INSTITUTE FOR
NETWORKED SOLUTIONS

Computernetze Lab

IPv6

Version 2.0
February 16, 2021
Institute for Networked Solutions

Revision History

Revision	Date	Author(s)	Description
1.0	15.05.2019	Illi Dominique	created document
1.1	16.05.2019	Illi Dominique	fixed spaces and flag description of mutlicast addresses
1.2	23.05.2019	Illi Dominique	fixed lab exercice 2.2
1.3	06.09.2019	Assuncao Myriam	additional material for security part, AH and ESP
1.4	27.01.2020	Erb Manuela	English review
1.5	30.01.2020	Philip Schmid	Update regarding the provided infrastructure
1.6	12.02.2020	Severin & Yannick	Lab: changes in exercises
1.7	19.02.2020	Yannick	Lab 1.4.2: added commands (help); Lab: 1.4.3: added portfast command to client ports; Lab: 1.5.2: added interface disable and re-enable instruction; Lab Exercise 1.15: added commands to troubleshoot; Lab: 2.1: added `accept-ra: false` to the DHCP server netplan IP configuration; Lab Exercise 2.7: added hint
1.8	29.12.2020	sebastian	Typography
2.0	26.1.2021	sebastian	Adapted for back part of the lab and enable to solve it from home.

Lab Rules

The European Credit Transfer System (ECTS) demands verification of learned knowledge within modules. Knowledge is verified using by taking the appropriate exams. As from spring semester 2010, the following lab rules apply to the computer network lab module:

Prestudy

As a preparation to this lab, you have to read all the lab associated documents and solve the exercises called prestudy before your assigned lab time begins. Send the solved prestudy to ins-abgabe@ost.ch at the latest by midnight before your lab starts. Without reading the documents or solving any prestudy exercises, you will not be able to pass the lab session within the given time. Assistants are instructed to dismiss any unprepared students.

Lab Attestation

To receive the attestation for a lab experiment, you must fulfill the following requirements:

- Study all material and solve all prestudy questions prior to the lab.
- During the lab session, you will elaborate all lab exercises with your partner. Our tutors will help you whenever you experience problems. However, before consulting the tutors think about the problems you face with the lab exercises, make use of your own CPU cycles and then start a discussion with your partner or ask your neighboring. will learn much more by finding the solution by yourself.
- Please clean up your desk which also includes cables, equipment, papers, etc. and do not forget to erase your configurations from all the devices such as routers and switches.
- Before leaving, discuss your lab results with your tutor. If you have successfully proved your knowledge, the lab is completed. In case you cannot finish the lab due to incomplete or inaccurate preparation, you fail your lab exercise and it will not count for the lab attestation.

Contents

Part I.

Prestudy

1. Introduction

1.1. IPv6 Overview

IPv6 is the latest revision of the Internet Protocol (IP), succeeding IPv4. It was standardized in 1998 by the Internet Engineering Task Force (IETF9) due to scarcity of IPv4 addresses. Hence, the size of the addresses was extended to 128 bits resulting in 340 sextillion ($3.4 * 10^{38}$) possible IPv6 addresses. The Internet Assigned Numbers Authority (IANA), responsible for the global coordination of IP addresses, assigned the last 8 address ranges to the Regional Internet Registrar (RIR) on 3 February 2011. A RIR is an organization that manages the allocation and registration of Internet number resources within a particular region of the world. The IPv4 address pool of APNIC, representing the RIR of Asia, ran out in April 2011. Even RIPE, which is the RIR of Europe, is no longer in a position to allocate any IPv4 addresses. As a consequence, new customers do not receive any IPv4 addresses anymore. In the first instance, it does not seem to be a matter of great concern. However, bear in mind that a customer who is only allocated IPv6 addresses, but who wants to access IPv4 services (e.g. NAT64 which is not part of this document though), must go through complex and expensive implementation procedures. A company which is cut off from the IPv6 network is not able to reach an increasing number of potential customers, especially in 2nd and 3rd world countries such as Asia and Africa.

2. Packet Header

The Packet Header of IPv6 has a fixed size of 40 bytes. Only relevant fields have been implemented. Rarely used information is placed in so-called Extension Headers and embedded before the payload. Headers are designed to process a multitude of 64 bits. Therefore, the memory access of the router is much faster.

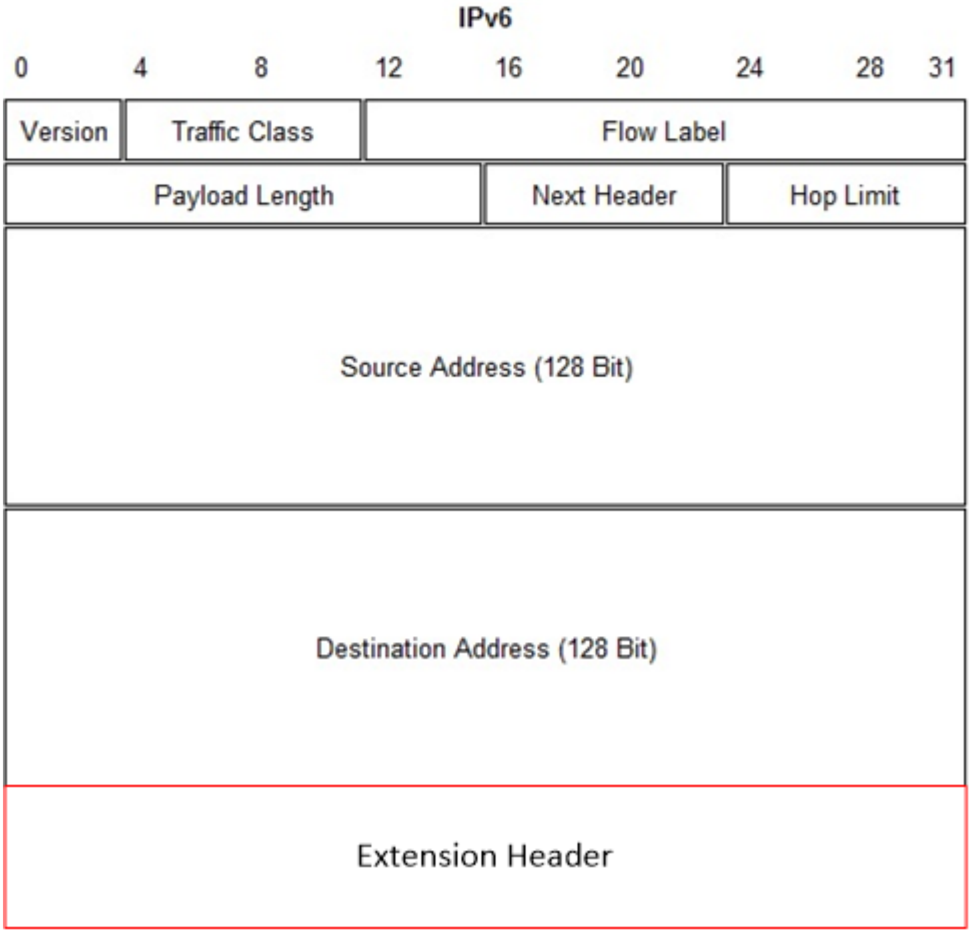


Figure 2.1.: IPv6 Header

IPv6 does not use checksums anymore. It only performs error corrections on the OSI Layers 2 and 4. The error rate of today‘s transmission media is 10^{-12} and thus very small. Therefore, error correction on OSI Layer 3 is not necessary and the router must not calculate the checksum for each packet. This saves CPU power. The single fields displayed in the Header have the following meanings:

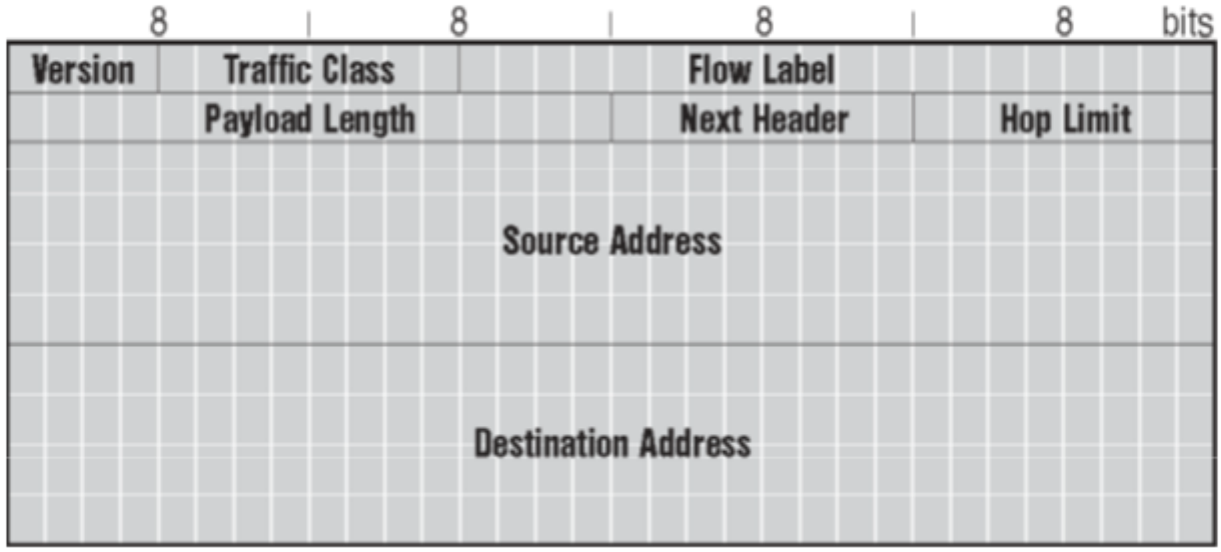
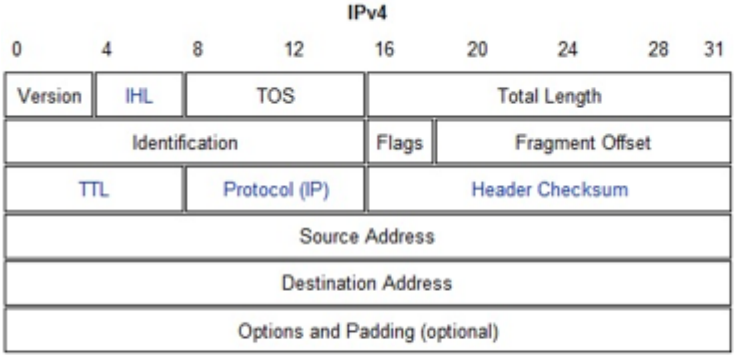


Figure 2.2.: IPv6 Header

- Version: 4bits. The value of this field indicates which IP-version is used (IPv4 or IPv6).
- Traffic Class 8 bits: This value is used to specify the Quality of Service (QoS). IETF established a standard for the Differentiated Service and published it under RFC 2474.
- Flow Label 20 bits: This field specifies the packet flow. Usually, packets have a flow label with value Null. If the value is unequal to Null, each router in a path can be sent a specific QoS requirement for the corresponding flow. It is still an experimental field. For real-time applications, however, it can be very interesting.
- Payload Length 16 bits: indicates the length of payload, including the Extension Header. The value is specified in bytes which implicates a maximum payload of 64 kbytes.
- Next Header 8 bits: defines the type of subsequent Headers. It can either represent the protocol of the higher OSI layers or an Extension Header. In the next chapter, Extension Headers are described in more detail.
- Hop Limit 8 bits: defines the lifetime of the packets. Each router decrements this value by 1. If the value reaches Zero, the packet will be dropped and an ICMP message (time exceeded) will be sent to the sender.
- Source Address 128 bits: represents the source IPv6 address.
- Destination Address 128 bits: represents the destination IPv6 address.

Below, you will find an IPv4 Header for comparison purposes:



IPv4

0 4 8 12 16 20 24 28 31

Version	IHL	TOS	Total Length	
Identification			Flags	Fragment Offset
TTL		Protocol (IP)	Header Checksum	
Source Address				
Destination Address				
Options and Padding (optional)				

Figure 2.3.: IPv4 Header

3. Extension Header

Extension Headers are optional extensions which can be embedded into the IPv6 Header. As they are optional, a way had to be found to recognize them. For this purpose, the so-called Header Chaining was developed. There is a field called „Next Header“ which indicates the type of the subsequent Extension Header. Each Extension Header owns a field called „Next Header“ and can thereby refer to the next Header. Finally, the last one refers to the protocol of the higher OSI layer.

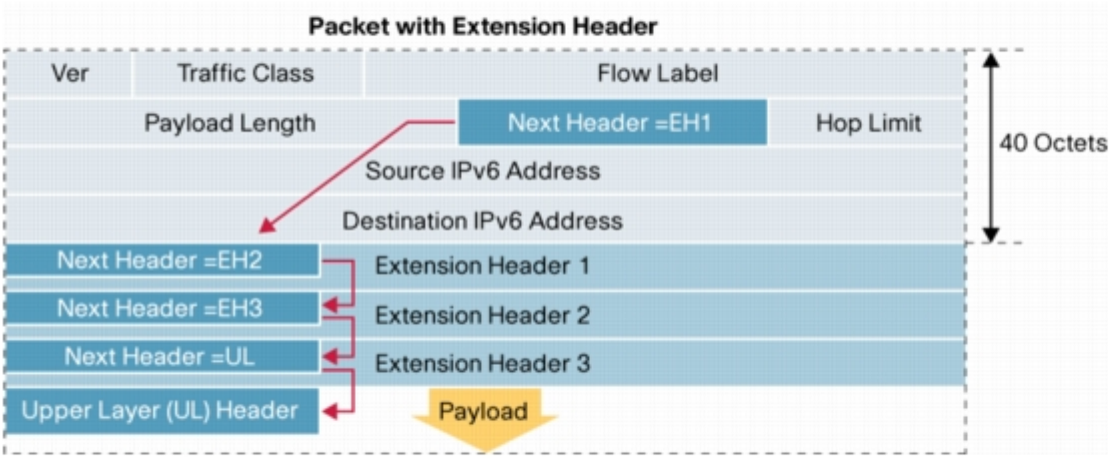


Figure 3.1.: Packet with Extension Header

If plenty of Extension Headers are used, a router must go through a long list which has a negative impact on the performance. To avoid such problems, the sequence of Headers is clearly defined. Extensions relevant for all routers (Hop-by-Hop Option Header) are listed at the beginning. Extensions relevant for the receiver (Destination Option Header) are listed further back. Hence, it may be possible that a router stops searching a list as soon as it has gathered the relevant information. Most of the packets can do without Extension Headers. In this case, the field called „Next Header“ is equally used as the field called „Protocol“ in IPv4. It defines the protocol on the transport layer.

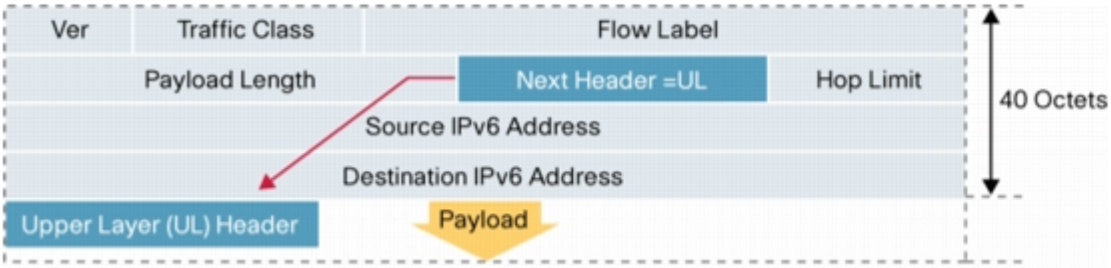


Figure 3.2.: Packet without Extension Header

An Extension Header represents one of the following types:

Value	Extension Header
0	Hop-by-hop option
43	Routing
44	Fragment
50	Encapsulating Security Payload (ESP)
51	Authentication Header (AH)
59	No next header
60	Destination Option
62	Mobility Header

3.1. Routing Extension Header

The Route Header has an influence on the path of packets. There are two different types of Routing Extension Headers: type 0 and type 2, indicated in an additional field within the Extension Headers. By means of type 0, a list of routers can be provided that a packet needs to pass. The first hop represents the destination and is entered in the regular Header. Any further hop is entered as sequence in the Routing Extension Header. The primary aim, however, is the last address in the Extension Header. The field „Segments Left“ indicates how many hops still have to be passed. If a packet reaches a hop, the subsequent address of the Extension Header is copied into the regular Header and the value of the field „Segments Left“ is decremented. If the value reaches Zero, the destination has been reached.

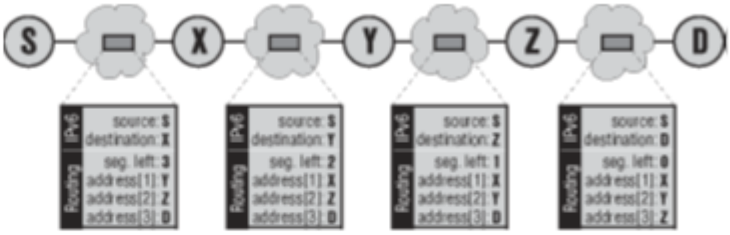


Figure 3.3.: Routing Extension Header

Type 2 is used for the mobility of a client. In the Extension Header, there is only one address listed. In Chapter „MobileIP“, this matter is examined in further detail.

3.2. Fragment Extension Header

A packet exceeding the Maximal Transmission Unit (MTU) needs to be fragmented before the transmission. Due to the fact that this procedure has a negative impact on the performance, fragmentation should be avoided, whenever possible. For IPv6, it was defined that each IPv6 node must detect the Path MTU for all of its routes. The Path MTU represents the smallest MTU on this path. So, the node sends a packet with „its“ MTU. If the node receives „ICMP Packet too big“, the MTU is reduced to the smallest value as the packet has simply been too big. In this case, the node sends a further packet with the new MTU. This procedure is being repeated until the destination is reached. As a matter of fact, only the sender is allowed to fragment a packet. A different router must reject the packet and send it back to the sender with the message „ICMP Packet too big“. Then, it adjusts the MTU. The minimal MTU must have 1280 bytes. This requirement ensures that a path will not be blocked by a MTU which is too low. A path can be dynamic. This means that rerouting can be performed. Due to its dynamic, it may happen that packets are rejected even after a Path MTU Discovery. In this case, the Path MTU will have to be changed once again. A fragmented packet is divided into a fragmentable and unfragmentable part. The part which must not be fragmented consists of the Header and Extension Header.

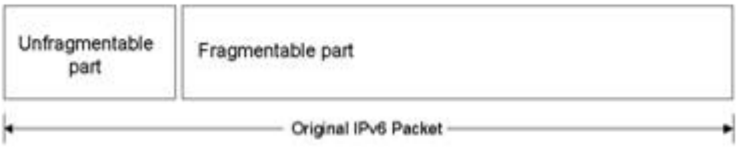


Figure 3.4.: Fragment Extension Header

The fragmentable part is splitted. An Extension Header called fragment is added to the Header which contains the following fields: an offset field with 13 bits, a field called “more Fragment Flag” and an identification field with 32 bits. The offset field specifies which part of the original packet consists of the fragment. Each fragment is flagged, except the last one. The identification number indicates which fragments belong to the same packet.

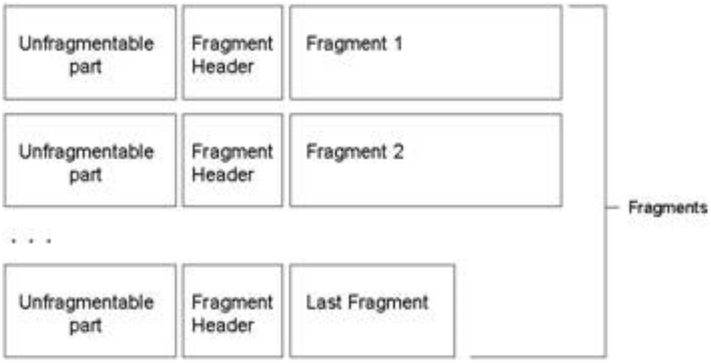


Figure 3.5.: Fragment Extension Header

3.3. Hop-by-Hop Option Headers

The Hop-by-Hop Option Headers are listed first in the Extension Header Chain. These Headers are relevant for all nodes within a path and can contain the following information:

Value	Type
0	Pad1
1	PadN
5	Router alert
194	Jumbo payload

- Pad1: With this field, maximum 8 bit may be inserted in order to align the Extension Header to an 8-bit limit.
- PadN: This field is used if more than 8 Padding bits have to be inserted.
- Router alert: This field can be used for alerting a router that a packet needs further processing. For instance, this field is used by RSVP.
- Jumbo payload: This field indicates if a packet exceeds 64 kB. Thus, it is possible to transmit packets up to 4 GB.

4. Address Format

An IPv6 address with 128 bits is four times as long as an IPv4 address. To display the address in a compact way, the hexadecimal and not the decimal number system is applied. The so-called Quad nibbles (also 16 bits) are separated by a colon. To avoid displaying the whole number of 32 hexadecimal characters for each address, the leading zeros can be omitted. Once per address, it is also possible to substitute the consecutive zeros by two colons, a so-called double colon. This is an example of a complete IPv6 address: `2001:0718:1c01:0016:020d:56ff:fe77:52a3` This version omits the leading zeros. `2001:718:1c01:16:20d:56ff:fe77:52a3` The following example shows the possible use of a double colon: `0:0:0:0:0:0:0:1` becomes `::1`

Prestudy Exercise 4.1

Write the following IPv6 address in a shorter format: `2001:0620:0000:0000:0B0A:0000:0000:C0AB`

Prestudy Exercise 4.2

Write down the prefix of the IPv6 default route.

A further change includes the removal of broadcast addresses. The multicast addresses take on their function. For this purpose, a new address type was introduced: the so-called anycast addresses. Below, the different address groups are examined in more detail.

4.1. Unicast Address

The unicast address represents the most important address type. This address is used for the communication with exactly one terminal, analogous to IPv4. A unicast address consists of a global routing prefix, a subnet ID and an interface ID:

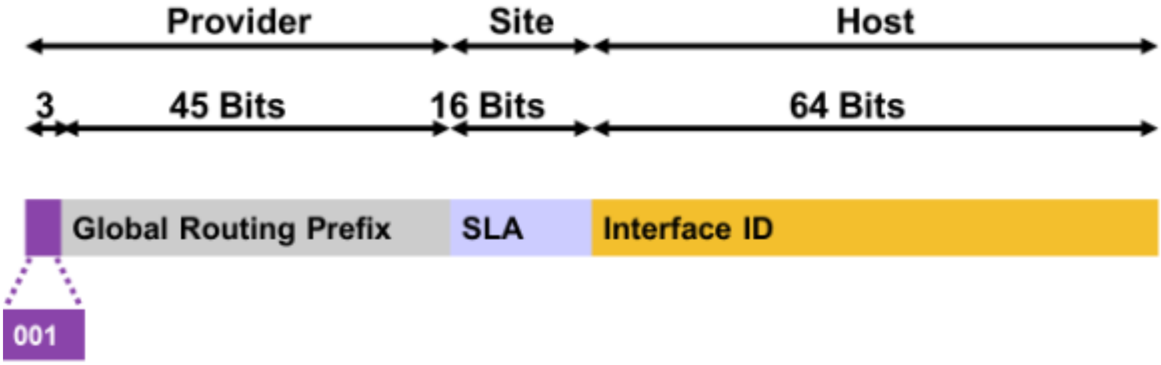


Figure 4.1.: IPv6 Unicast Address

The prefix defines the network which contains the unicast address. The subnet ID is used for the identification of the subnet, analogous to IPv4. The last 64 bits assign the host address. They may be assigned in several different ways:

- Auto-configured from a 48-bit MAC address (called EUI-64)
- Auto-generated pseudo-random number (to address privacy concerns)
- Assigned via DHCP
- Manually configured

Prestudy Exercise 4.3

What is the IPv6 Global Routing Prefix for HSR?

4.1.1. Subnetting

The subnetting process is slightly different (but easier) as in the IPv4 world. Take the HSR routing prefix and define subnets for the following networks:

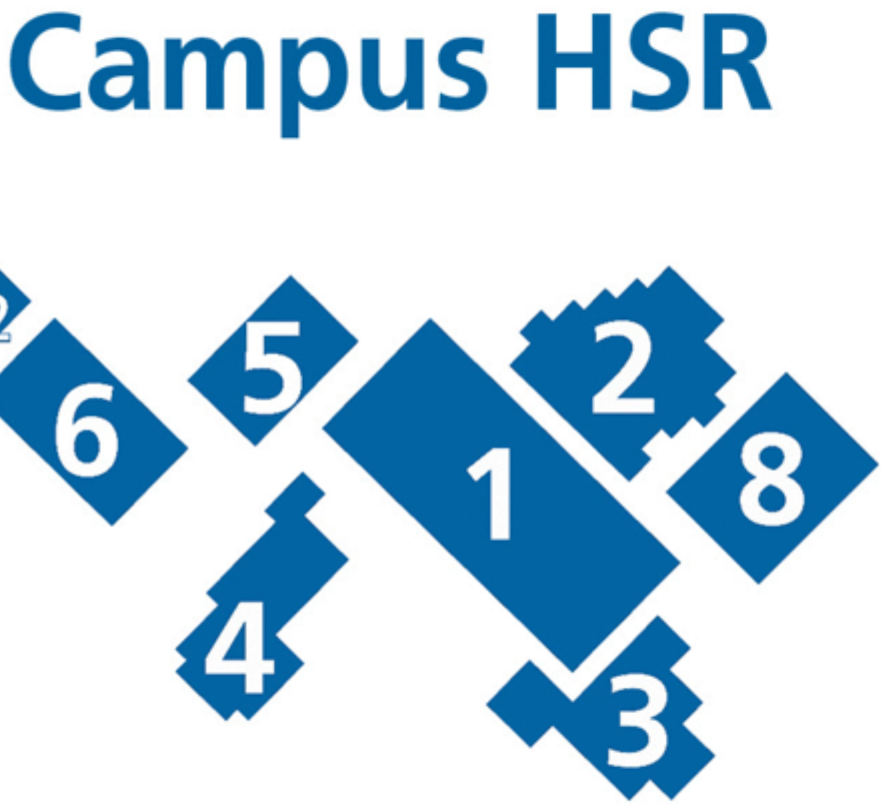


Figure 4.2.: Campus HSR

Each Building should get a subnet for the notebook network, the student network and the teacher network. In addition, there is a campus wide network administration network.

Prestudy Exercise 4.4

Define the IPv6 subnets' address for above networks. Try to use an "easy to remember" systematic approach.

4.1.2. EUI-64

EUI-64 represents an address format that supports a network device to generate an IPv6 address. To generate such an address, the MAC address of the interface is used and extended to 64 bits. The MAC address is divided between the third and the fourth bytes and 0xFFFE is integrated into the address. 48 bits of the MAC address are extended to 64 bits. Finally, the 7th most significant bit is inverted.

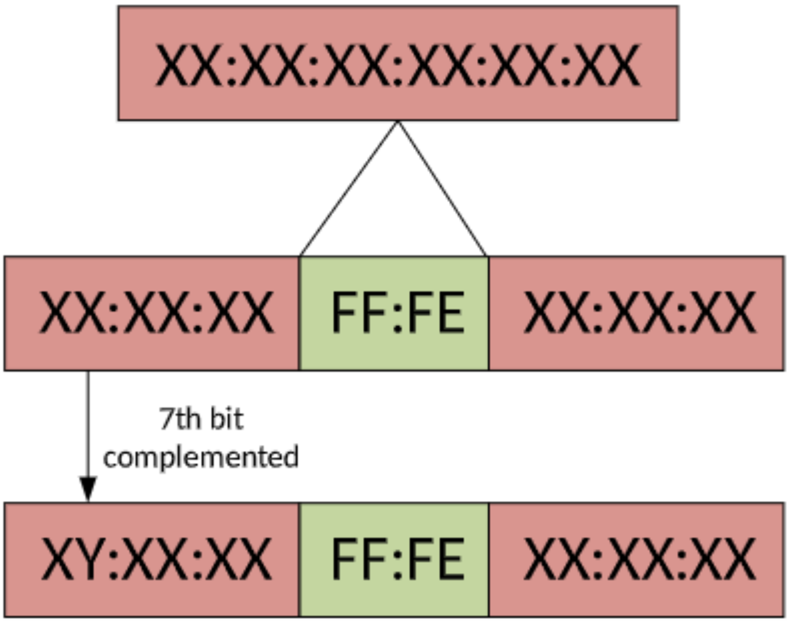


Figure 4.3.: EUI-64

As the MAC address is globally unique, the client can be identified anywhere in the world. Data protectors criticize that this circumstance may be misused for marketing purposes. As a result, the so-called privacy extension was introduced. Refer to Chapter Privacy Extension for detailed information.

Prestudy Exercise 4.5

Calculate the EUI-64 address with the following specifications:

- Prefix `2001:620:130::/44`
- Last subnet
- MAC address of the client: 00:19:99:91:1F:BD

4.1.3. Privacy Extension

Because a client with a EUI-64 address is clearly identifiable worldwide, privacy extension was standardized by RFC 4941. Hence, an additional IPv6 address can be generated for each interface. The IPv6 address is used for the communication in the internet. The Randomizer periodically generates a new address to avoid that a client can be identified by an IPv6 address. Therefore, companies that want to assign a specific profile to a client for marketing purposes, use other means. For example, a web browser can be recognized by the browser's ACCEPT Headers, user agent, installed plugins and cookie acceptance. Privacy extension, however, can cause problems. Troubleshooting gets complicated because the IPv6 address periodically changes. Entries in the reverse DNS must be updated more often. Access permissions cannot be set up based on an IP address. Finally, privacy extension facilitates address spoofing. BrowserFingerprint

Prestudy Exercise 4.6

Go to https://panopticlick.eff.org/ and test if your browser is unique. Is it unique? Which data was tested?

4.1.4. Randomizer

The Randomizer generates a random IPv6 address. In contrast to privacy extension, there is no additional address generated.

4.2. Multicast Address

A multicast address starts with the prefix `ff00::/8` and is mainly used for video and audio traffic. A multicast address has the following format:

8 Bit	4 Bit	4 Bit	112 Bit
FF	Flags	Scope	Group ID

The values of the flags are:

X	R	P	T

The most significant bit is reserved for future use. The significance of the other three bits will be examined at a later stage.

Bit	Flag	0	1
R	Rendezvous	The address of the Rendezvous Point is not integrated in the multicast address.	The address of the Rendezvous Point is integrated in the multicast address.
P	Prefix	Indicates a multicast address that is not assigned based on the network prefix.	Indicates a multicast address that is assigned based on the network prefix.
T	Transient	When T flag is set to 0, the multicast address is a permanently assigned (well-known) multicast IPv6 address.	When T flag is set to 1, the multicast address is a transient (dynamically assigned) multicast address.

The picture below describes how an IPv6 address of a Rendezvous Point is included in a IPv6 multicast address. The flags are set to 0111. This means that the Network Prefix defines the IPv6 address of the Rendezvous Point and the multicast address is static. With the “Network Prefix” and the “RPadr” field, the address of the Rendezvous Point can be calculated.

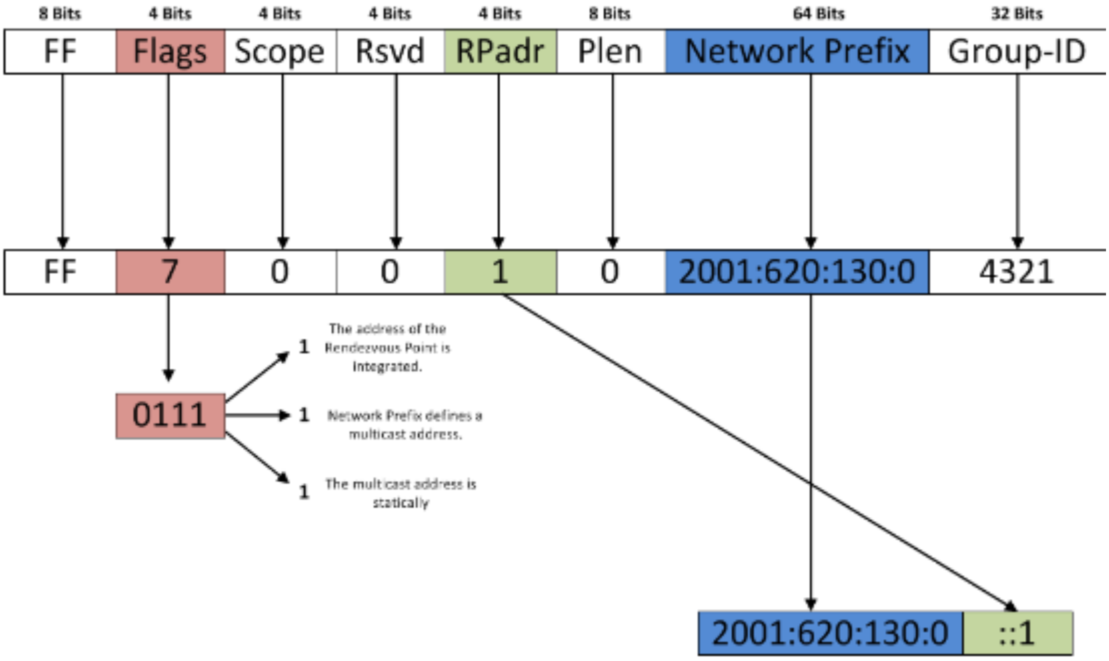


Figure 4.4.: Calculation of the Rendezvous Point IPv6 Address

The “scope” field is defined in the table below:

Scope field value	Scope
1	Node-local
2	Link-local
5	Site-local
8	Organization-local
E	Global

The advantage of the above mentioned method is that the administrator only has to configure the multicast address.

Prestudy Exercise 4.7

Calculate the IPv6 address of the Rendezvous Point. The multicast address that you have is: `FF75:B40:2001:DB8:BEEF:FEED::/96`

Bear in mind that some of the multicast addresses are reserved. They must not be configured manually. The table below shows a few of these addresses.

Multicast Address	Description
FF02::1	"All nodes" multicast address like the broadcast address in IPv4
FF02::2	All routers have to join this multicast group
FF02::5	Used by OSPFv6 to flood data to all OSPFv6 router
FF02::6	Used by OSPFv6 to send data to the DRs
FF02::D	All PIM enabled routers have to join this multicast group

4.2.1. Solicited-Node Multicast Address

A solicited-node multicast address is only valid in the local link. In other words, it is only intended for use in an Ethernet segment or a Frame Relay Cloud. Each IPv6-enabled device has a solicited-node multicast address per interface. It is generated by appending the last 24 bits of the IP address to a standardized the prefix. `ff02:0:0:0:0:1:ff00::/104`.

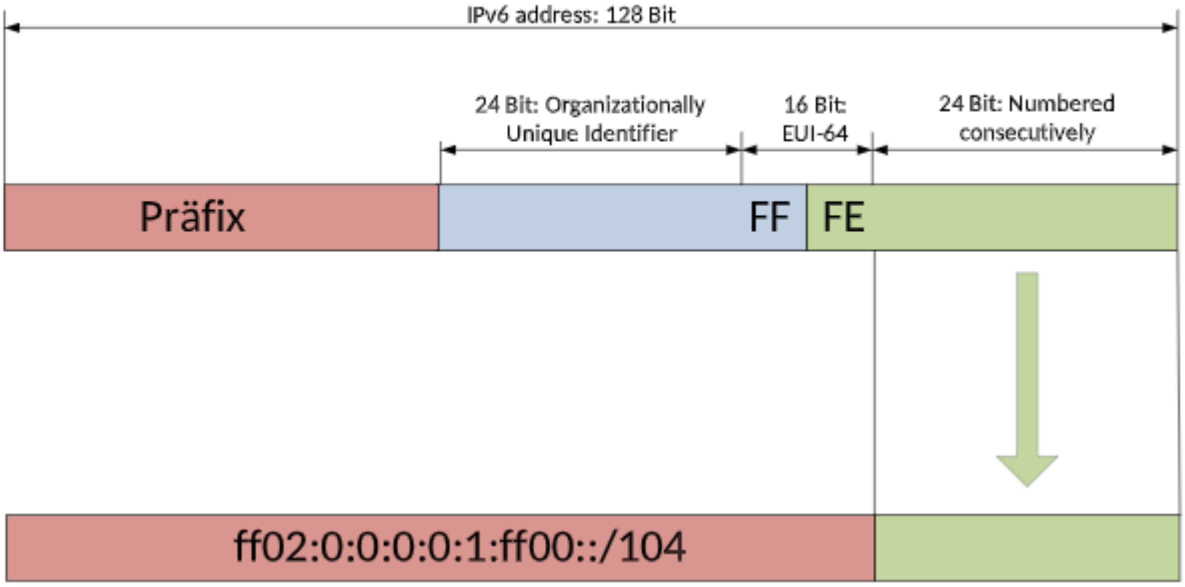

IPv6 address: 128 Bit
24 Bit: Organizationally Unique Identifier
16 Bit: EUI-64
24 Bit: Numbered consecutively
Präfix
FF
FE
ff02:0:0:0:0:1:ff00::/104

Figure 4.5.: Solicited-Node Multicast Address

Prestudy Exercise 4.8

Calculate the solicited-node multicast address for the following IPv6 address: `2001:620:130:ABCD:1234:5678:9ABC:A`

4.2.2. Anycast Address

With the anycast address, a packet can be sent to the „next“ destination. For this purpose, several nodes are formed to a group. All devices receive the same IPv6 address. The anycast address is distributed on different paths within the network. Afterwards, the client is forwarded to the „next“ node.

Prestudy Exercise 4.9

Which technical solution is responsible for finding the next destination?

5. Address Allocation

5.1. SLAAC

When using Stateless Address Autoconfiguration, the client first calculates a link-local address based on its MAC address. The 48 bit MAC address is extended to 64 bits on the basis of EUI-64. After the address has been checked for uniqueness in the network, it can be assigned to the interface. The client then sends a router solicitation packet to all routers in the network. If the client gets a response by a router advertisement, a globally valid address can be calculated with the prefix of the RA (Router Advertisement). This is done based on EUI-64. Even the globally valid address must first be checked for uniqueness. The client uses the source address of the RA as default gateway.

Prestudy Exercise 5.1

Calculate the globally unique IPv6 address with the following specifications:

- Prefix from the Router Advertisement: `2001:620:130:FFFF::/64`
- MAC address of the client: `00:AB:CD:EF:01:23`

5.2. Stateless Autoconfiguration and Stateless DHCP

In the router advertisements, the “Other-Bit” is set in a Header field. The client calculates an IPv6 address based on EUI-64. The address is checked for uniqueness by means of duplicated address detection. Afterwards, the DHCP server is queried for a DNS server. The DHCP Server sends the IPv6 address of a DNS server back to the client. The first idea was that a DHCP server should no longer be needed with IPv6. Yet, it was not taken into consideration or “forgotten” to specify a way in order to reach a DNS server. Well, stateless auto configuration and stateless DHCP is a possible solution. In practice, however, this is rather irrelevant.

5.3. Stateful Autoconfiguration

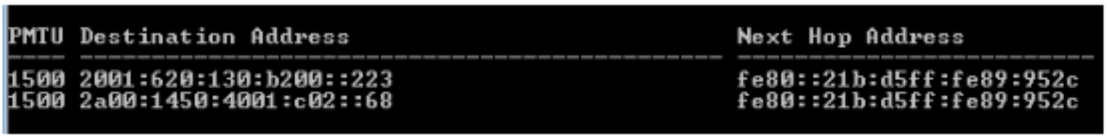
A client tries to obtain an IPv6 address of a DHCP server if the router advertisements fail to appear or the “Managed-Bit” is set. Each DHCPv6 server is member of two multicast groups: `FF02::1:2` is used for the communication between Relay Agents or DHCPv6 servers. `FF05::1:3` is used by a Relay Agent in order to communicate with a DHCPv6 server with an unknown unicast address. This is the most used variant in a practical network.

Prestudy Exercise 5.2

Why is this the most common variant in practice? What do you think?

6. ICMPv6

The neighbor list stores addresses of neighboring devices that exchanged data in the same network. For each IPv6 address, the link layer address is listed respectively. The destination list stores addresses of devices to which data were sent. On-link addresses are located in the same network, off-link addresses in different networks. The next hop is displayed in the neighbor list by a link. The path-MTU is also stored. The destination list is kept up-to-date by means of ICMP Redirection.



```
PMTU Destination Address                          Next Hop Address
---- -------------------------------------------  ---------------------------
1500 2001:620:130:b200::223                       fe80::21b:d5ff:fe89:952c
1500 2a00:1450:4001:c02::68                       fe80::21b:d5ff:fe89:952c
```

Figure 6.1.: Neighbor List

The prefix list is generated by the router advertisements. It only stores on-link addresses. Each entry has an Invalid Timer which is extracted from the router advertisement. The timer deletes expired entries and the value can be set on infinity. An ICMP packet is indicated with the value 58 in the field Next Header. The packet is listed after the Extension Header(s) - like a transport layer protocol.

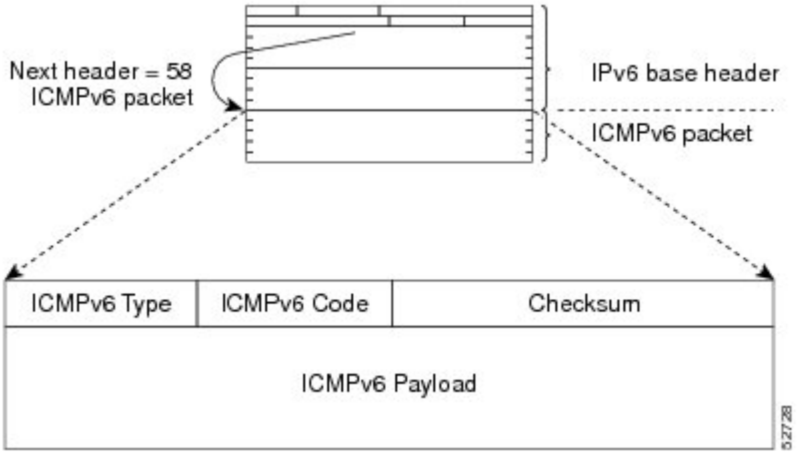


Figure 6.2.: ICMPv6 Header

6.1. IPv6 Ping

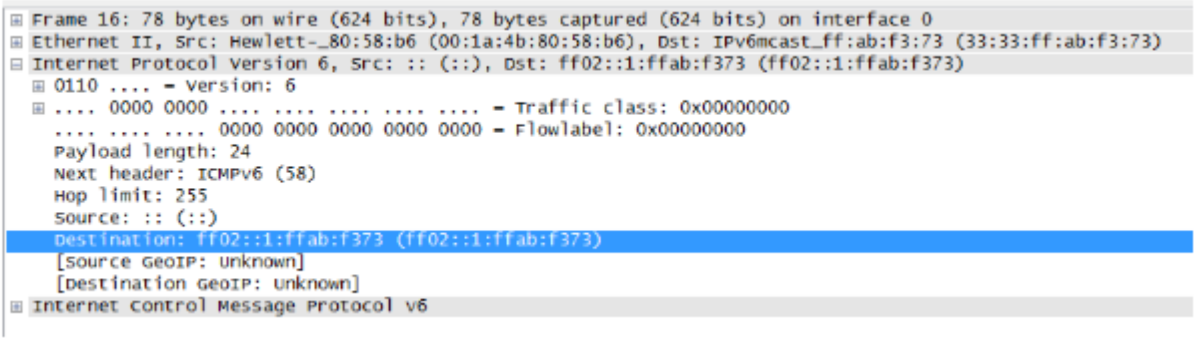
In order to test the IPv6 connectivity, you can use the ICMPv6 echo requests. This is similar to ICMPv4. On a Windows computer, you must use the command `ping -6 <ipv6 address>` On a Linux computer, you have to specify the interface on which you like to send the ICMPv6 echo requests. `ping6 -I <interface> <ipv6 address>`. On a Mac, you can use the same command as for Linux. An other useful tool for troubleshooting is Traceroute. Of course, this tool is also available for IPv6. The command on a Windows computer is: `tracert -6 <ipv6 address>` On Linux, use the command: `traceroute6 <ipv6 address>`

Prestudy Exercise 6.1

Try out these commands if your network environment supports IPv6. Which IPv6 addresses did you ping?

6.2. Duplicated Address Detection

In order to determine whether a generated IPv6 address has been previously used, the duplicated address detection is performed before the IPv6 address is assigned to an interface. The IPv6 address is temporarily flagged and a neighbor solicitation message is sent to its own solicited-node multicast address. Each device must join the corresponding solicited-node multicast address for each IPv6 address. Each node receives this message with the same IPv6 address and can respond to it. The solicited node multicast address consists of the prefix `ff02::1:ff00:0000/104` and the last 24 bits of the IPv6 address.



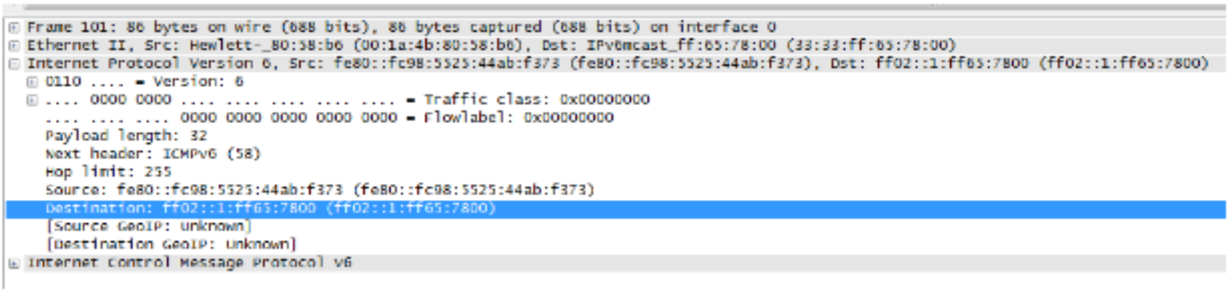
```
⊞ Frame 16: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
⊞ Ethernet II, Src: Hewlett-_80:58:b6 (00:1a:4b:80:58:b6), Dst: IPv6mcast_ff:ab:f3:73 (33:33:ff:ab:f3:73)
⊟ Internet Protocol Version 6, Src: :: (::), Dst: ff02::1:ffab:f373 (ff02::1:ffab:f373)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 24
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: :: (::)
    Destination: ff02::1:ffab:f373 (ff02::1:ffab:f373)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol v6
```

Figure 6.3.: Solicited Node Multicast - DAD

The sending node awaits the RETRANSMIT_TIMER before an address is defined to be unique. This procedure, however, is not secure because a neighbor solicitation packet can be lost. It is therefore possible that a neighbor solicitation message is transmitted several times. The variable DUP_ADDR_DETECT_TRANSMITS indicates such incidents. So, the chances are that a packet reaches its destination. By default, the value is set to 1. If the neighbor solicitation message is the first packet sent via the link, an additional delay is included in the process. The delay is randomly selected and takes up to one second. This process is performed to avoid an overflow if several nodes are simultaneously active on the link. This may occur after a power outage. In the worst case, the IPv6 address can only be assigned to the interface with a delay of 2 seconds (RETRANS_TIMER + MAX_RTR_SOLICITATION_DELAY). If a neighbor advertisement is transmitted, the address is already being used. Either a new address needs to be generated or the user configures a new one.

6.3. Neighbor Solicitation

Neigbor solicitation messages are used to discover the link-local address of an IPv6 node. These messages are comparable to ARP in IPv4. The IPv6 address of the interface is entered as source address, the solicited node multicast address as destination address. The receiver returns the link-local address.

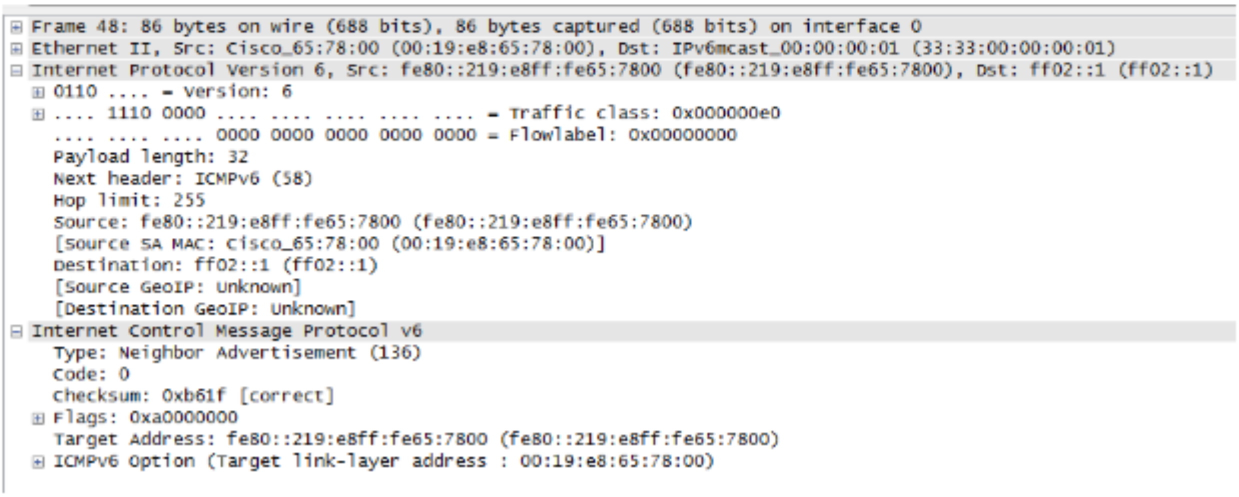


```
⊞ Frame 101: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
⊞ Ethernet II, Src: Hewlett-_80:58:b6 (00:1a:4b:80:58:b6), Dst: IPv6mcast_ff:65:78:00 (33:33:ff:65:78:00)
⊟ Internet Protocol Version 6, Src: fe80::fc98:5525:44ab:f373 (fe80::fc98:5525:44ab:f373), Dst: ff02::1:ff65:7800 (ff02::1:ff65:7800)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 32
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::fc98:5525:44ab:f373 (fe80::fc98:5525:44ab:f373)
    Destination: ff02::1:ff65:7800 (ff02::1:ff65:7800)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol v6
```

Figure 6.4.: Neighbor Solicitation Message

6.4. Neighbor Advertisement

If a network device receives a neighbor solicitation message, it returns a neighbor advertisement. A neighbor advertisement is an ICMPv6 packet of type 136. It contains the IPv6 address and the link-layer address of the sender. The destination address represents the IPv6 address of the network device sending neighbor solicitation messages.

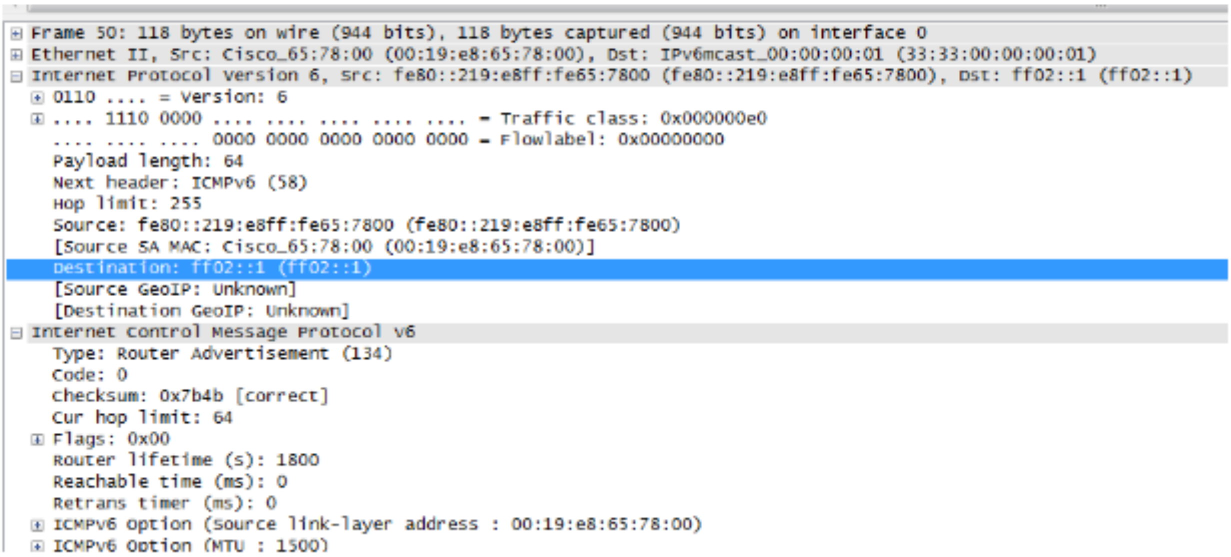


```
⊞ Frame 48: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
⊞ Ethernet II, Src: Cisco_65:78:00 (00:19:e8:65:78:00), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
⊟ Internet Protocol Version 6, Src: fe80::219:e8ff:fe65:7800 (fe80::219:e8ff:fe65:7800), Dst: ff02::1 (ff02::1)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 32
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::219:e8ff:fe65:7800 (fe80::219:e8ff:fe65:7800)
    [Source SA MAC: Cisco_65:78:00 (00:19:e8:65:78:00)]
    Destination: ff02::1 (ff02::1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0xb61f [correct]
  ⊞ Flags: 0xa0000000
    Target Address: fe80::219:e8ff:fe65:7800 (fe80::219:e8ff:fe65:7800)
  ⊞ ICMPv6 Option (Target link-layer address : 00:19:e8:65:78:00)
```

Figure 6.5.: Neighbor Advertisement

6.5. Router Advertisement

Router advertisements are sent to the all-nodes multicast address at given intervals. Only routers and firewalls can transmit these ICMPv6 packets of type 134. The router advertisements contain the prefix that a router is responsible for.

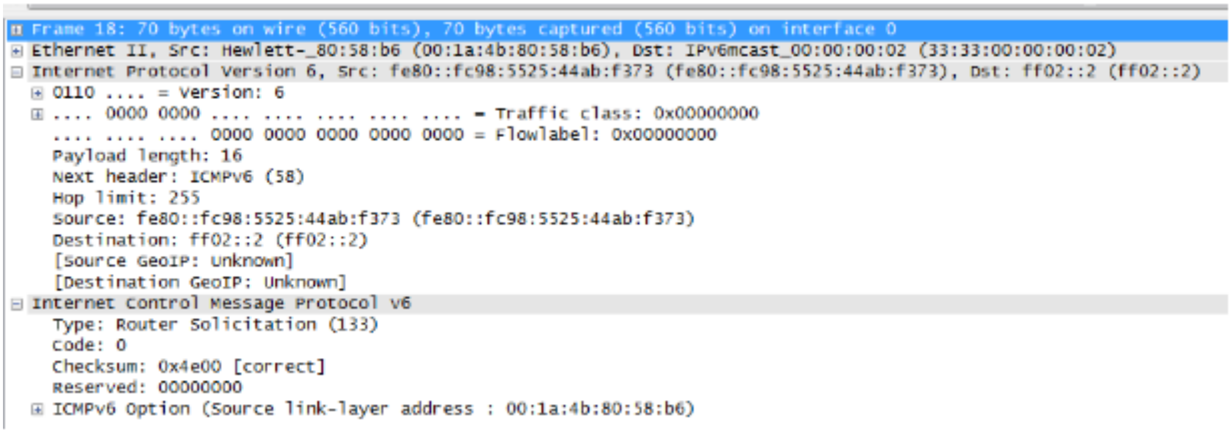


```
⊞ Frame 50: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
⊞ Ethernet II, Src: Cisco_65:78:00 (00:19:e8:65:78:00), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
⊟ Internet Protocol Version 6, Src: fe80::219:e8ff:fe65:7800 (fe80::219:e8ff:fe65:7800), Dst: ff02::1 (ff02::1)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 64
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::219:e8ff:fe65:7800 (fe80::219:e8ff:fe65:7800)
    [Source SA MAC: Cisco_65:78:00 (00:19:e8:65:78:00)]
    Destination: ff02::1 (ff02::1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x7b4b [correct]
    Cur hop limit: 64
  ⊞ Flags: 0x00
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ⊞ ICMPv6 Option (Source link-layer address : 00:19:e8:65:78:00)
  ⊞ ICMPv6 Option (MTU : 1500)
```

Figure 6.6.: Router Advertisement

6.6. Router Solicitation

When starting the system, the client sends a router solicitation to the all-routers multicast address. In response to this, the router responds with a router advertisement message which allows the client to generate an IPv6 address inside the router's prefix. The source address used is: `0:0:0:0:0:0:0:0`.



```
⊞ Frame 18: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
⊞ Ethernet II, Src: Hewlett-_80:58:b6 (00:1a:4b:80:58:b6), Dst: IPv6mcast_00:00:00:02 (33:33:00:00:00:02)
⊟ Internet Protocol Version 6, Src: fe80::fc98:5525:44ab:f373 (fe80::fc98:5525:44ab:f373), Dst: ff02::2 (ff02::2)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 16
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::fc98:5525:44ab:f373 (fe80::fc98:5525:44ab:f373)
    Destination: ff02::2 (ff02::2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol v6
    Type: Router Solicitation (133)
    Code: 0
    Checksum: 0x4e00 [correct]
    Reserved: 00000000
  ⊞ ICMPv6 Option (Source link-layer address : 00:1a:4b:80:58:b6)
```

Figure 6.7.: Router solicitation

6.7. Redirect

An ICMP Redirect message is used if packets have the option of a better First Hop. This may occur if several routers are available in a network which send router advertisements. Each router is added to the prefix list by the client. The router on the top of the list is used as default router. In case a router is used as default gateway, but proves to be suboptimal, it simply conveys the packet to the correct router. Additionally, an ICMP Redirect is transmitted to the client. The client adjusts the prefix list and sends the subsequent packets to the correct router.

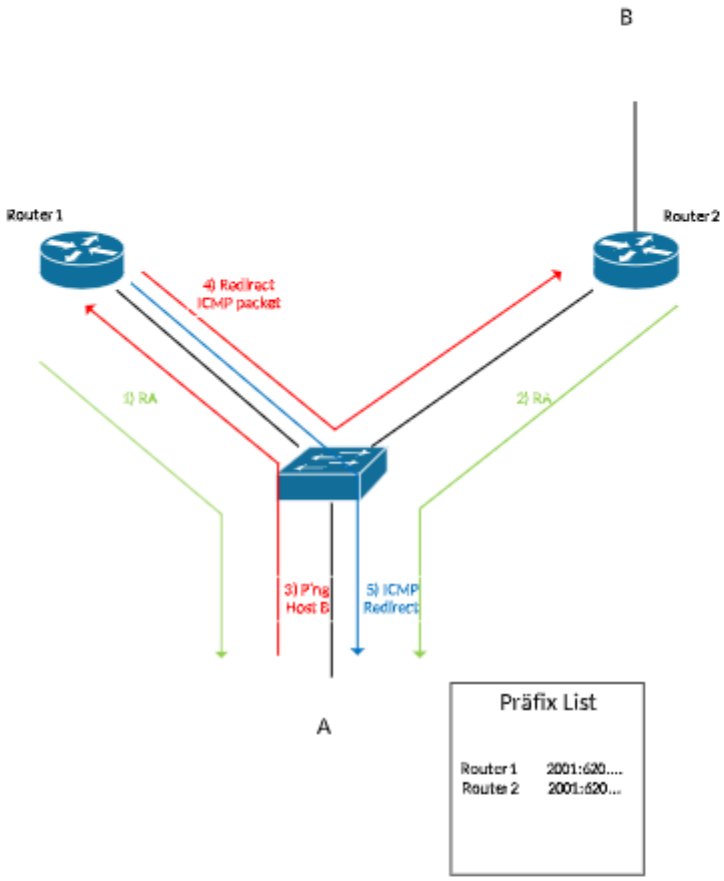


Figure 6.8.: Router Redirect

7. IPv6 Prefix Delegation (PD)

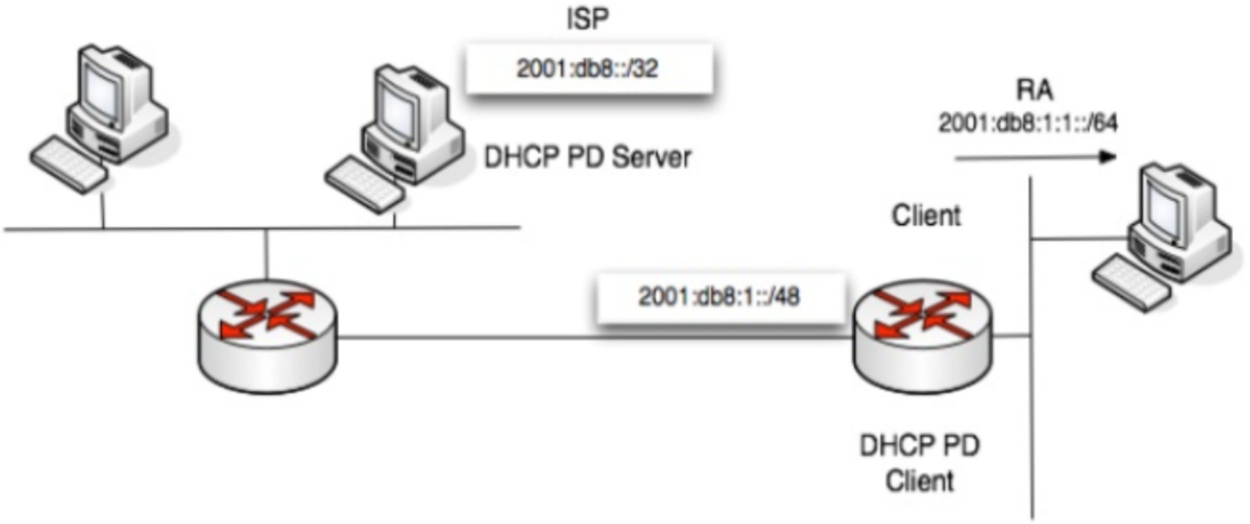


Figure 7.1.: IPv6 PD Delegation

A DHCPv6 server can be configured to delegate IPv6 addresses as well as IPv6 prefixes. An Internet Service Provider (ISP) does not have to "manually" assign prefixes. This task is taken over by the DHCPv6 Prefix Delegation server. In our example, the DHCP PD server manages the `2001:db8::/32` IPv6 address range. The DHCP PD client is going to receive a /48 IPv6 address range out of the network `2001:db8::/32` from the DHCP PD server. The DHCP PD server has allocated the IPv6 prefix `2001:db8:1::/48` to the DHCP PD client. In this case, the DHCP PD client has a dual function. Firstly, it is a client that receives a prefix from the ISP and secondly, a server for the distribution of prefixes to the end hosts. The DHCP PD client will segment the /48 IPv6 prefix(es) into smaller /64 prefixes which will be communicated to the end hosts via SLAAC. In our case, the prefix which is contained in the RA is sent to the LAN where the hosts are connected to. With regards to the above mentioned example, the LAN prefix could be `2001:db8:1:1::/64`.

8. Transition Technologies

In a dualstack environment, a client favors IPv6. This means that a web browser first tries to access a website via IPv6. In case of failure, the browser tries to get access via IPv4. This fallback procedure can take up to 30 seconds. For most users, this situation is unacceptable. To tackle this problem, the IETF organization has developed an algorithm called Happy Eyeballs. Happy Eyeballs allows a web browser to establish two connections in parallel: one via IPv4, the other one via IPv6. If there is no response via IPv6 within a certain time frame, the browser falls back on IPv4. That way, the response time can be minimized. This problem is one of many reasons why companies should offer their services in a dualstack environment.

8.1. IPv6 Rapid Deployment

When a service provider would like to enable IPv6 for its customers, it has to provide IPv6 on the whole infrastructure. This requires to replace every device. This is very cost- and time-intensive. A better solution would be to use a tunneling technique. In this lab, we will have a look at IPv6 rapid deployment. IPv6 rapid deployment is a mechanism enabling service providers to provide clients with IPv6 through an IPv4 infrastructure. The 6RD function is similar to 6to4. One difference is that globally valid IPv6 addresses are used, not the ones with the prefix `2002::/16`. The good thing about this is that you can calculate the IPv4 address out of the IPv6 address. This makes 6RD stateless which means that a Border Relay does not have to track connections of the users. In case a Border Relay fails, another one can take over without dropping the users' connections. In order to offer 6RD, a provider must provide at least one Border Relay and a Customer Edge Router. This router is the endpoint of the 6RD tunnel and is operated by the customer. Multiple 6RD Border Relays are announced in the network using anycast addresses. In the picture, below you can see a provider network which only supports IPv4. Between the Customer Edge Router (CE) and the Border Relay (BR), there is a 6RD tunnel established.

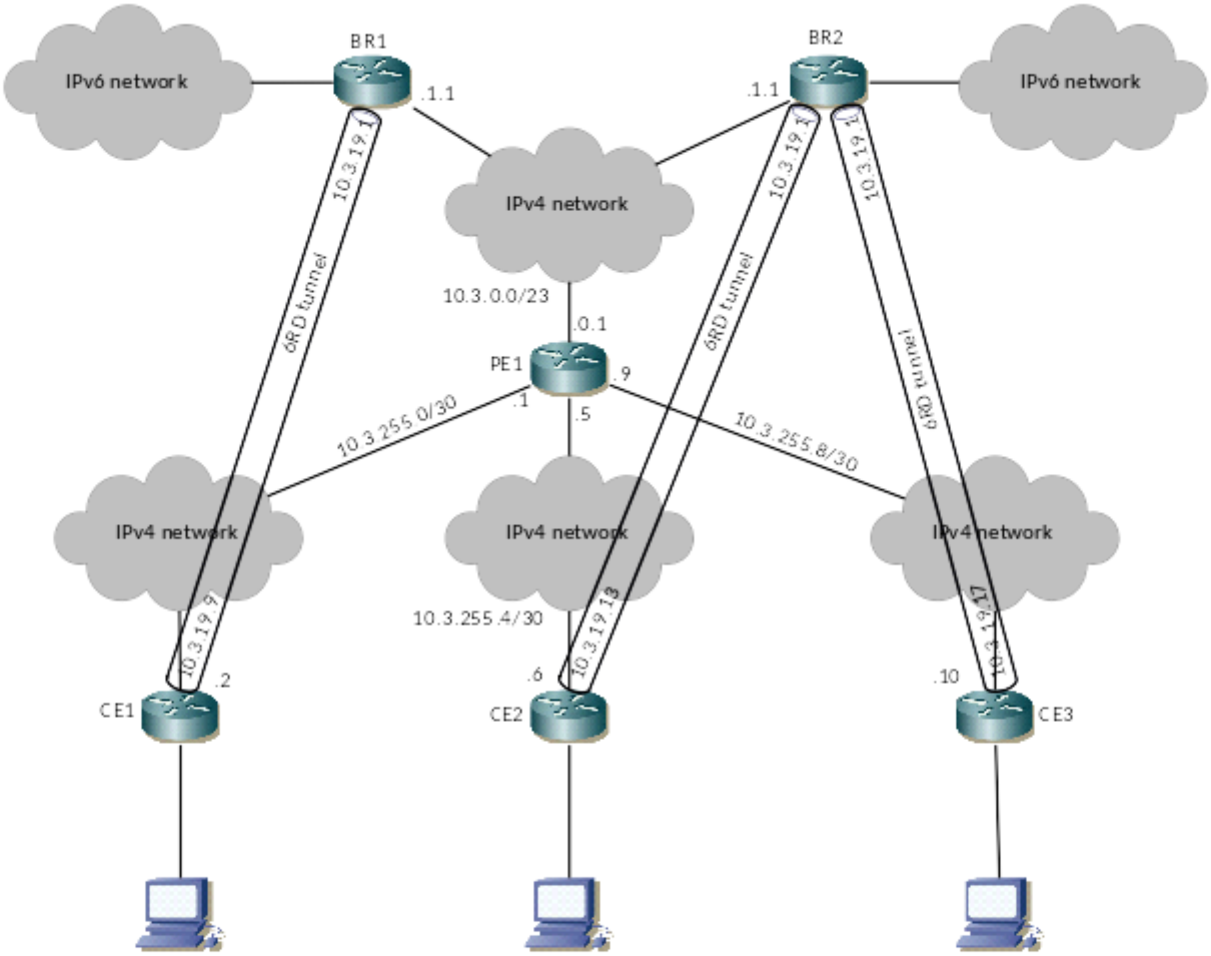


Figure 8.1.: Dual Stack Environment

Each Customer Edge Router (CE) establishes a 6RD tunnel to the Border Relay. IPv6 packets are transmitted via this tunnel. The client network can either be run in a dual-stack environment or with IPv6 only. To calculate the IPv6 address of the clients, you need the so-called Delegated Prefix. The Delegated Prefix contains the 6RD Prefix and the IPv4 address of the CE Router. In the picture below, you can see the calculation of the Delegated Prefix.

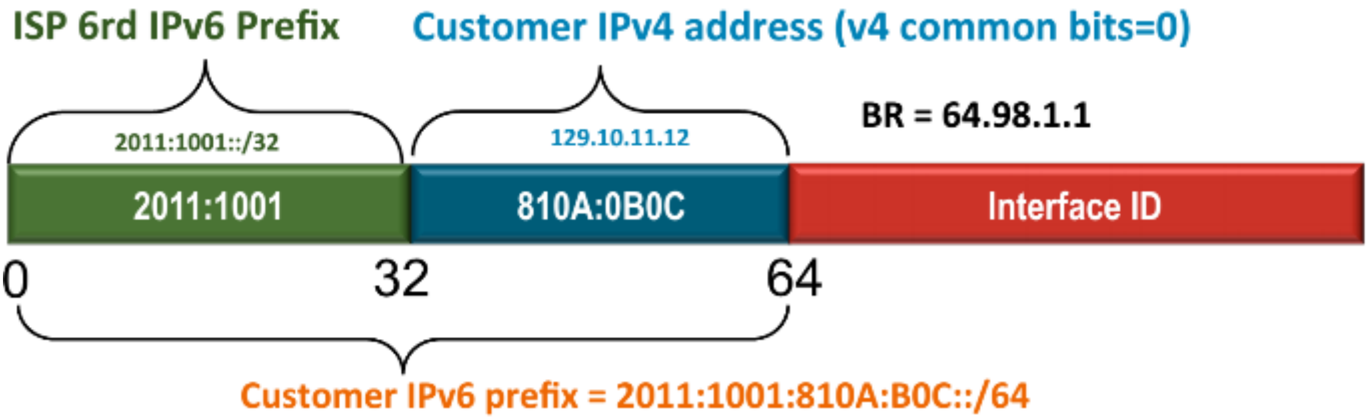


Figure 8.2.: Delegated Prefix Calculation

In this example, the whole 32 bit IPv4 address is converted into hex and appended to the 6RD prefix. It is not necessary to use all the 32 bit from the IPv4 address. If a client sends a packet to an IPv6 address, the CE checks in a first step whether the 6RD prefix has matched. A 6RD prefix defines a 6RD domain. If it has matched, the destination is in the same 6RD domain. Thus, data must not be sent through the Border Relay. They are directly transmitted to the relevant CE.

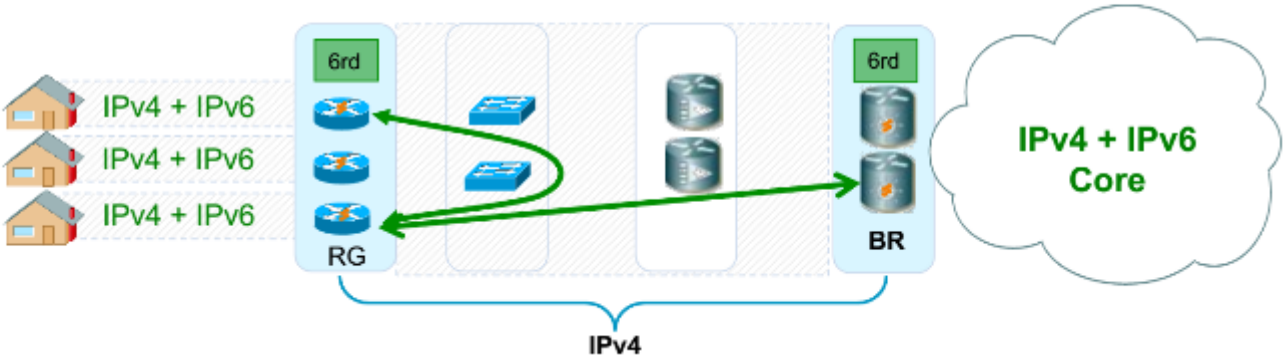


Figure 8.3.: Dual Stack Environment

In case the 6rd prefix has not matched, the packet is encapsulated in a IPv4 packet and transmitted to the Border Relay. The Border Relay removes the IPv4 header and forwards the packet to the IPv6 network. The BR does not save any connection state. On the way back, it decodes the IPv4 address of the Customer Edge Router based on the IPv6 address. The packet is then sent to the Customer Edge Router via IPv4.

Prestudy Exercise 8.1

Calculate the IPv6 source address of a package which is sent from a client to the Border Relay.

- The 6RD domain is: `2001:abcd:ef12::/48`
- The IPv4 Prefix is: `10.5.0.0/16`
- The IPv4 address of the Border Relay is `10.5.4.1`
- The IPv4 address of the Customer Edge Router is `10.5.4.10`

9. Mobile IP

Some applications such as VoIP and VPN face problems if IP addresses of clients change. In case of MobileIP, a mobile client keeps its IP even though it changes to another network. In this way, it can be reached on the same IPv6 address at all times. If a client changes to another network, it receives a second IPv6 address. The address is provided by the "foreign" network and is called care-of-address. Afterwards, the client has to register with its care-of-address at the Home Agent of the own network. The Home-Agent is then able to forward the packets to the mobile client. The Home Agent sends an all node multicast message to the home network of the mobile client. As of this point of time, all packets destined for the mobile client are transmitted to the Home-Agent. On the way back (to the home network of the mobile client), the packets are directly sent without involving the Home Agent. Thus, the load on the Home Agent can be reduced. The Home Agent must be fail-safe. Otherwise, the mobile clients cannot be reached anymore.

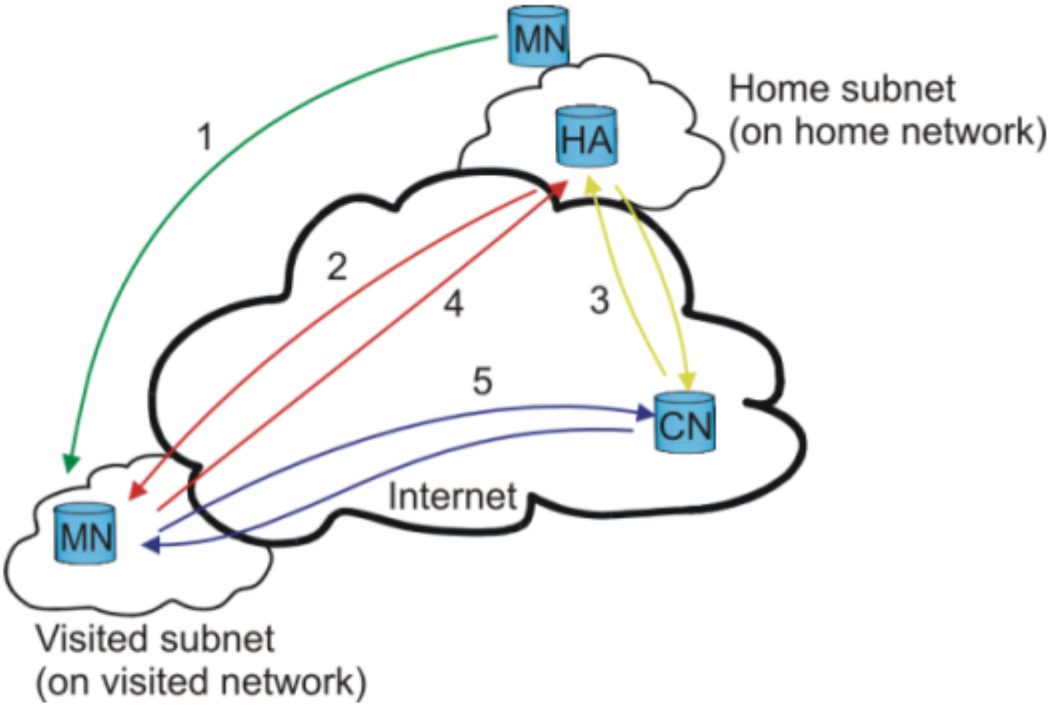


Figure 9.1.: Mobile IP

1. The Mobile Node (MN) travels to a foreign network and gets a new care-of-address.
2. The MN performs a binding update to its Home Agent (HA) (the new care-of-address gets registered at HA). HA sends a binding acknowledgement to MN.
3. A Correspondent Node (CN) wants to contact the MN. The HA intercepts packets destined to the MN.
4. The HA then tunnels all packets to the MN from the CN using MN's care-of-address.

5. When the MN answers the CN, it may use its current care-of-address (and perform a binding to the CN) and communicate with the CN directly (optimized routing) or it can tunnel all its packets through the HA.

10. IPv6 Packet Security

10.1. Overview

Encryption in IPv6 is implemented using IPsec. This means IPv6 can either use Authentication Header (AH) and/or Encrypted Security Payload (ESP) to keep its payload confidential and safe. An AH ensures the same level of integrity and data authenticity as it does in traditional IPv4 IPsec. In other words, it safeguards data against alterations and the client against spoofed packets. ESP encrypts and encapsulates data. Thus, data are protected against alterations. It also checks the sender of the packets for correctness. IPv6 Security (AH & ESP) is directly implemented via IPv6 Extension Headers. This is the main difference compared to IPv4 IPsec.

This means that IPv6 IPsec can be determined as Next Header.

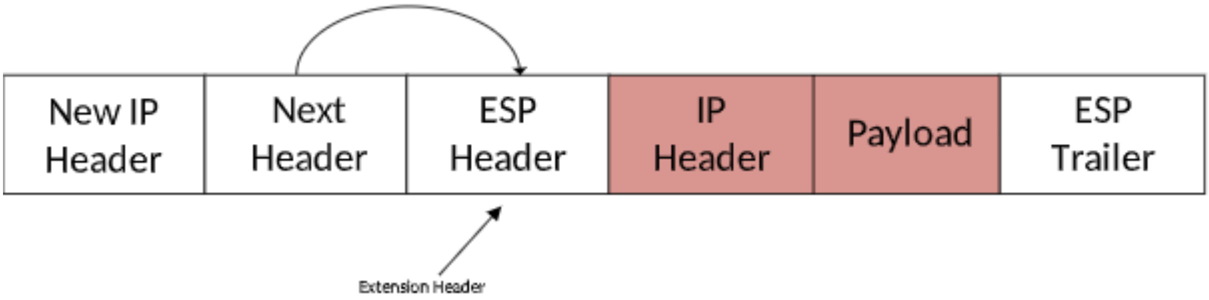


Figure 10.1.: IPv6 IPsec ESP

For comparison purposes, in IPv4 the original packet is considered as payload for the IPsec packet.

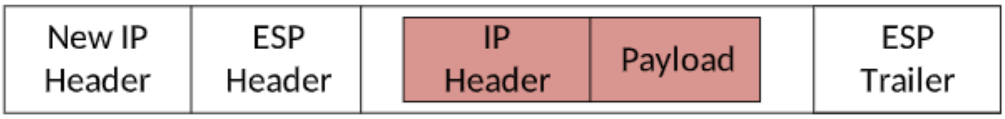


Figure 10.2.: IPv4 IPsec ESP

The following figure shows an overview of the headers that are authenticated/encrypted:

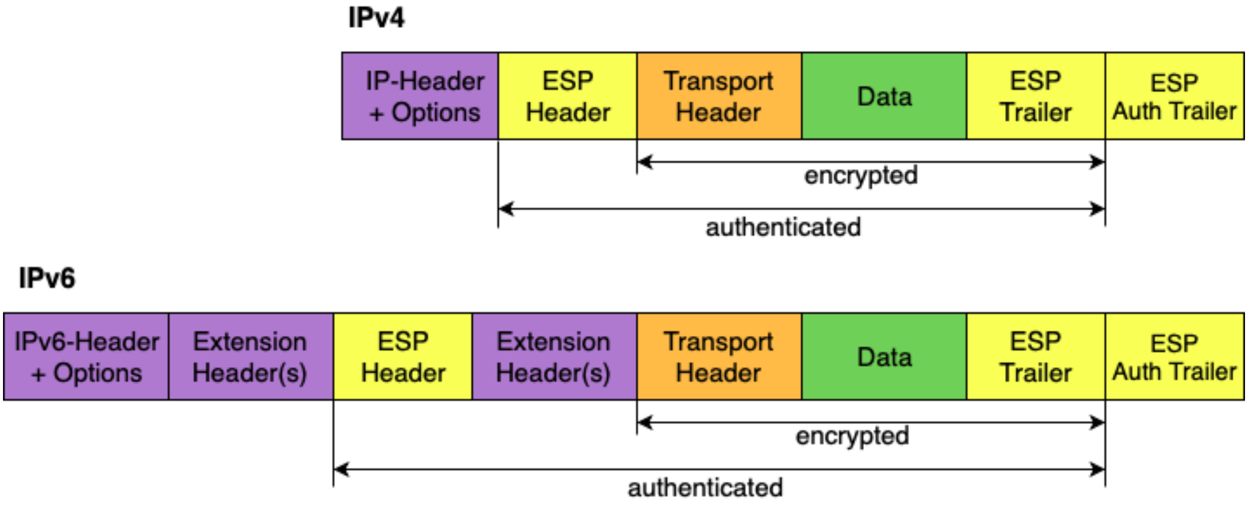


Figure 10.3.: IPv4 IPsec vs. IPv6 IPsec

IPsec defines cryptography-based security and is used to protect IP traffic on the network layer because the IP protocol has no integrated security features. IPsec provides the following features for protection:

- Confidentiality - the payload gets encrypted with ESP. Thus, no one except the sender and the receiver will be able to read the data in plain text.
- Integrity - the payload, the header and the unchanging fields of the IPv6 header and options in the packets should not be changed. This can be checked by calculating a hash value, the Integrity Check Value (ICV), by the sender and the receiver. If they do not have the same amount, there has been a change in the packet.
- Authentication - the sender and the receiver authenticate each other over AH to ensure each other's authenticity.
- Anti-replay - with sequence numbers, ESP or AH will not transmit any duplicate packets. Thereby, an attacker cannot capture packets and send them again.

10.2. IPsec Tunnel

To establish an IPsec tunnel, the protocol Internet Key Exchange (IKE) is used. It operates in 2 phases: IKE phase 1 and IKE phase 2. The IPsec process is a five-step process:

1. Initiation - to start the process of building a tunnel. It has to be triggered, for example, by an access-list on a router to verify what data is protected. The initiation can also be configured manually.
2. IKE phase 1 - the two peers have to negotiate a Security Association (SA) to build the IKE phase 1 tunnel (also called ISAKMP tunnel, Internet Security Association and Key Management Protocol). The agreed parameters are saved in a database of each endpoint.
3. IKE phase 2 - the IKE phase 2 tunnel is built within the IKE phase 1 tunnel. The IKE phase 2 tunnel is also called the IPsec tunnel.
4. Data transfer - user data that is sent through the IKE phase 2 tunnel is protected.
5. Termination - after a certain time, when the IPsec tunnel does not receive any user data to protect, it gets terminated

10.3. Internet Key Exchange (IKE)

It is used as one of the primary protocols for IPsec because it can establish the SA between two peers. There are two different versions of IKE: version 1 and version 2. A couple of improvements were built into the IKEv2:

- requiring less bandwidth
- supporting EAP authentication
- a built-in support for NAT transfer (is needed when a IPsec peer lays behind a NAT router)
- a built-in keep-alive mechanism for tunnels

10.3.1. IKEv1

10.3.1.1. IKE Phase 1

This tunnel is used as a secure method to establish the second tunnel called the IKE phase 2 tunnel or IPsec tunnel as well as for management traffic like keepalives. IKE phase 1 consists of three steps where the peers negotiate about collection of parameters (e.g. how to encrpyt and digitally sign traffic they exchange). This communication session is called Security Association (SA).

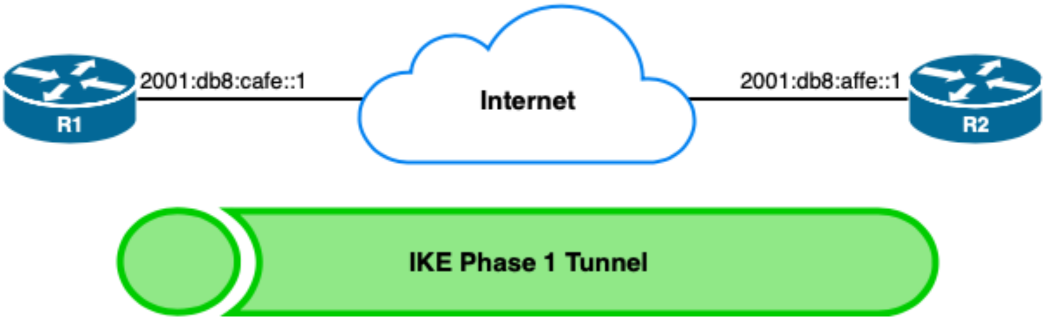


Figure 10.4.: IKE Phase 1

1. Negotiation - The initiator that wants to transmit confidential data represents the peer which will start the negotiation. The two peers are going to negotiate about the following points:
   - Hashing - to survey the integrity, a hashing algorithm like MD5 or SHA will be used.
   - Authentication - with a pre-shared key or digital certificates, the peer can prove its identity.
   - DH (Diffie Hellman) group - the strength of a key in a key exchange process can be determined by the DH group. The higher the value of the group numbers, the more secure. However, the calculation of the algorithms behind these numbers is more time-consuming.
   - Lifetime - set the duration (how long an IKE phase 1 tunnel stands). A short lifetime is more secure because new keying material is used for rebuilding a new tunnel. A common default value is 86400 seconds (1 day). Though, each vendor uses a different lifetime.
   - Encryption - which encryption algorithm should be used, like DES, 3DES or AES.

2. DH Key Exchange - After the negotiation, the peers can get a shared key because they know which policy they should use. In order to get the needed key material, they use the previously discussed DH group.

3. Authentication - The two peers authenticate each other by the authentication method that they agreed upon in their previous negotiation. After the authentication step, the whole IKE phase 1 is completed and an IKE phase 1 tunnel (ISAKMP tunnel) is generated that can work in both directions of the peers.

The IKE phase 1 can be completed with the help of two different modes: the main mode or the aggressive mode. The aggressive mode uses only three messages. It is quicker for two reasons. Firstly, it combines all information which is used for the DH exchange in the first two messages. Secondly, the identification is done only in clear-text. On the contrary, the main mode uses six messages. It is more secure as the identification is encrypted.

10.3.1.2. IKE Phase 2

The tunnel that is built into the IKE phase 2 (IPsec tunnel) is used to protect the user data. The IKE phase 2 only uses one mode called quick mode. In this phase, the peers negotiate again about several items:

- IPsec Protocol - will AH and/or ESP be used?
- Encapsulation Mode - will there be any transport or tunnel modes used?
- Encryption - which encryption algorithm will be used? DES, 3DES or AES?
- Authentication - will MD5 or SHA be used as authentication algorithm?
- Lifetime - how long will the IKE phase 2 tunnel be usable? When the tunnel expires, the peers have to refresh the keying material.
- (optional) Diffie-Hellman (DH) exchange - will be used for Perfect Forward Secrecy (PFS). It forces the peers to run the DH exchange again so they can get a new shared key in each quick mode of the IKE phase 2.

Because this negotiation is performed while the IKE phase 1 tunnel is active, no data is visible in the plain text.

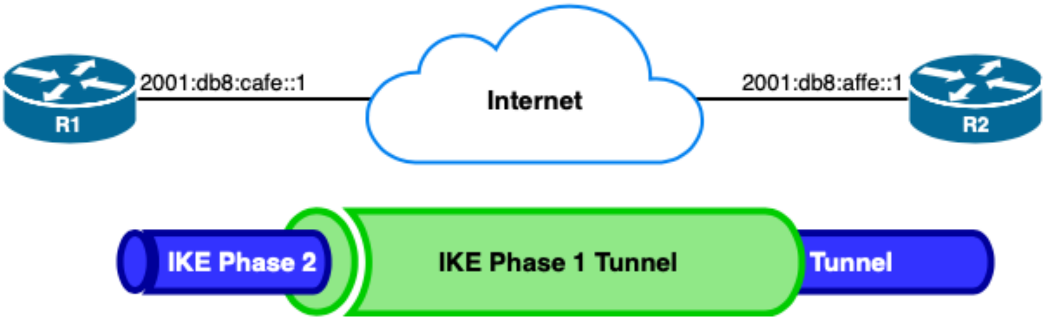


Figure 10.5.: IKE Phase 2

Finally, the actual user data is transferred via the IKE phase 2 tunnel:

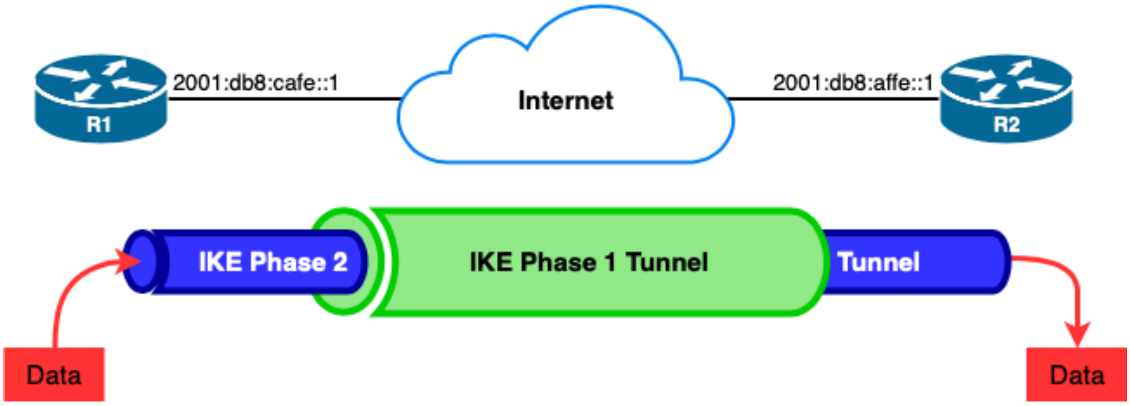


Figure 10.6.: IPsec Tunnel

10.3.2. IKEv2

This version only has one mode for phase 1 (unlike IKEv1) and has no quick mode for phase 2. The two phases are called IKE_SA_INIT and IKE_AUTH. Four messages are needed for the whole exchange.

10.4. IPsec Protocols

Two protocols, AH and/or ESP, are used to protect user data. Both can be used in transport or tunnel mode.

10.4.1. Authentication Header (AH) Protocol

AH offers authentication and integrity, however, it does not provide any encryption. In order to protect the IP packet, the AH calculates a hash value ICV over source and destination addresses. This is why AH cannot be used for traversing NATs in IPv4. In IPv6, this should no longer be an issue since it is best practice to use global unicast addresses which do not require a NAT. The excluded fields can be changed in the transit (TTL and header checksum).

10.4.1.1. Transport Mode

In this mode, an AH header is added after the original IP header.

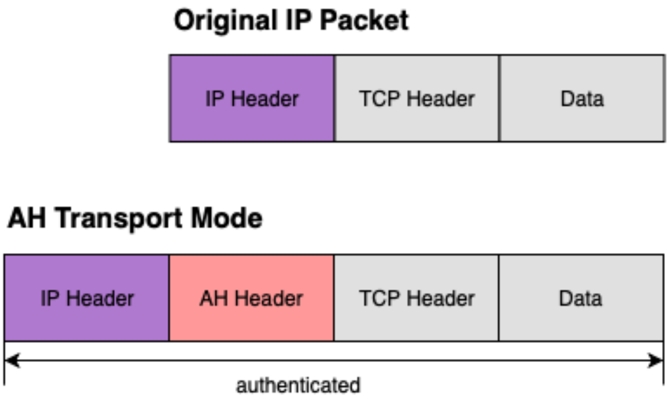


Figure 10.7.: AH in Transport Mode

The AH header lies between the IP header and the ICMP/TCP/UDP header. It consists of the following five fields:

- Next Header - identifies which protocol will be used next
- Length - defines how long the AH header is
- SPI (Security Parameters Index) - with this 32-bit long identifier, the receiver can define to which flow the packet belongs
- Sequence - a number that prevents replay attacks
- ICV (Integrity Check Value) - is the calculated hash for the whole packet. The sender and receiver both compute a hash. If the hash does not match, the connection might have been altered or a transmission failure might have occured.

10.4.1.2. Tunnel Mode

This mode adds a new IP header which encapsulates the original IP packet. It can be used for privately addressed IP packets in case traffic needs to be tunneled over the internet. Tunnel mode can be used in combination with AH. However, this only offers authenticity, but no confidentiality.

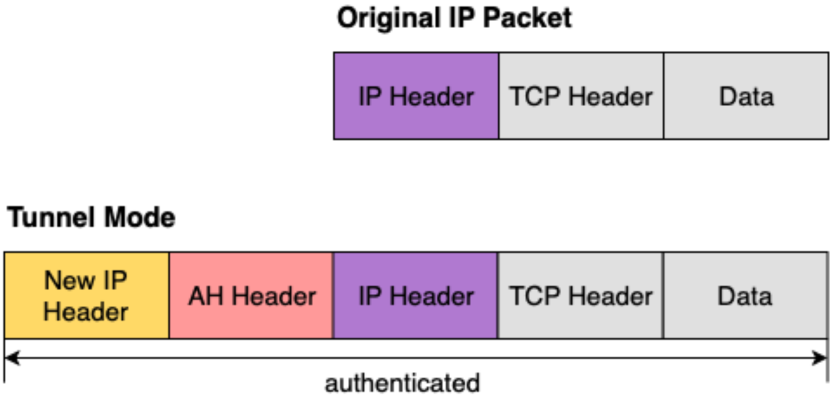


Figure 10.8.: AH in Tunnel Mode

Even if AH excludes IP Header fields like TTL and checksums from its hash calculations, it still does not work with NAT/PAT. This is because NAT/PAT changes IP addresses and port numbers which are part of the AH hash calculation. As a result, the ICV does not match anymore.

10.4.2. Encapsulation Security Payload (ESP) Protocol

ESP encrypts IP traffic. This is why this protocol is preferred over AH in most cases. For instance, ESP is used to build virtual private network tunnels over the internet for the interconnection between sites / branch offices.

10.4.2.1. Transport Mode

In the transport mode, the original IP header will be used with an inserted ESP header and trailer.

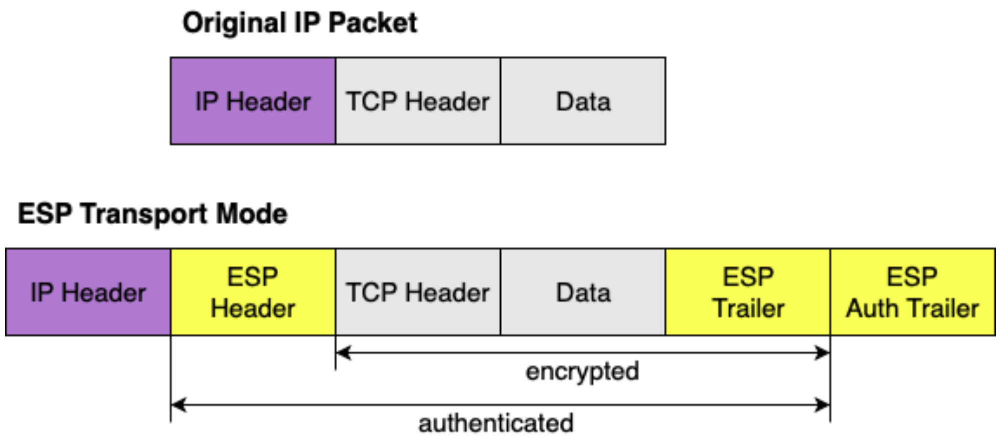


Figure 10.9.: ESP in Transport Mode

ESP encrypts the transport layer as well as the payload and authenticates a part of the packet, unlike AH. The original IP header is not encrypted. Therefore, it is visible in plain text.

10.4.2.2. Tunnel Mode

Unlike transport mode, in tunnel mode a new IP header is used. Therefore, this mode is useful for site-to-site (S2S) VPNs.

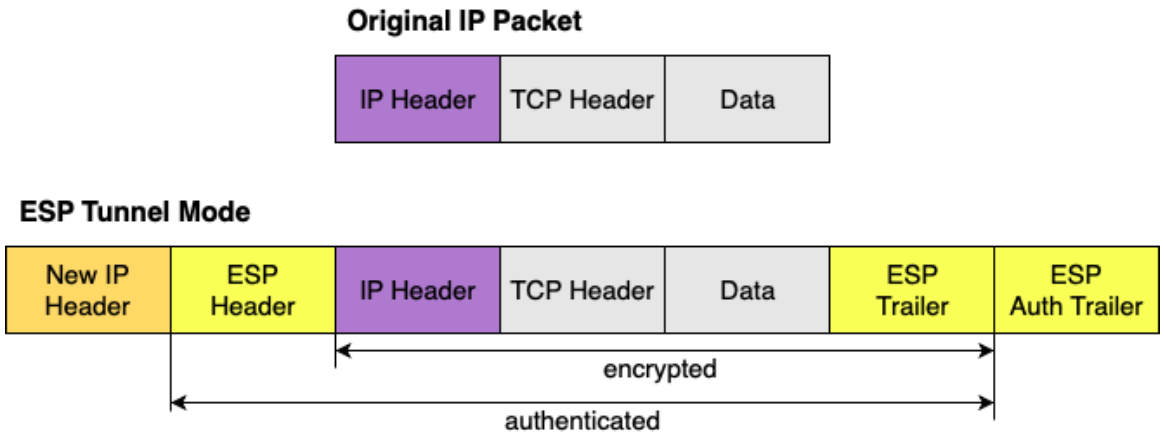


Figure 10.10.: ESP in Tunnel Mode

Due to the new IP header, the original one can now be encrypted. As a result, the original IP header will not be visible anymore.

10.5. AH and ESP

AH and ESP can be used at the same time.

10.5.1. Transport Mode

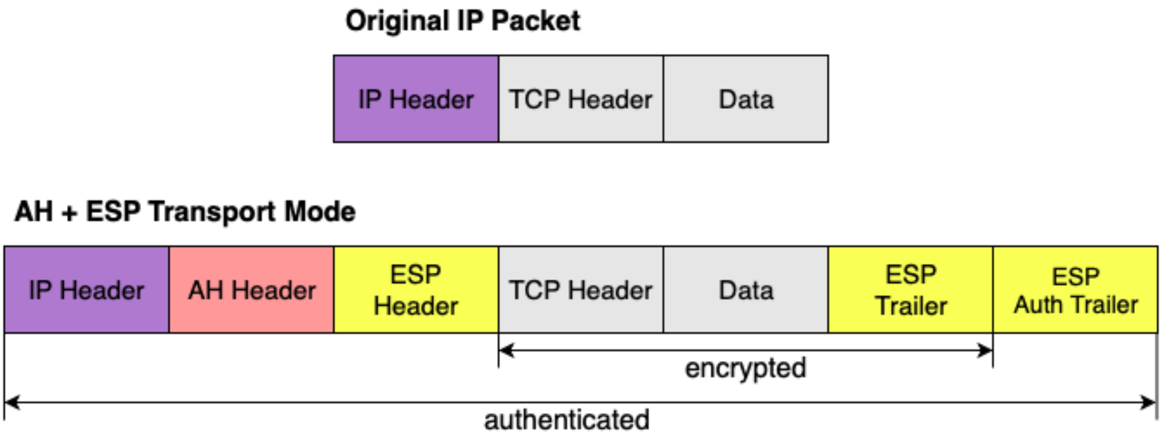


Figure 10.11.: AH + ESP in Transport Mode

In the transport mode, an AH and ESP header are added to the original IP header. Only the transport layer, the payload and the ESP trailer are encrypted. The whole IP packet is authenticated due to AH.

10.5.2. Tunnel Mode

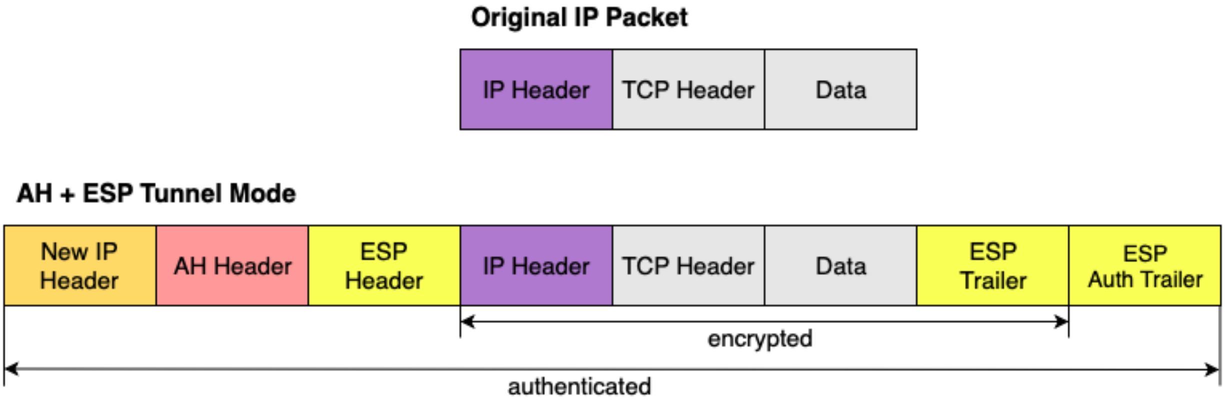


Figure 10.12.: AH + ESP in Tunnel Mode

In the above figure, a new IP header is used with an AH and an ESP header. The original IP packet is will be encrypted and the whole packet will be authenticated because of AH.