

Project no. 015926

6DISS

IPv6 Dissemination and Exploitation

Instrument: SPECIFIC SUPPORT ACTION

Thematic Priority 2

D13: E-learning Material

Due date of deliverable: 30th September 2005

Actual submission date: 8th November 2005

Start date of project: 1st April 2005

Duration: 30 months

Organisation name of lead contractor for this deliverable:

Cisco

Revision: V1.0

Abstract

This Deliverable outlines the content of the 6DISS on-line IPv6 e-learning package that complements all of the other dissemination activities within the project. This professional interactive e-learning package explains to users the main features of IPv6 and guides them to the appropriate reference material (e.g. 6NET Cookbooks, IETF standards). Tests are incorporated to assess whether the participant has understood the lessons. These tests can also be used to gauge the suitability of a person to attend the workshops.

Whilst this document is a useful hardcopy reference of what the course contains, the material can only be properly appreciated by accessing the on-line version at: www.6diss.org/e-learning

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of Contents

1. INTRODUCTION	3
2. THE CONTENTS OF THE MODULES	5
2.1. MODULE 0: INTRODUCTION TO THE E-LEARNING PACKAGE	5
2.2. MODULE 1: INTRODUCTION TO IPV6	8
2.3. MODULE 2: IPV6 ADDRESSING	10
2.4. MODULE 3: THE IPV6 HEADER	13
2.5. MODULE 4: IPV6 BASIC SERVICES	15
2.6. MODULE 5: SECURITY IN IPV6	20
2.7. MODULE 6: IPV6 ROUTING, MOBILITY AND MANAGEMENT	22
2.8. MODULE 7: COEXISTENCE WITH IPV4	26
3. CONCLUSION	29

1. Introduction

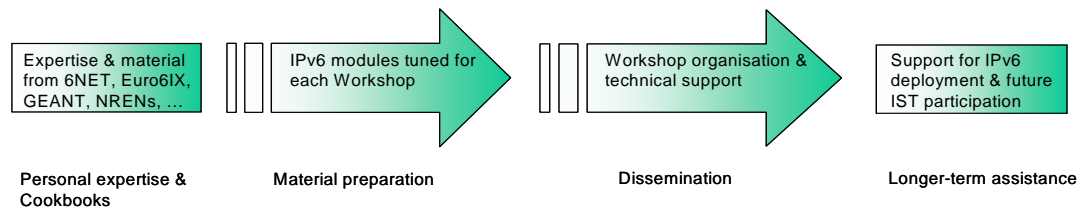
This Deliverable outlines the content of the 6DISS on-line IPv6 e-learning package that complements all of the other dissemination activities within the project. This professional interactive e-learning package explains to users the main features of IPv6 and guides them to the appropriate reference material (e.g. 6NET Cookbooks, IETF standards) if more information is needed. Tests are incorporated to assess whether the participant has understood the lessons. These tests can also be used to gauge the suitability of a person to attend the workshops.

The 6DISS e-learning package has 2 key objectives:

1. Introduce IPv6 to a large technical audience (not only the 6DISS target areas, but worldwide)
2. Serve as a teaser and preparation for 6DISS Workshop participants

The e-learning package is multimedia based and uses a combination of voice-over, animation and interaction. The total voice-over duration is about 40 minutes. The typical user experience of the e-learning will be 2-3 hours, depending upon the background of the user.

The e-learning package is an integral part of the “Dissemination” process in the chain of activities shown below:



The e-learning experience has the advantage that anyone connected to the Internet and able to find the 6DISS website has the possibility to access the 6DISS IPv6 e-learning package. The material will be actively promoted in the 6DISS target countries, but interested audiences anywhere in the world will be able to benefit from the e-learning course.

The technical level of the e-learning material assumes that participants have a networking background and a good basic understanding of TCP/IP concepts such as: IPv4 addressing, routing protocols, access lists, NAT, etc.

The typical profile of a target e-student is that of a network administrator, experienced in setting up an IP network environment. The approach within most of the e-learning modules is to compare the important aspects of IPv6 with those of IPv4.

After an initial module (Module 0) that describes the set of support and dissemination material that is available from 6DISS as a whole (ie. the Website, E-learning package, Workshops, Laboratories, Tiger Team, deliverables), and the role of e-learning within the whole dissemination framework, the e-learning package comprises the following technical modules. These are all based on - or aligned with - the workshop powerpoint slide sets:

Module 0: Introduction to the E-learning package

- The set of dissemination material that is available from 6DISS as a whole (the Website, E-learning package, Workshops, Laboratories, Tiger Team, deliverables)
- The positioning of the E-learning package within the whole framework

Module 1: Introduction to IPv6

- Limitations of IPv4

- Why IPv6 is needed

Module 2: IPv6 Addressing

- IPv6 address syntax
- Types of IPv6 addresses
- Automatic building of a host's interface identifier from its physical address

Module 3: The IPv6 Header

- Structure of an IPv6 packet header (and the differences between IPv4 and IPv6)
- IPv6 header functions
- IPv6 extension headers

Module 4: IPv6 Basic Services

- Internet Control Message Protocol (ICMP) for IPv6
- Neighbour Discovery Protocol (NDP)
- IPv6 stateless autoconfiguration
- DHCPv6
- DNSv6
- IPv6 Multicasting (incl. Multicast Listener Discovery - MLD)
- QoS

Module 5: Security in IPv6

- IPv6 security elements
- IPSec functions in IPv6 (and differences from IPv4)

Module 6: IPv6 Routing, Mobility and Management

- Interior and Exterior Gateway Protocols
- Mobile IPv6
- Network management

Module 7: Coexistence with IPv4

- Transition and coexistence mechanisms overview
- Dual-Stack techniques
- Tunnelling techniques

Every module contains the following:

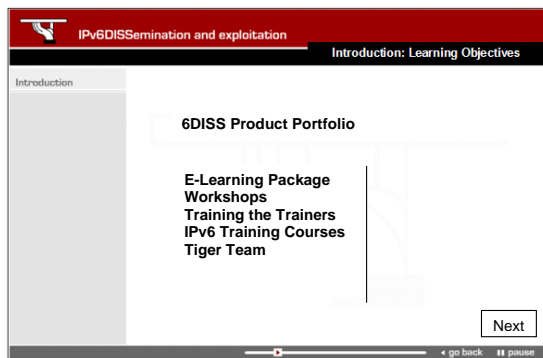
1. A voice-over guided explanation of the subject
2. After every relevant piece of content: an interactive overview screen with clickable objects. Users can click keywords, objects, elements within a graph for further, text-based explanations
3. A series of self-test multiple choice questions based on the content which is explained

2. The Contents of the Modules

The contents of each module (ie. the “Storyboard”) is as follows:

2.1. Module 0: Introduction to the E-learning package

Module 0 explains what dissemination material is available from 6DISS as a whole (the Website, E-learning package, Workshops, Laboratories, Tiger Team, deliverables), and the positioning of the E-learning package within the whole framework.



1. INTRODUCTION

Voice-over text:

This e-learning package is one element of a comprehensive set of facilities provided by the 6DISS project for **supporting the deployment of IP version 6**.

Other facilities offered by 6DISS are:

- 3-day **Workshops** at your location.
- **Training the Trainers** courses, in which we will train people who can then present our workshops on their own.
- **IPv6 [read: I-P-v-6] Training Courses**, in purpose built labs in either Brussels or Paris.
- A so-called “**Tiger Team**” of experts who can give on-line support for any aspect of your IPv6 deployment.

Click the “Next” button to continue.

2. E-LEARNING PACKAGE

Voice-over text:

The 6DISS e-learning package serves as an introduction to the 6DISS IPv6 dissemination content and has 2 main objectives:

- **To introduce IPv6 to a large technical audience (worldwide)**
- **To serve as a teaser and preparation for potential 6DISS workshop participants**

The e-learning package is **multimedia-based** and uses a combination of **voice-over, animation and interaction**. The total voice-over duration is about 40 minutes. The typical user experience of the e-learning material will last about 2-3 hours, depending on the background of the user.

A big advantage of the e-learning package is that **anyone connected to the Internet and able to find the 6DISS website has the possibility to access the 6DISS IPv6 e-learning material**.

The e-learning package is aimed at people with a networking background and having a good basic understanding of Internet concepts such as: IPv4 addressing, routing protocols, access lists, NAT, etc.

The typical profile of a target e-student is that of a network administrator, experienced in setting up an IP network environment. The approach within most of the e-learning modules is to **compare the important aspects of IPv6 with those of IPv4**.





3. WORKSHOPS

Voice-over text:

Workshops are the key mechanism through which information will be disseminated. Through our workshops we would like to raise awareness; exchange information about deployment experiences, pass on the results from European projects; and explain about activities related to standards and interoperability issues.

We have presentation material on all aspects of IPv6; namely:

- The IPv6 protocol
- DNS
- Addressing (and the administration of addresses)
- Routing
- RPSLng
- Autoconfiguration
- Multicast
- Security
- Mobility
- Quality of Service
- Co-existence with IPv4
- Network Management

We will also show how to **configure devices at your site**, or by accessing, remotely, one of our purpose-built laboratories.



4. TRAINING THE TRAINERS

Voice-over text:

Due to time and budget constraints, 6DISS cannot deliver an unlimited amount of workshops. However, by offering a **Training the Trainers** facility, 6DISS is able to train other people, who can then disseminate the information further.

These trainers will be given the full set of material, some guidelines for presenting the modules, additional notes to accompany the slides, and a list of key messages to get across to the participants.

The training can be given in Europe (Brussels or Paris), or at a local location; ideally immediately prior to - or after - a workshop.

This facility can be particularly useful where:

- regions wish to take advantage of the 6DISS material, independently from the workshops.
- people in the targeted regions wish to make some training prior to the workshop.
- due to high travel costs or other constraints, persons were not able to attend the workshop.
- due to the success of the workshop, the local organisations wish to run several more in the region themselves.
- as a result of a workshop on one particular topic, interest is generated in some of the other 6DISS topics (e.g. specialist programmes for Network Operation Centres, ISPs, or regulators).



5. IPV6 TRAINING

Voice-over text:

For people wanting a deeper technical training on IPv6, **6DISS has built 2 laboratories in Europe (Brussels and Paris)**. These can be accessed during the workshops to show how to configure equipment, but are also available for people to be trained more thoroughly on specific aspects of IPv6.

This course is **especially suitable for engineers and network managers, especially from ISPs.**

The training course will last 1-week and will cover the same items as in the workshops, but with more focus on hands-on practical examples. Equipment from Cisco, Alcatel and Juniper is available.



6. TIGER TEAM

Voice-over text:

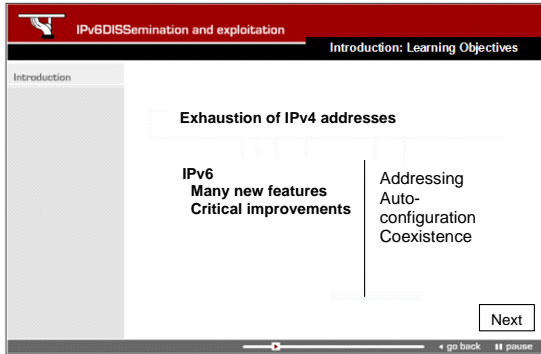
The Tiger Team offers an "after-workshop" support for deployers of IPv6 networks.

This team of experts is available to answer questions via e-mail and maintains a list of Frequently Asked Questions regarding equipment configuration, hardware and software requirements, RFCs, etc.

Examples of their support includes:

- giving advice on aspects of transition to - or coexistence with - IPv6
- the creation and maintenance of a Website that conveys information about the state of the art in IPv6 deployment, and offers visitors access to appropriate information to assist in their deployment of IPv6, including:
 - the receiving and publishing of relevant information
 - a discussion forum for specific technology (hosts, routers, etc.)
 - documenting answers to specific technology questions
- providing details of applications
- fact sheets on IPv6 deployment, e.g. IPv6 VPN, DHCPv6, etc
- interfacing to and assisting national IPv6 Task Forces and IPv6 Fora

2.2. Module 1: Introduction to IPv6



1. INTRODUCTION

Voice-over text:

Welcome to this e-learning course about **IP version 6**. IP version 6, or IPv6 for short, [\[read: I-P-v-6\]](#) is a new protocol designed to **replace** IPv4, the Internet protocol that is predominantly deployed and extensively used throughout the world. Although the **exhaustion of available IPv4 address space** has been the primary reason for the development of a new protocol, the designers of IPv6 have added **many new features** and a number of **critical improvements** to IPv4.

This e-learning course covers these aspects in a number of modules, including areas such as addressing, autoconfiguration and coexistence of IPv4 and IPv6.

- In this Introduction module, you will learn **why need a new IP protocol** is needed
- and what the advantages are of **IPv6**. Once completed, you will be able to describe the **main benefits** IPv6 will provide.

Click the "Next" button to continue.

2. LIMITATIONS OF IPv4

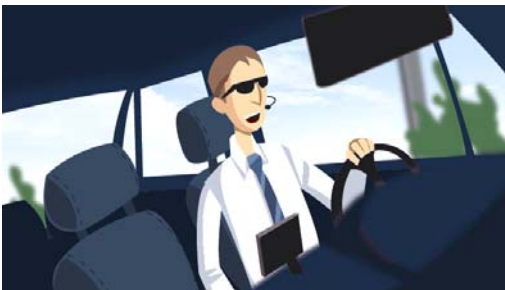
Voice-over text:

IPv4 has stood the test of scaling an internetwork to a global utility the size of the Internet today. But IPv4 wasn't initially designed to support a high number of network equipment.

Because of the recent exponential growth of the Internet, IPv4 is unable to satisfy the potential huge increase in the number of users or the geographical needs of the Internet expansion. As a result, **IPv4 address depletion** is approaching quickly. Additionally, emerging applications such as Internet-enabled [PDAs](#), [Home Area Networks](#), [mobile ad hoc networks](#), [IP wireless services](#) and [integrated IP telephony services](#) require a new internet protocol.

The lifetime of IPv4 has been extended using techniques such as address reuse with **Network Address Translation**, or **NAT** for short, **Classless Interdomain Routing**, or **CIDR**, and temporary address assignments such as the **Dynamic Host Configuration Protocol**, or **DHCP**.

[\[Read NAT as the word "nat", CIDR as C-I-D-R and DHCP as D-H-C-P\]](#)



Voice-over text:

These techniques appear to increase the address space and satisfy the traditional server/client setup, but **they fail to meet the requirements** of true network and user mobility. Applications need an increasing amount of bandwidth, while address translation has a performance impact on the network equipment.

Next, the need for **always-on environments** to be contactable prohibits these IP address conversion, pooling, and temporary allocation techniques.

Furthermore, the **'plug and play'** feature required by consumer Internet appliances further increases the **protocol requirements**. Millions of new technology devices such as [wireless phones](#), [PDA's](#), [cars](#) and [home appliances](#) will not be able to get global IPv4 addresses any longer. IPv4 will soon reach the stage where a choice has to be made between either new capabilities – or a larger network, but not both. In other words, we need a **new protocol** to provide **new and enhanced features** in addition to **solving the IP address exhaustion problem**. That new protocol is **IPv6**.

Click one of the items on the screen for more details. Or test your understanding by clicking the "Test" button. Or, click "Next" to continue.



3. WHY IPV6 IS NEEDED

Voice-over text:

IPv6 is designed to meet the requirements of the potentially huge Internet expansion. It will allow a return to a global environment where the addressing rules of the network are transparent to the applications again. Through **autoconfiguration** and **plug-and-play support**, **network devices** will be able to connect to the network without manual configuration and without any bootstrap services, such as DHCP servers.

IPv6 succeeds in doing this by providing the following benefits to network and IT professionals:

First, **IPv6** has a **larger address space** for global reachability and scalability. This will result in an almost unlimited number of IP addresses and a hierarchical network architecture for routing efficiency. This **eliminates the problems associated with NAT**. The ability to provide public addresses for each network device enables **end-to-end reachability**. And network management will be simpler and easier.

Figure 2: Comparison of IPv4 and IPv6 Headers

IPv4 Header				IPv6 Header		
Version	IHL	Type of Service	Total Length	Version	Traffic Class	Flow Label
Identification		Flags	Fragment Offset	Payload Length	Next Header	Hop Limit
Time to Live	Protocol	Header Checksum		Source Address		
Source Address				Destination Address		
Destination Address				Destination Address		
Options			Padding			

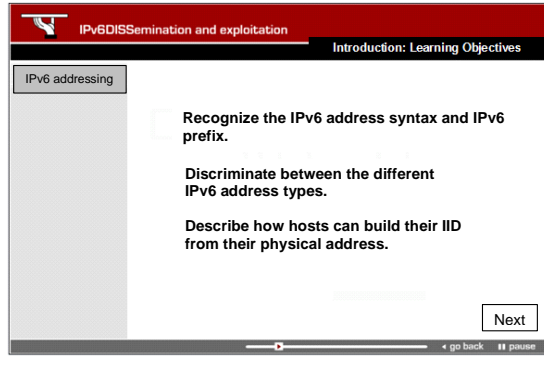
 Field name kept from IPv4 to IPv6
 Field not kept in IPv6
 Name and position changed in IPv6
 New field in IPv6

Voice-over text:

- Second, a **simplified header format** for efficient packet handling. 6 of the 12 IPv4 header fields have been removed in IPv6. Some IPv4 fields have been carried over with modified names, and some new fields have been added to **improve efficiency and introduce new features**.
- Third, a **hierarchical network architecture** for routing efficiency, that follows some of the IPv4 CIDR principles.
- Another important IPv6 benefit is the **embedded security** with **mandatory IPSec implementation**. [read: *I-P-Sec - with emphasis on "sec"*] While the use of IPSec is optional in IPv4, IPSec is mandatory in IPv6. IPSec is part of the IPv6 protocol suite. Therefore, network implementers could enable IPSec in every IPv6 node, potentially making the networks more secure.
- Additionally, IPv6 offers an increased number of **multicast addresses**. IPv6 will not use **broadcasts**, leading to a more performant network.
- Moreover, in IPv6, the new **[CMP protocol]** known as ICMPv6, [read: *I-C-M-P-v-6*] has become **much more powerful**, and includes new functions to support autoconfiguration, "neighbourship discovery" and multicasting.
- And finally, IPv6 offers **built-in mobility**, as the anticipated large rollout of wireless data services is a key IPv6 driver.

Click an interactive item for more details, or "Next" to continue.

2.3. Module 2: IPv6 Addressing



1. INTRODUCTION

Voice-over text:

In this module about IPv6 addressing, you will first learn how to **recognize the IPv6 address syntax, including the IPv6 prefix.**

Next, you will learn how to **discriminate between the different IPv6 address types.** After completion of this module, you'll also be able to **describe how hosts can automatically build their interface identifier from their physical address.**

Click the 'Next' button to continue.

2. IPv6 ADDRESSES SYNTAX

Voice-over text:

IP addressing changes significantly with IPv6. Instead of the 4 bytes in an IPv4 address, an **IPv6 address has 16 bytes.** Studies conducted say the 128 bits IPv6 address will lead to approximately 1000 addresses per person on this planet. Even if only a portion of the full IPv6 address space will effectively be used, IPv6 eliminates any possibility of IP address depletion.

IPv6 addresses are generally written in the following form. Each set of four x's represents a 16-bit hexadecimal field. Colons are used to separate the eight octets.

The hexadecimal numbers are not case-sensitive. For example, this is a valid IPv6 address: [\[address 1\] shown on screen](#).

As is the following: [\[address 2\] shown on screen](#)

XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
------	------	------	------	------	------	------	------

XXXX = 0000 through FFFF

$3.4 \times 10^{38} = 340,282,366,926,938,463,374,607,432,768,211,456$ IPv6 Addresses

2001:0:1234:0:0:C1C0:ABCD:876

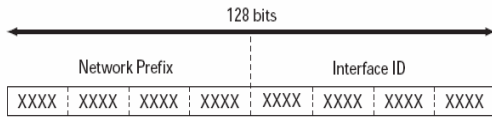
Voice-over text:

Additionally, **leading zeroes in a field can be compressed.** For example, "this" IPv6 address can also be written as follows:

2001:0:1234:0:0:C1C0:ABCD:876

IPv6 uses another important convention for shortening the IPv6 address to make it easier to represent: **successive fields of 0** are represented as a double colon. However, this is allowed only once in a valid IPv6 address.

For instance, the IPv6 address
2001:0:1234:0:0:C1C0:ABCD:876
 can be written as:
2001:0:1234::C1C0:ABCD:876
 but not as:
2001::1234::C1C0:ABCD:876.

**Voice-over text:**

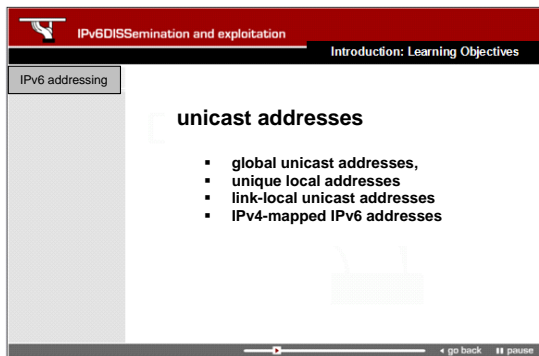
An IPv6 address can be expressed in the following format: **IPv6 address/prefix length**, in the same way an IPv4 address is represented in the "classless interdomain routing", or CIDR, notation [pronounce as 'cider']. For instance, **this**: [ause, address (1) is shown on screen] is an acceptable IPv6 prefix.

The prefix **length** is a decimal value that represents how many of the left most contiguous bits of the address comprise the prefix.

The IPv6 prefix itself can characterize a group of addresses and is also used to identify a network, such as a link, a site or even an Internet Service Provider network.

A link generally has a 64 bits long prefix, while a site generally has a 48 bits long prefix. In the latter case, 16 bits are allocated freely as a **subnet ID**, to build different subnets.

Click on one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'Next'.



The screenshot shows a presentation slide titled 'IPv6 addressing' with the subtitle 'Introduction: Learning Objectives'. The main content is 'unicast addresses' with a bulleted list:

- global unicast addresses,
- unique local addresses
- link-local unicast addresses
- IPv4-mapped IPv6 addresses

3. TYPES OF IPv6 ADDRESSES**Voice-over text:**

There is a major difference between the IP addressing of an IPv4 node and an IPv6 node. An IPv4 node typically has one IP address; but an IPv6 node generally has more than one IP address.

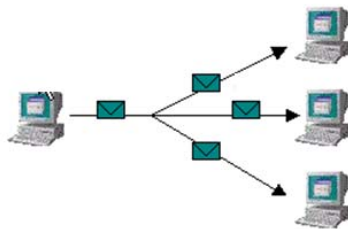
There are three major types of IPv6 addresses: **unicast**, **multicast** and **anycast**.

An IPv6 **unicast address** identifies a single interface. A packet that is sent to a unicast address is delivered to the interface identified by that address. The 64 lower bits of an IPv6 unicast address represent the **interface identifier** or IID.

IPv6 unicast addresses can be divided into four types:

- global unicast addresses,
- unique local addresses or ULAs
- link-local unicast addresses;
- and, finally, IPv4-mapped IPv6 addresses.

Additionally, there are **'special' unicast addresses**, such as the **unspecified address** and the **loopback address**.

**Voice-over text:**

An IPv6 **anycast address** identifies a set of interfaces that typically belong to different nodes. A packet sent to an **anycast address** is only delivered to the closest interface that is identified by the anycast address. Which interface is closest is determined by the routing protocols in use. This allows a node to trace the nearest server, for instance when searching a DNS server nearby.

An IPv6 **multicast address** is an identifier for a "set" of interfaces that typically belong to different nodes. A packet sent to an IPv6 **multicast address** is delivered to all host's interfaces having subscribed to this multicast address. It is replicated in the nodes on the path between the sender and the multiple receivers. Multicast addresses are in **FF00::8 prefix**, [F, zero zero, double colon, slash, 8].

IPv6 does not make use of "broadcasts". Broadcast addresses decreased IPv4 network performance, as every node on a link had to process all broadcasts for that link, while most broadcasts were irrelevant to most nodes. .

**Animation (screenshot):****FF02:0:0:0:0:0:1****Voice-over text:**

The IPv6 solution for the broadcast problem is the implementation of the multicast address 'all nodes on link', which has the following form. This multicast address is used to replace the broadcasts that are absolutely necessary. In other cases, more limited multicast messages are used.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'Next'.

2.4. Module 3: The IPv6 Header

IPv6DISSemination and exploitation

Introduction: Learning Objectives

IPv6 header

Learning Objectives

- Describe the differences between the IPv4 and IPv6 header structure
- Name the changed and new IPv6 header fields
- Explain the IPv6 header fields functions and specifics

1. INTRODUCTION

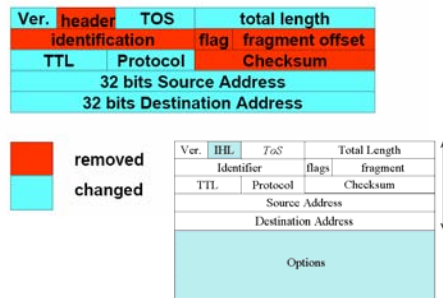
Voice-over text:

In this e-learning module about the IPv6 header, you will learn to **describe the differences between the IPv4 and the IPv6 header structure** and to **name the modified and the new IPv6 header fields**.

You will also learn to **explain the functions and specifics** of the IPv6 header fields.

Finally, after completion of this module, you will also be able to identify the seven different IPv6 **extension headers** and to describe their **functions**.

Click the "Next" button to continue.



2. STRUCTURE OF AN IPv6 PACKET

Voice-over text:

The **IPv6 header** is simpler and more efficient than the IPv4 header as it has a **fixed length** and a smaller number of fields. This enables **routing efficiency**, **higher performance** and **forwarding rate scalability**.

The **'Version Number'** field remains present and must be set to 6 to indicate an IPv6 packet. The **'Source Address'** and **'Destination Address'** fields are kept, except that both fields are **128-bits long** to embed the IPv6 addresses.

The **'options'** of IPv4 were part of the header. In IPv6 they have been replaced by a **chain of optional extension headers, positioned right after the IPv6 header**. **IPv6 extension headers** make it possible to implement options without decreasing performance, as it is no longer needed to have all routers capable of processing it. IPv6 extension headers will be detailed in a following part of this e-learning course.

Five other fields have been removed from the IPv4 header: The 'Header Checksum' disappeared, as link quality is now very high and other checksums are already performed at upper and lower layers.

The 'Header Length' has disappeared as the **header length** is fixed in IPv6. IPv6 also removed the three fields related to **data fragmentation** in IPv4: **Identification**, **Flags** and **Fragment Offset**. The fragmentation can be done with the use of the appropriate extension.

Figure 2: Comparison of IPv4 and IPv6 Headers

IPv4 Header				IPv6 Header			
Version	IHL	Type of Service	Total Length	Version	Traffic Class	Flow Label	
Identification		Flags	Fragment Offset	Payload Length		Next Header	Hop Limit
Time to Live	Protocol	Header Checksum		Source Address			
Source Address				Destination Address			
Destination Address				Options			
Options				Padding			

 Field name kept from IPv4 to IPv6
 Field not kept in IPv6
 Name and position changed in IPv6
 New field in IPv6

Voice-over text:

Four IPv4 header fields have been renamed and modified:

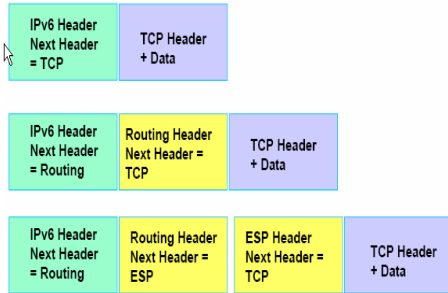
- the IPv4 'type of service' field has been replaced by the IPv6 **Traffic Class field**;
- the 'protocol type' field by the **Next Header field**;
- the 'total length' field by the **Payload Length field**;
- the 'Time To Live' field in the IPv4 header has been replaced by a **Hop Limit field** in the IPv6 header.

Finally, one field has been added. It is called the **'Flow Label'**.

As such, in contrast to IPv4's 13-field header, the IPv6 header only consists of 8 fields with a fixed length of 40 octets.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue with the e-learning course, click 'next'.

3. IPv6 EXTENSION HEADERS

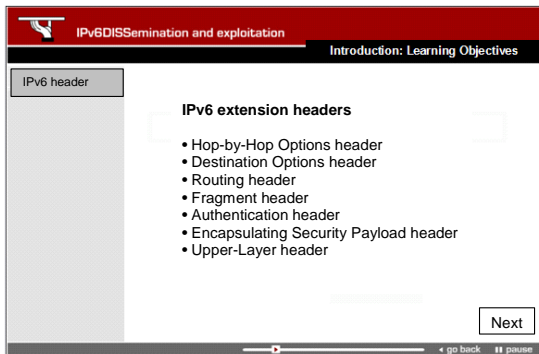


Voice-over text:

Contrary to IPv4, which defined options within the header, options in IPv6 are covered by extension headers. They can be inserted when needed, and are omitted if possible. The eight fields of the basic IPv6 header are followed by the optional extension headers and, next, by the data portion of the packet.

If present, each extension header is aligned to 64 bits. There is no fixed number of extension headers in an IPv6 packet. Together, the extension headers form a "chain of headers".

The "Next Header" field of the previous header identifies the extension header. Typically, the final extension header has a Next Header field of a transport layer protocol, such as TCP or UDP.



Voice-over text:

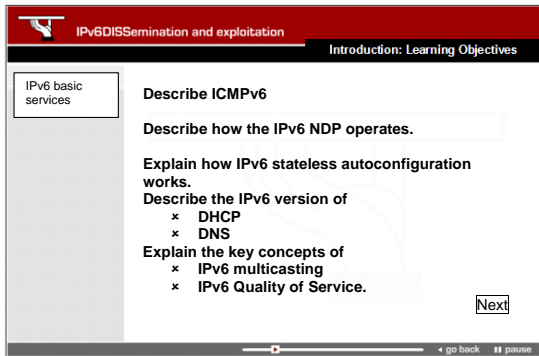
IPv6 extension headers are daisy-chained. When multiple extension headers are used in the same packet, the order of the headers should be as follows:

- first, the Hop-by-Hop Options header
- next, the Destination Options header
- followed by the Routing header
- next, the Fragment header
- followed by the Authentication header
- then the Encapsulating Security Payload header
- and finally, the Upper-Layer header

Alternatively, the Destination Options header can also be positioned here.

The source node should follow this header order, but destination nodes should be prepared to receive them in any order. Click one of the items on the screen for more details or test your understanding by clicking the 'Test' button. To continue with the e-learning course, click 'Next'.

2.5. Module 4: IPv6 Basic Services



1. INTRODUCTION

Voice-over text:

In this module, you will learn to identify the different IPv6 basic services.

On completion of this module, you will be able to **describe the Internet Control Message Protocol for IPv6**

Secondly, you will learn to **describe how the IPv6 Neighbour Discovery Protocol operates**. You will also be able to **explain how IPv6 stateless autoconfiguration works**.

Next, you will learn to describe the IPv6 versions of the Dynamic Host Configuration Protocol or **DHCP** and the Domain Name System or **DNS**.

Finally, you will also be able to explain the key concepts of IPv6 **multicasting and Quality of Service**.

Click the 'Next' button to continue.

2. ICMPv6

Voice-over text:

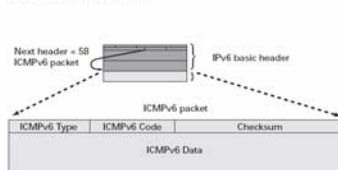
IP-nodes need a specific protocol for the transfer of messages related to IP conditions. This protocol, the **Internet Control Message Protocol**, or ICMP in short, is used for reporting fault- and information conditions and for diagnostic functions.

Generating error and information messages, ICMP in IPv6 basically functions the same as ICMP in IPv4. But additionally, **ICMP** packets in **IPv6** are used in the **IPv6 neighbour discovery** process, **IPv6 path MTU discovery**, and the **IPv6 Multicast Listener Discovery** or MLD protocol for IPv6.

ICMP packets in IPv6 are like a transport layer packet in the sense that the ICMP packet follows all the extension headers. These contain the **last pieces of information in the IPv6 packet**.

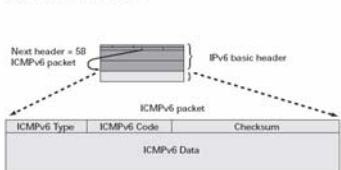
The ICMPv6 header is identified by a "Next Header" with a value of 58 in the immediately preceding header.

Figure 6: IPv6 ICMP Packet



Animation (screenshot):

Figure 6: IPv6 ICMP Packet



Voice-over text:

Within IPv6 ICMP packets, the **ICMPv6 Type and ICMPv6 Code fields** identify **IPv6 ICMP packet specifics**, such as the ICMP message type.

The value in the **Checksum field** is built from the fields in the IPv6 ICMP packet and the IPv6 header.

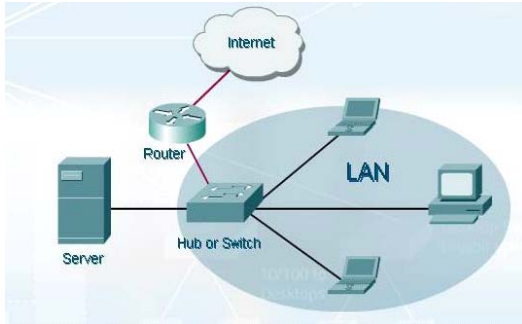
The ICMPv6 **Data field** contains error or diagnostic information relevant to IP packet processing.

Similar to ICMPv4, ICMPv6 is often blocked by security policies implemented in corporate firewalls because of ICMP based attacks. However, ICMPv6 is able to use **IPSec** authentication and encryption. These security services decrease the possibility of an attack based on ICMPv6.

The **ICMPv6 Type field** defines the Type of ICMPv6 message, such as : **destination unreachable**, **packet too big**, **time exceeded**, **parameter problem**, **echo request** or **echo reply**.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. Or click 'next' to continue.

3. NEIGHBOUR DISCOVERY



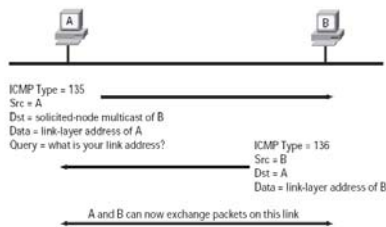
Voice-over text:

The IPv6 Neighbor Discovery protocol uses ICMPv6 messages and corresponds to an enhanced combination of the IPv4 protocols

- ARP,
- ICMP Router Discovery
- and ICMP Redirect.

[Nodes] such as [hosts] and [routers] use Neighbour Discovery to determine the link-layer addresses for neighbours known to reside on attached links and to quickly purge cached values that become invalid. Hosts also use Neighbour Discovery to find neighbouring routers that are willing to forward packets on their behalf. Finally, nodes use the protocol to actively keep track of which neighbours can be reached and which not, and to detect changed link-layer addresses.

Figure 14: Neighbor Solicitation Message



Voice-over text:

Neighbour discovery solves a set of problems related to the interaction between nodes attached to the same link. It defines mechanisms for solving the following problems:

- Router Discovery
- Prefix Discovery
- Parameter Discovery
- Address Autoconfiguration
- Address Resolution
- Next-hop Determination
- Neighbour Unreachability Detection
- Duplicate Address Detection
- [and]
- Redirect

To accomplish these tasks it uses five different ICMPv6 packet types

- Router Solicitation
- Router Advertisement
- Redirect messages
- Neighbour solicitation
- and Neighbour advertisement.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. Click 'next' to continue.

4. AUTOCONFIGURATION

Voice-over text:

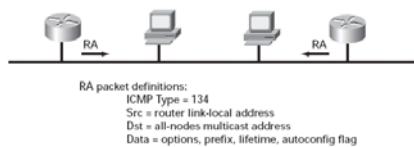
IPv6 defines both a stateful and **stateless** address autoconfiguration mechanism. Stateless autoconfiguration requires no manual configuration of hosts, minimal configuration of routers and no additional servers.

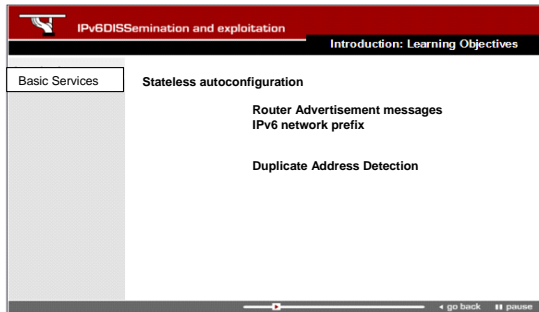
Stateless autoconfiguration is a key feature of IPv6, it allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. Stateless autoconfiguration simplifies **renumbering** in certain scenarios. It demands the local link supports multicast and the network interface is capable of sending and receiving multicast packets.

IPv6 nodes (hosts and routers) automatically create unique link-local addresses for all interfaces. IPv6 hosts use received **Router Advertisement** messages to automatically configure:

- x a default router.
- x the default setting for the Hop Limit field in the IPv6 header.
- x the timers used in Neighbour Discovery processes.
- x the maximum transmission unit or MTU of the local link.
- x and the list of network prefixes that are defined for the link.

Figure 15: Router Advertisement



**Voice-over text:**

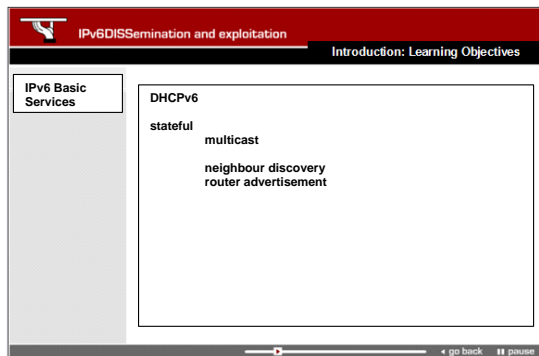
Each router advertisement message contains both the IPv6 **network prefix** and its valid and preferred **lifetimes**. If indicated, a **network prefix** is combined with the **interface identifier** to create a **stateless IPv6 address configuration** for the receiving interface.

This way, an IPv6 node can autoconfigure a globally unique IPv6 address by appending its link-layer address in EUI-64 format to the 64-bit local link prefix. The IPv6 node finally uses **DAD** or duplicate address detection to determine if the address is not already in use.

Router Advertisements contain two flags indicating what type of stateful autoconfiguration should be performed, if any. A "managed address configuration" flag indicates whether hosts should use stateful autoconfiguration to obtain addresses, or not.

An "other stateful configuration" flag indicates if hosts should use stateful autoconfiguration to obtain additional information, excluding addresses; such as the DNS server address. This is important because in stateless autoconfiguration there is no way of sending a DNS server address to clients.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. To continue, click 'next'.

5. DHCPv6**Voice-over text:**

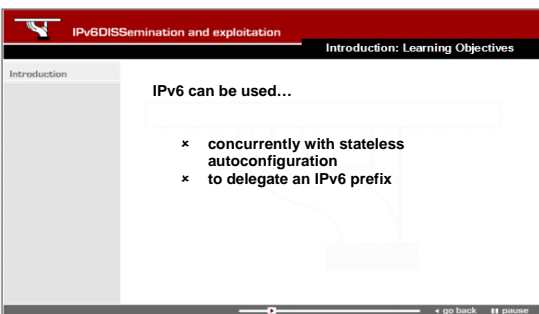
The **DHCP** for IPv6, DHCPv6, works in a **client/server model**. It enables DHCP servers to pass IPv6 addresses and other configuration parameters to IPv6 nodes. This protocol is a **stateful** counterpart to **IPv6 Stateless Address** [Autoconfiguration].

The process of acquiring configuration data for a client is similar to that in IPv4. However, DHCPv6 uses **multicast** for many of its messages. If a router is found, the client examines the **router advertisements** to determine if DHCP should be used. If the router advertisements enable use of DHCP or if no router is found, the client will contact the **DHCP server**.

Clients and servers exchange DHCP messages using UDP. DHCP servers receive messages from clients using a reserved, link-scoped multicast address, called **All_DHCP_Relay_Agents_and_Servers**. It has the **following form**: [address is shown on screen]

A DHCP client transmits most messages to this reserved multicast address. To allow a **DHCP client** to send a message to a DHCP server that is not attached to the same link, a **DHCP relay agent** on the client's link will relay messages between the client and server. The operation of the relay agent is transparent to the client.

The server optionally provides the client with IPv6 addresses and other configuration parameters, such as: DNS servers addresses, NTP servers addresses and other. But it isn't possible to send the default gateway address. This information must be obtained through stateless autoconfiguration.

**Voice-over text:**

DHCPv6 provides **more control than stateless autoconfiguration**, which sometimes is not appropriate. Different to DHCPv6, stateless autoconfiguration does not allow a network administrator to define admission control policies. With autoconfiguration, every host that connects to the network can get an IPv6 address assigned. In contrast, DHCPv6 servers provide means for **securing access control** to network resources by first **checking admission control policies** before replying to requests from clients.

Further benefits of DHCPv6 are the following:

- x it can be used **concurrently with stateless autoconfiguration**. For instance, you can get an IPv6 address from stateless autoconfiguration and the DNS server address from DHCPv6
- x Finally, it can be used to delegate an **IPv6 prefix** to customer-premise equipment or **CPE routers**.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. To continue, click 'Next'.

6. DNS

IPv6DISSemination and exploitation
Introduction: Learning Objectives

IPv6 basic services

Extensions made in DNS over the last years:

In use

- × AAAA record
- × PTR record (it's a similar record but with a different textual representation)
- × ip6.arpa
- × DNS queries

Experimental or deprecated

- × A6 and DNAME records
- × Binary Labels type
- × ip6.int domain

< go back || pause

Voice-over text:

The **Domain Name System** maps names to IP addresses (and vice-versa). DNS uses a hierarchic name space in which servers help to relate names to addresses at each hierarchic level. DNS was designed for processing 32-bit IPv4 addresses. Over the last few years some extensions have been made to make DNS compatible with IPv6, some extensions are still in use and others are already deprecated. In use are

- × the quad A record [[show AAAA record](#)],
- × the new textual representation in **PTR record**
- × ip6.arpa domain
- × and new DNS queries

Experimental or deprecated are

- × the **A6 and the DNAME records**,
- × **Binary Labels type**,
- × and **ip6.int domain**

It's not enough to have IPv6 records (AAAA) in the DNS contents, but it is also very important to issue queries and get DNS answers using the IPv6 transport layer. Of course, the data retrieved through IPv6 must be equal to the data retrieved using IPv4 in each given moment. Regarding the DNS root servers, only some of them can be reached through an IPv6 transport.

IPv6DISSemination and exploitation
Introduction: Learning Objectives

IPv6 basic services

PTR record

2.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.arpa PTR
www.organisation.com

< go back || pause

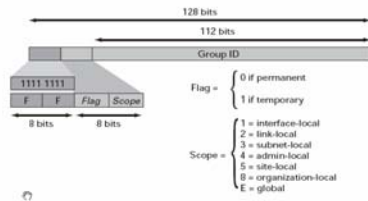
Voice-over text:

- × The **quad A record** maps a host name to an IPv6 address. This record is equivalent to an A record in IPv4 and uses the following format [[shown on screen](#)]. The IETF has decided to use this record for [host name-to-IPv6 address resolution](#).
- × The **PTR record** is equivalent to a pointer record that specifies address-to-host name mappings. **Inverse mapping** used in **IP address-to-host name look-up** uses the PTR record. PTR records storing IPv6 addresses use the following format: [[shown on screen](#)].
- × A special domain was defined to look up a record that was given an IPv6 address. The intent of this domain is to provide a way of mapping an IPv6 address to a host name, although it may be used for other purposes as well. The domain is rooted at **IP6.ARPA**.
- × Finally, existing **DNS queries** were revised so they were able to localise and process not only IPv4 addresses, but also IPv6 addresses.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. To continue, click 'next'.

7. MULTICASTING

Figure 12: IPv6 Multicast Address Format



Voice-over text:

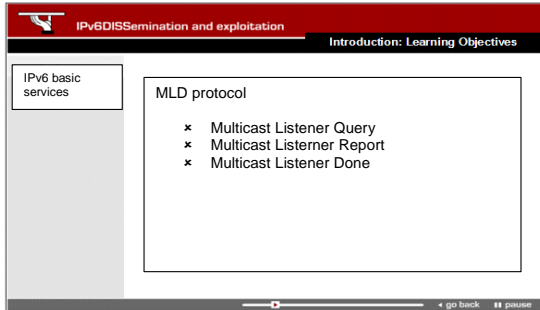
Multicasting is used mainly by the **new multimedia applications**. These often require **high bandwidth** to transmit certain data from a single source to many recipients. IPv6 uses **specific multicast addresses** for its various functions and uses a **4-bit Scope ID** to specify address ranges reserved for multicast addresses for each scope.

Thus, only **hosts** in a specified scope address range configured to listen to a specific multicast address receive the **multicast**. However, a host can be a member of several workgroups and can listen to several multicast addresses at the same time.

IPv6 provides a **larger range of multicast addresses** compared to IPv4. In other words, allocation of addresses for multicast groups will not be limited for the foreseeable future.

The major innovation introduced by IPv6 in the area of **multicasting** is this: all IPv6 implementations will have to include **native support** for this IP service right from the beginning. This is due to the introduction of the **scope field** in IPv6 addresses, together with the fact that multicasting management is no longer delegated to a separate protocol as it is in IPv4. The **MLD protocol**, in fact, is part of ICMPv6. MLD messages are identified in IPv6 packets by a preceding Next Header value of 58.

Animation (screenshot):

**Voice-over text:**

Under IPv4, moreover, several protocols for accomplishing multicast routing are defined, while IPv6 will rely entirely on a new version of the [PIM protocol](#).

Multicast Listener Discovery or MLD protocol can be used by an IPv6 router to discover the presence of multicast listeners on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighbouring nodes. This information is then provided to the PIM Protocol, in order to ensure that multicast packets are delivered to all links where there are interested receivers.

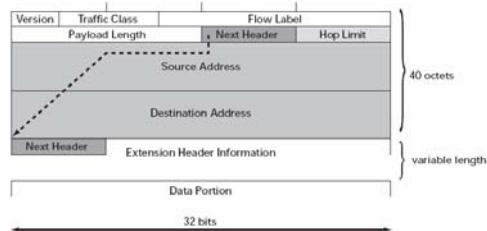
Three types of MLD messages exist, each one distinguished by the value in the type field:

- × [Multicast Listener Query](#)
- × [Multicast Listener Report](#)
- × and [Multicast Listener Done](#).

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'next'.

Animation (screenshot):

Figure 3: IPv6 Header Fields

**8. QoS: Quality of Service****Voice-over text:**

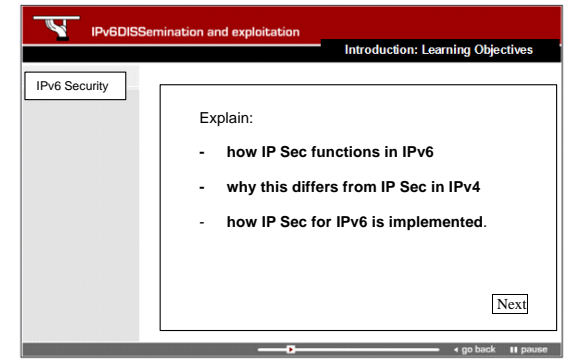
IPv6 offers extended possibilities in building **Quality of Service network architectures** that can carry **combined voice and data traffic** with minimum delay, jitter and packet loss. These possibilities are provided by two new fields in the IPv6 header: the [Traffic Class](#) and [Flow Label](#) fields.

The Traffic Class field lets the source host or the forwarding router identify the class or priority of the packet. And the 20-bit Flow Label field can be used to tag packets of a specific flow to differentiate the packets on the network layer. Hence, the Flow Label field enables **identification of a flow and per-flow processing by the routers in the path**. With this label, a router need not check deep into the packet to identify the flow because this [information is available in the IP packet header](#).

The Flow Label allows applications on the end system to easily [differentiate the traffic on the IP layer](#) making it easier to provide **Quality of Service** for packets that have been encrypted by [IPSec](#). For instance, a Quality of Service protocol such as the **Resource Reservation Setup Protocol** or [RSVP](#) can use the Traffic Class and Flow Label fields to conduct special handling, such as [real time video transmission](#). Click an interactive item for more details or 'next' to continue.

2.6. Module 5: Security in IPv6

1. INTRODUCTION



IPv6DISSemination and exploitation
Introduction: Learning Objectives

IPv6 Security

Explain:

- how IP Sec functions in IPv6
- why this differs from IP Sec in IPv4
- how IP Sec for IPv6 is implemented.

Next

← go back || pause

Voice-over text:

This module of the IPv6 e-learning course is about **IPv6 security**. Once you have completed it, you will be able to name the **specific security elements of IPv6**. Furthermore, you will be able to explain:

- × how the IP Security architecture **IP Sec functions in IPv6**,
- × why this differs from **IP Sec in IPv4**,
- × and how **IP Sec for IPv6 is implemented**.

2. IPv6 SECURITY ELEMENTS

XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
------	------	------	------	------	------	------	------

XXXX = 0000 through FFFF

$3.4 \times 10^{38} = \sim 340,282,366,926,938,463,374,607,432,768,211,456$ IPv6 Addresses

Voice-over text:

Because IPv6 offers globally unique addresses, it can provide **end-to-end security services** such as **access control, confidentiality and data integrity**. It does this without the need for additional firewalls that might introduce additional problems, including performance bottlenecks.

Due to the large IPv6 address space, network scanning for vulnerable systems is more complex in IPv6. Therefore, IPv6 could help to **reduce fast distribution of viruses, worms and spam**.

Additionally, IPv6 provides security extension headers, making it easier to implement **encryption, authentication**, and virtual private networks or **VPNs**.

IPv6 header	Extension header	ESP	Encrypted data
-------------	------------------	-----	----------------

Voice-over text:

The **IP security architecture** is called IPSec. It defines security services to be used in the IP layer of both IPv4 and IPv6.

IPSec protects all protocols in the TCP/IP suite and Internet communications by using **Layer Two Tunneling Protocol**.

IPSec implementation is optional in IPv4 but **mandatory in IPv6**. All full IPv6 implementations have to support IPSec.

In IPv6, IPSec is implemented using

- × the authentication extension header
- × and the ESP extension header,

Next header	Payload length	Reserved
SPI		
Sequence number		
Authentication Data (variable)		

SPI		
Sequence number		
Encrypted Data		
Authentication Data		

3. IPSec

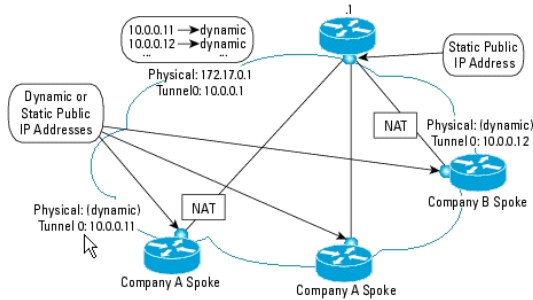
Voice-over text:

IPSec security services depend entirely on the mechanism of the authentication header and the encapsulating security payload header. These headers are defined for both IPv4 and IPv6. When used in IPv4, these security headers are added as options to the normal IPv4 header.

But while the use of IP Sec is optional in IPv4, it is **mandatory** in IPv6. In IPv6, IPSec is **part of the IPv6 protocol suite**. Therefore, network implementers should enable IPSec in every IPv6 node, potentially making the network more secure.

IPSec provides the following **optional network security services**:

- × first, **data confidentiality**: the IP sender can encrypt packets before sending them across a network
- × secondly, **data integrity**: the IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission
- × next, **data origin authentication**: the IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- × finally, **antireplay**: the IPSec receiver can detect and reject replayed packets.



Voice-over text:

With IPSec, data can be sent across a public network without observation, modification, or spoofing. IPSec functionality is essentially identical in both IPv6 and IPv4. However, IPSec in IPv6 can be deployed from **end-to-end**. Data may be encrypted along the entire path between a source node and a destination node.

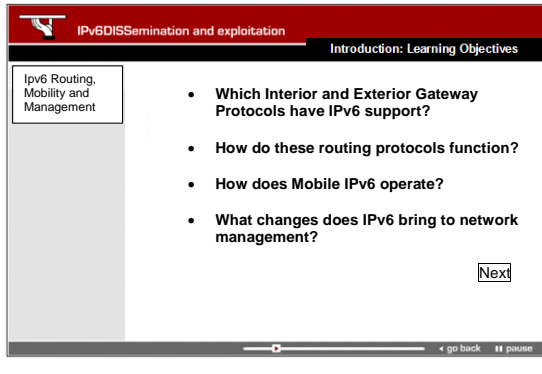
The **security of IPSec** for IPv6 is comparable to IPSec for IPv4. The IPSec functionality resides on the same protocol layer and the IPSec protocol specification, the algorithms and cryptography to be used are the same. Therefore, there is no major difference between IPSec for IPv6 and IPSec for IPv4.

However, **NAT or Network Address Translation boxes** in IPv4, modify IP packets. Therefore, they break end-to-end transparency. This modification also breaks end-to-end IP Sec. Due to the **disappearance of NAT boxes** in IPv6, large scale Deployment of IPSec will be easier in IPv6.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'next'.

2.7. Module 6: IPv6 Routing, Mobility and Management

1. INTRODUCTION



IPv6 Routing, Mobility and Management

Introduction: Learning Objectives

- Which Interior and Exterior Gateway Protocols have IPv6 support?
- How do these routing protocols function?
- How does Mobile IPv6 operate?
- What changes does IPv6 bring to network management?

Next

Voice-over text:

Welcome to this module about IPv6 routing, mobility and management.

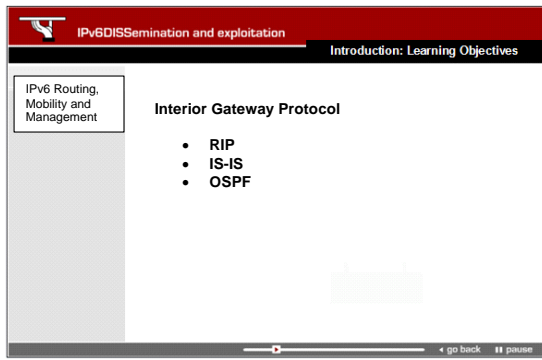
At the end of this module you will be able to list the **Interior and the Exterior Gateway Protocols** that have built-in IPv6 support. You will also be able to explain how these routing protocols function.

Also, you will be able to describe **Mobile IPv6** and to explain its operation.

Finally, you will be able to describe the changes that IPv6 brings to **network management**.

Click the 'Next' button to continue.

2. ROUTING PROTOCOLS



IPv6 Routing, Mobility and Management

Introduction: Learning Objectives

Interior Gateway Protocol

- RIP
- IS-IS
- OSPF

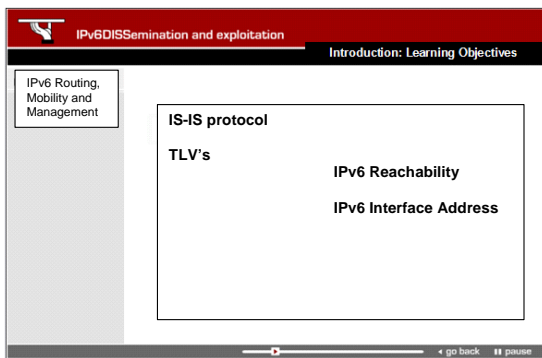
Voice-over text:

To enable scalable routing, IPv6 supports existing **Interior Gateway Protocols**, or IGPs, and **Exterior Gateway Protocols**, or EGPs for short. The longest prefix match is the basis for routing algorithms in IPv6, exactly like in IPv4.

An IGP or **Interior Gateway Protocol** is an Internet protocol which distributes routing information among routers or gateways within an autonomous system.

The most commonly used IGPs are:

- the **Routing Information Protocol**, known as **RIP** [*read: "rip"*]
- the **IS-IS** protocol, which stands for **Intermediate System to Intermediate System** Protocol
- and **OSPF**, or **Open Shortest Path First** Protocol.



IPv6 Routing, Mobility and Management

Introduction: Learning Objectives

IS-IS protocol

TLV's

- IPv6 Reachability
- IPv6 Interface Address

Voice-over text:

For IPv6, the **RIP** protocol has been extended to what is called "RIPng" [*read: rip-N-G*], which stands for "**Routing Information Protocol Next-Generation**". This protocol works in the same way and offers the same benefits as RIP version 2 in IPv4. IPv6 enhancements to RIP include **support for IPv6 addresses and prefixes**, such as "next hop IPv6 addresses".

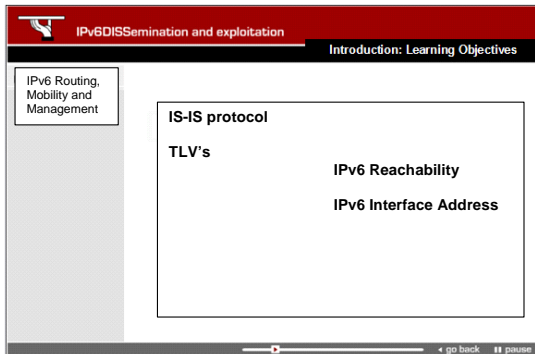
RIPng uses the "all-RIP routers" multicast group address **FF02::9** [*read: F-F-O-2-9*], as the destination address for RIP update messages. RIPng uses IPv6 as the transport layer for the protocol messages.

IS-IS is an IGP routing protocol. The new IPv6 routing capability has been added to the existing **IS-IS** protocol.

Exchanging IPv6 routing information using the **IS-IS** routing protocol is accomplished by adding 2 new type-length-values, or **TLVs**:

- « **IPv6 Reachability** » and
- « **IPv6 Interface Address** ».

A **new IPv6 protocol identifier** has also been added to IS-IS.


Voice-over text:

For IPv6, the **RIP** protocol has been extended to what is called "RIPng" [read: *rip-N-G*], which stands for "**R**outing **I**nformation **P**rotocol **N**ext-**G**eneration". This protocol works in the same way and offers the same benefits as RIP version 2 in IPv4. IPv6 enhancements to RIP include **support for IPv6 addresses and prefixes**, such as "next hop IPv6 addresses".

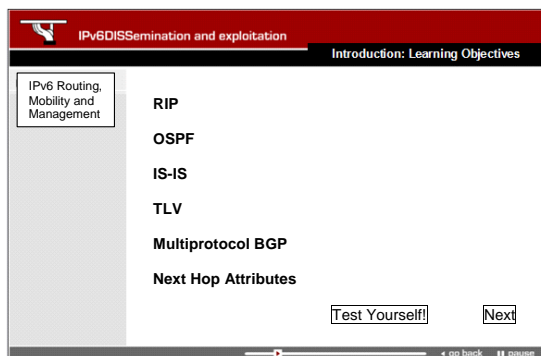
RIPng uses the "all-RIP routers" multicast group address **FF02::9** [read: *F-F-O-2-9*], as the destination address for RIP update messages. RIPng uses IPv6 as the transport layer for the protocol messages.

IS-IS is an IGP routing protocol. The new IPv6 routing capability has been added to the existing **IS-IS** protocol.

Exchanging IPv6 routing information using the **IS-IS** routing protocol is accomplished by adding 2 new type-length-values, or [TLVs]:

- « **IPv6 Reachability** » and
- « **IPv6 Interface Address** ».

A **new IPv6 protocol identifier** has also been added to IS-IS.


Voice-over text:

An **EGP** or **Exterior Gateway Protocol** is a protocol which distributes routing information among border routers of different autonomous systems.

Multiprotocol Border Gateway Protocol is a multiprotocol EGP which became the standard in the IPv4 and IPv6 Internet.

Only three pieces of information carried by BGP are **IPv4 specific**:

- the **NEXT_HOP** attribute, which is expressed as an IPv4 address,
- **AGGREGATOR**, which contains an IPv4 address),
- and **NLRI**, which is expressed as IPv4 address prefixes).

In other words, to provide backward compatibility, as well as simplify the introduction of the multiprotocol capabilities into BGP-4, two new optional attributes were created:

- Multiprotocol Reachable NLRI (MP_REACH_NLRI)
- and Multiprotocol Unreachable NLRI

The first one (niet lezen: MP_REACH_NLRI) is used to carry the set of reachable destinations together with the next hop information to be used for forwarding to these destinations. The second one (niet lezen: MP_UNREACH_NLRI) is used to carry the set of unreachable destinations.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'Next'.

3. MOBILITY**Voice-over text:**

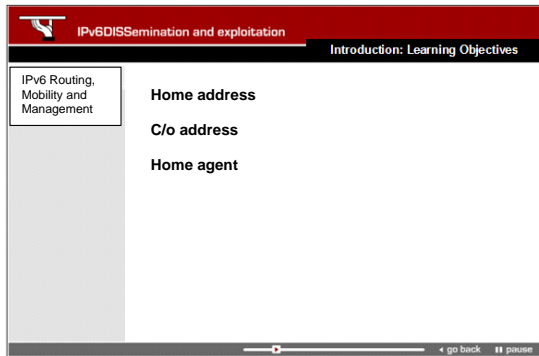
Mobile IP is an IETF standard that allows mobile devices to move around without breaking their existing connections. In IPv4, the mobility function must be added as a new feature. In IPv6, **mobility is built in** and any IPv6 node can use mobility as needed.

Mobile IPv6 is derived directly from Mobile IP, but it does not use IP encapsulation as in IPv4. In IPv6, the extension header for Mobile IP is used, more specifically the **Destination Options header**. This way, triangle routing is avoided. IPv6 mobility is thus much more efficient for end devices in IPv6.

Other **IPv6 innovations** have also significantly simplified procedures.

- × **Stateless autoconfiguration**,
- × the **Neighbour Discovery Protocol**
- × and the **authentication and encryption mechanisms**, ...

... make sure Mobile IPv6 will be much easier to implement and use than Mobile IPv4.



IPv6 Routing, Mobility and Management

Introduction: Learning Objectives

- Home address
- C/o address
- Home agent

← go back || pause

Voice-over text:

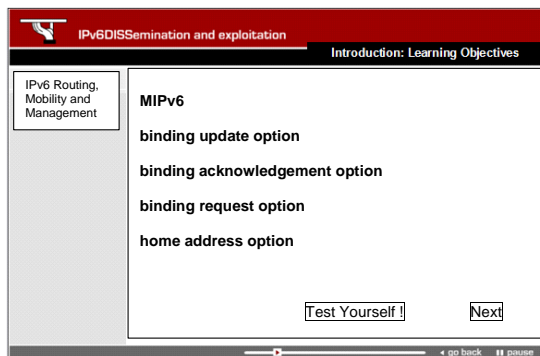
Mobile IPv6 will operate as follows:

A mobile host can change its access point to the Internet while still being reachable under its **home address**. The home address is the static IP address of the mobile host, valid at its home network.

IP packets addressed to the home address of a mobile node are transparently routed to its C/o- or **care-of address**. This is the temporary IP address of the mobile host, thus the IP address associated with a mobile node when it is visiting a particular subnet other than its own. Packets are routed from the home address to this care-of address by an entity called the **home agent**.

Mobile IPv4 tracks a moving host by registering the presence of the host with a foreign agent; the home agent then forwards packets to the remote network. With **IPv6, mobile IP has no foreign agent C/o- or care-of addresses**.

The association between or **binding** of the home address and the care-of address allows any packets destined for the mobile node to be directed to this care-of address. A **binding cache**, then, is a cache that retains previously acquired care-of addresses.



IPv6 Routing, Mobility and Management

Introduction: Learning Objectives

MIPv6

- binding update option
- binding acknowledgement option
- binding request option
- home address option

Test Yourself ! Next

← go back || pause

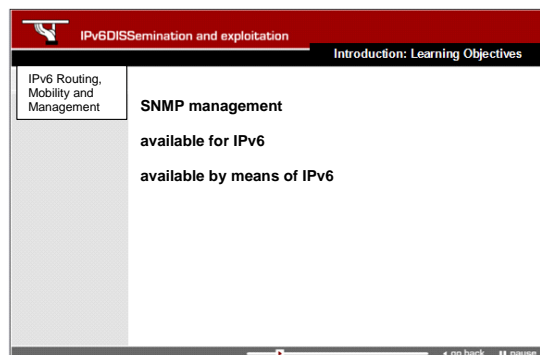
Voice-over text:

The care-of address is registered with the home agent using a **binding update message**, sent by the node to the home agent; and a **binding acknowledgement message**, sent by the home agent to the node in order to confirm the update.

To achieve this kind of host mobility, Mobile IPv6 defines four new IPv6 destination options:

- a binding update option
- a binding acknowledgement option
- a binding request option
- and a home address option

Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. To continue, click 'next'.

4. NETWORK MANAGEMENT


IPv6 Routing, Mobility and Management

Introduction: Learning Objectives

SNMP management

- available for IPv6
- available by means of IPv6

← go back || pause

Voice-over text:

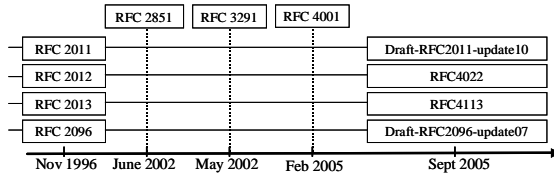
As the main management standard used for IPv4 networks is SNMP or Simple Network Management Protocol, an obvious goal to pursue was to make SNMP management also available for IPv6 and by means of IPv6.

Today many network vendors support SNMP over IPv6 and routers can be monitored in an IPv6-only environment. Equipment still not supporting SNMP over IPv6 can be managed over IPv4 as most IPv6 networks are running dual stack nowadays.

SNMP relies on **Management Information Bases** or MIBs. These MIBs also need to be able to collect IPv6 information. In **1998**, a **textual convention** was defined for IPv6 addresses only. This approach was chosen at the beginning of the IPv6 development. This made managing the IPv6 network without changing the existing MIBs possible.

For instance, in 1998, the **IPv6 MIB**, the **ICMPv6 MIB**, the **TCP over IPv6 MIB** and the **UDP over IPv6 MIB** were published. But this approach implied the partition of IPv4 and IPv6 MIBs. In other words, it would take double the effort to get all Management Information Bases ready for both versions of IP.

Animation (screenshot):

**Voice-over text:**

Fortunately, another approach is underway. It is based on a "unified MIB convention" where the same MIB can handle both IPv4 and IPv6. To be able to achieve this, the address data structure had to be changed again. Depending on the vendor, different MIB versions can be implemented.

SNMP is the most used protocol for **fault management**. However, network management covers many other aspects, including **accounting**. The **IPFIX standard** supports IPv6 **flow monitoring**. Moreover, certain proprietary protocols were updated to support IPv6 flow export. For example **Netflow v9** can export IPv6 flows.

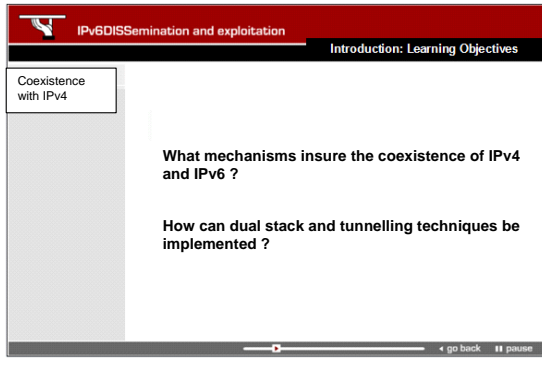
Configuration management can also be done over IPv6. The **TELNET**, **SSH**, **FTP** and **TFTP protocols** were updated and can be used to manage routers configuration over an IPv6-only network.

Even if IPv6 counters are not always updated and IPv6 network management still has missing components, because not all MIBs are being supported, there are **[emphasis: are]** plenty of tools capable of managing an IPv6 network. **Today, getting a good view at what is happening in an IPv6 network is possible.**

Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. To continue, click 'next'.

2.8. Module 7: Coexistence with IPv4

1. INTRODUCTION



Voice-over text:

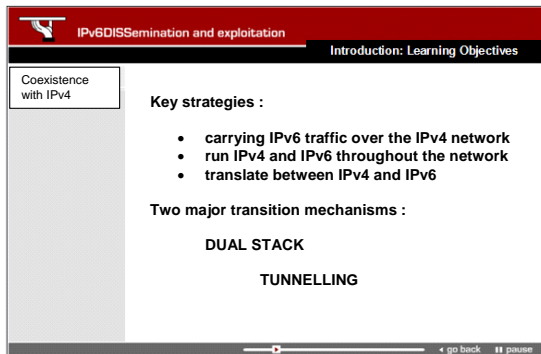
This module of the IPv6 e-learning course is about **IPv6 coexistence with IPv4**.

After completion of the module, you will be able to give an overview of **mechanisms** that can be used by network managers to **let the IPv6 protocol coexist with the IPv4 protocol**.

You will also be able to explain **how different dual stack and tunnelling techniques could be implemented**.

Click the 'next' button to continue.

2. TRANSITION AND COEXISTENCE MECHANISMS OVERVIEW



Voice-over text:

The Internet consists of **hundreds of thousands of IPv4 networks** and **millions of IPv4 nodes**. Any successful adoption of IPv6 will therefore be gradual. The challenge lies in making the integration and transition as transparent as possible to end users. It is expected that **IPv4 and IPv6 will coexist for a long time**.

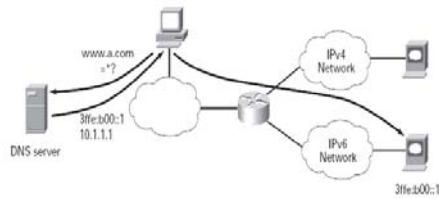
Network designers recommend **deploying IPv6** at the edge first and then **moving towards the network core** to reduce the cost and operational impacts of the integration.

The **key strategies** used in deploying IPv6 at the edge of a network involve **carrying IPv6 traffic over the IPv4 network**, allowing isolated IPv6 domains to communicate with each other before the full transition to a native IPv6 backbone.

It is also possible to run **IPv4 and IPv6 throughout the network**, from all edges through the core.

A third possibility is to **translate between IPv4 and IPv6**. This allows hosts to communicate transparently with hosts running the other protocol. All techniques allow networks to be upgraded and IPv6 deployed incrementally with little to no disruption of IPv4 services.

Networks can migrate to IPv6 gradually, using **two major transition mechanisms: dual stack and tunnelling**.

**Voice-over text:**

Tunnelling is a mechanism that has been defined to allow IPv6 packets to be encapsulated in IPv4 packets. All tunnelling mechanisms require that the endpoints of the tunnel run both IPv4 and IPv6 protocol stacks, that is, endpoints must run in dual-stack mode. These endpoints run both IPv4 and IPv6 protocols simultaneously and thus can communicate with both IPv4 and IPv6 systems and routers. A **dual-stack host** can send IPv6 packets through an IPv4 tunnel to a remote IPv6 host, without requiring an IPv6 infrastructure.

Deploying IPv6 over **dual-stack backbones** allows IPv4 and IPv6 applications to coexist in a dual IP layer routing backbone. All or most routers in a network must be upgraded to be dual stack, with IPv4 communication using the IPv4 protocol stack and IPv6 communication using the IPv6 stack.

Other transition strategies for the deployment of IPv6 are

- deploying IPv6 over [dedicated data links](#),
- deploying IPv6 over [MPLS backbones](#),
- and deploying IPv6 using [protocol translation mechanisms](#) such as [NAT-PT](#) or [ALG](#).

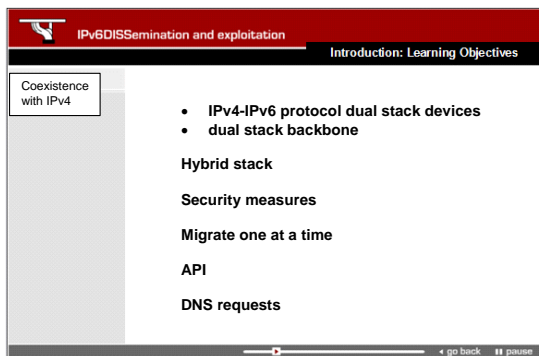
Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'next'.

3. DUAL-STACK TECHNIQUES**Voice-over text:**

IPv6 can be deployed using **IPv4-IPv6 protocol dual stack devices** or using a **dual stack backbone**. A network or backbone becomes dual-stack if the routers and switches building the network not only route and handle IPv4 but also route and handle IPv6.

Dual Stack is a method to **integrate IPv6 itself**. Therefore, no real transition mechanisms are needed. To make a node a dual stack node, one just has to **"switch on" IPv6**, on most platforms. This way the node becomes a **"hybrid stack"** host. Once IPv6 switched on, [security measures](#) must also be taken.

Dual-stack end systems allow applications to **migrate one at a time** from an IPv4 to an IPv6 transport. A new application-programming interface or [API](#) has been defined to support both IPv4 and IPv6 addresses and [DNS requests](#). This is the simplest and most desirable way for IPv4 and IPv6 to coexist, before a wider transition to an IPv6-only Internet can be achieved worldwide in the long term future.

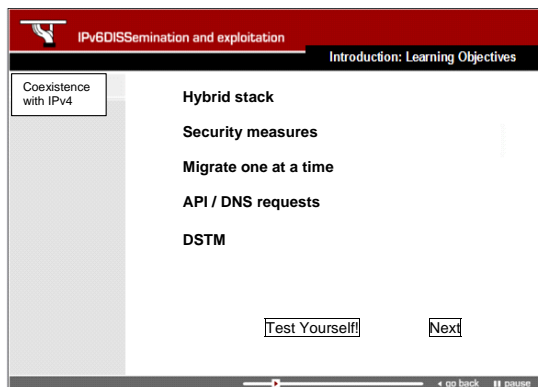

Voice-over text:

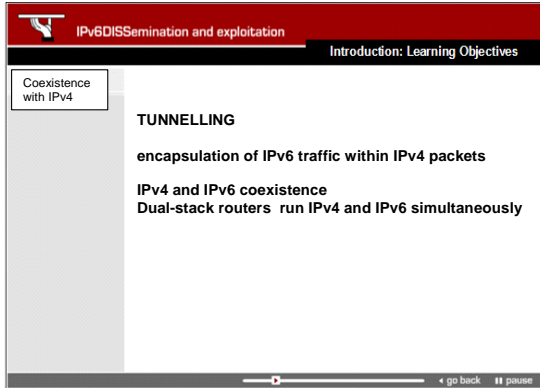
To deploy IPv6 using **dual stack backbone**, all routers in the network need to be upgraded to be dual stack. **IPv4 communication** uses the **IPv4 protocol stack** with forwarding of IPv4 packets based on routes learned through running **IPv4-specific routing protocols**, and **IPv6 communication** uses the **IPv6 stack** with routes learned through the **IPv6-specific routing protocols**.

Applications choose between using **IPv4 or IPv6**, based on the response from the **DNS resolver library**. The application selects the correct address based on the type of IP traffic and particular requirements of the communication. Dual-stack hosts that have not yet had an IPv4 address assigned, but need to communicate with IPv4 systems, can use a translation mechanism called [DSTM](#).

Today, **dual-stack routing** is a valid deployment strategy for specific network infrastructures with a mixture of IPv4 and IPv6 applications, requiring both protocols to be configured.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'next'.





IPv6DISSemination and exploitation
Introduction: Learning Objectives

Coexistence with IPv4

TUNNELLING

encapsulation of IPv6 traffic within IPv4 packets

IPv4 and IPv6 coexistence
Dual-stack routers run IPv4 and IPv6 simultaneously

← go back || pause

4. TUNNELLING TECHNIQUES

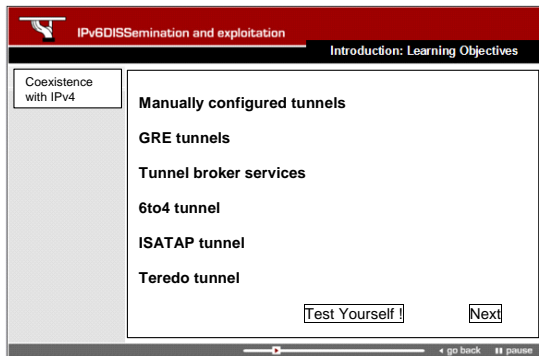
Voice-over text:

Tunnelling **encapsulates IPv6 traffic within IPv4 packets** so they can be sent over an IPv4 backbone, allowing isolated IPv6 end systems and routers to communicate without the need to upgrade the IPv4 infrastructure that exists between them. Tunnelling is one of the key deployment strategies during the period of **IPv4 and IPv6 coexistence**.

All tunnel mechanisms require that the endpoints of the tunnel run both IPv4 and IPv6 protocol stacks, that is, **endpoints must run in dual-stack mode**. **Dual-stack routers** running **IPv4 and IPv6** protocols **simultaneously** can thus interoperate directly with both IPv4 and IPv6 end systems and routers. For proper operation of the tunnel mechanisms, applications need appropriate entries in a **DNS**. This way, names and IP addresses for both IPv4 and IPv6 are mapped and the applications can choose the required address.

Tunnelling techniques include using

- x manually configured tunnels
- x generic routing encapsulation tunnels,
- x semiautomatic tunnel mechanisms such as tunnel broker services, and **fully automatic tunnel mechanisms**.



IPv6DISSemination and exploitation
Introduction: Learning Objectives

Coexistence with IPv4

Manually configured tunnels

GRE tunnels

Tunnel broker services

6to4 tunnel

ISATAP tunnel

Teredo tunnel

Test Yourself! Next

← go back || pause

Voice-over text:

Fully automatic tunnel services include:

- x the automatic 6to4 tunnel,
- x the intra-site automatic tunnel protocol or ISATAP tunnel
- x and the Teredo tunnel.

Manual tunnels are used between two points. They require configuration of both the source and destination address of the tunnel. **Automatic tunnel mechanisms** only need to be enabled and are more transient.

Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'next'.

3. Conclusion

The 6DISS e-learning package can be found at www.6diss.org/e-learning

This Deliverable has outlined the content of the 6DISS on-line IPv6 e-learning package that complements all of the other dissemination activities within the project. This professional interactive e-learning package explains to users the main features of IPv6 and guides them to the appropriate reference material (e.g. 6NET Cookbooks, IETF standards) if more information is needed. Tests are incorporated to assess whether the participant has understood the lessons. These tests can also be used to gauge the suitability of a person to attend the workshops.

The e-learning experience has the advantage that anyone connected to the Internet and able to find the 6DISS website has the possibility to access the 6DISS IPv6 e-learning package. The material will be actively promoted in the 6DISS target countries, but interested audiences anywhere in the world will be able to benefit from the e-learning course.

The technical level of the e-learning material assumes that participants have a networking background and a good basic understanding of TCP/IP concepts such as: IPv4 addressing, routing protocols, access lists, NAT, etc.

The typical profile of a target e-student is that of a network administrator, experienced in setting up an IP network environment. The approach within most of the e-learning modules is to compare the important aspects of IPv6 with those of IPv4.

After an initial module (Module 0) that describes the set of support and dissemination material that is available from 6DISS (ie. the Website, E-learning package, Workshops, Laboratories, Tiger Team, deliverables), and the role of e-learning within the whole dissemination framework, the e-learning package comprises the following technical modules. These are all based on - or aligned with - the workshop powerpoint slide sets:

Module 1: Introduction to IPv6

Module 2: IPv6 Addressing

Module 3: The IPv6 Header

Module 4: IPv6 Basic Services

Module 5: Security in IPv6

Module 6: IPv6 Routing, Mobility and Management

Module 7: Coexistence with IPv4

Every module contains the following:

1. A voice-over guided explanation of the subject
2. After every relevant piece of content: an interactive overview screen with clickable objects. Users can click keywords, objects, elements within a graph for further, text-based explanations
3. A series of self-test multiple choice questions based on the content which is explained

Ongoing work includes the translation of the key messages that appear as sub-titles throughout the e-learning package into the different languages of the target countries. The contents of the e-learning package will also be updated if any significant technical inaccuracies are discovered.