Planning for Information Network

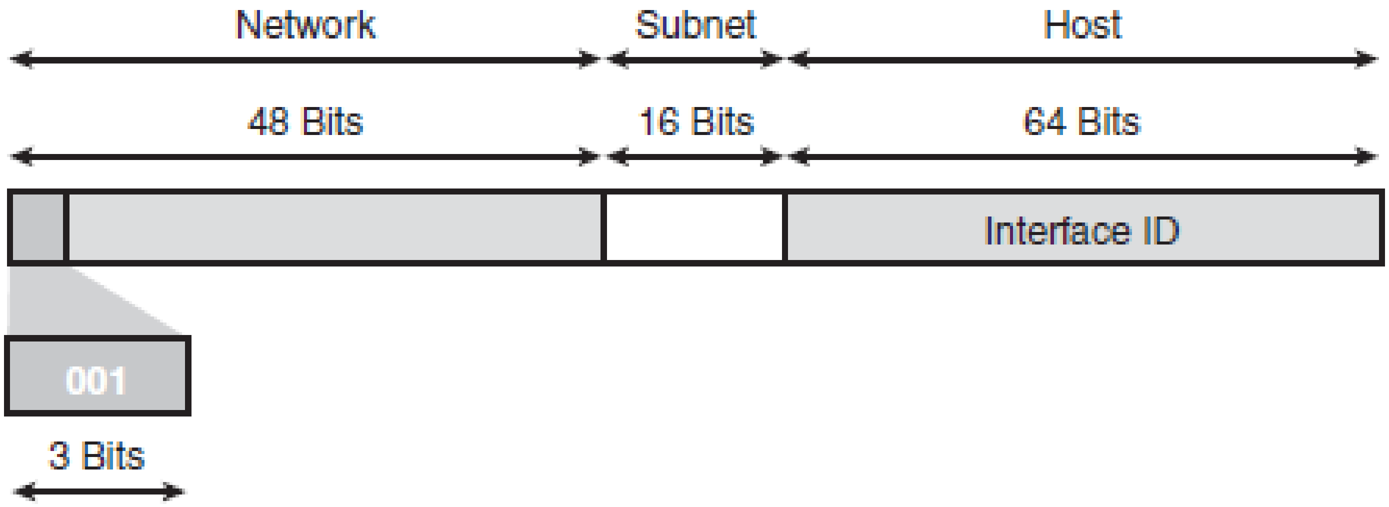
Lecture 8 and 9:

Introduction to IPv6

Global Aggregatable Unicast Addresses

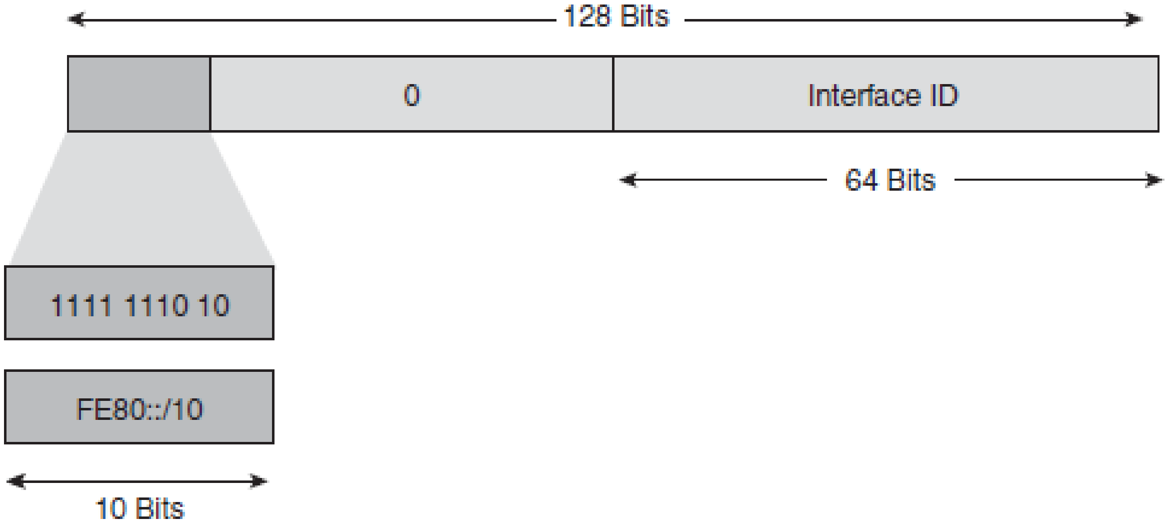
The subnet ID can be used by individual organizations to create their own local addressing hierarchy using subnets. This field allows an organization to use up to 65,536 individual subnets.

A fixed prefix of binary 2000::/3 (binary 001) indicates a global aggregatable IPv6 address; this is the current range of IPv6 global unicast addresses assigned by the Internet Assigned Numbers Authority (IANA).



Link-Local Unicast Addresses

A link-local address is useful only in the context of the local link network; its scope limits its relevance to only one link. A link-local address is an IPv6 unicast address that can be automatically configured on any interface by using the link-local prefix FE80::/10 (1111 1110 10) and the 64-bit interface identifier. Link-local addresses are used in the neighbor discovery protocol and the dynamic address assignment process.



Link-Local Unicast Addresses

A link-local unicast address connects devices on the same local network without requiring globally unique addresses.

When communicating with a link-local address, the outgoing interface must be specified, because every interface is connected to FE80::/10.

An IPv6 router must not forward packets that have either link-local source or destination addresses to other links.

IPv6 Address Assignment Strategies

As with IPv4, IPv6 allows two address assignment strategies:

Static and Dynamic

Static IPv6 Address Assignment

Static address assignment in IPv6 is the same as in IPv4—the administrator must enter the IPv6 address configuration manually on every device in the network.

Dynamic IPv6 Address Assignment

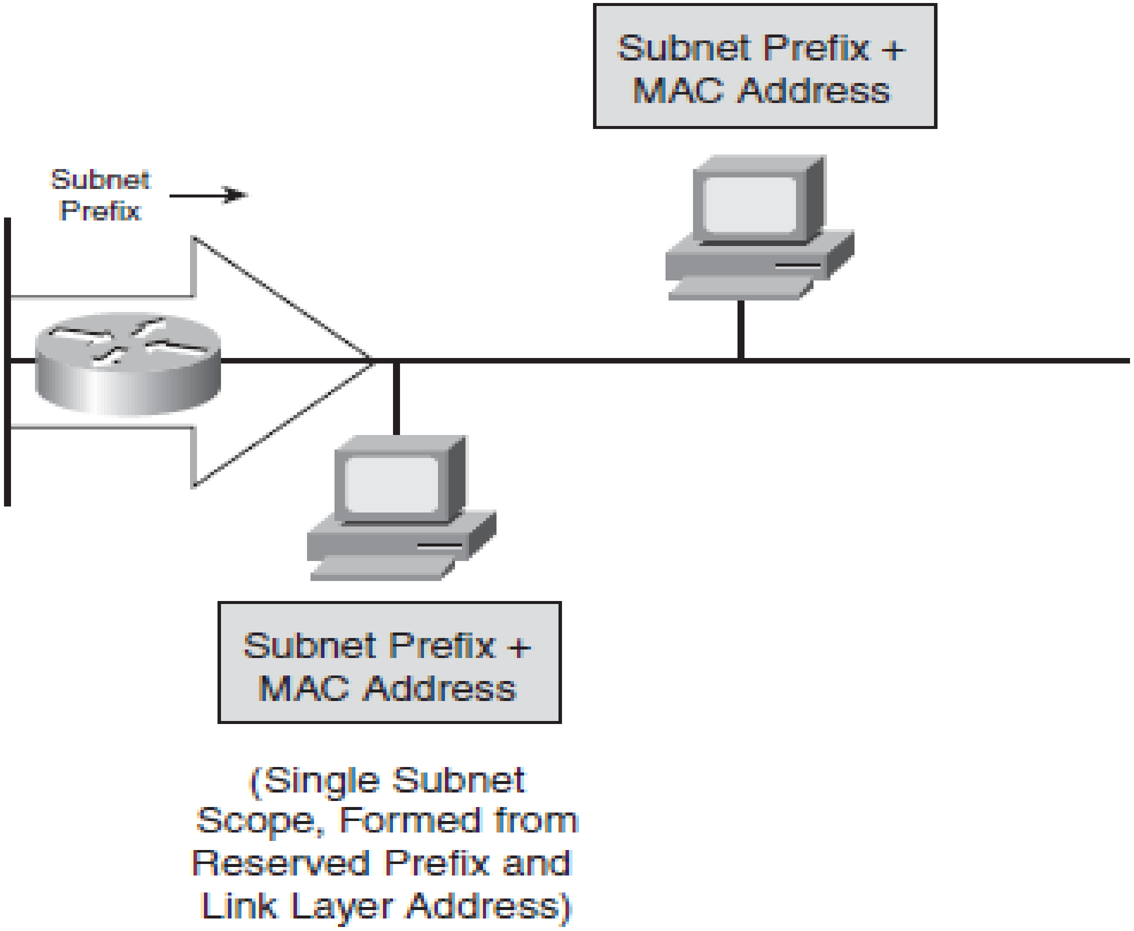
IPv6 dynamic address assignment strategies allow dynamic assignment of IPv6 addresses, as follows:

■ **Link-local address:** The host configures its own link-local address autonomously, using the link-local prefix FE80::0/10 and a 64-bit identifier for the interface, in an EUI-64 format.

■ **Stateless autoconfiguration:** A router on the link advertises—either periodically or at the host's request—network information, such as the 64-bit prefix of the local network and its willingness to function as a default router for the link. Hosts can automatically generate their global IPv6 addresses by using the prefix in these router messages; the hosts do not need manual configuration or the help of a device such as a DHCP server. For example, the following figure shows a host using the prefix advertised by the router as the top 64 bits of its address; the remaining 64 bits contain the host's 48-bit MAC address in an EUI-64 format.

Dynamic IPv6 Address Assignment

IPv6 Stateless Autoconfiguration Allows a Host to Automatically Configure Its IPv6 Address:



Subnet Prefix + MAC Address

Subnet Prefix →

Subnet Prefix + MAC Address

(Single Subnet Scope, Formed from Reserved Prefix and Link Layer Address)

Dynamic IPv6 Address Assignment

- **Stateful using DHCP for IPv6 (DHCPv6):** DHCPv6 is an updated version of DHCP for IPv4. DHCPv6 gives the network administrator more control than stateless autoconfiguration and can be used to distribute other information, including the address of the DNS server.

DHCPv6 can also be used for automatic domain name registration of hosts using a dynamic DNS server. **DHCPv6 uses multicast addresses.**

IPv4-to-IPv6 Transition Strategies and Deployments

Differences Between IPv4 and IPv6:

Regardless of which protocol is used, the communication between IPv4 and IPv6 domains must be transparent to end users. The major differences to consider between IPv4 and IPv6 include the following:

■ IPv4 addresses are 32 bits long, whereas IPv6 addresses are 128 bits long.

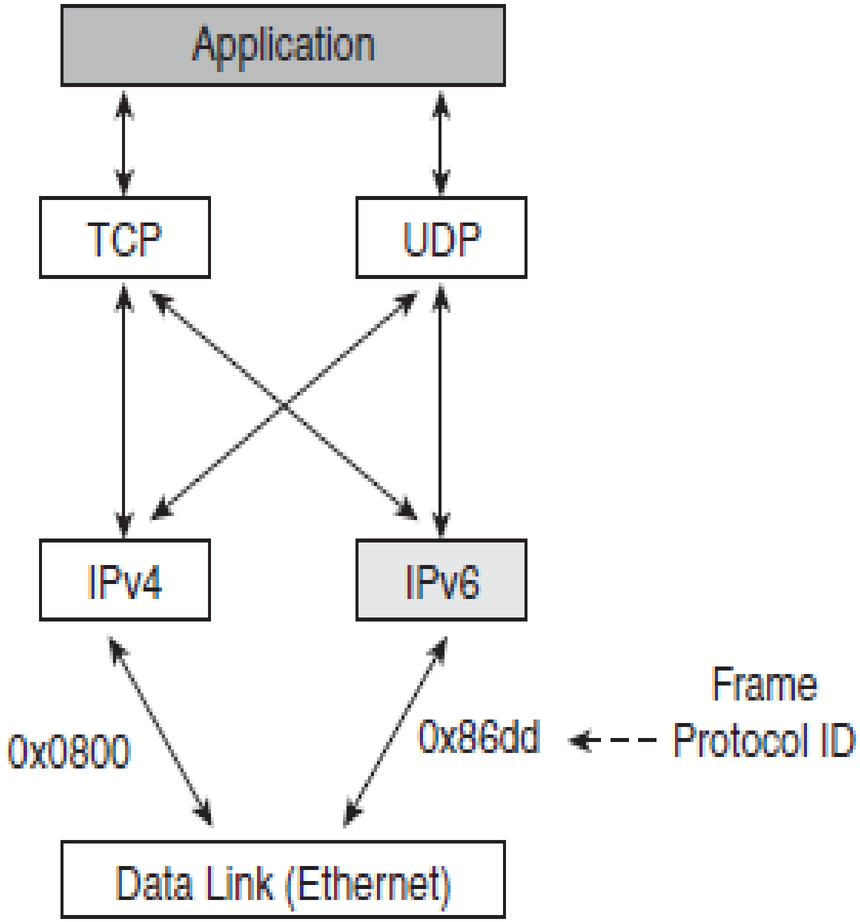
■ An IPv6 packet header is different from an IPv4 packet header. The IPv6 header is longer and simpler (new fields were added to the IPv6 header, and some old fields were removed).

■ IPv6 has no concept of broadcast addresses; instead, it uses multicast addresses.

■ Routing protocols must be changed to support native IPv6 routing.

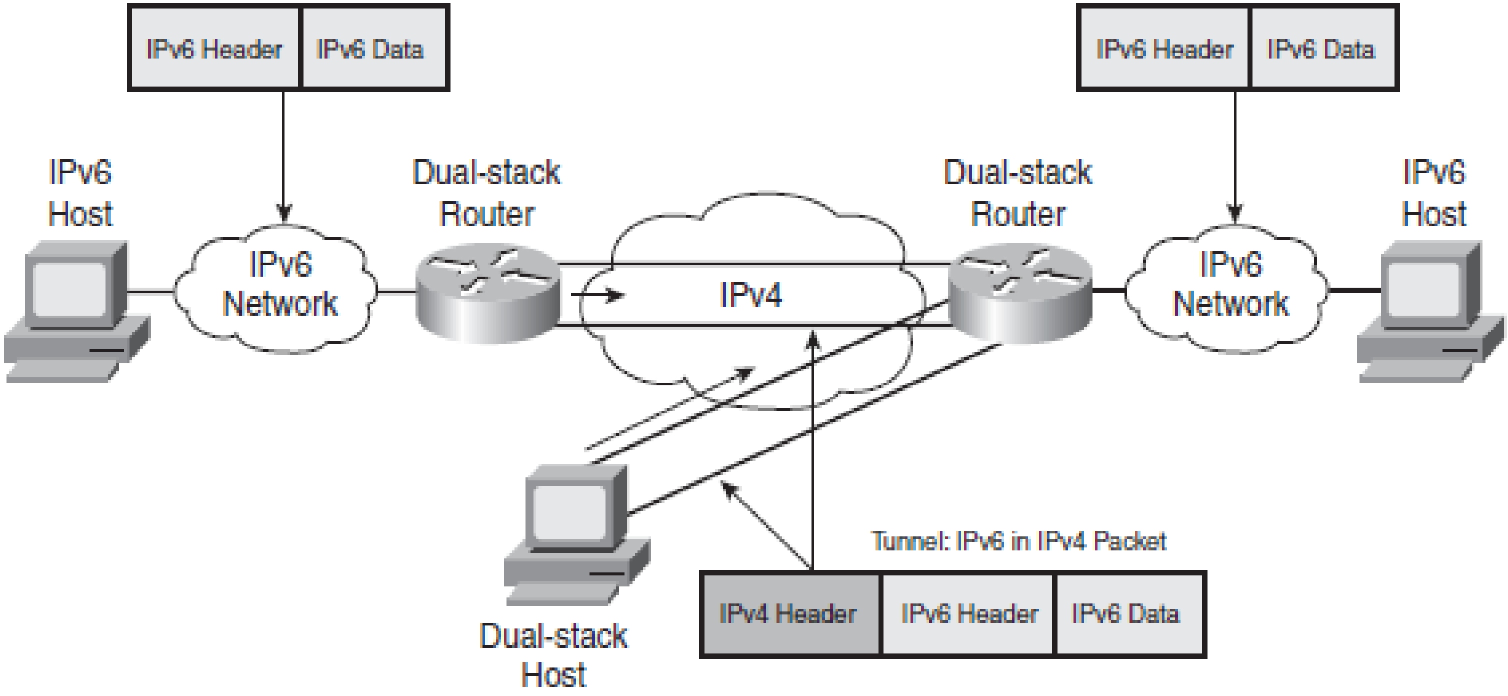
Dual-Stack Transition Mechanism

a dual-stack node enables both IPv4 and IPv6 stacks. Applications communicate with both IPv4 and IPv6 stacks; the IP version choice is based on name lookup and application preference. This is the most appropriate method for campus and access networks during the transition period, and it is the preferred technique for transitioning to IPv6. A dual-stack approach supports the maximum number of applications. Operating systems that support the IPv6 stack include FreeBSD, Linux, Sun Solaris, and Windows 2000, XP, and Vista.



Tunneling Transition Mechanism

The purpose of tunneling is to encapsulate packets of one type in packets of another type. When transitioning to IPv6, tunneling encapsulates IPv6 packets in IPv4 packets, as shown in the following figure.



Tunneling Transition Mechanism

By using overlay tunnels, isolated IPv6 networks can communicate without having to upgrade the IPv4 infrastructure between them. Both routers and hosts can use tunneling. The following different techniques are available for establishing a tunnel:

■ **Manually configured:** For a manually configured tunnel, the tunnel source and tunnel destination are manually configured with static IPv4 and IPv6 addresses. Manual tunnels can be configured between border routers or between a border router and a host.

■ **Semi-automated:** Semi-automation is achieved by using a tunnel broker that uses a web based service to create a tunnel. A tunnel broker is a server on the IPv4 network that receives tunnel requests from dual-stack clients, configures the tunnel on the tunnel server or router, and associates the tunnel from the client to one of the tunnel servers or routers. A simpler model combines the tunnel broker and server onto one device.

Tunneling Transition Mechanism

■ **Automatic:** Various automatic mechanisms accomplish tunneling, including the following:

— IPv4-compatible: The tunnel is constructed dynamically using an IPv4-compatible IPv6 address (an IPv6 address that consists of 0s in the upper bits and an embedded IPv4 address in the lower 32 bits). Because it does not scale, this mechanism is appropriate only for testing.

NOTE The format of an IPv4-compatible IPv6 address is 0:0:0:0:0:0:A.B.C.D, or ::A.B.C.D, where A.B.C.D is the IPv4 address in dotted-decimal notation. The entire 128-bit IPv4- compatible IPv6 address is used as a node's IPv6 address, and the IPv4 address that is embedded in the low-order 32 bits is used as the node's IPv4 address. For example, the IPv4 address 192.168.30.1 would convert to the IPv4-compatible IPv6 address 0:0:0:0:0:0:192.168.30.1. Other acceptable representations for this address are ::192.168.30.1 and ::C0A8:1E01.

Tunneling Transition Mechanism

— IPv6-to-IPv4 (6-to-4): The 6-to-4 tunneling method automatically connects IPv6 islands through an IPv4 network. Each 6-to-4 edge router has an IPv6 address with a /48 prefix that is the concatenation of 2002::/16 and the IPv4 address of the edge router; 2002::/16 is a specially assigned address range for the purpose of 6-to-4. The edge routers automatically build the tunnel using the IPv4 addresses embedded in the IPv6 addresses. For example, if the IPv4 address of an edge router is 192.168.99.1, the prefix of its IPv6 address is 2002:C0A8:6301::/48 because 0xC0A86301 is the hexadecimal representation of 192.168.99.1.

When an edge router receives an IPv6 packet with a destination address in the range of 2002::/16, it determines from its routing table that the packet must traverse the tunnel. The router extracts the IPv4 address embedded in the third to sixth octets, inclusive, in the IPv6 next-hop address. This IPv4 address is the IPv4 address of the 6-to-4 router at the destination site—the router at the other end of the tunnel. The router encapsulates the IPv6 packet in an IPv4 packet with the destination edge router's extracted IPv4 address. The packet passes through the IPv4 network. The destination edge router unencapsulates the IPv6 packet from the received IPv4 packet and forwards the IPv6 packet to its final destination. A 6-to-4 relay router, which offers traffic forwarding to the IPv6 Internet, is required for reaching a native IPv6 Internet.

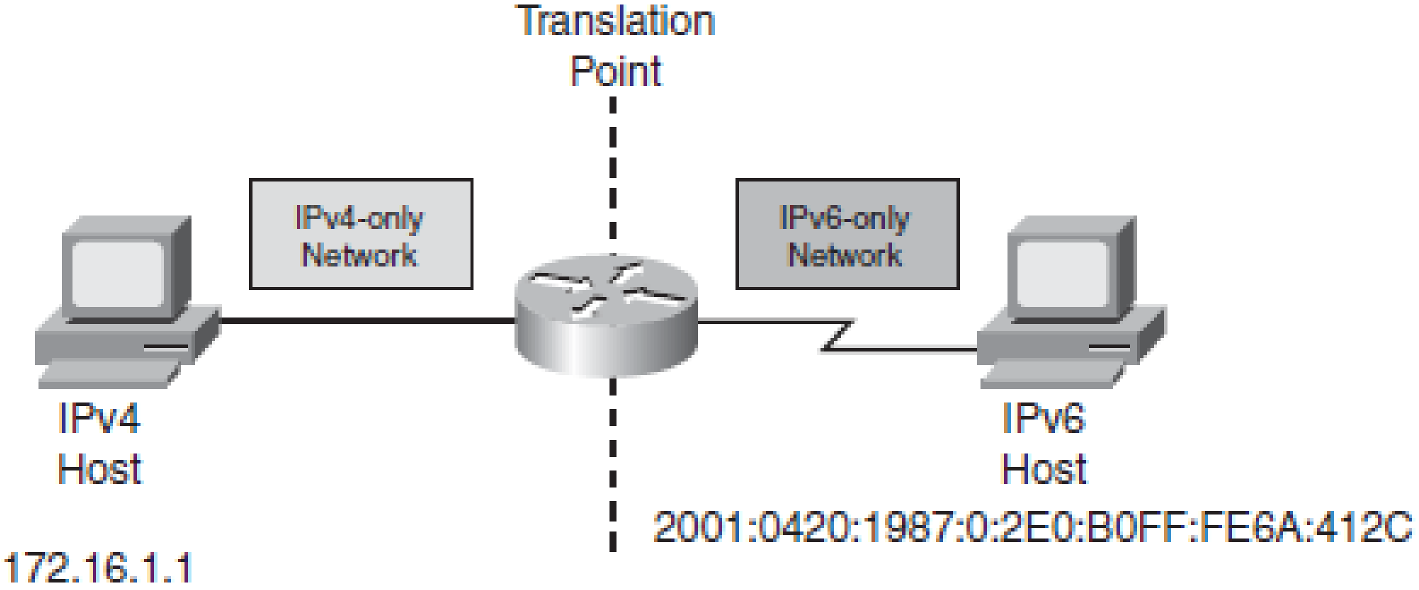
Tunneling Transition Mechanism

— 6over4: A router connected to a native IPv6 network and with a 6over4-enabled interface can be used to forward IPv6 traffic between 6over4 hosts and native IPv6 hosts. IPv6 multicast addresses are mapped into the IPv4 multicast addresses. The IPv4 network becomes a virtual Ethernet for the IPv6 network; to achieve this, an IPv4 multicast-enabled network is required.

Translation Transition Mechanism

Dual-stack and tunneling techniques manage the interconnection of IPv6 domains. For legacy equipment that will not be upgraded to IPv6 and for some deployment scenarios, techniques are available for connecting IPv4-only nodes to IPv6-only nodes, using translation, an extension of NAT techniques.

As shown in the following figure, an IPv6 node behind a translation device has full connectivity to other IPv6 nodes and uses NAT functionality to communicate with IPv4 devices.



Translation Transition Mechanism

Translation techniques are available for translating IPv4 addresses to IPv6 addresses and vice versa. Similar to current NAT devices, translation is done at either the transport layer or the network layer.

NAT - Protocol Translation (NAT-PT) is the main translation technique; the Dual- Stack Transition Mechanism (DSTM) might also be available.

The NAT-PT translation mechanism translates at the network layer between IPv4 and IPv6 addresses and allows native IPv6 hosts and applications to communicate with native IPv4 hosts and applications. An application-level gateway (ALG) translates between the IPv4 and IPv6 DNS requests and responses.

Thank you