Internet Protocol, Version 6 (IPv6)

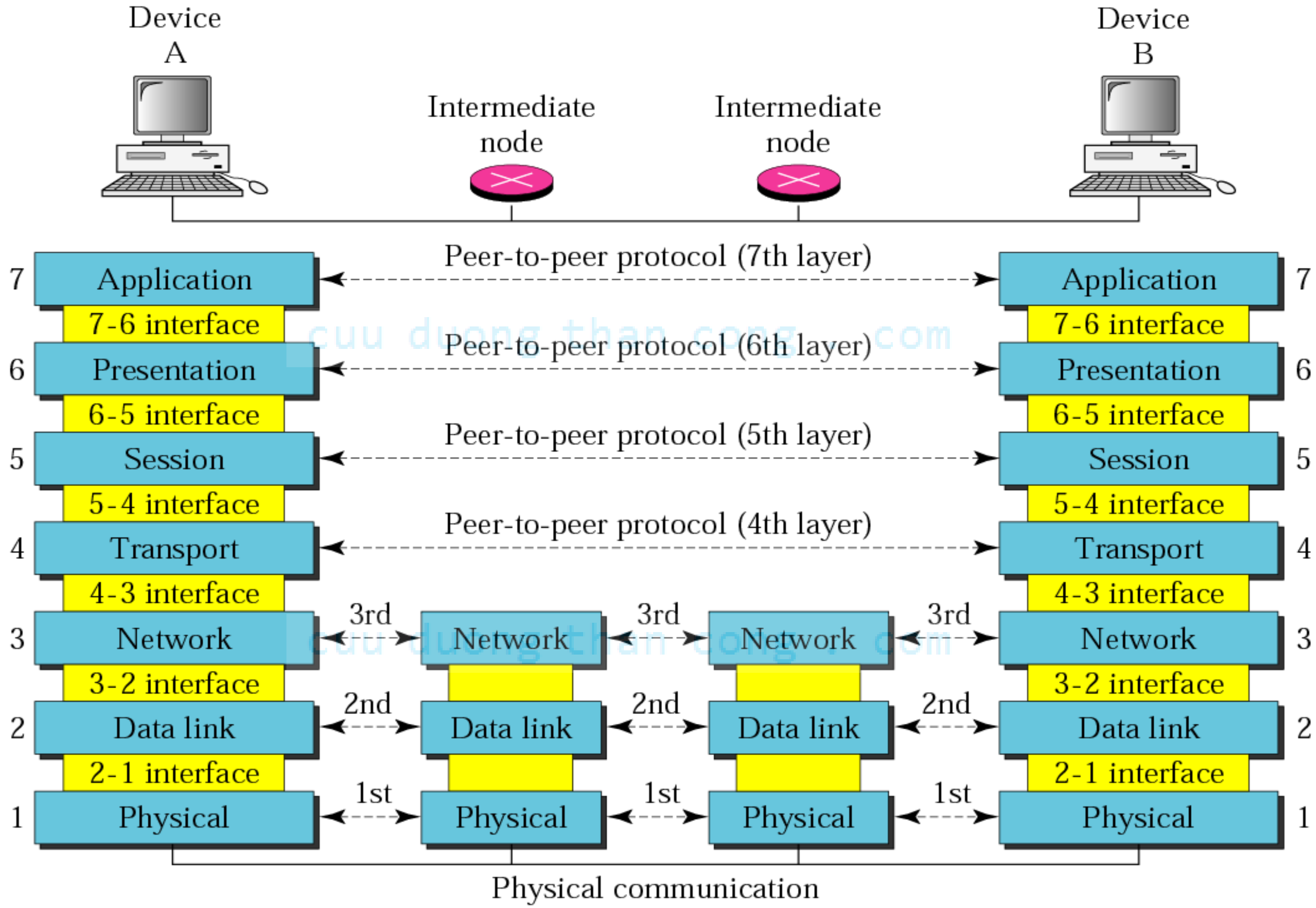
MẠNG MÁY TÍNH NÂNG CAO

lnson@fit.hcmus.edu.vn

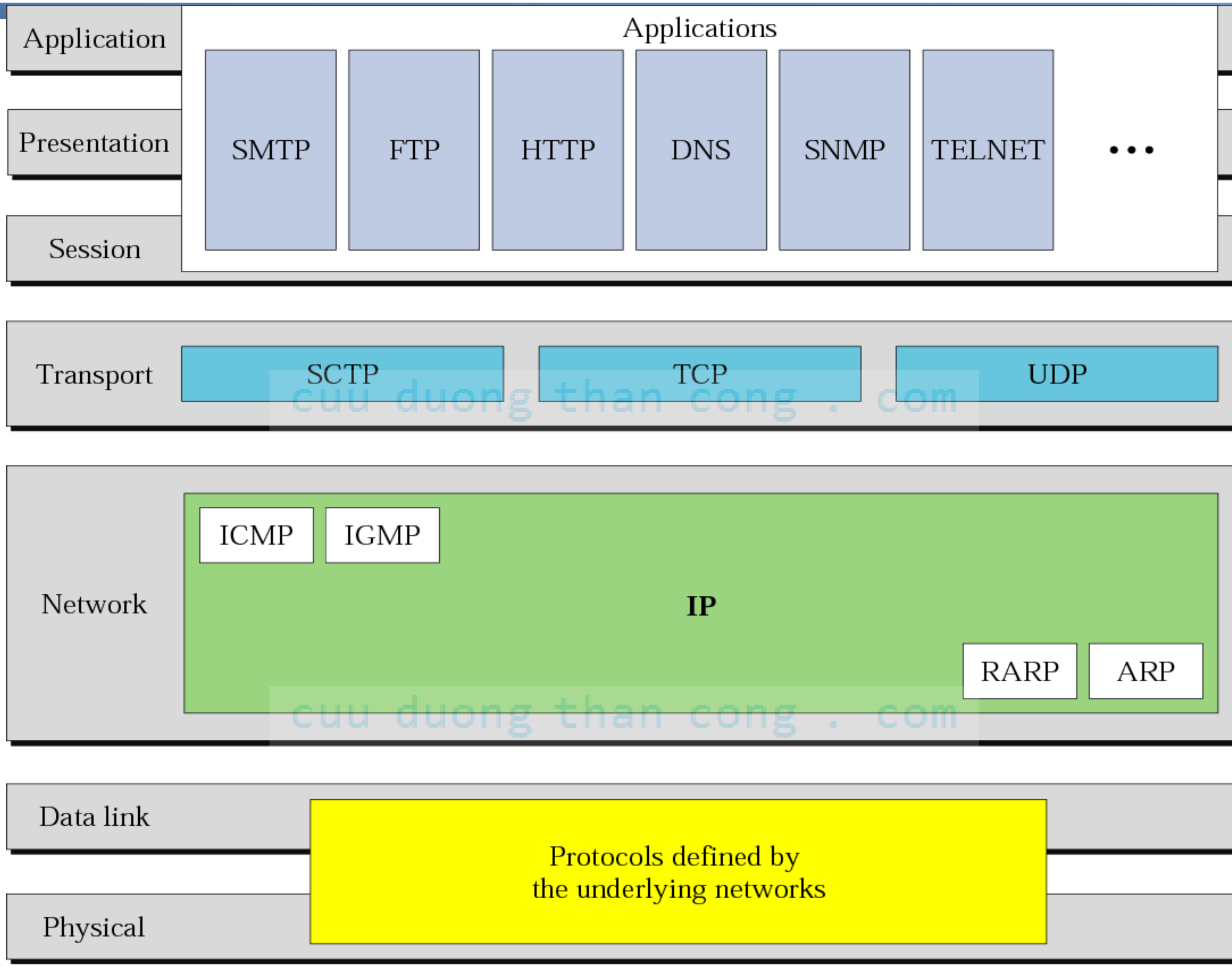
Outline

- ❑ Networking Basics
- ❑ Introduction to IPv6
- ❑ IPv6 Header Format
- ❑ IPv6 Addressing Model
- ❑ ICMPv6
- ❑ Neighbor Discovery
- ❑ Transition from IPv4 to IPv6
- ❑ IPv6 vs. IPv4

Basics: OSI 7-Layer



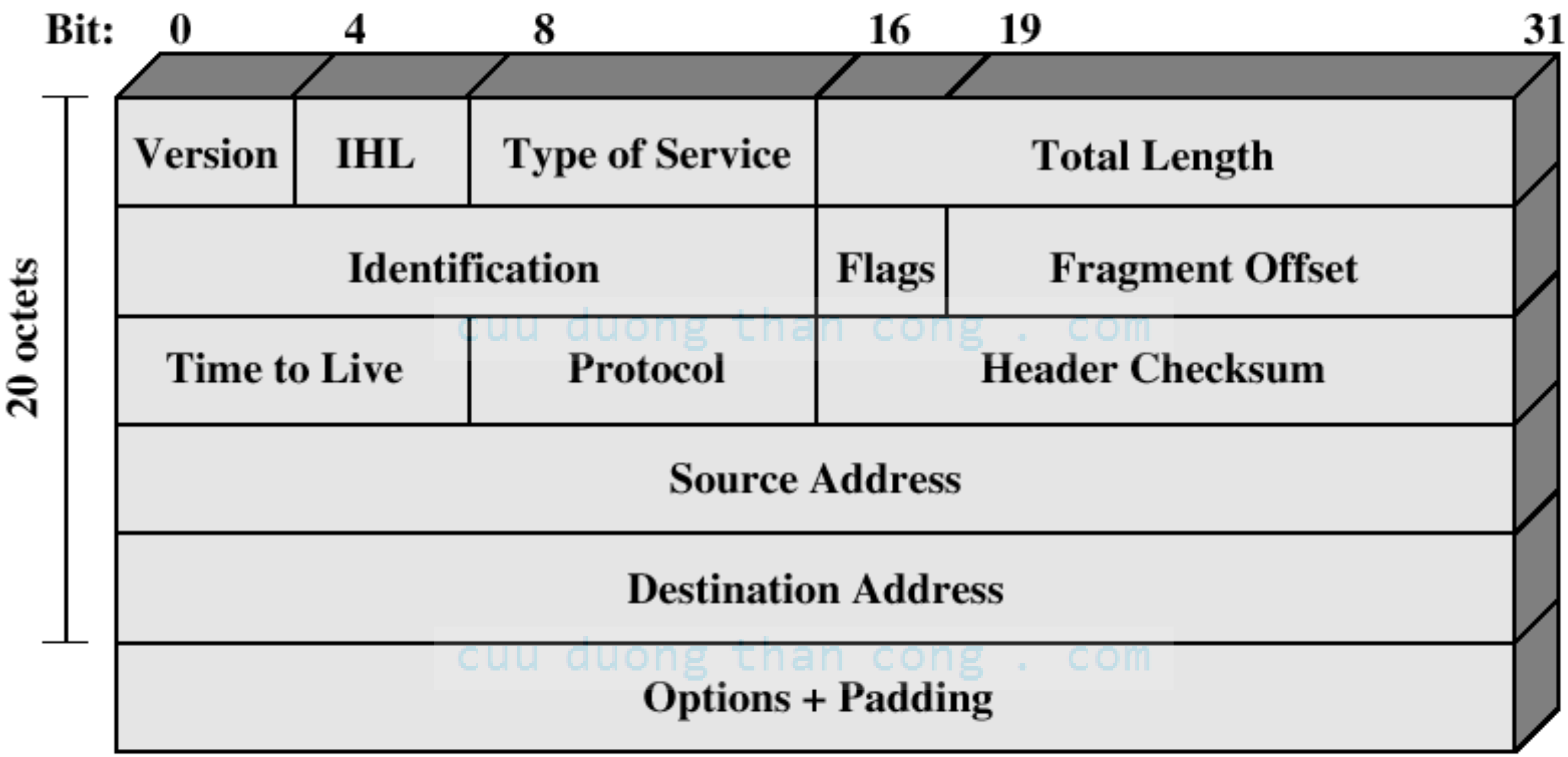
Basics: TCP/IPv4 Protocol Suite



Internet Protocol (IP)

- Features:
  - Layer 3 (Network layer)
  - Unreliable, Connectionless, Datagram
  - Best-effort delivery
- Popular version: IPv4
- Major functions
  - Global addressing
  - Datagram lifetime
  - Fragmentation & Reassembly

IPv4 Header



Bit: 0 4 8 16 19 31
20 octets
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + Padding

IPv4 companion protocols (1)

- ARP: Address Resolution Protocol
  - Mapping from IP address to MAC address
- ICMP: Internet Control Message Protocol
  - Error reporting & Query
- IGMP: Internet Group Management Protocol
  - Multicast member join/leave
- Unicast Routing Protocols (Intra-AS)
  - Maintaining Unicast Routing Table
  - E.g. RIP, OSPF (Open Shortest Path First)

IPv4 companion protocols (2)

- Multicast Routing Protocols
  - Maintaining Multicast Routing Table
  - E.g. DVMRP, MOSPF, CBT, PIM
- Exterior Routing Protocols (Inter-AS)
  - E.g. BGP (Border Gateway Protocol)
- Quality-of-Service Frameworks
  - Integrated Service (ISA, IntServ)
  - Differentiated Service (DiffServ)

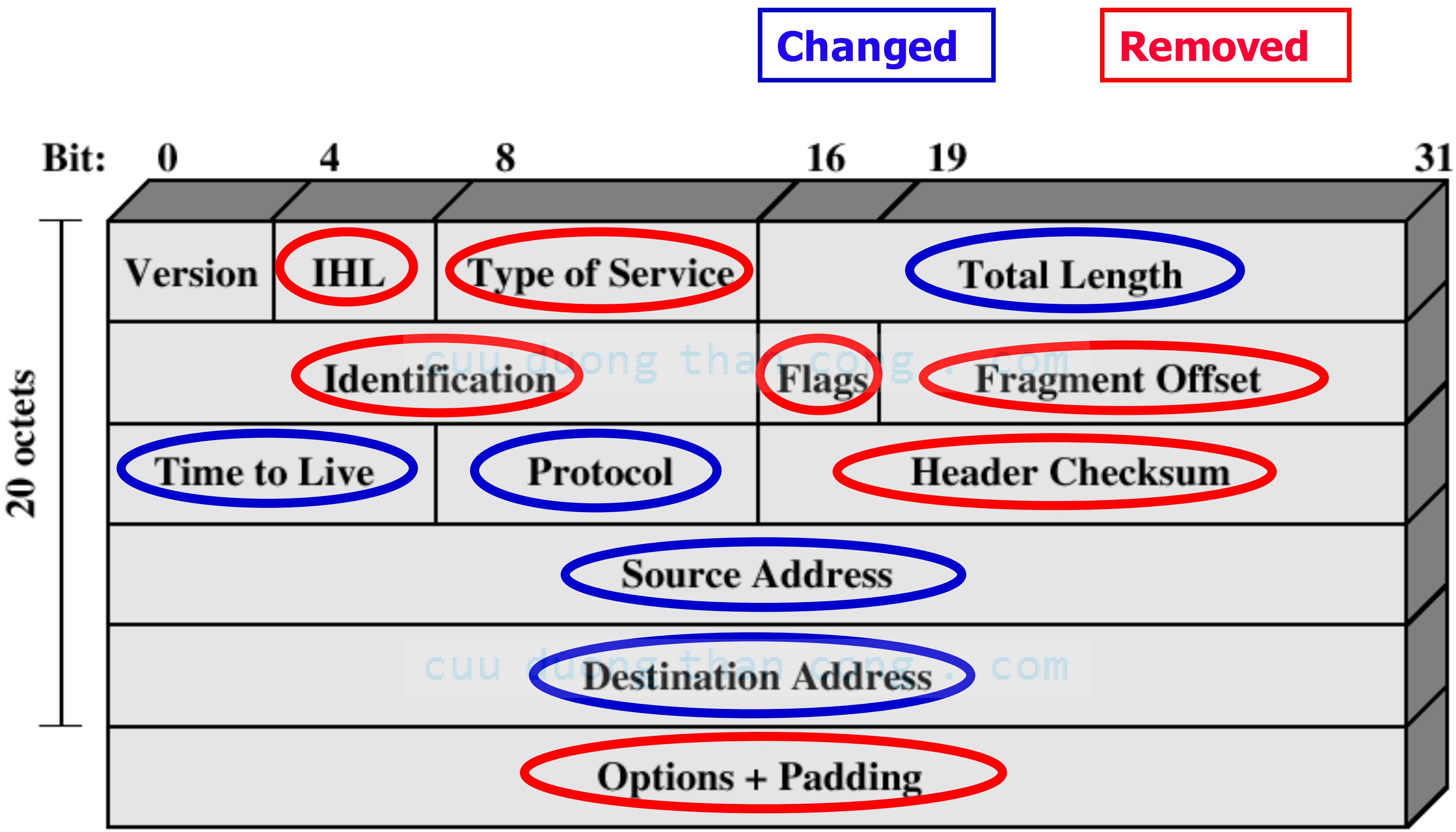
Why IPv6?

- ❑ Deficiency of IPv4
- ❑ Address space exhaustion
- ❑ New types of service → Integration
  - Multicast
  - Quality of Service
  - Security
  - Mobility (MIPv6)
- ❑ Header and format limitations

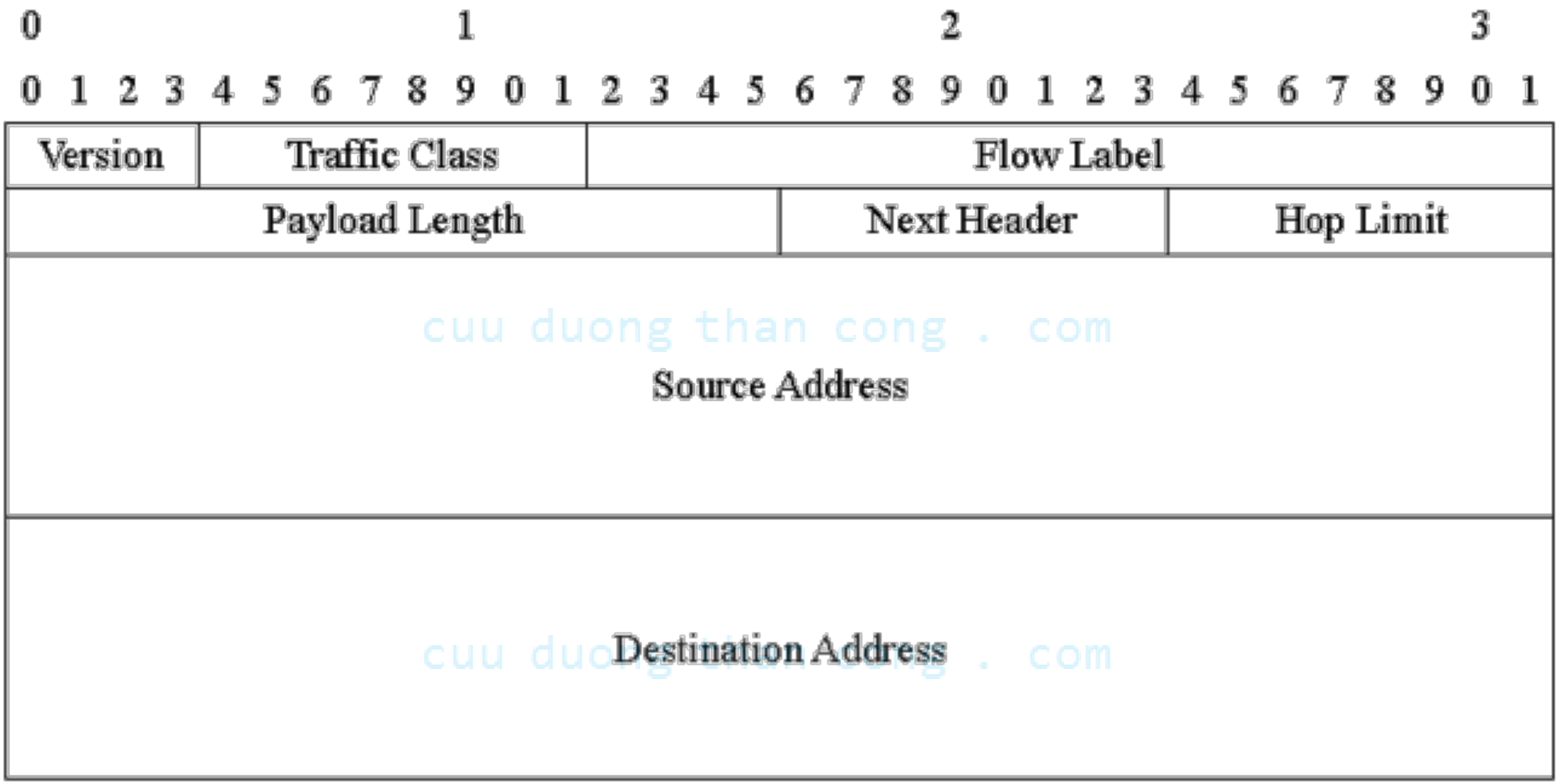
Advantages of IPv6 over IPv4

- Larger address space
- Better header format
- New options
- Allowance for extension
- Support for resource allocation
- Support for more security
- Support for mobility

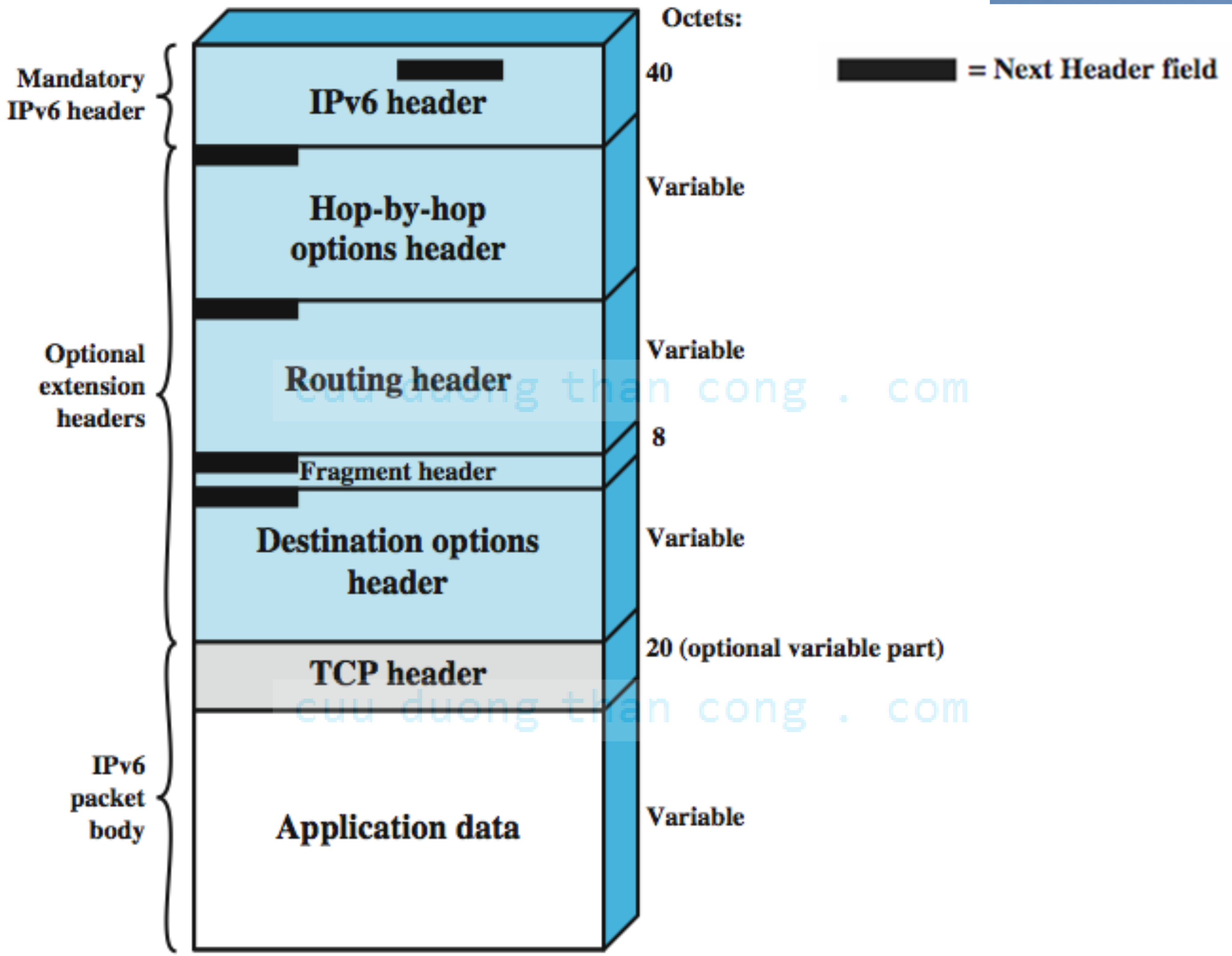
Header: from IPv4 to IPv6



IPv6 Header Format



IPv6 Packet (PDU) Structure



Traffic Class

- The 8-bit field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.
  - E.g., used as the codepoint in DiffServ
- General requirements
  - Service interface must provide means for upper-layer protocol to supply the value of traffic class
  - Value of traffic class can be changed by source, forwarder, receiver
  - An upper-layer protocol should not assume the value of traffic class in a packet has not been changed.

IPv6 Flow Label

- Related sequence of packets
- Needing special handling
- Identified by src & dest addr + flow label
- Router treats flow as sharing attributes
  - E.g. path, resource allocation, discard requirements, accounting, security
- May treat flows differently
  - Buffer sizes, different forwarding precedence, different quality of service
- Alternative to including all info. in every header

Payload Length

- 16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets.
- Note that any extension headers present are considered part of the payload, i.e., included in the length count.

Extension Header Order

Order	Header Type	Next Header Code
1	Basic IPv6 Header	
2	Hop-by-Hop Options	0
4	Routing header	43
5	Fragment header	44
6	Authentication header	51
7	Encapsulation Security Payload header	50
8	Destination Options	60
9	Mobility header	135
	No Next header (Null)	59
	Upper layer: TCP, UDP, ICMP	6, 17, 58

Hop-by-Hop Options

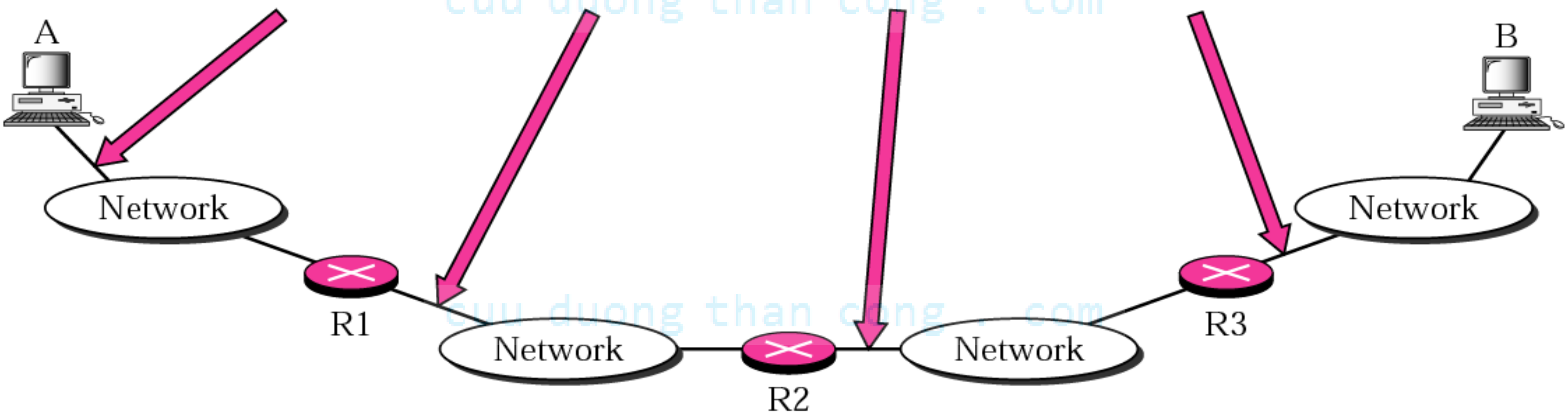
- Must be examined by every router
  - Specifies discard/forward handling
- Options
  - Pad1
  - PadN
  - Jumbo payload
  - Router alert (can be used for RSVP)

Routing Header

- List of one or more intermediate nodes to visit
- Header includes
  - Next Header
  - Header extension length
  - Routing type (e.g. type 0 = Source Routing)
  - Segments left

Source Routing Example

Source: A	Source: A	Source: A	Source: A
Destination: R1	Destination: R2	Destination: R3	Destination: B
Left: 3	Left: 2	Left: 1	Left: 0
R2	R1	R1	R1
R3	R3	R2	R2
B	B	B	R3



Fragment Header (1)

- Fragment Offset: 8-bit unsigned integer
  - The offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the original packet
  - Unfragmentable part: IPv6 header + any extension headers that must be processed by nodes en route


```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |   Reserved    |      Fragment Offset    |Res|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Identification                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fragment Header (2)

- M flag: 1=more fragments, 0=last fragment
- Identification: combined with the src & dest addr uniquely identifies the original packet

```
+------------------+--------+--------------+
|  Unfragmentable  |Fragment|    first     |
|       Part       | Header |   fragment   |
+------------------+--------+--------------+

+------------------+--------+--------------+
|  Unfragmentable  |Fragment|    second    |
|       Part       | Header |   fragment   |
+------------------+--------+--------------+
                       o
                       o
                       o
+------------------+--------+----------+
|  Unfragmentable  |Fragment|   last   |
|       Part       | Header | fragment |
+------------------+--------+----------+
```

Reassembly (1)

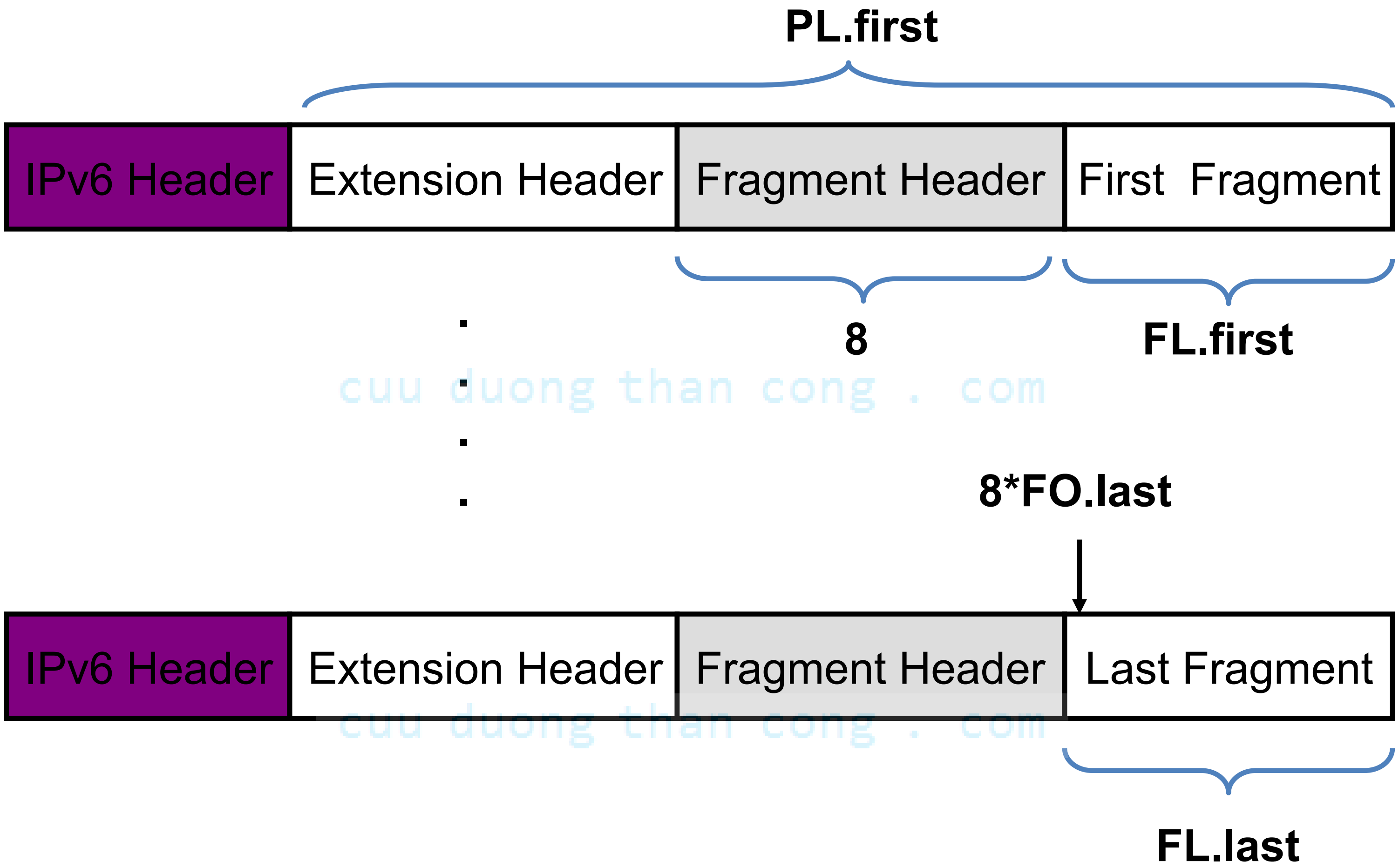
- The Unfragmentable Part of the reassembled packet consists of all headers up to, but not including, the Fragment header of the first fragment packet
- The Next Header field of the last header of the Unfragmentable Part is obtained from the Next Header field of the first fragment's Fragment header
- The Payload Length of the reassembled packet is computed from the length of the Unfragmentable Part and the length and offset of the last fragment.

Reassembly (2)

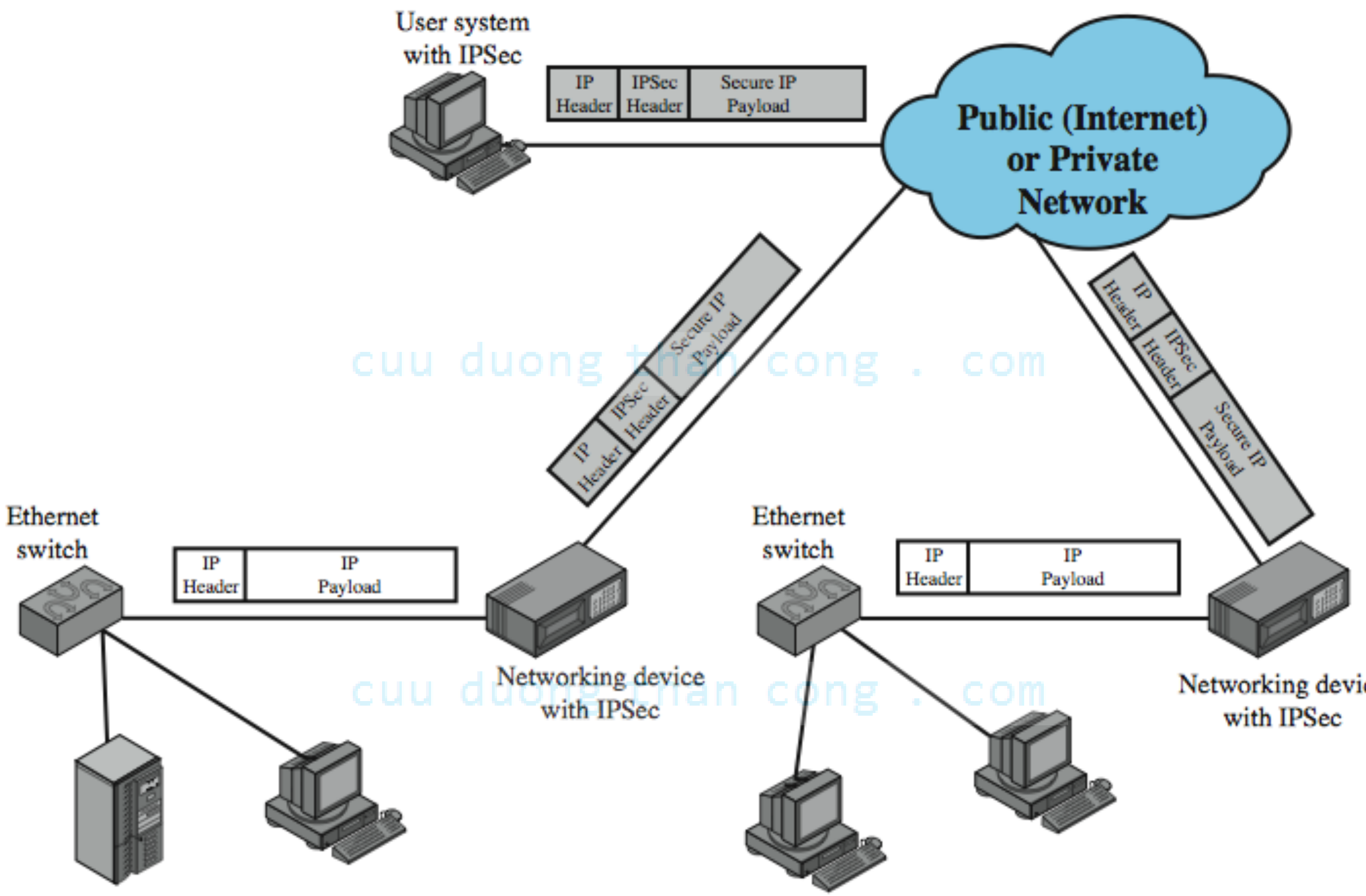
- PL.orig = ~~PL.first - FL.first - 8 +~~ (8 * FO.last) + FL.last

  - PL.orig = Payload Length field of reassembled packet.
  - PL.first = Payload Length field of first fragment packet.
  - FL.first = length of fragment following Fragment header of first fragment packet.
  - FO.last = Fragment Offset field of Fragment header of last fragment packet.
  - FL.last = length of fragment following Fragment header of last fragment packet.

Reassembly (3)



IPsec Scenario



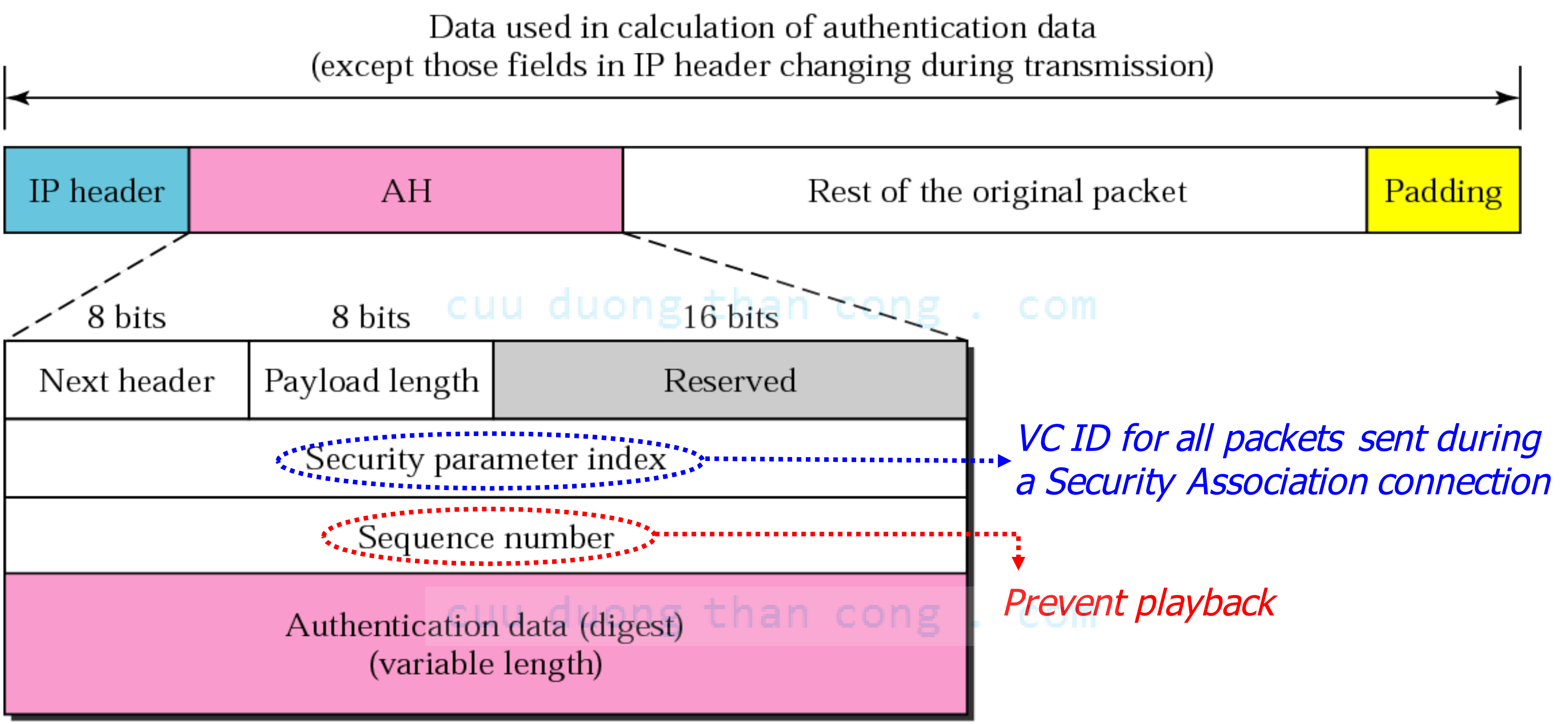
IPSec Benefits

- ❑ Provides strong security for external traffic
- ❑ Resistant to bypass
- ❑ Below transport layer hence transparent to applications
- ❑ Can be transparent to end users
- ❑ Can provide security for individual users if needed

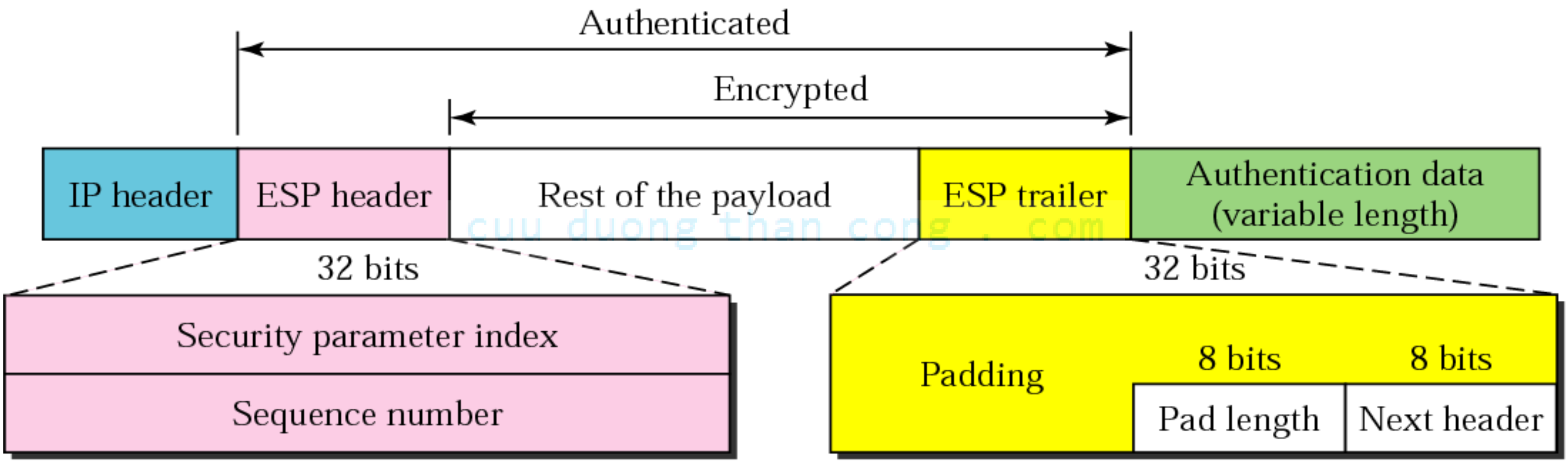
IPSec Functions

- ❑ Authentication Header
  - for authentication/integrity only
- ❑ Encapsulating Security Payload (ESP)
  - for authentication/integrity/encryption (privacy)
- ❑ A key exchange function
  - Manual or automated
- ❑ VPNs usually need combined function

Authentication Header



Encapsulating Security Payload



IPv6 Addressing Model

- Addresses are assigned to interfaces, not hosts
- Interface expected to have multiple addresses
- Addresses have scope
  - Link-Local
  - Site-Local → Unique Local
  - Global

IPv6 Addressing Model

3FFE:085B:1F1F:0000:0000:0000:00A9:1234

128bits = 8 groups of 16-bit hexadecimal numbers sep

Leading zeros can be removed

3FFE:85B:1F1F::A9:1234

:: = all zeros in one or more group of 16-bit hexadecimal numbe

Text Representation of Address

❑ Colon-Hex

- 3ffe:3600:2000:0800:0248:54ff:fe5c:8868

❑ Compressed Format:

- 3ffe:0b00:0c18:0001:0000:0000:0000:0010

➔ 3ffe:b00:c18:1::10

Types of IPv6 Addresses

- Unicast
  - Address of a single interface
  - Delivery to single interface
- Multicast
  - Address of a set of interfaces
  - Delivery to all interfaces in the set
- Anycast
  - Address of a set of interfaces
  - Delivery to a single interface in the set
- No more broadcast addresses

Address Type Prefixes

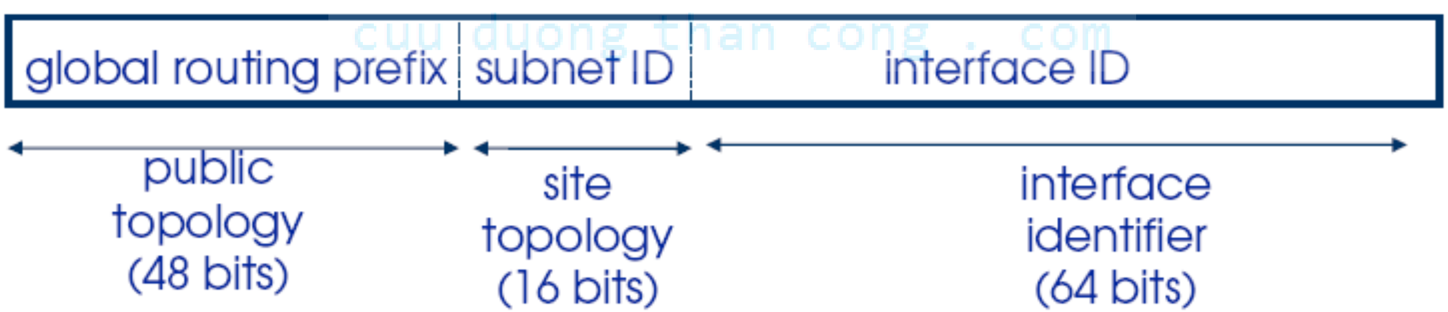
Address type	Binary prefix
IPv4-compatible	0000...0 (96 zero bits)
global unicast	001
link-local unicast	1111 1110 10
site-local unicast	1111 1110 11
multicast	1111 1111

- all other prefixes reserved (approx. 7/8ths of total)
- anycast addresses allocated from unicast prefixes

Global Unicast Address

- Global routing prefix
  - A (typically hierarchically-structured) value assigned to a site (a cluster of subnets/links)
- Subnet ID
  - An identifier of a subnet within the site
- Interface ID
  - Constructed in Modified EUI-64 format

RFC 3587 - IPv6 Global Unicast Address Format

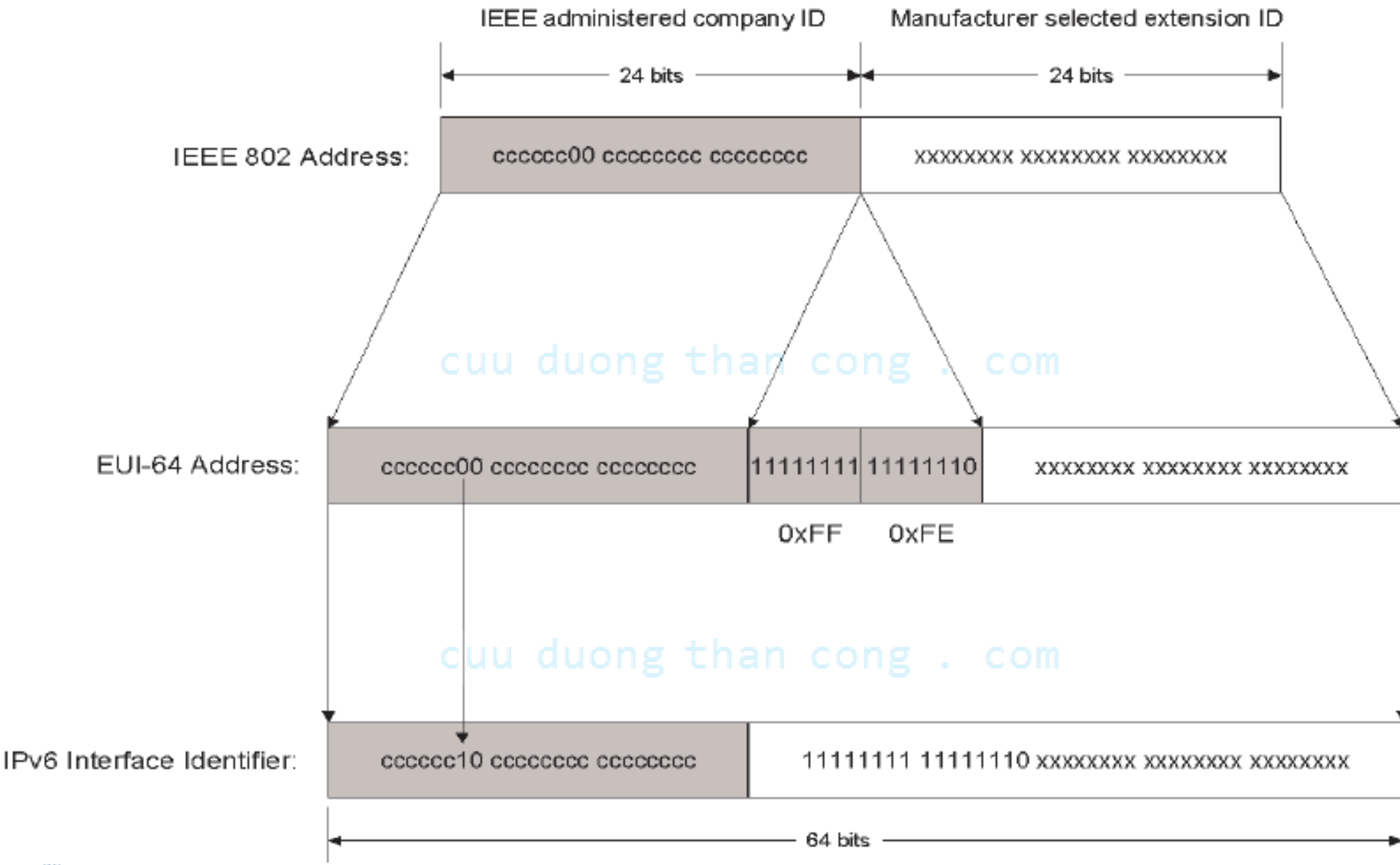


Interface Identifier

may be assigned in several different ways:

- auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address (e.g., Ethernet address)
- auto-generated pseudo-random number (to address privacy concerns)
- assigned via DHCP
- manually configured
- possibly other methods in the future

IEEE 802 → IPv6 Interface ID



Site-Local Address

- Meaningful only in a single site zone, and may be re-used in other sites
- Equivalent to the IPv4 private address space
- Address are not automatically configured and must be assigned
- Prefix= FEC0::/48

Link-Local Address

- Meaningful only in a single link zone, and may be re-used on other links
- Link-local addresses for use during auto-configuration and when no routers are present
- Required for Neighbor Discovery process, always automatically configuration
- An IPv6 router never forwards link-local traffic beyond the link
- Prefix= FE80::/64

Special IPv6 Address

- ❑ Loopback address (0:0:0:0:0:0:0:1 or ::1)
  - Identify a loopback interface
- ❑ IPv4-compatible address (0:0:0:0:0:0:w.c.x.z or ::w.c.x.z)
  - Used by dual-stack nodes
  - IPv6 traffic is automatically encapsulated with an IPv4 header and send to the destination using the IPv4 infrastructure
- ❑ IPv4 mapped address (0:0:0:0:0:FFFF:w.c.x.z or ::FFFF:w.c.x.z)
  - Represent an IPv4-only node to an IPv6 node
  - Only use a single listening socket to handle connections from client via both IPv6 and IPv4 protocols.
  - Never used as a source or destination address of IPv6 packet
  - Rarely implemented

Address Autoconfiguration (1)

- Allow plug and play
- BOOTP and DHCP are used in IPv4
- DHCPng will be used with IPv6
- Two Methods: Stateless and Stateful
- Stateless:
  - A system uses link-local address as source and multicasts to "All routers on this link"
  - Router replies and provides all the needed prefix info
  - All prefixes have a associated lifetime
  - System can use link-local address permanently if no router

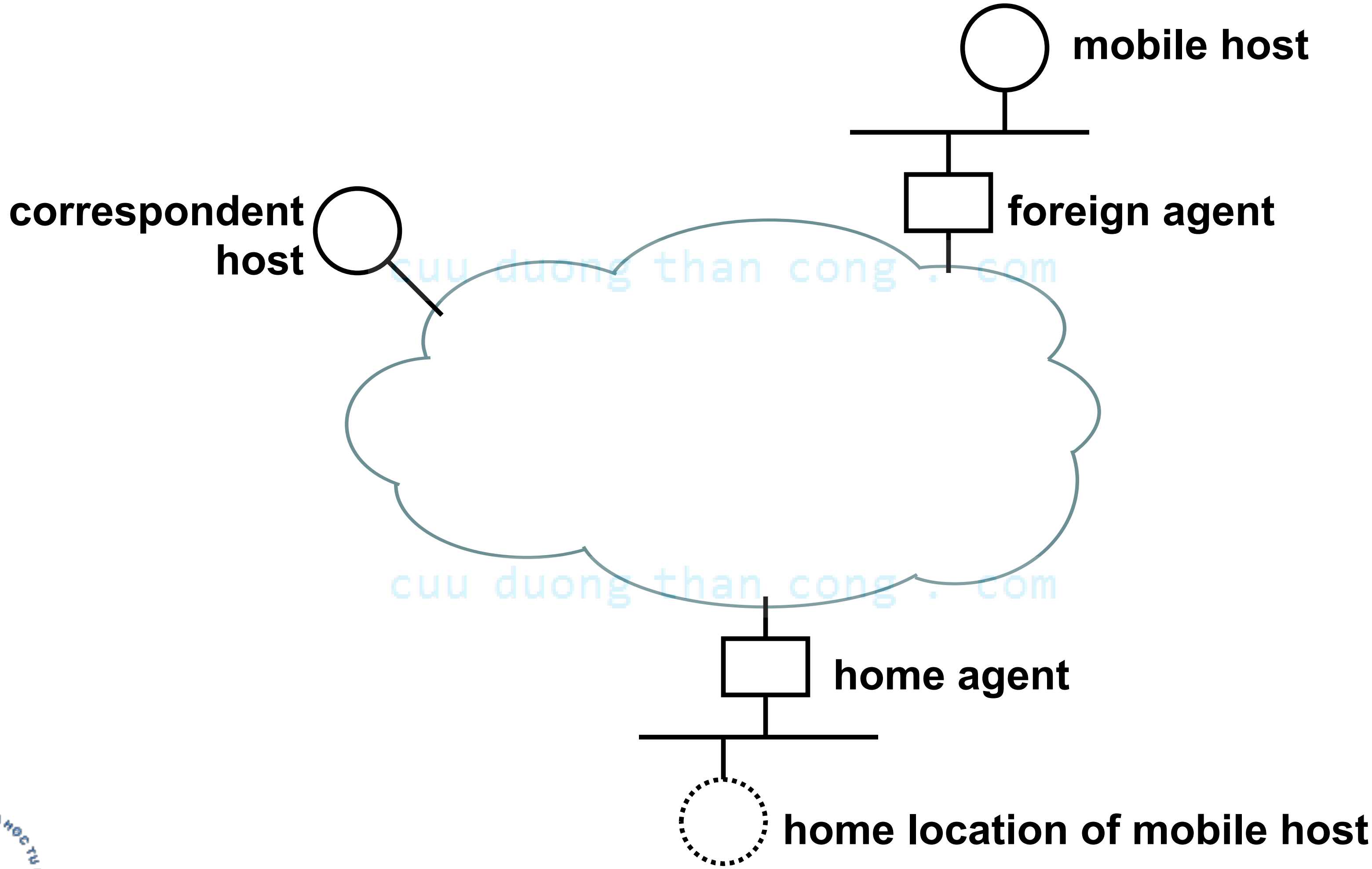
Address Autoconfiguration (2)

- Stateful:
  - Problem w/ stateless: Anyone can connect
  - Routers ask the new system to go DHCP server (by setting managed configuration bit)
  - System multicasts to "All DHCP servers"
  - DHCP server assigns an address

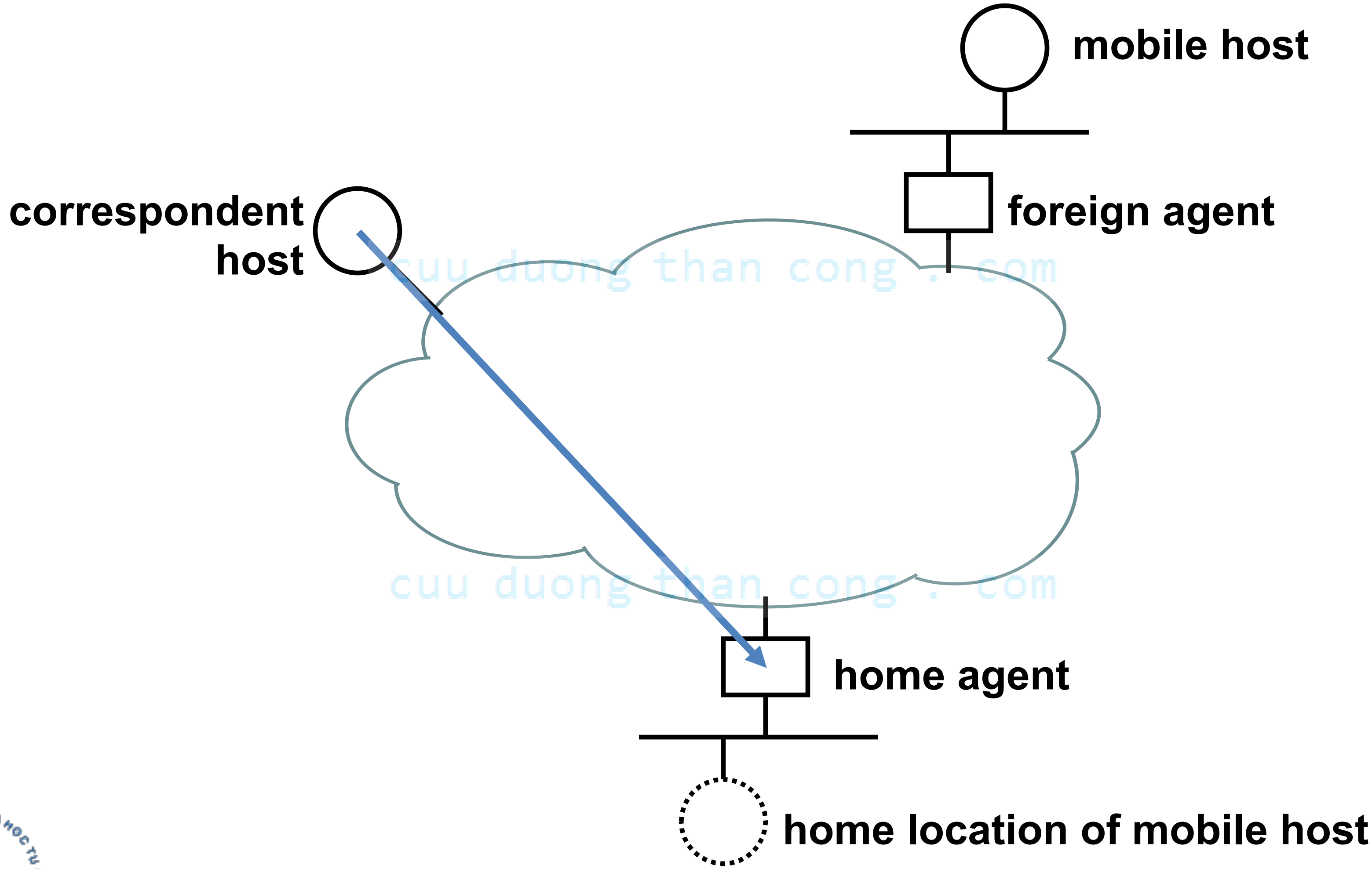
IPv6 Mobility

- Mobile hosts have one or more home address
  - relatively stable; associated with host name in DNS
- A Host will acquire a foreign address when it discovers it is in a foreign subnet (i.e., not its home subnet)
  - 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 IPv6 hosts will send binding-updates to correspondent to remove home agent from flow

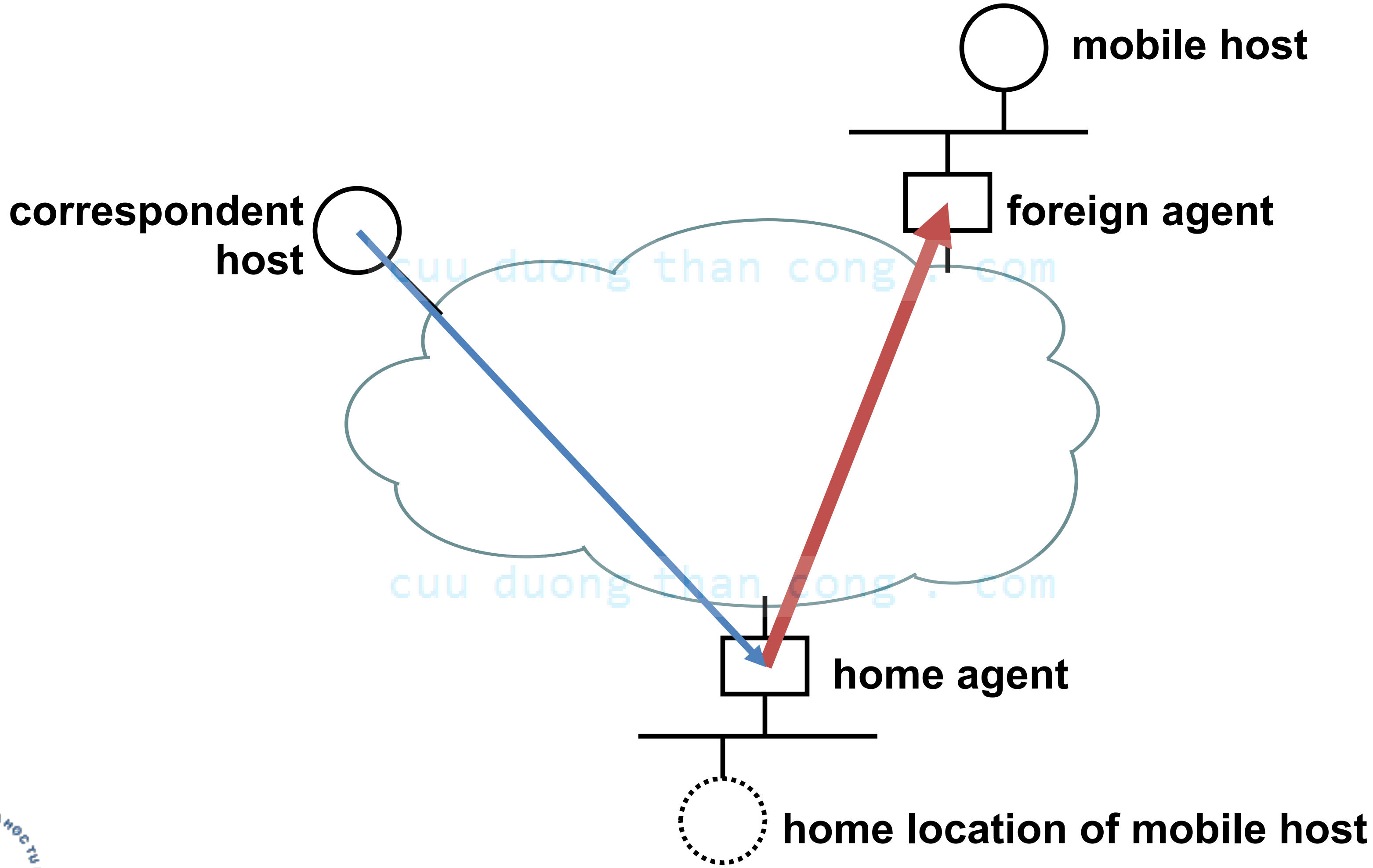
Mobile IP (v4 version)



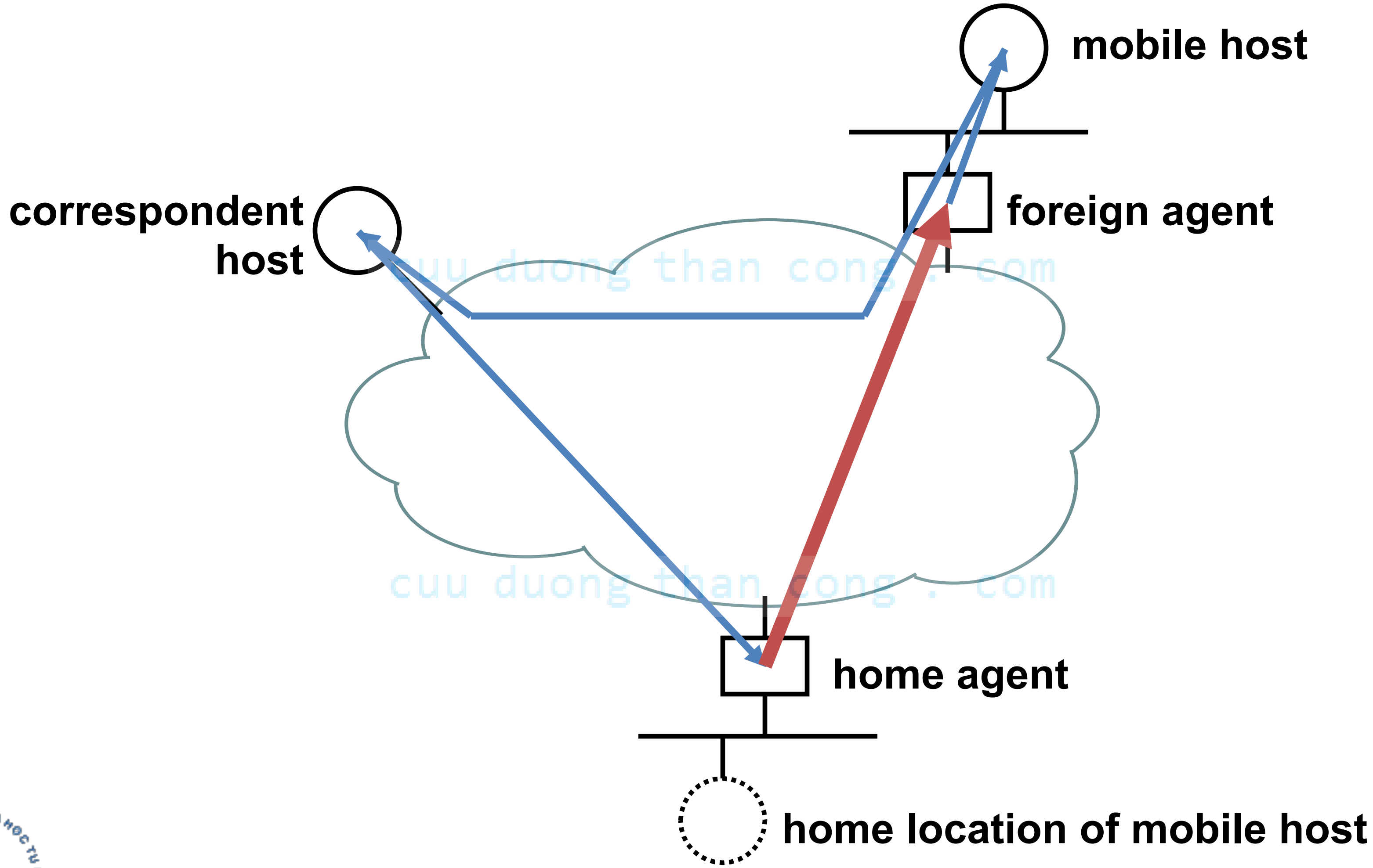
Mobile IP (v4 version)



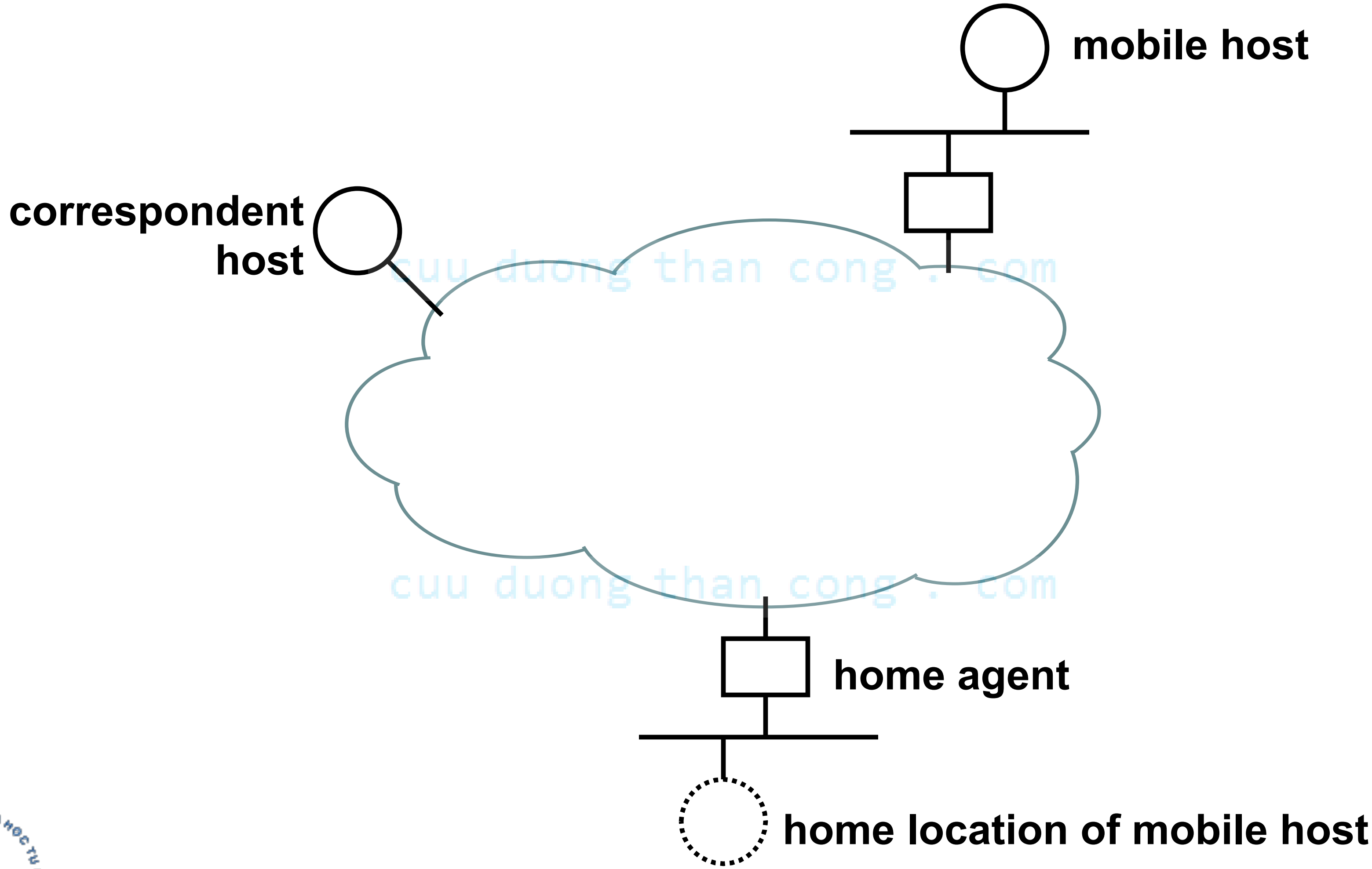
Mobile IP (v4 version)



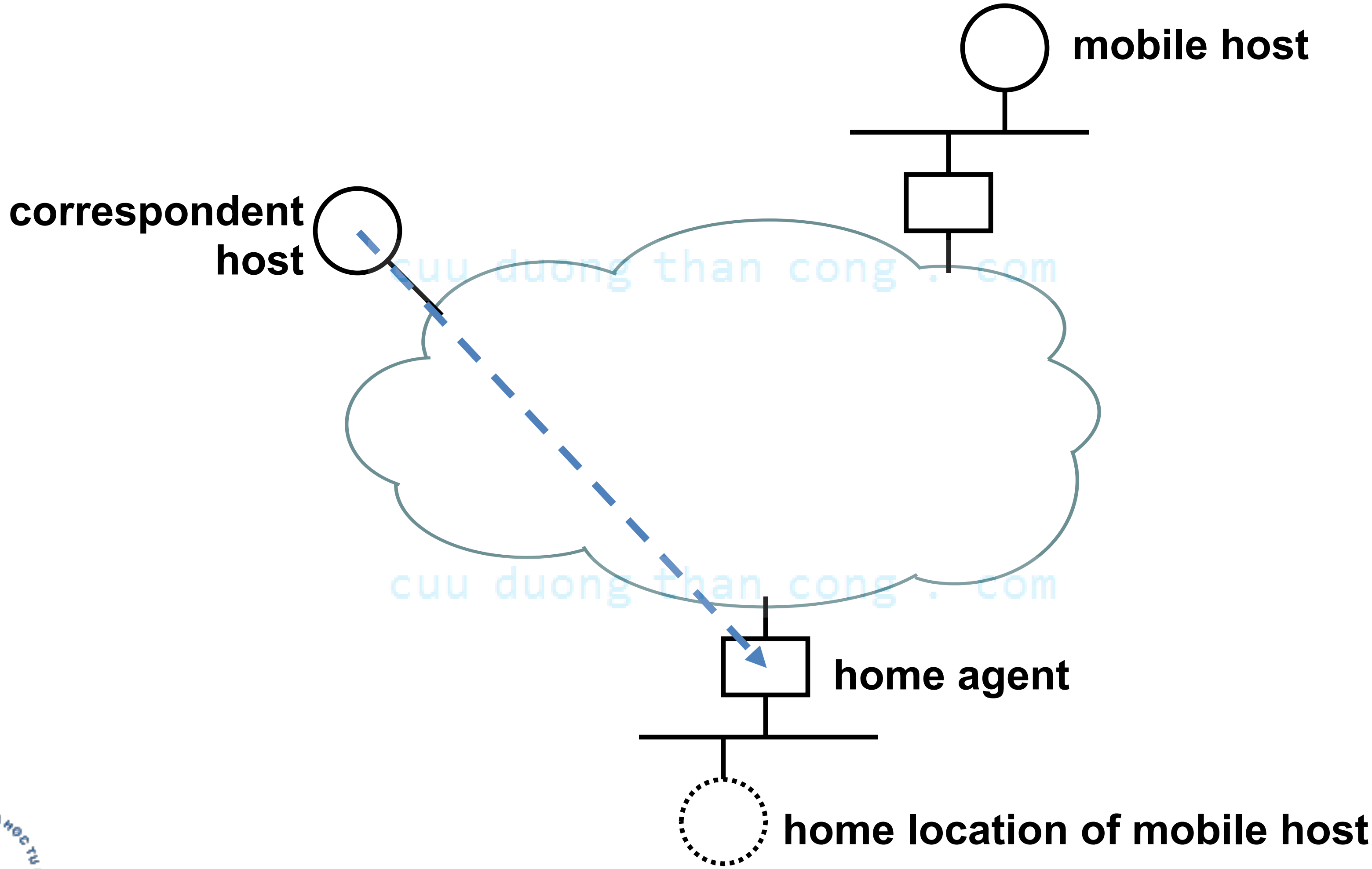
Mobile IP (v4 version)



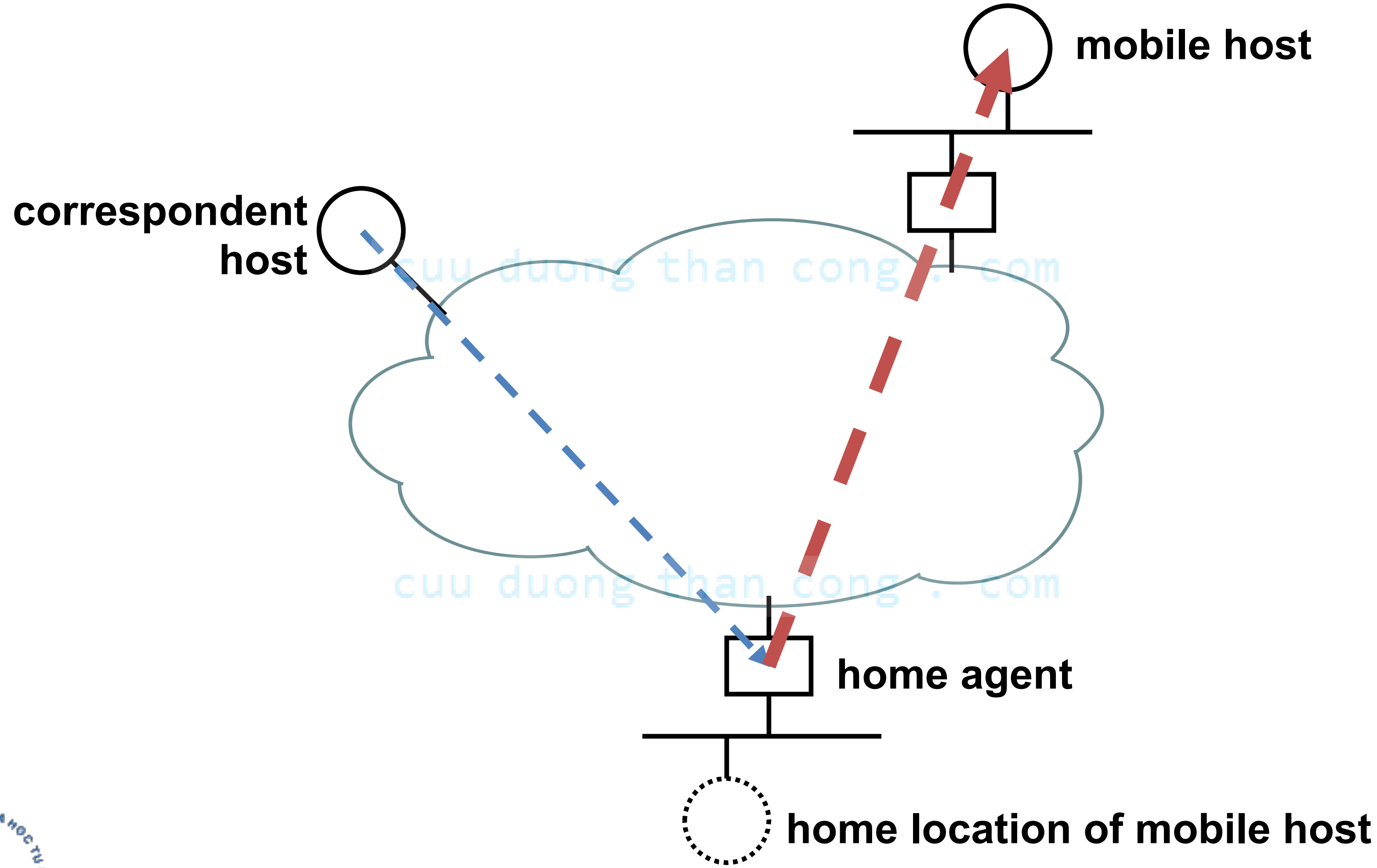
Mobile IP (v6 version)



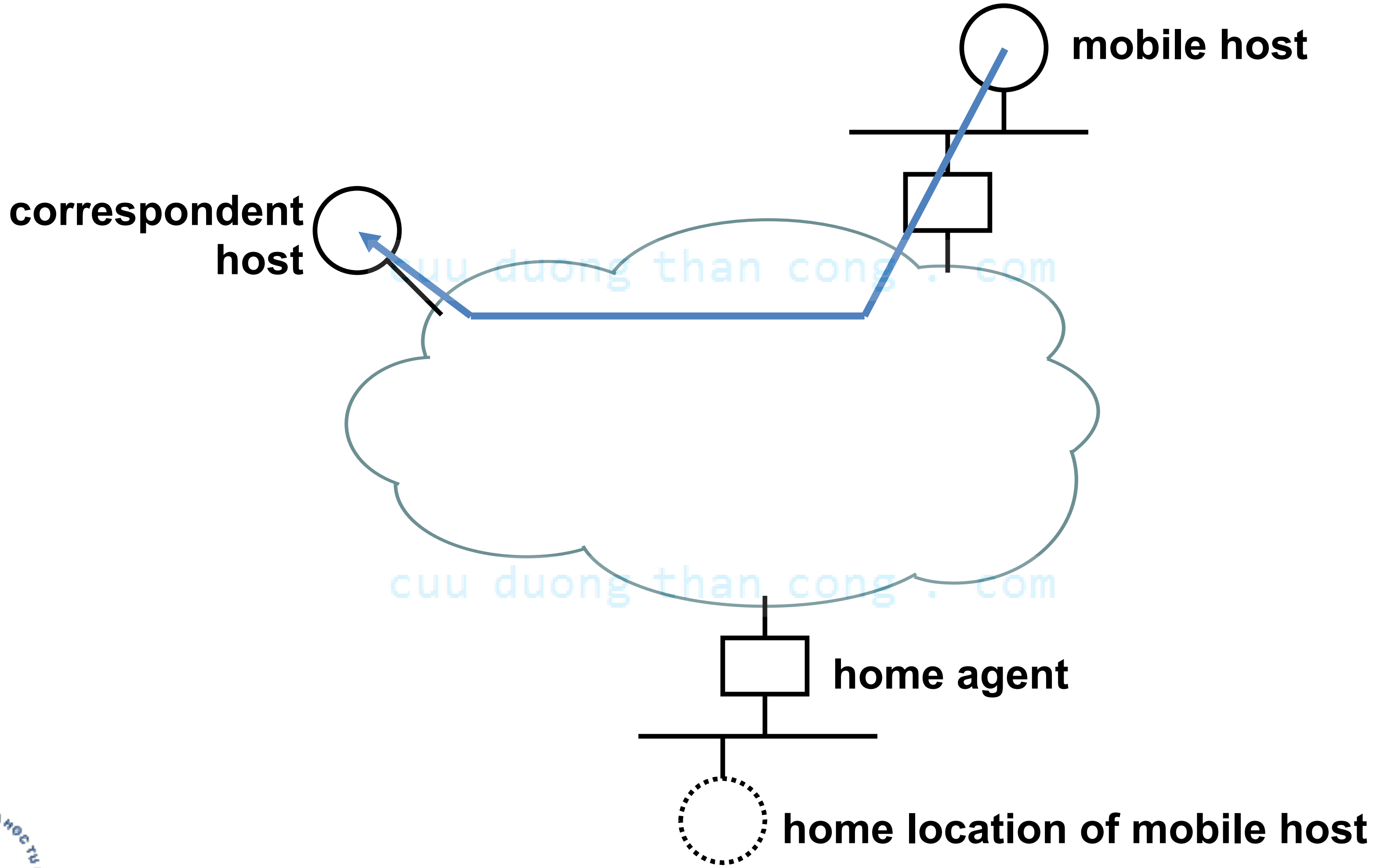
Mobile IP (v6 version)



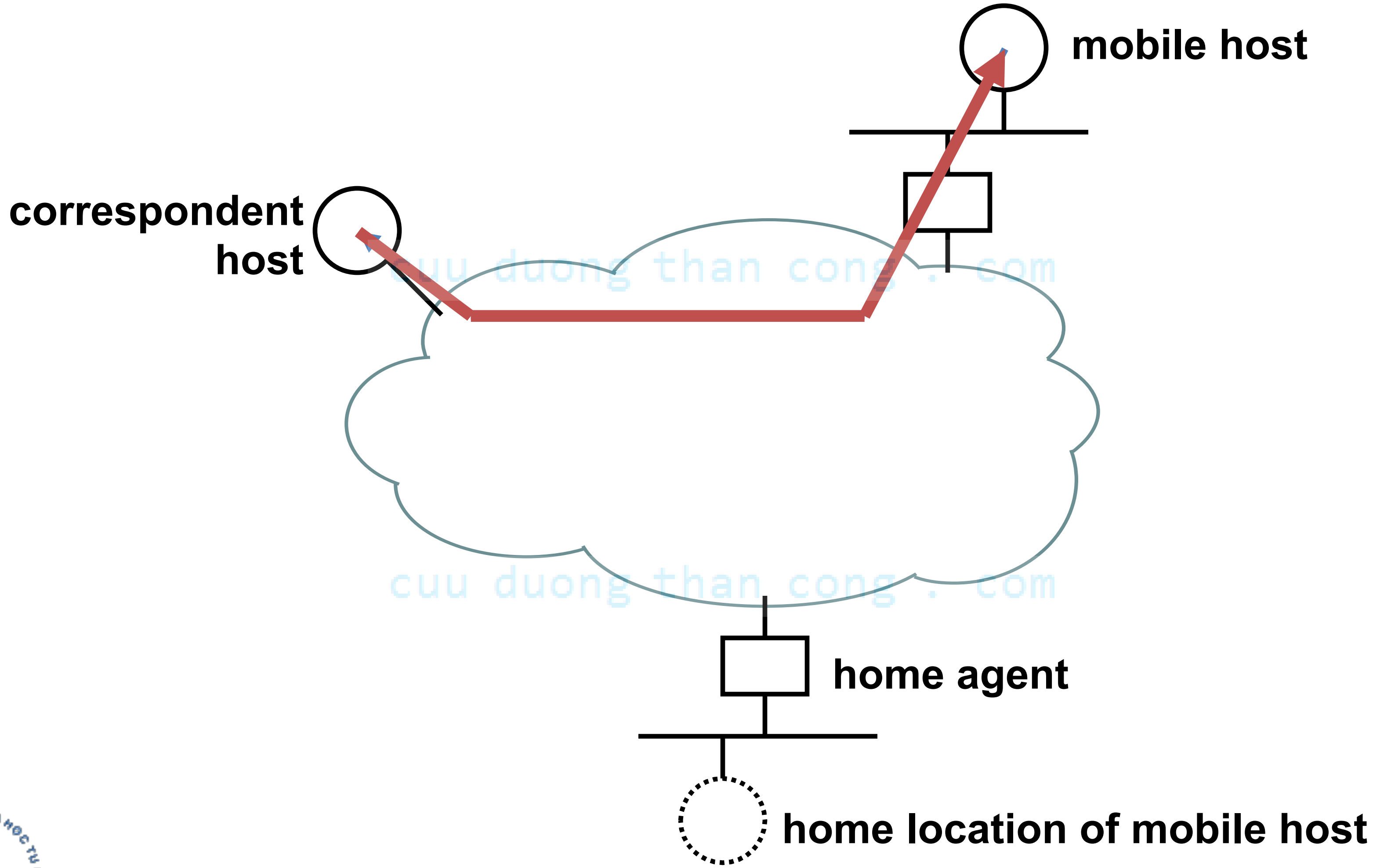
Mobile IP (v6 version)



Mobile IP (v6 version)



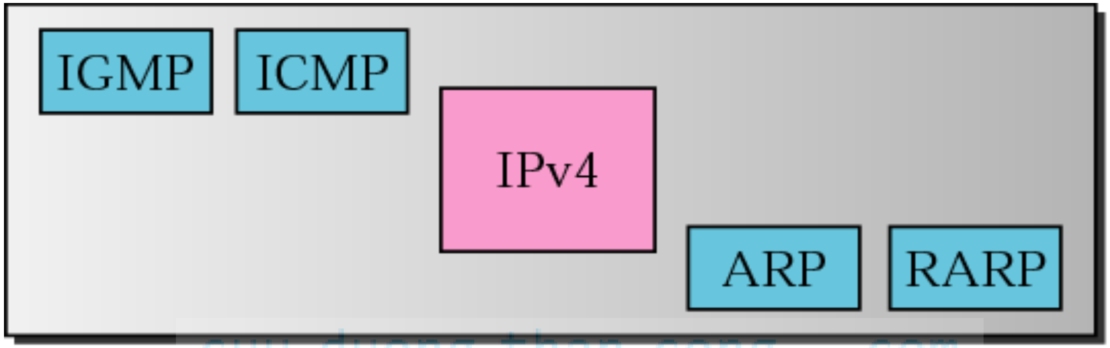
Mobile IP (v6 version)



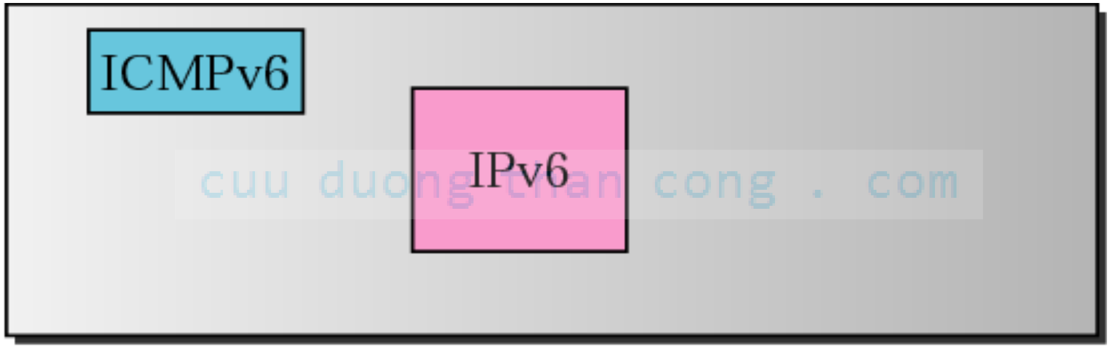
Routing in IPv6

- As in IPv4, IPv6 has 2 families of routing protocols: IGP and EGP, and still uses the longest-prefix match routing algorithm
- IGP
  - RIPng (RFC 2080)
  - Cisco EIGRP for IPv6
  - OSPFv3 (RFC 2740)
  - Integrated IS-ISv6 (draft-ietf-isis-ipv6-02)
- EGP : MP-BGP4 (RFC 2858 and RFC 2545)
- Cisco IOS supports all of them
  - Pick one meeting your objectives

Network Layer in v4 & v6



Network layer in version 4

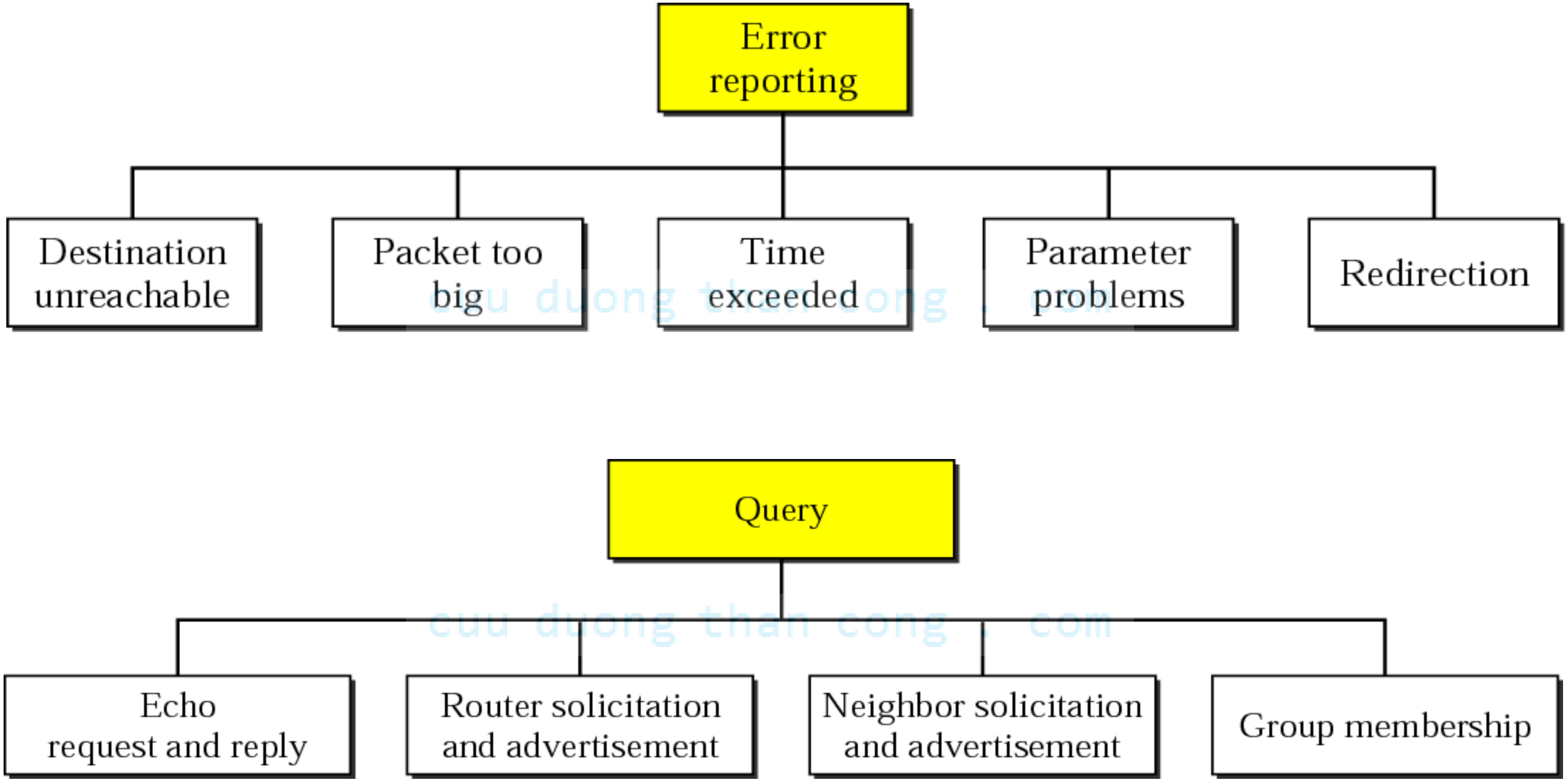


Network layer in version 6

ICMPv6

- An integral part of IPv6 and MUST be fully implement by every IPv6 node (RFC 2463)
- Next Header value= 58
- Report delivery or forwarding errors
- Provide simple echo service for troubleshooting
- Neighbor Discovery (ND): 5 ICMP messages
- Multicast Listener Discovery (MLD): 3 ICMP messages

ICMPv6 Messages



Neighbor Discovery (ND)

- Node (Hosts and Routers) use ND to determinate the link-layer addresses for neighbors known to reside on attached links and quick purge cached valued that become invalid
- Hosts also use ND to find neighboring router that 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
- Replace ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4

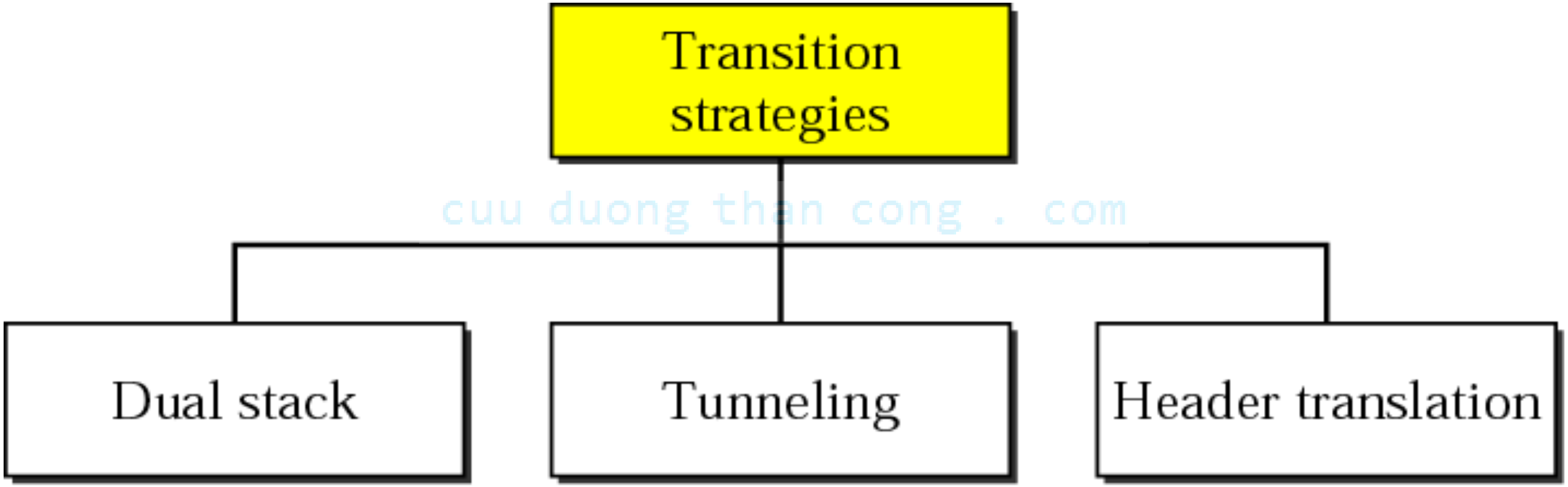
IPv6 ND Mechanisms (1)

- Router discovery
  - Equivalent to ICMPv4 Router Discovery
- Prefix discovery
  - Equivalent to ICMPv4 Address Mask Request/Reply
- Parameter discovery
  - Discovery additional parameter (ex. link MTU, default hop limit for outgoing packet)
- Address auto-configuration
  - Configure IP address for interfaces
- Address resolution: Equivalent to ARP in IPv4

IPv6 ND Mechanisms (2)

- Next-hop determination
  - Destination address, or
  - Address of an on-link default router
- Neighbor unreachable detection (NUD)
- Duplicate address detection (DAD)
  - Determine that an address considered for use is not already in use by a neighboring node
- First-hop Redirect function
  - Inform a host of a better first-hop IPv6 address to reach a destination,
  - Equivalent to ICMPv4 Redirect

Transition from IPv4 to IPv6



Advantages of IPv6 over IPv4 (1)

Feature	IPv4	IPv6
Source and destination address	32 bits	128 bits
IPSec	Optional	required
Payload ID for QoS in the header	No identification	Using Flow label field
Fragmentation	Both router and the sending hosts	Only supported at the sending hosts
Header checksum	included	Not included
Resolve IP address to a link layer address	broadcast ARP request	Multicast Neighbor Solicitation message

Advantages of IPv6 over IPv4 (2)

Feature	IPv4	IPv6
Determine the address of the best default gateway	ICMP Router Discovery(optional)	ICMPv6 Router Solicitation and Router Advertisement (required)
Send traffic to all nodes on a subnet	Broadcast	Link-local scope all-nodes multicast address
Configure address	Manually or DHCP	Autoconfiguration
Manage local subnet group membership	(IGMP)	Multicast Listener Discovery (MLD)

IPv6 References

- RFC 2460: IPv6
- RFC 2461: Neighbor Discovery
- RFC 2462: Stateless Address Autoconfiguration
- RFC 3513: Addressing Architecture
- RFC 3679: Flow Label Specification
- RFC 4443: ICMPv6
- RFC 3810: Multicast Listener Discovery (MLDv2)

Hỏi & Đáp