UNIT - II

 U2.1

Learning Objectives

- Overview of IP Address
- Discuss IPv4 And IPV6
- Different Types of IPV6 Addresses
- Overview of ATM
- ATM Layered Architecture

 U2.2

IPV6

IPv6 Features - The following are the features of the IPv6 protocol:

- New header format
- Large address space
- Efficient and hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Built-in security
- Better support for prioritized delivery
- New protocol for neighboring node interaction
- Extensibility

 U2.3

IPV6

New Header Format

- The IPv6 header has a new format that is designed to keep header overhead to a minimum.
- This is achieved by moving both non-essential fields and optional fields to extension headers that are placed after the IPv6 header.
- The streamlined IPv6 header is more efficiently processed at intermediate routers.
- IPv4 headers and IPv6 headers are not interoperable. IPv6 is not a superset of functionality that is backward compatible with IPv4.
- A host or router must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats

IPV6

Large Address Space

- IPv6 has 128-bit (16-byte) source and destination IP addresses.
- Although 128 bits can express over 3.4´10^{38} possible combinations, the large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization.
- Even though only a small number of the possible addresses are currently allocated for use by hosts, there are plenty of addresses available for future use.

IPV6

Efficient and Hierarchical Addressing and Routing Infrastructure

- IPv6 global addresses used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical, and summarizable routing infrastructure that is based on the common occurrence of multiple levels of Internet service providers.

IPV6

Stateless and Stateful Address Configuration

- To simplify host configuration, IPv6 supports both stateful address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration (address configuration in the absence of a DHCP server).
- With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses) and with addresses derived from prefixes advertised by local routers.
- Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration

IPV6

Better Support for Prioritized Delivery

- New fields in the IPv6 header define how traffic is handled and identified.
- Traffic identification using a Flow Label field in the IPv6 header allows routers to identify and provide special handling for packets belonging to a flow, a series of packets between a source and destination.
- Because the traffic is identified in the IPv6 header, support for prioritized delivery can be achieved even when the packet payload is encrypted with IPsec.

IPV6

New Protocol for Neighboring Node Interaction

- The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes (nodes on the same link).
- Neighbor Discovery replaces the broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages.

IPV6

Extensibility

- IPv6 can easily be extended for new features by adding extension headers after the IPv6 header.
- Unlike options in the IPv4 header, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet.

 U2.10

IPV6

The IPv6 Address Space

- The most obvious distinguishing feature of IPv6 is its use of much larger addresses.
- The size of an address in IPv6 is 128 bits, which is four times the larger than an IPv4 address.
- A 32-bit address space allows for 2^{32} or 4,294,967,296 possible addresses. A 128-bit address space allows for 2^{128} or 340,282,366,920,938,463,463,374,607,431,768, 211,456 (or 3.4´10^{38} or 340 undecillion) possible addresses.

 U2.11

IPV6

- IPv4 addresses are represented in dotted-decimal format. This 32-bit address is divided along 8-bit boundaries. Each set of 8 bits is converted to its decimal equivalent and separated by periods.
- For IPv6, the 128-bit address is divided along 16-bit boundaries, and each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons. The resulting representation is called colon-hexadecimal.
- The following is an IPv6 address in binary form:

  0010000000000001000011011011100000000000000000000000101110011101100000010101010100000000 111
  1111111111110001010001001110001011010

 U2.12

IPV6

- The 128-bit address is divided along 16-bit boundaries:
  0010000000000001 0000110110111000
  0000000000000000 0010111100111011
  0000001010101010 0000000011111111
  1111111000101000 1001110001011010
- Each 16-bit block is converted to hexadecimal and delimited with colons. The result is:
- 2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A
- IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. With leading zero suppression, the address representation becomes:
- 2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

 U2.13

IPV6

Compressing Zeros

- Some types of addresses contain long sequences of zeros. To further simplify the representation of IPv6 addresses, a contiguous sequence of 16-bit blocks set to 0 in the colon hexadecimal format can be compressed to "::", known as *double-colon*.
- For example,
- the link-local address of FE80:0:0:0:2AA:FF:FE9A:4CA2 can be compressed to FE80::2AA:FF:FE9A:4CA2.
- The multicast address FF02:0:0:0:0:0:0:2 can be compressed to FF02::2.

 U2.14

IPV6

- Zero compression can only be used to compress a single contiguous series of 16-bit blocks expressed in colon hexadecimal notation.
- You cannot use zero compression to include part of a 16-bit block.
- For example, you cannot express FF02:30:0:0:0:0:0:5 as FF02:3::5. The correct representation is FF02:30::5.

 U2.15

IPV6

- To determine how many 0 bits are represented by the "::", you can count the number of blocks in the compressed address, subtract this number from 8, and then multiply the result by 16.
- For example, in the address FF02::2, there are two blocks (the "FF02" block and the "2" block.) The number of bits expressed by the "::" is 96 (96 = (8 – 2)×16).

 U2.16

IPV6

Types of IPv6 Addresses There are three types of IPv6 addresses:

Unicast –

- A unicast address identifies a single interface within the scope of the type of unicast address.
- With the appropriate unicast routing topology, packets addressed to a unicast address are delivered to a single interface.

 U2.17

IPV6

Multicast –

- A multicast address identifies multiple interfaces.
- With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address.
- A multicast address is used for one-to-many communication, with delivery to multiple interfaces.

 U2.18

IPV6

Anycast –

- An anycast address identifies multiple interfaces.
- With the appropriate routing topology, packets addressed to an anycast address are delivered to a single interface, the nearest interface that is identified by the address.
- The “nearest” interface is defined as being closest in terms of routing distance. An anycast address is used for one-to-one-of-many communication, with delivery to a single interface.

IPV6

Unicast IPv6 Addresses The following types of addresses are unicast IPv6 addresses:

- Global unicast addresses
- Link-local addresses
- Site-local addresses
- Unique local IPv6 unicast addresses
- Special addresses

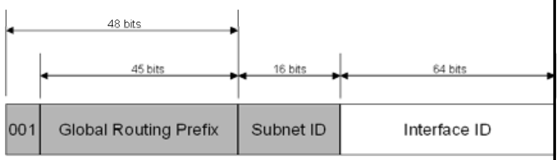
IPV6

Global Unicast Addresses

- Global unicast addresses are equivalent to public IPv4 addresses.
- They are globally routable and reachable on the IPv6 portion of the Internet.
- Unlike the current IPv4-based Internet, which is a mixture of both flat and hierarchical routing, the IPv6-based Internet has been designed from its foundation to support efficient, hierarchical addressing and routing.

IPV6

- The fields in the global unicast address are the following:
- **Fixed portion set to 001** – The three high-order bits are set to 001. The address prefix for currently assigned global addresses is 2000::/3.



IPV6

Global Routing Prefix –

- Indicates the global routing prefix for a specific organization's site.
- The combination of the three fixed bits and the 45-bit Global Routing Prefix is used to create a 48-bit site prefix, which is assigned to an individual site of an organization.
- Once assigned, routers on the IPv6 Internet forward IPv6 traffic matching the 48-bit prefix to the routers of the organization's site.

IPV6

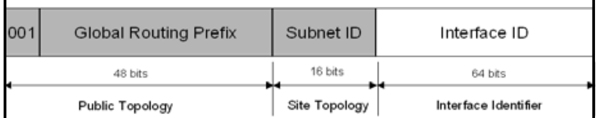
Subnet ID –

- The Subnet ID is used within an organization's site to identify subnets.
- The size of this field is 16 bits.
- The organization's site can use these 16 bits within its site to create 65,536 subnets or multiple levels of addressing hierarchy and an efficient routing infrastructure.

IPV6

- **Interface ID** – Indicates the interface on a specific subnet within the site. The size of this field is 64 bits.

The fields within the global unicast address create a three-level structure



•The public topology is the collection of larger and smaller ISPs that provide access to the IPv6 Internet.
•The site topology is the collection of subnets within an organization's site. The interface identifier identifies a specific interface on a subnet within an organization's site.

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U2.25

IPV6

Local-Use Unicast Addresses

There are two types of local-use unicast addresses:

- Link-local addresses are used between on-link neighbors and for Neighbor Discovery processes.
- Site-local addresses are used between nodes communicating with other nodes in the same site.

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U2.26

IPV6

Link-Local Addresses

- Link-local addresses are used by nodes when communicating with neighboring nodes on the same link. For example, on a single link IPv6 network with no router, link-local addresses are used to communicate between hosts.
- A link-local address is required for Neighbor Discovery processes and is always automatically configured, even in the absence of all other unicast addresses. e link.

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Vishal Jain U2.27

IPV6

10 bits	54 bits	64 bits
1111 1110 10	000 . . . 000	Interface ID

- Link-local addresses always begin with FE80. With the 64-bit interface identifier, the prefix for link-local addresses is always FE80::/64. An IPv6 router never forwards link-local traffic beyond the link.

IPV6

Site-Local Addresses

- Site-local addresses are equivalent to the IPv4 private address space (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16).
- For example, private intranets that do not have a direct, routed connection to the IPv6 Internet can use site-local addresses without conflicting with global unicast addresses.
- Site-local addresses are not reachable from other sites, and routers must not forward site-local traffic outside the site.
- Site-local addresses can be used in addition to global unicast addresses.

IPV6

10 bits	54 bits	64 bits
1111 1110 11	Subnet ID	Interface ID

- The first 10-bits are always fixed for site-local addresses (FEC0::/10).
- After the 10 fixed bits is a Subnet ID field that provides 54 bits with which you can create a hierarchical and summarizable routing infrastructure within the site.
- After the Subnet ID field is a 64-bit Interface ID field that identifies a specific interface on a subnet.

IPV6

Zone IDs for Local-Use Addresses

- Unlike global addresses, local-use addresses can be reused.
- Link-local addresses are reused on each link. Site-local addresses can be reused within each site of an organization.
- Because of this address reuse capability, link-local and site-local addresses are ambiguous.
- To specify which link on which an address is assigned or located or within which site an address is assigned or located, an additional identifier is needed.

 U2.31

IPV6

Unique Local IPv6 Unicast Addresses

- Site-local addresses provide a private addressing alternative to using global addresses for intranet traffic.
- However, because the site-local address prefix can be used to address multiple sites within an organization, a site-local address prefix address can be duplicated.
- The ambiguity of site-local addresses in an organization adds complexity and difficulty for applications, routers, and network managers.

 U2.32

IPV6

7 bits		40 bits	16 bits	64 bits
1111 110	L	Global ID	Subnet ID	Interface ID

- The first 7 bits have the fixed binary value of 1111110.
- All unique local addresses have the address prefix FC00::/7.
- The Local (L) flag is set 1 to indicate a local address.
- The L flag value set to 0 has not yet been defined.
- Therefore, unique local addresses with the L flag set to 1 have the address prefix of FD00::/8.
- The Global ID identifies a specific site within an organization and is set to a randomly derived 40-bit value.

 U2.33

IPV6

Special IPv6 Addresses

The following are special IPv6 addresses:

Unspecified address

- The unspecified address (0:0:0:0:0:0:0:0 or ::) is only used to indicate the absence of an address.
- It is equivalent to the IPv4 unspecified address of 0.0.0.0.
- The unspecified address is typically used as a source address for packets attempting to verify the uniqueness of a tentative address.
- The unspecified address is never assigned to an interface or used as a destination address.

 U2.34

IPV6

Loopback address

- The loopback address (0:0:0:0:0:0:0:1 or ::1) is used to identify a loopback interface, enabling a node to send packets to itself.
- It is equivalent to the IPv4 loopback address of 127.0.0.1.
- Packets addressed to the loopback address must never be sent on a link or forwarded by an IPv6 router.

 U2.35

IPV6

Multicast IPv6 Addresses

- In IPv6, multicast traffic operates in the same way that it does in IPv4.
- Arbitrarily located IPv6 nodes can listen for multicast traffic on an arbitrary IPv6 multicast address.
- IPv6 nodes can listen to multiple multicast addresses at the same time. Nodes can join or leave a multicast group at any time.

 U2.36

IPV6

8 bits	4 bits	4 bits	112 bits
1111 1111	Flags	Scope	Group ID

- IPv6 multicast addresses have the first eight bits set to 1111 1111.
- An IPv6 address is easy to classify as multicast because it always begins with “FF”.
- Multicast addresses cannot be used as source addresses or as intermediate destinations in a Routing extension header.

IPV6

Flags – Indicates flags set on the multicast address.

- The size of this field is 4 bits.
- The first low-order bit is the Transient (T) flag. When set to 0, the T flag indicates that the multicast address is a permanently assigned (well-known) multicast address allocated by IANA.
- When set to 1, the T flag indicates that the multicast address is a transient (non-permanently-assigned) multicast address.
- The second low-order bit is for the Prefix (P) flag, which indicates whether the multicast address is based on a unicast address prefix.

IPV6

Scope – Indicates the scope of the IPv6 internetwork for which the multicast traffic is intended.

- The size of this field is 4 bits. In addition to information provided by multicast routing protocols, routers use the multicast scope to determine whether multicast traffic can be forwarded.
- The most prevalent values for the Scope field are 1 (interface-local scope), 2 (link-local scope), and 5 (site-local scope).
- For example, traffic with the multicast address of FF02::2 has a link-local scope. An IPv6 router never forwards this traffic beyond the local link.

IPV6

Group ID – Identifies the multicast group and is unique within the scope.

- The size of this field is 112 bits.
- Permanently assigned group IDs are independent of the scope.
- Transient group IDs are only relevant to a specific scope.
- Multicast addresses from FF01:: through FF0F:: are reserved, well-known addresses.

IPV6

To identify all nodes for the interface-local and link-local scopes, the following addresses are defined:

- FF01::1 (interface-local scope all-nodes multicast address)
- FF02::1 (link-local scope all-nodes multicast address)

IPV6

To identify all routers for the interface-local, link-local, and site-local scopes, the following addresses are defined:

- FF01::2 (interface-local scope all-routers multicast address)
- FF02::2 (link-local scope all-routers multicast address)
- FF05::2 (site-local scope all-routers multicast address)

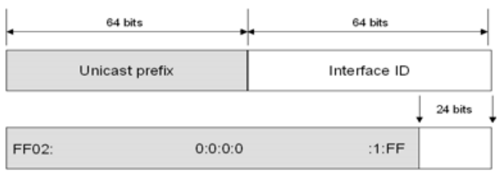
IPV6

Solicited-Node Address

- The solicited-node address facilitates the efficient querying of network nodes during address resolution.
- In IPv4, the ARP Request frame is sent to the MAC-level broadcast, disturbing all nodes on the network segment, including those that are not running IPv4.
- IPv6 uses the Neighbor Solicitation message to perform address resolution.
- However, instead of using the local-link scope all-nodes multicast address as the Neighbor Solicitation message destination, which would disturb all IPv6 nodes on the local link, the solicited-node multicast address is used.

 U2.43

IPV6



 U2.44

IPV6

Anycast IPv6 Addresses

- An anycast address is assigned to multiple interfaces.
- Packets addressed to an anycast address are forwarded by the routing infrastructure to the nearest interface to which the anycast address is assigned.
- In order to facilitate delivery, the routing infrastructure must be aware of the interfaces assigned anycast addresses and their "distance" in terms of routing metrics.
- At present, anycast addresses are only used as destination addresses and are only assigned to routers.

 U2.45

IPV6

- **IPv6 Header**
- The IPv6 header is a streamlined version of the IPv4 header. It eliminates fields that are unneeded or rarely used and adds fields that provide better support for real-time traffic.
- **Structure of an IPv6 Packet**

IPv6 Header	Extension Headers	Upper Layer Protocol Data Unit

← Payload → (Extension Headers + Upper Layer Protocol Data Unit)

← IPv6 Packet →

IPV6

- The IPv6 header and extension headers replace the existing IPv4 IP header with options.
- The new extension header format allows IPv6 to be augmented to support future needs and capabilities.
- Unlike options in the IPv4 header, IPv6 extension headers have no maximum size and can expand to accommodate all the extension data needed for IPv6 communication.

IPV6

IPv6 Header

- The IPv6 header is always present and is a fixed size of 40 bytes.

Extension Headers

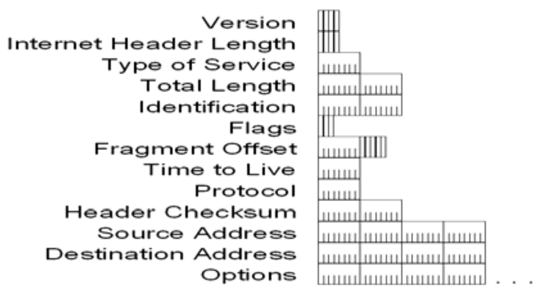
- Zero or more extension headers can be present and are of varying lengths.
- A Next Header field in the IPv6 header indicates the next extension header. Within each extension header is a Next Header field that indicates the next extension header.
- The last extension header indicates the upper layer protocol (such as TCP, UDP, or ICMPv6) contained within the upper layer protocol data unit.

IPV6

- **Upper Layer Protocol Data Unit**
- The upper layer protocol data unit (PDU) usually consists of an upper layer protocol header and its payload (for example, an ICMPv6 message, a UDP message, or a TCP segment).
- The IPv6 packet payload is the combination of the IPv6 extension headers and the upper layer PDU.
- Normally, it can be up to 65,535 bytes long.
- Payloads greater than 65,535 bytes in length can be sent using the Jumbo Payload option in the Hop-by-Hop Options extension header.

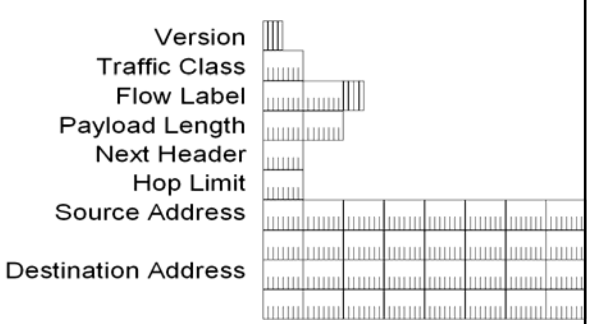
IPV6

- **IPv4 Header**



IPV6

- **IPv6 Header**



IPV6

- **IPv6 Header**
- **Version** – 4 bits are used to indicate the version of IP and is set to 6.
- **Traffic Class** – Like the IPv4 Type of Service field, specifies a DSCP values and flags for ECN. The size of this field is 8 bits.
- **Flow Label** – Indicates that this packet belongs to a specific sequence of packets between a source and destination, requiring special handling by intermediate IPv6 routers. The size of this field is 20 bits.

IPV6

Payload Length –

- Indicates the length of the IPv6 payload. The size of this field is 16 bits.
- The Payload Length field includes the extension headers and the upper layer PDU. With 16 bits, an IPv6 payload of up to 65,535 bytes can be indicated.
- For payload lengths greater than 65,535 bytes, the Payload Length field is set to 0 and the Jumbo Payload option is used in the Hop-by-Hop Options extension header.

IPV6

Next Header –

- Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6).
- The size of this field is 8 bits.
- When indicating an upper layer protocol above the Internet layer, the same values used in the IPv4 Protocol field are used here.

IPV6

Hop Limit –

- Indicates the maximum number of links over which the IPv6 packet can travel before being discarded. The size of this field is 8 bits.
- The Hop Limit is similar to the IPv4 TTL field except that there is no historical relation to the amount of time (in seconds) that the packet is queued at the router.
- When the Hop Limit equals 0, an ICMPv6 Time Exceeded message is sent to the source address and the packet is discarded.

Source Address –

- Stores the IPv6 address of the originating host. The size of this field is 128 bits.

 U2.55

IPV6

Destination Address –

- Stores the IPv6 address of the current destination host.
- The size of this field is 128 bits. In most cases the Destination Address is set to the final destination address.
- However, if a Routing extension header is present, the Destination Address might be set to the next router interface in the source route list.

 U2.56

IPV6

IPv6 Extension Headers

- The IPv4 header includes all options.
- Therefore, each intermediate router must check for their existence and process them when present.
- This can cause performance degradation in the forwarding of IPv4 packets.
- With IPv6, delivery and forwarding options are moved to extension headers.
- The only extension header that must be processed at each intermediate router is the Hop-by-Hop Options extension header.
- This increases IPv6 header processing speed and improves forwarding process performance.

 U2.57

IPV6

Following IPv6 extension headers that must be supported by all IPv6 nodes:

- Hop-by-Hop Options header
- Destination Options header
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header

IPV6

Extension Headers Order

Extension headers are processed in the order in which they are present. Extension headers be placed in the IPv6 header in the following order:

- Hop-by-Hop Options header
- Destination Options header (for intermediate destinations when the Routing header is present)
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header
- Destination Options header (for the final destination)

IPV6

Extension Headers Order

Extension headers are processed in the order in which they are present. Because the only extension header that is processed by every node on the path is the Hop-by-Hop Options header, it must be first. Extension headers be placed in the IPv6 header in the following order:

- Hop-by-Hop Options header
- Destination Options header (for intermediate destinations when the Routing header is present)
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header
- Destination Options header (for the final destination)

IPV6

Hop-by-Hop Options Header

- The Hop-by-Hop Options header is used to specify delivery parameters at each hop on the path to the destination. It is identified by the value of 0 in the IPv6 header's Next Header field.

Destination Options Header

- The Destination Options header is used to specify packet delivery parameters for either intermediate destinations or the final destination. This header is identified by the value of 60 in the previous header's Next Header field.

IPV6

The Destination Options header is used in two ways:

- If a Routing header is present, it specifies delivery or processing options at each intermediate destination.
- It specifies delivery or processing options at the final destination.

IPV6

Routing Header

- Similar to the loose source routing supported by IPv4, IPv6 source nodes can use the Routing extension header to specify a loose source route, a list of intermediate destinations for the packet to travel to on its path to the final destination.

- The Routing header is identified by the value of 43 in the previous header's Next Header field.

IPV6

Fragment Header

- The Fragment header is used for IPv6 fragmentation and reassembly services.

Authentication Header

- The Authentication header provides data authentication (verification of the node that sent the packet), data integrity (verification that the data was not modified in transit), and anti-replay protection (assurance that captured packets cannot be retransmitted and accepted as valid data) for the IPv6 packet.

IPV6

Encapsulating Security Payload Header and Trailer

- The Encapsulating Security Payload (ESP) header and trailer provide data confidentiality, data authentication, and data integrity services to the encapsulated payload.
- In contrast, the Authentication header provides data authentication and integrity services for the entire IPv6 packet.
- The ESP header and trailer are identified by the value of 50 in the previous header's Next Header field.

ICMP V6

The ICMPv6 protocol also provides a framework for the following:

- **Multicast Listener Discovery (MLD)** MLD is a series of three ICMPV6 messages that replace version 2 of the Internet Group Management Protocol (IGMP) for IPv4 to manage subnet multicast membership.
- **Neighbor Discovery (ND)** Neighbor Discovery is a series of five ICMPv6 messages that manage node-to-node communication on a link. Neighbor Discovery replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and the ICMPv4 Redirect message.

ICMP V6

There are two types of ICMPv6 messages:

Error messages

- Error messages are used to report errors in the forwarding or delivery of IPv6 packets by either the destination node or an intermediate router.
- The value of the 8-bit Type field in ICMPv6 error messages is in the range of 0 through 127 (the high order bit is set to 0).
- ICMPv6 error messages include Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.

ICMP V6

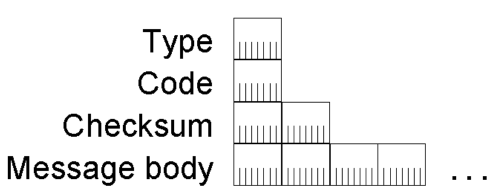
Informational messages

- Informational messages are used to provide diagnostic functions and additional host functionality such as MLD and Neighbor Discovery.
- The value of the Type field in ICMPv6 informational messages is in the range of 128 through 255 (the high order bit is set to 1).

ICMP V6

ICMPv6 Header

- An ICMPv6 header is indicated by setting the previous header's Next Header field to 58



ICMP V6

- **Type** – Indicates the type of ICMPv6 message. The size of this field is 8 bits. In ICMPv6 error messages, the high-order bit is set to 0. In ICMPv6 informational messages, the high-order bit is set to 1.
- **Code** – Differentiates among multiple messages within a given message type. The size of this field is 8 bits. If there is only one message for a given type, the Code field is set to 0.
- **Checksum** – Stores a checksum of the ICMPv6 message. The size of this field is 16 bits. The IPv6 pseudo-header is added to the ICMPv6 message when calculating the checksum.
- **Message body** – Contains ICMPv6 message-specific data.

ICMP V6

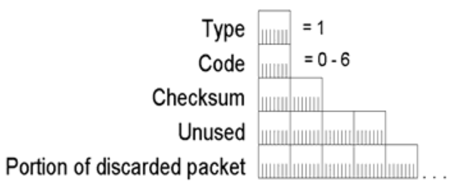
ICMPv6 Error Messages

- ICMPv6 error messages are used to report forwarding or delivery errors by either a router or the destination host.
- To conserve network bandwidth, ICMPv6 error messages are not sent for every error encountered. Instead, ICMPv6 error messages are rate limited.
- Rate limiting reduces the amount of bandwidth consumed by reporting errors.

.

ICMP V6

- **Destination Unreachable**
- An ICMPv6 Destination Unreachable message is sent by either a router or a destination host when the packet cannot be forwarded to its destination.



ICMP V6

In the Destination Unreachable message:-

- the Type field is set to 1 and the Code field is set to a value in the range of 0 through 4.
- After the Checksum field is the 32-bit Unused field and the portion of the discarded packet that makes the entire IPv6 packet containing the ICMPv6 message no larger than 1280 bytes (the minimum IPv6 MTU).
- The number of bytes of the discarded packet included in the message varies if there are IPv6 extension headers present.

 U2.73

ICMP V6

Code value - Description

- 0 - No route matching the destination was found in the routing table.
- 1 - The communication with the destination is prohibited by administrative policy. This is typically sent when the packet is discarded by a firewall.
- 2 - The address is beyond the scope of the source address.
- 3 - The destination address is unreachable. This is typically sent because of an inability to resolve the destination's link layer address.

 U2.74

ICMP V6

Code value - Description

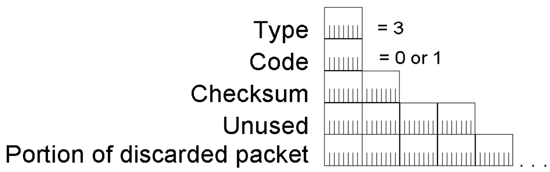
- 4 - The destination port was unreachable. This is typically sent when an IPv6 packet containing a UDP message arrived at the destination but there were no applications listening on the destination UDP port.
- 5 - The packet with this source address is not allowed due to inbound (ingress) or outbound (egress) packet filtering policies.
- 6 - The packet matched a reject route and was discarded. A reject route is an address prefix configured on a router for traffic that the router must immediately discard.

 U2.75

ICMP V6

Time Exceeded

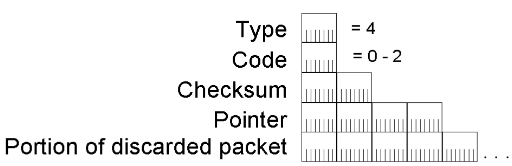
- An ICMPv6 Time Exceeded message is typically sent by a router when the Hop Limit field in the IPv6 header is zero, either upon receipt or after decrementing its value during the forwarding process.



ICMP V6

Parameter Problem

- An ICMPv6 Parameter Problem message is either sent by a router or by the destination. This occurs when an error is encountered in either the IPv6 header or an extension header, preventing IPv6 from performing further processing.



ICMP V6

Code value – Description

- 0 - An error in a field within the IPv6 header or an extension header was encountered.
- 1 - An unrecognized Next Header field value was encountered. This is equivalent to the IPv4 Destination Unreachable-Protocol Unreachable message.
- 2 - An unrecognized IPv6 option was encountered.

ICMP V6

ICMPv6 Informational Messages

Echo Request

- An ICMPv6 Echo Request message is sent to a destination to solicit an immediate Echo Reply message.
- The Echo Request/Echo Reply message facility provides a simple diagnostics function to aid in the troubleshooting of a variety of reachability and routing problems.

Echo Reply

- An ICMPv6 Echo Reply message is sent in response to the receipt of an ICMPv6 Echo Request message.

ICMP V6

Path MTU Discovery

- The path MTU is the smallest link MTU of any link in the path between a source and a destination.
- IPv6 packets with a maximum size of the path MTU do not require fragmentation by the host and will be successfully forwarded by all routers on the path.
- To discover the path MTU, the sending node uses the receipt of ICMPV6 Packet Too Big messages.

ICMP V6

The path MTU is discovered through the following process:

1. The sending node assumes that the path MTU is the link MTU of the interface on which the traffic is being forwarded.
2. The sending node sends IPv6 packets at the path MTU size.
3. If a router on the path is unable to forward the packet over a link with a link MTU that is smaller than the size of the packet, it discards the IPv6 packet and sends an ICMPV6 Packet Too Big message back to the sending node. The ICMPV6 Packet Too Big message contains the link MTU of the link on which the forwarding failed.
4. The sending node sets the path MTU for packets being sent to the destination to the value of the MTU field in the ICMPv6 Packet Too Big message.

ICMP V6

The sending node starts again at step 2 and repeats steps 2 through 4 for as many times as are necessary to discover the path MTU.

The path MTU is determined when either no additional ICMPv6 Packet Too Big messages are received or an acknowledgment is received from the destination.

ICMP V6

Multicast Listener Discovery

- Multicast Listener Discovery (MLD) is the IPv6 equivalent of Internet Group Management Protocol version 2 (IGMPv2) for IPv4.
- MLD is a set of messages exchanged by routers and nodes, enabling routers to discover the set of multicast addresses for which there are listening nodes for each attached interface.
- Like IGMPv2, MLD only discovers the list of multicast addresses for which there is at least one listener, not the list of individual multicast listeners for each multicast address.

ICMP V6

MLD Messages -

1. Multicast Listener Query

- Multicast Listener Query is used by a router to query a link for multicast listeners.
- There are two types of Multicast Listener Query messages: The General Query and the Multicast-Address-Specific Query.
- The General Query is used to query for multicast listeners of all multicast addresses.
- The Multicast-Address-Specific Query is used to query for multicast listeners of a specific multicast address.
- The two message types are distinguished by the multicast destination address in the IPv6 header and a multicast address within the Multicast Listener Query message.

ICMP V6

2. Multicast Listener Report

- Multicast Listener Report is used by a multicast listener to either report interest in receiving multicast traffic for a specific multicast address or to respond to a Multicast Listener Query.

3. Multicast Listener Done

- Multicast Listener Done is used by a multicast listener to report that it is no longer interested in receiving multicast traffic for a specific multicast address.

ICMP V6

Format of an MLD message packet.

IPv6 Header	Hop-by-Hop Options Header	MLD Message
Next Header = 0 (Hop-by-hop Options)	IPv6 Router Alert Option Next Header = 58 (ICMPv6)	

ICMP V6

- **Neighbor Discovery**
- IPv6 Neighbor Discovery (ND) is a set of messages and processes that determine relationships between neighboring nodes. ND replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4 and provides additional functionality.

ICMP V6

ND is used by hosts to:
- Discover neighboring routers.
- Discover addresses, address prefixes, and other configuration parameters.

ND is used by routers to:
- Advertise their presence, host configuration parameters, and on-link prefixes.
- Inform hosts of a better next-hop address to forward packets for a specific destination.

 U2.88

ICMP V6

ND is used by nodes to:
- Resolve the link-layer address of a neighboring node to which an IPv6 packet is being forwarded and determine when the link-layer address of a neighboring node has changed.
- Determine whether a neighbor is still reachable.

 U2.89

ICMP V6

IPv6 Neighbor Discovery Processes

- **Router discovery** The process by which a host discovers the local routers on an attached link. Equivalent to ICMPv4 Router Discovery.
- **Prefix discovery** The process by which hosts discover the network prefixes for local link destinations. Similar to the ICMPv4 Address Mask Request/Reply.
- **Parameter discovery** The process by which hosts discover additional operating parameters, including the link MTU and the default hop limit for outgoing packets.

 U2.90

ICMP V6

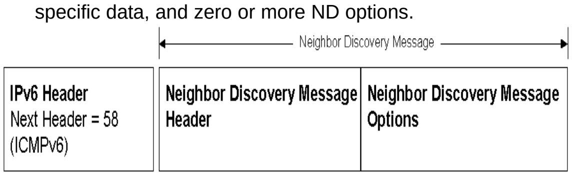
- **Address autoconfiguration** The process for configuring IP addresses for interfaces in either the presence or absence of a stateful address configuration server such as Dynamic Host Configuration Protocol version 6 (DHCPv6).
- **Address resolution** The process by which nodes resolve a neighbor's IPv6 address to its link-layer address. Equivalent to ARP in IPv4.
- **Next-hop determination** The process by which a node determines the IPv6 address of the neighbor to which a packet is being forwarded based on the destination address. The forwarding or next-hop address is either the destination address or the address of an on-link default router.

ICMP V6

- **Neighbor unreachability detection** The process by which a node determines that the IPv6 layer of a neighbor is no longer receiving packets.
- **Duplicate address detection** The process by which a node determines that an address considered for use is not already in use by a neighboring node. Equivalent to using gratuitous ARP frames in IPv4.
- **Redirect function** The process of informing a host of a better first-hop IPv6 address to reach a destination. Equivalent to the use of the IPv4 ICMP Redirect message.

ICMP V6

- **Neighbor Discovery Message Format** Like Multicast Listener Discovery (MLD) messages, ND messages use the ICMPv6 message structure and ICMPv6 types 133 through 137. ND messages consist of an ND message header, composed of an ICMPv6 header and ND message-specific data, and zero or more ND options.



ICMP V6

- IPv6 Neighbor Discovery Option Types

Type	Option Name
1	Source Link-Layer Address
2	Target Link-Layer Address
3	Prefix Information
4	Redirected Header
5	MTU

 U2.94

ICMP V6

Source/Target Link-Layer Address Option

- The **Source Link-Layer Address** option indicates the link-layer address of the ND message sender. The Source Link-Layer Address option is included in the Neighbor Solicitation, Router Solicitation, and Router Advertisement messages. The Source Link-Layer Address option is not included when the source address of the ND message is the unspecified address (::).
- The **Target Link-Layer Address** option indicates the link-layer address of the neighboring node to which IPv6 packets should be directed. The Target Link-Layer Address option is included in the Neighbor Advertisement and Redirect messages.

 U2.95

ICMP V6

Prefix Information Option

- The Prefix Information option is sent in Router Advertisement messages to indicate both address prefixes and information about address autoconfiguration. There can be multiple Prefix Information options included in a Router Advertisement message, indicating multiple address prefixes.

 U2.96

ICMP V6

Redirected Header Option

- The Redirected Header option is sent in Redirect messages to specify the IPv6 packet that caused the router to send a Redirect message. It can contain all or part of the redirected IPv6 packet, depending on the size of the IPv6 packet that was initially sent.

 U2.97

ICMP V6

MTU Option

- The MTU option is sent in Router Advertisement messages to indicate the IPv6 MTU of the link. This option is typically used only when the IPv6 MTU for a link is not well known or needs to be set due to a translational or mixed-media bridging configuration. The MTU option overrides the IPv6 MTU reported by the interface hardware.

 U2.98

ICMP V6

There are five different ND messages:

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

 U2.99

ICMP V6

Router Solicitation

- The Router Solicitation message is sent by IPv6 hosts to discover IPv6 routers present on the link. A host sends a multicast Router Solicitation to prompt IPv6 routers to respond immediately, rather than waiting for a periodic Router Advertisement message.

Router Advertisement

- IPv6 routers send the Router Advertisement message either periodically or in response to the receipt of a Router Solicitation message. It contains the information required by hosts to determine the link prefixes, the link MTU, whether or not to use address autoconfiguration, and the duration for which addresses created through address autoconfiguration are both valid and preferred.

 U2.100

ICMP V6

Neighbor Solicitation

- The Neighbor Solicitation message is sent by IPv6 hosts to discover the link-layer address of an on-link IPv6 node. It includes the link-layer address of the sender.

- Typical Neighbor Solicitations are multicast for address resolution and unicast when the reachability of a neighboring node is being verified.

 U2.101

ICMP V6

Neighbor Advertisement

- The Neighbor Advertisement message is sent by an IPv6 node in response to the receipt of a Neighbor Solicitation message.

- An IPv6 node also sends unsolicited Neighbor Advertisements to inform neighboring nodes of changes in link-layer addresses.

- The Neighbor Advertisement contains information required by nodes to determine the type of Neighbor Advertisement message, the link-layer address of the sender, and the sender's role on the network.

 U2.102

ICMP V6

Redirect

- The Redirect message is sent by an IPv6 router to inform an originating host of a better first-hop address for a specific destination.
- Redirect messages are only sent by routers for unicast traffic, are only unicast to originating hosts, and are only processed by hosts.

 U2.103

ICMP V6

Neighbor Discovery Processes

- The ND protocol provides message exchanges for the following processes:
- Address resolution (including duplicate address detection)
- Router discovery (includes prefix and parameter discovery)
- Neighbor unreachability detection
- Redirect function

 U2.104

ICMP V6

Address Autoconfiguration

- One of the most useful aspects of IPv6 is its ability to automatically configure itself, even without the use of a stateful configuration protocol such as Dynamic Host Configuration Protocol for IPv6 (DHCPv6).
- By default, an IPv6 host can configure a link-local address for each interface.
- By using router discovery, a host can also determine the addresses of routers, other configuration parameters, additional addresses, and on-link prefixes.
- Included in the Router Advertisement message is an indication of whether a stateful address configuration protocol should be used.

 U2.105

ICMP V6

Types of Autoconfiguration

There are three types of autoconfiguration:

- **Stateless -** Configuration of addresses is based on the receipt of Router Advertisement messages with the Managed Address Configuration and Other Stateful Configuration flags set to 0 and one or more Prefix Information options.

ICMP V6

- **Stateful -** Configuration is based on the use of a stateful address configuration protocol such as DHCPv6 to obtain addresses and other configuration options.
- A host uses stateful address configuration when it receives Router Advertisement messages with no prefix options where either the Managed Address Configuration flag or the Other Stateful Configuration flag is set to 1.
- A host will also use a stateful address configuration protocol when there are no routers present on the local link.

ICMP V6

- **Both -** Configuration is based on receipt of Router Advertisement messages with Prefix Information options and the Managed Address Configuration or Other Stateful Configuration flags set to 1.
- For all types, a link-local address is always configured.

ICMP V6

Autoconfiguration Process

The address autoconfiguration process for the physical interface of an IPv6 node is the following:

- A tentative link-local address is derived based on the link-local prefix of FE80::/64 and the 64-bit interface identifier.
- Using duplicate address detection to verify the uniqueness of the tentative link-local address, a Neighbor Solicitation message is sent with the Target Address field that is set to the tentative link-local address.

ICMP V6

- If a Neighbor Advertisement message sent in response to the Neighbor Solicitation message is received, this indicates that another node on the local link is using the tentative link-local address and address autoconfiguration stops. At this point, manual configuration must be performed on the node.
- If no Neighbor Advertisement message (sent in response to the Neighbor Solicitation message) is received, the tentative link-local address is assumed to be unique and valid. The link-local address is initialized for the interface. The corresponding solicited-node multicast link-layer address is registered with the network adapter.

ATM

- Introduction
- Architecture
- Switching
- ATM Layers

ATM

Asynchronous Transfer Mode (ATM) is an International Telecommunication Union-Telecommunications Standards Section (ITU-T) standard for cell relay wherein information for multiple service types, such as voice, video, or data, is conveyed in small, fixed-size cells. ATM networks are connection-oriented. Asynchronous transfer mode (ATM) is a technology that has its history in the development of broadband ISDN in the 1970s and 1980s.

ATM is designed for high-performance multimedia networking.

ATM integrates the multiplexing and switching functions, is well suited for bursty traffic (in contrast to circuit switching), and allows communications between devices that operate at different speeds.

 U2.112

ATM

- ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic).
- It provides scalable bandwidth from a few megabits per second (Mbps) to many gigabits per second (Gbps).
- Because of its asynchronous nature, ATM is more efficient than synchronous technologies, such as *time-division multiplexing (TDM)*.

 U2.113

ATM

The high-level benefits delivered through ATM services can be summarized as follows:

- Dynamic bandwidth for bursty traffic meeting application needs and delivering high utilization of networking resources; most applications are or can be viewed as inherently bursty, for example voice is bursty, as both parties are neither speaking at once nor all the time; video is bursty, as the amount of motion and required resolution varies over time.

 U2.114

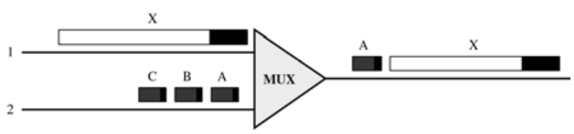
ATM

- Smaller header with respect to the data to make the efficient use of bandwidth.
- Can handle Mixed network traffic very efficiently: The variety of packet sizes make traffic unpredictable. All network equipments should incorporate elaborate software systems to manage the various sizes of packets. ATM handles these problems efficiently with the fixed size cell.
- Cell network: All data is loaded into identical cells that can be transmitted with complete predictability and uniformity.
- Class-of-service support for multimedia traffic allowing applications with varying throughput and latency requirements to be met on a single network.

 U2.115

ATM

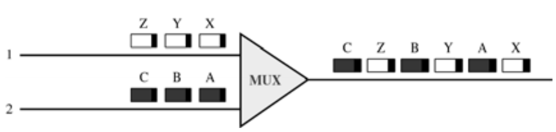
Multiplexing Using Different Packet Sizes



 U2.116

ATM

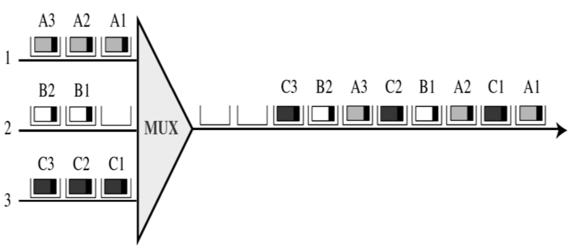
Multiplexing Using Cells



 U2.117

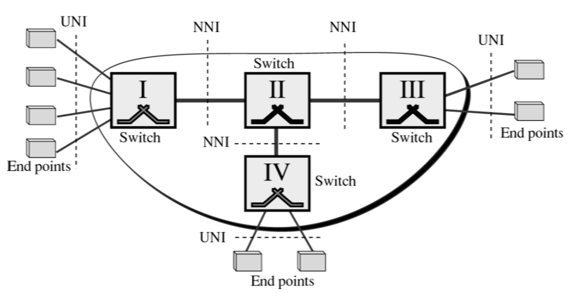
ATM

ATM Multiplexing



ATM

Architecture of an ATM Network



ATM

ATM Devices

- An ATM network is made up of an ATM switch and ATM endpoints. An ATM switch is responsible for cell transit through an ATM network.
- The job of an ATM switch is well defined. It accepts the incoming cell from an ATM endpoint or another ATM switch.
- It then reads and updates the cell header information and quickly switches the cell to an output interface towards its destination. An ATM endpoint (or end system) contains an ATM network interface adapter.
- Examples of ATM endpoints are workstations, routers, digital service units (DSUs), LAN switches, and video coder-decoders (Codec's).

ATM

ATM Network Interfaces

- An ATM network consists of a set of ATM switches interconnected by point-to-point ATM links or interfaces. ATM switches support two primary types of interfaces: UNI and NNI as shown in Fig.
- The UNI (User-Network Interface) connects ATM end systems (such as hosts and routers) to an ATM switch.
- The NNI (Network-Network Interface) connects two ATM switches.

ATM

- Depending on whether the switch is owned and located at the customer's premises or is publicly owned and operated by the telephone company, UNI and NNI can be further subdivided into public and private UNIs and NNIs.
- A private UNI connects an ATM endpoint and a private ATM switch. Its public counterpart connects an ATM endpoint or private switch to a public switch.
- A private NNI connects two ATM switches within the same private organization.
- A public one connects two ATM switches within the same public organization.

ATM

ATM Cell Format

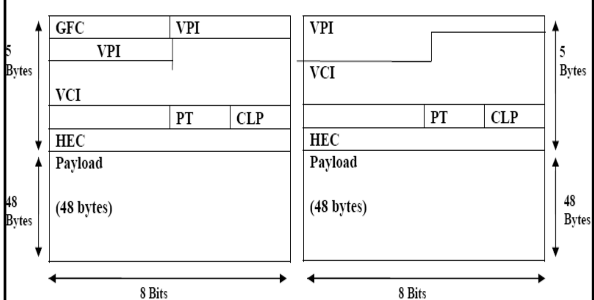
- ATM transfers information in fixed-size units called cells. Each cell consists of 53 octets, or bytes.
- The first 5 bytes contain cell-header information, and the remaining 48 contain the payload (user information).
- Small, fixed-length cells are well suited to transfer voice and video traffic because such traffic is intolerant to delays that result from having to wait for a large data packet to download, among other things.

ATM

- An ATM cell header can be one of two formats: UNI or NNI. The UNI header is used for communication between ATM endpoints and ATM switches in private ATM networks.
- The NNI header is used for communication between ATM switches. Figure depicts the ATM UNI cell header format, and the ATM NNI cell header format. Unlike the UNI, the NNI header does not include the Generic
- Flow Control (GFC) field. Additionally, the NNI header has a Virtual Path Identifier (VPI) field that occupies the first 12 bits, allowing for larger trunks between public ATM switches.

 U2.124

ATM



UNI Cell **NNI Cell**

 U2.125

ATM

The following descriptions summarize the ATM cell header fields shown in Fig.

Generic Flow Control (GFC)—Provides local functions, such as identifying multiple stations that share a single ATM interface. This field is typically not used and is set to its default value of 0 (binary 0000).

Virtual Path Identifier (VPI)—In conjunction with the VCI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.

 U2.126

ATM

Payload Type (PT)—Indicates in the first bit whether the cell contains user data or control data. If the cell contains user data, the bit is set to 0. If it contains control data, it is set to 1. The second bit indicates congestion (0 = no congestion, 1 = congestion), and the third bit indicates whether the cell is the last in a series of cells that represent a single AAL5 frame (1 = last cell for the frame).

Cell Loss Priority (CLP)—Indicates whether the cell should be discarded if it encounters extreme congestion as it moves through the network. If the CLP bit equals 1, the cell should be discarded in preference to cells with the CLP bit equal to 0.

 U2.127

ATM

Header Error Control (HEC)—Calculates checksum only on the first 4 bytes of the header. HEC can correct a single bit error in these bytes, thereby preserving the cell rather than discarding it.

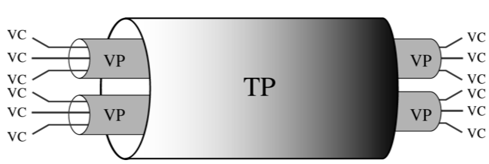
 U2.128

ATM

ATM standard defines two types of ATM connections:

virtual path connections (VPCs), which contain virtual channel connections (VCCs)

TP, VPs, and VCs



 U2.129

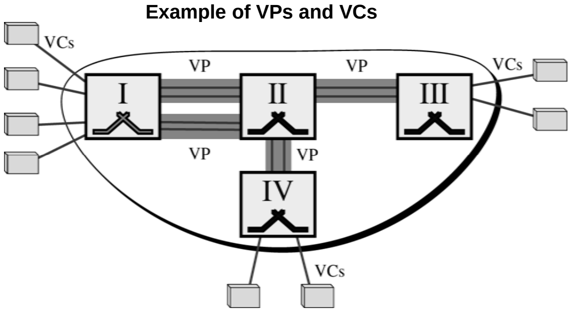
ATM

- A virtual channel connection (or virtual circuit) is the basic unit, which carries a single stream of cells, in order, from user to user.
- A collection of virtual circuits can be bundled together into a virtual path connection.
- A virtual path connection can be created from end-to-end across an ATM network.

 U2.130

ATM

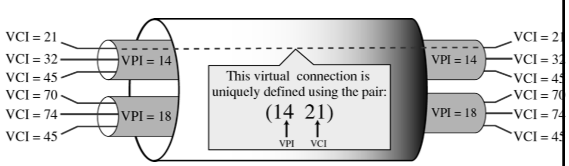
Example of VPs and VCs



 U2.131

ATM

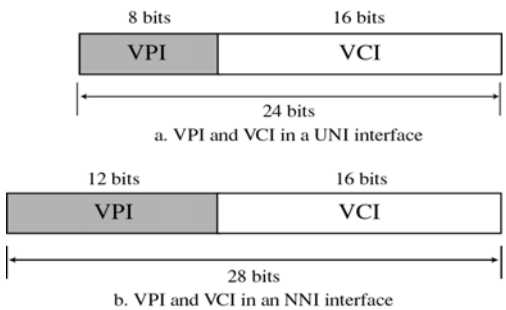
Connection Identifiers



 U2.132

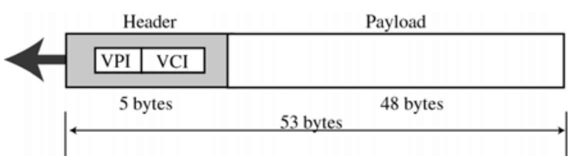
ATM

Virtual Connection Identifiers in UNIs and NNIs



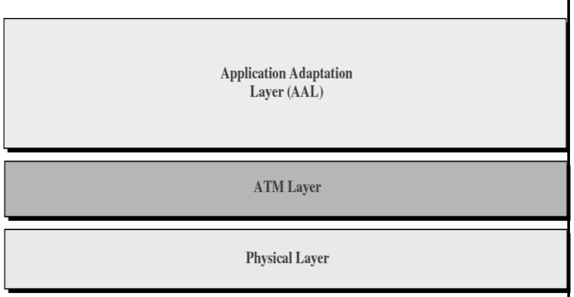
ATM

An ATM Cell



ATM

ATM Layers



ATM

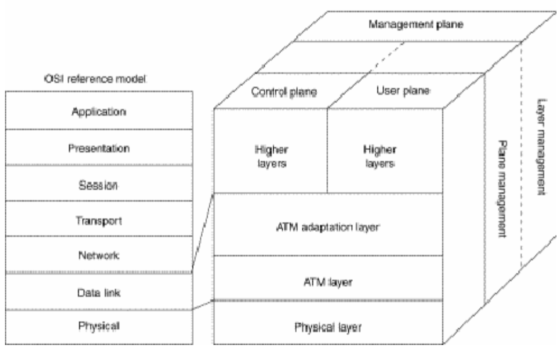
ATM Reference Model

The ATM architecture uses a logical model to describe the functionality that it supports. ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model.

- **Control—**This plane is responsible for generating and managing signaling requests.
- **User—**This plane is responsible for managing the transfer of data.
- **Management—This plane contains two components:**
- Layer management manages layer-specific functions, such as the detection of failures and protocol problems.
- Plane management manages and coordinates functions related to the complete system.

 U2.136

ATM



 U2.137

ATM

The ATM reference model consists of the following ATM layers:

Physical layer—Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.

ATM layer—Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.

 U2.138

ATM

ATM adaptation layer (AAL)—

- Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model.
- The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes.
- The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads.

 U2.139

ATM

The ATM Physical Layer

The main functions of the ATM physical layer are as follows:

- Cells are converted into a bit stream,
- The transmission and receipt of bits on the physical medium are controlled,
- ATM cell boundaries are tracked,
- Cells are packaged into the appropriate types of frames for the physical medium.

The ATM physical layer is divided into two parts: the physical medium-dependent (PMD) sub layer and the transmission convergence (TC) sub layer.

 U2.140

ATM

The PMD sub layer provides two key functions.

- It synchronizes transmission and reception by sending and receiving a continuous flow of bits with associated timing information.
- It specifies the physical media for the physical medium used, including connector types and cable.

 U2.141

ATM

The TC sub layer has four functions:

- Cell delineation, it maintains ATM cell boundaries, allowing devices to locate cells within a stream of bits.
- Generates and checks the header error control code to ensure valid data.
- Cell-rate decoupling, maintains synchronization and inserts or suppresses idle (unassigned) ATM cells to adapt the rate of valid ATM cells to the payload capacity of the transmission system.
- Transmission frame adaptation packages ATM cells into frames acceptable to the particular physical layer implementation.

ATM

ATM Layer

- The ATM layer provides routing, traffic management, switching and multiplexing services. It processes outgoing traffic by accepting 48-byte segment from the AAL sub-layers and transforming them into 53-byte cell by addition of a 5-byte header.

ATM

Adaptation Layers

- ATM adaptation layers allow existing packet networks to connect to ATM facilities.
- AAL Protocol accepts transmission from upper layer services (e.g.: packet data) and map them into fixed-sized ATM cells.
- These transmissions can be of any type, variable or fixed data rate.
- At the receiver, this process is reversed and segments are reassembled into their original formats and passed to the receiving services.
- Instead of one protocol for all types of data, the ATM standard divides the AAL layer into categories, each supporting the requirements of different types of applications.

ATM

- There are four types of data streams that are identified: Constant-bit rate, variable bit-rate, connection oriented packet data transfer, connectionless packet data transfer.
- In addition to dividing AAL by category (AAL1, AAL2 and so on), divides it on the basis of functionality.
- Each AAL layer is actually divided into two layers: the
  - **convergence sub-layer**
  - **Segmentation and reassembly (SAR) sub-layer.**

 U2.145

ATM

AAL1:

AAL1, a connection-oriented service, is suitable for handling constant bit rate sources (CBR), such as voice and videoconferencing.

AAL1 requires timing synchronization between the source and the destination. For this reason, AAL1 depends on a medium, such as SONET, that supports clocking.

 U2.146

ATM

The AAL1 process prepares a cell for transmission in three steps.

- First, synchronous samples (for example, 1 byte of data at a sampling rate of 200 microseconds) are inserted into the Payload field.
- Second, Sequence Number (SN) and Sequence Number Protection (SNP) fields are added to provide information that the receiving AAL1 uses to verify that it has received cells in the correct order.
- Third, the remainder of the Payload field is filled with enough single bytes to equal 48 bytes.

 U2.147

ATM

AAL1 : Quality of Service Parameter

Constant Bit rate (CBR)

- This class is used for emulating circuit switching. The cell rate is constant with time.
- CBR applications are quite sensitive to cell-delay variation.
- Examples of applications that can use CBR are telephone traffic (i.e., nx64 kbps), videoconferencing, and television.

 U2.148

ATM

AAL 2:

- The AAL2 process uses 44 bytes of the cell payload for user data and reserves 4 bytes of the payload to support the AAL2 processes.
- VBR traffic is characterized as either real-time (VBR-RT) or as non-real-time (VBR-NRT). AAL2 supports both types of VBR traffic.

 U2.149

ATM

AAL 2: Quality of Service Parameter

Variable Bit Rate - non-real time (VBR–NRT)

This class allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia e-mail is an example of VBR–NRT.

Variable bit rate–real time (VBR–RT)

This class is similar to VBR–NRT but is designed for applications that are sensitive to cell-delay variation. Examples for real-time VBR are voice with speech activity detection (SAD) and interactive compressed video.

 U2.150

ATM

AAL3/4:

- AAL3/4 supports both connection-oriented and connectionless data. AAL3/4 prepares a cell for transmission in four steps.
- First, the convergence sub layer (CS) creates a protocol data unit (PDU) by prepending a beginning/end tag header to the frame and appending a length field as a trailer.
- Second, the segmentation and reassembly (SAR) sub layer fragments the PDU and prepends a header to it.
- Then the SAR sub layer appends a CRC-10 trailer to each PDU fragment for error control.
- Finally, the completed SAR PDU becomes the Payload field of an ATM cell to which the ATM layer prepends the standard ATM header.

 U2.151

ATM

AAL3/4: Quality of Service Parameter

Connection oriented packet transfer Or available bit rate (ABR)

- This class of ATM services provides rate-based flow control and is aimed at data traffic such as file transfer and e-mail.
- Although the standard does not require the cell transfer delay and cell-loss ratio to be guaranteed or minimized, it is desirable for switches to minimize delay and loss as much as possible.
- Depending upon the state of congestion in the network, the source is required to control its rate.
- The users are allowed to declare a minimum cell rate, which is guaranteed to the connection by the network.

 U2.152

ATM

AAL 5:

- AAL5 is the primary AAL for data and supports both connection-oriented and connectionless data.
- It is used to transfer most non-SMDS data, such as classical IP over ATM and LAN Emulation (LANE).
- AAL5 also is known as the simple and efficient adaptation layer (SEAL)

 U2.153

ATM

AAL 5: Quality of Service Parameter

Connectionless data transfer or unspecified bit rate (UBR)
This class is the catch-all, other class and is widely used today for TCP/IP.

 U2.154

ATM

ATM Applications
ATM is used in both LANs and WANs

ATM WANs:

- ATM is basically a WAN technology that delivers cell over long distances.
- Here ATM is mainly used to connect LANs or other WANs together.
- router between ATM network and the other network serves as an end point.
- This router has two stacks of protocols: one belonging to ATM and other belonging to other protocol.

 U2.155

ATM

ATM LANs:

- High data rate (155 and 622 Mbps) of ATM technology attracted designers to think of implementing ATM technology in LANs too.
- At the surface level, to implement an ATM LAN ATM switch will replace the traditional Ethernet switch, in a switched LAN.
- But few things have to be kept in mind and software modules would be needed to map the following differences between the two technologies:

 U2.156

ATM

Connectionless versus connection-oriented:
ATM is a virtual connection oriented technology, while traditional Ethernet uses connectionless protocols.

Physical address versus virtual circuit identifier:
In the Traditional LAN packets are routed based on the source and destination addresses, while in ATM cells are routed based on the virtual circuit identifiers (VPI-VCI pair).

 U2.157

Summary

•To simplify host configuration, IPv6 supports both stateful address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration (address configuration in the absence of a DHCP server).

•IPv6 Neighbor Discovery (ND) is a set of messages and processes that determine relationships between neighboring nodes. ND replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4 and provides additional functionality.

 U2.158

Summary

•ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic).

•IPv6 Neighbor Discovery (ND) is a set of messages and processes that determine relationships between neighboring nodes. ND replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4 and provides additional functionality.

•The ATM architecture uses a logical model to describe the functionality that it supports. ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model.

 U2.159

Short Questions

1. Why we use IPV6?
2. What is the basic extension of IPV6?
3. Explain Quality of Service.
4. Describe the term neighbor discover.
5. Define auto-configuration with DHCP.
6. Difference between uncast and multicast routing.
7. How Tunneling works?
8. What do you mean by programming interface for IPV6.6 bone.
9. What are the responsibilities of AAL0?
10. What do you mean by Home Agent?
11. Explain care-of-address.

 U2.160

Long Questions

1. Explain Unicast, Multicast and Anycast address of IPV6.
2. Compare Header fields for IPV4 and IPV6 packet.
3. What are the different types of Neighbor Discovery process?
4. What are the different types of IPV6 extension Header? Explain its uses.
5. What are the different types of Error Messages and Query Messages is ICMPV6.
6. Explain Multi Cast Listener Discovery and its different message formats.
7. How Mobile IP works?

 U2.161

References

1. W. ER. Stevens, “TCP/IP illustrated, Volume 1: The protocols”, Addison Wesley, 1994.
2. G. R. Wright, “TCP/IP illustrated volume 2. The Implementation”, Addison Wesley,1995.
3. Forouzan, “TCP/IP Protocol Suite”, Tata Mc Grew Hill, 4th Ed., 2009.
4. William Stalling, “Cryptography and Network Security”, Pearson Publication.
5. James Martin, Joseph Lebin, Kavanagh Chapman “Asynchronous Transfer Model : ATM Architecture and Implementation”, Prentice Hall PTR, Facsimile Ed.

 U2.162