ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΣΔΟ

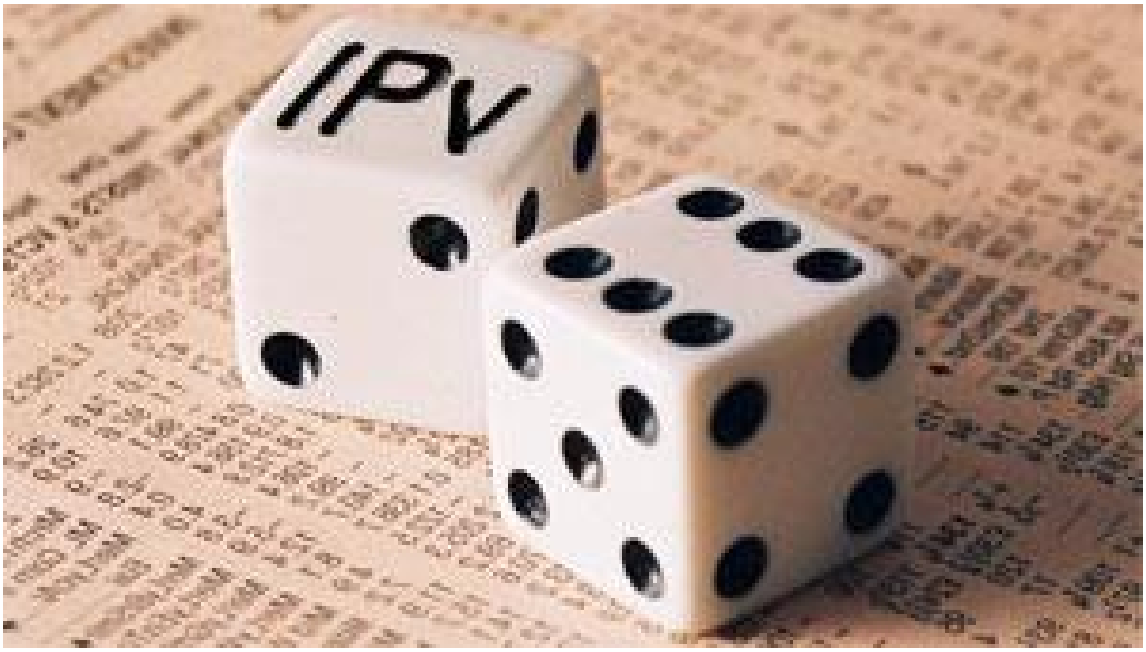
ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΩΤΩΝ

ΠΡΩΤΟΚΟΛΛΟ IPv6-ΠΑΡΟΥΣΙΑΣΗ-ΜΕΛΛΟΝΤΙΚΕΣ ΕΞΕΛΙΞΕΙΣ

Σπουδαστες : Καυκάς Γεώργιος

Μαυρομμάτης Θεόδωρος

Σελιμάς Ανάργυρος



ΜΑ'Ι'ΟΣ 2011

ΕΙΣΗΓΗΤΗΣ

Δαρσινός Βασίλειος

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ ΣΤΟ IPv6

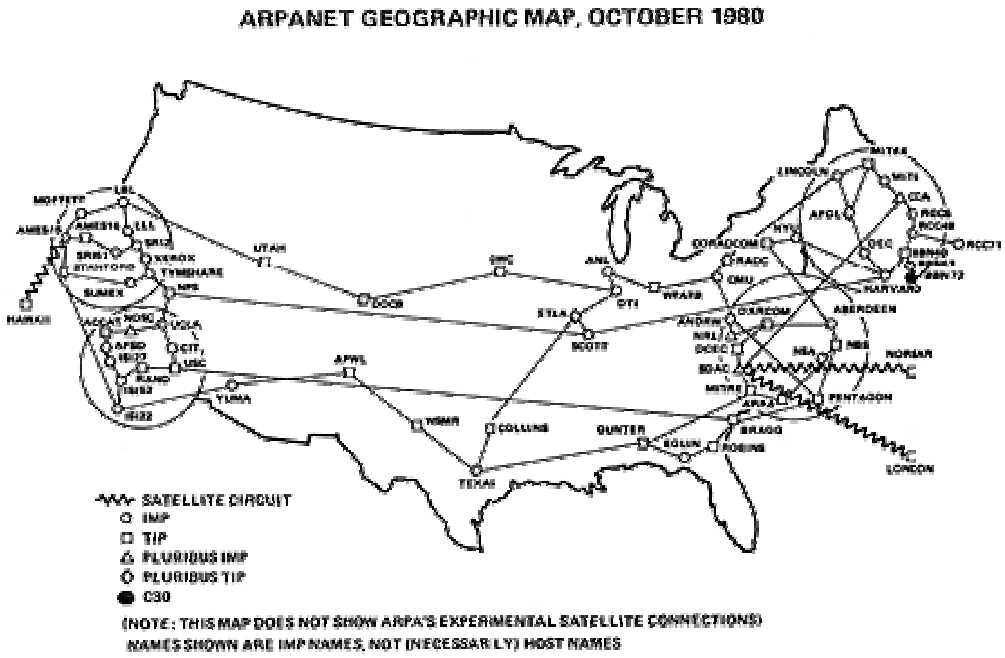
1.1 Η Γέννηση του διαδικτύου.

Ενώ οι υπολογιστές δεν ήταν μια νέα έννοια στη δεκαετία του 1950, υπήρχαν σχετικά λίγοι υπολογιστές σε λειτουργία και ο τομέας της επιστήμης της πληροφορικής ήταν ακόμα σε εμβρυικό επίπεδο. Οι περισσότερες από τις εξελίξεις στον τομέα οφείλονταν σε στρατιωτικές επιχειρήσεις κατά τη διάρκεια του Β 'Παγκοσμίου Πολέμου και ήταν στην πραγματικότητα οι δραστηριότητες της κυβέρνησης που οδήγησαν στην ανάπτυξη του Διαδικτύου.

Στις 4 Οκτωβρίου 1957, οι Σοβιετικοί εκτόξευσαν το Σπούτνικ, την πρώτη απόπειρα του ανθρώπου προς το διάστημα, και η αμερικανική κυβέρνηση υπό τον πρόεδρο Αϊζενχάουερ ξεκινήσει στη συνέχεια μια επιθετική στρατιωτική εκστρατεία για να ανταγωνιστεί και να ξεπεράσει τη Σοβιετική Ένωση. Το Advanced Research Projects Agency (ARPA) γεννήθηκε. Το ARPA ήταν οργανισμός για την έρευνα της κυβέρνησης των ΗΠΑ για όλο το διάστημα και της στρατηγικής έρευνας πυραύλων.

Το 1958, δημιουργήθηκε η NASA, έτσι η ARPA απομακρύνθηκε από την αεροναυτική και εστίασε κυρίως στην επιστήμη των υπολογιστών και επεξεργασίας πληροφοριών. Ένας από τους στόχους του ARPA ήταν να συνδέσει κεντρικούς υπολογιστές πανεπιστημίων όλης της χώρας έτσι ώστε να μπορούν να επικοινωνούν μεταξύ τους. Για να επιτευχθεί κάτι τέτοιο οι

υπολογιστές εντός του μεγάλου αυτού δικτύου θα έπρεπε να μιλούν την ίδια γλώσσα, ή αλλιώς να χρησιμοποιούν ένα **κοινό πρωτόκολλο επικοινωνίας** .Έτσι δημιουργήθηκε το ARPAnet το 1969, το πρώτο δίκτυο ευρείας περιοχής (WAN) που για μέσο μετάδοσης χρησιμοποίησε το τηλεφωνικό δίκτυο της εποχής. Βασική ιδέα του δικτυού αυτού ήταν η συνεχής και αδιάκοπη επικοινωνία μεταξύ των κόμβων. Ακόμα και αν μερικοί έβγαιναν εκτός λειτουργίας, το δίκτυο δεν κατέρρεε. Οι τεχνολογίες δρομολόγησης έκαναν την εμφάνιση τους.



Εικ 1.1 Το Αρχικό ARPAnet αυξήθηκε τελικά και έγινε το Internet.

Πηγή:

- http://www.webopedia.com/didyouknow/internet/2002/birthoftheinternet.asp

1.2 Η εξέλιξη του IPv4

Όταν οι ερευνητές τις εποχής , όπως ο όπως ο Vint Cerf και ο Bob Kahn, σχεδίαζαν το Transmission Control Protocol (TCP) σύντομα αντιληφθήκαν ότι θα έπρεπε να προσδιορίσουν τοποθεσίες έτσι ώστε να στέλνουν δεδομένα από το ένα σημείο στο άλλο. Όπως και στο τηλεφωνικό δίκτυο, χρειαζόταν ένα πρωτόκολλο που να επιτρέπει σε αριθμούς να προσδιορίζουν συγκεκριμένες συσκευές του δικτύου και να επινοήσουν μεθόδους για να δρομολογείται η κίνηση δεδομένων από μία συσκευή στην άλλη. Την λύση στα παραπάνω προβλήματα έφερε το Internet Protocol (IP) και η πρώτη σημαντική έκδοση του ήταν το IPv4 το οποίο χρησιμοποιείται μέχρι σήμερα.

Το IPv4 για πρώτη φορά κυκλοφόρησε το Σεπτέμβριο του 1981, και το 1985, ειδικές μέθοδοι χρησιμοποιήθηκαν για την υποδιαίρεση των δικτύων IP. Τα πρώτα δίκτυα υπολογιστών σχεδιάσθηκαν για τους ερευνητές να επικοινωνούν και να μοιράζονται ιδέες ταχύτατα, έτσι μεγάλα τμήματα των διευθύνσεων είχαν ανατεθεί στα πανεπιστήμια, ομάδες προβληματισμού και άλλες τέτοιες οργανώσεις. Κάθε μπλοκ διευθύνσεων χωρίστηκε σε δύο τμήματα, δικτύων και κόμβων. Δίκτυα είχαν διατεθεί σε κάθε οργανισμό που επιθυμούσε να συνεργαστεί και να ανταλλάσσει δεδομένα διαμέσου του πρώιμου διαδικτύου.

Ωστόσο, η κατανομή των διευθύνσεων ήταν ατελής. Όχι τόσο λανθασμένη όσο αφελής και ιδεαλιστική. Από τα 4,2 δισεκατομμύρια διευθύνσεις, των 32bit μεγέθους, φαινόταν πρακτικό να δώσει δεκάδες χιλιάδες διευθύνσεις σε μεγάλα ιδρύματα. Καθώς όλο και περισσότερες αιτήσεις είχαν υποβληθεί για επιπλέον δίκτυα και κόμβους, κατέστη προφανές ότι μια επίπεδη δομή των δικτύων και κόμβων ήταν ο μόνος τρόπος για να διαιρεθούν οι διαθέσιμες διευθύνσεις, δηλαδή θα χρειαζόταν κάποια βελτίωση. Η βελτίωση έγινε γύρω στο 1993, με αποτέλεσμα την σύγχρονη εκδοχή των διευθύνσεων του IP, όπως το γνωρίζουμε με τέσσερις ομάδες του ενός byte. (πχ. 255.255.255.255)

Το ενδεχόμενο ότι το Internet θα γίνει το World Wide Web γεμάτο κοινωνικά δίκτυα, κινητές συσκευές, οικιακές συσκευές και ασύρματα hotspots δεν το είχαν λάβει υπ’ όψιν τους οι ερευνητές όταν ίδρυσαν το IPv4. Όμως, αυτό

ακριβώς συνέβη. Το διαδίκτυο έχει ξεπεράσει τον αρχικό του στόχο και τώρα έχουμε την ανταλλαγή πληροφοριών με ταχύτητα φωτός. Αντί να πάτε σε μια βιβλιοθήκη για να μάθετε για το IPv4, μπορείτε απλώς να σερφάρετε στο Wikipedia, ή αντί να στείλετε σε κάποιον μια επιστολή απλά χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο. Βρήκαμε νέους και δημιουργικούς τρόπους για να αντιστοιχίσουμε IP διευθύνσεις στα πάντα, από τον προγραμματισμό του δορυφορικού αποκωδικοποιητή μας μέχρι το ξεκλείδωμα του αυτοκινήτου μας.

Το IPv4 έχει χρησιμοποιηθεί περισσότερο από ό, τι θα μπορούσαμε ποτέ να περιμένουμε με περισσότερες, πια, IP συσκευές από τις διαθέσιμες διευθύνσεις IPv4. Χρόνια πριν έχει προβλεφθεί ότι θα εξαντλούταν τελικά ο αριθμός διευθύνσεων που είναι διαθέσιμος. Λοιπόν, ο χρόνος έχει έρθει τελικά.Σηματοδοτώντας ένα ορόσημο στην ιστορία του Ίντερνετ. Τριάντα χρόνια μετά τη δημιουργία των πρώτων διευθύνσεων του διαδικτύου, το 2011, οι διαθέσιμες ηλεκτρονικές διευθύνσεις, που ήσαν περισσότερες από 4 δισεκατομμύρια, εξαντλήθηκαν και τώρα πρέπει να γίνει οργανωμένα η διεθνής μετάβαση σε ένα νέο σύστημα διευθύνσεων.

http://portal.kathimerini.gr/4dcgi/_w_articles_kathciv_1_04/02/2011_376661

Εικ. 1.2 Τελετή απόδοσης των τελευταίων πακέτων διευθύνσεων

Σε μια ειδική «τελετή» στο Μαϊάμι των ΗΠΑ στις 3 Φεβρουαρίου 2011 - σύμφωνα με τα πρακτορεία Ρόιτερ και Γαλλικό-, όπως άρμοζε στην περίσταση, ο διεθνής μη κερδοσκοπικός Οργανισμός ICANN που εποπτεύει την απόδοση και κατανομή των διαδικτυακών διευθύνσεων σε παγκόσμιο επίπεδο, παραχώρησε και τα τελευταία πέντε διαθέσιμα πακέτα διευθύνσεων (αριθμών IP) με βάση το υπάρχον πρωτόκολλο IPv4.

Επομένως, πώς θα υποστηρίξει τις συσκευές, τους ανθρώπους, τους διακομιστές, και τους δικτυακούς τόπους που πρέπει να επικοινωνούν μεταξύ τους; Ευτυχώς, η βιομηχανία της πληροφορικής έχει σχεδιάσει ένα πρωτόκολο για να παρακάμψει τον υπερπληθυσμό των διευθύνσεων IP. Το όνομα αυτού, ***IPv6***

1.3 Το IPv6

Το επίσημο όνομα του είναι IPv6 (Internet Protocol version 6) και έρχεται να δώσει λύση στο εμφανές πρόβλημα της έλλειψης διευθύνσεων που παρουσιάζει το IPv4 και όχι μόνο, γιατί λόγω του βελτιωμένου σχεδιασμού του καθορίζει μία ομάδα από υπηρεσίες όπως ασφάλεια, υψηλή απόδοση, εύκολη διευθέτηση(configuration), δημιουργώντας με αυτό το τρόπο ένα πιο αξιόπιστο δίκτυο με λιγότερο διαχειριστικό βάρος. Όμως η πραγματική πρόκληση για το IPv6 είναι για το εάν θα επιτύχει να ‘δέσει’ το περιβάλλον του επερχόμενου δικτύου όπου εκτός από τους συμβατικούς υπολογιστές θα αποτελείται από μυριάδες άλλες συσκευές. Η επιτυχία του IPv6 θα βασιστεί όμως και στη δυνατότητα του να εντάξει το παλιό στο καινούργιο. Είναι γνωστό το μέγεθος που έχει ήδη το Διαδίκτυο και η μετάβαση από το IPv4 στο IPv6 δεν είναι απλή υπόθεση αλλά απαιτεί σωστή στρατηγική έτσι ώστε να παραμείνει αδιάλειπτη και αποδοτική η λειτουργία του Διαδικτύου.

Πηγή:

- http://www.webopedia.com/didyouknow/internet/2002/birthoftheinternet.asp (Posted: 06-24-2010 , Last Updated: 06-24-2010 author:unknown)
- http://www.ipv6-taskforce.gr/ (Ελληνικής Ομάδας Δράσης IPv6, Τετάρτη, 8 Ιουνίου 2011)
- http://en.wikipedia.org/wiki/IPv4#Address_representations/(From Wikipedia, 20 June 2011)
- http://www.alertlogic.com/the-history-of-ipv4/(2, Feb 2011 by Eric Irvin)
- http://portal.kathimerini.gr/4dcgi/_w_articles_kathciv_1_04/02/2011_376661 (*04-02-11*, από Καθημερινή με πληροφορίες από ΑΠΕ-ΜΠΕ)

ΚΕΦΑΛΑΙΟ 2. ΣΥΓΚΡΙΣΗ IPv6 ΜΕ IPv4

2.1 Πλεονεκτήματα IPv6

Εισαγωγή

Τα οφέλη του νέου πρωτοκόλλου είναι πολλά. Τα σημαντικότερα εν συντομία είναι: 1) Το μεγαλύτερο εύρος διευθύνσεων, από 2^{32} που είχαμε στο IPv4 , σε 2^{128}.2)Μεγαλύτερη ασφάλεια, χάρη στη μορφή αυθεντικοποίησης και κρυπτογραφίας. 3) Ποιότητα υπηρεσίας, με ετικέτες ροών δεδομένων. 4)Αυτόματη ρύθμιση συσκευών κατά τη σύνδεση στο δίκτυο κερδίζοντας με αυτό τον τρόπο πολύτιμο χρόνο. 5)Καλύτερη υποστήριξη μετακινούμενων συσκευών και χρηστών. 6)Ενσωματώνει καλές πρακτικές και αναιρεί τις μη χρησιμοποιούμενες, από το IPv4. 7)Βελτιώνει το σύστημα διευθύνσεων και ιεραρχία δρομολόγησης. 8) από τα πολύ σημαντικά πλεονεκτήματα είναι ότι έχει σχεδιαστεί με τέτοιο ώστε να είναι επεκτάσιμο. Όταν η IETF έθεσε ως στόχο να δημιουργήσει «IPng», το Internet Protocol επόμενης γενιάς, εκμεταλεύτηκε την ευκαιρία να βελτιώσει την IPv4, όπου είναι δυνατόν.

2.1.1.Μεγαλύτερος χώρος διευθύνσεων

Με διαφορά πιο μεγάλο πλεονέκτημα της καινούριας έκδοσης του IP είναι ο πολύ μεγαλύτερος αριθμός διευθύνσεων. Ο αριθμός διαθέσιμων διευθύνσεων για την τωρινή έκδοση του πρωτοκόλλου είναι:

4.294.967.296

Ο ακριβής αριθμός διευθύνσεων για το IPv6 είναι:

340.282.366.920.938.463.463.374.607.431.768.211.456 (128 bit)

Αυτός ο χώρος διευθύνσεων είναι αρκετά μεγάλος ώστε να αντιστοιχεί σε **155.000.000.000** 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. Με το μεγαλύτερο χώρο διευθύνσεων τεχνικές, όπως η NAT (Network Address Translators) δεν χρειάζονται πλέον. Αυτό επιτρέπει ολοκληρωμένη παγκόσμια IP συνδεσιμότητα για IP-based μηχανές αλλά και νέες κινητές συσκευές όπως κινητά τηλέφωνα και PDAs. Μπορούν να υπάρχουν πολλαπλές διευθύνσεις για μια μόνο διεπαφή όπου οι διευθύνσεις μπορούν να χρησιμοποιηθούν για διαφορετικές λειτουργίες. Ο μεγάλος χώρος διευθύνσεων επιτρέπει απλούστερη από άκρο σε άκρο ασφάλεια, απλοποιημένο IPv6 renumbering μηχανισμό, ξεχωριστή διευθυνσιοδότηση και δρομολόγηση.

2.1.2 Καινοτομία

Ένας λόγος για τον οποίο οι διευθύνσεις IPv4, δεν εξαντλούνται τόσο γρήγορα, όπως αναμενόταν πριν από 10 χρόνια είναι επειδή τα περισσότερα IP συστήματα χρησιμοποιούν σήμερα ιδιωτικό χώρο διευθύνσεων και για να συνδεθούν με το Internet χρησιμοποιούν την τεχνική Network Address Translation (NAT). Ωστόσο, η τεχνολογία NAT είναι ένα δίκοπο μαχαίρι. Για κλασσικες εφαρμογές 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 «ανεξάρτητος» 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 αριθμό διευθύνσεων κάθε Η/Υ μπορεί να έχει τη δική του διεύθυνση.

2.1.3 Αυτορρύθμιση διεύθυνσης (StatelessAutoconfiguration)

Στο IPv4 χρησιμοποιούνταν το πρωτόκολλο DHCP για να λάβει 1 μηχάνημα αυτόματα IP διεύθυνση. Αυτό έχει δύο μεγάλα μειονεκτήματα: Πρώτον το ότι χρειαζεται ένα DHCP server και δεύτερον δεν υπάρχει εγγύηση ότι το ίδιο μηχάνημα θα λάβει την ίδια διεύθυνση(εκτός και γίνει σωστή ρύθμιση με αντιστοίχηση στους MAC διεύθυνσής του).

Στο IPv6 υπάρχει μεν μια ανανεωμένη έκδοση του DHCP το DHCPv6 αλλά υπάρχει και άλλη επιλογή για την αυτόματη ρύθμιση των διευθύνσεων, 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 στους 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.

2.1.4 Εύκολη αλλαγή διεύθυνσης (Renumbering)

Διαφορετικό από το IPv4,το IPv6 μας επιτρέπει να ορίσουμε περισσότερες από μία διευθύνσεις σε ένα ενιαίο περιβάλλον την ίδια στιγμή. Μαζί με το Stateless Autoconfiguration αυτό καθιστά εφικτή την αλλαγή διεύθυνσης IPv6 σε ένα δίκτυο χωρίς κανένα “downtime”.Στη θεωρία αυτό ακούγεται αρκετά απλό. Στην πράξη όμως η διαδικασία της αρίθμησης απαιτεί λίγο προγραμματισμό και προσπάθεια στην ουσία όμως αυτό γινεται ομαλά και χωρίς διακοπή της υπηρεσίας. Υποθέτουμε ότι θέλουμε να αντικαταστήσουμε ένα πρόθεμα με ένα άλλο, διατηρώντας τα αναγνωριστικά δευτερεύοντος δικτύου και διεπαφή αμετάβλητη.

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.

2.1.5 Αποδοτικότητα

Μετά από δύο δεκαετίες χρήσης του IPv4 έχει αποκομιστεί αρκετή εμπειρία στο ποια χαρακτηριστικά είναι χρήσιμα και ποια όχι στο IPv4 και ποια λειτουργούν ως ρυθμιστές της ταχύτητας. Στο IPv6 έχουν ενσωματωθεί αυτές οι βελτιώσεις και πράγματι έχει πολύ καλύτερη απόδοση.

Παρ' όλο που τώρα τα πεδία διευθύνσεων είναι τέσσερις 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:

1. Η επικεφαλίδα του IPv6 έχει σταθερό μήκος
2. Η επικεφαλίδα του IPv6 είναι βελτιστοποιημένη για επεξεργασία 64 bit τη φορά σε σχέση με τα 32 bit του IPv4.
3. Το checksum της επικεφαλίδας IPv4 που υπολογίζεται κάθε φορά που 1 πακέτο περνά από 1 δρομολογητή, αφαιρέθηκε από το IPv6.
4. Οι δρομολογητές δεν είναι υποχρεωμένοι να χωρίζουν 1 μεγάλο πακέτο σε μικρότερα κομμάτια και μπορούν απλά να στείλουν σήμα να τους έρχονται μικρότερα πακέτα.
5. 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.

2.1.6 Ποιότητα υπηρεσιών IPv6

Μετά από πολλά χρόνια εξέτασης από την παγκόσμια τηλεφωνία η στοίβα TCP / IP κρίθηκε κατώτερη από την στοίβα ISO / OSI επειδή η καλύτερη στρατηγική για την προώθηση των πακέτων κρίθηκε ακατάλληλη για υπηρεσίες «near-realtime» όπως η τηλεφωνία. Η IETF προσπάθησε να προσθέσει σαν λειτουργία την ποιότητα υπηρεσιών (Quality of Service - Ποιότητα Υπηρεσίας) στο IPv6 και να γίνει το IPv6 «near-realtime ικανό». Από τότε, το H.323 πρωτόκολλο έναρξης περιόδου λειτουργίας (SIP) και ιδιοκτησιακά πρωτόκολλα όπως το Skype έχουν αποδείξει ότι ακόμη και στο IPv4 χωρίς ποιότητα υπηρεσιών είναι "αρκετά καλή" για τις τηλεφωνικές υπηρεσίες. Επίσης, οι QoS δυνατότητες καθορίζονται, έτσι ώστε να μπορούμε να ρίξουμε μια ματιά σε αυτά έστω και αν οι υλοποιήσεις δεν είναι διαθέσιμες γενικώς.

Βέβαια κάθε IPv6 διαχειριστικό τμήμα (domain) πρέπει να αναπτύσσει ένα συνδιασμό από μηχανισμούς για την επίτευξη υπηρεσιών QoS. Η IETF έχει προτείνει διάφορα μοντέλα και μηχανισμούς για την επίτευξη QoS σε επίπεδο δικτύου που βρίσκουν εφαρμογή είτε στο IPv4 είτε στο IPv6. Τα πιο σημαντικά μοντέλα είναι:

Integrated services (IntServ): Στην περίπτωση αυτή πραγματοποιείται κράτηση πόρων (resource reservation), όπου οι πόροι του δικτύου διατίθενται με βάση τις ανάγκες των εφαρμογών και του χρήστη. Πιο συγκεκριμένα, για κάθε πελάτη που επιθυμεί κάποια ποιότητα υπηρεσίας γίνεται στο δίκτυο κράτηση πόρων ώστε να εξυπηρετούνται οι ανάγκες του. Για παράδειγμα αν ο χρήστης θέλει να προσπελαστεί πολυμέσα (βίντεο, μουσική κτλ) πρέπει βάση της ποιότητας υπηρεσιών να υπάρξει μεν κάποια καθυστέρηση αρχικά λόγω φόρτου, αναπαράγοντας δε χωρίς ενδιάμεσες διακοπές.

Differentiated Service Architecture (DiffServ - DS): Στην περίπτωση αυτή γίνεται διάκριση των πακέτων και παρέχεται προτεραιότητα σε ορισμένα από αυτά. Η κίνηση του δικτύου διαχωρίζεται και οι πόροι διανέμονται κατάλληλα με βάση τα κριτήρια αστυνόμευσης και διαχείρισης του εύρους ζώνης

(bandwidth). Προκειμένου να επιτευχθεί ποιότητα στην υπηρεσία, οι κατηγορίες (classifications) που έχουν μεγαλύτερες απαιτήσεις απολαμβάνουν προνομιακή μεταχείριση από το δίκτυο.

2.1.6.1 Η αρχιτεκτονική Integrated Service (IntServ)

Η IETF ανταποκρινόμενη στην απαίτηση για ανάπτυξη ολοκληρωμένων υπηρεσιών στο Διαδίκτυο, προχώρησε στην ανάπτυξη της αρχιτεκτονικής Ολοκληρωμένων Υπηρεσιών (Integrated Services architecture ή εν συντομία (IntServ). Η αρχιτεκτονική IntServ σχεδιάστηκε αρχικά για να παρέχει ένα σύνολο προεκτάσεων στο παραδοσιακό μοντέλο μετάδοσης «καλύτερης προσπάθειας» (best effort) του Διαδικτύου. Στόχος της ήταν να παρέχει κάποια ιδιαίτερη μεταχείριση σε ορισμένους τύπους κυκλοφορίας κίνησης και ένα μηχανισμό στις εφαρμογές ώστε αυτές να έχουν τη δυνατότητα να επιλέξουν ανάμεσα σε πολλά επίπεδα υπηρεσιών μετάδοσης.

Η βασική ιδέα της αρχιτεκτονικής IntServ είναι ότι δεν απαιτείται να τροποποιηθεί η βασική υποκείμενη αρχιτεκτονική του Διαδικτύου, αλλά αρκεί να προστεθούν κάποιες προεκτάσεις που θα παρέχουν υπηρεσίες πέρα από την παραδοσιακή υπηρεσία «καλύτερης προσπάθειας» (best effort). Η ομάδα εργασίας τον μοντέλου IntServ έχει εστιάσει στους εξής στόχους:

- Στον ξεκάθαρο καθορισμό των υπηρεσιών που θα παρέχονται..
- Στον καθορισμό των υπηρεσιών στο επίπεδο της εφαρμογής, του χρονοπρογραμματισμού των δρομολογητών του Διαδικτύου σχετικά με τη δέσμευση των δικτυακών πόρων, και των διασυνδέσεων των δρομολογητών μεταξύ τους.
- Στην ανάπτυξη απαιτήσεων εγκυρότητας στους δρομολογητές του Διαδικτύου για να εξασφαλίζεται η παροχή της κατάλληλης υπηρεσίας. Το Διαδίκτυο θα συνεχίσει να περιέχει ένα ετερογενές σύνολο δρομολογητών, να τρέχει διάφορα πρωτόκολλα δρομολόγησης και να χρησιμοποιεί διαφορετικούς αλγορίθμους δρομολόγησης. Για αυτό η ομάδα εργασίας πρέπει να θέσει κάποιες

απαιτήσεις στους δρομολογητές που θα εξασφαλίζουν ότι το Διαδίκτυο μπορεί να υποστηρίξει το νέο μοντέλο υπηρεσιών.

Ο όρος «Εγγύηση Ποιότητας Υπηρεσίας» (Quality of Service - QoS) στο περιβάλλον του IntServ αναφέρεται στη φύση της υπηρεσίας μετάδοσης πακέτων που παρέχεται από το δίκτυο, όπως αυτή χαρακτηρίζεται από παραμέτρους όπως το εύρος ζώνης, η καθυστέρηση μετάδοσης πακέτων και ο ρυθμός απώλειας πακέτων. Κόμβος του δικτύου θεωρείται κάθε συνιστώσα του δικτύου που χειρίζεται πακέτα δεδομένων και έχει τη δυνατότητα επιβολής ελέγχου ποιότητας υπηρεσίας στα δεδομένα που ρέουν διαμέσου της. Στους κόμβους συμπεριλαμβάνονται οι δρομολογητές, τα τελικά συστήματα και τα υποδίκτυα. Ένας IntServ-capable κόμβος είναι κόμβος του δικτύου που μπορεί να παρέχει μία ή περισσότερες υπηρεσίες του μοντέλου IntServ. Ένας IntServ-aware κόμβος είναι ένας κόμβος του δικτύου που υποστηρίζει τις συγκεκριμένες διασυνδέσεις που απαιτούνται από το μοντέλο αλλά που δεν μπορεί να παρέχει τη ζητούμενη υπηρεσία. Παρόλο που ένας IntServ-aware κόμβος δεν μπορεί να παρέχει καμία από τις υπηρεσίες QoS, μπορεί απλά να κατανοεί τις παραμέτρους της ζητούμενης υπηρεσίας και να απαντάει αρνητικά σε αυτές τις αιτήσεις.

Σημαντικό ρόλο στο μοντέλο IntServ παίζει η έννοια του ελέγχου των πόρων. Οι πόροι του δικτύου (π.χ. εύρος ζώνης) πρέπει να ελέγχονται ώστε να επιτευχθεί το επιθυμητό επίπεδο ποιότητας υπηρεσίας. Μια θεμελιώδης αρχή του μοντέλου IntServ είναι ότι η κυκλοφορία που διαχειρίζεται από αυτό το μοντέλο πρέπει να υπόκειται σε μηχανισμούς ελέγχου αποδοχής. Επίσης, εκτός από τον έλεγχο αποδοχής, το μοντέλο IntServ φροντίζει για ένα μηχανισμό δέσμευσης πόρων. Οι εφαρμογές πραγματικού χρόνου δεν μπορούν να ικανοποιηθούν χωρίς εγγυήσεις πόρων, και οι εγγυήσεις πόρων δεν μπορούν να γίνουν χωρίς δέσμευση πόρων. Για την υλοποίηση αυτού του μηχανισμού δέσμευσης πόρων χρησιμοποιείται ένα πρωτόκολλο, όπως το RSVP (Resource Reservation Setup Protocol). Σκοπός του πρωτοκόλλου αυτού είναι να αποτελεί το μέσο καθορισμού των πόρων του δικτύου που απαιτούνται για την επίτευξη της απαιτούμενης ποιότητας υπηρεσίας. Η λογική του RSVP είναι πως πρέπει, κατά μήκος όλης της διαδρομής που

ακολουθούν τα πακέτα, να γίνουν δεσμεύσεις πόρων σύμφωνα με ης ανάγκες της κάθε εφαρμογής. Η διαδικασία δέσμευσης πόρων είναι ακολουθιακή και ο πρώτος δρομολογητής στέλνει κατάλληλο μήνυμα στον επόμενο, όπου ζητά δέσμευση πόρων. Η διαδικασία αυτή εξελίσσεται μέχρι να φτάσει στον παραλήπτη, ο οποίος τότε στέλνει στην αντίθετη διαδρομή επιβεβαιώσεις κράτησης. Οι IntServ υπηρεσίες που έχουν προταθεί έως σήμερα είναι η Guaranteed, που είναι η πλησιέστερη δυνατή στα αφιερωμένα ιδεατά κυκλώματα (dedicated virtual circuits) και η Controlled Load, που είναι ισοδύναμη με την υπηρεσία καλύτερης προσπάθειας σε συνθήκες έλλειψης φόρτου.

2.1.6.2 Εισαγωγή στο πρωτόκολλο RSVP

Το RSVP (Resource ReSerVation Protocol) πρωτόκολλο αποτελεί μέρος μιας ευρύτερης προσπάθειας να αξιοποιηθεί η υπάρχουσα υποδομή του

Διαδικτύου προσφέροντας υποστήριξη για QoS στις υπηρεσίες. Το πρώτο RSVP χρησιμοποιείται από έναν κόμβο-χρήστη, προκειμένου να απαιτήσει από το δίκτυο συγκεκριμένη ποιότητα για ροη δεδομένων συγκεκριμένων εφαρμογών. Το RSVP χρησιμοποιείται από δρομολογητές ώστε αυτοί να μεταφέρουν τις συγκεκριμένες QoS απαιτήσεις σε όλους τους κόμβους του μονοπατιού της ροής των δεδομένων αλλά και να εξασφαλίσουν ότι όντως οι συγκεκριμένες απαιτήσεις πληρούνται.

Το RSVP αποτελεί ένα πρωτόκολλο για multicast και unicast σηματοδότηση το οποίο σχεδιάστηκε για την εγκατάσταση και τη συντήρηση σταθμών πληροφοριών σε κάθε δρομολογητή που βρίσκεται στο μονοπάτι μετάδοσης δεδομένων, κατά τη μετάδοση δεδομένων. Το RSVP επιτρέπει στον παραλήπτη να ζητήσει μία ορισμένη από άκρο σε άκρο ποιότητα υπηρεσίας. Οι εφαρμογές πραγματικού χρόνου χρησιμοποιούν το RSVP για να δεσμεύσουν τους απαραίτητους πόρους στους δρομολογητές κατά μήκος του μονοπατιού μετάδοσης, έτσι ώστε να είναι διαθέσιμη η απαιτούμενη χωρητικότητα όταν λάβει χώρα η μετάδοση των πολυμεσικών δεδομένων. Κατά συνέπεια, το RSVP είναι ένα πρωτόκολλο ελέγχου δικτύου που

καθιστά τις διαδικτυακές εφαρμογές ικανές να αποκτήσουν QoS χαρακτηριστικά. Το RSVP καταλαμβάνει τη θέση ενός πρωτοκόλλου μεταφοράς στο μοντέλο OSI των 7 επιπέδων, παρόλο που το ίδιο το RSVP δεν μεταφέρει τα δεδομένα.

Για τη μετάδοση δεδομένων πολυμέσων πάνω από ένα δίκτυο είναι αναγκαίο να ικανοποιούνται τρία βασικά χαρακτηριστικά:

- Η μεταφορά των δεδομένων να γίνεται με όσο το δυνατόν πιο γρήγορο τρόπο.
- Να παρέχεται δυνατότητα multicast
- Να υπάρχει δυνατότητα για εξασφάλιση στη μεταφορά των δεδομένων με βάση τις απαιτήσεις που έχει ορίσει εκ των προτέρων ο χρήστης.

Τα δεδομένα πολυμέσων είναι μεγάλα σε όγκο και επομένως πρέπει να παρέχονται αποδοτικοί μηχανισμοί αποστολής τέτοιων δεδομένων. Το RSVP δείχνει περισσότερο ενδιαφέρον στη διατήρηση των παρεχόμενων πόρων και δεν μπορεί να επέμβει στη δρομολόγηση των δεδομένων που έχουν αποσταλεί.

Η πρώτη έκδοση του RSVP, που προέκυψε από τη συνεργασία μίας ομάδας ερευνητικών κέντρων, καθορίζεται από το RFC 2205 και η 1ETF έχει καταλήξει στην καθιέρωση των τεχνικών προδιαγραφών του πρωτοκόλλου σαν ένα Internet Proposed Standard.

Η παροχή Ποιότητας Υπηρεσίας, χρησιμοποιώντας το RSVP, υλοποιείται για μια συγκεκριμένη ροή δεδομένων με μηχανισμούς ελέγχου κυκλοφορίας, οι οποίοι είναι οι εξής:

- Έλεγχος Αποδοχής (Admission Control): Ο μηχανισμός ελέγχου αποδοχής αποφασίζει αν ο κόμβος μπορεί να ικανοποιήσει το απαιτούμενο επίπεδο QoS.

- Έλεγχος Πολιτικής (Policy Control): Ο μηχανισμός ελέγχου πολιτικής αποφασίζει αν ο χρήστης έχει την άδεια (π.χ. αν είναι διαχειριστής του δικτύου) να κάνει τη δέσμευση.
- Χρονοδρομολογητής Πακέτων (Packet Scheduler): Ο χρονοδρομολογητής πακέτων καθορίζει τη κλάση του QoS, και πιθανόν τη δρομολόγηση, για κάθε πακέτο. Ο packet scheduler είναι αυτός που επιτυγχάνει το επιθυμητό επίπεδο QoS.
- Ταξινομητής Πακέτων (Packet Classifier): Ο ταξινομητής πακέτων καθορίζει την κλάση QoS για κάθε πακέτο.

Οι μηχανισμοί του RSVP πρωτοκόλλου παρέχουν τη δυνατότητα δημιουργίας και συντήρησης κατανεμημένης δέσμευσης κατά μήκος ενός μεγάλου αριθμού multicast και unicast μονοπατιών. Το RSVP μεταφέρει και χειρίζεται τις παραμέτρους του QoS και του ελέγχου πολιτικής σαν απλά δεδομένα, μεταφέροντάς τα στις αντίστοιχες ρουτίνες (modules) του μηχανισμού για επεξεργασία. Καθώς είναι πολύ πιθανό η συμμετοχή σε μια multicast ομάδα να αλλάζει με την πάροδο κάποιου χρονικού διαστήματος, το RSVP υποστηρίζει, αν αυτό είναι επιθυμητό, την αποστολή περιοδικών μηνυμάτων προκειμένου να συντηρήσει την κατάσιαση σε όλα τα δεσμευμένα μονοπάτια.

Το RSVP πρωτόκολλο έχει τα παρακάτω χαρακτηριστικά:

- Η ροή δεδομένων στο RSVP είναι μονής κατεύθυνσης. Το πρωτόκολλο διαχωρίζει τους αποστολείς από τους παραλήπτες. Παρόλο που σε πολλές περιπτώσεις ο αποστολέας μπορεί να είναι και παραλήπτης, το RSVP δεσμεύει πόρους μόνο προς τη μία κατεύθυνση.
- Το RSVP υποστηρίζει και multicast και unicast και προσαρμόζεται στις συνεχείς αλλαγές ενός δυναμικού περιβάλλοντος. Δηλαδή, επιτρέπεται η δυναμική σύνδεση και αποσύνδεση παραληπτών σε multicast σύνοδο. Παρέχει πληθώρα μοντέλων και «μορφών» (styles) ώστε να εξυπηρετεί μεγάλη ποικιλία εφαρμογών. • Το RSVP είναι προσανατολισμένο προς τον αποδέκτη (receiver-

oriented) και μπορεί να χειριστεί διαφορετικές κατηγορίες παραληπτών. 0 κάθε παραλήπτης είναι υπεύθυνος για να διαλέξει το δικό του επίπεδο QoS. Ο αποστολέας διαχωρίζει την κίνηση σε ξεχωριστές ροές, μία για κάθε διαφορετικό επίπεδο QoS.

- Το RSVP είναι συμπληρωματικό του IP ελέγχοντας τον τρόπο με τον οποίο το IP μεταδίδει τα πακέτα του. Προορίζεται κυρίως για έλεγχο των δεδομένων που αποστέλλονται και όχι για μεταφορά δεδομένων. Είναι αναγκαίο να υπάρχει ενημέρωση για τους διαθέσιμους πόρους πριν γίνουν αλλαγές στη δρομολόγηση.
- Χρησιμοποιώντας το RSVP ένας αποστολέας δεν γνωρίζει ποιοι παραλαμβάνουν τα δεδομένα που αποστέλλει.
- Το RSVP έχει καλή συμβατότητα. Τρέχει πάνω από IPv4 και IPv6. Επίσης, λειτουργεί ακόμα και όταν ένας δρομολογητής στο μονοπάτι ροής δεδομένων δεν το υποστηρίζει με τη χρήση τεχνικής tunneling (απλά τα RSVP μηνύματα «περνάνε» χωρίς να υπόκεινται σε επεξεργασία).

2.1.6.3 Η αρχιτεκτονική Differentiated Service (DiffServ)

Το μοντέλο DiffServ αποτελεί τη δεύτερη σημαντική προσπάθεια για την παροχή εγγυήσεων ποιότητας υπηρεσίας (QoS) στο Διαδίκτυο. Το IntServ εμφάνισε αρκετά μειονεκτήματα, με κυριότερο αυτό της μη επεκτασιμότητας σε μεγάλα δίκτυα. Ο σκοπός της ομάδας εργασίας DiffServ της IETF ήταν να ορίσει το DS πεδίο στην επικεφαλίδα των IP πακέτων, αντικαθιστώντας το πεδίο TOS (στο IPv4) ή το πεδίο Traffic Class (στο IPv6).

Οι DiffServ υπηρεσίες χαρακτηρίζονται από το γεγονός ότι παρέχονται προς μία κατεύθυνση (unidirectional) και άρα είναι μη συμμετρικές. Η αρχιτεκτονική DiffServ μπορεί να χρησιμοποιηθεί μόνο για unicast μετάδοση και το μοντέλο δεν μπορεί ακόμα να υποστηρίξει multicast μετάδοση.

Περιληπτικά η λειτουργία του μοντέλου έχει ως εξής: Οι πελάτες ζητούν ένα συγκεκριμένο επίπεδο υπηρεσίας, μαρκάροντας το DS πεδίο του κάθε πακέτου με μια συγκεκριμένη τιμή. Η τιμή αυτή προσδιορίζει την ανά κόμβο συμπεριφορά του δικτύου (Per-Hop Behaviour - PHB) ως προς το πακέτο. Οι τιμές του DS πεδίου είναι μέσα στα πλαίσια της συμφωνίας ανάμεσα στον πάροχο και στον πελάτη

(Service Level Agreement - SLA) και ορίζουν τις παραμέτρους του επιπέδου υπηρεσίας, όπως το ρυθμό μετά- δόσης, την προτεραιότητα μετάδοσης και απόρριψης, την εξυπηρέτηση στην ουρά κ.ά.

Η λογική της αρχιτεκτονικής DiffServ είναι να αναγνωρίζει κάποιες ροές πακέτων και να τις διαχειρίζεται προνομιακά έναντι των υπολοίπων. Γενικά έχουν προταθεί 2 είδη DiffServ υπηρεσιών (per hop behaviors), που περιγράφονται παρακάτω. Με τον όρο per hop behavior εννοούμε τη συμπεριφορά προώθησης (forwarding behavior) που εφαρμόζεται στα πακέτα σε κάθε κόμβο του DiffServ διαχειριστικού τμήματος.

- Expedited Forwarding (EF): Σε αυτή την κατηγορία υπηρεσιών στόχος είναι η ελαχιστοποίηση της καθυστέρησης και της διακύμανσης καθυστέρησης (jitter), ενώ παράλληλα επιδιώκεται η παροχή ποιότητας υπηρεσίας στον υψηλότερο βαθμό. Τα πακέτα που υπερβαίνουν το προφίλ της κίνησης που έχει συμφωνηθεί ότι θα εισάγει ο χρήστης (στο SLA που υπογράφηκε) απορρίπτονται. Γενικά οι υπηρεσίες αυτής της κατηγορίες εξομοιώνουν τη λειτουργία μιας εικονικής μισθωμένης γραμμής.
- Assured Forwarding (AF): Η κατηγορία αυτή διαθέτει το πολύ 4 κλάσεις εξυπηρέτησης και το πολύ 3 επίπεδα απόρριψης για κάθε κλάση. Η AF κίνηση που υπερβαίνει τα χαρακτηριστικά διανέμεται με μικρότερη πιθανότητα απ' ό,τι η εντός προφίλ κίνηση, γεγονός που σημαίνει ότι μπορεί να υποβιβάζεται αλλά όχι απαραίτητα ότι απορρίπτεται.

Η λειτουργία της DiffServ αρχιτεκτονικής βασίζεται σε μια σειρά από μηχανισμούς οι οποίοι ενεργούν πάνω στις ροές:

- Ταξινόμηση των πακέτων (packet classification). Ο μηχανισμός αυτός ταξινομεί τα πακέτα που φτάνουν σε έναν κόμβο σε ροές ή συνενώσεις ροών ώστε στη συνέχεια αυτά να εξυπηρετηθούν κατάλληλα.

• Μαρκάρισμα (marking) των πακέτων. Με το μηχανισμό αυτό τα πακέτα μαρκάρονται ανάλογα με την κλάση στην οποία ανήκουν (προέκυψε από τον προηγούμενο μηχανισμό της ταξινόμησης), είτε με δάση άλλα κριτήρια, όπως τα χαρακτηριστικά της κίνησης που παρουσιάζουν κ.λπ.

• Μέτρηση (metering) της κίνησης. Στην προκειμένη περίπτωση ο μηχανισμός αυτός ελέγχει το προφίλ της κίνησης που δέχεται και το συγκρίνει με το προσυμφωνηθέν προφίλ κίνησης όπως προκύπτει από το SLA που έχει υπογράφει με το διαχειριστή του δικτύου. Στη συνέχεια ο μηχανισμός αυτός διαχωρίζει τα πακέτα σε έναν αριθμό κατηγοριών (ανάλογα με το αν βρίσκονται στα νόμιμα πλαίσια ή όχι). Ο αριθμός των κατηγοριών αυτών εξαρτάται από τη συμφωνία που έχει γίνει με τον παροχέα, όπου επίσης καθορίζεται η μεταχείριση που θα έχουν τα πακέτα όλων των κατηγοριών.

• Μηχανισμός μορφοποίησης (shaping) της κίνησης, όπου τροποποιούνται τα χαρακτηριστικά της κίνησης που έλαβε ο κόμβος (δρομολογητής). Επίσης, αντί του μηχανισμού αυτού μπορεί να υπάρχει μηχανισμός απόρριψης (dropping) των πακέτων.

Γενικά η σειρά με την οποία συνήθως χρησιμοποιούνται αυτοί είναι και η σειρά με την οποία παρουσιάστηκαν. Πρέπει στο σημείο αυτό να αναφέρουμε ότι είναι επίσης δυνατόν οι μηχανισμοί μαρκαρίσματος και μέτρησης του προφίλ της κίνησης να εμφανίζονται αντίστροφα, δηλαδή πρώτα μέτρηση του προφίλ της κίνησης και ύστερα, με βάση αυτό το κριτήριο, μαρκάρισμα των πακέτων. Επίσης, μετά τη διαδικασία μέτρησης του προφίλ, σε ορισμένες «κατηγορίες» πακέτων (και κυρίως σία νόμιμα πακέτα) συνήθως δεν εφαρμόζεται κανένας περαιτέρω μηχανισμός και εισάγονται έτσι στο δίκτυο. Στο σημείο αυτό είναι αναγκαίο να τονιστεί

πως όλοι οι παραπάνω μηχανισμοί και λειτουργικότητες εφαρμόζονται στους συνοριακούς δρομολογητές (edge routers) σε ένα DiffServ-enabled (ικανό να υποστηρίξει την αρχιτεκτονική DiffServ) διαχειριστικό τμήμα (domain). Αντίθετα, στους ενδιάμεσους δρομολογητές (core routers) η DiffServ αρχιτεκτονική προσδιορίζει πως οι παραπάνω μηχανισμοί δεν έχουν καμία εφαρμογή.

Πηγή:

- Π. Γανός, Α. Γκάμας, Α. Καραλιώτας, Χ. Μπούρας, Δ. Πρίμπας, Κ. Στάμος, IPv6: Το πρωτόκολλο και οι τεχνικές μετάβασης και μεταφερσιμότητας

2.2. Σύγκριση IPv4 με IPv6

2.2.1 Σύγκριση στην διαθεσιμότητα διευθύνσεων

Όσον αφορά τη μορφή της διεύθυνσης είναι κάπως πιο σύνθετη από το IPv4. Οκτώ πεδιά των 16-bit δεκαεξαδικες τιμές διαχωρισμένες με ερωτηματικό αντί για τέσσερα πεδία των 8-bit δεκαδικές τιμές που χωρίζονται από τελείες. Μια τυπική διεύθυνση IPv6 βλέπουμε παρακάτω:

2001: db8: 31:1:20 α: 95ff: fef5: 246e

Σημειώστε ότι τα αρχικά μηδενικά συνήθως φεύγουν κ αυτό συμβαίνει για να μειώσουν τα άσκοπα μηδενικά ακόμα περισσότερο. Μόνο σε μία ακολουθία μηδενικών τιμών διαχωρίζονται με άνω και κάτω τελεία όπου μπορεί και να αφαιρεθεί. Έτσι, η διεύθυνση 2001: db8: 31:0:0:0:0:1 μπορεί επίσης να γραφεί ως το 2001: db8: 31:: 1.

Το IPv4 λόγω του 32 bit μήκους διευθύνσεων μπορεί να διευθυνσιοδοτήσει το πολύ 2^{32} κόμβους. Εξαιτίας του τρόπου ανάθεσης των διευθύνσεων μόνο ένα ποσοστό από αυτές είναι αξιοποιήσιμες. Αυτό έχει ως αποτέλεσμα την

εξάντληση τους μέσα στο 2011. Επιπλέον, ένα μεγάλο πλήθος συσκευών που δεν είναι υπολογιστές έχει αρχίσει να χρησιμοποιεί το IP. Το IP θεωρείται το μέσο που θα ολοκληρώσει τα δεδομένα, τη φωνή, τον ψηφιακό ήχο και την ψηφιακή εικόνα. Για παράδειγμα, οι συσκευές κινητής τηλεφωνίας έχουν αρχίσει να υποστηρίζουν το IP. Το έτος 2005 υπήρχαν περισσότερες από 1,5 δισεκατομμύρια συσκευές κινητής τηλεφωνίας, ενώ το 2010, 1 δισεκατομμύριο αυτοκίνητα υποστήριζαν το πρωτόκολλο GPS και υπηρεσίες καταλόγου. Παράλληλα, η ανάπτυξη νέων τεχνολογιών όπως xDSL, ασύρματα δίκτυα κλπ. δίνουν τη δυνατότητα στους χρήστες να έχουν πραγματική πρόσβαση στο Διαδίκτυο με υψηλές ταχύτητες και επομένως μπορούν να χρησιμοποιούν εφαρμογές που απαιτούν μοναδικές διευθύνσεις και αποκλείουν τεχνικές δεξαμενής (pool) διευθύνσεων που μοιράζονται σε πολλούς χρήστες, που χρησιμοποιούν οι παροχείς υπηρεσιών Διαδικτύου (ISPs) σήμερα. Το IPv6 δεν πρόκειται να παρουσιάσει αντίστοιχα προβλήματα εξαιτίας του μήκους των 128 bits διευθύνσεων που έχει, δηλαδή περίπου $3,4 \times 10^{38}$ διευθύνσεις. Χαρακτηριστικό παράδειγμα στην διαφορά μεγέθους, αν στο IPv4 τις συνολικές διευθύνσεις τις παρομοιάζαμε με ένα μπαλάκι του γκολφ στο IPv6 μπορούσαμε να πούμε ότι έχει το μέγεθος του ήλιου όπου είναι τόσο μεγάλος που θα μπορούσε να χωρέσει πάνω 1 εκατομμύριο πλανήτες στο μέγεθος της γης.

2.2.2 Από την χρήση της μεθόδου NAT στο IPv6

Ένα τρόπος για να αντιμετωπίσουμε το πρόβλημα διευθύνσεων στο IPv4 είναι η τεχνική NAT η οποία λειτούργει με τέτοιο τρόπο ώστε να δημιουργεί υποδίκτυα. Όμως οι τεχνικές που χρησιμοποιεί το NAT είναι περιοριστικές για διάφορες εφαρμογές που απαιτούν να γνωρίζουν τη διεύθυνση των κόμβων με τους οποίους επικοινωνούν και μάλιστα αυτή να είναι μοναδική. Επίσης, το NAT αποτελεί φραγμό για την ασφάλεια και ακεραιότητα απ' άκρη σ' άκρη, αφού παρεμβαίνει και αλλάζει τις επικεφαλίδες των πακέτων. Επιπλέον, η χρήση NAT αποτελεί περιοριστικό παράγοντα για την mobile IP όσο και για τη χρήση της υπηρεσίας τηλεφωνίας πάνω από το IP. Γι’ αυτό έρχεται το IPv6 το οποίο καταργεί τη τεχνική NAT και όλα της τα προβλήματα.

Το IPv6 έχει λάβει υπόψη στο σχεδιασμό του να δημιουργήσει μία καθολική (για το Διαδίκτυο), ευέλικτη και επεκτάσιμη ιεραρχία στη δρομολόγηση. Έτσι ακολουθείται ένα ιεραρχικό σχήμα διευθυνσιοδότησης σε σχέση με τους ISPs κατά αντιστοιχία με τα εθνικά και διεθνή τηλεφωνικά κέντρα. Αυτό στην πράξη σημαίνει ότι στους δρομολογητές κορμού του Διαδικτύου δεν θα απαιτείται ο πολύ μεγάλος αριθμός των καταχωρήσεων στους πίνακες δρομολόγησης που υπάρχει σήμερα. Αντίθετα, με ένα πρόθεμα λίγων bits θα είναι δυνατή η δρομολόγηση των πακέτων, κάτι που απλουστεύει την αρχιτεκτονική των υπαρχόντων δρομολογητών και αυξάνει την απόδοση τους. Το IPv4, παρά τα πλεονεκτήματα της χρήσης CIDR και του πρωτοκόλλου δρομολόγησης BGP, εξακολουθεί να αντιμετωπίζει προβλήματα, αφού οι καταχωρήσεις στους πίνακες δρομολόγησης των δρομολογητών κορμού έχουν αυξηθεί υπερβολικά.

Με το IPv6 είναι πολύ εύκολο να προσδιοριστεί το πού ακριβώς βρίσκεται ο αποστολέας και ο παραλήπτης ενός πακέτου, αφού θα πρέπει να ελεγχθούν τα αντίστοιχα πεδία ιεραρχίας και μόνο. Αντίθετα, στο IPv4 εξαιτίας της πολιτικής που ακολουθήθηκε στην ανάθεση χώρου διευθύνσεων αυτό είναι δύσκολο έως αδύνατο.

2.2.3 Απλοποίηση διαχείρισης δικτύων και ρυθμίσεων

Οι μηχανισμοί απλούστευσης της διαχείρισης των κόμβων που δημιουργήθηκαν (DHCP & BOOTP) ανήκουν στην κατηγορία των μηχανισμών πλήρους κατάστασης (statefull), που σημαίνει ότι και πάλι απαιτείται διαχείριση και συντήρηση των δεδομένων από το διαχειριστή. Επιπλέον, παρουσιάζουν σημαντικά προβλήματα διότι απαιτούν αντίστοιχες εφαρμογές σε εξυπηρετητές δημιουργώντας "single points of failure" («αχίλλειες πτέρνες»·). Τέλος, οι μηχανισμοί αυτοί δεν προβλέπουν την ασφάλεια του δικτύου και την αυτόματη ενημέρωση της υπηρεσίας ονοματολογίας. Για την υποστήριξη αυτών απαιτούνται επιπλέον μηχανισμοί, κάνοντας εξαιρετικά πολύπλοκο το όλο σχήμα.

Αντίθετα, το IPv6 προβλέπει μηχανισμούς με τους οποίους ένας σταθμός μπορεί να δημιουργήσει μόνος του την IPv6 διεύθυνσή του. Επιπλέον, οι μηχανισμοί φροντίζουν τόσο για την ασφάλεια των κόμβων και του δικτύου όσο και για την αυτόματη ενημέρωση της *υπηρεσίας* ονοματολογίας. Πρέπει να σημειωθεί ότι το IPv6 υποστηρίζει τόσο stateless μηχανισμούς (χωρίς διατήρηση κατάστασης) όσο και statefull (με διατήρηση κατάστασης). Τέλος, επειδή αυτές οι υπηρεσίες μπορούν να αντιστοιχιστούν σε διευθύνσεις τύπου anycast εξασφαλίζεται και η ευρωστία (robustness) των μηχανισμών.

Στο IPv4 η διαδικασία της εκ νέου αριθμοδότησης του δικτύου είναι εξαιρετικά δύσκολη και πολύπλοκη. Απαιτείται να αλλαχτούν οι ρυθμίσεις που αφορούν τη διεύθυνση του κόμβου, τη μάσκα δικτύου, τον προκαθορισμένο δρομολογητή, τον εξυπηρετητή ονοματολογίας κ.λπ. Αξίζει να σημειωθεί ότι η διαδικασία της αριθμοδότησης εκ νέου ενός δικτύου δεν είναι σπάνια και μπορεί να συμβεί, για παράδειγμα, εάν ένας οργανισμός αλλάξει παροχέα Διαδικτύου (και δεν έχει χώρο διευθύνσεων ανεξάρτητο από παροχέα [provider independent] - κάτι που είναι εξαιρετικά σπάνιο) ή ακόμα και αν ο διαχειριστής του δικτύου διαπιστώσει ότι ο τρόπος με τον οποίο έχει αριθμοδοτήσει το δίκτυό του δεν τον βολεύει καθώς πρέπει να δημιουργήσει περισσότερα υποδίκτυα ή έχει αυξηθεί ο αριθμός των κόμβων ενός υποδικτύου. Αντίθετα, στο IPv6 η αλλαγή αριθμοδότησης του δικτύου είναι απλούστατη, γιατί άλλωστε αποτελούσε και έναν από τους στόχους του IPv6, και ο διαχειριστής δικτύου απλώς αλλάζει το πρόθεμα του δικτύου στον κεντρικό δρομολογητή και αυτόματα ενημερώνονται όλοι οι κόμβοι του δικτύου να αλλάξουν τις διευθύνσεις τους.

Το IPv6 προσφέρει καλύτερη διαχείριση της κυκλοφορίας των IP πακέτων, αφού χρησιμοποιεί την τεχνική multicast καταργώντας την τεχνική broadcast. Αντίθετα, το IPv4 χρησιμοποιεί ευρέως την τεχνική broadcast, κάτι που έχει αποδειχθεί ότι είναι σημαντικός περιοριστικός παράγοντας στην απόδοση ενός δικτύου.

2.2.4 Ποιότητα υπηρεσιών

Quality of Service (QoS) είναι ένα σημαντικό χαρακτηριστικό των σύγχρονων δικτύων. Τα IPv4 δίκτυα συνήθως δίνουν σε κάθε πακέτο ένα καλύτερο επίπεδο προσπάθειας (best level of effort) σε υπηρεσία, ακόμη και αν το περιεχόμενο του κάθε πακέτου δεν είναι πραγματικά σημαντικό. Ένα σύστημα βασισμένο στο IPv4 δεν έχει τον τρόπο να διαφοροποιήσει τα δεδομένα που είναι ωφέλιμα ή ευαίσθητα φορτία, όπως streaming βίντεο, ήχο κτλ καθώς και εκείνα που δεν είναι ευαίσθητα στον παράγοντα χρόνου. Streaming audio και video εφαρμογές είναι πολύ ευαίσθητα σε καθυστέρηση μερικών πακέτων, δυστυχώς ομως το IPv4 δεν έχει τρόπο να αποτρέψει αυτά τα προβλήματα. Αν ένα πακέτο έχει χαθεί κατά τη μεταφορά, το TCP αναγνωρίζει την απώλεια και ζητά την αναμετάδοση εκπομπής, όσον αφορά όμως την καθυστέρηση είναι αναπόφευκτη. Η καθυστέρηση πακέτου TCP είναι πιθανόν μέρος ενός πολύ μεγαλύτερου πακέτου των δεδομένων ήχου ή βίντεο, έτσι ώστε ολόκληρο το μεγάλο πακέτο να έχει καθυστερήσει και ίσως να χαθεί επειδή το μικρότερο πακέτο δεν φθάνει στην ώρα του. Το IPv6 παρέχει έναν τρόπο για τις εφαρμογές, χωρίς καθυστέρηση, σε όλη την WAN. Αυτό συχνά χρησιμοποιείται για να περιγράψει μια χαμηλή λανθάνουσα κατάσταση. Συνεχής ροή ήχου και βίντεο απαιτεί χαμηλή λανθάνουσα κατάσταση μέσα από υψηλή προτεραιότητα. Για να αποφευχθούν οι διακοπές,οι εφαρμογές μπορούν να μοιράζονται τη σύνδεση μέσω του επίπεδο προτεραιότητας.

Το IPv4 και το IPv6 καθορίζουν την κυκλοφορία χάρη σε ενα μικρό πεδίο στην επικεφαλίδα που χρησιμοποιείται για να κραταει τον "τύπος υπηρεσίας" και τις πληροφορίες προτεραιότητας. Το πεδίο αυτό καθορίζεται με τη χρήση με του «differentiated services» (DiffServ). Ωστόσο, το IPv6 έχει επίσης ένα πεδίο που το IPv4 δεν έχει: την ετικέτα ροής (flow label). Η ετικέτα της ροής δεν χρησιμοποιείται στην πραγματικότητα, και η μόνη χρήση της είναι να αναγνωρίζει διαφορετικές περιόδους επικοινωνίας, κάτι που εύκολα γίνεται και από την εξέταση της TCP ή του αριθμού UDP θύρας. Το IPv6 μπορεί να κερδίσει QoS πλεονεκτήματα σε σχέση με το IPv4, όταν η ετικέτα ροής τεθεί σε καλή χρήση στο μέλλον.

Το IPv4 στην επικεφαλίδα του έχει ορισμένο το πεδίο TOS μεγέθους ενός byte για την παροχή Ποιότητας Υπηρεσίας μέσω της αρχιτεκτονικής DiffServ. Αντίστοιχα, το IPv6 έχει το πεδίο Traffic Class στην επικεφαλίδα του. Και τα δύο πρωτόκολλα μπορούν να υποστηρίξουν το πρωτόκολλο RSVP για υπηρεσίες με συγκεκριμένες απαιτήσεις ποιότητας (QoS). Επιπλέον, το IPv6 περιλαμβάνει ένα πεδίο μεγέθους 20 bits, το πεδίο Ετικέτας Ροής (Row Label) το οποίο μπορεί να έχει σημαντικό ρόλο στην υποστήριξη μηχανισμών ποιότητας υπηρεσίας.

Ένας δρομολογητής που υποστηρίζει το IPv4 για να αναγνωρίσει μία ροή θα πρέπει να αναλύσει τις διευθύνσεις IP τόσο του αποστολέα όσο και του παραλήπτη και τη θύρα (port) που βρίσκεται στην επικεφαλίδα του πρωτοκόλλου μεταφοράς. Αυτό σημαίνει υπερβολικό κόστος επεξεργασίας στους δρομολογητές που πιθανόν να θέσει σε κίνδυνο την ίδια την ποιότητα υπηρεσίας. Αντίθετα, το IPv6 περιλαμβάνει όλα αυτά τα στοιχεία στο πεδίο Flow Label και επομένως επιτρέπει την ταχύτατη επεξεργασία από τους δρομολογητές χωρίς να απαιτείται να εξεταστούν τα υπόλοιπα πεδία (ούτε καν οι διευθύνσεις αποστολέα και παραλήπτη).

Εάν στο IPv4 ενεργοποιηθούν οι μηχανισμοί ασφάλειας του IPsec, τότε κωδικοποιούνται τα δεδομένα των επιπέδων «πάνω» από το επίπεδο του δικτύου. Αυτό σημαίνει ότι οι δρομολογητές δεν θα είναι σε θέση να αναγνωρίσουν τις θύρες (ports) του επιπέδου μεταφοράς και άρα να αναγνωρίσουν μία ροή δεδομένων και να προσφέρουν την ποιότητα υπηρεσίας. Αντίθετα, στο IPv6 οι μηχανισμοί ασφάλειας και ποιότητας υπηρεσίας είναι σχεδιασμένοι ώστε να μη δημιουργούν τέτοια προβλήματα.

2.2.5 Υποστήριξη κινητών χρηστών

Ενώ και τα δύο πρωτόκολλα υποστηρίζουν κινητούς χρήστες, στο IPv6 η υποστήριξη είναι ενσωματωμένη, πράγμα που απλοποιεί τη διαχείριση της υπηρεσίας.

Στο IPv4 υπάρχει ένα πρόβλημα που ονομάζεται δρομολόγησης τριγώνου (triangular routing), αφού ο κινητός κόμβος επικοινωνεί με τους υπόλοιπους

κόμβους μέσω του home πράκτορα (home agent) ο οποιος είναι συνήθως ένα router «κάτοικος» ενός Mobile κόμβου που προωθεί τα πακέτα με ανεξάρτητα από το εάν Mobile κόμβος είναι μακριά από το οικιακό δίκτυο ή όχι. Αντίθετα, το IPv6 έχει ενσωματωμένη τη βελτιστοποίηση της δρομολόγησης με χρήση της τεχνικής ενημέρωσης binding (binding update). Ο κινητός κόμβος μπορεί να ειδοποιήσει το δρομολογητή για την care-of (προσωρινή) διεύθυνση του με χρήση ενημέρωσης binding, όπως και οποιονδήποτε κόμβο τού αποστέλλει πακέτα, ώστε ο κόμβος αυτός να του στέλνει τα πακέτα στην care-of διεύθυνση και όχι στη home (οικεία/μόνιμη) διεύθυνση. Οι διάφορες τεχνικές που προσπαθούν να εφαρμοστούν στο IPv4 για την εξάλειψη του συγκεκριμένου προβλήματος βασίζονται σε συνδυασμό πολλών πρωτοκόλλων και είναι εξαιρετικά πολύπλοκες.

Οι μηχανισμοί του IPv6 για την υποστήριξη αυτόματης ρύθμισης των σταθμών εργασίας μειώνουν το κόστος διαχείρισης, αφού ο κινητός κόμβος μπορεί να αποκτήσει την care-of διεύθυνση με χρήση stateless ή statefull μηχανισμών. Αντίθετα, στο IPv4 απαιτείται και ύπαρξη DHCP εξυπηρετητή δημιουργώντας μια αχίλλειο πτέρνα (single point of failure). Επιπλέον, ο κινητός κόμβος μπορεί να χρησιμοποιεί διευθύνσεις τύπου anycast για να ανακαλύψει τους home πράκτορες (home agents), στέλνοντας ένα μήνυμα ενημέρωσης binding (binding update) στη διεύθυνση anycast, μειώνοντας έτσι το κόστος διαχείρισης (μπορούν να υπάρχουν πολλοί δρομολογητές ικανοί να είναι home πράκτορες, άρα δεν υπάρχει κίνδυνος single point of failure). Επιπλέον, δεν απαιτείται ο κινητός κόμβος να γνωρίζει τη διεύθυνση του home πράκτορα, κάτι που ήταν περιοριστικός παράγοντας στο IPv4. Τέλος, ο home πράκτορας μπορεί να διαφημίζει τον εαυτό του με χρήση του μηχανισμού διαφήμισης γείτονα (neighbor advertisement). Όλες οι παραπάνω διαδικασίες είναι εξαιρετικά πολύπλοκες στο IPv4.

Το IPv6 μπορεί να χρησιμοποιήσει τους ενσωματωμένους μηχανισμούς ασφάλειας που διαθέτει ώστε να πιστοποιήσει ότι ο κόμβος που επικοινωνεί με το home πράκτορα είναι ο κινητός κόμβος. Αντίθετα, το IPv4 είναι αρκετά πολύπλοκο να υποστηρίξει μηχανισμούς ασφάλειας για τους κινητούς κόμβους, αφού θα πρέπει να υποστηρίζονται από τα δίκτυα στα οποία συνδέεται ο κινητός κόμβος.

Το IPv6 έχει ενσωματωμένους μηχανισμούς ώστε σαν διεύθυνση αποστολέα στα μηνύματα του κινητού κόμβου να είναι η care-of διεύθυνση και όχι η home διεύθυνση, εξαλείφοντας το πρόβλημα δρομολόγησης στους δρομολογητές που για λόγους ασφάλειας πραγματοποιούν φιλτράρισμα εισερχόμενης κίνησης (ingress-filtering).

Το IPv6 έχει ενσωματωμένη υποστήριξη για VPNs (Virtual Private Networks - Εικονικά Ιδιωτικά Δίκτυα) και επομένως υποστηρίζει καλύτερα τους απομακρυσμένους χρήστες.

Το IPv4 παρουσιάζει προβλήματα στην περίπτωση που ο κινητός κόμβος κάνει χρήση του μηχανισμού multicast. Όταν ο κινητός κόμβος δεν βρίσκεται στο home υποδίκτυο, δεν μπορεί να αποστείλει multicast πακέτα. Η λύση της δημιουργίας αντίστροφων καναλιών δημιουργεί επιπλέον πολυπλοκότητα, ενώ παρουσιάζει και σημαντικότατα προβλήματα ασφάλειας. Αντίθετα, στο IPv6 η υποστήριξη του μηχανισμού multicast είναι ενσωματωμένη και δεν παρουσιάζονται τέτοια προβλήματα.

Το IPv6 παρέχει μηχανισμούς ώστε τόσο ο κινητός κόμβος όσο και ο δρομολογητής στο ξένο υποδίκτυο (foreign subnet) να γνωρίζουν αν ο κινητός κόμβος έχει αλλάξει δίκτυο. Έτσι δεν υπάρχουν τα φαινόμενα "black hole" («μαύρης τρύπας») που εμφανίζει το IPv4 όπου η σύνδεση του κινητού κόμβου με το δρομολογητή παρουσιάζει αστάθεια από τη μία κατεύθυνση.

2.2.6 Ασφάλεια

Πολλοί άνθρωποι υποστηρίζουν ότι το IPv6 είναι πιο ασφαλές από το IPv4. Πολλές πτυχές της ασφάλειας του IPv6 παρουσιάζουν βελτίωση σε σχέση με αυτές του IPv4. Επίσης, το IPv6 έχει χαρακτηριστικά που αψηφούν σύγκριση με το IPv4. Το πιο σημαντικό, μιλάμε για «ασφάλεια» σαν να επρόκειτο για κάποιο είδος καρυκεύματος. Πέρα όμως από αυτό το IPv6 δική του “κρίση”. Αυτό σημαίνει ότι μπορεί να γνωρίζει τι μπορεί να πάει στραβά, λαμβάνοντας εύλογα μέτρα για να αποφευχθούν οι καταστάσεις αυτές. Αυτό έρχεται σε αντίθεση με την ανθρώπινη φύση, που μας οδηγεί για τη διατήρηση της ψυχικής ενέργειας, αλλά είναι δίκοπο μαχαίρι γιατί μπορεί να αγνοούν άλλα πιθανά αποτελέσματα.

Ενώ στο IPv6 η ασφάλεια είναι υποχρεωτική, στο IPv4 είναι προαιρετική. Επειδή στο IPv4 η υποστήριξη του πρωτοκόλλου IPsec είναι επιπρόσθετη, γίνεται χρήση του πεδίου IP Options και αυξάνει την πολυπλοκότητα επεξεργασίας των πακέτων. Αντίθετα, στο IPv6 η υποστήριξη είναι ενσωματωμένη και επομένως η υλοποίηση και η λειτουργία είναι απλούστερες.

Οι μηχανισμοί ασφάλειας στο IPv6 μπορούν να χρησιμοποιηθούν από οποιονδήποτε άλλο μηχανισμό. Αντίθετα, στο IPv4 σε κάθε επέκτασή του θα πρέπει ο μηχανισμός να εξασφαλίζει μηχανισμούς ασφάλειας.

Η χρήση των μηχανισμών του IPsec στο IPv4 είναι εξαιρετικά πολύπλοκη, αφού σε αυτό το IPsec υλοποιείται «πάνω» από όλες τις άλλες εφαρμογές όπως από Mobile IP. Επιπλέον, η χρήση NAT από τα IPv4 δίκτυα καταργεί την ασφάλεια που προσφέρουν οι μηχανισμοί του IPsec. Αντίθετα, στο IPv6 η υποστήριξη του IPsec είναι πρωτογενής και δεν παρουσιάζει αντίστοιχα προβλήματα.

Στο IPv6 η ασφάλεια βασίζεται αποκλειστικά στο επίπεδο IP (IP level Security), δηλαδή όλες οι διαδικασίες ασφάλειας έχουν σκοπό την προστασία του IP πακέτου από κάθε είδος επίθεσης κατά την πορεία του μέσα από το δίκτυο. Η ασφάλεια στο επίπεδο IP μπορεί να παρέχει τις εξής δυνατότητες:

Πιστοποίηση (Authentication)

Πιστοποίηση είναι η ικανότητα να γνωρίσουμε ότι τα δεδομένα που παραλήφθηκαν είναι αυτά που έστειλε ο αποστολέας και ότι ο αποστολέας είναι αυτός που ισχυρίζεται.

Ακεραιότητα πληροφορίας (Integrity)

Η ακεραιότητα της πληροφορίας είναι η δυνατότητα να ανιχνεύεται οποιαδήποτε αλλαγή της πληροφορίας στην ενδιάμεση διαδρομή από τον αποστολέα στον παραλήπτη.

Απόρρητο της πληροφορίας (Confidentiallity)

Το απόρρητο της πληροφορίας είναι η δυνατότητα να είναι διαθέσιμη σε κατανοητή μορφή μόνο από τους πραγματικούς παραλήπτες. Με αυτό τον

τρόπο είναι σχεδόν αδιάφορο ποιοι μπορούν να υποκλέψουν την πληροφορία κατά την διάρκεια της πορείας της προς τον τελικό προορισμό της .

Απόδειξη αποστολής δεδομένων από τον αποστολέα (Non-repudiation)

Με αυτή την δυνατότητα είναι αδύνατο να αρνηθεί ένας αποστολέας το γεγονός της αποστολής των δεδομένων. Η δυνατότητα αυτή είναι διαθέσιμη μόνο όταν χρησιμοποιείται ένας ασύμμετρος αλγόριθμος κρυπτογράφησης.

Η ασφάλεια σε επίπεδο IP και σαν συνέπεια η ασφάλεια που παρέχει το IPv6. δεν μπορεί να καλύψει όλες τις περιπτώσεις επιθέσεων. Μια τέτοια περίπτωση είναι η περίπτωση της ανάλυσης της ροής της πληροφορίας (traffic analysis). Η ανάλυση αυτή μπορεί να παρέχει χρήσιμες πληροφορίες για έναν πιθανό εισβολέα, όπως η συχνότητα ανταλλαγής πληροφοριών των μηχανισμών ασφαλείας, το μέγεθος των πακέτων ή ακόμα και ο τύπος της πληροφορίας που κάποιος χρήστης αναζητεί στο Internet.

2.2.6.1 Μηχανισμοί ασφάλειας του IPv6

Το IPv6 χρησιμοποιεί δύο βασικούς μηχανισμούς για να παρέχει τις υπηρεσίες ασφάλειας που αναφέρθηκαν στην προηγούμενη παράγραφο. Οι μηχανισμοί αυτοί είναι :

- IP Authentication Header
- IP Encapsulating Security Payload

Οι δύο αυτοί μηχανισμοί βασίζονται κυρίως σε εξωτερικούς μηχανισμούς κρυπτογράφησης για να παρέχουν ασφάλεια. Να σημειώσουμε ότι η κρυπτογράφηση χρησιμοποιεί κάποια κλειδιά η διαχείριση των οποίων είναι ένα πολύ σημαντικό θέμα. Ο κυρίως λόγος είναι ότι η διαχείριση δεν είναι στενά συνδεδεμένη με την δομή και λειτουργία του IPv6 και μπορεί να αλλάξει στο μέλλον χωρίς απαραίτητα να επηρεάσει το IP.

2.2.6.1.1 Κρυπτογράφηση

Η κρυπτογράφηση είναι η διαδικασία μετατροπής της πληροφορίας σε μια μορφή η οποία αποκρύπτει το πραγματικό της περιεχόμενο και η ανάκτηση της είναι δυνατή μόνο από άτομα που έχουν την απαραίτητη έγκριση. Η κρυπτογράφηση είναι προϊόν της επιστήμης που ονομάζεται κρυπτογραφία. Η κρυπτογραφία εξελίσσεται συνεχώς και νέοι μέθοδοι κρυπτογράφησης εμφανίζονται.

Η πληροφορία που πρόκειται να κρυπτογραφηθεί ονομάζεται plaintext, ενώ η κρυπτογραφημένη cyphertext. Για να γίνει η κρυπτογράφηση απαιτείται ένας μηχανισμός κρυπτογράφησης ο οποίος είναι ένα πρόγραμμα υπολογιστή το οποίο υλοποιεί τον αλγόριθμο κρυπτογράφησης. Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση η οποία δέχεται σαν είσοδο της, την πληροφορία (plaintext) και μια ακολουθία από bit που ονομάζεται κλειδί και παράγει την κρυπτογραφημένη πληροφορία. Είναι προφανές ότι το αποτέλεσμα που μας δίνει ο αλγόριθμος πρέπει να είναι μοναδικό για κάθε συνδυασμό πληροφορίας (Plaintext) και κλειδιού. Η ανάκτηση την πληροφορίας από το cyphertext απαιτεί την ύπαρξη ενός μηχανισμού αποκρυπτογράφησης και το αντίστοιχο κλειδί.

Οι αλγόριθμοι κρυπτογράφησης χωρίζονται σε δυο βασικές κατηγορίες, τους συμμετρικούς και τους ασύμμετρους.

Συμμετρικοί αλγόριθμοι: Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για την διαδικασία της κρυπτογράφησης/αποκρυπτογράφησης. Ένας πολύ γνωστός τέτοιος αλγόριθμος είναι ο D.E.S (Data Encryption Standard). Βασικό μειονέκτημα των αλγόριθμων αυτού του τύπου είναι η διανομή του κλειδιού και η προστασία της μυστικότητας του.

Ασύμμετροι αλγόριθμοι: Η βασικότερη διαφορά των αλγόριθμων αυτών από την προηγούμενη κατηγορία είναι η ύπαρξη δύο διαφορετικών κλειδιών. Το ένα χρησιμοποιείται για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση της πληροφορίας. Η ύπαρξη δύο κλειδιών κάνει δυνατή

την εύκολη την διανομή των κλειδιών. Αρκεί να κρατηθεί μυστικό το ένα κλειδί, ενώ το άλλο μπορεί να διανεμηθεί ελεύθερα.

Η ασφάλεια που παρέχουν οι αλγόριθμοι βασίζεται την πολυπλοκότητα και δυσκολία επίλυσης της συνάρτησης που χρησιμοποιείται. Η συνάρτησης αυτή είναι πολύ εύκολο να υπολογιστή προς την μία κατεύθυνση (Κρυπτογράφηση) , ενώ είναι φοβερά χρονοβόρα προς την αντίθετη (Αποκρυπτογράφηση). Για μια όμως συγκεκριμένη περίπτωση, η επίλυση και προς την αντίθετη κατεύθυνση είναι εύκολη, αυτή είναι η περίπτωση στην οποία υπάρχει το κλειδί που απαιτείται για την αποκρυπτογράφηση. Η ανεύρεση τέτοιων συναρτήσεων είναι εξαιρετικά δύσκολη και ακόμα ποιο δύσκολη είναι η πιστοποίηση της ιδιότητας τους. Οι συναρτήσεις αυτές ονομάζονται trap door functions. Όλα τα παραπάνω προϋποθέτουν ότι τα κλειδιά είναι διαθέσιμα μόνο στα εξουσιοδοτημένα άτομα.

2.2.6.1.2 Ψηφιακές Υπογραφές

Εκτός από την κρυπτογράφηση των πληροφοριών, η κρυπτογραφία δίνει την δυνατότητα της ψηφιακής υπογραφής με την οποία είναι δυνατές οι εξής λειτουργίες :

- Πιστοποίηση (Authentication).
- Ακεραιότητας την πληροφορίας (Integrity).

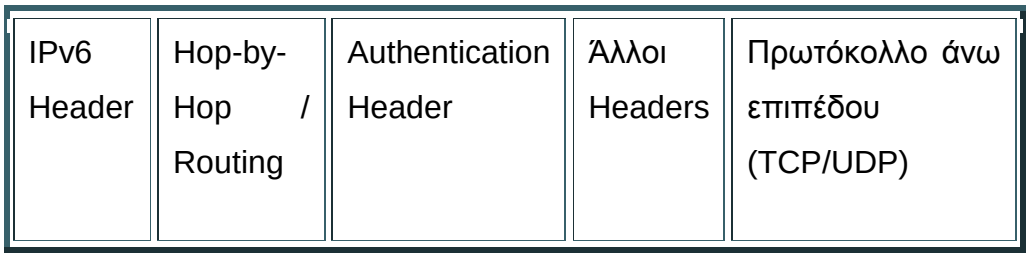
Οι συναρτήσεις που χρησιμοποιούνται για την ψηφιακοί υπογραφή κειμένων ονομάζονται hash functions. Μια τέτοια συνάρτηση δέχεται σαν είσοδο ένα μήνυμα και δημιουργεί έναν αριθμό σταθερού μήκους (συνήθως 128 bits) που αντιπροσωπεύει το μήνυμα. Είναι εξαιρετικά δύσκολο να δημιουργηθεί ένα μήνυμα το οποίο θα κάνει τον αλγόριθμο να παράγει μια συγκεκριμένη τιμή και για αυτό τον λόγο είναι σχεδόν αδύνατο να μεταβληθεί το περιεχόμενο ενός μηνύματος χωρίς αυτό να γίνει αντιληπτό. Δύο βασικοί αλγόριθμοι που χρησιμοποιούνται σήμερα είναι ο Keyed HMAC MD5 και ο Keyed HMAC SHA.

2.2.6.2 IP Authentication Header

Ο μηχανισμός του IP authentication Header μπορεί να παρέχει τις εξής δυνατότητες ασφάλειας:

- Πιστοποίηση (Authentication).
- Ακεραιότητας την πληροφορίας (Integrity).
- Απόδειξη αποστολής δεδομένων από τον αποστολέα (Non-repudiation).

Ο μηχανισμός αυτός στο IPv6 προστίθεται σαν μια έξτρα επικεφαλίδα όπως φαίνεται και στο Σχήμα 2.1. Η κύρια πληροφορία που υπάρχει στην επικεφαλίδα αυτή είναι ένα νούμερο το οποίο είναι το αποτέλεσμα της εφαρμογής του χρησιμοποιούμενου αλγόριθμου κρυπτογράφησης σε όλο το πακέτο.



Σχήμα 2.1 Μορφή IP πακέτου με Authentication Header

IP Encapsulating security Payload (ESP)

Ο μηχανισμός του IP Encapsulating security Payload μπορεί να παρέχει τις εξής δυνατότητες ασφάλειας:

- Ακεραιότητας την πληροφορίας (Intergrity).
- Απόρρητο της πληροφορίας (Confidentiality)
- Απόδειξη αποστολής δεδομένων από τον αποστολέα (Non-repudiation).

Η λειτουργία αυτού του μηχανισμού βασίζεται στην κρυπτογράφηση της προς μετάδοσης πληροφορίας. Με αυτό τον τρόπο μόνο ο παραλήπτης που έχει

στην κατοχή του το κατάλληλο κλειδί μπορεί να αποκρυπτογραφήσει την πληροφορία. Η γενική μορφή ενός πακέτου IP που χρησιμοποιεί την λειτουργία IP .

Ο μηχανισμός του ESP μπορεί να χρησιμοποιηθεί με δύο τρόπους:

1. **Εφαρμογή σε Transport επίπεδο.**Σε αυτή την περίπτωση η κρυπτογραφημένη πληροφορία περιέχει μόνο το πακέτο του επιπέδου μεταφοράς (Transport TCP/UDP). Δηλαδή την επικεφαλίδα του επιπέδου Transport και τα δεδομένα του χρήστη. Σαν αποτέλεσμα δεν έχουμε προστασία των IP Headers.
2. **Εφαρμογή σε Tunnel επίπεδο.**Σε αυτή την περίπτωση γίνεται κρυπτογράφηση ολόκληρου του IP πακέτου. Ο τρόπος αυτός χρήσης είναι ιδιαίτερα χρήσιμος για την δημιουργία VPNs
3. **Καθορισμός των παραμέτρων ασφαλείας μιας σύνδεσης**.Οι μηχανισμοί ασφαλείας χρησιμοποιούν την έννοια του Security Association. Ένα Security Association αποτελείται από ένα σύνολο επιλογών σχετικές με την εφαρμογή των μηχανισμών ασφαλείας και την διεύθυνση προορισμού των πακέτων της πληροφορίας. Οι βασικές επιλογές που πρέπει να υπάρχουν σε ένα security association παρουσιάζονται περιληπτικά στην συνέχεια :

- Αλγόριθμος Πιστοποίησης (Authentication) που χρησιμοποιεί το IP Authentication Header
- Κλειδιά που χρησιμοποιεί ο αλγόριθμος Πιστοποίησης (Authentication) που χρησιμοποιείται από το IP Authentication Header
- Αλγόριθμος κρυπτογράφησης που χρησιμοποιεί το IP Encapsulating Header (ESP).
- Κλειδιά που χρησιμοποιεί ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται από το IP Encapsulating Header(ESP).
- Παρουσία/απώλεια και μέγεθος του πεδίου κρυπτογραφικού συγχρονισμού ή πεδίο ανύσματος εκκίνησης για τον αλγόριθμο κρυπτογράφησης (ESP).

- Αλγόριθμος Πιστοποίησης (Authentication) που χρησιμοποιεί το IP Encapsulating Header (ESP).
- Κλειδιά που χρησιμοποιεί ο αλγόριθμος Πιστοποίησης (Authentication) που χρησιμοποιείται από το IP Encapsulating Header (ESP).
- Διάρκεια ζωής των κλειδιών ή ώρα που θα αλλάξουν τα κλειδιά.
- Διάρκεια ζωής του συγκεκριμένου security association.
- Διεύθυνση(-σεις) πηγής (Source) του security association.
- Επίπεδο ευαισθησίας της πληροφορίας (π.χ. Μυστική, μη κατηγοριοποιημένη)

Τα security association είναι μιας κατεύθυνσης και σαν συνέπεια θα πρέπει να δημιουργείται ένα για κάθε κατεύθυνση μια αμφίδρομης σύνδεσης. Η δημιουργία ενός security association ξεκινάει από την μηχανή που παίζει το ρόλο του αποστολέα για την συγκεκριμένη κατεύθυνση της επικοινωνίας, ή οποία και στέλνει τις επιλογές που εκφράζουν τις απαιτήσεις σε ασφάλεια της επικοινωνίας. Η δημιουργία ολοκληρώνεται από την μηχανή παραλήπτη που απαντάει με ένα νούμερο το λεγόμενο Δείκτη Παραμέτρων Ασφαλείας(Security Parameters Index - SPI) για την συγκεκριμένη σύνδεση. Η αναγνώριση του security association γίνεται για τον αποστολέα με το συνδυασμό του SPI και της ταυτότητας του χρήστη (userid), ενώ για τον παραλήπτη από το συνδυασμό του SPI και την διεύθυνση προορισμού του πακέτου. Τέλος πρέπει να σημειώσουμε ότι η μηχανισμοί ασφάλειας μπορούν να χρησιμοποιηθούν και σε διευθύνσεις multicast.

Πηγή:

- Π. Γανός, Α. Γκάμας, Α. Καραλιώτας, Χ. Μπούρας, Δ. Πρίμπας, Κ. Στάμος, IPv6: Το πρωτόκολλο και οι τεχνικές μετάβασης και μεταφερσιμότητας, εκδόσεις Ελληνικά Γράμματα, ISBN 960-442-277-4
- http://www.islab.demokritos.gr (Internet Cinematics Labs, Δίκτυο Αριάδνη Ε.ΚΕ.ΦΕ. Δημόκτιρος)
- http://ru6.cti.gr/bouras/en/index.php (Christos J. Bouras)

3.Η ΔΟΜΗ ΤΟΥ IPv6

3.1 Επισκόπηση των αλλαγών της επικεφαλίδας

Οι αλλαγές από το IPv4 στο IPv6 μπορούν να συνοψισθούν στις παρακάτω κατηγορίες.

- Εκτεταμένη δυνατότητα διευθυνσιοδότησης. Στο νέο πρωτόκολλο έχει αυξηθεί το μέγεθος της επικεφαλίδας από 32 σε 128 bits, προσφέροντας δυνατότητες για περισσότερα επίπεδα διευθυνσιοδότησης, σχεδόν 'ανεξάντλητο' χώρο διευθύνσεων και απλούστερη αυτοδιαμόρφωση των διευθύνσεων (autoconfiguration). Η διαβαθμισιμότητα της δρομολόγησης multicast επίσης έχει βελτιωθεί, προσθέτοντας το πεδίο scope στη διεύθυνση.

- Απλοποιημένη επικεφαλίδα. Κάποια από τα πεδία του IPv4 απουσιάζουν από το IPv6 ή έχουν γίνει προαιρετικά. Έτσι μειώνεται το κόστος δρομολόγησης για κάθε πακέτο και το κόστος σε εύρος ζώνης που καταναλώνει η επικεφαλίδα. Η επικεφαλίδα, επίσης, έχει σταθερό μήκος, βοηθώντας έτσι τους δρομολογητές να έχουν καλύτερη απόδοση.

- Autoconfiguration : Το autoconfiguration είναι το πιο συναρπαστικό σημείο στην υιοθέτηση του IPv6. Οι συσκευές που έχουν ενεργοποιημένο το νέο πρωτόκολλο έχουν την δυνατότητα να αυτορυθμιστούν δυναμικά όταν συνδέονται σε ένα δίκτυο

- Βελτιωμένη υποστήριξη για επεκτάσεις και επιλογές της επικεφαλίδας. Το IPv6 διαθέτει υποστήριξη προαιρετικών πεδίων σε ξεχωριστές επικεφαλίδες. Αυτό κάνει το νέο πρωτόκολλο τροποποιήσιμο και εύπλαστο διότι θα μπορούμε να προσθέσουμε καινούριους τύπους κεφαλίδων αν προκύψει η ανάγκη για κάτι τέτοιο. Επίσης διευκολύνει την απόδοση της

δρομολόγησης, χωρίς να χρειάζεται ο κάθε δρομολογητής να επεξεργαστεί αυτά τα πεδία, αν κάτι τέτοιο δεν είναι αναγκαίο.

- Έλεγχος ροής στο επίπεδο IP. Μια καινούρια λειτουργία έχει προστεθεί που κατηγοριοποιεί τα πακέτα ενός αποστολέα σε μια συγκεκριμένη ροή (flow). Αυτή η ροή μπορεί να αντιμετωπιστεί από τους δρομολογητές με κάποιο ειδικό τρόπο (π.χ. μια ροή δεδομένων live streaming video)

- Ασφάλεια στο επίπεδο IP. Το IPv6 προσφέρει, μέσω των επικεφαλίδων επέκτασης, ασφάλεια και απόκρυψη δεδομένων.

3.2 Η βασική επικεφαλίδα του IPv6

32 bit

Version (Έκδοση)	Traffic Class (Τάξη Κυκλοφορίας)	Flow Label (Ετικέτα Ροής)	
Payload Length (Μήκος Πακέτου)		Next Header (Επόμενη Επικεφαλίδα)	Hop Limit (Όριο Βημάτων)
Source IP Address (Διεύθυνση Αφετηρίας)			
Destination IP Address (Διεύθυνση Προορισμού)			

Σχήμα 3.1 Η βασική επικεφαλίδα του IPv6

- Version(Έκδοση) : Έχει μήκος 4 bits και για το IPv6 πρέπει να είναι ίσο με 6
- Traffic Class(Τάξη Κυκλοφορίας) : Έχει μήκος 8 bits και προσδιορίζει ότι μια συγκεκριμένη υπηρεσία παρέχεται σ' αυτό το πακέτο. Η προκαθορισμένη τιμή του είναι με όλα μηδέν.

- Flow Label(Ετικέτα Ροής) : Έχει μήκος 20 bit και χρησιμοποιείται για να γνωστοποιεί ποια πακέτα ανήκουν σε μια συγκεκριμένη ροή. Ένας κόμβος μπορεί να είναι η αφετηρία για πάνω από μια ροές ταυτόχρονα. Γι αυτό η ετικέτα ροής σε συνδυασμό με τη διεύθυνση της αφετηρίας μπορούν να αναγνωρίσουν μονοσήμαντα μια ροή.

- Payload length(Μήκος Πακέτου) : Αυτό το πεδίο καταλαμβάνει 16 bits και περιέχει μια δυαδική τιμή ίση με το μήκος του πακέτου σε bytes. Το μήκος αυτό αφορά το μέρος του πακέτου που ξεκινά αμέσως μετά τη βασική επικεφαλίδα. Δηλαδή οι επικεφαλίδες επέκτασης συνυπολογίζονται σ' αυτό το μέγεθος.

- Next header (Επόμενη επικεφαλίδα) : Ένα πεδίο των 8 bit που η τιμή του δείχνει το είδος της επόμενης επικεφαλίδας. Η επόμενη επικεφαλίδα μπορεί να είναι η επικεφαλίδα του επιπέδου μεταφοράς (TCP, UDP) ή μια επικεφαλίδα επέκτασης.

- Hop-limit (Όριο βημάτων) : Αυτό το 8 bit πεδίο μειώνεται κατά ένα κάθε φορά που το πακέτο προωθείται στον επόμενο κόμβο. Αν το Hop-limit φτάσει το μηδέν το πακέτο απορρίπτεται. Αντίθετα με το IPv4, όπου το πεδίο time to live παίζει παρόμοιο ρόλο, η πρόθεση στο IPv6 είναι να μην καθορίζεται ο χρόνος ζωής ενός πακέτου στο επίπεδο δικτύου, αλλά σε ανώτερα επίπεδα.

- Source/Destination Address(Διεύθυνση Αφετηρίας/Προορισμού) : Οι 128 bit διευθύνσεις αφετηρίας και προορισμού του πακέτου. Όσον αφορά τη

δεύτερη, αυτή μπορεί να είναι μια unicast, multicast ή anycast διεύθυνση. Αν χρησιμοποιείται επικεφαλίδα δρομολόγησης η διεύθυνση προορισμού μπορεί να είναι ένας από τους κόμβους της διαδρομής και όχι απαραίτητα ο τελικός κόμβος.

3.3 Οι επικεφαλίδες επέκτασης του IPv6

Στο IPv6, προαιρετικές πληροφορίες του επιπέδου δικτύου βρίσκονται σε ξεχωριστές επικεφαλίδες, που τοποθετούνται μεταξύ της βασικής επικεφαλίδας του IPv6 και της επικεφαλίδας του επιπέδου μεταφοράς. Κάθε μια από τις επικεφαλίδες επέκτασης προσδιορίζεται από μια συγκεκριμένη τιμή του πεδίου Next header. Οι επικεφαλίδες επέκτασης είναι ένας πολύ έξυπνος τρόπος να αποφευχθεί η περιττή πληροφορία και επιπλέων να την επεξεργάζεται μόνο η συσκευή που την αφορά η πληροφορία αύτη. Όπως φαίνεται στα παρακάτω παραδείγματα, ένα πακέτο IPv6, μπορεί να μην έχει καμία, να έχει μια ή περισσότερες επικεφαλίδες επέκτασης. Κάθε μια από αυτές προσδιορίζεται από το πεδίο Next Header της προηγούμενης επικεφαλίδας

IPv6 header Next Header = TCP	TCP header	data

Σχήμα 3.2. Καμία επικεφαλίδα επέκτασης

IPv6 header Next Header = Routing header	Routing header Next Header = TCP	TCP header	data

Σχήμα 3.3 Μια επικεφαλίδα επέκτασης

IPv6 header Next Header = Routing Header	Routing header Next Header = Fragment Header	Fragment header Next Header = TCP	TCP header	Data

Σχήμα 3.4. Δυο επικεφαλίδες επέκτασης

Με μια εξαίρεση, οι επικεφαλίδες επέκτασης δεν εξετάζονται ή επεξεργάζονται από τους ενδιάμεσους κόμβους, που βρίσκονται πάνω στη διαδρομή του πακέτου. Αυτό γίνεται μόνο όταν φτάσουν στον κόμβο ή κόμβους (περίπτωση multicast) προορισμού. Εκεί η μετάφραση του πεδίου Next header της βασικής επικεφαλίδας του IPv6, οδηγεί στην επεξεργασία της πρώτης επικεφαλίδας επέκτασης ή της επικεφαλίδας επιπέδου μεταφοράς. Το περιεχόμενο και τα πεδία κάθε επικεφαλίδας επέκτασης καθορίζουν αν πρέπει να προχωρήσουμε στην επόμενη επικεφαλίδα. Γι' αυτό, οι επικεφαλίδες επέκτασης πρέπει να επεξεργάζονται με την ακριβή σειρά με την οποία συναντώνται στο πακέτο.

Η εξαίρεση που αναφέραμε στην προηγούμενη παράγραφο αφορά την επικεφαλίδα επέκτασης Hop-by-Hop, η οποία περιέχει πληροφορίες που πρέπει να εξεταστούν από όλους τους κόμβους πάνω στη διαδρομή του πακέτου, συμπεριλαμβανομένων και των κόμβων αφετηρίας και προορισμού. Η επικεφαλίδα Hop-by-Hop, όταν υπάρχει, πρέπει να ακολουθεί αμέσως μετά από τη βασική επικεφαλίδα. Η παρουσία της δηλώνεται με την τιμή μηδέν στο πεδίο Next header της βασικής επικεφαλίδας του IPv6.

Αν κάποιος κόμβος επεξεργαζόμενος ένα IPv6 πακέτο χρειάζεται να μεταβεί στην επόμενη επικεφαλίδα, αλλά δεν μπορεί να μεταφράσει το πεδίο Next header της προηγούμενης, τότε πρέπει να απορρίψει το πακέτο. Κατόπιν αυτού πρέπει να στείλει ένα ICMP(*Internet Control Message Protocol*) μήνυμα στην πηγή του πακέτου με κωδικό 2 ("Μη αναγνωρίσιμος τύπος Next Header"), που θα περιέχει την τιμή του πεδίου Next Header που δεν μπόρεσε να αναγνωρίσει. Το ίδιο θα πρέπει να γίνεται αν ένας κόμβος συναντήσει τιμή μηδέν στο πεδίο Next Header κάποιας άλλης επικεφαλίδας εκτός από την επικεφαλίδα του IPv6.

Μια πλήρης υλοποίηση του IPv6 περιλαμβάνει τις εξής επικεφαλίδες επέκτασης :

Τιμη πεδίου Next Header	**Περιγραφή**
0	Hop-by-Hop Header
43	Routing Header (RH)
44	Fragmentation Header (FH)
51	Authentication Header (AH)
52	Encapsulated Security Payload (ESP)
59	No Next Header
60	Destination Options Header

Πίνακας 3.5. Οι επικεφαλίδες επέκτασης του IPv6

Όταν χρησιμοποιούνται περισσότερες από μια επικεφαλίδες επέκτασης στο ίδιο πακέτο, αυτές οι επικεφαλίδες θα πρέπει να εμφανίζονται με την εξής σειρά :

1. IPv6 header
2. Hop-by-Hop Options header
3. Destination Options header (επεξεργάζεται από τον τελικό προορισμό, καθώς επίσης και οποιοδήποτε άλλο προορισμό που περιέχεται στην επικεφαλίδα δρομολόγησης RH)
4. Routing header
5. Fragment header
6. Authentication header
7. Encapsulation Security Payload (ESP) header
8. Destination Options header (επεξεργάζεται μόνο από τον τελικό προορισμό όταν γίνεται χρήση επικεφαλίδας δρομολόγησης RH)
9. Upper-layer header

Όπως φαίνεται παραπάνω η επικεφαλίδα επέκτασης προορισμού (Destination Options header) μπορεί να εμφανίζεται δυο φορές σε ένα πακέτο, όταν χρησιμοποιείται επικεφαλίδα δρομολόγησης (RH).

3.4 Επικεφαλίδες Επέκτασης Επιλογών (Options Extension Headers)

Κάθε μια από τις επικεφαλίδες επέκτασης επιλογών περιέχουν έναν αριθμό επιλογών μεταβλητού μήκους. Τέτοιες επικεφαλίδες είναι οι επικεφαλίδες Hop-by-Hop και Προορισμού. Οι επιλογές τους ακολουθούν την εξής μορφή :

Είδος Επιλογής (Option Type)	Μήκος Επιλογής (Opt Data Len)	Δεδομένα Επιλογής (Opt Data)

Σχήμα 3.6. Μορφή των επιλογών των επικεφαλίδων επέκτασης

Option Type : 8-bit προσδιοριστής του είδους επιλογής.

Opt Data Len : 8-bit unsigned integer, που περιέχει το μήκος της επιλογής σε bytes.

Opt Data : Μεταβλητού μήκους δεδομένα της επιλογής.

Οι επιλογές μέσα στην επικεφαλίδα πρέπει να επεξεργάζονται με την αυστηρή σειρά με την οποία εμφανίζονται. Ο παραλήπτης δεν πρέπει να ψάξει στην επικεφαλίδα για την επιλογή που τον ενδιαφέρει χωρίς να έχει επεξεργαστεί πριν τις προηγούμενες επιλογές.

Ο αριθμός Option Type έχει κωδικοποιηθεί με τέτοιο τρόπο ώστε τα δυο υψηλότερα bits να προσδιορίζουν την ενέργεια που θα πρέπει να ληφθεί αν ο IPv6 κόμβος δεν αναγνωρίζει το είδος της επιλογής :

00 – προσπέρασε την επιλογή και συνέχισε την επεξεργασία της επικεφαλίδας..

01 – απόρριψε το πακέτο.

10 – απόρριψε το πακέτο και στείλε μήνυμα ICMP, με κωδικό 2, στην αφετηρία, ενημερώνοντάς την για το είδος της επιλογής.

11 – απόρριψε το πακέτο και μόνο όταν ο προορισμός δεν είναι multicast στείλε ICMP μήνυμα στην πηγή.

Το τρίτο ψηλότερο bit στο Option Type, προσδιορίζει το αν μπορεί το περιεχόμενο της επιλογής να αλλάξει κατά τη δρομολόγηση. Όταν χρησιμοποιείται επικεφαλίδα Authentication στο πακέτο της οποίας το περιεχόμενο μπορεί να αλλάξει κατά τη δρομολόγηση, το περιεχόμενό της δεν πρέπει να λαμβάνεται υπόψη κατά τον υπολογισμό της τιμής authentication.

0 – Η επιλογή δεν αλλάζει κατά τη δρομολόγηση

1 – Η επιλογή μπορεί να αλλάξει κατά τη δρομολόγηση

3.5 Η επικεφαλίδα επέκτασης Hop-by-Hop

Η επικεφαλίδα Hop-by-Hop μεταφέρει προαιρετικές πληροφορίες, που, αν υπάρχουν, θα πρέπει να εξεταστούν από κάθε κόμβο της διαδρομής. Η επικεφαλίδα αυτού του τύπου έχει την τιμή 0 στο πεδίο Next header της επικεφαλίδας IPv6 και ακολουθεί την παρακάτω μορφή.

Next Header	Hdr Ext Len	Επιλογές (Options)

Σχήμα 3.7 Επικεφαλίδα Hop-by-Hop

Next Header : Επιλογέας των 8 bit, που προσδιορίζει το είδος της επικεφαλίδας που ακολουθεί.

Hdr Ext Len : Ένας αριθμός των 8 bit που περιέχει το μήκος της

επικεφαλίδας σε bytes, χωρίς να συνυπολογίζει το πεδίο Next Header στο μήκος αυτό.

Options : Περιέχει επιλογές μεταβλητού μήκους, της μορφής που προσδιορίσαμε παραπάνω.

Μια από τις επιλογές που έχουν οριστεί από το νέο πρωτόκολλο για την επικεφαλίδα Hop-by-Hop είναι η επιλογή μεγάλου πακέτου (*Jumbo Payload Option*).

	Option Type=194	Opt Data len=4
Jumbo Payload Length		

Σχήμα 3.8 Jumbo Payload Option.

Η επιλογή μεγάλου πακέτου χρησιμοποιείται για να στείλει IPv6 πακέτα με μέγεθος μεγαλύτερο των 65,535 bytes. Το πεδίο Jumbo Payload Length είναι το μέγεθος του πακέτου σε bytes εξαιρώντας τη βασική επικεφαλίδα IPv6, και πρέπει να είναι μεγαλύτερο του 65,535. Αν ληφθεί πακέτο με Jumbo Payload μικρότερο ή ίσο τoy 65,535 στέλνεται ICMP μήνυμα στην αφετηρία με κωδικό 0, ενημερώνοντάς την για το λάθος.

Το πεδίο Payload Length της επικεφαλίδας IPv6 πρέπει να τίθεται ίσο με μηδέν όταν το πακέτο έχει Jumbo Payload. Επίσης δεν επιτρέπεται ένα πακέτο να έχει επικεφαλίδα Fragment και Jumbo Payload ταυτόχρονα. Τέλος ένα network interface που δεν υποστηρίζει Jumbo Payload, δε μπορεί να διασυνδεθεί με network interfaces των οποίων το MTU(Maximum Transfer Unit Μέγιστη μονάδα Μεταφοράς) σύνδεσης είναι μεγαλύτερο του 65,575 (40 bytes IPv6 Header συν 65,535 bytes payload). Με την επιλογή Jumbo Payload, το IPv6 έχει την δυνατότητα να υποστηρίξει πακέτα τεράστιου μεγέθους έως και πάνω από 4.000.000.000 bytes (4,000,000,000 B = 3,906,250 KB = 3,814 MB) ! Με αυτή την λειτουργία διευκολύνεται η μετάδοση μεγάλων πακέτων βίντεο επιτρέποντας έτσι στο IPv6 να εκμεταλλεύεται με τον καλύτερο δυνατό τρόπο το διαθέσιμο εύρος ζώνης πάνω σε οποιοδήποτε μέσο μετάδοσης.

3.6 Επικεφαλίδα Δρομολόγησης (Routing Header)

Η επικεφαλίδα δρομολόγησης χρησιμοποιείται όταν η πηγή θέλει το πακέτο να περάσει από ένα ή περισσότερους ενδιάμεσους (συγκεκριμένους) κόμβους στην πορεία του προς τον προορισμό. Η επικεφαλίδα δρομολόγησης έχει κωδικό στο πεδίο Next Header, της αμέσως προηγούμενης επικεφαλίδας ίσο με 43. Η γενικότερη μορφή της επικεφαλίδας δρομολόγησης έχει ως εξής :

Next Header	Hdr Ext Len	Routing Type	Segments Left
type-specific data			

Σχήμα 3.9 Η Επικεφαλίδα Δρομολόγησης

Next Header : Επιλογέας των 8 bit, που προσδιορίζει το είδος της επόμενης επικεφαλίδας.

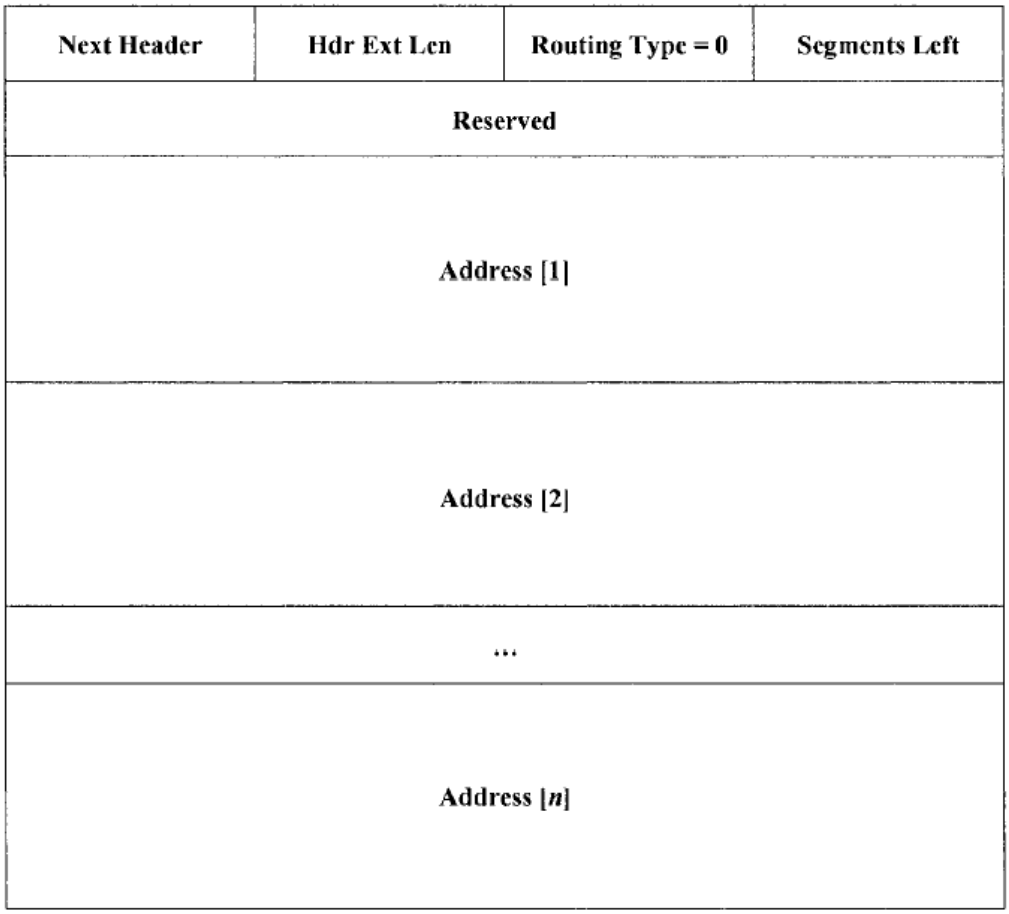
Hdr Ext Len : Ένας αριθμός των 8 bit που περιέχει το μήκος της επικεφαλίδας σε bytes, χωρίς να συνυπολογίζει το πεδίο Next Header στο μήκος αυτό.

Routing Type : 8-bit πεδίο που προσδιορίζει το είδος της επικεφαλίδας δρομολόγησης.

Segments Left : 8-bit πεδίο που περιέχει το πλήθος των ενδιάμεσων κόμβων που το πακέτο πρέπει να επισκεφτεί, ακόμα, για να φτάσει στον τελικό προορισμό.

type-specific data: Πεδίο μεταβλητού μήκους, με μορφή που καθορίζεται από την τιμή του πεδίου Routing Type, και μέγεθος τέτοιο ώστε το συνολικό μήκος της επικεφαλίδας να είναι ακέραιο πολλαπλάσιο των 8 bit.

Η μόνη συγκεκριμένη δομή του routing header που έχει καθοριστεί στο RFC 1883 είναι το type 0 και φαίνεται στο παρακάτω σχήμα



Σχήμα 3.10 Η Επικεφαλίδα Δρομολόγησης type 0

Όταν χρησιμοποιείτε ο τύπος 0 στην επικεφαλίδα δρομολόγησης, η πηγή δεν τοποθετεί τον τελικό προορισμό στην βασική επικεφαλίδα IPv6. Η διεύθυνση του τελικού προορισμού τοποθετείται στο τέλος της λίστας διευθύνσεων (address [n] στο σχήμα) της επικεφαλίδας δρομολόγησης και στην θέση του στην βασική επικεφαλίδα IPv6 τοποθετείται ο πρώτος μεσολαβητής κόμβος που επιθυμεί η πηγή να περάσει το πακέτο. Η επικεφαλίδα δρομολόγησης δεν θα εξεταστεί ούτε θα επεξεργαστεί έως ότου φτάσει στον προορισμό που αναγράφεται στην βασική κεφαλίδα. Σε αυτό το σημείο το πακέτο θα επεξεργαστεί και θα τροποποιηθεί από τον κόμβο αλλάζοντας το πεδίο destination στην βασική επικεφαλίδα IPv6 με τον επόμενο επιθυμητό προορισμό στην λίστα διευθύνσεων. Επίσης θα μειώσει κατά ένα το πεδίο segments left. Η διαδικασία αυτή θα επαναλαμβάνεται μέχρι το πακέτο να φτάσει στον τελικό του προορισμό. Όταν το πεδίο rooting type είναι 0 θα

πρέπει επίσης να μην περιέχεται καμιά διεύθυνση εκπομπής multicast ούτε στην βασική κεφαλίδα IPv6 ούτε στην επικεφαλίδα δρομολόγησης.

3.7 Επικεφαλίδα Διάσπασης (Fragment Header)

Η Επικεφαλίδα Διάσπασης χρησιμοποιείται από την πηγή για να στείλει πακέτα μεγαλύτερα από το MTU μονοπατιού(το μέγιστο μήκος πακέτου που υποστηρίζεται από όλους τους συνδέσμους της διαδρομής). Αντίθετα με το IPv4 η διάσπαση (*fragmentation*) των πακέτων γίνεται μόνο από την πηγή και όχι από τους δρομολογητές που βρίσκονται πάνω στη διαδρομή, έτσι οι δρομολογητές γίνονται πιο αποδοτικοί. Έχει κωδικό 44 στο πεδίο Next Header της προηγούμενης επικεφαλίδας και ακολουθεί την παρακάτω μορφή.

Next Header	Reserved	Fragment Offset	Res	M flag
Identification				

Σχήμα 3.11 Η Επικεφαλίδα Διάσπασης

Next Header : Επιλογέας των 8 bit, που προσδιορίζει το είδος της επόμενης επικεφαλίδας.

Reserved : αχρησιμοποίητο πεδίο των 8 bit

Fragment Offset : unsigned integer των 13 bit. Περιέχει την απόσταση των δεδομένων που ακολουθούν αυτήν την επικεφαλίδα από την αρχή του αρχικού πακέτου μετρημένη σε λέξεις των 64 bit.

Res : 2-bit αχρησιμοποίητο πεδίο. Αρχικοποιείται σε μηδέν κατά τη μετάδοση και αγνοείται κατά τη λήψη.

M flag : 1 = κι άλλα κομμάτια, 0=τελευταίο κομμάτι.

Identification : Πεδίο μήκους 32 bit. Θα αναφερθούμε σ’ αυτό παρακάτω.

Για να μπορέσει να στείλει ένα πακέτο αρκετά μεγάλο για να χωρέσει στο MTU μονοπατιού, η αφετηρία πρέπει να χωρίσει το αρχικό πακέτο σε κομμάτια και να στείλει το κάθε ένα από αυτά ως ξεχωριστό πακέτο. Το αρχικό πακέτο θα επανενωθεί στον τελικό προορισμό.

Για κάθε πακέτο προς διάσπαση, η πηγή δημιουργεί μια τιμή Identification. Η τιμή αυτή πρέπει να είναι διαφορετική από το Identification κάθε άλλου πρόσφατου πακέτου με την ίδια πηγή και προορισμό. Αν το πακέτο διαθέτει επικεφαλίδα δρομολόγησης ο προορισμός που μας ενδιαφέρει είναι ο τελικός προορισμός. Το ίδιο το πεδίο Identification γι' αυτό το σκοπό έχει επιλεγεί να έχει 32 bit μήκος (2^{32}=4 δισεκατομμύρια περίπου δυνατά μοναδικά identification), έτσι ώστε να διασφαλίζεται η μοναδικότητα του πεδίου Identification.

Το αρχικό, πριν τη διάσπαση, πακέτο θεωρητικά αποτελείται από δυο μέρη.

αρχικό πακέτο :

Μη διασπώμενο μέρος	Διασπώμενο μέρος

Σχήμα 3.12 Τα δυο μέρη του αρχικού πακέτου

Το μη διασπώμενο μέρος αποτελείται από την επικεφαλίδα του IPv6 μαζί με τις όποιες επικεφαλίδες επέκτασης χρειάζεται να επεξεργαστούν από τους ενδιάμεσους κόμβους της διαδρομής.

Το διασπώμενο μέρος αποτελείται από το υπόλοιπο του πακέτου, δηλαδή τις επικεφαλίδες επέκτασης που δε χρειάζεται να επεξεργαστούν από τους ενδιάμεσους κόμβους, την επικεφαλίδα ανωτέρου επιπέδου και τα δεδομένα. Το διασπώμενο μέρος διαιρείται σε κομμάτια, όπου το καθένα (ίσως εκτός από το τελευταίο) έχει μήκος ίσο με ένα ακέραιο πολλαπλάσιο των 8 bytes. Έπειτα τα κομμάτια μεταδίδονται με τη μορφή πακέτων κομματιών (*fragment packets*) όπως φαίνεται παρακάτω :

αρχικό πακέτο :

Μη διασπώμενο μέρος	Πρώτο κομμάτι	Δεύτερο κομμάτι	.....	Τελευταίο κομμάτι

Σχήμα 3.13 Διάσπαση και μεταφορά ενός πακέτου

Πακέτα κομματιών :

Μη διασπώμενο μέρος	Επικεφαλίδα διάσπασης	Πρώτο κομμάτι

Μη διασπώμενο μέρος	Επικεφαλίδα διάσπασης	Δεύτερο κομμάτι

*
*
*

Μη διασπώμενο μέρος	Επικεφαλίδα διάσπασης	Τελευταίο κομμάτι

Σχήμα 3.14 Διάσπαση και μεταφορά ενός πακέτου (αναλυτικά)

Κάθε πακέτο κομματιού αποτελείται από :

1. Το μη διασπώμενο μέρος του αρχικού πακέτου με το πεδίο μήκους πακέτου (*Payload Length*) της επικεφαλίδας IPv6 να περιέχει τώρα το μέγεθος του κομματιού, και το πεδίο Next header της τελευταία επικεφαλίδας του μη διασπώμενου μέρους να έχει αλλαχθεί σε 44.

2. Μια Επικεφαλίδα Διάσπασης (*Fragmentation Header*) που περιέχει :

   - Το πεδίο Next Header που αντιστοιχεί στην πρώτη επικεφαλίδα, που ανήκει στο διασπώμενο μέρος του αρχικού πακέτου.
   - Το Fragment Offset που περιέχει την απόσταση του κομματιού, μετρημένη σε λέξεις των 8 bytes, από την αρχή του διασπώμενου μέρους του αρχικού πακέτου
   - Η flag M που έχει τιμή 0 αν το κομμάτι είναι το τελευταίο, αλλιώς έχει τιμή 1
   - Το πεδίο Identification που αντιστοιχεί στο αρχικό πακέτο.

3. Το ίδιο το κομμάτι (fragment) του διασπώμενου μέρους του αρχικού πακέτου

Εφόσον τα πακέτα δεν τεμαχίζονται στην πορεία αλλά εξ΄αρχής από τον αποστολέα, θα πρέπει ο ίδιος πριν την αποστολή τους να εκτελέσει έναν αλγόριθμο εύρεσης μονοπατιού που του επιτρέπει να μάθει το μικρότερο MTU (maximum transfer unit) διαδρομής, δηλαδή το μικρότερο μέγεθος πακέτου που επιτρέπεται να περάσει από την επιλεγμένη διαδρομή. Γνωρίζοντας αυτό ο αποστολέας μπορεί να τεμαχίσει τα πακέτα και να τα στείλει. Διαφορετικά η πηγή θα τεμαχίσει τα πακέτα σε μέγεθος 576bytes, το οποίο είναι το μικρότερο δυνατό MTU που πρέπει να υποστηρίζεται από όλα τα υποδίκτυα. Τέλος, στον προορισμό τα πακέτα ανασυντίθενται με βάση την πληροφορία που βρίσκεται στους Fragment headers.

3.8 Επικεφαλίδα Επιλογών Προορισμού(Destination Options Header)

Η Επικεφαλίδα Επιλογών Προορισμού μεταφέρει προαιρετικές πληροφορίες, που χρειάζεται να εξεταστούν μόνο από τους κόμβους προορισμού. Έχει κωδικό 60 στο πεδίο Next Header της προηγούμενης επικεφαλίδας και έχει την εξής μορφή :

Next Header	Hdr Ext Len	Options(Επιλογές)

Σχήμα 3.15 Επικεφαλίδα Επιλογών Προορισμού

Next Header : Επιλογέας των 8 bit, που προσδιορίζει το είδος της επικεφαλίδας που ακολουθεί.

Hdr Ext Len : Ένας αριθμός των 8 bit που περιέχει το μήκος της επικεφαλίδας σε bytes, χωρίς να συνυπολογίζει το πεδίο Next Header στο μήκος αυτό.

Options : Περιέχει επιλογές μεταβλητού μήκους, της μορφής που προσδιορίσαμε παραπάνω.

Η μορφή της επικεφαλίδας επιλογών προορισμού είναι παρόμοια με την επικεφαλίδα Hop-by-hop.

3.9 Authentication Header

Αυτή η επικεφαλίδα προσφέρει ένα μηχανισμό υπολογισμού ενός κρυπτογραφικού αθροίσματος ελέγχου πάνω στο πακέτο IPv6. Ήρθε για να αντικαταστήσει το Header Checksum από το IPv4. Περιγράφεται αναλυτικά στο Κεφάλαιο 6.

3.10 Encapsulation Security Payload

Αυτή η επικεφαλίδα θα είναι πάντα η τελευταία μη κρυπτογραφημένη επικεφαλίδα οποιουδήποτε πακέτου. Δείχνει ότι το υπόλοιπο μέρος του πακέτου είναι κρυπτογραφημένο, και δίνει στοιχεία για τον εξουσιοδοτημένοπροορισμό να το αποκρυπτογραφήσει. Περιγράφεται αναλυτικά στο Κεφάλαιο 6.

ΠΗΓΗ:

- Π. Γανός, Α. Γκάμας, Α. Καραλιώτας, Χ. Μπούρας, Δ. Πρίμπας, Κ. Στάμος, IPv6: Το πρωτόκολλο και οι τεχνικές μετάβασης και μεταφερσιμότητας, κεφάλαιο 3.1, ISBN 960-442-277-4
- William Stallings, High-Speed Networks, TCP/IP and ATM Design Principles, Κεφάλαιο 11.2, ISBN*:* 0-13-525965-7
- Ed Taylor, Tcp/Ip Complete, κεφάλαια 8.1 εως 8.8,ISBN 0-07-063400-9
- Youngsong Mun, Hyewon K. Lee, Understanding IPv6, κεφάλαιο 2, ISBN 9780387256146

4. ΔΡΟΜΟΛΟΓΗΣΗ

4.1 Τα πρωτόκολλα δρομολόγησης

Τα πρωτόκολλα δρομολόγησης χωρίζονται σε 2 κατηγορίες: Interior Gateway Protocols (IGPs), τα οποία χρησιμοποιούνται για την δρομολόγηση εντός των Αυτόνομων Συστημάτων (Autonomous Systems - AS) και Exterior Gateway Protocols (EGPs) , τα οποία χρησιμοποιούνται για την δρομολόγηση μεταξύ Αυτόνομων Συστημάτων. Ένα Αυτόνομο Σύστημα είναι ένα δίκτυο του οποίου τη διαχείριση έχει ένας φορέας. Τα σημαντικότερα πρωτόκολλα δρομολόγησης είναι τα RIP και OSPF (IGP πρωτόκολλο) και το BGP (EGP πρωτόκολλο). Και τα τρία έχουν επεκταθεί ώστε να υποστηρίζουν το IPv6. Αυτές τις τροποποιήσεις και επεκτάσεις θα εξετάσουμε παρακάτω.

Η φιλοσοφία των πρωτοκόλλων δρομολόγησης έχει αλλάξει ελάχιστα στο IPv6. Αυτό είναι συνέπεια του γεγονότος ότι περιορίστηκε το μέγεθος των καταχωρήσεων στους πίνακες δρομολόγησης και επομένως οι υπάρχοντες αλγόριθμοι δρομολόγησης απαιτούν ελάχιστη τροποποίηση για να επιτευχθεί βέλτιστη απόδοση. Οι περισσότερες τροποποιήσεις μάλιστα έγιναν απλώς για να επεκτείνουν τα υπάρχοντα πρωτόκολλα στο να χειρίζονται τις διευθύνσεις IPv6 που έχουν μεγαλύτερο μέγεθος, ενώ παράλληλα καταργήθηκαν διαδικασίες που αντάλλασσαν πληροφορίες πιστοποίησης, διότι η πιστοποίηση ενσωματώθηκε στο πακέτο IPv6, καθώς και κάποιες πληροφορίες που αφορούν πεδία του IPv4 πακέτου (όπως το πεδίο Type of Service).

Έτσι για τη δρομολόγηση εντός του δικτύου ενός οργανισμού (Interior Routing) τροποποιήθηκαν τα ήδη υπάρχοντα πρωτόκολλα δρομολόγησης όπως το RIP και OSPF για να μπορούν να λειτουργήσουν με το νέο πρωτόκολλο IPv6. Τέλος, για τη δρομολόγηση στο εξωτερικό του δικτύου ενός οργανισμού (Exterior Routing) χρησιμοποιείται το πρωτόκολλο BGP, στο οποίο έχουν γίνει οι κατάλληλες προσθήκες προκειμένου να υποστηρίζει πολλαπλά δικτυακά πρωτόκολλα σύμφωνα με το RFC 2545.

4.2 Το πρωτόκολλο RIPv6

Το πρωτόκολλο Routing Information Protocol (RIP) προέρχεται από το IGP πρωτόκολλο το οποίο είχε αρχικά σχεδιαστεί από την Xerox για τα δίκτυα XNS. Είναι ένα distance vector (πίνακα αποστάσεων) πρωτόκολλο όπου κάθε δρομολογητής αποστέλλει τον πίνακα αποστάσεων του στους γειτονικούς δρομολογητές κάθε 30 δευτερόλεπτα. Στους πίνακες δρομολόγησης αποθηκεύεται μόνο η καλύτερη διαδρομή προς κάθε κατεύθυνση. Ο βασικός περιορισμός του πρωτοκόλλου είναι ότι ο μέγιστος αριθμός βημάτων (hops) που υποστηρίζει είναι 15 βήματα και κάθε προορισμός με απόσταση μεγαλύτερη των 15 βημάτων θεωρείται μη προσβάσιμος. Επιπλέον, το RIP αγνοεί τις ταχύτητες μετάδοσης των δικτυακών συνδέσεων και επιτρέπει τον ορισμό κόστους ή άλλων μετρικών οι οποίες βασίζουν τη δρομολόγηση μόνο στην ελαχιστοποίηση του αριθμού των βημάτων που απαιτούνται για την πρόσβαση σε έναν προορισμό. Σε περίπτωση αλλαγών στην τοπολογία του δικτύου το RIP είναι αργό στην προσαρμογή στη νέα τοπολογία του δικτύου. Για τους παραπάνω λόγους το RIP χρησιμοποιείται κυρίως σε μικρά δίκτυα.

Η σχεδίαση του πρωτοκόλλου RIP εμπεριέχει ορισμένους περιορισμούς, όπως:

- Τη χρήση σε δίκτυα με διάμετρο (το μέγιστο μονοπάτι) το πολύ 15 βήματα (hops).
- Την κατάσταση «μετρώντας το άπειρο» (counting to infinity), η οποία μπορεί να οδηγήσει σε μεγάλες καθυστερήσεις ή μεγάλη κατανάλωση εύρους ζώνης, και η οποία εμφανίζεται όταν ένας δρομολογητής στέλνει λανθασμένη πληροφορία σε έναν άλλο δρομολογητή, ο οποίος στέλνει επιπλέον λανθασμένη πληροφορία σε έναν άλλο δρομολογητή κ.ο.κ., και η οποία μπορεί να προκύψει όταν, για παράδειγμα, χαλάσει ένας σύνδεσμος που λειτουργούσε πριν, καθώς το πρωτόκολλο θα αργήσει να το αντιληφθεί.
- Τον υπολογισμό του «Βέλτιστου» μονοπατιού Βάσει σταθερών μετρικών και άρα την αδυναμία προσαρμογής σε παραμέτρους όπως μέτρηση καθυστέρησης, φόρτος δικτύου ή αξιοπιστία γραμμών.

Το RIPv6 είναι η έκδοση του RIP η οποία μπορεί να χρησιμοποιηθεί σε δίκτυα IPv6. Το RIPv6 χειρίζεται τις νέες 128bit διευθύνσεις του IPv6 χωρίς να παρέχει κάποια νέα χαρακτηριστικά και χωρίς να έχουν εξαλειφθεί οι περιορισμοί οι οποίοι αναφέρονται παραπάνω. Ο λόγος για την παραπάνω επιλογή είναι η ανάγκη για το πρωτόκολλο RIPv6 να παραμείνει όσο πιο απλό γίνεται ετσι ώστε να μπορεί να υλοποιηθεί σε πολύ απλές συσκευές στις οποίες η υλοποίηση του OSPFv6 θα ήταν προβληματική. Το RIPv6 χρησιμοποιεί δύο ειδών μηνύματα του τύπου αίτηση (request) και απόκριση (response) τα οποία μεταδίδονται με τη χρήση του πρωτοκόλλου UDP User Datagram Protocol). Στο RIPv6 ένας περιορισμένος αριθμός από προορισμούς επιτρέπεται σε κάθε πακέτο έτσι ώστε το IPv6 πακέτο να μην ξεπερνά το MTU.

Κάθε δρομολογητής που υλοποιεί το RIPv6 έχει στον πίνακα δρομολόγησης εγγραφές για κάθε προορισμό σε όλο το δίκτυο που τρέχει το RIPv6. Κάθε εγγραφή πρέπει να περιέχει τουλάχιστον την ακόλουθη πληροφορία:

- Το IPv6 πρόθεμα του προορισμού.
- Μία μετρική που αντιπροσωπεύει το ολικό κόστος του να πάει ένα πακέτο από το δρομολογητή στον προορισμό, η οποία είναι το άθροισμα από τα κόστη για όλες τις γραμμές που πρέπει να διασχίσει για να φτάσει στον προορισμό.
- Την IPv6 διεύθυνση του επόμενου δρομολογητή πάνω στο μονοπάτι που πρέπει να ακολουθηθεί για τον προορισμό, εκτός και αν ο προορισμός βρίσκεται στο ίδιο δίκτυο με το συγκεκριμένο δ*ρομολογητή.*
- Ένα flag που δείχνει αν η πληροφορία στο δρομολογητή έχει αλλάξει πρόσφατα.
- Μετρητές που σχετίζονται με τη δρομολόγηση.

4.3 Το πρωτόκολλο OSPFv6

Το πρωτόκολλο Open Shortest Path First (OSPF) προσφέρει ορισμένα πλεονεκτήματα σε σχέση με το πρωτόκολλο RIP:

- Δυνατότητα για καθορισμό ιεραρχικών επίπεδων διευθύνσεων.

- Χρήση σε μεγαλύτερα δίκτυα.
- Υπολογισμό πολλαπλών βέλτιστων μονοπατιών για καλύτερη εξισορρόπηση της κίνησης.
- Δυνατότητα χρήσης μάσκας υποδικτύου μεταβλητού μήκους.

Το πρωτόκολλο OSPF αποτελεί ένα πρωτόκολλο το οποίο στηρίζεται στην έννοια της ιεραρχίας. Η κορυφή της ιεραρχίας είναι ένα Αυτόνομο Σύστημα (Autonomous System - AS) το οποίο μπορεί να χωριστεί σε περιοχές (areas), στις οποίες περιέχονται ομάδες διασυνδεδεμένων υποδικτύων. Η δρομολόγηση σε κάθε περιοχή ονομάζεται "intra-area" και η δρομολόγηση ανάμεσα σε διαφορετικές περιοχές ονομάζεται "inter-area". Κάθε AS διαθέτει μια περιοχή κορμού (backbone area).

Ένας OSPF δρομολογητής μπορεί να κατηγοριοποιηθεί σε μια από τις παρακάτω περιπτώσεις:

- Εσωτερικός δρομολογητής (internal router): Είναι ένας δρομολογητής ο οποίος συνδέει υποδίκτυα τα οποία ανήκουν στην ίδια περιοχή. Οι δρομολογητές αυτοί χρησιμοποιούν μια μόνο οντότητα (instance) του OSPF αλγορίθμου. Δρομολογητές οι οποίοι συνδέονται μόνο στην περιοχή κορμού ανήκουν σε αυτή την κατηγορία.
- Συνοριακός δρομολογητής περιοχής (area border router): Είναι ένας δρομολογητής ο οποίος συνδέεται στην περιοχή κορμού (backbone area) και σε μία ή περισσότερες περιοχές. Οι δρομολογητές αυτοί εκτελούν περισσότερες από μία οντότητες του OSPF αλγορίθμου, μια για το δίκτυο κορμού και μια για κάθε περιοχή στην οποία συνδέονται. Οι δρομολογητές αυτοί συλλέγουν πληροφορίες από τις περιοχές στις οποίες είναι συνδεδεμένοι και τις προωθούν στην περιοχή κορμού.
- Δρομολογητής περιοχής κορμού (backbone router): Είναι ένας δρομολογητής ο οποίος συνδέεται μόνο στην περιοχή κορμού. Οι δρομολογητές αυτοί συνδέονται σε περισσότερες από μία περιοχές μέσω των αντίστοιχων συνοριακών δρομολογητών (border routers). Πρέπει να τονίσουμε ότι οι δρομολογητές της περιοχής κορμού οι οποίοι έχουν

συνδέσεις μόνο στο δίκτυο κορμού ανήκουν στην κατηγορία των εσωτερικών δρομολογητών (internal routers).

- Συνοριακός δρομολογητής AS (AS boundary router): Είναι ένας δρομολογητής ο οποίος ανταλλάσσει πληροφορίες δρομολόγησης με δρομολογητές οι οποίοι ανήκουν σε διαφορετικά AS. Σύμφωνα με αυτό τον ορισμό, ένας συνοριακός δρομολογητής AS είναι είτε ένας εσωτερικός δρομολογητής είτε ένας συνοριακός δρομολογητής περιοχής.

Οι αλλαγές που έγιναν στο πρωτόκολλο OSPF για να υποστηρίζει το IPv6 εστιάζονται κυρίως σε θέματα διαφορετικής σημειολογίας μεταξύ IPv4 και IPv6 και χειρισμού των μεγαλύτερων IPv6 διευθύνσεων. Οι θεμελιώδεις μηχανισμοί του πρωτοκόλλου παραμένουν ίδιοι. Οι Βασικές διαφορές του πρωτοκόλλου OSPFv6 σε σχέση με το πρωτόκολλο OSPF είναι οι εξής:

- Το πρωτόκολλο OSPFv6 λειτουργεί πάνω στη λογική των συνδέσεων και όχι των υποδικτύων. Μία σύνδεση μπορεί να περιλαμβάνει περισσότερα του ενός υποδίκτυα και δύο κόμβοι μπορούν να επικοινωνούν απευθείας αν βρίσκονται στην ίδια σύνδεση, ακόμα και αν ανήκουν σε διαφορετικά υποδίκτυα.
- Υπάρχει η δυνατότητα να τρέχουν πολλαπλές οντότητες του OSPF αλγορίθμου ταυτόχρονα στην ίδια σύνδεση. Αυτή η δυνατότητα επιτρέπει, για παράδειγμα, σε διαφορετικές OSPF περιοχές που μοιράζονται κάποια σύνδεση να παραμένουν ξεχωριστές.
- Το πρωτόκολλο OSPF υποθέτει ότι κάθε δρομολογητής έχει μια link-local unicast διεύθυνση για κάθε φυσική του σύνδεση. Τα OSPF πακέτα στέλνονται χρησιμοποιώντας τη link-local διεύθυνση της σύνδεσης ως πηγή. Ένας δρομολογητής μαθαίνει τις link-local διευθύνσεις όλων των άλλων δρομολογητών στις συνδέσεις του και τις χρησιμοποιεί στην πληροφορία για τον επόμενο κόμβο κατά την προώθηση των πακέτων.
- Δεν γίνεται πλέον πιστοποίηση (authentication) από πρωτόκολλο δρομολόγησης αφού το IPv6 έχει ενσωματωμένες τέτοιες δυνατότητες. Για προστασία από αλλοίωση των δεδομένων λόγω λαθών χρησιμοποιείται το

στάνταρτ 16-bit άθροισμα ελέγχου (checksum) του IPv6, το οποίο καλύπτει όλο το OSPF πακέτο και την προπορευόμενη IPv6 επικεφαλίδα.

- Οι γειτονικοί δρομολογητές σε μία δεδομένη σύνδεση αναγνωρίζονται πάντοτε από το Router ID τους, ενώ στην προηγούμενη έκδοση αναγνωρίζονταν άλλοτε από το Router ID τους και άλλοτε από τις IPv4 διευθύνσεις των συνδέσεων τους.

4.4 Το πρωτόκολλο BGP

Το πιο διαδεδομένο EGP πρωτόκολλο είναι το πρωτόκολλο BGP, το οποίο χρησιμοποιεί το TCP για μεγαλύτερη αξιοπιστία κατά την επικοινωνία μεταξύ Αυτόνομων Συστημάτων (AS). Η βασική λειτουργία του BGP είναι η ανταλλαγή πληροφορίας μεταξύ Αυτόνομων Συστημάτων ως προς το σε ποια δίκτυα μπορεί το καθένα να έχει πρόσβαση και κατά συνέπεια το σχηματισμό ενός γράφου που αναπαριστά όλα τα δυνατά μονοπάτια. Η τελευταία έκδοση του BGP είναι η BGP-4.

Το πρωτόκολλο BGP χρησιμοποιεί τους παρακάτω τέσσερις τύπους μηνυμάτων:

- OPEN: Το μήνυμα αυτό αρχικοποιεί την BGP επικοινωνία.
- UPDATE: Το μήνυμα αυτό χρησιμοποιείται για τη μεταφορά πληροφορίας σχετικά με τη δρομολόγηση.
- KEEPALIVE: Το μήνυμα αυτό ανταλλάσσεται σε τακτά χρονικά διαστήματα για να επιβεβαιώσει αν είναι δυνατή η επικοινωνία.
- NOTIFICATION: Το μήνυμα αυτό στέλνεται όταν γίνει αντιληπτό κάποιο λάθος και προκαλεί τη διακοπή της BGP σύνδεσης.

Το πρωτόκολλο BGP-4 αλλά και γενικότερα τα πρωτόκολλα της κατηγορίας του είναι γενικά ανεξάρτητα του πρωτοκόλλου δικτύου, γι' αυτό το πρωτόκολλο BGP-4 είναι κατάλληλο και για το IPv6, χωρίς την ανάγκη ιδιαίτερων μετατροπών.

Αν και οι διευθύνσεις link-local χρησιμοποιούνται για να προσδιοριστεί το επόμενο βήμα (hop) κατά τη δρομολόγηση από το πρωτόκολλο RIPng και το πρωτόκολλο OSPF και κάθε δρομολογητής έχει μία διεύθυνση link-local επόμενου βήματος (hop) για όλους τους άμεσα συνδεδεμένους δρομολογητές (αυτούς δηλαδή που έχουν το ίδιο πρόθεμα υποδικτύου), δεν είναι κατάλληλες να χρησιμοποιηθούν από το πρωτόκολλο BGP για να ορίσουν το επόμενο βήμα κατά τη δρομολόγηση λόγω της φύσης του πρωτοκόλλου BGP ως EGP πρωτόκολλο. Έτσι είναι ορισμένες φορές απαραίτητο να προσδιορίζεται το επόμενο βήμα από ένα πεδίο που περιέχει μία οικουμενική και μία διεύθυνση link-local.

ΠΗΓΗ:

- Π. Γανός, Α. Γκάμας, Α. Καραλιώτας, Χ. Μπούρας, Δ. Πρίμπας, Κ. Στάμος, IPv6: Το πρωτόκολλο και οι τεχνικές μετάβασης και μεταφερσιμότητας, κεφάλαιο 3.3, εκδόσεις Ελληνικά Γράμματα, ISBN 960-442-277-4

ΚΕΦΑΛΑΙΟ 5. ΜΕΤΑΒΑΣΗ ΑΠΟ ΤΟ IPv4 ΣΤΟ IPv6-ΒΑΘΜΟΣ ΕΤΟΙΜΟΤΗΤΑΣ

5.1 Γιατί η Μετάβαση από IPv4 σε IPv6 είναι αναγκαία

Θα έλεγε κανείς ότι το IPv4 δουλεύει αρκετά καλά, ιδιαίτερα λαμβάνοντας υπόψη την ηλικία του. Πολλά συστήματα ακόμα ανά τον κόσμο χρησιμοποιούν το πρωτόκολλο IPv4, οπότε κάθε σύστημα θα πρέπει να αναβαθμιστεί, προκειμένου να υποστηρίζεται το IPv6. Πρόκειται για ένα αριθμό συστημάτων της τάξης των 100 εκατομμυρίων, που χρησιμοποιούν διάφορες εκδόσεις δικτυακού λογισμικού για TCP/IP, που τρέχουν σε μια πληθώρα λειτουργικών συστημάτων και υλικού.

Υπάρχει το ερώτημα αν θα μπορούσε να αποφευχθεί το κόστος που μια ενδεχόμενη αναβάθμιση στο IPv6 θα μπορούσε να επιφέρει. Βασικά όλα εξαρτώνται από το βαθμό που ένα νέο πρωτόκολλο είναι αναγκαίο. Αν το μόνο πρόβλημα που αντιμετώπιζε το IPv4 ήταν η έλλειψη διευθύνσεων, θα μπορούσε να επιβιώσει για κάμποσο ακόμα χρησιμοποιώντας τεχνικές όπως το NAT (Network Address Translation), το CIDR (Classless Inter-Domain Routing) και το subnetting. Φυσικά αυτές είναι βραχυπρόθεσμες λύσεις που χρησιμοποιούνται χρόνια τώρα. Η ανάπτυξη του διαδικτύου στο απώτερο μέλλον δεν θα είναι δυνατή αν το πρωτόκολλο IP δεν αναβαθμιστεί.

Το IPv4 επιδέχεται κι άλλες βελτιώσεις εκτός από την αύξηση του χώρου διευθύνσεων. Αυτές έχουν να κάνουν με τη διαχείριση (administration), με τη δρομολόγηση (routing), την ποιότητα υπηρεσιών, την ιεραρχία και την ασφάλεια. Το IPv4 είναι γνωστό οτι δουλεύει καλά, άρα επιδέχεται βελτιώσεων, τι θα ήταν επιθυμητό να προστεθεί και τι όχι είναι προς εξέταση. Οπότε η μετάβαση από το IPv4 δεν έχει να κάνει με την αντικατάσταση μιας γνωστής ποσότητας με μια άγνωστη. Οι σχεδιαστές του IPv6 έχτισαν το καινούριο πρωτόκολλο πάνω στο IPv4, κρατώντας ότι δούλευε καλά, βελτιώνοντας το, αφαιρώντας ότι ζημίωνε την λειτουργικότητα και την απόδοση, ενώ προσέθεσαν καινούρια χαρακτηριστικά που ήταν φανερό ότι χρειάζονταν μεγάλη αλλαγή σε:

1. **Θέματα έλλειψης διευθύνσεων**: Αν και οι χρήστες πιστεύουν ότι αυτός εμφανίζεται σαν ο βασικότερος λόγος αναβάθμισης του IPv4, ουσιαστικά πρόκειται μόνο για ένα από τα προβλήματα που απασχολούν την κοινότητα του Διαδικτύου.

2. **Θέματα απόδοσης**: Παρ' όλο που το IP λειτουργεί αποδοτικά τα 20 και πλέον χρόνια που χρησιμοποιείται, υπάρχουν πάρα πολλές βελτιώσεις που μπορούν να γίνουν. Οι διαχειριστές γνωρίζουν καλύτερα από όλους το κόστος διαχείρισης των routing entries εξαιτίας της έλλειψης επιπέδων ιεραρχίας στις IP διευθύνσεις. Επίσης αρκετές εφαρμογές απαιτούν υποστήριξη ποιότητας υπηρεσίας (QoS) από το IPv4 και προσπαθούν να ξεπεράσουν αυτή του την αδυναμία με χρήση άλλων πρωτοκόλλων σε υψηλότερα επίπεδα, μην πετυχαίνοντας όμως τα αναμενόμενα.

3. **Θέματα ασφάλειας**: Μετά την τεράστια εξάπλωση που γνώρισε το Διαδίκτυο και τη χρήση του σε κάθε είδος οικονομικής συναλλαγής διαπιστώθηκε ότι η ασφάλεια δεν μπορεί να απασχολεί μόνο τις εφαρμογές, αλλά το ίδιο το IP θα πρέπει να έχει μηχανισμούς ασφάλειας.

4. **Θέματα αυτόματης ανάθεσης διεύθυνσης**: Είναι γνωστό ότι οι ρυθμίσεις του IPv4 στους κόμβους είναι σχετικά πολύπλοκη διαδικασία. Οι χρήστες θα επιθυμούσαν μία λειτουργία "plug and play" με την έννοια του να μπορεί κάποιος να συνδέει τον υπολογιστή του στο δίκτυο IP και αυτός να μπορεί αυτόματα να βρίσκει τις ρυθμίσεις του. Οι ανάγκες των συνεχώς αυξανόμενων χρηστών που δεν έχουν σταθερό χώρο εργασίας (mobile users) απαιτούν αυτόματες ρυθμίσεις ανεξάρτητα του δικτύου που χρησιμοποιούν κάθε φορά για να συνδεθούν

5.2 Διαδικασίες-τεχνικές μετάβασης στο IPv6

Για να δουλέψει το IPv6, δεν χρειάζεται να αναβαθμιστούν όλα τα interfaces που είναι συνδεδεμένα στο δίκτυο την ίδια στιγμή. Φυσικά κάτι τέτοιο δεν είναι

εφικτό ούτως ή άλλως, λόγω του μεγέθους και των πολλών ειδικών περιπτώσεων του προβλήματος. Οι άνθρωποι που εργάζονται πάνω στη μετάβαση στο IPv6 έχουν εφεύρει μηχανισμούς για να γίνει αυτή σταδιακά και με μικρό κόστος. Η αναβάθμιση των είδη υπαρχόντων δικτύων σε δίκτυα IPv6 μπορεί να γίνει με σχετικά μικρές επιπτώσεις, εφόσον χρησιμοποιηθεί μεθοδικότητα και ακολουθηθούν έξυπνες λύσεις. Παρακάτω περιγράφονται μερικοί από τους μηχανισμούς που θα οδηγήσουν σε μια ομαλή μετάβαση στο IPv6.

Εκτός από το γεγονός ότι η μετάβαση στο IPv6 θα γίνει σταδιακά, θα γίνει επίσης και σχετικά αργά, καθώς λίγοι θα είναι αρχικά οι “τολμηροί” χρήστες που θα έχουν μεγάλη ανάγκη από τις λύσεις που προσφέρει το IPv6. Γιατί είναι γνωστό πως κάθε τι καινούριο ενδέχεται να έχει bugs και γενικότερα προβλήματα. Τα πράγματα θα αλλάζουν σιγά-σιγά καθώς οι σχεδιαστές υλικού και λογισμικού θα αποκτούν πείρα πάνω στο IPv6 και θα προσφέρουν ολοκληρωμένες και bug-free λύσεις για IPv6. Αναμένεται, δηλαδή, ότι το IPv6 θα συνυπάρχει με το IPv4 για πολύ καιρό –ίσως και για πάντα.

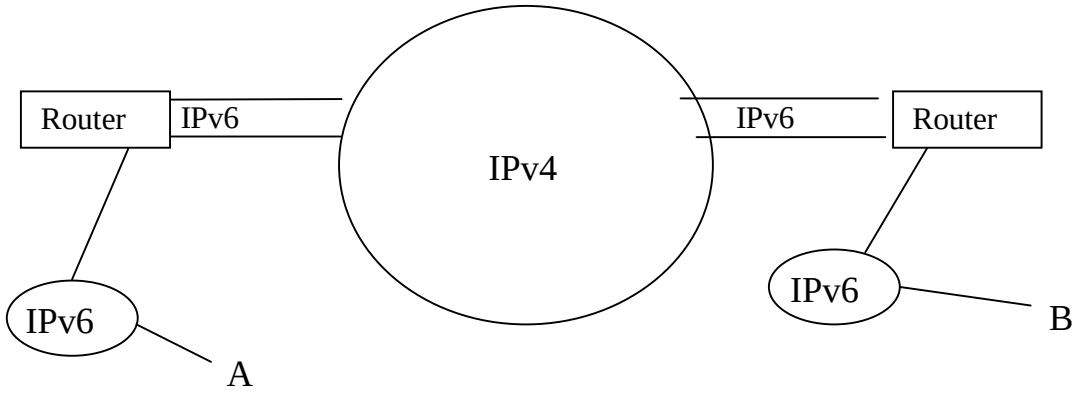
Οι περισσότερες στρατηγικές για τη μετάβαση βασίζονται σε μια προσέγγιση δύο κατευθύνσεων. Η μια χρησιμοποιεί protocol tunneling, όπου τα IPv6 πακέτα ενθυλακώνονται μέσα σε IPv4 πακέτα για τη μετακίνηση τους μεταξύ απομονωμένων IPv6 δικτύων διαμέσου του IPv4 διαδικτύου. Ακόμα και στα προχωρημένα στάδια της μετάβασης, η ενθυλάκωση (encapsulation) του IPv6 θα συνεχίσει να είναι χρήσιμη για να προσφέρει σύνδεση διαμέσου των εναπομεινάντων IPv4-only backbones. Η άλλη κατεύθυνση της στρατηγικής είναι η προσέγγιση διπλής στοίβας (dual stack), όπου οι hosts και οι routers θα τρέχουν και IPv4 και IPv6 στοίβες πάνω στα ίδια network interfaces. Με αυτόν τον τρόπο, ένας κόμβος διπλής στοίβας θα μπορεί να δέχεται και να μεταδίδει IPv4 και IPv6 πακέτα, ώστε τα δυο πρωτόκολλα να συνυπάρχουν πάνω στο ίδιο δίκτυο. Παρακάτω θα δούμε αυτές τις τεχνικές αναλυτικά.

5.2.1 Η προσέγγιση του IPv6 Protocol Tunneling

Αυτή η προσέγγιση είναι χρήσιμη για τη σύνδεση απομονωμένων IPv6 νησιών μέσα σε ένα IPv4 ωκεανό, όπως φαίνεται στο Σχήμα 1.Το tunneling

απαιτεί να υπάρχει ένας κόμβος IPv6, που να μπορεί να μεταδώσει IPv4 πακέτα (κόμβος διπλής στοίβας) σε κάθε μια από τις δυο άκρες του tunnel. Η ενθυλάκωση ενός IPv6 πακέτου μέσα σε ένα IPv4 πακέτο βασικά λειτουργεί όπως η ενθυλάκωση πρωτοκόλλου (protocol encapsulation). Ο κόμβος στην μια άκρη του tunnel παίρνει το IPv6 πακέτο και το μεταχειρίζεται ως τμήμα δεδομένων ενός IPv4 πακέτου, που πρέπει να φτάσει στον κόμβο που βρίσκεται στην άλλη άκρη του tunnel. Το αποτέλεσμα είναι μια ροή από IPv4 πακέτα, που περιέχουν IPv6 πακέτα.

Όπως φαίνεται στο Σχήμα 5.1, ο κόμβος Α και ο κόμβος Β είναι IPv6 κόμβοι. Για να πάει ένα πακέτο από τον Α στον Β, ο κόμβος Α απλά τοποθετεί στο πεδίο διεύθυνσης προορισμού του πακέτου την IPv6 διεύθυνση του κόμβου Β. Κατόπιν το πακέτο πηγαίνει στον δρομολογητή Χ, που ενθυλακώνει το IPv6 πακέτο που προορίζεται για τον κόμβο Β και το στέλνει στην IPv4 διεύθυνση του δρομολογητή Υ. Ο δρομολογητής Υ λαμβάνει το IPv4 πακέτο και το ξετυλίγει. Έτσι ανακτά το αρχικό IPv6 πακέτο το οποίο προωθεί κατάλληλα στον κόμβο Β.



Σχήμα 5.1: Διασύνδεση απομονωμένων IPv6 δικτύων διαμέσου ενός IPv4 διαδικτύου, με τη βοήθεια ενός tunnel που έχει στις άκρες του διπλής στοίβας δρομολογητές IPv4/IPv6

5.2.1.1 IPv4-compatible IPv6 διευθύνσεις

Υπάρχει μία κατηγορία IPv6 διευθύνσεων που περιέχουν IPv4 διευθύνσεις. Διακρίνουμε δύο είδη μεταξύ αυτών. Τις IPv4-compatible και τις IPv4-mapped διευθύνσεις. Οι IPv4-compatible διευθύνσεις είναι απλά διευθύνσεις των 128 bit από τα οποία τα ψηλότερα 96 είναι μηδέν και τα χαμηλότερα 32 περιέχουν μια IPv4 διεύθυνση. Οι διευθύνσεις αυτές χρησιμοποιούνται από κόμβους διπλής στοίβας ικανούς να κάνουν αυτόματο tunneling IPv6 πακέτων μέσα από IPv4 δίκτυα.

Ο κόμβος διπλής στοίβας θα λέγαμε τότε ότι χρησιμοποιεί την “ίδια” διεύθυνση τόσο για IPv4 όσο και για IPv6 πακέτα. Οι IPv4 κόμβοι μπορούν να στέλνουν πακέτα στον κόμβο διπλής στοίβας χρησιμοποιώντας την IPv4 διεύθυνσή του, ενώ οι IPv6 κόμβοι μπορούν να στέλνουν πακέτα στην IPv6 διεύθυνση (που ουσιαστικά είναι η IPv4 διεύθυνση συμπληρωμένη με μηδενικά από αριστερά ώστε να έχει μήκος 128 bits). Γενικά αυτό το είδος του κόμβου θα είναι ένας δρομολογητής που θα συνδέει IPv6 δίκτυα με αυτόματο tunneling διαμέσου IPv4 δικτύων. Ο δρομολογητής αυτός δέχεται IPv6 πακέτα από το τοπικό του IPv6 δίκτυο και θα τα ενθυλακώνει σε IPv4 πακέτα που προορίζονται για ένα άλλο κόμβο διπλής στοίβας, που επίσης θα χρησιμοποιεί IPv4-compatible διεύθυνση, και βρίσκεται κάπου στην άλλη άκρη του IPv4 διαδικτύου. Ο κόμβος αυτό θα ξετυλίγει τα πακέτα, όπως περιγράψαμε και προηγουμένως, και θα τα στέλνει στον IPv6 προορισμό τους.

5.2.1.2 Configured Tunneling και Αυτόματο Tunneling

Η διαφορά μεταξύ configured και αυτόματου tunneling έγκειται κυρίως στο γεγονός ότι το αυτόματο tunneling χρησιμοποιεί δρομολογητές διπλής στοίβας με IPv4-compatible διευθύνσεις στις άκρες του tunnel. Τα αυτόματα tunnels δεν χρειάζονται παραμετροποίηση για να δουλέψουν οι IPv4 διευθύνσεις των δρομολογητών διπλής στοίβας. Αντίθετα στο configured tunneling οι IPv4 διευθύνσεις των κόμβων διπλής στοίβας πρέπει να παρέχονται μέσω κάποιου μηχανισμού (για παράδειγμα, μέσω DHCP ή μέσω των διαχειριστών του δικτύου).

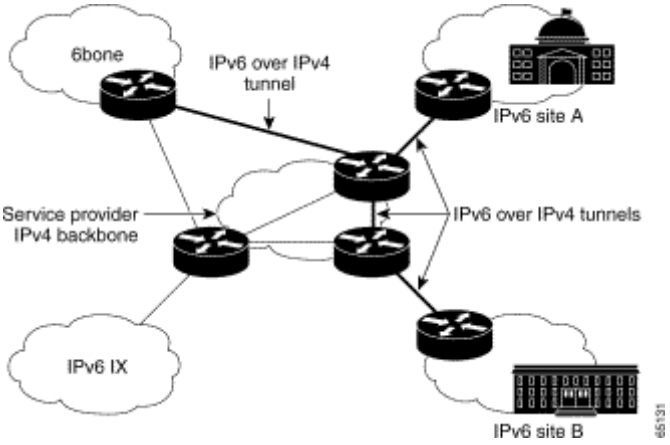
5.2.1.2.1 Configured Tunnels

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. Πάνω από τα tunneling interface οι δρομολογητές μπορούν και τρέχουν διάφορα IPv6-enabled routing πρωτόκολλα Μία κλασική περίπτωση εφαρμογής της συγκεκριμένης τεχνικής παρουσιάζεται στο Σχήμα 5.2



Σχήμα 5.2: Εφαρμογή των Configured Tunnels

Η χρησιμότητα της συγκεκριμένης τεχνικής είναι πολύ μεγάλη καθώς επιτρέπει την παράλληλη ανάπτυξη του IPv6 δικτύου χωρίς να απαιτεί την δαπάνη κονδυλίων για την χρήση ξεχωριστών φυσικών διασυνδέσεων.

5.2.1.2.2 Automatic Tunnels

Η Τεχνική Automatic Tunneling κάνει χρήση των IPv4 συμβατών (compatible) IPv6 διευθύνσεων. 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.

Το συγκεκριμένο λογισμικό δεν είναι τίποτα άλλο παρά ένα pseudo-interface, το οποίο αναλαμβάνει να κάνει την ενθυλάκωση των IPv6 πακέτων μέσα σε IPv4 και την προώθηση τους πάνω από το IPv4 interface.

Τα IPv4 πακέτα έχουν type code 41, διεύθυνση προορισμού την IPv4 διεύθυνση που είναι κωδικοποιημένη μέσα στο IPv6 πακέτο και ως πηγαία (source) διεύθυνση την IPv4 διεύθυνση του σταθμού - αποστολέα. Εννοείται πως οι σταθμοί που χρησιμοποιούν αυτήν την τεχνική πρέπει να έχουν ενεργοποιημένες και τις δύο stack των πρωτοκόλλων.

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. Ο router ο οποίος χρησιμοποιείται ως tunnel endpoint στην συγκεκριμένη περίπτωση, πρέπει να έχει σύνδεση με το native IPv6 δίκτυο.

Η αντίστροφη φορά της επικοινωνίας επιτυγχάνεται ως εξής: Ο native IPv6 host πρέπει, αφού διαπιστώσει πως η source διεύθυνση ανήκει στην κλάση των IPv4-compatible διευθύνσεων, να προωθήσει τα πακέτα (destination address IPv4 compatible) προς ένα router, ο οποίος μπορεί να εφαρμόσει την τεχνική automatic tunneling.

Γενικά θεωρείται σαν αρχή να αποφεύγεται η εισροή των IPv4 routing entries στο IPv6 Backbone. Υπάρχουν όμως περιπτώσεις, στις οποίες αυτό είναι αναπόφευκτο. Μια από αυτές είναι για παράδειγμα η περίπτωση που η τεχνική automatic tunneling χρησιμοποιείται στο τμήμα μεταξύ του router και ενός host, ο οποίος έχει IPv4-compatible διεύθυνση.

Ας θεωρήσουμε την περίπτωση όπου ο source host A έχει native IPv6 διεύθυνση και έχει σύνδεση με κάποιο τοπικό IPv6 enable router, ενώ ο destination host B δεν έχει πρόσβαση σε κανένα router συνδεδεμένο στο 6bone και χρησιμοποιεί IPv4-compatible IPv6 διευθύνσεις. Παρατηρούμε πως ο μόνος τρόπος για να επιτευχθεί η επικοινωνία A→B, είναι μέσω ενός router, ο οποίος έχει σύνδεση στο IPv6 δίκτυο και ταυτόχρονα εκτελεί automatic tunneling. Έτσι επιτυγχάνεται επικοινωνία χρησιμοποιώντας IPv6 routing μέχρι τον router και Router-to-Host automatic tunnel. Όμως προκειμένου τα

πακέτα που προορίζονται για το σταθμό Β (και γενικά για σταθμούς με IPv4-compatible διευθύνσεις) να προωθούνται μέχρι τον συγκεκριμένο router, πρέπει να διαφημίζει μέσα στην IPv6 routing υποδομή, το τμήμα των IPv4-compatible διευθύνσεων που μπορεί να εξυπηρετήσει. Σε αυτή την περίπτωση έχουμε εισροή των IPv4 routing entries στο IPv6 δίκτυο.

Γενικά οι συστάσεις είναι: Όπου δεν μπορεί να αποφεύγεται η συγκεκριμένη τακτική, να εφαρμόζεται με πολύ προσοχή και πιο συγκεκριμένα να φιλτράρονται οι IPv4 routing entries, έτσι ώστε να “διαρρέουν” μόνο αυτές που οδηγούν σε IPv6 –capable δίκτυα.

Συνοψίζοντας, επειδή η συγκεκριμένη τεχνική tunneling επιτρέπει σε απομονωμένους σταθμούς να έχουν πρόσβαση στο IPv6 δίκτυο και ο τρόπος λειτουργίας της είναι αρκετά απλός και ευέλικτος, μπορεί να συνδυαστεί με αρκετές άλλες τεχνικές προκειμένου να επιτευχθεί end-to-end επικοινωνία.

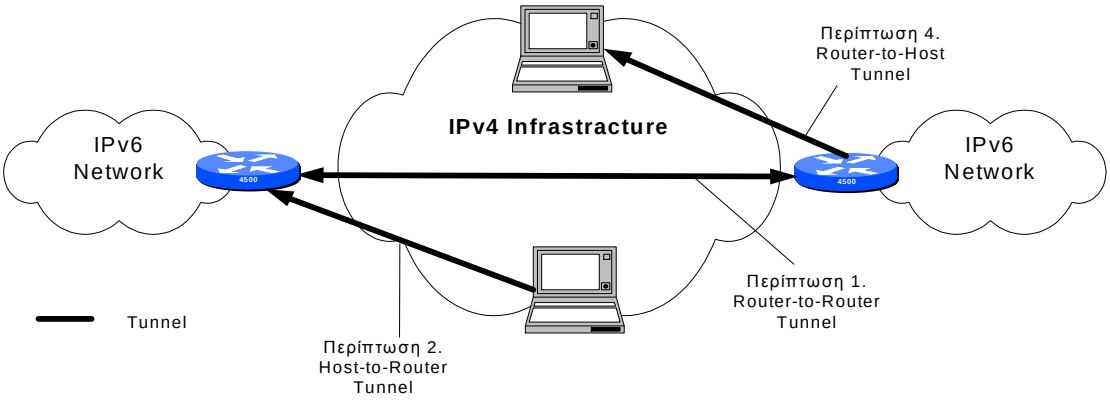
5.2.1.3 Τα είδη των IPv6 Tunnels

Υπάρχουν αρκετοί διαφορετικοί συνδυασμοί κόμβων που μπορεί να παίζουν το ρόλο των ακραίων σημείων ενός tunnel. Ως αποτέλεσμα υπάρχουν διαφορετικά είδη tunneling τα οποία έχουν ως εξής :

- **Router-to-router tunneling:** IPv4/IPv6 routers που συνδέονται μεταξύ τους μέσω μιας IPv4 δομής που κάνουν tunneling IPv6 πακέτων μεταξύ τους. Σ’ αυτήν την περίπτωση το tunnel αντιστοιχεί σε ένα μεσαίο τμήμα της συνολικής διαδρομής του IPv6 πακέτου.
- **Host-to-router tunneling:** IPv4/IPv6 hosts που κάνουν tunneling IPv6 πακέτων προς ένα ενδιάμεσο IPv4/IPv6 router, στον οποίο έχουν πρόσβαση μέσω μιας IPv4 δομής. Σ’ αυτήν την περίπτωση το tunnel αντιστοιχεί στο αρχικό τμήμα της συνολικής διαδρομής.
- **Host-to-host tunneling:** IPv4/IPv6 hosts που είναι συνδεδεμένοι μεταξύ τους μέσω μιας IPv4 δομής κάνουν tunneling IPv6 πακέτων μεταξύ τους. Σ’ αυτήν την περίπτωση το tunnel αντιστοιχεί στη συνολική διαδρομή.
- **Router-to-host:** IPv4/IPv6 routers που κάνουν tunneling IPv6 πακέτων στον τελικό τους προορισμό, που είναι ένας IPv4/IPv6 host. Σ’ αυτήν την

περίπτωση το tunnel αντιστοιχεί στο τελικό τμήμα της συνολικής διαδρομής.

Οι παραπάνω περιπτώσεις απεικονίζονται στο Σχήμα 5.3



Σχήμα 5.3: Περιπτώσεις εφαρμογής Tunnels

Στις δύο πρώτες από τις περιπτώσεις που αναφέρθηκαν παραπάνω (router-to router και host-to-router), το τέλος του tunnel είναι ένας router, ο οποίος είναι μεν ενδιάμεσος 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.

Αντίθετα στις δύο τελευταίες περιπτώσεις (host-to-host και router-to-host), τα IPv6 πακέτα ενθυλακώνονται προς έναν σταθμό, ο οποίος αποτελεί και τον τελικό αποδέκτη της μεταδιδόμενης πληροφορίας. Δηλαδή, τόσο η IPv6 διεύθυνση όσο και η IPv4 δείχνουν προς τον ίδιο σταθμό. Αυτό το γεγονός μπορεί να χρησιμοποιηθεί με την εφαρμογή κατάλληλων τεχνικών, έτσι ώστε

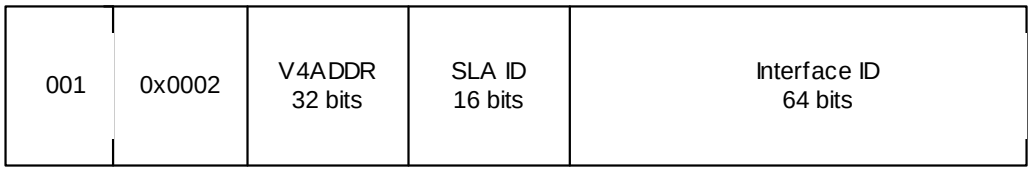
η IPv4 διεύθυνση του τελικού σταθμού προορισμού να κωδικοποιείται μέσα στην IPv6 διεύθυνση του πακέτου. Αποτέλεσμα αυτού είναι, να μπορεί ο κόμβος που κάνει την ενθυλάκωση (δημιουργεί το tunnel) να καταλαβαίνει αυτόματα την IPv4 διεύθυνση του σταθμού προορισμού. Αυτό φυσικά έχει ως σημαντικό όφελος τη μείωση του διαχειριστικού κόστους, σε σχέση με αυτό που θα απαιτούνταν για τον άμεσο (χειρωνακτικό) ορισμό των tunnels.

5.2.1.4 Μηχανισμός μετάβασης 6to4

Ο μηχανισμός μετάβασης 6to4 είναι μια τεχνική που μπορεί να χρησιμοποιηθεί για την επίτευξη connectivity μεταξύ IPv6-enabled hosts ακόμα και αν δεν υπάρχει IPv6 υποστήριξη στο δίκτυο που ανήκουν. Το γεγονός ότι δεν κάνει χρήση configured tunnels, δίνει μεγάλη ευελιξία στον τρόπο εφαρμογής, αφού το χαρακτηριστικό αυτό εξασφαλίζει ελάχιστο διαχειριστικό κόστος. Περιγράφεται στο RFC 3056.

Γενικά η τεχνική 6to4 χρησιμοποιεί και αυτή την IPv4 υποδομή, προκειμένου να επιτύχει τη διασύνδεση απομακρυσμένων IPv6 sites. Συγκεκριμένα, βλέπει το IPv4 δίκτυο σαν ένα unicast point to point link layer και χρησιμοποιώντας τεχνικές ενθυλάκωσης, υλοποιεί το IPv6 δίκτυο. Για τον μηχανισμό 6to4 έχει αποδοθεί από τις αρμόδιες αρχές διαχείρισης του IPv6 address space, ένα 13bit IPv6 top level Aggregator identifier (TLA) κάτω από το IPv6 prefix 001. Η δεκαεξαδική του αναπαράσταση είναι 0x0002 και συνεπώς το IPv6 prefix που έχει αποδοθεί είναι 2002::/16(hex).

Κάθε site που έχει τουλάχιστον μια routable IPv4 διεύθυνση, μπορεί να κάνει χρήση του μηχανισμού 6to4. Οι IPv6 διευθύνσεις που μπορεί να χρησιμοποιήσει, είναι αυτές που παράγονται από το IPv6 prefix 2002:V4ADDr::/48. Η μορφή των διευθύνσεων που χρησιμοποιούνται είναι αυτή που φαίνεται στο Σχήμα 5.4



Σχήμα 5.4: Δομή IPv6 διεύθυνσης που χρησιμοποιείται στην 6to4 τεχνική

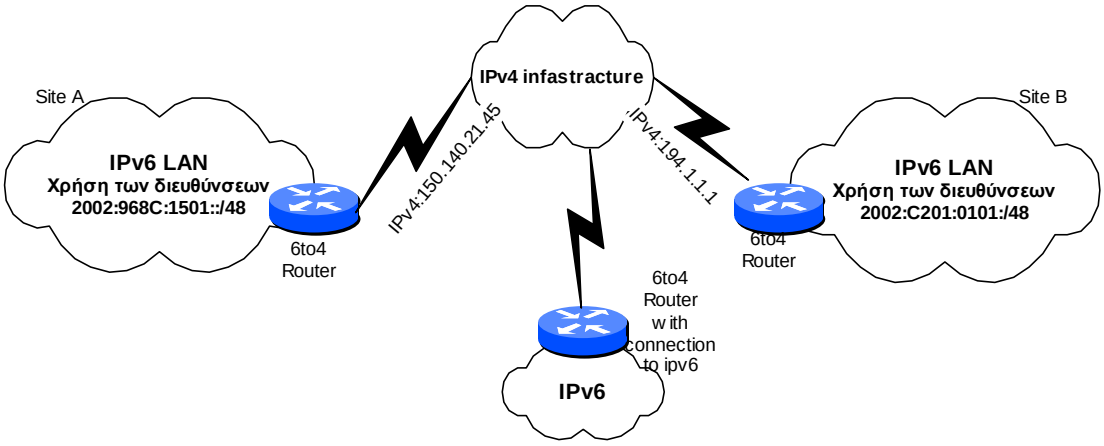
Οι διευθύνσεις αυτές είναι κανονικές IPv6 διευθύνσεις (όχι της μορφής IPv4-compatible) και συνεπώς μπορούν να χρησιμοποιηθούν σε διαδικασίες auto configuration (stateless/state full), DHCP, κλπ.

Από τα παραπάνω φαίνεται πως όλα τα sites που χρησιμοποιούν τον 6to4 μηχανισμό, δημιουργούν μια “κλάση” στο σύνολο των IPv6 διευθύνσεων, αυτών που η διεύθυνση τους αρχίζει με το prefix 2002::.

Όταν ένας σταθμός σε ένα 6to4 site θέλει να επικοινωνήσει με άλλον IPv6 σταθμό, εκτός του site για τον οποίον ξέρει ότι έχει διεύθυνση που ανήκει στην κλάση των 6to4 διευθύνσεων, τότε απλώς προωθεί τα IPv6 πακέτα προς εκείνο τον router/host που έχει το interface, το οποίο έχει την IPv4 που βγαίνει προς το Internet. Σε αυτό το interface είναι ορισμένο ένα 6to4 pseudo-interface, το οποίο και κάνει το encapsulation των IPv6 πακέτων μέσα σε IPv4 και τα προωθεί προς το αντίστοιχο IPv4 interface που εξυπηρετεί το απέναντι 6to4 site. Η IPv4 διεύθυνση του απέναντι interface είναι γνωστή, αφού είναι κωδικοποιημένη πάνω στην διεύθυνση προορισμού του IPv6 πακέτου. Έτσι δεν χρειάζεται ο άμεσος ορισμός της IP του απέναντι interface (automatic tunneling). Επίσης πρέπει να τονιστεί πως μεταξύ των 6to4 routers δεν απαιτείται να υπάρχει κάποιο IPv6 exterior routing πρωτόκολλο. Όλη η απαιτούμενη routing διαδικασία γίνεται από το IPv4.

Στο σημείο αυτό πρέπει να τονιστεί πως η σωστή λειτουργία του 6to4 μηχανισμού εξαρτάται από τον τρόπο, με βάση τον οποίο οι σταθμοί επιλέγουν ποια διεύθυνση θα χρησιμοποιήσουν, από αυτές που επιστρέφονται στο σταθμό από την DNS υπηρεσία. Δηλαδή, έστω ένας σταθμός που έχει 6to4 διεύθυνση και ρωτάει για την IPv6 διεύθυνση ενός άλλου σταθμού. Εάν η υπηρεσία DNS του επιστρέψει δύο IPv6 διευθύνσεις που αντιστοιχούν σε δύο IPv6 interfaces, μία native και μια 6to4, είναι αναγκαίο ο σταθμός να χρησιμοποιήσει την 6to4 διεύθυνση στην προσπάθεια του να επικοινωνήσει με τον άλλο σταθμό. Στην περίπτωση που ο άλλος

σταθμός έχει μόνο native IPv6 διεύθυνση, τότε η επικοινωνία μπορεί να επιτευχθεί μόνο με την χρήση ενός relay router δηλαδή ενός router που έχει connectivity και με το native IPv6 δίκτυο αλλά και με το 6to4. Ο τελευταίος τρόπος είναι και ο μοναδικός, με τον οποίο μπορεί να επιτευχθεί η επικοινωνία μεταξύ των 6to4 IPv6 δικτύων και αυτών που χρησιμοποιούν native IPv6 διευθύνσεις. Δηλαδή ο 6to4 router ενός site πρέπει να έχει μια τουλάχιστον σύνδεση με κάποιον router, ο οποίος να είναι 6to4 router, αλλά επιπλέον να διαθέτει και σύνδεση με το native IPv6 δίκτυο. Προκειμένου να γίνει πιο κατανοητή η λειτουργία και τα χαρακτηριστικά της συγκεκριμένης τεχνικής, παρουσιάζεται ένα σενάριο λειτουργίας στο Σχήμα 5.5.



Σχήμα 5.5: Περίπτωση εφαρμογής 6to4 τεχνικής

Στην περίπτωση που ένας σταθμός στο site A θέλει να επικοινωνήσει με κάποιον άλλον που βρίσκεται στο site B, τότε έχουμε μια τυπική περίπτωση 6to4 IPv6 επικοινωνίας όπως αυτή περιγράφηκε ανωτέρω.

Στην περίπτωση που σταθμοί είτε από το site A είτε από το site B θέλουν να επικοινωνήσουν με IPv6 σταθμούς, που έχουν native IPv6 διευθύνσεις, τότε όπως προαναφέρθηκε πρέπει να διαμεσολαβήσει ένας IPv6 relay router, ο οποίος δεν είναι τίποτε άλλο παρά ένας IPv6 router, ο οποίος όμως έχει ορισμένο πάνω του ένα 6to4 pseudo-interface, σύνδεση με το IPv4 δίκτυο και τουλάχιστον ένα native IPv6 interface.

Στο παραπάνω σενάριο πρέπει να θεωρήσουμε τρία διαφορετικά routing domains:

1. Το εσωτερικό routing domain καθενός 6to4 site: Όπως προαναφέρθηκε, η δρομολόγηση εσωτερικά σε ένα 6to4 δίκτυο γίνεται με τους γνωστούς τρόπους, όταν πρόκειται για εσωτερικές IPv6 (6to4) διευθύνσεις και με χρήση κάποιου default ή έμμεσου route που να δείχνει προς τον 6to4 router του site.

2. Το εξωτερικό routing domain που διασυνδέει ένα σύνολο από border 6to4 routers και το οποίο περιλαμβάνει και τους 6to4 relay routers: Στην περίπτωση αυτή υπάρχουν δυο διαφορετικές επιλογές για να υλοποιηθεί το σχήμα δρομολόγησης:

- Χωρίς την χρήση κάποιου IPv6 πρωτοκόλλου δρομολόγησης, αφού και τα πρωτόκολλα δρομολόγησης που τρέχουν για το IPv4 μπορούν να εξασφαλίσουν τη διασύνδεση μεταξύ των 6to4 sites.
- Με χρήση κάποιου εξωτερικού IPv6 πρωτοκόλλου δρομολόγησης. Ένα σύνολο 6to4 routers, εάν έχουν διασύνδεση με κάποιον 6to4 router, από τον οποίον μπορούν να μαθαίνουν τα native IPv6 routes, μπορούν να τρέχουν μεταξύ τους κάποιο IPv6 capable routing πρωτόκολλο όπως το BGP4+. Προϋπόθεση για το παραπάνω αποτελεί ο relay router να διαφημίζει τις απαραίτητες native IPv6 routes (IPv6 prefixes) πάνω στο 6to4 pseudo-interface του. Ουσιαστικά με αυτόν τον τρόπο δηλώνει για ποιο κομμάτι του IPv6 δικτύου είναι διαθέσιμος ως relay router. Αν και αυτή η προσέγγιση είναι διαχειριστικά πιο πολύπλοκη, εντούτοις δίνει το πλεονέκτημα ότι παρέχει εργαλεία για τον έλεγχο της πολιτικής.

3. Το εξωτερικό IPv6 routing domain από κάθε IPv6 δίκτυο: Κάθε relay router πρέπει να διαφημίζει το 2002::/16 prefix πάνω στην native IPv6 διεύθυνση που διαθέτει. Είναι θέμα routing πολιτικής πόσο μακριά μέσα στο native IPv6 routing σύστημα θα φτάσει αυτή η διαφήμιση (advertisement). Δεδομένου ότι γενικά θα υπάρχουν πολλοί 6to4 relay routers, οι οποίοι θα διαφημίζουν το συγκεκριμένο prefix, είναι θέμα πολιτικής, ποιους θα επιλέγει κάθε native IPv6 site.

Απαιτείται η εφαρμογή προσεκτικού filtering από τους διαχειριστές των δικτύων.Πιο λεπτομερή 2002:: prefixes (π.χ. 2002::/48) δεν πρέπει να

διαδίδονται μέσα στο IPv6 routing σχήμα, προκειμένου να μην μολύνεται αυτό από routing entries του IPv4 δικτύου και απαιτείται από τους διαχειριστές των δικτύων να φιλτράρουν και να απορρίπτουν τέτοια prefixes.

Γενικά ο μηχανισμός 6to4 παρέχει την δυνατότητα για άμεση σύνδεση στο IPv6 δίκτυο οποιουδήποτε το επιθυμεί χωρίς να υπάρχει αντίστοιχη υποστήριξη στο πρωτόκολλο από τον παροχέα (provider) του φορέα.

Το μεγάλο πλεονέκτημα που παρέχει είναι, ότι επιτρέπει την πρόοδο της διαδικασίας μετάβασης, χωρίς να απαιτείται η εγκατάλειψη άλλων μηχανισμών ή πρωτοκόλλων. Επιτρέπει το σταδιακό migration από IPv4 σε 6to4 και έπειτα σε native IPv6. Αυτό γίνεται ακολουθώντας τα παρακάτω βήματα:

1. Εφαρμογή του IPv6 εσωτερικά στο δίκτυο του φορέα ή στο σταθμό, αν πρόκειται για μεμονωμένο χρήστη. Η εφαρμογή οποιουδήποτε μηχανισμού είναι επιτρεπτή όπως native IPv6, 6over4 και tunnels.
2. Ρύθμιση ενός router, ο οποίος είναι συνδεμένος με το Internet, έτσι ώστε να υποστηρίζει 6to4. Το χαρακτηριστικό αυτό ήδη παρέχεται από τους περισσότερους κατασκευαστές δικτυακών συσκευών π.χ. Cisco. Ο συγκεκριμένος δρομολογητής πρέπει επίσης να διαφημίζει προς τα έξω το 2002::/16 prefix. Τέλος, πρέπει να ενημερωθούν οι DNS entries, έτσι ώστε να περιλαμβάνουν αυτό το prefix. Σ' αυτό το σημείο ο μηχανισμός 6to4 είναι ήδη διαθέσιμος και το site κάνει χρήση ενός 2002:IPv4ADDR::/48 prefix.
3. Εάν η διασύνδεση με το native IPv6 δίκτυο είναι επιθυμητή, τότε πρέπει το site/host να βρει έναν διαθέσιμο relay router, ο οποίος θα τον διασυνδέει με το native IPv6 δίκτυο. Ο relay router μπορεί να ανήκει είτε σε κάποιο άλλο συνεργαζόμενο 6to4 site είτε να προσφέρεται ως υπηρεσία από τον provider. Όσον αφορά τα θέματα δρομολόγησης, εάν δεν χρησιμοποιείται κάποιο exterior routing πρωτόκολλο από το 6to4 site, τότε πρέπει να υπάρχει ένα default route που να δείχνει προς τον relay router. Εάν αντίθετα χρησιμοποιείται κάποιο exterior routing πρωτόκολλο, όπως BGP, τότε το site πρέπει να ρυθμιστεί έτσι ώστε να δημιουργήσει τα κατάλληλα BGP peerings με αυτόν.
4. Όταν κάποια στιγμή μία native IPv6 σύνδεση γίνει διαθέσιμη, τότε πρέπει

να προστεθεί ένα δεύτερο (native) prefix στον 6to4 router, όπως επίσης να ενημερωθεί και ο DNS.

5. Όταν αργότερα διαπιστωθεί πως έχει ολοκληρωθεί η μετάβαση σε native IPv6, τότε μπορεί πολύ εύκολα να απομακρυνθεί το 6to4 configuration.

Σημαντικό πλεονέκτημα επίσης του 6to4 μηχανισμού αποτελεί το γεγονός ότι μπορεί να χρησιμοποιηθεί σε δίκτυα, τα οποία χρησιμοποιούν private IPv4 διευθύνσεις και μόνο μια routable. Επίσης δεν επηρεάζεται καθόλου από την παρουσία firewalls ή NAT boxes στο δίκτυο.

5.2.1.5 6over4

Η μέθοδος 6over4 έχει αναπτυχθεί με κύριο σκοπό να επιτρέψει σε κάποιον απομονωμένο σταθμό IPv6, ο οποίος βρίσκεται πάνω σε φυσικό σύνδεσμο (link) χωρίς την παροχή native IPv6 υποστήριξης, να γίνει ένας πλήρως λειτουργικός IPv6 σταθμός με πρόσβαση στο IPv6 δίκτυο. Ο μηχανισμός 6over4 περιγράφεται στο RFC 2529.

Ο μηχανισμός 6over4 κάνει χρήση του IPv4 multicast domain, το οποίο θεωρείται ως το link layer πάνω από το οποίο δομείται η IPv6 Stack. Προκειμένου να χρησιμοποιηθεί η 6over4 μέθοδος, πρέπει το IPv4 domain να υποστηρίζει multicast. Επίσης, εάν απαιτείται να υπάρχει σύνδεση με εξωτερικά sites (IPv6), πρέπει απαραίτητα να υπάρχει και κάποιος router που να εφαρμόζει την ίδια μέθοδο στο link που συνδέεται με το multicast domain. Η 6over4 μέθοδος είναι εφαρμόσιμη στα όρια του ίδιου site και εξαιτίας του γεγονότος ότι δεν χρησιμοποιεί IPv4-compatible IPv6 διευθύνσεις ή configured tunnels, παρέχει μεγάλη ανεξαρτησία, όσον αφορά την τεχνολογία των links που χρησιμοποιούνται αλλά και την τοπολογία του IPv6 δικτύου που επιχειρείται να εφαρμοστεί. Συχνά η μέθοδος 6over4 αναφέρεται και ως virtual Ethernet.

Ο τρόπος λειτουργίας της συγκεκριμένης τεχνικής είναι σχετικά απλός: Για κάθε IPv6 LAN ορίζεται ένα multicast session, το οποίο “ακούν” τόσο οι hosts που συμμετέχουν στο IPv6 subnet, όσο και ο router που δρομολογεί την κίνηση του προς τα έξω (λειτουργίες IPv6 neighbour/router discovery).

Απαραίτητη προϋπόθεση και πάλι αποτελεί ο router να έχει υλοποιημένες και τις δύο stack στο interface που εξυπηρετεί το virtual LAN.

Προκειμένου οι hosts που χρησιμοποιούν την συγκεκριμένη τεχνική να μπορούν να υποστηρίξουν stateless auto configuration, έχει οριστεί ότι το συμπλήρωμα του prefix FE80:0000/64 (χρησιμοποιείται στην stateless auto configuration διαδικασία) θα είναι η unicast IPv4 διεύθυνση του link, συμπληρωμένη (padded) από τα αριστερά με 32 bits, προκειμένου να συμπληρωθεί το σύνολο των 128 bits που αποτελούν την IPv6 διεύθυνση.

Ιδιαίτερη προσοχή πρέπει να δοθεί στην τιμή TTL που δίνεται στα multicast IPv4 πακέτα που μεταφέρουν την IPv6 κίνηση, έτσι ώστε η τιμή του να είναι αρκετά μικρή προκειμένου να μην υπάρχουν διαρροές IPv6 κίνησης έξω από το Multicast domain.

5.2.2 Η Προσέγγιση IPv4 / IPv6 Διπλής Στοίβας

Αναμφισβήτητα το IPv4 θα είναι μαζί μας για πολύ καιρό ακόμα. Γιατί πάνω από όλα η αναβάθμιση σε IPv6 κοστίζει, τόσο σε καινούριο λογισμικό όσο και υλικό. Όλο αυτό τον καιρό τα αναβαθμισμένα συστήματα θα πρέπει να διατηρήσουν την επικοινωνία τους με τα IPv4 συστήματα. Αυτό θα επιτευχθεί με τη χρήση συστημάτων που υποστηρίζουν και τα δυο IP πρωτόκολλα (IPv6, IPv4).

Η ιδέα της διπλής στοίβας δεν είναι καινούρια. Χρησιμοποιήθηκε και χρησιμοποιείται για τη διασύνδεση LAN, που τρέχουν παλιό δικτυακό λογισμικό της Novell (που υλοποιούσε το πρωτόκολλο δικτύου IPX), με το internet(TCP/IP). Η σύνδεση με το internet γίνεται μέσω της στοίβας TCP/IP, ενώ η σύνδεση με το δίκτυο Novell γίνεται μέσω της IPX στοίβας. Καθώς πακέτα λαμβάνονται στο επίπεδο σύνδεσης δεδομένων και ξετυλίγονται, οι επικεφαλίδες τους δηλώνουν αν το πακέτο προορίζεται για την TCP/IP στοίβα ή την IPX στοίβα –και το πακέτο επεξεργάζεται από την αντίστοιχη στοίβα.

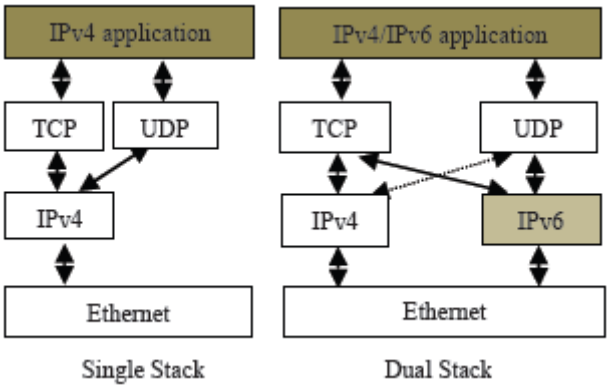
5.2.2.1 Κόμβοι Διπλής Στοίβας

Οι κόμβοι διπλής στοίβας IPv4/IPv6 δουλεύουν περίπου με τον ίδιο τρόπο που δουλεύουν και άλλα είδη κόμβων πολλαπλής στοίβας. Καθώς πακέτα λαμβάνονται στο 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 στην 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).

Η λειτουργία του μηχανισμού φαίνεται παραστατικά στο Σχήμα 5.6.



Σχήμα 5.6: Κόμβος διπλής στοίβας (dual stack)

5.2.2.2 Προβλήματα –Απαιτούμενες διευκρινίσεις

Στην υλοποίηση της dual stack τεχνικής εισέρχονται κάποια θέματα και προβλήματα, τα οποία πρέπει να διευκρινιστούν προκειμένου να γίνει η εφαρμογή της αποδοτική.

Το πρώτο από αυτά είναι η Υπηρεσία Ονοματολογίας (DNS) και ο τρόπος με τον οποίο αυτή επηρεάζει την “προτίμηση” που θα έχουν οι dual stack σταθμοί προς το ένα ή το άλλο πρωτόκολλο. Επίσης σημαντική είναι η επίδραση της στην απόδοση του δικτύου.

Για την υλοποίηση της Υπηρεσίας Ονοματολογίας, έτσι ώστε να υποστηρίζει το IPv6, έχει εισαχθεί και οριστεί ένα νέο είδος record για την βάση δεδομένων του DNS, το A6 record το οποίο αποτελεί συνέχεια / εξέλιξη του AAAA record. Έτσι προκειμένου ένας σταθμός να είναι ικανός να επικοινωνεί χρησιμοποιώντας και τα δύο πρωτόκολλα, πρέπει να διαθέτει τις απαιτούμενες βιβλιοθήκες, για να “ρωτάει” την Υπηρεσία Ονοματολογίας για την IP address σταθμών IPv4, IPv6 και IPv4/IPv6. Με άλλα λόγια, οι βιβλιοθήκες αυτές να είναι ικανές να χειρίζονται τα A records (IPv4) αλλά και τα AAAA/A6 records (IPv6).

Για να αποσαφηνιστεί περισσότερο η επίδραση της Υπηρεσίας Ονοματολογίας στην εφαρμογή τεχνικών Dual Stack, ας θεωρήσουμε την περίπτωση κατά την οποία ένας dual stack σταθμός “ρωτάει” την Υπηρεσία Ονοματολογίας για την IP διεύθυνση ενός σταθμού και βρίσκει ότι στο συγκεκριμένο όνομα αντιστοιχεί τόσο μια IPv4 address όσο και μια IPv6. Σε αυτή την περίπτωση οι βιβλιοθήκες που διαθέτει ο σταθμός για το DNS έχουν τις εξής επιλογές ως προς την απάντηση που θα επιστρέψουν στην εφαρμογή:

1. Να επιστρέψουν μόνο την IPv4 διεύθυνση
2. Να επιστρέψουν μόνο την IPv6 διεύθυνση
3. Να επιστρέψουν και τις 2 διευθύνσεις διαταγμένες σε μία σειρά IPv4 – IPv6 ή αντίστροφα

Σε κάθε περίπτωση η επιλογή που γίνεται από τις DNS βιβλιοθήκες καθορίζει και το πρωτόκολλο που θα χρησιμοποιηθεί. Η σύσταση που έχει γίνει προτείνει ότι η επιλογή αυτή πρέπει να γίνεται από τις εφαρμογές και όχι αυθαίρετα από τις βιβλιοθήκες resolve των σταθμών.

Για την Υπηρεσία Ονοματολογίας κατά την διάρκεια της μετάβασης από IPv4 σε IPv6, έχει γίνει η εξής σύσταση προκειμένου να αποφευχθούν διάφορα δυσάρεστα φαινόμενα:

Ένα AAAA/A6 record για ένα host θα πρέπει να καταχωρείται στη DNS database μόνο όταν και οι τρεις παρακάτω προτάσεις είναι αληθείς.

1. Η IPv6 διεύθυνση έχει αποδοθεί σε ένα interface του host
2. Η IPv6 διεύθυνση έχει γίνει configured στο interface του host
3. Το συγκεκριμένο interface έχει σύνδεση προς το IPv6 δίκτυο

Τα παραπάνω έχουν αντίστοιχη εφαρμογή κατά τα τελευταία στάδια της μετάβασης και πιο συγκεκριμένα για το πότε το record που αντιστοιχεί σε μια IPv4 διεύθυνση, η οποία έχει απενεργοποιηθεί από το Interface ενός σταθμού, αφαιρείται από την DNS βάση.

5.2.2.3 Dual Stack Transition Mechanism (DSTM)

Η Τεχνική Dual Stack Transition Mechanism (DSTM) έχει αναπτυχθεί, προκειμένου να επιτρέψει την επικοινωνία μεταξύ των IPv6 σταθμών και των IPv4 only δικτύων που υπάρχουν σήμερα. Είναι μια εναλλακτική πρόταση στις τεχνικές μετάφρασης επικεφαλίδας.

Ο DSTM ουσιαστικά αποτελεί ένα μηχανισμό, ο οποίος προκύπτει από το συνδυασμό τεχνικών απόδοσης IPv4 διευθύνσεων σε IPv6 hosts και Dynamic Tunneling Interfaces (DTI).

Η τεχνική DSTM βασίζεται στη χρήση ενός DHCPv6 server, ο οποίος αποδίδει προσωρινά global IPv4 διευθύνσεις στους IPv6 σταθμούς που θέλουν να επικοινωνήσουν με κάποιον IPv4 only σταθμό. Τα IPv4 πακέτα ενθυλακώνονται σε IPv6 μέσω ενός DTI interface και μεταφέρονται μέσα στο IPv6 δίκτυο μέχρι τον Border Router που το διασυνδέει με το IPv4 δίκτυο.

Η λειτουργία του μηχανισμού είναι δικατευθυντήρια (bi-directional), δηλαδή η αρχικοποίηση της επικοινωνίας μπορεί να γίνει είτε από την πλευρά του IPv6 host είτε από την πλευρά του IPv4. Αυτό αποτελεί και σημαντικό πλεονέκτημα της συγκεκριμένης μεθόδου σε σχέση με άλλες τεχνικές, οι οποίες επιτρέπουν

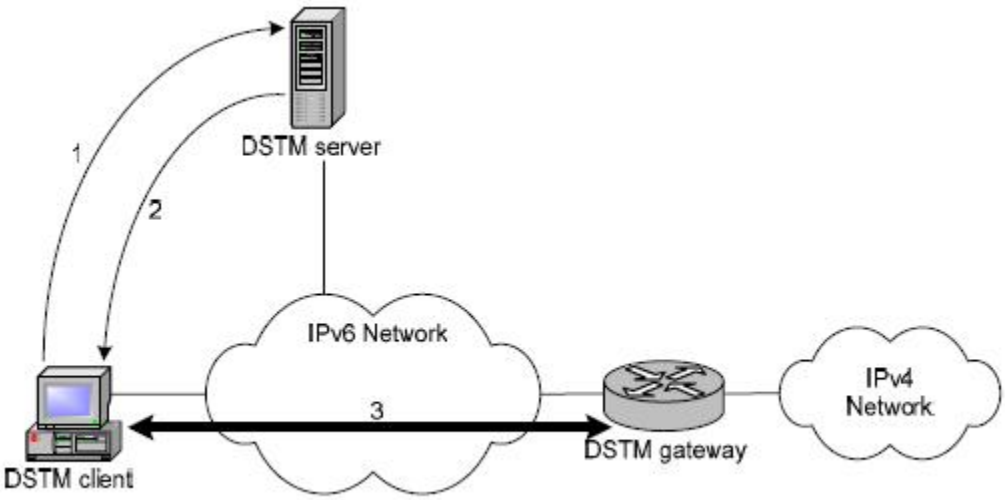
την επικοινωνία των IPv6 σταθμών με το IPv4 δίκτυο και απαιτούν την αρχικοποίηση της επικοινωνίας μόνο από τον IPv6 host.

Ο τρόπος λειτουργίας της συγκεκριμένης τεχνικής επεξηγείται αναλυτικά στη συνέχεια για τις εξής δύο περιπτώσεις: Ι) η επικοινωνία αρχικοποιείται από τον IPv6 host και ΙΙ) η επικοινωνία αρχικοποιείται από τον IPv4 host.

Ι.Στην πρώτη περίπτωση ο IPv6 σταθμός στέλνει IPv4 πακέτα στον απέναντι σταθμό μέσω του DTI interface, το οποίο υλοποιεί την ενθυλάκωση σε IPv6 πακέτα και στη συνέχεια τα προωθεί προς το άλλο άκρο του Tunneling interface (συνήθως είναι ένας DSTM router που βρίσκεται στα όρια του IPv6 δικτύου και του IPv4 κόσμου). Εκεί τα πακέτα απενθυλακώνονται και προωθούνται πλέον κανονικά προς τον IPv4 προορισμό τους. Με βάση τα ανωτέρω συμπεραίνεται ότι για να έχει αποτέλεσμα ο παραπάνω μηχανισμός, θα πρέπει ο border router, που εξυπηρετεί την επικοινωνία των δύο δικτύων IPv4 και IPv6, να διαφημίζει προς το IPv4 δίκτυο το τμήμα των IPv4 διευθύνσεων που χρησιμοποιούνται για προσωρινή απόδοση στους σταθμούς. Ένα ακόμη σημείο στο οποίο πρέπει να δοθεί προσοχή, είναι ο τρόπος που λειτουργεί η υπηρεσία DNS και οι βιβλιοθήκες resolve των clients, αφού η επιλογή της χρήσης της μεθόδου εξαρτάται από αυτό.

Αναλυτικότερα, στην αρχή ο IPv6 host ρωτάει την υπηρεσία DNS για ένα AAAA record για τον IPv4 host και προφανώς παίρνει ως απάντηση ένα μήνυμα λάθους. Στη συνέχεια ρωτάει την υπηρεσία για ένα A record, που αντιστοιχεί στην IP του και παίρνει ως απάντηση την διεύθυνση του σταθμού. Αφού πλέον καταλαβαίνει πως ο σταθμός είναι IPv4, ρωτάει τον DHCPv6 server για μια προσωρινή IPv4 διεύθυνση, προκειμένου να την χρησιμοποιήσει στην επικοινωνία του με τον σταθμό.

Το ανωτέρω σενάριο περιγράφεται στο Σχήμα 5.7.



Σχήμα 5.7: Λειτουργία μηχανισμού DSTM

II. Στην περίπτωση κατά την οποία η επικοινωνία αρχικοποιείται από την πλευρά του IPv4 host, λαμβάνει χώρα η εξής σειρά ενεργειών: Ο IPv4 σταθμός ρωτάει την υπηρεσία DNS για την IPv4 διεύθυνση του IPv6 σταθμού. Με την σειρά του ο DNS server ενημερώνει τον AIIH(Assignment of IPv4 global addresses to IPv6 Hosts) server ότι πρέπει να αποδώσει μια διεύθυνση στον IPv6 σταθμό και αφού συμβεί αυτό, στη συνέχεια πρέπει να την δηλώσει στη βάση της DNS Υπηρεσίας. Ο IPv6 host ενημερώνεται για την διεύθυνση που του αποδίδεται και πλέον η επικοινωνία μπορεί να αρχικοποιηθεί.

Ο DSTM μηχανισμός βασίζεται στην χρήση ενός DHCP server και προαιρετικά στην χρήση ενός DNS server. Συνεπώς ο σχεδιασμός του ταιριάζει αρκετά σε μικρού και μεσαίου μεγέθους οργανισμούς που ήδη χρησιμοποιούν ένα DHCP server προκειμένου να μοιράσουν τις global IPv4 διευθύνσεις.

Η κύρια δυσκολία εφαρμογής του έγκειται στο γεγονός της μη διαθεσιμότητας του DHCPv6 server, δεδομένου ότι η διαδικασία προτυποποίησης του δεν έχει ακόμα ολοκληρωθεί.

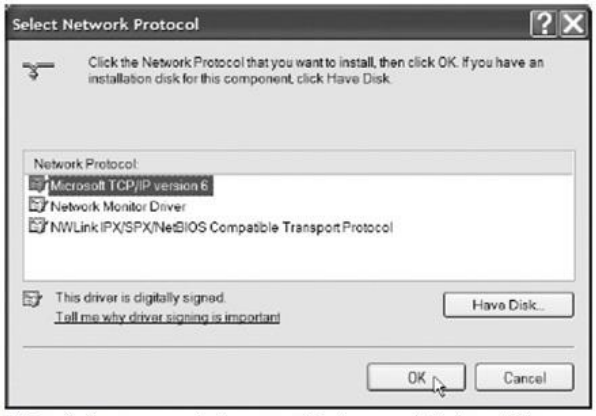
5.3 Βαθμός ετοιμότητας των συστημάτων

Παρά την προχωρημένη φάση στην οποία βρίσκεται η διαδικασία προτυποποίησης του πρωτοκόλλου, δεν υπάρχει αντίστοιχη υποστήριξη σε επίπεδο εφαρμογών από την μεριά του χρήστη. Η Microsoft ενσωματώνει στα Windows XP την IPv6 stack(χρειάζεται εγκατάσταση από το χρήστη), κάτι που δεν ισχύει για τα Windows 2000, στα οποία μεν εγκαθίσταται η IPv6 stack αλλά η λειτουργικότητα της είναι αρκετά περιορισμένη και προκαλεί αρκετά προβλήματα στη όλη λειτουργία του σταθμού.

Για να ενεργοποιήσουμε την υποστήριξη στα Windows XP:

Start **à** Run και πληκτρολογούμε cmd. Στο παράθυρο που ανοίγει πληκτρολογούμε ipv6 install**.**

Η διασύνδεση των ρυθμίσεων του δικτύου στα Window XP



Η διασύνδεση των ρυθμίσεων του δικτύου στα Windows XP

Επισκόπηση των IPv6 διευθύνσεων:

Start **à** *Run πληκτρολογούμε cmd και στη συνέχεια:*

C:\>netsh

netsh>interface ipv6

netsh interface ipv6>show addres

Querying active state...

Interface 6: Local Area Connection 3

Addr Type DAD State Valid Life Pref. Life Address

--------- ---------- ------------ ------------ ----------------------------

Temporary Preferred 6d23h38m55s 23h36m8s

2001:db8:1dde:1:6d16:9d1:b1ec:2245

Public Preferred 29d23h59m30s 6d23h59m30s

2001:db8:1dde:1:201:2ff:fe29:23b6

Link Preferred infinite infinite fe80::201:2ff:fe29:23b6

Interface 1: Loopback Pseudo-Interface

Addr Type DAD State Valid Life Pref. Life Address

--------- ---------- ------------ ------------ ----------------------------

Loopback Preferred infinite infinite ::1

Link Preferred infinite infinite fe80::1

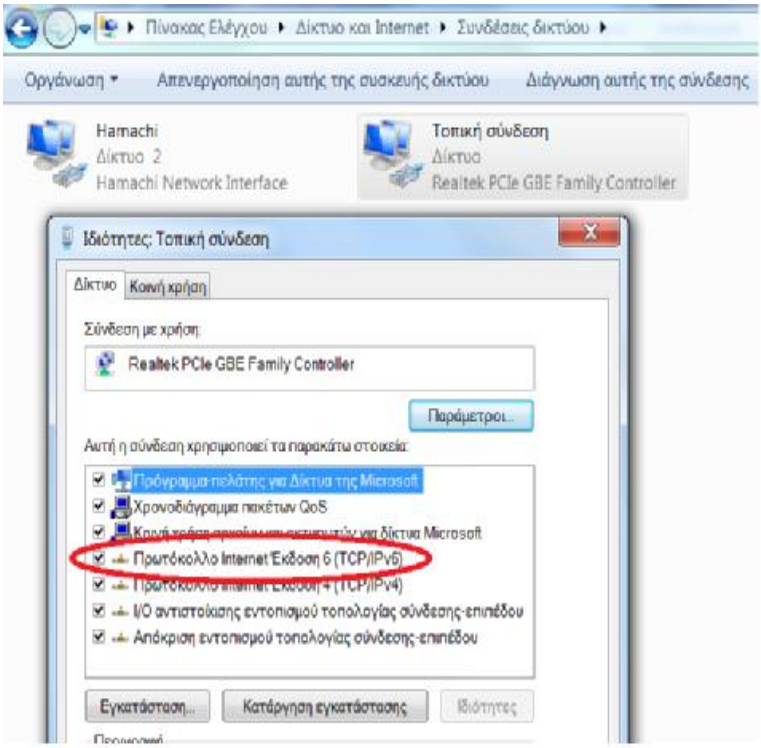
Τα Windows Vista είναι το πρώτο λειτουργικό σύστημα που επιτρέπει την αυτόματη εγκατάσταση του IPv6.Έχει Dual Stack Αρχιτεκτονική που υποστηρίζει tunneling του IPv6. Το IPSec δουλέυει τόσο για το IPv4 όσο και για το IPv6.Μερικά ονομαστικά νέα χαρακτηριστικά του IPv6 στο λειτουργικό σύστημα των Windows Vista είναι:

1. Dual Stack Αρχιτεκτονική
2. Αυτόματη εγκατάσταση και ενεργοποίηση
3. GUI που βασίζεται σε χειροκίνητες ρυθμίσεις
4. Υποστήριξη IP ασφάλειας για το IPv6
5. Listener discovery έκδοση 2(MLDv6)
6. Πραγματικές IPv6 διευθύνσεις
7. Υποστήριξη PPP(Point-to-Point Protocol v6)

8. Dynamic host configuration protocol για το IPv6 (DHCPv6)
9. Teredo

Όσον αφορά τα Windows 7, είναι γεγονός ότι υποστηρίζουν το πρωτόκολλο Ipv6 σε μεγαλύτερο βαθμό σε σχέση με τα προγενέστερα λειτουργικά συστήματα των Windows.Είναι γεγονός πως οι διευθύνσεις στο IPv4 βρίσκονται στα πρόθυρα της εξάντλησης και οι μεγαλύτεροι πάροχοι καθώς και πολλές γνωστές διαδικτυακές τοποθεσίες έχουν εφαρμόσει το προηγμένο αυτό πρωτόκολλο Ipv6 σίγουρα τραβάει την προσοχή μεγάλων εταιριών με σκοπό την προώθηση του και φυσικά το κέρδος, ωστόσο τα λειτουργικά συστήματα της Microsoft προσπαθούν να κάνουν την μετάβαση αυτή όσο πιο ομαλή γίνεται σε επίπεδο χρήστη και μέχρι στιγμής τα καταφέρνει καλά ενσωματώνοντας το στα Windows 7.

Οι ρυθμίσεις του πρωτοκόλλου γίνονται αυτόματα διευκολύνοντας τον χρήστη προσφέροντας του αρκετά νέα χαρακτηριστικά στην επικοινωνία του και στον τρόπο διασύνδεσης του με εσωτερικές διαδικασίες του υπολογιστή του ή στον τρόπο δικτύωσης του με τον “έξω κόσμο”. Στα Windows 7 εκτελούνται τόσο το IPv4 όσο και το Ipv6 με διάφορες τεχνικές με κυριότερη αυτή της Ipv6 over IPv4.Η παράλληλη εκτέλεση αυτών των δύο πρωτοκόλλων δεν είναι αναγκαστική, καθώς ο χρήστης μπορεί να απενεργοποιήσει την καινούρια έκδοση με πολύ απλό τρόπο όπως φαίνεται στο παρακάτω σχήμα:
Πίνακας ελέγχου-Δίκτυο και Internet-Συνδέσεις δικτύου-ιδιότητες στην τοπική μας σύνδεση και εμφανίζεται το παράθυρο με διάφορες ρυθμίσεις. Μπορούμε απλά να “ξεκλικάρουμε” την επιλογή του TCP/IPv6, ώστε να εκτελείται μόνο η έκδοση 4.



Σχήμα 5.9 εναλλαγή μεταξύ των πρωτοκόλλων

Υποσημείωση: Οι αλλαγές αυτές θα πρέπει να γίνονται εφόσον ο χρήστης είναι εξοικειωμένος με το περιβάλλον των Windows.

Κάποιος χρήστης ενδέχεται να επιλέξει την απενεργοποίηση της έκδοσης 6 για λόγους που αφορούν την απόδοση του συστήματος του καθώς καταλαμβάνει επιπλέον πόρους και ίσως φανεί υπερβολικό να εκτελούνται και τα δύο πρωτόκολλα από τη στιγμή που μόνο η έκδοση 4 έχει πλήρη εφαρμογή στο σύστημα του.

Όσον αφορά άλλα λειτουργικά συστήματα, μεγάλη υποστήριξη του IPv6 υπάρχουν σε εκδόσεις του Linux και του BSD όπου βρίσκεται μεγάλη ποικιλία εφαρμογών τόσο σε επίπεδο εξυπηρετητή όσο και σε επίπεδο πελάτη. Αυτό συμβαίνει γιατί το BSD είναι το λειτουργικό πάνω στο οποίο κυρίως εργάζεται το KAME Group από την Ιαπωνία, που είναι από τις σημαντικότερες προσπάθειες για την προώθηση του IPv6.

Το IPv6 στο Linux είναι ενεργοποιημένο αυτόματα από την έκδοση πυρήνα 2.1.18 και μετά.

Προεπισκόπηση της σύνδεσης:

 # /sbin/ifconfig eth0

eth0 Link encap:Ethernet HWaddr 00:01:02:29:23:B6

inet addr:192.0.2.8 Bcast:192.0.2.255 Mask:255.255.255.0

inet6 addr: fe80::201:2ff:fe29:23b6/64 Scope:Link

inet6 addr: 2001:db8:1dde:1:201:2ff:fe29:23b6/64 Scope:Global

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:226 errors:0 dropped:0 overruns:0 frame:0

TX packets:76 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:27348 (26.7 Kb) TX bytes:13251

Interrupt:10 Base address:0xd000

Τέλος καλό θα ήταν να κάνουμε μια αναφορά στις απαιτούμενες ενέργειες τόσο σε υλικό όσο και σε λογισμικό για την μετάβαση αυτή.Δηλαδή τις ενέργειες που απαιτούνται τόσο απο την πλευρά των παρόχων όσο και απο την πλευρά των χρηστών. Οι ενέργειες πρέπει να γίνουν βασικά από τους παρόχους υπηρεσιών διαδικτύου. Αυτοί πρέπει να προχωρήσουν σε αναβάθμιση του δικτυακού τους εξοπλισμού, ώστε να υποστηρίζει τις νέου τύπου διευθύνσεις και τις παλαιού τύπου, ταυτοχρόνως. Επίσης οι εφαρμογές περιεχομένου που φιλοξενούνται από τους αντίστοιχους παρόχους να είναι προσβάσιμες και μέσω του πρωτοκόλλου IPv6. Στο απώτερο μέλλον, θα εκχωρούνται νέες διευθύνσεις μόνο στο πρωτόκολλο IPv6, αφού βέβαια διασφαλιστεί ότι όλοι οι χρήστες θα μπορούν να προσπελάσουν sites που είναι σε IPv6. Υπάρχουν ορισμένοι πάροχοι που έχουν ήδη αναβαθμίσει τον εξοπλισμό τους και σήμερα υποστηρίζουν το πρωτόκολλο IPv6 στο δίκτυό τους ως πιλοτική «υπηρεσία» καθώς δεν έχουν δοκιμάσει ακόμη την υποδομή τους σε πραγματικές συνθήκες. Υπάρχουν βέβαια και πάροχοι που βρίσκονται πίσω.

Ο έλεγχος πρέπει να γίνει από την αρχή μέχρι το τέλος, μέχρι και τον τερματικό εξοπλισμό του χρήστη, επειδή κάποιοι μπορεί να έχουν παλαιότερα modem που δεν υποστηρίζουν IPv6 και πρέπει να αντικατασταθούν, κάποιοι άλλοι χρειάζονται απλώς αναβάθμιση του λογισμικού και κάποιοι το

υποστηρίζουν ήδη και απλώς πρέπει να το ενεργοποιήσουν. Εφόσον ο χρήστης έχει τον κατάλληλο τελικό εξοπλισμό πρακτικά δεν θα έχει πρόβλημα, καθώς όλα τα λειτουργικά συστήματα υποστηρίζουν την πρόσβαση στο IPv6. Αρκεί βέβαια οι ιστοσελίδες στις οποίες απευθύνεται να βρίσκονται σε παρόχους με προδιαγραφές IPv6. Κανείς δεν γνωρίζει το πότε θα γίνει η πλήρης μετάβαση και όλοι αναγνωρίζουν το γεγονός ότι σημαντικό τμήμα του Διαδικτύου θα συνεχίσει να βασίζεται στο IPv4 για πολλά ακόμα χρόνια παρά τους περιορισμούς που θα υπάρξουν. Πιστεύουμε πάντως ότι μετά τις 8 Ιουνίου(**World IPv6 Day**), οι εξελίξεις θα επιταχυνθούν εφόσον οι συμμετοχή των εταιριών θα είναι μεγάλη. Όταν μάλιστα αρχίσουν να εμφανίζονται οι πρώτοι πάροχοι περιεχομένου που θα λειτουργούν μόνο στο IPv6, τότε θα υπάρξει ακόμα μεγαλύτερη επιτάχυνση στη διαδικασία της μετάβασης.

5.4 8-6-11: Παγκόσμια Μέρα IPv6

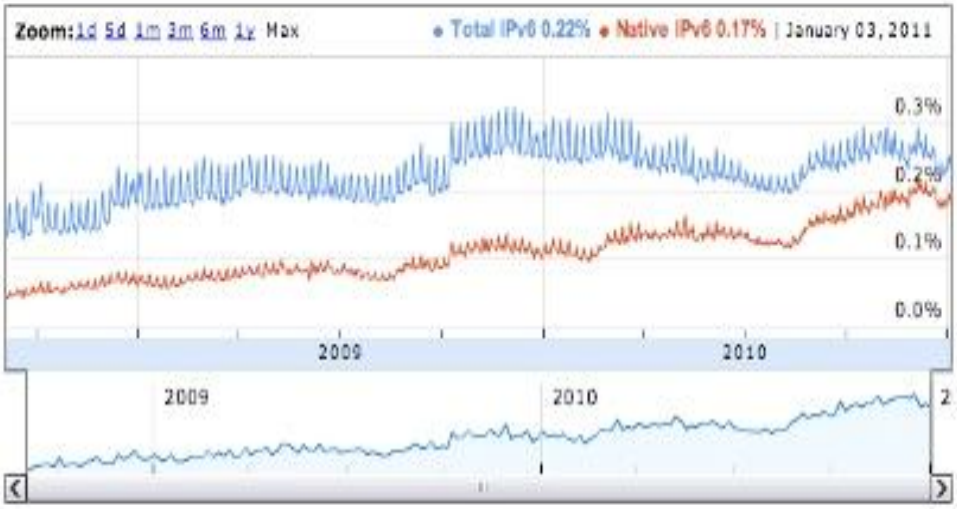
Οι μεγαλύτερες εταιρείες του Internet αποφάσισαν να ενεργοποιήσουν την υποστήριξη IPv6 στις 8 Ιουνίου του 2011. Εκείνη την ημέρα οι ειδικοί υπολογίζουν ότι περίπου το 5% των χρηστών θα αντιμετωπίσει κάποιο πρόβλημα στη σύνδεση του με διάφορες ιστοσελίδες. Παρόλα αυτά η υποστήριξη του IPv4 θα συνεχίσει να υπάρχει, παράλληλα με την καινούργια, για μερικά χρόνια ακόμα.

Την υλοποίηση του IPv6 αναλαμβάνουν συνήθως οι πάροχοι πρόσβασης (ISP) και οι δικτυακοί τόποι, όχι οι τελικοί χρήστες. Μπορείτε και εσείς να δείτε εάν η σύνδεσή σας στο Internet είναι έτοιμη για διευθύνσεις IPv6, χρησιμοποιώντας το κατατοπιστικό δωρεάν online εργαλείο http://test-ipv6.com/. Παρόλα αυτά, αν δεν σας παρέχεται υποστήριξη από τώρα μην ανησυχείτε καθώς ανήκετε στην πλειοψηφία των χρηστών.

Η Google ανακοίνωσε ότι μαζί με την Yahoo, και άλλες εταιρείες θα κάνουν το επόμενο μεγάλο βήμα προς την υιοθέτηση της επόμενης γενιάς του Internet Protocol (IPv6).

Στις 8 Ιουνίου θα ενεργοποιήσουν για 24 ώρες από κοινού το IPv6 σε όλα τα websites τους. Θα είναι η πρώτη φορά που θα δοκιμαστεί το νέο πρωτόκολλο σε τόσο μεγάλη κλίμακα.

Σύμφωνα με την ανακοίνωση, οι διαθέσιμες διευθύνσεις του IPv4 αναμένεται να τελειώσουν μέσα στο 2011.Αυτή τη στιγμή, λιγότερο από το 0.2% των χρηστών του Internet χρησιμοποιούν το IPv6.



Το ποσοστό το χρηστών που χρησιμοποιούν το νέο πρωτόκολλο IPv6.

Με αυτή τη λογική ενέργησε το IETF δίνοντας την δυνατότητα στους διαχειριστές δικτύων να πραγματοποιήσουν με ελαστικότητα την αναβάθμιση των δικτύων τους. Η ελαστικότητα έγκειται στο ότι δεν είναι απαραίτητη η άμεση και ολοκληρωμένη αναβάθμιση ολόκληρων πληθυσμών στο νέο πρωτόκολλο γιατί είναι δεδομένη η συλλειτουργία των IPv4 και IPv6 και δεν υπάρχει το πρόβλημα της απομόνωσης ή του μεγάλου χρόνου μη λειτουργίας. Όμως κατά την αναβάθμιση σε πολλούς δρομολογητές ή hosts θα πρέπει να κρατούνται και οι λειτουργίες του IPv4 (downward compatibility) για την επικοινωνία με τους δικτυακούς χώρους όπου δεν έχει πραγματοποιηθεί η μετάβαση.

Για να επιτύχουν λοιπόν οι παραπάνω στόχοι της μετάβασης έχει γίνει σοβαρός σχεδιασμός στο IPv6 το οποίο βασίζεται σε μηχανισμούς όπως Hosts και δρομολογητές που υποστηρίζουν και τα δύο πρωτόκολλα IPv4 και IPv6 (dual-stack),και πραγματοποίηση σήραγγας (tunnelling) του IPv6 διαμέσου IPv4.

Σίγουρα η τεχνολογία του IPv6 έχει να προσφέρει πολλά στο χώρο των δικτύων και να εξελίξει το Διαδίκτυο δίνοντας του εφόδια ώστε να αντιμετωπίσει τις μελλοντικές προκλήσεις. Η μεγαλύτερη όμως πρόκληση για

την επιτυχή εφαρμογή του IPv6 είναι η μετάβαση του Διαδικτύου από το IPv4 στο νέο πρωτόκολλο. Το μεγάλο μέγεθος του Διαδικτύου όπου περιέχει εκατομμύρια δικτυακών συσκευών καθιστά βέβαιο ότι η μετάβαση δεν πρόκειται να πραγματοποιηθεί μέσα σε μια νύκτα αλλά θα υπάρχει μια μακρά περίοδος συνύπαρξης του IPv4 με το IPv6.

Πηγή:

- Bouras, P. Ganos, A. Karaliotas, The deployment of IPv6 in an IPv4 world and Transition Mechanisms, Internet Research: Electronic Networking, Applications and Policy, Emerald, Volume 13, Number 2, 2003, pp. 86-93.
- IPv6 Forum : Driving IPv6 Deployment, http://www.ipv6forum.com
- Guide to DIGITAL UNIX IPv6, http://www.ipv6.zk3-x.dec.com/

ΚΕΦΑΛΑΙΟ 6. ΑΣΦΑΛΕΙΑ - ΑΠΟΔΟΧΗ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ

6.1 Εισαγωγικά

Ο αρχικός σχεδιασμός του IPv4 δεν είχε λάβει υπόψη του κανένα θέμα ασφάλειας λόγω της φύσης του δικτύου (επιδίωκε να συνδέσει ακαδημαϊκά ιδρύματα). Έτσι **το** IPv4 δεν είχε χαρακτηριστικά που θα μπορούσαν να χρησιμοποιηθούν στην ασφάλεια των δικτύων και έτσι η προσπάθεια είχε κατευθυνθεί στη χρήση μεθόδων που βασίζονται στο network επίπεδο. Μετά την τεράστια εξάπλωση που γνώρισε το Διαδίκτυο και τη σημασία που απέκτησε στον τομέα των επιχειρήσεων και του ηλεκτρονικού εμπορίου η ασφάλεια έγινε μία από τις πιο απαιτητικές ανάγκες στο Διαδίκτυο. Για να καλύψει τις ανάγκες αυτές η IETF(internet engineering task force) δημιούργησε το IP Security Working Group με στόχο να σχεδιάσει μία αρχιτεκτονική ασφαλείας και τα αντίστοιχα πρωτόκολλα, ώστε να παρέχεται ασφάλεια βασισμένη στην κρυπτογραφία για το IPv6 πρωτόκολλο. Η αρχιτεκτονική αυτή είναι γνωστή και ως IPsec και περιγράφεται στο RFC 1825. Καθώς προχωρούσαν οι εργασίες διαπιστώθηκε ότι η προτεινόμενη αρχιτεκτονική ασφαλείας για το IPv6 μπορούσε να ενσωματωθεί και στο IPv4 και έτσι το τελευταίο ορίστηκε σαν επιπλέον στόχος.

Πρέπει να τονιστεί ότι αυτή η αρχιτεκτονική αφορά το πρωτόκολλο IP και δεν προτείνει μία αρχιτεκτονική ασφάλειας για το Διαδίκτυο. Ορίζει τις υπηρεσίες ασφάλειας που μπορούν να χρησιμοποιηθούν στο επίπεδο δικτύου τόσο από το IPv4 όσο και από το IPv6. Η υλοποίηση βέβαια αυτών των υπηρεσιών διαφέρει, αφού στο IPv4 θα πρέπει να υπάρχουν οι κατάλληλες AH (Authentication) και ESP(Encryption) επικεφαλίδες στο πεδίο IP Options, κάτι που είναι αρκετά πιο δύσκολο σε σχέση με το IPv6 που αυτές οι λειτουργίες υλοποιούνται εύκολα γιατί έλαβε υπόψη του αυτές τις απαιτήσεις στο σχεδιασμό του.

Οι λειτουργίες Authentication (επιβεβαίωση αυθεντικότητας) και Encryption (κρυπτογράφηση) έχουν διαχωριστεί έτσι ώστε οι διάφορες υλοποιήσεις να

μπορούν να χρησιμοποιούν μία από τις δύο ή και τις δύο ανάλογα με τις ανάγκες των εφαρμογών των ανώτερων επιπέδων.

Authentication θεωρείται η ιδιότητα του να γνωρίζουμε ότι τα δεδομένα που λαμβάνουμε είναι ίδια με τα δεδομένα που μας στέλνονται και ότι αυτός που μας τα στέλνει είναι αυτός που ισχυρίζεται ότι είναι, με την επιπλέον ιδιότητα του ότι ένα μεμονωμένο IP πακέτο δεν έχει αλλοιωθεί (**connectionless integrity – ακεραιότητα χωρίς σύνδεση)** .

Encryption είναι ο μηχανισμός που μετατρέπει δεδομένα από μια κατανοητή μορφή (plaintext) σε μία μη-κατανοητή (ciphertext), παρέχοντας έτσι **confidentiality (εμπιστευτικότητα)**, δηλαδή προστασία των δεδομένων από μη-εξουσιοδοτημένη πρόσβαση σε αυτά.

Καθώς οι λειτουργίες αυτές παρέχουν ασφάλεια στο επίπεδο του IPv6 (επίπεδο δικτύου), εξασφαλίζεται προστασία και για το IPv6 και για τα ανώτερα επίπεδα.. Παρέχεται η δυνατότητα σε ένα σύστημα να διαλέγει τα απαραίτητα πρωτόκολλα ασφάλειας, να καθορίζει τους αλγορίθμους που θα χρησιμοποιηθούν για την υπηρεσία αυτή, και να δημιουργεί τυχόν κρυπτογραφικά κλειδιά απαραίτητα για την παροχή της υπηρεσίας. Οι υπηρεσίες ασφάλειας του IPv6 μπορούν να χρησιμοποιηθούν για να προστατέψουν την επικοινωνία μεταξύ δύο hosts, μεταξύ δύο security gateways ή μεταξύ ενός host και μιας security gateway. **Security gateway (ασφαλή πύλη)** εννοούμε ένα σύστημα το οποίο λειτουργεί ως ενδιάμεσος μεταξύ δύο δικτύων. Οι hosts και τα δίκτυα στην εξωτερική πλευρά μιας security gateway θεωρούνται ως μη-έμπιστα (untrusted) συστήματα, ενώ οι hosts και τα δίκτυα στην εσωτερική πλευρά της security gateway ως έμπιστα (trusted).

Βασική ιδέα στον τομέα της ασφάλειας είναι η έννοια της **σχέσης ασφάλειας (Security Assosiation – SA)** . Είναι μία μονόδρομη (simplex) λογική σύνδεση η οποία παρέχει υπηρεσίες ασφάλειας στα δεδομένα που διακινούνται πάνω από αυτή τη σύνδεση. Υπηρεσίες SA παρέχονται είτε μέσω Authentication

είτε από Encryption. Αν είναι επιθυμητή και Authentication και Encryption τότε απαιτούνται δύο SAs.

Υπάρχουν δύο τύποι SA :

1. **Transport Mode** : Υφίσταται ανάμεσα σε δύο hosts. Η επικεφαλίδα του πρωτοκόλλου ασφάλειας (AH ή ESP) εμφανίζεται μετά την επικεφαλίδα του IP πακέτου και άλλες επικεφαλίδες επέκτασης (extension headers), και πριν από επικεφαλίδες πρωτοκόλλων ανώτερων επιπέδων, όπως TCP και UDP. Όταν χρησιμοποιείται Authentication παρέχεται ασφάλεια για τμήμα της IPv6 επικεφαλίδας και για τα ανώτερα επίπεδα. Όταν χρησιμοποιείται Encryption παρέχεται προστασία μόνο για τα ανώτερα επίπεδα.

2. **Tunnel mode** : Η σχέση ασφάλειας (SA) εφαρμόζεται πάνω σε ένα tunnel. Σε αυτήν την περίπτωση υπάρχουν δύο IP επικεφαλίδες :

   - Μία εξωτερική που καθορίζει τον προορισμό όπου θα γίνει η επεξεργασία των υπηρεσιών ασφάλειας.
   - Μία εσωτερική που καθορίζει τον τελικό προορισμό του πακέτου.

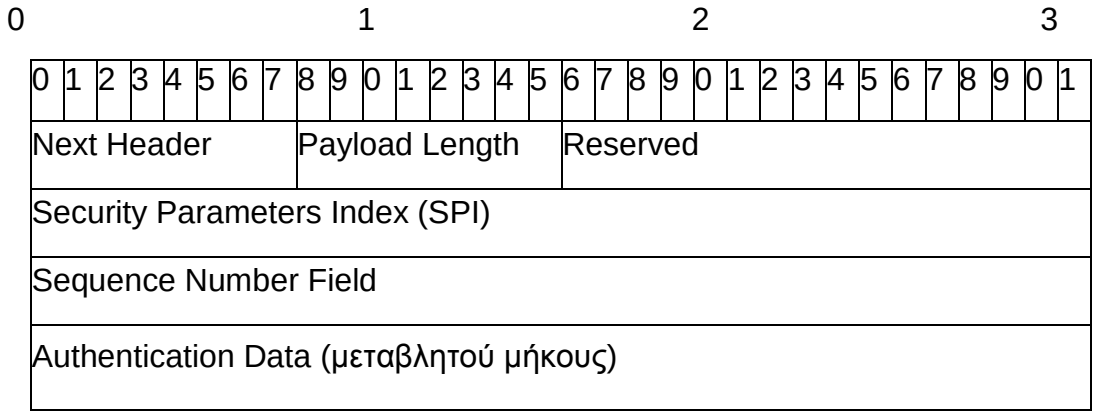
Όταν χρησιμοποιείται AH σε tunnel mode παρέχεται ασφάλεια για τμήματα της εξωτερικής IP επικεφαλίδας και όλο το εσωτερικό πακέτο (που διέρχεται το tunnel), ενώ όταν χρησιμοποιείται ESP παρέχεται προστασία μόνο για το εσωτερικό πακέτο.

Εάν η σχέση ασφάλειας είναι μεταξύ δύο hosts μπορεί να χρησιμοποιηθεί είτε transport είτε tunnel mode. Αν ένα από τα άκρα είναι security gateway τότε μπορεί να χρησιμοποιηθεί μόνο tunnel mode.

6.2 Authentication

Η Authentication επικεφαλίδα παρέχει εμπιστευτικότητα χωρίς σύνδεση (connectionless integrity), επιβεβαίωση αυθεντικότητας προέλευσης δεδομένων (data origin authentication) και προστασία από επαναλήψεις (anti-

replay protection). Η τελευταία είναι προαιρετική και μπορεί να επιλεγεί από το δέκτη κατά την αρχικοποίηση μιας σχέσης εμπιστοσύνης (SA).



Σχήμα 6.1 Authentication επικεφαλίδα

Όλα τα παραπάνω πεδία είναι υποχρεωτικά.

- **Next Header** : Ένα 8-bit πεδίο που καθορίζει τον τύπο των δεδομένων που ακολουθούν.
- **Payload Length** : Ένα 8-bit πεδίο που δίνει το μήκος της AH επικεφαλίδας σε λέξεις (words) των 32-bit, μείον “2” (δύο 32-bit words). Στη συνηθισμένη περίπτωση η τιμή αυτή θα είναι 4.
- **Reserved** : Ένα 16-bit πεδίο για μελλοντική χρήση. Πρέπει να έχει τιμή μηδέν.
- **Security Parameters Index (SPI)** : Ένα 32-bit πεδίο το οποίο σε συνδυασμό με τη διεύθυνση προορισμού του IP πακέτου και το πρωτόκολλο ασφάλειας (AH) προσδιορίζει μοναδικά τη σχέση ασφάλειας (SA) για αυτό το datagram. Η τιμή μηδέν έχει κρατηθεί για τοπική χρήση.
- **Sequence Number** : Ένα μη-προσημασμένο 32-bit πεδίο το οποίο αυξάνει μονότονα. Αρχικά οι μετρητές στα άκρα μιας SA είναι μηδέν, αυξάνουν πριν κάθε αποστολή και άρα το πρώτο πακέτο που στέλνεται σε μια συγκεκριμένη SA έχει Sequence Number 1. Για αποφυγή επαναλήψεων το πεδίο αυτό δεν πρέπει να μετράει κυκλικά. Μετά τη μετάδοση του 2^{32} πακέτου μιας SA τα δύο άκρα πρέπει να αρχικοποιήσουν ξανά τους μετρητές τους. Για τον έλεγχο των πακέτων και την αποφυγή διπλότυπων πακέτων χρησιμοποιείται ένα

παράθυρο με μέγεθος τουλάχιστον 32 αλλά προτιμότερα 64. Ένα πακέτο με Sequence Number αριστερότερα του παραθύρου (με μικρότερο δηλαδή Sequence Number) απορρίπτεται.

Αν έχει Sequence Number μέσα στο παράθυρο και είναι καινούριο ή αν έχει Sequence Number δεξιότερα του παραθύρου γίνεται ο έλεγχος του ICV, όπως εξηγείται παρακάτω. Αν ο έλεγχος είναι επιτυχής το παράθυρο ανανεώνεται.

- **Authentication Data** : Πεδίο μεταβλητού μήκους που περιέχει την **τιμή ελέγχου ακεραιότητας (ICV – Integrity Check Value)** για αυτό το πακέτο. Το μήκος του πρέπει να είναι ακέραιο πολλαπλάσιο των 32 bits, και για αυτό το λόγο μπορεί να χρησιμοποιηθεί padding (συμπλήρωμα).

Σε transport mode η Authentication επικεφαλίδα εισάγεται μετά την βασική IPv6 επικεφαλίδα και τις επεκτάσεις της Hop-by-hop, Routing και Fragmentation, αν αυτές υπάρχουν. Η επέκταση της επικεφαλίδας Destination options μπορεί να μπει είτε πριν είτε μετά την AH επικεφαλίδα, ανάλογα με τη σημασία που θέλουμε να δοθεί.

Βασική IPv6 επικεφαλίδα	Επεκτάσεις επικεφαλίδας (αν υπάρχουν)	TCP	Δεδομένα

Σχήμα 6.2 Πριν την εισαγωγή της authentication επικεφαλίδας

Βασική IPv6 επικεφαλίδα	Hop-by-hop, destination*, routing, fragmentation	Authentication Header	Destination options*	TCP	Δεδομένα

Σχήμα 6.3 Μετά την εισαγωγή της authentication επικεφαλίδας

Σε tunnel mode όπως αναφέραμε η εσωτερική IPv6 επικεφαλίδα μεταφέρει τις τελικές διευθύνσεις πηγής και προορισμού, ενώ η εξωτερική επικεφαλίδα μπορεί να μεταφέρει ίσως και διαφορετικές διευθύνσεις, για παράδειγμα διευθύνσεις security gateways. Έτσι η AH επικεφαλίδα προστατεύει όλο το πακέτο, συμπεριλαμβάνοντας και όλη την εσωτερική επικεφαλίδα.

Η σχετική θέση της AH επικεφαλίδας ως προς την εξωτερική IPv6 επικεφαλίδα είναι ίδια όπως σε transport mode :

Νέα IPv6 επικεφαλίδα	Επεκτάσεις επικεφαλίδας (αν υπάρχουν)	Authentication Header	Αρχική IPv6 επικεφαλίδα	Επεκτάσεις επικεφαλίδας (αν υπάρχουν)	TCP	Δεδομένα

Σχήμα 6.4 Επικεφαλίδα σε transport mode

Αν χρειάζονται περισσότερες της μιας επικεφαλίδες ασφάλειας (AH ή ESP) είτε χρησιμοποιείται transport mode είτε tunnel mode, κάθε επικεφαλίδα αγνοεί την ύπαρξη των επόμενων, ενώ η σειρά τους καθορίζεται από την πολιτική ασφάλειας της υλοποίησης.

Ο αλγόριθμος που θα χρησιμοποιηθεί για authentication καθορίζεται από την SA. Για επικοινωνία σημείου-προς-σημείο κατάλληλοι αλγόριθμοι είναι οι Message Authentication Codes (MACs) οι οποίοι βασίζονται σε αλγόριθμους συμμετρικής κρυπτογράφησης (symmetric encryption algorithms, π.χ. DES) ή σε συναρτήσεις one-way hash (π.χ. MD5 ή SHA-1). Μία υλοποίηση θα παρέχει σίγουρα τους αλγορίθμους HMAC με MD5 και HMAC με SHA-1.

Το ICV στα Authentication Data της AH επικεφαλίδας υπολογίζεται βάσει :

- Των πεδίων της IPv6 επικεφαλίδας που είτε είναι αμετάβλητα κατά τη μεταφορά του πακέτου ή που οι αλλαγές τους είναι προβλέψιμες σαν τιμή με την άφιξή τους στο άλλο άκρο της AH SA.

- Της AH επικεφαλίδας (Next Header, Payload Length, Reserved, SPI, Sequence Number, Authentication Data (τα οποία θεωρούνται μηδέν για αυτόν τον υπολογισμό) και τυχόν padding bytes).
- Τα δεδομένα των πρωτοκόλλων ανώτερων επιπέδων που θεωρούνται αμετάβλητα κατά τη μεταφορά.

Τα πεδία της βασικής IPv6 επικεφαλίδας μπορούν να χωριστούν ως εξής:

Αμετάβλητα	Version Payload Length Next Header (που πρέπει να έχει την τιμή 51 για AH) Source Address Destination Address (χωρίς Routing Extension Header)
Μεταβλητά αλλά προβλέψιμα	Destination Address (με Routing Extension Header)
Μεταβλητά (μηδενίζονται πριν τον υπολογισμό του ICV)	Class Flow Label Hop Limit

Σχήμα 6.5 Τα πεδία της βασικής IPv6 επικεφαλίδας

Οι επεκτάσεις τη επικεφαλίδας Hop-by-Hop και Destination περιέχουν ένα bit που δείχνει αν η τιμή τους μπορεί να αλλάξει απρόβλεπτα κατά τη μεταφορά. Αν το bit λέει ότι μπορεί να αλλάξουν τότε για τον υπολογισμό του ICV γίνονται μηδέν. Αν λέει ότι θα μείνουν αμετάβλητα τότε συμπεριλαμβάνονται στον υπολογισμό.

Με τη λήψη ενός πακέτου που περιέχει μια AH επικεφαλίδα ο δέκτης προσδιορίζει την κατάλληλη SA, βάσει της διεύθυνσης προορισμού, του πρωτοκόλλου ασφάλειας (AH) και του SPI. Η SA καθορίζει αν θα ελεγχθεί το Sequence Number, ποιος αλγόριθμος θα χρησιμοποιηθεί για τον υπολογισμό του ICV και το κλειδί για να ελεγχθεί η εγκυρότητα του ICV. Αν δεν υπάρχει SA για αυτή τη σύνοδο ο δέκτης απορρίπτει το πακέτο και καταγράφει την τιμή SPI, την ημερομηνία και την ώρα που παραλήφθηκε, τις διευθύνσεις πηγής και προορισμού καθώς και το Flow ID.

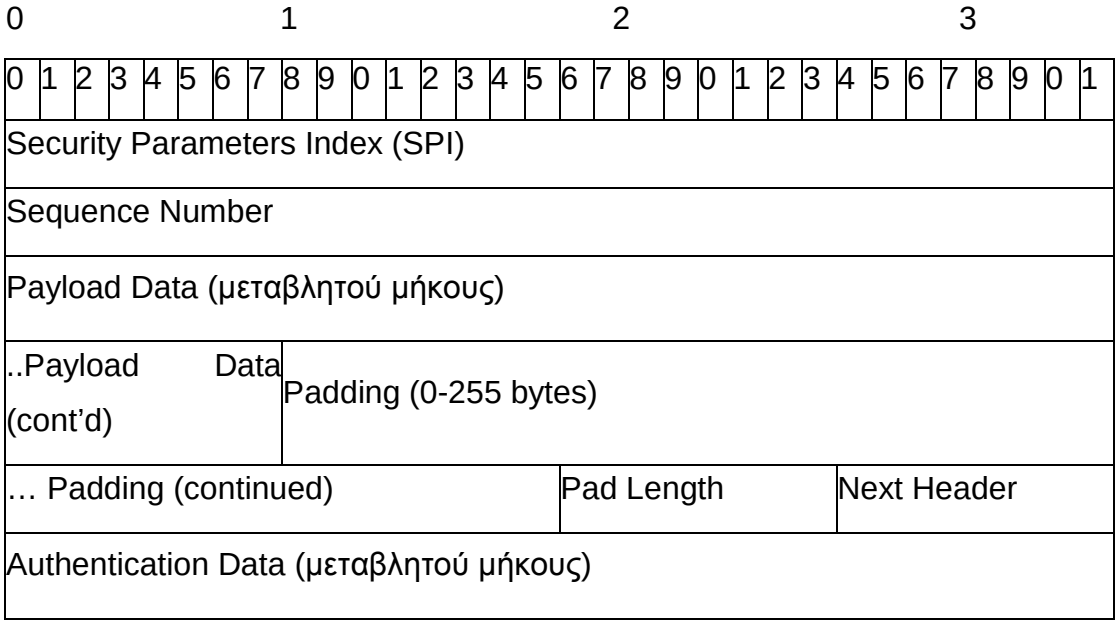
Αν βρεθεί η κατάλληλη SA ο δέκτης υπολογίζει το ICV βάσει των κατάλληλων πεδίων του πακέτου χρησιμοποιώντας τον αλγόριθμο που καθορίζει η SA και ελέγχει αν είναι ίδιο με το ICV που περιέχεται στα Authentication Data.
Αν είναι ίδιο τότε το πακέτο είναι έγκυρο και γίνεται αποδεκτό. Αν όχι τότε το πακέτο απορρίπτεται ως μη έγκυρο και καταγράφεται η τιμή SPI, η ημερομηνία και η ώρα που παραλήφθηκε, οι διευθύνσεις πηγής και προορισμού καθώς και το Flow ID.

6.3 Encryption

Η επικεφαλίδα Encapsulating Security Payload (ESP) προσφέρει μία ποικιλία υπηρεσιών ασφάλειας και, όπως αναφέρθηκε μπορεί να χρησιμοποιηθεί μόνη της, ή σε συνδυασμό με την Authentication επικεφαλίδα. Παρέχει εμπιστευτικότητα (confidentiality), επιβεβαίωση αυθεντικότητας προέλευσης δεδομένων (data origin authentication), ακεραιότητα χωρίς σύνδεση (connectionless integrity), προστασία από επαναλήψεις (anti-replay) και περιορισμένη εμπιστευτικότητα ροής κίνησης (traffic flow confidentiality). Μία υλοποίηση μπορεί να παρέχει ορισμένες μόνο από τις υπηρεσίες αυτές, και η εμπιστευτικότητα μπορεί να επιλεγεί ανεξάρτητα από τις άλλες υπηρεσίες. Παρ' όλα αυτά η χρήση της εμπιστευτικότητας χωρίς ακεραιότητα και επιβεβαίωση αυθεντικότητας προέλευσης δεδομένων είτε από το ESP είτε σε συνδυασμό με την AH επικεφαλίδα μπορεί να υποστεί επιθέσεις που θα υπονομεύσουν και την εμπιστευτικότητα και γι' αυτό δεν συνίσταται. Η

επιβεβαίωση της αυθεντικότητας της πηγής προέλευσης και η χωρίς σύνδεση ακεραιότητα είναι ενιαίες υπηρεσίες και προσφέρονται ως επιλογή με την εμπιστευτικότητα. Αν και η εμπιστευτικότητα και η αυθεντικότητα είναι προαιρετικές, μία τουλάχιστον από αυτές πρέπει να επιλεγεί. Η προστασία από επαναλήψεις προϋποθέτει επιβεβαίωση αυθεντικότητας προέλευσης και η ενεργοποίησή της εξαρτάται από τον δέκτη, ενώ η εμπιστευτικότητα ροής είναι δυνατή μόνο σε tunnel mode.

Παρακάτω δίνεται η ESP επικεφαλίδα :



Σχήμα 6.6 Η ESP επικεφαλίδα

Ορισμένα από τα πεδία είναι **προαιρετικά (optional)** και άλλα **υποχρεωτικά (mandatory)**. Προαιρετικά σημαίνει ότι το πεδίο μπορεί να μην περιέχεται στο πακέτο, δηλαδή να μην είναι παρόν κατά τη μετάδοσή του ούτε να υπολογίζεται για το ICV. Το αν ένα πεδίο θα περιέχεται ή όχι καθορίζεται κατά

την αρχικοποίηση της SA και άρα τα ESP πακέτα έχουν την ίδια μορφή καθ' όλη τη διάρκεια μιας SA. Υποχρεωτικά πεδία σημαίνει ότι βρίσκονται πάντα στο ESP πακέτο για όλες τις SA.

- **Security Parameters Index (SPI)** : Ένα 32-bit υποχρεωτικό πεδίο. Σε συνδυασμό με τη διεύθυνση προορισμού του IP πακέτου και το πρωτόκολλο ασφάλειας (AH) προσδιορίζει μοναδικά τη σχέση ασφάλειας (SA) για αυτό το datagram. Η τιμή μηδέν έχει κρατηθεί για τοπική χρήση.

- **Sequence Number** : Ένα 32-bit μη-προσημασμένο υποχρεωτικό πεδίο το οποίο αυξάνει μονότονα. Αρχικά οι μετρητές στα άκρα μιας SA είναι μηδέν, αυξάνουν πριν κάθε αποστολή και άρα το πρώτο πακέτο που στέλνεται σε μια συγκεκριμένη SA έχει Sequence Number 1. Για αποφυγή επαναλήψεων το πεδίο αυτό δεν πρέπει να μετράει κυκλικά. Μετά τη μετάδοση του 2^{32} πακέτου μιας SA τα δύο άκρα πρέπει να αρχικοποιήσουν ξανά τους μετρητές τους. Για τον έλεγχο των πακέτων και την αποφυγή διπλότυπων πακέτων χρησιμοποιείται ένα παράθυρο με μέγεθος τουλάχιστον 32 αλλά προτιμότερα 64. Ένα πακέτο με Sequence Number αριστερότερα του παραθύρου (με μικρότερο δηλαδή Sequence Number) απορρίπτεται. Αν έχει Sequence Number μέσα στο παράθυρο και είναι καινούριο ή αν έχει Sequence Number δεξιότερα του παραθύρου γίνεται ο έλεγχος του ICV, όπως εξηγείται παρακάτω. Αν ο έλεγχος είναι επιτυχής το παράθυρο ανανεώνεται.

- **Payload Data**:Υποχρεωτικό πεδίο μεταβλητού μήκους (ακέραιου αριθμού bytes) που περιέχει τα δεδομένα που περιγράφονται στο πεδίο Next Header.

- **Padding**:Το πεδίο αυτό είναι προαιρετικό και το μέγεθός του κυμαίνεται από 0-255 bytes. Χρησιμοποιείται στις εξής περιπτώσεις :

  ο Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται απαιτεί το plaintext (δηλαδή τα πεδία Payload Data, Pad Length, Next Header και

Padding) να είναι πολλαπλάσια ενός αριθμού bytes, οπότε συμπληρώνεται από τα bytes του Padding. Σε αυτήν την περίπτωση ο υπολογισμός του Padding δεν λαμβάνει υπόψη του τα πεδία Pad Length, Next Header και το Initialization Vector (IV – πίνακα αρχικοποίησης) που χρησιμοποιεί ο αλγόριθμος για την κρυπτογράφηση του φορτίου.

ο Τα πεδία Pad Length και Next Header πρέπει να βρίσκονται όπως φαίνεται στο σχήμα της ESP επικεφαλίδας στο τέλος μιας τετράδας bytes και τα Authentication Data να ξεκινούν σε μία καινούρια τετράδα bytes. Σε αυτήν την περίπτωση ο υπολογισμός του Padding λαμβάνει υπόψη του τα πεδία Pad Length, Next Header και το Initialization Vector (IV – πίνακα αρχικοποίησης) που χρησιμοποιεί ο αλγόριθμος για την κρυπτογράφηση του φορτίου.

ο Το Padding μπορεί επίσης να χρησιμοποιηθεί για να αποκρύψει το πραγματικό μέγεθος του φορτίου, για τους σκοπούς της εμπιστευτικότητας της ροής της κίνησης.

- **Pad Length** : Υποχρεωτικό πεδίο που παίρνει τις τιμές 0-255 και δείχνει τον αριθμό των bytes στο Padding πεδίο. Η τιμή μηδέν σημαίνει ότι δεν υπάρχει Padding.

- **Next Header** : Υποχρεωτικό 8-bit πεδίο που δείχνει τον τύπο των δεδομένων που περιέχονται στο πεδίο Payload Data, π.χ. μία επικεφαλίδα επέκτασης ή το αναγνωριστικό ενός πρωτοκόλλου ανώτερου επιπέδου.

- **Authentication Data** : Προαιρετικό πεδίο μεταβλητού μήκους, το οποίο περιέχει την τιμή ελέγχου ακεραιότητας (ICV – Integrity Check Value) η οποία υπολογίζεται από το ESP πακέτο εκτός του πεδίου αυτού. Υφίσταται αν η υπηρεσία επιβεβαίωσης αυθεντικότητας έχει επιλεγεί για τη συγκεκριμένη SA και το μήκος του εξαρτάται από τη μέθοδο που χρησιμοποιείται.

Σε transport mode η ESP επικεφαλίδα εισάγεται μετά την βασική IPv6 επικεφαλίδα και τις επεκτάσεις της Hop-by-hop, Routing και Fragmentation, αν αυτές υπάρχουν. Η επέκταση της επικεφαλίδας Destination options μπορεί να μπει είτε πριν είτε μετά την ESP επικεφαλίδα, ανάλογα με τη σημασία που θέλουμε να δοθεί. Επειδή όμως η ESP υπηρεσία προστατεύει μόνο τα πεδία που ακολουθούν την ESP επικεφαλίδα είναι γενικά προτιμότερο να βρίσκεται μετά την ESP επικεφαλίδα.

Βασική IPv6 επικεφαλίδα	Επεκτάσεις επικεφαλίδας (αν υπάρχουν)	TCP	Δεδομένα

Σχήμα 6.7 Πριν την εισαγωγή της authentication επικεφαλίδας

Βασική IPv6 επικεφαλίδα	Hop-by-hop, destination*, routing, fragmentation	ESP Header	Destination options*	TCP	Δεδομένα	ESP Trailer	ESP Authentication

Σχήμα 6.8 Μετά την εισαγωγή της authentication επικεφαλίδας

Σε tunnel mode όπως αναφέραμε η εσωτερική IPv6 επικεφαλίδα μεταφέρει τις τελικές διευθύνσεις πηγής και προορισμού, ενώ η εξωτερική επικεφαλίδα μπορεί να μεταφέρει ίσως και διαφορετικές διευθύνσεις, για παράδειγμα διευθύνσεις security gateways. Έτσι η ESP επικεφαλίδα προστατεύει όλο το πακέτο, συμπεριλαμβάνοντας και όλη την εσωτερική επικεφαλίδα. Η σχετική

θέση της ESP επικεφαλίδας ως προς την εξωτερική IPv6 επικεφαλίδα είναι ίδια όπως σε transport mode :

Νέα IPv6 επικεφαλίδα	Νέες επεκτάσεις επικεφαλίδας	ESP Header	Αρχική IPv6 επικεφαλίδα	Αρχικές επεκτάσεις επικεφαλίδας	TCP	Δεδομένα	ESP Trailer	ESP Authentication

Σχήμα 6.9 Μετά την εισαγωγή της authentication επικεφαλίδας σε transport mode

Οι αλγόριθμοι που θα χρησιμοποιηθούν για authentication και encryption καθορίζονται από την SA. Για επικοινωνία σημείου-προς-σημείο κατάλληλοι authentication αλγόριθμοι είναι οι Message Authentication Codes (MACs) οι οποίοι βασίζονται σε αλγόριθμους συμμετρικής κρυπτογράφησης (symmetric encryption algorithms, π.χ. DES) ή σε συναρτήσεις one-way hash (π.χ. MD5 ή SHA-1). Μία υλοποίηση θα παρέχει σίγουρα τους αλγορίθμους HMAC με MD5, HMAC με SHA-1, DES σε CBC mode, NULL Authentication και NULL Encryption.

Η διαδικασία κρυπτογράφησης στον αποστολέα είναι η εξής :

1. Ενθυλάκωση στο ESP Payload πεδίο των δεδομένων ανώτερων πρωτοκόλλων αν έχουμε transport mode ή ολόκληρου του IPv6 datagram αν έχουμε tunnel mode.
2. Προσθήκη Padding αν χρειάζεται.
3. Κρυπτογράφηση των πεδίων Payload Data, Padding, Pad Length, Next Header χρησιμοποιώντας κλειδί, αλγόριθμο και τρόπο λειτουργίας αλγορίθμου όπως ορίζει η σχέση ασφάλειας (SA).

Αν έχει επιλεγεί authentication γίνεται πρώτα η κρυπτογράφηση, η οποία δεν περιλαμβάνει το πεδίο Authentication Data. Κατόπιν γίνεται υπολογισμός του ICV πάνω στο ESP πακέτο χωρίς τα Authentication Data, δηλαδή πάνω στα

πεδία SPI, Sequence Number, Payload Data, Padding, Pad Length και Next Header, με τα τέσσερα τελευταία πεδία να είναι σε κρυπτογραφική μορφή λόγω της κρυπτογράφησης που προηγήθηκε.

Με τη λήψη ενός πακέτου που περιέχει μια ESP επικεφαλίδα ο δέκτης προσδιορίζει την κατάλληλη SA, βάσει της διεύθυνσης προορισμού, του πρωτοκόλλου ασφάλειας (ESP) και του SPI. Η SA καθορίζει αν θα ελεγχθεί το Sequence Number, αν πρέπει να υπάρχουν Authentication Data στο πακέτο, ποιοι αλγόριθμοι θα χρησιμοποιηθούν για την αποκρυπτογράφηση και για τον υπολογισμό του ICV και το κλειδί για να ελεγχθεί η εγκυρότητα του ICV. Αν δεν υπάρχει SA για αυτή τη σύνοδο ο δέκτης απορρίπτει το πακέτο και καταγράφει την τιμή SPI, την ημερομηνία και την ώρα που παραλήφθηκε, τις διευθύνσεις πηγής και προορισμού καθώς και το Flow ID.

Αν βρεθεί η κατάλληλη SA και έχει επιλεγεί επιβεβαίωση αυθεντικότητας προέλευσης (authentication) ο δέκτης υπολογίζει το ICV βάσει των κατάλληλων πεδίων του πακέτου χρησιμοποιώντας τον αλγόριθμο που καθορίζει η SA και ελέγχει αν είναι ίδιο με το ICV που περιέχεται στα Authentication Data. Αν είναι ίδιο τότε το πακέτο είναι έγκυρο και γίνεται αποδεκτό. Αν όχι τότε το πακέτο απορρίπτεται ως μη έγκυρο και καταγράφεται η τιμή SPI, η ημερομηνία και η ώρα που παραλήφθηκε, οι διευθύνσεις πηγής και προορισμού καθώς και το Flow ID.

Η διαδικασία αποκρυπτογράφησης είναι η εξής :

1. δέκτης αποκρυπτογραφεί τα πεδία Payload Data, Padding, Pad Length και Next Header χρησιμοποιώντας το κλειδί, τον αλγόριθμο, τον τρόπο λειτουργίας του αλγορίθμου και τυχόν δεδομένα συγχρονισμού κρυπτογράφησης (cryptographic synchronization data) που έχουν επιλεγεί από την SA.
2. Επεξεργάζεται το πεδίο Padding όπως έχει οριστεί από την κρυπτογράφηση.

3. Ανακατασκευάζει το αρχικό IPv6 πακέτο από την αρχική επικεφαλίδα συν αρχικά δεδομένα πρωτοκόλλων ανώτερων επιπέδων στο Payload πεδίο αν πρόκειται για transport mode, ή από την εξωτερική IPv6 επικεφαλίδα και όλο το IPv6 datagram στο Payload πεδίο.

Αν έχει επιλεγεί authentication, ο έλεγχος του ICV και η αποκρυπτογράφηση μπορούν να γίνουν είτε σειριακά είτε παράλληλα. Αν γίνουν σειριακά πρέπει να γίνει πρώτα ο έλεγχος του ICV ενώ αν γίνουν παράλληλα πρέπει ο έλεγχος να έχει ολοκληρωθεί πριν το αποκρυπτογραφημένο πακέτο προωθηθεί για περαιτέρω επεξεργασία.

6.4 Η ασφάλεια που ορίζει το IPsec

Το IPsec πρότυπο ορίζει τους μηχανισμούς ασφάλειας που μπορούν να χρησιμοποιηθούν από το IP πρωτόκολλο ανεξαρτήτως έκδοσης ώστε να επιτυγχάνεται ασφάλεια στο επίπεδο δικτύου. Ένα σύστημα χρησιμοποιεί το IPsec για να απαιτήσει από τους κόμβους που επικοινωνεί να κάνουν χρήση συγκεκριμένων αλγορίθμων και πρωτοκόλλων ασφαλείας. Το IPsec παρέχει και τα εργαλεία με τα οποία ένα σύστημα μπορεί να διαπραγματευτεί με άλλα συστήματα για να καταλήξουν για παράδειγμα σε κοινή χρήση ενός αλγόριθμου κωδικοποίησης.
Οι υπηρεσίες που μπορούν να θεωρηθούν μέρος του IPsec περιλαμβάνουν:

- **Έλεγχο πρόσβασης**: Η πρόσβαση σε οποιαδήποτε υπηρεσία ή σύστημα απαιτεί τον κατάλληλο κωδικό. Υπάρχουν διάφορα πρωτόκολλα ασφάλειας που μπορούν να χρησιμοποιηθούν για να ορίσουν μία ασφαλή ανταλλαγή κλειδιών.
- **Ακεραιότητα δεδομένων**: Είναι δυνατή η πιστοποίηση ακεραιότητας ενός οποιουδήποτε IP πακέτου χωρίς την ανάγκη να ελεγχθεί άλλο πακέτο πριν ή μετά από το πακέτο που πρέπει να ελεγχθεί. Αυτό μπορεί να επιτευχθεί με χρήση τεχνικών hashing.

- **Πιστοποίηση του αποστολέα**: Είναι δυνατή η πιστοποίηση του αποστολέα με χρήση των κατάλληλων αλγορίθμων ψηφιακών υπογραφών.
- **Προστασία εναντίον επιθέσεων τύπου packet replay**: Παρέχονται μηχανισμοί προστασίας του κόμβου αποστολέα από επιθέσεις όπου ο επιτιθέμενος προσπαθεί να βλάψει τη διαθεσιμότητα του συστήματος, υποκλέπτοντας ένα πακέτο και στέλνοντάς το πολλές φορές στον αποστολέα.
- **Κωδικοποίση-των-δεδομένων**:Παρέχονται-μηχανισμοί κωδικοποίησης για να εξασφαλιστεί το απόρρητο των δεδομένων.
- **Εξασφάλιση απορρήτου της ροής των δεδομένων**: Παρέχονται μηχανισμοί προστασίας της ροής των πακέτων ώστε ο επιτιθέμενος να μην μπορεί να βγάλει συμπεράσματα παρακολουθώντας ένα προς ένα τα πακέτα (που μπορεί να είναι κωδικοποιημένα).

6.5 Εφαρμογή των μηχανισμών ασφαλείας

Οι μηχανισμοί ασφάλειας του IP μπορούν να εφαρμοστούν σε παραλλαγές που επιτρέπουν την συμμετοχή μηχανών που δεν έχουν στη στοίβα τους υποστήριξη για τους μηχανισμούς αυτούς. Οι τρεις δυνατές περιπτώσεις περιγράφονται στην συνέχεια.

- **Σταθμός εργασίας με Σταθμό εργασίας**

  Σε αυτή την περίπτωση έχουμε επικοινωνία μεταξύ δύο υπολογιστών, όπου και οι δύο έχουν την ικανότητα να χρησιμοποιήσουν τους μηχανισμούς ασφαλείας.

- **Δρομολογητής/ Πύλη Ασφάλειας με Σταθμό εργασίας**

Ο ένας από τους δύο host διαθέτει μηχανισμό ασφαλείας. Ο άλλος host βρίσκεται σε κάποιο δίκτυο στο οποίο όλοι οι host θεωρούνται έμπιστοι μεταξύ τους και ένα gateway αναλαμβάνει να διασφαλίσει την ασφάλεια των επικοινωνιών με τον υπόλοιπο κόσμο, εκτός του εσωτερικού δικτύου.

- **Δρομολογητής/ Πύλη Ασφάλειας με Δρομολογητή/ Πύλη Ασφάλειας**
  Τέλος έχουμε την περίπτωση δύο δικτύων που εμπιστεύονται όλους τους host που το καθένα περιλαμβάνει, και επιθυμούν να μιλήσουν μεταξύ τους εξασφαλίζοντας ασφάλεια από το υπόλοιπο δίκτυο. Ουσιαστικά αυτή η περίπτωση απεικονίζει ένα VPN. Εδώ βρίσκει εφαρμογή το Tunnel επίπεδο λειτουργίας της μεθόδου IP Encapsulating security Payload του IPv6.

6.6 Αποδοχή του πρωτοκόλλου

Από την άποψη της ασφάλειας, το νέο πρωτόκολλο IPv6 αποτελεί μια σημαντική πρόοδο σε σχέση με το παλιό IPv4. Ωστόσο, παρά τις αναρίθμητες αρετές του, το IPv6 εξακολουθεί να είναι κατά πολύ ευάλωτο.Είναι σημαντικό να αναγνωρίσουμε ότι το IPv6 δεν είναι αναγκαστικά πιο ασφαλές από το IPv4. Στην πραγματικότητα, το IPv6 όσον αφορά την ασφάλεια είναι μόνο οριακά καλύτερο από το IPv4.Σε αυτή την ενότητα θα αναδείξουμε ορισμένες από τις περιοχές του IPv6, όπου η ασφάλεια εξακολουθεί να αποτελεί σημαντικό ζήτημα.

6.6.1.Dual-stack

Σήμερα, το Διαδίκτυο εξακολουθεί να χρησιμοποιεί ως επί το πλείστον το IPv4. Ωστόσο, είναι εύλογο να αναμένεται ότι αυτό θα αλλάξει σύντομα, καθώς όλο και περισσότερα δίκτυα μετανάστευσαν στο νέο πρωτόκολλο.Δυστυχώς, μεταναστεύουν εκατομμύρια οπότε πρόκειται να

πάρει αρκετό καιρό.Ωστώσο κάποια μορφής 6to4 διπλής στοίβας θα βγει στην αγορα πετυχαίνοντας την επιθυμητή λειτουργικότητα.

6.6.2.Θέματα ασφάλειας επικεφαλίδων

Η χρήση των επικεφαλίδων επέκτασης και IPSec μπορεί να αποτρέψει μερικές κοινές επίθεσης με βάση την διαχείρηση της κεφαλίδας. Ωστόσο, το γεγονός ότι η Authentication Header(EH) πρέπει να γίνεται από όλες τις στοίβες μπορούν να αποτελέσουν πηγή του προβλήματος-μια μακρά αλυσίδα EH ή κάποια πολύ μεγάλου μεγέθους θα μπορούσε να χρησιμοποιηθεί για να συντρίψει ορισμένους κόμβους (π.χ. firewalls) ή μεταμφίεση μια επίθεσης. Οι βέλτιστες πρακτικές συνιστούν να φιλτράρει την κυκλοφορία, ωστόσο ο κίνδυνος της πλαστογράφησης συνεχίζει να υφίσταται σε δίκτυα IPv6.

6.6.3.Θέματα που αφορούν το Flooding

Σάρωση για έγκυρες διευθύνσεις και υπηρεσιών είναι πολύ πιο δύσκολο σε IPv6 δίκτυα από ό, τι σε δίκτυα IPv4.Για να ανιχνεύσει αποτελεσματικά μια ολόκληρη κατηγορία IPv6 μπορεί να διαρκέσει έως και 580 δισεκατομμυρίων χρόνια, επειδή ο χώρος διευθύνσεων χρησιμοποιεί 64 bits.Νέα χαρακτηριστικά όπως είναι οι διευθύνσεις multicast εξακολουθούν να είναι πηγή προβλημάτων.

6.6.4.Mobility

Το Mobility είναι ένα εντελώς νέο χαρακτηριστικό του IPv6 που δεν ήταν διαθέσιμο στο προκατόχου του. Το Mobility είναι ένα πολύ σύνθετο στην λειτουργία του που εγείρει ένα σημαντικό μέρος των ανησυχιών κατά την εξέταση της ασφάλειας.Το Mobility χρησιμοποιεί δύο τύπους διευθύνσεων, η πραγματική διεύθυνση και η κινητή διεύθυνση. Το πρώτο είναι ένα τυπικό υπόδειγμα διεύθυνσης IPv6 που περιέχονται στην επέκταση της κεφαλίδα. Η δεύτερη είναι μια προσωρινή διεύθυνση που περιέχεται στην επικεφαλίδα IP. Λόγω των χαρακτηριστικών της εν λόγω δικτύων (κάτι πιο

πολύπλοκο, αν λάβουμε υπόψη την ασύρματη mobility), η προσωρινή διεύθυνση ενός κόμβου θα μπορούσε να εκτεθεί σε πλαστογράφηση. Το Mobility απαιτεί ειδικά μέτρα ασφάλειας και οι διαχειριστές του δικτύου πρέπει να γνωρίζουν καλά και να λάβουν όλες τις παραμέτρους υπ΄όψιν.

Δεν υπάρχει καμία αμφιβολία, το IPv6 αποτελεί σημαντική βελτίωση σε σύγκριση με το παλαιό πρωτόκολλο IPv4 stack. Η νέα σουίτα πρωτοκόλλων προβλέπει αναρίθμητες δυνατότητες που βελτιώνουν τόσο την λειτουργικότητα, καθώς και ορισμένες ειδικές λειτουργίες ασφαλείας. Ωστόσο, απέχει πολύ από το να είναι άρτια αξιόπιστο. Παρά το γεγονός ότι το IPv6 προσφέρει καλύτερη ασφάλεια (ευρύτερο χώρο για διευθύνσεις και χρήση των κρυπτογραφημένων επικοινωνιών), το πρωτόκολλο θέτει επίσης νέες προκλήσεις για την ασφάλεια. Τελικά, το νέο πρωτόκολλο δημιουργεί και πολλά νέα προβλήματα ασφαλείας που λύνει παλιά. Και αν αυτό δεν είναι αρκετό, η μετάβαση από το παλαιό πρωτόκολλο στοίβας στο νέο μπορεί να παρουσιάσει ακόμη περισσότερες προκλήσεις, κάτι που θα εγγυάται την αφθονία της διασκέδασης για τους επαγγελματίες του δικτύου ασφαλείας στο άμεσο μέλλον.

Πηγή:

- http://www.islab.demokritos.gr/
- http://ru6.cti.gr/bouras/en/index.php
- http://www.cis.ohio-state.edu/~jain/cis788/ipng/index.html (IP: the next genetation, Written by Scott Phillips
- http://www.msci.magic.net/docs/internet-drafts/internet-drafts.html
- "Security Architecture for the Internet Protocol", S. Kent,

ΚΕΦΑΛΑΙΟ 7. IPv6 ΚΑΙ INTERNET

7.1 Είσοδος του IPv6 στο χώρο του Διαδικτύου

Η αύξηση της ζήτησης για υπηρεσίες που βασίζονται στο διαδίκτυο συνεπάγεται ότι, αν δεν ληφθούν μέτρα, ο αριθμός των διαδικτυακών διευθύνσεων για την υποστήριξη αυτής της αναμενόμενης ανάπτυξης σε λίγο δεν θα επαρκεί. Εάν ενθαρρυνθούν οι χρήστες και οι παροχείς του διαδικτύου να υιοθετήσουν το πλέον πρόσφατο πρωτόκολλο Ίντερνετ (IPv6) θα υπάρξει μαζική αύξηση του διαθέσιμου χώρου για διευθύνσεις, κατά τον ίδιο τρόπο που, στον 20ο αιώνα, αυξήθηκαν τα ψηφία στους αριθμούς τηλεφώνων.

Η Ευρωπαϊκή Επιτροπή έθεσε ως στόχο το 25% των βιομηχανικών επιχειρήσεων, των δημόσιων αρχών και των νοικοκυριών της ΕΕ να έχουν υιοθετήσει το IPv6 μέχρι το 2010, και απηύθυνε έκκληση για συντονισμένη δράση σε ευρωπαϊκό επίπεδο ώστε να προετοιμαστούν όλοι οι ενεχόμενοι παράγοντες για την έγκαιρη και αποτελεσματική μετάβαση στο νέο πρωτόκολλο, προκειμένου να αποφευχθεί πρόσθετη επιβάρυνση των καταναλωτών και να δοθεί στις καινοτόμες ευρωπαϊκές επιχειρήσεις ανταγωνιστικό πλεονέκτημα.

«Η πρόληψη είναι καλύτερη από τη θεραπεία, αυτό είναι κάτι που ισχύει απόλυτα στην περίπτωση αυτή» δήλωσε η Επίτροπος, αρμόδια για την Κοινωνία της Πληροφορίας και τα Μέσα Επικοινωνίας, Βίβιαν Ρέντινγκ. Και συμπλήρωσε πως, «βραχυπρόθεσμα, οι επιχειρήσεις και οι δημόσιες αρχές ενδέχεται να δοκιμάσουν να περιορίσουν τις ανάγκες τους στον περιορισμένο χώρο του παλαιού συστήματος, αυτό όμως σημαίνει ότι η Ευρώπη δεν θα μπορέσει να εκμεταλλευτεί την πλέον πρόσφατη διαδικτυακή τεχνολογία και ενδέχεται να αντιμετωπίσει κρίση όταν το παλαιό σύστημα κορεστεί εντελώς από διευθύνσεις. Το IPv6 δίνει τη δυνατότητα για περισσότερες διευθύνσεις στον κυβερνοχώρο από τους κόκκους άμμου των παραλιών όλου του κόσμου. Εάν οι Ευρωπαίοι επιθυμούν να χρησιμοποιήσουν τις τελευταίες διαδικτυακές εφαρμογές όπως έξυπνες ετικέτες στα καταστήματα, στα

εργοστάσια και στα αεροδρόμια, έξυπνα συστήματα θέρμανσης και φωτισμού τα οποία εξοικονομούν ενέργεια, και συστήματα δικτύωσης και πλοήγησης στα αυτοκίνητά τους, τότε η ζήτηση για διευθύνσεις διαδικτύου θα πολλαπλασιαστεί επί χίλια. Με το νέο Πρωτόκολλο Ίντερνετ, το IPv6, θα διατίθεται ένας σχεδόν απεριόριστος αριθμός διαδικτυακών διευθύνσεων εξασφαλίζοντας την υποστήριξη των νέων εφαρμογών που βασίζονται στη χρήση συσκευών οι οποίες θεωρούνται υπερβολικά πολυάριθμες ή ακριβές για το IPv4.Κατά συνέπεια, θα είναι πολύ ευκολότερο για τους οικιακούς χρήστες να κατασκευάζουν τα δικά τους ιδιωτικά δίκτυα και να τα συνδέουν με το Διαδίκτυο.

Το IPv6 θα δώσει ώθηση στη δημιουργία περισσότερο καινοτόμων εφαρμογών του Διαδικτύου, ιδίως εκείνων που βασίζονται στη δικτύωση τεράστιου αριθμού μικρών και απλών συσκευών. Για παράδειγμα, η διαχείριση της ενέργειας για τον φωτισμό των οδών και στα έξυπνα κτίρια θα μπορούσε να βελτιωθεί, το δε Διαδίκτυο θα μπορούσε με μικρό κόστος και αξιόπιστο τρόπο να συνδέσει τηλεχειριζόμενους αισθητήρες στις οικιακές συσκευές καθημερινής χρήσεως.Η δυνατότητα αυτή θα αποτελέσει με τη σειρά της κίνητρο και ευκαιρία για τις επιχειρήσεις να αναπτύξουν κι άλλες καινοτομίες και έτσι να δημιουργήσουν τη νέα γενεά διαδικτυακών εφαρμογών.Οι περισσότεροι νέοι υπολογιστές και εξυπηρετητές που πωλούνται από τους μεγάλους κατασκευαστές είναι ήδη συμβατοί με το πρωτόκολλο IPv6, όμως είναι προσιτοί μόνο μέσω των παλαιών διευθύνσεών του IPv4.Το δίκτυο κορμού για την έρευνα στην Ευρώπη, το GEANT, είναι ήδη συμβατό κατά 100% με το IPv6 και αυτό έχει ως αποτέλεσμα η Ευρώπη να διαθέτει τον μεγαλύτερο αριθμό διευθύνσεων IPv6 από οποιαδήποτε άλλη περιοχή του κόσμου. Όμως, αυτή η εξέλιξη δεν έχει ακόμα περάσει στο δημόσιο διαδίκτυο. Απαιτείται, επομένως, συντονισμένη δράση σε όλη την Ευρώπη, από όλους τους ενδιαφερόμενους, προκειμένου να εξασφαλιστεί ότι η χρήση του IPv6 θα διαδοθεί γρήγορα, τα δε δίκτυα κορμού θα υποστηρίζουν τόσο το IPv4 όσο και το IPv6.

Εν τω μεταξύ, στην Ιαπωνία, μεγάλες εταιρείες τηλεφωνίας διαθέτουν ήδη ένα δημόσιο δίκτυο κορμού IPv6, η δε Κίνα είχε εγκαταστήσει, πριν από τους

Ολυμπιακούς Αγώνες του Πεκίνου, δίκτυα που θα είναι συμβατά και με το IPv4 και με το IPv6.Η κυβέρνηση των Ηνωμένων Πολιτειών επιβάλλει το IPv6 ως απαίτηση στις δημόσιες συμβάσεις, αλλά στην πράξη η διαδικτυακή τεχνολογία τους παραμένει ιδίου επιπέδου με αυτή της ΕΕ.Η Επιτροπή ζήτησε από τα κράτη μέλη να θέσουν τον δημόσιο τομέα τους στην πρωτοπορία της ανάπτυξης του νέου συστήματος μετατρέποντας από IPv4 σε IPv6 τις διαδικτυακές συνδέσεις τους, τους ιστοτόπους του δημοσίου και τις υπηρεσίες ηλεκτρονικών κρατικών υπηρεσιών.Η Επιτροπή επιθυμεί, επίσης, οι σημαντικότεροι ιστότοποι της Ευρώπης να ηγηθούν της προσπάθειας αυτής και σκοπεύει να εξασφαλίσει δεσμεύσεις από τουλάχιστον 100 γνωστούς φορείς εκμετάλλευσης ιστοχώρων όπως οι ραδιοτηλεοπτικοί σταθμοί ή τα διαδικτυακά πρακτορεία ειδήσεων.

Για να παροτρυνθεί η ευρωπαϊκή βιομηχανία τεχνολογιών των πληροφοριών να κινηθεί δυναμικά, τα κράτη μέλη πρέπει να καταστήσουν τη χρήση του IPv6 προϋπόθεση στις δημόσιες συμβάσεις (όπως έχουν ήδη πράξει η Ευρωπαϊκή Επιτροπή και η κυβέρνηση των ΗΠΑ), να ευαισθητοποιήσουν περισσότερο τις επιχειρήσεις και τους οργανισμούς και να βοηθήσουν τη μετάβασή τους στο νέο σύστημα.

7.2 Ένα βήμα πριν τη μετάβαση

Η πραγματική πρόκληση για το IPv6 είναι για το εάν θα επιτύχει να ‘δέσει’ το περιβάλλον του επερχόμενου δικτύου όπου εκτός από τους συμβατικούς υπολογιστές θα αποτελείται από μυριάδες άλλες συσκευές όπως προσωπικοί επεξεργαστές δεδομένων μεγέθους παλάμης (palmtop personal data assistants-PDA), υβριδικά κινητά τηλέφωνα με υπολογιστικές δυνατότητες, έξυπνα κουτιά με ενσωματωμένους Web browsers καθώς και από φωτοτυπικά μηχανήματα ενός γραφείου έως και συσκευές που χρησιμοποιούνται στην κουζίνα ενός σπιτιού. Η επιτυχία του IPv6 θα βασιστεί όμως και στη δυνατότητα του να εντάξει το παλιό στο καινούργιο. Είναι γνωστό το μέγεθος που έχει ήδη το Διαδίκτυο και η μετάβαση από το IPv4 στο

IPv6 δεν είναι απλή υπόθεση αλλά απαιτεί σωστή στρατηγική έτσι ώστε να παραμείνει αδιάλειπτη και αποδοτική η λειτουργία του Διαδικτύου.

Σύμφωνα με τον Μπέκστρομ της ICANN, η πλήρης μετάβαση στο νέο πρότυπο θα πάρει χρόνια, με συνολικό κόστος μερικών δισεκατομμυρίων δολαρίων διεθνώς. Μεγάλοι "παίκτες" του διαδικτύου θα προσθέσουν μαζικά διευθύνσεις IPv6 δοκιμαστικά και ταυτόχρονα, στις 8 Ιουνίου 2011 (ώρα 00:01 Γκρίνουιτς), για να ελέγξουν τυχόν προβλήματα κατά την μετάβαση.

Πηγή:

- http://www.enet.gr (Ελευθεροτυπία)
- http://dast.nlanr.net/Projects/Iperf
- http://www.sniff-em.com/

ΚΕΦΑΛΑΙΟ 8. ΣΥΜΠΕΡΑΣΜΑΤΑ - ΜΕΛΛΟΝΤΙΚΕΣ ΕΞΕΛΙΞΕΙΣ

Σε λιγότερο από ενάμιση χρόνο αναμένεται να εξαντληθούν οι ομάδες διευθύνσεων του Internet που βασίζονται στο πρωτόκολλο IPv4, σύμφωνα με τις τελευταίες εκτιμήσεις. Οι ειδικοί προειδοποιούν ότι μετά τις 9 Σεπτεμβρίου 2011 δε θα υπάρχουν διαθέσιμα πακέτα διευθύνσεων και οι τελευταίες IP θα έχουν δοθεί στους ενδιαφερόμενους μέχρι τον Απρίλιο του 2012. Δεν αποκλείεται, μάλιστα, το όριο αυτό να έρθει πιο κοντά όσο περνά ο καιρός.Όταν άρχισε να δημιουργείται το Internet με τη μορφή που γνωρίζουμε σήμερα, το πρωτόκολλο IPv4 διέθετε περίπου τέσσερα δισεκατομμύρια διευθύνσεις. Το νούμερο αυτό φάνταζε μυθώδες πριν από 30 και πλέον χρόνια, ωστόσο η ραγδαία ανάπτυξη του Internet έδειξε ότι το τέλος του IPv4 δε θα αργούσε να έρθει. Η εκρηκτική αύξηση της φορητότητας συνέβαλε τα μέγιστα στην εξάντληση των αποθεμάτων. Ο διευθυντής της Ripe NCC, η οποία δίνει διευθύνσεις στην Ευρώπη, λέει χαρακτηριστικά: "*Πριν από δέκα χρόνια, λέγαμε ότι η εξάντληση των διευθύνσεων θα γίνει κάποια στιγμή στο μακρινό μέλλον. Τώρα που κυκλοφορούμε όλοι με iPhone, έχουμε ήδη φτάσει στο μακρινό μέλλον*".Αυτή τη στιγμή, μόνο το **7%** των διευθύνσεων του IPv4 είναι ελεύθερο. Αυτό, βέβαια, δε σημαίνει ότι το Internet θα πεθάνει σε δύο χρόνια. Το επόμενο βήμα είναι η υιοθέτηση του πρωτοκόλλου IPv6, η οποία όμως γίνεται με πολύ αργούς ρυθμούς. Αν και τα δύο πρωτόκολλα μπορούν να λειτουργούν παράλληλα, η συνύπαρξη είναι προβληματική σε πολλές περιπτώσεις, καθώς η μετάφραση μιας διεύθυνσης από το ένα πρωτόκολλο στο άλλο συνεπάγεται χρονική καθυστέρηση.

Το IPv6 είναι ένα πρωτόκολλο που θέλοντας και μη, αργά ή γρήγορα θα μας απασχολήσει όλους. Όσο νωρίτερα προετοιμαστούμε τόσο το καλύτερο και τόσο πιο ανώδυνη θα είναι η μετάβαση όταν έρθει ο καιρός για να μεταφέρουμε τα δίκτυά μας σε αυτό. Από την μια μπορεί να αναρωτιόμαστε γιατί να καταφύγουμε στην ακραία λύση να σχεδιάσουμε από την αρχή ένα πρωτόκολλο από τη στγμή που το κόστος είναι τόσο υψηλό και να μην

βρούμε μια άλλη λύση που θα ήταν, για παράδειγμα, να μεγαλώσει η διεύθυνση του IPv4 και να αφεθεί το πρωτόκολλο κατά τα άλλα ως έχει. Αυτό θα σήμαινε ότι οι στοίβες του TCP/IP έπρεπε να ενημερωθούν όλες την ίδια στιγμή. Τελικά το κόστος μιας τέτοιας απλής αλλαγής θα ήταν συγκρίσιμο με αυτό της ολοκληρωτικής αντικατάστασης του με το IPv6 Οπότε είναι προτιμότερο να γίνει η μετάβαση και να υπάρχει ένα καινούριο και καλύτερο πρωτόκολλο δικτύου όπως το IPv6. Κατά το διάστημα της μετάβασης από IPv4 σε IPv6, το οποίο εκτιμάται ότι θα είναι μεγάλο, οι εταιρίες παροχής υπηρεσιών ιντερνέτ (ISPs) θα πρέπει αρχικά να παρέχουν στους πελάτες τους παράλληλα διασύνδεση μέσω διευθύνσεων IPv4 και IPv6 (dual stack).

Το νέο πρωτόκολλο έχει σχεδιαστεί για να ξεπεράσει τους περιορισμούς του IPv4. Όπως προαναφέραμε, η μεγάλη σχεδιαστική φιλοσοφία πίσω από το IPv6 είναι να επεκταθεί η IP διεύθυνση και ταυτόχρονα, να καταστήσει το πρωτόκολλο απλούστερο στη χρήση και πιο αποτελεσματικό στη λειτουργία του. Προφανώς, πρόθεση τους είναι να μεταναστεύσουν σε ένα πρωτόκολλο πολλαπλών υπηρεσιών. Ωστόσο, βασίστηκε σε όλη τη διαδικασία σχεδιασμού πάνω στο IPv4 το οποίο είχε μεγάλη επιτυχία, και τα περισσότερα από τα χαρακτηριστικά που έχουν διατηρηθεί. Επιπλέον, το IPv6 έχει σχεδιαστεί για να συμπληρώνει και άλλα σχετικά πρωτόκολλα που έχουν αναπτυχθεί ή βρίσκονται υπό ανάπτυξη όπως για παράδειγμα πρωτόκολλα που ασχολούνται με την υποστήριξη της φωνής, βίντεο, δεδομένων, ή άλλων διαδικασιών μέσω διαδικτύου.

Πολλές προτάσεις ανά διατήρηση με το μέγεθος του χώρου διευθύνσεων είχαν τεθεί πριν από την IETF. Οι συζητήσεις ξεκίνησαν το 1992, με την τελική ολοκλήρωση των προδιαγραφών για το 1995. Στην ουσία, η σχεδίαση του IPv6 που πραγματοποιήθηκε γρήγορα με την έννοια ότι το Διαδίκτυο θα πρέπει να είναι σε θέση να συνδέσει οποιονδήποτε θέλει να συνδεθεί με αυτό οπουδήποτε στη γη. Μερικές μελέτες υποθέτουν ότι στο μέλλον ίσως ένα πρόσωπο που θα μπορούσε να χρησιμοποιήσει μέχρι και 100 υπολογιστές.

Αυτό μπορεί να φαίνεται παρατραβηγμένο, αλλά να θυμάστε ότι οι υπολογιστές είναι σχεδόν σε κάθε πτυχή της ζωής μας. Υπολογιστές λειτουργούν στα ρολόγια μας και ακόμα και στα αυτοκίνητα μας. LANs κάτω

από καπό του αυτοκινήτου μας, και όλα αυτά τα συστατικά βάσει διευθύνσεων, προκειμένου να λειτουργήσουν σωστά.

Με τον τεράστιο αριθμό διευθύνσεων του IPv6 μας δίνονται σχεδόν άπειρες δυνατότητες δικτύωσης. Είναι πολύ δύσκολο να προβλέψουμε μέχρι που μπορεί να φτάσει αυτό το πρωτόκολλο. Ακόμα και σε κάθε δέντρο του πλανήτη, γίνεται να αναθέσουμε μια ξεχωριστή διεύθυνση IP αν το θελήσουμε χωρίς κανένα πρόβλημα. Υπάρχει η δυνατότητα, σήμερα με το νέο πρωτόκολλο να δώσουμε ζωή σε οποιαδήποτε συσκευή επιθυμούμε δικτυώνοντας την αποκτώντας την δυνατότητα να την χειριστούμε απομακρυσμένα. Μετά την ηλεκτρονική χαρτογράφηση το επόμενο βήμα θα μπορούσε να είναι ο απομακρυσμένος χειρισμός οπουδήποτε οχήματος. Θα μπορούσαμε για παράδειγμα να δικτυώσουμε όλα τα αυτοκίνητα του πλανήτη που αυτή τη στιγμή ο αριθμός τους φτάνει περίπου το ένα δισεκατομμύριο, να ήταν συνδεδεμένα ασύρματα με έναν κεντρικό υπερυπολογιστή που θα διέθετε η κάθε πόλη ο οποίος θα μπορεί να χειρίζεται όλη την κυκλοφορία. Το μόνο όριο του IPv6 είναι η φαντασία μας.

ΚΕΦΑΛΑΙΟ 9. ΒΙΒΛΙΟΓΡΑΦΙΑ

Έντυπη

1. Douglas E. Comer, Δίκτυα και διαδίκτυα υπολογιστών , Τρίτη αμερικάνικη έκδοση, εκδόσεις κλειδάριθμος, ISBN 960-209-584-9

2. Π. Γανός, Α. Γκάμας, Α. Καραλιώτας, Χ. Μπούρας, Δ. Πρίμπας, Κ. Στάμος, IPv6: Το πρωτόκολλο και οι τεχνικές μετάβασης και μεταφερσιμότητας, εκδόσεις Ελληνικά Γράμματα, ISBN 960-442-277-4

3. Bouras, A. Gkamas, D. Primpas, K. Stamos, "Performance Evaluation of the Impact of Quality of Service mechanisms in an IPv6 network for IPv6 - capable real time applications", Journal of Network and Systems Management, Kluwer Academic Publishers, Volume 12, Issue 4, December 2004, pp. 463-483.

4. William Stallings, High-Speed Networks, TCP/IP and ATM Design Principles, Κεφάλαιο 11.2, ISBN: 0-13-525965-7

5. Ed Taylor, Tcp/Ip Complete, κεφάλαια 8.1 εως 8.8, ISBN 0-07-063400-9

6. Youngsong Mun, Hyewon K. Lee, Understanding IPv6, κεφάλαιο 2, ISBN 9780387256146

7. Bouras, P. Ganos, A. Karaliotas, The deployment of IPv6 in an IPv4 world and Transition Mechanisms, Internet Research: Electronic Networking, Applications and Policy, Emerald, Volume 13, Number 2, 2003, pp. 86-93.

Web Sites

1. http://www.islab.demokritos.gr/
2. http://ru6.cti.gr/bouras/en/index.php
3. http://portal.kathimerini.gr/4dcgi/_w_articles_kathciv_1_04/02/2011_37
4. http://www.ipv6-taskforce.gr/
5. http://www.cisco.com
6. http://www.sun.com
7. http://www.atmforum.com
8. http://www.data.com
9. http://www.cis.ohio-state.edu/~jain/cis788/ipng/index.html
10. http://www.msci.magic.net/docs/internet-drafts/internet-drafts.html
11. http://www.student.mckenna.edu/student/ns/krae/thesis/index.html
12. http://playground.sun.com/pub/ipng/html/ipng-main.html
13. http://www.enet.gr
14. http://www.cis.ohio-state.edu/~jain/cis788/ipng/index.html
15. http://www.msci.magic.net/docs/internet-drafts/internet-drafts.html
16. "Security Architecture for the Internet Protocol", S.
17. Kent, http://www.networkworld.com
18. http://itexpertvoice.com
19. http://dast.nlanr.net/Projects/Iperf
20. http://www.sniff-em.com/
21. IPv6 Forum :: Driving IPv6 Deployment, http://www.ipv6forum.com/
22. http://www.webopedia.com/didyouknow/internet/2002/birthoftheinternet.asp

ΚΕΦΑΛΑΙΟ 10. ΛΕΞΙΚΟ ΤΕΧΝΙΚΩΝ ΟΡΩΝ

AH	Authentication Header
AIIH	Assignment of IPv4-gIobal addresses to IPv6 Hosts
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CIDR	Classless Inter-Domain Routing
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DSTM	Dual Stack Transition Mechanism
DTI	Dynamic Tunneling Interface
EGP	External Gateway Protocol
ESP	Encapsulating Security Payload
FH	Fragmentation Header
FTP	File Transfer Protocol
GPS	Global Positioning System
HMAC	keyed-Hash Message Authentication Code
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IGMP	Internet Group Membership Protocol
IGP	Interior Gateway Protocol
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internet Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
LAN	Local Area Networks
MAC address	Medium Access Control
MD5	Message Digest 5
MTU	Maximum Transfer Unit
NAT	Network Address Translation

OSPF	Open Shortest Path First
PDA	Personal Digital Assistant
PPP	Point to Point Protocol
QoS	Quality of Service
RFC	Request For Comments
RH	Routing Header
RIP	Routing Information Protocol
RIPE	Reseaux IP Europeens
RSVP	Resource Reservation Protocol
SA	Security Association
SHA	Secure Hash Algorithm
SPI	Security Parameter Index
TOS	Type Of Service
TTL	Time To Live
UDP	User Datagram Protocol
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Networks
WFQ	Weighted Fair Queuing
XNS	Xerox Network System
TCP	Transmision Control Protocol

ΛΕΞΙΚΟ

Address	Διεύθυνση
Agent	Πράκτορας - η οντότητα που εκτελεί μια λειτουργία εκ μέρους μιας άλλης.
Aggregation	Συνάθροιση
Authentication	Πιστοποίηση
Automatic	Αυτόματος - διαδικασία που δεν απαιτεί τη μεσολάβηση ανθρώπου/διαχειριστή.
Backbone	Δίκτυο κορμού
Bandwidth	Εύρος ζώνης, καθορίζει το ποσό της πληροφορίας που μπορεί να μεταδοθεί από ένα δικτυακό σύνδεσμο στη μονάδα του χρόνου.
Binding	Δέσιμο - ο συνδυασμός της οικείας (home) διεύθυνσης ενός κινητού κόμβου με την προσωρινή (care-of) διεύθυνση και τη χρονική διάρκεια εγκυρότητας του συνδυασμού.
Bit	Δυαδικό ψηφίο
Broadcast	Ευρεία αναμετάδοση

Byte	Μία οκτάδα δυαδικών ψηφίων
Care-of	Η προσωρινή διεύθυνση που αποκτά ένας κινητός κόμβος όταν βρίσκεται σε ένα ξένο υποδίκτυο.
Confidentiality	Εμπιστευτικότητα
Configuration	Ρύθμιση/διαμόρφωση
Data	Δεδομένα
Database	Βάση δεδομένων
Default	Προεπιλεγμένος
Destination	Προορισμός
Domain	Αυτόνομο σύστημα (σύνολο από κόμβους) σε ένα δίκτυο, που συνήθως διαχειρίζεται από μία οντότητα.
Dual stack	Διπλής στοίβας (ένας σταθμός που υποστηρίζει IPv4 και IPv6)
Encapsulation	Ενθυλάκωση
Encryption	Απόκρυψη/κωδικοποίηση
End-to-end	Από-άκρο-σε-άκρο μιας σύνδεσης
Error	Σφάλμα/λάθος
Firewall	Ρυθμιστής της δικτυακής κίνησης μεταξύ δικτύων
Class	Κλάση/κατηγορία
Client	Πελάτης - το μηχάνημα/πρόγραμμα/διεργασία που ζητάει μια υπηρεσία από έναν εξυπηρετητή (server).
Flag	Σημαία - ένα bit που ανάλογα με την τιμή 0 ή 1 που παίρνει σηματοδοτεί κάτι.Περιέχονται πληροφορίες που αφορουν το πακέτο και τις λαμβάνει ο παραλήπτης.
Flow	Ροή
Push	Προώθηση πακέτων
Fragment	Κομμάτι από διασπασμένο πακέτο
Gateway	Πύλη
Global	Οικουμενικός
Hardware	Υλικό ενός υπολογιστικού συστήματος ορίζεται το σύνολο των φυσικών εξαρτημάτων ενός υπολογιστή, όπως π.χ. ηλεκτρικά και ηλεκτρονικά στοιχεία, μικροτσίπ κλπ. Το υλικό καθοδηγείται κατά τη λειτουργία του από το λογισμικό.
Hash function	Μαθηματική διαδικασία που δημιουργεί μία σύνοψη συγκεκριμένου μεγέθους ενός μηνύματος, η οποία δεν μπορεί εύκολα να χρησιμοποιηθεί για την ανάκτηση του αρχικού μηνύματος χωρίς το Βοηθητικό αλγόριθμο hashing.
Header	Επικεφαλίδα

Home	Οικείος
Hop	Βήμα σε ένα δικτυακό μονοπάτι
Host	Σταθμός
Identifier	Αναγνωριστικό
Index	Δείκτης που καθορίζει την τρέχουσα θέση επεξεργασίας για ένα σύνολο.
Integrity	Ακεραιότητα
Interface	Διεπαφή - Ένα δικτυακό interface είναι το σημείο επαφής ενός κόμβου με ένα δικτυακό σύνδεσμο (link).
Internet	Διαδίκτυο
Jumbo	Πολύ μεγάλο
Label	Ετικέτα
Laptop	Φορητός υπολογιστής
Layer	Επίπεδο
Length	Μήκος
Link	Δικτυακός σύνδεσμος
Local	Τοπικός
Management	Διαχείριση
Mobile	Κινητός
Native IPv6	Γνήσιος - υποστήριξη του IPv6 πρωτοκόλλου
Network	Δίκτυο
Offset	Αριθμός που δείχνει τη μετατόπιση σε σχέση με κάποιο σημείο αναφοράς.
Option	Επιλογή
	Επιβάρυνση
Packet	Πακέτο - ένα σύνολο από bits που μεταδίδονται μαζί στο δίκτυο.
Padding	Συμπλήρωμα που χρησιμοποιείται στα πεδία της επικεφαλίδας ενός πακέτου ώστε αυτά να στοιχίζονται κατάλληλα (συνήθως σε μία δύναμη του 2).
Path	Δικτυακό μονοπάτι
Payload	Ωφέλιμο φορτίο
Port	θύρα
Prefix	Πρόθεμα
	Διεργασία
Protocol	Πρωτόκολλο
Provider	Παροχέας
Proxy	Αντιπρόσωπος - μία οντότητα που εκτελεί μια διαδικασία εκ μέρους μιας άλλης και της μεταδίδει το αποτέλεσμα.
Quality of Service	Ποιότητα Υπηρεσίας

Relay	Αναμεταδότης
Reply	Απάντηση
Request	Αίτημα
Reserved	Δεσμευμένο
Robustness	Ευρωστία
Router	Δρομολογητής
Security	Ασφάλεια
Segment	Τεμάχιο
Server	Εξυπηρετητής - το μηχάνημα/πρόγραμμα/διεργασία που παρέχει μια υπηρεσία σε έναν πελάτη (client).
Session	Σύνοδος
Single point of failure	Ένα σημείο ενός συστήματος το οποίο αν αποτύχει παρασύρει ολόκληρο το σύστημα («αχίλλειος πτέρνα»).
Site	Χρησιμοποιείται για να προσδιορίσει έναν οργανισμό ή μία τοποθεσία στα πλαίσια ενός ευρύτερου δικτύου, αν και ο ακριβής ορισμός αλλάζει ανάλογα με τον τρόπο χρήσης του όρου.
Software	Λογισμικό που εκτελείται σε ένα υπολογιστικό σύστημα.
Source	Αφετηρία/πηγή
Stack	Στοίβα
Standard	Πρότυπο
Stateful	Μηχανισμός/πρωτόκολλο που λειτουργεί κρατώντας μνήμη προηγούμενης κατάστασης.
Stateless	Μηχανισμός/πρωτόκολλο που λειτουργεί μη
	κρατώντας μνήμη προηγούμενης κατάστασης, οπότε κάθε ενέργεια είναι ανεξάρτητη.
Streaming	Μετάδοση πακέτων πάνω από δίκτυο τα οποία Επεξεργάζοται καθώς καταφθάνουν
Live Streaming	την πραγματικού χρόνου μετάδοση πολυμέσων.
Subnet	Υποδίκτυο
Traffic	Δικτυακή κίνηση
Translation	Μετάφραση
Tunnel	Σήραγγα
Update	Ενημέρωση/ανανέωση
Valid	Έγκυρος
Version	Έκδοση