ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μετάβαση από IPv4 σε IPv6

Λάμπρος Π. Δημόπουλος

Επιβλέποντες: **Παναγιώτης Γεωργιάδης,**Καθηγητής

ΑΘΗΝΑ

ΙΟΥΛΙΟΣ 2011

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μετάβαση από το IPV4 στο IPV6

Λάμπρος Π. Δημόπουλος
Α.Μ.: 1023

ΕΠΙΒΛΕΠΟΝΤΕΣ: Παναγιώτης Γεωργιάδης,Καθηγητής

Ιούλιος 2011

ΠΕΡΙΛΗΨΗ

Με τη παρούσα εργασία γίνεται μια προσπάθεια προσέγγισης σε θέματα που άπτονται τη μετάβαση από το IPv4 στο IPv6. Αρχικά γίνεται μια αναφορά στα στοιχεία εκείνα που κάνουν επιτακτική ανάγκη την μετάβαση από το ένα πρωτόκολλο στο άλλο κάνοντας σχετικές αναφορές στα δύο πρωτόκολλα.Στη συνέχεια γίνεται μια ανάλυση της δομής αλλά και της λειτουργίας του πρωτοκόλλου IPv6.Γίνεται εκτενής αναφορά στη δομή μιας διευθυνσης IPv6 και αναλύνται όλα τα χαρακτηριστικά της.Στη συνέχεια και στο κεφάλαιο 3 αναλύονται οι μηχανισμοί που θα οδηγήσουν μια ασφαλή μεταφορά από το ένα πρωτόκολλο στο άλλο.Αναλύονται τρόποι όπως dual stack,tunneling,translation καθώς και αναπτύσεται το 6to4 μηχανισμος.

Στα κεφάλαια 4 και 5 γίνεται αναφορά σε θέματα ασφαλείας του πρωτοκόλλου IPv6 Αφού τα εξετάσαμε, είδαμε το πώς μπορεί ένα πρωτόκολλο να πέσει θύμα κακόβουλης ενέργειας. Περιγράψαμε και ομαδοποιήσαμε αυτές τις επιθέσεις. Έπειτα αναλύσαμε το IPSec, ένα ευρέως διαδεδομένο πρωτόκολλο για να ασφαλίζει το IP, το οποίο προσαρμόζεται ανάλογα με τις ανάγκες. Εξετάσαμε τα πρωτόκολλα σχετικά με τις επιθέσεις, είδαμε ποιες αρχές ασφάλειες προσφέρουν, και όπου κρίθηκε αναγκαίο εφαρμόσαμε χαρακτηριστικά του IPSec. Τέλος συνοψίσαμε τα συμπεράσματα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ:Πρωτόκολλα μεταφοράς,IPv4,IPv6,IPsec,διευθυνσιοδότηση,διπλή στοίβα,,tunneling,δρομολογητής,κόμβος

ABSTRACT

This present work aims to approach issues related to the transition from IPv4 to IPv6. First Of all there is a a reference to the elements that make imperative the transition from one protocol to another by making references tothese protocolls.After there is an analysis of the structure and operation of the IPv6 protocol.It is being an extensive reference and analization to the structure of an IPv6 address. In Chapter 3 we examine the mechanisms that will lead to a safe transfer from one protocolto another with ways such as as dual stack,tunneling,translation,develops6to4

In Chapters 4 and 5 there are references about security issues of IPv6.After the examination of IPV6 we saw how it is possible to be a victim to malicious action. Then we described and grouped these attacks. In continueing we analyze the IPSec, a widely used protocol for securing the IP, which can be adapted to needs. We reviewed the protocols that are connected with attacks, and we saw which authorities have insurance offer, and where it was necessary we applied characteristics of IPSec. Finally we have summarized the findings of this exercise.

KEY WORDS: Transmission protocol,IPv4,IPv6,IPsec,adressing ,dual stack,,tunneling,router,node

ΕΥΧΑΡΙΣΤΙΕΣ

Θερμές ευχαριστίες στο καθηγητή κ. Γεωργιάδη Παναγιώτη που μου έδωσε την ευκαρία να ασχοληθώ μα το συγκεκριμένο αντικείμενο καθώς και για τις χρήσιμες και πολύτιμες συμβουλές του.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Κάθε συσκευή που συνδέεται στο Ίντερνετ απαιτεί μια μοναδική αριθμητική διεύθυνση. Το IPv4, το σημερινό σύστημα απόδοσης αριθμών χρησιμοποιείται από το 1977 και είναι ικανό να δημιουργήσει 4 δισεκατομμύρια διαφορετικές διευθύνσεις. Όμως, οι ειδικοί λένε ότι η συντριπτική πλειονότητά τους έχει ήδη αποδοθεί, σε τέτοιο βαθμό που θεωρείται πλέον πιθανό να δημιουργηθεί μια μαύρη αγορά για τη διάθεση των λιγοστών ακόμα διαθέσιμων.

Από την άλλη, η επόμενη έκδοση του πρωτοκόλλου, το IPv6, μπορεί να παράξει απίστευτα μεγαλύτερο αριθμό διευθύνσεων (340τρισεκατομμύρια τρισεκατομμυρίων τρισεκατομμύρια ;-), τόσων που αν οι 4 δισ. διευθύνσεις του IPv4 χωρούσαν σε... ένα Blackberry, οι διευθύνσεις του IPv6 θα χρειάζονται ολόκληρη τη Γη.

Εντούτοις, το σημερινό σύστημα δεν είναι συμβατό με το νέο και ως εκ τούτου θα έπρεπε να μεσολαβήσει μια μεταβατική περίοδος συνύπαρξης του IPv4 και του IPv6. Η ασυμβατότητα αυτή είναι που θα εμπόδιζε έναν υπολογιστή που έχει αριθμητική διεύθυνση IP σύμφωνα με το IPv6 να δει ένα σάιτ που εξυπηρετείται από έναν server που έχει αριθμητική διεύθυνση με το IPv4, αν προηγουμένως δεν μεσολαβούσε ένας «μεταφραστής» της διεύθυνσής του.

Επίσης, η μετάβαση έχει κόστος για τους παρόχους ιντερνετικών υπηρεσιών (τους ISP και όχι μόνο), καθώς θα πρέπει να επενδύσουν σε χρήμα και χρόνο και να διατηρήσουν σε λειτουργία και το παλιό σύστημα παράλληλα με το νέο. Επίσης, σημαντικές επενδύσεις θα πρέπει να γίνουν για την μετάβαση στο νέο σύστημα διαδικτυακών υπηρεσιών και εφαρμογών. Ωστόσο, το μόνο «κίνητρο» για να εγκριθούν αυτές οι επενδύσεις είναι η αναγκαιότητα της μετάβασης, γι'αυτό είναι παραδεκτό ότι η υιοθέτηση του IPv6 δεν προχωράει με τους απαιτούμενους ρυθμούς, χωρίς ωστόσο η ανεπάρκεια διευθύνσεων να αποτελεί ανασταλτικό παράγοντα σύνδεσης ολοένα περισσότερων συσκευών στο Ίντερνετ.

Από την άλλη, κακώς το υπαρκτό αυτό πρόβλημα συγκρίνεται με τον λεγόμενο «ιό του 2000» -η ημέρα που θα στερέψουν οι ιντερνετικές διευθύνσεις δεν είναι σαφώς ορισμένη αν και πολύς λόγος γίνεται για το 2012, ενώ διάφορες μέθοδοι έχουν ήδη επινοηθεί για να το επιλύσουν προσωρινά -να επαναχρησιμοποιηθούν διευθύνσεις του IPv4 που έχουν δεσμευτεί αλλά δεν χρησιμοποιούνται είτε να μοιράζονται την ίδια IP διαφορετικές συσκευές.

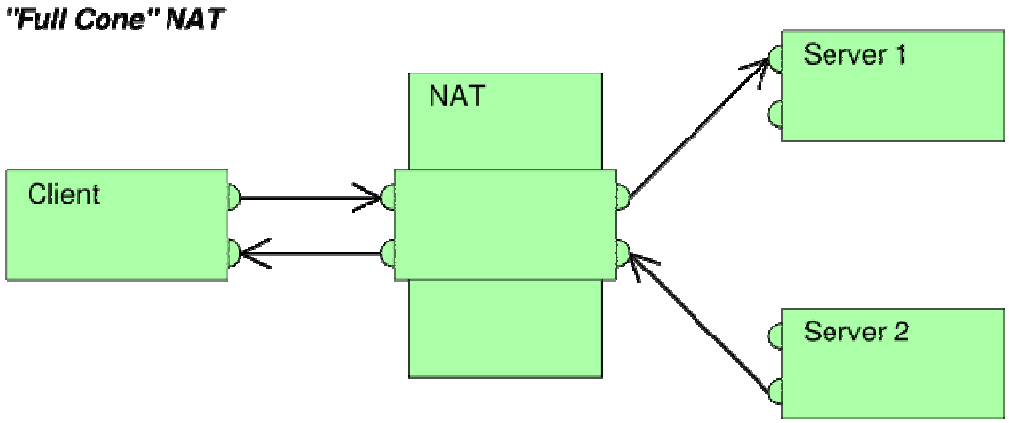
Επιπλέον, η αλλαγή του συστήματος αριθμοδότησης δεν είναι η πρώτη την οποία υφίσταται το Ίντερνετ: από το dial-up περάσαμε στο DSL, από τα αρχεία σε host στο μητρώο διευθύνσεων. Αν και πιο περίπλοκο θέμα, η μετάβαση στο IPv6 θα γίνει.

1.-ΕΙΣΑΓΩΓΗ

1.1. Γενικά-Ανάγκες Μετάβασης- Σύγκριση IPv4 με IPv6

Η παρούσα έκδοση του πρωτοκόλλου IP (γνωστή ως έκδοση 4 ή IPv4) παραμένει ουσιαστικά ως έχει από τη δημοσίευση του εντύπου RFC 791 το 1981. Το πρωτόκολλο IPv4 αποδείχτηκε εύκολα υλοποιήσιμο και λειτουργικό ανεξαρτήτως πλατφόρμας υλοποίησής του. Όμως, ο αρχικός σχεδιασμός του πρωτοκόλλου δεν είχε λάβει υπ' όψη του τους παρακάτω παράγοντες:

- Την πρόσφατη, ταχύτατη –με εκθετικό ρυθμό- ανάπτυξη του διαδικτύου και τη συνακόλουθη εξάντληση του χώρου διευθύνσεων του πρωτοκόλλου IPv4. Οι IPv4 διευθύνσεις που έχουν απομείνει προς διάθεση είναι πλέον τόσο λίγες, ώστε κάποιοι οργανισμοί έχουν αναγκαστεί να χρησιμοποιούν το πρωτόκολλο NAT (Network Address Translator), το οποίο αντιστοιχεί πολλές ιδιωτικές («ψεύτικες», «αόρατες» για τους χρήστες των λοιπών δημοσίων IPv4 διευθύνσεων) IP διευθύνσεις σε μια δημόσια IPv4,διεύθυνση



Σχήμα 1. Απεικόνιση δικτύου NAT.

- Παρ' ότι όμως το πρωτόκολλο NAT επιλύει ένα μέρος του προβλήματος, έχει αρκετά μειονεκτήματα. Συγκεκριμένα, δεν υποστηρίζει την προτυποποιημένη ασφάλεια σε επίπεδο στρώματος δικτύου, η αντιστοίχιση των ιδιωτικών διευθύνσεων σε μια δημόσια δε γίνεται σωστά στα πρωτόκολλα που ανήκουν στα ανώτερα επίπεδα της στοίβας πρωτοκόλλων του δικτύου και μπορεί να δημιουργηθούν προβλήματα κατά τη διασύνδεση δύο οργανισμών, οι οποίοι χρησιμοποιούν ιδιωτικό χώρο διευθύνσεων. Τέλος ακόμα και αν δε ληφθούν υπ' όψη τα παραπάνω μειονεκτήματα, η εκθετική αύξηση των μηχανημάτων που απαιτούν IP διευθύνσεις, αργά ή γρήγορα θα οδηγήσει στην εξάντληση και των επιπλέον διευθύνσεων που προσφέρονται μέσω του πρωτοκόλλου NAT.
- Την ανάπτυξη του διαδικτύου και ικανότητα των δρομολογητών του δικτύου κορμού του διαδικτύου να διατηρούν μεγάλους πίνακες δρομολόγησης. Λόγω του τρόπου με τον οποίο διανέμονται οι διευθύνσεις δικτύου στο IPv4 υπάρχουν πάνω από 70000 καταχωρήσεις διαδρομών στους δρομολογητές του δικτύου κορμού του διαδικτύου. Η παρούσα υποδομή για τη δρομολόγηση στο πρωτόκολλο IPv4 είναι συνδυασμός επίπεδης και ιεραρχικής δρομολόγησης.
- Η ανάγκη για απλούστερη ρύθμιση παραμέτρων. Οι περισσότερες από τις παρούσες υλοποιήσεις του πρωτοκόλλου IPv4 απαιτούν η ρύθμιση των

μηχανημάτων του δικτύου να γίνεται είτε με μη αυτόματο τρόπο, είτε με τη χρήση stateful address configuration protocols, όπως το πρωτόκολλο DHCP (Dynamic Host Configuration Protocol). Λόγω της παρουσίας πολύ περισσότερων μηχανημάτων που θα χρησιμοποιούν IP διευθύνσεις, υπάρχει ανάγκη να βρεθεί ένας απλούστερος και πιο αυτοματοποιημένος τρόπος ρύθμισης των IP διευθύνσεων και των άλλων παραμέτρων του δικτύου, ο οποίος δε θα επαφίεται στη διαχείριση μιας υποδομής βασισμένης στο πρωτόκολλο DHCP.

- Η αναγκαιότητα ασφάλειας στο επίπεδο IP της στοίβας πρωτοκόλλου δικτύου. Η προσωπική επικοινωνία πάνω από ένα δημόσιο μέσο, όπως είναι το διαδίκτυο απαιτεί υπηρεσίες κρυπτογράφησης, οι οποίες θα προστατεύουν τα δεδομένα που αποστέλλονται από υποκλοπή ή παραποίηση κατά τη μεταφορά τους. Παρ' όλο που υπάρχει ένα πρότυπο ασφαλείας στο πρωτόκολλο IPv4, γνωστό ως πρωτόκολλο (IPsec), το πρότυπο αυτό δεν είναι υποχρεωτικό να ακολουθείται και υπάρχουν συχνά διαφορετικές, μη συμβατές μεταξύ τους υλοποιήσεις.
- Η ανάγκη για καλύτερη υποστήριξη ροής δεδομένων σε πραγματικό χρόνο, γνωστή ως εξασφάλιση ποιότητας υπηρεσίας (QoS Quality of Service). Ενώ υπάρχει το πρότυπο για την υποστήριξη εξασφάλισης ποιότητας υπηρεσίας στο πρωτόκολλο IPv4, η υποστήριξη ροής δεδομένων σε πραγματικό χρόνο βασίζεται στο πεδίο είδος υπηρεσίας (TOS) του πρωτοκόλλου IPv4 και την ταυτοποίηση του φόρτου χρησιμοποιώντας μια θύρα του πρωτοκόλλου TCP ή UDP. Δυστυχώς, το πεδίο είδος υπηρεσίας του πρωτοκόλλου IPv4 έχει περιορισμένη λειτουργικότητα και ανά τα χρόνια υπήρξαν διάφορες τοπικές ερμηνείες του. Επίσης η ταυτοποίηση του φόρτου χρησιμοποιώντας θύρες των πρωτοκόλλων TCP και UDP δεν είναι δυνατή όταν το packet payload είναι κρυπτογραφημένο.

Για να αντιμετωπίσει αυτά τα ζητήματα, η επιτροπή Internet Engineering Task Force (IETF) έχει αναπτύξει μια σουΐτα πρωτοκόλλων και προτύπων γνωστά και ως IPv6 (Internet Protocol version 6 – Πρωτόκολλο Δικτύου έκδοση 6). Αυτή η καινούργια έκδοση, η οποία καλούταν προηγουμένως ως IPng (IP next generation), ενσωματώνει τα θέματα πολλών προτεινόμενων μεθόδων για την αναβάθμιση του πρωτοκόλλου IPv4. Η σχεδίαση του IPv6 στοχεύει σκοπίμως τον ελάχιστο αντίκτυπο στα υψηλότερα και χαμηλότερα στρώματα πρωτοκόλλων αποφεύγοντας την τυχαία προσθήκη νέων χαρακτηριστικών.

1.2 Σύγκριση IPv6 με IPv4

Πλεονεκτήματα IPv6

- **Μεγαλύτερος χώρος διευθύνσεων**

Το πιο προφανές και με διαφορά πιο σημαντικό πλεονέκτημα της καινούριας έκδοσης του IP είναι ο πολύ μεγαλύτερος χώρος διευθύνσεων. Ο θεωρητικός αριθμός διαθέσιμων διευθύνσεων για την τωρινή έκδοση του πρωτοκόλλου είναι **4.294.967.296(32 bit)**.Για λόγους σύγκρισης παραθέτουμε τον αντίστοιχο αριθμό για το IPv6: **340,282,366,920,938,463,463,374,607,431,768,211,456 (128 bit)**

Αυτός ο χώρος διευθύνσεων είναι αρκούντως μεγάλος ώστε να αντιστοιχεί σε 155 δισεκατομμύρια IPv4 δίκτυα σε κάθε τετραγωνικό χιλιοστό της γης συμπεριλαμβανομένων και των ωκεανών! Ακόμα και αν η αύξηση σε απαιτήσεις για χώρο διευθύνσεων διπλασιαζόταν κάθε 5 χρόνια όπως γινόταν για κάποιο χρονικό διάστημα, που είναι εκθετικός ρυθμός αύξησης, τότε οι διαθέσιμες διευθύνσεις θα τελείωναν το 2485. Ουσιαστικά δηλαδή λύνει το πρόβλημα του χώρου διευθύνσεων. Βέβαια το πρόβλημα το χώρου διευθύνσεων δεν είναι τόσο μεγάλο πια και το πότε θα τελειώσει παραμένει

αναπάντητο, σίγουρα όμως είναι ένα φλέγον ζήτημα και το πιθανότερο είναι ότι σε κάποια χρόνια θα τελειώσει.

- **Καινοτομία**

Ο κυριότερος λόγος γιατί το πρόβλημα του χώρου διευθύνσεων δεν είναι τόσο σημαντικό πια είναι γιατί χρησιμοποιείται ευρύτατα η τεχνολογία NAT κατά την οποία πολλοί υπολογιστές «μοιράζονται» την ίδια IP διεύθυνση. Βέβαια αυτό είναι δίκοπο μαχαίρι. Για κλασικές εφαρμογές client/server π.χ email,web και άλλες η τεχνολογία NAT λύνει το πρόβλημα(αν είναι clients οι Η/Υ που μοιράζονται την ίδια IP), γι' άλλες εφαρμογές όμως όπως VoIP όπου κάθε Η/Υ πρέπει να είναι «διακριτός» και για όσους είναι έξω του δικτύου που χρησιμοποιεί NAT, η τεχνολογία NAT σίγουρα δυσκολεύει τη λειτουργία τους.

Το IPv6 λύνει αυτό το πρόβλημα αφού πλέον με τόσο μεγάλο χώρο διευθύνσεων κάθε Η/Υ μπορεί να έχει τη δική του διεύθυνση.

- **Αυτορύθμιση διεύθυνσης**

Στο IPv4 χρησιμοποιούνταν το πρωτόκολλο DHCP για να λάβει 1 μηχάνημα αυτόματα IP διεύθυνση. Αυτό έχει 2 μεγάλα μειονεκτήματα: 1)χρειάζεται 1 DHCP server. 2)δεν υπάρχει εγγύηση ότι το ίδιο μηχάνημα θα λάβει την ίδια διεύθυνση(εκτός βέβαια και αν ρυθμιστεί ρητά με αντιστοίχηση της MAC διεύθυνσής του).

Με το IPv6 υπάρχει μεν μια ανανεωμένη έκδοση του DHCP το DHCPv6 αλλά με το IPv6 υπάρχει και άλλη επιλογή για την αυτόματη ρύθμιση της διεύθυνσης, που ονομάζεται stateless autoconfiguration. Με αυτή την επιλογή κάθε δικτυακή συσκευή περιμένει να «ακούσει» ποια 64 bit να χρησιμοποιήσει για το πρώτο μέρος της IPv6 διεύθυνσης. Όσες συσκευές είναι μέρος του ίδιου δικτύου έχουν το ίδιο 64-bit πρόθεμα. Τα υπόλοιπα bit συμπληρώνονται από τη MAC διεύθυνση των συσκευών αυτών. Οι MAC διευθύνσεις είναι 48 bit συνεπώς τα υπόλοιπα 16 συμπληρώνονται κατά 1 προσυμφωνημένο τρόπο, συνήθως με 1. Με αυτόν τον τρόπο ο ίδιος Η/Υ παίρνει την ίδια IP κάθε φορά στο ίδιο δίκτυο και χωρίς την ανάγκη ύπαρξης DHCP server. Βέβαια οι δρομολογητές συνεχίζουν να «διαφημίζουν» στους Η/Υ ποιους δρομολογητές μπορούν να χρησιμοποιήσουν για να επικοινωνήσουν με το υπόλοιπο Internet.

- **Εύκολη αλλαγή διεύθυνσης**

Σύμφωνα με τον παραπάνω τρόπο αυτόματης ρύθμισης της διεύθυνσης, είναι πολύ εύκολο οι δικτυακές συσκευές ενός ολόκληρου δικτύου να αλλάξουν διεύθυνση. Απλά αλλάζει το 64-bit που διαφημίζεται με 1 καινούριο. Οι παλιές διευθύνσεις βέβαια παραμένουν σε ισχύ για τυχόν επικοινωνίες που είναι ήδη ανοιχτές ή δεν έχουν ενημερωθεί για την αλλαγή αλλά όσες καινούριες φτιάχνονται χρησιμοποιούν τις καινούριες, αλλαγμένες διευθύνσεις.

- **Αποδοτικότητα**

Μετά από 3 δεκαετίες εμπειρίας χρήσης του IPv4 έχει αποκομιστεί αρκετή εμπειρία στο ποια χαρακτηριστικά είναι χρήσιμα και ποια όχι στο IPv4 και ποια λειτουργούν ως bottlenecks της ταχύτητας. Στο IPv6 έχουν ενσωματωθεί αυτές οι βελτιώσεις και πράγματι έχει πολύ καλύτερη απόδοση. Παρ' όλο που τώρα τα πεδία διευθύνσεων είναι 4 φορές μεγαλύτερα σε σχέση με το IPv4, η συνολική επικεφαλίδα είναι μόνο 40 bytes εν συγκρίσει με τα 20 bytes μιας τυπικής επικεφαλίδας IPv4. Οι βελτιώσεις που υπάρχουν είναι οι εξής:

α. Η επικεφαλίδα του IPv6 έχει σταθερό μήκος

β. Η επικεφαλίδα του IPv6 είναι βελτιστοποιημένη για επεξεργασία 64 bit τη φορά σε σχέση με τα 32 bit του IPv4.

γ. Το checksum της επικεφαλίδας IPv4 που υπολογίζεται κάθε φορά που 1 πακέτο περνά από 1 δρομολογητή, αφαιρέθηκε από το IPv6.

δ. Οι δρομολογητές δεν είναι υποχρεωμένοι να χωρίζουν 1 μεγάλο πακέτο σε μικρότερα κομμάτια και μπορούν απλά να στείλουν σήμα να τους έρχονται μικρότερα πακέτα.

ε. Το broadcast που χρησιμοποιούνταν ευρέως στο IPv4 αντικαταστάθηκε με τα multicast στο IPv6 με τα οποία δεν διακόπτονται όλες οι δικτυακές συσκευές για να επεξεργαστούν το μήνυμα που έρχεται αλλά μόνο όσες «ακούνε» εκείνη τη στιγμή.

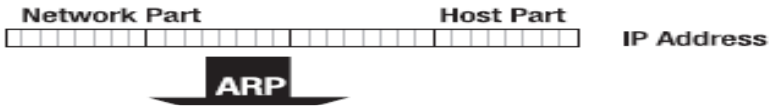
1.3 Διαφορές μεταξύ IPv4 και IPv6

Εκτός από τις διαφορές που έχουν ήδη αναφερθεί υπάρχουν και άλλες διαφορές μεταξύ των 2 πρωτοκόλλων.Το IPv4 έχει κλάσεις διευθύνσεων: η κλάση A χρησιμοποιεί 7 bit για τα πιθανά υποδίκτυα και 24 bit για τις δικτυακές συσκευές που μπορούν να συνδεθούν στα υποδίκτυα. Η κλάση B χρησιμοποιεί 14 bit για τον αριθμό των υποδικτύων και 16 bit για τους hosts. Η κλάση C χρησιμποποιεί 21 bit για τα δίκτυα και 8 bit για τους hosts.

Η κλάση B αποδείχθηκε η πιο διάσημη γιατί οι περισσότερες επιχειρήσεις ήθελαν περισσότερες από 255 διευθύνσεις όμως συνήθως και πολύ λιγότερες από 65535. Στην αρχή όσοι είχαν ανάγκη για παραπάνω από 255 διευθύνσεις τους έδιναν 1 κλάση B. Στις αρχές του 1990, είχε γίνει προφανές ότι τελείωναν πολύ γρήγορα οι διευθύνσεις, και πολλές από αυτές ήταν αχρησιμοποίητες με αυτή τη μέθοδο, γι' αυτό άρχισαν να δίνονται και μέρη διευθύνσεων της κλάσης C αντί για μια ολόκληρη κλάση B.

Το πρόβλημα βρήκε λύση το 1993 με την υιοθέτηση του CIDR(Classless Interdomain Routing). Με το CIDR η διάκριση σε κλάσεις δεν χρειαζόταν πια. Μια τιμή τώρα πια υποδείκνυε τη διάκριση σε bits που δείχνουν τα υποδίκτυα και τα bits που δείχνουν τις δικτυακές συσκευές στα υποδίκτυα. Το IPv6 και αυτό δεν έχει κλάσεις και χρησιμοποιεί τεχνική παρόμοια με αυτή του CIDR.

Στα δίκτυα IPv4 δεν υπάρχει καμία σχέση ανάμεσα στη διεύθυνση MAC ενός υπολογιστή σε ένα δίκτυο Ethernet με την IP που του είχε ανατεθεί. Έτσι υπήρχε ανάγκη για ένα πρωτόκολλο που να αντιστοίχιζε τις διευθύνσεις IP με τις διευθύνσεις MAC. Το πρωτόκολλο αυτό ονομάζεται ARP(Address Resolution Protocol). Αρχικά όταν κάποιος θέλει να στείλει 1 μήνυμα σε μια διεύθυνση IP κάνει broadcast τη διεύθυνση στην οποία θέλει να στείλει το μήνυμα και ο υπολογιστής που την κατέχει απαντά. Έτσι μαθαίνει τη διεύθυνση MAC που έχει ο υπολογιστής και σε ποια IP αντιστοιχεί.

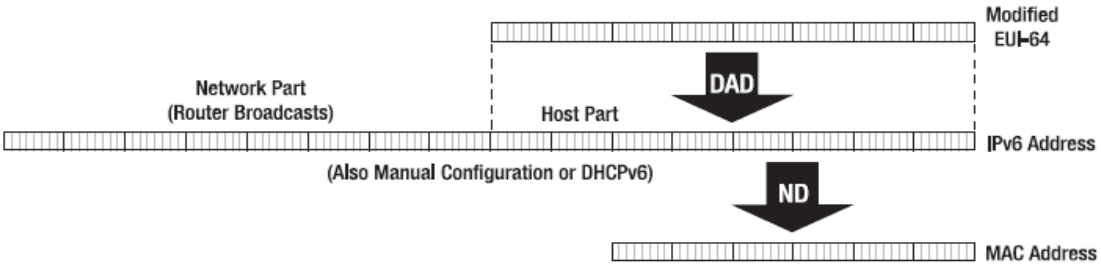


Σχήμα 2:Αντιστοίχιση IP διεύθυνσης με την αντίστοιχη MAC με χρήση του ARP πρωτοκόλλου.

Στο IPv6 πολλές φορές μπορεί να μην εμπεριέχεται η MAC διεύθυνση και γι' αυτό υπάρχει και εδώ 1 παρόμοιος μηχανισμός με το πρωτόκολλο ARP. Το ARP όμως χρησιμοποιεί broadcasts που το IPv6 δεν υποστηρίζει. Αντίθετα το IPv6 χρησιμοποιεί εκτενώς multicasts. Στο multicast τα πακέτα μεταδίδονται μόνο σε 1 ορισμένη ομάδα δικτυακών συσκευών και όχι σε όλες. Στο IPv6 το αντίστοιχο πρωτόκολλο του ARP είναι το

ND (Neighbor Discovery) και βασίζεται σε multicasts, είναι πιο γενικό από το ARP και όχι τόσο εξαρτώμενο από τα δίκτυα Ethernet.

Στο IPv6 επίσης χρησιμοποιείται η τεχνολογία DAD(Duplicate Address Detection) δανεισμένη από το πρωτόκολλο AppleTalk και ανιχνεύει όπως λέει και το όνομά της αν υπάρχουν δικτυακές συσκευές που έχουν την ίδια IP ώστε να αποφευχθεί κάτι τέτοιο.

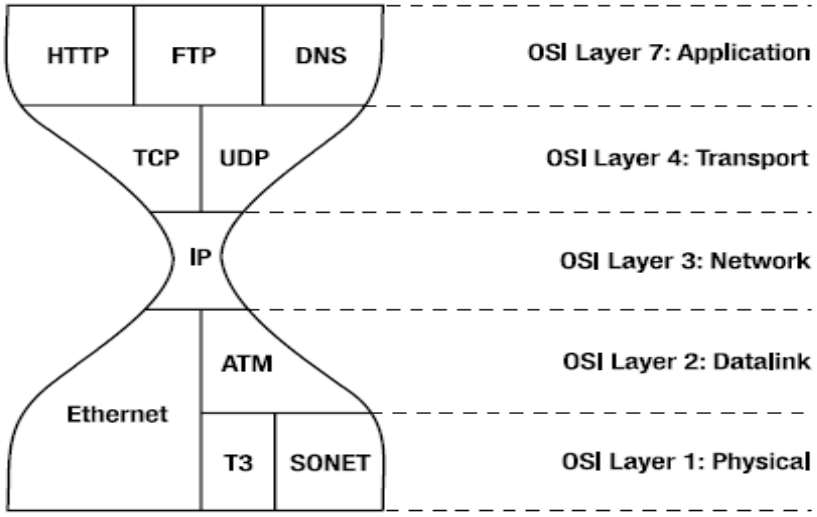


Σχήμα 3:Τεχνολογία Duplicate address detection

2. Το Πρωτοκολλο IPV6

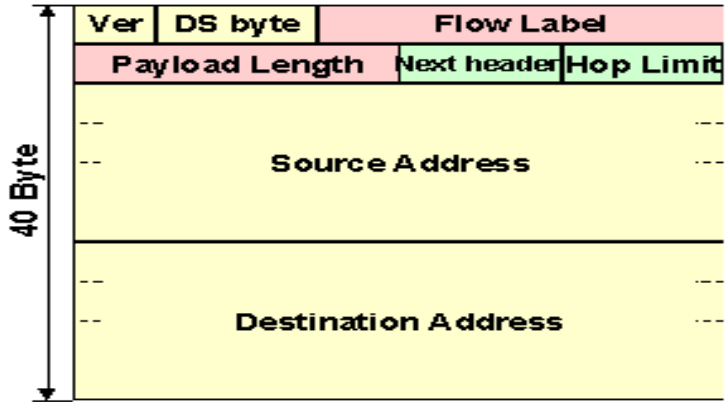
2.1 Δομή του IPv6.

Έχει ειπωθεί από δημιουργούς του IPv6 ότι τα πρωτόκολλα όλων των επιπέδων θα μπορούσαμε να τα παραστήσουμε με μια κλεψύδρα, και σ' αυτή την περίπτωση το IP βρίσκεται ακριβώς στη μέση της κλεψύδρας (συνδέει δηλαδή συνήθως τα πρωτόκολλα που υλοποιούνται στο hardware με αυτά που υλοποιούνται σε software), γι'αυτό έχει ιδιαίτερο ενδιαφέρον να μελετήσουμε τη δομή του.



Σχήμα 4:Το μοντέλο της κλεψύδρας για παράσταση των πρωτοκόλλων

Οι βασικές κεφαλίδες του IPv6



Σχήμα 5:Η βασική κεφαλίδα του IPv6.

Επεξήγηση των πεδίων του βασικού header του IP:

Ver(version):δείχνει την έκδοση του IP.

DS byte (8 bit): Το πεδίο χρησιμοποιείται για να βρεθεί η κλάση κίνησης του πακέτου.

flow label (20 bit): Δε χρησιμοποιείται για ουσιαστικό λόγο προς το παρόν.

payload length (16 bit): Δείχνει το μήκος του πεδίου δεδομένων.

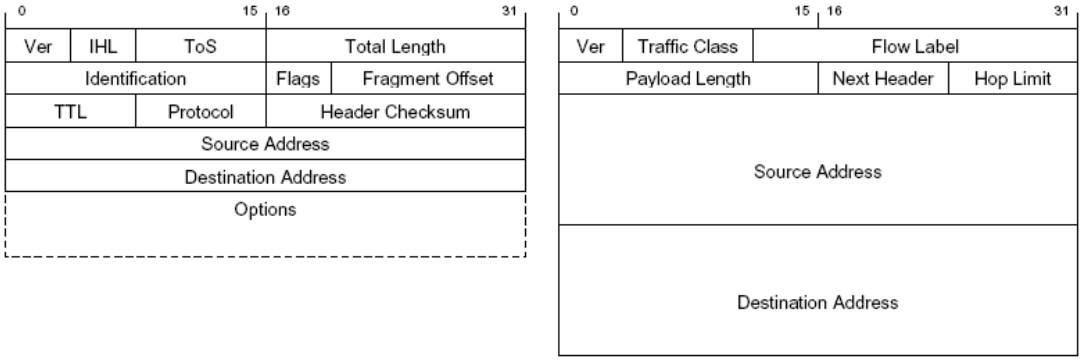
next header (8 bit):): Υποδεικνύει τον τύπο header που ακολουθεί.

hop limit (8 bit): Αντικαθιστά το πεδίο TTL, έχει μια αρχική τιμή και μειώνεται κάθε φορά που το πακέτο μεταδίδεται μέσα από μια δικτυακή συσκευή. Όταν μηδενιστεί το πακέτα απορρίπτεται.

source address (128 bit): Η διεύθυνση του αποστολέα.

destination address (128 bit) : Η διεύθυνση του παραλήπτη.

Το IPv6 παρουσιάζει σημαντικές βελτιώσεις σε σχέση με τον προκάτοχό του IPv4. Η μορφή της επικεφαλίδας στο IPv6 έχει αλλάξει από μια μεταβλητού μεγέθους επικεφαλίδα με δώδεκα πεδία και επιλογές σε μια σταθερού μεγέθους επικεφαλίδα μήκους 40 bytes, η οποία περιέχει μόνο οκτώ πεδία όπως φαίνεται και στο σχήμα 5.



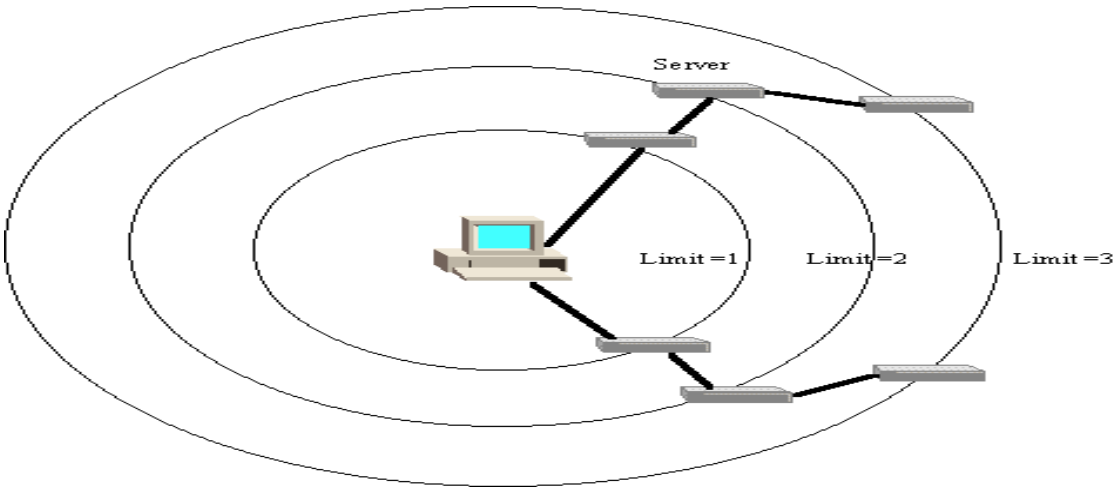
Σχήμα 6: Μορφή της επικεφαλίδας των πρωτοκόλλων IPv4(αρ.) και IPv6 (δεξ)

Οι διαφορές μεταξύ των δύο εκδόσεων του πρωτοκόλλου IP όσον αφορά τη μορφή της επικεφαλίδας αναφέρονται εν συντομία παρακάτω:

Το πεδίο Type of Service (ToS) έχει αντικατασταθεί από το πεδίο Traffic Class, το οποίο μαζί με το καινούριο πεδίο Flow Label παρέχει δυνατότητες καθορισμού προτεραιότητας κυκλοφορίας πακέτων και ποιότητας υπηρεσίας (Quality Of Service).

Το πεδίο Time To Live (TTL) έχει αντικατασταθεί από το πεδίο Hop Limit, το οποίο προσδιορίζει πιο σωστά τη σημασία του πεδίου.Το hop limit αντικατέστησε το TTL για τους εξής λόγους. Κατ'αρχάς, για λόγους απλότητας αφού το TTL είχε ως μονάδα μέτρησης το second, και έπρεπε οι δρομολογητές να μετατρέπουν συνεχώς τα hops σε seconds και αντίστροφα. Επίσης το hop limit είναι ανεξάρτητο των χαρακτηριστικών του επιπέδου 1 όπως το εύρος ζώνης.

Το hop limit όμως χρησιμοποιείται και για μια άλλη λειτουργία: για την «ανακάλυψη» άλλων εξυπηρετητών που κάνουν την ίδια δουλειά με τον τρέχοντα. Αρχικά, στέλνεται 1 μήνυμα που απευθύνεται σε συγκεκριμένο είδος εξυπηρετητή με hop limit=1. Αν δεν υπάρξει απάντηση σε ορισμένο χρονικό διάστημα στέλνεται το ίδιο μήνυμα με hop limit=2 κ.ο.κ μέχρι να ανακαλυφθεί ο κοντινότερος εξυπηρετητής που κάνει τη δουλειά που θέλουμε. Στο IPv6 μπορούμε όμως να κάνουμε την ίδια δουλειά που περιγράψαμε χρησιμοποιώντας διευθύνσεις τύπου anycast.



Σχήμα 7:Παράδειγμα χρήσης του πεδίου hop limit.

Το πεδίο Header Checksum έχει αποσυρθεί εντελώς στο IPv6, αφού ο έλεγχος σφαλμάτων στις περισσότερες περιπτώσεις πραγματοποιείται στα άλλα επίπεδα του TCP/IP. 'Ετσι υπάρχει κέρδος σε ταχύτητα γιατί δεν χρειάζεται να υπολογίζεται συνέχεια το checksum των επικεφαλίδων δίνοντας μια μεγάλη ώθηση στις επιδόσεις των δρομολογητών και των firewalls, αφού δε χρειάζεται να ξαναϋπολογίσουν ένα Checksum, όταν κάτι αλλάξει στην επικεφαλίδα (π.χ. η διάρκεια ζωής του πακέτου στο πεδίο TTL).

Τα πεδία Fragmentation Offset και Options έχουν αποσυρθεί εντελώς από την επικεφαλίδα του IPv6. Αντί αυτών, αυτή η πληροφορία τίθεται σε ξεχωριστές επικεφαλίδες επέκτασης (extension headers) που εισάγονται μεταξύ της επικεφαλίδας του IPv6 και του ωφέλιμου φορτίου (payload) . Η διαδικασία φαίνεται στο σχήμα 6. Κάθε επικεφαλίδα επέκτασης έχει ένα πεδίο Next Header (επόμενη επικεφαλίδα), το οποίο περιγράφει τον τύπο της επόμενης επικεφαλίδας. Αυτή η τεχνική διευκολύνει το χειρισμό επιπλέον επιλογών στην επικεφαλίδα καθώς και τις περιπτώσεις ειδικού τρόπου παράδοσης πακέτου. Επίσης παρέχει δυνατότητες εύκολης μελλοντικής επέκτασης με νέα είδη επικεφαλίδων.

Σε αντίθεση με το IPv4, οι επικεφαλίδες του IPv6 έχουν σταθερό μέγεθος ορισμένο στα 40KB. Έτσι δεν υπάρχει ανάγκη για πεδίο που να υποδηλώνει το μέγεθος της επικεφαλίδας, και μπορούν να υπάρξουν διάφορες βελτιστοποιήσεις στους δρομολογητές για ακόμα καλύτερη απόδοση. Το payload length που δείχνει το μέγεθος των δεδομένων είναι 16 bit που σημαίνει ότι κάθε πακέτο το πολύ να μεταφέρει 64 KB δεδομένα, που εξασφαλίζει πολύ καλή απόδοση για τους δρομολογητές. Για μερικούς υπερυπολογιστές όμως που συνδέονται απευθείας αυτό μπορεί να είναι πολύ περιοριστικό. Η λύση που έχει δοθεί σε αυτό είναι να τίθεται 0 το payload length και έτσι μπορούν να σταλούν και παραπάνω από 64 KB. Επίσης με το IPv6 αποφεύγεται και το fragmentation των πακέτων μέσω της τεχνικής MTU(Maximum Transmission Unit) discovery. Με την τεχνική αυτή ανακαλύπτεται κάθε φορά το μέγιστο μέγεθος πακέτου που μπορεί να μεταφερθεί χωρίς να χωριστεί σε κομμάτια(ελάχιστο μέγεθος 1280 bytes), και γίνεται συμφωνία να μη γίνεται χωρισμός και επανασύνδεση των πακέτων στους ενδιάμεσους δρομολογητές αλλά να στέλνονται από όλους πακέτα μεγέθους MTU και έτσι εξοικονομείται πολύς χρόνος και ανεβαίνει η απόδοση.

2.1.1 IPv6 και εφαρμογές πραγματικού χρόνου

Το Internet σχεδιάστηκε για να προσφέρει best effort κίνηση και βασίζεται στην ιδέα ότι το δίκτυο θα κάνει όλες τις δυνατές προσπάθειες για να παραδώσει ένα πακέτο,χωρίς όμως να παρέχει κάποια εγγύηση για την επιτυχή παραλαβή του πακέτου ή τον πραγματικό χρόνο που αυτή θα γίνει. Οι εφαρμογές πραγματικού χρόνου (real time applications) παράγουν τη λεγόμενη κίνηση πραγματικού χρόνου (real time traffic). Η κίνηση πραγματικού χρόνου είναι ένα είδος κίνησης ευαίσθητο στις καθυστερήσεις και τις απώλειες κατά τη διάρκεια της μετάδοσης των πακέτων. Επιπλέον, η κίνηση πραγματικού χρόνου συχνά απαιτεί την ύπαρξη ενός ελάχιστου εγγυημένου bandwidth. Η εισαγωγή των υπηρεσιώνπραγματικού χρόνου (real time services) στα δίκτυα έχει κάνει επιτακτική την ανάγκη για υποστήριξη Quality of Service (QoS). Η υποστήριξη για Quality of Service θα πρέπει επίσης να παρέχεται και για τη multicast μετάδοση δεδομένων, γιατί η multicast μετάδοση δεδομένων χρησιμοποιείται συχνά από τις εφαρμογές πραγματικού χρόνου.

Η παροχή εγγυήσεων ποιότητας στις εφαρμογές πραγματικού χρόνου συνδέεται στενά με την δυνατότητα διαχείρισης των δικτυακών πόρων (δηλ. το bandwidth). Για να μπορεί το δίκτυο να παρέχει εγγυήσεις ποιότητας, πρέπει να ενσωματωθούν στο δίκτυο μηχανισμοί που χειρίζονται τους δικτυακούς πόρους και μηχανισμοί που δέχονται ή απορρίπτουν αιτήσεις (Admission Control). Η multimedia επικοινωνία επηρεάζεται από αρκετά χαρακτηριστικά του IPv6:

• Χαρακτηριστικά που προσφέρει το IPv6 για την παροχή QoS σε εφαρμογές πραγματικού χρόνου.

• Ενσωματωμένη υποστήριξη IP Multicast.

• Μεγάλος χώρος διευθύνσεων.

• Χαρακτηριστικά που επιτρέπουν το autoconfiguration.

• Αποτελεσματική και γρήγορη δρομολόγηση.

• Υποστήριξη μηχανισμών ασφάλειας στο επίπεδο δικτύου.

Μερικά από τα χαρακτηριστικά του IPv6 μπορούν να βελτιώσουν σημαντικά την υποστήριξη για εφαρμογές πραγματικού χρόνου, και ειδικότερα τα δύο νέα πεδία επικεφαλίδας:

• Το μήκους 8 bit πεδίο Traffic Class

• Το μήκους 20 bit πεδίο Flow Label

Το πεδίο Traffic Class αναμένεται να έχει ανάλογη λειτουργικότητα με τα πεδία Type Of Service και Precedence του IPv4. Το πεδίο Flow Label μπορεί να χρησιμοποιηθεί για να διαφοροποιήσει πακέτα που ανήκουν σε διαφορετικές ροές δεδομένων. Επιπλέον, τα πρωτόκολλα που συνοδεύουν το IPv6 όπως το ICMPv6 (το οποίο συμπεριλαμβάνει λειτουργικότητα για τη διαχείριση multicast groups) και το OSPFv6 (το οποίο διαχειρίζεται multicast δέντρα) επίσης συνεισφέρουν στη βελτίωση της υποστήριξης εφαρμογών πραγματικού χρόνου.

Οι βελτιώσεις που προσφέρει το IPv6 δεν είναι βέβαια δυνατόν να υποστηρίξουν όλες τις εφαρμογές πραγματικού χρόνου πάνω από ένα δίκτυο best-effort όπως το Internet. Έτσι το IPv6 ήταν αρχικά μέρος του φιλόδοξου σχεδίου Integrated Services, το οποίο στοχεύει στην επέκταση της αρχιτεκτονικής του Internet ώστε να μπορεί να υποστηρίζει και κίνηση πραγματικού χρόνου. Επιπλέον, ο τελικός καθορισμός της χρήσης των Traffic Class και Flow Label πεδίων δεν έχει γίνει ακόμα. Το πεδίο Traffic Class μπορεί να χρησιμοποιηθεί για να διαφοροποιηθεί ο χειρισμός της κίνηση βάσει της τιμής κάθε πακέτου σε αυτό το πεδίο. Όταν εμφανίζεται συμφόρηση, μπορεί να χρησιμοποιηθεί ένας προκαθορισμένος κανόνας βασισμένος στο Traffic Class πεδίο, ώστε κάποια πακέτα να πετάγονται.

Επομένως το πεδίο μπορεί να αποβεί χρήσιμο για την υλοποίηση QoS μηχανισμών βασισμένων στην DiffServ αρχιτεκτονική (για παράδειγμα η Thomson edge device χρησιμοποιεί το πεδίο Traffic Class για την υλοποίηση QoS βασισμένου στην DiffServαρχιτεκτονική).

Το πεδίο Flow Label στην επικεφαλίδα των IPv6 πακέτων σχεδιάστηκε ώστε να μπορεί μία ροή κίνησης να αναγνωριστεί, και άρα να μπορούν οι ενδιάμεσοι κόμβοι να χρησιμοποιήσουν την ετικέτα αυτή για να αναγνωρίσουν ροές κίνησης και να τις χειριστούν ανάλογα (χρησιμοποιώντας για παράδειγμα ένα πρωτόκολλο κράτησηςπόρων όπως το RSVP). Η χρήση του πεδίου Flow Label στα IP πακέτα μπορεί να βοηθήσει τους ενδιάμεσους κόμβους ώστε να επεξεργαστούν την κίνηση ταχύτερα,αν τα μονοπάτια και οι κρατήσεις για συγκεκριμένες ομάδες ροών έχουν νωρίτερα καθοριστεί στους ενδιάμεσους αυτούς κόμβους. Η τιμή του πεδίου Flow Label αρχικοποιείται από τις πηγές των ροών. Αυτό σημαίνει ότι το πεδίο Flow Label μπορεί να χρησιμοποιηθεί για την υλοποίηση QoS σχημάτων βασισμένων στην IntServ αρχιτεκτονική (για παράδειγμα ο Lancaster RSVP media server χρησιμοποιεί το πεδίο Flow Label για την υλοποίηση QoS βασισμένου στην IntServαρχιτεκτονική).

Το IPv6 προσφέρει επίσης τη δυνατότητα χρήσης επιπλέον επικεφαλίδων μέσω του πεδίου Next Headers. Αυτή η δυνατότητα μπορεί να χρησιμοποιηθεί για την υλοποίηση Quality of Service σχημάτων βασισμένων σε νέες επικεφαλίδες. Η χρήση του IPv6 έχει το μειονέκτημα της μεταφοράς μιας σημαντικά μεγαλύτερης επικεφαλίδας, η οποία συνεπάγεται μεγαλύτερο RTP / UDP / IP overhead. Αυτό το overhead μπορεί να επηρεάσει αρνητικά τα χαμηλής ταχύτητας δίκτυα και άρα πρέπει να χρησιμοποιηθούν κάποιοι αποτελεσματικοί μηχανισμοί συμπίεσης.

Το IPv6 συμπεριλαμβάνει επίσης μηχανισμούς ασφάλειας μέσω δύο επικεφαλίδων επέκτασης, των Authentication Header (AH) και Encrypted Security Payload (ESP). Η Authentication Header προσφέρει τη δυνατότητα για εξακρίβωση αυθεντικότητας χρήστη (user authentication) και διασφάλιση ακεραιότητας IP πακέτων (IP packet integrity), και προλαμβάνει την μη εξουσιοδοτημένη τροποποίηση ενός πακέτου ή την ψευδή αποστολή πακέτων (packet spoofing). Η Encrypted Security Payload επικεφαλίδα προσφέρει ενθυλάκωση κρυπτογραφημένων δεδομένων (encrypted data encapsulation) έτσι ώστε μόνο ο επιθυμητός κόμβος αποστολής να μπορεί να διαβάσει τα δεδομένα του πακέτου. Οι δύο αυτές επικεφαλίδες χρησιμοποιούν την έννοια του Security Association (SA), σε Transport και Tunnel mode. Κατά την χρήση της Authentication Header σε tunnel mode, η ασφάλεια παρέχεται για τμήματα της εξωτερικής IP επικεφαλίδας και ολόκληρο το εσωκλειόμενο πακέτο (το οποίο περνάει μέσα από το tunnel), ενώ όταν χρησιμοποιείται η Encrypted Security Payload, προστατεύεται μόνο το εσωκλειόμενο πακέτο. Αν έχει εγκαθιδρυθεί Security Association μεταξύ των δύο επικοινωνούντων κόμβων, τότε είτε transport είτε tunnel mode μπορεί να χρησιμοποιηθεί. Αν μία από τις ακμές είναι ένα security gateway τότε μόνο tunnel mode μπορεί να χρησιμοποιηθεί.

2.2 ICMPv6

Το IPv6 χρησιμοποιεί το Internet Control Message Protocol v6 (πρωτόκολλο μηνυμάτων ελέγχου δικτύου έκδοση 6), το οποίο είναι μια περαιτέρω ανάπτυξη του ICMP που είναι διαθέσιμο στο IPv4. Οι αλλαγές από την έκδοση 4 στην έκδοση 6 περιλαμβάνουν την αφαίρεση των σπάνια χρησιμοποιούμενων μηνυμάτων και την εισαγωγή των μηνυμάτων Internet Group Management Protocol (Πρωτόκολλο διαχείρισης ομάδων διαδικτύου) που χρησιμοποιείται για την είσοδο και την αποχώρηση από ομάδες πολλαπλής διανομής (multicast groups). Το ICMPv6 χρησιμοποιείται επίσης για διαγνωστικούς λόγους (π.χ.

Ping) και autoconfiguration (αυτόματη απόκτηση ρυθμίσεων). Ο πίνακας 2.1 παρουσιάζει τα μηνύματα του ICMPv6, τα οποία έχουν μέχρι στιγμής οριστεί.

Πίνακας 2.1 Τα μηνύματα του ICMPv6

ID	Message
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

2.3 Διευθυνσιοδότηση

Το μήκος των διευθύνσεων στο IPv6 είναι 128 bit, αντί των 32 bit που χρησιμοποιούνταν στο IPv4. Με 128 bit είναι θεωρητικά δυνατό να ανατεθούν περίπου 665,985,621,475,071,937 διευθύνσεις IP ανά τετραγωνικό χιλιοστό στην επιφάνεια της γης, έτσι το πρόβλημα της έλλειψης των IP διευθύνσεων φαίνεται να επιλύεται. Όμως στην πράξη, ο τεράστιος χώρος διευθύνσεων θα χρησιμοποιηθεί για να εισάγει μια πιο ιεραρχική δομή διευθύνσεων από αυτή του παρόντος πρωτοκόλλου IPv4. Μια ιεραρχική δομή επίσης θα βελτιστοποιήσει τη δρομολόγηση στα δίκτυα, αφού οι δρομολογητές δε θα χρειάζεται να εξετάζουν ολόκληρη τη διεύθυνση.

2.3.1. Σημειογραφία διευθύνσεων

Οι διευθύνσεις στο IPv4 είναι γραμμένες στη λεγόμενη μορφή “four dotted decimal” (δεκαδική με τέσσερις τελείες) , όπως π.χ. η διεύθυνση 147.102.220.210. Με τα 128 Bits αντί των 32 bits αυτή η σημειογραφία θα απαιτούσε 16 δεκαδικούς ακεραίους για να σχηματιστεί μια IPv6 διεύθυνση, η οποία θα ήταν δύσχρηστη. Αντί για αυτό οι IPv6 διευθύνσεις γράφονται σαν 8 ομάδες 16-bit δεκαεξαδικών λέξεων, χωρισμένων μεταξύ τους με άνω και κάτω τελείες, όπως π.χ. οι διευθύνσεις:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

FE80:0000:0000:0000:0200:F8FF:FE22:26C8

Χρησιμοποιώντας δεκαεξαδικά ψηφία αυτή η μορφή είναι μικρότερη από τη μορφή με δεκαδικά ψηφία, αλλά ακόμα και έτσι η διεύθυνση παραμένει αρκετά μακροσκελής και δύσχρηστη. Για να μειωθεί ακόμα περισσότερο το μήκος υπάρχουν κάποιες περαιτέρω απλοποιήσεις.

Σε μια IPv6 διεύθυνση πιθανόν να υπάρχουν πολλά μηδενικά, λόγω του μεγάλου διαθέσιμου χώρου διευθύνσεων. Αφαιρώντας τα μηδενικά που βρίσκονται στην αρχή της λέξης και επομένως αντικαθιστώντας λέξεις όπως το 0200 με το 200, η διεύθυνση απλοποιείται. Επιπλέον οι λέξεις που απαρτίζονται ολοκληρωτικά από μηδενικά (0000) μπορούν να αντικατασταθούν από δύο συνεχόμενες άνω και κάτω τελείες (::) . Η διπλή άνω και κάτω τελεία μπορεί να αναπαριστά μια ή περισσότερες διαδοχικές λέξεις αυτού του είδους και μπορεί επομένως να απλοποιήσει περαιτέρω τη σημειογραφία των IPv6 διευθύνσεων. Η συμπιεσμένη μορφή της διεύθυνσης :

FE80:0000:0000:0000:0200:F8FF:FE22:26C8

γράφεται ως εξής :

FE80::200:F8FF:FE22:26C8.

Για να γραφεί μια IPv6 διεύθυνση αυτής της μορφής ξανά σε αναλυτική μορφή αρκεί να αντικατασταθούν οι δύο άνω και κάτω τελείες με τόσα μηδενικά όσα χρειάζονται για να συμπληρωθεί το απαιτούμενο μήκος της διεύθυνσης. Δεν είναι δυνατόν να υπάρχουν δύο φορές συνεχόμενες άνω και κάτω τελείες σε μια IPv6 διεύθυνση, γιατί αυτό θα καθιστούσε το συμβολισμό διφορούμενο.

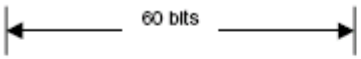
Ένας βολικός τρόπος για να γραφούν IPv6 διευθύνσεις που προκύπτουν από IPv4 διευθύνσεις είναι ο ακόλουθος. Οι διευθύνσεις αυτές γράφονται σαν έξι δεκαεξαδικές ομάδες ακολουθούμενες από τη γνωστή “four dotted decimal” μορφή των IPv4 διευθύνσεων. Π.χ. η διεύθυνση :

0:0:0:0:0:0:192.168.0.1

γράφεται σε συμπιεσμένη μορφή ως :

::192.168.0.1

Εκτός από τις IPv6 διευθύνσεις που ανατίθενται σε ξεχωριστούς υπολογιστές (hosts), το IPv6 καθιερώνει τα address prefixes (προθέματα διευθύνσεων). Το πρόθεμα διεύθυνσης στο IPv6 είναι παρόμοιο με το network prefix (πρόθεμα δικτύου), το οποίο χρησιμοποιείται στο IPv4 και λειτουργεί με τον ίδιο τρόπο. Το πρόθεμα διεύθυνσης δηλώνεται σαν μια IPv6 διεύθυνση ακολουθούμενη από μια πλάγια γραμμή (/) και το μήκος του προθέματος σε bits. Τα επόμενα παραδείγματα παρουσιάζουν το ίδιο πρόθεμα γραμμένο με τρεις διαφορετικούς τρόπους:




```
3FFE:0000:0A12:1200:0000:0000:0000:0000/60
3FFE::A12:1200:0:0:0:0/60
3FFE:0:A12:1200::/60
```

Ακόμα και αν μας ενδιαφέρουν μόνο τα πρώτα 60 bits, οι επόμενες σημειογραφίες δεν είναι νόμιμες:

```
3FFE::A12:1200/60 →
3FFE:0000:0000:0000:0000:0000:0A12:1200/60 =
3FFE::/60


3FFE:0:A12:120::/60 →
3FFE:0000:0A12:0120:0000:0000:0000:0000/60 =
3FFE:0:A12:0120::/60
```

2.3.2. Ανάθεση διευθύνσεων

Οι IPv6 διευθύνσεις ανατίθενται σε interfaces (διαπροσωπείες), όπως τα Ethernet NICs (κάρτες διαπροσωπειών δικτύου), virtual interfaces PPP (εικονικές διαπροσωπείες πρωτοκόλλου σημείου προς σημείο) κ.ο.κ. Παρ' όλα αυτά, μια διαπροσωπεία δεν περιορίζεται σε μια μοναδική διεύθυνση, όπως στο IPv4 αλλά στην πραγματικότητα μπορεί να έχει έναν άπειρο αριθμό διευθύνσεων ανατεθειμένων σε αυτή. Αυτό είναι πολύ χρήσιμο για το διαχωρισμό των διαφόρων ειδών κυκλοφορίας του δικτύου μέσα από το ίδιο interface.

2.3.3 Ο χώρος διευθύνσεων του IPv6

Ο χώρος διευθύνσεων του IPv6 είναι γιγάντιος. Η μετάβαση από 32 σε 128 bits μήκος διευθύνσεων σημαίνει δραστική αύξηση των διαθέσιμων διευθύνσεων. Επιπλέον, τα 128 bits δεν κάνουν μόνο δυνατή την ανάθεση εκατομμυρίων των εκατομμυρίων host, αλλά παρέχουν μεγαλύτερη ιεραρχική δομή από τα επίπεδα δικτύου, υποδικτύου και host που ορίζονται στο IPv4.

Στην κορυφή της ιεραρχίας του χώρου διευθύνσεων του IPv6, διάφοροι τύποι διευθύνσεων ορίζονται. Κάθε τύπος έχει το δικό του υποχώρο διευθύνσεων αναγνωρισμένο από ένα πρόθεμα διεύθυνσης όμοιο με αυτό που χρησιμοποιείται στο Classless Inter-domain Routing CIDR (Αταξική Δρομολόγηση μεταξύ Περιοχών). Ο πίνακας 2.2 παρουσιάζει την αρχική ανάθεσή όπως έχει οριστεί στο RFC 2373. Ο πίνακας δείχνει την ονομαστική ανάθεση μαζί με το αντίστοιχο πρόθεμα ακολουθούμενο από το κλάσμα του χώρου διευθύνσεων που κατανέμει.

Πίνακας 2.2. Αρχική κατανομή των προθεμάτων διευθύνσεων

Allocation	Prefix (binary)	Prefix (hex)	Fraction of address space	
Reserved	0000 0000	::/8	1/256	(0.4%)
Unassigned	0000 0001	100::/8	1/256	
NSAP Allocation	0000 001	200::/7	1/128	(0.8%)
IPX Allocation	0000 010	400::/7	1/128	
Unassigned	0000 011	600::/7	1/128	
Unassigned	0000 1	800::/5	1/32	(3.1%)
Unassigned	0001	1000::/4	1/16	(6.3%)
Aggregatable Global Unicast Addresses	001	2000::/3	1/8	(12.5%)
Unassigned	010	4000::/3	1/8	
Unassigned	011	6000::/3	1/8	
Unassigned	100	8000::/3	1/8	
Unassigned	101	A000::/3	1/8	
Unassigned	110	C000::/3	1/8	
Unassigned	1110	E000::/4	1/16	(6.3%)
Unassigned	1111 0	F000::/5	1/32	(3.1%)
Unassigned	1111 10	F800::/6	1/64	(1.6%)
Unassigned	1111 110	FC00::/7	1/128	(0.8%)
Unassigned	1111 1110 0	FE00::/9	1/512	(0.2%)
Link-Local Unicast Addresses	1111 1110 10	FE80::/10	1/1024	(0.1%)
Site-Local Unicast Addresses	1111 1110 11	FEC0::/10	1/1024	
Multicast Addresses	1111 1111	FF::/8	1/256	(0.4%)

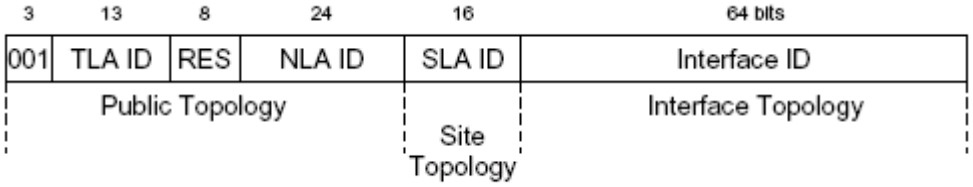
Όπως φαίνεται και στον πίνακα, περισσότερο από το 70% του χώρου διευθύνσεων παραμένει απροσδιόριστο. Αυτά το απροσδιόριστα προθέματα μπορούν αργότερα να αντικατασταθούν από επιπλέον υπάρχοντες τύπους διευθύνσεων (π.χ. περισσότερες multicast και aggregatable διευθύνσεις) ή με καινούργιους. Υπάρχουν ήδη σχέδια να συμπεριληφθεί ένα γεωγραφικά βασισμένο σχέδιο όπου η διεύθυνση αντιστοιχεί σε μια γεωγραφική τοποθεσία και αντίστροφα.

2.3.4. Διευθύνσεις Unicast (μόνο-μετάδοσης)

Μια unicast διεύθυνση προσδιορίζει ένα μοναδικό interface και πακέτα, τα οποία στέλνονται σε μια unicast διεύθυνση προορισμού παραδίδονται σε αυτό και μόνο το interface. Το IPv6 περιλαμβάνει διάφορους υποτύπους unicast διευθύνσεων.

2.3.4.1. Aggregatable unicast διευθύνσεις

Οι aggregatable global unicast διευθύνσεις είναι ένα ιεραρχικά δομημένο σχήμα διευθύνσεων, το οποίο αποτελεί το αρχικά χρησιμοποιούμενο πλάνο ανάθεσης διευθύνσεων για τους IPv6 κόμβους. Αυτή η μορφή διευθύνσεων έχει σχεδιαστεί για να βελτιστοποιήσει τη δρομολόγηση υψηλών ταχυτήτων στα δίκτυα κορμού του διαδικτύου εισάγοντας μια πολυεπίπεδη τοπολογία διευθύνσεων χωρισμένες σε *public, site, interface* τοπολογίες. Η μορφή της διεύθυνσης είναι όπως στο παρακάτω σχήμα:



Σχήμα 8: Μορφή aggregatable unicast διευθύνσεων

Η μορφή της διεύθυνσης αποτελείται από τα τέσσερα πεδία Id για μια ιεραρχική δομή τεσσάρων επιπέδων :

- Top-Level Aggregation Identifiers (TLA ID) : χρησιμοποιούνται στην κορυφή της ιεραρχίας.
- Next Level Identifiers (NLA ID) : χρησιμοποιούνται από οργανισμούς
- Site Level Aggregation Identifiers (SLA ID) : αντιστοιχεί στα σημερινά υποδίκτυα του IPv4
- Interface ID : προσδιορίζει ένα μοναδικό Interface ενός IPv6 host

Υπάρχει επίσης ένα δεσμευμένο πεδίο (RES) , το οποίο είναι δυνατόν να προσφέρει μελλοντική αναβάθμιση των TLA ή/και NLA πεδίων.

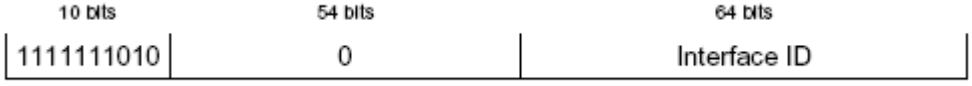
2.3.4.2 Local Addresses (Τοπικές διευθύνσεις)

Το IPv6 προσδιορίζει τρεις τύπους διευθύνσεων για τοπική χρήση και μόνο, δηλαδή IP πακέτα που περιέχουν τοπική διεύθυνση πηγής ή προορισμού περιορίζονται σε μια φυσική περιοχή. Τα τοπικά πακέτα δε δρομολογούνται ποτέ έξω από αυτή τη φυσική περιοχή.

Η Loopback διεύθυνση, 0:0:0:0:0:0:0:1 (::1) αναφέρεται στο εικονικό Interface, το οποίο είναι ενσωματωμένο σε κάθε IPv6 host για τοπική εντός host επικοινωνία. Έχει την ίδια λειτουργικότητα με το localhost interface (127.0.0.1) του IPv4.

Οι Link local διευθύνσεις χρησιμοποιούνται για επικοινωνία σε ένα μοναδικό τμήμα (segment) του δικτύου IPv6. Αυτό θα μπορούσε να συμβαίνει σε ένα οικιακό δίκτυο, μια μικρή επιχείρηση ή σε 2 υπολογιστές συνδεδεμένους απ' ευθείας μεταξύ τους. Κάθε IPv6 interface απαιτείται να έχει τουλάχιστον μια link local διεύθυνση ανατεθειμένη και αυτόματα αναθέτει στον εαυτό του μια κατά τη στιγμή της εκκίνησής του. Το πώς πραγματοποιείται αυτή η ανάθεση εξαρτάται στο υποκείμενο μέσο (π.χ. Ethernet, ATM, IEEE 1394 κ.ο.κ.).

Μια link local διεύθυνση κατασκευάζεται με το πρόθεμα FE80::/10 και ένα 64 bit interface id συμπληρωμένο με 54 μηδενικά bit ενδιάμεσα. Η μορφή της διεύθυνσης φαίνεται στο σχήμα 8

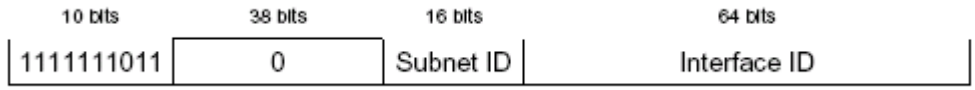


Σχήμα 9: Η link local διεύθυνση

Οι link local διευθύνσεις χρησιμοποιούνται ευρέως στις διαδικασίες αυτόματης ρύθμισης παραμέτρων (autoconfiguration) του IPv6.

Οι Site Local διευθύνσεις έχουν σχεδιαστεί για να επιτρέπουν σε τοποθεσίες με πολλαπλούς συνδέσμους ή τμήματα δικτύου να επικοινωνούν τοπικά χωρίς την ανάγκη ενός γενικού (global) προθέματος. Αυτή θα μπορούσε να είναι η περίπτωση ενός απομονωμένου εταιρικού δικτύου ή μιας κατοικημένης περιοχής χωρίς την ανάγκη γενικής (global) επικοινωνίας.

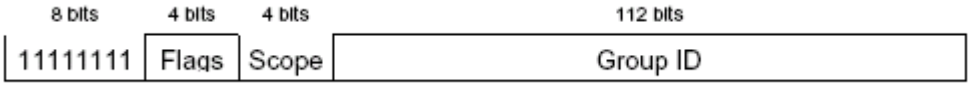
Η δομή μιας site local διεύθυνσης είναι όμοια με τη δομή της link local διεύθυνσης, εκτός από το καινούριο πρόθεμα FEC0::/10 και το καινούριο πεδίο subnet id (αναγνωριστικό υποδικτύου). Η δομή φαίνεται στο παρακάτω σχήμα



Σχήμα 10:. Η site local διεύθυνση

2.3.5. Διευθύνσεις multicast (πολλαπλής διανομής)

Μια multicast διεύθυνση χρησιμοποιείται για να στέλνει πακέτα από μια πηγή σε πολλαπλούς προορισμούς. Το IPv6 θα κάνει το multicasting έναν πιο κοινό τρόπο επικοινωνίας, αφού κάθε IPv6 δρομολογητής απαιτείται να χειρίζεται τη δρομολόγηση multicast. Μια multicast IPv6 διεύθυνση αποτελείται από το πρόθεμα διεύθυνσης 11111111 (FF::/8) ακολουθούμενο από μερικές σημαίες (flags), την εμβέλεια του multicast και τέλος ένα αναγνωριστικό της ομάδας στην οποία λαμβάνει χώρα το multicast (multicast group). Στην εικόνα 2.6 φαίνεται η δομή της multicast διεύθυνσης.



Σχήμα 11: Η multicast διεύθυνση

Στο πεδιο flags, το τέταρτο bit υποδεικνύει, αν η multicast διεύθυνση είναι παροδική (transient) ή όχι. Οι παροδικές διευθύνσεις κατασκευάζονται για προσωρινές συνόδους (sessions) multicasting, όπως μια τηλεδιάσκεψη, ενώ μια μη παροδική διεύθυνση (non transient) είναι δεσμευμένη για ειδικές προκαταχωρημένες υπηρεσίες. Για παράδειγμα, το multicast group FF02::1 αναφέρεται σε όλους τους κόμβους στην τρέχουσα σύνδεση και το FF02::2 αναφέρεται σε όλους τους δρομολογητές. Μια πλήρης λίστα των καταχωρημένων multicast διευθύνσεων υπάρχει στο δικτυακό χώρο του IANA[1].

Το πεδίο scope (εμβέλεια) υποδεικνύει μέχρι πού μπορούν να δρομολογηθούν τα πακέτα που στέλνονται στο multicast group. Ο πίνακας 2.3 παρουσιάζει τις μέχρι στιγμής ανατεθειμένες τιμές εμβέλειας όπως ορίζονται στο RFC 2373 [2].

Πίνακας 2.3: Τιμές εμβέλειας του multicast

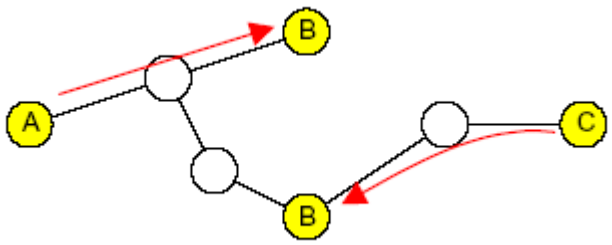
Value	Definition Scope
0	Reserved
1	Node-local scope
2	Link-local scope
5	Site-local scope
8	Organization-local scope
E	Global scope
F	Reserved

Οι τιμές που απουσιάζουν από τον πίνακα, δεν έχουν μέχρι στιγμής καταχωρηθεί και είναι διαθέσιμες στους διαχειριστές του δικτύου για να τις ορίσουν οι ίδιοι.

Τέλος, το πεδίο group identifier της διεύθυνσης διαχωρίζει μια multicast σύνοδο μέσα στην τρέχουσα εμβέλεια. Στο IPv6, το multicast θεωρείται σαν ένας κοινός τρόπος επικοινωνίας, σε αντίθεση με ότι συνέβαινε στο IPv4. Αυτό καθίσταται πολύ εύκολα αντιληπτό παρατηρώντας το αναγνωριστικό μήκους 112 bit του IPv6 σε σχέση με τα 28 bits που είναι διαθέσιμα στις διευθύνσεις τάξεως D του IPv4. Για παράδειγμα το multicast στο IPv6 αντικαθιστά το broadcast στο IPv4.

2.3.6. Διευθύνσεις anycast (μετάδοση σε οποιονδήποτε)

Το anycast είναι ένα καινούριο χαρακτηριστικό που παρουσιάζεται για πρώτη φορά στο IPv6. Μια anycast διεύθυνση είναι μια IPv6 διεύθυνση ανατεθειμένη σε πολλαπλά interfaces, η οποία συχνά ανήκει σε διαφορετικούς κόμβους. Οι anycast διευθύνσεις δε διακρίνονται από τις unicast και μπορεί να χρησιμοποιήσουν οποιοδήποτε σχήμα ανάθεσης unicast διεύθυνσης. Τα πακέτα που στέλνονται σε μια anycast διεύθυνση παραλαμβάνονται από το κοντινότερο, σύμφωνα με την απόσταση δρομολόγησης, στον αποστολέα interface.Το παρακάτω σχήμα απεικονίζει ένα απλό παράδειγμα με 2 hosts (A και C), όπου και οι δύο ορίζουν τον B σαν τη διεύθυνση προορισμού.



Σχήμα 12: Anycasting

Το anycasting μπορεί να χρησιμοποιηθεί για load balancing (εξισορρόπηση φόρτου δικτύου) μεταξύ πολλαπλών DNS, web ή database εξυπηρετητών. Η fuzzy (ασαφής) δρομολόγηση είναι άλλο ένα πιθανό χαρακτηριστικό με διευθύνσεις anycast όπου ο αποστολέας προσδιορίζει ότι τα πακέτα θα πρέπει να δρομολογηθούν μέσω οποιουδήποτε δρομολογητή σε ένα καθορισμένο δίκτυο. Επειδή είναι ένα νέο χαρακτηριστικό στον κόσμο του διαδικτύου, το anycast είναι ακόμα ένα θέμα προς έρευνα και καινούριες εφαρμογές εξελίσσονται συνεχώς.

2.3.7. Domain Name System (Σύστημα ονομασίας περιοχών)

Οι επεκτάσεις του DNS προκειμένου να υποστηρίζουν το IPv6 περιλαμβάνουν ένα νέο τύπο record (εγγραφής) για τις IPv6 διευθύνσεις που ονομάζεται AAAA και μια νέα περιοχή (domain) DNS για την IPv6 διεύθυνση την IP6.INT . Επομένως μια IPv6 διεύθυνση όπως η :

4321:0:1:2:3:4:567:89ab

θα έχει τη διεύθυνση αναζήτησης στο DNS:

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT.

Το IPv6 εισάγει τον όρο autoconfiguration, δηλαδή την ικανότητα ρύθμισης ενός κόμβου χωρίς τη μεσολάβηση του ανθρώπινου παράγοντα. Αυτό είναι ένα ευπρόσδεκτο χαρακτηριστικό για τους διαχειριστές δικτύου, αλλά επίσης και για τους άπειρους χρήστες.

2.3.8 Μηχανισμοί autoconfiguration

Το IPv6 παρέχει τη λειτουργικότητα του autoconfiguration χρησιμοποιώντας τρεις μηχανισμούς:

- Neighbor discovery (ανακάλυψη γειτονικών κόμβων): Είναι ουσιαστικά ένα σύνολο από ICMPv6 μηνύματα, τα οποία αντικαθιστούν τις υπηρεσίες που παρέχονται από το ARP και το Router Discovery όπως αυτά ορίζονται στο IPv4.
- Stateless autoconfiguration: Αναθέτει μια παγκοσμίως νόμιμη διεύθυνση σε ένα interface συνδυάζοντας την link local διεύθυνσή του με την πληροφορία του προθέματος διεύθυνσης που δημοσιοποιείται (advertised) από τους κοντινούς δρομολογητές. Καμία αλληλεπίδραση από εξυπηρετητές ή ανθρώπους δεν απαιτείται για αυτή τη διαδικασία
- Stateful autoconfiguration: Παρέχει επιπρόσθετες παραμέτρους αυτόματης ρύθμισης, όπως τους εξυπηρετητές DNS χρησιμοποιώντας το πρωτόκολλο DHCP για το IPv6 (DHCPv6). Αυτή είναι και η προτιμώμενη μέθοδος ανάθεσης διευθύνσεων, αφού δίνει στους διαχειριστές πλήρη έλεγχο της διαδικασίας ανάθεσης.

Αυτοί οι μηχανισμοί μπορούν να χρησιμοποιηθούν μαζί ή ξεχωριστά αναλόγως της τοπολογίας δικτύου και των παραμέτρων δρομολογητή που ορίζονται από το διαχειριστή του δικτύου.

2.4. Διαδικασία αυτόματης ρύθμισης παραμέτρων

Η αυτόματη ρύθμιση παραμέτρων ενός κόμβου είναι μια διαδικασία που αποτελείται από πολλά βήματα. Η πλήρης διαδικασία είναι η ακόλουθη:

1) Το interface ενεργοποιείται

2) Μια link local διεύθυνση δημιουργείται (αλλά δεν ανατίθεται στο interface) συνενώνοντας το προκαθορισμένο πρόθεμα FE80::/10 με ένα 64-bit αναγνωριστικό του interface (interface identifier), όπως περιγράφεται στην ενότητα 2.3.4. Το αναγνωριστικό του interface μπορεί τυπικά να είναι η IEEE 802 διεύθυνση της κάρτας του interface δικτύου (π.χ. Ethernet, FDDI) ή ένας άλλος μοναδικός αριθμός που έχει ληφθεί από άλλα τμήματα του κόμβου (π.χ. ο σειριακός αριθμός της μητρικής πλακέτας).

3) Κατόπιν χρησιμοποιείται το neighbor discovery για να ελέγξει, αν η νέα διεύθυνση είναι μοναδική (στη ζεύξη). Αυτό γίνεται στέλνοντας μηνύματα αιτήσεις neighbor discovery με την διεύθυνση προορισμού να τίθεται στη διεύθυνση που ελέγχεται και τη διεύθυνση πηγής να τίθεται στην ακαθόριστη διεύθυνση (::). Αν μέσω μηνυμάτων neighbor discovery ληφθεί η πληροφορία ότι η διεύθυνση δεν είναι μοναδική, τότε χρειάζεται να επαναδημιουργηθεί είτε χειροκίνητα, είτε τυχαία και να επαναληφθεί η διαδικασία.

4) Όταν διαπιστωθεί ότι η link local διεύθυνση είναι μοναδική, η διεύθυνση ανατίθεται στο interface που ρυθμίζεται εκείνη τη στιγμή.

5) Χρησιμοποιώντας τη νέα link local διεύθυνση ως διεύθυνση πηγής, στέλνεται ένα μήνυμα αίτησης neighbor discovery για δρομολογητές στο multicast group «όλοι οι δρομολογητές» (FF02::2).

6) Προς απάντηση στις αιτήσεις neighbor discovery για δρομολογητές, οι δρομολογητές στέλνουν ένα unicast μήνυμα δημοσιοποίησης neighbor discovery για δρομολογητές προς τον κόμβο. Η δημοσιοποίηση ορίζει, αν ο κόμβος θα πρέπει να χρησιμοποιήσει stateless ή stateful autoconfiguration θέτοντας τη σημαία managed configuration κατάλληλα. Αν χρησιμοποιηθεί stateless autoconfiguration, κατασκευάζεται μια site local ή global διεύθυνση χρησιμοποιώντας ένα πρόθεμα διεύθυνσης, το οποίο συμπεριλαμβάνεται στη δημοσιοποίηση καθώς και την τρέχουσα link local διεύθυνση. Η νέα διεύθυνση ανατίθεται κατόπιν στο interface (το οποίο τώρα έχει δύο διευθύνσεις). Ο host τώρα ρυθμίζεται για επικοινωνία μέσα στο τμήμα του δικτύου ή ακόμα και σε όλο το διαδίκτυο.

7) Αν δεν υπάρχει καμία απάντηση από δρομολογητή, ή αν η σημαία managed configuration από το μήνυμα δημοσιοποίησης ορίζει ότι η διευθυνσιοδότηση δεν μπορεί να γίνει αυτόματα από το ίδιο το host, τότε χρησιμοποιείται stateful autoconfiguration. Αυτό επιτυγχάνεται μέσω του πρωτοκόλλου DHCPv6 το οποίο ορίζει τύπους μηνυμάτων για τη ρύθμιση όλων των απαραίτητων παραμέτρων.

2.5 Υποστήριξη εφαρμογών πραγματικού χρόνου

Το IPv6 για να ικανοποιήσει τις απαιτήσεις της σημερινής αύξησης των real time εφαρμογών, όπως ροές εικόνας και ήχου (streaming video,audio, έχει τα εξής νέα χαρακτηριστικά.

2.6. Ροές (Flows)

Στην επικεφαλίδα του πακέτου IPv6 υπάρχει ένα πεδίο μήκους 20-bit, το οποίο λέγεται flow label (ετικέτα ροής). Μια ροή (flow) ορίζεται ως ένα σύνολο πακέτων, τα οποία έρχονται από την ίδια πηγή και κατευθύνονται στον ίδιο προορισμό (unicast ή multicast) έχοντας την ίδια ετικέτα ροής (flow label). Οι νέες ετικέτες ροής λαμβάνουν τυχαίες τιμές που κυμαίνονται μεταξύ της τιμής 0x1 και 0xFFFFF.

Οι ροές μπορεί να χρησιμοποιηθούν για να υποδηλώσουν ότι ορισμένα πακέτα απαιτούν ειδική μεταχείριση από τους δρομολογητές IPv6 στο δίκτυο όπως χαμηλή καθυστέρηση ή υψηλό εύρος ζώνης (bandwidth). Επίσης μπορεί να χρησιμοποιηθεί σε συνδυασμό με την επικεφαλίδα του δρομολογητή για να αναγκάσει όλα τα πακέτα να ακολουθήσουν το ίδιο μονοπάτι στο δίκτυο. Αν χρειάζεται διαχείριση των διαθέσιμων πόρων του δικτύου μπορεί να χρησιμοποιηθεί ένα πρωτόκολλο όπως το RSVP (Resource Reservation Protocol – πρωτόκολλο δέσμευσης πόρων). Το RSVP είναι βασισμένο στη χρήση ροών και επομένως είναι κατάλληλο για το IPv6[3].

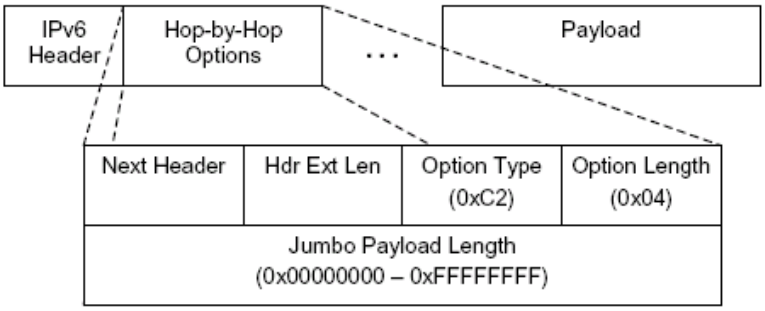
2.6.1 Traffic class (τάξη κυκλοφορίας δικτύου)

Το πεδίο traffic class μήκους 8-bit αποτελεί ένα ακόμα πεδίο της επικεφαλίδας του IPv6. Παρομοίως με το πεδίο TOS (τύπος υπηρεσίας) του IPv4, το πεδίο traffic class παρέχει τη δυνατότητα χρήσης διαφοροποιημένων υπηρεσιών. Παρέχει επίσης τη δυνατότητα δρομολόγησης βάση προτεραιότητας, όπου πακέτα από την ίδια πηγή μπορεί να φτάνουν γρηγορότερα αν έχει καθοριστεί για αυτά υψηλότερη προτεραιότητα.

2.6.2 Jumbograms (γιγαντογραφήματα)

Το IPv6 προκειμένου να υποστηρίξει κυκλοφορία υψηλών ταχυτήτων σε πραγματικό χρόνο, παρέχει τη δυνατότητα αποστολής πολύ μεγάλων πακέτων, των λεγόμενων γιγαντογραφημάτων (jumbograms). Συνήθως το 16-bit πεδίο payload της επικεφαλίδας του IPv6 πακέτου περιορίζει το μήκος του μέγιστου ωφέλιμου φορτίου πακέτου στα 65535 bytes. Χρησιμοποιώντας την επιλογή jumbo payload σε μια επικεφαλίδα επέκτασης hop-by-hop,το μέγιστο μήκος επεκτείνεται στα 4294967295 bytes (χρησιμοποιώντας ένα πεδίο μήκους 32 bit). Παρ' όλα αυτά η χρήση των γιγαντογραφημάτων απαιτεί το υποκείμενο επίπεδο ζεύξης δεδομένων να έχει τιμή MTU (μέγιστης μεταφερόμενης μονάδας πληροφορίας) τουλάχιστον 65575 bytes (65535 + 40 bytes για την επικεφαλίδα του IPv6).

Όταν χρησιμοποιούνται οι επιλογές jumbo payload, η τιμή του πεδίου payload length στην επικεφαλίδα του IPv6, πρέπει να τίθεται στο μηδέν. Η τιμή του πεδίου next header (επόμενη επικεφαλίδα) της επικεφαλίδας του πακέτου IPv6 πρέπει επίσης να τίθεται στο μηδέν ώστε να δείχνει την επόμενη hop-by-hop επικεφαλίδα επέκτασης, όπου το πραγματικό μήκος του ωφέλιμου φορτίου του πακέτου μπορεί να ληφθεί όπως φαίνεται στο σχήμα 13.



Σχήμα 13: Η επιλογή Jumbo Payload

3. ΜΗΧΑΝΙΣΜΟΙ ΜΕΤΑΒΑΣΗΣ

3.1 Γενικά

Οι μηχανισμοί μετάβασης που έχουν επινοηθεί μπορούν να κατηγοριοποιηθούν στις εξής κατηγορίες::

- Διπλή στοίβα (ή αλλιώς «διπλού επιπέδου»)
- Τούνελ
- Μετάφραση και εξουσιοδότηση.

Όταν υποστηρίζεται IPv6 σ' ένα δίκτυο αυτό προσθέτει πολλές νέες δυνατότητες χωρίς να ακυρώνει τις ήδη υπάρχουσες. Βέβαια έχοντας 2 πρωτόκολλα επ' αόριστον δεν λύνει κανένα πρόβλημα και σε κάποια χρονική στιγμή πρέπει να γίνει πλήρης μετάβαση. Μια διπλή στοίβα μπορεί να επικοινωνήσει με τον καθένα. Η προώθηση μέσω «τούνελ» είναι ένας πολύ δυνατός μηχανισμός μετάβασης, αφού επιτρέπει την τρέχουσα IPv4 υποδομή να χρησιμοποιηθεί για επικοινωνία με IPv6. Τα τούνελ μπορούν να απομακρυνθούν μία τη φορά μόλις γίνει διαθέσιμη εγγενής συνδεσιμότητα με IPv6, κι έτσι αυτός ο μηχανισμός δεν προσθέτει δυσκολίες μετάβασης

Η μετάφραση μεταξύ IPv4 και IPv6 είναι από τους πιο αντιλεγόμενους μηχανισμούς μετάβασης αφού η μετάφραση μεταξύ διαφορετικών εκδόσεων IP έχει πολλούς περιορισμούς παρόμοιους με το NAT, κάτι που υποτίθεται έχει ξεφορτωθεί το IPv6. Από την άλλη, αν δεν υπάρχει κάποιας μορφής μετάφραση, υπάρχουν μόνο 2 επιλογές, ή να αναβαθμιστούν όλοι οι υπολογιστές και να έχουν διπλή στοίβα πριν αρχίσει κάποιος υπολογιστής να τρέχει μόνο IPv6 ή να μην μπορούν να επικοινωνούν άμεσα οι υπολογιστές που χρησιμοποιούν μόνο IPv4 με αυτούς που χρησιμοποιούν μόνο IPv6.

Σχεδιάζοντας τη μετάβαση

Στο RFC 3194 προτείνεται 1 τρόπος για να υπολογιστεί το πόσο χρησιμοποιούνται οι διευθύνσεις έτσι ώστε να μπορούν να βγουν συμπεράσματα σύμφωνα με την εμπειρία μας. Ο αριθμός αυτός είναι «ο λόγος HD» που μπορεί να υπολογιστεί ως εξής:

$$HD = \frac{\log(\chi\rho\eta\sigma\iota\mu o\pi o\iota\eta\mu\acute{\varepsilon}\nu\varepsilon\varsigma\_\delta\iota\varepsilon\upsilon\theta\acute{\upsilon}\nu\sigma\varepsilon\iota\varsigma)}{\log(\sigma\acute{\upsilon}\nu o\lambda o\_\delta\iota\varepsilon\upsilon\theta\acute{\upsilon}\nu\sigma\varepsilon\omega\nu)}$$

Έτσι αν μια εταιρεία έχει ένα παλιό δίκτυο κλάσης Β με 65.535 διευθύνσεις και χρησιμοποιεί 4096, ο λόγος log(4096)/log(65536)=12/16 = 0.75 ή 75%. Σε αυτό το παράδειγμα, η βάση του λογαρίθμου είναι το 2 αλλά γενικότερα δεν έχει σημασία η βάση γιατί ο λόγος είναι αυτός που μετράει. Μελετώντας το τηλεφωνικό δίκτυο ένας λόγος HD 80% ή μικρότερος αναπαριστά ένα καλό επίπεδο που μπορεί μια εταιρεία εύκολα να διαχειριστεί. Αντίθετα ένας λόγος από 87% και πάνω αναπαριστά μια κατάσταση όπου ο χώρος διευθύνσεων είναι τόσο δύσκολο στη διαχείριση τους ώστε υιοθετούνται τεχνικές για να μειώσουν τις χρησιμοποιούμενες διευθύνσεις και το μήκος των διευθύνσεων αυξάνεται.

Για το χώρο διευθύνσεων του IPv4 με 317 εκατομμύρια χρησιμοποιούμενες διευθύνσεις από τις 3.7 δισεκατομμύρια, ο λόγος HD=88.9%. Με υπολογισμούς που έχουν γίνει υπάρχει χώρος ακόμα για περίπου 163 εκατομμύρια διευθύνσεις, με συνολικό αριθμό υπολογιστών 480 εκατομμύρια.

Λαμβάνοντας υπόψη το λόγο HD και τους περιορισμούς NAT, μπορούμε λογικά να υποθέσουμε γιατί η υιοθέτηση του IPv6 σε κάποιο σημείο στο μέλλον μπορεί είναι πολύ πιθανή. Υπάρχουν 4 φάσεις μεγάλης σημασίας κατά τη μετάβαση:

Απόκτηση εμπειρίας με το IPv6. Αυτή η φάση συνεπάγεται την ενεργοποίηση του IPv6 πρώτα δοκιμαστικά σε ένα μικρό αριθμό συστημάτων, την παρακολούθηση του τι συμβαίνει και τη διεξαγωγή κάποιων πειραμάτων..

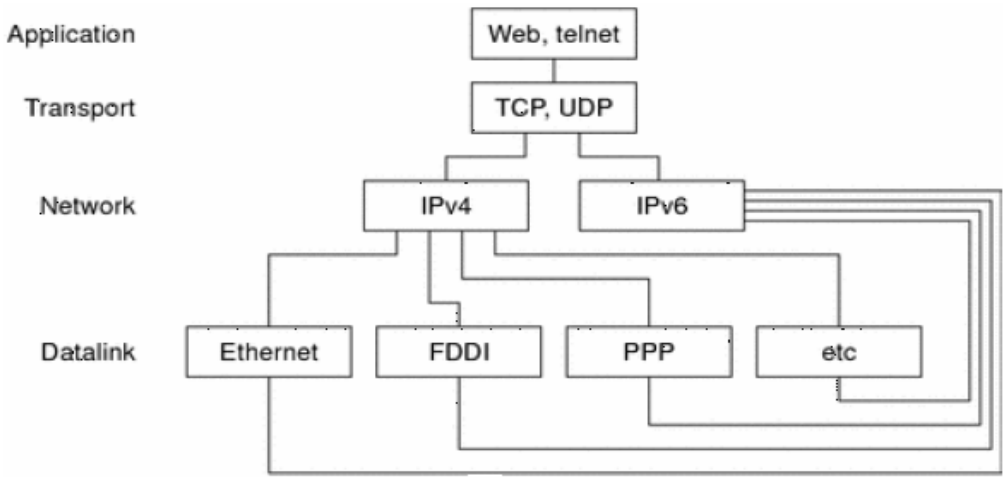
Προσθήκη μειωμένης υποστήριξης IPv6. Σε αυτό το σημείο, είναι πιθανό να γίνουν διάφορες τεχνικές αλλαγές για την καλύτερη απόδοση στο IPv6 αλλά μπορεί να χρειάζεται ακόμα IPv4 συνδεσιμότητα..

Προαγωγή του IPv6 σε αντίστοιχο με το IPv4. Αυτό σημαίνει την απόσυρση του υλικού που χρησιμοποιεί μόνο IPv4 πρωτόκολλο καθώς και του αντίστοιχου λογισμικού ή την υιοθέτηση τεχνικών μετάβασης ώστε να είναι δυνατή η παροχή και IPv4 υπηρεσιών. Είναι δύσκολη η επιστροφή στο IPv4 μετά από αυτό το σημείο γιατί οι χρήστες μπορεί τώρα να εξαρτώνται από τις δυνατότητες μόνο του IPv6.

Τερματισμός χρήσης του IPv4. Το να σταματήσει κανείς να χρησιμοποιεί IPv4 δε θα είναι δυνατό για λίγο χρόνο ακόμα, αλλά το να υπάρχουν κομμάτια δικτύου που θα υποστηρίζουν μόνο IPv6 είναι κάτι που μπορεί να συμβεί σχετικά σύντομα, ειδικά με τη βοήθεια των τεχνικών μετάβασης έτσι ώστε να είναι δυνατή μέχρι τότε η χρήση υπηρεσιών IPv4.

Ένας καλός τρόπος σχεδιασμού θα έφτανε μέχρι τη φάση 3 της μετάβασης σε 3 χρόνια, με ενδιάμεσους στόχους κατά περίπτωση.

3.2 Μηχανισμοί Dual Stack



Σχήμα 14:dual stack

Οι κόμβοι διπλής στοίβας IPv4/IPv6 δουλεύουν περίπου με τον ίδιο τρόπο που δουλεύουν και άλλα είδη κόμβων πολλαπλής στοίβας. Καθώς πακέτα λαμβάνονταιστο επίπεδου δικτύου από το επίπεδο σύνδεσης, ξετυλίγονται και εξετάζονται οι επικεφαλίδες τους. Αν το πεδίο έκδοσης (version) της επικεφαλίδας είναι τέσσερα,τότε το πακέτο επεξεργάζεται από την IPv4 στοίβα. Ενώ αν είναι έξι τότε επεξεργάζεται από την IPv6 στοίβα.

Ο μηχανισμός ουσιαστικά αναφέρεται στην ενεργοποίηση και των 2 πρωτοκόλλων στο δίκτυο και βασίζεται στη πολύ απλή ιδέα της ενεργοποίησης και των δύο stacks των πρωτοκόλλων στα δικτυακά interfaces του εξοπλισμού. Με τον τρόπο αυτό επιτυγχάνεται σχετικά απλά η επικοινωνία των κόμβων του δικτύου με άλλους, είτε αυτοί χρησιμοποιούν το IPv4 πρωτόκολλο είτε το IPv6 ή και τα δύο.

Η επιλογή για το ποιο από τα δύο πρωτόκολλα θα χρησιμοποιήσει κάθε εφαρμογή εξαρτάται είτε από εσωτερική επιλογή (από τον κατασκευαστή του λογισμικού) είτε από την απάντηση της υπηρεσίας ονοματολογίας του δικτύου (DNS). Οι μηχανισμοί αυτοί είναι απλοί στην υλοποίηση τους, η οποία έγκειται απλώς στην εγκατάσταση και των δυο πρωτοκόλλων στα λειτουργικά συστήματα των μηχανημάτων του δικτύου.

Έτσι τα μηχανήματα στα οποία υπάρχει εγκατεστημένο και το IPv4 και το IPv6 πρωτόκολλο μπορούν να λάβουν και να προωθήσουν πακέτα και από τα δυο πρωτοκολλά. Η επιλογή της στοίβας η οποία θα χρησιμοποιηθεί γίνεται κυρίως βάση του αποτελέσματος της DNS αναζήτησης. Δηλαδή, αν ο κόμβος με τον οποίο θα γίνει επικοινωνία έχει καταγραμμένη μόνο IPv6 διεύθυνση, χρησιμοποιείται η IPv6 στοίβα, αν υπάρχει μόνο IPv4 διεύθυνση χρησιμοποιείται η IPv4 στοίβα και στην περίπτωση που υπάρχουν εγγραφές τόσο IPv4 όσο και IPv6 διευθύνσεων, η default συμπεριφορά είναι να χρησιμοποιηθούν οι IPv6. Σε αυτό το σημείο πρέπει να τονιστεί ότι για να εγγράψει ο κόμβος την IPv6 σύνδεση του, πρέπει με κάποιο τρόπο να του παρέχεται IPv6 συνδεσιμότητα (είτε native είτε μέσω tunnel), εκτός από το να έχει απλώς εγκαταστήσει το IPv6 πρωτόκολλο. Και αυτή ακριβώς είναι κυρίως η αδυναμία της συγκεκριμένης κατηγορίας μηχανισμών στον παρόν στάδιο μετάβασης. Δηλαδή, απομονωμένοι dual-stack κόμβοι στους οποίους δεν παρέχεται IPv6 σύνδεση, δεν μπορούν να επικοινωνήσουν μεταξύ τους και σε αυτές τις περιπτώσεις είναι απαραίτητη η συνεργασία της συγκεκριμένης κατηγόριας μηχανισμών με κάποιο άλλο μηχανισμό μετάβασης, όπως για παράδειγμα με τους μηχανισμούς tunneling, η οποία είναι μια τεχνική που χρησιμοποιείται κατά κόρον σήμερα. Λογικά όμως, σε μεταγενέστερα σταδία μετάβασης, αυτή η κατηγόρια θα χρησιμοποιηθεί περισσότερο.

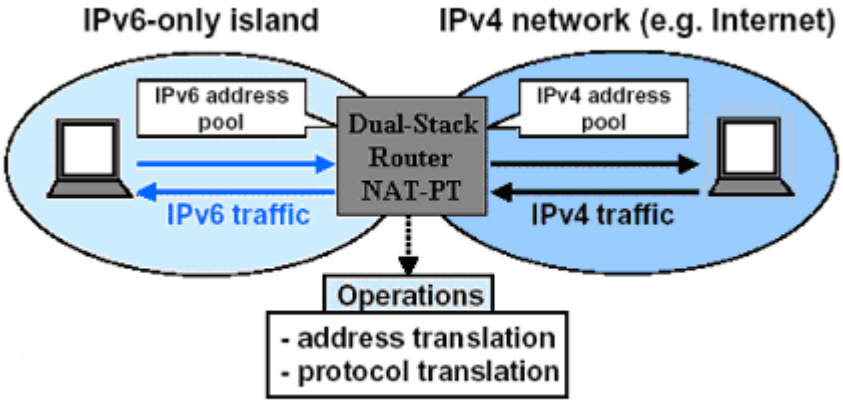
3.3 Μηχανισμοί Translation

Οι μηχανισμοί αυτοί επιτρέπουν την επικοινωνία μεταξύ κόμβων που υποστηρίζουν μόνο IPv4 (IPv4-only) και κόμβων που υποστηρίζουν μόνο IPv6 (IPv6-only), και ουσιαστικά ‘μεταφράζουν’ την κίνηση από το ένα πρωτόκολλο στο άλλο. Αναμένεται ότι θα χρησιμοποιηθούν αρκετά στα τελευταία σταδία μετάβασης, και κυρίως για τις περιπτώσεις μηχανημάτων που δεν μπορούν να αναβαθμιστούν στο IPv6.

Οι κυριότεροι μηχανισμοί αυτής της κατηγορίας είναι ο **NAT-PT** (Network Address Translation – Protocol Translation) ο οποίος χρησιμοποιεί SIIT (Stateless IP ICMP Translation) αλγόριθμους για μετατροπή των IPv6 πακέτων σε IPv4 και αντίστροφα και οι **BIS** (Bump In The Stack) και **BIA** (Bump in the API) οι οποίοι εκτελούν τις ίδιες διαδικασίες, αλλά ο ένας στο επίπεδο μεταφοράς και ο τελευταίος στο επίπεδο εφαρμογής.

3.3.1 NAT-PT

Ο NAT-PT ((Network Address Translation – Protocol Translation) μηχανισμός, ο πλέον διαδεδομένος και καθιερωμένος της κατηγορίας των translation mechanisms , στηρίζεται σε λειτουργία παρόμοια με αυτή των κλασσικών NATs.



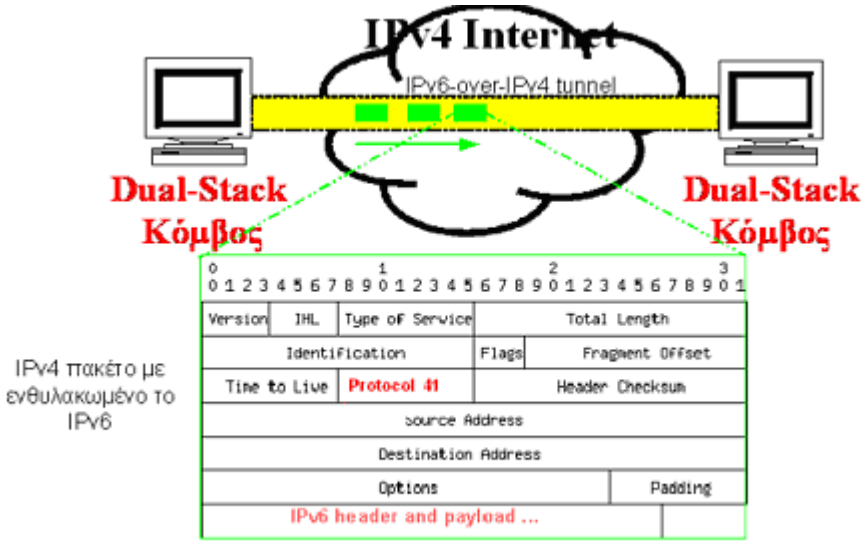
Σχήμα 15: NAT-PT μηχανισμός

Υπάρχει ο δρομολογητής στο σύνορο μεταξύ του IPv6 και του IPv4 δικτύου, στον οποίο εγκαθίσταται το NAT-PT, ο οποίος διατηρεί δυο δεξαμενές (pools) διευθύνσεων, μια με IPv6 διευθύνσεις και μια με IPv4, τις οποίες αντιστοιχεί δυναμικά για να δημιουργηθεί η συνοδός για επικοινωνία μεταξύ του IPv4 host με τον IPv6. Επιπλέον όμως, παράλληλα με την μετάφραση των διευθύνσεων, γίνεται και μετάφραση της IPv6 επικεφαλίδας σε IPv4 και αντίστροφα. Αυτό φυσικά, προσθέτει στο συγκεκριμένο μηχανισμό και το μειονέκτημα ότι κάποια services που προσφέρει το ένα πρωτόκολλο αλλά όχι και το άλλο είναι πιθανό να χαθούν κατά την ‘μετάφραση’ αφού οι επικεφαλίδες των δυο πρωτοκόλλων δεν είναι ίδιες. Επιπλέον, οι μηχανισμοί αυτοί φέρουν και τα μειονεκτήματα των κλασικών NATs, λόγω της ‘μετάφρασης’ διευθύνσεων και πρωτοκόλλου που εκτελείται. Και σε αυτή την περίπτωση ισχύει η “best effort” προσέγγιση, και επιπλέον η απ’ άκρου σ’ άκρου ασφάλεια σε επίπεδο δικτύου είναι αδύνατη. Για αυτόν ακριβός τον λόγο, οι συγκεκριμένοι μηχανισμοί πρέπει να χρησιμοποιούνται μόνο στην περίπτωση που υπάρχει ανάγκη επικοινωνίας IPv4-only και IPv6-only hosts, και όχι σε άλλες περιπτώσεις.

3.4 Μηχανισμοί Tunneling

Για όσο διάστημα διευρύνεται η χρήση του IPv6 είναι χρήσιμο αλλά και αναγκαίο, τουλάχιστον στο μεταβατικό στάδιο, η IPv4 υποδομή να παραμείνει λειτουργική και να χρησιμοποιηθεί επίσης στην μετάδοση φορτίου. Η πιο διαδεδομένη τεχνική, με την οποία γίνεται η εκμετάλλευση της υποδομής IPv4 για την μεταφορά IPv6 πακέτων είναι οι μηχανισμοί tunneling, η τρίτη και σημαντικότερη κατηγορία των μηχανισμών μετάβασης. Το tunneling γενικότερα είναι μια τεχνική που χρησιμοποιείται σε μεγάλο βαθμό σήμερα και στηρίζεται στην ενθυλάκωση ενός πρωτοκόλλου ενός δικτύου σε πακέτα αλλού πρωτοκόλλου για μετάδοση τους πάνω από άλλο δίκτυο (παραδείγματα το GRE και το PPTP πρωτόκολλα που χρησιμοποιούνται σήμερα σε μεγάλο βαθμό). Η τεχνική αυτή χρησιμοποιείται και στο μεταβατικό στάδιο από το IPv4 στο IPv6.Πιο συγκεκριμένα, IPv6 hosts και routers έχουν την δυνατότητα να ανταλλάσσουν IPv6 πακέτα, τα οποία ενθυλακώνουν μέσα σε IPv4 πακέτα, μεταδίδοντας τα έτσι πάνω από το ήδη υπάρχον δίκτυο (internet). Με αυτό τον τρόπο οι ενδιάμεσοι δρομολογητές, αν και δεν υποστηρίζουν

το IPv6 πρωτόκολλο, προωθούν τα ενθυλακωμένα πακέτα σαν να πρόκειται για κανονικά IPv4 πακέτα. Για την λειτουργία των μηχανισμών tunneling πρέπει οι δυο κομβόι στα άκρα του tunnel - οι κομβόι που κάνουν την ενθυλάκωση και την απενθυλάκωση - να είναι dual-stack, να έχουν δηλαδή εγκατεστημένες και τις δυο στοίβες πρωτοκόλλων IPv4 και IPv6. Πιο κάτω φαίνεται η διάδοση των ενθυλακωμένων IPv6 πακέτων, κάτω από IPv4 επικεφαλίδα, πάνω από την IPv4 υποδομή, καθώς και η μορφή των πακέτων που μεταδίδονται.



Σχήμα 16: Μηχανισμοί tunneling.

Για να γίνει πιο κατανοητή η διαδικασία και να αποφευχθούν λάθος συμπεράσματα παραθέτονται οι ακόλουθες έννοιες

IPv4-only node: Ένας κόμβος που υλοποιεί μόνο IPv4 και έχει μόνο IPv4 διεύθυνση. Ο κόμβος αυτός δεν υποστηρίζει IPv6.

IPv6-only node: Ένας κόμβος που υποστηρίζει μόνο IPv6 και μπορεί να επικοινωνήσει μόνο με IPv6 κόμβους και εφαρμογές.

IPv6/IPv4 node: Κόμβος που υλοποιεί τόσο IPv6 όσο και IPv4.

IPv4 node: Κόμβος που υλοποιεί IPv4 (στέλνει και λαμβάνει IPv4 πακέτα). Ο κόμβος αυτός μπορεί να είναι IPv4-only ή IPv6/IPv4 κόμβος.

IPv6 node : Κόμβος που υλοποιεί IPv6 (στέλνει και λαμβάνει IPv6 πακέτα). Ο κόμβος αυτός μπορεί να είναι IPv6-only ή IPv6/IPv4 κόμβος.

3.4.1 Είδη μηχανισμών tunneling:

Οι μηχανισμοί tunneling κατηγοριοποιούνται, ως προς τον μηχανισμό με τον οποίο ο κόμβος εισόδου, ο οποίος πραγματοποιεί την ενθυλάκωση, καθορίζει την διεύθυνση του κόμβου εξόδου(άλλο άκρο του τούνελ), σε μηχανισμούς configured tunnelling και automatic tunnelling.

Στο **configured tunneling** Με τον όρο Configured Tunnel εννοείται το tunnel στο οποίο σε κάθε άκρο ορίζεται ρητά η IPv4 διεύθυνση του απέναντι άκρου. Η τεχνική της διασύνδεσης IPv6 νησίδων πάνω από το IPv4 δίκτυο με την χρήση configured tunnels είναι ο τρόπος που καταρχήν χρησιμοποιήθηκε για την δημιουργία των IPv6 δικτύων. Η τεχνική αυτή

στηρίχτηκε στις τεχνικές tunneling που ήδη υπήρχαν και είναι ευρέως γνωστές. Για το λόγο αυτό παρακάτω ακολουθεί μια αρκετά σύντομη περιγραφή της λειτουργίας της. Τα IPv6 πακέτα προκειμένου να διασχίσουν το IPv4 δίκτυο ενθυλακώνονται σε IPv4 πακέτα των οποίων το πεδίο Identification έχει την τιμή 41, τιμή η οποία χρησιμοποιείται για να δηλώσει ότι το IPv4 πακέτο περιέχει ένα άλλο IPv6. Εννοείται πως το δίκτυο που διασχίζουν τα IPv6 πακέτα πρέπει να επιτρέπει την διέλευση των IPv4 πακέτων με τιμή 41 στο αντίστοιχο πεδίο.

Η διεύθυνση προορισμού των IPv4 πακέτων είναι αυτή που ρητά έχει δηλωθεί κατά

την δημιουργία του tunneling interface στον δρομολογητή (tunnel destination) ενώ

αντίστοιχα η διεύθυνση αποστολέα είναι η IPv4 διεύθυνση του interface. Με αυτόν

τον τρόπο οι δρομολογητές χτίζουν point-to-point links πάνω από την IPv4 υποδομή

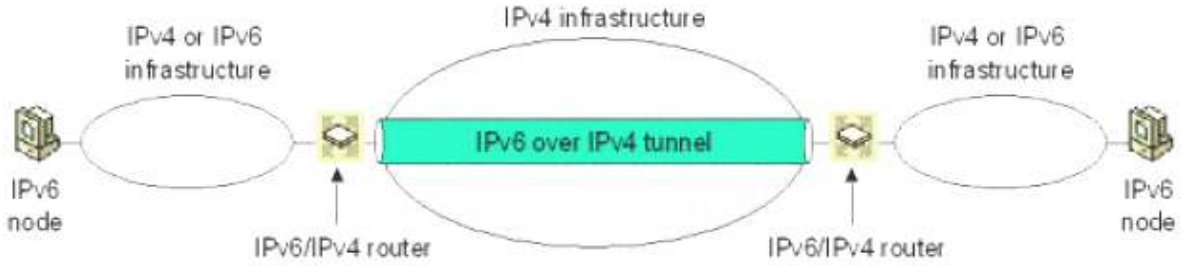
και τα οποία χρησιμοποιούν για την μεταφορά των IPv6 πακέτων

Στο **automatic tunneling** Η Τεχνική Automatic Tunneling κάνει χρήση των IPv4 συμβατών (compatible) IPv6διευθύνσεων. Από τον τρόπο που είναι δομημένες οι διευθύνσεις αυτές, ο σταθμός μπορεί εύκολα να καταλάβει ποιο είναι το άλλο άκρο του tunnel που πρόκειται να δημιουργήσει, για να επικοινωνήσει με τον απέναντι IPv6 σταθμό. Έτσι για να εφαρμοστεί η συγκεκριμένη τεχνική χρειάζεται μόνο να εγκατασταθεί στους σταθμούς των χρηστών το κατάλληλο λογισμικό, το οποίο να εφαρμόζει την τεχνική αυτή.

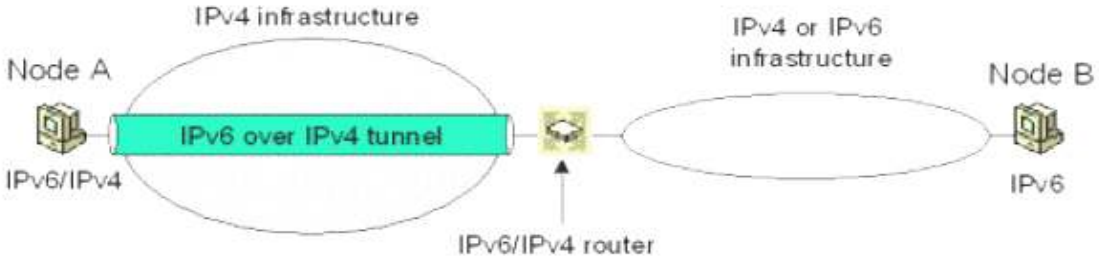
Η IPv4 διεύθυνση του άκρου του τούνελ, μπορεί να προκύψει από την IPv6 διεύθυνση προορισμού του πακέτου που πρόκειται να μεταδοθεί μέσω του τούνελ. Αυτή μπορεί να είναι είτε 6to4 διεύθυνση (επόμενη ενότητα “6to4 Μηχανισμός”) είτε IPv4-compatible διεύθυνση (0:0:0:0:0:0:IPv4 Address) είτε γενικά διεύθυνση στην οποία η IPv4 εμπεριέχεται με κάποιο τρόπο στην IPv6 διεύθυνση. Στην περίπτωση αυτή οι IPv6/IPv4 κομβόι επικοινωνούν πάνω από την IPv4 υποδομή δρομολόγησης χωρίς να χρειάζεται να έχουν γίνει εκ των προτέρων configured τα τούνελ που θα χρησιμοποιηθούν.

Στην πρώτη κατηγορία tunneling συγκαταλέγονται κυρίως οι περιπτώσεις επικοινωνίας

i. Router-to-Router



ii. Host-to-Router



Σχήμα 17: είδη μηχανισμών tunneling

όπου τα πακέτα προωθούνται σε ένα ενδιάμεσο δρομολογητή (router) όπου θα γίνει η απενθυλάκωση τους. Σε αυτή την περίπτωση η διεύθυνση του άκρου του τούνελ είναι διαφορετική από την τελική διεύθυνση προορισμού, άρα απαιτείται η χρήση configured tunneling, αφού η διεύθυνση του router (άκρο του τούνελ) δεν μπορεί να προκύψει από την διεύθυνση προορισμού του πακέτου. Εξαίρεση σε αυτό παρουσιάζει ο 6to4 μηχανισμός και γενικά οι μηχανισμοί όπου ο μεταβατικός μηχανισμός υλοποιείται στον συνοριακό δρομολογητή του site (από την διεύθυνση του οποίου καθορίζονται οι διευθύνσεις του site), οι οποίοι αν και συγκαταλέγονται στην Router-to-Router περίπτωση επικοινωνίας, μπορεί από την διεύθυνση προορισμού να υπολογιστεί η διεύθυνση του router που θα εκτελέσει την απενθυλάκωση, και έτσι οι μηχανισμοί αυτοί εντάσσονται στην κατηγόρια των automatic tunnelling.

Στην δεύτερη κατηγορία ανήκουν οι περιπτώσεις:

Host to host IPv4/IPv6 hosts που κάνουν tunneling IPv6 πακέτωνπρος ένα ενδιάμεσο IPv4/IPv6 router, στον οποίο έχουν πρόσβαση μέσω μιας IPv4 δομής. Σ' αυτήν την περίπτωση το tunnel αντιστοιχεί στο αρχικό τμήμα της και router to host όπου το πακέτο μεταδίδεται μέσω του τούνελ μέχρι τον τελικό προορισμό. Σε αυτή την περίπτωση, η διεύθυνση σς του IPv6 πακέτου περιέχει με κάποιο τρόπο την IPv4 διεύθυνση προορισμού που θα χρησιμοποιηθεί στην εξωτερική IPv4 επικεφαλίδα, έτσι δεν χρειάζεται να έχει καθοριστεί εκ των πρότερων το άλλο άκρο του τούνελ, απλοποιώντας σημαντικά την διαδικασία υλοποίησης του τούνελ.

Στις δύο παραπάνω περιπτώσεις που αναφέρθηκαν παραπάνω (router-to router και host-to-router), το τέλος του tunnel είναι ένας router, ο οποίος είναι μενενδιάμεσος κόμβος και όχι ο τελικός προορισμός της μεταδιδόμενης πληροφορίας. Η λειτουργία αυτού του κόμβου είναι απλώς να απενθυλακώσει τα IPv6 πακέτα και να τα προωθήσει προς τον τελικό προορισμό τους. Έτσι η IPv6 διεύθυνση των πακέτων που ενθυλακώνονται, δεν

μπορεί να παρέχει καμιά πληροφορία σχετικά με την IPv4 διεύθυνση του τέλους του tunnel και συνεπώς αυτή η πληροφορία πρέπει να γίνει

διαθέσιμη μέσω configuration. Τα tunnels που χρειάζονται απευθείας χειρωνακτικό

ορισμό της διεύθυνσης τέλους τους ονομάζονται configured tunnels.

3.4.2 Λειτουργία των μηχανισμών tunneling :

Προκειμένου να λειτουργήσει ο μηχανισμός αυτός, πρέπει οι IPv4 διευθύνσεις των σταθμών να είναι globally routable, δηλαδή αποκλείονται private διευθύνσεις.Συνήθως η τεχνική των αυτόματων tunnels χρησιμοποιείται σε συνδυασμό με κάποιο configured tunnel, προκειμένου ο IPv6 σταθμός να είναι ικανός να επικοινωνήσει με το σύνολο των IPv6 σταθμών (δηλαδή των native IPv6 σταθμών και των σταθμών που χρησιμοποιούν 6to4 τεχνική) και όχι μόνο με όσους χρησιμοποιούν automatic tunneling.

Έτσι οι σταθμοί χρησιμοποιώντας automatic tunnels, επικοινωνούν με ανάλογους σταθμούς. Επίσης με την χρήση κάποιου configured tunnel, προωθούν πακέτα που έχουν σαν IPv6 διεύθυνση προορισμού κάποια, που ανήκει στο σύνολο των native διευθύνσεων, προς ένα router, ο οποίος έχει σε κάποιο από τα interfaces του IPv4- compatible IPv6 διεύθυνση. Επισημαίνεται πως configured tunnel ονομάζεται εκείνο, που η IP του άλλου endpoint παρέχεται από configuration πληροφορία και μπορεί να χρησιμοποιεί οποιουδήποτε τύπου IPv6 διευθύνσεις, native, IPv4-compatible.

Τα κύρια χαρακτηριστικά λειτουργίας των μηχανισμών είναι ίδια και για τις δυο κατηγορίες tunnels :

- Ο κόμβος εισόδου (ο κόμβος στον οποίο θα γίνει η ενθυλάκωση) δημιουργεί την IPv4 επικεφαλίδα με τιμή 41 στο πεδίο protocol, κάτω από την οποία ενθυλακώνει το IPv6 πακέτο, και ακολούθως δρομολογεί το πακέτο με κανονική IPv4 δρομολόγηση, θέτοντας ως διεύθυνση προορισμού την IPv4 διεύθυνση του κόμβου εξόδου, όπου θα γίνει η απενθυλάκωση.
- Στο άλλο άκρο του τούνελ, ο κόμβος εξόδου (ο κόμβος στον οποίο θα γίνει η απενθυλάκωση), παραλαμβάνει το ενθυλακωμένο πακέτο, το επανασυναρμολογεί αν προέκυψε κατατεμαχισμός του, και αφού δει την τιμή 41 στο πεδίο protocol αφαιρεί την IPv4 επικεφαλίδα. Ακολούθως, αν η διεύθυνση προορισμού του IPv6 πακέτου είναι διαφορετική από την δική του, προωθεί το πακέτο στον προορισμό με κανονική IPv6 δρομολόγηση. Πρέπει να σημειωθεί ότι κατά την φάση της απενθυλάκωσης δεν μεταβάλλεται η IPv6 επικεφαλίδα και απλώς μειώνεται το hop limit κατά ένα σε περίπτωση περαιτέρω προώθησης του πακέτου.
- Ίσως ο κόμβος εισόδου χρειάζεται να κρατά πληροφορίες για κάποιες παραμέτρους όπως το MTU (Maximum Transfer Unit - το μέγεθος του μεγαλύτερου IPv6 πακέτου που μπορεί να δρομολογηθεί) και το Hop Limit (το αντίστοιχο του TTL στο IPv4 πρωτόκολλο - ο αριθμός των ενδιάμεσων κόμβων από όπου θα περάσει το πακέτο μέχρι να απορριφθεί αν δεν έχει φτάσει στον προορισμό του), ούτως ώστε να προωθήσει τα IPv6 πακέτα μέσα στο tunnel.

3.4.3 Maximum Transfer Unit (MTU) του tunnel και Κατατεμαχισμός των πακέτων

Αν και όχι καταστροφικός, ο κατατεμαχισμός των IPv6 πακέτων για την μετάδοση τους μέσω του τούνελ είναι ανεπιθύμητος. Ο κατατεμαχισμός αυτός μπορεί να μειωθεί στο ελάχιστο έχοντας τον κόμβο εισόδου να ανιχνεύει το IPv4 Path MTU κατά μήκος του tunnel, χρησιμοποιώντας το IPv4 Path MTU Discovery Protocol (RFC 2185) και να

καταγράφει το path MTU το οποίο έχει υπολογίσει. Έτσι, το IPv6 στρώμα(network layer) βλέπει το τούνελ σαν να πρόκειται για στρώμα ζεύξης (link layer), με MTU ίσο με το IPv4 MTU path που έχει καταγράψει μείον το μέγεθος της IPv4 επικεφαλίδας (20 bytes).

Όμως υπάρχει και η περίπτωση που ο κατατεμαχισμός των IPv6 πακέτων είναι αναπόφευκτος. Αυτό συμβαίνει στην περίπτωση που το IPv4 path MTU υπολογίζει MTU μικρότερο από 1280 bytes, όπου 1280 είναι το μικρότερο μέγεθος που μπορεί να έχει ένα IPv6 πακέτο. Σε αυτή την περίπτωση, το στρώμα IPv6 (network layer) πρέπει να 'δει' ένα στρώμα ζεύξης (link layer) με MTU 1280 bytes και ο κόμβος εισόδου να χρησιμοποιήσει IPv4 κατατεμαχισμό, κατά την προώθηση των πακέτων. Σε αυτή την περίπτωση, το Don't Fragment bit δεν πρέπει να τίθεται στην IPv4 επικεφαλίδα.

Στην περίπτωση όμως που οι κομβόι εισόδου έχουν να υλοποιήσουν μεγάλο αριθμό tunnels, αποφεύγεται ο υπολογισμός του IPv4 Path MTU, και αντί αυτού χρησιμοποιείται η τιμή του MTU του στρώματος ζεύξης(link layer) που είναι κάτω από το στρώμα δικτύου. Και σε αυτή την περίπτωση μπορεί το MTU του στρώματος ζεύξης να είναι μικρότερο από 1280, και όπως και πριν, το MTU για το tunnel πρέπει να τεθεί σε 1280 και το Don't Fragment bit στην τιμή 0 (να επιτρέπεται δηλαδή ο τεμαχισμός)

3.4.4 Hop Limit

Τα IPv6-πανω από-IPv4 tunnels ανήκουν στην κατηγορία "single-hop", δηλαδή το IPv6 hop limit μειώνεται κατά ένα όταν τα IPv6 πακέτα διασχίζουν το τούνελ. Με αυτό τον τρόπο κρύβεται η παρουσία του τούνελ και η ύπαρξη του είναι άγνωστη για τον χρηστή του δικτύου που δεν μπορεί να τα εντοπίσει με διαγνωστικά εργαλεία όπως το traceroute.

Για την υλοποίηση του single hop μοντέλου, οι δυο κόμβοι στα άκρα του tunnel, μεταχειρίζονται το πεδίο IPv6 hop limit όπως στην περίπτωση προώθησης ενός πακέτου σε ένα άλλο κόμβο, δηλαδή μειώνοντας το hop limit κατά 1 όταν προωθούν ένα IPv6 πακέτο, σαν να μην υπήρχαν οι ενδιάμεσοι IPv4 κομβόι (ο κόμβος προορισμού δεν μειώνει το hop limit).

Ο κύριος λόγος ύπαρξης του TTL είναι για να διασφαλίσει ότι κάποιο πακέτο δεν θα περιφέρεται συνεχώς από κόμβο σε κόμβο επειδή ο παραλήπτης του δεν μπορεί να βρεθεί. Εάν δεν υπήρχε, τότε οι κόμβοι του δικτύου θα γέμιζαν από τέτοια πακέτα με αποτέλεσμα το δίκτυο να σταματήσει την σωστή λειτουργία του και να παγώσει.

Όσον αφορά το πεδίο TTL της εξωτερικής IPv4 επικεφαλίδας που χρησιμοποιείται για την ενθυλάκωση, επαφίεται στον εκάστοτε διαχειριστή να το θέσει στην τιμή μου επιθυμεί.

Θεωρητικά, το πεδίο TTL περιέχει το χρονικό διάστημα σε δευτερόλεπτα μέσα στο οποίο θα πρέπει το πακέτο να έχει παραδοθεί. Πρακτικά όμως, κάθε κόμβος του δικτύου στον οποίο φτάνει το πακέτο, μειώνει την τιμή του πεδίου κατά μία μονάδα. Άρα λοιπόν πρακτικά το πεδίο αυτό περιέχει τον μέγιστο αριθμό κόμβων από τους οποίους πρέπει να περάσει το πακέτο έως ότου τελικά παραδοθεί στον παραλήπτη. Στο νέο πρωτόκολλο IPv6, το πεδίο αυτό ονομάζεται hop limit αντί για Time to live.

Σε ένα σενάριο IPv4, το πεδίο TTL δίνει τον αριθμό των hops που καλύπτονται. Αυτός ο αριθμός hops διακόπτεται από μια αίτηση Ping.

Παρακάτω είναι μια απάντηση δείγματος που λαμβάνεται από ένα αίτημα ping στο www.google.com

Reply from 216.239.61.104: bytes=32 time=66ms TTL=240 Απάντηση από 216.239.61.104: bytes = 32 χρόνος = 66ms TTL = 240

Κάθε φορά που ένας δρομολογητής διασχίζεται ,η αξία του αριθμού TTL γενικά μειώνεται κατά 1.. Σε αυτό το σενάριο, η τιμή εκκίνησης του router θα ήταν 256.

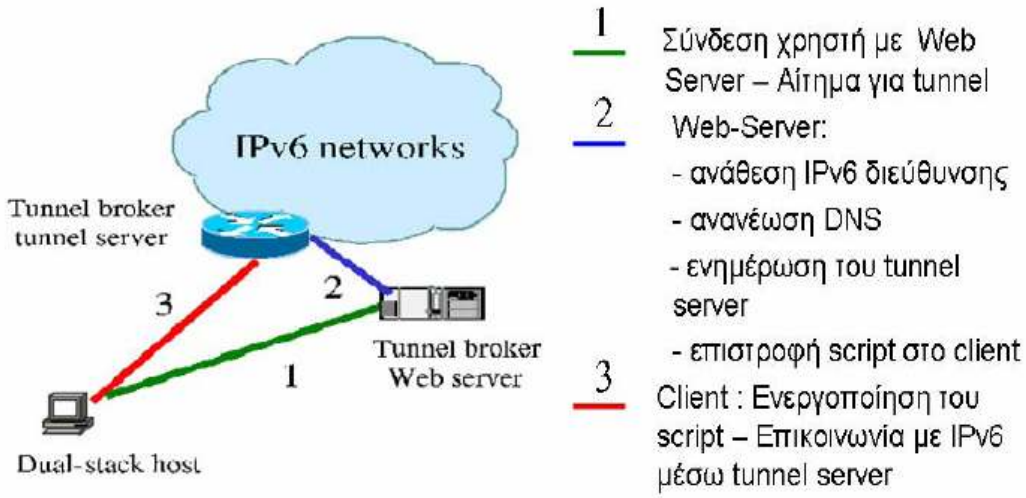
3.5. Μηχανισμοί Automatic tunneling

Στην συνέχεια περιγράφονται συνοπτικά οι σημαντικότεροι μηχανισμοί automatic tunneling που έχουν χρησιμοποιηθεί και χρησιμοποιούνται μέχρι σήμερα. Στους μηχανισμούς αυτούς περιλαμβάνεται και ο 6to4 , ο οποίος θα περιγράφει εκτενέστερα σε επόμενες ενότητες. Οι υπόλοιποι μηχανισμοί δίνονται πιο κάτω

3.5.1Tunnel Broker

Ο συγκεκριμένος μηχανισμός παρέχει τον απλούστερο τρόπο σε ένα dual-stack host που βρίσκεται σε IPv4 δίκτυο να επικοινωνήσει με IPv6 κόμβους. Ο χρηστής που επιθυμεί IPv6 σύνδεση, συνδέεται σε ένα Web Server και αιτείται IPv6 σύνδεση. Κατόπιν, ο Web Server του αναθέτει μια IPv6 διεύθυνση, ανανεώνει αυτόματα το DNS, ενημερώνει τον Tunnel Broker Tunnel Server, μέσω του οποίου θα γίνει η σύνδεση και τέλος αποστέλλει ένα script στον χρηστή. Όταν ο χρήστης το τρέξει εγκαθίσταται ένα IPv6-over-IPv4 tunnel με τον broker server και η επικοινωνία με το IPv6 host γίνεται μέσω του broker server.

Ο tunnel broker μηχανισμός ,όπως αναφέρθηκε, είναι ο απλούστερος τρόπος για τους απλούς dial-up χρηστές να ενωθούν στο IPv6 δίκτυο και σήμερα προσφέρεται δωρεάν στις περισσότερες περιπτώσεις. Παρόλα αυτά υπάρχουν ακόμη κάποια προβλήματα όσον αφορά την ανακατανομή των δυναμικών IPv4 διευθύνσεων καθώς και κάποια ζητήματα ασφαλείας. Επίσης, ένα άλλο πρόβλημα που συχνά παρουσιάζεται είναι ότι οι διαχειριστές δεν γνωρίζουν για την ύπαρξη των μηχανισμών και τα περισσότερα firewalls αποκόπτουν τα πακέτα με τιμή του πεδίου protocol

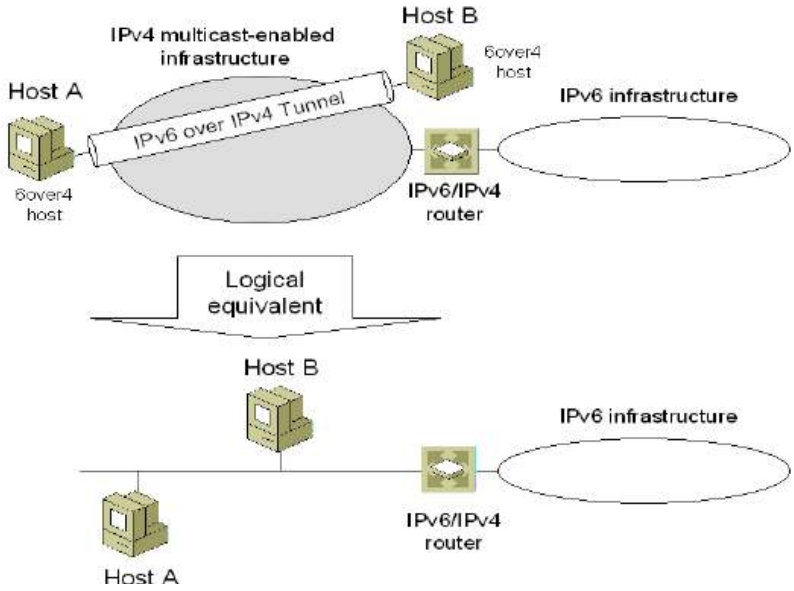


Σχήμα 18: Μηχανισμός Tunnel Broker

3.5.2 6over4 (ή αλλιώς multicast tunnelling)

Ο μηχανισμός αυτός επιτρέπει την επικοινωνία αποκομμένων IPv6 host (6over4) που βρίσκονται σε ένα IPv4 domain που υποστηρίζει IPv4 multicast να επικοινωνούν μέσω αυτόματων τούνελ . Οι ίδιοι οι hosts σε αυτή την περίπτωση ενθυλακώνουν τα πακέτα και επικοινωνούν μεταξύ τους μέσω τούνελ μέσα στο IPv4 δίκτυο ή στέλνουν τα πακέτα σε ένα δρομολογητή με IPv6 σύνδεση που καταλαβαίνει 6over4 (συνήθως ένα 6to4 router) για επικοινωνία με native IPv6 hosts ή άλλους 6over4 που ανήκουν σε άλλο δίκτυο.

Ο μηχανισμός αυτός είναι γνωστός και ως multicast tunnelling, αφού χρησιμοποιεί την IPv4 υποδομή σαν να επρόκειτο για ένα τμήμα φυσικής ζεύξης, δηλαδή ένα LAN (Local Area Network), όπως φαίνεται στο πιο κάτω σχήμα.



Σχήμα19: Μηχανισμός 6over4

Οι κομβόι στους οποίους έχει εγκατασταθεί 6over4 κάνουν αυτόματα μόνοι τους configure την link-local διεύθυνση του FE80::*WWXX*:*YYZZ* (όπου ww.xx.yy.zz η IPv4 διεύθυνση του – παγκόσμια ή ιδιωτική) και χρησιμοποιούν τις διεργασίες του Neighbour Discovery (address resolution και router discovery) όπως γίνεται σε μια φυσική ζεύξη με δυνατότητες multicast . Συγκεκριμένα, ο μηχανισμός παρέχει ένα σύνολο συσχετισμών των IPv4 multicast διευθύνσεων με τις αντίστοιχες IPv6, έτσι ώστε να επιτευχθούν οι λειτουργίες του IPv6 multicast πάνω από το IPv4 multicast, και οι 6over4 κομβόι στο IPv4 δίκτυο να επικοινωνούν μέσω των link-local διευθύνσεων τους.

Ο συγκεκριμένος μηχανισμός δεν χρησιμοποιήθηκε σε μεγάλο βαθμό λόγω ακριβώς της απαίτησης του για IPv4 multicast, κάτι που οι περισσότεροι παρόχοι ISP και οι κομβόι στους οποίους έχει εγκατασταθεί 6over4 κάνουν αυτόματα μόνοι τους configure την link-local διεύθυνση του FE80::*WWXX*:*YYZZ* (όπου ww.xx.yy.zz η IPv4 διεύθυνση του – παγκόσμια ή ιδιωτική) και χρησιμοποιούν τις διεργασίες του Neighbour Discovery (address resolution και router discovery) όπως γίνεται σε μια φυσική ζεύξη με δυνατότητες multicast . Συγκεκριμένα, ο μηχανισμός παρέχει ένα σύνολο συσχετισμών των IPv4 multicast διευθύνσεων με τις αντίστοιχες IPv6, έτσι ώστε να επιτευχθούν οι λειτουργίες του IPv6 multicast πάνω από το IPv4 multicast, και οι 6over4 κομβόι στο IPv4 δίκτυο να επικοινωνούν μέσω των link-local διευθύνσεων τους.

3.5.3 ISATAP

Το ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) είναι η εναλλακτική λύση στο πρόβλημα του 6over4, αφού και πάλι χρησιμοποιεί την IPv4 υποδομή σαν ένα ιδεατό

link χωρίς όμως να απαιτείται IPv4 multicast. Επιπλέον, και σε αυτή την περίπτωση ο μηχανισμός δουλεύει και κάτω από NAT (Network Address Translation).

Χρησιμοποιώντας το link-local πρόθεμα fe80::/64 και τον interface identifier 0μ:5EFE:w.x.y.z (οπου w.x.y.z η IPv4 διεύθυνση του interface – παγκόσμια ή ιδιωτική) σχηματίζεται η link-local διεύθυνση για επικοινωνία με τον ISATAP router. Μόλις αρχικοποιηθεί ένας ISATAP κόμβος ψάχνει μέσω DNS για το όνομα “ISATAP” λαμβάνοντας έτσι τις διευθύνσεις όλων των ISATAP routers και φτιάχνει την Potential Router List (PRL). Ακολούθως, ο κόμβος στελνει μήνυμα Router Solicitation για να λάβει το πρόθεμα από τον router και να φτιάξει την παγκόσμια IPv6 ISATAP διεύθυνση του.

Έτσι, ο router στέλνει μήνυμα router-advertisement στον κόμβο, όπου μέσα περιέχεται το site-prefix έτσι ώστε ο κόμβος να φτιάξει την δική του παγκόσμια μοναδική διεύθυνση. Στην περίπτωση επικοινωνίας μέσα στο ίδιο site, ενθυλακώνονται τα πακέτα από τον ISATAP κόμβο και χρησιμοποιείται σαν IPv4 διεύθυνση προορισμού η διεύθυνση που προκύπτει από τον Interface Identifier της διεύθυνσης προορισμού (τα τελευταία 4 bytes). Στην περίπτωση που η επικοινωνία είναι με ISATAP ή native IPv6 κόμβο αλλού site, τα πακέτα ενθυλακώνονται και στέλνονται στον ISATAP router (που και σε αυτή την περίπτωση είναι συνήθως ένας 6to4 router).

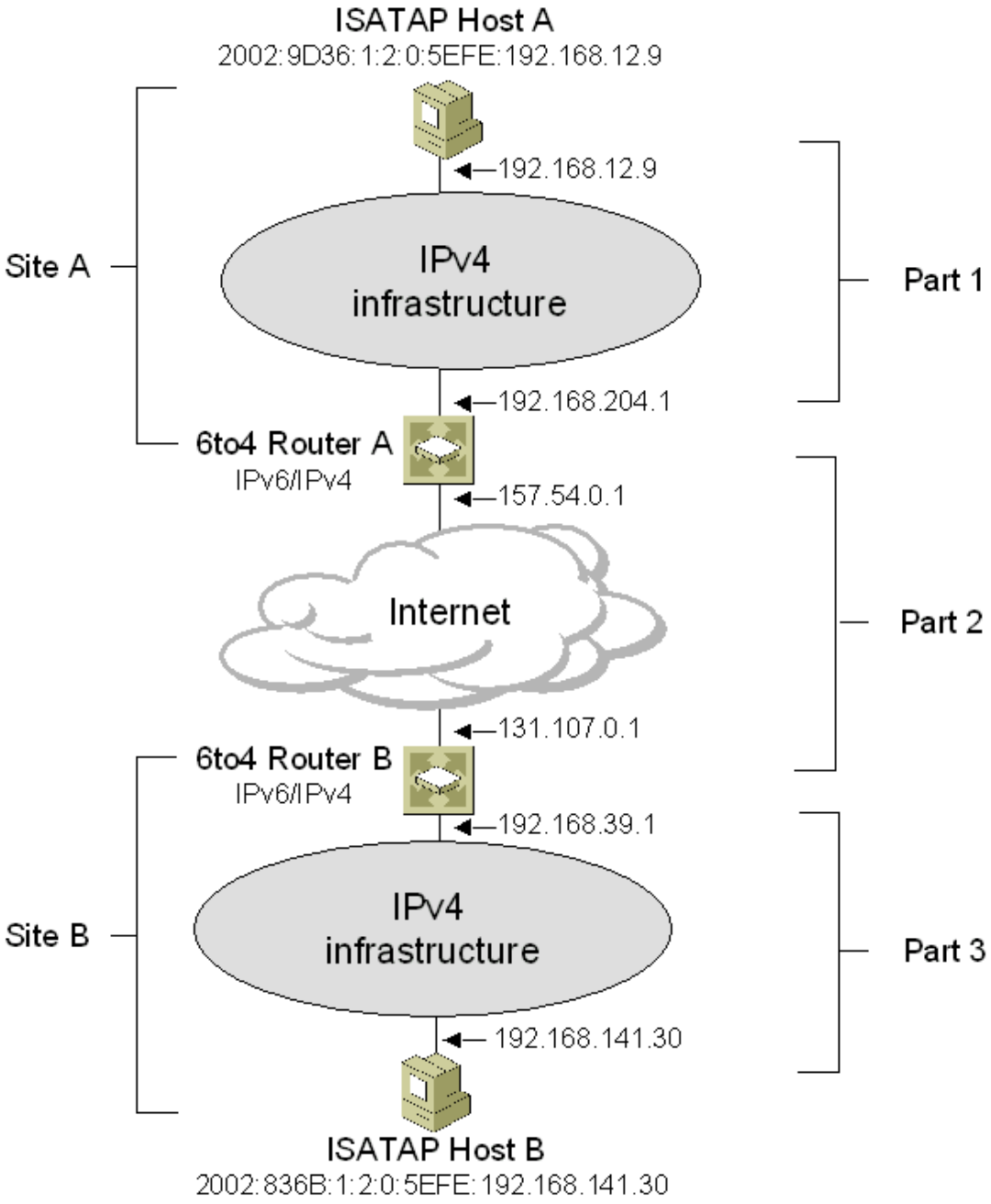
Ο μηχανισμός αυτός παρέχει εύκολη υλοποίηση του IPv6 σε διασκορπισμένους κόμβους μέσα σε IPv4 domain και υποστηρίζεται στα περισσότερα λειτουργικά συστήματα. Επιπλέον δουλεύει και κάτω από NAT.

Όσον αφορά την ασφάλεια, υπαρχουν και σε αυτή την περίπτωση κάποια κενά κυρίως ως προς τους ISATAP routers. Γενικά όμως, το μοντέλο αυτό υπερτερεί των υπόλοιπων μηχανισμού αυτομάτου tunneling, τόσο στο ότι παρέχει IPv4 ingress filtering και ip-protocol-41 filtering στους συνοριακούς δρομολογητές του site όσο και στο γεγονός ότι πιο δύσκολα ένας κακόβουλος κόμβος θα ‘υποδυθεί’ τον ISATAP router, αφού ο τελευταίος δέχεται πακέτα μόνο από τους δρομολογητές που είναι καταγραμμένοι στην Potential Router List (PRL).

Τα μειονεκτήματα του μηχανισμού είναι η δυσκολότερη υλοποίηση του από τους άλλους μηχανισμούς, το γεγονός ότι ακόμα δεν έχει γίνει standard αν και στην πραγματικότητα όμως χρησιμοποιείται ήδη στις περισσοτερες πλατφόρμες .

Συνήθως, ο ISATAP μηχανισμός συνδυάζεται με το 6to4, κυρίως σε περιπτώσεις που η υλοποίηση γίνεται κάτω από NAT. Έτσι, εσωτερικά στο site χρησιμοποιείται ο ISATAP, και η σύνδεση με το IPv6 γίνεται μέσω του 6to4 router, ο οποίος διαφημίζει εσωτερικά το 6to4 πρόθεμα 2002::V4ADDR::/64 έτσι ώστε να σχηματιστούν οι global διευθύνσεις(2002:V4ADDR:1:5EFE:x.y.z.w οπου x.y.z.w η ιδιωτικη ή παγκοσμια IPv4 διεύθυνση του host) για επικοινωνία εκτός του site. Το σενάριο αυτό δίνεται στο πιο κάτω σχήμα:

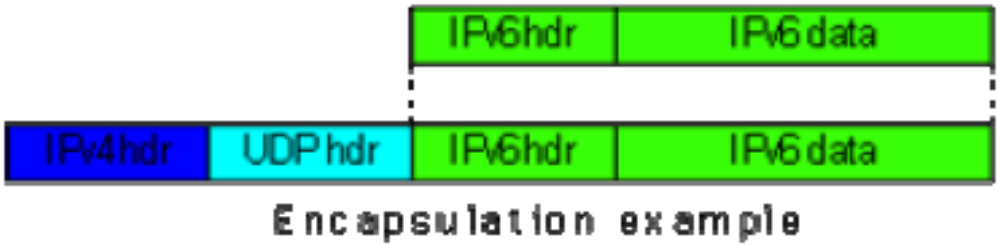
.



Σχήμα 20:ISATAP

3.5.4 Teredo

Επιτρέπει σε host που βρίσκονται πίσω από ένα ή περισσότερα επίπεδα NAT να επικοινωνούν μέσω τούνελ με IPv6 κόμβους. Η ενθυλάκωση των πακέτων γίνεται σε IPv4 UDP πακέτα τα οποία προωθούνται στο teredo relay- που είναι συνδεδεμένος με το IPv6 δίκτυο, για απενθυλάκωση- στην περίπτωση που η επικοινωνία είναι με native IPv6.



Σχήμα 21: Μηχανισμός Teredo. Ενθυλάκωση σε IPv4 UDP πακέτο

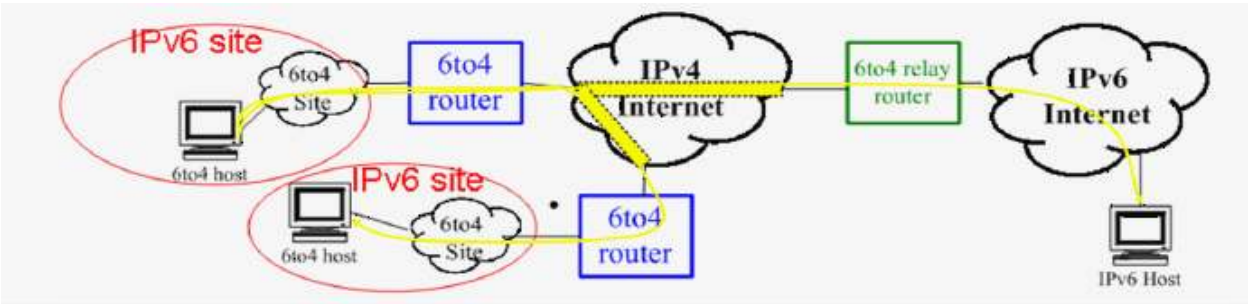
Στο σημείο αυτό έγκειται και η διάφορα του Teredo από τον 6to4, στο ότι δηλαδή η ενθυλάκωση γίνεται από τον κόμβο, και όχι στον συνοριακό δρομολογητή. Επίσης, λόγω του ότι τα περισσότερα NATs δεν επιτρέπουν πακέτα protocol 41 να διαπεράσουν το NAT, η ενθυλάκωση γίνεται σε IPv4 UDP πακέτα (δηλαδή στο πεδίο.Στο σημείο αυτό έγκειται και η διάφορα του Teredo από τον 6to4, στο ότι δηλαδή η ενθυλάκωση γίνεται από τον κόμβο, και όχι στον συνοριακό δρομολογητή. Επίσης, λόγω του ότι τα περισσότερα NATs δεν επιτρέπουν πακέτα protocol 41 να διαπεράσουν το NAT, η ενθυλάκωση γίνεται σε IPv4 UDP πακέτα (δηλαδή στο πεδίο protocol τίθεται η τιμή του πρωτοκόλλου UDP) , όπου τα UDP συνήθως περνάνε από τα διάφορα επίπεδα NAT.

Ο μηχανισμός αυτός αποτελεί την τελευταία λύση όταν δεν υπάρχει δυνατότητα υλοποίησης των υπόλοιπων μηχανισμών. Η υλοποίηση του είναι περίπλοκη και μπορεί να λειτουργήσει μόνο κάτω από συγκεκριμένα είδη NAT, η διαχείριση του δύσκολη και σήμερα δεν υπάρχουν ακόμη αρκετοί teredo relays για σύνδεση με native IPv6 hosts.

3.6 Μηχανισμός 6to4

Το 6to4 είναι ένας μηχανισμός αυτόματου tunneling που παρέχει την δυνατότητα σε απομονωμένα IPv6 sites, στα οποία δεν υπάρχει ευρύτερη IPv6 συνδεσιμότητα και υπηρεσίες από κάποιο πάροχο ISP, να επικοινωνούν μεταξύ τους πάνω από το ήδη υπάρχον IPv4 δίκτυο. Επιπλέον δίνεται η δυνατότητα να επικοινωνούν με sites που ανήκουν στο native IPv6 δίκτυο μέσω relay router. Ο μηχανισμός αυτός σχεδιάστηκε για το μεταβατικό στάδιο από τις IPv4 στις IPv6 διευθύνσεις ,κατά την περίοδο δηλαδή που οι δυο διευθύνσεις θα συνυπάρχουν. Σκοπός του μηχανισμού είναι απομονωμένες νησίδες IPv6 που έχουν πρόσβαση στο IPv4 wide area network , το οποίο δεν υποστηρίζει IPv6, να επικοινωνούν μεταξύ τους με εύκολο και αυτόματο τρόπο.

Με τον 6to4 μηχανισμό κάθε site που έχει μια **παγκόσμια μοναδική unicast IPv4 διεύθυνση** μπορεί χρησιμοποιώντας ενθυλάκωση με automatic tunneling να μεταδώσει πακέτα πάνω από το παγκόσμιο IPv4 δίκτυο χρησιμοποιώντας ένα μοναδικό πρόθεμα (prefix) 2002::/16. Εκτός από τον 6to4 router, οι υπόλοιποι τοπικοί hosts και routers κάτω από αυτόν δεν χρειάζεται να υλοποιούν τον 6to4 μηχανισμό και οι διάφορες λειτουργίες του εσωτερικού δικτύου γίνονται όπως ορίζει το IPv6 πρωτόκολλο.



Σχήμα 22:Μηχανισμός 6over4

Ο 6to4 μηχανισμός, επικράτησε των υπόλοιπων μηχανισμών μετάβασης και αντικατέστησε γρήγορα τα configured tunnels που αρχικά χρησιμοποιούνταν, τόσο λόγω της ευκολίας υλοποίησης του αλλά και των ελάχιστων απαιτήσεων , οι οποίες είναι:

- Ο συνοριακός δρομολογητής του site, ο οποίος είναι ο μόνος που υλοποιεί τον 6to4 μηχανισμό, πρέπει να είναι dual-stack.
- Το site πρέπει να διαθέτει μια παγκόσμια unicast IPv4 διεύθυνση για την επικοινωνία πάνω από την IPv4 υποδομή.
- Ένας 'διαθέσιμος' relay router, για την περίπτωση επικοινωνίας του 6to4 site με το native IPv6 δίκτυο. (δηλαδή με διευθύνσεις προορισμού με παγκόσμιο unicast TLA 2001 ή 3ffe)

Έτσι, απλά υλοποιώντας τον 6to4 μηχανισμό στον συνοριακό δρομολογητή του 6to4 site, το οποίο είναι στην ουσία ένα κανονικό IPv6 site, προσφέρεται σε όλους τους hosts IPv6 συνδεσιμότητα, χωρίς οι ίδιοι να υλοποιούν 6to4, και χωρίς να χρειάζεταινα κάνουν κάποια ειδική διαδικασία, εκτός του ότι καθορίζουν στο default route τους, next hop τη διεύθυνση του 6to4 router. Επιπλέον, ο 6to4 μηχανισμός δεν επιβαρύνει με επιπρόσθετες έγγραφες τους IPv4 πίνακες δρομολόγησης και δεν απαιτεί κάποιο εξωτερικό IPv6 πρωτόκολλο δρομολόγησης αφού το αντίστοιχο IPv4 εκτελεί την απαιτούμενη διαδικασία δρομολόγησης.

Πιο κάτω δίνεται η ορολογία σε 6 to 4 μηχανισμό

6to4 pseudo-interface: Αντιστοιχεί σε ένα IPv6 interface και είναι το σημείο στο οποίο γίνεται η ενθυλάκωση του IPv6 πακέτου στο IPv4. Το 6to4 pseudo-interface είναι το end-point του τούνελ.

6to4 prefix: Το IPv6 πρόθεμα που φτιάχνεται όπως περιγράφεται στην επόμενη ενότητα.

6to4 address: Η 6to4 διεύθυνση που κατασκευάζεται βάσει του 6to4 προθέματος.

Native IPv6 address:IPv6 διεύθυνση που κατασκευάζεται χρησιμοποιώντας διαφορετικό πρόθεμα από το 6to4 prefix.

6to4 router :Ένας IPv6 router(δρομολογητής) ο οποίος υποστηρίζει το IPv6 pseudo-interface. Είναι ο συνοριακός δρομολογητής μεταξύ του IPv6 site και του wide-area IPv4 network. Δρομολογεί το διακινούμενο φορτίο μεταξύ των 6to4 hosts μέσα στο ίδιο το site και μεταξύ άλλων 6to4 routers και relay routers πάνω από ένα IPv4 inter-network όπως το Internet. Ο 6to4 router χρειάζεται επιπλέον manual configuration για το 6to4 pseudo-interface όπου θα γίνεται η ενθυλάκωση και η απενθυλάκωση των IPv6 πακέτων.

6to4 host: Ένας IPv6 host που έχει τουλάχιστον μια 6to4 διεύθυνση. Κατά τα αλλά είναι ένας κανονικός IPv6 host.Οι 6to4 hosts δεν χρειάζονται καθόλου manual configuration και δημιουργούν από μόνοι τους τις 6to4 διευθύνσεις τους χρησιμοποιώντας τους standard μηχανισμούς address autoconfiguration.

6to4 site: Ένα site που εσωτερικά χρησιμοποιεί το IPv6 πρωτόκολλο και περιέχει τουλάχιστον ένα 6to4 host και τουλάχιστον ένα 6to4 router.

Relay router: Ένας 6to4 router ο οποίος έχει συντονισθεί έτσι ώστε να υποστηρίζει δρομολόγηση μεταξύ 6to4 διευθύνσεων και native IPv6 διευθύνσεων. Ουσιαστικά είναι ένας κανονικός IPv6 router με τουλάχιστον ένα 6to4 pseudo-interface και τουλάχιστον ένα IPv6 interface.

IPv4-only node: Ένας κόμβος που υλοποιεί μόνο IPv4 και έχει μόνο IPv4 διεύθυνση. Ο κόμβος αυτός δεν υποστηρίζει IPv6.

IPv6-only node: Ένας κόμβος που υποστηρίζει μόνο IPv6 και μπορεί να επικοινωνήσει μόνο με IPv6 κόμβους και εφαρμογές.

IPv6/IPv4 node: Κόμβος που υλοποιεί τόσο IPv6 όσο και IPv4.

IPv4 node: Κόμβος που υλοποιεί IPv4 (στέλνει και λαμβάνει IPv4 πακέτα). Ο κόμβος αυτός μπορεί να είναι IPv4-only ή IPv6/IPv4 κόμβος.

IPv6 node : Κόμβος που υλοποιεί IPv6 (στέλνει και λαμβάνει IPv6 πακέτα). Ο κόμβος αυτός μπορεί να είναι IPv6-only ή IPv6/IPv4 κόμβος.

3.6.1 Διευθύνσεις 6to4

Προσδιορισμός του προθέματος 6to4:

Ο μηχανισμός 6to4 εφαρμόζεται σε ένα site που έχει τουλάχιστον μια παγκόσμια μοναδική IPv4 διεύθυνση(αναφέρεται ως V4ADDR από τώρα και στο εξής). Η IANA έχει ορίσει το unicast 6to4 πρόθεμα (TLA) **2002::/16** για αποκλειστική χρήση από τον 6to4 μηχανισμό. Το 6to4 πρόθεμα μαζί με την IPv4 διεύθυνση σχηματίζουν το /48 πρόθεμα του site (site prefix) 2002::V4ADDR/48, το οποίο είναι και αυτό μοναδικό λόγω του ότι προκύπτει από τη μοναδική V4ADDR. Πιο κάτω δίνεται ένα παράδειγμα του σχηματισμού του 6to4 προθέματος του site από την IPv4 διεύθυνση:

Το πρόθεμα που αυτό είναι ένα κανονικό IPv6 πρόθεμα, επιτρέποντας έτσι στο IPv6 domain (το 6to4 site στην περίπτωση μας) να το χρησιμοποιήσει όπως κάθε έγκυρο IPv6 πρόθεμα (αυτόματη ανάθεση διευθύνσεων και discovery καθώς και native IPv6 routing). Επιπλέον, με αυτό τον τρόπο σχηματίζονται αμέσως 2^{16} υποδίκτυα με 2^{64} κόμβους το καθένα, κάτω από μια και μοναδική IPv4 διεύθυνση, δίνοντας έτσι και ο ίδιος ο μηχανισμός μια λύση στο πρόβλημα της έλλειψης των IPv4 διευθύνσεων.

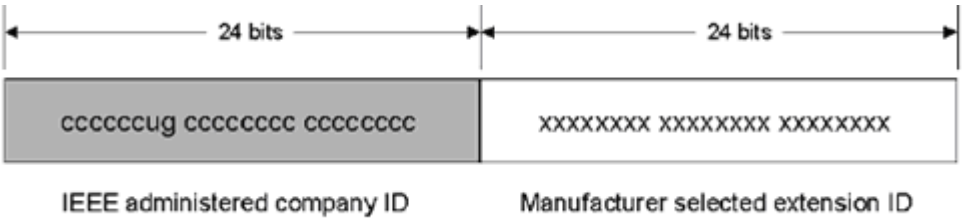
Αφότου καθοριστεί το 6to4 πρόθεμα του site /48, καθορίζονται τα διάφορα υποδίκτυα του site, παίρνοντας το καθένα μοναδική τιμή για το SLA ID, έτσι που τελικά σχηματίζεται το μοναδικό 2002:V4ADDR:SLA ID::/64 πρόθεμα του υποδικτύου (subnet prefix). Το πρόθεμα αυτό διαφημίζεται από τους 6to4 routers με μηνύματα Router Advertisements όπως ορίζει το Neighbor Discovery (ND) protocol έτσι ώστε οι hosts να σχηματίσουν από μόνοι τους την 6to4 παγκόσμια διεύθυνση τους με Stateless Address Autoconfiguration. Συγκεκριμένα, οι 6to4 hosts υπολογίζουν από μόνοι τους τα τελευταία 64 bit, τα οποία είναι ο μοναδικός για τον κάθε κόμβο interface identifier, και σε συνδυασμό με τα 64 bit του

προθέματος υποδικτύου που περιέχονται στις διαφημίσεις του 6to4 router, σχηματίζεται η παγκόσμια IPv6 (6to4) διεύθυνση τους (σχήμα πιο κάτω),με την οποία θα εγγράφουν στο DNS καθιστώντας έτσι δυνατή την ανάγνωση της από άλλους IPv6 κόμβους, δίνοντας τους έτσι την δυνατότητα επικοινωνίας τόσο με άλλους 6to4 κόμβους όσο και με native IPv6 κόμβους

Bits 0-16	17-48	49-64	65-128
2002	IPv4 Address	SLA ID	Interface ID (probably the EUI-64 ID)

Interface Identifier

Μέσα σε ένα site ο κάθε host έχει να σχηματίσει τα τελευταία 64-bit που είναι γνωστά σαν ο Interface Identifier, και είναι μοναδικά για τον κάθε κόμβο. Έχουν προταθεί και έχουν υλοποιηθεί διάφοροι τρόποι για τον προσδιορισμό του Interface ID. Στην συγκεκριμένη αναφορά περιγράφεται ο EUI-64, ο οποίος είναι ο πιο καθιερωμένος και χρησιμοποιείται σήμερα από τα περισσότερα συστήματα. Ο Extended Unique Identifier (EUI)-64 address-based interface identifier ορίστηκε από το Institute of Electrical and Electronic Engineers (IEEE) και χρησιμοποιεί για τον υπολογισμό του Interface ID την 48-bit μοναδική για κάθε κατασκευαστή διεύθυνση MAC, ορίζοντας έτσι μοναδικά τον Interface ID. Πιο κάτω φαίνονται τα 48-bit της MAC διεύθυνσης:

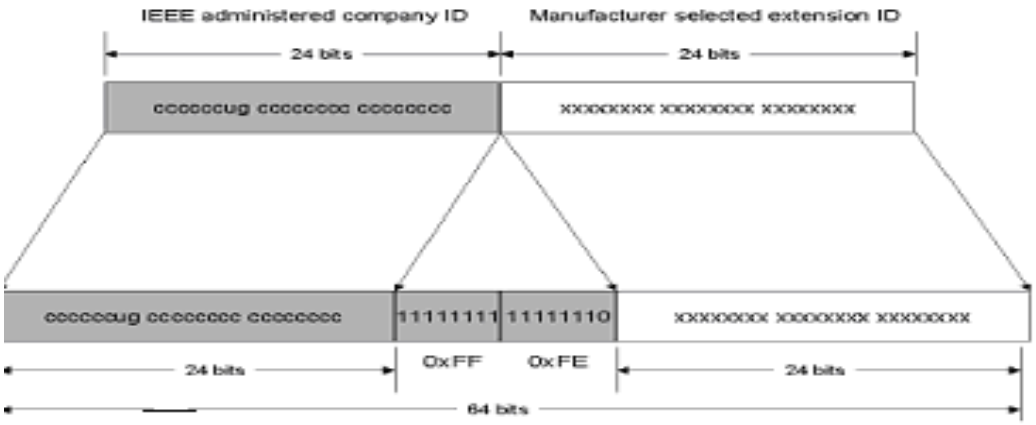


Σχήμα 22:Σχηματισμός interface –identifier

Όπου με το γράμμα u συμβολίζεται το Universal/Local (U/L) bit το οποίο είναι το διπλανό του low order bit του πρώτου byte.

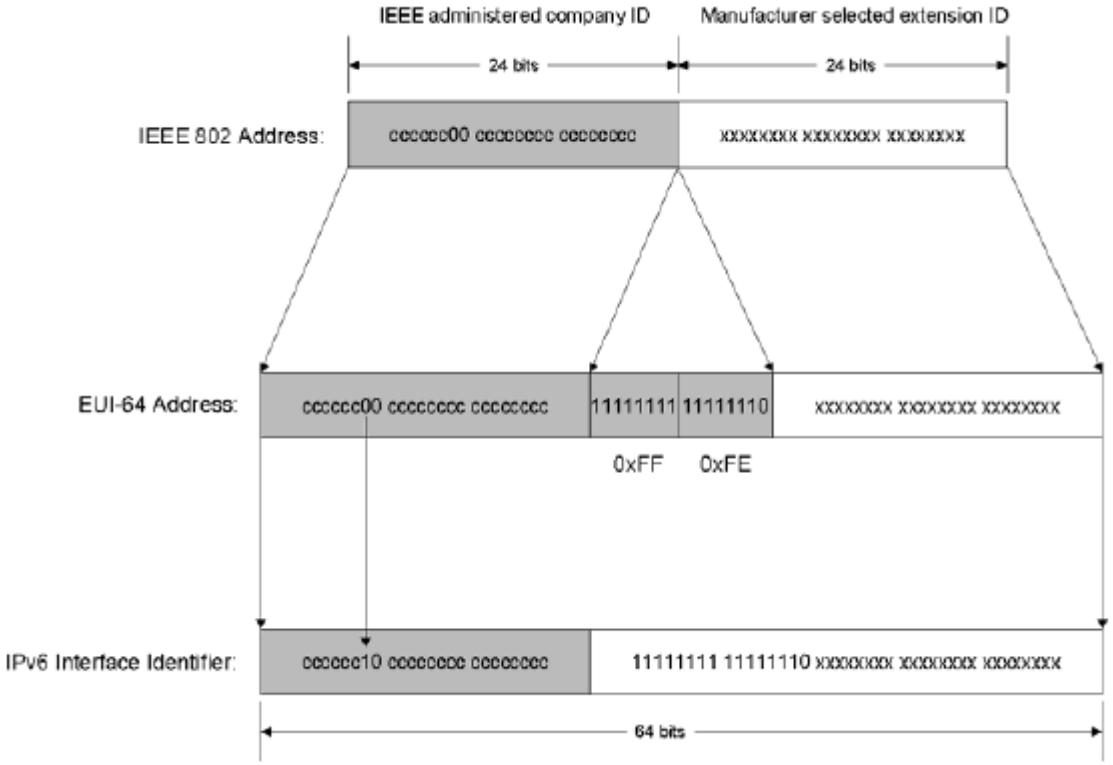
Η διαδικασία προσδιορισμού του EUI-64 έχει ως εξής:

Επειδή ο Interface ID έχει μήκος 64-bit και η MAC διεύθυνση 48-bit, 16 επιπλέον bits με τιμή 11111111 11111110 (0xFFFE) εισέρχονται στη MAC διεύθυνση μεταξύ του company ID και του extension ID, όπως φαίνεται στο πιο κάτω σχήμα:



Σχήμα 24:Σχηματισμός interfaceID

Και τέλος παίρνεται το συμπλήρωμα του U/L (αν είναι 1 τίθεται σε 0 και αν είναι 0 σε 1) σχηματίζοντας έτσι τον μοναδικό Interface ID. Ολόκληρη η διαδικασία φαίνεται στο πιο κάτω σχήμα:



Σχήμα 25:Σχηματισμός interface ID (3/3)

3.6.2 Επιλογή Διευθύνσεων

(RFC 3484)

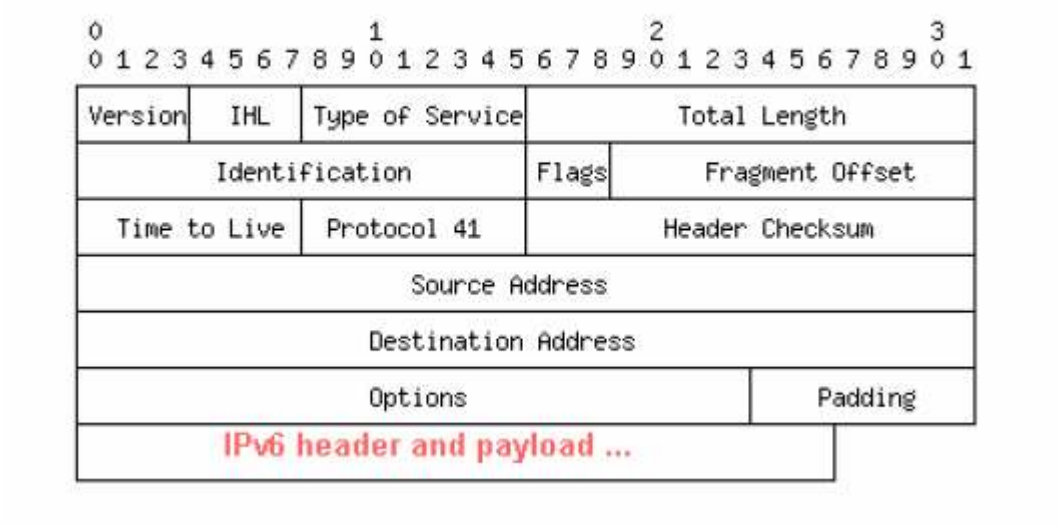
Για να διασφαλιστεί η σωστή λειτουργία του 6to4 μηχανισμού πρέπει να υλοποιηθεί κατάλληλα η επιλογή της διεύθυνσης πηγής και της διεύθυνσης προορισμού. Για αυτό έχουν προταθεί οι παρακάτω κανόνες που επιτρέπουν την σωστή λειτουργία του μηχανισμού:

- Αν ένας host έχει μόνο 6to4 διεύθυνση και ο άλλος έχει και 6to4 και native IPv6 διεύθυνση, τότε και οι δυο θα χρησιμοποιήσουν την 6to4 διεύθυνση.
- Αν και οι δυο έχουν και 6to4 διεύθυνση και native IPv6 διεύθυνση τότε η native IPv6 διεύθυνση θα χρησιμοποιηθεί και από τους δυο.

Ενθυλάκωση(Encapsulation) /Απενθυλάκωση (Decapsulation) των 6to4 πακέτων – Μηχανισμοί Tunneling:

Τα IPv6 πακέτα ενθυλακώνονται σε IPv4 πακέτα όταν φτάσουν στον 6to4 router στο σύνορο του 6to4 site, έτσι ώστε να μεταδοθούν πάνω στο ήδη υπάρχον IPv4 δίκτυο μεσώ τούνελ. Συγκεκριμένα, όσα IPv6 πακέτα φτάσουν στον 6to4 router με διεύθυνση προορισμού που δεν ανήκει στο συγκεκριμένο site, προωθούνται στο 6to4 interface για να μεταδοθούν μεσώ τούνελ είτε στον προορισμό κατευθείαν αν πρόκειται για κάποιον 6to4 host, είτε στον configured relay router αν προορίζονται για κάποιον native IPv6 host. Τα IPv6 πακέτα ταξιδεύουν μέσα στα IPv4 πακέτα με τιμή 41 στο πεδίο protocol της IPv4 επικεφαλίδας, έτσι ώστε ο δρομολογητής-παραλήπτης, να αντιλαμβάνεται ότι έχει γίνει ενθυλάκωση, και να ξεφλουδίζει τα πακέτα για να τα προωθεί στον τελικό προορισμό τους. Επιπλέον, στην IPv4 επικεφαλίδα περιέχονται οι IPv4 διευθύνσεις πηγής και προορισμού. Η μια (ή και οι δυο αν ο προορισμός είναι επίσης 6to4 κόμβος) είναι η V4ADDR που έχει οριστεί πιο πάνω, η μοναδική δηλαδή παγκόσμια IPv4 διεύθυνση του εκάστοτε 6to4 site. Στην άλλη περίπτωση (native IPv6 site) η διεύθυνση προορισμού στην εξωτερική IPv4 επικεφαλίδα είναι η IPv4 διεύθυνση του Relay Router που έχει καθοριστεί από τον διαχειριστή στον πίνακα δρομολόγησης του 6to4 router.

Συγκεκριμένα, αφού προωθηθούν τα πακέτα στο 6to4 interface, γράφεται στο πεδίο source address της IPv4 επικεφαλίδας η IPv4 διεύθυνση του site. Ακολούθως, αν τα πρώτα 16-bits της διεύθυνση προορισμού αντιστοιχούν στην στατική έγγραφη του routing table 2002::/16 (άρα πρόκειται για 6to4 διεύθυνση προορισμού) και το πρόθεμα /48 είναι διάφορο του τοπικού site, τότε αποσπάται η IPv4 (V4ADDR) διεύθυνση του 6to4 site και γράφεται στο πεδίο destination address της IPv4 επικεφαλίδας. Αν όμως ο η διεύθυνση προορισμού δεν αντιστοιχεί σε 6to4 διεύθυνση (δηλ. η διεύθυνση προορισμού δεν ταιριάζει στο πρόθεμα 2002::/16) αλλά σε άλλη IPv6 unicast διεύθυνση, τίθεται σαν διεύθυνση προορισμού στην IPv4 επικεφαλίδα η διεύθυνση του relay router που έχει καθοριστεί για το συγκεκριμένο route, κάποια συγκεκριμένη unicast IPv4 διεύθυνση του Relay Router ή εναλλακτικά η anycast διεύθυνση 192.88.99.0/24 (RFC 3068 - An Anycast Prefix for 6to4 Relay Routers) για τον πλησιέστερο Relay Router. Κατόπιν, αφού έχει γίνει η ενθυλάκωση προωθούνται μέσω τούνελ τα IPv4 πακέτα (που περιέχουν την επικεφαλίδα IPv6 και τα δεδομένα) με IPv4 δρομολόγηση πάνω από το IPv4 δίκτυο. Φαίνεται πιο κάτω το τελικό IPv4 πακέτο που μεταδίδεται:



Σχήμα 26: Το IPv4 πακέτο όπως μεταδίδεται μέσα από το tunnel

Τέλος, στην άλλη πλευρά του τούνελ ο 6to4 router του site στο οποίο ανήκει η διεύθυνση προορισμού, αν δει τιμή 41 στο πεδίο protocol της επικεφαλίδας, προωθεί τα πακέτα στο δικό του 6to4 interface, όπου αφού κάνει κάποιους έλεγχους ασφάλειας, ¨ξεφλουδίζει¨ με την ίδια διαδικασία την IPv4 επικεφαλίδα, βλέπει την 6to4 διεύθυνση προορισμού και με κανονική IPv6 δρομολόγηση στέλνει τα πακέτα στον προορισμό τους. Ομοίως, και ο Relay Router, αφού πάρει τα πακέτα μέσα από το τούνελ και διαπιστώσει ότι προέρχονται από 6to4 site, αφαιρεί την IPv4 επικεφαλίδα και προωθεί τα πακέτα με IPv6 δρομολόγηση μέσα στο native IPv6 site.

Κατά την ενθυλάκωση, τα 8-bits του πεδίου TimetoLive της IPv4 επικεφαλίδας τίθενται όπως τα 8-bits του πεδίου Hop Limit της επικεφαλίδας IPv6 (αφού ουσιαστικά δεν υπάρχει διάφορα στην υλοποίηση τους από τα upper-layer protocols που βασίζονται στο στρώμα δικτύου IP), εκτός αν οριστεί διαφορετικά από τον διαχειριστή του συστήματος.

Σημαντικό να αναφερθεί είναι το ότι ο 6to4 μηχανισμός δεν πρέπει να αποστέλλει πακέτα σε broadcast ή multicast IPv4 προορισμούς. Γενικά πρέπει να απορρίπτει όλα τα πακέτα που οι IPv4 και IPv6 διευθύνσεις δεν είναι παγκόσμιες unicast. (Αναλυτικότερα στην παράγραφο ¨Θέματα Ασφαλείας¨).

3.6.3 Maximum Transmission Unit

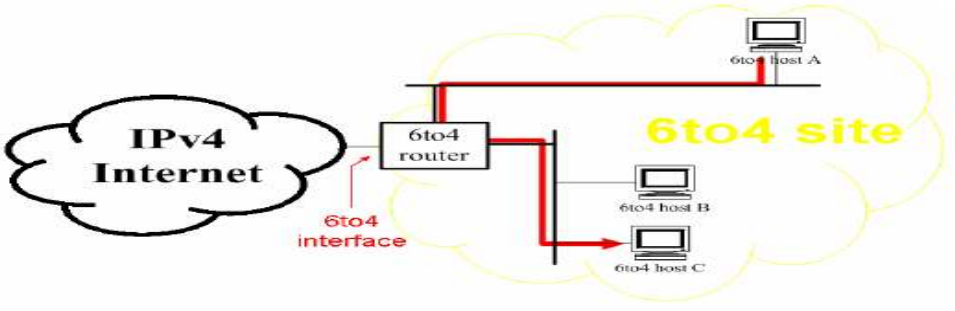
Σε ότι αφορά το μέγιστο μέγεθος μετάδοσης του πακέτου, ισχύουν τα όσα αναφέρθηκαν στην αντίστοιχη παράγραφο για το MTU για τους μηχανισμούς tunneling. Αν το μέγεθος της MTU είναι πολύ μεγάλο για κάποια ενδιάμεσα site, θα πραγματοποιηθεί IPv4 κατατεμαχισμός(fragmentation) των πακέτων. Αν και όχι επιθυμητός δεν είναι καταστροφικός εκτός από την περίπτωση της anycast διεύθυνσης για relay routers, που μπορεί τα τεμάχια να καταλήξουν σε διαφορετικούς IPv4 προορισμούς. Γενικά, το IPv4 "do not fragment" bit δεν πρέπει να τεθεί ¨1¨ στην επικεφαλίδα του ενθυλακωμένου πακέτου.

3.7 Σενάρια χρήσης του 6to4

Μέσα στο ίδιο site

Σε αυτή την περίπτωση χρησιμοποιείται μόνο IPv6 δρομολόγηση μέσα στο ίδιο το site και οι hosts συμπεριφέρονται σαν δυο κανονικοί IPv6 κόμβοι. Γενικά, μέσα στο 6to4 site χρησιμοποιείται κάποιο πρωτόκολλο εσωτερικής δρομολόγησης όπως το RIPng (Routing Information Protocol Next Generation – το αντίστοιχο του RIP για IPv6) και η μόνη διάφορα από τα αλλά native IPv6 sites είναι μια εγγραφή στους πίνακες δρομολόγησης του προθέματος 2002::/16 με next-hop την διεύθυνση του 6to4 router, ο οποίος έστειλε τις διαφημίσεις από τις οποίες προέκυψαν οι IPv6 διευθύνσεις των κόμβων και η οποία χρησιμοποιείται μόνο στην περίπτωση επικοινωνίας με κάποιο IPv6 (6to4 ή native) κόμβο εκτός του site. Το 6to4 interface δεν χρησιμοποιείται σε αυτό το σενάριο επικοινωνίας.

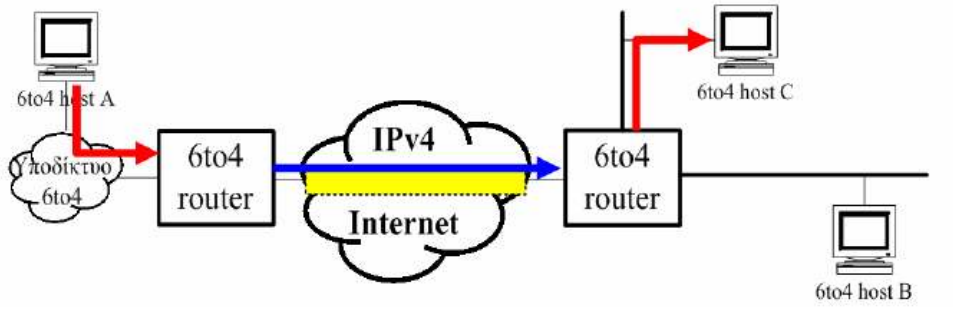
Η περίπτωση του πρώτου σεναρίου επικοινωνίας φαίνεται στο πιο κάτω σχήμα μεταξύ του host A και του host C.



Σχήμα 27: Περίπτωση επικοινωνίας 6to4 hosts στο ίδιο 6to4 site

Επικοινωνία μεταξύ δυο διαφορετικών 6to4 sites

Για αυτή την περίπτωση είναι αναγκαίο τα sites που πρόκειται να επικοινωνήσουν να διαθέτουν από τουλάχιστον μια παγκόσμια μοναδική IPv4 διεύθυνση. Αυτό το σενάριο υλοποιείται για τα sites που αρχίζουν να χρησιμοποιούν IPv6 αλλά ακόμα δεν μπορούν να έχουν πρόσβαση σε native ISP services. Μέσα στο site όλοι οι host υλοποιούν το IPv6 πρωτόκολλο , οι διευθύνσεις ορίζονται μεσώ των διαφημίσεων του router (router advertisement□□stateless address autoconfiguration) και οι hosts έχουν τις DNS name/address έγγραφες τους , έτσι ώστε να είναι δυνατό ένας host από κάποιο άλλο site να αποκτήσει την διεύθυνση τους.(Σε επόμενη παράγραφο περιγράφεται το DNS στο IPv6). Στο σενάριο αυτό το tunnel εγκαθίσταται μεταξύ των συνοριακών δρομολογητών των δυο sites στα οποία ανήκουν οι 6to4 hosts που πρόκειται να επικοινωνήσουν και τα πακέτα δρομολογούνται κατευθείαν από τον ένα 6to4 router στον άλλο χωρίς την παρουσία κάποιου ενδιάμεσου relay. Η περίπτωση του δεύτερου σεναρίου φαίνεται πιο κάτω μεταξύ του host A και του host C.



Σχήμα28: Περίπτωση επικοινωνίας 6to4 host με 6to4 host που ανήκει σε άλλο site

Διαδικασία:

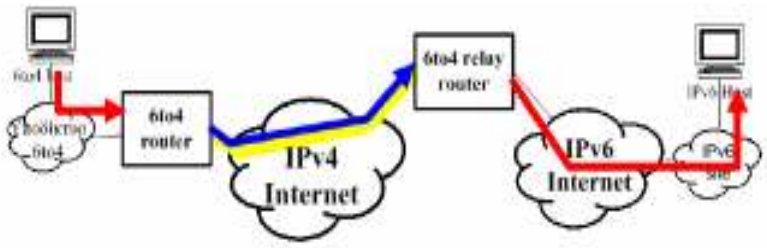
Ο 6to4 host στο ένα site(ουσιαστικά ένας IPv6 host) μαθαίνει μεσώ DNS αναζήτησης την διεύθυνση του αλλού 6to4 host. Μέσα στο site εκτός από τις 2002:V4ADDR::/48 διευθύνσεις, οι υπόλοιπες χειρίζονται σαν οποιεσδήποτε μη τοπικές διευθύνσεις και στέλνονται μεσώ του default route στο 6to4 router. Όταν ο router δει το 2002::/16 και επιπλέον ότι ο προορισμός δεν ανήκει στο τοπικό δίκτυο, προωθεί τα πακέτα στο 6to4 pseudo-interface, γίνονται οι απαραίτητοι έλεγχοι ασφάλειας και ακολούθως γίνεται η ενθυλάκωση σε IPv4 πακέτα. Το πεδίο protocol της εξωτερικής IPv4 επικεφαλίδας τίθεται σε 41 και κατόπιν τα πακέτα στέλνονται με κανονική IPv4 δρομολόγηση στον προορισμό τους με διεύθυνση προορισμού την IPv4 διεύθυνση που προκύπτει από το 2002::V4ADDR::/48 της IPv6 διεύθυνσης προορισμού, αν αφαιρεθούν τα πρώτα 2002::/16 bit ,και διεύθυνση προελεύσεως την IPv4 διεύθυνση του site που είναι και η διεύθυνση του εξωτερικού interface προς το Internet, από όπου θα σταλούν τα πακέτα.

Όταν ο 6to4 router του site προορισμού πάρει το πακέτο και δει στο IPv4 protocol 41 ‘ξεφλουδίζει’ την IPv4 επικεφαλίδα αφού γίνουν οι απαραίτητοι έλεγχοι ασφάλειας και προωθεί το πακέτο σαν με κανονική IPv6 δρομολόγηση μέσα στο 6to4 site προορισμού.

Έτσι αν γίνουν οι κατάλληλες έγγραφες DNS , ο οποιαδήποτε αριθμός sites μπορεί να επικοινωνήσουν μεταξύ τους, χωρίς την χρήση εξωτερικού πρωτοκόλλου δρομολόγησης (π.χ. BGP4+)αφού το ήδη υπάρχον IPv4 πρωτόκολλο εκτελεί την απαραίτητη διαδικασία.

Επικοινωνία 6to4 site με site που είναι συνδεδεμένο στο native IPv6 δίκτυο

Για αυτή την περίπτωση επικοινωνίας χρειάζεται τουλάχιστον ένας relay router, ο οποίος είναι στην ουσία ένας κανονικός IPv6 router με επιπλέον ένα 6to4 pseudo-interface όπου εκεί εκτελούνται η ενθυλάκωση και απενθυλάκωση των IPv6 πακέτων. Στη συγκεκριμένη αναφορά αναλύεται μόνο η περίπτωση που δεν χρησιμοποιείται κάποιο εξωτερικό πρωτόκολλο δρομολόγησης αλλά απλά ο 6to4 router του site που θέλει να στείλει σε site που ανήκει στο native IPv6 δίκτυο έχει καταγραμμένη στο routing table του την διεύθυνση του relay router που θα χρησιμοποιηθεί. Η διεύθυνση αυτή μπορεί να είναι είτε η unicast IPv4 διεύθυνση του relay είτε η anycast διεύθυνση 192.88.99.1 που καθορίζεται από το σχετικό RFC 3068 “An Anycast Prefix for 6to4 Relay Routers” για προώθηση των πακέτων προς τον πλησιέστερο για το 6to4 site relay router. Το σενάριο αυτό έχει επικρατήσει και χρησιμοποιείται αποκλειστικά σήμερα για αυτή την περίπτωση επικοινωνίας. Το σενάριο αυτό φαίνεται στο πιο κάτω σχήμα.



Σχήμα 29: Περίπτωση επικοινωνίας 6to4 host με host που ανήκει στο native IPv6 δίκτυο

Διαδικασία:

- **Αποστόλη πακέτων από host του 6to4 site σε host που ανήκει σε native IPv6 domain:**

Αφού βρεθεί μεσώ DNS η διεύθυνση του host όπου θα αποσταλεί το πακέτο, ο 6to4 host στέλνει το πακέτο στον 6to4 router του site μέσω το default route. Ο 6to4 router βλέπει την διεύθυνση προορισμού και προωθεί το πακέτο στο 6to4 interface, όπου αφού γίνουν οι απαραίτητοι ελέγχοι ασφαλείας, ενθυλακώνεται

το IPv6 πακέτο κάτω από την IPv4 επικεφαλίδα. Διεύθυνση προορισμού τίθεται η διεύθυνση του relay router που υπάρχει σαν next-hop στον πίνακα δρομολόγησης για τον συγκεκριμένο προορισμό. Αυτή μπορεί να είναι είτε η unicast διεύθυνση του relay είτε η anycast διεύθυνση, για τον πλησιέστερο προς το 6to4 site relay. Διεύθυνση προελεύσεως τίθεται η παγκόσμια IPv4 διεύθυνση του site, το πεδίο protocol στην τιμή 41 και προωθούνται τα πακέτα με κανονική IPv4 δρομολόγηση.

Ακολούθως, αφού ο relay router πάρει τα πακέτα και δει το IPv4 protocol 41, κάνει τους απαραίτητους έλεγχους ασφάλειας, ¨ξεφλουδίζει¨ την IPv4 επικεφαλίδα και προωθεί κανονικά με IPv6 δρομολόγηση το πακέτο στον προορισμό του.

Αποστόλη πακέτων από το native IPv6 site στο 6to4 site:

Ο 6to4 relay router διαφημίζει στο το πρόθεμα 2002::/16 μέσα στο native IPv6 δίκτυο, έτσι ώστε ο κάθε κόμβος να έχει ένα route 2002::/16 με next-hop την διεύθυνση του relay router που έστειλε τις διαφημίσεις.(Είναι σημαντικό οι υπόλοιποι κομβόι του native IPv6 να φιλτράρουν και να αποβάλλουν διαφημίσεις με προθέματα μεγαλύτερα από 16-bits, έτσι ώστε να μην διογκώνονται οι πίνακες δρομολόγησης). Αν ο IPv6-only node θέλει να στείλει σε ένα 6to4 host, μεσώ του route prefix 2002::/16 που έχει στο table του από τις διαφημίσεις του relay router στέλνει τα πακέτα στον router, όπου ακολούθως αφού η next-hop IPv6 διεύθυνση ταιριάζει στο πρόθεμα 2002::/16, γίνεται η προώθηση τους στο 6to4 pseudo-interface όπως στα προηγούμενα και η ενθυλάκωση των πακέτων, για να αποσταλούν με IPv4 στον 6to4 router του site προορισμού, με IPv4 διεύθυνση προελεύσεως την διεύθυνση του εξωτερικού interface του relay router.

3.8 Θέματα ασφαλείας του 6to4 μηχανισμού

3.8.1 Απειλές-είδη επιθέσεων

Όπως περιγράφτηκε πιο πάνω ο 6to4 μηχανισμός περιλαμβάνει 6to4 routers και 6to4 relay routers που δέχονται και ¨ξεφλουδίζουν¨ IPv4 protocol 41 πακέτα από οποιονδήποτε κόμβο μέσα στο Internet καθώς και πακέτα IPv6 (οι relay routers) από οποιονδήποτε IPv6 κόμβο. Αυτά κυρίως τα χαρακτηριστικά καθιστούν τον μηχανισμό - όπως και γενικά όλους τους μηχανισμούς automatic tunneling, οι οποίοι δεν γνωρίζουν εκ των πρότερων τον κόμβο προελεύσεως των πακέτων- ευάλωτο σε κακόβουλες επιθέσεις κυρίως Denial of Service (DoS) και διευκολύνουν το spoofing των IPv6 διευθύνσεων από κακόβουλους κόμβους. Και το πρόβλημα δεν είναι τόσο η ζημία που οι επιθέσεις αυτές μπορεί να προκαλέσουν στο μηχάνημα που υλοποιεί τον 6to4 μηχανισμό, όσο το γεγονός ότι ο μηχανισμός χρησιμοποιείται για την απόκρυψη των ιχνών του επιτιθέμενου.

Για την σωστή και ασφαλή υλοποίηση του 6to4 μηχανισμού πρέπει να λαμβάνονται σοβαρά υπόψη τα διάφορα είδη επιθέσεων στα οποία ο 6to4 μηχανισμός είναι ευάλωτος.

Συγκεκριμένα οι 6to4 μηχανισμοί μπορούν να υποστούν τις πιο κάτω απειλές:

- Επιθέσεις Άρνησης Υπηρεσίας (Denial-of-Service - DoS) κατά τις οποίες ο κακόβουλος κόμβος εμποδίζει τον κόμβο που δέχεται την επίθεση να επικοινωνήσει με άλλους κόμβους.
- Επιθέσεις Άρνησης Υπηρεσίας με 'ανάκλαση'(reflected Denial-of-Service) όπου ο κακόβουλος κόμβος αντανακλά το διακινούμενο φορτίο από ανυποψίαστους κόμβους σε ένα κόμβο (ο οποίος δέχεται την επίθεση), εμποδίζοντας έτσι την επικοινωνία του με άλλους κόμβους.
- 'Υποκλοπή υπηρεσιών' (service theft)κατά την οποία ο κακόβουλος κόμβος/site/χρηστής μπορεί να χρησιμοποιήσει υπηρεσίες του relay router χωρίς αρμοδιότητα. Συγκεκριμένα, ενώ ο διαχειριστής του relay router θέτει περιορισμούς έτσι ώστε μόνο περιορισμένα 6to4 sites και συγκεκριμένα IPv6 sites να χρησιμοποιούν τον relay ,οι χρηστές είτε με χρήση την IPv4 διεύθυνσης του relay (αντί της anycast στην οποία εφαρμόζονται οι περιορισμοί) είτε χρησιμοποιώντας άλλες μεθόδους αποκτούν πρόσβαση στον relay.
- Επιθέσεις με μηνύματα ND
- Τοπικές IPv4 Broadcast Επιθέσεις

Οι δυο τελευταίες επιθέσεις αντιμετωπίζονται εξ' ολοκλήρου με σωστή υλοποίηση των Sanity Checks, τους οποίους πραγματοποιούν οι περισσότερες σήμερα tunnel devices, και ουσιαστικά ο κίνδυνος τους πλέον δεν υφίσταται.

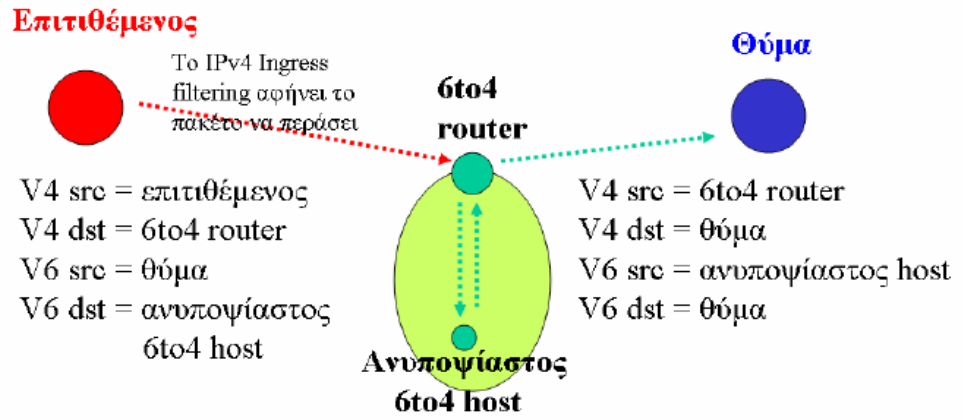
3.8.2 Λόγοι που καθιστούν δυνατές τις επιθέσεις

Οι 6to4 routers πρέπει να δέχονται και να απενθυλακώνουν IPv4 πακέτα από όλους τους relay routers. Και δεν είναι δυνατό να γνωρίζουν αν ο relay από τον οποίο προέρχονται τα πακέτα είναι έμπιστος και για την ακρίβεια ούτε καν αν είναι υπαρκτός. Αυτό είναι κυρίως το τρωτό σημείο του 6to4 μηχανισμού και για το οποίο έχει γίνει και συνεχίζει να γίνεται η περισσότερη ερευνά. Ο 6to4 router είναι αδύνατο να γνωρίζει την πραγματική διεύθυνση του relay router (που μπορεί να είναι οποιαδήποτε unicast διεύθυνση) που αναγράφεται στην εξωτερική IPv4 επικεφαλίδα ως η διεύθυνση προελεύσεως. Έτσι απλούστατα οποιοσδήποτε IPv4 ή IPv6 χρηστής μπορεί να στείλει πακέτα σε κάποιο 6to4 χρηστή, με οποιαδήποτε IPv6 διεύθυνση προελεύσεως αφού στην περίπτωση επικοινωνίας μέσω relay δεν μπορεί να γίνει καμία αντιστοίχηση.

Οι relay routers πρέπει να δέχονται πακέτα από όλους τους 6to4 routers και επιπλέον από όλους τους native IPv6 κόμβους, τα οποία ανάλογα ενθυλακώνουν ή απενθυλακώνουν χωρίς να γίνεται κάποιος έλεγχος στα δεδομένα των πακέτων.

Η ελλιπής, και πολλές φορές λανθασμένη υλοποίηση και διαχείριση των 6to4 και των Relay Routers, που αφήνει σημαντικά κενά ασφάλειας. Επιπλέον, Οι λανθασμένοι ή όχι πλήρεις έλεγχοι ασφάλειας που γίνονται στους δυο πιο πάνω δρομολογητές.

Πιο κάτω δίνεται ένα κλασικό παράδειγμα όπου ο επιτιθέμενος, ένας IPv4 χρηστής χρησιμοποιεί τον 6to4 μηχανισμό για να εξαφανίσει τα ίχνη του.



Σχήμα 30: Χρήση του 6to4 μηχανισμού σε επίθεση Reflected DoS

Για τον πρώτο θέμα ασφαλείας, που είναι και το μείζον πρόβλημα του μηχανισμού δεν έχει βρεθεί ακόμη κάποια οριστική λύση και η έρευνα συνεχίζεται. Στο RFC 3964 (“Security Considerations for 6to4”) προτείνεται σαν η καλύτερη προς το παρών λύση όλοι οι relay routers να ρυθμίζονται και να διαφημίζουν το anycast prefix 192.88.99.0/24, καθιστώντας έτσι δυσκολότερο το spoofing των διευθύνσεων. Επιπλέον να εκτελούν ingress filtering στα πακέτα που προέρχονται από το IPv6 δίκτυο και να κάνουν τους έλεγχους ασφαλείας (Sanity Checks) που δίνονται πιο κάτω.

Όμως, η μεγαλύτερη σημασία για την αντιμετώπιση των ενδεχόμενων κενών ασφαλείας του μηχανισμού πρέπει να δοθεί στο στάδιο της υλοποίησης του και στην κατόπιν διαχείριση του. Σωστή υλοποίηση, διαχείριση και εφαρμογή των απαραίτητων έλεγχων θα ελαττώσει τους πιθανούς κίνδυνους και ουσιαστικά όπως έχει αποδειχτεί ένα σύστημα με σωστά και ολοκληρωμένα υλοποιημένο τον 6to4 μηχανισμό είναι τόσο ευάλωτο όσο ένα οποιοδήποτε άλλο σύστημα χωρίς 6to4.

Οι πιο κάτω έλεγχοι είναι απαραίτητοι για την ασφαλή λειτουργία:

3.8.3 Ασφάλεια 6to4 Router

Πρέπει να εφαρμόζει τους έλεγχους ασφάλειας καθώς και τα Sanity Checks στο διακινούμενο φορτίο που λαμβάνει τόσο από το τοπικό 6to4 site όσο και από τους

άλλους 6to4 routers και τους relay routers. Οι ελέγχοι αυτοί εκτός από την προστασία που παρέχουν ενάντια στα διάφορα είδη επιθέσεων, εγγυούνται και την καλή λειτουργία του μηχανισμού, ότι δηλαδή τα πακέτα από το 6to4 site που διαχειρίζεται ο εκάστοτε διαχειριστής δεν θα απορριφθούν από άλλους 6to4 ή relay routers που εκτελούν τους συγκεκριμένους ελέγχους. Στους έλεγχους πρέπει να περιλαμβάνονται τα πιο κάτω:

- Τόσο στη φάση της εισόδου, όσο και της εξόδου των πακέτων από το 6to4 interface όπου γίνεται η ενθυλάκωση/απενθυλάκωση, να ελέγχεται αν η IPv4 διεύθυνση (V4ADDR) που προκύπτει αν αφαιρεθεί το 2002::/16 από την 6to4 διεύθυνση (2002:V4ADDR:) ταιριάζει με την IPv4 διεύθυνση του εξωτερικού πακέτου (εκτός φυσικά όταν τα πακέτα προέρχονται από κάποιο relay router όπου αυτό δεν είναι δυνατό).
- **"Λογικοί έλεγχοι" ("Sanity Checks") IPv4**.

  Να μην επιτρέπονται οι διευθύνσεις οι οποίες είναι ιδιωτικές,broadcast ή δεσμευμένες. Συγκεκριμένα δεν θα επιτρέπεται η ενθυλάκωση και απενθυλάκωση των πιο κάτω IPv4 διευθύνσεων:

  ο 0.0.0.0/8 (not assigned yet)

- o 10.0.0.0/8 (private)
- o 127.0.0.0/8 (loopback)
- o 172.16.0.0/12 (private)
- o 192.168.0.0/16 (private)
- o 169.254.0.0/16 (IANA Assigned DHCP link-local)
- o 224.0.0.0/4 (multicast)
- o 240.0.0.0/4 (reserved and broadcast)
- o Τοπικές broadcast διευθύνσεις

• **"Λογικοί έλεγχοι" ("Sanity Checks") IPv6**

Να μην επιτρέπει την διακίνηση πακέτων όταν η IPv6 διεύθυνση προορισμού δεν είναι παγκόσμια unicast διεύθυνση. Συγκεκριμένα απορρίπτονται οι πιο κάτω διευθύνσεις:

- o 0::/16 (compatible, mapped addresses, loopback, unspecified, ...)
- o fe80::/10 (link-local)
- o fec0::/10 (site-local)
- o ff00::/8 (any multicast)

• Να δίνεται ιδιαίτερη προσοχή κατά τον καθορισμό των routes στον πίνακα δρομολόγησης έτσι ώστε πακέτα προς αλλά 6to4 sites να μην δρομολογούνται μέσω relay router.

• Να απορρίπτουν πακέτα που προέρχονται από άλλο 6to4 domain μεσώ relay router.

3.8.4 Ασφάλεια Relay Router

Πρέπει να εφαρμόζει έλεγχους ασφάλειας και τα Sanity Checks στο διακινούμενο φορτίο που λαμβάνει τόσο από το native IPv6 site όσο και από τους 6to4 routers. Στους έλεγχους πρέπει να περιλαμβάνονται τα πιο κάτω:

• Να μην επιτρέπει διακίνηση πακέτων που έχουν ιδιωτικές,broadcast ή δεσμευμένες IPv4 διευθύνσεις στο τούνελ ή στο 6to4 πρόθεμα τους.(οι συγκεκριμένες διευθύνσεις δίνονται πιο πάνω – IPv4 Sanity Checks)

• Να μην επιτρέπει διακίνηση πακέτων από 6to4 routers όταν η IPv4 διεύθυνση πηγής του τούνελ δεν ταιριάζει με την V4ADDR της 6to4 διεύθυνση(2002:V4ADDR) του ενθυλακωμένου πακέτου.

• Να εμποδίζει τα πακέτα με διεύθυνση προορισμού μη παγκόσμια IPv6 διεύθυνση (IPv6 Sanity Checks).

• Αποβάλλει πακέτα που προέρχονται από 6to4 routers και έχουν στη διεύθυνση προορισμού το πρόθεμα 6to4.

• Να φιλτράρει και να αποβάλλει τα πακέτα με protocol 41 τα οποία δεν έχουν την anycast διεύθυνση προορισμού 192.88.99.1 . (περίπτωση που ρυθμίζεται στην anycast διεύθυνση)

• Αν εξυπηρετεί μικρό αριθμό δικτύων, να χρησιμοποιεί access lists για έλεγχο της πρόσβασης.

• Χρήση Ingress Filtering για τα πακέτα από το IPv6 site.

4-ΑΣΦΑΛΕΙΑ IPV4 ΚΑΙ IPV6

Το 1994.το Συμβούλιο Αρχιτεκτονικής Διαδικτύου(Internet Architecture Board-IAB) έκδωσε μια έκθεση με τίτλο Ασφάλεια στην Αρχιτεκτονική του Διαδικτύου (RFC 1636).Η έκθεση δήλωνε τη γενική ομοφωνία πως το Διαδίκτυο χρειάζεται περισσότερη και καλύτερη ασφάλεια και προσδιόρισε περιοχές κλειδιά για τους μηχανισμούς ασφαλείας.Μεταξύ αυτών ήταν να ασφαλιστεί η υποδομή του δικτύου από μη εξουσιοδοτημένα παρακολούθηση και έλεγχο της κίνησης τδικτύου,΄όπως επίσης και η ανάγκη να ασφαλιστεί η κίνηση τερματικού χρήστη προς τερματικό χρήστη χρησιμοποιώντας πιστοποίηση και μηχανισμούς κρυπτογράφησης.

Αυτά τα ενδιφέροντα είναι πληρως δικαιολογημένα.Ως επιβεβαίωση,η ετήσια έκθεση του 1998 από την Computer Emergency Response Team (CERT) καταγράφει περισσότερα από 1300 αναφερθέντα περιστατικά ασφαλείας που επηρέασαν σχεδόν 20,000 τοποθεσίες (sites).ΟΙ περισσότερο σημαντικοί τύποι επιθέσεων περιλάμβαναν εξαπάτηση IP,στις οποίες οι εισβολείς δημιούργησαν πακέτα με ψεύτικες διευθύνσεις IP και εκμεταλλεύτηκαν εφαρμογές που χρησιμοποιούν πιστοποίηση βασισμ΄ενη στη διεύθυνση IP,διάφορες μορφές κρυφακούσματος και αναρρόφηση πακέτων,στις οπίες οι επιτιθέμενοι διάβασαν μεταδόμενη πληροφορία,περιλαμβάνοντας πληροφορία logon και περιεχόμενα βάσης δεδομένων.

Σε απόκριση σε αυτά τα ζητήματα,το IAB περιέλαβε την πιστοποίηση και την κρυπτογράφηση ως απαραίτητα χαρακτηριστικά ασφαλείας στο IP επόμενης γενεάς,το οποίο έχει εκδοθεί ως IPv6.Ευτυχώς,όμως αυτές οι δυνατότητες ασφαλείας σχεδιάστηκαν για να είναι χρησιμοποιήσιμες τόσο με το IPv4 όσο και με το IPV6.Αυτό σημαίνει ότι οι κατασκευαστές μπορούν να ξεκινήσουν να προσφέρουν αυτά τα χαρακτηριστικά τώρα και πολλοί κατασκευαστές έχουν ήδη δυνατότητα IPsec στα προιόντα τους.

Έχοντας αναλύσει τα πρωτόκολλα και τις επιθέσεις πάνω σε αυτά στα προηγούμενα κεφάλαια μπορούμε να αρχίσουμε να σκεφτόμαστε το τι θέλουμε από ένα πρωτόκολλο έτσι ώστε να το θεωρήσουμε ασφαλές; αφού αναγνωρίσουμε αυτό, τι είναι αυτό που πρέπει να κάνουμε ώστε να γίνει ασφαλές;

Μια αρχική σκέψη είναι να μη μπορεί κάποιος να διαβάσει εύκολα την πληροφορία από τα πακέτα που στέλνουμε και λαμβάνουμε. Αυτό είναι η μία παράμετρος αλλά όχι μια ολική λύση στο πρόβλημα της ασφάλειας. Σύμφωνα με τη θεωρία ένα ασφαλές δίκτυο παρέχει τα εξής χαρακτηριστικά:

1. Πιστοποίηση (Authentication)

2. Ακεραιότητα (Integrity)

3. Εμπιστευτικότητα (Confidentiality)

4. Κρυπτογράφηση (Encryption)

5. Μη αποκήρυξης (Non – repudiation)

Τα οποία έχουμε αναλύσει αρχικά.

Η ακεραιότητα, η εμπιστευτικότητα, η κρυπτογράφηση και σε ορισμένες περιπτώσεις η πιστοποίηση, μπορούν να διασφαλιστούν με τη διαδικασία της κρυπτογράφησης στα πακέτα και τα σήματα που ανταλλάσσονται στο δίκτυο. Υπάρχουν και ιδικές τεχνικές που προσφέρουν πιστοποίηση.

Υπάρχουν δυο κατηγορίες αλγόριθμων κρυπτογράφησης, οι συμμετρικοί και οι ασύμμετροι αλγόριθμοι. Οι συμμετρικοί εκτελούν την κρυπτογράφηση και την αποκρυπτογράφηση με το ίδιο κλειδί, ενώ οι ασύμμετροι παράγουν το κρυπτόγαμμα (το αποτέλεσμα μετά την κρυπτογράφηση) με ένα κλειδί που είναι συνήθως δημόσιο και αποκρυπτογραφούν με ένα άλλο που κρατιέται κρυφό. Το πρόβλημα με τους συμμετρικούς αλγορίθμους είναι το πώς δυο κόμβοι που θέλουν να επικοινωνήσουν θα ανταλλάξουν το κλειδί τους.

Όπως μπορούμε να καταλάβουμε τεράστιας σημασίας για τους αλγορίθμους κρυπτογράφησης είναι το κλειδί, όσον αφόρα το μέγεθος του και το πώς αυτό θα (μυστικά) διανεμηθεί. Γενικά ένα άλλο συστατικό είναι πολύ σημαντικό για την ασφάλεια ενός πρωτοκόλλου και αυτό είναι το IKE.

Το πρόβλημα τις μη αποκήρυξης λύνεται με traffic analysis τεχνικές. Είναι ιδιαίτερα σημαντικό πρόβλημα καθώς αν καταφέρει κάποιος να αποκλίσει ένα κόμβο κλειδί για τη λειτουργία του δικτύου (λχ home agent) τότε θα έχει παραλύσει όλο το δίκτυο.

Τα πρωτόκολλα τα οποία έχουν φτάσει σε επίπεδο να έχουν RFC προβλέπουν μέτρα προστασίας για μερικούς ή όλους του τύπους απειλών. Άρα, από τα πρωτόκολλα πρέπει να δούμε για ποιές απειλές μεριμνούν και αν αφήνουν κενά πώς αυτά καλύπτονται.

4.1 Εφαρμογές του IPsec

Στο IPv6 έγινε υποχρεωτική η υποστήριξη του IPsec από όλες τις εφαρμογές. Υπάρχουν 2 επικεφαλίδες IPsec: η επικεφαλίδα πιστοποίησης(AH) που παρέχει υπηρεσίες πιστοποίησης και η επικεφαλίδα Encapsulating Security Payload(ESP) που παρέχει είτε πιστοποίηση είτε κρυπτογράφηση είτε και τα 2. Η διαφορά μεταξύ της επικεφαλίδας AH και της πιστοποίησης-μόνο ESP είναι ότι η AH προστατεύει επιπλέον και τα περισσότερα πεδία της επικεφαλίδας IP ενώ η ESP μπρεί μόνο να προστατέψει τις επικεφαλίδες και τα δεδομένα που ακολουθούν την επικεφαλίδα ESP. Και η AH και η ESP εφαρμόζονται σε 2 καταστάσεις: κατάσταση μεταφοράς και κατάσταση τούνελ. Στην κατάσταση τούνελ, η επικεφαλίδα AH ή ESP προηγούνται της επικεφαλίδας IP και μια καινούρια επικεφαλίδα IP τοποθετείται μπροστά από τις επικεφαλίδες AH ή ESP. Για την πιστοποίηση χρησιμοποιούνται ο αλγόριθμος HMAC-MD5-96 και για κρυπτογράφηση οι 3DES και AES.

Το Ipsec έχει τη δυνατότητα να ασφαλίζει τις επικοινωνίες κατά μήκος ενός δικτύου-ιδιωτικού ή δημόσιου και κατά μήκος του Διαδικτύου.Παράδειγματα της χρήσης του περιλαμβάνουν τα ακόλουθα:

- **Ασφάλιση συνδεσιμότητας υποκαταστημάτων πάνω στο Διαδίκτυο**:Μια εταιρεία μπορεί να οικοδομήσει ένα ασφαλές νοητό δίκτυο πάνω από το διαδικτυο ή πάνω από κάποιο δημόσιο δίκτυο ευρείας περιοχής.Αυτό επιτρέπει σε μια επιχειρηση να βασίζεται ισχυρα στο Διαδίκτυομειώνοντας την ανάγκη της για ιδιωτικά δίκτυα,γλιτώνοντας κόστος και επιβάρυνση διαχε'ιρισης δικτύου.
- **Ασφαλή απομακρυσμένη πρόσβαση πάνω στο Διαδίκτυο**:ένας τερματικός χρήστης του οποίου το σύστημα είναι εφοδιασμένο με πρωτόκολλα ασφαλείας IP μπορεί να κάνει μια τοπική κλήση σε ένα παροχέα υπηρεσίας διαδικτύου (ISP) και να πετύχει ασφαλή πρόσβαση σε ένα εταιρικό δίκτυο.
- **Αποκατάσταση εξωδικτυακής και ενδοδικτυακής συνδεσιμότητας με συναιτέρους**.:Το IP sec μπορεί να ασφαλίσει την επικοινωνία με άλλους οργανισμούς,εξασφαλίζοντας πιστοποίηση και εμπιστευτικότητα και παρέχοντας ένα μηχανισμό ανταλλαγής κλειδιού.

- **Εμπλουτισμός ασφαλείας ηλεκτρονικού εμπορίου**:Το IPsec εμπλουτίζει τιε εφαρμογές του διαδικτύου και ηλεκτρονικού εμπορίου παρόλο που έχουν ήδη ενσωματωμέν απρωτόκολλα ασφαλείας.

Το βασικό χαρακτηριστικό του IPsec είναι που του επιτρέπει να υποστηρίζει αυτές τις ποικίλες εφαρμογές είναι ότι μπορεί να κρυπτογραφήσει και να πιστοποιήσει όλη την κίνηση στο επίπεδο IPsec.Έτσι μπορούν ναασφαλιστούν όλες οι κατανεμημένες εφαρμογές συμπεριλαμβανομένης του απομακρυσμένου logon ,εφαρμογές client/server,ηλεκτρονικό ταχυδρομεί,μεταφορά αρχείων και ούτω καθεξής.

Ο Σκοπός του IPsec

Όπως ανφέρθηκε το IPsec παρέχει τρεις ευκολίες:μια λειτουργία μόνο πιστοποίησης αναφερόμενη ως επικεφαλίδα Πιστοποίησης(AH),μια συνδυασμένη λειτουργία πιστοποίησης/κρυπτογράφησης ονομαζόμενη Ενθυλακωμένο Φορτίο Ασφαλείας(ESP) και μια λειτουργία ανταλλαγής κλειδιού.Για τα νοητά ιδιωτικά δίκτυα,είναι συνήθως επιθυμητ'ή τόσο η πιστοποίηση όσο και η κρυπτογράφηση,επειδήείναι σημαντικό να εξασφαλίζει πως μη εξουσιοδοτημένοι χρήστες δε διαπερνούν το νοητό ιδιωτικό δίκτυο και να εξασφαλίζεται πως αυτοί που "κρυφακούν" στο διαδίκτυο δε μπορούν να διαβάσουν μηνύματα που στέλνονται πάνω στο νοητό ιδιωτικό δίκτυο.Επειδή και τα δύο χαρακτηριστικά είναι επιθυμητά,οι περισσότερες υλοποιήσεις είναι πολύ πιθανό να χρησιμοποιούν το ESP παρά το AH.Η λειτουργία ανταλλαγής κλειδιών όπως επίσης και ένα αυτοματοποιημένο σχήμα..

4.2 Σχέσεις Ασφαλείας

Μια βασική ιδέα που εμφανίζεται τόσο στους μηχανισμούς πιστοποίησης όσο και στους μηχανισμούς εμπιστευτικότητας για το Ipsec είναι η σχέση ασφαλείας (SA).Μια σχέση είναι μια μονόδρομη συγγένεια μεταξύ ενός αποστολέα και ενός παραλήπτη που παρέχει υπηρεσίες ασφαλείας στην κίνηση που μεταφέρεται πάνω σε αυτή.Εαν απαιτείται μια ομότιμη συγγένεια,για μια αμφίδρομη ασφαλή ανταλλαγή,τότε απαιτούνται δύο σχέσεις ασφαλείας.Οι υπηρεσίες ασφαλείας παρέχονται σε μια SA για τη χρήση των AH ή ESP αλλά όχι και των δύο.

Μια σχέση ασφαλείας είναι μοναδικά προσδιορισμένη από τρεις παραμέτρους:

- **Κατάλογος παραμέτρων ασφαλείας (SPI):**Μια σειρά bit εκχωρημένη σε αυτή την SA η οποία έχει μόνον τοπική σημασία.Ο SPI μεταφέρεται μέσα στις επικεφαλίδες AH και ESP για να επιτρέψει στο λαμβάνον σύστημα να επιλέξει τη SA κάτω από την οποία θα επεξεργάζεται ένα ληφθεν πακέτο.

- **Διεύθυνση προορισμού IP:**Επί του παρόντος επιτρέπεται μόνο διευθύνσεις μονής αποστολής.Αυτ'η είναι η διεύθυνση του προοριζόμενου τερματικού σημείου της SA, η οποία μπορεί να είναι ένα σύστημα τερματικού χρήστη ή ένα σύστημα δικτύου όπως ένας τοίχος προστασίας (firewall) ή των δρομολογητών.

- **Αναγνωριστής πρωτοκόολου ασφαλείας:**Αυτός προορίζεται εάν η σχέση είναι μια μέση σχέση ασφαλείας AH ή ESP.

Για το λόγο αυτό σε κάθε πακέτο IP, η σχέση ασφαλείας είναι μοναδικά προσδδιορισμένη από τη Διεύθυωση Προορισμού στη κεφαλίδα του Ipv4 ή Ipv6 και το SPI στην Εσωκλειώμενη επικεφαλίδα επέκτασης (AH ή ESP).

Μια υλοποίηση IPsec περιλαμβάνει μια βάση δεδομένων σχέσεων ασφαλείας ππου καθορίζεται από τις ακόλουθες παραμέτρους:

- **Μερητής αριθμού ακολουθίας:**Μια 32 bit τιμή που χρησιμοποιείται για να παράγει το πεδίο αριθμού ακολουθίας στις επικεφαλίδες AH ή ESP.
- **Μετρητής υπερχείλισης ακολουθίας:**Ενας δείκτης που υποδηλώνει εάν η υπερχείλιση του μετρητή αριθμού ακολουθίας θα μπορούσε να παράγει ένα εξεταστέο συμβάν και να αποτρέψει την περαιτέρω μετάδοση πακέτων σε αυτή τη SA.
- **Παράθυρο αποτροπής επανεκτέλεσης:** Χρησιμοποείται για να προσδιορίσει ένα εισερχόμενο πακέτο AH ή ESP είναι μια επανεκτελεση,καθορίζοντας ένα παράθυρο ολίσθησης εντός του οποίου πρέπει να πέφτει ο αριθμός ακολουθίας.
- **ΠληροφορίαAH:**Αλγόριθμος πιστοποιήσης,κλειδιά,τιμές αρχικοποίησης,διάρκειες ζωής κλειδιώνκαι σχετικές παράμετροι που χρησιμοποιούνται με το ESP.
- **Πληροφορία ESP:**Αλγόριθμος κρυπτογράφησης και πιστοποίησης,κλειδιά,τιμές αρχικοποίησης,διάρκεια ζωής κλειδιών και σχετικές παράμετροι που χρησιμοποιούνται με το ESP.
- **Διάρκεια ζωής αυτής της σχέσης ασφαλείας:** Μια μέτρηση χρονικού διαστήματος ή byte μετά την οποία μια SA πρέπει να αντικατασταθεί με μια νέα SA (ΚΑΙ ΝΈΟ SPI) ή να τερματιστεί,συν μια ένδειξη για ποιες από αυτές τις ενέργειες θα προκύψουν.
- Τύπος πρωτοκόλλου IPsec:Σήραγγας,μεταφοράς ή χαρακτήρων (wildcard)
- Διαδρομή MTU:Οποιαδήποτε παρατηρούμενη διαδρομή μ΄λεγιστης μεταφοράςν (μέγιστο μέγεθος πακέτου που μπορεί να διαδοθεί χωρίς τεμαχισμό) και μεταβλητές που πλαισιώνουν (απαιτείται για όλες τις υλοποιήσεις)

Ο μηχανισμός διαχείρισης κλειδιού που χρησιμοποιείται για τη διανομή των κλειδιών είναι συνδυασμένος με τους μηχανισμούς πιστοποίησης και μυστικότητας μόνο μέσω του καταλόγου των παραμέτρων ασφαλείας.Για ρτο λόγο αυτό,η πιστοποίηση και η μυστικότητα έχουν καθοριστεί ανεξάρτητα από οποιονδήποτε συγκεκριμένο μηχανισμό διαχείρισης κλειδιού.

4.3 Τύποι Μεταφοράς και Σήραγγας.

Τόσο η AH όσο και το ESP υποστηρίζουν δύο τύπους χρήσης:τους τύπους μεταφοράς και τους τύπους σήραγγας.

Τύποι Μεταφοράς

Ο τύπος μεταφοράς παρέχει προστασία για πρωτόκολλα ανωτέρου επιπέδου.Δηλαδή,η προστασία του τύπου εκτείνεται στο φορτίο ενός πακέτου IP.Παραδείγματα περιλαμβάνουν ένα τεμάχιοTCP ή UDP,ή ένα πακέτο ICMP,από τα οποία όλα λειτουργούν απευθείας πάνω στο IP σε μια στοίβα πρωτοκόλλων ενός υπολογιστή.Συνήθως,ο τύπος μεταφοράς χρησιμοποιείται για επικοινωνία από άκρο σε άκρο μεταξύ δύο υπολογιστών.Όταν ένας υπολογιστής εκτελεί AH ή ESP πάνω στο IPV4 ,το φορτίο είναι δεδομένα που κανονικά ακολουθπούν τόσο την επικεφαλίδα IP όσο και οποιεσδηποτε επικεφαλίδες επέκτασης του IPV6 είναι παρούσες,με την πιθανή εξαίρεση της επικεφαλίδας επιλογών προορισμού,η οποία μπορεί να περιλαμβάνεται εντός της προστασίας.

Το ESP σε τύπο μεταφοράς κρυπτογραφεί και προαιρετικά πιστοποιεί το φορτίο IP ,όχι όμως και την επικεφαλίδα IP.Η AH σε τύπο μεταφοράς πιστοποιεί το φορτίο IP και επιλεγμένα τμήξματα της επικεφαλίδας IP.

Τύπος Σήραγγας

Ο τύπος σήραγγας παρέχει προστασία σε ολόκληρο το πακέτο IP.Για να το επιτύχει,αφού προστεθούν τα πεδία AH ή ESP στο πακέτο IP,ολόκληρο το πακέτο συν τα πεδία ασφαλείας μεταχειρίζεται ως το φορτίο ενός καινούργιιου «εξωτερικού» πακέτου IP με μια καινούργια επικεφαλίδα IP.Ολόκληρο το αρχικό ή εσωτερικό πακέτο ταξιδεύει διμέσου μιας «σήραγγας» από το ένα άκρο ενός δικτύου IP στο άλλο.Κανένας δρομολογητής δεν είναι ικανός να εξετάσει την εσωτερική επικεφαλίδα IP.Επειδή το αρχικό πακέτο είναι ενθυλακωμένο,το καινούργιο,μεγαλύτερο πακέτο μπορεί να έχει τελείως διαφορετικές διευθύνσεις πηγής – προορισμου προσθέτοντας σε ασφάλεια.Με τον τύπο της σήραγγας ένας αριθμός από υπολογιστές σε δίκτυα πάνω σε από τοίχους προστασίας μπορεί να συμμετάσχει σε ασφαλείς επικοινωνίες χωρίς την υλοποίηση του IPsec.Τα απροστάτευτα πακέτα που παράγονται από τέτοιους υπολογισμούς μπαίνουν σε σήραγγα διαμέσου εξωτερικών δικτύων από SA τα'υπου σήξραγγας εγκατεστημένων από λογισμικό IPSsec στο τοίχο προστασίας ή στον ασφαλή δρομολογητή στο όριο του τοπικού δικτύου.

4.4 Επικεφαλίδα Πιστοποίησης.

Η επικεφαλίδα πιστοποίησης παρέχει δυνατότητα για υποστήριξη και ακεραιότητα δεδομένων και πιστοποίηση των πακέτων IP.Το χαρακτηριστικό ακεραιότητας δεδομένων εξασφαλίζει πως είναι αδυνατό να μην ανιχνευθεί τροποποίηση στο περιεχόμενο ενός πακέτου κατά τη μεταφορά.Το χαρακτηριστικό πιστοποίησης επιτρέπει σε ένα τερματικό σύστημα ή σε μια συσκευή του δικτύου να πιστοποιεί τον χρήστη ή την εφαρμογή και να φιλτράρει ανάλογα την κίνηση.Επίσης εμποδίζει τις επιθέσεις εξαπάτησης διευθύνσεων που παρατηρούνται στο διαδίκτυο.Η πιστοποίηση βασίζεται στο κώδικα πιστοποίησης μηνύματος (MAC).Η επικεφαλίδα πιστοποίησης αποτελείται από τα ακόλουθα πεδία:

- Επόμενη Επικεφαλίδα (8 bit) Προσδιορίζει το τύπο της επικεφαλίδας που ακολουθεί άμεσα αυτήν την επικεφαλίδα.
- Μήκους φορτίου (8 bit): Το μήκος της επικεφαλίδας πιστοποίησης σε 32 bit λέξεις μείον 2.
- Δεσμευμένο (16 bit):Για μελλοντική χρήση
- Κατάλογος παραμέτρων ασφαλείας(32 bit):Προσδιορίζει μια σχέση ασφαλείας
- Αριθμός ακολουθίας(32 bit):Μια μονοτονικά αυξανόμενη τιμή μετρητή
- Δεδομένα πιστοποίησης (μεταβλητό):Ένα μεταβλητού μήκους πεδίο που περιέχει την τιμή ελέγχου ακεραιότητας (ICV) ,ή MAC γι αυτό το πακέτο.
- Το πεδίο πιστοποίησης Δεδομένων υπολογίζεται πάνω στα παρακάτω:
- Πεδία επικεφαλίδας IP που είτε δεν αλλάζουν στη μεταφορά είτε είναι προβλέψιμα στην τιμή επί της άφιξης στο ακραίο σημείο για την AH SA.
- Την επικεφαλίδα AH αλλιώς το πεδίο Δεδομένων Πιστοποίησης το οπίο τίθεται στο μηδέν για λόγους υπολογισμού τόσο στην πηγή όσος και στον προορισμό.
- Όλα τα δεδομένα πρωτοκόλλου ανωτέρου επιπέδου,τα οπία θεωρούνται αμετάβλητα κατά τη μεταφορά.

- Για το IPv6 , παραδείγματα στη βασική επικεφαλίδα είναι η ΄Εκδοση,η διεύθυνση προορισμού και ο Προσδιορισμός Ροής.

4.5 Ενθυλάκωση Φορτίου Ασφαλείας

Το ενθυλακωμένο φορτίονασφαλείας παρέχει υπηρεσίες εμπιστευτικότητας τόσο των περιεχομένων του μηνύματος όσο και της ροής της κίνησης.Η μορφή ενός πακέτου ESP παρέχει τα ακόλουθα πεδία:

- **Κατάλογος παραμέτρων ασφαλείας (32 bit):**Προσδιορίζει μια σχέση ασφαλείας
- **Αριθμός ακολουθίας (32 bit) :Μια μονοτονική αυξανόμενη τιμή** μετρητή
- **Φορτίο δεδομένων**:Είναι ένα μεταβλητό τεμάχιο επιπέδου μεταφοράς ή πακέτο IP που προστατεύεται με κρυπτογράφηση
- **Συμπληρώματα (0-255 Byte):**Μπορεί να απαιτείατι εάν ο αλγόριθμος κρυπτογράφησης απαιτεί το μη κωδικοποιημένο κείμενο να είναι πολλαπλάσιο κάποιου αριθμού από οκτάδες.
- **Μήκος συμπλήρωσης(8 Bit):**Προσδιορίζει τον αριθμό των byte συμπλήρωσης αμέσως πριν αυτό το πεδίο.
- **Επόμενη επικεφαλίδα(8 bit):**Προσδιορίζει τον τύπο των δεδομένων που περιέχονται στο πεδίο φόρτο δεδομένων.
- **Δεδομένα πιστοποίησης**:Μεταβλητό πεδίο που περιέχει την τιμή ελέγχου ακεραιότητασπου υπολογίστηκε επί του πακέτου ESP.
-

4.6 Διαχείριση Κλειδιού

Το τμήμα διαχείρισηςκλειδιού του ISPsec περιλαμβάνει τον προσδιορισμό και την κατανομή των μυστικών κλειδιών.Το έγγραφο της Αρχιτεκτονικής του IP sec διευθύνει υποστήριξη για δύο τύπους κλειδιού:

- **Χειροκίνητη:** Ένας διαχειριστής του συστήματος ρυθμίζει χειροκίνητα κάθε σύστημα με τα δικά του κλειδιά και με τα κλειδιά αάλλων επικοινωνούντων συστημάτων
- **Αυτοματοποιημένη:**ένα αυτοματοποιημένο σύστημα επιτρέπει την επί ζήτησης δημιουργία κλειδιών για Sas και διευκολύνει τη χρήση των κλειδιών σες ένα μεγάλο κατανεμημένο σύστημα με μια αναπτυγμένη διάταξη.
- **Πρωτόκολλο προσδιορισμού κλειδιού Oakley:**Το Oakley είναι ένα πρωτόκολλο ανταλλαγής κλειδιού βασισμένο στον αλγόριθμο Diffie-Hellman ,αλλά παρέχει επιπρόσθετη ασφάλεια.Συγκεκριμένα ο αλγοριθμός αυτός δεν πιστοποιεί μόνος του τους δύπ χρήστες που ανταλλάσουν κλειδιά,κάνοντας το πρωτόκολλο ευπρόσβλητο στην προσωποποίηση.
- **Πρωτόκολλο σχέσης Ασφάλειας διαδικτύου και Διαχείρισης Κλειδιού**
- **(ISAKAMP):**Το ISAKAMP παρέχει ένα πλαίσιο διεργασίας για διαχείριση κλειδιού διαδικτύου και παρέχειν την ειδική υποστήριξη πρωτοκόολου περιλαμβάνοντας τις διατάξεις,για διαπραγμλατευση των χαρακτηριστικών ασφαλείας.

5- ΕΠΙΘΕΣΕΙΣ ΣΤΑ ΔΙΚΤΥΑ

Οι επιθέσεις στα δίκτυα χωρίζονται σε τρεις κατηγορίες. Επιθέσεις κατά της διεύθυνσης: αυτές οι επιθέσεις στοχεύουν στο να υποκλέψει ή να προσποιηθεί μια διεύθυνση ένας κακόβουλος κόμβος, επιθέσεις κατά άλλων κόμβων του δικτύου. Αυτές οι επιθέσεις στοχεύουν στο να υπερφορτώσουν κάποιο κόμβο του δικτύου έτσι ώστε να μη μπορεί να διαχειριστεί το φόρτο και ως αποτέλεσμα να τον καταστήσει άχρηστο. Επιθέσεις κατά Binding Update: Αυτές οι επιθέσεις στοχεύουν στις πηγές των κόμβων που επικοινωνούν με τον κόμβο θύμα ή και τον ίδιο τον κόμβο θύμα. Οι επιθέσεις γενικά έχουν ως σκοπό είτε να υποκλέψουν πληροφορία (attack to confidentiality), είτε να την αλλάξουν(attack to message integrity), ακόμη και να παρεμποδίσουν την επικοινωνία.

5.1 Επιθέσεις κατά της διεύθυνσης

5.1.1 Κλοπή διεύθυνσης κόμβου (address stealing of node)

Ο πιο προφανής κίνδυνος για ένα δίκτυο είναι η προσποίηση ενός επιτιθέμενου ο οποίος είναι ένας κόμβος εγγεγραμμένος στο δίκτυο. Αυτό γίνεται με το να εμφανίσει τη διεύθυνση του άλλου ως δική του και να κλέψει την ροή των δεδομένων που προορίζονταν για τον άλλον. Αυτό γενικά είναι εφικτό με πλαστό binding update για την αλλαγή του “care of address” του κόμβου. Με απλά λόγια αλλαγή της διεύθυνσης αποστολής των πακέτων στον home agent και ως επέκταση της ροής τους. Στη πιο απλή του μορφή δηλαδή, χωρίς να υπάρχει κάποιου είδους πιστοποίηση των binding updates αρκεί να γίνει από οποιονδήποτε ένα binding update με πλαστά στοιχεία και αυτομάτως αλλάζει η ροή της πληροφορίας προς τον επιτιθέμενο.

Σε αυτό τον τύπο ο επιτιθέμενος πρέπει να ξέρει ή να υποθέσει τις διευθύνσεις IP και τις πηγές των πακέτων που εκτρέπονται και του προορισμού των πακέτων. Αυτό σημαίνει ότι είναι δύσκολο να επαναπροσανατολιστούν όλα τα πακέτα σε ή από έναν συγκεκριμένο κόμβο επειδή ο επιτιθέμενος θα πρέπει να ξέρει τις διευθύνσεις IP όλων των κόμβων με τους οποίους επικοινωνεί.

Οι κόμβοι με τις γνωστές διευθύνσεις, όπως οι server και εκείνοι που χρησιμοποιούν stateful configuration, είναι περισσότερο τρωτοί. Κόμβοι που είναι μέρος της υποδομής δικτύου, όπως DNS, είναι ιδιαίτερα ενδιαφέροντες στόχοι για τους επιτιθεμένους και ιδιαίτερα εύκολο να προσδιοριστούν. Οι κόμβοι που αλλάζουν συχνά τις διευθύνσεις τους είναι σχετικά ασφαλείς. Εντούτοις, εάν καταχωρούν την IP τους στο DNS, είναι και αυτοί εκτεθειμένοι. Το IPv6 εξετάζοντας τα χαρακτηριστικά γνωρίσματα της επίθεσης μετριάζει αυτούς τους κινδύνους.

Γενικά είναι δυνατόν να κλαπεί η διεύθυνση ενός stationary node του δικτύου εάν αρχικά μπορέσουμε να απομονώσουμε τον stationary node με κάποια επίθεση denial-of-service και στη συνεχεία προσποιηθεί ο επιτιθέμενος ότι είναι ο απομονωμένος stationary node.

5.1.2 Κλοπή μελλοντικής διεύθυνσης κινητού κόμβου (Future Stealing Addresses)

Όπως καταλαβαίνουμε και από τον τίτλο, η επίθεση αυτή στοχεύει τις μελλοντικές διευθύνσεις που μπορεί να πάρει ένας κόμβος ο όποιος αποτελεί το στόχο αυτής της επίθεσης. Ένας επιτιθέμενος μπορεί να έχει τη δυνατότητα να μαντέψει ή να γνωρίζει ποια διεύθυνση θα υιοθετήσει ο κόμβος-στόχος. Είναι εφικτό να γίνει αυτού του είδους η επίθεση εάν ο home agent του δικτύου επιτρέπει τη δυναμική δέσμευση διευθύνσεων από τους κινητούς κόμβους. Με τη διεύθυνση της πρόβλεψης ο επιτιθέμενος δημιουργεί μια

εγγραφή στο Binding Cache με αυτή τη διεύθυνση στο home address του επιτιθέμενου. Η εγγραφή της διεύθυνσης στο Binding Cache ενόσω είναι σε ισχύ, ο επιτιθέμενος και ο κόμβος στόχος θα έχουν την ιδία διεύθυνση. Αυτό δίνει τη δυνατότητα στον επιτιθέμενο να διαπράξει τις επιθέσεις man in the middle και denial of service.

5.1.3 Man in the middle (Επίθεση του ενδιάμεσου κόμβου)

Η επίθεση αυτή έχει ως στόχο να την κλοπή ή και την αλλαγή πληροφοριών μεταξύ της επικοινωνίας ενός κινητού κόμβου με κάποιον Home Agent. Επιτυγχάνεται με το να στείλει ο επιτιθέμενος δυο binding updates, ένα στον κινητό κόμβο-στόχο και ένα στον agent με τον όποιο επικοινωνεί. Αυτό πρέπει να γίνει με τέτοιο τρόπο ώστε να αλλάξει τη ροή της πληροφορία που ανταλλάσουν μεταξύ τους με τέτοιο τρόπο ώστε να γίνει ένας αναμεταδότης τους. Με αυτό τον τρόπο θα έχει πρόσβαση στο περιεχόμενο των μηνυμάτων τους.

5.2 Denial of service (Άρνηση παροχής υπηρεσίας)

Η απλούστερη μορφή επιθέσεως ονομάζεται denial of service (παλιά την αποκαλούσαν ping of death) και συνίσταται στην αποστολή πάρα πολλών "νόμιμων" αιτημάτων προς το δίκτυο του θύματος. Για παράδειγμα, αν ο δεχόμενος την επίθεση έχει ένα web site (όπως συνέβη στην περίπτωση των Yahoo!, Amazon, eBay, CNN και άλλων) ο επιτιθέμενος του αποστέλλει διαρκώς από πλαστές διευθύνσεις αιτήματα λήψης web σελίδων. Για να ικανοποιήσει αυτά τα αιτήματα ο web server είτε προσπαθεί να στείλει web σελίδες σε παραλήπτες που δεν τις ζήτησαν, είτε τις στέλνει σε διευθύνσεις που δεν υπάρχουν. Και στις δύο περιπτώσεις οι σελίδες δεν παραδίδονται ποτέ (ο web server καταλαβαίνει το λάθος του και σταματά την αποστολή). Το σύστημα όμως καταναλώνει μεγάλα ποσά υπολογιστικής ισχύος και bandwidth στην προσπάθειά του να παραδώσει τις σελίδες και να καταλάβει τι συμβαίνει. Αν λοιπόν τα ψεύτικα αιτήματα που λαμβάνει είναι πάρα πολλά, τότε το σύστημα υπερφορτώνεται και παύει πλέον να λειτουργεί ή καθυστερεί πάρα πολύ να εξυπηρετήσει ένα "νόμιμο" αίτημα διότι είναι απασχολημένο με την διαχείριση όλων των πλαστών αιτημάτων τα οποία λαμβάνει συνεχώς. Όπως φαίνεται από την παραπάνω περιγραφή, οι επιθέσεις αυτής της μορφής δεν κλέβουν δεδομένα ούτε επιτρέπουν στον επιτιθέμενο να αποκτήσει τον έλεγχο του εξοπλισμού μιας επιχείρησης. Απλώς δεν επιτρέπουν στο θύμα να εξυπηρετήσει τους πελάτες και τους συνδρομητές του (γι' αυτό και ονομάζονται denial of service). Αυτή η ιδιαιτερότητα όμως δεν τις καθιστά λιγότερο επίφοβες. Το πρόβλημα με τις επιθέσεις denial of service είναι πως δεν υπάρχει ακόμη κάποιος απλός και αποτελεσματικός τρόπος προστασίας από αυτές. Συνήθως, ο επιτιθέμενος αποστέλλει τα αιτήματά του από πολλά μηχανήματα μέσα στο δίκτυο (distributed denial-of-service ή DDS), κρύβοντας έτσι τα ίχνη του και κάνοντας πολύ δύσκολη την αναγνώριση μιας επίθεσης denial of service μέχρι να είναι αργά (επειδή είναι πολύ δύσκολο να καταλάβει κανείς ότι τα αιτήματα που λαμβάνει είναι πλαστά, ο συναγερμός δεν δίνεται παρά μόνο όταν το δίκτυο δέχεται πλέον τόσο μεγάλο όγκο αιτημάτων που σχεδόν παύει να λειτουργεί). Δυστυχώς, το πρωτόκολλο IP version 4 που χρησιμοποιούμε αυτή τη στιγμή δεν επιτρέπει την εύκολη αποκάλυψη του πραγματικού αποστολέα κάθε πακέτου δεδομένων. Το πρόβλημα αυτό θα λυθεί πλήρως μόνο με την υιοθέτηση του νεότερου πρωτοκόλλου IP version 6 (IPv6) το οποίο διαθέτωντας εξαιρετικά μεγάλο αριθμό IP διευθύνσεων έχει ως αποτέλεσμα κάθε συσκευή και κάθε χρήστης να έχουν μια αποκλειστικά δική τους διεύθυνση, καθιστώντας εξαιρετικά δύσκολη οποιαδήποτε πλαστοπροσωπία. Ωστόσο, αυτή η λύση δεν φαίνεται να αρέσει σε πολλούς, καθώς (παρά την ενσωματωμένη κρυπτογράφηση που διαθέτει) το IPv6 καταργεί πλήρως την ανωνυμία του δικτύου και κάνει εφικτή την παρακολούθηση όλων των δραστηριοτήτων

οποιουδήποτε χρήστη. Έτσι μια δικτατορική κυβέρνηση (π.χ. Κίνα, Ιράκ, Βόρεια Κορέα κ.λπ.) δεν θα χρειάζεται να ανησυχεί πλέον για τις επιπτώσεις της ανωνυμίας του δικτύου αφού θα μπορεί να παρακολουθεί με άνεση τις online κινήσεις όλων των κατοίκων της.

5.3 Επανάληψη και παρεμπόδιση των Binding Updates (Replaying and Blocking Binding Updates)

Στόχος αυτής της επίθεσης είναι τα δίκτυα που χρησιμοποιούν σύστημα πιστοποίησης για τα binding update. Ο επιτιθέμενος είναι σε θέση να καταγράψει τα πιστοποιημένα binding update. Εφόσον ο κινητός κόμβος – στόχος αλλάξει Agent, ο επιτιθέμενος επαναλαμβάνει τη διαδικασία με τα κλεμμένα και πιστοποιημένα binding update. Έτσι, με αυτόν τον τρόπο, παίρνει τη προηγούμενη θέση του κινητού κόμβου – στόχου και αναπροσαρμόζει τη ροή της πληροφορία προς αυτή. Με αυτό τον τρόπο μπορεί να προκαλέσει τις επιθέσεις denial of service και κλοπής πακέτων ακόμα και να προσποιηθεί ο επιτιθέμενος ότι είναι ο κινητός κόμβος.

Μια παραλλαγή της επίθεσης αυτής είναι το ότι ο επιτιθέμενος παρεμποδίζει τα binding update του κινητού κόμβου από την καινούρια του θέση. Αυτό είναι εφικτό με το να μορφή αυτής της επίθεσης ο επιτιθέμενος καλεί ένα μεγάλο όγκο πληροφορίας προς το μέρος του και έπειτα τον ανακατευθύνει προς το στόχο με ένα binding update. Για να συνεχιστεί η ροή της πληροφορίας προς το στόχο και να μη διακοπεί λόγω μη αποστολής acknowledgments (εφόσον τα πακέτα δε του έρχονται από δική του κλήση), ο επιτιθέμενος στέλνει πλαστά acknowledgments.

Return-to-Home Flooding

Μια παραλλαγή του παραπάνω είναι ο στόχος της επίθεσης να είναι ο home agent ή το οικείο δίκτυο (ή κάποιο δίκτυο το όποιο επισκέφθηκε ο στόχος) αντί ο στόχο να είναι ο κινητός κόμβος. Θα μπορούσε απλά να ανακατευθύνει τη δεδομένα προς τη διεύθυνση του δικτύου και να στέλνει acknowledgments. Αλλιώς, ο επιτιθέμενος θα μπορούσε να ισχυριστεί ότι είναι ένα κόμβος με διεύθυνση ίδια με τη διεύθυνση του δικτύου-στόχου. Ενόσω ο επιτιθέμενος στέλνει πλαστά μηνύματα ότι είναι εκτός οικείου δικτύου, θα άρχιζε να καλεί μεγάλα stream δεδομένων με στόχο το δίκτυο. Τέλος θα μπορούσε να κατακλείσει τον agent με πλαστά binding updates.

5.3.1 Επιθέσεις κατά Binding Update

Unnecessary Binding Updates

Όταν ένας κινητός κόμβος λαμβάνει ένα πακέτο από ένα νέο correspondent node μέσω του home agent, τότε μπορεί να κάνει ένα binding update. Ένας επιτιθέμενος μπορεί να το εκμεταλλευτεί αυτό και να στέλνει πλαστά πακέτα που να φαίνεται ότι προέρχονται από ένα νέο correspondent node. Έτσι, ο home agent μπορεί να ξεκινήσει να κάνει binding updates για κάθε νέο (πλαστό) correspondent node. Η λήψη απόφασης για την εγγράφη των binding updates μπορεί να εξαρτάται από πολλούς παράγοντες. Η μη καταγραφή των binding update μπορεί να μετριάσει τις επιθέσεις αυτές, αλλά δεν θα τις σταματήσει εντελώς. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να προκαλέσει την κατασπατάληση των πόρων.

Reflection attack

Είναι μια παραλλαγή του flooding attack αλλά αντί ο επιτιθέμενος να στέλνει τη ροή πληροφοριών απευθείας στον στόχο και να τον κατακλίσει από το φόρτο προκαλώντας

denial of service, ξεγελά και αναγκάζει ένα τρίτο κόμβο να στείλει τη ροή στο κόμβο. Με αυτό τον τρόπο δεν είναι εύκολα εφικτό στο να ανακαλύψει κάποιος τον πραγματικά επιτιθέμενο αφού κάνει την επίθεση έμμεσα. Η επίθεση αυτή είναι πιο επικίνδυνη αν με ένα σήμα του επιτιθέμενου προς τον τρίτο κόμβο, τον αναγκάζει να στείλει πολλαπλά πακέτα. Σε αυτή την επίθεση εύκολα μπορούν να γίνουν στόχοι οι agent του συστήματος, διότι μπορεί ο επιτιθέμενος να αναγκάσει τον τρίτο κόμβο να στείλει τα πακέτα σε ένα κόμβο όπου για να γίνει εφικτό αυτό θα πρέπει τα πακέτα να περάσουν έναν agent. Έτσι μπορεί να προκαλέσει μεγαλύτερης κλίμακας προβλήματα. Γενικά θεωρείται πολύ επικίνδυνος τύπος επίθεσης.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το IPv6 είναι το επόμενο επίπεδο των IPs. Από ότι φαίνεται η έκδοση 6, θα είναι κατά πάσα πιθανότητα το επόμενο ευρέως διαδεδομένο πρωτόκολλο Internet. Σε σύγκριση με το IPv4 το οποίο επιτρέπει μόνο 4.294.967.296 μοναδικές διευθύνσεις, το IPv6 που χρησιμοποιεί ένα σύστημα 128-bit που θα μπορεί να δώσει 340 - ενδεκάκις εκατομμύρια [undecillion] (34, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000 , 000) ο αριθμός αυτός είναι τόσο μεγάλος ώστε υπάρχουν πιο πολλές μοναδικές διευθύνσεις IP από τα αστέρια στο σύμπαν, όπως το γνωρίζουμε σήμερα. Ωστόσο, το IPv6 δεν θα βγει πριν το 2025, επειδή χρειάζονται χρόνο για να διορθωθούν τα σφάλματα στο πρωτόκολλο. Ένα παράδειγμα του IPv6 είναι:
207. 142. 131. 235. 207. 142. 131. 235. 207. 142. 131. 235. 207. 142. 131. 235.

Ο λόγος για τον οποίο χρειάζεται να μεταβούμε από IPv4 σε IPv6 είναι λόγω του πληθυσμού του κόσμου που μεγαλώνει ραγδαία καθώς και η αύξηση υπολογιστών laptop και desktop. Επίσης, στο μέλλον όλα τα οχήματα θα είναι πιθανώς δικτυωμένα για να χρησιμοποιείτε συσκευές πλοήγησης που θα έχουν την ανάγκη μιας IP. Έτσι, τελικά, θα χρειαζόμασταν περισσότερες διευθύνσεις IP από τον αριθμό που έχουμε τώρα με το πρωτόκολλο IPv4.

Το IPv6 σχεδιάστηκε επίσης για να διευκολύνει ορισμένα χαρακτηριστικά, των οποίων η έλλειψη ήταν αισθητή στο IPv4. Στα χαρακτηριστικά αυτά περιλαμβάνεται η ποιότητα της παρεχόμενης υπηρεσίας, η αυτοδύναμη διάρθρωση, η ασφάλεια και η κινητικότητα. Εν τω μεταξύ, ωστόσο, τα περισσότερα από τα χαρακτηριστικά αυτά έχουν ενταχθεί μέσα και γύρω στο αρχικό πρωτόκολλο v4. Ο μεγάλος όμως χώρος διευθύνσεων είναι αυτός που καθιστά το IPv6 ελκυστικό για μελλοντικές εφαρμογές, καθώς θα απλουστεύσει τον σχεδιασμό τους σε σύγκριση με το IPv4.

Τα οφέλη του IPv6 προκύπτουν, επομένως, προφανέστατα στις περιπτώσεις που μεγάλος αριθμός διατάξεων προϊόντων πρέπει να δικτυωθούν εύκολα και να καταστούν δυνητικά ορατά και απευθείας προσβάσιμα μέσω του Ίντερνετ. Μια μελέτη που χρηματοδοτήθηκε από την Επιτροπή κατέδειξε το δυναμικό αυτό σε σειρά τομέων της αγοράς, όπως οικιακά δίκτυα, διαχείριση κτιρίων, κινητές επικοινωνίες, αμυντικός τομέας και ασφάλεια, καθώς και αυτοκινητοβιομηχανία.

Η ταχεία και αποτελεσματική υιοθέτηση του IPv6 παρέχει στην Ευρώπη δυναμικό καινοτομίας και πρωτοπορίας στην προώθηση του Ίντερνετ. Άλλες περιφέρειες, ιδίως η ασιατική, έχουν ήδη εκδηλώσει ισχυρό ενδιαφέρον για το IPv6. Λόγου χάρη, ο ιαπωνικός κλάδος ηλεκτρονικών καταναλωτικών αγαθών αναπτύσσει διαρκώς περισσότερα προϊόντα που βασίζονται σε IP και αποκλειστικά για το IPv6. Ο ευρωπαϊκός κλάδος πρέπει επομένως να ανταποκριθεί σε μελλοντική ζήτηση για υπηρεσίες, εφαρμογές και συσκευές που βασίζονται σε IPv6 εξασφαλίζοντας έτσι ανταγωνιστικό πλεονέκτημα σε παγκόσμιες αγορές.

Το IPv6 όπως εξετάσαμε δεν είναι απευθείας διαλειτουργικό με το IPv4. Συσκευές IPv6 και IPv4 μπορούν να επικοινωνούν μεταξύ τους μόνο χρησιμοποιώντας ειδικές δικτυακές πύλες ανά εφαρμογή. Δεν πρόκειται για γενική και ανθεκτική στο χρόνο λύση όσον αφορά τη διαφανή διαλειτουργικότητα.

Το IPv6 μπορεί, ωστόσο, να ενεργοποιηθεί παράλληλα με το IPv4, στην ίδια συσκευή και στο ίδιο υλικό δίκτυο. Θα υπάρξει μια μεταβατική φάση (που αναμένεται να διαρκέσει 10, 20 ή και περισσότερα έτη) κατά την οποία το IPv4 και το IPv6 θα συνυπάρχουν στις ίδιες

συσκευές (η λύση αυτή αναφέρεται συχνά ως “dual stack” – διπλή στοίβα) και θα μεταδίδονται μέσω των ίδιων δικτυακών συνδέσμων. Εξάλλου, άλλα πρότυπα και τεχνολογίες (που ονομάζονται “tunnelling” – φαινόμενο σήραγγας/λαθροδιοχέτευση) παρέχουν σε δέσμες IPv6 την δυνατότητα μετάδοσης με χρήση μηχανισμών IPv4 για διευθυνσιοδότηση και δρομολόγηση και, τελικά, επιτρέπουν και την αντίστροφη κίνηση[13]. Τούτο παρέχει την τεχνική βάση για την βήμα προς βήμα εισαγωγή του IPv6.

Συνοψίζοντας, το κύριο πλεονέκτημα του IPv6 έναντι του IPv4 είναι ο τεράστιος και ευκολότερα διαχειριζόμενος χώρος διευθύνσεων. Το γεγονός αυτό επιλύει σήμερα και για μακρύ χρονικό διάστημα το μελλοντικό πρόβλημα της διάθεσης διευθύνσεων. Παρέχει την βάση για καινοτομία, ανάπτυξη και εισαγωγή υπηρεσιών και εφαρμογών που ενδεχομένως θα ήταν υπερβολικά περίπλοκες ή δαπανηρές σε περιβάλλον IPv4. Επίσης, ενισχύει την θέση των χρηστών, παρέχοντάς τους την δυνατότητα να διαθέτουν το δικό τους δίκτυο σε σύνδεση με το Ίντερνετ.

ΣΥΝΤΜΗΣΕΙΣ ΑΡΤΙΚΟΛΕΞΑ ΑΚΡΩΝΥΜΙΑ

IPV4	Internet Protocol version 4 (IPv4)
IPV6	Internet Protocol version 6 (Ipv6)
TTL	Time to live
NAT	Network Address Translation
MAC	Media Access Control address

ΑΝΑΦΟΡΕΣ

[1] DEPLOYING IPV6,Alain Durand,pp 83-85

[2] IPv6-to-IPv4 Transition And Security Issues Block K, Information Technology & State StoreBuilding,

Jalan Gadong pp 7-10

[3]Μετάβαση IPv4 στο IPv6-Μελέτη μηχανισμου 6 to 4,Δημήτριου Φιλλιπίδη

[4] Μελέτη των πρωτοκόλλων IPv6 και Mobile IPv6 και ανάπτυξη εφαρμογής με χρήση των προαναφερθέντων πρωτοκόλλων Γεώργιος Α. Φουντάς,Κωνσταντίνος Μ. Παγανέλης

[5] *Communication from the Commission to the European Parliament, the Council, the European Economicand Social Committee and the Committee of the Regions onAdvancing the Internet Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe,* European Economic and Social Committee