Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. "Ασφάλεια Ψηφιακών Συστημάτων"

Διπλωματική Εργασία

"Ζητήματα Ασφάλειας στο πρωτόκολλο IPv6"

Ευάγγελος Θ. Όθων

Επιβλέπων: Επίκουρος Καθηγητής κ. Κωνσταντίνος Λαμπρινουδάκης

Πειραιάς, Απρίλιος 2013

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα της μεταπτυχιακής διπλωματικής μου εργασίας, Επίκουρο Καθηγητή κ. Κωνσταντίνο Λαμπρινουδάκη, για την δυνατότητα που μου προσέφερε να ασχοληθώ με αυτό το ενδιαφέρον και σύγχρονο θέμα, όπως και για την πολύτιμη βοήθεια που μου παρείχε καθ' όλη την διάρκεια εκπόνησης της διπλωματικής εργασίας.

Περίληψη

Το πρωτόκολλο IPv6, η νέα έκδοση του διαδικτυακού πρωτοκόλλου IP, αναπτύχθηκε με σκοπό να αντικαταστήσει το προγενέστερο πρωτόκολλο IPv4, παρέχοντας νέες υπηρεσίες και υποστηρίζοντας την ανάπτυξη του Διαδικτύου. Παρόλο που το IPv6 παρέχει αρκετές βελτιώσεις σχετικά με την ταχύτητα δρομολόγησης, την ποιότητα υπηρεσίας δικτύου (QoS) και την αντιμετώπιση σημαντικών ζητημάτων ασφάλειας στο IPv4, φέρνει νέες προκλήσεις στο προσκήνιο. Οι υπηρεσίες και τα πρωτόκολλα που προσφέρει, παρουσιάζουν νέες ευπάθειες, οι οποίες ευνοούν την επίτευξη νέων επιθέσεων. Τα προβλήματα ασφάλειας γίνονται ακόμα πιο κρίσιμα, αν αναλογιστούμε την υποχρεωτική συνύπαρξη των δύο πρωτοκόλλων για μεγάλο χρονικό διάστημα. Οι σχεδιαστικές προκλήσεις που παρουσιάζουν τα ήδη υπάρχοντα μέτρα προστασίας για την προσαρμογή τους στο νέο πρωτόκολλο είναι μεγάλες. Όπως μεγάλες είναι και οι απαιτήσεις για την σχεδίαση και υλοποίηση νέων μέτρων ασφάλειας. Τελικά, ποιο από τα δύο πρωτόκολλα είναι πιο ασφαλές; Υπάρχει απάντηση;

Λέξεις Κλειδιά: IPv6, επιθέσεις, μέτρα προστασίας, IPsec, SEND, Firewalls, Easy-SEND, THC-IPv6-Attack-Toolkit

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

1

Εισαγωγή

Την δεκαετία του 70 όταν πραγματοποιήθηκε ο σχεδιασμός και η υλοποίηση του πρωτοκόλλου IPv4, κανείς δεν μπορούσε να φανταστεί την αυξανόμενη ζήτηση σε παγκόσμιες διευθύνσεις IP. Η ζήτηση αυτή προέκυψε λόγω της μετατροπής του διαδικτύου από ένα μικρό ερευνητικό δίκτυο σε ένα πολυπληθές παγκόσμιο δίκτυο. Αρχικά, το IPv4 ανταποκρινόταν με επιτυχία στις απαιτήσεις του διαδικτύου, όντας ένα πρωτόκολλο ιδιαίτερα εύρωστο και εύκολα υλοποιήσιμο. Ωστόσο, αποτέλεσε θύμα της δικής του επιτυχίας, με αποτέλεσμα την τεράστια ζήτηση IP διευθύνσεων και κατ' επέκταση την συνεχόμενη εξάντληση του χώρου διευθύνσεων. Έτσι οι ερευνητές οδηγήθηκαν στην ανάγκη σχεδιασμού και ανάπτυξης ενός νέου πρωτοκόλλου, καθώς οι μελλοντικές απαιτήσεις για IP διευθύνσεις είναι τεράστιες[1]. Ήδη, από το 1990 είχαν ξεκινήσει οι έρευνες για τον σχεδιασμό ενός νέου πρωτοκόλλου, με αποτέλεσμα το 1998 να γίνει η εισαγωγή του λεγόμενου IPv6 πρωτοκόλλου[2].

1.1 Αντικείμενο μεταπτυχιακής εργασίας

Η παρούσα μεταπτυχιακή διπλωματική εργασία αποσκοπεί στην μελέτη των ζητημάτων ασφάλειας που αφορούν το νέο πρωτόκολλο δικτύου, το IPv6, δίνοντας έμφαση στις επιθέσεις και στα μέτρα προστασίας.

Στόχος είναι να περιγραφούν εις βάθος όλες οι κατηγορίες επιθέσεων που μπορούν να επιτευχθούν στο IPv6. Συγκεκριμένα, θα γίνει θεωρητική μελέτη των επιθέσεων που αποσκοπούν στην εκμετάλλευση των αδυναμιών των νέων λειτουργιών που φέρει το IPv6. Επίσης, θα μελετηθούν επιθέσεις που εμφανίζονται και στα δύο πρωτόκολλα (IPv4 – IPv6), αλλά με διαφορετική μορφή. Επιπλέον, θα γίνει σύντομη περιγραφή των επιθέσεων εκείνων που δεν εμφανίζουν καμία διαφορά στα δύο πρωτόκολλα. Τέλος, θα μελετηθούν εις βάθος επιθέσεις που οφείλονται στην συνύπαρξη των δύο πρωτοκόλλων. Όσον αφορά το τεχνικό κομμάτι των επιθέσεων, θα γίνει επίδειξη αυτών με κατάλληλο εργαλείο.

Σχετικά με τα μέτρα προστασίας, στόχος είναι η θεωρητική μελέτη των μέτρων ασφάλειας που μπορούν να χρησιμοποιηθούν για να μετριάσουν ή αντιμετωπίσουν τις επιθέσεις. Θα μελετηθούν τρία μέτρα προστασίας, δύο από τα οποία είναι ήδη γνωστά στο

[1] Υπάρχουν ιδέες για χρήση των IP διευθύνσεων σε τεχνολογίες RFID, οικιακές συσκευές, όπως τηλεοράσεις αλλά και σε PDA , κινητά τηλέφωνα [1].

[2] Επίσης, καλείται IPng: IP next generation.

IPv4, δίνοντας έμφαση στις αλλαγές που πρέπει να γίνουν στο νέο πρωτόκολλο IPv6. Όσον αφορά το τεχνικό κομμάτι των μέτρων προστασίας, θα παρουσιαστεί πρακτική εφαρμογή δύο εξ' αυτών με χρήση κατάλληλων εργαλείων και εφαρμογών.

1.2 Εύρος και όρια μεταπτυχιακής εργασίας

Η παρούσα μεταπτυχιακή εργασία περιλαμβάνει όλες τις επιθέσεις του IPv6 που έχουν περιγραφεί στην διεθνή βιβλιογραφία τα τελευταία δέκα χρόνια. Επιπλέον, περιλαμβάνει τα σημαντικότερα μέτρα ασφάλειας που έχουν προταθεί από την διεθνή κοινότητα της ασφάλειας πληροφοριακών συστημάτων.

Η εκπόνηση της μεταπτυχιακής εργασίας έγινε στο χρονικό διάστημα μεταξύ Νοέμβριου 2012 και Απρίλιου 2013. Για την θεωρητική μελέτη χρησιμοποιήθηκε μεγάλος αριθμός δημοσιεύσεων, βιβλίων και πηγών από το διαδίκτυο (άνω των 50). Για την τεχνική μελέτη χρησιμοποιήθηκε εικονικό περιβάλλον από υπολογιστές με τα εξής λειτουργικά συστήματα: Ubuntu 12.04, Windows XP SP2, Backtrack 5 R3. Επιπλέον, χρησιμοποιήθηκαν ειδικά εργαλεία, όπως το THC-IPv6-Attack-Toolkit και εφαρμογές όπως το Easy-SEND, οι οποίες θα παρουσιαστούν παρακάτω.

1.3 Οργάνωση κειμένου

Η παρούσα εργασία αποτελείται από 15 κεφάλαια.

Στο κεφάλαιο 2 περιγράφονται τα προβλήματα που παρουσιάζει το πρωτόκολλο IPv4 και γίνεται μια σύντομη εισαγωγή στο πρωτόκολλο IPv6, δίνοντας έμφαση στην σύγκρισή του με το προγενέστερο πρωτόκολλο.

Στο κεφάλαιο 3 περιγράφονται οι τύποι διευθύνσεων στο IPv6 και αναφέρονται τα νέα πρωτόκολλα που αυτό φέρει.

Στο κεφάλαιο 4, γίνεται μελέτη των επιθέσεων που εκμεταλλεύονται τις αδυναμίες των νέων πρωτοκόλλων που φέρει το IPv6.

Στο κεφάλαιο 5, αναλύονται οι επιθέσεις που εμφανίζονται και στα δύο πρωτόκολλα, ωστόσο παρουσιάζουν σημαντικές διαφορές ως προς την μέθοδο και ευκολία/δυσκολία επίτευξης.

Στο κεφάλαιο 6, γίνεται σύντομη περιγραφή των επιθέσεων που εμφανίζονται και στα δύο πρωτόκολλα, χωρίς να παρουσιάζουν σημαντικές διαφορές.

Στο κεφάλαιο 7, γίνεται μελέτη των μηχανισμών μετάβασης από το IPv4 στο IPv6, δίνοντας ιδιαίτερη έμφαση στα ζητήματα ασφάλειας που αφορούν τους tunneling μηχανισμούς.

Στο κεφάλαιο 8, παρουσιάζεται το Internet Protocol Security (IPsec).

Στο κεφάλαιο 9, εφαρμόζεται το IPsec σε ένα εικονικό περιβάλλον από μηχανές Windows XP S2.

Στο κεφάλαιο 10, παρουσιάζονται οι σχεδιαστικές προκλήσεις των Firewalls και IDSs σε IPv6 περιβάλλοντα.

Στο κεφάλαιο 11, μελετάται το Secure Neighbor Discovery (SEND) πρωτόκολλο, δίνοντας έμφαση στις Cryptographically Generated Addresses (CGA).

Στο κεφάλαιο 12, γίνεται υλοποίηση του SEND, μέσω της εφαρμογής Easy-SEND.

Στο κεφάλαιο 13, υλοποιούνται επιθέσεις στο πρωτόκολλο IPv6, κάνοντας χρήση του εργαλείου THC-IPv6-Attack-Toolkit.

Στο κεφάλαιο 14, καταγράφονται τα συμπεράσματα που προκύπτουν ενώ στο κεφάλαιο 15 καταγράφονται οι βιβλιογραφικές πηγές.

2

Εισαγωγή στο πρωτόκολλο IPv6

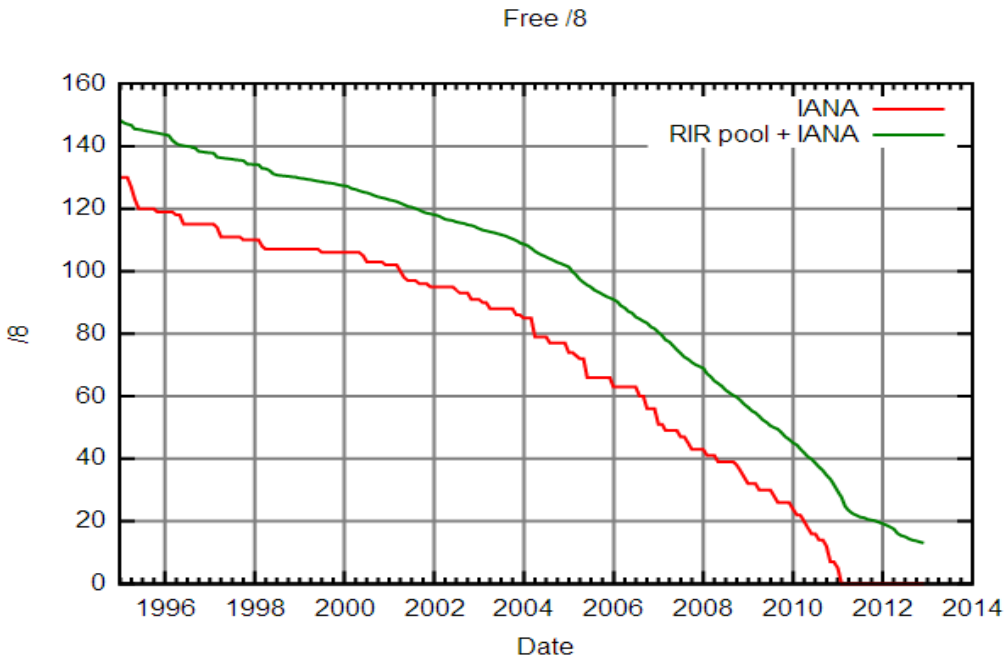
Το πρωτόκολλο IPv6[3] αποτελεί την νέα έκδοση πρωτοκόλλου σε επίπεδο δικτύου, αναπτύχθηκε από την κοινότητα IETF(Internet Engineering Task Force) και εμφανίστηκε στην παγκόσμια κοινότητα αρχικά το 1995 και σε τελική μορφή το 1998 (περιγράφεται στο έγγραφο RFC 2460). Με την χρήση του IPv6, προσδοκάται η βελτίωση αρκετών υπηρεσιών του IPv4, η προσφορά νέων υπηρεσιών, η λύση ορισμένων προβλημάτων και ιδιαίτερα η παροχή μεγαλύτερης ασφάλειας στο διαδίκτυο [2].

Βέβαια, υπάρχουν απόψεις με αρνητική στάση απέναντι στην υιοθέτηση του νέου πρωτοκόλλου, καθώς θεωρείται αποτυχημένο και ότι δεν παρέχει κανένα πλεονέκτημα σε σύγκριση με το προγενέστερο πρωτόκολλο. Ωστόσο, η αποδοχή του νέου πρωτοκόλλου είναι αναπόφευκτη και σε πολλές χώρες, κυρίως Ευρωπαϊκές και Ασιατικές, η μετανάστευση από το IPv4 στο IPv6 αποτελεί εθνική προτεραιότητα [2]. Όπως έχει γίνει κατανοητό το IPv6 αναπτύχθηκε για την αντιμετώπιση ορισμένων προβλημάτων του IPv4 και για παροχή νέων πρωτοκόλλων και λειτουργιών. Παρακάτω γίνεται αναφορά στα προβλήματα του IPv4.

2.1 Προβλήματα που παρουσιάζει το IPv4

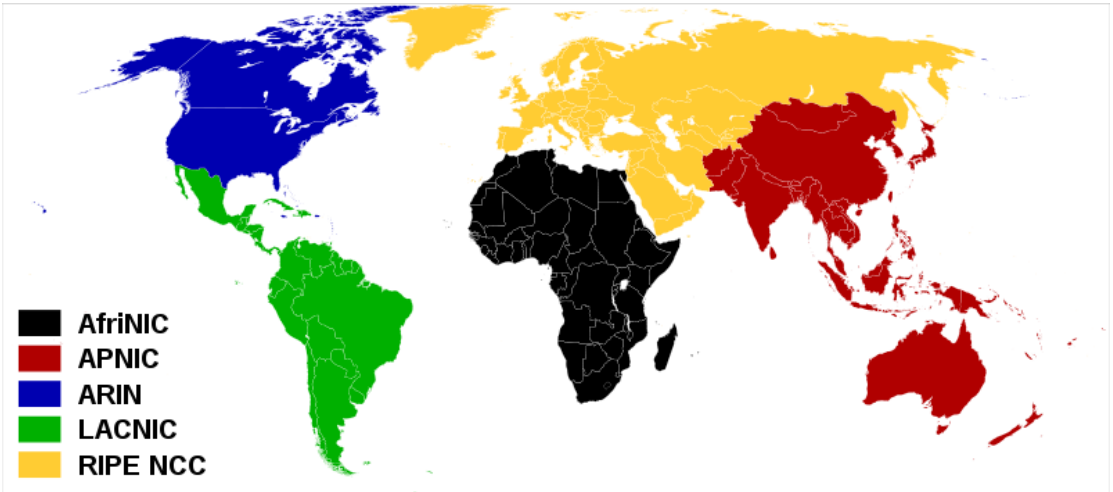
Ο βασικότερος παράγοντας της ανάπτυξης του πρωτοκόλλου IPv6 ήταν η συνεχής εξάντληση του χώρου διευθύνσεων που προσφέρει το πρωτόκολλο IPv4 [3] (2^{32} διαθέσιμες διευθύνσεις). Η παγκόσμια αρχή ανάθεσης IP διευθύνσεων – Internet Assigned Numbers Authority (IANA), διαμοίρασε στις 31 Ιανουαρίου 2011 την τελευταία IPv4 διεύθυνση σε έναν από τους πέντε περιφερειακούς καταχωρητές διαδικτύου – Regional Internet Registries (RIR). Στην Εικόνα 2.1 γίνεται σύγκριση μεταξύ του IANA και των πέντε RIR σχετικά με τον διαμοιρασμό διευθύνσεων.

[3] Το πρωτόκολλο IPv5 αναπτύχθηκε για πειραματικό σκοπό



Εικόνα 2.1: Εξάντληση IPv4 διευθύνσεων από το 1995

Στην Εικόνα 2.2 φαίνονται οι πέντε RIR. Ήδη, δύο από τους πέντε καταχωρητές έχουν διαμοιράσει όλες τις IPv4 διευθύνσεις τους. Συγκεκριμένα, ο καταχωρητής της Ασίας/Αυστραλίας (APNIC) στις 15 Απριλίου 2011 και ο καταχωρητής της Ευρώπης/Κεντρικής Ασίας (RIPE NCC) στις 14 Σεπτεμβρίου 2012 [27]. Αναμένεται τα επόμενα χρόνια και οι υπόλοιποι καταχωρητές να εξαντλήσουν τις IPv4 διευθύνσεις τους.



Εικόνα 2.2: Regional Internet Registries

Η αρχική μέθοδος που χρησιμοποιήθηκε για την διανομή των διευθύνσεων (class – based σχεδιασμός), είχε ως αποτέλεσμα μια μη αποδοτική χρήση του χώρου διευθύνσεων.

Νέες μέθοδοι παρουσιάστηκαν, όπως το NAT (Network Address Translation) με σκοπό να απαλύνουν το πρόβλημα μείωσης των διαθέσιμων διευθύνσεων [3]. Παρόλο το γεγονός, ότι το NAT αποτέλεσε μια σημαντική (προσωρινή[4]) λύση, είχε το μειονέκτημα ότι "έκοβε" την από άκρη σε άκρη (end-to-end) συνδεσιμότητα μεταξύ των υπολογιστών/συστημάτων ενός ιδιωτικού δικτύου και εκείνων που βρίσκονταν στο διαδίκτυο. Έτσι το NAT έπρεπε να διαχειριστεί τις προκλήσεις που προέρχονταν από εφαρμογές που απαιτούσαν από άκρη σε άκρη επικοινωνία [2]. Ωστόσο, η ρήξη της end-to-end συνδεσιμότητας είχε θετικό αποτέλεσμα όσον αφορά στην ασφάλεια, καθώς έκρυβε το εσωτερικό – ιδιωτικό δίκτυο από το εξωτερικό δίκτυο.

Επιπλέον, το IPv4 σχεδιάστηκε για να χρησιμοποιηθεί σε ένα "φιλικό" περιβάλλον, χωρίς να υπάρχουν σκέψεις σχετικά με το επίπεδο ασφάλειας. Με την αύξηση των κόμβων στο διαδίκτυο, το περιβάλλον άρχισε να γίνεται εχθρικό, με αποτέλεσμα διάφορες εφαρμογές να επιτάσσουν την ανάγκη για ένα ορισμένο επίπεδο ασφάλειας. Ενώ σχεδιάστηκαν λύσεις ασφάλειας για το επίπεδο μεταφοράς – εφαρμογών (όπως το Secure Sockets Layer), δεν υπήρχε κάτι παρόμοιο στο επίπεδο δικτύου [2,3].

Η διαμόρφωση και διαχείριση (configuration – management) των IPv4 δικτύων αποτελεί ένα ακόμη σημαντικό πρόβλημα, καθώς οι συγκεκριμένες λειτουργίες είναι ιδιαίτερα επιρρεπείς σε λάθη και απαιτούν συνεχώς την ανθρώπινη παρέμβαση. Τα λάθη διαμόρφωσης (όπως για παράδειγμα address collisions) που προκαλούνται μέσα σε ένα IPv4 δίκτυο δίνουν την ευκαιρία για επίτευξη διαφόρων ειδών επιθέσεων [3].

Μερικές εφαρμογές, που χαρακτηρίζονται από μετάδοση ήχου ή βίντεο απαιτούν μια ιδιαίτερη υποστήριξη από τα δίκτυα, με σκοπό την διατήρηση ορισμένων σημαντικών παραμέτρων, όπως η καθυστέρηση και το jitter[5] μέσα σε συγκεκριμένα όρια. Το IPv4 έχει περιορισμένες δυνατότητες όσον αφορά στην υποστήριξη Quality of Service (QoS) χαρακτηριστικών [3]. Τέλος, σημαντικό ζήτημα αποτελεί η συνεχής μεγέθυνση των πινάκων δρομολόγησης, με αποτέλεσμα την μειωμένη ταχύτητα δρομολόγησης και κατά συνέπεια την χαμηλή απόδοση του δικτύου [4].

Όταν πρωτοεμφανίστηκε το πρωτόκολλο IPv4, χρησιμοποιήθηκε κυρίως για ερευνητικούς και αναπτυξιακούς λόγους, με αποτέλεσμα να μην δοθεί ιδιαίτερη σημασία σε θέματα ασφάλειας. Έτσι, το IPv4 σχεδιάστηκε με ελάχιστες επιλογές για παροχή ασφάλειας και αυτό είχε ως αποτέλεσμα η ασφάλεια να υλοποιείται στα παραπάνω επίπεδα (επίπεδα μεταφοράς , εφαρμογής).

2.2 Αλλαγές και Βελτιώσεις που παρουσιάζει το IPv6

Το πρόβλημα εξάντλησης του χώρου των IPv4 διευθύνσεων, υπήρξε το βασικό κίνητρο για τον σχεδιασμό και την υλοποίηση του πρωτοκόλλου IPv6. Το νέο πρωτόκολλο έφερε μια σειρά από αλλαγές και βελτιώσεις. Παρακάτω γίνεται μια αναφορά σε αυτές τις αλλαγές – βελτιώσεις.

[4] Ο αριθμός των χρηστών με xDLS ή mobile GPRS αυξάνεται συνεχώς, καθιστώντας το NAT προσωρινή λύση

[5] Στιγμιαίες αποκλίσεις καθοριστικών τμημάτων ενός ψηφιακού σήματος σε σχέση με τις ιδανικές θέσεις τους στο χρόνο. (ορισμός από τον διεθνή οργανισμό τηλεπικοινωνιών)

- Σε αντίθεση με τις IPv4 διευθύνσεις, οι οποίες δεσμεύουν 32 bits, οι IPv6 διευθύνσεις αποτελούνται από 128 bits. Έτσι το IPv6 παρέχει 3.4×10^{38} διευθύνσεις[6], αριθμός που μπορεί να καλύψει τις ανάγκες των επόμενων τουλάχιστον 50 χρόνων [5]. Επίσης, με την χρήση του IPv6 εξαλείφεται η ανάγκη για χρήση τεχνικών, όπως το NAT επιτρέποντας την από "άκρη σε άκρη" επικοινωνία [2].
- Το IPv6 προσφέρει καλύτερη διαχείριση του χώρου διευθύνσεων σε σχέση με το IPv4. Η χρήση των 128 bits, επιτρέπει την δημιουργία μιας ιεραρχίας διευθύνσεων, καθιστώντας πιο ευέλικτη την διευθυνσιοδότηση αλλά και την δρομολόγηση [5]. Έτσι ο σχεδιαστής ενός δικτύου έχει την δυνατότητα να αναθέσει παγκόσμιες (global unicast) διευθύνσεις μόνο στις συσκευές που επιθυμούν να επικοινωνήσουν με το διαδίκτυο, ενώ μπορεί να αναθέσει τοπικές (site local) διευθύνσεις σε συσκευές που χρειάζεται να επικοινωνήσουν μόνο εντός του δικού τους δικτύου.
- Η κεφαλίδα ενός πακέτου IPv6 (IPv6 datagram header) είναι εντελώς διαφορετική σε σχέση με αυτή του IPv4. Πολλά πεδία της κεφαλίδας του IPv4, όπως το checksum, IHL, identification flag και fragment offset δεν εμφανίζονται στην κεφαλίδα του νέου πρωτοκόλλου, καθιστώντας την ιδιαίτερα απλή [6].
- Το πρωτόκολλο IPv6 παρέχει νέους Extension Headers[7], καθιστώντας το ιδιαίτερα ευέλικτο. (Routing Header, Authentication Header, Encapsulating Security Payload, Fragmentation Header, Destination Options Header, Hop-by-Hop Options Header).
- Το IPv6 απαιτεί η λειτουργία του κατακερματισμού (fragmentation) και της επανασυναρμολόγησης (reassembly) των πακέτων να πραγματοποιείται στα άκρα της επικοινωνίας, δηλαδή στον αποστολέα και παραλήπτη. Αυτό έχει ως αποτέλεσμα την βελτίωση της λειτουργίας των δρομολογητών, καθώς δεν είναι πλέον υπεύθυνοι για τον κατακερματισμό και την ανά-συναρμολόγηση των πακέτων [7]. Επίσης, το IPv6 υποστηρίζει την μεταφορά πακέτων με ωφέλιμο φορτίο μεγαλύτερο από 64 Kbytes [6].
- Η κεφαλίδα του IPv6 περιέχει το πεδίο Flow Label, η χρήση του οποίου προσφέρει το χαρακτηριστικό Quality of Service (QoS). Το QoS είναι ένα χαρακτηριστικό που χρησιμοποιείται με σκοπό να εξασφαλίσει ότι ορισμένα πακέτα θα φτάσουν στον προορισμό τους μέσα σε ένα έγκαιρο χρονικό διάστημα. Αυτή η λειτουργία είναι απαραίτητη σε εφαρμογές που απαιτούν την μεταφορά βίντεο ή σε VoIP, καθώς απαιτείται τα πακέτα να φτάνουν το ένα μετά το άλλο, ώστε να ελαχιστοποιείται η καθυστέρηση [8].
- Κάθε νέος κόμβος που επιθυμεί να συνδεθεί στο δίκτυο, πρέπει να χαρακτηρίζεται από μια IP διεύθυνση. Στο πρωτόκολλο IPv4, η ανάθεση IP διευθύνσεων γίνεται μέσω stateful πρωτοκόλλων, όπως το Dynamic Host Configuration Protocol (DHCP), το οποίο χρειάζεται έναν εξυπηρετητή με σκοπό την διατήρηση στατικών πινάκων που αποφασίζουν για την ανάθεση διευθύνσεων σε συσκευές [2,8]. Το IPv6 εκτός από την υποστήριξη του stateful auto-configuration μέσω του DHCPv6, προσφέρει την δυνατότητα για stateless auto-configuration με την βοήθεια του πρωτοκόλλου Neighbor Discovery[8]. Το stateless auto-configuration δεν απαιτεί καμία χειροκίνητη

[6] Το IPv4 παρέχει 2^{32} = 4,294,967,296 διευθύνσεις
[7] Οι Extension Headers του πρωτοκόλλου IPv6 περιγράφονται παρακάτω
[8] Περιγράφεται κεφάλαιο 3

ρύθμιση των hosts[9], ελάχιστη διαμόρφωση (δεν χρειάζεται πάντα) των δρομολογητών και κανέναν επιπρόσθετο εξυπηρετητή. Ο stateless auto-configuration μηχανισμός επιτρέπει σε έναν host να δημιουργήσει την δική του διεύθυνση χρησιμοποιώντας έναν συνδυασμό από τοπικές διαθέσιμες πληροφορίες και πληροφορίες που γνωστοποιούνται (advertised) από τους δρομολογητές. Οι δρομολογητές γνωστοποιούν prefixes, τα οποία προσδιορίζουν το δίκτυο, ενώ οι hosts δημιουργούν έναν προσδιοριστή διεπαφής (interface identifier), ο οποίος προσδιορίζει μοναδικά μια διεπαφή σε ένα δίκτυο. Μια διεύθυνση σχηματίζεται από τον συνδυασμό του prefix και interface identifier. Όταν στην παραπάνω διαδικασία απουσιάζουν οι δρομολογητές, ένας host μπορεί να σχηματίσει μόνο link-local διευθύνσεις, δηλαδή διευθύνσεις οι οποίες είναι επαρκείς για την επικοινωνία κόμβων[10] μέσα στο ίδιο δίκτυο, ενώ δεν επιτρέπουν την επικοινωνία με κόμβους εκτός δικτύου [23]. Αυτή η λειτουργία μειώνει τα καθήκοντα των διαχειριστών όσον αφορά την ρύθμιση και ανάθεση IP διευθύνσεων, γεγονός ιδιαίτερα σημαντικό αν αναλογιστούμε τον τεράστιο αριθμό αλλά και την μεγάλη ποικιλία IPv6 συσκευών στο μέλλον.

- Κατά τον σχεδιασμό και την υλοποίηση του πρωτοκόλλου IPv6, το θέμα της ασφάλειας αποτέλεσε πρωταρχικής σημασίας ζήτημα. Για αυτό το λόγο αναπτύχθηκε το πρωτόκολλο ασφάλειας IPsec[11], το οποίο παρέχει ασφάλεια σε επίπεδο δικτύου με σκοπό την διατήρηση της ακεραιότητας, εμπιστευτικότητας και αυθεντικότητας των δεδομένων. Η υλοποίηση του IPsec είναι υποχρεωτική στο IPv6 (ωστόσο η χρήση του δεν είναι), ενώ η υλοποίηση του στο IPv4 είναι προαιρετική.

2.3 Σχεδιαστικές προκλήσεις του IPv6

Ο σχεδιασμός του πρωτοκόλλου IPv6 φέρνει νέες προκλήσεις στο προσκήνιο, αναγκάζοντας τους διαχειριστές δικτύων να προσαρμόσουν την πολιτική τους σε αυτά τα νέα δεδομένα. Ορισμένες προκλήσεις που δημιουργούνται από τον σχεδιασμό του IPv6 είναι οι εξής:

- Ορισμένες λειτουργίες στο IPv6, όπως οι stateless auto-configuration και Path MTU discovery, καθιστούν απαραίτητη την χρήση Internet Control Message Protocol (ICMP) μηνυμάτων, κάτι που δεν συμβαίνει στο IPv4 [1]. Έτσι οι διαχειριστές οφείλουν να αλλάξουν πολιτική ως προς την αντιμετώπιση των ICMP μηνυμάτων. Αυτό συνεπάγεται την αλλαγή πολιτικής ελέγχου στα Firewalls και IDSs, τα οποία στο IPv4 συνήθως φίλτραραν και απέρριπταν τα ICMP πακέτα, ενώ στο IPv6 οφείλουν να επιτρέπουν κατά περίπτωση την είσοδο και έξοδό τους από ένα δίκτυο.
- Νέες προκλήσεις φέρνουν οι μηχανισμοί μετάβασης (transition mechanisms)[12] του πρωτοκόλλου IPv6. Οι μηχανισμοί αυτοί επιτρέπουν την συνύπαρξη των δύο πρωτοκόλλων, με αποτέλεσμα οι διαχειριστές να προσαρμόζουν τις πολιτικές τους ανάλογα με το πρωτόκολλο που χρησιμοποιείται. Οι συνύπαρξη των δύο

[9] Οποιοσδήποτε κόμβος δικτύου δεν είναι δρομολογητής
[10] Οποιαδήποτε συσκευή υλοποιεί το IPv6. Άρα μπορεί να είναι host ή δρομολογητής
[11] Γίνεται εκτενής αναφορά στο κεφάλαιο8
[12] Θα εξεταστούν εκτενώς στο κεφάλαιο 7

πρωτοκόλλων επιφέρει πολλές ευπάθειες, οι οποίες θα αναλυθούν στο αντίστοιχο κεφάλαιο.

- Ο χειρισμός των Extension Headers αποτελεί μια νέα πρόκληση για τους διαχειριστές, καθώς η χρήση τους στα πακέτα IPv6 μπορεί να οδηγήσει σε εκμετάλλευση των ευπαθειών τους και κατά συνέπεια σε επίτευξη επιθέσεων.
- Λόγω των κρυπτογραφημένων μηνυμάτων που αποστέλλονται στο IPv6 μέσω του IPsec, υπάρχει μεγάλη δυσκολία στην διαδικασία ελέγχου – επιθεώρησης των πακέτων που περνάνε από ένα firewall. Έτσι, νέες προκλήσεις εμφανίζονται σχετικά με το πόσο ασφαλή θα θεωρηθούν αυτά τα πακέτα από μηχανισμούς ασφάλειας, όπως τα firewalls [24].
- Μέθοδοι αξιολόγησης της ασφάλειας ενός συστήματος, όπως το penetration testing οφείλουν να αναδιαμορφωθούν, λόγω του τεράστιου χώρου διευθύνσεων που πρέπει να σαρώσουν.

2.4 Σύγκριση IPv4 – IPv6 κεφαλίδας

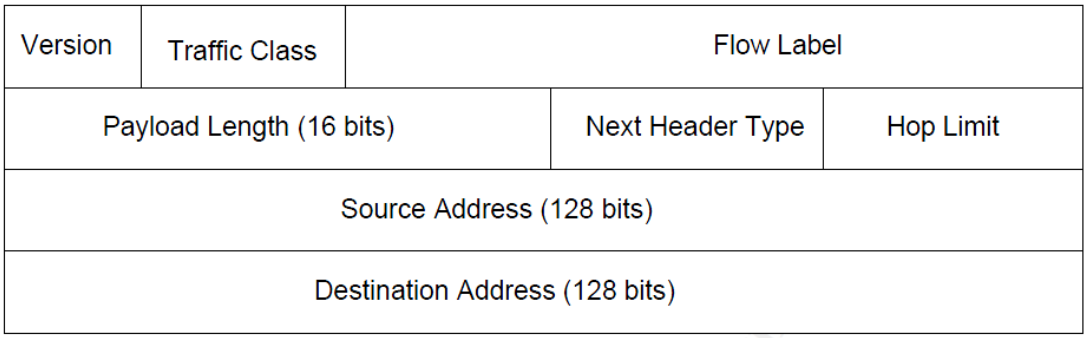
Η κεφαλίδα IPv6 σχεδιάστηκε με σκοπό να εκσυγχρονίσει την κεφαλίδα του IPv4 και να προσφέρει νέες λειτουργίες. Κατά τον σχεδιασμό της IPv6 κεφαλίδας, ορισμένα πεδία της κεφαλίδας του IPv4 απομακρύνθηκαν, άλλα μετονομάστηκαν (παρέχοντας την ίδια λειτουργικότητα με πριν), ενώ υπήρχαν πεδία που μετακινήθηκαν στις νέες προαιρετικές εκτεταμένες κεφαλίδες (IPv6 Extension Headers). Η δομή της κεφαλίδας του IPv4 φαίνεται στην Εικόνα 2.3 .

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="6">Source Address</td></tr>
<tr><td colspan="6">Destination Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Εικόνα 2.3: IPv4 Κεφαλίδα

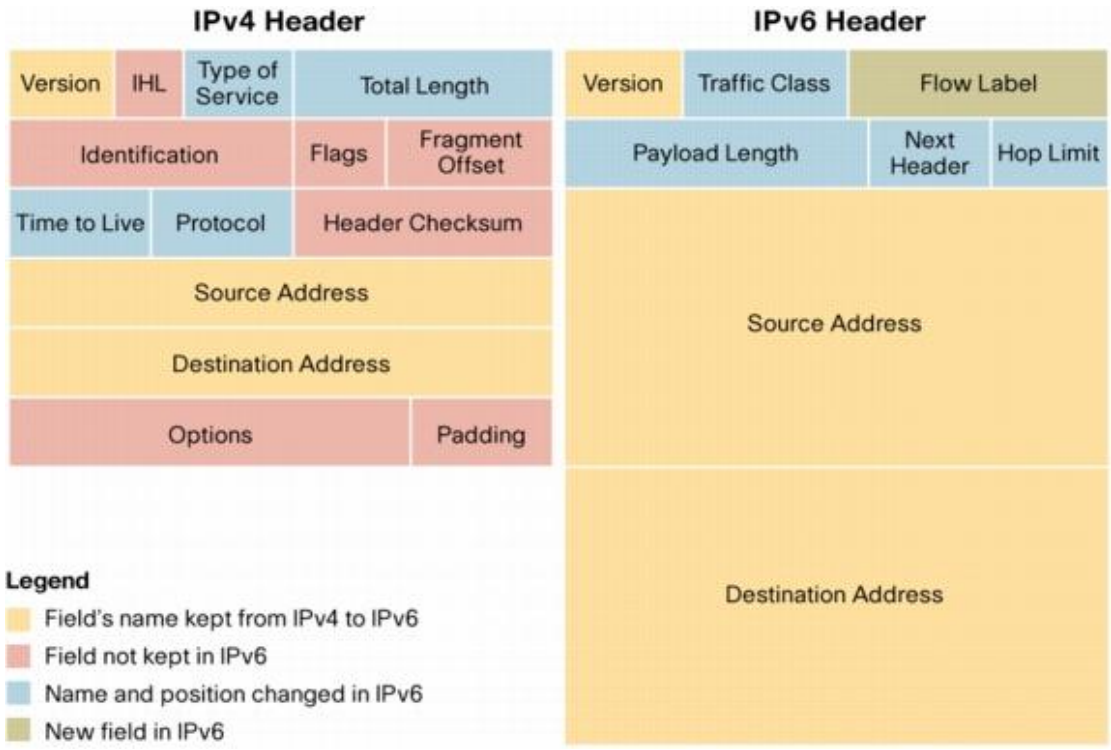
Το πεδίο "IHL" (Internet Header Length) έχει απομακρυνθεί από την κεφαλίδα του IPv6, διότι το μέγεθος της κεφαλίδας είναι πλέον σταθερό. Τα πεδία "Type of Service" και "Total Length" του IPv4 είναι ισοδύναμα με τα "Traffic class" και "Payload Length" αντίστοιχα του IPv6. Από την στιγμή που ο κατακερματισμός των πακέτων στο IPv6 πραγματοποιείται στους κόμβους πηγής και προορισμού και όχι στους δρομολογητές όπως συμβαίνει στο IPv4, τα πεδία ελέγχου (Identification, Flags, Fragment Offset fields) έχουν μετακινηθεί στο Fragment Extension Header του IPv6. Τα πεδία "Time to Live" και "Protocol" του IPv4 έχουν αντικατασταθεί από τα πεδία "Hop Limit" και "Next Header" αντίστοιχα. Το "Header Checksum" πεδίο έχει αφαιρεθεί, με κύριο πλεονέκτημα την αποφυγή σπατάλης χρόνου κατά την διαδικασία ελέγχου (checksum). Ωστόσο, η απομάκρυνση του checksum εισάγει το ρίσκο της μη ανίχνευσης σφαλμάτων, το οποίο

όμως είναι ελάχιστο, λόγω των πολλών ελέγχων που διενεργούνται στις περισσότερες διαδικασίες ενθυλάκωσης [9] των ανώτερων επιπέδων του IP/TCP μοντέλου. Τέλος, το πεδίο “Options” του IPv4 δεν αποτελεί πεδίο της κεφαλίδας του IPv6, αφού έχει μετακινηθεί στις προαιρετικές IPv6 Extension Headers, καθιστώντας πιο αποτελεσματική την δρομολόγηση, καθώς οι δρομολογητές επεξεργάζονται μόνο τις πληροφορίες που χρειάζονται [8]. Οι παραπάνω αλλαγές στο σχεδιασμό της κεφαλίδας του IPv6, οδήγησαν σε μια νέα δομή, η οποία φαίνεται στην Εικόνα 2.4.



Εικόνα 2.4: IPv6 κεφαλίδα

Οι διαφορές στις κεφαλίδες των δύο πρωτοκόλλων φαίνονται στην Εικόνα 2.5.



Εικόνα 2.5: Σύγκριση IPv4 - IPv6 κεφαλίδων

2.4.1 Πεδία IPv6 κεφαλίδας

Στο συγκεκριμένο σημείο θα γίνει μια αναφορά στα πεδία της IPv6 κεφαλίδας.

- **Version:** Προσδιορίζει την έκδοση του πρωτοκόλλου IP που χρησιμοποιείται για να παραχθεί το πακέτο. Το πεδίο χρησιμοποιείται με τον ίδιο τρόπο όπως στο IPv4, με την διαφορά ότι περιέχει την τιμή 6 αντί για την τιμή 4 [10].
- **Traffic Class:** Αντικαθιστά το πεδίο Type of Service της κεφαλίδας IPv4. Χρησιμοποιείται με την μέθοδο Differentiated Services (DS) που ορίζεται στο RFC 2474, το οποίο καθορίζει τις Quality of Service (QoS) τεχνικές για το IPv6 [10].
- **Flow Label:** Δημιουργήθηκε με σκοπό να παρέχει μια επιπρόσθετη υποστήριξη των real-time πακέτων που διανέμονται, καθώς και quality of service χαρακτηριστικά. Η έννοια της ροής (flow), ορίζεται από το RFC 2460 ως μια σειρά από πακέτα που αποστέλλονται από μια συσκευή που παίζει το ρόλο πηγής σε έναν ή περισσότερους προορισμούς. Μια μοναδική ετικέτα ροής (flow label) χρησιμοποιείται για να προσδιορίσει όλα τα πακέτα μιας συγκεκριμένης ροής, έτσι ώστε οι δρομολογητές που βρίσκονται ανάμεσα στην πηγή και τον προορισμό να τα χειρίζονται με τον ίδιο τρόπο. Αυτό βοηθάει στην εξασφάλιση ομοιομορφίας, όσον αφορά στον τρόπο που διανέμονται τα πακέτα μιας ροής. Η χρησιμοποίηση του συγκεκριμένου πεδίου από μια συσκευή πηγή είναι προαιρετική και εξαρτάται από το αν η συσκευή και οι δρομολογητές μπορούν να υποστηρίξουν χειρισμό ετικέτας ροής [10].
- **Payload Length:** Το συγκεκριμένο πεδίο αντικαθιστά το πεδίο "Total Length", αλλά χρησιμοποιείται με διαφορετικό τρόπο. Σε αντίθεση με το "Total Length", το οποίο υπολογίζει το μήκος ολόκληρου του πακέτου, το Payload Length περιέχει μόνο τον αριθμό των bytes του ωφέλιμου φορτίου [10].
- **Next Header:** Αντικαθιστά το πεδίο "Protocol" και έχει δύο χρήσεις. Όταν το πακέτο έχει extension headers, τότε το πεδίο "Next Header" προσδιορίζει την ταυτότητα του πρώτου extension header, που στην ουσία είναι η επόμενη κεφαλίδα του πακέτου. Όταν το πακέτο έχει μόνο την κύρια κεφαλίδα και κανένα extension header, τότε το πεδίο "Next Header", έχει τον ίδιο ρόλο με το πεδίο "Protocol" του IPv4. Σε αυτή την περίπτωση, το πεδίο "Next Header" περιέχει το πρωτόκολλο που χρησιμοποιεί το πιο πάνω επίπεδο, που συνήθως είναι το TCP,UDP [10,11] .
- **Hop Limit:** Το συγκεκριμένο πεδίο αντικαθιστά το πεδίο "Time to Live (TTL)" της κεφαλίδας του IPv4. Η χρήση είναι η ίδια, αλλά το όνομα "Hop Limit" αντανακλά με καλύτερο τρόπο την χρήση του TTL, αφού υπολογίζει βήματα (hops) και όχι χρόνο (time) [10].
- **Source Address:** Περιέχει την 128-bit IP διεύθυνση του δημιουργού του πακέτου, δηλαδή της πηγής, από την οποία αποστέλλεται το πακέτο στο δίκτυο.
- **Destination Address:** Περιέχει την 128-bit IP διεύθυνση του παραλήπτη του πακέτου. Ο παραλήπτης αποτελεί τον τελικό προορισμό και όχι τους δρομολογητές που ενδεχομένως βρίσκονται μεταξύ αποστολέα και παραλήπτη.

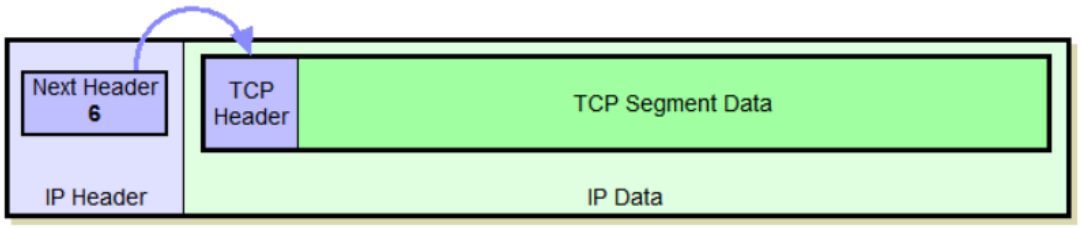
2.5 IPv6 Extension Headers

Μετά την "κύρια" κεφαλίδα ένας ή περισσότεροι Extension Headers είναι δυνατόν να εμφανιστούν πριν από το ενθυλακωμένο ωφέλιμο φορτίο. Αυτές οι κεφαλίδες σχεδιάστηκαν με σκοπό να παρέχουν ευελιξία και αποδοτικότητα στα IPv6 πακέτα. Οι συγκεκριμένες κεφαλίδες περιέχουν πεδία, τα οποία παρέχουν πρόσθετες λειτουργίες στο πακέτο, γι' αυτό το λόγο είναι προαιρετικές, σε αντίθεση με τα πεδία της κύριας κεφαλίδας που προσφέρουν σημαντικές και απαραίτητες λειτουργίες [10]. Οι περισσότεροι extension headers υπόκεινται σε επεξεργασία μόνο στον κόμβο προορισμού (για παράδειγμα οι κεφαλίδες που σχετίζονται με την ασφάλεια), για αυτό τον λόγο δεν επηρεάζουν την αποδοτικότητα των δρομολογητών. Ο μόνος τύπος extension header που υποβάλλεται σε έλεγχο από τους δρομολογητές είναι η Hop-by-Hop Options Header, η οποία όταν χρησιμοποιείται πρέπει να ακολουθεί πάντα την κύρια κεφαλίδα [11]. Οι Extension Headers, η προτεινόμενη σειρά τους (σύμφωνα με το RFC 1883) σε ένα πακέτο και ο κωδικός τους φαίνεται στην Εικόνα 2.6.

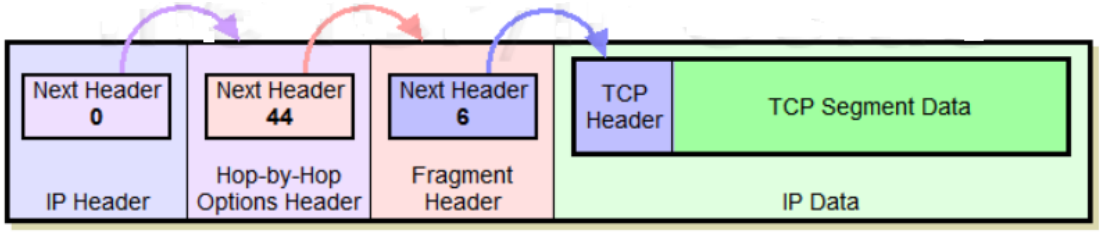
Order	Header Type	Next Header Code
1	**Basic IPv6 Header**	-
2	**Hop-by-Hop Options**	0
3	**Destination Options (with Routing Options)**	60
4	**Routing Header**	43
5	**Fragment Header**	44
6	**Authentication Header**	51
7	**Encapsulation Security Payload Header**	50
8	**Destination Options**	60
9	**Mobility Header**	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Εικόνα 2.6: IPv6 Extension Headers

Στην Εικόνα 2.7 φαίνεται ένα IPv6 datagram όταν δεν χρησιμοποιείται κάποιο Extension Header και στην Εικόνα 2.8 φαίνεται ένα IPv6 datagram όταν χρησιμοποιούνται δύο Extension Headers.



Εικόνα 2.7: IPv6 Datagram που μεταφέρει TCP segment χωρίς κάποιο Extension Header



Εικόνα 2.8: IPv6 Datagram με δύο Extension Headers

2.5.1 Συνοπτική περιγραφή των Extension Headers

- **Hop-by-Hop Options Header:** Η Hop-by-Hop option header πρέπει να υποβάλλεται σε επεξεργασία σε κάθε κόμβο που φτάνει το πακέτο [10].
- **Routing Header:** Χρησιμοποιείται από την IPv6 πηγή για να προσδιορίσει την λίστα με τους ενδιάμεσους κόμβους, από τους οποίους οφείλει να περάσει ένα πακέτο για να φτάσει στον προορισμό του [10].
- **Fragment Header:** Περιέχει τα πεδία Fragment Offset, Identification και άλλα πεδία κατακερματισμού. Η Fragment Header υπόκεινται σε επεξεργασία μόνο από τον κόμβο προορισμού, σε αντίθεση με το IPv4, όπου ο κατακερματισμός γίνεται σε κάθε ενδιάμεσο κόμβο [10].
- **Destination Options Header:** Περιέχει ορισμένες επιλογές που πρέπει να υποβληθούν σε επεξεργασία από τον κόμβο προορισμού. Η Destination Options Header είναι η μοναδική κεφαλίδα που μπορεί να εμφανίζεται δύο φορές σε ένα πακέτο. Αυτό συμβαίνει διότι ορισμένες επιλογές πρέπει να εξεταστούν από μια λίστα από συσκευές που προσδιορίζονται σε κάθε δρομολόγιο. Σε αυτή την περίπτωση η κεφαλίδα τοποθετείται πριν από την κεφαλίδα Routing Header [10].
- **Authentication Header[13] (AH):** Χρησιμοποιείται για διατήρηση της ακεραιότητας και αυθεντικότητας των δεδομένων που μεταφέρονται.
- **Encapsulation Security Payload[14] (ESP):** Χρησιμοποιείται για διασφάλιση της εμπιστευτικότητας των δεδομένων. Επίσης, προσφέρει περιορισμένης έκτασης υπηρεσίες αυθεντικότητας.

[13] Εκτενής περιγραφή του AH γίνεται στο κεφάλαιο 8
[14] Εκτενής περιγραφή του ESP γίνεται στο κεφάλαιο 8

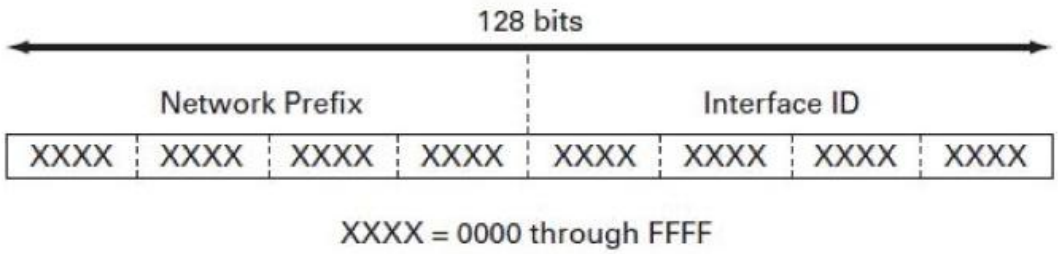
3

Διευθύνσεις και νέα πρωτόκολλα στο IPv6

Μια IPv6 διεύθυνση είναι 128 bits, σε αντίθεση με μια IPv4 διεύθυνση, η οποία είναι 32 bits. Αναπαριστάται σε δεκαεξαδική μορφή κάνοντας χρήση του συμβόλου “ : “ . Ένα παράδειγμα IPv6 διεύθυνσης είναι: 1254:1532:26B1:CC14:0123:1111:2222:3333. Κάθε γκρουπ (πεδίο) δεκαεξαδικών ψηφίων είναι 16 bits και συνολικά κάθε διεύθυνση έχει 8 πεδία [36].

3.1 IPv6 Prefix

Το πρωτόκολλο IPv4 χρησιμοποιεί μια μάσκα υποδικτύου (subnet mask) για να προσδιορίσει ποιο είναι το prefix και ποιο το host τμήμα μιας διεύθυνσης. Η μάσκα υποδικτύου μπορεί επίσης να αναπαρασταθεί και σε Classless Inter-Domain Routing (CIDR) μορφή. Το πρωτόκολλο IPv6 χρησιμοποιεί πάντοτε CIDR σημειογραφία για να προσδιορίσει ποια bits της διεύθυνσης αναπαριστούν το prefix τμήμα. Έστω για παράδειγμα η IPv6 διεύθυνση: 1254:1532:26B1:CC14:123:1111:2222:3333/64. Το prefix ID είναι το τμήμα 1254:1532:26B1:CC14: και το Host ID είναι το τμήμα 123:1111:2222:3333. Το /64 υποδεικνύει ότι τα πρώτα 64 bits της διεύθυνσης προσδιορίζουν το prefix. Στην Εικόνα 3.1 φαίνεται η γενική δομή μιας IPv6 διεύθυνσης.



Εικόνα 3.1: Δομή μιας IPv6 διεύθυνσης

3.2 IPv6 Interface ID και EUI-64 Format

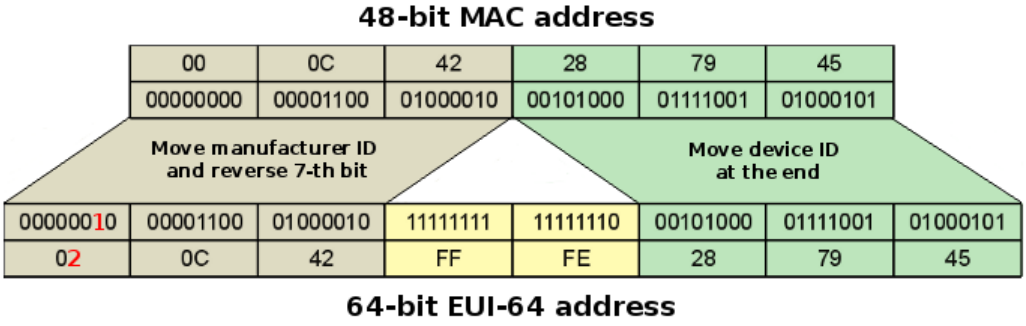
Στο πρωτόκολλο IPv4 το host τμήμα της διεύθυνσης δεν βασίζεται στην διεύθυνση υλικού της διεπαφής, αλλά στο Address Resolution Protocol. Στο πρωτόκολλο IPv6, τα πρώτα 64 bits χρησιμοποιούνται για να προσδιορίσουν το δίκτυο (prefix ID) και τα υπόλοιπα 64 bits

για να προσδιορίσουν τον host (interface ID). Το interface ID βασίζεται στην διεύθυνση υλικού της διεπαφής και ακολουθεί την IEEE 64-bit Extended Unique Identifier (EUI-64) μορφή. Από την στιγμή που οι περισσότερες διεπαφές χρησιμοποιούν την 48-bit MAC διεύθυνση, η MAC πρέπει να μετατραπεί σε EUI-64 μορφή.

Τα πρώτα 24 bits μιας MAC διεύθυνσης προσδιορίζουν τον κατασκευαστή και τα υπόλοιπα 24 bits προσδιορίζουν μοναδικά τον host. Για να μετατραπεί η MAC διεύθυνση σε EUI-64 μορφή ακολουθούνται τα παρακάτω βήματα [36]:

1. Τα πρώτα 24 bits της MAC διεύθυνσης, γίνονται τα πρώτα 24 bits του interface ID με EUI-64 μορφή.
2. Το έβδομο bit των πρώτων 24 bit της MAC διεύθυνσης αλλάζει από "0" σε "1".
3. Τα επόμενα 16 bits του interface ID είναι FFFE.
4. Τα τελευταία 24 bits της MAC διεύθυνσης, γίνονται τα τελευταία 24 bits του interface ID.

Για παράδειγμα η 48 bit MAC διεύθυνση 000C.4228.7945 θα μετατραπεί σε 020C.42FF.FE28.7945, η οποία είναι σε 64 bit EUI-64 μορφή και αποτελεί το interface ID της IPv6 διεύθυνσης. Στην Εικόνα 3.2 φαίνεται η μετατροπή της 48 bit MAC διεύθυνσης σε 64 bit EUI-64 μορφή.



Εικόνα 3.2: Μετατροπή 48-bit MAC διεύθυνσης σε 64-bit EUI-64 μορφή

3.3 Ιεραρχία IPv6 διευθύνσεων

Στο πρωτόκολλο IPv4 ο χώρος των διευθύνσεων χωρίζεται σε συγκεκριμένες "τάξεις" (Classes). Η class μιας IPv4 διεύθυνσης προσδιορίζεται από τα "σημαντικά" bits της πρώτης οκτάδας.

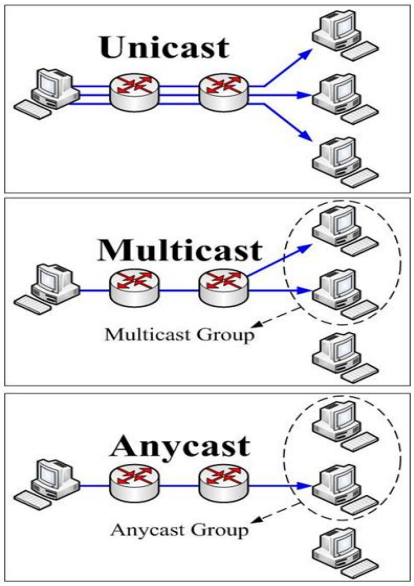
- Class A: (00000001 – 01111111) ή (1 – 127)
- Class B: (10000000 – 10111111) ή (128 – 191)
- Class C: (11000000 – 11011111) ή (192 – 223)
- Class D: (11100000 – 11101111) ή (224 – 239)

Η IPv6 δομή διευθυνσιοδότησης είναι πολύ πιο scalable. Οι διευθύνσεις αυτές κατηγοριοποιούνται με βάση δύο παραμέτρους, τον τύπο και το πεδίο [12].

Τύπος:

- **Unicast addresses:** Ένα πακέτο παραδίδεται σε μια διεπαφή.

- **Multicast addresses:** Ένα πακέτο παραδίδεται σε πολλαπλές διεπαφές ενός γκρουπ.
- **Anycast addresses:** Ένα πακέτο παραδίδεται στην κοντινότερη διεπαφή μεταξύ πολλαπλών διεπαφών ενός γκρουπ [12].



Εικόνα 3.3: Unicast, Multicast, Anycast διευθύνσεις

Οι unicast και anycast διευθύνσεις έχουν τα παρακάτω πεδία [12].

Πεδία:

- **Link-Local:** Το πεδίο είναι ένας τοπικός σύνδεσμος (κόμβοι στο ίδιο υποδίκτυο).
- **Site-Local:** Το πεδίο είναι ένας οργανισμός (ιδιωτικός χώρος διευθύνσεων).
- **Aggregate Global:** Το πεδίο είναι παγκόσμιο (IPv6 διευθύνσεις διαδικτύου).

3.3.1 Anycast Addresses

Αυτού του τύπου οι διευθύνσεις προσδιορίζουν ένα γκρουπ διεπαφών μεταξύ πολλαπλών hosts. Οι πολλαπλοί hosts διαμορφώνονται με μια identical διεύθυνση. Τα πακέτα αποστέλλονται στον πιο κοντινό host ενός γκρουπ από hosts.

3.3.2 Multicast Addresses

Οι multicast IPv6 διευθύνσεις είναι οι αντίστοιχες multicast διευθύνσεις του πρωτοκόλλου IPv4. Οι διεπαφές μπορούν να ανήκουν σε ένα ή περισσότερα multicast γκρουπ. Έτσι, μπορούν να αποδεχθούν ένα multicast πακέτο μόνο εάν ανήκουν σε αυτό το γκρουπ. Το πρώτο πεδίο μιας multicast IPv6 διεύθυνσης αρχίζει πάντα με FFxx και οι συγκεκριμένες διευθύνσεις αντιστοιχούν στο 1/256 του διαθέσιμου χώρου των IPv6 διευθύνσεων.

3.3.3 Special (Reserved) IPv6 Addresses

Το πρώτο πεδίο μιας reserved IPv6 διεύθυνσης αρχίζει πάντα με 00xx. Οι reserved διευθύνσεις αντιστοιχούν στο 1/256 του διαθέσιμου χώρου IPv6 διευθύνσεων. Υπάρχουν διάφορα είδη reserved διευθύνσεων, περιλαμβάνοντας:

- 0:0:0:0:0:0:0:0 (ή ::) : Αποτελεί μια απροσδιόριστη ή άγνωστη διεύθυνση. Στο IPv4 η αντίστοιχη διεύθυνση είναι η 0.0.0.0, η οποία υποδηλώνει την απουσία μιας διαμορφωμένης διεύθυνσης. Στους πίνακες δρομολόγησης, μια απροσδιόριστη διεύθυνση χρησιμοποιείται για να προσδιορίσει όλα ή any πιθανά δίκτυα ή hosts.
- 0:0:0:0:0:0:0:1 (ή ::1) : Αποτελεί την localhost διεύθυνση. Στο IPv4 η αντίστοιχη διεύθυνση είναι η 127.0.0.1.

3.3.4 Link-Local IPv6 Addresses

Οι Link-Local IPv6 διευθύνσεις χρησιμοποιούνται μόνο σε ένα ξεχωριστό σύνδεσμο (υποδίκτυο). Οποιοδήποτε πακέτο περιέχει μια link-local διεύθυνση πηγής ή προορισμού δεν μπορεί να δρομολογηθεί σε ένα άλλο σύνδεσμο – υποδίκτυο. Οποιαδήποτε IPv6 διεπαφή ενός host (ή ενός δρομολογητή) έχει μια link-local διεύθυνση. Αυτή η διεύθυνση μπορεί να ανατεθεί χειροκίνητα ή μέσω της διαδικασίας auto-configuration (αυτό-διαμόρφωσης). Το πρώτο πεδίο μια link-local IPv6 διεύθυνσης αρχίζει πάντα με FE8x. Οι συγκεκριμένες διευθύνσεις είναι unicast και αντιστοιχούν στο 1/1024 του διαθέσιμου χώρου των IPv6 διευθύνσεων.

3.3.5 Site Local IPv6 Addresses

Οι site-local IPv6 διευθύνσεις είναι οι αντίστοιχες ιδιωτικές (private) διευθύνσεις του πρωτοκόλλου IPv4. Οποιοδήποτε πακέτο περιέχει μια site-local διεύθυνση πηγής ή προορισμού μπορεί να δρομολογηθεί εντός ενός οργανισμού, αλλά όχι στο παγκόσμια στο διαδίκτυο. Το πρώτο πεδίο μια site-local IPv6 διεύθυνσης αρχίζει πάντα με FECx. Οι συγκεκριμένες διευθύνσεις είναι unicast και αντιστοιχούν στο 1/1024 του διαθέσιμου χώρου των IPv6 διευθύνσεων.

3.3.6 Aggregate global Addresses

Οι aggregate global διευθύνσεις είναι οι αντίστοιχες δημόσιες (public) διευθύνσεις του πρωτοκόλλου IPv4. Οι συγκεκριμένες διευθύνσεις μπορούν να δρομολογηθούν δημόσια στο διαδίκτυο. Για αυτό το λόγο οποιαδήποτε συσκευή επιθυμεί να επικοινωνεί με κόμβους του διαδικτύου θα πρέπει να προσδιορίζεται μοναδικά από μια aggregate global διεύθυνση. Οι συγκεκριμένες διευθύνσεις αρχίζουν πάντα με 2xxx, είναι unicast και αντιστοιχούν στο 1/8 του διαθέσιμου χώρου των IPv6 διευθύνσεων.

3.4 ICMPv6

Τα ICMP πακέτα του πρωτοκόλλου IPv6 (ICMPv6) αποτελούν σημαντικό συστατικό για την λειτουργία του πρωτοκόλλου IPv6. Το ICMPv6 παρέχει αρκετές υπηρεσίες, ορισμένες από τις οποίες είναι:

- Μηνύματα Σφάλματος (Error Messages)
- Μηνύματα Ενημέρωσης (Informational Messages) – π.χ. echo
- Path Maximum Transmission Unit Discovery (PMTUD)
- Neighbor Discovery

Υπάρχουν τέσσερα ICMPv6 μηνύματα σφάλματος:

Destination Unreachable (ICMP τύπος πακέτου 1)
Υποδηλώνει ότι το πακέτο δεν μπορεί να προωθηθεί στον προορισμό του. Ο κόμβος που αποστέλλει αυτό το μήνυμα περιλαμβάνει έναν κωδικό επεξήγησης.

- 0: Καμία δρομολόγηση στον προορισμό
- 1: Απαγορεύεται η πρόσβαση από τον διαχειριστή
- 3: Απρόσιτη διεύθυνση
- 4: Απρόσιτη θύρα

Packet Too Big (ICMP τύπος πακέτου 2)
Υποδηλώνει ότι το πακέτο είναι μεγαλύτερο από το MTU του συνδέσμου, μέσα στο οποίο πρόκειται να δρομολογηθεί. Όπως έχει αναφερθεί οι IPv6 δρομολογητές δεν κατακερματίζουν τα πακέτα. Τα Packet Too Big μηνύματα αποστέλλονται στην πηγή (στην συσκευή από την οποία προέρχεται το πακέτο), με σκοπό να μειωθεί το μέγεθος του πακέτου ανάλογα με το MTU.

Time Exceeded (ICMP τύπος πακέτου 3)
Υποδηλώνει ότι η τιμή του hop έχει φτάσει στο όριο, usually indicating a routing loop

Parameter Problem (ICMP τύπος πακέτου 4)
Υποδηλώνει ένα σφάλμα στην IPv6 κεφαλίδα ή σε μια από τις κεφαλίδες επέκτασης. Ο κόμβος που στέλνει το συγκεκριμένο μήνυμα περιλαμβάνει και ένα επεξηγηματικό κωδικό:

- 0: Εσφαλμένο πεδίο κεφαλίδας
- 1: Μη αναγνωρίσιμη επόμενη κεφαλίδα (next header)
- 2: Μη αναγνωρίσιμη IPv6 επιλογή (option)

3.5 Neighbor Solicitation and Advertisement Messages

Για την ορθή λειτουργία των παρακάτω πρωτοκόλλων και λειτουργιών είναι απαραίτητη η χρήση ορισμένων μηνυμάτων, τα οποία χρησιμοποιούνται στις διαδικασίες Next-hop Determination, Neighbor Unreachability Detection και γενικότερα στην Address Resolution [25]. Τα μηνύματα αυτά είναι ICMPv6 πακέτα και περιλαμβάνουν το Neighbor Solicitation

Message (NS) και το Neighbor Advertisement Message (NA). Το NS μήνυμα επιτρέπει σε μια συσκευή να εξετάσει εάν υπάρχει ένας γείτονας και εάν είναι προσεγγίσιμος, ώστε στην συνέχεια να προβεί σε Address Resolution. Το (NA) μήνυμα επιβεβαιώνει την ύπαρξη ενός host ή δρομολογητή και παρέχει διευθύνσεις επιπέδου 2 (data link layer), όποτε είναι αναγκαίο [25].

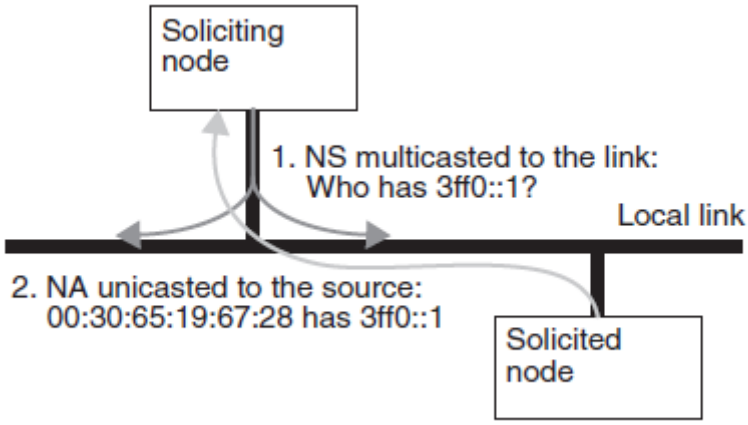
Στην περίπτωση που ένας host επιθυμεί να κάνει Router Discovery, δηλαδή να εντοπίσει έναν δρομολογητή και να μάθει σημαντικές παραμέτρους που σχετίζονται με την λειτουργία του τοπικού δικτύου, στέλνει ένα Router Solicitation Message (RS) και περιμένει απάντηση από τον δρομολογητή μέσω ενός Router Advertisement Message (RA) [25]. Και σε αυτή την περίπτωση τα Router Solicitation /Advertisement Messages είναι στην ουσία ICMPv6 πακέτα.

3.6 Neighbor Discovery Protocol

Σκοπός του πρωτοκόλλου Neighbor Discovery που υποστηρίζεται από το IPv6, είναι η παροχή ενός μέσου στους IPv6 κόμβους, για την ανακάλυψη παρουσίας άλλων κόμβων, καθώς και των link-layer διευθύνσεων που έχουν αυτοί οι κόμβοι μέσα σε ένα τοπικό σύνδεσμο (link layer) [13]. Επιπροσθέτως, το Neighbor Discovery Protocol (NDP) παρέχει μεθόδους για την εύρεση δρομολογητών μέσα σε ένα local link, μεθόδους για την ανίχνευση περιπτώσεων που ένας τοπικός κόμβος γίνεται απρόσιτος, τεχνικές για επίλυση προβλημάτων με διπλότυπες διευθύνσεις (Duplicate Addresses), καθώς και ενημέρωση των κόμβων από τους δρομολογητές, όταν ένας άλλος δρομολογητής είναι πιο κατάλληλος για να δρομολογήσει τα πακέτα από και προς τον κόμβο (redirect) [14]. Στα επόμενα υποκεφάλαια, θα αναλυθούν αυτές οι λειτουργίες ξεχωριστά.

3.6.1 Address Resolution

Όταν ένας κόμβος επιθυμεί να πληροφορηθεί για την link-layer διεύθυνση ενός άλλου κόμβου, ο οποίος εικάζεται ότι βρίσκεται μέσα στο local layer, στέλνει ένα Neighbor Solicitation (NS**,** ICMP τύπος πακέτου 135) μήνυμα σε μια multicast διεύθυνση, η οποία καθορίζεται από την διεύθυνση – στόχο (target address). Αν ο κόμβος – στόχος είναι εντός του δικτύου, τότε ακούει στην multicast διεύθυνση και στην συνέχεια απαντάει στην παράκληση (solicitation) στέλνοντας ένα Neighbor Advertisement (NA**,** ICMP τύπος πακέτου 136) μήνυμα [14]. Στην Εικόνα 3.4 φαίνεται η παραπάνω λειτουργία.



Εικόνα 3.4: Basic Discovery Protocol

3.6.2 Neighbor Unreachability Detection

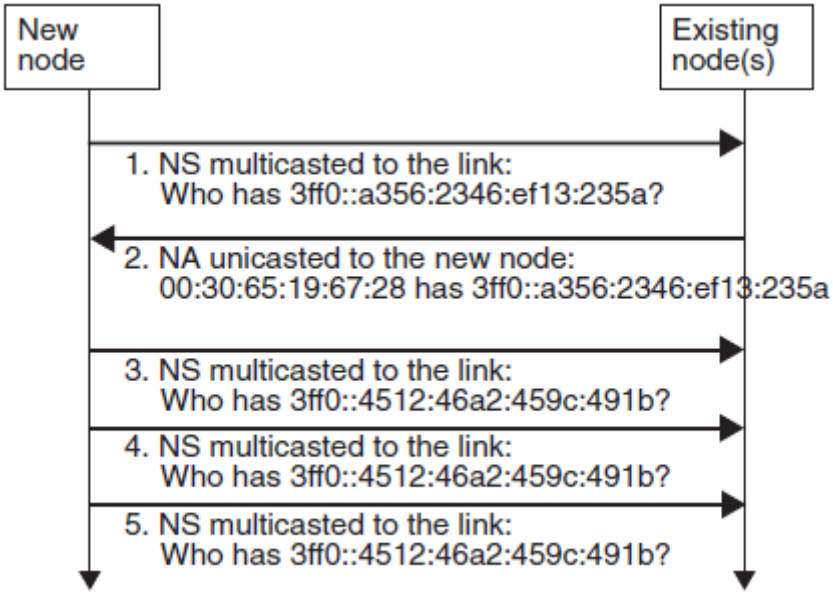
Οι κόμβοι μέσα σε έναν σύνδεσμο μπορούν να ελέγχουν την δυνατότητα προσέγγισης ορισμένων τοπικών κόμβων, μέσω της διαδικασίας Neighbor Unreachability [13]. Κατά κανόνα, οι κόμβοι βασίζονται σε πληροφορίες που παρέχει το υψηλότερο επίπεδο για να αποφασίσουν εάν ένας κόμβος είναι προσεγγίσιμος. Ωστόσο, εάν υπάρχει αρκετά μεγάλη καθυστέρηση στη κυκλοφορία του πιο πάνω επιπέδου ή εάν ένας κόμβος σταμάτησε να δέχεται αποκρίσεις από έναν ομότιμο κόμβο, τότε επικαλείται η λειτουργία NUD [14].

Αρχικά, ο κόμβος περιμένει για μια μικρή καθυστέρηση και στην συνέχεια στέλνει ένα Neighbor Solicitation (NS) μήνυμα στον ομότιμο κόμβο. Αν ο κόμβος είναι ακόμα προσεγγίσιμος, θα απαντήσει με ένα Neighbor Advertisement (NA) μήνυμα. Εάν ο κόμβος που στέλνει το NS δεν λάβει καμία απάντηση, θα προσπαθήσει να στείλει ορισμένα ακόμα NS μηνύματα. Εάν δεν λάβει ούτε τώρα απάντηση, θα διαγράψει την καταχώρηση του κόμβου από την μνήμη (neighbor cache entry) [14]. Καμία κίνηση υψηλότερου επιπέδου δεν μπορεί να προχωρήσει, εάν η διαδικασία NUD βγάλει από την μνήμη την καταχώρηση κάποιου κόμβου ύστερα από απόφαση (ίσως να είναι και λανθασμένη), ότι ο κόμβος δεν είναι πλέον προσιτός.

3.6.3 Duplicate Address Detection

Όταν ένας κόμβος σχεδιάζει να λάβει μια νέα διεύθυνση για προσωπική χρήση, θα πρέπει να σιγουρευτεί ότι κανένας άλλος κόμβος μέσα στον τοπικό σύνδεσμο δεν χρησιμοποιεί την ίδια διεύθυνση. Αυτό μπορεί να πραγματοποιηθεί με την αποστολή μιας σειράς Neighbor Solicitation μηνυμάτων στο local link [14]. Αυτά τα μηνύματα περιέχουν την δοκιμαστική διεύθυνση που ο υπολογιστής/σύστημα επιθυμεί να χρησιμοποιήσει. Αν η δοκιμαστική διεύθυνση χρησιμοποιείται ήδη από κάποιον άλλο υπολογιστή/σύστημα, τότε ο κόμβος που έχει αυτή την διεύθυνση στέλνει ένα Neighbor Advertisement ως απάντηση και ο αρχικός υπολογιστής/σύστημα θα πρέπει να επιλέξει μια νέα δοκιμαστική διεύθυνση. Αν ο αρχικός υπολογιστής/σύστημα δεν λάβει καμία απάντηση στα μηνύματα NS, τότε είναι

ελεύθερος να χρησιμοποιήσει την διεύθυνση [14]. Στην Εικόνα 3.5 φαίνεται η duplicate address detection διαδικασία.



Εικόνα 3.5: Duplicate Address Detection

3.7 Router Discovery

Με τις λειτουργίες που προσφέρει το Neighbor Discovery Protocol, επιτρέπει σε ένα host να ανακαλύψει άλλους host και να επικοινωνήσει μαζί τους μέσα σε ένα local link. Όμως, οι host έχουν την ανάγκη να παίρνουν πληροφορίες και για τους δρομολογητές που βρίσκονται μέσα στο link. Το IPv6 προσφέρει λειτουργίες router discovery, έτσι ώστε ένας host να πληροφορηθεί για την παρουσία του δρομολογητή και στη συνέχεια να αποκτήσει παγκόσμια διεύθυνση (global address) [14].

Κατά κανόνα, όλοι οι δρομολογητές στέλνουν Router Advertisement (RA, ICMP πακέτο με τύπο 134) μηνύματα μέσα σε ένα local link μέσω multicast διευθύνσεων. Τα μηνύματα αυτά περιέχουν έναν αριθμό από routing prefixes, τα οποία μπορούν να χρησιμοποιηθούν από τους hosts, έτσι ώστε να αποκτήσουν παγκόσμιες διευθύνσεις. Γενικότερα, ένας host μπορεί να ξεκινήσει την ανακάλυψη ενός δρομολογητή (router discovery) στέλνοντάς του Router Solicitation (RS, ICMP πακέτο με τύπο 133) μηνύματα. Στην συνέχεια, ο host περιμένει μια απάντηση RA από τον δρομολογητή, ενώ εάν δεν του έρθει καμία απάντηση μπορεί να επαναλάβει την αποστολή RS μηνυμάτων [14]. Ο αποστολέας δρομολογητής θέτει ένα όριο 255 hops σε ένα RA, ωστόσο το πακέτο RA δεν πρέπει να δρομολογηθεί εκτός του τοπικού συνδέσμου (local link). Τα RA μηνύματα περιέχουν τις παρακάτω πληροφορίες για τους hosts:

- Την link-layer διεύθυνση του δρομολογητή
- Ένα ή περισσότερα prefixes δικτύου
- Ένα χρόνο ζωής (μετρημένα σε δευτερόλεπτα) για τα prefixes

- Το MTU του συνδέσμου

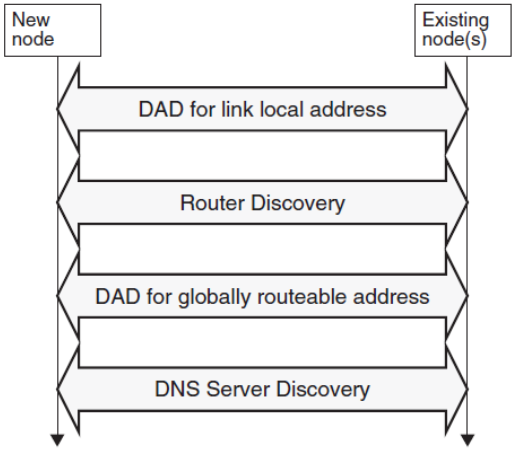
3.7.1 Redirects

Όταν ένας host επιθυμεί να στείλει ένα πακέτο σε έναν προορισμό, ένας δρομολογητής μπορεί να τον ενημερώσει για το ποιο είναι το καλύτερο πρώτο βήμα, μέσω της διαδικασίας ανακατεύθυνσης (redirect). Οι hosts μπορούν να έχουν πολλαπλούς δρομολογητές στην λίστα δρομολογητών τους, αλλά ένας από αυτούς επιλέγεται ως ο default δρομολογητής που θα χρησιμοποιεί. Εάν ο default δρομολογητής θεωρήσει ότι ένας άλλος δρομολογητής έχει ένα καλύτερο δρομολόγιο για τον προορισμό, τότε προωθεί ένα μήνυμα ανακατεύθυνσης στον αποστολέα host [36]. Επομένως, η διαδικασία ανακατεύθυνσης έχει σκοπό την βελτιστοποίηση δρομολόγησης πακέτων [14]. Ωστόσο, μια επικοινωνία μπορεί να εγκαθιδρυθεί και να διατηρηθεί χωρίς την χρήση της λειτουργίας ανακατεύθυνσης, ακόμα και αν τα πακέτα δεν ακολουθούν την καλύτερη διαδρομή, άρα η συγκεκριμένη διαδικασία είναι προαιρετική.

Τα μηνύματα ανακατεύθυνσης χρησιμοποιούνται αποκλειστικά από την διαδικασία ανακατεύθυνσης και αποστέλλονται πάντα από μια unicast διεύθυνση στην διεύθυνση πηγής του πακέτου που πυροδότησε την διαδικασία ανακατεύθυνσης [13]. Όπως συμβαίνει με όλα τα μηνύματα που συζητάμε στο παρόν κεφάλαιο, τα μηνύματα ανακατεύθυνσης χρησιμοποιούνται για link local (επικοινωνία μέσα σε ένα υποδίκτυο) σκοπούς και όχι για end-to-end επικοινωνίες.

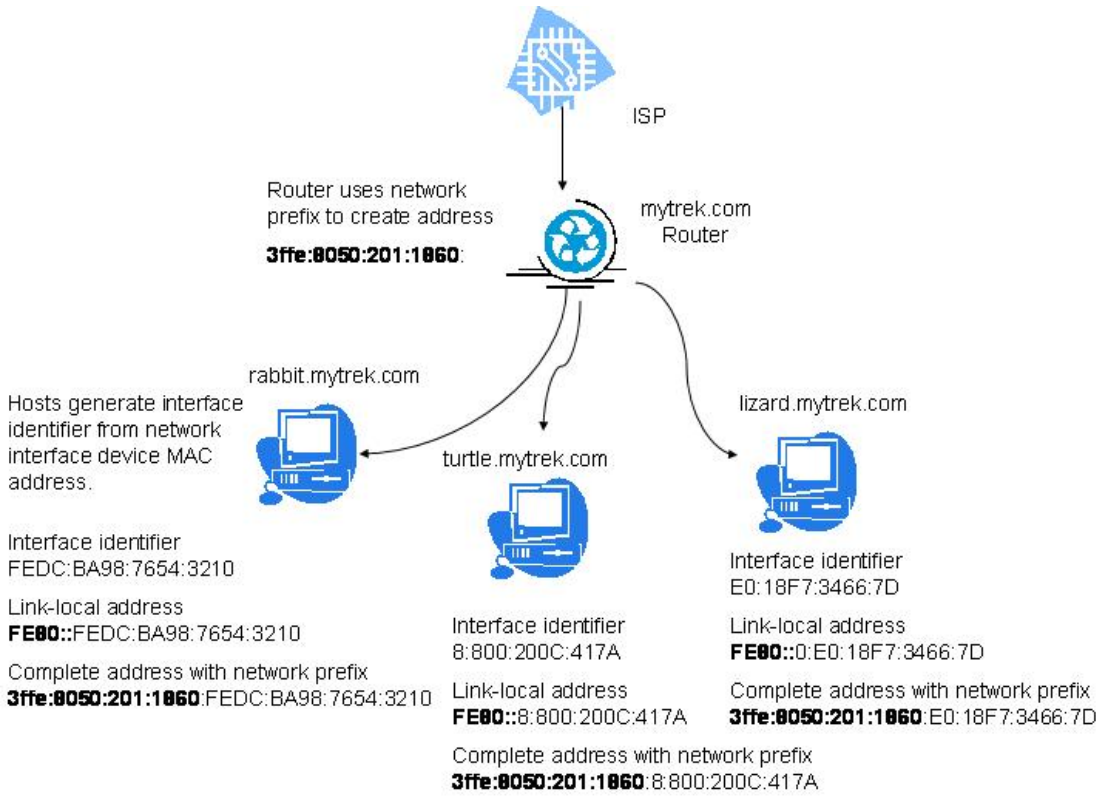
3.8 Auto-configuration

Είναι η διαδικασία κατά την οποία ένας IPv6 κόμβος δημιουργεί αυτόματα μια διεύθυνση για προσωπική χρήση. Ο κόμβος μπορεί να ρυθμίσει την διεύθυνσή του με δύο είδη αυτό-διαμόρφωσης (auto-configuration) stateless ή stateful. Κατά την stateless auto-configuration διαδικασία, ο host πρώτα διαμορφώνει για τον εαυτό του μια link-local διεύθυνση, η οποία σχηματίζεται από τον συνδυασμό δύο κομματιών πληροφορίας: από το link-local prefix και από το interface ID του κόμβου (EUI-64 MAC διεύθυνση)[2, 36].Στην συνέχεια ο host στέλνει ένα Router Solicitation μήνυμα σε μια multicast διεύθυνση δρομολογητή και αποκτά ένα ή περισσότερα network prefixes, τα οποία του αποστέλλονται μέσω Router Advertisement μηνύματος. Ο host συνδυάζει αυτά τα prefixes με το interface ID του για να δημιουργήσει την site local ή την global IPv6 διεύθυνσή του [36]. Στην Εικόνα 3.6 φαίνεται το τυπικό μοντέλο της stateless address auto-configuration διαδικασίας.



Εικόνα 3.6: Stateless Auto-configuration διαδικασία

Στην Εικόνα 3.7 φαίνεται ότι κάθε host αρχικά δημιουργεί το interface identifier, το οποίο χρησιμοποιεί για την κατασκευή της link-local διεύθυνσής του. Στην συνέχεια αποκτά το network prefix από τον δρομολογητή με σκοπό την ολοκλήρωση δημιουργίας της διεύθυνσής του.



Εικόνα 3.7: Αποτέλεσμα της Stateless Address Auto-Configuration διαδικασίας

Όσον αφορά στην διαδικασία stateful auto-configuration, ο κόμβος απευθύνεται σε έναν DHCPv6 εξυπηρετητή για να αποκτήσει την απαιτούμενη διεύθυνση και πληροφορίες για το δίκτυο [14]. Η λειτουργία του DHCPv6 είναι παρόμοια με αυτή του DHCP στο

πρωτόκολλο IPv4. Το DHCPv6 παρέχει επιπλέον πληροφορίες στον host, όπως πληροφορίες για DNS εξυπηρετητές. Το DHCPv6 μπορεί επίσης να χρησιμοποιηθεί στην περίπτωση που δεν υπάρχει κάποιος δρομολογητής στον τοπικό σύνδεσμο [36].

3.9 Μηχανισμοί Προστασίας Ιδιωτικότητας

Ένα σημαντικό ζήτημα ασφάλειας που προκύπτει από την stateless address auto-configuration λειτουργία είναι η προστασία της ιδιωτικότητας (privacy) των χρηστών. Ο default τρόπος λειτουργίας του IPv6 stateless address auto-configuration κάνει χρήση της MAC διεύθυνσης, με σκοπό την απόκτηση του interface identifier, ο οποίος είναι απαραίτητος για την δημιουργία μιας link-local διεύθυνσης. Ωστόσο, σύμφωνα με το RFC 3041, ο συγκεκριμένος μηχανισμός έχει σοβαρά προβλήματα ιδιωτικότητας, καθώς οι IPv6 διευθύνσεις ενός δεδομένου interface που δημιουργήθηκαν μέσω stateless auto-configuration περιέχουν το ίδιο interface identifier, ασχέτως το σημείο του διαδικτύου από το οποίο συνδέεται η συσκευή [28].

Ένας τρόπος για να αποφύγουμε το πρόβλημα είναι η χρήση DHCP για απόκτηση διεύθυνσης. Ωστόσο, στην περίπτωση που θέλουμε να χρησιμοποιήσουμε stateless auto-configuration μια προσέγγιση στο παραπάνω πρόβλημα είναι η συνεχής αλλαγή τμήματος του interface id μιας διεύθυνσης και η δημιουργία νέων διευθύνσεων [28]. Ωστόσο, όταν τα πρωτόκολλα κάνουν χρήση ψευδό-τυχαίων πεδίων, αυτά μπορούν να χρησιμοποιηθούν ως covert channels (κρυφά κανάλια) [29]. Αυτό σημαίνει ότι το stateless address auto-configuration μπορεί να χρησιμοποιηθεί ως covert channel, δίνοντας την δυνατότητα για κοινολόγηση κάθε μυστικού και κατά συνέπεια καταστρατήγηση της ιδιωτικής ζωής του χρήστη.

Η χρήση του SEcure Neighbor Discovery (SEND)[15] πρωτοκόλλου έναντι του απλού Neighbor Discovery προτείνεται ως λύση στο πρόβλημα των covert channels. Το SEND κάνει χρήση CGA διευθύνσεων , οι οποίες απαλύνουν επιθέσεις κατά του stateless address auto-configuration. Η ιδέα πίσω από τις CGA είναι ότι το interface identifier είναι στην πραγματικότητα ένας host (υπολογιστής/σύστημα) identifier. Ο υπολογιστής/σύστημα έχει ένα ζευγάρι δημοσίου/ιδιωτικού κλειδιού και μια σύνοψη (χρήση hash function) του δημοσίου κλειδιού, η οποία χρησιμοποιείται στον interface identifier. Οι CGA αντιμετωπίζουν αποτελεσματικά την πιθανότητα χρήσης μια διεύθυνσης ως covert channel, επειδή κάθε bit έχει σημασία. Εάν η διεύθυνση δεν ταιριάζει με την σύνοψη του δημοσίου κλειδιού που χρησιμοποιείται στο SEND , είναι εύκολο να συμπεράνουμε ότι κάποιος επιτιθέμενος έχει παρέμβει [29].

[15] Αναφορά στο κεφάλαιο 11

4

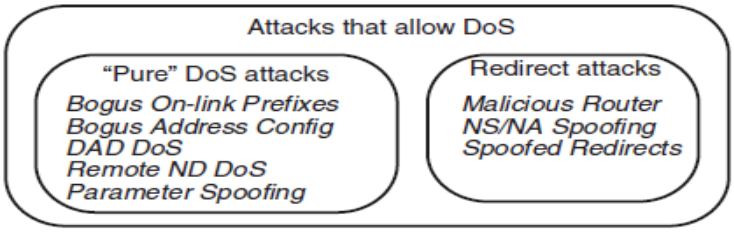
Επιθέσεις στο Neighbor & Router Discovery Protocol

Η λειτουργία stateless address auto-configuration, αποτελεί ένα ιδιαίτερο χαρακτηριστικό των IPv6 δικτύων προσφέροντας την δυνατότητα στους κόμβους για αυτόματη δημιουργία διευθύνσεων, είτε link-local (υποδικτύου) είτε global (παγκόσμιες). Ωστόσο, το stateless address auto-configuration έχει μια σειρά από ευπάθειες, τις οποίες μπορεί να εκμεταλλευτεί ένας επιτιθέμενος.

Το κυριότερο πρόβλημα που φέρει το stateless address auto-configuration είναι το μοντέλο εμπιστοσύνης, δηλαδή η εμπιστοσύνη που δείχνει ένα δίκτυο σε έναν νεοεισερχόμενο κόμβο [1]. Όπως έχει αναφερθεί μέσω της λειτουργίας stateless address auto-configuration, ένας κόμβος μπορεί να αποκτήσει link-local διεύθυνση χωρίς την οποιαδήποτε έγκριση ή έλεγχο. Οι δυνατότητες του κόμβου δεν περιορίζονται μόνο στην απόκτηση link-local διεύθυνσης, καθώς μπορεί να αποκτήσει και παγκόσμια διεύθυνση, χωρίς κάποιον ιδιαίτερο έλεγχο. Όλες οι παραπάνω λειτουργίες γίνονται μέσω των πρωτοκόλλων Neighbor Discovery και Router Discovery, τα οποία εμφανίζουν ευπάθειες και μπορεί να οδηγήσουν στην επίτευξη βασικών επιθέσεων [1].Γενικά υπάρχουν δύο τύποι απειλών στο Neighbor/Router Discovery Protocol [42]:

1. Διάφορες Denial of Service (DoS) (άρνηση υπηρεσίας) απειλές ,κατά τις οποίες ένας κακόβουλος κόμβος εμποδίζει την επικοινωνία μεταξύ του κόμβου – θύματος και των υπόλοιπων κόμβων του δικτύου.
2. Απειλές ανακατεύθυνσης (redirect), κατά τις οποίες ένας επιτιθέμενος ανακατευθύνει πακέτα μακριά από τον τελευταίο δρομολογητή προς έναν άλλο κόμβο του δικτύου. Οι επιθέσεις ανακατεύθυνσης μπορούν να χρησιμοποιηθούν με σκοπό την επίτευξη DoS επίθεσης.

Η σχέση μεταξύ των δύο κατηγοριών επιθέσεων, δηλαδή επιθέσεις που επιτρέπουν μόνο DoS και επιθέσεις που επιτρέπουν συνδυασμό DoS και ανακατεύθυνσης φαίνεται στην Εικόνα 4.1.



Εικόνα 4.1: Κατηγορίες Επιθέσεων

Στην συνέχεια παρουσιάζονται οι επιθέσεις που μπορούν να επιτευχθούν στο πρωτόκολλο Neighbor/Router Discovery.

4.1 Redirect Επιθέσεις

4.1.1 Malicious Last Hop Router

Ένας κακόβουλος δρομολογητής που βρίσκεται μέσα σε ένα δίκτυο μπορεί να ανακατευθύνει όλη την κυκλοφορία που του αποστέλλεται [26,27]. Η επίθεση έχει ως εξής: Ένας επιτιθέμενος μεταμφιέζεται ως ένας last hop δρομολογητής με την multicast ή unicast αποστολή φαινομενικά νόμιμων Router Advertisement μηνυμάτων, τα οποία απαντάνε στα multicast Router Solicitations. Εάν ένας υπολογιστής/σύστημα επιλέξει τον επιτιθέμενο ως τον default δρομολογητή του, τότε ο επιτιθέμενος έχει την ευκαιρία να αναρροφήσει (siphon off) κυκλοφορία από τον υπολογιστή/σύστημα [14].

4.1.2 Neighbor Solicitation/Advertisement Spoofing

Ένας επιτιθέμενος κόμβος μπορεί να προκαλέσει τα πακέτα που προορίζονται για νόμιμους χρήστες (hosts [υπολογιστές/συστήματα], routers [δρομολογητές]) να αποστέλλονται σε μια link-layer διεύθυνση. Αυτό μπορεί να γίνει είτε στέλνοντας ένα Neighbor Solicitation μήνυμα με μια spoofed πηγή που έχει την link-layer διεύθυνση, είτε στέλνοντας ένα Neighbor Advertisement μήνυμα κάνοντας spoof την διεύθυνση στόχο link-layer address. Εάν η spoofed link-layer διεύθυνση είναι έγκυρη και υπό τον όρο ότι ο επιτιθέμενος συνεχίσει να ανταποκρίνεται στα Neighbor Solicitation μηνύματα που του αποστέλλονται ως μέρος του Neighbor Unreachability Detection (NUD), τα πακέτα θα συνεχίσουν να ανακατευθύνονται (redirect) [14]. Αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί για την επίτευξη μιας DoS επίθεσης προσδιορίζοντας μια αχρησιμοποίητη link-layer διεύθυνση. Ωστόσο, η συγκεκριμένη επίθεση είναι περιορισμένης διάρκειας, καθώς μετά από 30-50 δευτερόλεπτα (default τιμές) ο μηχανισμός NUD θα ξεφορτωθεί την ακατάλληλη link-layer διεύθυνση και θα ψάξει για νέα. Κατά συνέπεια, ο επιτιθέμενος εάν επιθυμεί να συνεχίσει την επίθεση οφείλει να ανταποκρίνεται συνεχώς με παραποιημένες link-layer διευθύνσεις [14].

4.1.3 Spoofed Redirect Messages

Το redirect μήνυμα μπορεί να χρησιμοποιηθεί για να ανακατευθύνει πακέτα που προορίζονται για μια δοσμένη IP διεύθυνση σε οποιαδήποτε link-layer διεύθυνση εντός του δικτύου. Ο επιτιθέμενος χρησιμοποιεί την link-local διεύθυνσή του τρέχοντος first-hop δρομολογητή ως την διεύθυνση πηγής με σκοπό να αποστείλει ένα redirect μήνυμα σε έναν νόμιμο host. Από την στιγμή που ο host εξακριβώσει ότι το μήνυμα προέρχεται από τον first hop δρομολογητή, αποδέχεται το redirect. Εφόσον ο επιτιθέμενος ανταποκρίνεται στα

Neighbor Unreachability Detection probes στην link-layer διεύθυνση, το redirect θα συνεχίσει να επιδρά [14].

4.2 DoS Επιθέσεις

4.2.1 Bogus On-Link Prefix

Ένας επιτιθέμενος κόμβος μπορεί να στείλει ένα Router Advertisement μήνυμα καθορίζοντας ότι μερικά prefix αυθαίρετου μήκους είναι on-link. Εάν ένας υπολογιστής/σύστημα θεωρήσει ότι το prefix είναι on-link, δεν θα στείλει ποτέ κανένα πακέτο για αυτό το prefix στον δρομολογητή. Αντιθέτως, θα προσπαθεί να εκτελέσει address resolution στέλνοντας Neighbor Solicitations, αλλά αυτά τα μηνύματα δεν θα λάβουν ποτέ απάντηση, προκαλώντας άρνηση υπηρεσίας στο θύμα – host [14].

4.2.2 Bad prefixes

Ο κακόβουλος κόμβος, που παίζει τον ρόλο του δρομολογητή μπορεί να δημοσιεύει άκυρα prefixes, δηλαδή prefixes που δεν ανήκουν στον σύνδεσμο. Κόμβοι που αυτό-διαμορφώνονται (auto-configure) με αυτά τα prefixes σχηματίζουν άκυρες διευθύνσεις, οπότε δεν μπορούν να επικοινωνήσουν με τους υπόλοιπους κόμβους [1].

4.2.3 Failure of Duplicate Address Detection Process

Ένας κακόβουλος κόμβος μπορεί να ανταποκρίνεται λανθασμένα σε DAD αιτήσεις, με σκοπό ένας νέος κόμβος να μην μπορέσει να συνδεθεί στο υποδίκτυο. Αυτό συμβαίνει διότι ο επιτιθέμενος ισχυρίζεται ότι η δοκιμαστική διεύθυνση του νεοεισερχόμενου κόμβου χρησιμοποιείται ήδη και αναγκάζει τον κόμβο να δοκιμάσει νέα διεύθυνση, εμποδίζοντάς τον να αποκτήσει link-local διεύθυνση [1].

4.2.4 Neighbor Discovery DoS Attack

Σε αυτή την επίθεση, ο επιτιθέμενος κόμβος παραποιεί διευθύνσεις με το subnet prefix του στόχου – δικτύου και συνεχώς στέλνει πακέτα στο δίκτυο αυτό. Ο last hop δρομολογητής του δικτύου είναι υποχρεωμένος να αναλύσει αυτές τις διευθύνσεις κάνοντας χρήση του πρωτοκόλλου Neighbor Discovery. Όταν ένας νόμιμος χρήστης επιχειρήσει να εισαχθεί στο δίκτυο, ενδέχεται να μην είναι σε θέση να αποκτήσει Neighbor Discovery υπηρεσία από τον last hop δρομολογητή, καθώς ο δρομολογητής αυτός είναι ήδη απασχολημένος με την ανάλυση των πλαστών διευθύνσεων [14]. Αυτή η DoS επίθεση είναι διαφορετική από τις άλλες, διότι ο επιτιθέμενος ενδέχεται να είναι εκτός του συνδέσμου – off link (σε άλλο υποδίκτυο). Σε αυτή την περίπτωση η επίθεση γίνεται σε μια εννοιολογική neighbor cache, η οποία γεμίζει με απόπειρες ανάλυσης IPv6 διευθύνσεων (οι οποίες έχουν έγκυρο prefix και άκυρο suffix) [14].

4.2.5 Parameter Spoofing

Τα Router Advertisement μηνύματα περιέχουν ορισμένες παραμέτρους που χρησιμοποιούνται από τους hosts, καθώς και μια σημαία, η οποία ενημερώνει τους hosts αν πρέπει ή όχι να εκτελέσουν stateful address configuration [26]. Ένας επιτιθέμενος κόμβος μπορεί να στείλει ένα φαινομενικά έγκυρο RA μήνυμα, το οποίο είναι πιστή αντιγραφή του μηνύματος του νόμιμου δρομολογητή, εκτός από τις τιμές κάποιων παραμέτρων που έχουν παραποιηθεί με σκοπό την διαταραχή της νόμιμης κυκλοφορίας [14]. Έτσι για παράδειγμα ένας επιτιθέμενος μπορεί να κάνει broadcast έναν ψεύτικο ισχυρισμό, ότι το δίκτυο χρησιμοποιεί DHCP εξυπηρετητή για address configuration. Οι κόμβοι του δικτύου θα επιχειρούσαν να έρθουν σε επαφή με αυτόν τον ανύπαρκτο DHCP εξυπηρετητή με αποτέλεσμα να μην έπαιρναν ποτέ παγκόσμια διεύθυνση.

4.2.6 Failure of NUD process

Ένας κακόβουλος δρομολογητής μπορεί να εμποδίσει ένα κόμβο να προσεγγίσει έναν άλλο, στέλνοντας του πλαστά Neighbor Advertisement μηνύματα, δηλώνοντάς του ότι ο κόμβος που επιθυμεί να προσεγγίσει είναι απρόσιτος [1].

4.2.7 A non-existent address

Ένας εξωτερικός host μπορεί να στείλει κίνηση σε μια φαινομενικά νόμιμη διεύθυνση, αλλά με άκυρο interface ID. Ο δρομολογητής θα προσπαθήσει να αναλύσει αυτή την (άκυρη) διεύθυνση (ενδέχεται να λάβει και άλλες άκυρες διευθύνσεις) σπαταλώντας πόρους και ίσως γίνει θύμα μιας DoS επίθεσης [1].

4.2.8 Attack on legitimate router

Ένας κακόβουλος κόμβος μπορεί να επιτεθεί σε έναν νόμιμο δρομολογητή που βρίσκεται στο ίδιο υποδίκτυο (link router). Έχει λοιπόν την δυνατότητα να κάνει spoof την διεύθυνση του νόμιμου δρομολογητή και να εκδώσει ένα router advertisement (RA) μήνυμα με μηδενικό router lifetime, καθιστώντας τον νόμιμο δρομολογητή μη διαθέσιμο. Εναλλακτικά, ο κακόβουλος κόμβος μπορεί να επιτεθεί απευθείας στον νόμιμο δρομολογητή, με σκοπό την ανά-διαμόρφωσή του και κατά συνέπεια την δυσλειτουργία του [1].

5

Επιθέσεις που εμφανίζονται σε IPv4 και IPv6 περιβάλλοντα και παρουσιάζουν διαφορές

Στο συγκεκριμένο κεφάλαιο θα μελετήσουμε επιθέσεις που εμφανίζονται και στα δύο πρωτόκολλα IPv4 και IPv6. Ωστόσο, όταν εκτελούνται στο IPv6 παρουσιάζουν σημαντικές διαφορές. Σε ορισμένες περιπτώσεις είναι πιο εύκολες, σε άλλες πιο δύσκολες και υπάρχουν περιπτώσεις όπου αλλάζει μόνο η μέθοδος.

5.1 Reconnaissance Attack

IPv4

Η Reconnaissance Attack (αναγνωριστική επίθεση) αποτελεί συνήθως την πρώτη επίθεση που εκτελεί ένας επιτιθέμενος. Σε αυτή την επίθεση, ο επιτιθέμενος επιχειρεί να μάθει όσο το δυνατόν περισσότερες πληροφορίες για το δίκτυο του θύματος. Η συγκεκριμένη επίθεση περιλαμβάνει τόσο ενεργητικές μεθόδους εντός του δικτύου, όπως σάρωμα (scanning), όσο και παθητική εξόρυξη δεδομένων, όπως έρευνα μέσω μηχανών αναζήτησης και δημόσιων εγγράφων του θύματος. Οι ενεργητικές μέθοδοι, έχουν σκοπό να εφοδιάσουν τον επιτιθέμενο με συγκεκριμένες πληροφορίες για τα συστήματα/εξυπηρετητές και τις δικτυακές συσκευές που χρησιμοποιούνται στο δίκτυο του θύματος, για τις διασυνδέσεις τους καθώς και για τις πιθανές αδυναμίες, μέσω των οποίων μπορεί να επιτευχθεί μια πιο ενεργητική επίθεση [18]. Σε ένα IPv4 δίκτυο ο επιτιθέμενος διαθέτει αρκετές καθιερωμένες μεθόδους για την συγκέντρωση τέτοιων πληροφοριών. Τέτοιες μέθοδοι είναι [18]:

- **Ping sweeps**. Προσδιορίζοντας τις IPv4 διευθύνσεις που χρησιμοποιούνται σε έναν οργανισμό (μέσω ενεργών ερευνών [active probes]), ένας επιτιθέμενος μπορεί να σαρώσει ένα δίκτυο στέλνοντας ICMP μηνύματα (ή μηνύματα επιπέδου μεταφοράς), επιδιώκοντας μια απάντηση (τα μηνύματα δεν φιλτράρονται στα σύνορα του δικτύου). Ακολουθώντας αυτήν τη σάρωση, ο επιτιθέμενος χρησιμοποιεί τα δεδομένα για να σχηματίσει μια γενική εικόνα, σχετικά με την διάταξη του δικτύου [18]. Το traceroute και firewalk αποτελούν εργαλεία, τα οποία μπορούν να βοηθήσουν τον επιτιθέμενο να συλλέξει δεδομένα.
- **Port scans**. Μετά τον προσδιορισμό των προσεγγίσιμων συστημάτων, ο επιτιθέμενος διερευνά τις θύρες (επίπεδο μεταφοράς) κάθε συστήματος, με σκοπό να προσδιορίσει ποιες είναι ενεργές και στην συνέχεια να εξετάσει ποιες υπηρεσίες τρέχουν σε αυτές τις θύρες. Αφού συγκεντρώσει πληροφορίες για τις θύρες και τις αντίστοιχες υπηρεσίες μπορεί να προχωρήσει στην επόμενη φάση [18].

- **Application and vulnerability scans.** Στην συνέχεια ο επιτιθέμενος μπορεί να αποκτήσει πιο συγκεκριμένες πληροφορίες, όπως ποιο λειτουργικό σύστημα τρέχει στην συσκευή του θύματος, καθώς και να εξετάσει για τυχόν παρουσία γνωστών ευπαθειών, με σκοπό την εκμετάλλευσή τους (exploitation). Όλες οι παραπάνω σαρώσεις μπορούν να επιτευχθούν την ίδια στιγμή κάνοντας χρήση εργαλείων, όπως το Nmap [18].

IPv6

Σε ένα δίκτυο IPv6, η αναγνωριστική επίθεση είναι διαφορετική από αυτή που συμβαίνει σε ένα IPv4 δίκτυο, κυρίως για δύο λόγους [18]. Ο πρώτος είναι ότι όταν εκτελούνται ping sweeps ή port scans, με σκοπό την απαρίθμηση των υπολογιστών/συστημάτων σε ένα IPv6 υποδίκτυο, είναι πολύ πιο δύσκολο να ολοκληρωθούν σε σχέση με το αν εκτελούνταν σε ένα IPv4 δίκτυο. Ο δεύτερος λόγος είναι ότι οι νέες multicast διευθύνσεις του IPv6, δίνουν την δυνατότητα σε έναν επιτιθέμενο να ανακαλύψει ορισμένα συστήματα ζωτικής σημασίας (key systems [routers, Network Time Protocol servers, κτλ.]) πιο εύκολα. Στην συνέχεια θα γίνει ανάλυση των δύο παραπάνω λόγων που διαφοροποιούν μια reconnaissance attack στα δίκτυα IPv4 και IPv6.

Πρώτος λόγος διαφοροποίησης

Το μέγεθος ενός IPv6 δικτύου είναι 64 bits, σε αντίθεση με το μέγεθος ενός IPv4 δικτύου που είναι 8 bits. Αυτό αυξάνει το μέγεθος σαρώματος για τον έλεγχο κάθε host κατά 2^{64}-2^{8} (περίπου 18 εξάκις εκατομμύρια). Έτσι, ενώ σε ένα δίκτυο απαιτούνταν η αποστολή 256 probes, τώρα απαιτούνται περισσότερα από 18 εξάκις εκατομμύρια probes για να καλύψουν ολόκληρο το δίκτυο. Παρακάτω αναφέρεται ένα παράδειγμα [18] με σκοπό να γίνει αντιληπτή η δυσκολία σάρωσης ενός IPv6 δικτύου. Έστω ένα δίκτυο που περιέχει 10,000 υπολογιστές/συστήματα (έστω επίσης ότι μία στις 1,8 πεντάκης εκατομμύριο διευθύνσεις είναι απασχολημένες). Ακόμα και με ένα σάρωμα που θα είχε ρυθμό 1 εκατομμύριο probes/sec (περισσότερα από 400Mbps δικτυακής κυκλοφορίας), θα απαιτούνταν περισσότερα από 28 χρόνια συνεχόμενου σαρώματος μέχρι να βρισκόταν ο πρώτος ενεργός υπολογιστής/σύστημα[16].

Παρόλο που ο χώρος αναζήτησης σε ένα δίκτυο IPv6 είναι τεράστιος, υπάρχουν ορισμένες παράμετροι [18] που βοηθούν το σάρωμα ενός επιτιθέμενου. Πρώτον, οι δημόσιες υπηρεσίες του διαδικτύου χρειάζεται να είναι προσεγγίσιμες με το DNS, δίνοντας στον επιτιθέμενο την δυνατότητα για επίθεση σε τουλάχιστον ένα μικρό αριθμό από κρίσιμους υπολογιστές/συστήματα. Δεύτερον, η τεράστια μορφή που έχουν οι IPv6 διευθύνσεις και η έλλειψη ανάγκης για Network Address Translation (NAT), προκαλεί την ανάγκη στα δίκτυα να υιοθετήσουν δυναμικούς DNS ή άλλους μηχανισμούς, ώστε να διασφαλίσουν ότι οι υπολογιστές/συστήματα έχουν μια έγκυρη διεύθυνση. Αυτό σημαίνει ότι μια επίθεση σε έναν DNS server στο εσωτερικό ενός οργανισμού θα μπορούσε να αποφέρει τεράστια caches από υπολογιστές/συστήματα [18]. Τρίτον, οι διαχειριστές για την διευκόλυνσής τους μπορούν να επιλέξουν ευκολομνημόνευτες διευθύνσεις για κάποια key systems (συστήματα – κλειδιά), με αποτέλεσμα ένας αντίπαλος να είναι σε θέση να

[16] Υποθέτουμε ότι η πρώτη επιτυχία συμβαίνει μετά το 50% των πρώτων πεντάκις εκατομμυρίων διευθύνσεων.

εκτελέσει επίθεση σε αυτά τα key systems. Τέλος, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί τις ευπάθειες ενός μη ασφαλούς δρομολογητή ή άλλης gateway συσκευής, ώστε να παρακολουθήσει την neighbor-discovery cache data (ισοδύναμη με μια ARP cache), να ανακαλύψει διαθέσιμους υπολογιστές/συστήματα και να εκτελέσει επιθέσεις σε αυτούς τους υπολογιστές [18].

Δεύτερος λόγος διαφοροποίησης

Ο δεύτερος λόγος για τον οποίο διαφέρει μια αναγνωριστική επίθεση σε ένα IPv6 δίκτυο από αυτή ενός IPv4 δικτύου είναι οι νέες multicast διευθύνσεις του IPv6. Οι multicast διευθύνσεις του IPv6 δίνουν την δυνατότητα σε έναν επιτιθέμενο να προσδιορίσει σημεία – κλειδιά μέσα σε ένα δίκτυο και να επιτεθεί σε αυτά [18]. Σύμφωνα με το RFC 2375 αυτές οι διευθύνσεις έχουν ένα κόμβο, ένα σύνδεσμο ή ένα site-specific domain για χρήση. Έτσι, για παράδειγμα όλοι οι δρομολογητές (FF05::2) και όλοι οι DHCP servers (FF05::4) έχουν μία site-specific διεύθυνση. Οπότε για λόγους ασφάλειας, είναι σημαντικό να μην επιτρέπεται η πρόσβαση σε αυτές τις διευθύνσεις εσωτερικής χρήσης από υπολογιστές/συστήματα που βρίσκονται εκτός δικτύου. Αυτό μπορεί να επιτευχθεί με το φιλτράρισμα της δικτυακής κίνησης στα "σύνορα" του δικτύου.

5.2 Unauthorized Access

Η μη εξουσιοδοτημένη πρόσβαση αναφέρεται στην τάξη επιθέσεων, κατά τις οποίες ο επιτιθέμενος επιχειρεί να εκμεταλλευτεί την ανοιχτή πολιτική ασφάλειας που εμπεριέχεται στο πρωτόκολλο IPv4. Στην στοίβα πρωτοκόλλου IP, τίποτα δεν περιορίζει ένα σύνολο από hosts να εγκαθιδρύσουν σύνδεση με έναν άλλο host μέσα σε ένα IP δίκτυο. Οι επιτιθέμενοι βασίζονται πάνω σε αυτό το γεγονός με αποτέλεσμα να εγκαθιδρύουν συνδέσεις έχοντας κακόβουλο σκοπό [18].

IPv4 δίκτυα

Τα IPv4 δίκτυα περιορίζουν το πρόβλημα μη εξουσιοδοτημένης πρόσβασης (unauthorized access), αναπτύσσοντας μηχανισμούς ελέγχου πρόσβασης εντός των end systems (τελικών συστημάτων) αλλά και στις gateway συσκευές που βρίσκονται μεταξύ των τελικών χρηστών. Οι έλεγχοι αυτοί μπορούν να εφαρμοστούν στο επίπεδο δικτύου (Layer 3) και στο επίπεδο μεταφοράς (Layer 4). Στο επίπεδο δικτύου, ο αμυνόμενος χρησιμοποιεί βασικές λίστες ελέγχου πρόσβασης (access control lists [ACLS]), ώστε να επιτρέπει μόνο στους εγκεκριμένους hosts να στέλνουν πακέτα σε μια συσκευή [18]. Τα ACLS χρησιμοποιούν συγκεκριμένες πολιτικές ασφάλειας που θέτουν ορισμένα όρια στην κίνηση που εισέρχεται ή εξέρχεται από μια συσκευή, με σκοπό να περιοριστούν οι λεωφόροι επίθεσης σε συγκεκριμένες υπηρεσίες που είναι διαθέσιμες στο δίκτυο. Στα IPv4 δίκτυα, οι έλεγχοι πρόσβασης υλοποιούνται σε δικτυακές συσκευές (firewalls) και σε end συσκευές (host firewalls).

IPv6 δίκτυα

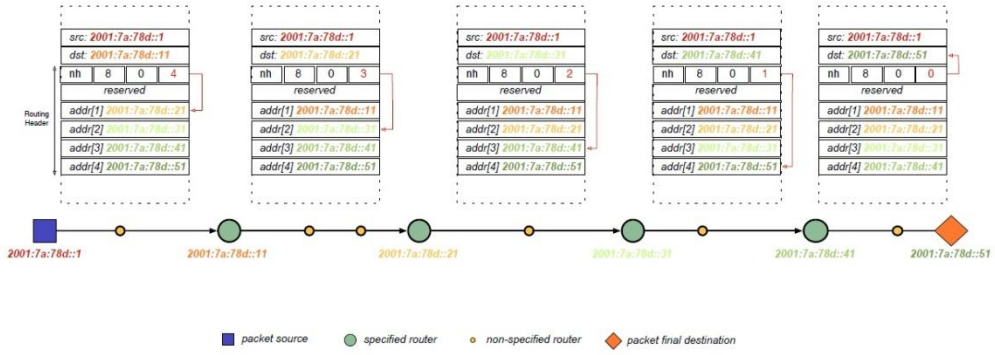
Η ανάγκη για τεχνολογίες ελέγχου πρόσβασης είναι ίδιες στα πρωτόκολλα IPv4 και IPv6, παρόλο που η απαίτηση για χρήση IPsec (στο IPv6) διευκολύνει τον έλεγχο πρόσβασης [18].

Ο έλεγχος πρόσβασης στο IPv6 αλλάζει σε σχέση με το IPv4, λόγω της διαφορετικής αρχιτεκτονικής που χρησιμοποιείται στα συστήματα διευθυνσιοδότησης και δρομολόγησης. Έτσι για παράδειγμα ένας σχεδιαστής δικτύου IPv6 μπορεί να αναθέσει global unicast διευθύνσεις μόνο στις συσκευές εκείνες που χρειάζονται να επικοινωνήσουν με κόμβους του διαδικτύου, ενώ αναθέτει site-local διευθύνσεις σε συσκευές που χρειάζεται να επικοινωνήσουν εντός ενός οργανισμού, έτσι ο έλεγχος πρόσβασης περιορίζεται μόνο στους τελικούς κόμβους.

5.3 Routing Header

Ένα σημαντικό ζήτημα ασφάλειας, που έχει σχέση με τον έλεγχο πρόσβασης προκύπτει από τους routing headers που χρησιμοποιούνται στο IPv6. Σύμφωνα με την τεκμηρίωση του πρωτοκόλλου IPv6, όλοι οι IPv6 κόμβοι πρέπει να είναι ικανοί να επεξεργαστούν routing headers. Δυστυχώς, οι routing headers μπορούν να χρησιμοποιηθούν για να αποφευχθεί ο έλεγχος πρόσβασης [4], συμπεριφορά που μπορεί να δημιουργήσει προβλήματα ασφάλειας. Υπάρχει λοιπόν η πιθανότητα, ένας εισβολέας να στείλει ένα πακέτο σε μια δημόσια προσπελάσιμη διεύθυνση με έναν routing header, ο οποίος να περιέχει μια “forbidden” (απαγορευμένη) διεύθυνση (διεύθυνση δικτύου του θύματος). Σε αυτή την περίπτωση ο δημόσια προσπελάσιμος υπολογιστής/σύστημα θα προωθήσει το πακέτο στην διεύθυνση προορισμού που δηλώνεται στον routing header (“forbidden” address), παρόλο που αυτή είναι φιλτραρισμένη (filtered) [4], έχοντας έτσι την δυνατότητα να προβεί σε κακόβουλες ενέργειες. Άρα ο επιτιθέμενος καταφέρνει να προσπελάσει έναν “κρυφό” host, μέσω ενός ορατού host.

Για να γίνει πιο κατανοητή η επίθεση θα χρησιμοποιήσουμε ένα παράδειγμα. Ένας επιτιθέμενος στέλνει ένα πακέτο από την διεύθυνση πηγής 2001:7a:78d::1 στην διεύθυνσης προορισμού 2001:7a:78d::11. Ο επιτιθέμενος δεν επιθυμεί το πακέτο να δρομολογηθεί απευθείας από την διεύθυνση πηγής στην διεύθυνση προορισμού, αλλά χρησιμοποιεί το routing header επιχειρώντας να προσπελάσει “αόρατες – απαγορευμένες” διευθύνσεις. Έτσι στο routing header χρησιμοποιεί διευθύνσεις, όπως 2001:7a:78d::21, 2001:7a:78d::31 και 2001:7a:78d::41, οι οποίες είναι απαγορευμένες. Στην Εικόνα 5.1 φαίνεται η διαδικασία προσέγγισης απαγορευμένων hosts μέσω του routing header.



Εικόνα 5.1: Προσέγγιση forbidden host μέσω routing header

5.4 Header Manipulation & Fragmentation

Σε αυτή την κατηγορία ανήκουν επιθέσεις κατακερματισμού (fragmentation attack) και επιθέσεις που βασίζονται στην αθέμιτη εκμετάλλευση της κεφαλίδας ενός πακέτου (manipulation attack). Αυτή η κατηγορία επιθέσεων χρησιμοποιείται για δύο σκοπούς. Η πρώτη επιδίωξη είναι η χρήση του κατακερματισμού ως ένα μέσο για αποφυγή των δικτυακών συσκευών ασφαλείας, όπως Network Intrusion Detection Systems (NIDS) και stateful firewalls.[17] Ο δεύτερος σκοπός είναι η χρήση fragmentation ή header manipulation για άμεση επίτευξη επίθεσης σε μια δικτυακή υποδομή [18].

IPv4 δίκτυα

Ο κατακερματισμός στα IPv4 δίκτυα είναι μια τεχνική που χρησιμοποιείται για να “ταιριάξει” το IPv4 datagram στο μικρότερο MTU μέσα σε ένα μονοπάτι μεταξύ τελικών hosts. Στο IPv4 ο κατακερματισμός μπορεί να χρησιμοποιηθεί για να παρακάμψει τους ελέγχους πρόσβασης σε συσκευές, όπως δρομολογητές και αναχώματα ασφάλειας (firewalls). Επίσης, ο κατακερματισμός μπορεί να χρησιμοποιηθεί για να “θολώσει” σκόπιμα μια επίθεση, με σκοπό να παρακάμψει την εποπτεία κάποιου μηχανισμού ασφάλειας, όπως NIDS [18]. Γενικότερα, μεγάλα ποσά κατακερματισμένης κυκλοφορίας συνηθίζεται να χρησιμοποιούνται ως ένδειξη απόπειρας εισβολής, καθώς από στατιστικά δεδομένα φαίνεται ότι το ποσοστό κατακερματισμένης κυκλοφορίας που “ταξιδεύει” μέσα στο διαδίκτυο είναι μικρό [32].

IPv6 δίκτυα

Σύμφωνα με την τεκμηρίωση του IPv6 πρωτοκόλλου, ο κατακερματισμός των πακέτων (fragmentation packet) δεν επιτρέπεται από τους ενδιάμεσους κόμβους ενός μονοπατιού. Από την στιγμή που η χρήση της μεθόδου MTU discovery αποτελεί υποχρέωση σε ένα δίκτυο IPv6, ο κατακερματισμός των πακέτων είναι δυνατό να συμβαίνει μόνο στον κόμβο πηγή [4]. Η πιο κοινή επίθεση κατακερματισμού, χρησιμοποιεί overlapping fragments

[17] Περιγράφονται στο κεφάλαιο 10

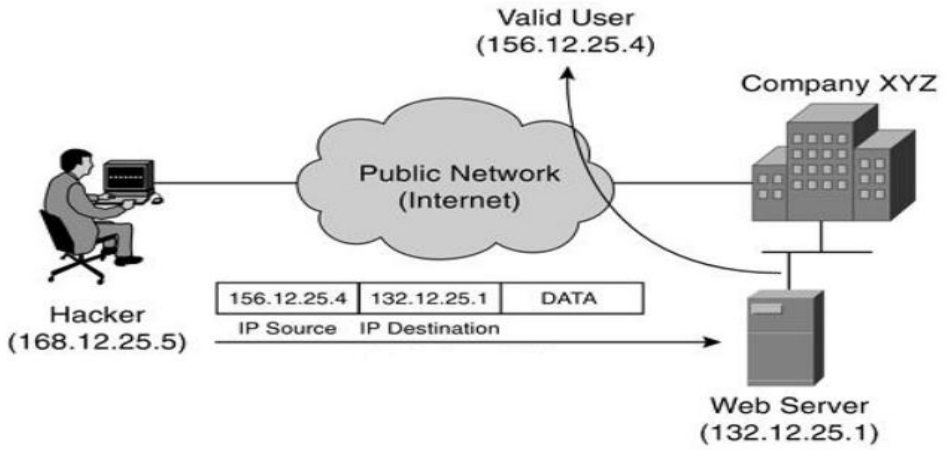
(επικαλυπτόμενα τμήματα) για να καλύψει επιθέσεις από την εποπτεία IPv4 συσκευών ασφάλειας. Ωστόσο, στο IPv6 η χρήση overlapping fragments δεν ενδείκνυται, καθώς μπορούν να θεωρηθούν ως απόπειρα επίθεσης και να απορριφθούν. Επιπλέον, αν επιτραπεί στα overlapping fragments να παρακάμψουν μια συσκευή ασφάλειας, αρκετά λειτουργικά συστήματα των τελικών hosts θα “ρίξουν” τα overlapping fragments στο λογισμικό της στοίβας του IPv6 [18]. Ωστόσο, εάν τα λειτουργικά συστήματα δεν αποδέχονται overlapping fragments, δεν υπάρχει κάτι που να εμποδίζει τον επιτιθέμενο να εκτελέσει μια επίθεση όμοια με αυτή στο IPv4, κάνοντας χρήση overlapping fragments. Επιπλέον, ένας επιτιθέμενος μπορεί να επιχειρήσει να χρησιμοποιήσει out-of-order fragments για να παρακάμψει τις string signatures ενός network-based IDS [18].

Σύμφωνα με το RFC 2460, το ελάχιστο MTU σε ένα δίκτυο IPv6 είναι 1280 octets. Για αυτό το λόγο οι διαχειριστές επιτρέπουν σε μια συσκευή ασφαλείας να απορρίπτει fragments μικρότερα από 1280 octets, εκτός αν το πακέτο είναι το τελευταίο σε μια ροή. Οι διαχειριστές μπορούν να εκτελέσουν την παραπάνω διαδικασία, εάν το λειτουργικό σύστημα του αποστολέα κατακερματίζει τα πακέτα βάση του MTU (με την βοήθεια PMTU μηνυμάτων) και συνεχίζει να δημιουργεί αυτό το μέγεθος θραυσμάτων (fragments) μέχρι να σταλεί και το τελευταίο κομμάτι πακέτου [18]. Εάν το λειτουργικό σύστημα του υπολογιστή (host) δεν συμπεριφέρεται με αυτόν τον τρόπο, τότε η συσκευή ασφάλειας (που βρίσκεται στον προορισμό) θα συνεχίσει να αποδέχεται και να επεξεργάζεται τα IPv6 fragments ακόμα και αν αυτά έχουν μέγεθος μικρότερο από 1280 octets. Αυτή η συμπεριφορά επιτρέπει σε έναν επιτιθέμενο να κάνει ασαφείς τις επιθέσεις, στέλνοντας μεγάλα ποσά μικρών κατακερματισμένων πακέτων [18].

Παρόμοια με το IPv4, τα τωρινά IPv6 firewalls και IDS υλοποιούν ελέγχους κατακερματισμού με σκοπό να απαλύνουν τις fragmentation επιθέσεις. Αυτοί οι έλεγχοι κατακερματισμού περιλαμβάνουν εξέταση των εκτός σειράς (out-of-sequence) fragments και αντιμετάθεσή τους στην σωστή σειρά. Επίσης, εξετάζουν των αριθμό fragments που στέλνονται από μια συγκεκριμένη IP με έναν μοναδικό προσδιοριστή (identifier) για να προσδιορίσουν τυχόν denial-of-service επιθέσεις.

5.5 Layer 3 – Layer 4 Spoofing

Ένα στοιχείο κλειδί που επιτρέπει την επίτευξη διαφόρων τύπων IP επιθέσεων, είναι η δυνατότητα που έχει ένας επιτιθέμενος να αλλάξει την IP διεύθυνση πηγής και τις θύρες επικοινωνίας με σκοπό να φαίνεται ότι η δικτυακή κυκλοφορία προέρχεται από κάποια άλλη τοποθεσία ή από κάποια άλλη εφαρμογή [18]. Αυτή η τεχνική ονομάζεται spoofing attack (Εικόνα 5.2) και είναι ιδιαίτερα διαδεδομένη παρόλο την ύπαρξη διαφόρων πρακτικών που μετριάσουν την χρησιμότητά της.



Εικόνα 5.2: IP Spoofing

IPv4 δίκτυα

Οι επιθέσεις τύπος spoofing (κυρίως του επιπέδου 3 – επίπεδο δικτύου) αποτελούν επιθέσεις που συμβαίνουν σε καθημερινή βάση. Επιθέσεις όπως DoS, spam και virus attack είναι δυσκολότερο να αποτραπούν αν γίνεται χρήση spoofing τεχνικών. Γενικά οι spoofing επιθέσεις επιπέδου 3 δεν χρησιμοποιούνται σε διαδραστικές επιθέσεις, αφού η "επιστρέφουσα" κυκλοφορία δρομολογείται προς την spoofed τοποθεσία, απαιτώντας από τον επιτιθέμενο να "μαντέψει" το περιεχόμενο αυτής της κυκλοφορίας [18]. Σε αντίθεση, το spoofing επιπέδου 4 (επίπεδο μεταφοράς) μπορεί να χρησιμοποιηθεί σε διαδραστικές επιθέσεις με σκοπό να κάνει την κυκλοφορία να δείχνει ότι προέρχεται από μια τοποθεσία, η οποία είναι διαφορετική από την πραγματική τοποθεσία προέλευσης της κυκλοφορίας. Σύμφωνα με το RFC 2827 υπάρχουν μέθοδοι για την υλοποίηση φίλτρων εισόδου, τα οποία εμποδίζουν την spoofed κυκλοφορία στο επίπεδο 3. Ωστόσο, σε γενικές γραμμές αυτές οι μέθοδοι φιλτραρίσματος δεν υλοποιούνται και επειδή απαιτείται ευρεία χρήση τέτοιων μεθόδων για να υπάρξει σημαντικό όφελος, η spoofed κυκλοφορία παραμένει συνηθισμένο χαρακτηριστικό. Επίσης, σύμφωνα με το RFC 2827 δεν γίνεται spoofed ολόκληρη η IP διεύθυνση, έτσι το network κομμάτι της διεύθυνσης δεν μπορεί να τροποποιηθεί (spoofed), σε αντίθεση με το host κομμάτι. Για παράδειγμα έστω ότι έχουμε ένα δίκτυο με διεύθυνση 192.0.2.0/24, το οποίο φιλτράρει και απορρίπτει πακέτα που προέρχονται από διευθύνσεις εκτός δικτύου. Έτσι εάν ένας επιτιθέμενος κάνει spoofed μια διεύθυνση, έχοντας ως διεύθυνση προέλευσης την 192.0.3.0, τότε η κυκλοφορία που προέρχεται από αυτή την διεύθυνση θα απορριφθεί αμέσως. Από την άλλη μεριά, αν γίνει spoofed μια εσωτερική διεύθυνση (192.0.2.0-255) η κυκλοφορία θα θεωρηθεί ότι προέρχεται από την διεύθυνση που δηλώνεται και δεν θα γίνει αντιληπτή η spoofing επίθεση [18].

Η πρώτη ενέργεια στην οποία πρέπει να προβεί ένας διαχειριστής για να αποφύγει τέτοιου είδους επιθέσεις είναι να κάνει track (ανίχνευση της πορείας που ακολούθησε το πακέτο για να φτάσει στον προορισμό) της επίθεσης, μια δυνατότητα που προσφέρεται στους διαχειριστές σύμφωνα με το RFC 2827. Επιπλέον, ένας διαχειριστής έχει την δυνατότητα βάση μιας πολιτικής ασφάλειας να μην διανέμει στους υπολογιστές/συστήματα ένα σύνολο από διευθύνσεις, οι οποίες μπλοκάρονται [18]. Όταν ένα πακέτο προέρχεται από μια τέτοια διεύθυνση γίνεται αντιληπτό ότι πρόκειται για

spoofing επίθεση, καθώς αυτή η διεύθυνση δεν χρησιμοποιείται, οπότε το πακέτο απορρίπτεται και η spoofing επίθεση αντιμετωπίζεται με επιτυχία.

IPv6 δίκτυα

Όσον αφορά το spoofing επιπέδου 3 σε ένα δίκτυο IPv6, σημαντικό ρόλο παίζει η παγκόσμια ενιαία φύση των IPv6 διευθύνσεων [18]. Σε αντίθεση με το IPv4, στο IPv6 ο καταμερισμός των διευθύνσεων γίνεται με τέτοιο τρόπο, ώστε να μπορούν εύκολα να συνοψιστούν σε διάφορα σημεία του δικτύου. Αυτό επιτρέπει στους παρόχους υπηρεσιών διαδικτύου (Internet Service providers [ISPs]) να εφαρμόσουν τις μεθόδους φιλτραρίσματος που περιγράφει το RFC 2827 με σκοπό να εξασφαλίσουν ότι τουλάχιστον οι δικοί τους πελάτες δεν θα κάνουν spoofing διευθύνσεις που βρίσκονται έξω από το φάσμα διευθύνσεων που παρέχει ο ISP [18]. Δυστυχώς, η παραπάνω διαδικασία δεν αποτελεί πρότυπο, οπότε δεν έχει καθιερωθεί και απαιτεί ευσυνείδητη υλοποίηση από την πλευρά των παρόχων. Οι spoofing επιθέσεις επιπέδου 4 (επίπεδο μεταφοράς) δεν παρουσιάζουν αλλαγές στο IPv6, καθώς τα πρωτόκολλα του συγκεκριμένου επιπέδου δεν αλλάζουν όσον αφορά το spoofing [18]. Κατά την παρούσα περίοδο, το spoofing στο επίπεδο 3 μπορεί να μετριασθεί κάνοντας χρήση όμοιων τεχνικών με αυτές του IPv4, όπως ACLS (access control list). Επιπλέον, μια spoofed κυκλοφορία μπορεί να ανιχνευθεί κάνοντας χρήση IPv6 firewalls ή IDSs.

5.6 DHCPv6 Επιθέσεις

Το Dynamic Host Configuration Protocol (DHCP) υπάρχει και στο IPv6 και προσδιορίζεται στο RFC 3315. Το DHCPv6 μπορεί να αντικαταστήσει την stateless address auto-configuration (SLAAC) λειτουργία παρέχοντας μια IPv6 διεύθυνση σε ένα κόμβο (stateful κατάσταση) ή μπορεί να συμπληρώσει την SLAAC γνωστοποιώντας διάφορες πληροφορίες στον κόμβο, όπως διευθύνσεις του Domain Name System (DNS) εξυπηρετητή ή του Network Time Protocol (NTP) εξυπηρετητή [33]. Όταν μια διεύθυνση "νοικιάζεται - μισθώνεται" (leased) σε έναν κόμβο, αυτό ονομάζεται stateful λειτουργία, επειδή ο DHCP εξυπηρετητής πρέπει να διατηρήσει μια κατάσταση (την IPv6 διεύθυνση που νοικιάζεται στον DHCP πελάτη). Το DHCPv6 είναι παρόμοιο με το IPv4 DHCP με τις ακόλουθες εξαιρέσεις [33]:

- Ένας DHCPv6 πελάτης μπορεί να κάνει αίτηση για πολλαπλές IPv6 διευθύνσεις.
- Το DHCPv6 δεν βασίζεται στο broadcast αλλά στο multicast. Χρησιμοποιεί την ff02::1:2, δηλαδή την link-local multicast address για όλους τους DHCP servers και agents.
- Οι πελάτες και οι εξυπηρετητές προσδιορίζονται από έναν μοναδικό προσδιοριστή (DHCP Unique Identifier [DUID]), ο οποίος δημιουργείται τοπικά (για παράδειγμα, βασίζεται στον χρόνο και στην link-local address).
- Όλες οι ανταλλαγές μηνυμάτων περιλαμβάνουν ένα 24-bit προσδιοριστή συναλλαγής (transaction identifier), που χρησιμοποιείται για να συγχρονίζει την αποκρίσεις του server στα μηνύματα του πελάτη.

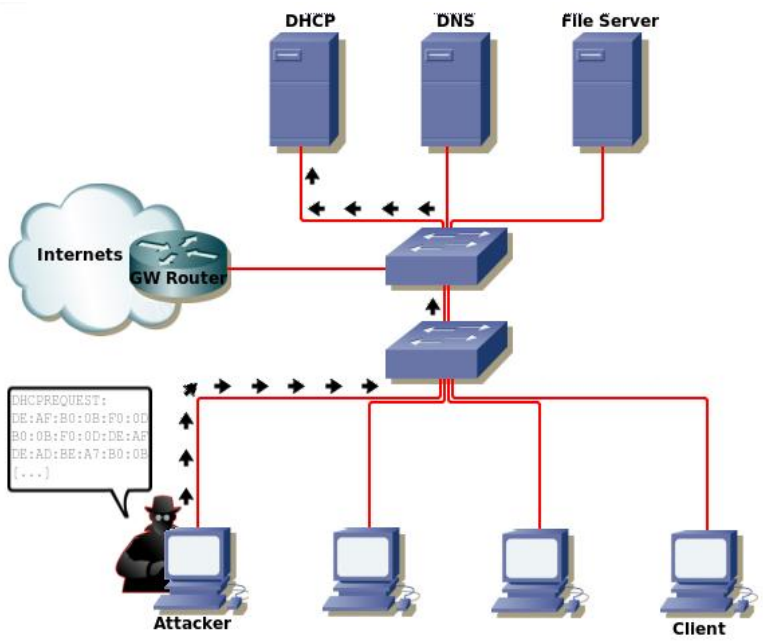
- Τα μηνύματα μπορούν προαιρετικά να αυθεντικοποιηθούν με την βοήθεια ενός Hash-based Message Authentication Code (HMAC)[18], που εφαρμόζεται σε ολόκληρο το μήνυμα.
- Οι πελάτες ακούνε (listen) στην UDP θύρα 546 και οι εξυπηρετητές στην UDP θύρα 547.

Απειλές στο DHCPv6

Σε αυτό το σημείο θα γίνει περιγραφή των βασικών απειλών που λαμβάνουν χώρα στο DHCPv6 [33]:

- **Starvation:** Ο επιτιθέμενος παίζει τον ρόλο πολλών DHCPv6 πελατών και απαιτεί πάρα πολλές διευθύνσεις, κατάσταση που μειώνει τις IPv6 διευθύνσεις (Εικόνα 5.3).
- **Denial of Service (DoS):** Ο επιτιθέμενος στέλνει μία τεράστια ποσότητα από SOLICIT μηνύματα στους εξυπηρετητές, αναγκάζοντάς τους να εγκαταστήσουν μία κατάσταση (state) προκαλώντας ένα τεράστιο φορτίο, το οποίο πρέπει να τεθεί σε επεξεργασία από τους επεξεργαστές των εξυπηρετητών (server's CPU). Το φορτίο είναι τόσο μεγάλο που όλοι οι πόροι του εξυπηρετητή δαπανώνται στην επεξεργασία του, με αποτέλεσμα οι νόμιμοι πελάτες να μην μπορούν να εξυπηρετηθούν.
- **Scanning:** Αν οι διευθύνσεις που παρέχονται από τον DHCPv6 εξυπηρετητή δημιουργούνται ακολουθούμενες μια διαδοχική αρίθμηση (sequential numbering), τότε το σάρωμα ενός IPv6 δικτύου (reconnaissance attack) γίνεται πιο εύκολο και κατ' επέκταση διευκολύνεται η ανίχνευση συστημάτων κλειδιών.
- **Misinformation (rogue DHCPv6 server):** Ο επιτιθέμενος στέλνει πλαστογραφημένα ADVERTISE και REPLY μηνύματα στους νόμιμους πελάτες. Αυτά τα πλαστογραφημένα μηνύματα περιέχουν παραποιημένες πληροφορίες για τους default gateway, DNS servers κτλ. με σκοπό την ανακατεύθυνση (redirect) της δικτυακής κυκλοφορίας. Η misinformation απειλή είναι ιδιαίτερα σημαντική στο IPv6, καθώς το sniffing (υποκλοπή) είναι πιθανό να συμβεί ακόμα και σε switched δίκτυο, σε αντίθεση με το IPv4, όπου ο επιτιθέμενος χρειάζεται να είναι στο ίδιο LAN με το θύμα, καθώς στο IPv4 δεν μπορεί να εισαγάγει τον εαυτό του στο DHCPv4 relay configuration.

[18] Στην κρυπτογραφία, το HMAC αποτελεί μια συγκεκριμένη δομή για τον υπολογισμό ενός message authentication code (MAC), κάνοντας χρήση μιας κρυπτογραφικής συνάρτησης κατακερματισμού (cryptographic hash function) σε συνδυασμό με ένα μυστικό κλειδί. Το HMAC μπορεί να χρησιμοποιηθεί για επιβεβαίωση αυθεντικότητας και επαλήθευση ακεραιότητας του μηνύματος .



Εικόνα 5.3: DHCP starvation attack

5.7 Broadcast Amplification Attacks (Smurf)

Οι Broadcast amplification επιθέσεις, γνωστές ως smurf επιθέσεις, αποτελούν DoS επιθέσεις. Ο επιτιθέμενος αποστέλλει ένα echo-request μήνυμα με διεύθυνση προορισμού την broadcast διεύθυνση ενός δικτύου και με διεύθυνση πηγής την IP διεύθυνση του θύματος, αφού πρώτα έχει κάνει χρήση spoof τεχνικής. Με αυτό τον τρόπο πετυχαίνει μια DoS επίθεση στο θύμα, καθώς όλοι οι hosts του δικτύου θα απαντήσουν στην spoof διεύθυνση πηγής με echo-reply μηνύματα, προκαλώντας πλημμύρα [18].

IPv4

Στα IPv4 δίκτυα η συγκεκριμένη επίθεση μπορεί να περιορισθεί εάν απενεργοποιηθεί από τον δρομολογητή η broadcast διεύθυνση του δικτύου. Έτσι, εάν ο επιτιθέμενος στείλει ένα echo-request μήνυμα στην broadcast διεύθυνση του δικτύου (έχοντας κάνει spoof την διεύθυνση του θύματος), τότε ο δρομολογητής θα στείλει ένα μόνο echo-reply μήνυμα στο θύμα. Άρα, ο επιτιθέμενος δεν θα μπορέσει να πραγματοποιήσει την DoS επίθεση.

IPv6

Στο πρωτόκολλο IPv6 δεν υπάρχουν broadcast διευθύνσεις, οπότε μας απασχολούν μόνο οι multicast. Για να αντιμετωπιστούν οι smurf επιθέσεις, το RFC 2463 δηλώνει ότι ένα ICMPv6 μήνυμα δεν θα πρέπει να δημιουργείται και να αποστέλλεται ως απάντηση σε έναν αποστολέα που έστειλε ένα πακέτο σε μια multicast διεύθυνση του υποδικτύου [18].

5.8 Misuse of ICMPv6

IPv4 δίκτυα

Στα IPv4 δίκτυα, τα περισσότερα ICMP μηνύματα μπλοκάρονται, χωρίς να επηρεάζουν την λειτουργικότητα του δικτύου. Για αυτό το λόγο, το να μπλοκάρονται τα ICMP είναι μια κοινή πρακτική που βελτιώνει την ασφάλεια των IPv4 δικτύων.

IPv6 δίκτυα

Από την άλλη μεριά, στα IPv6 δίκτυα ορισμένοι σημαντικοί μηχανισμοί (όπως το neighbor discovery και path maximum transmission unit discovery mechanisms [PMTUD]) εξαρτώνται από την χρήση ICMPv6 μηνυμάτων [30]. Κατά συνέπεια, μερικά ICMPv6 μηνύματα πρέπει να επιτρέπονται λόγω την ανάγκης που υπάρχει για ορθή λειτουργία του δικτύου. Για παράδειγμα ένα "packet too big" μήνυμα απαιτείται για την διαδικασία Path MTU Discovery, ενώ ένα "parameter problem" μήνυμα είναι απαραίτητο όταν μία μη αναγνωρίσιμη option συνέβη στην κεφαλίδα του IPv6 πακέτου [4]. Τα ICMPv6 μηνύματα διακρίνονται στους παρακάτω τύπους:

- ICMPv6 Messages
    1. Informational Notification
    2. Error Notification
- ICMPv6 Sub Protocols
    1. Path MTU Discovery (PMTUD)
    2. ND and Address Resolution
    3. Router and Prefix Discovery
    4. Redirect

(Τα ICMPv6 μηνύματα που έχουν σχέση με ND/Address Resolution, Router and Prefix Discovery και Redirect έχουν περιγραφεί παραπάνω).

Informational Notification

Τα δύο ICMPv6 informational (πληροφοριακά) μηνύματα είναι τα "Echo Request" και "Echo Replay" messages. Αυτά τα μηνύματα χρησιμοποιούνται για διαγνωστικούς σκοπούς μέσα σε ένα δίκτυο και μπορούν να χρησιμοποιηθούν κακόβουλα από έναν επιτιθέμενο για εκτέλεση επιθέσεων (π.χ. ping attacks) [31].

Error Notification

Τα Error Notification μηνύματα παρέχουν μια μέθοδο για ανίχνευση και αντιμετώπιση των δυσλειτουργιών άλλων συστημάτων. Οι ακόλουθοι τύποι επιθέσεων εκμεταλλεύονται τα ICMPv6 error notification messages [31] :

- Πλαστογραφημένα ICMPv6 "Packet too big" μηνύματα μπορούν να προκαλέσουν την αποτυχία μιας λειτουργίας MTU discovery (Spoofing).
- Πλαστογραφημένα ICMPv6 "Destination Unreachable" μηνύματα που αποστέλλονται από έναν δρομολογητή μπορούν να πυροδοτήσουν routing storms (DoS attack).

- Πλαστογραφημένα ICMPv6 “Destination Unreachable” μηνύματα που αποστέλλονται από έναν υπολογιστή/σύστημα μπορούν να διακόψουν την κυκλοφορία (DoS).
- Πλαστογραφημένα ICMPv6 “Time Exceeded” μηνύματα μπορούν να διακόψουν την κυκλοφορία και να πυροδοτήσουν routing storms (DoS).
- Πλαστογραφημένα ICMPv6 “Parameter Problem” μηνύματα προκαλούν προβλήματα στην επεξεργασία πακέτων και έχουν ως αποτέλεσμα την επίτευξη DoS επιθέσεων σε δρομολογητές και υπολογιστές/συστήματα.

Path MTU Discovery

Χρησιμοποιείται με σκοπό να απαλλάξει τους IPv6 end systems από την διαδικασία κατακερματισμού (fragmentation) των πακέτων. Αν κάποιο από τα πακέτα είναι πολύ μεγάλο (too large) για να προωθηθεί από έναν κόμβο στο μονοπάτι, ο κόμβος το απορρίπτει και στέλνει ένα ICMPv6 “Packet too big” μήνυμα. Η PMTUD διαδικασία τελειώνει όταν η εκτίμηση ενός κόμβου για το PMTU είναι μικρότερη ή ίση από το πραγματικό PMTU. Οι επιθέσεις που μπορούν να επιτευχθούν κατά την διαδικασία PMTUD είναι όμοιες με τις επιθέσεις που προκύπτουν από τα ICMPv6 error notification μηνύματα [31].

Επιπλέον, το PMTUD υποστηρίζει multicast συνδέσεις, κατά τις οποίες κάθε μονοπάτι μπορεί να έχει διαφορετικό PMTU. Ένα ξεχωριστό multicast πακέτο μπορεί να έχει ως αποτέλεσμα την πολλαπλή απάντηση “Packet Too Big” μηνυμάτων από κάθε προορισμό [31]. Όπως έχει αναφερθεί το multicast είναι ευπαθές σε DoS επιθέσεις, κατά συνέπεια το PMTUD είναι και αυτό ευπαθές σε τέτοιου είδους επιθέσεις.Σε αυτό το σημείο θα γίνει μια συνοπτική αναφορά στις ICMPv6 επιθέσεις, όπου συμπεριλαμβάνονται και αυτές που προκύπτουν από ICMPv6 Neighbor Solicitation/Advertisement μηνύματα [30].

- Τα ICMPv6 μηνύματα μπορούν να χρησιμοποιηθούν με σκοπό να πείσουν τον παραλήπτη ότι το μήνυμα προέρχεται από μια άλλη πηγή, η οποία είναι διαφορετική από την πραγματική πηγή του μηνύματος. Η προστασία απέναντι σε αυτή την επίθεση μπορεί να επιτευχθεί εφαρμόζοντας τους μηχανισμούς αυθεντικοποίησης που παρέχει το IPv6.
- Τα ICMPv6 μπορούν να αποτελέσουν αντικείμενο ενεργειών που έχουν ως σκοπό το μήνυμα (ή η απάντηση σε αυτό) να σταλεί σε διαφορετική διεύθυνση από αυτή που επιθυμεί ο δημιουργός του. Ο υπολογισμός του ICMP checksum, αποτελεί σημαντικό μηχανισμό για προστασία απέναντι σε αλλαγές στις διευθύνσεις, όπως και η χρήση του IPsec για διασφάλιση ακεραιότητας μηνυμάτων μέσω του AH.
- Επίσης, μέσω των ICMPv6 μηνυμάτων, μπορούν να επιτευχθούν αλλαγές στα πεδία του μηνύματος καθώς και στο ωφέλιμο φορτίο αυτού. Πάλι, το AH και ESP αποτελούν σημαντικούς μηχανισμούς προστασίας.
- Επιπλέον, ICMPv6 μηνύματα μπορούν να χρησιμοποιηθούν ως απόπειρες εκτέλεσης denial of service επιθέσεων, στέλνοντας εσφαλμένα IP πακέτα.

5.9 Viruses and Worms

Οι ιοί και αναπαραγωγοί (virus/worms) παραμένουν ένα από τα πιο σημαντικά προβλήματα στο χώρο του διαδικτύου, καθώς πίσω από σχεδόν κάθε καταστροφική επίθεση υπάρχει ένας ιός ή αναπαραγωγός.

IPv4 δίκτυα

Στο IPv4, οι ιοί και αναπαραγωγοί δεν προκαλούν ζημιές μόνο στον υπολογιστή/σύστημα-στόχο, αλλά μπορούν να προκαλέσουν φθορά και στην κυκλοφορία του δικτύου μέσω του αυξανόμενου φόρτου που μεταφέρεται στους δρομολογητές, στους mail εξυπηρετητές και γενικότερα στον χώρο του διαδικτύου.Timely patching, host antivirus και ανίχνευση μέσω perimeter blocking είναι οι τρεις τεχνικές που χρησιμοποιούνται στο IPv4 για αντιμετώπιση ιών και αναπαραγωγών [18].

IPv6 δίκτυα

Ένας παραδοσιακός ιός δεν παρουσιάζει καμία αλλαγή μέσα σε ένα δίκτυο IPv6, έτσι η μορφή ενός email based ιού ή ενός ιού που μολύνει ένα αφαιρούμενο μέσο παραμένει ως έχει. Ωστόσο, σημαντική διαφορά παρατηρείται στους αναπαραγωγούς εκείνους που χρησιμοποιούν κάποιο είδος σάρωσης του διαδικτύου με σκοπό να βρουν ευάλωτους υπολογιστές/συστήματα. Οι συγκεκριμένοι αναπαραγωγοί αντιμετωπίζουν σημαντικά εμπόδια στην εξάπλωση – διάδοσή τους (propagation) σε ένα δίκτυο IPv6, λόγω του μεγάλου χώρου διευθύνσεων που έχουν να σαρώσουν [18]. Έτσι ο δημιουργός ενός αναπαραγωγού οφείλει να βρει νέες τεχνικές για να βελτιώσει την αποδοτικότητα του, σχετικά με την εξάπλωσή του [18].

Φαίνεται ότι ένας αναπαραγωγός τύπου SQL slammer[19] είναι αρκετά λιγότερο αποτελεσματικός σε ένα περιβάλλον IPv6 λόγω της ανικανότητάς του να ανακαλύψει ενεργούς κόμβους με σκοπό την μόλυνσή τους και κατά συνέπεια την ανικανότητά τους να προκαλέσουν flooding αποτελέσματα. Οι τρεις τεχνικές που χρησιμοποιούνται στο IPv4 για άμβλυνση των συμπτωμάτων από μόλυνση ιών/αναπαραγωγών είναι διαθέσιμες και στο IPv6. Ωστόσο, στο IPv6 δεν υπάρχει ακόμα ευρεία υποστήριξη από προϊόντα IDS [18].

5.10 Multiple Addresses

Το IPv6 επιτρέπει την ανάθεση πολλαπλών (multiple) διευθύνσεων σε μια διεπαφή. Ωστόσο, αυτό το χαρακτηριστικό περιπλέκει τους κανόνες φιλτραρίσματος σε κάποιο firewall ή access control list [1].

Σε αντίθεση με το IPv4, το φιλτράρισμα που βασίζεται σε μια διεύθυνση δεν είναι πλέον ιδιαίτερα επιτεύξιμο, επειδή όλες οι διευθύνσεις που ανατίθενται στις διεπαφές ενός κόμβου, θα πρέπει να περιληφθούν για να μπλοκάρουν τον κόμβο, πράγμα που δεν είναι εφικτό όταν αυτές οι διευθύνσεις είναι auto-configured ή για λόγους προστασίας της ιδιωτικής ζωής αλλάζουν με έναν επιθυμητό ρυθμό [1]. Σε αυτές τις περιπτώσεις ένα

[19] Αποτελεί ένα τύπο αναπαραγωγού που προκαλεί DoS επιθέσεις σε ορισμένους hosts του διαδικτύου και μειώνει δραματικά τον ρυθμό της διαδικτυακής κυκλοφορίας.

firewall θα πρέπει να μαθαίνει τις διευθύνσεις δυναμικά και οι κανόνες φιλτραρίσματος να δημιουργούνται αυτόματα κάνοντας χρήση πολύπλοκων πολιτικών. Τέτοιοι μηχανισμοί δεν είναι ακόμα διαθέσιμοι, για αυτό τον λόγο θα πρέπει να εφαρμόζονται πιο απλές τεχνικές, όπως η χρήση κάποιου είδους αναγνωριστικού συμβόλου (identification token) αντί για διευθύνσεις, με σκοπό τον προσδιορισμό ενός υπολογιστή/συστήματος ή μιας διεπαφής [1]. Λόγω της μη διάθεσης πολύπλοκων πολιτικών ασφάλειας, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί την δυνατότητα που προσφέρει το IPv6 μέσω των multiple διευθύνσεων και να περάσει τους ελέγχους ενός firewall ή access control list.

5.11 DNS Updates

Όταν μια διεύθυνση αποκτηθεί από έναν κόμβο, συμβαίνει μια αναβάθμιση στον DNS εξυπηρετητή και συγκεκριμένα στην αντίστοιχη καταχώριση (DNS entry) [1]. Η stateless address auto-configuration λειτουργία απαιτεί από έναν κόμβο να αναβαθμίσει την DNS καταχώρηση. Στην περίπτωση που γίνεται χρήση IPsec στην επικοινωνία του κόμβου με τον DNS εξυπηρετητή μπορεί να δημιουργηθεί σημαντικό πρόβλημα. Ο DNS server εξυπηρετεί έναν αριθμό από κόμβους με αποτέλεσμα να δημιουργούνται security associations (συσχετίσεις ασφάλειας) μεταξύ των κόμβων και του DNS . Το πλήθος των συσχετίσεων ασφάλειας ενδέχεται να είναι πολύ μεγάλο, με αποτέλεσμα ο DNS εξυπηρετητής να μην είναι σε θέση να τις διαχειριστεί και κατά συνέπεια να μην εξυπηρετεί κόμβους [1]. Έτσι, ένας επιτιθέμενος έχει την δυνατότητα να δημιουργήσει πολλές συσχετίσεις ασφάλειας, να προκαλέσει το παραπάνω πρόβλημα και να θέσει εκτός λειτουργίας έναν DNS εξυπηρετητή, ο οποίος δεν θα είναι σε θέση να εξυπηρετήσει νόμιμους χρήστες. Επιπλέον, το πρόβλημα μπορεί να γίνει χειρότερο, όταν οι κόμβοι χρησιμοποιούν διευθύνσεις ιδιωτικότητας, οι οποίες αλλάζουν περιοδικά απαιτώντας την συχνή αναβάθμιση των DNS καταχωρήσεων [1].

6

Επιθέσεις με ομοιότητες στα IPv4-IPv6

Στο συγκεκριμένο κεφάλαιο θα γίνει αναφορά στις απειλές και επιθέσεις που παρουσιάζουν ομοιότητες στα πρωτόκολλα IPv4 και IPv6. Υπάρχουν επιθέσεις που προκύπτουν από την εκμετάλλευση των ευπαθειών που παρουσιάζουν τα πρωτόκολλα και οι υπηρεσίες που παρέχει το IPv6 (μελετήθηκαν σε παραπάνω κεφάλαια), αλλά και είδη επιθέσεων που εμφανίζονται στο πρωτόκολλο IPv4 και συνεχίζουν να απειλούν το νέο πρωτόκολλο IPv6. Σε γενικές γραμμές οι τύποι επιθέσεων που είναι γνωστοί στο IPv4 και δεν έχουν αλλάξει στο IPv6 είναι οι παρακάτω [17,18]:

- **Sniffing attacks**
- **Application layer attacks**
- **Rogue devices**
- **Man-in-the-middle attacks**
- **Flooding attacks**
- **Brute force attacks**
- **Social Engineering attacks**

6.1 Sniffing Attacks

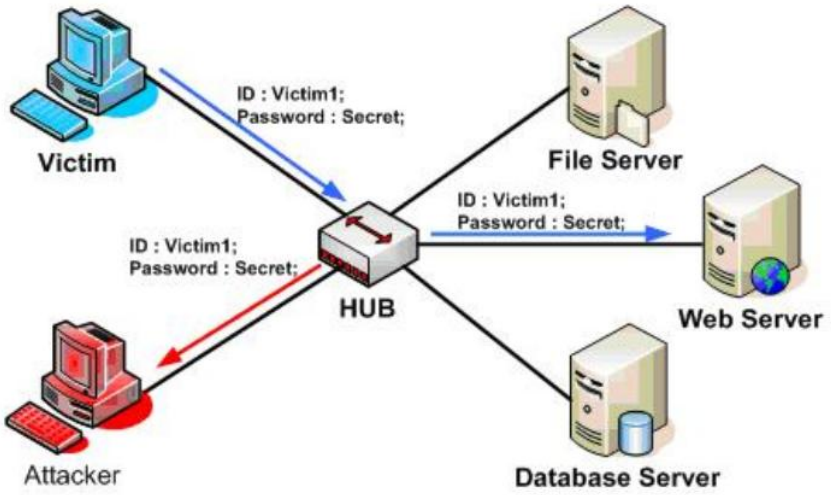
Ένα τυπικό παράδειγμα επίθεσης που επηρεάζει και τα δύο πρωτόκολλα επιπέδου δικτύου είναι η επίθεση υποκλοπής (sniffing attack). Μια sniffing επίθεση, η οποία καλείται και Eavesdropping επίθεση (Εικόνα 6.1) περιλαμβάνει την σύλληψη (υποκλοπή) των πακέτων που μεταδίδονται σε ένα δίκτυο μεταξύ κόμβων [18]. Η σύλληψη των πακέτων οδηγεί στην ανάγνωση ευαίσθητων δεδομένων, όπως συνθηματικών, session tokens[20] και κάθε είδους απόρρητης πληροφορίας [19].

Η επίθεση μπορεί να επιτευχθεί με χρήση ειδικών εργαλείων, που ονομάζονται network sniffers. Αυτά τα εργαλεία διαφέρουν ως προς την ποιότητα και αναλόγως μπορούν να υποκλέψουν πληροφορίες, όπως διευθύνσεις πηγής - προορισμού, θύρες που χρησιμοποιούνται, πληροφορίες ανώτερου επιπέδου (TCP/UDP), protocol decoders κτλ. [19].

Μια sniffing επίθεση μπορεί να αποφευχθεί με χρήση του πρωτοκόλλου IPsec [18], το οποίο μέσω του Encapsulating Security Payload (ESP) παρέχει κρυπτογράφηση των δεδομένων, γεγονός που διαφυλάσσει την εμπιστευτικότητα των μεταδιδόμενων

[20] Ένα session token αποτελεί έναν μοναδικό προσδιοριστή που δημιουργείται και αποστέλλεται από έναν server σε έναν client για να προσδιορίσει την τρέχουσα σύνοδο(session).

πληροφοριών από τους παθητικούς επιτιθέμενους. Ωστόσο, η κρυπτογράφηση δεδομένων, οδηγεί στην ανάγκη χρήσης κλειδιών από τις οντότητες που επικοινωνούν, άρα απαιτείται διαχείριση κλειδιών (key management).



Εικόνα 6.1: Sniffing Attack

6.2 Application Layer Attacks

Οι επιθέσεις επιπέδου εφαρμογών (application layers attacks) είναι οι πιο κοινές επιθέσεις στην σημερινή εποχή. Σε αυτή την κατηγορία επιθέσεων ανήκουν οι επιθέσεις buffer overflow, web application επιθέσεις (π.χ. sql injections, cross site scripting) [18]. Λόγω του γεγονότος ότι οι επιθέσεις αυτές εκτελούνται στο επίπεδο εφαρμογών (application layer), τα IPv4 και IPv6 δεν μπορούν να εμποδίσουν την δράση τους ή να απαλύνουν τις συνέπειές τους, καθώς αποτελούν πρωτόκολλα επιπέδου δικτύου. Έτσι η μετάβαση από το IPv4 στο IPv6, δεν οδηγεί σε καμία βελτίωση όσον αφορά στην αντιμετώπιση τέτοιων επιθέσεων.

Ακόμα και στην περίπτωση που μια σύνδεση είναι κρυπτογραφημένη με χρήση του IPsec, μια επίθεση επιπέδου εφαρμογής δεν εμποδίζεται από τίποτα να διασχίσει τον κρυπτογραφημένο σύνδεσμο και να προκαλέσει την ίδια ζημιά, όπως στην περίπτωση ενός μη κρυπτογραφημένου συνδέσμου [18]. Η μόνη διαφορά (ιδιαίτερα σημαντική) στην περίπτωση του κρυπτογραφημένου συνδέσμου είναι η δυνατότητα ανίχνευσης της πραγματικής διεύθυνσης του αποστολέα, η οποία θα ήταν πιο εύκολο να βρεθεί λόγω χρήσης μεθόδων αυθεντικοποίησης.

6.3 Rogue Devices

Οι rogue devices είναι συσκευές που εμφανίζονται σε ένα δίκτυο χωρίς να είναι εξουσιοδοτημένες, έχοντας κακόβουλο σκοπό. Μια τέτοια συσκευή μπορεί να είναι ένα απλό laptop, ένα rogue wireless access point, ένας δρομολογητής ή ένας DHCP / DNS

εξυπηρετητής [18]. Τέτοιου είδους επιθέσεις στο IPv6 είναι σχεδόν όμοιες με αυτές των IPv4 δικτύων.

Η χρήση πιστοποίησης / αυθεντικοποίησης μέσω του IPsec μπορεί να μετριάσει το πρόβλημα εμφάνισης μη εξουσιοδοτημένων συσκευών. Επιπλέον, το 802.1x πρωτόκολλο που επιτρέπει την αυθεντικοποίηση των συσκευών σε ένα δίκτυο, φαίνεται να αποτελεί καλή λύση για την αντιμετώπιση rogue συσκευών. Η αυθεντικοποίηση στο 802.1x γίνεται συνήθως με πιστοποιητικά (certificates). Κατά συνέπεια, εάν ένας υπολογιστής (στην συγκεκριμένη περίπτωση μια rogue συσκευή) δεν διαθέτει το κατάλληλο πιστοποιητικό δεν μπορεί να συνδεθεί στο δίκτυο [18].

6.4 Man-in-the-Middle Attacks

Οι κεφαλίδες των IPv4 και IPv6 δεν διαθέτουν από μόνες τους κανέναν μηχανισμό ασφάλειας, έτσι κάθε πρωτόκολλο βασίζεται στο IPsec για παροχή ασφάλειας. Για αυτό το λόγο το Internet Key Exchange (IKE) αποτελεί στόχο για τους επιτιθέμενους. Ήδη, υπάρχουν καταγεγραμμένα εργαλεία για επίθεση στο IKE, με σκοπό την απόκτηση του διαμοιρασμένου κλειδιού. Ωστόσο, το IKEv2[21] λύνει αρκετά προβλήματα που παρουσιάζει το IKE.

6.5 Flooding Attacks

Μία από τις πιο συχνές επιθέσεις στα IPv4 δίκτυα είναι η flooding επίθεση. Το όνομά της υποδηλώνει τον κατακλυσμό (πλημμύρα) μιας δικτυακής συσκευής (π.χ. δρομολογητής) ή ενός υπολογιστή με τεράστια ποσά δικτυακής κίνησης. Μια τέτοια συσκευή, η οποία αποτελεί τον στόχο της επίθεσης είναι αδύνατον να υποβάλλει σε επεξεργασία το τεράστιο ποσό δικτυακής κίνησης (μεγάλος αριθμός πακέτων) που της ανατίθεται, με αποτέλεσμα την "κατάρρευσή" της και κατά συνέπεια την μη διαθεσιμότητά της και την μη παροχή υπηρεσιών [4].

Μια επίθεση τύπου flooding μπορεί να είναι μία τοπική επίθεση, δηλαδή μέσα σε ένα local link, αλλά και μία distributed denial of service attack (DDoS) [20], όταν η δικτυακή συσκευή - στόχος πλημμυρίζεται με δικτυακή κίνηση από πολλούς υπολογιστές/συστήματα ταυτόχρονα. Αυτός ο τύπος επίθεσης, μπορεί επίσης να επηρεάσει τα IPv6 δίκτυα, ίσως με διαφορετικής μορφής πλημμύρα, ωστόσο οι βασικές αρχές μιας flooding επίθεσης παραμένουν ίδιες με αυτές που ισχύουν στο IPv4 [4]. Για παράδειγμα, μια συσκευή σε ένα IPv6 δίκτυο μπορεί να κατακλυστεί από ICMPv6 μηνύματα, γεγονός που δεν μπορεί να συμβεί στο IPv4, διότι συνήθως τα ICMP μηνύματα φιλτράρονται. Ωστόσο, έχει ακολουθηθεί μια πολιτική flooding επίθεσης, όπως θα συνέβαινε αν είχαμε ένα IPv4 δίκτυο.

[21] Περιγράφεται στο κεφάλαιο 8

6.6 Brute-Force Attacks

Μια brute-force επίθεση είναι μια αυτοματοποιημένη διαδικασία δοκιμών με σκοπό τον εντοπισμό προσωπικών στοιχείων, όπως όνομα χρήστη, συνθηματικό, αριθμός πιστωτικής κάρτας και κρυπτογραφικών κλειδιών [22].

Πολλά συστήματα επιτρέπουν την χρήση αδύναμων κωδικών και κρυπτογραφικών κλειδιών, ενώ οι χρήστες συχνά επιλέγουν εύκολους ως προς τον εντοπισμό κωδικούς, τους οποίους μπορεί να βρει κάποιος μέσα σε ένα λεξικό. Ένας επιτιθέμενος μπορεί να δοκιμάσει σε ένα σύστημα όλες τις λέξεις-φράσεις του λεξικού μία προς μία έως ότου βρει το έγκυρο συνθηματικό. Όταν ένα από τα δοκιμαστικά συνθηματικά επιτρέψει την πρόσβαση στο σύστημα, μια brute-force επίθεση ολοκληρώνεται με επιτυχία και δίνεται στον επιτιθέμενο η δυνατότητα πρόσβασης στον λογαριασμό του θύματος [22].

Η ίδια trial-and-error (δοκιμή και σφάλμα) τεχνική είναι επίσης εφαρμόσιμη στον εντοπισμό κρυπτογραφικών κλειδιών. Όταν μια ιστοσελίδα χρησιμοποιεί ένα αδύναμο ή ένα μικρό σε μέγεθος κλειδί, δίνεται η δυνατότητα σε έναν επιτιθέμενο να βρει το σωστό κλειδί, ελέγχοντας όλα τα δυνατά κλειδιά [22].

Κατά κύριο λόγο, υπάρχουν δύο τύποι Brute force επιθέσεων: η normal Brute Force και η reverse Brute Force. Μία normal Brute Force επίθεση χρησιμοποιεί μόνο ένα όνομα χρήστη και πολλά συνθηματικά (δοκιμές πολλών passwords σε ένα μόνο username). Ενώ η Reverse Brute Force επίθεση κάνει χρήση πολλών usernames δοκιμάζοντας μόνο ένα password [22]. Μια Brute Force τεχνική είναι μια δημοφιλής και συχνά επιτυχημένη επίθεση που μπορεί να εφαρμοστεί με τον ίδιο τρόπο σε δίκτυα IPv4 και IPv6, η οποία μπορεί να διαρκέσει ώρες , εβδομάδες ή και χρόνια (θεωρητικά - μη πρακτικό) για να ολοκληρωθεί.

6.7 Social Engineering Attack

Ένα άλλο είδος επίθεσης που είναι παρόμοιο στα πρωτόκολλα IPv4 και IPv6 είναι οι επιθέσεις social engineering [17]. Μια social engineering,αποτελεί την επίθεση κατά την οποία το επιδιωκόμενο θύμα πείθεται να εκτελέσει τις εντολές ενός επιτιθέμενου [21].

Ένα παράδειγμα αποτελεί η αποστολή ενός phishing email και η ανταπόκριση του θύματος σε αυτό, ακολουθώντας τον σύνδεσμο που του δίνεται. Το θύμα μεταφέρεται σε έναν δόλιο δικτυακό χώρο, όπου του ζητείται η επιβεβαίωση στοιχείων πρόσβασης για να αποκτήσει πρόσβαση στις υπηρεσίες του site. Συνήθως, αυτή η δικτυακή σελίδα έχει ακριβώς την ίδια μορφή με την ιστοσελίδα κάποιας τράπεζας (ή άλλης υπηρεσίας) που χρησιμοποιεί το θύμα, με αποτέλεσμα να πείθεται να δώσει τα στοιχεία του. Έτσι ο επιτιθέμενος αποκτά τα στοιχεία πρόσβασης (credentials) του χρήστη ή άλλες απόρρητες πληροφορίες, τις οποίες χρησιμοποιεί για κακόβουλο σκοπό.

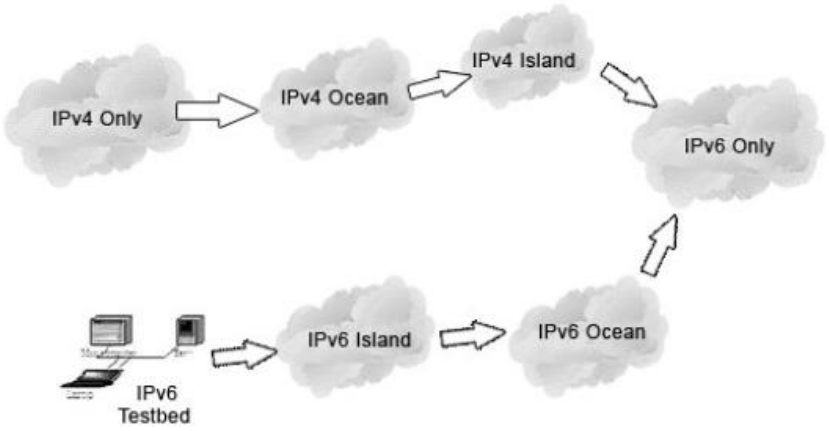
Επίσης, μια social engineering επίθεση μπορεί να χρησιμοποιηθεί για να πειστεί ένας χρήστης να εκτελέσει μια διαδικασία με σκοπό την μόλυνση του συστήματός του [21]. Ένα παράδειγμα αποτελεί η αποστολή ενός email που περιέχει έναν σύνδεσμο, ο οποίος οδηγεί σε μια σελίδα για το “κατέβασμα” κάποιου υποτιθέμενου video codec, το οποίο όμως περιέχει ιομορφικό λογισμικό. Το θύμα ανακατευθύνεται στην συγκεκριμένη

ιστοσελίδα, “κατεβάζει” και εγκαθιστά το ιομορφικό video codec και χωρίς να το αντιληφθεί μολύνει το σύστημά του με κάποιο Trojan ή Keystroke logger [21].

7

IPv4/IPv6 Μηχανισμοί Μετάβασης

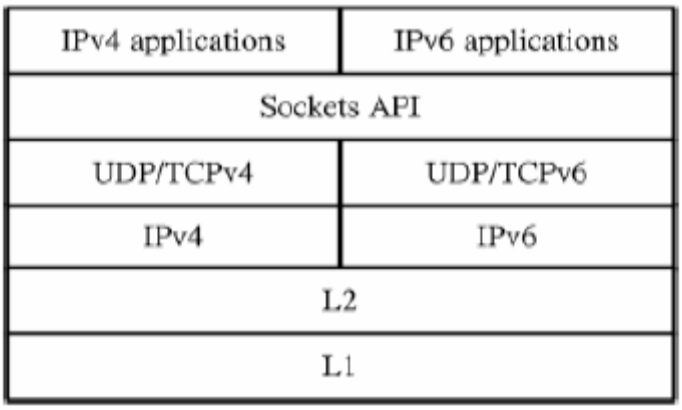
Από την στιγμή που η μετάβαση από το IPv4 στο IPv6 πρωτόκολλο δεν γίνεται απότομα (λόγω του τεράστιου μεγέθους των παγκόσμιων IPv4 δικτύων), για μια χρονική περίοδο τα δύο πρωτόκολλα θα πρέπει να συνυπάρξουν και η μετάβαση να γίνεται σταδιακά [4]. Η Εικόνα 7.1 δείχνει τις φάσεις μετάβασης. Για την ομαλή και σταδιακή μετάβαση από το ένα πρωτόκολλο στο άλλο, απαιτείται η ύπαρξη ενός μηχανισμού που θα παρέχει την απαραίτητη υποστήριξη στην προσωρινή συνύπαρξη των δύο πρωτοκόλλων. Οι ποικίλες μεταβατικές στρατηγικές μπορούν να διαιρεθούν σε τρεις γενικές κατηγορίες: dual stack, tunneling και translation μηχανισμοί [39].



Εικόνα 7.1: IPv4/IPv6 φάσεις μετάβασης

7.1 IPv4/IPv6 Dual-Stack Mechanisms

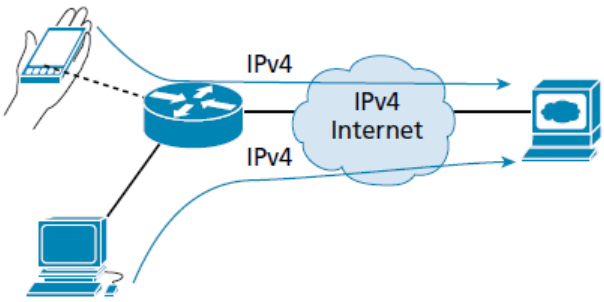
Οι dual-stack μηχανισμοί περιλαμβάνουν δύο στοίβες πρωτοκόλλου, οι οποίες λειτουργούν παράλληλα και επιτρέπουν στους δικτυακούς κόμβους να επικοινωνούν είτε μέσω IPv4 είτε μέσω IPv6 [40]. Οι μηχανισμοί αυτοί μπορούν να υλοποιηθούν τόσο σε τερματικά συστήματα (end systems) όσο και σε ενδιάμεσους κόμβους. Στα τερματικά συστήματα επιτρέπουν στις IPv4 και IPv6 εφαρμογές να λειτουργούν ταυτόχρονα. Επιπλέον, οι δυνατότητες των dual-stack μηχανισμών υποστηρίζουν την μεταφορά όχι μόνο IPv4 αλλά και IPv6 πακέτων [38]. Η Εικόνα 7.2 δείχνει την διατήρηση μιας IPv4 και IPv6 στοίβας ταυτόχρονα από έναν κόμβο. Οι IPv4 εφαρμογές χρησιμοποιούν την IPv4 στοίβα, ενώ οι IPv6 εφαρμογές κάνουν χρήση της IPv6 στοίβας.



Εικόνα 7.2: Dual Stack Μηχανισμός Μετάβασης

Μόνο IPv4

Σε ένα δικτυακό περιβάλλον, το οποίο αποτελείται μόνο από IPv4 υποδομή η επικοινωνία γίνεται με χρήση μόνο του πρωτοκόλλου IPv4 (Εικόνα 7.3).

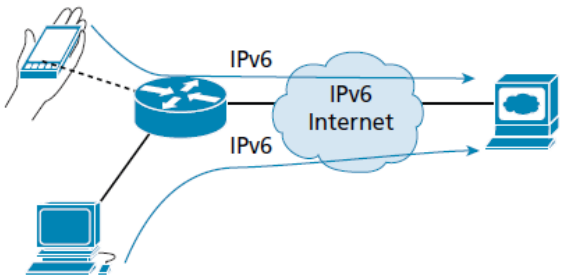


Εικόνα 7.3: Χρήση μόνο του πρωτοκόλλου IPv4

Όταν ένας πελάτης επιχειρεί να συνδεθεί σε έναν απομακρυσμένο εξυπηρετητή, για παράδειγμα στο www.example.com, πρώτα κάνει μια DNS αίτηση, ώστε να αντιστοιχήσει το όνομα του προορισμού σε μια IPv4 διεύθυνση. Όταν ο πελάτης αποκτήσει αυτή την IP διεύθυνση μπορεί να ξεκινήσει την http (ή οποιαδήποτε άλλη) σύνδεση. Σε ένα περιβάλλον που χρησιμοποιείται μόνο IPv4 υποδομή, η σύνδεση και επικοινωνία θα γίνει βάση του IPv4 πρωτοκόλλου [53].

Μόνο IPv6

Σε ένα δικτυακό περιβάλλον, το οποίο αποτελείται μόνο από IPv6 υποδομή η επικοινωνία γίνεται με χρήση του πρωτοκόλλου IPv6. Η διαδικασία σύνδεσης και επικοινωνίας μεταξύ ενός πελάτη και ενός εξυπηρετητή είναι ίδια με το IPv4 (Εικόνα 7.4).



Εικόνα 7.4: Χρήση μόνο του πρωτοκόλλου IPv6

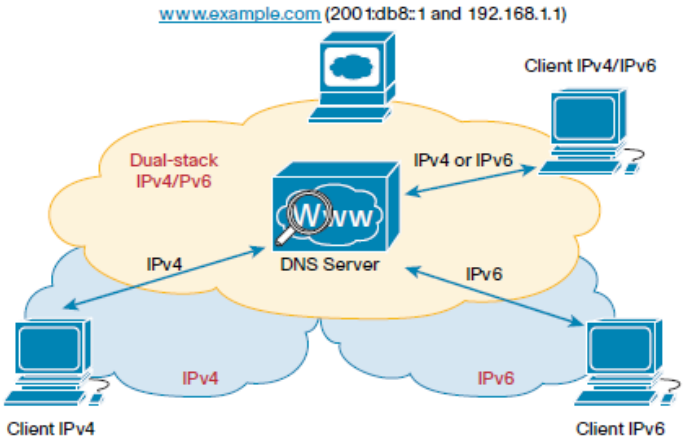
Dual Stack IPv4/IPv6

Όταν μια συσκευή έχει dual stack (διπλής στοίβας) δυνατότητες, τότε έχει πρόσβαση τόσο σε IPv4 όσο και σε IPv6 δικτυακό περιβάλλον και μπορεί να χρησιμοποιήσει παράλληλα και τις δύο τεχνολογίες για σύνδεση σε έναν απομακρυσμένο εξυπηρετητή [53].

Όταν ένας πελάτης θέλει να συνδεθεί σε έναν εξυπηρετητή (π.χ. www.example.com), τότε κάνει δύο DNS αιτήσεις ταυτόχρονα: μια αίτηση για IPv4 διεύθυνση και μια για IPv6 διεύθυνση. Όταν λάβει τις απαντήσεις, ο πελάτης ακολουθεί την διαδικασία που περιγράφεται στο RFC 3484 “Default Address Selection for IPv6”, επιλέγοντας την IPv6 διεύθυνση. Εάν για κάποιο λόγο η χρήση της συγκεκριμένης διεύθυνσης γίνει χωρίς επιτυχία, τότε ο πελάτης χρησιμοποιεί την IPv4 διεύθυνση που έλαβε για να συνδεθεί με τον εξυπηρετητή [53].

Στην παραπάνω περίπτωση έχουμε μια επικοινωνία πελάτη – εξυπηρετητή, όπου και οι δύο υποστηρίζουν dual-stack μηχανισμό. Επιπλέον, είναι δυνατή η σύνδεση μιας dual-stack συσκευής (πελάτης) με μια IPv4-only ή IPv6-only συσκευής (εξυπηρετητής). Ο πελάτης επιλέγει IP πρωτόκολλο βάση του είδους της IP διεύθυνσης που θα επιστρέψει ο DNS. Ένα ο DNS εξυπηρετητής επιστρέψει μόνο IPv4 διεύθυνση τότε ο πελάτης επιλέγει την IPv4 στοίβα, ενώ εάν επιστραφεί IPv6 διεύθυνση ο πελάτης επιλέγει την IPv6 στοίβα. Η συγκεκριμένη διαδικασία φαίνεται στην Εικόνα 7.5.

Όσον αφορά την επικοινωνία πελάτη – DNS εξυπηρετητή αυτή μπορεί να γίνει συνήθως με την χρήση και των δύο πρωτοκόλλων, καθώς οι περισσότεροι DNS εξυπηρετητές, υποστηρίζουν τόσο IPv4 όσο και IPv6 αιτήσεις.



Εικόνα 7.5: Ταυτόχρονη χρήση IPv4 - IPv6

Πολλά από τα λειτουργικά συστήματα του εμπορίου χρησιμοποιούν ήδη dual-stacks. Ο dual-stack μηχανισμός είναι η πιο συχνά χρησιμοποιούμενη μεταβατική λύση, ωστόσο ένα βασικό μειονέκτημα που εντοπίζεται είναι η χαμηλή απόδοση των κόμβων που χρησιμοποιούν και τα δύο πρωτόκολλα, καθώς απαιτείται υψηλή υπολογιστική ισχύς σε σύγκριση με ένα κόμβο που χρησιμοποιεί μόνο ένα από τα δύο πρωτόκολλα.

Μία συσκευή που υποστηρίζει έναν dual-stack μηχανισμό οφείλει να παρέχει προστασία απέναντι σε επιθέσεις που μπορούν να επιτευχθούν και στα δύο πρωτόκολλα (IPv4, IPv6) [41]. Κατά συνέπεια, μηχανισμοί ελέγχου που υλοποιούνται σε έναν υπολογιστή/σύστημα, όπως firewalls και IDSs θα πρέπει να επιθεωρούν την κυκλοφορία που προέρχεται και από τα δύο πρωτόκολλα και να μπλοκάρουν συγκεκριμένη κυκλοφορία όποτε είναι απαραίτητο. Αυτό που οφείλει να κάνει ένας διαχειριστής δικτύου είναι να επεκτείνει το ήδη υπάρχον firewall με ένα σύνολο κανόνων που θα εφαρμόζονται στο IPv6 ή να υλοποιήσει ένα ξεχωριστό IPv6-firewall, το οποίο θα παρέχει προστασία στους υπολογιστές/συστήματα όπως το αντίστοιχο IPv4-firewall [41]. Επιπροσθέτως, κατάλληλες IPv6 λίστες ελέγχου πρόσβασης (access control lists [ACLs]) είναι δυνατόν να κατασκευασθούν ώστε να υλοποιούν ίδιους περιορισμούς με αυτούς των IPv4 ACLs [41].

7.2 IPv4/IPv6 Translation Mechanisms

Οι translation μηχανισμοί (μηχανισμοί μετάφρασης) χρησιμοποιούνται στην περίπτωση που ένας IPv6-only host θέλει να επικοινωνήσει με έναν IPv4-only host. Οι συγκεκριμένοι μηχανισμοί δρουν μεταξύ των IPv6-only και IPv4-only hosts, χωρίς να χρειάζεται κάποια αλλαγή σε αυτούς. Βασίζονται σε δύο τύπους μετάφρασης πρωτοκόλλου (protocol translation), το IP protocol translation και το IP-related translation. Το πρώτο αναφέρεται στην αντικατάσταση της IP κεφαλίδας (από IPv4 σε IPv6 και αντίστροφα) και το δεύτερο αναφέρεται στο ICMP και στην ανταλλαγή IP πληροφορίας (π.χ. FTP) [Enterprise IPv6].

Υπάρχουν αρκετοί μηχανισμοί μετάφρασης, όπως NAT-Protocol Translation (NAT-PT), TCP-UDP relay, Bump-In-the-Stack (BIS) κτλ. Ο NAT-PT μηχανισμός δεν χρησιμοποιείται πλέον λόγω των πολλών προβλημάτων που παρουσιάζει [43]. Ο πιο σημαντικός περιορισμός του NAT-PT είναι η αδυναμία για ασφάλεια στο επίπεδο δικτύου σε end-to-end περιπτώσεις. Επίσης, όταν γίνεται χρήση του NAT-PT στα επίπεδα μεταφοράς και εφαρμογών δεν μπορεί να υπάρξει ασφάλεια στις εφαρμογές που μεταφέρουν τις IP διευθύνσεις στο επίπεδο εφαρμογών. Αυτός είναι ένας έμφυτος περιορισμός της Network Address Translation (NAT) λειτουργίας [44].

Γενικότερα, οι translation τεχνικές δεν χρησιμοποιούνται ευρέως, επειδή μειώνουν σημαντικά την ροή των πακέτων. Επιπλέον, δεν επιτρέπουν στο δίκτυο να εκμεταλλευτεί συγκεκριμένες δυνατότητες που προσφέρουν τα πρωτόκολλα IPv4 και IPv6 [2].

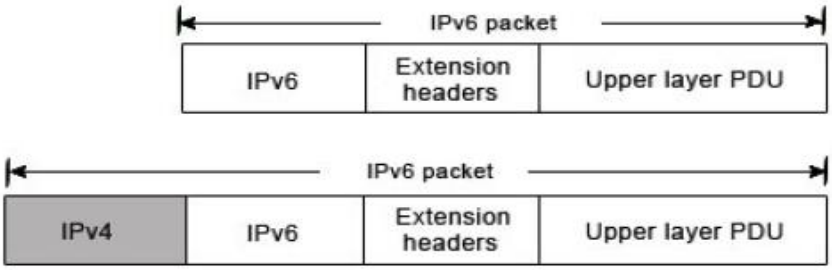
7.3 IPv4/IPv6 Tunneling Mechanisms

Το Tunneling από την προοπτική του transitioning (μετάβασης), καθιστά ικανή την γεφύρωση ασύμβατων δικτύων και συνήθως εφαρμόζεται με έναν point-to-point τρόπο. Επιτρέπει IPv6 δικτυακή κυκλοφορία να μεταφερθεί πάνω από μια IPv4 δικτυακή υποδομή

μεταξύ δύο τελικών κόμβων. Μια εικονική από άκρη σε άκρη σύνδεση (ή tunnel) εγκαθιδρύεται μεταξύ δύο dual-stack κόμβων. Συνήθως όλοι οι κόμβοι μεταξύ των τελικών κόμβων είναι IPv4-only. Αυτό που συμβαίνει με τους tunneling μηχανισμούς είναι η ενθυλάκωση IPv6 πακέτων εντός IPv4 πακέτων, ώστε να μπορούν να δρομολογηθούν εντός ενός IPv4 δικτυακού περιβάλλοντος. Οι τρεις μηχανισμοί που θα παρουσιαστούν είναι: IP v6 over IPv4, IPv6 to IPv4 automatic tunneling και Tunnel Broker [38].

7.3.1 IPv4 over IPv6 Mechanism

Ο IPv6 over IPv4 μηχανισμός "εμφυτεύει" μια IPv4 διεύθυνση στο identifier τμήμα μιας IPv6 link layer διεύθυνσης (Εικόνα 7.6) και καθορίζει το Neighbor Discovery πάνω από το IPv4 χρησιμοποιώντας μια local multicast [45].



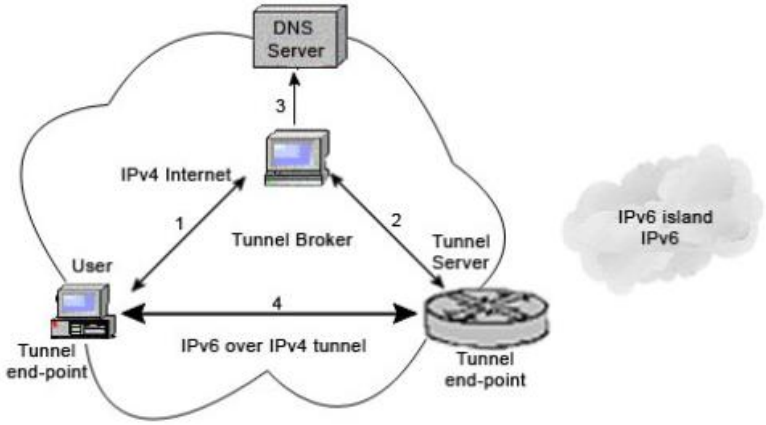
Εικόνα 7.6: 6over4 Address Link Layer Identifier

Ένα IPv4 domain είναι ένα σύνολο από IPv4 υποδίκτυα που συνδέονται μεταξύ τους στο πεδίο μιας μοναδικής local multicast διεύθυνσης, μέσα στο οποίο υπάρχουν τουλάχιστον δύο IPv6 κόμβοι. Ο IPv6 over IPv6 tunneling μηχανισμός παρέχει μια λύση σε αυτούς τους IPv6 "σκορπισμένους" κόμβους που βρίσκονται μέσα σε ένα IPv4 domain και δεν έχουν IPv6 συνδεσιμότητα [38]. Ο μηχανισμός επιτρέπει σε κόμβους, οι οποίοι συνδέονται απευθείας με IPv6 δρομολογητές να γίνονται πλήρως λειτουργικοί IPv6 κόμβοι.

7.3.2 IPv6 Tunnel Broker

Το IPv6 Tunnel Broker παρέχει μια αυτόματη υπηρεσία διαμόρφωσης για IPv6 over IPv4 tunnels σε χρήστες που συνδέονται στο IPv4 διαδίκτυο [46]. Απαιτείται μια IPv4 συνδεσιμότητα μεταξύ του χρήστη και του παρόχου υπηρεσίας. Η υπηρεσία λειτουργεί ως εξής (Εικόνα 7.7) [38]:

1. Ο χρήστης επικοινωνεί με τον Tunnel Broker και εκτελεί την διαδικασία εγγραφής.
2. Ο χρήστης έρχεται ξανά σε επαφή με τον Tunnel Broker για αυθεντικοποίηση και παροχή πληροφοριών ρύθμισης (IP διεύθυνση, λειτουργικό σύστημα κτλ.)
3. Ο Tunnel Broker ρυθμίζει το end-point του δικτύου, τον DNS εξυπηρετητή και το τερματικό του χρήστη.
4. Το tunnel είναι ενεργό και ο χρήστης είναι συνδεδεμένος σε IPv6 δίκτυα.



Εικόνα 7.7: IPv6 Tunnel Broker

Παρόλο που το Tunnel Broker είναι γενικά εύκολο στην χρήση, υπάρχει σημαντικό ζήτημα για τους διαχειριστές, σχετικά με το αν είναι πληροφορημένοι για τους χρήστες που χρησιμοποιούν tunnel brokers. Η έλλειψη πληροφόρησης από τους διαχειριστές για χρήση tunnel brokers μπορεί να επιφέρει την ύπαρξη security holes (τρύπες ασφάλειας), για τις οποίες ο διαχειριστής δεν γνωρίζει [41].

7.3.3 IPv6 to IPv4 Automatic Tunneling Mechanisms

Το αυτόματο tunneling αναφέρεται σε μία τεχνική κατά την οποία η διαδικασία δρομολόγησης αποφασίζει αυτόματα τα tunnel endpoints .Οι δύο μέθοδοι αυτόματου tunneling που θα μελετήσουμε είναι το 6to4 και το Teredo. Ο 6to4 tunneling μηχανισμός υποδηλώνει την ενθυλάκωση ενός IPv6 πακέτου μέσα σε ένα IPv4 πακέτο. Ο Teredo tunneling μηχανισμός αναφέρεται στην ενθυλάκωση ενός IPv6 πακέτου μέσα σε ένα IPv4 UDP πακέτο [4].

7.3.3.1 6to4 Tunneling Mechanism

Ο 6to4 tunneling μηχανισμός χρησιμοποιείται για μετάδοση IPv6 πακέτων μέσα σε ένα IPv4 δίκτυο. Ειδικοί relay εξυπηρετητές τοποθετούνται σε κατάλληλα σημεία για να επιτρέπουν στα 6to4 δίκτυα να επικοινωνούν με native IPv6 δίκτυα. Ο 6to4 μηχανισμός μπορεί να χρησιμοποιηθεί από έναν υπολογιστή/σύστημα ή από ένα τοπικό IPv6 δίκτυο. Όταν χρησιμοποιείται από έναν υπολογιστή/σύστημα, πρέπει να έχει μια παγκόσμια IPv4 διεύθυνση και ο υπολογιστής είναι υπεύθυνος για ενθυλάκωση (encapsulation) των εξερχόμενων IPv6 πακέτων και decapsulation των εισερχόμενων 6to4 πακέτων. Εάν ο υπολογιστής/σύστημα είναι διαμορφωμένος να προωθεί πακέτα σε άλλους υπολογιστές/συστήματα, τότε αποτελεί έναν δρομολογητή [47].

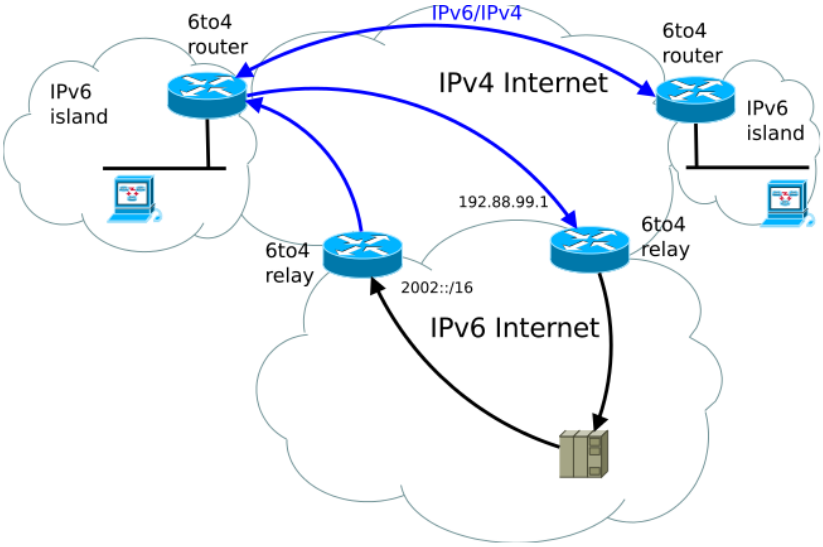
Τα περισσότερα IPv6 δίκτυα χρησιμοποιούν την auto-configuration λειτουργία, η οποία απαιτεί τα τελευταία 64 bits για τον υπολογιστή/σύστημα. Τα πρώτα 64 bits είναι το IPv6 prefix. Τα πρώτα 16 bits του prefix είναι πάντοτε 2002:, τα επόμενα 32 bits είναι η IPv4

διεύθυνση και τα τελευταία 16 bits του prefix είναι αυθαίρετα επιλεγμένα από τον δρομολογητή. Από την στιγμή που οι IPv6 υπολογιστές/συστήματα χρησιμοποιήσουν την λειτουργία auto-configuration προσδιορίζουν με μοναδικό τρόπο το 64 bit τμήμα της διεύθυνσης του υπολογιστή, και απλά αναμένουν για το Router Advertisement που θα τους υποδείξει τα πρώτα 64 bits του prefix για να αποκτήσουν μια ολοκληρωμένη IPv6 διεύθυνση [47]. Ένας 6to4 δρομολογητής θα γνωρίζει ότι πρέπει να στείλει ένα ενθυλακωμένο πακέτο απευθείας πάνω από ένα IPv4 δίκτυο, εάν τα πρώτα 16 bits είναι 2002, χρησιμοποιώντας τα επόμενα 32 bits ως τον προορισμό, διαφορετικά θα αποστείλει το πακέτο σε έναν γνωστό relay εξυπηρετητή, ο οποίος θα έχει πρόσβαση σε ένα native IPv6 δίκτυο.

Λειτουργία 6to4

Ο μηχανισμός 6to4 εκτελεί τρεις λειτουργίες [47] (Εικόνα 7.8):

- Εκχωρεί ένα μπλοκ του IPv6 χώρου διευθύνσεων σε έναν υπολογιστή/σύστημα ή δίκτυο, το οποίο έχει μια παγκόσμια IPv4 διεύθυνση.
- Ενθυλακώνει IPv6 πακέτα στο εσωτερικό των IPv4 πακέτων για μετάδοση πάνω από ένα IPv4 δίκτυο.
- Δρομολογεί την κυκλοφορία μεταξύ 6to4 και native IPv6 δικτύων.



Εικόνα 7.8: Μηχανισμός 6to4

Address block allocation

Για κάθε 32 bit παγκόσμια IPv4 διεύθυνση που ανατίθεται σε έναν υπολογιστή/σύστημα, υπάρχει δυνατότητα κατασκευής ενός 48 bit 6to4 IPv6 prefix επισυνάπτοντας την IPv4 διεύθυνση στο 2002::/16. Οποιαδήποτε IPv6 διεύθυνση που ξεκινάει με το 2002:: /16 prefix είναι γνωστή ως 6to4 διεύθυνση, σε αντίθεση με μια native IPv6 διεύθυνση, η οποία δεν κάνει χρήση τεχνολογιών μετάβασης [47].

Ενθυλάκωση και μετάδοση

Ο 6to4 μηχανισμός ενσωματώνει ένα IPv6 πακέτο μέσα σε ένα IPv4 πακέτο, έτσι ώστε το IPv6 πακέτο να αποτελεί ωφέλιμο φορτίο του IPv4 πακέτου. Για να σταλεί ένα IPv6 πακέτο σε έναν 6to4 προορισμό πάνω από ένα IPv4 δίκτυο, απαιτείται μια προθεματική IPv4 κεφαλίδα, η οποία θα προηγείται του IPv6 πακέτου. Η IPv4 διεύθυνση προορισμού της προθεματικής κεφαλίδας προέρχεται από την IPv6 διεύθυνση προορισμού του εσωτερικού πακέτου (η οποία είναι σε μορφή 6to4 διεύθυνσης), εξάγοντας τα 32 bits που ακολουθούν το 2002:: /16 prefix της IPv6 διεύθυνσης προορισμού. Η IPv4 διεύθυνση πηγής στην προθεματική κεφαλίδα είναι η IPv4 διεύθυνση του υπολογιστή/συστήματος ή δρομολογητή στον οποίο πρόκειται να σταλεί το πακέτο πάνω από το IPv4 δίκτυο [47].

Δρομολόγηση μεταξύ 6to4 και native IPv6 δικτύου

Για να επιτραπεί στους υπολογιστές/συστήματα και στα δίκτυα που χρησιμοποιούν 6to4 διευθύνσεις να ανταλλάξουν δικτυακή κυκλοφορία με υπολογιστές/συστήματα που κάνουν χρήση native IPv6 διευθύνσεων, απαιτείται η εγκατάσταση relay routers [47]. Ένας relay router συνδέεται σε ένα IPv4 και ένα IPv6 δίκτυο. Τα 6to4 πακέτα που φτάνουν σε μια IPv4 διεπαφή θα έχουν τα IPv6 ωφέλιμα φορτία τους έτοιμα για δρομολόγηση στο IPv6 δίκτυο, ενώ τα πακέτα που φτάνουν σε μια IPv6 διεπαφή με prefix διεύθυνσης προορισμού το 2002::/16 θα ενθυλακώνονται και θα προωθούνται πάνω από ένα IPv4 δίκτυο. Στην ουσία ένας relay router είναι ένας 6to4 δρομολογητής που υποστηρίζει δρομολόγηση πακέτων μεταξύ 6to4 διευθύνσεων και native IPv6 διευθύνσεων [47].

Υπάρχει μια διαφορά ανάμεσα σε έναν relay δρομολογητή και σε έναν border δρομολογητή (γνωστός και ως 6to4 border router). Ένας 6to4 border δρομολογητής είναι ένας IPv6 δρομολογητής που υποστηρίζει μια 6to4 pseudo-interface. Κατά κανόνα είναι ο border δρομολογητής ανάμεσα σε μια IPv6 τοποθεσία και ένα IPv4 δίκτυο, όπου η IPv6 τοποθεσία κάνει χρήση του 2002::/16. Από την άλλη μεριά, ένας relay router είναι ένας 6to4 δρομολογητής ρυθμισμένος με τέτοιο τρόπο ώστε να υποστηρίζει δρομολόγηση μεταξύ 6to4 διευθύνσεων και native IPv6 διευθύνσεων.

Επιθέσεις σε 6to4 δίκτυα

Σε αυτό το σημείο θα γίνει περιγραφή των επιθέσεων που μπορούν να επιτευχθούν εναντίον 6to4 δικτύων. Οι επιθέσεις αυτές είναι οι εξής [48]:

- Attacks with Neighbor Discovery (ND) Messages
- Spoofing traffic to 6to4 nodes
- Reflecting traffic from 6to4 nodes
- Local IPv4 broadcast attack

Attacks with ND Messages

Από την στιγμή που ο 6to4 δρομολογητής υποθέτει ότι όλοι οι άλλοι 6to4 δρομολογητές και 6to4 relays είναι "on-link", είναι πιθανό να επιτευχθεί μια επίθεση στον 6to4 δρομολογητή κάνοντας χρήση ND μηνυμάτων από οποιοδήποτε κόμβο μέσα στο IPv4 δίκτυο, εκτός εάν έχει προηγηθεί η εγκατάσταση μιας σχέσης εμπιστοσύνης [48]. Οι επιθέσεις στοχεύουν στην 6to4 pseudo-interface. Εφόσον οι 6to4 διευθύνσεις δεν χρησιμοποιούνται στην διεύθυνση πηγής / προορισμού ενός πακέτου, οι έλεγχοι ασφάλειας που γίνονται από τον 6to4 μηχανισμό δεν παίρνουν καμία θέση απέναντι σε αυτά τα πακέτα. Τυπικά

χρησιμοποιούνται link-local διευθύνσεις. Για παράδειγμα [48] μια επίθεση μπορεί να είναι ένα Route Advertisement ή Neighbor Advertisement μήνυμα που κατασκευάστηκε με σκοπό να προκαλέσει ζημιά. Οι διευθύνσεις σε ένα τέτοιο πακέτο μπορεί να έχουν την παρακάτω μορφή:

src_v6 = fe80::2 (πλαστογραφημένη διεύθυνση)
dst_v6 = fe80::1 (έγκυρη ή άκυρη διεύθυνση)
src_v4 = 8.0.0.1 (έγκυρη ή πλαστογραφημένη διεύθυνση)
dst_v4 = 9.0.0.2 (έγκυρη διεύθυνση, matches dst_v6)

Spoofing traffic to 6to4 Nodes

Ένας επιτιθέμενος, που μπορεί να είναι ένας κακόβουλος IPv4 ή IPv6 κόμβος μπορεί να στείλει πακέτα σε έναν 6to4 κόμβο, για τα οποία είναι δύσκολο να ανιχνευθούν τα ίχνη τους μέσα στο δίκτυο (για παράδειγμα λόγω spoofing). Οι IPv6 και IPv4 διευθύνσεις μπορούν να έχουν την ακόλουθη μορφή [48]:

src_v6 = 2001:db8::1 (πλαστογραφημένη διεύθυνση)
dst_v6 = 2002:0900:0002::1 (έγκυρη διεύθυνση)
src_v4 = 8.0.0.1 (έγκυρη ή πλαστογραφημένη διεύθυνση)
dst_v4 = 9.0.0.2 (έγκυρη διεύθυνση, matches dst_v6)

Για επιθέσεις που εξαπολύονται από έναν native IPv6 κόμβο, η src_v4 θα είναι η διεύθυνση του relay μέσω του οποίου η κυκλοφορία θα φτάνει τον 6to4 κόμβο. Από επιθέσεις που γίνονται από IPv4 κόμβους, η src_v4 μπορεί να είναι είτε μία spoofed διεύθυνση προορισμού είτε μια πραγματική διεύθυνση. Ο 6to4 δρομολογητής λαμβάνει τα πακέτα που προέρχονται από την διεύθυνση 8.0.0.1, τα “απενθυλακώνει” (decapsulate), ξεφορτώνεται την IPv4 κεφαλίδα που περιέχει την διεύθυνση πηγής 8.0.0.1 και τα επεξεργάζεται κανονικά. Αυτή η επίθεση είναι μιας DoS επίθεση στους 6to4 κόμβους [48].

Reflecting Traffic to 6to4 Nodes

Μια spoofed κυκλοφορία μπορεί να σταλεί σε native IPv6 κόμβους για να εκτελέσουν μια reflection επίθεση εναντίον 6to4 κόμβων. Η spoofed κυκλοφορία αποστέλλεται σε έναν native IPv6 κόμβο, είτε από έναν IPv4 κόμβο (μέσω ενός 6to4 relay) είτε από έναν native IPv6 κόμβο (εκτός αν υπάρχει φιλτράρισμα κατά την είσοδο). Βάση του προηγούμενου παραδείγματος έχουμε τις ακόλουθες διευθύνσεις:

Src_v6 = 2002:1234:1234::1 (πλαστογραφημένη διεύθυνση του 6to4 κόμβου-στόχου)
dst_v6 = 2002:0900:0002::1 (έγκυρη διεύθυνση)
src_v4 = 8.0.0.1 (έγκυρη ή άκυρη διεύθυνση)
dst_v4 = 9.0.0.2 (έγκυρη διεύθυνση, matches dst_v6)

Να σημειώσουμε ότι μια επίθεση μέσω ενός relay εμποδίζεται εάν το relay χρησιμοποιεί κατάλληλους ελέγχους ασφάλειας κατά την διαδικασία decapsulation, εκτός αν ο IPv4 κόμβος μπορεί να κάνει spoof την διεύθυνση πηγής για να ταιριάξει με την src_v6. Τέτοιες επιθέσεις μπορούν να ξεκινήσουν από native IPv6 ή IPv4 ή 6to4 κόμβους [48].

Local IPv4 Broadcast Attack

Αυτή η απειλή είναι εφαρμόσιμη όταν ο 6to4 δρομολογητής δεν ελέγχει αν η IPv4 διεύθυνση, στην οποία προσπαθεί να στείλει τα ενθυλακωμένα IPv6 πακέτα είναι μια local broadcast διεύθυνση ή μια multicast διεύθυνση. Στην πράξη υπάρχουν δύο είδη επίθεσης: όταν ένας τοπικός 6to4 χρήστης προσπαθεί να στείλει πακέτα στην διεύθυνση που αντιστοιχεί στην broadcast address και όταν κάποιος προσπαθεί να κάνει κάτι στον ελάχιστο βαθμό [48].

Στην πρώτη επίθεση, υποθέτουμε ότι η 9.0.0.255 είναι broadcast διεύθυνση του 6to4 δρομολογητή. Αφού λάβει το πακέτο με μια διεύθυνση προορισμού π.χ. "2002:0900:00ff::bbbb" από έναν τοπικό 6to4 κόμβο, εάν ο δρομολογητής δεν ελέγξει την διεύθυνση προορισμού, θα στείλει το ενθυλακωμένο πακέτο στην διεύθυνση 9.0.0.255. Αυτό το πακέτο θα παραληφθεί από όλους τους κόμβους του υποδικτύου και όλες οι απαντήσεις θα κατευθυνθούν προς τον 6to4 δρομολογητή, με αποτέλεσμα να επιτευχθεί μια DoS επίθεση.

Το δεύτερο είδος επίθεσης είναι περισσότερο περίπλοκο: Η επίθεση μπορεί να ξεκινήσει από IPv4 κόμβους που δεν ανήκουν στο τοπικό δίκτυο, με την προυπόθεση ότι μπορούν να στείλουν δικτυακή κυκλοφορία με άκυρη διεύθυνση πηγής (για παράδειγμα : 2002:0900:00ff::bbbb). Ο 6to4 δρομολογητής πρέπει να ανταποκριθεί στην κυκλοφορία αυτή, στέλνοντας ICMPv6 πακέτα πίσω στην πηγή. Το πακέτο θα είναι ως εξής :

Src_v6 = 2002:0800:00ff::bbbb (broadcast address του δρομολογητή)
Dst_v6 = 2002:0800:0001::0001 (έγκυρη μη υπάρχουσα διεύθυνση)

Και το δεύτερο είδος επίθεσης αποτελεί μια DoS attack.

7.3.3.2 Teredo Tunneling Mechanism

Το Teredo είναι ένας μηχανισμός μετάβασης που δίνει πλήρη IPv6 συνδεσιμότητα σε IPv6 υπολογιστές/συστήματα που βρίσκονται μέσα στο IPv4 διαδίκτυο, αλλά δεν έχουν άμεση φυσική σύνδεση σε ένα IPv6 δίκτυο. Σε σχέση με άλλα παρόμοια πρωτόκολλα το ιδιαίτερο χαρακτηριστικό του Teredo είναι ότι εκτελεί τις λειτουργίες του ακόμα και πίσω από network address translation (NAT) συσκευές, όπως οι οικιακοί δρομολογητές [49].

Το Teredo λειτουργεί με σκοπό να παρέχει IPv6 συνδεσιμότητα, ενθυλακώνοντας IPv6 πακέτα μέσα σε IPv4 User Datagram Protocol (UDP) πακέτα. Αυτά τα πακέτα μπορούν να δρομολογηθούν στο IPv4 διαδίκτυο και διαμέσου NAT συσκευών.

Σκοπός

Ο 6to4 μηχανισμός μετάβασης, απαιτεί το tunnel endpoint να έχει μια δημόσια IPV4 διεύθυνση, Ωστόσο, κατά την παρούσα περίοδο αρκετοί υπολογιστές/συστήματα συνδέονται σε μια ή περισσότερες NAT συσκευές, συνήθως λόγω της έλλειψης IPv4 διευθύνσεων. Σε αυτή την περίπτωση η μόνη διαθέσιμη δημόσια IPv4 διεύθυνση ανατίθεται στην NAT συσκευή και το 6to4 tunnel endpoint χρειάζεται να υλοποιηθεί από μόνο του στην NAT συσκευή. Ωστόσο, αρκετές NAT συσκευές που σχεδιάζονται δεν μπορούν να αναβαθμιστούν ώστε να υλοποιούν τον 6to4 μηχανισμό, για τεχνικούς ή οικονομικούς λόγους [49].

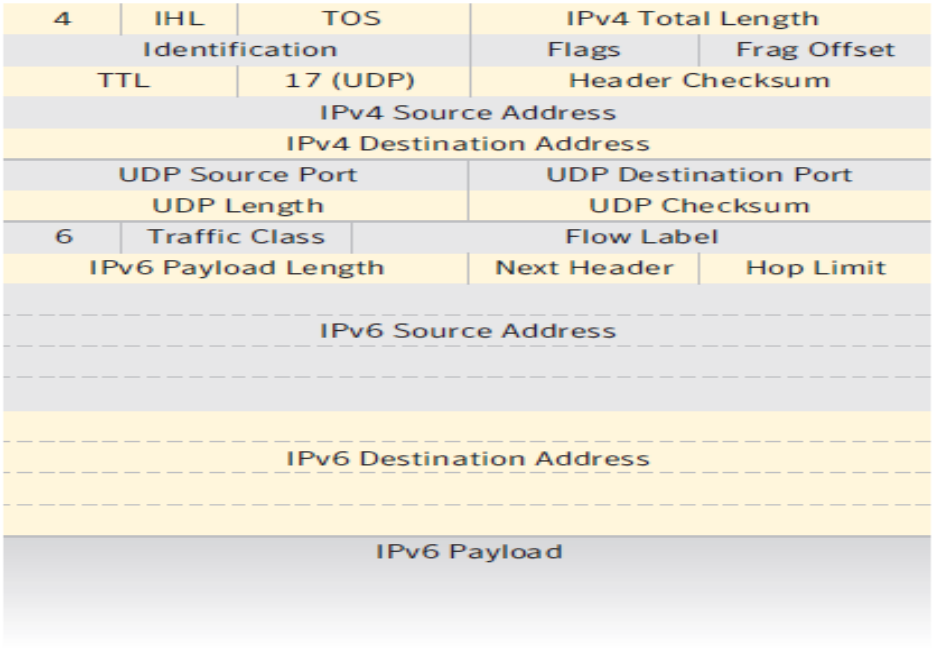
Το Teredo αντιμετωπίζει το παραπάνω πρόβλημα ενθυλακώνοντας τα IPv6 πακέτα μέσα σε IPv4 UDP datagrams, τα οποία οι περισσότερες NAT συσκευές είναι σε θέση να προωθήσουν με σωστό τρόπο. Κατά συνέπεια οι IPv6 υπολογιστές/συστήματα που βρίσκονται πίσω από τις NAT συσκευές μπορούν να χρησιμοποιηθούν ως Teredo tunnel endpoints ακόμα και όταν δεν έχουν μια δημόσια IPv4 διεύθυνση [49].

Το Teredo προτίθεται να είναι ένα προσωρινό μέτρο, με σκοπό στο μέλλον όλοι οι IPv6 υπολογιστές/συστήματα να κάνουν χρήση native IPv6 συνδεσιμότητας [49].

Teredo λειτουργίες και node types

Οι λειτουργίες που εκτελεί ο Teredo μηχανισμός είναι οι εξής [49] (Εικόνα 7.9):

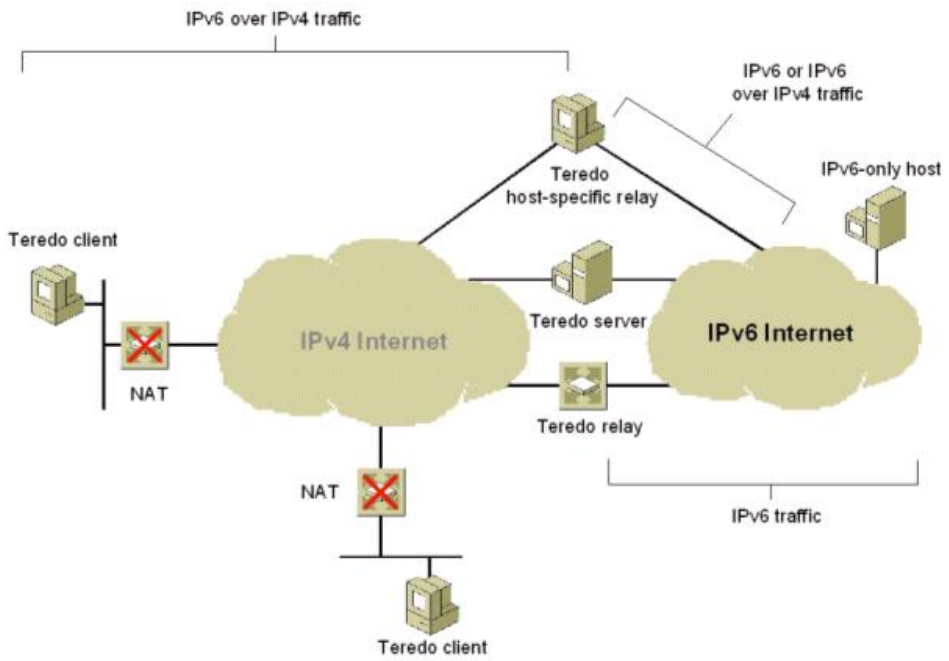
1. Διάγνωση συνδεσιμότητας UDP πάνω από IPv4 και ανακάλυψη του είδους του NAT.
2. Ανάθεση μιας μοναδικής παγκόσμιας IPv6 διεύθυνσης σε κάθε υπολογιστή/σύστημα που χρησιμοποιεί το Teredo.
3. Ενθυλάκωση IPv6 πακέτων μέσα σε UDPv4 datagrams για μετάδοση πάνω από ένα IPv4 δίκτυο.
4. Δρομολόγηση κυκλοφορίας ανάμεσα σε Teredo υπολογιστές/συστήματα και native IPv6 υπολογιστές/συστήματα.



Εικόνα 7.9: Teredo Μηχανισμός - Ενθυλάκωση IPv6 πακέτου μέσα σε ένα IPv4 UDP πακέτο

Το Teredo προσδιορίζει διάφορα είδη κόμβων. Αυτά είναι τα εξής [50] (Εικόνα 7.10):

- **Teredo client:** Ένας host, ο οποίος έχει IPv4 συνδεσιμότητα στο διαδίκτυο πίσω από μια NAT συσκευή και χρησιμοποιεί το Teredo tunneling για πρόσβαση στο IPv6 διαδίκτυο. Στους teredo πελάτες (clients) ανατίθεται μια IPv6 διεύθυνση που ξεκινά με το Teredo prefix (2001:0::/32).
- **Teredo server:** Ένας γνωστός υπολογιστής/σύστημα, ο οποίος χρησιμοποιείται για την αρχική διαμόρφωση ενός Teredo tunnel. Ένας Teredo εξυπηρετητής (server) δεν προωθεί ποτέ κυκλοφορία για έναν πελάτη (εκτός από IPv6 pings) και για αυτό τον λόγο έχει μέτριες απαιτήσεις σε bandwidth, το οποίο επιτρέπει σε έναν εξυπηρετητή να υποστηρίζει μεγάλο αριθμό πελατών.
- **Teredo relay:** Αποτελεί το απομακρυσμένο άκρο ενός Teredo tunnel. Ένα Teredo relay πρέπει να προωθεί όλα τα δεδομένα για λογαριασμό των Teredo clients που εξυπηρετεί. Για αυτό τον λόγο, ένα relay απαιτεί πολύ bandwidth και μπορεί να εξυπηρετήσει ένα περιορισμένο αριθμό από ταυτόχρονους πελάτες (clients). Κάθε Teredo relay εξυπηρετεί μία γκάμα από IPv6 hosts (για παράδειγμα μια μοναδική εταιρία, έναν ISP ή ένα ολόκληρο δίκτυο) και προωθεί την κυκλοφορία ανάμεσα στους Teredo clients και τους παραπάνω hosts.
- **Teredo host-specific relay:** Ένα relay του οποίου των φάσμα υπηρεσιών είναι περιορισμένο σε έναν μόνο υπολογιστή/σύστημα συνεχίζει με αμείωτο ρυθμό. Ως εκ τούτου δεν έχει ιδιαίτερες απαιτήσεις σχετικά με το bandwidth και την δρομολόγηση. Ένας υπολογιστής με ένα host-specific relay θα χρησιμοποιούσε το Teredo για να επικοινωνήσει με τους Teredo clients, αλλά θα κολλούσε στον κύριο πάροχο IPv6 συνδεσιμότητας με σκοπό να φτάσει το υπόλοιπο του IPv6 διαδικτύου.



Εικόνα 7.10: Συστατικά στοιχεία μιας Teredo υποδομής

Επιθέσεις στο Teredo

Ο αντικειμενικός σκοπός του Teredo είναι να παρέχει μια παγκόσμια IPv6 διεύθυνση στους κόμβους που βρίσκονται πίσω από μια NAT συσκευή. Οι κόμβοι του Teredo μπορούν να κάνουν χρήση IPsec υπηρεσιών, όπως Internet Key Exchange (IKE), Authentication Header (AH), ή Encapsulation Security Payload (ESP). Ως εκ τούτου, μπορούμε να υποστηρίξουμε ότι το Teredo έχει μια θετική επιρροή στην ασφάλεια του δικτύου. Ωστόσο, πρέπει να αναλογιστούμε και την άλλη μεριά του Teredo, εκείνη που επιφέρει αρνητικές επιπτώσεις στην ασφάλεια του δικτύου. Το Teredo είναι ευπαθές σε μια σειρά από επιθέσεις, οι οποίες μπορούν να συγκεντρωθούν στις ακόλουθες τέσσερις κατηγορίες [51]:

- Opening a hole in the NAT
- Using the Teredo service for a Man-in-the-Middle attack
- Denial of the Teredo service
- Denial of service against non Teredo nodes

Opening a Hole in the NAT

Ο πιο σημαντικός σκοπός της Teredo υπηρεσίας είναι να κάνει μια μηχανή προσεγγίσιμη μέσω του IPv6. Εξορισμού, η μηχανή που χρησιμοποιεί το Teredo εγκαταλείπει οποιαδήποτε υπηρεσία firewall που είναι διαθέσιμη στην NAT συσκευή. Οι υπηρεσίες που "ακούνε" στην Teredo IPv6 διεύθυνση, θα γίνουν ο πιθανός στόχος για επιθέσεις από ολόκληρο το IPv6 διαδίκτυο. Υπάρχουν τρεις παράγοντες [51] που μετριάζουν το παραπάνω πρόβλημα.

Ο πρώτος παράγοντας είναι η δυνατότητα που υπάρχει να περιοριστούν μερικές υπηρεσίες, με σκοπό να αποδέχονται κυκλοφορία μόνο από τοπικούς γείτονες, για παράδειγμα χρησιμοποιώντας link-local διευθύνσεις. Το Teredo δεν υποστηρίζει επικοινωνία κάνοντας χρήση link-local διευθύνσεων, κάτι που υποδηλώνει ότι οι link-local υπηρεσίες δεν θα μπορούν να προσπελαστούν διαμέσου του Teredo.

Ο δεύτερος παράγοντας άμβλυνσης είναι η δυνατότητα χρήσης ενός "τοπικού" firewall. Για παράδειγμα μπορεί να γίνει χρήση ενός λογισμικού που θα εκτελεί τοπικά ένα είδος επιθεώρησης και φιλτραρίσματος.

Ο τρίτος παράγοντας μετριασμού του προβλήματος είναι η διαθεσιμότητα IPsec υπηρεσιών, όπως IKE,AH ή ESP. Η χρήση τέτοιων υπηρεσιών σε συνδυασμό με το Teredo είναι μια πολύ καλή πολιτική, καθώς προστατεύει τον πελάτη από πιθανές επιθέσεις σε ενδιάμεσους εξυπηρετητές, όπως το NAT, Teredo server ή Teredo relay.

Using the Teredo Service for a Man-in-the-Middle Attack

Υπάρχει ένα σύνολο από πιθανές επιθέσεις που μπορούν να επιτευχθούν εναντίον του Teredo, κατά τις οποίες ένας επιτιθέμενος υποκλέπτει ένα router solicitation μήνυμα, απαντάει με ένα spoofed router advertisement μήνυμα και παρέχει μια εσφαλμένη διεύθυνση σε έναν Teredo clients. Ο επιτιθέμενος έχει έναν από τους δύο παρακάτω στόχους: (i) προσπαθεί να αρνηθεί την υπηρεσία στον Teredo clients παρέχοντάς του μια διεύθυνση που στην πραγματικότητα είναι μη προσεγγίσιμη (unreachable), ή (ii) προσπαθεί να εισάγει τον εαυτό του ως ένα relay για όλες τις επικοινωνίες ενός πελάτη, πετυχαίνοντας μια ποικιλία από man-in-the-middle επιθέσεις [51].

Denial of the Teredo service

Υπάρχουν πέντε επιθέσεις που έχουν στόχο την απάρνηση της Teredo υπηρεσίας. Παρακάτω περιγράφονται αυτές οι επιθέσεις και τα αντίστοιχα αντίμετρα.

- **Denial of Service by a Rogue Relay:** Μια επίθεση μπορεί να τοποθετηθεί στην μεριά IPv6 της υπηρεσίας Teredo, εγκαθιστώντας ένα rogue relay και επιτρέποντας αυτό το relay να γνωστοποιεί ένα δρομολόγιο στο Teredo IPv6 prefix. Αυτή είναι μια επίθεση εναντίον του IPv6 routing, η οποία μπορεί να αμβλυνθεί χρησιμοποιώντας μεθόδους για την εξάλειψη των κάλπικων route advertisements μηνυμάτων. Οι dual-stack κόμβοι που υλοποιούν "host local" Teredo relays είναι άτρωτοι σε αυτή την επίθεση [51].
- **Denial of Service by Server Spoofing:** Γίνεται χρήση spoofed router advertisements με σκοπό να εκχωρηθεί στον πελάτη μια εσφαλμένη διεύθυνση, η οποία μπορεί να είναι είτε μια μη υπάρχουσα IPv4 διεύθυνση είτε μια IPv4 διεύθυνση μιας τρίτης οντότητας. Ο Teredo client θα ανιχνεύσει αυτή την επίθεση όταν θα αποτύχει να λάβει κυκλοφορία μέσω την νέας αποκτηθείσας IPv6 διεύθυνσης. Η επίθεση μπορεί να μετριασθεί κάνοντας χρήση μηχανισμών αυθεντικοποίησης [51].
- **Denial of Service by Exceeding the Number of Peers:** Ο Teredo client διαχειρίζεται μια μνήμη (cache) με τους πρόσφατα χρησιμοποιούμενους peers, γεγονός που κάνει το Teredo stateful (διατήρηση καταστάσεων). Υπάρχει δυνατότητα να επιτευχθεί μια επίθεση εναντίον ενός πελάτη προκαλώντας τον να ανταποκριθεί σε πακέτα που φαίνεται να προέρχονται από έναν μεγάλο αριθμό από Teredo peers. Αυτό έχει ως συνέπεια να αχρηστεύεται η cache και να μην επιτρέπεται η απευθείας επικοινωνία ανάμεσα στους peers (αφού η cache αλλάζει συνεχώς). Η επίδραση διατηρείται για όσο χρονικό διάστημα υφίσταται η επίθεση [51].
- **Attacks against the Local Discovery Procedure:** Υπάρχει η δυνατότητα επίτευξης μιας denial of service επίθεσης ενάντια στην διαδικασία ανακάλυψης τοπικού peer (local peer discovery procedure), εάν οι επιτιθέμενοι μπορούν να στείλουν spoofed local discovery bubbles σε έναν Teredo client [51].
- **Attacking the Teredo Servers and Relays:** Υπάρχει η δυνατότητα να επιτευχθεί μια denial of service επίθεση εναντίον των Teredo servers, στέλνοντάς τους έναν μεγάλο αριθμό από πακέτα. Μια brute force επίθεση που γίνεται εναντίον των Teredo servers μπορεί να μετριασθεί εάν οι πελάτες είναι έτοιμοι να απευθυνθούν σε έναν άλλο εξυπηρετητή. Το "γεφύρωμα" των εξυπηρετητών, ωστόσο, αναγκάζει τους πελάτες που αλλάζουν εξυπηρετητές να επαναριθμούν την Teredo διεύθυνσή τους. Επίσης, είναι να δυνατόν να επιτευχθεί μια brute force επίθεση εναντίον ενός Teredo relay. Αυτή η επίθεση μπορεί να αμβλυνθεί εάν το relay που βρίσκεται υπό επίθεση σταματήσει να ανακοινώνει στο IPv6 δίκτυο την δυνατότητα προσέγγισης της Teredo υπηρεσίας [51].

Denial of Service against Non-Teredo Nodes

Υπάρχει μια ευρέως εκφρασμένη ανησυχία ότι οι μηχανισμοί μετάβασης, όπως το Teredo μπορούν να χρησιμοποιηθούν για επίτευξη denial of service επιθέσεων, σε τοποθεσίες που δεν αναμένεται να υποστούν επίθεση. Αυτές οι επιθέσεις συγκεντρώνονται σε τρεις

κατηγορίες: χρήση των Teredo servers σαν ένα κάτοπτρο για denial of service επίθεση, χρήση του Teredo server για επίτευξη μιας denial of service επίθεσης εναντίον των IPv6 κόμβων και χρήση των Teredo relays για επίτευξη μιας denial of service επίθεση εναντίον IPv4 κόμβων [51].

8

Internet Protocol Security

Το IPsec είναι μια σουίτα πρωτοκόλλων που ορίζουν ορισμένες υπηρεσίες ασφάλειας που χρησιμοποιούνται στο επίπεδο δικτύου από τα πρωτόκολλα IPv4 και IPv6. Το IPsec αποτελεί αναπόσπαστο κομμάτι του IPv6, δίνοντας την δυνατότητα για διασφάλιση της εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας μιας επικοινωνίας. Το IPsec υποστηρίζει δύο τρόπους λειτουργίας, την transport mode και την tunnel mode.

Στην transport mode (μεταφοράς) λειτουργία, η ασφάλεια εφαρμόζεται μεταξύ των υπολογιστών/συστημάτων (end-to-end) και μόνο το ωφέλιμο φορτίο του πακέτου αυθεντικοποιείται ή κρυπτογραφείται, ενώ η κεφαλίδα του IP πακέτου μένει αμετάβλητη και δεν προστατεύεται [15]. Στην tunnel mode (διόδου) λειτουργία, ολόκληρο το πακέτο ενθυλακώνεται σε ένα νέο πακέτο, ώστε το εσωτερικό (αρχικό) πακέτο να αποτελεί ωφέλιμο φορτίο του εξωτερικού (νέου) πακέτου. Το νέο IP πακέτο οδεύεται από την μία IP gateway στην άλλη, χωρίς να είναι απαραίτητη η υλοποίηση IPsec δυνατοτήτων στους end υπολογιστές/συστήματα [15]. Το IP security έχει τέσσερις κύριες λειτουργίες [6]:

- Security Associations (SA)
- Authentication only (Authentication Header ή AH
- Encryption και authentication γνωστή ως Encapsulating Security Payload (ESP)
- Key management

8.1 Security Association (SA)

Μια βασική έννοια που εμφανίζεται στους αλγορίθμους πιστοποίησης και κρυπτογράφησης για το IP είναι η συσχέτιση ασφάλειας (security association). Η συσχέτιση ασφάλειας είναι μια μονόδρομη σχέση μεταξύ του αποστολέα και παραλήπτη και παρέχει υπηρεσίες ασφάλειας στην κυκλοφορία που διεξάγεται σε αυτήν [15]. Εάν απαιτείται μια ισότιμη σχέση για αμφίδρομες ασφαλείς συναλλαγές, τότε απαιτούνται δύο SA. Μια συσχέτιση ασφάλειας προσδιορίζεται μοναδικά από τρεις παραμέτρους:

- **Security Parameter Index (SPI):** Μια σειρά από bit που προσδιορίζει την συσχέτιση ασφάλειας και έχει μόνο τοπική σημασία [6, 15]. Ο δείκτης SPI μεταφέρεται στις κεφαλίδες AH και ESP έτσι ώστε να επιτρέψει στο σύστημα του παραλήπτη να επιλέξει την SA με βάση την οποία θα επεξεργασθεί το πακέτο που παρέλαβε.
- **IP Destination Address:** Υποστηρίζει μόνο unicast διευθύνσεςι. Η συγκεκριμένη παράμετρος αποτελεί την διεύθυνση προορισμού της SA [6, 15].

- **Security Protocol Identifier:** Η συγκεκριμένη παράμετρος δηλώνει εάν η συσχέτιση ασφάλειας αφορά το AH ή το ESP [6, 15].

Κάθε συσχέτιση ασφάλειας διατηρεί μια βάση δεδομένων (Security association database, SAD), η οποία περιέχει ορισμένες σημαντικές παραμέτρους, όπως: δεδομένα που χρησιμοποιήθηκαν για αυθεντικοποίηση (AH ή ESP πρωτόκολλα, δημόσια κλειδιά, χρονική διάρκεια κλειδιών), δεδομένα που χρησιμοποιήθηκαν για εμπιστευτικότητα (ESP πρωτόκολλο κρυπτογράφησης, δημόσια κλειδιά, χρονική διάρκεια κλειδιών), δεδομένα που χρησιμοποιήθηκαν για προστασία από επανεκπομπή (μετρητές υπερχείλισης, IP packet sequence numbers), τρόπος λειτουργίας του IPsec (transport mode ή tunnel mode), καθώς και διάρκεια ζωής της SA (σε bytes ή χρόνο) [15].

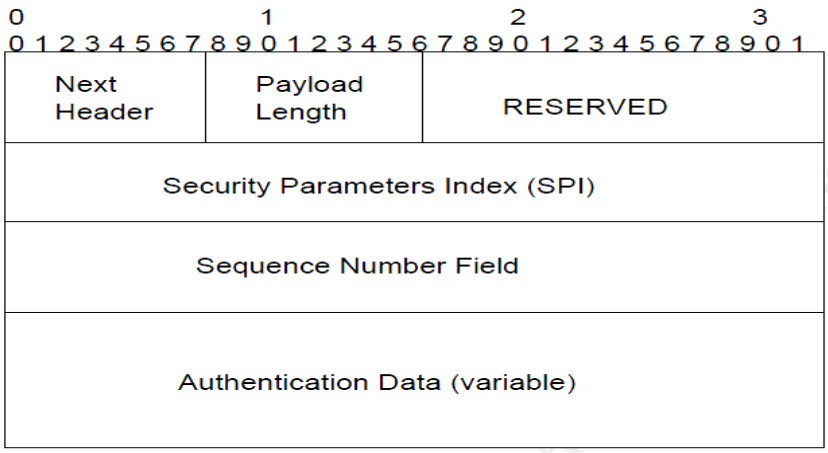
8.2 Authentication Header (AH)

Το IP Authentication Header (AH) χρησιμοποιείται για διατήρηση ακεραιότητας και πιστοποίηση αυθεντικότητας του IP πακέτου, καθώς και για anti replay προστασία απέναντι σε anti replay επιθέσεις.

Η πιστοποίηση αυθεντικότητας των δεδομένων αναφέρεται στο γεγονός ότι εάν ένας υπολογιστής/σύστημα λάβει ένα IP πακέτο από μια συγκεκριμένη διεύθυνση πηγής (που δίνεται στην κεφαλίδα IP), τότε πράγματι το πακέτο προέρχεται από την διεύθυνση πηγής που αναφέρει η κεφαλίδα IP. Η διατήρηση της ακεραιότητας των δεδομένων έχει σχέση με την εξασφάλιση αποφυγής τροποποίησης (σκόπιμη ή μη) των δεδομένων κατά την διάρκεια μεταφοράς του πακέτου από την πηγή στον προορισμό. Η anti replay προστασία αναφέρεται στην προστασία που παρέχεται σε έναν υπολογιστή/σύστημα, ώστε να αποφεύγεται η αποδοχή πακέτων που έχει ήδη λάβει, τα οποία ενδέχεται να περιέχουν τροποποιημένα δεδομένα [8]. Η Authentication Header αποτελείται από τα ακόλουθα πεδία [16] (Εικόνα 8.1):

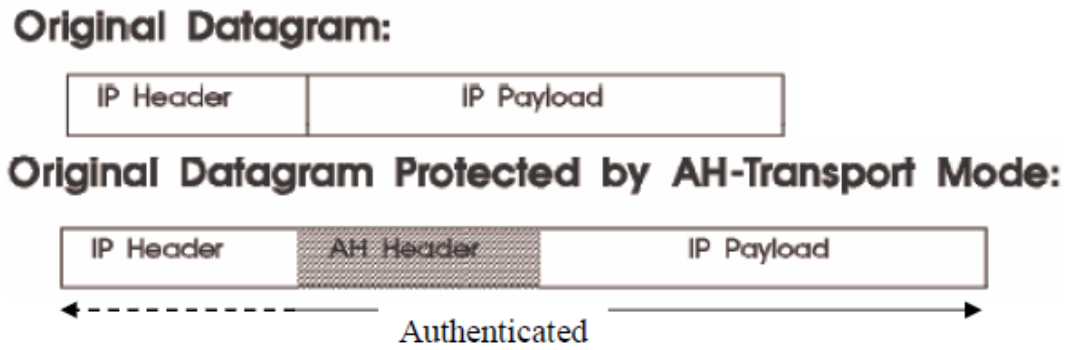
- **Next Header:** Ο τύπος της κεφαλίδας που έπεται του AH. Η τιμή του επιλέγεται από το σύνολο των IP Ptotocol Numbers, όπως ορίζονται από το INA (π.χ TCP).
- **Payload Length:** Μήκος του AH σε 32-bits words.
- **Reserved:** Για μελλοντική χρήση.
- **Security Parameter Index (SPI):** Προσδιορίζει την ασφάλεια συσχέτισης που χρησιμοποιείται.
- **Sequence Number:** Αυξάνων μετρητής. Χρήση για προστασία έναντι anti replay επιθέσεων.
- **Authentication Data:** Περιέχει Integrity Check Value (ICV) ή MAC[22] για αυτό το πακέτο.

[22] Αποτελεί μια τεχνική αυθεντικοποίησης μηνύματος και διασφάλιση ακεραιότητας μηνύματος. Η τεχνική απαιτεί την χρήση ενός μυστικού κλειδιού, ώστε να παραχθεί ένα μικρό τμήμα δεδομένων το οποίο προσαρτάται στο μήνυμα. Ο αποστολέας στέλνει το μήνυμα μαζί με το MAC που έχει υπολογίσει μέσω του μυστικού κλειδιού. Ο παραλήπτης υπολογίζει εκ νέου το MAC (MAC΄΄) και το συγκρίνει με αυτό που του εστάλη. Εάν τα δύο MAC είναι ίσα τότε το μήνυμα δεν έχει τροποποιηθεί (ακεραιότητα) και προέρχεται από την διεύθυνση/πηγή που το πακέτο δηλώνει (αυθεντικοποίηση) [16].



Εικόνα 8.1: Authentication Header (AH)

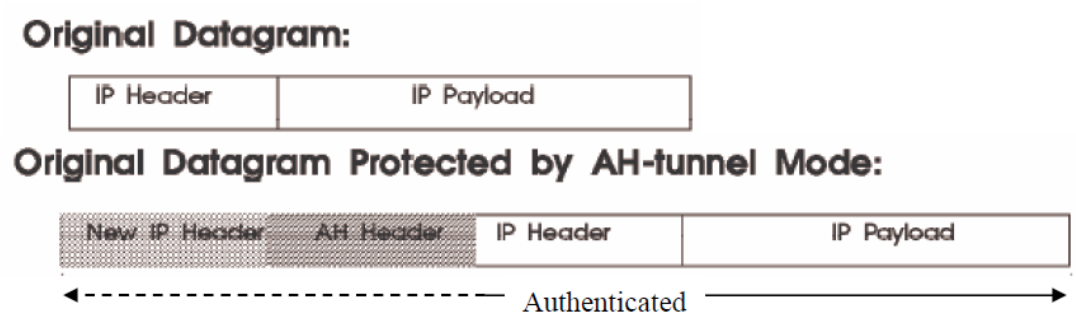
Η κεφαλίδα Authentication Header μπορεί να χρησιμοποιηθεί είτε σε transport mode είτε σε tunnel mode. Στην λειτουργία transport mode (Εικόνα 8.2) η αρχική κεφαλίδα του IP πακέτου είναι η εξωτερική κεφαλίδα του νέου IP πακέτου, ακολουθούμενη από την AH κεφαλίδα και στην συνέχεια ακολουθεί το ωφέλιμο φορτίο του αρχικού IP πακέτου [15]. Στην transport mode λειτουργία αυθεντικοποιείται το ωφέλιμο φορτίο του IP πακέτου και μέρος[23] της κεφαλίδας του IP πακέτου [15].



Εικόνα 8.2: Authentication in Transport Mode

Στην λειτουργία tunnel mode (Εικόνα 8.3) αυθεντικοποιείται ολόκληρο το IP πακέτο. Το πακέτο ενθυλακώνεται μέσα σε ένα νέο IP πακέτο, έτσι το εσωτερικό (αρχικό) πακέτο αποτελεί ωφέλιμο φορτίο του εξωτερικού (νέου) πακέτου. Το ενθυλακωμένο πακέτο περιέχει την IP διεύθυνση του end υπολογιστή/συστήματος, ενώ το εξωτερικό πακέτο περιέχει στην κεφαλίδα του την IP διεύθυνση του gateway[24]. Σε αυτή την περίπτωση αυθεντικοποιείται το ωφέλιμο φορτίο του πακέτου, δηλαδή ολόκληρο το εσωτερικό πακέτο και μέρος της κεφαλίδας του εξωτερικού πακέτου [15].

[23] Τα πεδία της κεφαλίδας που δεν αλλάζουν κατά την μεταφορά από την πηγή στον προορισμό του πακέτου.
[24] Μπορεί να είναι ένας router ή ένα firewall



Εικόνα 8.3: Authentication in Tunnel Mode

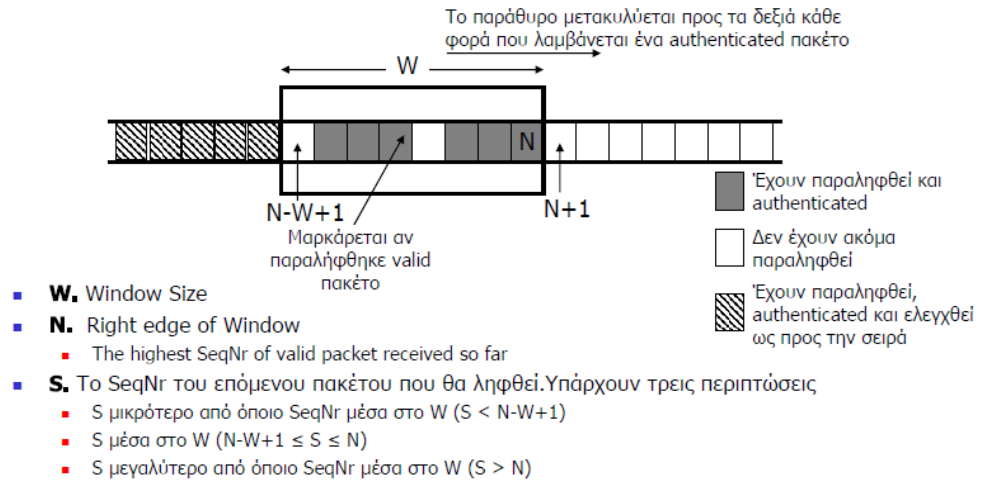
Αντιμετώπιση Replay Επίθεσης

Μία replay attack [15] είναι μια επίθεση, κατά την οποία ο επιτιθέμενος αποκτά ένα αντίγραφο ενός αυθεντικοποιημένου πακέτου και στην συνέχεια το μεταδίδει στον προορισμό. Αυτό έχει ως αποτέλεσμα την παραλαβή διπλότυπων αυθεντικοποιημένων IP πακέτων, που μπορεί να επιφέρουν διαταραχή στην υπηρεσία ή άλλα ανεπιθύμητα αποτελέσματα.

Η αποτροπή τέτοιου είδους επιθέσεων γίνεται με χρήση του πεδίου sequence number (αριθμός σειράς). Όταν μια νέα συσχέτιση ασφάλειας (SA) εγκαθιδρύεται, ο αποστολέας αρχικοποιεί το sequence number δίνοντας την τιμή 0. Κάθε φορά που ένα πακέτο αποστέλλεται μέσω αυτής της SA, ο αποστολέας αυξάνει την τιμή του πεδίου sequence number κατά ένα [15]. Κατά αυτόν τον τρόπο, η πρώτη τιμή του πεδίου είναι η 1. Εάν έχει ενεργοποιηθεί η επιλογή anti-replay, τότε ο αποστολέας δεν πρέπει να επιτρέψει στο πεδίο Sequence Number να ξεπεράσει το $2^{32} - 1$ και να επιστρέψει στο μηδέν. Διαφορετικά, θα μπορούν να υπάρχουν πολλά έγκυρα πακέτα με ίδια τιμή στο πεδίο sequence number. Εάν φτάσει στο όριο $2^{32} - 1$, ο αποστολέας πρέπει να τερματίσει την συγκεκριμένη SA και να διαπραγματευτεί την εγκαθίδρυση μιας νέας SA με νέο κλειδί [15].

Λόγω του γεγονότος ότι το IP είναι ένα αναξιόπιστο πρωτόκολλο, δεν εγγυάται ότι τα πακέτα θα φτάσουν με την σωστή σειρά, ούτε ότι θα φτάσουν όλα [15]. Για αυτό τον λόγο, το IPsec υποχρεώνει τον παραλήπτη να διατηρεί ένα παράθυρο (anti replay window) (Εικόνα 8.4), με ένα μέγεθος W [25]. Το δεξιό άκρο του παραθύρου αντιπροσωπεύει την υψηλότερη τιμή N του πεδίου sequence number, που έχει ληφθεί μέχρι στιγμής από κάποιο έγκυρο πακέτο.

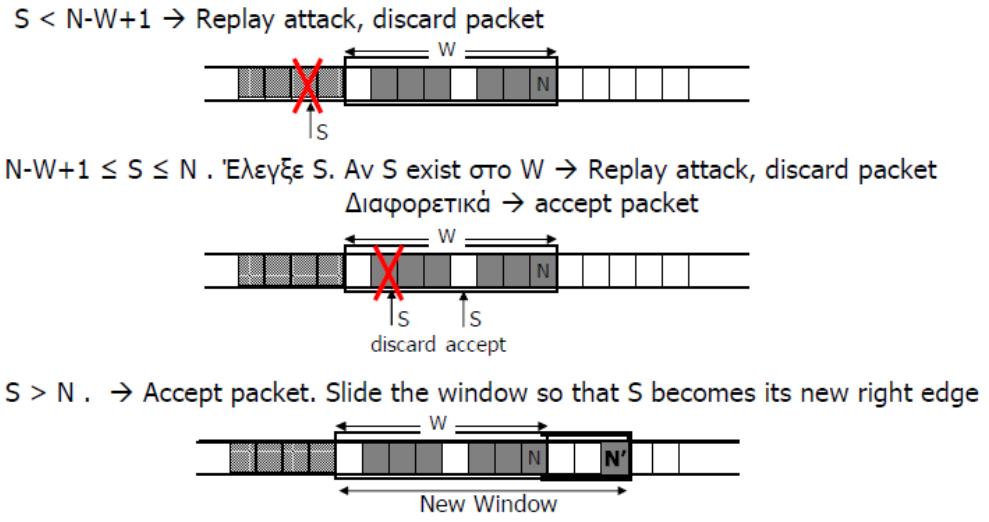
[25] Προεπιλογή είναι το W = 64



Εικόνα 8.4: Anti Replay Window

Για το επόμενο πακέτο που θα ληφθεί ισχύουν τρεις περιπτώσεις όσον αφορά την τιμή του sequence number (S) [16] (Εικόνα 8.5):

- S μικρότερο από οποιοδήποτε SeqNr μέσα στο W (S < N-W+1). Σε αυτή την περίπτωση έχουμε replay attack και το πακέτο απορρίπτεται από τον παραλήπτη.
- N-W+1 <= S <= N Σε αυτή την περίπτωση ο παραλήπτης ελέγχει την τιμή S. Αν υπάρχει ίδια τιμή μέσα στο W, τότε πρόκειται για replay attack και το πακέτο απορρίπτεται. Διαφορετικά γίνεται αποδοχή του πακέτου από τον παραλήπτη.
- S > N Ο παραλήπτης αποδέχεται το πακέτο και το παράθυρο κυλίεται, έτσι ώστε το S να γίνει το νέο δεξιό άκρο του παραθύρου.

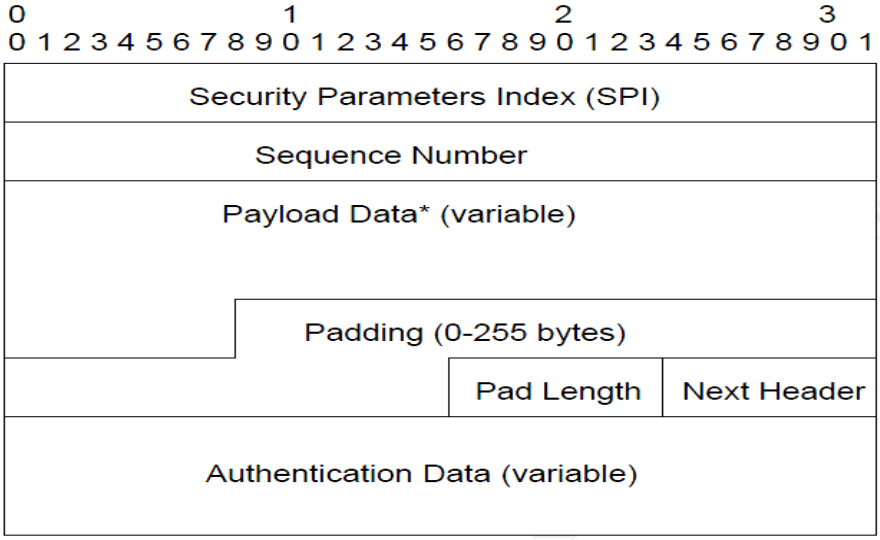


Εικόνα 8.5: Αντιμετώπιση Replay Attack για διαφορετικές τιμές sequence number

8.3 Encapsulating Security Payload (ESP)

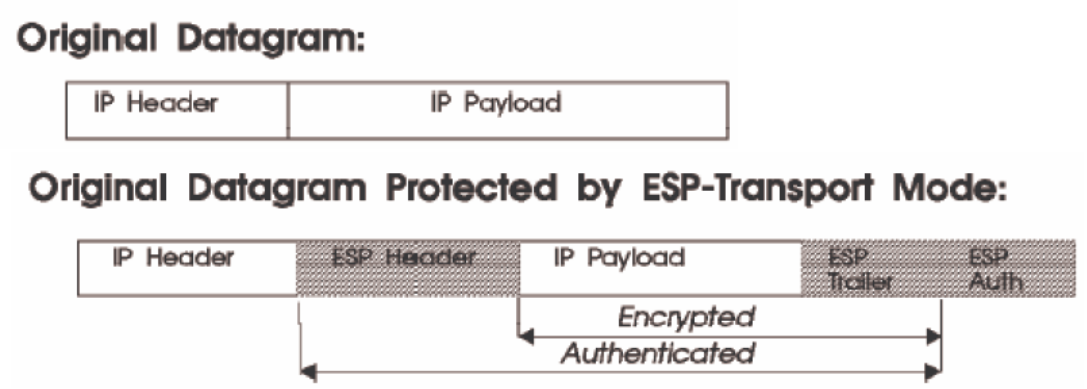
Η Encapsulating Security Payload κεφαλίδα χρησιμοποιείται για παροχή υπηρεσιών εμπιστευτικότητας και περιορισμένης έκτασης υπηρεσίες αυθεντικοποίησης. Η ESP μπορεί να εφαρμοσθεί μόνη της ή σε συνδυασμό με την AH. Μια κεφαλίδα ESP αποτελείται από τα ακόλουθα πεδία [16] (Εικόνα 8.6):

- **Security Parameter Index (SPI):** Προσδιορίζει μια SA.
- **Sequence Number:** Μετρητής που αυξάνει με την μετάδοση κάθε πακέτου.
- **Payload Data:** Κρυπτογραφημένα δεδομένα του IP πακέτου.
- **Padding:** Προσθήκη χαρακτήρων για να προκύψουν αποδεκτά πολλαπλάσια μήκη πακέτου. Αυτή η ενέργεια απαιτείται από τον αλγόριθμο κρυπτογράφησης στην περίπτωση που χρειάζεται να συμπληρώσει κάποιο block με bytes πριν περάσει από το στάδιο κρυπτογράφησης.
- **Pad length:** Ο αριθμός padding χαρακτήρων.
- **Next Header:** Ο τύπος του header που έπεται του ESP.
- **Authentication Data:** Περιέχει integrity check value (ICV) για αυτό το πακέτο.



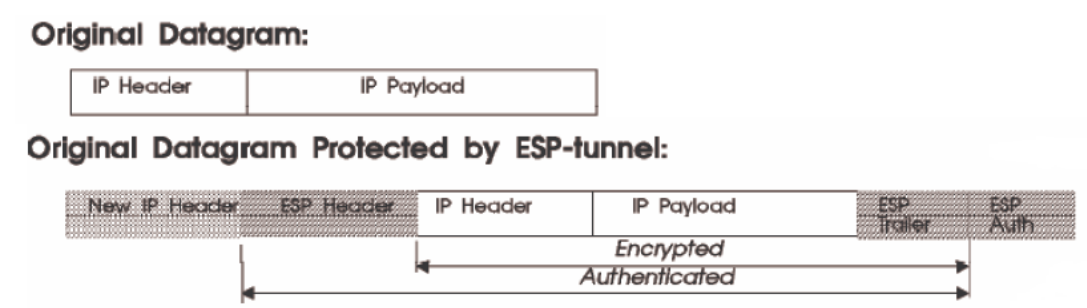
Εικόνα 8.6: Encapsulating Security Payload

Η κεφαλίδα Encapsulating Security Payload μπορεί να χρησιμοποιηθεί είτε σε transport mode είτε σε tunnel mode. Στην λειτουργία transport mode (Εικόνα 8.7) έχουμε κρυπτογράφηση των δεδομένων του IP πακέτου, δηλαδή του ωφέλιμου φορτίου του πακέτου. Η κεφαλίδα του IP πακέτου μένει απροστάτευτη, έτσι πληροφορίες όπως διευθύνσεις αποστολέα – παραλήπτη είναι ορατές. Η υπηρεσία αυθεντικοποίησης είναι προαιρετική και εφαρμόζεται και αυτή στα δεδομένα του πακέτου και όχι στην IP κεφαλίδα. Η ESP κεφαλίδα εισάγεται μετά την IP κεφαλίδα, ενώ το ESP trailer (padding, padding length , Next Header) εισάγεται στο τέλος του IP πακέτου. Σε περίπτωση αυθεντικοποίησης τα αυθεντικοποιημένα δεδομένα τοποθετούνται μετά τον ESP trailer [15].



Εικόνα 8.7: Encryption in Transport Mode

Στην tunnel mode (Εικόνα 8.8) λειτουργία το IP πακέτο ενθυλακώνεται σε ένα άλλο πακέτο. Έτσι κρυπτογραφείται ολόκληρο το εσωτερικό (αρχικό) πακέτο, το οποίο αποτελεί ωφέλιμο φορτίο του εξωτερικού (νέου) πακέτου. Σε αυτή την περίπτωση οι διευθύνσεις αποστολέα και παραλήπτη είναι κρυπτογραφημένες κατά την διάρκεια μεταφοράς του πακέτου μεταξύ δύο IP gateways. Όπως και στην περίπτωση της λειτουργίας transport mode, η ESP κεφαλίδα εισάγεται μετά τη νέα IP κεφαλίδα, το ESP trailer εισάγεται στο τέλους του αρχικού – εσωτερικού πακέτου, ενώ αν εφαρμόζεται αυθεντικοποίηση, τα αυθεντικοποιημένα δεδομένα τοποθετούνται μετά τον ESP trailer [15].



Εικόνα 8.8: Encryption in Tunnel Mode

8.4 Key Management

Οι παραπάνω λειτουργίες που προσφέρουν τα AH και ESP, προϋποθέτουν την χρήση κρυπτογραφικών αλγορίθμων. Η διαδικασία της κρυπτογράφησης απαιτεί τον προσδιορισμό και την διανομή κάποιων μυστικών κλειδιών. Η αρχιτεκτονική που περιγράφεται στην τεκμηρίωση του IPsec επιβάλλει την υποστήριξη δύο τρόπων διαχείρισης κλειδιών [15]:

- **Manual:** Ο διαχειριστής διαμορφώνει χειροκίνητα κάθε σύστημα με τα κλειδιά του και με τα κλειδιά των άλλων συστημάτων που επικοινωνούν με αυτό. Αυτός ο τρόπος διαχείρισης κλειδιών είναι πρακτικός για μικρής κλίμακας IP δίκτυα.

- **Automated:** Μετά από απαίτηση των κόμβων, ένα αυτόματο σύστημα δημιουργεί κλειδιά για τις SA. Ιδανικός τρόπος για μεγάλα κατανεμημένα συστήματα.

Το προεπιλεγμένο πρωτόκολλο αυτόματης διαχείρισης κλειδιών για το IPsec ονομάζεται ISAKMP/Oakley.

8.4.1 Πρωτόκολλο προσδιορισμού κλειδιών Oakley

Το Oakley είναι ένα πρωτόκολλο ανταλλαγής κλειδιών που βασίζεται στον αλγόριθμο Diffie-Hellman[26], αλλά παρέχει μεγαλύτερη ασφάλεια. Επίσης, είναι γενικό και δεν υπαγορεύει κάποια συγκεκριμένη διαμόρφωση. 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.

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. 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 (man-in-the-middle) 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 πρώτη επίθεση χρησιμοποιείται ο μηχανισμός cookies και στη δεύτερη πραγματοποιείται πιστοποίηση ανταλλαγής μηνυμάτων.

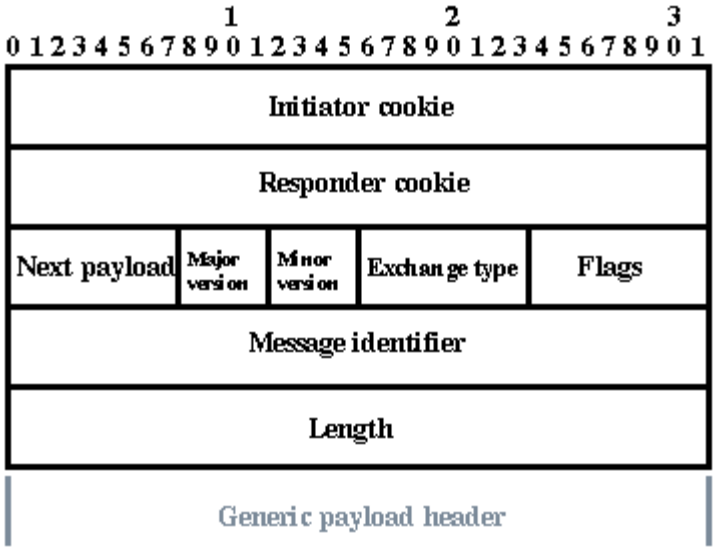
8.4.2 Πρωτόκολλο διαχείρισης συσχετίσεων ασφάλειας Διαδικτύου και κλειδιών (Internet SecurityAssociation and Key Management Protocol, ISAKMP)

Στο 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 επικοινωνιών που γίνονται μέσω του διαδικτύου. Το ISAKMP ορίζει συγκεκριμένες διαδικασίες και τύπους πακέτων για την διαπραγμάτευση, τροποποίηση και διαγραφή των SA. Το SA περιέχει όλη την απαιτούμενη πληροφορία για την εκτέλεση υπηρεσιών ασφαλείας δικτύου. 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

[26] Ο πρώτος αλγόριθμος για ασύμμετρο κρυπτοσύστημα δημοσιεύτηκε στην εργασία των Diffie-Hellman που όριζε την κρυπτογραφία με ασύμμετρο κρυπτοσύστημα και είναι γνωστός ως ανταλλαγή κλειδιών κατά Diffie-Hellman. Σκοπός του αλγορίθμου είναι να καταστήσει εφικτή και ασφαλή μεταξύ δύο χρηστών την ανταλλαγή ενός μυστικού κλειδιού, το οποίο ακολούθως θα χρησιμοποιηθεί για κρυπτογράφηση μηνυμάτων. Ο αλγόριθμος περιορίζεται ακριβώς στην ανταλλαγή των κλειδιών [16].

άλλα πρωτόκολλα εγκαθίδρυσης κλειδιών όπως το Oakley που περιγράψαμε στην προηγούμενη ενότητα.

Το ISAKMP εισάγει την έννοια του “cookie” , προκειμένου να αποτρέψει επιθέσεις τύπου clogging, όπως αναφέραμε στο Oakley, 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. Στην Εικόνα 8.9 φαίνεται η δομή της κεφαλίδας ISAKMP.



Εικόνα 8.9: ISAKMP Header

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.

8.4.3 Πρωτόκολλο Ανταλλαγής Κλειδιών (Internet Key Exchange, IKE)

Το Internet Key Exchange (IKE) αποτελεί επέκταση των παραπάνω πρωτοκόλλων που περιγράψαμε και δημιουργεί ένα 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. Σχεδιάστηκε για την υποστήριξη

αυτοματοποιημένων διαπραγματεύσεων των SA και αυτοματοποιημένης δημιουργίας και ανανέωσης κρυπτογραφικών κλειδιών. Η IETF αρχικά πρότεινε το IKEv1 το οποίο αναλύεται στο RFC 2409 και αργότερα ανανεώθηκε από το RFC 4109. Οι αλλαγές έγιναν έτσι ώστε να διασφαλιστεί ότι οι προτεινόμενοι αλγόριθμοι αντικατοπτρίζουν την τρέχουσα κατάσταση.

Το IKEv1 έχει δύο φάσεις:

1. Οι κόμβοι που επιθυμούν να επικοινωνήσουν με ασφαλή τρόπο, διαπραγματεύονται ένα ασφαλές κανάλι επικοινωνίας που λέγεται ISAKMP SA. Η φάση αυτή βασίζεται στον αλγόριθμό Diffie – Hellman. Η αυθεντικοποίηση γίνεται είτε με προ-μοιρασμένα κλειδιά είτε με το δημόσιο κλειδί του παραλήπτη.
2. Οι κρυπτογραφικοί αλγόριθμοι και τα κλειδιά μπορούν να σταλούν μέσω του ασφαλούς καναλιού. Το αποτέλεσμα της δεύτερης αυτής φάσης είναι η δημιουργία μιας IPsec SA.

Το IKEv2 αναλύεται στο RFC 4306.

Στην αρχική ανταλλαγή (πρώτη φάση για το IKEv1) ανταλλάσσονται δυο ζευγάρια μηνυμάτων:

1. Διαπραγμάτευση κρυπτογραφικών αλγόριθμων και nonces (μεγάλοι τυχαίοι αριθμοί).
2. Αυθεντικοποίηση του πρώτου μηνύματος ανταλλάσοντας πιστοποιητικά.

Μια χαρακτηριστική διαφορά ανάμεσα στις δυο εκδοχές του IKE είναι ότι στο IKEv1 η διάρκεια ζωής μιας SA είχε προκαθοριστεί. Στο IKEv2 κάθε άκρο της SA είναι υπεύθυνο για την εφαρμογή δικής του διάρκειας ζωής στην SA. Το άκρο με τη μικρότερη διάρκεια ζωής είναι υπεύθυνο να ζητήσει ξανά έκδοση κλειδιού αφού οι πολιτικές διάρκειας ζωής των δυο άκρων είναι διαφορετικές. Το IKE διαπραγματεύεται απευθείας τις Συσχετίσεις Ασφαλείας (SA) του IPsec και δίνει την δυνατότητα στο IPsec για ασφαλείς επικοινωνίες χωρίς προ-ρυθμίσεις κάτι που θα επιβάρυνε με επιπλέον κόστος. Πιο συγκεκριμένα το IKE προσφέρει:

- Καταργεί την ανάγκη χειροκίνητης ρύθμισης όλων των IPsec παραμέτρων ασφαλείας και στις δύο οντότητες που επικοινωνούν.
- Επιτρέπει τον καθορισμό της διάρκειας ζωής της Συσχέτισης Ασφάλειας του IPsec.
- Επιτρέπει την αλλαγή των κλειδιών κρυπτογράφησης κατά την διάρκεια των διαπραγματεύσεων στο IPsec.
- 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 αυθεντικοποίηση 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 οι μηχανές έχουν αυθεντικοποιηθεί.

- **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, 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):** Κάθε μηχανή παράγει έναν ψευδοτυχαίο 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 οτιδήποτε λαμβάνουν από το συνομιλητή τους. Υποστηρίζεται μόνο ο αλγόριθμος δημοσίων κλειδιών RSA.

Η αποτελεσματικότητα μιας κρυπτογραφικής λύσης εξαρτάται περισσότερο από την ασφαλή μετάδοση του κλειδιού παρά από την επιλογή του αλγορίθμου. Έτσι, το IETF IPSec Working Group έχει περιγράψει μια σειρά από ιδιαίτερα ανθεκτικά πρωτόκολλα ανταλλαγής Oakley που χρησιμοποιούνται στο IKE. Αυτά χρησιμοποιούν μια προσέγγιση δύο φάσεων:

1. Στην πρώτη φάση μετά από μια σειρά από διαπραγματεύσεις εγκαθίσταται ένα master κλειδί, από το οποίο θα παράγονται όλα τα υπόλοιπα κρυπτογραφικά κλειδιά. Στην γενικότερη περίπτωση αυτό το κλειδί θα πραγματοποιήσει μια ασφαλή σύνδεση πάνω στην οποία θα μεταδίδονται τα μηνύματα του IKE.
2. Η δεύτερη φάση είναι η ανταλλαγή των μηνυμάτων, αφού πρώτα γίνει η ασφαλής σύνδεση από την πρώτη φάση, για την παραγωγή των κλειδιών με τα οποία θα εξασφαλιστεί η ασφαλής επικοινωνία των δεδομένων.

8.5 Τρόποι υλοποίησης IPsec αρχιτεκτονικής

Υπάρχουν αρκετοί πιθανοί τρόποι υλοποίησης μιας IPsec αρχιτεκτονικής [4]. Το IPsec μπορεί να υλοποιηθεί ως μέρος της IPv6 στοίβας. Αυτή η προσέγγιση υποδηλώνει πλήρη υποστήριξη για την κεφαλίδα ασφάλειας του IP, η οποία ενσωματώνεται στην στοίβα πρωτοκόλλου IP. Αυτή η ενσωμάτωση καθιστά το IPsec τμήμα ζωτικής σημασίας για την υλοποίηση του IP πρωτοκόλλου και απαιτεί την συνεχή αναβάθμιση (λογισμικού και υλικού) ολόκληρης της στοίβας πρωτοκόλλου, που έχει ως αποτέλεσμα την εμφάνιση αρκετών ελαττωμάτων [4].

Μια άλλη προσέγγιση αναπαριστά την υλοποίηση του IPsec ως "bump in the stack" (BITS). Αυτή η μέθοδος εμπλέκει την εισαγωγή του κώδικα λογισμικού του IPsec μέσα στην στοίβα πρωτοκόλλου, κάτω από το υπάρχον λογισμικό του επιπέδου δικτύου και πάνω από το υπάρχον λογισμικό του επιπέδου συνδέσμου μετάδοσης δεδομένων[27]. Αυτός ο κώδικας

[27] Αναφέρεται και ως επίπεδο ζεύξης δεδομένων

λογισμικού που εισάγεται στην στοίβα, υποκλέπτει πακέτα από το επίπεδο δικτύου και εκτελεί μηχανισμούς ασφάλειας πάνω σε αυτά, πριν τα προωθήσει στο επίπεδο συνδέσμου μετάδοσης δεδομένων. Ένα μεγάλο πλεονέκτημα αυτής της προσέγγισης είναι η πιθανότητα υλοποίησης του IPsec χωρίς την ανάγκη επαναπρογραμματισμού του κώδικα λογισμικού της IP στοίβας [4].

Τέλος, η αρχιτεκτονική IPsec μπορεί να υλοποιηθεί και ως “bump in the wire” (BITW). Αυτή η μέθοδος υποδηλώνει την χρήση υλικού (hardware) για έλεγχο της ασφάλειας. Η εξωτερική συσκευή (υλικό) συνήθως δρα σαν μια IP security gateway για όλα τα πακέτα που προορίζονται στον υπολογιστή/σύστημα, ο οποίος είναι συνδεδεμένος με αυτή την συσκευή. Η προσέγγιση BITW είναι παρόμοια με την BITS όταν χρησιμοποιείται για την προστασία ενός μόνο υπολογιστή/συστήματος, αλλά με την μέθοδο BITW είναι δυνατή η παροχή προστασίας σε πολλαπλούς υπολογιστές/συστήματα μέσω μιας μόνο BITW συσκευής. Αυτό αποτελεί σημαντικό πλεονέκτημα έναντι της προσέγγισης BITS [4].

8.6 Απειλές και Επιθέσεις στο IPsec

Το IPsec παρόλο που παρέχει σημαντική προστασία μέσω των κεφαλίδων AH και ESP (διασφάλιση αυθεντικότητας, ακεραιότητας και εμπιστευτικότητας μηνυμάτων), παρουσιάζει ορισμένες ευπάθειες, τις οποίες μπορούν να εκμεταλλευτούν οι επιτιθέμενοι.

Οι δύο λειτουργίες του IPsec (transport mode και tunnel mode) στο IPv6, απαιτούν μια διαδικασία ανταλλαγής μυστικού κλειδιού, ώστε τα μηνύματα να μπορούν να κρυπτογραφηθούν και υπογραφούν. Έτσι, ένας αντίπαλος μπορεί να στρέψει την προσοχή του στην επίτευξη μιας επίθεσης απόκτησης αυτού του μυστικού κλειδιού. Παρόλο που μια τέτοια επίθεση είναι ιδιαίτερα δύσκολη και επίπονη να επιτευχθεί υπάρχει πιθανότητα να συμβεί, και από την στιγμή που ένας επιτιθέμενος αποκτήσει το μυστικό κλειδί μπορεί να προσπελάσει την ασφαλή επικοινωνία που υφίσταται μεταξύ των δύο οντοτήτων, χωρίς αυτές να αντιληφθούν κάτι. Με την απόκτηση του μυστικού κλειδιού, ο επιτιθέμενος μπορεί να αποκρυπτογραφήσει ή και να τροποποιήσει το μήνυμα [34]. Επιπλέον, μπορεί να δημιουργήσει άλλα μυστικά κλειδιά και να αποκτήσει πρόσβαση σε άλλες ασφαλείς επικοινωνίες.

Επιπροσθέτως, όταν το IPsec κάνει χρήση της ESP κεφαλίδας, το firewall ενός συστήματος δεν μπορεί να επιθεωρήσει τα κρυπτογραφημένα δεδομένα, οπότε αν υπάρχει ενσωματωμένη μια απειλή, δεν μπορεί να γίνει αντιληπτή [34]. Ακόμα, η χρήση του IPsec μπορεί οδηγήσει σε μια νέα Denial of Service Attack. Η κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων ξοδεύει πολλούς πόρους της CPU ενός υπολογιστή/συστήματος. Έτσι, ένας επιτιθέμενος μπορεί να στέλνει συνεχώς κρυπτογραφημένα πακέτα, με φαινομενικά σωστά δεδομένα αλλά στην πραγματικότητα τυχαία άκυρα δεδομένα και να κατακλύζει την CPU ενός υπολογιστή/συστήματος, η οποία θα ξοδεύει χρόνο στην επεξεργασία αυτών των λανθασμένων δεδομένων και δεν θα ανταποκρίνεται σε άλλες νόμιμες αιτήσεις [34].

Το IPsec υστερεί σε visit control (έλεγχος επίσκεψης) [34]. Η λειτουργία του visit control είναι να προσδιορίσει και εξετάσει το ID του επισκέπτη. Χωρίς το visit control, οποιοσδήποτε μπορεί να αποκτήσει πρόσβαση σε όποιον υπολογιστή επιθυμεί και να προβεί σε κακόβουλες ενέργειες. Επιπλέον, στο IPsec όλες οι παράμετροι ασφάλειας που

χρησιμοποιούνται στην επικοινωνία, βρίσκονται σε μια συγκεκριμένη βάση δεδομένων, την λεγόμενη Security Association Database (SAD). Αν ο επιτιθέμενος καταφέρει να αποκτήσει πρόσβαση σε αυτή την βάση, θα αποκτήσει τις συσχετίσεις ασφάλειας (security associations) και κατά συνέπεια κρυφές πληροφορίες μεταξύ των οντοτήτων. Τέλος, ιδιαίτερη σημασία έχει ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται, καθώς κάποιοι αλγόριθμοι κρυπτογράφησης, όπως ο DES παρουσιάζουν αδυναμίες και είναι σχετικά εύκολο να “σπάσουν”.

9

Πρακτική Εφαρμογή IPsec

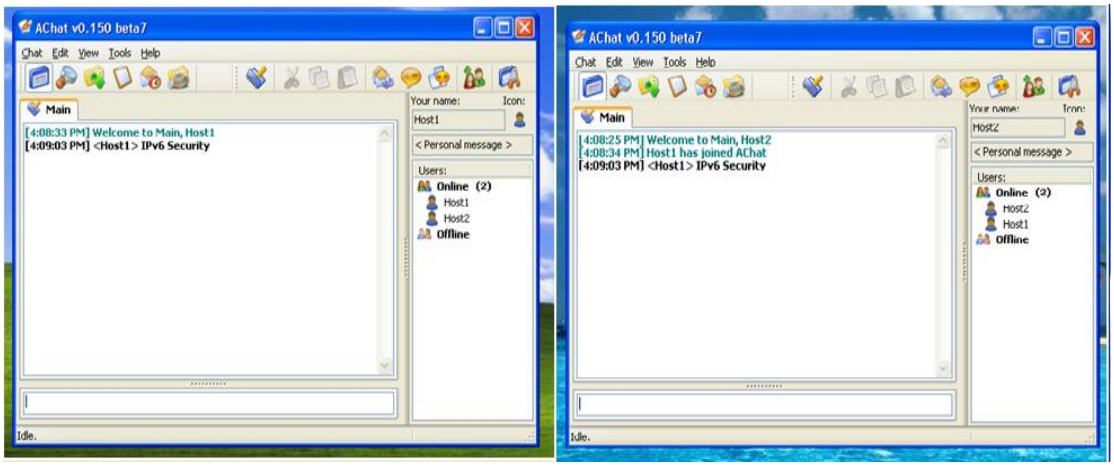
Για την εφαρμογή του IPsec σε ένα τοπικό δίκτυο έγινε χρήση δύο εικονικών υπολογιστών, οι οποίοι είχαν ως λειτουργικό σύστημα Windows XP (SP3). Στους δύο υπλογιστές εγκαταστάθηκε το Achat (v0.150 beta7) [54], το οποίο είναι ένα εργαλείο επικοινωνίας δικτύου. Επιπλέον, στους δύο υπολογιστές εγκαταστάθηκε η Java SE (7) πλατφόρμα . Επίσης στον πρώτο υπολογιστή έγινε εγκατάσταση του αναλυτή δικτυακής κίνησης Wireshark (1.8.5) (Πίνακας 1). Πρέπει να επισημανθεί ότι όλη η διαδικασία έγινε χειροκίνητα (manual), κάτι το οποίο είναι μη πρακτικό σε μεγάλης κλίμακας δίκτυα. Η συγκεκριμένη εφαρμογή έγινε για εκπαιδευτικούς σκοπούς και δεν μπορεί να εφαρμοστεί σε εταιρικά δίκτυα ή δίκτυα μεγάλων οργανισμών.

Πίνακας 1: Λεπτομέρειες για τους εικονικούς υπολογιστές

	Υπολογιστής 1	**Υπολογιστής 2**
Λειτουργικό Σύστημα	Windows XP	Windows XP
Εργαλείο Επικοινωνίας Δικτύου	Achat	Achat
Java SE πλατφόρμα	Έκδοση 7	Έκδοση 7
Αναλυτής Δικτυακής Κίνησης	Wireshark	-

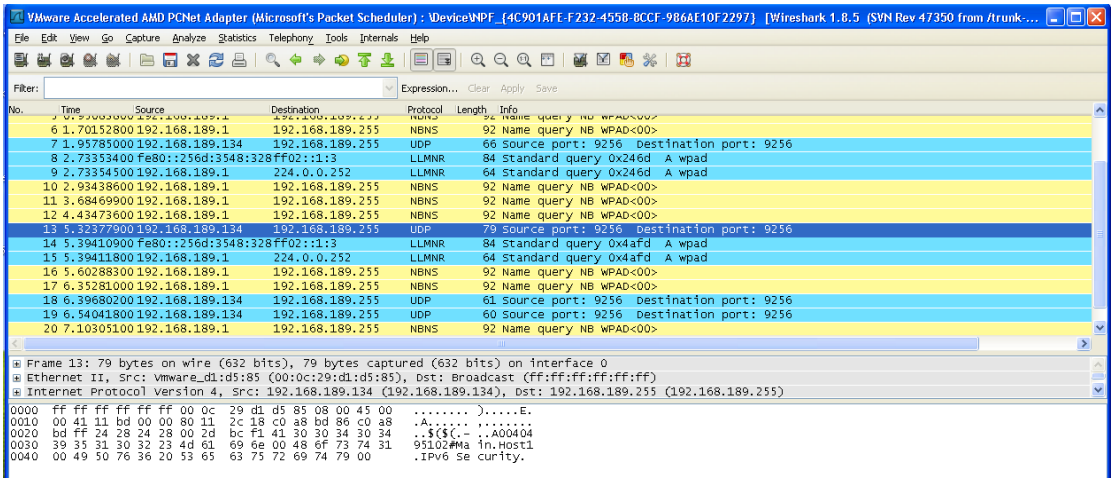
Στόχος είναι η αποστολή ενός μηνύματος από τον υπολογιστή1 στον υπολογιστή2 αρχικά χωρίς την χρήση IPsec. Στην συνέχεια επαναλαμβάνεται η ίδια διαδικασία, αυτή την φορά με χρήση IPsec. Στο τέλος συγκρίνονται τα αποτελέσματα των παραπάνω διαδικασιών.

Αρχικά στέλνουμε το μήνυμα "IPv6 Security" από τον υπολογιστή1 στον υπολογιστή2 μέσω του Achat (Εικόνα 9.1).



Εικόνα 9.1: Ανταλλαγή μηνύματος "IPv6 Security" μεταξύ δύο υπολογιστών μέσω Achat

Χρησιμοποιώντας το Wireshark καταφέρνουμε να υποκλέψουμε το συγκεκριμένο μήνυμα. Στο κάτω μέρος του παραθυρικού περιβάλλοντος του Wireshark, φαίνεται το μήνυμα “IPv6 Security” (Εικόνα 9.2).

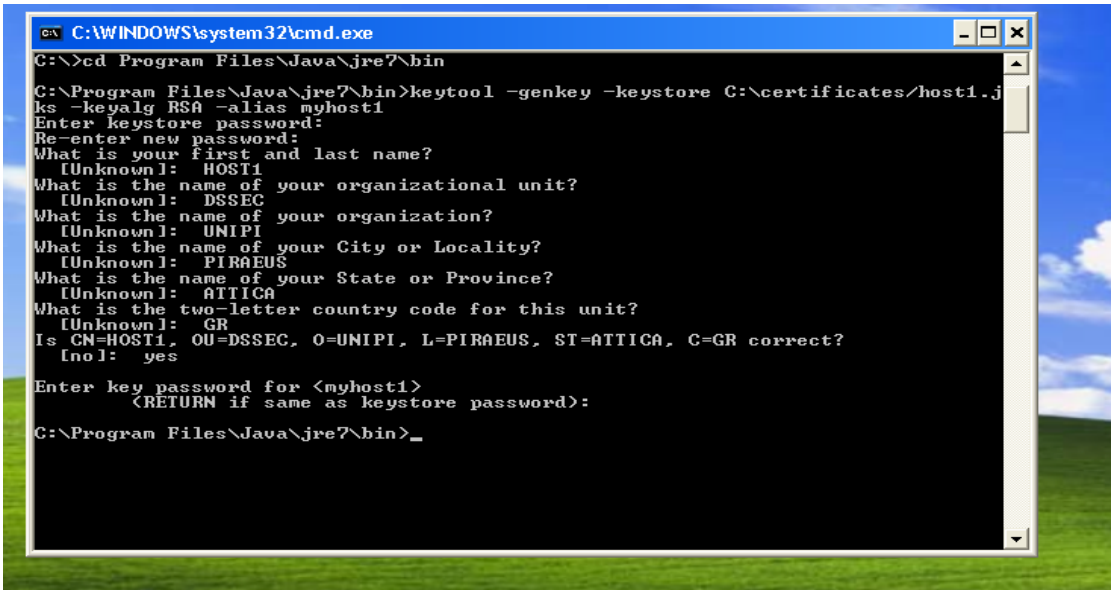


Εικόνα 9.2: Υποκλοπή μηνύματος μέσω Wireshark

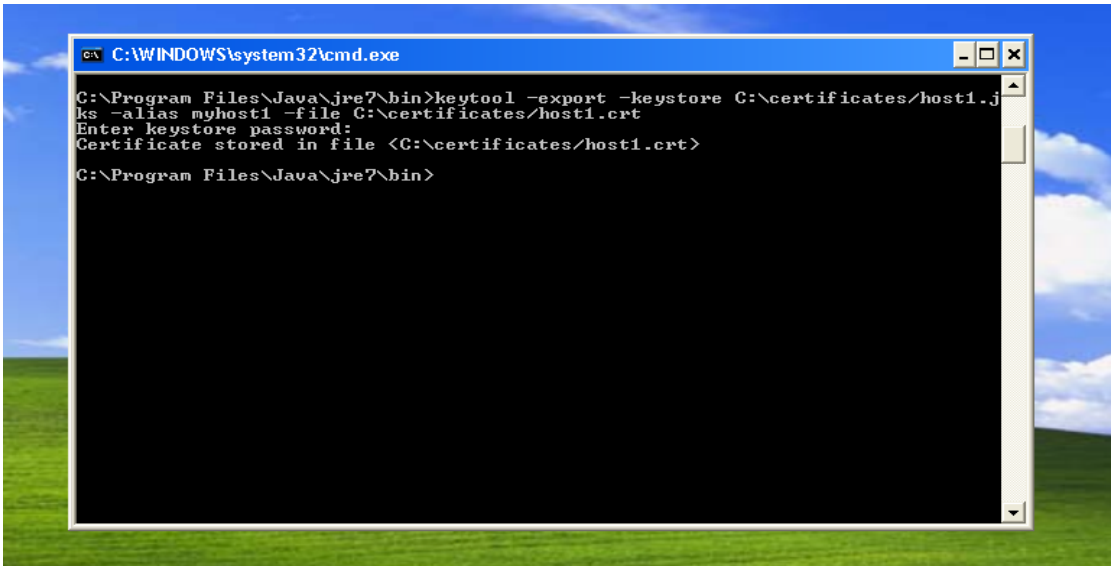
Στόχος μας είναι να προστατέψουμε την επικοινωνία μεταξύ των δύο υπολογιστών, γι’αυτό το λόγο θα εφαρμόσουμε το IPsec. Αρχικά, οι υπολογιστές θα πρέπει να αυθεντικοποιούνται μεταξύ τους, οπότε γίνεται χρήση πιστοποιητικών. Για την δημιουργία των πιστοποιητικών χρησιμοποιήσαμε ένα εργαλείο της java, το keytool. Η δημιουργία ενός πιστοποιητικού χωρίζεται σε δύο μέρη:

1. Δημιουργία του keystore.jks. Το keystore περιέχει όλα τα πιστοποιητικά που εμπιστεύεται μια οντότητα (υπολογιστής). Κάθε υπολογιστής θα πρέπει να έχει το δικό του keystore, δηλαδή μια αποθήκη για κλειδιά και πιστοποιητικά που θα χρησιμοποιηθούν για την αυθεντικοποίηση των υπολογιστών. Μέσω της εντολής *C:\Program Files\Java\jre7\bin>keytool -genkey -keystore C:\certificates/host1.jks -keyalg RSA -alias myhost1* δημιουργούμε το keystore για τον υπολογιστή1 με όνομα host1.jks (Εικόνα 9.3).

2. Δημιουργία του πιστοποιητικού (certificate.crt) από το keystore.jks. Η εντολή που χρησιμοποιούμε είναι *C:\Program Files\Java\jre7\bin>keytool -export –keystore C:\certificates/host1.jks -alias myhost1 -file C:\certificates/host1.crt* (Εικόνα 9.4).

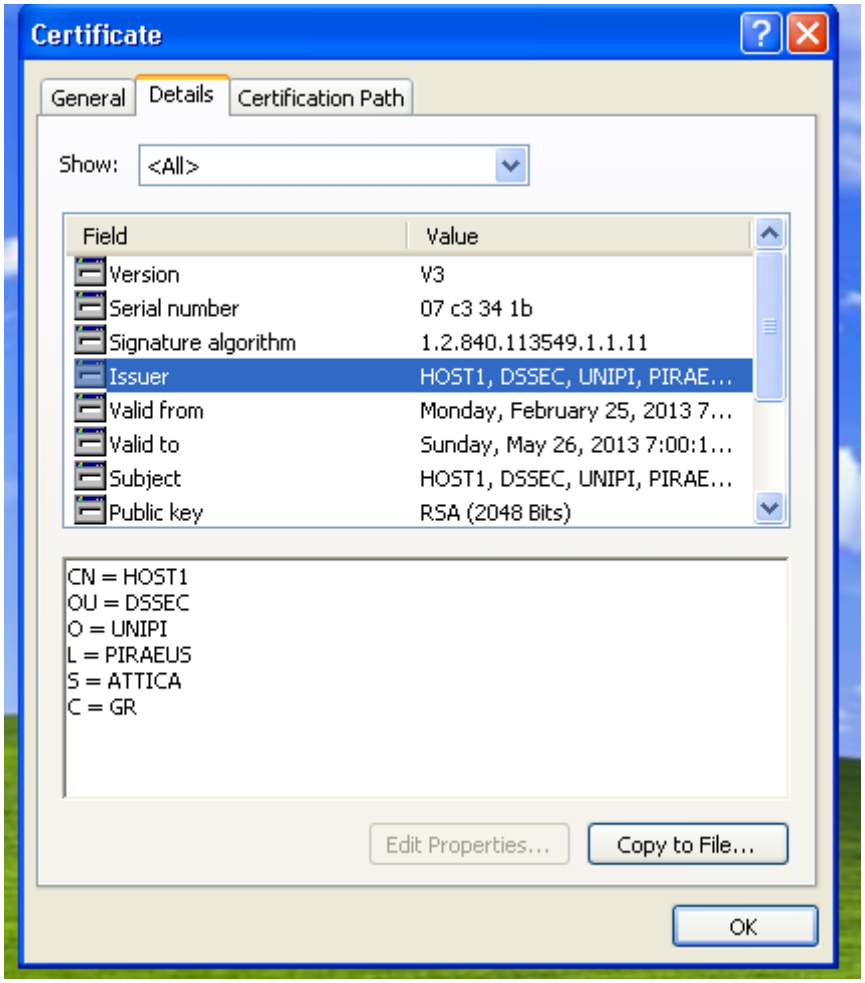


Εικόνα 9.3: Δημιουργία keystore για υπολογιστή1 με όνομα host1.jks



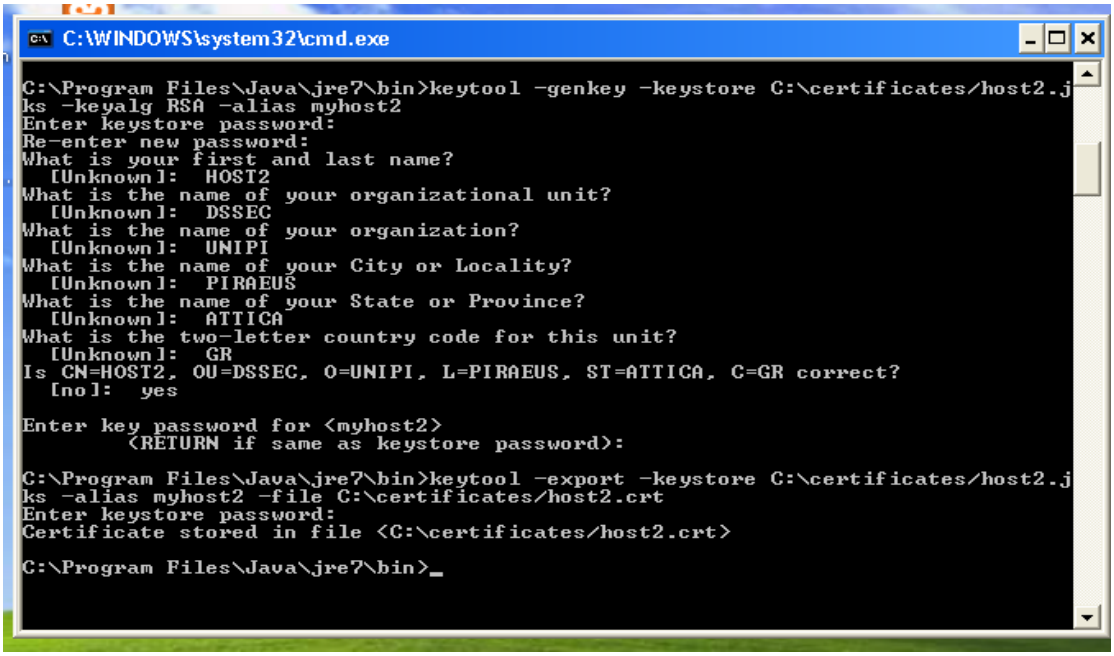
Εικόνα 9.4: Δημιουργία πιστοποιητικού host1.crt για τον υπολογιστή1

Στην Εικόνα 9.5 φαίνεται το πιστοποιητικό του υπολογιστή1 σε περιβάλλον Windows.



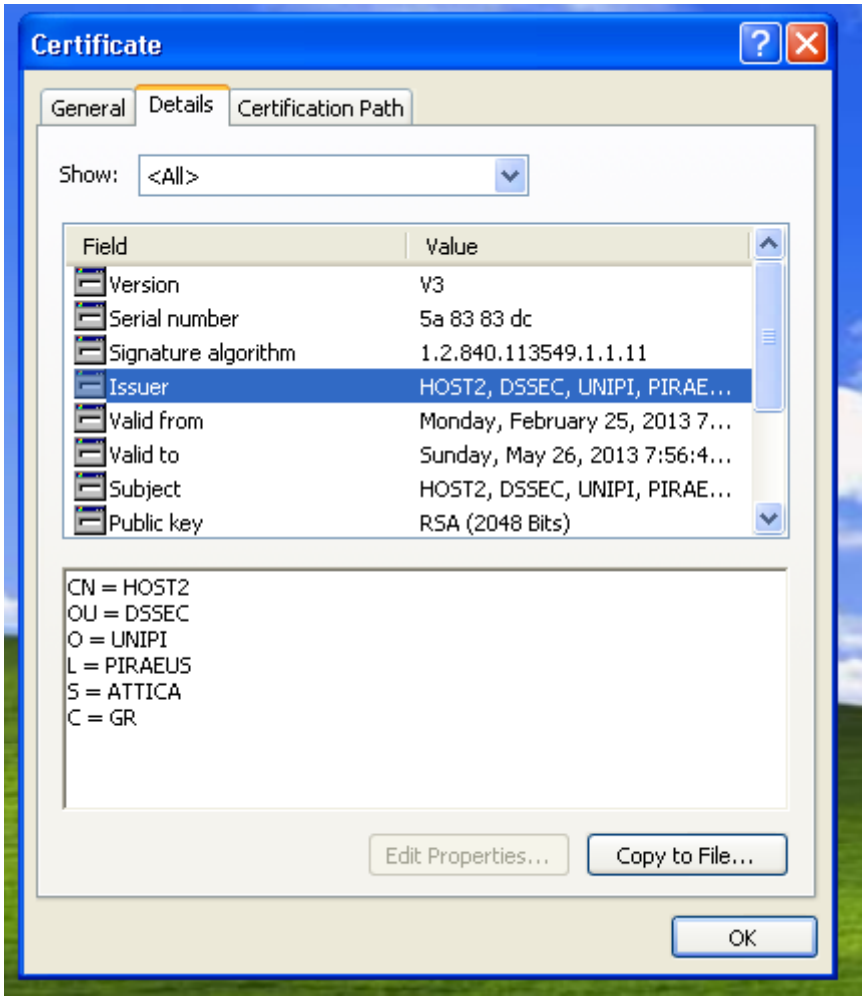
Εικόνα 9.5: Πιστοποιητικό του host1

Με τον ίδιο τρόπο δημιουργούμε keystore και πιστοποιητικό για τον host2 (Εικόνα 9.6).



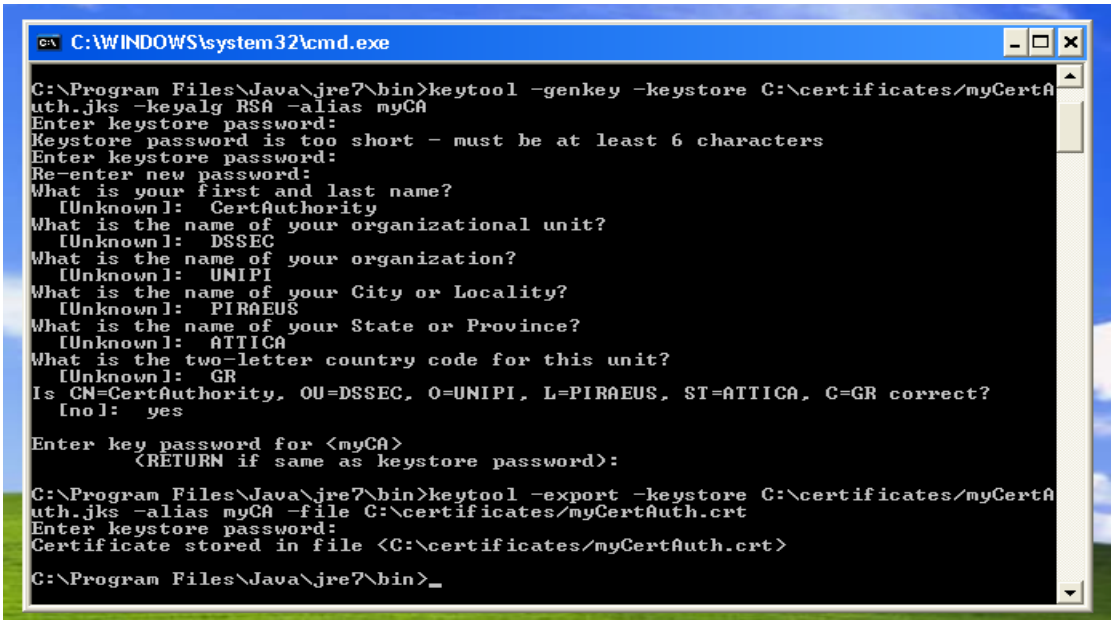
Εικόνα 9.6: Δημιουργία keystore και πιστοποιητικού για τον host2

Παρακάτω φαίνεται το πιστοποιητικό του υπολογιστή2 σε περιβάλλον Windows (Εικόνα 9.7).

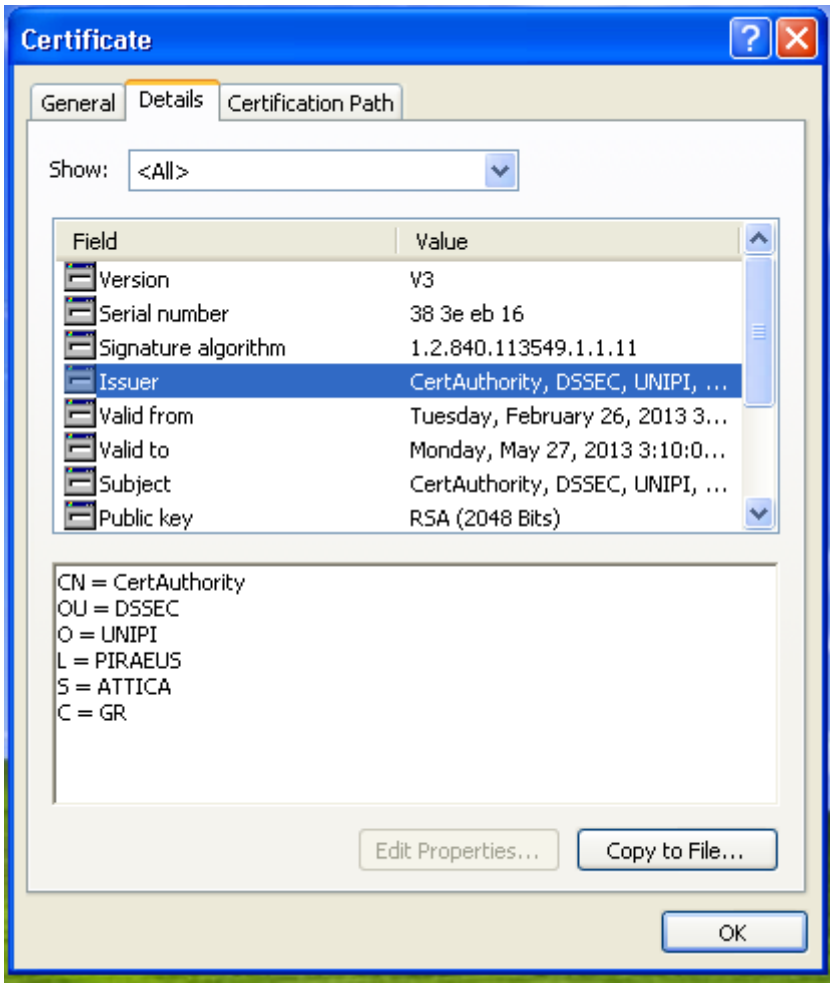


Εικόνα 9.7: Πιστοποιητικό host2

Επιπλέον δημιουργούμε keystore και πιστοποιητικό για την Certification Authority (Εικόνα 9.8). Στην Εικόνα 9.9 φαίνεται το πιστοποιητικό της Certification Authority.

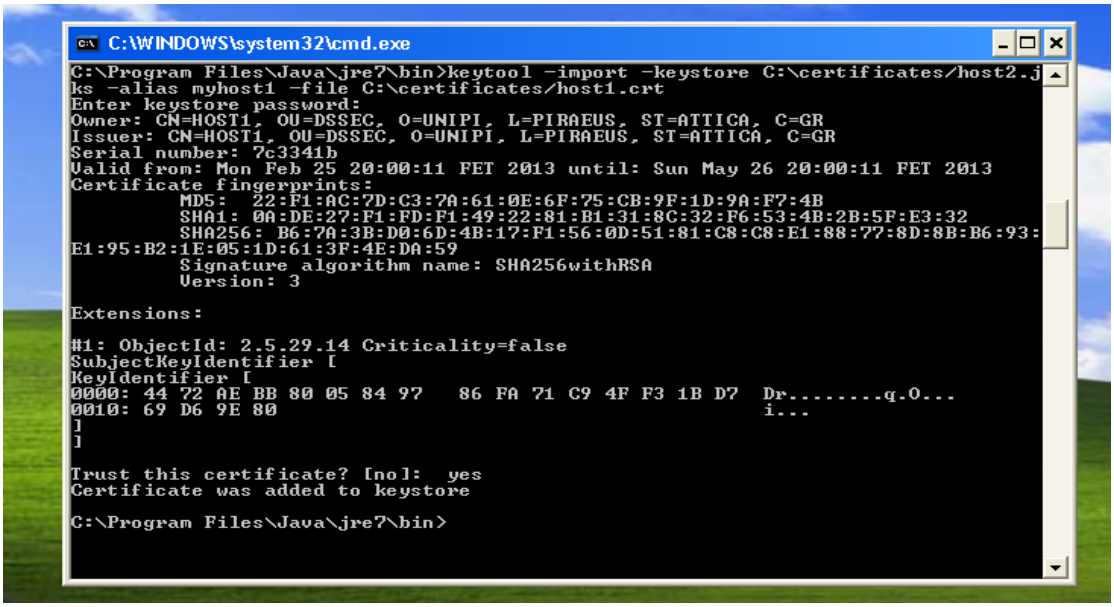


Εικόνα 9.8: Δημιουργία keystore και πιστοποιητικού για την Certification Authority

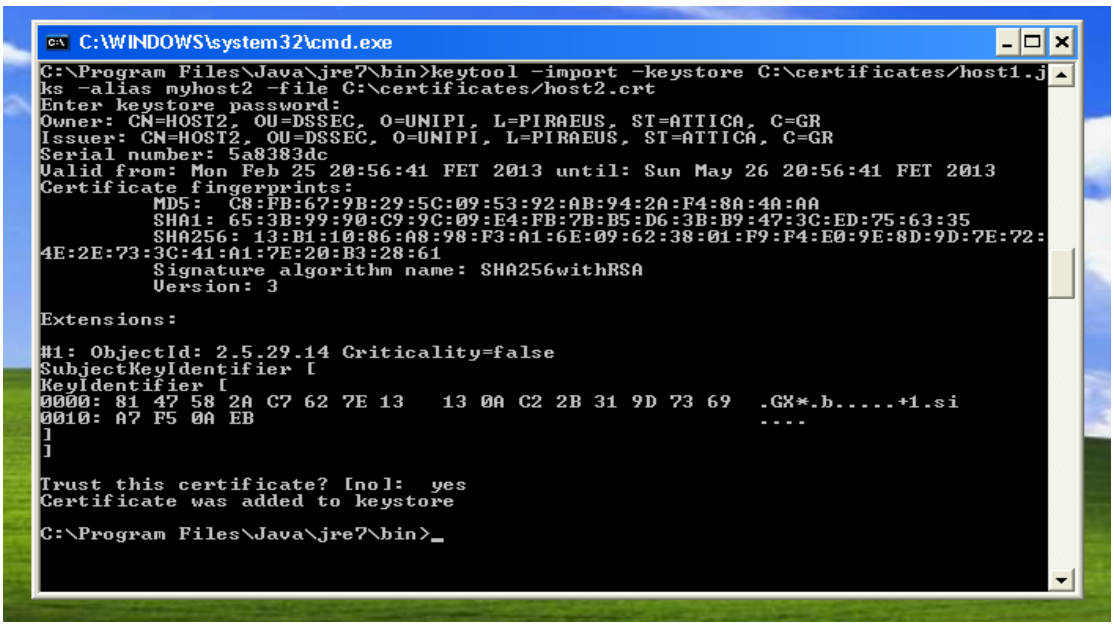


Εικόνα 9.9: Πιστοποιητικό Certification Authority

Όταν ολοκληρωθεί η διαδικασία δημιουργίας keystore και πιστοποιητικών για κάθε οντότητα, θα πρέπει να εισάγουμε σε κάθε keystore, τα πιστοποιητικά που εμπιστεύεται η κάθε οντότητα. Για να εισάγουμε το πιστοποιητικού του host2 στο keystore του host1 χρησιμοποιούμε την εντολή *C:\Program Files\Java\jre7\bin>keytool -import -keystore C:\certificates/host1.jks -alias myhost2 -file C:\certificates/host2.crt* (Εικόνα 9.10, 9.11).

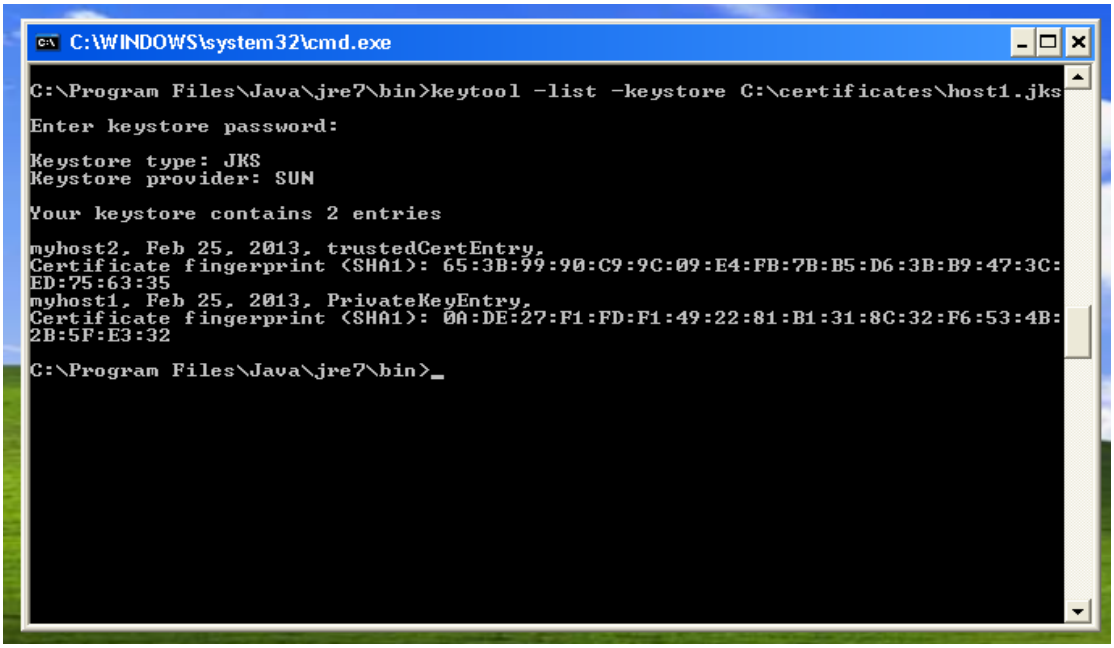


Εικόνα 9.10: Εισαγωγή του πιστοποιητικού του host2 στο keystore του host1



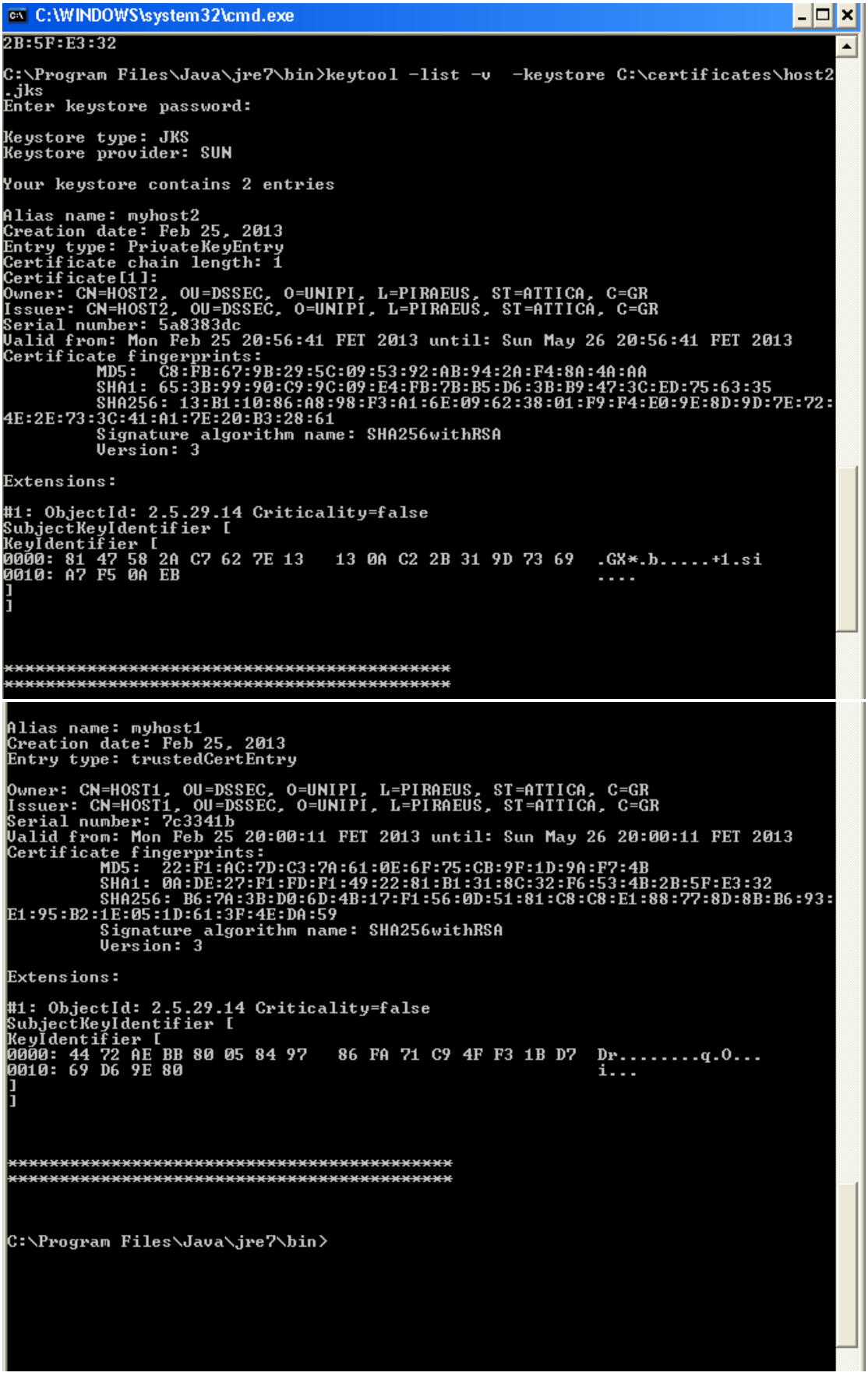
Εικόνα 9.11: Εισαγωγή του πιστοποιητικού του host1 στο keystore του host2

Με την εντολή *C:\Program Files\Java\jre7\bin>keytool -list -keystore C:\certificates/host1.jks* μπορούμε να δούμε το περιεχόμενο του keystore του host1 (Εικόνα 9.12).



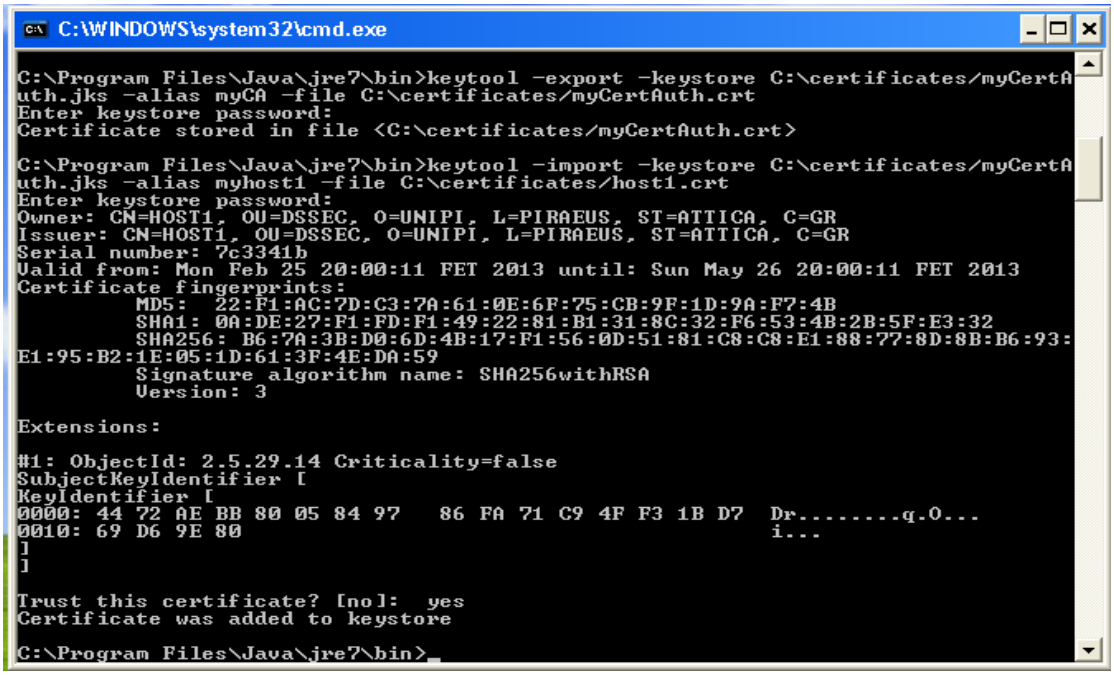
Εικόνα 9.12: Περιεχόμενα keystore του host1

Με την εντολή *C:\Program Files\Java\jre7\bin>keytool -list -v -keystore C:\certificates/host2.jks* παίρνουμε τα περιεχόμενα του keystore του host2 σε ποιο αναλυτική μορφή (Εικόνα 9.13).

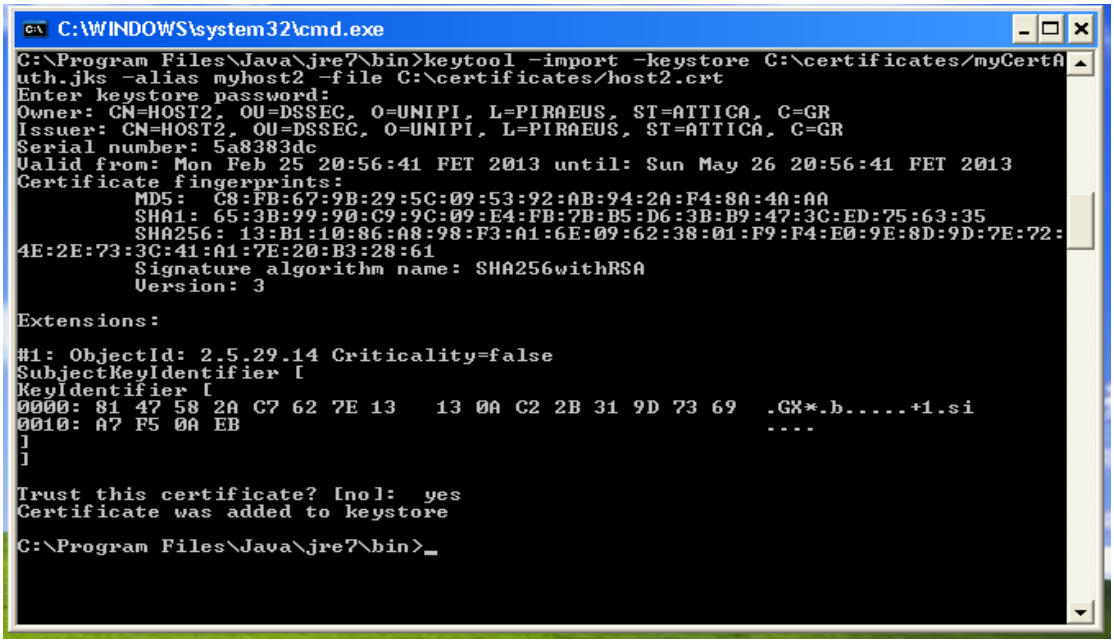


Εικόνα 9.13: Περιεχόμενα keystore του host2 σε πιο αναλυτική μορφή

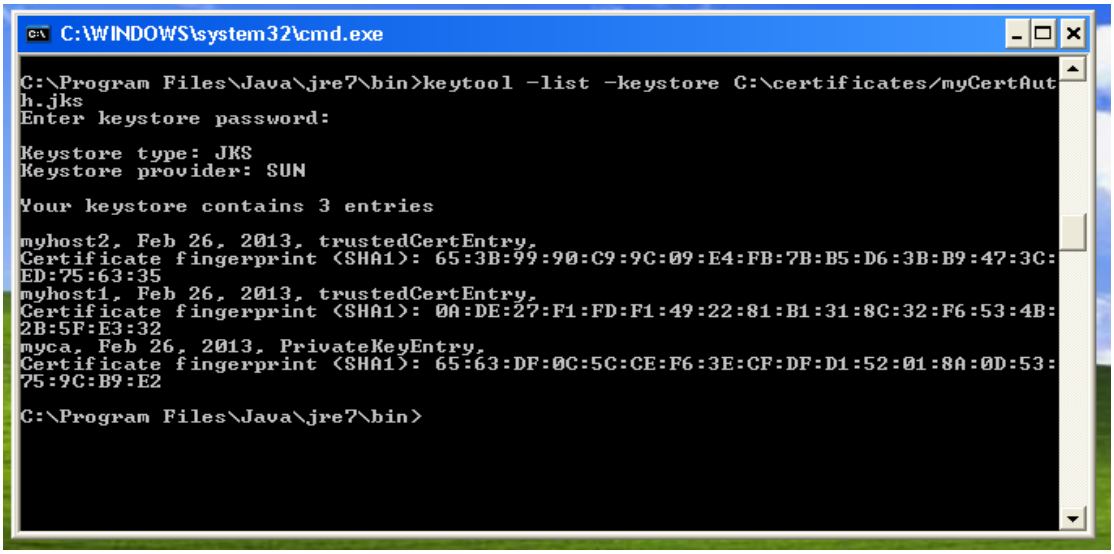
Επιπλέον, πρέπει να εισάγουμε το πιστοποιητικό του host1 και host2 στο keystore της Certificate Authority (Εικόνα 9.14, 9.15). Στην Εικόνα 9.16 φαίνονται τα περιεχόμενα keystore της CA.



Εικόνα 9.14: Εισαγωγή πιστοποιητικού host1 στο keystore της CA

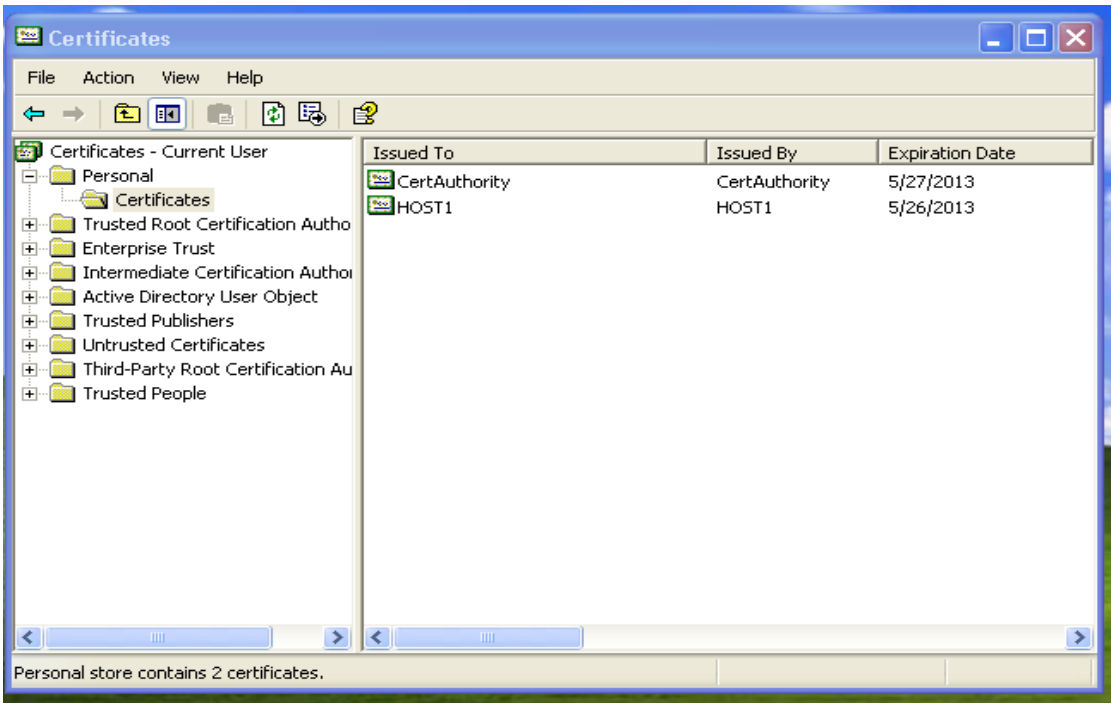


Εικόνα 9.15: Εισαγωγή πιστοποιητικού host2 στο keystore της CA

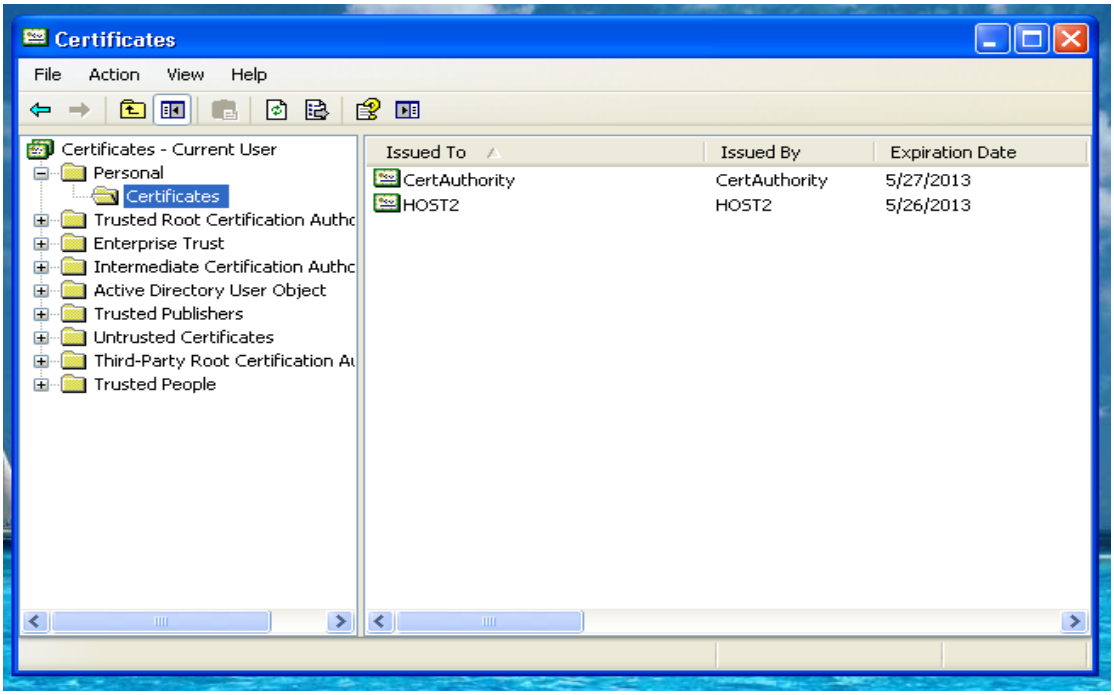


Εικόνα 9.16: Περιεχόμενα keystore της Certificate Authority

Όσα περισσότερα πιστοποιητικά περιέχει ένα keystore μιας οντότητας, τόσο πιο ψηλά είναι στην ιεραρχία. Μια Certification Authority είναι η ρίζα της ιεραρχίας και περιέχει όλα τα πιστοποιητικά των οντοτήτων που βρίσκονται κάτω από αυτή. Αφού έχουμε δημιουργήσει τα πιστοποιητικά των δυο οντοτήτων που θα επικοινωνήσουν και της Certification Authority, πρέπει να δημιουργήσουμε μια πολιτική ασφαλείας που θα τα χρησιμοποιήσει για αυθεντικοποίηση.

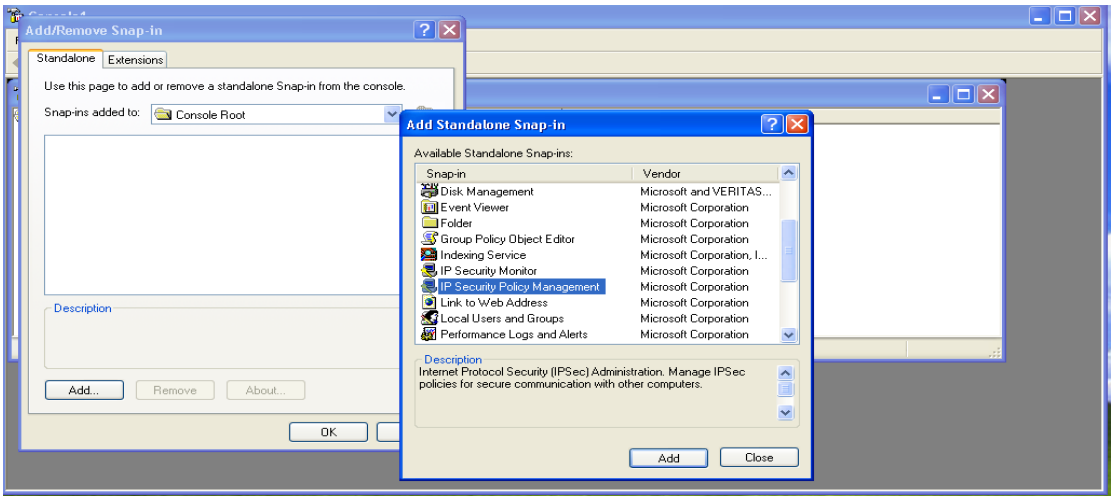


Εικόνα 9.17: Εισαγωγή πιστοποιητικών host1 και CA στον υπολογιστή1

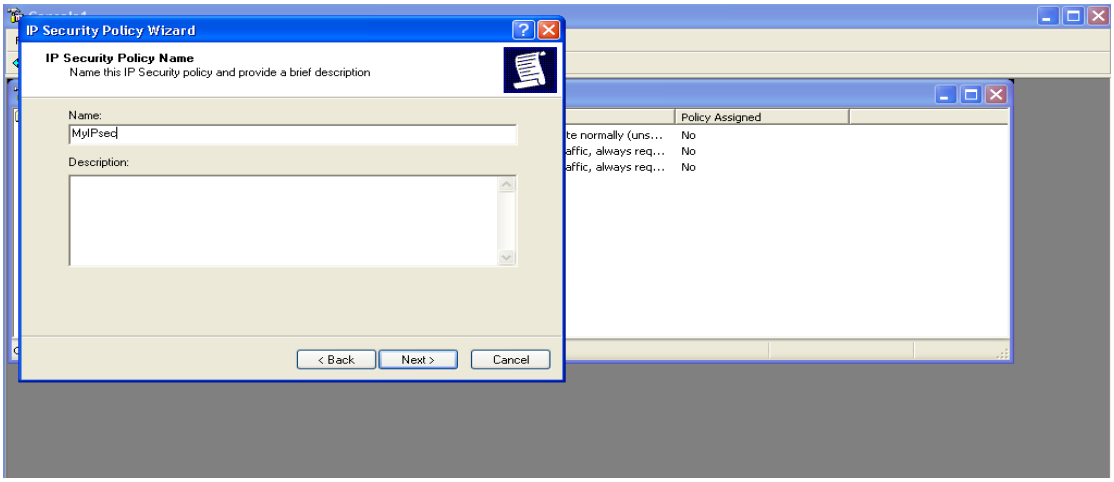


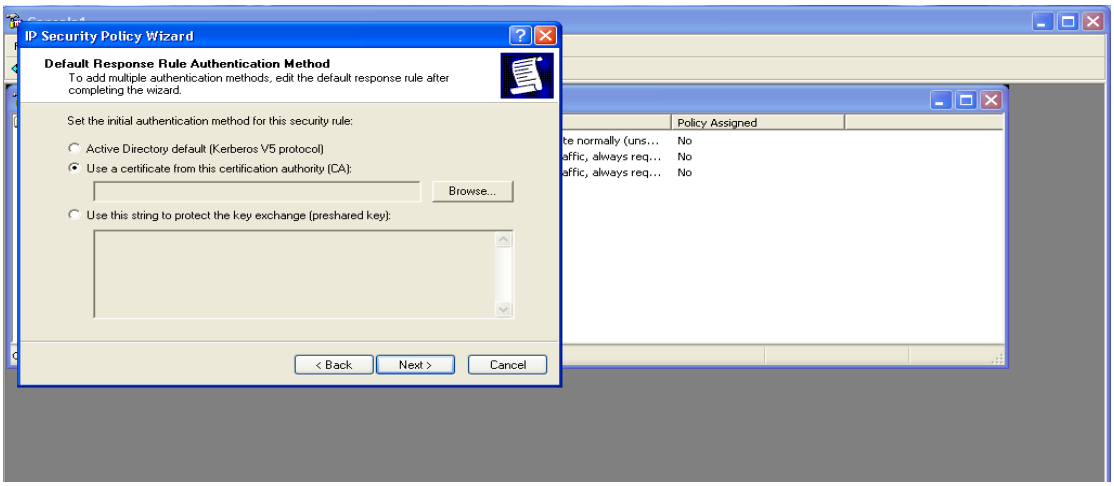
Εικόνα 9.18: Εισαγωγή πιστοποιητικών host2 και CA στον υπολογιστή2

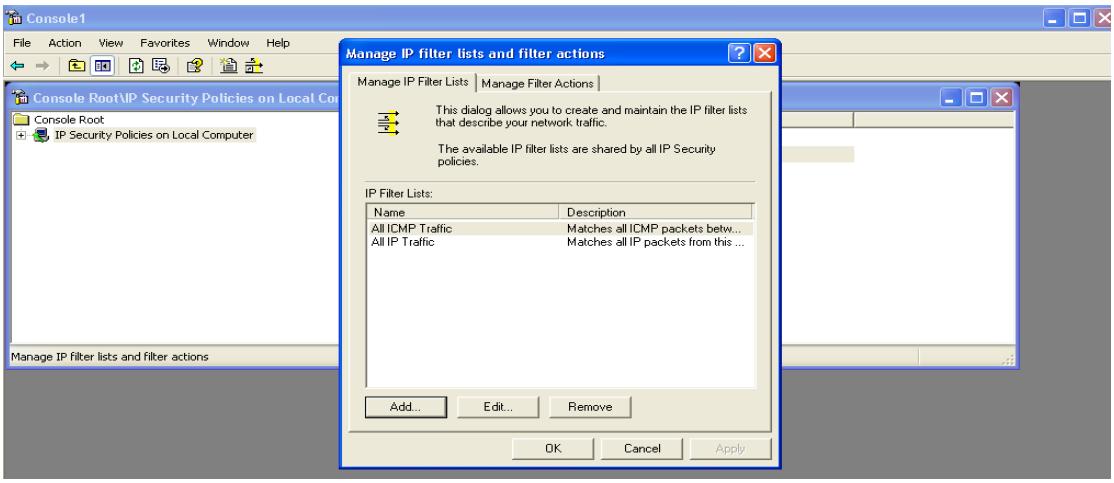
Στην συνέχεια δημιουργούμε μια πολιτικής ασφάλειας στα windows. Την ίδια πολιτική εφαρμόζουμε και στους δύο υπολογιστές (Εικόνα 9.19).

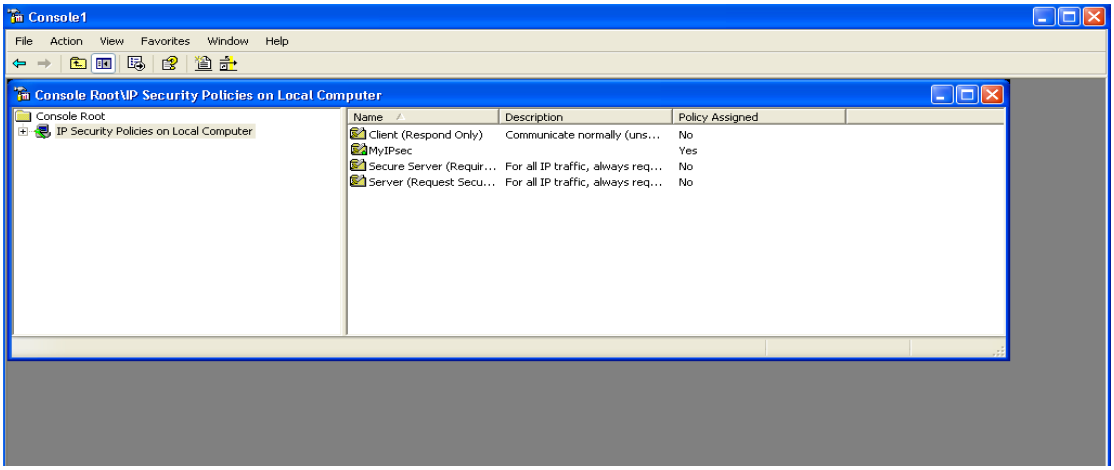


Εικόνα 9.19: Δημιουργία πολιτικής ασφάλειας

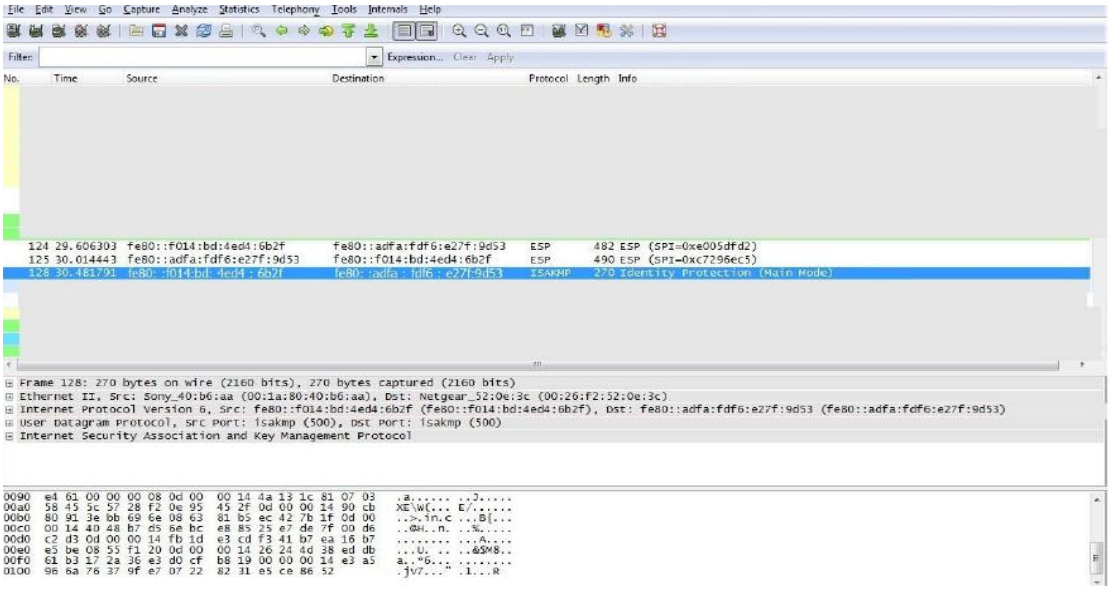

IP Security Policy Wizard
IP Security Policy Name
Name this IP Security policy and provide a brief description
Name:
MyIPsec
Description:
< Back
Next >
Cancel
Policy Assigned
No
No
No


IP Security Policy Wizard
Default Response Rule Authentication Method
To add multiple authentication methods, edit the default response rule after completing the wizard.
Set the initial authentication method for this security rule:
Active Directory default (Kerberos V5 protocol)
Use a certificate from this certification authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
< Back
Next >
Cancel
Policy Assigned
No
No
No


Console1
File
Action
View
Favorites
Window
Help
Console Root
IP Security Policies on Local Computer
Manage IP filter lists and filter actions
Manage IP Filter Lists
Manage Filter Actions
This dialog allows you to create and maintain the IP filter lists that describe your network traffic.
The available IP filter lists are shared by all IP Security policies.
IP Filter Lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
Add...
Edit...
Remove
OK
Cancel
Apply



Με τις παραπάνω διαδικασίες αρχικά δημιουργήσαμε πιστοποιητικά για να μπορούν να αυθεντικοποιούνται οι δύο υπολογιστές. Στην συνέχεια δημιουργήσαμε μια πολιτική ασφάλειας, βάση της οποίας λειτουργεί το IPsec. Στέλνουμε ξανά το μήνυμα “IPv6 Security” από τον υπολογιστή1 στον υπολογιστή2 μέσω του Achat. Χρησιμοποιούμε πάλι το Wireshark για να υποκλέψουμε το μήνυμα (Εικόνα 9.20). Αυτή την φορά αποτυγχάνουμε να διαβάσουμε το μήνυμα διότι η επικοινωνία είναι κρυπτογραφημένη μέσω του ESP πρωτοκόλλου του IPsec.



Εικόνα 9.20: Αποτέλεσμα Wireshark ασφαλούς επικοινωνίας μέσω IPsec

10

IPv6 Firewalls & IDSs

Το συγκεκριμένο κεφάλαιο είναι αφιερωμένο στα αναχώματα ασφάλειας (firewalls) και στα intrusion detection systems (IDSs) του πρωτοκόλλου IPv6. Αρχικά γίνεται μια περιγραφή των βασικών δυνατοτήτων ενός Firewall (γενικότερα στο πρωτόκολλο IPv4) και στην συνέχεια εξετάζεται η περίπτωση των Firewalls στο πρωτόκολλο IPv6. Στο τέλος, γίνεται μια αναφορά στα IDSs του πρωτοκόλλου IPv6.

10.1 Δυνατότητες Αναχωμάτων Ασφάλειας

Η τεχνολογία των αναχωμάτων ασφάλειας (Firewalls) και η χρήση τους παρουσιάζει ουσιώδεις αλλαγές και βελτιώσεις στην πάροδο των χρόνων. Ωστόσο, οι βασικές αρχές είναι ίδιες και στην ουσία ένα Firewall είναι μια διαδικτυακή συσκευή ασφάλειας που επιβάλλει μια συγκεκριμένη πολιτική ασφάλειας σε έναν οργανισμό, εγκρίνοντας ή απορρίπτοντας (δια)δικτυακή κυκλοφορία.

Με σκοπό την ορθή λειτουργία του Firewall και την τήρηση των απαιτήσεων ενός οργανισμού είναι αναγκαίο από τον διαχειριστή ασφάλειας να δημιουργήσει ένα σύνολο κανόνων, βάση των οποίων θα λειτουργεί το Firewall. Ένα Firewall εξετάζει τα εισερχόμενα – εξερχόμενα πακέτα και βάση του συνόλου κανόνων παίρνει ορισμένες αποφάσεις σχετικά με την διαχείριση τους [52]. Γενικότερα τα Firewalls έχουν τις ακόλουθες δυνατότητες:

- Network address translation
- Virtual private networks
- Demilitarized zones
- Anti-spoofing

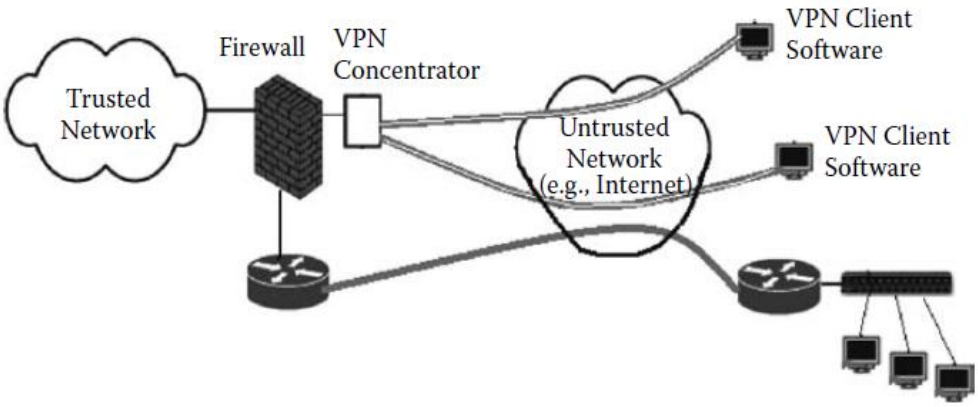
10.1.1 Network Address Translation

Σε ένα IPv4 περιβάλλον, το NAT βοηθάει στην διευκόλυνση της επικοινωνίας ανάμεσα στους τελικούς κόμβους (endpoints) και επίσης παρέχει μια αυξημένη λειτουργία ασφάλειας. Το NAT παρέχει μια σημαντική λύση στην έλλειψη διαθέσιμων IPv4 διευθύνσεων. Η λειτουργία του NAT είναι να ξαναγράψει τα περιεχόμενα μιας κεφαλίδας ενός πακέτου IP, έτσι ώστε να φαίνεται ότι το πακέτο προέρχεται από μια μοναδική (διαφορετική) IP διεύθυνση. Αυτή η δυνατότητα επιτρέπει στους οργανισμούς να κρύψουν λεπτομέρειες σχετικά με την τοπολογία του εσωτερικού τους δικτύου, κάνοντας όλα τα

πακέτα των εσωτερικών endpoints να φαίνεται ότι προέρχονται από μια μοναδική IP διεύθυνση [52].

10.1.2 Virtual Private Networks

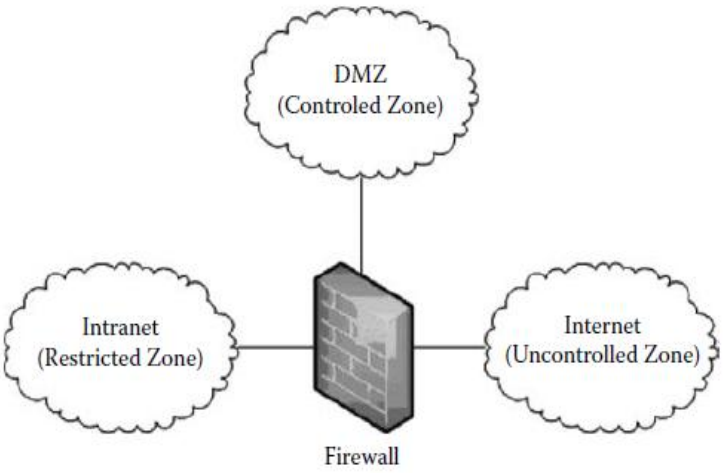
Ένα Virtual Private Network (VPN) (Εικόνα 10.1), είναι ένα ιδιωτικό δίκτυο που χρησιμοποιεί ένα δημόσιο δίκτυο (συνήθως το Διαδίκτυο) για να συνδέσει απομακρυσμένες τοποθεσίες και χρήστες μεταξύ τους. Ένα VPN αντί να κάνει χρήση μιας πραγματικής-παγκόσμιας σύνδεσης, όπως μιας “μισθωμένης” (leased) γραμμής, χρησιμοποιεί “εικονικές” (virtual) συνδέσεις που δρομολογούνται μέσω του Διαδικτύου από το ιδιόκτητο (ιδιωτικό) δίκτυο της εταιρείας στην απομακρυσμένη τοποθεσία [52].



Εικόνα 10.1: Virtual Private Network

10.1.3 Demilitarized Zones

Στην εποχή που ζούμε η άμεση επικοινωνία είναι απαραίτητη, για αυτό είναι αναγκαίο για τους οργανισμούς να μπορούν να συνδέονται άμεσα με τον οποιοδήποτε, αλλά ταυτόχρονα να προστατεύονται σημεία ζωτικής σημασίας (ως προς την ασφάλεια) για τον οργανισμό. Αυτή την απαίτηση την αναλαμβάνει ένα DMZ, το οποίο επιτρέπει την παροχή δημόσιων υπηρεσιών, ενώ ταυτόχρονα προστατεύει τον οργανισμό, όπως για παράδειγμα εξυπηρετητές Email και Web. Ένα DMZ θέτει ορισμένα όρια ανάμεσα σε δύο δίκτυα (Εικόνα 10.2). Το ένα δίκτυο είναι έμπιστο και συνήθως είναι το εσωτερικό δίκτυο. Το δεύτερο δίκτυο είναι το DMZ, το οποίο είναι μη έμπιστο, καθώς είναι διαδικτυακά προσπελάσιμο. Μία σημαντική δυνατότητα του Firewall είναι να μπορεί να δημιουργήσει μια DMZ και στην συνέχεια να ελέγχει την πρόσβαση εντός και εκτός δικτύου, προστατεύοντας τις δημόσιες υπηρεσίες που προσφέρονται [51].



Εικόνα 10.2: Demilitarized Zones

10.1.4 Anti-Spoofing

Όπως έχει αναφερθεί, τα Firewalls υλοποιούν πολιτικές ασφάλειας που βασίζονται σε σύνολα κανόνων, τα οποία προσδιορίζονται από τους διαχειριστές ασφάλειας. Ο πυρήνας ενός συνόλου κανόνων είναι η περιγραφή της τοπολογίας του δικτύου σε ένα Firewall, έτσι ώστε η απόφαση που παίρνεται, να βασίζεται στην τοποθεσία των endpoints. Συγκεκριμένα, το σύνολο κανόνων εξετάζει τις IP διευθύνσεις με σκοπό να διευκρινίσει την προέλευση των πακέτων. Το Antispoofing είναι μια δυνατότητα που έχουν ορισμένα Firewalls, με σκοπό να διαβεβαιώνουν ότι ένας επιτιθέμενος δεν μπορεί να κάνει spoof μια διεύθυνση πηγής, και κατά συνέπεια δεν είναι σε θέση να εξαπατήσει το Firewall με το να επιτρέψει μια σύνδεση που θα έπρεπε να είχε αρνηθεί. Τα Firewalls υλοποιούν την antispoofing δυνατότητα ελέγχοντας την διεύθυνση πηγής κάθε πακέτου, εξετάζοντας παράλληλα μια προκαθορισμένη άποψη της τοπολογίας του δικτύου [52].

10.2 Αναχώματα Ασφάλειας σε IPv6 περιβάλλοντα

Τα Firewalls μπορούν να λειτουργήσουν σε ένα περιβάλλον που υποστηρίζει μόνο το πρωτόκολλο IPv6 ή κατά κανόνα, σε ανάμεικτα IPv4/IPv6 περιβάλλοντα. Σε τέτοιου είδους περιβάλλοντα, τα Firewalls χρειάζεται να διατηρούν πίνακες καταστάσεων τόσο για το IPv4 όσο και για το IPv6 και να μπορούν να παρακολουθούν ταυτόχρονα την δικτυακή κίνηση που προέρχεται από τα δύο πρωτόκολλα [52].

Ένα firewall εφαρμόζει ένα σύνολο κανόνων με σκοπό την επιθεώρηση και το φιλτράρισμα των εισερχόμενων-εξερχόμενων πακέτων. Οι τρεις τύποι επιθεώρησης της δικτυακής κυκλοφορίας που χρησιμοποιούνται στο παραδοσιακό IPv4 είναι: static packet filtering, stateful packet inspection και application-layer inspection. Οι ίδιοι τύποι επιθεώρησης απαιτούνται και στα IPv6 περιβάλλοντα, ωστόσο υπάρχει επιπλέον ανάγκη για διαχείριση των tunneled συνδέσμων. Κάποια τυπικά ζητήματα που ισχύουν στα

Firewalls γενικότερα είναι (1) η ύπαρξη πολλών τρυπών (too many holes) κάτι που επιτρέπει το πέρασμα πολλών διαφορετικών πρωτοκόλλων, (2) επιφανειακή εξέταση της εισερχόμενης κυκλοφορίας, χωρίς να γίνεται αναλυτική επιθεώρηση των πακέτων ή (3) ορισμένα από τα δεδομένα που διέρχονται είναι μη ορατά από το Firewall, λόγω του γεγονότος ότι είναι κρυπτογραφημένα. Τα συγκεκριμένα ζητήματα αφορούν τόσο "καθαρά" IPv6 περιβάλλοντα όσο και ανάμεικτα IPv6 περιβάλλοντα [52].

Ένα IPv6 Firewall εκτός από την ικανότητα φιλτραρίσματος πρέπει να έχει την δυνατότητα να κάνει τουλάχιστον τα εξής: να προωθεί IPv6 κυκλοφορία ανάμεσα σε εσωτερικές και εξωτερικές διεπαφές, ή να είναι ικανό να αποδέχεται IPv4 datagrams, τα οποία προέρχονται από εσωτερικά δίκτυα και υπολογιστές/συστήματα οι οποίοι είναι IPv4-only, να ενθυλακώνει τα IPv4 datagrams ως ωφέλιμα φορτία των IPv6 datagrams και να τα προωθεί σε IPv6 προορισμούς.

Ένα σημαντικό πρόβλημα που έχουν να αντιμετωπίσουν τα IPv6 Firewalls είναι η διαχείριση του IPsec tunneling και της κρυπτογράφησης που αυτό παρέχει [52]. Έτσι όταν γίνεται χρήση του IPsec ένα Firewall δεν είναι σε θέση να επιθεωρήσει τα πακέτα και συγκεκριμένα τα δεδομένα, καθώς αυτά είναι κρυπτογραφημένα. Έτσι για παράδειγμα δίνεται η δυνατότητα σε έναν επιτιθέμενο να ενσωματώσει ιομορφικό κώδικα στα κρυπτογραφημένα δεδομένα, να διαπεράσει το Firewall και να προκαλέσεις ζημιές στο εσωτερικό του δικτύου. Για αυτό το λόγο όταν γίνεται χρήση του IPsec είναι απαραίτητη η χρήση host-based Firewalls (firewalls, τα οποία είναι εγκατεστημένα τοπικά στους υπολογιστές/συστήματα), τα οποία θα μπορούν να εξετάσουν τα αποκρυπτογραφημένα πακέτα.

10.2.1 Φιλτράρισμα Πακέτων

Συνήθως, ένα Firewall όταν φιλτράρει πακέτα χρησιμοποιεί κανόνες, οι οποίοι βασίζονται σε παράγοντες, όπως [52]: διεύθυνση πηγής/προορισμού, πρωτόκολλο, θύρες πηγές/προορισμού και άλλα πεδία όπως Traffic Class ή Flow Label. Φίλτρα, τα οποία βασίζονται σε διευθύνσεις πηγής/προορισμού είναι σχετικά εύκολο να υλοποιηθούν, ωστόσο η δυνατότητα που δίνεται στους IPv6 υπολογιστές/συστήματα να διατηρούν αρκετές διευθύνσεις περιπλέκει το θέμα.

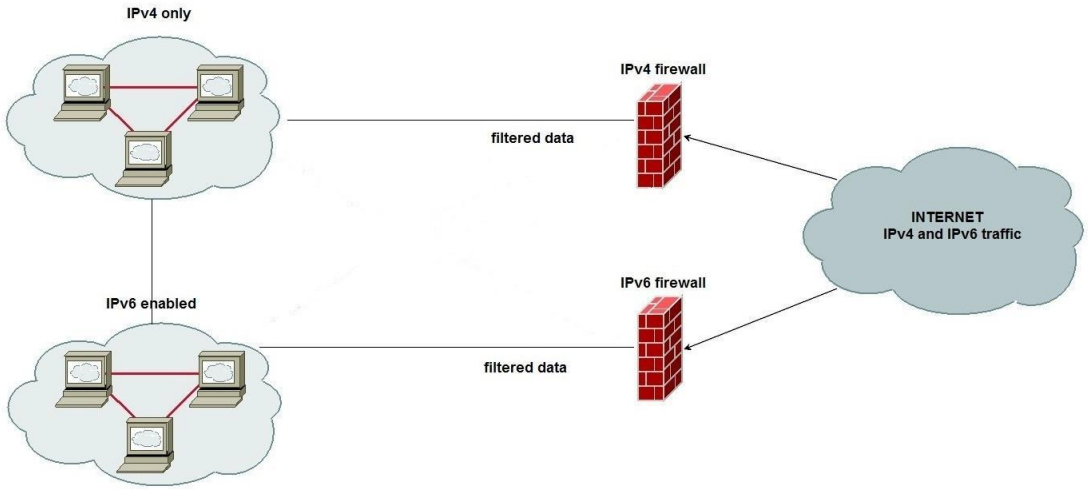
Μια άλλη σημαντική δυσκολία προκύπτει από την χρήση τυχαίων (randomized) διευθύνσεων στο IPv6, αλλά και από την χρήση ICMPv6 πακέτων [52], ορισμένα από τα οποία είναι απαραίτητα για την ορθή λειτουργία των IPv6 λειτουργιών. Έτσι, ενώ τα IPv4 Firewalls, συνήθως φιλτράρουν και απορρίπτουν τα ICMP μηνύματα, τα IPv6 Firewalls οφείλουν να επιτρέπουν την είσοδο στα ICMPv6 μηνύματα για να λειτουργήσουν ορθά ορισμένα πρωτόκολλα, όπως το Neighbor και Router Discovery.

Υπάρχουν διαφορετικές εφαρμογές των firewalls που μπορούν να ταξινομηθούν με διαφορετικούς τρόπους:

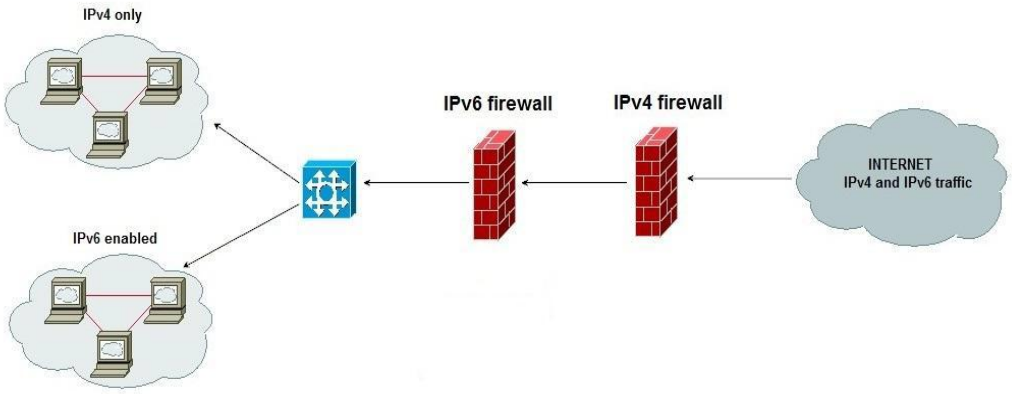
- **Packet Filtering Gateways:** Τα Packet Filtering Firewalls χρησιμοποιούν δρομολογητές με τους κανόνες φιλτραρίσματος πακέτων (packet filtering rules) για να εγκρίνουν ή να απορρίψουν την πρόσβαση βάση της source address, της destination address και της θύρας (port). Προσφέρουν την ελάχιστη ασφάλεια αλλά με πολύ χαμηλό κόστος, και μπορούν να είναι η καταλληλότερη επιλογή για ένα

περιβάλλον χαμηλού κινδύνου. Είναι γρήγορα, εύκαμπτα, και διαφανή. Οι κανόνες φιλτραρίσματος δεν είναι συχνά εύκολα συντηρήσιμοι σε έναν δρομολογητή, αλλά υπάρχουν εργαλεία διαθέσιμα που απλοποιούν την διαδικασία δημιουργίας και συντήρησης των κανόνων.

- **Application Gateways:** Ένα Application Gateway χρησιμοποιεί server programs που ονομάζονται proxies, τα οποία τρέχουν στο Firewall. Αυτά τα proxies παίρνουν τα εξωτερικά αιτήματα, τα εξετάζουν, και προωθούν (forward) τα νόμιμα αιτήματα στον εσωτερικό Η/Τ που παρέχει την αρμόδια υπηρεσία. Τα application gateways μπορούν να υποστηρίξουν λειτουργίες, όπως η αυθεντικοποίηση χρηστών και logging.
- **Hybrid or Complex Gateways:** Τα Hybrid Gateways συνδυάζουν δύο ή περισσότερους από τους ανωτέρω τύπους Firewall και τους εφαρμόζουν στη σειρά παρά παράλληλα. Εάν συνδέονται στη σειρά (Εικόνα 10.4), η γενική ασφάλεια ενισχύεται, αφ' ετέρου, εάν συνδέονται παράλληλα (Εικόνα 10.3), η περίμετρος ασφάλειας του δικτύου θα είναι μόνο τόσο ασφαλής όσο και η πιο ελάχιστα ασφαλής μέθοδος από αυτές που χρησιμοποιούνται.



Εικόνα 10.3: Υβριδικό Firewall. Παράλληλη τοποθέτηση IPv4 και IPv6 Firewall



Εικόνα 10.4: Υβριδικό Firewall. Σε σειρά τοποθέτηση IPv4 και IPv6 Firewall

10.3 Intrusion Detection Systems

Το intrusion detection system (IDS) είναι ένα σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την εποπτεία και ανάλυση των διαφόρων γεγονότων που συμβαίνουν σε ένα δίκτυο ή σε έναν συγκεκριμένο υπολογιστή/σύστημα. Το IDS σύστημα αναλύει τα διαδικτυακά γεγονότα ψάχνοντας για ενδείξεις μη εξουσιοδοτημένη εισβολής. Η έννοια “εισβολή” (intrusion) υποδηλώνει όλες τις προσπάθειες που θέτουν σε κίνδυνο την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα ενός υπολογιστή ή ενός δικτύου, δηλαδή όλες τις απόπειρες αποφυγής δικτυακών μηχανισμών ασφάλειας (π.χ. Firewalls). Μια εισβολή μπορεί να επιτευχθεί από έναν εξωτερικό επιτιθέμενο, αλλά επίσης και από εξουσιοδοτημένους χρήστες που προσπαθούν να κερδίσουν επιπλέον δικαιώματα σε ένα σύστημα [4].

Η λειτουργία ενός intrusion detection system έχει τρεις διαφορετικές φάσεις [4]. Στην πρώτη φάση το IDS σύστημα συγκεντρώνει πληροφορίες σχετικά με τα διάφορα γεγονότα που μπορούν να συμβούν στο επιτηρούμενο σύστημα. Μέσω της δεύτερης φάσης το IDS σύστημα οργανώνει και αναλύει τις συγκεντρωθείσες πληροφορίες με σκοπό να αναγνωρίσει μη εξουσιοδοτημένες δραστηριότητες. Η τρίτη φάση περιλαμβάνει τις δράσεις και τα μέτρα που αναλαμβάνει το σύστημα όταν συμβεί μια μη εξουσιοδοτημένη εισβολή. Αυτά τα μέτρα μπορεί να είναι “ενεργά” (κάποιο είδος αυτόματης ανταπόκρισης-αντίδρασης) ή “παθητικά” (επαγρύπνηση ενός εξουσιοδοτημένου χρήστη).

10.3.1 Δυνατότητες ενός IDS σε IPv6 δίκτυα

Στα IPv4 δίκτυα υπάρχουν ορισμένα open source IDS συστήματα. Χρησιμοποιώντας IDS συστήματα στα IPv4 δίκτυα, η διαδικασία ανίχνευσης μιας εισβολής μπορεί να είναι πλήρως αυτοματοποιημένη. Σε αυτή την περίπτωση μια απόπειρα για μη εξουσιοδοτημένη εισβολή θα αναγνωριστεί και θα αντιμετωπιστεί από το IDS σύστημα [4].

Όσον αφορά στο IPv6, τα εμπορικά IDS που διατίθενται δεν είναι ιδιαιτέρως αναπτυγμένα και η παραπάνω αυτοματοποιημένη διαδικασία ανίχνευσης είναι σε πρώιμο

στάδιο. Στο IPv6 η ανίχνευση εισβολής απαιτεί έναν εκπαιδευμένο διαχειριστή, που είναι ικανός να αναγνωρίσει την απόπειρα επίτευξης της, συλλαμβάνοντας ένα δείγμα δικτυακή κυκλοφορίας [4]. Ένα IDS σύστημα που υποστηρίζει το πρωτόκολλο IPv6, οφείλει να λαμβάνει υπόψη του τα νέα χαρακτηριστικά του συγκεκριμένου πρωτοκόλλου.

Το IPv6 προσδιορίζει μια νέα μορφή κεφαλίδας, η οποία πρέπει να αναγνωριστεί σωστά από το IDS σύστημα. Το IPv6 εισάγει extension headers (hop-by-hop, routing header, fragment header, destination options header, authentication header, encapsulation security payload) με σκοπό να απλοποιήσει την κύρια κεφαλίδα. Επίσης, η μορφή του next header επιτρέπει τον προσδιορισμό και την υλοποίηση νέων τύπων IPv6 extension headers αργότερα. Το IDS σύστημα πρέπει να υλοποιεί έναν σωστό τρόπο υποστήριξης όλων των IPv6 extension headers. Επιπλέον, όπως έχει αναφερθεί σε προηγούμενα κεφάλαια, τα extension headers πρέπει να ακολουθούν μια συγκεκριμένη σειρά, έτσι είναι ιδιαίτερα επιθυμητό το IDS (που υποστηρίζει το πρωτόκολλο IPv6), να μπορεί να ελέγξει την σειρά εμφάνισης των IPv6 extension headers [4]. Συνιστάται το IDS να απορρίπτει ένα πακέτο με μια απροσδιόριστη next header τιμή και να το καταγράφει ως συμβάν. [4]

Η μόνη κεφαλίδα που εξετάζεται στους ενδιάμεσους κόμβους ενός μονοπατιού από τον κόμβο πηγή στον κόμβο προορισμό είναι η hop-by-hop options κεφαλίδα. Επειδή αυτή μπορεί να περιλαμβάνει πολλαπλές ή επαναλαμβανόμενες επιλογές ένα IPv6 IDS σύστημα πρέπει να ανιχνεύει “ακανόνιστες” και διπλότυπες επιλογές. Επιπροσθέτως, η κεφαλίδα destinations option δέχεται επεξεργασία από τον κόμβο προορισμού και θα πρέπει να ελέγχεται επίσης από το IDS με σκοπό να ανιχνευθούν διπλότυπες επιλογές. Αυτός ο έλεγχος είναι απαραίτητος, επειδή μια εσφαλμένη destination option ή μια hop-by-hop option μπορεί να εγκατασταθεί σκόπιμα από έναν επιτιθέμενο [4]. Εάν ο δικτυακός κόμβος πρέπει να στείλει ένα ICMPv6 error μήνυμα σε περίπτωση εσφαλμένων επιλογών (bad options), μπορεί να χρησιμοποιηθεί κακόβουλα για επίτευξη DoS επιθέσεων. Μία επίθεση θα στοχεύει πίσω στην spoofed διεύθυνση πηγής μέσω του απομακρυσμένου δικτύου. Επιπλέον, ένα IPv6 IDS σύστημα οφείλει να αναγνωρίζει και αναλύει σωστά την IPv6 κυκλοφορία που γίνεται tunneled σε ένα IPv4 δίκτυο. Αυτό υποδηλώνει την αναγκαιότητα για υποστήριξη τόσο αυτόματων όσο και χειροκίνητων tunnels [4].

Τέλος, εάν ένας κόμβος ή δίκτυο έχει ξεχωριστές συνδέσεις σε IPv4 και IPv6 δίκτυα, είναι αναγκαία η ανάπτυξη του κατάλληλου IDS για κάθε σύνδεση. Ένα intrusion detection system που αναπτύσσεται σε έναν dual-stack κόμβο με μία μοναδική σύνδεση πρέπει να αναγνωρίζει και υποστηρίζει και τα δύο πρωτόκολλα (IPv4/IPv6). Εάν η IPv6 κυκλοφορία περνάει μέσα από σήραγγα (tunneled), μια καλή πρακτική ασφάλειας είναι να τερματίσουμε το tunnel έξω από το IPv6 Firewall και να αναπτύσσουμε το IDS στο σημείο εισόδου του δικτύου [4].

11

Secure Neighbor Discovery

Για την αντιμετώπιση των επιθέσεων που μπορούν να επιτευχθούν στο Neighbor Discovery Protocol, το RFC 3971 προτείνει ένα νέο πρωτόκολλο ασφάλειας, το οποίο ονομάζεται Secure Neighbor Discovery (SEND). Προτού αναλύσουμε το SEND, πρέπει να τονιστεί το Neighbor Discovery Protocol (NDP) specification αναφέρει ότι για την προστασία των NDP μηνυμάτων θα πρέπει να χρησιμοποιείται το IPsec, ωστόσο δεν αναφέρει πώς μπορεί να χρησιμοποιηθεί το IPsec.

Το IPsec δεν είναι κατάλληλο για την προστασία του NDP, διότι χρησιμοποιεί το Internet Key Exchange, το οποίο απαιτεί οι κόμβοι να είναι addressable (δηλαδή να έχουν έγκυρη διεύθυνση) προτού χρησιμοποιηθεί το IPsec. Οι κόμβοι πρέπει να έχουν έγκυρη διεύθυνση για να μπορούν να δημιουργηθούν τα security associations μεταξύ τους. Όμως, ένας νεοεισερχόμενος κόμβος σε ένα IPv6 δίκτυο δεν έχει έγκυρη διεύθυνση, άρα δεν μπορεί να σχηματίσει συσχέτιση ασφάλειας με τους υπόλοιπους κόμβους. Γι' αυτό το λόγο, χρησιμοποιείται το νέο πρωτόκολλο SEND, το οποίο θα περιγράψουμε στην συνέχεια.

Το SEND προσφέρει τρία επιπλέον χαρακτηριστικά στο NDP: απόδειξη ιδιοκτησίας διεύθυνσης, προστασία μηνύματος και μηχανισμό εξουσιοδότησης του δρομολογητή. Για την επίτευξη αυτών των χαρακτηριστικών, το SEND χρησιμοποιεί τέσσερις νέες επιλογές (CGA διευθύνσεις, RSA υπογραφές, nonce και Timestamp) και δύο ICMPv6 μηνύματα για την διαδικασία εξουσιοδότησης δρομολογητή. Παρακάτω θα αναλύσουμε αυτές τις τέσσερις νέες επιλογές [55].

11.1 Cryptographically Generated Addresses

Οι Cryptographically generated addresses (CGA) είναι IPv6 διευθύνσεις, όπου μερικά από τα bits της διεύθυνσης, συνήθως τα 64-bit του interface identifier, δημιουργούνται από μια κρυπτογραφημένη σύνοψη του δημοσίου κλειδιού του ιδιοκτήτη της διεύθυνσης [35]. Ο ιδιοκτήτης της διεύθυνσης χρησιμοποιεί το αντίστοιχο ιδιωτικό κλειδί για να υπογράψει τα μηνύματα που στέλνει ή για να επιβεβαιώσει την ιδιοκτησία της διεύθυνσης. Οποιοσδήποτε μπορεί να επαληθεύσει αυτή την ιδιοκτησία κάνοντας χρήση του δημοσίου κλειδιού του αποστολέα. Ο μόνος τρόπος για να παρακάμψει κάποιος αυτή την αυθεντικοποίηση είναι να βρει ένα άλλο δημόσιο κλειδί, το οποίο να παράγει την ίδια σύνοψη (hash) [35].

Επιπλέον, το πρόβλημα αδυναμίας που παρουσίαζαν οι CGAs σχετικά με την ασφάλεια έχει επιλυθεί, απομακρύνοντας τον 64-bit περιορισμό του μήκους της σύνοψης (hash length). Η ασφάλεια βελτιώνεται μέσω της αύξησης τόσο του κόστους δημιουργίας

μιας νέας CGA διεύθυνσης όσο και του κόστους επίτευξης μιας brute-force επίθεσης, διατηρώντας αμετάβλητο το κόστος μιας CGA-based αυθεντικοποίησης [35]. Λόγω της συνεχούς ανάπτυξης της ισχύς των υπολογιστών, θα ήταν πολύ εύκολο στο άμεσο μέλλον για έναν επιτιθέμενο να “σπάσει” τον μηχανισμό αυθεντικοποίησης που γίνεται βάση CGA, αν συνέχιζε να ισχύει ο περιορισμός των 64-bit [35]. Από την στιγμή που καταργήθηκε ο συγκεκριμένος περιορισμός (δηλαδή η σύνοψη μπορεί να είναι μεγαλύτερη από 64 bits) το ενδεχόμενο πρόβλημα “σπασίματος” του μηχανισμού αυθεντικοποίησης παύει να ισχύει, ακόμα και εάν χρησιμοποιούνται μηχανές με τεράστια υπολογιστική ισχύ.

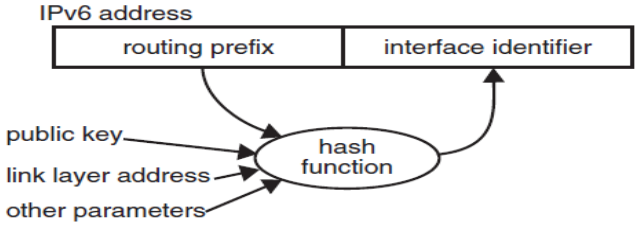
11.1.1 CGA παράμετροι και Hash τιμές

Για την δημιουργία μιας CGA διεύθυνσης χρησιμοποιείται μια συνάρτηση κατακερματισμού, η οποία λαμβάνει ως είσοδο το δημόσιο κλειδί του κόμβου και ορισμένες επικουρικές παραμέτρους. Αυτές οι βοηθητικές παράμετροι είναι οι ακόλουθοι 3 unsigned ακέραιοι [35]:

- Ένας 128-bit μετατροπέας (modifier), ο οποίος χρησιμοποιείται για υλοποίηση του επέκτασης κατακερματισμού (hash extension) και για ενίσχυση της ιδιωτικότητας, προσθέτοντας τυχαιότητα στην διεύθυνση.
- Το 64-bit prefix υποδικτύου της διεύθυνσης (subnet prefix).
- Μία 8-bit καταμέτρηση συγκρούσεων (collision count), η οποία έχει τιμές 0,1 και 2. Η συγκεκριμένη παράμετρος αυξάνεται κατά την διάρκεια δημιουργίας της CGA, όταν ανιχνευθεί κάποια σύγκρουση (collision) από την duplicate address detection διαδικασία.

11.1.2 Δομή των CGAs

Οι cryptographically generated addresses έχουν μία παράμετρο ασφάλειας (security parameter [Sec]), η οποία προσδιορίζει το επίπεδο ασφάλειας. Η διεύθυνση συνδυάζεται με ένα δημόσιο κλειδί και κάποιες επικουρικές παραμέτρους (Εικόνα 11.1), από τις οποίες δύο συνόψεις (hash values), Hash1 και Hash2 υπολογίζονται. Μια cryptographically generated address (CGA) ορίζεται ως μια IPv6 διεύθυνση, όπου τα 16 αριστερότερα bits (αν προσθέσουμε και το Sec) της Hash2 είναι μηδέν, ενώ τα δεξιότερα 64 bits της Hash1 είναι ίσα με το interface identifier της διεύθυνσης. Τα τρία αριστερότερα bits του interface identifier, που κρυπτογραφούν την παράμετρο ασφάλειας (Sec) αγνοούνται στην σύγκριση [35].

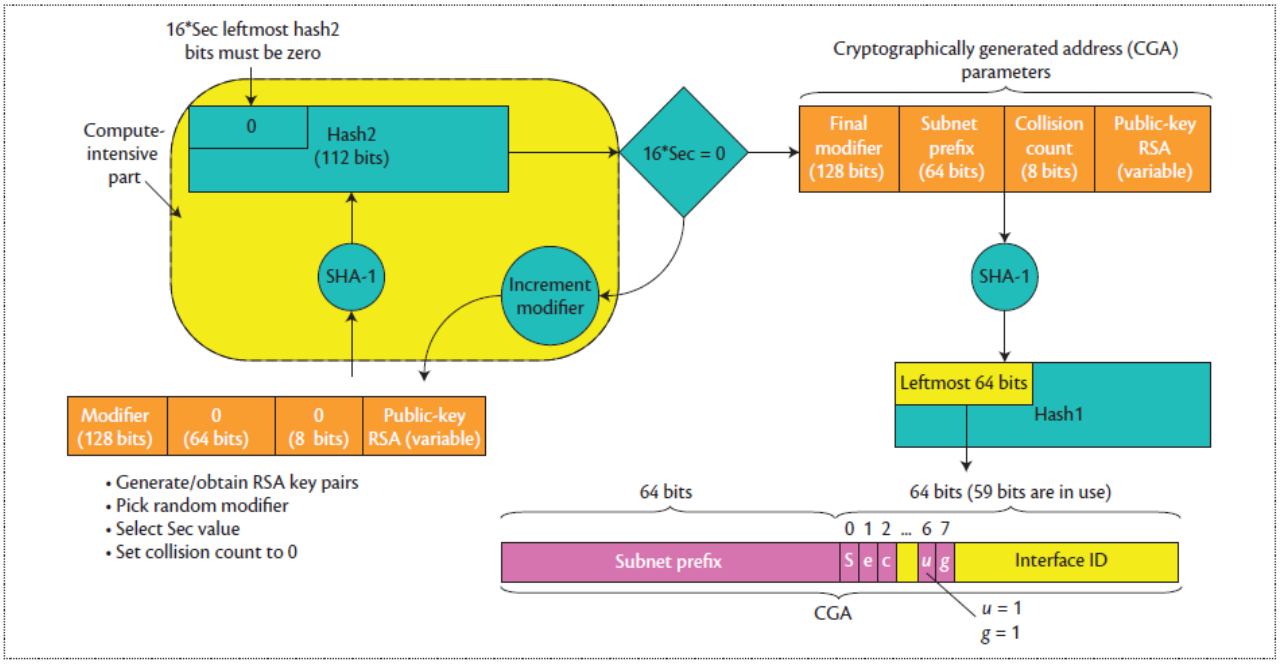


Εικόνα 11.1: Δημιουργία CGA διευθύνσεων

Πιο συγκεκριμένα, η δημιουργία μιας CGA διεύθυνσης (Εικόνα 11.2) ξεκινάει με τον δημιουργία του δημοσίου κλειδιού και με την επιλογή της τιμής για το επίπεδο ασφάλειας (Sec) που θα χρησιμοποιηθεί. Η παράμετρος ασφάλειας είναι ένας 3-bit unsigned ακέραιος, ο οποίος είναι κρυπτογραφημένος στα 3 πιο αριστερά bits ενός 64-bit interface identifier. Η συγκεκριμένη παράμετρος επιτρέπει στον ιδιοκτήτη της διεύθυνσης να αυξάνει την πολυπλοκότητα της διεύθυνσης και κατά συνέπεια το κόστος επίτευξης μιας brute-force επίθεσης εναντίον της διεύθυνσης [35]. Αυξάνοντας το Sec κατά ένα (1) προστίθενται 16 bits στο μήκος της σύνοψης που ο επιτιθέμενος πρέπει να “σπάσει”. Επίσης, από την στιγμή που η αξία της παραμέτρου ασφάλειας είναι κρυπτογραφημένη μέσα στην διεύθυνση, ο επιτιθέμενος δεν μπορεί να αλλάξει την αξία της χωρίς να αλλάξει την ίδια την διεύθυνση [35].

Στην συνέχεια υπολογίζεται η hash2 εντός ενός loop μέχρι να βρεθεί ο τελικός μετατροπέας (modifier). Η 112-bit Hash2 αποκτάται παίρνοντας τα αριστερότερα 112-bits της 160-bit SHA-1 hash τιμής [35], η οποία δέχεται ως είσοδο το δημόσιο κλειδί και όλες τις βοηθητικές παραμέτρους που περιγράψαμε παραπάνω (τα collision counts είναι μηδέν). Ο δημιουργός της διεύθυνσης (address generator) δοκιμάζει διάφορες τιμές για τον modifier έως ότου τα 16 αριστερότερα sec bits της hash2 γίνουν 0, όπου και τερματίζει το loop για την δημιουργία του hash2. Ο τελικός modifier που χρησιμοποιήθηκε για την hash2, αποθηκεύεται και χρησιμοποιείται ως είσοδος για τον υπολογισμό της hash1.

Η 64-bit hash1 αποκτάται παίρνοντας τα αριστερότερα 64-bits της 160-bit SHA-1 hash value [35], η οποία δέχεται ως είσοδο το δημόσιο κλειδί και όλες τις βοηθητικές παραμέτρους. Η τιμή hash1 που προκύπτει από την συνάρτηση κατακερματισμού αποτελεί το interface identifier. Η τιμή Sec κωδικοποιείται στα τρία αριστερότερα bits του interface identifier. Το 7ο και 8^{ο} bit από τα αριστερά του interface identifier είναι τα u και g bits αντίστοιχα. Το u bit, όταν έχει τιμή 1 υποδηλώνει δημόσια διεύθυνση, ενώ όταν έχει την τιμή 0 υποδηλώνει τοπική διεύθυνση. Το g bit είναι το individual/group bit (δες rfc 4291). Στο τέλος το πρωτόκολλο DAD διασφαλίζει ότι δεν υπάρχουν συγκρούσεις διευθύνσεων (address collisions) [55].



Εικόνα 11.2: Τα βήματα δημιουργίας μιας CGA διεύθυνσης

Ένα από τα βασικότερα μειονεκτήματα των GGA αποτελεί το υπολογιστικό κόστος. Οι υπολογισμοί για την δημιουργία μιας CGA διεύθυνσης απαιτούν πολύ χρόνο, ιδιαίτερα όταν έχουμε υψηλές Sec τιμές, δηλαδή όταν απαιτείται υψηλό επίπεδο ασφάλειας. Το πιο απαιτητικό μέρος ως προς την υπολογιστική δαπάνη για την δημιουργία μιας CGA είναι η εύρεση τιμής που να ικανοποιεί την hash2 συνθήκη.

11.2 RSA Signature

Το SEND χρησιμοποιεί την επιλογή της RSA υπογραφής για να αυθεντικοποιήσει την ταυτότητα του αποστολέα. Αρχικά, κάθε κόμβος πρέπει να δημιουργήσει ή να αποκτήσει ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού. Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό του κλειδί, το οποίο πρέπει να αντιστοιχεί με το δημόσιο κλειδί που χρησιμοποιεί για να δημιουργήσει την CGA διεύθυνση. Η χρήση της υπογραφής, εμποδίζει τους επιτιθέμενους να κάνουν spoof την CGA διεύθυνση.

11.3 Nonce

Η επιλογή nonce χρησιμοποιεί έναν τυχαίο αριθμό για να διασφαλίσει ότι ένα advertisement μήνυμα είναι μια “φρέσκια” ανταπόκριση σε ένα solicitation μήνυμα. Το SEND περιλαμβάνει μια nonce επιλογή στο solicitation μήνυμα και απαιτεί από τα advertisements μηνύματα να περιλαμβάνουν μια αντίστοιχη επιλογή. Η χρήση της nonce εμποδίζει την επίτευξη μια replay επίθεσης στα solicitation (NS ή RS) μηνύματα και στα advertisement (NA ή RA) μηνύματα.

11.4 Timestamp

Το SEND χρησιμοποιεί την Timestamp επιλογή για να διασφαλίσει προστασία απέναντι σε replay επιθέσεις στα unsolicited advertisements, όπως στα μηνύματα που στέλνει ένας δρομολογητής ανά διαστήματα (RAs), χωρίς να έχει λάβει κάποιο solicitation μήνυμα. Εδώ η υπόθεση είναι ότι όλοι οι κόμβοι έχουν συγχρονισμένα ρολόγια, έτσι ώστε ο κόμβος να μπορεί να εμποδίσει επιθέσεις τύπου replay, εκτελώντας ένας αλγόριθμο που θα ελέγχει τα timestamps.

11.5 Ασφάλεια στο Neighbor Discovery

Η χρήση CGA φαίνεται να είναι μια πολλά υποσχόμενη μέθοδος για ασφάλεια στο πρωτόκολλο Neighbor Discovery. Όπως αναφέρθηκε παραπάνω, η χρήση των CGAs γίνεται μέσω του SEcure Neighbor Discovery (SEND) πρωτοκόλλου, το οποίο αποτελεί επέκταση του Neighbor Discovery (ND) και χρησιμοποιείται για παροχή ασφάλειας στις λειτουργίες του ND. Όπως αρχικά αναφέρθηκε [37], οι CGAs μπορούν να χρησιμοποιηθούν για να αποδείξουν ότι η απάντηση προέρχεται από τον ιδιοκτήτη της διεύθυνσης (για παράδειγμα από τον κόμβο που δημιούργησε το μήνυμα). Αυτό γίνεται υπογράφοντας το μήνυμα με το κλειδί που χρησιμοποιείται για δημιουργία της διεύθυνσης [14]. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί για υπογραφή μηνυμάτων στις λειτουργίες Address Resolution, Duplicate Address Detection και Redirection.

11.5.1 Address Resolution

Ένας εύκολος τρόπος για να προστατέψουμε την address resolution λειτουργία είναι να συμπεριλάβουμε το αντίστοιχο δημόσιο κλειδί της CGA διεύθυνσης και μια υπογραφή σε όλα τα Neighbor Advertisement (NA) και Neighbor Solicitation (NS) πακέτα. Εάν οποιαδήποτε άλλη παράμετρος χρησιμοποιείται για δημιουργία της CGA, θα πρέπει να σταλεί, έτσι ώστε ο παραλήπτης να μπορεί να επαληθεύσει την τιμή της μονόδρομης συνάρτησης (hash value) [14].

Ένας κόμβος που λαμβάνει ένα NA ή NS μπορεί είτε να επαληθεύσει την διεύθυνση αμέσως, είτε να αποθηκεύσει τα μηνύματα για να τα επεξεργαστεί αργότερα. Εάν ο κόμβος αναβάλλει την παραπάνω επαλήθευση, μέχρι να χρειαστεί να χρησιμοποιήσει την διεύθυνση, μπορεί να αποφύγει μερικές απειλές τύπου denial-of-service [14].

Αρχικά, ο κόμβος που επαληθεύει (verifier), υπολογίζει ξανά την σύνοψη (hash) του δημοσίου κλειδιού και συγκρίνει το αποτέλεσμα με τον interface identifier. Ύστερα, επαληθεύει την υπογραφή του μηνύματος κάνοντας χρήση του δημοσίου κλειδιού του. Εάν και οι δύο έλεγχοι πετύχουν, ο verifier μπορεί να προσθέσει την διεύθυνση στην address resolution cache και να απορρίψει τα δεδομένα επαλήθευσης (verification data) [14].

11.5.2 Duplicate Address Detection

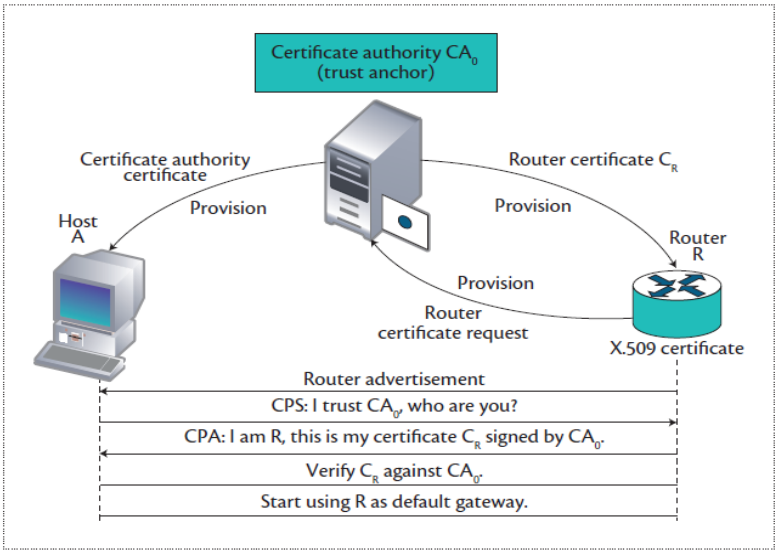
Από την στιγμή που μόνο ο ιδιοκτήτης μιας διεύθυνσης μπορεί να ανταποκριθεί με μια επαληθεύσιμη υπογραφή, όλες οι απόπειρες για spoofing στο DAD μπορούν να αποτραπούν [14]. Ωστόσο, ανάλογα με την local link, μπορεί να είναι πιθανό να εμποδίζονται έγκυρα μηνύματα να φτάσουν στους προοριζόμενους παραλήπτες.

Στην address auto-configuration διαδικασία του πρωτοκόλλου IPv6, είναι πιθανό να ανιχνευθεί μια address collision (σύγκρουση) και μια νέα διεύθυνση να χρειαστεί να δημιουργηθεί. Ωστόσο, είναι πολύ απίθανο να συμβεί μια address collision, εκτός αν είναι αποτέλεσμα μια επίθεσης στο πρωτόκολλο [14]. Τρεις συγκρούσεις (collisions) στην σειρά είναι πάρα πολύ απίθανο να συμβούν κατά τύχη, και είναι σχεδόν σίγουρα αποτέλεσμα μιας επίθεσης στο πρωτόκολλο ή ενός σφάλματος κατά την υλοποίησή του. Για το λόγο αυτό δεν επιτρέπεται η προσπάθεια δημιουργίας επιπλέον διευθύνσεων μετά από τρεις αλλεπάλληλες συγκρούσεις [14].

11.5.3 Securing Router Discovery

Ενώ οι CGAs φαίνεται να είναι ένας κατάλληλος μηχανισμός για παροχή ασφάλειας στις περισσότερες λειτουργίες του Neighbor Discovery, μονάχες τους δεν είναι επαρκείς για ασφάλεια στο Router Discovery. Αυτό συμβαίνει διότι δεν παρέχεται καμία πληροφορία, η οποία να επιβεβαιώνει ότι η συσκευή με την οποία επικοινωνεί ο υπολογιστής/σύστημα είναι ένας δρομολογητής. Έτσι, χρειαζόμαστε μια τρίτη έμπιστη οντότητα, η οποία να διασφαλίζει ότι ο κόμβος με τον οποίο επικοινωνεί ο υπολογιστής είναι πράγματι ένας δρομολογητής [55].

Το SEND χρησιμοποιεί το Authorization Delegation Discovery (ADD) για να ελέγξει και εξουσιοδοτήσει τους IPv6 δρομολογητές να λειτουργούν ως τα default gateways. Επιπλέον, το ADD χρησιμοποιείται για να καθορίσει ποια prefixes είναι εξουσιοδοτημένος ένας δρομολογητής να ανακοινώσει. Το ADD βασίζεται στα ψηφιακά πιστοποιητικά που εκδίδονται από μια έμπιστη τρίτη οντότητα. Προτού ένας κόμβος αποδεχτεί έναν δρομολογητή ως τον default δρομολογητή του, ο κόμβος θα πρέπει να διαμορφωθεί, χρησιμοποιώντας μια έμπιστη "άγκυρα πιστοποίησης", η οποία θα μπορεί να πιστοποιήσει τον δρομολογητή μέσω "μονοπατιών πιστοποίησης". Έτσι, ο κόμβος απαιτεί από τον δρομολογητή να παρουσιάσει το δικό του X.509 "μονοπάτι πιστοποίησης", το οποίο θα οδηγεί σε μια έμπιστη άγκυρα πιστοποίησης. Στην Εικόνα 11.3 φαίνεται ο μηχανισμός εξουσιοδότησης ενός δρομολογητή [55].



Εικόνα 11.3: Μηχανισμός εξουσιοδότησης δρομολογητή

Το SEND προσφέρει δύο νέους τύπους ICMPv6 μηνυμάτων για τον μηχανισμό της εξουσιοδότησης δρομολογητή. Το certificate path solicitation (CPS) και το certificate path advertisement (CPA). Ο υπολογιστής (host) στέλνει ένα CPS μήνυμα, το οποίο είναι ένα ICMPv6 μήνυμα τύπου 148, απαιτώντας ένα “μονοπάτι πιστοποίησης”, μεταξύ ενός δρομολογητή και μιας από του host έμπιστης “άγκυρας πιστοποίησης”. Το CPA μήνυμα, το οποίο είναι ένα ICMPv6 μήνυμα τύπου 149, αποστέλλεται ως απάντηση στο CPS μήνυμα και περιέχει το πιστοποιητικό του δρομολογητή (η συγκεκριμένη διαδικασία φαίνεται στην παραπάνω εικόνα).

12

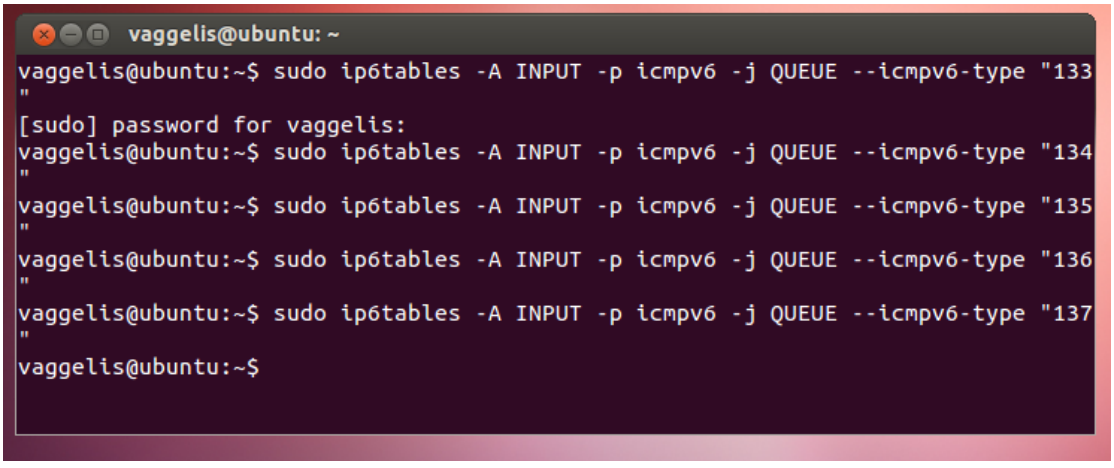
Υλοποίηση SEND

Για την υλοποίηση του Secure Neighbor Discovery πρωτοκόλλου χρησιμοποιήσαμε την εφαρμογή Easy-SEND [56]. Η συγκεκριμένη εφαρμογή τρέχει σε Linux συστήματα και χρησιμοποιεί την java. Αποτελείται από δύο αρχεία .jar, το cgagen.jar, το οποίο χρησιμοποιείται για την δημιουργία CGA διευθύνσεων και από το sendapp.jar, το οποίο χρησιμοποιείται για να τρέξει η εφαρμογή. Η συγκεκριμένη εφαρμογή τρέχει σε γραμμή εντολών.

Η δικτυακή μας υποδομή αποτελείται από δύο εικονικές μηχανές Ubuntu 12.04, στις οποίες έχουμε κατεβάσει την εφαρμογή Easy-SEND και σε κάθε μια έχει εγκατασταθεί η java 1.7.0.17. Επιπλέον, χρησιμοποιούμε το Wireshark, μέσω του Backtrack 5 R3, με σκοπό να αναλύσουμε την δικτυακή κυκλοφορία. Στόχος μας είναι να κάνουμε ping από τον ένα host στον άλλο, ενώ τρέχουμε την εφαρμογή Easy-SEND και να παρατηρήσουμε τα αποτελέσματα στον αναλυτή Wireshark.

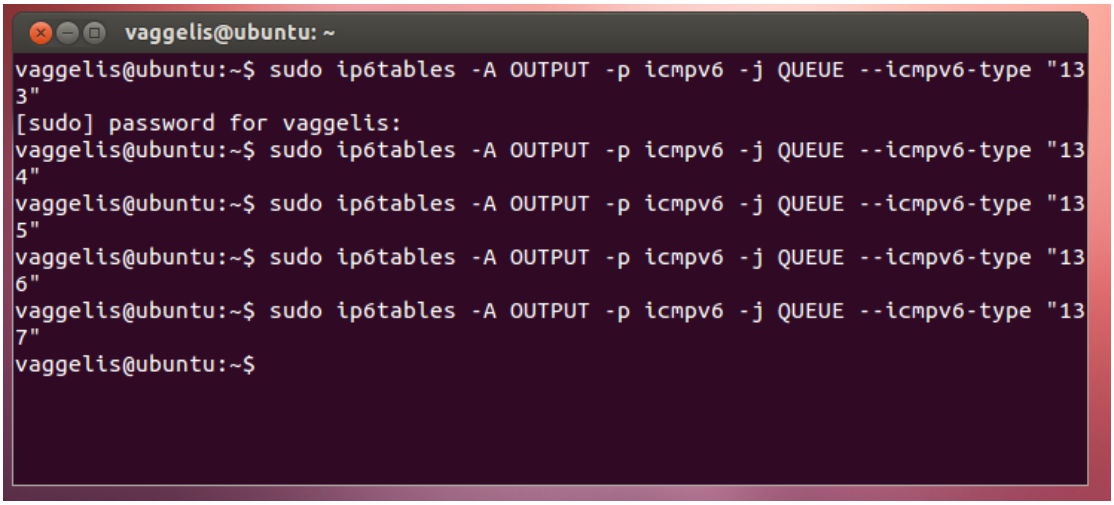
12.1 Βήματα Easy-SEND εφαρμογής

Αρχικά σε κάθε host θα πρέπει να εισάγουμε μέσω του ip6tables ορισμένους κανόνες για την εισερχόμενη και εξερχόμενη δικτυακή κυκλοφορία. Συγκεκριμένα, μας ενδιαφέρουν τα icmpv6 πακέτα Router Solicitation (τύπος πακέτου 133), Router Advertisement (τύπος πακέτου 134), Neighbor Solicitation (τύπος πακέτου 135), Neighbor Advertisement (τύπος πακέτου 136) και Redirect (τύπος πακέτου 137). Στην Εικόνα 12.1 φαίνεται η εισαγωγή των κανόνων (ως root) σε κάθε Ubuntu μηχανή για τα εισερχόμενα πακέτα.



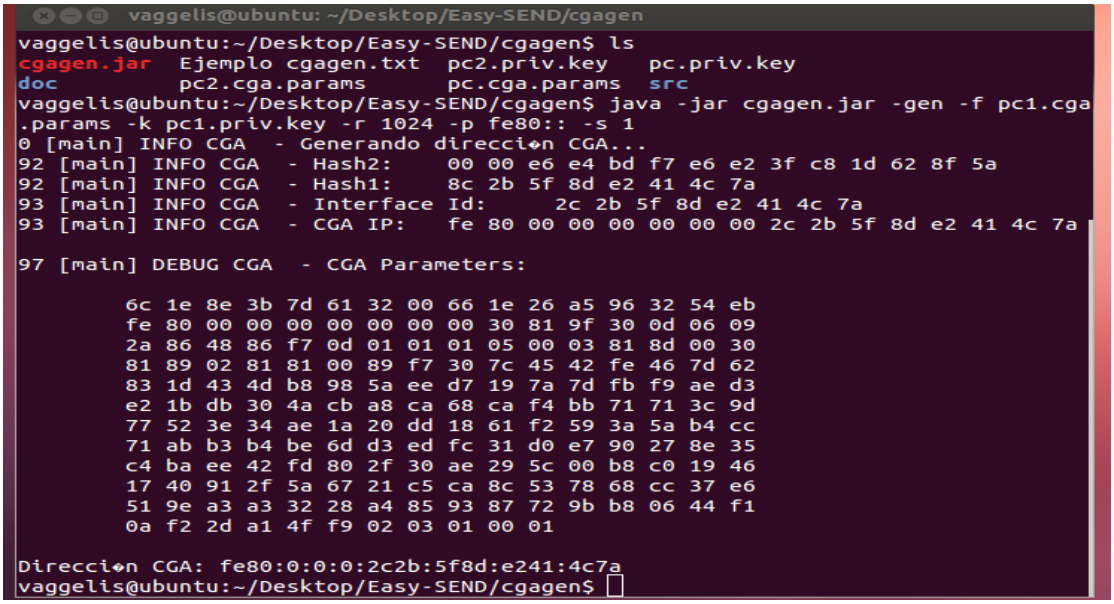
Εικόνα 12.1: ip6tables κανόνες εισερχόμενης κυκλοφορίας

Στην Εικόνα 12.2 φαίνεται η εισαγωγή των κανόνων σε κάθε host για τα εξερχόμενα πακέτα.



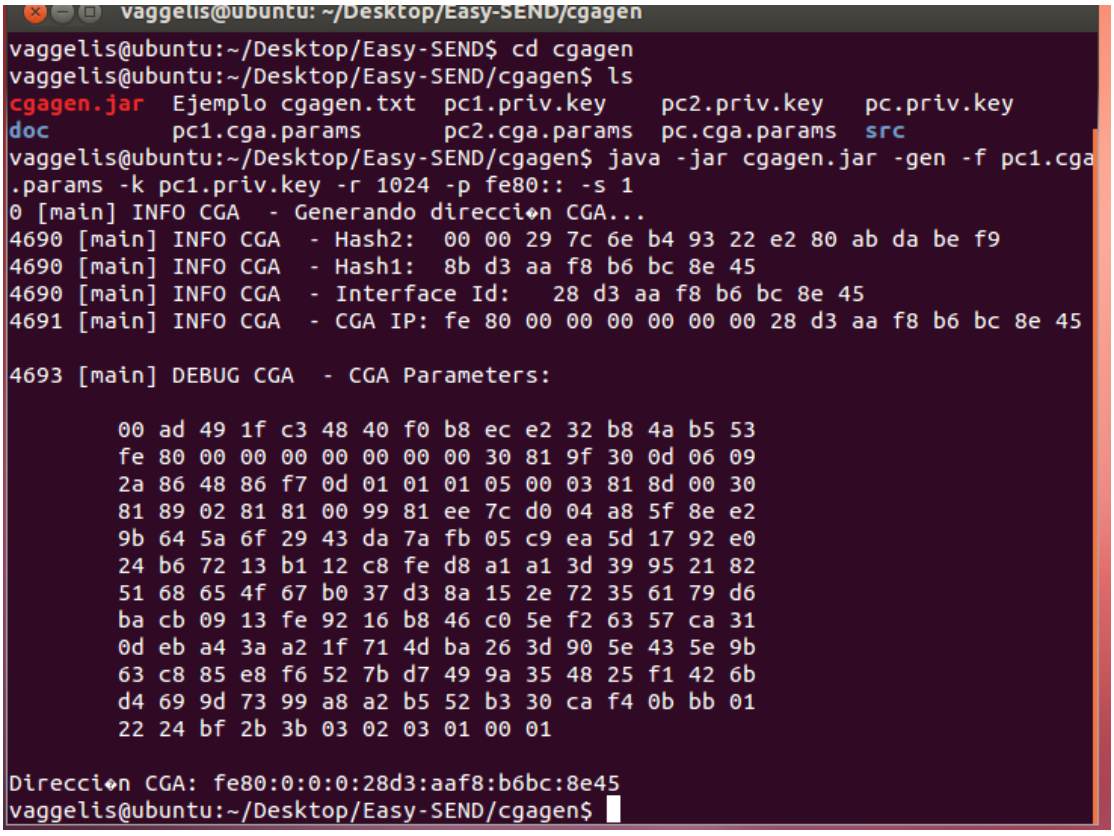
Εικόνα 12.2: ip6tables κανόνες εξερχόμενης κυκλοφορίας

Στην συνέχεια δημιουργούμε τις CGA διευθύνσεις για κάθε host, μέσω της εφαρμογής cgagen.jar. Η γενική μορφή της εντολής που χρησιμοποιούμε είναι: *java –jar cgagen.jar <παράμετροι>*. Στην συγκεκριμένη περίπτωση χρησιμοποιούμε την εντολή: *java –jar cgagen.jar –gen –f pc1.cga.params –k pc1.priv.key –r 1024 –p fe80:: -s 1* (Εικόνα 12.3). Στην παραπάνω εντολή η παράμετρος pc1.cga.params, είναι ένα αρχείο που περιέχει τις βοηθητικές παραμέτρους για την δημιουργία της cga διεύθυνσης. Το pc1.priv.key αρχείο περιέχει το ιδιωτικό κλειδί του host, το οποίο είναι 1024 bits. Επίσης, χρησιμοποιούμε ως πρόθεμα το fe80::, ώστε η CGA διεύθυνσή μας να είναι link-local. Τέλος, η παράμετρος s, υποδηλώνει το επίπεδο ασφάλειας (sec level), που θα χρησιμοποιήσουμε για την δημιουργία της CGA διεύθυνσης.



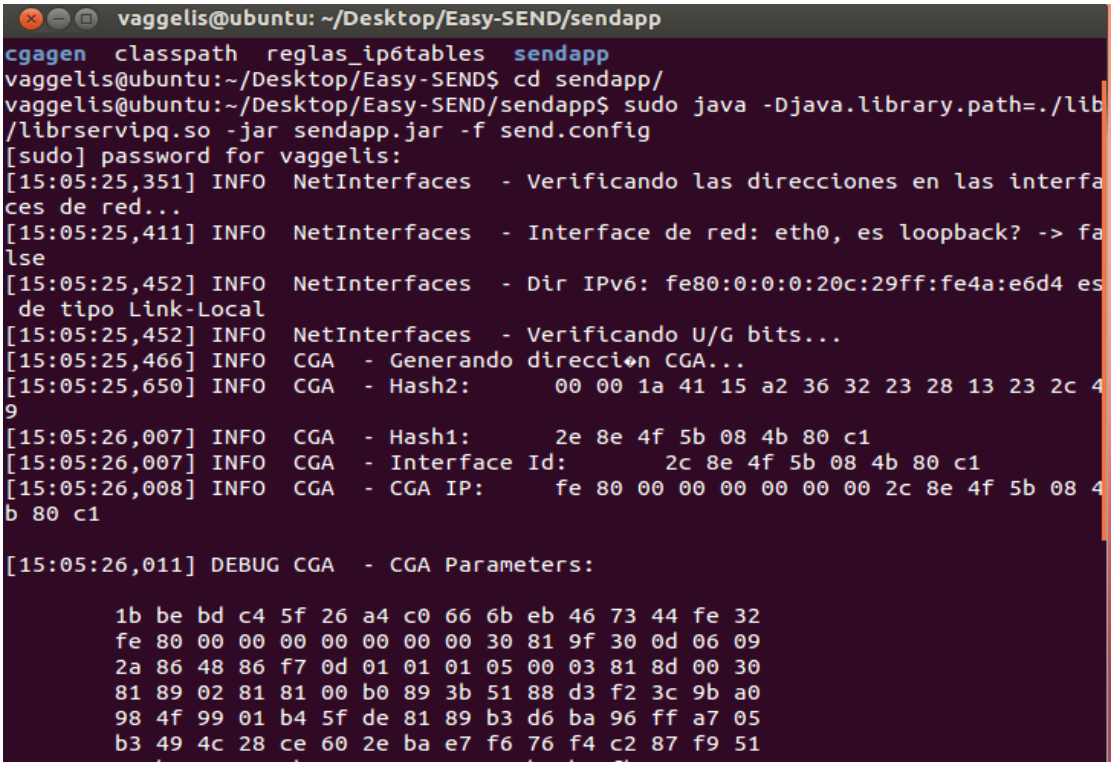
Εικόνα 12.3: Δημιουργία CGA διεύθυνσης για τον host1

Στην παραπάνω εικόνα φαίνεται η hash2 τιμή, η hash1 τιμή και στο κάτω μέρος φαίνεται η CGA διεύθυνση για τον host1, η οποία είναι fe80:0:0:0:2c2b:5f8d:e241:4c7a. Την παραπάνω εντολή εκτελούμε και στον host2, με αποτέλεσμα να πάρουμε διεύθυνση fe80:0:0:0:28d3:aaf8:b6bc:8e45 (Εικόνα 12.4).



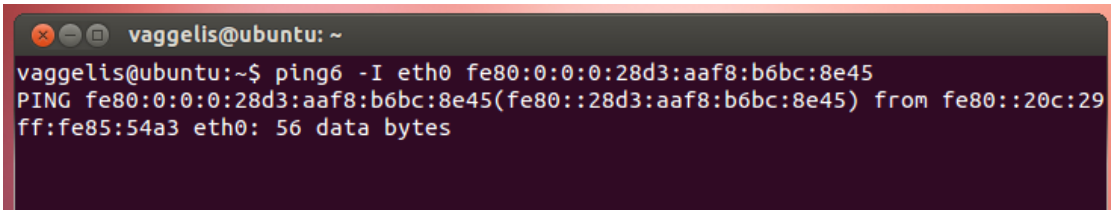
Εικόνα 12.4: Δημιουργία CGA διεύθυνσης για τον host2

Στην συνέχεια εκτελούμε ως root την εφαρμογή sendapp.jar, με την εντολή *sudo java –Djava.library.path=./lib/libvservipq.so –jar sendapp.jar –f send.config* (Εικόνα 12.5).



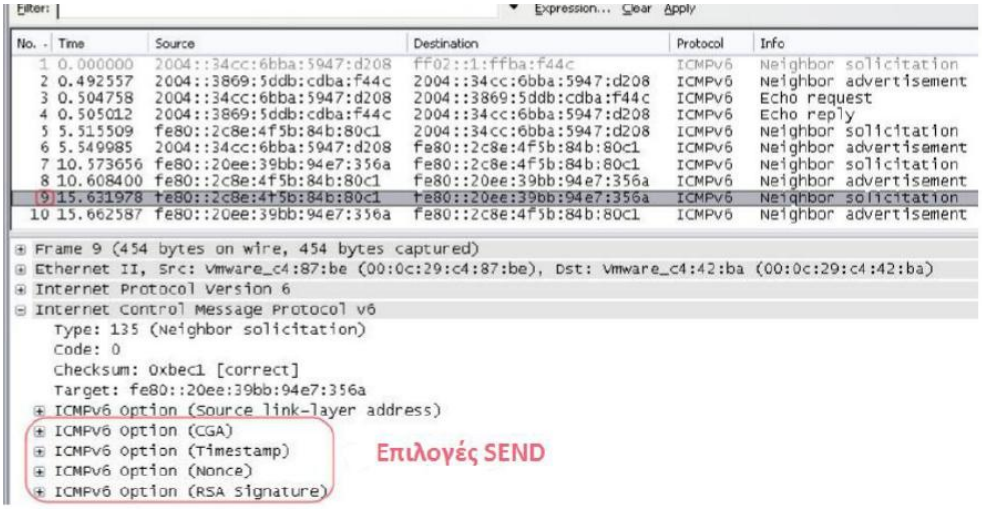
Εικόνα 12.5: "Τρέξιμο" εφαρμογής sendapp.jar

Τέλος, κάνουμε ping τον host2, από τον host1 (Εικόνα 12.6) και χρησιμοποιούμε το Wireshark για να υποκλέψουμε τα πακέτα και να αναλύσουμε την δικτυακή κίνηση. Η εντολή για ping στο πρωτόκολλο IPv6 είναι: *ping6 –I eth0 fe80:0:0:0:28d3:aaf8:b6bc:8e45* . Η διεύθυνση που κάνουμε ping είναι η CGA διεύθυνση του host2.



Εικόνα 12.6: ping host2 από host1

Στην Εικόνα 12.7 παρατηρούμε ότι στο Wireshark εμφανίζονται οι επιλογές του πρωτοκόλλου SEND (CGA, Timestamp, Nonce, RSA signature), οπότε η εφαρμογή του Easy-SEND, το οποίο υλοποιεί το SEND έγινε με επιτυχία.



Εικόνα 12.7: Εμφάνιση επιλογών SEND στο Wireshark

13

Επιθέσεις στο IPv6 μέσω του THC-IPv6-Attack-Toolkit

Για την υλοποίηση των επιθέσεων, χρησιμοποιήσαμε το λειτουργικό Backtrack 5 R3, το οποίο ενσωματώνει μια γνωστή σουίτα εργαλείων για επιθέσεις σε IPv6 δίκτυα, η οποία είναι γνωστή με το όνομα THC-IPv6 Attack Toolkit [57]. Το δίκτυό μας αποτελείται από τον επιτιθέμενο (Backtrack 5 R3), το θύμα, το οποίο τρέχει σε μηχανή Ubuntu 12.04 και έναν απλό κόμβο δικτύου, ο οποίος τρέχει και αυτός σε Ubuntu 12.04. Όλες οι μηχανές τρέχουν στο VMware Workstation. Συγκεκριμένα έχουμε τα παρακάτω:

Guest Μηχανή: Windows 7 Home Premium EN

Virtualization Λογισμικό: VMware Workstation

VM Hosts: Backtrack 5 R3 (Επιτιθέμενος)
Ubuntu 12.04 LTS (Θύμα)
Ubuntu 12.04 LTS (Απλός υπολογιστής δικτύου, ο οποίος συνεισφέρει στην επίθεση, εν αγνοία του)

Σουίτα εργαλείων: THC-IPv6 Attack Toolkit

Οι local link IPv6 διευθύνσεις των hosts είναι

Επιτιθέμενος : fe80::20c:29ff:feeb:1796/64
Θύμα: fe80::20c:29ff:fe4a:e6d4/64
Απλός κόμβος: fe80::20c:29ff:fe85:54a3/64
Δρομολογητής : fe80::256d:3548:328c:5b17/64
(Host’s VM adapter address)

13.1 Neighbor Solicitation/Advertisement Spoofing

Κατά την διάρκεια της συγκεκριμένης επίθεσης, ο επιτιθέμενος δημιουργεί πλαστά Neighbor Advertisement (NA) μηνύματα, ως απάντηση στα Neighbor Solicitation (NS) μηνύματα, με σκοπό να ανακατευθύνει ολόκληρη την δικτυακή κυκλοφορία στο σύστημά του. Για την επίτευξη της επίθεσης, χρησιμοποιούμε την εφαρμογή parasite6 και συγκεκριμένα την εντολή *parasite6 eth0* (Εικόνα 13.1).

Εικόνα 13.1: Εφαρμογή parasite6

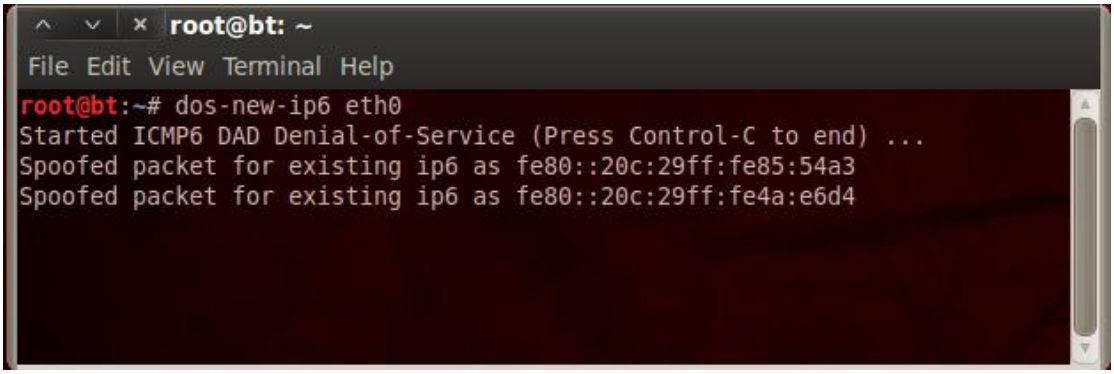
13.2 Duplicate Address Detection Attack

Ο IPv6 stateless auto-configuration μηχανισμός, χρησιμοποιεί την διαδικασία Duplicate Address Detection (DAD), για να βεβαιωθεί ότι μια IPv6 διεύθυνση δεν έχει δοθεί σε περισσότερους από έναν κόμβους εντός ενός δικτύου. Σύμφωνα με το DAD κάθε κόμβος που αποκτά μια IPv6 διεύθυνση πρέπει να ελέγξει εάν η συγκεκριμένη διεύθυνση χρησιμοποιείται από κάποιον άλλο κόμβο.

Ένας επιτιθέμενος μπορεί να δίνει "ψεύτικες" απαντήσεις, δηλώνοντας ότι κατέχει την εκάστοτε IPv6 διεύθυνση που επιθυμούν να λάβουν οι κόμβοι – θύματα. Με αυτό τον τρόπο ο επιτιθέμενος δεν επιτρέπει σε έναν κόμβο – θύμα να πάρει IPv6 διεύθυνση, άρα επιτυγχάνει μια DoS επίθεση. Το εργαλείο που χρησιμοποιεί ο επιτιθέμενος είναι το *dos-new-ip6*. Αρχικά εκτελούμε την επίθεση, πριν εισέλθουν οι κόμβοι στο δίκτυο (Εικόνα 13.2).

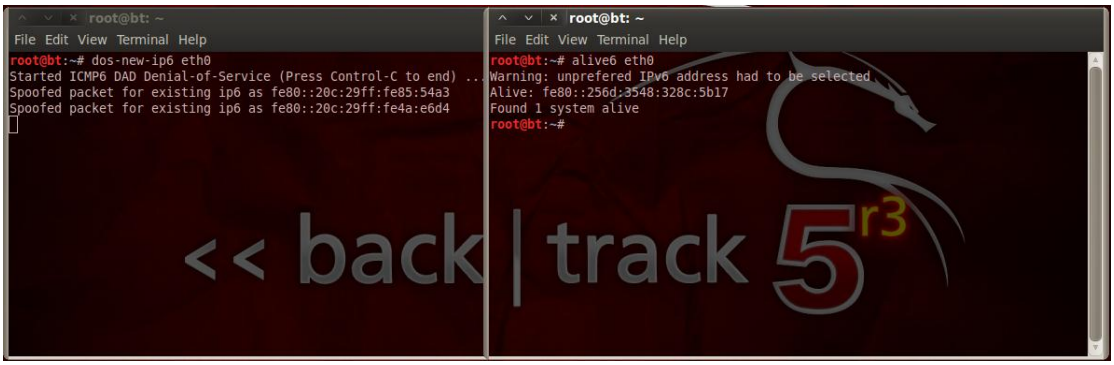
Εικόνα 13.2: Εφαρμογή dos-new-ip6

Στην συνέχεια εισέρχονται hosts στο δίκτυο (δηλαδή κάνουμε boot τους υπολογιστές) (Εικόνα 13.3).



Εικόνα 13.3: Εισαγωγή hosts στο δίκτυο

Στην Εικόνα 12.4 παρατηρούμε ότι όσο “τρέχει” η επίθεση, οι κόμβοι δεν μπορούν να πάρουν IPv6 διεύθυνση, γι’ αυτό το λόγο όταν εκτελούμε την εντολή alive6 eth0, εμφανίζεται ως “ζωντανός” κόμβος μόνο ο δρομολογητής.

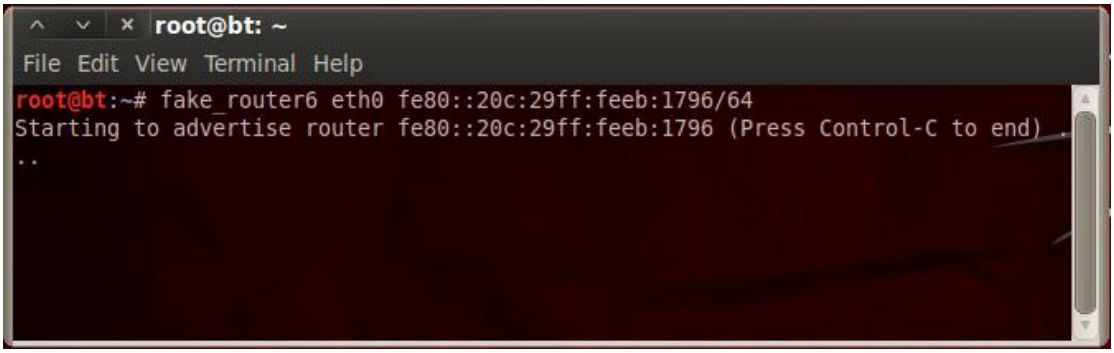


Εικόνα 13.4:Εφαρμογή alive6. Οι hosts δεν μπορούν να λάβουν IPv6 διεύθυνση

13.3 Router Redirection Attacks

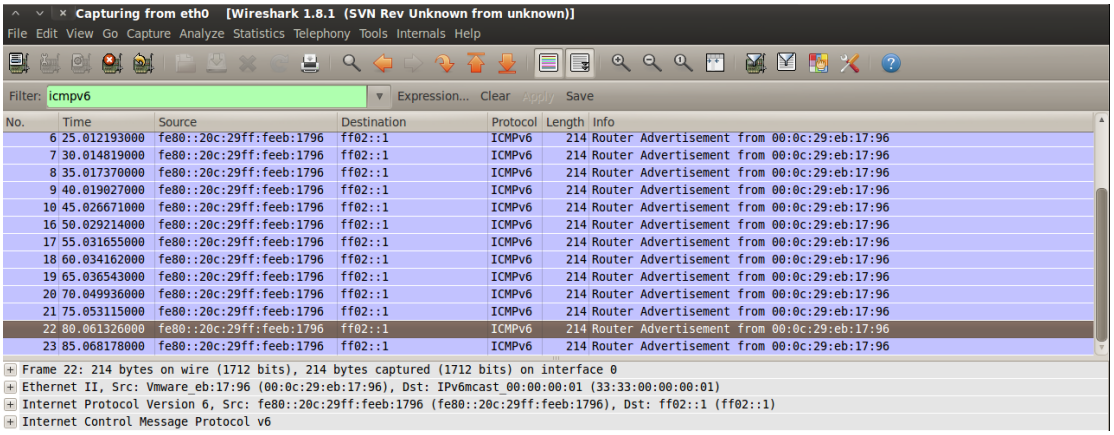
Ο επιτιθέμενος στέλνει ένα spoofed ICMP Echo Request, (χρησιμοποιώντας την διεύθυνση ενός απλού κόμβου του δικτύου - fe80::20c:29ff:fe85::54a3), στο θύμα. Το θύμα θα απαντήσει με ένα ICMP Echo reply και ο επιτιθέμενος θα εκμεταλλευτεί το συγκεκριμένο γεγονός δημιουργώντας μία πλαστή απάντηση ανακατεύθυνσης (fake redirect reply), στο θύμα, υπονοώντας ότι το συγκεκριμένο μήνυμα στάλθηκε από τον αυθεντικό δρομολογητή. Έτσι το θύμα όταν στέλνει μηνύματα στον απλό κόμβο, θα χρησιμοποιεί αυτό τον πλαστό δρομολογητή, ο οποίος στην πραγματικότητα είναι ο επιτιθέμενος. Άρα όλη η δικτυακή κυκλοφορία που ξεκινάει από το θύμα θα διέρχεται από τον επιτιθέμενο.

Αρχικά, ο επιτιθέμενος διαφημίζει τον εαυτό του, εμφανιζόμενος ως ένας δρομολογητής, χρησιμοποιώντας την εφαρμογή fake_router6 (Εικόνα 13.5).



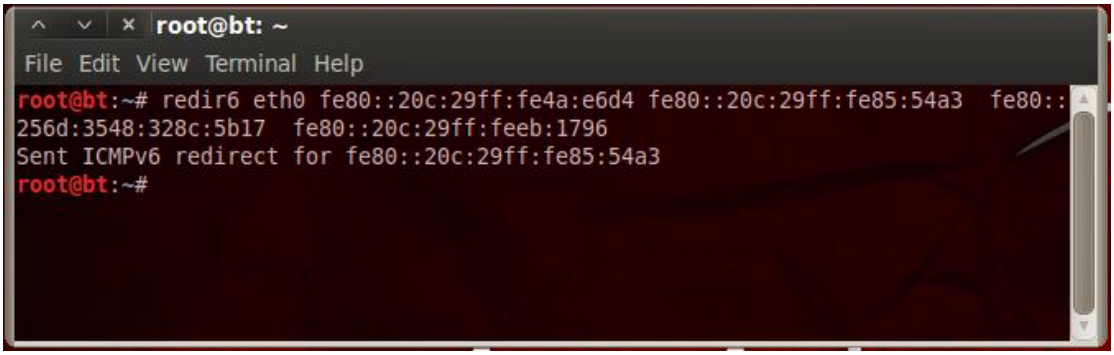
Εικόνα 13.5: Εφαρμογή fake_router6

Ένα advertised ICMPv6 πακέτο, αποστέλλεται σε όλους τους κόμβους, όπως φαίνεται στην Εικόνα 13.6.



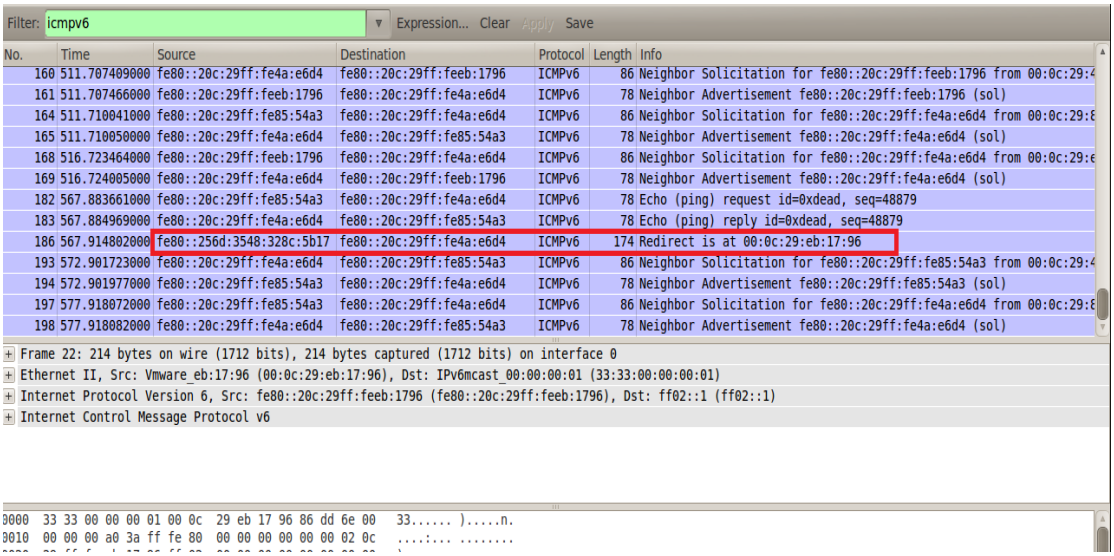
Εικόνα 13.6: Αποτελέσματα fake_router6

Το επόμενο βήμα είναι να ανακατευθύνουμε οποιαδήποτε κυκλοφορία προέρχεται από το θύμα στον απλό κόμβο, χρησιμοποιώντας ως δρομολογητή την μηχανή του επιτιθέμενου. Η συγκεκριμένη διαδικασία γίνεται με την εφαρμογή redir6 (Εικόνα 13.7).



Εικόνα 13.7: Εφαρμογή redir6

Χρησιμοποιώντας το Wireshark στην μηχανή του επιτιθέμενου, μπορούμε να δούμε το μήνυμα ανακατεύθυνσης που αποστέλλεται στο θύμα (Εικόνα 13.8).

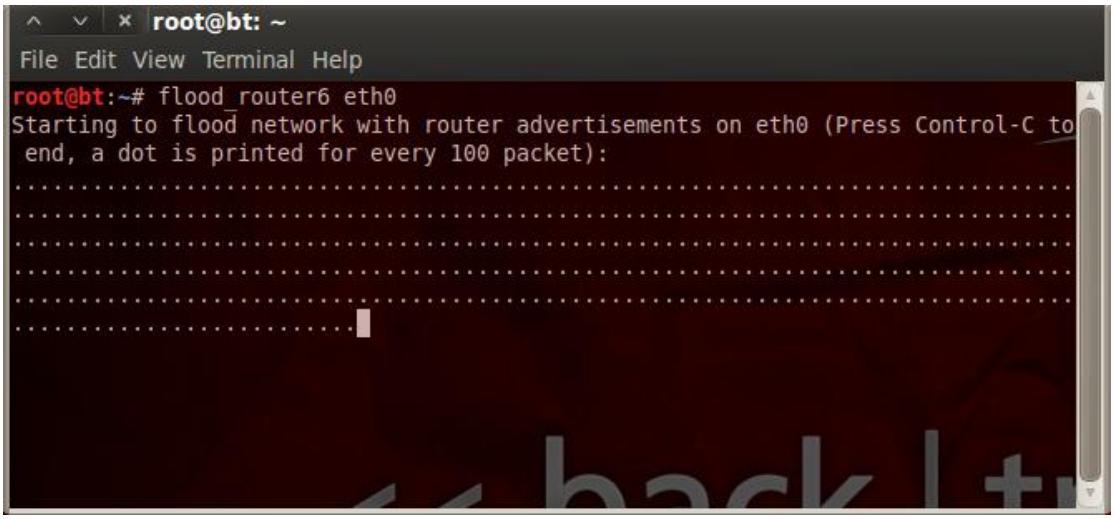


Εικόνα 13.8: Αποτελέσματα redir6

Το μήνυμα φαίνεται ότι στέλνεται από τον πραγματικό δρομολογητή (πεδίο Source), στο θύμα (πεδίο Destination), προτείνοντας την μηχανή του επιτιθέμενου ως την καταλληλότερη επιλογή για δρομολόγηση πακέτων.

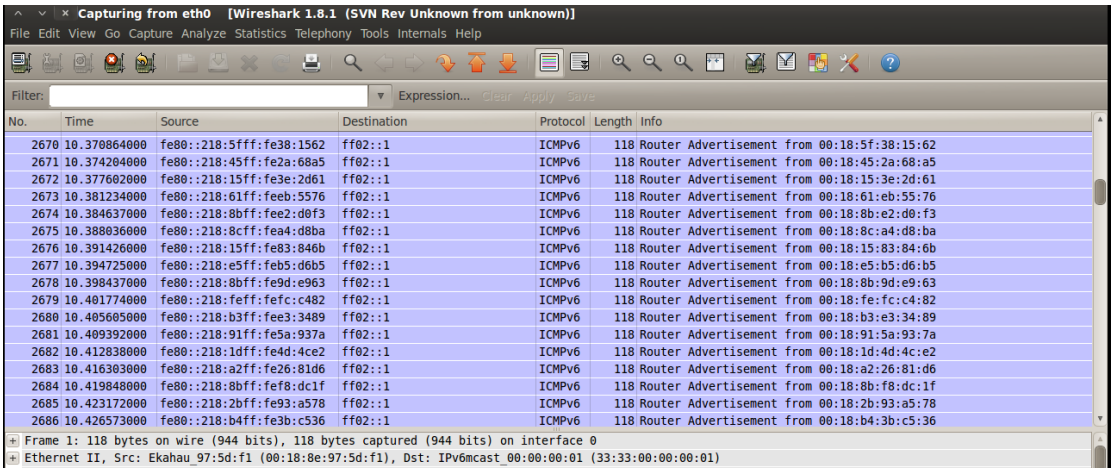
13.4 Router Advertisement Flooding Attack

Η συγκεκριμένη επίθεση βασίζεται στο γεγονός, ότι οποιοσδήποτε κόμβος έχει την δυνατότητα να στέλνει Router Advertisements (RA) μηνύματα. Ο επιτιθέμενος εκμεταλλεύεται το συγκεκριμένο γεγονός και αποστέλλει μεγάλο αριθμό RA πακέτων, με αποτέλεσμα να προκαλεί μεγάλη δικτυακή κυκλοφορία. Οι κόμβοι δεν μπορούν να επεξεργαστούν τόσο μεγάλο αριθμό πακέτων με αποτέλεσμα να γίνονται ακατάλληλοι για χρήση και να μην μπορούν να ανταποκριθούν. Ο επιτιθέμενος απλά χρησιμοποιεί την εφαρμογή flood_router6 (Εικόνα 13.9).



Εικόνα 13.9: Εφαρμογή flood_router6

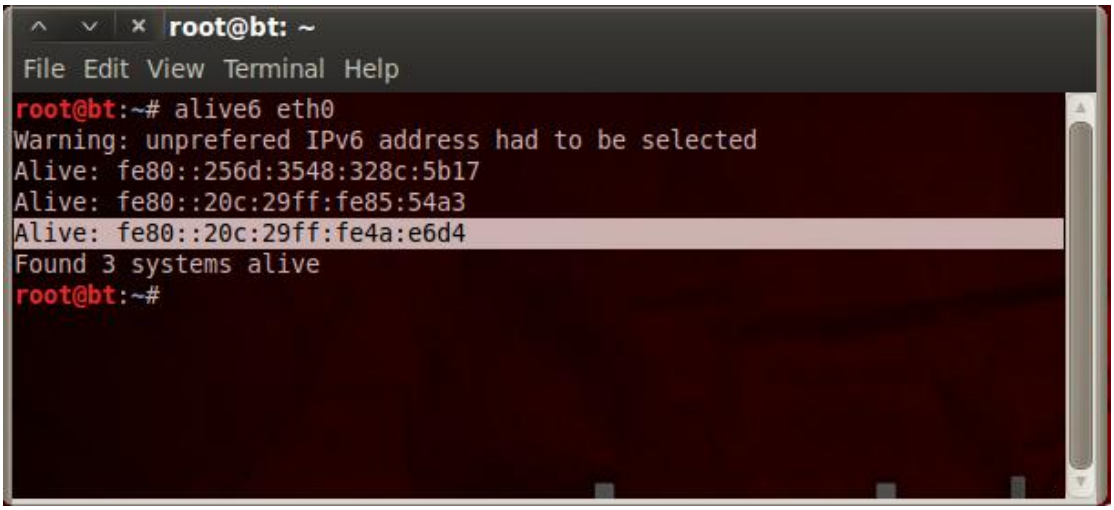
Στην Εικόνα 13.10 φαίνονται τα αποτελέσματα της συγκεκριμένης εφαρμογής.



Εικόνα 13.10: Αποτελέσματα flood_router6

13.5 Broadcast Amplification Attack (Smurf)

Κατά την διάρκεια της επίθεσης, ο επιτιθέμενος τρέχει την εφαρμογή alive6, με σκοπό να εμφανιστούν οι κόμβοι που έχουν IPv6 διεύθυνση εντός του δικτύου (Εικόνα 13.11).

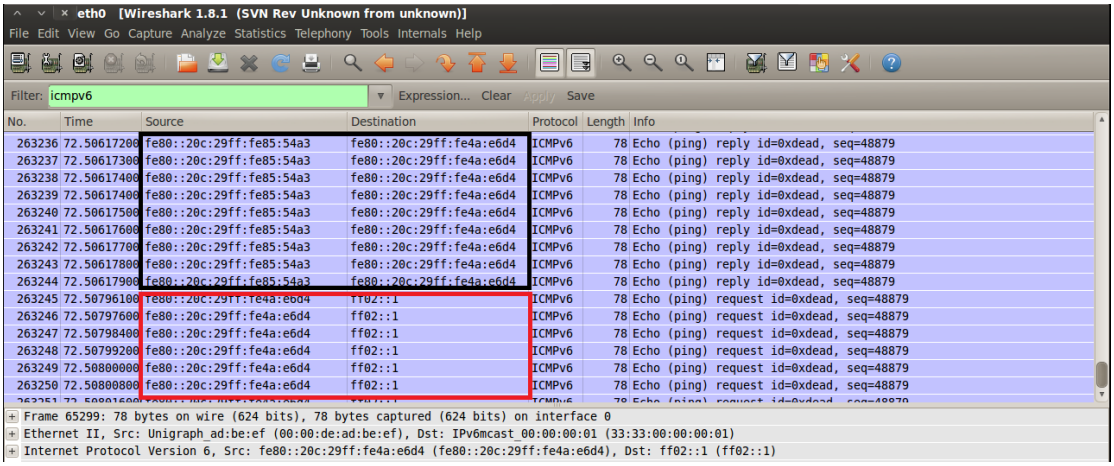


Εικόνα 13.11: Εφαρμογή alive6

Εμφανίζονται τρεις κόμβοι με IPv6 διεύθυνση. Επιλέγουμε τον κόμβο με την διεύθυνση fe80::20c:29ff:fe4a:e6d4 να είναι το θύμα της επίθεσης. Στην συνέχεια ο επιτιθέμενος τρέχει την smurf6 εφαρμογή με σκοπό να εκτελέσει την επίθεση (Εικόνα 13.12).

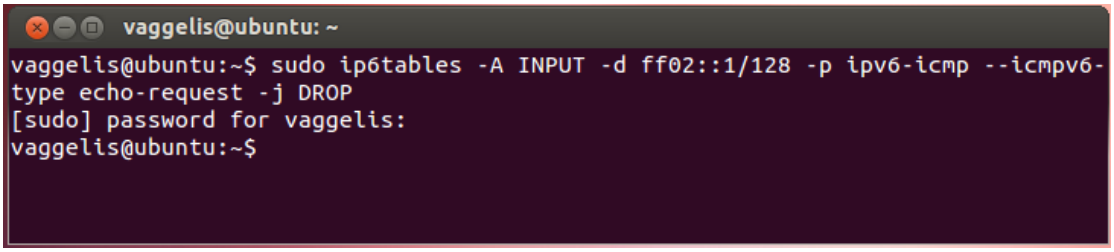
Εικόνα 13.12: Εφαρμογή smurf6

Στο σύστημα του επιτιθέμενου χρησιμοποιούμε την εφαρμογή Wireshark, με σκοπό να παρακολουθήσουμε την δικτυακή κυκλοφορία και συγκεκριμένα τα ICMPv6 requests και replies, που αποστέλλονται και λαμβάνονται από τους άλλους κόμβους του δικτύου. Όπως φαίνεται στην Εικόνα 13.13, αφού ο επιτιθέμενος τρέξει την smurf6 εφαρμογή, ο κόμβος με την διεύθυνση fe80::20c:29ff:fe85::54a3, ο οποίος παίζει τον ρόλο όλων των κόμβων που βρίσκονται εντός του δικτύου λαμβάνει ένα spoofed multicast (ff02::1/128) ICMPv6 Echo Request, το οποίο προορίζεται για όλους τους κόμβους του δικτύου, το οποίο φαίνεται ότι έχει σταλεί από την διεύθυνση του θύματος (fe80::20c:29ff:fe4a:e6d4)ενώ στην πραγματικότητα έχει σταλεί από τον επιτιθέμενο. Ο απλός κόμβος, όπως επίσης οποιοσδήποτε κόμβος βρίσκονταν στο δίκτυο, θα απαντήσει στην διεύθυνση του θύματος με ένα ICMPv6 Echo reply, όπως φαίνεται και στην εικόνα. Μπορεί εύκολα να γίνει αντιληπτό, ότι ανάλογα με το μέγεθος του δικτύου (πλήθος κόμβων), η συγκεκριμένη διαδικασία μπορεί να οδηγήσει σε μια DoS επίθεση, αφού το θύμα κατακλύζεται από μεγάλο αριθμό ICMPv6 πακέτων, τα οποία επηρεάζουν την δικτυακή του απόδοση.



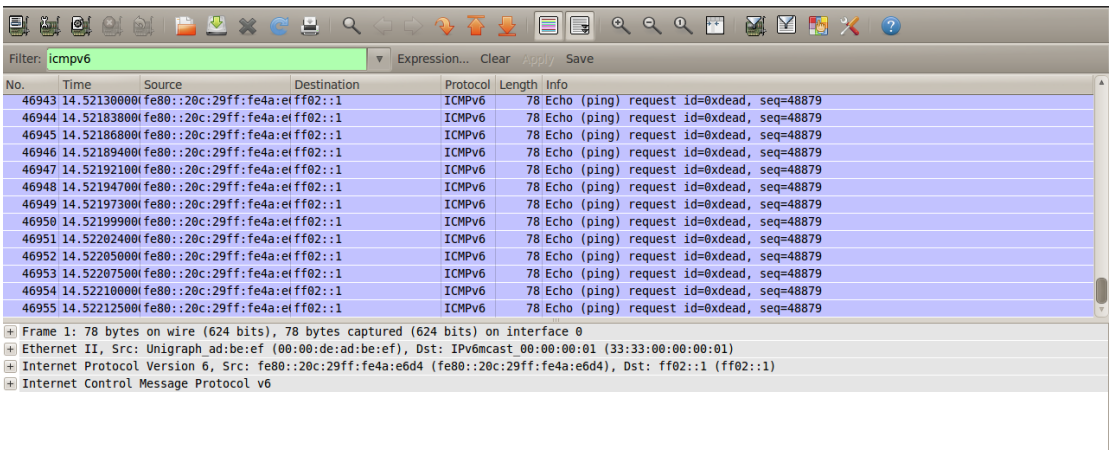
Εικόνα 13.13: Αποτελέσματα smurf6

Για την αντιμετώπιση της συγκεκριμένης απειλής το RFC 2463 προτείνει να μην δημιουργούνται απαντήσεις για τα ICMPv6 Echo Request μηνύματα με διεύθυνση προορισμού την local link multicast διεύθυνση (ff02::1/128) όλων των κόμβων. Γι’ αυτό τον λόγο χρησιμοποιούμε το ip6tables για δημιουργήσουμε έναν κανόνα φιλτραρίσματος στον υπολογιστή, που παίζει τον ρόλο του απλού host στο δίκτυο (τον ίδιο κανόνα πρέπει να εφαρμόσουμε σε κάθε host στο δίκτυο) (Εικόνα 13.14)



Εικόνα 13.14 : ip6tables κανόνας φιλτραρίσματος

Στην συνέχεια δοκιμάζεται η ίδια επίθεση (smurf6) από τον επιτιθέμενο. Στην Εικόνα 13.15, μέσω του Wireshark παρατηρούμε ότι δεν δημιουργούνται απαντήσεις (replies) στα request μηνύματα. Άρα η επίθεση μπλοκάρεται με επιτυχία μέσω του παραπάνω κανόνα φιλτραρίσματος στο ip6tables.



Εικόνα 13.15: Αποτέλεσμα smurf6 μετά από εφαρμογή κανόνα φιλτραρίσματος στο ip6tables

14

Συμπεράσματα

Η καθιέρωση του νέου πρωτοκόλλου IPv6 στην παγκόσμια διαδικτυακή κοινότητα αποτελεί πλέον αναγκαιότητα λόγω της εξάντλησης των διευθύνσεων IPv4. Το πρωτόκολλο IPv6 παρουσιάζει δύο όψεις ως προς τον τομέα της ασφάλειας. Αντιμετωπίζει αποτελεσματικά μια σειρά από επιθέσεις, οι οποίες λαμβάνουν χώρα στο προγενέστερο IPv4 (για παράδειγμα fragmentation επιθέσεις στους ενδιάμεσους κόμβους), ωστόσο παρουσιάζει νέες ευπάθειες, κυρίως μέσω των νέων πρωτοκόλλων και υπηρεσιών που προσφέρει, όπως Neighbor Discovery και Stateless Address Auto-configuration.

Οι ευπάθειες που προκύπτουν από τα νέα πρωτόκολλα δεν μπορούν να αντιμετωπιστούν αποτελεσματικά από τα ήδη υπάρχοντα μέτρα προστασίας. Γι’ αυτό το λόγο οι ερευνητές έστρεψαν το ενδιαφέρον τους στην δημιουργία ενός νέου πρωτοκόλλου για την αντιμετώπιση επιθέσεων στο Neighbor Discovery. Το νέο πρωτόκολλο είναι το Secure Neighbor Discovery, το οποίο μέσω των Cryptographically Generated Addresses, δίνει απαντήσεις σε νέες επιθέσεις τύπου Duplicate Address Detection Attack.

Επιπλέον, οι ερευνητές οφείλουν να προσαρμόσουν τα ήδη υπάρχοντα μέτρα (κυρίως IPsec και Firewalls) στις νέες απαιτήσεις που φέρει το IPv6. Το IPsec δεν παρουσιάζει καμία απολύτως διαφορά στο IPv6. Πολύ θεωρούν ότι το IPv6 είναι πιο ασφαλές από το IPv4, διότι το IPsec είναι υποχρεωτικό στο IPv6. Η συγκεκριμένη άποψη προκαλεί σύγχυση και είναι λανθασμένη, διότι η υλοποίηση του IPsec είναι υποχρεωτική στο IPv6 και όχι η χρήση του. Αυτό σημαίνει ότι όλοι οι κόμβοι έχουν την δυνατότητα να υλοποιήσουν το IPsec μέσω των Extension Header (AH και ESP) που προσφέρει το IPv6, αλλά η εφαρμογή αυτών των Extension Header είναι προαιρετική. Από την άλλη τα Firewalls στο IPv6 παρουσιάζουν σχεδιαστικές προκλήσεις. Γίνονται σημαντικές προσπάθειες στον σχεδιασμό και υλοποίηση Firewalls, τα οποία να μπορούν να επιθεωρήσουν κρυπτογραφημένα πακέτα, όταν γίνεται χρήση του IPsec. Επιπλέον, νέες πολιτικές ασφάλειας πρέπει να εφαρμοστούν, ώστε να επιτρέπεται η κυκλοφορία στα ICMPv6 πακέτα, τα οποία είναι απαραίτητα για την ορθή λειτουργία πρωτοκόλλων, όπως το Neighbor Discovery. Ένα άλλο σημαντικό ζήτημα που έχουν να αντιμετωπίσουν τα Firewalls είναι ο έλεγχος ενθυλακωμένων πακέτων, το οποίο αποτελεί συχνό φαινόμενο όταν γίνεται χρήση tunneling μηχανισμών.

Σχετικά με την υλοποίηση του IPsec και του Easy-SEND έχουμε τα εξής αποτελέσματα: Εφαρμόσαμε το IPsec σε ένα τοπικό δίκτυο και τα αποτελέσματα ήταν θετικά. Τα μηνύματα που ανταλλάσσαμε ήταν κρυπτογραφημένα μέσω του ESP. Ωστόσο, η διαχείριση κλειδιών έγινε χειροκίνητα. Κάτι τέτοιο είναι μη πρακτικό σε μεγάλης κλίμακας δίκτυα, όπως είναι τα IPv6 περιβάλλοντα. Η εφαρμογή έγινε για εκπαιδευτικούς λόγους και δεν μπορεί να εφαρμοστεί σε μεγάλα δίκτυα. Όσον αφορά το πρωτόκολλο SEND, γίνονται

συνεχόμενες έρευνες, με ιδιαίτερη έμφαση στις CGA διευθύνσεις. Παρ’ όλο τις θεωρητικές έρευνες και αναλύσεις, δεν υπάρχουν αξιόλογες υλοποιήσεις του SEND. Η Easy-SEND εφαρμογή που χρησιμοποιήσαμε μας έδωσε τα αποτελέσματα που επιθυμούσαμε, ωστόσο δεν μπορεί να εφαρμοστεί σε πραγματικά εταιρικά περιβάλλοντα και σε δίκτυα μεγάλων οργανισμών. Σχετικά με τις επιθέσεις που υλοποιήσαμε, κάναμε χρήση του εργαλείου THC-IPv6-Attack-Toolkit. Είναι το μοναδικό εργαλείο υλοποίησης επιθέσεων στο πρωτόκολλο IPv6, το οποίο ενσωματώνει μια σειρά από εφαρμογές. Η χρήση του THC είναι σχετικά εύκολη, καθώς οι εφαρμογές του ενσωματώνονται στο Bakctrack και μπορούν να εκτελεστούν με μεγάλη επιτυχία.

Η απάντηση στο ερώτημα-ποιο από τα δύο πρωτόκολλα είναι πιο ασφαλές;-αποτελεί δύσκολο εγχείρημα. Δεν μπορούμε να δώσουμε ολοκληρωμένη και τεκμηριωμένη απάντηση, διότι το μεν IPv4 είναι δοκιμασμένο πάνω από 20 χρόνια, το δε IPv6 είναι ένα νέο πρωτόκολλο, το οποίο δεν έχει ωριμάσει. Οι επιθέσεις και τα μέτρα ασφάλειας στο IPv4 είναι γνωστά, σε αντίθεση με το IPv6, το οποίο δεν έχει λειτουργήσει αυτόνομα, άρα δεν έχει παρουσιάσει όλες τις πιθανές ευπάθειες που ενδεχομένως κρύβει. Το μόνο σίγουρο είναι ότι το νέο πρωτόκολλο, έχει κεντρίσει το ενδιαφέρον των επιτιθέμενων, με αποτέλεσμα νέες επιθέσεις να εμφανίζονται και νέα μέτρα ασφάλειας να απαιτούνται. Οι ερευνητές οφείλουν να στρέψουν την προσοχή τους στους μηχανισμούς μετάβασης από το IPv4 στο IPv6, καθώς εκτιμάται ότι τα δύο πρωτόκολλα θα συνυπάρχουν για αρκετά μεγάλο χρονικό διάστημα.

15

Αναφορές – Βιβλιογραφία

Παρακάτω ακολουθούν οι βιβλιογραφικές πηγές που χρησιμοποιήθηκαν στην παρούσα μεταπτυχιακή διπλωματική εργασία. Το πρότυπο σύμφωνα με το οποίο συντάχθηκαν οι βιβλιογραφικές πηγές είναι το "ISO 690 – Numerical Reference".

[1]. **Choudhary A.R,** "In-depth Analysis of IPv6 Security Posture", *Collaborative Computing: Networking, Applications and Worksharing, 5th International Conference,* pp. 1-7, November 2009

[2]. **Caicedo C.E, Joshi J.B.D., Tuladhar S.R.,** "IPv6 Security Challenges", *Computer*, IEEE Computer Society, Vol. 42, No. 2, pp. 36-42, February 2009

[3]. **Szigeti S., Risztics P.,** "Will IPv6 bring better security?", *Euromicro Conference,2004.Proceeding.30th* , pp. 532-537, 2004

[4]. **Zagar D., Grgić K., Rimac-Drlje.,** "Security aspects in IPv6 networks – implementation and testing", *Computers & Electrical Engineering*, Vol. 33, No. 5-6, pp. 425-437, September 2007

[5]. **Radhakrishman R., Jamil M., Mehfuz S., Moinuddin M.,** "Security issues in IPv6", *3th International Conference on Networking and Services (ICNS)*, IEEE Computer Society, pp. 110-114, Greece 2007

[6]. **Heidari M.,** "IPv6 Security Considerations" (article), September 2004

[7]. **Shin M.K., Kim H.J., Santay D., Montgomery D.,** "An Empirical Analysis of IPv6 Transition Mechanisms", *Advanced Communication Technology, 2006. ICACT 2006, The 8th International Conference*, No.6, pp. -1996, February 2006

[8]. **Hermann-Setton P.,** "Security Features in IPv6", *SANS Institute Information Security Reading Room*, GIAC GSEC Practical Assignment v1.4, Option 1, 2002

[9]. **Huitema C.,** *Routing in the Internet (2nd Edition)*, Prentice Hall,
December 1999

[10]. **Kozierok C.M.,** *IPv6 Datagram Main Header Format*, *tcpipguide.com Website*. Version 3.0, [Online] September 20, 2005. [Accessed: November, 2012.]

http://www.tcpipguide.com/free/t_IPv6DatagramMainHeaderFormat.htm

[11]. **Gai S.,** *Internetworking IPv6 with Cisco Routers*, McGraw-Hill Computer Communications Series, March 1998

[12]. **Microsoft Windows Server TechCenter,** *IPv6 Address Types, technet.microsoft.com Website.* [Online] March 28, 2003. [Accessed: November, 2012.] http://technet.microsoft.com/en-us/library/cc757359%28WS.10%29.aspx

[13]. **Narten T., Nordmark E., Simpson W.,** *Neighbor Discovery for IP Version 6 (IPv6)*, RFC 2461, IETF, December 1998

[14]. **Arkko J., Aura T., Kempf J., Mäntylä V., Nikander P., Roe M.,** "Securing IPv6 Neighbor and Router Discovery", *in Proceedings of the 1st ACM workshop on Wireless Security*, pp. 77-86, 2002

[15]. **Stallings W.,** *ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ: Εφαρμογές και πρότυπα,* τρίτη αμερικάνικη έκδοση, Κλειδάριθμος, Αθήνα 2008

[16]. **Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ.,** *Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν και Ηλεκτρονικής Διακυβέρνησης*, Παπασωτηρίου, Αθήνα 2003

[17]. **The Government of the HKSAR** (*Hong Kong Special Administrative Region)*, "IPv6 SECURITY", February 2008

[18]. **Convery S., Miller D.,** "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)", *Cisco Systems*, 2004

[19]. **Open Web Application Security Project,** *Network Eavesdropping*, *owasp.org Website.* [Online] July 10, 2012. [Accessed: December, 2012.] https://www.owasp.org/index.php/Network_Eavesdropping

[20]. **Douligeris C., Mitrokosta A.,** "DDoS attacks and defense mechanisms: classification and state-of-the-art", *Computer Networks,* Elsevier Science, Vol.44, 2004

[21]. **Landesman M.,** *What are Social Engineering Attacks?, antivirus software Website.* [Online] October 10, 2008. [Accessed: December, 2012.] http://antivirus.about.com/b/2008/10/10/what-are-social-engineering-attacks.htm

[22]. **OpenSourceProject.org.cn** , *Brute Force Attack*, *OpenSourceProject.org.cn Website.*[Accessed:December,2012.] http://book.opensourceproject.org.cn/sysadmin/apache/prewebattacks/opensource/0321321286/ch07lev1sec4.html

[23]. **Thomson S., Narten T.,** *IPv6 Stateless Address Autoconfiguration,* RFC 2462, IETF, December 1998

[24]. **Ramblings S.,** *IPv6 Challenges, stephanfreeman.wordpress.com Website.* [Online] March 21, 2011. [Accessed: December, 2012.]
http://stephanfreeman.wordpress.com/2011/03/21/ipv6-challenges/

[25]. **Kozierok C.M.,** *ICMPv6 Neighbor Advertisement and Neighbor Solicitation Messages*, *tcpipguide.com Website*. Version 3.0, [Online] September 20, 2005. [Accessed: November, 2012.]
http://www.tcpipguide.com/free/t_ICMPv6NeighborAdvertisementandNeighborSolicitation.htm

[26]. **Kozierok C.M.,** *TCP/IP IPv6 Neighbor Discovery Protocol (ND)*, *tcpipguide.com Website*. Version 3.0, [Online] September 20, 2005. [Accessed: November, 2012.]
http://www.tcpipguide.com/free/t_TCPIPIPv6NeighborDiscoveryProtocolND.htm

[27]. **Wikipedia The Free Encyclopedia,** *IPv4 address exhaustion, en.wikipedia.org Website.* [Online] December 15, 2012. [Accessed: January, 2013.]
http://en.wikipedia.org/wiki/IPv4_address_exhaustion

[28]. **Narten T., Draves R.,** *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, RFC 3041, IETF, January 2001

[29]. **Lindqvist J.,** "IPv6 is Bad for your Privacy", *defcon 15*, Las Vegas, August 2007

[30]. **Conta A., Deering S.,** *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, RFC 2463, IETF, December 1998

[31]. **Martin C., Dunn J.,** "INTERNET PROTOCOL VERSION 6(IPV6) PROTOCOL SECURITY ASSESSMENT", *Military Communications Conference, 2007.MILCOM,* pp.1-7, USA, October 2007

[32]. **Shannon C., Moore D., Claffy K.,** "Characteristics of Fragmented IP Traffic on Internet Links", *in Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, pp.83-97, USA 2001

[33]. **Hogg S., Vyncke E.,** *IPv6 Security (1st Edition)*, Cisco Press, USA 2008

[34]. **Yang D., Song X., Guo Q.,** "Security on IPv6", *Advanced Computer Control (ICACC), 2010 2nd International Conference*, pp. 323-326, China, March 2010

[35]. **Tuomas A.,** "Cryptographically Generated Addresses (CGA)", In Proc. *6th Information Security Conference (ISC'03),* Vol. 2851 of LNCS, pp. 29-43, Springer, United Kingdom, October 2003

[36]. **Balchunas A.,** "IPv6 Addressing v1.11", *routeralley,* 2006

[37]. **Nikander P.,** "A Scalable Architecture for IPv6 Address Ownership", *Internet Draft* (2001)

[38]. **Shalini D., Sankaranarayanan K.,** "IPv4/IPv6 Transition Mechanisms", *European Journal of Scientific Research*, Vol. 34, No. 1, pp. 110-124, 2009

[39]. **Hagen S.,** *IPv6 Essentials*, O'Reilly, July 2002

[40]. **Wang K., Yeo A.K., Ananda A.L.,** "DTTS: a Transparent and Scalable Solution for IPv4 to IPv6 Transition", *Proceedings of the 10th International Conference on Computer Communications and Networks*, pp. 248-253, 2001

[41]. **Taib A.H.M., Budiarto R.,** "Security Mechanisms for the IPv4 to IPv6 Transition", *5th Student Conference on Research and Development – SCOReD 2007*, pp.1-6, Malaysia, December 2007

[42]. **Kempf J.**, **Nordmark E.**, "Threat Analysis for IPv6 Public Multi-Access Links," draft-kempf-netaccess-threats-00.txt,work in progress, 2002

[43]. **Tsirtsis G., Srisuresh P.,** *Network Address Translation – Protocol Translation (NAT-PT)*, RFC 2766, IETF, February 200

[44]. **Egevang K., Francis P.,** *The IP Network Address Translator (NAT)*, RFC 1631, IETF, May 1994

[45]. **Carpenter B., Jung C.,** *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*, RFC 2529, IETF, March 1999

[46]. **Durand A., Fasano P., Guardini I., Lento D.,** *IPv6 Tunnel Broker*, RFC 3053, IETF, January 2001

[47]. **Wikipedia The Free Encyclopedia,** *6to4*, *enwikipedia.org Website*. [Online] June 27, 2011. [Accessed: December, 2012.]
http://en.wikipedia.org/wiki/6to4

[48]. **Savola P., Patel C.,** *Security Considerations for 6to4*, RFC 3964, IETF, December 2004

[49]. **Wikipedia The Free Encyclopedia,** *Teredo Tunneling, enwikipedia.org Website.* [Online] June 6, 2011. [Accessed: December, 2012.]
http://en.wikipedia.org/wiki/Teredo_tunneling

[50].**Microsoft Windows Server TechCenter,** *Teredo Overview, technet.microsoft.com Website.* [Online] January 01, 2003. (update 2007) [Accessed: December, 2012.] http://technet.microsoft.com/en-us/library/bb457011.aspx

[51]. **Huitema C.,** *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*, RFC 4380, IETF, February 2006

[52]. **Minoli D., Kouns J.,** *Security in an IPv6 Environment (1st Edition)*, Auerbach Publications, USA 2008

[53]. **Cisco Systems,** "Dual Stack IPv4/IPv6 Devices", 2010

[54]. **Achat v0.150 Beta 7,** [Online] September 30, 2010. [Accessed: December, 2012.] http://www.afterdawn.com/software/network/instant_messaging/achat.cfm#description

[55]. **Alsa A., Meinel S.,** "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations", *IEEE Security & Privacy Magazine,* Vol. 10, No. 4, pp. 26-34, August 2012

[56]. **Easy-SEND,** [Online] February 18, 2011. [Accessed: March, 2013] http://sourceforge.net/projects/easy-send/

[57]. **THC-IPv6-Attack-Toolkit v2.1,** [Online] January 21, 2013. [Accessed: February, 2013] http://www.thc.org/thc-ipv6/