ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Διαχείριση Δικτύων

Ονόματα ομάδας:

Αγγελική Δηλάκη	1115 2012 00031
Κωνσταντίνα Χατζηελευθερίου	1115 2012 00198

Επιβλέπουσα:

Λέκτορας Α. Αλωνιστιώτη

Μάιος 2016

Περιεχόμενα

1 Συλλογή Δεδομένων

Για τη συλλογή δεδομένων χρησιμοποιήσαμε τα εξής προγράμματα που προτείνονται και στο μάθημα:

- IP Scanner
- WiFi Inspector Xirrus
- Net View
- WireShark

Το IP Scanner ανιχνεύει όλες τις διαθέσιμες IP που βρίσκονται στο ίδιο δίκτυο, ώστε να ξέρει ο χρήστης ποιες IP είναι δεσμευμένες και ποιες πόρτες έχουν ανοικτές οι συγκριμένες IP διευθύνσεις. Εμείς χρησιμοποιήσαμε τα δεδομένα του προγράμματος αυτού, ώστε να μετρήσουμε πληροφορίες που σχετίζονται με την πληρότητα του δικτύου.

Το Wifi Inspector Xirrus ανιχνεύει πληροφορίες τόσο για το συνδεδεμένο δίκτυο, όσο και για τα γειτονικά δίκτυα που ανιχνεύονται. Έχει επίσης τη δυνατότητα να ανιχνεύει την κατεύθυνση που βρίσκεται το access point, ώστε να το δείχνει σχηματικά πάνω σε έναν χάρτη. Στην καταγραφή των δεδομένων καταγράφει πληροφορίες όπως το SSID, η MAC address, τον τρόπο κρυπτογράφησης (αν υπάρχει), κτλ.

Παρόμοιες πληροφορίες καταγράφει και το πρόγραμμα net view, το οποίο καταγράφει τα detected networks που βρίσκει. Πέρα από τις παραπάνω πληροφορίες, καταγράφει επίσης και το ποσοστό ανίχνευσης του κάθε δικτύου, έτσι ώστε να βλέπουμε πόσο συχνά γίνεται εμφανές κάθε δίκτυο. Δηλαδή αν το ποσοστό εμφάνισης είναι 98-100%, τότε το δίκτυο αυτό ανιχνεύεται σχεδόν συνέχεια από το χρήστη.

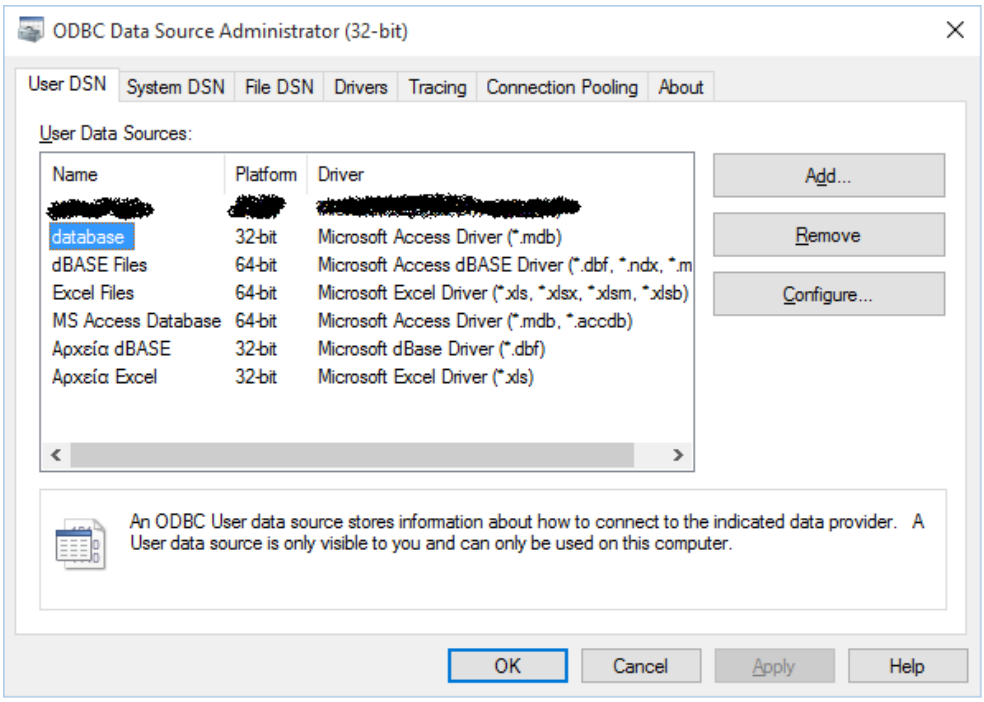
Τέλος, το WireShark κάνει ανίχνευση πακέτων στο δίκτυο, ώστε να μπορεί ο χρήστης που καταγράφει τα δεδομένα να διαπιστώσει ειδικές πληροφορίες για τα πακέτα, όπως σε ποιο πρωτόκολλο ανήκουν, διεύθυνση πηγής, διεύθυνση προορισμού κτλ. Τις πληροφορίες του προγράμματος αυτού δεν τις χρησιμοποιήσαμε για τη λήψη απόφασης βελτιστοποίησης δικτύου με το πρόγραμμα, καθώς τα προηγούμενα προγράμματα κάλυψαν τις ανάγκες που θέλαμε επαρκώς.

Οι μετρήσεις στα παραπάνω προγράμματα έγιναν σε διάφορες ώρες της ημέρας, ώστε να είναι όσο γίνεται πιο αμερόληπτες και αντικειμενικές ως προς το φόρτο του δικτύου. Αποθηκεύσαμε τις μετρήσεις σε αρχεία csv, και στη συνέχεια τις ενώσαμε σε ένα αρχείο ανά πρόγραμμα. Οπότε πρακτικά έχουμε συλλέξει 4 μεγάλα αρχεία, τα οποία τα εισάγαμε σε μια βάση δεδομένων της Microsoft Access. Κάθε αρχείο αποτελεί και ξεχωριστό πίνακα στη βάση δεδομένων.

2 Διασύνδεση των Δεδομένων με το πρόγραμμα

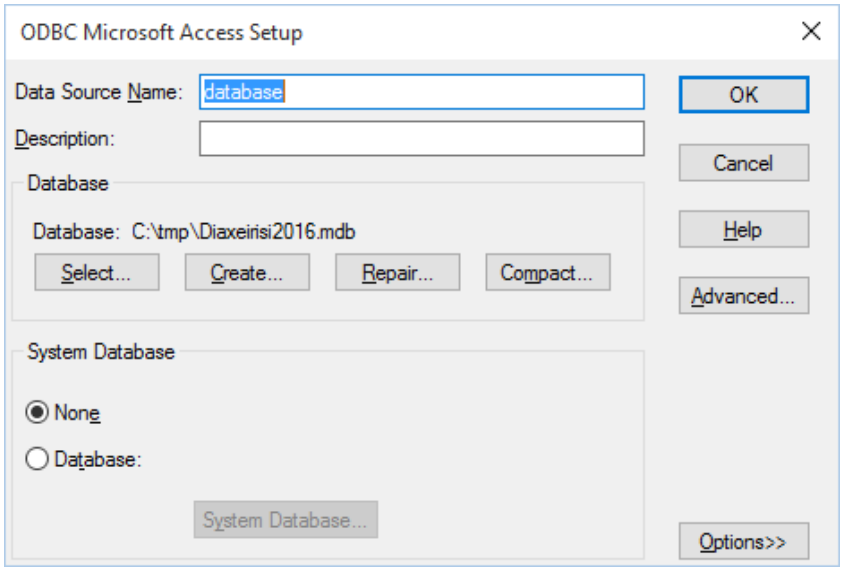
Για τη διασύνδεση της βάσης δεδομένων με το πρόγραμμα λήψης απόφασης χρησιμοποιήσαμε τον ODBC driver της Microsoft Access. Το πρόγραμμα για τη λήψη απόφασης έχει γραφτεί σε γλώσσα C++, σε Microsoft Visual Studio 2015.

Για το λόγο αυτό, φτιάξαμε ένα User Data Source με όνομα database, όπως φαίνεται παρακάτω:



Εικόνα 1: Ρυθμίσεις του ODBC driver

Το συγκεκριμένο User Data Source παραπέμπει στη βάση δεδομένων, το οποίο φαίνεται και στο Configure:

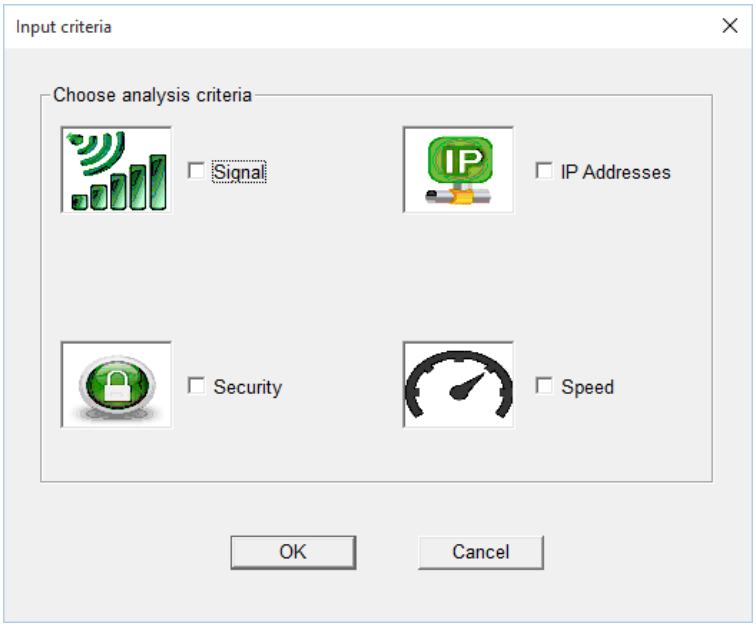


Εικόνα 2: Επιπλέον ρυθμίσεις του ODBC driver

Το πρόγραμμα λήψης απόφασης λαμβάνει δηλαδή ουσιαστικά την είσοδο του χρήστη που επιλέγει τα κριτήρια που θέλει να αναλυθούν. Στη συνέχεια, για τα κριτήρια αυτά, συνδέεται με τα δεδομένα για να κάνει τις αντίστοιχες επερωτήσεις στη βάση δεδομένων και τελικά τα αποτελέσματα των επερωτήσεων εμφανίζονται στο χρήστη. Τα αποτελέσματα αυτά, γράφονται πρακτικά σε ένα αρχείο html, το οποίο και εμφανίζεται με την ολοκλήρωση του προγράμματος.

3 Σχολιασμός προγράμματος

Κατά την εκκίνηση της εκτέλεσης του προγράμματος, εμφανίζεται στο χρήστη ένα παράθυρο με 4 επιλογές, ανάλογα με τα κριτήρια που θέλει να αναλυθούν.



Εικόνα 3: Είσοδος του χρήστη για τα κριτήρια ανάλυσης

Το πρώτο κριτήριο αφορά τη σηματοδοσία του δικτύου, δηλαδή αν είναι ικανοποιητική η στάθμη λήψης του σήματος. Θεωρούμε προφανώς ότι πρόκειται για ασύρματο δίκτυο, ώστε οι μετρικές που θα αναλυθούν να έχουν νόημα.

Το δεύτερο κριτήριο αφορούν τη διευθυνσιοδότηση IP και τη σωστή οργάνωση του δικτύου. Θεωρώντας ότι ο χρήστης έχει εισάγει μάσκα υποδικτύου το 255.255.255.0 (κλασική μάσκα υποδικτύου σε ένα εσωτερικό δίκτυο), μελετάται αν το δίκτυο μπορεί να εξυπηρετήσει επιπλέον χρήστης ή όχι.

Το τρίτο κριτήριο αφορά την ασφάλεια της ασύρματης διεπαφής και τον τρόπο κρυπτογράφησης των δεδομένων. Ελέγχεται δηλαδή αν υπάρχει κρυπτογράφηση στα δεδομένα που αποστέλλονται στο ασύρματο κανάλι.

Το τέταρτο κριτήριο αφορά στην ταχύτητα του ασύρματου καναλιού, για να διαπιστωθεί αν αυτή είναι ικανοποιητική ή όχι.

3.1 Πίνακες βάσης δεδομένων

Η βάση δεδομένων αποτελείται όπως είπαμε από 4 πίνακες, η δομή των οποίων φαίνεται στις ακόλουθες εικόνες.

IPScanner

Field Name	Data Type
ID	AutoNumber
Status	Short Text
IP	Short Text
MAC_address	Short Text

Εικόνα 4: Πίνακας δεδομένων προγράμματος IP Scanner

Shark

Field Name	Data Type
ID	AutoNumber
Time	Number
Source	Short Text
Destination	Short Text
Protocol	Short Text
Length	Number
Info	Long Text

Εικόνα 5: Πίνακας δεδομένων προγράμματος WireShark

Wireless

Field Name	Data Type
ID	AutoNumber
SSID	Short Text
Average_Signal	Number
Detection_Counter	Number
Pct Detection	Number
Authentication	Short Text
Cipher	Short Text
PHY_Types	Short Text
MAC_Address	Short Text
RSSI	Number
Frequency	Number
Channel	Number
Max_Speed	Short Text

Εικόνα 6: Πίνακας δεδομένων του Net View

Xirrus

Field Name	Data Type
ID	AutoNumber
Connected	Short Text
SSID	Short Text
Signal	Number
Network Mode	Short Text
Encryption	Short Text
Auth	Short Text
Vendor	Short Text
BSSID	Short Text
Channel	Short Text
Frequency	Number
Network Type	Short Text
Adapter Description	Short Text

Εικόνα 7: Πίνακας δεδομένων του Wifi Inspector Xirrus

3.2 Επερωτήσεις σηματοδοσίας

Για τη σηματοδοσία έχουμε θεωρήσει ότι η ικανοποιητική ισχύς λήψης είναι $\geq -45\ dBm$. Σε περίπτωση που η μέση ισχύς λήψης είναι χειρότερη από το όριο αυτό κρίνουμε ότι χρειάζεται βελτιστοποίηση, όπως αλλαγή της θέσης του access point, αλλαγή της θέσης του laptop, αφαίρεση εμποδίων που μειώνουν τη λήψη του σήματος, κτλ.

Η επερώτηση που εκτελείται για τον συγκεκριμένο έλεγχο είναι η εξής:

SELECT SSID, BSSID, AVG(Signal) AS Average

FROM XIRRUS

WHERE Connected="True"

GROUP BY SSID, BSSID

Επίσης, θέλουμε να δούμε αν στα δίκτυα που έχουν εντοπιστεί, υπάρχει κάποιο σε κοντινή συχνότητα που ανιχνεύεται σε πάνω από το 80% των δειγμάτων και λειτουργεί στην ίδια συχνότητα με αυτή του δικού μας δικτύου. Αν δεν υπάρχει κάποια κεραία στην ίδια συχνότητα, τότε κρίνουμε ότι δεν υπάρχει κάποιο πρόβλημα παρεμβολής, αλλιώς συνιστούμε αλλαγή της συχνότητας λειτουργίας.

Η επερώτηση που εκτελείται για τον συγκεκριμένο έλεγχο είναι η εξής:

```
SELECT SSID, MAC_ADDRESS, MAX(AVERAGE_SIGNAL) AS ['Average Signal
%'], SUM(DETECTION_COUNTER) AS ['Detected Count'], FREQUENCY
FROM WIRELESS
WHERE AVERAGE_SIGNAL >= 0.8 AND DETECTION_COUNTER > 10
GROUP BY SSID, MAC_ADDRESS, FREQUENCY
ORDER BY MAX(AVERAGE_SIGNAL) DESC;
```

3.3 Επερώτηση διευθυνσιοδότησης IP

Για τη διευθυνσιοδότηση, εξετάζουμε το πλήθος των διαφορετικών IP διευθύνσεων που βρέθηκαν σε όλα τα δείγματα των μετρήσεων που κάναμε. Αν αυτές είναι λιγότερες από 200, τότε δεν υπάρχει κάποιο θέμα αλλαγής των ρυθμίσεων του δικτύου, αλλιώς προτείνουμε επανέλεγχο της μάσκας υποδικτύου.

Η επερώτηση που εκτελείται για τον συγκεκριμένο έλεγχο είναι η εξής:

```
SELECT IP, MAC_ADDRESS
FROM IPSCANNER
WHERE STATUS <> "Unknown"
GROUP BY IP, MAC_ADDRESS
ORDER BY IP;
```

3.4 Επερώτηση ασφάλειας δικτύου

Για τον έλεγχο της ασφάλειας του δικτύου, εξετάζουμε όπως είπαμε τους τρόπους κρυπτογράφησης των δεδομένων, όταν αυτά αποστέλλονται στο ασύρματο κανάλι. Αν ο τρόπος αυτός είναι None, τότε συνεπάγεται ότι τα δεδομένα είναι ακρυπτογράφητα, άρα και ανασφαλή. Για το λόγο αυτό, συνιστούμε αλλαγή στις ρυθμίσεις ασφάλειας του δικτύου, εισάγοντας π.χ. κωδικοποίηση WPA2.

Η επερώτηση που εκτελείται για τον συγκεκριμένο έλεγχο είναι η εξής:

```
SELECT SSID, BSSID, ENCRYPTION, AUTH
FROM XIRRUS
WHERE Connected="True"
GROUP BY SSID, BSSID, ENCRYPTION, AUTH;
```

3.5 Επερώτηση ταχύτητας δικτύου

Για την ταχύτητα του δικτύου εξετάζουμε το πρωτόκολλο με το οποίο λειτουργεί το συγκεκριμένο ασύρματο κανάλι. Υπάρχουν 4 κατηγορίες πρωτοκόλλων:

- 802.11b
- 802.11g
- 802.11n
- 802.11a

Η πρώτη κατηγορία έχει μέγιστη ταχύτητα τα 11 Mbps, το οποίο είναι αρκετά λίγο για τα σημερινά σύγχρονα δεδομένα ενός δικτύου. Στην περίπτωση αυτή, συνιστούμε επανέλεγχο της ταχύτητα του δικτύου. Στις άλλες περιπτώσεις, η ταχύτητα είναι ικανοποιητική και δε συνιστούμε αλλαγή στις ρυθμίσεις που αφορούν αυτές τις πληροφορίες.

Η επερώτηση που εκτελείται για τον συγκεκριμένο έλεγχο είναι η εξής:

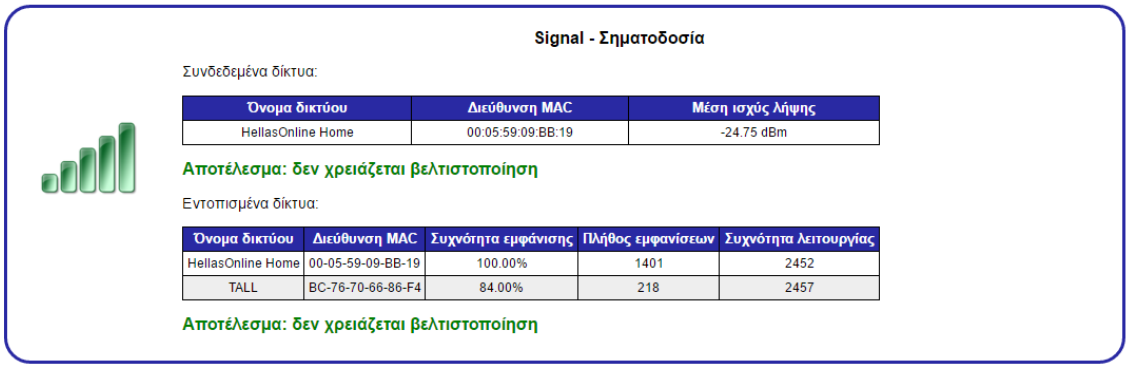
```
SELECT PHY_TYPES, MAX_SPEED
FROM WIRELESS
WHERE SSID=(SELECT DISTINCT SSID FROM XIRRUS WHERE
Connected='True')
GROUP BY PHY_TYPES, MAX_SPEED;
```

4 Αποτελέσματα προγράμματος

Όπως αναφέρθηκε, τα αποτελέσματα του προγράμματος είναι ένα αρχείο html που εμφανίζεται αυτόματα με την ολοκλήρωση της εκτέλεσης του προγράμματος. Το αρχείο αυτό αποτελείται από τόσα τμήματα, όσα αντίστοιχα κριτήρια ανάλυσης επέλεξε ο χρήστης στην αρχή (το πολύ 4).

Στη συνέχεια εμφανίζονται οι διάφορες επιλογές που είναι πιθανόν να εμφανιστούν στο χρήστη:

4.1 Αποτελέσματα σηματοδοσίας



Signal - Σηματοδοσία

Συνδεδεμένα δίκτυα:

Όνομα δικτύου	Διεύθυνση MAC	Μέση ισχύς λήψης
HellasOnline Home	00:05:59:09:BB:19	-24.75 dBm

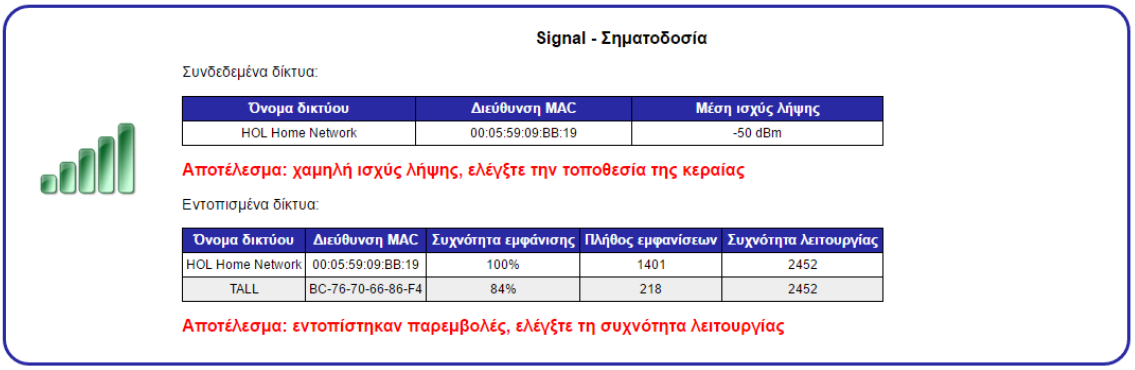
Αποτέλεσμα: δεν χρειάζεται βελτιστοποίηση

Εντοπισμένα δίκτυα:

Όνομα δικτύου	Διεύθυνση MAC	Συχνότητα εμφάνισης	Πλήθος εμφανίσεων	Συχνότητα λειτουργίας
HellasOnline Home	00-05-59-09-BB-19	100.00%	1401	2452
TALL	BC-76-70-66-86-F4	84.00%	218	2457

Αποτέλεσμα: δεν χρειάζεται βελτιστοποίηση

Εικόνα 8: Σηματοδοσία όταν όλα είναι χωρίς πρόβλημα



Signal - Σηματοδοσία

Συνδεδεμένα δίκτυα:

Όνομα δικτύου	Διεύθυνση MAC	Μέση ισχύς λήψης
HOL Home Network	00:05:59:09:BB:19	-50 dBm

Αποτέλεσμα: χαμηλή ισχύς λήψης, ελέγξτε την τοποθεσία της κεραίας

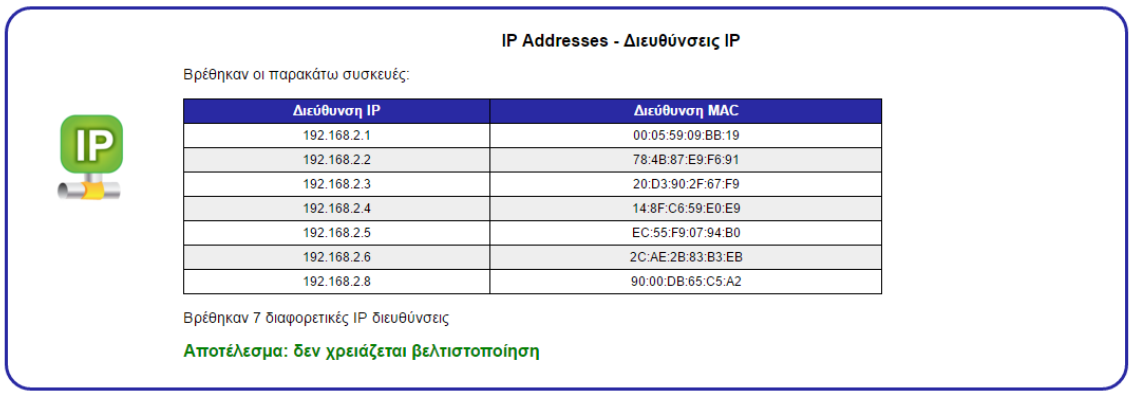
Εντοπισμένα δίκτυα:

Όνομα δικτύου	Διεύθυνση MAC	Συχνότητα εμφάνισης	Πλήθος εμφανίσεων	Συχνότητα λειτουργίας
HOL Home Network	00:05:59:09:BB:19	100%	1401	2452
TALL	BC-76-70-66-86-F4	84%	218	2452

Αποτέλεσμα: εντοπίστηκαν παρεμβολές, ελέγξτε τη συχνότητα λειτουργίας

Εικόνα 9: Σηματοδοσία όταν υπάρχουν προβλήματα και χρειάζεται βελτιστοποίηση

4.2 Αποτελέσματα διευθυνσιοδότησης



IP Addresses - Διευθύνσεις IP

Βρέθηκαν οι παρακάτω συσκευές:

Διεύθυνση IP	Διεύθυνση MAC
192.168.2.1	00:05:59:09:BB:19
192.168.2.2	78:4B:87:E9:F6:91
192.168.2.3	20:D3:90:2F:67:F9
192.168.2.4	14:8F:C6:59:E0:E9
192.168.2.5	EC:55:F9:07:94:B0
192.168.2.6	2C:AE:2B:83:B3:EB
192.168.2.8	90:00:DB:65:C5:A2

Βρέθηκαν 7 διαφορετικές IP διευθύνσεις

Αποτέλεσμα: δεν χρειάζεται βελτιστοποίηση

Εικόνα 10: Αποτελέσματα διευθυνσιοδότησης όταν δεν υπάρχει κάποιο πρόβλημα

4.3 Αποτελέσματα ασφάλειας δικτύου

Εικόνα 11: Αποτελέσματα ασφάλειας δικτύου όταν δεν υπάρχει κάποιο πρόβλημα

4.4 Αποτελέσματα ταχύτητας δικτύου

Εικόνα 12: Αποτελέσματα ταχύτητας δικτύου όταν δεν υπάρχει κάποιο πρόβλημα

5 Συσχετισμός με το μοντέλο FCAPS

Σύμφωνα με τον οργανισμό ISO, οι λειτουργικές περιοχές της διαχείρισης δικτύων είναι οι εξής πέντε:

- ✓ Performance
- ✓ Fault
- ✓ Accounting
- ✓ Configuration
- ✓ Security

Έτσι το μοντέλο διαχείρισης δικτύων του εν λόγω οργανισμού ονομάζεται FACPS ως ακρωνύμιο των παραπάνω περιοχών. Μπορούμε επίσης τις περιοχές αυτές, να τις διαχωρίσουμε σε δύο κατηγορίες. Σε αυτές που αφορούν στην επίβλεψη του δικτύου (performance, fault, accounting) και σε αυτές που αφορούν στον έλεγχο του δικτύου (configuration, security).

Στα πλαίσια της εργασίας δεν ασχοληθήκαμε καθόλου με θέματα Accounting και γι' αυτό δεν αναλύεται περαιτέρω η συγκεκριμένη περιοχή.

5.1 Fault Management

Fault είναι ένα event που έχει αρνητική επίπτωση σε ένα σύστημα. Fault Management είναι ο εντοπισμός, η απομόνωση, η διόρθωση και η καταγραφή των faults που συμβαίνουν στο σύστημα, καθώς επίσης και η χρησιμοποίηση trends για την πρόβλεψη λαθών, έτσι ώστε το δίκτυο να είναι πάντα διαθέσιμο. Για παράδειγμα, τα ιστογράμματα μας βοηθούν να

απεικονίσουμε τα events (αλλαγή κατάστασης για κάποιο service) σε σχέση με τον χρόνο και έτσι να έχουμε μια καλύτερη άποψη για το πότε συμβαίνει τι. Επίσης είναι χρήσιμο να μελετάμε τα logs των services για να πάρουμε μια πιο λεπτομερή άποψη για κάποιο fault που συμβαίνει. Τέλος, μέρος της ενημέρωσης του administrator του δικτύου είναι και τα μηνύματα βελτιστοποίησης που εμφανίζονται από το πρόγραμμά μας, όταν προκύψει κάποιο πρόβλημα, έτσι ώστε να ύπαρξη δυνατότητα άμεσης αντίδρασης και αντιμετώπισης αυτού.

5.2 Configuration Management

Στόχοι του configuration management είναι η συλλογή και αποθήκευση ρυθμίσεων από όλες τις συσκευές του δικτύου (είτε τοπικά είτε και σε remote hosts), η απλοποίηση των ρυθμίσεων μιας συσκευής, ο εντοπισμός και η οργάνωση των αλλαγών που γίνονται σε μια συσκευή, καθώς και ο σχεδιασμός για μελλοντικές επεκτάσεις και κλιμακώσεις του δικτύου. Αυτό επιτυγχάνεται με τον έλεγχο της διευθυνσιοδότησης, ώστε να βλέπουμε αν τελικά οι παραμετροποίησεις που έχουν γίνει στο δίκτυο είναι σωστές και βοηθούν στην βέλτιστη λειτουργία του.

5.3 Performance Management

Το performance management δίνει την δυνατότητα στον διαχειριστή να προετοιμάσει το δίκτυο για το μέλλον, καθώς επίσης και να προσδιορίσει την αποτελεσματικότητα του τρέχοντος δικτύου. Στην περίπτωση της δικής μας εργασίας, βλέπουμε αν η ταχύτητα λειτουργίας του δικτύου είναι ικανοποιητική (όπως προαναφέραμε) ή προτείνουμε στο διαχειριστή του συστήματος να ελέγξει τις σχετικές ρυθμίσεις.

5.4 Security Management

Στόχος του security management είναι η "διαχείριση" της ασφάλειας του δικτύου, αν δηλαδή το δίκτυο είναι ευάλωτο σε εξωτερικές επιθέσεις που μπορούν να πραγματοποιηθούν. Αν τα δεδομένα που μεταδίδονται είναι ανασφαλή, τότε επισημαίνουμε με το πρόγραμμά μας στο διαχειριστή του συστήματος, να προσθέσει κάποιο είδος κωδικοποίησης των δεδομένων, ώστε τα δεδομένα να μεταδίδονται πλέον με ασφάλεια.