Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Ηλεκτρολογίας
ΑΤΕΙ Κρήτης

Quality of Service Στο Internet Protocol version 6 (QoS Στο IPv6)

Μασαλής Ιωάννης

Ηράκλειο
2012

QoS ΣΤΟ IPv6

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος

Σκοπός του φοιτητή στη παρούσα εργασία, είναι να παραθέσει και να αναλύσει την λειτουργία των ασυρμάτων δικτύων στις μέρες μας σε συνδυασμό με την εφαρμογή του IPv6 και το πώς μπορεί να εφαρμοσθεί η ποιότητα υπηρεσιών στην εφαρμογή της συγκεκριμένης τεχνολογίας. Αντίστοιχα λοιπόν, στο πρώτο κεφάλαιο αναλύονται οι συνθήκες και λειτουργίες των ασυρμάτων δικτύων στις μέρες μας, ποια τα πλεονεκτήματα τα οποία προσφέρουν αλλά και ποιες οι σχετικές τεχνολογίες που τα πλαισιώνουν.

Στο δεύτερο κεφάλαιο, αναλύονται τα χαρακτηριστικά του ασυρμάτου δικτύου IPv6, ποια τα πλεονεκτήματα που προσφέρει η συγκεκριμένη τεχνολογία αλλά και ποια η σχετική ανάπτυξη στην Ελλάδα.

Στο τρίτο κεφάλαιο αναλύονται οι συνθήκες εφαρμογής QoS στο IPv6, μέσω των χαρακτηριστικών που θα πρέπει να φέρουν οι συγκεκριμένες τεχνολογίες, ποιοι οι τρόποι επίτευξης του QoS στην αναφερόμενη τεχνολογία, ποιες οι σχετικές δυσκολίες εφαρμογής καθώς και ποιες οι προτάσεις που θα μπορούσαν να γίνουν με σκοπό την καλύτερη λειτουργία του IPv6 μέσω της εφαρμογής του QoS.

Εισαγωγή

Μιλώντας κάποιος για «ασύρματο δίκτυο», εννοεί τα συστήματα εκείνα τα οποία χρησιμοποιούν οι άνθρωποι στις καθημερινές τους ενέργειες είτε στον ιδιωτικό τους χώρο είτε στις επιχειρήσεις στις οποίες εργάζονται με σκοπό να ανακτήσουν τις πληροφορίες που χρειάζονται από το διαδίκτυο και τις οποίες μπορούν να ανακτήσουν στους προσωπικούς τους ηλεκτρονικούς υπολογιστές αλλά και στα τελευταίας τεχνολογίας κινητά τηλέφωνα[1]. Είναι γεγονός πως ένα ασύρματο δίκτυο σχετίζεται άμεσα με τις επιχειρήσεις και εταιρείες εκείνες, οι οποίες αποσκοπούν στην πλήρη εκμετάλλευση των πηγών των πληροφοριών. Οι πηγές αυτές μπορούν να κατηγοριοποιηθούν σε πέντε βασικές κατηγορίες ως ακολούθως[2] :

- *Φορείς πληροφοριών*
- *Μεταφορείς πληροφοριών*
- *Αισθητήρες πληροφοριών*
- *Καταγραφείς πληροφοριών*
- *Διεκπεραιωτές πληροφοριών*

Οι κατηγορίες αυτές που αναφέρονται παραπάνω δεν σημαίνει ότι ακολουθούν πάντα την συγκεκριμένη αυτή σειρά, καθώς κάθε μια από αυτές μπορεί να επιτελεί περισσότερες από μια λειτουργία. Επιχειρώντας τη διεξαγωγή μιας ανάλυσης στις πέντε αυτές κατηγορίες πηγών, θα μπορούσαν να αναφερθούν τα εξής. Οι φορείς πληροφοριών είναι τα μέσα εκείνα τα οποία κατέχουν τις όποιες πληροφορίες. Κάθε αντικείμενο μπορεί να χαρακτηριστεί ως κάτοχος πληροφοριών. Στα αντικείμενα αυτά μπορούν να συμπεριλαμβάνονται η μνήμη των ανθρώπων, κάθε γραπτό μέσο, οι δίσκοι και οι χώροι αποθήκευσης των υπολογιστών, η μνήμη που διαθέτουν καθώς και όποια πληροφορία βρίσκεται αποθηκευμένη σε αυτούς.

---

1 McCarthy, L., 1997, "*Intranet Security*", Prentice Hall

2 Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

Οι μεταφορείς πληροφοριών χαρακτηρίζονται ως συστήματα και αντικείμενα επικοινωνιών, τα οποία έχουν την ικανότητα να διακινούν ή να διαβιβάζουν πληροφορίες από ένα συγκεκριμένο μέρος σε κάποιο άλλο. Στα συστήματα αυτά συμπεριλαμβάνονται τα άτομα τα οποία μεταφέρουν τις πληροφορίες, τα διάφορα οχήματα και γενικά τα μέσα μεταφοράς καθώς και τα διάφορα μέσα μαζικής επικοινωνίας[3].

Σχετικά με τους αισθητήρες πληροφοριών, θα μπορούσε να αναφερθεί πως αυτές είναι συσκευές οι οποίες συλλέγουν πληροφορίες από άλλα αντικείμενα, αλλά και από το περιβάλλον στο οποίο βρίσκονται. Στην κατηγορία αυτή ανήκουν τα scanners, τα ραντάρ και οι φωτογραφικές μηχανές και τα οποία μπορούν να συνδεθούν με τα διάφορα ασύρματα δίκτυα. Τέλος, ως καταγραφείς των πληροφοριών χαρακτηρίζονται οι συσκευές εκείνες οι οποίες τοποθετούν κάποιες πληροφορίες στους φορείς. Σε αυτές συγκαταλέγονται οι ανθρώπινες ενέργειες, οι οδηγοί cd καθώς και οι εκτυπωτές. Οι διεκπεραιωτές πληροφοριών είναι τα αντικείμενα εκείνα που χειρίζονται τις πληροφορίες και εσωκλείουν το υλικό μέρος των υπολογιστών, τους μικροεπεξεργαστές αλλά και τα διάφορα προγράμματα που λειτουργούν με ασύρματα δίκτυα.

Όλες αυτές οι πηγές που αναφέρθηκαν παραπάνω, έχουν την ικανότητα να συνεργάζονται μεταξύ τους έτσι ώστε οι πληροφορίες να μεταβιβάζονται από την μια κατηγορία στην άλλη με ασύρματο τρόπο. Οι αισθητήρες είναι εκείνοι οι οποίοι συλλέγουν τις πληροφορίες από το ευρύτερο περιβάλλον, αυτές κατόπιν εισέρχονται στον υπολογιστή, εκτυπώνονται και μεταβιβάζονται από τα διάφορα τηλεπικοινωνιακά μέσα. Η αλληλοσύνδεση αυτή που υπάρχει, μπορεί να τροφοδοτεί κατάλληλα με πληροφορίες τις επιχειρήσεις που χρησιμοποιούν την ασύρματη τεχνολογία[4].

---

[3] Timpton, H., F., Ruthberg, Z., G., 2003, "*Handbook of Information Security Management*", Acerbic

[4] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

Στην διαδικασία αυτή, εμπλέκεται επίσης και ο όρος «πληροφοριακή υποδομή» ο οποίος αναφέρεται σε εκείνες τις πηγές πληροφοριών όπου και εσωκλείονται και τα ασύρματα συστήματα επικοινωνιών. Τα συστήματα αυτά μπορούν να υποστηρίζουν κατάλληλα μια βιομηχανία ή και ένα διεθνές οργανισμό. Χαρακτηριστικό παράδειγμα αποτελεί η πληροφοριακή υποδομή που αποκτούν οργανισμοί και επιχειρήσεις, καθώς και κρατικοί φορείς. Ο χώρος της πληροφορικής αναφέρεται στο σύνολο του στις διάφορες πηγές πληροφοριών και οι οποίες μπορούν να είναι προσιτές σε μια ευρύτερη οντότητα. Η οντότητα αυτή μπορεί να περιλαμβάνει τα συστήματα των υπολογιστών, τα έγγραφα, τα συστήματα επικοινωνιών αλλά και τις κωδικοποιημένες πληροφορίες. Ως παράδειγμα στην περίπτωση αυτή, μπορεί να αναφερθεί ο ευρύτερος χώρος του ίντερνετ ο οποίος περιλαμβάνει ένα μεγάλο σύνολο δικτύων αλλά και ηλεκτρονικών υπολογιστών[5].

Σημαντική τεχνολογική όμως εφαρμογή και η οποία συνδέεται με την ανάπτυξη τεχνολογίας του διαδικτύου και των ασυρμάτων δικτύων σε αυτό, είναι το IPv6 και του οποίου τα βασικά χαρακτηριστικά αναλύονται στη παρούσα πτυχιακή και σε συνδυασμό με την εφαρμογή QoS, κάτι που θα κάνει το συγκεκριμένο ασύρματο δίκτυο να λειτουργεί κάτω από καλύτερες συνθήκες και τεχνολογίες ανάπτυξης.

[5] Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

1. Κεφάλαιο 1^{ο} : Λειτουργία και Χαρακτηριστικά των Ασυρμάτων Δικτύων

1.1 Η Έννοια του Ασύρματου Δικτύου

1.1.1 Τι Είναι τα Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα ή διαφορετικά Wi-Fi Networks - εμφανίζονται πλέον ολοένα και περισσότερο στη ζωή μας. Θεωρούνται η εξέλιξη των ενσύρματων δικτύων και αποτελούν ίσως κατά το κοινώς λεγόμενο, το μέλλον στην επικοινωνία μεταξύ των συσκευών. Μιλώντας κανείς για ασύρματα δίκτυα αναφέρεται στη σύνδεση μεταξύ 2-ή περισσοτέρων ηλεκτρονικών υπολογιστών με σκοπό την ανταλλαγή δεδομένων χωρίς όμως να παρεμβάλλονται καλώδια ή κάποιο είδος οργανικής σύνδεσης ανάμεσά τους[6]. Ο συγκεκριμένος όρος δεν είναι ιδιαίτερα σαφής σε έναν χρήστη ο οποίος δεν είναι επαρκώς εξοικειωμένος με τις νέες τεχνολογίες για το λόγο ότι αποδίδει μόνο ένα μικρό μέρος της ευρείας χρήσης που μπορούν αυτά τα συστήματα να έχουν. Για παράδειγμα μπορεί να αναφερθεί πως τα στοιχεία ενός ηλεκτρονικού υπολογιστή περιέχονται πια σε κινητά τηλέφωνα, φορητές συσκευές ήχου και εικόνας, υπολογιστές παλάμης, εκτυπωτές και γενικά συσκευές γραφείου, κάτι που σημαίνει πως όλα αυτά έχουν πλέον τη δυνατότητα να συνδεθούν σε ένα ασύρματο δίκτυο[7].

Όπως όμως κάθε μέθοδος σύνδεσης συστημάτων, έτσι και τα ασύρματα δίκτυα ακολουθούν πιστά κάποια πρωτόκολλα και πρότυπα μοντέλα τα οποία τις περισσότερες φορές ορίζονται από διεθνείς οργανισμούς όπως το Ινστιτούτο Ηλεκτρολόγων Μηχανικών - IEEE - μη κερδοσκοπικός οργανισμός ο οποίος ασχολείται και με την προτυποποίηση τεχνικών μέσων και τεχνολογιών) το οποίο όρισε τα πρωτόκολλα 802.11a, 802.11b, 208.11g και άλλα ενώ ταυτόχρονα ανέπτυξε και το γνωστό Bluetooth - πρωτόκολλο

6 Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

7 Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

802.15 και το οποίο ανήκει στην κατηγορία των PAN ή γνωστό ως Personal Area Networks[8]. Για την επικοινωνία αυτή χρησιμοποιούνται κάποιες υψηλές συχνότητες της τάξης των 2.4 Gigahertz ή ελεύθερη ζώνη.
Οι λόγοι για τους οποίους τα ασύρματα δίκτυα πιθανώς διαδραματίσουν κυρίαρχο ρόλο στη σύνδεση μεταξύ υπολογιστών στο μέλλον είναι πολλοί και αναφέρονται ως ακολούθως[9] :

- *Παρέχουν κάποιες πραγματικά μεγάλες ταχύτητες μεταφοράς δεδομένων από κάποιες εκατοντάδες Kbps (kilo bits per second), έως και πολλές δεκάδες Mbps, αναφορικά στα 54 Mbps για το 802.11a και g, με τη διαφορά όμως ότι το a λειτουργεί στα 5 GHz ενώ το g στα 2.4 GHz και 11Mbps για το 802.11b το μέγιστο, γύρω στα 5 στην πράξη.*
- *Η υλοποίηση τους στις μέρες μας έχει πολύ χαμηλό κόστος, υπολογίζεται περίπου στα 150 ευρώ και είναι προσιτό στον καθένα που επιθυμεί να εγκαταστήσει ένα τέτοιο δίκτυο, ενώ η τεχνογνωσία για αυτό παρέχεται εν αφθονία στο διαδίκτυο*
- *Η εμβέλεια τους είναι επαρκής και κυμαίνεται ανάλογα με τη χρήση που απαιτεί ο κάθε χρήστης. Έτσι για σύνδεση μεταξύ οικιακών συσκευών χρησιμοποιείται κυρίως το Bluetooth που έχει εμβέλεια έως τα 10 μέτρα και μπορεί να φτάσει τα 100 μέτρα αλλά με συσκευές υψηλότερης ενέργειας. Για τη δημιουργία ενός τοπικού, οικιακού δικτύου το οποίο χρησιμοποιείται συνήθως για ανταλλαγή ψηφιακών αρχείων ή για παιχνίδια πολλαπλών παικτών, χρησιμοποιούνται τα 802.11a, 802.11b και 802.11g, με εμβέλεια από 40 μέτρα για κλειστούς χώρους ως 100 μέτρα και πολύ περισσότερο έως και 300 μέτρα για ανοικτούς χώρους.*
- *Για σύνδεση μεταξύ κτιριακών εγκαταστάσεων επιχειρήσεων τα τελευταία χρησιμοποιούνται νέες τεχνολογίες οι οποίες φτάνουν σε εμβέλεια τα 4 χιλιόμετρα. Απαραίτητη όμως προϋπόθεση για τις παραπάνω κατηγορίες έτσι ώστε αυτές να αποδώσουν τα μέγιστα*

---

8 McCarthy, L., 1997, "*Intranet Security*", Prentice Hall

9 Timpton, H., F., Ruthberg, Z., G., 2003, "*Handbook of Information Security Management*", Acerbic

θεωρείται η οπτική επαφή, και αν αυτή δεν είναι δυνατή, η αποφυγή μεσολάβησης μεταλλικών αντικειμένων ή αντικειμένων που περιέχουν νερό.

- *Τα ασύρματα δίκτυα παρέχουν μια μεγάλη διευκόλυνση καθώς σημαίνουν το τέλος με τα πολλά καλώδια που όλους λίγο πολύ τους έχουν κουράσει στην δικτύωση τους στο Ίντερνετ*

1.1.2 Για Ποιο Λόγο η Ασύρματη Δικτύωση Θεωρείται Καλύτερη

Η χρήση του ασύρματου μέσου μετάδοσης διαθέτει μια σειρά από πλεονεκτήματα τα οποία αναφέρονται ως ακολούθως[10] :

- *Κινητικότητα Χρήστη*

Οι χρήστες έχουν την ικανότητα να μετακινούνται εντός της εμβέλειας του ασύρματου δικτύου, δηλαδή σε χώρο στον οποίο θα έχουν επαρκές σήμα, διατηρώντας έτσι την συνδεσιμότητα τους με αυτό. Αυτό έχει ως αποτέλεσμα την μεγαλύτερη παραγωγικότητα και αποτελεσματικότητα στο εργασιακό περιβάλλον και όχι μόνο

- *Ευκολία, Ευελιξία και Απλότητα Εγκατάστασης*

Δεν χρειάζεται κάποιος να εγκαταστήσει καλωδιώσεις μέσα από τοίχους και ταβάνια. Μπορεί να γίνει η δικτύωση σε μέρη όπου η καλωδίωση θα ήταν αδύνατη, ή μη επιθυμητή, όπως η δικτύωση γραφείων τα οποία βρίσκονται σε μεγάλη απόσταση μεταξύ τους. Η εγκατάσταση στις περισσότερες των περιπτώσεων μπορεί να διεξαχθεί εύκολα αν ακολουθηθούν κάποιοι βασικοί κανόνες εγκατάστασης στη κάθε περίπτωση

- *Κλιμάκωση, Δυνατότητα Επέκτασης*

Τα ασύρματα δίκτυα μπορούν να διαρθρωθούν σε ένα πλήθος από τοπολογίες, έτσι ώστε να ταιριάξουν στις απαιτήσεις των διαφόρων

---

[10] Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

εφαρμογών. Οι τοπολογίες αλλάζουν εύκολα αλλά και επεκτείνονται από απλά δίκτυα με μικρό αριθμό χρηστών, ως μεγάλες δομές δικτύων με εκατοντάδες χρήστες και δυνατότητα περιαγωγής, δηλαδή του *roaming*.

- *Κόστος*

Παρά το γεγονός ότι το αρχικό κόστος εγκατάστασης θεωρείται υψηλότερο σε σχέση με τις λύσεις ενσύρματης δικτύωσης, το κόστος για όλη τη διάρκεια ζωής της επένδυσης μπορεί να είναι ιδιαιτέρως μικρότερο, ιδιαίτερα σε δυναμικό περιβάλλον που απαιτεί συχνές αλλαγές, αναδιαρθρώσεις και μετακινήσεις. Επιπλέον το κόστος υλοποίησης - εγκατάστασης και συντήρησης - διαχείρισης του δικτύου είναι επίσης πολύ μικρό. Το σημαντικότερο μέρος του κόστους είναι η αγορά του εξοπλισμού. Επίσης με την εμφάνιση των περισσότερων κατασκευαστών και τον έντονο ανταγωνισμό μεταξύ τους το κόστος έχει μειωθεί αισθητά, ενώ παράλληλα οι συσκευές έχουν αποκτήσει περισσότερα ποιοτικά χαρακτηριστικά. Έτσι, ενώ το 2000 ένα σημείο πρόσβασης - Access Point - είχε κόστος 1000-2000$, τώρα έχει κόστος δέκα φορές μικρότερο κόστος. Μάλιστα τα περιθώρια κέρδους έχουν συμπιεστεί σε πολύ μεγάλο βαθμό για τους κατασκευαστές και προς όφελος βέβαια του κάθε καταναλωτή.

- *Ταχύτητες Μετάδοσης*

Όσο περισσότερο αναπτύσσεται η τεχνολογία γίνεται δυνατή η μετάδοση μεγαλύτερων ρυθμών δεδομένων. Ήδη ο μέγιστος ρυθμός μετάδοσης δεδομένων, από τα 2Mbps που μπορούσαν να επιτευχθούν αρχικά, έφτασε στις μέρες μας σε ταχύτητες πάνω από 100Mbps ενώ ήδη έχουν εξαγγελθεί ακόμα μεγαλύτερες ταχύτητες για το μέλλον.

- *Αξιοπιστία - Ανεξαρτησία*

Ένα ασύρματο δίκτυο το οποίο είναι κατάλληλα διαμορφωμένο μπορεί να διαθέτει μεγάλη αξιοπιστία. Έτσι μπορεί να σχεδιαστεί με απώτερο σκοπό να μπορεί να «εργάζεται» όταν συμβαίνουν διακοπές ρεύματος και να

περιλαμβάνει πολλές εναλλακτικές διαδρομές έως οι υπηρεσίες φθάσουν στον χρήστη.

- *Εμβέλεια*

Η εμβέλεια ενός ασύρματου δικτύου σε ένα περιβάλλον γραφείου μπορεί να είναι μερικές δεκάδες μέτρα. Τα ραδιοκύματα σε κάθε εσωτερικό χώρο έχουν να διαπεράσουν τοίχους και οροφές οπότε υποκύπτουν σε μια σημαντική απόσβεση. Σε ανοικτό χώρο όπου υπάρχει οπτική επαφή ανάμεσα στις ασύρματες συσκευές, οι αποστάσεις οι οποίες μπορούν να καλυφθούν είναι μεγαλύτερες.

- *Συμβατότητα με το Υπάρχον Δίκτυο*

Τα περισσότερα ασύρματα δίκτυα διαθέτουν ένα προτυποποιημένο τρόπο σύνδεσης με τα υπάρχοντα ενσύρματα δίκτυα. Με το τρόπο αυτό, η προσθήκη ασύρματης δικτύωσης σε υπάρχουσες δομές δικτύων μπορεί να επιτευχθεί με τον ευκολότερο τρόπο. Πολλές φορές δε, αποτελούν και επέκταση ενός ενσύρματου δικτύου.

1.1.3 Σε Ποιες Περιπτώσεις δεν Χρειάζεται Ασύρματη Δικτύωση

Η χρήση της ασύρματης τεχνολογίας σε καμία περίπτωση δεν παραγκωνίζει τις λύσεις της ενσύρματης δικτύωσης[11]. Οι δύο «οικογένειες» τεχνολογιών θεωρούνται συμπληρωματικές και όχι ανταγωνιστικές. Δεν θα πρέπει λοιπόν να γίνεται χρήση της ασύρματης τεχνολογίας στις ακόλουθες περιπτώσεις[12] :

---

11 Adams, J., 1998, "*The next world war*", Simon and Schuster

12 Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

- Όταν ο χρήστης διαθέτει κατευθείαν εύκολη πρόσβαση στο ενσύρματο δίκτυο, για παράδειγμα αναφέρεται η σύνδεση ενός δύο υπολογιστών που βρίσκονται δίπλα δίπλα σε ένα γραφείο με ένα απλό *ethernet* καλώδιο

- Στις περιπτώσεις όπου ο χρήστης και η εφαρμογή απαιτεί αρκετά μεγάλο ρυθμό μετάδοσης, όπου δεν μπορεί να καλυφθεί από το ασύρματο δίκτυο. Έτσι για παράδειγμα εάν κάποιος επιθυμεί μια διασύνδεση με ρυθμό 1Gbps, μπορεί να την υλοποιήσει με πολύ χαμηλό κόστος με συσκευές οι οποίες υποστηρίζουν *Gigabit Ethernet* και την κατάλληλη καλωδίωση. Η ασύρματη τεχνολογία δεν προβλέπεται να φτάσει ποτέ αυτές τις ταχύτητες. Επιπρόσθετα, ήδη έχουν κυκλοφορήσει λύσεις ενσύρματης δικτύωσης οι οποίες φτάνουν στα 10Gbps αν και δεν είναι κοινή ακόμα η χρήση τους[13].

- Σε δίκτυα τα οποία απαιτούν μεγάλο βαθμό ασφαλείας, οι ενσύρματες λύσεις είναι σαφώς καλύτερες. Σε ένα καλώδιο το οποίο θεωρείται ήδη προστατευμένο κάτω από ψευδοπατώματα, δεν είναι δυνατή η φυσική πρόσβαση στο καλώδιο προκειμένου να γίνει υποκλοπή. Αντίθετα, στην περίπτωση κάποιας ασύρματης υλοποίησης, επειδή δεν είναι δυνατό να περιορίσει κανείς τα ραδιοκύματα, είναι εύκολο να γίνει ανίχνευση της μεταδιδόμενης πληροφορίας. Σε περίπτωση δε όπου η πληροφορία δεν είναι κωδικοποιημένη μπορεί να διεξαχθεί ανάκτηση της. Για μπορέσουν όμως να φτάσουν σε παρόμοιο βαθμό ασφαλείας τα ασύρματα δίκτυα, θα πρέπει να εφαρμοστούν σε αυτά περίπλοκες τεχνικές αυθεντικοποίησης και κωδικοποίησης και μάλιστα σε ένα επίπεδο εφαρμογής. Άλλωστε αυτός είναι και ένας από τους λόγους που δεν χρησιμοποιούνται σε κρίσιμες στρατιωτικές εφαρμογές οι συμβατικές ασύρματες τεχνολογίες, για παράδειγμα επικοινωνία συσκευών, εφαρμογών, προσωπικού, σε ένα πολεμικό πλοίο ή εντός μιας στρατιωτικής βάσης.

[13] Adams, J., 1998, "*The next world war*", Simon and Schuster

- Σε περιοχές οι οποίες έχουν μεγάλο ηλεκτρομαγνητικό θόρυβο, γεγονός που έχει ως αποτέλεσμα κάποιες προβληματικές και μη αξιόπιστες συνδέσεις.

1.2 Ο Ρόλος και η Σημασία του Ασύρματου Δικτύου στην Επικοινωνία - Κατηγορίες Ασυρμάτων Δικτύων

1.2.1 Κατηγορία Ασύρματα Δίκτυα PAN

Το προσωπικό δίκτυο (PAN) Bluetooth θεωρείται μια τεχνολογία η οποία επιτρέπει στα άτομα να δημιουργήσουν ένα δίκτυο Ethernet με ασύρματες συνδέσεις μεταξύ των φορητών υπολογιστών, κινητών τηλεφώνων και συσκευές χειρός[14]. Μπορεί επίσης κανείς να συνδέσει τους τύπους συσκευών με δυνατότητα Bluetooth, οι οποίες είναι συμβατές με προσωπικά δίκτυα όπως η συσκευή χρήστη προσωπικού δικτύου (PANU), συσκευή δικτύου ad hoc ομάδας (GN) ή συσκευή σημείου πρόσβασης σε δίκτυο (NAP)[15]

Οι συσκευές PANU με δυνατότητα Bluetooth δημιουργούν ένα δίκτυο ad-hoc το οποίο συμπεριλαμβάνει τον υπολογιστή του κάθε ατόμου και τη συσκευή. Οι συσκευές GN με δυνατότητα Bluetooth δημιουργούν ένα δίκτυο ad-hoc το οποίο συμπεριλαμβάνει τον υπολογιστή του κάθε ατόμου, τη συσκευή GN και άλλες συσκευές PANU οι οποίες είναι όλες μαζί συνδεδεμένες με την ίδια συσκευή GN. Τέλος οι συσκευές NAP με δυνατότητα Bluetooth, επιτρέπει στα άτομα να συνδέσουν τον υπολογιστή τους σε ένα μεγαλύτερο δίκτυο, όπως σε ένα οικιακό δίκτυο, σε ένα εταιρικό δίκτυο ή στο Ίντερνετ απευθείας.

---

14 McCarthy, L., 1997, "*Intranet Security*", Prentice Hall

15 Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

Τι κάνει όμως το Bluetooth; Θα πρέπει να αναφερθεί πως το Bluetooth αναφέρεται σε μια ανοικτή προδιαγραφή για μια τεχνολογία η οποία έχει σκοπό να επιτρέψει τις περιορισμένου φάσματος ασύρματες μεταδόσεις φωνής και στοιχείων σε οποιοδήποτε μέρος στον κόσμο. Αυτή η συνάμα απλή και απλή περιγραφή της Bluetooth τεχνολογίας περιλαμβάνει κάποια διάφορα σημεία που είναι βασικά στην κατανόησή της. Το πρώτο σημείο είναι η «ανοικτή» προδιαγραφή της η οποία εντοπίζεται στην ειδική ομάδα ενδιαφέροντος Bluetooth – SIG και η οποία έχει παραγάγει μια προδιαγραφή για την ασύρματη επικοινωνία Bluetooth και η οποία είναι δημόσια διαθέσιμη με ελεύθερο δικαίωμα πρόσβασης[16].

Το δεύτερο σημείο είναι το περιορισμένου φάσματος ραδιόφωνο στο οποίο υπάρχουν πολλές περιπτώσεις περιορισμένου φάσματος ψηφιακής επικοινωνίας μεταξύ των συσκευών υπολογισμού και επικοινωνιών. Στις μέρες μας ένα μεγάλο μέρος αυτής της επικοινωνίας πραγματοποιείται χωρίς τη χρήση καλωδίων. Αυτά τα καλώδια συνδέονται με ένα πλήθος συσκευών χρησιμοποιώντας και με μια ευρεία ποικιλία των συνδέσμων, μεγεθών και αριθμού δικτύων τα οποία προσφέρουν συγκεκριμένα πλεονεκτήματα στους χρήστες.

Με την τεχνολογία Bluetooth, αυτές οι συσκευές μπορούν να επικοινωνήσουν χωρίς καλώδια και πέρα από ένα ενιαίο κτιριακό συγκρότημα, χρησιμοποιώντας ουσιαστικά τα ραδιο κύματα για να μεταδώσουν και να λάβουν τα απαιτούμενα στοιχεία. Η ασύρματη τεχνολογία Bluetooth έχει σχεδιαστεί συγκεκριμένα για τις περιορισμένου φάσματος έως και 10 μέτρα αντίστοιχες επικοινωνίες με αποτέλεσμα αυτό το σχέδιο να χρησιμοποιεί μια πολύ μικρή κατανάλωση ισχύος, η οποία καθιστά την τεχνολογία αυτή ιδιατέρως αποτελεσματική και άμεση[17].

---

16 Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

17 Timpton, H., F., Ruthberg, Z., G., 2003, "*Handbook of Information Security Management*", Acerbic

1.2.2 Κατηγορία Ασύρματα Δίκτυα LAN

Ένα ασύρματο τοπικό δίκτυο υπό μορφή LAN επιτρέπει ουσιαστικά τη σύνδεση των υπολογιστών χωρίς καλώδια. Αν κάποιος για παράδειγμα σε μια επιχείρηση χρειάζεται ένα έγγραφο και βρίσκεται στην αίθουσα συσκέψεων, τότε μπορεί απλά με την ασύρματη σύνδεση LAN να το ανακτήσει από έναν άλλο υπολογιστή. Με ένα ασύρματο δίκτυο LAN κάτι τέτοιο καθιστάται ιδιαιτέρως εύκολο, καθώς χρησιμοποιεί ραδιοκύματα για να επιτρέπει τη σύνδεση και την επικοινωνία κινητών συσκευών εντός μιας συγκεκριμένης εμβέλειας[18]. Τα πλεονεκτήματα της ασύρματης δικτύωσης LAN είναι βραχυπρόθεσμα και μακροπρόθεσμα και αναφέρονται ως ακολούθως :

- *Ευκολία χρήσης*. Στις μέρες μας όλοι οι φορητοί υπολογιστές και πολλά κινητά τηλέφωνα είναι εξοπλισμένα με τεχνολογία Wi-Fi η οποία απαιτείται για απευθείας σύνδεση σε ένα ασύρματο δίκτυο LAN. Οι εργαζόμενοι μπορούν να συνδέονται με ασφάλεια στους πόρους του δικτύου της κάθε εταιρίας από οπουδήποτε εντός της εμβέλειας κάλυψης του δικτύου. Η περιοχή κάλυψης είναι κατά κανόνα οι εγκαταστάσεις της επιχείρησής όπου εργάζονται, ωστόσο μπορεί να επεκτείνεται και σε περισσότερα κτίρια

- *Φορητότητα*. Οι εργαζόμενοι μπορούν να παραμένουν συνδεδεμένοι στο δίκτυο, ακόμα και όταν δεν βρίσκονται στο γραφείο τους εντός της επιχείρησης. Οι συμμετέχοντες σε συσκέψεις μπορούν να έχουν πρόσβαση σε έγγραφα και εφαρμογές ταυτόχρονα. Οι πωλητές μπορούν να εντοπίζουν στο δίκτυο σημαντικές λεπτομέρειες από οποιαδήποτε τοποθεσία και αν βρίσκονται.

- *Παραγωγικότητα*. Η πρόσβαση στις πληροφορίες και στις βασικές εφαρμογές της εταιρείας μπορεί να υποστηρίζει το προσωπικό κατά τη διεκπεραίωση των εργασιών και να ενθαρρύνει τη συνεργασία. Οι

[18] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

επισκέπτες όπως πελάτες, συνεργάτες ή προμηθευτές μπορούν επίσης να έχουν πρόσβαση υψηλής ασφαλείας στο Ίντερνετ και στα επιχειρηματικά δεδομένα τους.

- *Εύκολη ρύθμιση*. Εφόσον δεν απαιτείται η τοποθέτηση καλωδίων σε ένα χώρο, τότε η εγκατάσταση μπορεί να ολοκληρωθεί γρήγορα και οικονομικά. Τα ασύρματα δίκτυα LAN διευκολύνουν επίσης τη συνδεσιμότητα δικτύου σε κάποιους δυσπρόσιτους χώρους, όπως οι αποθήκες ή οι εγκαταστάσεις εργοστασιακής παραγωγής.

- *Δυνατότητα κλιμάκωσης.* Καθώς οι διάφορες επιχειρηματικές δραστηριότητές των επιχειρήσεων αναπτύσσονται, ενδεχομένως να απαιτείται άμεση επέκταση του δικτύου τους. Τα ασύρματα δίκτυα μπορούν κατά κανόνα να επεκταθούν με τον υπάρχοντα εξοπλισμό, ενώ ένα ενσύρματο δίκτυο ενδέχεται να απαιτεί κάποια επιπλέον καλωδίωση.

- *Ασφάλεια*. Ο έλεγχος και η διαχείριση της πρόσβασης στο ασύρματο δίκτυό των επιχειρήσεων θεωρείται μέγιστης σημασίας για την επιτυχία τους. Οι εξελιγμένες δυνατότητες της τεχνολογίας Wi-Fi προσφέρουν μια ισχυρή προστασία, ώστε τα δεδομένα των επιχειρήσεων να είναι εύκολα προσβάσιμα μόνο από τους χρήστες στους οποίους επιτρέπεται η πρόσβαση.

- *Κόστος*. Μπορεί να αποδειχθεί οικονομικότερη η λειτουργία ενός ασύρματου δικτύου LAN, το οποίο εξαλείφει ή μειώνει το κόστος καλωδίωσης σε περιπτώσεις μετακόμισης, αναδιάταξης ή επέκτασης γραφείων της κάθε επιχείρησης

1.2.3 Κατηγορία Ασύρματα Δίκτυα WAN & MAN

Ένα ασύρματο WAN ή διαφορετικά Wide Area Network θεωρείται ένα δίκτυο ασύρματων υπηρεσιών το οποίο λειτουργεί πέρα από ένα κτίριο και παρέχεται από κάποιον φορέα, όπως το φορέα κινητής τηλεφωνίας που

χρησιμοποιείτε[19]. Σε ένα ασύρματο WAN, μπορεί κανείς να μεταβεί ασύρματα στο δίκτυο φωνητικών υπηρεσιών ή δεδομένων αντί να συνδέσει το *notebook* σε μια τηλεφωνική υποδοχή και να καλέσει τον αριθμό σύνδεσης στο Ίντερνετ ή να συνδεθεί σε ένα δημόσιο hot-spot. Σε ένα ασύρματο δίκτυο WAN, κάθε φορητή συσκευή επικοινωνεί με το σταθμό βάσης της υπηρεσίας παροχής[20].

Τα ασύρματα δίκτυα WAN θεωρούνται μια από τις πιο συνηθισμένες μορφές ενός ασύρματου δικτύου ευρείας περιοχής. Πολλοί άνθρωποι σε όλο τον κόσμο χρησιμοποιούν τα κινητά τους τηλέφωνα για να συνδεθούν σε κάποιο *Δημόσιο Τηλεφωνικό Δίκτυο* ή διαφορετικά Public Switched Telephone Network - PSTN*.* Οι διάφορες εταιρείες παροχής υπηρεσιών κινητής τηλεφωνίας έχουν επενδύσει αστρονομικά ποσά για τη δημιουργία μιας επικοινωνιακής δομής, η οποία θα μπορεί να συνδέσει τις κεραίες τους μέσω κάποιων κέντρων μεταγωγής κινητών τηλεπικοινωνιών σε κάποιο κεντρικό κόμβο και από εκεί στο αντίστοιχο δημόσιο τηλεφωνικό δίκτυο. Έχουν επίσης αναπτυχθεί πολλά πρότυπα για τις κινητές τηλεπικοινωνίες στην Ευρώπη και στις Ηνωμένες Πολιτείες, καθώς άλλα είναι προσανατολισμένα στην αναλογική και άλλα στην ψηφιακή τεχνολογία. Τέλος οι υπηρεσίες παροχής εγκαθιστούν δίκτυα σταθμών βάσης, παρόμοιους με τους σταθμούς κινητής τηλεφωνίας σε μεγάλες γεωγραφικές περιοχές, παρέχοντας ουσιαστικά κάλυψη σε μεγάλες περιοχές, ακόμα και χώρες[21].

Σχετικά με τα ασύρματα δίκτυα MAN, θα ήταν χρήσιμο να αναφερθεί πως η ανάπτυξη των Μητροπολιτικών Δικτύων στην Περιφέρεια μιας χώρας θα μπορούσε να παρομοιαστεί με τη διάνοιξη μίας «*Εθνικής Οδού*» η οποία φέρνει την ευρυζωνικότητα σε κάθε σημείο του χάρτη. Ως Μητροπολιτικά Δίκτυα (MAN) ορίζονται τα ευρυζωνικά δίκτυα, τα οποία αναπτύσσονται

---

19 Adams, J., 1998, "*The next world war*", Simon and Schuster

20 Timpton, H., F., Ruthberg, Z., G., 2003, "*Handbook of Information Security Management*", Acerbic

21 Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

κυρίως σε πόλεις και στα οποία συνδέονται χρήστες όπως δημόσιοι φορείς, επιχειρήσεις, πολίτες, κ.λπ. με τη χρήση Η/Υ ή άλλων ηλεκτρονικών μέσων σε κάποιες πολύ υψηλές ταχύτητες[22]. Τα ασύρματα αυτά δίκτυα χρησιμοποιούν συνήθως οπτικές ίνες και ασύρματες τεχνολογίες και το μέγεθός τους είναι μεγαλύτερο από τα τοπικά δίκτυα δηλαδή τα Local Area Networks - LAN και μικρότερο από τα δίκτυα ευρείας περιοχής όπως Wide Area Networks - WAN. Με δεδομένο ότι η έννοια των Μητροπολιτικών Δικτύων θεωρείται στενά συνυφασμένη με την ευρυζωνικότητα, θα μπορούσε κανείς να λάβει υπ'όψιν του αρχικά τα πλεονεκτήματα που προσφέρονται από αυτή και ακολούθως να επεκταθεί στα ασύρματα δίκτυα MAN[23].

1.3 Τομείς Λειτουργίας Ασυρμάτων Προτύπων Δικτύων

Η ασύρματη δικτύωση 802.11 και η οποία ονομάζεται επίσης και "Wi-Fi", αποτελεί ένα σύνολο πρωτοκόλλων τα οποία χρησιμοποιούνται ευρέως σε μικρά τοπικά δίκτυα[24]. Ένα άλλο πρωτόκολλο είναι εκείνο το οποίο ονομάζεται Bluetooth και όπως ήδη αναλύθηκε στις προηγούμενες ενότητες αυτής της πτυχιακής εργασίας, επιτρέπει στις συσκευές να επικοινωνούν ασύρματα αλλά είναι χρήσιμο μόνο για επικοινωνία πολύ μικρής εμβέλειας και γενικότερα δεν χρησιμοποιείται για οικιακή δικτύωση. Το Bluetooth μπορεί επίσης να είναι χρήσιμο για τη δικτύωση προσωπικών συσκευών μέσα στα όρια μιας μικρής περιοχής. Ένα τέτοιο δίκτυο συχνά καλείται δίκτυο προσωπικής περιοχής ή διαφορετικά γνωστό ως Personal Area Network – PAN.

Στην πραγματικότητα το πρωτόκολο 802.11 περικλείει πολλαπλά διαφορετικά πρωτόκολλα. Τα τελευταία γράμματα δηλαδή τα 802.11a ή

---

22 Σταμάτης, Κ., Ν., 2002, «*Η Αβέβαιη Κοινωνία της Γνώσης*», Εκδόσεις Σαββάλας

23 Timpton, H., F., Ruthberg, Z., G., 2003, "*Handbook of Information Security Management*", Acerbic

24 McCarthy, L., 1997, "*Intranet Security*", Prentice Hall

802.11b υποδεικνύουν τις διάφορες ταχύτητες και ζώνες συχνοτήτων που χρησιμοποιούνται. Οι σημαντικότερες ζώνες συχνοτήτων και ταχύτητες είναι το πρότυπο 802.11g το οποίο επικοινωνεί στα 54 Mbps. Ο εξοπλισμός 100/125 Mbps 802.11g θα εκπέμπει με τη διπλάσια ταχύτητα όταν χρησιμοποιείται με άλλο εξοπλισμό 100/125 Mbps. Επιπρόσθετα, θα "χαμηλώσει" για να επικοινωνήσει με 802.11g στα 54 Mbps ή 802.11b στα 11 ή τα 22 Mbps. Το πρότυπο 802.11b επικοινωνεί στα 11 Mbps. Ο εξοπλισμός 22 Mbps 802.11b θα εκπέμπει με τη διπλάσια ακριβώς ταχύτητα όταν χρησιμοποιείται με άλλο εξοπλισμό 22 Mbps. Επίσης, θα "χαμηλώσει" για να επικοινωνήσει με 802.11b στα 11 Mbps[25].

Θα πρέπει να σημειωθεί πως τα πρότυπα 802.11a και 802.11b δεν είναι άμεσα συμβατά μεταξύ τους, αλλά ίσως στο μέλλον δημιουργηθούν προϊόντα για να "γεφυρωθούν" αποτελεσματικά τα δύο δίκτυα και να επιτρέψουν στις συσκευές αυτές να επικοινωνούν μεταξύ τους. Αυτή τη στιγμή πάντως, όλα τα ασύρματα προϊόντα της εταιρίας *U.S. Robotics* για παράδειγμα χρησιμοποιούν το πρωτόκολλο 802.11b, σε ταχύτητες 11 Mbps ή 22 Mbps ή το πρωτόκολλο 802.11g στα 54 Mbps, στα 100 Mbps ή στα 125 Mbps[26].

Έτσι λοιπόν σήμερα βλέπουμε πολλούς χρήστες οι οποίοι έχουν δημιουργήσει από μόνοι τους, χωρίς πολλές γνώσεις πάνω σε δίκτυα, ένα ασύρματο δίκτυο. Υπάρχουν πολυκατοικίες οι οποίες προχωρούν σε τέτοιες εγκαταστάσεις, πόλεις 150.000 κατοίκων να έχουν 220 χρήστες δικτυωμένους μεταξύ τους όπως το Ηράκλειο Κρήτης για παράδειγμα, το οποίο αποτελεί ένα από τα μεγαλύτερα δίκτυα της Ελλάδος. Εκτός των άλλων βέβαια η Αθήνα η οποία σήμερα αριθμεί πάνω από 4.000 χρήστες συνδεδεμένους αυτοβούλως στο ίδιο δίκτυο και θα πρέπει να σημειωθεί ότι είναι το δίκτυο με τους περισσότερους κόμβους σε όλη την Ευρώπη- και η Θεσσαλονίκη η οποία αριθμεί περίπου στους 800 χρήστες. Όμως δεν σταματάει εκεί η τεχνολογία,

---

25 Pfleeger, C., P., 1997, “*Security in Computing*”, Prentice Hall

26 Adams, J., 1998, “*The next world war*”, Simon and Schuster

αεροδρόμια, καφετέριες και πανεπιστήμια έχουν δημιουργήσει "hot spots", δηλαδή σε κάποιο σημείο της εγκατάστασης υπάρχει συσκευή η οποία επιτρέπει σε μια κάποια εμβέλεια του χώρου, πρόσβαση μέσω ασύρματης τεχνολογίας στο διαδίκτυο μέσω μιας φορητής συσκευής, όπως φορητός υπολογιστής, υπολογιστής παλάμης, κλπ. Η υπηρεσία παρέχεται άλλες φορές με χρέωση και άλλες όχι. Ενδεικτικά αναφέρεται ότι στο Διεθνές Αεροδρόμιο Αθηνών «Ελ. Βενιζέλος» η υπηρεσία έχει χρέωση 10 ευρώ για 3 ώρες πρόσβαση που πρέπει να χρησιμοποιηθούν σε ένα μήνα.

1.4 Τρόπος Λειτουργίας Ασυρμάτων Δικτύων Μέσω Οικογένειας Πρωτοκόλλων 802.11

1.4.1 Το Πρωτόκολλο 802.11

Όπως αναφέρθηκε και στις παραπάνω σελίδες, η οικογένεια πρωτοκόλλων 802.11 περικλείει πολλαπλά και διαφορετικά πρωτόκολλα. Τα τελευταία γράμματα (δηλαδή τα 802.11a) υποδεικνύουν τις διάφορες ταχύτητες και ζώνες συχνοτήτων που χρησιμοποιούνται οι οποίες αναφέρονται στον ακόλουθο πίνακα[27] :

Πρότυπο	***Ταχύτητα***	***ζώνη 2,4 GHz***	***ζώνη 5 GHz***	***Λεπτομέρειες***

[27] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

802.11	1-2 Mbps	X		Αυτό το πρότυπο είναι παλαιότερο και τα περισσότερα προϊόντα στην αγορά δεν το υποστηρίζουν.
802.11a	54 Mbps		X	Αυτή τη στιγμή, κυκλοφορούν στην αγορά ορισμένα προϊόντα που χρησιμοποιούν αυτό το πρότυπο, αλλά δεν είναι συμβατά με οποιαδήποτε από τα προϊόντα που χρησιμοποιούν τη συχνότητα των 2,5 GHz. Ως αποτέλεσμα, δεν είναι συμβατά με τον εξοπλισμό 802.11b που ίσως χρησιμοποιείτε.
802.11b (11 Mbps)	11 Mbps	X		Τα ασύρματα προϊόντα πρόσβασης των 11 Mbps χρησιμοποιούν αυτό το πρότυπο. Αυτά τα προϊόντα είναι ιδιαίτερα προσιτά και συμβατά με τα προϊόντα 802.11b που κατασκευάζονται από άλλες εταιρείες.
802.11b **(**22 Mbps**)**	22 Mbps	X		Τα ασύρματα προϊόντα πρόσβασης των 22 Mbps είναι συμβατά με το πρότυπο 802.11b (στα 11 Mbps) και είναι συμβατά με το πρότυπο 802.11g (στα 54/100/125 Mbps). Τα προϊόντα των 22 Mbps είναι συμβατά με τις παλαιότερες και τις νεότερες εκδόσεις αυτών των προτύπων. Όταν χρησιμοποιούνται με τα προϊόντα των 11 Mbps, αυτά τα προϊόντα σας δίνουν ένα ισχυρότερο σήμα, μεγαλύτερο εύρος και 70% μεγαλύτερο χώρο κάλυψης.
802.11g	54 Mbps	X		Τα ασύρματα προϊόντα πρόσβασης των 54 Mbps είναι συμβατά με το πρότυπο 802.11b (στα 11 και τα 22 Mbps) και είναι συμβατά με τα ασύρματα προϊόντα πρόσβασης των 100/125 Mbps. Αν έχετε προϊόντα 22 Mbps 802.11b, θα έχετε τη δυνατότητα να προσθέσετε προϊόντα 802.11g χωρίς να χρειαστεί να αντικαταστήσετε τον τρέχοντα

				εξοπλισμό σας.
802.11g (Wireless Turbo)	100/125 Mbps	X		Τα ασύρματα προϊόντα πρόσβασης των 100/125 Mbps είναι συμβατά με το πρότυπο 802.11g (στα 100 και τα 54 Mbps) και με το 802.11b (στα 11 και τα 22 Mbps). Αν έχετε προϊόντα 22 Mbps 802.11b ή προϊόντα 802.11g στα 54 Mbps, θα έχετε τη δυνατότητα να προσθέσετε προϊόντα 802.11g χωρίς να χρειαστεί να αντικαταστήσετε τον τρέχοντα εξοπλισμό σας.
802.11g (Wireless MAXg)	125 Mbps	X		Τα ασύρματα προϊόντα πρόσβασης των 125 Mbps είναι συμβατά με το πρότυπο 802.11g (στα 125 και τα 54 Mbps) και με το 802.11b (στα 11). Αν έχετε προϊόντα 802.11b ή προϊόντα 802.11g στα 54 Mbps, θα έχετε τη δυνατότητα να προσθέσετε προϊόντα Wireless MAXg 802.11g χωρίς να χρειαστεί να αντικαταστήσετε τον τρέχοντα εξοπλισμό σας.

Η 802.11 θεωρείται μια οικογένεια προτύπων η οποία περιγράφει τη λειτουργία των ασύρματων τοπικών δικτύων όπως WLAN ή Wireless Local Access Network. Περιγράφονται τα δύο πρώτα επίπεδα του O.S.I., δηλαδή το φυσικό επίπεδο PHY - Physical Layer και το επίπεδο σύνδεσης δεδομένων όπως MAC - Medium Access Control. Τα πρωτόκολλα αυτά δημοσιεύονται από την IEEE γεγονός που είναι σημαντικό για την διαλειτουργικότητα, δηλαδή την ικανότητα συνεργασίας των συσκευών που το ακολουθούν.

Η IEEE 802.11 περιγράφει μόνο τα δύο κατώτερα επίπεδα του OSI, επιτρέποντας έτσι σε οποιαδήποτε εφαρμογή να μπορεί να εργάζεται πάνω σε συσκευή 802.11 όπως ακριβώς θα εργαζόταν πάνω από *Ethernet*. Οι

συσκευές 802.11 δηλαδή μπορούν και μεταφέρουν διαφανώς την πληροφορία από τα πιο πάνω επίπεδα του OSI[28].

Το έτος 1997, μετά από επτά χρόνια μελέτης, η IEEE δημοσίευσε επιτέλους το πρότυπο IEEE 802.11, το πρώτο πρότυπο για την ασύρματη δικτύωση. Το πρότυπο αυτό προβλέπει ρυθμούς μετάδοσης 1 και 2 Mbps. Η μετάδοση γίνεται με ασύρματο τρόπο με χρήση διαμόρφωσης FHSS ή DSSS σε ζώνες συχνοτήτων 915MHz, 2.4GHz, 5.2GHz ή υπέρυθρη μετάδοση στα 850nm ως 900nm[29]. Υποστηρίζει επίσης δυνατότητες όπως την προτεραιοποίηση της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής. Το πρότυπο γνώρισε βέβαια περιορισμένη επιτυχία λόγω των πολύ χαμηλών ρυθμών μετάδοσης.

1.4.2 Το Πρωτόκολλο 802.11b

Το πρωτόκολλο 802.11b αναπτύχθηκε το έτος 1999 και αποτελεί μια επέκταση στο αρχικό πρότυπο. Συγκεκριμένα υποστηρίζει τη μετάδοση επιπλέον σε ρυθμούς 5.5 και 11Mbps με κωδικοποίηση CCK - Complementary Code Keying. Μια δεύτερη κωδικοποίηση, η PBCC - Packet Binary Convolutional Code ορίστηκε για προαιρετική υλοποίηση υποστηρίζοντας μετάδοση 5.5 και 11Mbps και έχοντας βέβαια ελαφρά καλύτερη ευαισθησία δέκτη με αντίτιμο την πολυπλοκότητα. Η μετάδοση τους γίνεται στη ζώνη συχνοτήτων των 2.4GHz Είναι το πιο δημοφιλές από όλα τα πρότυπα και το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα, όντας ένα στιβαρό, αποτελεσματικό και δοκιμασμένο πρότυπο.

Οι προσθήκες της 802.11b και σε σχέση με την 802.11 αφορούν μόνο τον τρόπο μετάδοσης, ενώ ο τρόπος πρόσβασης των συσκευών και οι τρόποι λειτουργίας μένουν οι ίδιοι. Μια συσκευή η οποία εργάζεται ακολουθώντας το 802.11b, υλοποιεί και τους τρόπους μετάδοσης του 802.11 και έτσι μπορεί να

---

28 Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA

29 Pfleeger, C., P. 1997, "*Security in Computing*", Prentice Hall

θεωρείται συμβατή με αυτό. Αυτή η ιδιότητα ονομάζεται συμβατότητα προς τα πίσω, δηλαδή ότι οι καινούργιες συσκευές θα μπορούν να συνεργαστούν και με παλιότερες, προκειμένου να μην αναγκαστεί ο καταναλωτής να αλλάξει εξ ολοκλήρου τον εξοπλισμό του για ένα ασύρματο δίκτυο.

Τέλος θα πρέπει να σημειωθεί πως το δίκτυο 802.11b ή WI-FI παρέχει μετάδοση 11 Mbps στη ζώνη 2.4 GHz. Δεν είναι δυνατό να χρησιμοποιηθεί με το 802.11a εντούτοις. Προσφέρει πρόσβαση σε κάποια δεδομένα σε απόσταση μέχρι τα 100 μέτρα από το σταθμό βάσης. Η ισχύς που ορίζει το στάνταρτ στις εξόδους κεραίας των εμπορικών συσκευών είναι τα 0.2mw. Στο αρχικό πρωτόκολλο του 802.11, καθορίζονται δύο τρόποι κωδικοποίησης, ο FHSS - Frequency Hopping Spread Spectrum) και ο DSSS - Direct Sequence Spread Spectrum[30].

1.4.3 Το Πρωτόκολλο 802.11a

Το έτος 1999 δημιουργήθηκε η επέκταση στο αρχικό πρότυπο που προβλέπει τη μετάδοση στη ζώνη συχνοτήτων U-NII των 5GHz με ρυθμούς μετάδοσης 1, 2, 5.5, 11, 6, 12, 24 Mbps και προαιρετικά 36, 48, 54 Mbps χρησιμοποιώντας τη OFDM - Orthogonal Frequency Division Multiplexing) διαμόρφωση[31]. Η επέκταση αυτή αποσκοπούσε να καλύψει την άμεση ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης. Επιλέχθηκε λοιπόν η λειτουργία σε μια υψηλότερη ζώνη συχνοτήτων, αφενός για να καταστεί δυνατόν να υποστηριχθούν οι μεγαλύτεροι ρυθμοί και αφετέρου ώστε να μην υπάρχει παρεμβολή από τις προηγούμενες συσκευές.

Οι αντίστοιχες βέβαια συσκευές είναι ασύμβατες με αυτές που εργάζονται με το 802.11b, αφού ο τρόπος μετάδοσης τους αλλά και οι

---

30 McCarthy, L., 1997, "*Intranet Security*", Prentice Hall

31 Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

ραδιοσυχνότητες που χρησιμοποιούνται είναι διαφορετικές. Το πρωτόκολλο 802.11a μπορεί και παρέχει μια μετάδοση μέχρι 54 Mbps στη ζώνη των 5GHz καθώς και λιγότερο δυναμικό για παρεμβολή σε ραδιοσυχνότητα από το 802.11b και το 802.11g. Σε σχετικά μικρότερη εμβέλεια και περίπου τα 60 μέτρα από το 802.11b καθώς επίσης δεν είναι δυνατό να χρησιμοποιηθεί ταυτόχρονα με το 802.11b[32].

1.4.4 Το Πρωτόκολλο 802.11g

Το πρωτόκολλο 802.11g παρέχει μια μετάδοση μέχρι 54 Mbps και τυπικά στα 22 Mbps στη ζώνη 2.4 GHz. Θεωρείται ότι είναι ουσιαστικά ο διάδοχος του και συμβατός με το 802.11b. Προσφέρει μια πρόσβαση υψηλής ταχύτητας σε δεδομένα σε απόσταση μέχρι 100 μέτρα από το σταθμό βάσης. Το πρωτόκολλο 802.11g αποτελεί επέκταση στο 802.11b ώστε να υποστηρίζει μεγαλύτερους ρυθμούς. Με το τρόπο αυτό και εκτός από τους ρυθμούς μετάδοσης του 802.11b, με CCK διαμόρφωση, μπορεί και υποστηρίζει και ρυθμούς μέχρι 54Mbps χρησιμοποιώντας την OFDM διαμόρφωση. Οι αντίστοιχες συσκευές εργάζονται στη ζώνη συχνοτήτων των 2.4GHz, διατηρώντας έτσι την συμβατότητα προς τα πίσω με το 802.11b[33].

Κάποια προϊόντα wireless είναι βασισμένα στο πρωτόκολλο 802.11g στα 54Mbps, το νέο standard ασύρματης δικτύωσης το οποίο είναι σχεδόν 5 φορές ταχύτερο από το παλαιότερο μοντέλο 802.11b. Καθώς όμως με το παλαιότερο αυτό πρωτόκολλο μοιράζονται την ίδια συχνότητα στα 2.4GHz, οι ασύρματες συσκευές μπορούν να συνεργαστούν και με εξοπλισμό 802.11b στα 11Mbps. Το 802.11g επιτρέπει σε κάποιον να συνδέσει συσκευές wireless στο δίκτυο. Καθώς και τα δύο standards είναι ενσωματωμένα, μπορεί κάποιος να προστατεύει την επένδυσή του σε υφιστάμενη υποδομή 802.11b, και να ενοποιεί τους clients του δικτύου στο νέο, ταχύτερο standard Wireless καθώς οι ανάγκες του μεγαλώνουν.

---

32 Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

33 Σταμάτης, Κ., Ν., 2002, «*Η Αβέβαιη Κοινωνία της Γνώσης*», Εκδόσεις Σαββάλας

Τέλος θα πρέπει να αναφερθεί πως για την προστασία του κάθε δικτύου, το 802.11g μπορεί να κρυπτογραφήσει όλες τις ασύρματες μεταδόσεις δεδομένων και να υποστηρίζει το εργοστασιακό πρότυπο ασφαλείας WPA. Το φίλτρο MAC διευθύνσεων επιτρέπει στους χρήστες να επιλέξουν ποιος θα έχει πρόσβαση στο ασύρματο δίκτυό. Η παραμετροποίηση γίνεται πολύ απλά, με το εργαλείο παραμετροποίησης που είναι βασισμένο σε μονάδα web.

1.4.5 Τα Υπόλοιπα Πρωτόκολλα

1.4.5.1 Πρωτόκολλο 802.11h

Το πρωτόκολλο 802.11h είναι ένα πρότυπο, συμπληρωματικό του IEEE 802.11 και συμβατό με τους ευρωπαϊκούς κανονισμούς. Προσθέτει έναν σωστό έλεγχο της ισχύος της μετάδοσης και επιλογή δυναμικής συχνότητας. Η ιδιότητα του δικτύου 802.11h+d βέβαια ρυθμίζει τις παραμέτρους προηγμένου ελέγχου ραδιοεπικοινωνίας της κάρτας wireless WLAN του κάθε υπολογιστή μέσω συνδεδεμένου ρούτερ / AP[34]. Τα στοιχεία ελέγχου ενεργοποιούνται φυσικά όταν η ιδιότητα 802.11h+d έχει ρυθμιστεί σε θέση "*Χαλαρή 11h*", "*Χαλαρή 11h+d*", ή "*Βασική11h*". Όταν η ρύθμιση είναι "*Βασική 11h*", η κάρτα wireless WLAN του υπολογιστή συνδέεται μόνο σε σημεία πρόσβασης που υποστηρίζουν πρωτόκολλα IEEE 802.11h κατά τη λειτουργία και σε περιοχές με ειδικούς περιορισμούς όσον αφορά τις ραδιοεπικοινωνίες.

Όταν η ρύθμιση είναι "*Χαλαρή 11h*", ο προσαρμογέας της κάρτας δεν περιορίζει τις συνδέσεις βάσει της υποστήριξης ασύρματου μεταξύ ρούτερ/AP IEEE 802.11h. Όταν τέλος η ρύθμιση είναι "*Χαλαρή 11h+d*", ο προσαρμογέαςτης κάρτας δεν περιορίζει τις συνδέσεις βάσει του ασύρματου ρούτερ/AP IEEE 802.11h ή IEEE 802.11d της υποστήριξης[35].

1.4.5.2 Πρωτόκολλο 802.11e

---

34 Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

35 Σταμάτης, Κ., Ν., 2002, «*Η Αβέβαιη Κοινωνία της Γνώσης*», Εκδόσεις Σαββάλας

Το πρωτόκολλο 802.11e ή QoS το οποίο προσπαθεί να διασφαλίσει ποιότητα υπηρεσιών για εφαρμογές πραγματικού χρόνου που εκτελούνται πάνω σε ένα WLAN ελαχιστοποιώντας ή μεγιστοποιώντας ένα από τα παρακάτω κριτήρια: μέση καθυστέρηση από άκρο σε άκρο, μέση μεταβολή της καθυστέρηση ή μέσο ποσοστό επιτυχούς παράδοσης πλαισίων. Αυτό το επιτυγχάνει βελτιώνοντας τους μηχανισμούς DCF και PCF με τους μηχανισμούς EDCF, ο οποίος αναθέτει προτεραιότητες στα πλαίσια δεδομένων ανάλογα με το πόσο χρονικά κρίσιμη είναι η παράδοση τους και με τα μεγαλύτερης προτεραιότητας πλαίσια να έχουν περισσότερες πιθανότητες να κερδίσουν στον ανταγωνισμό για την πρόσβαση στο κοινό μέσο, και HCF, ο οποίος περιορίζει το μέγιστο χρόνο δέσμευσης του καναλιού από ένα τερματικό, αντίστοιχα[36].

Στο πεδίο των τηλεπικοινωνιών και των δικτύων υπολογιστών ο όρος ποιότητα υπηρεσιών (αγγλιστί Quality of Service, QoS) αναφέρεται σε μηχανισμούς διασφάλισης της στατικής ανάθεσης δικτυακών πόρων σε συνδέσεις οι οποίες το απαιτούν. Η ποιότητα υπηρεσιών υλοποιείται με απόδοση προτεραιοτήτων στις διαφορετικές συνδέσεις ενός δικτύου, έτσι ώστε όσες χρειάζονται σταθερούς πόρους (π.χ. εφαρμογές πραγματικού χρόνου, όπως βιντεοδιάσκεψη ή άλλες υπηρεσίες πολυμέσων) να είναι βέβαιο ότι τους διαθέτουν.

Οι εν λόγω πόροι διασφαλίζουν χαρακτηριστικά της σύνδεσης όπως τον απαιτούμενο ρυθμό μετάδοσης δεδομένων, την απαιτούμενη καθυστέρηση, μεταβολή της καθυστέρησης, πιθανότητα απώλειας πακέτων κλπ. Οι μηχανισμοί ποιότητας υπηρεσιών παρέχουν εγγυήσεις για τη σταθερότητα ενός ή περισσότερων από αυτά τα χαρακτηριστικά της σύνδεσης υπό συνθήκες συμφόρησης και περιορισμένης χωρητικότητας του τηλεπικοινωνιακού καναλιού. Επίσης η ποιότητα υπηρεσιών είναι απαραίτητη μόνο σε δίκτυα μεταγωγής πακέτων, αφού σε δίκτυα μεταγωγής κυκλώματος ο τύπος και τα χαρακτηριστικά κάθε σύνδεσης γίνονται αντικείμενο

[36] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

διαπραγμάτευσης κατά την εγκαθίδρυση της τελευταίας και παραμένουν σταθερά μέχρι τον τερματισμό της[37].

1.4.5.3 Πρωτόκολλο 802.11c,d,f

Τα πρωτόκολλα 802.11c,d,f διαχωρίζονται με βάση το βαθμό λειτουργιών τους και αναφέρονται ως ακολούθως :

- *Πρωτόκολλο 802.11c το οποίο έχει ως σκοπό τη λειτουργία γεφύρωσης (bridging) πλαισίων 802.11*
- *Το πρωτόκολλο 802.11d το οποίο λειτουργεί με επεκτάσεις στο πρότυπο ώστε να λειτουργεί σε επιπλέον ρυθμιστικά πλαίσια δηλαδή άλλες ζώνες συχνοτήτων*
- *Το πρωτόκολλο 802.11f το οποίο αποτελεί μια συνιστώμενη πρακτική για το πρωτόκολλο IAPP - Inter Access Point Protocol*

1.4.5.4 Πρωτόκολλο 802.11i

Το πρωτόκολλο 802.11i εμπλουτίζει ουσιαστικά το υπόστρωμα MAC προκειμένου να αντιμετωπίσει τα ζητήματα ασφαλείας που σχετίζονται με το Wired Equivalent Privacy (WEP)[38]. Οι αλγόριθμοι της κρυπτογράφησης που χρησιμοποιούνται στις μέρες μας, όπως ο WEP - Wired Equivalent Privacy, ο WPA - Wi-Fi Protected Access και IP SEC παρουσιάζουν κάποια σημαντικά προβλήματα. Για παράδειγμα μπορεί να αναφερθεί πως ο πρώτος εμφανίζει σημαντικά κενά ασφαλείας, ο WPA ενώ έρχεται να καλύψει τα κενά του WEP, στην πραγματικότητα δεν καλύπτει την ουσιαστική ασφάλεια στα ασύρματα τοπικά δίκτυα. Τέλος, ο IP SEC εφαρμόζεται τοπικά σε κάθε χρήστη και καλύπτει *Point-to-Point* συνδέσεις.

Το υπάρχον βέβαια πρότυπο πρωτόκολλο 802.11 προδιαγράφει τη χρήση σχετικά αδύναμων, στατικών κρυπτογραφικών κλειδιών χωρίς καμία απολύτως μορφή διαχείρισης της κατανομής των κλειδιών. Αυτό προσφέρει

---

37 McCarthy, L., 1997, "*Intranet Security*", Prentice Hall

38 Σταμάτης, Κ., Ν., 2002, «*Η Αβέβαιη Κοινωνία της Γνώσης*», Εκδόσεις Σαββάλας

τη δυνατότητα σε *hackers* να αποκτήσουν σημαντική πρόσβαση και να αποκρυπτογραφήσουν δεδομένα του ασύρματου δικτύου (WLAN) τα οποία έχουν κρυπτογραφηθεί με τον αλγόριθμο WEP. Η ομάδα αναθεώρησης του 802.11i θα προσπαθήσει να αντικαταστήσει το WEP και την υποστήριξή του σε συσκευές, αρχικά με την δημιουργία ενός ανώτερου πρωτοκόλλου ασφαλείας και προς τα πίσω συμβατό με το WEP, και τελικά με την πλήρη κατάργησή του.

2. Κεφάλαιο Δεύτερο : Ασύρματο Δίκτυο IPV6

2.1 Ορισμός του IPv6

Το ***Internet Protocol version 6 (IPv6)*** αποτελεί τη νεώτερη έκδοση του πρωτοκόλλου IPv4, το οποίο σταδιακά θα αντικατασταθεί στο μέλλον. Η σχεδίαση του IPv6 στηρίχθηκε στην εκτεταμένη εμπειρία που αποκτήθηκε με το πέρασμα του χρόνου από τη λειτουργία και τη ραγδαία εξάπλωση του Διαδικτύου. Το IPv6 περιλαμβάνει σειρά λειτουργικών βελτιώσεων και απλοποιήσεων σε σχέση με το IPv4. Μία βασική βελτίωση του IPv6 είναι το μεγαλύτερο εύρος διευθύνσεων που θα επιτρέψει την απρόσκοπτη επέκταση του Διαδικτύου με νέες συσκευές, όπως έξυπνα τηλέφωνα (smartphones),

αισθητήρες (sensors), κλπ. Το IPv6 θα συμβάλει επίσης στην ασφάλεια των ψηφιακών επικοινωνιών και στην κινητικότητα (mobility) των χρηστών[39].

Θα πρέπει αρχικά να σημειωθεί πως την περίοδο 1993-1998, η επιστημονική κοινότητα ανέπτυξε ένα νέο πρωτόκολλο, το IPv6, το οποίο προσφέρει ένα πρακτικά απεριόριστο φάσμα διευθύνσεων, με μακροπρόθεσμο στόχο να αντικαταστήσει πλήρως το IPv4. Το IPv6 είναι βελτιωμένο στους τομείς της διαχείρισης, της φορητότητας, της ασφάλειας, της ποιότητας υπηρεσιών και της πολυπλοκότητας του δικτύου[40].

Στον τομέα της κινητικότητας (mobility), το πρωτόκολλο Mobile IPv6 επιτρέπει την απρόσκοπτη επικοινωνία των χρηστών, καθώς μετακινούνται ανάμεσα σε ζώνες ενός δικτύου ή ανάμεσα σε διαφορετικά δίκτυα, αξιοποιεί τις δυνατότητες διευθυνσιοδότησης και ασφάλειας του IPv6 και βελτιστοποιεί τη δρομολόγηση των πακέτων. Στον τομέα της ασφάλειας, το πρότυπο του IPv6 ενσωματώνει την υποστήριξη των βασικών μηχανισμών ασφάλειας, που αποτελούσαν προαιρετικές επεκτάσεις του IPv4 και προσφέρει μεγαλύτερη προστασία από επιθέσεις (fragmentation, broadcast amplification attacks), για την από άκρη-σε-άκρη ασφάλεια των επικοινωνιών στο Διαδίκτυο[41]

Το IPv6 υποστηρίζει την κατηγοριοποίηση πακέτων με προτεραιότητες δρομολόγησης, ώστε να επιτυγχάνεται η επιθυμητή ποιότητα υπηρεσίας, και με το πρακτικά απεριόριστο φάσμα διευθύνσεων, επιτρέπει την ευρεία διάδοση και χρήση δημόσιων διευθύνσεων IPv6 στα τοπικά δίκτυα, διευκολύνοντας την απευθείας επικοινωνία των συσκευών του Διαδικτύου, χωρίς τη μεσολάβηση συσκευών NAT, και απλοποιώντας την ανάπτυξη, εγκατάσταση και χρήση εφαρμογών client-server και peer-to-peer (P2P).

---

39 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

40 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

41 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

Το IPv6 ήδη υποστηρίζεται από ένα ευρύ φάσμα σύγχρονων λειτουργικών συστημάτων για προσωπικούς υπολογιστές, φορητές συσκευές και συσκευές δικτύου, όπως είναι τα Microsoft Windows XP SP2/VISTA/ Server 2008, Apple Mac OS X, Linux, Symbian OS 7 και Windows Mobile. Επίσης, τμήματα του κορμού του Διαδικτύου υποστηρίζουν το νέο πρωτόκολλο. Παρόλα αυτά, η χρήση του δεν έχει ακόμη διαδοθεί ανάμεσα στους παρόχους υπηρεσιών πρόσβασης στο Διαδίκτυο, στις επιχειρήσεις[42].

Η μετάβαση στο IPv6 δημιουργεί νέες προκλήσεις κι επιχειρηματικές ευκαιρίες. Το IPv6 δεν είναι άμεσα συμβατό με το IPv4. Οι συσκευές που υποστηρίζουν μόνον το ένα πρωτόκολλο δεν μπορούν να επικοινωνήσουν απευθείας με συσκευές που υποστηρίζουν το άλλο. Συνεπώς, η μετάβαση προϋποθέτει τη χρήση κατάλληλων στρατηγικών και τεχνικών, όπως είναι η παράλληλη χρήση και των δύο πρωτοκόλλων επικοινωνίας και η χρήση συστημάτων «σήραγγας» (tunneling) και «μετάφρασης» (translation). Η εγκατάσταση και λειτουργία του νέου πρωτοκόλλου συνεπάγεται κόστη εκπαίδευσης προσωπικού, αναβάθμισης δικτύων και εξοπλισμού[43].

Η Ευρωπαϊκή Ένωση έχει χρηματοδοτήσει περισσότερα από 30 έργα έρευνας και ανάπτυξης για την προώθηση του IPv6, επιτυγχάνοντας την απόκτηση τεχνογνωσίας κι εμπειρίας στην υλοποίηση και στη λειτουργία των IPv6 δικτύων. Ανάμεσα σε αυτά είναι το 6net και το δίκτυο GÉANT στα οποία συμμετέχει ενεργά από το 2000. Σήμερα, το δίκτυο του ΕΔΕΤ παρέχει διασύνδεση και τεχνογνωσία IPv6 σε Πανεπιστημιακά ιδρύματα και σε σχολεία της χώρας μας. Το επόμενο βήμα, στην υιοθέτηση και στην αξιοποίηση του IPv6, θα γίνει με την παροχή και υποστήριξη υπηρεσιών πρόσβασης και διασύνδεσης από τους εμπορικούς τηλεπικοινωνιακούς

---

[42] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

[43] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

παρόχους (ISPs). Η υποστήριξη του νέου πρωτοκόλλου θα αποτελέσει ανταγωνιστικό πλεονέκτημα, καθώς όλο και περισσότερες επιχειρήσεις και καταναλωτές ενημερώνονται για τα πλεονεκτήματα και προσβλέπουν στην αποδέσμευση των δικτύων τους από το σύστημα NAT, και στην αξιοποίηση των δυνατοτήτων του IPv6[44].

Τέλος, η μετάβαση στο νέο πρωτόκολλο θα πραγματοποιηθεί ομαλά και εποικοδομητικά από την αγορά μέσα από την ενημέρωση, την εκπαίδευση και τον συντονισμό των ενδιαφερόμενων. Οι χρήστες, οι οργανισμοί και οι χώρες, που θα αξιοποιήσουν εγκαίρως τις δυνατότητες και τις προοπτικές που δημιουργεί το νέο πρωτόκολλο, επενδύοντας στην ανάπτυξη και στην αξιοποίηση νέων, καινοτόμων, δημοφιλών υπηρεσιών, θα αποκτήσουν σημαντικά ανταγωνιστικά πλεονεκτήματα[45].

2.2 Προκλήσεις του IPv6 στην Ασύρματη Τεχνολογία

Το επίσημο όνομα του είναι IPv6 (Internet Protocol version 6) και έρχεται να δώσει λύση στο εμφανή 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[46].

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 όπως

---

44 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

45 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

46 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

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.

Τέλος, θα πρέπει να σημειωθεί πως 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.

2.3 Περιγραφή Βημάτων του IPv6

Με την προοπτική να αντιμετωπισθούν οι απαιτήσεις του νέου δικτύου όπου θα υπάρχει αλλαγή από τις συσκευές που θα το αποτελούν έως και τις εφαρμογές (multimedia περιβάλλον) που θα υποστηρίζει, το IETF έδωσε προσοχή στους εξής τομείς[47]:

<u>Διευθυνσιοδότηση</u>

Το IPv6 χρησιμοποιεί ένα σχήμα διευθυνσιοδότησης μεγέθους 128-bit. Το μέγεθος των διευθύνσεων που παράγονται είναι τόσο μεγάλο ώστε είναι δυνατό ο κάθε κάτοικος αυτού του πλανήτη να έχει τόσες διευθύνσεις για το δίκτυο του όσες το τωρινό Διαδίκτυο. Το βασικότερο όμως δεν είναι η δημιουργία ενός σχήματος διευθυνσιοδότησης που θα παράγει πολλές σε αριθμό διευθύνσεις όσο η κατανομή των διευθύνσεων αυτών. Το IPv6 κατανέμει τις διευθύνσεις με ιεραρχικό τρόπο αποφεύγοντας έτσι τα προβλήματα του IPv4 όπου και παραγόταν υπέρογκη πληροφορία για τη δρομολόγηση πάνω στα συστήματα και οι διευθύνσεις έμεναν αχρησιμοποίητες[48].

---

47 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

48 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

Οι τάξεις των διευθύνσεων στο IPv6 απευθύνονται καλύτερα στους χρήστες απ' ότι στο IPv4. Υπάρχουν βασικά τρεις κατηγορίες δικτυακών χρηστών: αυτοί που χρησιμοποιούν το δίκτυο ενός οργανισμού και μέσω αυτού και το Διαδίκτυο, αυτοί που χρησιμοποιούν μόνο το δίκτυο του οργανισμού με πιθανότητα να χρησιμοποιήσουν το Διαδίκτυο στο μέλλον και χρήστες που συνδέονται στο Διαδίκτυο διαμέσου τηλεφωνικών γραμμών. Για την καλύτερη εξυπηρέτηση αυτών των δικτυακών χρηστών το IPv6 παρέχει τρεις τύπους διευθύνσεων, τις unicast, τις multicast και τις anycast.

Απόδοση

Η δικτυακή απόδοση έχει άμεση σχέση με την δρομολόγηση των πακέτων. Το ποσό της πληροφορίας που παράγεται συνεχώς αυξάνει και σε αυτό συντελούν και οι νέου είδους εφαρμογές. Οι ταχύτητες όμως που υποστηρίζουν τα LANs και τα WANs αυξάνουν και αυτές και έτσι οι λειτουργίες επεξεργασίας και προώθησης των IP πακέτων από τους δρομολογητές θα πρέπει να γίνονται ακόμα ταχύτερα.

Με αυτή τη λογική το IPv6 περιέχει λιγότερα πεδία στη κεφαλή (header) του πακέτου απ' ότι το IPv4 και εισάγει την χρήση των επεκτάσεων των κεφαλών οι οποίες βρίσκονται μεταξύ της IPv6 κεφαλής και της κεφαλής του transport επιπέδου. Η ταχύτητα λοιπόν επεξεργασίας και προώθησης του πακέτου από τους δρομολογητές αυξάνει γιατί οι περισσότερες από τις επεκτάσεις των κεφαλών δεν εξετάζονται από τους ενδιάμεσους δρομολογητές, οι οποίοι έχουν να επεξεργαστούν μόνο σταθερού μήκους IPv6 κεφαλές απλοποιώντας κατά πολύ την επεξεργασία και προώθηση. Επίσης ο φόρτος στους ενδιάμεσους δρομολογητές μειώνεται περισσότερο αφού την διαδικασία τεμαχισμού (fragmentation)και ανασχηματισμού (reassembly) των πακέτων αναλαμβάνουν οι επικοινωνούντες hosts[49].

Η απόδοση με το IPv6 βελτιώνεται με την χρήση του πεδίου της κεφαλής flow label, όπου κατορθώνεται να ζητηθούν συγκεκριμένες απαιτήσεις από τους δρομολογητές για κάποια διαδρομή. Οι απαιτήσεις

[49] Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

σχετίζονται με την προτεραιότητα, τη καθυστέρηση ή το εύρος ζώνης (bandwidth) που ζητούν κάποιες εφαρμογές όπως αυτές που μεταδίδουν video κ.α.

Ασφάλεια

Η ανάπτυξη και η εκτεταμένη χρήση του Διαδικτύου έφερε καινούργιες απαιτήσεις από τους χρήστες οι οποίοι ζητούν οι συναλλαγές τους και η πρόσβαση στις πηγές τους να γίνονται με ασφάλεια. 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[50].

Το IPv6 όμως παρέχει εγγενής δυνατότητες για παροχή ασφάλειας οι οποίες βασίζονται στις προσαρμοστικές επεκτάσεις της κεφαλής του IPv6 πακέτου. Η επέκταση της πιστοποίησης (authentication header extension) εξασφαλίζει ότι όντως το πακέτο έρχεται από τον host που δείχνει η διεύθυνση της πηγής. Αυτή η πιστοποίηση είναι σημαντική στη προστασία έναντι των εισβολέων, οι οποίοι ρυθμίζουν ένα host να παράγει πακέτα με πλαστή διεύθυνση πηγής. Αυτή η μεταμφίεση μπορεί να ξεγελάσει (IP spoofing) και να υπάρξει παράτυπη πρόσβαση σε πολύτιμα δεδομένα ή σε κρίσιμες δικτυακές λειτουργίες. Η σημερινή αντιμετώπιση αυτού του προβλήματος γίνεται με τους Firewalls, η χρήση των οποίων παρουσιάζει μία σειρά από προβλήματα όπως μείωση στην απόδοση, περιοριστική δικτυακή πολιτική και περιορισμένη διασύνδεση με το Διαδίκτυο[51].

Μία άλλη διαδεδομένη παγίδα στο Διαδίκτυο είναι οι αναλυτές της κυκλοφορίας της πληροφορίας (sniffers) οι οποίοι λαθραία παρακολουθούν τη πληροφορία που διέρχεται στο δίκτυο. Με αυτό το τρόπο μπορούν να γίνουν

---

50 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

51 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

γνωστά εμπορικά μυστικά, αριθμοί τραπεζικών λογαριασμών και πλαστικών καρτών, συνθηματικά (passwords) καθώς και άλλα πολύτιμα δεδομένα. Το IPv6 παρέχει και σε αυτό το πρόβλημα εγγενή λύση μέσω της επέκτασης για κρυπτογράφηση της κεφαλής του IPv6 πακέτου όπου διαμέσου κλειδιών κρυπτογράφησης γίνεται κρυπτογράφηση του περιεχομένου (payload) του πακέτου. Η χρήση των επεκτάσεων ασφαλείας μπορεί να γίνει απ' ευθείας μεταξύ δύο hosts ή σε συνδυασμό με μία πύλη ασφαλείας (security gateway) η οποία και προσθέτει ένα βαθμό περισσότερης ασφάλειας[52].

Αυτόματη Διευθέτηση (Autoconfiguration)

Οι ρυθμίσεις των IPv4 συστημάτων είναι συνήθως δύσκολες και προβληματικές. Το IPv6 προσφέρει δύο τρόπους αυτόματης διευθέτησης των δικτυακών υπολογιστικών συστημάτων: την stateful και την statelless. Με την stateful αυτόματη διευθέτηση παρόχων μπορούν δυναμικά να καθορίζουν διευθύνσεις στα υπολογιστικά συστήματα τις οποίες παίρνουν από μία βάση δεδομένων με καταχωρημένες από πριν διευθύνσεις. Με τον ίδιο τρόπο λειτουργεί και το πρωτόκολλο DHCP στο IPv4 και ουσιαστικά μία πιο εξελιγμένη έκδοση του DHCP έχει αναπτυχθεί στο IPv6 για να προσφέρει stateful αυτόματη διευθέτηση[53].

Το IPv6 εισάγει όμως και την statelless αυτόματη διευθέτηση κατά την οποία δεν είναι απαραίτητη η παρουσία του παρόχου. Κατά την statelless αυτόματη διευθέτηση τα συστήματα μπορούν να ρυθμίσουν μόνα τους τις διευθύνσεις με τη βοήθεια του τοπικού IPv6 δρομολογητή. Η διεύθυνση είναι συνδυασμός της 48-bit MAC-διεύθυνσης (πχ. η διεύθυνση του ethernet interface) με πρόθεμα (prefix) της δικτυακής διεύθυνσης που μαθαίνει από το τοπικό δρομολογητή.

---

[52] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

[53] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

Οι δυνατότητες της αυτόματης διευθέτησης διευθύνσεων μειώνει πάρα πολύ το βάρος της εργασίας του διαχειριστή ενός δικτύου και ωφελεί τους δικτυακούς χρήστες. Παράδειγμα όπου βοηθάει αποτελεσματικά η αυτόματη διευθέτηση διευθύνσεων είναι η περίπτωση όπου μία επιχείρηση αλλάζοντας παροχέα-ISP χρειάζεται καινούργιες διευθύνσεις (renumbering) για όλους τους σταθμούς εργασίας. Επίσης η λειτουργία αυτή του IPv6 είναι απαραίτητη και σε μία επιχείρηση όπου υπάρχουν μετακινήσεις και αλλαγές στο πληθυσμό οπότε χρειάζεται και εδώ μια δυναμική παροχή διευθύνσεων. Σημαντική όμως είναι η βοήθεια στο τομέα του mobile computing όπου η αυτόματη διευθέτηση διευθύνσεων παρέχει τη δυνατότητα στους κινητούς υπολογιστές να αποκτήσουν αυτόματα IP διεύθυνση από οπουδήποτε και αν συνδέονται στο δίκτυο[54].

Μετάβαση

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[55].

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 συνλειτουργία των IPv4 και IPv6 και δεν

---

54 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

55 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

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.

2.4 Προτάσεις Σχετικά με την Καλύτερη και Αποδοτικότερη Λειτουργία του IPv6 στις Επικοινωνίες

2.4.1 Εφαρμογή Inter Domain Routing Protocol για Χρήση σε IPv6

Τα πρώτα χρόνια της λειτουργίας του Internet οι routers δεν χρησιμοποιούσαν submasks για να βρουν τη διεύθυνση δικτύου από μια IP, αλλά την καθόριζαν από την κλάση της IP (τα τρία πρώτα bits). Με τον καιρό ο αριθμός των δικτύων με IP κλάσης Β και C αυξήθηκε και ήταν αδύνατο για κάθε router να περιέχει στον πίνακα δρομολόγησης μία διεύθυνση για κάθε δίκτυο στο Internet. Το CIDR (ή superneting) είναι μια τεχνική σύμφωνα με την οποία ο router δεν γνωρίζει μεμονωμένες διευθύνσεις δικτύων αλλά μια περιοχή (ένα εύρος διευθύνσεων δικτύων). Π.χ. έστω 4 δίκτυα κλάσης C με IP διευθύνσεις 147.102.28.X, 147.102.29.X, 147.102.30.X, 147.102.31.X.[56]

Η διεύθυνση δικτύου έχει 24 bit μήκος. Το 3ο byte για κάθε διεύθυνση είναι 00011100, 00011101, 00011110, 00011111. Από το byte αυτό τα 6 πρώτα bit είναι σταθερά. Συνεπώς ο Router αρκεί αντί να ξέρει 4 IP αρκεί να ξέρει μόνο μία IP όπου το μήκος διεύθυνσης δικτύου είναι 22 bits αντί για 24.

---

[56] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

Το CIDR χρησιμοποιεί τον συμβολισμό 14.102.28.0/22 για μια IP που το /22 δηλώνει το μήκος της διεύθυνσης δικτύου. Με την τεχνική CIDR δίνεται επίσης η δυνατότητα σε έναν ISP να παραχωρήσει σε κάποιον πελάτη που χρειάζεται περισσότερες από 256 IPs μια ομάδα συνεχόμενων διευθύνσεων IP κλάσης C, αντί να του δώσει μια IP κλάσης B, και με αυτό τον τρόπο γίνεται εξοικονόμηση διευθύνσεων[57].

Στην εποχή του ARPANET υπήρχαν λίγα δίκτυα τα οποία ήταν αρκετά μεγάλα και η IP διεύθυνση των 32 bit χωριζόταν ως εξής: τα 8 πρώτα bit ήταν η διεύθυνση του δικτύου και τα υπόλοιπα 24 bit ήταν οι υπολογιστές του δικτύου. Αυτή η χρήση της IP διεύθυνσης είχε ως αποτέλεσμα να υπάρχουν 256 διαθέσιμες διευθύνσεις δικτύων οι οποίες ήταν εμφανές ότι δεν θα επαρκούσαν από τη στιγμή που τα πρώτα LAN έκαναν την εμφάνισή τους. Ως λύση ανάγκης οι IP διευθύνσεις προσαρμόστηκαν έτσι ώστε να επιτρέπουν την επιλογή από τρία διαφορετικά μεγέθη για την διεύθυνση του δικτύου[58].

Σήμερα χρησιμοποιείται μόνο ένα υποσύνολο ολόκληρου του προτύπου OSI. Θεωρείται ότι ένα μεγάλο μέρος των προδιαγραφών του είναι πάρα πολύ περίπλοκο και ότι η πλήρης ενσωμάτωση και λειτουργία του θα καθυστερήσει πολύ, αν και υπάρχουν πολλοί άνθρωποι που το υποστηρίζουν έντονα. Το Internet Protocol (IP) βρίσκεται στο Network layer του TCP/IP model και, όπως είπαμε, είναι ένα από τα σημαντικότερα πρωτόκολλα του. Ενσωματώνεται σε τεχνολογίες που βρίσκονται στο αμέσως από κάτω του επίπεδο, το Data Link layer, όπως για παράδειγμα το Ethernet. Είναι ένα data-oriented πρωτόκολλο, το οποίο χρησιμοποιείται για να στέλνονται δεδομένα σε μορφή πακέτων μέσα από ένα δίκτυο υπολογιστών. Τα πακέτα είναι μικρές ακολουθίες από bytes που αποτελούνται από την επικεφαλίδα (header) και το κυρίως μέρος. Η επικεφαλίδα περιγράφει τον προορισμό του πακέτου, τον οποίο χρησιμοποιούν τα routers στο Internet για

---

57 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

58 Black Uyless. *IP Routing Protocols: RIP, OSPF, BGP, PNNI and Cisco Routing Protocols*. Prentice Hall, 2000

να κατευθύνουν το πακέτο στον τελικό του προορισμό. Τα κύρια χαρακτηριστικά του Internet Protocol είναι τα εξής :

• Είναι Connectionless πρωτόκολλο - Για να πάνε τα δεδομένα από έναν υπολογιστή σε έναν άλλο δεν χρειάζεται κάποια προηγούμενη επικοινωνία.

• Είναι αναξιόπιστο - Αυτό σημαίνει ότι υλοποιεί τα λεγόμενο best effort delivery. Δεν υπάρχει εγγύηση για τα πακέτα ότι δεν θα χαθούν, αλλοιωθούν ή ότι θα φτάσουν με τη σωστή σειρά. Από πλευράς αξιοπιστίας το μόνο που κάνει το IP είναι να ελέγχει την επικεφαλίδα του πακέτου που θα στείλει ότι είναι error free, με τη χρήση checksum.

Σε περίπτωση συμφόρησης δεδομένων το IP μπορεί να απορρίψει πακέτα ή ακόμα, για λόγους αποδοτικότητας, 2 συνεχόμενα πακέτα να τα στείλει από διαφορετικές διευθύνσεις. Το IPv6 πρωτόκολλο σχεδιαστικά αποτελεί την εξέλιξη του επιτυχημένου IPv4. Η λειτουργία του σημερινού Διαδικτύου (Internet) βασίζεται στο IPv4 το οποίο όμως αδυνατεί πλέον να ικανοποιήσει τις ανάγκες που διαμορφώνονται στο χώρο των δικτύων.

Σε αυτές τις ανάγκες που δημιουργούνται από τις εξελίξεις που μας οδηγούν στο νέο δίκτυο έρχονται να δώσουν λύσεις το IPv6 και το ATM. Το νέο δίκτυο θα αποτελείται από παντός είδους συσκευές όπως ισχυρά υπολογιστικά συστήματα, ασύρματα τηλέφωνα έως και ηλεκτρικές συσκευές που θα επικοινωνούν μεταξύ τους διαμέσου καλωδιακών, δορυφορικών και ασύρματων (με χρήση υπέρυθρων ή εκτεταμένου φάσματος ραδιοφωνικών συχνοτήτων ή packet radio) συνδέσεων[59].

Θα υποστηρίζει νέου είδους εφαρμογές που απαιτούν εγγύηση στη μετάδοση ήχου και εικόνας και θα αντιμετωπίσει με την πολιτική που θα ακολουθήσει τον όλο και αυξανόμενο όγκο πληροφορίας που θα εισέρχεται στο δίκτυο. Οι λύσεις στα ζητήματα λειτουργίας του νέου δικτύου δεν θα

[59] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

έρθουν αποκλειστικά από το ATM ή το IPv6 αλλά μπορεί και τα δύο συγχρόνως να αποτελούν μέρος του νέου δικτύου. Ένα από τα προβλήματα που οι δύο τεχνολογίες δίνουν μεγάλο βάρος είναι το ζήτημα της ασφάλειας των δικτύων (security). Παρατηρήσαμε όμως ότι λύσεις που δίνονται στην ασφάλεια με τη τεχνολογία του σήμερα υιοθετούνται και στις νέες αυτές τεχνολογίες[60].

3. Κεφάλαιο Τρίτο : Εφαρμογή QoS (Quality of Service) στο IPv6

60 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

3.1 Τρόποι Επίτευξης QoS στο IPv6

Το QoS στο IPv6 μπορεί να επιτευχθεί μέσω των πολιτικών ασφάλειας οι οποίες εφαρμόζονται στο συγκεκριμένο σύστημα αλλά και τις τεχνικές παράτασης ζωής και καλύτερης λειτουργίας.[61] . Τα προβλήματα του IPv4 και πριν ξεκινήσει η εφαρμογή του IPv6, θέτουν ένα σαφές και πολύ περιορισμένο όριο ζωής στο πρωτόκολλο, που δεν άφηνε τα χρονικά περιθώρια για την ανάπτυξη μιας ολοκληρωτικής λύσης. Για την επέκταση της βιωσιμότητας του IPv6 σε συνδυασμό με την επίτευξη QoS και του Internet αναπτύχθηκαν μερικές λύσεις ως εξής[62] :

<u>Ιεραρχημένη διευθυνσιοδότηση και Classless Inter Domain Routing</u>

Ο συνδυασμός της ιεραρχημένης διευθυνσιοδότησης και του C.I.D.R. επιτρέπει την απόδοση διευθύνσεων σε κομμάτια ανάλογα με τις απαιτήσεις κάθε δικτύου χωρίς περιττές σπατάλες. Επίσης μειώνεται δραστικά το μέγεθος των πινάκων δρομολόγησης (routing tables) και τους ρυθμούς ανάπτυξης τους, αφού πλέον είναι δυνατό να περιληφθούν σε μία και μόνο διαδρομή (routing entry) πολλά δίκτυα. Ένα παράδειγμα ιεραρχημένης διευθυνσιοδότησης φαίνεται στο σχήμα No.1. Σε αυτό το παράδειγμα παρουσιάζεται μια ιεραρχία βασισμένη στην γεωγραφική θέση των δικτύων. Σε κάθε χώρα έχει αποδοθεί ένα κομμάτι του χώρου διευθύνσεων. Με αυτό το τρόπο είναι εύκολο να συμπεράνουμε για κάποιο δίκτυο χρήσιμες πληροφορίες γνωρίζοντας μόνο την διεύθυνση του.

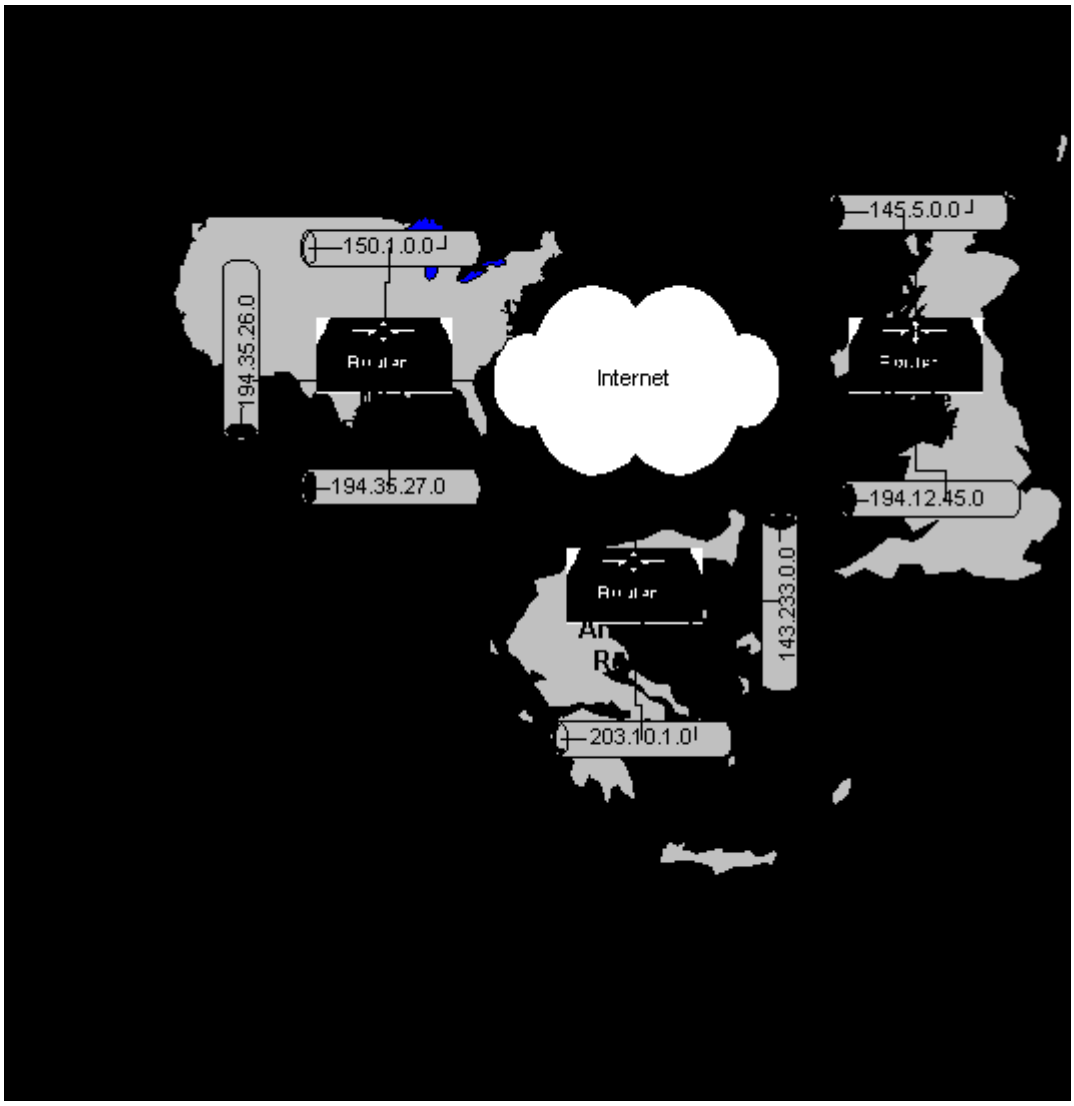
<u>Network Address Translation N.A.T και Application Proxies</u>

---

[61] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

[62] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

Και οι δύο μέθοδοι έχουν σκοπό να δώσουν πρόσβαση στο Internet σε ένα δίκτυο το οποίο χρησιμοποιεί τις ειδικές διευθύνσεις που έχουν παρακρατηθεί για ιδιωτικά δίκτυα. Το δίκτυο αυτό γνωρίζει σαν μοναδική διέξοδο (Gateway) προς το Internet μία μηχανή που χρησιμοποιεί μια από τις μεθόδους (NAT, Application Proxing). Οι βασικότερη διαφορά των δύο μεθόδων είναι ότι το NAT λειτουργεί στο επίπεδο IP (IP Level) ενώ τα Application proxies λειτουργούν στο επίπεδο εφαρμογής (Application Level). Οι τεχνικές NAT και Application proxies είναι ταυτόχρονα αποδοτικές μέθοδοι για την αύξηση της ασφάλειας ενός δικτύου[63].



63 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

Σχήμα Νο. 1 - Ιεραρχική απόδοση διευθύνσεων

Οι τεχνικές για την επίλυση των προβλημάτων διευθυνσιοδότησης που αναφέρθηκαν προηγουμένως και χρησιμοποιούνται στο σημερινό Internet δεν μπορούν να δώσουν μακροχρόνια λύση στο πρόβλημα για τρεις βασικούς λόγους[64]:

- Το CIDR δεν είναι δυνατό να εφαρμοσθεί στις διευθύνσεις που είχαν είδη αποδοθεί σε δίκτυα πριν την χρησιμοποίηση του, αλλά μόνο σε όσα δίκτυα αποδόθηκαν διευθύνσεις μετά από την εφαρμογή του.
- Ακόμα και με την χρήση του CIDR ο χώρος διευθυνσιοδότησης του IPv4 εξακολουθεί να μην επαρκεί.
- Η λύσεις των N.A.T. και Proxies δεν παρέχουν πλήρη πρόσβαση στο δίκτυο. Οι περιορισμοί αυτοί καθιστούν το N.A.T. και τα Proxies μη εφικτές λύσεις σε κάποιες περιπτώσεις.

3.2 Δυσκολίες Εφαρμογής QoS στο IPv6

Οι περισσότερες δυσκολίες επίτευξης QoS στο IPv6, αναφέρονται στο θέμα της ασφάλειας και των συγκεκριμένων βημάτων που θα πρέπει να εφαρμοσθούν σχετικά και με σκοπό την καλύτερη λειτουργία του συστήματος αλλά και θα ενισχύσουν την εμπιστοσύνη από μέρους των πελατών για χρήση του συγκεκριμένου συστήματος. 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[65]:

---

64 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

65 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

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.

3.2.1 Μηχανισμοί Ασφάλειας του IPv6 που Ενισχύουν το QoS

Το IPv6 χρησιμοποιεί δύο βασικούς μηχανισμούς για να παρέχει τις υπηρεσίες ασφάλειας που αναφέρθηκαν στην προηγούμενη παράγραφο. Οι μηχανισμοί αυτοί είναι[66] :

- IP Authentication Header
- IP Encapsulating Security Payload

Οι δύο αυτοί μηχανισμοί βασίζονται κυρίως σε εξωτερικούς μηχανισμούς κρυπτογράφησης για να παρέχουν ασφάλεια. Για αυτό το λόγο κρίνεται σκόπιμο σε αυτό το σημείο να γίνει μια σύντομη αναφορά στο θέμα της κρυπτογράφησης. Να σημειώσουμε ότι η κρυπτογράφηση χρησιμοποιεί κάποια κλειδιά η διαχείριση των οποίων είναι ένα πολύ σημαντικό θέμα το οποίο όμως δεν καλύπτεται σε αυτό το βιβλίο. 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.

3.2.2 Κρυπτογράφηση και QoS στο IPv6

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[67].

Για να γίνει η κρυπτογράφηση απαιτείται ένας μηχανισμός κρυπτογράφησης ο οποίος είναι ένα πρόγραμμα υπολογιστή το οποίο

---

66 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

67 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

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 της 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 κρυποτγράφησης / 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 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.

3.2.3 Ψηφιακές Υπογραφές

Εκτός από την κρυπτογράφηση των πληροφοριών, η κρυπτογραφία δίνει την δυνατότητα της ψηφιακής υπογραφής με την οποία είναι δυνατές οι εξής λειτουργίες[68] :

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

Οι συναρτήσεις που χρησιμοποιούνται για την ψηφιακή 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.

3.2.4 IP Authentication Header

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

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

---

[68] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

- Απόδειξη αποστολής δεδομένων από τον αποστολέα (Non-repudiation).

Ο μηχανισμός αυτός στο IPv6 προστίθεται σαν μια έξτρα επικεφαλίδα όπως φαίνεται και στο Σχήμα No.2. 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.

IPv6 Header	Hop-by-Hop / Routing	Authentication Header	Άλλοι Headers	Πρωτόκολλο άνω επιπέδου (TCP/UDP)

Σχήμα No. 2 - Μορφή IP πακέτου με Authentication Header

3.2.5 IP Encapsulating security Payload (ESP)

Ο μηχανισμός του IP Encapsulating security Payload μπορεί να παρέχει τις εξής δυνατότητες ασφάλειας[69]:

- 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 Encapsulating security Payload φαίνεται στο Σχήμα No.3

[69] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

Σχήμα No. 3 - Μορφή IP πακέτου με IP Encapsulating security Payload

Ο μηχανισμός του ESP μπορεί να χρησιμοποιηθεί με δύο τρόπους[70]:

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

3.2.6 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[71] :

---

70 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

71 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

- 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 μιας 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[72].

3.3 Πλεονεκτήματα που Προσφέρει η Εφαρμογή QoS στο IPv6

Τα πλεονεκτήματα που προσφέρονται στην εφαρμογή QoS στο IPv6, αναφέρονται κυρίως στην αύξηση απόδοσης του IPv6 καθώς και στην εγγυημένη απόδοση του, μέσω δύο κατευθύνσεων, ως εξής[73].

- ***Πρόβλεψη για Εγγυημένη ποιότητα εξυπηρέτησης από το δίκτυο Q.o.S.***

Η απαίτηση για Q.o.S. είναι μια απαίτηση που εμφανίζεται κυρίως λόγο των νέων δικτυακών εφαρμογών πολυμέσων. Οι εφαρμογές αυτές στις περισσότερες περιπτώσεις περιλαμβάνουν εικόνα, ήχο, και αλληλεπίδραση ανάμεσα στους συμμετέχοντες, γεγονός που απαιτεί επικοινωνία πραγματικού χρόνου (real time). Η ιδιαιτερότητα αυτή μεταφράζεται σε σχέση με το δίκτυο σε δύο πράγματα:

- Ο όγκος των πληροφοριών είναι μεγάλος και στο μεγαλύτερο μέρος τους έχουν ένα σταθερό ρυθμό bit κατά την διάρκεια της μετάδοσης (Constant Bit Rate -CBR).
- Η ποιότητα του αποτελέσματος επηρεάζεται σε πολύ μεγάλο βαθμό από την καθυστέρηση που κατά περίπτωση μπορεί να υπάρχει στην μεταφορά την πληροφορίας.

Αυτά τα δύο βασικά σημεία κάνουν πολύ δύσκολη την χρησιμοποίηση των εφαρμογών αυτών στο σημερινό Internet με το IPv4 το οποίο δεν είχε σχεδιαστεί για μεταφορά πληροφορίας πραγματικού χρόνου. Τέτοιου τύπου εφαρμογές είναι επιθυμητό να χρησιμοποιούν κανάλια με μικρή καθυστέρηση

---

72 Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

73 Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

και εάν είναι δυνατό μεγάλου bandwidth, αλλά κανάλια που εισάγουν μεγάλη καθυστέρηση είναι άσχημη επιλογή ανεξάρτητος του bandwidth που παρέχουν. Στο IPv6 αναπτύσσονται ειδικοί μηχανισμοί για να εξυπηρετήσουν την νέα αυτή ανάγκη. Η ανάπτυξη όμως της δυνατότητας Q.o.S. είναι αυτή τη στιγμή η πιο πειραματική από όλες τις άλλες δυνατότητες που παρέχει το Ipv6[74].

- ***Βελτιωμένη εσωτερική σχεδίαση του πρωτοκόλλου.***

Η επιλογή για σχεδίαση του πρωτοκόλλου IPv6 από την αρχή και όχι απλά εξελίσσοντας τον κώδικα που είδη είναι γραμμένος για το IPv4 παρέχει πλεονεκτήματα και στον τομέα της απόδοσης του IPv6.

- ***Εγγυημένη Ποιότητα Εξυπηρέτησης από το Δίκτυο - Q.o.S.***

Το IPv6 λαμβάνει υπόψη τις νέες απαιτήσεις των σύγχρονων εφαρμογών και περιλαμβάνει ειδικές τεχνικές για την επίτευξη της ποιότητας εξυπηρέτησης που επιθυμεί η εκάστοτε εφαρμογή. Το θεμέλιο του Q.o.S. μπαίνει στην επικεφαλίδα του IPv6 με τα δύο πεδία Priority και Flow Label που φαίνονται στο σχήμα 1.

- ***Επίπεδα Προτεραιότητας (Priority Level)***

Το IPv6 χωρίζει την πληροφορία την οποία προωθεί σε κατηγορίες με αντίστοιχες απαιτήσεις για ποιότητα εξυπηρέτησης - προτεραιότητα (Priority). Τα επίπεδα προτεραιότητας χωρίζονται σε δύο βασικές κατηγορίες:

- Πληροφορίες που έχουν μηχανισμούς αποτροπής κορεσμού του δικτύου (congestion-controlled traffic) και περιγράφονται στον πίνακα που ακολουθεί.

[74] Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/

Προτεραιότητα	Τύπος πληροφορίας
0	μη χαρακτηρισμένη πληροφορία
1	"filler" traffic (π.χ., netnews)
2	Μη παρακολουθούμενη μεταφορά μεγάλης ποσότητας δεδομένων (π.χ. email)
3	μελλοντική χρήση
4	Παρακολουθούμενη μεταφορά μεγάλης ποσότητας δεδομένων (π.χ.., FTP, NFS)
5	μελλοντική χρήση
6	Αλληλεπιδραστική πληροφορία (π.χ telnet, X Windows)
7	Πληροφορία ελέγχου του Internet (π.χ. πρωτόκολλα δρομολόγησης, SNMP)

- *Πληροφορίες που δεν έχουν μηχανισμούς αποτροπής κορεσμού του δικτύου (non-congestion-controlled traffic).*

Αυτού του είδους η πληροφορία έχει αριθμούς προτεραιότητας από 8-15. Η μικρότερη προτεραιότητα θα πρέπει να χρησιμοποιείται για πληροφορία που η απώλεια της θα επηρεάσει λιγότερο σε περίπτωση κορεσμού του δικτύου (π.χ. υψηλής ποιότητας εικόνα). Αντίστοιχα η μεγαλύτερη θα πρέπει να χρησιμοποιείται για πιο απαραίτητη πληροφορία όπως χαμηλής ποιότητας ήχος.

3.3.1 Ροές Πληροφοριών (Flows) για Επίτευξη QoS στο IPv6

Το IPv6 εισάγει την έννοια της ροής πληροφορίας, θεωρώντας ότι τα πακέτα της πληροφορίας ρέουν μέσα από ένα ιδεατό κανάλι. Οι δρομολογητές που αποτελούν αυτό το ιδεατό κανάλι έχουν φροντίσει με κάποιο μηχανισμό να παρακρατήσουν τους απαραίτητους πόρους για την εξυπηρέτηση της ροής. Επιπλέον οι απαραίτητοι υπολογισμοί για την προώθηση κάθε πακέτου που ανήκει σε μια ροή γίνονται μόνο για το πρώτο πακέτο της πληροφορίας και εφαρμόζονται σε κάθε πακέτο της ίδιας ροής , γλιτώνοντας έτσι υπολογιστική ισχύ στον δρομολογητή και μειώνοντας σημαντικά την καθυστέρηση δρομολόγησης του πακέτου.
Η αναγνώριση της ροής στην οποία ανήκει το πακέτο επιτυγχάνεται με το πεδίο Flow Label της επικεφαλίδας του IPv6[75].

3.3.2 Δημιουργία και Κατάργηση Ροών με το Πρωτόκολλο Παρακράτησης Πόρων (Resource Reservation Protocol - RSVP)

Το RSVP είναι ένα βοηθητικό πρωτόκολλο επιπέδου μεταφοράς (Transport Level)

<table>
<tr><td colspan="2">Επίπεδο Μεταφοράς (TCP/UDP)</td></tr>
<tr><td></td><td>RSVP</td></tr>
<tr><td colspan="2">Internet επίπεδο (IP)</td></tr>
<tr><td colspan="2">Επίπεδο Σύνδεσης (Link Level)</td></tr>
<tr><td colspan="2">Φυσικό Επίπεδο (Physical Level)</td></tr>
</table>

Σχήμα Νο. 4 - Επίπεδο λειτουργίας του RSVP

Το RSVP χρησιμοποιείται από μια μηχανή για να πραγματοποιήσει την αίτηση για ένα συγκεκριμένο επίπεδο εξυπηρέτησης (Q.o.S.) από το δίκτυο, εκ μέρους μιας εφαρμογής και από τους δρομολογητές για να μοιράσουν την αίτηση για Q.o.S. κατά μήκος όλης της διαδρομής που θα ακολουθήσει μια

75

ροή και να παρακρατηθούν οι αντίστοιχοι πόροι (εάν είναι δυνατό) σε κάθε δρομολογητή.

Η διαδικασία της παρακράτησης πόρων είναι δυνατό να επιτευχθεί για συνδέσεις είτε unicast, είτε multicast εφαρμογών. Για να επιτευχθεί καλύτερη απόδοση ειδικά σε εφαρμογές multicasting το RSVP αφήνει τον παραλήπτη να δημιουργήσει την αίτηση για Q.o.S. Η κατάσταση των ροών ανανεώνεται περιοδικά επιτρέποντας την ανανέωση των στοιχείων μιας ροής, γεγονός που είναι ιδιαίτερα χρήσιμο σε εφαρμογές multicasting, όπου μηχανές εισάγονται και αφαιρούνται από τις ομάδες multicasting δυναμικά. Ένα σημαντικό χαρακτηριστικό του RSVP είναι η δημιουργία ροών μιας κατεύθυνσης ανεξάρτητα εάν η επικοινωνία είναι αμφίδρομη, πράγμα που σημαίνει ότι για μια unicast εφαρμογή αμφίδρομης επικοινωνίας θα πραγματοποιηθούν δύο αιτήσεις μία από κάθε μέλος της επικοινωνίας.

Στο Σχήμα No. 4, παρουσιάζεται η λειτουργία του RSVP στην περίπτωση επικοινωνίας 2 μηχανών (hosts) διάμεσο ενός ή περισσότερων δρομολογητών. Κάθε μηχανή και δρομολογητής που παρέχει την δυνατότητα Q.o.S. πρέπει οπωσδήποτε να περιέχει στο λειτουργικό του, τις διεργασίες που παρουσιάζονται στον Πίνακα No.1

Διεργασία	*Λειτουργία*
RSVP	*Υλοποίηση του πρωτοκόλλου RSVP*
Admission Control	*Ελέγχει εάν η μηχανή έχει την δυνατότητα να παρέχει το ζητούμενο Q.o.S.*
Policy Control	*Ελέγχει εάν επιτρέπεται στον χρήστη το ζητούμενο Q.o.S.*
Classifier	*Καθορίζει το Q.o.S και την διαδρομή κάθε εισερχόμενου πακέτου.*
Packet Scheduler	*Λαμβάνει αποφάσεις για την προώθηση των εξερχόμενων πακέτων από ένα interface, έτσι ώστε να επιτευχθεί το επιθυμητό Q.o.S.*

Routing	*Παρέχει τις πληροφορίες με τις οποίες θα αποφασισθεί το μονοπάτι που θα ακολουθήσει το πακέτο, ώστε να επιτευχθεί το ζητούμενο Q.o.S.*

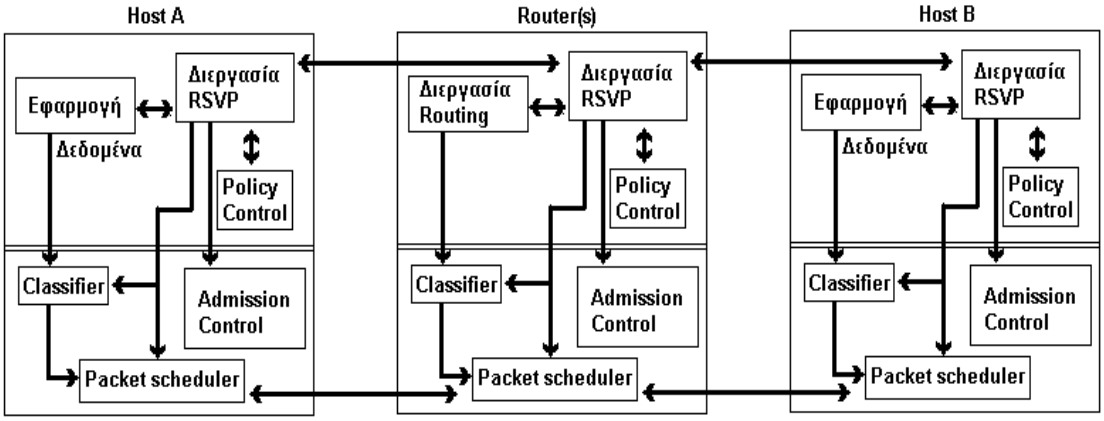
Πίνακας Νο.1 - Λογικές μονάδες που απαιτούνται για την παροχή Q.o.S.

Για να επιτευχθεί η επικοινωνία με την απαιτούμενη ποιότητα εξυπηρέτησης από το δίκτυο ακολουθούνται τα παρακάτω βήματα[76]:

- Η εφαρμογή στο Host A ζητάει το απαιτούμενο Q.o.S. από την διεργασία RSVP του Host B.
- Η διεργασία RSVP ζητάει από το Admission Control να γίνει έλεγχος για την διαθεσιμότητα των απαιτούμενων πόρων.
- Η διεργασία RSVP ζητάει από το Policy control να γίνει έλεγχος εάν ο χρήστης έχει άδεια να ζητήσει το συγκεκριμένο Q.o.S.
- Εάν τα βήματα 2 και 3 είναι επιτυχή τότε γίνεται η ρύθμιση του packet scheduler και του classifier για την δημιουργία της ροής. Σε αντίθετη περίπτωση επιστρέφεται ένα μήνυμα λάθους στην αρχική εφαρμογή που ζήτησε το Q.o.S. και διαγράφονται οι πληροφορίες σχετικά με την συγκεκριμένη ροή.
- Μετά την δημιουργία της ροής στην μηχανή, η διεργασία του RSVP επικοινωνεί με την επόμενη μηχανή στην οποία θα σταλεί το πακέτο (δρομολογητής ή τελικός παραλήπτης) και ζητάει και σε αυτή την δημιουργία της αντίστοιχης ροής.
- Τα βήματα 2 έως 5 επαναλαμβάνονται μέχρι να δημιουργηθεί η ροή σε όλες τις μηχανές από τις οποίες θα διέλθει το πακέτο και στην μηχανή παραλήπτη.
- Τα βήματα 1 έως 6 επαναλαμβάνονται προς την αντίθετη φορά δηλαδή από το Host B στο Host A.

[76] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

Με την ολοκλήρωση της διαδικασίας των επτά (7) βημάτων, το δίκτυο είναι έτοιμο να παρέχει το απαιτούμενο επίπεδο εξυπηρέτησης στις εφαρμογές και η επικοινωνία μπορεί να αρχίσει. Αξίζει να σημειωθεί πως η διαδικασία παρακράτησης πόρων είναι μια διαδικασία που εκτελείται μόνο μια φορά σε κάθε δημιουργία ροής και για αυτό δεν υπάρχει κάποιος μηχανισμός που να εγγυάται την επιτυχία της. Τέλος πρέπει να διευκρινίσουμε ότι η διαδικασία ελέγχου δεν είναι μέρος του RSVP, το οποίο συμπεριφέρεται απλά σαν ένας πράκτορας που μεταφέρει πληροφορίες χωρίς συγκεκριμένο νόημα για τον ίδιο.



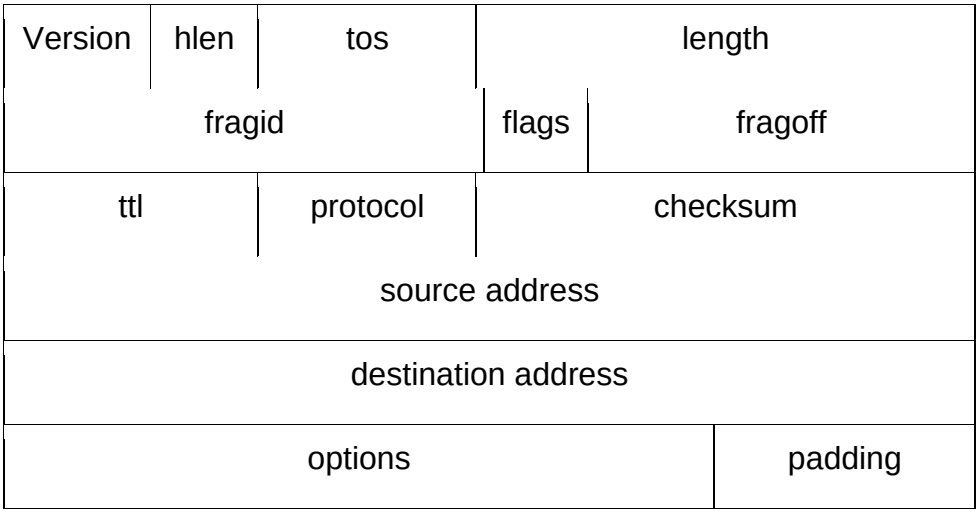
Σχήμα No. 6 - Λειτουργία RSVP

3.4 Σύγκριση Μορφών Επικεφαλίδων IPv4 και IPv6 για Καλύτερη Εφαρμογή QoS στο IPV6 στο Μέλλον

Η εμπειρία που έχει αποκτηθεί από την πολύχρονη χρήση και βελτίωση του IPv4, οδήγησαν στην απόρριψη χαρακτηριστικών που αποδείχτηκαν μη αποδοτικά ή δεν χρειάζονταν πλέον. Αυτές οι αλλαγές φαίνονται καθαρά στην καινούργια μορφή της επικεφαλίδας του IPv6, η οποία φαίνεται στο σχήμα 7:

Version	priority	Flow Label	
Payload Length		Next Header	Hop Limit

Σχήμα No. 7 - Μορφή Επικεφαλίδας IPv6



Σχήμα No. 8 - Μορφή Επικεφαλίδας IPv4

Πεδίο Επικεφαλίδας	Μήκος (bit)	Σύντομη περιγραφή
Version	4	Αριθμός έκδοσης του IP (6)
Priority	4	Προτεραιότητα πακέτου
Flow Label	24	Αναγνωριστικό ροής
Payload Length	16	Μήκος της μεταφερόμενης πληροφορίας που ακολουθεί την επικεφαλίδα.

Next Header	8	Ο τύπος της επικεφαλίδας που ακολουθεί μετά την επικεφαλίδα του IPv6
Hop Limit	8	Μέγιστος αριθμός δρομολογητών που επιτρέπεται να περάσει το πακέτο πριν απορριφθεί.
Source Address	128	Διεύθυνση αποστολέα
Destination Address	128	Διεύθυνση παραλήπτη.

Πίνακας Νο. 2 - Πεδία της επικεφαλίδας του IPv6

Συγκρίνοντας την επικεφαλίδα του IPv6 με την επικεφαλίδα του IPv4 στο σχήμα Νο.7 και Νο.8, αμέσως παρατηρούμε την απλοποίηση που έχει γίνει στην μορφή της επικεφαλίδας κρατώντας μόνο τις άκρως απαραίτητες πληροφορίες. Σαν αποτέλεσμα έχουμε διπλάσιο μήκος σε bit της επικεφαλίδας του IPv6 σε σχέση με το IPv4 παρόλο που το μέγεθος των διευθύνσεων έχει τετραπλασιαστεί. Οι επιλογές πλέον προστίθενται σαν επιπλέον επικεφαλίδες που ακολουθούν την επικεφαλίδα του IPv6 όταν αυτές χρειάζονται. Οι σχεδιαστές για να μειώσουν τον χρόνο που ένας δρομολογητής χρειάζεται για να επεξεργαστεί ένα πακέτο φρόντισαν ώστε[77] :

- Οι δρομολογητές να χρειάζεται να επεξεργαστούν το πολύ μια επιπλέον επιλογή ενώ οι υπόλοιπες να ελέγχονται μόνο από τον παραλήπτη του πακέτου.
- Το πακέτο πρέπει να ξεκινάει από τον αποστολέα με κατάλληλο μέγεθος ώστε να είναι δυνατή η μετάδοση του, από όλες τις τεχνολογίες δικτύου που πρόκειται να συναντήσει στην πορεία του, χρησιμοποιώντας την τεχνική αναζήτησης της μέγιστης δυνατής μονάδας πληροφορίας (Path MTU Discovery).

[77] Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998

- Τέλος η δυνατότητα μεγάλων IP πακέτων (Jumbograms) που επιτρέπει το μεγέθους του IP πακέτου να ξεπεράσει το όριο των 65Kb που θέτει το IPv4 επιτρέπει την καλύτερη εκμετάλλευση των νέων τεχνολογιών δικτύων υψηλών ταχυτήτων όπως ATM, GigaBit Ethernet, κ.α.

4. Κεφάλαιο 4^{ο} : Επίλογος

Στην παρούσα εργασία, παρατέθηκε και αναλύθηκε η λειτουργία των ασυρμάτων δικτύων στις μέρες μας σε συνδυασμό με την εφαρμογή του IPv6 και το πώς μπορεί να εφαρμοσθεί η ποιότητα υπηρεσιών στην εφαρμογή της συγκεκριμένης τεχνολογίας. Θα πρέπει να σημειωθεί πως η ασύρματη

δικτύωση 802.11 και η οποία ονομάζεται επίσης και "Wi-Fi", αποτελεί ένα σύνολο πρωτοκόλλων τα οποία χρησιμοποιούνται ευρέως σε μικρά τοπικά δίκτυα. Ένα άλλο πρωτόκολλο είναι εκείνο το οποίο ονομάζεται Bluetooth, επιτρέπει στις συσκευές να επικοινωνούν ασύρματα αλλά είναι χρήσιμο μόνο για επικοινωνία πολύ μικρής εμβέλειας και γενικότερα δεν χρησιμοποιείται για οικιακή δικτύωση. Το Bluetooth μπορεί επίσης να είναι χρήσιμο για τη δικτύωση προσωπικών συσκευών μέσα στα όρια μιας μικρής περιοχής. Ένα τέτοιο δίκτυο συχνά καλείται δίκτυο προσωπικής περιοχής ή διαφορετικά γνωστό ως Personal Area Network – PAN.

Αντίστοιχα, πρέπει να σημειωθεί πως αποτελεί γεγονός πως η Κοινωνία της Πληροφορίας στις μέρες μας θεωρείται ως μια μοναδική πρόκληση και ευκαιρία με σκοπό την ανάπτυξη της περιοχής των Βαλκανίων και της Ευρώπης. Προς την κατεύθυνση αυτή απαιτείται η σύγκλιση των πολιτικών αρχηγών, ο εκσυγχρονισμός των διαφόρων υποδομών και η ανάληψη κοινών δράσεων και έργων από μέρους των υπευθύνων. Σε αυτό το πλαίσιο, ο ρόλος της χώρας της Ελλάδας είναι ιδιαίτερα σημαντικός, δεδομένου ότι είναι η μόνη χώρα των Βαλκανίων που ανήκει στην Ευρωπαϊκή Ένωση, ενώ οι υπόλοιποι ελληνικοί φορείς διαθέτουν την εμπειρία και της τεχνογνωσία στους τομείς της πληροφορικής και των τηλεπικοινωνιών με χρήση ασυρμάτων δικτύων.

Το ***Internet Protocol version 6 (IPv6)*** αποτελεί τη νεώτερη έκδοση του πρωτοκόλλου IPv4, το οποίο σταδιακά θα αντικατασταθεί στο μέλλον. Η σχεδίαση του IPv6 στηρίχθηκε στην εκτεταμένη εμπειρία που αποκτήθηκε με το πέρασμα του χρόνου από τη λειτουργία και τη ραγδαία εξάπλωση του Διαδικτύου. Το IPv6 περιλαμβάνει σειρά λειτουργικών βελτιώσεων και απλοποιήσεων σε σχέση με το IPv4. Μία βασική βελτίωση του IPv6 είναι το μεγαλύτερο εύρος διευθύνσεων που θα επιτρέψει την απρόσκοπτη επέκταση του Διαδικτύου με νέες συσκευές, όπως έξυπνα τηλέφωνα (smartphones), αισθητήρες (sensors), κλπ. Το IPv6 θα συμβάλει επίσης στην ασφάλεια των ψηφιακών επικοινωνιών και στην κινητικότητα (mobility) των χρηστών.

Το IPv6 ήδη υποστηρίζεται από ένα ευρύ φάσμα σύγχρονων λειτουργικών συστημάτων για προσωπικούς υπολογιστές, φορητές συσκευές

και συσκευές δικτύου, όπως είναι τα Microsoft Windows XP SP2/VISTA/ Server 2008, Apple Mac OS X, Linux, Symbian OS 7 και Windows Mobile. Επίσης, τμήματα του κορμού του Διαδικτύου υποστηρίζουν το νέο πρωτόκολλο. Παρόλα αυτά, η χρήση του δεν έχει ακόμη διαδοθεί ανάμεσα στους παρόχους υπηρεσιών πρόσβασης στο Διαδίκτυο, στις επιχειρήσεις. 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

Βιβλιογραφία

- Adams, J., 1998, "*The next world war*", Simon and Schuster
- BloomBecker, B., 1990, "*Spectacular Computer Crimes*", Dow Jones – Irwin
- Ransom, A. W., 1994, "*Who Owns Information*", Basic Books
- Cavoukian, A., Tapscott, D., 1997, "*Who Knows",* McGraw-Hill
- Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley
- Diffie, W., Landau, S., 1998, "*Beyond Calculation*", The MIT Press
- Hager, N., 1996, "*Secret Power*", Craig Cotton Publishing, New Zealand, 1996
- Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA
- McCarthy, L., 1997, "*Intranet Security*", Prentice Hall
- Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications
- Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall
- Rosenoer, J., 1997, "*CyberLaw"*, Springer – Verlag
- Timpton, H., F., Ruthberg, Z., G., 2003, "*Handbook of Information Security Management*", Acerbic
- Saunders et all, (2005), "*Specified ways for research and analysis of data*", Prentice Hall
- Sekaran U., (1992), "*Research Methods for Business, A Skill Building Approach*". New York: John Wiles and Sons Inc.
- Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall
- Slade, P., 1994, "*Guide to Computer Viruses*", Springer – Verlag
- Schweizer, P., 1993, "*Friendly Spies*", The Atlantic Monthly Press
- Sterling, B., 1992, "*The Hacker Crackdown*", Bantam
- Taylor, A., 1999, "*The Hackers*", Routledge
- Wayner, P., 1996, "*Disappearing Cryptography*", Academic Press

- Zikmund W.G., (2000), "*Business Research Methods*". London: Harcourt college publishers.
- Καλλίνικος Χρ., Κουτσούρης Χαρ., (1998), *Μια Πειραματική Μελέτη των Νέων Δικτυακών Τεχνολογιών, Το IPv6 και η Διάσταση της Ασφάλειας*, Δημοκρίτειο Πανεπιστήμιο, Έκδοση Φεβρουάριος 1998
- Σταμάτης, Κ., Ν., 2002, «*Η Αβέβαιη Κοινωνία της Γνώσης*», Εκδόσεις Σαββάλας
- Εθνικό Κέντρο Τεκμηρίωσης: http://www.ekt.gr
- Γενική Διεύθυνση "*Κοινωνία της Πληροφορίας*" της Ευρωπαϊκής Επιτροπής: http://europa.eu.int/comm/dgs/information_society/index_en.htm
- www.eseeurope.org
- Fast Handovers for Mobile IPv6, RFC 4068, ftp://ftp.rfc-editor.org/in-notes/rfc4068.txt
- Merike Kaeo, "*IPv6 Security Technology Paper*", North American IPv6 Task Force (NAv6TF) Technology Report.
- http://www.nav6tf.org/documents/nav6tf.security_report.pdf
- GÉANT project, http://www.geant.net/
- Εθνικό Ίδρυμα Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ), http://www.grnet.gr/