Introduction to IPv6

Praveen Gupta
pgupta@mobilestack.com

Why IPv6 ?

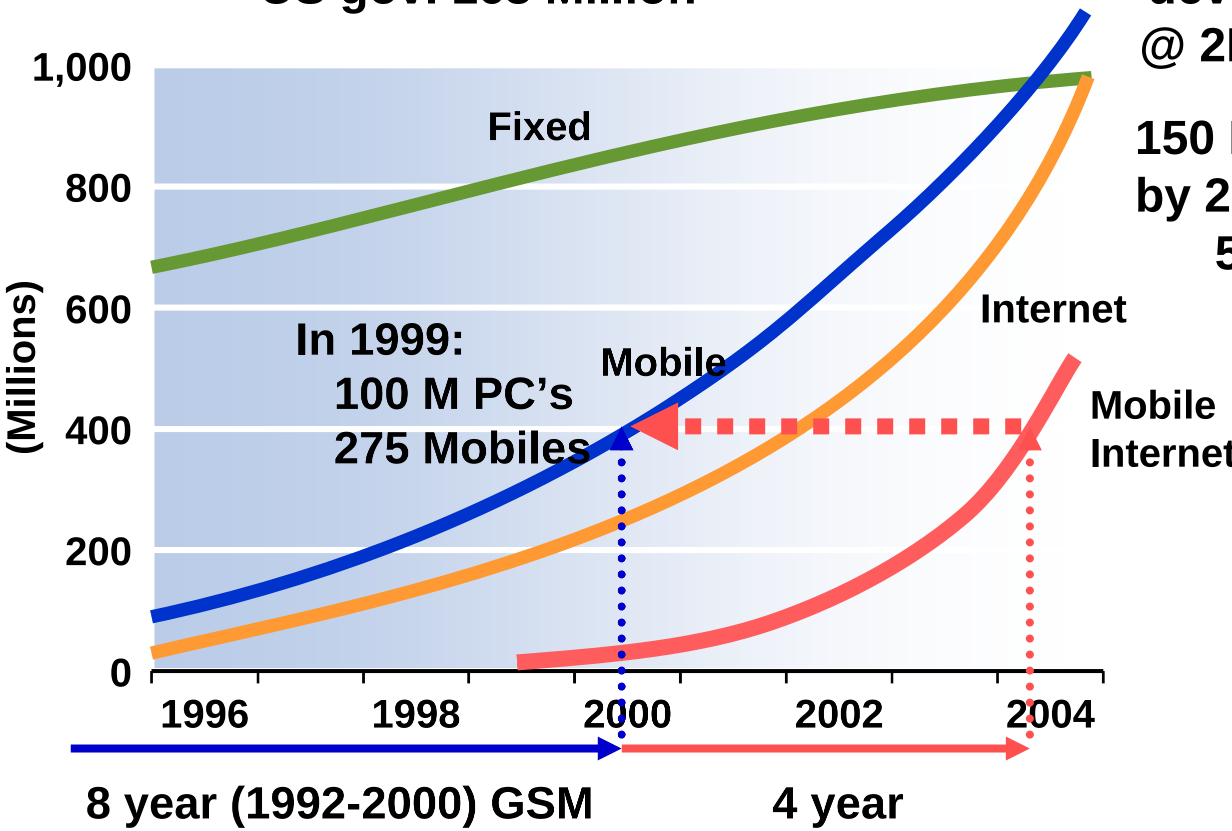
- The Mobile Internet
- Addressing
- Scalability
  - Autoconfiguration
  - End to end security (from day one)
  - End to end mobility (from day one)
  - Renumbering and multi-homing support
- Easy IP layer extensibility
- Migration from IPv4

Growth of the Mobile Internet

IPv4 addresses: 4B theoretical
- **China: 9 Million**
- **Europe: 80 Million**
- **US gov. 168 Million**

1980: 200 user on 1 mainframe
2000: 1 mobile + 1 PC per user
2020: 200 Embedded, wireless devices per user
@ 2B humans is 400B

150 Million new users by 2003-2004 implies 500.000/day



IPv4 vs IPv6

Addressing

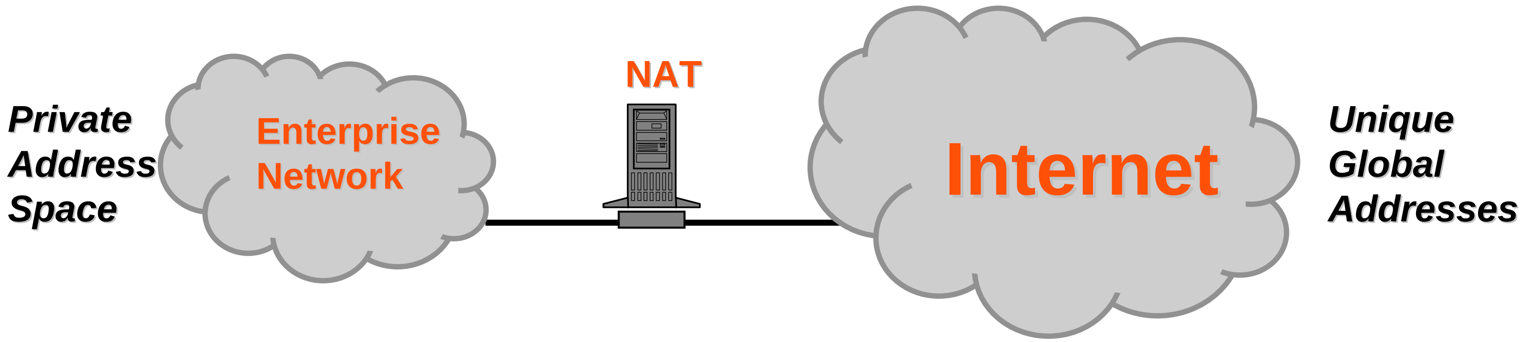
- Improved Addressing and Routing
  - IPv6 defines a Multi-level Hierarchical Global routing architecture
  - Scalable routing hierarchy
  - Decreases the size of the routing tables
  - Faster updates of routing tables

IPv4 Approach

- Classless InterDomain Routing (CIDR)
- CIDR does not guarantee an efficient and scalable hierarchy
- Renumbering is complex

End to End communication

- Eliminating Special Cases
  - Problems for Enterprises to summarize its routes
    - » No need for private addresses



IPv4 Approach (NAT and Gateway)

- Substituting addresses is very demanding
- NAT causes scalabilty problems
- Less reliability
- Must parse all applications that embed IP addresses
- Can break DNS (DNS works above the network layer)
- NAT breaks end-to-end security

End to end communication

- Security
  - IPv6 offers security header extensions (AH and ESP)
  - Standard method to achieve network security
  - Required to support MD5 and SHA-1 for authentication and integrity
  - The specification is algorithm-independent, other techniques may be used
  - True end-to-end security

IPv4 Approach

  - Install Firewalls (for packet filtering and security checks)
  - IPv4 supports ESP, but not mandated in the standard

End to end communication

- Minimizing Administrative Workload
  - Uses stateless autoconfiguration to create:
    - Local IPv6 addresses
    - Global IPv6 addresses (using a local IPv6 router)
  - Stateful address autoconfiguration (DHCPv6)

IPv4 Approach

- Network information have to be installed at each network node
- DHCP is better but gives new problems
- Problems to change IP address when ISP is changed

Mobility

- Mobility
  - Mobility is part of the IPv6 implementation
  - End to end route optimisation
  - More efficient tunnelling

IPv4 Approach

- Needs a forwarding address at each new point of attachment (FA)
- Requires more network support
- Authentication not commonly deployed in IPv4 nodes
- Route optimization is not end to end and only works for CNs supporting MIP.
- Route optimisation unlikely to be widely deployed

A deeper look..

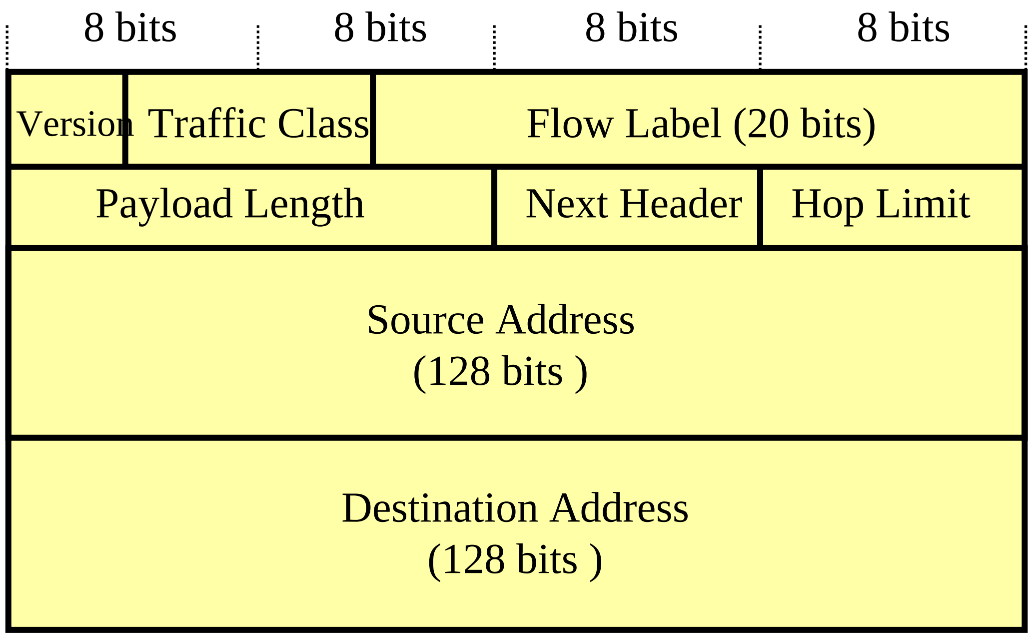
Introduction

- Defined in RFC 2460
- Expanded addressing Capabilities
  - Increases the address size from 32 bits to 128 bits.
  - Support more levels of addressing hierarchy.
  - Possible to address a much greater number of nodes.
  - Simpler auto-configuration of addresses.
- Header Format Simplification
  - Some IPv4 headers have been dropped or made optional.
  - Faster processing of the IPv6 header.
- Improved Support for Extensions and Options
  - IP header options are encoded in a way that allows more efficient forwarding.
  - Less stringent limits on the length of options.
  - Greater flexibility for introducing new options in the future.

Introduction

- Flow Labeling Capability
  - Possible to label packets belonging to particular traffic flows for which the sender requests special handling.
  - Standardization in progress
- Authentication and Privacy Capabilities
  - Extensions defined to support:
    - Authentication
    - Data integrity
    - Data confidentiality

IPv6 Header Format



Version	6	**Payload Length**	Length of IPv6 payload
Traffic Class	Priority of IPv6 packets	**Next Header**	Type of header following the IPv6 header
Flow Label	Special handling of packet	**Hop Limit**	Decremented by 1 in each router

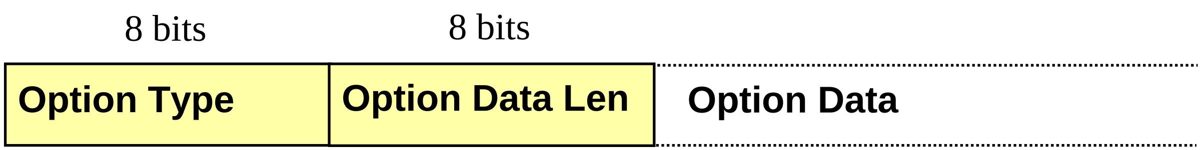
IPv6 Extension Headers

- IPv6 Header
- Hop-by-Hop Options Header
- Destination Options Header-1
- Routing Header
- Fragmentation Header
- Authentication Header
- Encapsulation Security Payload Header
- Destination Options Header-2
- Upper-layer Headers
- Payload

The suggested order for the extension headers

Hop-by-Hop & Destination Headers

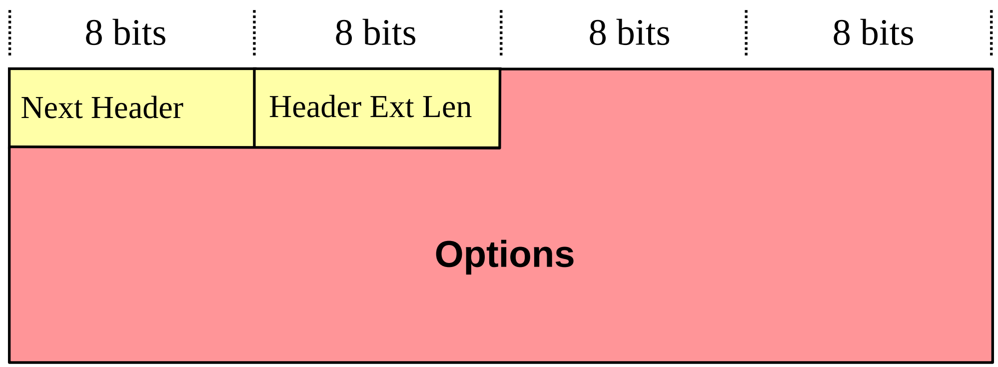
- The Hop-by-Hop and Destination Headers carry a variable number of type-length-value (TLV) encoded options



Option Type Identifier of the type of option

Option Data Len Length of the Option Data field of this option

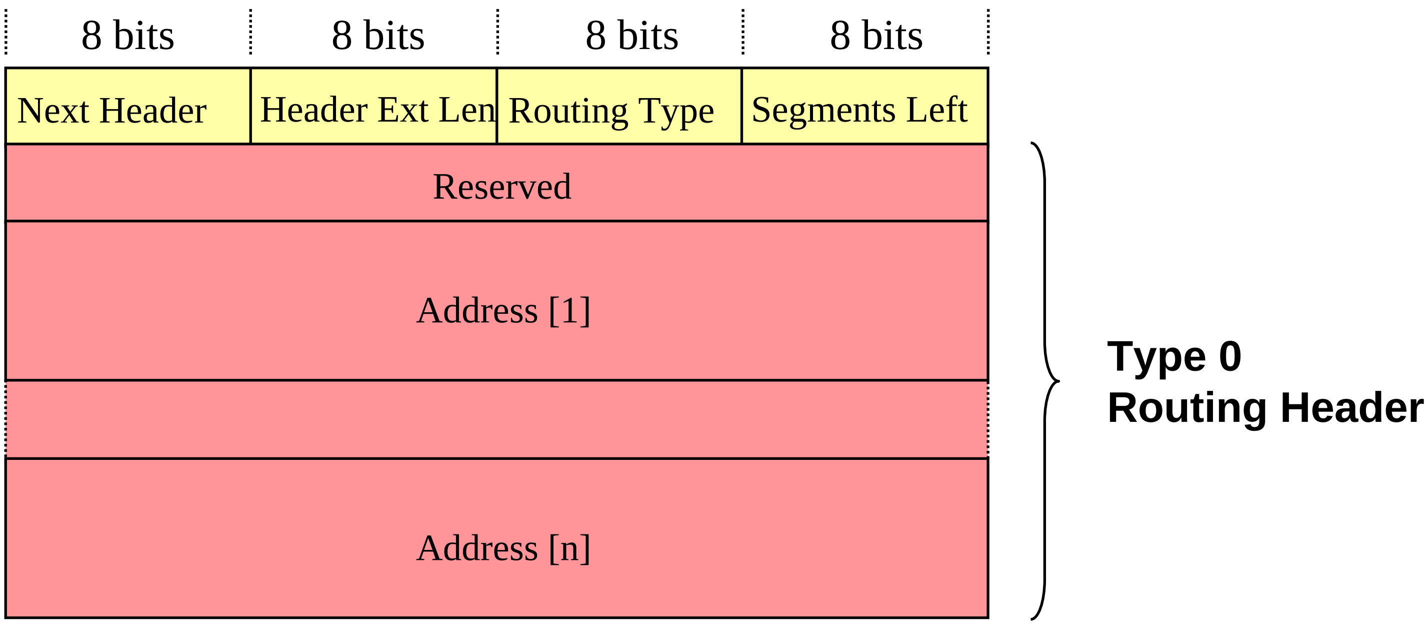
Option Data Option type specific data of variable length
It may include sub-options being TLV encoded



Hop-by-Hop Options Header
&
Destination Options Header

Routing Header

- Used by an IPv6 source to list one or more intermediate nodes to be routed through on the way to the packets destination.

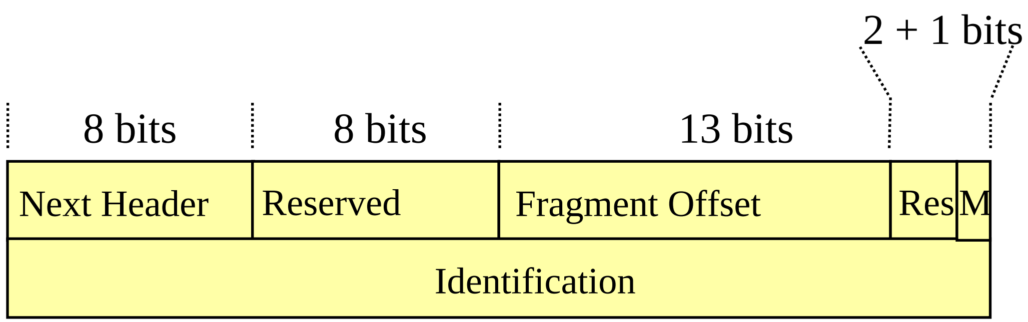


Routing Type Identifier of a particular Routing header variant

Segments Left Number of route segments remaining to be visited

Fragment Header

- Used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination.
- Fragmentation is only performed by the source node.



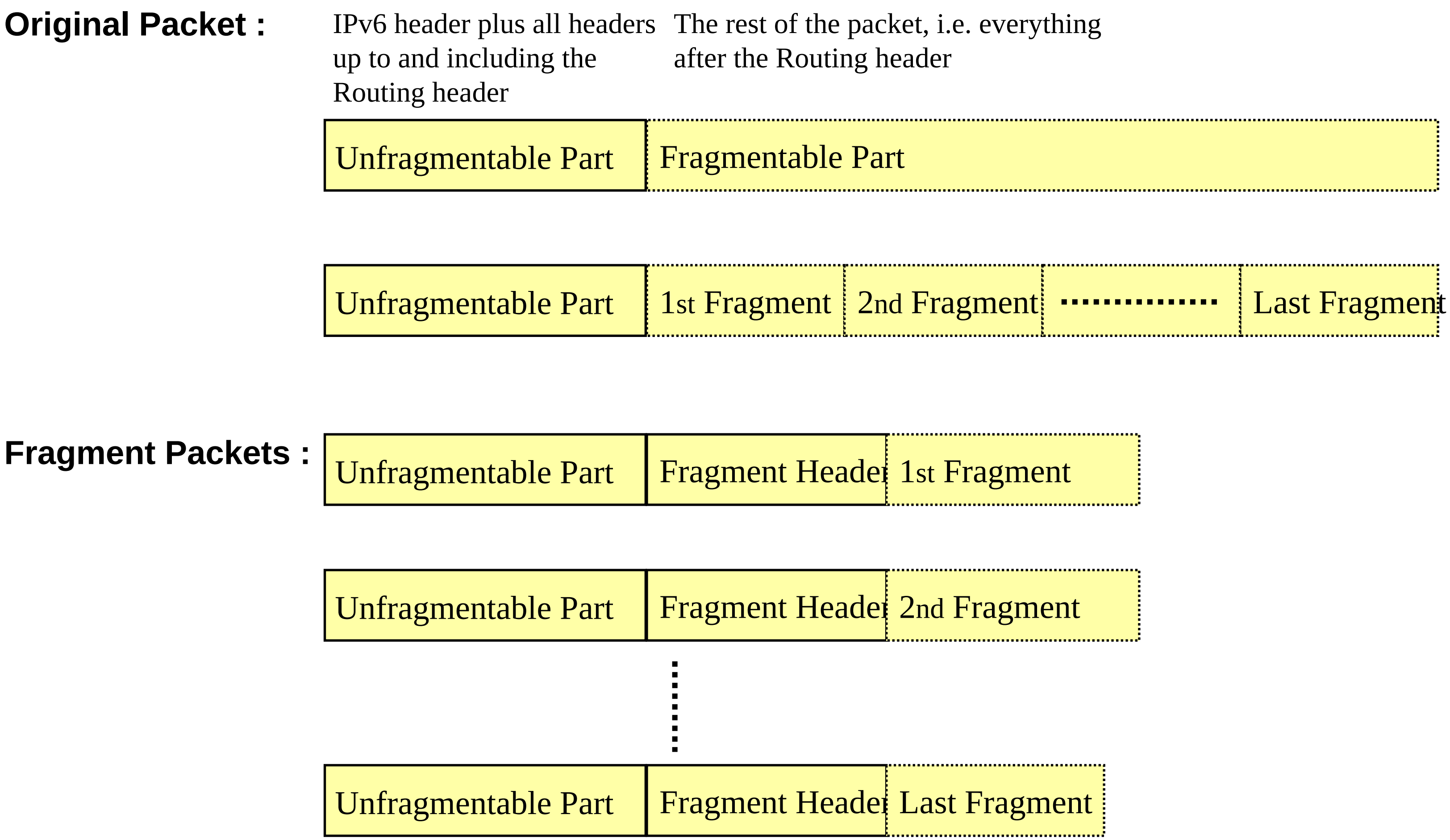
Next Header Identifies the initial header type of the fragmentable part of the original packet.

Fragment Offset The offset of the data following this header.

M flag 1 = more fragments; 0 = last fragment

Identification Unique identifier for each fragmented packet.

Fragment Header (cont.)



Packet Size Issues

- IPv6 requires that every link have an MTU of 1280 octets or greater.
- Implementation of path MTU discovery (RFC 1981) recommended.
- Links not able to convey 1280 octet packets must perform fragmentation and re-assembly at a layer below IPv6.

Support for Network renumbering and multihoming

- Renumbering is needed for corporate mergers, change of ISP's, Network expansion ..etc
- IPv6 allows for a smooth renumbering mechanisms using the Neighbour Discovery specification
- Renumbering can take place over weeks
- Hosts are multihomed during renumbering
- Multihoming can also be used for reliability (connecting to two ISPs)
- Several proposals currently exist to solve the multihoming problem in IPv6

IP Security

Authentication Header

- Provides authentication of IP datagrams.
- Authentication for parts of the IP header and upper layer protocols.

8 bits	8 bits	16 bits
Next Header	Payload Len	Reserved
Security Parameter Index (SPI)		
Sequence Number Field		
Authentication Data (variable)		

Payload Len The length of the AH in 32-bit words.

SPI An arbitrary 32-bit value that in combination with the destination IP address and AH uniquely identifies the SA for this datagram.

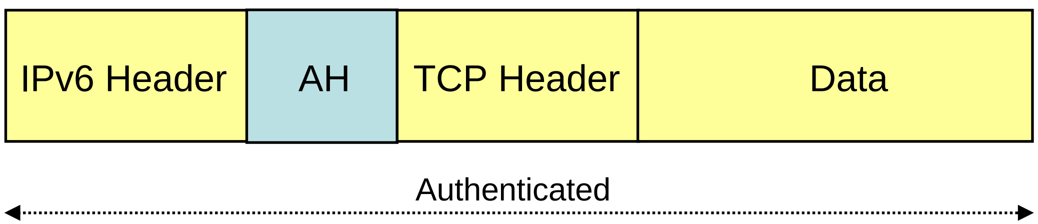
Seq no Field Increasing counter value.

Auth. data Contains the Integrity Check Value (ICV) for the packet.

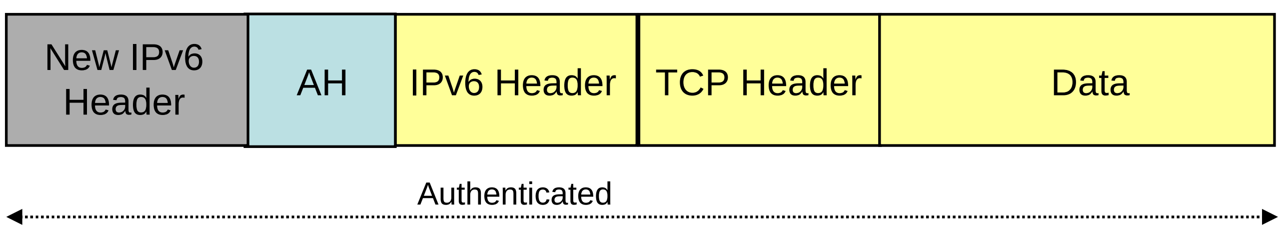
Authentication Header (cont.)

- The AH may be applied in transport or tunnel mode

Transport Mode:

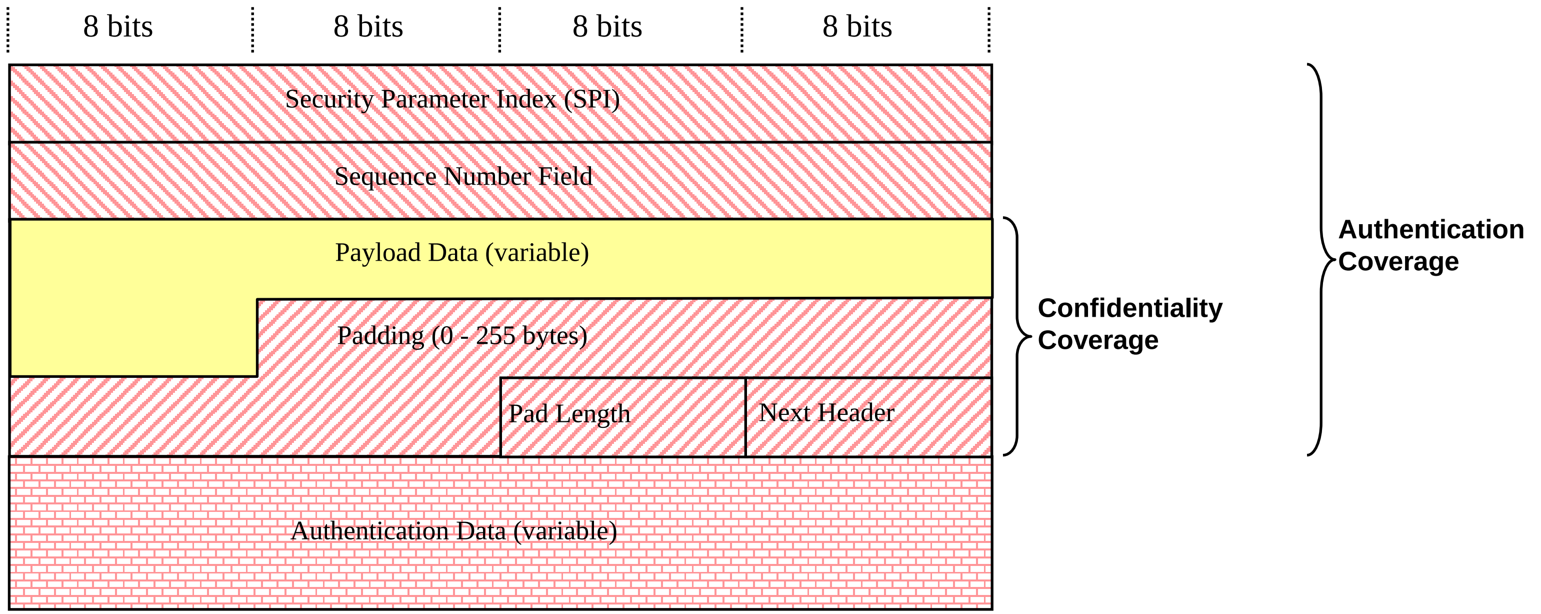


Tunnel Mode:



Encryption Security Payload Header

- Provides confidentiality and authentication of IP datagrams.



Payload Data Contains data described by the next header field.

Padding Only used if required for ESP calculation.

Pad Length The number of pad bytes.

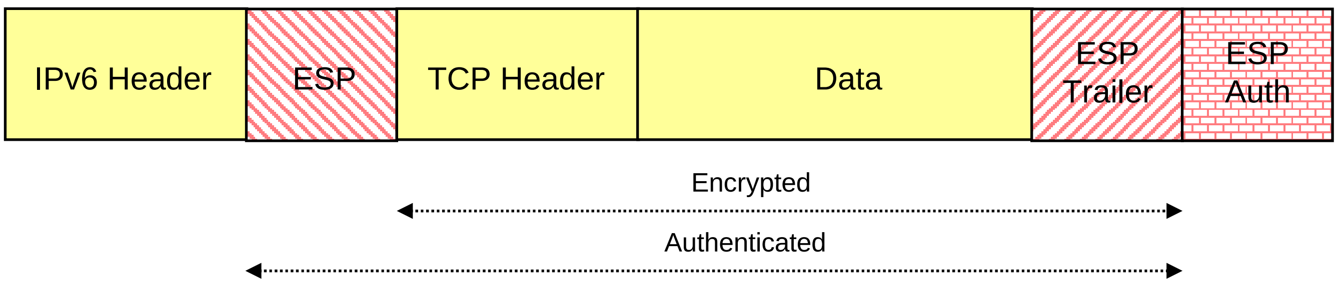
Next Header Identifies the type of data contained in the Payload Data field.

Auth. data Contains the Integrity Check Value (ICV) for the ESP packet not including the Authentication Data field.

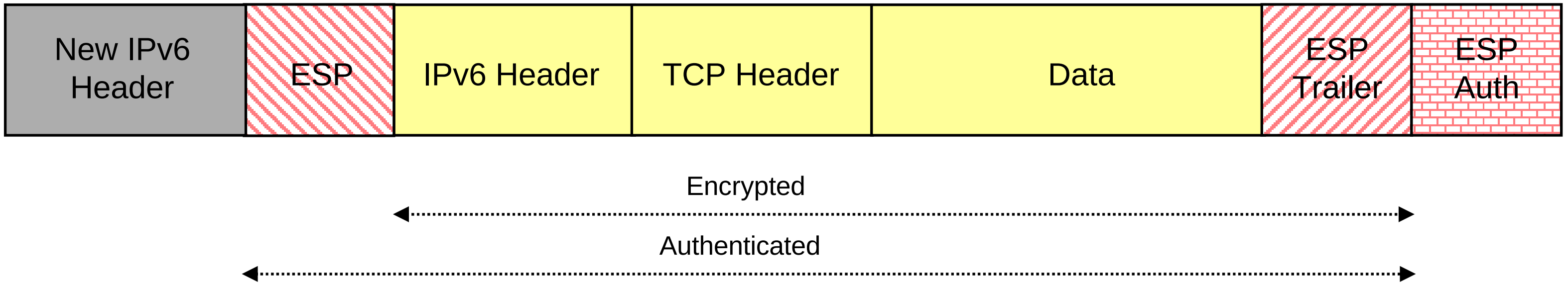
Encryption Security Payload Header (cont.)

- The AH may be applied in transport or tunnel mode

Transport Mode:

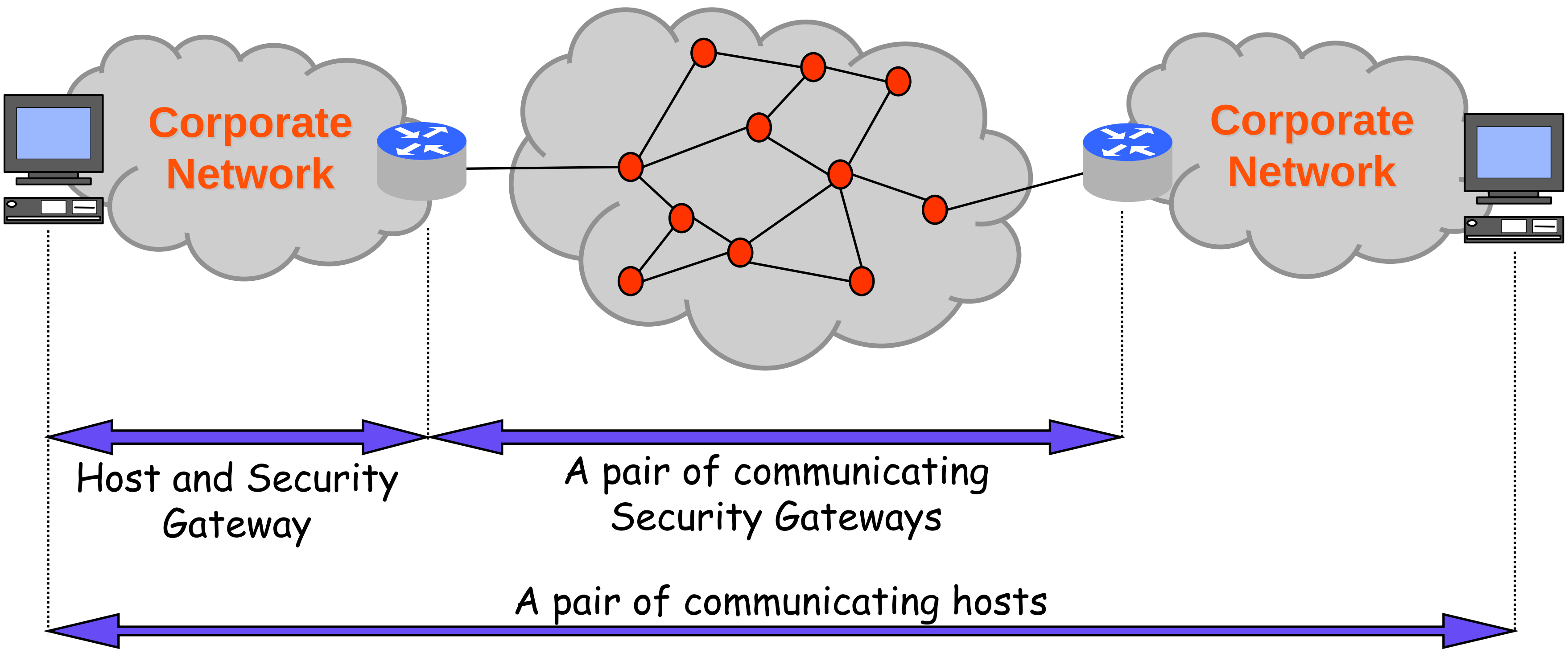


Tunnel Mode:



Security Services

Security services can be provided between:



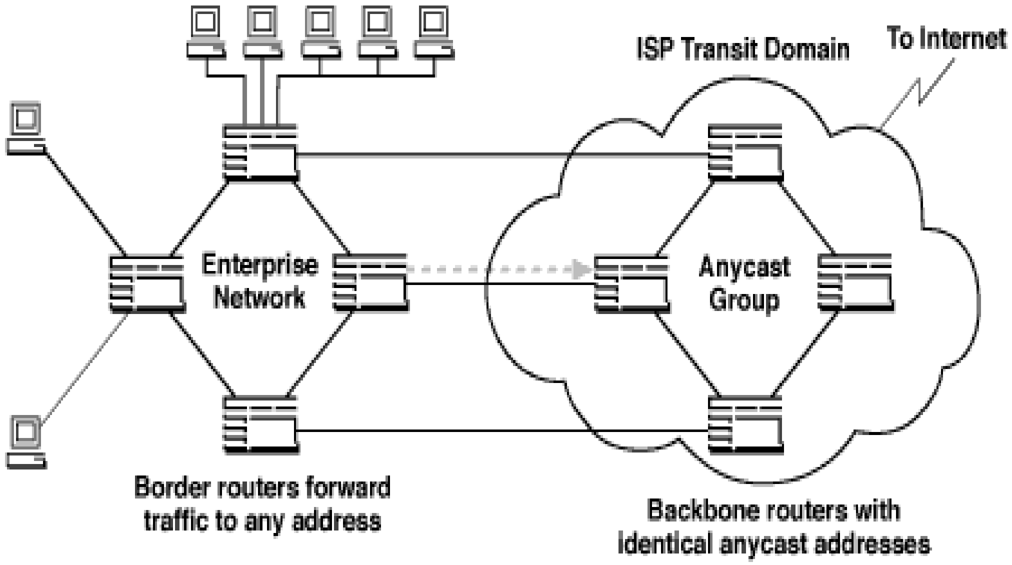
Addressing

Address Types

There are three different addresses

•	Unicast	An identifier for a single interface
•	Anycast	An identifier for a set of interfaces. A packet sent to an Anycast address is ***delivered to one of the interfaces*** identified by that address
•	Multicast	An identifier for a set of interfaces. A packet sent to a multicast address is ***delivered to all interfaces*** identified by that address.

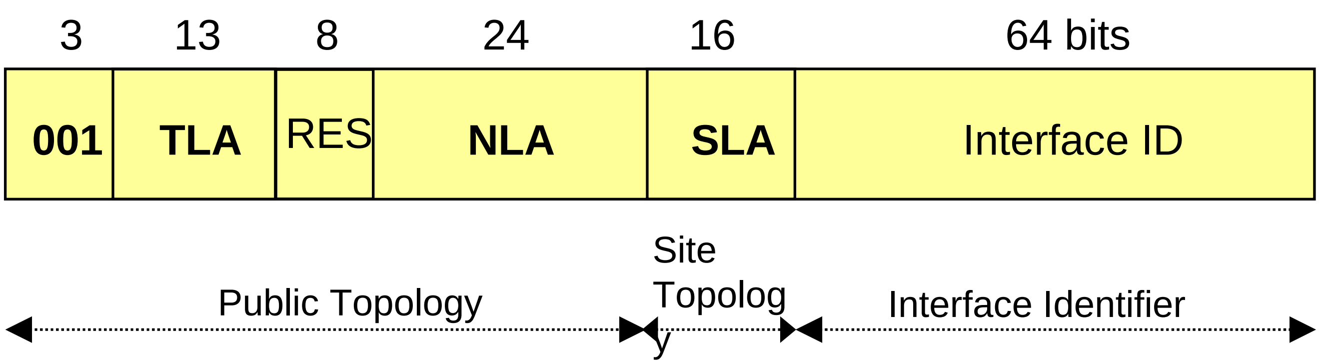
Anycast addresses could be used for the nearest node of a certain service



The Aggregatable Address

IPv6 Aggregatable Global Unicast Address Format

- Scalable design
- Efficient routing hierarchy
  - TLA - Top Level Aggregator
  - NLA - Next Level Aggregator
  - SLA - Site Level Aggregator



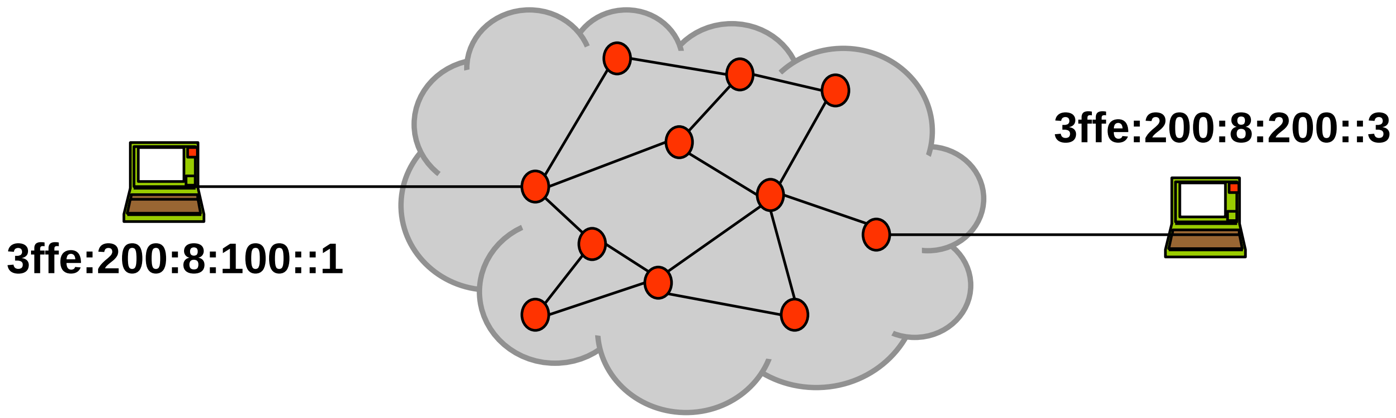
Neighbour discovery

- Based on assembling all ARP (IPv4) functions and more on the IP layer
- Allows for the use of security
- Based on ICMP messages
  - Neighbour solicitation
  - Neighbour advertisement
  - Router solicitation
  - Router advertisement
    - Contains several options (sets of information)
    - Prefix, MTU, Link layer address and other possible extensions
  - Allows for stateless address autoconfiguration
  - Allows for easy renumbering by advertising multiple prefixes
  - Allows for multihoming by advertising multiple prefixes

Mobility

Internet Routing

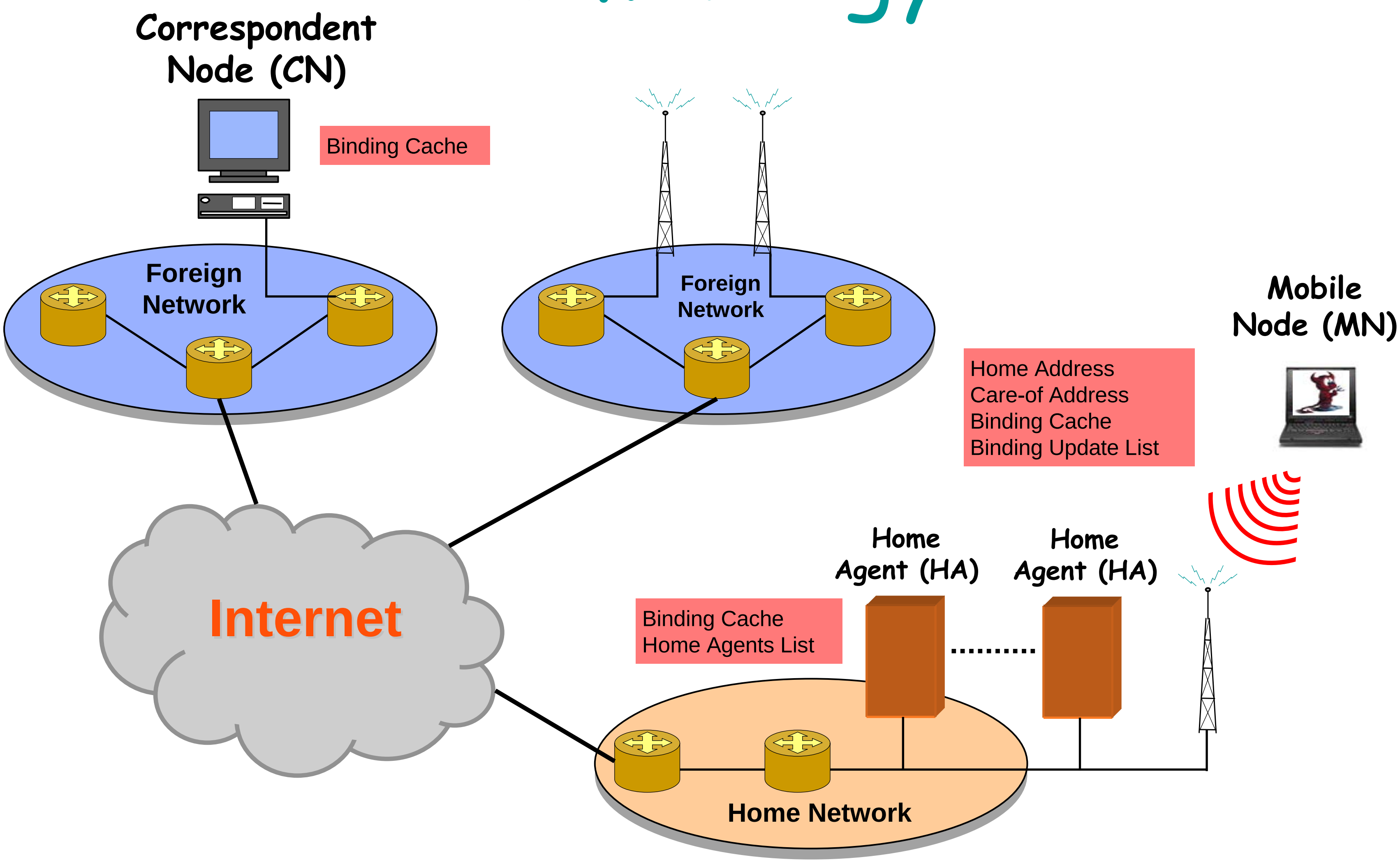
- IP Datagrams flow between links via routers
- Hosts send packets based on their IP address (DNS resolving)
- Internet routing is dynamic, unpredictable and best-effort




```
Connection = {source IP, source port, dest. IP, dest. port}
```

- **Underlying assumption: IP addresses define the topology of connections between hosts (hierarchical topologically-based addressing)**

Terminology



Control Messages

Binding Update Option

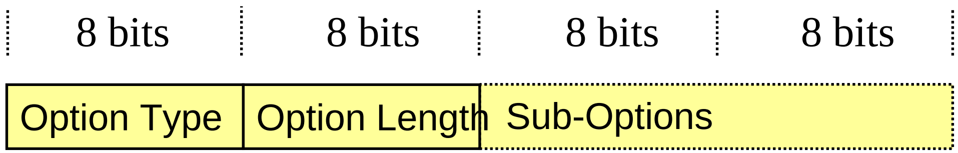
8 bits	8 bits	8 bits	8 bits
		Option Type	Option Length
A H R D	Prefix Length	Sequence Number	
Lifetime			
Sub-Options			

Binding Acknowledgement Option

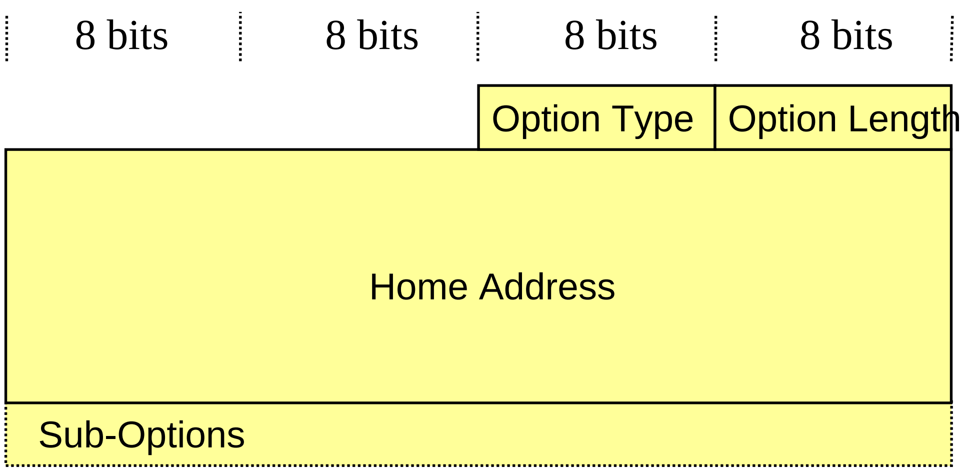
8 bits	8 bits	8 bits	8 bits
			Option Type
Option Length	Status	Sequence Number	
Lifetime			
Refresh Time			
Sub-Options			

Control Messages

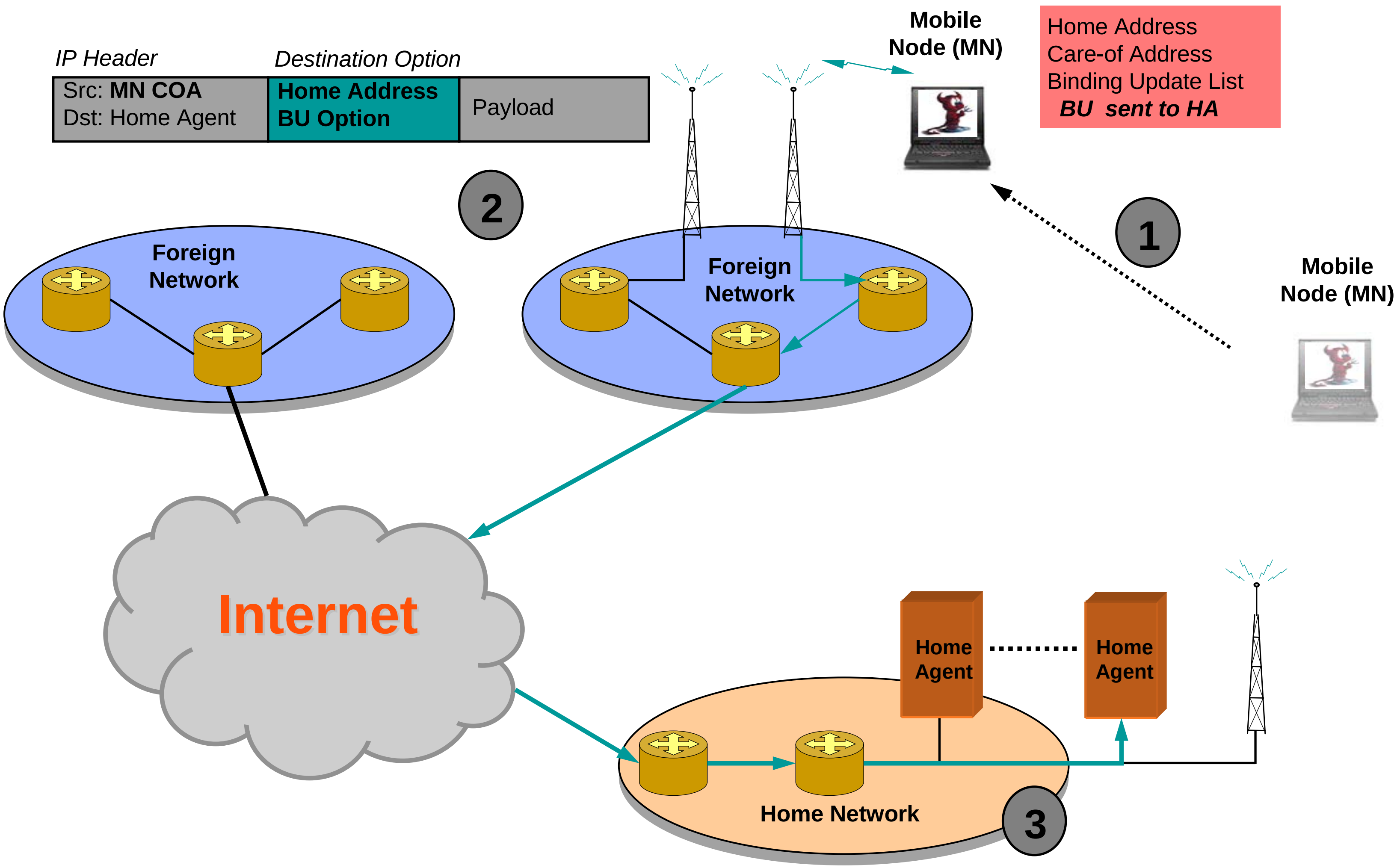
Binding Request Option



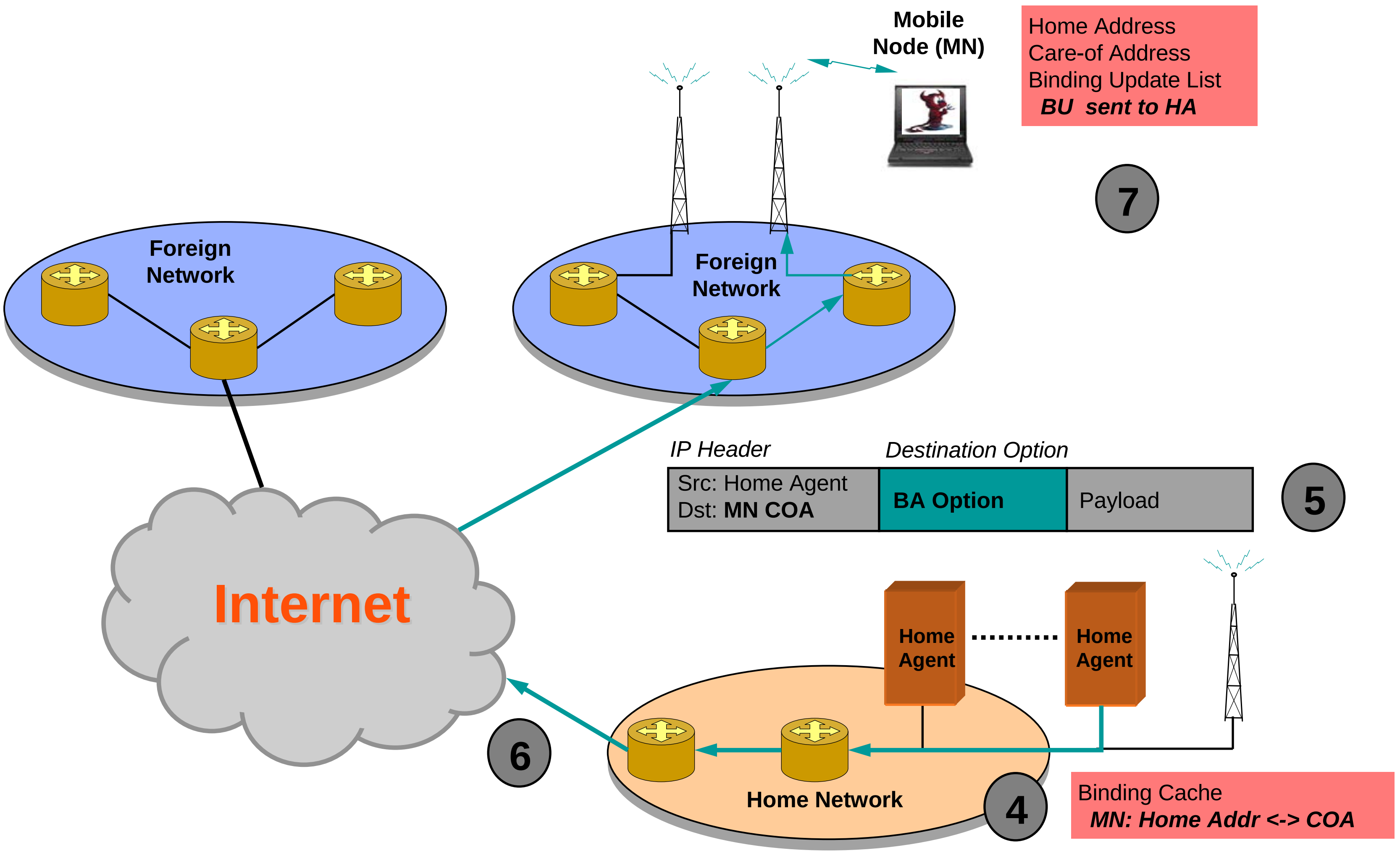
Home Address Option



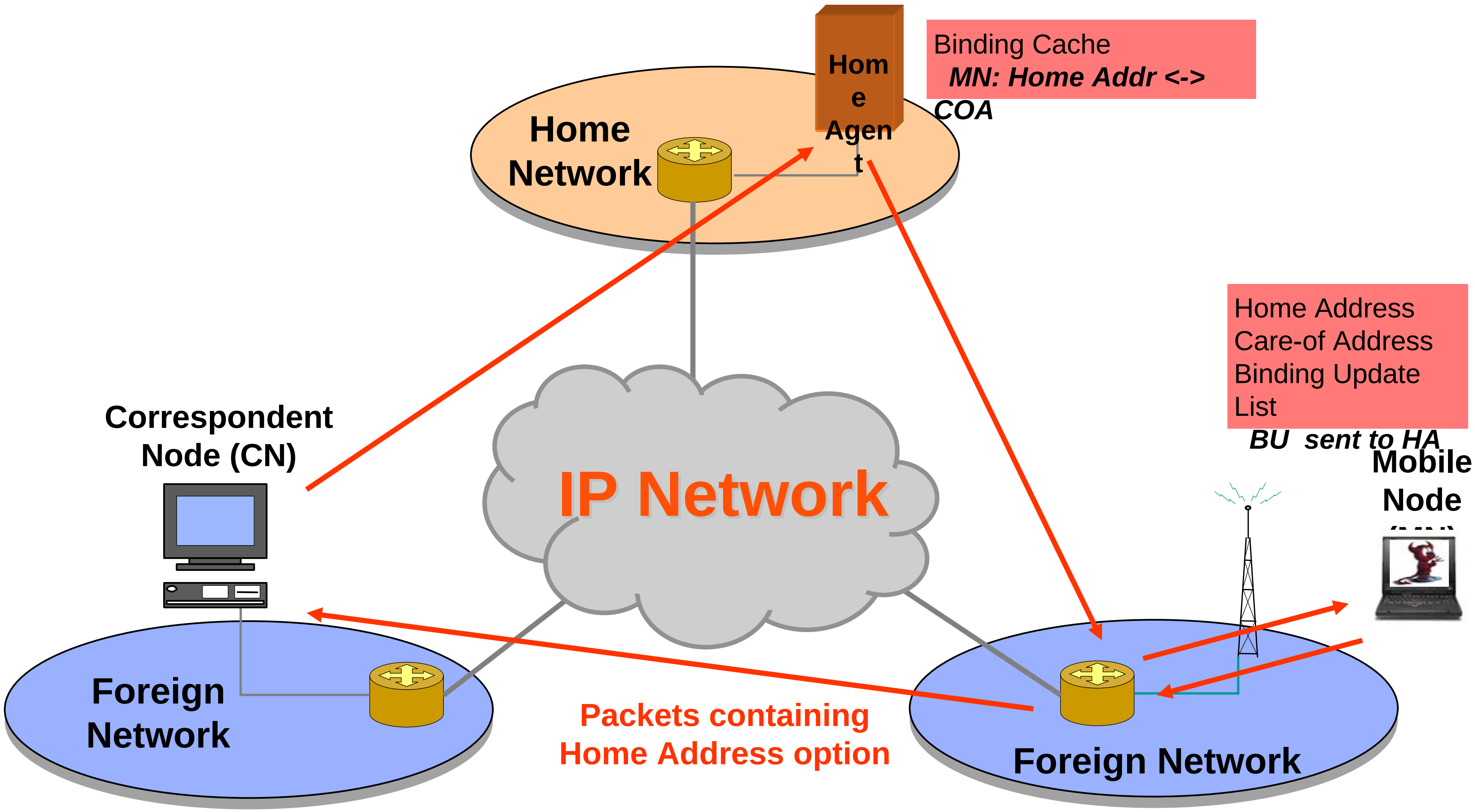
Registration



Registration (cont.)



Triangular Routing



Route Optimization