv6 Host B
IPv6 Network
2002:c0a8:1e01::2

IPv4
192.168.30.1

S=2002:c0a8:6301::1
D=2002:c0a8:1e01::2

IPv4 Header
IPv6 Header
IPv6 Data

S(v4)=192.168.99.1
D(v4)=192.168.30.1
S(v6)=2002:c0a8:6301::1
D(v6)=2002:c0a8:1e01::2
Automatic 6to4 Relay

6to4 Relay:

- Is a gateway to the rest of the IPv6 Internet
- Is a default router
ISATAP Tunneling
Intrasite Automatic Tunnel Address Protocol

- RFC 4214
- This is for enterprise networks such as corporate and academic networks
- Scalable approach for incremental deployment
- ISATAP makes your IPv4 infrastructure as transport (NBMA) network
Intrasite Automatic Tunnel Address Protocol

- RFC 4214
- To deploy a router is identified that carries ISATAP services
- ISATAP routers need to have at least one IPv4 interface
- DNS entries are created for each of the ISATAP routers’ IPv4 addresses
- Hosts will automatically discover ISATAP routers and can get access to global IPv6 network
- Host can apply the ISATAP service before all this operation but its interface will only have a link local v6 address until the first router appears
Intrasite Automatic Tunnel Address Protocol

Use IANA's OUI 00-00-5E and Encode IPv4 Address as Part of EUI-64

- ISATAP is used to tunnel IPv4 within an administrative domain (a site) to create a virtual IPv6 network over a IPv4 network
- Supported in Windows XP Pro SP1 and others
Automatic Address Assignment of Host and Router

- ISATAP host A receives the ISATAP prefix `2001:db8:ffff:2`/64 from ISATAP Router 1.

- When ISATAP host A wants to send IPv6 packets to `2001:db8:ffff:2::5efe:ce7b:1fc8`, ISATAP host A encapsulates IPv6 packets in IPv4. The IPv4 packets of the IPv6 encapsulated packets use IPv4 source and destination address.
IPv6 in DOCSIS 3.0
To Internet

Management prefix: 2001:DB8:FFFF:0::/64
Service prefix: 2001:DB8:FFFE:0::/64
Customer 2 prefix: 2001:DB8:2::/48
Customer 3 prefix: 2001:DB8:3::/48

HFC link; assigned 2001:DB8:FFFF:0::/64 (mgmt) and 2001:DB8:FFFE:0::/64 (service)
Customer 2 premises link; assigned 2001:DB8:2:1::/64
Customer 3 premises link; assigned 2001:DB8:3:1::/64

Routers span customer and MSO administrative domains
HFC link; assigned 2001:DB8:FFFF:0::/64 (mgmt) and 2001:DB8:FFFE:0::/64 (service)
Customer 3 premises link 0; assigned 2001:DB8:3:0::/64
Customer 3 premises link 1; assigned 2001:DB8:3:1::/64
Customer 3 premises link 2; assigned 2001:DB8:3:2::/64

CM router receives 2001:DB8:3::/48 through prefix delegation; assigns /64 prefixes from 2001:DB8:3::/48 to customer network links
IPv6 Features in DOCSIS 3.0

- Customer will have premises network, not individual CPEs on HFC
  - “Lightweight router” function to be defined as eSAFE function
  - Customer will be assigned /48 prefix for sub-delegation within premises network

- CM can be provisioned and managed exclusively through IPv6
  - Relieves pressure on IPv4 address space
  - Customer can still receive IPv4 service (dual-stack network)

- HFC may have management prefix for CMs and managed CPEs, and service prefix for data service

- DHCPv6 used for address assignment to meet MSO requirement for IPv6 address control

- Fields, options and sub-options from DHCPv4 redefined as vendor-specific options in DHCPv6