ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Μελέτη, υλοποίηση και παρακολούθηση συμπεριφοράς σύγχρονου Σχολικού δικτύου με τεχνολογίες ασφάλειας και ασύρματης - ενσύρματης πρόσβασης.

ΒΑΣΙΛΕΙΑΔΗΣ ΟΡΕΣΤΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γιάννακας Γεώργιος

ΣΥΝΕΠΙΒΛΕΠΩΝ

Ξενάκης Απόστολος
Επίκουρος Καθηγητής

Λαμία, **Μάρτιος 2022**

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Design, Implementation and Monitoring of a Secure High School Wired and Wireless Local Network

VASILIADIS ORESTIS

FINAL THESIS

ADVISOR

Giannakas Georgios

CO ADVISOR

Xenakis Apostolos
Assistant Professor

Lamia, **March 2022**

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από τις διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω τον συγγραφέα, τη χρονολογία, την σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στην συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 19/02/2022

Ο Δηλών.
ΒΑΣΙΛΕΙΑΔΗΣ ΟΡΕΣΤΗΣ

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Στην συγκεκριμένη εργασία γίνεται ανάλυση της σχεδίασης και της κατασκευής ενός σύγχρονου τοπικού δικτύου για τις κτηριακές εγκαταστάσεις ενός σχολείου. Στο πρώτο κεφάλαιο γίνεται αναφορά σε τεχνολογίες ενσύρματης πρόσβασης και πιο συγκεκριμένα σε δίκτυα οπτικών ινών και δίκτυα Ethernet. Στο δεύτερο κεφάλαιο γίνεται αναφορά σε τεχνολογίες ασύρματης πρόσβασης, στις διαφορετικές γενιές του πρωτοκόλλου 802.11, στον τρόπο λειτουργίας του σε φυσικό και λογικό επίπεδο και σε τεχνολογίες περιαγωγής μεταξύ σημείων πρόσβασης. Στο τρίτο κεφάλαιο γίνεται αναφορά στη διαδικασία σχεδιασμού του νέου δικτύου. Περιγράφεται η υφιστάμενη κατάσταση, τα κριτήρια που τέθηκαν υπόψη για την σχεδίαση του νέου δικτύου σχετικά με την υποδομή ενσύρματης και ασύρματης πρόσβασης και η τεχνοοικονομική μελέτη που συντάχθηκε με την ολοκλήρωση του σχεδιασμού. Στο τέταρτο κεφάλαιο περιγράφεται η υλοποίηση της δικτυακής υποδομής, σχετικά με την εγκατάσταση αλλά και την παραμετροποίηση της. Στο πέμπτο κεφάλαιο γίνεται αναφορά στα συστήματα που έχουν εγκατασταθεί για την παρακολούθηση της συμπεριφοράς του δικτύου. Τέλος στο έκτο κεφάλαιο εξάγονται κάποια συμπεράσματα για τη βελτίωση των παρεχόμενων υπηρεσιών με την εγκατάσταση της νέας υποδομής, τόσο για τους μαθητές όσο και για τους εκπαιδευτικούς.

ABSTRACT

This thesis is about the design and implementation of a high-end local area network for a school building. The first chapter talks about wired network access technologies, more specifically optical and ethernet networks. The second chapter describes wireless network access technologies, the different iterations of the 802.11 protocol, how it works at the physical and logical layer and roaming technologies between different access points of the same wireless network. The third chapter is related to the design process for the school network. It depicts the current network implementation, different criteria taken into account while designing the wired and wireless network access topologies and the techno-economic study written after the finalisation of the above criteria. The fourth chapter depicts the implementation of the different systems, both regarding their physical installation and their software configuration. The fifth chapter describes the monitoring systems that are running to collect and graph system metrics and network traffic statistics. The last chapter describes the conclusions reached regarding the improvement of network access for the members of the school, both teachers and students

Table of Contents

ΚΕΦΑΛΑΙΟ 1 Σύγχρονες Τεχνολογίες Ενσύρματης Πρόσβασης

(Δίκτυα Οπτικών Ινών 1.1)

(Εισαγωγή 1.1.1)

Η χρήση του φωτός ως μέσο μετάδοσης πληροφορίας δεν είναι κάποια νέα ανακάλυψη. Συνέβαινε από την αρχαιότητα. Στην αρχαία Ελλάδα, οι Έλληνες χρησιμοποιούσαν τις Φρυκτωρίες. Οι Φρυκτωρίες ήταν μεγάλες φωτιές που τοποθετούσαν κυρίως βραδινές ώρες σε ψηλές κορυφές βουνών. Αυτές χρησιμοποιούνταν για τη μετάδοση μηνυμάτων από περιοχή σε περιοχή, ιδίως σε περιόδους πολέμου. Ο συγκεκριμένος τρόπος είχε επιλεγεί καθώς το φως συνέβαλε στην πολύ γρήγορη μετάδοση πληροφορίας, κάτι που συμβαίνει ακόμα και σήμερα.

Ακόμη στις αρχές του 19ου και του 20ου αιώνα οι καπετάνιοι των πλοίων χρησιμοποιούσαν ισχυρούς φακούς για την επικοινωνία τους με άλλα πλοία. Πιο συγκεκριμένα αναβόσβηναν τους ισχυρούς φακούς σύμφωνα με τον κώδικα Morse και έτσι μπορούσαν να ανταλλάσσουν μηνύματα μεταξύ τους.

Σε κάθε περίπτωση αποδεικνύεται ότι το φως αποτελούσε πάντα έναν εύκολο και γρήγορο τρόπο μεταφοράς δεδομένων. Ωστόσο δεν έλειπαν και τα μειονεκτήματα. Κακές καιρικές συνθήκες όπως η ομίχλη προκαλούσαν προβλήματα στην ορατότητα μεταξύ του αποστολέα και του παραλήπτη των μηνυμάτων. Ακόμη το συχνά εξασθενημένο φως από μια φωτιά ή έναν φακό, σήμαινε ότι η πληροφορία δε μπορούσε να φτάσει πολύ μακριά καθώς ο παραλήπτης δε μπορούσε να διακρίνει το φως και να λάβει το μήνυμα.

Στην σημερινή εποχή το φως συνεχίζει να αποδεικνύεται ένας από τους καλύτερους τρόπους μεταφοράς δεδομένων. Η επικοινωνία μέσω φωτός που χρησιμοποιούσε τον αέρα ως μέσο διάδοσης έχει κατά κύριο λόγο δώσει τη θέση της στην επικοινωνία με χρήση οπτικών ινών. Σε αυτή την περίπτωση πάλι έχουμε έναν αποστολέα και έναν παραλήπτη μηνυμάτων. Ωστόσο το μέσο μετάδοσης δεδομένων δεν είναι πια ο αέρας αλλά ένα νήμα κατασκευασμένο από γυαλί ή πλαστικό. Με αυτόν τον τρόπο μπορούν να μεταφερθούν πληροφορίες από σημείο σε σημείο σε αποστάσεις δεκάδων και εκατοντάδων χιλιομέτρων, κάτι που τις κάνει αναπόσπαστο κομμάτι των σύγχρονων τηλεπικοινωνιακών δικτύων.

(Κατασκευαστικά Στοιχεία 1.1.2)

Οι οπτικές ίνες αποτελούν έναν από τους πιο διαδεδομένους τρόπους μετάδοσης δεδομένων στα σύγχρονα δίκτυα επικοινωνιών. Οι οπτικές ίνες είναι πολύ λεπτά νήματα που κατασκευάζονται από πλαστικό ή γυαλί. Έχουν πολύ μικρό πάχος που μετριέται σε μικρόμετρα, λίγο παραπάνω από μια ανθρώπινη τρίχα. Τα υλικά από τα οποία μπορεί να κατασκευαστεί μια οπτική ίνα είναι πολλαπλά. Μπορεί να είναι κατασκευασμένη από διοξείδιο του πυριτίου, που είναι και το πιο κοινό υλικό κατασκευής, γυαλί από φθόριο (Fluoride Glass) αλλά και από πλαστικό. Οι οπτικές ίνες από γυαλί έχουν πολύ μικρότερο δείκτη διάθλασης από τις οπτικές

ίνες με πλαστικό. Αυτό σημαίνει ότι η απώλεια φωτεινής ενέργειας από τις πλαστικές οπτικές ίνες είναι μεγαλύτερη και αυτό περιορίζει κατά πολύ το μήκος που μπορούν να καλύψουν τα δίκτυα που χρησιμοποιούν πλαστικές οπτικές ίνες.

Οι οπτικές ίνες κατασκευάζονται με τη διαδικασία του Glass Drawing. Αρχικά δημιουργείται ένα υλικό το οποίο αποτελείται από διοξείδιο του πυριτίου ή το υλικό που έχει επιλεγεί για να κατασκευαστεί η συγκεκριμένη οπτική ίνα. Το συγκεκριμένο υλικό έχει ήδη τον επιθυμητό δείκτη διάθλασης και θα πρέπει στη συνέχεια να εφαρμοστεί η διαδικασία του Drawing για να φτάσει στο επιθυμητό μήκος ή πάχος. Η συγκεκριμένη διαδικασία πραγματοποιείται σε έναν πύργο που ονομάζεται drawing tower. Εκεί το γυαλί θερμαίνεται και λιώνει, ρέοντας έτσι μέσα από μια οπή. Το νήμα γυαλιού που βγαίνει τεντώνεται ενώ παράλληλα ελέγχεται τόσο το μήκος του νήματος που έχει παραχθεί όσο και το πάχος του έτσι ώστε να παραμένει στα επιθυμητά επίπεδα.

Το πάχος μια οπτικής ίνας μετριέται σε microns, με βάση την εξωτερική διάμετρο του νήματος που παρήχθη από την προηγούμενη διαδικασία. Το πιο συνηθισμένο πάχος του νήματος της οπτικής ίνας είναι 125 microns. Ωστόσο υπάρχουν και οπτικές ίνες με 50 microns και 62.5 microns πάχος.

Ωστόσο τα καλώδια οπτικών ινών συνήθως δεν αποτελούνται μόνο από μια οπτική ίνα. Αν συνέβαινε αυτό οι οπτικές ίνες θα ήταν ιδιαίτερα εύθραυστες ενώ και ένα μεγάλο ποσοστό της φωτεινής ενέργειας θα διέρρεε προς το περιβάλλον από τα πλάγια τοιχώματα του νήματος μέσω της διάθλασης. Αντίθετα γύρω από το νήμα της οπτικής ίνας υπάρχει μια επικάλυψη από ένα υλικό το οποίο έχει χαμηλότερο δείκτη διάθλασης από αυτόν του γυαλιού από το οποίο αποτελείται ο πυρήνας της οπτικής ίνας. Αυτή η επικάλυψη παγιδεύει το φως μέσα στον πυρήνα, αντανακλώντας το φως που πάει να διαρρεύσει πάλι πίσω.

Αυτό το περίβλημα στην συνέχεια περιβάλλεται από έναν μανδύα. Ο συγκεκριμένος μανδύας κατασκευάζεται συνήθως από ακρυλικά υλικά. Προστατεύει το εύθραυστο νήμα της οπτικής ίνας από υγρασία και σκόνη, ενώ παράλληλα τον καθιστά πιο ανθεκτικό, τόσο στην μεταφορά του όσο και στις καταπονήσεις που δέχεται κατά τη διαδικασία εγκατάστασης της.

Τέλος το ακρυλικό περίβλημα περιβάλλεται και αυτό με την σειρά του από μια σκληρή ρητίνη και στην συνέχεια ένα περίβλημα πλαστικού. Τα συγκεκριμένα περιβλήματα παρέχουν επιπλέον σταθερότητα στην οπτική ίνα αλλά δε συμβάλλουν στην βελτίωση των ιδιοτήτων της στην αγωγή του φωτός.

(Τύποι Καλωδίων Οπτικών Ινών 1.1.3)

Τα καλώδια οπτικών ινών χωρίζονται σε 2 μεγάλες κατηγορίες. Τις μονότροπες οπτικές ίνες (Single Mode Fibers) και τις πολύτροπες οπτικές ίνες (Multimode Fibers).

Οι μονότροπες οπτικές ίνες κατασκευάζονται κυρίως από πυρίτιο, ένα υλικό που έχει πολύ χαμηλό δείκτη διάθλασης. Στις μονότροπες οπτικές ίνες το φως κατευθύνεται μέσα στην οπτική ίνα από ένα μόνο μονοπάτι. Μια μονότροπη οπτική ίνα έχει διάμετρο πυρήνα που κυμαίνεται από 8 έως 10 μικρόμετρα. Αυτός ο πολύ λεπτός πυρήνας σημαίνει ότι το φως ταξιδεύει χωρίς να υφίσταται πολύ μεγάλα φαινόμενα διάθλασης. Έτσι δίνεται η δυνατότητα στο φως να ταξιδεύει σε μεγάλες αποστάσεις χωρίς να χάνει μεγάλο μέρος της ενέργειας του, θέτοντας τις

μονότροπες οπτικές ίνες μονόδρομο σε συνδέσεις από σημείο σε σημείο μεταξύ των όπου υπάρχει πολύ μεγάλη απόσταση. Οι ταχύτητες που μπορούν να επιτευχθούν στις μονότροπες οπτικές ίνες φτάνουν μέχρι και τα 40Gb/s ενώ με τη χρήση τεχνικών DWDM που διοχετεύουν πολλαπλές δέσμες φωτός σε διαφορετικά μήκη κύματος μέσα στην ίδια οπτική ίνα, μπορούν να επιτευχθούν ταχύτητες από 100Gb/s έως και πολλά Tb/s. Οι συγκεκριμένες ταχύτητες μπορούν να επιτευχθούν σε αποστάσεις από δεκάδες έως εκατοντάδες χιλιόμετρα, ανάλογα και τους πομποδέκτες που χρησιμοποιούνται στα άκρα των οπτικών ινών.

Οι πολύτροπες οπτικές ίνες κατασκευάζονται κυρίως από διαφανές πλαστικό. Ο πυρήνας από τις πολύτροπες οπτικές ίνες έχει έως και 10 φορές μεγαλύτερη διάμετρο από τον πυρήνα των μονότροπων οπτικών ινών. Αυτό σημαίνει ότι η διάθλαση του φωτός καθώς ταξιδεύει μέσα στην οπτική ίνα συμβαίνει σε μεγαλύτερο βαθμό από τις μονότροπες οπτικές ίνες. Αυτό το φαινόμενο περιορίζει κατά πολύ τις αποστάσεις που μπορούν να καλύψουν οι πολύτροπες οπτικές ίνες μιας και η ενέργεια του φωτός εξασθενεί πολύ γρηγορότερα. Οι πολύτροπες οπτικές ίνες μπορούν να καλύψουν αποστάσεις μέχρι και 2 χιλιόμετρα σε ταχύτητες 100Mb/s, 1000 μέτρα σε ταχύτητα 1Gb/s και 550 μέτρα σε ταχύτητα 10Gb/s. Χάρη στο μικρό τους κόστος, μεγάλη χωρητικότητα σε μικρές αποστάσεις και μεγάλη αξιοπιστία, οι πολύτροπες οπτικές ίνες αποτελούν την πιο δημοφιλή λύση για την καλωδίωση κορμού κτιρίων.

(Οπτικοί Πομποδέκτες 1.1.4)

Ο οπτικός πομποδέκτης είναι μία συσκευή η οποία χρησιμοποιεί οπτικές ίνες με σκοπό να μεταδώσει και να λάβει δεδομένα. Αποτελείται από έναν οπτικό πομπό, ο οποίος συνήθως είναι μια δίοδος LED ή LASER και έναν δέκτη ο οποίος αναλαμβάνει να μετατρέψει τους παλμούς φωτός σε ηλεκτρικά σήματα τα οποία στην συνέχεια θα αποκωδικοποιηθούν. Ακόμη αποτελείται από τα κυκλώματα τροφοδοσίας, τα κυκλώματα κωδικοποίησης και αποκωδικοποίησης, την ηλεκτρική διεπαφή με τη δικτυακή συσκευή στην οποία συνδέεται, και την υποδοχή για τον οπτικό σύνδεσμο που αναλαμβάνει να συγκρατήσει το οπτικό καλώδιο συνδεδεμένο αλλά και να αποτρέψει τη διαρροή του μεταφερόμενου φωτεινού παλμού. Όλα αυτά είναι συγκεντρωμένα μέσα στο ίδιο συμπαγές περίβλημα το οποίο συνήθως είναι μεταλλικό για λόγους ηλεκτρικής απομόνωσης από παρεμβολές γειτονικών κυκλωμάτων, αλλά και για την απαγωγή της παραγόμενης θερμότητας.

Οι οπτικοί πομποδέκτες είναι συνήθως γνωστοί με το όνομα SFP από τα αρχικά Small Form Factor Pluggable Transceiver, όταν αφορούν εφαρμογές μεταφοράς δεδομένων. Με βάση το είδος των οπτικών ινών που συνδέονται οι οπτικοί πομποδέκτες χωρίζονται σε πομποδέκτες για μονότροπες οπτικές ίνες και πομποδέκτες για πολύτροπες οπτικές ίνες. Οι πομποδέκτες για πολύτροπες οπτικές ίνες μπορούν να καλύψουν αποστάσεις από 500 μέτρα έως 2 χιλιόμετρα και συνήθως χρησιμοποιούν διόδους LED για την παραγωγή του φωτεινού παλμού.

Οι πομποδέκτες για μονότροπες οπτικές ίνες μπορούν να καλύψουν αποστάσεις αρκετών δεκάδων έως λίγων εκατοντάδων χιλιομέτρων. Με βάση την εφαρμογή τους οι οπτικοί πομποδέκτες διακρίνονται σε οπτικούς πομποδέκτες για εφαρμογές όπως Ethernet, SONET/SDH, Fiber Channel κλπ. Με βάση το μέγεθος και τις δυνατότητες τους διακρίνονται σε: Οπτικούς πομποδέκτες GBIC/SFP που μπορούν

να υποστηρίξουν ταχύτητες 100Mb/s και 1Gb/s, SFP+ που μπορούν να υποστηρίξουν ταχύτητες 10Gb/s και SFP28 που υποστηρίζουν ταχύτητες 25Gb/s. Ακόμη υπάρχουν οι οπτικοί πομποδέκτες QSFP+ (Quad SFP+) που πρακτικά είναι 4 SFP+ πομποδέκτες και μπορούν να υποστηρίξουν ταχύτητες 4x10Gb/s=40Gb/s και QSFP28 που πρακτικά είναι 4 SFP28 πομποδέκτες και μπορούν να υποστηρίξουν ταχύτητες 100Gb/s (4x25Gb/s). Άλλες παλαιότερες τεχνολογίες οπτικών πομποδεκτών αποτελούν οι XFP και οι XENPAK πομποδέκτες που μπορούν να υποστηρίξουν ταχύτητες 10Gb/s.

(Οπτικοί Πομποδέκτες 1.1.5)

Τα καλώδια οπτικών ινών χωρίζονται σε πολλές κατηγορίες με βάση το υλικό κατασκευής του προστατευτικού μανδύα τους, το είδος χρήσης και τον αριθμό των νημάτων οπτικών ινών που περικλείουν μέσα τους. Έτσι με βάση το υλικό κατασκευής του προστατευτικού μανδύα, έχουμε καλώδια από LZSH, πολυβινύλιο, πολυαιθυλένιο, πολυουρεθάνη και polyamide.

Ακόμη, με βάση το υλικό κατασκευής της οπτικής ίνας, τα καλώδια χωρίζονται σε αυτά που η οπτική ίνα είναι κατασκευασμένη από πλαστικό και σε αυτά που η οπτική ίνα είναι κατασκευασμένη από γυαλί. Οι οπτικές ίνες από πλαστικό χρησιμοποιούνται για εμπορικές εφαρμογές που χρειάζονται να καλύψουν μικρές αποστάσεις ενώ τα καλώδια από γυαλί χρησιμοποιούνται για εφαρμογές που χρειάζεται να καλύψουν μεσαίες και μεγάλες αποστάσεις.

Στην συνέχεια με βάση το είδος χρήσης που πρόκειται να εξυπηρετήσουν τα καλώδια χωρίζονται σε τερματισμένα οπτικά καλώδια και μη τερματισμένα οπτικά καλώδια. Στα πρώτα οι ακροδέκτες έχουν συγκολληθεί από το εργοστάσιο και είναι συγκεκριμένου μήκους, το οποίο συχνά είναι τυποποιημένο και δε διαφέρει από κατασκευαστή σε κατασκευαστή. Στη δεύτερη περίπτωση το οπτικό καλώδιο δεν έχει συγκολλημένους τους ακροδέκτες στις άκρες του. Αντίθετα αφού οριστεί το επιθυμητό μήκος, γίνεται συγκόλληση του επιθυμητού ακροδέκτη με το οπτικό καλώδιο μέσω μιας διαδικασίας που ονομάζεται fusion splicing. Στην συγκεκριμένη διαδικασία τα δύο άκρα των οπτικών ινών καθαρίζονται και “σπάνε” και από τις δύο πλευρές με σκοπό να δημιουργηθεί μια ίσια επιφάνεια που θα κολλήσει σωστά με την άλλη. Στην συνέχεια τα δύο άκρα τοποθετούνται μέσα στο μηχάνημα συγκόλλησης το οποίο αναλαμβάνει να τα μετακινήσει το ένα απέναντι από το άλλο και στην συνέχεια μέσω ενός ηλεκτρικού τόξου που δημιουργείται, να τα συγκολλήσει μέσω της τήξης του υλικού από το οποίο είναι κατασκευασμένες. Τέλος ένα προστατευτικό πλαστικό περικλείει το σημείο της συγκόλλησης με σκοπό να το προστατεύσει.

Τα προτερματισμένα καλώδια οπτικών ινών τείνουν να χρησιμοποιούν έναν χρωματικό κώδικα. Έτσι τα πορτοκαλί καλώδια είναι πολύτροπες οπτικές ίνες, ενώ τα κίτρινα καλώδια είναι μονότροπες οπτικές ίνες. Τέλος τα μπλε καλώδια συνήθως αποτελούν πολωμένες οπτικές ίνες όπου το φως εισάγεται με συγκεκριμένη πόλωση και εξέρχεται από την οπτική ίνα με την ίδια πόλωση.

Επιπλέον υπάρχουν τα καλώδια πολλαπλών οπτικών ινών. Στην συγκεκριμένη περίπτωση πολλαπλά καλώδια οπτικών ινών περικλείονται από ένα προστατευτικό περίβλημα. Τα καλώδια οπτικών ινών ξεχωρίζουν μεταξύ τους με βάση το χρώμα του προστατευτικού μανδύα που περικλείει καθένα από τα καλώδια ξεχωριστά. Τα

συγκεκριμένα καλώδια είναι ιδιαίτερα δημοφιλή σε περιπτώσεις συνδέσεων μεταξύ κτιρίων αλλά και μεταξύ διαφορετικών περιοχών, επειδή δίνεται η δυνατότητα για ύπαρξη εφεδρείας για μελλοντικές επεκτάσεις, είναι πιο εύκολο να εγκατασταθεί κάτω από τη γη ή μέσα από ηλεκτρολογικές οδεύσεις ένα καλώδιο σε σχέση με πολλαπλά και επειδή οι εργασίες όδευσης καλωδίων κάτω από τη γη είναι ιδιαίτερα κοστοβόρες συμφέρει να πραγματοποιηθούν μια φορά.

(Ακροδέκτες 1.1.6)

Υπάρχουν πολλαπλά είδη ακροδεκτών τα οποία χρησιμοποιούνται στις τηλεπικοινωνιακές εφαρμογές:

- Οι ακροδέκτες SC:

Οι συγκεκριμένοι ακροδέκτες δημιουργήθηκαν στα μέσα του 1980. Αποτελούνται από έναν μηχανισμό push pull που μανδαλώνει στην οπτική υποδοχή του πομποδέκτη με τη βοήθεια ενός ελατηρίου. Αρχικά σχεδιάστηκαν για ταχύτητες του 1Gb/s ενώ είναι ιδιαίτερα διαδεδομένοι σε εφαρμογές παθητικών οπτικών δικτύων αλλά και εφαρμογές μετάδοσης δεδομένων, όντας ο δεύτερος πιο διάσημος τύπος οπτικού ακροδέκτη. Οι ακροδέκτες SC χωρίζονται και σε δύο ακόμα κατηγορίες, τους ακροδέκτες SC UPC και SC APC. Στην περίπτωση των UPC ακροδεκτών το άκρο του ακροδέκτη είναι ίσιο με αποτέλεσμα οποιαδήποτε αντανάκλαση του φωτός να επιστρέφει ευθεία πίσω στο καλώδιο της οπτικής ίνας. Στην περίπτωση των APC ακροδεκτών, το άκρο του ακροδέκτη είναι καμπυλωμένο. Αυτό έχει ως αποτέλεσμα το φως να αντανακλάται υπό γωνία σε σχέση με τη φωτεινή δέσμη που έρχεται από την οπτική ίνα. Το συγκεκριμένο φαινόμενο προκαλεί κάποιες διαφορές στην απώλεια φωτεινής ενέργειας από τον έναν τύπο ακροδέκτη στον άλλο. Τα πρότυπα ορίζουν ότι ένας ακροδέκτης APC πρέπει να έχει απώλειες από -60 dB και πάνω, ενώ ένας ακροδέκτης UPC πρέπει να έχει απώλειες από -50 dB και πάνω. Όσο πιο μεγάλος είναι ο αριθμός, τόσο το καλύτερο. Έτσι σε εφαρμογές που έχει μεγάλη σημασία να μην υπάρχει μεγάλη απώλεια οπτικής ενέργειας όπως για παράδειγμα εφαρμογές ράδιο-τηλεπικοινωνιών ή παθητικών οπτικών δικτύων FTTH, ένας ακροδέκτης APC είναι προτιμητέος. Αντίθετα σε εφαρμογές που δεν παίζει τόσο μεγάλο ρόλο η απώλεια οπτικής ενέργειας τότε μπορεί να χρησιμοποιηθεί και ένας ακροδέκτης UPC

- Οι ακροδέκτες SC-DC και SC-QC

Οι ακροδέκτες SC-DC και SC-QC πήραν το όνομα τους από τα αρχικά SC - Dual Contact και SC Quad Contact. Στην περίπτωση του SC-DC αποτελούν δύο ακροδέκτες SC υπό του ίδιου κελύφους ενώ στην περίπτωση του SC-DC αποτελούν τέσσερις ακροδέκτες SC υπό του ίδιου κελύφους,

- Οι Ακροδέκτες LC:

Οι ακροδέκτες LC αποτελούν τον πιο διάσημο τύπο οπτικού ακροδέκτη και την εξέλιξη των SC ακροδεκτών. Και αυτοί έχουν έναν μηχανισμό push pull που στην συγκεκριμένη περίπτωση μανδαλώνει με τη βοήθεια ενός ελαστικού σύρτη. Οι ταχύτητες που μπορούν να υποστηρίξουν κυμαίνονται στις δεκάδες έως εκατοντάδες Gb/s. Οι LC ακροδέκτες είναι πιο λεπτοί από τους SC ακροδέκτες,

κάτι που τους κάνει ιδιαίτερα διάσημους σε εφαρμογές δομημένης καλωδίωσης με μεγάλη πυκνότητα συνδέσεων όπως είναι για παράδειγμα τα οπτικά patch panels μέσα σε ικριώματα.

- Οι Ακροδέκτες MPO/MTP:

Η ονομασία των MPO ακροδεκτών προκύπτει από τα αρχικά Multi Fiber Patch On. Οι συγκεκριμένοι ακροδέκτες μπορούν να υπάρχουν είτε για μονότροπες είτε για πολύτροπες οπτικές ίνες και συγκεντρώνουν οχτώ, δώδεκα και εικοσιτέσσερις οπτικές ίνες μέσα στον ίδιο ακροδέκτη ενώ για πιο εξειδικευμένες εφαρμογές όπως οπτικούς διαμεταγωγείς υπάρχουν ακροδέκτες MPO για τριάντα δύο, σαράντα οχτώ, εξήντα και εβδομήντα δυο οπτικές ίνες. Οι ακροδέκτες αυτοί χρησιμοποιούνται σε περιπτώσεις που είναι επιθυμητή η εγκατάσταση προ-τερματισμένων οπτικών ινών σε μέρη με μεγάλη πυκνότητα καλωδίων όπως σε περιπτώσεις κέντρων δεδομένων.

- Οι ακροδέκτες ST:

Τέλος αρκετά διάσημοι ιδιαίτερα τη δεκαετία του 1980 και 1990, σε εφαρμογές μεταγωγής δεδομένων είναι οι ακροδέκτες ST. Οι συγκεκριμένοι ακροδέκτες έχουν σπείρωμα στο εσωτερικό τους και βιδώνονται στα οπτικά patch panels με σκοπό να στερεωθούν σε αυτά. Χρησιμοποιούνται κυρίως για πολύτροπες οπτικές ίνες και λιγότερο για μονότροπες οπτικές ίνες.

(Πρωτόκολλα Οπτικών Επικοινωνιών 1.1.7)

Επειδή η κυρίαρχη εφαρμογή των οπτικών ινών στα τηλεπικοινωνιακά δίκτυα είναι η επέκταση δικτύων Ethernet σε μεγάλες αποστάσεις, θα αναφερθούμε σε πρωτόκολλα που επιτρέπουν τη μετάδοση πλαισίων Ethernet πάνω από καλώδια οπτικών ινών.

Έτσι αρχικά όσο αναφορά τον 10Mb/s Ethernet έχουμε την οικογένεια πρωτοκόλλων 10Base-F. Η συγκεκριμένη οικογένεια αποτελείται από το πρωτόκολλο 10Base-FL το οποίο προσφέρεται για δίκτυα Ethernet με μέγιστο μήκος 2 χιλιόμετρα πάνω από πολύτροπη οπτική ίνα καθώς και το 10Base-FB και 10Base-FP τα οποία δε χρησιμοποιήθηκαν ποτέ.

Στην συνέχεια όσον αναφορά το 100Mb/s Ethernet αρχικά έχουμε το πρωτόκολλο 100Base-FX. Το συγκεκριμένο πρωτόκολλο χρησιμοποιεί δύο ίνες πολύτροπης οπτικής ίνας και μπορεί να καλύψει αποστάσεις τετρακοσίων μέτρων σε half duplex επικοινωνία και 2 χιλιόμετρα σε full duplex επικοινωνία. Έπειτα υπάρχει το πρωτόκολλο 100Base-SX το οποίο επιτρέπει ταχύτητες 100Mb/s πάνω από πολύτροπη οπτική ίνα σε αποστάσεις μέχρι τριακόσια μέτρα. Τέλος υπάρχουν τα πρωτόκολλα 100Base-BX τα οποία επιτρέπουν ταχύτητες 100Mb/s πάνω από μια μονότροπη οπτική ίνα σε αποστάσεις μέχρι και δέκα χιλιόμετρα με επικοινωνία full duplex και 100Base-LX που επιτρέπουν ταχύτητες 100Mb/s πάνω από ένα ζεύγος μονότροπων οπτικών ινών σε αποστάσεις μέχρι και δέκα χιλιόμετρα με επικοινωνία full duplex.

Ακόμη όσον αφορά το Gigabit Ethernet υπάρχουν τα πρωτόκολλα 1000Base-LX και 1000Base-SX. Το 1000Base-LX πρωτόκολλο επιτρέπει ταχύτητες 1Gb/s πάνω

από πολύτροπη οπτική ίνα σε αποστάσεις μέχρι πεντακόσια πενήντα μέτρα ενώ το 1000Base-SX επιτρέπει ταχύτητες 1Gb/s πάνω από πολύτροπη οπτική ίνα σε αποστάσεις μέχρι πεντακόσια πενήντα μέτρα η πάνω από μονότροπη οπτική ίνα σε αποστάσεις μέχρι πέντε χιλιόμετρα. Επιπλέον υπάρχουν τα πρωτόκολλα 1000Base-LX10 και 1000Base-SX10. Το πρωτόκολλο 1000Base-LX10 επιτρέπει ταχύτητες του 1Gb/s σε αποστάσεις μέχρι δέκα χιλιόμετρα πάνω από ένα ζεύγος πολύτροπων οπτικών ινών. Το πρωτόκολλο 1000Base-SX10 επιτρέπει ταχύτητες 1Gb/s σε αποστάσεις μέχρι 10 χιλιόμετρα πάνω από 1 μονότροπη οπτική ίνα.

Επιπρόσθετα, όσον αφορά το 10 Gigabit Ethernet υπάρχει αρχικά το πρωτόκολλο 10GBASE-SR το οποίο επιτρέπει ταχύτητες 10Gb/s πάνω από πολύτροπες οπτικές ίνες σε αποστάσεις από είκοσι πέντε έως τετρακόσια μέτρα. Στη συνέχεια το πρωτόκολλο 10GBASE-LX4 επιτρέπει ταχύτητες 10Gb/s πάνω από πολύτροπες οπτικές ίνες σε αποστάσεις διακόσια πενήντα έως τριακόσια μέτρα αλλά και πάνω από μονότροπες οπτικές ίνες σε αποστάσεις έως δέκα χιλιόμετρα. Ακόμη το πρωτόκολλο 10GBASE-LR επιτρέπει ταχύτητες 10Gb/s πάνω από μονότροπη οπτική ίνα σε αποστάσεις μέχρι δέκα χιλιόμετρα ενώ το πρωτόκολλο 10BASE-BX επιτρέπει ταχύτητες 10 Gb/s, σε αποστάσεις έως ογδόντα χιλιόμετρα πάνω από μονότροπη οπτική ίνα.

Στο 25 Gigabit Ethernet έχουμε το πρωτόκολλο 25GBASE-SR το οποίο επιτρέπει ταχύτητες 25Gb/s πάνω πολύτροπες οπτικές ίνες σε αποστάσεις μέχρι εκατό μέτρα και το πρωτόκολλο 25GBASE-LR το οποίο επιτρέπει ταχύτητες 25Gb/s πάνω από μονότροπες οπτικές ίνες σε αποστάσεις έως δέκα χιλιόμετρα.

Τέλος στα 40 Gb/s Ethernet το πρωτόκολλο 40GBASE-SR4 επιτρέπει ταχύτητες 40Gb/s πάνω από πολύτροπες οπτικές ίνες σε αποστάσεις έως εκατό μέτρα ενώ το 40GBASE-LR4 επιτρέπει ταχύτητες 40Gb/s πάνω από μονότροπες οπτικές ίνες σε αποστάσεις έως δέκα χιλιόμετρα.

Πέρα από το πρωτόκολλο Ethernet, οι οπτικές ίνες είναι ιδιαίτερα δημοφιλείς σε τηλεπικοινωνιακές εφαρμογές γι' αυτό που ονομάζεται τελευταίο μίλι, την πρόσβαση δηλαδή των τελικών καταναλωτών σε ένα δίκτυο με χρήση δικτύων οπτικών ινών και πιο συγκεκριμένα παθητικών οπτικών δικτύων, δίκτυα δηλαδή χωρίς ενεργό δικτυακό εξοπλισμό κοντά στον πελάτη.

Στην συγκεκριμένη περίπτωση το πρωτόκολλο που χρησιμοποιείται από τα παθητικά δίκτυα οπτικών ινών είναι γνωστό με την ονομασία GPON. Το συγκεκριμένο πρωτόκολλο κατά τη λήψη στέλνει τα ίδια δεδομένα σε όλους τους καταναλωτές και είναι δουλειά της δικτυακής συσκευής του χρήστη να διαχωρίσει τα δεδομένα που την ενδιαφέρουν ενώ στην αποστολή κάθε χρήστης εκπέμπει στη χρονοθυρίδα που του έχει ανατεθεί χρησιμοποιώντας τεχνικές πολλαπλής πρόσβασης με διαίρεση χρόνου (TDMA).

Το GPON μπορεί να επιτύχει ταχύτητες μέχρι 2.5Gb/s Downstream και 1.25Gb/s Upstream, ωστόσο αυτή η ταχύτητα μοιράζεται μεταξύ των διαφορετικών καταναλωτών. Εξελίξεις του GPON αποτελούν το XG-PON το οποίο μπορεί να πετύχει ταχύτητες έως 10Gb/s Downstream και 2.5Gb/s Upstream, το XGS-PON το οποίο μπορεί να πετύχει ταχύτητες 10Gb/s Downstream και 10Gb/s Upstream και το WDM-PON το οποίο πια χρησιμοποιεί τεχνικές πολυπλεξίας με διαίρεση οπτικού φάσματος και μπορεί να πετύχει ταχύτητες 40Gb/s Downstream και 40Gb/s Upstream.

(Δίκτυα Ethernet 1.2)

Το Ethernet είναι ένα σύνολο από τεχνολογίες δικτύωσης υπολογιστικών συστημάτων που χρησιμοποιεί τόσο σε τοπικά δίκτυα όσο και σε δίκτυα ευρείας περιοχής όπως είναι το διαδίκτυο.

(Ιστορικά Στοιχεία 1.2.1)

Το πρωτόκολλο Ethernet εμφανίστηκε το 1980 για πρώτη φορά αλλά έγινε πρότυπο του IEEE το 1983 ως IEEE 802.3. Με την εισαγωγή του και το πέρασμα των χρόνων το Ethernet πρωτόκολλο αντικατέστησε παλαιότερες τεχνολογίες και πρωτόκολλα δικτύωσης όπως είναι το Token Ring, το FDDI και το ARCNET. Από την πρώτη εμφάνιση του πρωτοκόλλου το 1983 και με την τεχνολογική εξέλιξη, το Ethernet έχει βελτιωθεί για να μπορεί να υποστηρίξει μεγαλύτερες ταχύτητες, περισσότερους κόμβους πάνω στο ίδιο δίκτυο καθώς και να μπορεί να καλύψει μεγαλύτερες αποστάσεις.

Το πρωτόκολλο Ethernet δημιουργήθηκε από τα εργαστήρια Xerox PARC την περίοδο από το 1973 έως το 1974. Βασίστηκε πάνω στο πρωτόκολλο δικτύωσης ALOHANet το οποίο είχε μελετήσει ο Dr Robert Macalfe, εργαζόμενος στην συγκεκριμένη εταιρεία, ως κομμάτι της διδακτορικής διατριβής του. Το 1975 η εταιρεία Xerox έκανε αίτημα για να κάνει πατέντα το πρωτόκολλο Ethernet ορίζοντας ως εφευρέτες του τον Dr Robert Metcalfe, David Boggs, Chuck Thacker και Butler Lampson. Παράλληλα το 1976 που τέθηκε πρώτη φορά για παραγωγική λειτουργία στα εργαστήρια PARC το συγκεκριμένο πρωτόκολλο, ο Dr Robert Metcalfe και ο David Boggs δημοσίευσαν επιστημονικό άρθρο πάνω στην συγκεκριμένη εφεύρεση.

Η αρχική ταχύτητα του πρωτοκόλλου ήταν 2.94 Mb/s. Ο Ron Crane, Bob Garner και Roy Ogus αναβάθμισαν την ταχύτητα του πρωτοκόλλου στα 10Mb/s το 1980 όταν και δόθηκε σε εμπορική διαθεσιμότητα στην αγορά.

Στη συνέχεια η Digital Equipment Corporation, σε συνεργασία με την Intel και την Xerox προώθησαν το Ethernet ως πρότυπο δικτύωσης κάτι και το οποίο επέτυχε μιας και το 1980 δημοσιεύθηκε για πρώτη φορά το Ethernet πρότυπο με τον τίτλο «The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications.» Το συγκεκριμένο δημοσίευμα όριζε το Ethernet ως ένα πρωτόκολλο δικτύωσης με ταχύτητα 10Mb/s και διευθύνσεις προέλευσης και προορισμού μεγέθους 48 bit, τις γνωστές MAC διευθύνσεις.

Η 3Com, η εταιρεία στην οποία προσλήφθηκε ο Dr Robert Metcalfe μετά την αποχώρηση του από την Xerox προσέφερε στην αγορά την πρώτη δικτυακή διεπαφή για υπολογιστές με ταχύτητα 10Mb/s ενώ τον ίδιο χρόνο ξεκίνησε να παρέχει σε εμπορικό επίπεδο διεπαφές Ethernet και για υπολογιστές τύπου PDP-11 αλλά και VAX καθώς και για υπολογιστές των εταιρειών Intel αλλά και Sun Microsystems οι οποίοι ήταν βασισμένοι πάνω στον Multibus[1] δίαυλο. Η εταιρεία Digital Equipment Corporation στη συνέχεια δημιούργησε έναν προσαρμογέα από Unibus[1] σε Ethernet ο οποίος χρησιμοποιήθηκε τόση για εμπορική χρήση όσο και

1. Τόσο το Unibus όσο και το Multibus είναι πρότυπα διαύλων επικοινωνίας τα οποία χρησιμοποιούσαν οι υπολογιστές της εποχής με σκοπό την επικοινωνία των διαφόρων συσκευών που τους απαρτίζουν.

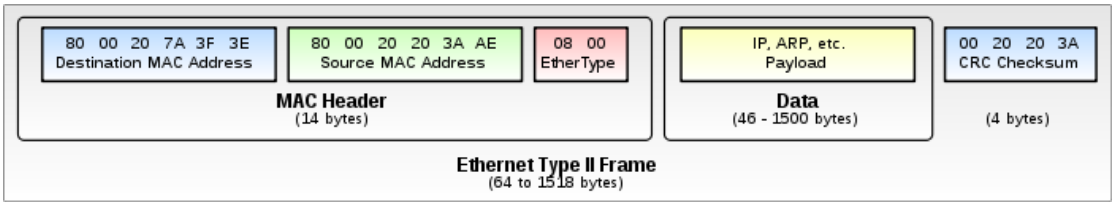
εσωτερικά από την εταιρεία, με σκοπό να στήσει το εταιρικό της δίκτυο βασισμένο στο πρωτόκολλο Ethernet. Ακόμη, η εταιρεία IBM το 1982 δημιούργησε έναν προσαρμογέα Ethernet για το IBM PC.

Η Ethernet δικτύωση μεταξύ υπολογιστών δεν έγινε ωστόσο ιδιαίτερα διαδεδομένη καθ' όλη τη διάρκεια της δεκαετίας του 1980. Αντιθέτως γνώρισε τεράστια ανάπτυξη στα τέλη της συγκεκριμένης δεκαετίας όταν το πρωτόκολλο Ethernet έγινε διάσημο σε σχολεία και οργανισμούς με σκοπό τον διαμοιρασμό αρχείων αλλά και τη δικτυακή εκτύπωση.

Από τότε η τεχνολογία Ethernet συνεχώς βελτιώνεται με σκοπό να μπορεί να πετύχει όλο και μεγαλύτερες ταχύτητες αλλά και ανάγκες της αγοράς. Το Ethernet πια χρησιμοποιείται για να διασυνδέσει πέρα από υπολογιστές και άλλες προσωπικές και μη συσκευές και μηχανήματα ενώ έχει αντικαταστήσει παλαιότερα δίκτυα μεταφοράς δεδομένων σε παγκόσμιο επίπεδο.

(Δομή ενός πλαισίου Ethernet 1.2.2)

Το βασικό μέσο μετάδοσης του πρωτοκόλλου Ethernet είναι τα πλαίσια που το απαρτίζουν. Το πλαίσιο Ethernet αποτελείται από τρία βασικά μέρη. Το πρώτο μέρος ενός πλαισίου Ethernet είναι το «προοίμιο» (preamble) του πακέτου που λειτουργεί ως ειδοποίηση ότι φτάνει ένα πλαίσιο Ethernet. Στην συνέχεια ακολουθεί ο Start Frame Delimiter (SFD), ο οποίος δείχνει την έναρξη ενός πλαισίου Ethernet. Στο δεύτερο και κύριο μέρος ενός πλαισίου Ethernet υπάρχει η κεφαλίδα του πλαισίου η οποία αποτελείται από τη διεύθυνση MAC της πηγής και τη διεύθυνση MAC του προορισμού που πρέπει να αποσταλεί το συγκεκριμένο πακέτο. Ακόμη αποτελείται από το πεδίο Ethertype που δείχνει είτε τον τύπο του πρωτοκόλλου που μεταφέρεται στο χώρο του payload είτε το μήκος του payload που θα μεταφερθεί. Στο τέλος του πλαισίου Ethernet υπάρχει πεδίο CRC που έχει μήκος 32 bit που χρησιμοποιείται για να ελέγξει εάν υπήρξε αλλοίωση στα μεταφερόμενα δεδομένα κατά την διάρκεια της μεταφοράς τους.



Εικόνα 1: Πλαίσιο Ethernet [1]

(Διευθυνσιοδότηση και Επικοινωνία 1.2.3)

Στα δίκτυα Ethernet η επικοινωνία γίνεται με τη χρήση διευθύνσεων που έχουν μήκος 48 bit και ονομάζονται Media Access Control (MAC) Addresses. Κάθε διεπαφή Ethernet έχει προγραμματισμένη από την κατασκευή της μια διεύθυνση MAC η οποία είναι μοναδική σε παγκόσμιο επίπεδο. Η διεύθυνση

προέλευσης και προορισμού του πακέτου Ethernet περιλαμβάνεται στην κεφαλίδα του πλαισίου.

(Κωδικοποίηση και Μεταφορά Δεδομένων 1.2.4)

Το πρότυπο 802.3 (Ethernet) περιγράφει ένα δίκτυο μεταφοράς δεδομένων το οποίο χρησιμοποιεί για την κωδικοποίηση των σημάτων επάνω στο μέσο μεταφοράς, την τεχνολογία πολλαπλής πρόσβασης με ανίχνευση φέροντος και συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance). Συγκρούσεις υπάρχουν όταν πολλαπλοί σταθμοί επιχειρούν να επικοινωνήσουν την ίδια στιγμή. Αυτό αναγκάζει τους σταθμούς να επιχειρήσουν να επικοινωνήσουν μεταξύ τους ξανά, κάτι το οποίο μειώνει την ταχύτητα και αυξάνει την καθυστέρηση.

Αρχικά οι υπολογιστές και γενικότερα οι κόμβοι ενός δικτύου Ethernet ήταν διασυνδεδεμένοι και επικοινωνούσαν μεταξύ τους μέσω ενός κοινού ομοαξονικού καλωδίου μέσω ενός πομποδέκτη που ονομαζόταν Attachment Unit Interface (AUI) Transceiver. Τα ομοαξονικά καλώδια αρχικά είχαν διάμετρο 9.5 χιλιοστά και το δίκτυο ήταν γνωστό ως Thick Ethernet ή thicknet. Αργότερα όμως προτιμήθηκε το πρότυπο ομοαξονικού καλωδίου RG-58 το οποία ήταν πιο ευρέως διαδεδομένο και έτσι η εγκατάσταση του δικτύου ήταν πιο εύκολη αλλά και λιγότερο κοστοβόρα. Ωστόσο η συγκεκριμένη υλοποίηση με διαμοιρασμό ενός ομοαξονικού καλωδίου μπορεί να ήταν εφικτή σε μικρά τοπικά δίκτυα αλλά δεν είναι εφικτή σε μεγάλα δίκτυα όπου διακοπή του ομοαξονικού καλωδίου λόγω βλάβης μπορούσε να καταστήσει όλο το δίκτυο μη λειτουργικό. Επιπλέον αδυναμίες της συγκεκριμένης λύσης ήταν ότι μιας και όλη η επικοινωνία γίνεται πάνω από το ίδιο καλώδιο όλοι οι υπολογιστές του δικτύου λαμβάνουν πλαίσια Ethernet ακόμα και αν αυτά δεν απευθύνονται σε αυτούς. Επιπλέον μιας και υπάρχει κοινό μέσο επικοινωνίας το μέγιστο διαθέσιμο εύρος ζώνης διαιρείται με τον αριθμό των κόμβων που απαρτίζουν το συγκεκριμένο δίκτυο.

Τα συγκεκριμένα προβλήματα έφεραν την εξέλιξη του δικτύου Ethernet. Τα μοντέρνα δίκτυα που χρησιμοποιούν το συγκεκριμένο πρωτόκολλο για τη μεταφορά δεδομένων και είναι βασισμένα στις BaseT προδιαγραφές, αντί για ομοαξονικό καλώδιο χρησιμοποιούν συνεστραμμένα ζεύγη καλωδίων για την ηλεκτρική επικοινωνία. Ακόμη δεν υπάρχει κοινός δίαυλος επικοινωνίας. Αντιθέτως, κάθε κόμβος έχει το δικό του καλώδιο το οποίο καταλήγει σε έναν κεντρικό συγκεντρωτή ο οποίος παλαιότερα ονομαζόταν repeater ή hub και στις μοντέρνες υλοποιήσεις διαμεταγωγέας (switch). Έτσι το Ethernet είναι ένα δίκτυο διαμεταγωγής πακέτων.

Στην περίπτωση του repeater, όταν ένα πλαίσιο Ethernet έφτανε σε μία από τις πόρτες της συσκευής τότε η συσκευή επαναλάμβανε τα πλαίσια σε όλες τις άλλες πόρτες. Αυτό ωστόσο δημιουργούσε πρόβλημα με συγκρούσεις όταν πολλαπλοί κόμβοι του Ethernet δικτύου προσπαθούσαν να μιλήσουν μεταξύ τους.

Την επίλυση αυτού το προβλήματος την έφερε η αλλαγή των repeaters με διαμεταγωγείς. Στην συγκεκριμένη περίπτωση όταν ένα πλαίσιο Ethernet φτάνει στην πόρτα της συσκευής, τότε η συσκευή αναλαμβάνει να προωθήσει το πλαίσιο στον προορισμό του. Σε αυτή την περίπτωση οι πιθανότητες για συγκρούσεις είναι ελάχιστες και θα συμβούν μόνο εάν ο κόμβος και ο διαμεταγωγέας επιχειρήσουν να

επικοινωνήσουν την ίδια στιγμή. Σε εξέλιξη του συγκεκριμένου θέματος, με την εισαγωγή του 10 Base-T δημιουργήθηκε η δυνατότητα full-duplex επικοινωνίας. Στην συγκεκριμένη περίπτωση τόσο ο κόμβος όσο και ο διαμεταγωγέας μπορεί να στείλει και να λάβει την ίδια στιγμή. Αυτό έχει ως αποτέλεσμα οι συγκρούσεις να είναι πια μηδενικές.

(Κατηγορίες Καλωδίων 1.2.5)

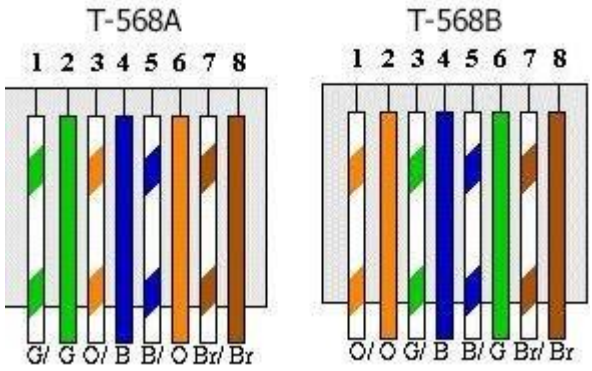
Τα καλώδια που χρησιμοποιούνται για την μετάδοση των ηλεκτρικών σημάτων του πρωτοκόλλου Ethernet αποτελούνται από 8 αγωγούς οι οποίοι ανά 2 είναι συνεστραμμένοι μεταξύ τους δημιουργώντας 4 ζεύγη. Ο λόγος που υπάρχει αυτή η συστροφή είναι για να υπάρχει προστασία από τις ηλεκτρομαγνητικές παρεμβολές μεταξύ ηλεκτρικών αγωγών που βρίσκονται ο ένας δίπλα στον άλλο. Το ηλεκτρομαγνητικό πεδίο 2 καλωδίων τα οποία βρίσκονται το ένα δίπλα στο άλλο ακυρώνεται μιας και είναι αντίστροφο ενώ με την συστροφή επιτυγχάνεται ακόμα μεγαλύτερη ακύρωση. Στη συνέχεια τα 4 αυτά ζεύγη περικλείονται από ένα ακόμα στρώμα μόνωσης ώστε να κατασκευασθεί το τελικό καλώδιο. Το συγκεκριμένο καλώδιο ονομάζεται UTP (Unshielded Twisted Pair) εάν βασίζεται μόνο στην συστροφή για τη μείωση των ηλεκτρομαγνητικών παρεμβολών. Εάν τα συνεστραμμένα ζεύγη περιβάλλονται από ένα ακόμα μεταλλικό κέλυφος τότε το καλώδιο ονομάζεται STP (Shielded Twisted Pair).

Τα συγκεκριμένα καλώδια χωρίζονται επιπλέον σε κατηγορίες με βάση τη μόνωση τους και τις ταχύτητες που μπορούν να επιτευχθούν σε δεδομένες αποστάσεις. Οι πιο βασικές κατηγορίες είναι οι Category 3, Category 5, Category 5-e και Category 6. Η κατηγορία Cat3 χρησιμοποιήθηκε στην πρώτη έκδοση του Ethernet για ταχύτητες 10Mb/s. Η κατηγορία Cat5 διαδέχθηκε την Cat3 και μπορούσε να μεταφέρει ταχύτητες 10 και 100Mb/s ενώ μπορούσε να επιτευχθεί και ταχύτητα 1Gb/s. Την κατηγορία Cat5 ακολούθησε η κατηγορία Cat5E. Η συγκεκριμένη κατηγορία έχει τα ίδια φυσικά χαρακτηριστικά με την Cat5 αλλά έχει υψηλότερες προδιαγραφές κατασκευής. Αυτό έχει ως αποτέλεσμα να μπορεί να αποδώσει καλύτερα στις υψηλότερες συχνότητες και ταχύτητες. Η κατηγορία Cat6 έχει πιο πυκνά συνεστραμμένα ζεύγη καλωδίων με αποτέλεσμα να μειώνεται ακόμα περισσότερο η ηλεκτρομαγνητική παρεμβολή. Επιπλέον ανάμεσα στα καλώδια υπάρχει ένας πυρήνας φτιαγμένος από νάιλον ο οποίος προσδίδει στο καλώδιο περισσότερη αντοχή και στιβαρότητα ενώ μειώνει και αυτός τις ηλεκτρομαγνητικές παρεμβολές μεταξύ των ζευγών. Τα καλώδια Cat6 μπορούν να υποστηρίξουν μέχρι και 10Gb/s ταχύτητες επικοινωνίας αλλά αυτό μπορεί να γίνει σε αποστάσεις μέχρι 50 μέτρα.

(Ακροδέκτες 1.2.6)

Στα 2 άκρα των καλωδίων, ανεξάρτητα του τύπου τους χρησιμοποιούνται ακροδέκτες με την ονομασία RJ-45 (Registered Jack - 45) οι οποίοι είναι πλαστικοί ή μεταλλικοί ακροδέκτες οι οποίοι έχουν 8 pins. Η σειρά με την οποία θα συνδεθούν οι 8 αγωγοί του UTP ή STP καλωδίου με τον ακροδέκτη καθορίζεται

από 2 πρότυπα: το T-568A και T-568B. Η πιο διαδεδομένη σειρά σύνδεσης είναι η T-568B



Εικόνα 2: Πρότυπα Τερματισμού Καλωδίων [2]

(Ταχύτητες και Μέσα Επικοινωνίας 1.2.7)

Οι πιο κοινές ταχύτητες στις οποίες λειτουργεί ένα δίκτυο Ethernet είναι στα 10Mb/s, 100Mb/s και 1Gb/s με βάση τα πρότυπα 10BaseT, 100BaseT και 1000BaseT. Όλες οι υλοποιήσεις τύπου BaseT λειτουργούν πάνω από 4 συνεστραμμένα ζεύγη ενώ χρησιμοποιούν συνδέσμους 8P8C στις άκρες τους.

Στο Ethernet πάνω από συνεστραμμένα ζεύγη προβλέπεται επικοινωνία τόσο σε full duplex όσο και σε half duplex. Ακόμη τα 2 άκρα της σύνδεσης μπορούν να επικοινωνήσουν μεταξύ τους με σκοπό να διαπραγματευτούν αυτόματα την ταχύτητα της σύνδεσης πάνω από την οποία επιθυμούν να επικοινωνήσουν, μέσω της διαδικασίας του Auto Negotiation. Η διαπραγμάτευση της ταχύτητας σύνδεσης εισήχθη με το 100BaseT πρότυπο αλλά είναι και συμβατή με το 10BaseT. Στο πρότυπο 1000BaseT και πάνω, η αυτόματη διαπραγμάτευση της ταχύτητας σύνδεσης είναι υποχρεωτική.

Τα δίκτυα Ethernet μπορούν να υποστηρίξουν και αυξημένες ταχύτητες πάνω από συνεστραμμένα ζεύγη όπως είναι τα 2.5Gb/s μέσω του 2.5GBaseT και τα 10Gb/s μέσω του 10GBaseT.

Τέλος δίκτυα Ethernet μπορούν να υλοποιηθούν και πάνω από οπτικές ίνες, ιδιαιτέρως όταν είναι επιθυμητή η κάλυψη μεγάλων αποστάσεων. Στη συγκεκριμένη περίπτωση οι ταχύτητες που υποστηρίζονται είναι 1Gb/s, 10Gb/s, 25Gb/s, 40Gb/s, 100Gb/s, 200Gb/s και 400Gb/s με τη χρήση των αντίστοιχων προτύπων δημοσιευμένων από το IEEE.

Αναφορές Κεφαλαίου 1.3

1.
https://en.wikipedia.org/wiki/Ethernet_frame#/media/File:Ethernet_Type_II_Frame_format.svg

2.
https://networkengineering.stackexchange.com/questions/37995/what-is-the-reason-for-t568a-and-t568b-termination

ΚΕΦΑΛΑΙΟ 2 Σύγχρονες Τεχνολογίες Ασύρματης Πρόσβασης

(Ιστορικά Στοιχεία 2.1)

Η δημιουργία του προτύπου 802.11 ξεκίνησε το 1985, όταν το FCC, η επιτροπή τηλεπικοινωνιών των ΗΠΑ έδωσε το φάσμα των 2.4GHz για μη αδειοδοτημένη χρήση. Τότε ο Vic Hayes, ο οποίος ήταν μέλος της IEEE σε συνεργασία με τον Bruce Tuch, ο οποίος εργαζόταν στην Bell Labs, αποφάσισαν να δημιουργήσουν ένα πρότυπο ασύρματης τοπικής δικτύωσης. Έτσι σε συνεργασία με το IEEE δημιούργησαν τα πρώτα πρότυπα IEEE 802.11b και IEEE 802.11a. Από τότε τα συγκεκριμένο πρότυπο αλλά και οι αλλαγές και προσθήκες σε αυτό ελέγχονται από το IEEE. Η πρώτη έκδοση δημοσιεύθηκε το 1997. Η εμπορική ονομασία του συγκεκριμένου προτύπου ήταν WiFi. Το 1999 δημιουργήθηκε το WiFi Alliance με σκοπό να διαχειριστεί το κατοχυρωμένο όνομα WiFi κάτω από την οποία πωλούνται τα περισσότερα προϊόντα που χρησιμοποιούν το συγκεκριμένο πρότυπο.

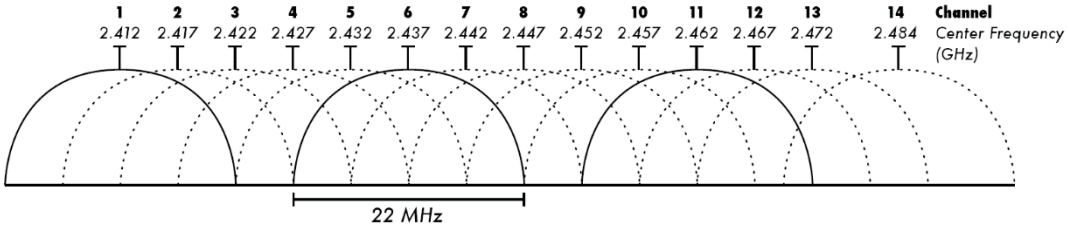
(Περιγραφή του Προτύπου 802.11 2.2)

Στο πρότυπο 802.11 η επικοινωνία είναι half-duplex και γίνεται ασύρματα. Χρησιμοποιείται τεχνολογία πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance). Έτσι ο εξοπλισμός ελέγχει στο κανάλι αν εκπέμπει κάποιος άλλος χρήστης πριν εκπέμψει ο ίδιος.

(Συχνότητες και Κανάλια 2.2.1)

Οι συχνότητες που χρησιμοποιούνται από την οικογένεια πρωτοκόλλων 802.11 είναι οι 2.4GHz και 5GHz. Η τελευταία προσθήκη στην οικογένεια αυτή, το 802.11ax μπορεί να χρησιμοποιήσει και την συχνότητα των 6GHz. Σε αυτές τις συχνότητες μπορεί να γίνει εκπομπή χωρίς να είναι αναγκαία η λήψη άδειας από κάποιο ρυθμιστικό φορέα.

Το φάσμα των 2.4GHz είναι χωρισμένο σε 11 ή 13 κανάλια ανάλογα με την χώρα στην οποία λειτουργεί. Κάθε κανάλι έχει πλάτος 20 MHz. Ωστόσο τα 11 αυτά κανάλια συμπίπτουν το ένα με το άλλο εκτός από τα κανάλια 1, 6 και 11 τα οποία δεν έχουν κοινές συχνότητες με κάποιο άλλο κανάλι. Επιπλέον στις συγκεκριμένες συχνότητες λειτουργούν και άλλα πρωτόκολλα και συσκευές που εκμεταλλεύονται την μη-αδειοδοτήσιμη φύση του συγκεκριμένου φάσματος. Τέτοιες μπορεί να είναι οι συσκευές που κάνουν χρήση του πρωτοκόλλου Bluetooth καθώς και οι φούρνοι μικροκυμάτων και τα ασύρματα τηλέφωνα.



Εικόνα 3: Διαχωρισμός του Φάσματος των 2.4GHz σε κανάλια [3]

Ως μια προσπάθεια για την επίλυση των παρεμβολών που προκαλούνται από την κοινή χρήση του συγκεκριμένου φάσματος είναι η χρήση της συχνότητας 5GHz. Το συγκεκριμένο φάσμα συχνοτήτων χωρίζεται σε 23 κανάλια με πλάτος 20MHz το κάθε ένα. Στα 5 GHz τα κανάλια δεν έχουν κοινές συχνότητες το ένα με το άλλο.

Ασύρματα Δίκτυα 802.11 2.3

(802.11 Legacy 2.3.1)

Το πρώτο πρωτόκολλο που εντάχθηκε στην οικογένεια του 802.11 ήταν το 802.11 legacy. Το συγκεκριμένο πρωτόκολλο μπορούσε να λειτουργήσει σε συχνότητες 1Mb/s και 2Mb/s. Χρησιμοποιούσε τεχνολογία Direct Sequence Spread Spectrum (DSSS) για την κωδικοποίηση των πλαισίων. Γρήγορα αντικαταστάθηκε με το 802.11b.

(802.11b 2.3.2)

Το πρωτόκολλο 802.11b είναι μια επέκταση των δυνατοτήτων του αρχικού 802.11 legacy πρωτοκόλλου, χρησιμοποιεί τον ίδιο τρόπο πρόσβασης στο μέσο και δημοσιεύθηκε ως πρότυπο το 1999. Μπορεί να επιτύχει ταχύτητες στο φυσικό επίπεδο μέχρι και 11Mb/s. Η ραγδαία αύξηση της ταχύτητας που προσέφερε το συγκεκριμένο πρωτόκολλο οδήγησε στην προτίμηση του από τους κατασκευαστές και στην αντικατάσταση του 802.11 legacy από αυτό.

(802.11g 2.3.3)

Το πρωτόκολλο 802.11g δημιουργήθηκε το 2003. Μπορεί να επιτύχει ταχύτητες στο φυσικό μέσο μέχρι και 54Mb/s. Για την κωδικοποίηση των πλαισίων στο φυσικό μέσο χρησιμοποιεί Orthogonal Frequency Division Multiplexing. Οι ασύρματες διεπαφές που υποστηρίζουν 802.11g είναι συμβατές και με το πρωτόκολλο 802.11b με αποτέλεσμα στο ίδιο δίκτυο να μπορούν να συνυπάρχουν συσκευές που υποστηρίζουν το ένα από τα 2 πρωτόκολλα. Κάτι τέτοιο όμως μειώνει κατά πολύ την ταχύτητα που μπορεί να επιτευχθεί στο φυσικό μέσο.

(802.11n 2.3.4)

Το πρωτόκολλο 802.11n δημοσιεύθηκε το 2006 αλλά αναγνωρίστηκε επίσημα από το IEEE το 2009. Ενώ τα προηγούμενα πρωτόκολλα, 802.11b, 802.11g και 802.11n χρησιμοποιούσαν μόνο το φάσμα των 2.4GHz για την επικοινωνία μεταξύ των συσκευών το πρωτόκολλο 802.11n μπορεί να χρησιμοποιήσει τόσο τα 2.4GHz όσο και τα 5GHz. Η ταχύτητα που μπορεί να επιτευχθεί με το συγκεκριμένο πρωτόκολλο στο φυσικό επίπεδο κυμαίνεται από 54Mb/s έως 600Mb/s. Το 802.11n εισήγαγε την δυνατότητα να χρησιμοποιηθεί η τεχνολογία MIMO (Multiple In Multiple Out) η οποία επιτρέπει να υπάρχουν πολλαπλά streams μεταξύ του σταθμού βάσης και της συσκευής και αυξάνει την ταχύτητα της σύνδεσης.

(802.11ac 2.3.5)

Το πρωτόκολλο 802.11ac δημοσιεύθηκε το 2013 και είναι μια εξέλιξη του πρωτοκόλλου 802.11v. Αρχικά χρησιμοποιεί μόνο το φάσμα των 5GHz. Μπορεί να υποστηρίξει πλάτος καναλιού 80MHz και 160MHz επιπλέων των 20MHz, περισσότερες ροές δεδομένων (streams) όταν γίνεται χρήση της τεχνολογίας Multiple In Multiple Out (MIMO) και βελτιωμένη κωδικοποίηση Orthogonal Frequency Division Multiplexing (OFDM). Ακόμη προστέθηκε η δυνατότητα χρήσης της τεχνολογίας Multi User – Multiple In Multiple Out (MU-MIMO) όπου πολλαπλές συσκευές μπορούν να επικοινωνούν την ίδια στιγμή με τον σταθμό βάσης αντί για μία κάθε φορά.

(802.11ax 2.3.6)

Η τελευταία έκδοση της οικογένειας πρωτοκόλλων 802.11 είναι η 802.11ax. Αναγνωρίστηκε από το IEEE το 2021 παρότι η ενσωμάτωση του σε σταθμούς βάσης και συσκευές ξεκίνησε νωρίτερα. Το συγκεκριμένο πρωτόκολλο πέρα από το φάσμα συχνοτήτων των 2.4GHz και 5GHz μπορεί να χρησιμοποιήσει και το φάσμα των 6GHz για την επικοινωνία μεταξύ των συσκευών. Έχουν ενσωματωθεί σε αυτό βελτιώσεις ώστε να αυξηθεί η απόδοση των ασύρματων δικτύων σε συνθήκες μεγάλου πλήθους συσκευών (High Density Environments), επιτυγχάνοντας έτσι τετραπλάσια απόδοση σε σχέση με το 802.11ac.

Πλαίσια 802.11 2.4)

Κάθε πακέτο των πρωτοκόλλων της οικογένειας 802.11 ονομάζεται πλαίσιο. Το πλαίσιο αποτελείται από συγκεκριμένα πεδία τα οποία είναι η κεφαλίδα MAC (Media Access Control), ο χώρος του payload στον οποίο αποθηκεύονται τα δεδομένα που μεταφέρονται και το πεδίο Frame Check Sequence το οποίο χρησιμοποιείται για την ανίχνευση και την διόρθωση λαθών.

Τα πρώτα 2 bytes της κεφαλίδας περιγράφουν τον τύπο και τη λειτουργία του πλαισίου και περιλαμβάνουν πληροφορίες για την έκδοση του πρωτοκόλλου, τον τύπο του πλαισίου, αν είναι δηλαδή πλαίσιο Ελέγχου (Control), Δεδομένων (Data) ή Διαχείρισης (Management), την ύπαρξη ή όχι επανάληψης στην εκπομπή του, bits διαχείρισης ενέργειας σε περίπτωση που η τελική συσκευή έχει ολοκληρώσει την εκπομπή της και επιθυμεί να μπει σε λειτουργία χαμηλότερης κατανάλωσης ενέργειας, εάν τα πλαίσια είναι κρυπτογραφημένα και την σειρά των πλαισίων. Στην συνέχεια η κεφαλίδα περιέχει δεδομένα για το τι μέγεθος έχει το πλαίσιο, ώστε οι υπόλοιπες συσκευές να γνωρίζουν πότε θα είναι το κανάλι ξανά διαθέσιμο για εκπομπή. Ακολουθούν οι διευθύνσεις Media Access Control (MAC) του αποστολέα και του παραλήπτη, ενώ το πλαίσιο ολοκληρώνεται με το πεδίο που περιγράφει την σειρά των πακέτων ώστε να μην υπάρξουν διπλότυπα πακέτα.

Στην συνέχεια ακολουθεί ο χώρος που αποθηκεύονται τα δεδομένα προς μεταφορά (payload) και το πεδίο ελέγχου σφάλματος στα δεδομένα όπως προαναφέρθηκε.

(Πλαίσια Διαχείρισης (Management Frames) 2.4.1)

Δεν είναι απαραίτητο όλα τα πλαίσια να περιέχουν δεδομένα προς μεταφορά. Κάποια πλαίσια χρησιμοποιούνται για τη διαχείριση της ασύρματης σύνδεσης μεταξύ του σταθμού βάσης και της συσκευής του τελικού χρήστη και ονομάζονται πλαίσια Διαχείρισης (Management Frames). Οι λειτουργίες που επιτελούν τα συγκεκριμένα πλαίσια είναι λειτουργίες πιστοποίησης μεταξύ του σταθμού βάσης και της συσκευής (Authentication Frames), αιτημάτων διαφήμισης της ύπαρξης του συγκεκριμένου σταθμού βάσης (Beacon Frames) και σύνδεσης του σταθμού βάσης και της συσκευής (Association Request/Response Frames). Ακόμη υπάρχουν πλαίσια για την αποσύνδεση της συσκευής από τον σταθμό βάσης (Disassociation Frame και Deauthentication Frame). Τέλος υπάρχουν πλαίσια που χρησιμοποιούνται από τους σταθμούς για την αποστολή ερωτημάτων προς άλλες συσκευές όπως για τις δυνατότητες τους και τις υποστηριζόμενες ταχύτητες επικοινωνίας (Probe Request Frame και Probe Response Frame) καθώς και πλαίσια που αποστέλλονται από την συσκευή για την επανασύνδεση με κάποιο σταθμό βάσης (Reassociation Request Frame και Reassociation Response Frame).

(Πλαίσια Ελέγχου (Control Frames) 2.4.2)

Για τον συντονισμό της επικοινωνίας μεταξύ του σταθμού βάσης και των τελικών συσκευών υπάρχει μια ομάδα πλαισίων που αποστέλλονται και ονομάζονται πλαίσια Ελέγχου (Control Frames). Τα συγκεκριμένα πλαίσια είναι τα πλαίσια αποδοχής (Acknowledgement Frames), τα οποία αποστέλλονται μόλις η συσκευή λάβει ένα πλαίσιο με σκοπό την ενημέρωση του σταθμού βάσης ότι η μετάδοση ήταν επιτυχής, τα πλαίσια αιτήματος επικοινωνίας (Request To Send Frames), στα οποία η συσκευή πριν αποστείλει ένα πλαίσιο δεδομένων «ρωτάει» τον σταθμό βάσης εάν το κανάλι είναι καθαρό και μπορεί να εκπέμψει. Η συγκεκριμένη ενέργεια γίνεται με σκοπό να αποφευχθούν οι συγκρούσεις. Τέλος υπάρχει τα πλαίσια ενημέρωσης για δυνατότητα επικοινωνίας (Clear To Send

Frames) τα οποία εκπέμπονται ως απάντηση στα πλαίσια αιτήματος για επικοινωνία και ενημερώνουν την συσκευή ότι μπορεί να εκπέμψει και για πόσο χρόνο μπορεί να το κάνει αυτό, ενώ παράλληλα ενημερώνει και όλες τις υπόλοιπες συσκευές στο ίδιο δίκτυο να μην εκπέμψουν για την ίδια χρονική διάρκεια.

(Πλαίσια Δεδομένων (Data Frames) 2.4.3)

Τα πλαίσια δεδομένων μεταφέρουν πακέτα των διαφόρων πρωτοκόλλων που λειτουργούν σε υψηλότερα επίπεδα της ιεραρχίας του OSI όπως είναι το πρωτόκολλο TCP και UDP. Τα συγκεκριμένα πλαίσια περιλαμβάνουν την κεφαλίδα και στο κύριο μέρος ένα πεδίο Destination Service Access Point (DSAP) το οποίο περιγράφει το πρωτόκολλο που μεταφέρεται και ένα πεδίο με την ονομασία Subnetwork Access Protocol (SNAP).

Πιστοποίηση και Κρυπτογράφηση της Σύνδεσης 2.5)

Κατά την εγκαθίδρυση της σύνδεσης ανάμεσα στον σταθμό βάσης και τις συσκευές που απαρτίζουν το ασύρματο δίκτυο WiFi αλλά και κατά τη διάρκεια της σύνδεσης, εάν τα πακέτα δεν χρησιμοποιούν κάποιο είδος κρυπτογράφησης, τότε κάποιος τρίτος μπορεί να λάβει τα πλαίσια που εκπέμπονται και να υποκλέψει τις πληροφορίες που μεταδίδονται. Επιπλέον, ενώ κατά τη χρήση ενσύρματων δικτύων, κάποια συσκευή για να μπορεί να έχει πρόσβαση στο δίκτυο θα έπρεπε να βρίσκεται στο εσωτερικό του κτηρίου και κοντά σε μία θύρα Ethernet, στα ασύρματα δίκτυα, μία συσκευή αρκεί να βρίσκεται εντός της εμβέλειας του ασύρματου δικτύου για να μπορεί να έχει πρόσβαση σε αυτό. Αυτό έχει ως αποτέλεσμα μια παράνομη πρόσβαση να μη μπορεί να γίνει εύκολα αντιληπτή. Για αυτούς τους λόγους και με σκοπό τη δυνατότητα ελέγχου πρόσβασης των συσκευών στο δίκτυο αλλά και προστασίας των δεδομένων που μεταφέρονται μέσω αυτού, στα ασύρματα δίκτυα 802.11 υπάρχει η δυνατότητα πιστοποίησης των χρηστών και κρυπτογράφησης της σύνδεσης τους. Έτσι, με βάση το πρωτόκολλο πιστοποίησης και κρυπτογράφησης που χρησιμοποιούν τα ασύρματα δίκτυα WiFi χωρίζονται σε δίκτυα χωρίς πιστοποίηση και κρυπτογράφηση, δίκτυα με χρήση Wired Equivalent Privacy (WEP), δίκτυα με χρήση WiFi Protected Access (WPA), WiFi Protected Access II (WPA2) και WiFi Protected Access III (WPA3).

(Wired Equivalent Privacy (WEP) 2.5.1)

Ο αλγόριθμος WEP εισήχθη μαζί με το αρχικό πρωτόκολλο 802.11 το 1997 με την ιδέα να παρέχει προστασία στα δεδομένα ίδια με αυτή ενός ενσύρματου δικτύου. Το κλειδί του έχει μήκος 40 bits ή 104 bits. Ωστόσο και οι συσκευές που υποστηρίζουν το πρωτόκολλο 802.11b έχουν το WEP ως τον μόνο υποστηριζόμενο αλγόριθμο προστασίας των δεδομένων που μεταδίδονταν. Το WEP πραγματοποιεί κρυπτογράφηση με τη χρήση του Stream Cipher RC4.

Η διαδικασία της ταυτοποίησης και κρυπτογράφησης των δεδομένων μπορεί να γίνει με δύο τρόπους: Στον πρώτο τρόπο που ονομάζεται «Open System Authentication» η συσκευή που επιθυμεί να συνδεθεί στον σταθμό βάσης δεν παρέχει τα στοιχεία πρόσβασης σε αυτόν. Αντιθέτως συνδέεται απευθείας χωρίς να γίνεται κάποια απόπειρα πιστοποίησης και το WEP κλειδί χρησιμοποιείται για την κρυπτογράφηση των πλαισίων. Έτσι η συσκευή πρέπει να έχει το σωστό κλειδί για να γίνει εφικτή η επικοινωνία με τον σταθμό βάσης.

Στον δεύτερο τρόπο, ο οποίος ονομάζεται «Shared Key authentication», η διαδικασία της ταυτοποίησης γίνεται με την συσκευή που επιθυμεί να συνδεθεί στο σταθμό βάσης να στέλνει το αίτημα της για σύνδεση, ο σταθμός βάσης να απαντά με ένα σύνολο δεδομένων τα οποία η συσκευή θα πρέπει να κρυπτογραφήσει με το προρυθμισμένο κλειδί και να τα αποστείλει πίσω στον σταθμό βάσης. Ο σταθμός βάσης αποκρυπτογραφεί τα δεδομένα με το ίδιο κλειδί και αν τα δεδομένα είναι ίδια με αυτά που απέστειλε στην συσκευή, τότε επιτρέπει στην συσκευή να συνδεθεί. Η συγκεκριμένη διαδικασία ονομάζεται Challenge-Response Authentication. Στην συνέχεια το ίδιο κλειδί χρησιμοποιείται και για την κρυπτογράφηση των πλαισίων με τη χρήση του RC4 Stream Cipher, όπως αναφέρθηκε και προηγουμένως.

Ωστόσο, το 2001 δημοσιεύθηκε[2] η πρώτη επίθεση ενάντια στον WEP αλγόριθμο από τον Scott Fluhrer, Itsik Mantin και Adi Shamir, λόγω αδυναμίας στον τρόπο που εκτελείται η κρυπτογράφηση με τη χρήση του RC4 Stream Cipher, όπου ανάλογα και την κίνηση στο δίκτυο το κλειδί μπορούσε να βρεθεί ακόμα και μέσα σε ένα λεπτό. Ακόμη το 2006 δημοσιεύθηκαν περαιτέρω παρατηρήσεις για τις ευπάθειες της εφαρμογής του RC4 Stream Cipher από τον Andreas Klein[3]. Τα επόμενα χρόνια περαιτέρω ευπάθειες που ανακαλύφθηκαν στην εφαρμογή του πρωτοκόλλου οδήγησαν στην απαξίωση του συγκεκριμένου αλγορίθμου και την προτροπή στη χρήση νέων πιο ασφαλών αλγορίθμων όπως είναι ο WPA και WPA2.

(WiFi Protected Access (WPA) 2.5.2)

Με σκοπό την επίλυση των προβλημάτων που δημιουργήθηκαν από την ελλιπή ασφάλεια του αλγορίθμου WEP το WiFi Alliance δημοσίευσε το 2003 τον αλγόριθμο WPA. Ο αλγόριθμος WPA θα ήταν ένα ενδιάμεσο στάδιο μέχρι τη δημοσίευση του αλγορίθμου WPA2 ή 802.11i από το IEEE. Το WPA χρησιμοποιεί για την πιστοποίηση των συσκευών και την κρυπτογράφηση των πακέτων το Temporal Key Integrity Protocol (TKIP) το οποίο κάνει χρήση του RC4 cipher για την κρυπτογράφηση των δεδομένων. Το μέγεθος των κλειδιών μπορεί να είναι 64bit ή 128 bit. Σε αντίθεση με το WEP το κλειδί κρυπτογράφησης των πλαισίων δεν παραμένει το ίδιο αλλά για κάθε πλαίσιο δημιουργείται ένα νέο κλειδί, αποφεύγοντας έτσι τις ευπάθειες του WEP αλγορίθμου.

Παράλληλα με σκοπό την αποφυγή της τροποποίησης και στην συνέχεια αποστολής πακέτων από κάποιο επιτιθέμενο το WPA περιλαμβάνει έναν έλεγχο

[2] Fluhrer, Scott; Mantin, Itsik; Shamir, Adi (2001). "Weaknesses in the Key Scheduling Algorithm of RC4"

[3] Andreas Klein (2005). "Attacks on the RC4 Stream Cipher"

της ακεραιότητας του μηνύματος (Message Integrity Check), το οποίο και αντικαθιστά τον Cyclic Redundancy Check, τον έλεγχο ακεραιότητας μηνύματος που χρησιμοποιούσε το WEP και αποδείχθηκε ανεπαρκής. Το WPA χρησιμοποιεί το Temporal Key Integrity Protocol (TKIP) με σκοπό την εκτέλεση αυτού του ελέγχου ακεραιότητας.

(WiFi Protected Access II (WPA2) 2.5.3)

Το 2004 δημοσιεύθηκε από το IEEE[4] ο αλγόριθμος WiFi Protected Access II (WPA2) με σκοπό και επίσημα την αντικατάσταση του επισφαλούς αλγορίθμου WEP. Επιπλέον, ενίσχυσε τις δυνατότητες και την ασφάλεια του WPA αλγορίθμου ο οποίος είχε δημοσιευθεί από το WiFi Alliance ως μια προσωρινή λύση μέχρι την τελική δημοσίευση του WPA2.

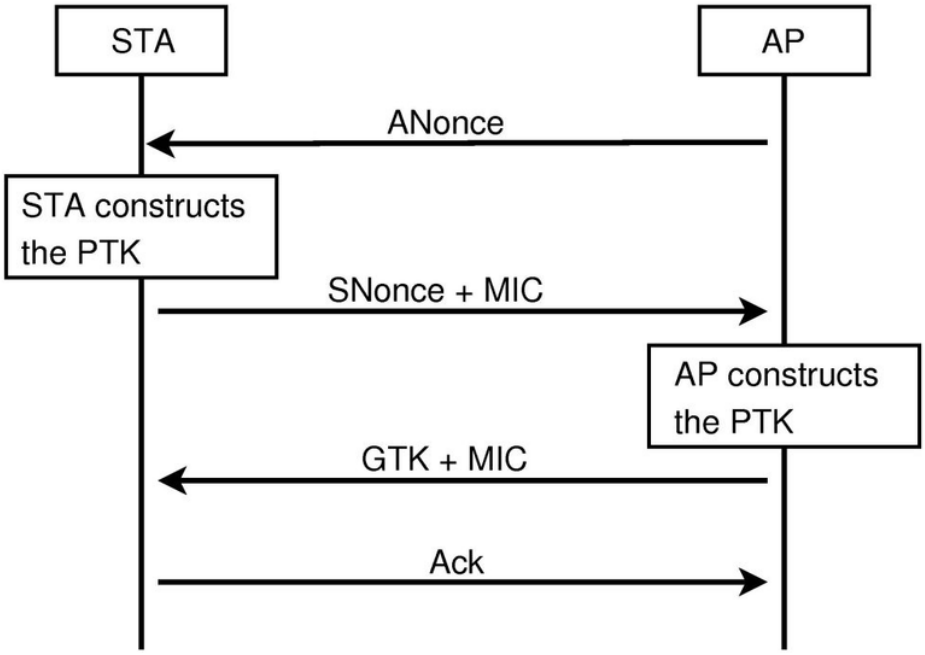
Για την κρυπτογράφηση των δεδομένων, την ταυτοποίηση των συσκευών και τον έλεγχο της ακεραιότητας των δεδομένων ο αλγόριθμος WPA2 χρησιμοποιεί το Temporal Key Integrity Protocol, το οποίο και αναλύθηκε στην προηγούμενη ενότητα και το Counter Mode Cipher Block Chaining Message Authentication Code Protocol, γνωστό εν συντομία ως CCMP. Το CCMP βασίζεται στον αλγόριθμο AES για την κρυπτογράφηση των δεδομένων και χρησιμοποιεί κλειδιά κρυπτογράφησης μήκους 128 bit.

Η διαδικασία επικοινωνίας και εγκαθίδρυσης σύνδεσης μεταξύ της συσκευής και του σταθμού βάσης γίνεται με τη χρήσης μιας «Τετραπλής Χειραψίας» (4-way handshake). Αρχικά η πιστοποίηση της συσκευής γίνεται είτε με ένα κλειδί το οποίο έχει ρυθμιστεί τόσο στον σταθμό βάσης όσο και στην συσκευή, είτε με τη χρήση του πρωτοκόλλου 802.1x το οποίο περιλαμβάνει όνομα χρήστη και κωδικό ή και πιστοποιητικά βασισμένα σε υποδομή δημοσίου και ιδιωτικού κλειδιού. Μετά από οποιαδήποτε από αυτές τις 2 διαδικασίες, δημιουργείται ένα νέο κλειδί το οποίο είναι γνωστό και από τη συσκευή αλλά και από τον σταθμό βάσης. Το συγκεκριμένο κλειδί μετέπειτα παραμένει σταθερό καθ' όλη τη διάρκεια της σύνδεσης ενώ για την κρυπτογράφηση των πλαισίων δημιουργούνται νέα κλειδιά τα οποία πηγάζουν από αυτό το αρχικό κλειδί.

Για τη δημιουργία αυτών των νέων κλειδιών κρυπτογράφησης χρησιμοποιείται η Τετραπλή Χειραψία που αναφέρθηκε προηγουμένως. Τα συγκεκριμένα κλειδιά χρησιμοποιούνται για την κρυπτογράφηση κίνησης με συγκεκριμένο παραλήπτη (Unicast Traffic) και ονομάζονται Pairwise Transient Keys (PTK). Για την κρυπτογράφηση κίνησης που απευθύνεται σε παραπάνω από ένα παραλήπτες (Broadcast Traffic και Multicast Traffic) χρησιμοποιείται ένα κλειδί με την ονομασία Group Temporal Key.

Όταν μια συσκευή αποσυνδεθεί από τον σταθμό βάσης, το Group Temporal Key θα πρέπει να αλλάξει σε συντονισμό με όλες τις υπόλοιπες συσκευές του δικτύου. Ο λόγος που γίνεται αυτό είναι για να μη μπορεί η συσκευή που έχει πια αποσυνδεθεί να αποκρυπτογραφήσει την κίνηση τύπου Broadcast και Multicast.

[4] "IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements"



Εικόνα 4: 4-way Handshake [4]

(WiFi Protected Access III (WPA3) 2.5.4)

Το 2018, το WiFi Alliance ανακοίνωσε την αντικατάσταση του WPA2 από το WiFi Protected Access III (WPA3). Οι βελτιώσεις που επέφερε η συγκεκριμένη αναβάθμιση ήταν πολλαπλές.

Αρχικά τα πλαίσια Διαχείρισης (Management Frames) είναι πια κρυπτογραφημένα με αποτέλεσμα να μη μπορούν να πλαστογραφηθούν από κάποιον τρίτο. Επιπλέον βελτιώθηκε η διαδικασία ανταλλαγής κλειδιών μεταξύ του σταθμού βάσης και της συσκευής με την οποία γίνεται η επικοινωνία. Τέλος ενισχύθηκε η ασφάλεια της κρυπτογραφημένης σύνδεσης καθιστώντας απαραίτητη προϋπόθεση τη χρήση κλειδιών μεγαλύτερου μήκους από το WPA2 και πιο συγκεκριμένα 192 bit εάν γίνεται χρήση της διαδικασίας πιστοποίησης WPA3-Enterprise και τουλάχιστον 128 bit αν γίνεται χρήση της διαδικασίας πιστοποίησης WPA3-Personal.

Ακόμη το WPA3 έφερε και περιορισμό των προσωπικών δεδομένων που μπορεί να διαρρεύσουν. Πιο συγκεκριμένα κάθε συσκευή που υποστηρίζει το WPA3 πρωτόκολλο είναι υποχρεωμένη να δημιουργεί ξεχωριστή διεύθυνση MAC για τη δικτυακή διεπαφή της εκτός και αν ο χρήστης επιλέξει συνειδητά να μη γίνει κάτι τέτοιο. Αυτό αποτρέπει την παρακολούθηση των κινήσεων μιας συσκευής κατά τη διάρκεια του χρόνου μέσω του συσχετισμού των κοινών διευθύνσεων MAC που συνδέθηκαν σε πολλαπλούς διαφορετικά σημεία πρόσβασης (BSSIDs).

Τρόποι Λειτουργίας 2.6

(Infrastructure Mode 2.6.1)

Στην περίπτωση του Infrastructure Mode υπάρχει ένα σύνολο από συσκευές το οποίο συνδέεται στο δίκτυο μέσω ενός σταθμού βάσης, που είναι γνωστός με την ονομασία «Σημείο Πρόσβασης» (Access Point). Σε αυτή την περίπτωση, ο σταθμός βάσης είναι συνδεδεμένος με το υπόλοιπο δίκτυο του κτηρίου μέσω καλωδίου. Η θέση των Σταθμών Βάσης παραμένει σταθερή, συνήθως σε υψηλά σημεία, με σκοπό το βέλτιστο σήμα από και προς τις συσκευές. Εάν έχουμε παραπάνω από ένα σημείο πρόσβασης, τοπολογία η οποία θα αναλυθεί παρακάτω τότε το λογισμικό της συσκευής επιλέγει να συνδεθεί στο σημείο πρόσβασης με το βέλτιστο σήμα.

(Ad-Hoc Mode 2.6.2)

Στην περίπτωση του Ad-Hoc Mode, δεν υπάρχει κάποιος σταθμός βάσης, Αντιθέτως οι συνδέσεις είναι τύπου peer-to-peer, δηλαδή κάθε συσκευή συνδέεται απευθείας με μία ή περισσότερες άλλες συσκευές, Για να λειτουργήσει η συγκεκριμένη τοπολογία πρέπει οι συσκευές να βρίσκονται σε κοντινή απόσταση. Αυτό απαιτείται ώστε να υπάρχει επαρκές σήμα για τη μεταξύ τους επικοινωνία αλλά και για να μπορεί να λειτουργήσει ο αλγόριθμος πρόσβασης στο μέσο με αποφυγή συγκρούσεων (CSMA/CA).[5] Αδυναμία μιας συσκευής να αντιληφθεί την εκπομπή της άλλης λόγω ασθενούς σήματος μπορεί να οδηγήσει σε ταυτόχρονη εκπομπή και άρα σε σύγκρουση.

(Wireless Distribution System (WDS) 2.6.3)

Κατά τη χρήση του Wireless Distribution System (WDS) είναι εφικτό πολλαπλοί σταθμοί βάσης ενός ασύρματου δικτύου WiFi να συνδεθούν μεταξύ τους ασύρματα, χωρίς να χρειάζεται η ύπαρξη κάποιας καλωδιακής υποδομής από πίσω. Επιπλέον, η σύνδεση αυτή είναι τελείως διάφανη για τις τελικές συσκευές με αποτέλεσμα οι MAC διευθύνσεις των 802.11 πλαισίων να μπορούν να παραμείνουν άθικτες. Σε μια τοπολογία WDS κάθε σταθμός βάσης μπορεί να έχει τρεις ρόλους. Έτσι μπορεί να είναι ο «κύριος σταθμός» (Main Base Station) ο οποίος αναλαμβάνει τον ρόλο να διασυνδέσει το σύστημα WDS με το ενσύρματο δίκτυο Ethernet, ο «Σταθμός Αναμετάδοσης» (Relay Base Station) ο οποίος έχει τον ρόλο του αναμεταδότη δεδομένων μεταξύ απομακρυσμένων σταθμών βάσης, αναμεταδοτών σταθμών βάσης και συσκευών του ασύρματου δικτύου και τέλος ο «Απομακρυσμένος Σταθμός» (Remote Base Station), ο οποίος έχει τον ρόλο του να διασυνδέει τις συσκευές με τους άλλους σταθμούς αναμετάδοσης αλλά και κύριους σταθμούς. Για την επικοινωνία μεταξύ των σταθμών βάσης μπορεί να γίνει χρήση κρυπτογράφησης με τους αλγόριθμους WEP, WPA και WPA2. Το βασικό

[5] CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

μειονέκτημα της συγκεκριμένης τεχνολογίας είναι ότι η ταχύτητα μετάδοσης δεδομένων μειώνεται στο μισό κάθε φορά που τα πλαίσια περνούν από ένα σταθμό βάσης. Ο λόγος που συμβαίνει αυτό είναι γιατί το WiFi είναι μια half duplex τεχνολογία και αυτό σημαίνει ότι ο σταθμός βάσης μπορεί μόνο το μισό χρόνο να λαμβάνει και τον άλλο μισό χρόνο να εκπέμπει.

Ονοματοδοσία Ασύρματου Δικτύου 2.7

Με σκοπό τον διαχωρισμό ενός ασύρματου δικτύου WiFi από άλλα ασύρματα δίκτυα είναι επιθυμητή η ονοματοδοσία του. Το όνομα του ασύρματου δικτύου προκύπτει από ένα μοναδικό αναγνωριστικό που έχει κάθε ασύρματο δίκτυο 802.11 και ονομάζεται Service Set Identifier (SSID) ή Extended Service Set Identifier (ESSID). Το συγκεκριμένο αναγνωριστικό μεταδίδεται ανά τακτά χρονικά διαστήματα από τους σταθμούς βάσης με σκοπό να ανακοινώσουν την ύπαρξη τους. Το μέγεθος τους μπορεί να είναι από 0 έως 32 bytes. Η κωδικοποίηση των χαρακτήρων είναι UTF-8 και αυτό σημαίνει ότι εκτός από χαρακτήρες το SSID μπορεί να περιλαμβάνει και σύμβολα. Όπως αναφέρθηκε, είναι εφικτό το SSID να μην περιέχει κανένα χαρακτήρα και να έχει μηδενικό μήκος. Στη συγκεκριμένη περίπτωση το ασύρματο δίκτυο δεν εμφανίζεται στη λίστα με τα διαθέσιμα για σύνδεση SSIDs μιας συσκευής και ονομάζεται Hidden SSID. Επιπλέον υπάρχει ένα ακόμα αναγνωριστικό το οποίο είναι μοναδικό μεταξύ σταθμών βάσεων ακόμα και αν το SSID είναι κοινό το οποίο είναι το Basic Service Set Identifier (BSSID). Το συγκεκριμένο αναγνωριστικό αντιστοιχεί με την διεύθυνση MAC της ασύρματης δικτυακής διεπαφής του σταθμού βάσης.

Πολλαπλά Σημεία Πρόσβασης (Extended Service Set) 2.8

Συχνά, σε μεγάλες εγκαταστάσεις ασύρματων δικτύων WiFi, παρατηρείται ότι ένας σταθμός βάσης και μόνο δεν είναι επαρκής για την κάλυψη των αναγκών σε στάθμη σήματος και άρα ποιότητας σύνδεσης για το σύνολο των συσκευών που είναι επιθυμητό να συνδεθούν στο συγκεκριμένο ασύρματο δίκτυο. Συχνά μάλιστα, ένας σταθμός βάσης δεν είναι επαρκής για να εξυπηρετήσει πάνω από συγκεκριμένο αριθμό συσκευών πελατών.

Για αυτό το λόγο χρησιμοποιούνται περισσότεροι από ένα σταθμοί βάσης οι οποίοι εκπέμπουν το ίδιο SSID. Έτσι για τις συσκευές που θα συνδεθούν στο ασύρματο δίκτυο, το δίκτυο φαίνεται ως ένα ενιαίο σύστημα με το ίδιο όνομα και οι συσκευές μπορούν να μετακινηθούν μεταξύ των σταθμών βάσης χωρίς να υπάρξει διακοπή στις υπηρεσίες που τους παρέχονται ή ανάγκη για επανάληψη της ταυτοποίησης των χρηστών. Οι σταθμοί βάσης παρέχουν πρόσβαση στο ίδιο υποδίκτυο και παρότι μια συσκευή μπορεί να κινείται μεταξύ των σταθμών βάσεων διατηρεί την πρόσβαση της στο λογικό επίπεδο (Επίπεδο 2) της ιεραρχίας OSI.

Με σκοπό την επίτευξη της αδιάκοπης επικοινωνίας κατά την διαδικασία της περιαγωγής από σταθμό σε σταθμό έχουν δημοσιευθεί από τον IEEE κάποια

πρότυπα στην οικογένεια 802.11 τα οποία και διευκολύνουν την συγκεκριμένη διαδικασία. Τα πρότυπα αυτά είναι το 802.11k, 802.11r και 802.11v.

(802.11k 2.8.1)

Το 802.11k είναι δημοσιεύθηκε από το IEEE το 2008. Με τη χρήση του συγκεκριμένου προτύπου, ο σταθμός βάσης παρέχει πληροφορίες στις συσκευές που είναι συνδεδεμένες σε αυτό για τους γειτονικούς σταθμούς βάσης που είναι διαθέσιμοι και πιο συγκεκριμένα τη διεύθυνση του σταθμού βάσης και το κανάλι στο οποίο αυτός ο σταθμός εκπέμπει. Λαμβάνοντας υπόψη αυτές τις πληροφορίες, η συσκευή μπορεί να πραγματοποιήσει την περιαγωγή από ένα σταθμό σε ένα άλλο πιο γρήγορα καθώς έχει μια συγκεκριμένη λίστα σταθμών στην οποία θα επιχειρήσει να συνδεθεί και δεν θα πρέπει να τους αναζητήσει πρώτα. Η εκπομπή της συγκεκριμένης ενημερωτικής πληροφορίας γίνεται όταν ο σταθμός βάσης αντιληφθεί πως η συσκευή απομακρύνεται από αυτόν λόγω της πτώσης στάθμης του σήματος. Εκεί ενημερώνει την συσκευή να προετοιμαστεί για την περιαγωγή σε έναν νέο σταθμό βάσης. Η συσκευή ζητάει μια λίστα από διαθέσιμους σταθμούς βάσης την οποία και παρέχει ο σταθμός βάσης στον οποίο είναι ήδη συνδεδεμένη. Τέλος η συσκευή μετακινείται στον βέλτιστο σταθμό με βάση την συγκεκριμένη λίστα.

(802.11r 2.8.2)

Το πρότυπο 802.11r δημοσιεύθηκε από το IEEE το 2011 και είναι γνωστό και με την ορολογία Fast BSS Transition (FT). Χρησιμοποιείται και αυτό για την επίτευξη της συνεχής επικοινωνίας της συσκευής με το δίκτυο στο οποίο είναι συνδεδεμένη κατά την διάρκεια της περιαγωγής.

Η χρήση του συγκεκριμένου προτύπου γίνεται σε δίκτυα που χρησιμοποιούν το πρότυπο WPA-Enterprise και 802.1x για την πιστοποίηση των χρηστών. Ο λόγος που συμβαίνει αυτό είναι γιατί η επανάληψη της πιστοποίησης των χρηστών στον νέο σταθμό βάσης χρειάζεται πολλαπλές ανταλλαγές μηνυμάτων, περισσότερες από αυτές κατά τη χρήση WPA-Personal με ένα κλειδί που το γνωρίζει τόσο η συσκευή όσο και ο σταθμός βάσης. Κατά τη διάρκεια της ταυτοποίησης δεν μπορούν να μεταδοθούν και να ληφθούν πακέτα δεδομένων. Αυτό σημαίνει ότι η σύνδεση της συσκευής με το δίκτυο διακόπτεται για αρκετά δευτερόλεπτα με αποτέλεσμα λειτουργίες που απαιτούν συνεχή ροή δεδομένων όπως για παράδειγμα μια τηλεφωνική κλήση να μη μπορεί να διατηρηθεί. Για να διορθωθεί το συγκεκριμένο θέμα, κατά την χρήση του 802.11r, το κλειδί που διαμορφώνεται κατά την αρχική πιστοποίηση του χρήστη αποθηκεύεται και επαναχρησιμοποιείται κατά την περιαγωγή από σταθμό σε σταθμό χωρίς να χρειάζεται να επαναληφθεί η πιστοποίηση του και κατά συνέπεια να διακοπεί η σύνδεση του στο δίκτυο.

(802.11v 2.8.3)

Το πρότυπο 802.11v δημοσιεύθηκε το 2011 από το IEEE και ξεκίνησε να χρησιμοποιείται το 2012. Το συγκεκριμένο πρότυπο επιτρέπει τις συσκευές που απαρτίζουν ένα ασύρματο δίκτυο να ανταλλάσσουν δεδομένα μεταξύ τους για το ηλεκτρομαγνητικό περιβάλλον στο οποίο βρίσκονται, τους σταθμούς βάσης που λαμβάνει η κάθε μία από τις συσκευές και την στάθμη σήματος. Ακόμη οι συσκευές μπορούν να πληροφορηθούν για τον αριθμό των συσκευών που είναι συνδεδεμένες σε κάθε σταθμό βάσης. Αυτή η γνώση επιτρέπει όλες τις συσκευές να γνωρίζουν την κατάσταση του ασύρματου δικτύου και έτσι να λάβουν τις βέλτιστες αποφάσεις για την περιαγωγή τους.

Αναφορές Κεφαλαίου 2.9

1. https://www.extremetech.com/wp-content/uploads/2014/03/1000px-2.4_GHz_Wi-Fi_channels_802.11bg_WLAN.svg_.png

2. https://commons.wikimedia.org/wiki/File:4-way-handshake_WPA2.png

ΚΕΦΑΛΑΙΟ 3 Σχεδιασμός Δικτύου και Τεχνοοικονομική Ανάλυση

Υφιστάμενη Κατάσταση 3.1

Κατά την πρώτη επίσκεψη στο σχολείο, έγινε καταγραφή της υπάρχουσας κατάστασης με σκοπό να γίνουν κατανοητές οι ελλείψεις της υποδομής και ο τρόπος που θα μπορούσαν να διευθετηθούν, με βάση τις ανάγκες των εκπαιδευτικών, των μαθητών και της διοίκησης. Πιο αναλυτικά στο σχολείο λειτουργούσαν δύο ανεξάρτητα τοπικά δίκτυα.

Τοπικό Δίκτυο Εργαστηρίων Πληροφορικής και Σχεδίου 3.1.1

Το σχολείο διαθέτει δύο εργαστήρια Πληροφορικής και ένα εργαστήριο Σχεδίου. Το πρώτο τοπικό δίκτυο κάλυπτε τις ανάγκες για πρόσβαση στο διαδίκτυο και διαμοιρασμού αρχείων αυτών των τριών εργαστηρίων. Όσο αφορά τη φυσική υποδομή, τα δύο εργαστήρια Πληροφορικής διέθεταν δομημένη καλωδίωση η οποία είχε κατασκευαστεί μαζί με τη δημιουργία των συγκεκριμένων εργαστηρίων.

Το πιο παλιό εργαστήριο Πληροφορικής, στο εξής γνωστό ως εργαστήριο Α, διέθετε δομημένη καλωδίωση με δεκατρείς πρίζες δικτύου. Η καλωδίωση του συγκεκριμένου εργαστηρίου κατέληγε σε ένα ικρίωμα 12 U θέσεων και εκεί τερματιζόταν σε ένα Patch Panel των είκοσι τεσσάρων θέσεων. Ο τρόπος τερματισμού των καλωδίων ήταν με βάση το πρότυπο T-568A ενώ τα καλώδια UTP που είχαν χρησιμοποιηθεί ήταν της κατηγορίας Cat5E. Στην συνέχεια και με τη χρήση προ-τερματισμένων UTP καλωδίων (Patch Cords), οι πρίζες αυτές συνδέονταν πάνω σε ένα διαμεταγωγέα του οίκου TP-Link είκοσι τεσσάρων διεπαφών δικτύου, ταχύτητας 10/100/1000Mb/s, ο οποίος ήταν τύπου unmanaged, δεν υποστήριζε δηλαδή πιο εξελιγμένες λειτουργίες, όπως η δημιουργία εικονικών τοπικών δικτύων (VLANs). Έπειτα ο συγκεκριμένος διαμεταγωγέας συνδεόταν με μία συσκευή Modem/Router μάρκας Speedport, η οποία εγκαταστάθηκε από τον ΟΤΕ με σκοπό την πρόσβαση του σχολείου στο Πανελλήνιο Σχολικό Δίκτυο.

Το νεότερο εργαστήριο Πληροφορικής, στο εξής γνωστό ως εργαστήριο Β, διέθετε δομημένη καλωδίωση με 16 θέσεις δικτύου. Η καλωδίωση του συγκεκριμένου εργαστηρίου κατέληγε σε ένα ικρίωμα 4U θέσεων. Ο τρόπος τερματισμού των καλωδίων ήταν με βάση το πρότυπο T-568B ενώ τα καλώδια που είχαν χρησιμοποιηθεί ήταν της κατηγορίας Cat6. Στην συνέχεια και με τη χρήση προ-τερματισμένων UTP Καλωδίων (Patch Cords), οι πρίζες αυτές συνδέονταν σε έναν διαμεταγωγέα του οίκου TP-Link, ίδιων χαρακτηριστικών και δυνατοτήτων με τον διαμεταγωγέα που βρισκόταν στο ικρίωμα του εργαστηρίου Α. Ο συγκεκριμένος διαμεταγωγέας συνδεόταν με την συσκευή Modem/Router που βρισκόταν στο ικρίωμα του εργαστηρίου Α μέσω καλωδίου UTP που διένυε την απόσταση μεταξύ των εργαστηρίων Α και Β και κάθε άκρο του κατέληγε στο ικρίωμα του εκάστοτε εργαστηρίου.

Τέλος για την εξυπηρέτηση του εργαστηρίου Σχεδίου, υπήρχε ένα καλώδιο UTP το οποίο ξεκινούσε από το ικρίωμα και διαμεταγωγέα του εργαστηρίου Β, διένυε τον κοινόχρηστο διάδρομο κάθετα και κατέληγε σε πρίζα δικτύου πίσω από τον σταθμό εργασίας που ήταν εγκατεστημένος στο συγκεκριμένο εργαστήριο. Το δίκτυο ήταν κοινό για τα τρία εργαστήρια, είχε μήκος μάσκας υποδικτύου /24 και χρησιμοποιούσε το Πανελλήνιο Σχολικό Δίκτυο με σκοπό την πρόσβαση του στο διαδίκτυο. Η σύνδεση ήταν τύπου ADSL και αναμενόταν η αναβάθμιση της σε VDSL.

Εικόνα 5: Πρώην Ικρίωμα Εργαστηρίου Α

Τοπικό Δίκτυο Γραφείων Διοίκησης 3.1.2

Το σχολείο διαθέτει τρία γραφεία που χρησιμοποιούνται από την διοίκηση του σχολείου και τους εκπαιδευτικούς του. Το πρώτο γραφείο είναι το γραφείο του Διευθυντή και της Γραμματείας του σχολείου και διαθέτει συνολικά τέσσερις σταθμούς εργασίας. Το δεύτερο γραφείο είναι το γραφείο των Υποδιευθυντών και διαθέτει συνολικά τέσσερις σταθμούς εργασίας. Το τρίτο γραφείο είναι το γραφείο των Εκπαιδευτικών που διαθέτει και αυτό τέσσερις σταθμούς εργασίας. Το δεύτερο τοπικό δίκτυο δημιουργήθηκε με σκοπό να καλύψει τις ανάγκες για πρόσβαση στο δίκτυο και διαμοιρασμού αρχείων μεταξύ των σταθμών εργασίας που χρησιμοποιούνται από το προσωπικό του σχολείου. Είχε αποφασισθεί να είναι ξεχωριστό για να εξασφαλισθεί μια ικανοποιητική ταχύτητα πρόσβασης στο διαδίκτυο, κάτι το οποίο δε θα ήταν εφικτό, εάν όλο το σχολείο μοιραζόταν τον ίδιο πάροχο διαδικτύου και πιο συγκεκριμένα το Πανελλήνιο Σχολικό Δίκτυο. Στο

συγκεκριμένο υποδίκτυο δεν υπήρχε δομημένη καλωδίωση. Αντιθέτως εγκαταστάθηκαν καλώδια UTP σε διαφορετικούς χρόνους και ανάλογα τις ανάγκες. Τα συγκεκριμένα καλώδια κατέληγαν μέσω οπών στους τοίχους σε έναν κεντρικό δρομολογητή του οίκου TP-Link, είκοσι τεσσάρων θέσεων με παρόμοια χαρακτηριστικά και δυνατότητες με τους διαμεταγωγείς που χρησιμοποιήθηκαν στα εργαστήρια Α και Β. Στη συνέχεια ο συγκεκριμένος διαμεταγωγέας συνδεόταν με τη συσκευή Modem/Router μάρκας Speedport, η οποία είχε εγκατασταθεί από τον ΟΤΕ με σκοπό την πρόσβαση στο διαδίκτυο μέσω του εμπορικού δικτύου του.

Το συγκεκριμένο δίκτυο ήταν κοινό για τα τρία γραφεία, είχε μήκος μάσκας υποδικτύου /24 και χρησιμοποιούσε το δίκτυο του ΟΤΕ με σκοπό την πρόσβαση του στο διαδίκτυο. Η σύνδεση ήταν τύπου ADSL. Ο δρομολογητής αναλάμβανε και την κάλυψη με δίκτυο WiFi και των γραφείων διοίκησης αλλά και αιθουσών που ήταν σε κοντινή απόσταση και η στάθμη του σήματος ήταν εφικτή καθώς και των φορητών συσκευών που ανήκαν στο εκπαιδευτικό προσωπικό. Τα 2 δίκτυα είχαν επικαλυπτόμενα εύρη διευθύνσεων IP με αποτέλεσμα οποιαδήποτε απόπειρα να ενοποιηθούν τα δύο δίκτυα να μην είναι εφικτή. Οι παραπάνω λόγοι καθιστούσαν την κατασκευή και ρύθμιση μιας νέας υποδομής απαραίτητη με σκοπό να εξαλειφθούν τα προβλήματα της παλαιότερης δικτυακής τοπολογίας.

Κριτήρια Σχεδιασμού 3.2

Τα κριτήρια σχεδιασμού της νέας υποδομής ήταν τα εξής:

- Ενοποίηση του δικτύου, χρήση ενός δρομολογητή/τείχους προστασίας που θα είχε την εποπτεία όλων των υποδικτύων και θα μεριμνούσε για την πρόσβαση τους στο διαδίκτυο από τον κατάλληλο πάροχο και την ασφάλεια της επικοινωνίας.
- Διαχωρισμός του δικτύου σε υποδίκτυα. Πιο συγκεκριμένα, διαφορετικό δίκτυο για το γραφείο εκπαιδευτικών, Διεύθυνσης και Υποδιεύθυνσης, για καθένα από τα δύο εργαστήρια Πληροφορικής, για τις αίθουσες και για το ασύρματο δίκτυο εκπαιδευτικών και μαθητών. Επιπλέον, ξεχωριστά υποδίκτυα για τις ανάγκες διαχείρισης του υπολογιστικού και δικτυακού εξοπλισμού καθώς και για τις συσκευές που ανήκουν στο σχολείο όπως είναι οι εκτυπωτές/φωτοτυπικά. Η συγκεκριμένη υλοποίηση θα διευκολύνει την παρακολούθηση των πόρων του δικτύου, την ανεξάρτητη επιλογή διαδικτυακού παρόχου ανάλογα με τον χώρο και το είδος των συσκευών που υπάρχουν σε κάθε VLAN καθώς και την εφαρμογή πολιτικών ασφαλείας που θα αποτρέψουν την πρόσβαση μη εξουσιοδοτημένων ατόμων σε σταθμούς εργασίας που ανήκουν στη διοίκηση και περιέχουν προσωπικά δεδομένα του εκπαιδευτικού προσωπικού και των μαθητών.
- Δημιουργία ασύρματου δικτύου μέσω της εγκατάστασης επαρκούς αριθμού σημείων πρόσβασης (Access Points) με στόχο τη βέλτιστη κάλυψη των αιθουσών και των γραφείων της διοίκησης με WiFi σύνδεση. Πολλαπλά SSIDs, διαφορετικά για τους καθηγητές, τους μαθητές και τις φορητές συσκευές που ανήκουν στο σχολείο όπως είναι laptops ή tablets.

- Προσθήκη δομημένης καλωδίωσης με πρίζες Ethernet σε όλες τις αίθουσες διδασκαλίας κοντά στις έδρες των εκπαιδευτικών, καθώς και στα γραφεία διοίκησης στους χώρους που ήδη υπάρχουν ή προβλέπεται να μπουν σταθμοί εργασίας. Ακόμη, προσθήκη κάποιων επιπλέον πριζών δικτύου στα δύο εργαστήρια Πληροφορικής λόγω αυξανόμενων αναγκών.
- Εγκατάσταση κεντρικού ικριώματος σε ειδικά διαμορφωμένο και κλιματιζόμενο χώρο. Στο συγκεκριμένο ικρίωμα θα στεγάζονται ο εξοπλισμός των παρόχων διαδικτύου (Modems, ONUs), ο κεντρικός δρομολογητής, ο οπτικός διαμεταγωγέας διαμοιρασμού (Distribution Switch) καθώς και διαμεταγωγείς πρόσβασης για την εξυπηρέτηση των αναγκών των αιθουσών που βρίσκονται στην πτέρυγα που βρίσκεται ο συγκεκριμένος χώρος καθώς και των γραφείων διοίκησης. Τα ικριώματα των δύο εργαστηρίων Πληροφορικής θα χρησιμοποιηθούν για την στέγαση των διαμεταγωγών πρόσβασης (Access Switches) που εξυπηρετούν τα δύο εργαστήρια καθώς και τις αίθουσες διδασκαλίας που βρίσκονται κοντά σε αυτά. Η σύνδεση μεταξύ των τριών ικριωμάτων θα πρέπει να γίνει με χρήση οπτικής ίνας λόγω της απόστασης μεταξύ τους αλλά και για λόγους υποστήριξης αυξημένων ταχυτήτων (10Gb/s) σε μελλοντικό χρόνο.
- Ανακατασκευή των ικριωμάτων στα δύο εργαστήρια Πληροφορικής με σκοπό την καλύτερη οργάνωση τους και την αντικατάσταση παθητικού εξοπλισμού που λόγω φθοράς, συχνά εμφανίζει θέματα με αποσυνδέσεις και περιορισμένη ταχύτητα.
- Αύξηση της ταχύτητας στο διαδίκτυο μέσω της χρήσης παρόχου οπτικής ίνας και αντικατάσταση του εμπορικού παρόχου ADSL καθώς και αίτηση για αναβάθμιση της ταχύτητας σύνδεσης που παρέχεται από το Πανελλήνιο Σχολικό δίκτυο σε VDSL, εφόσον υπάρχει η δυνατότητα.
- Δυνατότητα επιλογής του παρόχου διαδικτύου που θα χρησιμοποιεί το κάθε υποδίκτυο (VLAN).
- Δυνατότητα εποπτείας του δικτύου ως σύνολο και του εξοπλισμού που το απαρτίζει. Δημιουργία γραφημάτων για την κίνηση του δικτύου στη διάρκεια της ημέρας από την συνολική κίνηση προς το διαδίκτυο έως την κίνηση σε επίπεδο υποδικτύου και πρίζας Ethernet καθώς και του αριθμού των συσκευών που συνδέονται στο ασύρματο δίκτυο. Επιπλέον απεικόνιση μετρικών που δείχνουν στοιχεία λειτουργίας του δικτυακού εξοπλισμού όπως χρήση επεξεργαστή, μνήμης και θερμοκρασίας. Έκδοση ειδοποιήσεων σε περίπτωση κάποιας ανωμαλίας στην λειτουργία όπως είναι η διακοπή της σύνδεσης με κάποιον πάροχο διαδικτύου ή διακοπή λειτουργίας κάποιου στοιχείου του ενεργού εξοπλισμού όπως είναι ο κεντρικός δρομολογητής, οι διαμεταγωγείς και τα σημεία πρόσβασης του ασύρματου δικτύου.

Σχεδιασμός της Δομημένης Καλωδίωσης 3.3

Πριν οποιασδήποτε προσπάθειας σχεδιασμού των ενσύρματων και ασύρματων υποδικτύων θα έπρεπε να σχεδιασθεί η δομημένη καλωδίωση του ορόφου στον οποίο θα γινόταν η εγκατάσταση. Έτσι έγινε επίσκεψη στο σχολείο και σχεδιάσθηκε αρχικά μια κάτοψη όλων των χώρων του ορόφου στον οποίο στεγάζεται σε κατάλληλο σχεδιαστικό πρόγραμμα. Στη συνέχεια έγινε έρευνα για το που θα τοποθετηθούν οι πρίζες δικτύου.

Όσο αφορά τις αίθουσες διδασκαλίας, αποφασίσθηκε να τοποθετηθεί μία διπλή πρίζα δικτύου σε κάθε αίθουσα. Ο συγκεκριμένος αριθμός θα κάλυπτε τόσο την τοποθέτηση ενός σταθερού υπολογιστή σε κάθε αίθουσα όσο και κάποια επιπλέον συσκευή με ανάγκη σύνδεσης στο δίκτυο όπως ένας φορητός υπολογιστής που ανήκει σε κάποιον εκπαιδευτικό. Στα εργαστήρια Πληροφορικής οι επιπλέον πρίζες δικτύου αποφασίσθηκε να τοποθετηθούν κοντά στην έδρα του εκπαιδευτικού, όπου και υπήρχε έλλειψη. Στα γραφεία της διοίκησης και των εκπαιδευτικών αποφασίσθηκε να τοποθετηθούν διπλές πρίζες δικτύου κοντά στα γραφεία που υπάρχουν σταθμοί εργασίας με αριθμό ικανό ώστε να καλύπτουν τις τωρινές ανάγκες καθώς και επιπλέον μία οι δύο θύρες πρόσβασης ανά περίπτωση για μελλοντικές ανάγκες. Επιπρόσθετα αποφασίσθηκε η τοποθέτηση διπλών πριζών δικτύου δίπλα από το κεντρικό ικρίωμα με στόχο την σύνδεση σε αυτές ενός ή περισσότερων εξυπηρετητών που θα φιλοξενούσαν τις υποδομές παρακολούθησης του δικτύου. Διπλές πρίζες δικτύου αποφασίσθηκε να τοποθετηθούν και κοντά στις θέσεις που υπάρχουν εκτυπωτές αλλά και φωτοτυπικά καθώς και σε μέρη που προβλέπεται να εγκατασταθεί κάποιος υπολογιστής στο μέλλον.

Τέλος σχεδιάσθηκε να τοποθετηθούν και δώδεκα μονές πρίζες δικτύου στην οροφή 12 αιθουσών για την τροφοδοσία με ηλεκτρικό ρεύμα και σύνδεση στο δίκτυο δεδομένων των σημείων πρόσβασης WiFi. Οι τοποθεσίες αυτών προέκυψαν σύμφωνα και με τη μελέτη που πραγματοποιήθηκε για τη βέλτιστη κάλυψη του ασύρματου δικτύου και αναλύεται σε επόμενη ενότητα.

Εξ αρχής προβλέφθηκε τα καλώδια δικτύου να μην κυκλοφορούν εκτεθειμένα στους τοίχους και στις οροφές αλλά να χρησιμοποιηθούν πλαστικοί σωλήνες καλωδίων κατάλληλης διατομής, κανάλια καλωδίων και σχάρες καλωδίων για τη διέλευση από τους διαδρόμους.

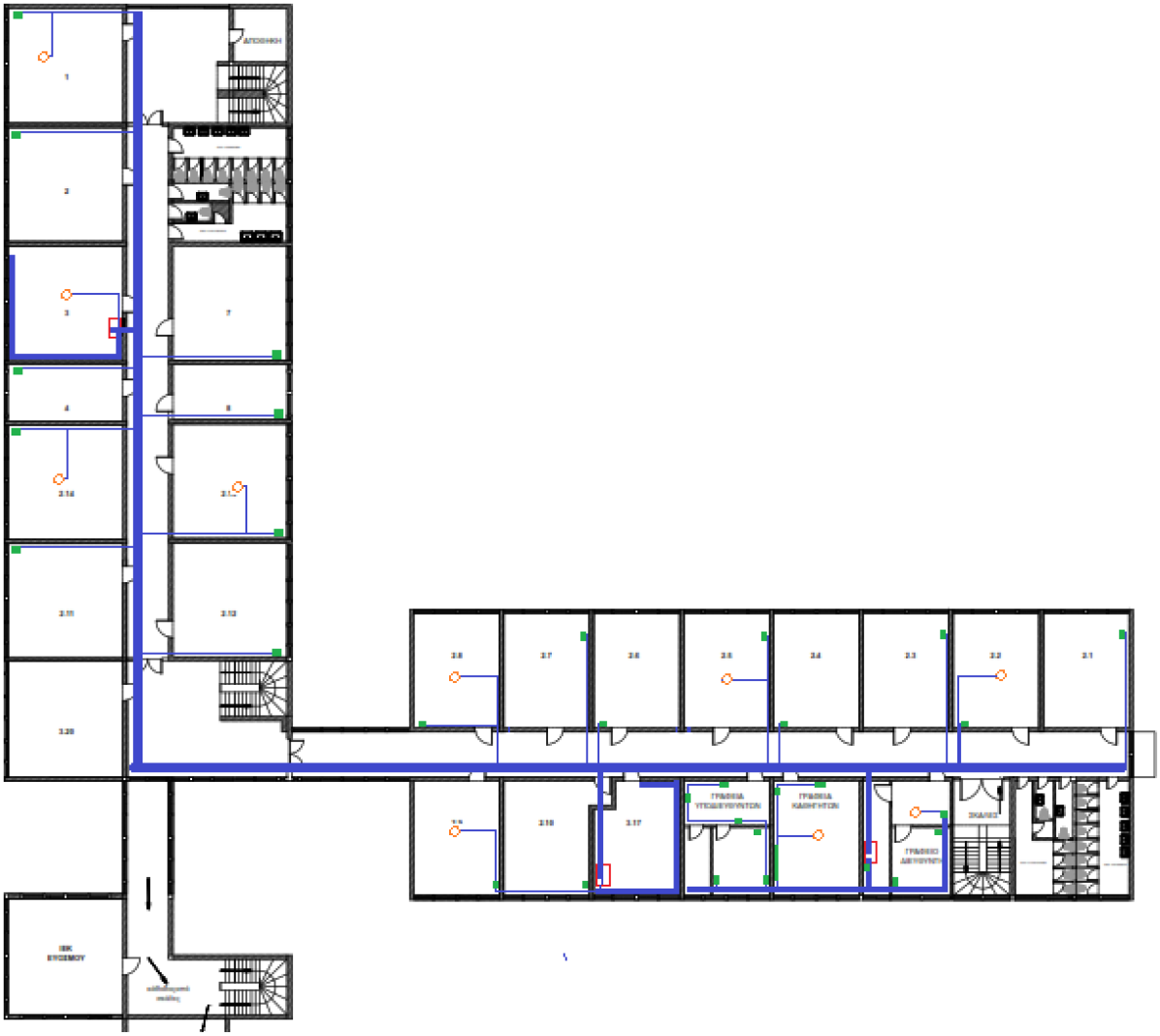
Για τον υπολογισμό του απαιτούμενου αριθμού των ικριωμάτων και την επιλογή του βέλτιστου σημείου τοποθέτησης λήφθηκαν υπόψη τα εξής κριτήρια:

- Το μήκος του καλωδίου από την πρίζα δικτύου μέχρι το ικρίωμα θα πρέπει να είναι το ελάχιστο δυνατό. Αυτό συμβαίνει λόγω της αδυναμίας λειτουργίας ενός καλωδίου UTP αν το μήκος του ξεπερνάει τα εκατό μέτρα λόγω πτώσης τάσης αλλά και για να περιορισθεί η πιθανότητα παρεμβολών από άλλες πηγές ηλεκτρομαγνητικών σημάτων.
- Δύο από τα ικριώματα θα πρέπει να βρίσκονται στα εργαστήρια Πληροφορικής και ιδανικά στους χώρους που υπάρχουν ήδη τα ικριώματα της παλιάς υποδομής. Αυτό συμβαίνει γιατί τα καλώδια της δομημένης καλωδίωσης των συγκεκριμένων εργαστηρίων καταλήγουν στους συγκεκριμένους χώρους, είναι περιορισμένου μήκους και απόπειρες επέκτασης των καλωδίων με χρήση συνδετήρων (couplers) δεν συνίστανται.

- Πρέπει να υφίσταται ένα κεντρικό rack στο σημείο που καταλήγουν οι συνδέσεις χαλκού και μελλοντικά οπτικών ινών από τους παρόχους διαδικτύου ώστε μέσα να στεγαστεί το σύνολο του εξοπλισμού τους.
- Δεν θα πρέπει να τοποθετηθούν ικριώματα σε κοινόχρηστους χώρους όπως είναι τα κλιμακοστάσια και οι διάδρομοι. Αυτό συμβαίνει γιατί από τους χώρους αυτούς διέρχεται πλήθος κόσμου και υπάρχει κίνδυνος δολιοφθοράς.

Για τους παραπάνω λόγους και σύμφωνα με τα κριτήρια σχεδιασμού αποφασίσθηκε να χρησιμοποιηθούν συνολικά τρία ικριώματα. Τα δύο από αυτά θα είναι καινούρια και θα έχουν ύψος 12U θέσεων ενώ το τρίτο θα είναι αυτό που ήδη υπάρχει στο εργαστήριο Α και το μέγεθος του είναι επίσης 12U και άρα επαρκές για τις ανάγκες της νέας υποδομής. Το ικρίωμα του Εργαστηρίου Α ανέλαβε τη στέγαση του παθητικού και ενεργού εξοπλισμού για το εργαστήριο Α και δύο αίθουσες προσκείμενες σε αυτό καθώς και για τα σημεία ασύρματης πρόσβασης που βρίσκονται εκεί. Το ικρίωμα του εργαστηρίου Β ανέλαβε την στέγαση του ενεργού και παθητικού εξοπλισμού για το εργαστήριο Β καθώς και των αιθουσών και σημείων ασύρματης πρόσβασης που είναι στην βορειοδυτική πτέρυγα του κτηρίου. Το κεντρικό ικρίωμα που βρίσκεται σε αποθηκευτικό χώρο του γραφείου διεύθυνσης ανέλαβε την στέγαση του ενεργού και παθητικού εξοπλισμού για τα γραφεία διοίκησης και τις αίθουσες που βρίσκονται στη βορειοανατολική πτέρυγα του κτηρίου καθώς και τα σημεία ασύρματης πρόσβασης που είναι εγκατεστημένα εκεί. Ακόμα στο συγκεκριμένο στεγάστηκε ο κεντρικός δρομολογητής του δικτύου καθώς και ο εξοπλισμός των παρόχων διαδικτύου.

Η κάτοψη του κτηρίου που ενσωματώνει τις παραπάνω προσθήκες φαίνεται στην παρακάτω εικόνα:



Εικόνα 6: Γενική Κάτοψη Δομημένης Καλωδίωσης

Ακόμη σχεδιάσθηκαν διαγράμματα της σειράς τοποθέτησης του εξοπλισμού στο εσωτερικό των ικριωμάτων με σκοπό την καλύτερη οργάνωση αυτών.

RACK A	RU	RACK B	RU	RACK C	RU
BLANK PANEL		BLANK PANEL		BLANK PANEL	
PATCH PANEL A	1	PATCH PANEL	1	PATCH PANEL	1
CABLE GUIDE	2	CABLE GUIDE	2	CABLE GUIDE	2
sw1-poe	3	sw4	3	sw5-poe	3
PATCH PANEL A	4	CABLE GUIDE	4	CABLE GUIDE	4
CABLE GUIDE	5	BLANK PANEL	5	PATCH PANEL	5
sw2	6		6	CABLE GUIDE	6
PATCH PANEL A	7	speedport-modem, ap-02,	7	sw6	7
CABLE GUIDE	8	ap-03 PoE injectors	8	CABLE GUIDE	8
sw3	9		9	PATCH PANEL	9
sw0-fiber	10	RACK SHELF	10	CABLE GUIDE	10
core-router	11	CABLE BRUSH	11	CABLE BRUSH	11
PDU	12	PDU	12	PDU	12

Εικόνα 7: Διαγράμματα Ικριωμάτων

Σχεδιασμός του Ασύρματου Δικτύου WiFi 3.4

Ένα από τα βασικά κριτήρια για την υλοποίηση της δικτυακής υποδομής του σχολείου ήταν η δημιουργία ασύρματου δικτύου WiFi το οποίο θα κάλυπτε επαρκώς τον όροφο του σχολικού συγκροτήματος στον οποίο στεγάζεται το συγκεκριμένο κτήριο. Για να βρεθούν τα σημεία που έπρεπε να τοποθετηθούν τα σημεία ασύρματης πρόσβασης με σκοπό τη βέλτιστη κάλυψη και στάθμη σήματος θα έπρεπε να γίνει μια μελέτη ραδιοκάλυψης του χώρου.

Επιλογή Σημείων Τοποθέτησης των Σημείων Πρόσβασης 3.4.1

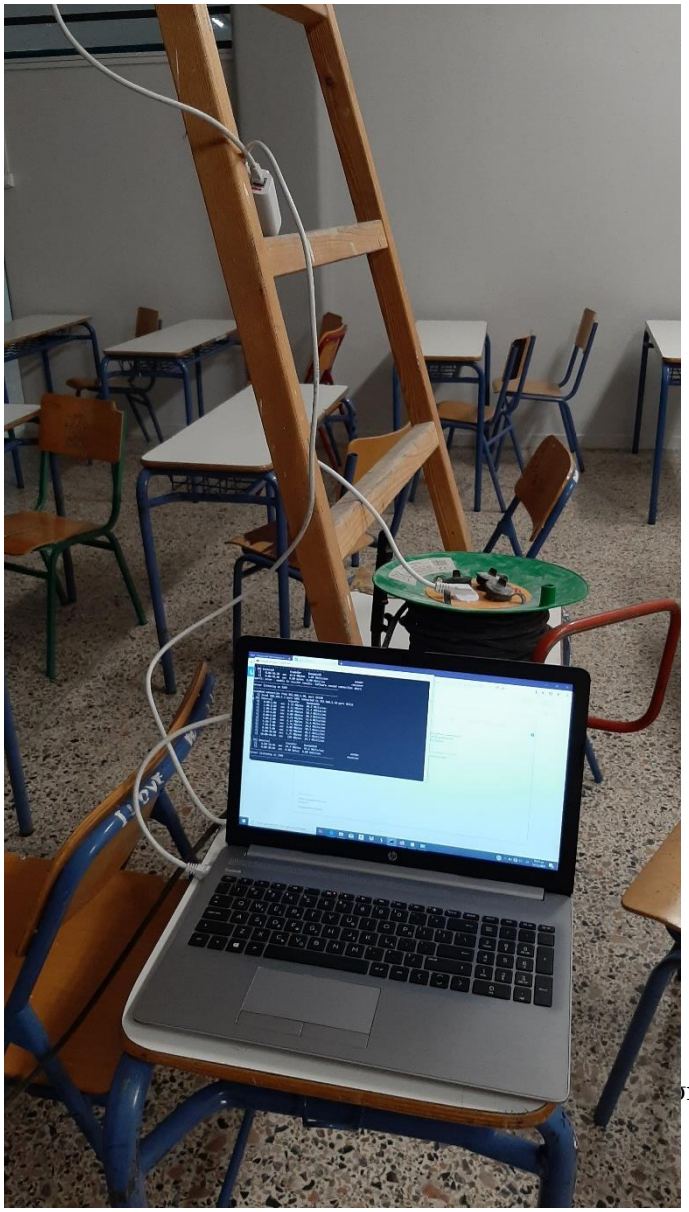
Η μελέτη ραδιοκάλυψης του χώρου έγινε με τον εξής τρόπο. Αρχικά χρησιμοποιήθηκε το σχέδιο της κάτοψης του ορόφου με σκοπό να σχεδιασθεί μια υπόθεση για το που θα μπορούσαν να τοποθετηθούν τα σημεία ασύρματης πρόσβασης (Access Points). Δοκιμάστηκε η υπόθεση κάθε σημείο πρόσβασης να αναλάβει την κάλυψη της αίθουσας μέσα στην οποία στεγάζεται και των δύο διπλανών αιθουσών. Στην περίπτωση της βορειοανατολικής πτέρυγας οι αίθουσες χωρίζονται με γυψοσανίδα ενώ στην περίπτωση της βορειοδυτικής πτέρυγας οι αίθουσες χωρίζονται με τοίχο από τούβλο. Σύμφωνα με την παραπάνω υπόθεση χρειάζονται 10 Access Points για την κάλυψη που ορίστηκε, τα οποία και φαίνονται στην παραπάνω κάτοψη του χώρου.

Για τη δοκιμή της συγκεκριμένης υπόθεσης επιλέχθηκε να στηθεί ένα Access Point σε ψηλό σημείο, προσωρινά στηριγμένο πάνω σε μία φορητή σκάλα και σε ύψος όσο το δυνατόν πιο κοντά στην οροφή της αίθουσας με στόχο να γίνεται προσομοίωση πραγματικών συνθηκών. Ακόμη επιλέχθηκε η σκάλα να είναι ξύλινη καθώς μεταλλική σκάλα μπορεί να προκαλούσε αντανακλάσεις και άλλα φαινόμενα που θα διαστρέβλωναν την ποιότητα του σήματος που λαμβάνεται και εκπέμπεται. Το σημείο πρόσβασης ρυθμίστηκε να εκπέμπει δύο δίκτυα WiFi, το ένα στα 2.4GHz και σε ένα τυχαίο κανάλι και το δεύτερο στα 5GHz και σε ένα τυχαίο κανάλι. Ακόμη τα δύο δίκτυα είχαν διαφορετικό όνομα με σκοπό τον ευκολότερο διαχωρισμό τους. Σχετικά με το εύρος ζώνη, αυτό ορίστηκε στα 20MHz και η ισχύς εκπομπής στο μέγιστο για τα 5GHz και στο ελάχιστο για τα 2.4GHz. Στη συνέχεια και με τη χρήση ενός iperf3[6] server και του εργαλείου InSSIDer σε έναν φορητό υπολογιστή με ασύρματη κάρτα δικτύου, που υποστηρίζει και τα δύο φάσματα συχνοτήτων έγιναν δοκιμές ταχύτητας. Οι συγκεκριμένες δοκιμές έγιναν στις τέσσερις γωνίες και των τριών αιθουσών και ελέγχθηκε αν οι ταχύτητες μετάδοσης είναι ικανοποιητικές και όσο το δυνατόν πιο κοντά στην ταχύτητα της ζεύξης και η στάθμη σήματος δεν πέφτει κάτω από -70dBm το οποίο θεωρείται ως βέλτιστη πρακτική[7] για τα ασύρματα δίκτυα. Το συγκεκριμένο πείραμα επαναλήφθηκε για όλες τις θέσεις που προτάθηκε να εγκατασταθούν Access Points.

[6] Iperf3: Πρόγραμμα που τρέχει στην γραμμή εντολών, έχει δομή client-server και επιτρέπει δοκιμές ταχύτητας ανταλλαγής αρχείων με πολλαπλές παραμέτρους πρωτοκόλλου, ταυτόχρονων συνδέσεων κλπ.

[7] https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/cisco_wlan_design_guide.pdf

Η συγκεκριμένη υπόθεση φάνηκε σωστή και με τις δοκιμές που ακολούθησαν οπότε οι θέσεις που ορίστηκαν αποφασίστηκε να είναι και οι θέσεις που θα εγκατασταθούν τα Access Points.



ης

Επιλογή Καναλιών και Ισχύος Εκπομπής 3.4.2

Επόμενο βήμα της επιλογής των θέσεων τοποθέτησης των Access Points ήταν η επιλογή των κατάλληλων καναλιών στα οποία θα ρυθμιστεί να εκπέμπει και να λαμβάνει το εκάστοτε Access Point με σκοπό να περιοριστούν οι παρεμβολές από γειτονικά Access Points άλλων σχολείων του συγκροτήματος, καθώς και γειτονικών κατοικιών. Το συγκεκριμένο σχολείο βρίσκεται στον τελευταίο όροφο ενός ψηλού κτηρίου με αποτέλεσμα να γίνονται παρεμβολές από πλήθος Access Points και ο περιορισμός αυτών να μην είναι τεχνικά εφικτός. Παρ' όλα αυτά

δόθηκε μέριμνα ώστε τα Access Points του σχολείου που ήδη λειτουργούσαν στους δρομολογητές του ΟΤΕ και του Πανελλήνιου Σχολικού Δικτύου να απενεργοποιηθούν ώστε να μην νοθεύσουν τις μετρήσεις. Τόσο στο φάσμα των 2.4GHz όσο και στο φάσμα των 5GHz, το εύρος ζώνης που αποφασίστηκε να χρησιμοποιηθεί είναι τα 20MHz επειδή το συγκεκριμένο εύρος ζώνης θα παρείχε τον μέγιστο αριθμό διαθέσιμων καναλιών προς χρήση. Έτσι στα 2.4GHz υπάρχουν 13 κανάλια από τα οποία έπρεπε να γίνει επιλογή ανάμεσα σε τρία, το κανάλι 1, 6 και 11 μιας και είναι τα μόνα που δεν μοιράζονται συχνότητες με άλλα κανάλια και άρα δεν υπάρχει ενδοκαναλική παρεμβολή (Co-Channel Interference). Όσο αφορά τα 5GHz έχουμε 25 κανάλια. Ωστόσο τα 21 από αυτά ανήκουν στην ζώνη των DFS[8] καναλιών. Αυτό σημαίνει ότι στην ίδια συχνότητα εκπέμπουν και λαμβάνουν μετεωρολογικά radars και σύμφωνα με τους κανονισμούς, εάν το Access Point αντιληφθεί εκπομπή από μετεωρολογικό radar τότε πρέπει άμεσα να διακόψει την εκπομπή του και να επιλέξει ένα άλλο κανάλι. Έτσι για λόγους μείωσης του διαχειριστικού φόρτου και πιθανών προβλημάτων διακοπής των συνδέσεων που μπορεί να προκύψουν επιλέχθηκε να χρησιμοποιηθούν μόνο τα κανάλια 36, 40, 44 και 48 που δεν ανήκουν στην ζώνη DFS. Στην συνέχεια και με τη χρήση του προγράμματος InSSIDer στον φορητό υπολογιστή, επαναλήφθηκαν μετρήσεις στις συστάδες από τρεις αίθουσες που είχαν οριστεί στο προηγούμενο στάδιο με σκοπό να βρεθεί το βέλτιστο κανάλι για τα 2.4GHz και τα 5GHz. Το πρόγραμμα παραμετροποιήθηκε ώστε να δείχνει SSIDs ανά κανάλι εκπομπής. Το κριτήριο με το οποίο θα γινόταν η επιλογή ήταν με βάση πιο κανάλι είναι το πιο άδειο στις συνολικά 12 δειγματοληψίες σήματος και πιο συγκεκριμένα 4 δειγματοληψίες στις 4 γωνίες κάθε αίθουσας για 3 αίθουσες. Η ίδια ενέργεια επαναλήφθηκε και για τα 2.4 αλλά και για τα 5GHz.

Μετά την επανάληψη της συγκεκριμένης ενέργειας στις δώδεκα θέσεις δοκιμών ανά τρεις αίθουσες καθώς και στους προσκείμενους σε αυτές διαδρόμους συντάχθηκε η λίστα με την βέλτιστη επιλογή καναλιών ανά Access Point και σημείο πρόσβασης. Δόθηκε σαφώς μέριμνα ώστε γειτονικά Access Points να μην βρίσκονται στο ίδιο κανάλι με σκοπό την αποφυγή παρεμβολών. Παρακάτω παρουσιάζεται η συγκεκριμένη λίστα.

Access Point Name	2.4GHz Channel	5GHz Channel
ap-01	6	36
ap-02	11	40
ap-03	1	44
ap-04	1	44
ap-05	6	40
ap-06	11	36

[8] DFS: Dynamic Frequency Selection

ap-07	6	36
ap-08	6	36
ap-09	1	48
ap-10	11	44

Όσο αφορά την ισχύ εκπομπής αυτή αποφασίσθηκε να είναι η μέγιστη δυνατή για τα 5GHz και η ελάχιστη δυνατή για τα 2.4GHz. Ο λόγος που αποφασίστηκε αυτό είναι ο εξής: Ο στόχος της σχεδίασης του ασύρματου δικτύου είναι όσο το δυνατόν περισσότερες συσκευές να προτιμούν τα 5GHz για την σύνδεση τους καθώς το συγκεκριμένο εύρος ζώνης είναι σαφώς λιγότερο επιβαρυμένο από παρεμβολές και επιπλέον μπορεί να επιτύχει υψηλότερους ρυθμούς μετάδοσης δεδομένων. Ο κάθε κατασκευαστής συσκευών πρόσβασης στο διαδίκτυο καθώς και το κάθε λειτουργικό σύστημα χρησιμοποιεί διαφορετικούς αλγόριθμους για να επιλέξει ποιο από τα δύο φάσματα συχνοτήτων θα χρησιμοποιήσει. Τεχνικές επιρροής της συγκεκριμένης επιλογής όπως το Band Steering εναπόκεινται στην σωστή εφαρμογή των προτύπων που δεν είναι πάντα δεδομένη και λειτουργούν διαφορετικά για κάθε κατασκευαστή. Για αυτό τον λόγο η άσκηση επιρροής με τη χρήση των λιγότερο επεμβατικών μεθόδων όπως το να υπάρχει στο δίκτυο των 5GHz καλύτερη στάθμη σήματος από τα 2.4GHz θεωρήθηκε η βέλτιστη δυνατή. Επιπλέον η συγκεκριμένη ρύθμιση ισχύος εκπομπής επιλέχθηκε και κατά την περίοδο δοκιμών ραδιοκάλυψης. Φάνηκε πως παρότι τα Access Points εξέπεμπαν στο μέγιστο της ισχύς τους η φύση του φάσματος των 5GHz να μην μπορεί να διαπερνά εύκολα τους τοίχους σε συνδυασμό με την απουσία γειτονικών Access Points στο ίδιο κανάλι εξασφάλιζε την απουσία εσωτερικών παρεμβολών.

Δημιουργία Πολλαπλών Ασύρματων Δικτύων 3.5

Στα κριτήρια υλοποίησης της δικτυακής υποδομής προβλεπόταν η δημιουργία διαφορετικών ασύρματων δικτύων (SSIDs) για τους μαθητές και το εκπαιδευτικό προσωπικό. Έτσι αποφασίστηκε η δημιουργία τριών διακριτών SSIDs. Τα 2 είναι για τους μαθητές και τους εκπαιδευτικούς ενώ δημιουργήθηκε και ένα τρίτο για την σύνδεση των συσκευών που ανήκουν στο σχολείο όπως Tablets και φορητοί υπολογιστές. Τα συγκεκριμένα SSIDs εκπέμπονται από το σύνολο των Access Points του ορόφου. Δικτυακή κίνηση από και προς τα τρία SSIDs διοχετεύεται με τη χρήση τριών διακριτών VLANs τα οποία θα είναι προσβάσιμα από το σύνολο των Access Points στο ενσύρματο δίκτυο.

SSID	VLAN ID	SUBNET	SECURITY
teachers-wifi	130	10.33.130.0/24	WPA2-PERSONAL
students-wifi	140	10.33.140.0/22	OPEN
devices-wifi	150	10.33.150.0/24	WPA2-PERSONAL

Διαχωρισμός σε Υποδίκτυα (VLANs) 3.6

Μετά από την ολοκλήρωση της σχεδίασης του ασύρματου και ενσύρματου δικτύου και σε συνεννόηση με τη διοίκηση του σχολείου και τους εκπαιδευτικούς Πληροφορικής, συμφωνήθηκε το δίκτυο του σχολείου να βασιστεί στο εύρος IPv4 διευθύνσεων 10.33.0.0/16 και το συγκεκριμένο εύρος στην συνέχεια να διαχωριστεί σε 16 υποδίκτυα. Όλα τα υποδίκτυα έχουν μήκος μάσκας υποδικτύου /24 εκτός από το υποδίκτυο του ασύρματου δικτύου των μαθητών το οποίο έχει μάσκα υποδικτύου /22 λόγω των αυξημένων αναγκών σε δικτυακές συσκευές που θα κληθεί να εξυπηρετήσει.

Ο παρακάτω πίνακας παραθέτει αναλυτικά τα υποδίκτυα που έχουν χρησιμοποιηθεί και την περιγραφή της χρήσης του καθενός από αυτά.

VLAN	Υποδίκτυο	Χωρητικότητα	Περιγραφή
10	10.33.10.0/24	251 πελάτες	Διαχείριση Δικτυακού Εξοπλισμού
20	10.33.20.0/24	251 πελάτες	Υπολογιστική Υποδομή (Servers/VMs)
30	10.33.30.0/24	251 πελάτες	Εκτυπωτές / Φωτοτυπικά
40	10.33.40.0/24	251 πελάτες	Πρόβλεψη για VoIP τηλεφωνία
50	10.33.50.0/24	251 πελάτες	Επισφαλείς Συσκευές (IoT)
60	10.33.60.0/24	251 πελάτες	Δίκτυο Διεύθυνσης
70	10.33.70.0/24	251 πελάτες	Δίκτυο Υποδιεύθυνσης
80	10.33.80.0/24	251 πελάτες	Δίκτυο Γραφείου Καθηγητών
90	10.33.90.0/24	251 πελάτες	Εργαστήριο Πληροφορικής Α
100	10.33.100.0/24	251 πελάτες	Εργαστήριο Πληροφορικής Β
110	10.33.110.0/24	251 πελάτες	Δίκτυο Αιθουσών Διδασκαλίας
120	10.33.120.0/24	251 πελάτες	Δίκτυο Ελεύθερης Ενσύρματης Πρόσβασης στο Internet
130	10.33.130.0/24	251 πελάτες	WiFi καθηγητών
140	10.33.140.0/22	1022 πελάτες	WiFi μαθητών
150	10.33.150.0/24	251 πελάτες	WiFi συσκευών

			ιδιοκτησίας του σχολείου (Laptops/Tablets)

Τεχνοοικονομική Ανάλυση 3.7

Μετά την ολοκλήρωση συγκέντρωσης των αναγκών συντάχθηκε μια οικονομοτεχνική μελέτη για τον υπολογισμό της ποσότητας των υλικών που απαιτούνται αλλά και του συνολικού κόστους.

Α/Α	ΚΑΤΗΓΟΡΙΑ ΠΡΟΪΟΝΤΟΣ	ΠΕΡΙΓΡΑΦΗ ΠΡΟΪΟΝΤΟΣ	ΤΙΜΗ	ΠΟΣΟΤΗΤΑ	ΤΕΛΙΚΗ ΤΙΜΗ
1	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	APC UPS BX1400U 1400VA	175.78	1	175.78
2	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	UBIQUITI EDGEROUTER 6P	235.79	1	235.79
3	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	UBIQUITI EDGESWITCH 12F FIBER SWITCH	219.73	1	219.73
4	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	UBIQUITI UNIFI NANOHD WIFI ACCESS POINT	152.439	9	1371.951
5	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	UBIQUITI UNIFI AC PRO WIFI ACCESS POINT	134.81	1	134.81
6	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	UBIQUITI EDGESWITCH 24 PORTS POE+	396	2	792
9	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	UBIQUITI EDGESWITCH 24 PORTS	224	4	896
10	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	CORSAIR ML 120 120MM FANS	28.135	6	168.81
7	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	EQUIP POWER STRIP 8 BAY	26.89	5	134.45
8	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	ΠΡΟΣΤΑΤΕΥΤΙΚΟ ΥΠΕΡΤΑΣΗΣ	10.899	3	32.697
11	ΕΝΕΡΓΟΣ ΕΞΟΠΛΙΣΜΟΣ	ΤΡΟΦΟΔΟΤΙΚΟ 24V/2A ΓΙΑ ΑΝΕΜΙΣΤΗΡΕΣ ΙΚΡΙΩΜΑΤΩΝ	3.0504	1	3.0504
1	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΣΩΛΗΝΑΣ ΚΟΥΒΙΔΗΣ 20mm ΑΝΟΙΧΤΟ ΓΚΡΙ 3Μ	0.838	152	127.376
2	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΒΑΣΗ ΣΤΗΡΙΞΗΣ ΠΡΙΖΑΣ ΓΙΑ ΚΑΝΑΛΙ ΟΡΙΖΟΝΤΙΟ 85ΜΜ	1.546	7	10.822
3	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	LEGRAND ΚΑΝΑΛΙ ΤΟΙΧΟΥ 105ΜΜx50ΜΜ 4 METER	10.1308	1	10.1308
4	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΜΟΥΦΑ ΣΩΛΗΝΑ 20ΜΜ	0.154	590	90.86
5	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΣΩΛΗΝΑΣ SPIRAL 20ΜΜ	0.7688	50	38.44
6	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΚΑΝΑΛΙ ΔΙΑΝΟΜΗΣ 60Χ40ΜΜ	2.019	12	24.228
7	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΚΑΝΑΛΙ ΔΙΑΝΟΜΗΣ 40Χ25ΜΜ	1.16	12	13.92
8	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΚΑΝΑΛΙ ΔΙΑΝΟΜΗΣ 25Χ25ΜΜ	0.838	64	53.632
9	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΣΧΑΡΑ ΚΑΛΩΔΙΩΝ 150ΜΜΧ0.6ΜΜ	2.3312	171	398.6352
10	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΟΔΗΓΟΣ ΚΑΛΩΔΙΩΝ	24.31	9	218.79
11	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΚΟΛΛΑΡΟ ΣΗΡΙΞΗΣ ΓΙΑ ΣΩΛΗΝΑ 20ΜΜ	0.18476	300	55.428
12	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΚΑΜΠΥΛΗ ΣΩΛΗΝΑ 20ΜΜ	0.5394	30	16.182
13	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΓΩΝΙΑ ΣΤΗΡΙΞΗΣ ΣΧΑΡΑΣ ΚΑΛΩΔΙΩΝ	0.974	103	100.322
14	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΓΩΝΙΑ ΣΧΑΡΑΣ 90 ΜΟΙΡΕΣ	3.379	4	13.516
15	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΔΙΑΚΛΑΔΩΣΗ Τ ΣΧΑΡΑΣ	4.182	4	16.728
16	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΣΥΝΔΕΣΜΟΣ ΣΧΑΡΑΣ	0.36456	132	48.12192
17	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΝΤΙΖΑ ΣΤΗΡΙΞΗΣ ΣΧΑΡΑΣ ΚΑΛΩΔΙΩΝ	1.128	85	95.88
18	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΣΤΕΡΩΤΙΚΑ ΝΤΙΖΑΣ ΣΤΟΝ ΤΟΙΧΟ	0.111	250	27.75
19	ΕΞΑΡΤΗΜΑΤΑ ΣΤΗΡΙΞΗΣ	ΠΑΞΙΜΑΔΙΑ	0.1	900	90

1	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	DIGITUS DN-9006-N ΕΠΙΤΟΙΧΙΑ ΠΡΙΖΑ 2XRJ-45 CAT6	6.45	43	277.35
2	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	EQUIP 235211 ΕΠΙΤΟΙΧΙΑ ΠΡΙΖΑ 1XRJ-45 CAT6	2.42	14	33.88
3	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 1M CABLE CAT6 BLUE	3.008	61	183.488
4	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 0.5M CABLE CAT6 RED	1.0044	4	4.0176
5	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 3M CABLE CAT6 BLUE	2.5	32	80
6	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 3M CABLE CAT6 YELLOW	2.2072	2	4.4144
7	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	PANDUIT CAT6 UTP CABLE 300M	120.1064	8	960.8512
8	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	LEGRAND MOSAIC ΠΡΙΖΑ ΔΙΚΤΥΟΥ ΓΙΑ ΚΑΝΑΛΙ CAT6	8.1026	7	56.7182
9	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	ROLINE UTP 1M CABLE CAT6 RED	2.5048	4	10.0192
10	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	INTELLINET PATCH PANEL 24 PORT CAT6 UTP	29.99	6	179.94
11	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 3M CABLE CAT6 BLUE	2.5048	11	27.5528
12	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 3M CABLE CAT6 WHITE	2.5048	6	15.0288
13	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 2M CABLE CAT6 YELLOW	1.798	14	25.172
14	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 1M CABLE CAT6 RED	1.2028	10	12.028
15	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	VALUE UTP 3M CABLE CAT6 BLACK	2.5048	10	25.048
16	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	RACK SCREWS & CAGE NUTS	15.004	1	15.004
17	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	INTELLINET UTP 0.25M CABLE CAT6 YELLOW	0.7936	10	7.936
18	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	ΚΕΝΟ PANEL 1U	2.74	10	27.4
19	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	ΕΠΙΤΟΙΧΙΟ ΗΛΕΚΤΡΟΛΟΓΙΚΟ ΚΟΥΤΙ	1.395	10	13.95
20	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	RACK 12U	189	2	378
21	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	UBIQUITI EDGEROUTER RACKMOUNT KIT	26.8	1	26.8
22	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	CABLE ENTRY BRUSH PANEL	12	2	24
23	ΠΑΘΗΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ	ΡΑΦΙ ΓΙΑ RACK 1U	16.6	1	16.6
1	SERVER	ΚΟΥΤΙ FRACTAL DESIGN DEFINE XL R2	156.88	1	156.88
2	SERVER	ΜΗΤΡΙΚΗ ASROCK X570D4U	396	1	396
3	SERVER	ΕΠΕΞΕΡΓΑΣΤΗΣ AMD RYZEN 9-3900X	419	1	419
4	SERVER	RAM KINGSTON SERVER PREMIER 32GBx2 DDR4 ECC	102	2	204
5	SERVER	ΨΥΚΤΡΑ COOLERMASTER HYPER 212	38	1	38
6	SERVER	SSD SAMSUNG 870 EVO 1TB	113.75	4	455
7	SERVER	HDD SEAGATE IRONWOLF PRO 4TB	124	2	248
8	SERVER	ΤΡΟΦΟΔΟΤΙΚΟ CORSAIR 750W	144	1	144
9	SERVER	ΚΑΡΤΑ ΔΙΚΤΥΟΥ 2xSFP+ 10G	233	1	233

Το συνολικό κόστος ανέρχεται στην τιμή των 10315 ευρώ.

ΚΕΦΑΛΑΙΟ 4 Φάσεις Υλοποίησης Δικτυακής Υποδομής

Γενική Περιγραφή 4.1

Μετά την ολοκλήρωση του σχεδιασμού της ενσύρματης και ασύρματης υποδομής και την αποδοχή της τεχνοοικονομικής μελέτης έφτασε η στιγμή της υλοποίησης του έργου. Η υλοποίηση πραγματοποιήθηκε σε διακριτά στάδια:

- Εγκατάσταση Ικριωμάτων
- Στερέωση Σχαρών Καλωδίων πάνω στις οποίες θα κυκλοφορούν τα UTP καλώδια και οι οπτικές ίνες από και προς τις αίθουσες και τα ικριώματα.
- Στερέωση πλαστικών σωλήνων και περιβλημάτων των πριζών δικτύου στους τοίχους.
- Στερέωση πλαστικών σωλήνων στις σχάρες για την προστασία των οπτικών ινών στη διαδρομή τους από το κεντρικό ικρίωμα προς τα δύο περιφερειακά στα εργαστήρια Πληροφορικής.
- Διέλευση των καλωδίων οπτικών ινών από το κεντρικό rack μέσω των πλαστικών σωληνώσεων στα περιφερειακά.
- Διέλευση των καλωδίων UTP από τις πρίζες δικτύου μέχρι τα ικριώματα στα οποία αντιστοιχούν
- Εγκατάσταση των patch panels στα τρία rack και τερματισμός των καλωδίων UTP πάνω σε αυτά.
- Εγκατάσταση των πριζών στις θέσεις που είχαν τοποθετηθεί τα περιβλήματα τους και τερματισμός των καλωδίων UTP σε αυτές.
- Δοκιμές της σωστής σύνδεσης των καλωδίων με τη χρήση δοκιμαστικού εργαλείου.
- Εγκατάσταση του ενεργού εξοπλισμού στο κεντρικό και περιφερειακά ικριώματα.
- Ηλεκτρική και δικτυακή διασύνδεση του ενεργού εξοπλισμού
- Παραμετροποίηση του ενεργού εξοπλισμού
- Δοκιμές Χρήσης και διόρθωση προβλημάτων που προέκυψαν.

Εγκατάσταση Ικριωμάτων 4.2

Το πρώτο βήμα της υλοποίησης ήταν η εγκατάσταση των ικριωμάτων στα οποία και θα στερεωνόταν ο ενεργός και παθητικός εξοπλισμός καθώς και θα τερματίζονταν τα καλώδια χαλκού και οπτικών ινών. Τα τρία ικριώματα εγκαταστάθηκαν στον αποθηκευτικό χώρο κοντά στο γραφείο της Διεύθυνσης καθώς και στα δύο εργαστήρια Πληροφορικής. Στα συγκεκριμένα ικριώματα εγκαταστάθηκε και σύστημα εξαερισμού για την απαγωγή της θερμότητας από τον ενεργό εξοπλισμό καθώς και σύστημα τροφοδοσίας με ρεύμα προστατευμένο από υπερτάσεις.

Εικόνα 9: Νέο Ικρίωμα Εργαστηρίου Β

Εικόνα 10: Νέο κεντρικό Ικρίωμα

Εγκατάσταση Σχαρών Καλωδίων 4.3

Για την στήριξη των καλωδίων στους διαδρόμους, στη διαδρομή από τα ικριώματα μέχρι τις πρίζες, επιλέχθηκε να χρησιμοποιηθούν σχάρες καλωδίων. Οι συγκεκριμένες σχάρες στηρίχθηκαν στην οροφή των διαδρόμων με τη χρήση κατάλληλων ντιζών, ενώ ενώθηκαν μεταξύ τους με μεταλλικούς συνδέσμους. Για τα σημεία που υπάρχουν γωνίες χρησιμοποιήθηκαν γωνιακοί σύνδεσμοι ενώ στα σημεία που τα καλώδια μεταβαίνουν από την σχάρα στις οπές των τοίχων και στα ικριώματα τοποθετήθηκαν πλαστικές καμπύλες για να αποφευχθεί πιθανή φθορά.

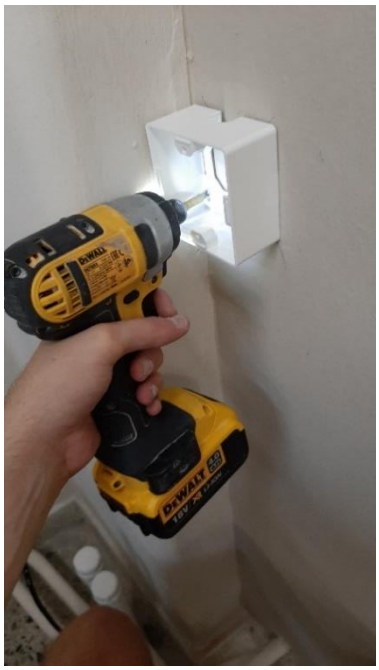
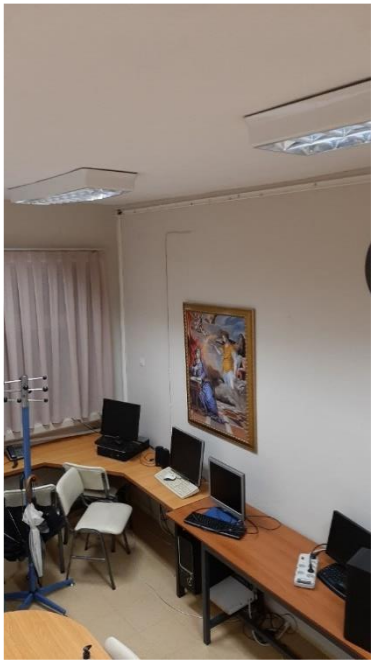


Εικόνα 11, 12, 13: Εγκατάσταση Σχαρών Καλωδίων

Εγκατάσταση Πλαστικών Σωλήνων και Περιβλημάτων Πριζών Δικτύου 4.4

Στη διαδρομή από τις σχάρες μέχρι τις πρίζες δικτύου χρησιμοποιήθηκαν τόσο κανάλια καλωδίων όσο και πλαστικοί σωλήνες σε συνδυασμό με γωνίες και σπιράλ στα σημεία που υπάρχουν καμπύλες. Ο λόγος που συνέβη αυτό είναι εξαιτίας της ανάγκης προστασίας των καλωδίων από φθορά τόσο από περιβαλλοντικούς παράγοντες όπως σκόνη όσο και από βανδαλισμό. Επιπρόσθετα, έτσι επιτυγχάνεται πιο οργανωμένη διαχείριση των καλωδίων και το βέλτιστο οπτικό αποτέλεσμα. Για την πιστοποίηση ότι οι σωλήνες και τα κανάλια έχουν βιδωθεί στην ευθεία και δε παρουσιάζουν κυρτώσεις χρησιμοποιήθηκε ειδικό αλφάδι με δέσμη laser. Η χρήση σωλήνων προτιμήθηκε στις αίθουσες που μέσα από κάθε σωλήνα μεταβαίνουν 2 ή 3 UTP καλώδια, ενώ στα γραφεία των εκπαιδευτικών που συχνά χρειάζεται να περάσουν από το ίδιο σημείο μέχρι και 12 καλώδια, επιλέχτηκαν κανάλια καλωδίων με το κατάλληλο πλάτος. Με την ολοκλήρωση της συγκεκριμένης

διαδικασίας στερεώθηκαν στις άκρες από τους σωλήνες και τα κανάλια τα πλαστικά πλαίσια στα οποία στην συνέχεια θα τοποθετούνταν οι πρίζες δικτύου.

Εικόνες 14, 15, 16: Εγκατάσταση καναλιών διέλευσης καλωδίων και πλαισίων πριζών δικτύου.

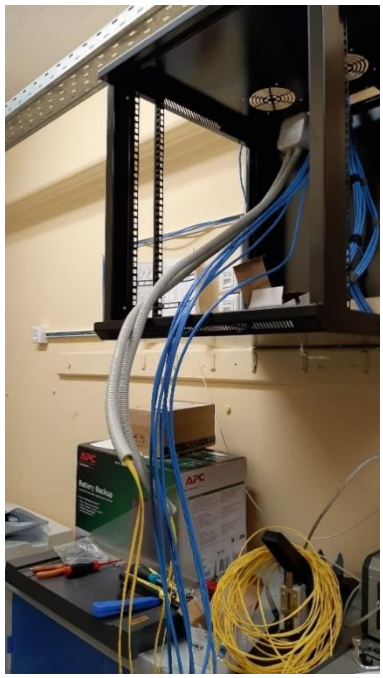
Εγκατάσταση Σωληνώσεων Διέλευσης Οπτικών Ινών στις σχάρες 4.5

Τα δύο ικριώματα στα εργαστήρια Πληροφορικής συνδέονται με το κεντρικό ικρίωμα με τη χρήση διπλών καλωδίων οπτικών ινών. Τα συγκεκριμένα οπτικά καλώδια χρησιμοποιούν τις σχάρες που αναρτήθηκαν στους διαδρόμους για τη διέλευση τους. Με σκοπό την προστασία τους από φθορές κατά τη διάρκεια διέλευσης των καλωδίων χαλκού πάνω στις σχάρες αλλά και στο μέλλον, λόγω και της ευθραυστότητας που τις διακρίνει, προτιμήθηκε να στερεωθούν στο εσωτερικό των σχαρών πλαστικοί σωλήνες, ίδιοι με αυτούς που χρησιμοποιήθηκαν για τη διέλευση των καλωδίων χαλκού από τις σχάρες μέχρι τις πρίζες δικτύου. Στην συνέχεια, με τη χρήση κατάλληλων πλαστικών στηριγμάτων, οι συγκεκριμένοι σωλήνες στερεώθηκαν πάνω στο μεταλλικό πλαίσιο με σκοπό την αποφυγή μετακινήσεων τους.

Διέλευση των Καλωδίων Οπτικών Ινών από το Κεντρικό Ικρίωμα στα Περιφερειακά 4.6

Μετά την στερέωση των σωλήνων για τις οπτικές ίνες επάνω στις σχάρες, έπρεπε να γίνει η διέλευση των ζευγών οπτικών ινών από αυτούς. Η διέλευση έγινε σταδιακά μέσα από κάθε σωλήνα και σύνδεσμο και στην συνέχεια οι δύο

σωλήνες ενώνονταν μεταξύ τους με τη χρήση του συγκεκριμένου συνδέσμου. Παράλληλα μαζί με το κάθε ζεύγος οπτικών ινών εγκαταστάθηκε και κομμάτι σπάγκου από το κεντρικό ικρίωμα προς τα δύο περιφερειακά. Η συγκεκριμένη ενέργεια έγινε ώστε να είναι πιο εύκολη η μελλοντική διέλευση ενός νέου οπτικού καλωδίου, η αντικατάσταση κάποιου άλλου χαλασμένου χωρίς να είναι απαραίτητη αποσυναρμολόγηση των ενώσεων των πλαστικών σωλήνων. Με την άφιξη της οπτικής ίνας στο εκάστοτε ικρίωμα, αυτή τοποθετήθηκε σε πλαστικό spiral μέχρι τις θύρες του διαμεταγωγέα, με σκοπό την προστασία της κατά τις παρεμβάσεις στο εσωτερικό του ικριώματος. Στο τέλος όλα τα ζεύγη οπτικών ινών δοκιμάστηκαν με την προσωρινή σύνδεση τους σε διαμεταγωγείς με σκοπό ότι επιτυγχάνεται η ταχύτητα σύνδεσης που αναμένεται και δεν υπήρξε κάποια θραύση των ινών κατά τη διάρκεια της εγκατάστασης.

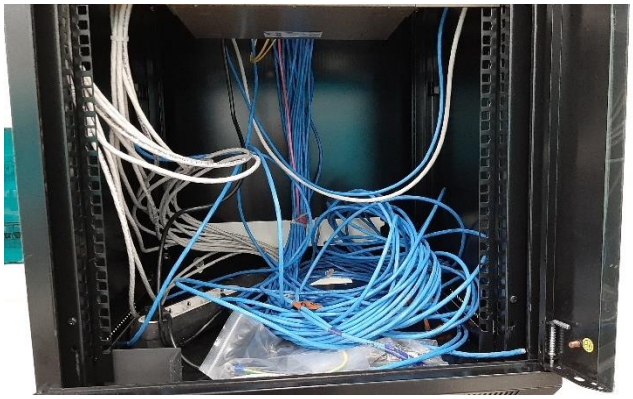



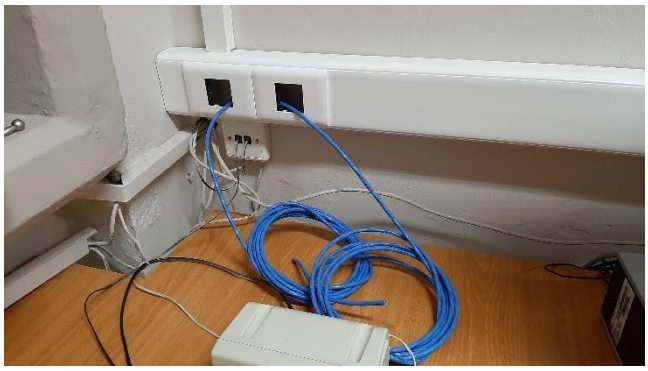

Εικόνες 17, 18, 19: Διέλευση Οπτικών Ινών από το κεντρικό Ικρίωμα προς τα περιφερειακά

Διέλευση των Καλωδίων UTP από τις Πρίζες Δικτύου μέχρι τα Ικριώματα 4.7

Μόλις ολοκληρώθηκε η διέλευση των οπτικών ινών από τους σωλήνες και προς τα περιφερειακά ικριώματα, επόμενο στάδιο της εγκατάστασης ήταν η διέλευση των καλωδίων από τις πρίζες δικτύου προς το ικρίωμα που αντιστοιχεί η κάθε μία μέσω των πλαστικών σωλήνων που εγκαταστάθηκαν στους τοίχους και των σχαρών που εγκαταστάθηκαν στις οροφές των διαδρόμων. Επιλέχθηκε η διέλευση να γίνει με αυτό τον τρόπο καθώς θα ήταν πιο εύκολο να υπολογιστεί πόσο μήκος καλωδίου θα χρειαστεί και επιπλέον τα καλώδια θα συναντούσαν λιγότερη τριβή και εμπόδια όπως γωνίες και στενές οπές από αυτές που θα συναντούσαν αν η διαδρομή πραγματοποιούνταν από τα ικριώματα προς τις πρίζες δικτύου. Το όνομα των πριζών δικτύου σημαδεύτηκε επάνω στα ζευγάρια πριν αυτά τοποθετηθούν στο

εσωτερικό των σωλήνων και ξεκινήσουν τη διαδρομή τους μέχρι το κατάλληλο ικρίωμα. Το ίδιο συνέβη και στην αντίθετη άκρη των ζευγών καλωδίων για κάθε διπλή πρίζα δικτύου. Δόθηκε ιδιαίτερη προσοχή ώστε να αφεθεί μεγάλη ποσότητα καλωδίου, περίπου δύο μέτρα από την πλευρά του ικριώματος και ένα μέτρο από την πλευρά της πρίζας δικτύου. Αυτό έγινε με σκοπό την διόρθωση τυχόν λάθους κατά τον τερματισμό του καλωδίου στην πρίζα δικτύου και στο patch panel, την καλύτερη οργάνωση των καλωδίων αλλά και την πρόβλεψη πιθανής αντικατάστασης του ικριώματος.





Εικόνες 20, 21, 22: Διέλευση καλωδίων UTP από τα ικριώματα προς τις πρίζες δικτύου

Εγκατάσταση των Patch Panels στα Τρία Ικριώματα και Τερματισμός των Καλωδίων UTP σε αυτά 4.8

Μετά την ολοκλήρωση της διέλευσης των καλωδίων μέχρι τα ικριώματα, επόμενο βήμα ήταν η οργάνωση των καλωδίων μέσα σε αυτά. Τα καλώδια χωρίστηκαν σε συστάδες καλωδίων με βάση το πιο patch panel θα τερματίζονταν. Προτιμήθηκε η τακτική κάθε patch panel να εξυπηρετεί έναν διαμεταγωγέα. Οι μονοί αριθμοί πριζών να τερματιστούν όλοι σε ένα patch panel, σε κάθε ικρίωμα, ενώ οι ζυγοί αριθμοί πριζών να τερματιστούν σε ένα άλλο. Αυτό συνέβη ώστε αν κάποιος διαμεταγωγέας σταματήσει να λειτουργεί λόγω βλάβης, να μη διακοπεί η πρόσβαση και στις δύο πόρτες μίας πρίζας δικτύου αλλά μόνο σε μία. Εξαίρεση αποτελούν οι πρίζες που εξυπηρετούν Access Points. Στην συγκεκριμένη

περίπτωση, οι πρίζες δικτύου πρέπει να καταλήγουν σε διαμεταγωγέα που να μπορεί να παρέχει και τροφοδοσία ρεύματος, οπότε η συγκεκριμένη ομάδα πριζών καταλήγει στο ίδιο patch panel. Οι συστάδες καλωδίων στην συνέχεια οργανώθηκαν με την χρήση Velcro δεματικών ώστε να μπορούν να μετακινηθούν πιο εύκολα. Τέλος, τα καλώδια τερματίστηκαν στα patch panels με βάση τον χρωματικό κώδικα και τα patch panels βιδώθηκαν στις κατάλληλες θέσεις στο ικρίωμα. Το καλώδιο που περισσεύει μαζεύτηκε στο εσωτερικό του ικριώματος με οργανωμένο τρόπο με σκοπό να μην παρεμποδίζει τη μετακίνηση του αέρα.

Εικόνες 23, 24, 25:Οργάνωση UTP καλωδίων και τερματισμός στα patch panels

Εγκατάσταση των Πριζών Δικτύου και Τερματισμός των καλωδίων σε αυτές 4.9

Στην συνέχεια πραγματοποιήθηκε ο τερματισμός των καλωδίων στις διπλές πρίζες δικτύου αλλά και στις πρίζες δικτύου που εξυπηρετούν τα Access Points, στις οροφές των αιθουσών με βάση τον χρωματικό κώδικα. Δόθηκε μέριμνα ώστε να αφεθεί περίσσια καλωδίου στο εσωτερικό του περιβλήματος πάνω στο οποίο καταλήγει η συγκεκριμένη πρίζα με σκοπό την ευκολότερη αντικατάσταση της σε μελλοντικό χρόνο σε περίπτωση βλάβης.

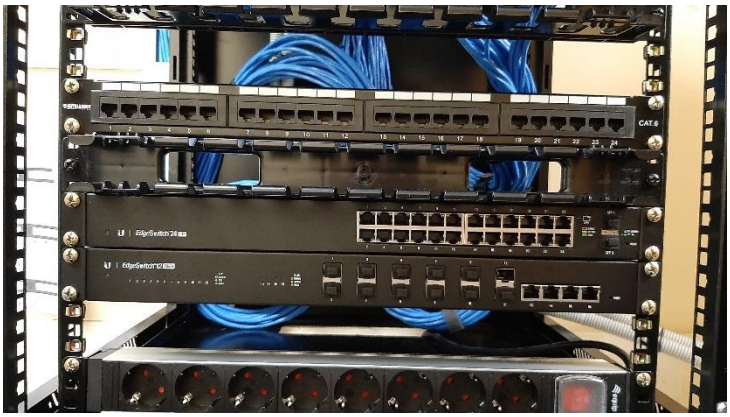
Εικόνες 26, 27: Τερματισμός καλωδίων UTP στις πρίζες δικτύου.

Δοκιμή Συνδέσεων με την χρήση Δοκιμαστικού Εργαλείου 4.10

Μόλις ολοκληρώθηκε ο τερματισμός των καλωδίων τόσο στα patch panels, όσο και στις πρίζες δικτύου έπρεπε να γίνει η δοκιμή των καλωδίων με σκοπό τον εντοπισμό λαθών και ελαττωματικών συνδέσεων. Οι δοκιμές έγιναν με κατάλληλο εργαλείο το οποίο συνδέεται και στα δύο άκρα της σύνδεσης, στην πρίζα δικτύου και στην αντίστοιχη πόρτα του patch panel και ελέγχει την ηλεκτρολογική συνέχεια και των οχτώ καλωδίων που διέρχονται μέσα από ένα UTP καλώδιο. Βρέθηκαν κάποιες ελαττωματικές συνδέσεις οι οποίες και διορθώθηκαν. Ακολούθησε επανέλεγχος των συγκεκριμένων συνδέσεων με σκοπό την διαβεβαίωση ότι το πρόβλημα έχει επιδιορθωθεί. Παράλληλα με τον έλεγχο των συνδέσεων έγινε και η σήμανση των πριζών δικτύου και των αντίστοιχων πορτών στα patch panels με τη χρήση ετικετογράφου. Οι διπλές πρίζες δικτύου σημάνθηκαν με το μοτίβο sXX.pYY όπου XX είναι ένας αύξοντας αριθμός της πρίζας και YY το νούμερο 1 ή 2 που δείχνει αν είναι η αριστερή ή δεξιά πόρτα αντίστοιχα. Στις μονές πρίζες δικτύου χρησιμοποιήθηκε μόνο το τμήμα sXX που είναι ο αύξοντας αριθμός της πρίζας

Εγκατάσταση του Ενεργού Εξοπλισμού στα Ικριώματα 4.11

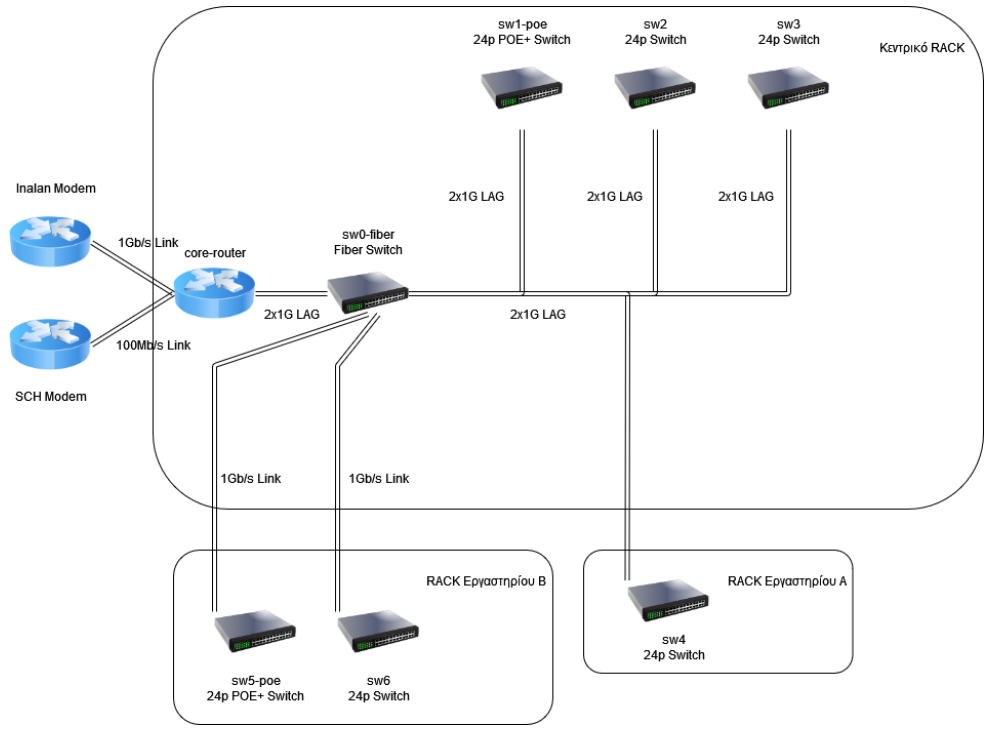
Με την ολοκλήρωση της εγκατάστασης του παθητικού εξοπλισμού στα ικριώματα ακολούθησε η εγκατάσταση του ενεργού εξοπλισμού. Στα περιφερειακά ικριώματα των δύο εργαστηρίων εγκαταστάθηκαν συνολικά τρεις διαμεταγωγείς. Πιο συγκεκριμένα στο ικρίωμα του εργαστηρίου Α εγκαταστάθηκε ένας διαμεταγωγέας και δύο PoE Injectors για τα δύο Access Points που εξυπηρετούνται από το συγκεκριμένο ικρίωμα. Στο ικρίωμα του Εργαστηρίου Β εγκαταστάθηκαν δύο διαμεταγωγείς εκ των οποίων ο ένας μπορεί να παρέχει και τροφοδοσία ρεύματος μέσω του καλωδίου UTP. Στο κεντρικό ικρίωμα εγκαταστάθηκε ο κεντρικός δρομολογητής, ο οπτικός διαμεταγωγέας που διασυνδέει τους μεταγωγείς πρόσβασης και τρεις διαμεταγωγείς πρόσβασης εκ των οποίων ο ένας μπορεί να παρέχει και τροφοδοσία ρεύματος μέσω του καλωδίου UTP. Ακόμη, πλησίον του ικριώματος εγκαταστάθηκε και ο εξοπλισμός του οπτικού παρόχου διαδικτύου καθώς και του Πανελλήνιου Σχολικού Δικτύου.



Εικόνες 28, 29, 30: Εγκατάσταση ενεργού εξοπλισμού στα Ικριώματα

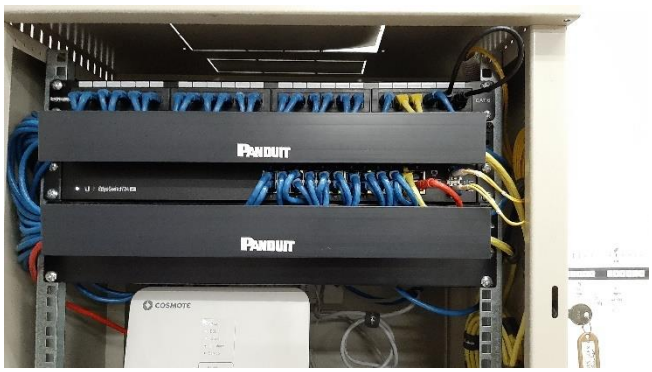
Ηλεκτρική και Δικτυακή Διασύνδεση του Ενεργού Εξοπλισμού 4.12

Με την ολοκλήρωση της εγκατάστασης του ενεργού εξοπλισμού έπρεπε να γίνει η διασύνδεση ανάμεσα στα διάφορα τμήματα που το απαρτίζουν. Αρχικά ο κεντρικός δρομολογητής συνδέθηκε με δύο από τις τέσσερις διεπαφές Ethernet του οπτικού διαμεταγωγέα. Ακόμη συνδέθηκε με το modem του Πανελλήνιου Σχολικού Δικτύου και του εμπορικού παρόχου. Στην συνέχεια ο οπτικός διαμεταγωγέας συνδέθηκε με τους τρεις διαμεταγωγείς που βρίσκονται επίσης στο κεντρικό ικρίωμα με τη χρήση ενός ζεύγους οπτικών ινών στο καθένα. Στην συνέχεια ο οπτικός διαμεταγωγέας συνδέθηκε με τον διαμεταγωγέα στο ικρίωμα του εργαστηρίου Α. Τέλος ο οπτικός διαμεταγωγέας συνδέθηκε με τους δύο διαμεταγωγείς στο εργαστήριο Β με μία οπτική ίνα στο κάθε ένα. Οι διασυνδέσεις φαίνονται και στο παρακάτω διάγραμμα.



Εικόνα 31: Διάγραμμα Διασυνδέσεων

Στην συνέχεια έγινε η διασύνδεση των διαμεταγωγέων χαλκού με το patch panel που αντιστοιχεί στον καθένα. Δημιουργήθηκε ένα σχεδιάγραμμα που να δείχνει ποια θύρα του εκάστοτε διαμεταγωγέα αντιστοιχεί σε ποια πόρτα του patch panel. Χρησιμοποιήθηκαν προτερματισμένα καλώδια UTP μήκους ενός μέτρου ενώ τηρήθηκε και ένας βασικός χρωματικός κώδικας. Πιο συγκεκριμένα, στις πόρτες που θα εξυπηρετούν εκτυπωτές και φωτοτυπικά χρησιμοποιήθηκαν μαύρα καλώδια, στις πόρτες που θα εξυπηρετούν σημεία πρόσβασης στο WiFi κίτρινα καλώδια, στις πόρτες που θα εξυπηρετούν στο μέλλον τηλεφωνία IP άσπρα καλώδια και σε όλες τις υπόλοιπες πόρτες μπλε καλώδια. Τα καλώδια οργανώθηκαν με τη χρήση οδηγών καλωδίων με σκοπό την ευκολότερη διαχείριση τους και την βελτίωση της ψύξης του ενεργού εξοπλισμού. Το τελικό αποτέλεσμα φαίνεται στις παρακάτω εικόνες.



Εικόνες 32, 33, 34: Τελικό αποτέλεσμα Ικριωμάτων

Παραμετροποίηση του Ενεργού Εξοπλισμού 4.13

Σε συνέχεια της εγκατάστασης και διασύνδεσης του ενεργού εξοπλισμού έπρεπε να γίνει η παραμετροποίηση του με σκοπό την σωστή δρομολόγηση των πακέτων και την εφαρμογή των πολιτικών ασφαλείας. Η συγκεκριμένη παραμετροποίηση έγινε σε στάδια τα οποία είναι τα εξής:

- Παραμετροποίηση του κεντρικού δρομολογητή
- Παραμετροποίηση του οπτικού διαμεταγωγέα
- Παραμετροποίηση των διαμεταγωγέων χαλκού

- Εγκατάσταση συστήματος Hypervisor για την υποστήριξη εικονικών μηχανών
- Εγκατάσταση του ελεγκτή του ασύρματου δικτύου και παραμετροποίηση των σημείων πρόσβασης

Παραμετροποίηση του κεντρικού δρομολογητή 4.13.1

Ο κεντρικός δρομολογητής διαθέτει πέντε διεπαφές χαλκού με την ονομασία από eth0 έως eth4 και μία διεπαφή οπτικής ίνας με την ονομασία eth5. Στην υλοποίηση χρησιμοποιήθηκαν οι πέντε διεπαφές χαλκού. Στη διεπαφή eth0 συνδέθηκε το modem του εμπορικού παρόχου ενώ στην διεπαφή eth1 συνδέθηκε το modem του Πανελλήνιου Σχολικού Δικτύου. Ο εμπορικός πάροχος χρησιμοποιεί το πρωτόκολλο dhcp για τον διαμοιρασμό IP διευθύνσεων οπότε ο κεντρικός δρομολογητής λειτουργεί ως dhcp client στη διεπαφή eth0. Αντιθέτως το Πανελλήνιο Σχολικό Δίκτυο χρησιμοποιεί το πρωτόκολλο PPPoE για τη δημιουργία tunnel και τον διαμοιρασμό διευθύνσεων οπότε ο κεντρικός δρομολογητής ρυθμίστηκε να πραγματοποιεί κλήση PPPoE από τη διεπαφή eth1. Έτσι δημιουργείται μια νέα ιδεατή διεπαφή με την ονομασία pppoe0.

Οι διεπαφές eth3 και eth4 χρησιμοποιούνται για τη διασύνδεση με τον οπτικό διαμεταγωγέα, Οι δύο αυτές φυσικές διεπαφές ρυθμίστηκαν ως μια ιδεατή διεπαφή με τη χρήση του πρωτοκόλλου LACP τόσο από την πλευρά του κεντρικού δρομολογητή όσο και από την πλευρά του οπτικού διαμεταγωγέα για λόγους αύξησης του εύρους ζώνης της διασύνδεσης. Η νέα ιδεατή διεπαφή στον κεντρικό δρομολογητή ονομάστηκε bond0. Η συγκεκριμένη ιδεατή διεπαφή απέκτησε την IP 10.33.10.1/24. «Επάνω» στην ιδεατή διεπαφή ρυθμίστηκαν τα 15 από τα 16 VLAN που περιγράφονται στον πίνακα της ενότητας 3.6 ως “tagged vlans”. Το VLAN 10 δεν απαιτεί κάποια επιπλέον ρύθμιση διότι είναι “untagged vlan” Η συγκεκριμένη ρύθμιση δημιούργησε 15 εικονικές διεπαφές της μορφής bond0.XX όπου XX είναι ο αριθμός του VLAN. Ακολούθως οι νέες αυτές διεπαφές απέκτησαν την IP 10.33.XX.1/24 εκτός από το VLAN 140 που απέκτησε την IP 10.33.140.1/22.

Στην συνέχεια ρυθμίστηκαν οι κανόνες NAT/PAT για το δίκτυο. Πιο συγκεκριμένα, επειδή από το ΠΣΔ και τον εμπορικό πάροχο παρέχεται μία μόνο IP, ενώ στο εσωτερικό του δικτύου φιλοξενούνται εκατοντάδες δικτυακές συσκευές, για να μπορέσει να πραγματοποιηθεί επιτυχής σύνδεση με το υπόλοιπο διαδίκτυο πρέπει ο κεντρικός δρομολογητής να υλοποιήσει μια διαδικασία μετάφρασης της διεύθυνσης πηγής (source address) του εκάστοτε πακέτου από την εσωτερική IP στην εξωτερική IP της διεπαφής του παρόχου που επιθυμούμε να χρησιμοποιεί το εκάστοτε VLAN. Ακόμη πρέπει να υλοποιηθεί και μια διαδικασία μετάφρασης των πορτών πηγής (source ports) σε κάποιες άλλες, δυναμικά καθορισμένες από τον κεντρικό δρομολογητή. Η ανάποδη διαδικασία πρέπει να συμβεί κατά την επιστροφή του πακέτου στο δίκτυο. Η συγκεκριμένη λειτουργία έγινε εφικτή με τη ρύθμιση δύο κανόνων NAT/PAT (Network Address Translation/Port Address Translation). Πιο συγκεκριμένα, σε όσα πακέτα κατευθύνονται στο διαδίκτυο μέσω του εμπορικού παρόχου, θα γίνεται μετάφραση της διεύθυνσης πηγής με τη διεύθυνση της διεπαφής eth0 και σε τυχαία πηγαία πόρτα. Σε όσα πακέτα κατευθύνονται στο διαδίκτυο μέσω του Πανελλήνιου Σχολικού Δικτύου θα γίνεται

μετάφραση της διεύθυνσης πηγής με τη διεύθυνση της διεπαφής pppoe0 και σε τυχαία πηγαία πόρτα.

Μετέπειτα έπρεπε να γίνει η ρύθμιση του DHCP Server ο οποίος είναι υπεύθυνος για τον διαμοιρασμό IP στις συσκευές που συνδέονται στο δίκτυο. Πέρα από τη διεύθυνση IP τους ενημερώνει και για την IP του δρομολογητή που πρέπει να χρησιμοποιήσουν, την μάσκα υποδικτύου καθώς και τις IP από τους DNS Servers. Ο DHCP Server αποφασίστηκε να χρησιμοποιηθεί για τα 14 από τα 16 VLANs της υποδομής και να εξαιρεθούν το VLAN 10 που είναι για τη διαχείριση του δικτυακού εξοπλισμού και το VLAN 20 που είναι για τους εξυπηρετητές, στα οποία δίκτυα η απόδοση διευθύνσεων χρειάζεται να γίνει χειροκίνητα. Οι αναλυτικές ρυθμίσεις του DHCP Server φαίνονται στον ακόλουθο πίνακα.

VLAN	ROUTER	START ADDRESS	END ADDRESS	PRIMARY DNS	SECONDARY DNS	LEASE TIME
30	10.33.30.1/24	10.33.30.235	10.33.30.254	1.1.1.1	1.0.0.1	24h
40	10.33.40.1/24	10.33.40.235	10.33.40.254	1.1.1.1	1.0.0.1	24h
50	10.33.50.1/24	10.33.50.235	10.33.50.254	1.1.1.1	1.0.0.1	24h
60	10.33.60.1/24	10.33.60.235	10.33.60.254	1.1.1.1	1.0.0.1	24h
70	10.33.70.1/24	10.33.70.235	10.33.70.254	1.1.1.1	1.0.0.1	24h
80	10.33.80.1/24	10.33.80.235	10.33.80.254	1.1.1.1	1.0.0.1	24h
90	10.33.90.1/24	10.33.90.235	10.33.90.254	1.1.1.1	1.0.0.1	24h
100	10.33.100.1/24	10.33.100.235	10.33.100.254	1.1.1.1	1.0.0.1	24h
110	10.33.110.1/24	10.33.110.235	10.33.110.254	1.1.1.1	1.0.0.1	24h
120	10.33.120.1/24	10.33.120.2	10.33.120.254	1.1.1.1	1.0.0.1	6h
130	10.33.130.1/24	10.33.130.2	10.33.130.254	1.1.1.1	1.0.0.1	6h
140	10.33.140.1/22	10.33.140.2	10.33.143.254	1.1.1.1	1.0.0.1	6h
150	10.33.150.1/24	10.33.150.235	10.33.150.254	1.1.1.1	1.0.0.1	6h

Όπως φαίνεται και στον πίνακα, πέρα από τα VLANs 120, 130 και 140 στα οποία γίνεται διευθυνσιοδότηση σε όλο το διαθέσιμο εύρος διευθύνσεων, στα υπόλοιπα VLANs γίνεται διευθυνσιοδότηση μόνο σε ένα εύρος 20 διευθύνσεων. Ο λόγος που συμβαίνει αυτό είναι γιατί θα γίνουν δεσμεύσεις στατικών διευθύνσεων τοπικά και η δικτυακή συσκευή χρειάζεται μόνο να πάρει μια προσωρινή IP μέχρι να αποδοθεί μία στατική. Ακόμη σε VLANs που δε γίνεται συχνή σύνδεση νέων χρηστών προτιμήθηκε η διάρκεια του lease να είναι 1 μέρα ενώ στα υπόλοιπα 6 ώρες.

Μετά τη δημιουργία των κανόνων NAT/PAT και τη ρύθμιση του DHCP Server ακολούθησε η ρύθμιση του συστήματος δρομολόγησης με βάση πολιτικών (Policy Based Routing). Πιο συγκεκριμένα, με σκοπό να επιτευχθεί η δυνατότητα επιλογής διαφορετικού παρόχου σύνδεσης στο διαδίκτυο ανά VLAN, πρέπει να δημιουργηθούν κάποιοι κανόνες που θα ορίζουν με βάση ποιον πίνακα δρομολόγησης θα δρομολογηθούν τα πακέτα. Έτσι αρχικά δημιουργήθηκαν δύο νέοι πίνακες δρομολόγησης, πλέον του πίνακα δρομολόγησης “main” ο οποίος ήδη υπάρχει στον δρομολογητή. Ο πίνακας δρομολόγησης “com_isp” στον οποίο ορίστηκε ένα νέο “default route” το οποίο στέλνει τα πακέτα προς τη διεπαφή eth0 και ο πίνακας δρομολόγησης “sch_isp” στον οποίο ορίστηκε ένα νέο “default route” το οποίο στέλνει τα πακέτα προς την διεπαφή pppoe0. Στην συνέχεια δημιουργήθηκε η εξής πολιτική: Όσα πακέτα έχουν διεύθυνση προορισμού κάποιο

από τα 16 VLAN χρησιμοποιούν τον πίνακα δρομολόγησης “main”. Ο συγκεκριμένος κανόνας υπάρχει για να μπορούν τα VLANs να επικοινωνούν εσωτερικά μεταξύ τους. Στην συνέχεια, στα VLAN 90 και 100 τα οποία αφορούν τα δύο εργαστήρια Πληροφορικής εφαρμόστηκε η πολιτική τα VLAN να επικοινωνούν με το διαδίκτυο με τη χρήση του Πανελλήνιου Σχολικού Δικτύου μέσω του πίνακα δρομολόγησης “sch_isp”. Στα υπόλοιπα VLANs εφαρμόστηκε η πολιτική να επικοινωνούν με το διαδίκτυο με τη χρήση του εμπορικού παρόχου μέσω του πίνακα δρομολόγησης “com_isp”. Αυτή είναι η αρχική πολιτική, η οποία στη συνέχεια μπορεί και να τροποποιηθεί ανάλογα με προς ανάγκες του σχολείου. Παρατίθεται πίνακας που αναλύονται οι πολιτικές επιλογής του παρόχου διαδικτύου.

VLAN	**ROUTING TABLE**
10	com_isp
20	com_isp
30	com_isp
40	com_isp
50	com_isp
60	com_isp
70	com_isp
80	com_isp
90	sch_isp
100	sch_isp
110	com_isp
120	com_isp
130	com_isp
140	com_isp
150	com_isp

Τέλος έπρεπε να γίνει ρύθμιση του τείχους προστασίας. Για να γίνει ο προσδιορισμός των κανόνων που πρέπει να τοποθετηθούν σε αυτό έπρεπε να δημιουργηθεί προς πίνακας με 16 σειρές και 16 στήλες. Στην συνέχεια στο συγκεκριμένο πίνακα και με κατεύθυνση από γραμμή προς στήλη σχεδιάσθηκε πιο υποδίκτυο μπορεί να επικοινωνεί με πιο άλλο. Πιο συγκεκριμένα απαγόρευση επικοινωνίας σημειώθηκε με κόκκινο χρώμα, ικανότητα επικοινωνίας σημειώθηκε με πράσινο χρώμα και ικανότητα επικοινωνίας μόνο για συνδέσεις που έχουν ήδη δημιουργηθεί από την απέναντι πλευρά σημειώθηκε με πορτοκαλί χρώμα. Ο πίνακας που προέκυψε είναι ο εξής:

	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150	INET
10	X	YES	NO	NO	NO	REL,EST	REL,EST	NO	NO	NO	NO	NO	REL,EST	NO	REL,EST	NO
20	YES	X	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
30	NO	REL,EST	X	NO	NO	REL,EST	REL,EST	REL,EST	REL,EST	REL,EST	NO	NO	REL,EST	NO	REL,EST	NO
40	NO	REL,EST	NO	X	NO	REL,EST	REL,EST	NO	NO	NO	NO	NO	NO	NO	NO	NO
50	NO	REL,EST	NO	NO	X	REL,EST	REL,EST	NO	NO	NO	NO	NO	NO	NO	NO	NO
60	YES	YES	YES	YES	YES	X	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES
70	YES	YES	YES	YES	YES	YES	X	YES	YES	YES	YES	NO	YES	YES	YES	YES
80	NO	REL,EST	YES	NO	NO	REL,EST	REL,EST	X	NO	NO	NO	NO	NO	NO	NO	YES
90	NO	REL,EST	YES	NO	NO	REL,EST	REL,EST	NO	X	NO	NO	NO	NO	NO	NO	YES
100	NO	REL,EST	YES	NO	NO	REL,EST	REL,EST	NO	NO	X	NO	NO	NO	NO	NO	YES
110	NO	REL,EST	NO	NO	NO	REL,EST	REL,EST	NO	NO	NO	X	NO	NO	NO	NO	YES
120	NO	REL,EST	NO	NO	NO	NO	NO	NO	NO	NO	NO	X	NO	NO	NO	YES
130	NO	YES	YES	NO	NO	REL,EST	REL,EST	NO	NO	NO	NO	NO	X	NO	NO	YES
140	NO	REL,EST	NO	NO	NO	REL,EST	REL,EST	NO	NO	NO	NO	NO	NO	X	NO	YES
150	NO	YES	YES	NO	NO	REL,EST	REL,EST	NO	NO	NO	NO	NO	NO	NO	X	YES

Εικόνα 35: Κανόνες τοίχους προστασίας

Στην συνέχεια και με βάση τον συγκεκριμένο πίνακα δημιουργήθηκαν τα 16 σύνολα από κανόνες του τοίχους προστασίας για καθένα από τα 16 VLANs. Σε κάθε σύνολο από κανόνες, ο πρώτος κανόνας αφορά την έγκριση κίνησης για συνδέσεις που ήδη έχουν δημιουργηθεί ώστε να είναι εφικτή η επιστροφή πακέτων στο εκάστοτε VLAN για συνδέσεις οι οποίες και ξεκίνησαν από αυτό όπως για παράδειγμα επικοινωνία με το διαδίκτυο. Δόθηκε ιδιαίτερη προσοχή ώστε επικοινωνία με υποδίκτυα που αφορούν τη διαχείριση του δικτύου, τους εξυπηρετητές και τα γραφεία της διοίκησης να μπορεί να γίνει μόνο από τα δίκτυα των γραφείων και από το ασύρματο δίκτυο των καθηγητών ενώ να απαγορεύεται από δίκτυα που έχουν πρόσβαση μαθητές και λοιπό προσωπικό όπως είναι τα υποδίκτυα εργαστηρίων, αιθουσών και το ασύρματο δίκτυο των μαθητών. Ο λόγος που συνέβη αυτό είναι το κριτήριο σχεδιασμού που απαιτούσε ελεγχόμενη πρόσβαση σε σταθμούς εργασίας και υποδομές που μπορεί να περιέχουν ευαίσθητες πληροφορίες.

Πραγματοποιήθηκαν δοκιμές σε περιορισμένη κλίμακα και αφού ήταν βέβαιο πως η εσωτερική επικοινωνία αλλά και η πρόσβαση στο διαδίκτυο ήταν εφικτή η διαδικασία προχώρησε στη ρύθμιση του οπτικού διαμεταγωγέα.

Παραμετροποίηση του οπτικού διαμεταγωγέα 4.13.2

Μετά τη ρύθμιση του κεντρικού δρομολογητή, ακολούθησε το επόμενο τμήμα της αλυσίδας πρόσβασης στο δίκτυο που είναι ο οπτικός διαμεταγωγέας ο οποίος παρέχει δικτύωση στους διαμεταγωγείς χαλκού που χρησιμοποιούνται για την πρόσβαση στο δίκτυο με τη χρήση ζευγών οπτικών ινών. Πριν τη ρύθμιση του διαμεταγωγέα, δημιουργήθηκε ένα σχεδιάγραμμα το οποίο και δείχνει για κάθε

μία από τις οπτικές πόρτες και πόρτες χαλκού της συγκεκριμένης συσκευής, την περιγραφή του διαμεταγωγέα που θα συνδεθεί σε αυτή, το VLAN που θα είναι untagged/native στην πόρτα του διαμεταγωγέα και τα VLANs τα οποία είναι tagged στην πόρτα του διαμεταγωγέα. Στην συνέχεια οι δύο πόρτες χαλκού στις οποίες συνδέεται ο κεντρικός δρομολογητής ενώθηκαν με τη χρήση του πρωτοκόλλου LACP με σκοπό να δημιουργηθεί μια ιδεατή πόρτα με αυξημένο εύρος ζώνης. Το ίδιο συνέβη και για τα ζευγάρια οπτικών πορτών στα οποία ήταν συνδεδεμένα οι διαμεταγωγείς sw1-poe, sw2, sw3, sw4. Οι πόρτες στις οποίες συνδέονται το sw5-poe και το sw6 δεν αποτελούν LAG[9]. Στην συγκεκριμένη πόρτα ορίστηκε ως untagged/native το VLAN 10 και ως tagged τα υπόλοιπα 15 VLANs. Παρακάτω παρατίθεται ο πίνακας βάση του οποίου έγινε η ρύθμιση του οπτικού διαμεταγωγέα.

PORT NUMBER	PORT DESCRIPTION	PORT GROUP	TAGGED VLAN	UNTAGGED VLAN
0/1	sw5-poe		30,100,110,120,130,140,150	10
0/2	sw6		100,110,120	10
0/3	sw1-poe	1	40,110,120,130,140,150	10
0/4	sw1-poe	1	40,110,120,130,140,150	10
0/5	sw2	2	30,60,70,80,90,100,110,120	10
0/6	sw2	2	30,60,70,80,90,100,110,120	10
0/7	sw3	3	30,60,70,80,90,100,110,120	10
0/8	sw3	3	30,60,70,80,90,100,110,120	10
0/9	sw4	4	90,110,120,130,140,150	10
0/10	sw4	4	90,110,120,130,140,150	10
0/11				
0/12				
0/13	Server			20
0/14				
0/15	core-router	5	20,30,40,50,60,70,80,90,100,110,120,130,140,150	10
0/16	core-router	5	20,30,40,50,60,70,80,90,100,110,120,130,140,150	10

[9] LAG: Link Aggregation Group, σύνολο από φυσικές θύρες που αποτελούν μια ιδεατή θύρα με την χρήση του πρωτοκόλλου LACP.

Παραμετροποίηση των διαμεταγωγέων χαλκού 4.13.3

Αφότου ολοκληρώθηκε η παραμετροποίηση του οπτικού διαμεταγωγέα, ακολούθησαν οι ρυθμίσεις των διαμεταγωγέων χαλκού. Αρχικά ρυθμίστηκαν οι οπτικές διεπαφές με τις οποίες συνδέεται ο κάθε διαμεταγωγέας με τον οπτικό διαμεταγωγέα. Στους διαμεταγωγείς sw1-poe, sw2, sw3 και sw4 ρυθμίστηκαν τα groups από πόρτες με τη χρήση του πρωτοκόλλου LACP μιας και οι συγκεκριμένοι διαμεταγωγείς συνδέονται με τη χρήση ζεύγους και όχι μονής οπτικής ίνας. Στην συνέχεια ρυθμίστηκαν τα vlans τα οποία πρέπει να είναι tagged και untagged/native στις συγκεκριμένες διεπαφές με βάση και τον πίνακα που παρατίθεται στην ενότητα 3.13.2. Με την ολοκλήρωση της συγκεκριμένης παραμετροποίησης, έγινε αντιστοίχηση των είκοσι τεσσάρων διεπαφών κάθε διαμεταγωγέα με το untagged vlan στο οποίο ανήκουν. Σε συγκεκριμένες διεπαφές στους διαμεταγωγείς sw1-poe, sw4 και sw5-poe συνδέονται σημεία πρόσβασης στο ασύρματο δίκτυο. Στις συγκεκριμένες διεπαφές, πέρα από το untagged vlan 10 για τη διαχείριση τους, ρυθμίστηκαν και ως tagged τα vlans 130,140,150 για τα τρία διαφορετικά ασύρματα δίκτυα. Παρατίθεται πίνακας του sw4 που δείχνει τη ρύθμιση των VLANs ανά διεπαφή του διαμεταγωγέα.

PORT NUMBER	PORT DESCRIPTION	PORT GROUP	TAGGED VLAN	UNTAGGED VLAN
0/1	s21.p01			120
0/2	s21.p02			110
0/3	s22.p01			120
0/4	s22.p02			110
0/5	s50			90
0/6	s51			90
0/7	s52			90
0/8	s53			90
0/9	s54			90
0/10	s55			90
0/11	s56			90
0/12	s57			90
0/13	s58			90
0/14	s59			90
0/15	s60			90
0/16	s61			90
0/17	s62			90
0/18	s63			120
0/19	s64			120
0/20	s65			90
0/21	s41		10,130,140,150	120
0/22	s42		10,130,140,150	120
0/23				

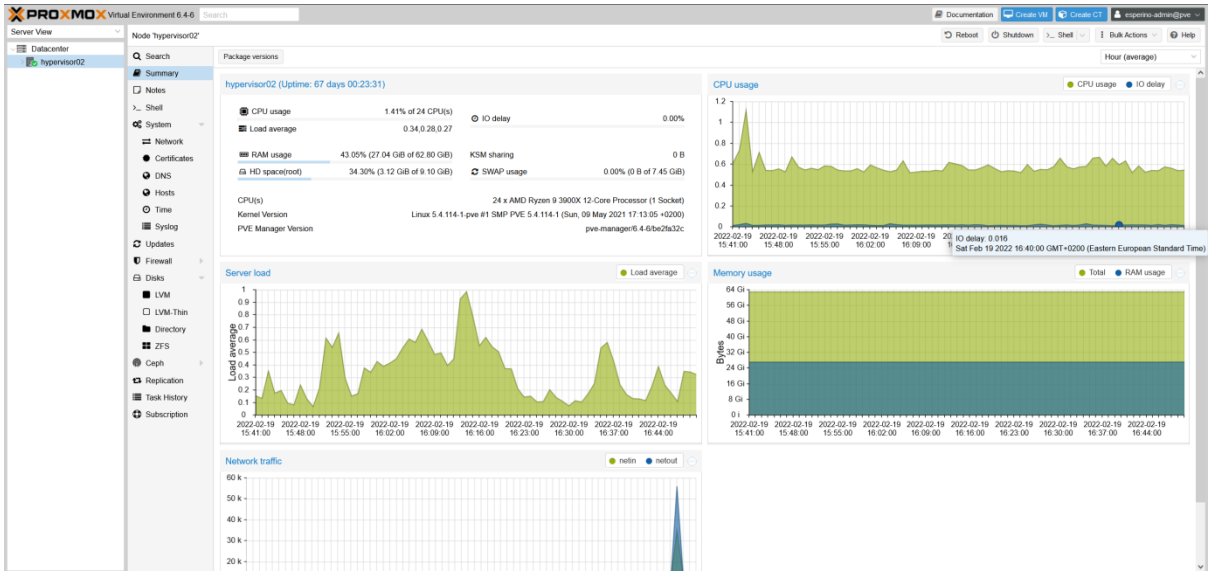
0/24				
0/25	sw0-fiber	4		
0/26	sw0-fiber	4		

Εγκατάσταση Συστήματος Hypervisor για την υποστήριξη Εικονικών Μηχανών 4.13.4

Στο σχολείο έχει εγκατασταθεί ασύρματο δίκτυο, του οποίου τα σημεία πρόσβασης χρειάζονται έναν ελεγκτή για να λειτουργήσουν σωστά. Ακόμη, έχει εγκατασταθεί σύστημα παρακολούθησης του δικτύου και έκδοσης στατιστικών λειτουργίας καθώς και ενημέρωσης των διαχειριστών σε περίπτωση προβλήματος. Για τη λειτουργία των συγκεκριμένων υποδομών χρειάζονται υπολογιστικοί πόροι. Με σκοπό την αποφυγή χρήσης πολλαπλών μηχανημάτων για την εξυπηρέτηση κάθε μίας ανάγκης αλλά και τη δυνατότητα προσθήκης επιπλέων υπηρεσιών στο μέλλον αποφασίστηκε η εγκατάσταση ενός συστήματος hypervisor το οποίο τρέχει το λογισμικό ανοιχτού κώδικα Proxmox για την υποστήριξη λειτουργίας πολλαπλών εικονικών μηχανών. Το συγκεκριμένο σύστημα έχει τα ακόλουθα χαρακτηριστικά:

ΕΞΑΡΤΗΜΑ	**ΠΕΡΙΓΡΑΦΗ**
CPU	ΕΠΕΞΕΡΓΑΣΤΗΣ 14 CORES/28 THREADS
RAM	DDR4 64GB
FAST STORAGE	4X1TB SATA SSDs in RAID 10 (2TB Usable)
LONG TERM STORAGE	2x4TB HDDS in RAID 1 (4TB Usable)

Το συγκεκριμένο μηχάνημα συνδέθηκε με το υπόλοιπο δίκτυο με τη χρήση μίας από τις διεπαφές χαλκού του οπτικού διαμεταγωγέα του δικτύου, στην οποία ρυθμίστηκε ως untagged το VLAN 20. Εγκαταστάθηκαν σε αυτό το λειτουργικό σύστημα Debian 10 και τα προγράμματα του Proxmox Hypervisor. Στην συνέχεια ορίστηκε στη δικτυακή του διεπαφή η διεύθυνση 10.33.20.3/24 για να μπορεί να έχει πρόσβαση στο δίκτυο και στο διαδίκτυο με τη χρήση του VLAN. Ακόμη ρυθμίστηκε ένα εσωτερικό «virtual switch» στο οποίο προστέθηκε και η δικτυακή διεπαφή του εξυπηρετητή με σκοπό να μπορούν και οι εικονικές μηχανές να έχουν πρόσβαση στο VLAN 20. Δημιουργήθηκε μια δοκιμαστική εικονική μηχανή η οποία βασιζόταν πάλι στα Debian 10 με σκοπό την διαβεβαίωση ότι όλα λειτουργούν σωστά και υπάρχει πρόσβαση τόσο στο δίκτυο όσο και στο διαδίκτυο από τις εικονικές μηχανές. Παρατίθεται λήψη από το περιβάλλον διαχείρισης των εικονικών μηχανών:

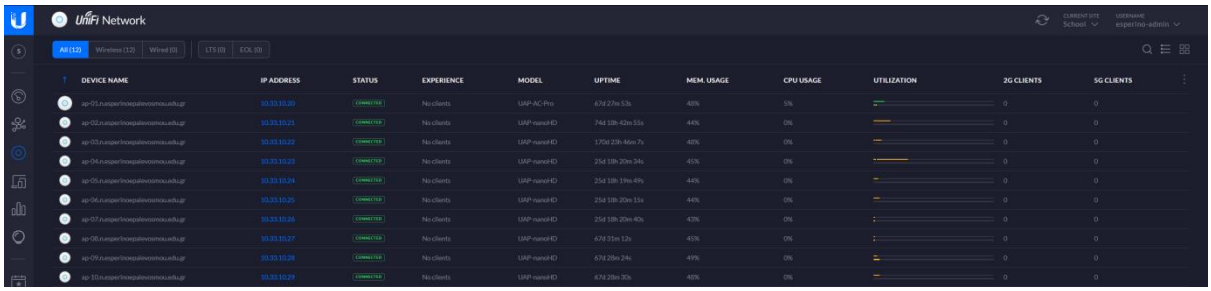


Εικόνα 36: Περιβάλλον διαχείρισης Proxmox

Εγκατάσταση του Ελεγκτή του Ασύρματου Δικτύου και Παραμετροποίηση των Σημείων Πρόσβασης 4.13.5

Αφότου δημιουργήθηκε η υποδομή φιλοξενίας εικονικών μηχανών, έπρεπε να δημιουργηθεί μια εικονική μηχανή η οποία θα φιλοξενήσει τον ελεγκτή των σημείων πρόσβασης. Η συγκεκριμένη μηχανή ονομάστηκε “unifi-controller”. Της αποδόθηκαν δύο εικονικοί επεξεργαστικοί πυρήνες (vCPUs) και 4GB μνήμης. Η συγκεκριμένη εικονική μηχανή έλαβε την στατική IP 10.33.20.7. Στην συνέχεια εγκαταστάθηκε το πακέτο των προγραμμάτων που απαρτίζουν τον ελεγκτή.
Με την ολοκλήρωση της συγκεκριμένης διαδικασίας, έγινε η πρώτη σύνδεση στο διαχειριστικό περιβάλλον του ελεγκτή μέσω ενός περιηγητή. Δημιουργήθηκε ένας νέος χρήστης ενώ δόθηκαν και στοιχεία για τον χώρο που είναι εγκατεστημένο το συγκεκριμένο δίκτυο.
Αποφασίστηκε πρώτα να ρυθμιστούν όλες οι παράμετροι του ασύρματου δικτύου και στην συνέχεια να συνδεθούν τα σημεία πρόσβασης και να μεταφορτωθούν οι ρυθμίσεις σε αυτά. Έτσι αρχικά δημιουργήθηκαν τρία ασύρματα δίκτυα με την ονομασία teachers-wifi, students-wifi και devices-wifi, όπως και είχε οριστεί από τα κριτήρια σχεδιασμού. Έγιναν οι αντιστοιχήσεις μεταξύ VLAN και SSID και πιο συγκεκριμένα το VLAN 130 για το SSID “teachers-wifi”, το VLAN 140 για το SSID “students-wifi” και το VLAN 150 για το SSID “devices-wifi”. Ακόμη ορίστηκε ότι τα συγκεκριμένα SSIDs θα εκπέμπονται από όλα τα Access Points, τόσο στα 2.4GHz όσο και στα 5GHz. Τέλος διεκόπη η διατήρηση στατιστικών για τους πελάτες με σκοπό την εναρμόνιση με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR).
Μόλις ολοκληρώθηκε η αρχική παραμετροποίηση του ελεγκτή έπρεπε να συνδεθούν τα σημεία πρόσβασης με αυτόν και να μεταφορτωθούν σε αυτά οι ρυθμίσεις. Την πρώτη φορά που γίνεται η σύνδεση με το δίκτυο, τα σημεία πρόσβασης αναμένουν να βρίσκονται σε δίκτυο στο οποίο λειτουργεί DHCP Server. Στην συνέχεια τη διεύθυνση του ελεγκτή τους μπορούν να την μάθουν μέσω μηνυμάτων ευρυεκπομπής (broadcast messages) εάν και ο ελεγκτής βρίσκεται στο

ίδιο VLAN ή μέσω μιας παραμέτρου που αποστέλλεται από τον DHCP Server αν ο ελεγκτής βρίσκεται σε διαφορετικό VLAN.
Στην περίπτωση του σχολικού δικτύου ισχύει το δεύτερο. Έτσι επιλέχθηκε να χρησιμοποιηθεί το VLAN 120 για την πρώτη ρύθμιση και στην συνέχεια να γίνει η εναλλαγή στο VLAN 10. Παράλληλα ρυθμίστηκε ο DHCP Server του VLAN 120 να μεταδίδει την πληροφορία ότι ο ελεγκτής του ασύρματου δικτύου έχει την IP 10.33.20.7.
Για να γίνει αυτό ρυθμίστηκαν προσωρινά οι διεπαφές πάνω στις οποίες θα συνδεθούν τα Access Points να έχουν ως untagged VLAN το VLAN 120 και στην συνέχεια τοποθετήθηκαν τα Access Points στα σημεία που είχαν οριστεί κατά τη διάρκεια της μελέτης ραδιοκάλυψης. Συνδέθηκαν με τις πρίζες δικτύου με τη χρήση κατάλληλου προτερματισμένου καλωδίου, μικρού μήκους και βεβαιώθηκε ότι ο ελεγκτής τους μπορεί να επικοινωνήσει με αυτά. Αφού ολοκληρώθηκε η συγκεκριμένη διαδικασία ορίστηκαν στατικές IP, αυτή τη φορά στο υποδίκτυο 10.33.10.0/24. Τα σημεία πρόσβασης αποσυνδέθηκαν από τον ελεγκτή τους. Μόλις ωστόσο έγινε η αλλαγή της παραμετροποίησης στους διαμεταγωγείς ώστε οι διεπαφές που χρησιμοποιούν να έχουν ως untagged VLAN το VLAN 10 ο ελεγκτής μπορούσε και πάλι να επικοινωνήσει μαζί τους.



Εικόνα 37: Τα σημεία πρόσβασης όπως φαίνονται από τον κεντρικό ελεγκτή

Στην συνέχεια ρυθμίστηκε στο εκάστοτε σημείο πρόσβασης η ένταση εκπομπής στα 2.4GHz και στα 5GHz καθώς και το κανάλι στο οποία θα πρέπει να εκπέμπουν στο καθένα από τα δύο φάσματα συχνοτήτων. Οι παραπάνω ρυθμίσεις έγιναν με βάση τον πίνακα που ακολουθεί:

AP NAME	2.4GHz Broadcast Power	2.4GHz Channel	5GHz Broadcast Power	5GHz Channel
ap-01	Low	6	High	36
ap-02	Low	11	High	40
ap-03	Low	1	High	44
ap-04	Low	1	High	44
ap-05	Low	6	High	40
ap-06	Low	11	High	36
ap-07	Low	6	High	36
ap-08	Low	6	High	36
ap-09	Low	1	High	48

ap-10	Low	11	High	44

Τέλος μεταφορτώθηκαν σε αυτά οι ρυθμίσεις για τα SSIDs και την αντιστοίχιση των VLANs με αυτά ενώ παράλληλα έγινε και ενημέρωση του λογισμικού τους στην τελευταία έκδοση. Το ασύρματο δίκτυο βρισκόταν πια σε λειτουργία και έπρεπε να γίνουν δοκιμές λειτουργίας

Δοκιμές Χρήσης 4.14

Το τελικό στάδιο της υλοποίησης αφορούσε τις δοκιμές λειτουργίας τόσο στο ασύρματο όσο και στο ενσύρματο δίκτυο με σκοπό την επιδιόρθωση τυχόν προβλημάτων που πιθανόν να υπάρχουν.

Δοκιμές χρήσης στο ενσύρματο δίκτυο 4.14.1

Με την ολοκλήρωση της εγκατάστασης του ενεργού και του παθητικού εξοπλισμού και τη ρύθμιση του, έγινε η μετάπτωση των σταθμών εργασίας και λοιπών ενσύρματων δικτυακών συσκευών. Χρησιμοποιήθηκαν νέα προτερματισμένα καλώδια UTP από τις πρίζες δικτύου μέχρι και την εκάστοτε συσκευή με σκοπό την εξάλειψη πιθανών προβλημάτων λόγω φθοράς των παλαιότερων καλωδίων. Στην συνέχεια έγινε επιβεβαίωση ότι όλες οι συσκευές μπορούν να επικοινωνήσουν μεταξύ τους, σε περίπτωση που αυτό επιτρέπεται από το τείχος προστασίας αλλά και με το διαδίκτυο, από τον σωστό πάροχο με βάση τις πολιτικές. Οι συγκεκριμένες δοκιμές ήταν επιτυχείς. Παράλληλα ορίστηκαν και στατικές διευθύνσεις IP σε όλες τις μόνιμα συνδεδεμένες δικτυακές συσκευές με σκοπό την ευκολότερη αναγνώριση τους. Η διεύθυνση MAC της συσκευής και η στατική διεύθυνση IP της καταγράφηκαν και σε ένα υπολογιστικό φύλλο με σκοπό την ευκολότερη αναζήτηση τους στο μέλλον.

80			
teachers-office-vlan			
MAC ADDRESS	IPv4 ADDRESS	ΑΠΟΔΟΣΗ ΔΙΕΥΘΥΝΣΕΩΝ	ΠΕΡΙΓΡΑΦΗ
N/A	**10.33.80.0**	N/A	net.teachers-office.esperinoepalevosmou.edu.gr
N/A	**10.33.80.1**	N/A	core-vlan80.teachers-office.esperinoepalevosmou.edu.gr
18:a9:05:2b:7c:6e	**10.33.80.2**	STATIC_DHCP_1d	teachers-pc-1.teachers-office.esperinoepalevosmou.edu.gr
00:1e:8c:8c:3c:d0	**10.33.80.3**	STATIC_DHCP_1d	teachers-pc-2.teachers-office.esperinoepalevosmou.edu.gr
00:1e:8c:0c:c3:1c	**10.33.80.4**	STATIC_DHCP_1d	teachers-pc-3.teachers-office.esperinoepalevosmou.edu.gr
18:a9:05:2b:7d:42	**10.33.80.5**	STATIC_DHCP_1d	teachers-pc-4.teachers-office.esperinoepalevosmou.edu.gr

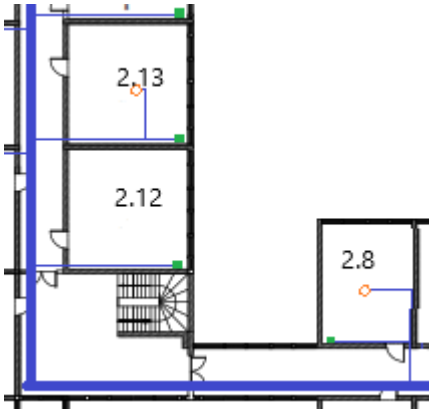
Εικόνα 38: Ενδεικτικό υπολογιστικό φύλλο που δείχνει τις στατικές διευθύνσεις στο γραφείο των εκπαιδευτικών

Δοκιμές χρήσης στο ασύρματο δίκτυο 4.14.2

Όσο αφορά το ασύρματο δίκτυο οι δοκιμές χρήσης έγιναν σε δύο στάδια. Δοκιμές συνδεσιμότητας και ομαλής περιαγωγής από σημείο πρόσβασης σε σημείο πρόσβασης χωρίς φόρτο και δοκιμές συνδεσιμότητας με φόρτο. Όσο αφορά το πρώτο στάδιο, με τη χρήση ενός φορητού υπολογιστή και του προγράμματος “InSSIDer”, έγιναν έλεγχοι σε κάθε αίθουσα ότι το σημείο πρόσβασης εκπέμπει με τις σωστές ρυθμίσεις, δεν υπάρχουν γειτονικά σημεία πρόσβασης που να εκπέμπουν στο ίδιο κανάλι και η στάθμη σήματος παραμένει σε ικανοποιητικό επίπεδο. Κατά τον συγκεκριμένο έλεγχο βρέθηκαν κάποια κενά στην κάλυψη τα οποία ήταν δύσκολο

να προβλεφθούν κατά τη διάρκεια του ελέγχου ραδιοκάλυψης. Πιο συγκεκριμένα, στο γραφείο της Διεύθυνσης και στο Εργαστήριο Σχεδίου στο τέλος της βορειοδυτικής πτέρυγας. Για τις δύο αυτές περιπτώσεις έχει δρομολογηθεί η εγκατάσταση δύο επιπλέων Access Points.

Παράλληλα έγινε αντιληπτό ότι υπάρχουν εσωτερικές παρεμβολές μεταξύ δύο σημείων πρόσβασης σε 2 αίθουσες στο σημείο που τέμνεται η βορειοανατολική και η βορειοδυτική πτέρυγα. Μεταξύ αυτών των δύο αιθουσών παρεμβάλλονται πολλαπλοί τοίχοι, ωστόσο οι δύο αίθουσες έχουν οπτική επαφή μέσω των παραθύρων τους. Έτσι το εκπεμπόμενο σήμα σε κάθε μία μπορεί να προκαλέσει παρεμβολές στην άλλη. Το συγκεκριμένο πρόβλημα λύθηκε με την αλλαγή του καναλιού εκπομπής στο ένα από τα δύο σημεία πρόσβασης.



Εικόνα 39: Ενδεικτικό υπολογιστικό φύλλο που δείχνει τις στατικές διευθύνσεις στο γραφείο των εκαπιδευτικών

Ο νέος πίνακας ρυθμίσεων για τα Access Points είναι ο ακόλουθος με τις αλλαγές στα κανάλια να φαίνονται με έντονο χρώμα:

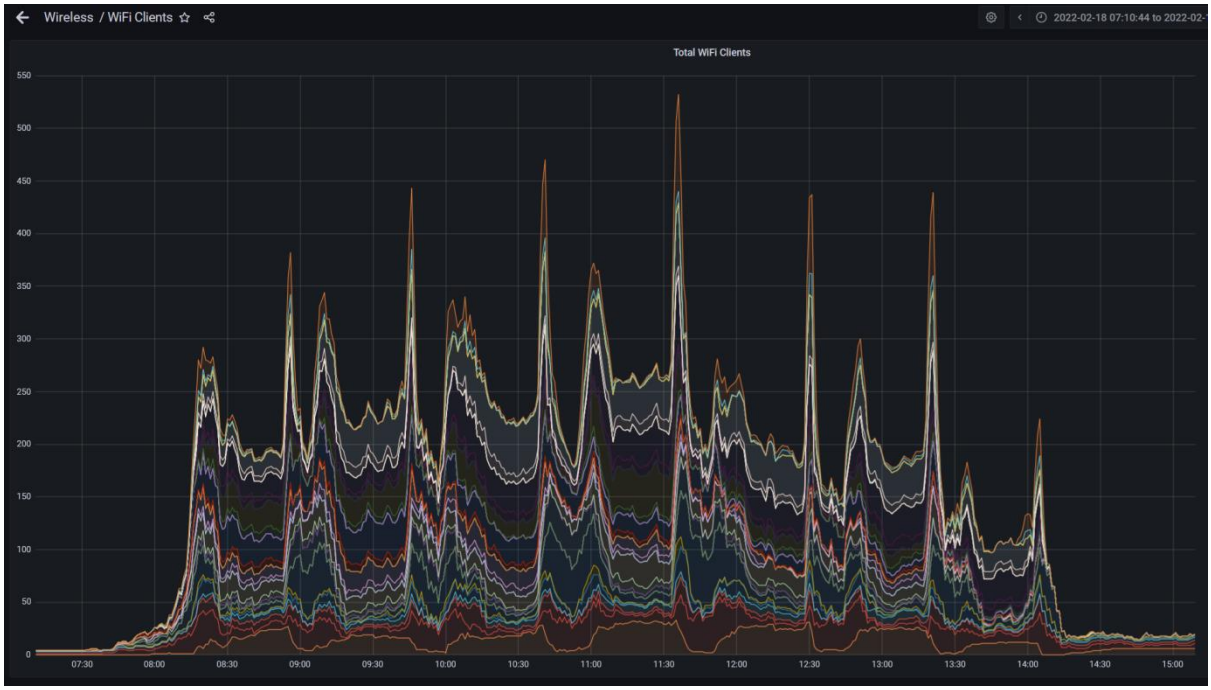
AP NAME	2.4GHz Broadcast Power	2.4GHz Channel	5GHz Broadcast Power	5GHz Channel
ap-01	Low	6	High	36
ap-02	Low	11	High	40
ap-03	Low	1	High	44
ap-04	Low	1	High	44
ap-05	Low	6	High	40
ap-06	Low	11	High	36
ap-07	**Low**	**6**	High	36
ap-08	**Low**	**11**	High	36
ap-09	Low	1	High	48
ap-10	Low	11	High	44

Για τη δοκιμή της ικανότητας επιτυχής περιαγωγής των συσκευών χρησιμοποιήθηκε και πάλι ένας φορητός υπολογιστής στον οποίο πραγματοποιήθηκε μια κλήση τηλεδιάσκεψης. Με την κλήση ενεργή έγινε επίσκεψη σε όλες τις αίθουσες και τους διαδρόμους του ορόφου με σκοπό να

ελεγχθεί αν θα διακοπεί η κλήση ή θα υπάρξει πτώση της ποιότητας. Η κλήση παρέμεινε ενεργή και διατήρησε τα ποιοτικά χαρακτηριστικά της καθ' όλη τη διάρκεια της δοκιμής, ενώ διεκόπη μόνο στα δύο σημεία που υπάρχει κενό στην κάλυψη και αναφέρθηκαν προηγουμένως. Η συγκεκριμένη δοκιμή δείχνει ότι η περιαγωγή από σημείο πρόσβασης σε σημείο πρόσβασης χωρίς τη διακοπή της σύνδεσης είναι εφικτή.

Το δεύτερο στάδιο των δοκιμών έπρεπε να γίνει με φόρτο. Γι' αυτό το λόγο τα σημεία πρόσβασης παρέμειναν σε λειτουργία, δημοσιεύθηκαν τα στοιχεία πρόσβασης στα ασύρματα δίκτυα τόσο για τους μαθητές όσο και για το εκπαιδευτικό προσωπικό και εγκαταστάθηκε σύστημα παρακολούθησης των δικτυακών συσκευών και δημιουργίας γραφημάτων το οποίο θα αναλυθεί στο κεφάλαιο 5. Εκεί μετρήθηκε ο αριθμός των συσκευών που συνδέονται στο δίκτυο, η δικτυακή κίνηση και πόσες από αυτές προτιμούν το φάσμα των 5GHz αντί για το φάσμα των 2.4GHz.

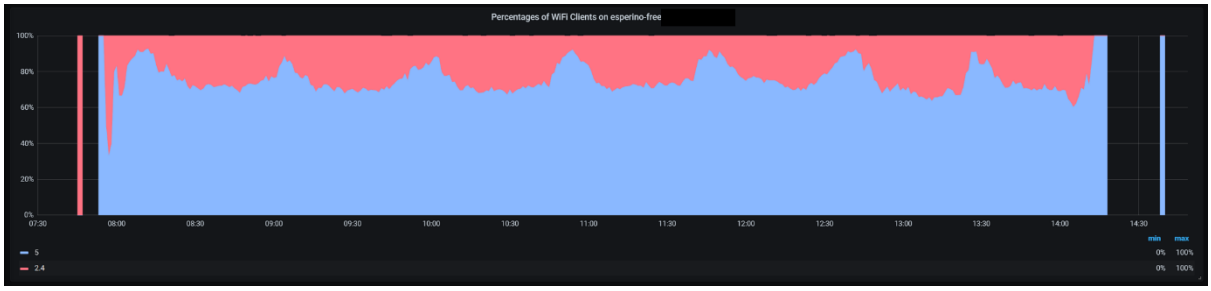
Ο μέγιστος αριθμός συσκευών που χρησιμοποιεί το δίκτυο ταυτόχρονα παρατηρήθηκε να φτάνει τις 200-250 συσκευές όπως φαίνεται και στο παρακάτω γράφημα.



Εικόνα 40: Συνολικός αριθμός συνδεδεμένων συσκευών κατά την διάρκεια του σχολικού ωραρίου

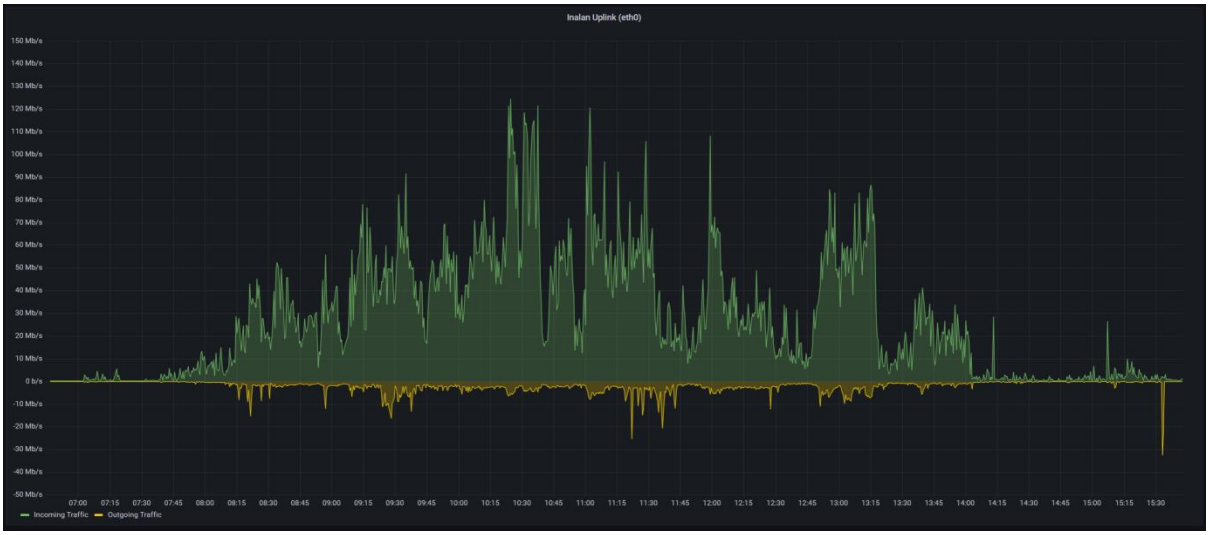
Οι ακμές που φαίνονται στο γράφημα συμβαίνουν τις χρονικές στιγμές έναρξης και λήξης των διαλειμμάτων και αποτελούν ψευδή νούμερα. Πιο αναλυτικά, η μαζική μετακίνηση των μαθητών κατά την έναρξη του διαλείμματος κατά μήκος του διαδρόμου και προς το κλιμακοστάσιο για την έξοδο τους από το κτήριο προκαλεί την περιαγωγή τους σχεδόν σε κάθε ένα από τα σημεία πρόσβασης. Όταν συνδέονται σε ένα σημείο πρόσβασης, αυξάνεται ένας μετρητής (SNMP counter), ο οποίος στην συνέχεια αποστέλλεται στο σύστημα παρακολούθησης του δικτύου. Στην συνέχεια η συσκευή αποσυνδέεται πολύ σύντομα, μιας και ο χρήστης

απομακρύνεται από αυτή αλλά η τιμή του συγκεκριμένου μετρητή δεν ανανεώνεται από το λογισμικό του σημείου πρόσβασης άμεσα. Έτσι μια συσκευή, όσο αφορά το σύστημα παρακολούθησης του δικτύου, φαίνεται συνδεδεμένη σε πολλαπλά σημεία πρόσβασης. Το ίδιο συμβαίνει και κατά την επιστροφή των μαθητών από την αυλή του σχολείου, στο κλιμακοστάσιο, κατά μήκος του διαδρόμου προς την αίθουσα τους. Όταν αυτό συμβεί αθροιστικά για πολλές συσκευές προκαλούνται οι συγκεκριμένες ακμές στο γράφημα συνδεδεμένων πελατών.
Όσο αφορά την προτίμηση των συσκευών, τις στιγμές που το δίκτυο χρησιμοποιείται από το μέγιστο πλήθος συσκευών, περίπου το 70% αυτών προτιμά το φάσμα των 5GHz και το υπόλοιπο 30% το φάσμα των 2.4GHz. Αν σε αυτό το ποσοστό γίνει συνυπολογισμός και των συσκευών που είναι παλαιότερης τεχνολογίας και δε μπορούν να χρησιμοποιήσουν τα 5GHz, το ποσοστό κρίνεται καλό και αποδεικνύει ότι δεν υπάρχουν ιδιαίτερα κενά στην κάλυψη.



Εικόνα 41: Ποσοστό ασύρματων συσκευών που επιλέγουν τα 5GHz

Τέλος όσο αφορά την κίνηση στο δίκτυο, αυτή είναι σαφώς μεταβλητή κατά τη διάρκεια της μέρας και καθώς συνδέονται όλο και περισσότερες συσκευές αυξάνεται μέχρι και τα 100Mb/s που είναι και η χωρητικότητα του κυκλώματος από τον εμπορικό πάροχο που χρησιμοποιούν τα συγκεκριμένα VLANs. Κατά μέσο όρο η κίνηση στα VLANs του ασύρματου δικτύου εκπαιδευτικού προσωπικού, μαθητών και συσκευών που ανήκουν στο σχολείο κυμαίνεται στα 30-40Mb/s



Εικόνα 42: Δικτυακή κίνηση από και προς τον εμπορικό πάροχο διαδικτύου

Κεφάλαιο 5 Παρακολούθηση Συμπεριφοράς του Δικτύου

Με σκοπό την παρακολούθηση της συμπεριφοράς της δικτυακής υποδομής, την πρόληψη προβλημάτων αλλά και την ευκολότερη επίλυση τους σε περίπτωση που αυτά εμφανιστούν, αποφασίστηκε η εγκατάσταση ενός συνόλου από εργαλεία. Τα συγκεκριμένα εργαλεία παρακολούθησης είναι υπεύθυνα για την επικοινωνία με τις δικτυακές συσκευές μέσω του πρωτοκόλλου SNMP, την συλλογή δεδομένων ανά τακτά χρονικά διαστήματα, την αποθήκευση τους σε βάση δεδομένων και την απεικόνιση τους με τη χρήση κατάλληλων γραφημάτων. Ακόμα είναι υπεύθυνα για την ειδοποίηση των διαχειριστών του δικτύου σε περίπτωση αδυναμίας επικοινωνίας με την χρήση κατάλληλων μηνυμάτων.

Πρωτόκολλα Επικοινωνίας 5.1

Πριν γίνει αναφορά στα εργαλεία που χρησιμοποιήθηκαν για την παρακολούθηση του δικτύου θα πρέπει να γίνει αναφορά στο βασικό πρωτόκολλο που χρησιμοποιείται για την επικοινωνία των συγκεκριμένων εργαλείων με τις δικτυακές συσκευές με σκοπό τη λήψη δεδομένων. Το πρωτόκολλο που χρησιμοποιείται ονομάζεται Simple Network Management Protocol (SNMP).

Ιστορικά Στοιχεία 5.1.1

Το συγκεκριμένο πρωτόκολλο δημιουργήθηκε από τους D.Harrington, R.Presuhn και B.Wignen, μέλη του IETF Network Working Group και προτυποποιήθηκε για πρώτη φορά ως RFC2271 τον Ιανουάριο του 1998. Από τότε έχει υποστεί βελτιώσεις με την τελευταία έκδοση να περιγράφεται στα RFC3411-3418 τον Δεκέμβριο του 2002.

Εκδόσεις 5.1.2

Από την εμφάνιση του πρωτοκόλλου μέχρι και σήμερα έχουν υπάρξει τρεις διαφορετικές εκδόσεις του πρωτοκόλλου SNMP. Η έκδοση 1, 2 και 3.
Η έκδοση 1 ήταν η πρώτη έκδοση που δημιουργήθηκε. Χρησιμοποιεί το πρωτόκολλο UDP και τη δικτυακή θύρα 161. Έχει δεχθεί σοβαρές κριτικές για την ασφάλεια της μιας και η επικοινωνία είναι μη κρυπτογραφημένη και ο μόνος τρόπος ταυτοποίησης του χρήστη είναι με τη χρήση ενός συνόλου από χαρακτήρες το οποίο ονομάζεται SNMP Community String.
Η έκδοση 2c έφερε βελτιώσεις στην πρώτη έκδοση του πρωτοκόλλου στον τομέα της απόδοσης αλλά και της ασφάλειας. Σχετικά με την απόδοση, εισήχθησαν νέες εντολές που επιτρέπουν την αίτηση για μεγάλο όγκο δεδομένων με ένα μόνο αίτημα. Ακόμη δημιουργήθηκαν νέοι τύποι δεδομένων και αυξήθηκαν τα μεγέθη

των μετρητών που υπάρχουν από 32bit σε 64bit. Αναφορικά με την ασφάλεια δημιουργήθηκε ένα νέο σύστημα ταυτοποίησης των αιτούντων δεδομένα το οποίο ήταν "party-based". Το συγκεκριμένο σύστημα ωστόσο αποδείχτηκε ιδιαίτερα περίπλοκο με αποτέλεσμα να μην υιοθετηθεί εκτενώς και να χρησιμοποιηθούν για άλλη μια φορά τα community strings με σκοπό τον έλεγχο πρόσβασης στα δεδομένα.
Τέλος, η έκδοση 3 δεν έφερε κάποια αλλαγή σε θέματα απόδοσης του πρωτοκόλλου, ωστόσο ενίσχυσε την ασφάλεια του. Εισήγαγε την έννοια της κρυπτογράφησης της επικοινωνίας, του ελέγχου ακεραιότητας των δεδομένων και της πιστοποίησης της πηγής των δεδομένων. Η κρυπτογράφηση των μηνυμάτων μπορεί να γίνει είτε μέσω του πρωτοκόλλου SSH, είτε μέσω του πρωτοκόλλου TLS. Ακόμη ο έλεγχος πρόσβασης στα δεδομένα δεν γίνεται μέσω του community string αλλά έχει δημιουργηθεί ένα σύστημα χρηστών. Έτσι κάθε πελάτης που αιτείται δεδομένα από τη δικτυακή συσκευή πρέπει να παρέχει ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Τέλος έχει δοθεί η δυνατότητα ελέγχου πρόσβασης σε συγκεκριμένα δεδομένα για κάθε χρήστη.

Δομή των δεδομένων 5.1.3

Τα δεδομένα στο πρωτόκολλο SNMP είναι ιεραρχημένα και ακολουθούν μια δενδροειδή δομή η οποία ονομάζεται Management Information Base (MIB). Στην κορυφή του δέντρου υπάρχει η διεύθυνση 1 η οποία είναι η ρίζα του δέντρου και ανήκει σε κάποιον οργανισμό τυποποίησης. Οι πληροφορίες που βρίσκονται σε επίπεδα κάτω από την ρίζα μπορεί είτε να είναι τυποποιημένες σε ορισμένες διευθύνσεις από κάποιον οργανισμό τυποποίησης και να επιστρέφουν την ίδια πληροφορία ανεξαρτήτως κατασκευαστή είτε να είναι ελεύθερες προς χρήση από τον εκάστοτε κατασκευαστή. Κάθε διαφορετική πληροφορία στο δέντρο έχει μια συγκεκριμένη διεύθυνση η οποία ονομάζεται Object Identifier (OID). Ο τύπος της πληροφορίας μπορεί να είναι είτε ένας ακέραιος (Integer), είτε ένα αλφαριθμητικό (String), είτε ένας μετρητής 32 ή 64bit (Counter). Ακόμη το κάθε OID μπορεί να είναι αυτούσιο είτε να αποτελεί τμήμα ενός πίνακα από πολλαπλά OIDs.

SNMP Traps 5.1.4

Επί το πλείστων η επικοινωνία στο πρωτόκολλο SNMP γίνεται με κάποιον χρήστη να αιτείται μια πληροφορία σε μία καθορισμένη διεύθυνση OID και την συσκευή να επιστρέφει την συγκεκριμένη πληροφορία. Αυτό είναι χρήσιμο για την άντληση στατιστικών αλλά ο μόνος τρόπος να εντοπιστούν αλλαγές σε κάποια κατάσταση, όπως για παράδειγμα η κατάσταση της σύνδεσης μιας πόρτας ενός διαμεταγωγέα είναι να γίνεται συνεχής και επαναλαμβανόμενος έλεγχος της κατάστασης της με αιτήματα από τον πελάτη στην συσκευή. Κάτι που σε μεγάλη κλίμακα είναι ανέφικτο. Γι' αυτό τον λόγο έχει προβλεφθεί η δυνατότητα, οι συσκευές να στέλνουν μηνύματα προς έναν κόμβο που είναι ρυθμισμένος για τη λήψη τους κάθε φορά που γίνεται μια αλλαγή κατάστασης. Τα συγκεκριμένα μηνύματα ονομάζονται SNMP Traps και έχουν μια συγκεκριμένη διεύθυνση OID. Ο κόμβος

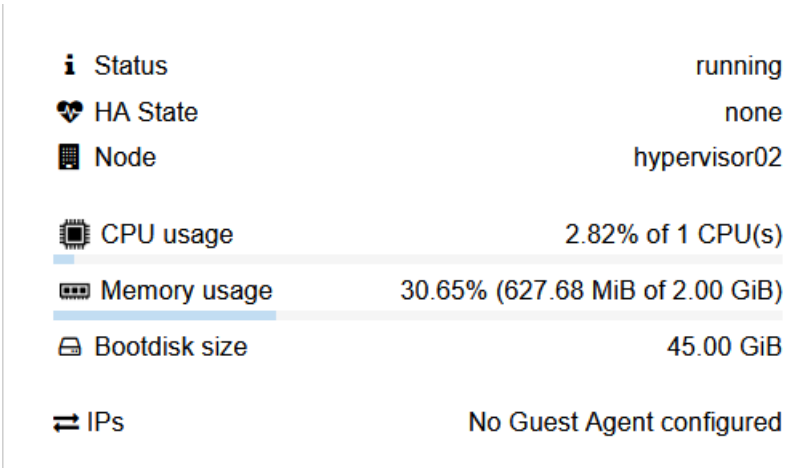
αποκωδικοποιεί την συγκεκριμένη διεύθυνση και μπορεί να κατανοήσει για ποια αλλαγή κατάστασης αναφέρεται το μήνυμα.

Εργαλεία που χρησιμοποιήθηκαν 5.2

Παρακάτω αναλύονται τα εργαλεία που χρησιμοποιήθηκαν για την παρακολούθηση της δικτυακής υποδομής.

Βάση Δεδομένων 5.2.1

Βασικό στοιχείο του συστήματος παρακολούθησης είναι η βάση δεδομένων στην οποία αποθηκεύονται τα δεδομένα. Για την συγκεκριμένη ανάγκη χρησιμοποιήθηκε το influxdb. Η συγκεκριμένη βάση δεδομένων είναι μία από τις πιο γνωστές “time series databases”. Οι συγκεκριμένες βάσεις δεδομένων είναι βελτιστοποιημένες για να αποθηκεύουν δεδομένα τύπου χρονοσειράς, άρα είναι η βέλτιστη λύση για ανάγκες παρακολούθησης της δικτυακής κίνησης κατά τη διάρκεια του χρόνου. Το συγκεκριμένο λογισμικό είναι γραμμένο στη γλώσσα προγραμματισμού Go και είναι ανοιχτού κώδικα. Χρησιμοποιεί ένα REST API για την εγγραφή και την ανάγνωση δεδομένων κάνοντας χρήση του πρωτοκόλλου HTTPS. Ακόμη έχει τη δυνατότητα να ρυθμιστεί να διαγράφει δεδομένα παλιότερα από κάποιο χρονικό διάστημα βελτιστοποιώντας τη χρήση του αποθηκευτικού χώρου.
Στην περίπτωση του σχολικού δικτύου, η συγκεκριμένη βάση δεδομένων εγκαταστάθηκε σε μια εικονική μηχανή η οποία χρησιμοποιεί τα Debian 10 ως λειτουργικό σύστημα, στον server που αναλύεται σε προηγούμενο κεφάλαιο. Η εικονική μηχανή έχει 1 vCPU, 2GB RAM και 45GB αποθηκευτικού χώρου. Δόθηκε αυξημένος αποθηκευτικός χώρος λόγω του όγκου των δεδομένων που αναμένεται να αποθηκευτούν.
Παρακάτω φαίνεται ένα στιγμιότυπο από τη χρήση των υπολογιστικών πόρων της συγκεκριμένης εικονικής μηχανής.



Εικόνα 43: Χρήση υπολογιστικών πόρων από το σύστημα δημιουργίας γραφημάτων

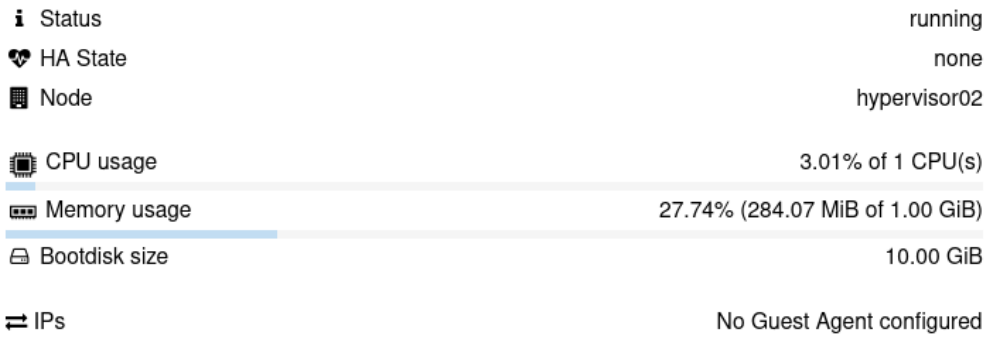
SNMP Client 5.2.2

Για την επικοινωνία με τις δικτυακές συσκευές και την συλλογή δεδομένων από αυτές με τη χρήση του πρωτοκόλλου SNMP επιλέχθηκε η λύση του λογισμικού με την ονομασία telegraf. Το telegraf είναι ένα λογισμικό ανοιχτού κώδικα το οποίο είναι γραμμένο στη γλώσσα προγραμματισμού Go και χρησιμοποιείται για την συλλογή μετρικών δεδομένων από συστήματα και την αποθήκευση τους σε βάσεις δεδομένων, με σκοπό την περαιτέρω ανάλυση τους. Χρησιμοποιεί μια plugin-based αρχιτεκτονική και στην περίπτωση του σχολικού δικτύου γίνεται η χρήση του SNMP plugin για την επικοινωνία με τις δικτυακές συσκευές και του Influxdb plugin για την επικοινωνία με την βάση δεδομένων και την εγγραφή δεδομένων σε αυτή.
Το telegraf χρησιμοποιεί συγκεκριμένα configuration files για τη ρύθμιση των παραμέτρων που απαιτούνται για τη λειτουργία του. Στην περίπτωση του σχολικού δικτύου υπάρχει ένα αρχείο ρυθμίσεων το οποίο αφορά τις γενικές ρυθμίσεις όπως πόσο συχνά θα πρέπει να επικοινωνεί το telegraf με τις δικτυακές συσκευές και να συλλέγει δεδομένα καθώς και τα διαπιστευτήρια του για την επικοινωνία με την βάση δεδομένων influxdb. Στην συνέχεια υπάρχει ένα αρχείο ρυθμίσεων για κάθε δικτυακή συσκευή με την οποία επικοινωνεί το telegraf. Μέσα στο συγκεκριμένο αρχείο υπάρχει κάθε SNMP Object Identifier για το οποίο είναι επιθυμητό να γίνει συλλογή δεδομένων, η ονομασία με την οποία αποθηκεύονται τα συγκεκριμένα δεδομένα μέσα στο influxdb, η διεύθυνση IP της δικτυακής συσκευής από την οποία και αντλούνται τα δεδομένα και το community string με το οποίο γίνεται έλεγχος πρόσβασης. Παρακάτω φαίνεται απόκομμα από το αρχείο ρυθμίσεων.

```
# Specify the amount of times telegraf will retry to poll data
retries = 3

# Specify the SNMP Protocol Version
version = 2

[[inputs.snmp.field]]

# Specify the OID of this metric
oid = ".1.3.6.1.2.1.2.2.1.10.1"

# Specify the name of this metric
name = "port-1-interface-in-octets"

[[inputs.snmp.field]]

# Specify the OID of this metric
oid = ".1.3.6.1.2.1.2.2.1.16.1"

# Specify the name of this metric
name = "port-1-interface-out-octets"

[[inputs.snmp.field]]

# Specify the OID of this metric
oid = ".1.3.6.1.2.1.2.2.1.11.1"

# Specify the name of this metric
name = "port-1-interface-in-unicast-packets"
```

Εικόνα 44: Τμήμα του αρχείου ρυθμίσεων του telegraf.

Το telegraf τρέχει σε μια εικονική μηχανή που χρησιμοποιεί το λειτουργικό σύστημα Debian 10. Στην συγκεκριμένη εικονική μηχανή έχει αποδοθεί 1 vCPU και 10GB μνήμη RAM. Τέλος έχουν αποδοθεί 10GB αποθηκευτικού χώρου μιας και δεν υπάρχουν ιδιαίτερες απαιτήσεις αποθήκευσης δεδομένων. Παρακάτω φαίνεται η χρήση των υπολογιστικών πόρων που αποδόθηκαν στην συγκεκριμένη εικονική μηχανή.



Εικόνα 45: Χρήση υπολογιστικών πόρων από το σύστημα συλλογής μετρικών δεδομένων από τις δικτυακές συσκευές.

Οι δικτυακές συσκευές που παρακολουθούνται από το telegraf είναι οι εξής:

- core-router
- sw0-fiber
- sw1-poe
- sw2
- sw3
- sw4
- sw5-poe
- sw6
- ap-01
- ap-02
- ap-03
- ap-04
- ap-05
- ap-06
- ap-07
- ap-08
- ap-09
- ap-10

Γραφική Απεικόνιση 5.2.3

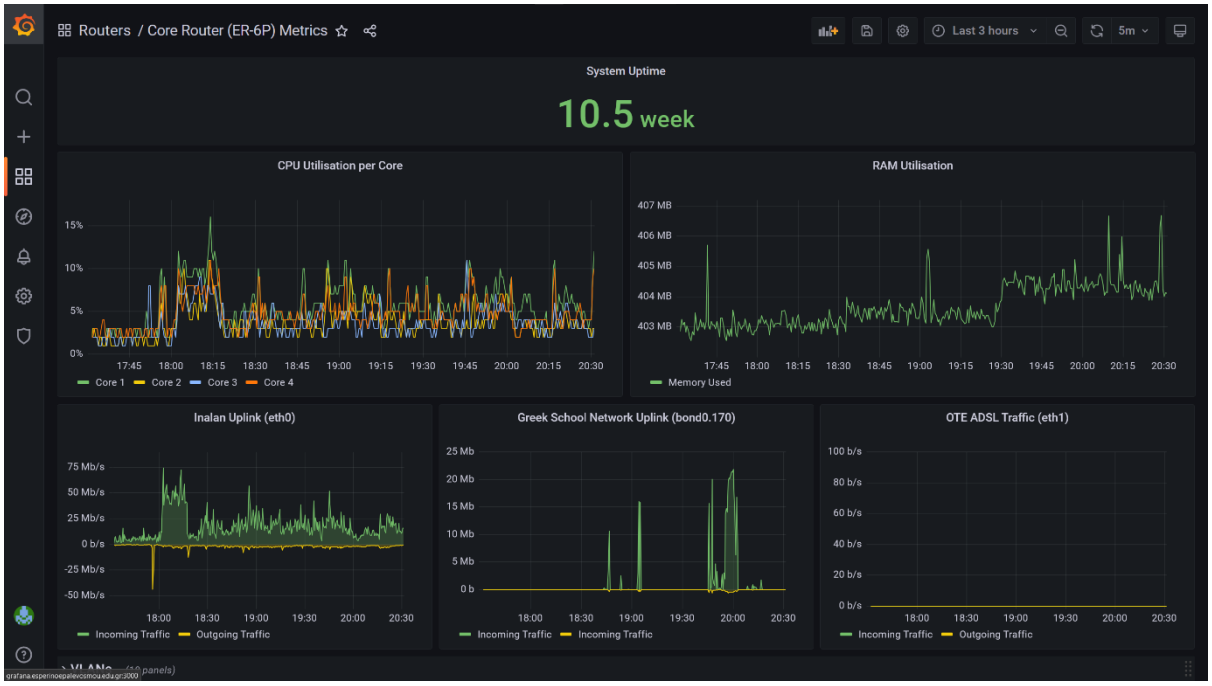
Για τη γραφική απεικόνιση των στατιστικών κίνησης της δικτυακής υποδομής χρησιμοποιήθηκε το λογισμικό Grafana. Η συγκεκριμένη λύση είναι ευρέως διαδεδομένη στις εταιρίες λογισμικού για τις ανάγκες γραφικής απεικόνισης καθώς παρέχει ένα πολύ μεγάλο σύνολο από δυνατότητες. Είναι λογισμικό ανοιχτού κώδικα και είναι γραμμένο στην γλώσσα προγραμματισμού Go.

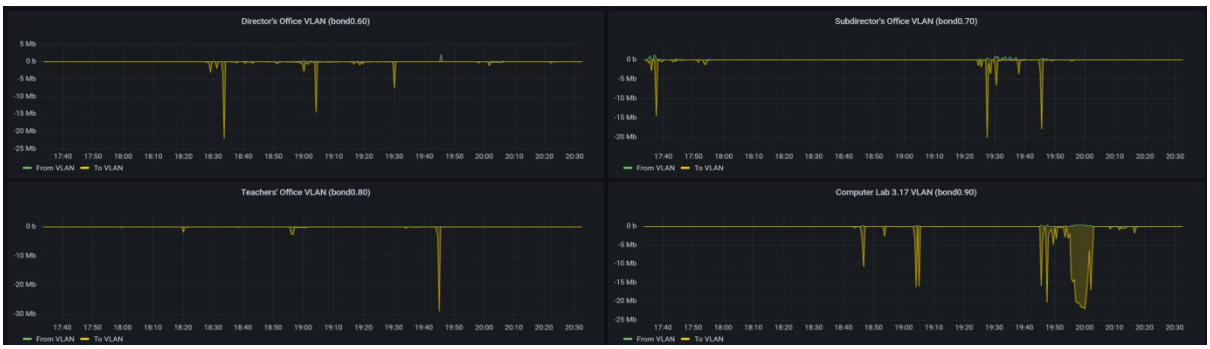
Το συγκεκριμένο λογισμικό μπορεί να χρησιμοποιήσει ένα σύνολο από πηγές για την άντληση δεδομένων προς απεικόνιση όπως για παράδειγμα τις βάσεις δεδομένων MySQL, PostgreSQL, Influxdb και Microsoft SQL Server, το σύστημα συλλογής μετρικών συστήματος Prometheus και άλλα. Στην περίπτωση της συγκεκριμένης υλοποίησης έχει γίνει χρήση του Influxdb ως πηγή των δεδομένων.

Το Grafana χρησιμοποιεί ένα αρχείο ρυθμίσεων για τις βασικές του ρυθμίσεις. Ωστόσο το μεγαλύτερο ποσοστό των παραμετροποιήσεων γίνεται στο γραφικό περιβάλλον με την χρήση ενός φυλλομετρητή.

Στην περίπτωση του σχολικού δικτύου αποφασίστηκε να δημιουργηθούν συνολικά πέντε πίνακες γραφικών απεικονίσεων.

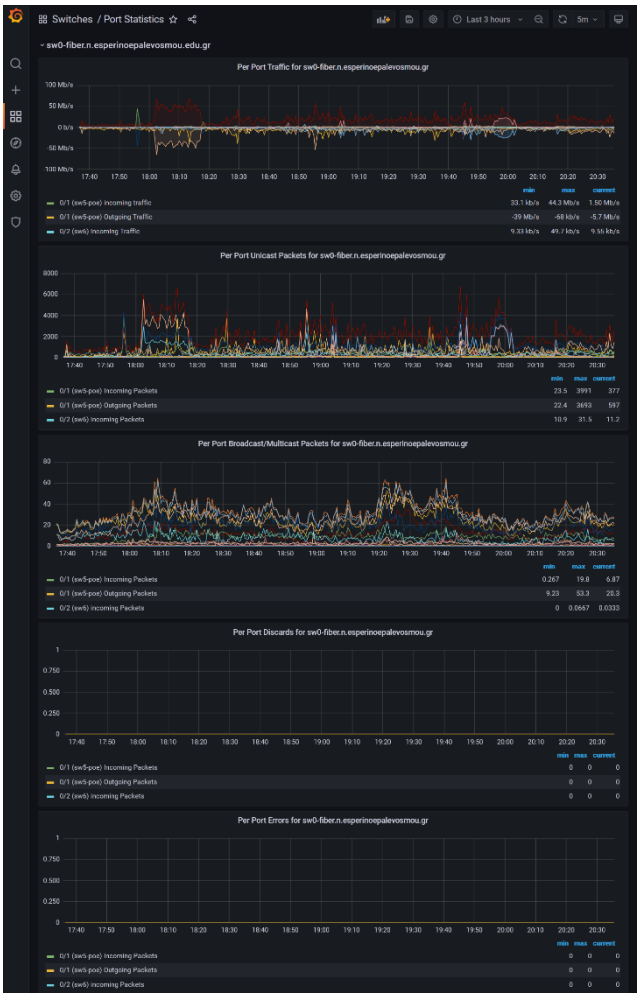
Ο πρώτος πίνακας ονομάστηκε “Core Router Metrics”. Αφορά στατιστικά κίνησης που αντλούνται από τον κεντρικό δρομολογητή. Στον συγκεκριμένο πίνακα γίνεται οπτικοποίηση της κίνησης ανά πάροχο διαδικτύου και στην συνέχεια της κίνησης ανά VLAN. Ακόμη γίνεται απεικόνιση της χρονικής διάρκειας που είναι λειτουργικός ο κεντρικός δρομολογητής (Uptime), της χρήσης του επεξεργαστή του (CPU Usage) και της μνήμης RAM (RAM Usage).





Εικόνα 46 & 47: Γραφική απεικόνιση στατιστικών του κεντρικού δρομολογητή και τμήματος των VLANs

Ο δεύτερος πίνακας ονομάστηκε “Port Statistics”. Αφορά στατιστικά κίνησης που αντλούνται από τον οπτικό διαμεταγωγέα και τους διαμεταγωγείς χαλκού. Στον συγκεκριμένο πίνακα γίνεται οπτικοποίηση της κίνησης για κάθε μία από τις πόρτες των διαμεταγωγέων που λειτουργούν στο δίκτυο.



Εικόνα 48: Γραφική απεικόνιση της κίνησης ανά διεπαφή σε έναν από τους διαμεταγωγείς.

Ο τρίτος πίνακας ονομάστηκε “WiFi Statistics”. Αφορά στατιστικά κίνησης που αντλούνται από τα δέκα σημεία πρόσβασης που λειτουργούν στον χώρο του σχολείου. Στον συγκεκριμένο πίνακα γίνεται οπτικοποίηση του αριθμού των πελατών στο ασύρματο δίκτυο συνολικά, του αριθμού των πελατών ανά SSID σε κάθε ένα από τα δέκα σημεία πρόσβασης αλλά και του ποσοστού των πελατών που προτιμά το φάσμα των 2.4GHz και 5GHz αθροιστικά αλλά και σε επίπεδο σημείου πρόσβασης.

Εικόνα 49: Γραφική απεικόνιση της κατάστασης του ασύρματου δικτύου.

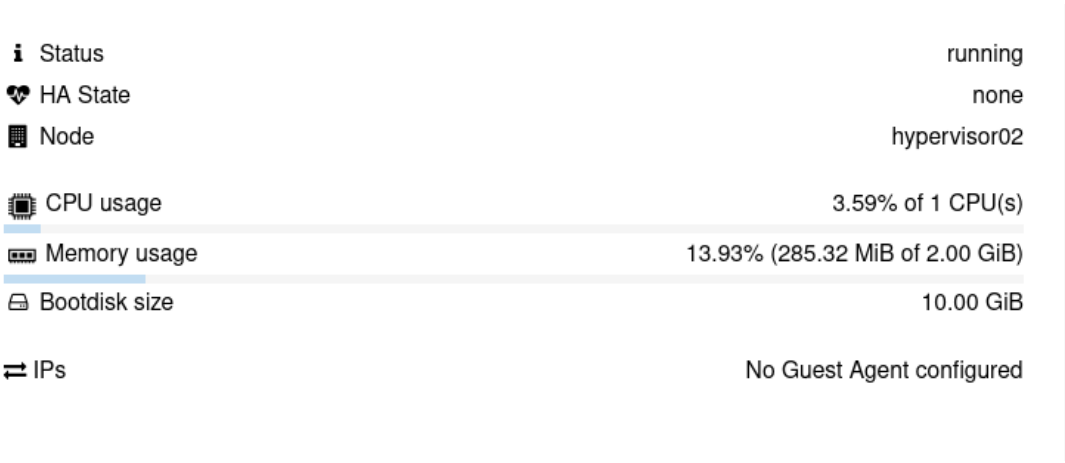
Ο τέταρτος πίνακας ονομάστηκε “Switch Internal Metrics” Αφορά μετρικά στοιχεία λειτουργίας των διαμεταγωγέων. Πιο συγκεκριμένα, στον πίνακα οπτικοποιούνται ο χρόνος λειτουργίας του εκάστοτε διαμεταγωγέα (Uptime), η χρήση του επεξεργαστή (CPU Usage) και της μνήμης (RAM Usage), η δικτυακή κίνηση προς τον ίδιο τον διαμεταγωγέα για διαχειριστικούς λόγους και οι θερμοκρασίες καθενός από τους διαμεταγωγείς.

Εικόνα 50: Γραφική απεικόνιση μετρικών λειτουργίας του οπτικού διαμεταγωγέα

Ο πέμπτος πίνακας ονομάστηκε “Access Points Internal Metrics” Αφορά μετρικά στοιχεία λειτουργίας των σημείων πρόσβασης. Πιο συγκεκριμένα στον πίνακα οπτικοποιούνται ο χρόνος λειτουργίας του εκάστοτε διαμεταγωγέα (Uptime), η χρήση του επεξεργαστή (CPU Usage) και της μνήμης (RAM Usage) αλλά και η κατάσταση του φάσματος (χρήση, παρεμβολές) από ένα υποσύνολο σημείων πρόσβασης που παρέχουν τις συγκεκριμένες πληροφορίες.

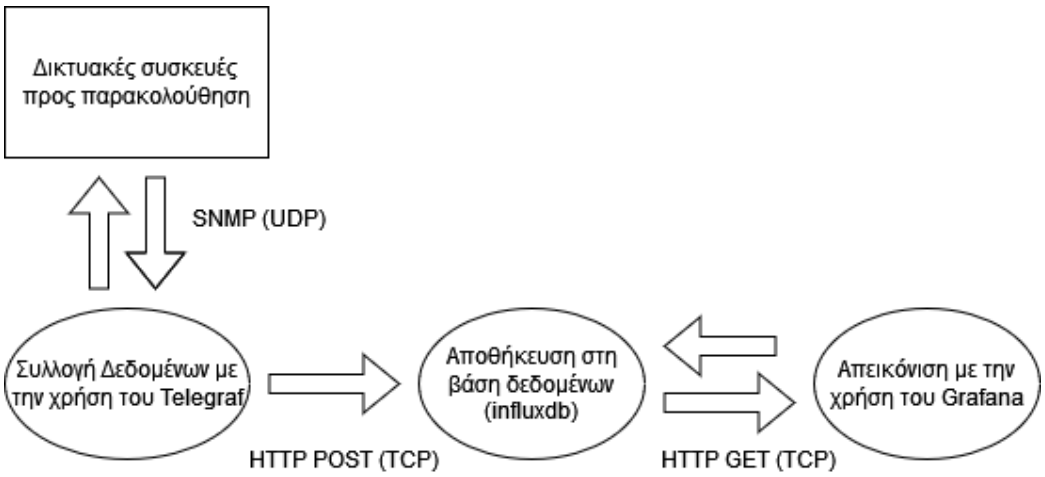
Εικόνα 51: Γραφική απεικόνιση μετρικών λειτουργίας ενός σημείου πρόσβασης

Το λογισμικό Grafana τρέχει σε μια εικονική μηχανή με λειτουργικό σύστημα Debian 10 και έχει αποδοθεί 1 vCPUs και 2GB RAM. Αναφορικά με τον αποθηκευτικό χώρο έχουν αποδοθεί 10GB μιας και δεν υπάρχουν ιδιαίτερες απαιτήσεις για αποθήκευση δεδομένων. Παρακάτω φαίνεται η χρήση των υπολογιστικών πόρων από την συγκεκριμένη εικονική μηχανή.



Εικόνα 52: Χρήση υπολογιστικών πόρων από το σύστημα δημιουργίας γραφημάτων

Συνοψίζοντας η ροή των δεδομένων από τις δικτυακές συσκευές ως την απεικόνιση τους ακολουθεί το παρακάτω διάγραμμα.



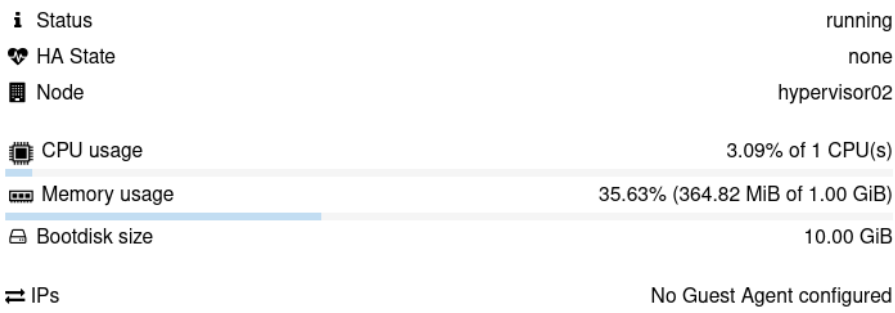
Εικόνα 53: Διάγραμμα ροής μετρικών δεδομένων δικτυακής κίνησης

Συγκέντρωση αρχείων καταγραφής 5.2.4

Κατά τη διαδικασία εύρεσης και επίλυσης προβλημάτων σημαντικό ρόλο παίζουν τα αρχεία καταγραφής, στα οποία η εκάστοτε συσκευή αποθηκεύει διάφορα συμβάντα κατά τη διάρκεια λειτουργίας της. Ωστόσο εάν τα αρχεία καταγραφής είναι διασκορπισμένα σε κάθε δικτυακή συσκευή και όχι συγκεντρωμένα σε ένα χώρο, η διαδικασία εύρεσης και συσχέτισης τους μπορεί να αποδειχθεί από εξαιρετικά χρονοβόρα έως αδύνατη. Επιπλέον μπορεί να υπάρχει αδυναμία πρόσβασης σε αυτά εάν η συσκευή η οποία τα παράγει έχει υποστεί βλάβη και δε λειτουργεί. Για αυτό το λόγο είναι καλή πρακτική η αποστολή των αρχείων καταγραφής, την ώρα της δημιουργίας τους σε έναν κεντρικό διακομιστή για την περαιτέρω επεξεργασία αλλά και αποθήκευση.

Η επικοινωνία και αποστολή των αρχείων καταγραφής γίνεται με τη χρήση ενός πρωτοκόλλου που ονομάζεται “syslog”. Χρησιμοποιεί είτε το πρωτόκολλο TCP στην πόρτα 6514 είτε το πρωτόκολλο UDP στην πόρτα 514 και υπάρχει αρχιτεκτονική ενός server και πολλαπλών clients. Ακόμη είναι εφικτή η κρυπτογράφηση της επικοινωνίας με τη χρήση του Transport Layer Security (TLS) όταν η επικοινωνία γίνεται από μη ασφαλή δίκτυα.

Στο σχολικό δίκτυο έχει δημιουργηθεί μια εικονική μηχανή για την συλλογή των αρχείων καταγραφής που χρησιμοποιεί το λογισμικό rsyslog για την αποδοχή μηνυμάτων από άλλους δικτυακούς κόμβους. Η συγκεκριμένη μηχανή χρησιμοποιεί το λειτουργικό σύστημα Debian 10 και τις έχει αποδοθεί 1 vCPU και 2GB RAM. Ακόμη έχουν αποδοθεί 10GB αποθηκευτικού χώρου. Παρακάτω φαίνεται η χρήση των υπολογιστικών πόρων από την συγκεκριμένη εικονική μηχανή.



Εικόνα 54: Χρήση υπολογιστικών πόρων από το σύστημα συγκέντρωσης αρχείων καταγραφής

Στην συγκεκριμένη εικονική μηχανή συγκεντρώνονται αρχεία καταγραφής από τα παρακάτω μηχανήματα.

- core-router
- sw0-fiber
- sw1-poe
- sw2
- sw3
- sw4
- sw5-poe
- sw6
- ap-01
- ap-02
- ap-03
- ap-04
- ap-05
- ap-06
- ap-07
- ap-08
- ap-09
- ap-10

Τα αρχεία καταγραφής διαχωρίζονται ανά συσκευή σε φακέλους. Το όνομα του φακέλου είναι η IP της δικτυακής συσκευής από την οποία γίνεται η συλλογή. Στην παρούσα περίοδο το σύστημα συγκέντρωσης αρχείων καταγραφής είναι ρυθμισμένο να διατηρεί όλα τα δεδομένα ανεξαρτήτου παλαιότητας.

Παρακολούθηση Συστήματος Αδιάλειπτης Παροχής Ισχύος (UPS) 5.2.5

Για την αδιάλειπτη τροφοδοσία του κεντρικού ικριώματος αλλά και του διακομιστή που φιλοξενεί τις εικονικές μηχανές που αναλύθηκαν παραπάνω και τον ασφαλή τερματισμό της λειτουργίας τους χωρίς το ρίσκο απώλειας δεδομένων έχει εγκατασταθεί ένα UPS 1400W. Το συγκεκριμένο μηχάνημα μπορεί να διατηρήσει σε λειτουργία τα μηχανήματα τα οποία τροφοδοτούνται από αυτό για χρονική διάρκεια δεκαπέντε λεπτών. Επικοινωνεί με τον διακομιστή μέσω USB. Στον διακομιστή έχει εγκατασταθεί το λογισμικό “apcupsd” το οποίο επικοινωνεί με το σύστημα αδιάλειπτης παροχής ισχύος. Μπορεί να αντλήσει πληροφορίες από αυτό για στοιχεία λειτουργίας του όπως είναι η τάση του δικτύου ηλεκτρικού ρεύματος, η τάση των συσσωρευτών του UPS και η θερμοκρασία του. Ακόμη σε περίπτωση που αντιληφθεί διακοπή παροχής ρεύματος από το δίκτυο ηλεκτροδότησης αναλαμβάνει να δώσει εντολή για ασφαλή τερματισμό λειτουργίας των εικονικών μηχανών και στη συνέχεια του διακομιστή που τις φιλοξενεί.

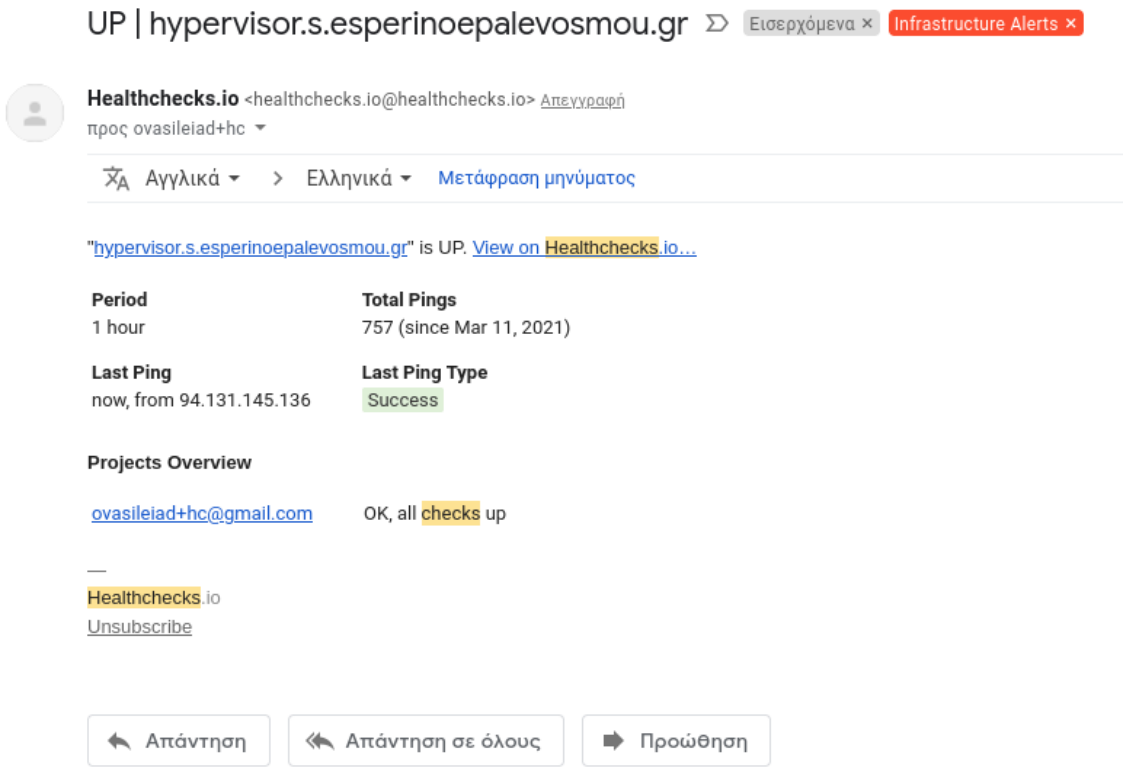
```
APC      : 001,036,0882
DATE     : 2022-02-28 15:14:21 +0200
HOSTNAME : hypervisor02
VERSION  : 3.14.14 (31 May 2016) debian
UPSNAME  : RACK_A_UPS
CABLE    : USB Cable
DRIVER   : USB UPS Driver
UPSMODE  : Stand Alone
STARTTIME: 2022-02-27 15:20:28 +0200
MODEL    : Back-UPS XS 1400U
STATUS   : ONLINE
LINEV    : 232.0 Volts
LOADPCT  : 30.0 Percent
BCHARGE  : 100.0 Percent
TIMELEFT : 17.3 Minutes
MBATTCHG : 5 Percent
MINTIMEL : 3 Minutes
MAXTIME  : 0 Seconds
SENSE    : Medium
LOTRANS  : 155.0 Volts
HITRANS  : 280.0 Volts
ALARMDEL : 30 Seconds
BATTV    : 27.1 Volts
LASTXFER : Automatic or explicit self test
NUMXFERS : 0
TONBATT  : 0 Seconds
CUMONBATT: 0 Seconds
XOFFBATT : N/A
SELFTEST : NO
STATFLAG : 0x05000008
SERIALNO : 4B1935P14356
BATTDATE : 2019-08-29
NOMINV   : 230 Volts
NOMBATTV : 24.0 Volts
NOMPOWER : 700 Watts
FIRMWARE : 926.T2 .I USB FW:T2
END APC  : 2022-02-28 15:14:27 +0200
```

Εικόνα 55: Πληροφορίες που αντλούνται από το σύστημα αδιάλειπτης παροχής ισχύος

Επιπλέον κατά τη διακοπή ρεύματος, επαναφορά της ηλεκτροδότησης ή άλλου σφάλματος το συγκεκριμένο λογισμικό είναι ρυθμισμένο να στέλνει μήνυμα ηλεκτρονικού ταχυδρομείου στο διοικητικό προσωπικό του σχολείου προς ενημέρωση τους.

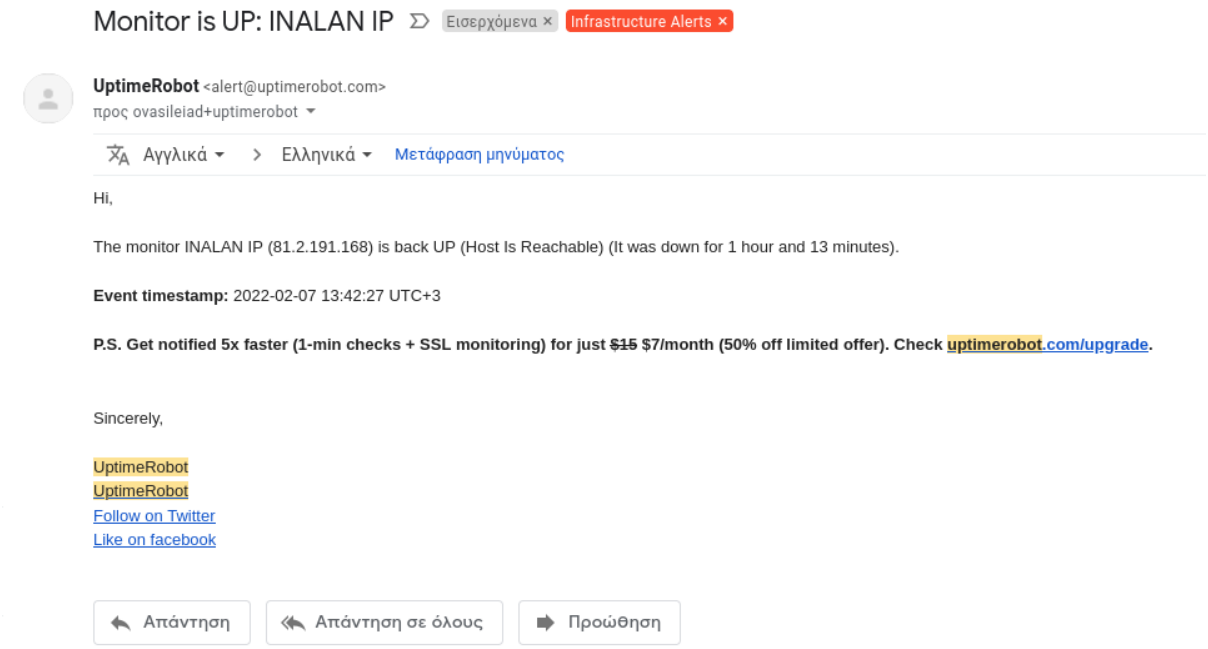
Παρακολούθηση Σύνδεσης στο Διαδίκτυο 5.2.6

Το βασικό γεγονός για το οποίο επιθυμούσε να είναι ενήμερο το διοικητικό προσωπικό του σχολείου είναι η κατάσταση σύνδεσης στο διαδίκτυο, για τη σωστή ενημέρωση στη συνέχεια του εκπαιδευτικού προσωπικού και των μαθητών και την εναλλαγή προς τον εφεδρικό πάροχο διαδικτύου με σκοπό την επιχειρησιακή συνέχεια του σχολείου. Γι' αυτό το λόγο έγινε χρήση δύο υπηρεσιών, του "healthchecks.io" και του "UptimeRobot". Στην περίπτωση του "healthchecks.io", έχει οριστεί στον διακομιστή των εικονικών μηχανών να τρέχει ένα script κάθε 15 λεπτά μέσω του συστήματος χρονοπρογραμματισμού cron, το οποίο εκτελεί ένα HTTP GET αίτημα σε διακομιστή της συγκεκριμένης πλατφόρμας. Εάν η συγκεκριμένη υπηρεσία δε λάβει αίτημα μετά από είκοσι λεπτά από το τελευταίο σημαίνει ότι ο διακομιστής δε λειτουργεί ή δεν έχει πρόσβαση στο διαδίκτυο και αποστέλλεται ένα μήνυμα ηλεκτρονικού ταχυδρομείου που ενημερώνει το διοικητικό προσωπικό για το συγκεκριμένο θέμα.



Εικόνα 56: Ειδοποίηση μέσω ηλεκτρονικού ταχυδρομείο από το healthchecks.io

Όσο αφορά το UptimeRobot, η συγκεκριμένη υπηρεσία λειτουργεί πραγματοποιώντας επαναλαμβανόμενα “Pings” προς συγκεκριμένες IP διευθύνσεις. Σε περίπτωση που δεν υπάρχει απάντηση σε αυτά τότε αποστέλλεται μήνυμα ηλεκτρονικού ταχυδρομείου προς το διοικητικό προσωπικό για ενημέρωση τους. Πράγματι με τη χρήση της συγκεκριμένης υπηρεσίας γίνεται παρακολούθηση των δημόσιων IP διευθύνσεων, τόσο του εμπορικού παρόχου όσο και του Πανελλήνιου Σχολικού Δικτύου. Παρακάτω φαίνεται παράδειγμα μιας ειδοποίησης από την συγκεκριμένη υπηρεσία.



Εικόνα 57: Ειδοποίηση μέσω ηλεκτρονικού ταχυδρομείο από το UptimeRobot

ΚΕΦΑΛΑΙΟ 6 - Συμπεράσματα

Συμπεραίνοντας, η βελτίωση στις παρεχόμενες υπηρεσίες για το εκπαιδευτικό προσωπικό αλλά και τους μαθητές ήταν ιδιαίτερα εμφανής. Υπάρχει σημαντική αναβάθμιση της ταχύτητας στο διαδίκτυο ικανή να υποστηρίξει τις νέες ανάγκες για τηλεκπαίδευση αλλά και χρήση πολυμεσικών εφαρμογών κατά τη διάρκεια του μαθήματος ενώ υπάρχει ενσύρματη πρόσβαση με ταχύτητες 1Gb/s τοπικά σε όλους του χώρους κάτι που προηγουμένως δεν υπήρχε και δυσχέραινε τόσο τη διοικητική όσο και την εκπαιδευτική διαδικασία, ενώ καθιστούσε ανέφικτη την ανταλλαγή δεδομένων. Επιπρόσθετα, η πλήρης κάλυψη του κτηρίου με ασύρματη πρόσβαση στο διαδίκτυο έδωσε τη δυνατότητα στους εκπαιδευτικούς να μπορούν να χρησιμοποιήσουν οποιαδήποτε αίθουσα για να πραγματοποιήσουν μαθήματα που απαιτούσαν προβολή κάποιων δεδομένων από το διαδίκτυο με τη χρήση των προσωπικών τους υπολογιστών και όχι μόνο τα εργαστήρια Πληροφορικής. Το ασύρματο δίκτυο έγινε ιδιαίτερα δημοφιλές και μεταξύ των μαθητών για τη μεταξύ τους επικοινωνία αλλά και άντληση πληροφοριών σχετικά με τα μαθήματα τους, κάτι που φαίνεται και από τους ιδιαίτερα υψηλούς αριθμούς συσκευών ταυτόχρονα συνδεδεμένων σε αυτό. Τέλος η νέα υποδομή βελτίωσε κατά πολύ τη δυνατότητα παρακολούθησης της καλής λειτουργίας του δικτύου και γρήγορης επιδιόρθωσης προβλημάτων που τυχόν να υπάρξουν από τους εκπαιδευτικούς Πληροφορικής και τη Διοίκηση του σχολείου χάρη στα συστήματα συλλογής και απεικόνισης στατιστικών, στην έκδοση ειδοποιήσεων σε περιπτώσεις βλαβών και μη απόκρισης κάποιας συσκευής αλλά και στην ενοποιημένη φύση του νέου δικτύου, σε αντίθεση με το παλαιότερο που ήταν διαχωρισμένο αλλά και επικαλυπτόμενο όσο αφορά την διευθυνσιοδότηση του.

Μελλοντικά σχεδιάζεται η περαιτέρω εκμετάλλευση της εγκατεστημένης υποδομής με την επέκταση του δικτύου στο αμφιθέατρο του σχολικού συγκροτήματος, την αντικατάσταση της τηλεφωνίας με νέα τεχνολογίας VoIP και την εγκατάσταση στον διακομιστή εφαρμογών όπως ηλεκτρονική τάξη(e-class), κοινόχρηστων χώρων αποθήκευσης και αυτοματοποιημένη λήψη αντιγράφων ασφαλείας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ethernet
   https://en.wikipedia.org/wiki/Ethernet

2. IEEE 802.3 Ethernet Working Group
   https://www.ieee802.org/3/

3. Fiber Optic Networks
   https://www.sciencedirect.com/topics/engineering/fiber-optic-networks

4. IEEE 802.11
   https://en.wikipedia.org/wiki/IEEE_802.11

5. High Density WiFi Deployments
   https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/High_Density_Wi-Fi_Deployments

6. Simple Network Management Protocol
   https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

7. Το πρωτόκολλο SNMP
   http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/teaching_m/management/snmp.htm

8. RFC2271 – An architecture for Describing SNMP Management Networks
   https://datatracker.ietf.org/doc/html/rfc2271

9. Attacks on the RC4 Stream Cipher, Andreas Klein (2007)
   https://membres-ljk.imag.fr/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/WEP/KleinRC4.pdf

10. RFC5424 – The Syslog Protocol
    https://datatracker.ietf.org/doc/rfc5424/