6DEPLOY Module 0: Introduction to the E-Learning Package

INTRODUCTION

This e-learning package is just one element of a comprehensive set of facilities provided by the 6DEPLOY project to **support the deployment of IP version 6**.

Other facilities offered by 6DEPLOY are:

- 3-day **Workshops** on site.
- **Training the Trainers** courses, in which we train people who can then give our workshops on their own.
- **IPv6 Training Courses**, either at one of our testbed sites or at your location.
- A so-called **"Tiger Team"** of experts who can give on-line support for any aspect of your IPv6 deployment.

Click "Next" to continue.

6DEPLOY Ενότητα 0: Εισαγωγή στην ενότητα ηλεκτρονικής εκμάθησης (e-Learning)

Εισαγωγή

Η παρούσα ενότητα ηλεκτρονικής εκμάθησης (e-learning) είναι ένα μόνο κομμάτι ενός ολοκληρωμένου συνόλου εργαλείων και δράσεων που αναπτύχθηκαν στο πλαίσιο του έργου 6DEPLOY για να υποστηρίξουν την εφαρμογή του πρωτόκολλου IP, έκδοση 6 (IPv6).

Τα υπόλοιπα εργαλεία και δράσεις που προσφέρονται από το έργο 6DEPLOY είναι:

- Τεχνικές ημερίδες, με διάρκεια μέχρι 3 ημέρες.
- Προγράμματα κατάρτισης για εκπαιδευτές, στα οποία εκπαιδεύουμε ανθρώπους που μπορούν να αναπαράγουν με ιδίους πόρους τις εκπαιδευτικές ημερίδες του έργου 6DEPLOY.
- Επιμορφωτικά μαθήματα για την τεχνολογία IPv6, είτε σε δικά μας εργαστήρια είτε στο χώρο των εκπαιδευόμενων.
- Τη αποκαλούμενη «Ομάδα Tiger» αποτελούμενη από εμπειρογνώμονες που μπορούν να δώσουν άμεση υποστήριξη για οποιαδήποτε πτυχή της ανάπτυξη του IPv6 από εσάς.

Πατήστε την επιλογή "Next" για να συνεχίσετε.

E-LEARNING PACKAGE

The 6DEPLOY e-learning package is an introduction to the 6DEPLOY 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 6DEPLOY workshop participants**

The e-learning package is **multimedia-based** and uses a combination of **voice-over,**

Ενότητα Ηλεκτρονικής Εκμάθησης (e-LEARNING)

Η ενότητα ηλεκτρονικής εκμάθησης περιλαμβάνει βασικές πληροφορίες για το διαθέσιμο περιεχόμενο σχετικά με το πρωτόκολλο IPv6 από το έργο 6DEPLOY και έχει δύο βασικούς στόχους:

- **την εισαγωγή του πρωτοκόλλου IPv6 σε μεγάλο, τεχνικά εξειδικευμένο, ακροατήριο (παγκοσμίως)**
- **να χρησιμεύσει ως ένα κίνητρο για την προετοιμασία των συμμετεχόντων σε πιθανές τεχνικές εκδηλώσεις του έργου 6DEPLOY.**

animation and interaction. The typical user experience of the e-learning material will last about 2 to 3 hours, depending on the user's background. A big advantage of the e-learning package is that **anyone connected to the Internet and able to find the 6DEPLOY website can access the 6DEPLOY IPv6 e-learning material**. The e-learning package is aimed at people with a networking background and a good basic understanding of Internet concepts such as: IPv4 addressing, routing protocols, access control 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 in most of the e-learning modules is a **comparison of IPv6's important aspects with those of IPv4**.	Η ενότητα ηλεκτρονικής εκμάθησης (e-learning) βασίζεται σε **πολυμέσα** και χρησιμοποιεί ένα συνδυασμό **φωνής, κινούμενου σχεδίου (animation)** και **αλληλεπίδρασης**. Η τυπική εμπειρία του χρήστη του υλικού ηλεκτρονικής εκμάθησης θα διαρκέσει περίπου 2 με 3 ώρες ανάλογα με το γνωστικό υπόβαθρο του. Ένα μεγάλο πλεονέκτημα της ενότητας ηλεκτρονικής εκμάθησης είναι ότι **οποιοσδήποτε που έχει πρόσβαση στο διαδίκτυο και είναι σε θέση να προσπελάσει τον ιστότοπο του έργου 6DEPLOY μπορεί ταυτόχρονα να έχει πρόσβαση το υλικό ηλεκτρονικής εκμάθησης σχετικά με το πρωτόκολλο IPv6**. Η ενότητα ηλεκτρονικής εκμάθησης απευθύνεται σε ανθρώπους με γνώσεις σε δίκτυα υπολογιστών, και με βασική κατανόηση των εννοιών του διαδικτύου, όπως: διευθυνσιοδότηση IPv4 (δηλ. IPv4 addressing), πρωτόκολλα δρομολόγησης, λίστες ελέγχου πρόσβασης, NAT, κλπ. **Το τυπικό προφίλ των χρηστών που προσπαθούμε να προσεγγίσουμε με το στο σύστημα ηλεκτρονικής εκμάθησης περιλαμβάνει διαχειριστές δικτύων, με εμπειρία στη δημιουργία δικτύων IP**. Η προσέγγιση που ακολουθούμε στις περισσότερες από τις ενότητες ηλεκτρονικής εκμάθησης αφορά **τη σύγκριση των σημαντικών πτυχών του πρωτοκόλλου IPv6 με εκείνες του πρωτοκόλλου IPv4**.

WORKSHOPS

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

We have presentation material on all aspects of IPv6; more specifically:

- **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 you how to **configure devices on site**, or by accessing, remotely, one of our purpose-built laboratories.

Ημερίδες

Οι πληροφορίες σχετικά με το IPv6 θα διαδοθούν κυρίως μέσα από ημερίδες. Σε αυτές επιθυμούμε να δοθεί δημοσιότητα, να επιτραπεί η ανταλλαγή εμπειριών από την εφαρμογή του IPv6, να επιτευχθεί η ευρεία διάχυση αποτελεσμάτων των ευρωπαϊκών έργων, και να εξηγηθούν οι δραστηριότητες που σχετίζονται με την ανάπτυξη προτύπων και την επίλυση ζητημάτων διαλειτουργικότητας.

Έχουμε υλικό σε μορφή παρουσιάσεων για όλες τις πτυχές του IPv6, και πιο συγκεκριμένα για:

- **Πρωτόκολλο IPv6**
- **Υπηρεσία ονοματολογίας - DNS**
- **Διευθυνσιοδότηση (και τη διαχείριση των διευθύνσεων)**
- **Δρομολόγηση**
- **RPSLng**
- **Αυτόματη Διαμόρφωση (autoconfiguration)**
- **Multicast**
- **Ασφάλεια**
- **Κινητικότητα (mobility)**
- **Ποιότητα Παροχής Υπηρεσιών (QoS)**
- **Συνύπαρξη με το πρωτόκολλο IPv4**
- **Διαχείριση δικτύων**

Στις τεχνικές ημερίδες θα σας δείξουμε πώς **να ρυθμίσετε δικτυακές συσκευές που λειτουργούν στο χώρο της εκπαίδευσης** ή είναι προσβάσιμες από μακριά στα ειδικά διαμορφωμένα εργαστήρια μας.

TRAINING THE TRAINERS

Due to time and budget constraints, 6DEPLOY cannot provide an unlimited number of workshops. However, 6DEPLOY is able to offer a **Training the Trainers** facility, allowing

Προγράμματα Κατάρτισης Εκπαιδευτών

Λόγω περιορισμών στο διαθέσιμο χρόνο και προϋπολογισμό, το έργο 6DEPLOY δεν μπορεί να οργανώσει απεριόριστο αριθμό τεχνικών ημερίδων. Ωστόσο, το

trainers to further disseminate the information. They will be given the full set of material, guidelines for presenting the modules, additional notes to accompany the slides, and a list of key messages to get across to participants. The training can be given either at one of our testbed sites or at a local location; ideally immediately prior to or directly following a workshop. This facility can be particularly useful when: ▪ regions wish to **take advantage of the 6DEPLOY material, independently from the workshops**. ▪ Or people in the targeted regions wish to have some **training prior to the workshop**. The facility will also be available to: • **people who were not able to attend the workshop,** due to high travel costs or other constraints. • and for **local organisations who; in their region; wish to run several more workshops themselves** due to the success of a previous workshop,. Finally, the 'Training the Trainers' facility will be useful when a specific workshop, **generates interest in some of the other 6DEPLOY topics** such as specialist programmes for Network Operation Centres, ISPs, or regulators.	6DEPLOY είναι σε θέση να προσφέρει ένα **πρόγραμμα κατάρτισης για εκπαιδευτές**, επιτρέποντας τους την περαιτέρω διάδοση των πληροφοριών. Στους καταρτισμένους εκπαιδευτές θα δοθεί το σύνολο του υλικού, οι κατευθυντήριες γραμμές για την παρουσίαση των ενοτήτων, συμπληρωματικές σημειώσεις που θα συνοδεύουν τις διαφάνειες, καθώς και κατάλογος των βασικών μηνυμάτων που θα πρέπει να μεταδοθούν στους συμμετέχοντες μιας ημερίδας. Η εκπαίδευση μπορεί να πραγματοποιηθεί είτε σε ένα από τα εργαστήριά μας ή σε ένα τοπικό εργαστήριο. Ιδεατό θα ήταν η εκπαίδευση να δοθεί πριν ή αμέσως μετά από μια ημερίδα. Αυτή η δυνατότητα μπορεί να αποδειχθεί ιδιαίτερα χρήσιμη στις ακόλουθες περιπτώσεις: • σε περιοχές που επιθυμούν **να επωφεληθούν του υλικού 6DEPLOY, ανεξάρτητα από τις προγραμματισμένες ημερίδες.** • σε περιπτώσεις που οι άνθρωποι στις επιλεγμένες περιοχές επιθυμούν να έχουν **εκπαίδευση πριν από κάποια προγραμματισμένη ημερίδα.** Το πρόγραμμα κατάρτισης θα είναι επίσης διαθέσιμο: • **σε ανθρώπους που δεν μπόρεσαν να παρακολουθήσουν τις ημερίδες,** πιθανότατα λόγω του υψηλού κόστους μετακίνησης ή άλλων περιορισμών. • στις τοπικές οργανώσεις που στην περιοχή τους επιθυμούν να οργανώσουν οι ίδιες πολλές περισσότερες ημερίδες**, λόγω της επιτυχίας της προηγούμενης ημερίδας.** Τέλος, το πρόγραμμα κατάρτισης των εκπαιδευτών θα είναι χρήσιμο όταν μία συγκεκριμένη ημερίδα δημιουργεί ενδιαφέρον για κάποια από τα άλλα θέματα που παρέχει το 6DEPLOY, όπως για παράδειγμα εξειδικευμένα προγράμματα για τα Κέντρα Λειτουργίας και Διαχείρισης Δικτύων, Πάροχους Υπηρεσιών Διαδικτύου (Internet Service Providers), ρυθμιστικές αρχές κλπ.

IPv6 TRAINING

To offer a more in-depth technical training on IPv6, 6DEPLOY has built 2 laboratories in Europe, one in Paris and the other in Sofia. A third lab is in Mauritius.

They can be accessed during the workshops for illustrations of equipment configuration, but the labs can also be used to provide a more in-depth training on specific aspects of IPv6.

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

The training course lasts 1 week and covers the same items as the workshops, but the focus will be on hands-on practical examples. Cisco, Alcatel and Juniper equipment will be available.

Εκπαίδευση IPv6

Για να συνεισφέρει στην εκ βαθέων τεχνική κατάρτιση σχετικά με το πρωτόκολλο IPv6, το έργο 6DEPLOY έχει χτίσει δύο εργαστήρια (labs) στην Ευρώπη, έναν στο Παρίσι και το άλλο στη Σόφια. Ένα τρίτο εργαστήριο είναι διαθέσιμο στο Μαυρίκιο.

Τα εργαστήρια μπορούν να χρησιμοποιηθούν κατά τη διάρκεια των ημερίδων για την καλύτερη κατανόηση της διαμόρφωσης του εξοπλισμού, αλλά και για να παρέχουν μια πιο εξειδικευμένη εκπαίδευση σε συγκεκριμένες πτυχές του πρωτοκόλλου IPv6.

Αυτό το πρόγραμμα εκπαίδευσης είναι ιδιαίτερα κατάλληλο για τους μηχανικούς και τους διαχειριστές δικτύων, ιδιαίτερα για όσους προέρχονται από Πάροχους Υπηρεσιών Διαδικτύου (ISPs).
Το εκπαιδευτικό πρόγραμμα διαρκεί μία εβδομάδα και καλύπτει τα ίδια στοιχεία με τις ημερίδες αλλά η εστίαση θα είναι σε πρακτικά παραδείγματα. Εξοπλισμός από τους κατασκευαστικούς οίκους Cisco, Juniper, και Alcatel θα είναι διαθέσιμος.

TIGER TEAM

The Tiger Team offers support for IPv6 network deployers.

This team of experts is on hand 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 support include:

- giving advice on aspects of transition to - or coexistence with - IPv6
- the creation and maintenance of a website that provides information about the state of the art in IPv6 deployment. This IPv6 website assists visitors in their

Ομάδα Tiger

Η «Ομάδα Tiger» προσφέρει υποστήριξη σε όσους εγκαθιστούν IPv6 στο δίκτυό τους.
Αυτή η ομάδα εμπειρογνωμόνων είναι σε ετοιμότητα για να απαντήσει σε ερωτήσεις μέσω ηλεκτρονικού ταχυδρομείου (e-mail) και διατηρεί μια λίστα από Συχνές Ερωτήσεις (Frequent Asked Questions - FAQ) σχετικά με τη διαμόρφωση του εξοπλισμού, απαιτήσεις σε υλικό (hardware) ή λογισμικό (software), RFC, κλπ.

Παραδείγματα υποστήριξης περιλαμβάνουν:

- τη παροχή συμβουλών σχετικά με ζητήματα συνύπαρξης πρωτοκόλλων IPv4 και IPv6 (ή μετάβασης στο πρωτόκολλο IPv6)
- τη δημιουργία και διατήρηση μιας ιστοσελίδας που παρέχει πληροφορίες σχετικά με την τρέχουσα κατάσταση στην ανάπτυξη του IPv6. Αυτή η

deployment of IPv6, by: o receiving and publishing relevant information o offering a discussion forum for specific technology; such as hosts or routers o documenting answers to specific technology questions ▪ providing details of applications ▪ providing fact sheets on IPv6 deployment, such as IPv6 VPN or DHCPv6 ▪ interfacing and assisting national IPv6 Task Forces and IPv6 Fora	ιστοσελίδα βοηθά τους επισκέπτες στην ανάπτυξη του IPv6 με τους εξής τρόπους: o τη λήψη και δημοσίευση των σχετικών πληροφοριών, o την παροχή ενός φόρουμ συζήτησης για την συγκεκριμένη τεχνολογία, όπως για την υποστήριξη IPv6 σε τελικά συστήματα και δρομολογητές o την τεκμηριωμένη απάντηση σε συγκεκριμένες τεχνικές ερωτήσεις • την παροχή λεπτομερειών για εφαρμογές, • την παροχή ενημερωτικών δελτίων για την εισαγωγή του IPv6, όπως το «IPv6 VPNs» ή «DHCPv6», • τη διασύνδεση και υποβοήθηση των Εθνικών Ομάδων Δράσης IPv6 και σχετικών φόρουμ.

6DEPLOY Module 1: Introduction to IPv6.	**6DEPLOY Ενότητα 1: Εισαγωγή στο IPv6.**
Welcome to this e-learning course about **IP version 6.**	Καλώς ήλθατε σε αυτή την ενότητα ηλεκτρονικής εκμάθησης (e-learning) για το πρωτόκολλο **IP, έκδοση 6**.
IP version 6, or IPv6 for short, is a new version of the Internet Protocol designed to replace IPv4, the Internet protocol that is predominantly deployed and extensively used throughout the world.	IP έκδοση 6, ή εν συντομία IPv6, είναι η νέα έκδοση του Πρωτοκόλλου Διαδικτύου (Internet Protocol) που σχεδιάστηκε για να αντικαταστήσει το IPv4, το πρωτόκολλο που χρησιμοποιείται ευρέως σε όλο τον κόσμο.
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.	Αν και **η εξάντληση του διαθέσιμου χώρου διευθύνσεων IPv4** ήταν ο κύριος λόγος για την ανάπτυξη ενός νέου πρωτοκόλλου, οι σχεδιαστές του πρωτοκόλλου IPv6 **έχουν προσθέσει αρκετές νέες λειτουργικές δυνατότητες** και **μια σειρά από κρίσιμες βελτιώσεις στο πρώτοκολλο 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.	Το παρόν πρόγραμμα ηλεκτρονικής εκμάθησης καλύπτει αυτές τις πτυχές σε μια σειρά από ενότητες που περιλαμβάνουν τομείς όπως η διευθυνσιοδότηση (addressing), autoconfiguration και τη συνύπαρξη των πρωτοκόλλων IPv4 και IPv6.
In this Introduction module, you will learn **why a new IP protocol** is needed and what the advantages are of **IPv6**.	Σε αυτή την εισαγωγική ενότητα θα μάθετε **γιατί ένα νέο πρωτόκολλο IP είναι αναγκαίο,** και ποια είναι **τα πλεονεκτήματα του IPv6**.
Click the “Next” button to continue.	Πατήστε την επιλογή "Next" για να συνεχίσετε.

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.	Το IPv4 έχει αντέξει με επιτυχία στην αύξηση της διασύνδεσης σε μια παγκόσμια υποδομή με το μέγεθος του σημερινού διαδικτύου. Όμως, το IPv4 δεν είχε αρχικά σχεδιαστεί για να υποστηρίζει ένα μεγάλο αριθμό δικτυακών συσκευών.
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.	Λόγω της πρόσφατης εκθετική αύξηση του διαδικτύου, το IPv4 δεν είναι σε θέση να ικανοποιήσει τις δυνητικά τεράστια αύξηση στον αριθμό των χρηστών ή την ανάγκη γεωγραφικής επέκτασης του Διαδικτύου.
As a result, **IPv4 address depletion** is approaching quickly.	Ως αποτέλεσμα, **η εξάντληση των διαθέσιμων IPv4 διευθύνσεων** πλησιάζει γρήγορα.
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.	Επιπλέον, νέες συσκευές, όπως PDAs (personal digital assistances) που συνδέονται στο διαδίκτυο, τοπικά δίκτυα στις οικίες (home area networks), κινητά δίκτυα ad hoc, ασύρματα υπηρεσίες πάνω από IP και ολοκληρωμένες υπηρεσίες τηλεφωνίας πάνω από IP απαιτούν ένα νέο πρωτόκολλο διαδικτύου.
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.	Η διάρκεια ζωής του IPv4 έχει επεκταθεί με τη χρήση τεχνικών όπως η επαναχρησιμοποίηση διευθύνσεων με τη χρήση των μεθόδων **Network Address Translation**, ή για συντομία NAT, **Classless Interdomain Routing**, ή εν συντομία CIDR, και την προσωρινή ανάθεση διευθύνσεων, όπως το πρωτόκολλο **Dynamic Host Configuration Protocol**, ή εν συντομία DHCP.
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.	Οι τεχνικές αυτές φαίνεται να αυξάνουν το χώρο διευθύνσεων και να ικανοποιούν τον παραδοσιακό μοντέλο επικοινωνίας μεταξύ εξυπηρετητή (server) και πελάτη (client). Παρόλα αυτά, το παραδοσιακό μοντέλο επικοινωνίας αποτυγχάνει να ανταποκριθεί στις απαιτήσεις των σύγχρονων δικτύων και στην κινητικότητα των χρηστών. Οι εφαρμογές απαιτούν να αυξηθεί το ποσό του εύρους ζώνης (bandwidth) ενώ η μετάφραση των διευθύνσεων (address translation) έχει επίδραση στην απόδοση του δικτυακού εξοπλισμού.
Next, the need for **always-on environments** to be contactable prohibits these IP address conversion, pooling, and temporary allocation techniques.	Στη συνέχεια, η ανάγκη για **περιβάλλοντα με δυνατότητα συνεχούς επικοινωνίας (always-on environments)** κάνει πρακτικά ανέφικτη τη χρήση τεχνικών μετατροπής των διευθύνσεων, συγκέντρωσης διευθύνσεων, και προσωρινής κατανομής

	διευθύνσεων IP..
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 version of the IP protocol** to provide **new and enhanced features** in addition to **solving the IP address exhaustion problem**. That new version of IP is **IPv6**.	Επιπλέον, η υποστήριξη λειτουργιών «**plug and play**» που απαιτούν οι ευρέων χρησιμοποιούμενες καταναλωτικές συσκευές **αυξάνουν περαιτέρω τις απαιτήσεις του πρωτοκόλλου**. Εκατομμύρια συσκευές νέας τεχνολογίας, όπως τα ασύρματα τηλέφωνα, PDAs, αυτοκίνητα και οικιακές συσκευές δεν θα είναι πια σε θέση να πάρουν μια παγκόσμια διεύθυνση IPv4. Το πρωτόκολλο IPv4 θα φτάσει σύντομα σε ένα σημείο όπου η επιλογή που πρέπει να ληφθεί θα απαιτεί είτε νέες δυνατότητες είτε ένα μεγαλύτερο δίκτυο, αλλά όχι και τα δύο. Με άλλα λόγια, χρειαζόμαστε **μια νέα έκδοση του πρωτοκόλλου IP** για την παροχή **νέων και βελτιωμένων λειτουργικών χαρακτηριστικών** πέρα από **την επίλυση του προβλήματος εξάντλησης των διευθύνσεων IP**. Η νέα έκδοση του IP είναι το **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.	Επιλέξτε ένα από τα στοιχεία που εμφανίζονται στην οθόνη για περισσότερες λεπτομέρειες. Διαφορετικά, για να δοκιμάσετε το βαθμό κατανόησής σας, πατήστε την επιλογή "test" ή πατήστε την επιλογή "Next" για να συνεχίσετε.
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.	Το IPv6 σχεδιάστηκε για να ικανοποιεί τις απαιτήσεις της δυνητικά τεράστιας επέκτασης του διαδικτύου. Θα επιτρέψει την δημιουργία ενός παγκόσμιου περιβάλλοντος όπου οι εφαρμογές θα χρησιμοποιούν ξανά με διαφάνεια (transparency) τους κανόνες διευθυνσιολόγησης του δικτύου. Μέσω της αυτόματης διαμόρφωσης (autoconfiguration) και της υποστήριξης της λειτουργίας plug-and-play, οι συσκευές θα είναι σε θέση να συνδεθούν στο δίκτυο χωρίς να απαιτούνται χειροκίνητες ρυθμίσεις ή υπηρεσίες εκκίνησης, όπως αυτές που προσφέρουν οι διακομιστές DHCP.
IPv6 succeeds in doing this by providing the following benefits to network and IT professionals:	Το IPv6 επιτυγχάνει τα παράπανω παρέχοντας τα εξής πλεονεκτήματα στους επαγγελματίες δικτύου και πληροφορικής:
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 global addresses for each network device enables **end-to-end reachability**. And network management will be simpler and easier.	Πρώτον, το IPv6 έχει ένα μεγαλύτερο χώρο διευθύνσεων για την παγκόσμια προσπελασιμότητα (reachability) και επεκτασιμότητα (scalability). Αυτό συνεπάγεται ένα σχεδόν απεριόριστο αριθμό διευθύνσεων IP και μια ιεραρχική δομή δικτύου για τη αποδοτική δρομολόγηση. Ως συνέπεια, εξαλείφονται τα προβλήματα που συνδέονται με τη χρήση λειτουργιών NAT. Η ικανότητά του IPv6

	να παρέχει παγκόσμιες διευθύνσεις για κάθε συσκευή δικτύου επιτρέπει την από άκρο-σε-άκρο (end-to-end) προσβασιμότητας. Επίσης, η διαχείριση του δικτύου θα είναι απλούστερη και ευκολότερη.
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**.	Δεύτερον, απλοποιημένη μορφή επικεφαλίδα για αποτελεσματική διαχείριση πακέτων. 6 από τα 12 πεδία της κεφαλίδας IPv4 έχουν αφαιρεθεί στο IPv6. Ορισμένα πεδία του IPv4 έχουν μεταφερθεί με τροποποιημένα ονόματα, και ορισμένα νέα πεδία έχουν προστεθεί για να βελτιώσει την αποτελεσματικότητα και να εισαγάγει νέα χαρακτηριστικά.
Third, a hierarchical network architecture for routing efficiency, that follows some of the IPv4 CIDR principles.	Τρίτον, μια ιεραρχική δομή του δικτύου για τη δρομολόγηση της αποτελεσματικότητας, που ακολουθεί κάποιες από τις αρχές του IPv4 CIDR.
Another important IPv6 benefit is the **embedded security** with mandatory IPSec implementation. 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 ICMP protocol has been revised. ICMPv6 has become **much more powerful**, and includes new functions to support autoconfiguration, neighbour discovery and multicasting. ▪ And finally, IPv6 offers **built-in mobility**, as the anticipated large rollout of wireless data services is a key IPv6 driver.	Ένα άλλο σημαντικό πλεονέκτημα του IPv6 είναι η ενσωματωμένη ασφάλεια με την υποχρεωτική εφαρμογή λειτουργιών IPSec. Ενώ η χρήση του IPSec είναι προαιρετική στο IPv4, η χρήση του είναι υποχρεωτική για το IPv6. Το IPSec είναι μέρος της σουίτα πρωτοκόλλου IPv6. Ως εκ τούτου, η υλοποίηση του δικτύου θα μπορούσε να επιτρέψει τη χρήση IPSec σε κάθε κόμβο IPv6, πιθανώς καθιστώντας τα πιο ασφαλή τα δίκτυα επικοινωνιών. ▪ Επιπλέον, το IPv6 προσφέρει αυξημένο αριθμό διευθύνσεων Multicast. Το IPv6 δεν χρησιμοποιεί broadcasts, οδηγώντας σε ένα πιο αποδοτικο δίκτυο. ▪ Επιπλέον, το πρωτόκολλο ICMP έχει αναθεωρηθεί στο IPv6. Το ICMPv6 έχει πλουσιότερη λειτουργικότητα και περιλαμβάνει νέες δυνατότητες για την υποστήριξη αυτόματης διαμόρφωσης, ανακάλυψη γειτονικών κόμβων και multicasting. ▪ Και τέλος, το IPv6 προσφέρει ενσωματωμένη λειτουργικότητα για κινητικότητα (mobility) καθώς η αναμενόμενη ραγδαία εξάπλωση των ασύρματων υπηρεσιών αποτελεί βασική αιτία για την εξάπλωση του IPv6.
Click an interactive item for more details, or “Next” to continue.	Για περισσότερες λεπτομέρειες πατήστε σε ένα διαδραστικό στοιχείο ή πατήστε την επιλογή "Next" για να συνεχίσετε.

6DEPLOY Module 2: IPv6 addressing	6DEPLOY Ενότητα 2: Διευθυνσιοδότηση IPv6
INTRODUCTION In this module about IPv6 addressing, you will first learn how to recognise the IPv6 address syntax, including the IPv6 prefix. Then, 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 'Next' to continue.	**Εισαγωγή** Στην ενότητα αυτή που αφορά τη διευθυνσιοδότηση IPv6 θα μάθετε αρχικά να αναγνωρίζετε την δομή των διευθύνσεων IPv6 συμπεριλαμβανομένου και του προθέματος IPv6. Στη συνέχεια θα μάθετε πώς να διακρίνετε μεταξύ των διαφορετικών κατηγοριών διευθύνσεων IPv6. Αφού ολοκληρώσετε αυτή την ενότητα θα μπορείτε επίσης να περιγράψετε πως τα τελικά συστήματα (hosts) μπορούν αυτόματα να διαμορφώσουν το «interface identifier" από τη φυσική διεύθυνση (physical address) τους. Πατήστε την επιλογή "Next" για να συνεχίσετε.

IPv6 ADDRESSES SYNTAX	Δομή IPv6 διευθύνσεων
IP addressing changes significantly with IPv6. Instead of the 4 bytes in an IPv4 address, an IPv6 address has 16 bytes. Studies say the 128 bits IPv6 address will result in at least 1,000 addresses per person on this planet. Even if only a portion of the full IPv6 address space is effectively used, IPv6 eliminates any possibility of IP address depletion.	Η διευθυνσιοδότηση IP αλλάζει σημαντικά με το IPv6. Σε αντίθεση με μια διεύθυνση IPv4 που αποτελείται από 4 byte, μία διεύθυνση IPv6 αποτελείται 16 bytes. Μελέτες υποστηρίζουν πως η χρήση διευθύνσεων IPv6 μεγέθους 128 bit θα έχει σαν αποτέλεσμα την ύπαρξη τουλάχιστον 1,000 διευθύνσεων ανά άτομο στον πλανήτη. Ακόμα και αν χρησιμοποιηθεί μόνο ένα μέρος του χώρου διευθύνσεων του πρωτοκόλλου IPv6 θα εξαλειφθεί κάθε πιθανότητα για εξάντληση των διευθύνσεων IP.
IPv6 addresses are generally written in the following format: each set of four x's represents a 16-bit hexadecimal field. Colons are used to separate the eight octets.	Οι διευθύνσεις IPv6 έχουν συνήθως την παρακάτω δομή: κάθε ομάδα από τέσσερα "x" αποτελεί ένα δεκαεξαδικό πεδίο των 16-bit. Για τον διαχωρισμό των ομάδων χρησιμοποιείται ο χαρακτήρας ":" (στα αγγλικά χρησιμοποιείται ο όρος **colon**).
The hexadecimal numbers are not case-sensitive. For example, this is a valid IPv6 address… as is the following…	Στα δεκαεξαδικά νούμερα δεν υπάρχει διάκριση μεταξύ πεζών και κεφαλαίων χαρακτήρων. Για παράδειγμα, αυτή είναι μία έγκυρη διεύθυνση IPv6 … όπως είναι και αυτή …
Additionally, leading zeroes in a field can be compressed. For example, 'this' IPv6 address can also be written as follows: …	Επιπλέον, αν σε ένα πεδίο οι αρχικοί χαρακτήρες είναι μηδέν τότε μπορούν να διαγραφούν. Για παράδειγμα, αυτή η διεύθυνση IPv6 μπορεί επίσης να γραφτεί και με την παρακάτω μορφή: …
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 … can be written as … but not as …	Το IPv6 χρησιμοποιεί ακόμα μία σημαντική σύμβαση για την ελάττωση του μήκους μιας διεύθυνσης IPv6 ώστε να γίνει ευκολότερη η αναπαράσταση της: διαδοχικά πεδία με τιμές 0 αναπαριστώνται ως διπλά «:» (colons). Αυτό επιτρέπεται μόνο μία φορά σε κάθε έγκυρη διεύθυνση IPv6. Για παράδειγμα, η διεύθυνση IPv6 … μπορεί να γραφτεί ως … αλλά όχι ως ...
An IPv6 address can be expressed in the following format: IPv6 address/prefix length.	Μία διεύθυνση IPv6 μπορεί να εκφραστεί στην παρακάτω μορφή: διεύθυνση IPv6 / μήκος προθέματος (IPv6 address / prefix length), με τον ίδιο τρόπο που μία διεύθυνση IPv4 αναπαριστάται σε μορφή "classless

In the same way an IPv4 address is represented in the “classless interdomain routing”, or CIDR, notation. For instance, ‘this’ 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 characterise 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 one of the items on the screen for more details. Or test your understanding by clicking the ‘Test’ button. To continue, click ‘Next’.	interdomain routing” ή για συντομία CIDR. Για παράδειγμα, αυτό είναι ένα αποδεκτό πρόθεμα IPv6. Το μήκος του προθέματος είναι μία δεκαδική τιμή που αναπαριστά πόσα από τα αριστερότερα bit της διεύθυνσης αποτελούν το πρόθεμα. Το πρόθεμα IPv6 (IPv6 prefix) μπορεί να χαρακτηρίσει μία ομάδα διευθύνσεων καθώς και για να ταυτοποιήσει ένα τοπικό δίκτυο, μια ομάδα διευθύνσεων σε ένα σημείο παρουσίας (site) ή ακόμα και το σύνολο του δίκτυου ενός Παρόχου Υπηρεσιών Διαδικτύου (ISP). Το πρόθεμα ενός τοπικού δικτύου έχει συνήθως μήκος 64 bits ενώ ενός σημείο παρουσίας (site) ενός οργανισμού έχει συνήθως μήκος 48 bit. Στη δεύτερη περίπτωση, 16 bit χρησιμοποιούνται ως «subnet ID” για τη δημιουργία διαφορετικών υποδικτύων (subnets). Πατήστε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις πατώντας την επιλογή “Test”. Για να συνεχίσετε, πατήστε την επιλογή “Next”

TYPES OF IPv6 ADDRESSES

A major difference exists 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.

Also, 'special' unicast addresses, such as the unspecified address and the loopback address exist.

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.

Κατηγορίες διευθύνσεων IPv6

Υπάρχει μία σημαντική διαφορά μεταξύ της διευθυνσιοδότησης μεταξύ ενός κόμβου IPv4 και ενός κόμβου IPv6. Ένας κόμβος IPv4 έχει συνήθως μόνο μία IP διεύθυνση. Αντιθέτως, ένας κόμβος IPv6 συχνά έχει περισσότερες από μία διευθύνσεις IP.

Υπάρχουν τρεις κύριες κατηγορίες διευθύνσεων IPv6: «unicast", «multicast" και «anycast».

Μία διεύθυνση IPv6 unicast προσδιορίζει ένα μοναδικό interface. Ένα πακέτο που αποστέλλεται σε μία διεύθυνση "unicast" παραδίδεται στο interface που προσδιορίζεται από τη διεύθυνση αυτή. Τα 64 λιγότερα σημαντικά bit μίας διεύθυνσης IPv6 unicast αποτελούν το interface identifier ή για συντομία IID.

Οι διευθύνσεις IPv6 unicast μπορούν να χωριστούν σε 4 τύπους:

- διευθύνσεις global unicast,
- διευθύνσεις unique local ή ULAs,
- διευθύνσεις link-local unicast,
- διευθύνσεις IPv4-mapped IPv6.

Επίσης, υπάρχουν και κάποιες ειδικές κατηγορίες διευθύνσεων unicast, όπως η διεύθυνση unspecified και η διεύθυνση loopback.

Μία διεύθυνση τύπου IPv6 anycast προσδιορίζει μία ομάδα από interfaces που συνήθως ανήκουν σε διαφορετικούς κόμβους. Ένα πακέτο που αποστέλλεται σε μία διεύθυνση anycast παραδίδεται μόνο στο κοντινότερο interface που χαρακτηρίζεται από αυτή τη διεύθυνση anycast. Το ποιο interface είναι το κοντινότερο χαρακτηρίζεται από τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται. Αυτό επιτρέπει σε ένα κόμβο να εντοπίσει τον κοντινότερο

	διακομιστή (server), για παράδειγμα όταν ένας κόμβος αναζητεί έναν κοντινό DNS server.
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 hosts’ interfaces that have 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.	Μία διεύθυνση τύπου IPv6 multicast είναι το αναγνωριστικό για μία ομάδα από interfaces που συνήθως ανήκουν σε διαφορετικούς κόμβους. Ένα πακέτο που αποστέλλεται σε μία διεύθυνση IPv6 multicast παραδίδεται σε όλα τα interfaces που έχουν εγγραφεί σε αυτή τη διεύθυνση multicast. Το πακέτο αντιγράφεται στους δικτυακούς κόμβους όπως προωθείται μεταξύ του αποστολέα και των πολλαπλών παραληπτών. Οι διευθύνσεις multicast έχουν πρόθεμα της μορφής FF00::/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.	Το πρωτόκολλο IPv6 δεν υποστηρίζει αποστολή πακέτων σε διευθύνσεις “broadcasts”. Η χρήση διευθύνσεων broadcast οδήγησε στη μείωση της επίδοσης των IPv4 δικτύων καθώς κάθε κόμβος σε ένα τοπικό δίκτυο όφειλε να επεξεργαστεί όλα τα πακέτα που είχαν αποσταλεί σε διεύθυνση broadcast παρά το γεγονός πως τα περισσότερα από τα πακέτα αυτά δεν είχαν σχέση με τον κόμβο.
The IPv6 solution for the broadcast problem is the implementation of the multicast address ‘all nodes on link’, which has the following format. This multicast address is used to replace essential broadcasts. In other cases, more limited multicast messages are used.	Η λύση του πρωτοκόλλου IPv6 για το πρόβλημα σχετικά με τα broadcastσ ήταν η υλοποίηση της διεύθυνσης multicast που αφορά όλους τους κόμβους στο τοπικό δίκτυο (all nodes on link), η οποία έχει την παρακάτω μορφή. Αυτή η διεύθυνση multicast χρησιμοποιείται για να αντικαταστήσει τα broadcasts που είναι απαραίτητο να παραδοθούν σε όλους τους κόμβους στο τοπικό δίκτυο. Σε όλες τις άλλες περιπτώσεις, χρησιμοποιούνται μηνύματα multicast για πιο περιορισμένο αριθμό παραληπτών.
Click one of the items on the screen for more details. Or test your understanding by clicking the ‘Test’ button. To continue, click ‘Next’	Πατήστε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις πατώντας την επιλογή “Test”. Για να συνεχίσετε, πατήστε την επιλογή “Next”.

6DEPLOY Module 3: The IPv6 Header **INTRODUCTION** 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 new IPv6 header fields. You will also learn to explain the functions and specifics of the IPv6 header fields. Finally, on completing this module, you will also be able to identify the seven different IPv6 extension headers and to describe their functions. Click “Next” to continue.	**6DEPLOY Ενότητα 3: Η Επικεφαλίδα IPv6** **Εισαγωγή** Στη παρούσα ενότητα που αφορά την επικεφαλίδα IPv6 (IPv6 header) θα ενημερωθείτε για τις διαφορές μεταξύ της δομής των επικεφαλίδων ενός πακέτου IPv4 και ενός πακέτου IPv6 καθώς και για τα νέα ή τροποποιημένα πεδία μίας επικεφαλίδας IPv6. Επίσης θα μάθετε να εξηγείτε τον ρόλο και τις διαφορετικές λεπτομέρειες των πεδίων μίας επικεφαλίδας IPv6. Τέλος, με την ολοκλήρωση της συγκεκριμένης ενότητας, θα μπορείτε επίσης να αναγνωρίζεται τις επτά διαφορετικές επικεφαλίδες επέκτασης (extension headers) και να περιγράφετε την λειτουργία τους. Πατήστε την επιλογή “Next” για να συνεχίσετε.
STRUCTURE OF AN IPv6 PACKET 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’ field are kept, except that both fields are 128-bits to embed the IPv6 addresses.	**Δομή ενός πακέτου IPv6** Η επικεφαλίδα IPv6 είναι απλούστερη και αποδοτικότερη από την επικεφαλίδα IPv4 αφού έχει σταθερό μήκος και μικρότερο πλήθος πεδίων. Οι παραπάνω αλλαγές έχουν ως αποτέλεσμα την αυξημένη απόδοση κατά τη δρομολόγηση, καλύτερες επιδόσεις καθώς και καλύτερη κλιμάκωση του ρυθμού προώθησης πακέτων (forwarding rate). Το πεδίο “version number” παραμένει και όταν φέρει την τιμή 6 υποδεικνύει ένα IPv6 πακέτο. Τα πεδία “source address” και ”destination address” παραμένουν με την διαφορά πως το μήκος τους αυξήθηκε σε 128 bits ώστε να μπορούν να πάρουν ως τιμή διευθύνσεις IPv6.

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 allow options to be implemented without decreasing performance, as it is no longer necessary for all routers to be able to process it. IPv6 extension headers will be detailed in a following part of this e-learning course.	Το πεδίο "options" της επικεφαλίδας IPv4, έχει αντικατασταθεί στην επικεφαλίδα IPv6 με μία αλυσίδα από προαιρετικές επικεφαλίδες επέκτασης (extension headers) τοποθετημένες ακριβώς μετά από την επικεφαλίδα IPv6. Οι επικεφαλίδες επέκτασης IPv6 επιτρέπουν την υλοποίηση των προαιρετικών λειτουργιών χωρίς μείωση της επίδοσης αφού δεν είναι πλέον απαραίτητο όλοι οι δρομολογητές να χρειάζεται να τις επεξεργαστούν. Οι επικεφαλίδες επέκτασης θα αναλυθούν σε επόμενη ενότητα.
Five other fields have been removed from the IPv4 header: The 'Header Checksum' has gone, as link quality is now very high and other checksums are already performed at upper and lower layers.	Πέντε άλλα πεδία που εμφανίζονται στην επικεφαλίδα IPv4 αφαιρέθηκαν από την επικεφαλίδα IPv6. Το πεδίο "header checksum" έχει αφαιρεθεί, καθώς η ποιότητα των δικτυακών συνδέσμων είναι πλέον πολύ υψηλή ενώ έλεγχοι λαθών (checksums) πραγματοποιούνται τόσο σε υψηλότερα όσο και σε χαμηλότερα επίπεδα.
The 'Header Length' has gone 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 using the appropriate extension.	Το πεδίο "Header Length" αφαιρέθηκε καθώς το μήκος της επικεφαλίδας είναι σταθερό στο πρωτόκολλο IPv6. Ακόμα από την επικεφαλίδα αφαιρέθηκαν τα τρία πεδία σχετικά με τον κατακερματισμό (**fragmentation**) δεδομένων: "identification", "flags", "fragment offset". Ο κατακερματισμός μπορεί να επιτευχθεί χρησιμοποιώντας την κατάλληλη επικεφαλίδα επέκτασης.
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.	Τέσσερα πεδία της επικεφαλίδας IPv4 έχουν μετονομαστεί και τροποποιηθεί: • το πεδίο "type of service" έχει αντικατασταθεί από το πεδίο "traffic class" • το πεδίο "protocol type" έχει αντικατασταθεί από το πεδίο "next header" • το πεδίο "total length" έχει αντικατασταθεί από το πεδίο "payload length" • το πεδίο "time to live" έχει αντικατασταθεί από το πεδίο "hop limit"
Finally, one field has been added. It is called the 'Flow Label'.	Τέλος, προστέθηκε ένα ακόμα πεδίο, το οποίο ονομάστηκε "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.	Οι παραπάνω αλλαγές είχαν σαν αποτέλεσμα η επικεφαλίδα IPv6 να έχει μόνο 8 πεδία (από 13 στην επικεφαλλίδα IPv4) με σταθερό συνολικό μήκος 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'.	Πατήστε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας την επιλογή "Test". Για να συνεχίσετε. πατήστε την επιλογή "Next".

IPv6 EXTENSION HEADERS

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, subsequently, 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.

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. Additionally, a Mobility Header is used by

Επικεφαλίδες επέκτασης IPv6

Σε αντίθεση με το IPv4 που ενσωμάτωνε το πεδίο "options" στην επικεφαλίδα, στο IPv6 η λειτουργικότητα αυτή εμπεριέχεται στις επικεφαλίδες επέκτασης (extension headers). Οι επικεφαλίδες αυτές μπορούν να συμπεριληφθούν όταν απαιτείται ενώ παραλείπονται όποτε είναι εφικτό. Τα οκτώ βασικά πεδία μιας επικεφαλίδας IPv6 ακολουθούνται από τις προαιρετικές επικεφαλίδες επέκτασης και εν συνεχεία από το κομμάτι δεδομένων του πακέτου.

Η κάθε επικεφαλίδα επέκτασης, εφόσον χρησιμοποιείται, καταλαμβάνει χώρο πολλαπλάσιο των 64 bit. Το πλήθος των επικεφαλίδων εκτεταμένης λειτουργικότητας που χρησιμοποιούνται μπορεί να μεταβάλλεται.

Το πεδίο "Next Header" της προηγούμενης επικεφαλίδας προσδιορίζει την τρέχουσα επικεφαλίδα εκτεταμένης λειτουργικότητας. Γενικά, το πεδίο "Next Header" της τελευταίας επικεφαλίδας εκτεταμένης λειτουργικότητας προσδιορίζει την επικεφαλίδα ενός πρωτοκόλλου του επίπεδου μεταφοράς, όπως TCP ή UDP.

Οι επικεφαλίδες εκτεταμένης λειτουργικότητας IPv6 είναι αλυσιδωτά συνδεδεμένες. Όταν πολλαπλές επικεφαλίδες επέκτασης χρησιμοποιούνται στο ίδιο πακέτο, η σειρά τους οφείλει να είναι η ακόλουθη:

- πρώτα η επικεφαλίδα "hop-by-hop options"
- αμέσως μετά η επικεφαλίδα "destination options"
- ακολουθούμενη από την επικεφαλίδα "routing"
- εν συνεχεία η επικεφαλίδα "fragment"
- ακολουθούμενη από την επικεφαλίδα "authentication"
- καθώς και την επικεφαλίδα "encapsulating security payload"
- τελευταία συμπεριλαμβάνεται η επικεφαλίδα "upper-layer"

Εναλλακτικά η επικεφαλίδα "destination options" μπορεί να τοποθετηθεί εδώ.

Ο κόμβος αποστολής πακέτων θα πρέπει να ακολουθήσει την παραπάνω σειρά ενώ οι κόμβοι προορισμού θα πρέπει να είναι προετοιμασμένοι να επεξεργαστούν

nodes implementing Mobile IP Version 6. 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'.	οποιαδήποτε σειρά επικεφαλίδων επέκτασης. Επιπροσθέτως, όσοι κόμβοι υλοποιούν το πρωτόκολλο Mobile IP version 6, χρησιμοποιείούν και η επικεφαλίδα "mobility". Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε πατήστε την επιλογή "Next".

6DEPLOY Module 4: IPv6 Basic Services **INTRODUCTION** 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 taught 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	**6DEPLOY Ενότητα 4: Βασικές υπηρεσίες του πρωτοκόλλου IPv6** **Εισαγωγή** Σε αυτή την ενότητα θα μάθετε να αναγνωρίζετε τις διάφορες βασικές υπηρεσίες του πρωτοκόλλου IPv6. Με την ολοκλήρωση της ενότητας θα μπορείτε να περιγράψετε το Internet Control Message Protocol για το IPv6 ή εν συντομία ICMPv6. Επιπλέον, θα ενημερωθείτε για την λειτουργικότητα του πρωτοκόλλου IPv6 "neighbour discovery". Επίσης θα διδαχτείτε τον τρόπο λειτουργίας του IPv6 "stateless autoconfiguration". Εν συνεχεία, θα μάθετε να περιγράφετε τις εκδόσεις των πρωτοκόλλων Dynamic Host Configuration και Domain Name System, ή εν συντομία DHCP και DNS. Τέλος θα είστε ικανοί να εξηγήσετε τα κύρια σημεία των υπηρεσιών IPv6 multicasting και Quality of service. Πατήστε την επιλογή "Next" για να συνεχίσετε.

ICMPv6	ICMPv6
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 diagnostic functions.	Οι κόμβοι IP χρειάζονται ένα συγκεκριμένο πρωτόκολλο για την μεταφορά μηνυμάτων σχετικά με τις συνθήκες λειτουργίας του IP. Το πρωτόκολλο Internet Control Message Protocol, ή εν συντομία ICMP, χρησιμοποιείται για την αναφορά σφαλμάτων και πληροφοριών (για τις συνθήκες λειτουργίας του δικτύου) καθώς και για διαγνωστικές λειτουργίες.
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, path MTU discovery, and the Multicast Listener Discovery or MLD protocol for IPv6.	Για την παραγωγή ενημερωτικών μηνυμάτων αλλά και μηνυμάτων σφάλματος, το ICMP στο IPv6 λειτουργεί με αντίστοιχο τρόπο με το IPv4. Επιπροσθέτως, όμως, στο πρωτόκολλο IPv6 τα πακέτα ICMP χρησιμοποιούνται στις διαδικασίες IPv6 ”neighbor discovery”, ”path MTU discovery” και ”multicast listener discovery” ή εν συντομία MLD.
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.	Τα πακέτα ICMP στο πρωτόκολλο IPv6 είναι σαν ένα πακέτο επιπέδου μεταφοράς καθώς τα πακέτα ICMP τοποθετούνται μετά από όλες τις επικεφαλίδες επέκτασης, καταλαμβάνοντας το τελευταίο τμήμα από το πακέτο IPv6.
The ICMPv6 header is identified by a “Next Header” with a value of 58 in the immediately preceding header.	Η επικεφαλίδα ICMPv6 αναγνωρίζεται από την τιμή 58 στο πεδίο “Next Header” της επικεφαλίδας που προηγείται.
Within IPv6 ICMP packets, the ICMPv6 Type field indicates the type of the message and ICMPv6 Code field provides further information on specific messages.	Μέσα στα πακέτα IPv6 ICMP, το πεδίο ICMPv6 Type υποδεικνύει τον τύπο του μηνύματος και το πεδίο ICMPv6 Code παρέχει περαιτέρω πληροφορίες για συγκεκριμένα μήνυμα.
The value in the Checksum field is built from the fields in the IPv6 ICMP packet and the IPv6 header.	Η τιμή του πεδίου Checksum παράγεται από τα πεδία του πακέτου IPv6 ICMP και την επικεφαλίδα IPv6.
The ICMPv6 Message Body contains error or diagnostic information relevant to IP packet processing.	Το πεδίο ICMPv6 Message Body περιέχει διαγνωστικές πληροφορίες ή πληροφορίες σφαλμάτων σχετικές με την επεξεργασία των IP πακέτων.
Similar to ICMPv4, ICMPv6 is often blocked by security policies implemented in corporate firewalls because of ICMP based attacks. However, ICMPv6 has the	Αντίστοιχα με το ICMPv4, το ICMPv6 συχνά μπλοκάρεται στο τοίχος προστασία (firewall) των εταιριών λόγω των επιθέσεων που βασίζονται στο ICMP. Όμως το

capability to use IPSec, granting authentication and encryption. These security services decrease the possibility of an attack based on ICMPv6.	ICMPv6 έχει την δυνατότητα να χρησιμοποιήσει το πρωτόκολλο IPSec που προσφέρει δυνατότητες πιστοποίησης και κωδικοποίησης. Αυτές οι υπηρεσίες ασφαλείας μειώνουν την πιθανότητα μίας πιθανής επίθεσης βασισμένης στο 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.	Το πεδίο ICMPv6 Type ορίζει τον τύπο ενός μηνύματος ICMPv6 όπως "destination unreachable (μη προσβάσιμος προορισμός)", "packet too big (υπερβολικά μεγάλο πακέτο)", "time exceeded (εξάντληση χρόνου)", "parameter problem (πρόβλημα παραμέτρων)", "echo request" ή "echo reply". Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε πατήστε την επιλογή "Next".

NEIGHBOUR DISCOVERY

The IPv6 Neighbour Discovery protocol uses ICMPv6 messages and corresponds with 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.

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:

Ανακάλυψη Γειτώνων (NEIGHBOUR DISCOVERY)

Το πρωτόκολλο IPv6 Neighbor Discovery χρησιμοποιεί μηνύματα ICMPv6 και αντιστοιχεί σε έναν «ενισχυμένο» συνδυασμό των πρωτοκόλλων του IPv4 όπως του ARP, ICMP Router Discovery και ICMP Redirect.

Δικτυακοί κόμβοι, όπως τελικά συστήματα (hosts) και δρομολογητές, χρησιμοποιούν το πρωτόκολλο neighbor discovery για να προσδιορίσουν τη διεύθυνση του επιπέδου συνδέσμου (link layer address) των γειτόνων και να αφαιρέσουν γρήγορα μη έγκυρες αποθηκευμένες τιμές. Τα τελικά συστήματα χρησιμοποιούν το Neighbor Discovery για να βρουν γειτονικούς δρομολογητές πρόθυμους να προωθήσουν πακέτα τους. Τέλος κόμβοι χρησιμοποιούν το πρωτόκολλο για να παρακολουθούν ενεργά με ποιους γειτονικούς κόμβους είναι δυνατή η επικοινωνία και με ποιους όχι καθώς και να ανιχνεύσουν διευθύνσεις επιπέδου συνδέσμου που έχουν μεταβληθεί.

Το πρωτόκολλο Neighbor Discovery λύνει μία ομάδα προβλημάτων σχετικά με την αλληλεπίδραση μεταξύ κόμβων του ίδιου συνδέσμου. Ορίζει μηχανισμούς για την επίλυση των παρακάτω προβλημάτων.

- Ανίχνευση Δρομολογητών Router Discovery
- Ανίχνευση Προθέματος (διευθύνσεων) Prefix Discovery
- Ανακάλυψη Παραμέτρων - Parameter Discovery
- Αυτόματη Ρύθμιση Διεύθυνσης - Address Autoconfiguration
- Address Resolution
- Next-hop Determination
- Neighbor Unreachability Detection
- Εντοπισμός Διπλής Διεύθυνσης - Duplicate Address Detection
- Redirect

Για να επιτύχει στα παραπάνω χρησιμοποιεί πέντε διαφορετικούς τύπους ICMP πακέτων:

• - 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.	• Router Solicitation • Router Advertisement • Redirect Messages • Neighbor Solicitation • Neighbor Advertisement Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε πατήστε την επιλογή "Next".

AUTOCONFIGURATION

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, 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.

IPv6 hosts use received Router Advertisement messages to automatically configure:

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

Αυτόματη ρύθμιση - AUTOCONFIGURATION

Το πρωτόκολλο IPv6 ορίζει τόσο έναν μηχανισμό με διατήρηση καταστάσεων (stateful) όσο και έναν μηχανισμό χωρίς διατήρηση καταστάσεων (stateless) για την αυτόματη ρύθμιση διευθύνσεων (address autoconfiguration). Το stateless autoconfiguration επιτρέπει την αυτόματη ρύθμιση των τελικών συστημάτων ενώ απαιτεί ελάχιστη ρύθμιση των δρομολογητών και δεν προϋποθέτει την ύπαρξη διακομιστή (server).

Το stateless autoconfiguration είναι βασικό χαρακτηριστικό του IPv6 που επιτρέπει σε έναν τελικό σύστημα να παράγει τη δική του διεύθυνση χρησιμοποιώντας ένα συνδυασμό τοπικά διαθέσιμων πληροφοριών και πληροφοριών που διαφημίζονται από τους δρομολογητές. Το stateless autoconfiguration απλοποιεί το αλλαγή των διευθύνσεων (renumbering) υπό προϋποθέσεις.

Απαιτεί ο τοπικός σύνδεσμος (local link) να υποστηρίζει multicast και το interface του δικτύου να έχει την δυνατότητα να λαμβάνει πακέτα multicast.

Οι κόμβοι IPv6 δημιουργούν αυτόματα μοναδικές διευθύνσεις link-local για όλα τα interfaces, προσαρτώντας την διεύθυνση του επιπέδου συνδέσμου σε μορφή EUI-64 στο πρόθεμα, μήκους 64bit, του τοπικού συνδέσμου (local link). Τέλος οι κόμβοι IPv6 χρησιμοποιούν τη λειτουργία Duplicate Address Detection ή, εν συντομία, DAD για να καθορίσουν αν η διεύθυνση βρίσκεται ήδη σε χρήση.

Τα τελικά συστήματα IPv6 χρησιμοποιούν τα μηνύματα Router Advertisement που έχουν λάβει για να ρυθμίσουν αυτόματα:

- τον προεπιλεγμένο δρομολογητή
- την προεπιλεγμένη τιμή του πεδίου Hop Limit για την επικεφαλίδα IPv6
- τους χρονομετρητές που χρησιμοποιούνται στην διαδικασία Neighbor Discovery
- το Maximum Transmission Unit ή MTU στο τοπικό δικτυο
- και τη λίστα με τα προθέματα των δικτύων που ορίζονται για το τοπικό

	δίκτυο
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.	Κάθε μήνυμα Router Advertisement περιέχει τόσο το πρόθεμα δικτύου IPv6 όσο και τα έγκυρα και προτιμώμενα «lifetimes». Αν απαιτείται, το πρόθεμα δικτύου συνδυάζεται με το αναγνωριστικό του interface ώστε να δημιουργηθεί μια stateless IPv6 διεύθυνση για το interface που λαμβάνει το μήνυμα.
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.	Τα μηνύματα router advertisements περιέχουν δύο σημαίες (flags) που υποδεικνύουν τον τύπο stateful autoconfiguration πρέπει να εκτελεστεί, εφόσον απαιτείται. Η σημαία “managed address configuration” υποδεικνύει αν τα τελικά συστήματα πρέπει να χρησιμοποιήσουν stateful autoconfiguration για να αποκτήσουν διευθύνσεις ή όχι. Η σημαία “other stateful configuration” υποδεικνύει αν τα τελικά συστήματα πρέπει να χρησιμοποιήσουν stateful autoconfiguration για να αποκτήσουν επιπρόσθετη πληροφορία (εξαιρώντας τις διευθύνσεις) όπως, για παράδειγμα, τη διεύθυνση του διακομιστή DNS. Αυτό είναι σημαντικό γιατί στο stateless configuration δεν υπάρχει κανένας τρόπος για την αποστολή της διεύθυνσης του DNS server στους πελάτες.
Click one of the items on the screen for more details. Or test your understanding by clicking the ‘test’ button. To continue, click ‘next’.	Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί “Test”. Για να συνεχίσετε πατήστε την επιλογή “Next”.

DHCPv6	DHCPv6
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.	Το DHCP για IPv6 (DHCPv6) χρησιμοποιεί το μοντέλο πελάτη / διακομιστή (client/server). Αυτό επιτρέπει στους διακομιστές DHCP να αποστέλλουν διευθύνσεις IPv6 καθώς και άλλες παραμέτρους σε κόμβους IPv6. Το πρωτόκολλο αυτό είναι το αντίστοιχο stateful πρωτόκολλο για το IPv6 Stateless Address Autoconfiguration.
The process for 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.	Η διαδικασία για την απόκτηση ρυθμίσεων για ένα πελάτη είναι παρόμοια με αυτήν του IPv4. Παρ' όλα αυτά το DHCPv6 χρησιμοποιεί multicast για πολλά από τα μηνύματα του. Αν βρεθεί ένας δρομολογητής, ο πελάτης εξετάζει τα μηνύματα router advertisements για να καθορίσει εάν πρέπει να χρησιμοποιηθεί το DHCP. Εάν τα μηνύματα router advertisements επιτρέπουν την χρήση του DHCP ή αν δεν βρεθεί δρομολογητής τότε ο πελάτης θα επικοινωνήσει με το διακομιστή DHCP.
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: …	Πελάτες και διακομιστές ανταλλάσσουν μηνύματα DHCP χρησιμοποιώντας το πρωτόκολλο UDP. Οι διακομιστές DHCP λαμβάνουν μηνύματα από τους πελάτες χρησιμοποιώντας μία δεσμευμένη (reserved), διεύθυνση link-scoped multicast που χαρακτηρίζεται ως "All DHCP Relay Agents and Servers ". Έχει την ακόλουθη μορφή: …
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.	Ένας πελάτης DHCP μεταδίδει τα περισσότερα μηνύματα στην δεσμευμένη multicast διεύθυνση. Για να επιτραπεί σε ένα πελάτη DHCP να στείλει ένα μήνυμα σε έναν διακομιστή DHCP ο οποίος δεν βρίσκεται στον ίδιο τοπικό δίκτυο, ένας DHCP relay agent θα αναμεταδώσει τα μηνύματα μεταξύ του πελάτη και του διακομιστή. Η λειτουργία του relay agent είναι διαφανής (transparent) στον πελάτη.
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.	Ο διακομιστής παρέχει προαιρετικά στον πελάτη μία διεύθυνση IPv6 καθώς και άλλες παραμέτρους διαμόρφωσης όπως: διακομιστές DNS, διακομιστές NTP κ.α. Αλλά δεν είναι δυνατόν να αποστείλει τη διεύθυνση της προκαθορισμένη πύλη (default gateway) καθώς η πληροφορία αυτή πρέπει να αποκτηθεί μέσω του

	stateless autoconfiguration.
DHCPv6 provides more control than stateless autoconfiguration. 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.	Το DHCPv6 προσφέρει μεγαλύτερο έλεγχο απ' ότι το stateless autoconfiguration. Μία ακόμα διαφορά είναι ότι το stateless autoconfiguration δεν επιτρέπει σε ένα διαχειριστή δικτύου να ορίσει πολιτικές ελέγχου πρόσβασης (admission control policy). Με το autoconfiguration κάθε τελικό σύστημα που συνδέεται στο δίκτυο μπορεί να αποκτήσει μία διεύθυνση IPv6. Αντίθετα οι διακομιστές DHCP προσφέρουν την δυνατότητα του ελέγχου της πρόσβασης σε πόρους του δικτύου καθώς ελέγχουν πρώτα τις πολιτικές ελέγχου πρόβασης πριν απαντήσουν σε αιτήματα από πελάτες.
Further, benefits of DCHPv6 are the following: • 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 • Finally, it can be used to delegate an IPv6 prefix to leaf customer-premise equipment or CPE routers.	Μερικά ακόμα πλεονεκτήματα του DHCPv6 είναι τα παρακάτω: • Μπορεί να χρησιμοποιηθεί παράλληλα με το stateless autoconfiguration. Για παράδειγμα μπορεί κάποιος να αποκτήσει διεύθυνση IPv6 μέσω stateless configuration και τη διεύθυνση του διακομιστή DNS μέσω DHCPv6. • Τέλος μπορεί να χρησιμοποιηθεί για να την ανάθεση προθέματος IPv6 σε δρομολογητές τελικών χρηστών.
Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. To continue, click 'Next'.	Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε επιλέξτε το κουμπί "Next".
DNS	**Σύστημα Ομματοδοσίας DNS**
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.	Το σύστημα Ονοματοδοσίας «Domain Name System" αντιστοιχεί ονόματα σε διευθύνσεις IP (και αντίστροφα). Το DNS χρησιμοποιεί έναν ιεραρχικό τόπο ονομάτων. Σε κάθε επίπεδο της ιεραρχίας, οι διακομιστές αντιστοιχούν ονόματα σε διευθύνσεις. Παρά το γεγονός πως το DNS σχεδιάστηκε για να επεξεργάζεται διευθύνσεις IPv4, μήκους 32 bits, τα τελευταία χρόνια έχουν δημιουργηθεί επεκτάσεις του πρωτοκόλλου που είναι συμβατές με το πρωτόκολλο IPv6. Μερικές από τις επεκτάσεις χρησιμοποιούνται ακόμα, ενώ άλλες έχουν καταργηθεί.
In use are: × the quad A record,	Σε χρήση βρίσκονται οι ακόλουθες επεκτάσεις:

× 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	• Quad A εγγραφή (**record** AAAA) • New textual representation στην εγγραφή PTR • Ο ip6.arpa τομέας (**domain**) • Νέα DNS ερωτήματα (**queries**) Οι επεκτάσεις που έχουν καταργηθεί ή χαρακτηρίζονται ως πειραματικές είναι οι εξής: • Τα A6 και DNAME records • Binary Labels • Το 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.	Εκτός από την ύπαρξη των εγραφών για το IPv6 (AAAA records) απαραίτητη είνα η δυνατότητα αποστολής αιτημάτων (queries) DNS και να λαμβάνεις απαντήσεις χρησιμοποιώντας γαι την μεταφορά των πληροφοριών το πρωτόκολλο IPv6. Τα δεδομένα που λαμβάνουμε μέσω μεταφοράς πάνω IPv6 πρέπει να είναι ίδια με τα δεδομένα που λαμβάνουμε μέσω μεταφοράς πάνω από IPv4. Όσον αφορά τους κεντρικούς (root) διακομιστές DNS, μόνο μερικοί έχουν την δυνατότητα να απαντήσουν σε ένα αίτημα πάνω από IPv6.
× 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: … . 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: … . × 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.	• Μία εγγραφή quad A αντιστοιχεί το όνομα ενός τελικού συστήματος (host name) σε μία διεύθυνση IPv6. Η εγγραφή αυτή είναι ισοδύναμη με μια εγγραφή A για το πρωτόκολλο IPv4 και έχει την ακόλουθη μορφή:… Το IETF έχει αποφασίσει να χρησιμοποιεί αυτό την εγγραφή για την αντιστοίχηση μίας διεύθυνσης IPv6 από ένα όνομα τελικού συστήματος. • Ένα PTR record είναι ισοδύναμο με ένα pointer record που αντιστοιχεί μία διεύθυνση σε ένα host name. Η αντίστροφη αυτή αντιστοιχία που χρησιμοποιείται σε αναζήτησης. • Ένα ειδικό domain ορίστηκε για την αναζήτηση των εγγραφών που έχουν αποδοθεί σε μια διεύθυνση IPv6. Η χρήση αυτού του domain είναι να παρέχει έναν τρόπο αντιστοίχισης μιας διεύθυνσης IPv6 σε ένα όνομα τελικού συστήματος, αν και ενδέχεται να χρησιμοποιηθεί για άλλους

× 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'.	σκοπούς. Το ειδικό domain χρησιμοποιεί τη ρίζα IP6.ARPA. • Τέλος, τα ερωτήματα DNS αναθεωρήθηκαν έτσι ώστε να εντοπίζουν και να επεξεργάζονται ταυτόχρονα διευθύνσεις IPv4 και IPv6. Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε επιλέξτε το κουμπί "Next".

MULTICASTING

Multicasting is mainly used by multimedia applications. These often require high bandwidth to transmit certain data from a single source to many recipients. It is used by some ISP's to provide TV service to their DSL customers, for example.

IPv6 multicast addresses are in FF00::/8 prefix. A 4-bit Scope ID field is used to specify address ranges reserved for multicast addresses for each scope, allowing easy control of the multicast boundary. A host can subscribe to different multicast addresses and “get every relative flow” at the same time.

IPv6 provides a larger range of multicast addresses compared to IPv4, which offers new perspectives for address allocation.

A major innovation introduced by IPv6 in the area of multcasting is that all IPv6 implementations will have to include native support for this IP service right from the beginning. The MLD protocol, responsible for multicasting management between hosts and routers, is no longer delegated to a separate protocol as it is in IPv4 and hence, must be supported on every single IPv6 stack. The MLD protocol, in fact, is part of ICMPv6.

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 neighboring nodes.

MULTICASTING (Πολλαπλή Διανομή)

Η λειτουγικότητα multicasting (πολλαπλή διανομή) χρησιμοποιείται κυρίως από εφαρμογές πολυμέσων. Οι εφαρμογές αυτές συχνά απαιτούν υψηλό εύρος ζώνης (**bandwidth**) για να μεταδώσουν δεδομένα από έναν αποστολέα σε πολλούς παραλήπτες. Για παράδειγμα χρησιμοποιείται συχνά από παρόχους υπηρεσιών διαδικτύου (**ISP**) για να παρέχουν τηλεοπτικές υπηρεσίες στους ευρυζωνικούς συνδρομητές τους.

Οι διευθύνσεις IPv6 multicast έχουν το πρόθεμα FFOO::/8. Το πεδίο scope ID, μήκους 4 bits, χρησιμοποιείται για να προσδιορίσει ζώνες διευθύνσεων που προορίζονται για συγκεκριμένους «χώρους» (scope) στο δικτύου, διευκολύνοντας τον έλεγχο των ορίων για τους «χώρους» αυτούς. Ένα τελικό συστημα μπορεί να εγγραφεί σε διαφορετικές διευθύνσεις multicast και να λαμβάνει όλες τις ροές δεδομένων, που αντιστοιχούν στις διευθύνσεις αυτές, την ίδια χρονική στιγμή.

Το πρωτόκολλο IPv6 παρέχει περισσότερες διευθύνσεις multicast σε σχέση με το IPv4, το οποίο δημιουργεί νέες δυνατότητες για την κατανομή των διευθύνσεων.

Μία σημαντική καινοτομία του πρωτοκόλλου IPv6 όσον αφορά το multicast είναι πως όλες οι υλοποιήσεις του πρωτοκόλλου οφείλουν να παρέχουν εγγενή υποστήριξη για την υπηρεσία αυτή. Το πρωτόκολλο MLD, υπεύθυνο για να διαχειρίζεται το multicast μεταξύ των τελικών συστημάτων και των διακομιστών, δεν αποτελεί πλέον ξεχωριστό πρωτόκολλο όπως ήταν στο IPv4 αλλά πρέπει να υποστηρίζεται από κάθε στοίβα πρωτοκόλλων IPv6. Το MLD αποτελεί τμήμα του ICMPv6.

Το πρωτόκολλο Multicast Listener Discovery ή εν συντομία MLD μπορεί να χρησιμοποιεί από ένα διακομιστή IPv6 για να ανακαλύψει την παρουσία ακροατών multicast (**multicast listeners**) στους άμεσους δικτυακούς συνδέσμους καθώς και να ανακαλύψει ποιες διευθύνσεις multicast ενδιαφέρουν αυτούς τους ακροατές.

There are three types of MLD messages, which are distinguished by the value in the type field: × Multicast Listener Query × Multicast Listener Report × and Multicast Listener Done. MLD has been updated to MLDv2. This new protocol allows the receiver to specify groups and sources of interest. It is needed for SSM services, or Source Specific Multicast. From data provided by MLD or MLDv2, distribution trees will be created over the IPv6 multicast network using the PIM protocol. A big difference with IPv4 multicast concerns the interdomain problem. While a protocol called MSDP was designed for IPv4 to allow source information to be exchanged between domains; a proposal called embedded-RP allows a shared Rendez-vous point resource to be used accross domains. Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'next'.	Υπάρχουν τρεις τύπου μηνυμάτων MLD, τα οποία διακρίνονται από την τιμή του πεδίου type: Multicast Listener Query • Multicast Listener Report • Multicast Listener Done Το MLD έχει επικαιροποιηθεί με την έκδοση MLDv2. Το νέο αυτό πρωτόκολλο επιτρέπει στον παραλήπτη να επιλέξει συγκεκριμένες ομάδες ή μεμονωμένες πηγές που τον ενδιαφέρουν. Απαιτείται για υπηρεσίες Source Specific Multicast ή SSM για συντομία. Από τις πληροφορίες που θα παρέχονται από τα πρωτόκολλα MLD ή MLDv2, δέντρα διανομής (distribution trees) θα δημιουργηθούν πάνω από το δίκτυο IPv6 multicast χρησιμοποιόντας το πρωτόκολλο PIM. Μία σημαντική διαφορά με το IPv4 multicast αφορά το πρόβλημα μεταξύ διαχειριστικών περιοχών (interdomain problem). Παρά τη σχεδίαση ενός πρωτοκόλλου, με το όνομα MSDP, που επιτρέπει την ανταλλαγή πληροφοριών μεταξύ διαχειριστικών περιοχών (domains), μία πρόταση που αποκαλείται embedded-RP επιτρέπει την δημιουργία ενός σημείο συνάντησης (Rendez-vous point) μεταξύ των διαφορετικών περιοχών. Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε επιλέξτε το κουμπί "Next".

QoS: Quality of Service	Ποιότητα Υπηρεσίας - QoS: Quality of Service
The term Quality of Service (QoS) is often used to describe the performance guarantees that a network provides to carried traffic. Strict requirements imposed by new advanced applications, such as Voice-over IP, high-quality video distribution, online gaming, tele-immersion, etcetera require the transport of packets with minimum delay, jitter and packet loss. Today's high-speed networks follow the Differentiated Services framework in order to provide Quality of Service and meet the aforementioned requirements.	Ο όρος Ποιότητα Υπηρεσίας (Quality of Service - QoS) συχνά χρησιμοποιείται για να περιγράψει εγγυήσεις για την επίδοση που προσφέρει ένα δίκτυο στα μεταφερόμενα δεδομένα. Οι απαιτήσεις που έχουν δημιουργηθεί από εφαρμογές όπως το Voice-over IP, η μεταφορά βίντεο υψηλής ποιότητας, τα δικτυακά παιχνίδια, tele-immersion κ.α. απαιτούν την μεταφορά πακέτων με ελάχιστη καθυστέρηση και αυξομειώσεις καθυστέρησης κατά τη λήψη, και απώλεια πακέτων. Σήμερα τα δίκτυα υψηλής ταχύτητας ακολουθούν το Differentiated Services framework ώστε να μπορέσουν να παρέχουν Quality of Service και να ικανοποιήσουν τις παραπάνω απαιτήσεις.
The IPv6 header includes two QoS related fields; the Traffic Class and Flow Label fields. The 8-bit *Traffic Class* field allows the source host or a forwarding router to identify the priority of the packet. This field is analogous to the *Type of Service* field found in the IPv4 header.	Η επικεφαλίδα IPv6 περιέχει δύο πεδία σχετικά με το QoS, το Traffic Class και Flow Label. Το πεδίο Traffic Class, μήκους 8 bits, επιτρέπει σε έναν τελικό σύστημα ή σε έναν διακομιστή να αναγνωρίσει την προτεραιότητα ενός πακέτου. Το πεδίο αυτό είναι ανάλογο του πεδίου Type of Service σε μία επικεφαλίδα IPv4.
The 20-bit *Flow Label* field has been proposed to identify packets of a specific flow. The source node gives the same value to the *Flow-Label* field for each transmitted packet belonging to a flow. The values remain unchanged as the packet is transported over the networks. Routers along the end-to-end path can easily identify the flows using the *flow label* field. On the contrary, in the IPv4 networks, routers have to access the transport header in the payload of the IP packets in order to collect flow information. This imposes significant processing overheads while packet fragmentation and encryption make it impossible to distinguish packets of a flow.	Το πεδίο Flow Label, μήκους 20 bits, έχει προταθεί για να βοηθήσει στην αναγνώριση πακέτων μιας συγκεκριμένης ροής. Ο κόμβος προέλευσης δίνει την ίδια τιμή στο πεδίο Flow Label για κάθε πακέτο μίας ροής που μεταδίδει. Οι τιμές παραμένουν αμετάβλητες καθώς το πακέτο μεταδίδεται μέσω του δικτύου. Οι διακομιστές που ανήκουν στην διαδρομή των πακέτων μπορούν εύκολα να αναγνωρίσουν τις διαφορετικές ροές χρησιμοποιώντας το πεδίο Flow Label. Αντίθετα σε ένα δίκτυο IPv4, οι διακομιστές πρέπει να ελέγξουν την επικεφαλίδα του επιπέδου μεταφοράς ώστε να συλλέξουν πληροφορία για μία ροή. Αυτό κοστίζει σε επεξεργαστική ισχύ ενώ ο κατακερματισμός των πακέτων και η κρυπτογράφηση τους καθιστούν αδύνατη τον διαχωρισμό των πακέτων σε ροές.
Finally, the IPv6 protocol, in terms of QoS support, is neither superior nor inferior to its IPv4 counterpart. However, the *flow label* field in the IPv6 header is expected to simplify the provision of services in the future.	Τέλος, το πρωτόκολλο IPv6, όσον αφορά την υποστήριξη του QoS, δεν είναι ούτε ανώτερο αλλά ούτε κατώτερο από το πρωτόκολλο IPv4. Παρ' όλα αυτά το πεδίο flow label στην επικεφαλίδα IPv6 αναμένεται να απλοποιήσουν την υποστήριξη των υπηρεσιών αυτών στο μέλλον.

Click an interactive item for more details or ‘next’ to continue.	Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή για να συνεχίσετε επιλέξτε το κουμπί “Next”.

6DEPLOY Module 5: IPv6 Basic Services	6DEPLOY Module 5: Ασφάλεια στο πρωτόκολλο IPv6
INTRODUCTION Welcome to this module about IPv6 security. On completion of this module, you will understand the generic problems in security, and be able to list the main threats to security. You will also be able to describe how the IP Security architecture IPsec functions in IPv6, and which new protocols have been defined for the new IPv6 environment. More specifically, you will be introduced to the techniques that are important for IPv6 security. Click 'next' to continue.	**Εισαγωγή** Καλώς ήρθατε στην ενότητα που αφορά την ασφάλεια στο πρωτόκολλο IPv6. Με την ολοκλήρωση της ενότητας θα έχετε κατανοήσει το πρόβλημα της δικτυακής ασφάλειας και θα είστε σε θέση να απαριθμήσετε τις κύριες απειλές της. Επίσης θα είστε σε θέση να περιγράψετε πως λειτουργεί το IPsec στο πρωτόκολλο IPv6, καθώς και ποια νέα πρωτόκολλα έχουν οριστεί για το νέο αυτό περιβάλλον. Πιο συγκεκριμένα θα ενημερωθείτε για τεχνικές ιδιαίτερα σημαντικές για την ασφάλεια για το πρωτόκολλο IPv6. Πατήστε την επιλογή "Next" για να συνεχίσετε.
AIMS OF SECURITY IN IPv6 The main aims of IPv6 security are the same as the security goals of any network infrastructure. They include the following: • Robustness of the infrastructure; • Authentication, confidentiality, and integrity; • Non-repudiation; • Access control; • And, finally, IP accounting and billing.	**Στόχοι της ασφάλειας του πρωτόκολλου IPv6** Οι κύριοι στόχοι της ασφάλειας του πρωτοκόλλου IPv6 είναι οι ίδιοι όπως και σε κάθε άλλη δικτυακή υποδομή. Οι στόχοι ασφάλειας περιλαμβάνουν τα ακόλουθα: • Ευρωστία (robustness) της υποδομής. • Πιστοποίηση (authentication), εμπιστευτικότητα (confidentiality) και ακεραιότητα (integrity) • Non-repudiation • Έλεγχος πρόσβασης • IP accounting και billing
THREATS TO SECURITY IN IPv6 To achieve these goals in IPv6, a number of threats need to be countered. We will discuss the following seven security threats:	**Απειλές για την ασφάλεια στο πρωτόκολλο IPv6** Για να επιτευχθούν οι παραπάνω στόχοι στο πρωτόκολλο IPv6 θα πρέπει προηγουμένως να αντιμετωπιστούν αρκετές απειλές. Στην ενότητα αυτή θα συζητήσουμε για τις παρακάτω επτά απειλές:

• the scanning of gateways and hosts for weaknesses • the scanning for multicast addresses • unauthorised access • exposing weaknesses with NAT and weaknesses in firewalls • performance attacks with fragmented headers • protocol weaknesses • and, finally, distributed denial of service, or “DDoS” for short	• τη σάρωση των δικτυακών πυλών (gateways) και των τελικών συστημάτων για αδυναμίες, • τη σάρωση σε διευθύνσεις multicast, • την μη εξουσιοδοτημένη πρόσβαση, • την αποκάλυψη αδυναμιών στο NAT και αδυναμίες στους τοίχους ασφάλειας (firewall) • επιθέσεις κατά της επίδοσης με τη χρήση κατακερματισμένων επικεφαλίδων (fragmented headers), • αδυναμίες των πρωτοκόλλων, • Κατανεμημένη επίθεση για την άρνησης υπηρεσίας (distributed denial of service - DDoS).
A first security threat is the scanning of gateways and hosts by hackers or systems that want to break into the network or attack it. They scan all external addresses of the gateways or hosts they encounter and look for weaknesses in their security protection. Due to the large IPv6 address space, network scanning for vulnerable systems has become more complex in IPv6. An exhaustive scan on every address of a subnet has therefore become very difficult to do. Besides, port scanning software such as NMAP does not even support IPv6 network scanning. Therefore, scanning methods are likely to change with IPv6. But obviously, scanning will still occur. Because of the need for public servers to be DNS-reachable, attackers still have hosts to attack.	Μία πρώτη απειλή είναι η σάρωση (scanning) των δικτυακών πυλών (gateways) και των τελικών συστημάτων (hosts) από χάκερς (hackers) ή από συστήματα που θέλουν να εισέλθουν παράνομα ή να επιτεθούν σε αυτές τις συσκευές. Οι χάκερς εξετάζουν όλες τις εξωτερικές διευθύνσεις των δικτυακών πυλών (gateways) ή των τελικών συστημάτων που συναντούν και αναζητούν αδυναμίες στην ασφάλεια τους. Λόγω του ιδιαίτερα μεγάλου χώρου διευθύνσεων του πρωτοκόλλου IPv6, η σάρωση του δικτύου για αδύναμα συστήματα έχει γίνει σημαντικά πιο περίπλοκη. Η εξαντλητική σάρωση κάθε διεύθυνσης ενός υποδικτύου έχει γίνει πρακτικά αδύνατη. Ως συνέπεια, εφαρμογές σάρωσης, όπως η εφαρμογή NMAP, δεν υποστηρίζουν πλέον την δυνατότητα σάρωσης ενός δικτύου IPv6. Για τον παραπάνω λόγο, οι μέθοδοι σάρωσης πιθανότατα θα αλλάξουν με την καθιέρωση του IPv6. Παρ΄ όλα αυτά επιθέσεις σάρωσης θα εξακολουθήσουν να υπάρχουν. Εξαιτίας της ανάγκης οι δημόσιοι διακομιστές να είναι προσβάσιμοι μέσω του συστήματος DNS, οι επιτιθέμενοι θα έχουν ακόμα διαθέσιμους στόχους.
Furthermore, administrators may also adopt easy-to-remember addresses. And the “fixed part” of the EUI-64 address eases the way for the attacker. New techniques to harvest addresses might use information from DNS zones or logs. And finally, hackers can find new addresses to scan by compromising routers at key transit points in a network.	Επιπλέον, οι διαχειριστές ενδέχεται να υιοθετήσουν διευθύνσεις που είναι εύκολο να απομνημονευθούν. Επίσης, το σταθερό μέρος της διεύθυνσης EUI-64 διευκολύνει ακόμα περαιτέρω έναν επιτιθέμενο. Επιπλέον, υπάρχει πάντα η πιθανότητα για την ανάπτυξη νέων τεχνικών για την συλλογή διευθύνσεων με τη χρήση πληροφοριών από τις ζώνες (zones) DNS ή τα αρχεία καταγραφών (logs).
A second threat is the scanning for multicast addresses; IPv6 expects all	

implementations to support multicast. The new multicast addresses that IPv6 supports can enable attackers to identify key resources on a network and attack these. The “all node” and “all router” multicast addresses may also be used as new attack vectors. In order to make multicast addresses unreachable from the outside, they must be filtered at the border. This is the default situation if no IPv6 multicasting is enabled.	Μία δεύτερη απειλή είναι η σάρωση διευθύνσεων multicast αφού το πρωτόκολλο IPv6 απαιτεί όλες οι υλοποιήσεις να υποστηρίζουν λειτουργίες multicast. Οι νέες διευθύνσεις multicast που υποστηρίζει το IPv6 μπορεί να βοηθήσουν τους επιτιθέμενους να εντοπίσουν σημαντικούς πόρους ενός δικτύου και να επικεντρώσουν τις επιθέσεις τους σε αυτούς. Οι ειδικές διευθύνσεις multicast “all node” και “all router” μπορούν να χρησιμοποιηθούν ως νέοι στόχοι για πολλαπλές επιθέσεις. Για να μην επιτρέπεται η πρόσβαση σε διευθύνσεις multicast εκτός του δικτύου, θα πρέπει όλα τα σχετικά πακέτα να φιλτράρονται στους συνοριακούς κόμβους. Αυτή η συμπεριφορά είναι προεπιλεγμένη εφόσον δεν έχει ενεργοποιηθεί η λειτουργία IPv6 multicasting.
The security of IPv6 addresses can be improved by using Cryptographically Generated Addresses or CGAs. They are IPv6 addresses, which carry hashed information about the public key in the identifier part. While they maintain privacy, accountability by link administrators is also possible. Cryptographically generated addresses provide a binding of the IP address to public keys without requiring a key management infrastructure. Additionally, CGAs help secure IPv6 Neighbour Discovery and could help further secure Mobile IPv6 Binding information.	Η ασφάλεια των διευθύνσεων IPv6 μπορεί να βελτιωθεί αν χρησιμοποιηθούν διευθύνσεις που δημιουργούνται με κρυπτογραφία (cryptographically generated addresses) ή εν συντομία CGAs. Οι διευθύνσεις CGAs πρόκειται για διευθύνσεις IPv6 που φέρουν κατακερματισμένες πληροφορίες (hashed information) σχετικά με το δημόσιο κλειδί (public key) στο τελευταίο τμήμα της διεύθυνσης IPv6. Ενώ είναι δυνατή η διατήρηση του απορρήτου, οι διαχειριστές του δικτύου έχουν τη δυνατότητα «ελέγχου» (accountability). Οι διευθύνσεις CGA δημιουργούν μια σύνδεση μεταξύ της διεύθυνση IP και τα δημόσια κλειδιά χωρίς όμως να απαιτείται η χρήση υποδομής διαχείρισης κλειδιών (key management infrastructure). Επιπλέον, οι διευθύνσεις CGAs βοηθούν στην ασφάλεια του IPv6, Neighbour Discovery ενώ θα μπορούσαν να βοηθήσουν περαιτέρω στην ασφάλεια των πληροφοριών που ανταλλάσσονται στο Mobile IPv6.
Unauthorised access is a third threat. In IPv6, Layer 3 and Layer 4 policy implementation is still done within firewalls. However, there are some design considerations: - site-scoped multicast addresses should be filtered at the site boundaries - IPv4 mapped IPv6 addresses should be filtered on the wire - and there should be multiple addresses per interface.	Η μη εξουσιοδοτημένη πρόσβαση (unathorised access) είναι η τρίτη απειλή. Στο IPv6, η εφαρμογή των πολιτικών πρόσβασης στο επίπεδο 3 και 4 εξακολουθεί να πραγματοποιείται με λειτουργίες από τα τείχη προστασίας (firewalls). Ωστόσο, έχουν γίνει οι παρακάτω σχεδιαστικές παραδοχές: • Οι διευθύνσεις site-scoped multicast θα πρέπει να φιλτράρεται στα όρια του site, • Οι διευθύνσεις IPv4-mapped IPv6 θα πρέπει να φιλτράρεται στο τοπικό υποδίκτυο, • θα πρέπει να υπάρχουν πολλές διευθύνσεις ανά διεπαφή (interface).

Mobile IPv6 uses PANA or the Protocol for Authentication and Network Access to prevent unauthorised access. PANA provides a link layer agnostic solution which enables network access authentication. In Mobile IPv4, a mobile node interacted with a Foreign Agent for its authentication. In Mobile IPv6 networks, this authentication function is not handled by an FA but by the PANA Authentication Agent, or PAA for short.	Το mobile IPv6 χρησιμοποιεί το πρώτοκολλο PANA (πρωτόκολλο για τον έλεγχο ταυτότητας - protocol for the authentication and network access) για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης. Το PANA επιτρέπει την πιστοποίηση (authentication) για τη πρόσβαση στο δίκτυο η οποία είναι διαφανής στο επίπεδο συνδέσμου (link layer). Στο Mobile IPv4, ένας κινούμενος κόμβος αλληλεπιδρά με ένα απομακριμένο αντιπρόσωπο (foreign agent) για τον έλεγχο πιστοποίησης. Στο Mobile IPv6, η λειτουργία ελέγχου ταυτότητας δεν υλοποιείται από το FA αλλά από το αντιπρόσωπο πιστοποίησης PANA (PANA Authentication Agent), ή εν συντομία PAA.
Weaknesses in firewalls are a fourth threat. In IPv6, firewalls can be set up in multiple ways. However, to eliminate weaknesses, both the IPv6 architecture and the firewall itself must meet certain requirements.	Οι αδυναμίες στις πύλες ασφάλειας (firewalls) είναι η τέταρτη απειλή. Στο IPv6, τα firewalls μπορεί να συγκροτηθούν με διαφορετικούς τρόπους. Ωστόσο, για να εξαλειφθούν οι αδυναμίες, τόσο η αρχιτεκτονική του IPv6 όσο και το ίδιο το τείχος προστασίας πρέπει να πληρούν ορισμένες προϋποθέσεις.
As IPv6 has no need for NAT, the same level of security and privacy as IPv4 is possible with IPv6. This level is even increased because of the end-to-end security offered by the mandatory implementation of IPSec.	Εφόσον το IPv6 δεν έχει καμία ανάγκη για το πρωτόκολλο NAT, το ίδιο επίπεδο ασφάλειας και προστασίας της ιδιωτικότητας είναι δυνατή στο IPv6 σε σύγκριση με το IPv4. Το επίπεδο ασφάλειας είναι αυξάνει περαιτέρω στο IPv6 λόγω της ασφάλειας από άκρο σε άκρο (end-to-end) που προσφέρεται από την υποχρεωτική υποστήριξη του IPSec.
And because there is no need for NAT, packet filtering weaknesses can no longer be hidden. Additionally, the IPv6 architecture and firewall must support both IPv6 header chaining and IPv4/IPv6 transition and coexistence. Finally, they must not break IPv4 security. It must be ensured that, in spite of the extra complexity of the gateways, there is no effective weakness as such.	Και επειδή δεν υπάρχει ανάγκη για χρήση του πρωτοκόλλου NAT, οι αδυναμίες στο φιλτράρισμα των πακέτων δεν μπορούν πλέον να κρυφτούν. Επιπλέον, σύμφωνα με την αρχιτεκτονική IPv6, οι πύλες ασφάλειας (firewall) πρέπει να υποστηρίζουν την αλυσιδωτή σύνδεση επικεφαλίδων (header chaining) και μηχανισμούς μετάβασης IPv4/IPv6 και της συνύπαρξης των δύο πρωτοκόλλων. Τέλος, δεν πρέπει να διαραγεί η ασφάλεια για το IPv4. Πρέπει να διασφαλιστεί ότι, παρά την επιπλέον πολυπλοκότητα των δικτυακών πυλών (gateways), δεν δημιουργείται κάποια αδυναμία.
A fifth threat consists of performance attacks with fragmented headers. To avoid	Η πέμπτη απειλή αφορά τις επιθέσεις με σκοπό τη μείωση απόδοσης με χρήση επικεφαλίδων σε κατακερματισμένα IPv6 πακέτα. Για να αποφευχθεί η απειλή, ο

these, any IPv6 network administrator should follow the following best practices: • First of all, deny the IPv6 fragments destined to an internetworking device which are used as a DOS vector to attack the infrastructure • Secondly, ensure adequate IPv6 fragmentation filtering capabilities. For example, drop all packets with a routing header if you don't support MIPv6. Next, all fragments with less than 1280 octets can potentially be dropped, except the last fragment. • And finally, all fragments should be delivered in 60 seconds. If not, they should be dropped.	διαχειριστής του δικτύου IPv6 θα πρέπει να ακολουθήσετε τις ακόλουθες βέλτιστες πρακτικές: • καταρχήν, να μην επιτρέπονται «θραύσματα» που προορίζονται σε δικτυακές συσκευής τα οποία χρησιμοποιούνται για DoS επιθέσεις στην υποδομή, • δεύτερον, να εξασφαλιστούν οι κατάλληλες δυνατότητες φιλτραρίσματος κατακερματισμένων πακέτων IPv6. Για παράδειγμα, απορρίψτε όλα τα πακέτα με routing header, εάν δεν υποστηρίζεται το MIPv6. Στη συνέχεια, όλα τα θραύσματα (fragments) πακέτου με λιγότερο από 1280 octets μπορούν δυνητικά να απορρίπτονται εκτός από το τελευταίο κομμάτι. • Και τέλος, όλα τα κομμάτια θα πρέπει να παραδοθεί σε 60 δευτερόλεπτα.Αν όχι, θα πρέπει να πέσει.
A sixth security threat is formed by protocol weaknesses. In IPv4, these weaknesses can lead to IPv4 Level 3 – Level 4 spoofing, or IPv4 ARP and DHCP attacks. In IPv6, this is no longer the case. However, the gateways between the two worlds remain a serious target.	Η έκτη απειλή ασφάλειας αφορά τις αδυναμίες του πρωτοκόλλου. Στο IPv4, οι αδυναμίες αυτές μπορούν να οδηγήσουν σε πλαστογράφηση (spoofing) διευθύνσεων IPv4 στο επίπεδο 3 και 4 ή IPv4 επιθέσεις ARP και DHCP. Στο IPv6, αυτό δεν είναι εφικτό. Ωστόσο, οι δικτυακές πύλες (gateways) μεταξύ των δύο «κόσμων» παραμένουν ένα βασικό στόχο.
While level 3 spoofing remains the same, IPv6 addresses are globally aggregated. This makes spoof mitigation at aggregation points easy to deploy. Spoof mitigation is easier since the IPv6 address is hierarchical. However, the host part of the IPv6 address is not protected. For accountability, mapping of the IPv6 address to the MAC address is needed.	Ενώ η πλαστογράφηση στο επίπεδο 3 παραμένει τα ίδια, οι διευθύνσεις IPv6 αθροίζονται σε παγκόσμιο επίπεδο. Αυτό καθιστά ευκολότερη την αντιμετώπιση των προβλημάτων πλαστογράφησης (spoof) στα σημεία συνάθροισης. Η αντιμετώπιση της πλαστογράγησης (spoof) είναι ευκολότερη καθώς η διεύθυνση IPv6 είναι ιεραρχική. Ωστόσο, το τμήμα της διεύθυνσης IPv6 που αφορά το τελικό σύστημα δεν προστατεύεται. Για λόγους ελέγχου (accountability) είναι απαραίτητη η χαρτογράφηση της διεύθυνσης IPv6 με τη διεύθυνση MAC.
In IPv4, ARP and DHCP attacks were able to subvert host initialization. In IPv6, ARP is replaced by Neighbour Discovery. With Neighbour Discovery, attack tools such as "ARP cache poisoning" disappear, but prevention tools such as DHCP snooping also cease to be. Therefore, Secure Neighbour Discovery is a better solution.	Στο IPv4, οι επιθέσεις ARP και DHCP ήταν σε θέση να ανατρέψει την σωστή αρχικοποίηση ενός συστηματος. Στο IPv6, το ARP αντικαθίσταται από το Neighbour Discovery. Με το Neighbour Discovery, τα εργαλεία επίθεσης, όπως « ARP cache poisoning» εξαλείφονται αλλά τα μέσα πρόληψης, όπως η υποκλοπή (snooping) DHCP επίσης παύει να υφίστανται. Ως αποτέλεσμα, το Secure Neighbour Discovery είναι η καλύτερη λύση.

Also possible are DHCP version 6, which includes authentication, and Neighbour Discovery with IPSec.	Επιπλέον, είναι επίσης εφικτό να χρησιμοποιηθεί το πρωτόκολλο DHCP έκδοση 6, το οποίο περιλαμβάνει λειτουργίες ταυτοποίησηςη, και το πρωτόκολλο Neighbour Discovery σε συνδιασμό με το πρωτόκολλο IPSec.
A final threat lies in Distributed Denial of Service attacks. Broadcast amplification and 'Smurf' attacks, that operate by sending ICMP packets to broadcast addresses, are eliminated in IPv6, because IPv6 uses global multicast addresses instead of broadcast addresses.	Μια τελευταία απειλή αφορά τις κατανεμημένες επιθέσεις για την άρνησης υπηρεσίας (distributed denial of service - DDoS). Ενίσχυση με χρήση τεχνικών «broadcast" και επιθέσεις «smurf», που που δημιουργούνται με την αποστολή πακέτων ICMP σε διευθύνσεις broadcast, έχουν εξαλειφθεί στο IPv6 επειδή το IPv6 χρησιμοποιεί παγκόσμιες διευθύνσεις multicast αντί για διευθύνσεις broadcast.
Furthermore, IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to global multicast addresses. The danger of ICMP packets with global multicast source addresses is still unknown.	Επιπλέον, οι προδιαγραφές IPv6 απαγορεύουν τη δημιουργία των πακέτων ICMPv6 ως απάντηση σε μηνύματα προς παγκόσμιες διευθύνσεις multicast. Ο κίνδυνος των πακέτων ICMP με χρήση διευθύνσης αποστολής (source address) μιας παγκόσμιας διεύθυνσης multicast είναι ακόμα άγνωστη.
To mitigate IPv6 amplification, any host implementation must follow RFC 2463 and implement RFC 2827 ingress filtering. Finally, ingress filtering must be applied to all IPv6 packets from an IPv6 multicast source address.	Για την άμβλυνση ενίσχυση επιθέσεων στο IPv6, τα τελικά συστήματα οφείλουν να ακολουθεί την λειτουργικότητα που περιγράφεται στα RFC2463 και να εφαρμόζουν της λειτουργίες φιλτραρίσματος εισερχόμενης κίνησης που αναφέρεται στο RFC2827. Τέλος, το φιλτράρισμα της εισερχόμενης κίνησης πρέπει να εφαρμόζεται σε όλα τα IPv6 πακέτα που προέρχονται από διεύθυνση αποστολής με IPv6 multicast.

IP SEC

Just like IPv4 networks, IPv6 networks need to cope with multiple threats. But unlike in IPv4, where IPSec is optional, in IPv6 the security infrastructure IPSec is part of the protocol suite; a compliant implementation must support IPSec.

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 IPSec is optional in IPv4, it is mandatory in IPv6.

IPSec provides the following optional network security services:

- data confidentiality: the IP sender can encrypt packets before sending them across a network
- data integrity: the IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission. Key management requires a PKI infrastructure and a key exchange mechanism such as the simplified Internet Key Exchange IKE version 2. A new and simplified IKE, IKE version 2, will be available soon.
- data origin authentication: the IPSec receiver can authenticate the source of the sent IPSec packets. This service is dependent on the data integrity service.
- antireplay: the IPSec receiver can detect and reject replayed packets.

IP SEC

Ακριβώς όπως δίκτυα IPv4, το δίκτυα IPv6 πρέπει να αντιμετωπίσουν πολλαπλές απειλές. Αλλά σε αντίθεση με το IPv4, όπου η υποστήριξη του IPSec είναι προαιρετική, στο IPv6 η υποστήριξη του IPSec είναι μέρος του πρωτοκόλλου. Μία πλήρη υλοποίηση πρέπει να υποστηρίζει το IPSec.

Οι υπηρεσίες IPSec εξαρτώνται εξ ολοκλήρου από τον μηχανισμούς που σχετίχονται με την επικεφαλίδα ταυτοποίησης (authentication header) και την επικεφαλίδα ασφαλούς ενθυλάκωσης του ωφέλιμου φορτίου (encapsulating security payload header). Οι δύο επικεφαλίδες ορίζονται τόσο για το IPv4 όσο και για IPv6. Όταν το IPSec χρησιμοποιείται στο IPv4, οι επικεφαλίδες ασφάλειας προστίθονται ως επιλογές (options) στην κύρια επικεφαλίδα IPv4. Όμως, ενώ η χρήση του IPSec είναι προαιρετική σε IPv4, είναι υποχρεωτική για το IPv6.

Το IPSec παρέχει τις ακόλουθες προαιρετικές δικτυακές υπηρεσίες ασφάλειας:

- εμπιστευτικότητα δεδομένων (data confidentiality): ο αποστολέας μπορεί να κρυπτογραφήσει τα πακέτα IP πριν από την αποστολή τους στο δίκτυο
- ακεραιότητα των δεδομένων (data integrity): ο δέκτης μπορεί να ταυτοποιήσει τα πακέτα που αποστέλλονται από τον αποστολέα που χρησιμοποιεί IPSec ώστε να διασφαλιστεί ότι τα δεδομένα δεν έχουν αλλαχτεί κατά τη μεταφορά τους. Η διαχείριση των κλειδιών (key management) απαιτεί την ύπαρξη υποδομής KPI και ένα βασικό μηχανισμό ανταλλαγής κλειδιών, όπως το «απλοποιημένο» Internet Key Exchange έκδοση ή εν συντομία IKE v2. Το νέο απλουστευμένο IKEv2 θα είναι σύντομα διαθέσιμο.
- ταυτοποίηση προέλευσης των δεδομένων (data origin authentications): ο παραλήπτης δεδομένων μπορεί ελέγξει την πηγή των πακέτων που προώθησε ένα αποσοτλέας με χρήση του IPSec. Η υπηρεσία αυτή εξαρτάται από την υπηρεσία της διασφάλισης της ακεραιότητας των δεδομένων (data integrity service).
- antireplay: ο παραλήπτης μπορεί να ανιχνεύσει και να απορρίψει τα πακέτα που έχουν εναπαληφθεί.

IPSec allows data to 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 end-to-end. Data may be encrypted along the entire path between a source node and a destination node. With IPsec, IPv6 is less likely to fall victim to a sniffing attack or a man-in-the-middle attack than IPv4. Additionally, to prevent IPv6 routing attacks, IPSec can secure protocols such as OSPF version 3 and RIP new generation. Therefore, network implementers should enable IPSec in every IPv6 node, potentially making the networks more secure. Click one of the items on the screen for more details. Or test your understanding by clicking the 'Test' button. To continue, click 'Next'.	Το IPSec επιτρέπει στα δεδομένα να σταλούν σε ένα δημόσιο δίκτυο χωρίς παρατήρηση, τροποποίηση, ή πλαστογράφηση. Η λειτουργικότητα IPsec είναι κατ' ουσίαν ταυτόσημη για το IPv6 και IPv4. Ωστόσο, το IPSec στο IPv6 μπορεί να εφαρμοστεί από άκρο σε άκρο (end-to-end). Τα δεδομένα μπορούν να κρυπτογραφηθούν σε όλο το μήκος της διαδρομής μεταξύ του αποστολέα και του παραλήπτη. Με το IPSec, η επικοινωνία πάνω από IPv6 είναι λιγότερο πιθανό να επηρεαστεί από επίθεσης sniffing ή επίθεση "man-in-the-middle" σε σχέση με το IPv4. Επιπλέον, για την αποτροπή επιθέσεων δρομολόγησης στο IPv6, το IPSec μπορεί να εξασφαλίσει πρωτόκολλα, όπως το OSPFv3 και RIPng. Ως εκ τούτου, οι διαχειριστές του δικτύου θα πρέπει να ενεργοποιούν το IPSec σε κάθε κόμβο IPv6, πιθανώς καθιστώντας τα πιο ασφαλή δίκτυα. Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε επιλέξτε το κουμπί "Next".

6DEPLOY Module 6: IPv6 Routing, mobility and management **INTRODUCTION** 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.	**6DEPLOY Ενότητα 6: Δρομολόγηση, Κινητικότητα και Διαχείριση στο πρωτόκολλο IPv6** **Εισαγωγή** Καλώς ήρθατε στην ενότητα για την δρομολόγηση, την κινητηκότητα και την διαχείριση στο πρωτόκολλο IPv6. Στο τέλος αυτής της ενότητας θα μπορείτε να απαριθμήσετε τα πρωτόκολλα Interior Gateway (IGP) και Exterior Gateway (EGP) που υποστηρίζουν το πρωτόκολλο IPv6. Επίσης θα μπορείτε να εξηγήσετε πως λειτουργούν τα παραπάνω πρωτόκολλα. Ακόμα θα μπορείτε να περιγράψετε το πρωτόκολλο Mobile IPv6 και να εξηγήσετε τον τρόπο λειτουργίας του. Τέλος θα μπορείτε να περιγράψετε τις αλλαγές που φέρνει το πρωτόκολλο IPv6 στον τομέα της διαχείρισης δικτύων. Πατήστε την επιλογή "Next" για να συνεχίσετε.

ROUTING PROTOCOLS

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
- the IS-IS protocol, which stands for Intermediate System to Intermediate System Protocol
- and OSPF, or Open Shortest Path First Protocol.

For IPv6, the RIP protocol has been extended to what is called “RIPng”, 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, as the destination address for RIP update messages. As the transport layer for the protocol messages, RIPng uses IPv6. Each address specified as a next hop must be a link-local address.

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

Πρωτόκολλα Δρομολόγησης

Για να ικανοποιήσει την απαίτηση για αλγορίθμους δρομολόγησης που κλιμακώνουν ικανοποιητικά, το πρωτόκολλο IPv6 υποστηρίζει τα υπάρχοντα πρωτόκολλα IGP και EGP. Όπως και στο IPv4 το κριτήριο για την δρομολόγηση είναι το μεγαλύτερο δυνατό ταίριασμα προθέματος.

Το IGP είναι ένα δικτυακό πρωτόκολλο που διανέμει πληροφορίες δρομολόγησης στους δρομολογητές και τις πύλες ενός αυτόνομου δικτύου.

Τα πιο διαδεδομένα πρωτόκολλα IGP είναι τα εξής:

- το Routing Information Protocol (RIP)
- το Intermediate System to Intermediate System (IS-IS)
- το Open Shortest Path First (OSPF)

Για το IPv6, το πρωτόκολλο RIP έχει επεκταθεί στο “RIPng”, ή αλλιώς “Routing Information Protocol Next-Generation”. Το πρωτόκολλο αυτό λειτουργεί με τον ίδιο τρόπο και προσφέρει τα ίδια πλεονεκτήματα όπως και η δεύτερη έκδοση του πρωτοκόλλου RIP για το IPv4. Οι επεκτάσεις του RIP περιλαμβάνουν υποστήριξη για διευθύνσεις και προθέματα IPv6, όπως το “next hop IPv6 addresses”.

Το RIPng χρησιμοποιεί την διεύθυνση multicast “all-RIP routers” (FF02::9) ως προορισμό για τα μηνύματα RIP update. Ως επίπεδο μεταφοράς για τα μηνύματα του πρωτοκόλλου το RIPng χρησιμοποιεί το IPv6. Κάθε διεύθυνση που χαρακτηρίζεται ως next hop πρέπει να είναι διεύθυνση link-local.

Το IS-IS είναι ένα πρωτόκολλο δρομολόγησης IGP. Δυνατότητα δρομολόγησης για το IPv6 έχει προστεθεί στο ήδη υπάρχον πρωτόκολλο.

Η ανταλλαγή πληροφορίας σχετική με την δρομολόγηση του IPv6, στο πρωτόκολλο IS-IS, επιτυγχάνεται με την προσθήκη των 2 παρακάτω type-length-values, ή TLVs για συντομία:

• « IPv6 Interface Address ». A new IPv6 protocol identifier has also been added to IS-IS. Most of the algorithms of Open Shortest Path First protocol or OSPF version 3 are the same in OSPFv2. Still, some changes have been made in OSPFv3. More specifically, they handle the increased address size in IPv6 and the fact that OSPFv3 runs directly over IPv6. Because OSPFv2 is heavily dependent on the IPv4 address for its operation, changes were necessary in the OSPFv3 protocol to support IPv6. Some of the notable changes include: • OSPFV3 runs per-link rather than per-subnet, • and offers explicit support for multiple instances per link. • Addressing semantics are removed, • a Link-local flooding scope is added • and changes are made in authentication and packet format. Like RIPng, IPv6 OSPFv3 uses IPv6 for transport and uses link-local addresses as source address. All routers running OSPF should be prepared to receive packets sent to the "ALLSPFRouters" multicast group address FF02::5, which has the following format. But the Designated Router and the Backup Designated Router must also be prepared to receive packets destined to the "ALLDRouters" multicast group address, which has the following format.	• το “IPv6 Reachability” • το “IPv6 Interface Address” Επίσης στο πρωτόκολλο IS-IS έχει προστεθεί ένα νέο αναγνωριστικό για το πρωτόκολλο IPv6. Οι περισσότεροι από τους αλγορίθμους του OSPFv3 είναι ίδιοι με τους αντίστοιχους αλγορίθμους για το OSPFv2. Παρ’ όλα αυτά υπήρξαν κάποιες αλλαγές στην τρίτη έκδοση του OSPF. Πιο συγκεκριμένα το OSPFv3 έχει την δυνατότητα να χειρίζεται τον μεγαλύτερο χώρο διευθύνσεων του IPv6, ενώ επίσης λειτουργεί πάνω από το πρωτόκολλο IPv6. Επειδή το OSPFv2 εμφάνιζε μεγάλη εξάρτηση από το IPv4 κατά την λειτουργία του, ήταν απαραίτητο να γίνουν κάποιες αλλαγές ώστε το OSPFv3 να υποστηρίζει το IPv6. Μερικές από τις πιο σημαντικές αλλαγές είναι οι εξής: • Το OSPFv3 λειτουργεί ανά τοπικό σύνδεσμο και όχι ανά υποδίκτυο • Προσφέρει υποστήριξη για πολλαπλά στιγμιότυπα ανά σύνδεσμο • Έχουν αφαιρεθεί τα addressing semantics • Έχει προστεθεί ένα link-local scope • Αλλαγές έχουν γίνει επίσης και στην διαδικασία ταυτοποίησης καθώς και στην δομή των πακέτων. Όπως και στο RIPng έτσι και το OSPFv3 χρησιμοποιεί το IPv6 στο επίπεδο μεταφοράς καθώς και link-local διευθύνσεις ως διευθύνσεις προέλευσης. Όλοι οι δρομολογητές που χρησιμοποιούν το OSPF θα πρέπει να είναι ικανοί να λαμβάνουν πακέτα σταλμένα στην διεύθυνση multicast “ALL SPF Routers” (F02::5) η οποία έχει την παρακάτω δομή. Ακόμα ο ορισμένος (designated) δρομολογητής και οι εφεδρικοί ορισμένοι (designated) δρομολογητές θα πρέπει να είναι προετοιμασμένοι να λάβουν πακέτα σταλμένα στην διεύθυνση multicast “ALLDRouters” η οποία έχει την παρακάτω δομή.

OSPFv3 is an IPv6-only protocol, but there is some work-in-progress about extensible mechanisms to enable it with the support for different address families. 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 Network Layer Reachability Information, which is expressed as an IPv4 address prefix. 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 • and Multiprotocol Unreachable NLRI The first attribute 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 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'.	Το OSPFv3 είναι ένα πρωτόκολλο που υποστηρίζει μόνο το IPv6, όμως είναι σε εξέλιξη προσπάθειες για την επέκταση του ώστε να γίνει συμβατό και με άλλες οικογένειες διευθύνσεων. Το EGP είναι ένα πρωτόκολλο που διανέμει πληροφορίες δρομολόγησης συνοριακών δρομολογητών (**border routers**) διαφορετικών αυτόνομων συστημάτων. Το Mutliprotocol Border Gateway Protocol είναι ένα πρωτόκολλο δρομολόγησης EGP που υποστηρίζει πολλά πρωτόκολλα μεταφοράς και το οποίο καθιερώθηκε τόσο για το IPv4 όσο και για το IPv6. Μόνο τρία στοιχεία του BGP σχετίζονται αποκλειστικά με το IPv4: • Το χαρακτηριστικό "NEXT_HOP", που εκφράζεται ως μία διεύθυνση IPv4 • Το "AGGREGATOR", που περιέχει μία διεύθυνση IPv4 • Το "Network Reachability Information", που εκφράζεται ως πρόθεμα μίας IPv4 διεύθυνσης Με άλλα λόγια, για να υπάρχει συμβατότητα με προηγούμενα πρωτόκολλα καθώς και για να απλοποιηθεί η εισαγωγή δυνατοτήτων υποστήριξης πολλαπλών πρωτοκόλλων στο BGP-4, δημιουργήθηκαν 2 νέα χαρακτηριστικά: • Το Multiprotocol Reachable NLRI • Το Multiprotocol Unreachable NLRI Το πρώτο χαρακτηριστικό διατηρεί τις διευθύνσεις με τις οποίες είναι εφικτή η επικοινωνία καθώς και την πληροφορία next hop, η οποία θα προωθηθεί στις διευθύνσεις αυτές. Το δεύτερο διατηρεί τις διευθύνσεις με τις οποίες δεν είναι εφικτή η επικοινωνία. Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε επιλέξτε το κουμπί "Next".

MOBILITY

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.

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

Κινητικότητα (Mobility)

Το Mobile IP είναι ένα πρότυπο (standard) το οποίο επιτρέπει στις φορητές συσκευές να μετακινούνται διατηρώντας τις υπάρχουσες συνδέσεις τους. Στο IPv4 η κινητικότητα (mobility) πρέπει να προστεθεί ως νέο χαρακτηριστικό. Αντίθετα στο IPv6 υπάρχει εγγενής υποστήριξη λειτουργιών κινητικότητας και κάθε κόμβος IPv6 μπορεί να την χρησιμοποιήσει όποτε είναι απαραίτητη.

Το Mobile IPv6 προέρχεται από το Mobile IP αλλά δεν χρησιμοποιεί την ενθυλάκωση (encapsulation) πακέτων IP όπως στο IPv4. Στο IPv6 χρησιμοποιείται η επικεφαλίδα επέκτασης (extension header) για το Mobile IP και ειδικότερα η επικεφαλίδα «Destination Options». Με τον τρόπο αυτό αποφεύγεται η τριγωνική δρομολόγηση (triangle routing). Η κινητικότητα στο IPv6 είναι πλέον πιο αποδοτική για τις τελικές συσκευές.

Περαιτέρω καινοτομίες του IPv6 έχουν εξίσου απλοποιήσει τους απαραίτητους μηχανισμούς όπως :

- Stateless autoconfiguration
- Neighbor Discovery Protocol

ενώ οι μηχανισμοί ταυτοποίησης και κρυπτογράφησης, … … κάνουν εμφανές ότι το Mobile IPv6 θα είναι ευκολότερο να υλοποιηθεί και να χρησιμοποιηθεί σε σχέση με το Mobile IPv4.

Το Mobile IPv6 θα λειτουργεί με τον ακόλουθο τρόπο:
Ένα κινούμενο τελικό σύστημα (host) μπορεί να μεταβάλλει το σημείο πρόσβασης του στο διαδίκτυο παραμένοντας όμως προσβάσιμος από την οικεία διεύθυνση (home address). Η οικεία διεύθυνση (home address) είναι η στατική διεύθυνση IP ενός κινούμενου συστήματος, η οποία είναι έγκυρη στο οικείο (home) δίκτυο του.

Τα IP πακέτα που έχουν ως προορισμό την οικεία διεύθυνση (home address) ενός κινούμενου συστήματος δρομολογούνται, με διαφανή τρόπο, στη διεύθυνση φιλοξενίας (C/o ή care-of address) του τελικού συστήματος. Η διεύθυνση

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. 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'.	φιλοξενίας (care-of address) είναι μία προσωρινή διεύθυνση IP και η οποία αντιστοιχεί στον κινούμενο σύστημα όταν συνδέεται σε υποδίκτυα διαφορετικά από το οικείο δίκτυο του. Τα πακέτα δρομολογούνται από την οικεία διεύθυνση (home address) στη διεύθυνση φιλοξενίας (care-of address) από μία λειτουργική οντότητα που ονομάζεται οικείος αντιπρόσωπος (home agent). Στο Mobile IPv4 εντοπίζεται έναν κινούμενο τελικό σύστημα όταν δηλώνει την παρουσία του σε έναν απομακρυσμένο εκπρόσωπο (foreign agent). Εν συνέχεια, ο οικείος εκπρόσωπος (home agent) αποστέλλει τα πακέτα στο απομακρυσμένο δίκτυο. Στο mobile IPv6 οι διευθύνσεις φιλοξενίας (care-of address) που αποδίδονται από τον απομακρυσμένο αντιπρόσωπο (foreign agent) έχουν καταργηθεί. Η συσχέτιση μεταξύ της οικείας διεύθυνσης (home address) και της διεύθυνσης φιλοξενίας (care-of address) επιτρέπει σε κάθε πακέτο που προορίζεται για τον κινούμενο κόμβο να δρομολογείται στην διεύθυνσης φιλοξενίας. Α ταχεία μνήμη δεσμεύσεων (binding cache) αποτελεί τη μνήμη που διατηρεί τη διεύθυνση φιλοξενίας (care-of addresses) που έχει προηγουμένως αποκτηθεί. Η διεύθυνση φιλοξενίας (care-of address) έχει καταγραφεί από τον οικείο αντιπρόσωπο (home agent) με τη χρήση μηνύματος «binding update», το οποίο αποστέλλεται από τον κόμβο στον οικείο αντιπρόσωπο (home agent), καθώς και με τη χρήση ενός μηνύματος binding acknowledgement, το οποίο αποστέλλεται από τον home agent στον κόμβο ώστε να επιβεβαιωθεί η ενημερωση. Για να επιτευχθεί αυτού του είδους η κινητικότητα, το Mobile IPv6 ορίζει τεσσερις νέες επιλογές για προορισμούς IPv6. • Την επιλογή binding update • Την επιλογή binding acknowledgement • Την επιλογή binding request • Την επιλογή home address Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις

	γνώσεις επιλέγοντας το κουμπί “Test”. Για να συνεχίσετε επιλέξτε το κουμπί “Next”.
NETWORK MANAGEMENT	**Διαχείριση Δικτύου**
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.	Το σημαντικότερο πρότυπο διαχείρισης που χρησιμοποιείται σε δίκτυα IPv4 είναι το SNMP ή αλλιώς Simple Network Management Protocol. Μια προφανής συνέπεια του παραπάνω είναι η επιδίωξη να επεκταθεί το SNMP ώστε να υποστηρίζει το 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.	Σήμερα πολλοί προμηθευτές δικτυακών υπηρεσιών υποστηρίζουν SNMP πάνω από IPv6 και οι δρομολογητές μπορούν πλέον να παρακολουθούνται (monitored) μέσω ενός περιβάλλοντος που υποστηρίζει μόνο IPv6. Συσκευές οι οποίες δεν υποστηρίζουν SNMP πάνω από IPv6 μπορούν να ελέγχονται μέσω IPv4 δεδομένου ότι τα περισσότερα δίκτυα στηρίζονται σε υβριδικές υλοποιήσεις διπλής στοίβας (dual stack).
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.	Το SNMP στηρίζεται στα Management Information Bases ή MIBs. Οι MIBs πρέπει να είναι ικανές να συλλέγουν πληροφορίες γαι το IPv6. Το 1988, ορίστηκε σύμβαση που περιέγραφε αποκλειστικά διευθύνσεις IPv6. Αυτή η προσέγγιση επιλέχθηκε στις αρχές της ανάπτυξης του πρωτοκόλλου IPv6 και επέτρεψε τη διαχείριση δικτύων IPv6 χωρίς να χρειάζεται μεταβολή στις ήδη υπάρχουσες MIBs.
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.	Για παράδειγμα, το 1988 δημοσιεύθηκαν οι IPv6 MIB, ICMPv6 MIB, TCP over IPv6 MIB και το UDP over IPv6 MIB. Η προσέγγιση αυτή όμως προϋπόθετε την διαφοροποίηση των IPv4 και IPv6 MIBs. Με άλλα λόγια θα έπρεπε να δαπανηθεί διπλή προσπάθεια για να υποστηρίξουν όλες οι MIBs και τις δύο εκδόσεις του πρωτοκόλλου IP.
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.	Ευτυχώς μία άλλη προσέγγιση βρισκόταν στα σκαριά. Στηριζόταν σε σύμβαση που αφορούσε μια ενιαία MIB (unified MIB), όπου η ίδια MIB μπορεί να εξυπηρετήσει τόσο το IPv4 όσο και το IPv6 πρωτόκολλο. Για να το επιτύχει, η δομή του «address data» έπρεπε να μεταβληθεί εκ νέου. Ανάλογα με τον κατασκευαστή εξοπλισμού, διαφορετικές MIB μπορούσαν πλέον να υλοποιηθούν.

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.	Το SNMP είναι το πιο διαδεδομένο πρωτόκολλο για τη διαχείριση σφαλμάτων (**fault management**). Όμως η διαχείριση δικτύων καλύπτει πολλούς ακόμα τομείς συμπεριλαμβανομένου και του «accounting» . Το πρότυπο IPFIX υποστηρίζει τον έλεγχο ροών IPv6. Ακόμα μερικά "κλειστά" (proprietary) πρωτόκολλα αναβαθμίστηκαν για να υποστηρίξουν την εξαγωγή ροών σε IPv6. Για παράδειγμα το πρωτόκολλο Netflow έκδοση v9 μπορεί να εξάγει ροές IPv6.
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.	Η διαχείριση συγκρότησης (configuration management) μπορεί επίσης να πραγματοποιηθεί μέσω IPv6. Τα πρωτόκολλα TELNET, SSH, FTP, TFTP αναβαθμίστηκαν και μπορούν να χρησιμοποιηθούν για να ελέγχουν την διαμόρφωση ενός δρομολογητή μέσω ενός δικτύου IPv6.
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 plenty of tools capable of managing an IPv6 network. Today, getting a good view at what is happening in an IPv6 network is possible.	Ακόμα και αν οι IPv6 counters δεν ενημερώνονται πάντα και απουσιάζουν σημαντικά συστατικά της διαχείρισης δικτύων, καθώς δεν υποστηρίζονται όλες οι MIBs, υπάρχει πληθώρα εργαλείων που μπορούν να διαχειριστούν ένα IPv6 δίκτυο. Στις μέρες μας είναι πλέον εφικτό να σχηματήσει κανείς μία καλή εικόνα για την κατάσταση ενός IPv6 δικτύου.
Click one of the items on the screen for more details. Or test your understanding by clicking the 'test' button. To continue, click 'next'.	Επιλέξτε ένα διαδραστικό στοιχείο για περισσότερες λεπτομέρειες ή δοκιμάστε τις γνώσεις επιλέγοντας το κουμπί "Test". Για να συνεχίσετε επιλέξτε το κουμπί "Next".

For any comments or corrections regarding the translation of the English text to Greek, please a message to the email address "aliako@grnet.gr"	*Για σχόλια που αφορούν την μετάφραση στα ελληνικά, παρακαλώ στείλτε μήνυμα στην ηλεκτρονική διεύθυνση "aliako@grnet.gr"*