ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ Σ.Τ.Ε.Φ.
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

Μελέτη και Υλοποίηση Πιλοτικού Δικτύου IPv6

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΤΩΝ

ΓΚΕΚΑ ΔΗΜΗΤΡΙΟ
ΠΑΠΑΓΕΩΡΓΙΟΥ ΙΩΑΝΝΗ

Επιβλέπων : ΖΑΧΟΣ ΧΡΙΣΤΟΣ
Εργαστήριο Δικτύων & Δικτυακών Πολυμέσων

ΘΕΣΣΑΛΟΝΙΚΗ
2010

Περίληψη

Εξαιτίας των ανησυχιών για την επικείμενη εξάντληση των διαθέσιμων IP διευθύνσεων του Διαδικτύου και της επιθυμίας να παρασχεθεί πρόσθετη λειτουργικότητα στις σύγχρονες συσκευές, είναι στο στάδιο δημιουργίας μιας βελτιωμένης εκδοχής της τρέχουσας έκδοσης του πρωτοκόλλου δικτύου (Internet Protocol - IP), αποκαλούμενης ως IPv4. Αυτή η νέα έκδοση, αποκαλούμενη ως Πρωτόκολλο Δικτύου Έκδοση 6 (Internet Protocol version 6 - IPv6), επιλύει τα δυσεπίλυτα σχεδιαστικά προβλήματα του IPv4 και είναι προορισμένη να οδηγήσει το Διαδίκτυο στον 21^{ο} αιώνα. Αυτή η πτυχιακή εργασία περιγράφει τα προβλήματα του πρωτοκόλλου IPv4, και περιγράφει πώς διευθετούνται από το IPv6. Σκοπός μας είναι να στηθεί ένα τοπικό πρότυπο δίκτυο εξολοκλήρου με IPv6 ώστε να μελετήσουμε τα πλεονεκτήματα και τα μειονεκτήματα του.

Ακόμα στην πτυχιακή θα μελετηθούν τα DNSv6 ICMPv6 DHCPv6 και Active directory. Στο πρακτικό μέρος πάρθηκαν μετρήσεις από το τοπικό δίκτυο που στήθηκε στο τμήμα ηλεκτρονικής στο Α.Τ.Ε.Ι. Θεσσαλονίκης για να παρατηρηθούν οι διαφορές στην ταχύτητα της απόδοσης των IPv4 και IPv6.

Abstract

Due to recent concerns over the impending depletion of the current pool of Internet addresses and the desire to provide additional functionality for modern devices, an upgrade of the current version of the Internet Protocol (IP), called IPv4, is in the process of standardization. This new version, called IP Version 6 (IPv6), resolves unanticipated IPv4 design issues and is poised to take the Internet into the 21st Century. This thesis describes the problems of ipv4 and show us they way that we can fixed with ipv6. Our goal is to set up a local area network that works only with IPv6 and in this way we will see the advantages and the disadvantages of our new IP(v6).

Plus in this thesis we will study about DNSv6 ICMPv6 DHCPv6 and Active directory.

In the practical part we take the results from the LAN that set up in the university of Thessaloniki at the electronic engineer department and observe the IPv6 versus IPv4.

Περιεχόμενα

Κεφάλαιο 1^{ο} – Σκοπός

1.1 Μελέτη και Υλοποίηση

Σκοπός της πτυχιακής εργασίας είναι η μελέτη ενός τοπικού δικτύου όπου επικοινωνεί μονό με IPv6. Γι' αυτό τον λόγο υλοποιήθηκε ένα πρότυπο δίκτυο εννέα υπολογιστών στο Τμήμα Ηλεκτρονικής του Α.Τ.Ε.Ι Θεσσαλονίκης με σκοπό την μελέτη λειτουργίας του δικτυού, την κατανόηση της δομής του, τα πλεονεκτήματα, τα μειονεκτήματα και γενικά τις καινοτομίες και διαφορές που έχει έναντι του IPv4.

1.2 Εύρεση Προβλημάτων – Λύσεις

Προβλήματα με το IPv6:

- Το βασικό πρόβλημα που αντιμετωπίσαμε ήταν ότι ενώ ¨βγαίναμε¨ στο internet με IPv6 τα πακέτα επέστρεφαν με IPv4. Αυτό γίνετε λόγο του ότι χρησιμοποιούμε την είδη υπάρχουσα εγκατάσταση της IPv4(dual stack) και ο DNS είναι σχεδιασμένος να μας απαντάει κατά αυτό τον τρόπο.

- Ένα ακόμα πρόβλημα της IPv6 ήταν η συμβατότητα με τα Windows XP. Όταν απεγκαταστήσαμε την IPv4 δεν μπορούσαμε να κάνουμε Ping σε κανέναν υπολογιστή ώστε να μπορέσουμε να πάρουμε μετρήσεις από το πρόγραμμα έτσι εγκαταστήσαμε τα Windows Server 2008,στα οποία το πρόβλημα λύθηκε.

1.3 Απόδοση

Όσο αφόρα την απόδοση του IPv4 σε σύγκριση με το IPv6 παρατηρήσαμε ότι η IPv4 υπερτερεί κατά έναν μικρό βαθμό σε ταχύτητα έναντι της IPv6.Αιτία του χαρακτηριστικού αυτού είναι η μεγαλύτερη επεξεργαστική ισχύς που χρειάζεται η νέα έκδοση λόγο του μεγαλύτερου όγκου δεδομένων .Όμως τα πλεονεκτήματα της IPv6 είναι τόσα πολλά που αυτό δεν θεωρείτε και τόσο σημαντικός παράγοντας(βλέπε κεφάλαιο 6^{ο}).

1.4 Πρότυπα και Πιλοτικά Δίκτυα

- Πρότυπα δίκτυα είναι αυτά που στήνονται ώστε να δοκιμαστεί η λειτουργία τους και να γίνει ο κατάλληλος έλεγχος της λειτουργίας του. Πρότυπο δίκτυο θεωρείται και αυτό που στήθηκε στο εργαστήριο για την υλοποίηση της εργασίας μας.
- Πιλοτικά είναι τα δίκτυα τα οποία είναι πλέον έτοιμα να βγουν στο internet και να λειτουργήσουν κανονικά.

Κεφάλαιο 2^{ο} - Γιατί IPv6;

2.1 Εισαγωγή

Το πρωτόκολλο που χρησιμοποιείται σήμερα ευρύτερα από κάθε άλλο είναι το IPv4. Αυτό μας παρέχει την δυνατότητα να έχουμε στο Internet περίπου 4 δισεκατομμύρια διαφορετικές διευθύνσεις. Ο αριθμός ακούγεται σχετικά μεγάλος, αλλά πρέπει να λάβουμε υπόψη κάποια γεγονότα.

- Το Internet αποκτά ολοένα και περισσότερους χρήστες, με πολυπληθείς χώρες όπως η Κίνα να υιοθετούν ολοένα και ταχύτερα την πρόσβασή τους σε αυτό.
- Οι IP enabled συσκευές που πωλούνται διεθνώς ολοένα και αυξάνονται. IP TVs, Internet Radios και network controlled ηλεκτρικές συσκευές γίνονται όλο και πιο δημοφιλείς.
- Πολλοί οικιακοί χρήστες και computer enthusiasts πλέον τρέχουν ιδιωτικούς servers για να παρέχουν διάφορες υπηρεσίες στον κοινωνικό τους περίγυρο και όχι μόνο.
- Τα κινητά τηλέφωνα και τα PDAs μετατρέπονται από μεμονωμένες συσκευές σε εργαλεία πρόσβασης σε μία σειρά υπηρεσιών που παρέχονται μέσω Internet.
- Η αυτοκινητοβιομηχανία θέλει να αποδίδει σε κάθε όχημα που κατασκευάζεται μία μοναδική διεύθυνση μέσω της οποίας θα μπορεί να ελέγχει την κατάσταση του οχήματος, καθώς και να παρέχει online υπηρεσίες όπως οι αναβάθμιση firmware και configurations στα επιμέρους τμήματα που το απαρτίζουν.

Με τα παραπάνω, γίνεται κατανοητό ότι οι διευθύνσεις που μας παρέχει το IPv4 πολύ σύντομα θα πληρωθούν και από ένα σημείο και μετά δεν θα υπάρχουν άλλες διαθέσιμες. Προγενέστερες έρευνες τοποθετούν την χρονολογία όπου το πρόβλημα θα εκδηλωθεί όχι νωρίτερα από το 2013,πιο πρόσφατες στα τέλη του 2012 ενώ μερικές προβλέπουν εκδήλωση του προβλήματος εντός του 2011! Όπως και να έχει, το πρόβλημα είναι υπαρκτό και επιβάλλεται η εύρεση μιας λύσης.

Το IPv6 δημιουργήθηκε με στόχο να επιλυθεί αυτό ακριβώς το πρόβλημα. Όπως ήταν αναμενόμενο, παρότι ο μοναδικός λόγος που ξεκίνησε η ανάπτυξή του ήταν ο παραπάνω, στην πορεία αποφασίστηκε ότι ήταν μια καλή ευκαιρία να γίνουν κάποιες βελτιώσεις σε επιμέρους ζητήματα όπου το IPv4 έχει επιδείξει κάποιες αδυναμίες.

2.2 Η Ιστορία του Internet Protocol

Το πρωτόκολλο Internet (Internet Protocol—IP) μπόρεσε να συνδέσει εκατομμύρια υπολογιστών και να φέρει μία καινούργια πραγματικότητα στην παροχή πρόσβασης στην πληροφορία. Το IP αναπτύχθηκε πριν είκοσι χρόνια σαν το πρωτόκολλο του network επιπέδου της αρχιτεκτονικής του Διαδικτύου (Internet) και μαζί με το πρωτόκολλο του transport επιπέδου TCP (Transmission Control Protocol) δημιούργησαν την οικογένεια πρωτοκόλλων TCP/IP.

Στην αρχή το TCP/IP χρησιμοποιήθηκε για την διασύνδεση των διαφορετικών υπολογιστικών συστημάτων που χρησιμοποιούσε η κυβέρνηση των Η.Π.Α αλλά λόγω της εξαιρετικής του δύναμης εξαπλώθηκε παγκοσμίως νικώντας τις άλλες δικτυακές κατευθύνσεις και τεχνολογίες όπως: OSI, SNA, DECnet, NETware, κ.α. Το IP λοιπόν έγινε η βάση της δημιουργίας πάρα πολλών client-server ή peer-to-peer εφαρμογών και εκμεταλλεύεται έτσι την δυνατότητα της δικτυακής σύνδεσης. Το σημερινό Internet αποτελεί εξέλιξη του **ARPANET**, ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του 60 στις ΗΠΑ.

Δεκαετία '60

Στα πανεπιστήμια των ΗΠΑ οι ερευνητές ξεκινούν να πειραματίζονται με τη διασύνδεση απομακρυσμένων υπολογιστών μεταξύ τους. Το δίκτυο **ARPANET** γεννιέται το 1969 με πόρους του προγράμματος ARPA (Advanced Research Project Agency) του Υπουργείου Άμυνας, με

σκοπό να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς και να αποτελέσει ένα πείραμα για τη μελέτη της αξιόπιστης λειτουργίας των δικτύων. Στην αρχική του μορφή, το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων (packet switching), σύμφωνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε πακέτα και πολλοί χρήστες μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή.

Στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας. Κάθε πακέτο θα είχε την πληροφορία που χρειάζονταν για να φτάσει στον προορισμό του, όπου και θα γινόταν η επανασύνθεσή του σε δεδομένα τα οποία μπορούσε να χρησιμοποιήσει ο τελικός χρήστης.

Το παραπάνω σύστημα θα επέτρεπε σε υπολογιστές να μοιράζονται δεδομένα και σε ερευνητές να υλοποιήσουν το ηλεκτρονικό ταχυδρομείο.

Δεκαετία '70

Το 1973, ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται Internetting Project (Πρόγραμμα Διαδικτύωσης) προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Στόχος είναι η διασύνδεση πιθανώς ανόμοιων δικτύων και η ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο. Από την έρευνα γεννιέται μια νέα τεχνική, το **Internet Protocol** (**IP**) (Πρωτόκολλο Διαδικτύωσης), από την οποία θα πάρει αργότερα το όνομά του το Internet. Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο IP μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Σε ένα δίκτυο IP όλοι οι υπολογιστές είναι ισοδύναμοι, οπότε τελικά οποιοσδήποτε υπολογιστής του διαδικτύου μπορεί να επικοινωνεί με οποιονδήποτε άλλον.

Επίσης, σχεδιάζεται μια άλλη τεχνική για τον έλεγχο της μετάδοσης των δεδομένων, το **Transmission Control Protocol** (**TCP**) (Πρωτόκολλο Ελέγχου Μετάδοσης). Ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (E-mail). Σταδιακά συνδέονται με το ARPANET ιδρύματα από άλλες χώρες, με πρώτα το University College of London (Αγγλία) και το Royal Radar Establishment (Νορβηγία).

Δεκαετία '80

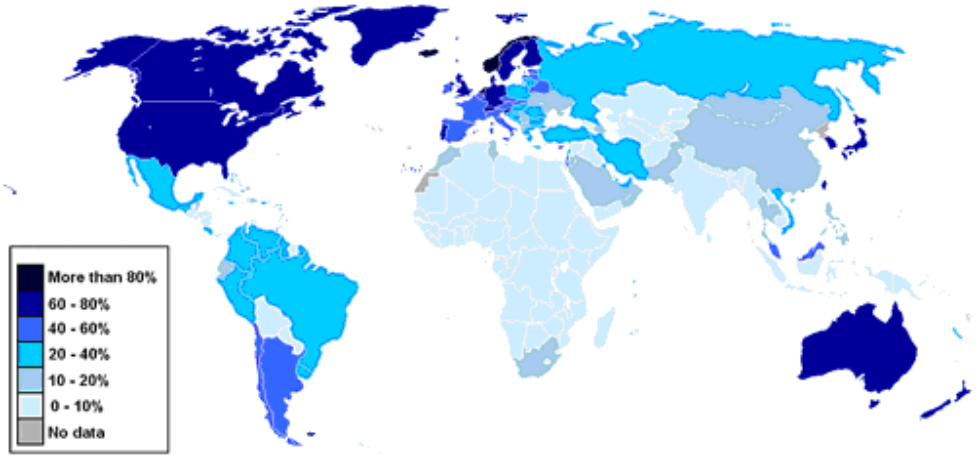
Το 1983, το πρωτόκολλο **TCP/IP** (δηλ. ο συνδυασμός των TCP και IP) αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Η έκδοση του λειτουργικού συστήματος Berkeley UNIX το οποίο περιλαμβάνει το TCP/IP συντελεί στη γρήγορη εξάπλωση της διαδικτύωσης των υπολογιστών. Εκατοντάδες Πανεπιστήμια συνδέουν τους υπολογιστές τους στο ARPANET, το οποίο επιβαρύνεται πολύ και το 1983, χωρίζεται σε δύο τμήματα: στο MILNET (για στρατιωτικές επικοινωνίες) και στο νέο ARPANET (για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση).

Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το **NSFNET** χρησιμοποιώντας το πρωτόκολλο TCP/IP, προκειμένου να συνδέσει πέντε κέντρα υπερ-υπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του '80, όλο και περισσότερες χώρες συνδέονται στο NSFNET (Καναδάς, Γαλλία, Σουηδία, Αυστραλία, Γερμανία, Ιταλία, κ.α.). Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο το οποίο αρχίζει να γίνεται γνωστό σαν **INTERNET** και να εξαπλώνεται με τρομερούς ρυθμούς σε ολόκληρο τον κόσμο. Περισσότεροι από 100,000 υπολογιστές έχουν συνδεθεί στα τέλη της δεκαετίας. Το 1990, το ARPANET πλέον καταργείται.

Δεκαετία '90

Όλο και περισσότερες χώρες συνδέονται στο NSFNET, μεταξύ των οποίων και η Ελλάδα το 1990. Το 1991, το εργαστήριο CERN στην Ελβετία παρουσιάζει το **World Wide Web** (**WWW**) (Παγκόσμιο Ιστό) που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη. Παράλληλα, εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Internet (Internet Service Providers - ISP) και προσφέρουν πρόσβαση στο Internet για όλους. Οποιοσδήποτε διαθέτει PC και modem μπορεί να συνδεθεί με το Internet σε τιμές που μειώνονται διαρκώς. Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο

του μεταφέρεται σε εμπορικά δίκτυα. Πλέον η απόκτηση doman names δεν είναι δωρεάν. Σαν αποτέλεσμα το'96 10,000 εταιρίες χάνουν τα domain names τους καθώς δεν είχαν πληρώσει για αυτά.



Σχ2.2.1 Η κατάσταση σύνδεσης ανά χώρα, όπως είχε το 2010

2.3 Προβλήματα Του IPv4

Το Διαδίκτυο αυτήν τη στιγμή χρησιμοποιεί την έκδοση τέσσερα (4) του Internet πρωτοκόλλου, γνωστή συνοπτικά σαν IPv4. Πρόκειται αναμφίβολα για το πιο πετυχημένο πρωτόκολλο με χρήση του οποίου συνδέθηκαν χιλιάδες κόμβοι εκατοντάδων διαφορετικών δικτύων δημιουργώντας αυτό που σήμερα ονομάζουμε Διαδίκτυο. Αρκετές δεκάδες εκατομμυρίων υπολογιστών και εκατοντάδες εκατομμυρίων χρηστών είναι συνδεμένοι στο Διαδίκτυο.

Η πρώτη έκδοση του IP έγινε τα μέσα του 1970. Επομένως θα έλεγε κανείς ότι το IPv4 δουλεύει αρκετά καλά, ιδιαίτερα αν αναλογιστούμε την ηλικία του. Κάθε σύστημα στον κόσμο σήμερα χρησιμοποιεί IPv4(εκτός από τα πειραματικά δίκτυα που χρησιμοποιούν από τώρα IPv6) . Μιλάμε για ένα αριθμό συστημάτων της τάξης των 100 εκατομμυρίων, που χρησιμοποιούν διάφορες εκδόσεις δικτυακού λογισμικού για TCP/IP, που τρέχουν σε μια πληθώρα λειτουργικών συστημάτων και υλικού. Αντιλαμβανόμαστε λοιπόν ότι μια πιθανή αναβάθμιση του πρωτοκόλλου θα επηρεάσει όλο το πιο πάνω αριθμό συστημάτων και οργανισμών αφού και αυτά πρέπει να αναβαθμιστούν ώστε να είναι συμβατά με το νέο πρωτόκολλο.

Οι βασικοί λόγοι που απαιτείται η αναβάθμιση είναι οι παρακάτω:

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

- *Θέματα απόδοσης:* Παρ' όλο που το IP λειτουργεί αποδοτικά τα 30 και πλέον χρόνια που χρησιμοποιείται, υπάρχουν πάρα πολλές βελτιώσεις που μπορούν να γίνουν. Οι διαχειριστές γνωρίζουν καλύτερα από όλους το κόστος διαχείρισης των routing entries εξαιτίας της έλλειψης επιπέδων ιεραρχίας στις IP διευθύνσεις. Επίσης αρκετές εφαρμογές απαιτούν υποστήριξη ποιότητας εξυπηρέτησης (QoS) από το IPv4 και προσπαθούν να ξεπεράσουν αυτή του την αδυναμία με χρήση άλλων πρωτοκόλλων σε υψηλότερα επίπεδα, μην πετυχαίνοντας όμως τα αναμενόμενα.

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

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

2.4 Πως Επιβίωσε το IPv4 ;

Σε αυτή την παράγραφο θα εξετάσουμε αναλυτικότερα το C.I.D.R. και το NAT που είναι οι βασικότεροι λόγοι επιβίωσης του IPv4. Με την εφαρμογή του TCP/IPv4 γρήγορα δημιουργήθηκαν προβλήματα, υπολογίστηκε ότι οι διευθύνσεις που παρέχει είναι λίγες και ότι

σύντομα θα έχουν εξαντληθεί. Καθώς η μετάβαση από το ένα πρωτόκολλο στο άλλο δεν ήταν δυνατή να γίνει σε μία μέρα, χρησιμοποιήθηκαν τεχνικές που θα έδιναν μια παράταση στο IPv4

Έτσι γεννήθηκαν:

1. το CIDR (Classless Interdomain Rooting) με το οποίο κάνουμε οικονομία στις public IP.Με το CIDR το μέγεθος των πινάκων που χρησιμοποιούν οι routers μειώθηκε δραστικά.
2. Το NAT (Network Address Translation).Επίσης και με αυτό κάνουμε ένα είδος οικονομίας στις public IP. Παράδειγμα, όλοι οι υπολογιστές ενός τοπικού δικτύου συνδέονται στο Internet χρησιμοποιώντας μία μόνο public IP) .

1) Το C.I.D.R εμπεριέχει τις εξής βασικές ιδέες :

- Ιεραρχημένη Διευθυνσιοδότηση
- Απόδοση διευθύνσεων σε μεταβλητού μεγέθους κομμάτια (Classless Address Allocation)
- Route Aggregation

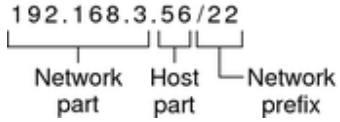
Ιεραρχημένη Διευθυνσιοδότηση:

Μια βασική απαίτηση για την εφαρμογή του CIDR είναι η ύπαρξη Ιεραρχημένης διευθυνσιοδότησης . Ένα είδος ιεραρχίας είναι η απόδοση διευθύνσεων ανάλογα με την γεωγραφική θέση του δικτύου. Πολλές φορές αυτός ο διαχωρισμός δεν είναι εφικτός γιατί πολλά δίκτυα παρόχων Internet αλλά και εταιριών απλώνονται ακόμα και σε διαφορετικές ηπείρους. Μια πιο λειτουργική προσέγγιση είναι η απόδοση μεγάλων κομματιών του χώρου διευθύνσεων στους παρόχους Internet. Κάθε νέο δίκτυο λοιπόν που συνδέετε στο Internet μέσω ενός παρόχου χρησιμοποιεί ένα κομμάτι διευθύνσεων που του παραχωρεί ο παροχέας του.

Αξίζει να σημειώσουμε ότι πλέον οι διευθύνσεις ενός δικτύου παραχωρούνται από τον παροχέα και για την σωστή λειτουργία του CIDR θα πρέπει να επιστρέφονται σε περίπτωση αλλαγής παροχέα και να αποδίδεται στο δίκτυο καινούργιο κομμάτι διευθύνσεων από των χώρο διευθυνσιοδότησης του νέου παροχέα. Η παραπάνω διαδικασία που μόλις περιγράψαμε είναι γνωστή και ως address renumbering ή renumbering.

Απόδοση διευθύνσεων σε μεταβλητού μεγέθους κομμάτια (Classless Address Allocation):

Το CIDR καταργεί τις τάξεις διευθύνσεων που χρησιμοποιούν μάσκες σταθερού μήκους και χρησιμοποιεί μάσκες μεταβλητού μήκους (Variable Length Masks - VLM). Με αυτό τον τρόπο χρησιμοποιώντας το ζευγάρι *Αρχική διεύθυνση / Μάσκα δικτύου* είναι δυνατό να καθορίσουμε ένα κομμάτι διευθύνσεων. Το ζευγάρι *Αρχική διεύθυνση / Μάσκα δικτύου* ονομάζεται πρόθεμα IP διεύθυνσης (IP Address Prefix) γιατί εάν πραγματοποιήσουμε την λογική πράξη *Αρχική Διεύθυνση και Μάσκα δικτύου* θα πάρουμε σαν αποτέλεσμα το κοινό μέρος που μοιράζονται όλες οι διευθύνσεις του κομματιού αυτού.



Σχήμα 2.4.1 IP διεύθυνση στο C.I.D.R.

(Route Aggregation):

Η άθροιση των διαδρομών είναι μία μέθοδος με την οποία είναι δυνατό να ανακοινωθούν με μία και μόνη διαδρομή ένας μεγάλος αριθμός δικτύων (από εκατοντάδες έως και χιλιάδες δίκτυα). Ο αλγόριθμος δρομολόγησης σε περίπτωση που υπάρχουν δύο δυνατές διαδρομές προς ένα δίκτυο επιλέγει εκείνη με το μεγαλύτερο πρόθεμα.

Το πλεονέκτημα της άθροισης των διαδρομών μειώνεται από δύο παράγοντες:

1. Από δίκτυα που έχουν συνδεθεί στο Internet μέσω δύο οι περισσότερων παρόχων.
2. Από δίκτυα που άλλαξαν παροχέα αλλά δεν πραγματοποίησαν renumbering.

2) NAT

Στα μέσα την δεκαετίας του ‘90,το NAT έγινε κύριο εργαλείο για την ανακούφιση της έλλειψης διευθύνσεων. Έχει αποδειχθεί ιδιαίτερα δημοφιλές στις χώρες που (για ιστορικούς λόγους)είχαν λιγότερους φραγμούς στο διάστημα διευθύνσεων που διέθεσαν κατά κεφαλή, παραδείγματος χάριν, οι Ηνωμένες Πολιτείες, οι οποίες χρησιμοποιούν σχεδόν το 60% τον δημόσιων διαθέσιμων διευθύνσεων. Έχει γίνει ένα τυποποιημένο και αναπόφευκτο χαρακτηριστικό

γνώρισμα στους δρομολογητές για τη σύνδεση στο διαδίκτυο, σπιτιών και μικρών γραφείων. Τα περισσότερα συστήματα που χρησιμοποιούν το NAT, το κάνουν αυτό προκειμένου να επιτρέψουν τη πρόσβαση στο Διαδίκτυο σε πολλαπλούς hosts που χρησιμοποιούν ιδιωτικό δίκτυο, χρησιμοποιώντας μια δημόσια διεύθυνση IP.Εντούτοις, το NAT «σπάει» το αρχικά προβλεπόμενο πρότυπο της IP end-to-end συνδεσιμότητας σε ολόκληρο το Διαδίκτυο, εισάγει περιπλοκές στην επικοινωνία μεταξύ των τελικών χρηστών και ασκεί επιδράσεις στην απόδοση. Επίσης υπάρχει μία μεγάλη λίστα από πρωτόκολλα και εφαρμογές οι οποίες αντιμετωπίζουν σοβαρά προβλήματα κατά την χρήση του NAT. Χαρακτηριστικά είναι οι peer to peer εφαρμογές(διαμοιρασμός αρχείων) καθώς και οι IPsec.

Το NAT κρύβει τη δομή ενός εσωτερικού δικτύου. Όλη η κυκλοφορία εμφανίζεται στα εξωτερικά συμβαλλόμενα μέρη σαν να προέρχεται από μια gateway μηχανή.

Η μετάφραση διευθύνσεων δικτύων περιλαμβάνει την επανεγγραφή των διευθύνσεων πηγής και προορισμού IP και συνήθως επίσης τους TCP/UDP αριθμούς πυλών των IP πακέτων, καθώς περνούν μέσω του NAT.

Κεφάλαιο 3^{ο} - Internet Protocol version 6

3.1 Εισαγωγή

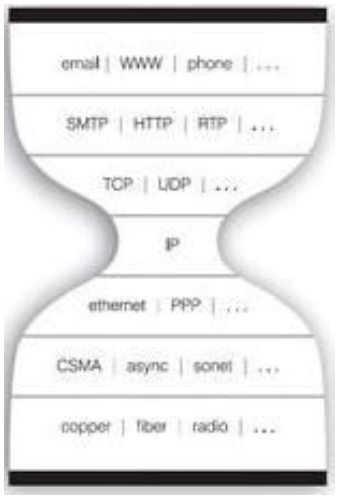
Η Internet Engineering Task Force (IEFT) κατά τις αρχές της δεκαετίας του 90’ ξεκίνησε μια προσπάθεια δημιουργίας ενός πρωτοκόλλου που θα διαδεχόταν το ήδη υπάρχον. Ταυτόχρονα την ίδια στιγμή ξεκίνησαν την προσπάθεια και πολλοί άλλοι. Η ημέρα όπου πλέον δεν θα υπάρχουν άλλες διαθέσιμες δημόσιες διευθύνσεις πλησίαζε. Η IEFT εξέταζε τις διαφορετικές προτάσεις κάνοντας συστάσεις για περεταίρω βελτιώσεις.

Το 1994 προτάθηκε επίσημα η δημιουργία του ΄΄IP Next Generation Protocol΄΄. Ταυτόχρονα συστάθηκε μια επιτροπή που σκοπός της ήταν να μελετήσει και να προσδιορίσει τα χρονικά περιθώρια για την ανάπτυξη του πρωτοκόλλου..Τα αποτελέσματα της έρευνας, βάση των τότε στατιστικών στοιχείων προσδιόρισαν το τέλος του IPv4 μεταξύ του 2005 και του 2011.

Έτσι ξεκίνησε η έρευνα και η ανάπτυξη της IPv6. Αρκετά χρόνια έχουν περάσει από τοτε και η έρευνα συνεχίζεται με συνεχείς προσθήκες νέων χαρακτηριστικών καθώς επίσης και προσπάθεια για την μετάβαση από το ένα πρωτόκολλο στο επόμενο.

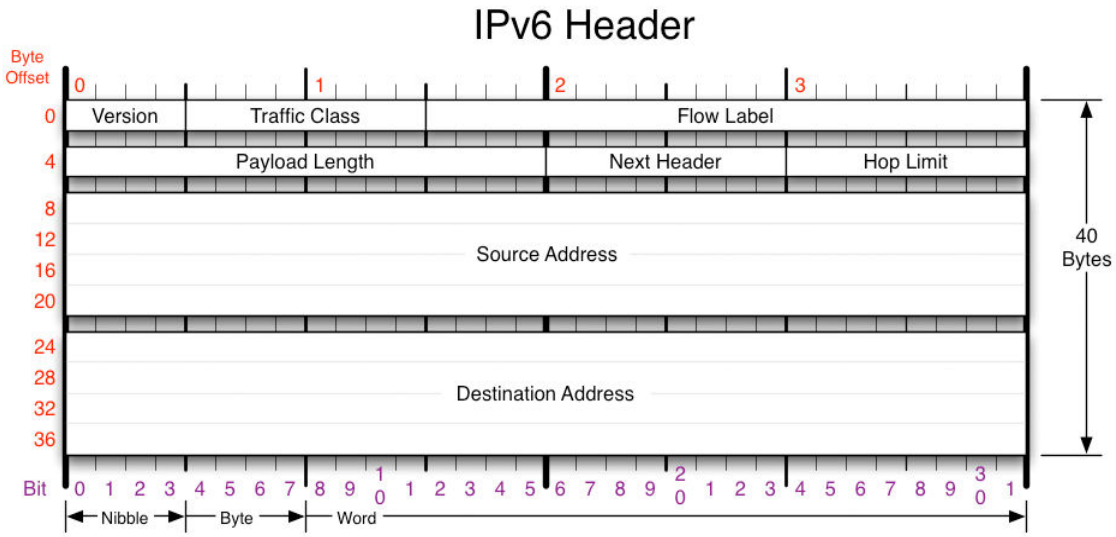
3.2 Η δομή της επικεφαλίδας στο IPv6

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



Σχήμα 3.2.1 Το μοντέλο της κλεψύδρας για παράσταση των πρωτοκόλλων

Στο IPv4 όλες οι επικεφαλίδες είναι οργανωμένες σε λέξεις των 32 bits. Στο IPv6 οι επικεφαλίδες είναι οργανωμένες σε λέξεις των 64 bits και το συνολικό μέγεθος των επικεφαλίδων είναι 40 bytes. Τα δύο πεδία της πηγής και του προορισμού χρησιμοποιούν συνολικά 32 bytes(16 bytes το κάθε ένα). Συνεπώς υπάρχουν μόνο 8 bytes διαθέσιμα για γενικές πληροφορίες της επικεφαλίδας. Επιπλέον στο IPv6 μπορούν να υπάρχουν προαιρετικά επικεφαλίδες επέκτασης που θα πρέπει να εμφανίζονται με συγκεκριμένη σειρά. Η κάθε επικεφαλίδα αναφέρει ποια είναι η επόμενη επικεφαλίδα που ακολουθεί ή αν είναι η τελευταία.



Εικόνα 3.2 .2 Η δομή μιας IPv6 επικεφαλίδας

Το πρωτόκολλο IPv6 περιλαμβάνει τα ακόλουθα πεδία στις επικεφαλίδες του:

- *Έκδοση (4 Bits):* Αναφέρεται η έκδοση του IP που χρησιμοποιείται (για το IPv6 είναι ίση με έξι (6).

- *Κλάση Κίνησης (1 Byte):* Έχει αντικαταστήσει τον ΄΄ Τύπο Υπηρεσίας ΄΄ της IPv4. Ορίζει το είδος υπηρεσίας, που ανήκει στο μοντέλο των differentiated υπηρεσιών, που πρέπει να δοθεί στο πακέτο. Είχε οριστεί για πρώτη φορά στο RFC 1883 σαν πεδίο προτεραιότητας. Κατόπιν το όνομα αλλάχτηκε σε κλάση και πρόσφατα χαρακτηρίζεται σαν κλάση κίνησης. Αναγνωρίζει και διαχειρίζεται την κίνηση των δεδομένων πραγματικού χρόνου και διαχωρίζει τις διαφορετικές κλάσεις και προτεραιότητες των πακέτων δεδομένων.

- *Ροή πακέτων (20 Bits):* Χρησιμοποιείται για να αναγνωριστούν τα πακέτα της ίδιας ροής με σκοπό να διαχειριστή η ροή δεδομένων πραγματικού χρόνου.

Ένας κόμβος μπορεί να έχει περισσότερες από μία ροές πακέτων. Ο Router επεξεργάζεται τα πακέτα που ανήκουν στην ίδια ροή πιο αποτελεσματικά καθώς δεν χρειάζεται να επεξεργάζονται ξανά και ξανά την επικεφαλίδα κάθε πακέτου, Στο RFC 1883 είχε οριστεί με μεγαλύτερο μέγεθος, αλλά κατόπιν της αύξησης του πεδίου κλάσης μειώθηκε το μέγεθός της.

- *Μήκος πακέτου (2 Bytes):* Είναι ένας αριθμός που δηλώνει το μήκος του πακέτου των δεδομένων –δηλαδή του πακέτου μετά το τέλος των επικεφαλίδων (payload) σε bytes. Ο μέγιστος όγκος του πακέτου ανέρχεται στα 64 KB.Όμως υπάρχει η δυνατότητα υποστήριξης μεγαλύτερων πακέτων με την χρήση μιας επικεφαλίδας επέκτασης αν η σύνδεση μας είναι μεγαλύτερη των 64KB.Τέλος, περιλαμβάνει και το μέγεθος των IPv6 επικεφαλίδων επεκτάσεως που τυχόν υπάρχουν.

- *Επόμενη επικεφαλίδα (1 Byte):* Αναφέρει πιο πρωτόκολλο χρησιμοποιείται στην επικεφαλίδα μετά το IPv6 πακέτο. Αν η επόμενη επικεφαλίδα είναι UDP ή TCP τότε το συγκεκριμένο πεδίο θα περιέχει τον αριθμό 6 ή 17 αντίστοιχα, ακριβώς όπως γινόταν και στην IPv4. Αν όμως χρησιμοποιούνται επικεφαλίδες επέκτασης τότε θα υπάρχει ο αριθμός που αντιστοιχεί και έχει οριστεί για κάθε μία. Οι επικεφαλίδες επέκτασης τοποθετούνται μεταξύ της IP επικεφαλίδας και της TCP ή UDP επικεφαλίδας.

- *Hop limit (2 Byte):* Κάθε φορά που ένας κόμβος προωθεί το πακέτο, μειώνει το μέγεθος του hop limit κατά ένα. Όταν αυτό μηδενιστεί το πακέτο διαγράφεται από το δίκτυο. Δεν είναι απίθανο να καταργηθεί αυτό το πεδίο, μιας και η τρέχουσα αίσθηση θέλει αντίστοιχες λειτουργίες να μεταφερθούν σε πρωτόκολλα ανώτερων επιπέδων.

- *Διεύθυνση αποστολέα (16 Bytes):* Είναι η IPv6 διεύθυνση του κόμβου που δημιούργησε το πακέτο.

- *Διεύθυνση παραλήπτη (16 Bytes):* Είναι η IPv6 διεύθυνση του ή των κόμβων που πρόκειται να παραλάβουν το πακέτο. Μπορεί να είναι διεύθυνση τύπου unicast, multicast ή anycast. Εάν στο πακέτο υπάρχει και routing extension που ορίζει το μονοπάτι που πρέπει να ακολουθήσει το πακέτο, τότε η διεύθυνση προορισμού μπορεί να είναι ένας από τους ενδιάμεσους κόμβους αντί αυτής που αναφέρεται στο πεδίο διεύθυνση παραλήπτη.

3.3 Οι επικεφαλίδες επέκτασης

Στο IPv4 το πρόβλημα με το πεδίο IP Options είναι ότι επειδή αλλάζει η μορφή των επικεφαλίδων θα πρέπει να αντιμετωπίζονται σαν ειδικές περιπτώσεις από τους δρομολογητές. Οι δρομολογητές όμως θα πρέπει να είναι βέλτιστοι για τα συνήθη πακέτα και άρα τα IPv4 χειρίζονται σαν ειδικές περιπτώσεις που αφήνονται να εξεταστούν αργότερα. Οι επικεφαλίδες επέκτασης στο IPv6 αντιμετωπίζουν αυτό το πρόβλημα γιατί έχουν μεταφερθεί από το κομμάτι της επικεφαλίδας του πακέτου στο κομμάτι των δεδομένων του πακέτου (payload). Έτσι αναγκάζουν τους δρομολογητές να αντιμετωπίζουν το ίδιο άμεσα ένα πακέτο με options και ένα πακέτο χωρίς options. Εξαίρεση σε αυτό αποτελούν οι Hop By Hop options που θα πρέπει να επεξεργάζονται από όλους τους ενδιάμεσους δρομολογητές.

Στο IPv4 μια επικεφαλίδα κυμαίνεται μεταξύ 20 με 60 Bytes με σκοπό να προσδιοριστούν επιλογές όπως ασφαλείας ή διαμοιρασμού. Αυτή η χρήση σπάνια συνέβαινε γιατί προκαλούσε μεγάλο όγκο δεδομένων προς επεξεργασία. Στην IPv6 υπάρχει ένας καινούριος διαχείρισης των επιλογών. Οι επιλογές περιλαμβάνονται σε επικεφαλίδες οι οποίες ονομάζονται επικεφαλίδες επέκτασης (Extension Headers). Οι επικεφαλίδες αυτές αντί να περιλαμβάνονται στην επικεφαλίδα του, ενσωματώνονται στο φορτίο όποτε χρειάζονται.

Οι επικεφαλίδες είναι οι εξής:

- *Hop-by-Hop Options Header:* Αυτή η επικεφαλίδα ακολουθεί πάντα την επικεφαλίδα του IPv6 πακέτου. Περιλαμβάνει δεδομένα που κάθε κόμβος θα πρέπει να επεξεργαστεί. Με την παρουσία αυτής της επικεφαλίδας, ο κάθε router γνωρίζει ότι δεν πρέπει να επεξεργαστεί το πακέτο και έτσι το προωθεί αμέσως στον τελικό του προορισμό. Αν υπάρχει η συγκεκριμένη επικεφαλίδα ο router εξετάζει μόνο την επικεφαλίδα και όχι ολόκληρο το πακέτο. Έτσι περιορίζεται σημαντικά ο όγκος δεδομένων προς επεξεργασία.

- *Routing Header:* Αναφέρονται οι διάφοροι κόμβοι που θα επισκεφτεί το πακέτο κατά τη διαδρομή από τον αποστολέα στον παραλήπτη. Ο κάθε κόμβος που παραλαμβάνει το πακέτο ελέγχει ποιος είναι ο επόμενος παραλήπτης στη λίστα και προωθεί το πακέτο σ' αυτόν.

- *Fragment Header:* Χρησιμοποιείται από τον κόμβο του αποστολέα προκειμένου να μεταδώσει πακέτα με μέγεθος μεγαλύτερο από το μέγιστο επιτρεπόμενο μέγεθος πακέτου (Path MTU) στο μονοπάτι από τον αποστολέα στον παραλήπτη. Αν το πακέτο είναι μεγαλύτερο από το επιτρεπόμενο στο δίκτυο τότε το πακέτο ΄΄σπάει΄΄ σε μικρότερα. Ο τελικός κόμβος προορισμού του πακέτου επανασυνδέει τα κομμάτια και δημιουργεί το αρχικό πακέτο.

- *Destination Options Header:* Περιέχει πληροφορίες που θα πρέπει να ελεγχθούν από τον τελικό παραλήπτη που αναφέρεται στη διεύθυνση προορισμού και στις διευθύνσεις που περιλαμβάνονται στο Routing Header.

- *Authentication Header:* Χρησιμοποιείται προκειμένου να εξασφαλιστεί ότι τα δεδομένα δεν έχουν αλλαχτεί κατά τη μετάδοση του πακέτου στο μονοπάτι από τον αποστολέα στον παραλήπτη. Η μέθοδος που χρησιμοποιείται για αυτό είναι ένα κρυπτογραφημένο checksum κάποιων από τις επικεφαλίδες του IPv6 και των δεδομένων (payload).

- *Encapsulating Security Payload Header:* Πρόκειται για την τελευταία επικεφαλίδα που μπορεί να υπάρξει στη σειρά των επικεφαλίδων επέκτασης που δεν έχει κωδικοποιηθεί (αν έχει επιλεγεί από τον κόμβο αποστολέα η κωδικοποίηση των δεδομένων που μεταδίδει). Χρησιμοποιείται προκειμένου να δείξει ότι ολόκληρο το πακέτο έχει κωδικοποιηθεί και παρέχει πληροφορία για τον κόμβο παραλήπτη για τη διαδικασία αποκρυπτογράφησης.

- *Destination Options Header:* Αντιστοιχεί στο πεδίο IP Options του IPv4. Ο κόμβος παραλήπτης επεξεργάζεται αυτήν την επικεφαλίδα αφού παραλάβει το πακέτο. Προς το παρόν δε χρησιμοποιείται καθόλου αυτό το πεδίο και απλώς συμπληρώνεται με bits (padding).

Όλες οι επικεφαλίδες στο IPv6 έχουν το ίδιο μέγεθος και την ίδια μορφοποίηση. Η διαφορά τους βρίσκεται στο πεδίο που αφορά την επόμενη επικεφαλίδα. Η σειρά με την οποία μπορούν να εμφανίζονται οι επικεφαλίδες είναι αυστηρά καθορισμένη.

3.4 Αλλαγές των πεδίων της επικεφαλίδας του IPv6

Οι τέσσερις μεγάλες αλλαγές που εισήγαγε το IPv6 στα πεδία της επικεφαλίδας ενός πακέτου αφορούν:

- την ύπαρξη ετικετών ροής και προτεραιότητας των πακέτων (Flow Labels)
- την ύπαρξη κλάσεων κίνησης (Traffic Classes)
- την αλλαγή στη φιλοσοφία της κατάτμησης του πακέτου (Fragmentation)
- την ύπαρξη επικεφαλίδων επέκτασης (Extension Headers)

3.4.1 Ετικέτες ροής

Οι προδιαγραφές του IPv4 προκειμένου να πετύχει σαν πρωτόκολλο σε δίκτυο μεταγωγής πακέτων ήταν να μπορεί κάθε πακέτο να βρίσκει το δικό του δρόμο προς τον προορισμό, πρόκειται δηλαδή για πρωτόκολλο χωρίς σύνδεση. Το προφανές πλεονέκτημα είναι ότι δύο πακέτα από τον ίδιο αποστολέα προς τον ίδιο παραλήπτη μπορούν να ακολουθήσουν διαφορετικά μονοπάτια μέχρι να καταλήξουν στον κόμβο προορισμό. Αυτό αυξάνει την ευρωστία του δικτύου και την ευελιξία σε περίπτωση που κάποιο από τα μονοπάτια παρουσιάσει πρόβλημα λειτουργίας. Παρ' όλα αυτά η αντιμετώπιση αυτή δεν είναι αποδοτική, ειδικά στην περίπτωση που τα πακέτα δεν είναι αυτόνομα αλλά πρόκειται για τμήματα από μία ροή δεδομένων μεταξύ εφαρμογών. Τότε ο κάθε δρομολογητής στο μονοπάτι αποστολέας – παραλήπτης θα πρέπει να επεξεργάζεται αυτό το πακέτο εισάγοντας επιπλέον καθυστέρηση που είναι γνωστή σαν latency. Αυτή η καθυστέρηση δε δημιουργούσε προβλήματα σε παραδοσιακές εφαρμογές όπως το ftp, το email κλπ. Όμως στις νέες προηγμένες υπηρεσίες που απαιτούν μεταφορά αλληλεπιδραστικού ήχου και κινούμενης εικόνας κάτι τέτοιο επηρεάζει σημαντικά την απόδοσή τους. Ένα ακόμη πρόβλημα της φιλοσοφίας αυτής του IPv4 είναι η αδυναμία να δρομολογηθεί συγκεκριμένος τύπος κίνησης σε μονοπάτια που το κόστος τους είναι χαμηλό. Για παράδειγμα η μεταφορά πακέτων ηλεκτρονικού ταχυδρομείου που δεν είναι εφαρμογή πραγματικού χρόνου και μπορεί να γίνει στο παρασκήνιο θα μπορούσε να γίνει πάνω από μία σύνδεση χαμηλής ταχύτητας άρα και χαμηλού κόστους, αφιερώνοντας έτσι τις συνδέσεις υψηλών ταχυτήτων (που έχουν και μεγάλο κόστος) σε εφαρμογές πραγματικού χρόνου.

Στο IPv6 αυτό το πρόβλημα έχει αντιμετωπιστεί και μία ροή πακέτων με ίδιους αποστολέα και

παραλήπτη θεωρείται ότι ανήκουν στην ίδια ροή και φυσικά έχουν την ίδια τιμή στο πεδίο της ετικέτας ροής και προτεραιότητας.

3.4.2 Κλάση κίνησης

Στην πρώτη έκδοση του IPv6 στο RFC 1883 υπήρχε ορισμένο ένα πεδίο προτεραιότητας τεσσάρων bits όπου μπορούν να οριστούν δεκαέξι διαφορετικές κλάσεις προτεραιότητας. Αργότερα το πεδίο αυτό μετονομάστηκε σε κλάση κίνησης με συνολικό μέγεθος ένα byte.

Η ακριβής χρήση αυτού του πεδίου δεν έχει ακόμα καθοριστεί. Ο στόχος της ύπαρξης και χρήσης αυτού του πεδίου είναι να επιτρέπει στους κόμβους αποστολείς και στους δρομολογητές να μαρκάρουν τα πακέτα που επιθυμούν να έχουν διαφορετική επεξεργασία από τη συνήθη. Να έχουν δηλαδή ειδική επεξεργασία όσον αφορά το κόστος, το εύρος ζώνης και το χρόνο latency ή και κάποια άλλα χαρακτηριστικά των συνδέσεων πάνω από τις οποίες δρομολογούνται.

3.4.3 Κατάτμηση πακέτων

Όπως προαναφέρθηκε στο IPv6, η κατάτμηση των πακέτων επιτρέπεται μόνο μεταξύ του κόμβου αποστολέα και του κόμβου παραλήπτη, απλοποιώντας έτσι την επικεφαλίδα του πακέτου και μειώνοντας το χρόνο δρομολόγησης. Η δυνατότητα να γίνεται κατάτμηση των πακέτων στο IPv4 από οποιονδήποτε κόμβο του μονοπατιού είναι ιδιαίτερα επιζήμια γιατί πιθανά είναι μία διαδικασία που θα πρέπει να γίνει αρκετές φορές. Επίσης η απώλεια ενός τμήματος (fragment) του πακέτου συνεπάγεται επανάληψη όλων των τμημάτων.

Για παράδειγμα έστω στο IPv4 ένας κόμβος μεταδίδει ένα πακέτο μεγέθους 1500 bytes προς έναν παραλήπτη στο Διαδίκτυο. Το πακέτο μεταδίδεται πάνω από το τοπικό δίκτυο Ethernet προς το δρομολογητή του δικτύου. Ο δρομολογητής αυτός το δρομολογεί πάνω από τη σειριακή του σύνδεση με τον παροχέα Διαδικτύου. Σε κάποιον ενδιάμεσο κόμβο της διαδρομής διαπιστώνεται ότι κάποια δικτυακή σύνδεση δεν μπορεί να χειριστεί πακέτα αυτού του μεγέθους. Τότε ο δρομολογητής που έχει αυτήν τη δικτυακή σύνδεση θα «σπάσει» το πακέτο σε μικρότερα ανάλογα με το μέγιστο μέγεθος πακέτου (Maximum Transmission Unit – MTU) για τη συγκεκριμένη δικτυακή σύνδεση. Έστω ότι το MTU είναι στη συγκεκριμένη περίπτωση 1280 bytes, οπότε ο δρομολογητής δημιουργεί δύο πακέτα, ένα με μέγεθος 1260 bytes (και 20 bytes

της επικεφαλίδας = 1280 bytes) και ένα μεγέθους 240 bytes (και 20 bytes της επικεφαλίδας = 260 bytes).Αυτή η διαδικασία θα επαναληφθεί όσες φορές χρειαστεί και ο κόμβος παραλήπτης θα ενώσει τα διαφορετικά τμήματα για να φτιάξει το πακέτο.

Αυτό αρχικά θεωρήθηκε σαν πλεονέκτημα του σχεδιασμού του IPv4. Όμως θέτει σημαντικά θέματα απόδοσης στους δρομολογητές καθώς η διαδικασία στοιχίζει αρκετά τόσο σε επεξεργασία όσο και σε χρόνο.

Για να λυθεί αυτό το πρόβλημα θα πρέπει να είναι εκ των προτέρων γνωστό το MTU του μονοπατιού). Δύο είναι οι λύσεις σε αυτό το πρόβλημα. Η μία που χρησιμοποιείται και στο IPv4 είναι ο δρομολογητής να στέλνει ένα πακέτο με μέγεθος όσο είναι το MTU της σύνδεσής του στον παραλήπτη. Εάν κάποια στιγμή αυτό το πακέτο πρέπει να «σπάσει» τότε με χρήση του πρωτόκολλο Internet Control Message Protocol (ICMP) ο δρομολογητής που έχει το πρόβλημα θα ενημερώσει τον αρχικό δρομολογητή για το δικό του MTU. Η διαδικασία επαναλαμβάνεται μέχρι να βρεθεί το MTU του μονοπατιού. Η τεχνική αυτή λέγεται Path MTU Discovery. Η άλλη τεχνική είναι να υπάρχει ένα ελάχιστο μέγεθος MTU που να πρέπει να υποστηρίζεται από όλα τα είδη συνδέσεων.

Το IPv6 υποστηρίζει και τις δύο λύσεις. Αρχικά μάλιστα το ελάχιστο MTU ήταν 576 bytes, αργότερα έγινε 1500 και κατόπιν 1280. Ο λόγος των αλλαγών είναι ότι το ελάχιστο MTU ουσιαστικά ορίζει ποιες τεχνολογίες θα εγκαταλείπονταν ενώ παράλληλα είναι και ένας από τους παράγοντες που επηρεάζει την απόδοση ενός δικτύου. Για να αντιμετωπίσει αυτό το πρόβλημα το IPv6 ορίζει ότι όλοι οι IPv6 κόμβοι πρέπει να υλοποιούν την τεχνική του Path MTU Discovery. Με χρήση του “Don’t Fragment” bit θα αναγκάζονται οι ενδιάμεσοι δρομολογητές να επιστρέφουν ICMP μηνύματα λάθους αναφέροντας ότι το μέγεθος του πακέτου είναι μεγάλο. Οι κόμβοι που δε θα χρησιμοποιούν αυτήν την τεχνική θα πρέπει να χρησιμοποιούν το ελάχιστο μέγεθος για το MTU.

3.5 Τύποι διευθύνσεων στο IPv6

Στο IPv6 υπάρχουν τρεις τύποι διευθύνσεων:

- Unicast: Αντιπροσωπεύει ένα interface.
- Anycast: Αντιπροσωπεύει σύνολο από interfaces (που ανήκουν συνήθως σε

διαφορετικούς κόμβους). Ένα πακέτο που αποστέλλεται σε μια διεύθυνση anycast παραδίδεται σε ένα μόνο interface (το πλησιέστερο, σύμφωνα με τον υπολογισμό απόστασης των πρωτοκόλλων δρομολόγησης). Έχει το ίδιο format με τις unicast διευθύνσεις.

- Multicast: Αντιπροσωπεύει σύνολο από interfaces (που ανήκουν συνήθως σε διαφορετικούς κόμβους). Ένα πακέτο που αποστέλλεται σε μια διεύθυνση multicast, παραδίδεται σε όλα τα interfaces που προσδιορίζονται από την διεύθυνση αυτή.

Κεφάλαιο 4^{ο} - Διαφορές IPv4 με IPv6

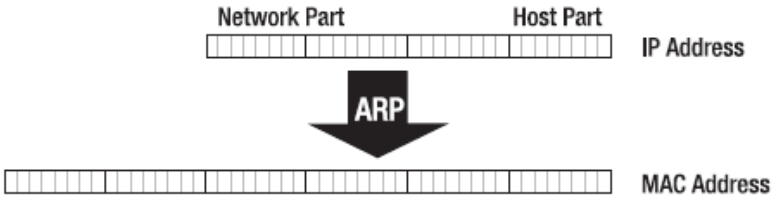
4.1 Εισαγωγή

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

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

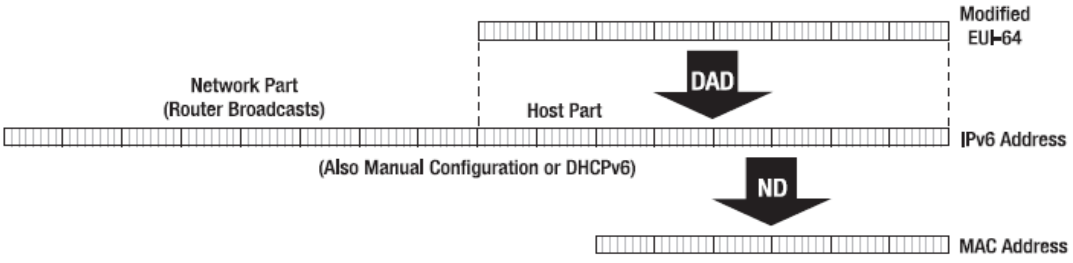
Το πρόβλημα βρήκε λύση το 1993 με την υιοθέτηση του CIDR (Classless Interdomain Routing). Με το CIDR η διάκριση σε κλάσεις δεν χρειαζόταν πια. Μια τιμή τώρα πια υποδείκνυε τη διάκριση σε bits που δείχνουν τα υποδίκτυα και τα bits που δείχνουν τις δικτυακές συσκευές στα υποδίκτυα. Το IPv6 και αυτό δεν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

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



Σχήμα 4.1.1 Αντιστοίχιση IP διεύθυνσης με την αντίστοιχη MAC με χρήση του ARP πρωτοκόλλου.

Στο IPv6 πολλές φορές μπορεί να μην εμπεριέχεται η MAC διεύθυνση και γι' αυτό υπάρχει και εδώ ένας παρόμοιος μηχανισμός με το πρωτόκολλο ARP. Το ARP όμως χρησιμοποιεί broadcasts που το IPv6 δεν υποστηρίζει. Αντίθετα το IPv6 χρησιμοποιεί εκτενώς multicasts. Στο multicast τα πακέτα μεταδίδονται μόνο σε μια ορισμένη ομάδα δικτυακών συσκευών και όχι σε όλες. Στο IPv6 το αντίστοιχο πρωτόκολλο του ARP είναι το ND(Neighbor Discovery) και βασίζεται σε multicasts, είναι πιο γενικό από το ARP και όχι τόσο εξαρτώμενο από τα δίκτυα Ethernet. Στο IPv6 επίσης χρησιμοποιείται η τεχνολογία DAD(Duplicate Address Detection) δανεισμένη από το πρωτόκολλο AppleTalk και ανιχνεύει όπως λέει και το όνομά της αν υπάρχουν δικτυακές συσκευές που έχουν την ίδια IP ώστε να αποφευχθεί κάτι τέτοιο.



Σχήμα 4.1.2 Αντιστοίχιση IP με DAD

4.2 Πλεονεκτήματα και Μειονεκτήματα του IPv6 σε σχέση με το IPv4

Το πιο προφανές και με διαφορά πιο σημαντικό πλεονέκτημα της καινούριας έκδοσης του IP είναι ο πολύ μεγαλύτερος χώρος διευθύνσεων. Επίσης προσφέρει βαθύτερη ιεραρχία διευθυνσιοδότησης αλλά και απλούστερες ρυθμίσεις. Μια μέρα θα έχουμε ξεχάσει πως ήταν να έχουμε μια διεύθυνση των 32 Bytes.Οι διαχειριστές δικτύων θα αγαπήσουν τους μηχανισμούς αυτοδιαμόρφωσης που παρέχει το νέο πρωτόκολλο. Ακόμα και αν η αύξηση σε απαιτήσεις για χώρο διευθύνσεων διπλασιαζόταν κάθε 5 χρόνια όπως γινόταν για κάποιο χρονικό διάστημα, που είναι εκθετικός ρυθμός αύξησης, τότε οι διαθέσιμες διευθύνσεις θα τελείωναν το 2485. Ουσιαστικά δηλαδή λύνει το πρόβλημα του χώρου διευθύνσεων.

- *Απλοποίηση της Επικεφαλίδας:* Στο IPv6 η επικεφαλίδα έχει μήκος 40 Bytes. Αυτό σημαίνει πως διαθέτουμε μόνο 8 Bytes για την επικεφαλίδα καθώς έχουμε και δύο IP διευθύνσεις. Του αποστολέα και του παραλήπτη. Κάποια πεδία από την επικεφαλίδα του IPv4 έχουν αφαιρεθεί. Με αυτή την αλλαγή τα πακέτα διαχειρίζονται γρηγορότερα και σαν αποτέλεσμα έχουμε την μείωση του επεξεργαστικού κόστους.

- *Αυξημένη υποστήριξη για επεκτάσεις και επιλογές:* Στην IPv4 οι επιλογές ήταν ενσωματωμένες στην βασική επικεφαλίδα. Πλέον, ορίζονται οι επικεφαλίδες επέκτασης. Τα χαρακτηρίστηκα τους είναι ότι είναι προαιρετικές και εισάγονται πάντα ανάμεσα στην βασική επικεφαλίδα και στο φορτίο. Με αυτόν τον τρόπο τα πακέτα γίνονται πολύ ευέλικτα. Η δρομολόγηση των πακέτων γίνεται πολύ περισσότερο αποτελεσματική. Οι επιλογές μπορούν να εισαχθούν με ευκολία.

- *Δυνατότητα μαρκαρίσματος των ροών κίνησης:* Τα πακέτα που ανήκουν στην ίδια ροή πακέτων απαιτούν ειδική διαχείριση και μπορουν να μαρκαριστούν από τον αποστολέα. Ένα παράδειγμα που εφαρμόζεται είναι οι υπηρεσίες πραγματικού χρόνου.

- *Καινοτομία:* Με την τεχνολογία NAT σήμερα συνεχίζεται η λειτουργιά του IPv4.Η συγκεκριμένη τεχνολογία λύνει κάποια προβλήματα, όχι όμως όλα. Για κλασικές εφαρμογές client/server π.χ email,web και άλλες, η τεχνολογία NAT λύνει το πρόβλημα, για άλλες εφαρμογές όμως, όπως VoIP, όπου κάθε Η/Υ πρέπει να είναι «διακριτός» και για όσους είναι

έξω του δικτύου που χρησιμοποιεί NAT, η τεχνολογία NAT σίγουρα δυσκολεύει τη λειτουργία τους.

- *Αυτορύθμιση διεύθυνσης:* Στο IPv4 χρησιμοποιούνταν το πρωτόκολλο DHCP για να λάβει μία συσκευή αυτόματα IP διεύθυνση. Αυτό έχει 2 μεγάλα μειονεκτήματα:

1) Χρειάζεται 1 DHCP server.

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

- *Εύκολη αλλαγή διεύθυνσης:* Σύμφωνα με τον παραπάνω τρόπο αυτόματης ρύθμισης της διεύθυνσης, είναι πολύ εύκολο οι δικτυακές συσκευές ενός ολόκληρου δικτύου να αλλάξουν διεύθυνση. Απλά αλλάζει το 64-bit που διαφημίζεται με ένα καινούριο. Οι παλιές διευθύνσεις βέβαια παραμένουν σε ισχύ για τυχόν επικοινωνίες που είναι ήδη ανοιχτές ή δεν έχουν ενημερωθεί για την αλλαγή αλλά όσες καινούριες φτιάχνονται χρησιμοποιούν τις καινούριες, αλλαγμένες διευθύνσεις.
- *Ασφάλεια:* Ο πιο διαδεδομένος μύθος για το IPv6 είναι ότι θα είναι πιο ασφαλές από το IPv4 επειδή θα έχει «υποχρεωτική» υποστήριξη του IPSec. Το IPSec παρέχει κρυπτογράφηση και πιστοποίηση στο επίπεδο του IP προστατεύοντας έτσι τα δεδομένα μιας εφαρμογής από το να αλλαχθούν κατά τη μεταφορά τους. Στην πραγματικότητα όμως το IPSec είναι ήδη διαθέσιμο και για το IPv4 και το γεγονός ότι συμπεριλαμβάνεται στο IPv6 δε σημαίνει ότι δε χρειάζεται εκτενείς προσπάθειες για τη ρύθμιση και τη λειτουργία του.

Στο IPv4 βέβαια, είναι ακόμα πιο δύσκολη η ρύθμισή του, καθώς το NAT περιπλέκει τα πράγματα, επειδή υπάρχει «μετάφραση» στη μέση.

Το IPv6 ωστόσο έχει ένα πλεονέκτημα ασφαλείας σε σχέση με το IPv4. Επειδή είναι μεγάλος ο χώρος διευθύνσεων, ένα worm είναι δύσκολο να «σκανάρει» όλο το υποδίκτυο. Στο IPv4, οι συσκευές ενός υποδικτύου το πολύ να είχαν μια 16 bit διεύθυνση, οπότε το worm μπορούσε συνήθως να κάνει port scanning σε όλους, ενώ με το IPv6, που ένα σύνηθες υποδίκτυο μπορεί να είναι ακόμα και 64 bit, είναι σχεδόν αδύνατο να το κάνει. Είναι σαν να «σκανάρει» ένα δίκτυο δύο φορές όσο το σημερινό IPv4 Internet.

- *Φορητότητα:* Με την χρήση του IPv4 για να επικοινωνήσει ένας φορητός κόμβος η διαδικασία ήταν η εξής: Τα πακέτα από τον φορητό κόμβο στέλνονται στον κεντρικό πάροχο και στην συνέχεια αυτός τα στέλνει στην τελική διεύθυνση και το ανάποδο. Με την χρήση του IPv6 η επικοινωνία μεταξύ του φορητού κόμβου και της διεύθυνσης επικοινωνίας είναι άμεση.
Το πλεονέκτημα είναι ότι μπορεί έτσι να χρησιμοποιηθεί τι συντομότερο μονοπάτι μεταξύ των δύο. Τα πακέτα δεν χρειάζεται πλέον να περνούν από τον κεντρικό πάροχο. Αυτό μειώνει το φορτίο στο δίκτυο. Πράγμα πολύ σημαντικό, όταν μιλάμε για μεγάλους αριθμούς κινητών κόμβων που χρησιμοποιούν για παράδειγμα VoIP.

- *Ποιότητα Υπηρεσίας:* Το υπάρχον IP πρωτόκολλο διαχειρίζεται όλα τα πακέτα με τον ίδιο τρόπο. Το πρώτο που έρχεται-πρώτο δρομολογείται. Τα QoS πρωτόκολλα έχουν την εργασία να παρέχουν διαφορετικές προτεραιότητες στα πακέτα όπως το εύρος ζώνης ή χρόνοι καθυστέρησης. Αυτή την στιγμή υπάρχουν δύο αρχιτεκτονικές. Η Integrated Services (IntServ) και οι Differential Services (Differv). Χρησιμοποιούνται για να κάνουν την δρομολόγηση σύμφωνα με συγκεκριμένα κριτήρια όπως για παράδειγμα αν υπάρχουν αρκετοί πόροι για να δρομολογηθούν τα δεδομένα. Επίσης μπορούν να ελέγξουν το κόστος εξαρτώμενα από διαφορετικά επίπεδα παροχής υπηρεσιών.
- *Αποδοτικότητα:* Μετά από δύο δεκαετίες εμπειρία χρήσης του IPv4 έχει αποκομιστεί αρκετή εμπειρία στο ποια χαρακτηριστικά είναι χρήσιμα και ποια όχι στο IPv4 και ποια λειτουργούν ως bottlenecks της ταχύτητας. Στο IPv6 έχουν ενσωματωθεί αυτές οι βελτιώσεις και πράγματι έχει πολύ καλύτερη απόδοση. Παρ' όλο που τώρα τα πεδία διευθύνσεων είναι 4 φορές μεγαλύτερα σε σχέση με το IPv4, η συνολική επικεφαλίδα είναι μόνο 40 bytes εν συγκρίσει με τα 20 bytes μιας τυπικής επικεφαλίδας IPv4.

Οι βελτιώσεις που υπάρχουν είναι οι εξής:

1) Η επικεφαλίδα του IPv6 έχει σταθερό μήκος

2) Η επικεφαλίδα του IPv6 είναι βελτιστοποιημένη για επεξεργασία 64 bit τη φορά σε σχέση με τα 32 bit του IPv4.
3) Το checksum της επικεφαλίδας IPv4 που υπολογίζεται κάθε φορά που 1 πακέτο περνά από 1 δρομολογητή, αφαιρέθηκε από το IPv6.
4) Οι δρομολογητές δεν είναι υποχρεωμένοι να χωρίζουν 1 μεγάλο πακέτο σε μικρότερα κομμάτια και μπορούν απλά να στείλουν σήμα να τους έρχονται μικρότερα πακέτα.
5) Το broadcast που χρησιμοποιούνταν ευρέως στο IPv4 αντικαταστάθηκε με τα multicast στο IPv6 με τα οποία δεν διακόπτονται όλες οι δικτυακές συσκευές για να επεξεργαστούν το μήνυμα που έρχεται αλλά μόνο όσες «ακούνε» εκείνη τη στιγμή.

- *Το κόστος της μετάβασης θα είναι υψηλό:* Στις περιπτώσεις που το υλικό δεν είναι συμβατό, ή δεν μπορεί να αναβαθμιστεί ώστε να είναι συμβατό με IPv6, πράγματι η μετάβαση θα είναι ακριβή. Το μεγάλο πρόβλημα όμως παραμένει στους ISP(Internet Service Providers) και στις μεγάλες επιχειρήσεις που έχουν μεγάλους και ακριβούς δρομολογητές. Όμως οι «δρομολογητές αιχμής» έχουν σχετικά μικρή «οικονομική ζωή», και σε λίγα χρόνια το κόστος δε θα αποτελεί πρόβλημα εκτός και αν συνεχιστεί η αγορά υλικού συμβατού μόνο με IPv4. Για τις μικρότερες δικτυακές συσκευές που δεν μπορούν να αναβαθμιστούν, είτε είναι πολύ φθηνή η αγορά καινούριων είτε μπορούν να χρησιμοποιηθούν οι μηχανισμοί μετάβασης που συζητιούνται αργότερα. Το μόνο κόστος που απομένει είναι αυτό της εκπαίδευσης προσωπικού.

4.3 Συνοπτικά οι κυριότερες διαφορές

Διαφορές	IPv4	IPv6
Χώρος διευθύνσεων	32 bits	128 bits
Υποστήριξη IPSec	Προαιρετικό	Απαιτούμενο
Διαμόρφωση των διευθύνσεων IP	Χειροκίνητος ή μέσω DHCP	Autoconfiguration - DHCP δεν απαιτείται πλέον.
Αναγνώριση πακέτων ροής QoS στο χειρισμό της κεφαλίδας	Δεν τα εντοπίζει	υπάρχει χειρισμός μέσω ενός τομέα
Broadcast διευθύνσεις	Οι Broadcast διευθύνσεις χρησιμοποιούνται για τη μετάδοση κίνησης σε όλους τους κόμβους σε ένα συγκεκριμένο υποδίκτυο.	Οι Broadcast διευθύνσεις έχουν αντικατασταθεί από ένα σύνδεσμο.
Fragmentation	Εκτελούνται από τον οργανισμό αποστολής και υποδοχής, σε δρομολογητές.	Πραγματοποιείται από την αποστολή υποδοχής.
Επανασυναρμολόγηση	576-byte	1500-byte
ARP	Χρησιμοποιείται	Δεν χρησιμοποιείται
ICMP Router Discovery	Χρησιμοποιείται	Αντικαταστάθηκε με ICMPv6 Router
Internet Group Management Protocol (IGMP)	Χρησιμοποιείται για τη διαχείριση των ομάδων στο τοπικό υποδίκτυο	Αντικαταστάθηκε με Multicast
Header checksum	Χρησιμοποιείται	Δεν χρησιμοποιείται

Π4.3.1 Κύριες διαφορές μεταξύ IPv6 και IPv4

Κεφάλαιο 5^{ο} – Καινοτομίες της IPv6

5.1.1 Εισαγωγή στην IPSec

Οι δημιουργοί του IPv4 δεν είχαν στο επίκεντρο την ασφάλεια. Το Ιντερνέτ στο αρχικό του στάδιο χρησιμοποιούταν μόνο από λίγα ασφαλή δίκτυα ερευνητών. Οι διαχειριστές αυτών των δικτύων , καθώς και αυτοί που είχαν πρόσβαση στις πληροφορίες που διακινούνταν ήταν απόλυτα έμπιστοι και δεν υπήρχε καμία περίπτωση επικίνδυνης συμπεριφοράς. Έτσι δεν εισάχθηκε κανένα πεδίο ασφάλειας για τις εκάστοτε εφαρμογές στην αρχιτεκτονική του πρωτοκόλλου. Πολλά χρόνια αργότερα, καθώς το IPv4 είχε ευρέως εξαπλωθεί, εισήχθηκε η IPsec. Όμως έπρεπε να εισαχθεί σε πληθώρα ήδη υπαρχόντων εφαρμογών. Έτσι, αντιμετώπισε πολλά θέματα συμβατότητας και απόδοσης σε πολλές περιπτώσεις. Σε αντίθεση με αυτό, στο IPv6 από την αρχή υπήρξε η γραμμή να εισαχτεί στο βασικό πρωτόκολλο ένα πεδίο ασφαλείας που θα είναι λειτουργικό σε κάθε πλατφόρμα του Ιντερνέτ.

5.1.2 Ορισμός της IPSec

Η IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών. Είναι βασισμένο στις προδιαγραφές που ανέπτυξε η ομάδα εργασίας του Internet (IETF). Η IPSec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο. Η IPSec παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφάλειας σε ένα δίκτυο. Έλεγχοι κρυπτογράφησης και πιστοποίησης ταυτότητας μπορούν να εφαρμοσθούν σε διάφορα επίπεδα στην δικτυακή υποδομή.

Πριν την άφιξη της IPSec στο προσκήνιο, εφαρμόζονταν αποσπασματικές λύσεις που αντιμετώπιζαν μέρος μόνο του προβλήματος. Για παράδειγμα, το SSL(Secure Sockets Layer) παρέχει κρυπτογράφηση σε επίπεδο εφαρμογής για Web browsers και άλλες εφαρμογές. Το SSL προστατεύει την πιστότητα των δεδομένων που στέλνονται από κάθε εφαρμογή που το χρησιμοποιεί, αλλά δεν προστατεύει τα δεδομένα που αποστέλλονται από άλλες εφαρμογές.

Κάθε σύστημα και εφαρμογή πρέπει να είναι προστατεμένη από το SSL για να του παρέχει το τελευταίο την προστασία.

Η IPSec υλοποιεί κρυπτογράφηση και πιστοποίηση επιπέδου δικτύου, παρέχοντας μια λύση ασφαλείας μέσα στην ίδια την αρχιτεκτονική του δικτύου. Έτσι τα συστήματα και οι εφαρμογές που βρίσκονται στις άκρες δεν χρειάζονται αλλαγές ή ρυθμίσεις για να έχουν το πλεονέκτημα της ισχυρής ασφάλειας. Επειδή τα κρυπτογραφημένα πακέτα μοιάζουν με κανονικά IP πακέτα μπορούν εύκολα να δρομολογηθούν μέσα από οποιοδήποτε IP δίκτυο, όπως το Internet, χωρίς καμία αλλαγή στον ενδιάμεσο δικτυακό εξοπλισμό. Οι μόνες συσκευές οι οποίες γνωρίζουν για την κρυπτογράφηση είναι αυτές στα ακραία σημεία. Αυτό το χαρακτηριστικό μειώνει δραστικά τόσο το κόστος της υλοποίησης όσο και το κόστος της διαχείρισης.

5.1.3 Λεπτομέρειες της IPSec

Η IPSec συνδυάζει τις παραπάνω τεχνολογίες ασφάλειας σε ένα ολοκληρωμένο σύστημα το οποίο παρέχει εμπιστευτικότητα, ακεραιότητα και πιστοποίηση της ταυτότητας των IP πακέτων. Η IPSec αναφέρεται και σε μια σειρά άλλων πρωτοκόλλων όπως ορίζεται στα RFC 1825-1829 και σε άλλες δημοσιεύσεις στο Internet.

Αυτές οι προδιαγραφές περιλαμβάνουν:

- Κατάλληλο IP πρωτόκολλο ασφαλείας. Ρόλος του είναι να καθορίζει την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι πιστότητας, ακεραιότητας και πιστοποίησης ταυτότητας, όπως επίσης καθορίζει και το πως πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου.

- Διαχείριση κλειδιών. Οι περισσότεροι από τους μηχανισμούς ασφαλείας που παρέχονται από την IPsec απαιτούν την χρήση κλειδιών κρυπτογράφησης. Ένα ξεχωριστό τμήμα τέτοιων μηχανισμών έχει δημιουργηθεί για διαχειρίζεται τα κλειδιά αυτά. Ο μηχανισμός αυτός ονομάζεται Internet Key Exchange (IKE). Δεν είναι απαραίτητο να χρησιμοποιηθεί το IKE, αλλά το να ρυθμιστούν χειροκίνητα οι συσχετισμοί ασφάλειας είναι μια δύσκολη και επίπονη διαδικασία. Το IKE πρέπει να χρησιμοποιείται στις περισσότερες εφαρμογές για να ενεργοποιεί ασφαλείς επικοινωνίες μεγάλης κλίμακας. Δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι

μεταξύ δύο κόμβων και κατόπιν διαπραγματεύεται τους συσχετισμούς ασφάλειας για την IPSec. Αυτή η διαδικασία απαιτεί από τους δύο κόμβους να πιστοποιήσουν ο ένας τον άλλον και να μοιράσουν κλειδιά.

- Πακέτα IPSec. Η IPSec ορίζει ένα νέο σετ επικεφαλίδων το οποίο προστίθεται στα IP πακέτα. Αυτές οι νέες επικεφαλίδες τοποθετούνται μετά την επικεφαλίδα IP και πριν το πρωτόκολλο επιπέδου 4 (τυπικά το TCP ή το UDP).

Αυτές οι νέες επικεφαλίδες παρέχουν πληροφορίες για την ασφάλεια του φορτίου των IP πακέτων όπως αναλύεται παρακάτω:

- Η επικεφαλίδα πιστοποίησης ταυτότητας (AH - Authentication Header) διασφαλίζει την ακεραιότητα και την ταυτότητα των δεδομένων που διακινούνται. Δεν παρέχει ασφάλεια πιστότητας. Η επικεφαλίδα αυτή τοποθετείται μεταξύ της IPv6 επικεφαλίδας και επικεφαλίδων υψηλότερου στρώματος (π.χ. TCP, UDP).
- Φορτίο ασφαλείας ενθυλάκωσης (ESP - Encapsulating Security Payload). Προστατεύει την ακεραιότητα και την ταυτότητα των δεδομένων. Τοποθετείται μπροστά από την μετάδοση (π.χ. UDP, TCP), τον έλεγχο του δικτύου (π.χ. ICMP) ή την επικεφαλίδα του πρωτοκόλλου δρομολόγησης.

Η IPSec παρέχει δυο καταστάσεις λειτουργίας: την transport και την tunnel:

- Στην κατάσταση transport,οι συσχετισμοί ασφάλειας γίνονται μεταξύ των δύο κόμβων που επικοινωνούν. Μόνο το IP φορτίο κρυπτογραφείται, ενώ οι αρχικές επικεφαλίδες μένουν ανέπαφες. Αυτή η κατάσταση λειτουργίας έχει το πλεονέκτημα της πρόσθεσης μόνο μερικών Bytes σε κάθε πακέτο. Επιπλέον, επιτρέπουν σε συσκευές στο δημόσιο δίκτυο να βλέπουν την τελική πηγή και τον προορισμό του πακέτου. Επιτρέπει ειδική επεξεργασία (για παράδειγμα QoS) στο ενδιάμεσο δίκτυο, βασισμένη στην πληροφορία που βρίσκεται στην IP επικεφαλίδα. Ωστόσο, η επικεφαλίδα θα κρυπτογραφηθεί περιορίζοντας τη δυνατότητα έρευνας των πακέτων.

- Στην κατάσταση λειτουργίας tunnel, οι συσχετισμοί ασφαλείας γίνονται μεταξύ δύο ασφαλών πυλών. Όλο το πακέτο κρυπτογραφείται, συμπεριλαμβανομένης και της βασικής

επικεφαλίδας και γίνεται το φορτίο ενός καινούριου IP πακέτου το οποίο έχει κρυπτογραφηθεί και έχει προστεθεί σε αυτό μια καινούρια επικεφαλίδα. Αυτή είναι η αρχή λειτουργίας για ένα ιδιωτικό εικονικό δίκτυο (VPN). Αυτή η κατάσταση λειτουργίας επιτρέπει σε μια δικτυακή συσκευή, όπως ένας δρομολογητής, να ενεργήσει σαν ένας IPSec proxy. Αυτό σημαίνει ότι ο δρομολογητής πραγματοποιεί κρυπτογράφηση για λογαριασμό των υπολογιστών του δικτύου. Η πηγή του δρομολογητή κρυπτογραφεί τα πακέτα και τα προωθεί στο IPSec tunnel. Ο προορισμός του δρομολογητή αποκρυπτογραφεί το αρχικό IP διάγραμμα και το προωθεί στο σύστημα προορισμού του. Το βασικό πλεονέκτημα αυτής της κατάστασης λειτουργίας είναι ότι τα ακραία συστήματα δεν χρειάζεται να ρυθμιστούν για να επικαρπωθούν τα πλεονεκτήματα της IPSec. Η κατάσταση λειτουργίας tunnel προστατεύει επιπλέον το σύστημα από την διαδικασία της ανάλυσης κίνησης. Σε αυτή την κατάσταση λειτουργίας ο επιτιθέμενος μπορεί να καθορίσει μόνο τα ακραία σημεία του tunnel και όχι την πραγματική πηγή και τον προορισμό των πακέτων που κυκλοφορούν μέσα σε αυτό, ακόμη και αν είναι τα ίδια με τα ακραία σημεία του tunnel.

Η κατάσταση λειτουργίας transport, μπορεί να χρησιμοποιηθεί μόνο όταν τόσο η πηγή, όσο και τα συστήματα προορισμού είναι συμβατά με την IPSec. Στις περισσότερες περιπτώσεις έχουμε όμως, έχουμε εφαρμογή της IPSec σε κατάσταση λειτουργίας tunnel. Έχουμε έτσι τη δυνατότητα να υλοποιήσουμε την IPSec στη δικτυακή υποδομή χωρίς να τροποποιήσουμε το λειτουργικό σύστημα ή οποιαδήποτε εφαρμογή στους servers και τους υπολογιστές του δικτύου.

5.1.4 Αλληλεπίδραση της IPsec με τα στοιχεία του IPv6

Η παρουσία της IPsec στο IPv6 είναι ένα μεγάλο βήμα για την ασφάλεια στο Ιντερνέτ. Υπάρχουν όμως κάποιες περιοχές που η IPsec δεν μπορεί εύκολα να συνυπάρξει με άλλες υπηρεσίες:

- Tunneling. Ένα στοιχείο της IPsec και πολλαπλοί μηχανισμοί μετάδοσης, δημιουργούν δυσκολίες για τα υπάρχοντα firewalls και τους διόδους ασφαλείας στο σύνολο του δικτύου. Ένα κρυπτογραφημένο IPsec τούνελ χτισμένο μέσα από ένα firewall προσφέρει από άκρη σ' άκρη ασφάλεια στους κόμβους της κάθε πλευράς, ενώ είναι απίθανο για το firewall να εντοπίσει πιθανές απειλές. Για να λυθεί αυτό το θέμα, ο μηχανισμός έπρεπε να εστιάσει μεταξύ των πυλών ασφαλείας και όχι μεταξύ των κόμβων. Ένα ακόμη πρόβλημα που έπρεπε να λυθεί ήταν ότι ξεχωριστά, το κάθε πακέτο μπορεί να έχει περιεχόμενο που μπορεί να αποτελεί απειλή για όλο το

δίκτυο. Αυτό θα μπορούσε να είναι πληροφορίες δρομολόγησης ή μηνύματα διαχείρισης του δικτύου.

- Ένα παρόμοιο πρόβλημα δημιουργείται με την χρήση του NAT, ειδικά σε περιπτώσεις που θα θέλαμε να χρησιμοποιούνταν η IPsec (π.χ. η πρόσβαση στο δίκτυο της επιχείρησης μας από το σπίτι). Το NAT κάνει μετάφραση της IP, αλλά σε πολλές περιπτώσεις και στην επικεφαλίδα. Αυτό προκαλεί προβλήματα όταν χρησιμοποιείται κρυπτογράφηση ή πιστοποίηση ταυτότητας. Στο μέλλον, όταν θα έχει γίνει η μετάβαση στο IPv6 δίκτυο το πρόβλημα θα εξαφανιστεί.

- Η ποιότητα υπηρεσίας (QoS), επιτρέπει στους router να σβήνουν πακέτα πληροφορίας σε διάφορα πεδία (π.χ. κλάσης και του πεδίου ροής). Η απώλεια πακέτων είναι μεγάλο πλήγμα στην ασφάλεια για την IPsec. Αυτή η κατάσταση μπορεί να οδηγήσει σε ένα αποτέλεσμα όπου σημαντικές υπηρεσίες δεν θα μπορούν να εγκατασταθούν.

- Οι επιλογές επέκτασης για την φορητότητα, που συνεχώς αλλάζουν την IP, οδηγούν σε καταστάσεις που είναι δύσκολο να ελεγχθούν από το περιβάλλον της IPsec. Οι δυναμικές διευθύνσεις δημιουργούν δυσκολίες αν χρησιμοποιούνται για έλεγχο ταυτότητας.

5.1.5 Γιατί χρειαζόμαστε την IPSec

Το Internet αποτελεί αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων, της πλαστοπροσωπίας και της άρνησης παροχής υπηρεσιών. Ο στόχος της IPSec είναι η αντιμετώπιση όλων αυτών των προβλημάτων μέσα στην ίδια την υποδομή του δικτύου χωρίς να είναι αναγκαία η εγκατάσταση και η ρύθμιση ακριβών μηχανών και λογισμικού.

Η IPSec παρέχει κρυπτογράφηση στο επίπεδο του IP και για αυτό το λόγο αποτελεί ένα αξιοσημείωτο κομμάτι της συνολικής ασφάλειας. Οι προδιαγραφές της IPSec ορίζουν δύο νέους τύπους δεδομένων στα πακέτα: την επικεφαλίδα πιστοποίησης *(AH-Authentication Header)*, για την παροχή υπηρεσίας ακεραιότητας δεδομένων και το φορτίο ενθυλάκωσης ασφάλειας *(ESP-Encapsulating Security Payload)* το οποίο παρέχει πιστοποίηση ταυτότητας και ακεραιότητα

δεδομένων. Ορίζονται επίσης οι παράμετροι επικοινωνίας μεταξύ δύο συσκευών που είναι η διαχείριση των κλειδιών και η συσχετισμοί ασφάλειας *(security associations)*.

Τα θέματα ασφαλείας που έχει να αντιμετωπίσει η IPsec περιγράφονται παρακάτω:

- *Απώλεια του Απορρήτου (Loss of Privacy*): Κάποιος που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνηση των τελευταίων στο Internet. Αυτή η δυνατότητα είναι ίσως ο μεγαλύτερος ανασταλτικός παράγοντας στις επικοινωνίες μεταξύ των επιχειρήσεων σήμερα. Χωρίς τη χρήση κρυπτογραφικών μεθόδων για κάθε πακέτο πληροφορίας υπάρχει η δυνατότητα ανάγνωσής του για όποιον έχει τα μέσα να το αιχμαλωτίσει. Το CERT (Computer Emergency Response Team Coordination Center) αναφέρεται στα προγράμματα «packet sniffers» ως την πιο συνηθισμένη περίπτωση επίθεσης από αυτές που συναντώνται.

- *Απώλεια της Ακεραιότητας των Δεδομένων (Loss of Data Integrity*): Ακόμα και για δεδομένα που δεν είναι εμπιστευτικά, πρέπει να λαμβάνονται μέτρα διασφάλισης της ακεραιότητάς τους. Μπορεί να μην μας ενδιαφέρει εάν κάποιος «δει» τη κίνηση ρουτίνας της δουλείας μας, αλλά σίγουρα θα μας προβλημάτιζε εάν αυτός αλλοίωνε κατά οποιοδήποτε τρόπο τα δεδομένα αυτά. Για παράδειγμα το να μπορεί κάποιος να πιστοποιεί με ασφάλεια τον εαυτό του στη τράπεζα κάνοντας χρήση ψηφιακών πιστοποιητικών δεν είναι αρκετό εάν η κύρια εργασία του στη τράπεζα θα μπορούσε να αλλοιωθεί με κάποιο τρόπο.

- *Πλαστοπροσωπία (Identity Spoofing) :* Εκτός της προστασίας των ίδιων των δεδομένων, θα πρέπει να παίρνουμε μέτρα ώστε να προστατεύεται και η ταυτότητά μας στο Internet. Ένας εισβολέας μπορεί να αποδειχθεί ικανός να κλέψει τη ταυτότητα κάποιου και έτσι να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες . Πολλά συστήματα ασφάλειας σήμερα, βασίζονται στην IP διεύθυνση για να αναγνωρίσουν μοναδικά τους χρήστες. Τα συστήματα αυτά είναι πολύ εύκολο να ξεγελαστούν και αυτό το γεγονός έχει οδηγήσει σε αναρίθμητες επιθέσεις διαφόρων συστημάτων.

- *Άρνηση Παροχής Υπηρεσιών (Denial-of-Service):* Εφόσον κάποιος οργανισμός εκμεταλλεύεται το Internet, πρέπει να λάβει κάποια μέτρα ώστε να διασφαλίσει τη

διαθεσιμότητα του συστήματός του σε αυτό. Τα τελευταία χρόνια διάφοροι hackers, έχουν βρει αδυναμίες στο πρωτόκολλο TCP/IP, που τους δίνει τη δυνατότητα να «ρίχνουν» τις μηχανές.

5.2.1 Mobile IPv6

Με το IPv4 αλλά και το IPv6, η μάσκα δικτύου αλλάζει κάθε φορά που αλλάζει το σημείο πρόσβασης στο δίκτυο. Όταν ένας κινητός κόμβος αλλάζει το σημείο πρόσβασής του, τότε αλλάζει και η IP διεύθυνσή του, πράγμα που διακόπτει τις TCP και UDP συνδέσεις του. Η χρήση του Mobile IP με το IPv4 έχει σοβαρούς περιορισμούς που το κάνουν ακατάλληλο για ένα παγκόσμιο δίκτυο. Ένας λόγος είναι ο περιορισμένος αριθμός διευθύνσεων. Αν φανταστούμε κάθε έξυπνο τηλέφωνο να έχει και από μία IP διεύθυνση τότε θα τελείωναν και οι τελευταίες διαθέσιμες διευθύνσεις άμεσα. Ο άλλος λόγος είναι ότι η IPv6 που διαθέτει επικεφαλίδες επέκτασης προσφέρει την δυνατότητα να τροποποιηθεί η δρομολόγηση σε ένα κόσμο με κινητά δίκτυα και αυτό είναι απαραίτητο αν θέλουμε να μιλάμε για δυνατότητα σύνδεσης σε τεράστιες μάζες συσκευών. Το γεγονός ότι το IPv6 χρησιμοποιεί το Neighbor Discovery κάνει το IPv6 πιο ανεξάρτητο στο στρώμα της δικτύωσης. Η Mobile IPv6 παίρνει την εμπειρία του IPv4 και τις ανώτερες δυνατότητες που προσφέρει το IPv6.

5.2.2 Λειτουργία του Mobile IPv6

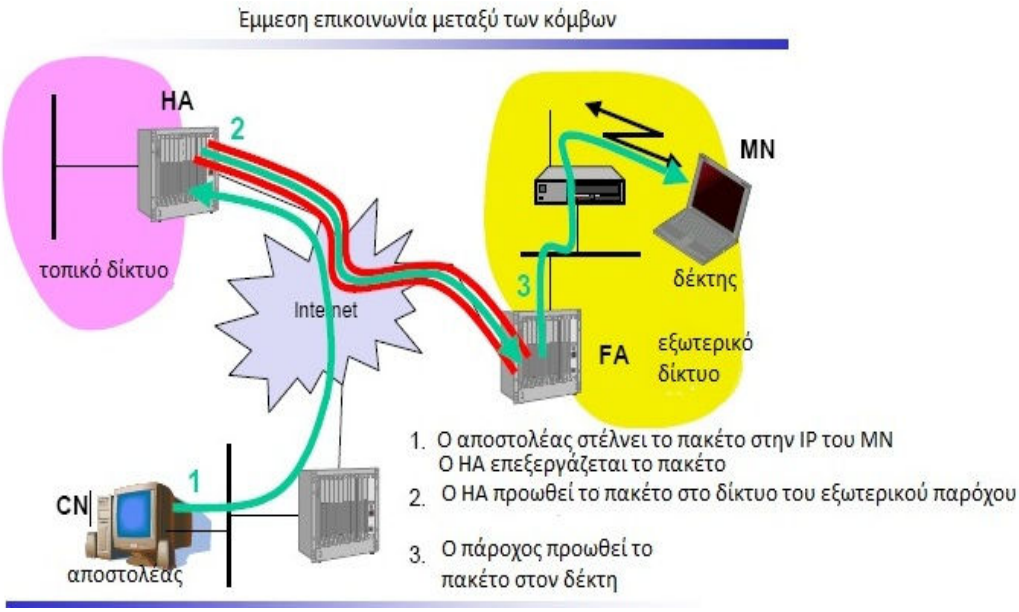
Η κεντρική διεύθυνση είναι η IPv6 διεύθυνση με το πρόθεμα της κεντρικής σύνδεσης ενός κινητού κόμβου (MN). Όσο ο κινητός κόμβος βρίσκεται σπίτι, δέχεται πακέτα μέσω των κανονικών IP μηχανισμών και συμπεριφέρεται σαν ένας κλασσικός κόμβος. Όταν ο κόμβος είναι έξω από το σπίτι και συνδεμένος σε ένα ξένο δίκτυο, έχει την ανάλογη διεύθυνση. Δέχεται την διεύθυνση αυτή από τους IPv6 μηχανισμούς, όπως ο DHCPv6.

Ο συσχετισμό μιας κεντρικής διεύθυνσης (Home address - HA) και μιας εξωτερικής διεύθυνσης ονομάζεται binding. Μακριά από το σπίτι, ο κινητός κόμβος καταγράφει την εξωτερική του διεύθυνση στον router του κεντρικού του δικτύου. Για την καταγραφή της διεύθυνσης ο κόμβος στέλνει ένα μήνυμα στο κεντρικό router και στην συνέχεια αυτός απαντάει ότι πλέον γνωρίζει την νέα εξωτερική διεύθυνση. Κάθε κόμβος που επικοινωνεί με έναν κινητό κόμβο ονομάζεται κόμβος αλληλογραφίας (Correspondent Node-CN). Οι κινητοί κόμβοι μπορούν να κάνουν καταγραφή της εξωτερικής τους διεύθυνσης κατευθείαν στον κόμβο αλληλογραφίας. Ένας

τέτοιος κόμβος δεν αποκλείεται να είναι και αυτός κινητός.

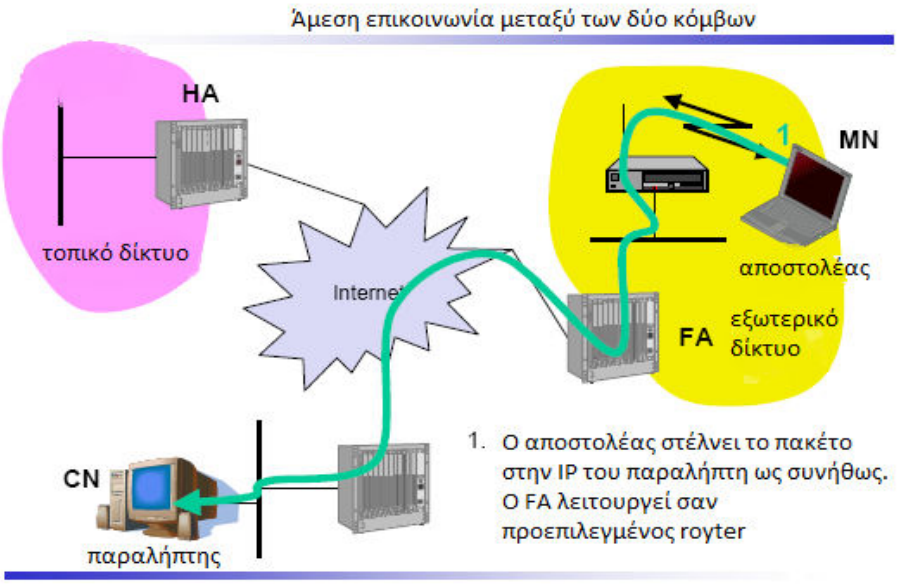
Υπάρχουν δύο τρόποι επικοινωνίας μεταξύ ενός κινητού και ενός κόμβου αλληλογραφίας:

- *Έμμεση επικοινωνία:* Τα πακέτα από τον κόμβο αλληλογραφίας στέλνονται στον κεντρικό πάροχο, αυτός τα μετατρέπει σε IPv6 και τα στέλνει στον κινητό κόμβο. Η αντίθετη διαδικασία γίνεται για να σταλούν πακέτα από τον κινητό κόμβο στον κόμβο αλληλογραφίας. Αυτή η διαδικασία δεν προϋποθέτει την χρήση του Mobile IPv6.



Εικόνα 5.5.1.1 Έμμεση Επικοινωνία Κόμβων

- *Άμεση επικοινωνία:* Η επικοινωνία μεταξύ των δύο κόμβων μπορεί να είναι άμεση χωρίς να γίνεται μέσω του κεντρικού παρόχου. Αυτό είναι και το βασικό πλεονέκτημα της Mobile IPv6 έναντι της Mobile IPv4. Η επιτυχία της σύνδεσης στηρίζεται στην καταχώρηση της εξωτερικής διεύθυνσης του κινητού κόμβου στον κόμβο αλληλογραφίας και η απάντηση από τον δεύτερο ότι τον έχει καταγράψει. Πλεονέκτημα αυτής της επικοινωνίας είναι ότι μπορεί να χρησιμοποιηθεί το συντομότερο μονοπάτι μεταξύ των δύο κόμβων. Σε περίπτωση αλλαγής της διεύθυνσης του κεντρικού παρόχου, ο κινητός κόμβος μπορεί να ενημερωθεί γι' αυτό με την χρήση της Dynamic Home Agent Prefix Discovery.



Εικόνα 5.5.1.2 Άμεση Επικοινωνία Κόμβων

5.2.3 Πλεονεκτήματα του Mobile IPv6

Η υποστήριξη κινητικότητας για τις συσκευές του διαδικτύου είναι δυνατή και προτυποποιημένη και για τις δύο εκδόσεις του πρωτοκόλλου IP, IPv4 και IPv6, αλλά λόγω της διευρυμένης λειτουργικότητας και του μεταγενέστερου σχεδιασμού του IPv6 μερικά χαρακτηριστικά, τα οποία αφορούν την υποστήριξη κινητικότητας έχουν ενσωματωθεί πιο αποτελεσματικά στο Mobile IPv6 σε σχέση με το Mobile IPv4. Ακολουθούν επιγραμματικά τα κύρια πλεονεκτήματα του Mobile IPv6

- Το Mobile IP πρέπει να αναθέτει global IP διευθύνσεις σε έναν φορητό κόμβο σε κάθε σημείο στο οποίο ατός συνδέεται με το διαδίκτυο. Σε ζεύξεις οι οποίες εξυπηρετούν φορητούς κόμβους πρέπει να δεσμευθεί ένα σύνολο IP διευθύνσεων (τουλάχιστο μία), οι οποίες θα ανατεθούν ως care-of διευθύνσεις των φορητών κόμβων. Λόγω της έλλειψης IP διευθύνσεων στο πρωτόκολλο IPv4 μπορεί να υπάρξουν προβλήματα ανικανότητας δέσμευσης αρκετών global

IPv4 διευθύνσεων σε ορισμένες ζεύξεις. Στο πρωτόκολλο IPv6 υπάρχουν αρκετές διαθέσιμες διευθύνσεις.

- Το IPv6 χρησιμοποιώντας διευθύνσεις τύπου anycast επιτρέπει σε έναν κόμβο να στέλνει ένα πακέτο σε κάποιο από τα πολλά συστήματα τα οποία έχουν ανατεθειμένη αυτήν την anycast διεύθυνση σε κάποιο από τα interface τους. Το Mobile IPv6 κάνει αποτελεσματική χρήση αυτού του μηχανισμού, στο μηχανισμό Δυναμικής Ανακάλυψης home agent στέλνοντας ένα Binding Update στην anycast διεύθυνση των home agents και λαμβάνοντας απάντηση από ακριβώς έναν από τους πολλούς home agents. Το IPv4 δεν παρέχει μια τέτοια δυνατότητα.
- Χρησιμοποιώντας μηχανισμούς όπως το stateless address autoconfiguration και το Neighbor Discovery για τη ρύθμιση των παραμέτρων του, το Mobile IPv6 δεν χρειάζεται ούτε το πρωτόκολλο DHCP ούτε foreign agents στις απομακρυσμένες ζεύξεις ώστε να ρυθμιστούν οι care-of διευθύνσεις των φορητών κόμβων του.
- Το Mobile IPv6 μπορεί να χρησιμοποιήσει το IPsec για όλες τις απαιτήσεις ασφάλειας όπως η πιστοποίηση αυθεντικότητας και η προστασία ακεραιότητας δεδομένων.
- Για να αποφύγει τη σπατάλη εύρους ζώνης, λόγω της δρομολόγησης τριγώνου, το Mobile IP καθορίζει μηχανισμούς βελτιστοποίησης διαδρομής (route optimization). Ενώ η βελτιστοποίηση διαδρομής αποτελεί μία επιπρόσθετη λειτουργικότητα για το Mobile IPv4, αποτελεί ένα ενσωματωμένο χαρακτηριστικό στο Mobile IPv6.

Υπάρχουν πολλοί δρομολογητές στο Διαδίκτυο οι οποίοι εκτελούν το λεγόμενο ingress-filtering για τα πακέτα τα οποία πρόκειται να προωθηθούν από αυτούς. Αυτό σημαίνει ότι ελέγχουν αν η διεύθυνση πηγής ενός πακέτου είναι προσβάσιμη από το interface από το οποίο ελήφθη το πακέτο. Το Mobile IPv6 μπορεί να συνυπάρχει με το ingress-filtering χωρίς προβλήματα. Ένας σε μία απομακρυσμένη ζεύξη χρησιμοποιεί την care-of διεύθυνσή του σαν διεύθυνση πηγής των πακέτων του και συμπεριλαμβάνει την home διεύθυνσή του στην επιλογή Home Address. Επειδή η care-of διεύθυνση αποτελεί μια έγκυρη διεύθυνση στην απομακρυσμένη ζεύξη (foreign link) το πακέτο θα περάσει από το μηχανισμό του ingress-filtering χωρίς κανένα πρόβλημα

5.2.4 Σύγκριση Mobile IPv6 και Mobile IPv4

Η σχεδίαση του κινητού IPv6 - Mobile IPv6 – ενισχύθηκε σημαντικά από τις εμπειρίες κατά τη σχεδίαση του Mobile IPv4 καθώς και από τα καινούρια χαρακτηριστικά του νέου πρωτοκόλλου

IPv6. έτσι το Mobile IPv6 έχει αρκετά κοινά χαρακτηριστικά με το Mobile IPv4 αλλά η λειτουργία του έχει ενσωματωθεί στο νέο πρωτόκολλο του στρώματος δικτύου IPv6 και προσφέρει μια σειρά πλεονεκτημάτων. Αυτή η παράγραφος αναφέρεται στις κύριες διαφορές που διέπουν την λειτουργία του Mobile IPv6 και του Mobile IPv4.

- Δεν υπάρχει λόγος να χρησιμοποιηθούν ειδικοί δρομολογητές ως ξένοι ατζέντηδες όπως στο Mobile IPv4. Το Mobile IPv6 λειτουργεί σε κάθε τοποθεσία χωρίς να απαιτείται ειδική υποστήριξη από τον τοπικό δρομολογητή
- Η υποστήριξη για την βέλτιστη δρομολόγηση είναι ένα θεμελιώδες χαρακτηριστικό του πρωτοκόλλου παρά ένα σύνολο από μη στάνταρ επεκτάσεις
- Η βέλτιστη δρομολόγηση στο Mobile IPv6 μπορεί να λειτουργήσει με ασφάλεια ακόμα και χωρίς προκαθορισμένες συσχετίσεις ασφαλείας. Αναμένεται ότι η βέλτιστη δρομολόγηση μπορεί να εφαρμοστεί σε παγκόσμια κλίμακα μεταξύ όλων των κινητών κόμβων και των κόμβων ανταπόκρισης
- Υπάρχει ενσωματωμένη υποστήριξη στο Mobile IPv6 για να επιτρέπει τη συνύπαρξη της βέλτιστης δρομολόγησης με τους δρομολογητές που εκτελούν φίλτρα εισόδου
- Ο μηχανισμός εκτίμησης απροσπέλαστων γειτόνων στο IPv6 επιβεβαιώνει τη συμμετρική προσπέλαση ανάμεσα στον κινητό κόμβο και τον προκαθορισμένο δρομολογητή στην τρέχουσα τοποθεσία
- Τα περισσότερα πακέτα που στέλνονται στον κινητό κόμβο όταν αυτός είναι μακριά από το δίκτυο σπιτιού του στο Mobile IPv6 στέλνονται χρησιμοποιώντας μια επικεφαλίδα δρομολόγησης IPv6 παρά ενθυλάκωση IP, μειώνοντας έτσι το ποσοστό συμφόρησης σε σχέση με το Mobile IPv4
- Το Mobile IPv6 έχει αποσυζευχθεί από οποιοδήποτε πρωτόκολλο του στρώματος ζεύξης δεδομένων καθώς χρησιμοποιεί το πρωτόκολλο εύρεσης γειτόνων του IPv6 αντί του ARP. Αυτό βελτιώνει την ανθεκτικότητα του πρωτοκόλλου

Ο μηχανισμός δυναμικής εύρεσης της διεύθυνσης του ατζέντη σπιτιού στο Mobile IPv6 επιστρέφει μια μόνο απάντηση στον κινητό κόμβο. Η απευθείας προσέγγιση εκπομπής μηνυμάτων που χρησιμοποιείται στο Mobile IPv4 επιστρέφει ξεχωριστές απαντήσεις από τον κάθε ατζέντη σπιτιού

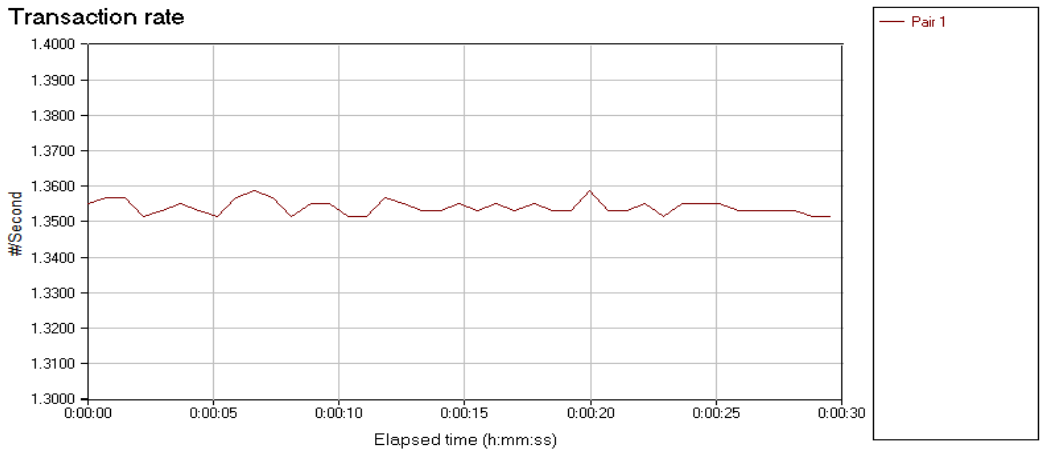
Κεφάλαιο 6ο- Πειραματικό Μέρος

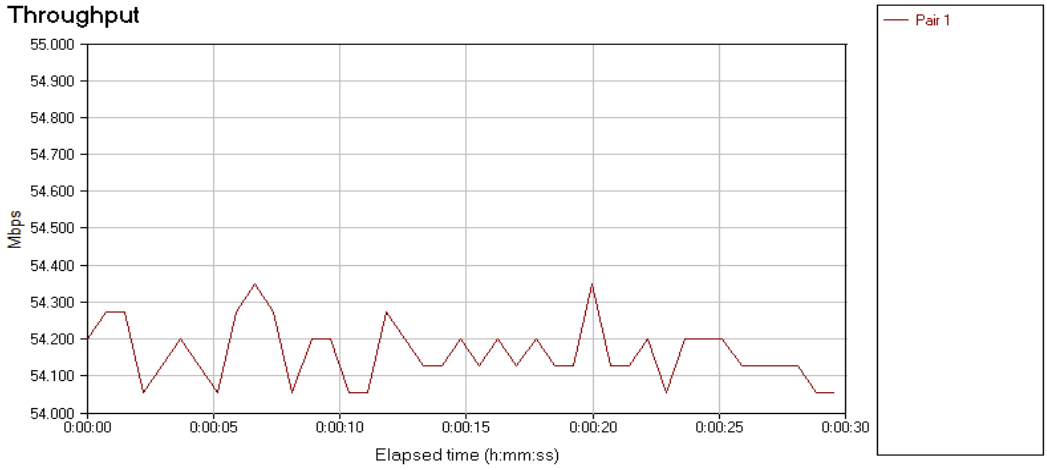
6.1 Διαφορές στην Απόδοση - Μετρήσεις

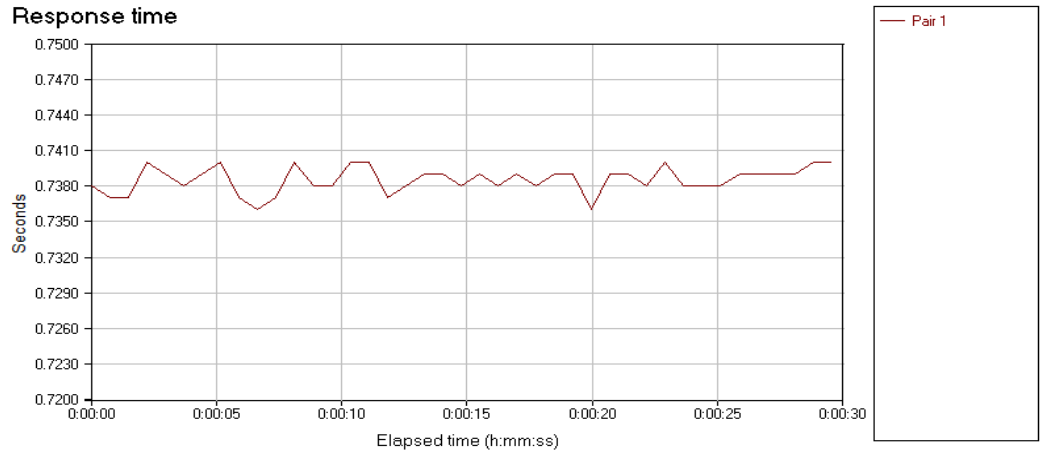
Οι μετρήσεις έγιναν σε εργαστήριο του Τμήματος Ηλεκτρονικής. Βάση των μετρήσεων που παρθήκαν στο τοπικό δίκτυο που στήθηκε, καταλήξαμε στο συμπέρασμα ότι η IPv4 είναι λίγο γρηγορότερη από την IPv6 αλλά δεν υπάρχει τόσο μεγάλη διαφορά ώστε να επισκιάζει τα πολλά θετικά της IPv6. Επίσης, εντοπιστήκαν προβλήματα συμβατότητας με λογισμικό, με λειτουργικό σύστημα όπως και προβλήματα επικοινωνίας με τον πάροχο Ίντερνετ.

6.1.1 Μετρήσεις με το IXIA (Με router 100MBITS)

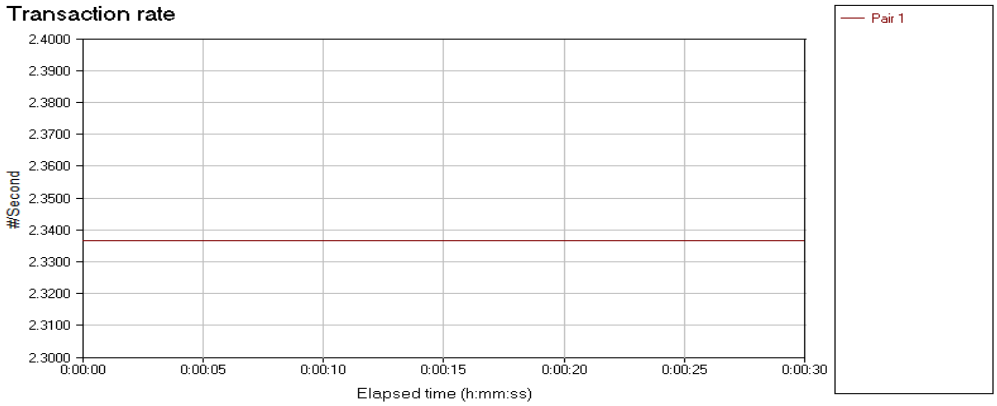
1. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές (Client 11 – Client 12) με UDP IPv6.

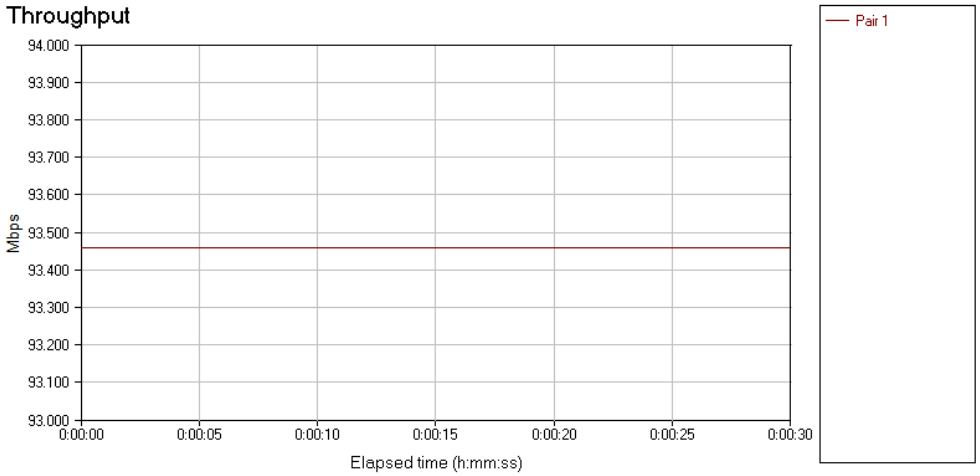


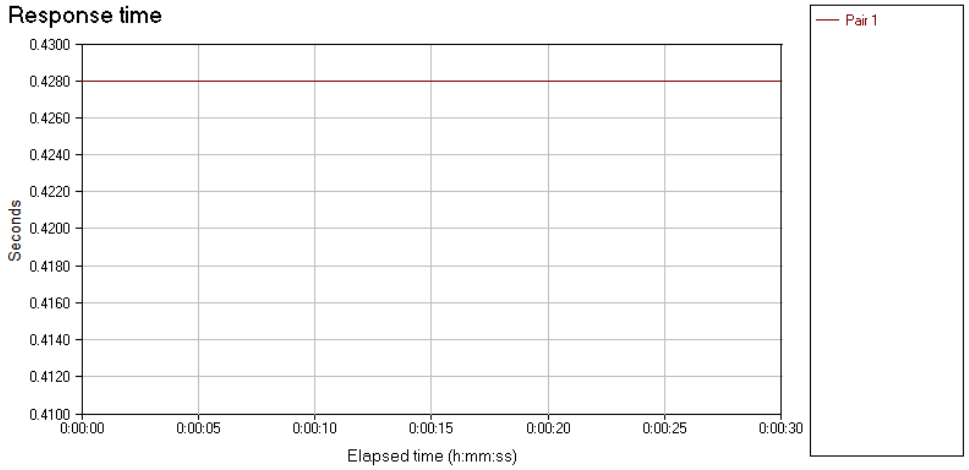




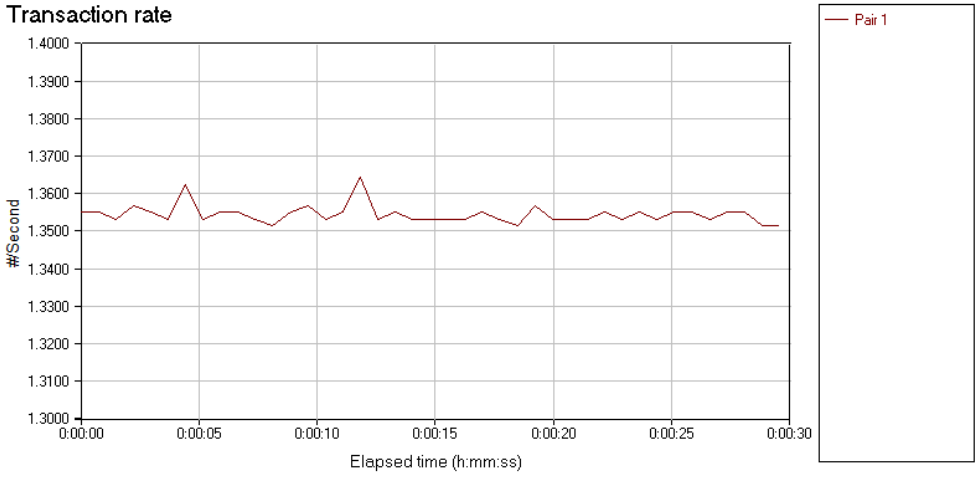
2. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές (Client 11 – Client 12) με TCP IPv6.

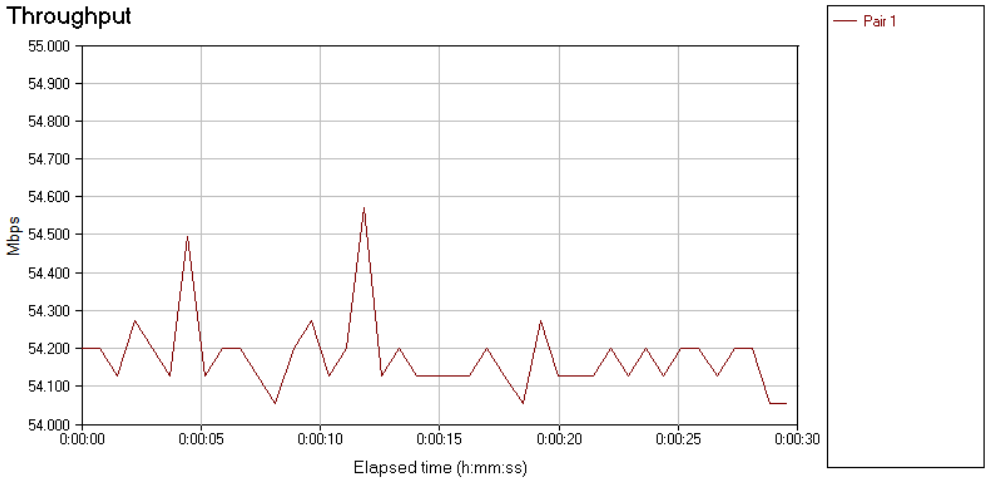


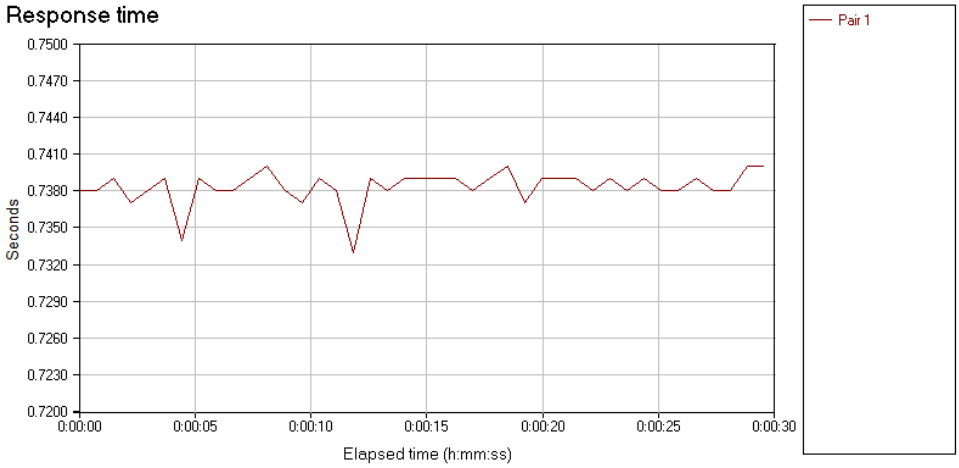




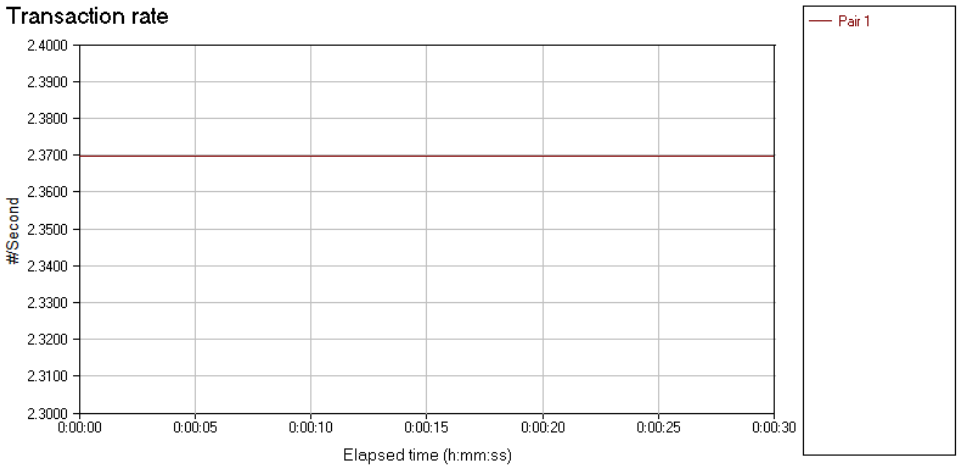
3. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές (Client 11 – Client 12) με UDP IPv4.

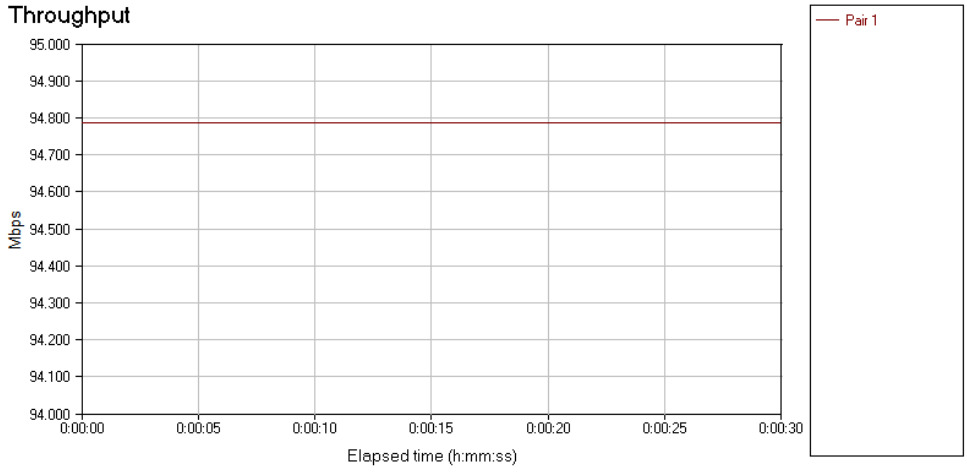


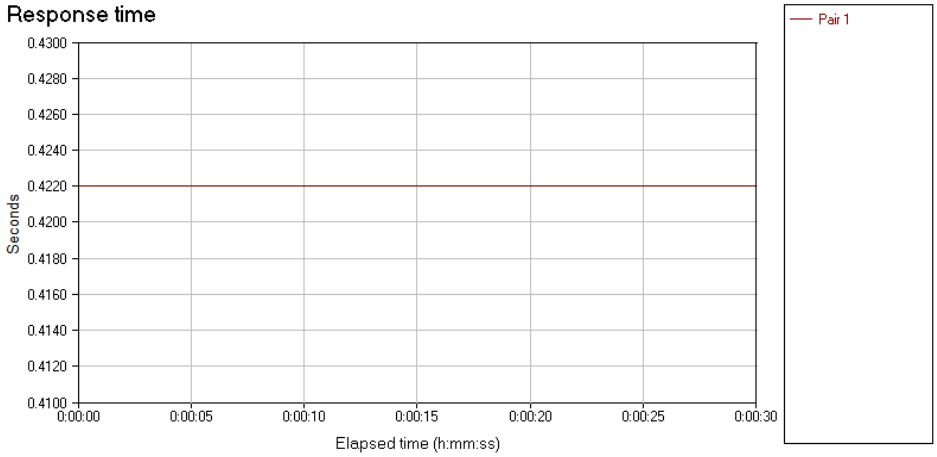




4. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές (Client 11 – Client 12) με TCP IPv4.

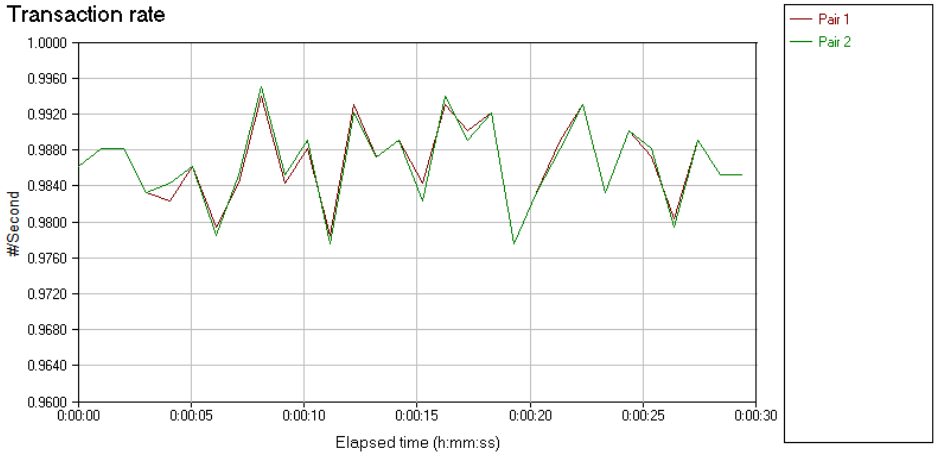


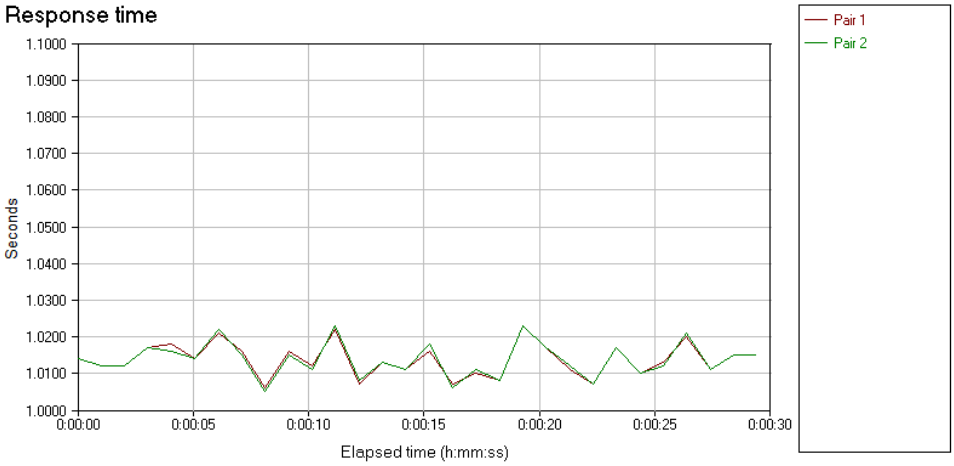


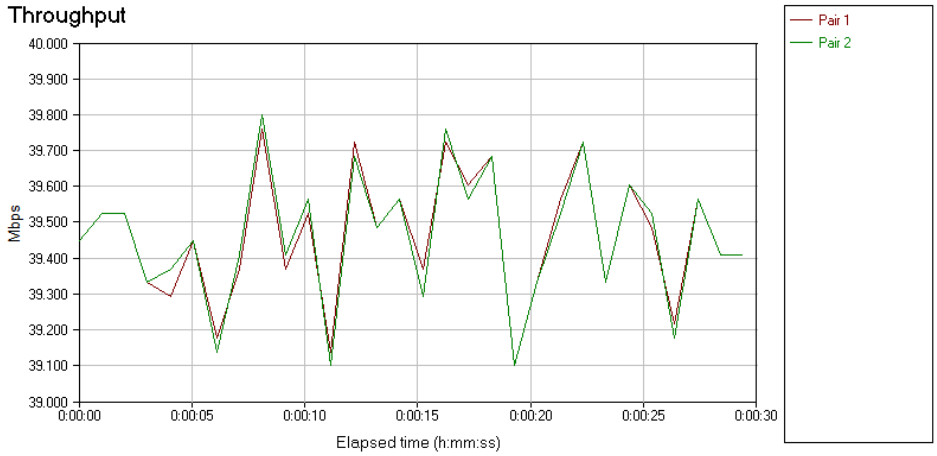


Παρατηρούμε ότι το IPv4 φαίνεται να είναι ελάχιστα ποιο γρήγορο από το IPv6. Επίσης παρατηρούμε ότι το TCP έχει σταθερή ταχύτητα σε αντίθεση με το UDP που έχουμε αυξομειώσεις. Αυτό σημβαίνει επειδή το TCP δεν κάνει έλεγχο των πακέτων που αποστέλονται..

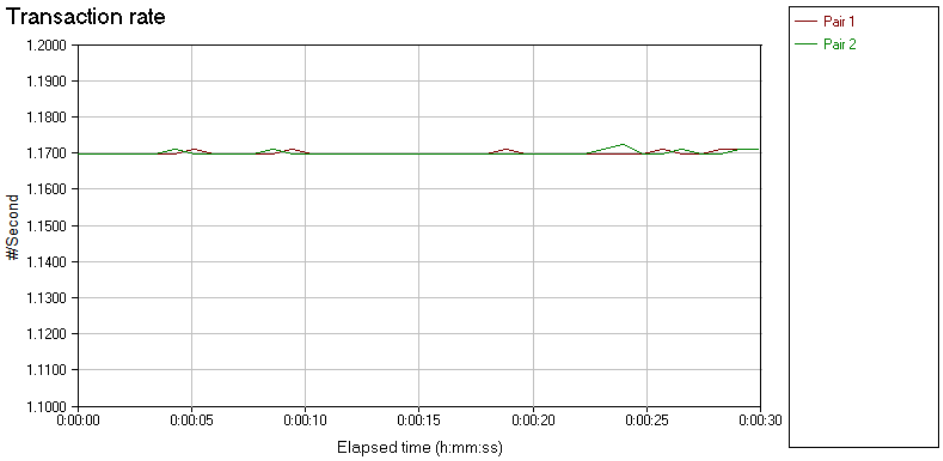
5. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές (Client 11 –> Client 12 και client 13) με UDP IPv6.

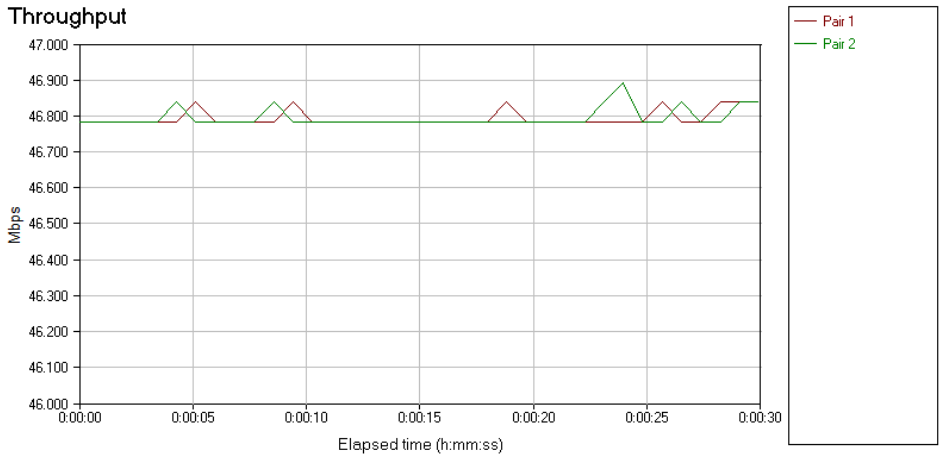

Transaction rate
Pair 1
Pair 2
#/Second
1.0000
0.9960
0.9920
0.9880
0.9840
0.9800
0.9760
0.9720
0.9680
0.9640
0.9600
0:00:00
0:00:05
0:00:10
0:00:15
0:00:20
0:00:25
0:00:30
Elapsed time (h:mm:ss)

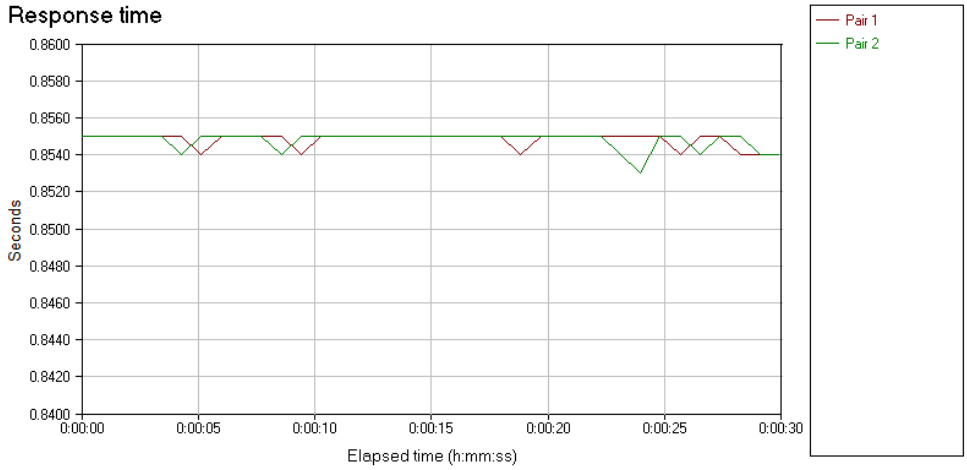

Response time
Pair 1
Pair 2
Seconds
1.1000
1.0900
1.0800
1.0700
1.0600
1.0500
1.0400
1.0300
1.0200
1.0100
1.0000
0:00:00
0:00:05
0:00:10
0:00:15
0:00:20
0:00:25
0:00:30
Elapsed time (h:mm:ss)


Throughput
Pair 1
Pair 2
Mbps
40.000
39.900
39.800
39.700
39.600
39.500
39.400
39.300
39.200
39.100
39.000
0:00:00
0:00:05
0:00:10
0:00:15
0:00:20
0:00:25
0:00:30
Elapsed time (h:mm:ss)

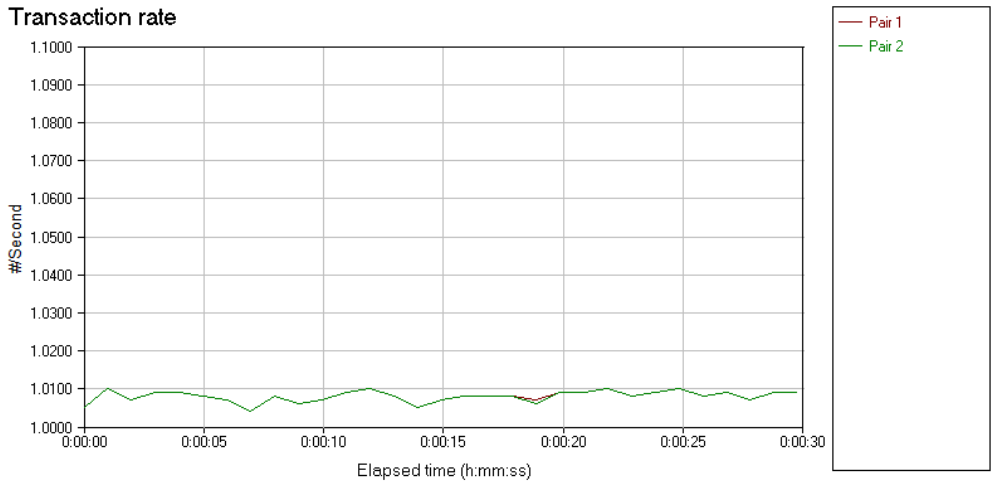
6. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές (Client 11 –> Client 12 και client 13) με TCP IPv6.

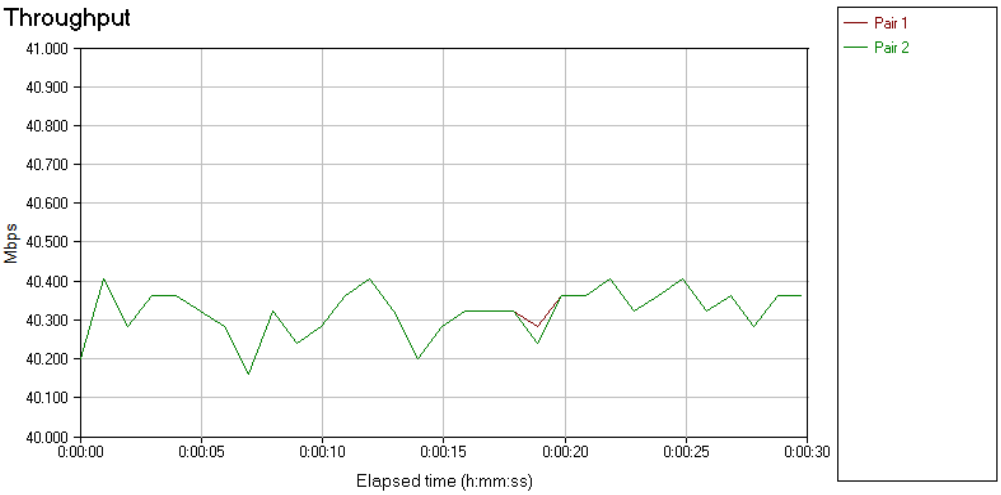


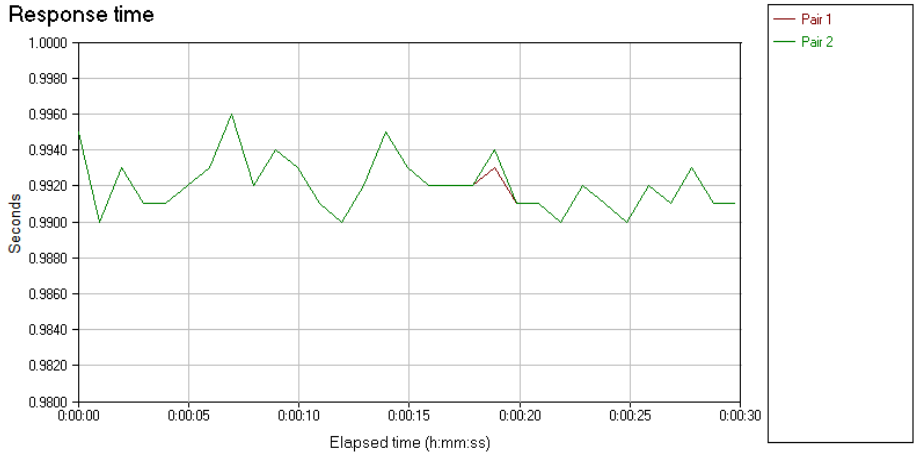




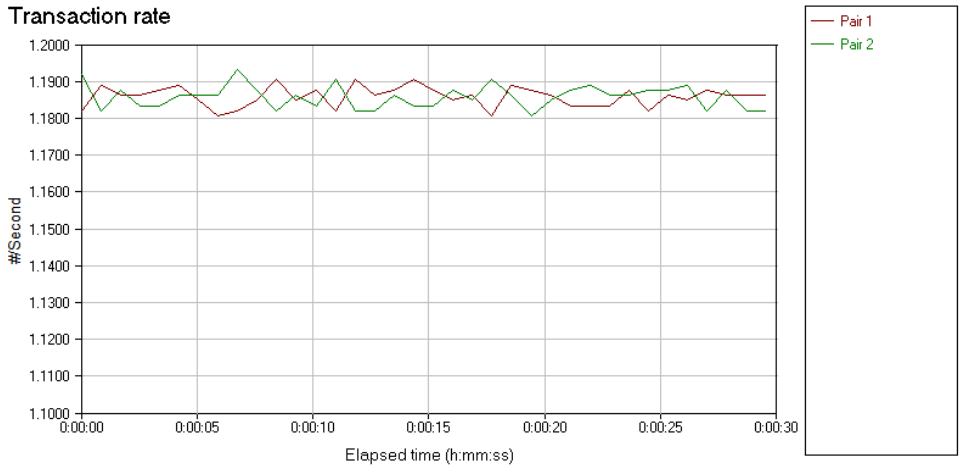
7. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές (Client 11 –> Client 12 και client 13) με UDP IPv4.

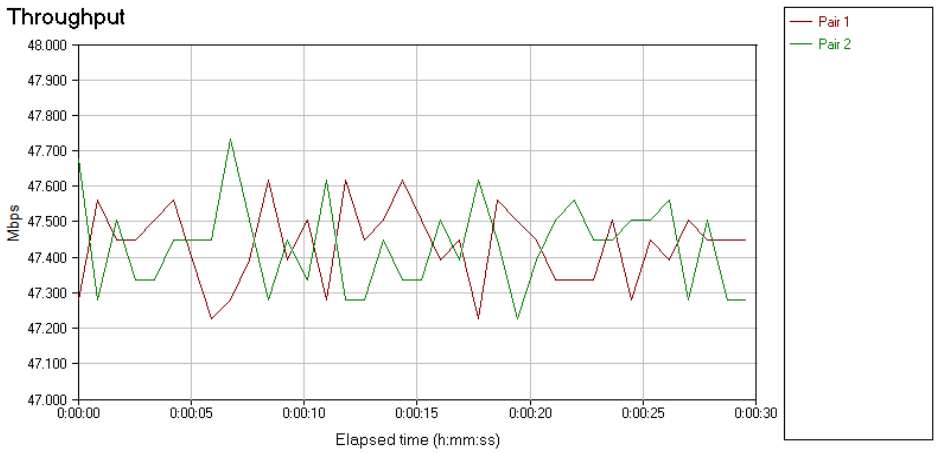


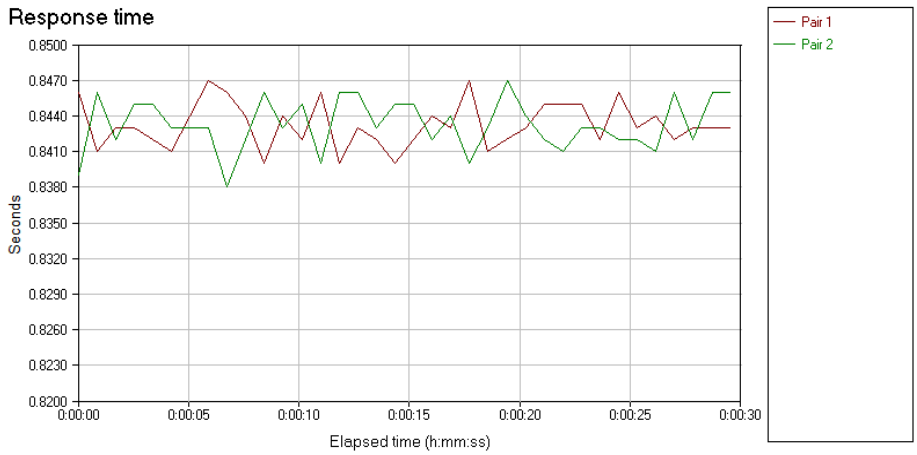




8. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές (Client 11 –> Client 12 και client 13) με TCP IPv4.

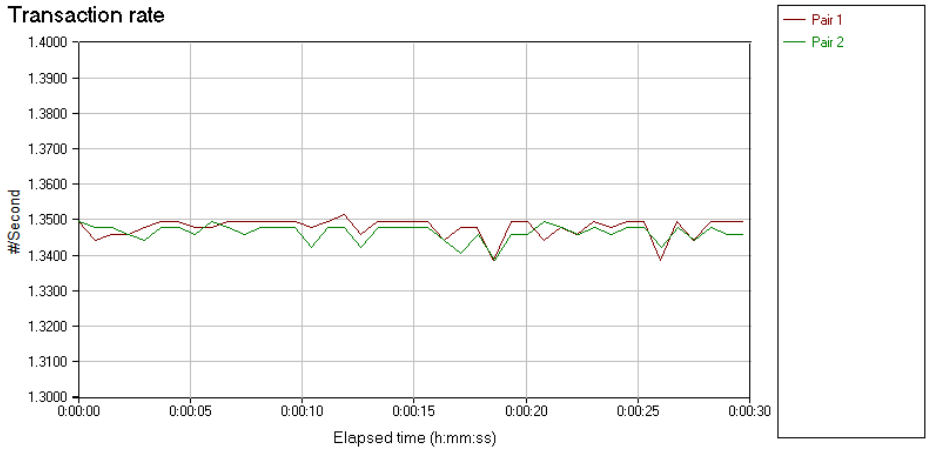


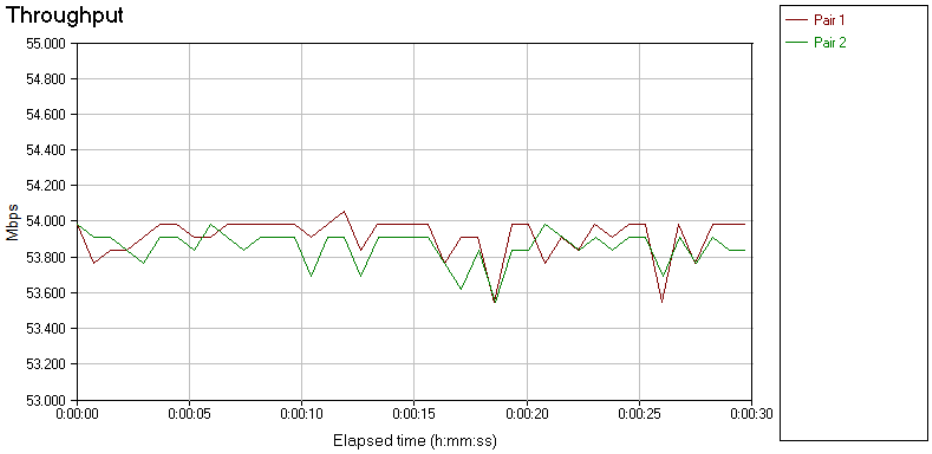


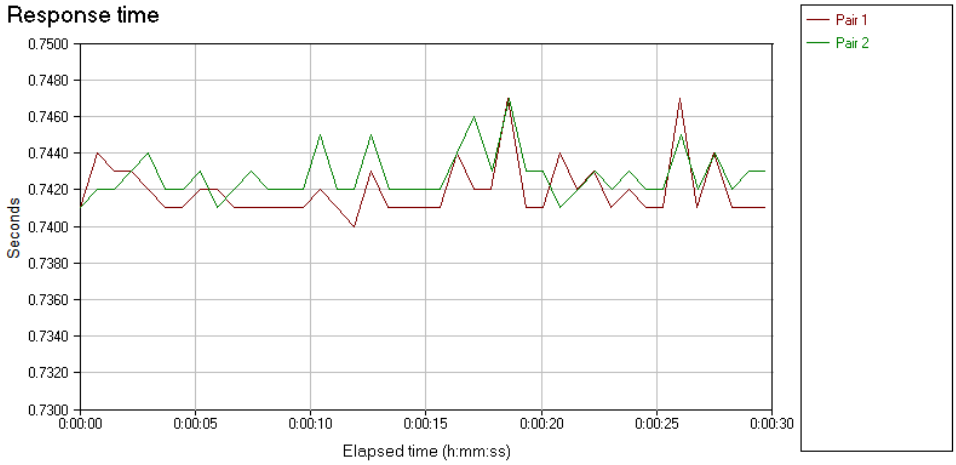


Παρατηρούμε ότι πάλι το IPv4 (TCP) είναι ποιο γρήγορο από το IPv6.

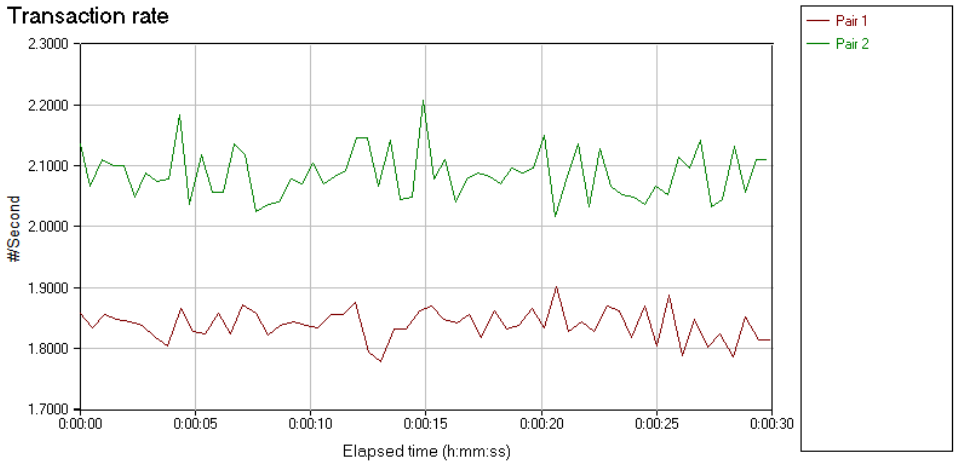
9. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με αμφίδρομη επικοινωνία (Client 11 <–> Client 12) με UDP IPv6.

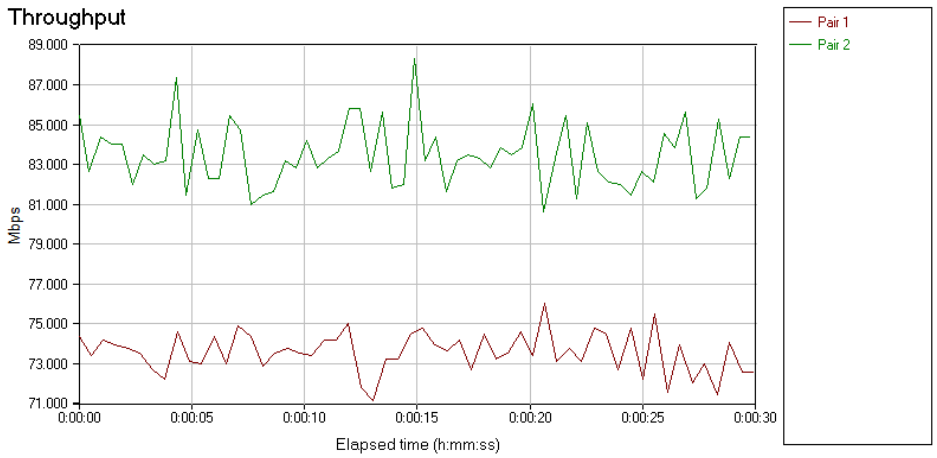


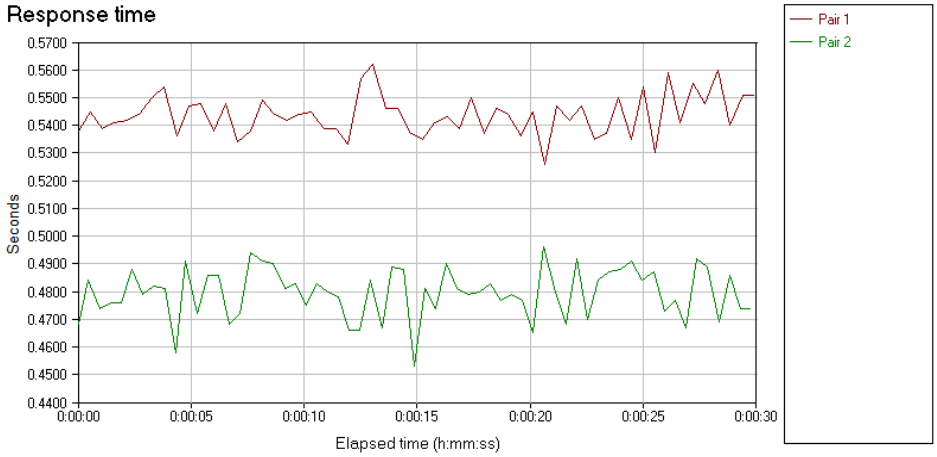




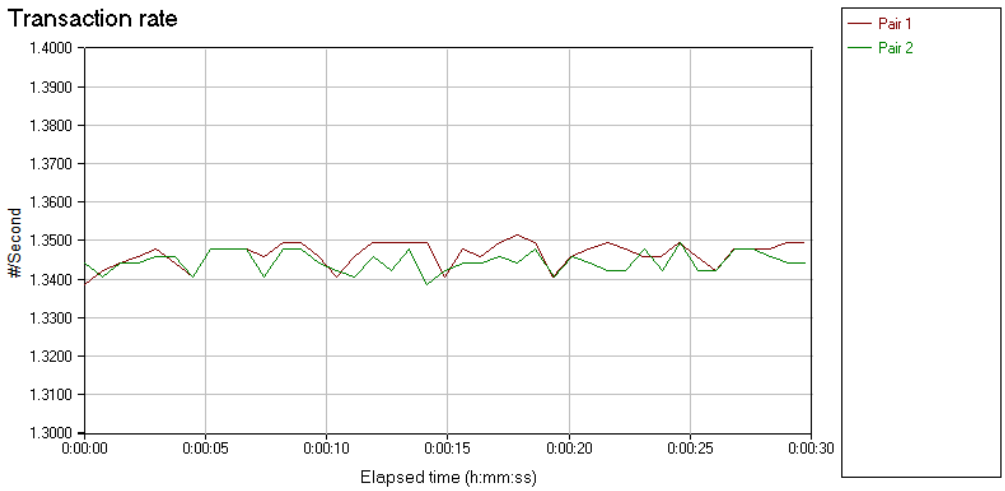
10. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με αμφίδρομη επικοινωνία (Client 11 <–> Client 12) με TCP IPv6

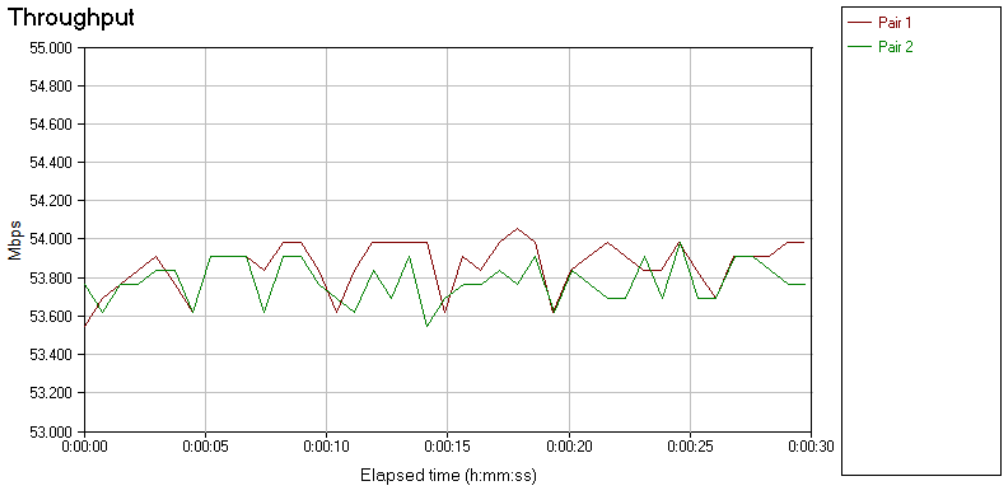


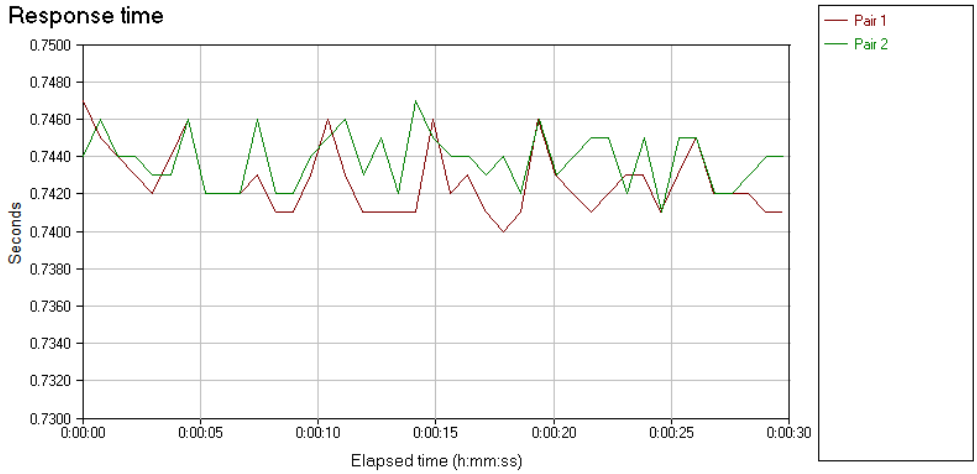




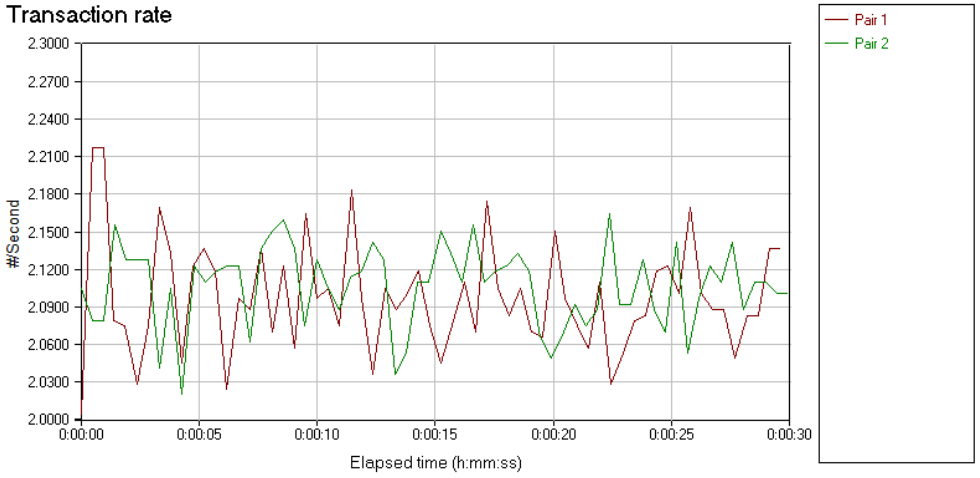
11. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με αμφίδρομη επικοινωνία (Client 11 <–> Client 12) με UDP IPv4

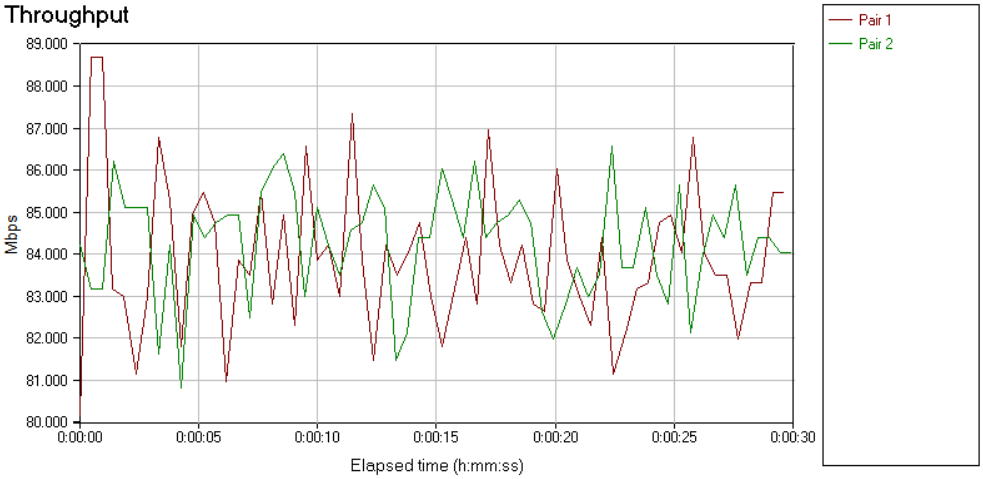


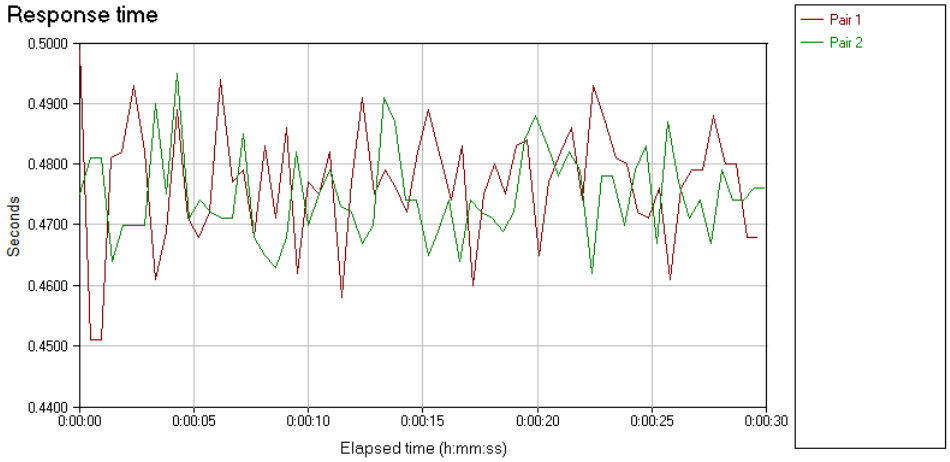




12. `Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με αμφίδρομη επικοινωνία (Client 11 <–> Client 12) με TCP IPv4

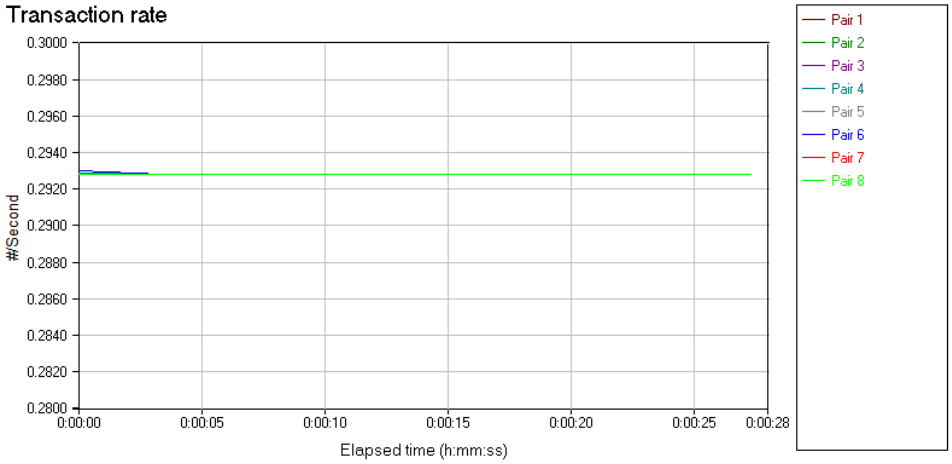


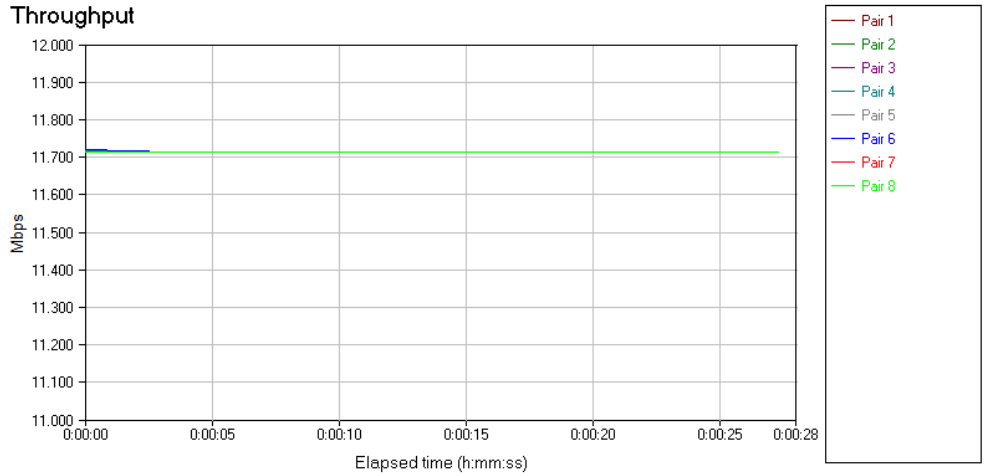


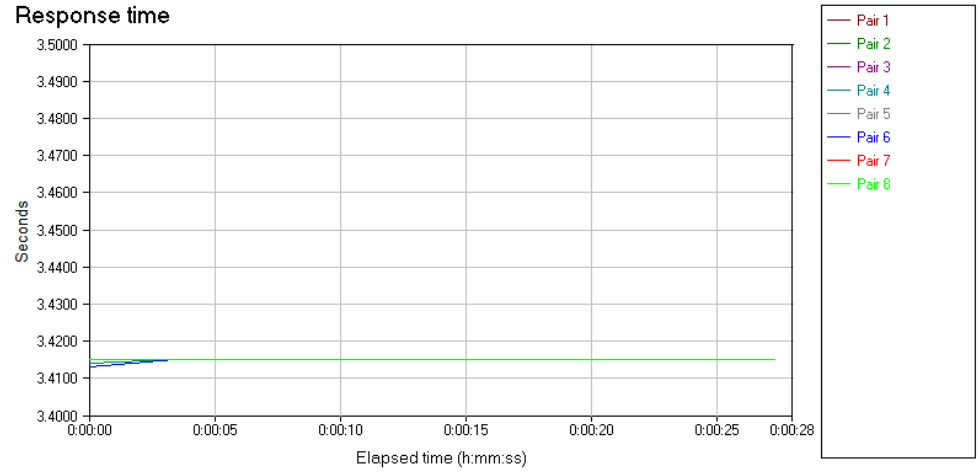


- Παρατηρούμε ότι και πάλι το IPv4 (TCP) είναι ποιο γρήγορο από το IPv6.

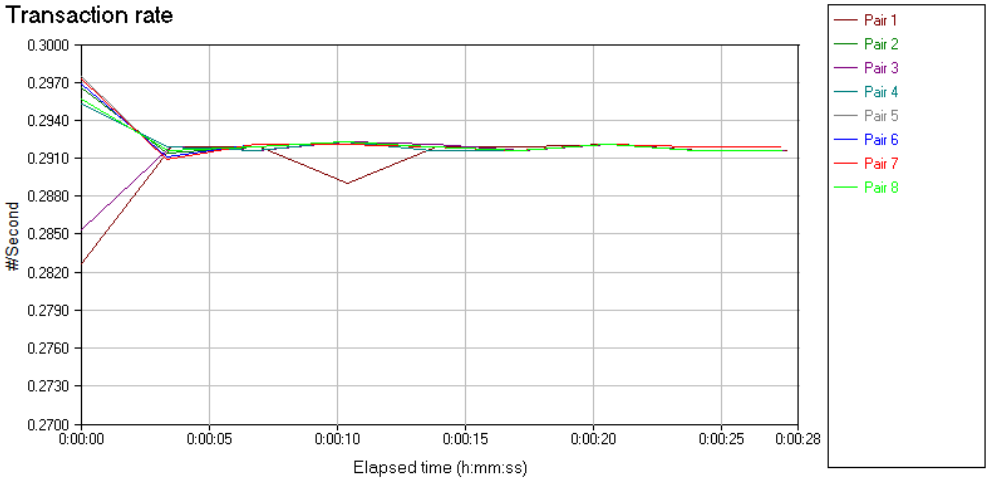
13. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από οχτώ υπολογιστές με επικοινωνία (Server –> Client 11 Client 12 Client 13 Client 14 Client 15 Client 16 Client 17 Client 18) με UDP IPv6

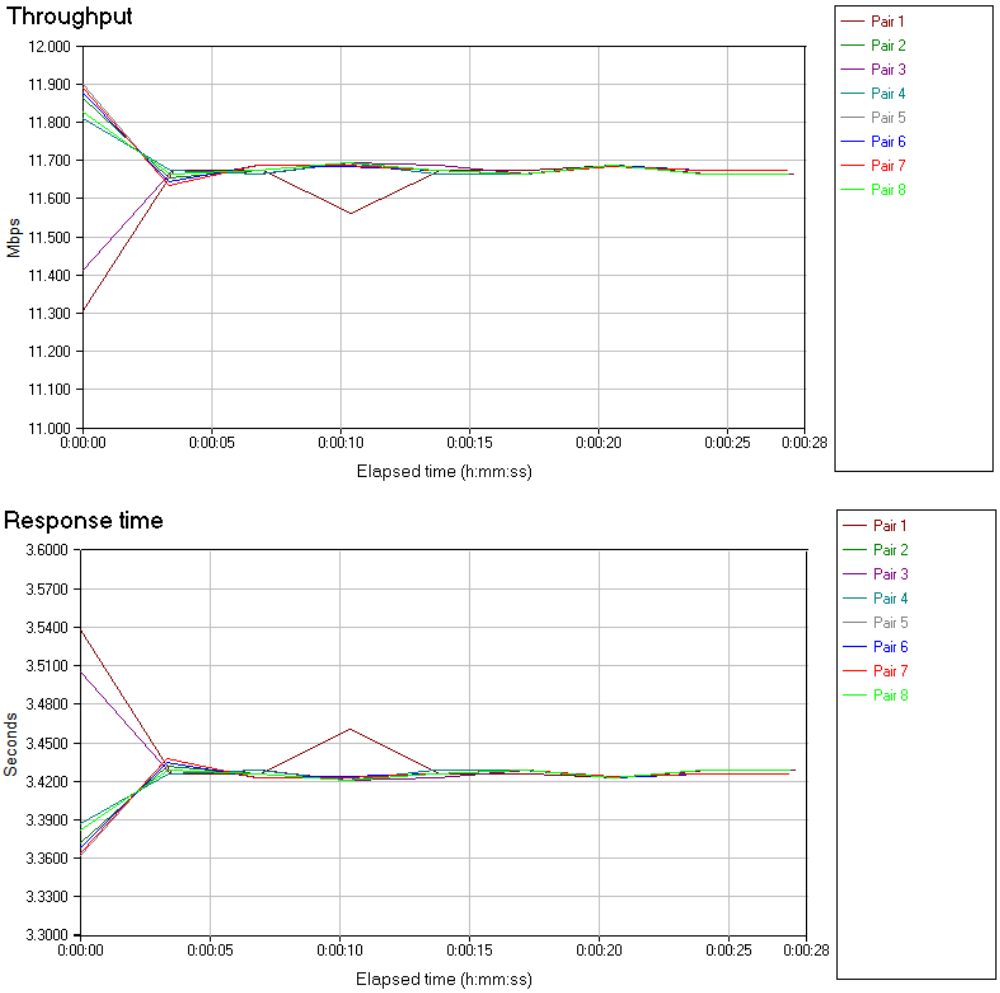




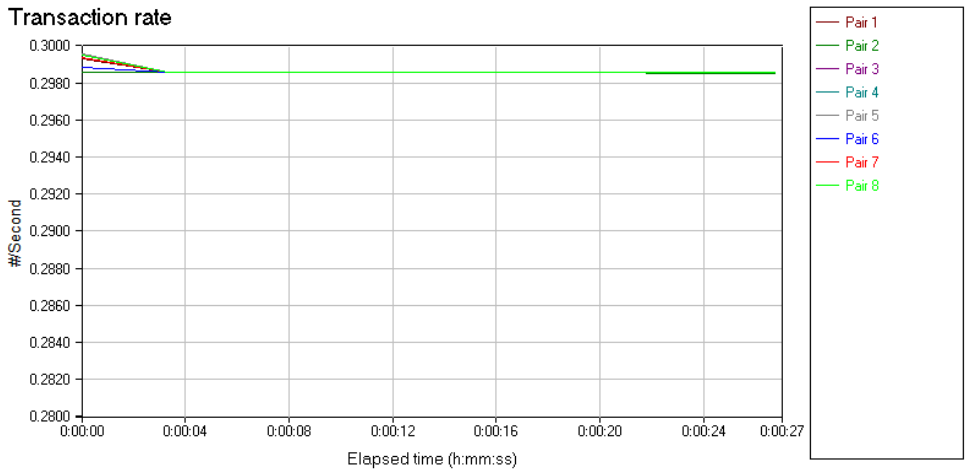


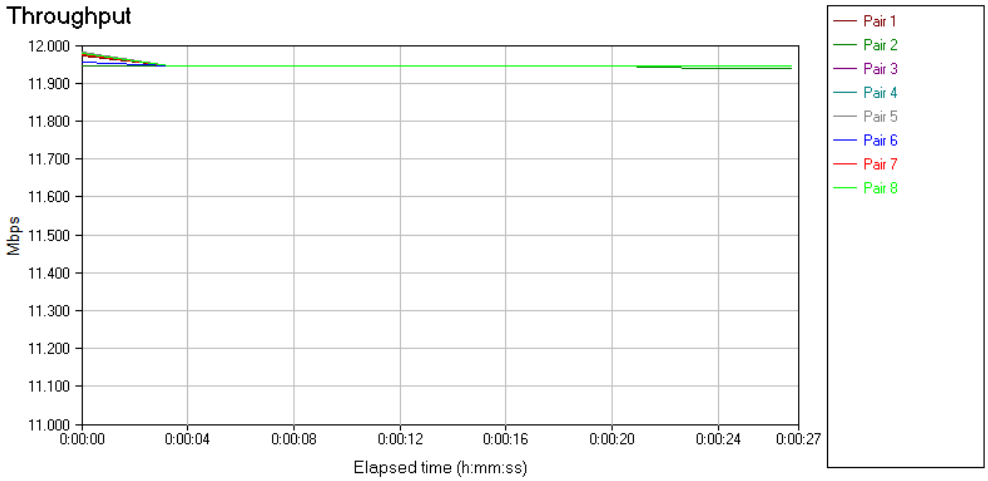
14. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από οχτώ υπολογιστές με επικοινωνία (Server –> Client 11 Client 12 Client 13 Client 14 Client 15 Client 16 Client 17 Client 18) με TCP IPv6

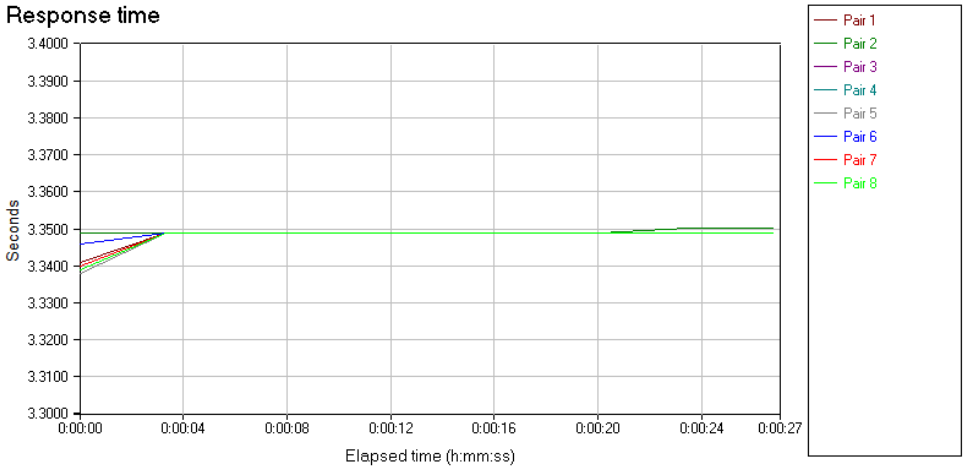




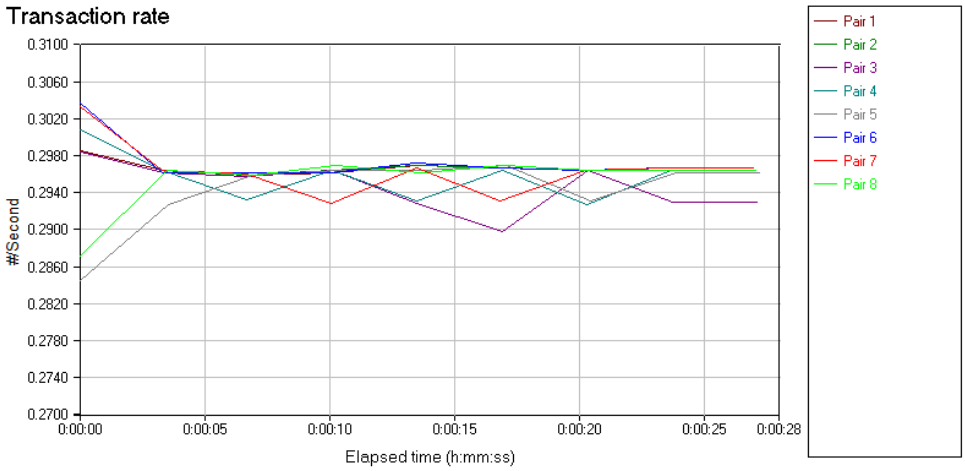
15. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από οχτώ υπολογιστές με επικοινωνία (Server –> Client 11 Client 12 Client 13 Client 14 Client 15 Client 16 Client 17 Client 18) με UDP IPv4

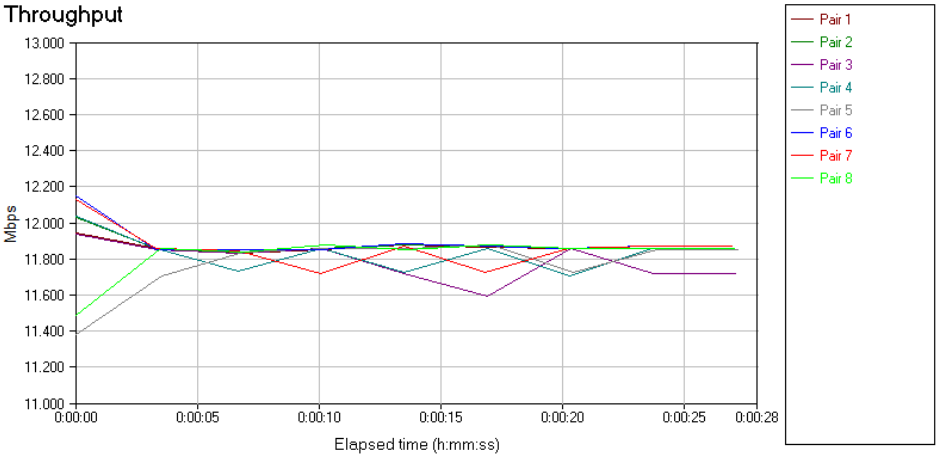


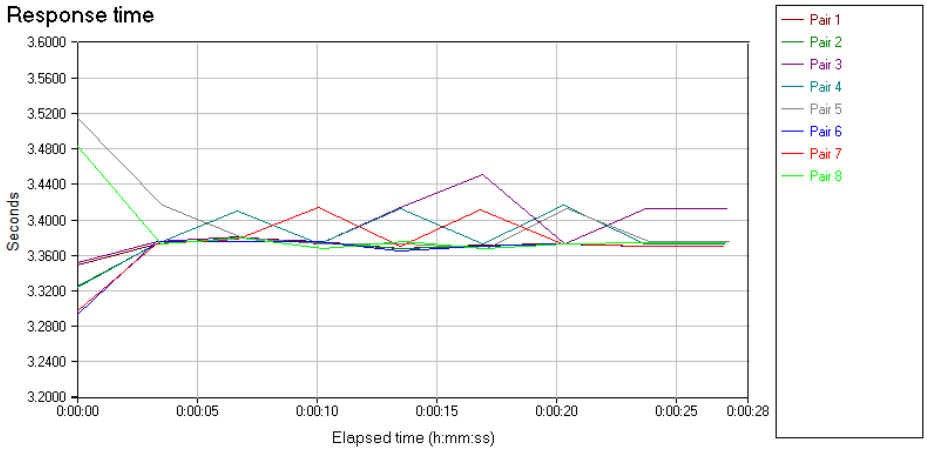




16. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από οχτώ υπολογιστές με επικοινωνία (Server –> Client 11 Client 12 Client 13 Client 14 Client 15 Client 16 Client 17 Client 18) με TCP IPv4

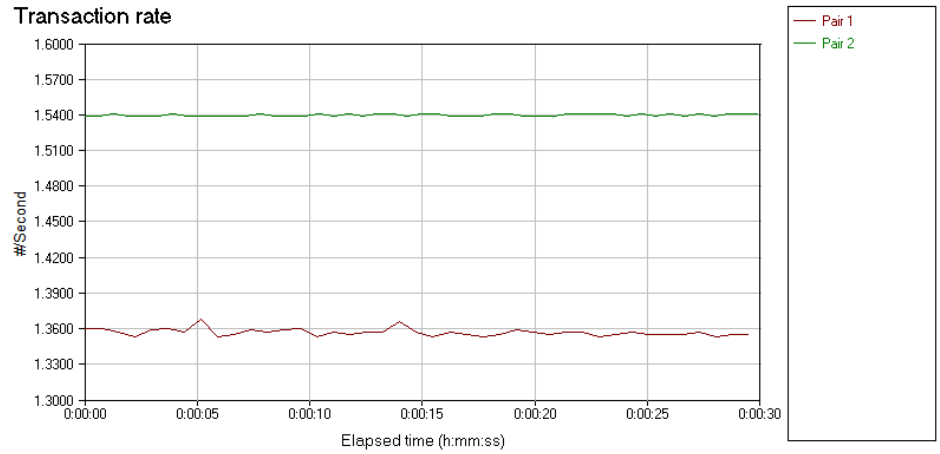


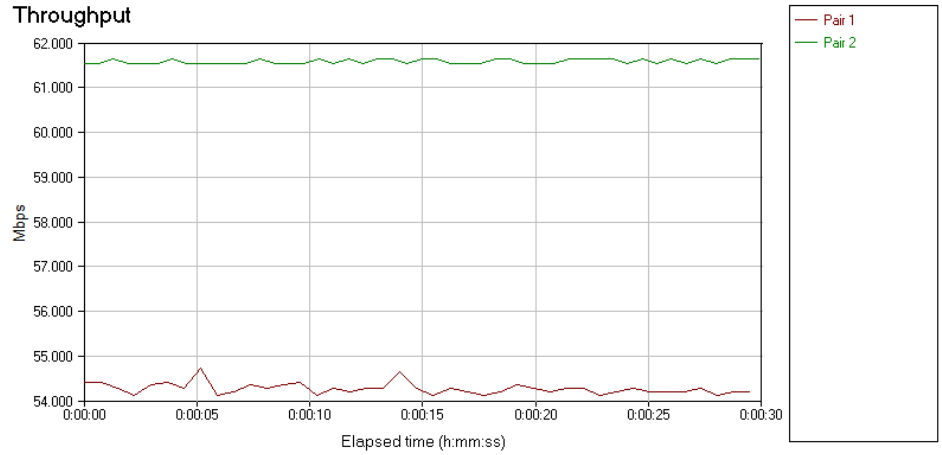


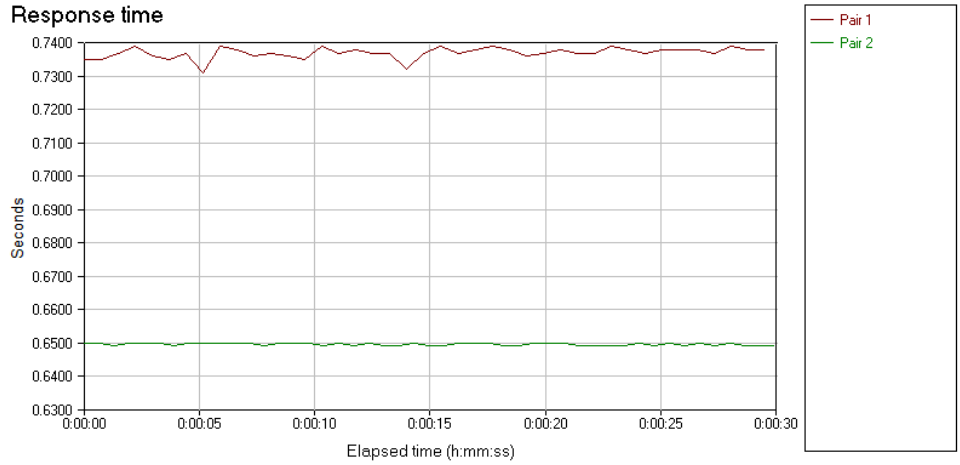


- Το βασικό χαρακτηριστικό των μετρήσεων είναι και πάλι ότι το IPv4 (TCP) είναι ποιο γρήγορο από το IPv6.

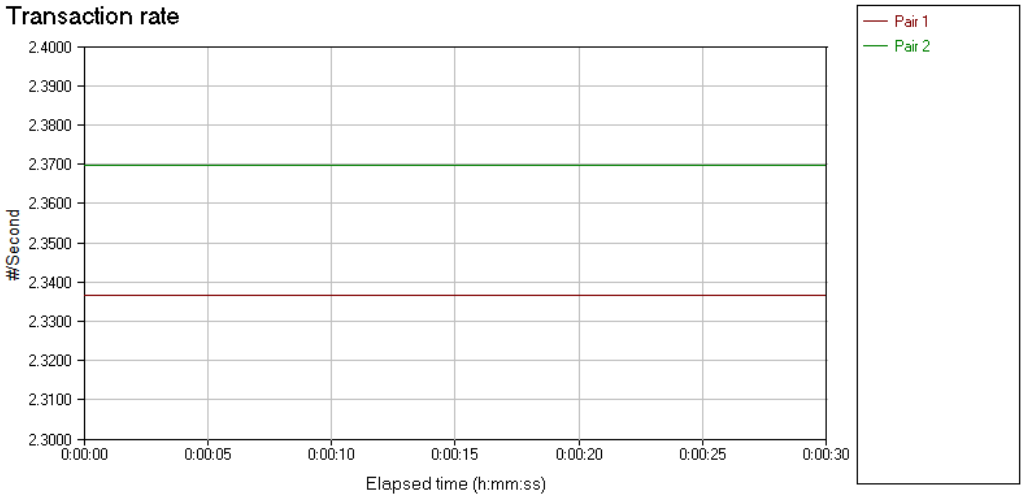
17. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τέσσερις υπολογιστές με επικοινωνία (Client 11-> Client 12) με UDP IPv6 (Client 13-> Client 14) με UDP IPv4

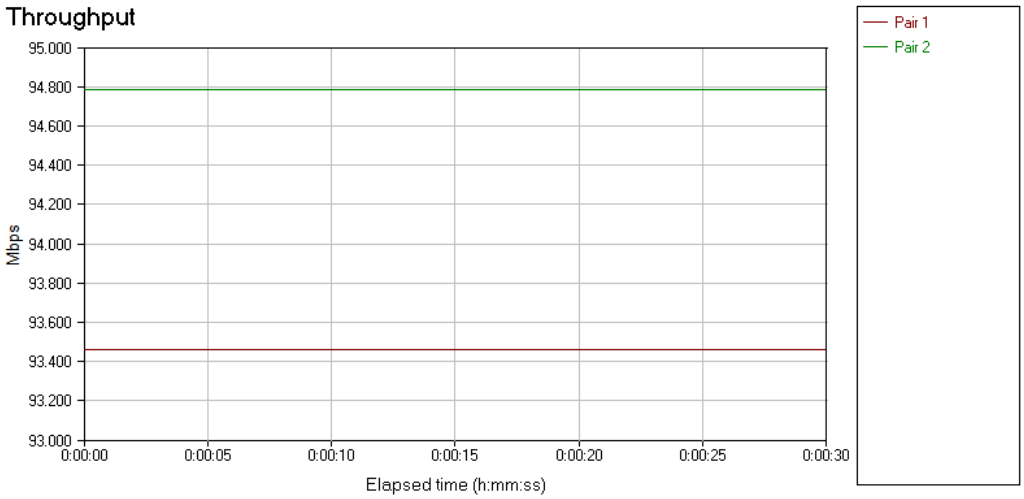


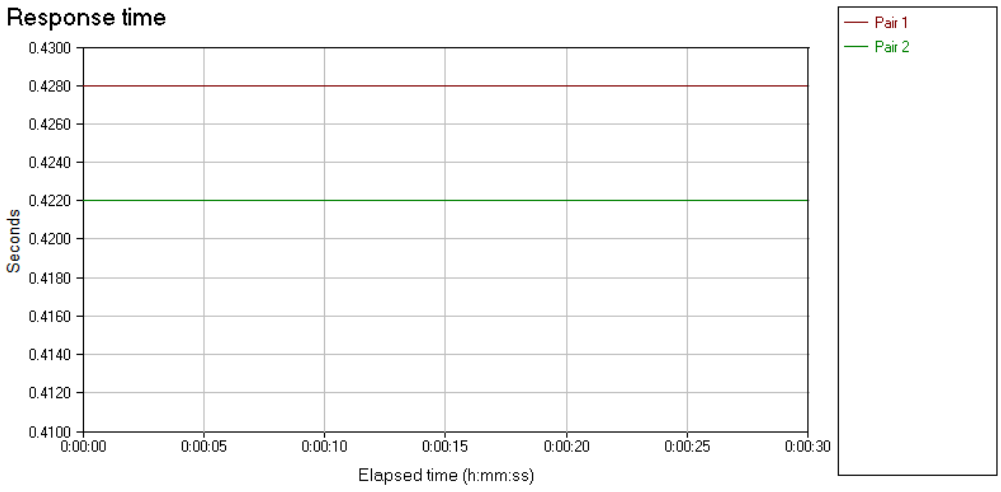




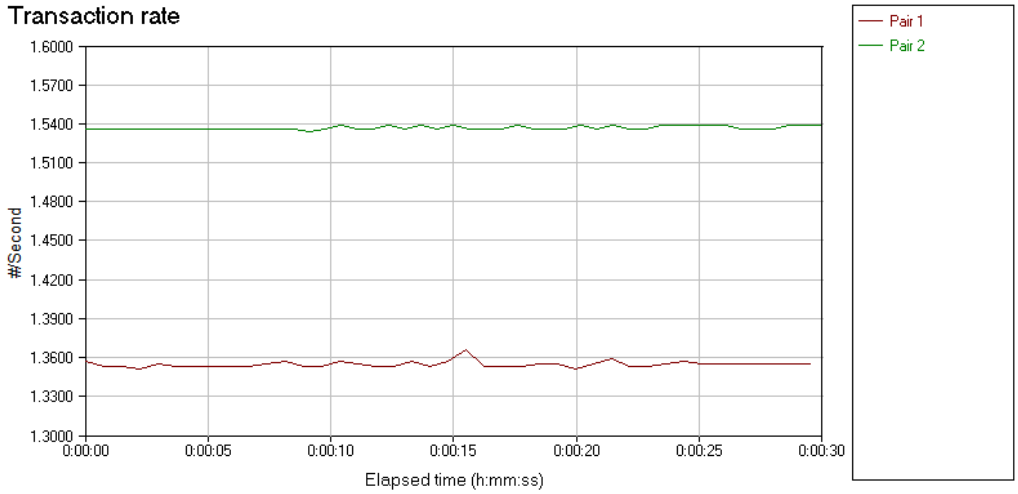
18. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τέσσερις υπολογιστές με επικοινωνία (Client 11-> Client 12) με TCP IPv6 (Client 13-> Client 14) με TCP IPv4

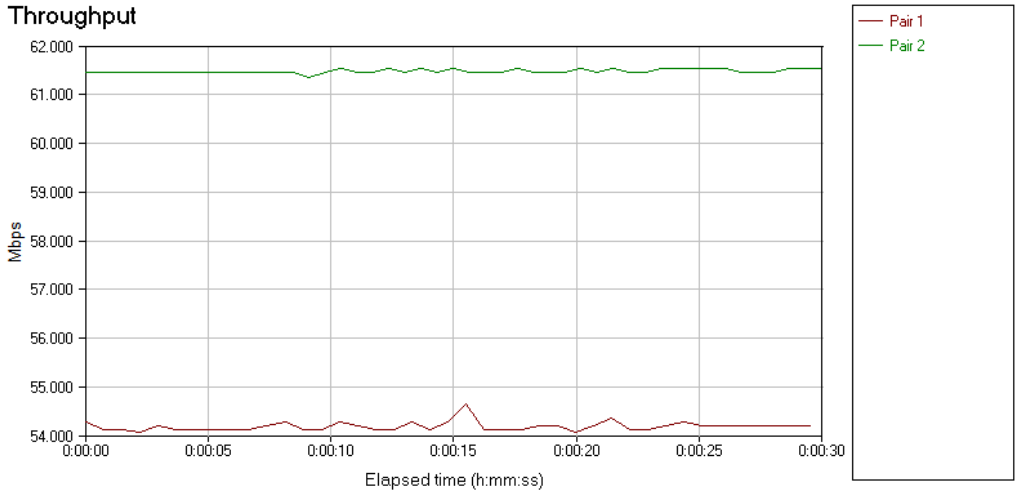


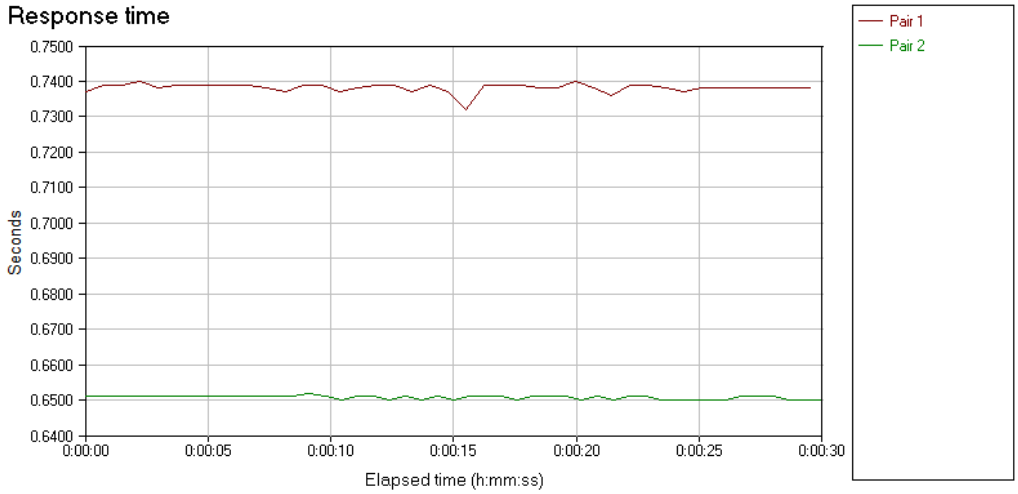




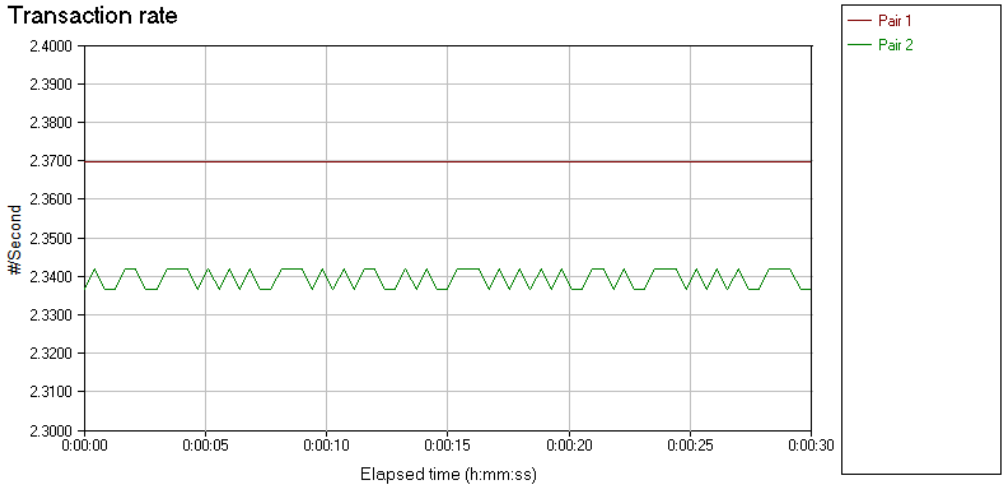
19. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τέσσερις υπολογιστές με επικοινωνία (Client 11-> Client 12) με UDP IPv4 (Client 13-> Client 14) με UDP IPv6

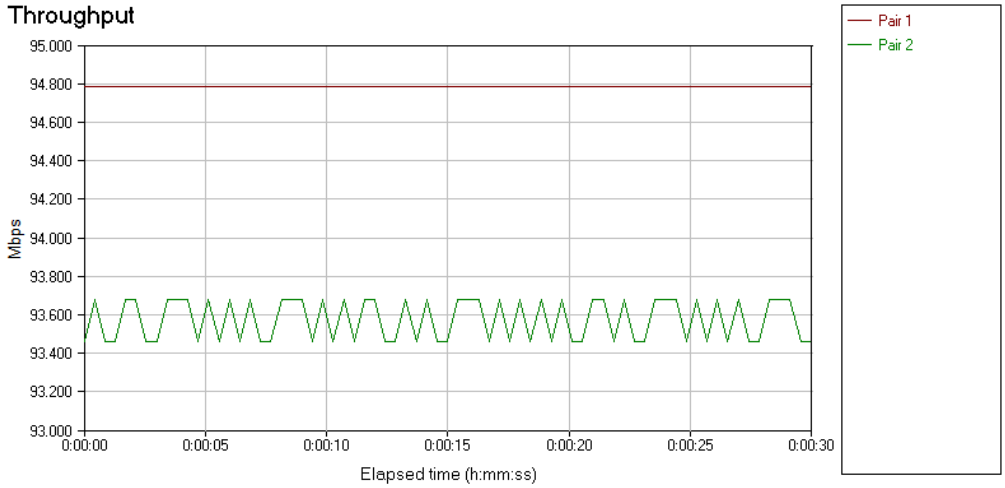


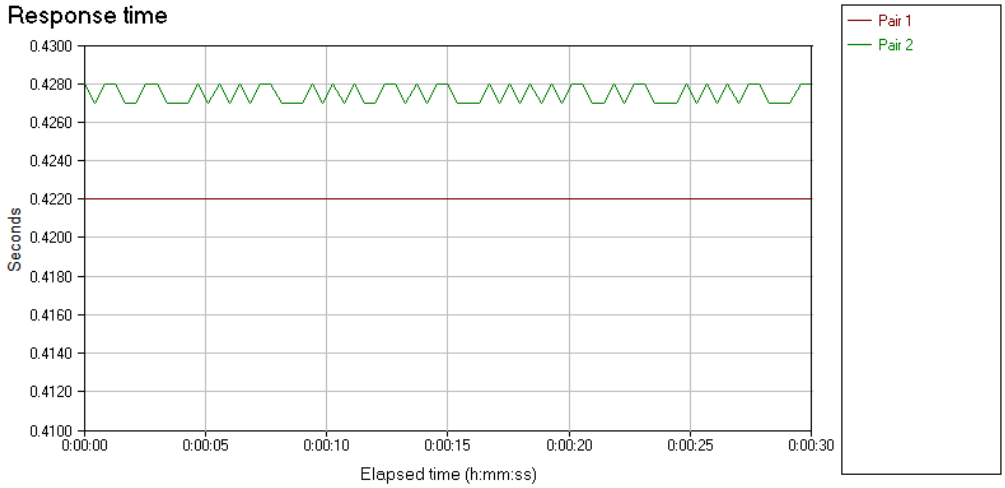




20. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τέσσερις υπολογιστές με επικοινωνία (Client 11-> Client 12) με TCP IPv4 (Client 13-> Client 14) με TCP IPv6



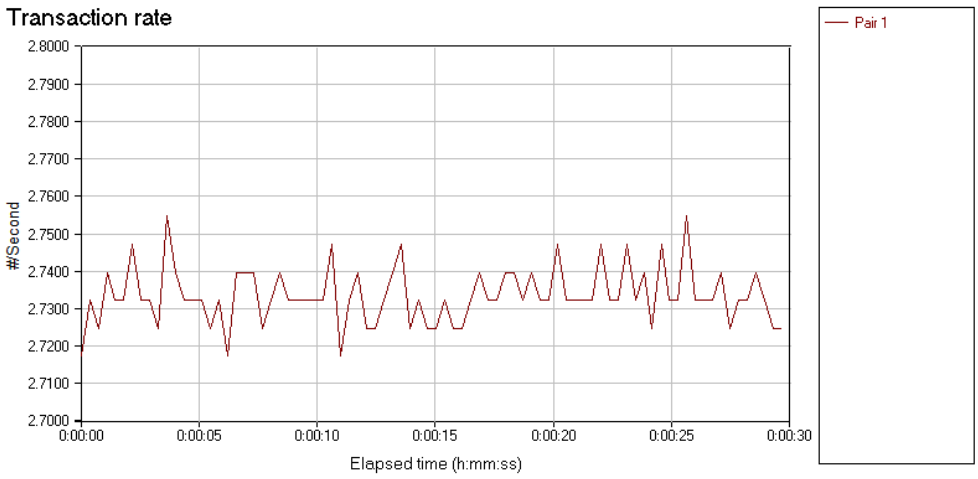


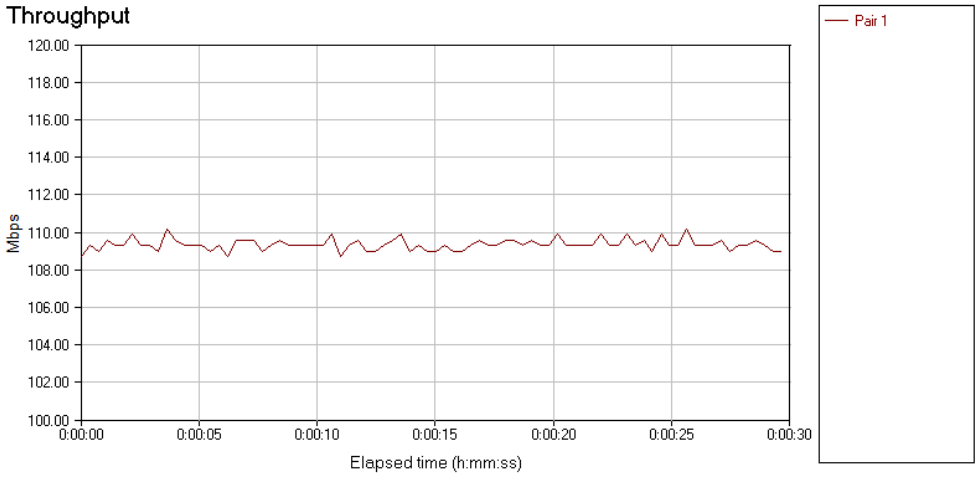


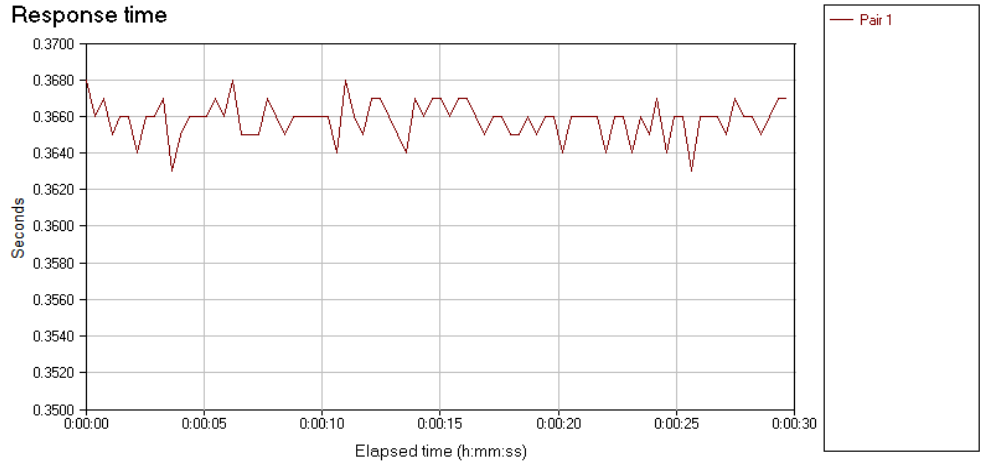
- Παρατηρούμε ότι πάλι το IPv4 (TCP) είναι ποιο γρήγορο από το IPv6.

6.1.2 Μετρήσεις με το IXIA (Με GIGABIT LAN)

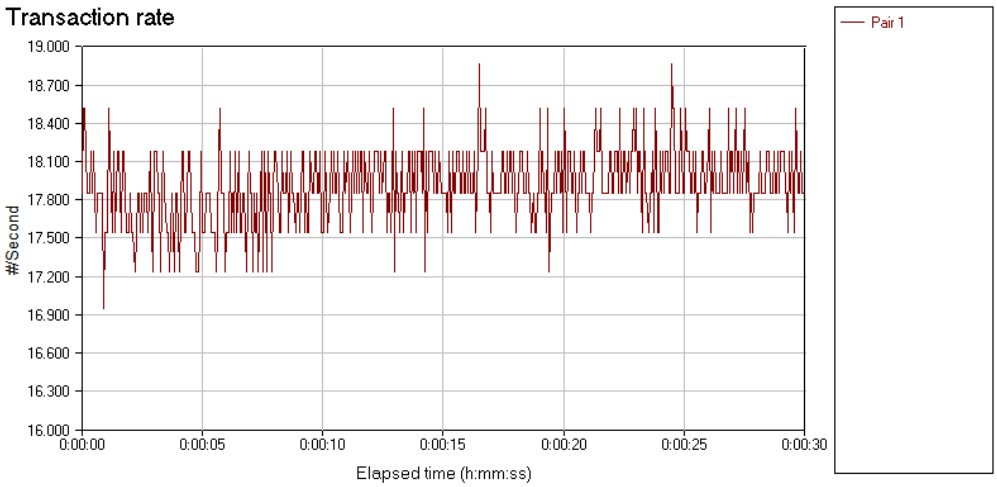
1. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με UDP IPv6

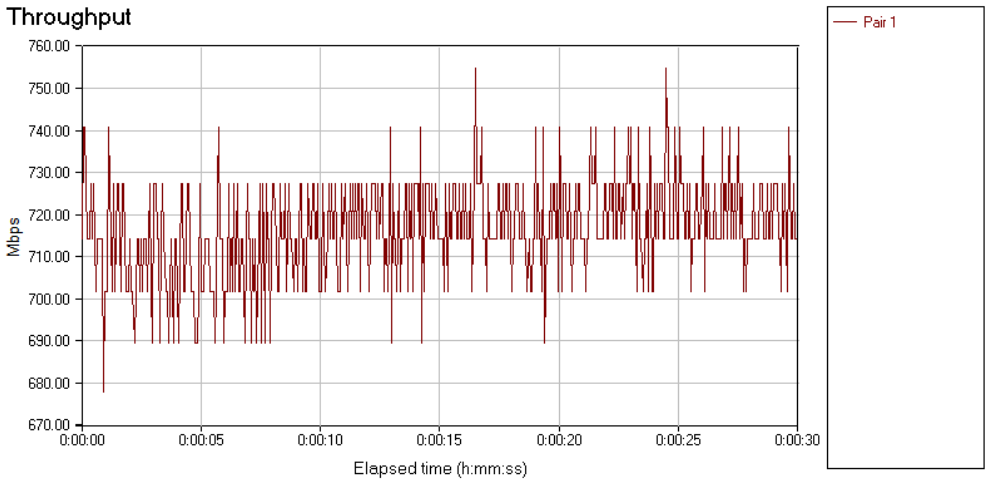


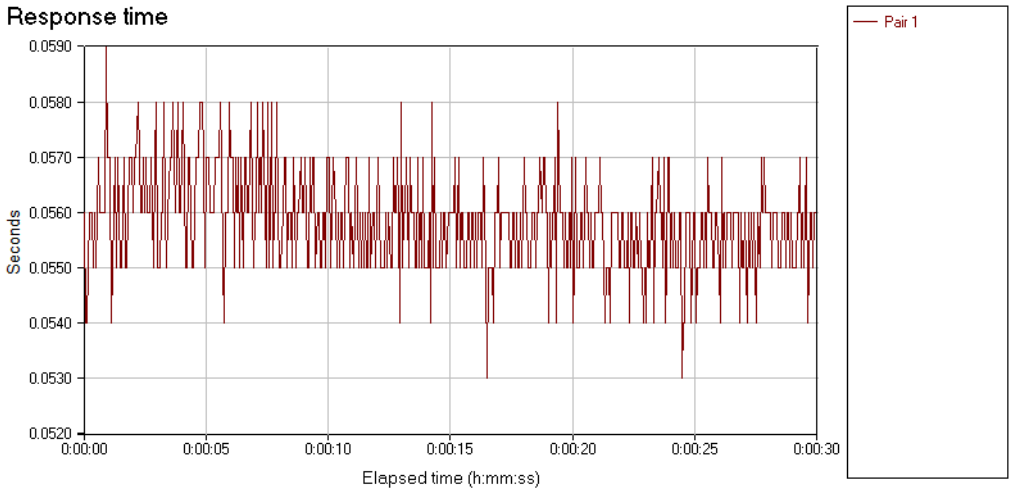




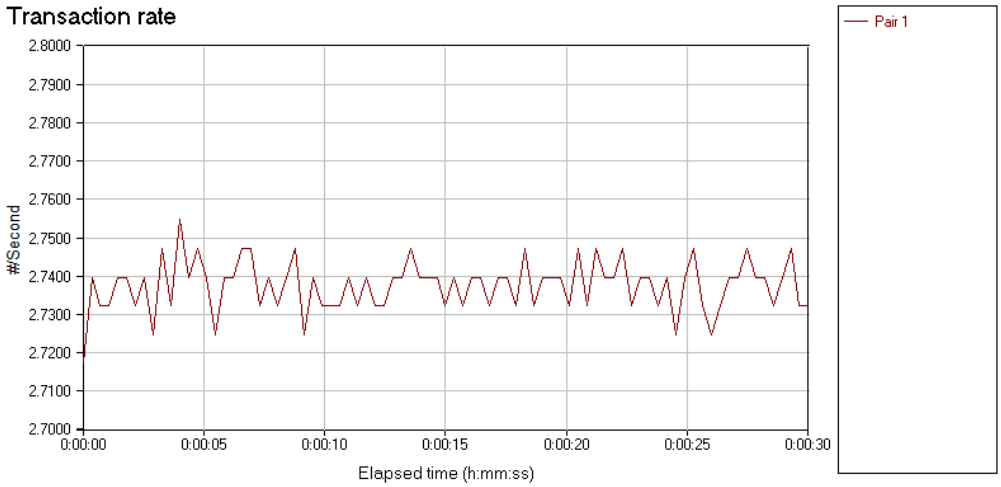
2. *Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με TCP IPv6*

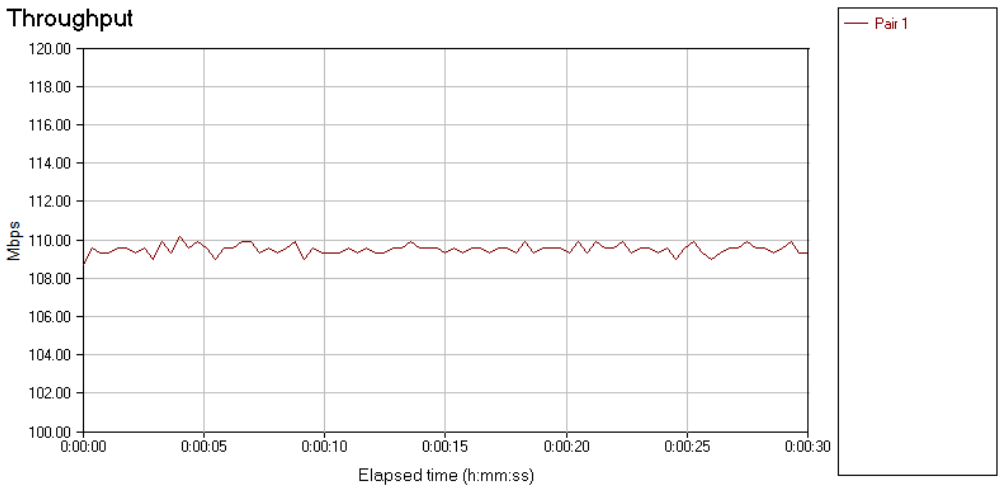


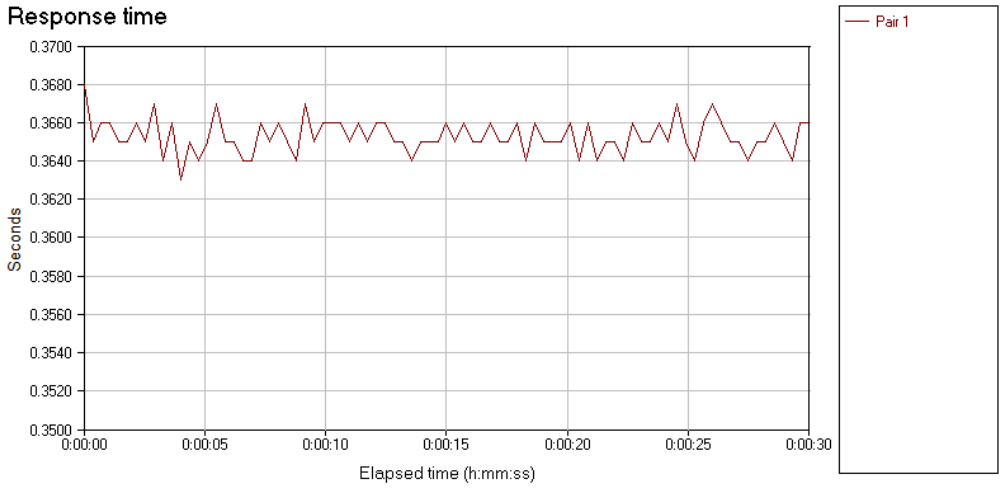




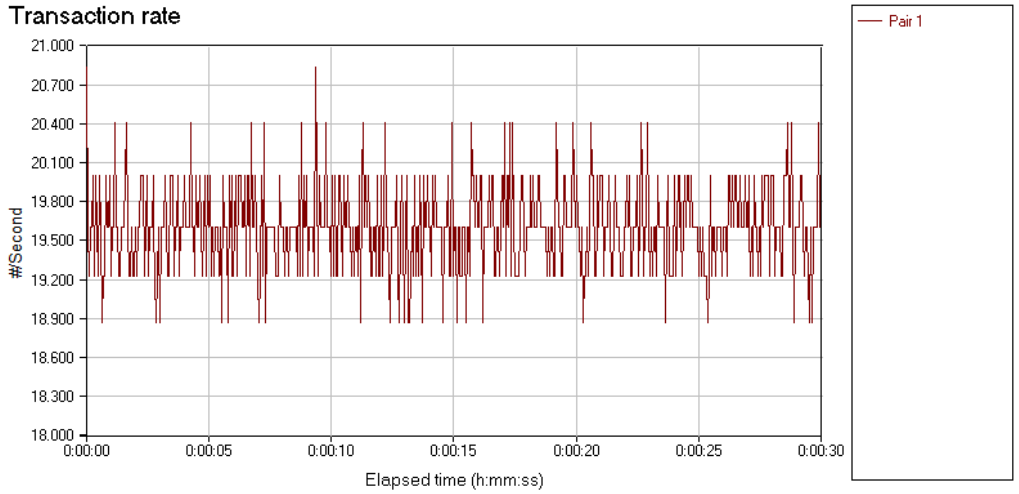
3. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με UDP IPv4

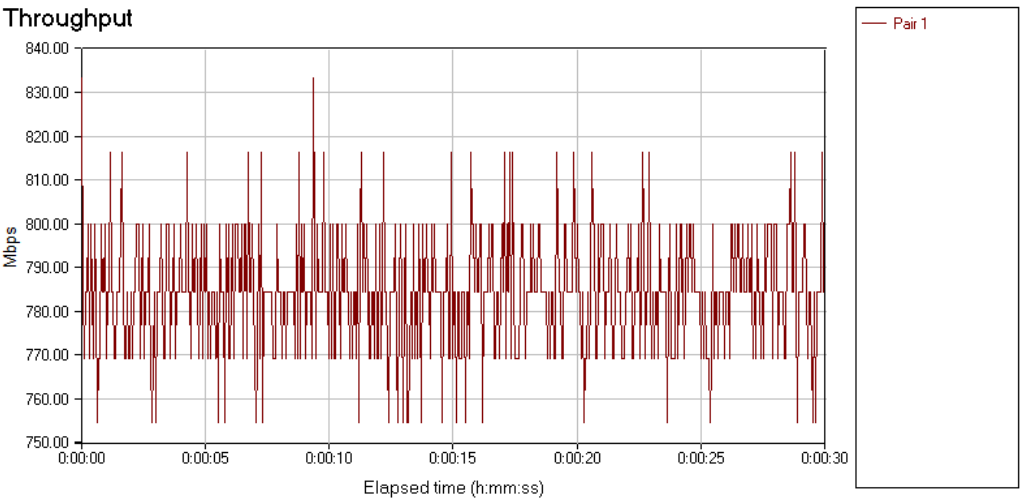


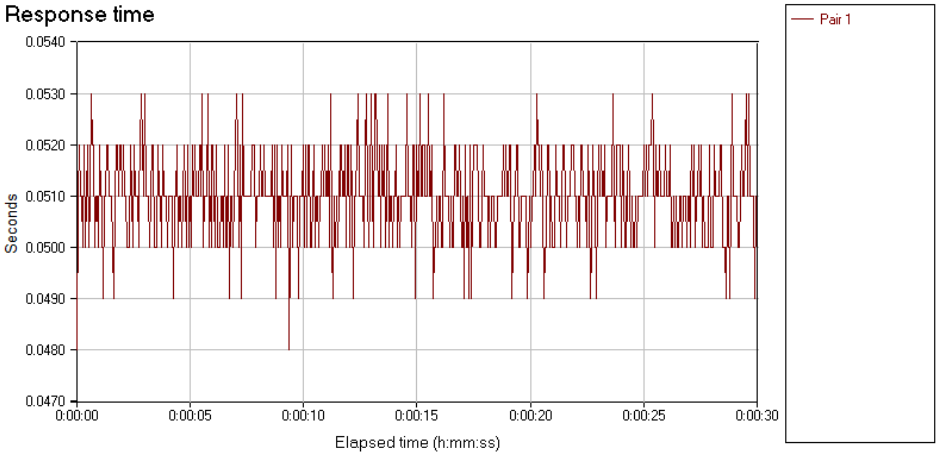




4. *Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με TCP IPv4*

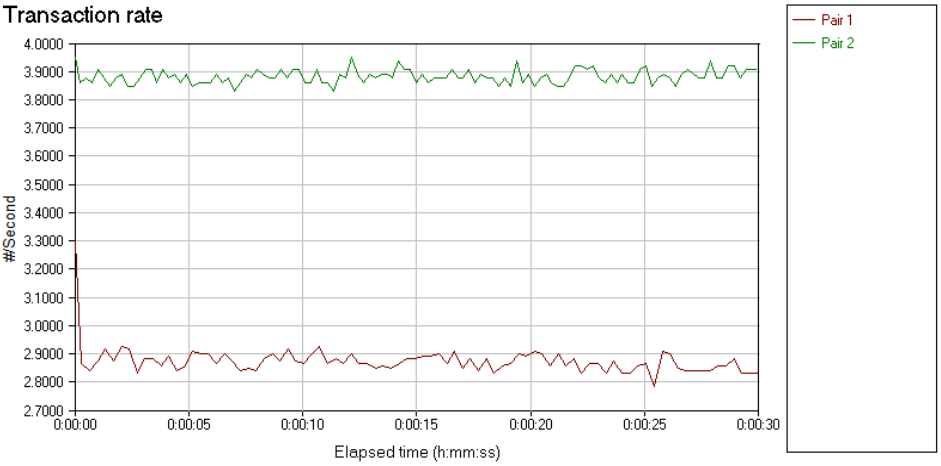


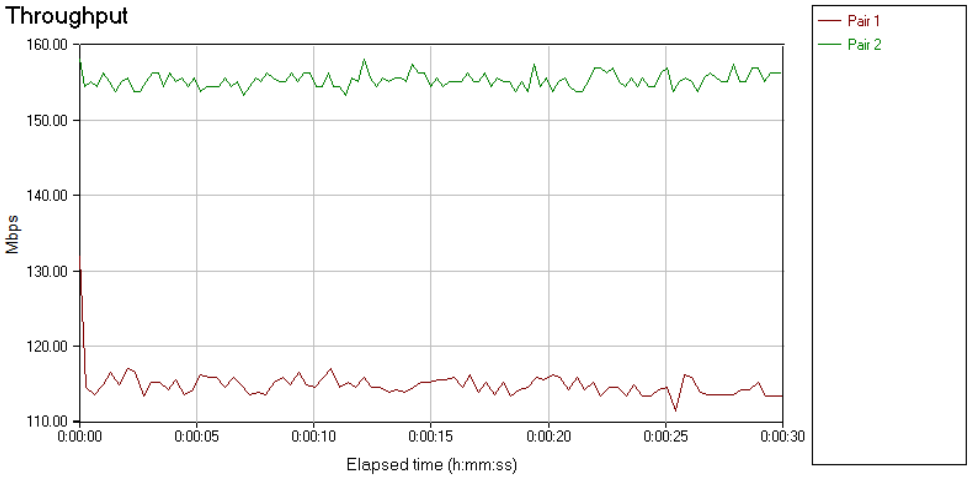


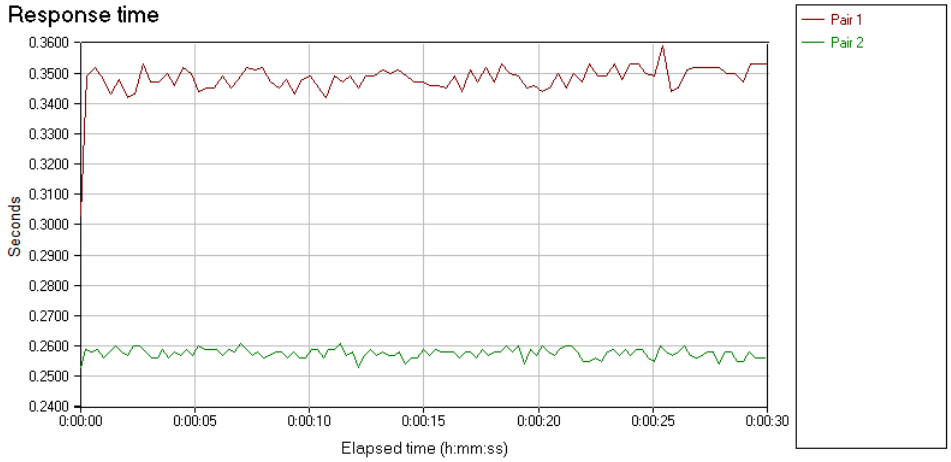


- Παρατηρούμε ότι πάλι το IPv4 (TCP) είναι ποιο γρήγορο από το IPv6

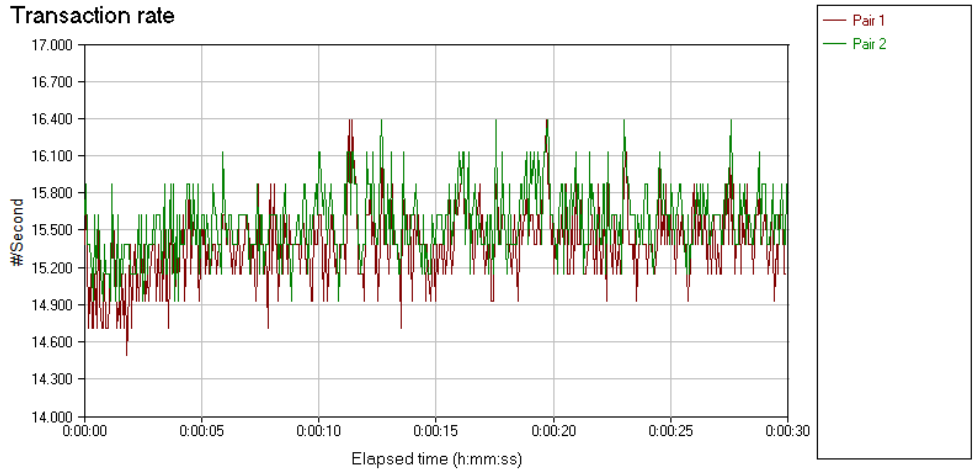
5. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με UDP IPv6

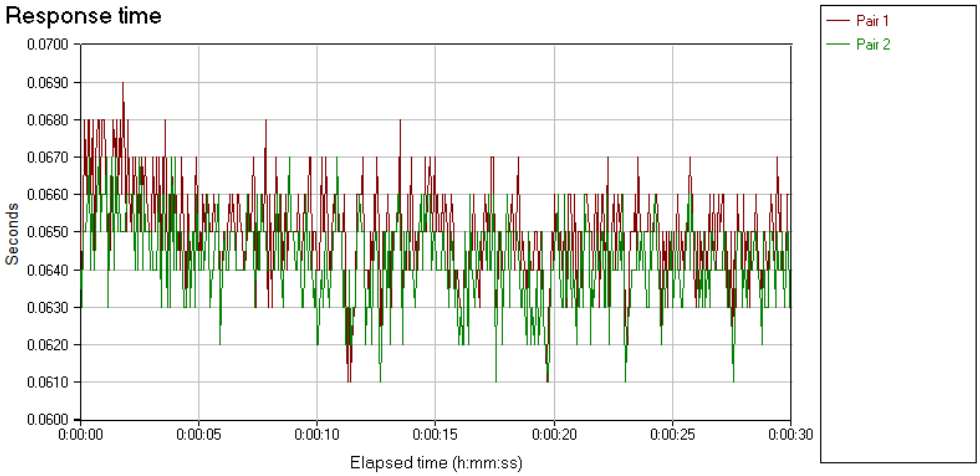


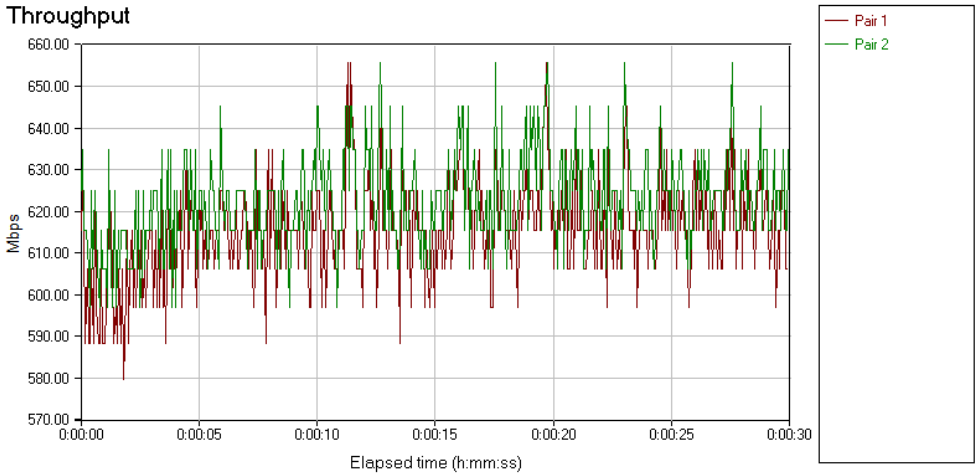




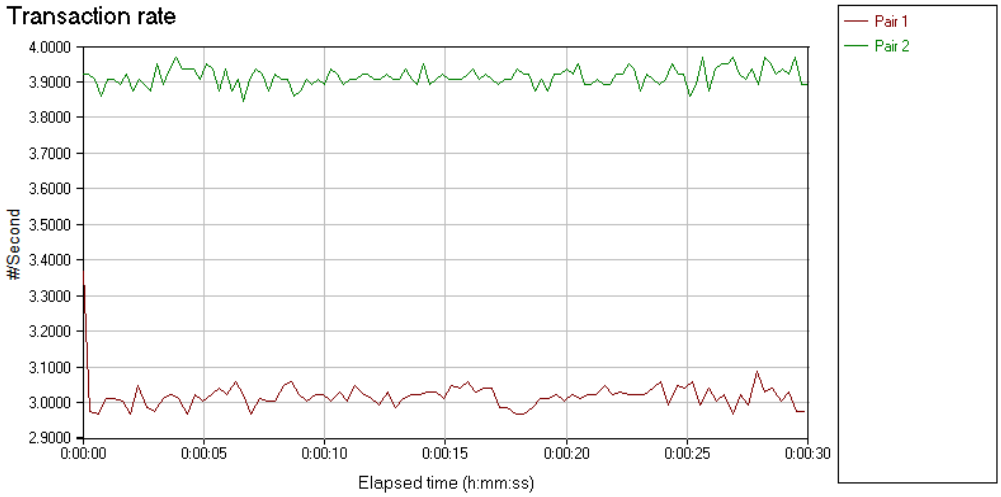
6. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με TCP IPv6

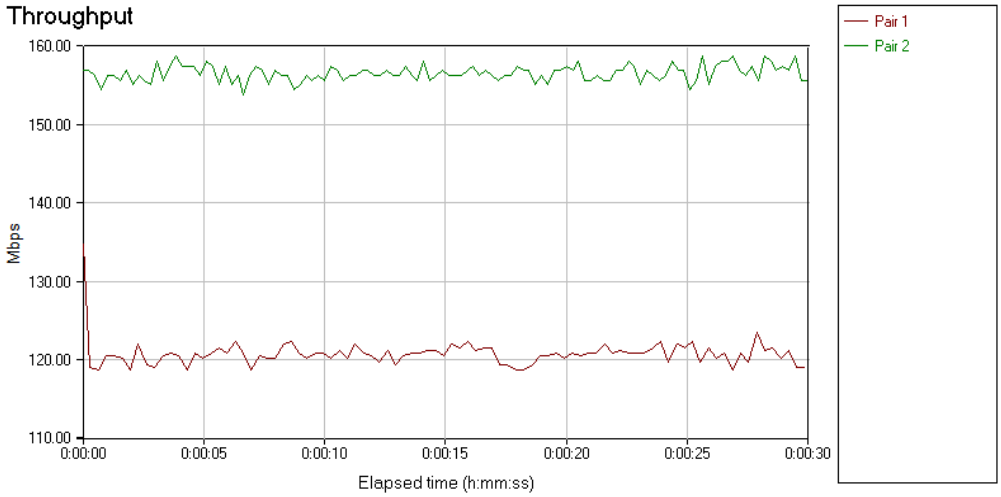

Transaction rate
Pair 1
Pair 2
17.000
16.700
16.400
16.100
15.800
15.500
15.200
14.900
14.600
14.300
14.000
#Second
0:00:00
0:00:05
0:00:10
0:00:15
0:00:20
0:00:25
0:00:30
Elapsed time (h:mm:ss)

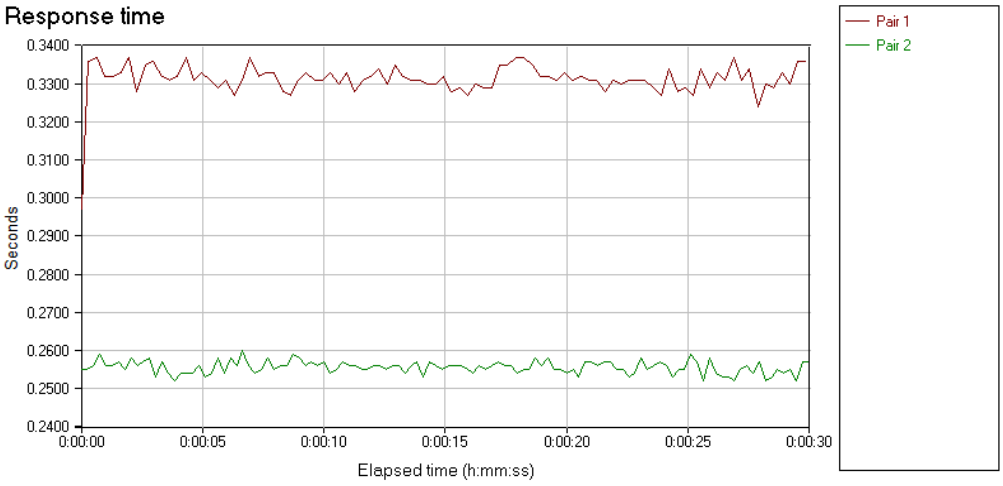

Response time
Pair 1
Pair 2
0.0700
0.0690
0.0680
0.0670
0.0660
0.0650
0.0640
0.0630
0.0620
0.0610
0.0600
Seconds
0:00:00
0:00:05
0:00:10
0:00:15
0:00:20
0:00:25
0:00:30
Elapsed time (h:mm:ss)


Throughput
Pair 1
Pair 2
660.00
650.00
640.00
630.00
620.00
610.00
600.00
590.00
580.00
570.00
Mbps
0:00:00
0:00:05
0:00:10
0:00:15
0:00:20
0:00:25
0:00:30
Elapsed time (h:mm:ss)

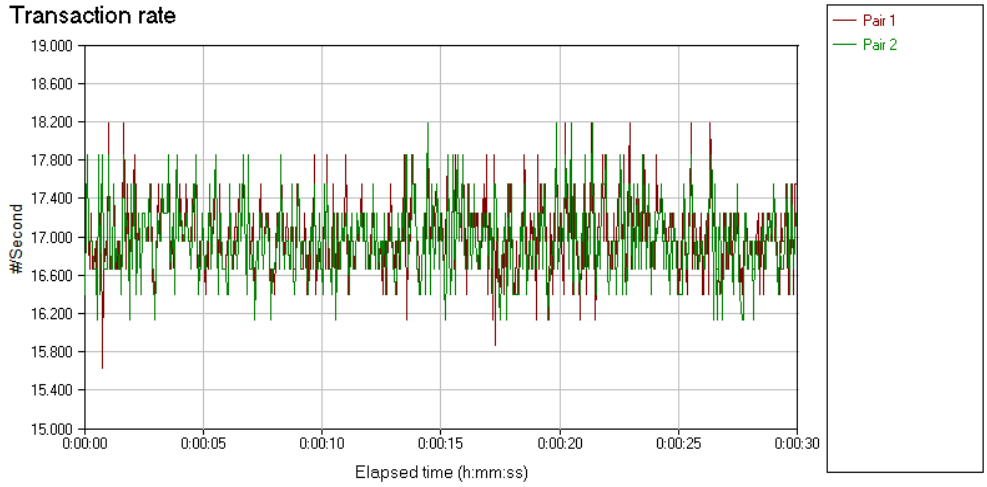
7. *Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με UDP IPv4*

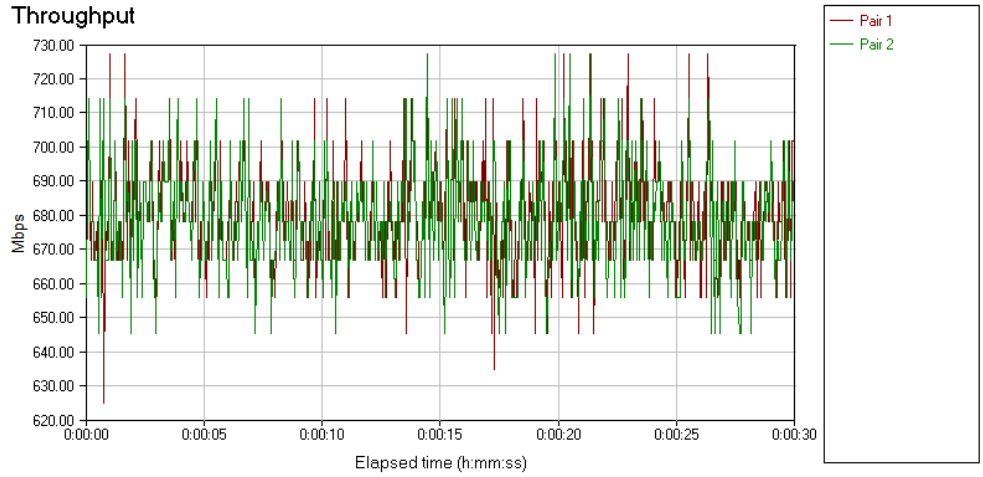


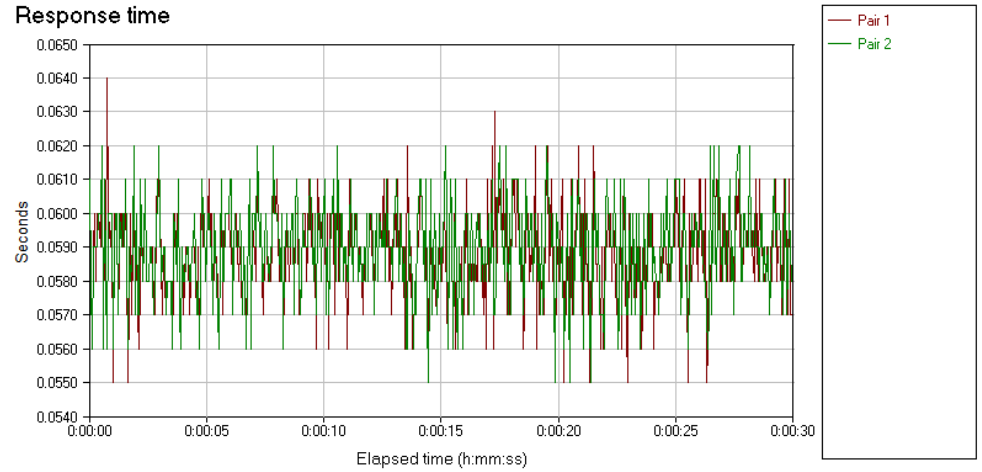




8. *Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από δυο υπολογιστές με επικοινωνία (Server -> Client 11) με TCP IPv4*

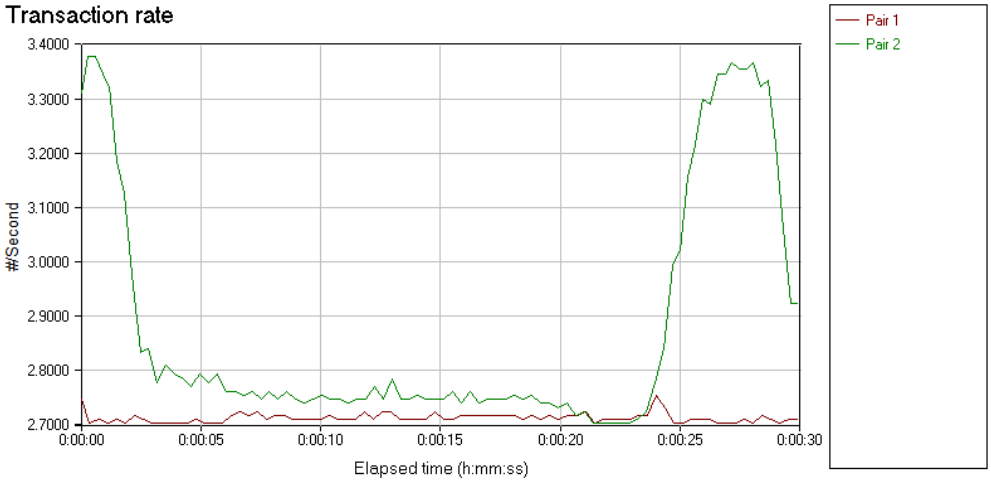


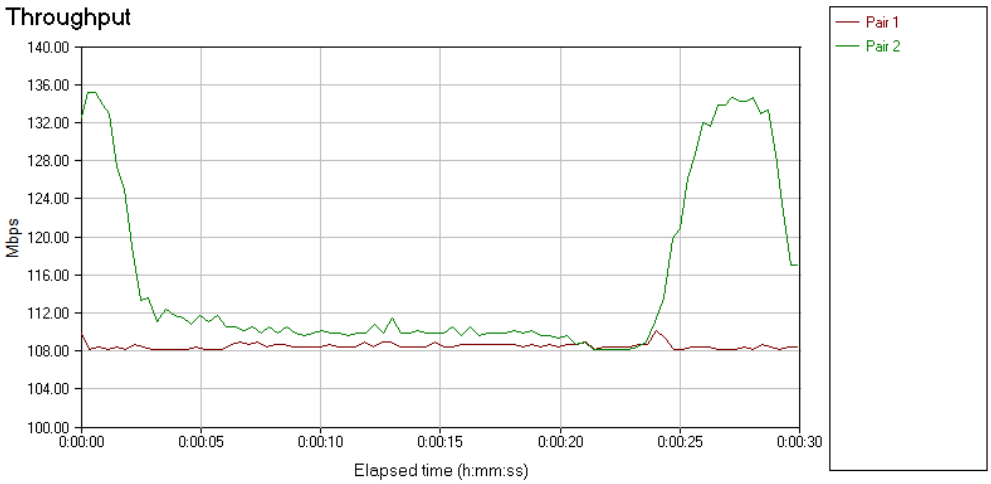


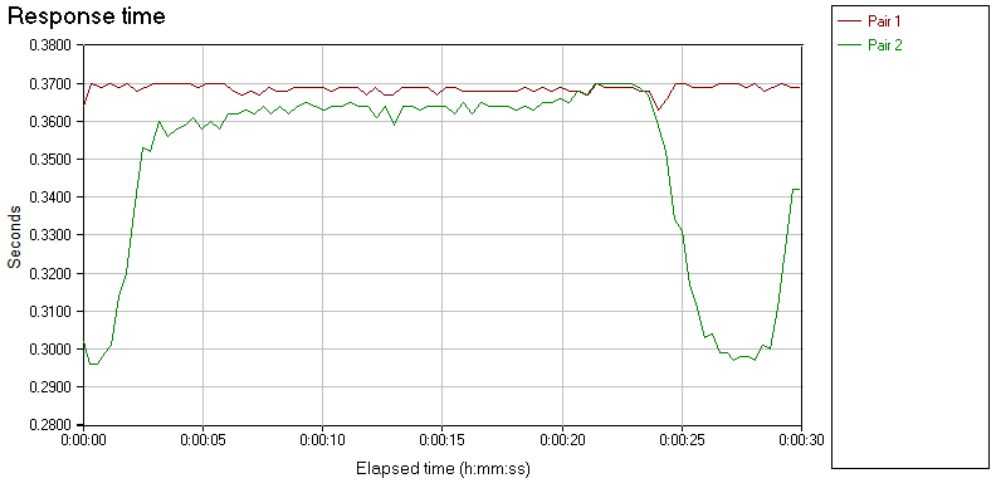


- Παρατηρούμε ότι πάλι το IPv4 (TCP) είναι ποιο γρήγορο από το IPv6.

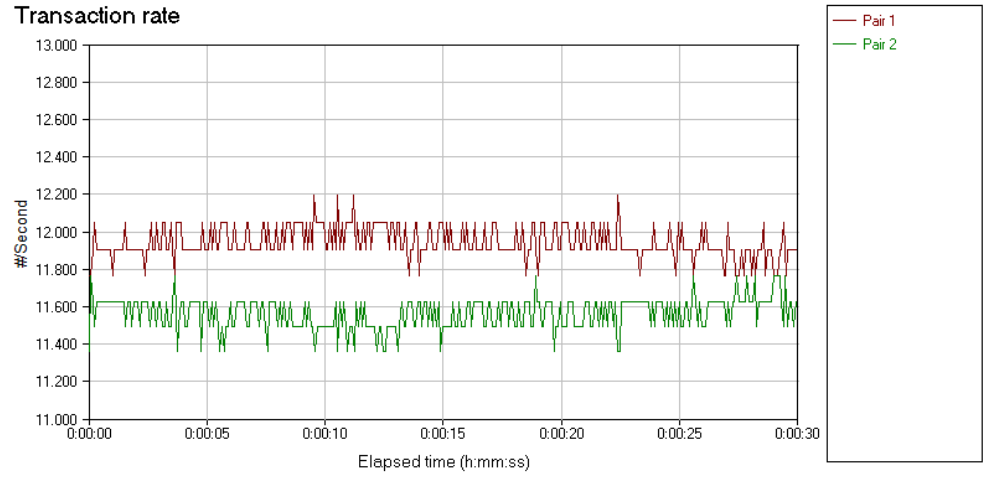
9. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές με επικοινωνία (Server -> Client 11 server -> Client12) με UDP IPv6

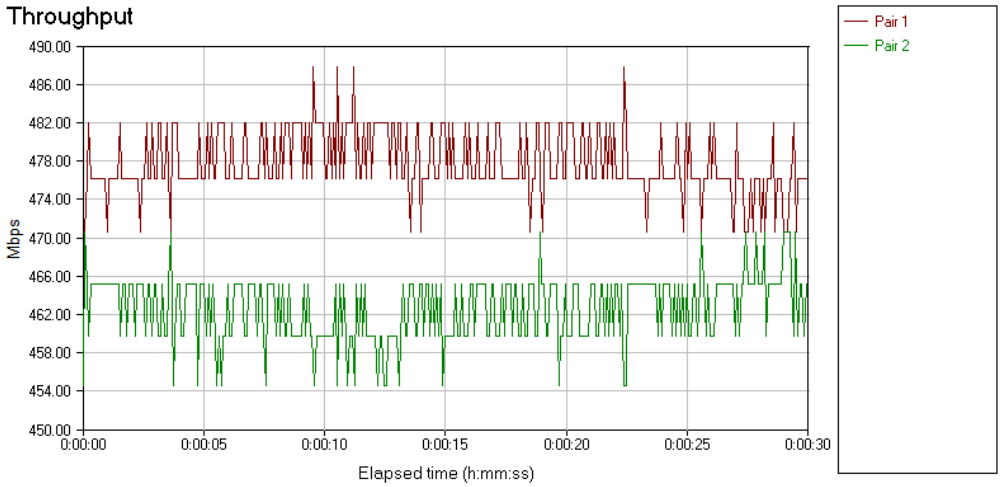


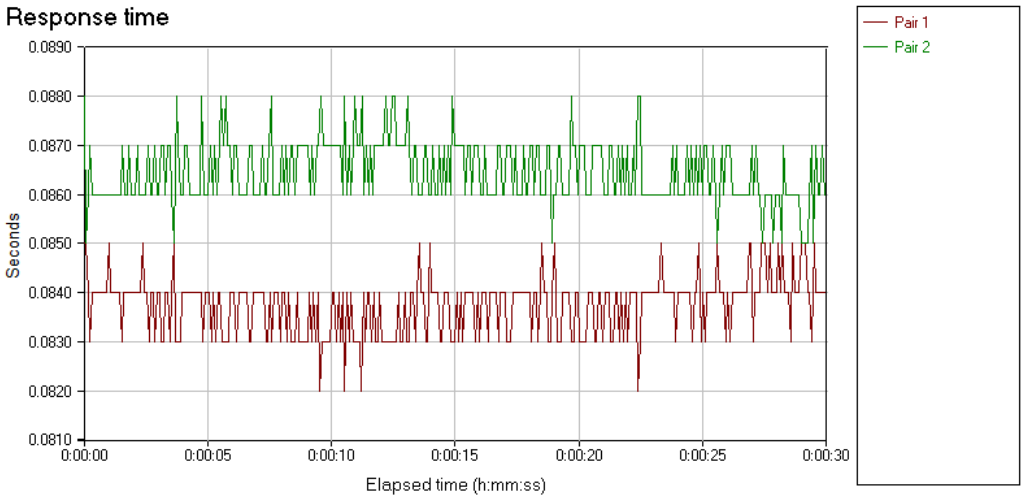




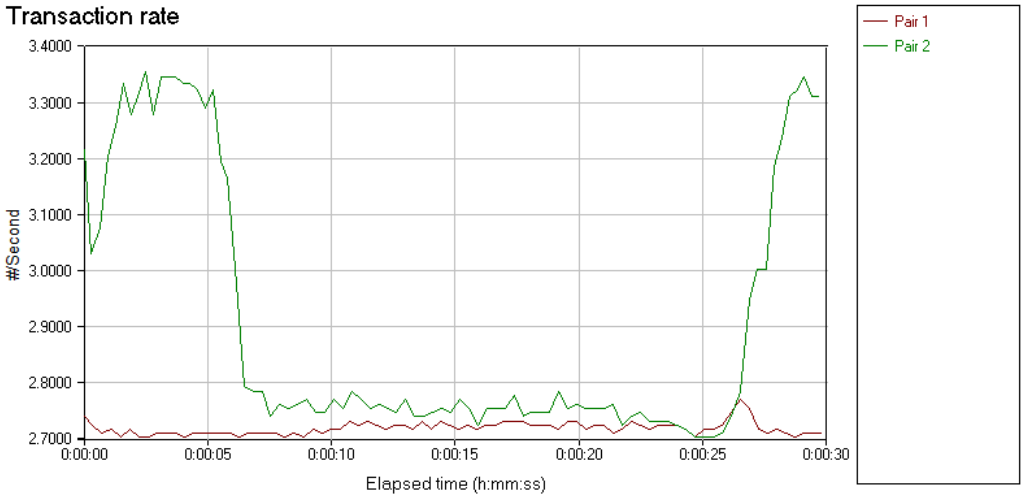
10. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές με επικοινωνία (Server -> Client 11 server -> Client12) με TCP IPv6

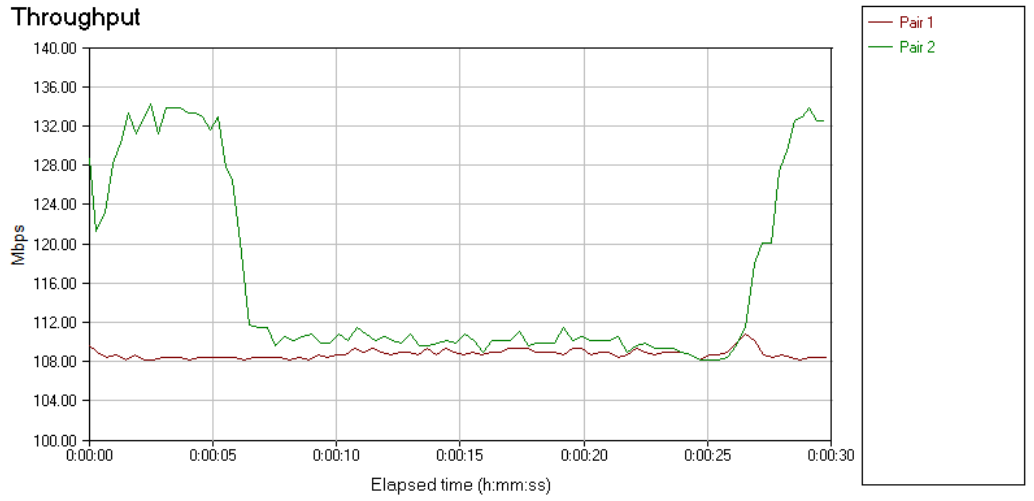


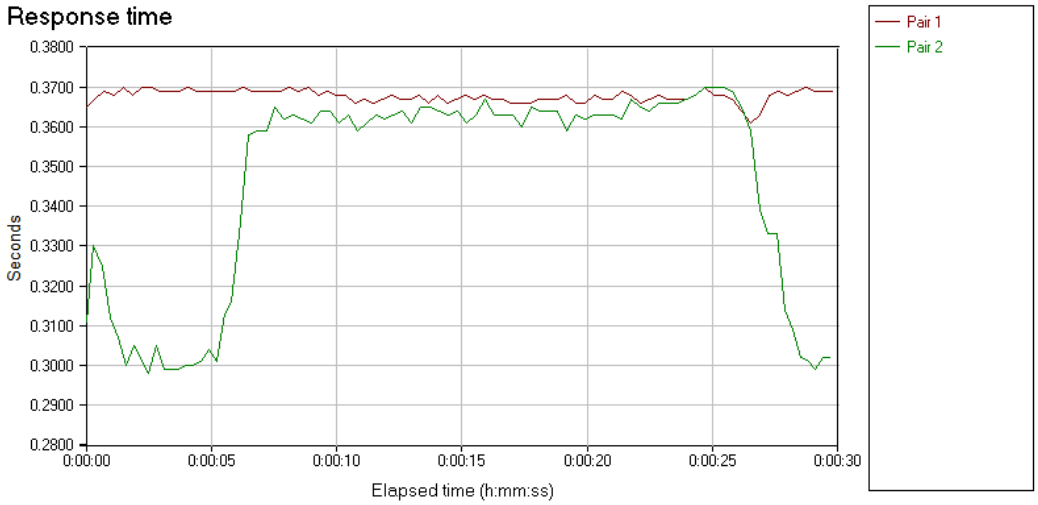




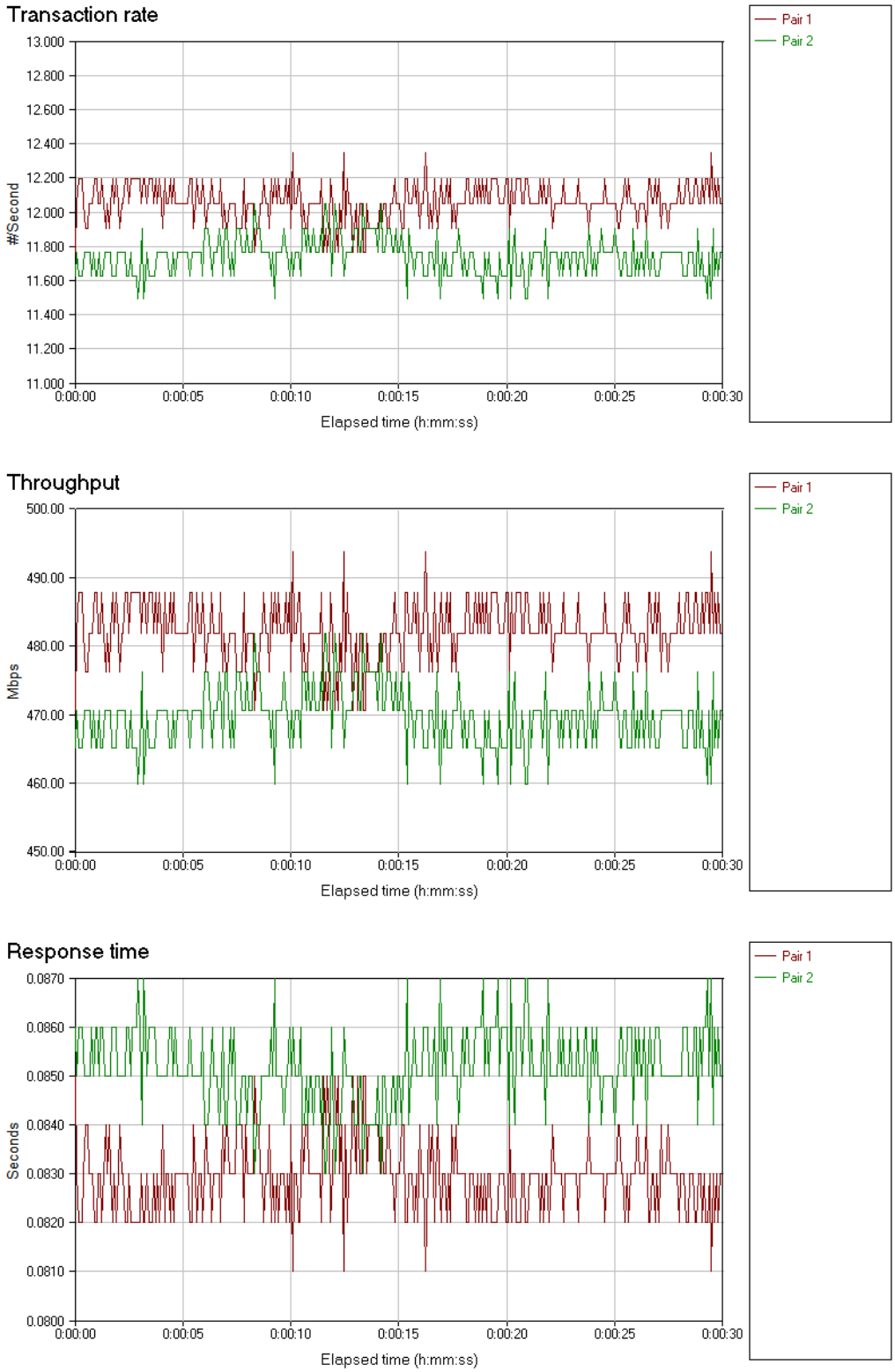
11. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές με επικοινωνία (Server -> Client 11 server -> Client12) με UDP IPv4







12. Παρακάτω βλέπουμε τις μετρήσεις που πήραμε από τρεις υπολογιστές με επικοινωνία (Server -> Client 11 server -> Client12) με TCP IPv4



Παρατηρούμε ότι πάλι το IPv4 (TCP) είναι ποιο γρήγορο από το IPv6.

Κεφάλαιο 7ο - Το τοπικό δίκτυο

7.1 Εισαγωγή

Δίκτυο καλείται μια ομάδα υπολογιστών οι οποίοι είναι συνδεδεμένοι μεταξύ τους, ενσύρματα ή ασύρματα, με σκοπό την ανταλλαγή δεδομένων ή την κοινή χρήση συσκευών. Όταν η εν λόγω ομάδα απαρτίζεται από μικρό αριθμό υπολογιστών που βρίσκονται σε διάμετρο μερικών μέτρων (λ.χ. σε μια μικρή επιχείρηση, σε ένα γραφείο κ.λπ.) τότε κάνουμε λόγο για ένα δίκτυο τοπικής εμβέλειας LAN (Local Area Network). Όταν αντίστοιχα το δίκτυο επεκτείνεται και συνδέει γεωγραφικά απομακρυσμένα σημεία, κάνουμε λόγο για WAN (Wide Area Network), δηλαδή για δίκτυο εκτεταμένης εμβέλειας.

Σε ένα τοπικό δίκτυο (Local Area Network, LAN), οι υπολογιστές είναι εφοδιασμένοι με μια κάρτα δικτύου που συνδέεται με το καλώδιο του δικτύου. Οι υπολογιστές, μαζί με έναν εξυπηρετητή αρχείων (file server) ο οποίος παρέχει αποθηκευτικό χώρο, και τις υπόλοιπες περιφερειακές συσκευές, όπως οι εκτυπωτές, αποτελούν τους κόμβους (nodes) του δικτύου. Όλοι οι κόμβοι ενός τοπικού δικτύου βρίσκονται συγκεντρωμένοι σε μια περιορισμένη γεωγραφικά περιοχή, ας πούμε σε μια ακτίνα μερικών εκατοντάδων μέτρων. Η πληροφορία μεταδίδεται σε κομμάτια που ονομάζονται πλαίσια (frames) και η μετάδοση τους γίνεται στη βασική ζώνη. Τα πλαίσια μεταδίδονται σε χρονικές σχισμές (time slices) που παρέχονται στους σταθμούς προσωρινά. Οι σχισμές δεν παρέχονται σύμφωνα με κάποιο πρόγραμμα, αλλά κάθε σταθμός τις δεσμεύει δυναμικά, ανάλογα με τις ανάγκες του.

Τα τελευταία χρόνια, οι προσωπικοί υπολογιστές δικτυώνονται με όλο και μεγαλύτερους ρυθμούς. Μέχρι το 2004 το 80% όλων των υπολογιστών που χρησιμοποιούνται σε επιχειρήσεις αποτελούσαν κόμβους κάποιου είδους τοπικού δικτύου. Ταυτόχρονα, ο μέσος αριθμός των χρηστών LAN αυξάνει συνεχώς, πράγμα που σημαίνει μικρότερο εύρος ζώνης ανά χρήστη.

Οι πιο δημοφιλείς τύποι LAN είναι το Ethernet και το Token Ring, τα οποία ακολουθούν τις τοπολογίες αρτηρίας και δακτυλίου αντίστοιχα. Ο σχεδιασμός αυτών των αρχιτεκτονικών είναι παλιός και αρχικά προορίζονταν για συνήθεις εφαρμογές και για μεταφορά αρχείων

περιορισμένου όγκου. Ο βασικός περιορισμός αυτών των δικτύων βρίσκεται στο γεγονός ότι πολλοί κόμβοι μοιράζονται το ίδιο φυσικό μέσο. Αυτό οδηγεί αναπόφευκτα σε συγκρούσεις, που είτε οδηγούν στην αναμονή κάποιου αποστολέα ή σε απώλεια των δεδομένων και επαναποστολή των δεδομένων αργότερα. Με άλλα λόγια, ο ρυθμός εξυπηρέτησης είναι συνήθως μικρότερος από την ταχύτητα πρόσβασης του δικτύου και μικραίνει όσο μεγαλώνει η κίνηση στο δίκτυο. Αυτό σημαίνει ότι η αποστολή μεγάλων όγκων από ένα χρήστη, έχει επιπτώσεις για όλους του χρήστες του δικτύου. Επιπλέον, η στατιστική φύση των καθυστερήσεων μεταφοράς δυσχεραίνει την αποστολή χρονικά εξαρτώμενης πληροφορίας. Ένα πλεονέκτημα του κοινού μέσου μεταφοράς είναι η εγγενής υποστήριξη του multicasting, γιατί κάθε πλαίσιο φθάνει σε όλους τους σταθμούς.

7.2 Πλεονεκτήματα των δικτύων

Οι δυνατότητες που προσφέρει η δικτύωση καθώς και τα οφέλη που απορρέουν από την ενσωμάτωσή της είναι σε γενικές γραμμές τα εξής:

- Διαμοιρασμός των ψηφιακών πόρων του συστήματος, δηλαδή προγραμμάτων, φακέλων, αρχείων κ.λπ. Αυτό πρακτικά σημαίνει ότι συγκροτείται ένας εικονικός κοινόχρηστος χώρος, όπου όλοι οι χρήστες, ανάλογα και με τα προνόμια - δικαιώματα που τους έχουν δοθεί από το διαχειριστή του δικτύου, έχουν πρόσβαση από τον υπολογιστή τους και μπορούν να χρησιμοποιούν τα ίδια αρχεία, τους ίδιους φακέλους και τις ίδιες εφαρμογές, ανεξάρτητα από το ποιος έχει δημιουργήσει το αρχείο ή σε ποιον υπολογιστή έχει εγκατασταθεί η εφαρμογή. Η δυνατότητα αυτή εξοικονομεί πολύτιμο χρόνο, καθώς οι χρήστες δεν χρειάζεται να αντιγράφουν σε δισκέτες, CD ή φορητές μνήμες τα αρχεία που θέλουν να μεταφέρουν από τον έναν υπολογιστή στον άλλο. Πλέον, αρκεί η είσοδος στον υπολογιστή τους. Στο ίδιο πλαίσιο, προκειμένου ένα πρόγραμμα να χρησιμοποιείται από όλους, αρκεί η εγκατάστασή του μία φορά και μόνο.

- Κοινή χρήση περιφερειακών συσκευών. Αυτό σημαίνει ότι τα μέλη του δικτύου μπορούν να χρησιμοποιούν από κοινού τις ίδιες περιφερειακές συσκευές. Έτσι, αν για παράδειγμα έχετε τέσσερις υπολογιστές, δεν χρειάζεται να έχετε και τέσσερις εκτυπωτές και τέσσερις σαρωτές. Αρκεί μία συσκευή από το κάθε είδος, η οποία θα χρησιμοποιείται από όλους. Η δυνατότητα αυτή μεταφράζεται ξεκάθαρα σε εξοικονόμηση κεφαλαίων αλλά και χώρου.

- Διαμοιρασμός μιας σύνδεσης Internet σε όλους τους υπολογιστές του δικτύου. Αυτό σημαίνει ότι η ύπαρξη μιας και μοναδικής σύνδεσης με το Διαδίκτυο αρκεί για να παράσχει πρόσβαση σε όλους τους υπολογιστές του τοπικού δικτύου. Η ταχύτητα σύνδεσης του κάθε υπολογιστή με το Internet εξαρτάται από το είδος της σύνδεσης (PSTN, ISDN, ADSL κ.λπ.) καθώς και από τον αριθμό των PC που βρίσκονται συνδεδεμένα στο Διαδίκτυο την ίδια στιγμή. Μία γρήγορη σύνδεση (ADSL ή ISDN, περίπου 24Mbps) αρκεί για να προσφέρει ικανοποιητική ταχύτητα σύνδεσης σε 3 υπολογιστές. Η δυνατότητα αυτή μειώνει σημαντικά το κόστος σύνδεσης και παροχής Internet.

- Αξιοποίηση υπολογιστών περιορισμένων δυνατοτήτων ή παλαιότερης τεχνολογίας. Αυτό σημαίνει ότι υπολογιστές που ως αυτόνομες μονάδες δεν μπορούσαν να χρησιμεύσουν σε κάτι αξιόλογο (λ.χ. επειδή δεν διέθεταν συσκευή ανάγνωσης CD-ROM ή επειδή ο σκληρός τους δίσκος είχε περιορισμένο αποθηκευτικό χώρο), μπορούν τώρα να ενταχθούν σε ένα μικρό δίκτυο και να παίξουν κάποιο ρόλο μέσα σ' αυτό.

Συμπερασματικά, η υλοποίηση ενός τοπικού δικτύου αποφέρει υπολογίσιμα οικονομικά, οργανωτικά, και λειτουργικά οφέλη.

7.3 Χαρακτηριστικά τοπικών δικτύων

Τρία είναι τα βασικά στοιχεία που συνθέτουν ένα τοπικό δίκτυο: η τοπολογία, το πρότυπο επικοινωνίας και η αρχιτεκτονική.

- Η τοπολογία απαντά στο "πώς" είναι συνδεδεμένοι μεταξύ τους οι υπολογιστές. Υπάρχουν διάφορες τοπολογίες δικτύων, καθεμία από τις οποίες απαιτεί ξεχωριστές τεχνολογικές υποδομές, για παράδειγμα διαφορετικά είδη καλωδίων.

Μία διαδεδομένη τοπολογία σε μικρά δίκτυα είναι αυτή του "αστεριού", όπου όλοι οι υπολογιστές συνδέονται μεταξύ του μέσω ενός hub (διανομέα) ή switch (ελεγκτή), διαμορφώνοντας ένα σχήμα που μοιάζει με αστέρι.

- Το πρότυπο ορίζει τους κανόνες βάσει των οποίων επιτυγχάνεται η επικοινωνία ανάμεσα στους υπολογιστές, και αναφέρεται τόσο στον εξοπλισμό όσο και στο λογισμικό. Υπάρχουν αρκετά πρότυπα, με πιο διαδεδομένο το Ethernet, το οποίο εδώ και χρόνια έχει καταστεί συνώνυμο της δικτύωσης στα LAN. Το Ethernet διακρίνεται σε υποκατηγορίες, βάσει ορισμένων

τεχνικών χαρακτηριστικών (π.χ. του είδους των καλωδίων που χρησιμοποιούνται στο δίκτυο, της ταχύτητας μεταφοράς δεδομένων που μπορεί να υποστηριχθεί κ.λπ.). Πιο διαδεδομένος είναι ο τύπος 100BaseT, που υποστηρίζει ταχύτητα 100Mbps ανά δευτερόλεπτο και απαιτεί καλωδίωση με καλώδια συνεστραμμένου ζεύγους UTP.

- Η αρχιτεκτονική σχετίζεται με το ρόλο και τα δικαιώματα των υπολογιστών που απαρτίζουν το δίκτυο. Η πιο συνηθισμένη αρχιτεκτονική αφορά στο σχήμα "διακομιστής προς κόμβους" (server - clients), όπου διακομιστής (server) είναι ένας κεντρικός υπολογιστής που συγκεντρώνει, αποθηκεύει και διανέμει δεδομένα, εφαρμογές, συνδέσεις κ.λπ. και κόμβοι (clients) είναι οι υπόλοιποι υπολογιστές, που χρησιμοποιούν τις υπηρεσίες και τα δεδομένα που τους προσφέρει ο server. Μία άλλη αρχιτεκτονική είναι αυτή του "κόμβου προς κόμβο" (peer to peer), όπου όλοι οι υπολογιστές συμμετέχουν στο δίκτυο ισότιμα, χωρίς αυτό να σημαίνει ότι επιτελούν και τις ίδιες λειτουργίες. Κάλλιστα, μπορεί ένας δεδομένος κόμβος τη μία στιγμή να λειτουργεί ως server και την άλλη ως client κ.ο.κ.

7.4 Απαιτούμενος εξοπλισμός

Προκειμένου να "στηθεί" ένα τοπικό δίκτυο, θα πρέπει προηγουμένως να έχει ολοκληρωθεί η σύνδεση σε επίπεδο υλικού εξοπλισμού και κατόπιν η σύνδεση σε επίπεδο λογισμικού. Σχετικά με τον εξοπλισμό, έστω ότι θέλουμε να δημιουργήσουμε ένα δίκτυο με τρεις ή περισσότερους υπολογιστές, ανάμεσα στους οποίους ο ένας θα είναι ο διακομιστής (server) και οι υπόλοιποι θα είναι οι κόμβοι (clients). Για την υλοποίηση του δικτύου θα απαιτηθούν: κάρτες δικτύου, καλώδια για τη σύνδεση των συσκευών και ένας διανομέας (hub ή switch).

Οι κάρτες δικτύου τοποθετούνται στην κεντρική μονάδα κάθε υπολογιστή (μία στον καθένα) και επιτρέπουν την επικοινωνία ανάμεσα στους κόμβους. Υπάρχουν διάφορα είδη καρτών, ανάλογα με το πρωτόκολλο επικοινωνίας που υποστηρίζουν, την ταχύτητα μεταφοράς δεδομένων κ.λπ. Θα χρειαστούμε ισάριθμες κάρτες με την ποσότητα των υπολογιστών, και συγκεκριμένα Ethernet κατηγορίας 100BaseT. Σήμερα είναι συνηθισμένο οι υπολογιστές να έχουν θύρα Ethernet ενσωματωμένη. Τα καλώδια ενώνουν τους υπολογιστές με το hub ή το switch. Η μία απόληξη συνδέεται στην κεντρική μονάδα κάθε υπολογιστή, στην έξοδο της κάρτας δικτύου, και η άλλη στην υποδοχή του hub. Για δίκτυο τριών υπολογιστών, χρειάζονται τρία καλώδια. Υπάρχουν διάφοροι τύποι καλωδίων. Ο καλύτερος τύπος για το δίκτυο που θέλουμε να

δημιουργήσουμε είναι το συνεστραμμένο ζεύγος UTP, το οποίο και αυτό απαντάται σε διάφορους τύπους ανάλογα με την ταχύτητα μεταφοράς δεδομένων που υποστηρίζει. Εμείς θα χρειαστούμε τρία καλώδια, που είναι κατάλληλα για Ethernet και ταχύτητα 100Mbps.

Το hub (διανομέας) είναι μία συσκευή πάνω στην οποία συνδέονται τα καλώδια των υπολογιστών του δικτύου, προκειμένου το ένα PC να επικοινωνεί με το άλλο. Το hub λαμβάνει τα δεδομένα από τους υπολογιστές και τα διανέμει στο δίκτυο, ακολουθώντας κάποιους κανόνες. Υπάρχουν διάφορα είδη hubs, που διαφέρουν μεταξύ τους στις δυνατότητες που προσφέρουν, στις υποδοχές που φέρουν (5, 8, 12, κ.λπ.), στο πρωτόκολλο που υποστηρίζουν κ.λπ. Εμείς θα χρειαστούμε ένα Fast Ethernet hub με 5 υποδοχές, ούτως ώστε να χρησιμοποιήσουμε τις τρεις και να αφήσουμε δύο ελεύθερες ως εφεδρικές, σε περίπτωση που μελλοντικά θελήσουμε να επεκτείνουμε το δίκτυο. Εναλλακτικά, μπορεί να χρησιμοποιηθεί ένα Ethernet switch. Το switch (ελεγκτής) είναι ένα είδος εξελιγμένου hub, που εξασφαλίζει μεγαλύτερη ταχύτητα μεταφοράς δεδομένων και ορθολογικότερη λειτουργία του δικτύου.

Συνοψίζοντας, αφού τοποθετήσουμε τις κάρτες δικτύου και "καλωδιώσουμε" υπολογιστές και hub, έχουμε ολοκληρώσει το κομμάτι του εξοπλισμού. Για να ολοκληρωθεί η εγκατάσταση, θα πρέπει να προβούμε και στις απαραίτητες ρυθμίσεις του λογισμικού, μέσα από το λειτουργικό μας σύστημα. Σημειώνεται ότι, αν η ταχύτητα των 100Mbps για τη μεταφορά των δεδομένων δεν μας καλύπτει, μπορούμε με τη χρήση διαφορετικού (και ακριβότερου) εξοπλισμού να φθάσουμε μέχρι και την ταχύτητα του 10Gbps.

7.5 Σκοποί των δικτύων

Οι σκοποί για τους οποίους δημιουργήθηκαν και αναπτύχθηκαν τα δίκτυα υπολογιστών είναι σε γενικές γραμμές :

- ο διαμερισμός των πόρων (προγράμματα, δεδομένα, εξοπλισμός)
- η παροχή υψηλής αξιοπιστία
- η εξοικονόμηση χρημάτων
- ισχυρό μέσο επικοινωνίας

7.6 Δομή δικτύου

Σε κάθε δίκτυο υπάρχει ένα πλήθος από μηχανήματα, τα οποία σκοπό έχουν να τρέχουν τα προγράμματα του χρήστη. Ακολουθούμε την ορολογία ενός από τα μεγαλύτερα δίκτυα, του ARPANET, και ονομάζουμε τα αυτά μηχανήματα hosts (κεντρικοί υπολογιστές). Οι hosts συνδέονται μεταξύ τους με το υποδίκτυο επικοινωνίας του οποίου το έργο είναι η μεταφορά μηνυμάτων από host σε host.

Στα περισσότερα δίκτυα ευρείας περιοχής το υποδίκτυο αποτελείται από δύο διακεκριμένα στοιχεία : τις γραμμές μετάδοσης και τα στοιχεία μεταγωγής. Οι γραμμές μετάδοσης μετακινούν bits ανάμεσα στα διάφορα μηχανήματα. Τα στοιχεία μεταγωγής είναι ειδικοί υπολογιστές που χρησιμοποιούνται για τι σύνδεση δύο η περισσοτέρων γραμμών μετάδοσης. Θα ονομάσουμε τα στοιχεία μεταγωγής IMPs (Interface Message proccesors).

Όταν ένα μήνυμα (στο περιβάλλον του υποδικτύου συνήθως ονομάζεται πακέτο) στέλνεται από έναν IMP σ' έναν άλλο μέσω ενός η περισσοτέρων ενδιάμεσων IMPs. το μήνυμα λαμβάνεται σε κάθε ενδιάμεσο IMP σε όλη του την έκταση, αποθηκεύεται εκεί, έως ότου η επιθυμητή γραμμή εξόδου είναι ελεύθερη και μετά προωθείται. Το υποδίκτυο που χρησιμοποιεί αυτή τη μέθοδο ονομάζεται από σημείο σε σημείο, αποθήκευσης και προώθησης ή μεταγωγής πακέτων υποδίκτυο.

7.7 Τα Πρωτόκολλα Σύνδεσης Τοπικών Δικτύων

- Το Fiber Distributed Data Interconnect(FDDI) είναι ένα LAN πρωτόκολλο που επιτρέπει επικοινωνία μεταξύ των κόμβων έως 100Mbps. Χρησιμοποιεί οπτικές ίνες και οι πληροφορία αποστέλλεται με παλμούς φωτός. Κάθε κόμβος που θέλει να αποστείλει πληροφορία περιμένει να έρθει η σειρά του, καθώς η αποστολή πακέτων στο δίκτυο γίνεται κυκλικά από τους κόμβους. Στο FDDI υπάρχουν πολλοί μηχανισμοί αυτοδιαμόρφωσης και αυτοδιόρθωσης. Το μέγιστο μέγεθος για ένα πακέτο είναι 4500Bytes. Στο μέλλον είναι πιθανό το μέγεθος του πακέτου να αυξηθεί.
- Το Token Ring. Η διακίνηση των δεδομένων γίνεται όπως και στο FDDI. Λειτουργεί στα 4 ή 16 Mbps. Το μέγεθος του πακέτου που μπορεί να στείλει ο κάθε κόμβος εξαρτάται από το χρονικό διάστημα που έχει δικαίωμα αποστολής.

- Το Point to Point Protocol (PPP). Είναι ένας μηχανισμός που τρέχει το IP και άλλα πρωτόκολλα μέσω μιας συριακής σύνδεσης. Υποστηρίζει σύγχρονη και ασύγχρονη μετάδοση. Το PPP Interface δεν έχει διεύθυνση MAC. Ένας μηχανισμός που ονομάζεται Interface Identifier παρέχει την δυνατότητα διαπραγμάτευσης μιας διεύθυνσης που είναι μοναδική για κάθε PPP σύνδεση. Στην IPv6 η απόκτηση διεύθυνσης είναι διαφορετική από την IPv4. Γίνεται μέσω του Neighbor Discovery που έχει αναφερθεί και προηγουμένως. Για τους παρόχους Ίντερενετ, το PPP σε συνδυασμό με το IPv6 παρέχει πάρα πολλά πλεονεκτήματα. Παράδειγμα, δεν είναι πλέον πρόβλημα να παρέχουν μία στατική διεύθυνση στους πελάτες τους καθώς το πρόβλημα έλλειψης έχει λυθεί. Μέχρι τώρα ήταν αναγκαίο να χρησιμοποιούνται δυναμικές διευθύνσεις. Επίσης, η λειτουργικότητα της IPv6 προσφέρει εύκολη διαχείριση και ρύθμιση για τον πελάτη, με ελάχιστο κόστος.
- Το Asynchronous Transfer Mode (ATM) είναι μία τεχνολογία δικτύωσης για πολύ υψηλές ταχύτητες και χρησιμοποιείται για LAN και WAN. Λειτουργεί μέσω οπτικής ίνας και φτάνει gigabit ταχύτητες χρησιμοποιώντας ειδικό hardware και software. Το ATM δίκτυο χρησιμοποιεί πακέτα ορισμένου μεγέθους που ονομάζονται κύτταρα. Κάθε κύτταρο έχει μέγεθος 53Bytes. Αυτό κάνει την επεξεργασία των πακέτων πολύ γρήγορη. Τα μεγάλα IP πακέτα διασπώνται σε μικρότερα με μία διαδικασία παρόμοια αυτής του fragmentation.Αν ένα κύτταρο χαθεί στην μετάδοση, τότε ολόκληρη η ομάδα κυττάρων πρέπει να ξανασταλθεί.

7.8 Το μοντέλο αναφοράς OSI

Το μοντέλο που βασίζεται σε πρόταση που αναπτύχθηκε από το Διεθνή οργανισμό Τυποποίησης (ISO) ως ένα πρώτο βήμα για την διεθνή τυποποίηση των διαφόρων πρωτοκόλλων ονομάζεται Μοντέλο αναφοράς OSI (Open Interconnection) του ISO διότι ασχολείται με συνδέσεις ανοιχτών συστημάτων, δηλαδή αυτά που είναι ανοικτά για επικοινωνία με άλλα συστήματα. Το μοντέλο OSI έχει 7 επίπεδα. Οι αρχές που εφαρμόζονται για να φτάσουμε σ' αυτά είναι οι ακόλουθες:

- Ένα επίπεδο πρέπει να δημιουργείται εκεί όπου χρειάζεται διαφορετικός βαθμός αφαίρεσης
- Κάθε επίπεδο πρέπει να εκτελεί μια καλά προσδιορισμένη λειτουργία
- Η λειτουργία κάθε επιπέδου πρέπει να επιλέγεται με βάση τα καθορισμένα διεθνή

τυποποιημένα πρωτόκολλα

- Η επιλογή των ορίων των επιπέδων πρέπει να γίνεται με σκοπό την ελαχιστοποίηση της ροής των πληροφοριών μέσω των διασυνδέσεων
- Ο αριθμός των επιπέδων θα πρέπει να είναι αρκετά μεγάλος, ώστε διακεκριμένες λειτουργίες να μην χρειάζεται να τοποθετηθούν μαζί στο ίδιο επίπεδο, χωρίς να υπάρχει τέτοια ανάγκη, και αρκετά μικρός ώστε η αρχιτεκτονική να μην γίνεται πολύπλοκη.

Σχ7.8.1 Μοντέλο OSI

Με βάση τα παραπάνω τα εφτά επίπεδα με βάση το μοντέλο OSI είναι:

1. Το Φυσικό επίπεδο, ασχολείται με τη μετάδοση ακατέργαστων bits σε ένα κανάλι επικοινωνίας.

2. Το επίπεδο Σύνδεσης Δεδομένων, του οποίου κύρια αποστολή είναι να μετασχηματίζει το ακατέργαστο μέσο μετάδοσης σε μια γραμμή που εμφανίζεται ελεύθερη από σφάλματα μετάδοσης στο επίπεδο δικτύου.

3. Το επίπεδο Δικτύου ασχολείται με τον έλεγχο της λειτουργίας του υποδικτύου.

4. Το επίπεδο Μεταφοράς, του οποίου βασική λειτουργία είναι η αποδοχή δεδομένων από το επίπεδο συνόδου, η διάσπαση αυτών σε μικρότερες μονάδες εάν χρειαστεί, η μεταφορά τους στο επίπεδο δικτύου και η διασφάλιση ότι όλα τα τμήματα φτάνουν σωστά στην άλλη πλευρά.

5. Το επίπεδο Συνόδου, το οποίο επιτρέπει στους χρήστες διαφορετικών μηχανημάτων να

εγκαθιστούν συνόδους μεταξύ τους.

6. Το επίπεδο Παρουσίασης, το οποίο εκτελεί συγκεκριμένες λειτουργίες οι οποίες ζητούνται αρκετά συχνά από τους χρήστες, για να εξασφαλίσουν την εύρεση μιας γενικής λύσης γι αυτούς, ώστε να μην αφήνεται κάθε χρήστης να λύνει τα προβλήματα μόνος του.

7. Το επίπεδο Εφαρμογής, το οποίο περιέχει μια ποικιλία πρωτοκόλλων που χρειάζονται συχνά.

Κεφάλαιο 8ο - Active Directory

8.1 Εισαγωγή

Το Active Directory είναι μια δομή που χρησιμοποιείται στα Windows, βασίζεται σε υπολογιστές και διακομιστές για την αποθήκευση πληροφοριών και δεδομένων σχετικά με δίκτυα και τομείς. Χρησιμοποιείται κυρίως για online πληροφορίες, δημιουργήθηκε αρχικά το 1996 και χρησιμοποιήθηκε για πρώτη φορά με τα Windows 2000.

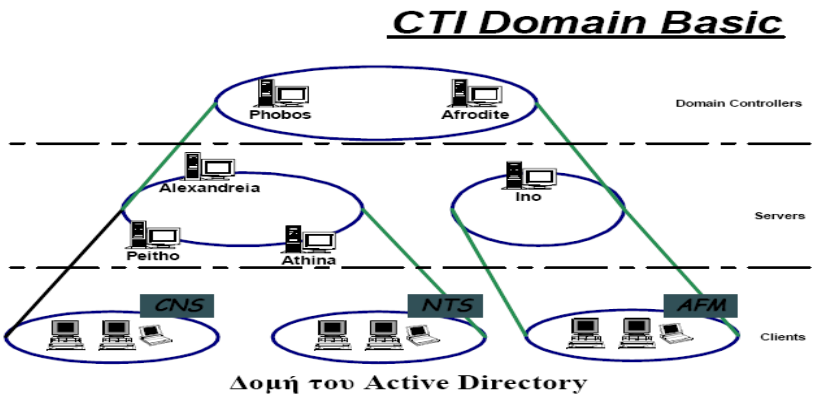
Το Active Directory κάνει μια ποικιλία λειτουργιών όπως είναι:

- Η ικανότητα παροχής πληροφοριών σχετικά με αντικείμενα,
- Βοηθά στην οργάνωση αυτόν των αντικειμένων για την ανάκτηση και την εύκολη πρόσβαση τους,
- Επιτρέπει την πρόσβαση από τους τελικούς χρήστες και τους διαχειριστές
- Και επιτρέπει στο διαχειριστή να ρυθμίζει την ασφάλεια των καταλόγων.

Το Active Directory μπορεί να οριστεί ως μια ιεραρχική δομή και η δομή αυτή συνήθως χωρίζεται σε τρεις βασικές κατηγορίες:

- Οι πόροι που περιλαμβάνει (το υλικό όπως εκτυπωτές)
- Υπηρεσίες για τελικούς χρήστες (όπως είναι το email)
- Και αντικείμενα (τα οποία είναι τα κύρια καθήκοντα του τομέα και του δικτύου)

8.2 Δομή του Active Directory



Σχ8.2.1 Δομή του Active Directory

8.3 Σχεδιασμένος και αξιοπιστία

Οι σύγχρονες εταιρείες θέλουν την τεχνολογία αδιάκοπο σύμμαχο της επιχειρηματικής αξίας. Θέλουν συστήματα που να λειτουργούν και να ανταποκρίνονται πάντα και απαιτούν ένα επίπεδο ασφαλείας αντάξιο των σύγχρονων προκλήσεων. Ο Windows Server 2008, περιλαμβάνει νέες δυνατότητες και βελτιώσεις που τον καθιστούν το πιο αξιόπιστο λειτουργικό σύστημα διακομιστή που έχει δημιουργήσει ποτέ η Microsoft για εταιρείες: η απόλυτη απόδειξη της δέσμευσης της Microsoft στη δημιουργία αξιόπιστων συστημάτων για υπολογιστές.

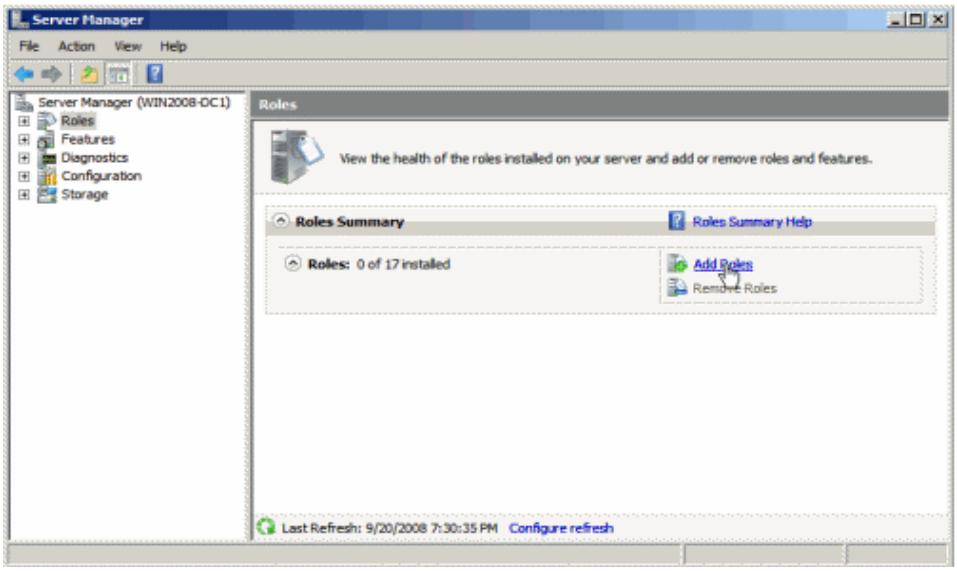
Έχουν βελτιωθεί οι τεχνολογίες που εφαρμόστηκαν αρχικά στον Windows 2008 Server, όπως η δυνατότητα εξισορρόπησης φόρτου δικτύου, τα συμπλέγματα διακομιστών και η υπηρεσία καταλόγου Active Directory. Επιπλέον, η Microsoft εισάγει νέες τεχνολογίες στον Windows Server 2008, Datacenter Edition όπως τον νέο κοινό χρόνο εκτέλεσης γλώσσας που προστατεύει δίκτυα από κακόβουλο ή κακά σχεδιασμένο κώδικα.

Οι επιδόσεις και η ευελιξία της υπηρεσίας καταλόγου Active Directory είναι πλέον ταχύτερες και σταθερότερες σε μη αξιόπιστες συνδέσεις δικτύων ευρείας ζώνης (WAN). Αυτό οφείλεται στον αποτελεσματικότερο συγχρονισμό και την αναπαραγωγή, καθώς και στην προσωρινή αποθήκευση πιστοποιήσεων σε ελεγκτές τομέα υποκαταστημάτων.

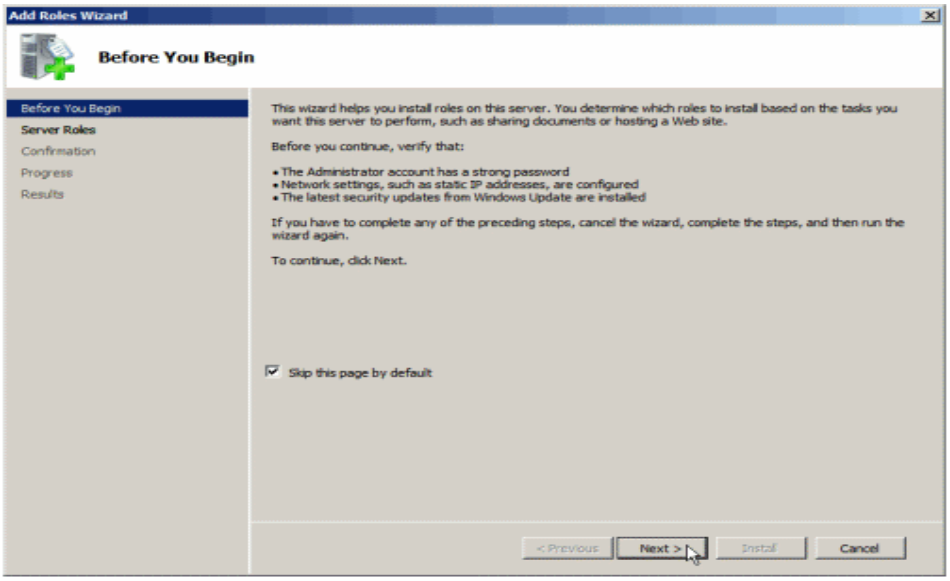
8.4 Υλοποίηση Active Director

Σε αυτήν την ενότητα θα δούμε πως υλοποιούμε το active directory στα windows server 2008

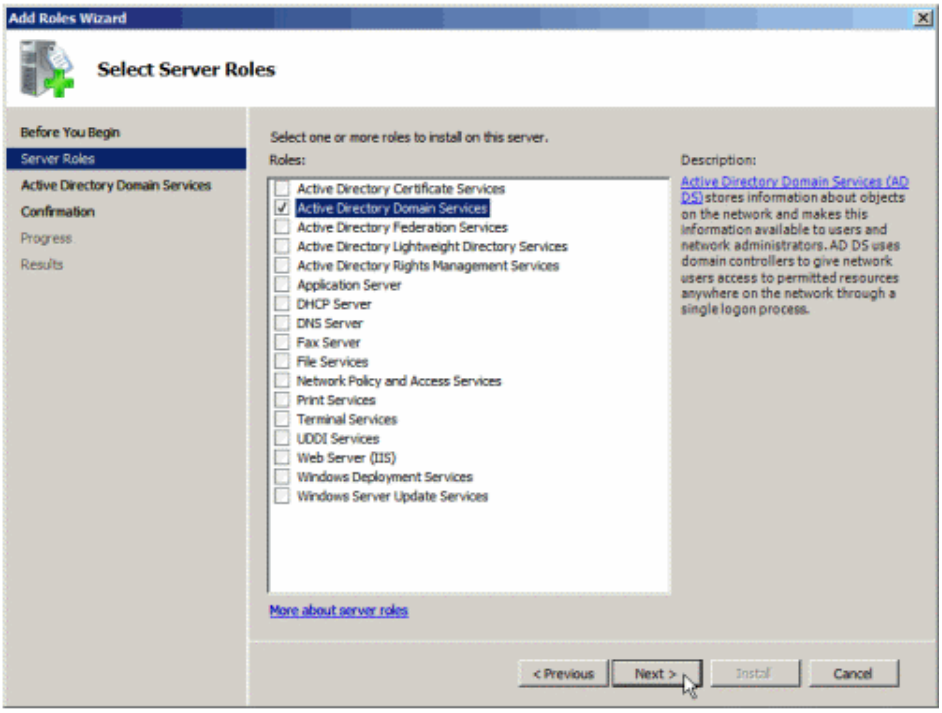
1. Ανοίγουμε το **Server Manager από την έναρξη**.
2. Πατάμε **Roles→ κα μετά Add Roles** .



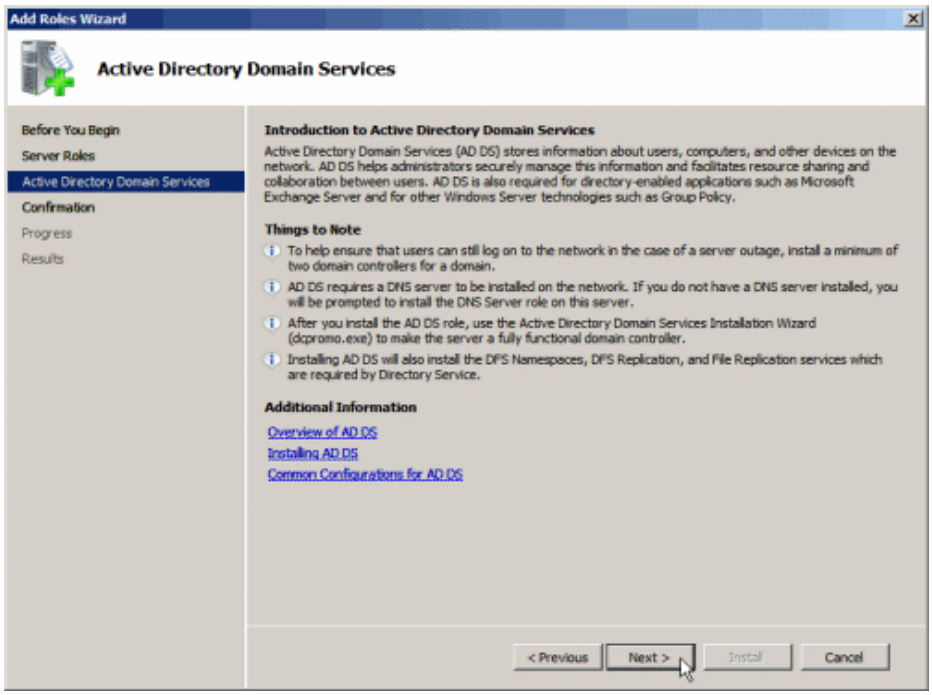
3. Μετά πατάμε **Next**.



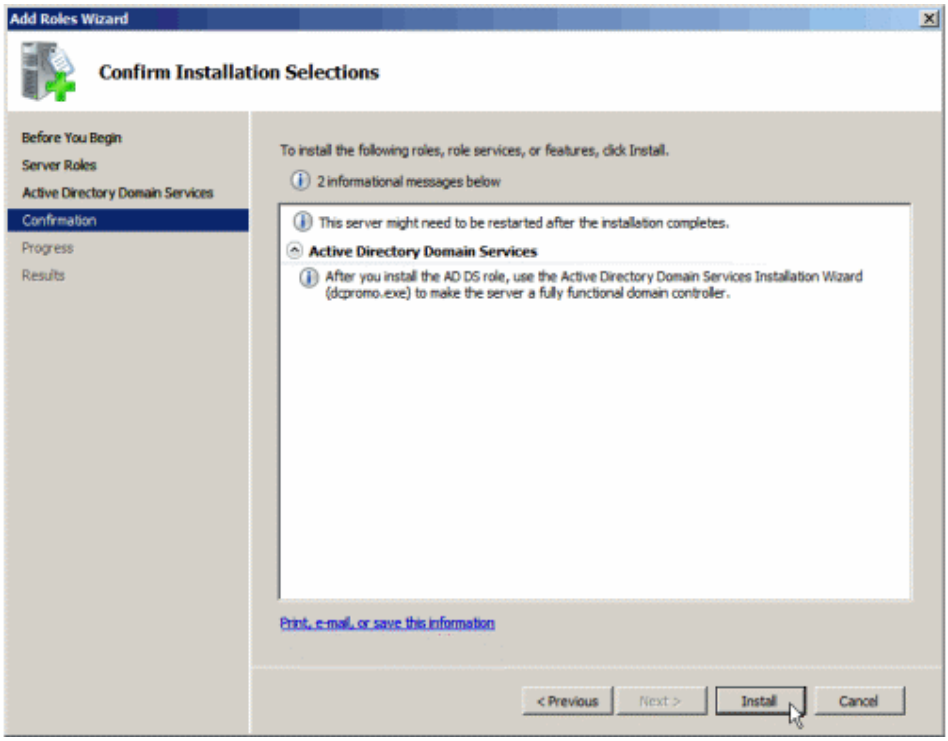
4. Επιλέγουμε το **Active Directory Domain Services**, και πατάμε **Next**.



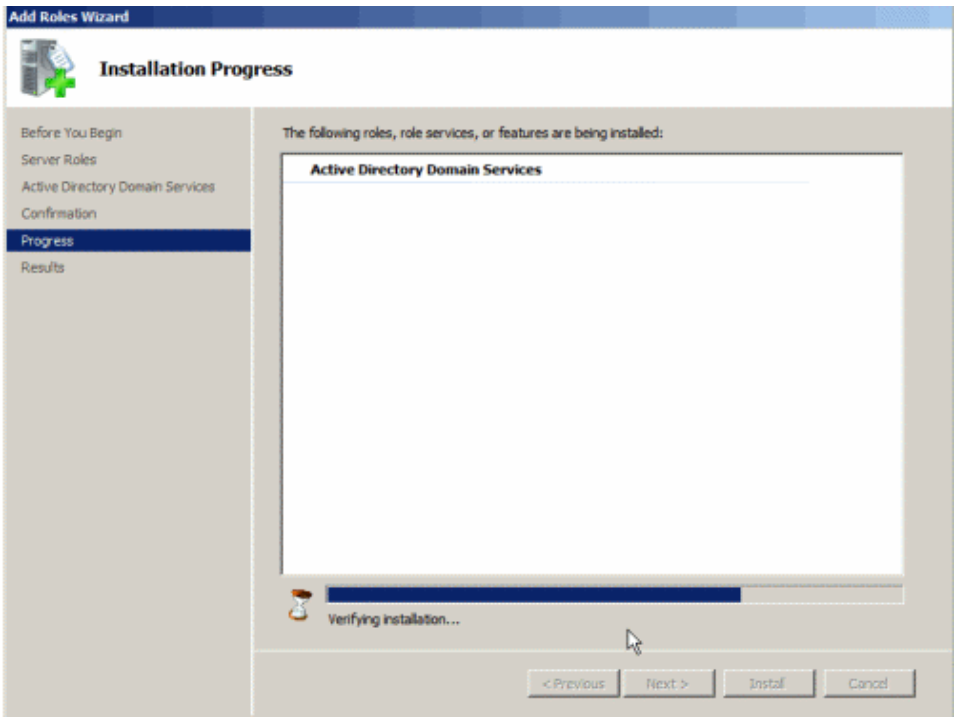
5. Στο παράθυρο Active Directory Domain Services window διαβάζουμε τις πληροφορίες και πατάμε **Next**.



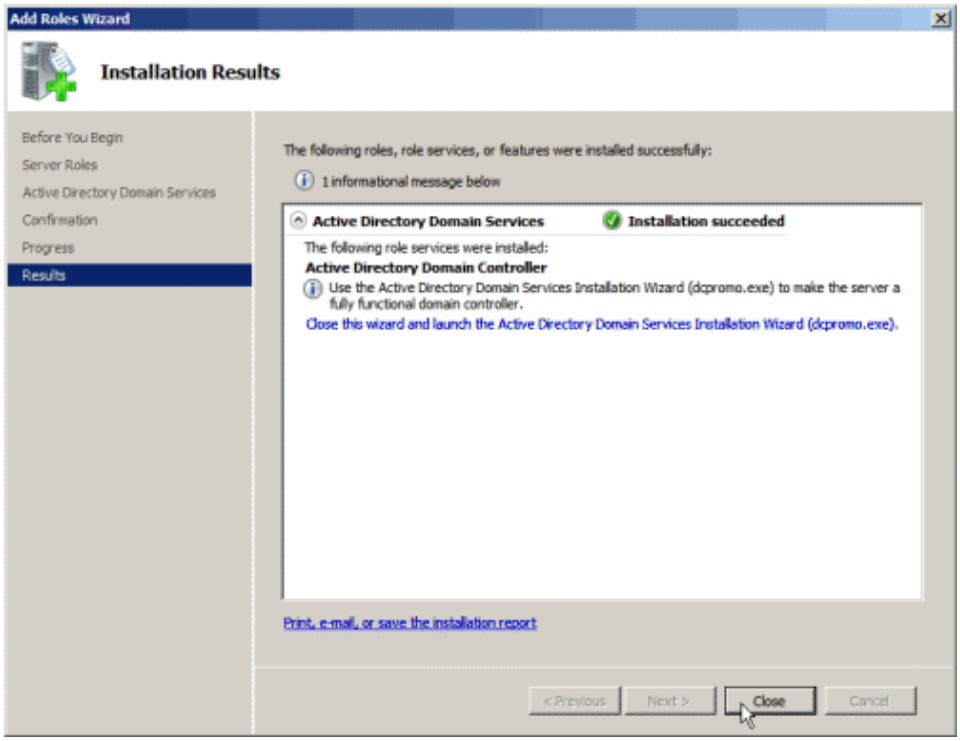
6. Διαβάζουμε τις πληροφορίες και πατάμε **Next**.



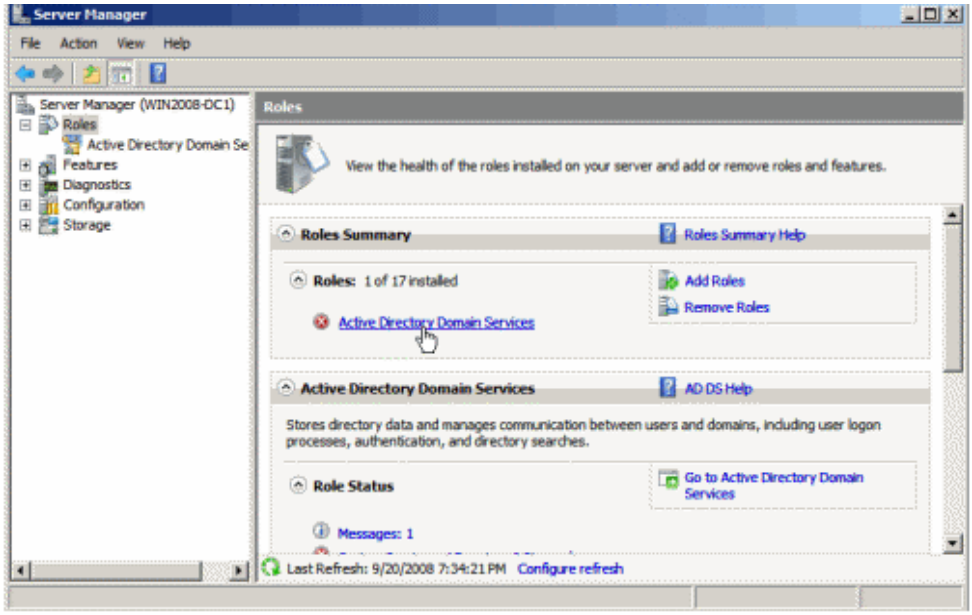
7. Περιμένουμε να ολοκληρωθεί η διαδικασία



8. Όταν τελειώσει πατάμε **Close**.



9. Πάμε πάλι στο Server Manager, πατάμε **Active Directory Domain Services**, και παρατηρούμε ότι δεν υπάρχουν οι διαθέσιμες πληροφορίες γιατί δεν έχουμε τρέξει την εντολή DCPROMO και να δημιουργήσουμε έναν DNS (βλέπε κεφάλαιο 10).



Κεφάλαιο 9ο - DNSv6

9.1 Εισαγωγή

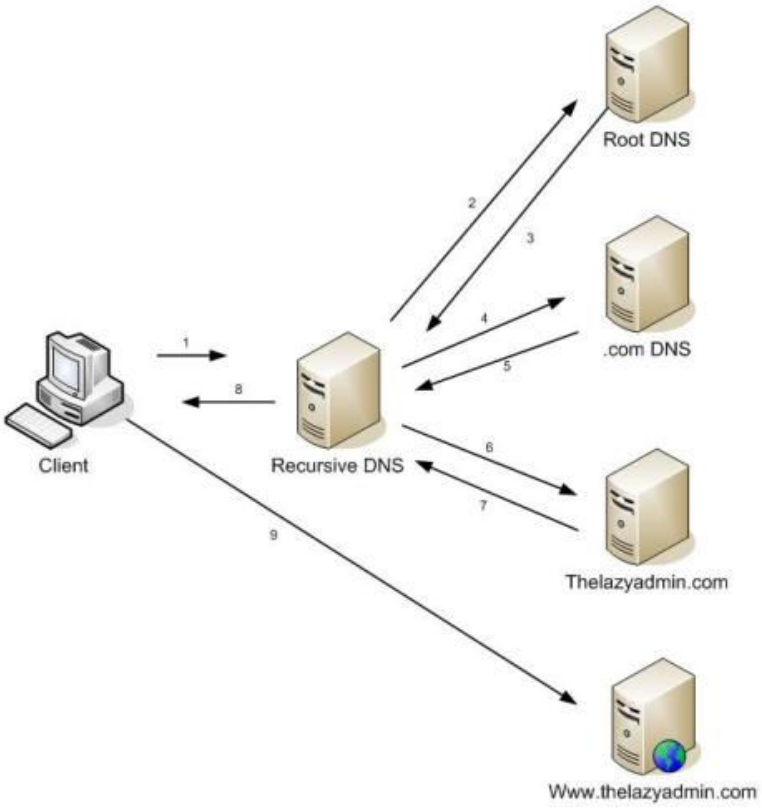
Η υπηρεσία DNS είναι βασική για την πλοήγηση των χρηστών στο Internet καθώς διασφαλίζει την αντιστοίχιση Internet ονομάτων σε IP διευθύνσεις (πχ το el.teithe.gr αντιστοιχίζεται στην IP διεύθυνση 195.251.241.50). Με το IPv6 η ανάγκη για το DNS είναι ακόμη μεγαλύτερη καθώς ο αριθμός των διευθύνσεως είναι ακόμη μεγαλύτερος.

9.2 Ονοματοδοσία

Τα τερματικά αναγνωρίζονται επίσης στο δίκτυο από τα ονόματά τους (*Host Names*). Τα ονόματα αυτά είναι καθοριζόμενα από τους χρήστες (ψευδώνυμα), τα οποία χρησιμοποιούνται για τη δήλωση των τερματικών συστημάτων. Μία σημαντική διάκριση μεταξύ ονομάτων και διευθύνσεων είναι ότι οι διευθύνσεις μπορεί να είναι συγκεκριμένες ανάλογα με το χρησιμοποιούμενο πρωτόκολλο (π.χ. IP διεύθυνση), αλλά τα ονόματα όχι. Τα ονόματα προσφέρουν ένα τρόπο αναφοράς από τις εφαρμογές στις οντότητες του δικτύου, χωρίς να χρειάζεται οι εφαρμογές αυτές να γνωρίζουν τίποτα επιπλέον για το υποκείμενο πρωτόκολλο δικτύου που χρησιμοποιείται. Κάτι τέτοιο είναι πολύ χρήσιμο αφού για τους χρήστες είναι πολύ πιο εύκολο να χρησιμοποιούν και να θυμούνται ονόματα σε σχέση με τις δύσχρηστες διευθύνσεις δικτύου.

Μολονότι λοιπόν οι εφαρμογές αναφέρονται στα τερματικά συστήματα με ονόματα, όταν τα πακέτα διακινούνται διαμέσου του Internet κάθε ένα από αυτά πρέπει να περιέχει μία IP διεύθυνση του κόμβου προορισμού. Αυτό γίνεται διότι οι δρομολογητές στο Internet δεν "καταλαβαίνουν" τα ονόματα, παρά μόνο μπορούν και μεταφράζουν διευθύνσεις. Απαιτείται συνεπώς ένας μηχανισμός μετασχηματισμού των ονομάτων των τερματικών σε διευθύνσεις. Για να εξυπηρετηθεί αυτό το τεράστιο και ραγδαία επεκτεινόμενο σύνολο ονομάτων, αναπτύχθηκε στο Internet ένας αποκεντρωμένος μηχανισμός ονοματοδοσίας ο οποίος λέγεται "*Domain Name System*" (*DNS*). Το σύστημα DNS αποθηκεύει την αντιστοιχία μεταξύ ονόματος και διεύθυνσης σε μια κατανεμημένη δομή δεδομένων και έτσι η εύρεση της διεύθυνσης ενός τερματικού αποτελεί ουσιαστικά μία λειτουργία εύρεσης καταλόγου (*directory lookup operation*). Όταν

λοιπόν δύο τερματικά χρειάζεται να επικοινωνήσουν στο Internet, ο κόμβος-πηγή εκτελεί μια DNS αναζήτηση για να προμηθευτεί τη διεύθυνση του κόμβου-προορισμού και στη συνέχεια ξεκινά μια διαδικασία εγκατάστασης σύνδεσης. Κατά τη διάρκεια της εγκατάστασης της σύνδεσης κάθε άκρο της σύνδεσης λαμβάνει και "μαθαίνει" τη διεύθυνση του άλλου άκρου. Για όσο διάστημα λοιπόν η σύνδεση παραμένει ενεργή, δεν γίνονται επιπλέον DNS αναζητήσεις αφού η συσχέτιση (*binding*) ονόματος και διεύθυνσης θεωρείται στατική και δεν αναμένεται να αλλάξει κατά τη διάρκεια της ύπαρξης της σύνδεσης.



Σχήμα 9.2.1 : Η λειτουργία του συστήματος DNS

9.3 Προβλήματα DNS

Στα δίκτυα όπου τα τερματικά είναι στατικά, η συσχέτιση μεταξύ ονομάτων και διευθύνσεων δεν αλλάζει ποτέ. Αντίθετα, η κινητικότητα των τερματικών κάνει αυτή τη συσχέτιση μια συνάρτηση του χρόνου. Επομένως είναι απαραίτητοι μηχανισμοί στο στρώμα του δικτύου για την ανάλυση των ονομάτων σε διευθύνσεις και για την ανίχνευση της θέσης των τερματικών καθώς αυτά

μετακινούνται. Το σύστημα DNS, το οποίο παρέχει την υπηρεσία μετάφρασης του ονόματος σε διεύθυνση στο Internet σήμερα, θα μπορούσε να εμπλουτιστεί έτσι ώστε να ικανοποιήσει τις επιπρόσθετες απαιτήσεις. Ωστόσο κάτι τέτοιο γίνεται εξαιρετικά δύσκολο εξαιτίας πολλών εμποδίων όπως:

- Στο DNS δεν υπήρχε πρόβλεψη για διευθέτηση δυναμικών ενημερώσεων και αυτό διότι αρχικά σχεδιάστηκε για να παρέχει υπηρεσίες εύρεσης ονομάτων μόνο για σταθερά τερματικά.
- Η σχεδίαση του DNS είναι τέτοια ώστε να βελτιστοποιεί το κόστος προσπέλασης (*access cost*) και όχι το κόστος ενημέρωσης (*update cost*). Τα αντίγραφα στους εξυπηρετητές και η αποθήκευση (*caching*) από τους πελάτες, προσδίδουν σημαντικά οφέλη στις επιδόσεις για συστήματα που εκτελούν μόνο προσπελάσεις αλλά έχουν ως αποτέλεσμα πολύ χαμηλές επιδόσεις όταν εκτελούνται ενημερώσεις. Σε ένα περιβάλλον κινητών τερματικών όμως, τόσο ενημερώσεις όσο και προσπελάσεις συμβαίνουν συνεχώς.
- Οι πελάτες του συστήματος DNS κάνουν cashing σε DNS πληροφορίες που έχουν ήδη λάβει έτσι ώστε να μειώνουν την καθυστέρηση για μελλοντικές προσπελάσεις καθώς και για να μειώνεται η επιβάρυνση στους εξυπηρετητές του συστήματος. Όμως, δεν υπάρχει γενικά διαθέσιμος μηχανισμός ανάκλησης από τους εξυπηρετητές στους πελάτες, για την περίπτωση που οι cache καταχωρίσεις έχουν καταστεί άκυρες.

Όσον αφορά το Internet λοιπόν, μια λύση βασισμένη σε κατανεμημένη υπηρεσία καταλόγου έτσι ώστε να υποστηρίζονται κινητά τερματικά δεν εμφανίζεται πολύ ελκυστική αφού δεν είναι δυνατόν να αναπτυχθεί χωρίς την αλλαγή του υπάρχοντος λογισμικού των τερματικών. Δεδομένου όμως του παρόντος μεγέθους του Internet γίνεται αντιληπτό ότι μια τέτοια αλλαγή στο λογισμικό είναι σχεδόν αδύνατο να επιτελεσθεί. Γι' αυτό το λόγο απαιτείται μια εναλλακτική λύση.

9.4 Διαφορές DNSv6 με DNSv4

Για την ορθή λειτουργία ενός δικτύου IPv6, είναι φανερό ότι εκτός από την ανάθεση διευθύνσεων IPv6 είναι αναγκαίες και άλλες συμπληρωματικές ρυθμίσεις, όπως π.χ. οι διευθύνσεις των εξυπηρετητών DNS. Στο IPv4 η μετάδοση της πληροφορίας του ποιοι είναι οι DNS servers στους πελάτες γινόταν με την βοήθεια των αντίστοιχων μηχανισμών του IPCP. Στο IPv6 PPP, το IPCPv6 δεν διαθέτει κάποιον ουσιώδη ρόλο όσον αφορά αυτή την λειτουργία. Αντ' αυτού, προσφέρονται οι εξής δυνατότητες σχετικά με τις ρυθμίσεις των DNS servers στους

τελικούς hosts:

- Μετάδοση των ρυθμίσεων μέσω ειδικού μηχανισμού στις ενημερώσεις των routers που στέλνουν οι gateways.
- Μετάδοση μέσω DHCPv6 stateless mode.
- Χρησιμοποίηση διευθύνσεων anycast.

9.5 Πλεονεκτήματα DNSv6

9.5.1 Διευθύνσεις Unicast (μόνο-μετάδοσης)

Μια unicast διεύθυνση προσδιορίζει ένα μοναδικό interface. Τα πακέτα τα οποία στέλνονται σε μια unicast διεύθυνση προορισμού, παραδίδονται σε αυτό και μόνο το interface.

Το IPv6 περιλαμβάνει διάφορους υποτύπους unicast διευθύνσεων:

- Aggregatable unicast διευθύνσεις: Οι aggregatable global unicast διευθύνσεις είναι ένα ιεραρχικά δομημένο σχήμα διευθύνσεων, το οποίο αποτελεί το αρχικά χρησιμοποιούμενο πλάνο ανάθεσης διευθύνσεων για τους IPv6 κόμβους. Αυτή η μορφή διευθύνσεων έχει σχεδιαστεί για να βελτιστοποιήσει τη δρομολόγηση υψηλών ταχυτήτων στα δίκτυα κορμού του διαδικτύου εισάγοντας μια πολύ επίπεδη τοπολογία διευθύνσεων χωρισμένες σε public, site, interface τοπολογίες.
- Local Addresses (Τοπικές διευθύνσεις): Το IPv6 προσδιορίζει τρεις τύπους διευθύνσεων για τοπική χρήση και μόνο, δηλαδή IP πακέτα που περιέχουν τοπική διεύθυνση πηγής ή προορισμού περιορίζονται σε μια φυσική περιοχή. Τα τοπικά πακέτα δε δρομολογούνται ποτέ έξω από αυτή τη φυσική περιοχή. Η Loopback διεύθυνση, 0:0:0:0:0:0:0:1 (::1) αναφέρεται στο εικονικό Interface, το οποίο είναι ενσωματωμένο σε κάθε IPv6 host για τοπική εντός host επικοινωνία. Έχει την ίδια λειτουργικότητα με το localhost interface (127.0.0.1) του IPv4. Οι Link local διευθύνσεις χρησιμοποιούνται για επικοινωνία σε ένα μοναδικό τμήμα (segment) του δικτύου IPv6. Αυτό θα μπορούσε να συμβαίνει σε ένα οικιακό δίκτυο, μια μικρή επιχείρηση ή σε 2 υπολογιστές συνδεδεμένους απ' ευθείας μεταξύ τους. Κάθε IPv6 interface απαιτείται να έχει τουλάχιστον μια link local διεύθυνση ανατεθειμένη και αυτόματα αναθέτει στον εαυτό του μια κατά τη στιγμή της εκκίνησής του. Το πώς πραγματοποιείται αυτή η ανάθεση εξαρτάται στο υποκείμενο μέσο (π.χ. Ethernet,

ATM, IEEE 1394 κ.ο.κ.). Οι link local διευθύνσεις χρησιμοποιούνται ευρέως στις διαδικασίες αυτόματης ρύθμισης παραμέτρων (autoconfiguration) του IPv6. Οι Site Local διευθύνσεις έχουν σχεδιαστεί για να επιτρέπουν σε τοποθεσίες με πολλαπλούς συνδέσμους ή τμήματα δικτύου να επικοινωνούν τοπικά χωρίς την ανάγκη ενός γενικού (global) προθέματος. Αυτή θα μπορούσε να είναι η περίπτωση ενός απομονωμένου εταιρικού δικτύου ή μιας κατοικημένης περιοχής χωρίς την ανάγκη γενικής (global) επικοινωνίας.

9.5.2 Διευθύνσεις multicast (πολλαπλής διανομής)

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

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

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

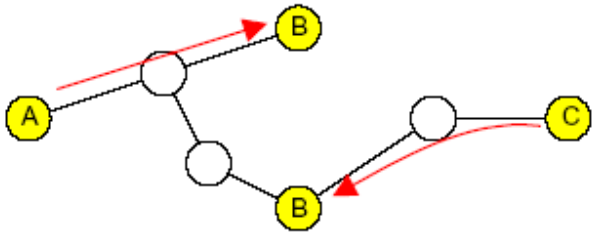
Οι τιμές που απουσιάζουν από τον πίνακα, δεν έχουν μέχρι στιγμής καταχωρηθεί και είναι διαθέσιμες στους διαχειριστές του δικτύου για να τις ορίσουν οι ίδιοι.

Τέλος, το πεδίο group identifier της διεύθυνσης διαχωρίζει μια multicast σύνοδο μέσα στην τρέχουσα εμβέλεια. Στο IPv6, το multicast θεωρείται σαν ένας κοινός τρόπος επικοινωνίας, σε αντίθεση με ότι συνέβαινε στο IPv4. Αυτό καθίσταται πολύ εύκολα αντιληπτό παρατηρώντας το

αναγνωριστικό μήκους 112 bit του IPv6 σε σχέση με τα 28 bits που είναι διαθέσιμα στις διευθύνσεις τάξεως D του IPv4. Για παράδειγμα το multicast στο IPv6 αντικαθιστά το broadcast στο IPv4.

9.5.3 Διευθύνσεις anycast (μετάδοση σε οποιονδήποτε)

Το anycast είναι ένα καινούριο χαρακτηριστικό που παρουσιάζεται για πρώτη φορά στο IPv6. Μια anycast διεύθυνση είναι μια IPv6 διεύθυνση ανατεθειμένη σε πολλαπλά interfaces, η οποία συχνά ανήκει σε διαφορετικούς κόμβους. Οι anycast διευθύνσεις δε διακρίνονται από τις unicast και μπορεί να χρησιμοποιήσουν οποιοδήποτε σχήμα ανάθεσης unicast διεύθυνσης. Τα πακέτα που στέλνονται σε μια anycast διεύθυνση παραλαμβάνονται από το κοντινότερο, σύμφωνα με την απόσταση δρομολόγησης, στον αποστολέα interface. Η εικόνα 10.2 απεικονίζει ένα απλό παράδειγμα με 2 hosts (A και C), όπου και οι δύο ορίζουν τον B σαν τη διεύθυνση προορισμού.



Σχ 9.5.3.1 Anycasting

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

9.6 Autoconfiguration (Αυτόματη απόκτηση παραμέτρων)

Η αυτόματη απόκτηση παραμέτρων ενός κόμβου είναι μια διαδικασία που αποτελείται από πολλά βήματα.

Η πλήρης διαδικασία είναι η ακόλουθη:

- Το interface ενεργοποιείται
- Μια link local διεύθυνση δημιουργείται (αλλά δεν ανατίθεται στο interface) συνενώνοντας το προκαθορισμένο πρόθεμα FE80::/10 με ένα 64-bit αναγνωριστικό του interface (interface identifier), όπως περιγράφεται στην ενότητα 2.3.4. Το αναγνωριστικό του interface μπορεί τυπικά να είναι η IEEE 802 διεύθυνση της κάρτας του interface δικτύου (π.χ. Ethernet, FDDI) ή ένας άλλος μοναδικός αριθμός που έχει ληφθεί από άλλα τμήματα του κόμβου (π.χ. ο σειριακός αριθμός της μητρικής πλακέτας).
- Κατόπιν χρησιμοποιείται το neighbor discovery για να ελέγξει, αν η νέα διεύθυνση είναι μοναδική (στη ζεύξη). Αυτό γίνεται στέλνοντας μηνύματα αιτήσεις neighbor discovery με την διεύθυνση προορισμού να τίθεται στη διεύθυνση που ελέγχεται και τη διεύθυνση πηγής να τίθεται στην ακαθόριστη διεύθυνση (::). Αν μέσω μηνυμάτων neighbor discovery ληφθεί η πληροφορία ότι η διεύθυνση δεν είναι μοναδική, τότε χρειάζεται να επαναδημιουργηθεί είτε χειροκίνητα, είτε τυχαία και να επαναληφθεί η διαδικασία.
- Όταν διαπιστωθεί ότι η link local διεύθυνση είναι μοναδική, η διεύθυνση ανατίθεται στο interface που ρυθμίζεται εκείνη τη στιγμή.
- Χρησιμοποιώντας τη νέα link local διεύθυνση ως διεύθυνση πηγής, στέλνεται ένα μήνυμα αίτησης neighbor discovery για δρομολογητές στο multicast group «όλοι οι δρομολογητές» (FF02::2).
- Προς απάντηση στις αιτήσεις neighbor discovery για δρομολογητές, οι δρομολογητές στέλνουν ένα unicast μήνυμα δημοσιοποίησης neighbor discovery για δρομολογητές προς τον κόμβο. Η δημοσιοποίηση ορίζει, αν ο κόμβος θα πρέπει να χρησιμοποιήσει stateless ή stateful autoconfiguration θέτοντας τη σημαία managed configuration κατάλληλα. Αν χρησιμοποιηθεί stateless autoconfiguration, κατασκευάζεται μια site local ή global διεύθυνση χρησιμοποιώντας ένα πρόθεμα διεύθυνσης, το οποίο συμπεριλαμβάνεται στη δημοσιοποίηση καθώς και την τρέχουσα link local διεύθυνση. Η νέα διεύθυνση ανατίθεται κατόπιν στο interface (το οποίο τώρα

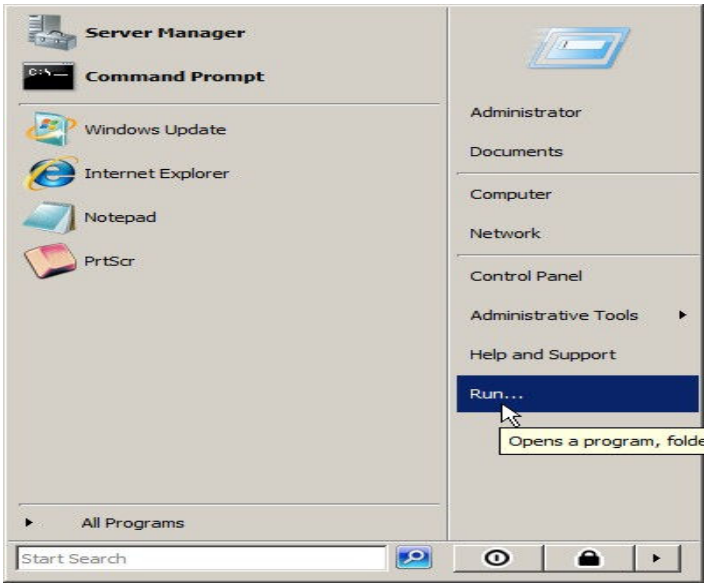
έχει δύο διευθύνσεις). Ο host τώρα ρυθμίζεται για επικοινωνία μέσα στο τμήμα του δικτύου ή ακόμα και σε όλο το διαδίκτυο.

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

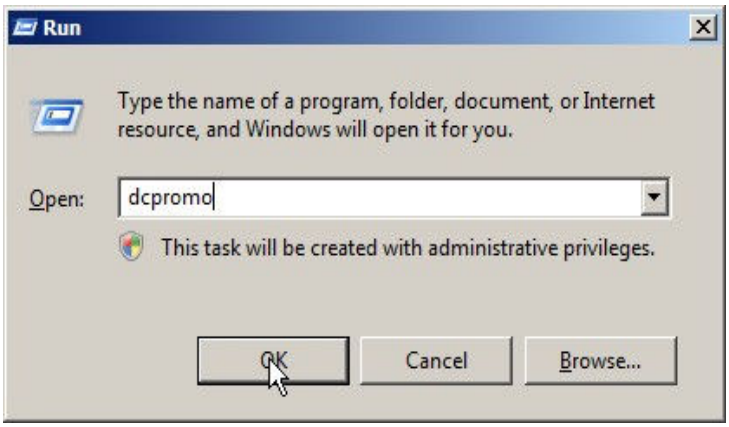
9.7 Υλοποίηση

Σε αυτή την ενότητα θα δούμε βήμα βήμα την διαδικασία δημιουργίας ενός DNS Server

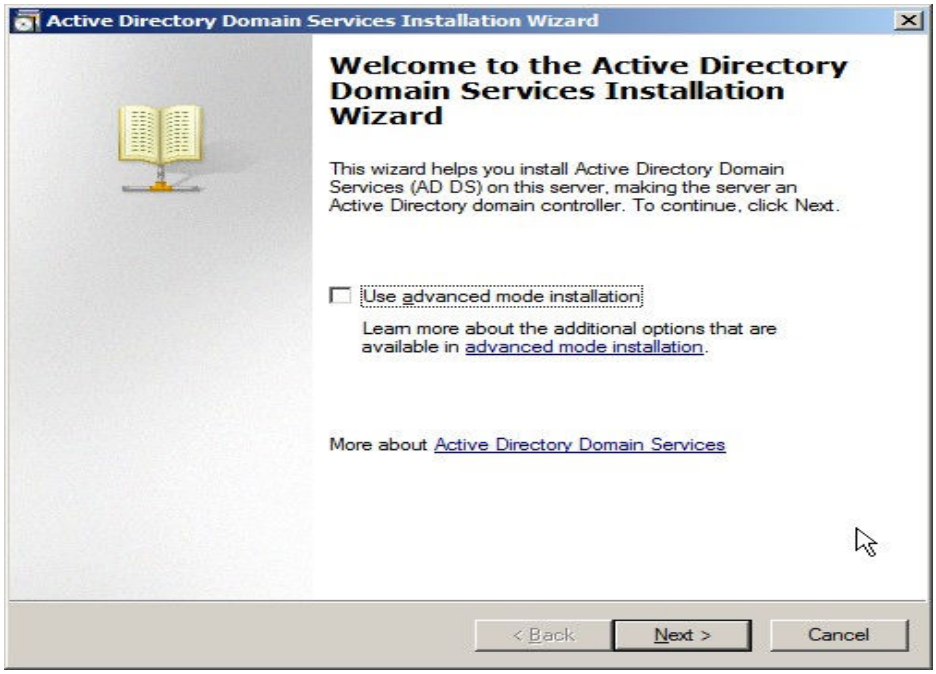
Πατάμε έναρξη και επιλέγουμε Run



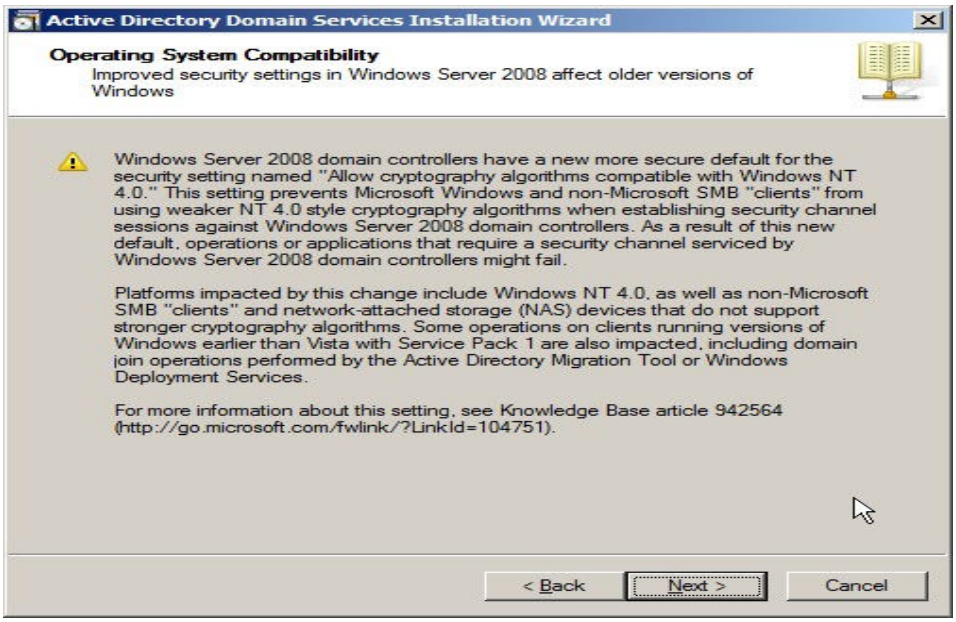
Γράφουμε την εντολή dcpromo και πατάμε OK



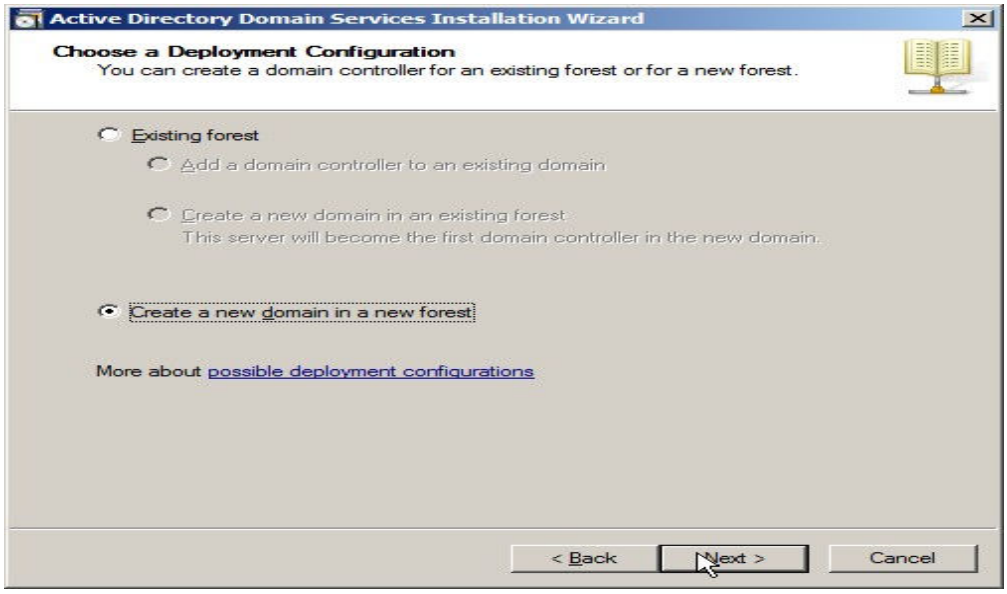
Μετά πατάμε Next



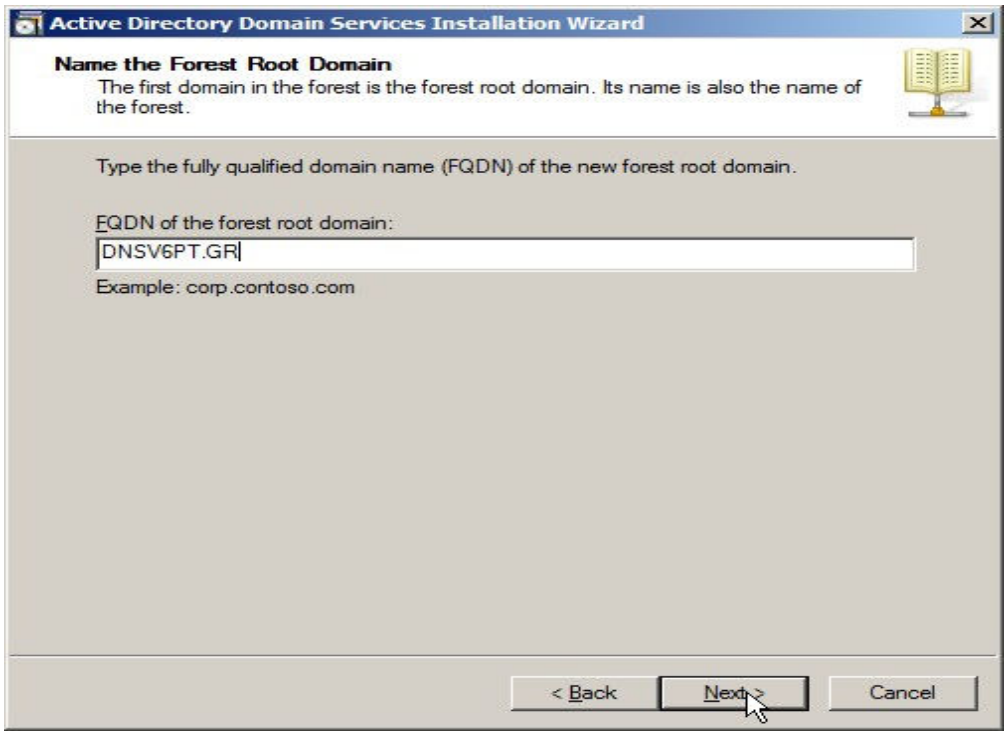
Μετά πατάμε Next



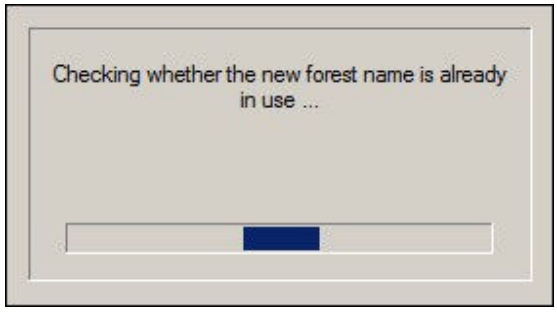
Μετά επιλεγούμε create a new domain in a new forest κα πατάμε Next



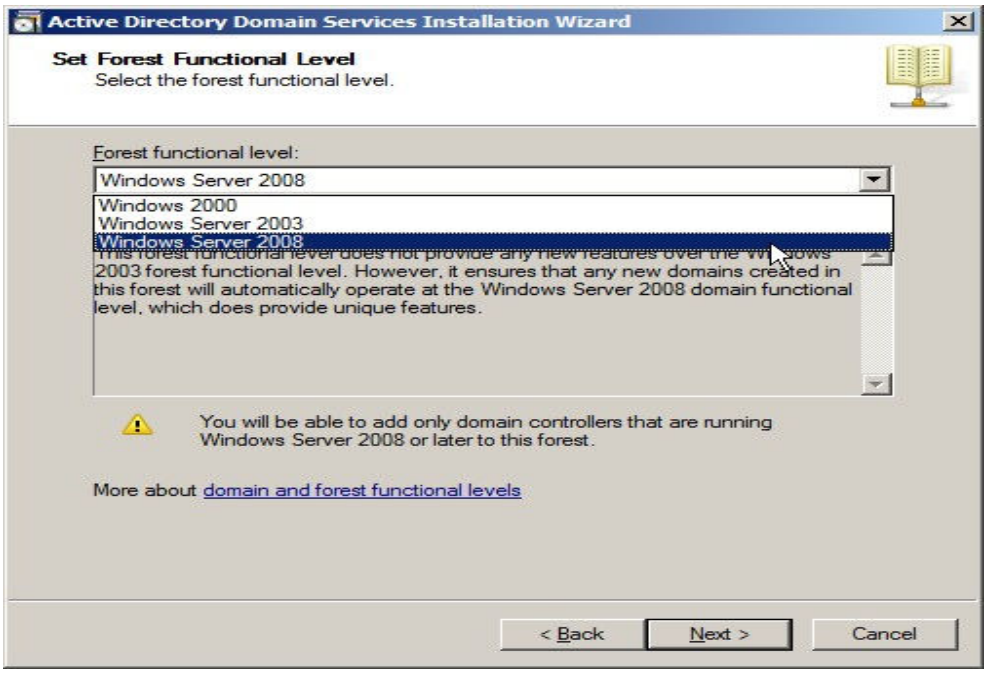
Δίνουμε το όνομα του DNS Server που θέλουμε και πατάμε Next



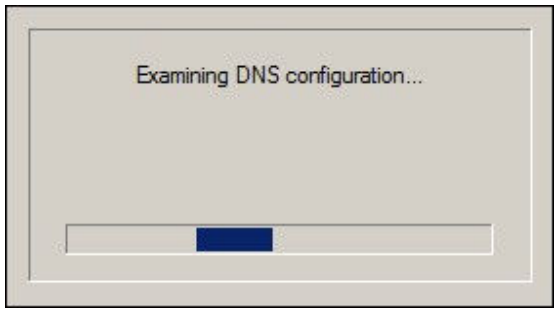
Περιμένουμε να γίνει έλεγχος στο εάν υπάρχει το όνομα που έχουμε δώσει



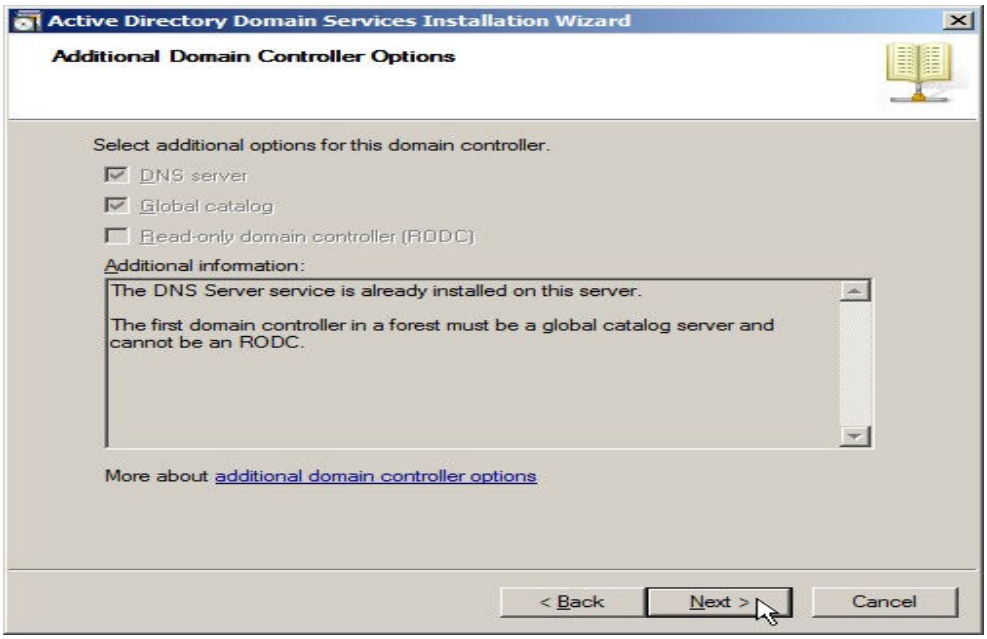
Επιλέγουμε τα Windows(στην προκειμένη windows server 2008) που έχουμε και πατάμε Next



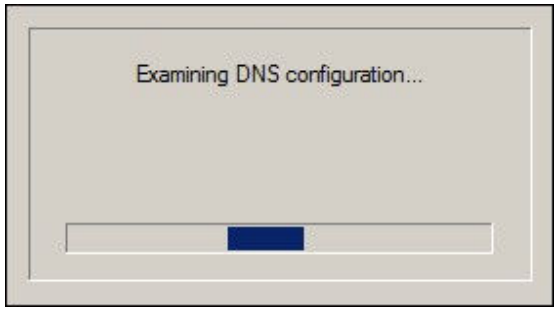
Και περιμένουμε να γίνουν οι ρυθμίσεις.



Μετά πατάμε Next

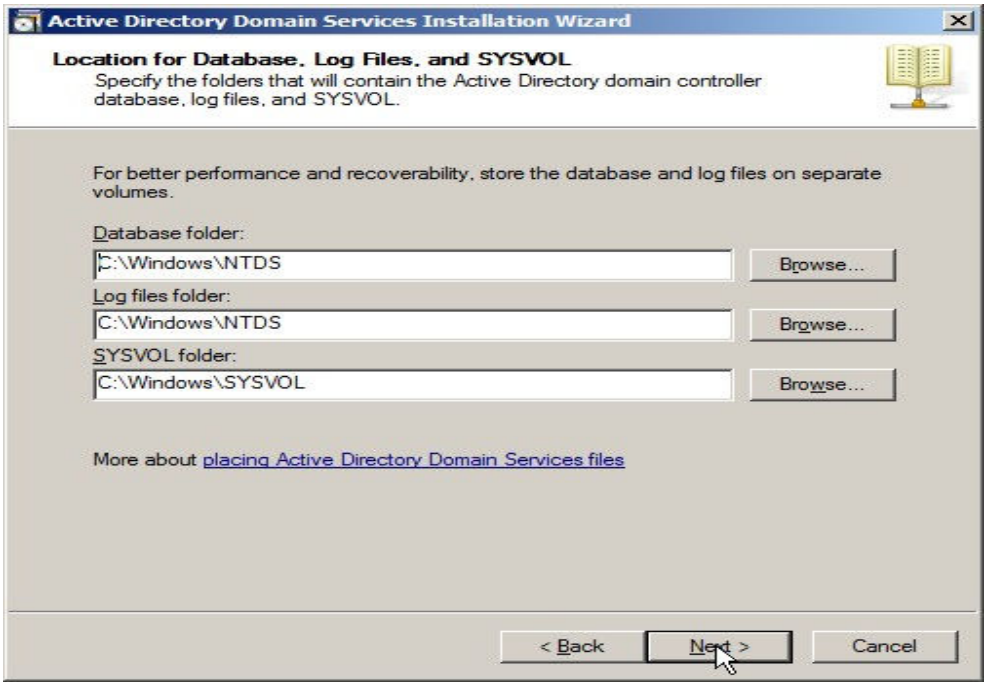


Και περιμένουμε να γίνουν οι ρυθμίσεις.

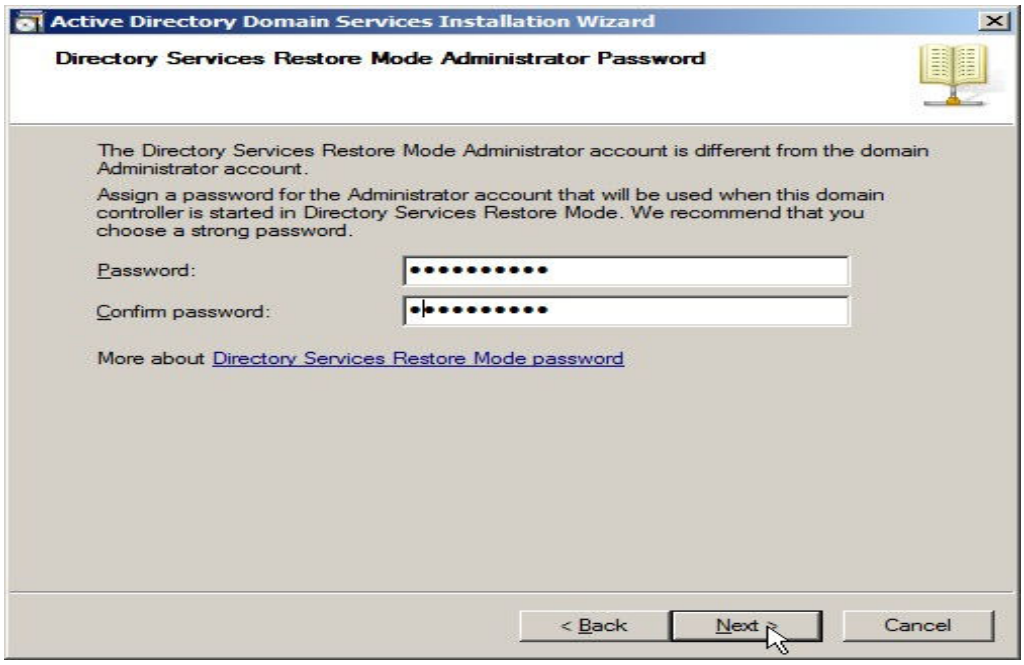


Ξανά πατάμε Next

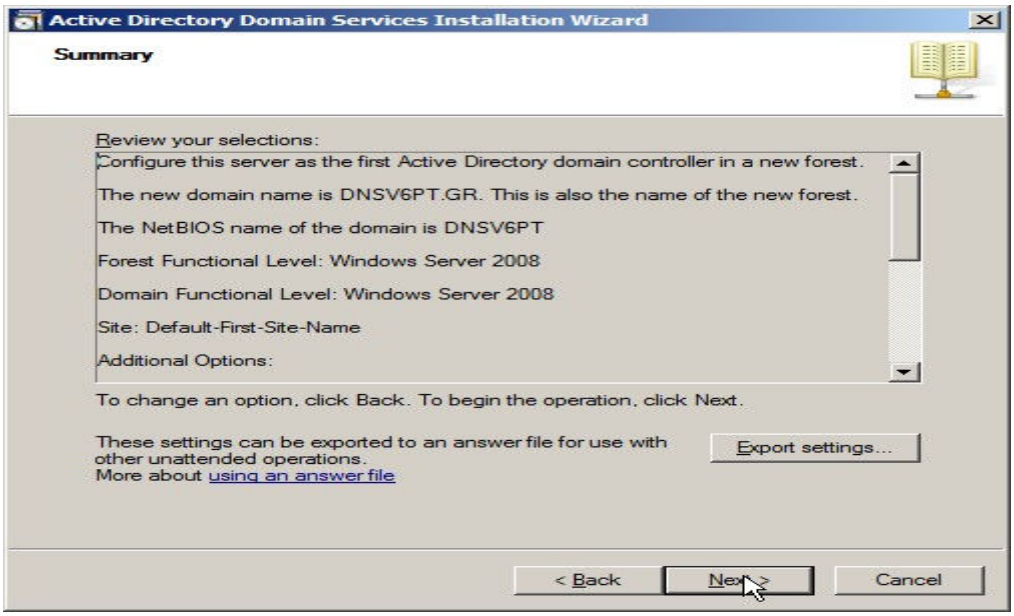
Δίνουμε την τοποθεσία των φακέλων Database Log και SYSVOL και πατάμε Next



Δίνουμε έναν κωδικό πρόσβασης και πατάμε Next

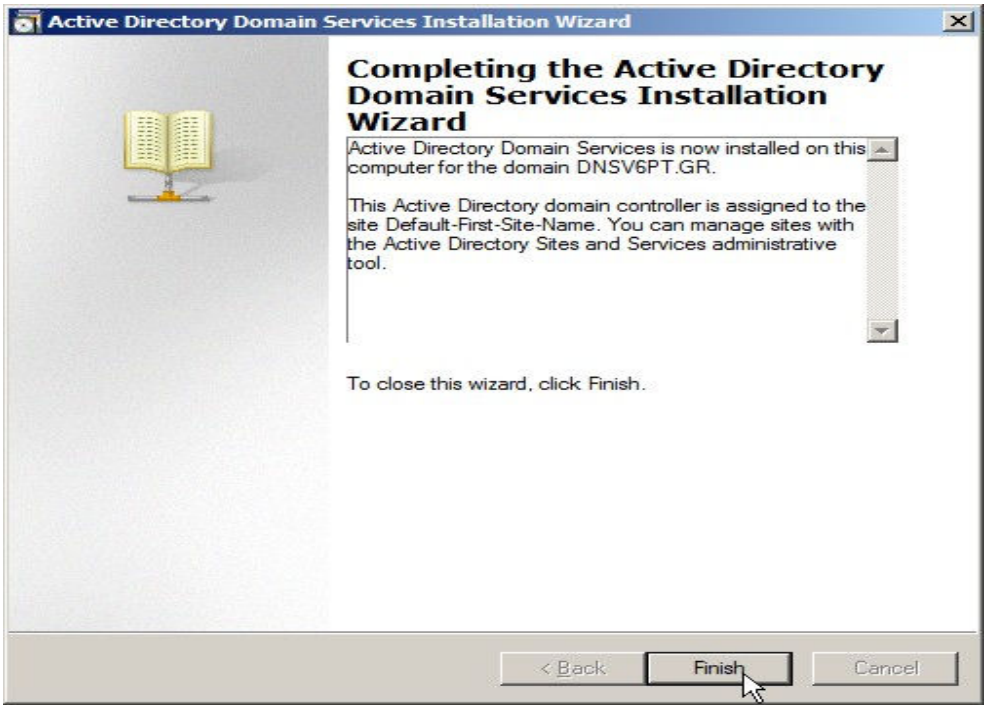


Ξανά επιλέγουμε Next

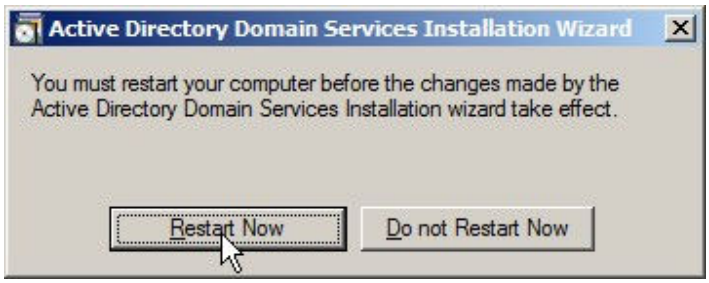


Περιμένουμε να γίνουν οι απαιτούμενοι έλεγχοι

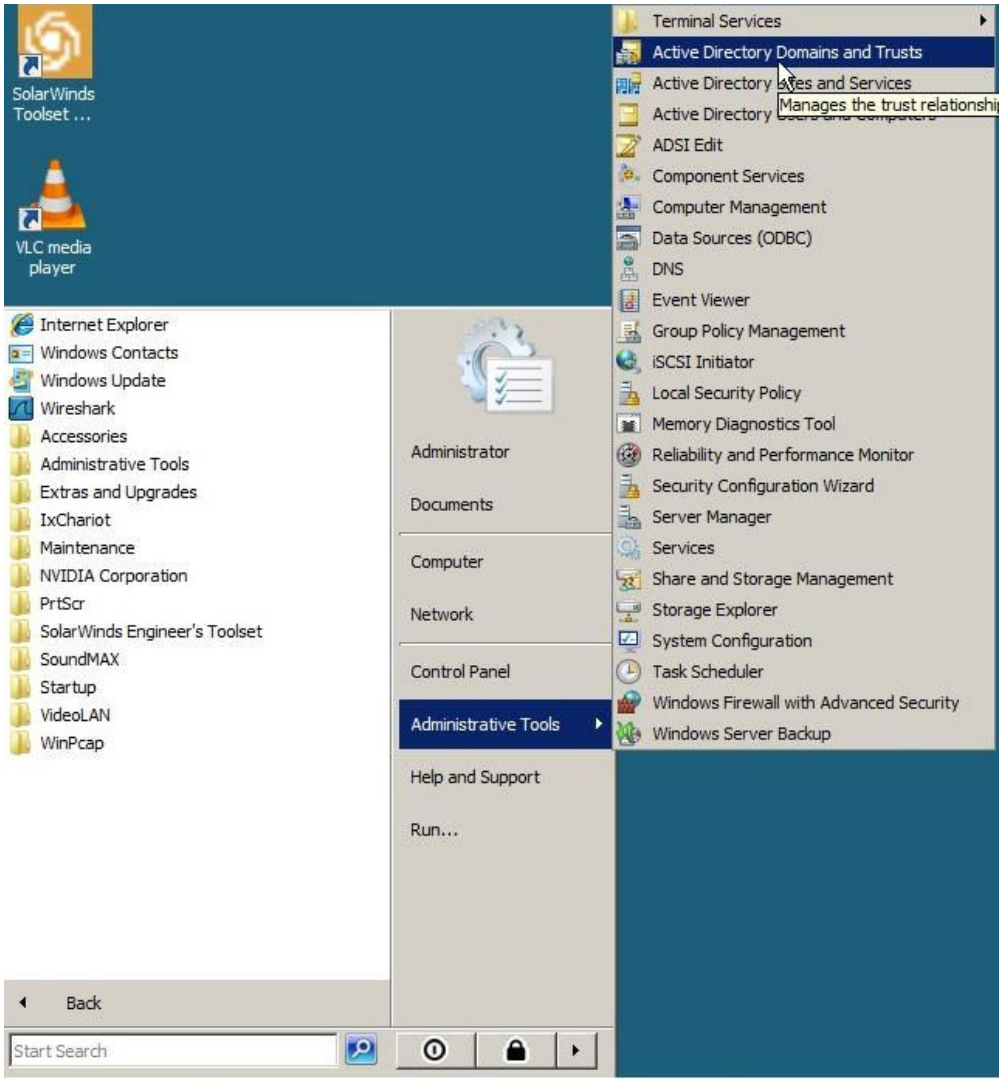
Επιλέγουμε Finish



Και κάνουμε επανεκκίνηση



Και τέλος επιλέγουμε DNS



Κεφάλαιο 10^{ο} - ICMPv6

10.1 Εισαγωγή

Το IPv6 χρησιμοποιεί το Internet Control Message Protocol v6 (πρωτόκολλο μηνυμάτων ελέγχου δικτύου έκδοση 6), το οποίο είναι μια περαιτέρω ανάπτυξη του ICMP που είναι διαθέσιμο στο IPv4. Αναλύει τα λάθει όταν τα πακέτα δεν μεταφέρονται σωστά και στέλνε μηνύματα σχετικά με την κατάσταση του δικτύου. Παράδειγμα, αν ένα πακέτο είναι πολύ μεγάλο για να σταλεί σε ένα δίκτυο, στέλνει ένα ICMP μήνυμα στον αποστολέα του πακέτου. Ο αποστολέας με την σειρά του, μπορεί να επαναπροσδιορίσει το μέγεθος του πακέτου ώστε αυτό να μπορεί να προωθηθεί. Επίσης, το ICMP διενεργεί διαγνωστικά τεστ, όπως αυτό του well known ping, το οποίο εξετάζει την διαθεσιμότητα του εκάστοτε κόμβου.

Το ICMPv6 είναι πολύ πιο ισχυρό από το ICMPv4 και διαθέτει βελτιωμένη λειτουργικότητα. Για παράδειγμα, η λειτουργία του Internet Group Management Protocol που διαχειρίζεται ένα multicast σύνολο μελών με IPv4 ενσωματώνεται στο ICMPv6. Το ίδιο συμβαίνει και με το ARP και το RARP που χρησιμοποιούνταν στο IPv4 για να χαρτογραφήσει τις διευθύνσεις στο δεύτερο στρώμα. Η Neighbor Discovery εισάγεται. Χρησιμοποιεί ICMPv6 μηνύματα για να προσδιορίσει τους γειτονικούς κόμβους που είναι συνδεδεμένοι στην ίδια γραμμή, να βρει routers και να εντοπίζει οποιαδήποτε αλλαγή προκύπτει. Νέοι τύποι μηνυμάτων εισάγονται για να κάνουν πιο εύκολη την ανανέωση των διευθύνσεων και των πληροφοριών μεταξύ των κόμβων και των routers. Η ICMPv6 υποστηρίζει επίσης την Mobile IPv6. Η ICMPv6 είναι κομμάτι της IPv6 και πρέπει να ενσωματώνεται σε κάθε IPv6 κόμβο.

Οι αλλαγές από την έκδοση 4 στην έκδοση 6 περιλαμβάνουν την αφαίρεση των σπάνια χρησιμοποιούμενων μηνυμάτων και την εισαγωγή των μηνυμάτων Internet Group Management Protocol (Πρωτόκολλο διαχείρισης ομάδων διαδικτύου) που χρησιμοποιείται για την είσοδο και την αποχώρηση από ομάδες πολλαπλής διανομής (multicast groups). Το ICMPv6 χρησιμοποιείται επίσης για διαγνωστικούς λόγους (π.χ. Ping) και autoconfiguration (αυτόματη απόκτηση ρυθμίσεων). Στην 4 έκδοση όταν ένας δρομολογητής στον προορισμό δεν μπορεί να

επεξεργαστεί σωστά το πακέτο στέλνει πίσω ένα μήνυμα λάθους ICMP μαζί με την αρχική επικεφαλίδα IP και τα πρώτα 8 bytes της επικεφαλίδας του επομένου επιπέδου. Για το TCP και το UDP αυτό είναι αρκετό ώστε να ξέρει η πηγή του αρχικού υπολογιστή ποια σύνοδος TCP ή UDP παρήγαγε το λάθος πακέτο. Επειδή το IPv6 υποστηρίζει αυθαίρετο αριθμό από επικεφαλίδες επέκτασης ανάμεσα στην επικεφαλίδα IP και την επικεφαλίδα του επομένου (υψηλότερου) επιπέδου, το ICMPv6 επιστρέφει ένα μέρος του αρχικού πακέτου μεγέθους όσο το MTU,1280 bytes. Επιπλέον των μηνυμάτων λάθους που αναγνωρίζονται από ένα ICMP τύπο 127 ή μικρότερο, υπάρχουν και αλλά «πληροφοριακά» μηνύματα με τύπο 128 ή μεγαλύτερο. Επειδή τα «πληροφοριακά» μηνύματα δεν είναι αποτέλεσμα λάθους, δεν περιλαμβάνουν το αρχικό πακέτο ή μέρους αυτού.

10.2 DHCPv6

Το DHCP χρησιμοποιείται ευρέως στο IPv4 για να ρυθμίσει τους κόμβους του δικτύου. Αν έχουμε ένα IPv6 δίκτυο δεν χρειαζόμαστε έναν DHCP server να ρυθμίσει τους κόμβους γιατί θα το κάνουν οι μηχανισμοί αυτοδιαμόρφωσης του IPv6. Το μόνο που πρέπει να κάνουμε είναι να ρυθμίσουμε τους routers μας με τα προθέματα των δικτύων που είναι συνδεδεμένοι. Όμως μας χρειάζεται ακόμη σε μερικές περιπτώσεις.
Ο DHCPv4 με το DHCPv6 είναι δύο ξεχωριστά στοιχεία. Αν θέλουμε να ρυθμίσουμε δύο κόμβους σε ένα dual stack δίκτυο χρειαζόμαστε δύο ξεχωριστές DHCP υπηρεσίες να τρέχουν. Μία για κάθε πρωτόκολλο. Σ' αυτή την περίπτωση υπάρχουν κάποια σημεία σύγκρουσης. Στον κόσμο του DHCPv4 ο κόμβος είναι ρυθμισμένος να ξέρει πότε χρειάζεται το DHCP. Στο DHCPv6 είναι δουλεία του Router Advertisement να ενημερώνει τον κόμβο πότε θα χρειαστεί το DHCP.

Χαρακτηριστικά του DHCPv6:

- Κάθε DHCP κόμβος ζητάει από τον DHCP server να του στείλει οδηγίες καταχώρισης.
- Κάθε DHCP server είναι ρυθμισμένος να απαντάει στα αιτήματα των κόμβων. Επίσης, δεν έχει σημασία αν είναι και οι δύο στην ίδια γραμμή.

- Όταν δεν υπάρχει DHCP server, δημιουργείται ένας διαχειριστής (relay agent) ο οποίος λαμβάνει το αίτημα και το προωθεί σε ένα η περισσότερους DHCP servers οι οποίοι μπορεί να είναι σε άλλο δίκτυο. Όταν λάβει την απάντηση την μεταφέρει στον κόμβο.
- Κάθε DHCP server έχει και έναν DHCP Unique Identifier (DUID). Χρησιμοποιείται για να αναγνωρίσει κόμβους ή ο κόμβος αναγνωρίζει DHCP servers.

10.3 Μηνύματα του ICMPv6

Διακρίνονται σε μηνύματα ενημέρωσης κάποιου σφάλματος ή ενημερωτικά μηνύματα για άλλο λόγο.

Τα πιο κοινά μηνύματα αναφοράς σφάλματος του ICMPv6 είναι:

- *Αδύνατη εύρεση προορισμού (Destination Unreachable):* Το μήνυμα αυτό δημιουργείται όταν μία IP διεύθυνση δεν μπορεί να βρεθεί. Αποστέλλεται στην διεύθυνση του αποστολέα του πακέτου. Οι πιο κοινοί λόγοι δημιουργίας αυτού του προβλήματος είναι: Το πρωτόκολλο μετάδοσης να μην μπορεί να επικοινωνήσει. Παράδειγμα, ένα DNS μήνυμα στέλνεται σε ένα κόμβο και ο DNS server δεν ανταποκρίνεται. Επίσης, υπάρχει το ενδεχόμενο ένας router να μην μπορεί να προωθήσει ένα πακέτο γιατί δεν υπάρχει καμία γραμμή συνδεδεμένη για το δίκτυο προορισμού.

- *Πολύ Μεγάλο Πακέτο (Packet Too Big):* Δημιουργείται αν ένας router δεν μπορεί να προωθήσει το πακέτο γιατί είναι μεγαλύτερο από το MTU. Έτσι, ο αποστολές του πακέτου, με χρήση του μηχανισμού του IPv6 που εξετάσαμε σε προηγούμενο κεφάλαιο (fragmentation) θα σπάσει το πακέτο σε μικρότερα ώστε να είναι δυνατή η αποστολή.

- *Τέλος Χρόνου (Time Exceeded):* Όταν ένας router προωθεί ένα πακέτο, μειώνει τον αριθμό του Hop Limit κατά ένα. Συνεπώς, όταν γίνει μηδέν, ο router θα διαγράψει το πακέτο αυτό από το δίκτυο. Ένα μήνυμα που θα ενημερώνει για την διαγραφή αυτή θα σταλεί στον αποστολέα.

- *Πρόβλημα Παραμέτρων (Parameter Problem*): Αν ένας IPv6 κόμβος δεν μπορεί να ολοκληρώσει την επεξεργασία ενός πακέτου εξ' αιτίας της μη αναγνώρισης του πεδίου της βασικής επικεφαλίδας ή μιας επικεφαλίδας επέκτασης, τότε θα πρέπει να διαγράψει το πακέτο και να ενημερώσει τον αποστολέα.

Μηνύματα ενημέρωσης:

- *Αίτημα επιβεβαίωσης ίχνους (Echo Request):* Είναι το πιο κοινό μήνυμα που χρησιμοποιείται από το TCP/IP. Ονομάζεται Packet Internet Groper, γνωστό ων Ping. Χρησιμοποιείται για να προσδιορίσει αν ένας συγκεκριμένος κόμβος είναι διαθέσιμος στο δίκτυο και έτοιμος να επικοινωνήσει.

- *Απάντηση επιβεβαίωσης ίχνους (Echo Reply):* Η επιβεβαίωση ότι ο κόμβος έχει βρεθεί και είναι έτοιμος για επικοινωνία.

- *Multicast listener query:* Οι δρομολογητές χρησιμοποιούν αυτή την ερώτηση για να ρωτήσουν τους υπολογιστές για το αν είναι μέλη σε multicast groups.

- *Multicast listener report:* Οι υπολογιστές χρησιμοποιούν αυτό το μήνυμα για να αναφέρουν το multicast group στο οποίο είναι μέλη.

- *Multicast listener done:* Οι υπολογιστές χρησιμοποιούν αυτό το μήνυμα για να αναφέρουν ότι «φεύγουν» από ένα multicast group.

- *Router solicitation:* Οι υπολογιστές στέλνουν αυτό το μήνυμα για να ενεργοποιήσουν μια διαφήμιση στο δρομολογητή.

- *Router advertisement:* Οι δρομολογητές στέλνουν αυτό το μήνυμα για να δώσουν άδεια στους υπολογιστές να κάνουν αυτορρύθμιση διεύθυνσης(Stateless Autoconfiguration).

- *Neighbor solicitation:* Οι δρομολογητές και οι υπολογιστές χρησιμοποιούν αυτό το μήνυμα για να ρωτήσουν για τη διεύθυνση MAC του «γείτονά» τους.

- *Neighbor advertisement:* Οι δρομολογητές και οι υπολογιστές στέλνουν αυτό το μήνυμα σε απάντηση του Neighbor solicitation.

- *Redirect message:* Οι δρομολογητές χρησιμοποιούν αυτό το μήνυμα για να ενημερώσουν τους υπολογιστές του δικτύου να χρησιμοποιήσουν διαφορετική διεύθυνση next hop για έναν συγκεκριμένο προορισμό.

Τα μηνύματα ICMP και ICMPv6 περιλαμβάνουν επίσης και ένα κωδικό που υποδεικνύει τον τύπο του μηνύματος που στέλνει το ICMP. Όπως το ICMP έτσι και το ICMPv6 υπολογίζει ένα άθροισμα ελέγχου(checksum) για το μήνυμα ελέγχου που στέλνει αλλά σε αντίθεση με το ICMP,

το ICMPv6 περιλαμβάνει και μια ψευδο-επικεφαλίδα στον υπολογισμό του αθροίσματος ελέγχου. Επίσης, υπάρχει περιορισμός στα ICMPv6 πακέτα που μπορούν να σταλούν κάτι που δεν υπήρχε στην προηγούμενη έκδοση του πρωτοκόλλου. Έτσι αν ένας δρομολογητής λαμβάνει εκατό πακέτα το δευτερόλεπτο που πρέπει να τα στείλει σε μη έγκυρο προορισμό, δεν υποχρεούται να στείλει πίσω πακέτα ICMPv6 με τον ίδιο ρυθμό, δηλαδή εκατό πακέτα/δευτερόλεπτο.

Όπως και στην έκδοση 4, με τη χρήση του πρωτοκόλλου μπορούν να ενημερωθούν για το αν μπορεί να γίνει επικοινωνία με ένα υπολογιστή από ένα συγκεκριμένο μονοπάτι, και αν τυχόν υπάρχουν εναλλακτικά μονοπάτια για να φτάσουν τα πακέτα στον προορισμό τους. Όμως στην καινούρια έκδοση το πρωτόκολλο μπορεί να ενημερώσει τους δρομολογητές αν δύο υπολογιστές βρίσκονται στο ίδιο τοπικό υποδίκτυο.

10.4 Ανακάλυψη Γειτόνων (Neighbor discovery)

Όταν ένα σύστημα θέλει να στείλει ένα πακέτο IPv6 σε ένα άλλο σύστημα που είναι συνδεδεμένο στο ίδιο υποδίκτυο ή καλώδιο, πρέπει να ξέρει τη διεύθυνση MAC (ή αλλιώς τη διεύθυνση σύνδεσης(link address) όπως είναι στην καινούρια ορολογία του IPv6) του υπολογιστή στον οποίο στέλνει το πακέτο. Η διαδικασία ανακάλυψης γειτόνων(Neighbor discovery) επιτρέπει στα συστήματα να ανακαλύψουν τις διευθύνσεις MAC του δικτύου, παρόμοια με το ARP στο IPv4.

Όποτε ένα σύστημα χρειάζεται να μάθει τη MAC διεύθυνση για έννα άλλο σύστημα που είναι στο ίδιο δίκτυο, στέλνει ένα μήνυμα “neighbor solicitation” (το είδαμε παραπάνω), στην IPv6 διεύθυνση με την οποία θέλει να επικοινωνήσει. Στο μήνυμα περιλαμβάνεται και η MAC διεύθυνση του αποστολέα ώστε να ξέρει ο παραλήπτης που να απαντήσει. Ένα σύστημα που λαμβάνει ένα μήνυμα “neighbor solicitation” πρώτα ελέγχει αν η αίτηση είναι πράγματι για μια από τις διευθύνσεις που είναι δικές του. Αν ισχύει κάτι τέτοιο, το σύστημα στέλνει πίσω το μήνυμα “neighbor advertisement” με τη δική του διεύθυνση MAC. Ταυτόχρονα, το σύστημα αποθηκεύει το συνδυασμό IPv6/MAC διευθύνσεων από την αίτηση στο neighbor discovery mapping table ή αλλιώς “neighbor cache”.

10.4.1 Ανίχνευση μη συνδεσιμότητας

Οι δρομολογητές και τα συστήματα IPv6, ψάχνουν ενεργά για το αν οι γείτονές τους είναι διαθέσιμοι στο δίκτυο. Για να το επιτύχουν αυτό, στέλνουν περιοδικά ένα μήνυμα "neighbor discovery" κατευθείαν στο γείτονά τους. Αν ο γείτονας απαντήσει, τότε κρίνεται διαθέσιμος, αλλιώς θεωρείται ότι υπάρχει κάποιο πρόβλημα και ξεκινά η διαδικασία «ανακάλυψης γειτόνων», αγνοώντας την τρέχουσα διεύθυνση MAC. Αυτό επιτρέπει στα συστήματα IPv6 να ανιχνεύσουν μη διαθέσιμους γείτονες ή γείτονες που άλλαξαν τη διεύθυνση MAC που είχαν. Αλλά η πιο σημαντική χρήση αυτής της διαδικασίας είναι για την ανίχνευση δρομολογητών που δεν είναι διαθέσιμοι, έτσι ώστε να χρησιμοποιηθεί κάποιος άλλος δρομολογητής.

10.4.2 Αυτορύθμιση διεύθυνσης

Τα συστήματα και οι δρομολογητές πάντα ρυθμίζουν τις διευθύνσεις link-local σε κάθε διεπαφή στην οποία το IPv6 είναι ενεργοποιημένο. Η διεύθυνση link-local σχεδόν πάντα παράγεται από τη διεύθυνση MAC αλλά για να υπάρχει εγγύηση μοναδικότητας, είναι απαραίτητο να γίνει Duplicate Address Detection(DAD).

Από τη στιγμή που το σύστημα έχει διεύθυνση, μπορεί να προχωρήσει στην απόκτηση και άλλης μίας ή περισσότερων διευθύνσεων IPv6 σύμφωνα πάντα με το RFC 2462. Οι δρομολογητές IPv6 στέλνουν πακέτα διαφήμισης δρομολογητή περιοδικά σε απάντηση της αίτησης "router solicitation".

Τα πακέτα αυτά περιέχουν:

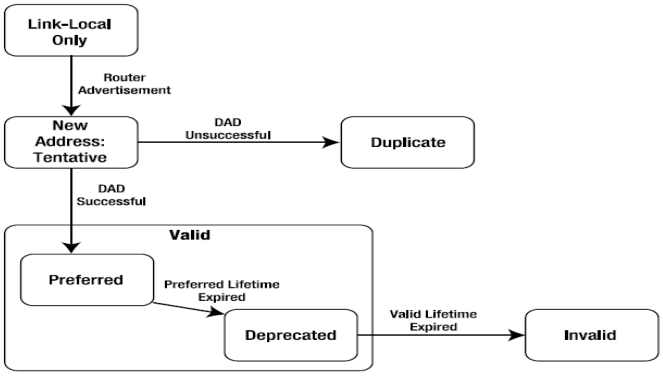
- 1 8-bit "cur hop limit" πεδίο που καθορίζει τι τιμή να χρησιμοποιηθεί στο πεδίο Hop Limit των εξερχόμενων πακέτων.
- Το flag M(managed address configuration). Δεν έχει οριστεί ακόμα η τελική μορφή αυτού του flag αλλά η βασική ιδέα είναι ότι όταν έχει τεθεί οι υπολογιστές χρησιμοποιούν DHCPv6 για να ρύθμιση των διευθύνσεών τους αλλιώς χρησιμοποιούν αυτορύθμιση.
- Το flag (O) (other stateful configuration). Το flag αυτό είναι παρόμοιο με το M flag αλλά υποδεικνύει ότι ο υπολογιστής θα πρέπει να χρησιμοποιήσει έναν μηχανισμό για να ανακαλύψει nonaddress ρυθμίσεις διεύθυνσης.

- Μια 16-bit τιμή που δείχνει τη «διάρκεια ζωής του δρομολογητή». Αυτή η τιμή λέει στα συστήματα για πόσο η διαδρομή που δημιουργήθηκε θα παραμείνει έγκυρη.
- Μια 32-bit τιμή που χρησιμοποιείται για να δείξει πόσο θα περιμένει το σύστημα που στέλνει αίτηση για να δει αν είναι διαθέσιμος ο υπολογιστής στον οποίο τη στέλνει. Όταν πεδία που καθορίζουν κάποια τιμή είναι 0, αυτό σημαίνει ότι η τιμή αυτή δεν ορίζεται, και τα συστήματα πρέπει να καθορίσουν αυτήν την τιμή με άλλο τρόπο. Επιπλέον αυτών, οι «διαφημίσεις των δρομολογητών» μπορεί να περιέχουν μία ή περισσότερες επιλογές όπως:
- "Source link-layer address", η MAC διεύθυνση του δρομολογητή.
- MTU, το μέγιστο μέγεθος πακέτου που πρέπει να χρησιμοποιηθεί στο τρέχον υποδίκτυο.
- Prefix information, που καθορίζει τα προθέματα που χρησιμοποιούνται στο υποδίκτυο και τις ιδιότητές τους. Η επιλογή "Prefix information" με τη σειρά της έχει τη δική της λίστα με ιδιότητες:
- Το πρόθεμα της διεύθυνσης και το μέγεθός του. Για να λειτουργήσει η αυτορύθμιση διεύθυνσης, το πρόθεμα πρέπει να είναι 64-bit.
- Το flag "on-link". Αυτό το flag υποδεικνύει ποια συστήματα με το πρόθεμα είναι ενεργά, έτσι συστήματα με διευθύνσεις που έχουν το πρόθεμα είναι διαθέσιμα στο ζητούμενο υποδίκτυο χωρίς τη βοήθεια του δρομολογητή.
- Το flag "autonomous address configuration". Αυτό το flag λέει στα συστήματα ότι μπορούν να δημιουργήσουν μια διεύθυνση για τον εαυτό τους συνδυάζοντας το πρόθεμα με την «ταυτότητα» της εκάστοτε διεπαφής.
- Μια 32-bit τιμή που συμβολίζει τον «έγκυρο χρόνο ζωής». Αυτή η τιμή υποδεικνύει για πόσο το πρόθεμα θα πρέπει να θεωρείται ενεργό και για πόσο οι αυτορυθμισμένες διευθύνσεις που χρησιμοποιούν το πρόθεμα μπορούν να χρησιμοποιηθούν.
- Μια 32-bit τιμή που συμβολίζει τον «προτεινόμενο χρόνο ζωής» σε δευτερόλεπτα. Αυτό το flag ενημερώνει τους hosts για πόσο οι αυτορυθμισμένες διευθύνσεις που χρησιμοποιούν το πρόθεμα θα προτιμώνται

10.4.3 Ανίχνευση Ίδιων Διευθύνσεων(DAD)

Για να αποφευχθεί η περίπτωση όπου 2 IPv6 συστήματα έχουν την ίδια διεύθυνση, τα συστήματα κάνουν ανίχνευση ίδιων διευθύνσεων για σχεδόν όλες τις καινούριες IPv6

διευθύνσεις πριν αυτές χρησιμοποιηθούν Το DAD γίνεται για καθολικές unicast διευθύνσεις και όχι μόνο για αυτές που δημιουργήθηκαν με αυτορύθμιση αλλά και για τις διευθύνσεις link-local. Για προφανείς λόγους δεν υπάρχει DAD για διευθύνσεις anycast αφού η ουσία των anycast διευθύνσεων είναι ότι πολλά μηχανήματα έχουν την ίδια διεύθυνση. Επιτρέπεται επίσης να μη χρησιμοποιηθεί το DAD για διευθύνεις όπου η «ταυτότητα διεπαφής» έχει ήδη ελεγχθεί.



Σχ. 10.4.3.1 «Ο κύκλος ζωής μιας IPv6 διεύθυνσης»

Όπως φαίνεται στο Σχήμα 10.4.3.1, ένα σύστημα αρχίζει μόνο με μία διεύθυνση link-local. Εκτελείται DAD για αυτή τη διεύθυνση αλλά δεν φαίνεται στην εικόνα. Όταν το σύστημα λαμβάνει μια «διαφήμιση δρομολογητή» που περιέχει ένα ή περισσότερα προθέματα με το flag autonomous address configuration ενεργοποιημένο, το σύστημα δημιουργεί διευθύνσεις με «ταυτότητες διεπαφής» που παράγονται σύμφωνα με το RFC 3041. Η διεύθυνση σημειώνεται ως «δοκιμαστική» και προχωρά στην εκτέλεση DAD.

Τότε μία από τις παρακάτων περιπτώσεις θα συμβεί:

- Ο υπολογιστής λαμβάνει μια διαφήμιση ενός γείτονα ότι χρησιμοποιείται ήδη η διεύθυνση.
- Ο υπολογιστής λαμβάνει ένα μήνυμα “neighbor solicitation”, από κάποιον άλλο υπολογιστή που εκτελεί DAD.
- Δεν έρχεται καθόλου απάντηση.

Η πρώτη από τις περιπτώσεις δείχνει διένεξη διευθύνσεων και οι διευθύνσεις μαρκάρονται ως «διπλές». Όταν συμβεί αυτό, η συγκεκριμένη διεύθυνση παραμένει αχρησιμοποίητη. Μόνο όταν δεν έρθει καμία απάντηση χρησιμοποιείται η διεύθυνση. Αν υπάρχει διένεξη το σύστημα υποτίθεται ότι θα καταγράψει το λάθος στο «ημερολόγιο» και θα περιμένει ανθρώπινη παρέμβαση.

10.4.4 Χρόνος ζωής διεύθυνσης

Αφού περάσουν και το «εμπόδιο του DAD» οι διευθύνσεις αυτορυθμίζονται και η ρύθμιση αυτή μπρεί να παραμείνει μέχρι το μήνυμα για τον «προτεινόμενο χρόνο ζωής» από το δρομολογητή λήξει. Στις περισσότερες περιπτώσεις, αυτό δε θα συμβεί επειδή καινούρια πακέτα από το δρομολογητή θα ανανεώσουν τους μετρητές. Αλλά αν δεν υπάρχουν τέτοια νέα πακέτα, τελικά ο «προτεινόμενος χρόνος ζωής» θα λήξει και η διεύθυνση θα μαρκαριστεί ως «παρωχημένη». Οι καινούριες σύνοδοι(sessions) που ανοίγονται δεν πρέπει να χρησιμοποιούν «παρωχημένες διευθύνσεις» αλλά να προτιμούν τις καινούριες διεύθυνσεις αν είναι διαθέσιμες. Παρ' όλα αυτά οι υπάρχουσες σύνοδοι συνεχίζουν να χρησιμοποιούν τις παρωχημένες διευθύνσεις. Τελικά ο «έγκυρος χρόνος ζωής» θα λήξει και οι παρωχημένες διευθύνσεις θα αφαιρεθούν από τη διεπαφή. Αυτό θα τερματίζει βίαια τυχόν συνόδους που ακόμα χρησιμοποιούν τη διεπαφή.

10.4.4.1 Εύρεση MTU μονοπατιού και τεμαχισμός.

Επειδή οι δρομολογητές δεν μπορούν να τεμαχίσουν τα πακέτα IPv6, χρησιμοποιούνται πάντα MTU μεγαλύτερα από 1280 bytes. Αυτό σημαίνει ότι πρέπει οι δρομολογητές να παράγουν ένα πακέτο ICMPv6 για τα πολύ μεγάλα πακέτα, ώστε να ξανασταλούν σε μικρότερα πακέτα.

Με το που λάβει το μήνυμα «πολύ μεγάλο πακέτο» το TCP θα μειώσει το μέγεθος του πακέτου ώστε να έχει μικρότερο MTU στο ζητούμενο μονοπάτι. Εντούτοις, τα πρωτόκολλα που τρέχουν σε UDP δεν μπορούν αυθαίρετα να μειώσουν το μέγεθος του πακέτου τους. Στο IPv4 τα πακέτα στέλνονται γενικώς χωρίς να έχει τεθεί το fragment bit, ώστε οι δρομολογητές να το τεμαχίσουν αν αυτό είναι απαραίτητο. Στο IPv6, αυτό δεν είναι δυνατό, αν το πακέτο είναι πολύ μεγάλο, ο αποστολέας πρέπει να το τεμαχίσει. Ο αποστολέας το κάνει αυτό χωρίζοντας πρώτα τα «τεμαχιζόμενα» και «μη-τεμαχιζόμενα» μέρη του πακέτου. Η επικεφαλίδα IPv6 και οποιεσδήποτε επικεφαλίδες που υπόκεινται σε επεξεργασία από τους δρομολογητές συνιστούν το

«μη-τεμαχιζόμενο μέρος». Τα δεδομένα Payload και τυχόν επικεφαλίδες που επεξεργάζονται μόνο στον παραλήπτη αποτελούν το «τεμαχιζόμενο» μέρος.

Μόλις λάβει το πρώτο τεμάχιο(που δεν είναι απαραίτητα το πρώτο τεμάχιο που έστειλε το αρχικό πακέτο), ο υπολογιστής περιμένει μέχρι 60 δευτερόλεπτα για να φτάσουν όλα τα άλλα τεμάχια, και αν φτάσουν, επανασυναρμολογεί το αρχικό πακέτο συνδυάζοντας όλα τα τεμάχια που έχουν τον ίδιο αποστολέα και παραλήπτη και πεδίο identification. Αν ένα ή περισσότερα από τα τεμάχια χαθούν τότε το πακέτο δεν μπορεί να επανασυναρμολογηθεί, κι έτσι ολόκληρο το πακέτο χάνεται.

Κεφάλαιο 11^{ο} - Αυτόματη διευθυνσιοδότηση - DHCPv6

11.1 Εισαγωγή

Το DHCPv6 είναι το αντίστοιχο του DHCP στο IPv6. Επειδή το IPv6 υποστηρίζει αυτορύθμιση διεύθυνσης, το DHCP χρειάζεται για διαφορετικούς λόγους από το IPv4. Παρόλο που οι λεπτομέρειες είναι διαφορετικές τα DHCPv4,DHCPv6 είναι αρκετά παρόμοια. Οι πιο σημαντικές διαφορές είναι στον τρόπο με τον οποίο χρησιμοποιείται το πρωτόκολλο. Έχει 3 κύριους σκοπούς:

- Ρύθμιση διεύθυνσης: Να δίνει διευθύνσεις σε κάθε σύστημα.
- Μη-ρύθμιση διεύθυνσης: Δίνει πληροφορίες όπως διευθύνσεις DNS εξυπηρετητών.
- Διαφήμιση προθεμάτων: Διαφημίζει ολόκληρα προθέματα στους δρομολογητές.

11.2 Λειτουργία του DHCPv6

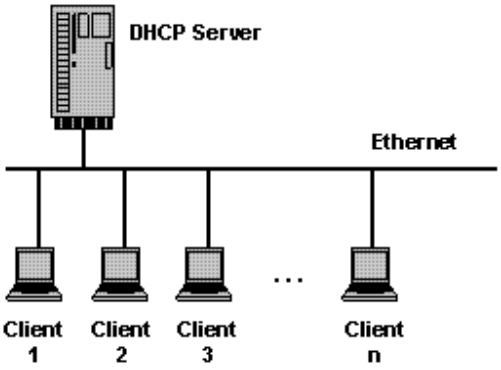
Ένας πελάτης DHCPv6 που ενδιαφέρεται να μάθει μια διεύθυνση ή άλλες πληροφορίες για ρυθμίσεις του δικτύου στέλνει ένα μήνυμα που υποδεικνύει ότι χρειάζεται τις link-local multicast διευθύνσεις στη θύρα 547. Ο πελάτης εκτιμά τους διαθέσιμους εξυπηρετητές που υπάρχουν στη διάθεσή του και στέλνει μια αίτηση στον εξυπηρετητή της προτίμησής του. Εναλλακτικά αν ο πελάτης θέλει μόνο να λάβει πληροφορίες ρυθμίσεων και καθόλου διευθύνσεις ή προθέματα, μπορεί να στείλει ένα μήνυμα που να απαιτεί πληροφορίες και ο εξυπηρετητής αμέσως στέλνει

ένα μήνυμα απάντησης, έτσι μόνο τα μισά μηνύματα ανταλλάσσονται και έτσι η διαδικασία τελειώνει πολύ πιο γρήγορα. Ο πελάτης μπορεί να ζητήση και «γρήγορη δέσμευση» με την οποία υποδεικνύει ότι θέλει να πάρει διεύθυνση από τον πρώτο εξυπηρετητή DHCPv6 που θα απαντήσει στο αίτημα. Όπως ήταν αναμενόμενο οι IPv6 διευθύνσεις που ανατίθενται με DHCPv6 έρχονται με προτεινόμενο και έγκυρο χρόνο ζωής. Καμιά φορά πριν τελειώσει ο timer ο πελάτης στέλνει ένα μήνυμα ανανέωσης ρωτώντας αν μπορεί να συνεχίσει να χρησιμοποιεί τη διεύθυνση. Όταν δεν θέλει πια να χρησιμοποιεί τη διεύθυνση, ο πελάτης στέλνει ένα μήνυμα απελευθέρωσης της διεύθυνσης. Υπάρχουν βέβαια και άλλες όχι τόσο κοινές περιπτώσεις.

Για να μπορούν οι εξυπηρετητές να αναγνωρίζουν τους πελάτες κάθε συσκευή που υλοποιεί το DHCPv6 έχει ένα DHCP Unique Identifier(DUID). Στο IPv4, οι πελάτες DHCP χρησιμοποιούν τη MAC διεύθυνση ή ένα αλφαριθμητικό οριζόμενο από το χρήστη γνωστό ως Client Identifier. Στο DHCPv6 αυτό είναι πάντα το DUID. Οι συσκευές μπορούν να δημιουργήσουν το δικό τους DUID βασισμένοι στη μικρότερη MAC στο σύστημα. Επειδή ακόμα και οι «αρθρωτοί» δρομολογητές της Cisco, έχουν σταθερές διευθύνσεις MAC αυτό λειτουργεί καλά. Για υπολογιστές με «αποσπώμενες» διεπαφές Ethernet το DUID βασίζεται στη διεύθυνση MAC και στην ημερομηνία δημιουργίας. Έτσι και αλλιώς, μια κάρτα Ethernet μπορεί να είναι σε έναν υπολογιστή μόνο τη φορά. Το παραγόμενο DUID αποθηκεύεται για περαιτέρω χρήση, ακόμα και αφού η κάρτα Ethernet, βγαίνει από το σύστημα.

Το DHCPv6 υποστηρίζει ένα μηχανισμό πιστοποίησης(authentication) που επιτρέπει στους πελάτες και εξυπηρετητές να αλληλεπιδράσουν με 1 ασφαλή τρόπο, ώστε τρίτοι να μην μπορούν να εισάγουν ψεύτικα μηνύματα DHCP ή να τροποποιήσουν κάποια πραγματικά. Παρ'όλα αυτά αυτός ο μηχανισμός πρέπει να προ-ρυθμιστεί με ανθρώπινη παρέμβαση σε όλους τους πελάτες και εξυπηρετητές «καταστρέφοντας» εν μέρει τα πλεονεκτήματα του DHCP σε σχέση με την ρύθμιση με το χέρι.

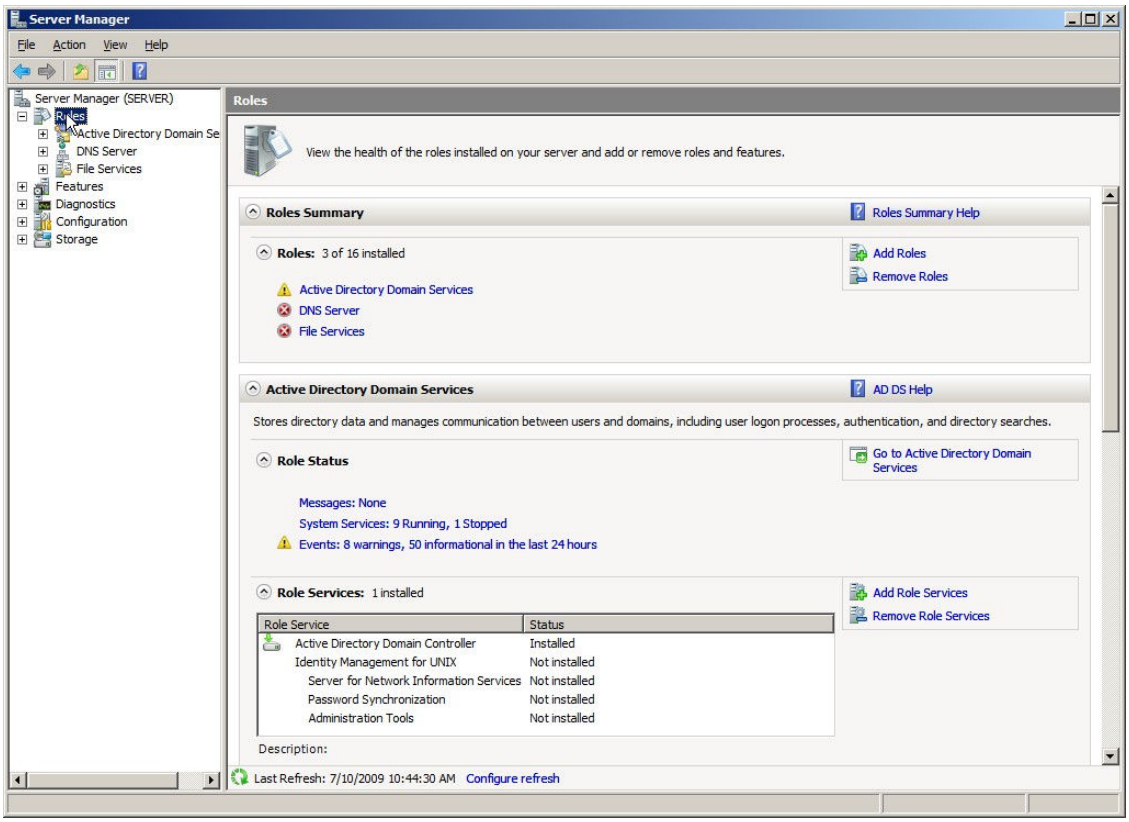
11.3 Υλοποίηση



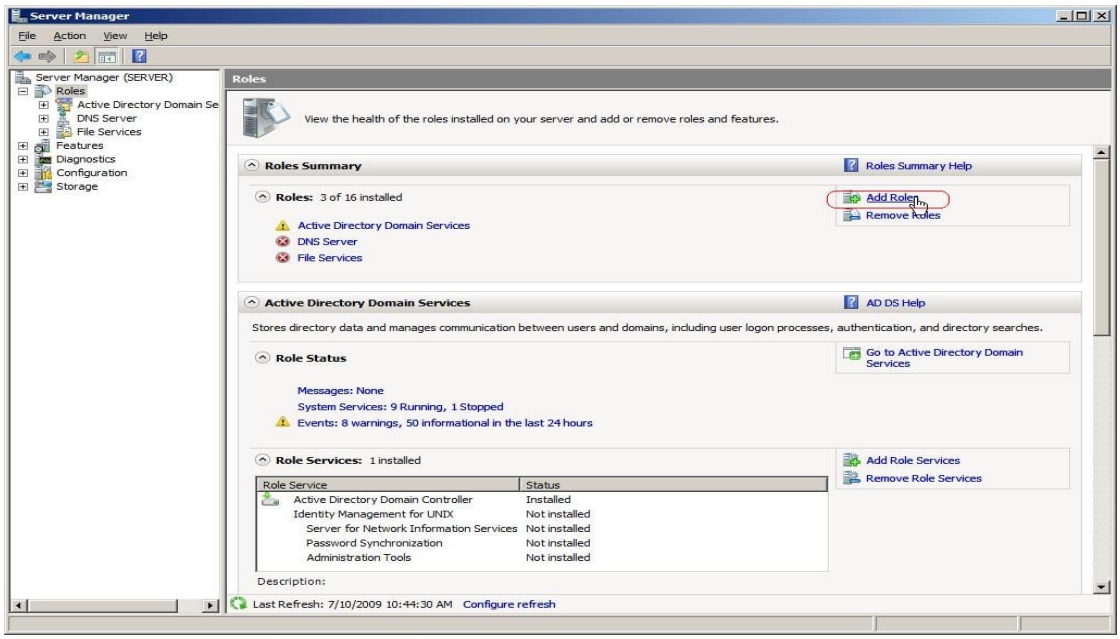
Σε αυτή την ενότητα θα δούμε βήμα βήμα την διαδικασία δημιουργίας ενός DHCP Server

Αρχικά ανοίγουμε το server manager από την έναρξη → Administrative tools → Server Manager

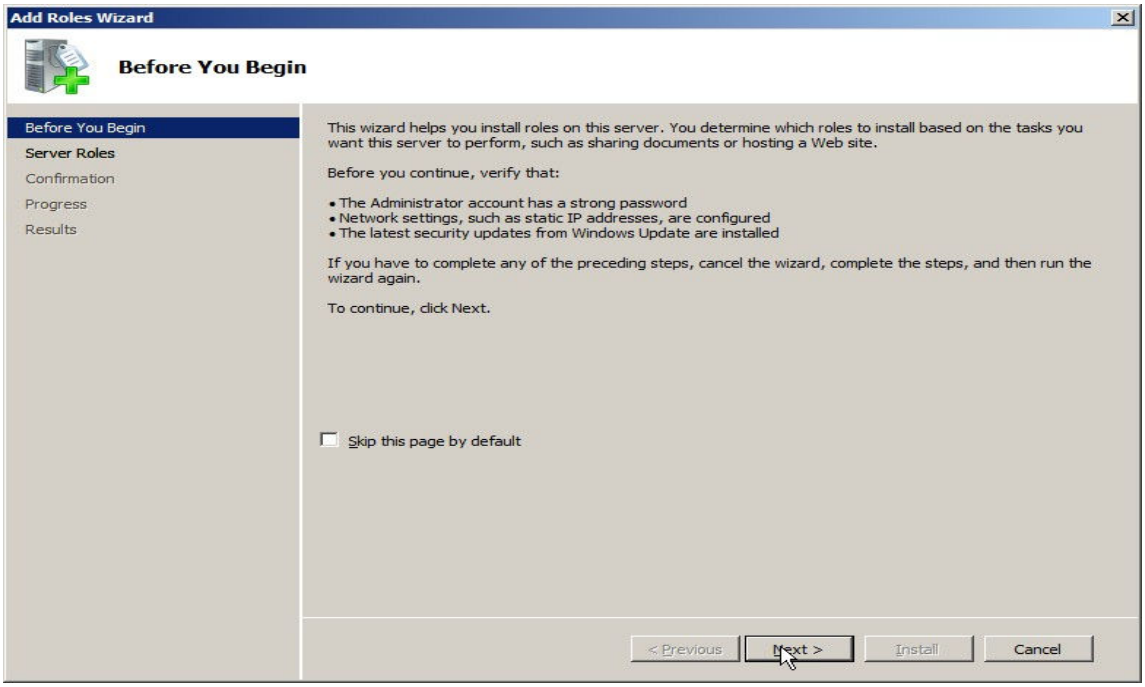
Όταν ανοίξουμε τον Server Manager πατάμε Role →Add Roles



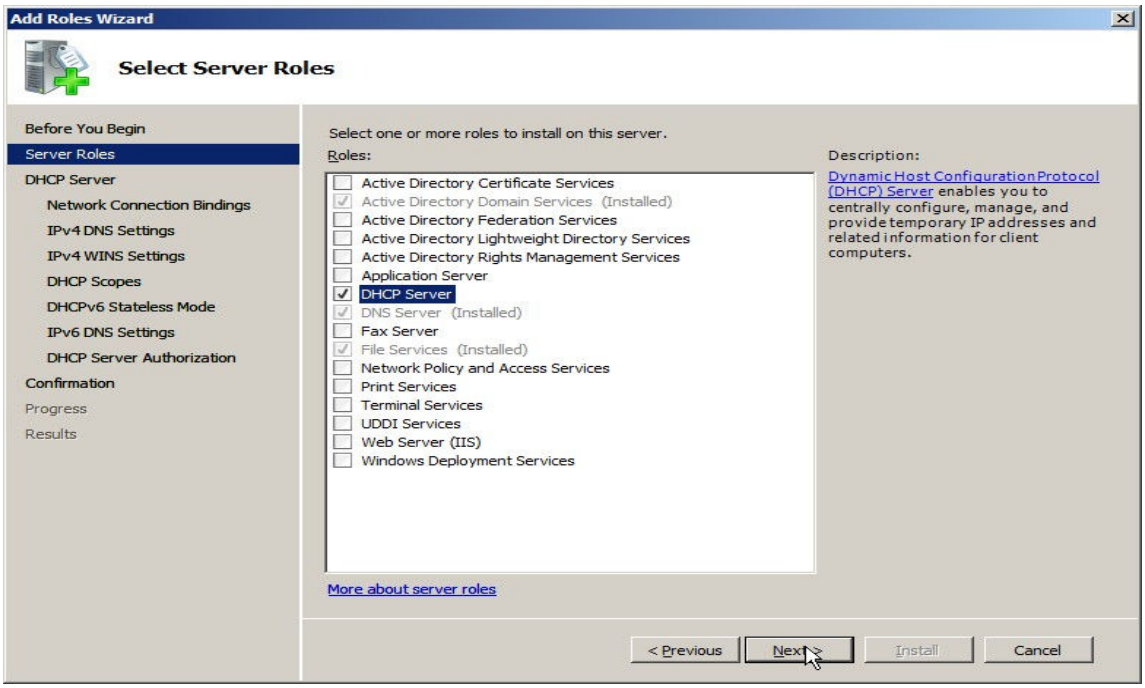
Όταν ανοίξει ο Server Manager πατάμε Role →Add Roles



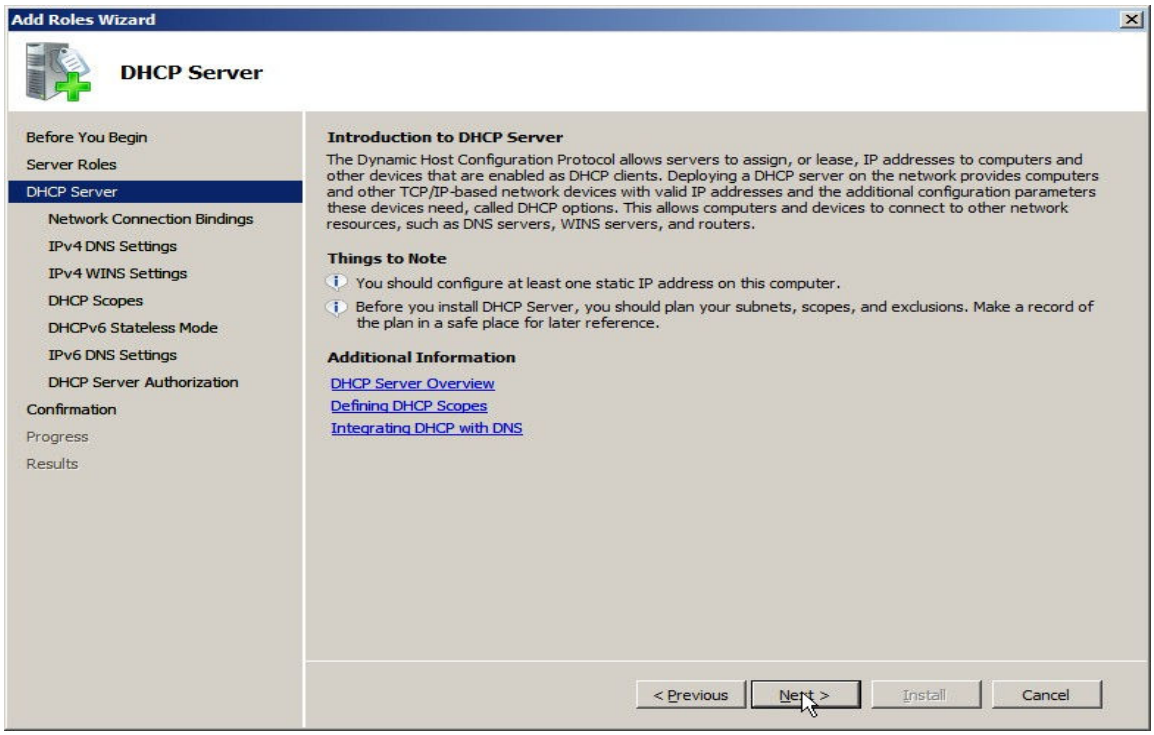
Τώρα πατάμε Next



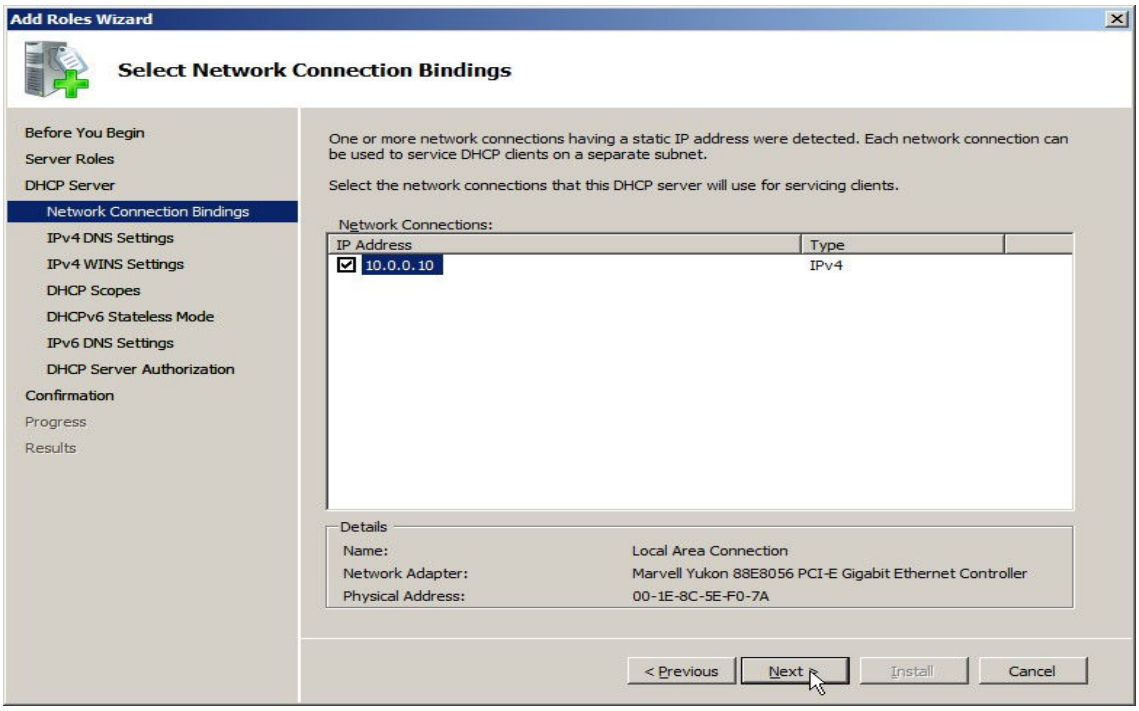
Επιλέγουμε DHCP Server και πατάμε Next



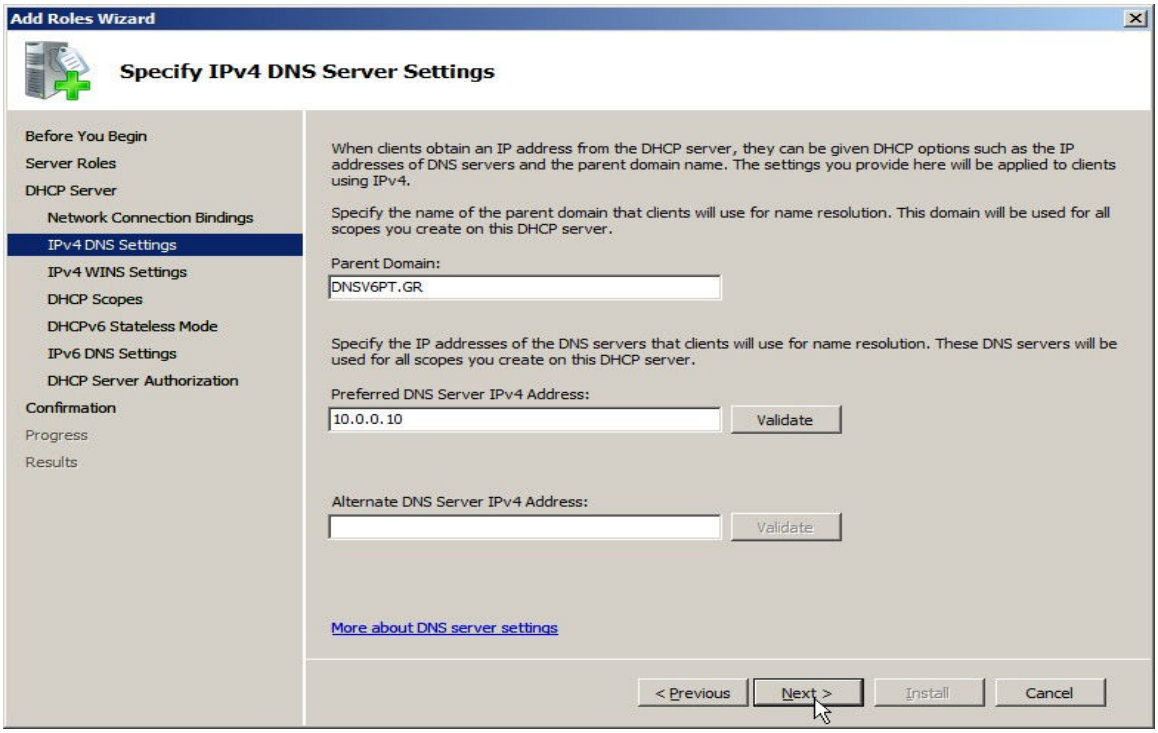
Ξανά πατάμε Next



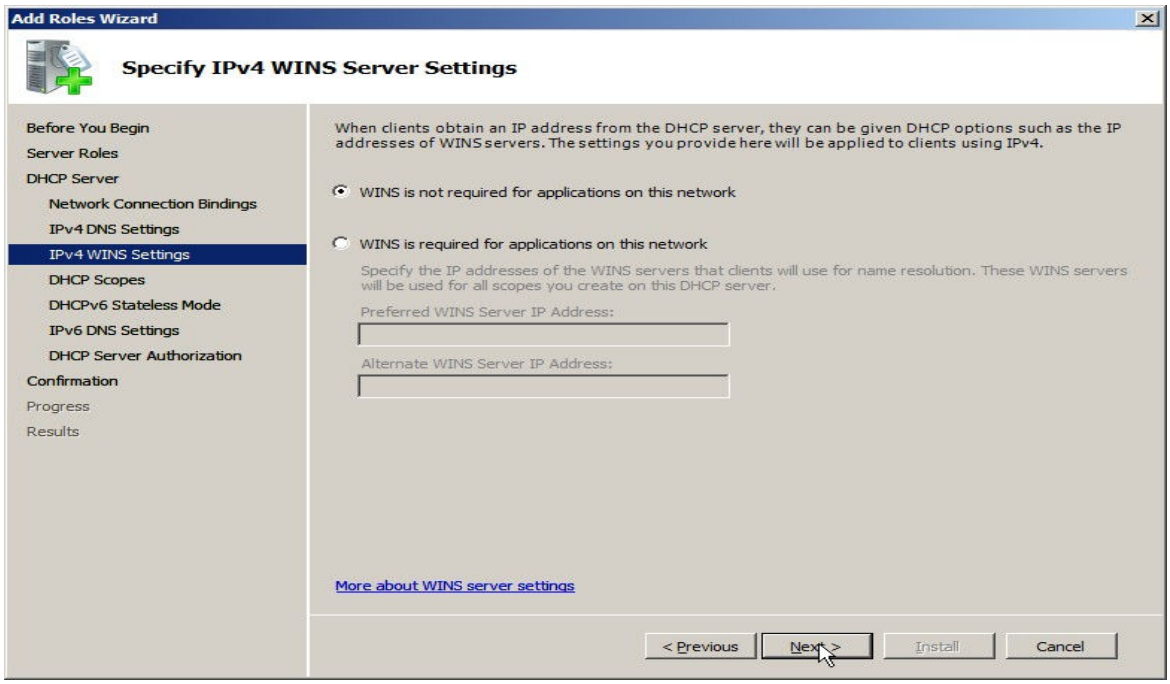
Ξανά πατάμε Next



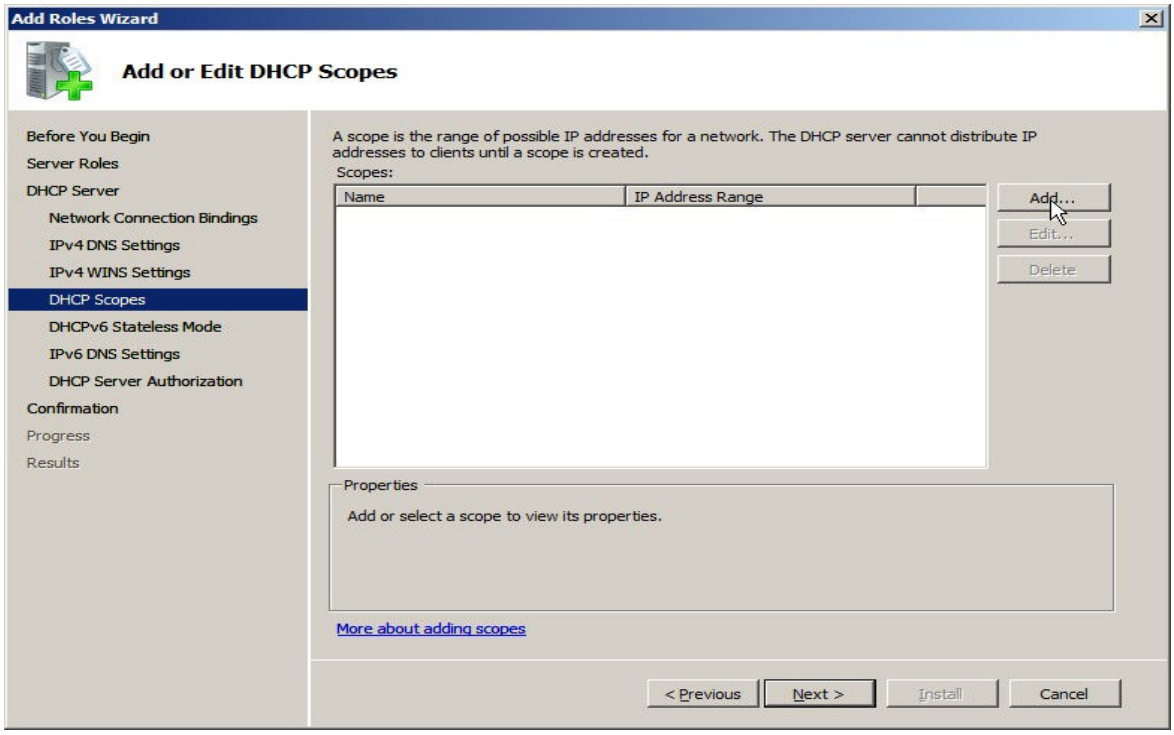
Εδώ βάζουμε το όνομα του DNS που δημιουργήσαμε στο κεφάλαιο 10 και πατάμε Next



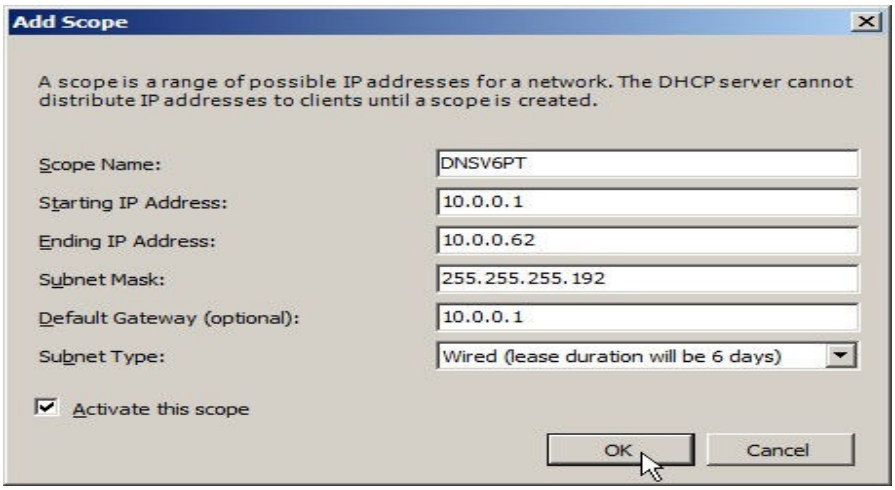
Εάν έχουμε WINS Server βάζουμε τα στοιχεία αλλιώς πατάμε Next



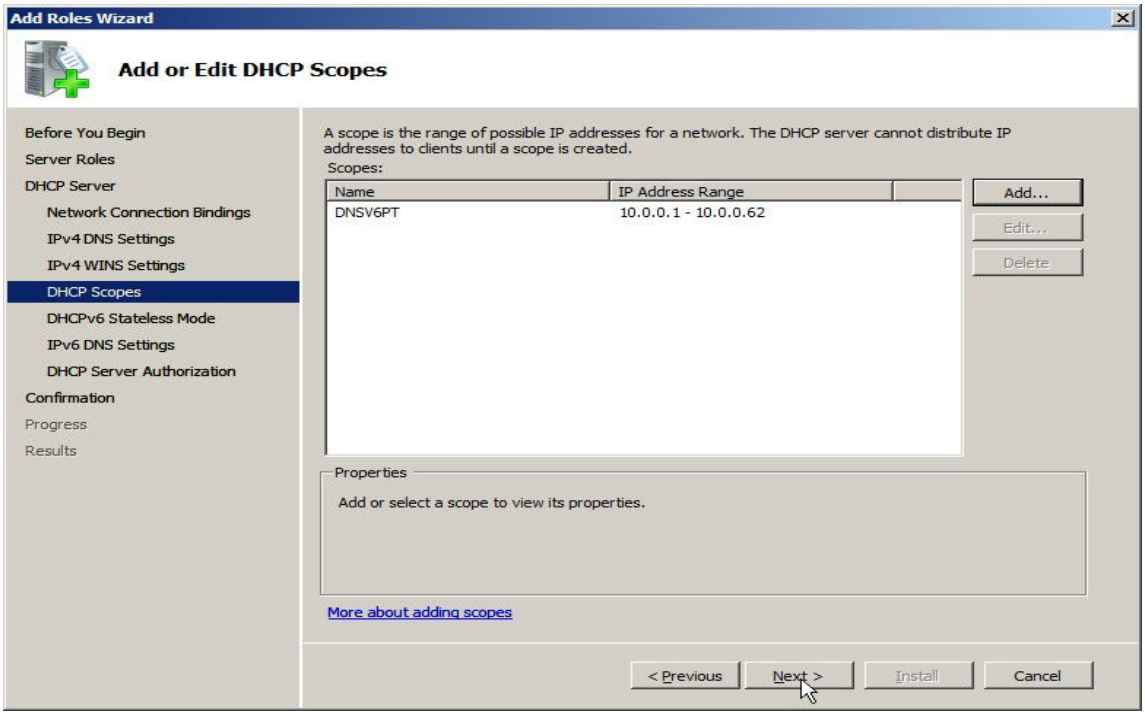
Τώρα πατάμε Add για να δώσουμε τα στοιχεία του DHCP Server



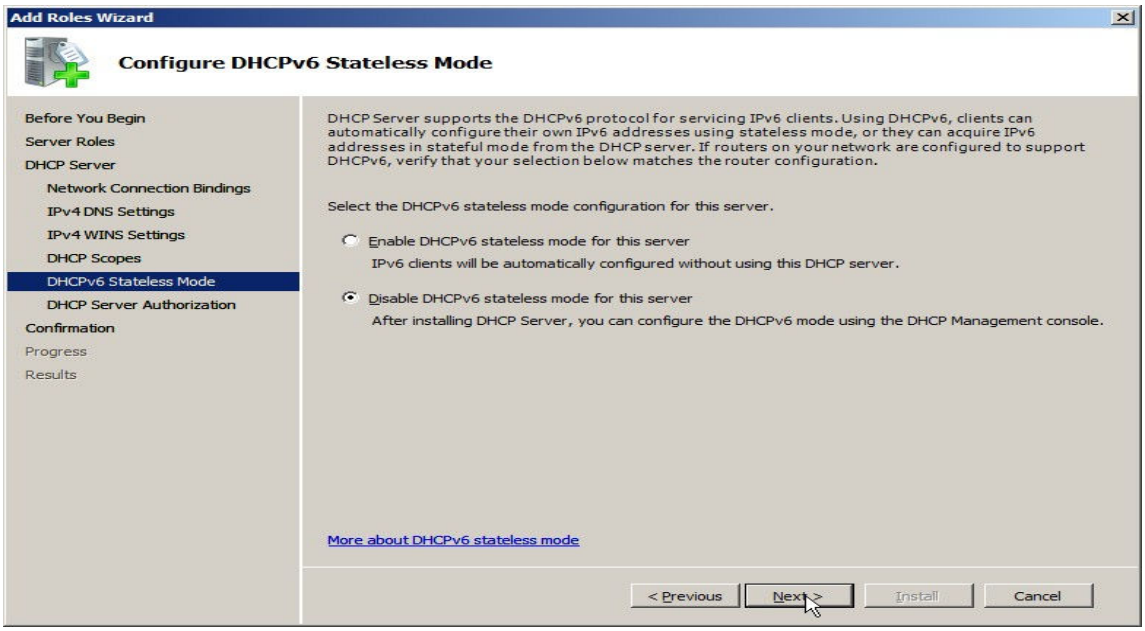
Βάζουμε τα στοιχεία ενεργοποιούμε το Activate this scope και πατάμε OK



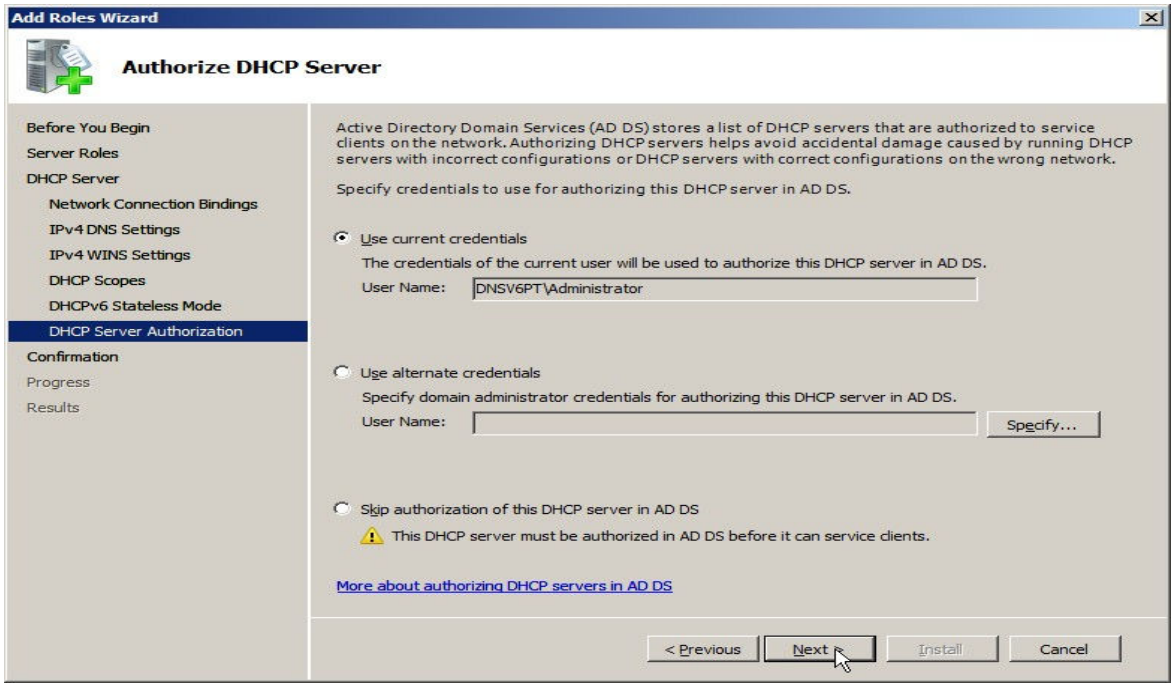
Πατάμε Next



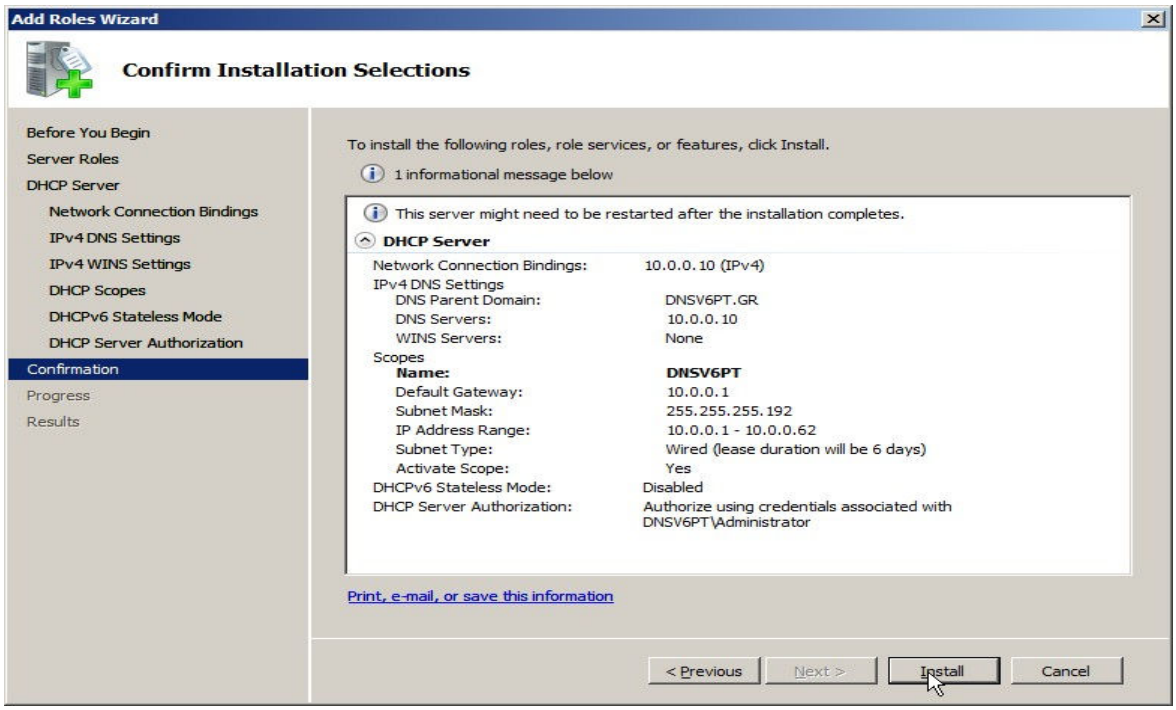
Άμα θέλουμε να ενεργοποιήσουμε την IPv6 επιλέγουμε enable DHCP Server (Εμείς επιλέγουμε το disable DHCP γιατί δεν θέλουμε να γίνετε αυτόματα αλλά να το ρυθμίσουμε εμείς).
Και μετά πατάμε Next.



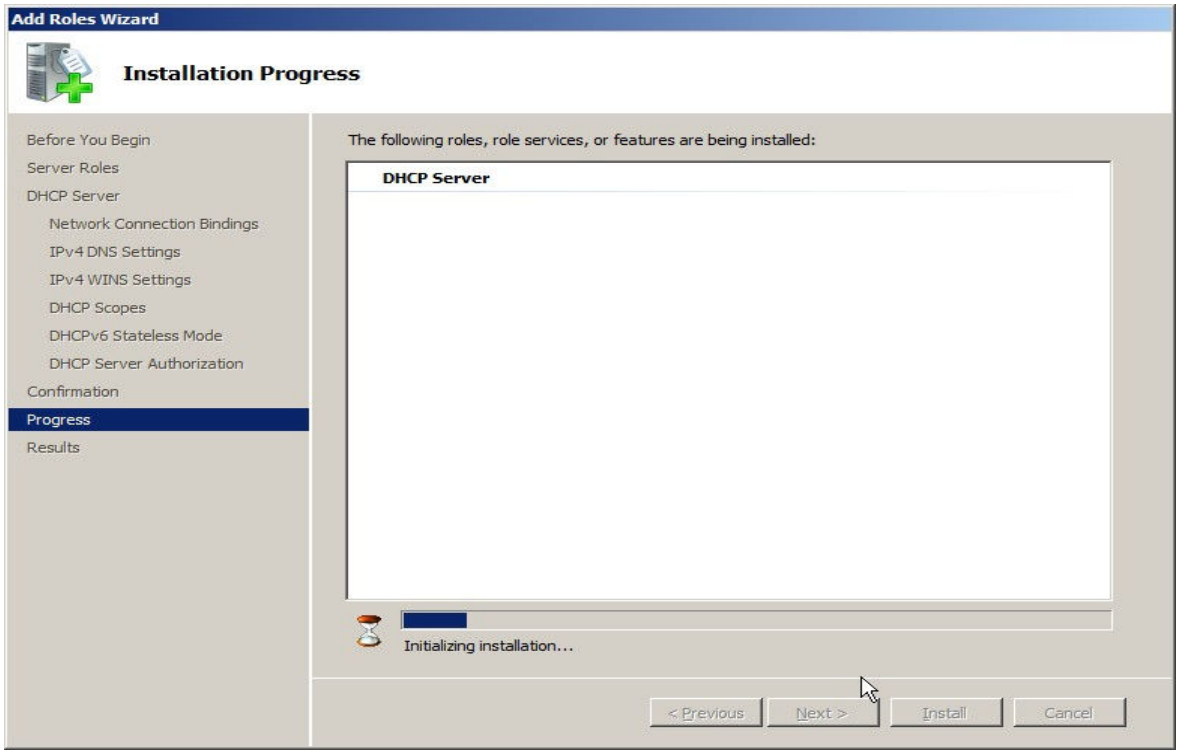
Επιλέγουμε User Credentials και πατάμε Next



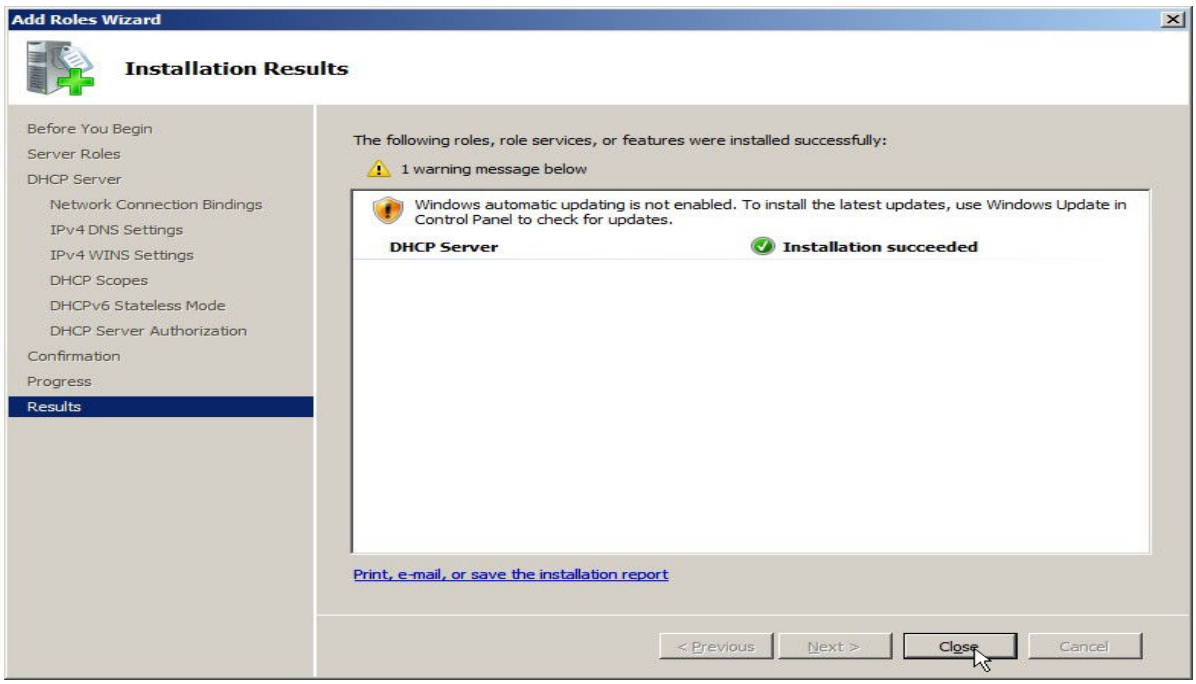
Επιβεβαιώνουμε ότι τα στοιχεία που δώσαμε είναι σωστά και πατάμε next



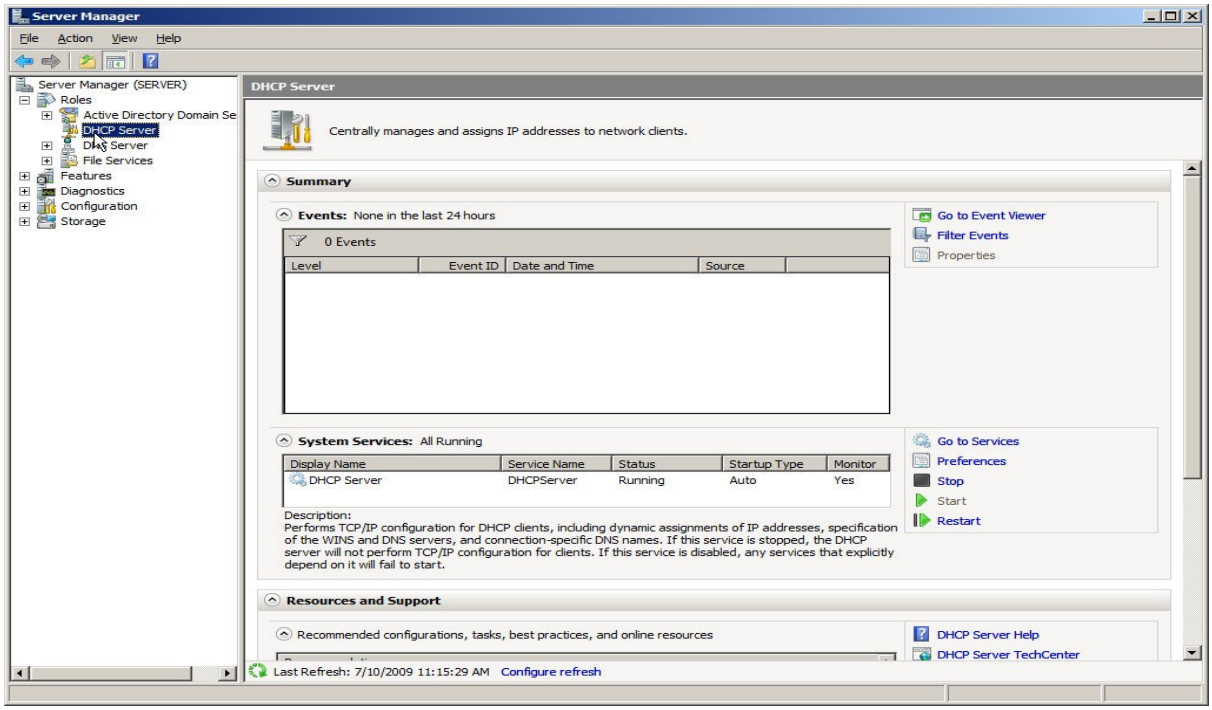
Περιμένουμε να γίνει η εγκατάσταση



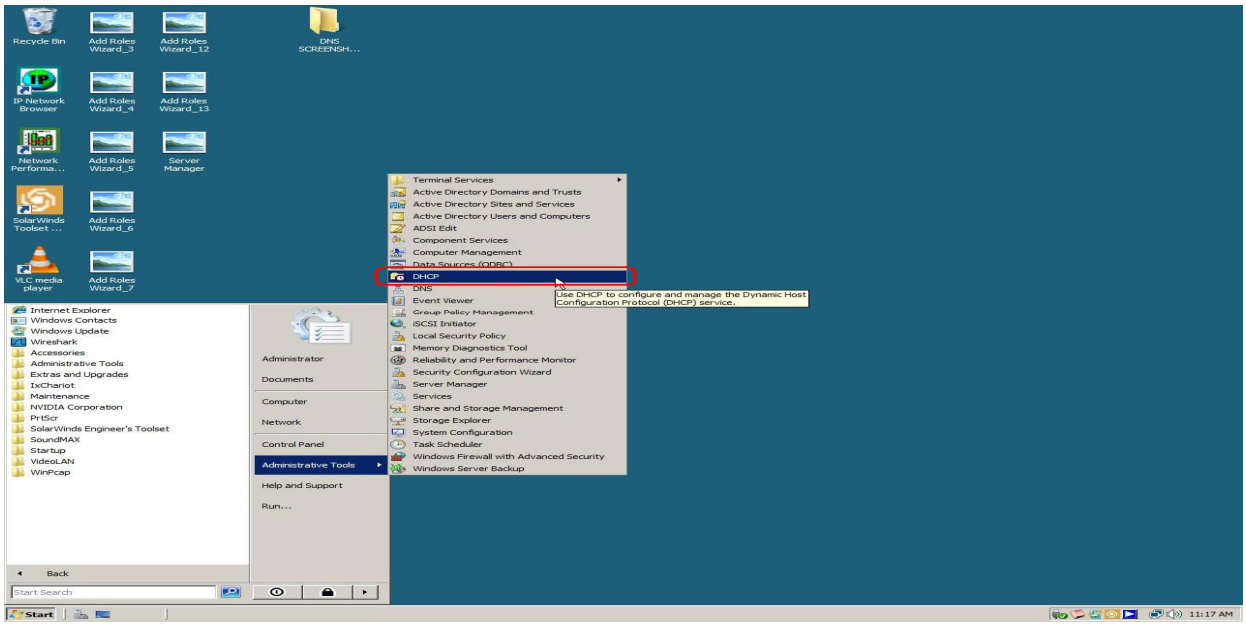
Βλέπουμε τα αποτελέσματα και πατάμε close



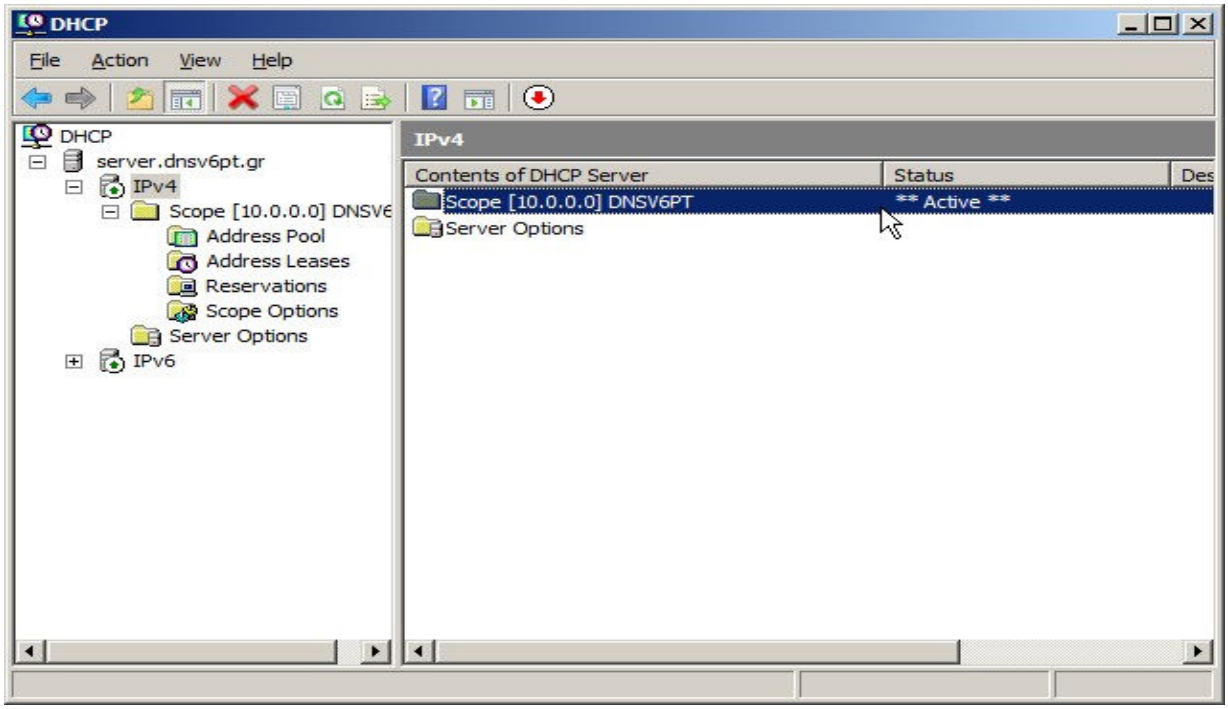
Τώρα κάνουμε επιβεβαίωση του DHCP Server από το server manager

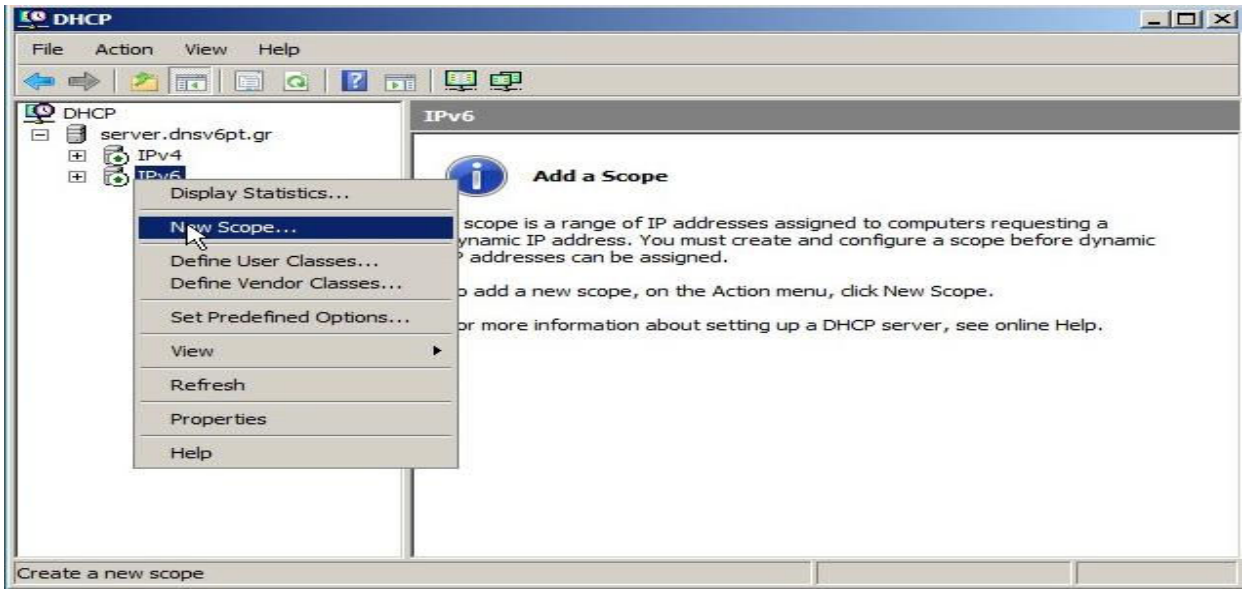


Ανοιγουμε τον DHCP Server από εναρξη → Administrative tools → DHCP

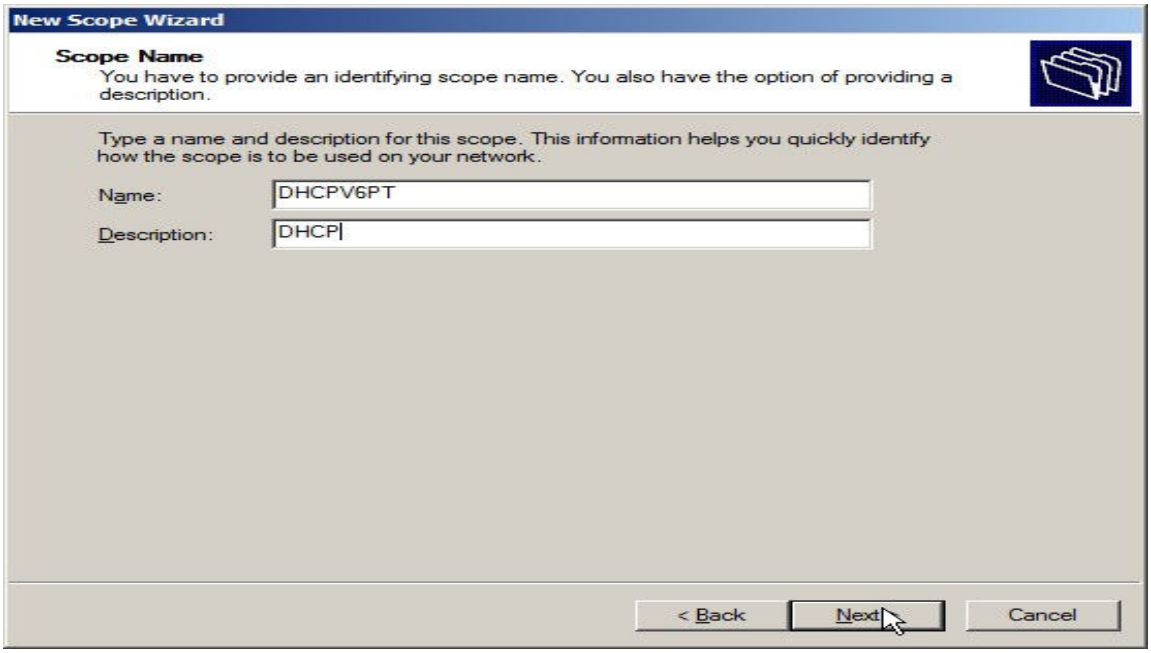


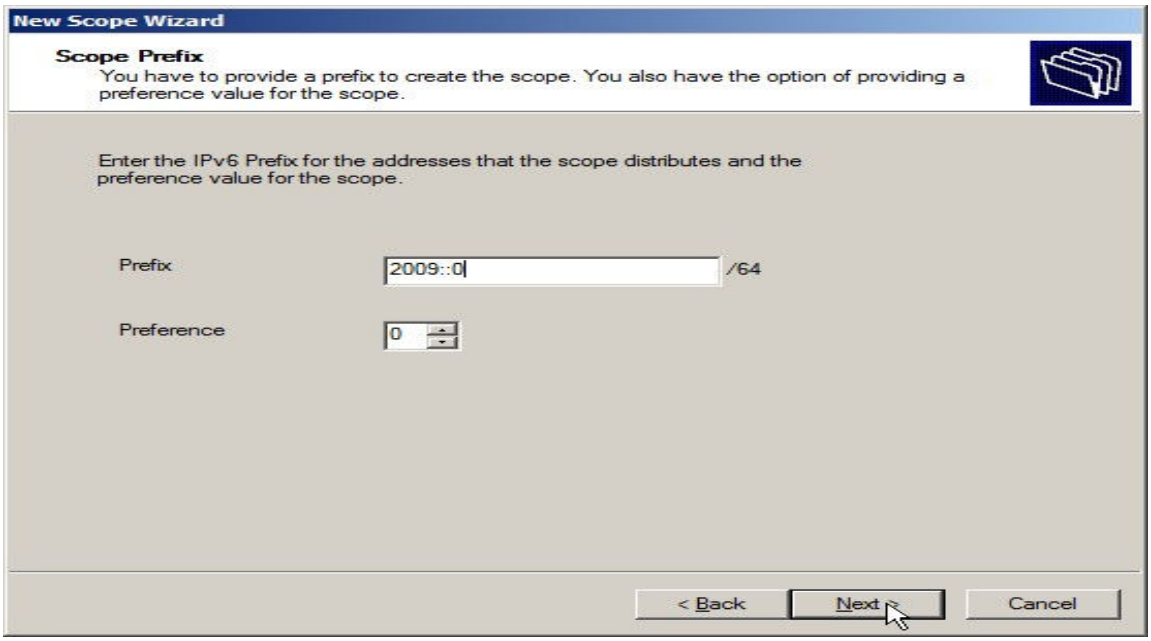
Δημιουργούμε ένα καινούργιο scope

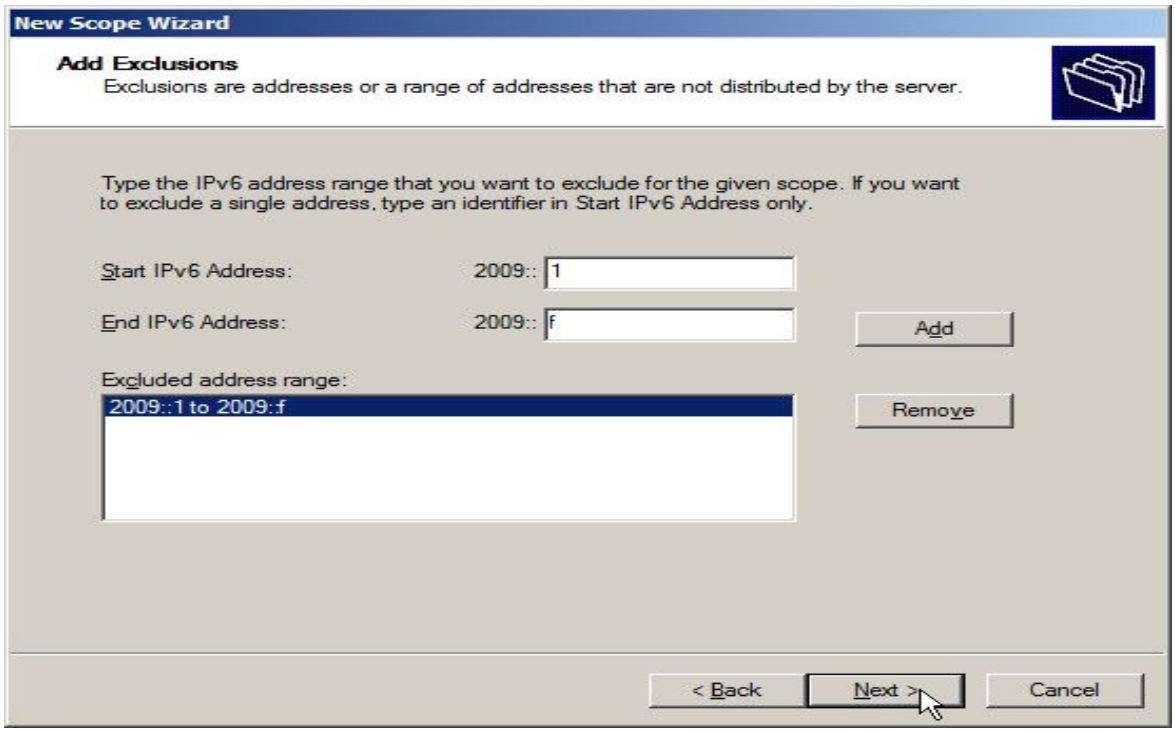


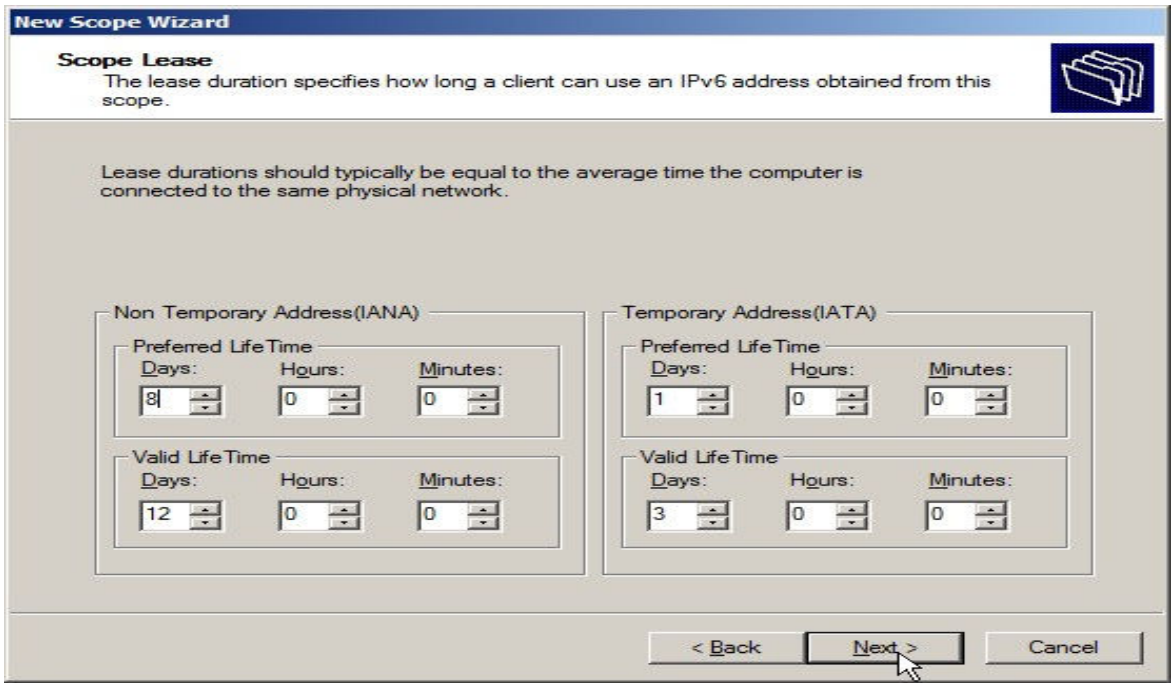


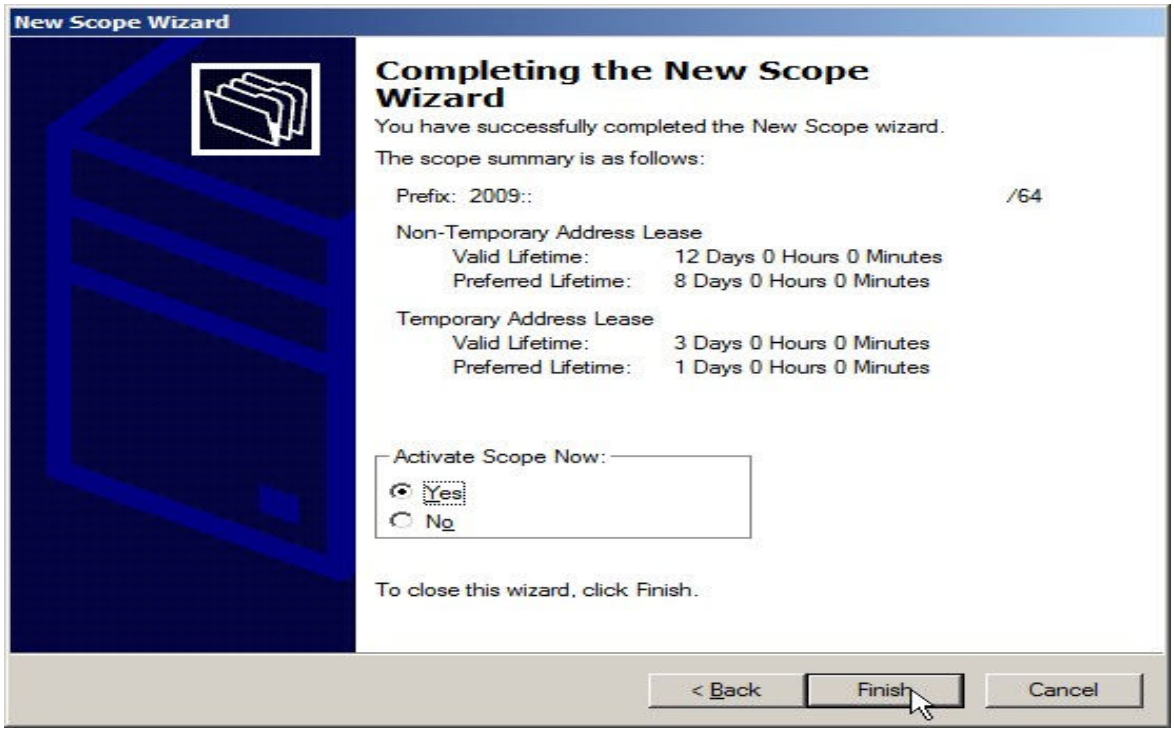
Και βάζουμε τα στοιχεία όπως φαίνετε παρακάτω



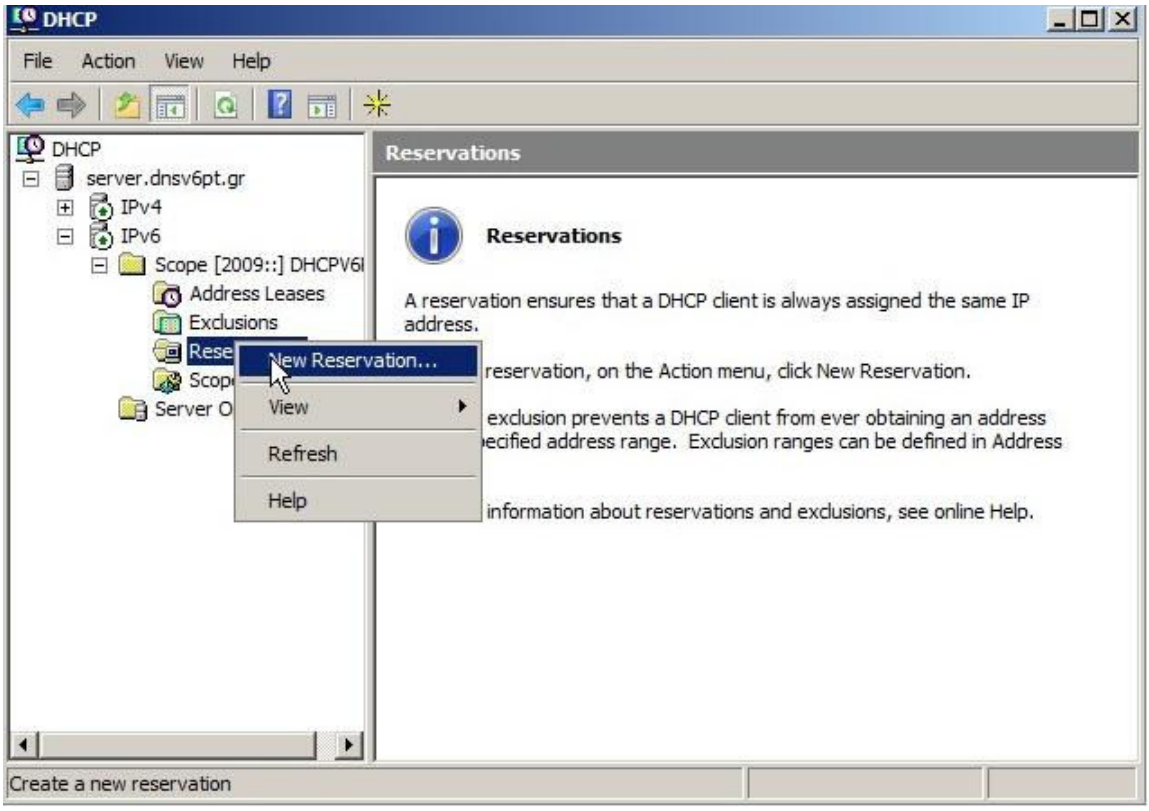

New Scope Wizard
Scope Prefix
You have to provide a prefix to create the scope. You also have the option of providing a preference value for the scope.
Enter the IPv6 Prefix for the addresses that the scope distributes and the preference value for the scope.
Prefix
2009::0
/64
Preference
0
< Back
Next >
Cancel


New Scope Wizard
Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.
Type the IPv6 address range that you want to exclude for the given scope. If you want to exclude a single address, type an identifier in Start IPv6 Address only.
Start IPv6 Address:
2009::
1
End IPv6 Address:
2009::
f
Add
Excluded address range:
2009::1 to 2009::f
Remove
< Back
Next >
Cancel





Και τέλος κάνουμε New Reservation με τον ίδιο τρόπο



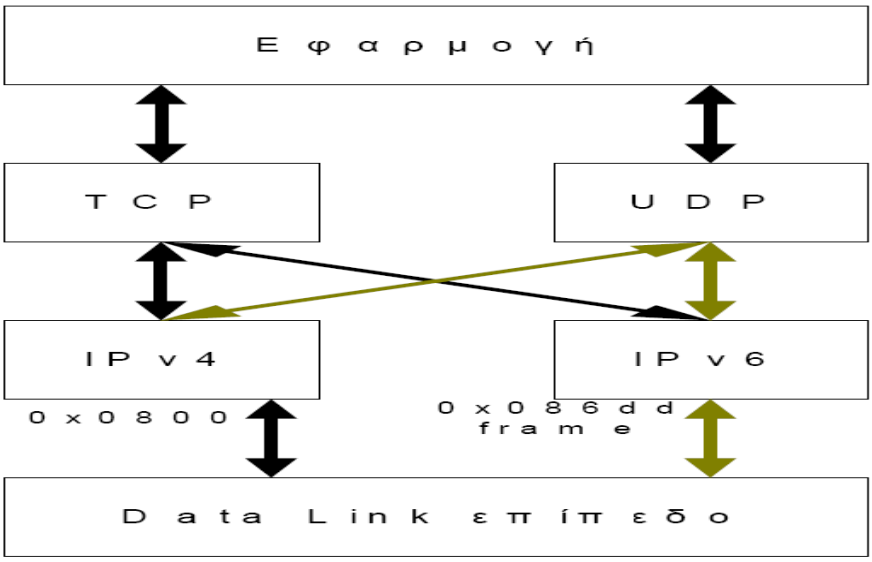
Κεφάλαιο 12^{o} - Σύνδεση σε υπάρχουσα Υποδομή

12.1 Υπάρχουσα υποδομή

Η τεχνική Dual Stack είναι η πιο διαδεδομένη και επιτρέπει σε ένα δίκτυο να υπάρχουν ταυτόχρονα hosts που λειτουργούν με IPv4 και άλλους με IPv6. Ο router που υποστηρίζει αυτή την εγκατάσταση θα πρέπει να εκτελεί τόσο την διεργασία IPv4 routing όσο και την IPv6, εξ ου και η ονομασία Dual Stack. Αυτό επιβαρύνει τον router, αλλά δίνει την δυνατότητα της ταυτόχρονης υποστήριξης IPv4 και IPv6.

Μία άλλη μεγάλη κατηγορία τεχνικής για την επίτευξη της μετάβασης από το IPv4 στο IPv6 είναι το tunneling. Μεταξύ άλλων, αναφέρουμε το 6to4 manual tunneling, 6to4 dynamic

tunneling και το λιγότερο διαδεδομένο και αρκετά πιο πολύπλοκο NAT-PT tunneling. Κάθε ένα καλύπτει διαφορετικές περιπτώσεις και ανάγκες. Η γενική ιδέα του tunneling είναι η ενθυλάκωση ενός IPv4 πακέτου σε ένα IPv6 και αντίστροφα. Οι routers που υποστηρίζουν τέτοιες εγκαταστάσεις οφείλουν να κάνουν encapsulation και decapsulation τα IP πακέτα από την μία έκδοση IP στην άλλη για την επικοινωνία των ανομοιογενών δικτύων. Κάτι τέτοιο προϋποθέτει την λειτουργία Dual Stack και συνεπώς η επιβάρυνση των routers είναι ακόμα μεγαλύτερη.



Σχ12.1.1 Dual Stack

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.

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 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.

	IPv4 server	**IPv6 server**
IPv4 client	Επικοινωνούν με IPv4	Επικοινωνούν με IPv4, ο server βλέπει την IPv4-mapped IPv6 διεύθυνση
IPv6 client	Μπορούν να επικοινωνήσουν εάν ο IPv6 client χρησιμοποιήσει μία IPv4-mapped IPv6 διεύθυνση	Επικοινωνούν με IPv6

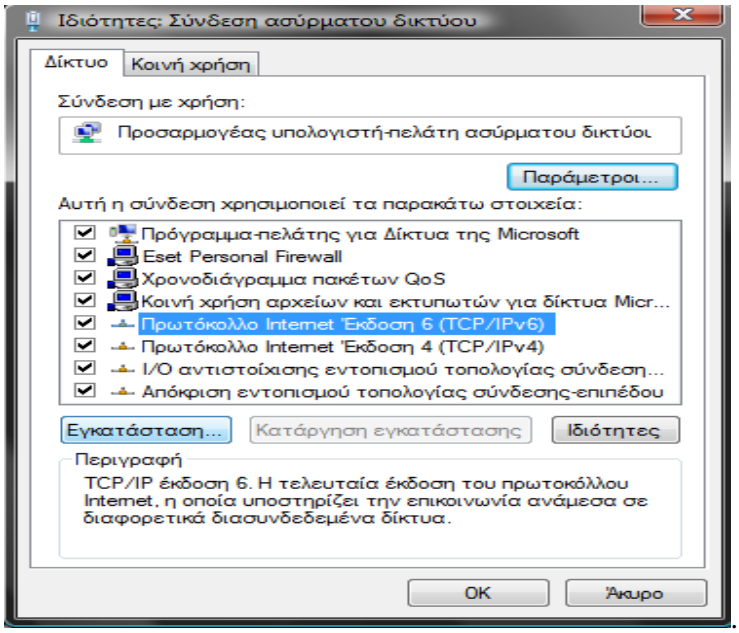
Π 12.1.1

12.2 Υλοποίηση

Παρακάτω δίνονται τα βήματα που έγιναν στο εργαστήριο για την ενεργοποίηση του IPv6 και την δημιουργία του δικτύου ώστε να παρθούν οι μετρήσεις

- Format στους εννέα υπολογιστές που θα αποτελούν το δίκτυο μας
- Εγκατάσταση των windows server 2008

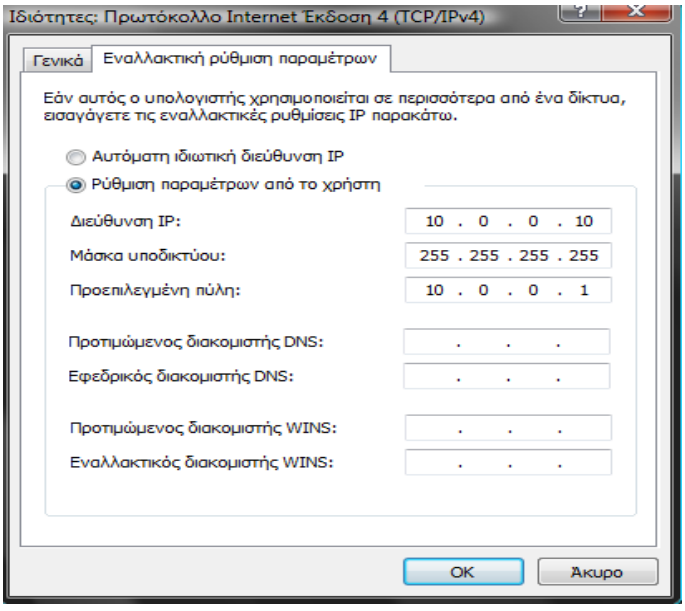
- Εγκατάσταση των Drivers και τον κατάλληλων προγραμμάτων για να παρθούν μετρήσεις
- Εγκατάσταση πρωτόκολλου IPv6



- Δόθηκαν οι στατικές ip

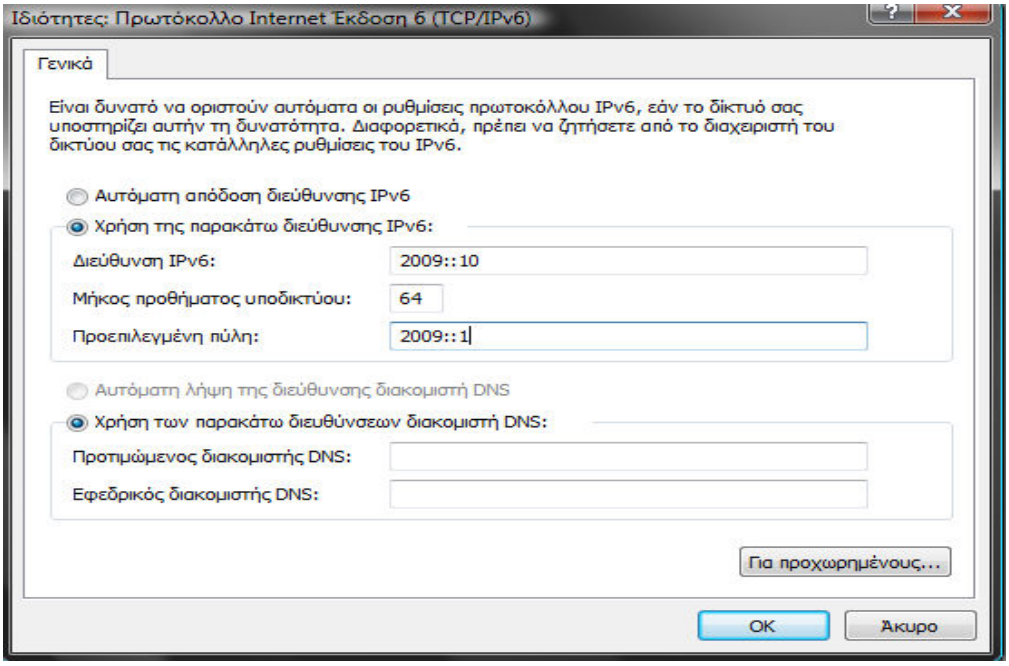
Για IPv4 ο server είχε την ip 10.0.0.10 με μάσκα 255.255.255.192

Και οι υπόλοιπη υπολογιστές 10.0.0.11-10.0.0.18

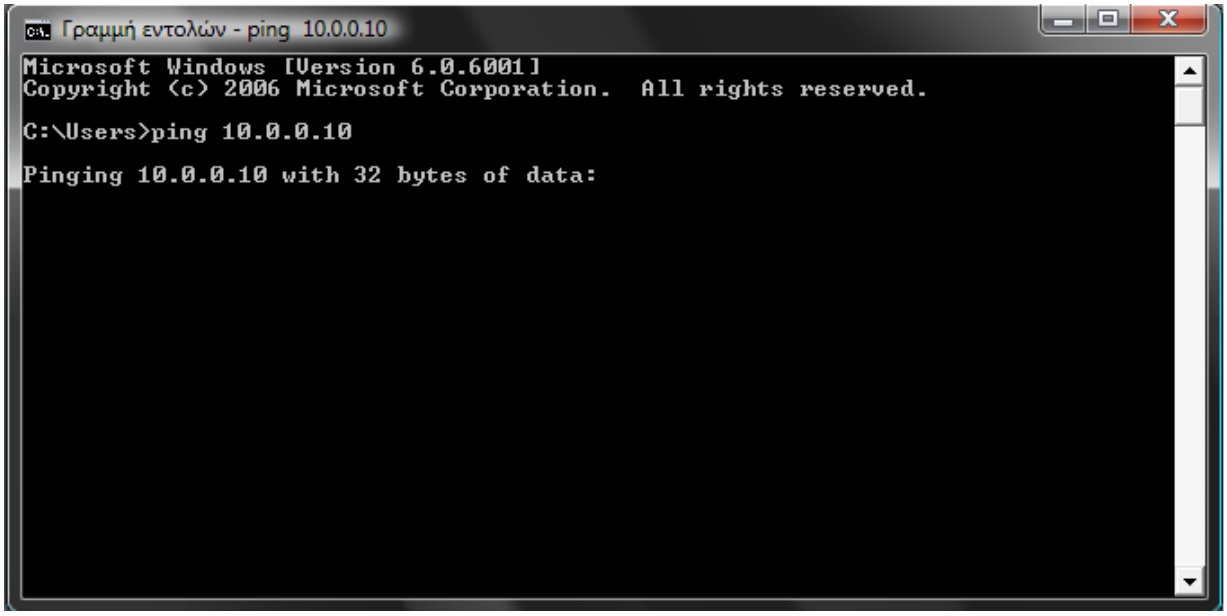


Για IPv6 ο server είχε την ip 2009::1 με μάσκα 255.255.255.192

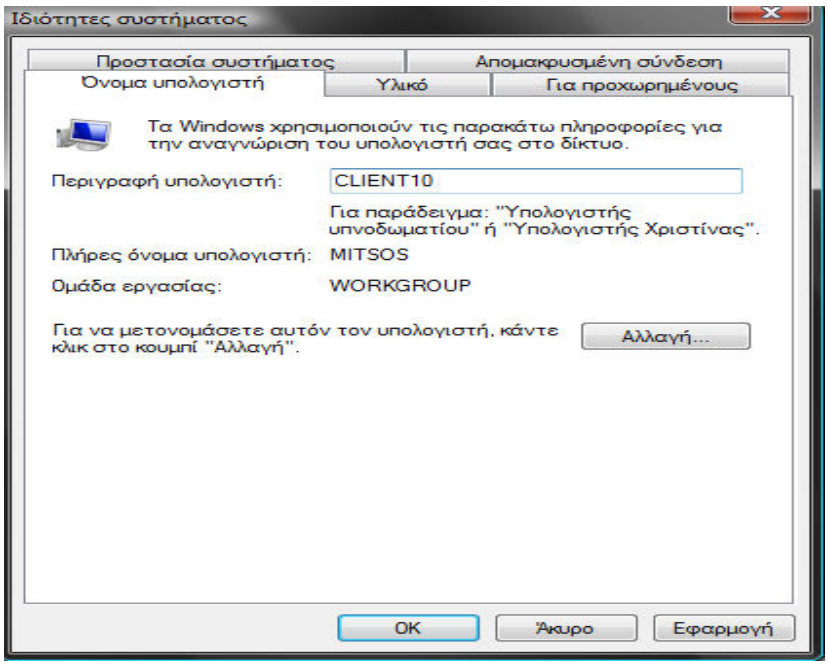
Και οι υπόλοιπη υπολογιστές 2009::1 - 2009::18



- Κάναμε ping στους υπολογιστές για να ελέγξουμε ότι επικοινωνούν.



- Τέλος όλοι οι υπολογιστές ονομάστηκαν client10-18



Κεφάλαιο 13ο - Προβλήματα στην Υιοθέτηση του IPv6

13.1 Εισαγωγή

Οι περισσότεροι ενδιαφερόμενοι δεν διαθέτουν, σήμερα, σαφή εικόνα των πλεονεκτημάτων από την υιοθέτηση του IPv6. Τα οφέλη είναι μακροπρόθεσμα και εξαρτώνται επίσης από αποφάσεις άλλων ενδιαφερόμενων σχετικά με τον χρόνο και τον τρόπο υλοποίησης του IPv6.

Όσο περισσότερο χρησιμοποιούν το IPv6 οι χρήστες, τόσο ελκυστικότερο καθίσταται και για τους λοιπούς. Με την αύξηση του αριθμού χρηστών περισσότερα προϊόντα και υπηρεσίες θα προσφέρονται σε χαμηλότερες τιμές και καλύτερη ποιότητα. Θα αυξηθεί επίσης η συνολική γνώση σχετικά με την λειτουργία και την διαχείριση του IPv6. Το αποτέλεσμα θα είναι ένα οικοσύστημα προμηθευτών και παρόχων υπηρεσιών που θα αλληλοενισχύονται, με αποτέλεσμα

βελτίωση της εμπιστοσύνης και επιτάχυνση της εισαγωγής του. Παρόμοιες δυνάμεις αγοράς επενεργούν, άλλωστε, και στο IPv4, όπου το εν λόγω οικοσύστημα υφίσταται για πολλά έτη με αποτέλεσμα μακρά παράδοση συσκευών και εφαρμογών.

Είναι δύσκολο να δοθεί ώθηση για ένα συλλογικό κίνημα εφαρμογής του IPv6, δεδομένου ότι οι ενδιαφερόμενοι δεν μπορούν εύκολα να λάβουν υπόψη τους τις αποφάσεις των άλλων. Δεν υπάρχει ενιαία καθοδηγητική αρχή για την εισαγωγή του IPv6 ή για την κατάρτιση ενός συντονισμένου ρυθμιστικού σχεδίου. Η διάδοση των IPv6 είναι επομένως μια αποκεντρωμένη διαδικασία που κατευθύνεται από την αγορά, σε παγκόσμια κλίμακα. Στην κατάσταση αυτή πολλοί ενδιαφερόμενοι τηρούν στάση αναμονής ("βλέποντας και κάνοντας") σχετικά με το IPv6 ή επιλέγουν την "σίγουρη και γνωστή" λύση του IPv4. Το σωρευτικό αποτέλεσμα που προκύπτει είναι η καθυστέρηση που περιγράφηκε στην ευρύτερη υιοθέτηση του IPv6. Πρόκειται για κατάσταση όπου η λήψη ενδεδειγμένων μέτρων πολιτικής θα μπορούσε να αποτελέσει κίνητρο για την αγορά, ενθαρρύνοντας άτομα και οργανισμούς να εξετάσουν με θετικό πνεύμα την μετάβαση στο νέο πρωτόκολλο. Τα μέτρα αυτά θα είναι αποτελεσματικότερα εφόσον ληφθούν συλλογικά, σε ευρωπαϊκή κλίμακα.

13.2 Διαθέσιμο Υλικό

Με την μετάβαση στο IPv6 δημιουργούνται διάφορα θέματα κυρίως τεχνικής φύσεως. Πέρα από την επιμόρφωση των τεχνικών τμημάτων, τις αλλαγές στα δίκτυα, τα λειτουργικά συστήματα και τις εφαρμογές και την αγορά και αναβάθμιση του εξοπλισμού, υπάρχουν θέματα που αφορούν την ίδια την διαδικασία του routing και την διαχείριση των IPv6 πακέτων. Οι διευθύνσεις στο IPv6 έχουν τετραπλάσιο μέγεθος από αυτές στο IPv4, γεγονός που επηρεάζει την λειτουργία των routers και όχι μόνο. Οι περισσότερες συσκευές είναι υλοποιημένες με ολοκληρωμένα κυκλώματα ASIC που μπορούν να διαχειρίζονται πολύ γρήγορα σε hardware επίπεδο τα IP πακέτα. Αυτά όμως είναι υλοποιημένα με 64 bit καταχωρητές (source και destination address) και γενικά είναι φτιαγμένα για να διαχειρίζονται 32 bit διευθύνσεις. Για την αποδοτική διαχείριση των IPv6 πακέτων πρέπει είτε να γίνει ένα είδος emulation της λειτουργίας των ASIC κυκλωμάτων είτε να κατασκευαστούν νέα που θα υποστηρίζουν εγγενώς το IPv6. Το πρώτο επιφέρει σημαντικές μειώσεις στην απόδοση των routers και αυξάνει κατά πολύ το φόρτο εργασίας τους, ενώ το δεύτερο αυξάνει το κόστος.

Επιπλέον, το IPv6 επιτρέπει ένας host να έχει πολλαπλές διευθύνσεις (multihomed hosts). Αυτό σημαίνει ότι στο routing table ενός router θα πρέπει να υπάρχουν πολλαπλές καταχωρήσεις για έναν host, κάθε μία από τις οποίες θα καταλαμβάνει στη μνήμη τετραπλάσιο χώρο από τις αντίστοιχες του IPv4. Αυτό αυξάνει τις απαιτήσεις τόσο σε μνήμη όσο και σε ταχύτητα, αφού κάθε αναζήτηση γίνεται ανάμεσα σε μεγαλύτερο όγκο δεδομένων.

Πρόκειται κυρίως για τεχνικά θέματα που αφορούν τους μηχανικούς που σχεδιάζουν τους routers τόσο σε hardware όσο και software επίπεδο και έχουν σαφές οικονομικό αντίκτυπο στα τελικά προϊόντα.

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

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

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

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

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

- *Απόκτηση εμπειρίας με το IPv6*: Αυτή η φάση συνεπάγεται την ενεργοποίηση του IPv6 σε ένα μικρό αριθμό συστημάτων, την παρακολούθηση του τι συμβαίνει και τη διεξαγωγή κάποιων πειραμάτων. Αυτό που χρειάζεται εδώ είναι ένα «τούνελ» IPv6 και κάποιο υλικό που δε χρησιμοποιείται για κάτι σημαντικό. Σε αυτό το σημείο, είναι πιθανό να εγκαταλειφθεί η προσπάθεια.
- *Προσθήκη μειωμένης υποστήριξης IPv6*: Σε αυτό το σημείο, είναι πιθανό να γίνουν διάφορα πράγματα στο IPv6 αλλά μπορεί να χρειάζεται ακόμα IPv4 συνδεσιμότητα. Υπάρχουν κάποιοι κίνδυνοι εδώ, αφού το IPv6 χρησιμοποιείται στην παραγωγή, αλλά η επιστροφή στο IPv4 είναι ακόμα πιθανή.
- *Προαγωγή του IPv6 σε αντίστοιχο με το IPv4*: Αυτό σημαίνει την απόσυρση του υλικού που χρησιμοποιεί μόνο IPv4 καθώς και του αντίστοιχου λογισμικού ή την υιοθέτηση τεχνικών μετάβασης ώστε να είναι δυνατή η παροχή IPv4 υπηρεσιών. Είναι δύσκολη η επιστροφή στο IPv4 μετά από αυτό το σημείο γιατί οι χρήστες μπορεί τώρα να εξαρτώνται από τις δυνατότητες του IPv6.
- *Τερματισμός χρήσης του IPv4*: Το να σταματήσει κανείς να χρησιμοποιεί IPv4 δε θα είναι δυνατό για αρκετό χρόνο ακόμα, αλλά το να υπάρχουν κομμάτια δικτύου που θα υποστηρίζουν μόνο IPv6 είναι κάτι που μπορεί να συμβεί σχετικά σύντομα, ειδικά με τη βοήθεια των τεχνικών μετάβασης έτσι ώστε να είναι δυνατή μέχρι τότε η χρήση υπηρεσιών IPv4.

13.3 Κόστος της εισαγωγής του IPv6

Η εγκατάσταση και λειτουργία του νέου πρωτοκόλλου συνεπάγεται κόστη εκπαίδευσης προσωπικού, αναβάθμισης δικτύων και εξοπλισμού. 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 6net7 και το δίκτυο GÉANT8, στα οποία το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ ΑΕ)9 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 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.

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.
Η αξιόπιστη εκτίμηση του κόστους της παγκόσμιας εισαγωγής του IPv6 είναι ουσιαστικά αδύνατη. Η σταθερά αυξανόμενη υιοθέτηση του IPv6 από τους διάφορους ενδιαφερομένους θα συμβάλει στον έλεγχο των δαπανών.

Η μετάβαση στο IPv6 έχει καθοριστική σημασία, καθότι οι διαθέσιμες διευθύνσεις του ισχύοντος Πρωτοκόλλου Ιντερνέτ του IPv4 εξαντλούνται με ταχύ ρυθμό: προβλέπεται ότι το απόθεμα των διευθύνσεων του IPv4 θα εξαντληθεί πριν από το 2012. Εάν δεν επιταχυνθεί δραστικά η εισαγωγή του IPv6, η ανάπτυξη του διαδικτύου θα σημειώσει δραματική επιβράδυνση, το δε κόστος της χρήσης του διαδικτύου θα επηρεασθεί αρνητικά από τα κατάλοιπα του IPv4 στα δίκτυα της ΕΕ. Η καθυστέρηση αυτή θα επιφέρει υψηλότερο κόστος σε όλους τους τομείς του εμπορίου μέσω του διαδικτύου, επιβράδυνση της καινοτομίας που βασίζεται στο IP, καθώς επίσης επιβράδυνση της οικονομικής ανάπτυξης.

13.4 Τρόποι παράτασης ζωής του IPv4

Στην παράταση ζωής του Του IPv4 συνέβαλαν πολύ οι μηχανισμοί NAT και CIDR. NAT όπως προαναφέρθηκε σε προηγούμενα κεφάλαια είναι ένα εργαλείο που βοήθησε στην ανακούφιση της IPv4 στην έλλειψης διευθύνσεων και το CIDR (Classless Interdomain Rooting) με το οποίο κάνουμε οικονομία στις public IP (βλέπε Κεφ. 3).

Προσωρινές λύσεις IPv4:

- IPv4 routing: μεγάλες λίστες στους δρομολογητές
- Subnetting: Χρήση subnet masks
- CIDR: Συνένωση υποδικτύων
- DHCP: Autoconfiguration, απαιτεί ρητή αρχικοποίηση DHCP server
- TOS: Πεδίο για παροχή ποιότητας υπηρεσίας
- IPsec: Υλοποίηση μηχανισμών ασφάλειας στο IPv4
- NAT: Ένα υποδίκτυο δεν δεσμεύει εσωτερικά μοναδικές IP διευθύνσεις, αλλά γίνεται χρήση ενός μεσολαβητή που μεταφράζει τις διευθύνσεις του υποδικτύου σε μοναδικές διευθύνσεις διαδικτύου, επιτρέποντας την έμμεση επικοινωνία με το διαδίκτυο

Συμπεράσματα

Στην πτυχιακή αυτή έγινε η σύγκριση του είδη υπάρχων IPv4 με το επερχόμενο IPv6 και καταλήγουμε στο συμπέρασμα ότι το IPv6 υπερτερεί έναντι του IPv4 στους περισσότερους τομής εκτός της μικρής διαφοράς στην απόδοση της ταχύτητας και του οικονομικού προβλήματος στην μετάβαση από την IPv4 στην IPv6.
Ακόμα το IPv6 υστερεί στην έλλειψη γνώσεως του αντικειμένου σε σχέση με το IPv4 από τους περισσότερους ώστε να ασχοληθεί ο καθένας χώρια και έτσι όλοι περιμένουν να δουν την εξέλιξη στους άλλους για να ασχοληθούν και αυτοί.

Μελλοντική εργασία

Πολιτικές Συνύπαρξης

Συνύπαρξη των Ipv4 και IPv6 γίνετε με τους τρόπους που έχουν προαναφερθεί σε προηγούμενα κεφάλαια όπως dual stack, Tunneling και Translation

Πρωτόκολλα Δρομολόγησης

Πρωτόκολλα δρομολόγησης IPv6:

- Επέκταση των υπαρχόντων πρωτοκόλλων δρομολόγησης IPv4 για χειρισμό μεγαλυτέρων διευθύνσεων
- RIPv6 (RFC 2080) παρόμοιο με RIPv2
- BGP4+ - Multi-Protocols Extensions (RFC 2283, 2545)
- Integrated IS-IS –Η δυνατότητα για διευθύνσεις NSAP μεγάλου μεγέθους επιτρέπει διευθύνσεις IPv6 (Draft-ietf-isis-ipv6-01)
- OSPFv3 (RFC 2740) ΝέαυλοποίησηγιαIPv6

IPv6 Δρομολόγηση Multicast:

- PIM με επεκτάσεις IPv6
- MOSPF με επεκτάσεις IPv6
- MBGP με επεκτάσεις IPv6
- IPv6 Multicast με περισσότερες διευθύνσεις με σημαντικά μικρότερο πρόβλημα για επικάλυψη διευθύνσεων IP

IPv6tunnels:

- IPv4-compatibleIPv6 διευθύνσεις
- IPv4-mappedIPv6 διευθύνσεις
- Configured Tunnels
- Automatic Tunnels
- Είδη tunnels
- Router-to-router tunneling
- Host-to-router tunneling
- Host-to-host tunneling
- Router-to-host

- 6to4
- 6over4

Mobile IPv6

Στο παρελθόν, συνηθίζαμε να κάνουμε τηλεφωνικές κλήσεις από το σπίτι ή το γραφείο. Τα κινητά τηλέφωνα μας έδωσαν την δυνατότητα να κάνουμε τηλεφωνήματα καθώς βρισκόμασταν σε κίνηση οπουδήποτε και οποιαδήποτε στιγμή. Η χρήση των φορητών υπολογιστών, των ασύρματων δικτύων και των φορητών συσκευών που έχουν δυνατότητα σύνδεσης στο διαδίκτυο συνεχώς αυξάνεται και εξαπλώνεται. Αν αυτές οι συσκευές χρησιμοποιούν την IP σαν πρωτόκολλο μετάδοσης, τότε χρειαζόμαστε την Mobile IP να κάνει την δουλειά. Ζητάμε από τις συσκευές μας να παραμένουν συνδεδεμένες στο δίκτυο, ενώ εμείς μετακινούμαστε και το σημείο πρόσβασης στο δίκτυο αλλάζει. Όπως ακριβώς συμβαίνει με τα δίκτυα κινητής τηλεφωνίας σήμερα. Για παράδειγμα, όταν χρησιμοποιούμε ένα PDA τηλέφωνο στο σπίτι και είμαστε συνδεδεμένοι στο διαδίκτυο, το τηλέφωνο χρησιμοποιεί το ασύρματο interface που διαθέτει. Όταν βγούμε από το σπίτι, το κινητό αλλάζει αυτόματα σε GPRS και παραμένει στο διαδίκτυο με όλες τις εφαρμογές που τρέχουν εκείνη την στιγμή να συνεχίζουν κανονικά

Βιβλιογραφία

Internet

1. www.Ipv6.com
2. http://www.zdnetasia.com/techguide/windows/0,39044904,62040433,00.htm

Βιβλία

1. Η Μετάβαση του Διαδικτύου από το IPv4 στο IPv6 - Του Δρ. Ν. Τσαρμπόπουλου
2. IPv6 Essentials, 2nd Edition (2006) - Silvia Hagen
3. Understanding IPv6 2ND Edition – Joseph Davies
4. Internet and Wireless Security - Robert Temple and John Regnault
5. Deploying IPv6 Networks 2006 - Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete
6. Migrating to Ipv6 – Marc Blanchet
7. DNS and BIND, by Paul Albitz and Cricket Liu (O'Reilly).
8. SSL VPN - Understanding Evaluating, And Planning Secure, Web-Based Remote Access – Joseph Steinberg