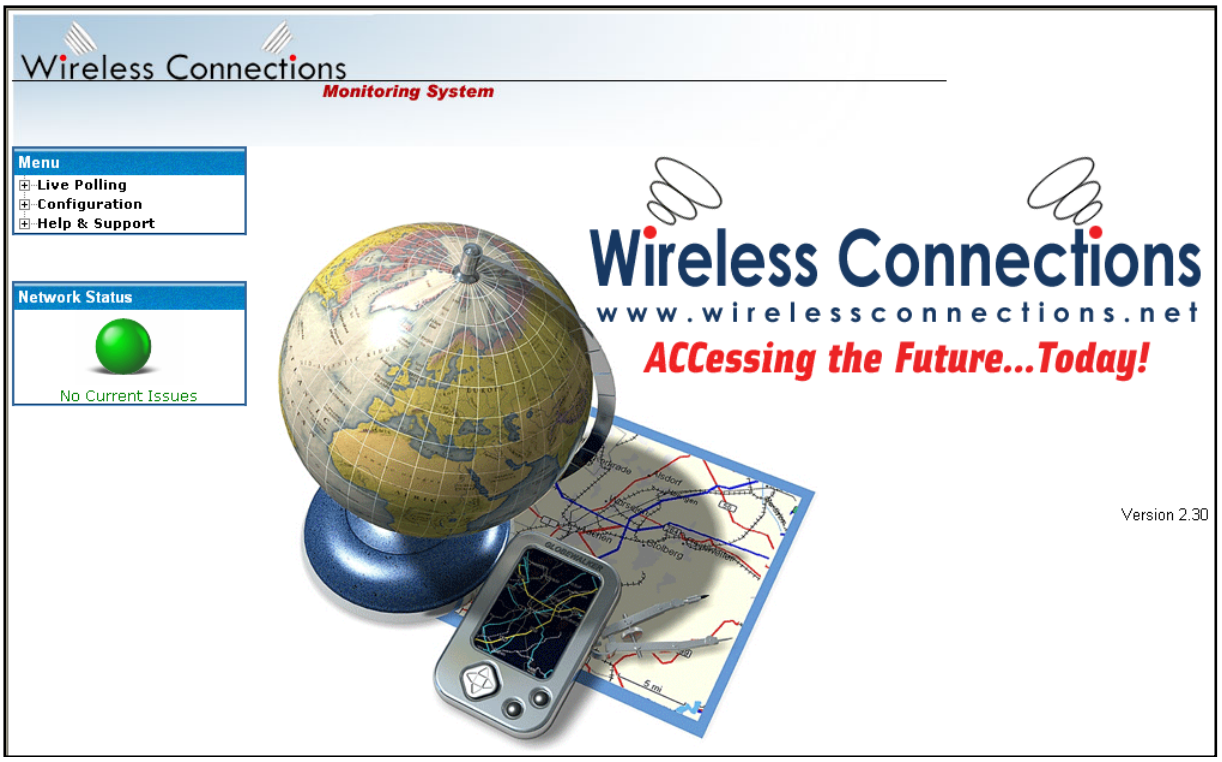
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΠΡΟΗΓΜΕΝΑ ΣΥΣΤΗΜΑΤΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

ΑΞΙΟΛΟΓΗΣΗ ΕΠΙΔΟΣΕΩΝ ΑΣΥΡΜΑΤΟΥ ΕΥΡΥΖΩΝΙΚΟΥ ΔΙΚΤΥΟΥ ΠΑΡΟΧΗΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΣΕ ΣΧΟΛΙΚΕΣ ΜΟΝΑΔΕΣ



Διπλωματική εργασία

Επιβλέπουσα: Αν. Καθηγήτρια Νιόβη-Φωτεινή Παυλίδου

Ανέστης Ζαγκάκης
Ηλεκτρολόγος Μηχανικός
zagakis@freemail.gr

Γρηγόριος Κυριακού
Χημικός Μηχανικός
grkyriakou@sch.gr

Γεώργιος Παλτόγλου
Μαθηματικός
gpalt@yahoo.com

Θεσσαλονίκη 2005

Περιεχόμενα

Πρόλογος

Οι ραγδαίες τεχνολογικές εξελίξεις της εποχής μας αλλάζουν μέρα με τη μέρα το τοπίο στις Τεχνολογίες των Επικοινωνιών και της Πληροφορίας. Ένας χώρος που (οφείλει να) παρακολουθεί στενά αυτές τις εξελίξεις με σκοπό να επωφεληθεί απ' αυτές είναι και η Εκπαίδευση και συγκεκριμένα η Δευτεροβάθμια Εκπαίδευση.

Μια ασύρματη νησίδα παροχής ευρυζωνικής πρόσβασης στο Διαδίκτυο που εγκαταστάθηκε και λειτουργεί στα σχολεία της Δευτεροβάθμιας Εκπαίδευσης της πόλης του Κιλκίς υπήρξε η αφορμή για τη σύλληψη της ιδέας και την εκπόνηση αυτής της διπλωματικής εργασίας.

Το έργο αυτό είναι προπομπός για άλλα μεγάλα έργα δικτύωσης. Η ανάπτυξη του «Σύζευξις» είναι όλο και πιο κοντά με τις ενσύρματες ευρυζωνικές επικοινωνίες να υλοποιούνται στις πόλεις με οπτικές ίνες και τη σύνδεση με απομακρυσμένα σημεία και οικισμούς να γίνεται με ασύρματες ζεύξεις.

Στόχοι μας ήταν η μελέτη αυτού του ασύρματου δικτύου, η διακρίβωση των ιδιαιτεροτήτων του σε σχέση με τα παραδοσιακά δίκτυα (ενσύρματα και στενής ζώνης), η αξιολόγηση των επιδόσεών του και, στο μέτρο του δυνατού, η εξαγωγή συμπερασμάτων χρήσιμων τόσο για τη βελτίωσή του, όσο και για μελλοντικές υλοποιήσεις.

Το αν αυτοί οι στόχοι επιτεύχθηκαν και σε ποιο βαθμό θα το κρίνει βεβαίως ο (ακαδημαϊκός ή μη) αναγνώστης. Αυτό που είναι σίγουρα το προκαταβολικό κέρδος της ομάδας εργασίας είναι η ενασχόληση με μια σειρά προβλημάτων που τέθηκαν και αντιμετωπίστηκαν «in vivo», δηλαδή σε πραγματικές «εξωεργαστηριακές» συνθήκες λειτουργίας που αφορούσαν από θέματα κακής συνδεσιμότητας συσκευών έως δυσμενείς καιρικές συνθήκες, τα οποία έπρεπε επιτακτικά να αντιμετωπιστούν για την εξασφάλιση της ομαλής συνέχειας της εργασίας.

Επίσης, δόθηκε η δυνατότητα της εμβάθυνσης στα θέματα που περιείχε το μάθημα του 2ου εξαμήνου του Προγράμματος Μεταπτυχιακών Σπουδών «Ευρυζωνικά Δίκτυα» της Αν. Καθηγήτριας Νιόβης-Φωτεινής Παυλίδου, το οποίο ήταν μια πρώτη αλλά πολύ ενδιαφέρουσα επαφή με το γνωστικό αντικείμενο αυτής της εργασίας για όλα τα μέλη της ομάδας και πραγματικά κίνησε το ενδιαφέρον μας για το αντικείμενο.

Για την αξιολόγηση χρησιμοποιήθηκε λογισμικό ελεύθερου και ανοιχτού κώδικα, ενώ οι μετρήσεις έγιναν σε διάφορα επίπεδα και πρωτόκολλα επικοινωνίας. Υπάρχει πληθώρα εφαρμογών και λειτουργικών συστημάτων, πρωτοκόλλων και υπηρεσιών που εξετάστηκαν. Έτσι έχουμε μετρήσεις με δύο εφαρμογές ανάλυσης των επιδόσεων του δικτύου: α) του Monitoring System της Wireless Connections και β) του Ethereal. Οι μετρήσεις έγιναν για μεγάλα χρονικά διαστήματα με διάφορες συνθήκες και σε διάφορα επίπεδα.

Έτσι με το Monitoring System έγιναν μετρήσεις σε επίπεδο δεδομένων. Οι μετρήσεις είναι μάλιστα διαθέσιμες on-line αφού ο διακομιστής στον οποίο εκτελείται η εφαρμογή είναι διαθέσιμος μέσω του Διαδικτύου στην ηλεκτρονική διεύθυνση
http://194.63.234.104/monitoringweb

Οι μετρήσεις με το Ethereal αφορούν το επίπεδο μεταφοράς (transport) και υπηρεσιών

(HTTP και FTP). Μάλιστα για τις μετρήσεις χρησιμοποιήθηκε και ειδικό πρωτόκολλο Enhanced TCP, το Snoop, το οποίο είναι σε ερευνητικό στάδιο και διαθέσιμο προς το παρόν μόνο για πλατφόρμα Linux.

Η εργασία περιλαμβάνει στοιχεία σχετικά με το έργο πάνω στο οποίο γίνεται η αξιολόγηση, το θεωρητικό υπόβαθρο των ασύρματων δικτύων, την παρουσίαση του λογισμικού καταγραφής τόσο για το Monitoring System, όσο και για το Ethereal. Γίνεται και ειδική αναφορά στο πρωτόκολλο Snoop. Έπειτα παρουσιάζονται τα αποτελέσματα των μετρήσεων με γραφικές παραστάσεις και στιγμιότυπα (screenshots). Τα αποτελέσματα σχολιάζονται συγκριτικά σε κάθε περίπτωση, ενώ εξάγονται συμπεράσματα σχετικά με τις επιδόσεις του δικτύου.

Από τη θέση αυτή επιθυμούμε να ευχαριστήσουμε θερμά:

- Την Αναπληρώτρια Καθηγήτρια του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του ΑΠΘ Νιόβη-Φωτεινή Παυλίδου, η οποία αποδέχθηκε αμέσως την ιδέα μας για την εκπόνηση αυτής της εργασίας και στη συνέχεια, ως επιβλέπουσα, μας βοήθησε καθ' όλη τη διάρκεια της δουλειάς μας.
- Τον Δρ. ηλεκτρολόγο μηχανικό Ιωάννη Γκραγκόπουλο, ερευνητή του ΙΠΤΗΛ, ο οποίος είχε την ευθύνη της άμεσης καθοδήγησής μας και μας βοήθησε καθοριστικά να διαπλατύνουμε τον ορίζοντα των θεμάτων που διαπραγματεύεται η εργασία αυτή.
- Τον ηλεκτρολόγο μηχανικό ΑΠΘ Ηλία Στραβάκο, ΜΔΕ «Πληροφοριακά Συστήματα Διοίκησης», ο οποίος, ως επικεφαλής της κεντρικής ομάδας διαχείρισης του Πανελληνίου Σχολικού Δικτύου για τον Νομό Κιλκίς, μας παρείχε κάθε δυνατή τεχνική βοήθεια και πραγματικά «ξεκλείδωσε» για μας όλα τα διαθέσιμα διαχειριστικά εργαλεία για να μπορέσουμε να δουλέψουμε απρόσκοπτα. Εξάλλου, η παρούσα εργασία μπορεί να θεωρηθεί συνέχεια της δικής του διπλωματικής εργασίας που αφορούσε τη μελέτη εφαρμογής ενός παρόμοιου δικτύου.
- Τέλος, την Τριμελή Εξεταστική Επιτροπή, αποτελούμενη, εκτός της παραπάνω καθηγήτριας, από τους διδάσκοντες του ίδιου Τμήματος Καθηγητή Γεώργιο Χασάπη και Επίκουρο Καθηγητή Αναστάσιο Ντελόπουλο για τις πολύ χρήσιμες παρατηρήσεις τους.

Θεσσαλονίκη, Μάρτιος 2005

Ανέστης Ζαγκάκης

Γρηγόριος Κυριακού

Γεώργιος Παλτόγλου

1. Εισαγωγή

Η ασύρματη νησίδα διασύνδεσης εκπαιδευτικών και διοικητικών μονάδων του Κιλκίς εγκαταστάθηκε στα μέσα του 2004 και τέθηκε σταδιακά σε λειτουργία αρχής γενομένης από το φθινόπωρο του ίδιου έτους.

Το έργο δεν είναι από τα συνήθη ούτε στον χώρο της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, ούτε στον χώρο της δημόσιας διοίκησης γενικότερα. Αρκεί να αναλογιστούμε ότι παρόμοια δίκτυα λειτουργούν πειραματικά μόλις σε δέκα πόλεις της Ελλάδας αυτήν τη στιγμή και από την καλή λειτουργία τους θα εξαρτηθεί η επέκτασή τους και σε άλλες πόλεις.

Τα στοιχεία αυτά, σε συνδυασμό με το γεγονός ότι όλα τα μέλη της ομάδας εκπόνησης αυτής της εργασίας είχαν ή έχουν μια σχέση με την εκπαίδευση, στάθηκαν η αφορμή για την πραγματοποίηση αυτής της εργασίας.

Για τον σκοπό αυτό, μελετήθηκαν, αξιολογήθηκαν και επιλέχθηκαν εργαλεία παρακολούθησης και καταγραφής δικτύων, εγκαταστάθηκαν σε υπολογιστές των σχολείων του δικτύου, λήφθηκαν ποικίλες μετρήσεις, οι οποίες αξιολογήθηκαν, και τελικά προέκυψαν ορισμένα συμπεράσματα που αποσκοπούν στη βελτίωση της λειτουργίας του δικτύου.

Για να γίνει κατανοητή η σημασία του έργου αλλά και το γενικότερο πλαίσιο έργων στο οποίο εντάσσεται, στο 2ο κεφάλαιο της εργασίας γίνεται μια σύντομη περιγραφή της αρχιτεκτονικής και των δικτυακών υπηρεσιών του Πανελληνίου Σχολικού Δικτύου (ΠΣΔ), που είναι ο φορέας υλοποίησης του έργου.

Στη συνέχεια, στο 3ο κεφάλαιο, γίνεται μια θεωρητική αναφορά στο βασικό δικτυακό πρότυπο της ασύρματης δικτύωσης IEEE 802.11, σε στοιχεία που αφορούν τις τεχνολογίες ασύρματων ζεύξεων που επιτρέπεται από το ισχύον κανονιστικό πλαίσιο να χρησιμοποιηθούν στην Ελλάδα και σε νέα πρωτόκολλα που βελτιώνουν τη συμπεριφορά του TCP/IP σε ασύρματα δίκτυα όπως το Snoop.

Στο 4ο κεφάλαιο αναλύεται η διαχείριση των δικτύων και ιδιαιτέρως των δικτύων TCP/IP με το πρωτόκολλο SNMP.

Στο 5ο κεφάλαιο γίνεται μια αναλυτική περιγραφή όλων των στοιχείων του υπάρχοντος ασύρματου δικτύου αφού πάνω σ' αυτό πραγματοποιήθηκε όλο το εργαστηριακό μέρος της εργασίας.

Το πρώτο εργαλείο παρακολούθησης και καταγραφής που χρησιμοποιήθηκε είναι το λογισμικό Monitoring System της Wireless Connections. Η εγκατάστασή του στο δίκτυό μας καθώς και η διαμόρφωσή του ώστε να προσαρμοστεί στις απαιτήσεις των μετρήσεών μας παρουσιάζονται στο 6ο κεφάλαιο.

Το δεύτερο εργαλείο παρακολούθησης και καταγραφής είναι το γνωστό Ethereal, η εγκατάσταση και διαμόρφωση του οποίου περιγράφονται στο 7ο κεφάλαιο.

Στο 8ο κεφάλαιο καταγράφονται όλα τα αποτελέσματα των μετρήσεων που πραγματοποιήθηκαν με ορισμένα σχόλια για κάθε περίπτωση.

Τα τελικά συμπεράσματα και η συνολική αξιολόγηση του δικτύου διατυπώνονται στο 9ο κεφάλαιο.

Τέλος, ο επίλογος αποτελεί το 10ο κεφάλαιο.

2. Περί του Πανελληνίου Σχολικού Δικτύου (ΠΣΔ)

2.1. Εισαγωγή

Το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ - http://www.sch.gr/) είναι το εκπαιδευτικό ενδοδίκτυο του Υπουργείου Εθνικής Παιδείας και Θρησκευμάτων (http://www.ypepth.gr), που διασυνδέει όλα τα σχολεία και τους παρέχει βασικές και προηγμένες τηλεματικές υπηρεσίες. Με τον τρόπο αυτό συντελεί στη δημιουργία μιας νέας γενιάς εκπαιδευτικών κοινοτήτων, η οποία αξιοποιεί τις Τεχνολογίες της Πληροφορικής και των Επικοινωνιών στην καθημερινή εκπαιδευτική διαδικασία [12].

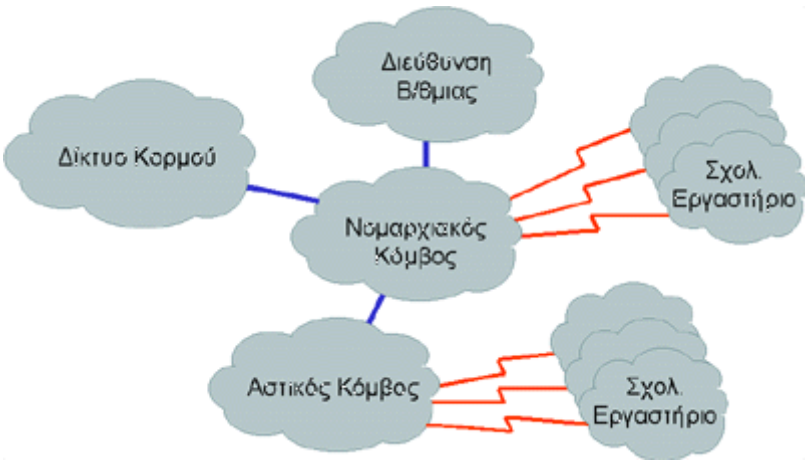
Η υλοποίηση γίνεται με τη στενή συνεργασία μεταξύ του ΥΠΕΠΘ και ενός σχήματος 12 Ερευνητικών Κέντρων και Εκπαιδευτικών Ιδρυμάτων της Τριτοβάθμιας Εκπαίδευσης, με εξειδίκευση στις τεχνολογίες δικτύων και Διαδικτύου.

2.2. Αρχιτεκτονική του δικτύου

2.2.1. Περιγραφή δικτύου

Το μοντέλο σχεδιασμού και οι λειτουργικές προδιαγραφές του Δικτύου βασίζονται στην τεχνολογία και μεθοδολογία διαδικτύωσης που έχει αναπτυχθεί στα πλαίσια της πλατιάς εξάπλωσης του Διαδικτύου σε όλο τον κόσμο και στηρίζεται στην οικογένεια πρωτοκόλλων Internet, γνωστή ως TCP/IP.

Ο σχεδιασμός του ολοκληρωμένου δικτύου σχολικών εργαστηρίων που έχει δημιουργηθεί έχει ιεραρχική δομή (Εικόνα 2-1) που αποτελείται από:



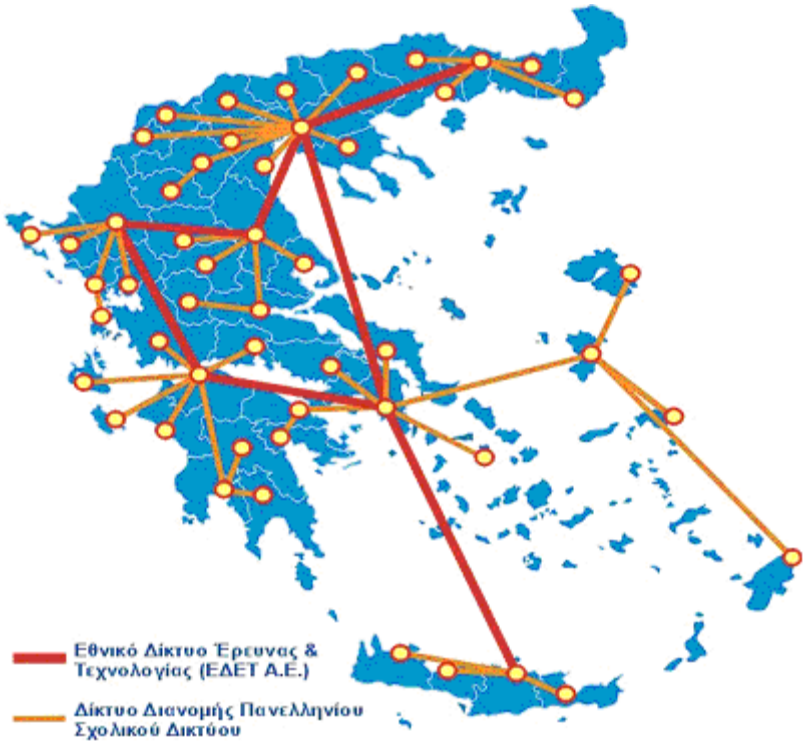
Εικόνα 2-1. Η ιεραρχική δομή του Πανελληνίου Σχολικού Δικτύου.

- Το **δίκτυο κορμού**, το οποίο είναι το Εθνικό Δίκτυο Έρευνας-Τεχνολογίας ΕΔΕΤ.
- Το **δίκτυο διανομής**, περιλαμβάνει τους νομαρχιακούς κόμβους και υλοποιείται από τα έργα **«Ασκοί του Αιόλου»** και
- Το **δίκτυο πρόσβασης** στα **σχολικά εργαστήρια** και τις Διευθύνσεις Δευτεροβάθμιας Εκπαίδευσης.

2.2.2. Δίκτυο κορμού

Το Πανελλήνιο Σχολικό Δίκτυο δεν αναπτύσσει δικό του δίκτυο κορμού, αλλά χρησιμοποιεί το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας ΕΔΕΤ.

Το Πανελλήνιο Σχολικό Δίκτυο διασυνδέεται με το ΕΔΕΤ σε επτά κύρια σημεία (Αθήνα, Θεσσαλονίκη, Πάτρα, Ηράκλειο, Λάρισα, Ιωάννινα και Ξάνθη) (Εικόνα 2-2).



Εικόνα 2-2. Σημεία διασύνδεσης του Πανελληνίου Σχολικού Δικτύου με το ΕΔΕΤ.

2.2.3. Δίκτυο διανομής

Το δίκτυο διανομής εξασφαλίζει την ολοκληρωμένη διασύνδεση των σχολικών και διοικητικών μονάδων με το δίκτυο κορμού. Διακρίνεται σε δύο επίπεδα:

- **Πρώτο επίπεδο,** το οποίο απαρτίζεται από 9 ευρύτερες γεωγραφικές περιοχές και αντιπροσωπεύουν τους κύριους κόμβους του δικτύου διανομής.
- **Δεύτερο επίπεδο,** το οποίο απαρτίζεται από 51 μικρότερες γεωγραφικές περιοχές (αντιστοιχούν στους νομούς της χώρας) και αντιπροσωπεύουν τους δευτερεύοντες κόμβους του δικτύου διανομής.

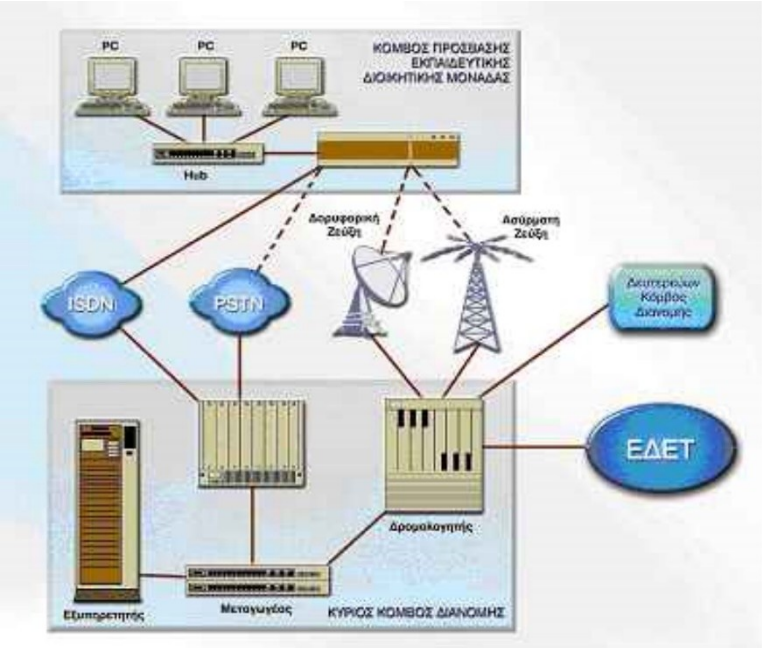
Στο κεντρικό κτίριο του ΟΤΕ στην πρωτεύουσα κάθε νομού εγκαθίσταται δικτυακός και υπολογιστικός εξοπλισμός με σκοπό τη βέλτιστη από τεχνικής και οικονομικής σκοπιάς, πρόσβαση των σχολείων του νομού στο δίκτυο και την παροχή των δικτυακών υπηρεσιών.

2.2.4. Δίκτυο πρόσβασης

Το δίκτυο πρόσβασης διασυνδέει άμεσα και με τις κατάλληλες τηλεπικοινωνιακές ζεύξεις τις σχολικές και διοικητικές μονάδες ενός νομού στον οικείο νομαρχιακό κόμβο (Εικόνα 2-3). Εναλλακτικά και ανάλογα με συγκεκριμένα τεχνικά και οικονομικά χαρακτηριστικά

επιλέγεται ο βέλτιστος τρόπος διασύνδεσης ανάμεσα σε:

- Ψηφιακό κύκλωμα ISDN
- Μισθωμένο αναλογικό κύκλωμα
- Απλό επιλεγόμενο αναλογικό κύκλωμα
- Ασύρματη ζεύξη (πιλοτική εφαρμογή)
- Δορυφορική ζεύξη (πιλοτική εφαρμογή - προσεχώς)



Εικόνα 2-3. Το δίκτυο πρόσβασης του ΠΣΔ.

2.3. Παρεχόμενες Υπηρεσίες

Σήμερα είναι σε χρήση και παρέχονται και υποστηρίζονται κανονικά από τις δομές του σχολικού δικτύου οι παρακάτω δικτυακές υπηρεσίες:

1. **Διαχείριση Χρηστών** (https://register.sch.gr/)
2. **Απομακρυσμένη Σύνδεση στο δίκτυο (dialup)**
3. **Ηλεκτρονικό Ταχυδρομείο (e-mail)** (https://webmail.sch.gr/)
4. **Ηλεκτρονικές Λίστες Επικοινωνίας** (mail lists)
5. **Δικτυακός Τόπος του Πανελληνίου Σχολικού Δικτύου** (https://www.sch.gr/).
6. **Υπηρεσία Διακομιστή Μεσολάβησης (proxy)**
7. **Φιλοξενία Ιστοσελίδων (web hosting)**
8. **Αυτόματη Δημιουργία**
9. **Ασύγχρονη Τηλε-εκπαίδευση** (http://e-learning.sch.gr/)
10. **Τηλεδιάσκεψη** (teleconference) (https://meeting.sch.gr/).

11. **Βίντεο κατ' Απαίτηση** (Video On Demand) (https://video.sch.gr/)

12. **Ζωντανές μεταδόσεις** εκδηλώσεων μέσω διαδικτύου (webcasting) (https://video.sch.gr/live).

13. **Χώροι Ανακοινώσεων** (https://www.sch.gr/news) και **Συζητήσεων** (https://www.sch.gr/forums).

14. **Ηλεκτρονικά περιοδικά** (https://schoolpress.sch.gr/)

15. **Προσωπικό Ημερολόγιο** (Calendar), **Προσωπικό Βιβλίο Διευθύνσεων** (Address Book) και **Λίστα Εργασιών & Σημειώσεων** (to do list και notes)

16. **Υπηρεσία Καταλόγου** (Directory Service)

17. **Σύστημα GIS**.

18. **Τηλεφωνία μέσω Δικτύου Δεδομένων** (Voice Over IP)

19. **Online Στατιστικά Στοιχεία** της χρήσης του δικτύου (https://analytics.sch.gr)

20. **Υποστήριξη Χρηστών** (Help-Desk) (https://helpdesk.sch.gr)

2.4. ΠΣΔ και Ευρυζωνικότητα

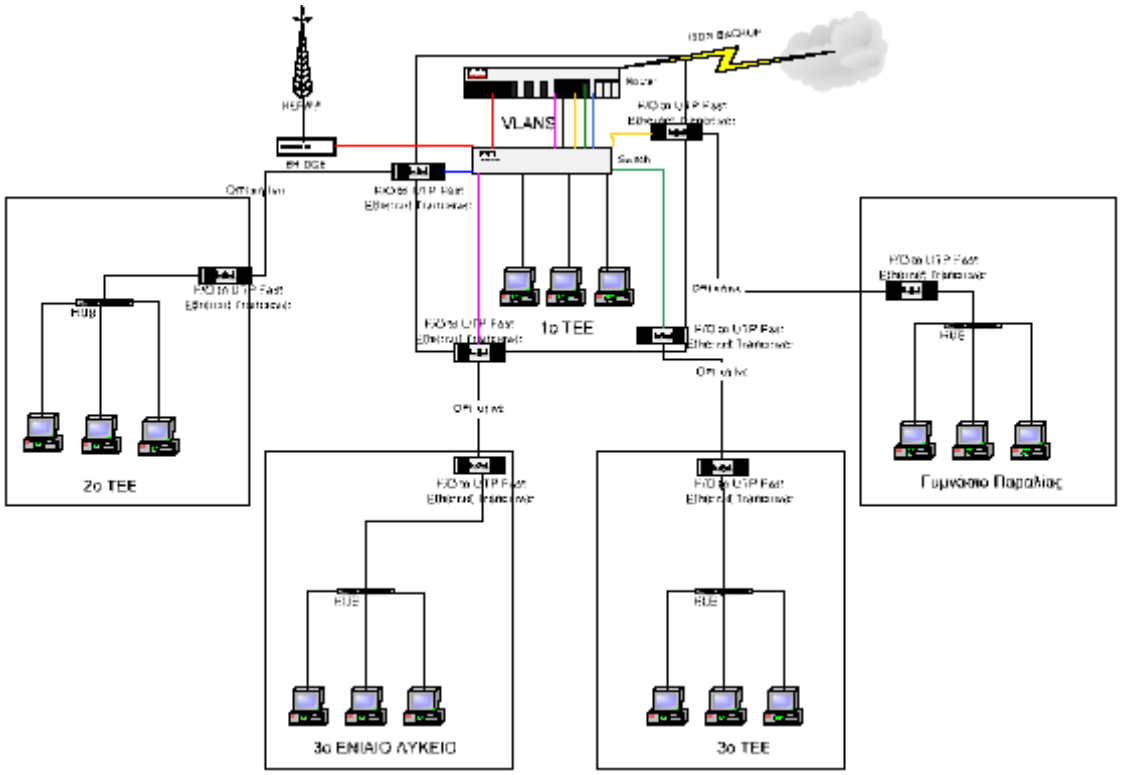
Για την επίτευξη των στόχων του e-Europe 2005[1] σχετικά με την απόκτηση ευρυζωνικών συνδέσεων σε όλα τα σχολεία, το ΠΣΔ [11] προχωρά στην αναβάθμιση του δικτύου πρόσβασης με την εγκατάσταση ευρυζωνικών συνδέσεων (500 συνδέσεις ADSL ταχύτητας 384/128 kbps σε πρώτη φάση και περισσότερες από 250 ασύρματες ζεύξεις υψηλής ταχύτητας 10 Mbps).

Σε ό,τι αφορά τα ασύρματα δίκτυα κατασκευάστηκαν και λειτουργούν 13 ασύρματες δικτυακές νησίδες στις εξής πόλεις: Αθήνα (3 νησίδες) Θεσσαλονίκη (2 νησίδες), Καλαμάτα, Σύρος, Βόλος, Ξάνθη, Κιλκίς, Ιωάννινα, Ρέθυμνο και Χανιά.

Μια τυπική περίπτωση νησίδας σχολείων που μεταξύ του διασυνδέονται με οπτικές υποδομές και χρησιμοποιούν μια κοινή ασύρματη σύνδεση στο Διαδίκτυο φαίνεται στην Εικόνα 2-4.

Σύμφωνα με τη σχεδίαση του δικτύου και τις ζητούμενες τεχνικές προδιαγραφές, τα έργα ασύρματων συνδέσεων συνδέουν το μεγαλύτερο μέρος των σχολικών μονάδων του ΠΣΔ που βρίσκονται σε μια δεδομένη πόλη με ασύρματες ζεύξεις. Συγκεκριμένα, με βάση τις δυνατότητες κάλυψης, έχουν επιλεγεί τα σχολεία που έχουν κατάλληλη γεωγραφική θέση, τα οποία μπορεί να είναι οργανωμένα σε νησίδες. Η κάθε νησίδα περιλαμβάνει έναν αριθμό σχολείων (συνήθως 3-4) τα οποία θα συνδέονται μεταξύ τους με δίκτυο υψηλών ταχυτήτων (διασύνδεση οπτικών ινών). Σε ένα από τα σχολεία της κάθε νησίδας έχει τοποθετηθεί μία κατευθυντική κεραία χαμηλής ισχύος εκπομπής, μέσω της οποίας συνδέεται η νησίδα σχολείων με το κεντρικό σύστημα. Το κεντρικό σύστημα αποτελείται από μία έως δυο κεραίες ευρείας περιοχής σε σημείο που θα υπάρχει οπτική επαφή (Line-Of-Sight).

[1] https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:l24226&from=EL



Εικόνα 2-4. Οπτικά διασυνδεδεμένη νησίδα σχολείων που χρησιμοποιεί κοινή ασύρματη πρόσβαση στο Διαδίκτυο (Πόλη: Καλαμάτα).

Πλεονεκτήματα

Παρατηρείται δυναμική αύξηση της ταχύτητας και της ποιότητας επικοινωνίας των σχολικών μονάδων μεταξύ τους, αλλά και με το Διαδίκτυο. Συγκεκριμένα, τα σχολεία εντός μιας νησίδας θα μπορούν να επικοινωνούν με ταχύτητες της τάξης των 100 Mbps, δίνοντας την δυνατότητα στους μαθητές και στους εκπαιδευτικούς να χρησιμοποιήσουν υπηρεσίες όπως τηλεδιάσκεψη, εφαρμογές πολυμέσων, βίντεο κατ' απαίτηση κ.λπ.

Ειδικά στη σύνδεση των σχολείων με το Διαδίκτυο, θα μπορούν να επιτυγχάνονται ταχύτητες έως και 10 Mbps. Ακόμα και στην περίπτωση όπου το πλήθος των σχολείων ταυτόχρονα επικοινωνεί στο ασύρματο δίκτυο, η σύνδεση τους θα είναι κατά πολύ υψηλότερη από τις τωρινές τους ταχύτητες, οι οποίες και περιορίζονται στα 128 Kbps.

Τέλος, θα υπάρξει σημαντική εξοικονόμηση τηλεπικοινωνιακών τελών, δεδομένου ότι τα κάθε σχολείο σήμερα χρησιμοποιεί δική του γραμμή για σύνδεση στο Διαδίκτυο.

Ασφαλής λειτουργία

Η ασύρματη επικοινωνία γίνεται με τέτοιο τρόπο ώστε να μην ενέχει απολύτως κανένα κίνδυνο για την υγεία των μαθητών και εκπαιδευτικών. Αυτό επιτυγχάνεται λόγω της εκπομπής στο συγκεκριμένο φάσμα συχνοτήτων της μικρής ισχύος εκπομπής και της κατευθυντικότητας των κεραιών στα σχολεία. Επίσης, λόγω του μικρού μεγέθους των κεραιών δεν αλλοιώνεται και η εικόνα του περιβάλλοντος χώρου. Αξίζει να σημειωθεί ότι η πρακτική δημιουργίας ασυρμάτων δικτύων με παρόμοιες προδιαγραφές έχει μεγάλη απήχηση στην Ελλάδα και στο εξωτερικό, χωρίς κανένα πρόβλημα για τους κατοίκους των περιοχών κάλυψης. Σε καμία περίπτωση δεν μπορούν να παραλληλιστούν με κεραίες κινητής τηλεφωνίας, οι οποίες είναι σαφώς πολύ υψηλότερης ισχύος εκπομπής και λειτουργούν σε διαφορετικές συχνότητες.

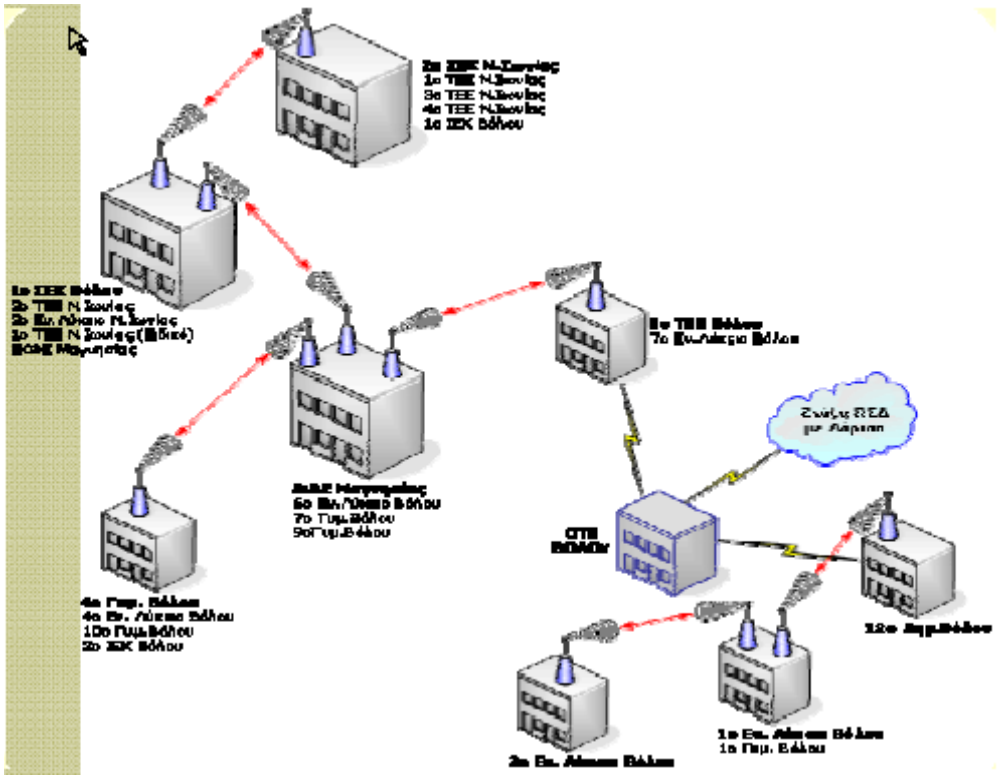
Ευρυζωνικές υπηρεσίες πάνω από το Local Loop

Μια άλλη δράση του Πανελλήνιου Σχολικού Δικτύου στην κατεύθυνση της εισαγωγής των ευρυζωνικών τεχνολογιών πρόσβασης στο δίκτυό του είναι η εφαρμογή της τεχνολογίας VDSL (Very high speed Digital Subscriber Line) σε επιλεγμένους κόμβους του.

Η τεχνολογία VDSL κάνει χρήση του συνδρομητικού χάλκινου βρόχου και εφαρμόζοντας προηγμένες τεχνικές διαμόρφωσης του σήματος καταφέρνει να πετύχει ταχύτητες πρόσβασης έως και 12 Mbps. Η εφαρμογή της έδωσε τη δυνατότητα διασύνδεσης σχολείων που βρίσκονται σε απόσταση έως και 1,5 χλμ. από τον κόμβο του δικτύου σε υψηλές ταχύτητες με τη χρήση μιας απλής μισθωμένης γραμμής.

Οι κόμβοι του δικτύου στους οποίους έχει εγκατασταθεί VDSL συγκεντρωτής είναι Αγρίνιο, Πάτρα, Σπάρτη, Τρίπολη, Βόλος, Ηράκλειο, Αθήνα, Θεσσαλονίκη, Ιωάννινα, Λάρισα και Σύρος. Η συγκεκριμένη δράση είναι ακόμη σε εξέλιξη με την έννοια πως ενώ έχει εγκατασταθεί η υποδομή στον κόμβο του Δικτύου Διανομής, οι φορείς του Σχολικού Δικτύου έχουν αναλάβει να εντοπίσουν τα σχολεία τα οποία πληρούν τα κριτήρια (απόσταση από τον κόμβο, καλή ποιότητα μισθωμένης γραμμής) για να χρησιμοποιήσουν τη συγκεκριμένη τεχνολογία πρόσβασης. Μέχρι στιγμής ο αριθμός των μονάδων που έχουν συνδεθεί με τον τρόπο αυτό είναι ακόμη μικρός (~15).

Στην Εικόνα 2-5 φαίνεται το διάγραμμα του ασύρματου δικτύου που έχει αναπτυχθεί στην πόλη του Βόλου. Το σύνολο των σχολείων που συμμετέχουν σε αυτό είναι 24. Το δίκτυο έχει δύο ευρυζωνικές εξόδους προς το Διαδίκτυο τεχνολογίας VDSL και ταχύτητας 10 Mbps η καθεμιά. Με τον τρόπο αυτό αναβαθμίζεται συνολικά η χωρητικότητα πρόσβασης των σχολείων με παράλληλη μείωση των τηλεπικοινωνιακών κυκλωμάτων που χρησιμοποιούνται. Συγκεκριμένα, το έργο «αντικατέστησε» 24 κυκλώματα πρόσβασης ISDN και Leased Line, τα οποία είχαν μέγιστη ταχύτητα 128 Kbps.



Εικόνα 2-5. Λογικό διάγραμμα ασύρματου δικτύου Βόλου.

3. Θεωρητικό Μέρος: Ασύρματες τεχνολογίες διασύνδεσης

3.1. Πρότυπο IEEE 802.11

Το 802.11 είναι το πρότυπο για τα Ασύρματα Τοπικά Δίκτυα (WLANs) που αναπτύχθηκε από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE). Μπορεί να συγκριθεί με το πρότυπο 802.3 για τα ενσύρματα Ethernet LANs. Ο στόχος αυτού του προτύπου είναι να καθιερώσει έναν τρόπο λειτουργίας προκειμένου να επιλυθούν ζητήματα συμβατότητας μεταξύ κατασκευαστών εξοπλισμού WLAN. Έτσι, η επιτροπή προτύπων IEEE 802.11 πρότεινε μια έκδοση ενός Υποεπιπέδου Ελέγχου Πρόσβασης στο Μέσο – Φυσικού Επιπέδου (Media Access Control – Physical Level, MAC-PHY).

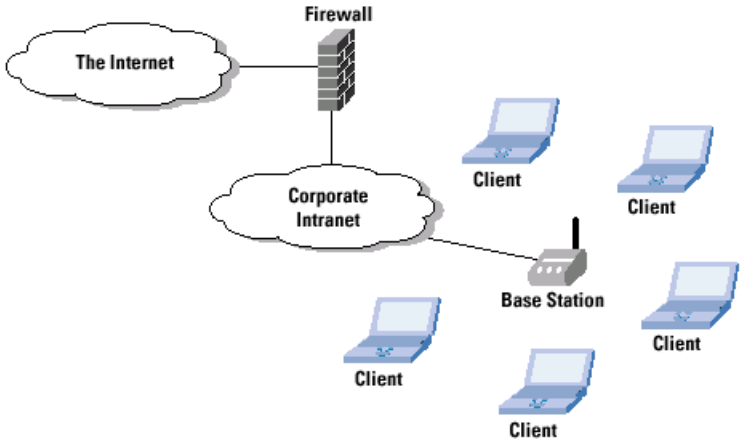
Το MAC κάτω από 802.11 αποτελείται από διάφορα λειτουργικά συγκροτήματα. Αυτά περιλαμβάνουν μηχανισμούς παροχής ελέγχου πρόσβασης με διενέξεις και χωρίς διενέξεις σε ποικίλα φυσικά επίπεδα. Οι λειτουργίες μέσα στο MAC είναι ανεξάρτητες από ρυθμούς μετάδοσης δεδομένων ή φυσικά χαρακτηριστικά.

Η θεμελιώδης μέθοδος προσπέλασης του 802.11 MAC είναι γνωστή ως πρωτόκολλο Πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance ή CSMA/CA). Το CSMA/CA εργάζεται με «σύστημα ακρόασης προ της ομιλίας». Αυτό σημαίνει ότι ένας σταθμός που επιθυμεί να μεταδώσει πρέπει πρώτα να «νιώσει» τον ασύρματο δίαυλο για να καθορίσει εάν ένας άλλος σταθμός μεταδίδει. Εάν το μέσο δεν είναι απασχολημένο, η μετάδοση μπορεί να προχωρήσει. Το σχήμα CSMA/CA εφαρμόζει ένα ελάχιστο χρονικό χάσμα μεταξύ πλαισίων από ένα δεδομένο χρήστη. Μόλις ένα πλαίσιο σταλεί από έναν εκπέμποντα σταθμό, αυτός ο σταθμός πρέπει να περιμένει ωσότου το χρονικό χάσμα παρέλθει για να δοκιμάσει να εκπέμψει πάλι. Μόλις περάσει ο χρόνος, ο σταθμός επιλέγει ένα τυχαίο χρονικό διάστημα (αποκαλούμενο διάστημα backoff) για να περιμένει πριν «ακροαστεί» πάλι για να βεβαιωθεί ότι είναι ελεύθερο το κανάλι στο οποίο προσπαθεί να εκπέμψει. Εάν το κανάλι είναι ακόμα απασχολημένο, επιλέγεται ένα άλλο διάστημα backoff που είναι μικρότερο από το πρώτο. Αυτή η διαδικασία επαναλαμβάνεται ωσότου ο αναμονής χρόνος πλησιάσει το μηδέν και ο σταθμός επιτρέπεται να εκπέμψει. Αυτός ο τύπος πολλαπλής πρόσβασης εξασφαλίζει δίκαιο καταμερισμό του καναλιού με αποφυγή των συγκρούσεων.

Αυτό το σχήμα επιτρέπει αυτόματο καταμερισμό του μέσου μεταξύ διάφορων συσκευών με συμβατά PHYs. Αυτή η μέθοδος προσπέλασης είναι ελκυστική επειδή παρέχει αποδοτικό φάσμα καθώς επίσης και ασύγχρονη μεταφορά δεδομένων. Τα σχήματα FDMA και CDMA δε θα ήταν επαρκή επειδή απαιτούν εύρος ζώνης που να χρησιμοποιείται από το σχήμα διαμόρφωσης. Καθαρό TDMA δε θα λειτουργούσε καλά επειδή απαιτεί συγχρονισμό. Κατά συνέπεια, το CSMA/CA, που μπορεί να θεωρηθεί ως εκδοχή του TDMA, ταιριάζει καλύτερα σ' αυτήν την εφαρμογή.

Το αρχικό πρότυπο 802.11 δημοσιεύτηκε από το IEEE (Institute of Electrical and Electronic Engineers) το 1997 και στόχος του ήταν να προδιαγράψει τεχνικά τη διασύνδεση σταθμών εργασίας με κάποιο «σταθμό βάσης» ο οποίος διαθέτει ενσύρματη σύνδεση με το υπάρχον τοπικό δίκτυο, ώστε να προκύψει ένα ασύρματο τοπικό δίκτυο (WLAN, Wireless LAN), όπως αυτό που φαίνεται στην Εικόνα 3-1. Στην εικόνα αυτή φαίνονται υπολογιστές οι οποίοι

συνδέονται με ένα σταθμό βάσης (Base Station), μέσω αυτού με το εταιρικό ενδοδίκτυο και μέσω αυτού με το Διαδίκτυο.



Εικόνα 3-1. Τυπική διαμόρφωση δικτύου IEEE 802.11 σε Infrastructure Mode.

Ο σταθμός βάσης με τη σειρά του εξασφαλίζει τη διασύνδεση με το υπάρχον δίκτυο δεδομένων (συνήθως ενσύρματο).

Το πρότυπο αυτό είναι γνωστό και ως IEEE 802.11-1997 και έχει ανανεωθεί φέροντας πλέον τον τίτλο IEEE 802.11-1999.

Παρότι, όπως προκύπτει από το παραπάνω σκεπτικό, το πρότυπο αυτό απευθύνεται σε ένα σαφώς περιορισμένο τύπο εφαρμογών, έμελλε να αποτελέσει την τεχνολογική βάση για την ανάπτυξη ενός πλήθους εφαρμογών ευρείας απήχησης και συγκεκριμένα της ευρυζωνικής πρόσβασης σε δημόσια δίκτυα. Στις ΗΠΑ η τεχνολογία αυτή είναι γνωστή ως BWA (Broadband Wireless Access).

Στις περιπτώσεις τέτοιων εφαρμογών οι σταθμοί εργασίας των χρηστών του δικτύου διασυνδέονται και πάλι με κάποιο σταθμό βάσης (ακριβώς όπως είχε αρχικά προβλεφθεί και όπως αναφέρθηκε παραπάνω), τον οποίο όμως (σταθμό βάσης) διαχειρίζεται και ελέγχει κάποιος πάροχος υπηρεσιών Διαδικτύου, ή κάποιος τηλεπικοινωνιακός φορέας, ενώ η τοπολογική έκταση του δικτύου είναι δυνατό να επεκτείνεται και σε εξωτερικούς χώρους, καλύπτοντας αποστάσεις αρκετών χιλιομέτρων.

Στο σημείο αυτό πρέπει να γίνει μία σαφής διάκριση στις δύο «τεχνοτροπίες» που αναφέρθηκαν παραπάνω.

Η περίπτωση των WLANs (Wireless LANs) έχει διαφορετικές ιδιότητες και απαιτεί διαφορετική μεταχείριση από την περίπτωση των δικτύων BWA. Εν κατακλείδι, η πρώτη περίπτωση αφορά κατά κύριο λόγο εγκαταστάσεις κλειστού χώρου, ενώ η δεύτερη εγκαταστάσεις ανοιχτού χώρου.

Το τρέχον πρότυπο έχει γίνει δεκτό ως αμερικανικό εθνικό πρότυπο από το American National Standards Institute (ANSI) και έχει υιοθετηθεί από τον International Organization for Standardization (ISO) ως ISO/IEC 8802-11:1999.

3.1.1. Υπο-πρότυπα του IEEE 802.11

Υπάρχουν αρκετές υπο-ομάδες στην ομάδα εργασίας του 802.11 που απασχολούνται με υπο-πρότυπα του 802.11, όπως:

- 802.11a: Παρέχει ρυθμό μετάδοσης έως 54 Mbps στη ζώνη των 5 GHz
- 802.11b: Παρέχει ρυθμό μετάδοσης έως 11 Mbps στη ζώνη των 2,4 GHz
- 802.11d: Πρόσθετοι Ρυθμιστικοί Τομείς (Additional Regulatory Domains)
- 802.11e: Ποιότητα υπηρεσιών (QoS)
- 802.11f: Inter-Access Point Protocol (IAPP)
- 802.11g: Υψηλότεροι ρυθμοί δεδομένων σε 2,4 GHz
- 802.11h: Δυναμική Επιλογή Καναλιού και Έλεγχος Ισχύος Εκπομπής
- 802.11i: Αυθεντικοποίηση και Ασφάλεια

3.1.2. DSSS και FHSS

Το PHY κάτω από 802.11 περιλαμβάνει διασπορά υπερύθρου (Diffused Infra-Red, DFIR – η χρησιμότητά του φαίνεται μέχρις στιγμής να είναι περιορισμένη), Διασπορά Φάσματος Άμεσης Ακολουθίας (Direct Sequence Spread Spectrum, DSSS) και Διασπορά Φάσματος με Αναπήδηση Συχνότητας (Frequency Hopped Spread Spectrum, FHSS). Και οι δύο τεχνικές διασποράς φάσματος χρησιμοποιούνται στη ζώνη των 2,4 GHz λόγω της ευρείας διαθεσιμότητας σε πολλές χώρες και των χαμηλότερων δαπανών υλικού σε σύγκριση με τις υψηλότερες μικροκυματικές συχνότητες.

Το αρχικό πρότυπο του 1997 όρισε ένα εύρος ζώνης 2 Mbps, με πτώση στο 1 Mbps σε περιβάλλον θορύβου χρησιμοποιώντας διαμόρφωση DSSS και εύρος ζώνης 1 Mbps χρησιμοποιώντας διαμόρφωση FHSS, με πιθανή λειτουργία στα 2 Mbps σε περιβάλλον στο οποίο υπάρχει απουσία θορύβου.

Το πρότυπο της IEEE υποστηρίζει το DSSS για χρήση με διαμόρφωση BPSK σε ρυθμό μετάδοσης δεδομένων 1 Mbps ή διαμόρφωση QPSK σε ρυθμό μετάδοσης 2 Mbps. Αυτό το γενικό σχέδιο ζωνών αποτελείται από πέντε υποζώνες που επικαλύπτουν 26 MHz και κεντροθετούνται στα 2,412, 2,427, 2,442, 2,457 και 2,470 GHz. Αυτό το σχήμα χρησιμοποιείται σε μία προσπάθεια να καταπολεμηθούν η παρεμβολή και η επιλεκτική εξασθένιση.

Το FHSS υποστηρίζεται από το 802.11 με διαμόρφωση GFSK και δύο σχέδια αναπήδησης με ρυθμούς μετάδοσης δεδομένων 1 Mbps και 2 Mbps. Σύμφωνα με αυτό το σχήμα, η ζώνη διαιρείται σε 79 υποζώνες με 1 MHz εύρος ζώνης η καθεμιά. Κάθε υποζώνη υπόκειται σε έναν ελάχιστο ρυθμό 2,5 hops/s χρησιμοποιώντας οποιοδήποτε από τρία πιθανά σχέδια αναπήδησης (22 αναπηδήσεις σε ένα δεδομένο σχέδιο). Ο ελάχιστος ρυθμός αναπήδησης εξασφαλίζει ότι κάθε πακέτο που στάλθηκε θα μπορούσε να διαβιβαστεί με μια απλή αναπήδηση έτσι ώστε οι πληροφορίες να μπορούν να ανακτηθούν σε μια άλλη αναπήδηση. Αυτό επιτρέπει μια αποτελεσματική ποικιλομορφία συχνοτήτων που παρέχει άριστα χαρακτηριστικά μετάδοσης.

Τα πρότυπα αυτά εμπλουτίστηκαν και οι τρέχουσες εκδόσεις τους, όπως επίσης και τα προϊόντα που κατασκευάστηκαν βάσει των προτύπων αυτών, ορίζουν ότι το DSSS μπορεί να λειτουργεί με εύρος ζώνης 1, 2, 5,5 ή 11 Mbps, ενώ το FHSS μπορεί να λειτουργεί με εύρος ζώνης 1, 2 ή 3 Mbps.

Και οι δύο μέθοδοι διαμόρφωσης λειτουργούν στη χρησιμοποιήσιμη άνευ αδείας ζώνη

των 2,4 GHz (2.400 – 2.483,5 MHz), που είναι περισσότερο γνωστή ως ISM (Industrial Scientific and Medical).

Οι τεχνολογίες DSSS και FHSS στηρίζονται στη διαμόρφωση διασποράς φάσματος (spread spectrum modulation), μία τεχνική η οποία έχει την προέλευσή της σε στρατιωτικούς ασυρμάτους. Στα σημαντικότερα πλεονεκτήματα των μεθόδων διαμόρφωσης που βασίζονται στη διασπορά φάσματος προσμετρώνται μεταξύ άλλων τα εξής:

- Αντοχή σε παρεμβολές από άλλες πηγές εκπομπής ραδιοσυχνοτήτων
- Ενσωματωμένοι μηχανισμοί ασφαλείας κατά τη μετάδοση δεδομένων
- Δυνατότητα ύπαρξης πολλαπλών συστημάτων (redundancy).

Η δυνατότητα συνύπαρξης πολλών συστημάτων που δεν παρεμβάλλουν μεταξύ τους αποτέλεσε την αιτία επιλογής αυτής της μεθόδου διαμόρφωσης για τα συστήματα που λειτουργούν στην αδέσμευτη ζώνη συχνοτήτων ISM, μιας και η ζώνη αυτή επιτρέπει σχεδόν σε οποιονδήποτε να χρησιμοποιεί τέτοιες συσκευές.

Από τις δύο τεχνολογίες, η τεχνολογία FHSS είναι πολύ ανθεκτική σε παρεμβολές, θορύβους, αντανακλάσεις και άλλους περιβαλλοντικούς παράγοντες και αυτοί οι λόγοι την καθιστούν καταλληλότερη για εφαρμογές από σημείο προς πολλά σημεία (point-to-multipoint) [13].

Σε αυτές τις περιπτώσεις όπου η χρήση κατευθυντικών κεραιών είναι αδύνατη, ενώ πρέπει να συνυπάρχουν πολλές συσκευές που εκπέμπουν στην ίδια συχνότητα έτσι ώστε να καλύπτονται περισσότερες περιοχές αλλά και να αυξάνεται το συνολικό παρεχόμενο εύρος ζώνης [4], **η χρήση συστημάτων FHSS είναι όχι μόνο προτεινόμενη αλλά και επιβεβλημένη**.

Όπως είναι σαφές οι περιπτώσεις δικτύων BWA (όπως για παράδειγμα το υπάρχον δίκτυο) ανήκουν στην κατηγορία αυτή.

3.1.3. Κεραίες

Οι κεραίες που χρησιμοποιούνται με τις συσκευές IEEE 802.11b μπορούν να ομαδοποιηθούν σε δύο κατηγορίες: πολυκατευθυντικές και κατευθυντικές ή από σημείο σε σημείο.

Προφανώς, οι πολυκατευθυντικές κεραίες είναι οι ευκολότερες να χρησιμοποιηθούν, επειδή δεν απαιτούν ακριβή ευθυγράμμιση της δέσμης ακτινοβολίας. Οι πολυκατευθυντικές κεραίες χρησιμοποιούνται στους περισσότερους σταθμούς βάσης, καθώς επίσης και στις περισσότερες κάρτες πρόσβασης. Εντούτοις, λόγω της φύσης τους, οι πολυκατευθυντικές κεραίες δε λειτουργούν καλά σε πολύ μεγάλες αποστάσεις, εκτός αν χρησιμοποιούνται με εξωτερικούς ενισχυτές· και αυτοί δεν είναι πάντα νόμιμοι ή κατάλληλοι για χρήση.

Οι κατευθυντικές ή από σημείο σε σημείο κεραίες, αφετέρου, απαιτούν προσεκτική και ακριβή ευθυγράμμιση και χρησιμοποιούνται υπαίθρια. Αν και το τυπικό εύρος για ένα πολυκατευθυντικό σύστημα κεραιών είναι 45 m, οι παραλλαγές με τις υψηλού κέρδους κατευθυντικές κεραίες μπορούν να λειτουργήσουν σε αποστάσεις μέχρι 40 km. Στις τοποθεσίες όπου επιτρέπονται οι ενισχυτές, η μέγιστη απόσταση μπορεί να αυξηθεί αρκετά και περιορίζεται μόνο από την ανάγκη άμεσης οπτικής επαφής.

3.2. Διαθέσιμες ζώνες συχνοτήτων για διασύνδεση δικτύων δεδομένων

Ο οργανισμός ETSI (European Telecommunications Standards Institute) στο πρότυπο υπ' αριθμόν 300-328 προδιαγράφει κάποιες ζώνες συχνοτήτων για τις οποίες δεν απαιτείται άδεια λειτουργίας (ISM – Industrial Scientific Medical) [13].

Προφανώς, οι διατάξεις του παραπάνω κανονισμού έχουν νόημα μόνο για τις ευρωπαϊκές χώρες.

Οι ασύρματες συσκευές που μπορούν να χρησιμοποιηθούν στο παρόν έργο θα πρέπει να λειτουργούν σε κάποιες από αυτές τις συχνότητες, μιας και το ελληνικό κανονιστικό πλαίσιο οφείλει να εναρμονίζεται σε σχέση με το αντίστοιχο ευρωπαϊκό, που στην προκειμένη περίπτωση είναι το ETSI.

Συγκεκριμένα, σύμφωνα με το παραπάνω πρότυπο, οι σχετικές ISM ζώνες συχνοτήτων που παρουσιάζουν ενδιαφέρον για την Ευρώπη είναι:

- 2,400 – 2,500 GHz
- 5,725 – 5,875 GHz Οι συσκευές που υποστηρίζουν το πρότυπο IEEE 802.11b λειτουργούν στη ζώνη συχνοτήτων 2,4000 – 2,4835 GHz.

Οι συσκευές που υποστηρίζουν το πρότυπο IEEE 802.11a λειτουργούν στη ζώνη συχνοτήτων 5 GHz UNII (Unlicensed National Information Infrastructure). Αυτή έχει καθορισθεί από τον οργανισμό FCC (Federal Communications Commission), ο οποίος έχει στις ΗΠΑ αντίστοιχο ρόλο με αυτόν που έχει ο οργανισμός ETSI στην Ευρώπη, και χωρίζεται σε τρεις μικρότερες ζώνες:

- UNII-1: 5,15 – 5,25 GHz
- UNII-2: 5,25 – 5,35 GHz
- UNII-3: 5,725 – 5,825 GHz

Οι δύο πρώτες, όμως, χρησιμοποιούνται στην Ευρώπη από τα συστήματα HiperLAN/1 και HiperLAN/2. Γι' αυτόν τον λόγο δεν έχει προχωρήσει η πιστοποίηση του 802.11a στην Ευρώπη. Στα πλαίσια της προσπάθειας να διορθωθεί αυτή η κατάσταση, έχουν προταθεί δύο προσθήκες στο πρότυπο 802.11a ώστε να είναι δυνατή η συνύπαρξη συστημάτων 802.11a και HiperLAN/2 (DCS – Dynamic Channel Selection, TPC – Transmit Power Control).

Η ζώνη συχνοτήτων 2,4000 – 2,4835 GHz μπορεί να χρησιμοποιηθεί στην Ελλάδα χωρίς άδεια από την ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων). Ωστόσο, δεν υπάρχει νομοθεσία που να αφορά το θέμα της χρήσης των ζωνών συχνοτήτων 5,15 – 5,35 GHz και 5,725 – 5,825 GHz **αν και αναμένεται να γίνει κάτι τέτοιο στο μέλλον**.

Συμπερασματικά, σύμφωνα με το άρθρο 5 της απόφασης 254/72 της ΕΕΤΤ, που περιέχεται στο ΦΕΚ Β΄ 895/16-07-2002, στην Ελλάδα επιτρέπεται ουσιαστικά η χρήση μόνο της ISM ζώνης 2.400-2.483,5 MHz.

3.3. Τεχνικές και πρωτόκολλα για βελτιστοποίηση απόδοσης του TCP σε ασύρματα δίκτυα

Στο μέρος αυτό της εργασίας θα γίνει μία σύντομη αναφορά σε τεχνικές και πρωτόκολλα τα οποία έχουν αναπτυχθεί για να βελτιστοποιήσουν την απόδοση του TCP σε ασύρματα

δίκτυα. Θα αναλυθούν τα αίτια ύπαρξης αυτών των πρωτοκόλλων, καθώς και η φιλοσοφία με την οποία επιχειρούν να άρουν τα προβλήματα του TCP σε ασύρματα δίκτυα [10]. Τέλος, θα αναλυθεί εις βάθος ένα από αυτά τα πρωτόκολλα, το Snoop, το οποίο βρέθηκε να έχει τα καλύτερα αποτελέσματα καθώς είναι και το πρωτόκολλο με το οποίο έκανε συγκριτικές μετρήσεις η ομάδα και το οποίο χρησιμοποιήθηκε για τη βελτίωση της αποδοτικότητας του δικτύου. Θα παρατεθούν κάποια εισαγωγικά στοιχεία που θα εξηγούν την προσέγγιση του συγκεκριμένου πρωτοκόλλου και στη συνέχεια θα γίνει μία αναφορά στον τρόπο λειτουργίας του και στον τρόπο που υλοποιήθηκε στο συγκεκριμένο δίκτυο.

3.3.1. Εισαγωγή

Δεν υπάρχει αμφιβολία ότι το πρωτόκολλο TCP είναι από τα πιο διαδεδομένα στις σύγχρονες τηλεπικοινωνίες. Η συντριπτική πλειοψηφία των υλοποιημένων δικτύων, τόσο ασύρματων όσο και ενσύρματων, βασίζεται σ' αυτό. Είναι παράλληλα όμως αλήθεια ότι το συγκεκριμένο πρωτόκολλο αναπτύχθηκε με κύριο γνώμονα τα ενσύρματα δίκτυα με αποτέλεσμα να παρουσιάζει βελτιστοποιημένη απόδοση σε αυτά, ενώ αντίθετα να έχει αισθητά μικρότερη απόδοση σε δίκτυα με διαφοροποιημένα χαρακτηριστικά, όπως τα ασύρματα [1].

Συγκεκριμένα, το πρωτόκολλο έχει πολύ καλή απόδοση σε δίκτυα με σχετικά μικρές απώλειες πακέτων (όπως είναι η πλειοψηφία των ενσύρματων) με το να προσαρμόζεται γρήγορα και εύκολα σε καθυστερήσεις και απώλειες πακέτων. Το επιτυγχάνει αυτό με το να κρατά έναν μέσο όρο του χρονικού διαστήματος που είναι απαραίτητο για την αποστολή και επιστροφή πακέτων (round-trip delay), καθώς και μιας μέσης απόκλισης (mean deviation). Το πρωτόκολλο ξαναστέλνει όποια πακέτα δεν έχουν ληφθεί εντός ενός χρονικού περιθωρίου ίσου με τέσσερις φορές τη μέση απόκλιση από τον μέσο όρο, με αποτέλεσμα να καταφέρνει έτσι να διατηρεί μία υψηλή συνολική αξιοπιστία και απόδοση στο δίκτυο. Λόγω ακριβώς του γεγονότος ότι στα ενσύρματα δίκτυα οι απώλειες είναι μικρές και οι οποιεσδήποτε καθυστερήσεις προκαλούνται κυρίως από φαινόμενα συμφόρησης (congestion)του δικτύου, το πρωτόκολλο σωστά αντιδρά στις καθυστερήσεις ενεργοποιώντας μηχανισμούς αποσυμφόρησης.

Σε περιβάλλοντα όμως όπου υπάρχουν πολλά σφάλματα και σημαντικές απώλειες (όπως στην πλειοψηφία των ασυρμάτων δικτύων, λόγω ασυνεχών συνδέσεων, καιρικών συνθηκών και αλλαγών κυψέλης – handoffs) το πρωτόκολλο αντιδρά σε απώλειες πακέτων όπως θα αντιδρούσε σε ενσύρματα δίκτυα θεωρώντας ότι οφείλονται σε συμφόρηση. Για να αντιμετωπίσει τις απώλειες αυτές, μειώνει το μέγεθος του παραθύρου αποστολής (transmission windows size) πριν επανεκπέμψει τα πακέτα και ενεργοποιεί άλλους μηχανισμούς ελέγχου συμφόρησης. Ως αποτέλεσμα, μειώνεται σημαντικά και μη αποτελεσματικά η απόδοση του ασύρματου δικτύου [3]. Τη συμπεριφορά αυτή του TCP φιλοδοξούν να αντιμετωπίσουν συγκεκριμένες τεχνικές και πρωτόκολλα.

Οι προσεγγίσεις που ακολουθούν γενικά αυτά τα πρωτόκολλα είναι δύο. Η πρώτη έχει ως σκοπό να κρύψει τελείως από τον πομπού το ασύρματο μέρος της σύνδεσης. Η φιλοσοφία πίσω από την προσέγγιση αυτή είναι ότι εφόσον το πρόβλημα είναι τοπικό (δηλαδή, μόνο στην ασύρματη επικοινωνία) θα πρέπει να λυθεί τοπικά. Το κέρδος που υπάρχει με αυτή την προσέγγιση είναι ότι δεν υπάρχει η ανάγκη για οποιαδήποτε αλλαγή στον τρόπο λειτουργίας του πομπού, καθώς δεν αντιλαμβάνεται οποιαδήποτε διαφοροποίηση στον τρόπο επικοινωνίας του με τους απομακρυσμένους χρήστες. Τέτοιου είδους πρωτόκολλα είναι τα split-connection και τα link-layer.

Η δεύτερη προσέγγιση επιχειρεί να κάνει τον πομπό να αναγνωρίσει ότι μέρος της

καναλιού επικοινωνίας με τους απομακρυσμένους χρήστες είναι ασύρματο και ότι μέρος των πακέτων χάνονται για λόγους πέρα από συμφόρηση δικτύου. Ο πομπός έτσι μπορεί να αποφύγει να ενεργοποιεί μηχανισμούς αποσυμφόρησης τους δικτύου όταν συμβαίνουν απώλειες που δεν οφείλονται σε αυξημένη κίνηση. Το μειονέκτημα με αυτή την προσέγγιση είναι ότι απαιτούνται αλλαγές στον τρόπο δρομολόγησης πακέτων από την μεριά του πομπού. Τέτοιου είδους πρωτόκολλα είναι τα end-to-end.

3.3.2. End-to-end πρωτόκολλα

Τα πρωτόκολλα end-to-end βασίζουν τη λειτουργία τους πάνω σε δύο τεχνικές. Πρώτον, χρησιμοποιούν επιλεκτικές αναγνωρίσεις (selective acknowledgements – SACKS) ώστε να επιτρέψουν στον πομπό να αντιμετωπίσει διαδοχικές απώλειες πακέτων χωρίς να καταφύγει σε μείωση του παράθυρου αποστολής. Παράλληλα, επιχειρούν να διαχωρίσουν τις απώλειες που λαμβάνουν χώρα στο δίκτυο, σε αυτές που προκαλούνται από συμφόρηση και σε αυτές που προκαλούνται από άλλους λόγους, κάνοντας χρήση ενός ειδικευμένου μηχανισμού ειδοποίησης (explicit loss notification mechanism – ELN).

3.3.3. Split-connection πρωτόκολλα

Τα πρωτόκολλα αυτά, αντιμετωπίζουν τις απώλειες με ένα εντελώς διαφορετικό τρόπο. Συγκεκριμένα, επιχειρούν να αποκρύψουν τελείως από τον πομπό την ύπαρξη του ασύρματου δικτύου, τερματίζοντας την TCP σύνδεση στη βάση (base station) και στη συνέχεια μεταφέροντας τα πακέτα μέσω μιας ξεχωριστής, πιο αξιόπιστης ασύρματης σύνδεσης ανάμεσα στην βάση και στον απομακρυσμένο χρήστη. Θεωρούν δηλαδή ότι το πρόβλημα είναι καθαρά τοπικό, στην ασύρματη σύνδεση και το αντιμετωπίζουν σαν τοπικό. Οι τεχνικές αυτές χρησιμοποιούν ποίκιλλες τεχνικές, όπως αρνητικές ή επιλεκτικές αναγνωρίσεις (selective – negative acknowledgements) για να επιτύχουν τη βελτιστοποίηση της μεταφοράς δεδομένων πάνω από την ασύρματη σύνδεση. Ένα τέτοιο πρωτόκολλο είναι το Indirect-TCP. Το συγκεκριμένο πρωτόκολλο χρησιμοποιεί το κλασικό TCP πρωτόκολλο για το ασύρματο μέρος της επικοινωνίας με μερικές τροποποιήσεις, με αποτέλεσμα ενώ έχει μία μικρή βελτίωση στη συμπεριφορά, να παρουσιάζει πολλά προβλήματα, κυρίως όσον αφορά φαινόμενα handoffs τα οποία γίνονται ιδιαίτερα αργά και με πολύπλοκο τρόπο.

3.3.4. Link-layer πρωτόκολλα

Η τρίτη αυτή προσέγγιση επιχειρεί να κρύψει πλήρως από τον πομπό τις απώλειες που οφείλονται στο ασύρματο μέρος της επικοινωνίας κάνοντας χρήση τοπικών επανεκπομπών των χαμένων πακέτων από τη βάση προς τον αποδέκτη χωρίς την ενημέρωση του πομπού. Οι επανεκπομπές αυτές γίνονται με τεχνικές κατάλληλα επιλεγμένες για τα συγκεκριμένα χαρακτηριστικά της ασύρματης σύνδεσης, ώστε να επιτυγχάνεται βελτίωση στην απόδοση. Το μειονέκτημα με αυτή την προσέγγιση είναι ότι ο πομπός δεν είναι πλήρως προστατευμένος από τις απώλειες πακέτων που συμβαίνουν στο ασύρματο μέρος της επικοινωνίας, καθώς αν οι απώλειες είναι μεγάλες και οι καθυστερήσεις επιστροφής των επιβεβαιώσεων (acknowledgements) υπερβούν κάποιο όριο, τότε αναπόφευκτα ο πομπός θα λάβει μέτρα αποσυμφόρησης του δικτύου, πράγμα που θα οδηγήσει σε μείωση της απόδοσης του, όπως προαναφέρθηκε. Τέτοιου είδους πρωτόκολλα είναι το CDMA και TDMA, που χρησιμοποιούνται από τις εταιρίες παροχής κινητής τηλεφωνίας στις ΗΠΑ καθώς και το AIRMAIL, το Tulip [6] και το Snoop, που θα αναλυθεί εις βάθος στη συνέχεια.

3.4. Πρωτόκολλο Snoop

3.4.1. Αρχές Λειτουργίας

Το Snoop φυσικά δεν αναπτύχθηκε για να αντικαταστήσει το TCP σε ασύρματα δίκτυα, αλλά για να λειτουργεί παράλληλα με αυτό βελτιστοποιώντας τη συμπεριφορά του στο συγκεκριμένο περιβάλλον των ασυρμάτων δικτύων. Ο σχεδιασμός και η υλοποίηση του Snoop στοχεύουν ακριβώς στην αναίρεση της μείωσης της απόδοσης που λαμβάνει χώρα σε τέτοιου είδους περιβάλλοντα λόγω του φύσης τους TCP πρωτοκόλλου, χωρίς όμως να επεμβαίνει στο ίδιο το πρωτόκολλο στους απομακρυσμένους χρήστες του δικτύου (hosts) και χωρίς την ανάγκη επαναμεταγλώττισης (recompilation) των εφαρμογών. Σύμφωνα με την κατηγοριοποίηση που παρατέθηκε, το Snoop μπορεί να θεωρηθεί ως ένα πρωτόκολλο επιπέδου σύνδεσης (link layer) το οποίο εκμεταλλεύεται το ανώτερο TCP πρωτόκολλο, σε θέματα acknowledgements.

Εφόσον το TCP είναι ένα τόσο διαδεδομένο πρωτόκολλο θα ήταν άσκοπο και λανθασμένο να επιχειρηθεί μία εκ βάθρων αλλαγή του σε όλο το μήκος του δικτύου. Για τον λόγο αυτό, το Snoop λειτουργεί μονάχα με το να τροποποιεί το TCP στη βάση του ασύρματου δικτύου (base station), με το σκεπτικό ότι αυτός θα είναι ο μόνος κόμβος στον οποίο θα υπάρχει πλήρης έλεγχος, από μεριάς διαχειριστή δικτύου. Σε περιπτώσεις δύο σταθερών απομακρυσμένων ασύρματων βάσεων, το πρωτόκολλο δύναται να εγκατασταθεί και στις δύο βελτιώνοντας ακόμα περισσότερο τη συνολική απόδοση του ασύρματου δικτύου.

3.4.2. Μεθοδολογία υλοποίησης

Στον σταθμό λειτουργίας του ασύρματου δικτύου (base station), τροποποιείται ο κώδικας του δρομολογητή ώστε να αποθηκεύει σε μία προσωρινή μνήμη (cache) όλα τα δεδομένα τα οποία αποστέλλονται προς τον δέκτη. Παράλληλα, γίνονται μερικές αλλαγές στον τρόπο με τον οποίο το δίκτυο αντιμετωπίζει τις επανεκπομπές (retransmissions) δεδομένων και τις αποδείξεις παραλαβής (acknowledgments) ώστε αυτές να λαμβάνουν υπόψιν τις ιδιαιτερότητες του ασύρματου δικτύου [2].

Συγκεκριμένα, ο κώδικας του δρομολογητή τροποποιείται με την προσθήκη ενός υπό-επιπέδου, που ονομάζεται επίπεδο Snoop, το οποίο παρακολουθεί κάθε πακέτο δεδομένων που αποστέλλεται ή λαμβάνεται. Το επίπεδο αυτό κρατά στην προσωρινή μνήμη πακέτα για τα οποία δεν υπάρχει επιβεβαίωση ότι έχουν ληφθεί από τον αποδέκτη. Όταν ένα νέα πακέτο φτάνει από τον πομπό (transmitter) προς αποστολή, το Snoop το προσθέτει στη μνήμη και στη συνέχεια συνεχίζει κανονικά τη δρομολόγησή του. Το πρωτόκολλο επίσης παρακολουθεί όλες τις επιβεβαιώσεις που αποστέλλονται προς τη βάση. Όταν μία επιβεβαίωση για ένα πακέτο που υπάρχει στην cache ληφθεί, τότε το πρωτόκολλο το σβήνει από τη μνήμη, ενώ όταν ανιχνευτεί μία απώλεια πακέτου (που συμβαίνει όταν μία επιβεβαίωση δε φτάσει εντός ενός χρονικού περιθωρίου ή σταλούν διπλές επιβεβαιώσεις), το χαμένο πακέτο επανεκπέμπεται στον αποδέκτη, ενώ παράλληλα διαγράφεται η διπλή επιβεβαίωση.

Με τον τρόπο αυτό, αποκρύπτεται έμμεσα από την πηγή των πακέτων η αποτυχημένη αποστολή των πακέτων που στέλνει, με αποτέλεσμα να μην υπάρχει η ανάγκη για την ενεργοποίηση μηχανισμών ελέγχου συμφόρησης από το πρωτόκολλο TCP σε αυτή. Το αποτέλεσμα είναι η βελτιστοποίηση της απόδοσης του ασύρματου δικτύου, ενώ παράλληλα βελτιώνεται και η συνολική αξιοπιστία του δικτύου σε περιπτώσεις μεγάλων απωλειών πακέτων. Μια τυπική τοπολογία χρήσης του πρωτοκόλλου φαίνεται στην Εικόνα 3-2.

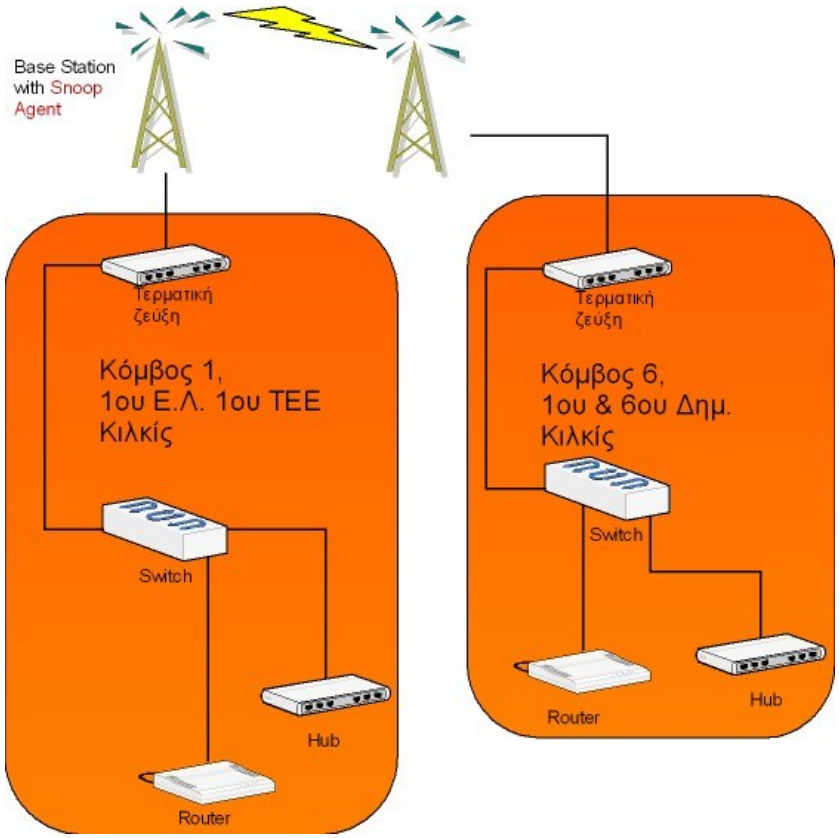
Εικόνα 3-2. Τρόπος λειτουργίας του Snoop.

3.4.3. Υλοποίηση του πρωτοκόλλου Snoop στο υπάρχον δίκτυο

Σύμφωνα με τις προδιαγραφές του πρωτοκόλλου Snoop, αλλαγές στο πρωτόκολλο TCP είναι απαραίτητες να γίνουν όχι σε όλο το εύρος του ασύρματου δικτύου, αλλά αποκλειστικά στη βάση του. Για τις ανάγκες των μετρήσεων που έκανε η ομάδα, κρίθηκε ότι το πρωτόκολλο θα μπορούσε να εγκατασταθεί στον κόμβο του 1ου ΤΕΕ Κιλκίς και στη συνέχεια θα μπορούσε η ομάδα να στείλει αιτήματα για δεδομένα από έναν άλλο κόμβο για να δοκιμάσει την απόδοση του δικτύου με και χωρίς το πρωτόκολλο. Για λόγους ευκολίας επιλέχθηκε ο κόμβος του 6ου Δημοτικού Σχολείου Κιλκίς, ο οποίος είναι σε κοντινή σχετικά απόσταση από τον προηγούμενο. Αν και το πρωτόκολλο παρουσιάζει βελτιστοποιημένη απόδοση σε συνθήκες όπου υπάρχουν μεγάλες απώλειες πακέτων, παρόλα αυτά δεν ήταν δυνατόν να βρεθεί καταλληλότερος (πιο απομακρυσμένος) κόμβος για τη διεξαγωγή των μετρήσεων στο χρονικό περιθώριο που ήταν διαθέσιμο.

Το Snoop αρχικά αναπτύχθηκε για το λειτουργικό OS/2 της IBM. Για τις ανάγκες του συγκεκριμένου δικτύου που είχε η ομάδα στη διάθεσή της, αναζητήθηκε στο Διαδίκτυο και βρέθηκε μία διανομή του πρωτοκόλλου για το λειτουργικό Linux. Έτσι, έγινε εγκατάσταση του λειτουργικού Linux, διανομή Red Hat, στον κόμβο του 1ου ΤΕΕ και στη συνέχεια στήθηκε ένας FTP και ένας HTTP διακομιστής με λογισμικό Apache. Όσον αφορά το πρωτόκολλο, έγινε χρήση της διανομής «Linux-Snoop», μιας υλοποίησης του Snoop για την πλατφόρμα Linux, πάνω στην οποία εγκαταστάθηκε το module του Snoop. Επίσης, το ίδιο λειτουργικό εγκαταστάθηκε και σε έναν υπολογιστή του κόμβου του 6ου Δημοτικού, ο οποίος λειτούργησε σαν πελάτης (client) για τις ανάγκες των μετρήσεων. Σχηματικά, το δίκτυο στο οποίο έγιναν οι μετρήσεις φαίνεται στην Εικόνα 3-3.

Για να λειτουργήσει το πρωτόκολλο είναι απαραίτητο να εισαχθεί στον πυρήνα (kernel) του λειτουργικού ώστε να έχει τη δυνατότητα να αλληλεπιδρά με τα εξερχόμενα/εισερχόμενα πακέτα. Για τις ανάγκες της εγκατάστασης είναι απαραίτητη η τροποποίηση δύο βασικών αρχείων του συστημάτων (ip_forward.c και netsyms.c) ώστε να συμπεριλάβουν το module και στη συνέχεια είναι απαραίτητη η επαναμεταγλώττιση του πυρήνα (kernel recompilation) ώστε να συμπεριληφθούν οι αλλαγές που έγιναν [7]. Έχοντας επιτυχώς επαναμεταγλωττίσει τον πυρήνα, δίνεται η δυνατότητα στον χρήστη αφενός μεν να λειτουργεί το δίκτυο με και χωρίς (load/unload) το πρωτόκολλο Snoop, καθώς και η δυνατότητα να το παραμετροποιεί σύμφωνα με τις ιδιαιτερότητες του δικτύου στο οποίο το εφαρμόζει. Έτσι, μπορεί να αλλάξει παραμέτρους όπως το μέγιστο μέγεθος του παραθύρου, ο μέγιστος αριθμός των συνδέσεων κ.λπ. Για τις μετρήσεις που λήφθηκαν χρησιμοποιήθηκαν οι προκαθορισμένες τιμές των παραμέτρων αυτών.



Εικόνα 3-3. Τμήμα του δικτύου στο οποίο έγιναν οι μετρήσεις με και χωρίς το πρωτόκολλο Snoop.

4. Περί Διαχείρισης δικτύου και Πρωτοκόλλων διαχείρισης (SNMP)

4.1. Εισαγωγή

Η ραγδαία εξέλιξη των δικτύων τα τελευταία χρόνια καθιστά τη συντήρησή τους από ανθρώπινο δυναμικό ασύμφορη και χρονοβόρα. Γι' αυτό σήμερα οι διάφοροι κατασκευαστές έχουν μεριμνήσει, ώστε το σύστημα να φροντίζει μόνο του για την καλή λειτουργία του, πράγμα που είναι πολύ πιο οικονομικό. Έτσι με τον όρο **διαχείριση δικτύου** εννοείται η διαδικασία του αυτόματου ελέγχου ενός οποιουδήποτε δικτύου υπολογιστών, με σκοπό την ελαχιστοποίηση του λειτουργικού κόστους συντήρησης του και τη μεγιστοποίηση της απόδοσης και της παραγωγικότητάς του [15].

Το μοντέλο που χρησιμοποιείται ευρύτατα στα δίκτυα υπολογιστών (Εικόνα 4-1) είναι της μορφής πελάτη-διακομιστή *(client-server)* και ονομάζεται στην ειδική αυτή περίπτωση **μοντέλο διαχειριστή – αντιπροσώπου** *(manager – agent model).* Αποτελείται από:

- τα διαχειριζόμενα **στοιχεία δικτύου** *(NE: Network Elements),* τα οποία διαχειρίζεται ο **διαχειριστής** *(manager)*,
- τους **αντιπροσώπους** *(agents)* και
- τη **βάση πληροφοριών διαχείρισης** του δικτύου *(MIB: Management Information Base).*

Εικόνα 4-1. Σύστημα διαχείρισης δικτύου.

Πιο αναλυτικά:

Ως διαχειριζόμενα στοιχεία δικτύου *(NE)* μπορούν να θεωρηθούν

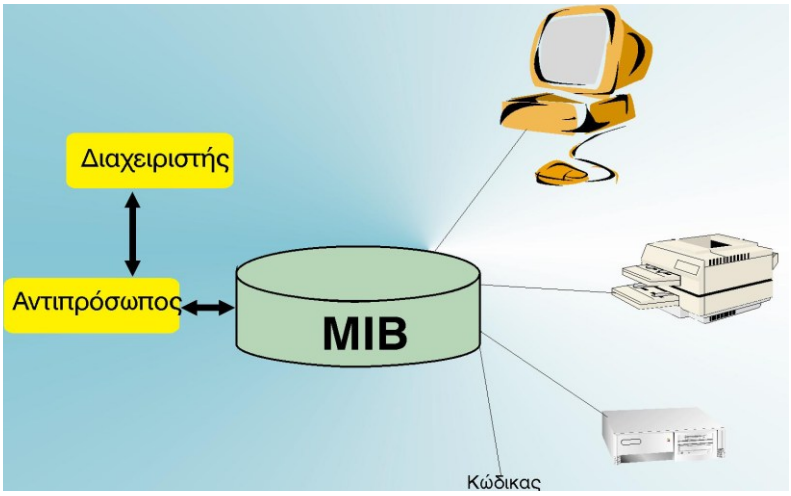
- οι σταθμοί εργασίας,
- οι δρομολογητές,
- οι γέφυρες,
- οι επαναλήπτες,
- τα μόντεμ και
- άλλες συσκευές τις οποίες μπορούμε να βρούμε σε ένα δίκτυο.

Ο διαχειριστής αναλαμβάνει τη διαχείριση του δικτύου μέσω πρωτοκόλλων επικοινωνίας, τα οποία μεταφέρουν πληροφορίες διαχείρισης προς και από τα *NE*. Τα πρωτόκολλα αυτά ονομάζονται **πρωτόκολλα διαχείρισης δικτύου** *(NMPs: Network Management Protocols)*.

Οι αντιπρόσωποι είναι το λογισμικό που συνήθως εγκαθίσταται στα *NE* και αναλαμβάνουν την αντιπροσώπευσή τους στο δίκτυο. Ενημερώνουν τον διαχειριστή σχετικά με την κατάσταση των *NE* και λαμβάνουν από αυτόν κατευθύνσεις για τις ενέργειες που πρέπει να κάνουν τα *NE* που αντιπροσωπεύουν.

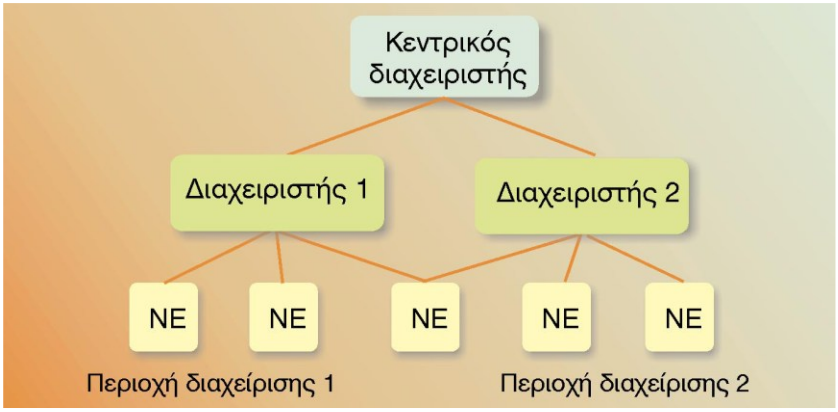
Εκτός από τους απλούς αντιπροσώπους, υπάρχουν και οι **πληρεξούσιοι αντιπρόσωποι** *(proxy agents)*. Η διαχείριση μέσω πληρεξούσιου αντιπροσώπου εκτελείται όταν ένα στοιχείο του δικτύου δεν έχει τη δυνατότητα να επικοινωνήσει απευθείας με έναν αντιπρόσωπο. Για παράδειγμα, συσκευές όπως η γέφυρα και το μόντεμ δεν είναι συνήθως ικανές να υποστηρίξουν πολύπλοκα πρωτόκολλα διαχείρισης. Έτσι, όταν ένα *NE* επιθυμεί να επικοινωνήσει με έναν αντιπρόσωπο-συσκευή που δεν μπορεί να υποστηρίξει κάποιο πρωτόκολλο διαχείρισης, απλώς κατευθύνει την κίνηση προς τον πληρεξούσιο αντιπρόσωπο. Αυτός έχει την ευθύνη να κατανοήσει το πρωτόκολλο διαχείρισης και να επιτελέσει τις λειτουργίες επικοινωνίας με τη διαχειριζόμενη συσκευή.

Η βάση πληροφοριών διαχείρισης *(MIB)* είναι μια βάση δεδομένων την οποία μοιράζονται μεταξύ τους οι διαχειριστές και οι αντιπρόσωποι και παρέχει πληροφορίες σχετικά με τα *NE* (Εικόνα 4-2). Τα *NE* εκπροσωπούν, νοητά, τα στοιχεία του δικτύου και βρίσκονται στη *MIB*. Η *MIB* χρησιμοποιείται επίσης στον καθορισμό της δομής και του περιεχομένου της διαχειριζόμενης πληροφορίας. Σχεδιαστικά απεικονίζεται με τη μορφή δένδρου, ενώ τα δεδομένα της παριστάνονται από τα φύλλα του δένδρου.



Εικόνα 4-2. Σχέση των επιμέρους μονάδων στη διαχείριση του δικτύου.

Ένα σύνθετο σύστημα διαχείρισης μπορεί να περιλαμβάνει πολλούς διαχειριστές και πολλούς αντιπροσώπους. Ένας διαχειριστής εκτελεί τη διαδικασία για τους δικούς του αντιπροσώπους, αλλά μπορεί ταυτόχρονα να αποτελεί αντιπρόσωπο για κάποια άλλη διαδικασία διαχείρισης. Κατ' αυτό τον τρόπο διαχειριστές και αντιπρόσωποι ορίζουν μια μορφή ιεραρχίας από πεδία διαχείρισης, καθένα από τα οποία αποτελεί το πεδίο δράσης ενός συστήματος διαχείρισης (Εικόνα 4-3). Τα πεδία αυτά ονομάζονται, σύμφωνα με την ορολογία του μοντέλου αναφοράς *OSI,* **περιοχές διαχείρισης** (*management domains*).



Εικόνα 4-3. Ιεραρχία διαχειριστικών συστημάτων.

Επειδή σήμερα έχουν επικρατήσει δύο αρχιτεκτονικές δικτύων υπολογιστών, η αρχιτεκτονική *TCP/IP* και η αρχιτεκτονική *OSI,* γίνεται ανάλογη διάκριση και στη διαχείριση δικτύων υπολογιστών, δηλαδή σε διαχείριση δικτύων *TCP/IP* και διαχείριση δικτύων *OSI.*

4.2. Πλατφόρμα διαχείρισης δικτύου

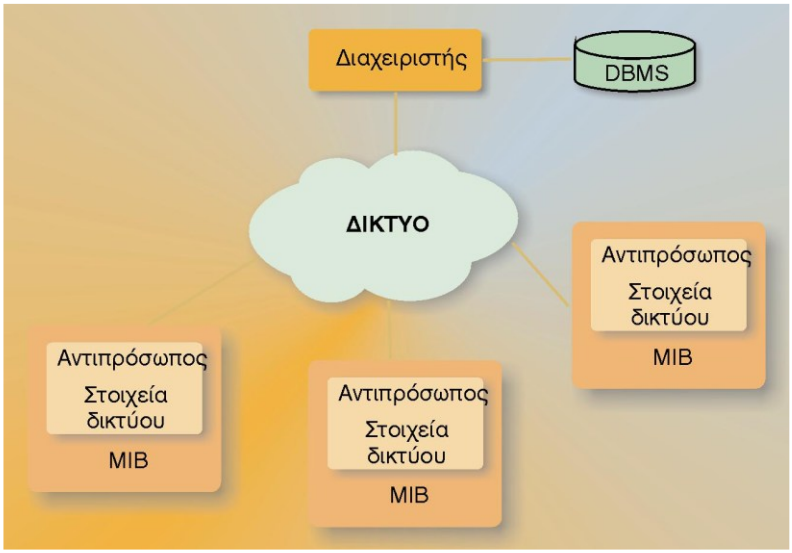
Λόγοι κυρίως οικονομικοί αλλά και εξοικονόμησης χώρου, καθώς και η έλλειψη έμπειρων τεχνικών, επέβαλαν την ανάγκη διαχείρισης των διάφορων στοιχείων του δικτύου από ένα και μοναδικό σύστημα, το οποίο θα παρουσίαζε τις διασυνδέσεις τους σε ένα δικτυακό χάρτη. Για την κάλυψη της παραπάνω ανάγκης δημιουργήθηκε η **πλατφόρμα διαχείρισης δικτύου** (*network management platform*). Πρόκειται για ένα πακέτο λογισμικού που έχει καθήκον να επιτελεί τις βασικές λειτουργίες διαχείρισης του δικτύου στα πολλά και διαφορετικά στοιχεία που το απαρτίζουν και τα οποία είναι:

- Η **γραφική διεπαφή χρήστη** (*GUI: Graphical User Interface*).
- Ο **δικτυακός χάρτης,** ο οποίος είναι χρησιμότατος σε κάθε περιοχή διαχείρισης του δικτύου. Περιλαμβάνει εργαλεία διαχείρισης βλαβών, που βοηθούν στον εντοπισμό της βλάβης με τη χρωματική παρουσίασή της στο δίκτυο, εργαλεία που εμφανίζουν με γραφική παράσταση τη φυσική και τη νοητή διαμόρφωση του δικτύου, καθώς και εργαλεία παρακολούθησης της απόδοσης του δικτύου, που παρουσιάζουν με χρωματική απεικόνιση την τρέχουσα απόδοση και τη διασύνδεση των συσκευών του δικτύου.
- Το **προσαρμοζόμενο σύστημα επιλογών**.
- Το **σύστημα διαχείρισης βάσης δεδομένων** *(DBMS: Database Management System), το* οποίο μπορούν να χρησιμοποιούν οι εφαρμογές για την αποθήκευση των πληροφοριών.
- Το **σύστημα πληροφόρησης,** το οποίο είναι μια τυποποιημένη μέθοδος για την άντληση πληροφοριών από τα στοιχεία του δικτύου.
- Το **ημερολόγιο συμβάντων**.
- Τα **εργαλεία γραφικών**.
- Η **διεπαφή προγράμματος εφαρμογής** (*API: Application Programming Interface*), η οποία είναι μια βιβλιοθήκη με συναρτήσεις-προγράμματα που επιτρέπουν την πρόσβαση στις πληροφορίες που υπάρχουν στην πλατφόρμα. Η *API* είναι αναγκαίο να είναι τυποποιημένη για όλες τις πλατφόρμες διαχείρισης του δικτύου και αυτό γιατί, στην περίπτωση που ένας οργανισμός αποφασίσει να αλλάξει πλατφόρμα, τότε θα πρέπει να αλλάξει και κάθε εφαρμογή που επικοινωνεί με την πλατφόρμα.
- Το **σύστημα ασφάλειας**.

4.3. Αρχιτεκτονικές διαχείρισης

Για να μπορεί μια πλατφόρμα να επιτελεί τις λειτουργίες που περιγράφηκαν στην προηγούμενη παράγραφο, θα πρέπει να χρησιμοποιεί κάποια αρχιτεκτονική διαχείρισης. Οι αρχιτεκτονικές διαχείρισης που ισχύουν προς το παρόν είναι η **κεντρική** (*centralized*), η **ιεραρχική** (*hierarchical*) και η **κατανεμημένη** (*distributed*).

- **Κεντρική αρχιτεκτονική.** Είναι η πιο απλή – κλασική πλέον – αρχιτεκτονική. Η πλατφόρμα διαχείρισης του δικτύου βρίσκεται μόνιμα σε ένα σταθμό εργασίας, ο οποίος είναι επιφορτισμένος με όλα τα καθήκοντα διαχείρισης του δικτύου. Η αρχιτεκτονική αυτή είναι συμβατή με το γνωστό μοντέλο διαχειριστή – αντιπροσώπου (Εικόνα 4-4).

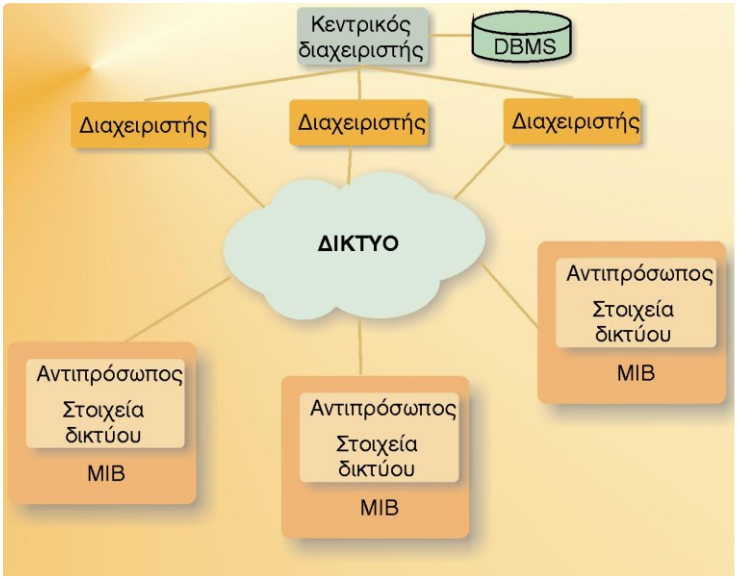


Εικόνα 4-4. Κεντρική αρχιτεκτονική διαχείρισης.

Η πλατφόρμα διαχείρισης, που είναι ο μόνος κεντρικός διαχειριστής του δικτύου, επιτελεί τις παρακάτω λειτουργίες:

- Αναλαμβάνει την επικοινωνία με όλα τα διαχειριζόμενα στοιχεία του δικτύου μέσω των αντιπροσώπων και του πρωτοκόλλου διαχείρισης.
- Διαχειρίζεται την αποθήκευση των πληροφοριών διαχείρισης του δικτύου. Η αποθήκευση των δεδομένων διαχείρισης μπορεί να είναι κεντρική ή για λόγους ασφάλειας κατανεμημένη, αλλά ο έλεγχος – όπως και όλος ο σχεδιασμός της αρχιτεκτονικής – είναι καθαρά κεντρικός.
- Παρέχει μια ενιαία εικόνα του διαχειριζόμενου δικτύου στον διαχειριστή μέσω του κατάλληλου περιβάλλοντος επικοινωνίας με τον χρήστη.

- **Ιεραρχική αρχιτεκτονική.** Η αρχιτεκτονική αυτή χρησιμοποιεί πολλές πλατφόρμες διαχείρισης. Μία από αυτές λειτουργεί σαν κεντρικός σταθμός εξυπηρέτησης του δικτύου, ενώ οι υπόλοιπες λειτουργούν σαν πελάτες. Οι πελάτες δεν έχουν ξεχωριστό **σύστημα διαχείρισης βάσης δεδομένων** (*DBMS*), αλλά χρησιμοποιούν το *DBMS* του διακομιστή, ενώ ο συντονισμός των λειτουργιών του γίνεται από τον διαχειριστή που βρίσκεται στο υψηλότερο επίπεδο της ιεραρχίας (Εικόνα 4-5).



Εικόνα 4-5. Ιεραρχική αρχιτεκτονική διαχείρισης.

Ορισμένες από τις λειτουργίες του συστήματος επιτελούνται από τον κεντρικό διαχειριστή, ενώ άλλες από τους επιμέρους διαχειριστές. Ο κεντρικός διαχειριστής συγκεντρώνει μόνο τις σημαντικές πληροφορίες, αφήνοντας τις λεπτομέρειες στους διαχειριστές του χαμηλότερου επιπέδου. Η επικοινωνία μεταξύ του κεντρικού και των επιμέρους διαχειριστών γίνεται είτε μέσω των *NE του* δικτύου, είτε μέσω ανεξάρτητου δικτύου διαχείρισης, ανάλογα με τις απαιτήσεις για αξιοπιστία.

Η ιεραρχική αρχιτεκτονική παρέχει καλύτερο έλεγχο και υψηλότερη απόδοση στη διαχείριση του δικτύου. Επίσης προσφέρεται για ετερογενή δίκτυα, διότι απομονώνει από το επίπεδο του κεντρικού διαχειριστή τα διαφορετικά πρωτόκολλα-διαχειριστές που βρίσκονται χαμηλότερα στην ιεραρχία. Έτσι εξασφαλίζεται ένα ομοιογενές διαχειριστικό περιβάλλον για το ετερογενές δίκτυο και επομένως κοινό περιβάλλον επικοινωνίας με τον χρήστη.

- **Κατανεμημένη αρχιτεκτονική.** Η αρχιτεκτονική αυτού του τύπου αποτελεί συνδυασμό της κεντρικής και της ιεραρχικής προσέγγισης (Εικόνα 4-6). Δε διαθέτει κεντρική πλατφόρμα διαχείρισης ή μια ιεραρχία από πλατφόρμες της μορφής πελάτη-διακομιστή, αλλά χρησιμοποιεί πολλές ομότιμες πλατφόρμες διαχείρισης, καθεμία από τις οποίες αποτελεί ένα κεντρικό σύστημα. Μία πλατφόρμα είναι επικεφαλής ενός συνόλου από ομότιμα συστήματα διαχείρισης (ιεραρχική αρχιτεκτονική). Κάθε πλατφόρμα μπορεί να έχει μια πλήρη βάση δεδομένων με στοιχεία που αφορούν οποιοδήποτε σημείο του δικτύου. Η διαχείριση κατανέμεται σε τοπικούς διαχειριστές και ως εκ τούτου έχει λιγότερες απαιτήσεις σε υλικό και σε υπολογιστική ισχύ από την κεντρική διαχείριση. Κάθε τοπικός διαχειριστής, απαλλαγμένος από το βάρος της παρακολούθησης ολόκληρου του δικτύου, διαχειρίζεται αρτιότερα τον τομέα της αρμοδιότητάς του, ενώ, όταν χρειαστεί πληροφορίες για περιοχές του δικτύου εκτός της δικής του αρμοδιότητας, τις ζητά από τον ομότιμό του διαχειριστή.

Εικόνα 4-6. Κατανεμημένη αρχιτεκτονική διαχείρισης.

4.4. Γενικά για τα πρωτόκολλα διαχείρισης δικτύου

Τα πρωτόκολλα διαχείρισης των δικτύων ευρείας περιοχής (WAN) χρησιμοποιούνται για την ανταλλαγή πληροφοριών διαχείρισης μεταξύ του διαχειριστή του δικτύου και των διαχειριζόμενων στοιχείων του δικτύου (*NE*). Τα πρωτόκολλα αυτά καθορίζουν:

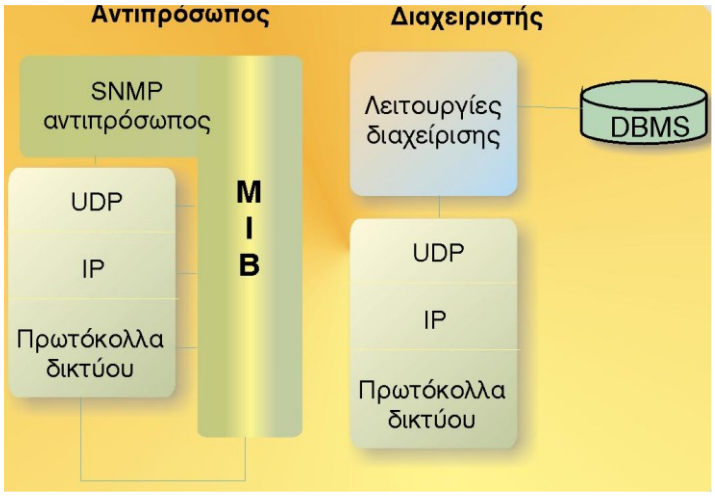
- τον ακριβή τρόπο επικοινωνίας μεταξύ του διαχειριστή και του αντιπροσώπου,
- τη μορφή και τη σημασία των μηνυμάτων που ανταλλάσσονται.

Το **πρωτόκολλο απλής διαχείρισης δικτύου** *(SNMP: Simple Network Management Protocol)* και το **πρωτόκολλο κοινής διαχείρισης πληροφοριών** *(CMIP: Common Management Information Protocol)* είναι τα δύο πιο σημαντικά πρωτόκολλα διαχείρισης. Το πρώτο, μαζί με τη **δομή πληροφοριών διαχείρισης** *(SMI: Structure of Management Information)* και τη βάση πληροφοριών διαχείρισης *(MIB),* αποτελεί έναν απλό αλλά λειτουργικό τρόπο διαχείρισης των δικτύων *TCP/IP.*

Το δεύτερο, μαζί με την **υπηρεσία κοινής διαχείρισης πληροφοριακών στοιχείων** *(CMISE: Common Management Information Service Element)* και τη γενικότερη αρχιτεκτονική των δικτύων *OSI,* αποτελεί μια μακροπρόθεσμη λύση στη διαχείριση μεγάλων ετερογενών δικτύων.

4.5. Διαχείριση TCP/IP - Πρωτόκολλο SNMP

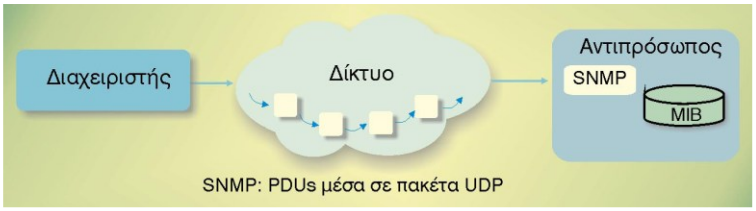
Σύμφωνα με το πρωτόκολλο *SNMP*, κάθε αντιπρόσωπος (λογισμικό) που είναι ενεργοποιημένος έχει στην κατοχή του ένα σύνολο από μεταβλητές (απεικονίσεις αντικειμένων), όπως διευθύνσεις, τύπους με διάφορα περιβάλλοντα διεπαφής, μετρητές κ.ά., των οποίων οφείλει να γνωρίζει τις τιμές και να τις παρουσιάζει. Οι απεικονίσεις αυτών των αντικειμένων είναι αφαιρετικές παραστάσεις πραγματικών στοιχείων του δικτύου, από τα οποία άλλα έχουν μία απεικόνιση και άλλα περισσότερες (όπως μια σύνδεση *TCP),* και οργανώνονται, σύμφωνα με το *SNMP,* σε έναν πίνακα. Το σύνολο των μεταβλητών αυτών αποτελεί τη βάση των πληροφοριών διαχείρισης *(MIB).* Το πρωτόκολλο *SNMP* δίνει τη δυνατότητα σε ένα σταθμό διαχείρισης να ελέγχει ή να μεταβάλλει τις μεταβλητές της *MIB* ενός αντιπροσώπου. Έτσι ο σταθμός διαχείρισης μπορεί να παρακολουθεί την απόδοση ενός δικτύου, να ελέγχει τις παραμέτρους που αφορούν την κατάσταση και τη λειτουργία του, να αναφέρει, να αναλύει και να απομονώνει σφάλματα (Εικόνα 4-7).



Εικόνα 4-7. Μοντέλο διαχείρισης δικτύων TCP/IP.

Κάθε αντιπρόσωπος κρατά πληροφορίες μόνο για ένα υποσύνολο απεικονίσεων της *MIB (MIB view),* ανάλογα με τα πρωτόκολλα που υλοποιούνται στο μηχάνημά του *(IP, TCP, UDP* κ.ά.), ενώ κάθε διαχειριστής διαθέτει διαφορετικό τρόπο πρόσβασης για κάθε απεικόνιση της *MIB* (ανάγνωση-εγγραφή, μόνο ανάγνωση). Με τους μηχανισμούς αυτούς επιτρέπεται η υλοποίηση κάποιου σχήματος ασφάλειας. Αν η απεικόνιση της *MIB* που κρατά ο αντιπρόσωπος δεν αφορά το μηχάνημα το οποίο εκτελεί τη διαχείριση αλλά κάποιο άλλο, τότε ο αντιπρόσωπος είναι πληρεξούσιος *(proxy agent).*

Το *SNMP* δίνει στις εφαρμογές διαχείρισης ένα πολύ μικρό σύνολο από πληροφοριακά στοιχεία για τον έλεγχο ή την αλλαγή των τιμών των απεικονίσεων της *MIB* στους διάφορους αντιπροσώπους. Η επικοινωνία μεταξύ διαχειριστών και αντιπροσώπων επιτυγχάνεται με την ανταλλαγή μονάδων δεδομένων πρωτοκόλλου *(PDUs: Protocol Data Units)*, καθεμία από τις οποίες κωδικοποιείται μέσα σε ένα μοναδικό πακέτο *UPD (UDP datagram)* και ανταλλάσσεται μέσω του πρωτοκόλλου *UDP.* Το *SNMP* είναι σχεδιασμένο έτσι, ώστε να εφαρμόζεται ακριβώς επάνω από το *UDP* (Εικόνα 4-8).



Εικόνα 4-8. Μεταφορά μηνυμάτων στο SNMP.

Το πρωτόκολλο *SNMP v.2* (δεύτερη έκδοση) αποτελεί εξέλιξη του πρωτοκόλλου *SNMP* και στοχεύει στην εξάλειψη πολλών μειονεκτημάτων της πρώτης έκδοσης, καθώς και στη διεύρυνση της εφαρμογής του σε δίκτυα βασισμένα τόσο στην ομάδα πρωτοκόλλων *TCP/IP*, όσο και σε πρότυπα του μοντέλου αναφοράς *OSI.* Οι βασικές βελτιώσεις και τα πρόσθετα στοιχεία του *SNMP v.2* συνοψίζονται στα παρακάτω:

- βελτιώσεις στη δομή των πληροφοριών διαχείρισης,
- εισαγωγή νέων λειτουργιών πρωτοκόλλου,
- νέες *MIB,*
- μεγαλύτερη ασφάλεια.

5. Περιγραφή του υπάρχοντος ασύρματου δικτύου

5.1. Εισαγωγή

Το παρόν έργο αποτελεί υλοποίηση ενός υποσυνόλου του «Πανελλήνιου Δικτύου για την Εκπαίδευση – EDUnet», το οποίο είναι οριζόντια δράση του ΥΠΕΠΘ σε ό,τι αφορά την υλοποίηση και λειτουργία της δικτυακής υποδομής και των υπηρεσιών τηλεματικής για την κάλυψη των αναγκών των εκπαιδευτικών και διοικητικών μονάδων της Δευτεροβάθμιας Εκπαίδευσης [14].

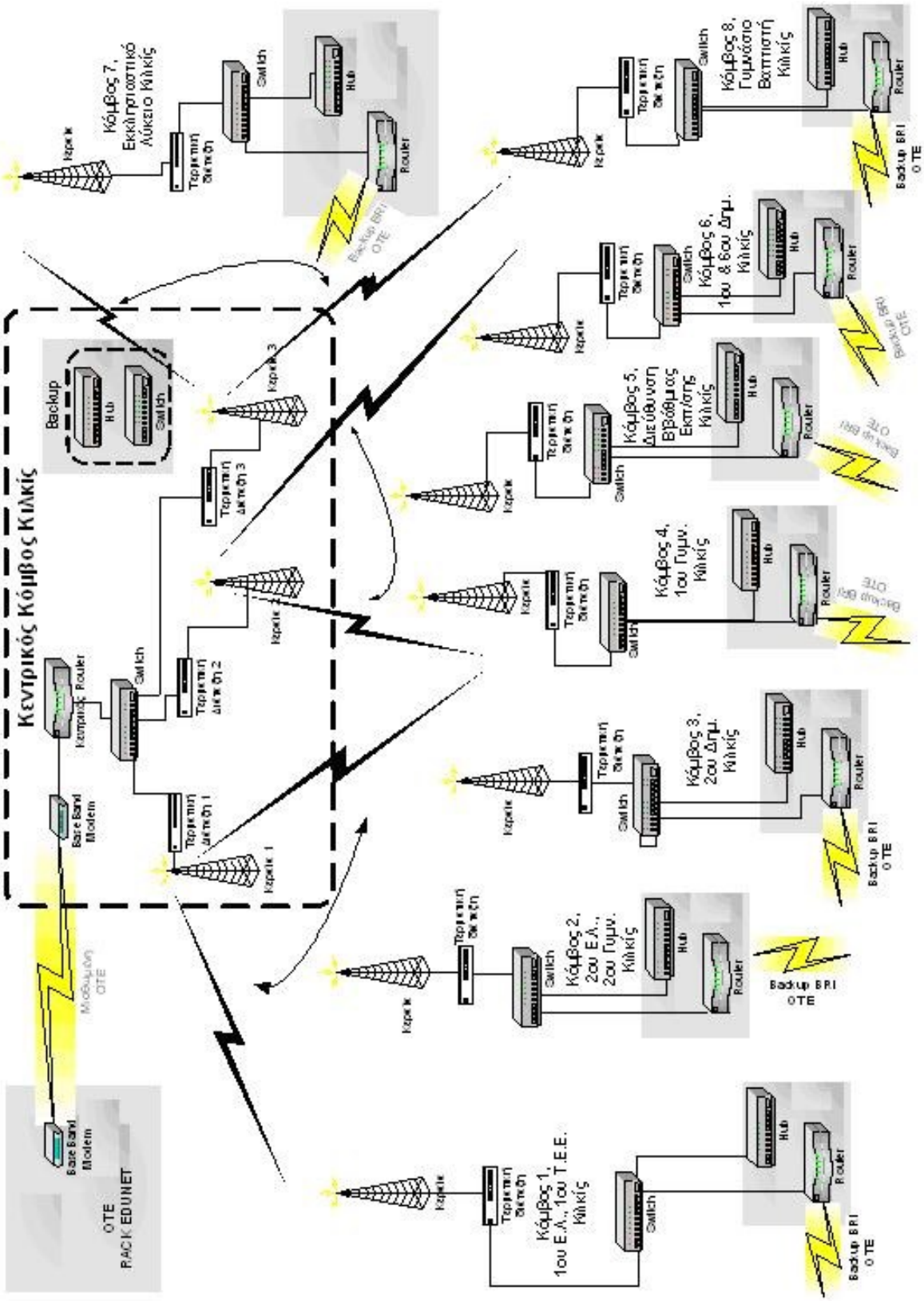
Πιο συγκεκριμένα πρόκειται για ένα πιλοτικό δικτυακό σύστημα ασύρματων ζεύξεων στα πλαίσια του δικτύου EDUnet, που επιτρέπει την πρόσβαση σε μονάδες της Εκπαίδευσης στην πόλη του Κιλκίς. Μέσω του πιλοτικού αυτού έργου μελετώνται οι δυνατότητες πρόσβασης με ασύρματες ζεύξεις και η ποιότητα των παρεχομένων υπηρεσιών.

Στο πιλοτικό έργο ακολουθούνται πιστά οι γενικές αρχές του EDUnet με μόνη διαφοροποίηση τον τρόπο πρόσβασης. Ως κόμβοι του δικτύου πρόσβασης για το EDUnet εννοούνται οι τερματικοί σταθμοί σε εκπαιδευτικές και διοικητικές μονάδες του ΥΠΕΠΘ. Το μοντέλο δικτύωσης που ακολουθείται είναι αυτό ενός ή περισσοτέρων τοπικών δικτύων που αναπτύσσονται στους χώρους συγκροτημάτων εκπαιδευτικών ή διοικητικών μονάδων. Οι αρχές επικοινωνίας και οι ορισμένοι ως κόμβοι EDUnet που συμμετέχουν παραμένουν αμετάβλητοι με μοναδική αλλαγή τον τρόπο πρόσβασης. Έχει δημιουργηθεί ένα υβριδικό μοντέλο συνύπαρξης ασύρματων και ενσύρματων ζεύξεων με σκοπό την αδιάλειπτη παροχή υπηρεσιών δικτύου με μεγαλύτερες ταχύτητες. Το βασικό δικτυακό πρωτόκολλο που υποστηρίζεται είναι το IP και η διεπαφή που πρέπει υποχρεωτικά να υποστηρίζεται είναι το Ethernet 10BaseT ή 100BaseT για σύνδεση σταθμών εργασίας στο τοπικό δίκτυο.

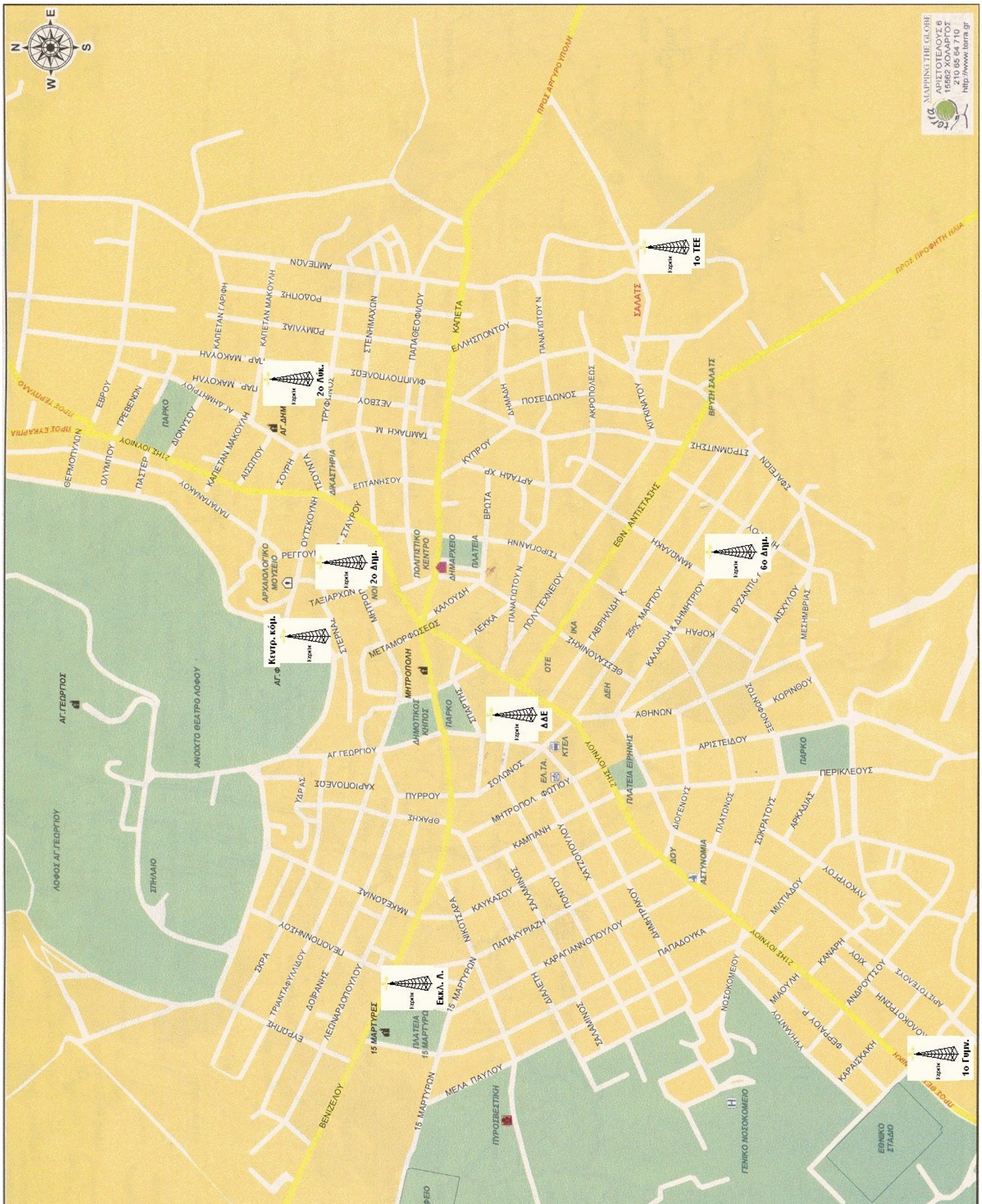
Ο εξοπλισμός του πιλοτικού έργου περιλαμβάνει:

1. **Ένα σύστημα ασυρμάτων ζεύξεων** βασισμένο στις αρχές του Broadband Wireless Access (BWA) και της τεχνολογίας FHSS που αποτελείται από **έναν κεντρικό σταθμό** με **2 μονάδες ασύρματης μετάδοσης** και **8 τερματικές μονάδες** με δυνατότητα επέκτασης και σε άλλα σημεία εντός της πόλης. Εδώ πρέπει να σημειωθεί ότι στον αρχικό σχεδιασμό προβλέπονταν 3 μονάδες ασύρματης μετάδοσης και αυτός ο αριθμός φαίνεται στο σχεδιάγραμμα της τοπολογίας του δικτύου.
2. **Ενεργά στοιχεία δικτύου** (Δρομολογητές, μεταγωγείς, μόντεμ κ.λπ.).
3. **Δομημένη καλωδίωση** σε επιλεγμένα σημεία των μονάδων σύμφωνα με το πρότυπο EIA /TIA 568 (στα τερματικά σημεία εκπαιδευτικών μονάδων και σε συστεγαζόμενες μονάδες) για τη φυσική διασύνδεση των ασυρμάτων σταθμών με τους τερματικούς σταθμούς του EDUnet.

Η τοπολογία του ασύρματου δικτύου φαίνεται στην Εικόνα 5-1 και η χωροταξική του ανάπτυξη στην πόλη του Κιλκίς στην Εικόνα 5-2.



Εικόνα 5-1. Τοπολογία συνολικού συστήματος.



Εικόνα 5-2. Χωροταξική ανάπτυξη του ασύρματου δικτύου στην πόλη του Κιλκίς.

Ως σημείο εγκατάστασης του κεντρικού κόμβου επιλέχθηκε το κτίριο πολυκατοικίας στην οδό Στέρνας αριθμός 7 επειδή εξαιτίας της ευνοϊκής θέσης του στους πρόποδες του λόφου του Αγίου Γεωργίου που δεσπόζει της πόλης του Κιλκίς (Εικόνα 5-3) διαθέτει οπτική επαφή με πολλές εκπαιδευτικές και διοικητικές μονάδες.

Εικόνα 5-3. Το κτίριο όπου εγκαταστάθηκε ο κεντρικός κόμβος του δικτύου.

Οι οκτώ τερματικοί κόμβοι εγκαταστάθηκαν στα εξής συγκροτήματα εκπαιδευτικών και διοικητικών μονάδων της πόλης του Κιλκίς:

<u>Σύνδεση με Α΄ Ασύρματη Διάταξη Κεντρικού Κόμβου</u>

1. Κτιριακό Συγκρότημα 6ου Δημοτικού και 1ου Δημοτικού
2. Κτίριο 1ου Γυμνασίου
3. Κτίριο Εκκλησιαστικού Λυκείου
4. Κτίριο Γυμνασίου Βαπτιστή (εκτός πόλεως)

<u>Σύνδεση με Β΄ Ασύρματη Διάταξη Κεντρικού Κόμβου</u>

5. Κτιριακό Συγκρότημα 1ου ΤΕΕ, 1ου Εν. Λυκείου, Εσπερινού Λυκείου και Εσπερινού Γυμνασίου
6. Κτιριακό Συγκρότημα 2ου Εν. Λυκείου και 2ου Γυμνασίου,
7. Κτίριο 2ου Δημοτικού
8. Διεύθυνση Δευτεροβάθμιας Εκπαίδευσης

Επειδή οι παραπάνω αντιστοιχίσεις δεν έχουν εφαρμοστεί ακόμη με μόνιμο τρόπο, κάθε τερματικός κόμβος επιλέγει ελεύθερα την ασύρματη διάταξη του κεντρικού κόμβου με την οποία συνδέεται με αποτέλεσμα η υπάρχουσα κατάσταση να μην ανταποκρίνεται στις παραπάνω αντιστοιχίσεις (βλ. παρακάτω Εικόνα 6-7).

Η μέγιστη απόσταση μεταξύ των τερματικών σημείων και του κεντρικού σταθμού εκτιμάται ότι δεν ξεπερνά τα 2 km, εκτός από το Γυμνάσιο Βαπτιστή το οποίο απέχει περίπου 6 km. Η ζεύξη είναι τεχνολογίας «σημείο προς πολλά σημεία» (point-to-multipoint). Η λειτουργία της κυμαίνεται σε φάσμα συχνοτήτων για το οποίο δεν απαιτείται ειδική άδεια (ζώνη ISM, δηλαδή 2,4 GHz) και υλοποιείται βασισμένο στις αρχές του Broadband Wireless Access (BWA) και σύμφωνα με την τεχνολογία Frequency Hopping Spread Spectrum. Δεν έγιναν δεκτές λύσεις βασισμένες σε Direct Sequence Spread Spectrum. Επίσης, εξασφαλίζεται η διατήρηση της ομοιογένειας του εξοπλισμού με το υπάρχον δίκτυο.

Θα πρέπει να σημειωθεί ότι η ισχύς εκπομπής όλων των ασύρματων συστημάτων (κεντρικών και τερματικών) είναι μικρότερη από το επιτρεπτό όριο το οποίο ορίζουν οι ελληνικοί και διεθνείς κανονισμοί. Συγκεκριμένα σύμφωνα με τον κανονισμό ETSI EN 300 328 - 1 v1.3.1 (12/2001) το όριο ισχύος εκπομπής (Effective Isotropic Radiated Power – EIRP) είναι 20 dBm (-10 dBW ή 100 mW).

5.2. Κεντρικός κόμβος

Ο κεντρικός κόμβος απαρτίζεται από ένα σύστημα Broadband Wireless Access (BWA) με ένα chassis στο οποίο είναι εγκατεστημένες δύο τερματικές διατάξεις (wireless stations) με δύο κεραίες τομέα (sectorial) (Εικόνα 5-4) για τη δημιουργία δύο επικαλυπτόμενων περιοχών. Η επιλογή δύο κεντρικών ασυρμάτων διατάξεων κρίθηκε αναγκαία ώστε να είναι δυνατή η επέκταση του ασύρματου δικτύου και σε άλλα σχολεία αν αυτό κριθεί σκόπιμο στο μέλλον, καθώς και για την αύξηση του διαθέσιμου εύρους ζώνης ανά μονάδα που συμμετέχει στην παρούσα πιλοτική εφαρμογή. Τα χαρακτηριστικά των κεντρικών κεραιών (γωνία κάλυψης, ευαισθησία, κέρδος κ.λπ.) είναι βέλτιστα για την καλύτερη εκμετάλλευση της παρεχόμενης ισχύος των ασυρμάτων διατάξεων. Αυτό επιτρέπει τη χρήση κεραιών χαμηλού κόστους στους τερματικούς κόμβους. Επιπλέον, βελτιστοποιείται η περιοχή κάλυψης τόσο σε απόσταση όσο και σε εύρος.

Εικόνα 5-4. Ο κεντρικός κόμβος του δικτύου με εγκατεστημένο σύστημα 2 κεραιών.

Η δικτύωση των ασυρμάτων διατάξεων γίνεται με τη βοήθεια δρομολογητή (router) και μεταγωγέα (switch). Ο δρομολογητής είναι σαφώς μοντέλο ανώτερων προδιαγραφών από τον αντίστοιχο των τερματικών κόμβων, ενώ ο μεταγωγέας είναι το ίδιο μοντέλο. Υπάρχει επίσης ένας (1) επιπλέον μεταγωγέας (switch) ως εφεδρεία. Η διασύνδεση με τον κόμβο του EDUnet

στο Κιλκίς πραγματοποιείται με χρήση μισθωμένης γραμμής και baseband μόντεμ όπως αναφέρεται στην παράγραφο 5.4.

5.3. Τερματικοί κόμβοι

Σε κάθε τερματικό κόμβο (εκπαιδευτική ή διοικητική μονάδα), μετά από επιτόπιο έλεγχο σχετικά με τη βέλτιστη θέση με κριτήριο την καλύτερη οπτική επαφή ανάμεσα στον τερματικό και τον κεντρικό κόμβο, έχει τοποθετηθεί σε κατάλληλο σημείο μια κατευθυντική κεραία (directional antenna) (Εικόνα 5-5) με τη χρήση ιστού και μια τερματική μονάδα (wireless station) η οποία αποτελείται από εξωτερική και εσωτερική συσκευή (Subscriber Unit, SU).

Εικόνα 5-5. Κατευθυντική κεραία εγκατεστημένη σε τερματικό κόμβο.

Επίσης, έχει τοποθετηθεί δρομολογητής και μεταγωγέας (Εικόνα 5-6), ώστε να επιτευχθεί η διασύνδεση της τερματικής μονάδας με τον κεντρικό κόμβο του EDUnet. Η δικτύωση γίνεται με τη χρήση πρωτοκόλλου 802.1q και δημιουργία VLANs. Επιπλέον, ο δρομολογητής κάθε τερματικού κόμβου διαθέτει backup σύνδεση μέσω ISDN γραμμής για την περίπτωση δυσλειτουργίας του ασύρματου δικτύου. Σε κάθε σχολικό συγκρότημα έχει εγκατασταθεί η απαραίτητη δομημένη καλωδίωση, είτε καλωδίων χαλκού UTP τουλάχιστον Cat. 5, είτε οπτικής ίνας με τους αντίστοιχους μετατροπείς, ώστε όλες οι μονάδες του συγκροτήματος να συνδεθούν με τον μεταγωγέα.

Εικόνα 5-6. Τηλεπικοινωνιακό ικρίωμα (rack) τερματικού κόμβου με εσωτερική συσκευή ασύρματης σύνδεσης, δρομολογητή και δύο μεταγωγείς.

5.3.1. Εσωτερική συσκευή ασύρματης σύνδεσης (Alvarion BreezeAccess II)

Η εσωτερική συσκευή ασύρματης σύνδεσης είναι το σύστημα Broadband Wireless Access (BWA) BreezeAccess II (Εικόνα 5-7) της Alvarion (http://www.alvarion.com) που λειτουργεί παγκοσμίως στην ελεύθερη από άδειες ISM ζώνη παρέχοντας υψηλής ταχύτητας ασύρματη πρόσβαση στο Διαδίκτυο. Η χρησιμοποίηση της χωρίς άδεια ζώνης 2,4 GHz επιτρέπει τη χρήση του φάσματος χωρίς τη δαπάνη αγοράς ή της υποβολής αίτησης για άδεια.

Εικόνα 5-7. Εσωτερική συσκευή ασύρματης σύνδεσης BreezeAccess II της Alvarion.

Άπαξ και η ασύρματη υποδομή τεθεί σε ισχύ, μπορεί να επεκταθεί για να υποστηρίξει χιλιάδες συνδρομητές ανά κελί.

Το BreezeAccess II λειτουργεί με αμφίδρομο καταμερισμό χρόνου (Time Division Duplex, TDD) χρησιμοποιώντας την αξιόπιστη τεχνολογία Διασποράς Φάσματος με Αναπήδηση Συχνότητας (FHSS) για να παράσχει μια λύση που είναι ιδιαίτερα ασφαλής, εύρωστη και αξιόπιστη.

Τα κυριότερα χαρακτηριστικά του BreezeAccess II:

- Ταχεία πρόσβαση στο Διαδίκτυο και άλλες βασισμένες στο IP υπηρεσίες
- Μεταγωγή πακέτων – βελτιστοποιημένη για επικοινωνίες IP
- Άμεση συνδεσιμότητα – ο συνδρομητής είναι πάντα on
- Η εγκαθιστώμενη από τον χρήστη CBE μειώνει τις δαπάνες ανάπτυξης
- Υψηλή ταχύτητα – μέχρι 3 Mbps ανά συνδρομητή
- Ταυτόχρονη υψηλή ταχύτητα δεδομένων και τηλεφωνία
- Υψηλή χωρητικότητα – χιλιάδες συνδρομητές ανά κελί
- Ευρεία κάλυψη – ακτίνα κελιών μέχρι 15 km
- Συμμετρική/ασύμμετρη CIR & MIR ανά συνδρομητή
- Ποιότητα υπηρεσίας (QoS) στην τηλεφωνία ανά συνδρομητή
- Ευρυζωνικές υπηρεσίες: VPNs, VLANs
- Υποστήριξη διαχείρισης SNMP
- Υποστήριξη λογαριασμών RADIUS
- Εύκολα εξελικτική αρχιτεκτονική
- Ώριμη, αξιόπιστη τεχνολογία

5.4. Εσωτερική διασύνδεση – Διασύνδεση με το Δίκτυο του EDUnet

Όλα τα σχολεία της ασύρματης νησίδας διασυνδέονται μεταξύ τους αποτελώντας ένα μικρό ενδοδίκτυο. Αυτό διαπιστώνεται εύκολα κατά τον έλεγχο της δρομολόγησης των δεδομένων από ένα σχολείο σε άλλο:

Από 6ο Δημοτικό:

```
C:\>tracert 194.63.209.76                          ← Linux Server 1ου ΤΕΕ

Tracing route to 194.63.209.76 over a maximum of 30 hops

  1   <10 ms   <10 ms   <10 ms  10.141.25.1     ← Δρομολογητής 6ου Δημοτικού
  2   120 ms    50 ms    40 ms  81.186.189.65   ← Κεντρ. δρομολ. ασύρμ. δικτύου
  3   180 ms   201 ms    40 ms  81.186.189.76   ← Δρομολογητής 1ου ΤΕΕ
  4   761 ms   370 ms   281 ms  194.63.209.76   ← Linux Server 1ου ΤΕΕ

Trace complete.
```

Η διασύνδεση με τον κόμβο του EDUnet γίνεται με μισθωμένη γραμμή του ΟΤΕ τύπου Μ-1020 και με δύο (2) Baseband μόντεμ.

5.5. Πρότυπα

Το ασύρματο δίκτυο χρησιμοποιεί τα πρότυπα της IEEE 802.3 (Ethernet) και 802.11

(Ασύρματα δίκτυα).

Επίσης, χρησιμοποιείται το πρότυπο 802.1q για τα VLANs.

Τα VLANs λειτουργούν για τη διασύνδεση των δρομολογητών των εκπαιδευτικών και διοικητικών μονάδων με τους κατά τόπους μεταγωγείς (switches) και κατ' επέκταση με τον κεντρικό κόμβο EDUnet σύμφωνα με τους εξής κανόνες:
Α) Κάθε εκπαιδευτική ή διοικητική μονάδα διαθέτει το δικό της VLAN
Β) Όλες οι ασύρματες τερματικές μονάδες ανήκουν σε ένα ξεχωριστό VLAN

5.6. Διεπαφές (interfaces)

Οι διεπαφές του δικτύου είναι:
- 802.11 για την ασύρματη σύνδεση
- 802.3u (Fast Ethernet) για τη διασύνδεση με τα LAN των σχολικών μονάδων
- ISDN για εναλλακτική δυνατότητα σύνδεσης

5.7. Ρυθμός μετάδοσης – Εύρος ζώνης

Η επικοινωνία του κόμβου του Κιλκίς με αυτόν της Θεσσαλονίκης γίνεται με τετρασύρματη γραμμή. Η μέγιστη ταχύτητα διασύνδεσης σήμερα είναι 2,3 Mbps σε δισύρματη γραμμή με δυνατότητα πιθανής αναβάθμισης του συνολικού εύρους ζώνης σε 4,6 Mbps με χρήση της τετρασύρματης.

Ο ρυθμός μετάδοσης στον αέρα είναι έως 3 Mbps half-duplex.

Η λειτουργία του δικτύου κυμαίνεται σε φάσμα συχνοτήτων για το οποίο δεν απαιτείται ειδική άδεια (ISM Band, δηλαδή 2,4 GHz) και υλοποιείται βασισμένο στις αρχές του Broadband Wireless Access (BWA) και σύμφωνα με την τεχνολογία Frequency Hopping Spread Spectrum.

5.8. Εφαρμογές για τις οποίες χρησιμοποιείται το δίκτυο

Ο λόγος εγκατάστασης του ασυρμάτου δικτύου είναι η παροχή πρόσβασης στο Διαδίκτυο σε σχολικές μονάδες της πόλης του Κιλκίς. Επειδή το δίκτυο είναι ευρυζωνικό, οι πιθανές εφαρμογές που θα μπορούν να υλοποιηθούν μέσω αυτού σχετίζονται με τις παραδοσιακές αλλά και τις προηγμένες υπηρεσίες που παρέχει το Πανελλήνιο Σχολικό Δίκτυο (EDUnet) στους χρήστες του:

1. **Σύνδεση στο δίκτυο** (connectivity) των σχολικών και διοικητικών μονάδων της εκπαίδευσης (ήδη σε λειτουργία)
2. **Ηλεκτρονικό Ταχυδρομείο** (E-mail). Παρέχεται μέσω POP3, IMAP και web mail (ήδη σε λειτουργία).
3. **Τηλεφωνία πάνω από το Πανελλήνιο Σχολικό Δίκτυο** (Voice over IP). Η υπηρεσία προβλέπεται να είναι διαθέσιμη σε 65 διευθύνσεις και γραφεία δευτεροβάθμιας σε διάφορους νομούς σε λίγο καιρό.
4. **Τηλεδιάσκεψη** (παρέχεται η δυνατότητα αλλά δεν έχει υλοποιηθεί ακόμη).
5. **Ασύγχρονη τηλεκπαίδευση** (παρέχεται η δυνατότητα αλλά δεν έχει υλοποιηθεί ακόμη).
6. **Βίντεο κατά παραγγελία** (Video On Demand) (παρέχεται η δυνατότητα αλλά δεν έχει υλοποιηθεί ακόμη).

6. Σύστημα παρακολούθησης και καταγραφής Monitoring System

Το Monitoring System της Wireless Connections[2] είναι λογισμικό που χρησιμοποιείται για την παρακολούθηση και καταγραφή της λειτουργίας ασύρματων δικτύων και παρέχεται δωρεάν από τον δικτυακό τόπο της κατασκευάστριας εταιρείας. Το λογισμικό μπορεί να εγκατασταθεί ακόμη και σε υπολογιστή εκτός του δικτύου. Δηλώνονται σ' αυτό οι συσκευές που θα παρακολουθεί με την IP διεύθυνσή τους (συνήθως πρόκειται για subscriber units των τερματικών κόμβων) χωρίς να απαιτείται καμιά απολύτως επέμβαση σ' αυτές. Η λειτουργία του Monitoring System συνίσταται στη συνεχή συλλογή δεδομένων από τους τερματικούς κόμβους μέσω προγραμμάτων που εκτελούνται συνεχώς και κατόπιν στη δημιουργία (βάσει αυτών των δεδομένων) διαφόρων γραφικών παραστάσεων. Η εγκατάσταση του Monitoring System απαιτεί την προεγκατάσταση άλλου λογισμικού.

6.1. Λογισμικό προαπαιτούμενο για την εγκατάσταση

6.1.1. Perl

Το ActivePerl της ActiveState (https://www.activestate.com/platform/supported-languages/perl/) είναι μια εγγυημένης ποιότητας, έτοιμη για εγκατάσταση διανομή της γλώσσας προγραμματισμού Perl, διαθέσιμη για Linux, Solaris και Windows.

Το ActivePerl περιέχει τα εξής: τον πυρήνα Perl, τον Perl Package Manager (PPM) για την εγκατάσταση πακέτων CPAN, δημοφιλών αρθρωμάτων (modules) λογισμικού και πλήρους online βοήθειας.

Η διανομή Windows παρέχει πρόσθετα χαρακτηριστικά γνωρίσματα που βοήθησαν να γίνει το ActivePerl παγκόσμιο πρότυπο για την Perl σε Windows.

6.1.2. RRD Tool και Cricket

Το RRD είναι το ακρωνύμιο για το Round Robin Database. Είναι ένα σύστημα για αποθήκευση και επίδειξη χρονοσειρών δεδομένων (π.χ. εύρος ζώνης δικτύων, θερμοκρασία μηχανοστασίου, μέσος όρος φορτίου διακομιστή). Αποθηκεύει τα δεδομένα με έναν πολύ συμπαγή τρόπο που δεν επεκτείνεται κατά τη διάρκεια του χρόνου και παρουσιάζει χρήσιμες γραφικές παραστάσεις επεξεργαζόμενο τα δεδομένα για να εφαρμόσει μια ορισμένη πυκνότητα δεδομένων. Μπορεί να χρησιμοποιηθεί είτε μέσω απλών scripts (από το κέλυφος ή την Perl), είτε μέσω front-ends που κάνουν δειγματοληψία σε συσκευές δικτύων και εμφανίζουν μια φιλική διεπαφή χρήστη (https://oss.oetiker.ch/rrdtool/download.en.html).

Το Cricket (https://cricket.sourceforge.net/) είναι ένα υψηλής απόδοσης, εξαιρετικά ευέλικτο σύστημα για καταγραφή τάσεων σε χρονοσειρές δεδομένων. Το Cricket αναπτύχθηκε επίτηδες για να βοηθήσει διαχειριστές δικτύων να απεικονίσουν και να καταλάβουν την κυκλοφορία στα δίκτυά τους, αλλά μπορεί να χρησιμοποιηθεί και για όλα τα είδη άλλων εργασιών.

Το Cricket έχει δύο συστατικά, έναν συλλέκτη και έναν δημιουργό γραφικών

[2] http://www.wirelessconnections.net/

παραστάσεων. Ο συλλέκτης εκτελείται από το χρονοδιάγραμμα εργασιών του υπολογιστή κάθε 5 λεπτά (ή με ένα διαφορετικό ρυθμό, εάν είναι ανάγκη), και αποθηκεύει τα στοιχεία σε μια δομή δεδομένων διαχειριζόμενη από το RRD Tool. Αργότερα, όταν θέλουμε να ελέγξουμε τα στοιχεία που έχουμε συλλέξει, μπορούμε να χρησιμοποιήσουμε μια βασισμένη στο Διαδίκτυο διεπαφή για να δούμε γραφικές παραστάσεις των δεδομένων.

Το Cricket διαβάζει ένα σύνολο αρχείων διαμόρφωσης που λέγεται δένδρο διαμόρφωσης (configuration tree). Το δένδρο διαμόρφωσης εκφράζει όλα όσα πρέπει να ξέρει το Cricket για τους τύπους δεδομένων που συλλέγονται, πώς να το πάρει και από ποιες πηγές πρέπει να συλλέξει δεδομένα. Το δέντρο διαμόρφωσης έχει σχεδιαστεί για να ελαχιστοποιεί τις περιττές πληροφορίες, που καθιστούν συμπαγές και εύκολο στη διαχείριση και που αποτρέπει τα ανόητα λάθη που εμφανίζονται οφειλόμενα σε σφάλματα αντιγραφής και επικόλλησης.

Το Cricket είναι γραμμένο εξ ολοκλήρου σε Perl και διανέμεται με GNU General Public License.[3]

6.2. Εγκατάσταση – διαμόρφωση – λειτουργία του Monitoring System

Παρακάτω αναφέρονται μερικά στοιχεία σχετικά με την εγκατάσταση, τη διαμόρφωση και τη λειτουργία του λογισμικού αυτού [9].

6.2.1. Απαιτήσεις συστήματος

Διακομιστής:

- Windows NT 4.0 με SP 6a / Windows 2000 Server με SP 2 ή νεότερο
- Microsoft Access 2000 ή νεότερο (προαιρετικό)
- Microsoft IIS 4.0 ή νεότερο
- MDAC 2.1 ή νεότερο
- ActiveState Perl 2.8.1 Build 810 ή νεότερο
- Cricket 1.0.5

Πελάτης:

- Microsoft Internet Explorer 5.0 ή νεότερο

6.2.2. Εγκατάσταση

Υπάρχουν 3 κύρια τμήματα που πρέπει να εγκατασταθούν ώστε να λειτουργήσει το Monitoring System. Αυτά είναι:
Perl, Cricket (RRD Tool) και ο Δικτυακός Τόπος.

Καταρχήν, πρέπει να εγκατασταθούν στον Windows Web Server μας τα Perl και Cricket. Η όλη εγκατάσταση γίνεται σε 7 βήματα:

[3] Αυτή είναι μια άδεια για λογισμικό της οποίας οι παροχές περιλαμβάνουν κυρίως τα εξής:
1. Πρέπει ο χρήστης να έχει πρόσβαση στον πηγαίο κώδικα του προγράμματος.
2. Έχει το δικαίωμα να τροποποιήσει τον πηγαίο κώδικα όπως επιθυμεί.
3. Είναι ελεύθερος να πετάξει ή να πουλήσει το πρόγραμμα.
4. Δεν μπορεί να αποτρέψει οποιονδήποτε άλλο από το να διανείμει είτε τον αρχικό κώδικα, είτε τις τροποποιήσεις του.

Βήμα 1 – Εγκατάσταση του ActiveState Perl

Εγκαθιστούμε το ActivePerl της ActiveState (βλ. παράγραφο 6.1.1) το οποίο εγκαθιστά PerlScript συνδέσμους στον IIS. Επίσης, εγκαθιστούμε τις ISAPI επεκτάσεις.

Βήμα 2 – Εξαγωγή της βάσης του Monitoring System

Πρόκειται για μια πλήρη δομή φακέλων που εξάγεται σε συγκεκριμένη θέση στον Windows Server (`\Monitoring`) και περιλαμβάνει τα βασικά αρχεία για το Monitoring System καθώς και τα Cricket 1.0.5 και RRD Tool (παρ. 6.1.2).

Βήμα 3 – Εγκατάσταση των Perl Cricket αρθρωμάτων

Πρόκειται για αρθρώματα (modules) Perl και SNMP που πρέπει να εγκατασταθούν ώστε να λειτουργήσει το τμήμα Cricket του Monitoring System. Η εγκατάσταση γίνεται αυτόματα με την εκτέλεση ενός αρχείου δέσμης (`.bat`) του Monitoring System.

Βήμα 4 – Εξαγωγή των αρχείων του Δικτυακού Τόπου

Πρόκειται για μια πλήρη δομή φακέλων που εξάγεται στην εξ ορισμού προσπελάσιμη από το Διαδίκτυο περιοχή του Web Server μας (`\Inetpub\wwwroot\monitoringweb`).

Βήμα 5 – Εγκατάσταση του Δικτυακού Τόπου στον IIS Server

Πρόκειται για τη μετατροπή (βλ. φάκελο `\Inetpub\wwwroot\monitoringweb` Βήματος 4) και τη δημιουργία (βλ. φάκελο `\Monitoring` Βήματος 2) εικονικών καταλόγων (virtual directories) στον IIS ώστε να είναι προσπελάσιμοι από το Διαδίκτυο, καθώς επίσης και για την προσθήκη υποστήριξης αρχείων `.cgi` στον IIS.

Βήμα 6 – Αλλαγή δικαιωμάτων στη βάση δεδομένων της Access 2000

Για να μπορεί η βάση δεομένων της Access 2000 να λειτουργήσει σωστά στο NTFS περιβάλλον του διακομιστή, είναι απαραίτητο να αλλάξουν τα δικαιώματα πρόσβασης από «Ανάγνωσης» μόνο σε «Ανάγνωσης/Εγγραφής».

Βήμα 7 – Εκκίνηση των αρχείων συλλογής δεδομένων

Πρόκειται για δύο αρχεία δέσμης τα οποία προγραμματίζονται να εκτελούνται κάθε 1 και 5 λεπτά αντίστοιχα και λειτουργούν ως συλλέκτες δεδομένων από τα στοιχεία του δικτύου που παρακολουθούνται.

6.2.3. Διαμόρφωση του λογισμικού

Αφού εγκατασταθεί το λογισμικό με επιτυχία, σε ένα πρόγραμμα πλοήγησης πληκτρολογούμε το URL http://<server name>/monitoringweb και εμφανίζεται η αρχική σελίδα της εφαρμογής (Εικόνα 6-1).

Προσθήκη νέων συσκευών

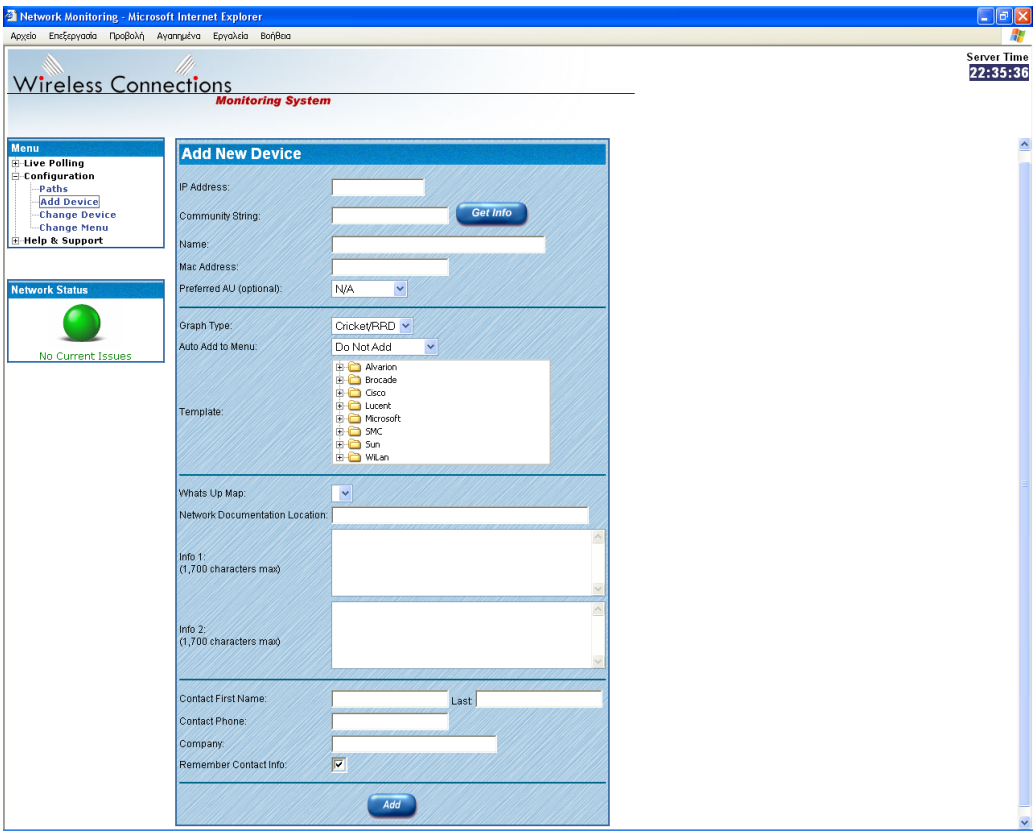
Οι συσκευές που προστίθενται για παρακολούθηση και καταγραφή στο Monitoring System είναι συνήθως:

- AU (Access Unit – Μονάδα Πρόσβασης) δηλ. κεντρική μονάδα μετάδοσης και
- SU (Subscriber Unit – Συνδρομητική μονάδα) δηλ. τερματική μονάδα.

Κάθε AU συνδέεται με έναν αριθμό SU όπως φαίνεται και στην Εικόνα 6-7.

Για να προσθέσουμε μια συσκευή, από το μενού του συστήματος επιλέγουμε **Configuration → Add Device**. Πρέπει να δούμε κάτι παρόμοιο με την Εικόνα 6-2.

Εικόνα 6-1. Η αρχική σελίδα της διαδικτυακής εφαρμογής Monitoring System της Wireless Connections.



Εικόνα 6-2. Η σελίδα προσθήκης νέας συσκευής (Add New Device).

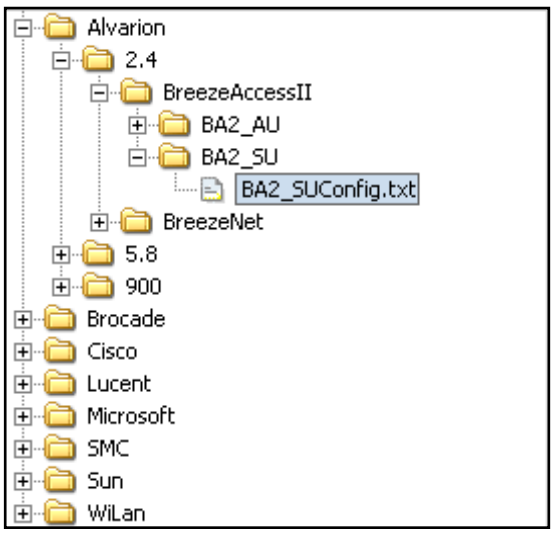
Οι συσκευές καθορίζονται σαν οποιαδήποτε συσκευή που υποστηρίζει SNMP στο δίκτυο την οποία χρειάζεται να καταγράψουμε σε γράφημα και η οποία έχει ένα πρότυπο εγκατάστασης στο σύστημα γι' αυτήν.

Για να προσθέσουμε νέα συσκευή απλώς πληκτρολογούμε τη διεύθυνση IP της συσκευής στο πεδίο **IP Address** και τη read only σειρά χαρακτήρων στο πεδίο **Community String**. Προαιρετικά, μπορούμε τώρα να πατήσουμε το κουμπί **Get Info**. Με το πάτημα αυτού του κουμπιού, το σύστημα θα επικοινωνήσει με το πρωτόκολλο SNMP με τη διεύθυνση IP που μόλις δώσαμε και θα προσπαθήσει να μας επιστρέψει το όνομα (**Name**) και τη διεύθυνση MAC (**MAC Address**) της συσκευής από τη MIB. Αν αυτό πετύχει, θα δούμε αυτές τις τιμές να συμπληρώνονται αυτόματα στα δύο αντίστοιχα πεδία. Αν οποιοδήποτε πεδίο συμπληρωθεί όχι όπως περιμένουμε, είμαστε ελεύθεροι να το αλλάξουμε οποιαδήποτε στιγμή.

Το επόμενο τμήμα είναι για τη διάρθρωση των γραφικών παραστάσεων. Το πεδίο **Graph Type** πρέπει να οριστεί ως **Cricket/RRD**. Προς το παρόν, αυτός είναι ο μόνος διαχειριστής γραφημάτων που υποστηρίζει το Monitoring System.

Το επόμενο πεδίο είναι για το μενού του συστήματος. Εξ ορισμού είναι επιλεγμένη η μη προσθήκη της νέας συσκευής (**Do Not Add**) στο μενού συστήματος. Αυτό μπορούμε να το αλλάξουμε με επιλογή όπου επιθυμούμε αυτή η συσκευή να μπει στο υπάρχον μενού συστήματος.

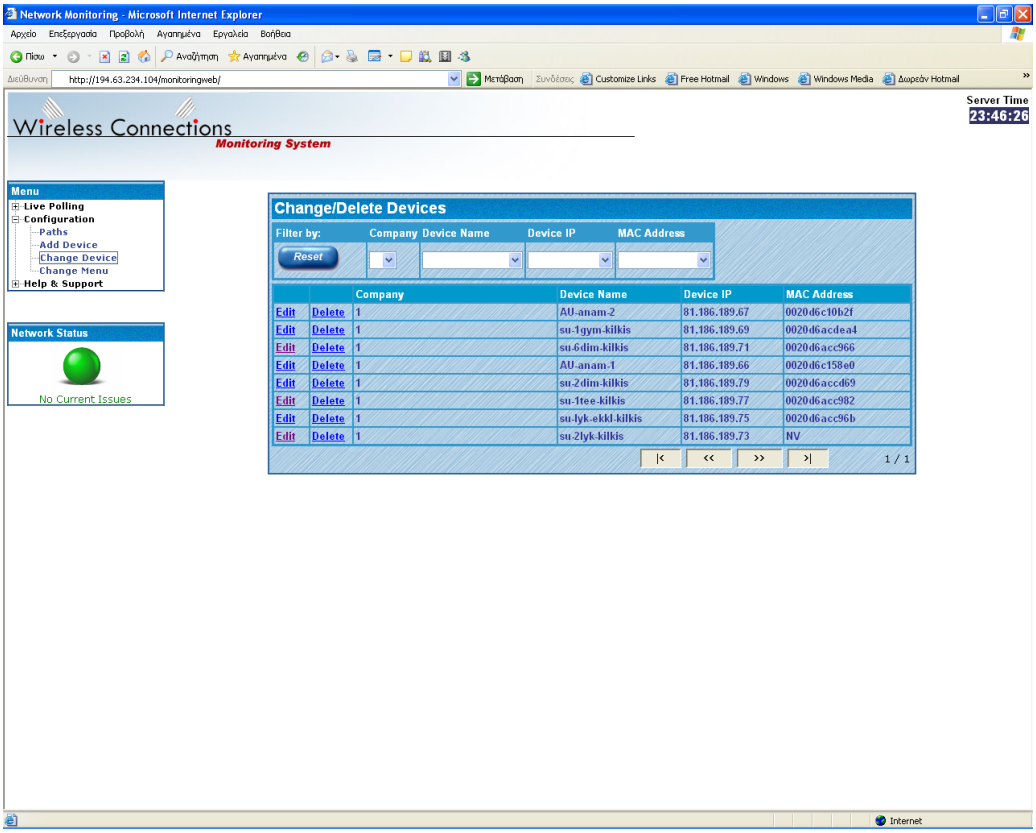
Ακολουθούν τα πρότυπα. Το Monitoring System προσφέρεται με προεπιλεγμένα πρότυπα που βασίζονται στο δένδρο διαμόρφωσης (configuration tree) του Cricket. Αυτά τα πρότυπα είναι ρυθμισμένα να λειτουργούν με συγκεκριμένες συσκευές και παρατίθενται από τον κατασκευαστή. Για να επιλέξουμε ένα πρότυπο, θα ανοίξουμε το δένδρο του κατασκευαστή που επιθυμούμε να χρησιμοποιήσουμε μέχρι να βρούμε το συγκεκριμένο όνομα συσκευής που χρειάζεται να καταγράψουμε. Πάντοτε επιλέγουμε το χαμηλοτέρου επιπέδου όνομα αρχείου στο δένδρο αρχείων και ποτέ δεν επιλέγουμε μόνο το όνομα φακέλου. Για παράδειγμα, στην περίπτωσή μας που έχουμε συσκευές SU τύπου **BreezeAccess II** της **Alvarion** τις οποίες θέλουμε να καταγράψουμε, πρέπει να επιλέξουμε το ανάλογο πρότυπο από τον κατάλογο των προτύπων (Εικόνα 6-3).



Εικόνα 6-3. Παράδειγμα καταλόγου προτύπων.

Αλλαγή συσκευών

Από το μενού συστήματος επιλέγουμε **Configuration → Change Device**. Εμφανίζεται ένα παράθυρο παρόμοιο με την Εικόνα 6-4.



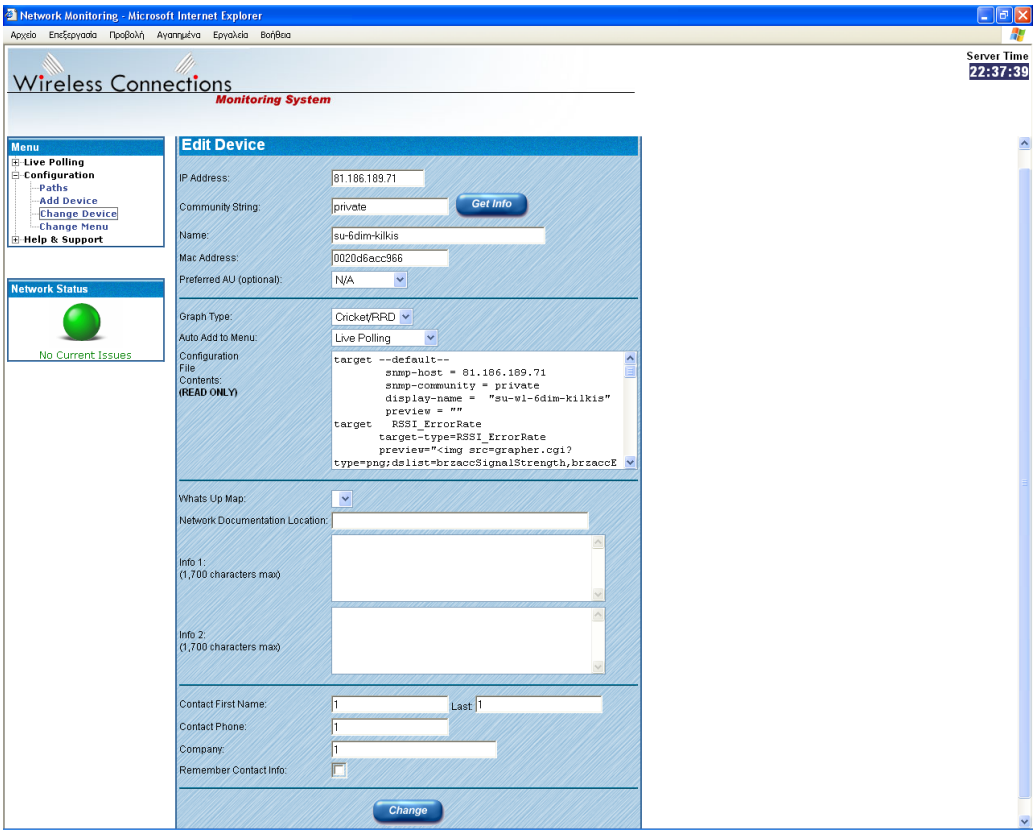
Εικόνα 6-4. Η σελίδα αλλαγής/διαγραφής συσκευών (Change/Delete Devices).

Για να επεξεργαστούμε μια συσκευή επιλέγουμε τον υπερσύνδεσμο **Edit** για τη συσκευή που επιθυμούμε να επεξεργαστούμε. Εμφανίζεται ένα παράθυρο παρόμοιο με την Εικόνα 6-5.

Μπορούμε να κάνουμε οποιοδήποτε αλλαγή χρειάζεται σε οποιοδήποτε από τα πλαίσια κειμένου. Μπορούμε να χρησιμοποιήσουμε το κουμπί **Get Info** αν επιθυμούμε να ανανεώσουμε τις πληροφορίες κατευθείαν από τη συσκευή υποθέτοντας ότι η διεύθυνση IP και η σειρά χαρακτήρων είναι σωστές.

Η μόνη περιοχή που δεν μπορούμε να αλλάξουμε είναι η **Configuration File Contents**. Αυτή είναι απεικόνιση μόνο για αναφορά και οποιεσδήποτε αλλαγές κάνουμε εδώ δε θα ενημερωθούν στο γράφημα του Cricket. Αν επιθυμούμε να αλλάξουμε τον τρόπο που αυτή η συσκευή καταγράφεται, είναι καλύτερα να προσθέσουμε τη συσκευή ως νέα συσκευή και να διαγράψουμε την υπάρχουσα συσκευή.

Άπαξ και τελειώσουμε τις αλλαγές, επιλέγουμε το κουμπί **Change** για να τις αποθηκεύσουμε.



Εικόνα 6-5. Η σελίδα επεξεργασίας συσκευής (Edit Device).

6.2.4. Αποτελέσματα δειγματοληψίας – Γραφικές παραστάσεις

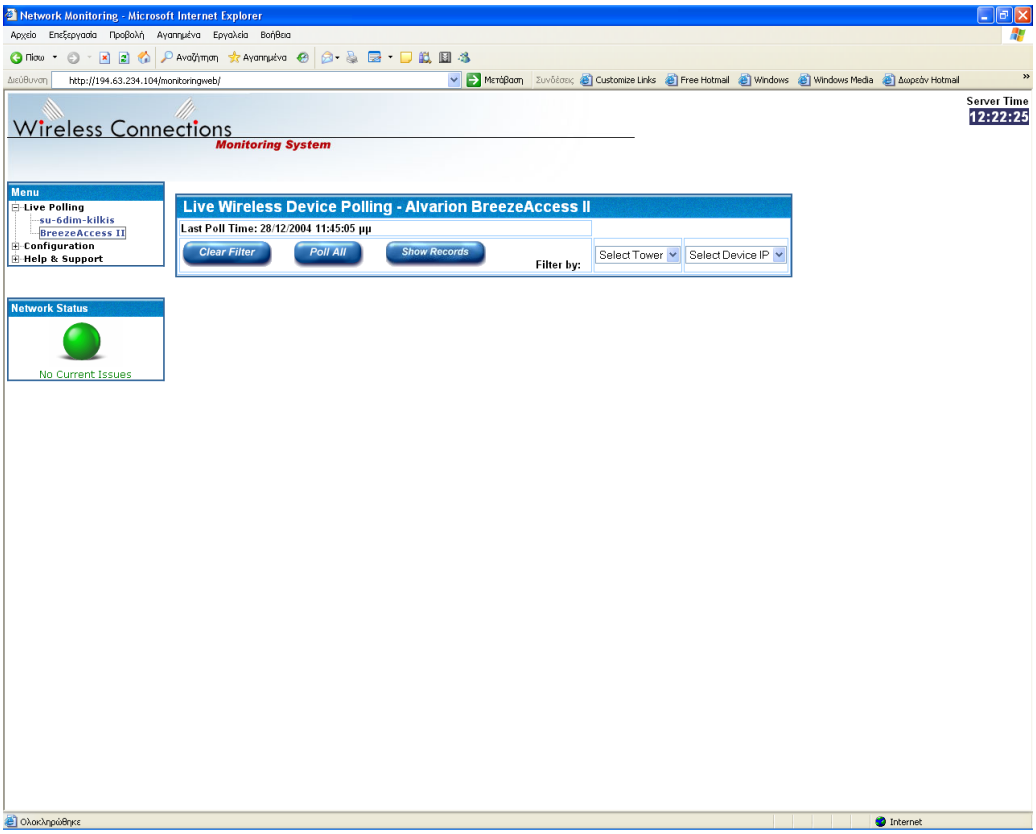
Για κάθε συσκευή που καταγράφεται, το Monitoring System μπορεί να μας δώσει συνοπτικά αποτελέσματα της καταγραφής.

Για να τα δούμε, από το μενού συστήματος επιλέγουμε **Live Polling → BreezeAccess II**. Πρέπει να δούμε το πλαίσιο διαλόγου **Live Wireless Device Polling – Alvarion BreezeAccess II** (Εικόνα 6-6).

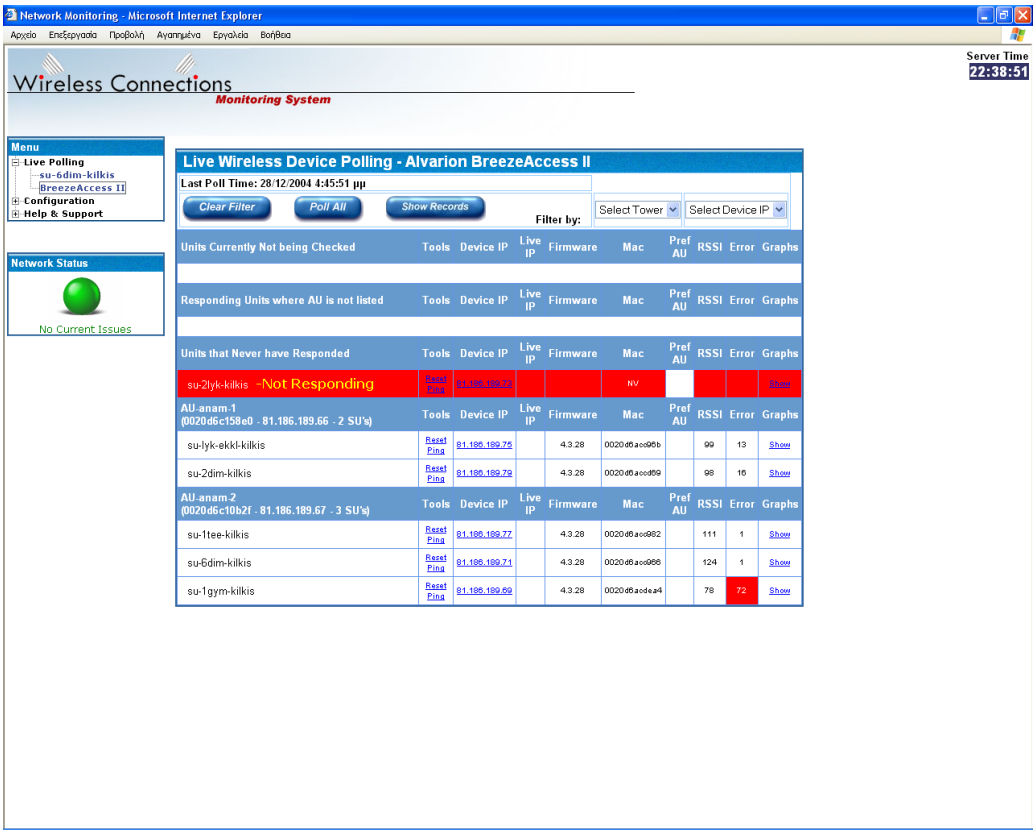
Αν θέλουμε να δούμε συγκεκριμένες μόνο συσκευές, μπορούμε από τα αντίστοιχα πλαίσια επιλογής να επιλέξουμε:

- **Tower**, δηλαδή κεντρικό αναμεταδότη (AU) οπότε θα δούμε όλες τις SU που είναι συνδεδεμένες μ' αυτόν ή
- **Device IP**, δηλαδή τερματικό σταθμό (SU), οπότε θα δούμε μόνο μία SU.

Αν θέλουμε να δούμε όλες τις συσκευές, πατάμε το κουμπί **Poll All**. Θα εμφανιστεί μια σελίδα με όλες τις μονάδες του δικτύου μας (Εικόνα 6-7).



Εικόνα 6-6. Η σελίδα επιλογών δειγματοληψίας ομάδας συσκευών.



Εικόνα 6-7. Η σελίδα αποτελεσμάτων δειγματοληψίας όλων των μονάδων του δικτύου μας.

Στη συνέχεια, μπορούμε να δούμε για κάθε συσκευή μια σειρά γραφικών παραστάσεων.

Το Monitoring System παρέχει γραφικές παραστάσεις 7 χαρακτηριστικών μεγεθών:

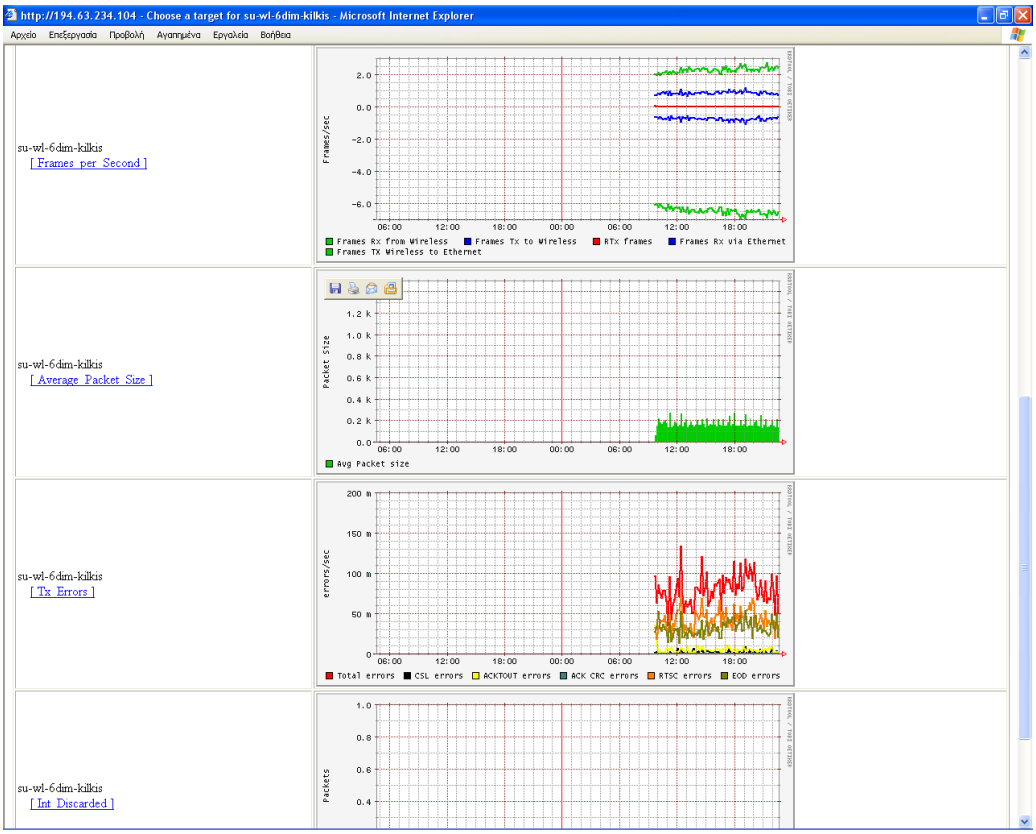
- Υστέρηση (Latency)
- Δείκτης ισχύος λαμβανομένου σήματος και ρυθμός λαθών (RSSI[4] Error Rate)
- Bytes ανά δευτερόλεπτο (Traffic Bytes per Second)
- Πλαίσια ανά δευτερόλεπτο (Frames per Second)
- Μέσο μέγεθος πακέτων (Average Packet Size)
- Λάθη κατά τη λήψη (Tx Errors)
- Εσωτερικώς απορριφθέντα πακέτα (Internally Discarded Packets)

Για να δούμε τις γραφικές παραστάσεις μιας συσκευής, στην αντίστοιχη σειρά πατάμε τον υπερσύνδεσμο **Show**. Εμφανίζεται μια σελίδα με γραφικές παραστάσεις (Εικόνα 6-8), όπου μπορούμε να δούμε τις 3 πρώτες διαθέσιμες γραφικές παραστάσεις.

Εικόνα 6-8. Γραφικές παραστάσεις Υστέρησης, RSSI και ρυθμού λαθών και Bytes ανά δευτερόλεπτο.

Αν μεταβούμε στο κάτω μέρος της σελίδας, μπορούμε να δούμε και τις υπόλοιπες 4 γραφικές παραστάσεις, όπως φαίνεται στην Εικόνα 6-9.

[4] RSSI: Received Signal Strength Indicator.

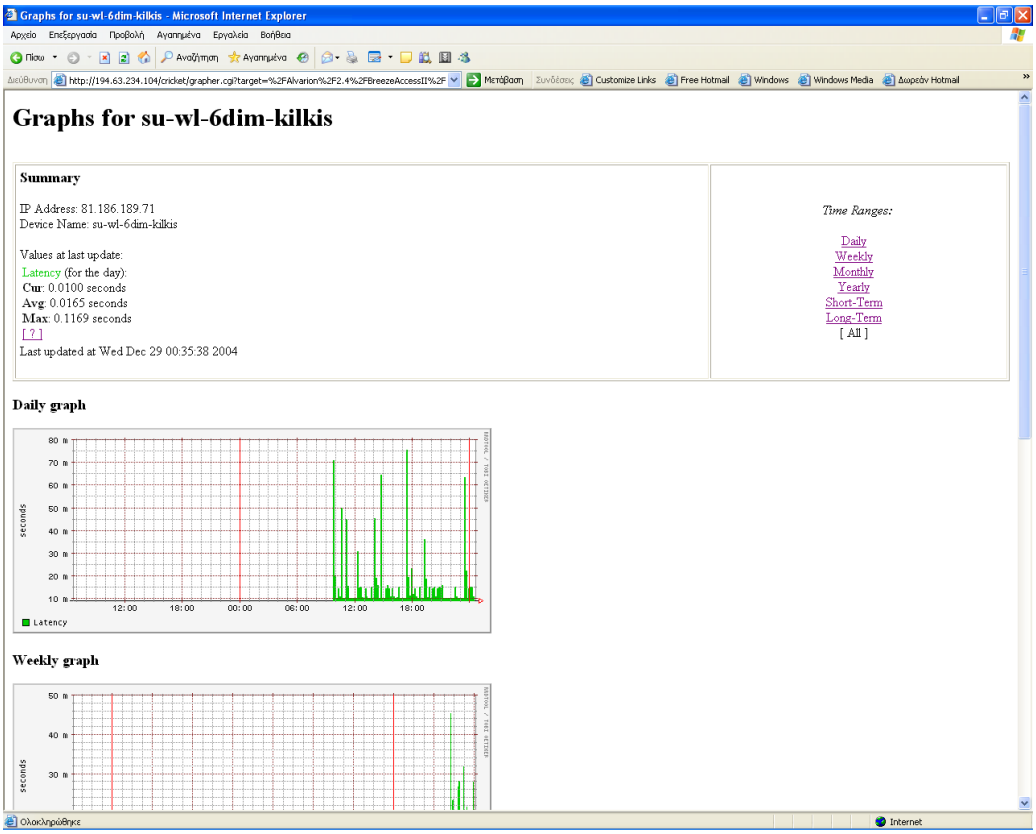


Εικόνα 6-9. Γραφικές παραστάσεις Πλαισίων ανά δευτερόλεπτο, Μέσου μεγέθους πακέτων, Tx λαθών και Πακέτων απορριφθέντων από το σύστημα.

Είναι προφανές ότι οι εμφανιζόμενες γραφικές παραστάσεις είναι ημερήσιες. Όμως, το Monitoring System παρέχει, για καθένα από τα παραπάνω 7 μεγέθη, 6 διαφορετικούς τύπους γραφικών παραστάσεων ανάλογα με τη χρονική διάρκεια καταγραφής + 1 συνολικό:

- Ημερήσιο (Daily)
- Εβδομαδιαίο (Weekly)
- Μηνιαίο (Monthly)
- Ετήσιο (Yearly)
- Βραχυπρόθεσμο (Short-term)
- Μακροπρόθεσμο (Long-term)
- Όλα (All)

Για να δούμε αυτούς τους τύπους γραφικών παραστάσεων, σε μια από τις προηγούμενες οθόνες, πατάμε στον υπερσύνδεσμο με το όνομα του μετρούμενου μεγέθους που φαίνεται στα αριστερά (π.χ. **Latency**). Εμφανίζεται μια σελίδα γραφικών παραστάσεων (Εικόνα 6-10).



Εικόνα 6-10. Γραφικές παραστάσεις ανάλογα με τη χρονική διάρκεια καταγραφής.

Στην οθόνη αυτή και από τη λίστα **Time Ranges** μπορούμε να επιλέξουμε τον τύπο γραφικής παράστασης ανάλογα με τη χρονική διάρκεια που επιθυμούμε και αμέσως αυτός εμφανίζεται στην οθόνη μας.

Τέλος, παρατηρούμε ότι στο πάνω δεξιό μέρος της σελίδας εμφανίζονται, για το συγκεκριμένο μέγεθος που παρατηρούμε, 3 στατιστικά στοιχεία:

- Τρέχουσα τιμή (Cur)
- Μέση τιμή (Avg)
- Μέγιστη τιμή (Max).

7. Σύστημα παρακολούθησης και καταγραφής Ethereal

7.1. Τι είναι το Ethereal

Το Ethereal είναι λογισμικό ανάλυσης πακέτων δικτύων (network packet analyzer). Το πρόγραμμα αυτό συλλαμβάνει πακέτα δικτύου με πληθώρα πληροφοριών γι' αυτά και δείχνει σε εξαιρετικά λεπτομερή βαθμό τις πληροφορίες του κάθε πακέτου. Τα εργαλεία αυτού του είδους στο παρελθόν ήταν είτε πολύ ακριβά, είτε ιδιόκτητα, είτε και τα δύο. Εντούτοις, με την εμφάνιση του Ethereal, όλα αυτά έχουν αλλάξει. Το Ethereal είναι λογισμικό ανοικτού κώδικα και είναι κοινά παραδεκτό ότι είναι το καλύτερο λογισμικό του συγκεκριμένου είδους.

7.1.1. Χρήσεις του Ethereal

Το Ethereal μπορεί να χρησιμοποιηθεί σε ένα μεγάλο πλήθος εφαρμογών. Έτσι:

- Οι διαχειριστές δικτύων το χρησιμοποιούν για **να ανιχνεύσουν λάθη και προβλήματα δικτύων**
- Οι μηχανικοί ασφάλειας δικτύων το χρησιμοποιούν για **να εξετάσουν τα προβλήματα ασφάλειας**
- Οι υπεύθυνοι για την ανάπτυξη εφαρμογών και κώδικα το χρησιμοποιούν για **να διορθώσουν τις εφαρμογές πρωτοκόλλων**
- Επίσης σπουδαστές και άτομα που ασχολούνται με τα δίκτυα το χρησιμοποιούν για **να μάθουν** τα ενδότερα των **πρωτοκόλλων των δικτύων**
- Εκτός από αυτά τα παραδείγματα, το Ethereal μπορεί να είναι χρήσιμο και σε πολλές άλλες περιπτώσεις.

ΠΑΡΑΤΗΡΗΣΗ: Αξίζει να σημειωθεί ότι με την ενασχόληση με το Ethereal στο περιβάλλον εργασίας, διαπιστώθηκαν κενά ασφάλειας στο εσωτερικό μας δίκτυο. Το πρόγραμμα σίγουρα θα χρησιμοποιηθεί στη συνέχεια για την ανάλυση και βελτίωση της ασφάλειας του δικτύου μας.

7.1.2. Χαρακτηριστικά γνωρίσματα του Ethereal

Τα παρακάτω είναι μερικά από τα χαρακτηριστικά γνωρίσματα του Ethereal:

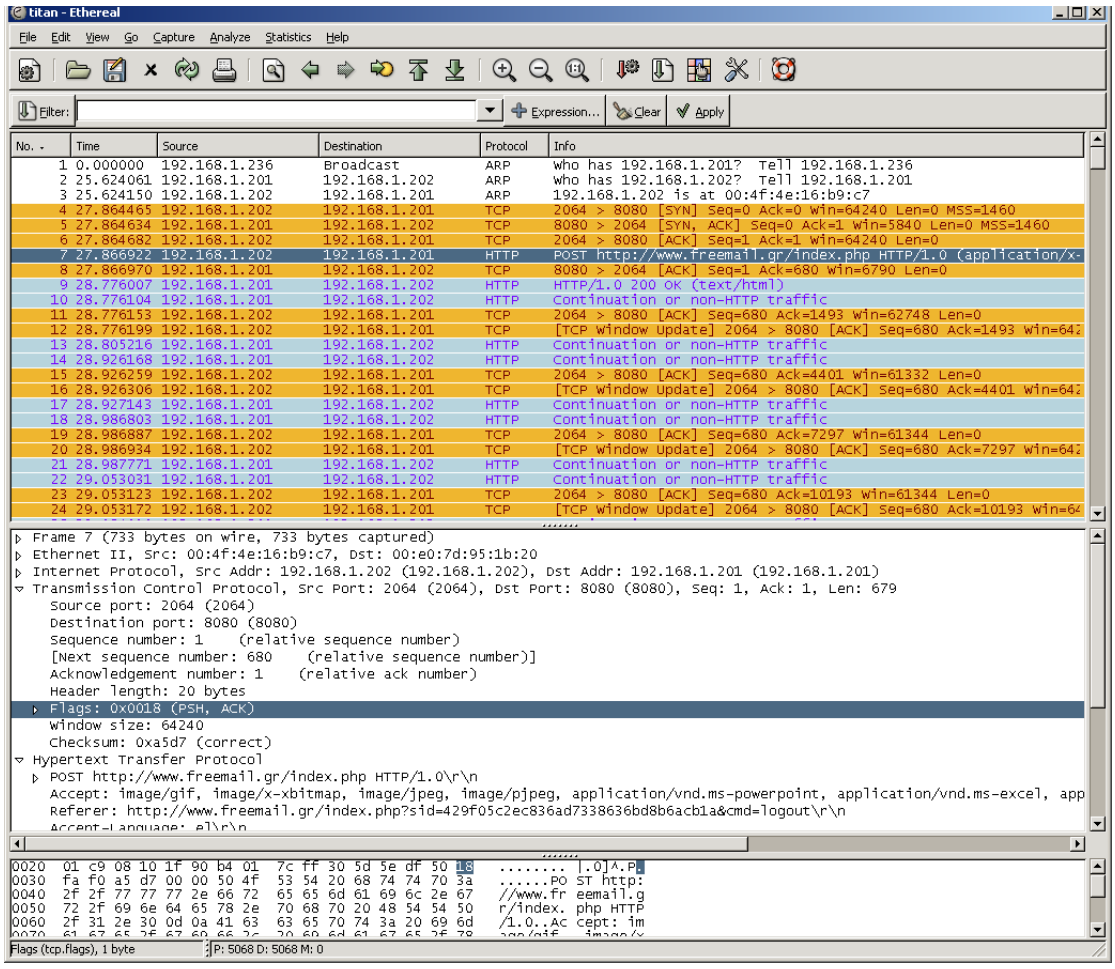
- Διαθέσιμο για **Unix-Linux** και **Windows**
- Σύλληψη **on-line** πακέτων σε ένα δίκτυο
- Προβολή των πακέτων με **λεπτομερείς πληροφορίες** πρωτοκόλλου
- **Δυνατότητα αποθήκευσης** των καταγεγραμμένων πακέτων και ανάλυσή τους αργότερα (**off - line**)
- **Εισαγωγή και εξαγωγή** πακέτων από μία πλατφόρμα λειτουργικού σε άλλη (π.χ. από Linux σε Windows)
- Δυνατότητα δημιουργίας **φίλτρων πακέτων** με πολλαπλά κριτήρια.
- **Παρακολούθηση και Αναζήτηση** των πακέτων.
- **Χρωματισμός** παρουσίασης πακέτων
- **Στατιστικές** αναφορές και **Γραφήματα**

7.1.3. Η εγκατάσταση του Ethereal

Η εγκατάσταση του Ethereal είναι σχετικά απλή. Στο περιβάλλον των **Windows** είναι μία τυπική διαδικασία εγκατάστασης προγράμματος. Αυτό όμως που πρέπει να προσεχθεί είναι ότι για να μπορεί το Ethereal να συλλαμβάνει (capture) πακέτα στο περιβάλλον των Windows (win32) πρέπει πρώτα να εγκατασταθεί ένα πρόσθετο, το **WinPcap.** Στο περιβάλλον του **Linux** το Ethereal έρχεται μέσα στα πακέτα των τελευταίων διανομών του λειτουργικού. Έτσι στη διανομή **Red Hat 9** που χρησιμοποιήσαμε (λόγω κυρίως του πρωτοκόλλου Snoop) το Ethereal είναι διαθέσιμο. Θα πρέπει όμως ο χρήστης να επιλέξει το συγκεκριμένο πακέτο για εγκατάσταση (custom setup).Οι επιλογές που υπάρχουν στο Ethereal είναι ελάχιστα διαφοροποιημένες στα δύο λειτουργικά συστήματα που το χρησιμοποιήσαμε. Στην παρουσίασή μας θα χρησιμοποιήσουμε στιγμιότυπα (screenshots) και από τις δύο πλατφόρμες των λειτουργικών συστημάτων.

7.1.4. Το περιβάλλον του Ethereal

Στην Εικόνα 7-1 βλέπουμε το κεντρικό παράθυρο του Ethereal και ενώ έχουμε ήδη συλλάβει δεδομένα από τον διακομιστή μας.



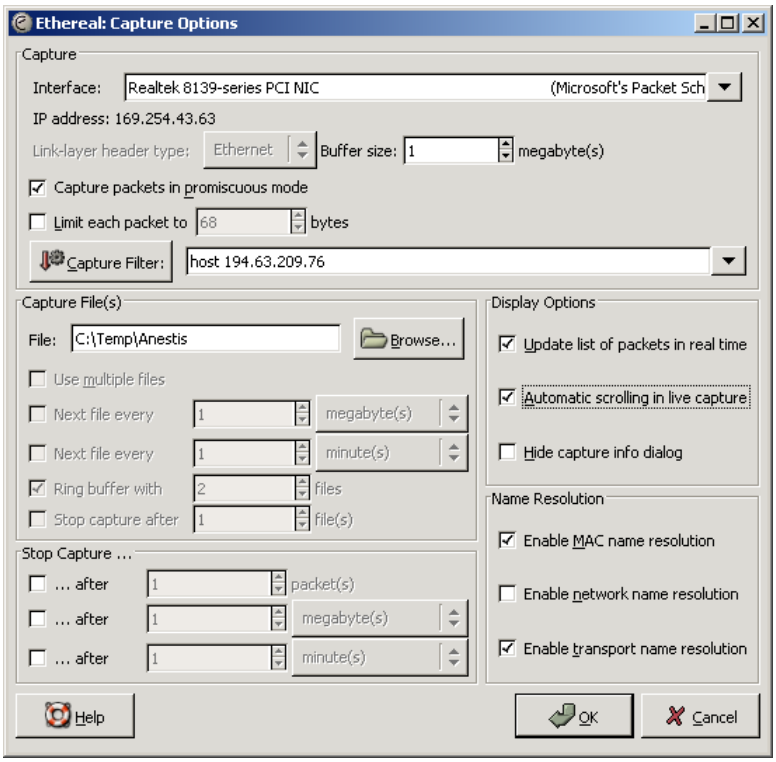
Εικόνα 7-1. Το κεντρικό παράθυρο του Ethereal.

Παρατηρούμε ότι το Ethereal καταγράφει την κίνηση σε πολλαπλά επίπεδα του μοντέλου OSI. Έτσι βλέπουμε στη μεσαία οθόνη, στοιχεία για ένα πακέτο (το επιλεγμένο) στο επίπεδο

frame, στο Ethernet, στο IP, στο TCP και στο HTTP. Είναι φανερές λοιπόν οι δυνατότητές του για ανάλυση τόσο στα υψηλά επίπεδα του μοντέλου OSI, όσο και στα χαμηλά.

Παρακάτω θα παρουσιάσουμε τις βασικές ενέργειες για τη σύλληψη των πακέτων που χρησιμοποιήσαμε στην εργασία μας. Οι επιλογές και η παραμετροποίηση του Ethereal είναι ένα θέμα αρκετά εκτεταμένο και δεν είναι σκοπός μας να το αναλύσουμε εδώ.

Για να συλλάβουμε πακέτα πηγαίνουμε στο μενού **Capture** και επιλέγουμε **Start**. Εμφανίζεται το πλαίσιο διαλόγου **Ethereal: Capture Options** (Εικόνα 7-2) (μία τυπική περίπτωση σε περιβάλλον Windows).



Εικόνα 7-2 : Το πλαίσιο διαλόγου των επιλογών σύλληψης (Capture Options).

Διακρίνουμε το πλαίσιο **Interface** όπου έχουμε το υλικό της διασύνδεσης με το δίκτυο (μία κάρτα δικτύου ηλεκτρονικού υπολογιστή).

Πολύ σημαντικό είναι το πλαίσιο **Capture Filter** όπου μπορούμε να έχουμε εκφράσεις για τη δημιουργία φίλτρων. Το τυπικό φίλτρο εδώ λέει να συλλαμβάνονται μόνο πακέτα από και προς τον διακομιστή με διεύθυνση 194.63.209.76 (είναι ο Linux Server). Η δημιουργία φίλτρων είναι από τα πλέον σημαντικά χαρακτηριστικά του Ethereal και χρησιμοποιήθηκε κατά κόρον στην παρούσα εργασία.

Στο πλαίσιο **File** μπορούμε να δηλώσουμε το αρχείο στο οποίο θα αποθηκευτούν τα δεδομένα των μετρήσεών μας. Αυτό είναι επίσης πολύ σημαντικό. Χρησιμοποιήσαμε την αποθήκευση για τα δεδομένα (πακέτα) που συλλέγαμε με το Ethereal σε Linux περιβάλλον και δουλέψαμε τα αρχεία αυτά στο Ethereal για Windows.

Οι υπόλοιπες επιλογές είναι σχετικά απλές και σχετίζονται κυρίως με την προβολή των στοιχείων.

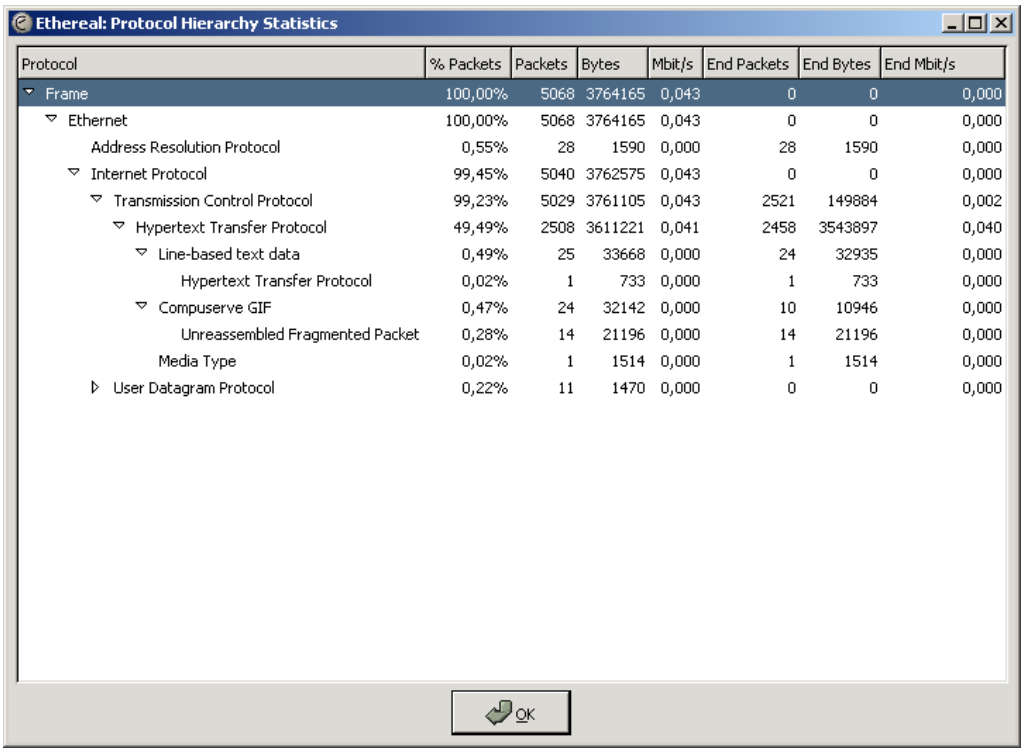
Μία σημαντική παρατήρηση είναι η διαφορά του **Capture Filter** από το **Display Filter**. Το πρώτο έχει σχέση με τη σύλληψη πακέτων. Όλα τα υπόλοιπα πακέτα τα αγνοεί και συλλαμβάνει μόνο αυτά που περνούν από το συγκεκριμένο φίλτρο. Αντίθετα το Display Filter συλλαμβάνει όλα τα πακέτα, όμως προβάλλει μόνο αυτά που περνούν από το φίλτρο.

Βλέποντας προσεκτικά την αρχική εικόνα του Ethereal μπορούμε να παρατηρήσουμε τα εξής:

- Στην πρώτη οθόνη στις στήλες βλέπουμε τον αύξοντα αριθμό του πακέτου, τον χρόνο από τη στιγμή της έναρξης της σύλληψης πακέτων, την προέλευση και τον προορισμό, το πρωτόκολλο μεταφοράς και τέλος τις αναλυτικές πληροφορίες του πακέτου.
- Στην επόμενη οθόνη εμφανίζονται οι αναλυτικές πληροφορίες του επιλεγμένου πακέτου στα διάφορα επίπεδα του μοντέλου OSI όπως ήδη αναφέρθηκε πιο πριν.
- Τέλος, η τρίτη οθόνη δίνει μία δεκαεξαδική προβολή του πακέτου (Hex Content - View).

Οι βασικές δυνατότητες του προγράμματος όσον αφορά τη σύλληψη και την έξοδο και σε σχέση με τις ανάγκες για τη συγκεκριμένη εφαρμογή είναι οι παρακάτω:

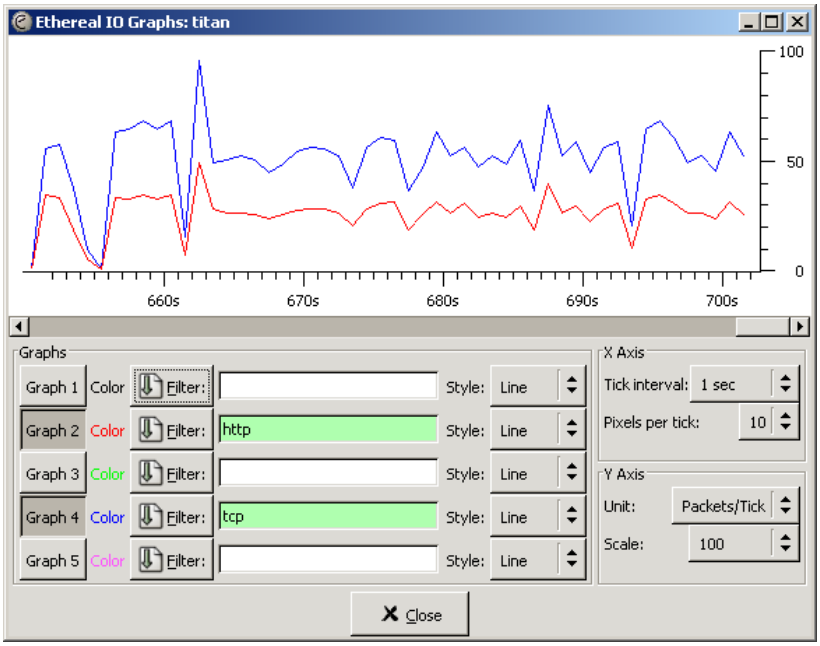
- Δυνατότητα χρωματισμού τύπου πρωτοκόλλου. Μπορούμε να βλέπουμε τα FTP πακέτα σε άλλο χρώμα foreground και background από τα HTTP. Αυτές οι επιλογές φαίνονται τόσο στην αρχική εικόνα, όσο και στα αποτελέσματα των μετρήσεων που έχουμε πραγματοποιήσει (Colorize).
- Δημιουργία στατιστικών στοιχείων για τη διάρκεια λειτουργίας του προγράμματος σε κατάσταση σύλληψης πακέτων (Summary). Στιγμιότυπα αυτής της δυνατότητας βρίσκονται στο κεφάλαιο των μετρήσεων.
- Επίσης, προβολή των πακέτων με μία ιεράρχηση των πρωτοκόλλων (Protocol Hierarchy Statistics) σύμφωνα με το μοντέλο OSI. Μία τέτοια οθόνη βλέπουμε στην Εικόνα 7-3 για την περίπτωση των πακέτων του διακομιστή του δικτύου μας. Αξίζει να παρατηρήσουμε το ίδιο επίπεδο του TCP με το UDP.



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	5068	3764165	0,043	0	0	0,000
Ethernet	100,00%	5068	3764165	0,043	0	0	0,000
Address Resolution Protocol	0,55%	28	1590	0,000	28	1590	0,000
Internet Protocol	99,45%	5040	3762575	0,043	0	0	0,000
Transmission Control Protocol	99,23%	5029	3761105	0,043	2521	149884	0,002
Hypertext Transfer Protocol	49,49%	2508	3611221	0,041	2458	3543897	0,040
Line-based text data	0,49%	25	33668	0,000	24	32935	0,000
Hypertext Transfer Protocol	0,02%	1	733	0,000	1	733	0,000
Compuserve GIF	0,47%	24	32142	0,000	10	10946	0,000
Unreassembled Fragmented Packet	0,28%	14	21196	0,000	14	21196	0,000
Media Type	0,02%	1	1514	0,000	1	1514	0,000
User Datagram Protocol	0,22%	11	1470	0,000	0	0	0,000

Εικόνα 7-3. Στατιστικά ιεραρχίας πρωτοκόλλων.

Επίσης υπάρχει δυνατότητα δημιουργίας γραφικών παραστάσεων και παραμετροποίησής τους (**IO Graphs**) (Εικόνα 7-4).



Εικόνα 7-4. Γραφική παράσταση κίνησης πακέτων.

Εδώ παρατηρούμε τη δυνατότητα φίλτρων για διάφορα πρωτόκολλα (HTTP κόκκινο και TCP μπλε). Γραφικές παραστάσεις υπάρχουν στο κεφάλαιο των αποτελεσμάτων μέτρησης.

Μπορούμε επίσης να δούμε κι άλλες γραφικές παραστάσεις και στατιστικά στοιχεία. Καλό είναι να επισημάνουμε εδώ ότι οι επιλογές στο περιβάλλον των Windows είναι σαφώς περισσότερες. Αυτός είναι και ο λόγος για τον οποίο οι μετρήσεις που έχουν ληφθεί σε περιβάλλον Linux αναλύθηκαν με το πρόγραμμα στο περιβάλλον των Windows. Το αρχείο στο οποίο αποθηκεύονται οι μετρήσεις με το Ethereal στο Linux είναι αναγνώσιμο από την εφαρμογή στο περιβάλλον των Windows.

7.2. Σχεδιασμός φίλτρων σύλληψης πακέτων στο Ethereal

Το πιο δυνατό σημείο του Ethereal είναι η δημιουργία φίλτρων για τη σύλληψη και προβολή πακέτων σε διάφορα πρωτόκολλα [5]. Ήδη έχουμε αναφερθεί λίγο στα φίλτρα πιο πριν. Θα εμβαθύνουμε όμως περισσότερο στο σημείο αυτό, τόσο όσο χρειάζεται για τις ανάγκες της εργασίας αυτής.

7.2.1. Ορισμός διακομιστή για σύλληψη πακέτων

Μπορούμε να ορίσουμε εκφράσεις μέσα σε ένα φίλτρο με το οποίο θα συλλέγονται μόνο πακέτα που αφορούν ένα διακομιστή. Μάλιστα μπορούμε να ορίσουμε αν τα πακέτα θα είναι εισερχόμενα ή εξερχόμενα. Ο διακομιστής μπορεί να οριστεί είτε με το όνομά του, είτε με την IP διεύθυνσή του. Αυτό λόγω της δυνατότητας επίλυσης του ονόματος (naming resolution) που παρέχουν τα Windows που μπορεί να μετατραπεί μία IP διεύθυνση στο hostname που συσχετίζεται με αυτήν (π.χ. η 194.63.238.249 σε https://gallery.sch.gr/).

Η σύνταξη για φιλτράρισμα βάσει διακομιστή

Σύνταξη	Περιγραφή
host host	host είναι είτε η IP είτε το όνομα
src host host	Σύλληψη όλων των πακέτων όπου ο host είναι η πηγή
dst host host	Σύλληψη όλων των πακέτων όπου ο host είναι ο προορισμός
Παραδείγματα	
host 10.10.10.10	Σύλληψη όλων των πακέτων από τον 10.10.10.10
src host 194.63.209.76	Σύλληψη όλων των πακέτων όπου ο **194.63.209.76** είναι η πηγή
dst host titan	Σύλληψη όλων των πακέτων όπου ο **titan** είναι ο προορισμός

7.2.2. Ορισμός θύρας για φιλτράρισμα

Μπορούμε να ορίσουμε εκφράσεις μέσα σε ένα φίλτρο με το οποίο θα συλλέγονται μόνο πακέτα που προέρχονται ή κατευθύνονται σε μια συγκεκριμένη θύρα του συστήματος.

Σύνταξη για φιλτράρισμα θύρας

Σύνταξη	Περιγραφή
port port	Σύλληψη όλων των πακέτων όπου το port είναι είτε πηγή είτε προορισμός
src port port	Σύλληψη όλων των πακέτων όπου το port είναι η πηγή
dst port port	Σύλληψη όλων των πακέτων όπου το port ο προορισμός
Παραδείγματα	
port 80	Σύλληψη όλων των πακέτων όπου η θύρα 80 είναι είτε πηγή είτε προορισμός
src port 20	Σύλληψη όλων των πακέτων που έρχονται από η θύρα 20 δηλαδή όλων των FTP data πακέτων που λαμβάνονται
dst port 23	Σύλληψη όλων των πακέτων που πηγαίνουν στη θύρα 23 δηλαδή όλων των telnet πακέτων που αποστέλλονται

7.2.3. Ορισμός πρωτοκόλλου για φιλτράρισμα

Μπορούμε να ορίσουμε εκφράσεις μέσα σε ένα φίλτρο με το οποίο θα συλλέγονται μόνο πακέτα που αναφέρονται σε ένα συγκεκριμένο πρωτόκολλο. Αυτά μπορούν να βασίζονται είτε στο Ethernet (Ethernet Based), είτε στο Internet (IP Based).

Βάσει Ethernet:

Σύνταξη	Περιγραφή
ether proto \[primitive name]	
Παραδείγματα	
ether proto \ip ή μόνο **ip**	Σύλληψη όλων των ip πακέτων
ether proto \arp ή μόνο **arp**	address resolution protocol πακέτων
ether proto \rarp ή μόνο **rarp**	Σύλληψη των reverse arp πακέτων

Βάσει IP:

Σύνταξη	Περιγραφή
ip proto \[primitive name]	
Παραδείγματα	
ip proto \tcp ή μόνο **tcp**	Σύλληψη όλων των TCP segments (πακέτων)
ip proto \udp ή μόνο **udp**	Σύλληψη όλων των UDP πακέτων
ip proto \icmp ή μόνο **icmp**	Σύλληψη όλων των ICMP πακέτων

Το Ethereal υποστηρίζει όλα τα γνωστά και συνήθως χρησιμοποιούμενα πρωτόκολλα επικοινωνίας και πολύ περισσότερα. Δίνει τη δυνατότητα ενεργοποίησης και απενεργοποίησης της σύλληψης, των πρωτοκόλλων αυτών. Επειδή όμως έχει επικρατήσει η εργασία με τα φίλτρα, δε χρησιμοποιήσαμε αυτόν τον τρόπο, αλλά τα φίλτρα. Είναι πιο απλό να επιτρέψει κανείς δύο-τρία πρωτόκολλα παρά να αποκλείσει δεκάδες ή εκατοντάδες.

Υπάρχουν και άλλες δυνατότητες για το φιλτράρισμα οι οποίες όμως ξεφεύγουν από τον σκοπό της εργασίας αυτής. Αυτό που πρέπει να αναφέρουμε είναι ότι μπορούν να γίνουν συνδυασμοί των παραπάνω φίλτρων με τη χρήση γνωστών λογικών εκφράσεων π.χ. && (and), || (or), not κ.λπ. Έτσι επιτυγχάνουμε να συλλέξουμε μόνο τα πακέτα που μας ενδιαφέρουν όπως θα δούμε και παρακάτω.

Παράδειγμα	
src host titan **&& port** 20	Λήψη πακέτων από τον titan όπου η θύρα είναι 20 δηλ. FTP data.

7.2.4. Παρατηρήσεις εκφράσεων φιλτραρίσματος – μετρήσεων

Στο σημείο αυτό πρέπει να αναφέρουμε ότι, ελλείψει της δυνατότητας ορισμού φίλτρου για πρωτόκολλα ανωτέρου επιπέδου (HTTP, FTP), το Ethereal μάς δίνει την εναλλακτική λύση να ορίσουμε ένα φίλτρο και να το «**αποκωδικοποιήσουμε**» ως ένα πρωτόκολλο με την επιλογή **Decode As**… Έτσι μπορούμε να του πούμε το «tcp and port 8080» να φαίνεται ως HTTP ή το «tcp and port 21» να φαίνεται ως FTP.

Στην εργασία μας τον σπουδαιότερο ρόλο στις μετρήσεις με το Ethereal έπαιξε η μεταφόρτωση (downloading) αρχείων με FTP. Στον Linux Server που στήθηκε (IP 194.63.209.76) εγκαταστάθηκαν τόσο HTTP Server (Apache), όσο και FTP Server. Η κίνηση που προκαλούσαμε με τη μεταφόρτωση σελίδων ήταν σχετικά μικρή. Οπότε το βάρος έπεσε στο FTP με τη μεταφόρτωση μικρών, μεσαίων και μεγάλων αρχείων. Στις μετρήσεις μας αυτό που μας ενδιέφερε ήταν τα δεδομένα με το FTP, δηλαδή τα FTP DATA. Αυτό που παρατηρήσαμε και το επιβεβαιώσαμε και με αντίστοιχη έρευνα και αναζήτηση πληροφοριών στο Διαδίκτυο είναι ότι το FTP DATA δε χρησιμοποιεί πάντα τη θύρα 20 αλλά και άλλες θύρες, μέσω των οποίων γινόταν η διακίνηση των συγκεκριμένων πακέτων (πάντα πάνω στο TCP πρωτόκολλο).

Αποτέλεσμα αυτών ήταν να κάνουμε τις μετρήσεις ως εξής: ξεκινούσαμε τη μεταφόρτωση ενός αρχείου χωρίς φίλτρο. Μόλις ξεκινούσε η μεταφόρτωση, κάναμε παύση. Παρατηρούσαμε τη θύρα στην οποία γινόταν η επικοινωνία. Θέταμε το κατάλληλο φίλτρο με τη θύρα και αποκωδικοποιούσαμε την έκφραση αυτή ως FTP DATA. Έπειτα συνεχίζαμε τη μεταφόρτωση του αρχείου. Με τον τρόπο αυτό απομονώναμε τα FTP DATA που μας ενδιέφεραν. Αυτό γινόταν για κάθε μέτρηση FTP είτε με ενεργό, είτε με ανενεργό το module του πρωτοκόλλου Snoop.

8. Μετρήσεις – Γραφικές παραστάσεις

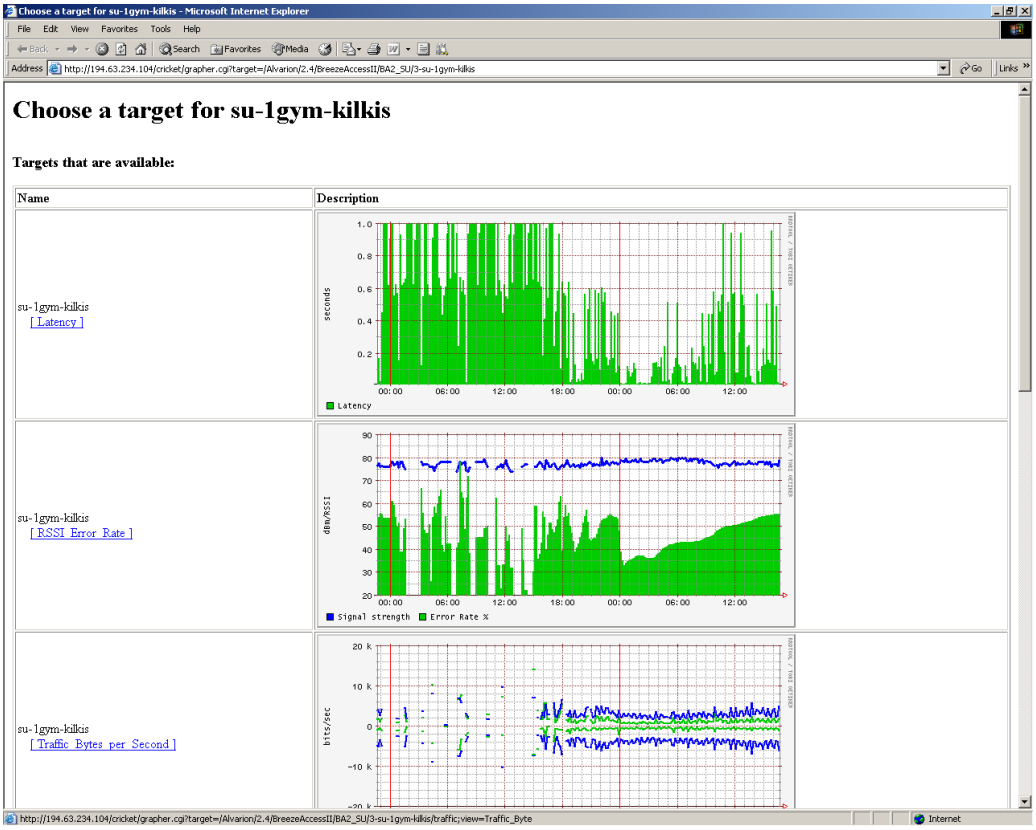
8.1. Σ+2ο επίπεδο του μοντέλου OSI (Monitoring System)

Για την πραγματοποίηση των μετρήσεων εκτελέστηκε η μεταφόρτωση αρχείων και συγκεκριμένα ενός μεγάλου αρχείου, του Windows XP SP2 ελληνικής έκδοσης, μεγέθους περίπου 260 MB, και στη συνέχεια λήφθηκαν γραφικές παραστάσεις και συνοπτικά στατιστικά στοιχεία από το Monitoring System. Το λογισμικό αυτό λειτουργεί στο 2ο επίπεδο του μοντέλου OSI (επίπεδο γραμμής δεδομένων).

Η λήψη του αρχείου εκτελέστηκε τρεις φορές, ως εξής:

1. Λήψη από τον δικτυακό τόπο της Microsoft με κανονικές καιρικές συνθήκες
2. Λήψη από τον δικτυακό τόπο της Microsoft με χιονόπτωση
3. Μετάδοση από κόμβο σε κόμβο (δηλ. από διακομιστή ενός σχολείου σε σταθμό εργασίας άλλου σχολείου), πάντα εντός της ασύρματης νησίδας.

Κατά τη διεξαγωγή των μετρήσεων, διαπιστώθηκε βλάβη σε έναν κόμβο και συγκεκριμένα στο 1ο Γυμνάσιο. Στην Εικόνα 8-1 που αφορά αυτό το σχολείο είναι φανερό ότι ο ρυθμός μετάδοσης είναι σχεδόν μηδενικός.



Εικόνα 8-1. Γραφικές παραστάσεις κόμβου που παρουσιάζει βλάβη.

Έγιναν μετρήσεις για τα παρακάτω μεγέθη:

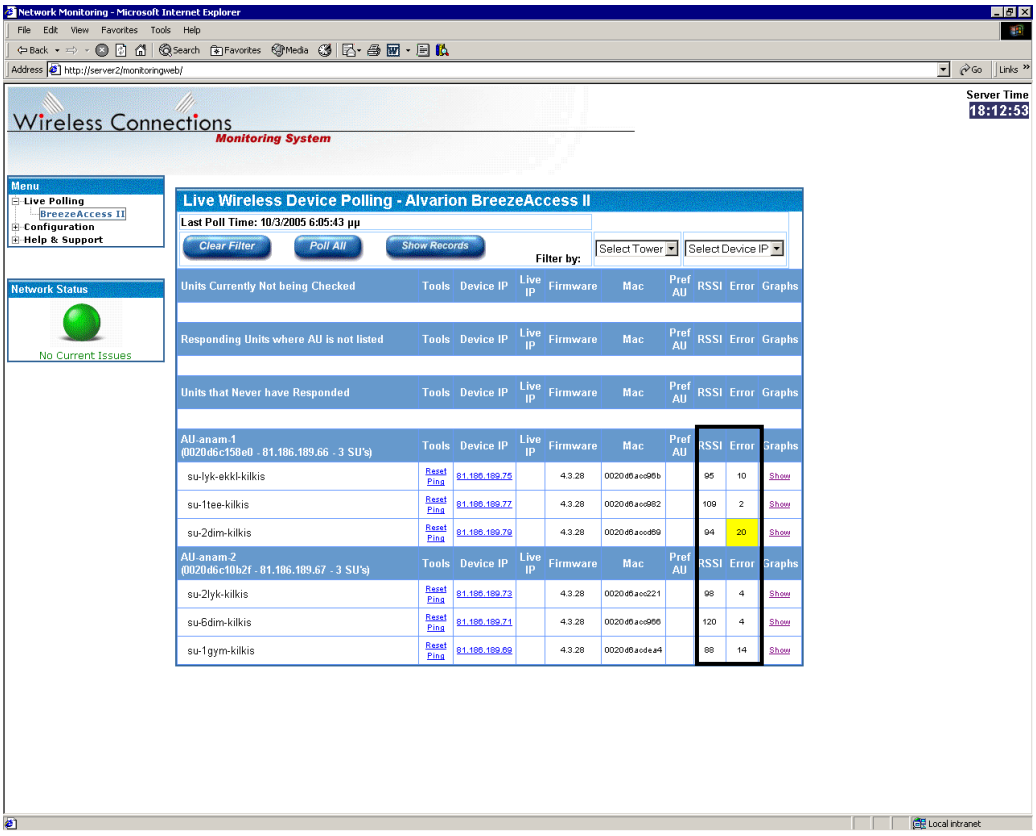
- Δείκτης ισχύος λαμβανομένου σήματος και ρυθμός λαθών (RSSI Error Rate)
- Bytes ανά δευτερόλεπτο (Traffic Bytes per Second)
- Πλαίσια ανά δευτερόλεπτο (Frames per Second)

- Μέσο μέγεθος πακέτων (Average Packet Size)
- Λάθη κατά τη λήψη (Tx Errors)

Αυτές παρουσιάζονται αναλυτικά στις επόμενες ενότητες.

8.1.1. Δείκτης ισχύος λαμβανομένου σήματος και ρυθμός λαθών (RSSI Error Rate)

Ο δείκτης ισχύος λαμβανόμενου σήματος (Received Signal Strength Indicator, RSSI) είναι ένας αυθαίρετος δείκτης για τον οποίο η κατασκευάστρια εταιρεία Wireless Connections προτείνει ως ελάχιστη αποδεκτή τιμή το 90. Ανατρέχοντας σε έναν ει δυνατόν συγκεντρωτικό πίνακα για όλους τους τερματικούς σταθμούς του δικτύου, παρατηρούμε ότι αυτός δίνεται από την Εικόνα 6-7. Μια πιο πρόσφατη μέτρηση φαίνεται στην Εικόνα 8-2.



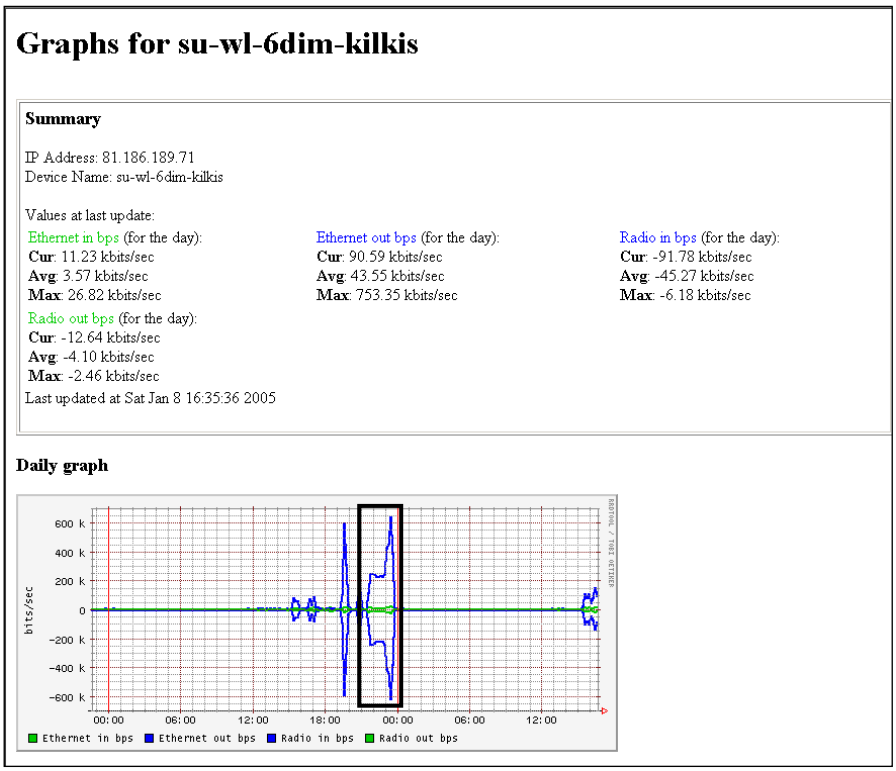
Εικόνα 8-2. Δείκτες ισχύος λαμβανομένου σήματος (RSSI) και λάθη (Error) για όλες τις μονάδες του δικτύου μας.

Παρατηρούμε ότι στους 5 σταθμούς οι τιμές του RSSI είναι σταθερά πάνω από 90 και μόνο στο 1ο Γυμνάσιο είναι οριακά παρακάτω (88). Αυτό οφείλεται στο ότι το 1ο Γυμνάσιο είναι το σχολείο που απέχει περισσότερο από οποιοδήποτε άλλο από τον κεντρικό κόμβο, όπως φαίνεται και στον χάρτη (Εικόνα 5-2).

Όσον αφορά τον ρυθμό λαθών (Error), στην ίδια εικόνα παρατηρούμε ότι διατηρείται σε χαμηλά επίπεδα. Μάλιστα επισημαίνεται με κίτρινο χρώμα η μεγαλύτερη τιμή αυτού του μεγέθους που τυχαίνει να αφορά το 2ο Δημοτικό.

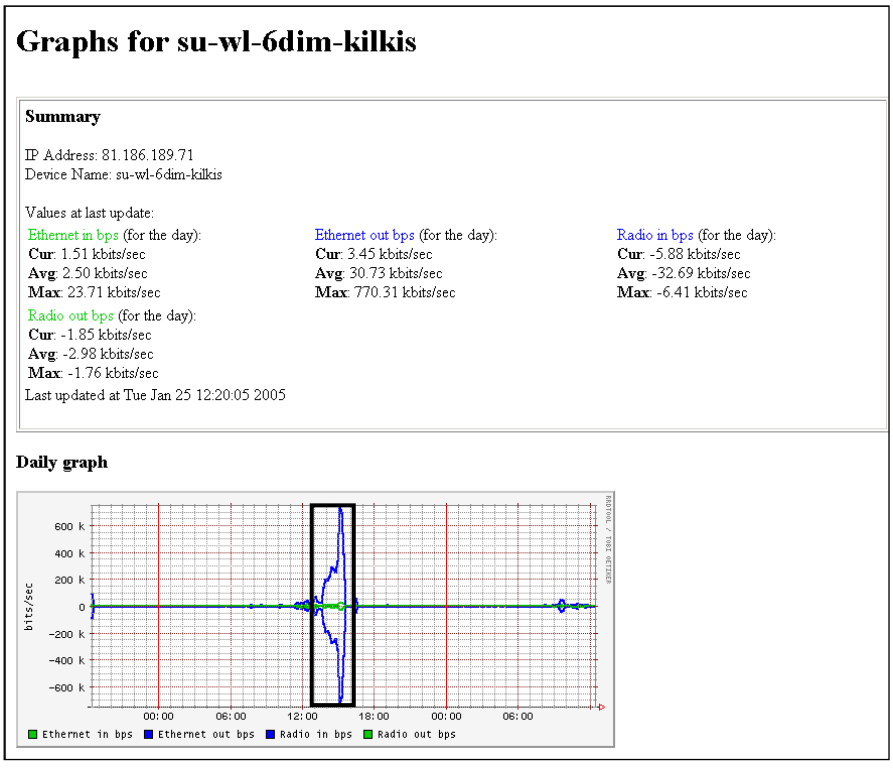
8.1.2. Bytes ανά δευτερόλεπτο (Traffic Bytes per Second)

Η γενική εικόνα του δικτύου είναι πολύ ικανοποιητική. Οι ρυθμοί μετάδοσης παραμένουν υψηλοί (αγγίζουν και ενίοτε ξεπερνούν τα 800 Kbps) (Εικόνα 8-3).



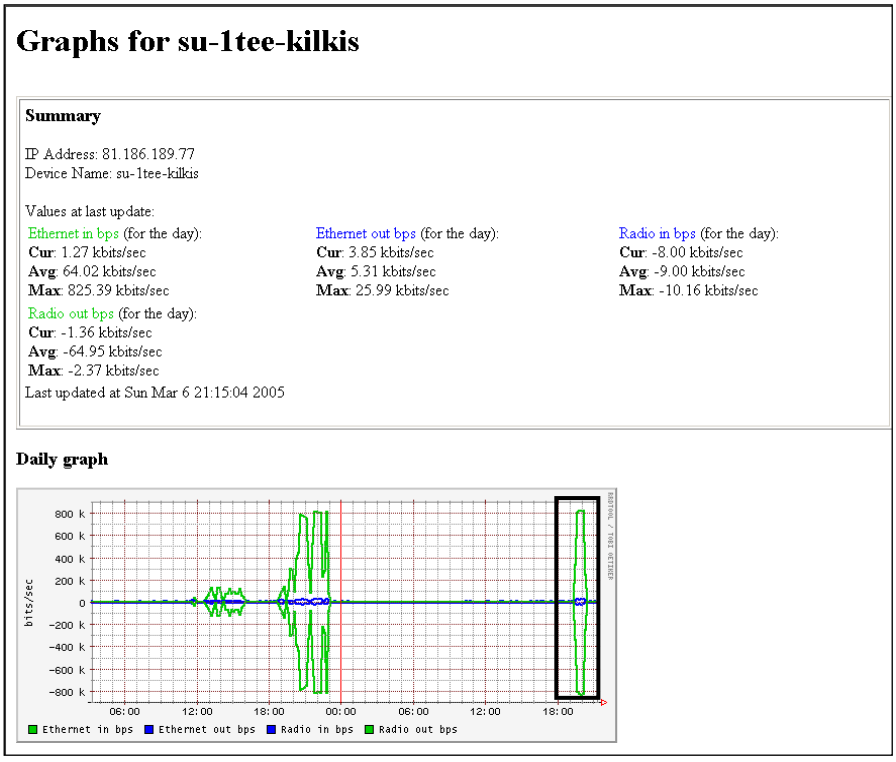
Εικόνα 8-3. Γραφική παράσταση ρυθμού μετάδοσης (bytes/sec) με κανονικές καιρικές συνθήκες.

Η χιονόπτωση επηρεάζει σαφώς τον ρυθμό μετάδοσης χωρίς να είναι απαγορευτική για τη λειτουργία του δικτύου η οποία κρίνεται ικανοποιητική (Εικόνα 8-4)

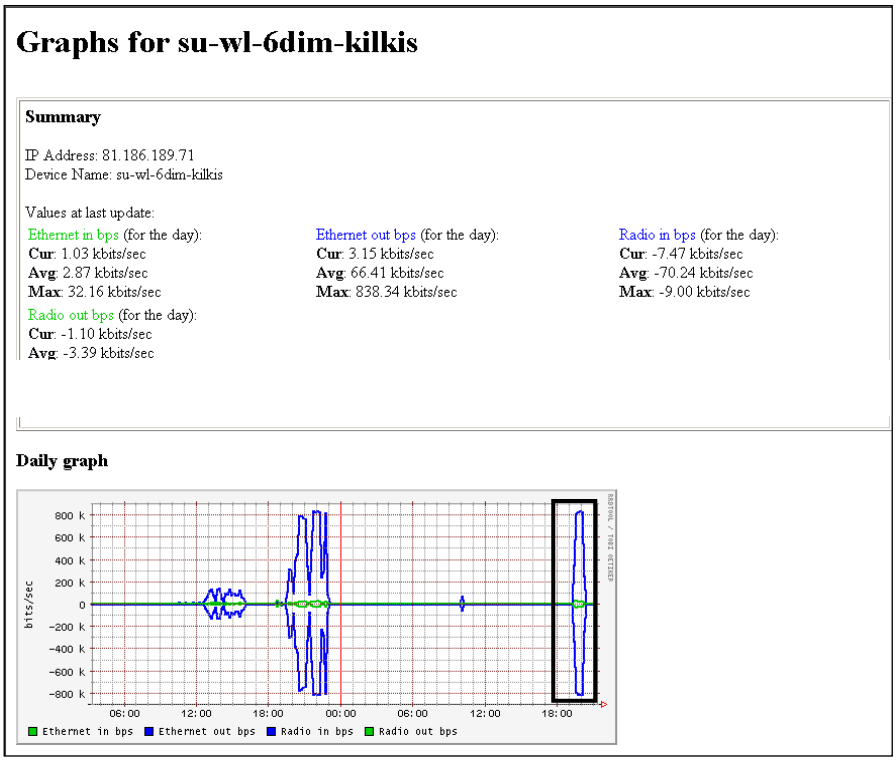


Εικόνα 8-4. Γραφική παράσταση ρυθμού μετάδοσης (bytes/sec) με χιονόπτωση.

Στην περίπτωση της μετάδοσης από σχολείο σε σχολείο, παρατηρούμε την απόλυτη αντιστοιχία των γραφικών παραστάσεων στις επιλεγμένες περιοχές που συνεπάγεται την ελάχιστη απώλεια δεδομένων (Εικόνα 8-5 και Εικόνα 8-6).



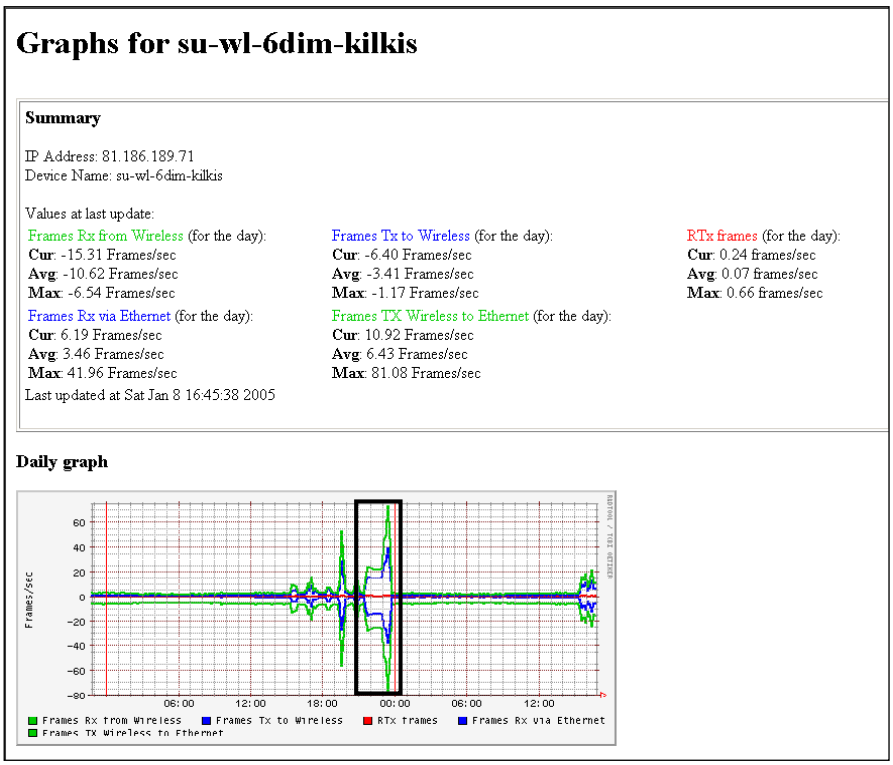
Εικόνα 8-5. Γραφική παράσταση ρυθμού μετάδοσης (bytes/sec) κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του πομπού.



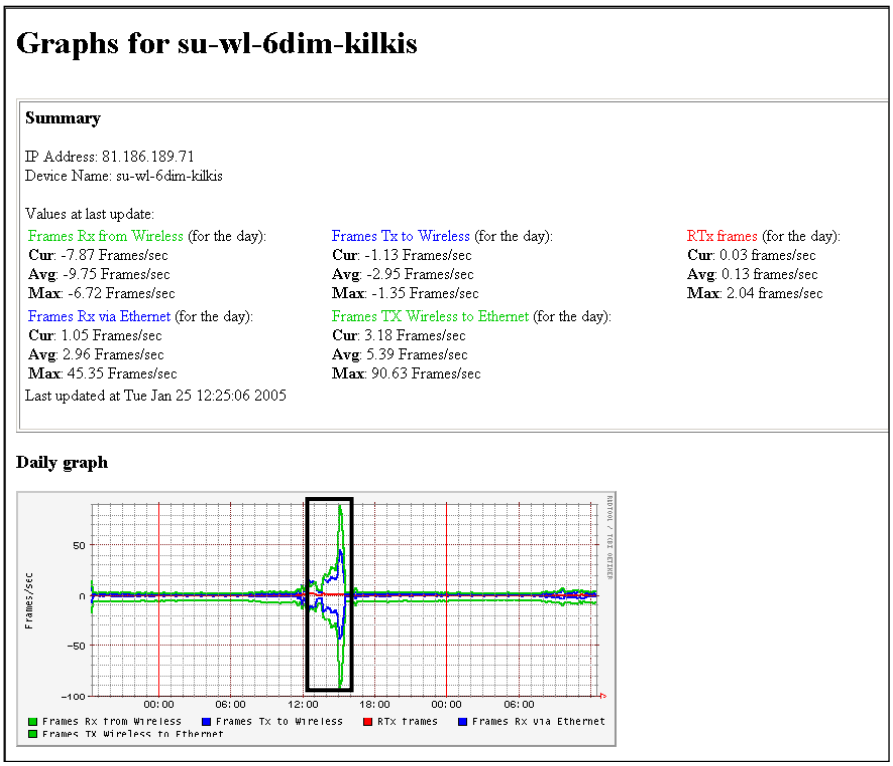
Εικόνα 8-6. Γραφική παράσταση ρυθμού μετάδοσης (bytes/sec) κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του δέκτη.

8.1.3. Πλαίσια ανά δευτερόλεπτο (Frames per Second)

Και πάλι είναι φανερή η επίδραση της χιονόπτωσης στον ρυθμό μετάδοσης frames/sec.

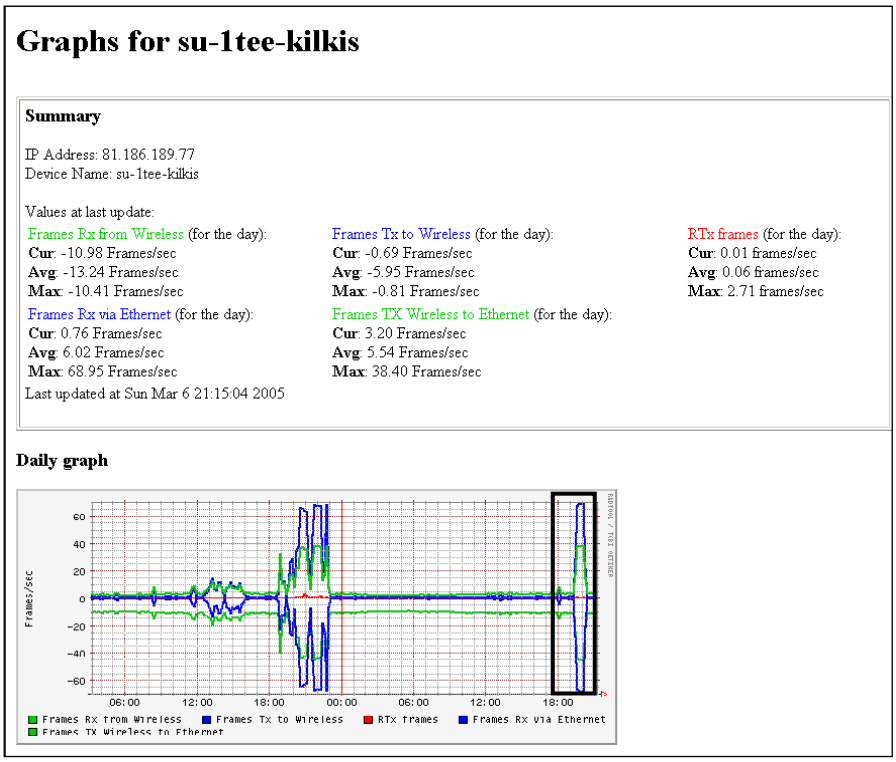


Εικόνα 8-7. Γραφική παράσταση ρυθμού μετάδοσης frames/sec με κανονικές καιρικές συνθήκες.

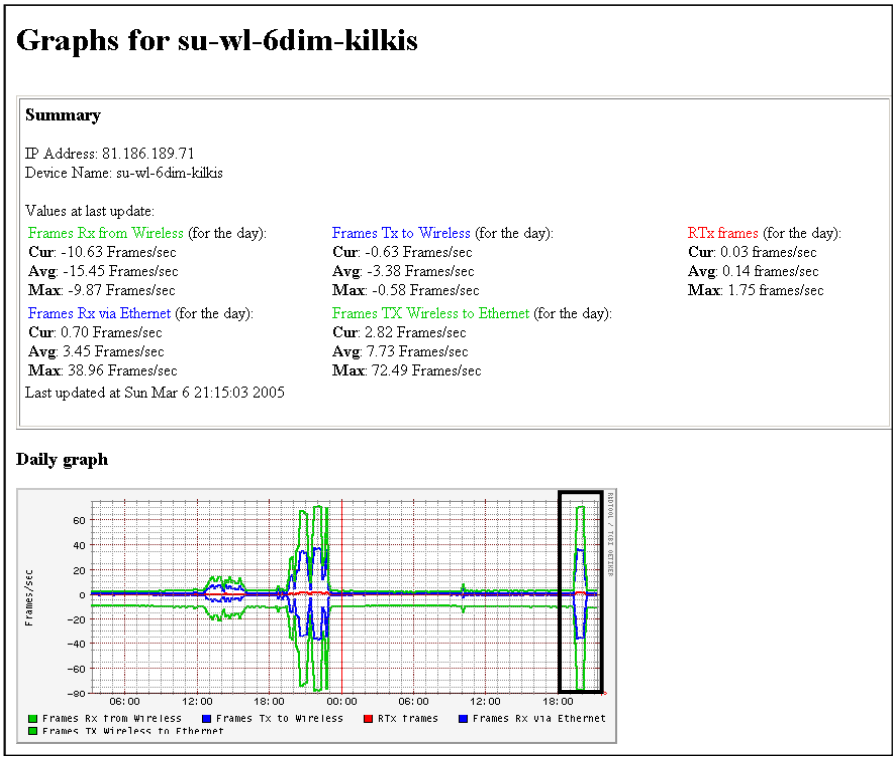


Εικόνα 8-8. Γραφική παράσταση ρυθμού μετάδοσης frames/sec με χιονόπτωση.

Η αντιστοιχία των ρυθμών μετάδοσης στην αποστολή και λήψη των πλαισίων είναι φανερή στις επιλεγμένες περιοχές. Πομπός και δέκτης συγχρονίζονται σε πολύ καλό βαθμό με ελάχιστη απώλεια δεδομένων.



Εικόνα 8-9. Γραφική παράσταση ρυθμού μετάδοσης frames/sec κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του πομπού.



Εικόνα 8-10. Γραφική παράσταση ρυθμού μετάδοσης frames/sec κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του δέκτη.

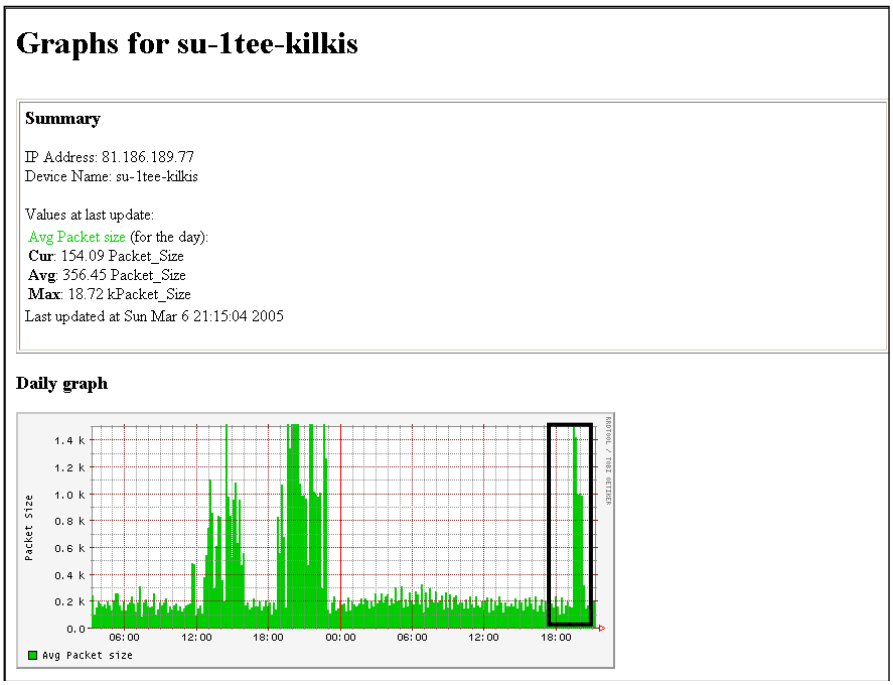
8.1.4. Μέσο μέγεθος πακέτων (Average Packet Size)

Οι γραφικές παραστάσεις δείχνουν το μέγεθος πακέτου που χρησιμοποιεί το σύστημα το οποίο στην περίπτωση που υπάρχει κίνηση στο ασύρματο δίκτυο είναι περίπου 1500 bytes. Ανάλυση σχετικά με την επίδραση του μήκους του πακέτου στον ρυθμό μετάδοσης γίνεται στην ενότητα 8.3.

Εικόνα 8-11. Γραφική παράσταση μέσου μεγέθους πακέτων με κανονικές καιρικές συνθήκες.

Εικόνα 8-12. Γραφική παράσταση μέσου μεγέθους πακέτων με χιονόπτωση.

Προφανώς τα μήκη των πακέτων που ανταλλάσσουν πομπός και δέκτης είναι ίσα.

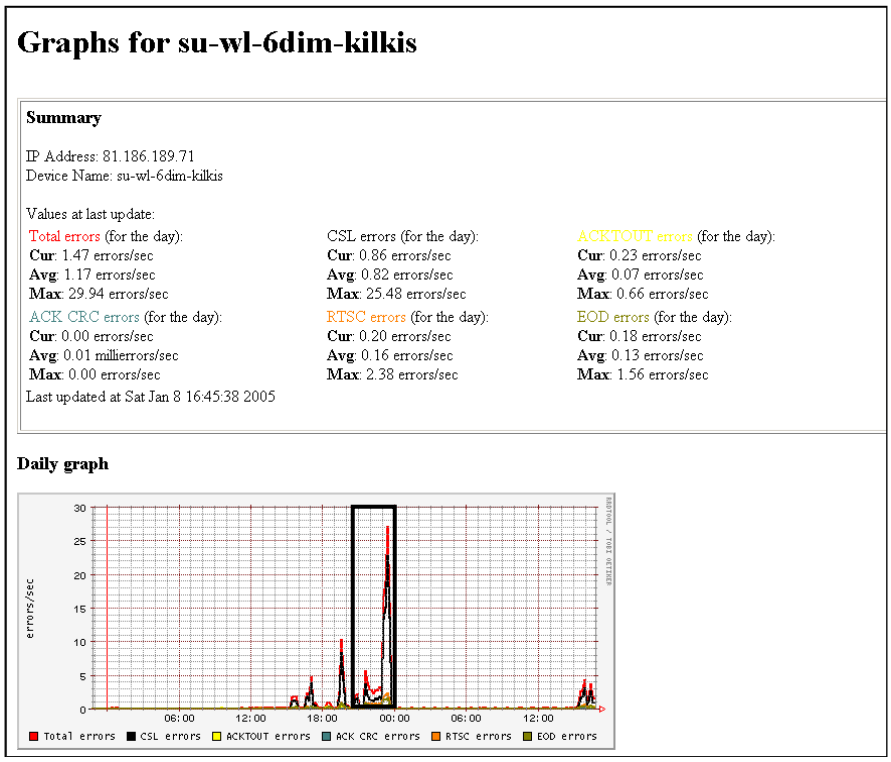


Εικόνα 8-13. Γραφική παράσταση μέσου μεγέθους πακέτων κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του πομπού.

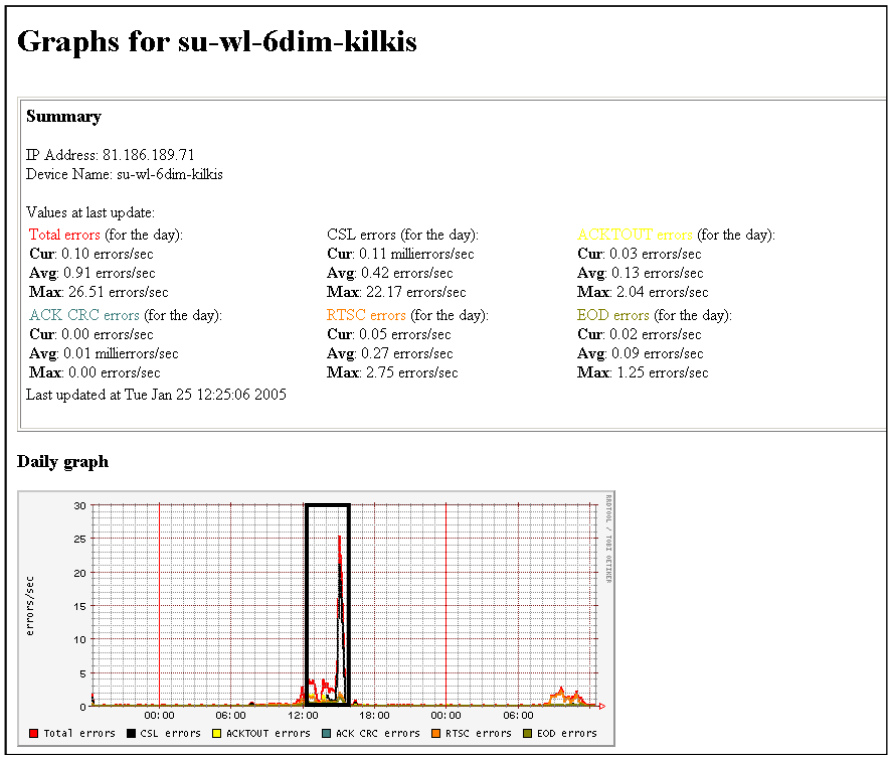
Εικόνα 8-14. Γραφική παράσταση μέσου μεγέθους πακέτων κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του δέκτη.

8.1.5. Λάθη (Tx Errors)

Στις επιλεγμένες περιοχές για την περίπτωση του καλού καιρού έχουμε μεγαλύτερο μέγιστο αριθμού λαθών στο μικρότερο χρονικό διάστημα της μεταφόρτωσης. Στην περίπτωση της χιονόπτωσης όπου είχαμε μεγαλύτερη διάρκεια μετάδοσης, είχαμε μικρότερο μεν μέγιστο αριθμού λαθών στη μονάδα του χρόνου, αλλά συνολικά μεγαλύτερο αριθμό λαθών.

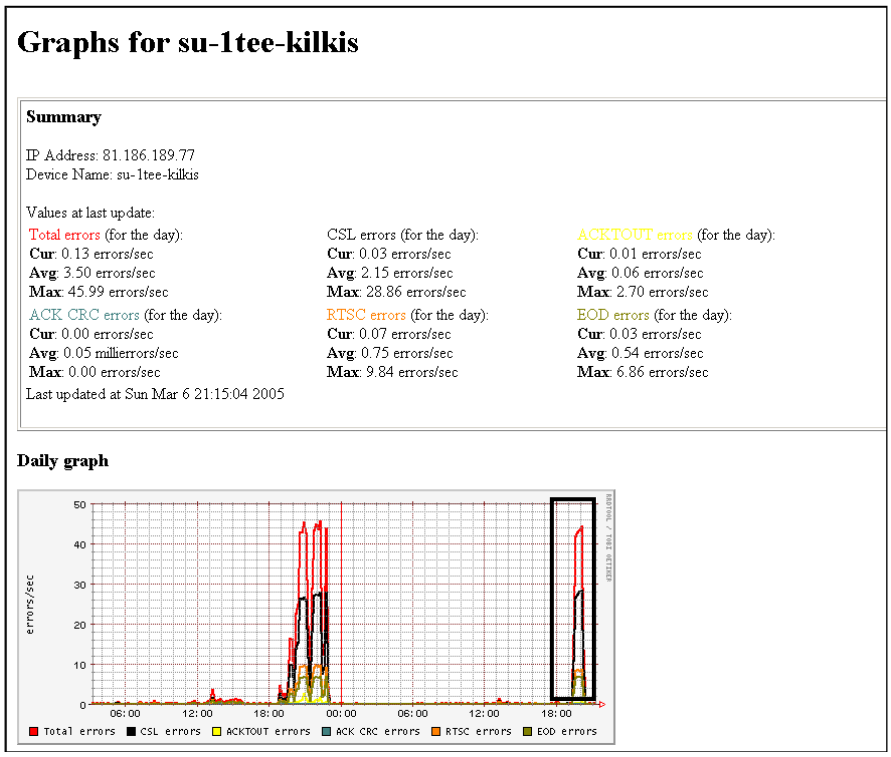


Εικόνα 8-15. Γραφική παράσταση λαθών κατά τη μετάδοση με κανονικές καιρικές συνθήκες.

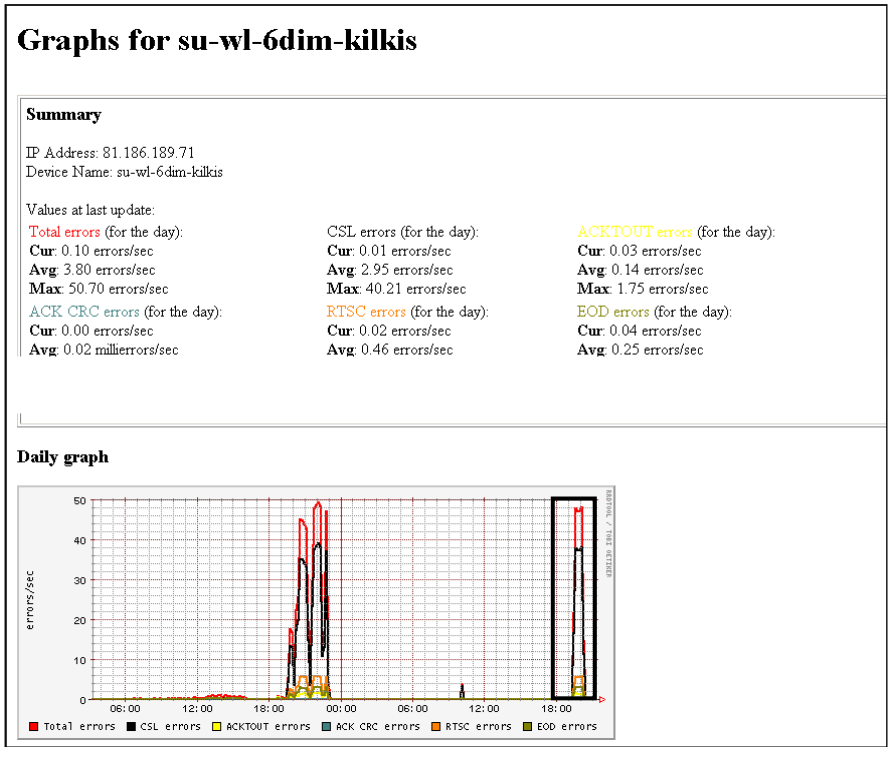


Εικόνα 8-16. Γραφική παράσταση λαθών κατά τη μετάδοση με χιονόπτωση.

Η αντιστοιχία των λαθών πομπού και δέκτη φανερή στις επιλεγμένες περιοχές. Πομπός και δέκτης παρουσιάζουν τον ίδιο αριθμό λαθών.



Εικόνα 8-17. Γραφική παράσταση λαθών κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του πομπού.

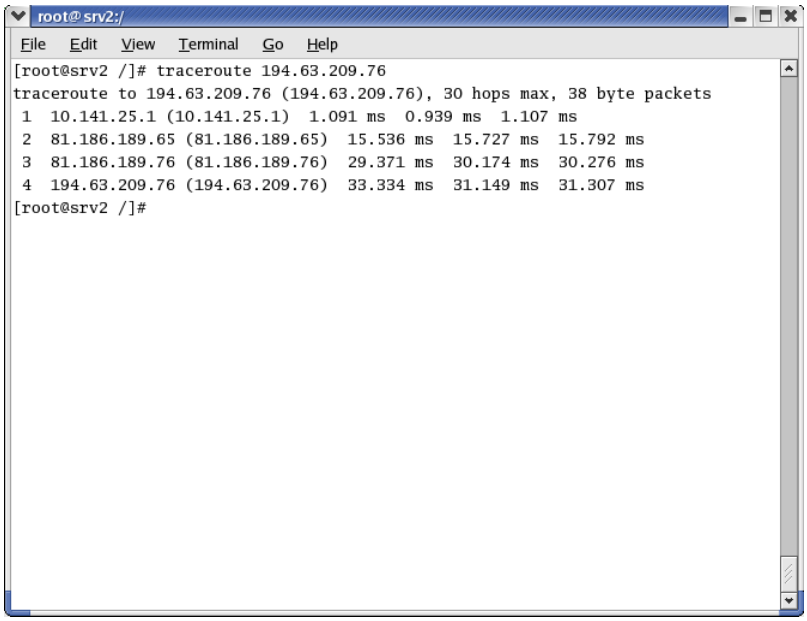


Εικόνα 8-18. Γραφική παράσταση λαθών κατά τη μετάδοση από κόμβο σε κόμβο από τη μεριά του δέκτη.

8.2. Σε ανώτερα επίπεδα του μοντέλου OSI (TCP/IP με Snoop και Ethereal)

Για τις μετρήσεις χρησιμοποιήθηκε το λογισμικό Ethereal. Οι μετρήσεις πλέον δεν αφορούν το 2ο επίπεδο του OSI, αλλά ανώτερα επίπεδα τα οποία μας επιτρέπουν να βλέπουμε πολύ περισσότερα στοιχεία. Έτσι μπορούμε να δούμε στοιχεία στο επίπεδο του TCP αλλά και του FTP και του HTTP που ενδιαφέρουν περισσότερο. Κύριος στόχος των μετρήσεων υπήρξε η αξιολόγηση της επίδοσης του δικτύου με τη χρήση του πρωτοκόλλου Snoop. Έτσι περιγράφουμε παρακάτω πώς έγιναν οι μετρήσεις μας.

Στο 1ο ΤΕΕ Κιλκίς ένας υπολογιστής με λειτουργικό Linux είναι ορατός από το Διαδίκτυο. Είναι και διακομιστής ιστοσελίδων Apache HTTP Server και διακομιστής αρχείων FTP Server. Επειδή η κίνηση σε όγκο σε σχέση με την υψηλή ταχύτητα της σύνδεσης για ιστοσελίδες είναι σχετικά χαμηλή, οι μετρήσεις έγιναν με τη μεταφόρτωση των αρχείων (FTP). Στο 6ο Δημοτικό Κιλκίς ένας δεύτερος υπολογιστής με λειτουργικό Linux μεταφόρτωσε μικρά και μεγάλα αρχεία. Οι μετρήσεις έγιναν με το πρωτόκολλο Snoop και ενεργοποιημένο και απενεργοποιημένο στον 1ο Υπολογιστή. Οι μετρήσεις έγιναν και με καλές συνθήκες και με άσχημες καιρικές συνθήκες (βροχή). Επειδή σε ορισμένες περιπτώσεις μετρήσεων (περίπτωση συγκριτικών μετρήσεων για μεταβλητό μήκος πακέτου TCP) ο καιρός ήταν άριστος, αποφασίσαμε να πάρουμε μετρήσεις από ένα τρίτο σημείο, το 1ο Γυμνάσιο Κιλκίς. Το σημείο αυτό παρουσιάζει προβλήματα στη λήψη. Αυτό είναι φανερό και από την ανάλυση με το Monitoring System. Η περίπτωση της προβληματικής λήψης μοιάζει με την περίπτωση και πάλι προβληματικής λήψης λόγω κακοκαιρίας. Στην Εικόνα 8-19 παρατηρούμε την άμεση σύνδεση των δύο υπολογιστών μέσω του ασύρματου δικτύου.



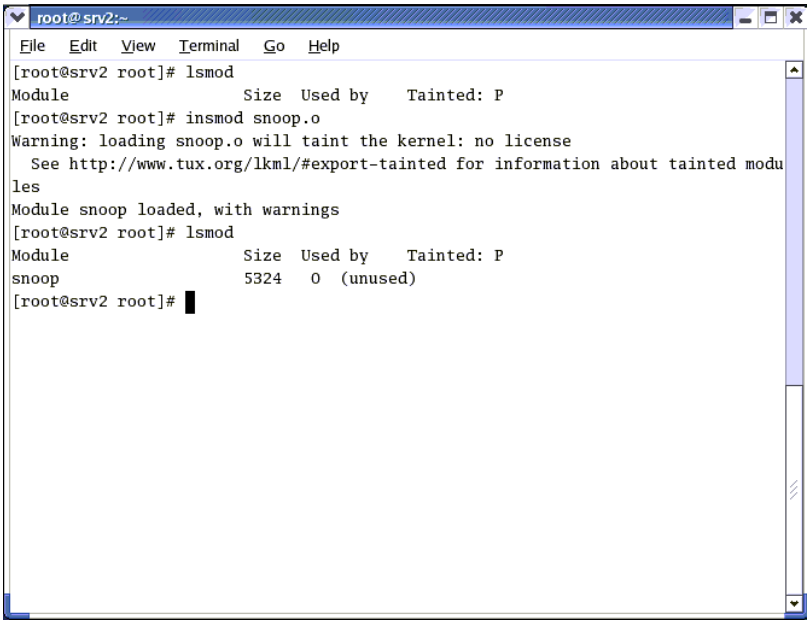
Εικόνα 8-19. Η σύνδεση μεταξύ των δύο υπολογιστών.

Από τον υπολογιστή του 6ου Δημοτικού καταγράφουμε τη διαδρομή που ακολουθείται για να φτάσουμε στον διακομιστή του 1ο ΤΕΕ. Παρατηρώντας την παραπάνω εικόνα, βλέπουμε ότι η σύνδεση των δύο υπολογιστών είναι ουσιαστικά άμεση μέσω του ασύρματου δικτύου και κάτω από φυσιολογικές συνθήκες δεν υπάρχουν προβλήματα στην επικοινωνία (πολύ καλή τοποθεσία και λήψη).

8.2.1. Εγκατάσταση και απεγκατάσταση του πρωτοκόλλου Snoop

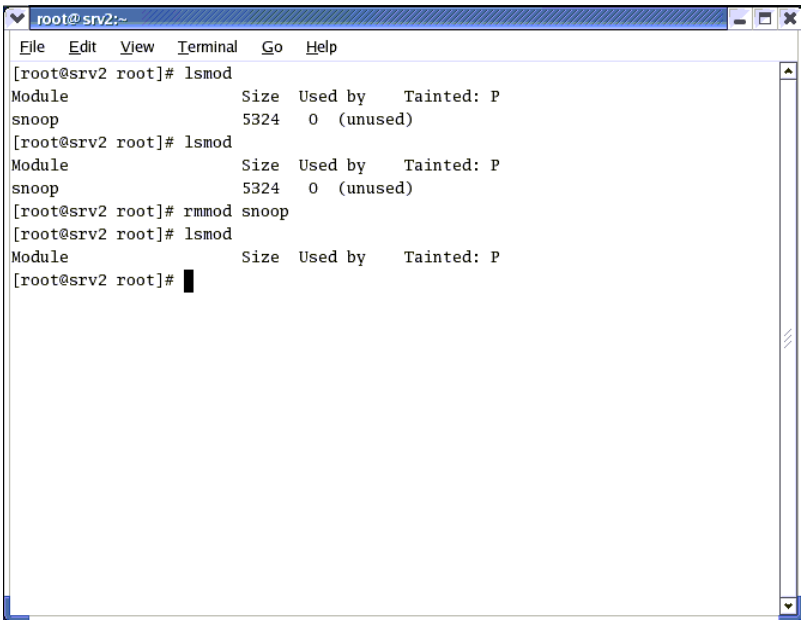
Οι μετρήσεις έγιναν με το Ethereal στο 6ο Δημοτικό (Linux Client). Ο διακομιστής ήταν στο 1ο ΤΕΕ. Η εισαγωγή και κατάργηση του πρωτοκόλλου Snoop γίνεται στον διακομιστή μέσω απομακρυσμένης διαχείρισης VNC. Για τον λόγο αυτό και στα δύο συστήματα με Linux εγκαταστήσαμε τον VNC Server και μόλις ξεκινούσαμε το κάθε σύστημα εκτελούσαμε την εντολή `vncserver` τέσσερις φορές ώστε να ανοίξουν τέσσερα X-Terminal Windows για την απομακρυσμένη σύνδεση.

Χρησιμοποιώντας τη σύνδεση VNC, εγκαθιστούσαμε και απεγκαθιστούσαμε το Snoop module από τον server από κάθε απομακρυσμένο χώρο εργασίας. Στην Εικόνα 8-20 φαίνεται η εγκατάσταση του πρωτοκόλλου στον διακομιστή με απομακρυσμένη σύνδεση VNC.



Εικόνα 8-20. Εγκατάσταση του πρωτοκόλλουSnoop μέσω VNC.

Ομοίως στην Εικόνα 8-21 φαίνεται η απεγκατάσταση του πρωτοκόλλου Snoop στον διακομιστή με απομακρυσμένη σύνδεση VNC.



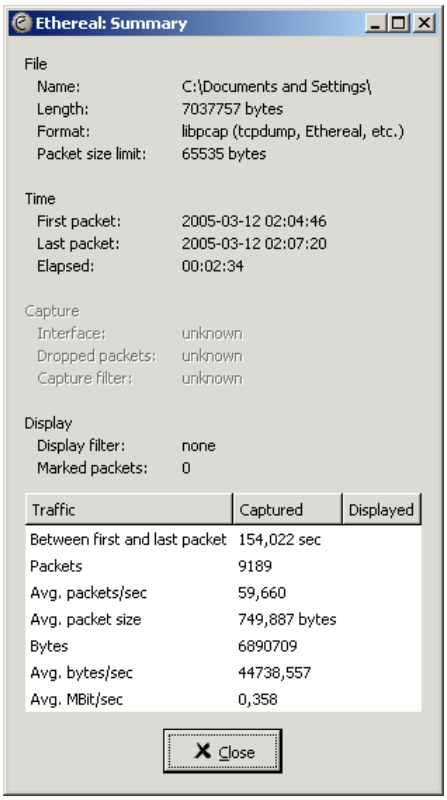
Εικόνα 8-21. Απεγκατάσταση του πρωτοκόλλου Snoop μέσω VNC.

8.2.2. Μέτρηση με μεταφόρτωση αρχείου 6,5 MB

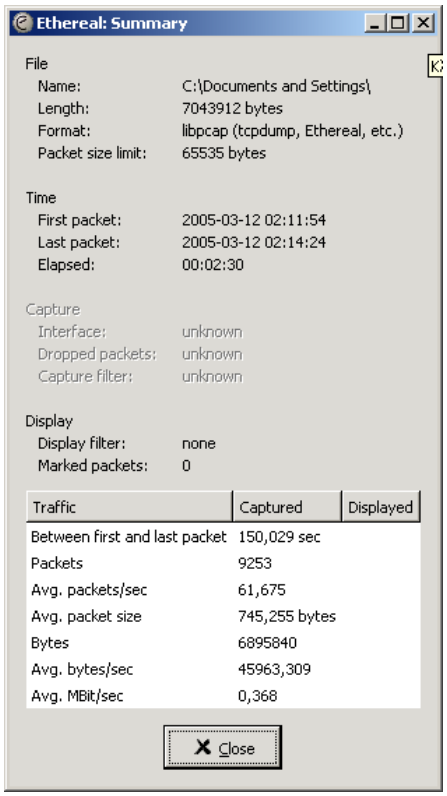
Για τη μέτρηση με μεταφόρτωση μικρού αρχείου επιλέχθηκε το αρχείο του Nero Express (6,5 MB). Το αρχείο μεταφορτώθηκε δύο φορές, με πολύ καλές καιρικές συνθήκες, με το Snoop τη μία φορά on και την άλλη off. Σε όλη τη διάρκεια των μετρήσεων αυτών υπήρχε πολύ καλός καιρός, καθαρός ουρανός και οι συνθήκες ήταν ακριβώς οι ίδιες και στις δύο υποπεριπτώσεις της μέτρησης. Αυτό μας βοήθησε στην εξαγωγή συγκεκριμένων συμπερασμάτων για την επίδραση του Snoop. Οι μετρήσεις έγιναν σε λειτουργικό Windows σε έναν τρίτο χώρο και συγκεκριμένα στο 1ο Γυμνάσιο Κιλκίς. Το συγκεκριμένο σημείο είναι αυτό που σε όλες τις περιπτώσεις παρουσιάζει μία σύνδεση όχι και τόσο καλή, κάτι που φαίνεται και στον ρυθμό μετάδοσης του δικτύου.

Επιλέξαμε για σύλληψη όλα τα πακέτα του αρχείου και στο τέλος της λήψης επεξεργαστήκαμε το αρχείο σύλληψης σε άλλον υπολογιστή. Τα αποτελέσματα των μετρήσεων φαίνονται στις παρακάτω εικόνες και με μια πρώτη ματιά γίνεται φανερό ότι σε συνθήκες καλού καιρού το Snoop δε βελτιώνει πολύ τη σύνδεση. Μία μικρή βελτίωση οφείλεται κυρίως στις δυσκολίες της σύνδεσης που έχουμε στον συγκεκριμένο χώρο, κάτι που φαίνεται και από την ανάλυση του Monitoring System.

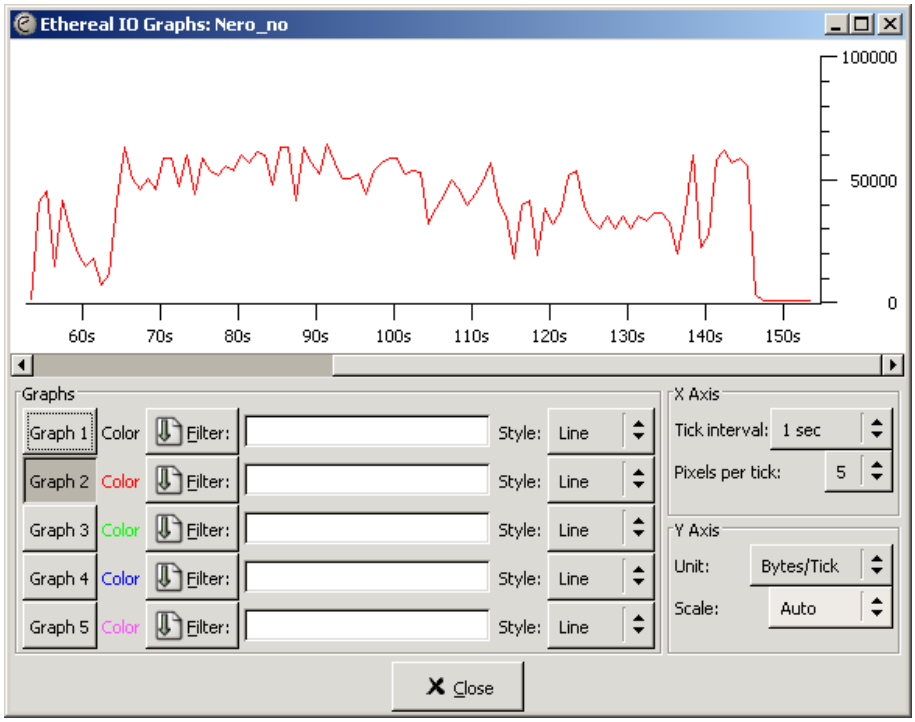
Στις επόμενες τέσσερις εικόνες βλέπουμε στιγμιότυπα για τις συνοπτικές πληροφορίες μετάδοσης και γραφικές παραστάσεις κίνησης δεδομένων με το Snoop on και off.



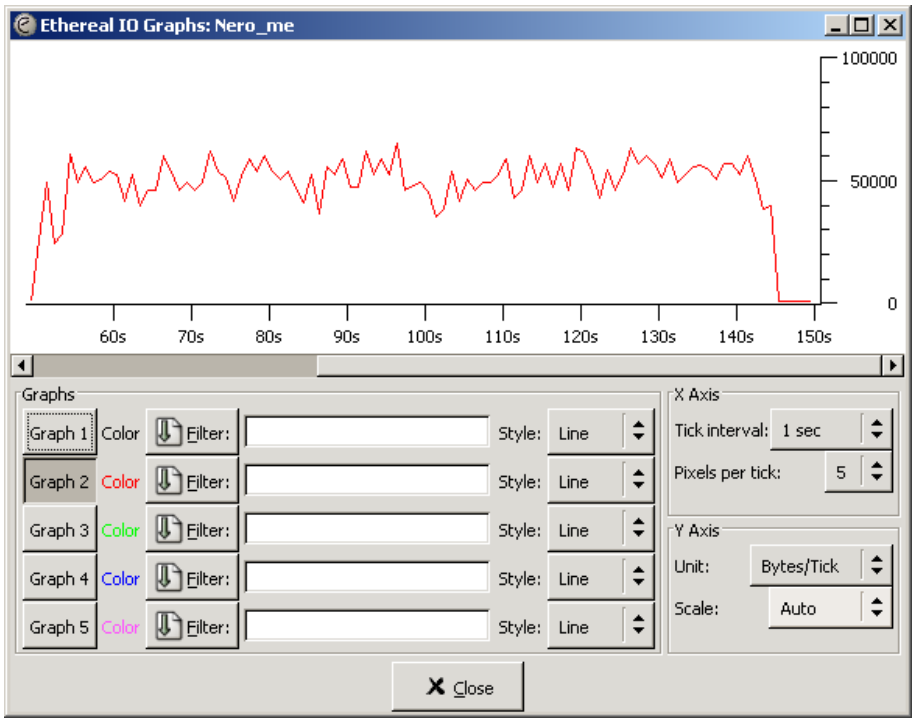
Εικόνα 8-22. Συνοπτικές πληροφορίες με Snoop off.



Εικόνα 8-23. Συνοπτικές πληροφορίες με Snoop on.

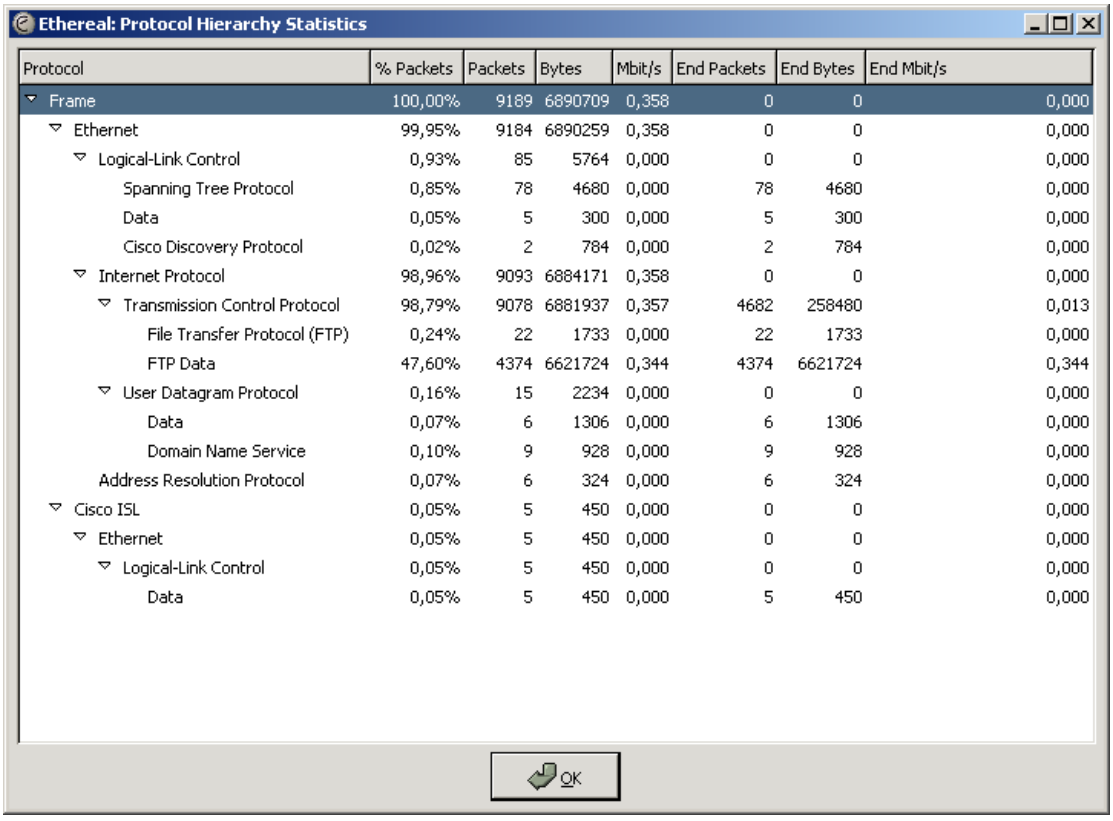


Εικόνα 8-24. Γραφική παράσταση κίνησης bytes αρχείου 6,5 MB με Snoop off.



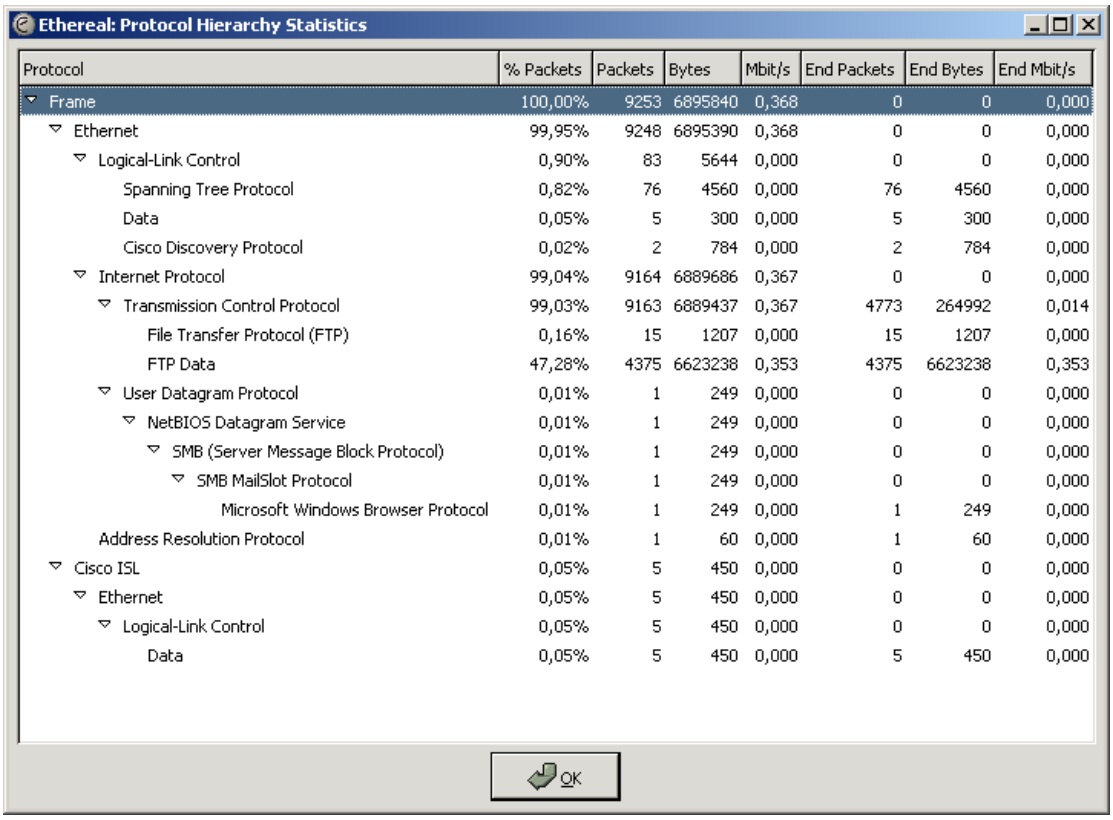
Εικόνα 8-25. Γραφική παράσταση κίνησης bytes αρχείου 6,5 MB με Snoop on.

Μία χρήσιμη έξοδος του Ethereal αφορά την ιεραρχία των πρωτοκόλλων. Στα παρακάτω στιγμιότυπα φαίνεται το ποσοστό της τηλεπικοινωνιακής κίνησης για κάθε πρωτόκολλο.



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	9189	6890709	0,358	0	0	0,000
Ethernet	99,95%	9184	6890259	0,358	0	0	0,000
Logical-Link Control	0,93%	85	5764	0,000	0	0	0,000
Spanning Tree Protocol	0,85%	78	4680	0,000	78	4680	0,000
Data	0,05%	5	300	0,000	5	300	0,000
Cisco Discovery Protocol	0,02%	2	784	0,000	2	784	0,000
Internet Protocol	98,96%	9093	6884171	0,358	0	0	0,000
Transmission Control Protocol	98,79%	9078	6881937	0,357	4682	258480	0,013
File Transfer Protocol (FTP)	0,24%	22	1733	0,000	22	1733	0,000
FTP Data	47,60%	4374	6621724	0,344	4374	6621724	0,344
User Datagram Protocol	0,16%	15	2234	0,000	0	0	0,000
Data	0,07%	6	1306	0,000	6	1306	0,000
Domain Name Service	0,10%	9	928	0,000	9	928	0,000
Address Resolution Protocol	0,07%	6	324	0,000	6	324	0,000
Cisco ISL	0,05%	5	450	0,000	0	0	0,000
Ethernet	0,05%	5	450	0,000	0	0	0,000
Logical-Link Control	0,05%	5	450	0,000	0	0	0,000
Data	0,05%	5	450	0,000	5	450	0,000

Εικόνα 8-26. Στατιστικά στοιχεία ιεραρχίας πρωτοκόλλων για αρχείο 6,5 MB με Snoop off.



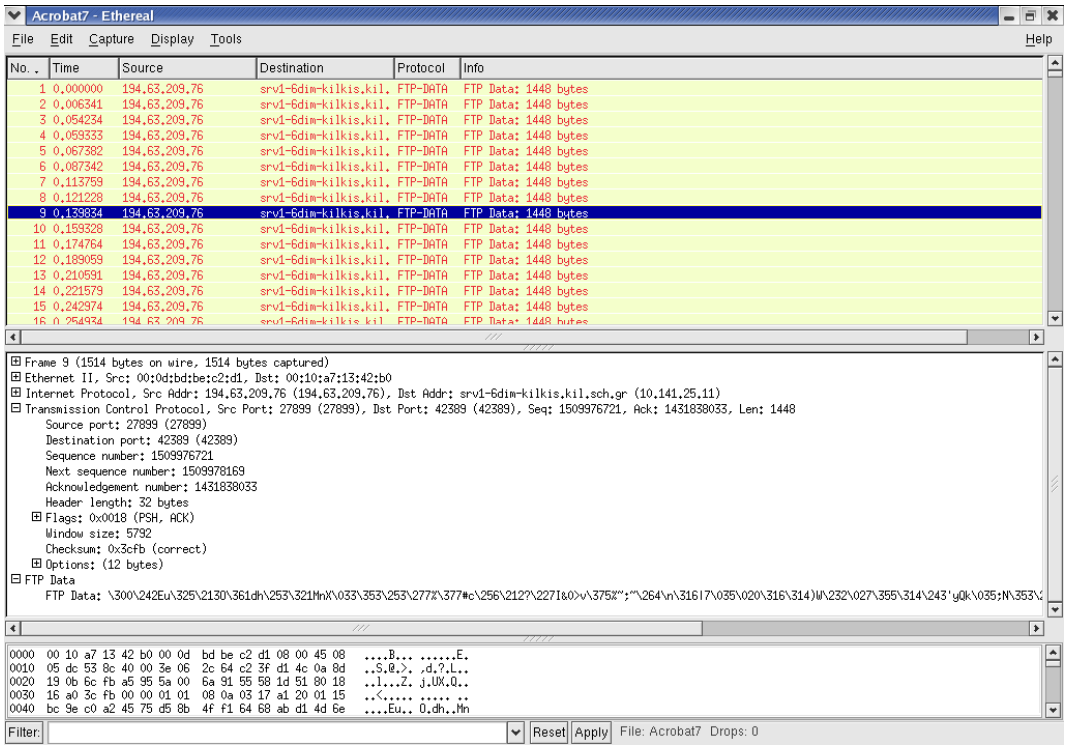
Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	9253	6895840	0,368	0	0	0,000
Ethernet	99,95%	9248	6895390	0,368	0	0	0,000
Logical-Link Control	0,90%	83	5644	0,000	0	0	0,000
Spanning Tree Protocol	0,82%	76	4560	0,000	76	4560	0,000
Data	0,05%	5	300	0,000	5	300	0,000
Cisco Discovery Protocol	0,02%	2	784	0,000	2	784	0,000
Internet Protocol	99,04%	9164	6889686	0,367	0	0	0,000
Transmission Control Protocol	99,03%	9163	6889437	0,367	4773	264992	0,014
File Transfer Protocol (FTP)	0,16%	15	1207	0,000	15	1207	0,000
FTP Data	47,28%	4375	6623238	0,353	4375	6623238	0,353
User Datagram Protocol	0,01%	1	249	0,000	0	0	0,000
NetBIOS Datagram Service	0,01%	1	249	0,000	0	0	0,000
SMB (Server Message Block Protocol)	0,01%	1	249	0,000	0	0	0,000
SMB MailSlot Protocol	0,01%	1	249	0,000	0	0	0,000
Microsoft Windows Browser Protocol	0,01%	1	249	0,000	1	249	0,000
Address Resolution Protocol	0,01%	1	60	0,000	1	60	0,000
Cisco ISL	0,05%	5	450	0,000	0	0	0,000
Ethernet	0,05%	5	450	0,000	0	0	0,000
Logical-Link Control	0,05%	5	450	0,000	0	0	0,000
Data	0,05%	5	450	0,000	5	450	0,000

Εικόνα 8-27. Στατιστικά στοιχεία ιεραρχίας πρωτοκόλλων για αρχείο 6,5 MB με Snoop on.

8.2.3. Μέτρηση με μεταφόρτωση αρχείου 20 MB

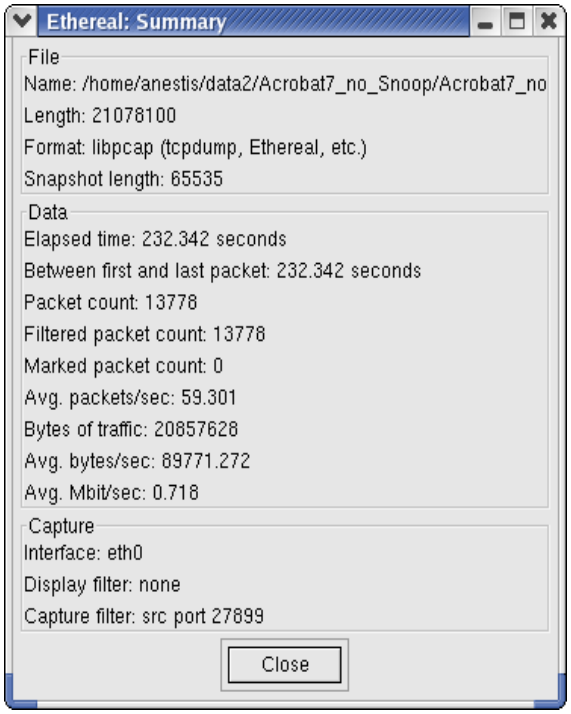
Για την παραπάνω μέτρηση επιλέχθηκε το αρχείο του Adobe Reader 7. Το αρχείο μεταφορτώθηκε δύο φορές, με συνθήκες βροχής με το Snoop τη μία φορά on και την άλλη off. Σε όλη τη διάρκεια των μετρήσεων αυτών υπήρχε έντονη βροχόπτωση, κάτι που μας βοήθησε για την εξαγωγή των συμπερασμάτων μας. Οι μετρήσεις έγιναν σε λειτουργικό Linux αλλά μερικές αναλύσεις έγιναν off-line σε Windows. Τα στιγμιότυπα (screenshots) είναι και από τις δύο πλατφόρμες.

Έγινε σύλληψη πακέτων μόνο FTP-DATA με τον τρόπο που περιγράψαμε και στην πρώτη περίπτωση. Παρουσιάζουμε μία εικόνα του προγράμματος Ethereal του αρχείου που μεταφορτώθηκε με το Snoop on (Εικόνα 8-28).

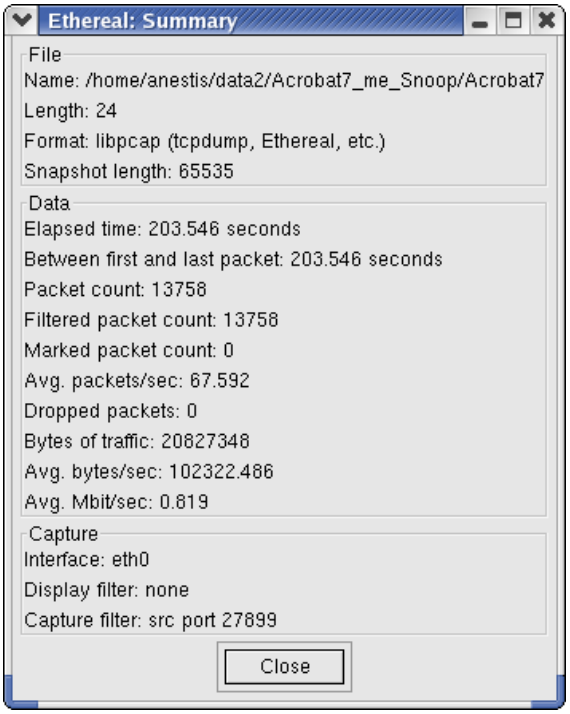


Εικόνα 8-28. Κίνηση πακέτων για αρχείο 20 MB με το Snoop on.

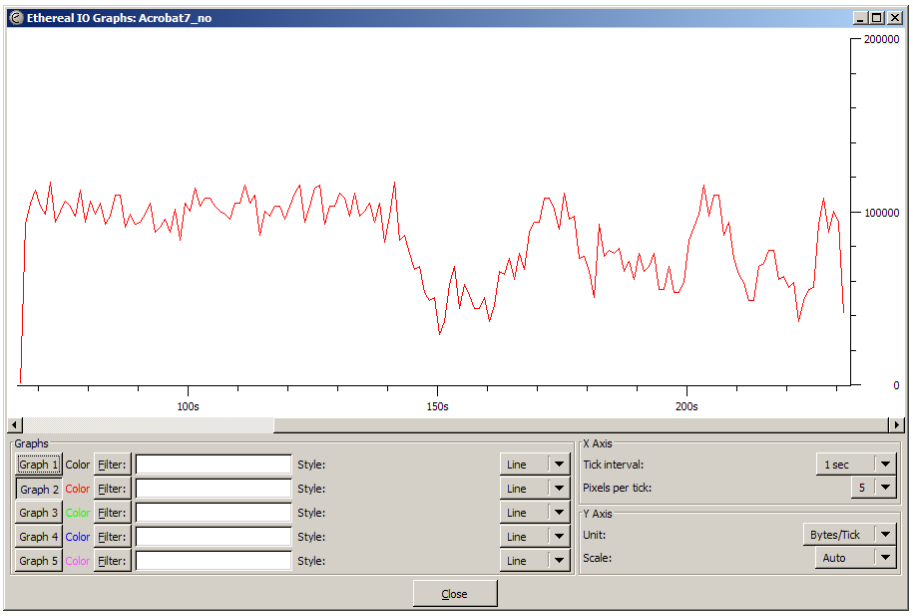
Παρακάτω βλέπουμε αντίστοιχα στιγμιότυπα, όπως και πριν, για τις συνοπτικές πληροφορίες λήψης και για τα διαγράμματα κίνησης με το Snoop On και Off.



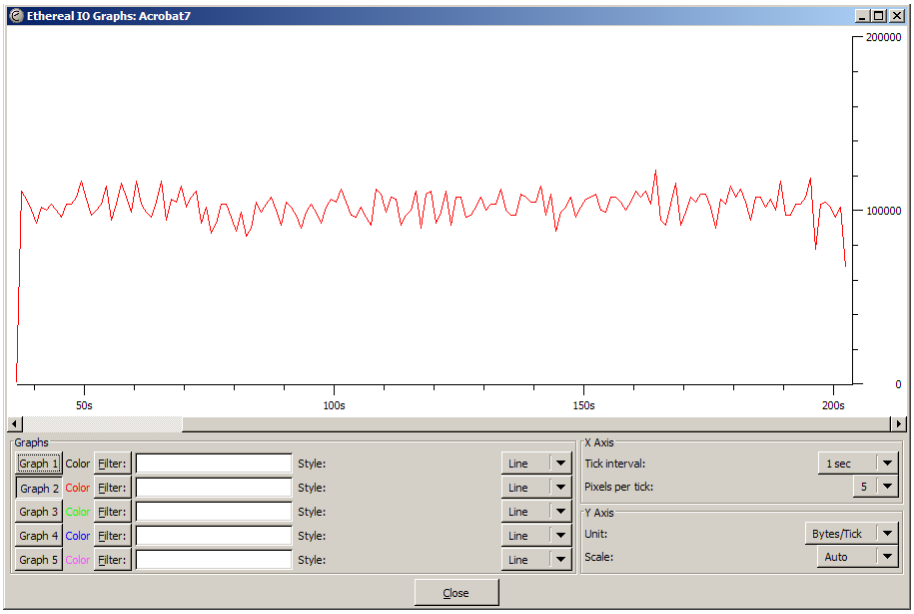
Εικόνα 8-29. Συνοπτικές πληροφορίες με Snoop off.



Εικόνα 8-30. Συνοπτικές πληροφορίες με Snoop on.



Εικόνα 8-31. Γραφική παράσταση κίνησης bytes αρχείου 20 MB με Snoop off.



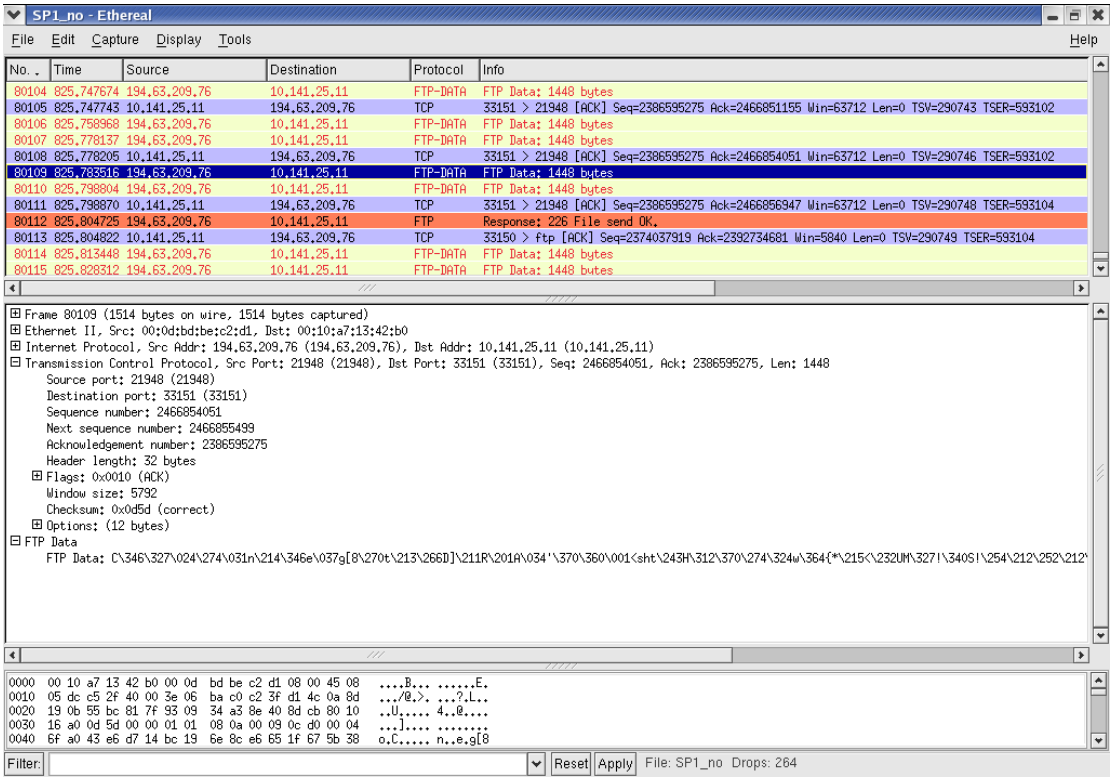
Εικόνα 8-32. Γραφική παράσταση κίνησης bytes αρχείου 20 MB με Snoop on.

Τα αποτελέσματα εδώ είναι πολύ καλά για το Snoop λόγω του μικρού σχετικά χρόνου μεταφόρτωσης του αρχείου. Πετύχαμε ίδιες συνθήκες και σχετικά πολύ άσχημες (έντονη βροχόπτωση) οπότε έγινε φανερή η βελτίωση με το Snoop.

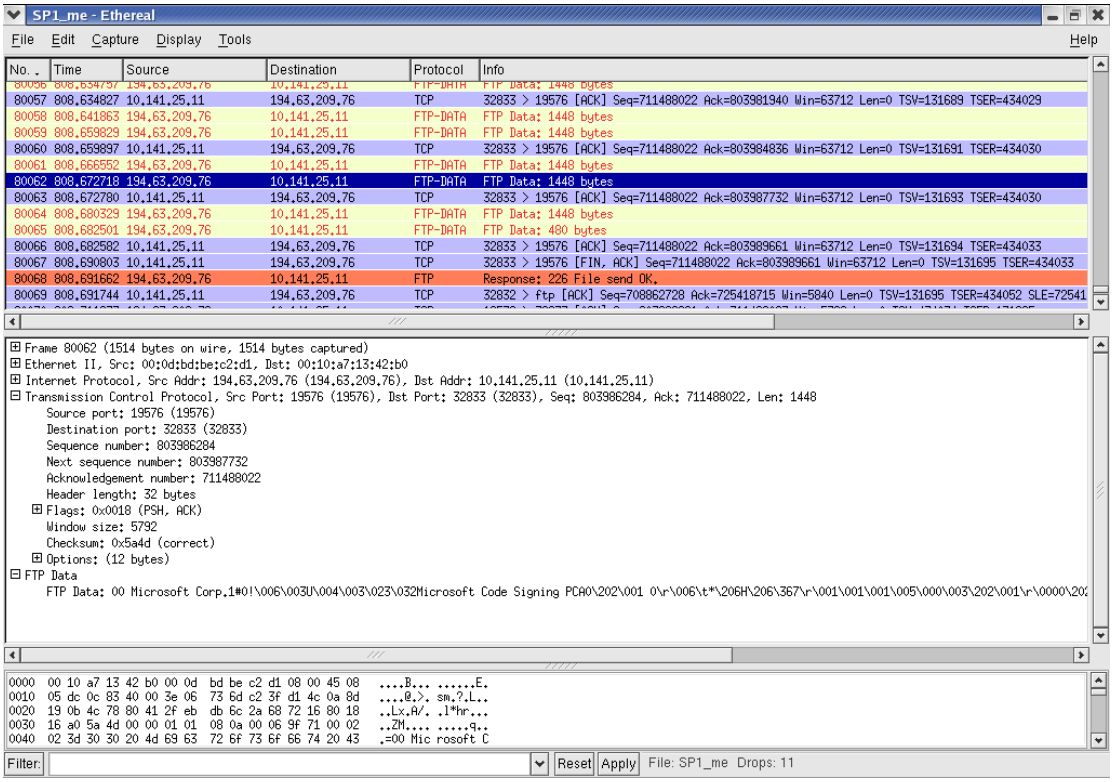
8.2.4. Μέτρηση με μεταφόρτωση αρχείου 72 MB

Για την παραπάνω μέτρηση επιλέχθηκε το αρχείο Microsoft Office 2003 SP1. Το αρχείο μεταφορτώθηκε δύο φορές, με συνθήκες συννεφιάς και υψηλής υγρασίας και έντονο άνεμο, με το Snoop τη μία φορά on και την άλλη off. Σε όλη τη διάρκεια των μετρήσεων αυτών υπήρχε έντονη βροχόπτωση, κάτι που μας βοήθησε για την εξαγωγή των συμπερασμάτων μας. Οι μετρήσεις έγιναν σε λειτουργικό Linux, αλλά μερικές αναλύσεις έγιναν off-line σε Windows. Τα στιγμιότυπα (screenshots) είναι και από τις δύο πλατφόρμες.

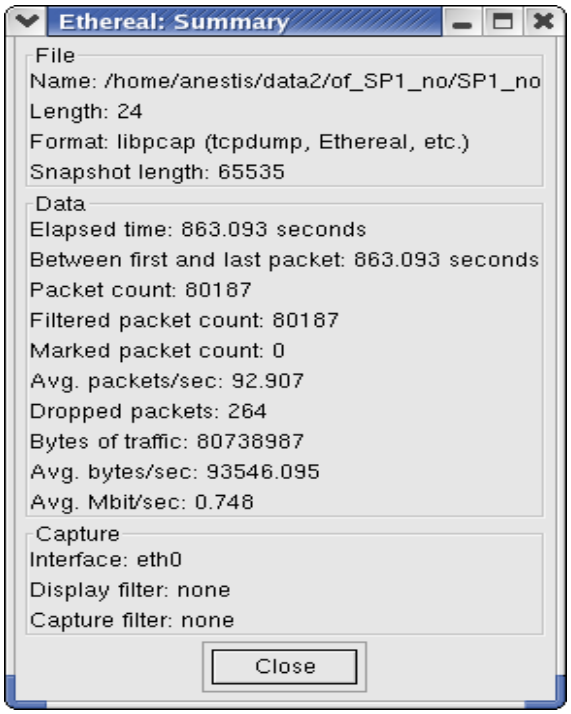
Αυτή τη φορά επιλέξαμε για σύλληψη όλα τα πακέτα του αρχείου και απλώς στο τέλος της λήψης χρωματίσαμε τα πακέτα για κάθε πρωτόκολλο, ώστε να είναι ορατά. Έχουμε λοιπόν για κάθε περίπτωση τα αποτελέσματα που φαίνονται στις παρακάτω 4 εικόνες.



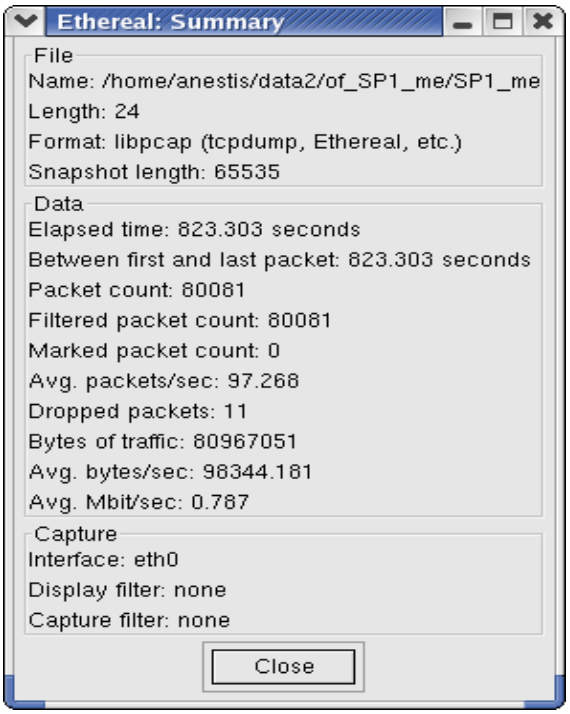
Εικόνα 8-33. Κίνηση πακέτων για αρχείο 72 MB με Snoop off.



Εικόνα 8-34. Κίνηση πακέτων για αρχείο 72 MB με Snoop on.

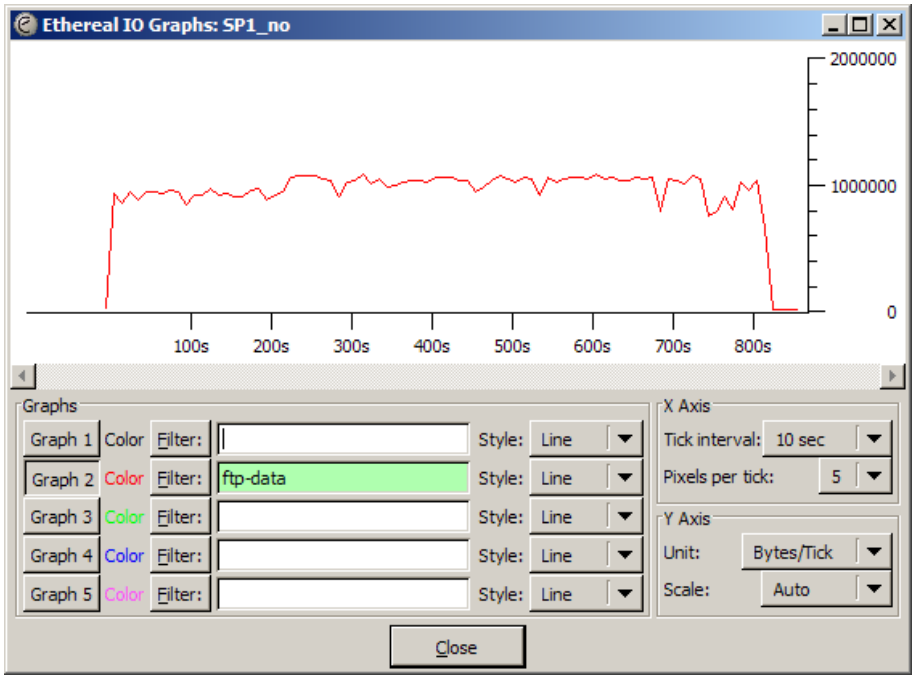


Εικόνα 8-35. Συνοπτικές πληροφορίες με Snoop off.

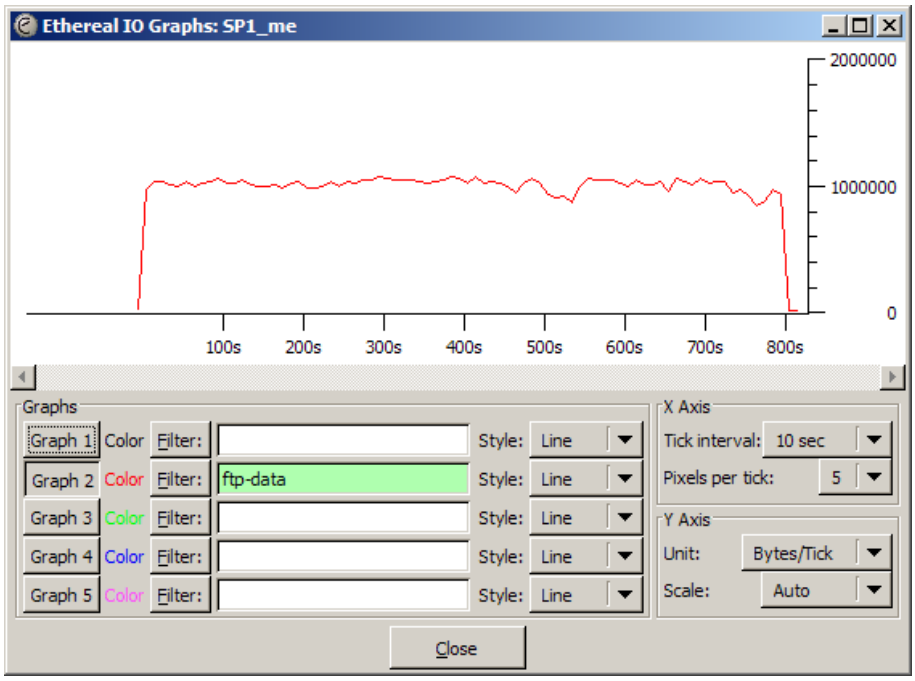


Εικόνα 8-36. Συνοπτικές πληροφορίες με Snoop on.

Παρατηρούμε από τα στατιστικά πάλι μία βελτίωση με το πρωτόκολλο Snoop on λόγω των κακών σχετικά καιρικών συνθηκών. Παρακάτω φαίνονται οι γραφικές παραστάσεις από την ανάλυση σε περιβάλλον Windows (Εικόνα 8-37 και Εικόνα 8-38).



Εικόνα 8-37. Γραφική παράσταση κίνησης bytes FTP-DATA αρχείου 72 MB με Snoop off.



Εικόνα 8-38. Γραφική παράσταση κίνησης bytes FTP-DATA αρχείου 72 MB με Snoop on.

8.2.5. Μέτρηση με μεταφόρτωση αρχείου 260 MB

Για τη μέτρηση αυτή επιλέχθηκε το αρχείο του Windows XP SP2. Το αρχείο μεταφορτώθηκε δύο φορές με συνθήκες βροχής και με το Snoop τη μία φορά off και την άλλη on. Σε όλη τη διάρκεια των μετρήσεων αυτών υπήρχε έντονη βροχόπτωση, γεγονός που μας βοήθησε για την εξαγωγή των συμπερασμάτων μας. Οι μετρήσεις έγιναν σε λειτουργικό Linux αλλά μερικές αναλύσεις έγιναν off-line σε Windows. Τα στιγμιότυπα (screenshots) είναι και από τις δύο πλατφόρμες.

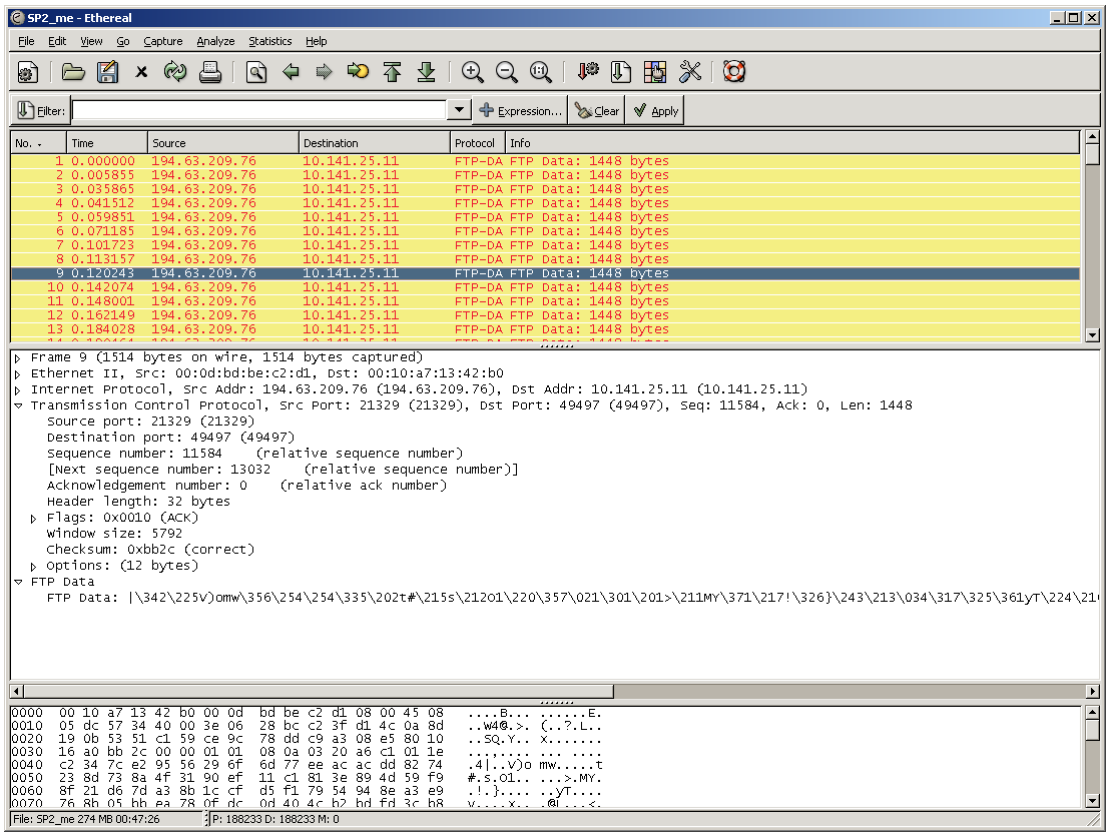
Επειδή το αρχείο είναι πολύ μεγάλο για λόγους εξοικονόμησης χώρου επιλέξαμε να συλλάβουμε μόνο τα πακέτα FTP-DATA. Έτσι χρησιμοποιήθηκε η τεχνική που αναφέραμε στα φίλτρα του Ethereal για τη σύλληψη μόνο των πακέτων FTP DATA.

Για την πρώτη μέτρηση με το Snoop off και εφαρμόστηκε ένα φίλτρο **«host 194.63.209.76 and src port 40501»** και καταγράφηκαν μόνο τα πακέτα αυτά. Τα δεδομένα αποθηκεύτηκαν σε αρχείο. Εδώ πρέπει να αναφέρουμε ότι το αρχείο με τα πακέτα σύλληψης είναι της τάξης μεγέθους του αρχείου που κατεβάζουμε. Η διαχείριση ενός τέτοιου αρχείου απαιτεί έναν ισχυρό σχετικά υπολογιστή. Ο Linux του 6ου Δημοτικού είναι ένας υπολογιστής που αργούσε με τα αρχεία αυτά. Έτσι η ανάλυση έγινε σε υπολογιστές πιο ισχυρούς όμως με λειτουργικό Windows. Τα πακέτα TCP από τη θύρα 40501 αποκωδικοποιήθηκαν ως (Decode As…) FTP-DATA για να τα βλέπουμε ως ftp-data.

Στη δεύτερη μέτρηση από το 6ο Δημοτικό και μέσω απομακρυσμένης σύνδεσης VNC ενεργοποιήσαμε το πρωτόκολλο Snoop στον διακομιστή του 1ο ΤΕΕ.

Χρησιμοποιήθηκε και πάλι η τεχνική που αναφέραμε στα φίλτρα του Ethereal για τη σύλληψη των πακέτων FTP DATA μόνο. Έτσι εφαρμόστηκε ένα φίλτρο **«host 194.63.209.76 and src port 21329»** και καταγράφηκαν μόνο τα πακέτα αυτά. Τα δεδομένα αποθηκεύτηκαν σε αρχείο. Και πάλι η ανάλυση έγινε σε υπολογιστές με λειτουργικό Windows.

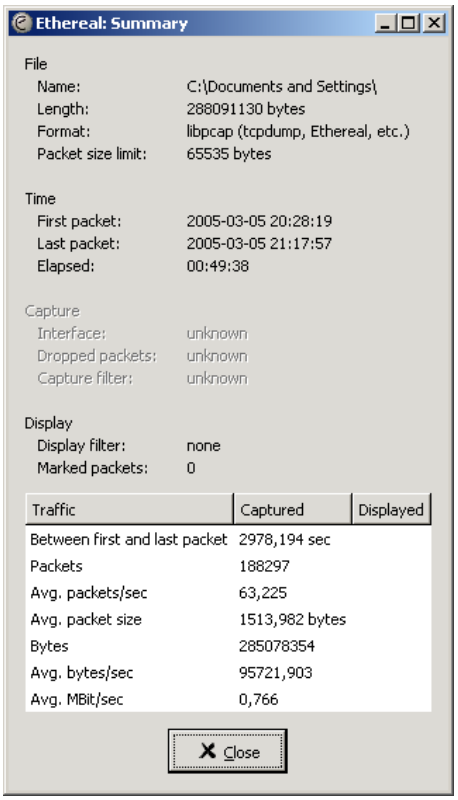
Τα πακέτα TCP από τη θύρα 21329 αποκωδικοποιήθηκαν ως (Decode As…) FTP-DATA και με τον χρωματισμό που επιλέξαμε πήραμε σε περιβάλλον Windows το αποτέλεσμα που φαίνεται στην Εικόνα 8-39. Η μέτρηση αυτή αφορά την περίπτωση με το Snoop on. Η οθόνη με τα πακέτα στην πρώτη περίπτωση με το Snoop off είναι παρόμοια με την Εικόνα 8-39.



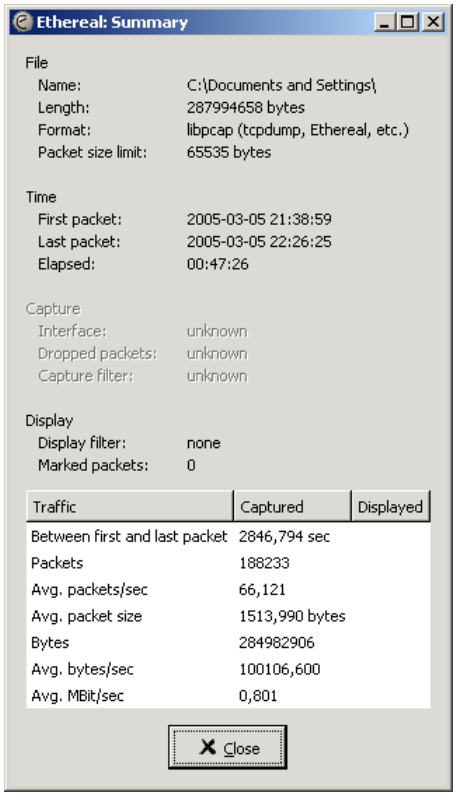
Εικόνα 8-39. Κίνηση πακέτων για αρχείο 260 MB με Snoop on.

Αυτό που έχει σημασία είναι τα συνοπτικά στατιστικά στοιχεία (Statistics → Summary), καθώς και η γραφική παράσταση των αποτελεσμάτων (Statistics → IO Graphs) και για τις δύο περιπτώσεις συγκριτικά. Όλα αυτά φαίνονται στις επόμενες τέσσερις εικόνες.

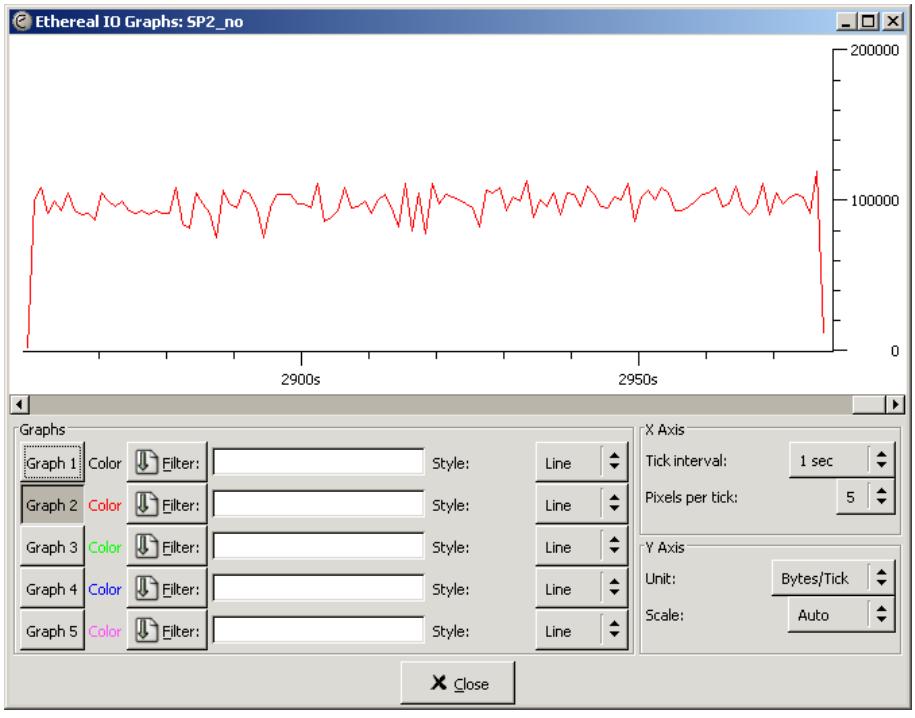
Παρατηρώντας τις μετρήσεις βλέπουμε τη βελτίωση που υπάρχει με τη χρήση του πρωτοκόλλου Snoop. Αν και η βελτίωση είναι σχετικά μικρή (έχουμε παρατηρήσει καλύτερα αποτελέσματα σε άλλες μετρήσεις), το κέρδος είναι και πάλι προφανές. Οι λόγοι της μικρής βελτίωσης σχετίζονται με τον σχετικά άστατο καιρό και με την αύξηση της έντασης της βροχόπτωσης προς το τέλος της μεταφόρτωσης του αρχείου με το Snoop. Αυτό γίνεται φανερό με τη βοήθεια των γραφικών παραστάσεων που φαίνονται στην Εικόνα 8-42 και στην Εικόνα 8-43.



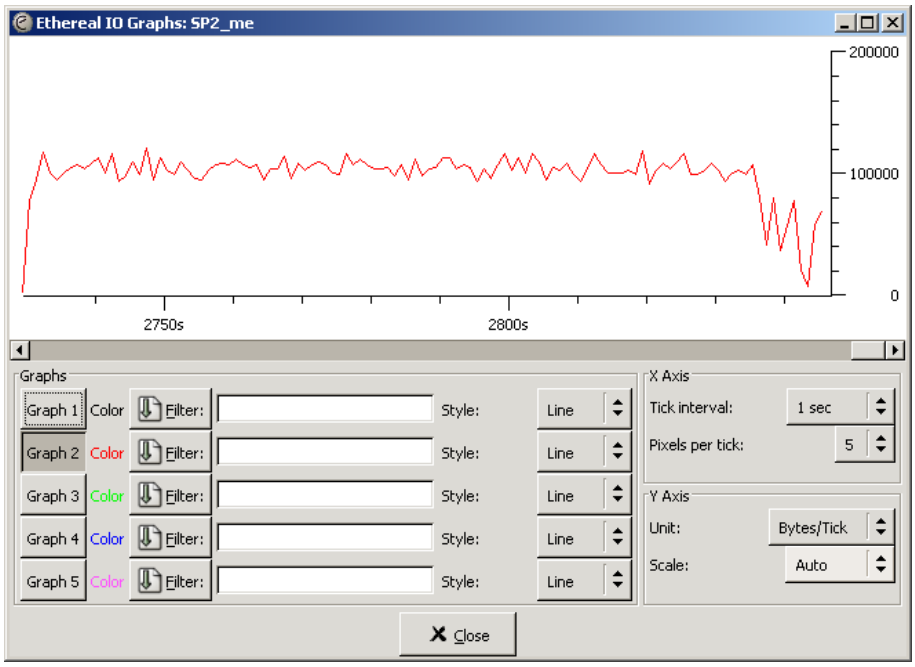
Εικόνα 8-40. Συνοπτικές πληροφορίες με Snoop off.



Εικόνα 8-41. Συνοπτικές πληροφορίες με Snoop on.



Εικόνα 8-42. Γραφική παράσταση κίνησης bytes αρχείου 260 MB με το Snoop off.



Εικόνα 8-43. Γραφική παράσταση κίνησης bytes αρχείου 260 MB με το Snoop on.

Ο λόγος για τον οποίο με το Snoop έχουμε μικρή σχετικά βελτίωση είναι φανερός: προς το τέλος της μέτρησης με το Snoop on είχαμε εξαιρετικά έντονη βροχόπτωση, κάτι που είναι προφανές στη γραφική παράσταση. Παρ' όλα αυτά, η γενική εικόνα δείχνει ότι το Snoop βελτιώνει πολύ την κατάσταση. Βασικό ρόλο εδώ έπαιξε η μεγάλη χρονική διάρκεια μεταφόρτωσης του μεγάλου αρχείου, οπότε είναι πιο πιθανό να παρατηρηθεί μεταβολή των καιρικών συνθηκών.

8.2.6. Σύνοψη αποτελεσμάτων μετρήσεων

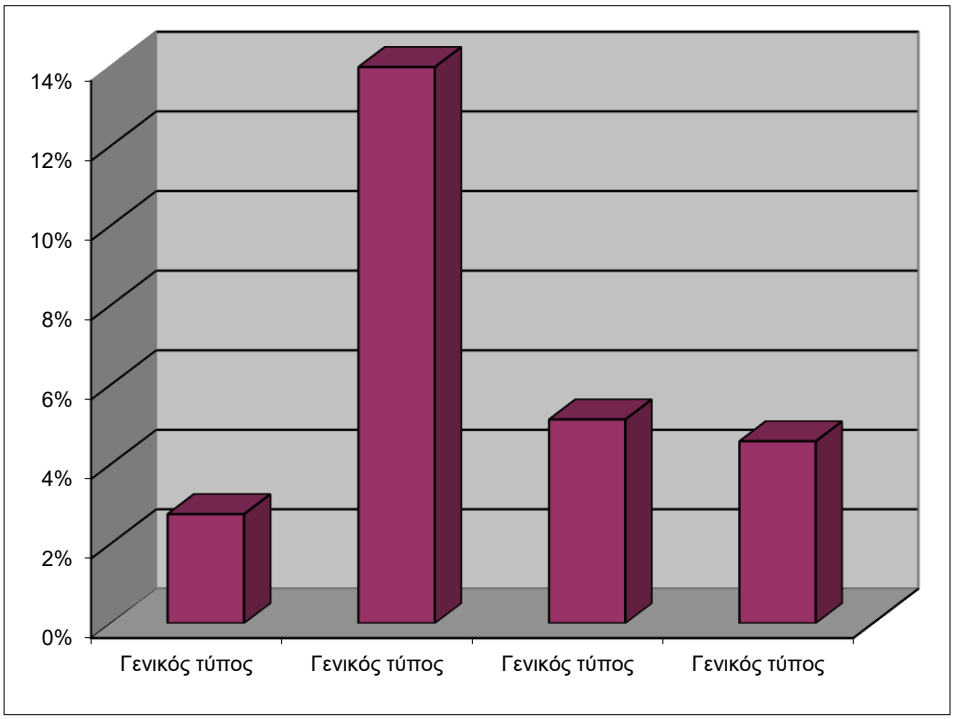
Μια γενική εικόνα της βελτίωσης που επιφέρει το πρωτόκολλο Snoop σε σχέση με το απλό TCP γίνεται φανερή με την παρακάτω σύγκριση (Πίνακας 1). Οι μετρήσεις έγιναν είτε με άσχημες καιρικές συνθήκες, είτε με δυσκολίες λήψης (περίπτωση 1ου Γυμνασίου). Ο Πίνακας 1 δημιουργήθηκε με τις μετρήσεις ταξινομημένες με βάση το μέγεθος του αρχείου μεταφόρτωσης για τη συγκριτική αξιολόγηση των αποτελεσμάτων.

Πίνακας 1. Μέσοι ρυθμοί μετάδοσης (bytes/sec) για διάφορα μεγέθη αρχείων με Snoop off και on.

Α/Α	Μέγεθος αρχείου	Average bytes/sec		Βελτίωση %	Καιρικές συνθήκες
		Snoop off	Snoop on		
1	6,5 MB	44.738	45.967	2,75%	Πολύ καλός καιρός
2	20 MB	89.771	102.322	13,98%	Πολύ ισχυρή βροχή
3	72 MB	93.546	98.344	5,13%	Άσχημος καιρός χωρίς βροχή
4	260 MB	95.722	100.106	4,58%	Συνεχής βροχή

Η 1η μέτρηση όπως αναφέραμε έγινε στο 1ο Γυμνάσιο όπου υπάρχουν δυσκολίες λήψης (χαμηλή ταχύτητα) μεν, αλλά είχαμε πολύ καλό καιρό, οπότε η βελτίωση δεν είναι σημαντική. Οι υπόλοιπες μετρήσεις έγιναν στο 6ο Δημοτικό. Η 2η μέτρηση έγινε σε πολύ ισχυρή βροχή και για τις δύο υποπεριπτώσεις. Είναι φανερή η επίδραση του Snoop στη βελτίωση της επικοινωνίας σε πολύ μεγάλο βαθμό. Η 3η μέτρηση έγινε με άσχημο σχετικά καιρό, όχι όμως βροχή. Και πάλι η βελτίωση με το Snoop είναι αισθητή. Για την 4η μέτρηση είχαμε μεν συνεχή βροχή,

αλλά, όπως προαναφέραμε, λόγω του μεγάλου χρόνου που είχαμε στη μεταφόρτωση του αρχείου δεν πετύχαμε ίδιες ακριβώς καιρικές συνθήκες για τις δύο υποπεριπτώσεις. Και πάλι όμως το αποτέλεσμα είναι ικανοποιητικό. Η βελτίωση που επιφέρει το πρωτόκολλο Snoop φαίνεται στην Εικόνα 8-44.



Εικόνα 8-44. Βελτίωση που επιφέρει το πρωτόκολλο Snoop στη μεταφόρτωση αρχείων διαφόρων μεγεθών.

8.3. Μετρήσεις με μεταβλητό μήκος δεδομένων πακέτου TCP

Πέρα από τις μετρήσεις επιδόσεων του δικτύου, καθώς και την απλή εφαρμογή του πρωτοκόλλου Snoop, έγιναν μετρήσεις και με αλλαγή του μήκους του πακέτου TCP. Στόχος είναι η μελέτη της επίδρασης της μεταβολής του μήκους δεδομένων του πακέτου TCP στην απόδοση του δικτύου τόσο με απλό TCP, όσο και με Improved TCP (με τη χρήση του Snoop).

Οι μετρήσεις έγιναν και σε περιβάλλον Windows και σε περιβάλλον Linux. Το μήκος του πακέτου είναι εξ ορισμού 1500 bytes που είναι η προτεινόμενη τιμή για τη βέλτιστη απόδοση ενός δικτύου Ethernet, DSL και ενσύρματων ευρυζωνικών συνδέσεων. Πάντα όμως υπάρχουν περιπτώσεις όπου προτείνονται άλλα μήκη, κυρίως μικρότερα, π.χ. σε Dial Up συνδέσεις προτείνεται μήκος 576 bytes [8]. Είχαμε τη δυνατότητα μόνο να μειώσουμε το μήκος του πακέτου. Ο περιορισμός αυτός τίθεται από τους δρομολογητές του δικτύου μας.

8.3.1. Αλλαγή μεγέθους πακέτου TCP

Σε περιβάλλον Windows

Για να επιτευχθεί η αλλαγή μεγέθους πακέτου TCP στα Windows απαιτείται επέμβαση στο μητρώο του συστήματος. Συγκεκριμένα πρέπει να τεθεί στο κλειδί HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\[Adapter ID] (όπου Adapter ID είναι η συσκευή που ρυθμίζει τη σύνδεση με το δίκτυο) μία

παράμετρος με τα παρακάτω ορίσματα και τιμές:

- **Value Name:** MTU
- **Data Type:** REG_DWORD (DWORD Value)
- **Value Data:** Default = 0xffffffff

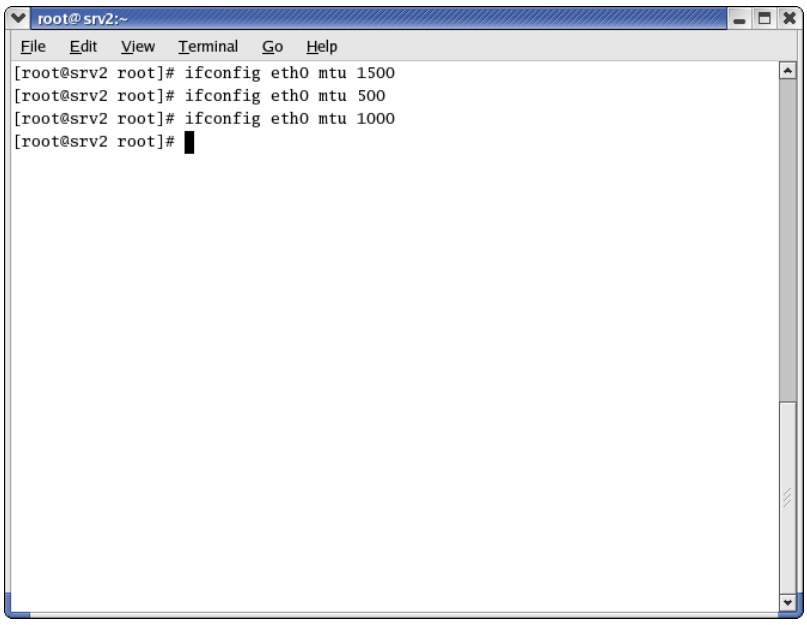
Η αλλαγή αυτή ισχύει για τα Windows 2000, XP και Server 2003, ενώ για τα 98 υπάρχει παρόμοια επέμβαση. Έτσι θέτοντας τιμή (Value Data) σε δεκαδική μορφή 500, 1000, 1500 πετύχαμε αντίστοιχες ρυθμίσεις για το μέγεθος του πακέτου TCP. Να σημειωθεί ότι μετά από κάθε αλλαγή απαιτείται επανεκκίνηση του συστήματος.

Σε περιβάλλον Linux

Για να επιτευχθεί η αλλαγή μεγέθους πακέτου TCP στο Linux απαιτείται μία απλή εντολή στη γραμμή εντολών. Αυτό ισχύει για τη μείωση του μήκους του πακέτου. Για την αύξηση του μήκους, την οποία όμως λόγω ρυθμίσεων δρομολογητή δεν μπορούσαμε να επιτύχουμε, χρειάζεται επέμβαση στο αρχείο **/etc/sysconfig/network-scripts/icfg-eth0** (το eth0 αφορά τη συσκευή διασύνδεσης και είναι φυσικά στην περίπτωσή μας η κάρτα δικτύου). Εκεί τίθεται μία νέα σειρά-παράμετρος π.χ. MTU=1500. Επίσης πρέπει να αλλαχθεί και το αρχείο **/etc/ppp/options** όπου πρέπει να τεθούν τιμές π.χ. MTU=1500 και MRU=1500. Αυτές οι ρυθμίσεις είναι σχετικές με τη διανομή που χρησιμοποιούμε (Red Hat) και απαιτούν επανεκκίνηση του συστήματος. Η απλή εντολή που χρησιμοποιήσαμε για την αλλαγή μήκους πακέτου TCP είναι η εξής:

```
ifconfig eth0 mtu 1500
```

όπου και πάλι eth0 είναι η συγκεκριμένη στην περίπτωσή μας συσκευή σύνδεσης στο δίκτυο, η κάρτα δικτύου. Παρακάτω βλέπουμε τις αλλαγές του μήκους του πακέτου στο Linux οι οποίες γίνονται χωρίς να απαιτείται επανεκκίνηση του συστήματος. Βλέπουμε στην Εικόνα 8-45 τις αλλαγές του μήκους πακέτου, όπως αυτές έγιναν σε ένα συγκεκριμένο σύνολο μετρήσεων. Οι μετρήσεις λαμβάνονταν αλλάζοντας κάθε φορά το μέγεθος του πακέτου βάσει των εντολών που φαίνονται στην Εικόνα 8-45.



Εικόνα 8-45. Αλλαγή μεγέθους πακέτου TCP σε Linux.

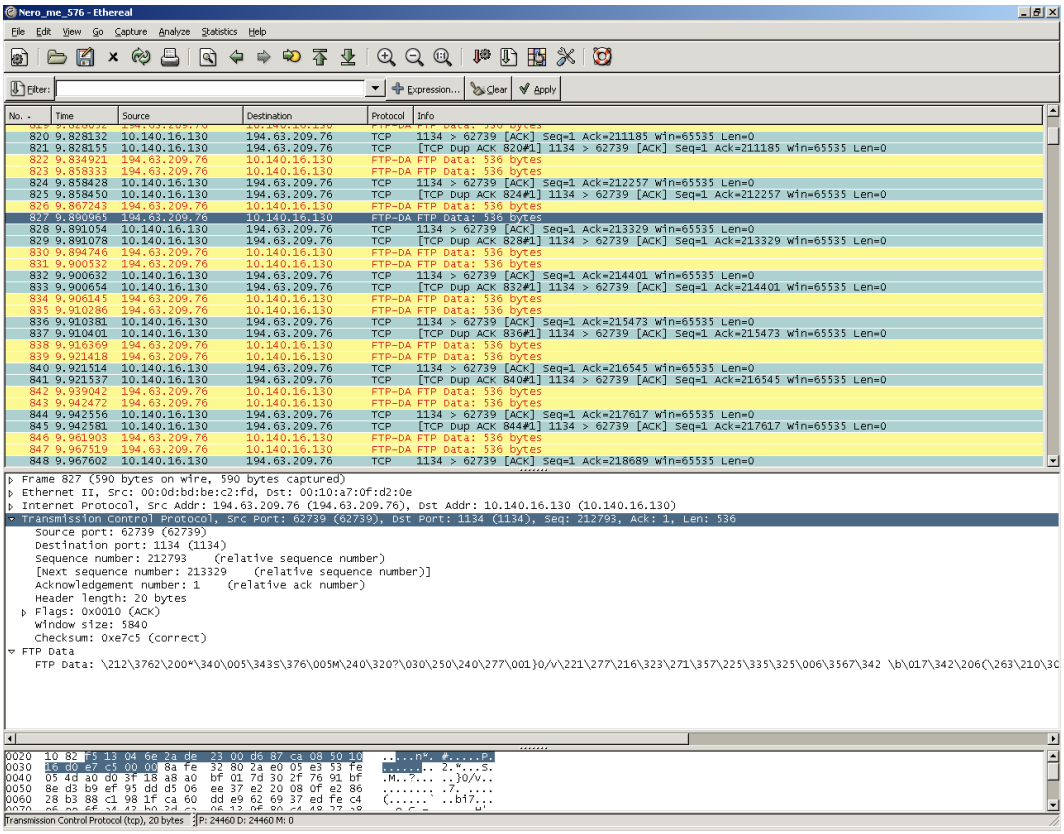
Οι μετρήσεις έγιναν με μεγέθη πακέτου TCP 500 και 1500 bytes σε περιβάλλον Windows και 500, 1000 και 1500 bytes σε περιβάλλον Linux.

8.3.2. Συγκριτικές μετρήσεις αρχείου 6,5 MB σε Windows

Οι πρώτες συγκριτικές μετρήσεις για την επίδραση του Snoop με ταυτόχρονη αλλαγή του μήκους του πακέτου έγιναν με τη χρήση του αρχείου του Nero Express. Οι μετρήσεις έγιναν στο 1ο Γυμνάσιο Κιλκίς, σε περιβάλλον Windows, με καλό καιρό, πρωινές ώρες, με τις ιδιαιτερότητες του σημείου αυτού να έχουν αναφερθεί σε προηγούμενα κεφάλαια.

Μετρήσεις με μέγεθος πακέτου TCP 500 bytes

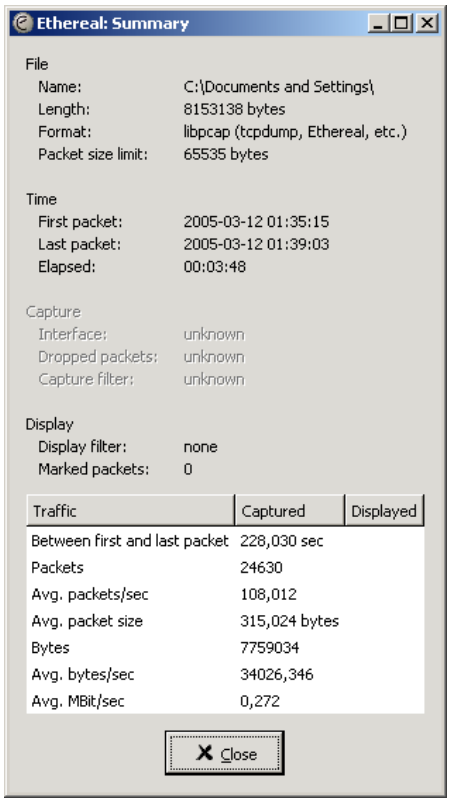
Παρακάτω βλέπουμε την οθόνη με το αρχείο σύλληψης στο Ethereal όπου και γίνεται φανερό το μέγεθος του πακέτου του TCP στην περίπτωση που το Snoop είναι on.



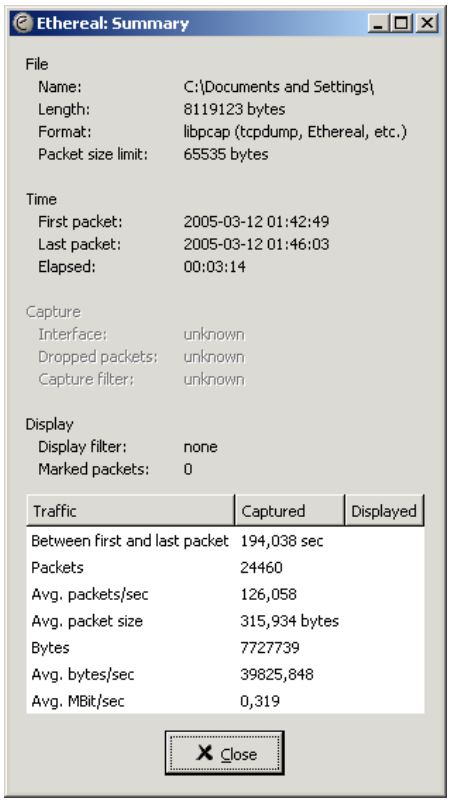
Εικόνα 8-46.. Κίνηση πακέτων για μήκος πακέτου TCP 500 bytes με Snoop on.

Ένα σχόλιο που είναι απαραίτητο αφορά το μήκος του πακέτου. Αν και εμείς το ορίζαμε 500 ή 1000 ή 1500, το σύστημα κάθε φορά χρησιμοποιούσε ένα μέγεθος πολύ κοντά στην τιμή που δίναμε, όχι όμως ακριβώς την ίδια. Αυτό διότι προσαρμόζεται το μήκος του πακέτου ανάλογα και με την επιπλέον πληροφορία (π.χ. δεδομένα ελέγχου, προορισμού κ.λπ.) που πρέπει να έχει αυτό. Για τον λόγο αυτό εδώ βλέπουμε το μήκος να είναι 536 bytes.

Για την περίπτωση του Snoop είναι off παίρνουμε μία αντίστοιχη εικόνα. Αυτό που μας ενδιαφέρει είναι τα συγκριτικά αποτελέσματα. Παρακάτω βλέπουμε τις συνοπτικές πληροφορίες για τις δύο περιπτώσεις.

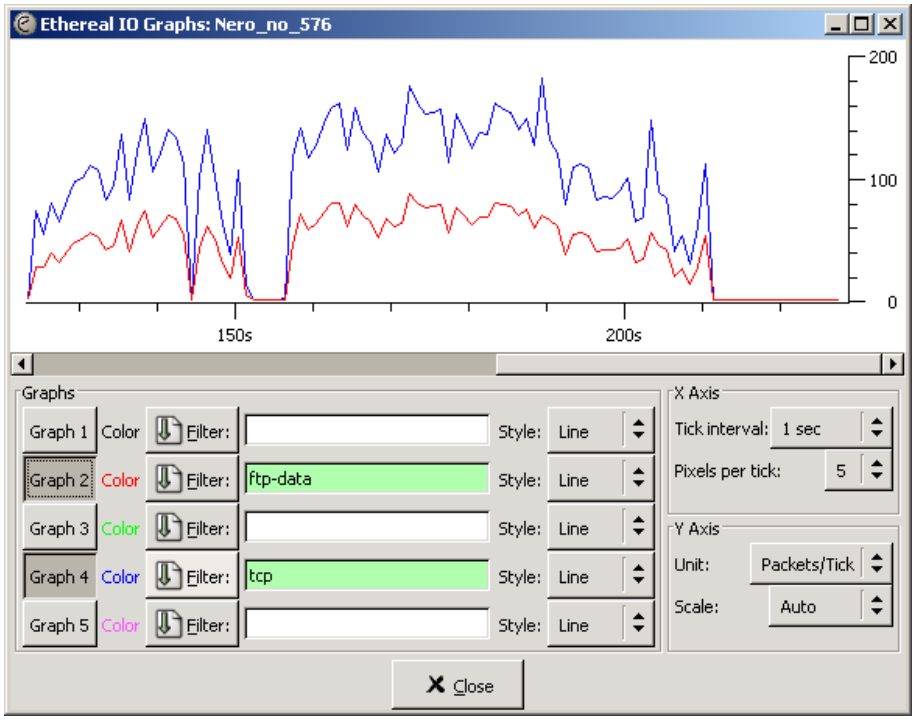


Εικόνα 8-47. Συνοπτικές πληροφορίες για μέγεθος πακέτου 500 bytes και Snoop off.

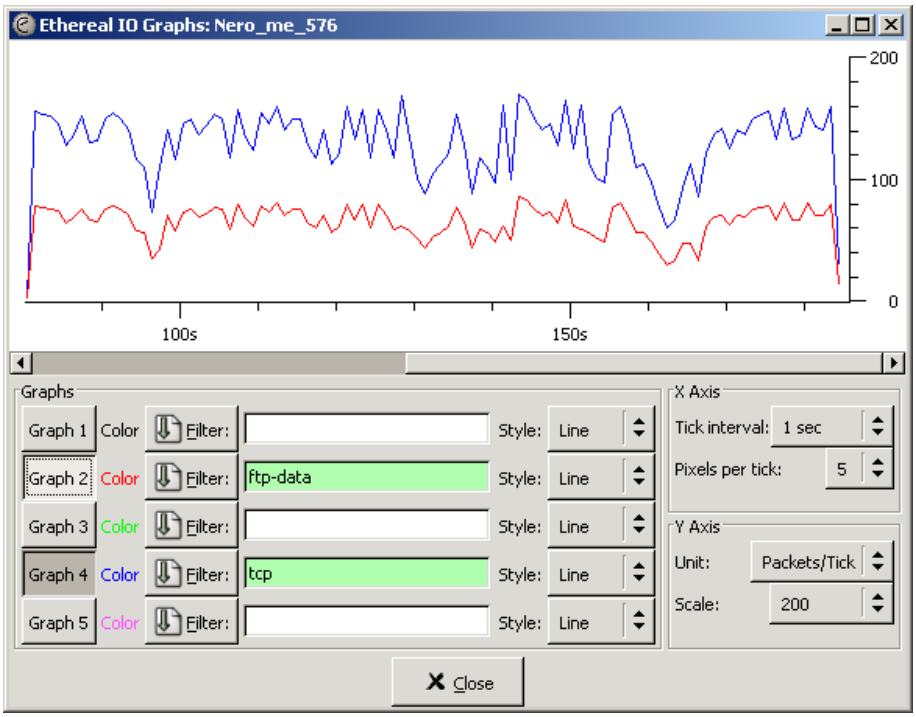


Εικόνα 8-48. Συνοπτικές πληροφορίες για μέγεθος πακέτου 500 bytes και Snoop on.

Τα διαγράμματα κίνησης στο δίκτυο των δύο επόμενων εικόνων φανερώνουν και πάλι τη βελτίωση με το πρωτόκολλο Snoop.



Εικόνα 8-49. Σχέση TCP με FTP-DATA με μέγεθος TCP πακέτου 500 bytes με Snoop off.



Εικόνα 8-50. Σχέση TCP με FTP-DATA με μέγεθος TCP πακέτου 500 bytesμε Snoop on.

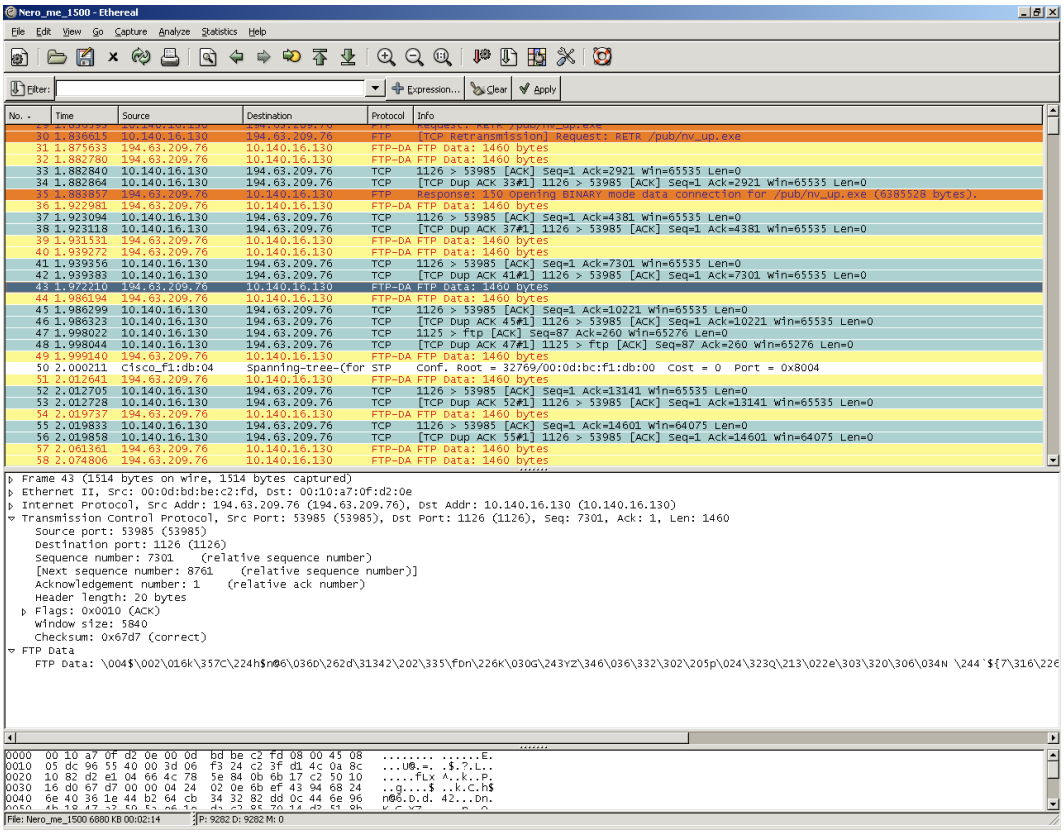
Από τα παραπάνω διαγράμματα γίνεται φανερό το γεγονός της μεγάλης βελτίωσης με το πρωτόκολλο Snoop.

Μετρήσεις με μέγεθος πακέτου TCP 1500 bytes

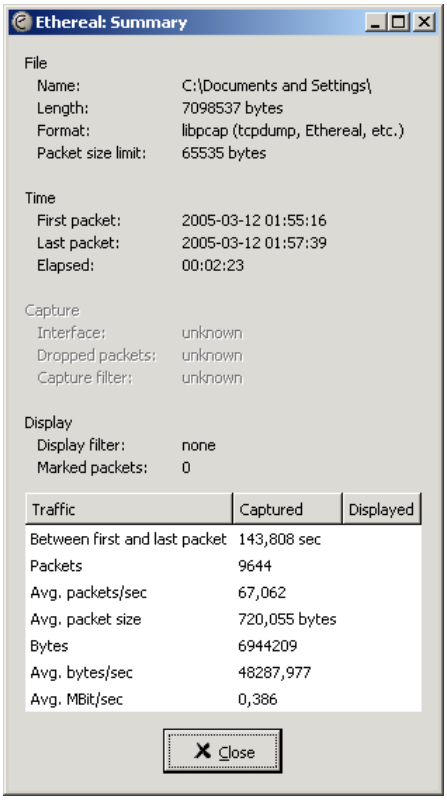
Ακριβώς η ίδια μέτρηση για το ίδιο αρχείο και με τις ίδιες συνθήκες, γίνεται και με το μήκος πακέτου TCP να είναι 1500 bytes. Παρακάτω βλέπουμε (Εικόνα 8-51) την οθόνη με το αρχείο σύλληψης στο Ethereal όπου και γίνεται φανερό το μέγεθος του πακέτου του TCP στην περίπτωση που το Snoop είναι on.

Ένα σχόλιο αφορά και πάλι το μήκος του πακέτου: για τον ίδιο λόγο που αναφέραμε και πιο πριν βλέπουμε το μήκος να είναι 1460 bytes.

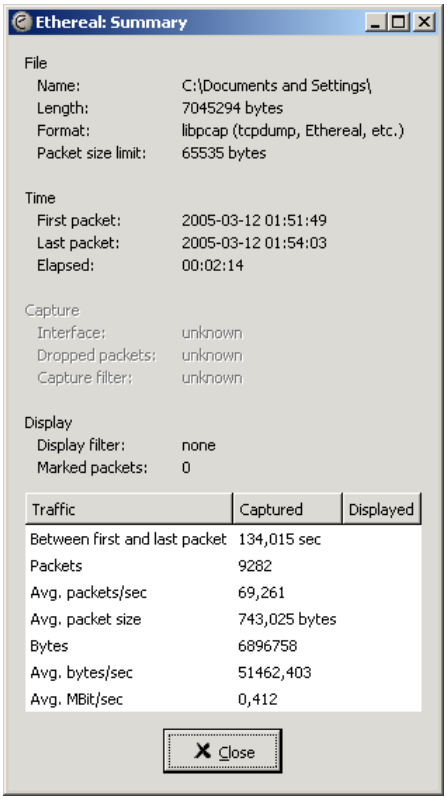
Για την περίπτωση του Snoop είναι Off παίρνουμε μία αντίστοιχη εικόνα. Αυτό που μας ενδιαφέρει είναι τα συγκριτικά αποτελέσματα. Παρακάτω βλέπουμε τις συνοπτικές πληροφορίες για τις δύο περιπτώσεις.



Εικόνα 8-51. Κίνηση πακέτων για μέγεθος πακέτου TCP 1500 bytes με Snoop on.

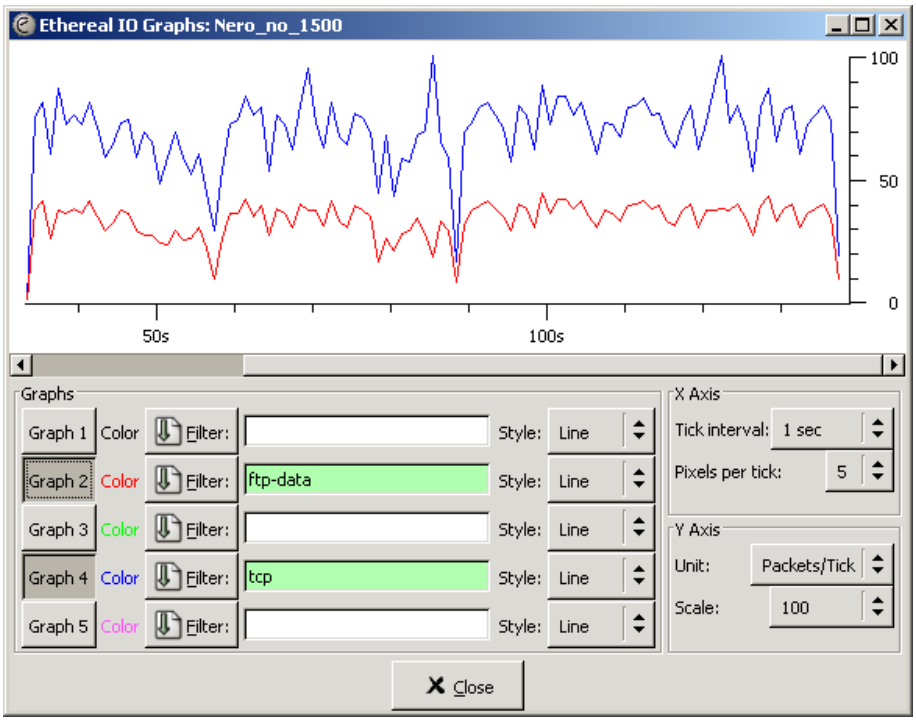


Εικόνα 8-52. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1500 bytes και Snoop off.

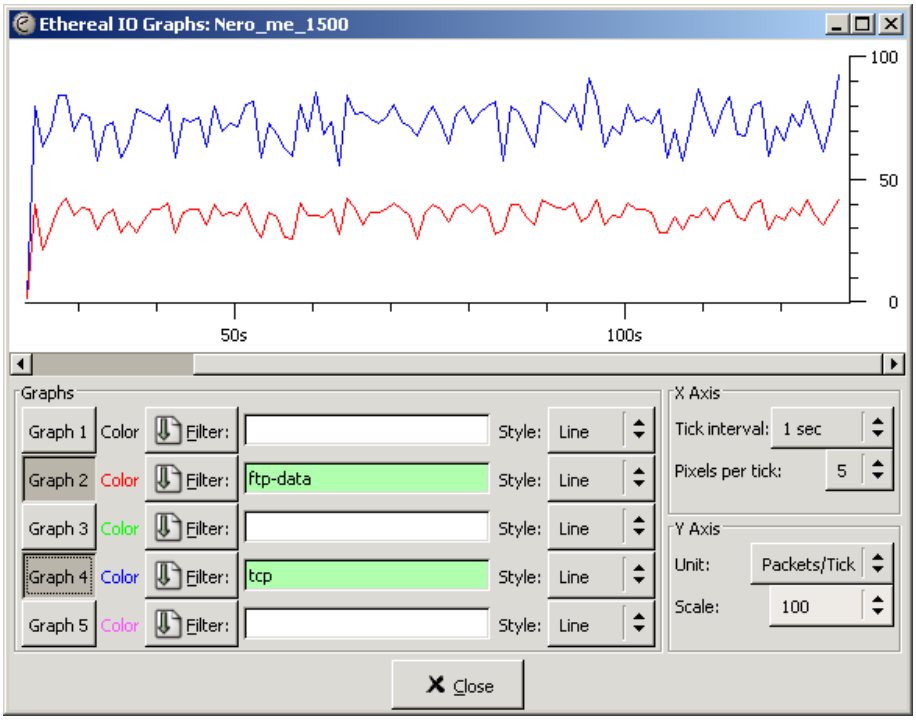


Εικόνα 8-53. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1500 bytes και Snoop on.

Ακολουθούν οι γραφικές παραστάσεις με την παράλληλη παρουσίαση της καμπύλης καθαρών FTP-DATA πακέτων με αυτήν που παρουσιάζει όλα τα TCP πακέτα. Η καμπύλη αυτή μάς δίνει τη δυνατότητα να σχολιάσουμε τη γενική επίδραση του μήκους του πακέτου στην επικοινωνία, αλλά και στην επίδραση του Snoop.



Εικόνα 8-54. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1500 B και Snoop off.



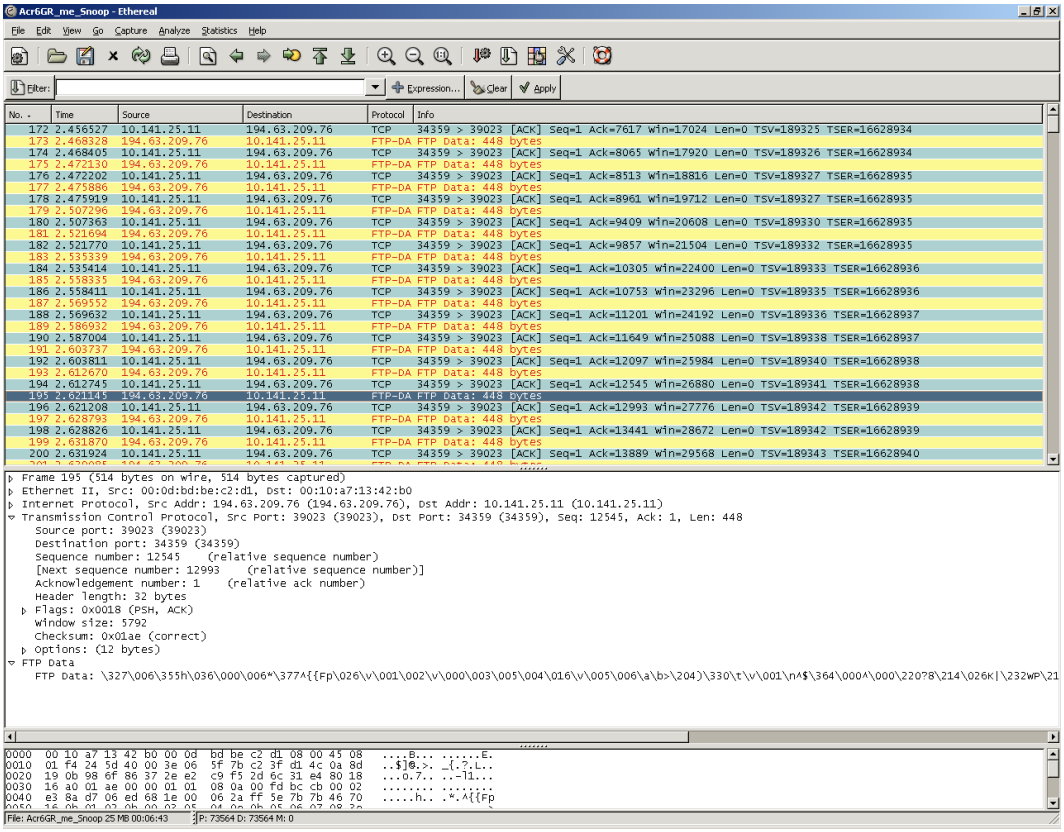
Εικόνα 8-55. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1500 B και Snoop on.

8.3.3. Συγκριτικές μετρήσεις αρχείου 20 MB σε Linux

Με αντίστοιχο τρόπο έχουμε και τις μετρήσεις για το αρχείο Acrobat Reader 6, ελληνική έκδοση, μεγέθους περίπου 20 MB. Η μετρήσεις έγιναν από το 6ο Δημοτικό με πολύ καλό καιρό σε τρεις περιπτώσεις μεγέθους πακέτου TCP 500, 1000, 1500 bytes.

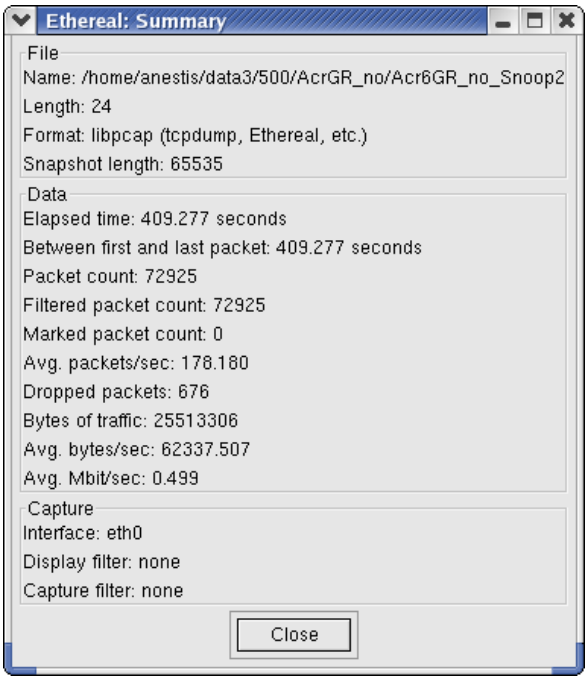
Μετρήσεις με μέγεθος πακέτου TCP 500 bytes

Στην Εικόνα 8-56 βλέπουμε την οθόνη με το αρχείο σύλληψης στο Ethereal όπου και γίνεται φανερό το μέγεθος του πακέτου του TCP στην περίπτωση που το Snoop είναι on.

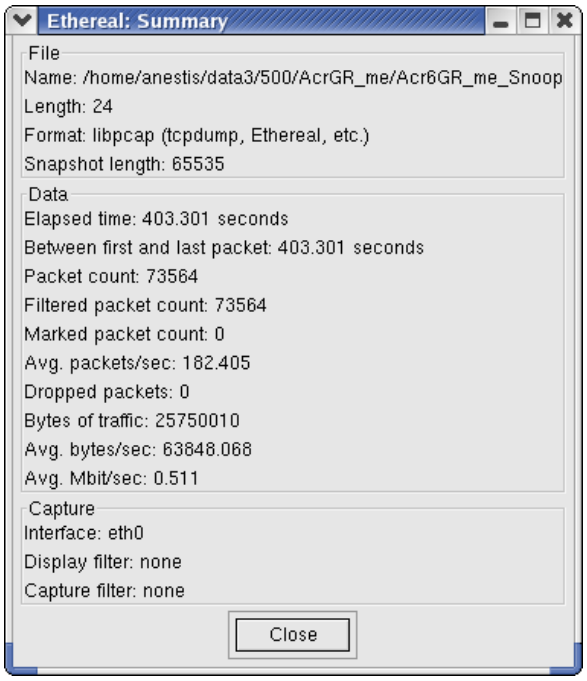


Εικόνα 8-56. Κίνηση πακέτων για μέγεθος πακέτου TCP 500 bytes με Snoop on.

Και πάλι ισχύουν τα σχόλια που κάναμε πιο πριν σχετικά με το ακριβές μήκος του πακέτου. Σε κάθε περίπτωση μας ενδιαφέρουν τα στατιστικά στοιχεία τα οποία βλέπουμε παρακάτω.

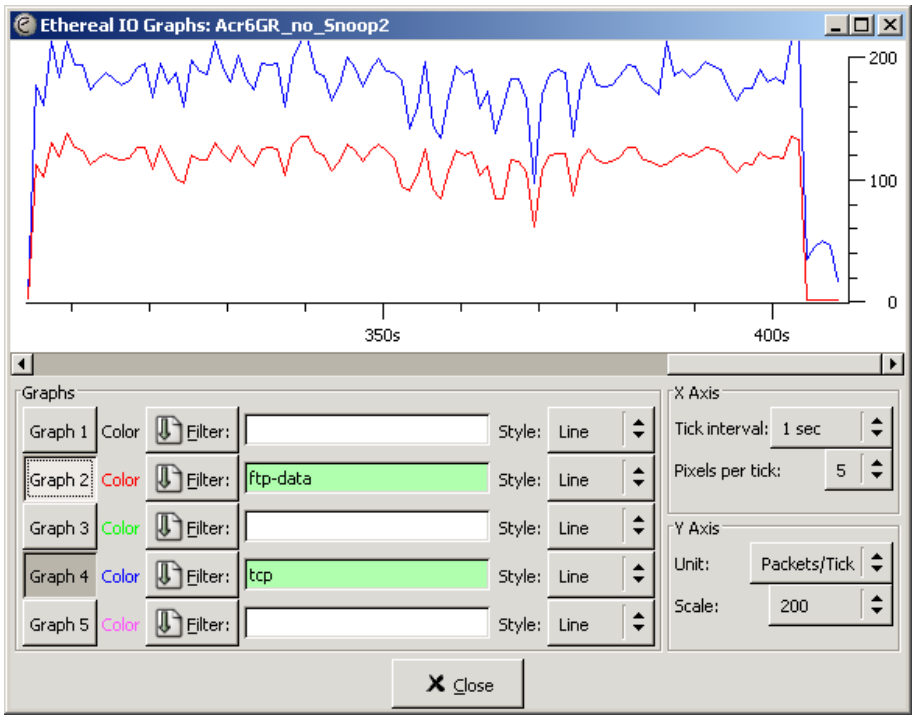


Εικόνα 8-57. Συνοπτικές πληροφορίες για μέγεθος πακέτου 500 bytes και Snoop off.

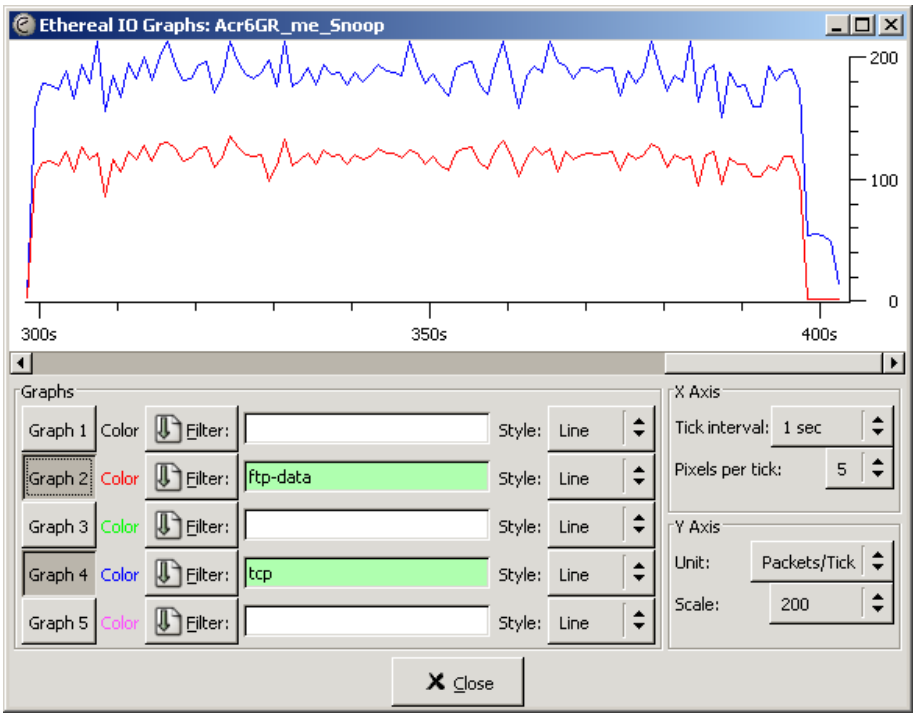


Εικόνα 8-58. Συνοπτικές πληροφορίες για μέγεθος πακέτου 500 bytes και Snoop on.

Ακολουθούν οι γραφικές παραστάσεις με την παράλληλη παρουσίαση της καμπύλης καθαρών FTP-DATA πακέτων σε αντιδιαστολή με αυτήν που παρουσιάζει όλα τα TCP πακέτα.



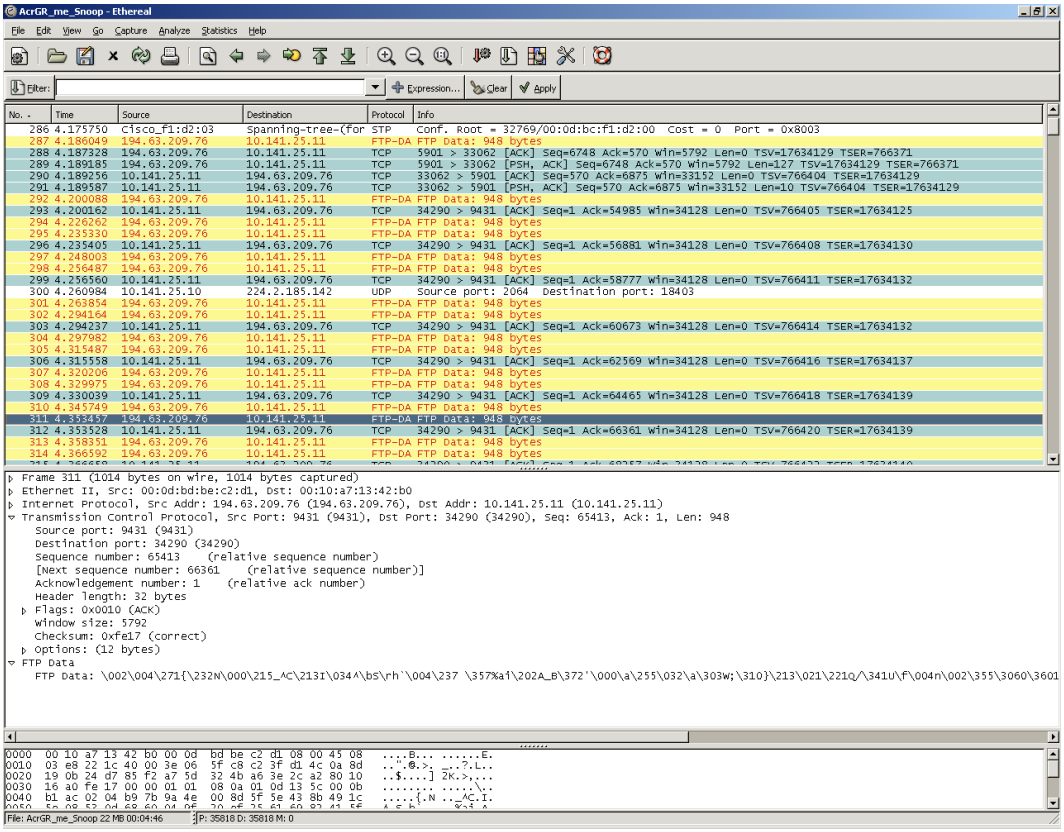
Εικόνα 8-59. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 500 B και Snoop off.



Εικόνα 8-60. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 500 B και Snoop on.

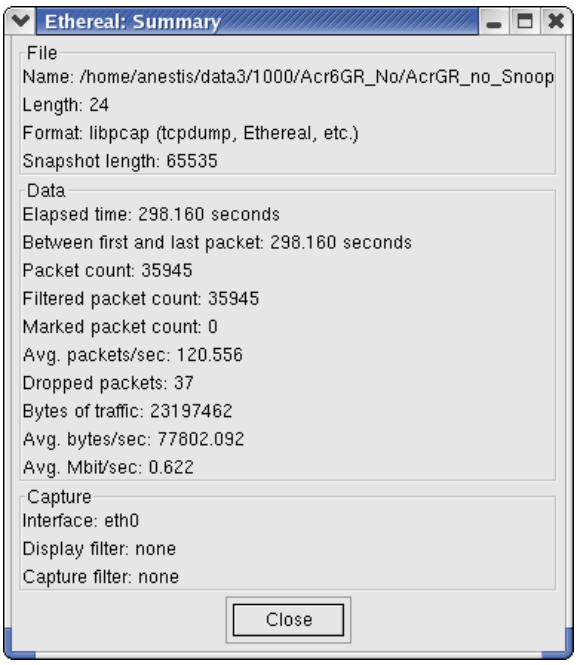
Μετρήσεις με μέγεθος πακέτου TCP 1000 bytes

Παρακάτω βλέπουμε την οθόνη με το αρχείο σύλληψης στο Ethereal όπου και γίνεται φανερό το μέγεθος του πακέτου του TCP στην περίπτωση που το Snoop είναι on.

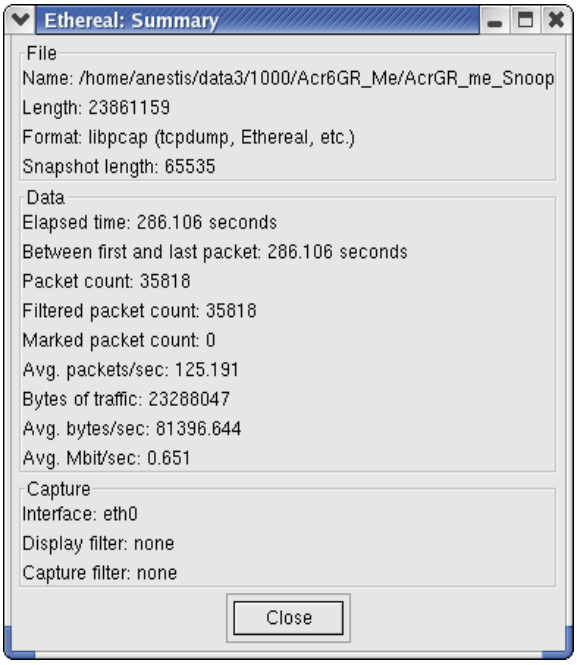


Εικόνα 8-61. Κίνηση πακέτων για μέγεθος πακέτου TCP 1000 bytes με Snoop on.

Για την περίπτωση του Snoop είναι Off παίρνουμε μία αντίστοιχη εικόνα. Αυτό που μας ενδιαφέρει είναι τα συγκριτικά αποτελέσματα. Παρακάτω βλέπουμε τις συνοπτικές πληροφορίες για τις δύο περιπτώσεις.

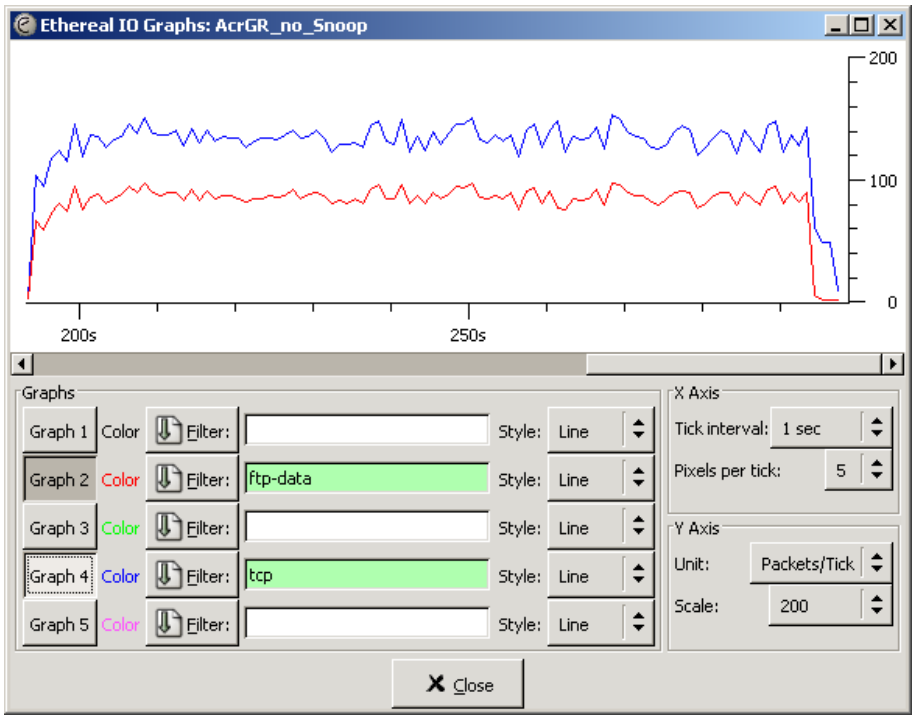


Εικόνα 8-62. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1000 bytes και Snoop off.

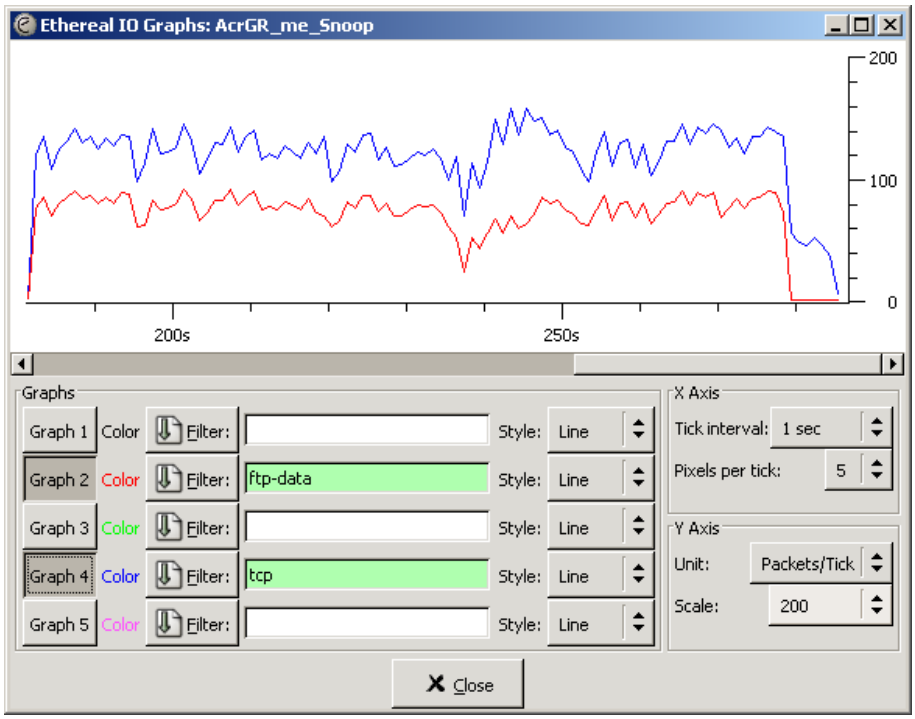


Εικόνα 8-63. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1000 bytes και Snoop on.

Ακολουθούν οι γραφικές παραστάσεις με την παράλληλη παρουσίαση της καμπύλης καθαρών FTP-DATA πακέτων με αυτήν που παρουσιάζει όλα τα TCP πακέτα.



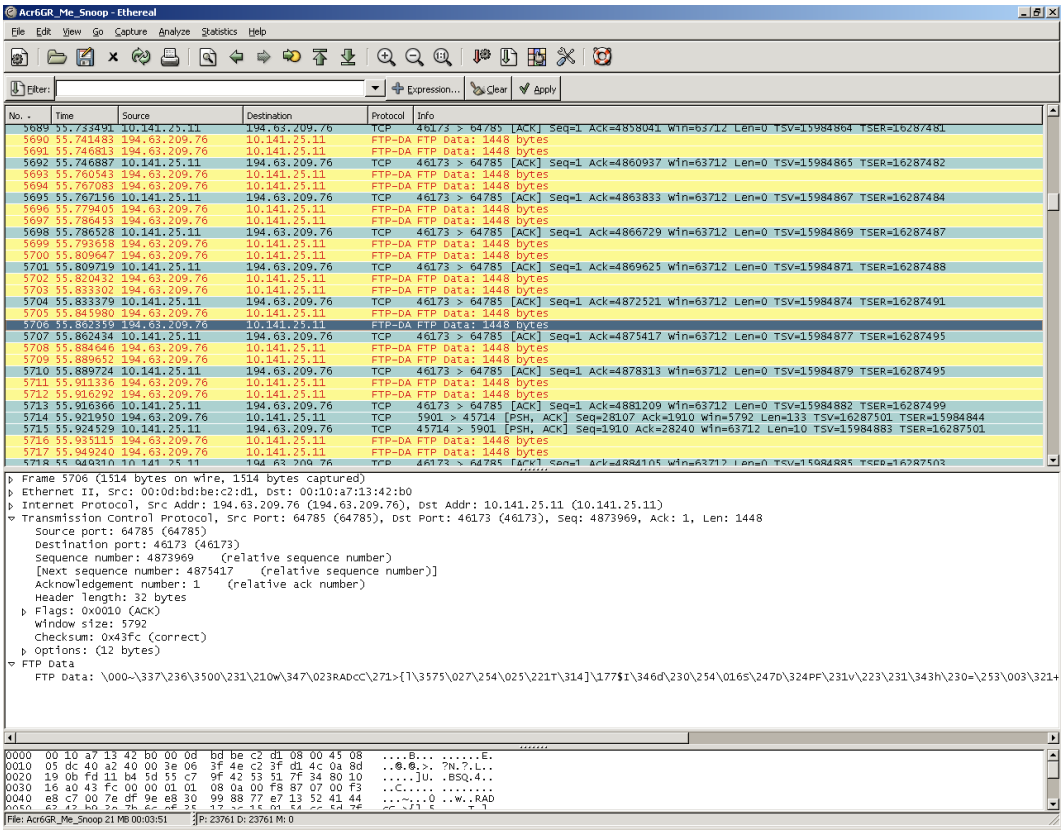
Εικόνα 8-64. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1000 B και Snoop off.



Εικόνα 8-65. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1000 B και Snoop on.

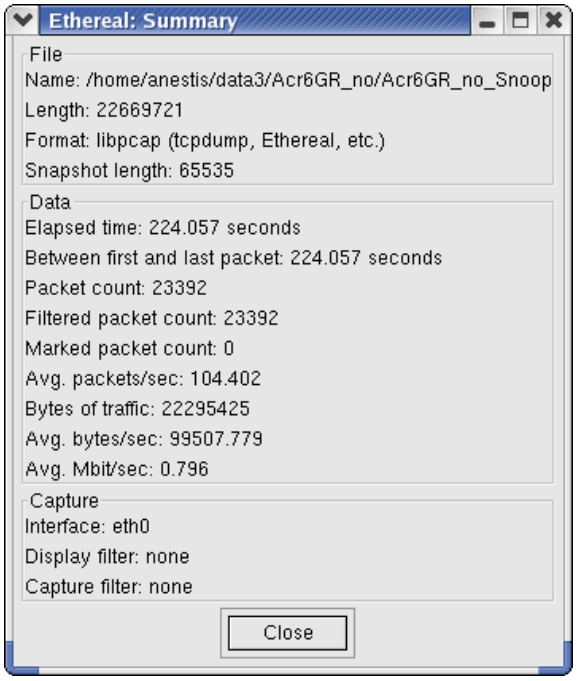
Μετρήσεις με μέγεθος πακέτου TCP 1500 bytes

Παρακάτω βλέπουμε την οθόνη με το αρχείο σύλληψης στο Ethereal όπου και γίνεται φανερό το μέγεθος του πακέτου του TCP στην περίπτωση που το Snoop είναι on.

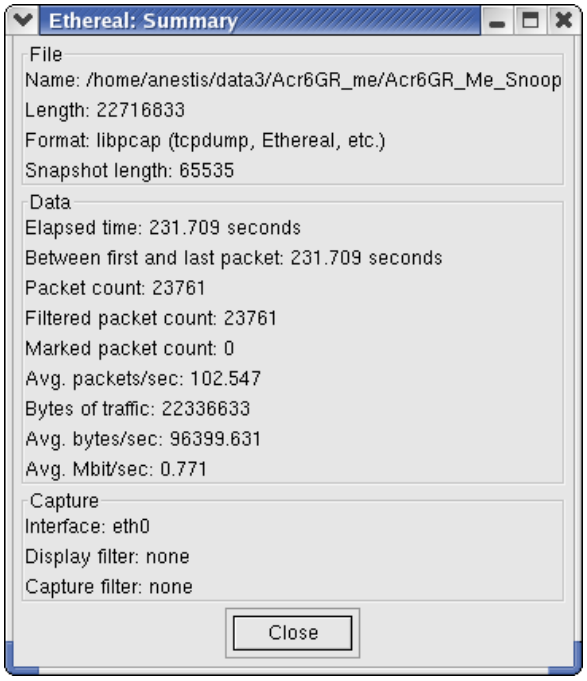


Εικόνα 8-66. Κίνηση πακέτων για μέγεθος πακέτου TCP 1000 bytes με Snoop on.

Για την περίπτωση του Snoop είναι off παίρνουμε μία αντίστοιχη εικόνα. Αυτό που μας ενδιαφέρει σε κάθε περίπτωση είναι τα συγκριτικά αποτελέσματα. Παρακάτω βλέπουμε τις συνοπτικές πληροφορίες για τις δύο περιπτώσεις.

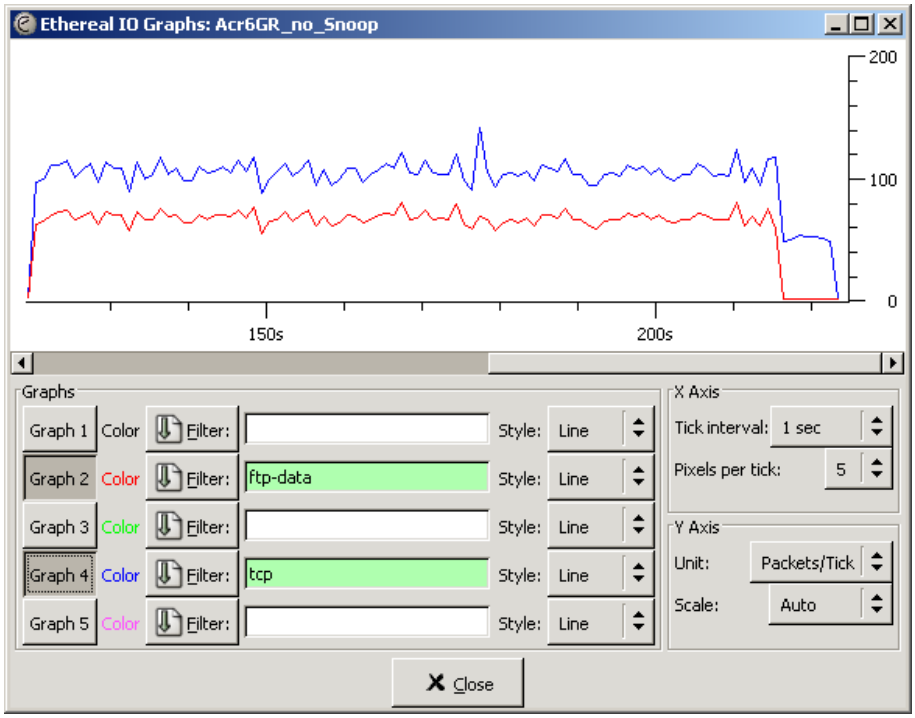


Εικόνα 8-67. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1000 bytes και Snoop off.

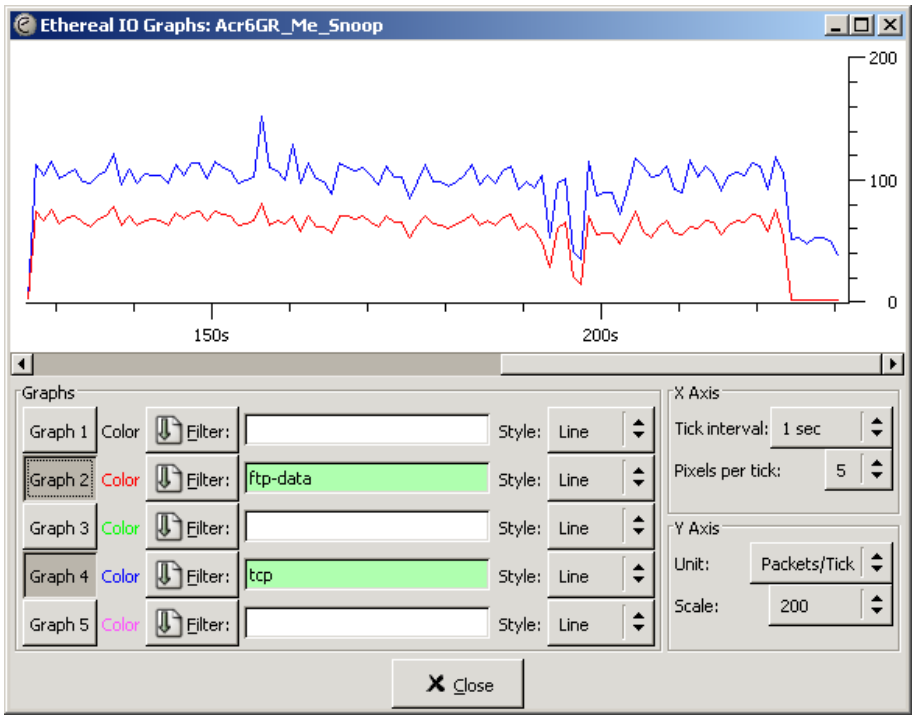


Εικόνα 8-68. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1000 bytes και Snoop on.

Ακολουθούν οι γραφικές παραστάσεις με την παράλληλη παρουσίαση της καμπύλης καθαρών FTP-DATA πακέτων με αυτήν που παρουσιάζει όλα τα TCP πακέτα.



Εικόνα 8-69. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1000 B και Snoop off.



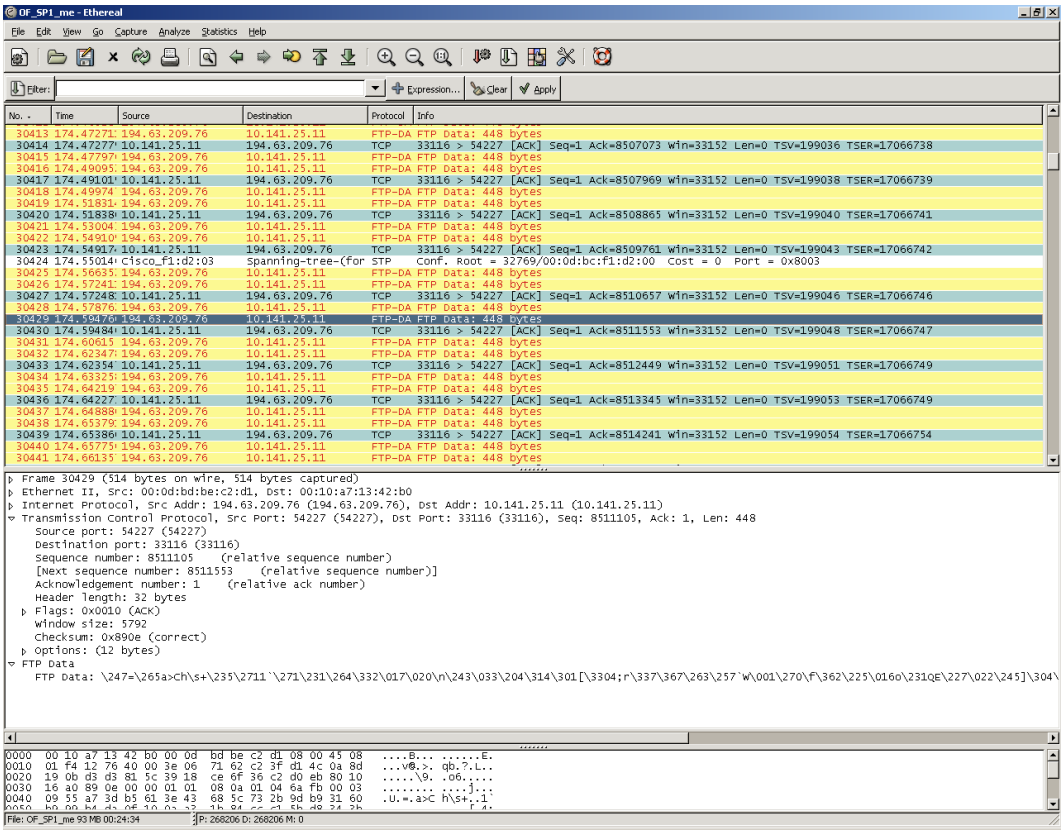
Εικόνα 8-70. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1000 B και Snoop on.

8.3.4. Συγκριτικές μετρήσεις αρχείου 72 MB σε Linux

Με αντίστοιχο τρόπο έχουμε και τις μετρήσεις για το αρχείο το αρχείο Microsoft Office 2003 SP1, ελληνική έκδοση, μεγέθους περίπου 72 MB. Η μετρήσεις έγιναν από το 6ο Δημοτικό με πολύ καλό καιρό σε δύο περιπτώσεις μεγέθους πακέτου TCP 500 και 1500 bytes.

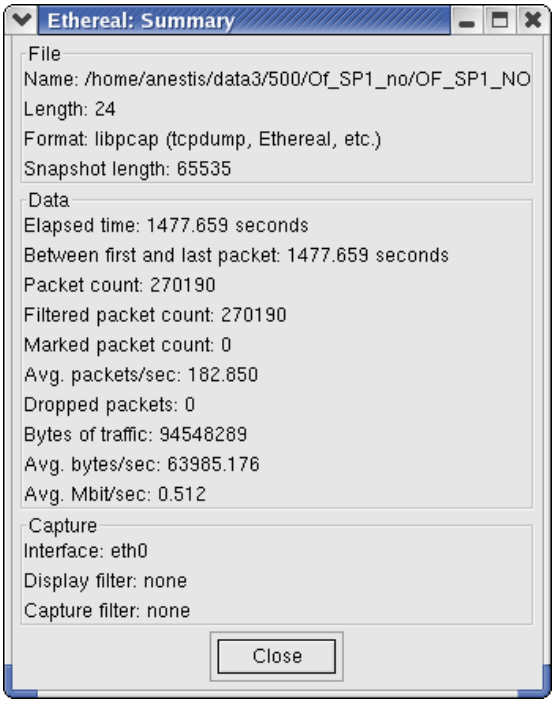
Μετρήσεις με μέγεθος πακέτου TCP 500 bytes

Παρακάτω βλέπουμε την οθόνη με το αρχείο σύλληψης στο Ethereal όπου γίνεται φανερό το μέγεθος του πακέτου του TCP στην περίπτωση που το Snoop είναι on.

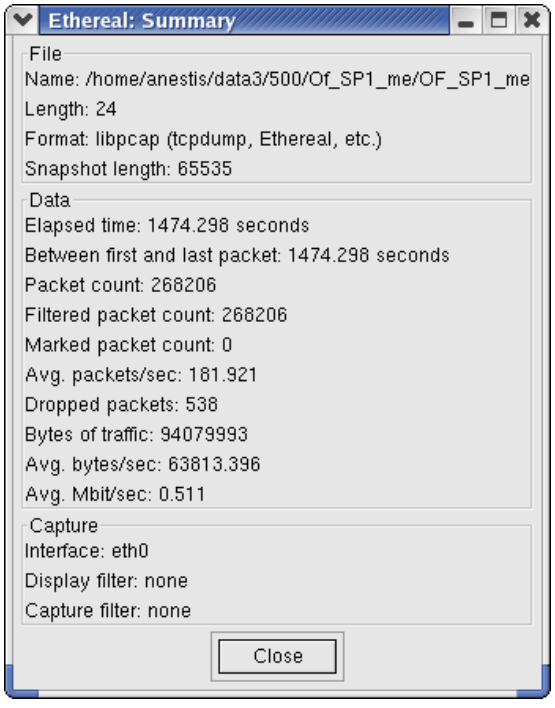


Εικόνα 8-71. Κίνηση πακέτων για μέγεθος πακέτου TCP 500 bytes με Snoop on.

Για την περίπτωση του Snoop είναι off παίρνουμε μία αντίστοιχη εικόνα.. Παρακάτω βλέπουμε τις συνοπτικές πληροφορίες για τις δύο περιπτώσεις, κάτι που μας βοηθά στην εξαγωγή συμπερασμάτων.

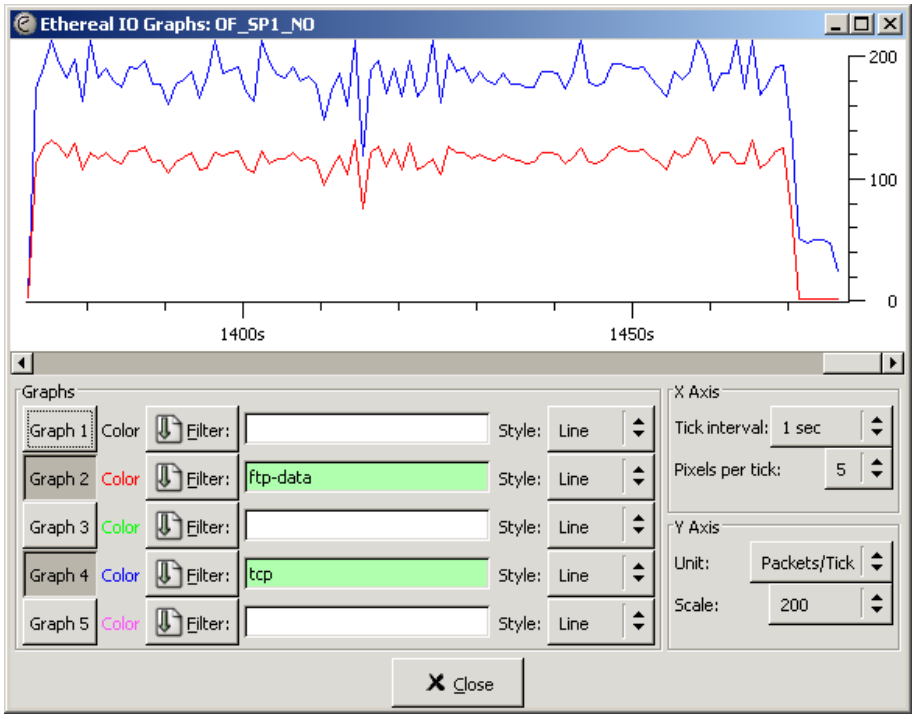


Εικόνα 8-72. Συνοπτικές πληροφορίες για μέγεθος πακέτου 500 bytes και Snoop off.

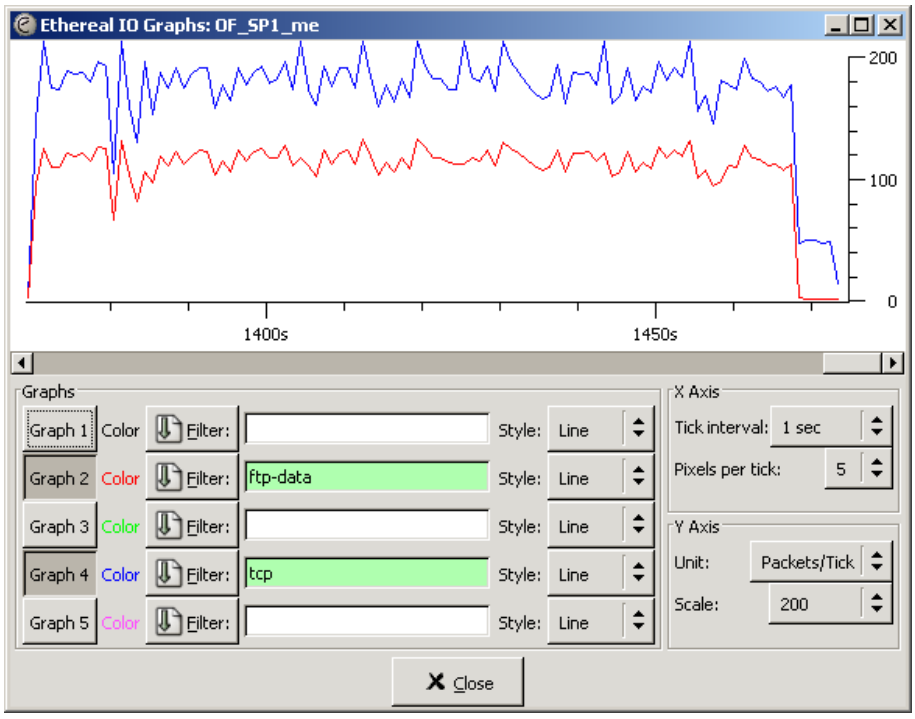


Εικόνα 8-73. Συνοπτικές πληροφορίες για μέγεθος πακέτου 500 bytes και Snoop on.

Ακολουθούν οι γραφικές παραστάσεις με την παράλληλη παρουσίαση της καμπύλης καθαρών FTP-DATA πακέτων με αυτήν που παρουσιάζει όλα τα TCP πακέτα.



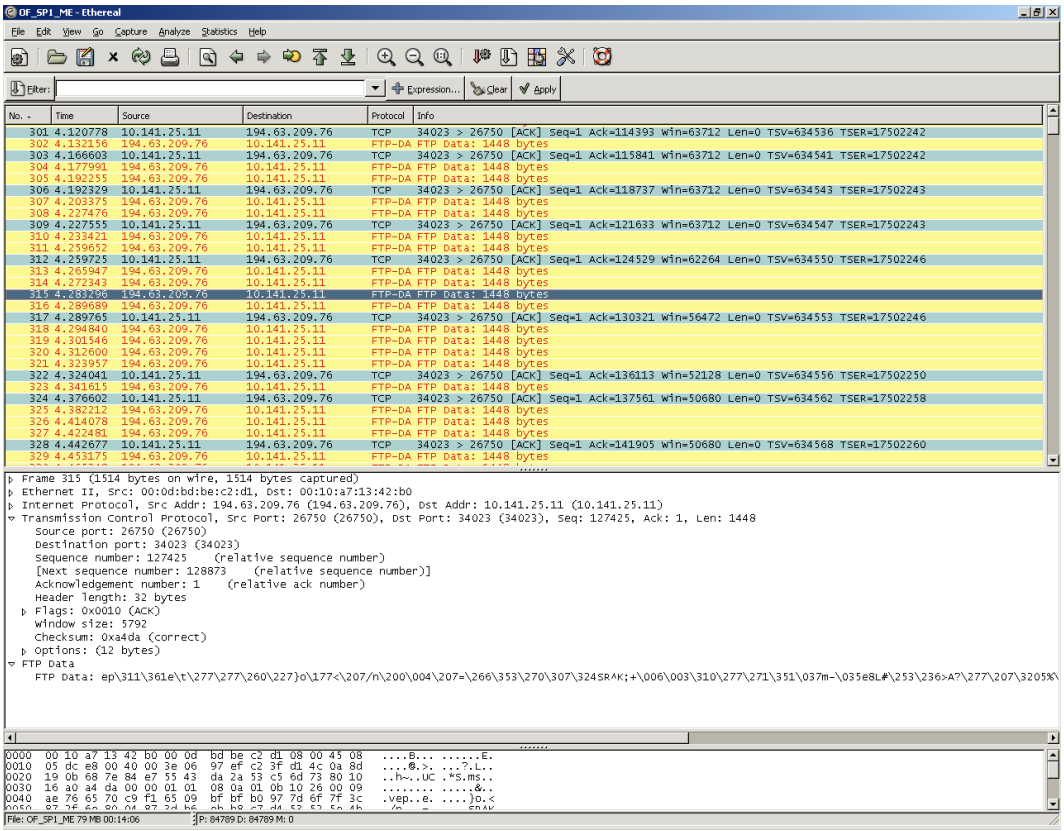
Εικόνα 8-74. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 500 B και Snoop off.



Εικόνα 8-75. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 500 B και Snoop on.

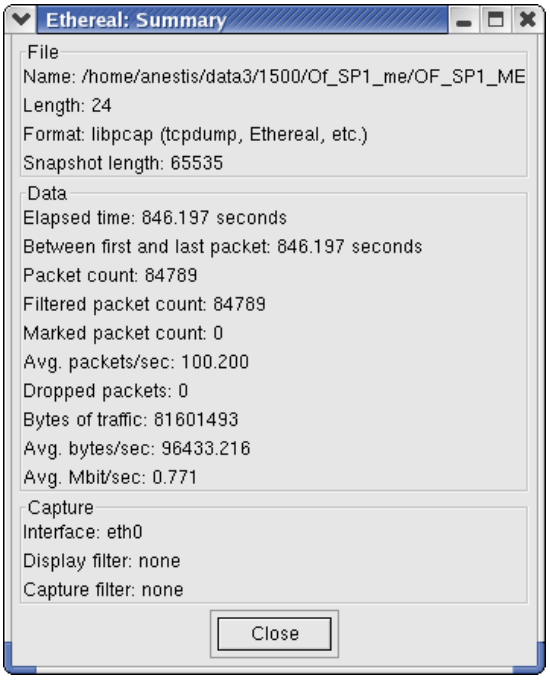
Μετρήσεις με μέγεθος πακέτου TCP 1500 bytes

Παρακάτω βλέπουμε την οθόνη με το αρχείο σύλληψης στο Ethereal όπου και γίνεται φανερό το μέγεθος του πακέτου του TCP στην περίπτωση που το Snoop είναι On.

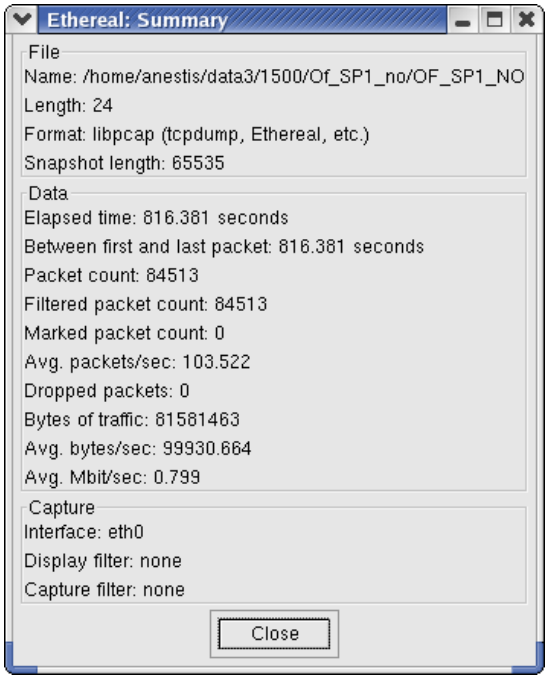


Εικόνα 8-76. Κίνηση πακέτων για μέγεθος πακέτου TCP 1500 bytes με Snoop on.

Για την περίπτωση του Snoop είναι Off παίρνουμε μία αντίστοιχη εικόνα. Αυτό που μας ενδιαφέρει είναι τα συγκριτικά αποτελέσματα. Παρακάτω βλέπουμε τις συνοπτικές πληροφορίες για τις δύο περιπτώσεις.

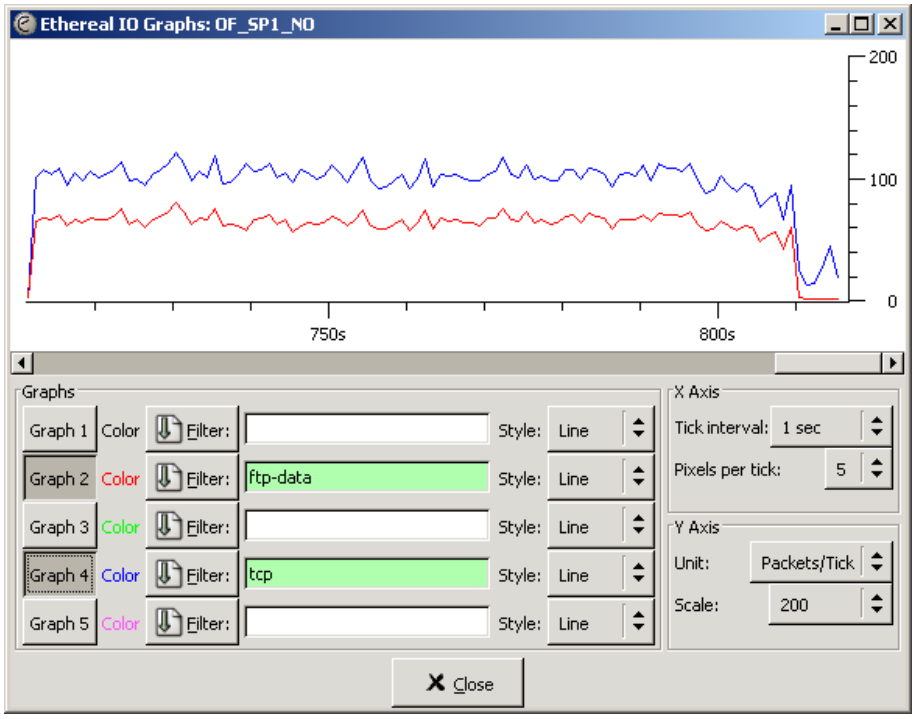


Εικόνα 8-77. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1500 bytes και Snoop off.

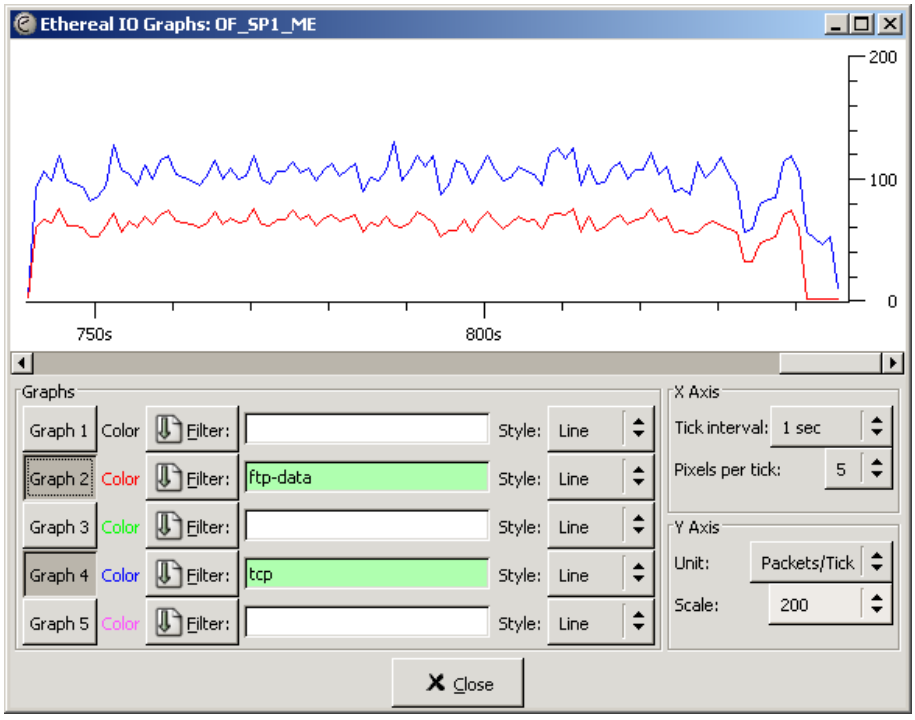


Εικόνα 8-78. Συνοπτικές πληροφορίες για μέγεθος πακέτου 1500 bytes και Snoop on.

Ακολουθούν οι γραφικές παραστάσεις με τη παράλληλη παρουσίαση της καμπύλης καθαρών FTP-DATA πακέτων με αυτήν που παρουσιάζει όλα τα TCP πακέτα



Εικόνα 8-79. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1500 B και Snoop off.



Εικόνα 8-80. Γραφική παράσταση TCP και FTP-DATA με μέγεθος πακέτου 1500 B και Snoop on.

8.3.5. Σύνοψη αποτελεσμάτων μετρήσεων

Στον παρακάτω πίνακα βλέπουμε μια γενική εικόνα του πρωτοκόλλου Snoop σε σχέση

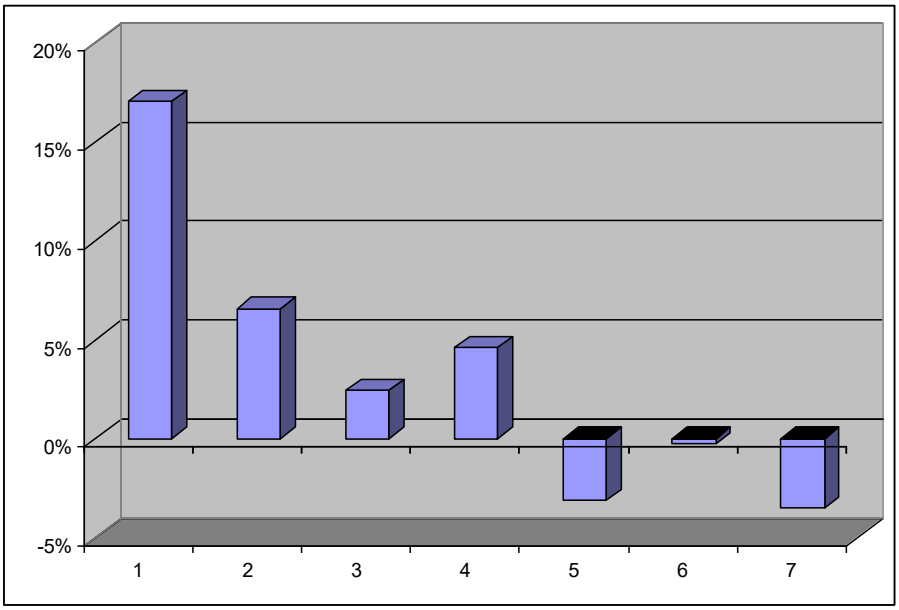
με το απλό TCP με δεδομένο τον μέσο όρο bytes/sec και για διαφορετικά μήκη πακέτων. Οι καιρικές συνθήκες ήταν συνεχώς πολύ καλές. Οι μετρήσεις όμως που λήφθηκαν από το 1ο Γυμνάσιο παρουσιάζουν μία διαφορετική εικόνα την οποία και σχολιάζουμε μετά το γράφημα.

Πίνακας 2. Μέσοι ρυθμοί μετάδοσης (bytes/sec) για διάφορα μεγέθη πακέτων και διάφορα μεγέθη αρχείων με Snoop off και on.

Α/Α	Μέτρηση	Average bytes/sec		Βελτίωση %	Λήψη
		Snoop off	Snoop on		
1	500 bytes Windows 1ο Γυμνάσιο 6,5 MB	34.026	39.826	17,05%	Δύσκολη
2	1500 bytes Windows 1ο Γυμνάσιο 6,5 MB	48.288	51.462	6,57%	Δύσκολη
3	500 bytes Linux 6ο Δημοτικό 20 MB	62.337	63.848	2,42%	Άριστη
4	1000 bytes Linux 6ο Δημοτικό 20 MB	77.802	81.396	4,62%	Άριστη
5	1500 bytes Linux 6ο Δημοτικό 20 MB	99.507	96.399	-3,12%	Άριστη
6	500 bytes Linux 6ο Δημοτικό 72 MB	63.985	63.813	-0,27%	Άριστη
7	1500 bytes Linux 6ο Δημοτικό 72 MB	99.930	96.433	-3,50%	Άριστη

Η 1η και 2η μέτρηση έγιναν στο 1ο Γυμνάσιο όπου υπάρχουν δυσκολίες λήψης. Αν και ο καιρός είναι εξαιρετικά καλός η επίδραση του πρωτοκόλλου Snoop είναι σημαντική. Επίσης γίνεται φανερό το γεγονός της καλύτερης ποσοστιαίας απόδοσης του Snoop στο μικρό μέγεθος πακέτου. Οι υπόλοιπες μετρήσεις είναι από το 6ο Δημοτικό. Η λήψη από το σημείο αυτό είναι άριστη και γίνεται φανερό ότι το πρωτόκολλο Snoop δε βελτιώνει σημαντικά τη λήψη. Μάλιστα σε μερικές περιπτώσεις η επίδοση με απλό TCP είναι καλύτερη. Πάλι όμως φαίνεται η επίδραση του Snoop σε σχέση με το μέγεθος του πακέτου TCP. Το πρωτόκολλο Snoop έχει καλύτερη επίδοση από το απλό TCP σε μικρό μήκος πακέτου. Όλα αυτά αναλύονται στο κεφαλαίο των συμπερασμάτων.

Το αντίστοιχο γράφημα δείχνει τη γενική εικόνα των μετρήσεων που έγιναν. Η επίδραση του πρωτοκόλλου Snoop γίνεται άμεσα αντιληπτή με το παρακάτω διάγραμμα.



Εικόνα 8-81. Βελτίωση που επιφέρει το πρωτόκολλο Snoop σε διάφορες περιπτώσεις μεταφόρτωσης αρχείων (Πίνακας 2).

9. Συμπεράσματα – Αξιολόγηση

Πολλά και σημαντικά είναι τα συμπεράσματα που μπορούν να αντληθούν από τα αποτελέσματα που λήφθηκαν κατά τη διάρκεια των μετρήσεών μας. Καταρχάς όμως, είναι σημαντικό να γίνουν κάποιες επισημάνσεις οι οποίες αφορούν τη συγκεκριμένη φύση του ασυρμάτου δικτύου που μελετήθηκε:

- Πρώτον, οι ασύρματοι κόμβοι βρίσκονταν συνεχώς σε σταθερή θέση και σε άμεση οπτική επαφή ο ένας με τον άλλο. Ως αποτέλεσμα, οι δυνατότητες βελτιστοποίησης της ασύρματης σύνδεσης είναι σαφώς περιορισμένες, καθώς το ίδιο το δίκτυο έχει εξ ορισμού πολύ καλή απόδοση. Επιπρόσθετα, η επιλογή των θέσεων τοποθέτησης των κεραιών σε κάθε περίπτωση ήταν τέτοια ώστε να επιτυγχάνεται όσο το δυνατόν πιο άμεση επαφή από τον έναν κόμβο στον άλλο, μειώνοντας ακόμα περισσότερο τα περιθώρια βελτίωσης του ασύρματου δικτύου. Σαφώς μεγαλύτερες δυνατότητες βελτιστοποίησης θα υπήρχαν σε περίπτωση που ένας από τους δύο κόμβους ήταν κινούμενος, οπότε θα λάμβαναν χώρα φαινόμενα ασυνεχών συνδέσεων και αλλαγής κυψέλης, φαινόμενα εξάλλου για τα οποία το πρωτόκολλο Snoop έχει ειδικά αναπτυχθεί για να τα αντιμετωπίζει αποτελεσματικότερα από το παραδοσιακό TCP.
- Δεύτερον, θα πρέπει να ληφθεί υπόψιν η αστάθεια των καιρικών φαινομένων. Αν και η ομάδα προσπάθησε να κάνει τις αντίστοιχες μετρήσεις όσο το δυνατόν πιο κοντά τη μία με την άλλη για να επιτύχει ομοιόμορφα αποτελέσματα, αυτό δυστυχώς δεν ήταν δυνατόν σε κάθε περίπτωση, ειδικά μάλιστα όταν η μέτρηση αφορούσε μεγάλου μεγέθους αρχεία. Ως αποτέλεσμα, σε μία περίπτωση υπήρξε επιδείνωση του καιρού προς το τέλος της μέτρησης, η οποία όμως, ενώ αλλοίωσε τα δεδομένα της, δεν αλλοίωσε τα τελικά συμπεράσματα, καθώς αυτά εξήχθησαν από το σύνολο της μέτρησης.

Μετρήσεις με το Monitoring System

Όσον αφορά τις μετρήσεις με το Monitoring System τα συμπεράσματα αφορούν την επίδοση του δικτύου σε επίπεδο δεδομένων. Αυτό που γίνεται φανερό είναι ότι το δίκτυο είναι εξαιρετικά δομημένο και ρυθμισμένο. Η επικοινωνία μεταξύ των κόμβων είναι πολύ καλή σε κάθε περίπτωση. Οι καιρικές συνθήκες και βέβαια επηρεάζουν την απόδοσή του, δεν είναι όμως απαγορευτικές για τη λειτουργία και την αξιοπιστία του. Αυτό φάνηκε στη μέτρηση σε συνθήκες χιονόπτωσης, όπου μπορεί να υπήρξε μείωση της επίδοσης, όμως η λειτουργία του δικτύου κρίθηκε ικανοποιητική.

Ένα άλλο σημείο στο οποίο πρέπει να γίνει αναφορά είναι επίδραση της απόστασης και της θέσης ενός σημείου. Αναφερόμαστε φυσικά στο 1ο Γυμνάσιο Κιλκίς, το οποίο είναι το πιο απομακρυσμένο σημείο του δικτύου. Η απόστασή του από τις κεντρικές κεραίες είναι περίπου 2 km. Επίσης η οπτική επαφή του με τον κεντρικό κόμβο παρουσιάζει προβλήματα, με ορισμένα δέντρα να δημιουργούν προβλήματα. Αυτά τα αποτελέσματα είναι προφανή από τις γραφικές παραστάσεις και από τη γενική οθόνη του Monitoring System. Ο συγκεκριμένος κόμβος επιλέχθηκε και για μετρήσεις με το Snoop λόγω αυτών των χαρακτηριστικών.

Μετρήσεις με το Ethereal

Για τις μετρήσεις με το Ethereal, μπορεί να ειπωθεί ότι η αποτελεσματικότητα του πρωτοκόλλου Snoop στη βελτιστοποίηση της απόδοσης του απλού TCP πρωτοκόλλου στο συγκεκριμένο ασύρματο δίκτυο είναι σημαντική. Ο βαθμός της αποτελεσματικότητας αυτής, όπως θα γίνει φανερό στη συνέχεια, δεν είναι πάντα σταθερός, αλλά μεταβάλλεται αναλόγως των

καιρικών συνθηκών που επικρατούν κατά μήκος της ασύρματης σύνδεσης και των ειδικών παραμέτρων της σύνδεσης (μέγεθος πακέτων κ.λπ.) που επιλέγονται κάθε φορά. Επηρεάζεται επίσης και από τις συνθήκες λήψης και την απόσταση. Βλέποντας τη σύνοψη των αποτελεσμάτων μετρήσεων στην παράγραφο 8.2.6, καθώς και τα αποτελέσματα της παραγράφου 8.3.4, με τους αντίστοιχους πίνακες και τα διαγράμματα, συνάγονται τα παρακάτω συμπεράσματα:

Μετρήσεις με καλές καιρικές συνθήκες

Σε περιπτώσεις όπου οι καιρικές συνθήκες είναι σχετικά καλές και υπάρχει έλλειψη ανασταλτικών παραγόντων όπως ομίχλης, βροχής ή χιονιού, παρατηρείται μία συμφωνία στις μετρήσεις που λαμβάνονται με και χωρίς το πρωτόκολλο Snoop. Δηλαδή σε συνθήκες όπου δε λαμβάνουν χώρα πολλές απώλειες πακέτων από την ασύρματη σύνδεση για οποιοδήποτε λόγο, το Snoop δε δείχνει να βελτιώνει την επίδοση σε σχέση με το απλό TCP πρωτόκολλο.

Έτσι, στην περίπτωση των απλών μετρήσεων και με σχετική δυσκολία λήψης έχουμε μία βελτίωση 2,75% που είναι αμελητέα. Ακόμη πιο χαρακτηριστικά είναι τα παραδείγματα από τις μετρήσεις σύγκρισης με διαφορετικά μήκη πακέτων TCP. Αυτές οι μετρήσεις έγιναν με πολύ καλό καιρό και με πολύ καλή λήψη από το 6ο Δημοτικό Σχολείο. Στις μετρήσεις αυτές το απλό TCP έδειξε καλύτερη απόδοση, ειδικά με το εξ ορισμού μήκος πακέτου δηλαδή τα 1500 bytes. Βλέπουμε λοιπόν μέχρι και μείωση της επίδοσης 3,50% στην περίπτωση αρχείου 72 MB και μήκος πακέτου TCP 1500 bytes.

Ο λόγος για τον οποίο συμβαίνει το γεγονός αυτό οφείλεται κυρίως στη λειτουργία της διαδικασίας που εισάγει το Snoop στον διακομιστή. Ποτέ δεν κερδίζεις κάτι χωρίς να χάσεις. Η επιβάρυνση του υπολογιστή με αλγόριθμους πρόσθετων υπολογισμών και με δέσμευση μνήμης για την επίτευξη των στόχων του Snoop δε βοηθά το σύστημα στην περίπτωση που οι συνθήκες λήψης είναι άριστες και δεν υπάρχει απώλεια πακέτων. Άλλωστε το Snoop σχεδιάστηκε για περιβάλλοντα με πολλές απώλειες.

Αυτή η εικόνα δείχνει να βελτιώνεται υπέρ του πρωτοκόλλου Snoop με τη μείωση του μήκους του πακέτου TCP. Και πάλι όμως με καλές συνθήκες δεν είναι ιδιαίτερα σημαντική. Έτσι, μπορεί με ασφάλεια να εξαχθεί το συμπέρασμα ότι **η χρήση του Snoop δεν είναι ενδεδειγμένη** σε περιβάλλοντα και συνθήκες μικρών απωλειών.

Μετρήσεις με δύσκολες συνθήκες λήψης

Οι περιπτώσεις τώρα που η λήψη είναι δύσκολη και ο καιρός καλός, παρατηρούμε μία μικρή βελτίωση με το πρωτόκολλο Snoop. Αυτή είναι 2,75% και 6,47% για δύο περιπτώσεις αρχείου 6,5 MB. Στην περίπτωση της χαμηλότερης επίδοσης είχαμε ουσιαστικά τέλειο καιρό και γι' αυτό υπάρχει αυτή η διαφοροποίηση.

Σημαντικότατη είναι στην περίπτωση αυτή η επίδραση του πρωτοκόλλου Snoop σε μετρήσεις με μικρότερο μήκος πακέτου TCP. Η αύξηση της επίδοσης φτάνει το 17% κάτι πολύ σημαντικό για την περίπτωση των dial-up συνδέσεων. Στο γεγονός αυτό θα αναφερθούμε διεξοδικά στη συγκριτική αξιολόγηση παρακάτω.

Γενικά το συμπέρασμα στο οποίο καταλήγουμε είναι ότι σε συνθήκες με δυσκολία λήψης **το Snoop αξίζει να χρησιμοποιηθεί** αφού επιφέρει μία υπολογίσιμη βελτίωση στην απόδοση του δικτύου.

Μετρήσεις με άσχημες καιρικές συνθήκες

Σε συνθήκες άσχημων καιρικών συνθηκών και σε διάφορου μεγέθους αρχεία, τα πλεονεκτήματα του πρωτοκόλλου Snoop έναντι του απλού TCP είναι ιδιαιτέρως σημαντικά.

Αξίζει να αναφερθούμε κυρίως στα αποτελέσματα που λήφθηκαν κατά τη μεταφόρτωση του αρχείου των 20 MB. Οι άσχημες συνθήκες εδώ ήταν παρόμοιες και λίγο πιο έντονες με αυτές στην περίπτωση του μεγάλου αρχείου 270 MB που εξετάζουμε παρακάτω, με ιδιαίτερα έντονη βροχόπτωση. Η σημαντικότητα της μέτρησης έγκειται στο ότι, λόγω του σχετικά περιορισμένου μεγέθους του αρχείου, ήταν εφικτό να γίνουν οι μετρήσεις σε πανομοιότυπες καιρικές συνθήκες, χωρίς να υπεισέλθουν φαινόμενα επιδείνωσης του καιρού, όπως στην πιο κάτω περίπτωση. Για τον λόγο αυτό στη μέτρηση αυτή φαίνεται ξεκάθαρα η αύξηση της απόδοσης της σύνδεσης που γίνεται χάρη στο Snoop. Συγκεκριμένα, η ταχύτητα με το Snoop ενεργοποιημένο κινήθηκε στα πλαίσια των 819 Kbytes/sec, ενώ με το Snoop απενεργοποιημένο στα 718 Kbytes/sec, μία αύξηση της τάξης του 14%. Ομοίως, οι αντίστοιχοι χρόνοι πλήρους μεταφόρτωσης του αρχείου ήταν 203 και 232 δευτερόλεπτα, υποδεικνύοντας μία βελτίωση της τάξης του 13,5%, η οποία κρίνεται ιδιαίτερα σημαντική.

Στη μεταφόρτωση του αρχείου μεγέθους 260 MB, παρατηρείται μία βελτίωση της τάξης του 4,60% στην απόδοση του δικτύου. Τα αποτελέσματα δεν είναι τόσο καλά όσο θα ήταν ενδεχομένως αναμενόμενο λόγω της σφοδρής επιδείνωσης του καιρού τα τελευταία λεπτά της μεταφόρτωσης του αρχείου με ενεργοποιημένο το Snoop. Παρ' όλα αυτά, η βελτιστοποιημένη συμπεριφορά της ασύρματης σύνδεσης είναι φανερή καθ' όλη τη διάρκεια της μέτρησης, καθώς η διακύμανση της ταχύτητας στις δύο περιπτώσεις (Εικόνα 8-42 και Εικόνα 8-43) είναι σαφώς μικρότερη με ενεργοποιημένο το Snoop. Εξάλλου, για τέτοιου μεγέθους αρχεία, ακόμα και μία πολύ μικρή βελτίωση της απόδοσης του δικτύου, σημαίνει σημαντική εξοικονόμηση σε χρόνο. Έτσι, ο απαραίτητος χρόνος για τη μεταφόρτωση του αρχείου στην πρώτη περίπτωση είναι 49΄38΄΄, ενώ με το Snoop ενεργοποιημένο 47΄26΄΄, ένα κέρδος 2 περίπου λεπτών. Το κέρδος δε αυτό, αν και φαινομενικά μικρό, μπορεί να ληφθεί σοβαρά υπόψιν αν αναφερόμαστε σε περιβάλλοντα ή εφαρμογές χρονοχρέωσης, όπου η κάθε καθυστέρηση σημαίνει αναπόφευκτα και μεγαλύτερη χρέωση.

Λαμβάνοντας υπόψιν ότι και ο μέσος όρος ταχύτητας της σύνδεσης με το Snoop είναι μεγαλύτερος κατά 4,60% (801 Kbytes/sec έναντι 766 Kbytes/sec), μπορούμε να ισχυριστούμε με συγκεκριμένα στοιχεία ότι υπάρχει μία σαφής βελτίωση της επίδοσης του δικτύου κάτι σημαντικό για την ποιότητα παροχής υπηρεσιών (Quality of Service) του δικτύου. Ως αποτέλεσμα, εφαρμογές που απαιτούν συνεχή και σταθερό ρυθμό διαμεταγωγής δεδομένων (όπως video streaming και live conferencing) οι οποίες θα παρουσίαζαν ασυνέχειες και προβλήματα με το απλό TCP, μπορούν να διεξαχθούν χωρίς πρόβλημα στην περίπτωση του Snoop, ακόμα και σε συνθήκες άσχημων καιρικών συνθηκών.

Ιδιαίτερα έντονη είναι και η βελτίωση που παρατηρήθηκε στη μεταφόρτωση του αρχείου 72 MB, όπου οι συνθήκες ήταν πάλι άσχημες (συννεφιά, έντονη υγρασία και άνεμος) χωρίς όμως βροχή. Η συγκεκριμένη μέτρηση είναι ιδιαιτέρως σημαντική, διότι αφενός πρόκειται για ένα επαρκώς μεγάλου όγκου αρχείο το οποίο μας επιτρέπει να φτάσουμε σε ασφαλή συμπεράσματα και αφετέρου οι καιρικές αυτές συνθήκες παρέμειναν σταθερές καθ' όλη τη διάρκεια και των δύο μετρήσεων. Τέλος, στη μέτρηση αυτή, έγινε σύλληψη όλων των πακέτων (όχι μονάχα των δεδομένων FTP, όπως έγινε παραπάνω) με αποτέλεσμα να φτάσουμε σε πιο ολοκληρωμένα συμπεράσματα. Έτσι, είναι και πάλι προφανής η βελτίωση της ποιότητας παροχής υπηρεσιών που προσφέρει το Snoop, καθώς οι διακυμάνσεις για άλλη μία φορά είναι σαφώς

μικρότερες από το απλό TCP. Ομοίως, ο ρυθμός διαμεταγωγής δεδομένων με χρήση του Snoop είναι βελτιωμένος κατά ένα ποσοστό της τάξης του 5,2% (787 Kbytes/sec έναντι 748 Kbytes/sec), ενώ ο συνολικός χρόνος κυμαίνεται σε καλύτερα πλαίσια κατά 4,8%.

Αυτό που έχει ιδιαίτερη σημασία στη μέτρηση αυτή είναι ο αριθμός των χαμένων πακέτων (dropped packets) που καταγράφηκαν στη μία και στην άλλη περίπτωση. Συγκεκριμένα, όταν δεν έγινε χρήση του Snoop τα χαμένα πακέτα ήταν 264, ενώ στην περίπτωση που έγινε χρήση του Snoop ήταν μόλις 11, μία πτώση της τάξης του 95,8%. Η διαφοροποίηση αυτή ακριβώς αποδεικνύει το αποτέλεσμα της λειτουργίας του Snoop, το οποίο απέκρυψε τα χαμένα πακέτα από τον πομπό, αποτρέποντάς τον από το να ενεργοποιήσει μεθόδους αποσυμφόρησης του δικτύου, και τα επανεξέπεμψε στον δέκτη. Δημιουργείται όμως τότε το ερώτημα: για ποιο λόγο στα 11 αυτά πακέτα που καταγράφηκαν σαν χαμένα δεν επενέβη το Snoop για να αποτρέψει την καταγραφή τους ως χαμένα; Η απάντηση βρίσκεται στο ότι το Snoop, όπως έχει προαναφερθεί, δεν είναι πλήρως προστατευμένο από απώλειες πακέτων. Συγκεκριμένα, για καθυστερήσεις που υπερβαίνουν κάποιο χρονικό διάστημα, ο πομπός δε λαμβάνει από το πρωτόκολλο την επιβεβαίωση παραλαβής (acknowledgement) του πακέτου με αποτέλεσμα να ενεργοποιεί μόνος του μηχανισμούς αποσυμφόρησης, οπότε συμβαίνει καταγραφή του πακέτου ως χαμένου. Οι καθυστερήσεις αυτές συνήθως λαμβάνουν χώρα όταν υπάρχουν συσσωρευμένες απώλειες πακέτων και η επανεκπομπή τους δε γίνεται με επαρκώς γρήγορο ρυθμό από το Snoop.

Το συμπέρασμα στο οποίο καταλήγουμε είναι ότι σε άσχημες καιρικές συνθήκες ακόμα και σε συνδέσεις, όπου η λήψη από άποψη θέσης και απόστασης είναι πολύ καλή, **η χρήση του Snoop είναι επιβεβλημένη** αφού επιφέρει μία πολύ σημαντική βελτίωση στην απόδοση του δικτύου και διασφαλίζει την ποιότητα των υπηρεσιών του δικτύου.

Μετρήσεις για μεταβλητό μήκος πακέτου TCP

Οι μετρήσεις αυτές έγιναν κύρια σε περιβάλλον καλών καιρικών συνθηκών και σε διάφορου μεγέθους αρχεία, με τη βελτίωση με τη χρήση του πρωτοκόλλου Snoop έναντι του απλού TCP είναι ιδιαιτέρως σημαντικά στα μικρά μεγέθη πακέτου TCP.

Έτσι στην κάθε περίπτωση η μείωση του μήκους του TCP πακέτου δίνει μεγαλύτερο ποσοστό βελτίωσης για την περίπτωση της χρήσης του Snoop. Στην περίπτωση των καλών καιρικών συνθηκών καθώς και συνθηκών λήψης, ενώ η επίδοση με το Snoop αρχικά υπολείπεται του απλού TCP, με τη μείωση του μήκους πακέτου το Snoop υπερτερεί έστω και ελαφρώς. Εκεί που η διαφορά είναι μεγάλη είναι στην περίπτωση των δύσκολων συνθηκών λήψης. Η μεταβολή του μήκους του πακέτου και συγκεκριμένα η μείωση αυτού, επιφέρει μία βελτίωση από 6,5% σε 17%.

Αυτή η βελτίωση είναι όμως ποσοστιαία και όχι απόλυτη. Αυτό διότι το βέλτιστο μήκος πακέτου για την περίπτωση του συγκεκριμένου δικτύου είναι 1500 bytes. Μειώνοντας το μήκος του πακέτου, απαιτείται μεγαλύτερος αριθμός πακέτων για τη μετάδοση των αρχείων. Άρα απαιτούνται και περισσότερα πακέτα TCP για το acknowledgment με αποτέλεσμα το ποσοστό των καθαρών δεδομένων της επικοινωνίας να είναι πιο μικρό. Αυτό γίνεται φανερό από τις γραφικές παραστάσεις όπου βλέπουμε και τα FTP-DATA πακέτα και τα TCP.

Το σημείο στο οποίο πρέπει να δοθεί προσοχή είναι η χρήση του μικρού μεγέθους μήκους πακέτου σε ορισμένες περιπτώσεις. Αυτό που προτείνεται [8] είναι σε συνδέσεις dial-up να χρησιμοποιείται αυτό το μικρό μέγεθος πακέτου. Άρα στις περιπτώσεις **όπου το ενδεδειγμένο**

μήκος του πακέτου είναι μικρό, τότε η χρήση του Snoop είναι επιβεβλημένη αφού επιφέρει μία πολύ σημαντική βελτίωση στην απόδοση του δικτύου.

Γενικά Συμπεράσματα

Οι βελτιστοποιήσεις αυτές στην απόδοση του δικτύου κρίνονται ιδιαίτερα σημαντικές, αν ληφθούν υπόψιν οι προδιαγραφές και του Πανελληνίου Σχολικού Δικτύου και ο ρόλος που καλείται να διαδραματίσει στη βελτίωση της ποιότητας της εκπαίδευσης στη χώρα μας. Υπηρεσίες όπως τηλεδιάσκεψη, βίντεο κατ' απαίτηση, σύγχρονη τηλεκπαίδευση και ζωντανές μεταδόσεις εκδηλώσεων θα ευεργετηθούν σημαντικά από μία βελτιστοποίηση της ποιότητας παροχής υπηρεσιών (Quality of Service) εντός του δικτύου. Λαμβάνοντας υπόψιν ότι κάθε δίκτυο κρίνεται από τον ασθενέστερο κρίκο του, μπορεί να εξαχθεί το συμπέρασμα ότι ιδιαίτερη προσοχή και βάρος θα πρέπει να δοθεί στο ασύρματο μέρος του δικτύου, καθώς αυτό κατά γενική ομολογία είναι το πιο επιρρεπές σε αυξομειώσεις απόδοσης λόγω φαινομένων τα οποία δε βρίσκονται εντός του ελέγχου των διαχειριστών, όπως καιρικές συνθήκες.

Η απαιτήσεις για συνεχή και αδιάλειπτη παροχή υπηρεσιών θα αυξάνονται συνεχώς όσο το σχολικό δίκτυο θα ολοκληρώνεται και θα αναπτύσσεται και νέες υπηρεσίες θα μπαίνουν σε εφαρμογή. Σε ένα τέτοιο ραγδαία αναπτυσσόμενο περιβάλλον, τα υπάρχον δίκτυο πρέπει συνεχώς να αναβαθμίζεται με νέο υλικό (hardware) ή να βρίσκονται τρόποι για την πλήρη αξιοποίηση της ήδη υπάρχουσας υποδομής, ώστε αυτή να παρέχει το μέγιστο των δυνατοτήτων της ανά πάσα στιγμή. Η χρήση του πρωτοκόλλου Snoop υπακούει σε αυτή ακριβώς την ανάγκη, με τρόπο που αφενός να είναι εύκολος στην εφαρμογή και αφετέρου δεν έρχεται σε αντιδιαστολή με την απαίτηση για εύκολη εγκατάσταση και χρήση διαδεδομένων πρωτοκόλλων, καθώς βασίζεται στην τροποποίηση μονάχα του κώδικα του πομπού, όπου οι διαχειριστές αναμένονται να έχουν συνεχή και πλήρη πρόσβαση.

Η ενεργοποίηση και η απενεργοποίηση του πρωτοκόλλου Snoop είναι ένα άλλο σημαντικό κεφάλαιο. Σε ένα περιβάλλον με δυσκολία λήψης, με συνεχείς άσχημες καιρικές συνθήκες καθώς και σε ένα τοπικό ασύρματο δίκτυο με φορητές συσκευές, το πρωτόκολλο μπορεί να είναι συνεχώς ενεργοποιημένο. Όταν όμως έχουμε μία σταθερή και καλή σύνδεση τότε τα πράγματα περιπλέκονται. Οι ιδέες για την αυτόματη ενεργοποίηση και απενεργοποίηση του είναι πολλές. Μπορεί με μερικά στατιστικά στοιχεία σύνδεσης των προηγούμενων χρονικών διαστημάτων και της προηγούμενης κατάστασης να παρακολουθεί την μεταβολή της επίδοσης του δικτύου και να αλλάζει κατάσταση. Άλλη ιδέα είναι η χρήση εξωτερικών συσκευών ανίχνευσης καιρικών δεδομένων και η επεξεργασία των δεδομένων τους από ένα πρόγραμμα σε υπολογιστή. Η έξοδος του προγράμματος θα είναι η ενεργοποίηση ή η απενεργοποίηση του πρωτοκόλλου. Όλα αυτά όμως προϋποθέτουν πολλές πειραματικές μετρήσεις και θα έχουν ισχύ μόνο για το συγκεκριμένο σημείο στο οποίο γίνονται οι μετρήσεις.

Οι ασύρματες συνδέσεις των δικτύων είναι όλο και καλύτερες και οι επιδόσεις τους βελτιώνονται συνεχώς. Αυτό που μπορούμε σίγουρα να πούμε είναι ότι υπάρχουν πολλά περιθώρια βελτίωσης. Η εργασία αυτή κινήθηκε προς αυτήν την κατεύθυνση και πιστεύουμε ότι έχει συμβάλει στην εξαγωγή ασφαλών και χρήσιμων συμπερασμάτων.

10. Επίλογος

Η ασύρματη δικτύωση αποτελεί σήμερα τον καλύτερο εναλλακτικό τρόπο δικτύωσης. Ειδικά σε περιοχές όπου η μορφολογία του εδάφους και η απόσταση είναι απαγορευτικές για τη χρήση οπτικών ινών, η ασύρματη δικτύωση είναι η ενδεδειγμένη λύση. Η τεχνολογία και τα προϊόντα ασύρματης δικτύωσης έχουν ωριμάσει και είναι σε θέση να χρησιμοποιηθούν για την υλοποίηση υπηρεσιών, τόσο για τον δημόσιο τομέα, όσο και τον ιδιωτικό.

Οι δημόσιες υπηρεσίες, οι επιχειρήσεις και οι επαγγελματίες μπορούν να επωφεληθούν από τις δυνατότητες που τους παρέχουν οι τεχνολογίες ασύρματης δικτύωσης και να αναπτύξουν νέες υπηρεσίες, να επεκτείνουν τα δίκτυά τους και να μειώσουν το ύψος των τηλεπικοινωνιακών τους τελών.

Με τη χρήση των Ασύρματων Δικτύων η επικοινωνία γίνεται πιο άμεση, το δίκτυο παρέχει κάλυψη χωρίς περιορισμούς και η επέκτασή του γίνεται πολύ πιο εύκολα και με μικρό σχετικά κόστος.

Επιπλέον, τα Ασύρματα Δίκτυα προσφέρουν διασύνδεση των καταστημάτων των επιχειρήσεων και των οργανισμών (π.χ. απομακρυσμένη διασύνδεση δημοτικών διαμερισμάτων σε δήμους) και δίνουν τη δυνατότητα της ανάπτυξης μιας μεγάλης γκάμας υπηρεσιών προς τους πελάτες και τους πολίτες.

Τη συγκεκριμένη χρονική στιγμή υπάρχει ένας οργασμός από πολλά και σημαντικά Ευρωπαϊκά Προγράμματα που βρίσκονται σε εξέλιξη και αφορούν τις ευρυζωνικές συνδέσεις σε όλους τους τομείς. Έτσι, η ειδική γραμματεία του Υπουργείου Οικονομικών για την Κοινωνία της Πληροφορίας, καθώς και η ΚτΠ Α.Ε., στην προσπάθειά τους για την εισαγωγή των διαφόρων τεχνολογιών της Κοινωνίας της Πληροφορίας στην καθημερινή ζωή και την εργασία του πολίτη, υποστηρίζουν οικονομικά μία σειρά από πρωτοβουλίες για τη διάδοση της χρήσης των ενσύρματων και ασυρμάτων τεχνολογιών δικτύωσης.

Σε κάθε χρονική στιγμή, είναι ανοιχτές διάφορες προσκλήσεις που αφορούν την ευρυζωνική σύνδεση και χρηματοδοτούνται από την Ευρωπαϊκή Ένωση. Έτσι πέρα από τη συγκεκριμένη υλοποίηση του δικτύου πάνω στο οποίο εκπονήθηκε η εργασία μας και χρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση, υπάρχουν πολλά έργα σε Μέτρα και Προσκλήσεις που χρηματοδοτούνται. Ενδεικτικά αναφέρουμε τα παρακάτω:

- Υπηρεσίες Ευρείας Ζώνης σε Φορείς Δημόσιας Διοίκησης (Wireless Administration)
- Ανάπτυξη Μητροπολιτικών Ευρυζωνικών Δικτύων Μέτρο 4.2 - (Πρόσκληση 93)

Όλες οι παραπάνω προσκλήσεις έχουν σχέση με το έργο «ΣΥΖΕΥΞΙΣ» όπου προβλέπεται η συνολική ευρυζωνική διασύνδεση των κυβερνητικών οργανισμών τόσο με ενσύρματη όσο και με ασύρματη δικτύωση.

Το Κιλκίς, μέσω του Δήμου, έχει ήδη υποβάλει πρόταση στην Πρόσκληση-93 και η ένταξη και χρηματοδότηση του έργου είναι απλώς θέμα χρόνου. Είναι επίσης πρωτοπόρο σε θέματα ασύρματης διασύνδεσης των σχολικών μονάδων με βάση το έργο πάνω στο οποίο εκπονήθηκε η εργασία αυτή.

Επίσης, το έργο της διασύνδεσης μέσω του «ΣΥΖΕΥΞΙΣ» βρίσκεται στο στάδιο της μελέτης από την ανάδοχο εταιρεία και συγκεκριμένα τον ΟΤΕ. Μέσα από μία σειρά

προγραμμάτων (π.χ. «ΘΗΣΕΑΣ») αναβαθμίζονται τα εσωτερικά δίκτυα των υπηρεσιών της πόλης. Τέλος υπάρχουν και άλλες προσκλήσεις που αφορούν τη διασύνδεση οικισμών με ασύρματες ευρυζωνικές ζεύξεις. Οι μελέτες για την υποβολή προτάσεων για τη χρηματοδότηση των έργων αυτών βρίσκονται σε εξέλιξη.

Γίνεται λοιπόν φανερό ότι στόχος μας δεν ήταν απλώς και μόνο η εκπόνηση μιας εργασίας για τη διεκπεραίωση των σπουδών μας. Η ενασχόλησή μας με τα θέματα των δικτύων, τόσο των ενσύρματων όσο και των ασύρματων, αποτελεί ένα καθημερινό και αναπόσπαστο κομμάτι της εργασίας μας. Οι ανάγκες για εμβάθυνση σε θέματα ασυρμάτων δικτύων, με την παράλληλη ανάλυση και αξιολόγηση αυτών, είναι προφανείς. Η επιστημονική ανησυχία που μας διακρίνει έχει ως αποτέλεσμα τη συνεχή παρακολούθηση των τεχνολογικών εξελίξεων. Η συνεχής μάθηση και επιμόρφωση αποτελεί για μας πρόκληση.

Κλείνουμε εκφράζοντας την ελπίδα ότι με την εργασία αυτή έχουμε συμβάλει κι εμείς στην ανάπτυξη και βελτίωση των ευρυζωνικών ασύρματων συνδέσεων στο μέτρο που αυτό ήταν δυνατό.

Αρκτικόλεξα

ADSL	Asymmetric DSL
ANSI	American National Standards Institute
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
AU	Access Unit
BPSK	Binary Phase Shift Keying
BWA	Broadband Wireless Access
CBE	Cell Broadcast Entity
CDMA	Code Division Multiple Access. Λέγεται και Spread Spectrum
CIR	Committed Information Rate
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
CPAN	Comprehensive Perl Archive Network
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DBMS	DataBase Management System
DCS	Dynamic Channel Selection
DFIR	Diffused Infra-Red
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EDUnet	EDUcational network
EIA/TIA	Electronics Industry Association/Telecommunications Industry Association
EIRP	Effective Isotropic Radiated Power
ETSI	European Telecommunications Standards Institute
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
GNU	GNU's not UNIX
GUI	Graphical User Interface
GUnet	Greek University network
HiperLAN	HIgh PERformance LAN
IAB	Internet Activities Board
IAPP	Inter-Access Point Protocol
IEEE	Institute of Electrical and Electronic Engineers
IIS	Internet Information Server
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISM	Industrial Scientific and Medical
ISO	International Standards Organization
IEC	International Electrotechnical Commission
LAN	Local Area Network
MAC	Medium Access Control
MDAC	Microsoft Data Access Components
MIB	Management Information Base
MIR	Minimum Information Rate

NE	Network Elements
NMP	Network Management Protocol
NT	New Technology
NTFS	New Technology File System
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
POP3	Post Office Protocol v.3
PPM	Perl Package Manager
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RRD	Round Robin Database
RSSI	Received Signal Strength Indicator
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SU	Subscriber Unit
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TDD	Time Division Duplex
TPC	Transmit Power Control
UDP	User Datagram Protocol
UNII	Unlicensed National Information Infrastructure
URL	Uniform Resource Locator
VDSL	Very high speed DSL
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
ΕΔΕΤ	Εθνικό Δίκτυο Έρευνας-Τεχνολογίας
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕΛ	Ενιαίο Λύκειο
ΟΤΕ	Οργανισμός Τηλεπικοινωνιών Ελλάδος
ΠΣΔ	Πανελλήνιο Σχολικό Δίκτυο
ΤΕΕ	Τεχνικό Επαγγελματικό Εκπαιδευτήριο
ΤΕΙ	Τεχνολογικό Εκπαιδευτικό Ίδρυμα
ΤΠΕ	Τεχνολογίες Πληροφοριών και Επικοινωνιών
ΥΠΕΠΘ	Υπουργείο Εθνικής Παιδείας και Θρησκευμάτων
ΦΕΚ	Φύλλο Εφημερίδας της Κυβερνήσεως

Αναφορές

1. Amir, E., H. Balakrishnan, S. Seshan & R. H. Katz, *Efficient TCP over Networks with Wireless Links*, University of California at Berkeley, 1995, https://www.researchgate.net/profile/Srinivasan-Seshan-2/publication/2607582_Efficient_TCP_over_Networks_with_Wireless_Links/links/09e41513970a614f62000000/Efficient-TCP-over-Networks-with-Wireless-Links.pdf
2. Balakrishnan, H., S. Seshan, E. Amir & R. H. Katz, *Improving TCP/IP Performance over Wireless Networks*, University of California at Berkeley, 1995, https://dl.acm.org/doi/pdf/10.1145/215530.215544
3. Balakrishnan, H., V. N. Padmanabhan, S. Seshan & P. H. Katz, *A Comparison of Mechanisms for Improving TCP Performance over Wireless Link*, IEEE/ACM Transactions on Networking, Vol. 5, No. 6, 1997, http://daedalus.cs.berkeley.edu/publications/sigcomm96.pdf
4. Cooper, G. R. & C. D. McGillem, *Modern Communications and Spread Spectrum*, McGraw-Hill, 1986, pp. 293-294
5. Horn, M., *Designing Capture Filters for Ethereal*, http://dant.net.ru/wiki/info/networking/ether-cap-filters
6. Parsa, C. & J. J. Garcia-Luna-Aceves, *TULIP: A Link-Level Protocol for Improving TCP over Wireless Links*, University of California, 2000, https://apps.dtic.mil/sti/pdfs/ADA461750.pdf
7. Saravanan, M. K., *MKS Linux Kernel How To*, http://puggy.symonds.net/~mksarav/tutorials/mks-linux-kernel-howto.txt
8. WinGuides Network for Windows, *How to Change the Maximum Transmission Unit (MTU) Size*, http://files.dlink.com.au/Products/!Routers/MTU_Win2K.XP.pdf
9. Wireless Connections, *Monitoring System – Installation and User Guide*, v. 2.35, 2004, http://www.wirelessconnections.net/main/support.asp?wid=99
10. Xylomenos, G., G. C. Polyzos, P. Mähönen & M. Saaranen, *TCP Performance Issues over Wireless Links*, 2001, IEEE Communications Magazine, Vol. 39, N. 4, 2001, pp. 52-58, https://www.researchgate.net/profile/Mika-Saaranen/publication/3196436_TCP_Performance_Issues_over_Wireless_Links/links/0c9605343f0dac3ebd000000/TCP-Performance-Issues-over-Wireless-Links.pdf
11. Πανελλήνιο Σχολικό Δίκτυο, *Ενημερωτικό υλικό για το ΠΣΔ – Ευρυζωνικές δράσεις*, https://www.sch.gr/files/PSD_Evrozonikes_draseis_GR.pdf
12. Πανελλήνιο Σχολικό Δίκτυο, *Αναλυτικό ενημερωτικό σημείωμα για το Πανελλήνιο Σχολικό Δίκτυο*, https://www.sch.gr/files/ENHMERWTIKO_SHMEIWMA_PSD.pdf
13. Στραβάκος, Η., *Μελέτη εφαρμογής ασύρματου δικτύου δεδομένων*, Διπλωματική εργασία ΜΔΕ, Πανεπιστήμιο Μακεδονίας, ΠΜΣ Πληροφοριακά Συστήματα Διοίκησης, 2003
14. ΤΕΙ Θεσσαλονίκης, *Διακήρυξη υπ' αριθμ. 13/2003 ανοικτού διαγωνισμού για την «Προμήθεια και εγκατάσταση δικτυακού εξοπλισμού και υποδομών για την ασύρματη σύνδεση εκπαιδευτικών μονάδων στο πολεοδομικό συγκρότημα του Κιλκίς»*, 2003
15. Τσιλιγκιρίδης, Θ. κ.ά., *Μετάδοση Δεδομένων & Δίκτυα Υπολογιστών I & II*, Τόμος ΙΙ, ΥΠΕΠΘ – Παιδαγωγικό Ινστιτούτο, Αθήνα, 2000, http://www.pi-schools.gr/lessons/tee/computer/