Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**IPv6 Ασφάλεια**
Ονοματεπώνυμο Φοιτητή	**Ιωάννης Κουριέρης**
Πατρώνυμο	**Παναγιώτης**
Αριθμός Μητρώου	**ΜΠΣΠ/09025**
Επιβλέπων	**Νικόλαος Αλεξανδρής, Καθηγητής**

Ημερομηνία Παράδοσης **Ιούλιος 2011**

Τριμελής Εξεταστική Επιτροπή

Νικόλαος Αλεξανδρής Καθηγητής	Γεώργιος Τσιχριντζής Καθηγητής	Παναγιώτης Κοτζανικολάου Λέκτορας

Ευχαριστώ θερμά τον Δρ. κ. Πατσάκη Κωνσταντίνο για την σημαντική βοήθεια και την καθοδήγησή του καθ' όλη την διάρκεια της συγγραφής της παρούσας μεταπτυχιακής διατριβής και την οικογένεια μου για την πολύτιμη συμπαράσταση της.

Περιεχόμενα

ΠΕΡΙΛΗΨΗ **8**

ABSTRACT **8**

ΕΙΣΑΓΩΓΗ **9**

ΚΕΦΑΛΑΙΟ 1 ..... **10**

ΑΝΑΓΚΗ ΚΑΙ ΛΟΓΟΙ ΜΕΤΑΒΑΣΗΣ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ IPV6 ..... **10**

1.1 Περιορισμενη διαθεσιμοτητα διευθυνσεων 10
1.2 Αυτορρυθμιση διευθυνσης και απλοποιηση της διαχειρισης δικτυων 11
1.3 Υποστηριξη φορητοτητας και αυξηση της αποδοτικοτητας 12
1.4 Αναβαθμιση της Ποιοτητας Υπηρεσιων 14
1.5 Ασφαλεια 15
1.6 Συμπερασματα 16

ΚΕΦΑΛΑΙΟ 2 ..... **17**

ΕΙΣΑΓΩΓΗ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ IPV6 ..... **17**

2.1 Η δομη του IPv6 17
2.2 Η διευθυνσιοδοτηση στο IPv6 21
2.3 Αυτορυθμιση διευθυνσεων και σταθμων 23
2.4 Η δρομολογηση στο IPv6 24
2.4.1 Τα πρωτόκολλα δρομολόγησης 25
2.4.2 Το πρωτόκολλο ICMPv6 26
2.4.3 Το πρωτόκολλο Εύρεσης Γειτόνων στο IPv6 27
2.5 Θεματα Αποδοσης 28

ΚΕΦΑΛΑΙΟ 3 ..... **29**

ΠΡΟΧΩΡΗΜΕΝΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΟΥ IPV6 ..... **29**

3.1 Δικτυα και Ασφαλεια 29
3.2 Στοχοι Επιτευξης Ασφαλειας 30
3.3 IP Security (IPsec) 31
3.4 Οι IPv6 Επικεφαλιδες Ασφαλειας 32
3.4.1 Επικεφαλίδα Encapsulating Security Payload (ESP) 32
3.4.2 Η Επικεφαλίδα Πιστοποίησης (AH-Authentication Header) 34
3.5 Διαχειριση Κλειδιου 35
3.5.1 Το Πρωτόκολλο Oakley Key Determination 36
3.5.2 Το πρωτόκολλο ISAKMP 37
3.5.3 Internet Key Exchange (IKE) 39
3.6 Εφαρμογες των χαρακτηριστικων ασφαλειας του IPv6 40
3.6.1 VPN (Εικονικά Ιδιωτικά Δίκτυα) 40

3.6.2 Ασφάλεια στο επίπεδο-εφαρμογών και δρομολόγησης *41*

ΚΕΦΑΛΑΙΟ 4 ..... **43**

Η ΔΙΑΣΦΑΛΙΣΗ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΜΕΤΑΒΑΣΗΣ **43**

4.1 Η ΚΑΤΑΝΟΗΣΗ ΤΩΝ ΜΗΧΑΝΙΚΩΝ ΜΕΤΑΒΑΣΗΣ ΑΠΟ ΤΟ IPv4 ΣΤΟ IPv6 43
4.1.1 Ο Μηχανισμός Διπλής Στοίβας (Dual-Stack) *43*
4.1.2 Οι Μηχανισμοί Tunneling *45*
4.2 ΤΕΧΝΙΚΕΣ ΜΕΤΑΦΡΑΣΗΣ 49
4.3 Η ΔΙΑΣΦΑΛΙΣΗ ΤΗΣ ΤΕΧΙΚΗΣ ΜΕΤΑΒΑΣΗΣ ΜΕΣΩ TUNNELS 50
4.3.1 Η ασφάλεια των στατικών Tunnels *51*
4.3.2 Η Ασφάλεια των Δυναμικών Tunnels *51*
4.4 IPv6 ΛΑΝΘΑΝΟΥΣΕΣ ΑΠΕΙΛΕΣ ΕΝΑΝΤΙΑ ΣΤΑ IPv4 ΔΙΚΤΥΑ 54
4.5 ΣΥΜΠΕΡΑΣΜΑΤΑ 55

ΚΕΦΑΛΑΙΟ 5 ..... **56**

ΕΠΙΘΕΣΕΙΣ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ IPV6 ..... **56**

5.1 ΕΠΙΘΕΣΕΙΣ ΣΤΑ ΔΙΚΤΥΑ ΓΕΝΙΚΑ 56
5.2 ΟΙ ΤΡΥΠΕΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ IPv6 57
5.3 ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΠΡΟΣΟΜΟΙΩΣΗΣ ΤΗΣ ΕΠΙΘΕΣΗΣ 59
5.4 ΕΠΙΚΕΦΑΛΙΔΑ ΔΙΑΣΠΑΣΗΣ 60
5.4.1 Θέματα Ασφαλείας από τον κατακερματισμό πακέτων *60*
5.4.2 Προσομοίωση Επίθεσης Κατακερματισμού *62*
5.4.3 Τρόπος Αντιμετώπισης των Επιθέσεων Κατακερματισμού *65*
5.5 Η ΔΙΑΔΙΚΑΣΙΑ ΡΥΘΜΙΣΗΣ ΤΟΥ ΔΡΟΜΟΛΟΓΗΤΗ 68

ΚΕΦΑΛΑΙΟ 6 ..... **73**

ΣΥΜΠΕΡΑΣΜΑΤΑ **73**

ΒΙΒΛΙΟΓΡΑΦΙΑ **74**

Λίστα Εικόνων

Εικονα 1.1 Χρηση του NAT για εξοικονομηση χωρου διευθυνσεων 10
Εικονα 1.2 Χρηση του Mobile Ipv6 13
Εικονα 2.1 Η βασικη επικεφαλιδα του Ipv6 17
Εικονα 2.2 Οι επικεφαλιδες επεκτασης του Ipv6 19
Εικονα 2.3 Η δομη του ICMPv6 μηνυματος στο Ipv6 πακετο 26
Εικονα 3.1: Μοντελο ασφαλειας IPv6 30
Εικονα 3.2: Δομη Πρωτοκολλου ESP-Encapsulating Security Payload 33
Εικονα 3.3: Η δομη της Επικεφαλιδας Πιστοποιησης 34
Εικονα 3.4: Η δομη της επικεφαλιδας ISAKMP 37
Εικονα 4.1: Ο μηχανισμος Μεταβασης Διπλης Στοιβας(Dual-Stack) 44
Εικονα 4.2: Διαδικασια επιλογης πρωτοκολλου επικοινωνιας ενος dual-stack σταθμου μεσω DNS 45
Εικονα 4.3: Site-to-Site τυπος tunnel 45
Εικονα 4.4: Η δομη του πακετου στην τεχνικη Configured Tunnels 46
Εικονα 4.5: Περιπτωση εφαρμογης της 6to4 τεχνικης 47
Εικονα 4.6: Περιπτωση χρησης του ISATAP μηχανισμου 48
Εικονα 4.7: Η αρχιτεκτονικη δικτυου με την χρηση Terredo Tunnel 49
Εικονα 4.8: Η λειτουργια του μηχανισμου μεταφρασης NAT-PT 50
Εικονα 5.1: Η διαδικασια κατακερματισμου πακετου 61
Εικονα 5.2: Απεικονιση διαγραμματος δικτυου επιθεσης κατακερματισμου 62
Εικονα 5.3: Δημιουργια κατακερματισμου πακετων 63
Εικονα 5.4:Έναρξη επιθεσης κατακερματισμου 64
Εικονα 5.5: Αποτελεσματα επιθεσης κατακερματισμου 64
Εικονα 5.6: ICMPv6 μηνυμα σφαλματος 64
Εικονα 5.7: Διαδικασια ελεγχου ενος non-stateful firewall 65
Εικονα 5.8: Διαδικασια ελεγχου ενος stateful firewall 65
Εικονα 5.9 : Ρυθμιση και εκχωρηση ονοματος στο interface του router 69
Εικονα 5.10 : Εκχωρηση κωδικου για την εισαγωγη στο interface του router 69
Εικονα 5.11: Εντολες διαμορφωσης εκκινησης ακολουθιας 70
Εικονα 5.12: Εντολες ρυθμισης Telnet 70
Εικονα 5.13: Εντολες ρυθμισης και εκχωρησης της IP address στο router 71

Λίστα Πινάκων

Πινακας 2.1 Η multicast Ipv6 διευθυνση 22
Πινακας 2.2 Συμπιεσμενη μορφη Ipv6 διευθυνσεων 23
Πινακας 2.3 Τα βασικα μηνυματα που χρησιμοποιει το ICMPv6 27
Πινακας 3.1 Τυποι των μηνυματων που ανταλλασουν οι δρομολογητες και χρηζουν προστασιας 42
Πινακας 5.1 : Εντολες δημιουργιας κατακερματισμου πακετου 63
Πινακας 5.2: Εντολες εναρξης και εμφανισης αποτελεσματων της επιθεσης κατακερματισμου 64
Πινακας 5.4: Αλγοριθμος για την διαδικασια ελεγχου fragments απο το firewall 66
Πινακας 5.5: Access List Control για την απορριψη των fragments 67
Πινακας 5.6: Εντολη ρυθμισης router απο την αρχη 68
Πινακας 5.7: Εντολες εκχωρησης ονοματος interface και κωδικου 69
Πινακας 5.7: Εντολη διαμορφωσης εκκινησης ακολουθιας 70
Πινακας 5.8: Εντολες ρυθμισης της IPv6 διευθυνσης του C1 υπολογιστη 71
Πινακας 5.9: Ολοκληρωση ρυθμισης της IPv6 διευθυνσης του C1 μηχανηματος 72
Πινακας 5.9: Επιτευξη IPv6 επικοινωνιας μεταξυ των υπολογιστων C1 και C2 72

Περίληψη

Το πρωτόκολλο IPv6 αποτελεί την νεώτερη έκδοση του πρωτοκόλλου το οποίο χρησιμοποιείται για την επικοινωνία στο Διαδίκτυο. Το IPv6 αναπτύσσεται πάνω από 10 χρόνια και ακόμα η εφαρμογή του είναι σε μικρό επίπεδο, σε σημείο να θεωρείται κυρίως «ερευνητικό εργαλείο». Η σχεδίασή του στηρίχθηκε στην εκτεταμένη εμπειρία που αποκτήθηκε με το πέρασμα των χρόνων από την λειτουργία και την ραγδαία ανάπτυξη του Διαδικτύου. Το IPv6 περιλαμβάνει μια σειρά λειτουργικών βελτιώσεων και απλοποιήσεων σε σχέση με το προγενέστερο του IPv4 κυρίως σε θέματα ασφάλειας των ψηφιακών επικοινωνιών αλλά και στην κινητικότητα των χρηστών.

Η παρούσα μεταπτυχιακή διατριβή έχει ως στόχο να αναλύσει το πόσο ασφαλής είναι το πρωτόκολλο IPv6 που έχει αναπτυχθεί και βρίσκεται ακόμα σε μικρό στάδιο εφαρμογής. Αφού αρχικά το εξετάσουμε, θα αναφερθούμε στους λόγους που καθιστούν αναγκαία την μετάβαση από το πρωτόκολλο IPv4 στο IPv6 και πως αυτό διασφαλίζεται. Έπειτα, αναπτύσσουμε το πώς το πρωτόκολλο IPv6 μπορεί να πέσει θύμα κακόβουλης ενέργειας και παραθέτουμε τρόπους αντιμετώπισης της. Τέλος συνοψίζουμε τα συμπεράσματά μας για την ασφάλεια του πρωτοκόλλου.

Λέξεις κλειδιά: Internet Protocol version 6 (IPv6), ασφάλεια, μηχανισμοί μετάβασης, επικεφαλίδα διάσπασης

Abstract

Internet Protocol version 6 (IPv6) is the next version of the protocol that is used for communications on the Internet. IPv6 has developed over 10 years and yet its application is in a small level, to the point that is mostly a “research tool”. The design was based on extensive experience which gained over the years of operation and rapid growth of the Internet. The IPv6 includes a series of operational improvements and simplifications that its predecessor IPv4, especially in matters of digital communications and the mobility of users.

This postgraduate thesis aims to analyze how safe is the IPv6 protocol which has been developed and is still in a small phase. After initially looking at, will discuss the reasons which make the transition from IPv4 to IPv6 protocol needed and how it ensured. Then explain how IPv6 protocol may fall victim to malicious acts and give protection measures to deal with. Finally we summarize our conclusions about the safety of the protocol.

Key words: Internet Protocol version 6 (IPv6), security, transition mechanisms, fragment header

Εισαγωγή

Το 1ο Κεφάλαιο τονίζει την αναγκαιότητα μετάβασης στο πρωτόκολλο IPv6. Μας περιγράφει και παραθέτει μια σειρά από λόγους που καθιστούν αυτήν την ενέργεια απαραίτητη καθώς και κάποια παραδείγματα.

Το 2ο Κεφάλαιο μας εισάγει στην δομή του πρωτοκόλλου IPv6 προκειμένου να μας αποσαφηνίσει σημαντικές λειτουργικές και άλλες ιδιότητές του. Στόχο του έχει να μας παρέχει μια σφαιρική αντίληψη και κατανόηση συνολικά του πρωτοκόλλου. Κάνει μια εισαγωγή στο πρωτόκολλο και μας αναλύει τα βασικά χαρακτηριστικά του.

Το 3ο Κεφάλαιο εισέρχεται σε προχωρημένα θέματα ασφαλείας σχετικά με το πρωτόκολλο IPv6 και περιγράφει θέματα όπως οι στόχοι ασφαλείας, τις εφαρμογές ασφαλείας του πρωτοκόλλου IPv6 αλλά και σε πιθανά προβλήματα ασφαλείας που μπορεί να δημιουργηθούν.

Το 4ο Κεφάλαιο παρουσιάζει τις πιο διαδεδομένες και σημαντικότερες τεχνικές που έχουν αναπτυχθεί έτσι ώστε να επιτευχθεί η αναγκαία και ομαλή μετάβαση από το πρωτόκολλο IP έκδοσης 4 σε αυτό της έκδοσης 6. Δίνει ιδιαίτερη έμφαση στον τρόπο που αυτό διασφαλίζεται από κάθε πιθανό κίνδυνο.

Το 5ο Κεφάλαιο πραγματεύεται τις ενδεχόμενες κακόβουλες ενέργειες που μπορεί να δεχθεί το πρωτόκολλο IPv6. Παρουσιάζονται τα είδη των επιθέσεων αλλά και το περιβάλλον που αναπτύχθηκε προκειμένου να προσομοιωθεί και να εξεταστεί κάποια από αυτές. Επίσης αναφέρεται ο τρόπος που οι επιθέσεις αυτές μπορούν να αποφευχθούν και τις δικλίδες ασφαλείας που χρειάζεται να θέσουμε.

Τέλος στο 6ο Κεφάλαιο αναφέρονται όλα τα γενικά συμπεράσματα που προέκυψαν από αυτή την μεταπτυχιακή διατριβή.

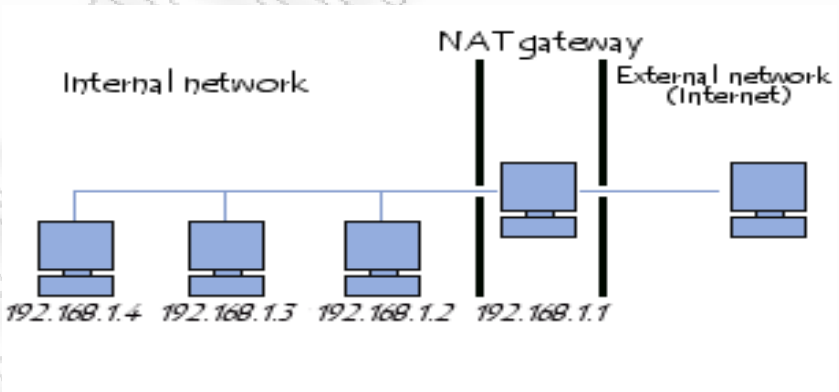
Κεφάλαιο 1

Ανάγκη και λόγοι μετάβασης στο πρωτόκολλο IPv6

1.1 Περιορισμένη διαθεσιμότητα διευθύνσεων

Το IPv6 είναι η νεότερη έκδοση πρωτοκόλλου σε επίπεδο δικτύου και επικοινωνίας του Διαδικτύου, και σχεδιάστηκε για να αντικαταστήσει το προγενέστερο IPv4. Η ανάγκη αυτή αρχικά προέκυψε από το γεγονός ότι ο χώρος διευθύνσεων του πρωτοκόλλου IPv4 λιγόστευε από τις αρχές του 1990 με ταχείς ρυθμούς. Υπήρχε μάλιστα η πρόβλεψη ότι αν συνέχιζε να μικραίνει ο χώρος διευθύνσεων με αυτόν τον ρυθμό μέχρι το 2005 θα είχαν τελειώσει όλες οι διευθύνσεις.

Για να αντιμετωπιστεί το πρόβλημα της έλλειψης διευθύνσεων προτάθηκε η χρήση NAT(Network Address Translation). Η βασική ιδέα του NAT είναι να χρησιμοποιούνται οι ιδιωτικές διευθύνσεις από τους κόμβους μέσα στο ιδιωτικό δίκτυο, και προτού επικοινωνήσουν με άλλους κόμβους στο Διαδίκτυο, μια πύλη NAT (gateway) να αναλαμβάνει να μεταφράζει τις εσωτερικές/ιδιωτικές διευθύνσεις των κόμβων σε μια κανονική IP διεύθυνση. Ωστόσο επειδή μια IP μοιράζεται σε πολλούς κόμβους εντός του δικτύου δημιουργούνται διάφορα προβλήματα, όπως του ότι είναι δύσκολο να κατανεμηθεί σωστά η εισερχόμενη κίνηση στους κόμβους του δικτύου, παρόλο που δεν δημιουργείται πρόβλημα όταν κάποιος κόμβος εντός του δικτύου θέλει να επικοινωνήσει με το Διαδίκτυο. Επίσης η πρόσβαση στο Internet και στις υπηρεσίες του δεν είναι απόλυτα διάφανη καθώς νέες εφαρμογές δεν μπορούν να υποστηριχτούν άμεσα και θα πρέπει να υπάρχει συνέχεια αναβάθμιση του πρωτοκόλλου. Πολλές εφαρμογές έχουν πρόβλημα στην λειτουργία τους λόγω της χρήσης NAT που δεν μπορεί να υποστηρίξει συγκεκριμένες υποθέσεις για τις διευθύνσεις των πακέτων.



Εικόνα 1.1 Χρήση του NAT για εξοικονόμηση χώρου διευθύνσεων
Πηγή: (http://en.kioskea.net/contents/internet/nat.php3)

Τέλος ένα επιπλέον πρόβλημα δημιουργείται στο γεγονός ότι το πρωτόκολλο NAT προϋποθέτει αλλαγή κάποιων πεδίων των πακέτων όταν αυτά περνούν από την πύλη NAT και κάτι τέτοιο μπορεί να χρησιμοποιηθεί σαν απόπειρα για σπάσιμο ασφάλειας στον κόμβο του παραλήπτη, μιας και δεν είναι δυνατό να γνωρίζει αν η συγκεκριμένη αλλαγή έγινε εξαιτίας του NAT ή κάποιου που προσπαθεί να διεισδύσει παράνομα στο δίκτυο.
Με την νέα έκδοση του πρωτοκόλλου πολλά από τα παραπάνω απαλείφονται λόγω του νέου σχεδιασμού του πρωτοκόλλου. Πιο συγκεκριμένα δημιουργεί μια πιο επεκτάσιμη και ευέλικτη ιεραρχία στην δρομολόγηση κάτι που σημαίνει καλύτερη δρομολόγηση των πακέτων αλλά και αύξηση της απόδοσης τους. Επιπλέον αυξάνεται το επίπεδο ασφάλειας μιας και προσδιορίζεται πλήρως το που βρίσκεται ο αποστολέας αλλά και ο παραλήπτης ενός πακέτου με έλεγχο μόνο στα αντίστοιχα πεδία της ιεραρχίας. Τέλος και όσον αφορά τον περιορισμό των διαθέσιμων διευθύνσεων του IPv4 σε σύγκριση με αυτούς του IPv6, το IPv4 λόγω του 32 bit μήκους διευθύνσεων μπορεί να διευθυνσιοδοτήσει το πολύ 2^32 κόμβους. Το IPv6 ξεπερνά αυτό το πρόβλημα εξαιτίας του μήκους των 128 bits διευθύνσεων που έχει υιοθετήσει, το οποίο προσφέρει 2^128 , δηλαδή περίπου 3.4 x 10^38 διευθύνσεις.

Έτσι καθίσταται εύκολα αντιληπτό ότι η νέα έκδοση του πρωτοκόλλου έρχεται να αντιμετωπίσει το σοβαρό πρόβλημα της περιορισμένης διάθεσης διευθύνσεων αλλά και να προσδώσει νέες μεγαλύτερες δυνατότητες που θα αναλύσουμε και στην συνέχεια.

1.2 Αυτορρύθμιση διεύθυνσης και απλοποίηση της διαχείρισης δικτύων

Το IPv4 επιδέχεται και άλλες βελτιώσεις εκτός της αύξησης του χώρου διευθύνσεων. Στην συγκεκριμένη ενότητα θα αναφερθούμε σε αυτή της διαχείρισης (administration). Το πρωτόκολλο Ipv4 κάθε άλλο παρά λειτουργικό θα το θεωρούσε κανείς τόσο από την πλευρά του χρήστη όσο και από αυτήν του διαχειριστή. Και ο λόγος είναι διότι αρχικά στον σχεδιασμό του δεν είχε δοθεί έμφαση στο πως θα είναι εύκολο στην χρήση του αλλά περισσότερο είχε σχεδιαστεί σαν ένα ερευνητικό εργαλείο. Έτσι η σύνδεση ενός κόμβου στο Διαδίκτυο περιελάμβανε μεγάλη πολυπλοκότητα αλλά και κόστος.

Μία αρχική λύση δόθηκε μέσω του πρωτοκόλλου BOOTP, όπου ένα κόμβος έπαιρνε σχετικά απλά τα στοιχεία του μέσω ενός BOOTP εξυπηρετητή. Ωστόσο αυτό αύξανε την δυσκολία από την πλευρά του διαχειριστή μιας και θα έπρεπε να διατηρεί μια λίστα που θα αντιστοιχίζει τις ρυθμίσεις σε επίπεδο IP με διευθύνσεις του επιπέδου σύνδεσης (Ethernet διευθύνσεις για παράδειγμα). Επιπλέον μεγάλωνε σημαντικά και το κόστος αφού αυτή η αντιστοιχία του κάθε κόμβου με μια IP διεύθυνση, θα χρειάζονταν τόσες IP όσοι και οι κόμβοι ανεξάρτητα αν ήταν ή όχι συνδεδεμένοι στο Internet, οπότε περισσότερες διευθύνσεις.

Ακόμα στο Ipv4 χρησιμοποιούνταν το πρωτόκολλο DHCP προκειμένου να λάβει ένα μηχάνημα αυτόματα IP διεύθυνση. Έδινε επίσης την δυνατότητα στον διαχειριστή να ορίζει χειρονακτικά διευθύνσεις για συγκεκριμένους κόμβους. Αυτό όμως με την σειρά του παρουσιάζει ορισμένα άλλα μειονεκτήματα. Στο ότι χρειάζεται υποχρεωτικά να υπάρχει ένας DHCP server, ότι δεν υπάρχει εγγύηση ότι το ίδιο το μηχάνημα θα λάβει την διεύθυνση και τέλος ότι ο διαχειριστής θα πρέπει να ορίσει επακριβώς στον DHCP εξυπηρετητή όλα τα στοιχεία των κόμβων πράγμα αρκετά πολύπλοκο και εξαιρετικά χρονοβόρο. Όλα αυτά συνθέτουν μια εικόνα αδυναμίας του IPV4 τόσο στην υποστήριξη των χρηστών χωρίς σταθερή θέση εργασίας όσο και στη διαχείριση του δικτύου.

Το Ipv6 δίνει μια ανανεωμένη έκδοση του DCHP το DHCPv6 και επιπλέον υπάρχει και άλλη επιλογή για την αυτόματη ρύθμιση της διεύθυνσης, που ονομάζεται stateless autoconfinguration. Σε αυτό το σημείο αξίζει να επισημάνουμε ότι το Ipv6 υποστηρίζει και statefull μηχανισμούς, δηλαδή με διατήρηση κατάστασης εκτός από stateless δηλαδή χωρίς διατήρηση κατάστασης. Με την επιλογή αυτή κάθε συσκευή που βρίσκεται συνδεδεμένη στο διαδίκτυο περιμένει να μάθει ποια 64 bit να χρησιμοποιήσει για το πρώτο μέρος της Ipv6 διεύθυνσης. Οι συσκευές που είναι συνδεδεμένες στο ίδιο δίκτυο έχουν και το ίδιο 64 –bit πρόθεμα. Τα υπόλοιπα bit συμπληρώνονται από την MAC διεύθυνση των συσκευών αυτών. Επειδή οι διευθύνσεις MAC αποτελούνται από 48 bit, τα 16 εναπομένοντα bit συμπληρώνονται συνήθως με άσσο. Έτσι ο ίδιος υπολογιστής παίρνει την ίδια IP κάθε φορά που συνδέεται στο ίδιο δίκτυο χωρίς να χρειάζεται η ύπαρξη ενός DHCP server. Με το Ipv6 προσφέρονται μηχανισμοί με τους οποίους ένας σταθμός μπορεί να δημιουργήσει την Ipv6 διεύθυνσή του από μόνος του.

Επίσης το Ipv6 παρέχει μεγάλο πλεονέκτημα όσον αφορά στην αριθμοδότηση του δικτύου. Δηλαδή ο διαχειριστής έχει την δυνατότητα με μία απλή αλλαγή του προθέματος του δικτύου στον κεντρικό δρομολογητή να ενημερωθούν αυτόματα και οι υπόλοιποι κόμβοι του δικτύου και να αλλάξουν τις διευθύνσεις τους. Εύκολα καταλαβαίνουμε την μεγάλη απλούστευση που προσφέρει το Ipv6 στην μεριά του διαχειριστή σε συνδυασμό με την καλύτερη διαχείριση της κυκλοφορίας των πακέτων μιας και χρησιμοποιεί την τεχνική multicast.

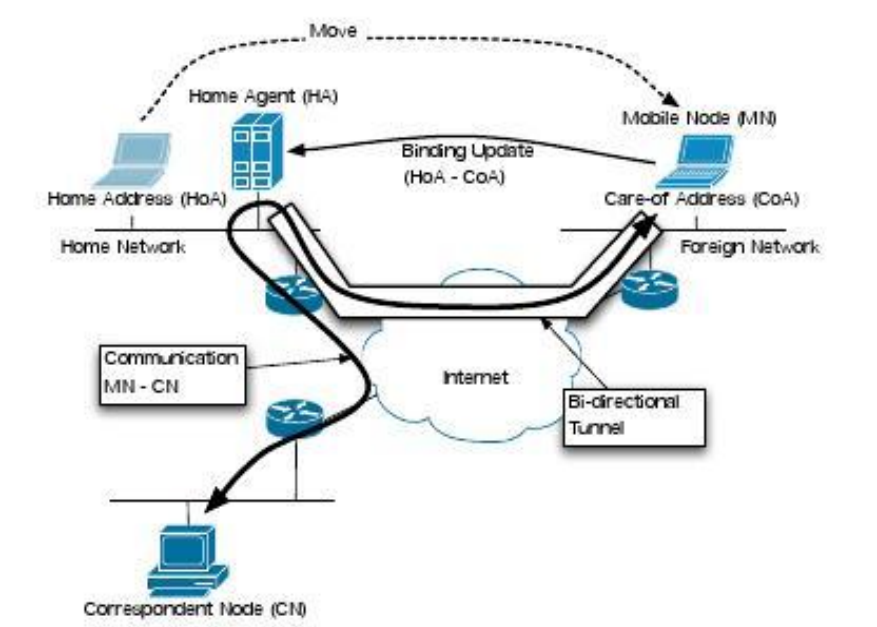
1.3 Υποστήριξη φορητότητας και αύξηση της αποδοτικότητας

Με τον όρο φορητότητα εννοούμε την δυνατότητα μιας συσκευής να συνδεθεί στο δίκτυο από διαφορετικά μέρη, σε διαφορετικές χρονικές στιγμές, ενώ διατηρεί συνόδους (sessions) της κανονικής του διεύθυνσης. Μέχρι και πριν από λίγα χρόνια οι περισσότερες δικτυωμένες συσκευές ήταν δύσκολο να μετακινηθούν λόγω μεγέθους. Τα τελευταία χρόνια όμως με την εισαγωγή των μικρών φορητών υπολογιστών, των κινητών τηλεφώνων αλλά και άλλων συσκευών που υποστηρίζουν το πρωτόκολλο IP, δημιουργήθηκε η ανάγκη ενός πρωτοκόλλου που να μπορεί να αντεπεξέλθει σε αυτές τις απαιτήσεις. Το κύριο πρόβλημα είναι ότι επειδή αυτές οι συσκευές είναι φορητές αλλάζουν διαρκώς δίκτυα και επομένως θα πρέπει να αλλάζουν και οι ρυθμίσεις IP καθώς επίσης θα πρέπει να ενημερώνονται και οι κόμβοι με τους οποίους έχουν επικοινωνία για τις αλλαγές αυτές των ρυθμίσεων. Έτσι και δημιουργήθηκε και η ανάγκη για το λεγόμενο Mobile IP.

Είναι γεγονός ότι υποστήριξη για φορητότητα υπάρχει στο IPv4, ωστόσο εξακολουθούν να υφίστανται πολλά προβλήματα. Μερικά από αυτά είναι η έλλειψη διευθύνσεων προκειμένου να αντιστοιχηθούν στην κατηγορία των κινητών χρηστών, παρουσιάζονται αδυναμίες ασφάλειας αλλά και αυξάνουν σημαντικά το φόρτο του δικτύου. Επίσης αξίζει να τονιστεί οι δυσκολίες που παρουσιάζονται στην πλευρά των διαχειριστών.

Στο Ipv6 η υποστήριξη των κινητών χρηστών είναι ενσωματωμένη, κάτι που απλοποιεί σε πολύ σημαντικό βαθμό την διαχείριση της υπηρεσίας. Σε αντίθεση με το Ipv4 όπου ο κινητός κόμβος επικοινωνεί με τους υπολοίπους μέσω της home πράκτορα (home agent), στο Ipv6 υπάρχει η βελτιστοποιημένη δρομολόγηση με την χρήση της binding update, δηλαδή της τεχνικής ενημέρωσης. Σύμφωνα με αυτήν ο δρομολογητής ειδοποιείται από τον κινητό κόμβο για την προσωρινή διεύθυνση του, δηλαδή την care-of διεύθυνσή του, με την χρήση της binding, αλλά μπορεί να ειδοποιεί και οποιονδήποτε άλλο κόμβο του στέλνει πακέτα, έτσι ώστε να του στέλνει

τα πακέτα στην προσωρινή και όχι στην home διεύθυνση. Κάτι τέτοιο είναι εξαιρετικά πολύπλοκο στο Ipv4.



Εικόνα 1.2 Χρήση του Mobile Ipv6
Πηγή: (http://my.opera.com/blu3c4t/blog/2008/12/20/mobile-ipv6-in-briefly)

Υπάρχουν ακόμα πολλές βελτιώσεις στην υποστήριξη της φορητότητας σε σχέση με το παλαιότερο πρωτόκολλο. Αυτά αφορούν την μείωση του κόστους διαχείρισης μιας και στο Ipv6 γίνεται χρήση statefull και stateless μηχανισμών για την απόκτηση των care-of διευθύνσεων. Επιπλέον ο κινητός κόμβος δεν χρειάζεται να γνωρίζει την διεύθυνση του home agent, κάτι που είναι πολύ περιοριστικό στο Ipv4. Στο IPV6 υπάρχουν ενσωματωμένοι μηχανισμοί ασφαλείας που πιστοποιούν ότι ο κόμβος που επικοινωνεί με τον home agent είναι ο κινητός κόμβος αλλά και ότι σαν διεύθυνση αποστολέα στα μηνύματα του κινητού κόμβου είναι η care-of διεύθυνσή του και όχι η home προκειμένου να εξαλειφθούν προβλήματα δρομολόγησης. Τέλος υπάρχουν μηχανισμοί όπου σε περίπτωση που ο κινητός κόμβος αλλάξει δίκτυο, ενημερώνουν τόσο τον κινητό κόμβο όσο και τον δρομολογητή του ξένου υποδικτύου (foreign subnet).

Συνοψίζοντας θα λέγαμε ότι το πρωτόκολλο Mobile Ipv6 επιτρέπει την απρόσκοπτη επικοινωνία των χρηστών, καθώς μετακινούνται ανάμεσα σε ζώνες ενός δικτύου ή ανάμεσα σε διαφορετικά δίκτυα, αξιοποιεί τις δυνατότητες διευθυνσιοδότησης και ασφάλειας του Ipv6 και βελτιστοποιεί την δρομολόγηση των πακέτων.

Αλλά και από την μεριά της αποδοτικότητας παρατηρούμε μεγάλες βελτιώσεις. Αυτό ήρθε σαν αποτέλεσμα από μια σειρά από νέα χαρακτηριστικά που προσφέρει το Ipv6 και βοηθούν στην αύξηση της αποδοτικότητας. Υιοθετήθηκαν τα ωφέλιμα χαρακτηριστικά του πρωτοκόλλου Ipv4, άλλα τροποποιήθηκαν και βελτιώθηκαν, αυτά που ήταν επιζήμια απομονώθηκαν, προστέθηκαν νεότερα και σχεδιάστηκαν καλύτερα. Ένα χαρακτηριστικό παράδειγμα είναι του πεδίου διευθύνσεων που παρόλο στο πρωτόκολλο Ipv6 είναι τέσσερις φορές μεγαλύτερο από αυτό του

Ipv4, η συνολική επικεφαλίδα είναι μόνο 40 bytes σε σύγκριση με τα 20 bytes μιας τυπικής επικεφαλίδας στο Ipv4. Πιο συγκεκριμένα παρακάτω αναφέρουμε μια σειρά βελτιώσεων που παρατηρούνται στην απόδοση:

- Στο πρωτόκολλο Ipv6 η επικεφαλίδα έχει σταθερό μήκος κάτι που προσφέρει μεγάλη ευκολία διαχείρισης και μείωση της πολυπλοκότητας
- Στο Ipv6 υπάρχει υποστήριξη του μηχανισμού multicast σε σχέση με την ευρεία αναμετάδοση που υπήρχε στο Ipv4 με αποτέλεσμα να διακόπτονται μόνο οι δικτυακές συσκευές που πρέπει να επεξεργαστούν ένα μήνυμα και όχι όλες όσες βρίσκονται συνδεδεμένες εκείνη την στιγμή.
- Όσον αφορά στην δρομολόγηση δεν υπάρχει η ανάγκη να διασπάται ένα πακέτο μεγάλου μεγέθους σε μικρότερα κομμάτια και επιπλέον υπάρχει η δυνατότητα να ενημερώνουν ώστε να δέχονται πακέτα μικρότερου μεγέθους. Γενικότερα οι δρομολογητές έχουν καλύτερη απόδοση για Ipv6 επικεφαλίδες.
- Το Ipv6 διαθέτει υποστήριξη προαιρετικών πεδίων σε ξεχωριστές επικεφαλίδες. Έτσι διευκολύνεται και αυξάνεται η απόδοση της απλής δρομολόγησης μιας και δεν είναι αναγκαίο κάθε δρομολογητής να επεξεργαστεί αυτά τα πεδία.

1.4 Αναβάθμιση της Ποιότητας Υπηρεσιών

Ένας τομέας στον οποίο δόθηκε ιδιαίτερη έμφαση κατά την σχεδίαση της νεότερης έκδοσης του πρωτοκόλλου IP είναι αυτού της ποιότητας των υπηρεσιών, γνωστή και ως Quality of Service (QoS). Το IPv6 υποστηρίζει την κατηγοριοποίηση πακέτων με προτεραιότητες δρομολόγησης ώστε να επιτυγχάνεται η επιθυμητή ποιότητα υπηρεσίας. Το Ipv4 έχει και αυτό την δυνατότητα υλοποίησης μηχανισμών QoS στο επίπεδο δικτύου με την χρήση του πεδίου TOS (Type of Service) μεγέθους ενός byte στην επικεφαλίδα του, όπου μπορεί να περιγράφει το είδος της υπηρεσίας που απαιτεί μια εφαρμογή. Ωστόσο εκτός του ότι παρέμεινε σε μεγάλο βαθμό ανεκμετάλλευτο, προαπαιτούσε από τα πρωτόκολλα δρομολόγησης να γνωρίζουν λεπτομέρειες και χαρακτηριστικά του πλήθος των μονοπατιών που το πακέτο έπρεπε να επιλέξει για να φτάσει στον προορισμό του, πράγμα που δημιουργούσε μείωση απόδοσης και αύξηση της πολυπλοκότητας στην μεριά των διαχειριστών και των κατασκευαστών των εφαρμογών.

Το Ipv6 βελτιώνει και επεκτείνει την ιδέα αυτή, παρέχοντας δύο νέα πεδία στην κύρια επικεφαλίδα. Αυτά είναι τα Traffic Class και Flow label (Ετικέτα Ροής) που παίζουν σημαντικό ρόλο στην υποστήριξη μηχανισμών και υπηρεσιών με συγκεκριμένες απαιτήσεις ποιότητας. Στο Ipv4 ένας δρομολογητής προκειμένου να ενημερωθεί για μια ροή χρειαζόταν να αναγνωρίσει και να αναλύσει τις διευθύνσεις IP των εμπλεκομένων στην επικοινωνία κόμβων, δηλαδή τόσο του αποστολέα όσο και του παραλήπτη καθώς και την θύρα που βρίσκεται στη επικεφαλίδα του πρωτοκόλλου μεταφοράς. Εύκολα αντιλαμβάνεται κανείς το υψηλό κόστος που χρειάζονται οι δρομολογητές για την επεξεργασία όλων αυτών των δεδομένων και συνεπώς θέτεται σε κίνδυνο η ίδια η ποιότητα υπηρεσίας. Η απόδοση ενός δρομολογητή είναι από τα πιο σημαντικά χαρακτηριστικά του και για τον λόγο αυτό οι κατασκευαστές δίνουν μεγάλη βαρύτητα στον τομέα αυτό.

Στο Ipv6 όλα αυτά αυτοματοποιούνται και επιτυγχάνονται σε υψηλές ταχύτητες καθώς όλες οι απαραίτητες πληροφορίες βρίσκονται μέσα στο πεδίο Ετικέτας Ροής χωρίς να χρειάζεται οι δρομολογητές να επεξεργαστούν κανένα από τα υπόλοιπα πεδία. Γενικότερα η χρήση των πεδίων αυτών στο Ipv6 βρίσκεται σε ερευνητικό στάδιο. Αποκτώντας όμως με τον καιρό το Ipv6 πρωταγωνιστικό ρόλο, παρουσιάζει ιδιαίτερο ενδιαφέρον η διερεύνηση του τρόπου με τον οποίο θα αξιοποιηθούν πρακτικά οι Quality of Service δυνατότητες που μπορεί να προσφέρει.

1.5 Ασφάλεια

Το Πρωτόκολλο Διαδικτύου (IP) είναι το πιο ευρέως διαδεδομένο πρωτόκολλο επικοινωνίας. Για το λόγω του ότι είναι η πιο διαδεδομένη τεχνολογία επικοινωνίας, συγκεντρώνει την προσοχή χιλιάδων επαγγελματιών στον τομέα του IT (Information Technology). Επειδή η χρήση του γίνεται από εκατομμύρια ανθρώπους στον κόσμο, ο τομέας της ασφάλειας του κρίνεται ίσως ο πιο σηματνικός.

Όταν είχε σχεδιαστεί αρχικά το IPv4 λόγω της φύσης του δικτύου, όπου ο στόχος του ήταν η επικοινωνία των ακαδημαϊκών ιδρυμάτων, δεν είχε λάβει υπόψη του θέματα ασφαλείας. Ωστόσο λόγω της εξάπλωσης του Διαδικτύου σε πολλούς τομείς των επιχειρήσεων αλλά και του ηλεκτρονικού εμπορίου, η ανάγκη για ασφάλεια έγινε επιτακτική. Ο αρχικός στόχος ήταν να σχεδιαστεί ένα πρωτόκολλο που να συνδέει ετερογενή δίκτυα έτσι ώστε οι υπολογιστές να προσδιορίζονται μοναδικά, να έχουν την δυνατότητα να επικοινωνούν και ν ανταλλάσουν δεδομένα σε μια κοινή μορφή και τα δεδομένα αυτά να μεταδίδονται χωρίς να δημιουργείται η ανάγκη οι υπολογιστές να πρέπει να γνωρίζουν τα στοιχεία και την δομή των δικτύων που βρίσκονται οι παραλήπτες. Από όλα αυτά καταλαβαίνουμε πόσα κενά ασφαλείας παρουσιάζει το πρωτόκολλο Ipv4.

Με την εξάπλωση του Διαδικτύου και την ανάγκη για ασφάλεια που δημιουργήθηκε, έγιναν προσπάθειες προκειμένου να προσαρμόσουν εργαλεία και να τροποποιήσουν το υπάρχον πρωτόκολλο. Η μεγαλύτερη προσπάθεια ήταν αυτή του Ipsec του οργανισμού IETF που είχε ασχοληθεί με αρκετούς μηχανισμούς και πρωτόκολλα για να εξασφαλίσει την ασφάλεια στην διαδικτυακή κυκλοφορία στο Ipv4 και αργότερα στο Ipv6. Το Ipsec παρέχει κρυπτογράφηση και πιστοποίηση στο επίπεδο IP προστατεύοντας έτσι τα δεδομένα μιας εφαρμογής από το να τροποποιηθούν και να αλλοιωθούν κατά τη μεταφορά τους. Ωστόσο υπάρχει μία βασική διαφορά στη χρησιμοποίηση του Ipsec από τα δύο πρωτόκολλα. Εξαιτίας του αρχικού σχεδιασμού του Ipv4 η υποστήριξη ασφάλειας είναι προαιρετική και έτσι ακόλουθα η υποστήριξη του πρωτοκόλλου Ipsec είναι επιπρόσθετη, γίνεται δηλαδή χρήση του πεδίου IP Options (ένα πεδίο μεταβλητού μήκους) που αυξάνει κατά πολύ την πολυπλοκότητα επεξεργασίας των πακέτων. Επιπλέον το NAT (Network Address Translation) που χρησιμοποιείται στο Ipv4 διακόπτει την end-to-end επικοινωνία του IP Security (Ipsec) που χρειάζεται για να είναι πλήρως αποδοτικό. Επειδή υπάρχει η μετάφραση στην μέση, των εσωτερικών διευθύνσεων σε κανονικές IP διευθύνσεις, και τα IP στις δύο άκρες δεν συμφωνούν αυτό προκαλεί σύγχυση στην εύρυθμη λειτουργία του Ipsec. Αυτό μοιάζει άλλωστε πολύ με την man-in-the-middle επίθεση όπου ο επιτιθέμενος παρεμποδίζει μια νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους και στην συνέχεια ο κακόβουλος host ελέγχει την ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλοιώσει τις πληροφορίες που στέλνονται από τους αρχικούς συμμετέχοντες.

Αντίθετα στο Ipv6 η υποστήριξη του IP Security είναι ενσωματωμένη και συνεπώς η υλοποίηση του αλλά και η λειτουργία του σαφώς απλούστερη. Επιπροσθέτως οι μηχανισμοί ασφαλείας που χρησιμοποιούνται από το Ipv6 μπορούν να χρησιμοποιηθούν εξίσου και από οποιουσδήποτε άλλους μηχανισμούς. Σε αντίθεση με το πρωτόκολλο Ipv4 όπου σε κάθε νέα επέκταση, ανανέωση ή τροποποίηση του θα πρέπει ο μηχανισμός να εξασφαλίζει μηχανισμούς ασφαλείας. Ακόμα λόγω του σχεδιασμού του πρωτοκόλλου Ipv4 όταν χρησιμοποιείται ασφάλεια στο επίπεδο μεταφοράς, δημιουργείται η ανάγκη να πρέπει οι εφαρμογές που χρησιμοποιούν αυτή την μέθοδο να ξαναγραφτούν, προκειμένου να μπορούν τόσο ο πελάτης όσο και ο εξυπηρετητής να χρησιμοποιήσουν την ασφάλεια αυτού του επιπέδου (γίνεται χρήση του

πρωτοκόλλου Secure Socket Layer ή αλλιώς SSL). Στο πρωτόκολλο Ipv6 δεν παρουσιάζονται αντίστοιχα προβλήματα.

Τέλος το Ipv6 έχει ένα ακόμη συγκριτικό πλεονέκτημα στο θέμα της ασφάλειας σε σχέση με το πρωτόκολλο Ipv4, και αυτό αφορά στους ιούς τύπου worm. Δηλαδή κακόβουλα προγράμματα που μπορεί να προξενήσουν βλάβες στους υπολογιστές και στα δεδομένα που περιέχουν, να επιβραδύνουν την ταχύτητα σύνδεσης στο Διαδίκτυο αλλά και να τους χρησιμοποιήσουν για ιδιοτελής σκοπούς. Ο νέος μεγάλος χώρος των διευθύνσεων που δημιουργείται με την εισαγωγή του νεότερου πρωτοκόλλου αποτελεί αποτρεπτικό παράγοντα. Στο Ipv4 οι συσκευές υποδικτύου μπορούσαν να έχουν το πολύ 16 bit διεύθυνση, πράγμα που έκανε εύκολο το έργο ενός ιού τύπου worm, μιας και μπορούσε να κάνει μέσα σε επιθυμητό χρόνο port scanning σε όλες. Αντίθετα στο Ipv6 η διεύθυνση υποδικτύου αυξάνεται στα 64 bit, πράγμα που κάνει σχεδόν αδύνατη μια πιθανή επίθεσή του, μιας και αναλογικά είναι σαν να πρέπει να κάνει scanning σε ένα δίκτυο, δύο φορές όσο σε όλο το Ipv4 διαδίκτυο.

1.6 Συμπεράσματα

Στο κεφάλαιο αυτό αναφέραμε συνοπτικά του κύριους λόγους που καθίσταται αναγκαία η μετάβαση από το πρωτόκολλο IPv4 σε αυτό του Ipv6. Είδαμε ότι το Ipv6 παρουσιάζει πολλά συγκριτικά πλεονεκτήματα σε σχέση με το προγενέστερό του. Παρακάτω παραθέτουμε συγκεντρωτικά τους λόγους που τονίσαμε και στο παρόν κεφάλαιο:

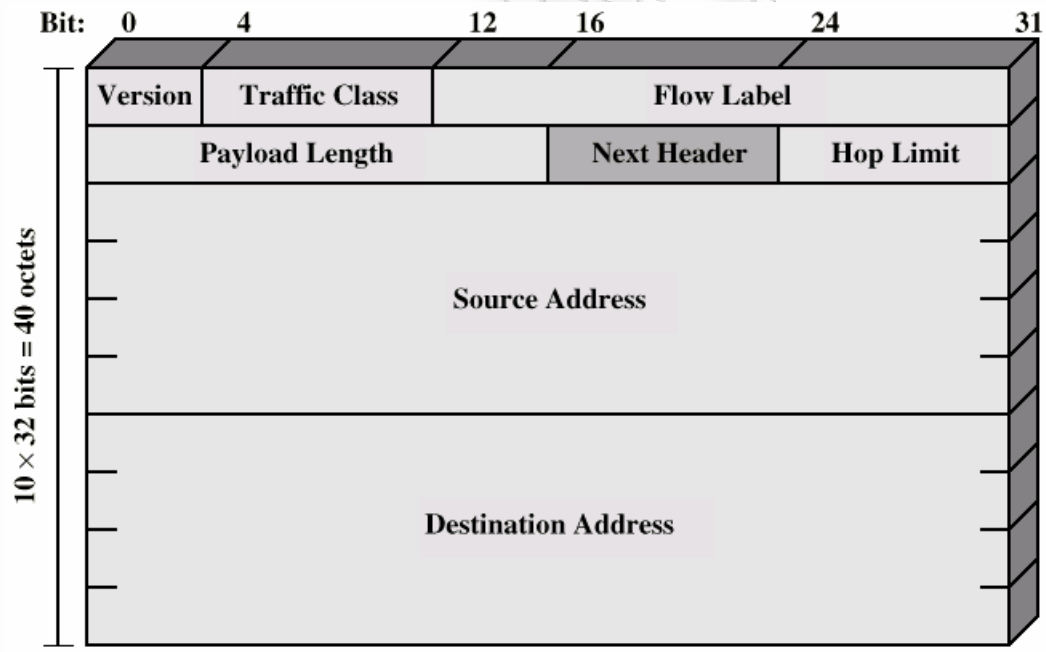
- Μεγαλύτερος χώρος διευθύνσεων: αύξηση του μεγέθους διεύθυνσης από 32 bits σε 128 bits
- Stateless autoconfiguration: η ικανότητα των κόμβων να προσδιορίζουν την διεύθυνσή τους
- Multicast: αυξάνει την απόδοση της χρήσης της επικοινωνίας ένας προς πολλούς
- Βελτίωση της Ποιότητας των Υπηρεσιών (QoS): το QoS marking των πακέτων και το πεδίο Ετικέτας Ροής (flow label) βοηθούν στην αποτελεσματική δρομολόγηση με την αναγνώριση της κίνησης με την μεγαλύτερη προτεραιότητα
- Φορητότητα: ευκολότερη διαχείριση των κινητών και απομακρυσμένων κόμβων
- Ασφάλεια: μέσω των επικεφαλίδων επέκτασης, ασφάλεια και απόκρυψη δεδομένων

Κεφάλαιο 2

Εισαγωγή στο πρωτόκολλο Ipv6

2.1 Η δομή του IPv6

Το κεφάλαιο αυτό μας εισάγει και μας αναλύει την δομή του πρωτοκόλλου Ipv6 και ιδιαίτερα της επικεφαλίδας του. Εξετάζει ειδικότερα τις επικεφαλίδες επέκτασης οι οποίες είναι νέες στο Ipv6. Η δομή της επικεφαλίδας ενός Ipv6 πακέτου περιγράφεται στο RFC 2460. Η επικεφαλίδα έχει σταθερό μήκος 40 bytes. Τα πεδία διεύθυνσης Προορισμού (Destination Address) και διεύθυνσης Αφετηρίας (Source Address) καταλαμβάνουν το καθένα 16 bytes (128 bits), και έτσι απομένουν μόνο 8 bytes για τις υπόλοιπες γενικές πληροφορίες της επικεφαλίδας. Αρχικά παραθέτουμε την βασική επικεφαλίδα του πρωτοκόλλου Ipv6:



Εικόνα 2.1 Η βασική επικεφαλίδα του Ipv6
Πηγή: (www.icsd.aegean.gr/lecturers/pavlos/lectrure notes/dcc/Internets & Intranets (ch.15-part2).pdf)

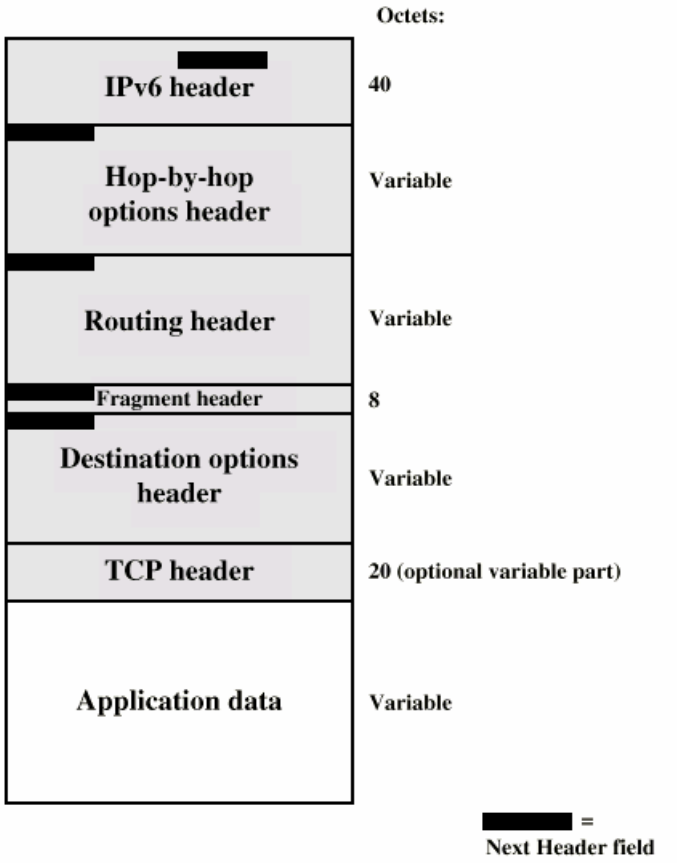
Παρακάτω θα επεξηγήσουμε τα πεδία του βασικού header του Ipv6:

- ***Version (Έκδοση)***: καταλαμβάνει 4 bits και δείχνει την έκδοση του IP που εδώ πρέπει να είναι ίσο με 6

- ***Traffic Class (Τάξη Κυκλοφορίας)***: καταλαμβάνει 8 bits και προσδιορίζει ότι μια συγκεκριμένη υπηρεσία παρέχεται σε αυτό το πακέτο. Έχει προκαθορισμένη τιμή ίση με 0.
- ***Flow Label (Ετικέτα Ροής)***: καταλαμβάνει 20 bits και χρησιμοποιείται για να γνωστοποιήσει ποια πακέτα ανήκουν σε μια συγκεκριμένη ροή.
- ***Playload length (Μήκος Πακέτου)***: καταλαμβάνει 16 bits και δείχνει το μήκος του πεδίου δεδομένων. Αφορά το μέρος του πακέτου που ξεκινά αμέσως μετά την βασική επικεφαλίδα.
- ***Next Header (Επόμενη Επικεφαλίδα)***: καταλαμβάνει 8 bits και υποδεικνύει τον τύπο header που ακολουθεί. Στο Ipv4 αυτό το πεδίο αντιστοιχούσε στο πεδίο του Τύπου Πρωτοκόλλου. Μετονομάστηκε στο Ipv6, ώστε να αντικατοπτρίζει την νέα οργάνωση των IP πακέτων. Εάν η Επόμενη Επικεφαλίδα είναι επιπέδου μεταφοράς UDP ή TCP, τότε αυτό το πεδίο περιέχει τους ίδιους αριθμούς πρωτοκόλλου όπως και στο Ipv4. Για παράδειγμα, αριθμός πρωτοκόλλου 6 για το TCP και 17 για το UDP. Αλλά αν οι επικεφαλίδες Επέκτασης χρησιμοποιούνται στο Ipv6, τότε το πεδίο περιέχει τον τύπο της επόμενης κεφαλίδας Επέκτασης. Αυτή βρίσκεται μεταξύ της κεφαλίδας IP και της TCP ή UDP κεφαλίδας.
- ***Hop Limit* (Όριο Βημάτων)**: καταλαμβάνει 8 bits αντικαθιστά το πεδίο TTL του Ipv4, έχει μία αρχική τιμή και μειώνεται ένα κάθε φορά που το πακέτο προωθείται στον επόμενο κόμβο. Το TTL περιέχει έναν αριθμό δευτερολέπτων, δηλώνοντας τον χρόνο που ένα πακέτο παρέμενε στο δίκτυο προτού καταστραφεί. Οι περισσότεροι δρομολογητές μείωναν αυτήν την αξία κατά ένα σε κάθε βήμα. Αυτό το πεδίο μετονομάστηκε σε Όριο Βημάτων στο Ipv6. Η τιμή σε αυτό το πεδίο τώρα εκφράζεται σε αριθμούς βημάτων και όχι σε δευτερόλεπτα. Αν το όριο βημάτων φτάσει στο μηδέν το πακέτο απορρίπτεται. Ο χρόνος ζωής του πακέτου τώρα καθορίζεται σε ανώτερα επίπεδα.
- ***Source address (Διεύθυνση Αποστολέα)****:* καταλαμβάνει 128 bits και μας ενημερώνει για την διεύθυνση του αποστολέα.
- ***Destination address (Διεύθυνση Προορισμού)****:* καταλαμβάνει 128 bits και μας ενημερώνει για την διεύθυνση του παραλήπτη. Στο Ipv4, αυτό το πεδίο περιείχε πάντα την διεύθυνση του τελικού προορισμού του πακέτου. Στο Ipv6, το πεδίο αυτό μπορεί να μην περιέχει τη IP διεύθυνση του τελικού προορισμού εάν η επικεφαλίδα Δρομολόγησης (καθορίζει την συγκεκριμένη διαδρομή που πρέπει να ακολουθήσει το πακέτο) είναι παρούσα. Μπορεί απλά να είναι ένας από τους κόμβους της διαδρομής. Η διεύθυνση προορισμού μπορεί να είναι μια unicast, multicast ή anycast διεύθυνση.

Η επικεφαλίδα Ipv4 μπορεί να επεκταθεί από τα ελάχιστα 20 bytes έως τα 60 bytes προκειμένου να καθορίσει τις επιλογές του όπως τις Επιλογές Ασφάλειας (Security Options), την αφετηρία δρομολόγησης (Source Routing) ή του Χρόνου Συμπίεσης (Timestamping). Η ικανότητα αυτή έχει σπάνια χρησιμοποιηθεί επειδή προκαλεί μείωση στην απόδοση. Για παράδειγμα, οι εφαρμογές διαβίβασης hardware στο Ipv4 πρέπει να περάσουν το πακέτο που περιέχει τις επιλογές στον κύριο επεξεργαστή (software handling – διαχείριση λογισμικού). Όσο απλούστερη είναι η επικεφαλίδα του πακέτου, τόσο πιο γρήγορη είναι και η επεξεργασία. Χειρίζεται επιλογές σε επιπρόσθετες επικεφαλίδες που ονομάζονται επικεφαλίδες Επέκτασης.
Στο Ipv6 οι προαιρετικές πληροφορίες του επιπέδου δικτύου βρίσκονται σε ξεχωριστές επικεφαλίδες, που τοποθετούνται μεταξύ της βασικής επικεφαλίδας Ipv6 και της επικεφαλίδας του επιπέδου μεταφοράς. Κάθε επικεφαλίδα επέκτασης προσδιορίζεται από μια συγκεκριμένη τιμή του πεδίου Next Header.

Ακόλουθα παραθέτουμε σχηματικά τις επικεφαλίδες επέκτασης στο Ipv6:



Εικόνα 2.2 Οι επικεφαλίδες επέκτασης του Ipv6
Πηγή: (www.icsd.aegean.gr/lecturers/pavlos/lectrure notes/dcc/Internets & Intranets (ch.15-part2).pdf)

Μπορεί να υπάρχει μία, καμία ή περισσότερες από μία επικεφαλίδες Επέκτασης μεταξύ της επικεφαλίδας Ipv6 και του ανωτέρου επιπέδου επικεφαλίδας πρωτοκόλλου. Κάθε κεφαλίδα Επέκτασης αναγνωρίζεται από το πεδίο του Next Header (επόμενης επικεφαλίδας) της προηγούμενης επικεφαλίδας. Οι επικεφαλίδες Επέκτασης, εξετάζονται ή επεξεργάζονται μόνο από τον κόμβο που αναγνωρίζεται στο πεδίο διεύθυνσης Προορισμού της επικεφαλίδας Ipv6. Εάν η διεύθυνση στο πεδίο διεύθυνσης Προορισμού είναι multicast διεύθυνση, οι επικεφαλίδες Επέκτασης εξετάζονται και υπολογίζονται από όλους τους κόμβους που ανήκουν σε αυτήν την multicast ομάδα. Οι επικεφαλίδες Επέκτασης πρέπει να είναι αυστηρά επεξεργασμένες προκειμένου να εμφανίζονται στην επικεφαλίδα του πακέτου.

Υπάρχει μια εξαίρεση στον παραπάνω κανόνα: μόνο ο κόμβος προορισμού θα επεξεργάζεται μία επικεφαλίδα Επέκτασης. Εάν η επικεφαλίδα επέκτασης είναι επικεφαλίδα Βήμα-προς-Βήμα Επιλογές (Hop-by-Hop Options header), η πληροφορία που φέρει πρέπει να εξεταστεί και να υπολογιστεί από κάθε κόμβο της διαδρομής του πακέτου, συμπεριλαμβανομένων των κόμβων

αφετηρίας και προορισμού. Η Hop-by-Hop επικεφαλίδα εάν υπάρχει, πρέπει να ακολουθήσει αμέσως μετά την Ipv6 επικεφαλίδα. Η παρουσία της δηλώνεται στο πεδίο Next Header της βασικής επικεφαλίδας του Ipv6. Ακόλουθα αναφέρουμε μερικές σύντομες πληροφορίες για κάθε μία από τις επικεφαλίδες επέκτασης:

- ***Hop-by-Hop Options Header (Επικεφαλίδα Βήμα-προς-Βήμα)***: αυτή η επικεφαλίδα επέκτασης μεταφέρει προαιρετικές πληροφορίες που πρέπει να εξεταστούν από κάθε κόμβο κατά μήκος της διαδρομής του πακέτου. Πρέπει να ακολουθεί αμέσως μετά την βασική επικεφαλίδα και αναγνωρίζεται από την παρουσία της στο πεδίο Next Header με την τιμή 0. Για παράδειγμα ο δρομολογητής Alert (RFC 2711) χρησιμοποιεί την επικεφαλίδα επέκτασης Βήμα-προς-Βήμα για πρωτόκολλα όπως το RSVP (Resource Reservation Protocol) ή MLD (Multicast Listener Discovery). Στο Ipv4, ο μόνος τρόπος για έναν δρομολογητή για να διαπιστωθεί αν χρειάζεται να εξετάσει ένα datagram, εν μέρει τουλάχιστον, ήταν να περάσει τα δεδομένα των ανωτέρων στρωμάτων σε όλα τα datagrams. Με το Ipv6, ελλείψει της κεφαλίδας επέκτασης Hop-by-Hop, ο δρομολογητής γνωρίζει ότι δεν πρέπει να επεξεργαστούν συγκεκριμένες πληροφορίες δρομολογητή και μπορεί να δρομολογήσει αμέσως το πακέτο στον τελικό προορισμό. Εάν υπάρχει η επικεφαλίδα επέκτασης Hop-by-Hop, ο δρομολογητής χρειάζεται να εξετάζει μόνο την επικεφαλίδα χωρίς να κοιτά περαιτέρω το πακέτο.
- ***Routing Header (Επικεφαλίδα Δρομολόγησης)***: χρησιμοποιείται όταν η πηγή θέλει το πακέτο να περάσει από ένα ή περισσότερους ενδιάμεσους κόμβους στην πορεία του προς τον τελικό προορισμό. Δίνει μια λίστα από έναν ή περισσότερους ενδιάμεσους κόμβους που πρέπει να επισκεφθεί στην πορεία του προς τον τελικό παραλήπτη. Στο Ipv4 αυτό καλείται Loose Source και Record Route επιλογή. Η Επικεφαλίδα Δρομολόγησης αναγνωρίζεται στο πεδίο Επόμενη Επικεφαλίδα (Next Header) έχοντας τιμή ίση με 43 της αμέσως προηγούμενης επικεφαλίδας. (με περισσότερες λεπτομέρειες θα αναφερθούμε στο 5^{ο} Κεφάλαιο της παρούσας μεταπτυχιακής διατριβής).
- ***Fragment Header (Επικεφαλίδα Διάσπασης)***: όταν ένας Ipv6 host θέλει να στείλει ένα πακέτο σε έναν Ipv6 προορισμό, αναγνωρίζει το MTU του μονοπατιού για τον καθορισμό του μέγιστου μεγέθους πακέτου που μπορεί να χρησιμοποιήσει στο μονοπάτι για τον συγκεκριμένο προορισμό. Εάν το πακέτο είναι μεγαλύτερο από αυτό που μπορεί να υποστηρίξει το MTU του μονοπατιού, ο host της αφετηρίας κατακερματίζει το πακέτο. Έτσι χρησιμοποιείται από την πηγή για να στείλει πακέτα μεγαλύτερα από το μέγιστο μήκος πακέτου που υποστηρίζεται από όλους τους συνδέσμους της διαδρομής. Σε αντίθεση με το Ipv4, στο Ipv6 , ένα πακέτο δεν διασπάται από έναν δρομολογητή κατά μήκος της διαδρομής παρά μόνο από την πηγή (θα αναφερθούμε εκτενέστερα σε αυτήν την επικεφαλίδα επέκτασης στο 5^{ο} Κεφάλαιο)
- ***Destination Options Header (Επικεφαλίδα Προορισμού)***: χρησιμοποιείται για να μεταφέρει προαιρετικές πληροφορίες, που χρειάζεται να εξεταστούν μόνο από τους κόμβους προορισμού. Η Επικεφαλίδα Δρομολόγησης αναγνωρίζεται στο πεδίο Επόμενη Επικεφαλίδα (Next Header) έχοντας τιμή ίση με 60 της αμέσως προηγούμενης επικεφαλίδας. Παρουσιάζει πολλές ομοιότητες με την επικεφαλίδα επέκτασης Βήμα-προς-Βήμα.

Επιπλέον μπορούμε ν αναφέρουμε τις Επικεφαλίδες Επέκτασης , Authentication Header (Επικεφαλίδα Πιστοποίησης) και Encapsulation Security Payload (Επικεφαλίδα Ενσωματωμένης Ασφάλειας) που ανήκουν στην κατηγορία της IP Security αλλά και την Επικεφαλίδα Υποστήριξης Φορητότητας (Mobility Header).

- ***Authentication Header (Επικεφαλίδα Πιστοποίησης)***: προσφέρει ένα μηχανισμό κρυπτογραφικού αθροίσματος ελέγχου.
- ***Encapsulation Security Payload (Επικεφαλίδα Ενσωματωμένης Ασφάλειας)***: είναι η τελευταία επικεφαλίδα και προσφέρει υπηρεσίες αποκρυπτογράφησης.
- ***Mobility Header (Επικεφαλίδα Φορητότητας)***: προσφέρει υπηρεσίες υποστήριξης των κινητών χρηστών στα Ipv6 δίκτυα.

2.2 Η διευθυνσιοδότηση στο IPv6

Το Ipv6 σχεδιάστηκε προκειμένου να επιλύσει πολλά από τα προβλήματα που παρουσιάζονται στο πρωτόκολλο Ipv4. Η νεότερη αυτή έκδοση του πρωτοκόλλου επιτελεί τις ίδιες αλλά και περισσότερες λειτουργίες από ότι στο Ipv4 και μάλιστα χωρίς τους περιορισμούς της. Το Ipv6 χρησιμοποιεί 128 bits για την διευθυνσιοδότηση των κόμβων του διαδικτύου αντί για τα 32 bits του Ipv4. Σύμφωνα με το Ipv4 μια IP διεύθυνση αποτελείται από τέσσερις οκτάδες (octets) δυαδικών ψηφίων. Για παράδειγμα μια ορθή Ipv4 διεύθυνση έχει την παρακάτω μορφή :
XXX.XXX.XXX.XXX όπου XXX είναι ο δεκαδικός αριθμός που προκύπτει από την κάθε οκτάδα των bit.
Με τα 128 bit του Ipv6 σημαίνει ότι η IP διευθύνσεις πλέον είναι πολύ περισσότερες. Άλλωστε αυτός είναι και ο κύριος λόγος μετάβασης στο νέο πρωτόκολλο διευθυνσιοδότησης. Υπάρχουν τριών ειδών τύπων διευθύνσεων:

- ***Unicast***: χρησιμοποιείται για τον προσδιορισμό μιας μεμονωμένης διεπαφής (interface), όπου διεπαφή ορίζουμε το σημείο επαφής ενός κόμβου με ένα δικτυακό σύνδεσμο, και ένας κόμβος μπορεί να έχει πολλαπλές διεπαφές. Υποστηρίζει διάφορους τύπους διευθύνσεων όπως οι global aggregatable, οι site –link-local, site-local και οι Ipv4-compatible. Οι global μπορούν να δρομολογηθούν σ ολόκληρο το Διαδίκτυο και επιτρέπουν την άθροιση των προθεμάτων δρομολόγησης προκειμένου να περιορίσουν τον αριθμό καταχωρίσεων στους global πίνακες δρομολόγησης. Η link-local διευθύνσεις (τοπικού συνδέσμου) εξαλείφουν την ανάγκη για globally μοναδικό πρόθεμα. Σχεδιάστηκαν για την χρήση σε ένα link με στόχο την αυτόματη απόδοση διευθυνσιοδότησης, ανακάλυψη γείτονα ή όταν δεν υπάρχουν δρομολογητές. Παρέχουν την δυνατότητα επικοινωνίας μεταξύ συσκευών σε τοπικό σύνδεσμο. Οι site-local (τοπικού οργανισμού), χρησιμοποιούνται ως ιδιωτικές διευθύνσεις για τη χρήση εσωτερικά σε οργανισμούς έχοντας ένα οικουμενικό πρόθεμα. Τέλος οι Ipv4-compatible Ipv6 διευθύνσεις, δηλαδή Ipv6 με ενσωματωμένες Ipv4 διευθύνσεις, συμπεριλαμβάνουν μια τεχνική ώστε οι κόμβοι και οι δρομολογητές να προωθούν Ipv6 πακέτα πάνω από Ipv4 υποδομή.
- ***Multicast***: χρησιμοποιείται για την αποστολή πακέτων σε πολλαπλούς προορισμούς. Η μετάδοση multicast στέλνει πακέτα σε όλες τις διεπαφές (interfaces) που αποτελούν κομμάτι μιας multicast ομάδας. Η ομάδα αντιπροσωπεύεται από την Ipv6 διεύθυνση προορισμού του πακέτου. Ένα πακέτο που αποστέλλεται σε μια διεύθυνση multicast παραδίδεται σε όλες τις διεπαφές που προσδιορίζονται από αυτήν την διεύθυνση. Είναι ένα όρισμα συνόλου interfaces. Μια διεύθυνση δηλώνεται ως multicast έχοντας στην αρχή της οχτώ άσσους (11111111). Η μορφή της Multicast Ipv6 διεύθυνσης είναι:

8 bits	4 bits	4 bits	112 bits
11111111	flgs	scop	group ID

Πίνακας 2.1 Η multicast Ipv6 διεύθυνση

Η πρώτη οκτάδα προσδιορίζει την διεύθυνση ως multicast διεύθυνση. Το πεδίο flgs των 4-bit προσδιορίζει πότε η multicast διεύθυνση είναι μια καλά αναγνωρισμένη διεύθυνση ή αν πρόκειται για μια παροδική multicast διεύθυνση. Το πεδίο scop προσδιορίζει το εύρος της ομάδας multicast αλλά και το σκοπό αυτής της διεύθυνσης. Τέλος το πεδίο group ID που είναι 112 bits καθορίζει την ομάδα multicast, είτε είναι μόνιμη είτε είναι προσωρινή.

- ***Anycast:*** χρησιμοποιείται για ένα σύνολο διεπαφών που ανήκουν σε διαφορετικούς κόμβους. Μια μετάδοση anycast στέλνει πακέτα σε ένα μόνο από τα interfaces που σχετίζονται με την διεύθυνση, και όχι σε όλα τα interfaces. Το interface αυτό είναι συνήθως το κοντινότερο interface, όπως ορίζεται από το πρωτόκολλο δρομολόγησης με την μέτρηση απόστασης που χρησιμοποιεί. Όμοια με τις διευθύνσεις multicast, οι διευθύνσεις anycast μπορούν να αποδοθούν σε περισσότερα από ένα interfaces τα οποία συνήθως ανήκουν σε διαφορετικούς κόμβους. Οι anycast διευθύνσεις χορηγούνται από τις τυπικό χώρο των unicast διευθύνσεων και έτσι δεν μπορούν να διακριθούν από μια unicast διεύθυνση ως προς την μορφή τους. Έτσι, κάθε μέλος μιας unicast ομάδας θα πρέπει να ρυθμιστεί ώστε να αναγνωρίζει συγκεκριμένες διευθύνσεις ως διευθύνσεις anycast.
- ***Loopback:*** γνωστή και ως διεύθυνση ανατροφοδότησης. Χρησιμοποιείται από έναν κόμβο για να στείλει ένα Ipv6 πακέτο στον εαυτό του. Μία Ipv6 διεύθυνση ανατροφοδότησης είναι όμοια με αυτή του Ipv4. Δεν πρέπει ποτέ να χρησιμοποιείται ως διεύθυνση αποστολέα πακέτου που στέλνεται έξω από τον κόμβο και δεν πρέπει να προωθείται ποτέ ένα τέτοιο πακέτο έξω από τον κόμβο.
- ***Unspecified:*** η απροσδιόριστη διεύθυνση υποδηλώνει την απουσία μιας Ipv6 διεύθυνσης. Για παράδειγμα, πρόσφατα αρχικοποιημένοι Ipv6 κόμβοι μπορεί να χρησιμοποιήσουν την απροσδιόριστη διεύθυνση σαν διεύθυνση αφετηρίας για τα πακέτα τους μέχρι να λάβουν μια Ipv6 διεύθυνση. Η μορφή της είναι: 0:0:0:0:0:0:0:0 και δεν αποδίδεται ποτέ σε κόμβο.

Οι διευθύνσεις Ipv6, όλων των τύπων αποδίδονται σε interfaces και όχι σε κόμβους. Το Ipv6 συνεχίζει το μοντέλο που υπάρχει και στο Ipv4 όπου το πρόθεμα του υποδικτύου συσχετίζεται με ένα δικτυακό σύνδεσμο και πολλά προθέματα μπορούν να συσχετιστούν με τον ίδιο δικτυακό σύνδεσμο. Η διεύθυνση Ipv6 αποτελείται από οχτώ δεκαεξαδικές ομάδες. Κάθε δεκαεξαδική ομάδα, διαχωρίζεται από μία κολόνα της μορφής (:) άνω και κάτω τελείας, αποτελούμενη από μια δεκαεξαδική τιμή. Ακόλουθα παραθέτουμε την μορφή μιας τυπικής Ipv6 διεύθυνσης:
X:X:X:X:X:X:X:X όπου τα X αντιστοιχούν σε δεκαεξαδικές τιμές των οχτώ 16-bit ομάδων της διεύθυνσης. Πιο συγκεκριμένα η μορφή είναι: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
και κάθε x αντιπροσωπεύει μία 4-bit δεκαεξαδική τιμή. Το παρακάτω είναι ένα παράδειγμα μιας πιθανής Ipv6 διεύθυνσης:
4FDE:0000:0000:0002:0202:B897:FF3B:AB3F
Λόγω ορισμένων μεθόδων απεικόνισης διευθύνσεων Ipv6 είναι σύνηθες οι διευθύνσεις αυτές να περιέχουν μεγάλες συμβολοσειρές μηδενικών bits. Για να απλοποιήσεις την απεικόνιση μιας Ipv6 διεύθυνσης μπορείς να χρησιμοποιήσεις δύο κολόνες (::) που προσδιορίζουν πολλαπλές

ομάδες μηδενικών 16-bits πεδίων. Αυτό μπορεί να εμφανιστεί μόνο μια φορά σε μία διεύθυνση. Μπορεί ακόμα να χρησιμοποιηθεί για συμπίεση των αρχικών ή των τελικών μηδενικών της διεύθυνσης. Παρακάτω παραθέτουμε έναν πίνακα με χαρακτηριστικά παραδείγματα συμπιεσμένων Ipv6 διευθύνσεων:

Τύπος Ipv6 διεύθυνσης	Πλήρης Μορφή	Συμπιεσμένη Μορφή
Unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01::101
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

Πίνακας 2.2 Συμπιεσμένη μορφή Ipv6 διευθύνσεων

2.3 Αυτορύθμιση διευθύνσεων και σταθμών

Το IPv6 προσφέρει την δυνατότητα σε ένα σταθμό εργασίας να συνδεθεί αυτόματα στο δίκτυο μέσω του νέου σχεδιασμού και των δυνατοτήτων που προσφέρονται για αυτόματη ρύθμιση παραμέτρων μέσω του DHCPv6, μία τεχνική για αυτόματη ρύθμιση διευθύνσεων με αποθήκευση κατάστασης. Η δυνατότητα αυτή προσφέρεται ακόμα και μέσω της αυτόματης ρύθμισης διευθύνσεων χωρίς αποθήκευση κατάστασης (stateless address autoconfiguration).
Στο Ipv4 η διευθυνσιοδότηση γινόταν είτε χειροκίνητα, είτε αυτόματα με την χρήση κάπου DHCP (Dynamic Host Configuration Protocol). Η διαδικασία αυτόματης ανάθεσης διεύθυνσης στο Ipv6 περιλαμβάνει την δημιουργία μιας τοπικής διεύθυνσης και επαλήθευση της μοναδικότητάς της σε μια σύνδεση. Παρακάτω παραθέτουμε πιο αναλυτικά τις δύο τεχνικές:

- ***Stateless Address Autoconfiguration***: είναι η διαδικασία που χρησιμοποιούν οι Ipv6 κόμβοι (σταθμοί ή δρομολογητές) προκειμένου να ρυθμίσουν αυτόματα τις Ipv6 διευθύνσεις για τα interfaces. Ένα κόμβος δημιουργεί διάφορες Ipv6 διευθύνσεις συνδυάζοντας το πρόθεμα μιας διεύθυνσης είτε με την MAC διεύθυνση του κόμβου είτε χρησιμοποιώντας έναν αναγνωριστή διεπαφής (interface identifier). Τα προθέματα περιλαμβάνουν το πρόθεμα τοπικού συνδέσμου (link-local prefix) δηλαδή της μορφής fe80::/10 και προθέματα μήκους 64 “διαφημιζόμενα” από τοπικούς Ipv6 δρομολογητές, εάν βέβαια υπάρχουν. Η Αυτόματη Ρύθμιση Διευθύνσεων Χωρίς Αποθήκευση Κατάστασης δημιουργεί επίσης κατάλληλα multicast interfaces όταν ο τύπος συνδέσμου είναι multicast ικανός. Δεν απαιτεί καμία χειροκίνητη διαμόρφωση των κόμβων, ελάχιστη έως και μηδαμινή διαμόρφωση των δρομολογητών και κανένα πρόσθετο server. Ο μηχανισμός stateless επιτρέπει σε έναν Ipv6 κόμβο να παράγει την διεύθυνσή του συνδυάζοντας απλά τοπικές διαθέσιμες πληροφορίες και πληροφορίες που διαφημίζονται από τους δρομολογητές. Οι κόμβοι παράγουν ένα “αναγνωριστή διεπαφής” που χαρακτηρίζει μοναδικά μια διεπαφή σε ένα υποδίκτυο και οι δρομολογητές διαφημίζουν τα προθέματα του υποδικτύου. Έτσι μια διεύθυνση διαμορφώνεται με τον συνδυασμό αυτών των δύο. Όταν απουσιάζουν οι δρομολογητές από την διαδικασία, ένας κόμβος έχει την δυνατότητα να μπορεί να παράγει διευθύνσεις τοπικού συνδέσμου, και οι οποίες να μπορούν να υποστηρίξουν επικοινωνία μεταξύ των κόμβων του ίδιου συνδέσμου. Πραγματοποιείται κατά την διαδικασία

αρχικοποίησης της διεπαφής, όπως για παράδειγμα κατά την εγκατάσταση ενός κόμβου και εκτελείται πλήρως μόνο σε τελικούς σταθμούς και όχι δρομολογητές.

- ***Stateful Address Autoconfiguration (DHCPv6)***: σε αυτό το μοντέλο αυτόματης ρύθμισης , οι κόμβοι λαμβάνουν τις διευθύνσεις των διεπαφών ή/και τις πληροφορίες διαμόρφωσης από έναν κεντρικό server (DHCPv6). Η stateful προσέγγιση χρησιμοποιείται όταν απαιτείται αυστηρότερος έλεγχος για ακριβείς αναθέσεις διευθύνσεων, σε αντίθεση με την stateless που χρησιμοποιείται όταν δεν ενδιαφερόμαστε ιδιαίτερα για την ακριβή ανάθεση διευθύνσεων, εφόσον αυτές είναι μοναδικές και κατάλληλα δρομολογήσιμες. Η Αυτόματη Ρύθμιση Διευθύνσεων Με Αποθήκευση Κατάστασης χρησιμοποιείται για την ρύθμιση διευθύνσεων μη τοπικού συνδέσμου (non-link-local addresses) μέσω της χρήσης ενός πρωτοκόλλου διαμόρφωσης, του DHCPv6, όπου δεν απαιτεί ρύθμιση παραμέτρων από τον χρήστη εκτός και αν το υπαγορεύουν συγκεκριμένες ανάγκες. Οι κεντρικοί υπολογιστές διατηρούν μια βάση δεδομένων που κρατάν τις ήδη χρησιμοποιημένες διευθύνσεις. Η όλη διαδικασία είναι ένα μοντέλο πελάτη-εξυπηρετητή και η επικοινωνία τους μπορεί να υφίσταται ακόμα και όταν βρίσκονται σε διαφορετικές συνδέσεις με την βοήθεια ενός ενδιάμεσου κόμβου του DHCP αναμεταδότη που βρίσκεται στην ίδια σύνδεση με τον πελάτη.

Τα δύο αυτά μοντέλα απόδοσης IP διευθύνσεων μπορούν να αλληλοσυμπληρώνονται. Για παράδειγμα ένας κόμβος μπορεί να χρησιμοποιεί τον stateful μηχανισμό για να λάβει επιπρόσθετες πληροφορίες, αλλά και τον stateless μηχανισμό για την απόκτηση και διαμόρφωση της διεύθυνσης του.

2.4 Η δρομολόγηση στο IPv6

Προκειμένου τα πακέτα Ipv6 να φτάσουν στους απομακρυσμένους τους προορισμούς πρέπει γενικά να περάσουν από διάφορους Ipv6 δρομολογητές. Γενικότερα ο δρομολογητής είναι ο ενδιάμεσος κόμβος στην επικοινωνία μεταξύ ενός σταθμού και του υπόλοιπου δικτύου Ipv6. Το σπουδαιότερο πράγμα που πετυχαίνει το πρωτόκολλο Ipv6 σε αυτόν τον τομέα είναι η ιεραρχική δρομολόγηση. Με αυτό πετυχαίνει να απλοποιήσει αρκετά την όλη διαδικασία της δρομολόγησης, μειώνοντας στο περισσότερο δυνατόν τους πίνακες δρομολόγησης των δρομολογητών. Έτσι ταυτόχρονα πετυχαίνει και μείωση του κόστους παράλληλα με την αύξηση της απόδοσης των δρομολογητών. Ένα επιπλέον στοιχείο που προστίθεται με τον νέο σχεδιασμό είναι ότι ο δρομολογητής τώρα όχι μόνο ξέρει πως θα μεταφέρει το πακέτο στον προορισμό του αλλά και που βρίσκεται.

Το Ipv6 είναι ο χώρος στον οποίο γίνεται η διαλογή και η παράδοση των πακέτων. Κάθε εισερχόμενο ή εξερχόμενο πακέτο, ονομάζεται πακέτο Ipv6. Ένα Ipv6 πακέτο περιλαμβάνει τόσο την διεύθυνση πηγής του αποστολέα όσο και την διεύθυνση προορισμού του παραλήπτη. Σε αντίθεση με τις διευθύνσεις link-layer, οι Ipv6 διευθύνσεις στην επικεφαλίδα Ipv6 παραμένουν το ίδιο όσο το πακέτο ταξιδεύει μέσα σε ένα Ipv6 δίκτυο. Η δρομολόγηση είναι η κύρια λειτουργία του Ipv6. Τα Ipv6 πακέτα ανταλλάσσονται και επεξεργάζονται σε κάθε σταθμό χρησιμοποιώντας το Ipv6 στο επίπεδο Διαδικτύου.

Στο Ipv6 οι διευθύνσεις επιτρέπεται να χαρακτηρίζονται με όσο το δυνατόν μικρότερη μάσκα από bits πράγμα πολύ σημαντικό στην απλοποίηση και απόδοση της δρομολόγησης, μιας και τώρα πια οι κεντρικοί δρομολογητές δεν θα χρειάζεται να αποθηκεύουν σε μεγάλους πίνακες αναλυτικά όλους τους αριθμούς των δικτύων που χρειάζονται προκειμένου να δρομολογήσουν

τα πακέτα τους. Οι Ipv6 δρομολογητές μπορούν να συνδέονται με δύο ή περισσότερα τμήματα Ipv6 δικτύων που έχουν την δυνατότητα να προωθούν πακέτα μεταξύ τους.

2.4.1 Τα πρωτόκολλα δρομολόγησης

Τα πρωτόκολλα δρομολόγησης διακρίνονται σε δύο μεγάλες κατηγορίες, σε αυτά τα οποία αναλαμβάνουν την δρομολόγηση εντός Αυτόνομων συστημάτων, τα οποία ονομάζονται IGPs (Interior Gateway Protocols) και αυτά τα οποία αναλαμβάνουν την δρομολόγηση μεταξύ Αυτόνομων συστημάτων και ονομάζονται EGPs (Exterior Gateway Protocols). Με τον όρο Αυτόνομα σύστημα ορίζουμε ένα δίκτυο του οποίου την διαχείριση τν έχει ένας φορέας. Οι διαφορές των πρωτοκόλλων δρομολόγησης του IPv6 σε σχέση με αυτών του Ipv4 δεν είναι μεγάλες και αυτό δικαιολογείται από το γεγονός του ότι μειώθηκε σημαντικά το μέγεθος των καταχωρήσεων στους πίνακες δρομολόγησης και έτσι οι αυτοί που ήδη προϋπήρχαν δεν χρειαζόταν να τροποποιηθούν σημαντικά προκειμένου να επιτύχουμε το επιθυμητό αποτέλεσμα.
Παρακάτω παραθέτουμε συνοπτικά τα πρωτόκολλα δρομολόγησης στο Ipv6:

- ***RIPv6 (Routing Information Protocol)***: το πρωτόκολλο αυτό είναι βασισμένο στο μοντέλο IGP και σχεδιάστηκε από την Xerox για τα XNS δίκτυα. Εισήχθη στην αρχιτεκτονική TCP/IP το 1982 από το πανεπιστήμιο της Καλιφόρνιας στο Berkeley και περιγράφεται από το RFC 1058 το 19885 και ανανεώθηκε από το RFC 1388 το 1996. Το RIP έχει υιοθετηθεί ευρέως, κυρίως για υλοποιήσεις προσωπικών υπολογιστικών δικτύων και πολλά άλλα πρωτόκολλα δρομολόγησης είναι βασισμένα από αυτό. Το RIP αποτελεί ένα πίνακα αποστάσεων πρωτόκολλο στο οποίο κάθε δρομολογητής αποστέλλει τον δικό του πίνακα αποστάσεων στους γειτονικούς του δρομολογητές κάθε 30 δευτερόλεπτα. Οι πίνακες δρομολόγησης αποθηκεύουν μόνο την καλύτερο επόμενο βήμα προς κάθε κατεύθυνση. Ο κύριος περιορισμός του RIP είναι ότι επιτρέπει το πολύ μέχρι 15 βήματα και κάθε προορισμός με απόσταση μεγαλύτερη των 15 βημάτων θεωρείται μη προσπελάσιμος. Το RIPv6 χρησιμοποιεί δύο ειδών μηνύματα, του τύπου request (αίτηση) και response (απόκριση), τα οποία μεταδίδονται με την χρήση του πρωτοκόλλου UDP (User Datagram Protocol).
- ***OSPFv6 (Open Shortest Path First)***: το πρωτόκολλο αυτό είναι και αυτό βασισμένο πάνω στο IGP και χρησιμοποιεί τον αλγόριθμο Dijkstra. Το OSPF είναι βασισμένο πάνω στην έννοια της ιεραρχίας. Η ρίζα της ιεραρχίας είναι το Αυτόνομο σύστημα που μπορεί να υποδιαιρεθεί σε τομείς, καθένας από τους οποίους περιλαμβάνει μια ομάδα διασυνδεδεμένων δικτύων. Η δρομολόγηση εντός της περιοχής ονομάζεται «intra-area» και η δρομολόγηση ανάμεσα σε διαφορετικές περιοχές «inter-area». Κάθε Αυτόνομο σύστημα έχει μία περιοχή κορμού (backbone area) που μπορεί να μην είναι συνεχόμενη. Σε αυτήν την περίπτωση, η ρύθμιση εικονικών συνδέσεων είναι απαραίτητα για την διασφάλιση της συνοχής του. Όλες οι άλλες περιοχές συνδέονται με την περιοχή κορμού. Λειτουργεί πάνω στην λογική των συνδέσεων και όχι των υποδικτύων. Επίσης έχει την δυνατότητα να τρέχουν πολλαπλές οντότητες του OSPFv6 αλγορίθμου ταυτόχρονα στη ίδια σύνδεση και δεν γίνεται πια πιστοποίηση από αυτό μιας και το Ipv6 έχει ενσωματωμένες τέτοιες δυνατότητες.
- ***IDRPv2 (Inter-Domain Routing Protocol):*** είναι ένα EGP πρωτόκολλο που χρησιμοποιείται στο Ipv6. Το IDRP είναι ένα “path vector” (πίνακας μονοπατιού) πρωτόκολλο σχεδιασμένο να χρησιμοποιείται στην αρχιτεκτονική OSI. Το IDRv2 χρησιμοποιεί τον όρο domain δρομολόγηση αντί του όρου αυτόνομη. Η δρομολόγηση

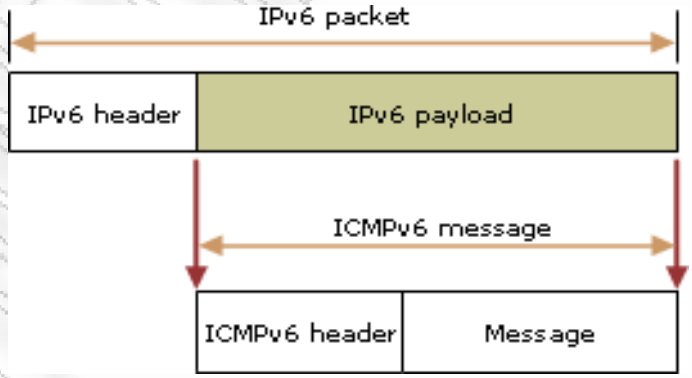
domain αναγνωρίζεται από ένα Ipv6 πρόθεμα (128-bit διεύθυνσης). Αυτός ο προσδιορισμός απλοποιεί το έργο της IANA επειδή τώρα εκχωρεί ρητά τα αναγνωριστικά του Αυτόνομου συστήματος, το οποίο στο Ipv4 ήταν 16 bits, και πλέον δεν είναι απαραίτητο. Οι τομείς δρομολόγησης μπορούν να ομαδοποιηθούν σε Routing Domain Confederation. Αυτοί οι τομείς δρομολογήσεις λογαριάζονται ως μοναδικές οντότητες και αναγνωρίζονται επίσης από τα Ipv6 προθέματα. Μπορούν επίσης να ομαδοποιηθούν εισάγοντας έναν αυθαίρετο αριθμό στο επίπεδο ιεραρχίας. Η επικεφαλίδα IDRP αναγνωρίζεται από την τιμή 45 στο πεδίο Next Header της προηγούμενης επικεφαλίδας.

Στις δύο επόμενες ενότητες παραθέτουμε πιο αναλυτικά δύο άλλα σημαντικά πρωτόκολλα δρομολόγησης το ICMPv6 και το πρωτόκολλο Εύρεσης Γειτόνων.

2.4.2 Το πρωτόκολλο ICMPv6

Το πρωτόκολλο δρομολόγησης Internet Control Message Protocol της νεότερης έκδοσης του πρωτοκόλλου IP έχει κατά κύριο λόγο τις ίδιες χρήσεις και ικανοποιεί κατά ένα μεγάλο ποσοστό τους ίδιους σκοπούς με την προγενέστερη έκδοσή του, ωστόσο υπάρχουν κάποιες πολύ σημαντικές αλλαγές. Αποτελεί αναπόσπαστο κομμάτι της αρχιτεκτονικής IPv6 και υποστηρίζεται από όλες τις Ipv6 υλοποιήσεις. Συνδυάζει λειτουργίες που προηγουμένως υποδιαιρούνταν μεταξύ διαφόρων πρωτοκόλλων όπως το ICMP (Internet Control Message Protocol), του IGMP (Internet Group Membership Protocol) και ARP (Address Resolution Protocol) και εισάγει κάποιες απλοποιήσεις περιορίζοντας ή και καταργώντας τύπους μηνυμάτων που δεν χρησιμεύουν πλέον.

Το ICMPv6 είναι ένα πρωτόκολλο πολλαπλού σκοπού. Για παράδειγμα χρησιμοποιείται για την αναφορά λαθών που αντιμετωπίζουν στον τομέα της επεξεργασίας των πακέτων, εκτελεί διάγνωση προβλημάτων και Neighbor Discovery (Εύρεση γειτόνων που θα εξηγηθεί αναλυτικότερα στην επόμενη ενότητα) και κάνει διαχείριση multicast ομάδων. Για το λόγο αυτό τα ICMPv6 μηνύματα χωρίζονται σε δύο κατηγορίες, στα μηνύματα λάθους (error messages) και στα μηνύματα πληροφοριών (information messages). Τα μηνύματα μεταφέρονται διαμέσου ενός Ipv6 πακέτου στου οποίου μπορεί να υπάρχουν ακόμα και επικεφαλίδες επέκτασης. Ένα ICMPv6 μήνυμα διακρίνεται με την τιμή 58 του πεδίου Next Header μιας Ipv6 επικεφαλίδας ή της προηγούμενης επικεφαλίδας.



Εικόνα 2.3 Η δομή του ICMPv6 μηνύματος στο Ipv6 πακέτο
Πηγή: (http://technet.microsoft.com/en-us/library/cc757063%28WS.10%29.aspx)

Στον ακόλουθο πίνακα παρουσιάζουμε τα βασικά μηνύματα που χρησιμοποιεί το ICMPv6 και τα οποία παρουσιάζουν αρκετές ομοιότητες με αυτά του προγενέστερου πρωτοκόλλου:

ICMPv6 Μήνυμα	Περιγραφή
Μη Προσβάσιμος Παραλήπτης (Destination Unreachable)	Ένα μήνυμα λάθους που ενημερώνει τον αποστολέα ότι το πακέτο δεν μπορεί να παραδοθεί
Πολύ Μεγάλο Πακέτο (Packet Too Big)	Ένα μήνυμα λάθους που ενημερώνει τον αποστολέα ότι το πακέτο είναι πολύ μεγάλο για να σταλεί
Λήξη Χρόνου (Time Exceeded)	Ένα μήνυμα λάθους που ενημερώνει τον αποστολέα ότι το ΄Οριο Βημάτων (Hop Limit) του Ipv6 πακέτου είναι 0 ή έχει μειωθεί στο 0
Προβλήματα Παραμέτρου (Parameter Problems)	Ένα μήνυμα λάθους ενημερώνει τον αποστολέα ότι υπήρξε σφάλμα κατά την επεξεργασία της Ipv6 επικεφαλίδας ή της Ipv6 επικεφαλίδα επέκτασης
Αίτηση Ηχούς (Echo Request)	Ένα διαγνωστικό μήνυμα που χρησιμοποιείται για να διαπιστώσει πότε ένας Ipv6 κόμβος είναι προσβάσιμος στο δίκτυο
Απάντηση Ηχούς (Echo Reply)	Ένα διαγνωστικό μήνυμα που χρησιμοποιείται για να απαντήσει στο ICMPv6 Echo Request

Πίνακας 2.3 Τα βασικά μηνύματα που χρησιμοποιεί το ICMPv6

2.4.3 Το πρωτόκολλο Εύρεσης Γειτόνων στο IPv6

Οι κόμβοι στο πρωτόκολλο Ipv6, είτε αυτοί είναι δρομολογητές είτε κόμβοι υποδοχής ή αποστολής πακέτων, κάνουν χρήση του πρωτοκόλλου Εύρεσης Γειτόνων προκειμένου να προσδιορίσουν την διεύθυνση σύνδεσης των γειτονικών κόμβων που γνωρίζουν ότι βρίσκονται στο ίδιο υποδίκτυο (ή στο ίδιο φυσικό μέσο) και για να εξαλείψουν άμεσα τις τιμές που έχουν χάσει την ισχύ τους. Επίσης χρησιμοποιείται προκειμένου να ανακαλύψει το πρόθεμα της διεύθυνσης της σύνδεσής τους έτσι ώστε να ξεχωρίζουν τους σταθμούς του υποδικτύου τους από τους υπόλοιπους. Πολύ σημαντικός είναι και ο ρόλος τους στην επέκταση του ICMPv6 που αφορά στη εύρεση του MTU μονοπατιού από τον κόμβο αποστολέα. Τέλος, κόμβοι χρησιμοποιούν αυτό το πρωτόκολλο ώστε να γνωρίζουν ποιοι γειτονικοί κόμβοι είναι προσβάσιμοι και ποιο όχι, και για την ανίχνευση άλλου επιπέδου σύνδεσης και διευθύνσεων. Όταν ένας δρομολογητής ή η διαδρομή προς αυτόν αποτύχει, αναζητούνται άμεσα εναλλακτικές λειτουργίες.

Σε αντίθεση με το πρωτόκολλο Ipv4 στο Ipv6 δεν χρησιμοποιούνται τα πρωτόκολλα ARP και RARP προκειμένου να συσχετιστούν οι διευθύνσεις IP με τις διευθύνσεις του επιπέδου σύνδεσης. Και αυτό γιατί τώρα χρησιμοποιείται η τεχνική multicast που αυτοματοποιεί τις διαδικασίες (δυνατότητα αυτόματης δημιουργίας διευθύνσεων), αν και είναι δύσκολη η υλοποίηση του σε δίκτυα που δεν παρέχουν δυνατότητα broadcast. Μέσα στους άλλους σκοπούς που εξυπηρετεί το πρωτόκολλο Εύρεσης γειτόνων είναι και η δυνατότητα ελέγχου της μοναδικότητας της διεύθυνσης, ώστε να ανακαλύψει ένας κόμβος ότι η διεύθυνση που χρησιμοποιεί είναι μοναδική στο τοπικό δίκτυο.

Θα δούμε σε επόμενο κεφάλαιο πως αυτό το πρωτόκολλο δρομολόγησης αποτελεί σημαντικό παράγοντα σε ενδεχόμενες επιθέσεις που μπορεί να δεχτεί το πρωτόκολλο Ipv6. Οι λειτουργίες που εξυπηρετεί αλλά και η χρησιμότητα του το καθιστούν από τους νούμερο έναν στόχους για

μια ενδεχόμενη κακόβουλη ενέργεια. Για το λόγο αυτό έχει μελετηθεί αρκετά κατά τον σχεδιασμό της νέας έκδοσης του πρωτοκόλλου το θέμα της ασφάλειας του. Το πρωτόκολλο Εύρεσης Γειτόνων κάνει χρήση των μηνυμάτων του ICMPv6 προκειμένου να επιτελέσει τις περισσότερες από τις λειτουργίες τους. Έτσι καθίσταται σαφές και η κρισιμότητα του πρωτοκόλλου ICMPv6 ως προς την ασφάλεια.

2.5 Θέματα Απόδοσης

Σε πολλά σημεία των παραπάνω ενοτήτων τονίσαμε την σημασία του πρωτοκόλλου IPv6 ως προς την βελτίωσης της αποδοτικότητας που έχει προσφέρει λόγω του σχεδιασμού αλλά και της γενικότερης δομής του. Ο απλούστερος σχεδιασμός των επικεφαλίδων του αλλά και το σταθερό μέγεθός τους βοηθούν στην γρηγορότερη και ευκολότερη επεξεργασία τους από τους δρομολογητές. Ένα επίσης σημαντικό στοιχείο που παρατηρούμε και βοήθησε και αυτό με την σειρά του στην αυξημένη απόδοση του πρωτοκόλλου IPv6 σε σχέση με το προγενέστερο του είναι η κατάργηση της χρήσης αθροισμάτων ελέγχου (checksums) που εξυπηρετούσε τον προσδιορισμό της ακεραιότητας του πακέτου. Αυτό τώρα υποστηρίζεται από το επίπεδο σύνδεσης (link-layer) και έτσι μειώνεται ο χρόνος που απαιτείται για την επεξεργασία των πακέτων.

Σημαντικό επίσης να τονίσουμε το γεγονός ότι από το IPv6 αφαιρέθηκαν εξ ολοκλήρου όλες εκείνες οι επικεφαλίδες που στο IPv4 έμεναν αχρησιμοποίητες. Με τον τρόπο αυτό αντισταθμίστηκε η διαφορά μεγέθους των IPv6 διευθύνσεων που ήταν τετραπλάσιες σε μέγεθος σε σχέση με αυτές του IPv4, μιας και το μήκος των IPv6 είναι μόλις το διπλάσιο από τις IPv4 υποχρεωτικές επικεφαλίδες και έτσι το overhead της επικεφαλίδας ελαχιστοποιείται. Επιπλέον το IPv6 υποστηρίζει τους μηχανισμούς multicast βοηθώντας στην απλοποίηση της διαχείρισης τους και οι θέσεις των επικεφαλίδων ασφαλείας και των κινητών κόμβων είναι προκαθορισμένος με αποτέλεσμα να μην χρειάζεται επιπλέον χρόνος προκειμένου να επεξεργαστούν τα πακέτα. Το IPv6 πετυχαίνει καταμερισμό του φόρτου είτε μέσω της ανάθεσης των βασικών υπηρεσιών του σε διευθύνσεις τύπου anycast είτε παραχωρώντας μία IPv6 διεύθυνση σε περισσότερες από μία διεπαφές.

Τέλος στο IPv4 σε περίπτωση που το πακέτο ήταν μεγαλύτερο από την MTU του μονοπατιού από τον αποστολέα στον παραλήπτη, τότε ο κάθε ενδιάμεσος κόμβος αυτής της διαδρομής αναγκαζόταν να κατακερματίσει το πακέτο που παρέλαβε. Στο IPv6 κάτι τέτοιο δεν συμβαίνει μιας και ο κάθε κόμβος που στέλνει το πακέτο εξασφαλίζει προτού στείλει το πακέτο ότι δεν θα χρειαστεί να κατακερματιστεί. Έτσι προσφέρει ευκολία στην μετάδοση με άμεσο επακόλουθο της αύξηση της αποδοτικότητας του πρωτοκόλλου.

Κεφάλαιο 3

Προχωρημένα Θέματα Ασφαλείας του IPv6

3.1 Δίκτυα και Ασφάλεια

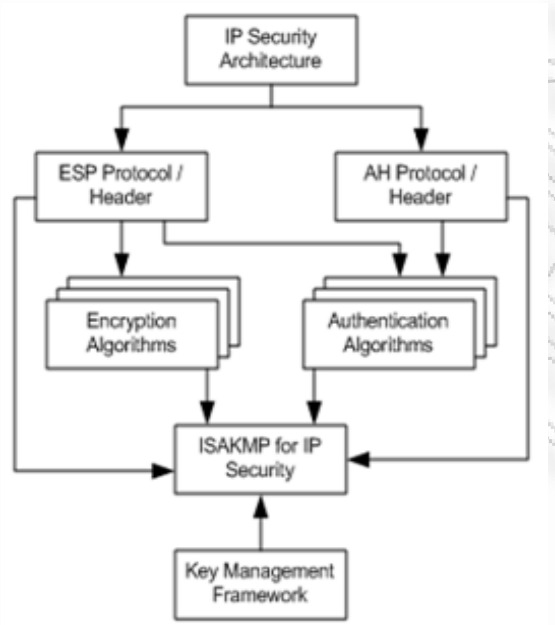
Η ανάπτυξη και η εκτεταμένη χρήση του Διαδικτύου έφερε καινούριες απαιτήσεις από τους χρήστες οι οποίοι ζητούν οι συναλλαγές τους και η πρόσβαση στις πηγές τους να γίνονται με ασφάλεια. Στο IPv4 δεν υπήρχαν τα χαρακτηριστικά εκείνα που θα μπορούσαν να χρησιμεύσουν στην ασφάλεια των δικτύων και έτσι η προσπάθεια έχει επικεντρωθεί στην χρήση μεθόδων στο επίπεδο δικτύου. Εξάλλου λόγω του αρχικού σκοπού χρήσης του πρωτοκόλλου IPv4 που ήταν να μπορούν να επικοινωνούν μεταξύ τους τα ακαδημαϊκά ιδρύματα, δεν είχε δοθεί καθόλου βάρος στο θέμα της ασφάλειας. Ωστόσο λόγω της μεγάλης εξάπλωσής του στο διαδίκτυο αλλά της εισχώρησής του στο χώρο του ηλεκτρονικού εμπορίου και των επιχειρήσεων γενικότερα, η ανάγκη για μεγαλύτερη ασφάλεια έγινε επιτακτική.

Προκειμένου να μπορέσει να ανταποκριθεί στις απαιτήσεις αυτές της σημερινής εποχής, η IETF δημιούργησε μία ομάδα εργασίας με συγκεκριμένο στόχο τον σχεδιασμό μιας αρχιτεκτονικής ασφαλείας και των αντίστοιχων πρωτοκόλλων βασισμένη στην κρυπτογραφία για το IPv6 πρωτόκολλο. Η αρχιτεκτονική αυτή, που αφορά το πρωτόκολλο IP και όχι την γενική αρχιτεκτονική ασφαλείας για το διαδίκτυο, ονομάζεται IPsec και προσαρμόζεται και στο πρωτόκολλο IPv4 με πολύ μεγαλύτερη όμως πολυπλοκότητα και κόστος. Και ο λόγος είναι διότι το πρωτόκολλο IPv6 σχεδιάστηκε ακολουθώντας και τηρώντας τις απαιτήσεις που όριζει το IPsec σε αντίθεση με το IPv4 που δεν παρέχει τις κατάλληλες επικεφαλίδες, Authentication Header και Encapsulating Security Payload στο πεδίο επικεφαλίδας IP επιλογών.

Έτσι το IPv6 παρέχει εγγενής τις δυνατότητες για παροχή ασφάλειας οι οποίες βασίζονται στις προσαρμοστικές επεκτάσεις της επικεφαλίδας του πακέτου IPv6. Όσον αφορά την επικεφαλίδα πιστοποίησης (Authentication Header) εξασφαλίζει την ορθότητα της ένδειξης της πηγής, που δείχνει από ποιον αποστολέα-κόμβο έρχεται το πακέτο. Πολύ σημαντική σε θέματα ασφαλείας, όπου κακόβουλοι χρήστες προσπαθούν να παράγουν πακέτα με πλαστή διεύθυνση πηγής. Η επίθεση αυτή, γνωστή με το όνομα IP spoofing, μπορεί να ξεγελάσει έναν εξυπηρετητή και έτσι να υπάρξει κακόβουλη πρόσβαση σε σημαντικά δεδομένα, πληροφορίες και λειτουργίες. Είναι ένας από τους πλέον διαδεδομένους τρόπους επίθεσης μιας και στο IPv4 δεν υπήρχε τρόπος ελέγχου και εξακρίβωσης ότι το πακέτο πράγματι προερχόταν από την διεύθυνσης πηγής που το ίδιο ανέφερε.

Το IPv6 παρέχει μεθόδους και επεκτάσεις για την κρυπτογράφηση της επικεφαλίδας του πακέτου IPv6, όπου μέσω κλειδιών κρυπτογράφησης πραγματοποιείται η κρυπτογράφηση του payload του πακέτου. Η χρήση των επεκτάσεων αυτών γίνεται είτε μεταξύ δύο κόμβων είτε σε συνδυασμό με μια security gateway (πύλη ασφαλείας) η οποία προσφέρει ακόμα μεγαλύτερο βαθμό ασφάλεια απέναντι σε κακόβουλες επιθέσεις. Γενικότερα στο IPv6 έχει δοθεί κατά τον σχεδιασμό του μεγάλο βάρος στην επίτευξη της μεγαλύτερης δυνατής ασφάλειας και ειδικότερα πάνω στις νέες τεχνολογίες. Άλλωστε πολλοί δεν κρύβουν το γεγονός ότι ένας από τους βασικούς λόγους μετάβασης από το πρωτόκολλο IPv4 σε αυτό του IPv6 ήταν το θέμα της ασφάλειας. Στις επόμενες ενότητες θα εντρυφήσουμε σε πιο προχωρημένα θέματα ασφαλείας.

Παρακάτω παραθέτουμε την εικόνα που δείχνει το μοντέλο ασφάλειας του πρωτοκόλλου IPv6:



Εικόνα 3.1: Μοντέλο ασφάλειας IPv6

Βλέπουμε ότι περιέχει μεθόδους κρυπτογράφησης (Encryption και Authentication Algorithms), μεθόδους πιστοποίησης (ESP Header και Authentication Header), συμπαγείς αλγορίθμους κρυπτογράφησης και υποστήριξη ανταλλαγής και διαπραγμάτευσης των χαρακτηριστικών ασφαλείας (ISAKMP) που θα περιγράψουμε σε επόμενη ενότητα πιο αναλυτικά.

3.2 Στόχοι Επίτευξης Ασφάλειας

Η επίτευξη της ασφάλειας στο πρωτόκολλο IPv6 βασίζεται στην επίτευξη τριών επιμέρους στόχων. Αρχικά της εξασφάλισης της εμπιστευτικότητας των δεδομένων αλλά και της δυνατότητας μετάδοσής τους έτσι ώστε να μπορούν να επεξεργαστούν και διαβαστούν μόνο από έναν συγκεκριμένο παραλήπτη και όχι από οποιοδήποτε ενδιάμεσο κόμβο της διαδρομής. Πράγμα πολύ σημαντικό προκειμένου να εξασφαλίζεται η ακεραιότητα της μετάδοσης της πληροφορίας στον συγκεκριμένο παραλήπτη. Επίσης σημαντικό κομμάτι στην επίτευξη της καθολικής ασφάλειας του πρωτοκόλλου είναι και αυτό της πιστοποίησης του παραλήπτη, γνωστό και ως authentication. Σύμφωνα με αυτό ελέγχονται τα δεδομένα αλλά και πιστοποιείται ότι ο κόμβος που απέστειλε τα δεδομένα αυτά είναι ο ίδιος που ορίζεται στο αντίστοιχο πεδίο του πακέτου (IP options). Τέλος ένας εξίσου σημαντικός στόχος ασφαλείας είναι αυτός της ακεραιότητας των ίδιων των δεδομένων. Δηλαδή, ελέγχεται και πιστοποιείται ότι τα δεδομένα δεν έχουν τροποποιηθεί κατά την μετάδοσή τους στην διαδρομή μεταξύ των κόμβων. Επίσης γίνεται χρήση της κωδικοποίησης με δημόσια κλειδιά προκειμένου να πιστοποιείται ο κόμβος που αποστέλλει τα δεδομένα.

Λόγω τους εύρους του διαδικτύου ελλοχεύουν πάρα πολλοί κίνδυνοι, μιας και υπάρχουν εξίσου πολλοί κόμβοι που μπορεί να γίνουν μέσα για κακόβουλες ενέργειες. Μια από τις πλέον διαδεδομένες παγίδες στο internet είναι οι αναλυτές της κυκλοφορίας της πληροφορίας, γνωστοί με το όνομα sniffers, οι οποίοι παρακολουθούν παράνομα την πληροφορία που διέρχεται στο δίκτυο. Η χρήση των κωδικοποιήσεων και των ψηφιακών υπογραφών σε κάποιες περιπτώσεις είναι πιθανό να μην μπορεί να εγγυηθούν την επίτευξη ασφάλειας σε ένα τέτοιο περιβάλλον. Ωστόσο λόγω του σχεδιασμού του πρωτοκόλλου IPv6 πάνω στις υπάρχουσες απαιτήσεις ασφαλείας, τις περισσότερες φορές οι κίνδυνοι κακόβουλων ενεργειών αποφεύγονται.

3.3 IP Security (IPsec)

Στο IPv6 η ασφάλεια βασίζεται κατά κύριο λόγο στο επίπεδο IP (IP level Security), όπου όλες οι διεργασίες ασφαλείας έχουν ως στόχο την διαφύλαξη της ακεραιότητας του IPv6 πακέτου από κάθε είδος επίθεσης κατά την μετάδοσή του μέσα στο δίκτυο. Το Διαδίκτυο όπως αναφέραμε και νωρίτερα αποτελεί στόχο πολλών ειδών επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου (confidentiality), της άρνησης παροχής υπηρεσιών (denial of services), της ακεραιότητας των δεδομένων (data integrity) αλλά και της πλαστοπροσωπίας. Ο σκοπός του IPsec είναι η αντιμετώπιση όλων αυτών των προβλημάτων μέσα στην ίδια υποδομή του δικτύου, χωρίς να υπάρχει η ανάγκη για εγκατάσταση και ρύθμιση ακριβών μηχανών και λογισμικού.

Ένα σύστημα χρησιμοποιεί το IPsec για να απαιτήσει από τους κόμβους που επικοινωνεί να κάνουν χρήση συγκεκριμένων αλγορίθμων και πρωτοκόλλων ασφαλείας. Το IPsec παρέχει κρυπτογράφηση στο επίπεδο του IP και αυτό είναι που το καθιστά και ακρογωνιαίο λίθο της συνολικής ασφάλειας. Οι προδιαγραφές του IPsec ορίζουν την επικεφαλίδα πιστοποίησης (AH-Authentication Header) για την παροχή υπηρεσίας ακεραιότητας δεδομένων και το φορτίο ενθυλάκωσης ασφάλειας (ESP-Encapsulating Security Payload) το οποίο με την σειρά του παρέχει πιστοποίηση ταυτότητας και ακεραιότητας δεδομένων. Επίσης έχουμε τον ορισμό των παραμέτρων επικοινωνίας μεταξύ δύο συσκευών που είναι η διαχείριση των κλειδιών και οι συσχετισμοί ασφάλειας (security associations).

Είναι πάνω από όλα ένα πρωτόκολλο ανοικτών προδιαγραφών για την διασφάλιση του απορρήτου των επικοινωνιών και παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφαλείας σε ένα δίκτυο. Οι βασικές υπηρεσίες του IPsec περιλαμβάνουν μεταξύ άλλων προστασία εναντίων επιθέσεων τύπου επανάληψης πακέτου (packet replay), όπου ο επιτιθέμενος προσπαθεί να προσβάλει την διαθεσιμότητα του συστήματος υποκλέπτοντας ένα πακέτο και στέλνοντάς το πολλές φορές στον κόμβο που το απέστειλε. Όπως επίσης παρέχει κωδικοποίηση των δεδομένων αλλά και εξασφάλιση της ακεραιότητας και του απορρήτου της ροής των δεδομένων. Το IPsec υλοποιεί κρυπτογράφηση και πιστοποίηση επιπέδου δικτύου, παρέχοντας μια λύση ασφαλείας μέσα στην ίδια την αρχιτεκτονική του δικτύου. Λόγο του γεγονότος αυτού τα συστήματα και οι εφαρμογές που βρίσκονται στις άκρες δεν χρειάζονται αλλαγές ή ρυθμίσεις για να έχουν το πλεονέκτημα της ισχυρής ασφάλειας. Επειδή τα κρυπτογραφημένα πακέτα μοιάζουν με κανονικά IP πακέτα μπορούν εύκολα να δρομολογηθούν μέσα από οποιοδήποτε IP δίκτυο, χωρίς να υποστούν καμία αλλαγή στον ενδιάμεσο δικτυακό εξοπλισμό. Οι συσκευές στα ακραία σημεία είναι οι μόνες οι οποίες γνωρίζουν για την κρυπτογράφηση. Πράγμα πολύ σημαντικό τόσο για την μείωση του κόστους διαχείρισης όσο και του κόστους υλοποίησης.

Παρακάτω αναφέρουμε συνοπτικά δύο έννοιες πολύ σημαντικές για την δομή της IPsec αρχιτεκτονική:

- ***Συσχετισμοί Ασφαλείας (Security Association)***: μια πολύ βασική έννοια για το IPsec. Η συσχέτιση ασφαλείας είναι μια μέθοδος που χρησιμοποιείται από την IPsec για την παρακολούθηση όλων των λεπτομερειών που αφορούν μια δεδομένη IPsec επικοινωνία. Μια Σχέση Ασφαλείας είναι μια συσχέτιση που υφίσταται μεταξύ δύο ή περισσοτέρων οντοτήτων που περιγράφει πώς οι οντότητες θα χρησιμοποιήσουν τις υπηρεσίες ασφαλείας για να επικοινωνήσουν με ασφάλεια. Η SA παρέχει υπηρεσίες ασφαλείας στη ροή δεδομένων που μεταφέρει. Για την ασφαλή επικοινωνία μεταξύ δύο συστημάτων απαιτούνται δύο διαφορετικές SA, μία για κάθε διεύθυνση προορισμού. Ο Συσχετισμός Ασφαλείας είναι μια δήλωση της διαπραγματεύσιμης πολιτικής ασφαλείας μεταξύ δύο συσκευών.
- ***Δείκτης Παραμέτρων Ασφαλείας (SPI-Security Parameter Index):*** ονομάζεται ο τυχαία επιλεγμένος μοναδικός αριθμός που αναγνωρίζει μοναδικά τον συσχετισμό ασφαλείας. Όταν ένα σύστημα στέλνει ένα πακέτο το οποίο απαιτεί IPsec προστασία κοιτάει τον συσχετισμό ασφαλείας στη βάση δεδομένων του, εφαρμόζει την συγκεκριμένη επεξεργασία και ακολούθως εισάγει τον SPI από τον συσχετισμό ασφαλείας στην IPsec επικεφαλίδα. Όταν το αντίστοιχο μηχάνημα IPsec λαμβάνει το πακέτο κοιτάει με την σειρά του το συσχετισμό ασφαλείας της διεύθυνσης προορισμού και του SPI και μετά επεξεργάζεται το πακέτο όπως αυτό ορίζεται.

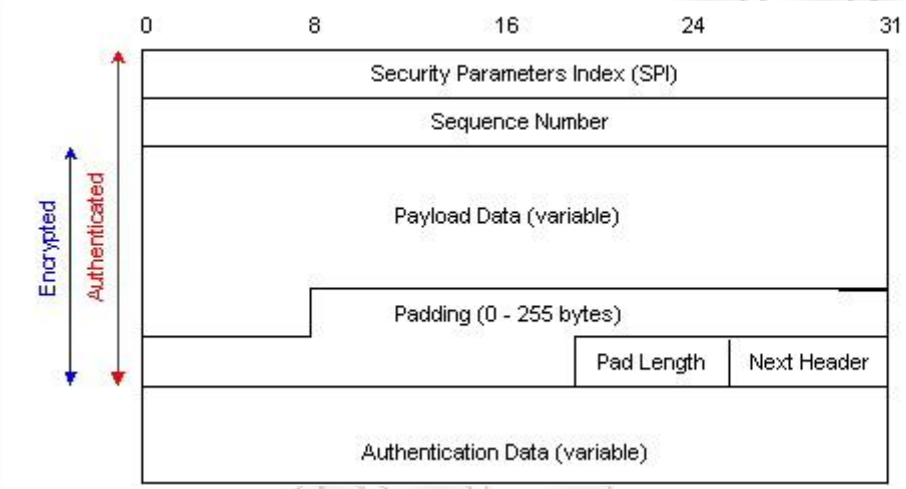
3.4 Οι IPv6 Επικεφαλίδες Ασφαλείας

Το IPv6 χρησιμοποιεί δύο βασικούς μηχανισμούς για να παρέχει τις υπηρεσίες ασφαλείας που αναφέραμε σε προηγούμενη ενότητα και αυτοί είναι οι IP Authentication Header (AH) και IP Encapsulating Security Payload (ESP). Και οι δύο αυτοί μηχανισμοί βασίζονται κυρίως σε εξωτερικούς μηχανισμούς κρυπτογράφησης για να παρέχουν ασφάλεια. Το IPv6 έχοντας λάβει υπόψη του στο σχεδιασμό του όλα τα θέματα ασφαλείας, εναρμονίζεται πλήρως και υποστηρίζει μάλιστα υποχρεωτικά την ομάδα πρωτοκόλλων του IP Security. Έτσι τόσο η επικεφαλίδα Πιστοποίησης όσο και η επικεφαλίδα Ενθυλακωμένου Φορτίου Ασφαλείας έχουν προκαθορισμένη θέση στο πεδίο των επικεφαλίδων επέκτασης (Extention Headers).

3.4.1 Επικεφαλίδα Encapsulating Security Payload (ESP)

Η επικεφαλίδα Encapsulating Security Payload εγγυάται την ακεραιότητα και την ταυτοποίηση των δεδομένων. Είναι σχεδιασμένη έτσι ώστε να επιτρέπει στους κόμβους να ανταλλάσουν τα πακέτα των οποίων τα δεδομένα είναι κωδικοποιημένα. Αν η επικεφαλίδα ESP χρησιμοποιείται για την επικύρωση της ακεραιότητας των δεδομένων τότε δεν περιλαμβάνει τα αμετάβλητα πεδία της IP επικεφαλίδας. Ανάλογα με τις απαιτήσεις ασφάλειας του κάθε χρήστη, ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση είτε ενός τμήματος του επιπέδου μεταφοράς (πχ TCP, UDP, ICMPv6, IGMP) είτε για ένα ολόκληρο IP datagram.
Η επικεφαλίδα ESP χρησιμοποιείται στην πιστοποίηση του αποστολέα με χρήση κωδικοποιήσεων δημοσίου κλειδιού και την μετάδοση των πακέτων με την χρήση πάλι της κωδικοποίησης για λόγους επίτευξης του απόρρητου των δεδομένων. Επίσης παρέχει υπηρεσίες για την προστασία από επιθέσεις τύπου επανάληψης (replay) και τύπου ελέγχου

κίνησης (traffic analysis) μέσω της χρήσης πυλών ασφαλείας (tunnel mode) και με τεχνικές συμπληρώματος (padding) προκειμένου το μέγεθος του πακέτου να μένει κρυφό.
Το ESP υποστηρίζει ένα μεγάλο αριθμό συμμετρικών αλγορίθμων κρυπτογράφησης, αλλά η εξ ορισμού συνηθισμένη προεπιλογή είναι ο αλγόριθμος AES (128-bit). Ωστόσο κάνει συχνή χρήση και άλλων αλγορίθμων όπως για παράδειγμα τον 3DES. Τα πεδία της κεφαλίδας ESP είναι 6 από τα οποία τα δύο τοποθετούνται πριν από το φορτίο του IP πακέτου (ESP Header) και τα υπόλοιπα τέσσερα μετά από αυτό. Τα πεδία SPI και Sequence Number έχουν την ίδια λειτουργία όπως και στην επικεφαλίδα Πιστοποίησης δηλαδή το πρώτο προσδιορίζει στον παραλήπτη ποια πρωτόκολλα ασφαλείας χρησιμοποιήθηκαν από τον αποστολέα και το δεύτερο αυξάνεται κατά ένα για κάθε νέο πακέτο που καταφτάνει στον δέκτη από τον ίδιο αποστολέα και με το ίδιο SPI. Το πεδίο Συμπλήρωσης (Padding) έχει μέγεθος το πολύ 255 bytes και χρειάζεται για να προσαρμόζεται το μέγεθός του IP πακέτου, ανάλογα με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται. Πιο συγκεκριμένα βλέπουμε παρακάτω την δομή του πρωτοκόλλου ESP:



Εικόνα 3.2: Δομή Πρωτοκόλλου ESP-Encapsulating Security Payload
Πηγή: (http://www.securityfocus.com/print/infocus/1616)

Ο μηχανισμός του ESP μπορεί να χρησιμοποιηθεί με δύο τρόπους:

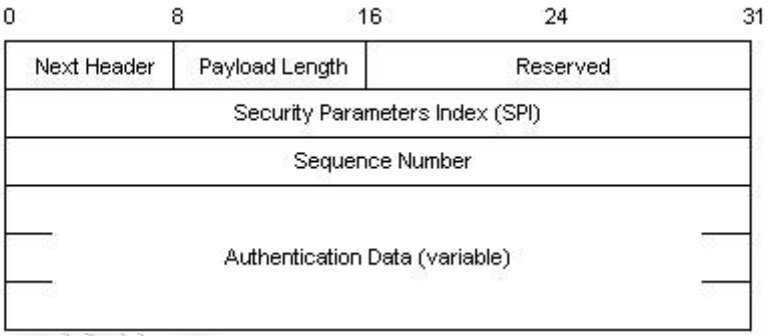
- ***Transport mode (τρόπος μεταφοράς)*** : όπου η επικεφαλίδα ESP χρησιμοποιείται για την απευθείας μετάδοση δεδομένων. Σε αυτήν την περίπτωση η κρυπτογραφημένη πληροφορία περιέχει μόνο το πακέτο του επιπέδου μεταφοράς (Transport TCP/UDP). Δηλαδή την επικεφαλίδα του επιπέδου Transport και τα δεδομένα του χρήστη. Έτσι έχουμε ως αποτέλεσμα την μη προστασία των IP Headers. Εξασφαλίζεται το ασφαλές των δεδομένων, αλλά είναι δυνατή η μελέτη της κυκλοφορίας μεταξύ αποστολέα και παραλήπτη από κάποιον επιτιθέμενο, και έτσι η εξαγωγή συμπερασμάτων που μπορεί να καταλήξει σε παραβίαση της ασφάλειας. Οι αρχικές επικεφαλίδες μένουν ανέπαφες και σε αυτήν την κατάσταση λειτουργίας μεταφοράς έχει το πλεονέκτημα της προσθήκης μόνο μερικών bytes σε κάθε πακέτο.
- ***Tunnel mode (τρόπος διόδου)*** : όπου η επικεφαλίδα χρησιμοποιείται για τη μετάδοση δεδομένων με την χρήση καναλιών. Χρησιμοποιούνται πύλες ασφαλείας και έτσι εξασφαλίζει το γεγονός ότι κανένας μη εξουσιοδοτημένος κόμβος δεν μπορεί να βγάλει

συμπεράσματα για την κυκλοφορία, αφού ολόκληρο το πακέτο είναι κωδικοποιημένο και ενθυλακωμένο σε νέο πακέτο που απευθύνεται στην πύλη. Ο τρόπος αυτός είναι ιδιαίτερα χρήσιμος για την δημιουργία VPN.

3.4.2 Η Επικεφαλίδα Πιστοποίησης (AH-Authentication Header)

Όταν προστίθεται αυτή η επικεφαλίδα σε ένα IP πακέτο, διασφαλίζει τη ακεραιότητα, την πιστοποίηση ταυτότητας των δεδομένων, καθώς και την αποφυγή διπλότυπων πακέτων. Ωστόσο δεν παρέχει ασφάλεια εμπιστευτικότητας. Η υπηρεσία αποφυγής διπλότυπων πακέτων (replay) που είναι μια προαιρετική υπηρεσία, μπορεί να επιλεγεί από τον παραλήπτη, όταν η Συσχέτιση Ασφαλείας είναι εγκατεστημένη. (Παρόλο που το εξ ορισμού αίτημα του αποστολέα για αύξηση του Sequence Number χρησιμοποιείται για την αποφυγή της επανάληψης, η υπηρεσία αυτή είναι αποτελεσματική μόνο εάν ο παραλήπτης ελέγχει το Sequence Number). Η Επικεφαλίδα Πιστοποίησης παρέχει έλεγχο ταυτοποίησης για όσο τον δυνατόν περισσότερες επικεφαλίδες IP, όσο και για δεδομένα πρωτοκόλλων ανωτέρου επιπέδου. Παρόλα αυτά, κάποια πεδία των κεφαλίδων IP μπορεί να τροποποιηθούν κατά την μετάδοσή τους και οι τιμές των πεδίων, όταν το πακέτο φτάνει στον παραλήπτη, μπορεί να μην είναι προβλέψιμες από τον αποστολέα. Οι τιμές αυτών των πεδίων δεν μπορούν να προστατευτούν από το AH. Έτσι η προστασία που παρέχεται στην επικεφαλίδα IP από την κεφαλίδα Πιστοποίησης είναι κάπως αποσπασματική.

Η επικεφαλίδα Πιστοποίησης μπορεί να χρησιμοποιηθεί σε συνδυασμό με την επικεφαλίδα ESP και μάλιστα γενικά προτείνεται η χρήση της για την πιστοποίηση των δεδομένων στη περίπτωση που δεν χρησιμοποιείται άλλος μηχανισμός πιστοποίησης στην επικεφαλίδα ESP. Μπορεί να χρησιμοποιηθεί είτε άμεσα είτε με την δημιουργία καναλιών (tunnels), δηλαδή μπορεί να χρησιμοποιηθεί για να πιστοποιεί τον αποστολέα στις απλές μεταδόσεις πακέτων ή να ενθυλακώνει όλη την ροή των πακέτων που στέλνεται από ή προς μια πύλη ασφαλείας (security gateway). Η δομή της ακολουθεί την μορφή των υπολοίπων επικεφαλίδων IPv6, αρχίζοντας από το πεδίο που περιγράφει την Next Header (Επόμενη Επικεφαλίδα) και συνεχίζοντας με το μήκος της Επικεφαλίδας Πιστοποίησης. Πιο συγκεκριμένα βλέπουμε την παρακάτω εικόνα που μας απεικονίζει την δομή της:



Εικόνα 3.3: Η δομή της Επικεφαλίδας Πιστοποίησης
Πηγή: (http://www.classle.net/bookpage/ip-security)

Τα πεδία της Επικεφαλίδας Πιστοποίησης:

- ***Next Header (Επόμενη Επικεφαλίδα)***: είναι ένα πεδίο 8-bit που προσδιορίζει τον τύπο του επόμενου φορτίου μετά την κεφαλίδα Πιστοποίησης.
- ***Payload Length (Μήκος Φορτίου)***: αυτό το πεδίο των 8-bit καθορίζει το μήκος της επικεφαλίδας Πιστοποίησης στα 32-bit.
- ***Reserved (Δεσμευμένο)***: είναι ένα πεδίο 16-bit δεσμευμένο για μελλοντική χρήση. Θα πρέπει να ρυθμίζεται στην τιμή 0. Αξίζει να σημειώσουμε ότι η τιμή περιλαμβάνεται στον υπολογισμό των δεδομένων Πιστοποίησης, αλλά σε κάθε άλλη περίπτωση αγνοείται από τον παραλήπτη.
- ***Security Parameters Index-SPI (Δείκτης Παραμέτρων Ασφαλείας):*** το SPI πρόκειται για μια αυθαίρετη τιμή των 32 bit που σε συνδυασμό με την διεύθυνση προορισμού IP και με το πρωτόκολλο ασφάλειας AH, προσδιορίζει μοναδικά την Συσχέτιση ασφαλείας (Security Association). Χρησιμοποιείται για να ξεχωρίζει διαφορετικές SA. Η τιμή 0 προορίζεται αποκλειστικά για τοπική χρήση και δεν πρέπει να χρησιμοποιείται στην μετάδοση πακέτων. Οι υπόλοιπες τιμές είναι δεσμευμένες από τον οργανισμό IANA (Internet Assigned Numbers Authority) για χρήση μελλοντικά.
- ***Sequence Number (Αριθμός Ακολουθίας):*** πρόκειται για ένα πεδίο των 32-bit που αυξάνεται κατά ένα από την αρχική του τιμή. Είναι υποχρεωτικό και υπάρχει πάντα ακόμα και αν ο παραλήπτης δεν επιλέξει να είναι διαθέσιμη η υπηρεσία αποφυγής διπλότυπων πακέτων για μια συγκεκριμένη Συσχέτιση Ασφάλειας. Αν ο παραλήπτης διαπιστώσει ίδιο sequence number σε διάφορα πακέτα τα αγνοεί και έτσι αποφεύγονται επιθέσεις τύπου επανάληψης (replay). Σε περίπτωση που ο αριθμός φτάσει το 2^32 τότε δημιουργείται καινούρια Συσχέτιση Ασφαλείας προκειμένου να αποφευχθεί ο κίνδυνος ο παραλήπτης να αγνοεί πακέτα που δεν πρέπει.
- ***Authentication Data (Δεδομένα Πιστοποίησης):*** είναι ένα πεδία μεταβλητού μήκους και περιέχει την Integrity Check Value (ICV) για αυτό το πακέτο. Το πεδίο αυτό πρέπει να είναι ακέραιο πολλαπλάσιο των 32-bits σε μήκος. Το πεδίο αυτό μπορεί να περιλαμβάνει και το πεδίο συμπληρώματος προκειμένου να εξασφαλίζει ότι το μήκος της επικεφαλίδας Πιστοποίησης είναι ακέραιο πολλαπλάσιο των 32 bits (IPv4) ή 64 bits (IPv6). Πρόκειται για το αποτέλεσμα κάποιου κατάλληλου αλγορίθμου Πιστοποίησης.

3.5 Διαχείριση Κλειδιού

Η διανομή και ο καθορισμός των κρυφών κλειδιών γίνεται από την διαχείριση κλειδιών. Η IPsec περιλαμβάνει εκτός από την επεξεργασία των πακέτων μέσω των κεφαλίδων AH και ESP, και πρωτόκολλα ανταλλαγής του κλειδιού. Μετά από εξέταση αρκετών εναλλακτικών λύσεων για την διαχείριση κλειδιού, η IETF επέλεξε αρχικά το ISAKMP/Oakley και τελικά κατέληξε σε μια επέκτασή του, στο IKE (Internet Key Exchange) σαν τρόπο ρύθμισης των συσχετίσεων ασφαλείας για το IPsec. Η IPsec αρχιτεκτονική ορίζει για την διαχείριση κλειδιού δύο τύπους:

- ***Χειροκίνητη Τεχνική (manual)***: αποτελεί την απλούστερη μορφή διαχείρισης στην οποία ο διαχειριστής διαμορφώνει χειροκίνητα τα κλειδιά σε κάθε σύστημα. Οι χειροκίνητες τεχνικές είναι πρακτικές στα μικρά και στατικά περιβάλλοντα αλλά δεν έχουν την δυνατότητα επεκτασιμότητας. Είναι πολύ χρήσιμο για τα VPN δίκτυα.
- ***Αυτόματη Τεχνική (automatic):*** η ευρεία διάδοση και χρήση του IPsec δημιούργησε την ανάγκη για ένα Διαδίκτυο που να είναι επεκτάσιμο, αυτοματοποιημένο και εύκολα διαχειρίσιμο. Ένα αυτόματο σύστημα επιτρέπει την δυναμική δημιουργία κλειδιών για

SA (Security Associations) όταν αυτά απαιτηθούν. Έτσι διευκολύνεται η διαχείριση σε δυναμικά περιβάλλοντα αλλά και σε μεγάλα κατανεμημένα συστήματα.

Στις παρακάτω ενότητες θα εξετάσουμε ξεχωριστά τα πρωτόκολλα διαχείρισης κλειδιού Oakley Key Determination, ISAKMP (Internet Security Association and Key Management Protocol) και IKE (Internet Key Exchange) που αποτέλεσαν τα τρία βασικότερα που στηρίχτηκε τελικά η IETF.

3.5.1 Το Πρωτόκολλο Oakley Key Determination

Το Oakley είναι ένα πρωτόκολλο ανταλλαγής κλειδιού που βασίζεται στον αλγόριθμο Diffie-Hellman με την προσθήκη επιπλέον ασφαλείας. Επίσης είναι γενικό και δεν υπαγορεύει κάποια συγκεκριμένη διαμόρφωση. Ο Diffie-Hellman είναι ένας μηχανισμός ανταλλαγής κλειδιών που αναπτύχθηκε από τους Diffie και Hellman το 1976.

Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές κανάλι. Είναι ένας κρυπτογραφικός αλγόριθμος δημοσίου κλειδιού. Το πρωτόκολλο έχει δύο παραμέτρους-αριθμούς: p και g. Το p είναι ένας πολύ μεγάλος πρώτος αριθμός και το g είναι ένας αριθμός με την ιδιότητα $g^k \neq 1 \bmod p$ για όλους τους k από 1 μέχρι p-2. Τα p,g τα γνωρίζουν όλοι – είναι δημοσίως γνωστά. Υποθέτοντας τώρα ότι δύο χρήστες, ο Α και ο Β, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο Α παράγει μία τυχαία τιμή x και ο Β μία τυχαία τιμή y (όπου τα x,y είναι μικρότερα του p). Τα x,y κρατούνται μυστικά – μόνο ο Α δηλαδή γνωρίζει το x και μόνο ο Β το y. Στη συνέχεια ο Α υπολογίζει τον αριθμό $x' = g^x \bmod p$ και ο Β τον αριθμό $y' = g^y \bmod p$. Κατόπιν, ο ένας στέλνει στον άλλον τις τιμές αυτές. Τέλος, ο Α κάνει τον υπολογισμό $(y')^x = g^{xy} \bmod p$ και ο Β κάνει με την σειρά του τον υπολογισμό $(x')^y = g^{xy} \bmod p$. Συνεπώς και οι δύο υπολογίζουν τον ίδιο αριθμό – ο οποίος θα είναι το μυστικό κλειδί που θα χρησιμοποιήσουν. Η ασφάλεια του πρωτοκόλλου αυτού βασίζεται στο γεγονός ότι ένας επιτιθέμενος, ο οποίος παρακολουθεί το τι ανταλλάσσουν οι Α και Β, δεν μπορεί από τα x΄, y΄ να υπολογίσει το μυστικό κλειδί: για να το κάνει αυτό θα πρέπει να ξέρει είτε το x είτε το y. Όμως, όταν τα p και g είναι πολύ μεγάλα, το να ξέρει κανείς το x΄ ή το y΄ δεν του αρκεί για να βρει το x ή το y.

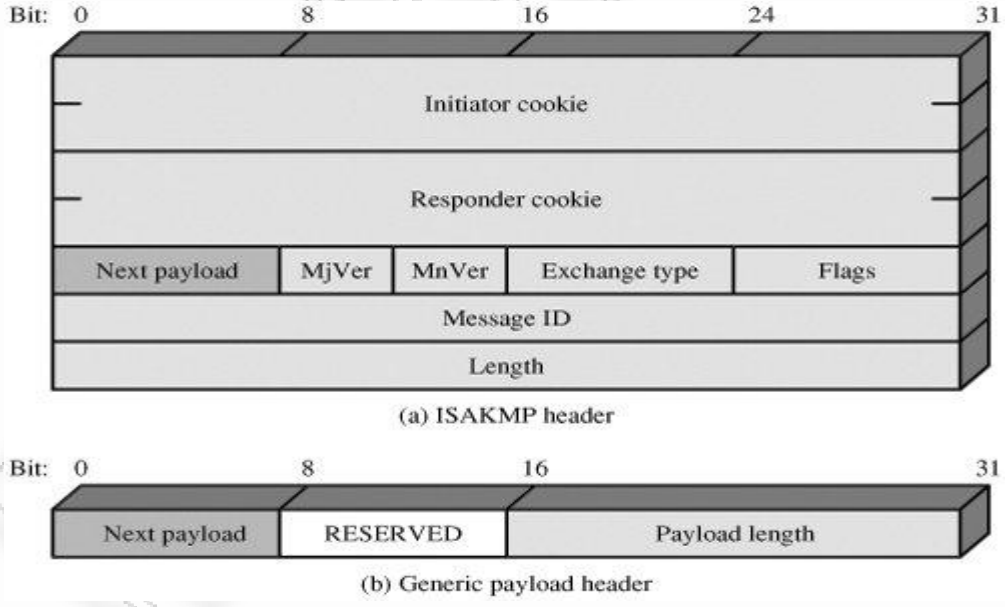
Έτσι ο αλγόριθμος αυτός είναι αρκετά χρήσιμος και ελκυστικός αφού τα μυστικά κλειδιά υπολογίζονται μόνο όταν χρειάζονται και έτσι δεν είναι αναγκαίο να αποθηκεύεται ένα κλειδί για μεγάλο χρονικό διάστημα, πράγμα που θα το καθιστούσε πολύ ευάλωτο σε πιθανές κακόβουλες ενέργειες. Ένα επιπλέον πλεονέκτημα είναι το γεγονός ότι δεν χρειάζεται καμία άλλη υποδομή πέραν από τις δημόσια γνωστές παραμέτρους g και p. Το πρωτόκολλο Oakley διατηρώντας αυτά τα πλεονεκτήματα του αλγορίθμου χρησιμοποιεί επίσης πεδία μίας χρήσης για να αποτρέψει επιθέσεις τύπου επανάληψης.

Ωστόσο υπάρχουν και αδύναμα σημεία στον αλγόριθμο , όπως ότι είναι ευάλωτος σε επιθέσεις τύπου clogging όπου ο επιτιθέμενος ζητάει έναν μεγάλο αριθμό κλειδιών οπότε αυτόματα ο αλγόριθμος γίνεται υπολογιστικά βαρύς και σε επιθέσεις τύπου man-in-the-middle. Μια πιο περίπλοκη επίθεση όπου ο κακόβουλος χρήστης κατά την ανταλλαγή των κλειδιών υποκλέπτει τα μηνύματα των χρηστών Α και Β και στέλνει ακόλουθα μηνύματα και στους δύο χρήστες προσποιούμενος τους ίδιους κατά την επικοινωνία τους και έτσι καταφέρνει να διαπραγματευτεί το κλειδί και να παρακολουθήσει όλη την διάρκεια της επικοινωνίας των δύο χρηστών-θυμάτων. Για το λόγο όμως αυτό έχουν μπει οι κατάλληλες δικλίδες ασφαλείας, όπου στην μεν πρώτη επίθεση χρησιμοποιείται ο μηχανισμός cookies και στο μεν δεύτερο πραγματοποιείται πιστοποίηση ανταλλαγής μηνυμάτων.

3.5.2 Το πρωτόκολλο ISAKMP

Το πρωτόκολλο ISAKMP (Internet Security Association and Key Management Protocol) συνδυάζει τις έννοιες της ασφάλειας της γνησιότητας, της διαχείρισης κλειδιών, και των σχέσεων ασφαλείας προκειμένου να καθορίζει την ασφάλεια των κυβερνητικών, εμπορικών και ιδιωτικών επικοινωνιών που γίνονται μέσω του διαδικτύου. Το ISAKMP ορίζει συγκεκριμένες διαδικασίες και τύπους πακέτων για την εγκαθίδρυση, διαπραγμάτευση, τροποποίηση και διαγραφή των Security Associations (SA). Το SA περιέχει όλη την απαιτούμενη πληροφορία για την εκτέλεση διαφόρων υπηρεσιών ασφαλείας δικτύων, όπως οι υπηρεσίες επιπέδου IP (όπως η επικεφαλίδα Πιστοποίησης και το Encapsulation φορτίο), μεταφοράς ή επιπέδου εφαρμογής, ή αυτοπροστασίας της κίνησης διαπραγμάτευσης. Το ISAKMP καθορίζει τα ωφέλιμα φορτία για την δημιουργία της ανταλλαγής των κλειδιών και πιστοποίησης των δεδομένων. Μπορεί ωστόσο να χρησιμοποιηθεί και σε συνδυασμό με άλλα πρωτόκολλα εγκαθίδρυσης κλειδιών όπως το Oakley που περιγράψαμε στην προηγούμενη ενότητα. Αυτοί οι τύποι παρέχουν ένα συνεκτικό πλαίσιο για την μεταφορά των κλειδιών και την πιστοποίηση των δεδομένων που είναι ανεξάρτητοι από την τεχνική δημιουργίας των κλειδιών, αλγόριθμο κρυπτογράφησης και μηχανισμό πιστοποίησης.

Το ISAKMP εισάγει την έννοια του “cookie” , προκειμένου να αποτρέψει επιθέσεις τύπου clogging που αναφέραμε στην παραπάνω ενότητα, και ταυτόχρονα να μην ξοδεύει μεγάλο αριθμό πόρων για τον καθορισμό της ταυτότητας. Ένα μήνυμα ISAKMP αποτελείται από την επικεφαλίδα ISAKMP ακολουθούμενη από ένα ή περισσότερα φορτία (payload). Μια σταθερή επικεφαλίδα, απλοποιεί τη ανάλυση, παρέχει το πλεονέκτημα του λογισμικού ανάλυσης του πρωτοκόλλου το οποίο είναι λιγότερο πολύπλοκο και πιο εύκολο να εφαρμοστεί. Παρακάτω παρουσιάζουμε την δομή της επικεφαλίδας ISAKMP:



Εικόνα 3.4: Η δομή της επικεφαλίδας ISAKMP
Πηγή: (http://flylib.com/books/en/3.190.1.139/1/)

Η επικεφαλίδα ISAKMP αποτελείται από τα εξής πεδία:

- ***Intiator Cookie (Κουπόνι Αρχικοποίησης)*** : είναι ένα πεδίο των 64 bits και αποτελεί την οντότητα cookie από όπου ξεκίνησε την εγκαθίδρυση, την ενημέρωση ή την διαγραφή της SA.
- ***Responder Cookie (Κουπόνι Απόκρισης) :*** είναι ένα πεδίο των 64 bits και αποτελεί την οντότητα cookie που απαντά στην εγκαθίδρυση, την ενημέρωση ή την διαγραφή της SA
- ***Next Payload (Επόμενο φορτίο):*** είναι ένα πεδίο των 8 bits και καθορίζει τον τύπο του πρώτου φορτίου στο μήνυμα.
- ***Major Version (Βασική Έκδοση):*** είναι ένα πεδίο των 4 bits και καθορίζει την βασική έκδοση του πρωτοκόλλου ISAKMP που χρησιμοποιείται. Οι υλοποιήσεις που είναι βασισμένες σε αυτήν την έκδοση του ISAKMP θα πρέπει να έχουν ως αριθμό βασικής έκδοσης τον αριθμό 1, ενώ αυτές που είναι βασισμένες στην προηγούμενη έκδοση τον αριθμό 0. Οι υλοποιήσεις δεν θα πρέπει ποτέ να δέχονται τα πακέτα όπου η τιμή βασική τους έκδοσης είναι μεγαλύτερη από την δική τους.
- ***Minor Version (Δευτερεύον Αριθμός Έκδοσης):*** είναι πεδίο των 4 bits και καθορίζει το δευτερεύοντα αριθμό της έκδοσης του ISAKMP πρωτοκόλλου που χρησιμοποιείται. Όπως και στην τιμή βασική έκδοσης δεν θα πρέπει να δέχονται πακέτα όπου το πεδίο αυτό έχει μεγαλύτερη τιμή από την δική τους, με δεδομένο ωστόσο ότι οι βασικοί αριθμοί έκδοσης είναι οι ίδιοι.
- ***Exchange Type (Τύπος Ανταλλαγής):*** είναι πεδίο 8 bits και ορίζει τον τύπο της ανταλλαγής που χρησιμοποιείται. Αυτό υπαγορεύει το μήνυμα και το ωφέλιμο φορτίο στις ανταλλαγές ISAKMP.
- ***Flags (Σημαίες):*** πεδίο των 8 bits που καθορίζει τις συγκεκριμένες επιλογές που έχουν οριστεί κατά την ανταλλαγή ISAKMP. Χρησιμοποιούνται μόνο τα τρία λιγότερο σημαντικά bits τα οποία είναι το Encryption bit που καθορίζει αν τα φορτία που ακολουθούν την επικεφαλίδα είναι κωδικοποιημένα ή όχι, το Commit bit που χρησιμοποιείται για τον συγχρονισμό ανταλλαγής κλειδιού έτσι ώστε η πληροφορία που έχει κωδικοποιηθεί να μην μπορεί να ληφθεί προτού η Συσχέτιση Ασφαλείας εγκατασταθεί και το Authentication Only Bit που χρησιμοποιείται έτσι ώστε να επιτρέψει την μετάδοση της πληροφορίας με έλεγχο ακεραιότητας. Συνήθως αυτή η πληροφορία δεν είναι κωδικοποιημένη.
- ***Message ID (Αναγνωριστικό μηνύματος):*** πεδίο των 32 bits χρησιμοποιείται για να προσδιορίσει την κατάσταση του πρωτοκόλλου ISAKMP κατά την διάρκεια των διαπραγματεύσεων. Μοναδικό ID για αυτό το μήνυμα.
- ***Length (Μήκος):*** πεδίο των 32 bits που δείχνει το μήκος ολόκληρου του μηνύματος (επικεφαλίδας και των φορτίων) σε bytes.

Οι πέντε προκαθορισμένοι τύποι ανταλλαγής μηνύματος που υποστηρίζει το πρωτόκολλο ISAKMP είναι η Βασική ανταλλαγή (Based) για ταυτόχρονη μετάδοση ανταλλαγής κλειδιού, η ανταλλαγή Προστασίας Ταυτότητας (Identity Protection Exchange) που αποτελεί επέκταση της Βασικής, την Επιθετική ανταλλαγή (Aggressive Exchange) όπου ελαχιστοποιεί τον αριθμό των ανταλλασσόμενων μηνυμάτων και τέλος την Πληροφοριακή ανταλλαγή (Informational Exchange) για την μετάδοση πληροφορίας στην μια κατεύθυνση. Έτσι το ISAKMP παρέχει ένα ευέλικτο και επεκτάσιμο πλαίσιο για την δημιουργία και διαχείριση της SA και των κρυπτογραφικών κλειδιών.

3.5.3 Internet Key Exchange (IKE)

Το Internet Key Exchange (IKE) αποτελεί επέκταση των παραπάνω πρωτοκόλλων που περιγράψαμε και δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι μεταξύ δύο οντοτήτων και έπειτα διαπραγματεύεται τις συσχετίσεις ασφαλείας για το IPsec. Αυτή η διαδικασία προβλέπει από τις δύο αυτές οντότητες αφού πιστοποιήσουν η μία την άλλη κατόπιν να κάνουν ανταλλαγή των κλειδιών τους. Αποτελεί το βασικό πρωτόκολλο διαχείρισης το οποίο χρησιμοποιείται σε συνδυασμό με το πρότυπο IPsec. Το IPsec μπορεί να ρυθμιστεί χωρίς το Internet Key Exchange, αλλά το IKE ενισχύει σημαντικά το IPsec παρέχοντας του συμπληρωματικά χαρακτηριστικά, ευελιξία και ευκολία διαμόρφωσης του προτύπου IPsec. Σχεδιάστηκε για την υποστήριξη αυτοματοποιημένων διαπραγματεύσεων των SA και αυτοματοποιημένης δημιουργίας και ανανέωσης κρυπτογραφικών κλειδιών.

Το IKE διαπραγματεύεται απευθείας τις Συσχετίσεις Ασφαλείας του IPsec και δίνει την δυνατότητα στο IPsec για ασφαλής επικοινωνίες χωρίς προ-ρυθμίσεις κάτι που θα επιβάρυνε με επιπλέον κόστος. Πιο συγκεκριμένα το IKE προσφέρει τις εξής παροχές:

- Καταργεί την ανάγκη χειροκίνητης ρύθμισης όλων των IPsec παραμέτρων ασφαλείας και στις δύο οντότητες που επικοινωνούν
- Επιτρέπει τον καθορισμό της διάρκειας ζωής της Συσχέτισης Ασφαλείας του IPsec
- Επιτρέπει την αλλαγή των κλειδιών κρυπτογράφησης κατά την διάρκεια των διαπραγματεύσεων στο IPsec
- Επιτρέπει στο IPsec να παρέχει μηχανισμούς αντιμετώπισης επιθέσεων τύπου επανάληψης
- Παρέχεται από την Αρχή Πιστοποίησης (CA-Certification Authority) υποστήριξη για μια εύχρηστη, και επεκτάσιμη IPsec εφαρμογή
- Επιτρέπει την δυναμική πιστοποίηση της γνησιότητας των οντοτήτων επικοινωνίας

Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μιας συγκεκριμένης διαδικασίας. Έτσι οι μέθοδοι που χρησιμοποιεί το πρωτόκολλο IKE για την εξακρίβωση γνησιότητας είναι οι παρακάτω:

- ***Προ-διαμοιρασμένα Κλειδιά (Pre-Shared Key)***: Το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας συνάρτησης κατακερματισμό) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.
- ***Ψηφιακές Υπογραφές (Digital Signatures-με DSS και RSA)***: Κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Ο αποστολέας χρησιμοποιεί το κρυφό του ιδιωτικό κλειδί για να υπογράψει ηλεκτρονικά τα δεδομένα του. Ο αποδέκτης του κειμένου χρησιμοποιεί το δημόσιο κλειδί του αποστολέα, το οποίο έτσι και αλλιώς γνωρίζει αφού είναι δημόσιο, για να ελέγξει την υπογραφή του αποστολέα. Αν αυτός ο έλεγχος είναι επιτυχής, αυτό σημαίνει ότι το κείμενο δεν έχει αλλαχθεί και έχει πιστοποιηθεί η ταυτότητα του αποστολέα Υποστηρίζονται τόσο ο

αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών DSS.

- ***Κρυπτογράφηση Δημοσίων Κλειδιών (Public Keys Encryption με RSA και revised RSA)***: Κάθε μηχανή παράγει έναν ψεύδοτυχαίο αριθμό τον οποίο και κρυπτογραφεί με το δημόσιο κλειδί της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια συνάρτηση κατακερματισμού του τυχαίου αριθμού, αποκρυπτογραφώντας με τα ιδιωτικά κλειδιά ό,τι λαμβάνουν από το συνομιλητή τους. Υποστηρίζεται μόνο ο αλγόριθμος δημοσίων κλειδιών RSA.

3.6 Εφαρμογές των χαρακτηριστικών ασφάλειας του IPv6

Οι επικεφαλίδες Authentication Header (AH) και Encapsulating Security Payload (ESP) μπορούν να χρησιμοποιηθούν με διάφορους τρόπους προκειμένου να παρέχουν ασφάλεια στις IP επικοινωνίες. Παρακάτω θα αναφέρουμε εν συντομία ορισμένες από τις πιο ενδιαφέρουσες εφαρμογές με παραπομπές στις αντίστοιχες αδυναμίες που παρουσίαζαν τα χαρακτηριστικά ασφαλείας του πρωτοκόλλου IPv4.

3.6.1 VPN (Εικονικά Ιδιωτικά Δίκτυα)

Την σημερινή εποχή, τεχνικοί και οικονομικοί λόγοι ωθούν τις εφαρμογές εταιρικών δικτύων ευρείας ζώνης να μεταβούν από τους ειδικές συνδέσεις και τις ιδιωτικές τεχνολογίες δικτύου σε λύσεις βασισμένες σε κοινές δημόσιες συνδέσεις και αρχιτεκτονικές ανοιχτού δικτύου. Αυτή μετάβαση δημιουργεί πολλά πλεονεκτήματα αλλά σήμερα παρουσιάζει ένα σοβαρό μειονέκτημα. Υπάρχει μια δραστική μείωση των εγγενών συστημάτων ασφαλείας, λόγω της χρήσης των κοινών σταθμών και συσκευών. Για να επανακτήσει το προηγούμενο επίπεδο ασφάλειας δικτύου, διατηρώντας παράλληλα τα οικονομικά πλεονεκτήματα που προσφέρονται από τα δημόσια δίκτυα, ένας οργανισμός πρέπει να πετύχει τον διαχωρισμό και την προστασία των δικών του δεδομένων στα πακέτα εντός του πλήθους των πακέτων που μεταδίδονται σε όλες τις δημόσιες συνδέσεις. Συνήθως, αυτό επιτυγχάνεται με την εγκατάσταση ενός Εικονικού Ιδιωτικού Δικτύου (VPN-Virtual Private Network). Στο IPv4 αυτό επιτυγχάνεται με την χρησιμοποίηση της τεχνικής tunneling IP, όπου σύμφωνα με αυτήν τα πακέτα IP που πρέπει να μένουν προστατευμένα, είναι μέσα σε ένα φάκελο ασφαλείας και ενθυλακωμένα μέσα σε κανονικά IP πακέτα που χρησιμοποιούνται για την μεταφορά των αρχικών πακέτων διαμέσου του δημόσιου δικτύου στον τελικό τους προορισμό. Συνήθως τα τελικά σημεία μίας σήραγγας δεν είναι δύο κόμβοι που θέλουν απλώς να ανταλλάξουν δεδομένα αλλά δύο firewalls που προστατεύουν το δίκτυο από εξωτερικές επιθέσεις.

Στο IPv6 η διαδικασία δημιουργίας ενός VPN είναι πιο εύκολη και πιο καθορισμένη από ότι στο IPv4 χάρης στις επικεφαλίδες AH και ESP. Αυτές χρησιμοποιούνται από τους κόμβους στα όρια ενός τοπικού δικτύου οι οποίοι έχουν αναλάβει να εξετάζουν τα εισερχόμενα πακέτα και να δημιουργούν ουσιαστικά το εικονικό ιδιωτικό δίκτυο. Ακόμα όμως και η χρήση της επικεφαλίδας AH σε συνδυασμό με αυτή της ESP δεν προστατεύει πλήρως την κίνηση. Μπορεί να διαγραφούν πακέτα από ενδιάμεσους κόμβους ή να καταγραφούν και μετέπειτα να επαναληφθούν. Αυτού του είδους οι επιθέσεις δεν είναι εύκολο να αποφευχθούν σε επίπεδο IP. Οι κατάλληλες άμυνες (όπως η χρήση των μοναδικών αναγνωριστικών πακέτων και η δημιουργία των “heartbeat” πακέτων) σε τέτοιου τύπου επιθέσεις συνήθως εφαρμόζονται και

υπάρχουν στα ανώτερα στρώματα της στοίβας του δικτύου. Μια κάποια λύση σε επίπεδο IP μπορεί να προσφερθεί από την νέα δομή και τους αλγορίθμους που πρόκειται να αντικαταστήσουν την υφιστάμενη AH επικεφαλίδα.

Η εφαρμογή του πρωτοκόλλου IPv6 στα Εικονικά Ιδιωτικά Δίκτυα υπερτερεί έναντι του IPv4, καθώς το τελευταίο δεν επιτρέπει την χρησιμοποίηση πολλαπλών επικεφαλίδων και το tunnel πρέπει να υλοποιηθεί με την εφαρμογή της ενθυλάκωσης. Αυτό προκαλεί σημαντικό πρόβλημα στην συμβατότητα μεταξύ των διαφορετικών firewall των τοπικών δικτύων που βρίσκονται στα άκρα της σήραγγας όπως επίσης και σημαντικά προβλήματα κατακερματισμού των πακέτων. Αυτό ερμηνεύεται από το γεγονός του ότι στη περίπτωση που το μέγεθος του πακέτου υπερκαλύπτει τον περιορισμό της MTU, δηλαδή βρίσκεται ήδη στο μέγιστο μέγεθος που ορίζει η IP, δεν υπάρχει η δυνατότητα ενθυλάκωσής του σε άλλο πακέτο και άρα πρέπει να κατακερματιστεί σε μικρότερα κομμάτια. Ο κατακερματισμός και η επανασυναρμολόγηση του πακέτου πρέπει να γίνεται στα δύο άκρα της σήραγγας. Κατά συνέπεια, έχουμε σημαντική μείωση της απόδοσης του εικονικού καναλιού έως και 50% της κανονικής ροής κίνησης. Η χειρότερη περίπτωση συμβαίνει στα μεγαλύτερα πακέτα, τα οποία συνήθως χρησιμοποιούνται για την μετάδοση μεγάλων δεδομένων, που αντιθέτως δεν θα χρειαστεί κατακερματισμός για να πετύχουν μέγιστη ταχύτητα κίνησης.

Στο IPv6 αντίθετα, έχουμε εντελώς διαφορετική κατάσταση μιας και η επικεφαλίδα έχει σταθερό μέγεθος και είναι ανεξάρτητη από την διάσταση του αρχικού πακέτου. Αυτό έχει ως αποτέλεσμα να αυξάνει σημαντικά η απόδοσή της για πακέτα με μεγάλο μέγεθος.

3.6.2 Ασφάλεια στο επίπεδο-εφαρμογών και δρομολόγησης

Δικτυακές εφαρμογές που εκτελούνται μέσω του πρωτοκόλλου IPv6 μπορεί να απαιτήσουν την χρήση καναλιού επικοινωνίας με χαρακτηριστικά πλήρως καθορισμένα. Για να αποφευχθεί η επικάλυψη λειτουργιών και κατά συνέπεια μείωση της απόδοσης, θα πρέπει να είναι σε θέση να προσδιορίσει τα χαρακτηριστικά ασφαλείας του επιπέδου μεταφοράς. Αυτό επιτυγχάνεται με την χρήση των κατάλληλων κλήσεων, όπως για παράδειγμα στην πρώτη εφαρμογή του BSD-UNIX του IPv6, έγινε χρήση της συνάρτησης setsocketoption(). Ωστόσο αυτή η λύση δεν καλύπτει απόλυτα σε ασφάλεια το επίπεδο-εφαρμογών μιας και επιτυγχάνεται προστασία μόνο έως ένα βαθμό. Η επικεφαλίδα AH παρέχει μόνο πιστοποίηση του τερματικού σταθμού ενώ από την άλλη οι εφαρμογές απαιτούν συνήθως επιπρόσθετη πιστοποίηση του χρήστη της εφαρμογής.

Οι επικεφαλίδες Πιστοποίησης και ESP παρέχουν προστασία στα δεδομένα μόνο κατά την μετάδοσή τους στο κανάλι. Αφότου τα δεδομένα παραληφθούν, οι επικεφαλίδες παύουν να παρέχουν προστασία και αφαιρούνται από το επίπεδο του δικτύου. Το γεγονός αυτό δεν θα αποτελούσε μειονέκτημα εάν ο κόμβος που παρελάμβανε τα δεδομένα ήταν ασφαλής. Ωστόσο υπάρχει μια πρόσθετη συνέπεια στο ότι η αρχική πιστοποίηση και οι ιδιότητες της ακεραιότητας των δεδομένων θα χάνονταν από την στιγμή που τα δεδομένα θα έφευγαν από το ασφαλές κανάλι. Μπορούμε έτσι να εξάγουμε το συμπέρασμα ότι τα χαρακτηριστικά ασφαλείας του IPv6 δεν εξαλείφουν την ανάγκη για άλλους μηχανισμούς ασφαλείας, οι οποίοι πιθανόν να παρέχουν και μεγαλύτερη ασφάλεια σε επίπεδο εφαρμογών.

Επειδή οι διευθύνσεις IPv6 ορίζονται δυναμικά αρκετά συχνά, έχει πολύ μεγάλη σημασία η διαδικασία αυτή να γίνεται με ασφαλή τρόπο. Επιπλέον, καθώς είναι διαθέσιμες πολλές διαφορετικές ιδιότητες ασφαλείας που προκύπτουν από τον συνδυασμό των επικεφαλίδων AH και ESP, είναι ιδιαίτερα επιθυμητό να εφαρμόζονται στα μηνύματα που ανταλλάσσονται μέσω των δρομολογητών έτσι ώστε να προστατεύονται από επιθέσεις που σκοπό έχουν να

ανατρέψουν την λογική της αρχιτεκτονικής του δικτύου. Οι τύποι των επικοινωνιών που θα πρέπει να προστατευτούν φαίνονται στον ακόλουθο πίνακα:

Τύποι Μηνυμάτων	Περιγραφή
ICMP μηνύματα	Σχετίζονται με ένα απρόσιτο κόμβο, αδυναμία εύρεσης κόμβου ή δικτύου, ή με λειτουργίες εύρεσης καλύτερης δρομολόγησης, ώστε να εξασφαλίζεται ότι αυτά τα μηνύματα προέρχονται από κόμβους ή δρομολογητές που βρισκόντουσαν στην αρχική διαδρομή των πακέτων που στάλθηκαν.
Routing Advertisement	Για να διασφαλίζεται ότι προήλθαν από εξουσιοδοτημένο δρομολογητή.
Neighbor Advertisement	Για να διασφαλιστεί ότι προέρχονται από εξουσιοδοτημένους κόμβους και να αποφευχθεί ο κίνδυνος κάποιος μη εξουσιοδοτημένος χρήστης να εισάγει σε ένα δίκτυο τερματικούς σταθμούς χωρίς την κατάλληλη εξουσιοδότηση.

Πίνακας 3.1 Τύποι των μηνυμάτων που ανταλλάσουν οι δρομολογητές και χρήζουν προστασίας

Η διασφάλιση αυτών των τύπων μηνυμάτων έχουν μεγάλη σημασία. Για παράδειγμα οι δρομολογητές διαφήμισης (routing advertisements) στέλνουν σε multicast ομάδες και ως εκ τούτου όλοι οι δρομολογητές της ομάδας πρέπει να γνωρίζουν το κοινό-μυστικό κλειδί που θα χρησιμοποιηθεί για την επαλήθευση και αποκρυπτογράφηση των μηνυμάτων. Με την σειρά του το γεγονός αυτό σημαίνει ότι μπορούν να «πλαστογραφήσουν» και να προσποιηθούν οποιοδήποτε δρομολογητή της ομάδας. Έχουν δοθεί λύσεις πάνω σ αυτά έχοντας δώσει προτεραιότητα στην φάση της ανάθεσης διεύθυνσης και στο δημόσιο κλειδί πιστοποίησης. Σε κάθε κόμβο εκχωρείται ένα ζεύγος κλειδιών, ιδιωτικού και δημόσιου κλειδιού, και θα πρέπει να έχουν διαμορφωθεί με το δημόσιο κλειδί που υπογράφει η αρχή πιστοποίησης για τους δρομολογητές και τα κέντρα διανομής διεύθυνσης.

Όσον αφορά την ασφάλεια των μηνυμάτων που χρησιμοποιούνται από τα διάφορα πρωτόκολλα δρομολόγησης, θα πρέπει να ανταλλάσσονται μόνο εντός του πλαισίου της Συσχέτισης Ασφάλειας και να προστατεύονται με την βοήθεια της επικεφαλίδας Πιστοποίησης. Χάριν γενικότητας, θα μπορούσαμε να πούμε ότι για αυτή τη λύση είναι προτιμότερο να χρησιμοποιούν μηχανισμούς αυθεντικοποίησης συγκεκριμένα για κάθε πρωτόκολλο δρομολόγησης. Γενικά θα πρέπει να αναφέρουμε ότι τα προβλήματα δρομολόγησης παραμένουν ακόμα ως πρόβλημα και στο πρωτόκολλο IPv6 αλλά σε πολύ μικρότερο βαθμό από ότι στο IPv4 και με περισσότερους τρόπους αντιμετώπισης και επίλυσης.

Κεφάλαιο 4

Η Διασφάλιση των Μηχανισμών Μετάβασης

4.1 Η κατανόηση των μηχανικών μετάβασης από το IPv4 στο IPv6

Η μετάβαση στο πρωτόκολλο IPv6 ήταν και θα παραμείνει για πολύ καιρό ακόμα μια χρονοβόρα διαδικασία. Το IPv6 και το IPv4 πρέπει να συνυπάρξουν για πολλά χρόνια ακόμα πριν το πρωτόκολλο IPv4 αντικατασταθεί πλήρως. Η IETF (Internet Engineering Task Force) έχει αναπτύξει πολλούς μηχανισμούς, μεταξύ άλλων σήραγγες (tunnels) και πρωτόκολλα μετάφρασης, για να είναι δυνατή η επικοινωνία κατά την διάρκεια αυτής της φάσης μετάβασης που εκτιμάται ότι θα διαρκέσει αρκετά χρόνια ακόμα μιας και δεν έχει οριστεί η αρχική και η τελική ημερομηνία υλοποίησης της μετάβασης.

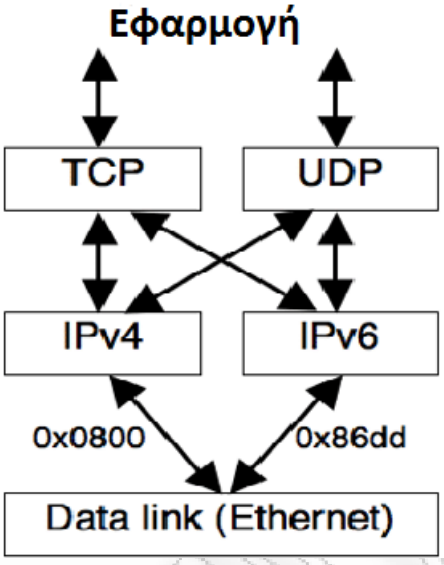
Τρεις είναι οι τεχνικές μετάβασης και είναι οι εξής παρακάτω:

- ***Dual Stack (Διπλής Στοίβας)***: Οι κόμβοι του δικτύου υλοποιούν και τις δύο στοίβες των εκδόσεων του πρωτοκόλλου και έτσι επιτυγχάνεται end-to-end επικοινωνία τόσο σε επίπεδο IPv6 όσο και σε επίπεδο IPv4.
- ***Tunnels (σήραγγες)***: Κόμβοι-υποδοχής ή δρομολογητές στέλνουν και λαμβάνουν IPv6 πακέτα χρησιμοποιώντας ένα επικαλυπτόμενο δίκτυο από tunnels πάνω από ένα IPv4 δίκτυο ή πάνω από ένα μονοπάτι μεταγωγής ετικέτας (LSP-Label Switched Path)
- ***Protocol translation (πρωτόκολλο μετάφρασης)***: Το πρωτόκολλο μετάφρασης λειτουργεί σαν ενδιάμεσος μεταξύ των δικτύων IPv4 και IPv6

Κάθε μία από τις προαναφερθέντες τεχνικές έχει τις δικές της περιπτώσεις χρήσεις όπως επίσης και τις δικές τις αδυναμίες ασφάλειας τις οποίες θα τονίσουμε στην παρούσα ενότητα εκτενώς μιας και αποτελεί σημείο αναφορά για την γενικότερα ασφάλεια του πρωτοκόλλου IPv6. Συνεπώς η εκτενής αναφορά και η εκτίμηση ενδεχόμενων κινδύνων ασφαλείας κρίνεται επιτακτική στα πλαίσια της παρούσας μεταπτυχιακής εργασίας.

4.1.1 Ο Μηχανισμός Διπλής Στοίβας (Dual-Stack)

Όπως αναφέραμε και προηγουμένως οι μηχανισμοί διπλής στοίβας χρησιμοποιούνται από τους κόμβους για IPv6 επικοινωνία πάνω από IPv4 υποδομή. Επειδή συνήθως μία από τις δύο εκδόσεις του πρωτοκόλλου IP εμφανίζεται να είναι πιο διαδεδομένη από την άλλη, τις πιο πολλές φορές αυτή η έκδοση χρησιμοποιείται συμβατικά κάτι που σημαίνει ότι εγκαθίσταται πάνω από το φυσικό interface, δηλαδή ISDN ή Ethernet, ενώ προκειμένου να καταφέρει να επικοινωνήσει με την άλλη έκδοση του IP πρωτοκόλλου η τεχνική dual-stack πολλές φορές συνδυάζεται με κάποια τεχνική tunneling.Στην παρακάτω εικόνα παρουσιάζουμε τον μηχανισμό μετάβασης της Διπλής στοίβας:

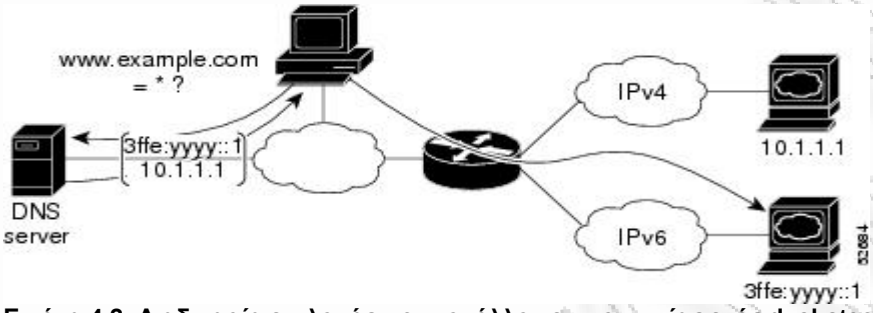


Εικόνα 4.1: Ο μηχανισμός Μετάβασης Διπλής Στοίβας(Dual-Stack)
Πηγή: (http://www.eetimes.com/design/other/4014747/Transition-IPv6-seamlessly-in-embedded-systems-item-1?pageNumber=1)

Η εικόνα 4.1 παρουσιάζει την προτεινόμενη τεχνική μετάβασης μεταξύ των πρωτοκόλλων IPv4 και IPv6, που είναι ασφαλώς η τεχνική της Διπλής Στοίβας. Όλοι οι κόμβοι, και οι clients και οι servers, όπως επίσης και οι συσκευές δικτύου τρέχουν όμοια και στις IPv4 και στις IPv6 στοίβες. Και οι δύο εκδόσεις του πρωτοκόλλου IP μπορούν να συνυπάρξουν στο ίδιο δίκτυο επειδή και οι δύο έχουν ένα συγκεκριμένο Επίπεδο 2 τύπου Ethernet, 0x0800 για το IPv4 και 0x86dd για το IPv6. Η τιμή στο πεδίο Τύπος για το Ethernet πληροφορεί τον κόμβο για το ποιο πρωτόκολλο Επιπέδου 3 ακολουθεί στο πλαίσιο Ethernet. Πάνω από το Data link επίπεδο, υπάρχουν δύο πρωτόκολλα για το επίπεδο δικτύου. Στην κορυφή του επιπέδου δικτύου, τα πρωτόκολλα μεταφοράς, UDP-User Datagram Protocol ή το πρωτόκολλο μετάδοσης TCP-Transmission Control Protocol, παραμένουν αμετάβλητα και τρέχουν πανομοιότυπα πάνω από το IPv4 και το IPv6. Στην κορυφή, οι εφαρμογές συνήθως δεν γνωρίζουν το βασικό επίπεδο δικτύου, εκτός του ότι κάνουν logging την απομακρυσμένη IP διεύθυνση ή πιστοποίηση που βασίζονται στις IP διευθύνσεις.

Ένα μικρό μειονέκτημα της λειτουργίας dual-stack είναι η αυξημένη κατανάλωση μνήμης στους δρομολογητές μιας και χρειάζονται να έχουν δύο πίνακες δρομολόγησης καθώς επίσης και μια μικρή αύξηση της CPU στους δρομολογητές (δύο πρωτόκολλα δρομολόγησης συνήθως απαιτούν: ένα για το IPv4 και ένα για το IPv6) ή στους πυρήνες των κόμβων. Όμως αντίθετα ένα από τα δυνατά χαρακτηριστικά των μηχανισμών αυτών είναι η απλότητα στην υλοποίηση τους. Το μόνο που προϋποθέτει είναι εγκατάσταση των δύο πρωτοκόλλων IP στα λειτουργικά συστήματα των μηχανημάτων του δικτύου και έτσι μπορούν να λάβουν αλλά και να προωθήσουν πακέτα και από τα δύο πρωτόκολλα. Στο σημείο αυτό το DNS δηλαδή η υπηρεσία Ονοματολογίας κάνει την επιλογή της στοίβας που θα χρησιμοποιηθεί, δηλαδή αν ο κόμβος με τον οποίο θα επικοινωνήσει έχει αποκλειστικά μόνο IPv6 διεύθυνση, θα χρησιμοποιηθεί η IPv6 στοίβα ενώ σε αντίθετη περίπτωση η IPv4 στοίβα. Στην περίπτωση όμως που ο κόμβος έχει και IPv4 και IPv6 εγγραφές τότε η προεπιλογή που υπάρχει καθιστά να χρησιμοποιηθεί το IPv6

όπως μπορούμε να δούμε και από την εικόνα 4.2. Για να γίνει όμως αυτό θα πρέπει να παρέχεται και με κάποια τεχνική (είτε native ή tunneling) η IPv6 συνδεσιμότητα ώστε να εγγράψει ο κόμβος την IPv6 σύνδεσή του. Για την υπηρεσία Ονοματολογίας έχει εισαχθεί ένα νέο είδος εγγραφής για τη βάση του DNS, η A6 εγγραφή η οποία αποτελεί επέκταση της AAAA εγγραφής.

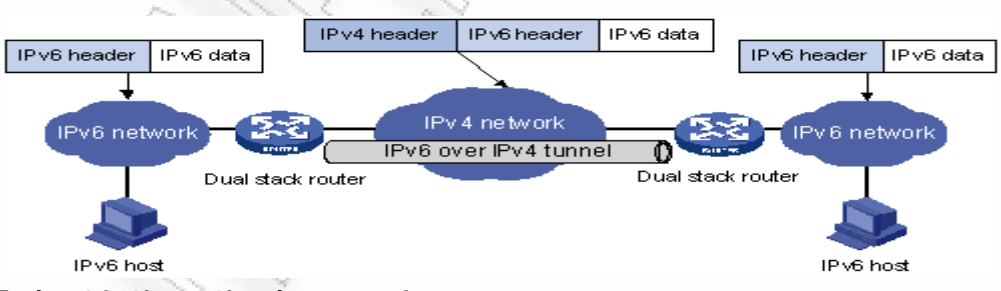


Εικόνα 4.2: Διαδικασία επιλογής πρωτοκόλλου επικοινωνίας ενός dual-stack σταθμού μέσω DNS
Πηγή:(http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/configuration/guides/fm_4_1/ipv6.html)

4.1.2 Οι Μηχανισμοί Tunneling

Η παραδοχή της τεχνικής dual-stack βασίζεται στην υπόθεση ότι υπάρχει συνδεσιμότητα ανάμεσα στον IPv4 και IPv6 χώρο. Αλλά γεννάται το ερώτημα το πώς ένας κόμβος χρησιμοποιεί το IPv6 όταν δεν υπάρχει φυσική IPv6 συνδεσιμότητα? Σε αυτή την περίπτωση, τα tunnels(σήραγγες) παίζουν σημαντικό ρόλο. Ωστόσο τα tunnels θέτουν περιορισμούς τόσο ως προς το μέγεθος του πακέτου όσο και στις διαδικασίες λειτουργίας, πράγμα που κάνει αυτήν την προσέγγιση όχι και τόσο αρεστή. Παρόλα αυτά η προσέγγιση tunnel είναι ίσως η μόνη πρακτική επιλογή για τα επόμενα χρόνια μέχρις ότου το πρωτόκολλο IPv6 γίνει το μοναδικό πρωτόκολλο IP.

Υπάρχουν πολλαπλοί τύποι tunnels για να μεταδώσουν IPv6 πάνω από IPv4 υποδομή. Αυτοί οι δύο είναι ο **Site-to-Site** (βλέπε εικόνα 4.3) όπου το tunnel ενεργεί ως ενδιάμεσος μεταξύ αρκετών IPv6 δικτύων και **Remote-access** όπου το tunnel συνδέει έναν IPv6 κόμβο με το υπόλοιπο IPv6 δίκτυο.



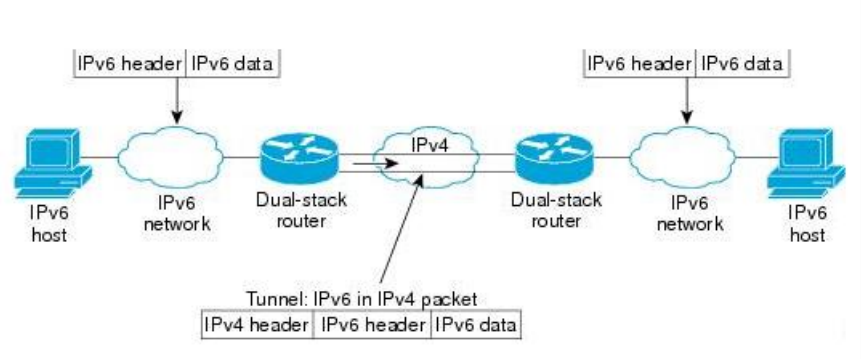
Εικόνα 4.3: Site-to-Site τύπος tunnel
Πηγή:(http://www.h3c.com/portal/Products___Solutions/Technology/IPv4___IPv6_Services/Technology_Introduction/200702/201180_57_0.htm)

Επίσης τα tunnels μπορούν να κατηγοριοποιηθούν και ως προς την κατάστασή τους. Πιο συγκεκριμένα έχουμε τα **Στατικά tunnels (Static)** όταν τα δύο τερματικά σημεία του tunnel έχουν ρυθμιστεί στατικά και τα **Δυναμικά tunnels (Dynamic)** όταν τουλάχιστον ένα τερματικό σημείο του tunnel δεν έχει οριστεί.
Ακόλουθα αναφέρουμε συνοπτικά τις διαφορετικές τεχνικές tunnel για διασύνδεση των IPv6 κόμβων πάνω από IPv4 δίκτυο:

- ***Configured Tunnels***: Ονομάζονται επίσης 6in4 tunnels. Με τον όρο Configures Tunnel εννοείται το tunnel στο οποίο σε κάθε άκρο ορίζεται ρητά η IPv4 διεύθυνση του απέναντι άκρου. Με την τεχνική αυτή τα IPv6 πακέτα ενθυλακώνονται μέσα σε IPv4 πακέτα προκειμένου να διασχίσουν ένα IPv4 δίκτυο. Η επικεφαλίδα του IPv4 πακέτου διαθέτει τις εξής πληροφορίες: Τη διεύθυνση πηγής και προορισμού, δηλαδή τις IPv4 διευθύνσεις των δρομολογητών των σημείων τερματισμού του tunnel.Το πεδίο πρωτοκόλλου, που έχει την τιμή 41 και χρησιμοποιείται για να δηλώσει ότι το IPv4 πακέτο περιέχει ένα άλλο IPv6 πακέτο. Περιέχει επίσης και άλλα πεδία όπως το ID και το πεδίο κατακερματισμού που χρησιμοποιείται εάν χρειαστεί κατακερματισμός του πακέτου μετά την ενθυλάκωση, Time-to-live (TTL) που ορίζεται σε μια προεπιλεγμένη τιμή κ.α. Οι δρομολογητές χτίζουν point-to-point συνδέσεις πάνω από το IPv4 δίκτυο και τις οποίες χρησιμοποιούν για να μεταφέρουν τα πακέτα IPv6. Επίσης είναι δυνατό να τρέχουν διάφορα IPv6-enabled πρωτόκολλα πάνω από τα tunneling interface.

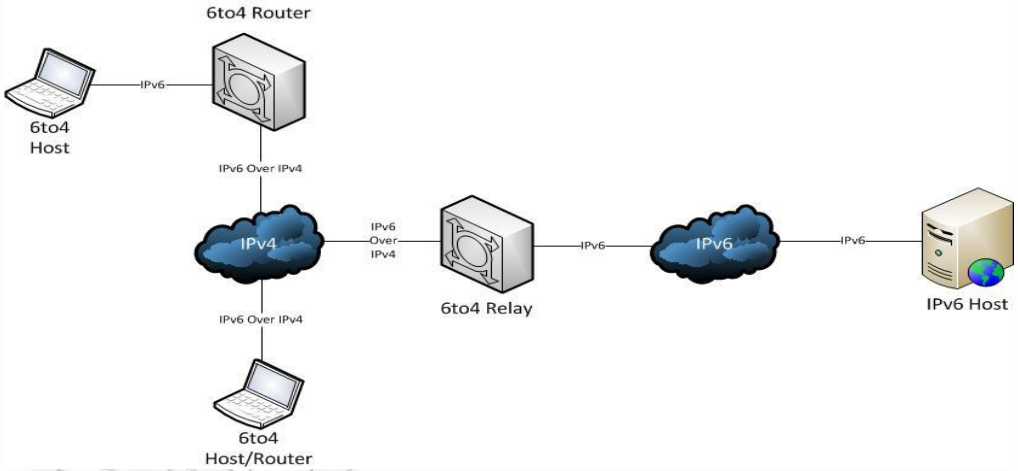
  Ωστόσο η τεχνική αυτή παρουσιάζει τρεις απαιτήσεις που αποδεικνύονται περιοριστικές σε κάποιες περιπτώσεις χρήσης. Πιο συγκεκριμένα μία πραγματική global unicast IPv6 διεύθυνση οφείλει να χρησιμοποιείται, πράγμα που σημαίνει ότι το δίκτυο πρέπει να έχει ένα global unicast IPv6 πρόθεμα που να το έχει λάβει από μία εγγραφή τύπου ARIN ή RIPE ή ISP(Internet Service Provider). Τα δύο τερματικά σημεία του tunnel πρέπει να έχουν στατική IPv4 διεύθυνση. Τέλος τα δύο τερματικά σημεία του tunnel πρέπει να έχουν ρυθμιστεί σε μία per-tunnel βάση, πράγμα που σημαίνει ότι θα πρέπει να έχει διευθετηθεί μια συμφωνία μεταξύ των δύο μεριών όταν τα τερματικά σημεία ανήκουν σε δύο διαφορετικούς οργανισμούς. Όλοι αυτοί οι περιορισμοί επιλύονται με την τεχνική 6to4 που βλέπουμε παρακάτω.

  Ακόλουθα βλέπουμε στην εικόνα 4.4 την δομή του πακέτου στην τεχνική Configured Tunnels:



Εικόνα 4.4: Η δομή του πακέτου στην τεχνική Configured Tunnels
Πηγή:(http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html)

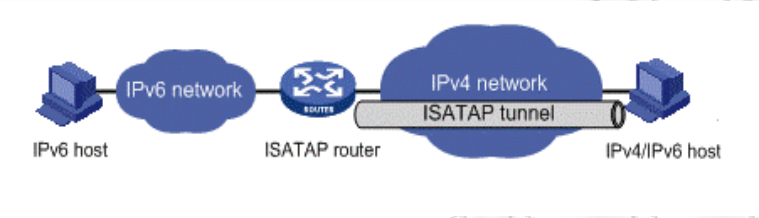
- ***6to4 Tunnels*:** Είναι ένας μηχανισμός που χρησιμοποιείται για την επίτευξη διασύνδεσης IPv6 enabled σταθμών, ακόμα και αν δεν παρέχεται IPv6 υποστήριξη στο δίκτυο στο οποίο και ανήκουν. Το όνομα 6to4 είναι όμοιο με αυτό της τεχνικής configured tunnels (6in4), ωστόσο τα 6to4 tunnels είναι δυναμικά και παρουσιάζουν ορισμένες διαφοροποιήσεις ως προς το πρόθεμα IPv6, το οποίο προέρχεται από τις IPv4 διευθύνσεις και επίσης δεν υπάρχει εδώ η per-tunnel ρύθμιση. Έτσι ένα tunnel interface μπορεί να δεχτεί αλλά και να στείλει πακέτα σε πολλαπλά απομακρυσμένα τερματικά σημεία άλλων tunnels.
  Ένας δρομολογητής με 6to4 tunnel που χρησιμοποιείται για να συνδέσει ένα εσωτερικό IPv6 δίκτυο με τον υπόλοιπο IPv6 «κόσμο» πάνω από IPv4 υποδομή δικτύου ονομάζεται 6to4 δρομολογητής. Κάθε IPv4 διεύθυνση χρησιμοποιείται για να υπολογίσει το IPv6 πρόθεμα δικτύου συνδυάζοντας το 6to4 2002::/16 πρόθεμα με την 32-bit IPv4 διεύθυνση του διαδικτυακού interface για να σχηματίσει ένα /48 πρόθεμα για το IPv6 δίκτυο. Γενικά η τεχνική 6to4 χρησιμοποιεί και αυτή την IPv4 υποδομή προκειμένου να επιτύχει την διασύνδεση των απομακρυσμένων IPv6 κόμβων. Πιο συγκεκριμένα χρησιμοποιεί το IPv4 δίκτυο σαν ένα unicast σημείο προς σημείο επίπεδο διασύνδεσης και χρησιμοποιώντας τεχνικές ενθυλάκωσης υλοποιεί το IPv6 δίκτυο. Ο δεσμός μεταξύ της IPv4 διεύθυνσης και του IPv6 προθέματος δικτύου κάνουν εύκολη την ρύθμιση του tunnel. Δεν υπάρχει ανάγκη να καθοριστεί η IPv4 διεύθυνση προορισμού του tunnel μιας και η IPv6 διεύθυνση προορισμού εμπεριέχει ήδη την IPv4 διεύθυνση. Παρακάτω παραθέτουμε μια εικόνα τυπικής περίπτωσης εφαρμογής της 6to4 τεχνικής:



Εικόνα 4.5: Περίπτωση εφαρμογής της 6to4 τεχνικής
Πηγή:(http://thelazyadmin.com/blogs/thelazyadmin/archive/2011/02/03/transitioning-to-ipv6-part-2.aspx)

Σε αυτήν την εικόνα (4.5) παρατηρούμε και άλλες συσκευές που παίζουν τον δικό τους ρόλο σε ένα 6to4 δίκτυο. Μία από αυτές είναι το **6to4 relay** όπου είναι ένας δρομολογητής που μπορεί να μεταδώσει μία 6to4 διεύθυνση κίνηση μεταξύ 6to4 δρομολογητών και σταθμών πάνω από IPv4 υποδομή. Έχει ορισμένο πάνω του ένα 6to4 pseudo-interface, σύνδεση με το IPv4 δίκτυο και τουλάχιστον ένα φυσικό IPv6 interface. Έτσι διευκολύνει και την λειτουργία του DNS μιας και ο αναμεταδότης δρομολογητής έχει διασύνδεση και με το native IPv6 δίκτυο αλλά και με το 6to4.

- ***ISATAP Tunnels:*** Το πρωτόκολλο ISATAP(Intra-Site Automatic Tunnel Addressing Protocol) είναι ένας μηχανισμός tunneling για περιπτώσεις χρήσης απομακρυσμένης πρόσβασης και είναι ορισμένο στο RFC 4214. Μία συνηθισμένη περίπτωση απομακρυσμένης πρόσβασης είναι όταν το ISATAP χρησιμοποιείται μεταξύ ενός οργανισμού προκειμένου να συνδέσει σταθμούς διπλής-στοίβας (dual-stack) στο IPv6 μέρος του οργανισμού. Συνδέει απομονωμένους dual-stack σταθμούς σε ένα IPv6 δίκτυο. Μέσα σ ένα υποδίκτυο χρειάζεται συνήθως μόνο ένας ISATAP δρομολογητής, οποίος λειτουργεί ως ISATAP server με σύνδεση στο IPv6 Internet για όλους τους κόμβους που εξυπηρετεί στο ISATAP υποδίκτυο.



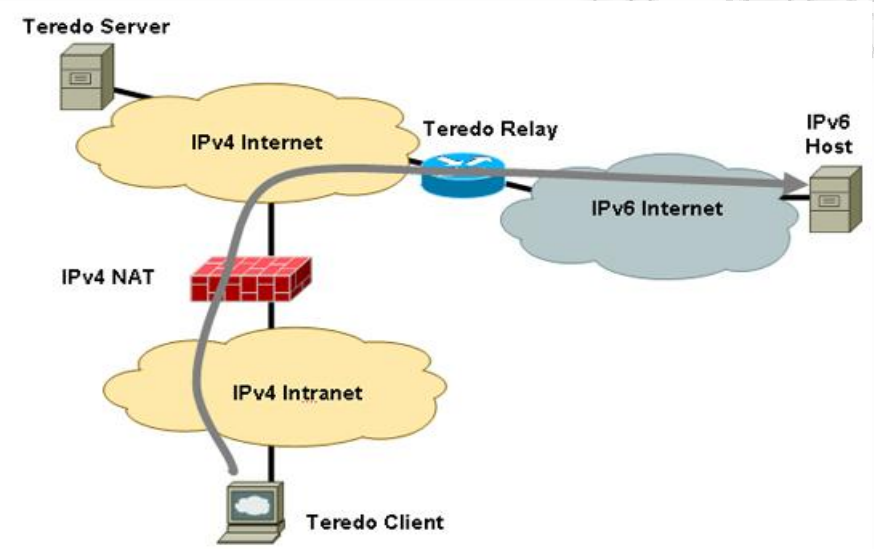
Εικόνα 4.6: Περίπτωση χρήσης του ISATAP μηχανισμού
Πηγή:(http://www.h3c.com/portal/Products___Solutions/Technology/IPv4___IPv6_Services/Technology_Introduction/200702/201180_57_0.htm)

Και εδώ όπως και στο configured tunnel που περιγράψαμε πιο πάνω τα πακέτα IPv6 ενθυλακώνονται μέσα σε IPv4 πακέτα χρησιμοποιώντας το πρωτόκολλο 41. Δεν υπάρχει τρόπος να ανιχνεύσεις τον ακριβή μηχανισμό tunneling κοιτώντας μόνο την IPv4 επικεφαλίδα. Ο ISATAP απαιτεί λίγη ρύθμιση από την μεριά του client. Απλά και μόνο των IPv4 διευθύνσεων των ISATAP δρομολογητών δημιουργεί την σύνδεση ανάμεσα στα IPv4 και IPv6 δίκτυα. Αυτή η ρύθμιση των IPv4 διευθύνσεων διαμορφώνει την ενδεχόμενη λίστα δρομολογητών (PRL-Potential Routers List). Οι ISATAP κόμβοι ενεργοποιούν αυτόματα τις δικές τους global unicast διευθύνσεις ακριβώς όπως και στο SLAAC(Stateless Address Autoconfiguration). Η βασική διαφορά του με το 6tp4 είναι ότι το ISATAP κάνει δυνατή την επικοινωνία στο εσωτερικό του υποδικτύου σε αντίθεση με το 6to4 που καθιστά δυνατή την επικοινωνία μεταξύ υποδικτύων. Έτσι ουσιαστικά συμπληρώνει αποτελεσματικά η μία την άλλη.

- ***Terredo Tunnels:*** Όλοι οι προηγούμενοι μηχανισμοί tunneling που περιγράψαμε εισαγάγανε το πακέτο IPv6 ακριβώς μετά την επικεφαλίδα IPv4 χρησιμοποιώντας το πρωτόκολλο τύπου 41 στην IPv4 επικεφαλίδα. Αυτή η ενθυλάκωση είναι παρόμοια με την ενθυλάκωση που συναντάμε στο IPsec με το πρωτόκολλο 50 για το ESP ή το πρωτόκολλο 51 για την επικεφαλίδα Πιστοποίησης-AH. Αυτός ο τρόπος ενθυλάκωσης πιθανόν να δείχνει ελκυστικός μιας και έχει μικρό overhead, αλλά μία τυπική συσκευή NAT δεν μπορεί να επεξεργαστεί τέτοια IPv4 πακέτα. Οι περισσότερες low-end NAT συσκευές υπερφορτώνουν μία μοναδική Internet-facing IPv4 διεύθυνση στην θέση αρκετών άλλων εσωτερικών IPv4 διευθύνσεων. Η δημόσια Internet-facing IPv4 διεύθυνση είναι global διεύθυνση, και όλες οι εσωτερικές διευθύνσεις είναι τοπικές διευθύνσεις. Όλο αυτές οι συσκευές είναι γνωστές με την ονομασία Port Address Translation(PAT).

  Εάν ένας σταθμός διπλής στοίβας βρίσκεται πίσω από μια τέτοια PAT συσκευή η προτεινόμενη λύση είναι η Terredo, δηλαδή tunneling IPv6 πάνω από UDP διαμέσου της διεύθυνσης δικτύου Μετάφρασης(Network Address Translation-NATs). Πιο συγκεκριμένα ενθυλακώνει ένα IPv6 πακέτο μέσα σε ένα UDP IPv4 datagram.

Απευθύνεται σε κόμβους των οποίων οι παροχείς δικτύου δεν είναι διατεθειμένοι να παρέχουν κανενός είδους υποστήριξη για IPv6. Βασίζεται στην αυτόματη δημιουργία tunnel και στην απόδοση διεύθυνσης. Δημιουργεί tunnels μέσω των οποίων στέλνει IPv6 κίνηση μεταξύ των συσκευών μέσα στα υποδίκτυα. Ο λόγος που ο Terredo μηχανισμός ενθυλακώνει τα IPv6 πακέτα ως IPv4 UDP μηνύματα με UDP και IPv4 επικεφαλίδες, είναι γιατί τα UDP μηνύματα μπορούν να περάσουν όλα τα NAT. Σε αντίθετη περίπτωση αυτό δεν θα μπορούσε να γίνει καθώς η μετάφραση του πρωτοκόλλου στην τιμή 41, που στην προκειμένη περίπτωση θα είχαν τα ενθυλακωμένα IPv6 πακέτα στα IPv4, δεν είναι χαρακτηριστικό των NAT.



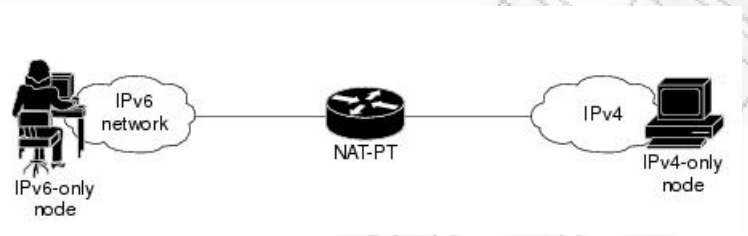
Εικόνα 4.7: Η αρχιτεκτονική δικτύου με την χρήση Terredo Tunnel
Πηγή:(http://www.cisco.com/web/services/news/ts_newsletter/tech/chalktalk/archives/200902.html)

4.2 Τεχνικές Μετάφρασης

Όταν δύο σταθμοί, οι οποίοι χρησιμοποιούν διαφορετικό πρωτόκολλο, προσπαθούν να επικοινωνήσουν τότε υπεισέρχεται η ιδέα των τεχνικών μετάφρασης. Η ιδέα της μετάφρασης των διευθύνσεων των πακέτων σε άλλες δεν είναι καινούρια και μάλιστα αποτελούσε μία από τις κύριες τεχνικές εξοικονόμησης διευθύνσεων στο πρωτόκολλο IPv4. Οι τεχνικές αυτές μπορούν να εφαρμοστούν σε διαφορετικά δικτυακά επίπεδα.

Η πιο διαδεδομένη τεχνική μετάφρασης είναι αυτή μέσω του μηχανισμού NAT-PT (Network Address Translation-Protocol Translation) που έχει διατυπωθεί στο RFC 2766 (και ανανεώθηκε από το RFC 3152) και επιτρέπει στου στους native IPv6-only σταθμούς να επικοινωνούν με τους native IPv4-only σταθμούς και αντίστροφα. Όπως μπορούμε να δούμε και στην εικόνα 4.8 ο NAT-PT μηχανισμός αποτελεί το σύνορο μεταξύ του IPv6 και IPv4 δικτύου. Κάθε NAT-PT μηχανισμός έχει μια ομάδα από globally δρομολογήσιμες IPv4 διευθύνσεις που εκχωρούνται δυναμικά στους IPv6 κόμβους. Οι NAT-PT μηχανισμοί έχουν Application Level Gateways(ALG) όπως ο IPv4 μηχανισμός NAT ή το firewall. Τα ALG είναι ενημερωμένα πρωτόκολλα και περιέχουν πρωτόκολλα όπως το DNS και μπορούν να ξαναγράψουν IPv6 διευθύνσεις με την χρησιμοποίηση των IPv4 διευθύνσεων από την ομάδα που έχει οριστεί για NAT-PT.

Η όλη διαδικασία της αρχιτεκτονικής NAT-PT είναι ότι ο IPv4 κόμβος κάνει ένα DNS ερώτημα για μια IPv4 διεύθυνση και ο μηχανισμός NAT-PT μεταφράζει αυτό το αίτημα σε ένα γενικό ερώτημα για κάθε τύπο διευθύνσεων της ζητούμενης διεύθυνσης. Όταν το DNS ερώτημα λαμβάνει απάντηση μόνο από IPv6 διεύθυνση, τότε το ερώτημα υποκλέπτεται από το μηχανισμό NAT-PT. Ακόλουθα πραγματοποιείται δυναμικό mapping μεταξύ της IPv6 διεύθυνσης της ζητούμενης IPv4 διεύθυνσης και της IPv4 διεύθυνσης της ομάδας του NAT-PT. Τέλος η DNS απάντηση ξαναγράφεται στην δυναμική κατανεμημένη IPv4 διεύθυνση από την ομάδα διευθύνσεων του μηχανισμού NAT-PT. Αξίζει να σημειώσουμε στο σημείο αυτό ότι μεταφράζονται και οι επικεφαλίδες των πακέτων από το ένα πρωτόκολλο στο άλλο έτσι ώστε η πληροφορία να μπορεί να μεταδοθεί από τα διαφορετικά δίκτυα.



Εικόνα 4.8: Η λειτουργία του μηχανισμού μετάφρασης NAT-PT
Πηγή:(http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-nat_trnsln.html)

Ορισμένα από τα μειονεκτήματα του συγκεκριμένου μηχανισμού παρουσιάζουν μεγάλες ομοιότητες με αυτά που συναντάμε και σε άλλες εφαρμογές μετάφρασης επικεφαλίδας. Το πιο προφανές μειονέκτημα του είναι ότι δεν μπορούν να εφαρμοστούν τεχνικές ασφαλείας από άκρο σε άκρο μιας και η διεύθυνση στην οποία θα μεταφραστή η αρχική διεύθυνση προορισμού δεν είναι από την αρχή γνωστή. Η διατήρηση ομάδας IPv4 διευθύνσεων από τον μηχανισμό NAT-PT, οι οποίες χρησιμοποιούνται προκειμένου να αποδοθούν δυναμικά σε IPv6 σταθμούς, αποτελεί και αυτό με την σειρά του ένα πρόσθετο μειονέκτημα λόγω του ότι μπορεί να προκαλέσει αισθητή μείωση στην απόδοση λόγω του μεγάλου χώρου άλλα και του φόρτου χρήσης του.

Επίσης μπορούμε να αναφέρουμε και άλλες δύο τεχνικές μετάφρασης:

- **Bump-in-the-stack (BIS)**: Η λειτουργία του βασίζεται στο γεγονός της παρέμβασής του στα IP πακέτα ενός κόμβου μεταξύ της κάρτας δικτύου του και της IP στοίβας προκειμένου να τα μεταφράζει από IPv6 σε IPv4 και αντίστροφα.
- **Bump-in-the-API (BIA)**: Η λειτουργία του μηχανισμού αυτού παρουσιάζει μεγάλες ομοιότητες με του BIS, αλλά στην προκειμένη περίπτωση κάνει μετάφραση των εξερχομένων πακέτων προτού αυτά δημιουργηθούν με παρέμβασή του στο επίπεδο API.

4.3 Η διασφάλιση της τεχικής μετάβασης μέσω tunnels

Όλοι οι διαφορετικοί μηχανισμοί tunneling που περιγράψαμε δεν σχεδιάστηκαν με γνώμονα την ασφάλεια και έτσι δεν συναντάμε καθόλου πιστοποίηση, έλεγχο ακεραιότητας και εμπιστευτικότητα. Έτσι αυτό αυτόματα μεταφράζεται σε ευπάθεια σε πολλούς κινδύνους όπως Tunnel injection και Tunnel sniffing. Σύμφωνα με τον πρώτο ο hacker μπορεί να εισβάλει παράνομα στην κίνηση του tunnel είτε προσποιούμενος ως νόμιμος χρήστης είτε ξεγελώντας τις

εξωτερικές IPv4 και εσωτερικές IPv6 διευθύνσεις. Όσον αφορά στο Tunnel sniffing, ένας «κατάσκοπος» που βρίσκεται στο IPv4 μονοπάτι του tunnel μπορεί να ανιχνεύσει τα IPv6 πακέτα που μεταδίδονται μέσω του tunnel και να αποκτήσει πρόσβαση στο περιεχόμενο της επικοινωνίας.
Η επίθεση τύπου Tunnel injection ξεκινάει δημιουργώντας ο επιτιθέμενος στο δίκτυο ένα IPv4 πακέτο που περιέχει ένα IPv6 πακέτο. Ακόλουθα το κακόβουλο πακέτο φτάνει στο ένα από τα δύο τερματικά σημεία του tunnel όπου βρίσκεται ένας IPv4 δρομολογητής, από-ενθυλακώνεται, προωθείται και ξανά-ενθυλακώνεται στο τερματικό σημείο του τελικού tunnel. Στο τερματικό σημείο tunnel του τελικού δρομολογητή το IPv6 πακέτο από-ενθυλακώνεται και μεταδίδεται στον τελικό IPv6 προορισμό.

4.3.1 Η ασφάλεια των στατικών Tunnels

Τα στατικά tunnels, όπως τα configured tunnels(6in4) ή GRE tunnels, είναι ευάλωτα και συχνά υπόκεινται σε επιθέσεις τύπου tunnel injection και tunnel sniffing. Για κάθε κακόβουλο πακέτο στο tunnel, ο κακόβουλος χρήστης πρέπει να στείλει ένα πακέτο. Επειδή τα τερματικά σημεία του tunnel είναι στατικά ρυθμισμένα, το δίκτυο έχει αρκετή πληροφορία προκειμένου να αυξήσει την ασφάλεια των tunnels. Έτσι τα configured tunnels μπορούν να προστατευτούν συνδυάζοντας τις παρακάτω τεχνικές:

- **Χρήση του IPsec**: Το IPsec μπορεί να χρησιμοποιηθεί για να προστατέψει οποιαδήποτε κίνηση συμπεριλαμβανομένης και της κίνησης στα tunnels. Αυτή η τεχνική προστατεύει αποτελεσματικά και από την επίθεση τύπου tunnel injection αλλά και tunnel sniffing.
- **Έλεγχος της IPv4 διεύθυνσης αφετηρίας:** Αυτή η τεχνική απορρίπτει όλα τα πακέτα που η διεύθυνση αφετηρίας τους δεν ταιριάζει με κανένα configured tunnel. Ωστόσο αυτή η τεχνική από μόνη της δεν αποτρέπει σε μεγάλο βαθμό την επίθεση μιας και πρέπει να ανακαλύψει και τα δύο τερματικά σημεία του tunnel.
- **Χρήση antispoofing τεχνικών:** Με την τεχνική αυτή απορρίπτονται όλα τα IPv6 πακέτα που εξέρχονται από το λάθος tunnel. Αυτή η τεχνική είναι κατάλληλη για την προστασία από επίθεση τύπου ειδώλου (reflection attack).

Σε αυτό το σημείο αξίζει να τονίσουμε ότι το IPsec από μόνο του δεν μπορεί να παρέχει ασφάλεια σε επιθέσεις τύπου spoofing μεταξύ νομίμων sites. Αυτό συμβαίνει όταν υπάρχει ένας κακόβουλος χρήστης (ή Trojan) σε ένα νόμιμο δίκτυο και στέλνει κακόβουλα IPv6 πακέτα. Αυτός είναι και ο λόγος που το IPsec πρέπει να συνδυάζεται με τους ελέγχους που παρέχει το Unicast RPF (Reserve Path Forwarding).

4.3.2 Η Ασφάλεια των Δυναμικών Tunnels

Προκειμένου ο χρήστης που κάνει επίθεση στο δίκτυο να μπορέσει να περάσει τα κακόβουλα πακέτα του σε ένα configured tunnel, θα πρέπει να γνωρίζει σε κάποιο βαθμό τις IPv4 διευθύνσεις των τερματικών σημείων του tunnel όπως επίσης και τις IPv6 διευθύνσεις. Με τα δυναμικά tunnels, τα τερματικά σημεία των tunnels θα πρέπει να αποδέχονται την ενσωματωμένη κίνηση από οπουδήποτε στον IPv4 χώρο. Έτσι εκτός από την χρήση του IPsec, λίγα πράγματα μπορούν να γίνουν για να απορριφθεί η νόμιμη κίνηση, όπως η εισχώρηση

πακέτου, για μια επίθεση ή την χρήση ενός IPv4-IPv6 αναμεταδότη χωρίς άδεια. Παρακάτω αναφέρουμε τους τρόπους αντιμετώπισης των δυναμικών tunnels 6to4, ISATAP και Teredo από κακόβουλες επιθέσεις.

6to4

Οι 6to4 σήραγγες παρουσιάζουν τρωτά σημεία όπως εισχώρηση κακόβουλων πακέτων, άρνηση υπηρεσιών (DoS-Denial of Services) και ανεξουσιοδοτημένη χρήση. Οι προτεινόμενες πρακτικές αντιμετώπισης είναι η χρήση του Unicast RPF που αναφέραμε και πιο πάνω και του ACL (Access Control List) για την κίνηση που εξέρχεται από το tunnel 6to4 στα νέα ενθυλακωμένα IPv6 πακέτα. Οι ενέργειες που διενεργεί το ACL προκειμένου να προστατέψει το 6to4 tunnel είναι οι εξής:

- ***Έλεγχος της IPv6 διεύθυνσης προορισμού***: Οι 6to4 δρομολογητές δέχονται πακέτα που έχουν μόνο το δικό τους IPv6 πρόθεμα.
- ***Εμποδίζεται η Εξερεύνηση Γειτόνων (Neighbor Discovery):*** Δεν υπάρχει ανάγκη για κάτι τέτοιο μιας και το mapping μεταξύ της 6to4 IPv6 διεύθυνσης και της συσχετιζόμενης IPv4 διεύθυνσης είναι αυτονόητο.
- ***Δεν επιτρέπονται Link-local και Site-local διευθύνσεις:*** Δεν υπάρχει λόγος για μια τέτοια κίνηση πάνω από ένα tunnel. Επιπλέον οι site-local διευθύνσεις είναι τώρα πια ελάχιστες.
- ***Απορρίπτεται ο επαναπροσδιορισμός του ICMP:*** Δεν υπάρχει ανάγκη για αυτό μιας και θα πρέπει να υπάρχει επαναπροσδιορισμός στα 6to4 tunnels επειδή το επόμενο βήμα, δηλαδή η IPv4 διεύθυνση στον 6to4 δρομολογητή, πάντα προέρχεται από την IPv6 διεύθυνση προορισμού.
- ***Απόρριψη ιδιωτικών διευθύνσεων:*** Οι ιδιωτικές διευθύνσεις δεν μπορούν να χρησιμοποιηθούν για την δημιουργία μιας έγκυρης 6to4 διεύθυνσης.

ISATAP

Οι ISATAP σήραγγες παρουσιάζουν πολλές ομοιότητες με τις 6to4 μιας και είναι επίσης δυναμικές. Είναι ευπαθείς σε εισχώρηση κακόβουλων πακέτων και χρήση χωρίς εξουσιοδότηση. Μπορεί να επιτύχουμε μια μερική μείωση του κινδύνου μέσω Unicast RPF ελέγχων και με κάποιες υπηρεσίες του ACL. Ωστόσο είναι λιγότερο επικίνδυνες από ότι στις 6to4 περιπτώσεις επειδή το ISATAP tunnel μπορεί να αναπτυχθεί στο δίκτυο μέσω ιδιωτικών IPv4 διευθύνσεων και απαιτεί τη χρήση RS μηνυμάτων για να πάρει το πρόθεμα του ISATAP δικτύου. Το Unicast RPF ελέγχει το tunnel και απορρίπτει όλες τις διευθύνσεις που δεν ταιριάζουν με το πρόθεμα του IPv6 tunnel. Βέβαια Unicast RPF έλεγχοι πρέπει να εφαρμόζονται και στα native IPv6 interfaces προκειμένου να αποτρέψουν έναν κακόβουλο χρήστη στο IPv6 Διαδίκτυο να στείλει κακόβουλα πακέτα προσποιούμενα ότι προέρχονται από το ISATAP tunnel.

Υπάρχει επίσης η δυνατότητα να χρησιμοποιηθεί το IPsec προκειμένου να προστατευθούν τα ISATAP tunnels απέναντι σε επιθέσεις κλοπής υπηρεσιών, εισβολής κακόβουλων πακέτων ή ανίχνευσης στην μεριά του IPv4, όπως προφανώς και στην μεριά του IPv6. Είναι συχνό το φαινόμενο να προσφέρεται απομακρυσμένη IPv6 πρόσβαση πάνω από το IPv4 Διαδίκτυο.

Teredo

Οι Teredo σήραγγες είναι επίσης ευάλωτες σε επιθέσεις εισχώρησης κακόβουλων πακέτων και χρήσης χωρίς εξουσιοδότηση. Εξαιτίας του πρωτοκόλλου, είναι σχεδόν απίθανο να προστατεύονται οι Teredo tunnels από αυτές τις επιθέσεις απλά με την χρήση του IPsec επειδή οι Teredo αναμεταδότες είναι δυναμικά επιλεγμένοι από τους IPv6 σταθμούς και θα μπορούσαν να είναι εκτός του τομέα διαχείρισης των Teredo χρηστών. Το μεγαλύτερο ζήτημα που προκύπτει ωστόσο από την χρήση της τεχνικής Teredo είναι η λεγόμενη IPv6 λανθάνουσα απειλή, ειδικότερα για τους υπολογιστές με λειτουργικό Windows, μιας και έχουν διαθέσιμο το IPv6 σαν προεπιλογή και η τεχνική Teredo tunnel είναι ήδη εν μέρει ρυθμισμένη. Ακόμα χειρότερα από την μεριά της ασφάλειας, υπάρχουν πολλά πακέτα λογισμικού που φορτώνοντάς τα(για παράδειγμα το Meeting Space), εγκαθίσταται όχι μόνο το λογισμικό αλλά ολοκληρώνεται ταυτόχρονα και η ρύθμιση της τεχνικής Teredo.

Έτσι φορτώνοντας το λογισμικό αυτό συνδέεται κάθε φορά στο Διαδίκτυο IPv6 μέσω του Teredo tunnel. Καθώς όμως η κίνηση Teredo εμφανίζεται ως IPv4 UDP σε όλα τα νόμιμα IPv4 firewall ή NAT μηχανήματα, υπάρχει η πιθανότητα να υπάρξει ελεύθερη ροή των IPv6 πακέτων μέσω των firewall χωρίς ούτε επιβολή πολιτικής ασφάλειας ούτε ελέγχου διαδρομής. Έτσι πολλές τρύπες ασφαλείας ανοίγονται για τους επίδοξους κακόβουλους χρήστες. Για τον λόγο αυτό έχει αυξηθεί η ασφάλεια της χρήσης αυτής της τεχνικής με τους εξής τρόπους:

- Απενεργοποίηση του μηχανισμού Teredo εκτός εάν υπάρχει ενεργοποιημένο κάποιο προσωπικό firewall
- Περιορίζοντας την χρήση του μηχανισμού Teredo να συνδέεται με κόμβους που υποστηρίζουν μόνο IPv6. Εάν ένας απομακρυσμένος server έχει και IPv4 αλλά και IPv6 διεύθυνση, το Teredo δεν χρησιμοποιείται.
- Απενεργοποιώντας το Teredo όταν ο μηχανισμός είναι κομμάτι ενός Active Directory Domain.

Επίσης οι διαχειριστές δικτύων μπορούν να εφαρμόσουν και άλλους τρόπους για να αποτρέψουν τον κίνδυνο της IPv6 λανθάνουσας απειλής στον Teredo μηχανισμό. Αυτοί είναι οι εξής:

- ***Αναπτύσσοντας ένα native IPv6 δίκτυο***: Οι σταθμοί με λειτουργικό Windows κάνουν χρήση του Teredo όταν δεν υπάρχει native IPv6 συνδεσιμότητα, ούτε ISATAP και ούτε 6to4 συνδεσιμότητα. Η χορήγηση native IPv6 μπορεί να προστατέψει την χρήση του μηχανισμού Teredo.
- ***Εμποδίζοντας όλα τα UDP πακέτα περιμετρικά του δικτύου***: Σε αυτήν την περίπτωση εξαιρούνται κάποιες πολύ καλά αναγνωρισμένες UDP πύλες όπως το πρωτόκολλο Network Time και το DNS. Επειδή ο Teredo μηχανισμός χρησιμοποιεί το UDP ως μέσω μετάδοσης, πετυχαίνει αποτελεσματική προστασία του Teredo tunnel.
- ***Εμποδίζοντας μόνο τα Teredo UDP πακέτα***: τα firewalls μπορούν να μπλοκάρουν έτσι τα Teredo πακέτα. Καμιά φορά όμως αυτό είναι λίγο περισσότερο πολύπλοκο.

Υπάρχει περίπτωση ένας χρήστης να κάνει χρήση της προεπιλεγμένης UDP πύλης 3544, η οποία είναι εύκολο να μπλοκαριστεί, αλλά ένας κακόβουλος χρήστης που επιθυμεί να κάνει χρήση του BitTorrent για να κατεβάσει παράνομα αρχεία πιθανόν θα αλλάξει την τιμή της UDP πύλης σε μία μη-προεπιλεγμένη τιμή. Αυτό κάνει το μπλοκάρισμα των Teredo πακέτων περισσότερο πολύπλοκο.

4.4 IPv6 Λανθάνουσες Απειλές ενάντια στα IPv4 δίκτυα

Οι απειλές ενάντια στις τεχνικές μετάβασης έχουν ως κοινό την IPv6 λανθάνουσα απειλή, η οποία οφείλεται στο ότι το IPv6 είναι ενεργοποιημένο ως προεπιλογή σε κάποια λειτουργικά συστήματα όπως τα Windows, Linux και OS X). Συνεπώς, αυτά τα μηχανήματα πρέπει να προστατευτούν από IPv6 επιθέσεις, ακόμα και αν το παρόν δίκτυο τους είναι μόνο IPv4. Ακόμα και αν τα μηχανήματα είναι συνδεδεμένα σε ένα IPv4 δίκτυο αποκλειστικά θα πρέπει να πραγματοποιούν τις παρακάτω ενέργειες:

- ***Αναζήτηση ενός ενεργοποιημένου ασύρματου IPv6 hotspot***: Ο δρομολογητής διαφήμισης (RA-Router Advertisement) στέλνει από τον ασύρματο δρομολογητή να συνδεθεί αμέσως ο σταθμός με το IPv6 Διαδίκτυο.
- ***Παραλαβή πλαστού RA μηνύματος***: Ο σταθμός είναι ρυθμισμένος να κάνει χρήση του IPv6
- ***Χρήση δρομολογήσιμης IPv4 διεύθυνσης:*** Ενεργοποίηση της 6to4 συνδεσιμότητας με το Διαδίκτυο, υποθέτοντας ότι δεν υπάρχει firewall που να μπλοκάρει το πρωτόκολλο 41.
- ***Σύνδεση του Teredo tunnel με ένα αποκλειστικά IPv6 κόμβο:*** Εάν οι συσκευές NAT/firewall αφήσουν τα εξερχόμενα UDP πακέτα και η λειτουργία NAT είναι αρκετά ανοικτή, τότε μία Teredo τρύπα ασφαλείας είναι φανερή στο firewall και επιτρέπει σε κάθε μηχάνημα που είναι συνδεδεμένο στο IPv6 Διαδίκτυο να συνδεθεί με τον Teredo client.

Σε μια συγκεκριμένη περίπτωση συνδυάζεται το πλαστό RA και η δρομολογήσιμη IPv4 διεύθυνση όταν το μηχάνημα είναι λανθασμένα ρυθμισμένο και είναι ενεργοποιημένη η ICS (Internet Connection Sharing), δηλαδή η κοινόχρηστη σύνδεση στο Διαδίκτυο. Ένας τέτοιος σταθμός επιτρέπει και κάνει χρήση του 6to4 tunnel σε ένα anycast 6to4 αναμεταδότη και επειδή έχει ενεργοποιημένη την ICS, ξεκινάει να στέλνει RA μηνύματα σε όλα τα άλλα interfaces χωρίς native IPv6 συνδεσιμότητα. Αυτό έχει ως αποτέλεσμα να διαφημίζει και να προσφέρει IPv6 συνδεσιμότητα σε όλους τους γειτονικούς κόμβους. Υπάρχουν ωστόσο αρκετοί τρόποι να μειώσουμε την επίδραση αυτής της λανθάνουσας απειλής και είναι οι εξής:

- ***Ενημέρωση για την ασφάλεια IPv6***: Ένας από τους πλέον κρίσιμους παράγοντες είναι η ενημέρωση των υπαλλήλων που χειρίζονται θέματα ασφάλειας αλλά και των διαχειριστών δικτύων πάνω σε θέματα που αφορούν τις λανθάνουσες απειλές αλλά και εκπαίδευση αυτών πάνω στα θέματα ασφαλείας του IPv6.
- ***Ρύθμιση των υπαρχόντων προϊόντων ασφαλείας πάνω στο IPv6***: Είναι πολύ σημαντική η ρύθμιση των ιδιωτικών firewalls, των IPSs (Security Agent) σταθμών και άλλων προϊόντων ασφαλείας πάνω στις απαιτήσεις του IPv6.
- ***Αντικατάσταση παλαιότερων προϊόντων ασφαλείας χωρίς IPv6 υποστήριξη***: Επιβάλλεται να υπάρξει μια εκ νέου αξιολόγηση, και όλα τα προϊόντα ασφαλείας που είναι σχεδιασμένα να παρέχουν ασφάλεια αποκλειστικά και μόνο σε IPv4 σταθμούς θα πρέπει να αντικατασταθούν με κάποιες αναβαθμισμένες εκδόσεις ή εξολοκλήρου νέα προϊόντα που να υποστηρίζουν το πρωτόκολλο IPv6.
- ***Απενεργοποίηση του IPv6 πρωτοκόλλου στοίβας από τους σταθμούς:*** Αυτό μπορεί να γίνει εύκολα μέσω των settings των Windows και πιο συγκεκριμένα του

Group Policy Object. Αξίζει να τονίσουμε ότι αυτός ο τρόπος δεν παρέχει προστασία για άλλες περιπτώσεις.

- ***Προσπάθεια να εμποδίσουμε την IPv6 κίνηση:*** Αυτός ο τρόπος δείχνεις ίσως ο πιο ελκυστικός από όλους ωστόσο κρύβει και πολλούς κινδύνους και είναι αρκετά πολύπλοκος. Αρχικά αυτή η απόφαση θα μπορούσε να αλλάξει την ανάπτυξη του IPv6 σε κάποια χρόνια για επιχειρηματικούς λόγους. Επίσης μόνο ορισμένα switches(διακόπτες δικτύου) έχουν την δυνατότητα αυτήν την χρονική στιγμή να μπλοκάρουν τα native IPv6 Ethernet frames. Τέλος, ενώ είναι ίσως κάπως τετριμμένη πια η παρεμπόδιση ορισμένων tunneling μηχανισμών που χρησιμοποιούν το πρωτόκολλο 41, είναι σίγουρα λιγότερο ασήμαντη η παρεμπόδιση του μηχανισμού Teredo που απαιτεί τον αποκλεισμό όλης της εξερχόμενης UDP κίνησης ή της χρήσης του FPM (Flexible Packet Matching).

4.5 Συμπεράσματα

Η μετάβαση από το πρωτόκολλο IPv4 σε αυτό του IPv6 θα πάρει ακόμα αρκετά χρόνια για να επιτευχθεί στον απόλυτο βαθμό, γι αυτό και η συνύπαρξη αυτών των δύων είναι απαραίτητη. Η IETF για τον σκοπό αυτό δημιούργησε μια σειρά από μηχανισμούς μετάβασης όπως:

- Dual Stack (Διπλής στοίβας)
- 6in4 Configured Tunnels
- 6to4 Tunnels
- ISATAP Tunnels
- Teredo Tunnels
- NAT-PT και NATP-PT

Η μέθοδος Dual Stack δικτύου, όπου οι σταθμοί τρέχουν παράλληλα το IPv6 και IPv4 πρωτόκολλο στοίβας, είναι αυτή που προτείνεται κατά κόρον μιας και είναι η πιο εύκολη να εφαρμοστεί και να αναπτυχθεί. Στις μέρες μας τα περισσότερα λειτουργικά συστήματα έχουν το IPv6 σαν προεπιλογή. Αυτό όμως αποτελεί ταυτόχρονα και πηγή κινδύνου με την γνωστή ονομασία λανθάνουσα IPv6 απειλή. Σύμφωνα με αυτή ακόμα και σε δίκτυα που επικοινωνία γίνεται αποκλειστικά μέσω του πρωτόκολλου IPv4, υπάρχουν μηχανήματα που θα μπορούσαν να γίνουν στόχοι IPv6 επιθέσεων. Οι προτεινόμενες λύσεις σε αυτό τον κίνδυνο είναι η εκπαίδευση και η γνώση των κατάλληλων ανθρώπων που ασχολούνται στον τομέα αυτό, όπως οι διαχειριστές και οι εργαζόμενοι δικτύων, πάνω σε θέματα ασφάλειας IPv6. Επίσης είναι επιτακτική η ανάγκη αναβάθμισης ή και αντικατάστασης των παλαιοτέρων προϊόντων ασφαλείας, με προϊόντα που ανταποκρίνονται στις απαιτήσεις ασφαλείας του νέου πρωτοκόλλου IP.

Οι κίνδυνοι που ελλοχεύουν και απειλούν τους μηχανισμούς μετάβασης είναι πολλοί και χρήζουν ιδιαίτερης αντιμετώπισης. Η ασφάλεια αυτών των μηχανισμών είναι βαρύνουσας σημασίας μιας και από αυτούς εξαρτάται η ασφαλής και επιτυχής εγκαθίδρυση του πρωτοκόλλου IPv6. Η γνώση και η ενημέρωση πάνω στα θέματα ασφαλείας του IPv6 είναι κρίσιμης σημασίας κατά το στάδιο της μετάβασης.

Κεφάλαιο 5

Επιθέσεις στο πρωτόκολλο IPv6

5.1 Επιθέσεις στα Δίκτυα γενικά

Θα ήταν καλό στην παρούσα ενότητα να κάνουμε μια γενική παρουσίαση των ειδών των επιθέσεων που απειλούν τα δίκτυα και κατ επέκταση το πρωτόκολλο IPv6 προτού προχωρήσουμε στην πιο ενδελεχή έρευνα και προσομοίωση μερικών από αυτών. Μπορούμε να τις χωρίσουμε σε διάφορες κατηγορίες ανάλογα με τον απώτερο σκοπό που διεξάγεται μία επίθεση αλλά και με τον τρόπο που υλοποιείται. Έτσι μπορούμε να τις διακρίνουμε στις εξής:

- ***Επιθέσεις τύπου Επανάληψης (Replay attacks):*** Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση replay attack. Ο εισβολέας συλλαμβάνει τα πακέτα που περιέχουν τους κωδικούς πρόσβασης ή τις ψηφιακές υπογραφές, όποτε αυτά περνούν μεταξύ δύο σταθμών ενός δικτύου. Στην προσπάθεια τους να αποκτήσουν πιστοποιημένη σύνδεση, οι επιτιθέμενοι στο δίκτυο ξαναστέλνουν στο σύστημα τα πακέτα που έχουν συλλάβει σε άλλη χρονική στιγμή.
- ***Επιθέσεις τύπου Άρνησης Εξυπηρέτησης (Denial of service attacks):*** Ο σκοπός αυτών των επιθέσεων είναι να μεταβεί το σύστημα σε τέτοια κατάσταση ώστε να μην καθίσταται δυνατόν να χρησιμοποιηθεί από τους εκάστοτε χρήστες. Ορισμένοι από τους τρόπους που γίνονται αυτού του είδους οι επιθέσεις είναι είτε να στείλουν κακόβουλα πακέτα ώστε να προκαλέσουν κατάρρευση του συστήματος είτε μέσω της στρατηγικής flooding, δηλαδή να πλημμυρίσουν το δίκτυο με μεγάλη κυκλοφορία δεδομένων ώστε να καταστήσουν την χρήση του αδύνατη. Μια τέτοια επίθεση έχει σκοπό να υπερφορτώσει τόσο πολύ το σύστημα-στόχο καταναλώνοντας μνήμη και bandwidth έτσι ώστε να μην είναι σε θέση πλέον να εξυπηρετήσει τους κανονικούς χρήστες του. Οι επιθέσεις αυτές εκμεταλλεύονται τις αδυναμίες του πρωτοκόλλου TCP/IP (Ping of Death, Teardrop, SYN Attack, Smurf Attack), IPv6 και προσπαθούν να εξαντλήσουν όλους τους πόρους (μνήμη , CPU, bandwidth) του συστήματος προκειμένου να προκαλέσουν διακοπή της λειτουργίας του. Σε κάθε περίπτωση όταν ο διαχειριστής του δικτύου αντιληφθεί επιθέσεις αυτού του είδους θα πρέπει να χρησιμοποιήσει το τείχος προστασίας προκειμένου να εμποδίσει τα κακόβουλα εισερχόμενα πακέτα και αιτήματα.
- ***Man-In-The-Middle attack :*** Η επίθεση Man-In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα. Δηλαδή ο κακόβουλος χρήστης παρεμβάλλεται ανάμεσα στην επικοινωνία μεταξύ δύο σταθμών αναλύει, τροποποιεί ή και καταστρέφει τα μεταδιδόμενα δεδομένα.

- ***Address spoofing :*** Το spoofing έχει να κάνει με την προσπάθεια κάποιου να προσποιηθεί ότι είναι κάποιος άλλος, αλλάζοντας την ταυτότητα του. Η αλλαγή αυτή συνήθως συμβαίνει είτε στην MAC είτε στην IP address του χρήστη. Η δρομολόγηση των πακέτων και οι πληροφορίες κεφαλής πακέτων είναι κατασκευασμένα έτσι ώστε να μην εγγυώνται τον αποστολέα του πακέτου και έτσι επιτρέπεται στους εισβολείς να προσποιηθούν ότι είναι κάποιος άλλος κατά την διάρκεια της επικοινωνίας με το σύστημα. Ο εισβολέας μπορεί να προσποιηθεί ότι είναι κάποιος από τους νόμιμους χρήστες αλλάζοντας την MAC address του. Αυτό μπορεί να επιτευχθεί εξαιρετικά εύκολα είτε με την ifconfig αν πρόκειται για χρήστη λειτουργικού συστήματος Linux, είτε με αλλαγή κάποιων κλειδιών στη registry αν πρόκειται για χρήστη Windows, είτε ακόμα και με εφαρμογές που δίνουν οι ίδιοι οι κατασκευαστές των ασύρματων αυτών καρτών. Οι μέθοδοι πιστοποίησης που προσφέρονται σε πολύ καλύτερο επίπεδο στο πρωτόκολλο IPv6 από ότι στο προγενέστερό του είναι και οι πιο αποτελεσματικοί μέθοδοι αντιμετώπισης αυτών των επιθέσεων.
- ***Session Hijacking :*** Η επίθεση αυτή που δεν έχει κάποια δόκιμη αντίστοιχη ορολογία στα ελληνικά παρουσιάζει πολλές ομοιότητες με αυτήν της man-in-the-middle που περιγράψαμε πιο πάνω. Και σε αυτήν την περίπτωση έχουμε να κάνουμε με την υποκλοπή δεδομένων από κάποιον κακόβουλο χρήστη που παρενέβη στην επικοινωνία. Αυτό το επιτυγχάνει με το να μεσολαβεί μεταξύ δύο νόμιμων σταθμών και να παρακολουθεί τα πακέτα που ανταλλάσσονται. Οι μελλοντικές του ενέργειες εξαρτάται από τον σκοπό και από τι διαθέσεις έχει ως προς αυτή την επίθεση. Μια γνωστή επίθεση που ανήκει σε αυτήν την κατηγορία είναι η λεγόμενη evil twins επίθεση. Αυτή είναι μία τεχνική κατά την οποία ο επιτιθέμενος παριστάνει τον διακομιστεί ηλεκτρονικής αλληλογραφίας ή τον εξυπηρετητή ενός οργανισμού προκειμένου να συλλέξει απόρρητες και σημαντικές πληροφορίες.
- ***Brute Force attack :*** Πραγματοποιείται χρησιμοποιώντας όλα τα πιθανά κλειδιά για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιημένα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά.

5.2 Οι τρύπες ασφαλείας του πρωτοκόλλου IPv6

Το πρωτόκολλο IPv6 θα φτάσει κάποια στιγμή να είναι τόσο διαδεδομένο όσο το IPv4 και ίσως ακόμα περισσότερο. Κατά την διάρκεια της επόμενης δεκαετίας που το IPv6 θα έχει αναπτυχθεί ακόμα περισσότερο, θα σχεδιαστούν συστήματα προκειμένου να αντικαταστήσουν αυτά που υποστηρίζουν το πρωτόκολλο IPv4. Και ενώ οι πρώτες εφαρμογές που έχουν σχεδιαστεί μπορούν να βοηθήσουν στην αποφυγή σφαλμάτων, υπάρχουν ωστόσο ακόμα πολλά θέματα που χρήζουν επίλυσης. Οι IPv6 εφαρμογές είναι ακόμα σχετικά νέες στο χώρο της αγοράς, και το software που έχει δημιουργήσει αυτά τα συστήματα δεν έχει εξεταστεί τόσο διεξοδικά στον χώρο αυτό όσο τα αντίστοιχα συστήματα του IPv4. Υπάρχει η πιθανότητα σε κάποιο χρονικό διάστημα να εμφανιστούν ελαττώματα, και οι πωλητές θα χρειαστεί να ανταποκριθούν άμεσα προκειμένου να αντιμετωπίσουν αυτά τα σφάλματα. Πολλές ομάδες ερευνούν διεξοδικά το πρωτόκολλο IPv6 και το δοκιμάζουν σε διάφορες εφαρμογές, προκειμένου να ανακαλύψουν τυχόν σφάλματα και να τα διορθώσουν προτού γίνει η πλήρης εγκατάσταση και εγκαθίδρυσή του στο χώρο. Παρόλα αυτά, οι περισσότερες εφαρμογές που έχουν να κάνουν με εξοπλισμό και software πληροφορικής έχουν παρουσιάσει προβλήματα ασφάλειας κάνοντας χρήση του IPv6. Όσο το πρωτόκολλο IPv6 συνεχίζει να υιοθετείται, τόσο αρχίζει να συγκεντρώνει την προσοχή των hackers.

Οι πρώτες εφαρμογές της IPv6 τεχνολογίας δείχνουν να είναι αρκετά αποδοτικές και βεβαιώνουν ότι η ασφάλεια αποτελεί σημαντικό μέλημα τους. Υπάρχουν ωστόσο ορατοί κίνδυνοι εάν τρέχουμε το πρωτόκολλο IPv6 σε ένα δίκτυο χωρίς παράλληλα να έχουμε πάρει τα κατάλληλα μέτρα ασφαλείας. Κάποια λειτουργικά συστήματα μπορούν να τρέχουν ταυτόχρονα και τα δύο είδη πρωτοκόλλων IP χωρίς την παρέμβαση του χρήστη. Έτσι αυτά τα λειτουργικά συστήματα πιθανών να προσπαθούν να συνδεθούν στο διαδίκτυο μέσω του IPv6 χωρίς ωστόσο ο χρήστης νωρίτερα να το έχει επιλέξει και ρυθμίσει. Εδώ ελλοχεύει ένα μεγάλος κίνδυνος. Εάν ο χρήστης δεν έχει αντίληψη αυτού του γεγονότος και παράλληλα δεν υπάρχει κάποια πολιτική ασφάλειας ή κάποια εφαρμογή προστασίας για IPv6 ασφάλεια, τότε υπάρχει μεγάλη πιθανότητα να δεχθεί επίθεση. Το IPv6 μπορεί να χρησιμοποιηθεί ως “backdoor protocol”, επειδή πολλά συστήματα ασφαλείας παρέχουν ασφάλεια μόνο για τα IPv4 πακέτα και αγνοούν αυτά του IPv6.

Ένα ακόμα στοιχείο που πρέπει να τονίσουμε είναι η έλλειψη της εμπειρίας IPv6 στις επιχειρήσεις. Δεν υπάρχει η απαραίτητη εμπειρία προκειμένου να παρέχουν ασφάλεια σε ένα IPv6 δίκτυο. Αυτός άλλωστε είναι και ένας από τους σημαντικούς λόγους που χρειάζεται να κατανοήσουμε τα θέματα ασφαλείας του IPv6 και να προετοιμάσουμε τις κατάλληλες δικλείδες ασφαλείας. Είναι επιτακτική ανάγκη να πραγματοποιηθεί αυτό προτού το IPv6 δίκτυο γίνει ακόμα μεγαλύτερος στόχος για τους hackers. Δεν έχουν ανακαλυφθεί ακόμα πολλές επιθέσεις που σχετίζονται με το πρωτόκολλο IPv6 ή δεν είναι ακόμα ευρέως γνωστές. Επιπρόσθετα στις μέρες μας υπάρχουν μόνο λίγες πρακτικές που παρέχουν ασφάλεια στα IPv6 συστήματα ή αρχιτεκτονικές ασφαλείας για το IPv6. Ορισμένες DoS επιθέσεις είναι διαθέσιμες και έχει ανακαλυφθεί επίσης ένα worm για το IPv6, ωστόσο υπάρχει πολύ μικρή πληροφορία για τις νέες IPv6 επιθέσεις.

Η IETF ορίζει τις προδιαγραφές του πρωτοκόλλου IPv6 που πρέπει να ακολουθούν οι εφαρμογές προκειμένου να δημιουργήσουν ένα διαλειτουργικό πρωτόκολλο. Ωστόσο κάποιες από αυτές είναι αμφιλεγόμενες και δεν έχουν ολοκληρωθεί ακόμη και μέχρι σήμερα. Συνεπώς μπορεί να εμφανιστούν απροσδόκητα θέματα ασφαλείας μετά την ανάπτυξη και εγκατάσταση του software. Για παράδειγμα, τα πακέτα που συναντάνε τις προδιαγραφές που έχουν διατυπωθεί από την IETF RFCs μπορεί να έχουν συνέπειες όταν στέλνονται ή παραλαμβάνονται στο δίκτυο. Ενώ είναι νόμιμα σύμφωνα με τις προδιαγραφές, κάποια πακέτα μπορεί να μην ακολουθούν την πρακτική λογική του πως η επικοινωνία πρέπει να γίνεται. Τα θέματα αυτά είναι ανεξάρτητα από την εκάστοτε κατάσταση του δικτύου , δηλαδή αν είναι τοπικό ή ευρύ, και ισχύουν για πολλούς τύπους δικτύων. Αυτές οι μικροδιαφορές μεταξύ των προδιαγραφών και των πρακτικών ανάπτυξης ανακαλύπτονται από τους hackers και αποτελούν τρύπες ασφαλείας για το δίκτυο.

Τέλος μια άλλη πηγή κινδύνων για το πρωτόκολλο IPv6 αφορά τους δρομολογητές. Οι δρομολογητές IPv6 δεν είναι συνήθως σε θέση να τρέχουν σε παραδοσιακό λογισμικό server ή σε εφαρμογές που παρουσιάζονται ευπαθή σε κινδύνους. Παρόλα αυτά, μπορεί να αποτελούν στόχο για υπερχείλιση μνήμης, όπου ο εισβολέας επιχειρεί να στείλει επιπλέον πληροφορία στον δρομολογητή προκειμένου να υπερβεί το όριο της εσωτερικής μνήμης. Αυτό μπορεί να προκαλέσει σημαντικά προβλήματα, από την δυσλειτουργία λογισμικού (την λεγόμενη “κατάρρευση” του υπολογιστή) μέχρι και την απομακρυσμένη πρόσβαση του εισβολέα. Όσο το νέο πρωτόκολλο αποκτά ακόμα πιο ευρεία χρήση τόσο ανακαλύπτονται καινούριοι κίνδυνοι που χρήζουν άμεσης αντιμετώπισης. Τα “ευπαθή” σημεία του πρωτοκόλλου IPv6 θα πρέπει άμεσα να τροποποιηθούν και να ρυθμιστούν προκειμένου να μην θέτουν σε κίνδυνο την ίδια την ύπαρξη του πρωτοκόλλου. Σε κάθε περίπτωση η επανεξέταση του πρωτοκόλλου σε τακτά χρονικά διαστήματα κρίνεται αναγκαία.

5.3 Παρουσίαση του Περιβάλλοντος Προσομοίωσης της Επίθεσης

Στο σημείο αυτό και προτού προχωρήσω στην διαδικασία προσομοίωσης επίθεσης ενάντια στο πρωτόκολλο IPv6 που επέλεξα να παρουσιάσω, θα ήταν δόκιμο να κάνω πρώτα μια αναφορά στα εργαλεία που χρησιμοποίησα αλλά και το περιβάλλον στο οποίο έγινε η προσομοίωση.

Αρχικά και όσον αφορά την προσομοίωση της επίθεσης έγινε σε περιβάλλον τοπικού (LAN-network) δικτύου αποτελούμενο από δύο ενεργά μηχανήματα. Τα λειτουργικά συστήματα ήταν σε Windows 7 και σε Ubuntu Linux. Επίσης το μηχάνημα με το λειτουργικό σύστημα των Windows 7 είχε ρυθμισμένη IPv6 διεύθυνση όπως άλλωστε παρέχεται από το ίδιο το λειτουργικό σύστημα των Windows 7 σαν προεπιλογή. Όσον αφορά τον άλλο υπολογιστή με το λειτουργικό σύστημα των Ubuntu ρυθμίσαμε χειροκίνητα την IPv6 διεύθυνσή του με την βοήθεια ενός IPv6 Tunnel Broker service που προσφέρει δωρεάν η Hurricane Electric (http://tunnelbroker.net/). Αυτό μας εξασφάλισε το γεγονός ότι η επικοινωνία θα γίνεται μέσω του πρωτοκόλλου IPv6.

Για την κατασκευή των κατάλληλων πακέτων προκειμένου να υλοποιηθεί η εκάστοτε επίθεση έγινε με την χρήση της βιβλιοθήκης scappy. Είναι γραμμένη σε γλώσσα Python και παρέχει μεγάλη ευελιξία στην κατασκευή πακέτων. Ένα ακόμα μεγάλο πλεονέκτημά της είναι η ταχύτητα και η ευκολία στην κατασκευή των πακέτων, ενώ παρέχει επίσης δυνατότητες σύλληψης πακέτων από το δίκτυο. Μας επιτρέπει να κατασκευάσουμε ένα μεγάλο αριθμό από διαφορετικού είδους πακέτα, χωρίς να απαιτεί ιδιαίτερα μεγάλη προσπάθεια, ενώ παράλληλα αποκρύπτει από τον προγραμματιστή ένα πολύ μεγάλο μέρος από τις κουραστικές λεπτομέρειες και τον κώδικα που απαιτούνται για την κατασκευή κάποιου πακέτου.

Επίσης για την επίτευξη της προσομοίωσης χρησιμοποιήθηκαν δύο ειδών routers, ένας της LinkSys και ο άλλος της Cisco, και πιο συγκεκριμένα το μοντέλο 2800 series. Όσον αφορά στον δεύτερο έχοντας το δικό του interface μας παρείχε την δυνατότητα του ACL-Access List(θα παρουσιαστεί εκτενέστερα σε επόμενη ενότητα) προκειμένου να διαχειριστούμε την ροή των πακέτων αλλά και κατανοώντας τον τρόπο της επίθεσης να μπορούμε να την αποτρέψουμε μέσα από την χρήση των κατάλληλων εντολών. Έτσι σε κάθε περίπτωση η κατανόηση του είδους άλλα και του τρόπου που υλοποιείται η επίθεση καθίσταται αναγκαία προκειμένου να αποτραπεί. Επιπρόσθετα λόγω του ότι το router 2800 series είναι configurable, χρειάστηκε να το ρυθμίσουμε από την αρχή με μια σειρά από εντολές προκειμένου να περάσουμε τις διευθύνσεις των υπολογιστών και να επιτευχθεί η μεταξύ τους επικοινωνία (περισσότερες λεπτομέρειες θα δούμε σε επόμενη ενότητα). Στο πλαίσιο των ρυθμίσεων του router μας βοήθησε και το πρόγραμμα putty που είναι ένα free open source terminal προκειμένου να γράφουμε τις εντολές στο interface του router.

Τέλος έγινε χρήση του εργαλείου gns3 για λόγους περισσότερο σχεδιασμού και γραφικής αναπαράστασης της επίθεσης. Το εργαλείο παρέχει όλα εκείνα τα αντικείμενα και τις σχέσεις που είναι απαραίτητες για την κατάλληλη απεικόνιση του δικτύου. Επίσης επειδή κατά βάση είναι ένας simulator βοήθησε ώστε να δοκιμάσουμε κάποιες εντολές και ρυθμίσεις προτού τις τρέξουμε απευθείας στο περιβάλλον της επίθεσης.

Όλα τα παραπάνω συνθέτουν το σκηνικό της προσομοίωσης των επιθέσεων που εκτελέσαμε προκειμένου να κατανοήσουμε ακόμα καλύτερα τον τρόπο που διενεργούνται, τις επιπτώσεις που έχουν στο σύστημα αλλά και να ανακαλύψουμε βαθύτερα τις άγνωστες πτυχές τους και να καταλήξουμε σε χρήσιμα συμπεράσματα.

5.4 Επικεφαλίδα Διάσπασης

Ο κατακερματισμός είναι η διαδικασία κατά την οποία ένα IP πακέτο διασπάται σε πολλά μικρότερα πακέτα προκειμένου να μεταδοθεί ευκολότερα σε ένα δίκτυο δεδομένων που δεν έχει την δυνατότητα μετάδοσης μεγάλων πακέτων. Ο κατακερματισμός εμφανίζεται σε δίκτυα διαφόρων μεγεθών MTU interface. Εάν ένα μεγάλο IPv4 πακέτο παραλαμβάνεται σε μια διασύνδεση με router και το μέγεθος MTU της εξωτερικής διασύνδεσης είναι πολύ μικρό, το πακέτο χρειάζεται να διασπαστεί σε μικρότερα πακέτα πριν την μετάδοσή του. Σε κάθε κομμάτι του κατακερματισμένου πακέτου, που είναι στην ουσία ένα μικρότερο πακέτο, δίνεται ένα μοναδικό αναγνωριστικό, γνωστό ως fragment ID, προκειμένου να διακρίνεται από τα υπόλοιπα κομμάτια(fragments) του αρχικού πακέτου. Επίσης σε κάθε fragment του πακέτου δίνεται μία offset τιμή του αριθμού των bytes που δείχνει πόσο μακριά βρίσκεται από το αρχικό fragmentable κομμάτι του αρχικού πακέτου. Ο σταθμός υποδοχής του πακέτου επανασυνδέει τα κομμάτια-πακέτα (fragments) τοποθετώντας τα όλα μαζί με την σειρά και έπειτα περνάει ολόκληρο το IP πακέτο στην στοίβα του πρωτοκόλλου. Αυτή είναι η φυσιολογική διαδικασία στα δίκτυα, ωστόσο μπορεί να οδηγήσει σε σοβαρά θέματα ασφαλείας.

5.4.1 Θέματα Ασφαλείας από τον κατακερματισμό πακέτων

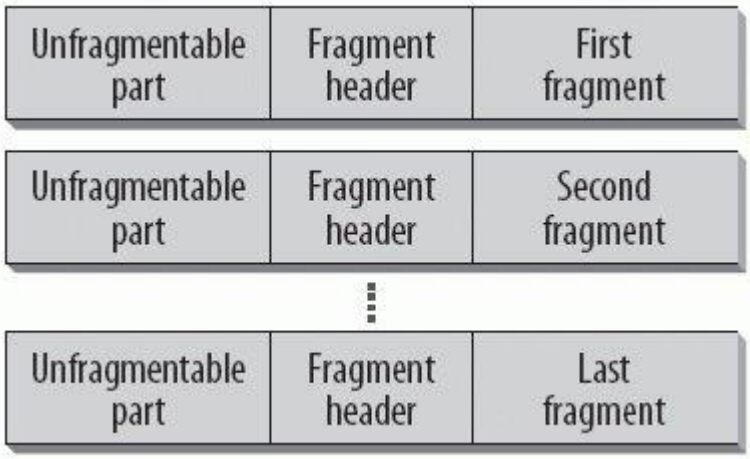
Ένα από τα κύρια θέματα που προκύπτουν από την διαδικασία του κατακερματισμού αφορά τη πληροφορία του ανωτέρου επιπέδου η οποία ενδέχεται να μην εμπεριέχεται εντός του πρώτου κομματιού. Ένα από τα κομμάτια (fragments) μπορεί να περιέχει την επικεφαλίδα TCP ή UDP η οποία απαιτείται από ένα firewall προκειμένου να αποφασίσει εάν το πακέτο μπορεί να περάσει. Σε κάθε άλλη περίπτωση, το firewall πρέπει να κοιτάξει πολλαπλά πακέτα προτού καταλήξει σε έναν ακριβή προσδιορισμό. Οι υπολογισμοί πόρων από τα firewall θα απαιτηθούν για να πραγματοποιηθεί η επανασυναρμολόγηση και έπειτα για την λεπτομερή ανάλυση του πακέτου. Παρόλα αυτά, τα firewalls αναμένεται να πάρουν αποφάσεις για τα κομμάτια του κατακερματισμένου πακέτου τα οποία έχουν μη επαρκή πληροφορίες πρωτοκόλλου.

Τα IPv6 κομμάτια του κατακερματισμένου πακέτου μπορεί να χρησιμοποιηθούν από τους εισβολείς είτε για να κρύψουν την επίθεσή τους είτε για να επιτεθούν σε έναν κόμβο. Τοποθετώντας την επίθεση στα πολλά μικρά κομμάτια του πακέτου που έχει διασπαστεί, ο κακόβουλος χρήστης προσπαθεί να παρακάμψει τον εντοπισμό ή το λεγόμενο filtering. Ο προσδιορισμός του πραγματικού σκοπού της επίθεσης θα απαιτούσε την επανασύνδεση όλων των κομματιών-πακέτων του αρχικού κατακερματισμένου πακέτου. Ένας εισβολέας μπορεί να διασπάσει τα πακέτα σε πολλά μικρότερα κομμάτια έτσι ώστε το κάθε ένα να δείχνει νόμιμο και τα εκάστοτε firewall να μην μπορούν να εντοπίσουν την επίθεση.

Οι εισβολείς θα μπορούν επίσης να δημιουργήσουν fragments με τέτοιο τρόπο ώστε να εκμεταλλευτούν τις αδυναμίες της μεθόδου που χρησιμοποιεί ο σταθμός προορισμού για να επανασυνδέσει τα κομμάτια του κατακερματισμένου πακέτου. Ένα τέτοια παράδειγμα θα ήταν η επικάλυψη των κομματιών, δηλαδή η επικάλυψη στην τιμή offset και στα εκτός λειτουργίας κομμάτια όπου το fragment ID τους δεν ταιριάζει ακριβώς με τα δεδομένα. Ένα άλλο είδος κατακερματισμού επίθεσης γίνεται όταν ο επιτιθέμενος στέλνει μία μη ολοκληρωμένη σειρά από fragments αναγκάζοντας τον σταθμό προορισμού να περιμένει το τελικό κομμάτι της σειράς. Ο προκαθορισμένος χρόνος αναμονής είναι εξήντα δευτερόλεπτα και μπορεί να καταναλώσει πόρους από ενδιάμεσα συστήματα που επανασυνδέουν και ανιχνεύουν πακέτα προς τον τελικό κόμβο προορισμού. Οι επιθέσεις κατακερματισμού μπορεί επίσης να περιλαμβάνουν

εμφωλευμένα κομμάτια ή αλλιώς κομμάτια μέσα σε άλλα κομμάτια, όπου το IPv6 πακέτο έχει πολλαπλές επικεφαλίδες διάσπασης. Άλλες επιθέσεις περιλαμβάνουν την χρήση κατακερματισμού μέσα σε tunnel, προκειμένου οι εξωτερικές IPv6 επικεφαλίδες να μην μπορούν να αντιληφθούν ότι γίνεται χρήση διάσπασης πακέτου εντός του tunnel.

Στο πρωτόκολλο IPv6, ο κατακερματισμός δεν πραγματοποιούνταν ποτέ από τους ενδιάμεσους δρομολογητές παρά μόνο από τους τελικούς κόμβους. Στο IPv6, μόνο στους τελικούς σταθμούς επιτρέπεται να δημιουργούν και να επανασυναρμολογούν κομμάτια. Οι δρομολογητές και τα ενδιάμεσα συστήματα δεν θα πρέπει να δημιουργούν fragments, αλλά χρειάζεται να επιτρέπουν τα τελικά συστήματα να επικοινωνούν με τα κατακερματισμένα πακέτα και να επιτρέπουν στους κόμβους να ανακαλύπτουν το βέλτιστο μέγεθος του πακέτου. Αυτή η αλλαγή που έγινε από το IPv4 στο IPv6 πρωτόκολλο, δημιουργήθηκε επειδή οι σχεδιαστές ανησύχησαν από την επίδραση που είχε ο κατακερματισμός στην απόδοση των ενδιάμεσων δρομολογητών. Τα τελικά συστήματα πρέπει πρώτα να ανακαλύψουν το μέγεθος του πακέτου που μπορεί να μεταδοθεί μεταξύ αυτών ή να συμφωνήσουν στην δημιουργία κατακερματισμού οποιονδήποτε πακέτων είναι μεγαλύτερα από το μέγεθος αυτό. Η διαδικασία αυτή είναι γνωστή με το όνομα Path MTU Discovery(PMTUD), και είναι ένα χαρακτηριστικό που παρέχεται από το πρωτόκολλο IPv6 με το ICMPv6 πρωτόκολλο. Το PMTUD ορίζει την χρήση του ICMPv6 μηνύματος σφάλματος τύπου 2 δηλαδή προειδοποιεί ότι το πακέτο είναι πολύ μεγάλο (ή γενικότερα μεγαλύτερο από την εκάστοτε Path MTU) έτσι ώστε να ενημερωθεί ο ενδιαφερόμενος κόμβος και να μειώσει το μέγεθος των πακέτων που στέλνει.



Εικόνα 5.1: Η διαδικασία κατακερματισμού πακέτου
Πηγή:(http://flylib.com/books/en/1.88.1.18/1/)

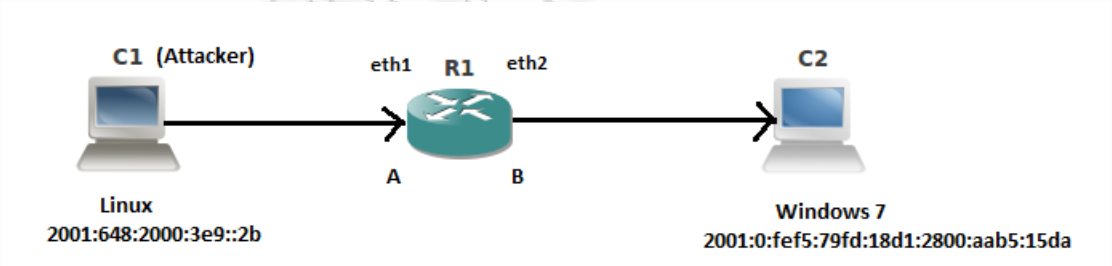
Κατά την διαδικασία κατακερματισμού ενός πακέτου όπως φαίνεται και στην εικόνα 5.1 το αρχικό πακέτο αποτελείται από ένα μέρος που δεν διασπάται και παραμένει και στα διασπώμενα κομμάτια του(unfragmentable part) όπου και περιέχει την επικεφαλίδα IPv6. Τα διασπώμενα μέρη του πακέτου περιέχουν τις άλλες επικεφαλίδες επέκτασης και τα δεδομένα που θέλει να μεταδώσει. Καθένα από τα κομμάτια του πακέτου που έχει κατακερματιστεί περιέχει το μη διασπώμενο μέρος του και την επικεφαλίδα διάσπασης του.

5.4.2 Προσομοίωση Επίθεσης Κατακερματισμού

Στην ενότητα αυτή θα γίνει προσομοίωση και επεξήγηση μιας πιθανής επίθεσης κατακερματισμού. Ο βασικότερος στόχος είναι να κατανοήσουμε πλήρως για το πώς πραγματοποιείται μια τέτοιου είδους επίθεσης αλλά και ποιους σκοπούς εξυπηρετεί. Το στάδιο της υλοποίησης δεν είναι τόσο βαρύνουσας σημασίας όσο στο να καταλάβουμε βαθύτερα τι γίνεται κατά την διάρκεια της επίθεσης κατακερματισμού και με ποιο τρόπο αυτή επιτυγχάνει να προκαλέσει προβλήματα στο δίκτυο.

Το IPv6 ορίζει την απαίτηση για κάθε IPv6 σύνδεσμο να έχει MTU(Maximum Transmission Unit) μεγαλύτερο ή ίσο των 1280 bytes. Έτσι οποιαδήποτε πολύ μικρά κομμάτια-πακέτα θα πρέπει να θεωρούνται ύποπτα και συνεπώς να απορρίπτονται. Επιθέσεις που κάνουν χρήση μεγάλου αριθμού από πολύ μικρά fragments είναι όμοια ύποπτα και θα πρέπει να αποτρέπονται. Γενικότερα στο IPv6, δεν υπάρχει κανένας απολύτως λόγος για να έχεις κομμάτια κατακερματισμένου πακέτου μικρότερα των 1280 bytes εκτός και αν το πακέτο είναι το τελικό fragment και το σύμβολο “m”, μου μας γνωστοποιεί αν υπάρχουν περισσότερα fragments, είναι στην τιμή 0. Τα πολύ μικρά πακέτα μπορεί να χρησιμοποιηθούν από έναν εισβολέα προκειμένου να προωθήσει το περιεχόμενο της επίθεσής σε μεταγενέστερα πακέτα που δεν θα μπορούν να ελεγχτούν από το εκάστοτε firewall. Τα πακέτα αυτά θα μπορέσουν να περάσουν επειδή τα firewall κοιτάνε μόνο την πληροφορία που υπάρχει στο unfragmentable μέρος του πακέτου. Για περισσότερη ασφάλεια, τα firewall πρέπει να απορρίπτουν όλα τα κομμάτια του κατακερματισμένου πακέτου που είναι κάτω από το συγκεκριμένο μέγεθος. Η εξαίρεση πρέπει να γίνεται για το τελευταίο πακέτο , που νόμιμα μπορεί να είναι μικρότερο.

Ο κατακερματισμός χρησιμοποιείται από τους κακόβουλους χρήστες για να «κουκουλώσει» τα δεδομένα τους και έτσι να περάσει από τα firewall η πληροφορία τους. Η επίθεση που προσομοιώνουμε παρακάτω μέσω της χρησιμοποίησης της βιβλιοθήκης scapy της γλώσσας python, γίνεται σε δίκτυο που χρησιμοποιεί το IPv6 πρωτόκολλο για την επικοινωνία και επιτυγχάνεται σε περίπτωση που μιλάμε για non-stateful firewall ή έχουμε απλώς χρήση δρομολογητών. Αρχικά δίνουμε μία εικόνα του δικτύου:



Εικόνα 5.2: Απεικόνιση διαγράμματος δικτύου επίθεσης κατακερματισμού

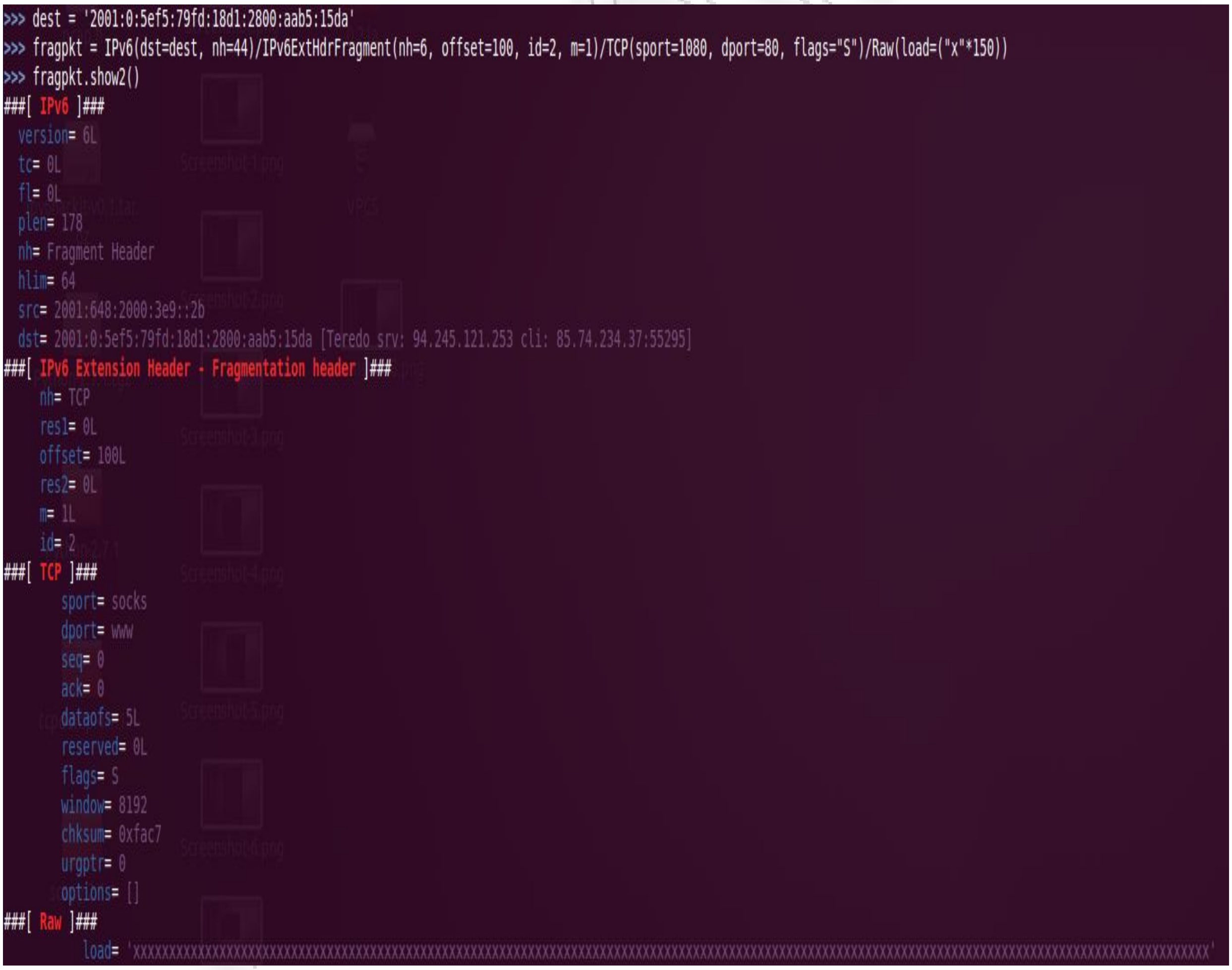
Όπως βλέπουμε από το παραπάνω διάγραμμα ο C1 είναι ο κακόβουλος χρήστης που θα προσπαθήσει να ξεγελάσει το R1 και να περάσει τα κομμάτια του κατακερματισμένου πακέτου που είναι μικρότερα των 1280 bytes στον τελικό του προορισμό που είναι το C2. Έτσι παρακάτω μέσω του scapy δημιουργούμε το κατακερματισμό πακέτου και τα στέλνουμε στον τελικό προορισμό τους. Η επικεφαλίδα IPv6 έχει σε κάθε επόμενη επικεφαλίδα(next header) του την τιμή 44, προκειμένου να υποδεικνύει ότι η επικεφαλίδα του fragment ακολουθάει την

επικεφαλίδα IPv6. Πιο συγκεκριμένα για να δημιουργήσουμε και να τρέξουμε την προσομοίωση μας αρκεί να γράψουμε τις παρακάτω εντολές:

```
>>> dest = '2001:0:5ef5:79fd:18d1:2800:aab5:15da'

>>> fragpkt = IPv6 (dst=dest, nh=44) / IPv6ExtHdrFragment (nh=6,
offset=100, id=2, m=1) /  TCP (sport=1080, dport=80, flags= "S") / Raw
(load=("X" *150))

>>> fragpkt.show2()
```

Πίνακας 5.1 : Εντολές δημιουργίας κατακερματισμού πακέτου

Όπου στο dest συμπληρώνουμε την διεύθυνση του σταθμού προορισμού ενώ στην εντολή fragpkt συμπληρώνουμε όλα εκείνα τα απαραίτητα στοιχεία προκειμένου να δημιουργήσουμε σωστά την διάσπαση του πακέτου. Έτσι τρέχοντας το έχουμε:



Εικόνα 5.3: Δημιουργία κατακερματισμού πακέτων

Στην συνέχεια κάνουμε έναρξη της επίθεσης και βλέπουμε τα αποτελέσματα της. Αυτό επιτυγχάνεται με τις παρακάτω εντολές:

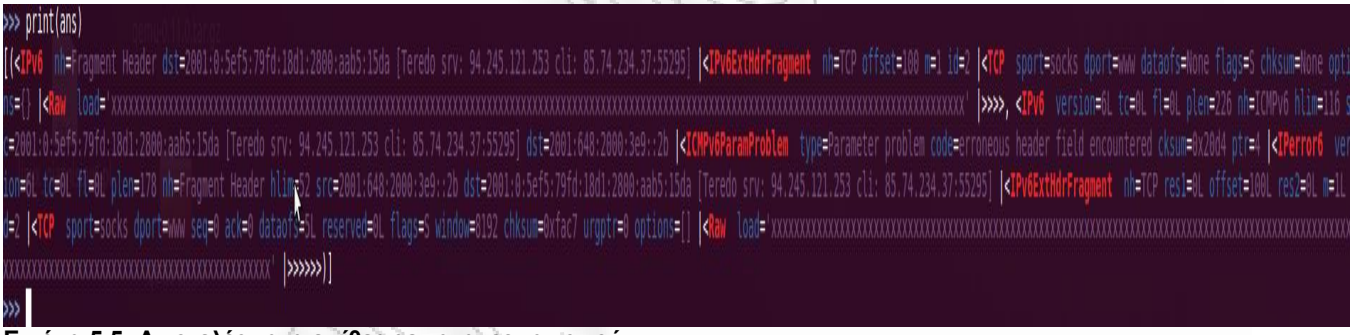
```
>>> ans,  unans = sr(fragpkt)

>>> print (ans)
```

Πίνακας 5.2: Εντολές έναρξης και εμφάνισης αποτελεσμάτων της επίθεσης κατακερματισμού

Δίνοντας έτσι αυτές τιε εντολές έχουμε τα παρακάτω αποτελέσματα:

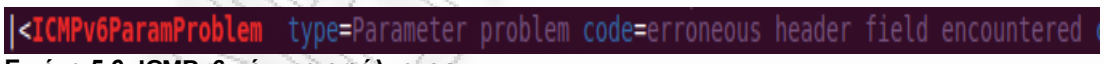
```
>>> ans,unans=sr(fragpkt)
Begin emission:
Finished to send 1 packets.
.....*
Received 6 packets, got 1 answers, remaining 0 packets
```

Εικόνα 5.4: Έναρξη επίθεσης κατακερματισμού



Εικόνα 5.5: Αποτελέσματα επίθεσης κατακερματισμού

Το πακέτο απάντησης που στέλνεται από το τελικό σταθμό είναι ένα ICMPv6 μήνυμα σφάλματος που δείχνει ότι υπάρχει ένα πρόβλημα παραμέτρου εξαιτίας μίας εσφαλμένης επικεφαλίδας. Πιο συγκεκριμένα:

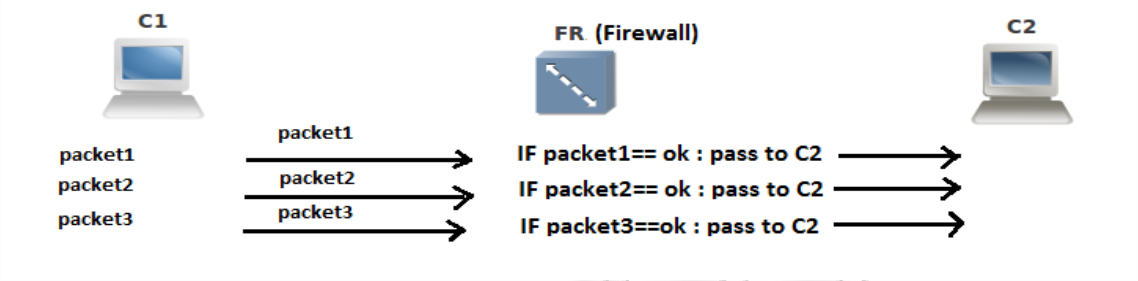


Εικόνα 5.6: ICMPv6 μήνυμα σφάλματος

Το πακέτο είναι λογικό να επιστρέφει ένα πρόβλημα παραμέτρου μιας και είναι μικρότερο των 1280 bytes και δεν είναι το τελικό fragment. Έτσι βλέπουμε ότι η επίθεση επιτυγχάνεται μιας και καταφέρνει να ξεγελάσει το router και το firewall. Οπότε ο εισβολέας σε αυτήν την επίθεση είναι σε θέση να περάσει τα κακόβουλα πακέτα του χωρίς να μπορέσει να εντοπιστεί και να αποτραπεί.

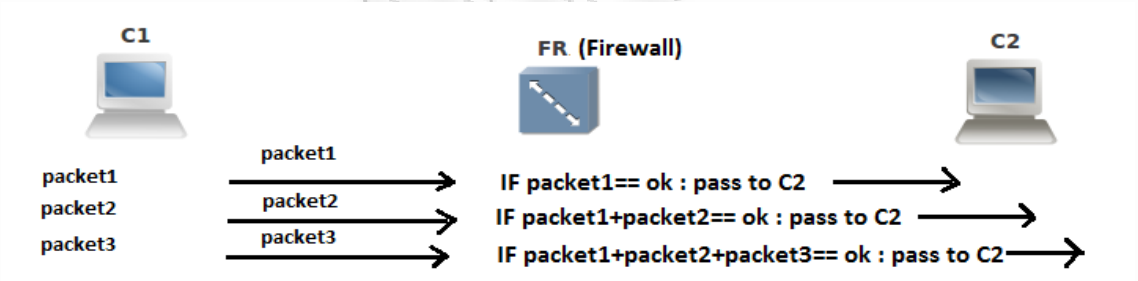
Ωστόσο εδώ θα ήταν καλό να τονίσουμε την διαφορά των αποτελεσμάτων που θα είχαμε μεταξύ σε ένα non-stateful και ένα stateful firewall. Δηλαδή να καταστήσουμε σαφές γιατί η επίθεση κατακερματισμού δεν θα ήταν επιτυχής στην περίπτωση που γινόταν σε ένα stateful firewall σε αντίθεση με αυτήν του non-statefull firewall. Η βασική διαφορά που κρίνει και την

επιτυχία της επίθεσης κρύβεται πίσω από τον τρόπο που το firewall διενεργεί έλεγχο στα πακέτα. Πιο συγκεκριμένα σε έναν non-stateful firewall όπως και στην περίπτωσή μας, το firewall ελέγχει τα πακέτα κάθε φορά που περνάνε από το firewall μεμονωμένα. Έτσι δεν μπορεί να ανιχνεύσει την κακόβουλη πληροφορία που κρύβεται αν αυτά τα κομμάτια-πακέτα (fragments) του κατακερματισμένου πακέτου δεν επανασυνδεθούν. Πιο συγκεκριμένα βλέπουμε την απεικόνιση στο παρακάτω διάγραμμα:



Εικόνα 5.7: Διαδικασία ελέγχου ενός non-stateful firewall

Αντίθετα στην περίπτωση του stateful firewall έχουμε έλεγχο με «διατήρηση μνήμης». Δηλαδή το firewall ελέγχει τα κομμάτια-πακέτα του κατακερματισμένου πακέτου όχι το καθένα μεμονωμένα όπως πριν αλλά αφού το επανασυνδέσει με το fragment που ακολουθεί. Έτσι ουσιαστικά επανασυνδέεται και ελέγχεται ολοκληρωμένο το κατακερματισμένο πακέτο και έτσι μπορεί να ανιχνεύσει τυχόν κακόβουλα δεδομένα που θα μπορούσαν να ανιχνευτούν μόνο στην περίπτωση που επανασυναρμολογούσαμε ολόκληρο το πακέτο ή τα συγκεκριμένα κομμάτια που κρύβουν τα κακόβουλα δεδομένα. Πιο συγκεκριμένα βλέπουμε στην εικόνα 5.8 :



Εικόνα 5.8: Διαδικασία ελέγχου ενός stateful firewall

5.4.3 Τρόπος Αντιμετώπισης των Επιθέσεων Κατακερματισμού

Στην παρούσα ενότητα θα παρουσιαστεί ο τρόπος με την οποία θα μπορέσει να αποτραπεί η παρούσα επίθεση κατακερματισμού. Όταν ένα IPv6 πακέτο ελεγχθεί, η Επόμενη επικεφαλίδα(Next header) της επικεφαλίδας επέκτασης θα πρέπει να περάσει προτού γίνει έλεγχος της επικεφαλίδας Διάσπασης για τον καθορισμό των flags και offset του fragment. Μπορεί να υπάρχουν επιπλέον Επόμενες επικεφαλίδες πριν την UDP ή TCP επικεφαλίδα, για να καθοριστεί εάν περιέχεται αρκετά η επικεφαλίδα ανώτερου επιπέδου πρωτοκόλλου (ULP) εντός του πρώτου κατακερματισμένου πακέτου. Το γεγονός αυτό καθιστά να υπάρχει μία μη

ντετερμινιστική πολιτική ταιριάσματος για το πρώτο κατακερματισμένο πακέτο, η οποία δεν προκαλεί μία ACL ή firewall πολιτική ταιριάσματος ή άδειας του πακέτου. Με πιο απλά λόγια, είναι δύσκολο να «κόψεις» με κάποιο firewall το πρώτο πακέτο, γιατί δεν μπορούμε να γνωρίζουμε την ακριβή του μορφή.

Το router της Cisco που χρησιμοποιήθηκε έχει την δυνατότητα να φιλτράρει την IPv6 κίνηση λόγω του επιπέδου interface που διαθέτει και της υποστήριξης του πρωτοκόλλου IPv6. Αυτό επιτυγχάνεται μέσω του Access Control List (ACL) που είναι εγκατεστημένο στους routers της Cisco και ειδικότερα με την χρήση του ipv6 access λίστας εντολών. Οι ACLs είναι μηχανισμοί ταξινόμησης πακέτων που ορίζουν την κίνηση σε ένα δίκτυο αν θα επιτραπεί ή απαγορευτεί. Το ACL αποτελείται από καταχωρίσεις ελέγχου πρόσβασης (ACE-Access Control Entries), οι οποίες είναι οι ατομικές ρυθμιστικές εντολές εντός της ACL πολιτικής. Συνεπώς, αυτές οι λίστες πρόσβασης αφήνουν τους μηχανισμούς δικτύου να εφαρμόσουν πολιτικές ασφαλείας δικτύου όταν το ACL εφαρμόζεται στο περιβάλλον διαμόρφωσης. Γενικότερα παρέχει όλα τα απαιτούμενα εφόδια στον διαχειριστή δικτύου προκειμένου να ρυθμίσει την κίνηση του δικτύου του και επομένως κατανοώντας την επίθεση να την αποτρέψει χρησιμοποιώντας τις κατάλληλες εντολές.

Το Ipv6 ACL χρησιμοποιεί την λέξη-κλειδί fragments που σημαίνει ότι το ACL ταιριάζει μη αρχικά Ipv6 fragments. Το αρχικό fragment είναι τυπικά το πακέτο που περιέχει την πληροφορία και του επιπέδου 3 (γνωστή και ως επίπεδο δρομολόγησης) και του επιπέδου 4 (επίπεδο μεταφοράς) που βοηθάει στην πολιτική του ταιριάσματος. Η λέξη-κλειδί fragments επίσης ταιριάζει το πρώτο κομμάτι-πακέτο εάν το πρωτόκολλο δεν μπορεί να αποφασίσει επειδή είναι μέσα σε ένα άλλο πακέτο. Το ACL χρησιμοποιεί αυτό το keyword για να επιτρέψει στα noninitial (μη αρχικά) κομμάτια-πακέτου να περάσουν, ακόμα και αν δεν περιέχουν την πληροφορία του επιπέδου 4 (Layer 4 information), που χρησιμοποιείται για να βοηθήσει στις αποφάσεις δρομολόγησης. Τα πιθανά σφάλματα του ACL από την πλευρά της υπερβολικής ανεκτικότητας λόγω του φόβου απόρριψης νόμιμων κατακερματισμένων πακέτων οφείλονται τις περισσότερες φορές εξαιτίας της μη επαρκούς πληροφορίας για την απόφαση εάν θα πρέπει να επιτραπεί ή να απορριφθεί το πακέτο. Αυτό είναι αποδεκτό, επειδή ο τελικός κόμβος που παραλαμβάνει το κομμάτι-πακέτο θα απορρίψει το πακέτο εάν ο σταθμός προορισμού δεν έχει επανασυνδέσει όλα τα κομμάτια. Μόνο εάν όλα τα κομμάτια παρουσιαστούν και υπολογιστούν θα μπορέσει ο κόμβος προορισμού να επανασυνδέσει το πακέτο και θα το αφήσει να περάσει την στοίβα του πρωτοκόλλου Ipv6.

Για να γίνουμε περισσότερο σαφής ως προς την όλη διαδικασία του ACL, αυτό που κάνουμε είναι να δημιουργήσουμε ένα pattern με τα συγκεκριμένα χαρακτηριστικά που θέλουμε. Κάθε ένα πακέτο που περνάει το συγκρίνουμε με τα συγκεκριμένα χαρακτηριστικά και εάν ταιριάζει δεν το αφήνουμε να περάσει. Και αυτό γιατί συνήθως αυτά που γράφουμε στο ACL είναι αυτά που δεν θέλουμε να περνάνε. Σε κάθε άλλη περίπτωση το αφήνουμε να περάσει. Στην συγκεκριμένη περίπτωση το firewall οφείλει να ακολουθεί την παρακάτω λογική προκειμένου να αποφευχθεί η επίθεση:

```
IF m in packet_field != 0 and size of (fragment) < 1280 :
      drop the packet ;
else
      allow;
```

Πίνακας 5.4: Αλγόριθμος για την διαδικασία ελέγχου fragments από το firewall

Δηλαδή εάν δεν είναι το τελευταίο πακέτο και είναι και μικρότερο των 1280 bytes, το firewall (ή router) θα πρέπει να το απορρίψει ενώ σε κάθε άλλη περίπτωση θα πρέπει να το αφήσει να περάσει. Τώρα κάνοντας χρήση του ACL στο interface «giannis» που ρυθμίστηκε στο router (θα δούμε περισσότερες λεπτομέρειες στο παράρτημα ως προς τις ρυθμίσεις που έγιναν στο Cisco router 2800 series) μπλοκάρουμε όλα τα fragments που έρχονται από τον εισβολέα-υπολογιστή. Πιο συγκεκριμένα αυτό επιτυγχάνεται γράφοντας τις παρακάτω εντολές:

```
giannis (config)#  ipv6 acess-list BLOCKFRAGMENTS
giannis (config-ipv6-acl)# permit 88 any any
giannis (config-ipv6-acl)# permit 103 any any
giannis (config-ipv6-acl)# permit icmp any any router-advertisement
giannis (config-ipv6-acl)# permit icmp any any router-solicitation
giannis (config-ipv6-acl)# deny ipv6 any 2001:0:5ef5::/64 fragments
giannis (config-ipv6-acl)# permit ipv6 any any
giannis (config-ipv6-acl)# interface FastEthernet 0/1
giannis (config)# ipv6 traffic-filter BLOCKFRAGMENTS in
```

Πίνακας 5.5: Access List Control για την απόρριψη των fragments

Στο σημείο αυτό θα ήταν καλό να εξηγήσουμε μερικές από τις παραπάνω εντολές προκειμένου να το καταστήσουμε περισσότερο σαφές. Έτσι έχουε:

- ***giannis (config)*** : Είναι το όνομα που έχει δοθεί στο router μετά από τις ρυθμίσεις που έγιναν για την ορθή λειτουργία του.
- ***permit 88 any any*** : Είναι το λεγόμενο permit eigrp για IPv6. Προέρχεται από τα αρχικά Enhanced Interior Gateway Routing Protocol και είναι ένα πρωτόκολλο δικτύου που επιτρέπει στο router να ανταλλάσει πιο αποτελεσματικά πληροφορίες σε σχέση με τα προηγούμενα πρωτόκολλα δικτύου. Χρησιμοποιώντας το EIGRP ο router κρατάει ένα αντίγραφο των πινάκων δρομολόγησης των γειτόνων του. Το EIGRP χρησιμοποιεί τον Diffusing-Update Algorithm (DUAL) προκειμένου να καθορίζει την πιο αποτελεσματική και σύντομη διαδρομή σε έναν προορισμό.
- ***permit 103 any any*** : Αυτό είναι το λεγόμενο permit PIM για IPv6. Προέρχεται από τα αρχικά Protocol Independent Multicast και είναι το πρωτόκολλο που επιτρέπει στους multicast δρομολογητές να εντοπίζουν άλλους multicast δρομολογητές που μπορεί να λαμβάνουν πακέτα.
- ***permit icmp any any* router-advertisement** : Με τον τρόπο αυτό επιτρέπουμε τις διαφημίσεις δρομολόγησης για το πρωτόκολλο ICMP(Internet Control Message Protocol). Κάθε δρομολογητής μεταδίδει περιοδικά ένα Router Advertisement για κάθε μία από τις multicast διεπαφές του, αναγγέλλοντας έτσι την διεύθυνση IP για αυτήν την διεπαφή. Οι σταθμοί ανακαλύπτουν τις διευθύνσεις των γειτονικών δρομολογητών απλά με το άκουσμα τον διαφημίσεων.
- ***permit icmp any any router-solicitation :*** Με τον τρόπο αυτό δίνουμε άδεια στο είδος ενός πακέτου ICMP. Ανήκει και αυτό όπως και το router advertisement στα μηνύματα ανακάλυψης (discovery messages) του δρομολογητή. Βοηθάει και αυτό με την σειρά του στην εύρεση γειτονικών router ή σταθμών.

- ***deny ipv6 any 2001:0:5ef5::/64 fragments :*** Με την εντολή αυτή φράζουμε την κίνηση των fragments από οπουδήποτε δίκτυο προς το δίκτυο με τον κόμβο-στόχο στο 2001:0:5ef5::/64 δίκτυο. Με τον τρόπο αυτό μπλοκάρεται το κατακερματισμένο πακέτο. Βάζουμε όλο το subnet που ανήκει η IP διεύθυνση προκειμένου να προστατέψουμε όλο το subnet.
- ***Interface FastEthernet 0/1 :*** Εδώ αναφέρεται το συγκεκριμένο interface που έχουμε βάλει το access list.

Όπως βλέπουμε παραπάνω αποκλείουμε την διεύθυνση προορισμού και όχι την διεύθυνση του εισβολέα. Θα μπορούσε κάποιος να αναρωτηθεί γιατί δεν μπλοκάρουμε τα πακέτα που έρχονται από τον εισβολέα δηλαδή την IP διεύθυνση του εισβολέα. Η απάντηση σε αυτό το ερώτημα είναι ότι το IP του εισβολέα δεν το γνωρίζουμε πάντα. Γνωρίζουμε όμως πάντα ποια ή ποιες διευθύνσεις θέλουμε να προφυλάξουμε. Για τον λόγο αυτό το γράφουμε έτσι στο Access List.

5.5 Η διαδικασία ρύθμισης του δρομολογητή

Στην παρούσα ενότητα θα γίνει αναφορά σε ένα αρκετά τεχνικό κομμάτι της μεταπτυχιακής διατριβής που ωστόσο παρουσιάζει μεγάλο ενδιαφέρον και έπαιξε καταλυτικό ρόλο στην επίτευξη της προσομοίωσης της επίθεσης που παρουσιάστηκε νωρίτερα. Πιο συγκεκριμένα θα γίνει αναφορά και επεξήγηση των εντολών που χρησιμοποιήθηκαν προκειμένου να ρυθμιστεί κατάλληλα ο δρομολογητής της Cisco μοντέλου series 2800. Μια διαδικασία αρκετά επίπονη και χρονοβόρα για κάποιον που δεν έχει ασχοληθεί με κάποιο παρόμοιο τεχνικό κομμάτι μιας και χρειάζεται ειδικές γνώσεις και χρήση συγκεκριμένων εντολών. Το router αυτό της Cisco είναι ένα configurable μηχάνημα, οπότε κάθε λειτουργία του χρειάζεται ρύθμιση και είναι στα αποκλειστικά χέρια του διαχειριστή. Μέσα στα πλεονεκτήματα που του προσφέρει είναι ότι μπορεί να καθορίσει έτσι όπως ακριβώς επιθυμεί την κίνηση στο δίκτυο του, να το προστατέψει αλλά και έχοντας κάποια βαθύτερη γνώση να αυξήσει την αποδοτικότητά του. Έχοντας το router το δικό του interface παρέχει όλες εκείνες τις ελευθερίες στον διαχειριστεί δικτύου προκειμένου να έχει την πλήρη εποπτεία.
Θα ήταν όμως θεμιτό να αναφέρουμε ότι η χρήση του γίνεται κυρίως στα πλαίσια μεγάλων επιχειρήσεων και όχι για οικιακή χρήση. Ο λόγος του ότι περιέχει πολλές και αρκετά δυσνόητες διαδικασίες διαδικασίες για έναν απλό χρήστη και απαιτεί την χρήση εξειδικευμένων γνώσεων. Ακόμα οι δυνατότητες του προορίζονται για μεγάλη ποσότητα δεδομένων και κίνηση δικτύου.
Τέλος διαθέτει μηχανισμούς ασφαλείας από επιθέσεις που συχνά εντοπίζονται στις μεγάλες επιχειρήσεις και σαφώς επιζητούν πολλές φορές πολύ λεπτούς χειρισμούς.
Τώρα πιο συγκεκριμένα περνώντας στην παρούσα μεταπτυχιακή διατριβή αρχικά εντοπίστηκε το πρόβλημα ότι ο router είχε ήδη χρησιμοποιηθεί και είχε περαστεί ένας κωδικός ο οποίος ήταν άγνωστος. Έτσι χρειάστηκε να ρυθμιστεί από την αρχή και να περαστεί νέος κωδικός. Αυτό επιτεύχθηκε μέσω της παρακάτω εντολής

```
Router(config)# config-register 0x2142
```

Πίνακας 5.6: Εντολή ρύθμισης router από την αρχή

Έπειτα δόθηκε νέος κωδικός και όνομα στο interface προκειμένου να προχωρήσουμε στις περαιτέρω ρυθμίσεις μας με τις παρακάτω εντολές:

```
Router# conf
Router# configure terminal
Router(config)# host
Router(config)# hostname giannis
giannis(config)# enable pas
giannis(config)# enable password giannis
giannis(config)#exit
```

Πίνακας 5.7: Εντολές εκχώρησης ονόματος interface και κωδικού

```
Router#conf
Router#configure termi
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host
Router(config)#hostname giannis
giannis(config)#copy runs
giannis(config)#copy runni
giannis(config)#exit
giannis#co
*Apr 30 11:47:32.259: %SYS-5-CONFIG_I: Configured from console by conso
giannis#copy run
giannis#copy running-config sta
giannis#copy running-config startup-config
Destination filename [startup-config]? startup-config
Building configuration...
[OK]
```

Εικόνα 5.9 : Ρύθμιση και εκχώρηση ονόματος στο interface του router

Με την εντολή “copy run” ζητάμε ό,τι έχουμε κάνει ως εκείνη την στιγμή στο router να το αντιγράψει στο αρχικό configuration που θα τρέχει ο router όταν ξεκινάει.

```
giannis#config
giannis#configure term
giannis#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
giannis(config)#enable sec
giannis(config)#enable pas
giannis(config)#enable password giannis
giannis(config)#exit
giannis#copy run
*Apr 30 11:54:23.931: %SYS-5-CONFIG_I: Configured from console by console
giannis#copy running-config star
giannis#copy running-config startup-config
Destination filename [startup-config]? startup-config
Building configuration...
[OK]
```

Εικόνα 5.10 : Εκχώρηση κωδικού για την εισαγωγή στο interface του router

Στην συνέχεια κάνουμε την λεγόμενη διαμόρφωση εκκίνηση ακολουθίας. Πιο απλά κάνουμε boot(εκκίνηση) τις ρυθμίσεις που πραγματοποιήθηκαν με την παρακάτω εντολή:

```
giannis(config)# config-register 0x2102
```

Πίνακας 5.7: Εντολή διαμόρφωσης εκκίνησης ακολουθίας

Με αυτόν τον τρόπο όλες οι παράμετροι και οι ρυθμίσεις που έχουμε κάνει μέχρι εκείνη την χρονική στιγμή αποθηκεύονται στο router και υπάρχουν κάθε φορά που ξεκινάει η λειτουργία του.

```
giannis#configure term
giannis#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
giannis(config)#config-r
giannis(config)#config-register 0x2102
giannis(config)#exit
giannis#copy ru
*Apr 30 11:55:25.395: %SYS-5-CONFIG_I: Configured from console by consol
% Incomplete command.

giannis#copy run
giannis#copy running-config star
giannis#copy running-config startup-config
Destination filename [startup-config]? startup-config
Building configuration...
[OK]
giannis#
```

Εικόνα 5.11: Εντολές διαμόρφωσης εκκίνησης ακολουθίας

Ακόλουθα ρυθμίζουμε το πρωτόκολλο Telnet προκειμένου να μπορείς να συνδεθείς στο router χωρίς να χρειάζεται μία com port. Με το που εγκατασταθεί ο telnet client στο router, λειτουργεί σαν virtual terminal, και έτσι επιτρέπει την επικοινωνία με το απομακρυσμένο μηχάνημα. Έτσι βλέπουμε παρακάτω την ρύθμισή του:

```
giannis#copy running-config startup-conf
giannis#copy running-config startup-config
Destination filename [startup-config]? startup-config
Building configuration...
[OK]
giannis#show run
giannis#show running-config
Building configuration...

Current configuration : 820 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname giannis
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
```

Εικόνα 5.12: Εντολές ρύθμισης Telnet

Έπειτα προχωράμε σε ρύθμιση της IP address του router:

```
giannis(config)#interf
giannis(config)#interface fas
giannis(config)#interface fastEthernet 0/1
giannis(config-if)#ip add
giannis(config-if)#ip address 192.168.3.2 255.255.255.0
giannis(config-if)#no shu
giannis(config-if)#no shutdown
giannis(config-if)#exit
giannis(config)#s
*Apr 30 12:05:23.407: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to u
giannis(config)#show ip addre
giannis(config)#exit
giannis#show iu
*Apr 30 12:05:34.607: %SYS-5-CONFIG_I: Configured from console by
giannis#show ip add
giannis#show runnin
giannis#show running-config
Building configuration...

Current configuration : 857 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

Εικόνα 5.13: Εντολές ρύθμισης και εκχώρησης της IP address στο router

Τέλος και προκειμένου να επιτύχουμε την επικοινωνία ανάμεσα στα μηχανήματα που υπήρχαν στο δίκτυο έπρεπε να τις ρυθμίσουμε την κάθε μία ξεχωριστά και να τις βάλουμε στο ίδιο υποδίκτυο. Πιο συγκεκριμένα:

```
C1>enable
C1#configure terminal
C1(config)#ipv6 unicast-routing
C1(config)#interface FastEthernet0/1
C1(config)#ipv6 address 2001:648:2000:3e9::2b/64
C1(config)#no shut
C1(config-if)#ipv6 nd prefix 2001:648:2000:3e9::2b/64
C1(config-if)#end
```

Πίνακας 5.8: Εντολές ρύθμισης της IPv6 διεύθυνσης του C1 υπολογιστή

```
C1-ipv6#show run
Building configuration...

Current configuration : 857 bytes
!
version 12.4
hostname C1-ipv6
!
boot system flash
logging buffered 4096 debugging
!
```

```
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
ipv6 unicast-routing
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
!
interface Ethernet0/1
 no ip address
 ipv6 address 2001:648:2000:3e9::2b/64
!
!
ip classless
!
ipv6 router rip 6bone
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
!
end
```

Πίνακας 5.9: Ολοκλήρωση ρύθμισης της IPv6 διεύθυνσης του C1 μηχανήματος

Η ίδια αντίστοιχη διαδικασία γίνεται και για το μηχάνημα C2. Και έτσι έχουμε επίτευξη της IPv6 εεπικοινωνίας μεταξύ των δύο υπολογιστών C1 και C2 :

```
C1#ping ipv6 2001:0:5ef5:79fd:18d1:2800:aab5:15da source
FastEthernet0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:0:5ef5:79fd:18d1:2800:aab5:15da, timeout is 2 seconds:
Packet sent with a source address of 2001:648:2000:3e9::2b!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/77/268
ms
C1#
```

Πίνακας 5.9: Επίτευξη IPv6 επικοινωνίας μεταξύ των υπολογιστών C1 και C2

ΚΕΦΑΛΑΙΟ 6

Συμπεράσματα

Η μεταπτυχιακή αυτή διατριβή ασχολείται με το θέμα της ασφάλειας της νεότερης έκδοσης του πρωτοκόλλου IP, του IPv6. Εξετάζει την υπάρχουσα δομή του, τους λόγους που καθιστούν αναγκαία την μετάβασή του από το πρωτόκολλο IPv4, την γενικότερη ασφάλεια που προσφέρει αλλά και τους κινδύνους που ελλοχεύουν από τις επιθέσεις που δέχεται από κακόβουλους χρήστες. Αποτελεί σταθμό και ακρογωνιαίο λίθο όχι μόνο για την συνέχιση της διαδικτυακής επικοινωνίας αλλά και για την ίδια την ύπαρξη του Διαδικτύου, με ότι αυτό συνεπάγεται.

Το πρωτόκολλο IPv6 βρίσκεται ακόμα σε μεταβατικό στάδιο ωστόσο η ανάγκη εγκαθίδρυσής του καθίσταται επιτακτική. Λόγοι αναβάθμισης υπηρεσιών, υποστήριξης κινητών χρηστών, έλλειψης απόδοσης διευθύνσεων από το προγενέστερο πρωτόκολλο, αυτόματης ρύθμισης διευθύνσεων και ευκολίας διαχείρισης δικτύου είναι μερικοί από τους πιο σημαντικούς λόγους για την μετάβαση αυτή. Ωστόσο το θέμα της ασφάλειας που παρέχει είναι αυτό που αποτελεί και το σημαντικότερο σημείο έρευνας και στην μεταπτυχιακή αυτή διατριβή εξετάστηκε ενδελεχώς προκειμένου να διασαφηνιστούν ορισμένα κρίσιμα ζητήματα ασφαλείας αλλά και για να εξαχθούν χρήσιμα συμπεράσματα.

Ένα από τα γενικά συμπεράσματα που μπορούν να ειπωθούν είναι ότι το πρωτόκολλο IPv6 κρατάει τα περισσότερα από τα θετικά χαρακτηριστικά του IPv4, ορισμένα αυτούσια και άλλα μερικώς τροποποιημένα, και αφαιρεί όλα εκείνα που αποτελούν τροχοπέδη στην απόδοση και την ασφάλεια. Δεν σχεδιάστηκε εξολοκλήρου από την αρχή αλλά βασίστηκε στο προγενέστερό του και στην εμπειρία που είχε αποκομισθεί από αυτό. Παρόλα αυτά τα νέα χαρακτηριστικά του IPv6 θα απαιτήσουν νέες λύσεις που θα βοηθήσουν στην προστασία της επόμενης γενιάς δικτύων.

Το θέμα της ασφάλειας του πρωτοκόλλου IPv6 είναι πολύ μεγάλο, με πολλές προεκτάσεις και πολύπλοκα τεχνικά χαρακτηριστικά και είναι δύσκολο στα πλαίσια μιας μεταπτυχιακής διατριβής να καλυφθεί πλήρως. Ωστόσο έγινε μια σημαντική προσπάθεια προκειμένου ο αναγνώστης να πάρει μια σημαντική γεύση για το τι μπορεί να προσφέρει η νέα έκδοση πρωτοκόλλου σε θέμα ασφάλειας και τους κινδύνους που υπάρχουν. Το IPv6 σχεδιάστηκε έτσι ώστε να μπορεί να αντιμετωπίσει πιο αποτελεσματικά τις εκάστοτε επιθέσεις και να δώσει μεγαλύτερη ευκολία στου διαχειριστές δικτύων.

Πολλά θέματα ασφαλείας που υπάρχουν σήμερα θα συνεχίσουν να υπάρχουν και μετά την μετάβαση στο πρωτόκολλο IPv6. Το IPv6 έχει ορισμένα μοναδικά χαρακτηριστικά που το καθιστούν πιο ασφαλή από το IPv4. Επίσης το IPv6 αλλάζει τον τρόπο με τον οποίο επικοινωνούμε, και οι αρχιτεκτονικές ασφαλείας μας θα πρέπει να υιοθετήσουν αυτές τις αλλαγές. Τα νέα προϊόντα ασφαλείας IPv6 βελτιώνουν και βοηθούν στην ασφαλή μετάβαση του. Το πιο σημαντικό ωστόσο από όλα είναι να συνεχίσουμε να μαθαίνουμε όσα περισσότερα μπορούμε για το πρωτόκολλο IPv6. Η συνεχής ενημέρωση και ασχολία είναι αυτή που θα μας επιτρέψει να προστατέψουμε το IPv6 δίκτυό μας αποτελεσματικά. Τέλος αξίζει να τονίσουμε ότι το πρωτόκολλο IPv6 συνεχίζει ακόμα και σήμερα να ερευνάται και να εξετάζεται και η μετάβαση θα είναι μια δύσκολη όσο και χρονοβόρα διαδικασία. Οι νέες δυνατότητες, μέθοδοι και χαρακτηριστικά που προσφέρει στον χώρο της ασφάλειας κρίνονται απαραίτητα για την βιωσιμότητα και εξέλιξη των δικτύων και του Διαδικτύου γενικότερα.

Βιβλιογραφία

[1] C. Bouras, P. Ganos, A. Karaliotas, “Transition Strategies from IPv4 to IPv6: The case of GRNET”, 3rd International Network Conference-INC 2002, Plymouth, UK, July 16-18 2002

[2] Internet Engineering Task Force RFC 2529 “Transmission of IPv6 over IPv4 Domains without Explicit Tunnels” B. Carpenter, C. Jung, March 1999

[3] R. Gilligan, E. Nordmark, Internet Engineering Task Force RFC 2893, “Transition Mechanisms for IPv6 Hosts and Routers”, August 2000

[4] R. Hinden, S. Deering, “RFC 2373 IP Version 6 Addressing Architecture”, July 1998

[5] A. Conta, S. Deering, M. Gupta, “RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)”, March 2006

[6] T. Narten, E. Nordmark, W. Simpson, H. Soliman, J. Tatuya, “Neighbor Discovery for IP version 6 (IPv6)”, Internet Draft, October 2003

[7] Popoviciu C.; Levy-Avegnoli, E.; Grossetete, P., Deploying IPv6 Networks, Cisco Press, Indianapolis, IN, 2006

[8] Szigeti, S.; Risztics, P., "Will IPv6 bring better security?,” Proceedings 30th Euromicro Conference, 2004, 31 Aug.-3 Sept. 2004

[9] Kent, S.; Seo, K., “Security Architecture for the Internet Protocol,” RFC 4301, Dec. 2005

[10] Friedl, S., “An illustrated Guide to IPSec,” Unixwiz.net, Aug. 2005

[11] J. Mohacsi, “IPv6 firewalls”, presentation on the 5th TF-NGN meeting, October 2001

[12] M. H. Warfield, “Security Implications of IPv6”, Internet Security Systems, March 2003

[13] A. Martelli, “Python in a Nutshell”, O'Reilly Media, August 2003

[14] C. Huitema, “Teredo: Tunneling IPv6 over UDP through network address translations (NATs),” IETF RFC 4380, February 2006

[15] J. Rosenberg *et al.*, “STUN - simple traversal of user datagram protocol (UDP) through network address translators (NATs),” IETF RFC 3489, March 2003

[16] S. Convery and D.Miller, “IPv6 and IPv4 threat comparison and best-practice evaluation,” http://seanconvery. com/v6-v4-threats.pdf, March 2004

[17] P. Biondi and A. Ebalard, “Ipv6 fragmentation header security,” in *CanSecWest Security Conference*, April 2007

[18] E. Nordmark and R. Gilligan, “Basic transition mechanisms for IPv6 hosts and routers,” IETF RFC 4213, October 2005

[19] S. Thomson and T. Narten, IPv6 Stateless Address Autoconfiguration, RFC2462, Internet Engineering Task Force, December 1998

[20] S. Hogg, E. Vyncke, “IPv6 Security”, Cisco Press, April 2009

[21] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315, Internet Engineering Task Force, July 2003

[22] T. Narten, E. Nordmark, W. Simpson, H. Soliman, RFC 4861 - Neighbor Discovery for IP version 6 (IPv6), 2007

[23] E. Vyncke, C. Paggen, “LAN Switch Security”, Cisco Press, March 2007

[24] B. Burns, J. Granick, S. Manzuik, “Security Power Tools”, O'Reilly Media, September 2007

[25] S. Thomson and T. Narten. “IPv6 Stateless Address Autoconfiguration” RFC 2462, Internet Engineering Task Force, December 1998

[26] G. Van de Velde, ”Local Network Protection for IPv6”, IETF RFC 4684, May 2007

[27] T. Doan, “IPv6 Security Assessment”, June 2006