IPv6 Tutorial

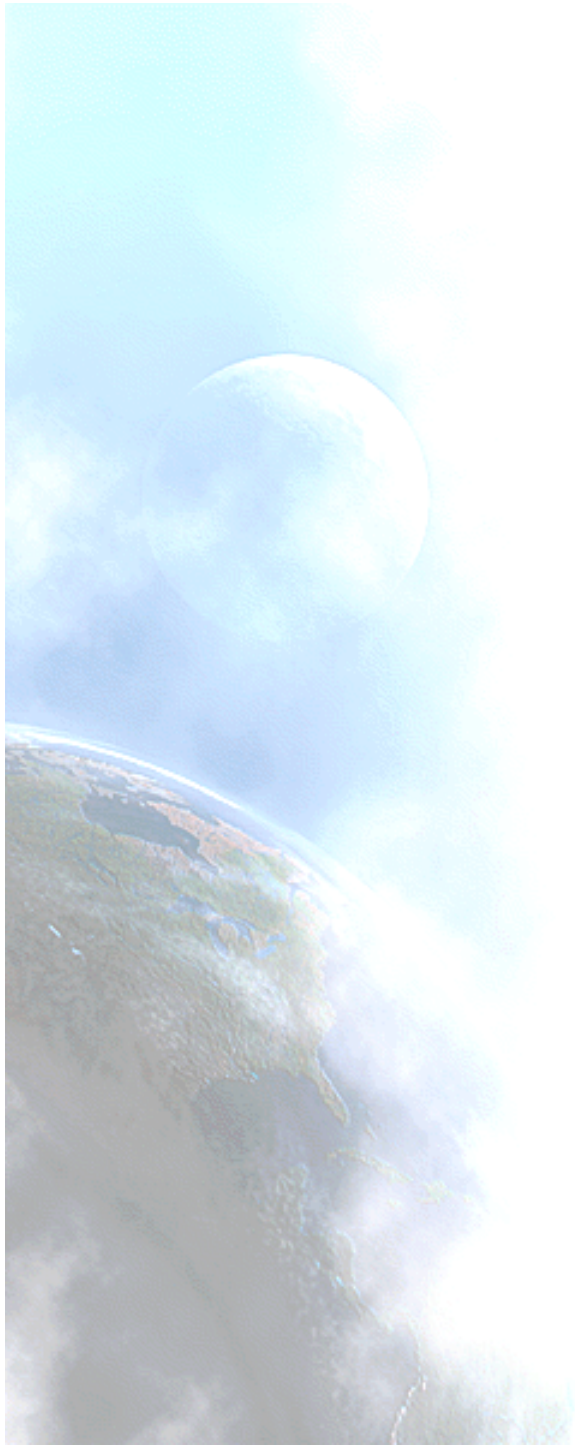
Jordi Palet (jordi.palet@consulintel.es)
Education, Promotion, Public Relations
and Awareness Working Group Chair
IPv6 Forum

IPv6 Tutorial

ICMPv6 & Neighbor Discovery

Agenda

ICMPv6
Neighbor Discovery
Autoconfiguration
DHCPv6
Router Renumbering



ICMPv6

RFC2463

- IPv6 uses the Internet Control Message Protocol (ICMP) as defined for IPv4 (RFC792)
- Some changes for IPv6: ICMPv6.
- Next Header value = 58.
- ICMPv6 is used by IPv6 nodes to report errors encountered in processing packets, and to perform other internet-layer functions, such as diagnostics (ICMPv6 "ping").
- ICMPv6 is an integral part of IPv6 and MUST be fully implemented by every IPv6 node.

ICMPv6 Messages

- Grouped into two classes:
  - Error messages
  - Informational messages.

bits 8	16	32
Type	Code	Checksum
Message Body		

- Error messages have a zero in the high-order bit of their message Type field values (message Types from 0 to 127)
- Informational messages have message Types from 128 to 255

Message Source Address Determination

- A node that sends an ICMPv6 message has to determine both the Source and Destination IPv6 Addresses in the IPv6 header before calculating the checksum.
- If the node has more than one unicast address, it must choose the Source Address of the message as follows:

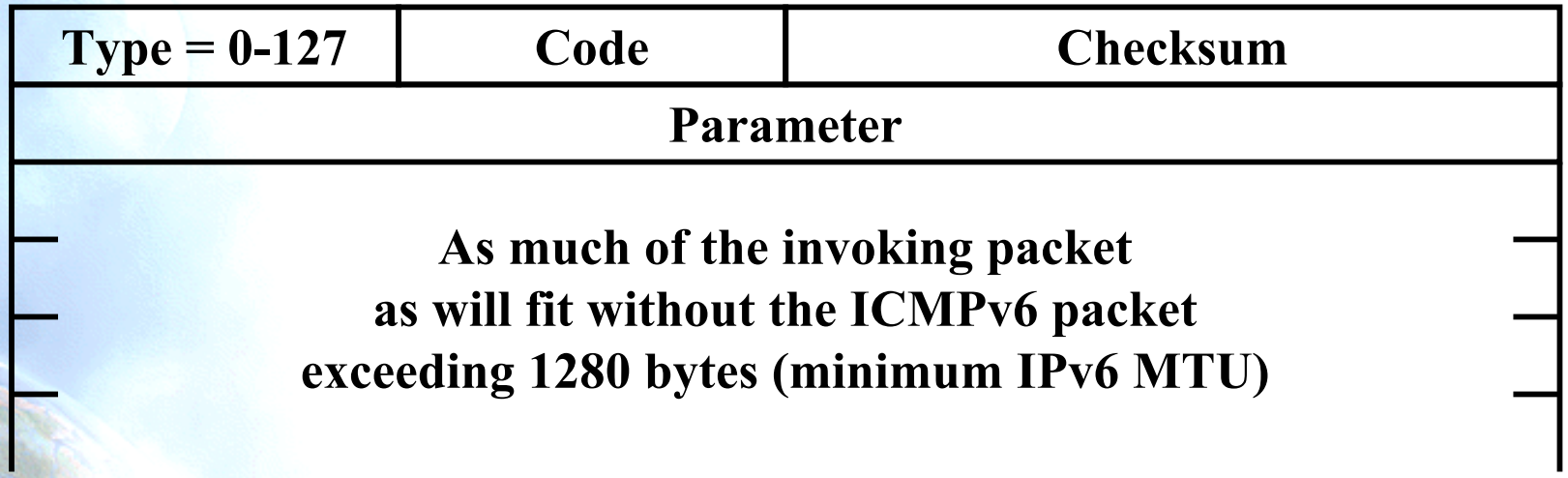
a) Message responding to a message sent to one of the node's unicast addresses, then Reply Source Address = Same Address.

b) Message responding to a message sent to a multicast or anycast group in which the node is a member, then Reply Source Address = unicast address belonging to the interface on which the multicast or anycast packet was received.

c) Message responding to a message sent to an address that does not belong to the node, then Source Address = unicast address belonging to the node that will be most helpful in diagnosing the error.

d) Otherwise, the node's routing table must be examined to determine which interface will be used to transmit the message to its destination, message Source Address = unicast address belonging to that interface.

ICMP Error Messages



ICMP Error Messages Types

- Destination Unreachable (type = 1, parameter = 0)
  - No route to destination (code = 0)
  - Communication with destination administratively prohibited (code = 1)
  - Not Assigned (code = 2)
  - Address Unreachable (code = 3)
  - Port Unreachable (code = 4)
- Packet Too Big (type = 2, code = 0, parameter = next hop MTU)
- Time Exceeded (type = 3, parameter = 0)
  - Hop Limit Exceeded in Transit (code = 0)
  - Fragment Reassembly Time Exceeded (code = 1)
- Parameter Problem (type = 4, parameter = offset to error)
  - Erroneous Header Field (code = 0)
  - Unrecognized Next Header Type (code = 1)
  - Unrecognized IPv6 Option (code = 2)

ICMP Informational Messages

- Echo Request (type =128, code = 0)
- Echo Reply (type = 129, code = 0)

Type = 128-255	Code	Checksum
Maximum Response Delay		Reserved
Multicast Address		

- Multicast listener discovery messages:

  - Query, report, done (like IGMP for IPv4):

Neighbor Discovery

RFC2461

- Defines the Neighbor Discovery (ND) protocol for IPv6.
- Nodes (hosts and routers) use Neighbor Discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid.
- Hosts also use Neighbor Discovery to find neighboring routers that are willing to forward packets on their behalf.
- Nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses.

Autoconfiguration Foundation

- ND is a very complete and sophisticated foundation to enable the autoconfiguration mechanism in IPv6.
- Enable extended support for proxy services, anycast addresses, load sharing balancing, among others.
- RFC2461 describes a conceptual model of one possible data structure organization that hosts (and to some extent routers) will maintain in interacting with neighboring nodes.

Interaction Between Nodes

- Defines mechanism to solve:
  - Router Discovery.
  - Prefix Discovery.
  - Parameter Discovery.
  - Address Autoconfiguration.
  - Address Resolution.
  - Next-hop Determination.
  - Neighbor Unreachability Detection (NUD).
  - Duplicate Address Detection (DAD).
  - First-Hop Redirect.

New ICMP Packet Types

- ND defines 5 packet types:
  - Router Solicitation.
  - Router Advertisement.
  - Neighbor Solicitation.
  - Neighbor Advertisement.
  - Redirect.

Router Advertisements

- On multicast-capable links, each router periodically multicasts a Router Advertisement packet.
- A host receives Router Advertisements from all routers, building a list of default routers.
- A separate Neighbor Unreachability Detection algorithm provides failure detection.
- Router Advertisements contain a list of prefixes used for on-link determination and/or autonomous address configuration.
- Router Advertisements allow routers to inform hosts how to perform Address Autoconfiguration.

Autoconfiguration

RFC2462

- The document specifies the steps a host takes in deciding how to autoconfigure its interfaces in IPv6.
- The autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both), and in the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both.
- IPv6 defines both a stateful and stateless address autoconfiguration mechanism.
- Stateless autoconfiguration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers.

Stateless or Serverless Autoconfiguration

- Stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers.
- Routers advertise prefixes that identify the subnet(s) associated with a link.
- Hosts generate an "interface identifier" that uniquely identifies an interface on a subnet, locally generated, e.g., using MAC address.
- An address is formed by combining the both.
- In the absence of routers, a host can only generate link-local addresses.
- Link-local addresses are sufficient for allowing communication among nodes attached to the same link.

Stateful Autoconfiguration

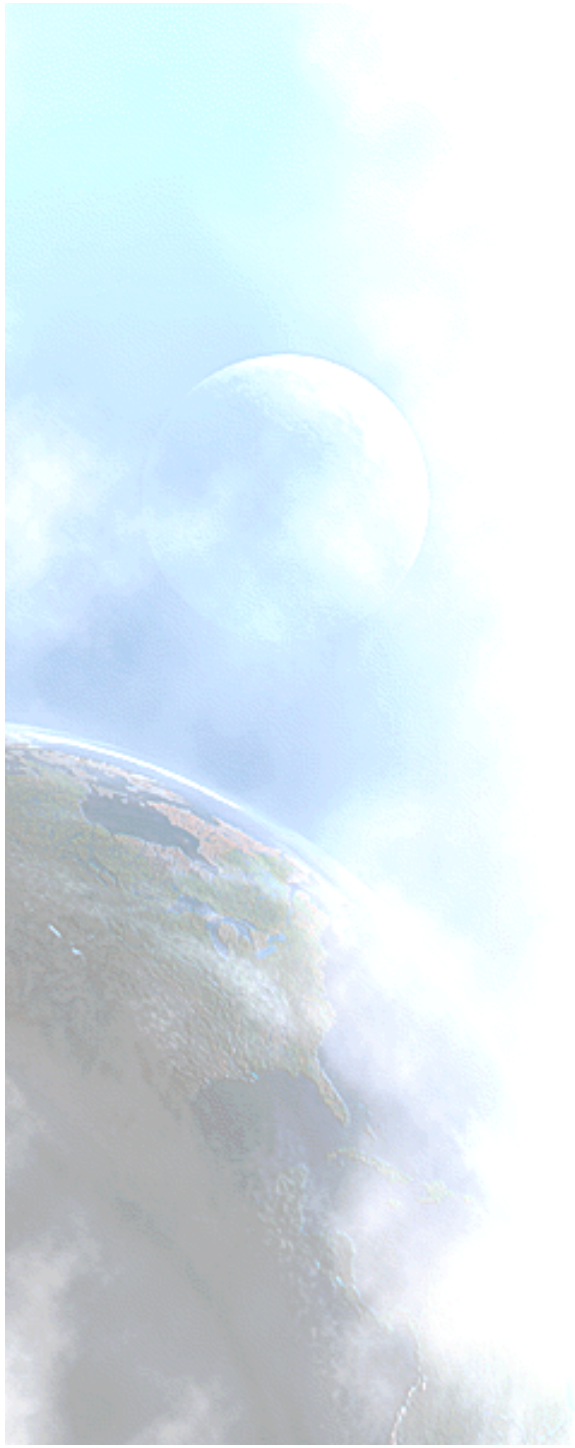
- Hosts obtain interface addresses and/or configuration information and parameters from a server.
- Servers maintain a database that keeps track of which addresses have been assigned to which hosts.
- Stateless and stateful autoconfiguration complement each other.
- Both stateful and stateless address autoconfiguration may be used simultaneously.
- The site administrator specifies which type of autoconfiguration to use through the setting of appropriate fields in Router Advertisement messages.

Address Life Time

- IPv6 addresses are leased to an interface for a fixed (possibly infinite) length of time, that indicates how long the address is bound to an interface.
- When a lifetime expires, the binding (and address) become invalid and the address may be reassigned to another interface elsewhere in the Internet.
- To handle the expiration of address bindings gracefully, an address goes through two distinct phases while assigned to an interface.
  - Initially, an address is "preferred", meaning that its use in arbitrary communication is unrestricted.
  - Later, an address becomes "deprecated" in anticipation that its current interface binding will become invalid.

Duplicate Address Detection

- To insure that all configured addresses are likely to be unique on a given link, nodes run a "duplicate address detection" algorithm on addresses before assigning them to an interface.
- The Duplicate Address Detection algorithm is performed on all addresses, independent of whether they are obtained via stateless or stateful autoconfiguration.
- The procedure for detecting duplicate addresses uses Neighbor Solicitation and Advertisement messages.
- Since host autoconfiguration uses information advertised by routers, routers will need to be configured by some other means. However, it is expected that routers will generate link-local addresses using the same mechanism.
- Routers are expected to successfully pass the Duplicate Address Detection procedure on all addresses prior to assigning them to an interface.



DHCPv6

RFC3315

- DHCP for IPv6 (DHCPv6) is an UDP client/server protocol designed to reduce the cost of management of IPv6 nodes in environments where network managers require more control over the allocation of IPv6 addresses and configuration of network stack parameters than that offered by "IPv6 Stateless Autoconfiguration".
- DHCP reduces the cost of ownership by centralizing the management of network resources rather than distributing such information in local configuration files among each network node.
- DHCP is designed to be easily extended to carry new configuration parameters through the addition of new DHCP "options" defined to carry this information.

New User Features with DHCPv6

- Configuration of Dynamic Updates to DNS.
- Address deprecation, for dynamic renumbering.
- Relays can be preconfigured with server addresses, or use of multicast.
- Authentication.
- Clients can ask for multiple IP addresses.
- Addresses can be reclaimed using the Reconfigure-init message.
- Integration between stateless and stateful address autoconfiguration.
- Enabling relays to locate off-link servers.

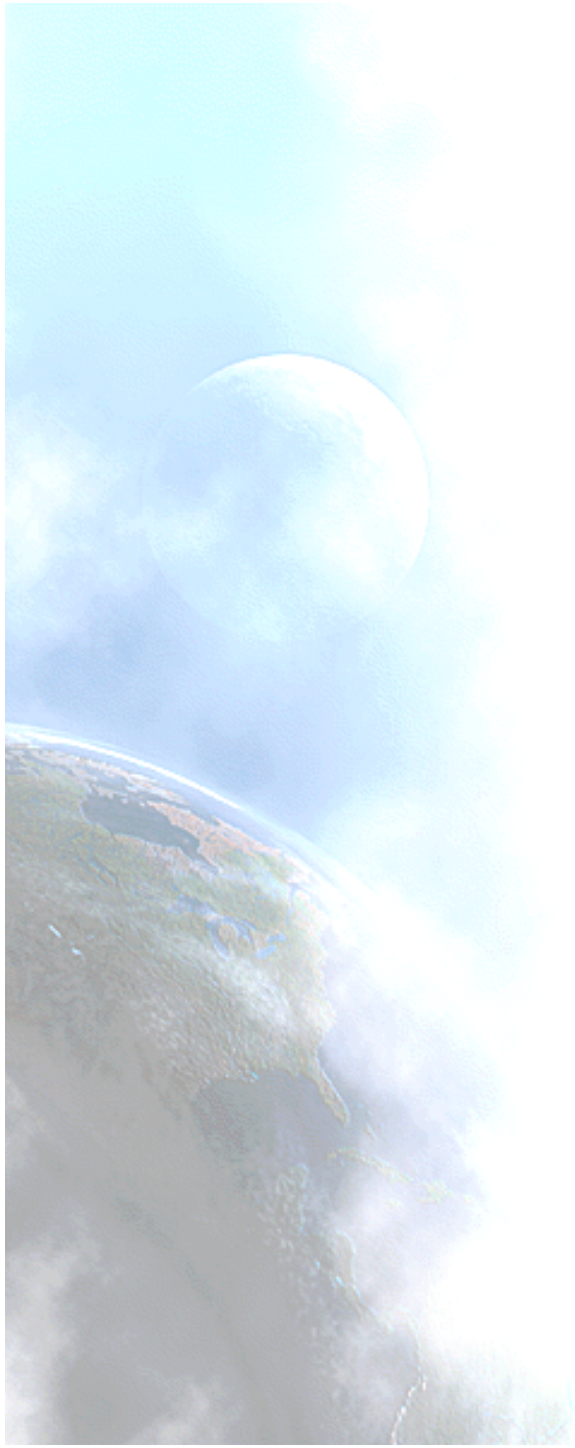
Router Renumbering

RFC2894

- IPv6 Neighbor Discovery and Address Autoconfiguration make initial assignments of address prefixes to hosts.
- These two mechanisms also simplify the reconfiguration of hosts when the set of valid prefixes changes.
- The Router Renumbering ("RR") mechanism allows address prefixes on routers to be configured and reconfigured almost as easily as the combination of Neighbor Discovery and Address Autoconfiguration works for hosts.
- Provides a means for a network manager to make updates to the prefixes used by and advertised by IPv6 routers throughout a site.

Functional Overview

- Router Renumbering Command packets contain a sequence of Prefix Control Operations (PCOs).
- Each PCO specifies an operation, a Match-Prefix, and zero or more Use-Prefixes.
- A router processes each PCO, checking each of its interfaces for an address or prefix which matches the Match-Prefix.
- Applied for every interface on which a match is found.
- The operation is one of ADD, CHANGE, or SET-GLOBAL to instruct the router to respectively add the Use-Prefixes to the set of configured prefixes, remove the prefix which matched the Match-Prefix and replace it with the Use-Prefixes, or replace all global-scope prefixes with the Use-Prefixes.



IPv6 Tutorial

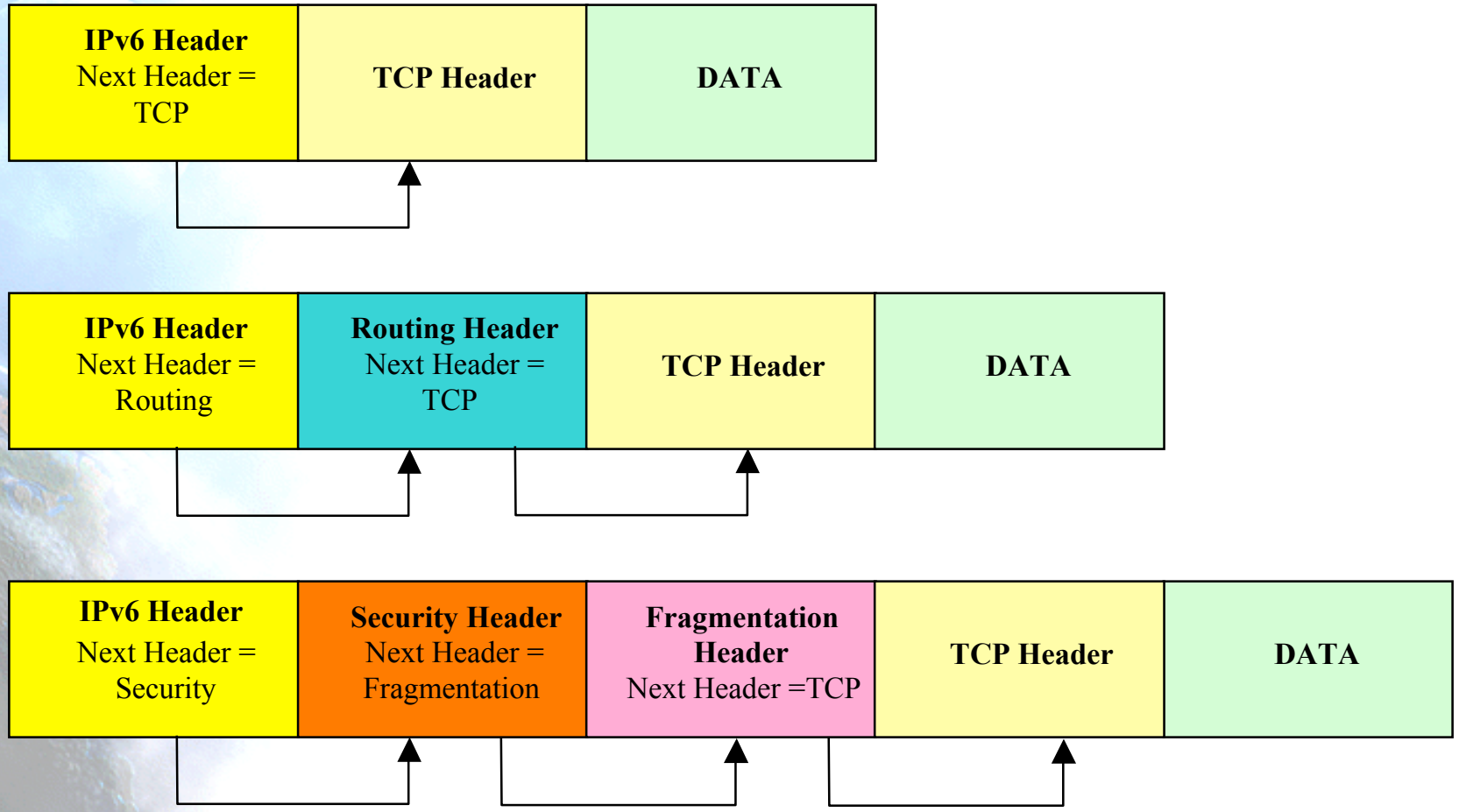
Security

Agenda

Basic Concepts
Security Associations
IPsec Headers
Transport and Tunnel Modes
Key Management

Extension Headers

- "Next Header" Field



Basic Concepts

IP Security

- RFC2401: Base architecture for IPsec compliant systems
- Goal: Provide various security services for traffic at the IP layer, in both IPv4 and IPv6 environments.
  - Security Protocols -- Authentication Header (AH – RFC2402, authentication ONLY) and Encapsulating Security Payload (ESP – RFC2406, encryption + authentication)
  - Security Associations - what they are and how they work, how they are managed, associated processing (RFC2407, RFC2408, RFC2412)
  - Key Management - manual and automatic: The Internet Key Exchange (IKE – RFC2409, ISAKMP, OAKLEY)
  - Algorithms for authentication and encryption

Security Services Set

- Security Services Set:
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Protection against replays (a form of partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality.
- IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6.

Traffic Security Protocols

- How to:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Use of cryptographic key management procedures and protocols.
  - The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations.
    - IPsec allows the user/system administrator to control the granularity at which a security service is offered.
- These mechanisms are designed to be algorithm-independent.
- IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

Modes of Use

- AH & ESP may be applied alone or in combination with each other to provide a desired set of security services in IPv4 and IPv6.
- Each protocol supports two modes of use:
  - Transport mode (protection primarily for upper layer protocols)
    - Direct between end-to-end systems
    - Both Remote systems must support IPsec !
  - Tunnel mode (protocols applied to tunneled IP packets)
    - Secure tunnel for encapsulating insecure IP packets
    - Between intermediate systems (not end-to-end)

IPv6 Security

- IPsec is part of the IPv6 "core" specs:
  - All implementations expected to support authentication and encryption headers ("IPsec")
- Authentication separate from encryption for use in situations where encryption is prohibited or prohibitively expensive
- Key distribution protocols are under development (independent of IP v4/v6)
- Support for manual key configuration required

Security Associations

The Concept

- Security Association (SA) is a fundamental concept for IPsec:
  - **A simplex "connection" that affords security services to the traffic carried by it.**
- AH & ESP use SA's.
- A major function of IKE is the establishment and maintenance of Security Associations.
- All implementations of AH & ESP MUST support the concept of a Security Association.

SA Identification

- Each SA is uniquely identified by a triple:
  - Security Parameter Index (SPI)
    - Bit String Assigned to the SA (local meaning), as a pointer to a SA Database (SPD or Security Policy Database).
  - IP Destination Address
  - Security protocol (AH or ESP) identifier
- Destination Address may be:
  - Unicast Address
  - IP broadcast address
  - Multicast group address

SA Database (SAD)

- In each IPsec implementation there is a nominal Security Association Database.
- Each entry defines the parameters associated with one SA.
- Each SA has an entry in the SAD.

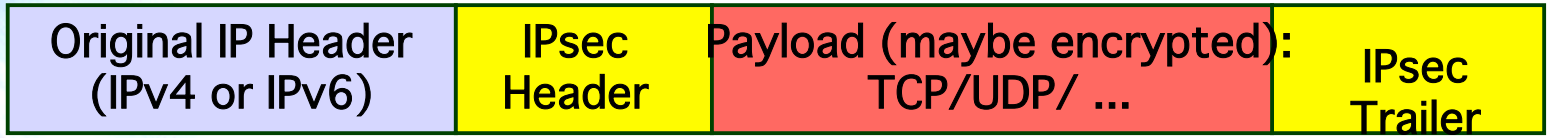
SAD Fields

- **Sequence Number Counter:** 32 bits value used to generate the sequence number transmitted in the AH and ESP headers.
- **Sequence Counter Overflow:** Indicates the action to trigger when the sequence number range is over.
- **Anti-Replay Window:** Window for limiting the acceptance of valid datagrams.
- **AH Information:** Authentication algorithms, keys, lifetimes, etc.
- **ESP Information:** Authentication and Encrypting algorithms, keys, lifetimes, initial values, etc.
- **IPsec Protocol Mode:** Transport, tunnel or wildcard.
- **SA Lifetime:** Time or bytes interval of a SA.
- **Path MTU:** Maximum packet size transmitted without fragmentation.

IPsec Headers

IPsec Transmission

- IPsec header inserted between the original header and the payload.
- If ESP is used, data is encrypted and am IPsec trailer is appended.

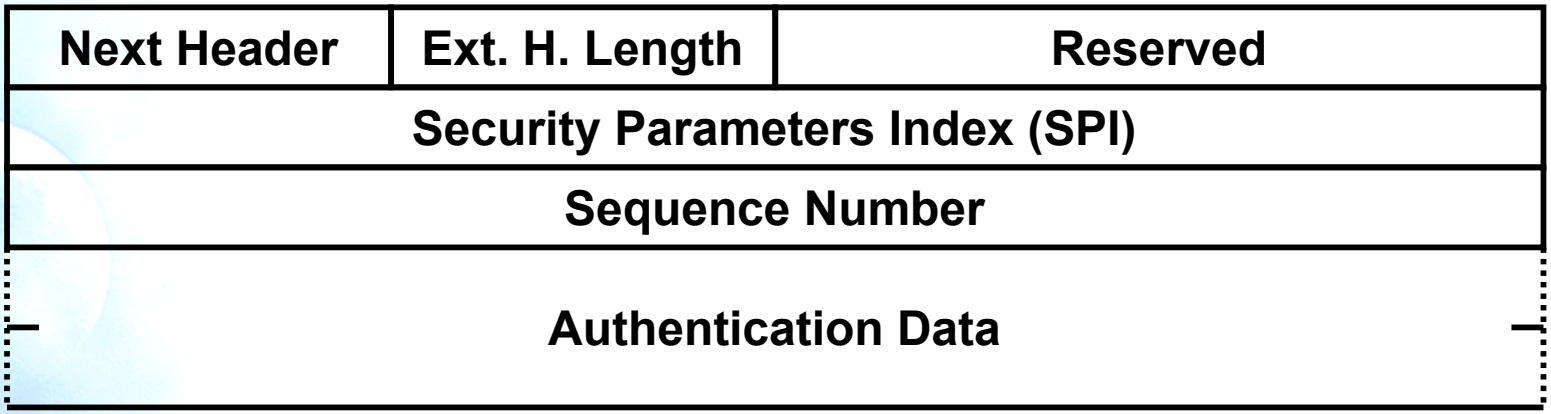


- Next Header value:
  - ESP = 50
  - AH = 51

Authentication Mode (RFC2402)

- Provides authentication and data integrity of the IP fields that don't change en-route:
  - Changes in the content are detected
  - Receivers can authenticate the sender
  - Avoids the IP-Spoofing attack
  - Protection against the replay attack.
- Default algorithms:
  - Keyed MD5
  - SHA-1

Authentication Header (AH)

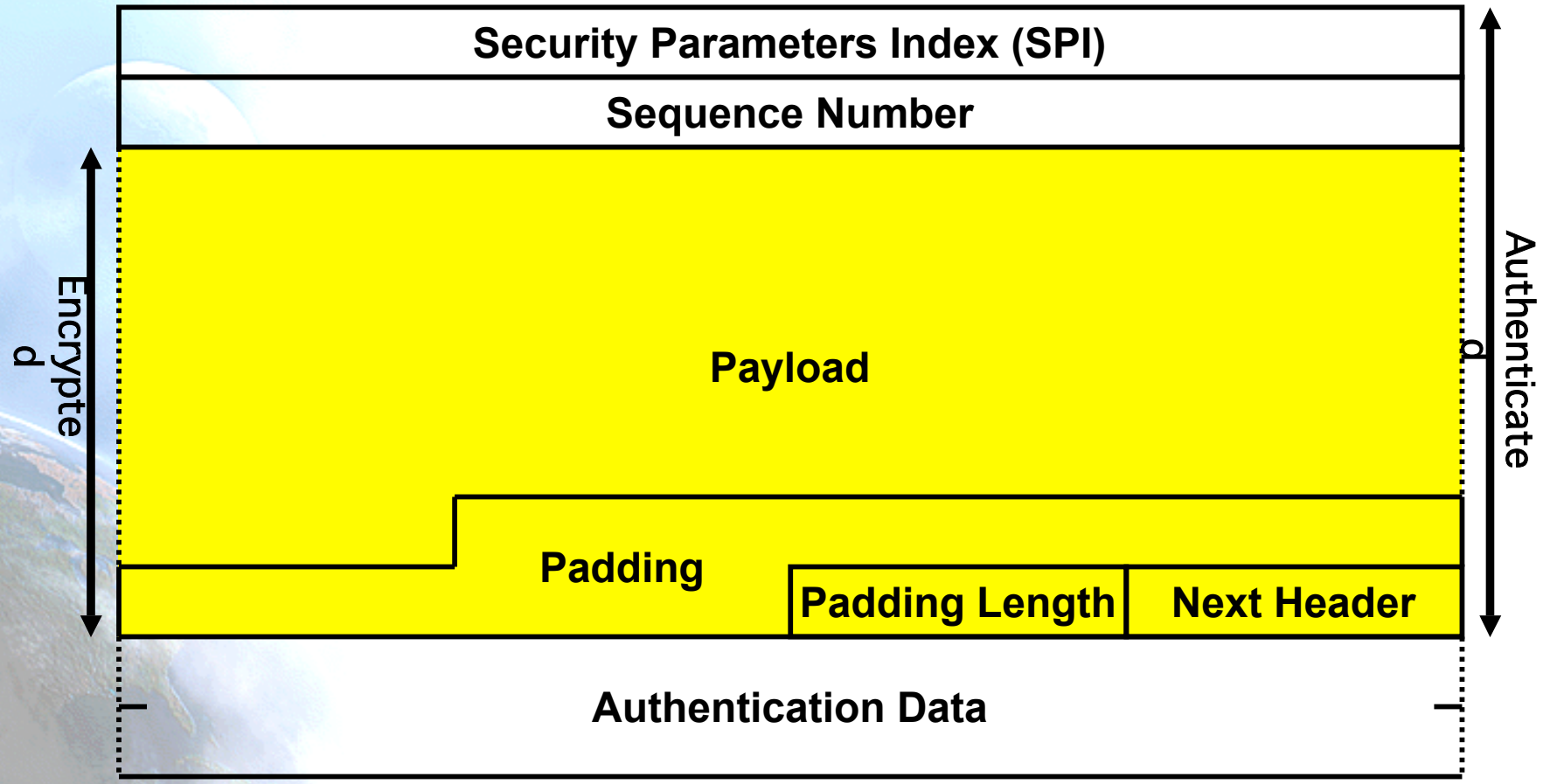


- SPI: Arbitrary 32-bit value that, in combination with the destination IP address and security protocol (AH), uniquely identifies the Security Association for this datagram.
- Sequence Number: Unsigned 32-bit field contains a monotonically increasing counter value.
- Authentication Data: Variable-length field that contains the Integrity Check Value (ICV) for this packet.

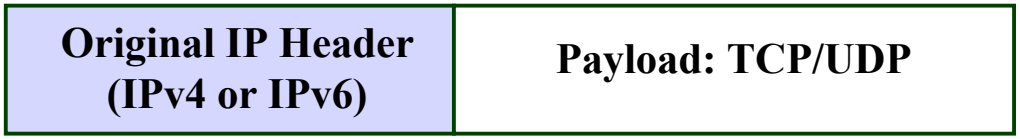
Encryption Mode (RFC2406)

- Provides:
  - Confidentiality
  - Data origin authentication
  - Connectionless integrity
  - Anti-Reply Service (Partial sequence integrity)
  - Limited traffic flow confidentiality

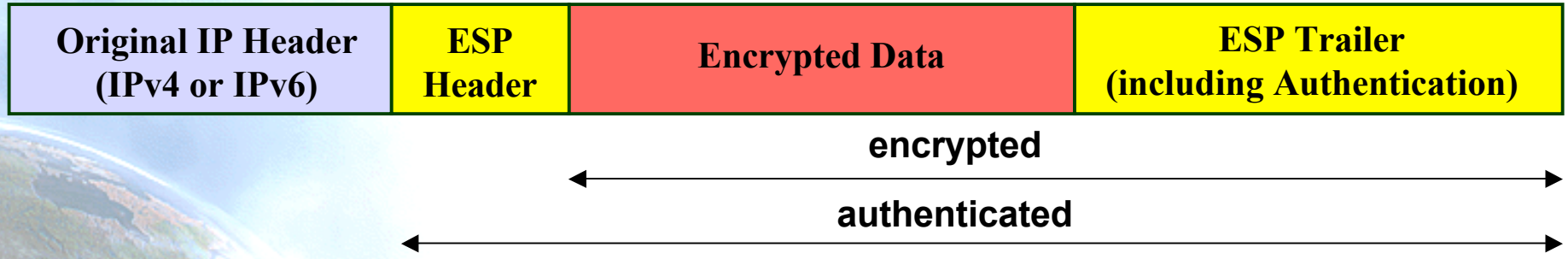
ESP Header


Security Parameters Index (SPI)
Sequence Number
Payload
Padding
Padding Length
Next Header
Authentication Data
Encrypted
Authenticated

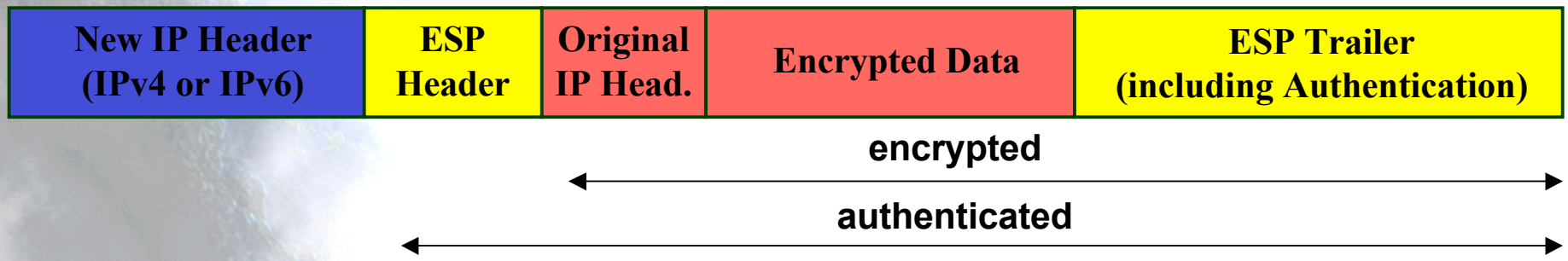
Transport and Tunnel Modes



Transport Mode



Tunnel Mode

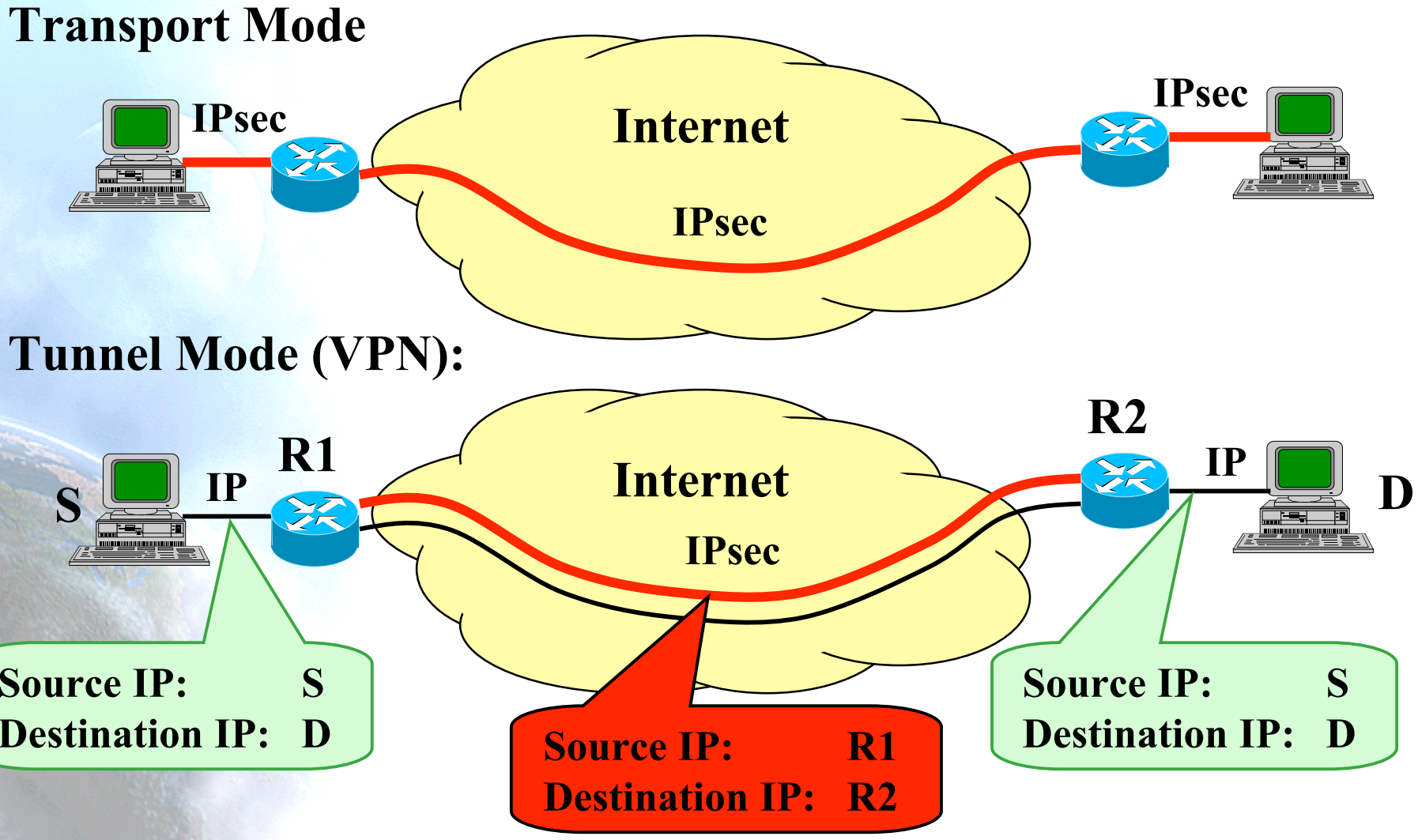


Algorithms

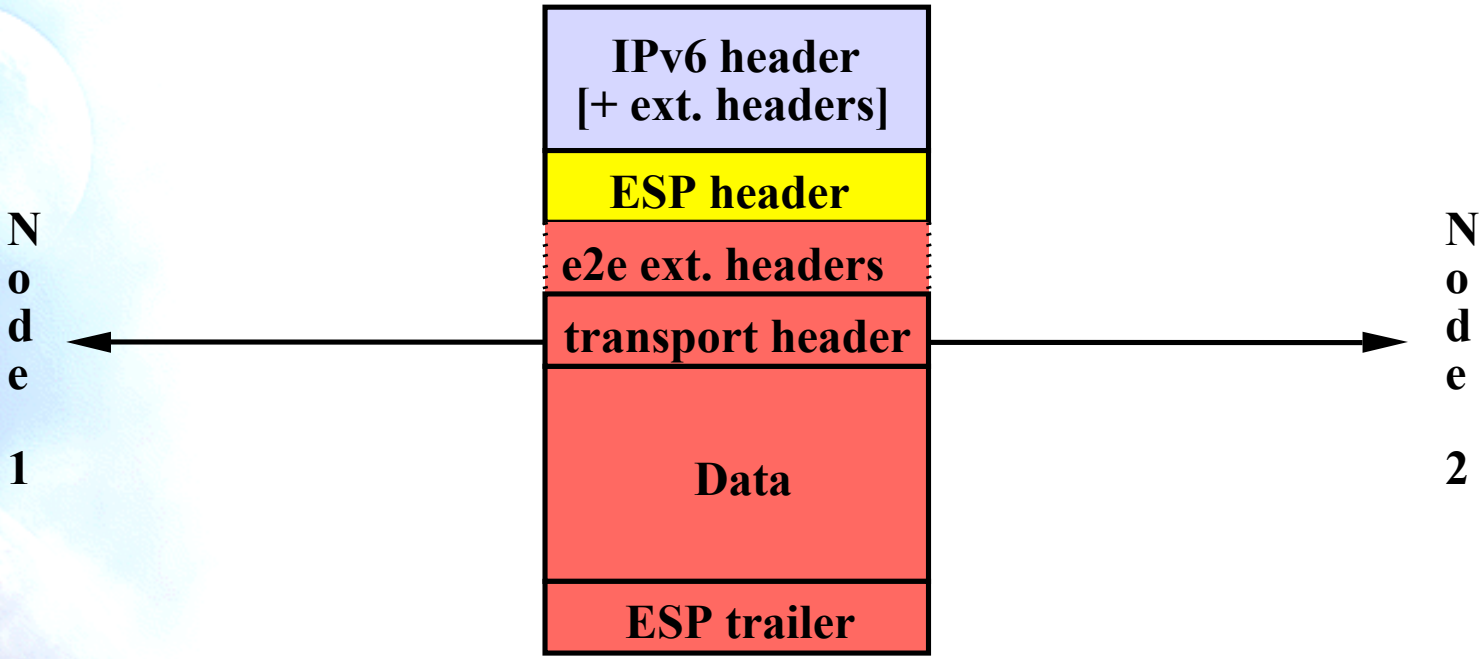
- Specified in the SA
- Encryption: Symmetric algorithms
- Interoperability support:
  - DES with CBC (encryption)
  - MD5 & SHA-1 (authentication)
- Others:
  - Triple DES, RC5, ...

Transport and Tunnel Modes

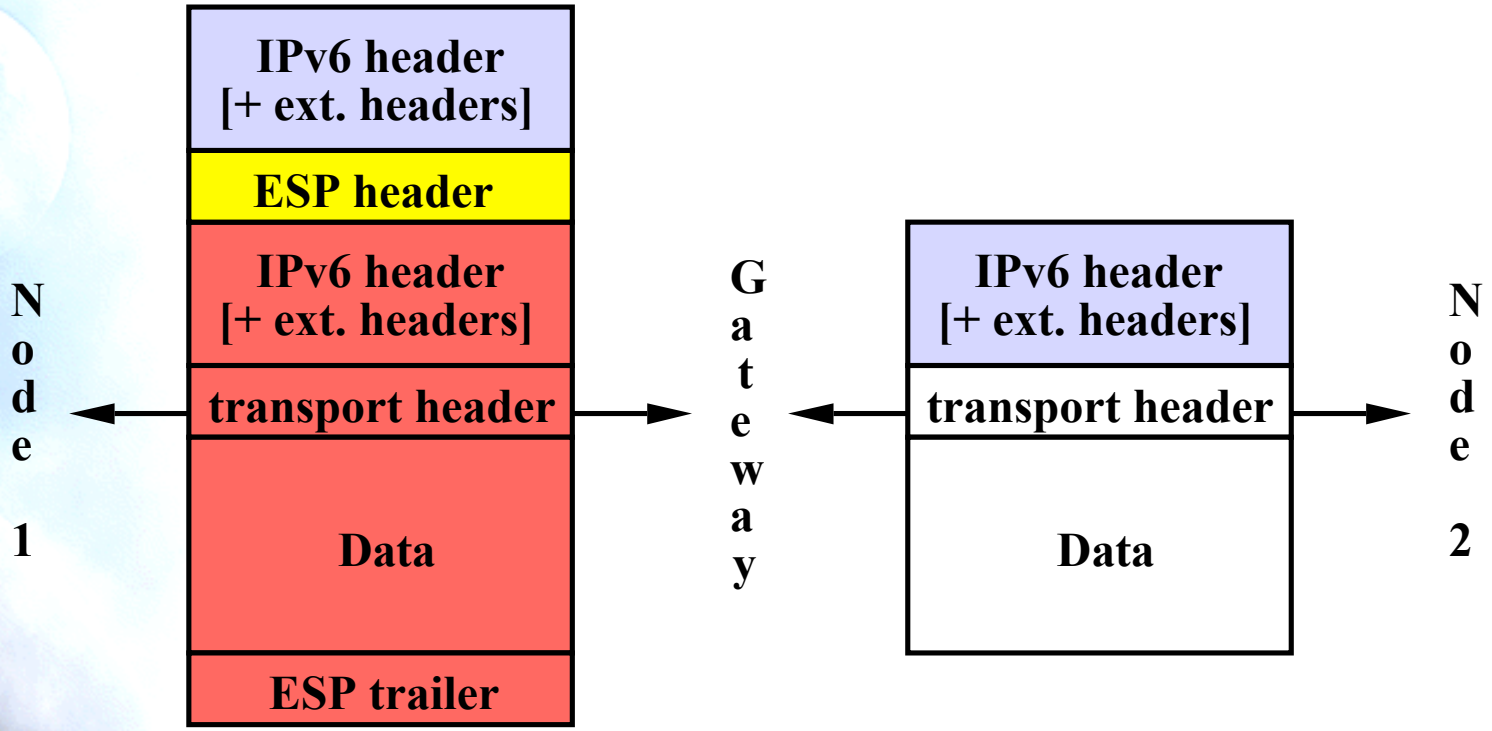
Transport vs. Tunnel Mode



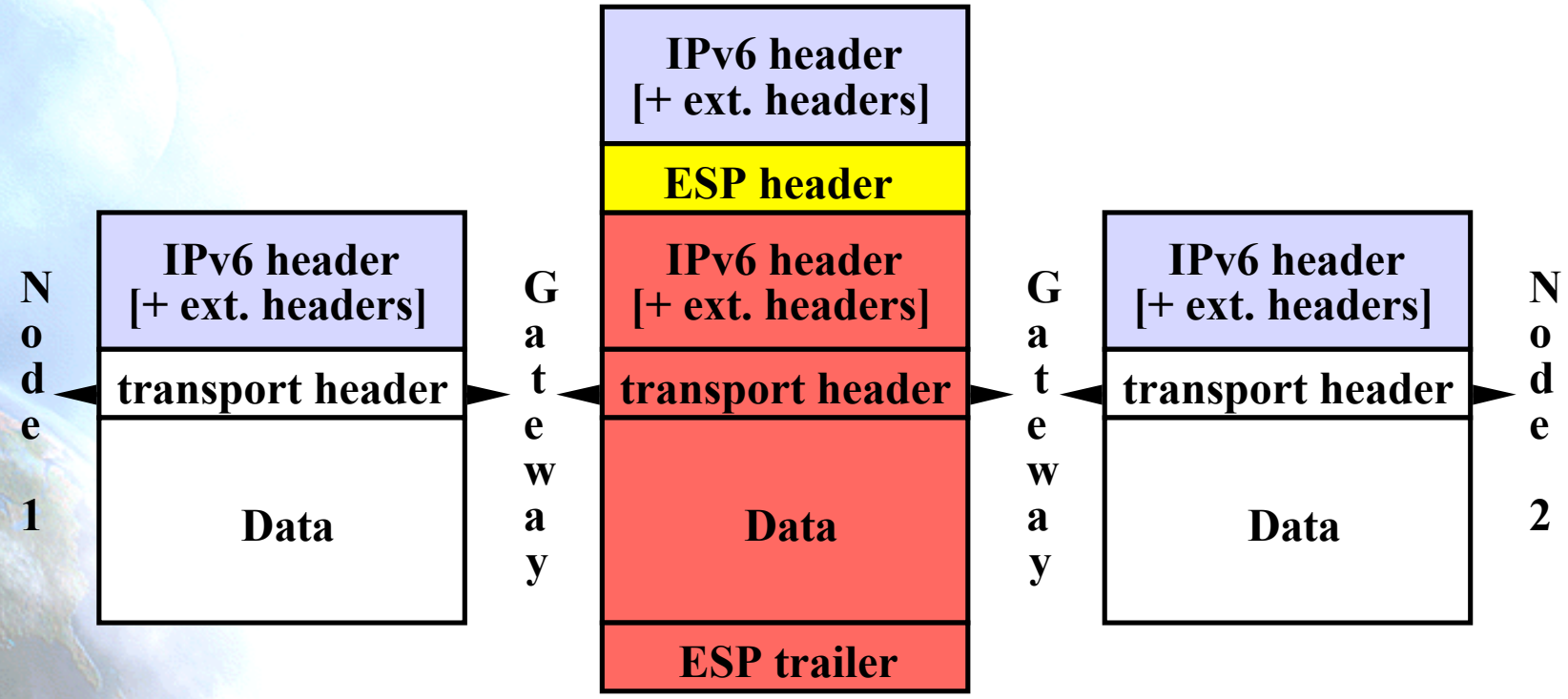
Transport Mode ESP End-to-End



Tunnel Mode ESP
End to Security Gateway



Tunnel Mode ESP
Gateway to Gateway



Key Management

Key Distribution

- Manual:
  - Simplest form of management.
  - Each system is configured with his own and others keys.
  - Practical in small, static environments.
  - Do not scale well.
- Automatic:
  - On-demand creation of SA´s.
  - The default is IKE – Internet Key Exchange (RFC2409).
  - Other automated SA management protocols MAY be employed.

IKE

- Standard Method to:
  - Dynamically authenticate IPsec peers
  - Negotiate security services
  - Generate shared keys
- Protocols:
  - ISAKMP (Internet Security Association and Key Management Protocol) defines the procedures for authenticating a communicating peer, creation and management of SA's, key generation techniques, and threat mitigation. (RFC2407-2408).
  - OAKLEY: Key exchange protocol (RFC2412).

IPv6 Tutorial

Quality of Service

Concept of QoS

- Quality: Reliable delivery of data ("better than normal")
  - Data loss
  - Latency
  - Jittering
  - Bandwidth
- Service: Anything offered to the user
  - Communication
  - Transport
  - Application

Abstract

- “Quality of Service is a measurement of the network behavior with respect to certain characteristics of defined services” !!!!!
- Common concepts to all definitions of QoS:
  - Traffic and type of service differentiation
  - Users may be able to treat one or more traffic classes differently

IP Quality of Service Approaches

Two basic approaches developed by IETF:

- "Integrated Service" (int-serv)
  - fine-grain (per-flow), quantitative promises (e.g., x bits per second), uses RSVP signalling
- "Differentiated Service" (diff-serv)
  - coarse-grain (per-class), qualitative promises (e.g., higher priority), no explicit signalling

IPv6 Support for Int-Serv

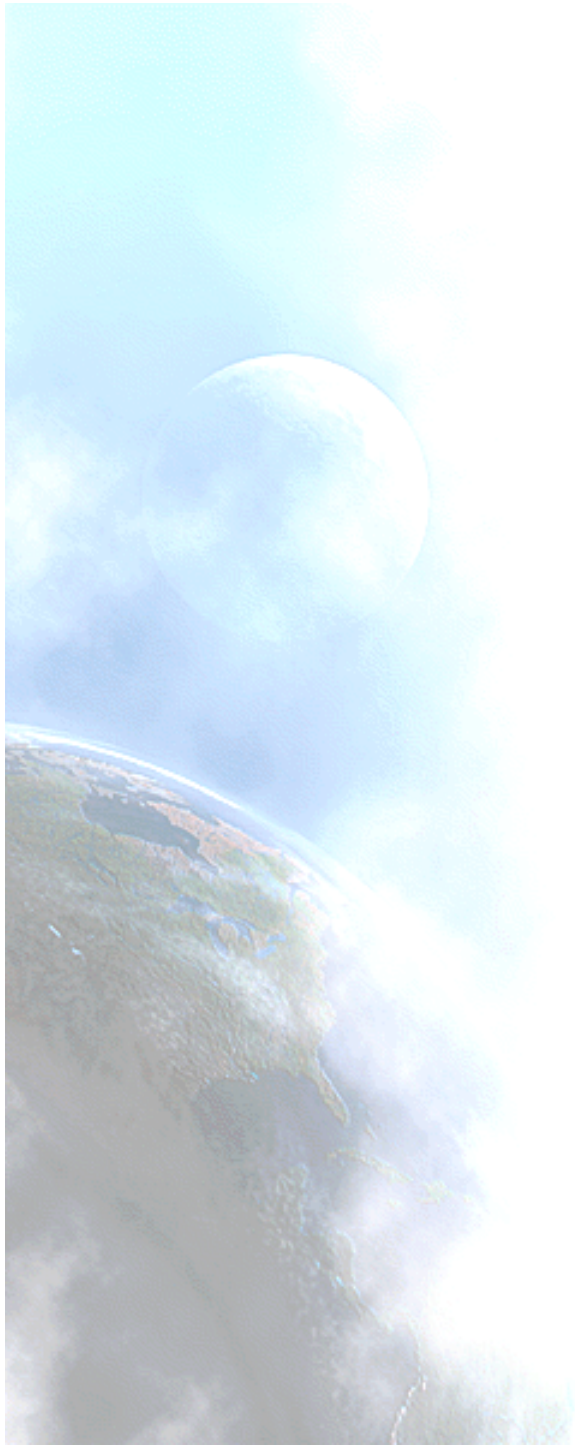
20-bit Flow Label field to identify specific flows needing special QoS

- each source chooses its own Flow Label values; routers use Source Addr + Flow Label to identify distinct flows
- Flow Label value of 0 used when no special QoS requested (the common case today)
- this part of IPv6 is not standardized yet, and may well change semantics in the future

IPv6 Support for Diff-Serv

8-bit Traffic Class field to identify specific classes of packets needing special QoS

- same as new definition of IPv4 Type-of-Service byte
- may be initialized by source or by router enroute; may be rewritten by routers enroute
- traffic Class value of 0 used when no special QoS requested (the common case today)



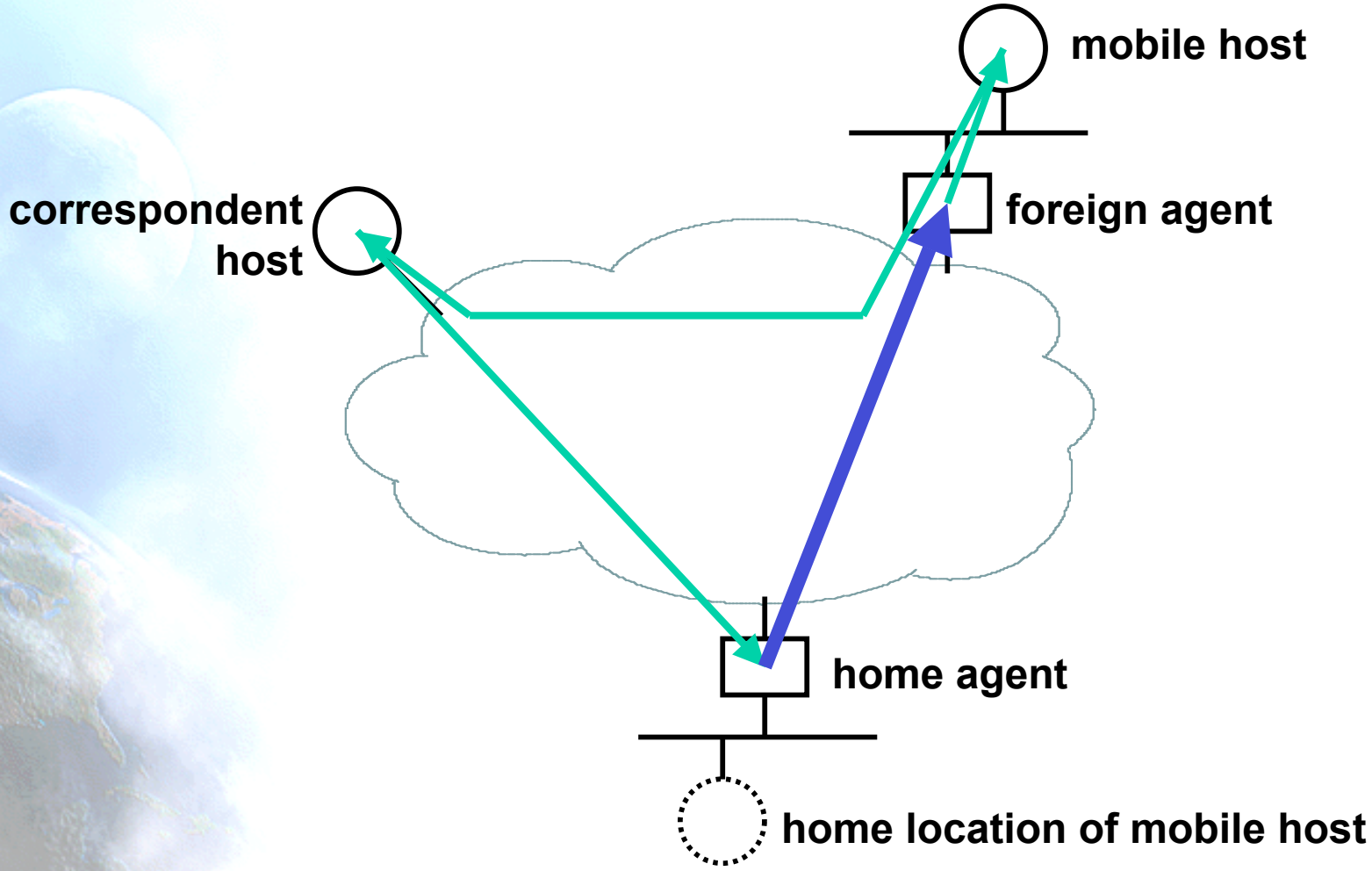
IPv6 Tutorial

Mobility

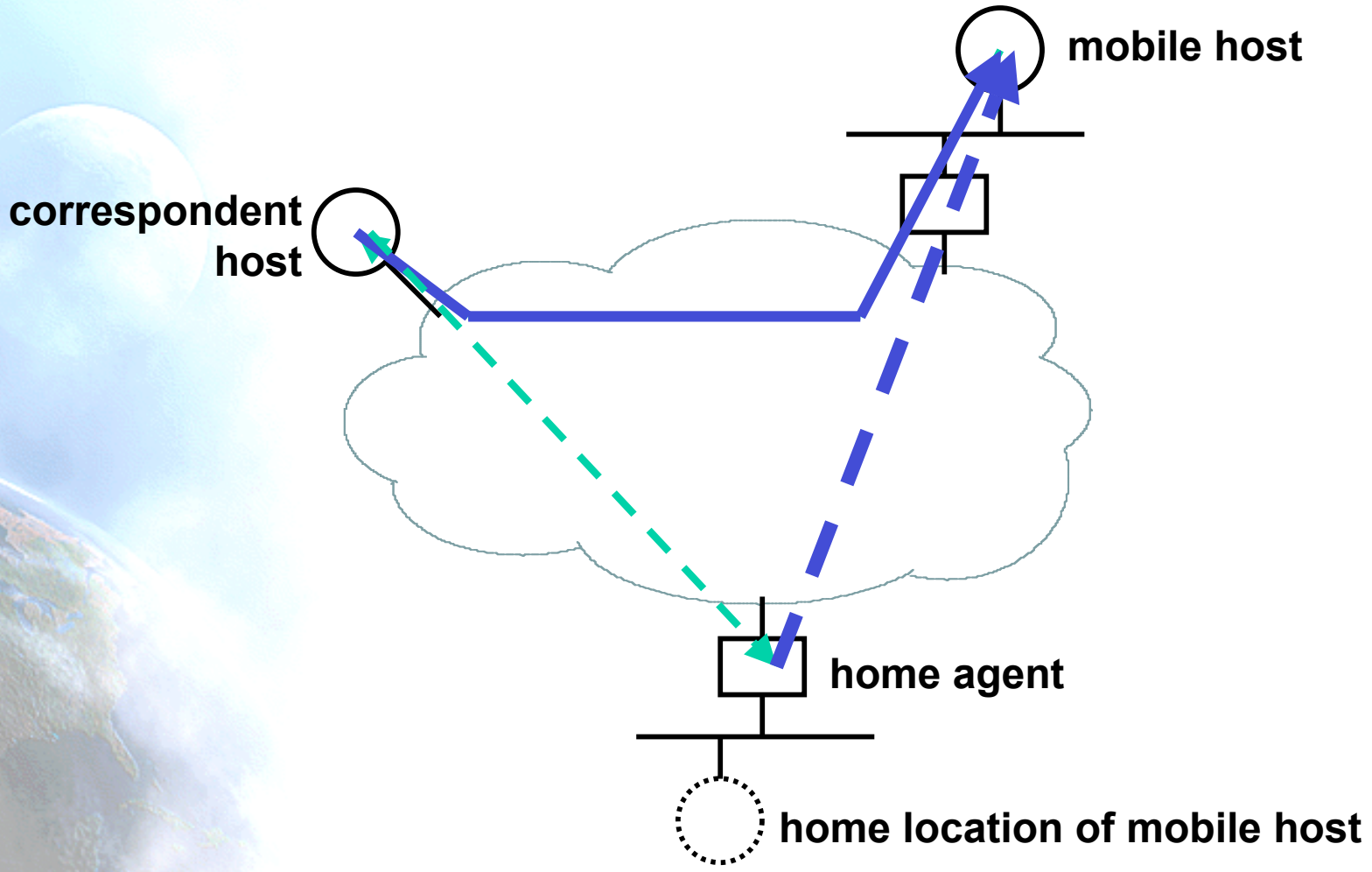
IPv6 Mobility

- A mobile host has one or more home address(es)
  - relatively stable; associated with host name in DNS
- When it discovers it is in a foreign subnet (i.e., not its home subnet), it acquires a foreign address
  - uses auto-configuration to get the address
  - registers the foreign address with a home agent, i.e, a router on its home subnet
- Packets sent to the mobile's home address(es) are intercepted by home agent and forwarded to the foreign address, using encapsulation

Mobile IP (v4 version)

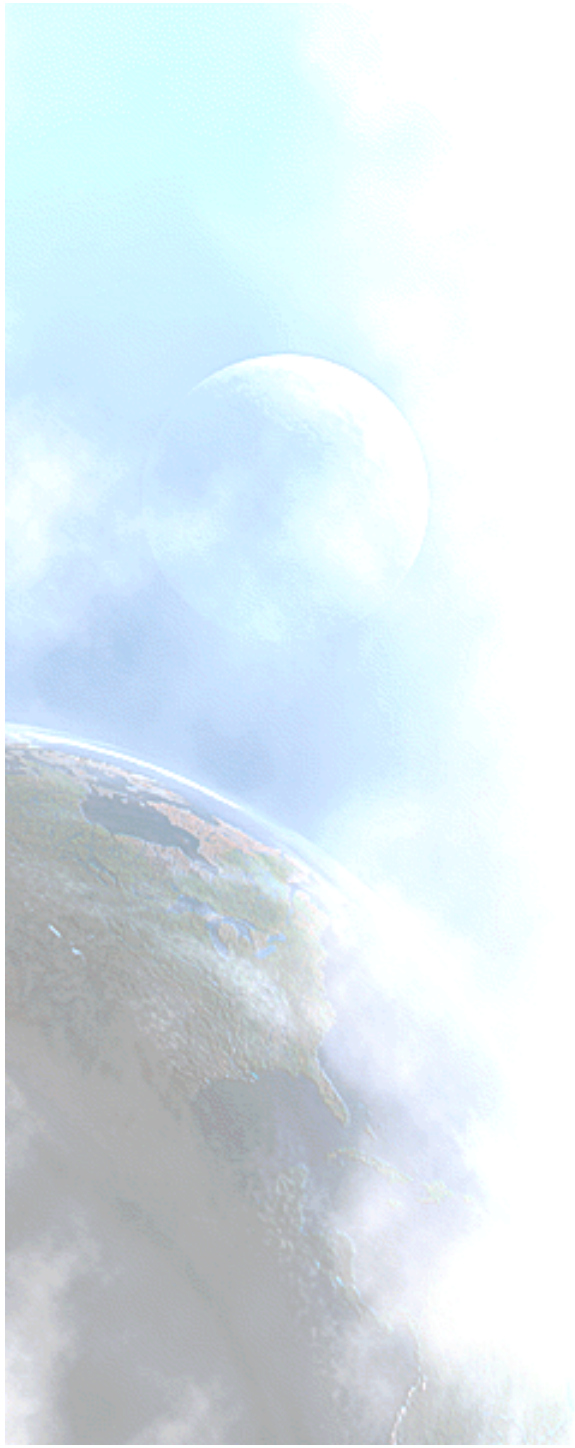


Mobile IP (v6 version)



Standards

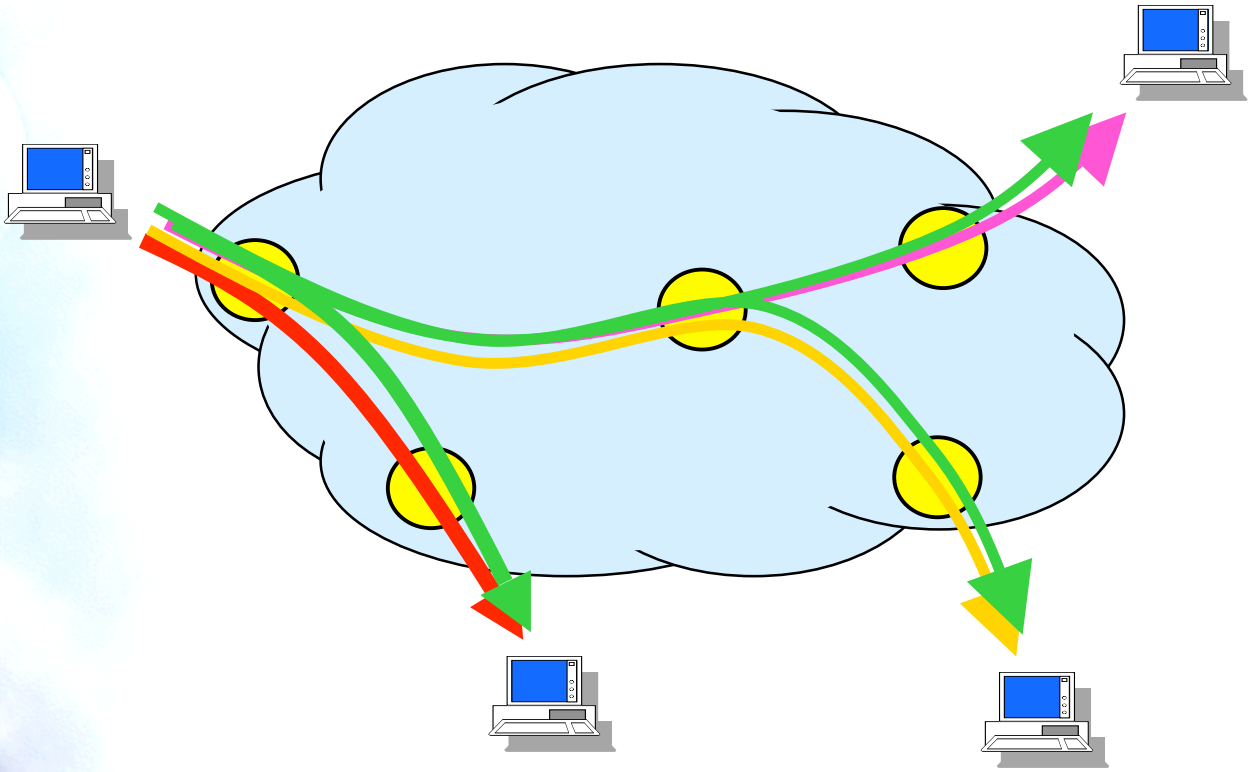
- Mobility Support in IPv6
  - RFC3775 – June 2004
- Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents
  - RFC3776 – June 2004



IPv6 Tutorial

Multicast

What's Multicast?



Applications

- Distributed systems
- Video on Demand (VoD)
- Radio/TV Diffusion
- Multipoint Conferencing (voice/video)
- Network Gaming
- Network level functions

How it Works ?

- The host joins/signoff the multicast group
- No restriction about number of groups or members per group
- Sending to the group don’t means belonging to it
- The destination address is a group address (multicast address)
- Connection-Less service

IPv4 vs. IPv6

- IPv4
  - Broadcast
    - Limited: 255.255.255.255
    - Directed: <network>11..1
  - Multicast
    - D Class:
      224.0.0.0 - 239.255.255.255
- IPv6
  - Multicast

Reserved Multicast Addresses (I)

- Node-Local Scope
  - FF01::1 All Nodes Address
  - FF01::2 All Routers Address

- Link-Local Scope
  - FF02::1 All Nodes Address
  - FF02::2 All Routers Address
  - FF02::4 DVMRP Routers
  - FF02::5 OSPFIGP
  - FF02::6 OSPFIGP Designated Routers
  - FF02::9 RIP Routers
  - FF02::B Mobile-Agents
  - FF02::D All PIM Routers
  - FF02::1:2 All-DHCP-agents
  - FF02::1:FFXX:XXXX Solicited-Node Address

Reserved Multicast Addresses (II)

- Site-Local Scope
  - FF05::2 All Routers Address
  - FF05::1:3 All-DHCP-servers
  - FF05::1:4 All-DHCP-relays

- Variable Scope Multicast Addresses
  - FF0X::101 Network Time Protocol (NTP)
  - FF0X::129 Gatekeeper
  - FF0X::2:0000-FF0X::2:7FFD Multimedia Conference Calls
  - FF0X::2:7FFE SAPv1 Announcements
  - FF0X::2:8000-FF0X::2:FFFF SAP Dynamic Assignments

Important Multicast Addresses

- FF01::1, FF02::1 All-nodes
- FF01::2, FF02::2, FF05::2 All routers

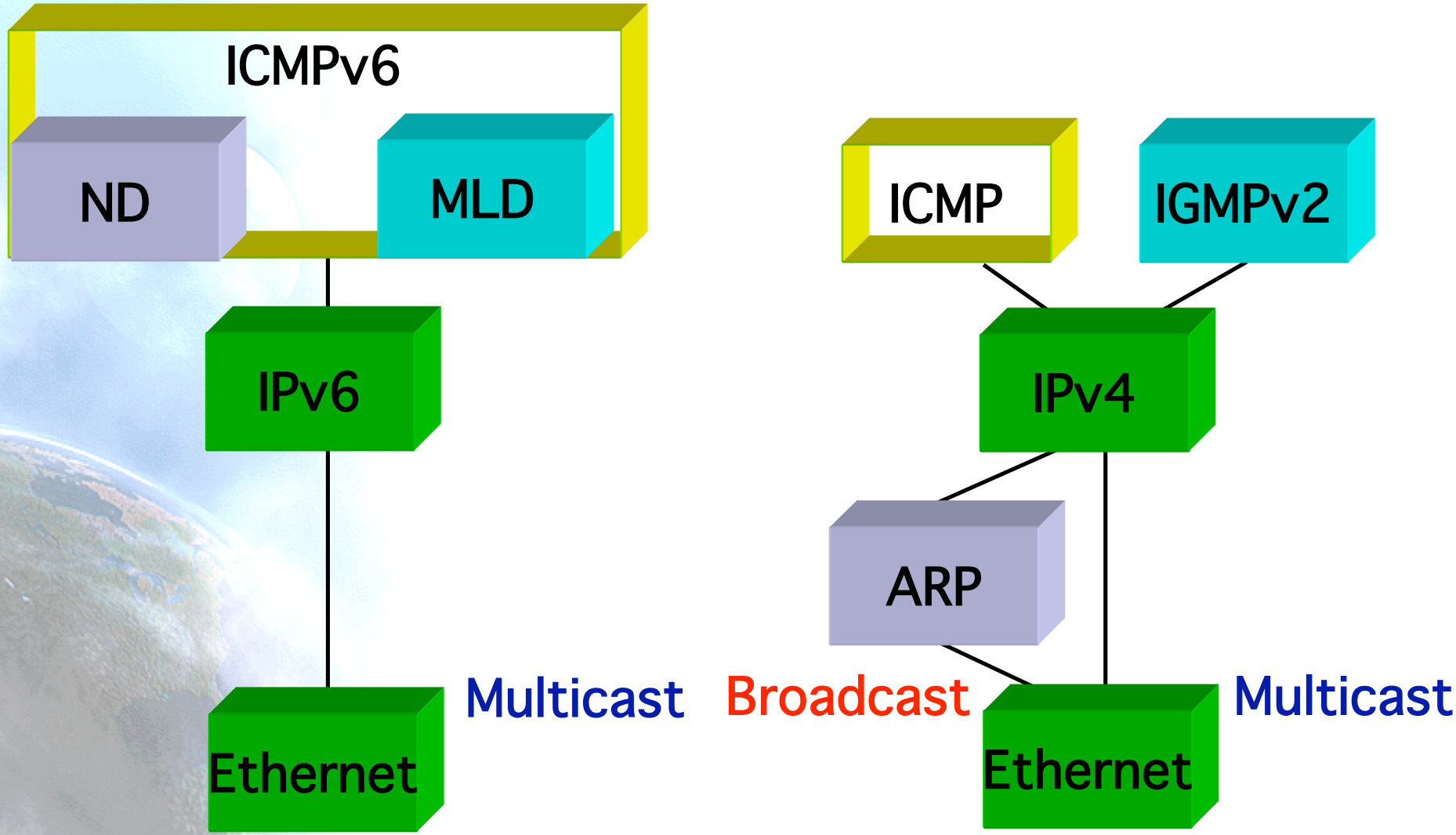
- Solicited Node (SN) address from a unicast one
  - For the address that finish with "XY:ZTUV"
  - the SN is FF02::1:FFXY:ZTUV

- Every IPv6 node must join SN for all its unicast and anycast addresses, and to "all-nodes"

Multicast Listener Discovery

- MLD (RFC2710) enables each IPv6 router to learn which multicast addresses have listeners on each of its directly attached links
- This is a mandatory function in IPv6 nodes
- Is used instead of IGMP

Control Plane IPv4 vs. IPv6



Multicast Routing

- Routers listen all the groups
- Multicast Routing Protocols:
- Dense Mode:
  - DVMRP
  - PIM-DM
  - MOSPF
- Sparse Mode:
  - CBT
  - PIM-SM

- Allow multicast tunnels over IPv6 unicast networks

IPv6 Tutorial

IPv4-IPv6 Coexistence & Transition

Transition / Co-Existence Techniques

A wide range of techniques have been identified and implemented, basically falling into three categories:

(1) dual-stack techniques, to allow IPv4 and IPv6 to co-exist in the same devices and networks

(2) tunneling techniques, to avoid order dependencies when upgrading hosts, routers, or regions

(3) translation techniques, to allow IPv6-only devices to communicate with IPv4-only devices

Expect all of these to be used, in combination

Dual-Stack Approach

- When adding IPv6 to a system, do not delete IPv4
  - this multi-protocol approach is familiar and well-understood (e.g., for AppleTalk, IPX, etc.)
  - note: in most cases, IPv6 will be bundled with new OS releases, not an extra-cost add-on
- Applications (or libraries) choose IP version to use
  - when initiating, based on DNS response:
    - if (dest has AAAA or A6 record) use IPv6, else use IPv4
  - when responding, based on version of initiating packet
- This allows indefinite co-existence of IPv4 and IPv6, and gradual app-by-app upgrades to IPv6 usage

Tunnels to Get Through IPv6-Ignorant Routers

- Encapsulate IPv6 packets inside IPv4 packets (or MPLS frames)
- Many methods exist for establishing tunnels:
  - manual configuration
  - "tunnel brokers" (using web-based service to create a tunnel)
  - "6-over-4" (intra-domain, using IPv4 multicast as virtual LAN)
  - "6-to-4" (inter-domain, using IPv4 addr as IPv6 site prefix)
- Can view this as:
  - IPv6 using IPv4 as a virtual link-layer, or
  - an IPv6 VPN (virtual public network), over the IPv4 Internet (becoming "less virtual" over time, we hope)

Translation

- May prefer to use IPv6-IPv4 protocol translation for:
  - new kinds of Internet devices (e.g., cell phones, cars, appliances)
  - benefits of shedding IPv4 stack (e.g., serverless autoconfig)
- This is a simple extension to NAT techniques, to translate header format as well as addresses
  - IPv6 nodes behind a translator get full IPv6 functionality when talking to other IPv6 nodes located anywhere
  - they get the normal (i.e., degraded) NAT functionality when talking to IPv4 devices
  - methods used to improve NAT functionality (e.g, RSIP) can be used equally to improve IPv6-IPv4 functionality

Thanks !

Contact:

- Jordi Palet Martínez (Consulintel): jordi.palet@consulintel.es

Madrid 2005 IPv6 Summit, soon available at:

www.ipv6-es.com