Mobility Management in the Internet

Yuri Ismailov
Ericsson Research, Stockholm, Sweden

Objectives

- To get acquainted with issues around networking and mobility
- To understand various approaches providing solutions for mobile networking
- To understand research issues in the area of mobile communications
- To inspire research in the area of mobile communications

Prerequisites

- Basic knowledge of computer communications
- Basic knowledge of TCP/IP communication suite

Outline

- Introduction
- OSI Model Walk Through (mobility related features)
- Mobility Management Mechanisms Overview
  - Mobile IPv4
    - Mobile IPv4 NAT traversal
  - IPv6 Essentials (mobility related focus)
  - Mobile IPv6
  - Identifier – Locator split
    - Step aside Introducing endpoints
    - Level 3 Multi-homing Shim Protocol for IPv6 (SHIM6)
    - Step aside to multi-access and IETF MEXT activities
    - Host Identity Protocol (HIP)
  - Transport Layer Solutions
    - Focus on "Migrate" and SCTP
  - Mobile Sockets proposals overview (a word on mobile agents)
  - Session Layer Proposal
- Conclusions: Issues, Challenges, Where are we heading to?

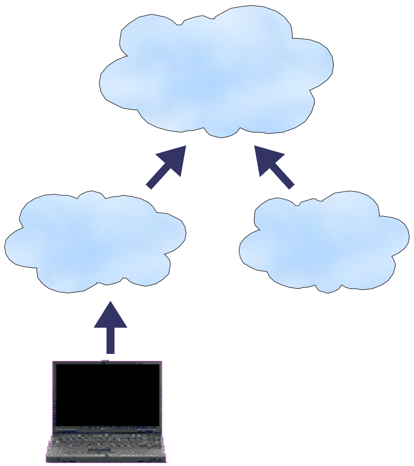
Introduction
What is Mobility and What is Mobile?

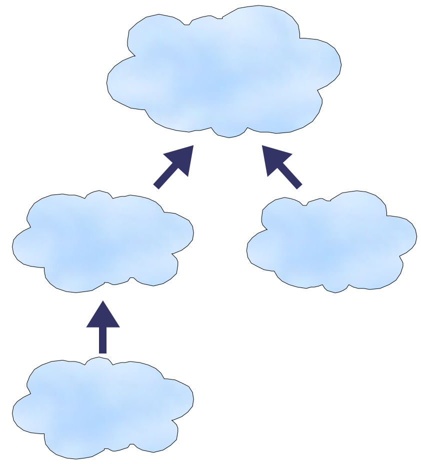
What is Mobility?

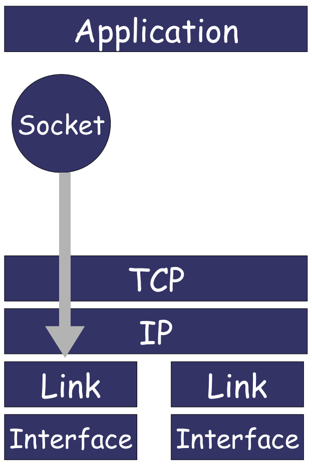
- There is no strict definition of mobility
- RFC 3344 "Mobility Support for IPv4" and RFC 3775 "Mobility Support in IPv6" mention the following:
  - Packets may be routed to the mobile node using this address (Home Address) regardless of the mobile node's current point of attachment to the Internet
  - For a node to change its point of attachment without losing its ability to communicate ...

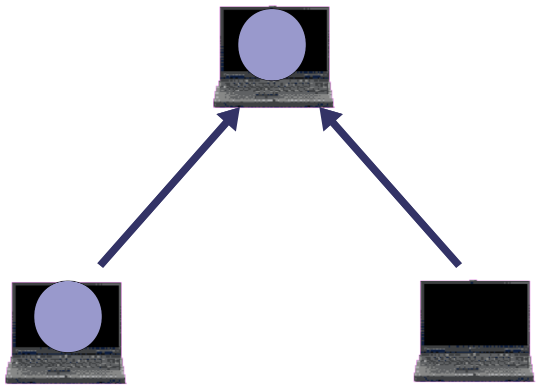
Mobile device changes its point of attachment to the network

Examples of What May be Mobile









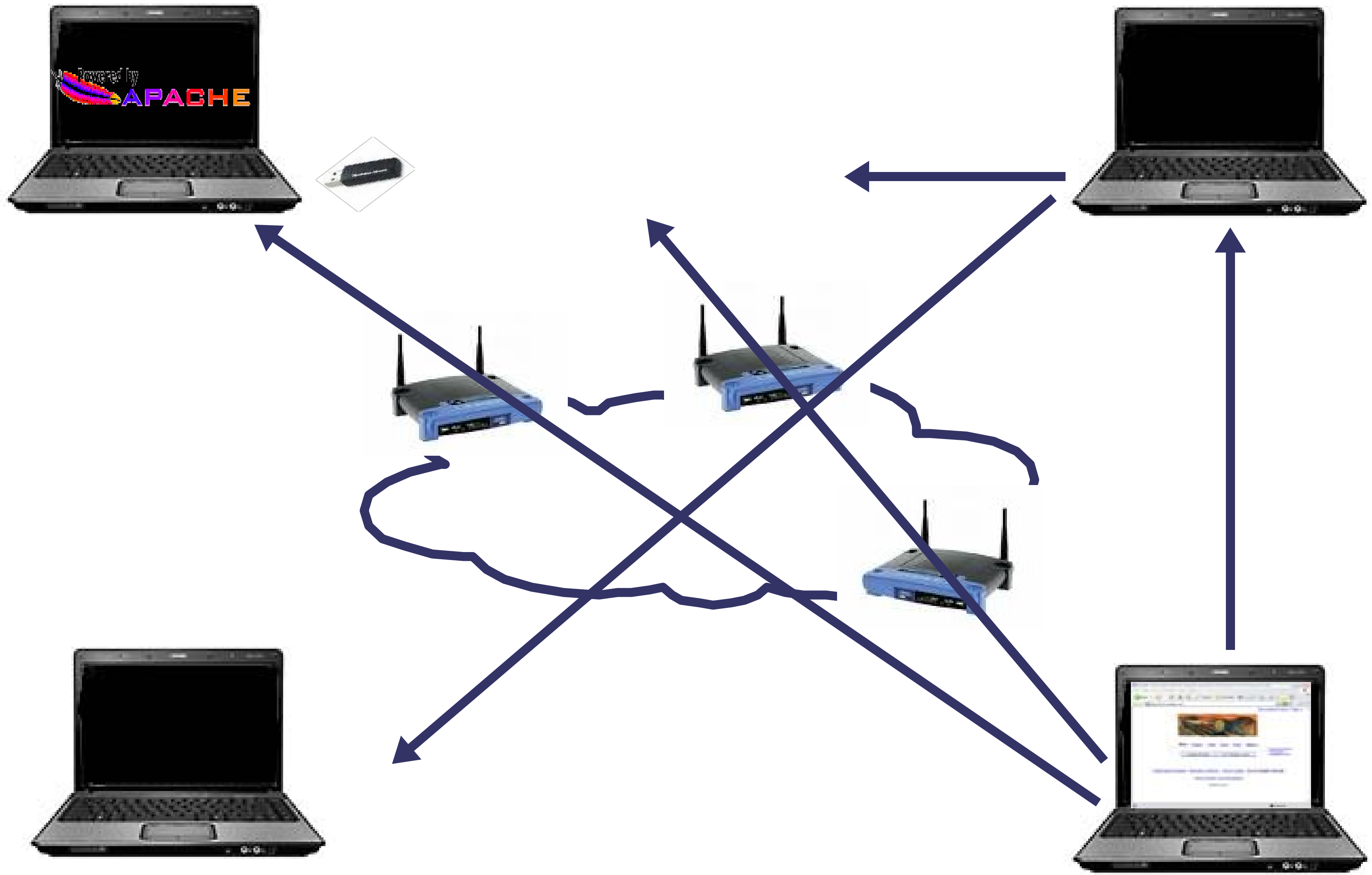
Vision

- Mobility is when something changes with regard to networked objects
- Mobility support is:
  - If mobile resource of any type changes its point of attachment, context, preferences, policies, and anything else, what can be change – this, results in adequate system reaction providing continuous reachability and communication continuity

Key Issues Influencing Mobility Support

- Naming and addressing – what to name and how (both syntax and semantics). How to resolve names and what should be the result of name resolution.
- Dynamic bindings – which part of the name is static and which can change (Locater-Identifier Split). How to keep consistency.
- State management – which state (part) information has to be preserved across a handover, temporarily disconnections, network outages, deliberate communication suspend/resume actions, etc.
- Utilization of information at all layers (sub-layers) of the stack – useful for optimizations and proper control of dynamic bindings
- Interaction with applications – revealing data from the stack to applications letting them to have some control over this data, and notifying applications about critical events taking place inside the stack
- Protocol support for consistent updates of involved in mobility support nodes

Naming and Addressing: What to Name?



Naming and Addressing: What to Name?

Static/Persistent Name vs. Dynamic/Changeable

http:// www.computer.com /whatever/directory/ file.html

- http:// → Service Name → Static → Mapped to Port Number → Dynamic
- www.computer.com → Computer Name → Static → Mapped to IP Address → Dynamic
- /whatever/directory/ → Directory Path Name → Dynamic
- file.html → File Name → Dynamic

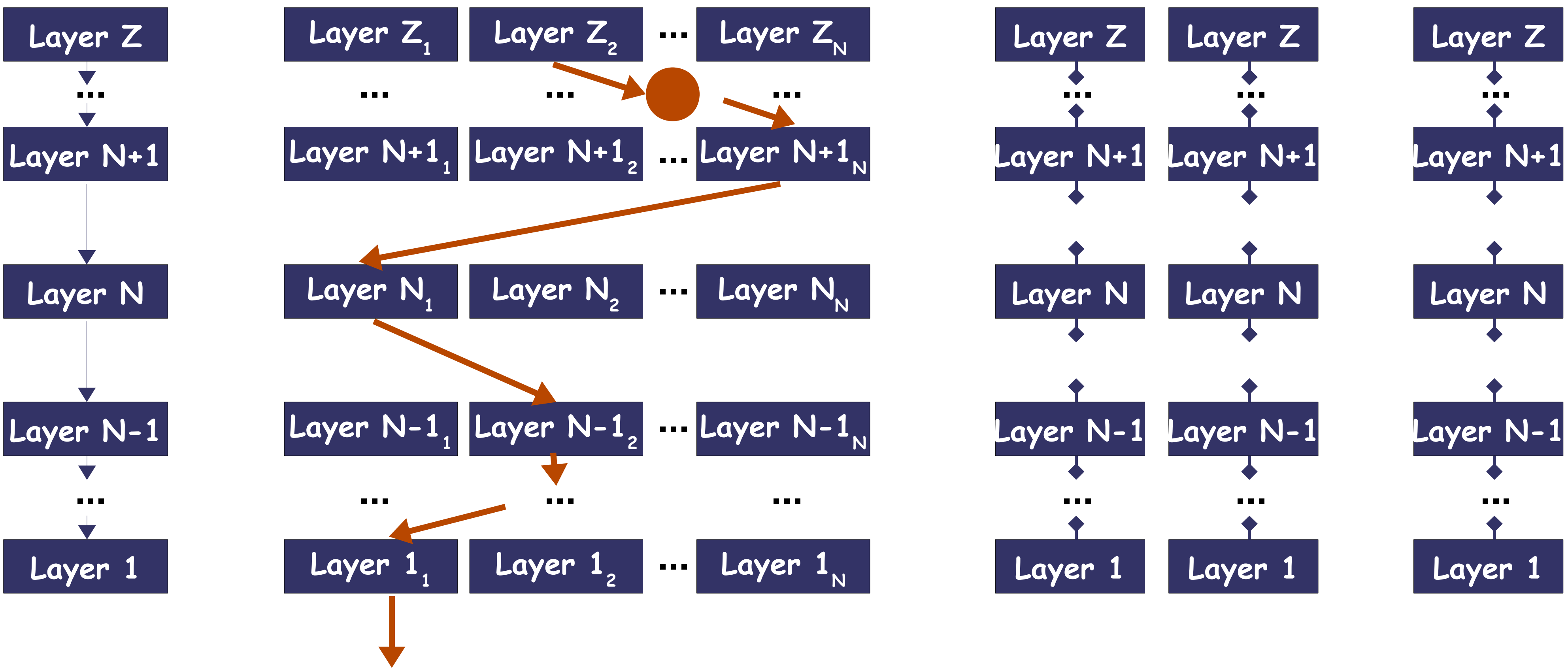
Think of two issues:

1. Naming and Addressing
2. Dynamic Bindings

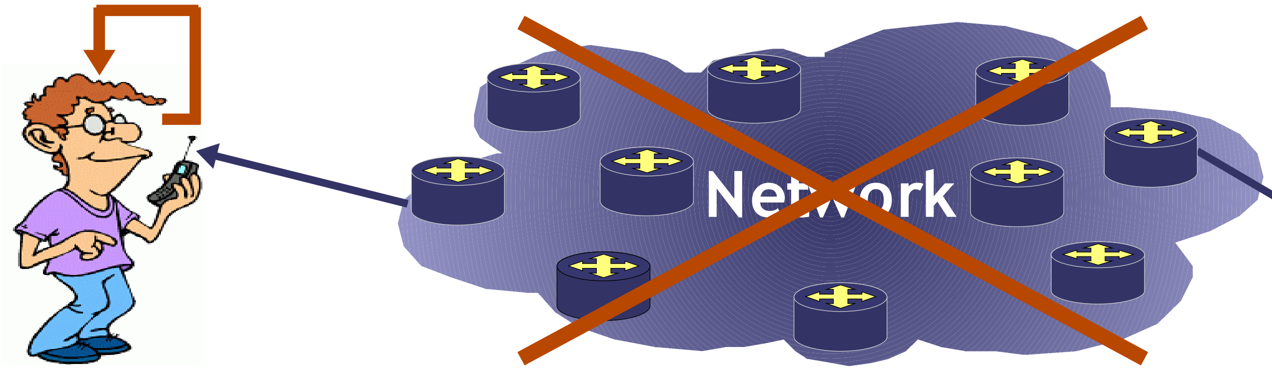
Naming and Addressing: Decoupling of Objects

- Decoupling of networked objects leads to:
  - Need of persistent name for each "movable" object
  - Need of capability to dynamically rebind persistent name to any other name with the life-time shorter than the persistent name of the object

Dynamic Bundling of Names



Example of State Preservation and Transfer



Session Establishment
(authentication and session state setup)

Hello, it's me, Bob →
← Hi, how are you doing

Communication
(state update)

Bla1, Bla2, Bla3, ..., Bla1372 →
← Oj1, oj2, oj3, ..., oj1973

Communication Interruption (Preserve/Save and Possibly Transfer current state)

Suspend Phase

Communication restored
(re-authentication)

↔ Hi, its me again

Communication Continued
(state update)

Bla1373, Bla1374, Bla1375, ... →
← Oj1974, oj1975, oj1976, ...

State Management

- Question: Which networked object do we mean and what comprises its state?
  - Moving a device with one interface
  - Moving one interface on a device with multiple interfaces
  - Moving an application
  - Moving a content
  - Moving a user between devices

Utilization of Information at All Layers

- Important for various optimizations during a handover
  - A handover is going to be performed to an interface with poorer characteristics. TCP timers can be handled accordingly
  - TCP experiences packet loss right after handover. There is no need to trigger "standard" TCP recovery mechanisms. Retransmissions can be triggered immediately, due to the known reason of packet loss
  - Assume an application has knowledge about available interfaces and decides to move its flow(s) between them. TCP can be instructed about adequate behavior
  - Any other ideas?

Interaction with Applications

- Notifications to applications from the stack can lead to various performance optimizations, for example:
  - If system prepares to perform handover, an application can use it as "stop sending data" instruction in order to reduce number of lost packets during handover
  - If TCP socket is going to be closed due to the time-out, an application can use it as "do not panic, preserve state" instruction
  - Assume there is a system support for re-opening of a socket after time-out, then an application can use it as "restore state and continue the session" instruction.
  - Any other ideas?

Protocol Support

- How to keep consistency after changes have taken place?
  - IP address change
  - Port number change
  - Interface characteristics change
  - Service move (decoupling of service and content)
  - Content move
  - User move

Questions and Discussions

Open Systems and Open Systems Interconnection

Open Systems: OSI Definition

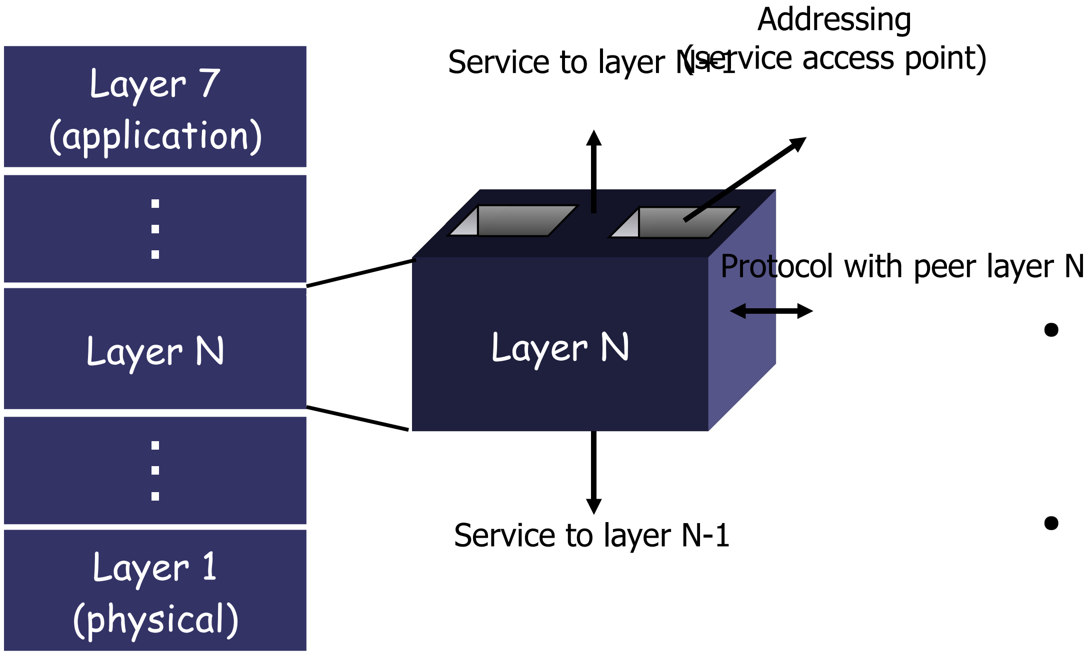
- The term Open Systems Interconnection (OSI) qualifies standards for the exchange of information among systems that are "open" to one another for this purpose by virtue of their mutual use of the applicable standards.***

*** Information Technology Open Systems Interconnection – Basic Reference Model: The Basic Model. iso_iec_7498-1.txt

Open Communication Systems – Design Approach

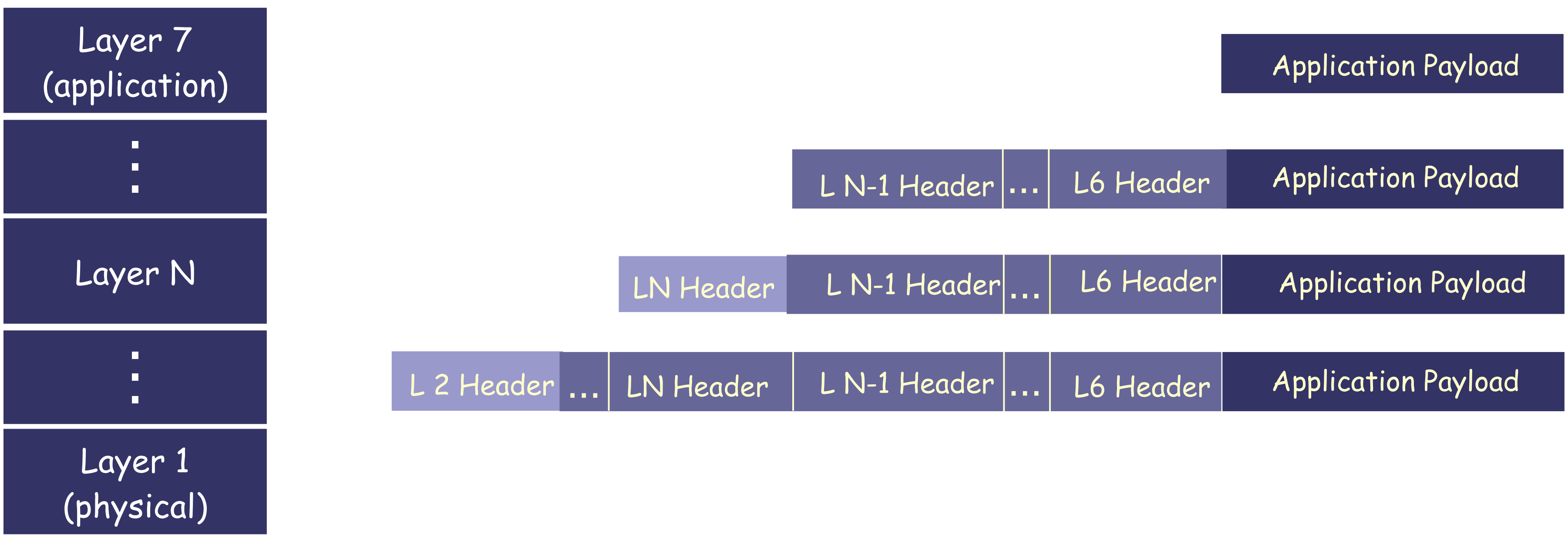
- Layered architecture
- Definition of functions for each layer (service definition)
- Definition of interconnection rules between layers (addressing, multiplexing)
- Definition of protocol(s) for each layer

Open Systems: OSI Layers



- **Naming & Addressing**
  - Scope
  - Semantic
  - Lifetime
  - Independence
  - Bundling policy
- **Service Definition**
  - Functional definition of what services are provided
- **Protocol specification**
  - Format of PDU
  - Semantics of fields
  - Allowable sequence of PDU

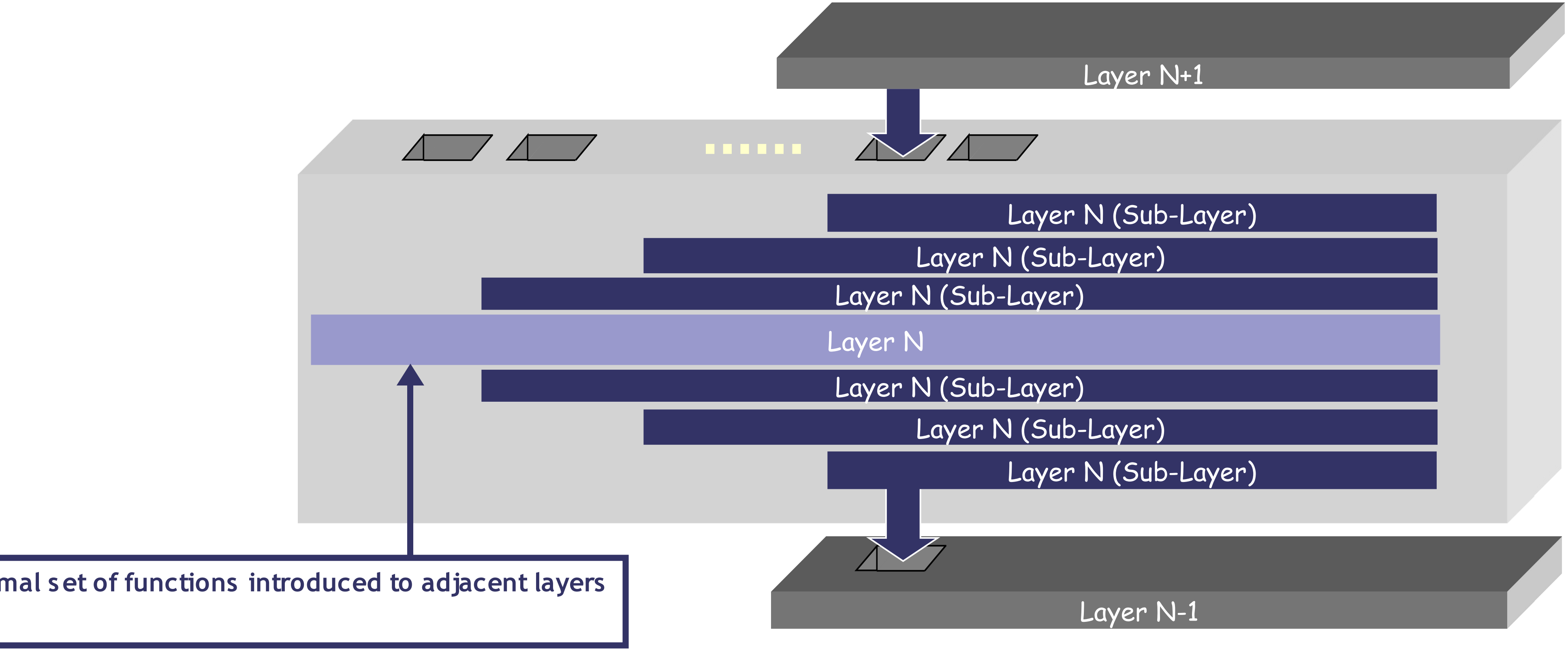
Open Systems: PDU Formation



Open Systems: Sub-layering

Layer service is the service, which can not be bypassed.

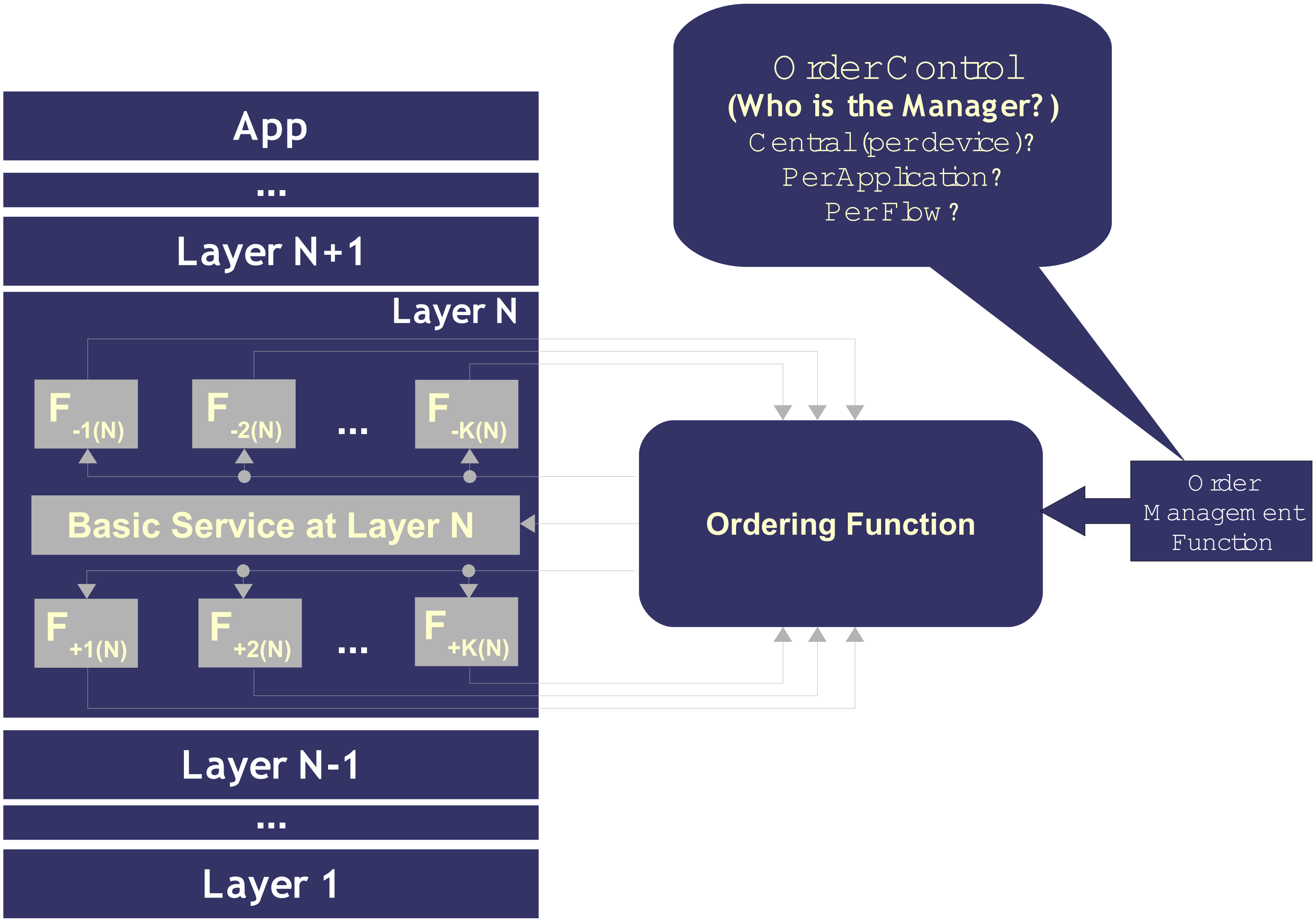
Sub-layer service may be bypassed and may not be mandatory for implementation



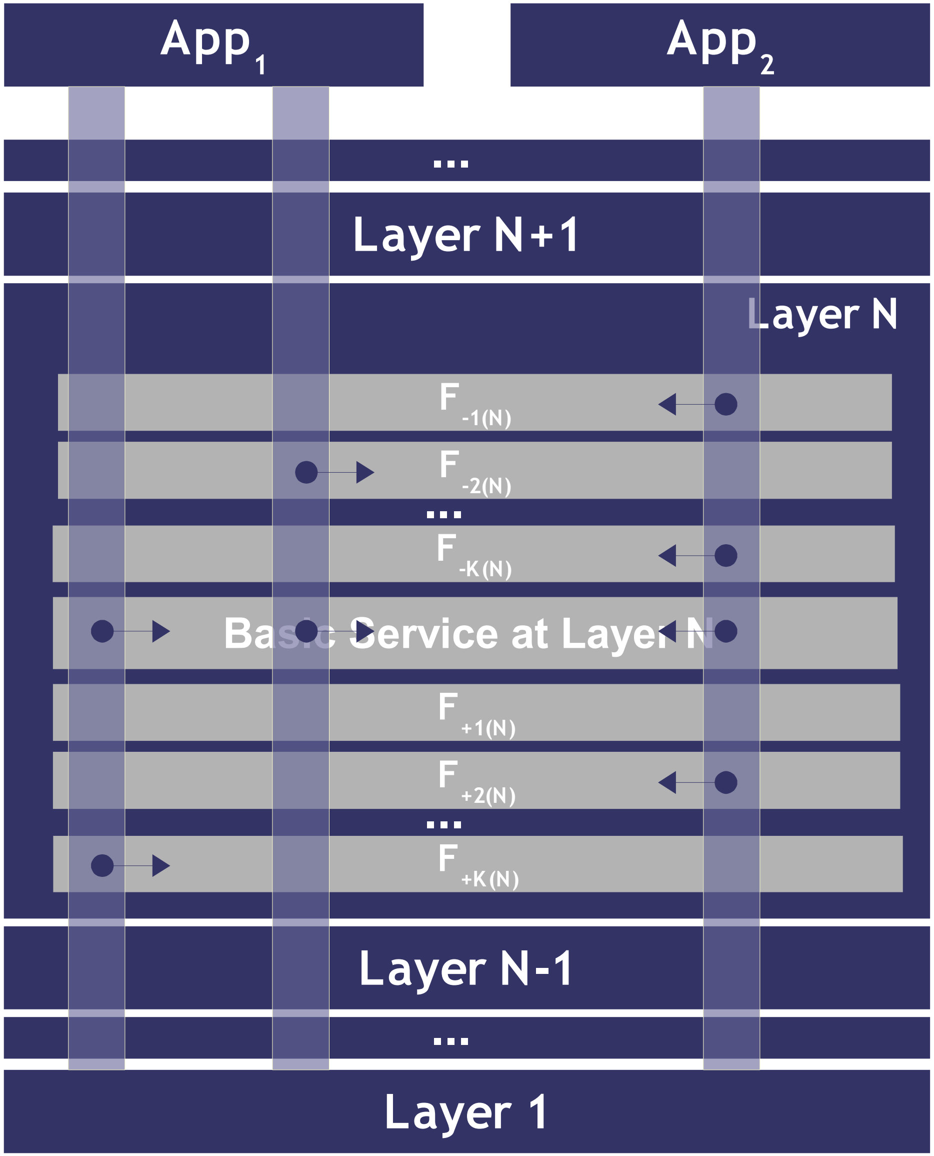
Invocation of a Sublayer Functions

- Questions with regard to introduction of sub-layers
  - What is used to identify flows/packets?
  - How to provide an oder of sub-layers functions execution?
  - How to provide an order of sub-layers functions execution per application/per flow?
  - How to provide a different subset of sub-layers functions per application/per flow?
  - How to change a set of sub-layer functions during run-time, i.e. for active flows?
  - How to apply proper subset of sub-layers functions to incoming packets
  - IP sub-layers: what is the role of traditional routing table?

Invocation of a Sublayer Functions



Invocation of Sublayer Functions



- Each application creates a dedicated ordering function
- An order of sub-layers invocation at each layer is specified at the creation time of dedicated ordering function
- For generic mobility purposes change of sub-layers functions and their order should be supported

TCP/IP Stack: Invocation of Sub-Layers (1)

- XFRM (Transformer) is a network programming framework included in Linux since kernel version 2.5
  - The idea is to be able to modify the path of packets through the networking stack based on some policies. The framework, originally designed to implement IPsec, has later been used for the Mobile IPv6 implementation [1]
  - Later on suggested to use the XFRM framework as a base for SHIM6 implementation [2]

---

[1] "IPv6 IPsec and Mobile IPv6 implementation of Linux". Kazunori MIYAZAWA, Masahide NAKAMURA. Proceedings of the Linux Symposium, Volume Two, July 21th–24th, 2004, Ottawa, Ontario, Canada

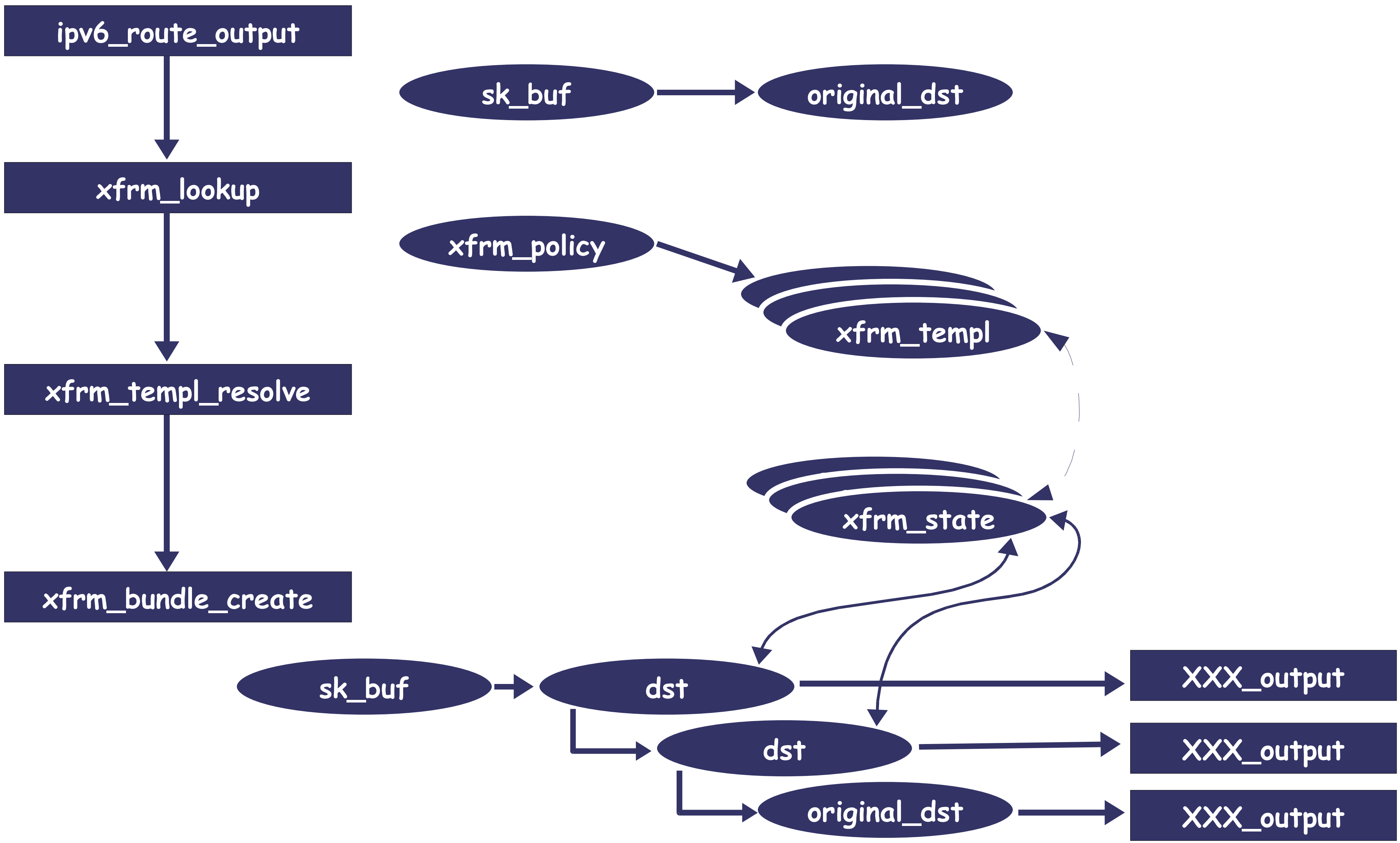
[2] "Implementing SHIM6 Using the Linux XFRM Framework". Sébastien Barré, Olivier Bonaventure. Routing in Next Generation Workshop, Madrid (Spain) - 13-14 December 2007.

TCP/IP Stack: Invocation of Sub-Layers (2)

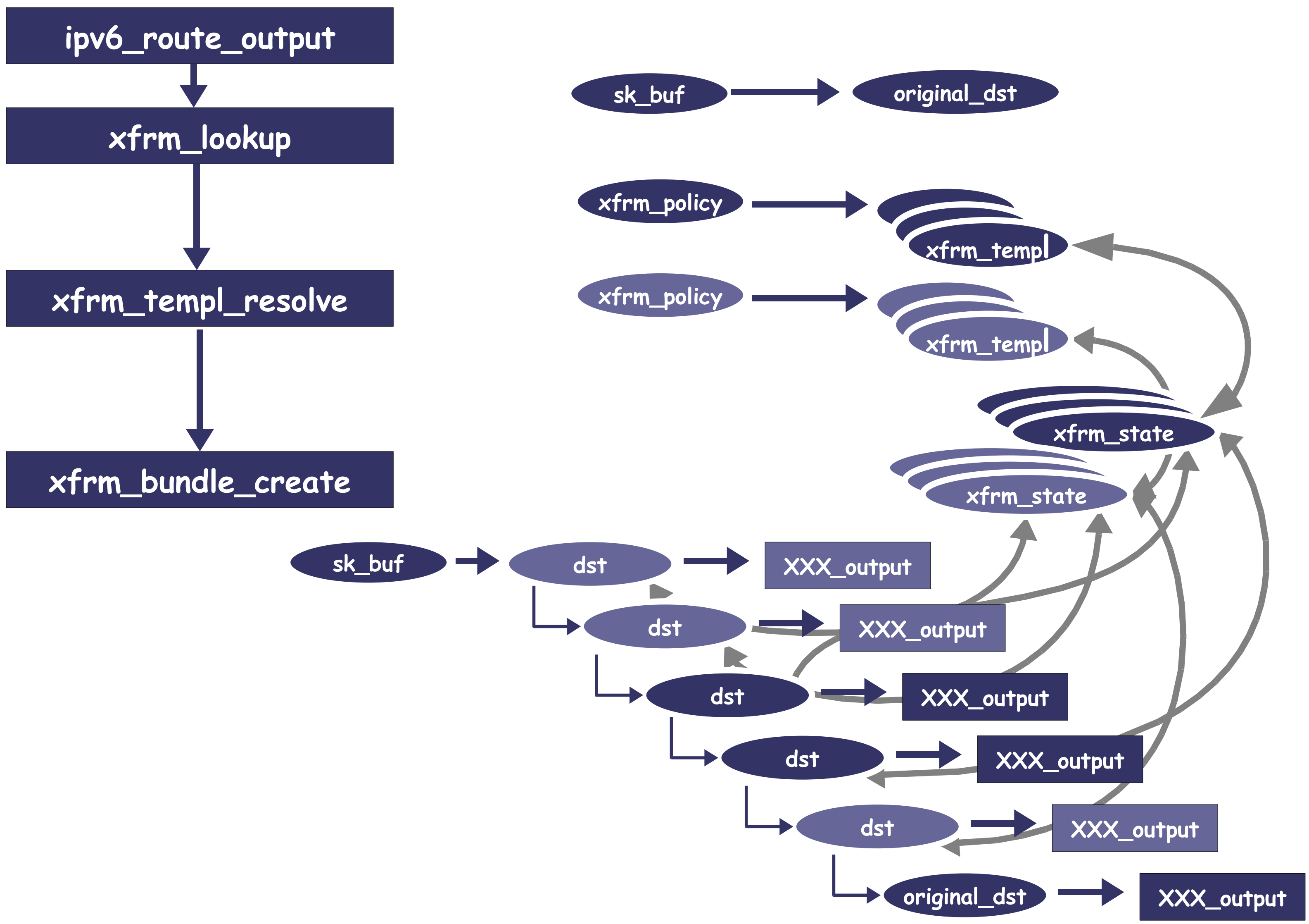
- **XFRM packet processing is based on the policies database** (RFC 4301 allows multiple policies databases)
  - A policy is made of a selector[1], a direction, an action and a template
  - The policy is applied to a packet if it matches the selector and is flowing in the direction of that policy (inbound or outbound)
  - The selector mechanism allows one to use the addresses, ports, address family and protocol number as fields for the matching
  - If a packet matches a given policy. In that case the template is used to get a description of the transformations needed for that kind of packet, and leads to an action to be applied for the packet

[1] "Security Architecture for IP". S. Kent, K. Seo. IETF RFC 4301

TCP/IP Stack: Invocation of Sub-Layers



TCP/IP Stack: Invocation of Sub-Layers (3)

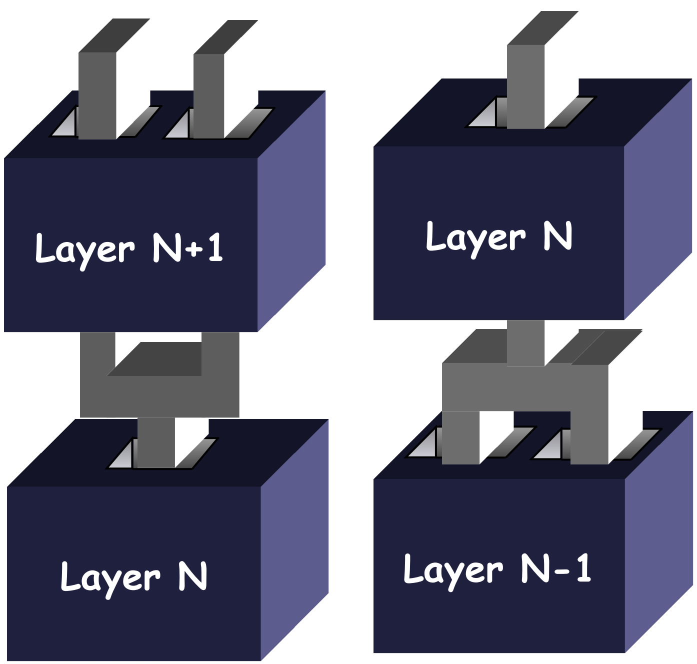


Open Systems: Multiplexing

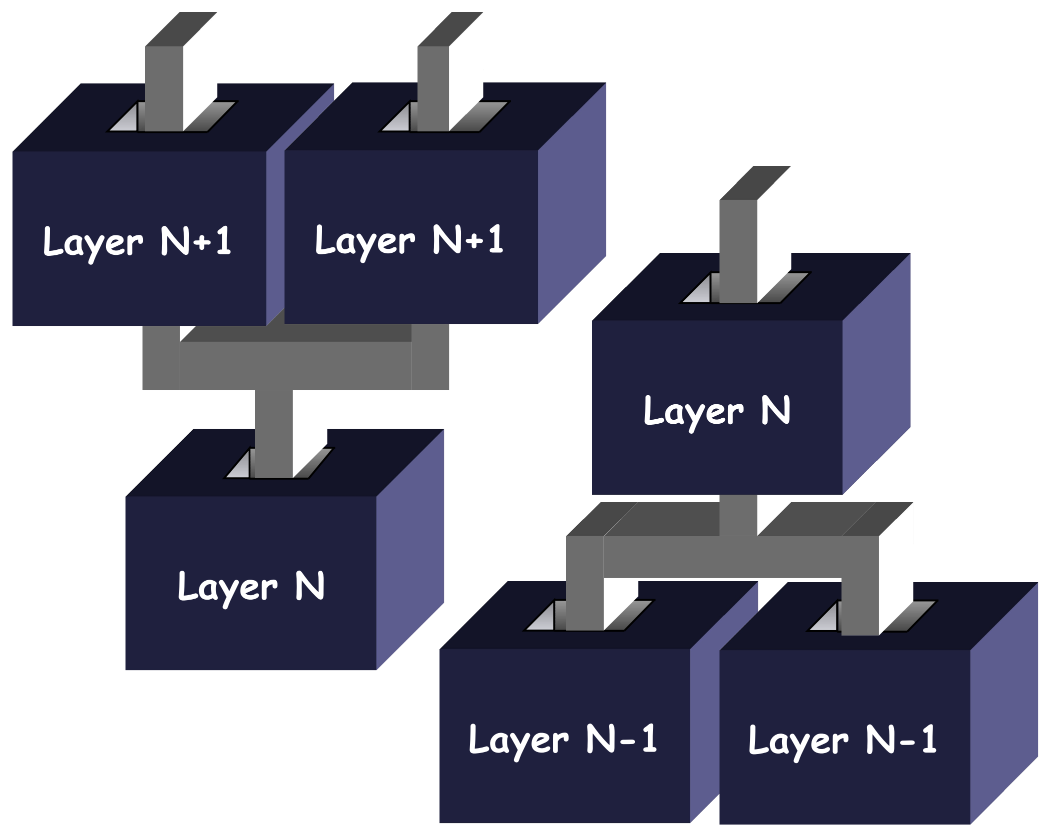
- Multiplexing/De-multiplexing is an important design feature of layered architecture.
- Multiplexing applicable at any layer.
- Upward multiplexing
- Downward multiplexing

Open Systems: Multiplexing

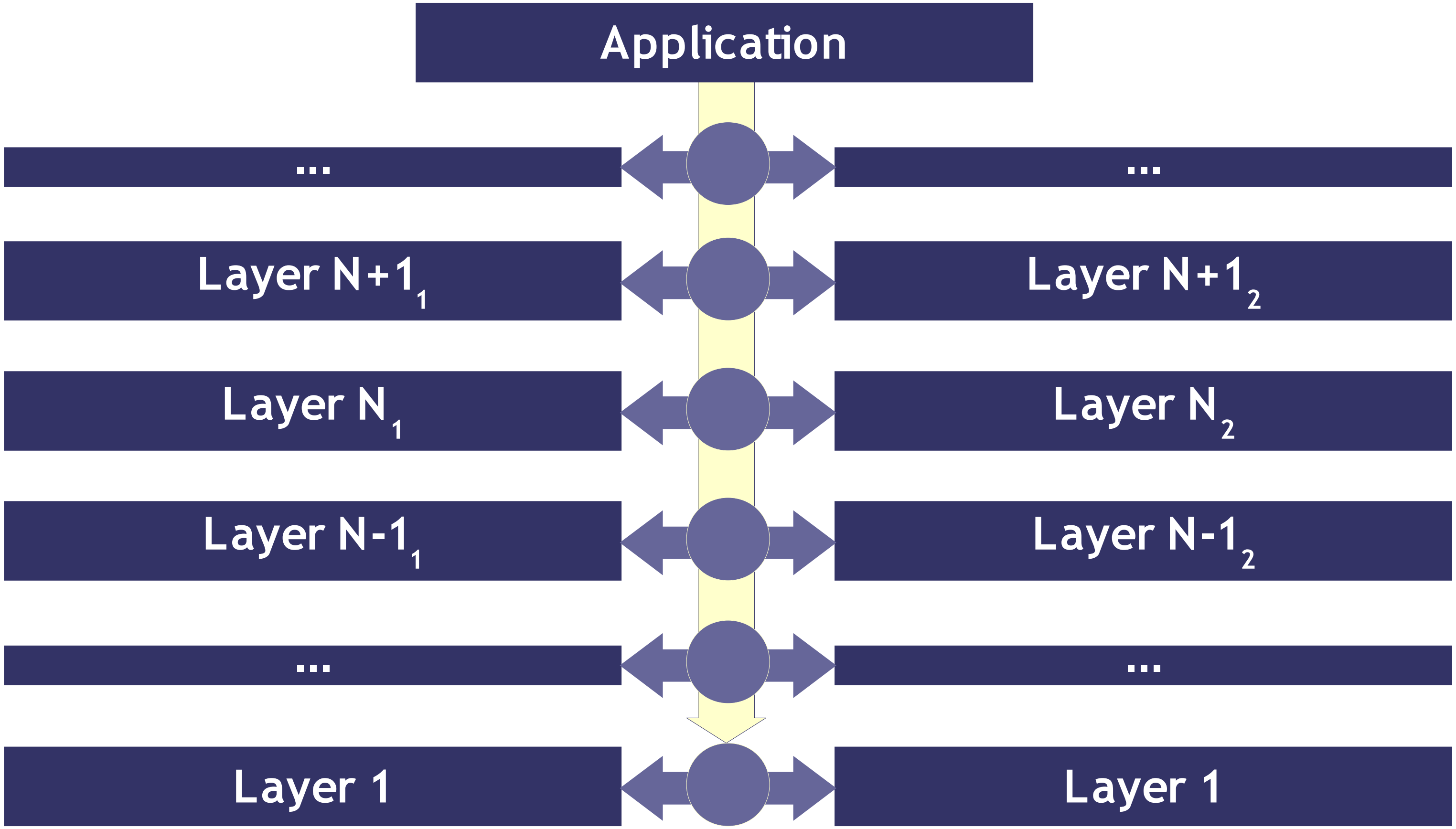
ultiplexing based on SAP diversity at a single layer



Multiplexing based on functional layer diversity



Invocation of Layers at Each Level

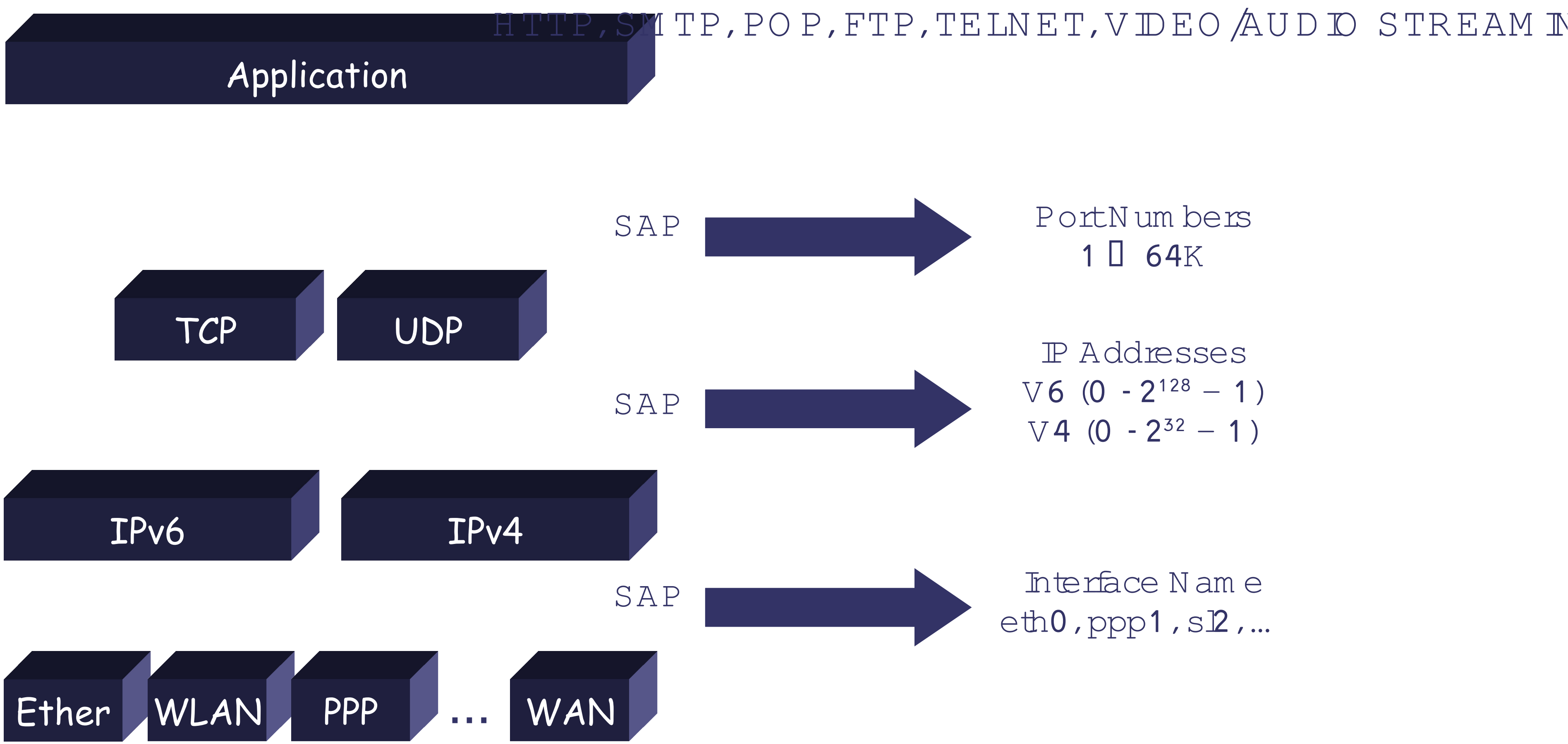


- Questions:
  - What is the mechanism of invoking different layers at each level in the current TCP/IP downwards?
  - What is the mechanism of invoking different layers at each level in the current TCP/IP upwards?

Open Systems: Multiplexing

- Downwards
  - Shared by the set of layers structure filled in by a creator of the whole or partial path.
  - A multiplexing mechanism implemented at a separate layer – need for unambiguous solution.
- Upwards
  - Fields in protocol header describing the upper layer receiver protocol and its SAP name.
  - These fields allow to provide unambiguous mapping of PDU to correspondent shared structure in order to reach appropriate end-point.
  - If multiplexing done based on SAP diversity then only field with SAP name is enough.
  - If multiplexing based on protocol diversity then only next protocol field enough.
  - In the most generic case both fields should be present

TCP/IP Protocol Stack: Mapping onto OSI SAP



TCP/IP Protocol Stack: Mapping onto OSI Multiplexing

Downwards

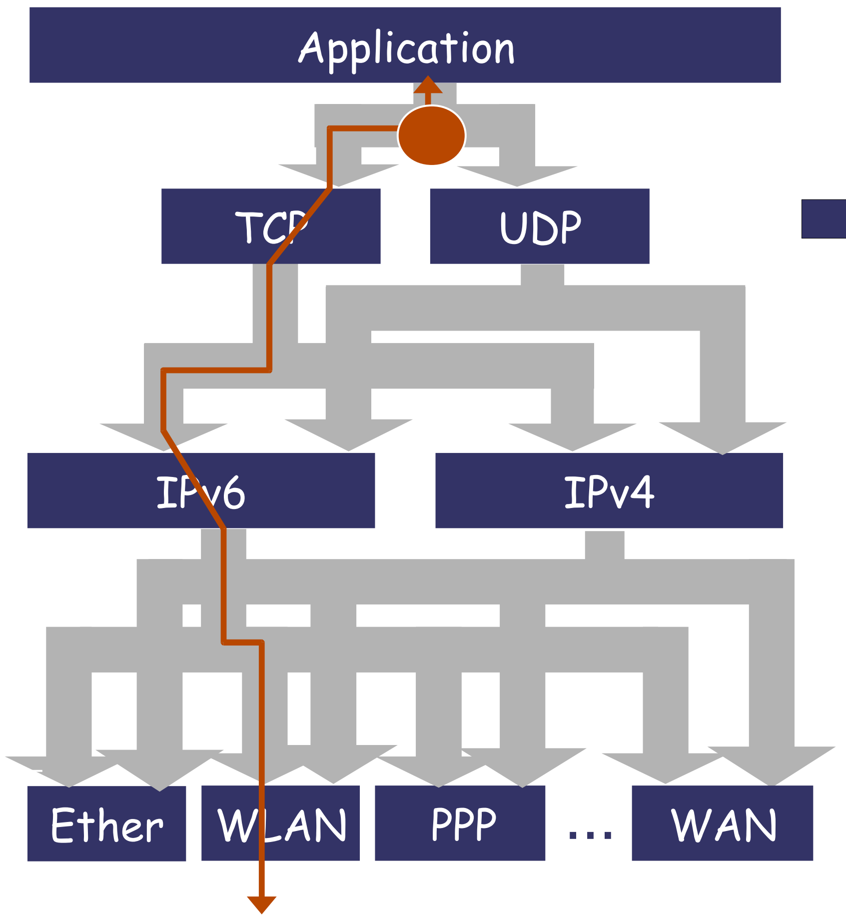
Upwards

Socket Structure

Transport Service
Port Number
Protocol Family

Routing Table

eth0, eth1, ppp2, sl1



Port Number

No Next Protocol???

Next Protocol

Next Protocol

Internet Architecture Highlights

- Fixed infrastructure (topology)
- IP address distribution is done in centralized way and they (IP addresses) belong to infrastructure.
- Name resolution is a centrally managed function
- Topological correctness of IP addresses is the key for correct functioning of IP routing.

References

- William Stallings. "Data and Computer Communications", 5th edition, ISBN 0-13-571274-2. (Chapter 15)
- Douglas E. Comer. "Computer Networks and Internets", ISBN 0-13-239070-1. (Chapters 10, 12)
- ISO Standard. "Information Processing Systems - OSI Reference Model - The Basic Model". http://www.acm.org/sigcomm/standards/iso_stds/OSI_MODEL/ISO_IEC_7498-1.T
- ISO Standard. "Open Systems Interconnection - Basic Reference Model: Naming and Addressing". http://www.acm.org/sigcomm/standards/iso_stds/OSI_MODEL/ISO_IEC_7498-3.T

Questions and Discussions

Mobility Management Solutions (Impact on the TCP/IP stack)

Mobility Management Solutions Space

- Below Transport Layer Solutions
  - Mobile IPv4
  - IPv6 Essentials
  - Mobile IPv6
  - Proxy Mobile IPv6
  - Shim6
  - Mobile IPv6 + MEXT (Mobile EXTensions)

Mobile IPv4

Mobile IPv4 (MIPV4)

- Motivation
  - The node must change its IP address whenever it changes its point of attachment, or
  - host-specific routes must be propagated throughout much of the Internet routing fabric.

- Both of these alternatives are often unacceptable. The first makes it impossible for a node to maintain transport and higher-layer connections when the node changes location. The second has obvious and severe scaling problems

MIPv4: Approach

- Approach (RFC 3344)
  - "A new, scalable, mechanism is required for accommodating node mobility within the Internet. This document defines such a mechanism, which enables nodes to change their point of attachment to the Internet without changing their IP address."

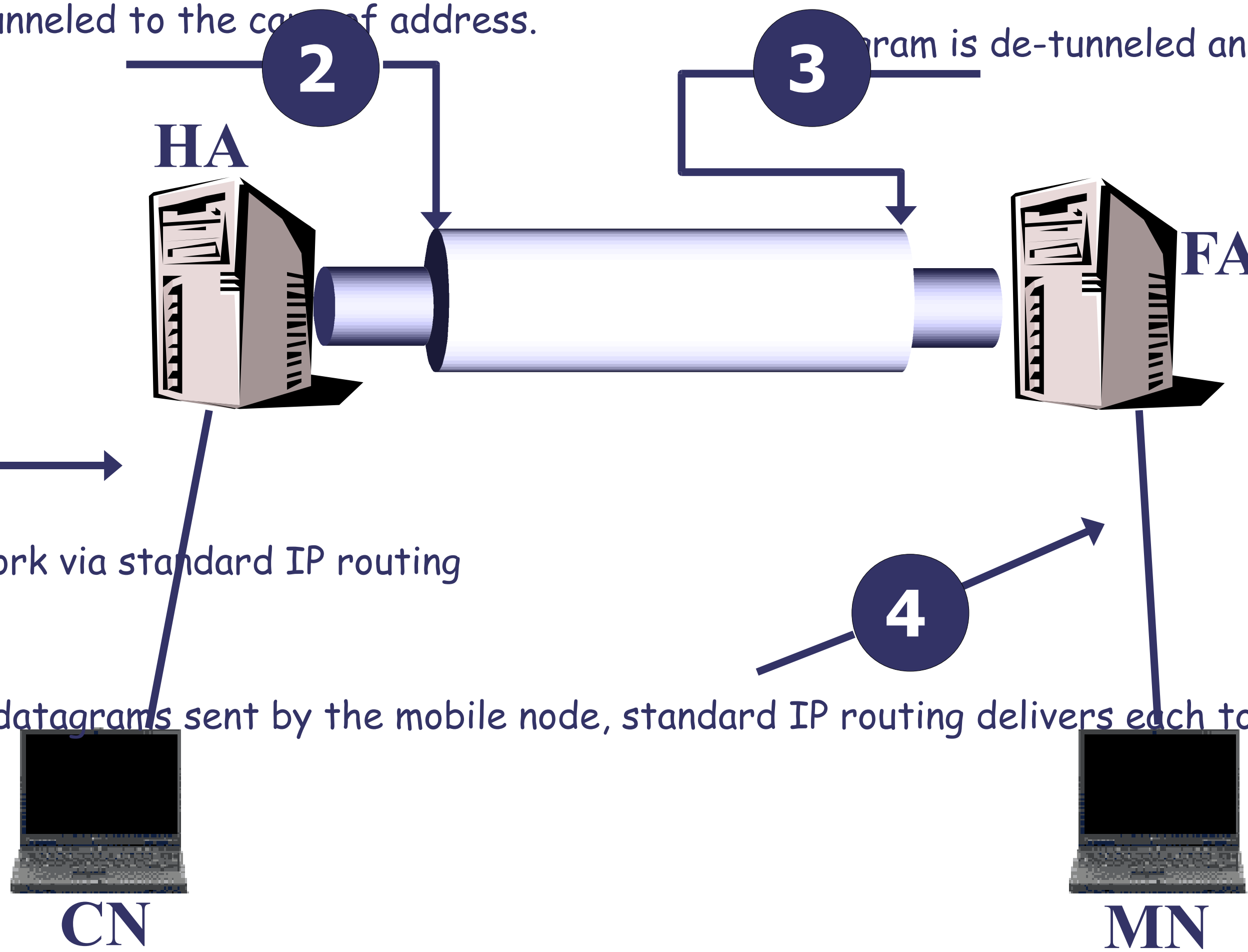
MIPv4: New Architectural Entities

- Mobile Node
  - A host or router that changes its point of attachment from one network or sub-network to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available.
- Home Agent
  - A router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.
- Foreign Agent
  - A router on a mobile node's visited network which provides routing services to the mobile node while registered. The foreign agent de-tunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

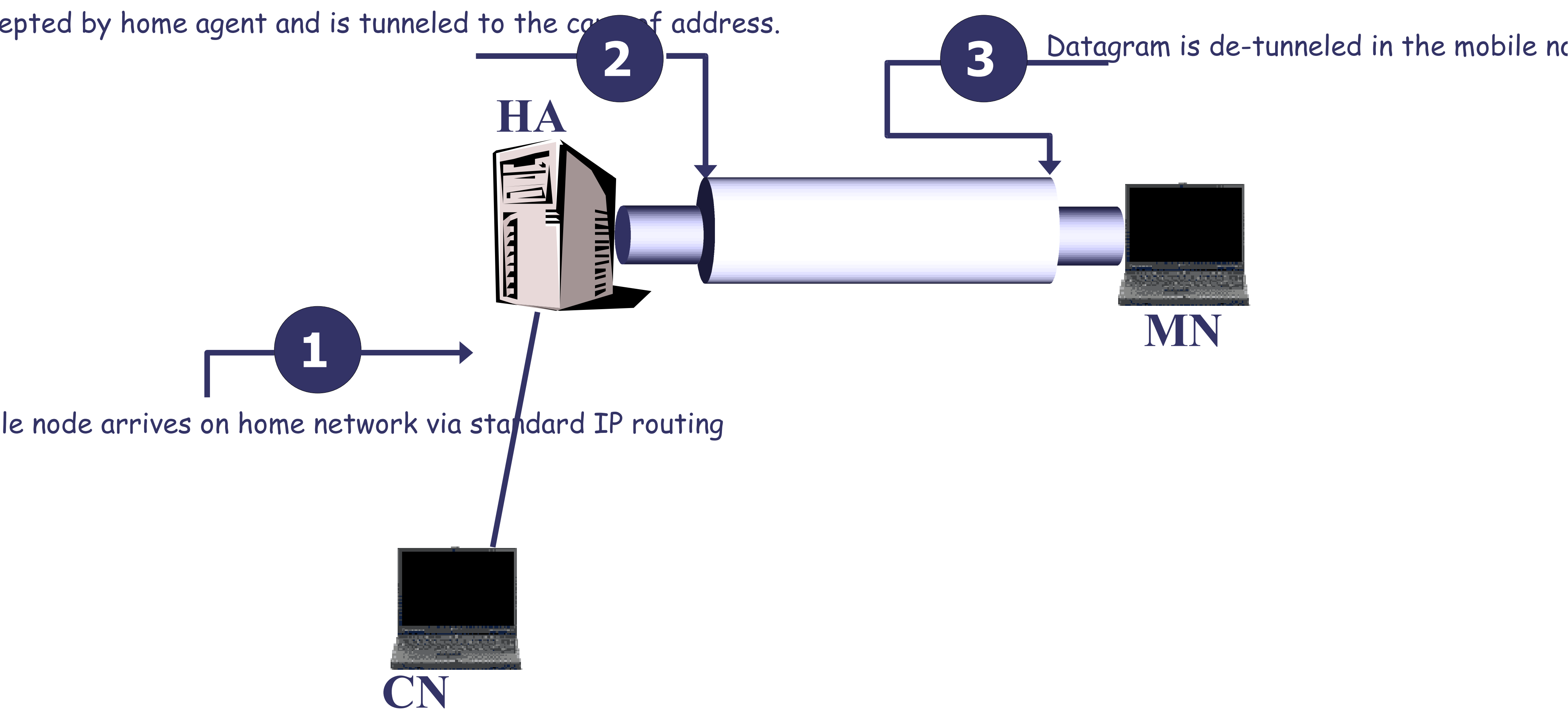
MIPv4: IP Addresses Assigned to a Mobile Node

- Home IP Address
  - Long term assignment.
  - Topologically belongs to the home network.
  - Can be statically mapped to FQDN and resolved through DNS.
- Care-of-Address (CoA)
  - Short term assignment
  - Topologically belongs to the visited network
  - Two types of Care-of-Addresses:
    - Foreign Agent Care-of-Address
    - Collocated Care-of-Address

MIPv4: Operation with Foreign Agent



MIPv4: Operation with Collocated CoA



MIPv4: Operation Procedures

- Agent Discovery
- Agent Advertisement
- Agent Solicitation
- Movement Detection
- Registration
- Tunneling

MIPv4: Registration

- Main features:
  - Request forwarding services when visiting a foreign network.
  - Inform their home agent of their current care-of address.
  - Renew a registration which is due to expire.
  - De-register when they return home.
- Optional features:
  - Discover its home address, if the mobile node is not configured with this information.
  - Maintain multiple simultaneous registrations, so that a copy of each datagram will be tunneled to each active care-of address.
  - De-register specific care-of addresses while retaining other mobility bindings.
  - Discover the address of a home agent if the mobile node is not configured with this information

MIPv4: Layered Model View

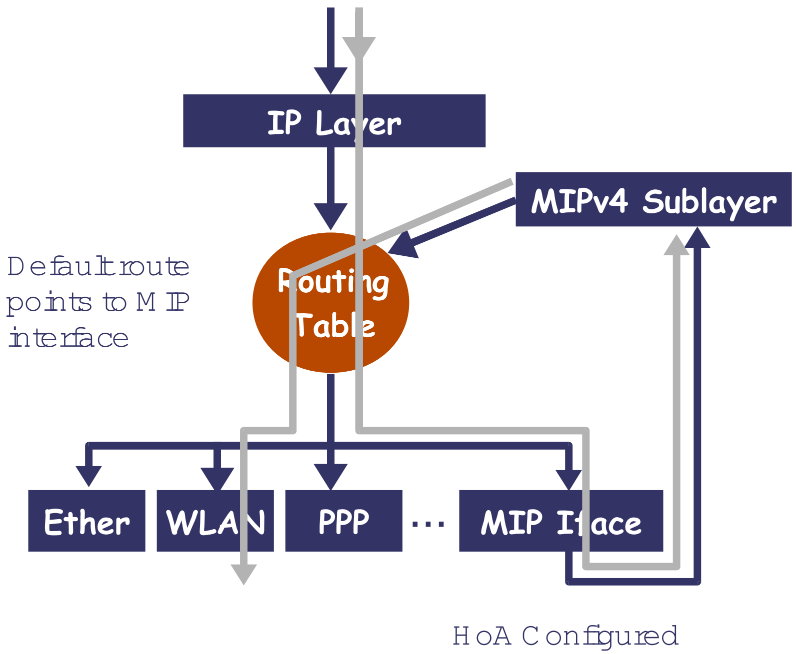
- According to PDU Formation and RFC 2003 “IP Encapsulation within IP” one can conclude that MIPv4 is the layer below IP layer.

PDU Formation:

SAP Names and Multiplexing:

- Use of the same SAP names syntax and semantics as above
- Lifetime of names at MIP4 layer is longer
- Bundling policy of names is different from IP layer

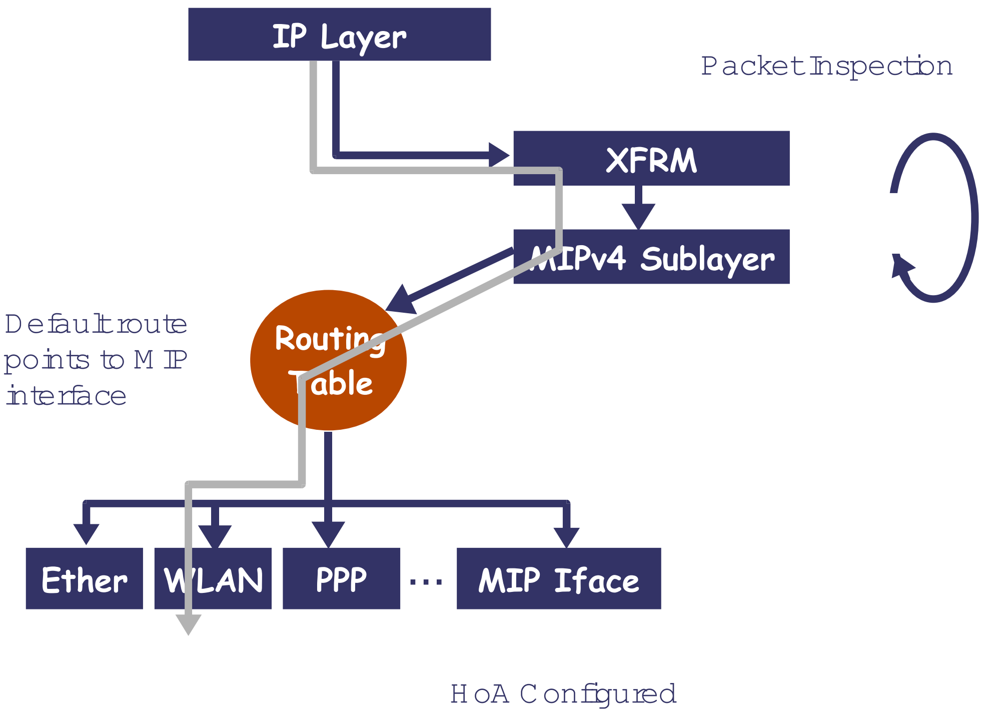
MIPv4: Layered Model View (Initial Design)



- More than one interface of the highest priority implemented through routing table multiplexing capabilities
- MIP adds multi-homing feature by nature
- In a multi-homed device an application may choose another, not MIP interface for sending data
- If multiple similar functions have to be applied, then each sublayer must be aware of its successor

MIPv4: Layered Model View (Currently Possible Design)

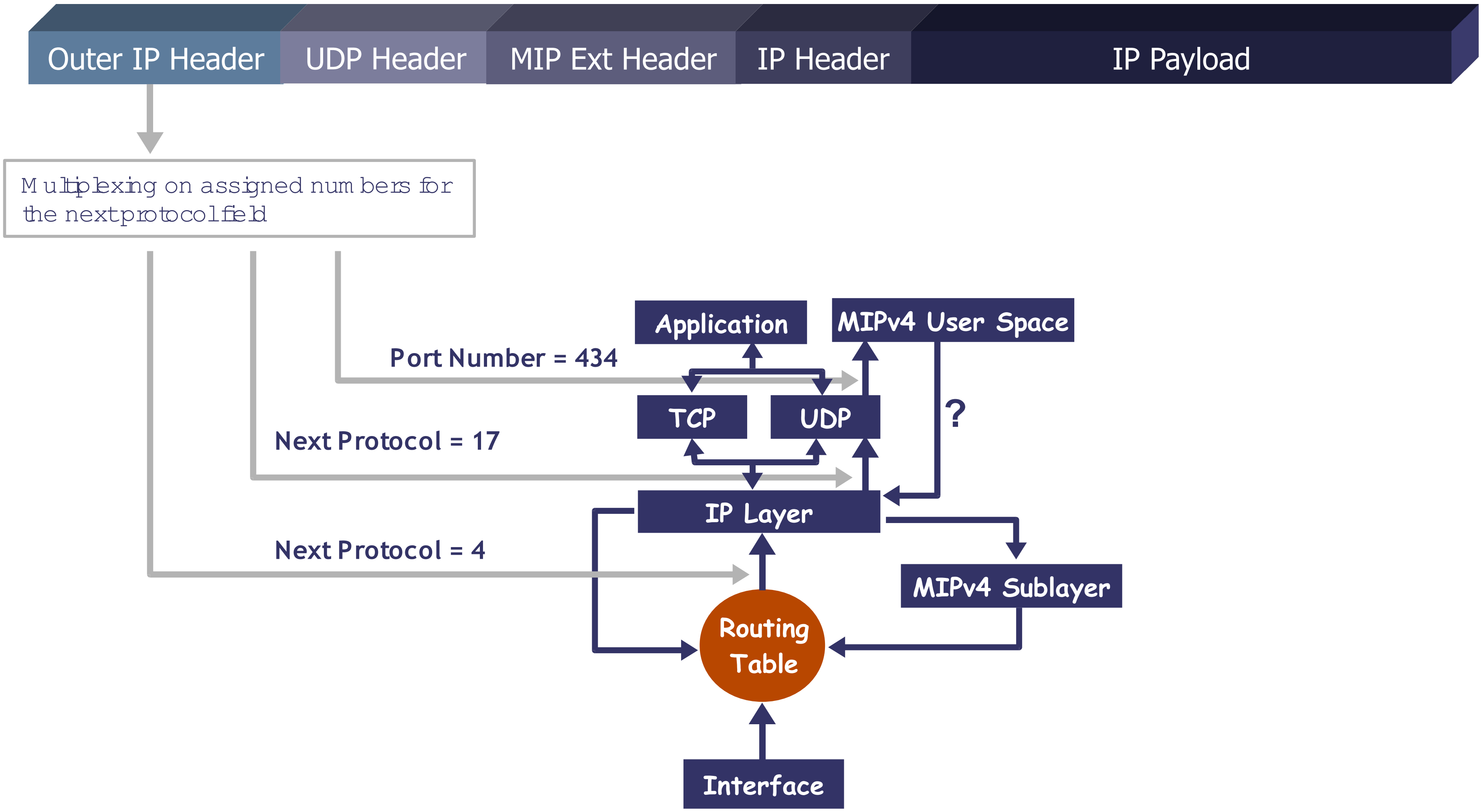
- Much cleaner design
- Tolerates application of multiple functions due to the introduction of policies controlled function ordering
- Routing table has to be queried once, which has cleaner names semantics
- May lead to ambiguity if more than one function requires default applications binding



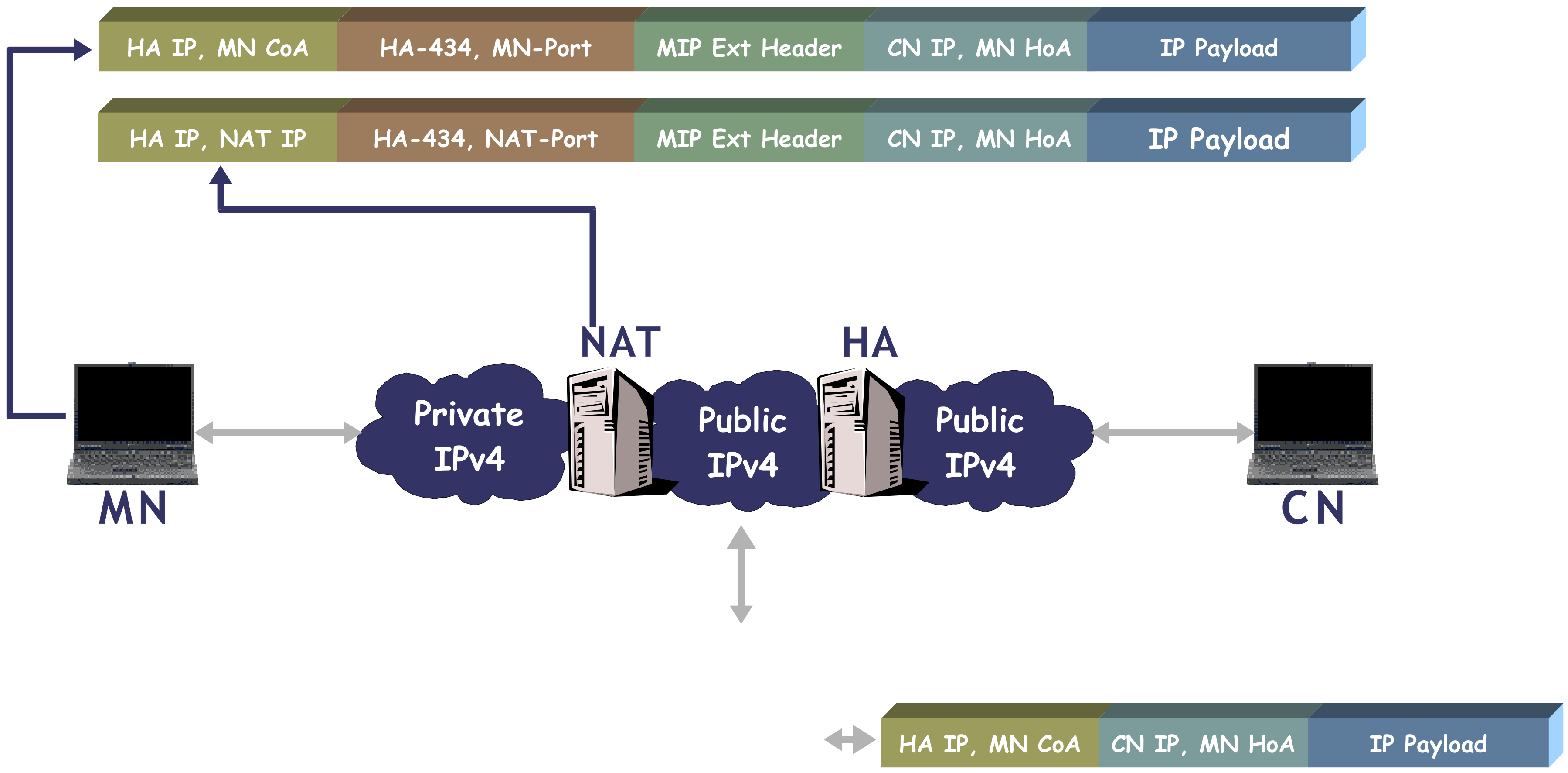
PDU Format:

- NAT allows outgoing traffic, which makes registration possible using IP in UDP encapsulation
- UDP well known port 434
- Reverse tunneling should be used because there is no requirement on CN to implement MIP
- Keep alive interval is set preventing outer NAT UDP port to timeout

MIPv4: NAT Traversal (Stack Projection)

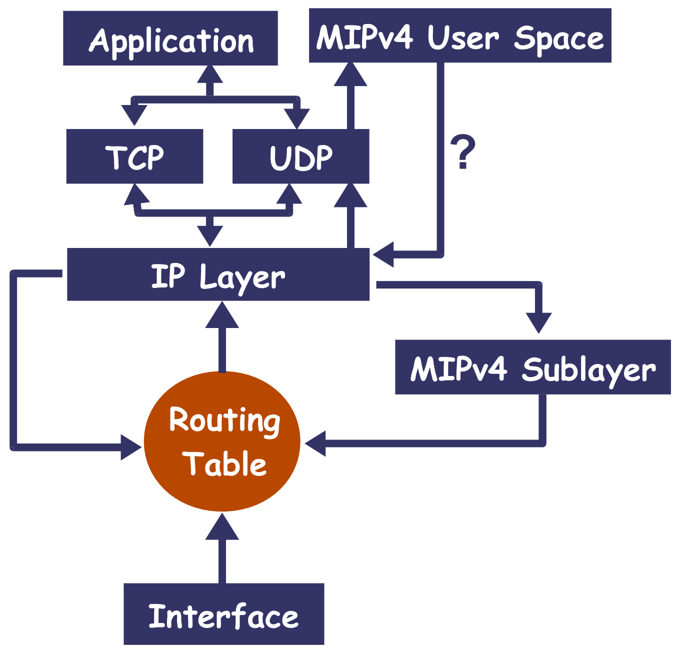


MIPv4: NAT Traversal (Session Continuity)



MIPv4: NAT Traversal (Session Continuity)

- The move from behind a NAT has to be recognized
- Looks like that there will be no impact on inbound traffic



- Outbound traffic processing has to be changed
- Using XFRM framework means changing of policies

MIPv4: References

- C. Perkins, Ed. "IP Mobility Support for IPv4", IETF RFC 3344, August 2002, http://www.ietf.org/rfc/rfc3344.txt
- J. Solomon. "Applicability Statement for IP Mobility Support", IETF RFC 2005, October 1996, http://www.ietf.org/rfc/rfc2005.txt
- G. Montenegro, Editor. "Reverse Tunneling for Mobile IP, revised", IETF RFC 3024, January 2001, http://www.ietf.org/rfc/rfc3024.txt
- H. Levkowetz, S. Vaarala. "Mobile IP Traversal of Network Address Translation (NAT) Devices", IETF RFC 3519, April 2003, http://www.ietf.org/rfc/rfc3519.txt
- P. Calhoun, C. Perkins. "Mobile IP Network Access Identifier Extension for IPv4", IETF RFC 2794, March 2000, http://www.ietf.org/rfc/rfc2794.txt

IPv6 Essentials

IPv6 Essentials

- Expanded Addressing Capabilities
- Header Format Simplification
  - Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header
- Improved Support for Extensions and Options
- Flow Labeling Capability
- Authentication and Privacy Capabilities

IPv6 Essentials: Header Format

<table>
<tr><td>Version</td><td>Traffic Class</td><td colspan="3">Flow Label</td></tr>
<tr><td colspan="3">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
</table>

- 4-bit Internet protocol version number = 6
- 8-bit traffic class field
- 20-bit flow label
- Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets.
- 8-bit selector. Identifies the type of header immediately following the IPv6 header
- Decremented by 1 by each node that forwards the packet

IPv6 Essentials

- Expanded Addressing Capabilities
- Header Format Simplification
- Improved Support for Extensions and Options
- Flow Labeling Capability
- Authentication and Privacy Capabilities

IPv6 Essentials: Extensions and Options

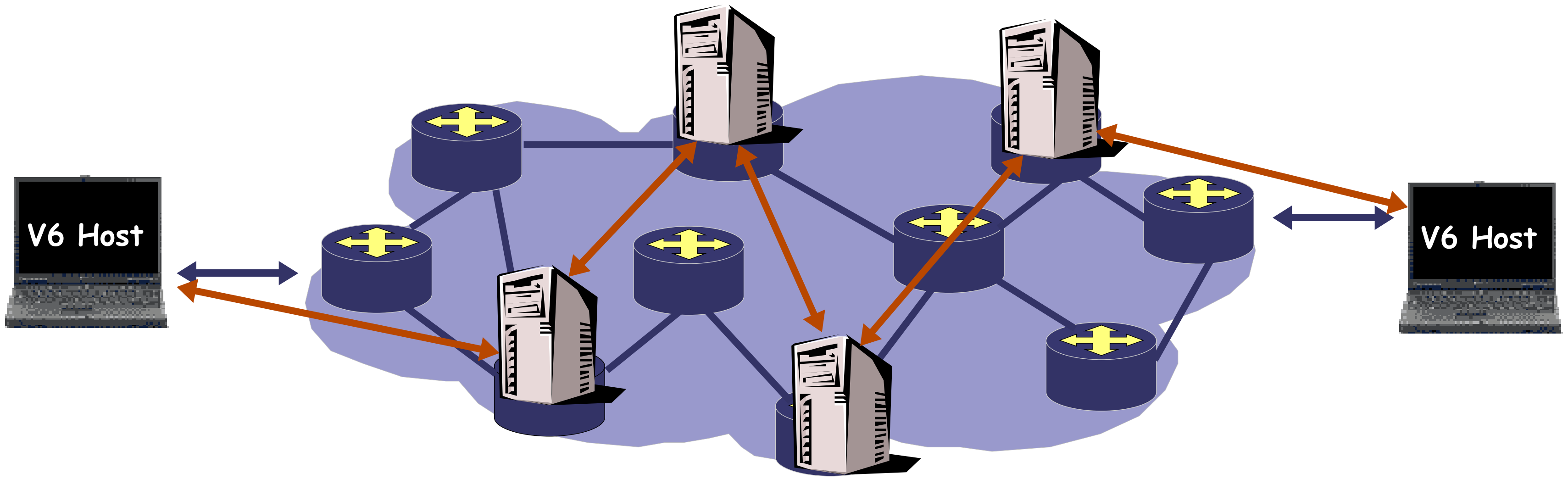
- A full implementation of IPv6 includes implementation of the following extension headers:
  - Hop-by-Hop Options
  - Destination Options
  - Routing
  - Fragment
  - Authentication (not defined by RFC 2460)
  - Encapsulating Security Payload (not defined by RFC 2460)
- Important! Each extension header should occur at most once

IPv6 Essentials: Routing Extension Header

Next Header	Header Ext Len	Routing Type=0	Segments Left
Reserved			
Address[1]			
Address[2]			
...			
Address[n]			

- Next Header identifies the type of header immediately following the Routing header
- Header Ext Len is the length of the routing header in 8-octet units not including the first 8 octets
- Segments Left is the number of explicitly listed intermediate nodes still to be visited before reaching the final destination

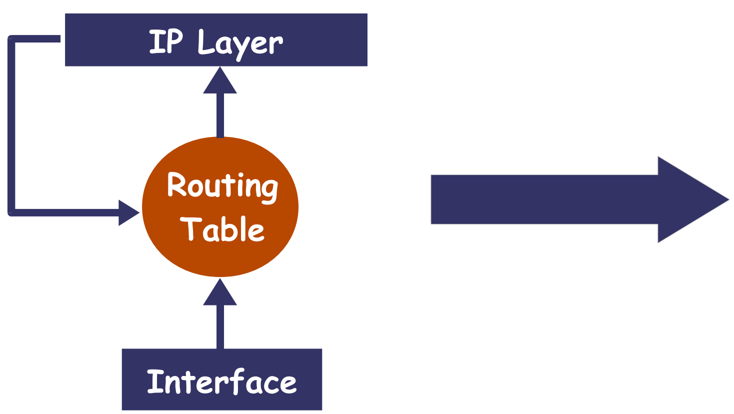
IPv6: Routing Extension Header



IPv6: Routing Header Stack View

Next Header	Header Ext Len	Routing Type=0	Segments Left
Reserved			
Address[1]			
Address[2]			
...			
Address[n]			

Assume that in the place of addresses we will specify the same address and it will be a destination address, then the packet will traverse the stack in the following way



Does this remind something?

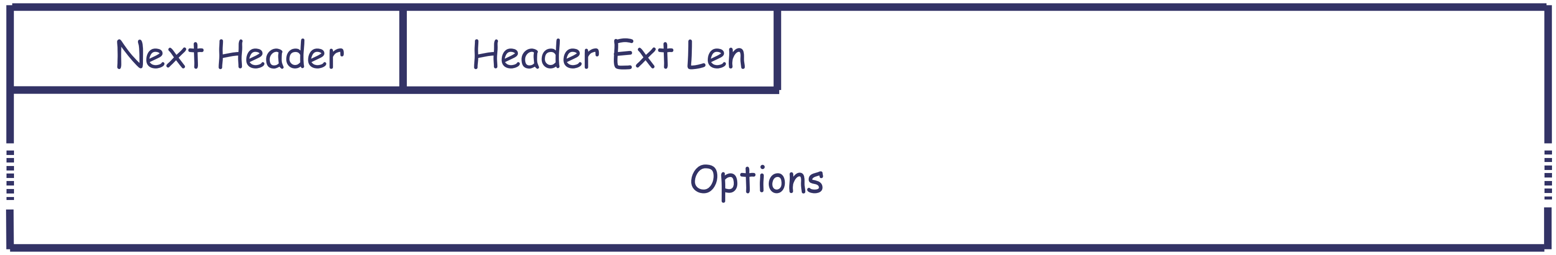
IPv6: Routing Header Deprecation

- The severity of this threat is considered to be sufficient to warrant deprecation of RH0 entirely. A side effect is that this also eliminates benign RH0 use-cases; however, such applications may be facilitated by future Routing Header specifications.
- An IPv6 node that receives a packet with a destination address assigned to it and that contains an RH0 extension header MUST NOT execute the algorithm specified in the latter part of Section 4.4 of [RFC2460] for RH0.
- Instead, such packets MUST be processed according to the behavior specified in Section 4.4 of [RFC2460] for a datagram that includes an unrecognized Routing Type value

RFC 5095 "Deprecation of Type 0 Routing Headers in IPv6"

IPv6: Destination Options

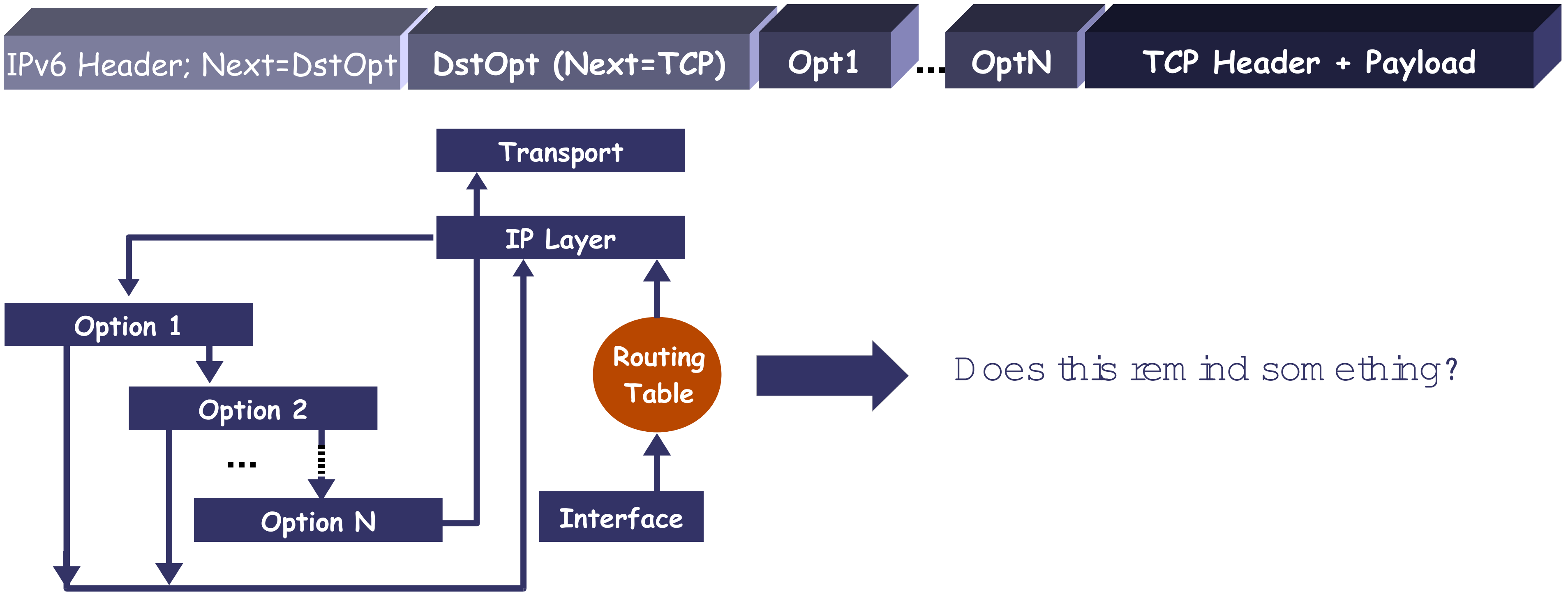
Destination Options Header Format



Type-Length-Value (TLV) Options Format

- The sequence of options within a header must be processed strictly in the order they appear in the header; a receiver must not, for example, scan through the header looking for a particular kind of option and process that option prior to processing all preceding ones.
- Each extension header should occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header).

IPv6: Destination Options Header Stack View



Does this remind something?

- Question:
  - Is that possible to use Destination Options protocol field and to provide support for mobility?
  - If no, why?

IPv6: References

- S. Deering, R. Hinden. "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 2460, December 1998
- J. Abley, P. Savola, G. Neville-Neil. "Deprecation of Type 0 Routing Headers in IPv6", IETF RFC 5095, December 2007
- R. Draves. "Default Address Selection for Internet Protocol version 6 (Ipv6)". IETF RFC 3484, February 2003

Mobile IPv6

Mobile IP Version 6 (MIPv6)

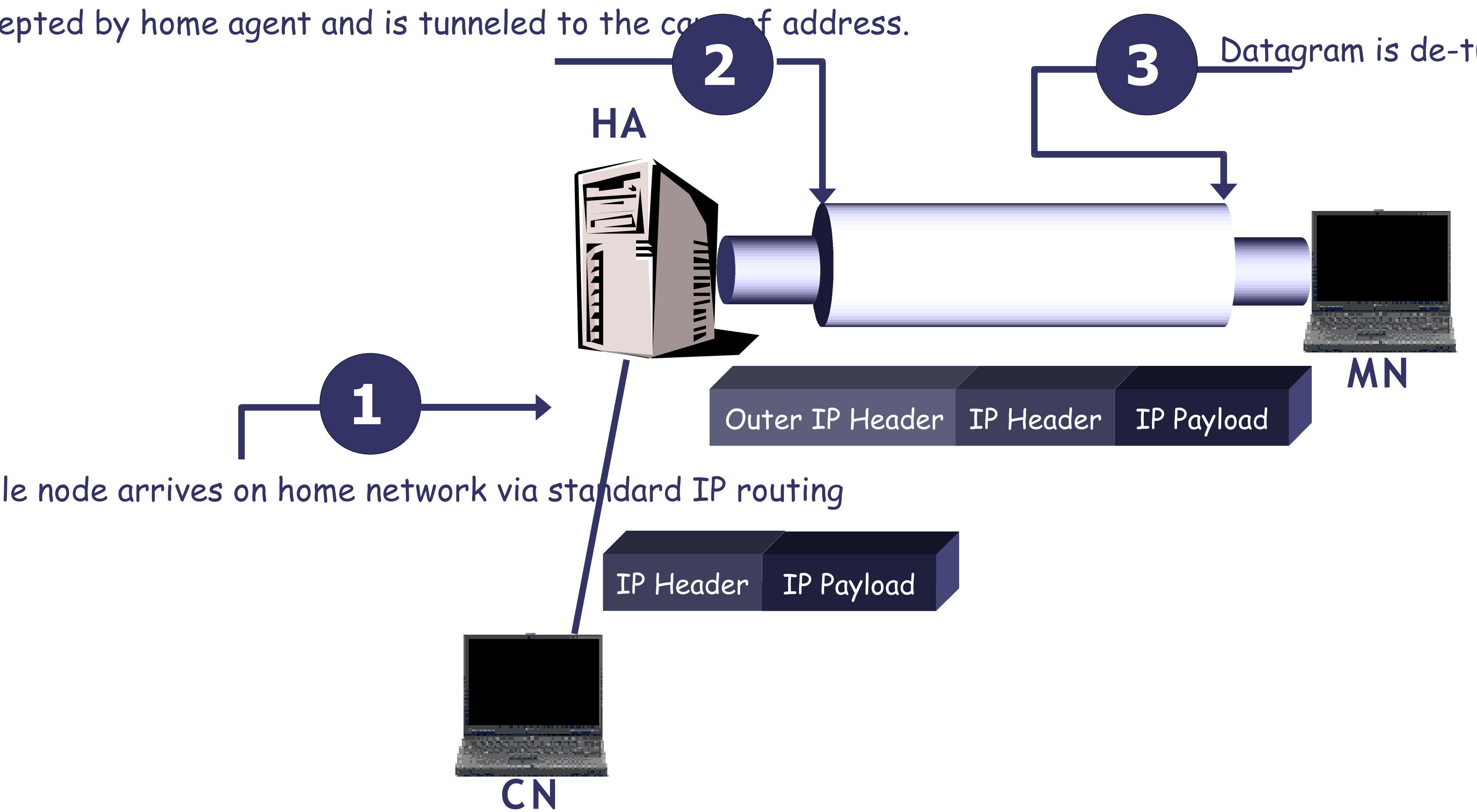
- Motivation is the same as for MIPv4

MIPv6: Differences to MIPv4

- There is no need to deploy special routers as "foreign agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.
- Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions.
- Mobile IPv6 route optimization can operate securely even without pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.
- Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering"
- The IPv6 Neighbor Unreachability Detection assures symmetric reachability between the mobile node and its default router in the current location.
- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.
- Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery [12] instead of ARP. This also improves the robustness of the protocol.
- The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".
- The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

MIPv6: Bidirectional Tunneling Mode

- Bidirectional tunneling does not require Mobile IPv6 support from the correspondent node and is available even if the mobile node has not registered its current binding with the correspondent node.



MIPv6: Route Optimization Mode

- "Route Optimization" mode requires the mobile node to register its current binding at the correspondent node. Packets from the correspondent node can be routed directly to the care-of address of the mobile node. When sending a packet to any Ipv6 destination, the correspondent node checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the mobile node by way of the care-of address indicated in this binding

MIPv6: Route Optimization Mode

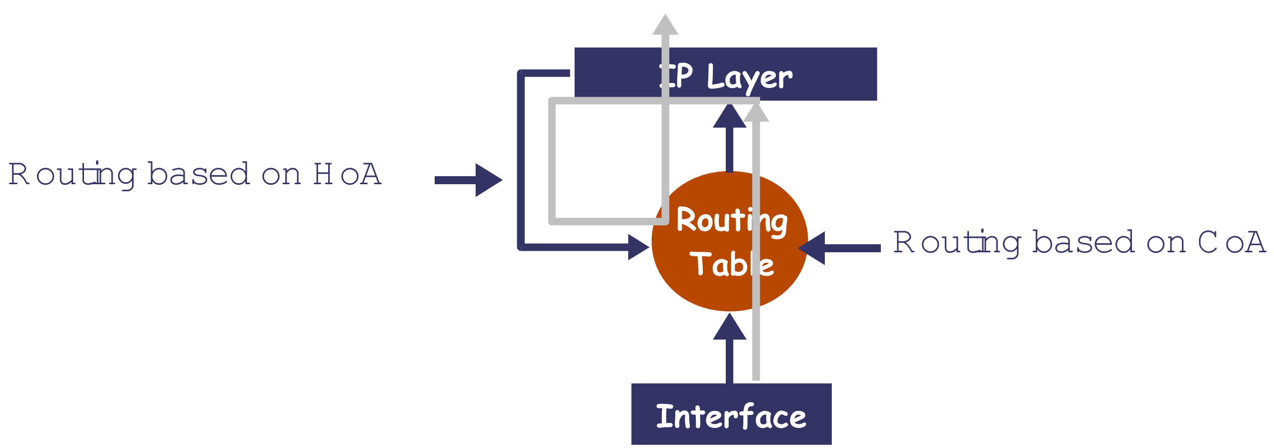
- New Type of Routing Header
- New IPv6 "Home Address" destination option to carry its home address. The inclusion of home addresses in these packets makes the use of the care-of address transparent above the network layer
- Mobile IPv6 defines a new IPv6 protocol, using the Mobility Header. This Header is used to carry the following messages:
  - Home Test Init
  - Home Test
  - Care-of Test Init
  - Care-of Test
    - These four messages are used to perform the return routability procedure from the mobile node to a correspondent node. This ensures authorization of subsequent Binding Updates

MIPv6: Routing Header (Type 2)

Routing Header (Type 2) Format

Next Header	Header Len	MH Type	Segments Left
Reserved			
Home Address			

- Once the packet arrives at the care-of address, the mobile node retrieves its home address from the routing header, and this is used as the final destination address for the packet



MIPv6: HoA Destination Option

- It is used in a packet sent by a mobile node while away from home, to inform the recipient of the mobile node's home address
- Standard TLV format within the destination options header
- For each IPv6 packet header, the Home Address Option MUST NOT appear more than once
- The Home Address option MUST be placed as follows:
  - After the routing header, if that header is present
  - Before the Fragment Header, if that header is present

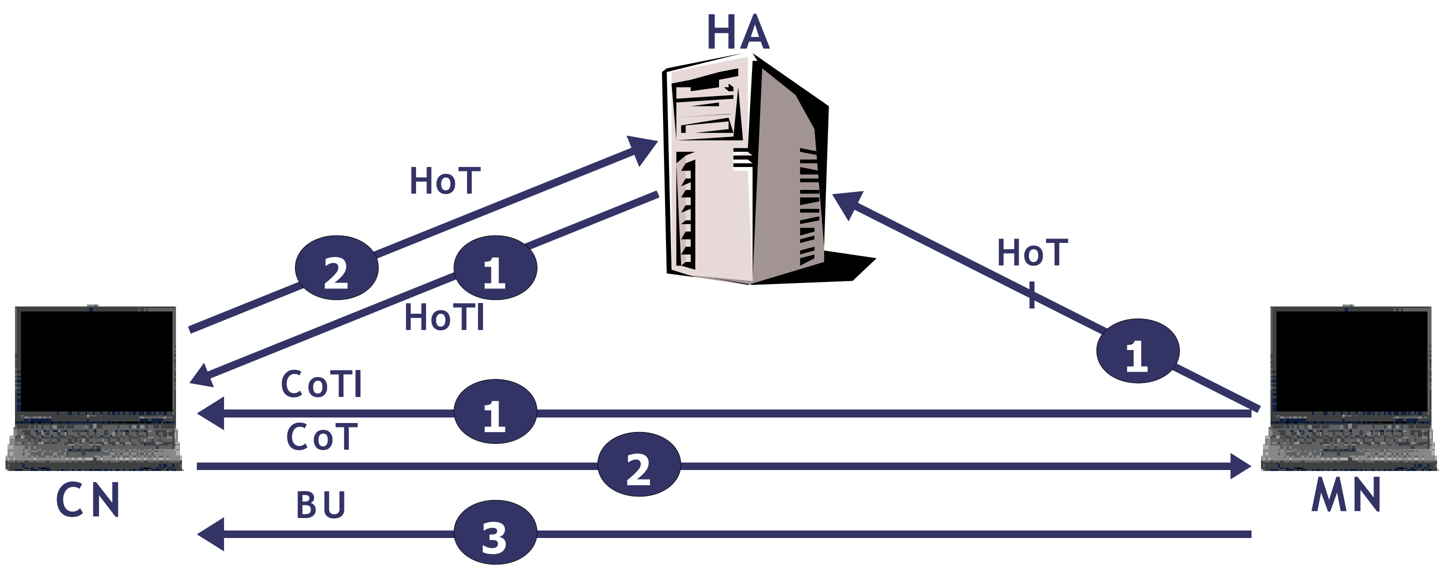
HoA Destination Option Format

Option Type	Option Len	Home Address

MIPv6 Mobility Header

Mobility Header Format

Next Header (Payload Protocol)	Header Len	MH Type	Reserved
Checksum			
Message Data			



MIPv6: Why Secure BU in RO Mode

- The BU orders the receiver to send traffic to a different IP address (e.g. packets intended for address X should be sent to Y)
- Attackers can:
  - Direct a MN's traffic to themselves (steal traffic)
  - Direct a MN's traffic somewhere else (Bombing attacks)
  - Deny a MN from communicating with other nodes (DoS attacks).
  - More attacks are possible.

MIPv6: Control and Data Messages

- Signaling messages for Return Routability Procedure, Binding Updates, etc.

- Data Messages from Mobile

- Data Messages to Mobile

MIPv6: References

- D. Johnson, C. Perkins, J. Arkko "Mobility Support in Ipv6". IETF RFC 3775, June 2004
- A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)". IETF RFC 4283, November 2005

Proxy MIPv6 (PMIPv6)

Client vs. Network Initiated Handover

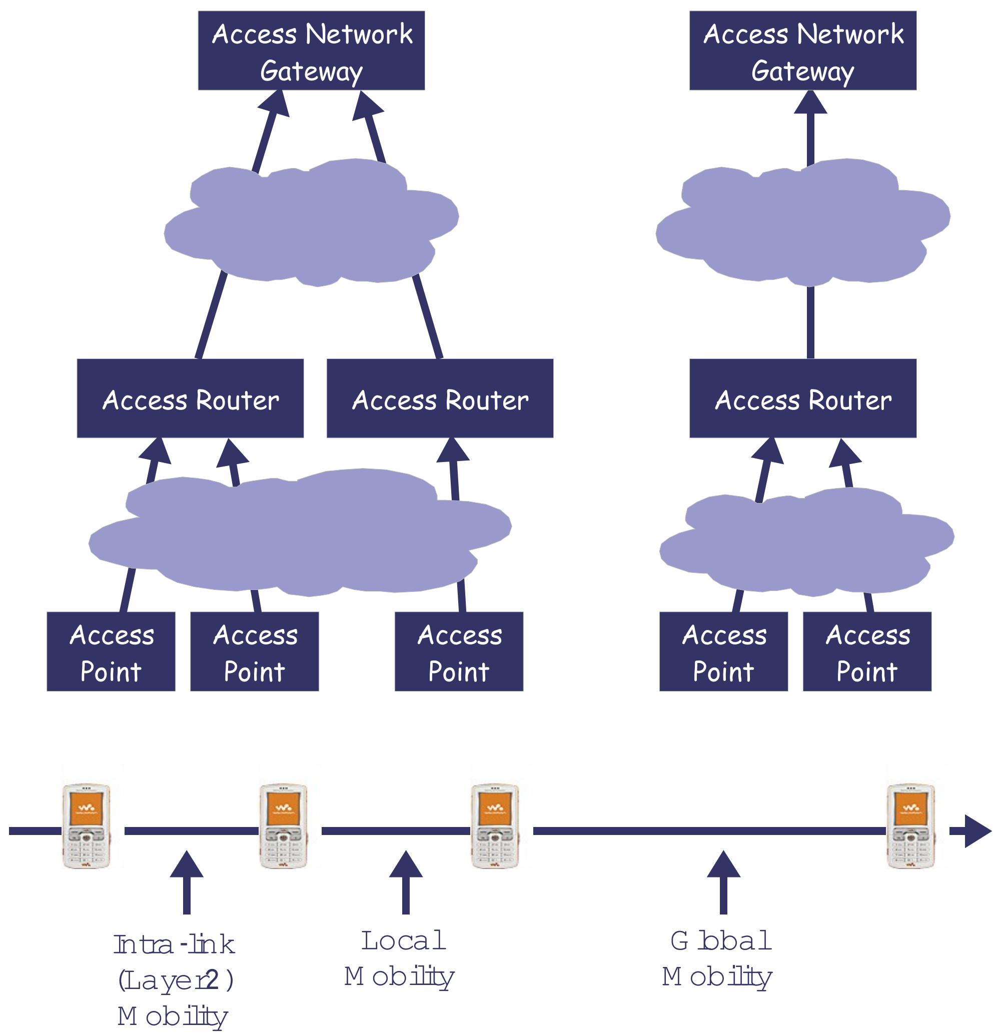
- MIPv6 and MIPv4 are typical examples of client initiated handover
  - A client has to detect movement
  - A client starts procedure to ensure delivery of subsequent packets to a new Care-of-Address
  - This is also called Break-Before-Make (BBM)
- Example of network Initiated handover is traditional Telecom network
  - A client reports signal strength and visible RBS up to the network
  - The network through Radio Resource Management support using sophisticated algorithms decides which RBS the client has to be connected to
  - The network sends commands to the client to perform handover
  - This is also called Make-Before-Break (MBB)

MIPv4 & MIPv6 can perform MBB as well if a client is capable of maintaining simultaneous connectivity to both networks

Global vs Local Mobility Support

- Local Mobility
  - Local Mobility is mobility over an access network. Note that although the area of network topology over which the mobile node moves may be restricted, the actual geographic area could be quite large, depending on the mapping between the network topology and the wireless coverage area
- Localized Mobility Management
  - Localized Mobility Management is a generic term for any protocol that maintains the IP connectivity and reachability of a mobile node for purposes of maintaining session continuity when the mobile node moves, and whose signaling is confined to an access network

Global vs Local Mobility Support: Scope



Local Mobility: Problem Statement

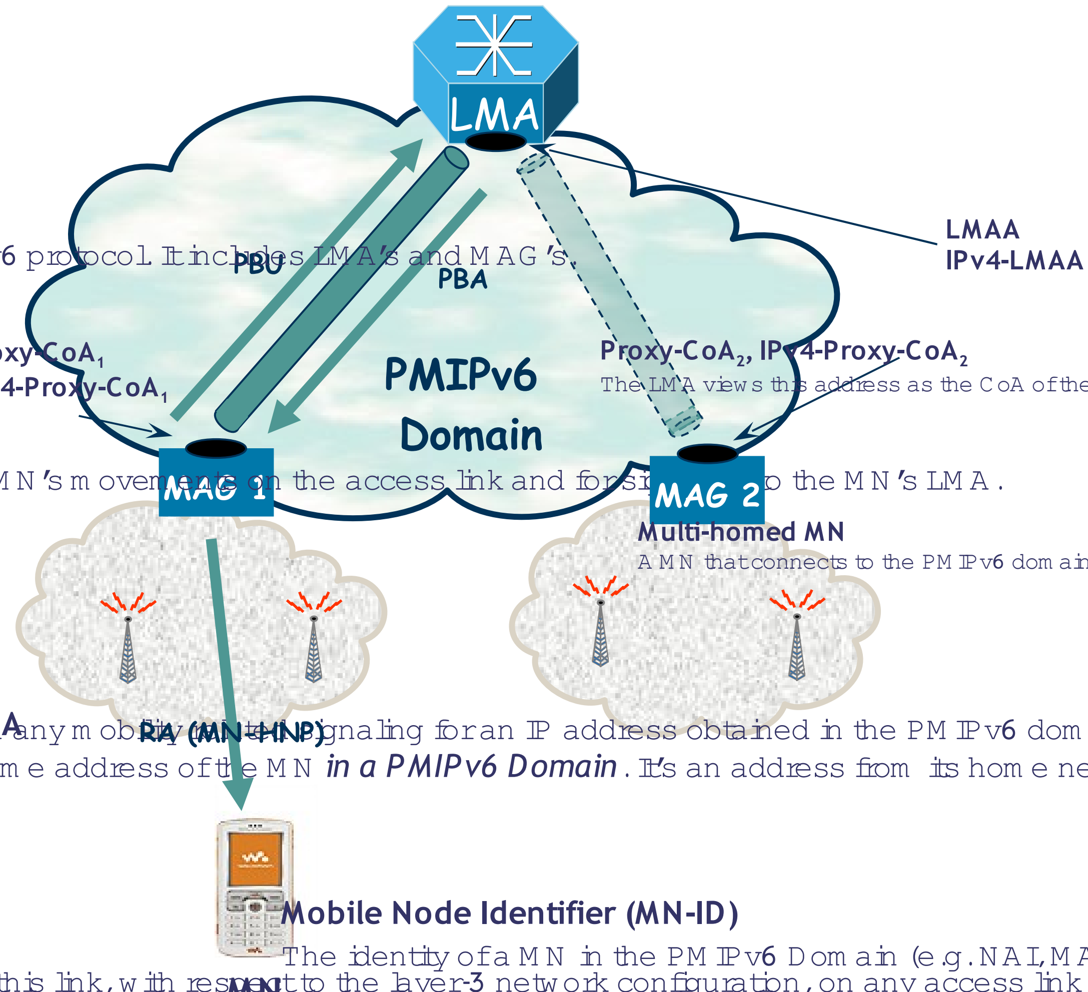
- Update latency. If the global mobility anchor point and/or correspondent node (for route-optimized traffic) is at some distance from the mobile node's access network, the global mobility update may require a considerable amount of time. During this time, packets continue to be routed to the old temporary local address and are essentially dropped
- Signaling overhead. The amount of signaling required when a mobile node moves from one last-hop link to another can be quite extensive, including all the signaling required to configure an IP address on the new link and global mobility protocol signaling back into the network for changing the permanent to temporary local address mapping. The signaling volume may negatively impact wireless bandwidth usage and real-time service performance.
- Location privacy. The change in temporary local address as the mobile node moves exposes the mobile node's topological location to correspondents and potentially to eavesdroppers. An attacker that can assemble a mapping between subnet prefixes in the mobile node's access network and geographical locations can determine exactly where the mobile node is located. This can expose the mobile node's user to threats on their location privacy

PMIPv6: Terminology

Local Mobility Anchor (LMA)

…red in the MN's LMA. The MN configures its interface with an address from this prefix. If the MN connects to the PMIPv6 Domain through multiple inte…

The home agent for the MN in the PMIPv6 Domain. *It's the topological anchor point for the MN's HNP* and it's t…



…nagement for a MN is handled by the PMIPv6 protocol. It includes LMA's and MAG's.

The LMA views this address as the CoA of the MN and registers it in the BC entry fo…

…access link. It's responsible for tracking the MN's movements on the access link and for si… to the MN's LMA.

Multi-homed MN

A MN that connects to the PMIPv6 domain simultaneously through multiple inter…

…dual mode. It is not required to participate in any mobility signaling for an IP address obtained in the PMIPv6 domain.

MN-HoA

The home address of the MN *in a PMIPv6 Domain*. It's an address from its home network prefix obtained by a M…

Mobile Node Identifier (MN-ID)

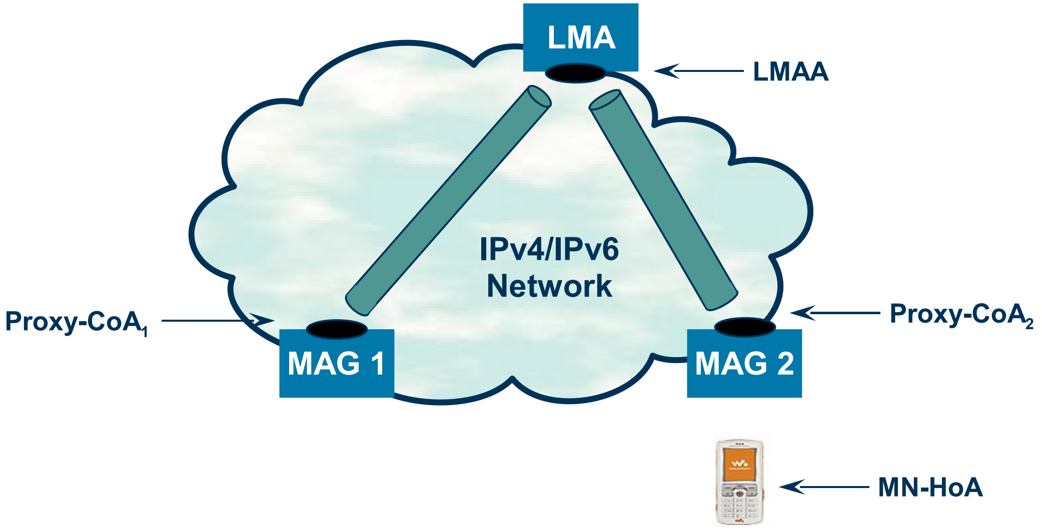
The identity of a MN in the PMIPv6 Domain (e.g. NAI, MAC address).

…network ensures that the MN always sees this link, with respect to the layer-3 network configuration, on any access link that it attaches to in the PM…

MN Interface Identifier (MN-Interface-ID)

Identifies a given interface of the MN. Could be based on a layer-2 ID, if present. May be generated by the MN and c…

PMIPv6: Architecture



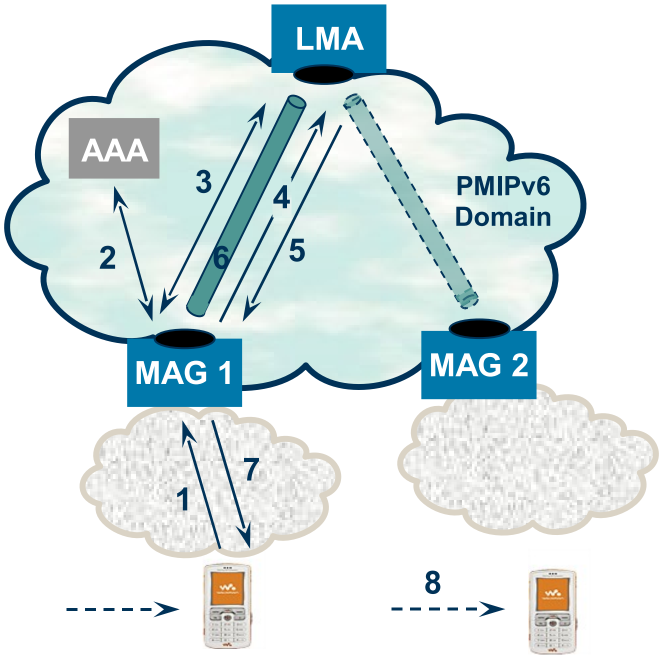
PMIPv6 Functional Entities

- LMA main functionality:
  - Responsible for maintaining the MN's reachability state (i.e. binding between HNP and Proxy-CoA).
  - The topological anchor point for the MN's home network prefix.
- MAG main functionality:
  - Performs mobility management on behalf of the MN.
  - Resides on the access link where the MN is anchored.
  - Responsible for detecting the MN's movement to and from the access link.
  - Sends binding registrations (PBU) to the MN's LMA.

PMIPv6: Signaling Flow

1. MN enters the PMIPv6 domain and attaches to an access link. A layer-2 access authentication, which may include the MN-ID, is done (the exact procedure is access link specific and outside the scope of the PMIPv6 specification).
2. MAG acquire MN's policy profile (incl. MN-ID) using for instance
   - Diameter
   - Pre-configured information in the MAG
   - Some other, proprietary, solution.

   MAG determine if MN is authorized for network-based IP mobility management service.
1. Establishment of a Security Association between the MAG and the LMA can be done either:
   - Dynamically (using IKEv2), or
   - Statically using a pre-configured SA.
2. MAG sends PBU to the LMA
   - LMA establishes a bi-directional tunnel to the MAG.
   - LMA creates BC entry for the MN's HNP and sets up a route for the prefix over the tunnel.
3. LMA sends PBA to the MAG
   - MAG establishes bi-directional tunnel to the LMA.
   - Sets up the data path for the MN's data traffic.
4. Bi-directional tunnel (IP-in-IP, RFC 2473) for the MN's data traffic established between the MAG and the LMA.
5. MAG sends RA advertising the MN's HNP and other configuration information
   - The MN will attempt to configure its interface, either using stateless or stateful address configuration. As a result the MN will end up with an address from its HNP.



When a MN changes MAG within the PMIPv6 domain the network ensures that the same HNP is advertised on the link where the MN is currently attached. i.e. the network ensures that the MN believes it is always on the same link where it obtained its initial address configuration.

PMIPv6: Stack Impact

- Any ideas?

PMIPv6: References

- Editor J. Kempf "NETLMM Problem Statement". Informational IETF RFC 4830, April 2007
- K. Leung, V. Devarapalli, K. Chowdhury, B. Patil "Proxy Mobile Ipv6", IETF RFC 5213, August 2008

Questions and Discussions