

Ολοκληρωμένη ΕΛΛΑΚ λύση δικτυακής οργάνωσης σχολικής μονάδας και συγκροτημάτων

Καλκάνης Θωμάς¹, Ταλάρη Αναστασία²

¹ Καθηγητής Πληροφορικής, 1ο Γενικό Λύκειο Γρεβενών

tkalkanis@sch.gr

² Καθηγήτρια Πληροφορικής, 1ο ΕΠΑ.Λ. Δυτικής Φραγκίστας Ν. Ευρυτανίας

atalari@sch.gr

ΠΕΡΙΛΗΨΗ

Στόχος της εργασίας είναι η παρουσίαση μίας ολοκληρωμένης λύσης για την υλοποίηση και την συντήρηση της δικτυακής υποδομής ενός σχολείου. Αρχικά παρουσιάζονται πιθανές τοπολογίες δικτύων με κατάλληλα υποδίκτυα και υπηρεσίες που απαιτούνται για την εύρυθμη διασύνδεσή τους. Στη συνέχεια περιγράφεται αναλυτικότερα ένα πιθανό σενάριο χρήσης που θα μπορούσε εύκολα να υλοποιηθεί με την εγκατάσταση του ΕΛΛΑΚ λογισμικού Zentyal. Τέλος, περιγράφονται τα αποτελέσματα που προέκυψαν από την υλοποίηση τμημάτων του πιθανού σεναρίου σε περιπτώσεις σχολείων μικρής και μεσαίας έκτασης.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: δικτυακές υποδομές, σχολικό εργαστήριο, zentyal

ΕΙΣΑΓΩΓΗ

Στην πορεία της σταδιοδρομίας μας στο δημόσιο σχολείο έχουμε συναντήσει πολλές και διαφορετικές τοπολογίες διασύνδεσης υπολογιστών εργαστηρίων και γραφείων. Σε προηγούμενα χρόνια, το κάθε εργαστήριο πληροφορικής (στο εξής απλά εργαστήριο) είχε την δική του σύνδεση στο Διαδίκτυο (στο εξής απλά Internet για ευκολία στην διάκριση από τους όρους δίκτυο και υποδίκτυο), ενώ το γραφείο του διευθυντή και η γραμματεία είχαν μια διαφορετική σύνδεση. Τα τελευταία χρόνια, με την αναβάθμιση των γραμμών σε τεχνολογία ADSL, τα διαφορετικά αυτά δίκτυα ενώθηκαν και απέκτησαν πρόσβαση στο Internet μέσω της ίδιας κοινής γραμμής. Ως αποτέλεσμα, αυτή τη στιγμή στα περισσότερα μικρά σχολεία, όλες οι συσκευές βρίσκονται πάνω στο ίδιο δίκτυο. Αν και υπάρχουν εξαιρέσεις, δυστυχώς δεν είναι ο κανόνας και η κάθε μία από τις διάφορες υλοποιήσεις είτε είναι διαφορετική σε οργάνωση, είτε είναι διαφορετική σε λογισμικό.

Έπειτα από συζητήσεις με τεχνικούς υπεύθυνους, από αναζητήσεις forum, αλλά και από άλλες πηγές, σε γενικές γραμμές προέκυψαν τα εξής:

- Τα εργαστήρια και το υλικό σε αυτά, δεν επαρκούν για το πλήθος των μαθητών
- Κάποιες φορές, τα εργαστήρια παραμένουν αδρανή (πχ χρήση μόνο για μια απλή παρουσίαση ή για την επίδειξη σελίδων στο Internet, χωρίς απαραίτητα να συμμετέχουν ενεργά οι μαθητές)
- Σε κάποιες άλλες περιπτώσεις, τα εργαστήρια χρησιμοποιούνται από εξωσχολικούς (προγράμματα εκπαίδευσης, σεμινάρια κ.α.)

- Οι τοπολογίες ποικίλουν, με κυρίαρχη αυτή στην οποία όλες οι συσκευές είναι ομότιμες
- Η πρόσβαση σε ασύρματα (wifi) δίκτυα είναι σχεδόν ελεύθερη με ταυτόχρονη πρόσβαση σε ευαίσθητα δεδομένα του σχολείου
- Οι κωδικοί ασφαλείας στα νευραλγικά μηχανήματα είναι συνήθως αδύναμοι
- Το εγκατεστημένο ιδιόκτητο λογισμικό έχει απαξιωθεί ή δεν είναι ενημερωμένο
- Δεν υπάρχουν σχεδόν πουθενά πολιτικές αποθήκευσης δεδομένων
- Η έννοια της διαχείρισης έχει σχεδόν καταργηθεί

Τα αναφερθέντα γεγονότα οδηγούν σε μια σειρά προβλημάτων στα οποία θα πρέπει να δοθεί ιδιαίτερη σημασία, αφού κατά κύριο λόγο έχουν σχέση με την ασφάλεια και τα προσωπικά δεδομένα.

ΠΡΟΒΛΗΜΑΤΑ

ΑΣΦΑΛΕΙΑΣ

Η πιο συνηθισμένη τοπολογία είναι αυτή στην οποία, όλες οι συσκευές είναι συνδεδεμένες πάνω στο ίδιο δίκτυο. Συνήθως αυτές οι συσκευές είναι οι υπολογιστές του εργαστηρίου, οι υπολογιστές των γραφείων της γραμματείας και του διευθυντή, οι υπολογιστές των γραφείων των καθηγητών και τα διάφορα Access Points. Τα προβλήματα μπορεί να προέλθουν:

- Από τις ασύρματες συσκευές: Δυστυχώς, δεν υπάρχει κάποιο απολύτως ασφαλές πρωτόκολλο σύνδεσης σε ασύρματα δίκτυα ευρείας χρήσης. Αυτό σημαίνει ότι οι συσκευές που συνδέονται στα Access Points δεν μπορούν να θεωρηθούν ασφαλείς. Υπάρχουν ήδη πάρα πολλές αναφορές για προβλήματα στην ασφάλεια των πρωτοκόλλων WEP και WPA και τα τελευταία δύο χρόνια ανακαλύφθηκαν προβλήματα και στο πρωτόκολλο WPA2 (AES και TKIP) (Kumkar et al., 2012; Sukhija & Gupta, 2012). Συνεπώς τα Access Points δεν θα πρέπει να έχουν σχέση με τα γραφεία της διεύθυνσης του σχολείου. Λαμβάνοντας υπόψη και το γεγονός ότι σε κάθε Access Point μπορεί να προσπαθήσει (και ίσως να επιτύχει) να συνδεθεί και οποιοσδήποτε εξωσχολικός παράγοντας, η προηγούμενη άποψη ενισχύεται αισθητά.
- Από τους υπολογιστές στο γραφείο των καθηγητών: Οι υπολογιστές στα γραφεία των καθηγητών χρησιμοποιούνται κυρίως, για την εκτύπωση ασκήσεων, για την αναζήτηση πληροφοριών και γενικά για θέματα που δεν αφορούν γραφειοκρατικές ή διοικητικές διαδικασίες, και βέβαια δεν απαιτούν πρόσβαση στα προσωπικά δεδομένα των μαθητών ή στα αρχεία και τα έγγραφα του σχολείου. Αν και οι συγκεκριμένες συσκευές συνήθως συντηρούνται σωστά (ενημερώσεις ασφαλείας, αντίϊκα λογισμικά κ.α.), πάντα υπάρχει η πιθανότητα να προσβληθούν από κακόβουλο λογισμικό του Internet ή από λογισμικό που μεταφέρθηκε σε αυτές από κάποιο εξωτερικό αποθηκευτικό μέσο (USB Stick, εξωτερικός σκληρός δίσκος κ.α.). Συνεπώς, στην καθημερινή χρήση, ούτε αυτές οι συσκευές θα έπρεπε να είναι συνδεδεμένες στο ίδιο δίκτυο με τη γραμματεία και τα Access Points.
- Από το εργαστήριο: Οι υπολογιστές του εργαστηρίου συντηρούνται περισσότερο από κάθε άλλο υπολογιστή σε μια σχολική μονάδα, κάτι που

όμως, δεν είναι αρκετό. Οι μαθητές φέρνουν μαζί τους τις δικές τους εξωτερικές συσκευές αποθήκευσης και πλοηγούνται οπουδήποτε θέλουν στο Internet. Συνάμα, με δεδομένα το μεγάλο πλήθος μαθητών και τον μοναδικό εκπαιδευτικό πληροφορικής, η κατάσταση δυσχεραίνει ιδιαίτερα. Τα πράγματα έχουν γίνει ακόμη πιο δύσκολα τα τελευταία χρόνια, όπου το εργαστήριο χρησιμοποιείται από καθηγητές κάθε ειδικότητας για την υλοποίηση Projects, Προγραμμάτων, διαφόρων εργασιών κ.α. Τέλος δεν πρέπει να παραληφθεί η αναφορά στην χρήση των εργαστηρίων από εξωσχολικούς εκπαιδευόμενους οι οποίοι είναι λογικό να μην γνωρίζουν τυχόν πολιτικές χρήσης, και να προκαλέσουν προβλήματα ακούσια ή εκούσια προσπαθώντας να εφαρμόσουν τις δικές τους εμπειρίες χρήσης.

Η μόνη γραμμή άμυνας αυτή τη στιγμή, σε υλοποιήσεις όπως οι προηγούμενες, είναι τα φίλτρα του σχολικού δικτύου, τα οποία δεν είναι αρκετά, αφού αφορούν και περιορίζουν μόνο την πρόσβαση μαθητών σε σελίδες προστατεύοντας αυτούς και τα μηχανήματα από κακόβουλο λογισμικό που πιθανόν να υπάρχει σε αυτές.

ΑΚΕΡΑΙΟΤΗΤΑΣ ΚΑΙ ΠΡΟΣΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Ένα άλλο συχνό πρόβλημα που συναντήσαμε είναι η μη λήψη αντιγράφων ασφαλείας, ή η μη οργανωμένη λήψη αυτών. Στα περισσότερα σχολεία οι διευθυντές και οι καθηγητές συνηθίζουν να δίνουν έμφαση μόνο σε συγκεκριμένες εφαρμογές του Υπουργείου (πχ εφαρμογές της εταιρείας Έπαφος) και κυριολεκτικά ξεχνούν όλα τα υπόλοιπα αρχεία. Αποτέλεσμα αυτού είναι να χάνεται πολλές φορές η ηλεκτρονική μορφή σημαντικών εγγράφων και η μόνη πρόσβαση σε πληροφορίες παλαιότερων ετών να γίνεται χειροκίνητα μέσα από στοίβες χαρτιού. Μερικώς το πρόβλημα θα εξαλειφθεί τα επόμενα χρόνια με την χρήση των online εφαρμογών του Υπουργείου, αλλά όχι πλήρως και σίγουρα όχι για τα έγγραφα του σχολείου.

Ένα άλλο γεγονός, το οποίο απλά είναι χρονοβόρο ή σε κάποιες περιπτώσεις μπορεί να γίνει και ενοχλητικό, είναι η αποθήκευση προσωπικών αρχείων των εκπαιδευτικών, είτε σε κοινόχρηστους υπολογιστές, είτε σε εξωτερικές μονάδες (με τον κίνδυνο μεταφοράς ιών) είτε σε κάποια υπηρεσία Cloud. Στην πρώτη περίπτωση, δεν υπάρχει καμία εγγύηση ότι τα έγγραφα του κάθε εκπαιδευτικού θα συνεχίσουν να βρίσκονται στον ίδιο υπολογιστή και τις επόμενες μέρες, εφόσον πρόκειται για κοινόχρηστο υπολογιστή. Οποιοσδήποτε ανήκει στο προσωπικό μπορεί να τον χρησιμοποιήσει, να προσπελάσει τα αποθηκευμένα σε αυτόν αρχεία, ακόμα και να σβήσει όποιο δεν θεωρεί χρήσιμο. Στην δεύτερη περίπτωση, η μεταφορά και μετάδοση ιών είναι πιθανή. Στην τρίτη περίπτωση, η πρόσβαση στο Cloud εξαρτάται από την πρόσβαση στο Internet και επομένως δεν είναι πάντα εγγυημένη.

Τελευταία επίσης, είναι εμφανές το πρόβλημα διαμοιρασμού της γραμμής του Internet. Όσο αυξάνονται οι online υπηρεσίες στις οποίες απαιτείται πρόσβαση (πχ myschool), τόσο πιο σημαντική είναι η άμεση πρόσβαση σε αυτές. Με την τωρινή κατάσταση, τη στιγμή που το εργαστήριο χρησιμοποιείται για κάποιο μάθημα και οι υπολογιστές είναι όλοι σε χρήση, το υπόλοιπο σχολείο έχει πρόσβαση στο Internet με πολύ μικρές ταχύτητες, γεγονός που κάνει την χρήση των εφαρμογών σχεδόν αδύνατη ή με μεγάλη πιθανότητα λαθών.

ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ

Ένα δίκτυο, οργανωμένο όπως το παραπάνω απαιτεί αρκετό χρόνο για την διαχείρισή του (ΥΠΑΙΘ, 2004). Οι κωδικοί στο ασύρματο θα πρέπει να αλλάζουν συχνά, οι καθηγητές να ενημερώνονται για όλες τις αλλαγές που τους επηρεάζουν, ο

κάθε υπολογιστής θα πρέπει να έχει ενεργοποιημένο και σωστά ρυθμισμένο κάποιο τείχος προστασίας, οι υπολογιστές να είναι πάντα ενημερωμένοι με τα τελευταία στοιχεία ασφαλείας κ.α. Αν και οι διαδικασίες συντήρησης σε ένα τέτοιο δίκτυο δεν είναι ιδιαίτερα σύνθετες, χρήζουν έως και καθημερινής επανάληψης σε κάθε υπολογιστή. Το πρόβλημα γίνεται ακόμη μεγαλύτερο σε πολύ μεγάλα συγκροτήματα σχολείων, όπου αυξάνει περισσότερο το πλήθος των εργαστηρίων και γενικότερα των υπολογιστών.

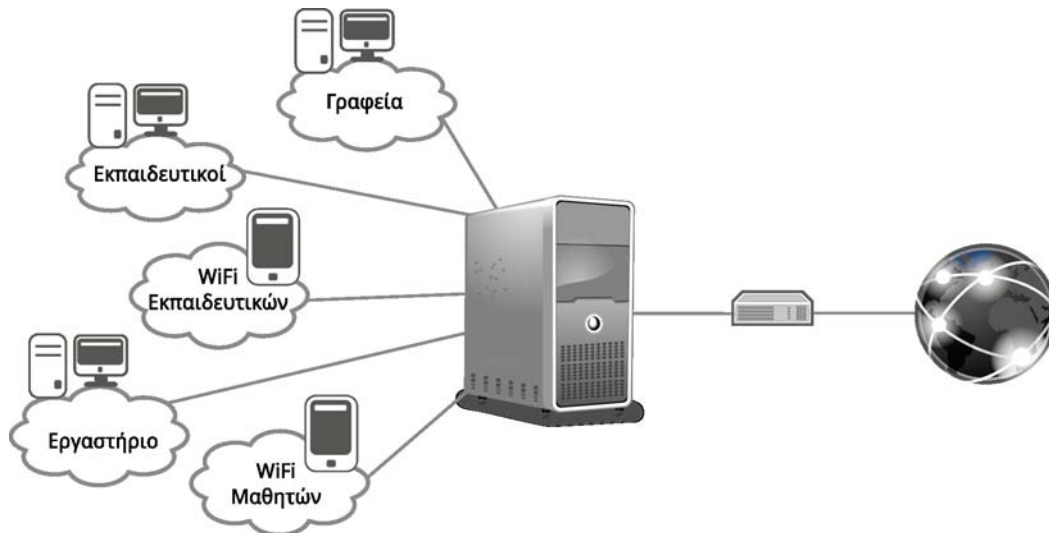
Στη διαχείριση του δικτύου θα πρέπει να συμπεριληφθεί και η διαχείριση της πρόσβασης στο Internet. Πάνω σε αυτό το θέμα γίνεται μια πολύ καλή προσπάθεια μέσα από τα online σεμινάρια του πανελλήνιου σχολικού δικτύου, προς εκπαιδευτικούς πληροφορικής, με θέμα την εγκατάσταση του squid proxy server. Όμως, η εγκατάσταση και η ρύθμιση ενός proxy δεν είναι ιδιαίτερα εύκολη και ο βαθμός δυσκολίας αυξάνει όταν πρέπει να ρυθμιστούν παράμετροι προτεραιότητας συσκευών. Τέλος, η λύση αυτή δεν ενδείκνυται ως έχει, για ασύρματες (ή ενσύρματες) συσκευές που φέρουν μαζί τους καθηγητές και μαθητές αφού απαιτούνται ρυθμίσεις στα μηχανήματα των χρηστών (είτε για τη είσοδο στο Domain, είτε για την αυτόματη απόδοση των ρυθμίσεων για το squid, είτε για την χειροκίνητη ρύθμιση) (Σιάχος, 2009).

ΥΠΟΔΟΜΗ

ΥΠΟΔΙΚΤΥΑ

Όπως έχει ήδη αναφερθεί, στα περισσότερα σχολεία η πρόσβαση στο Internet παρέχεται από το σχολικό δίκτυο και όλοι οι υπολογιστές των γραφείων και τα access points συνδέονται απευθείας πάνω στο switch του εργαστηρίου. Για να αποφευχθούν(ή έστω να περιοριστούν) τα προβλήματα που προαναφέραμε, η πρότασή μας είναι απλή και σχετικά φθηνή. Όσον αφορά το υλικό μέρος, πιστεύουμε ότι θα πρέπει να δημιουργηθούν, τόσα σε πλήθος πραγματικά (ή εικονικά VLAN) υποδίκτυα σε πλήθος, όσες και οι διαφορετικές εργασίες που εξυπηρετούν. Για το κάθε υποδίκτυο θα πρέπει να δημιουργηθούν κανόνες στο τείχος προστασίας, ώστε να επιτρέπεται η πρόσβαση στα μηχανήματα με τα κρίσιμα δεδομένα, μόνο όταν απαιτείται. Για παράδειγμα, δεν πρέπει να επιτρέπεται σε καμία ασύρματη συσκευή να έχει πρόσβαση στο υποδίκτυο της γραμματείας και της διεύθυνσης. Ενδεικτικά, (και όχι απαραίτητα όλα όσα αναφέρονται παρακάτω) μερικά τέτοια υποδίκτυα, όπως αναπαρίστανται και στο Σχήμα 1, θα μπορούσαν να είναι:

- Εξωτερικό: Για την πρόσβαση στο Internet
- Εργαστηρίου/ων: Μόνο για τους υπολογιστές όλων των εργαστηρίου
- Wifi καθηγητών: Μόνο για τις ασύρματες συνδέσεις των καθηγητών
- Wifi μαθητών: Μόνο για τις ασύρματες συνδέσεις των μαθητών
- Διεύθυνση και γραμματεία: Για τα μηχανήματα των γραφείων
- Καθηγητές: Για τα μηχανήματα του σχολείου που χρησιμοποιούν οι καθηγητές ή αυτά που φέρνουν μαζί τους



Σχήμα 1: Τυπική αναπαράσταση υποδικτύων

Όλα τα παραπάνω υποδίκτυα θα μπορούσαν να υλοποιηθούν σε πολύ μεγάλα σχολεία. Σε γενικές γραμμές, για τυπικές περιπτώσεις σχολείων, που διαθέτουν το πολύ δύο εργαστήρια, έναν με δύο υπολογιστές στη γραμματεία και το γραφείο της διεύθυνσης, το πολύ δύο υπολογιστές για το εκπαιδευτικό προσωπικό και πιθανόν εγκατεστημένη υποδομή παροχής ασύρματης πρόσβασης, τα παρακάτω υποδίκτυα είναι αρκετά:

- Εξωτερικό
- Εργαστηρίου/ων
- Διεύθυνση και γραμματεία
- Wifi και ενσύρματο καθηγητών
- Wifi μαθητών

Ακόμη πιο οικονομική λύση είναι η ακόλουθη όπου στα περισσότερα σχολεία, τα τρία ή και τα τέσσερα από τα παρακάτω υποδίκτυα είναι αρκετά:

- Εξωτερικό
- Εργαστηρίου/ων
- Διεύθυνση, γραμματεία και καθηγητές
- Wifi (απαραίτητα συνδυασμένο με κάποιο Captive Portal)

Σε ιδιαίτερες περιπτώσεις, όπως για παράδειγμα πολύ μεγάλα συγκροτήματα κτιρίων, ΣΕΚ κ.α. θα μπορούσαν όλες οι εξωτερικές γραμμές να συνδεθούν στο εξωτερικό υποδίκτυο και τα εσωτερικά υποδίκτυα θα μπορούσαν να χωριστούν κατάλληλα και ανάλογα με την λειτουργία τους:

- Ένα εξωτερικό υποδίκτυο (όλα τα modems)
- Υποδίκτυα ομάδων εργαστηρίων (μία ή περισσότερες)
- Υποδίκτυα γραφείων (ένα για κάθε μονάδα)
- Κοινό Wifi Μαθητών όλων των μονάδων
- Κοινό Wifi Καθηγητών όλων των μονάδων

Το κόστος όλων των παραπάνω λύσεων έχει σχέση με το πλήθος των υποδικτύων, άρα και με το πλήθος των καρτών δικτύου και των επιπλέον switch, συνεπώς είναι χαμηλό. Στην χειρότερη περίπτωση μπορεί να χρειαστούν μερικές δεκάδες μέτρα επιπλέον καλωδίου δικτύου, αλλά και πάλι το κόστος παραμένει χαμηλό. Τα παραπάνω θα μπορούσαν να υλοποιηθούν και με εικονικά δίκτυα (VLAN), αυξάνοντας όμως το κόστος, λόγω του εξειδικευμένου υλικού (managed switches)

που θα χρειαζόταν, αλλά και τον χρόνο της καμπύλης μάθησης μαζί με τους απαιτούμενους χρόνους εγκατάστασης και συντήρησης.

ΚΕΝΤΡΙΚΟΣ ΔΙΑΚΟΜΙΣΤΗΣ SBS

Για να υποστηριχθεί ένα δίκτυο με τόσα υποδίκτυα, χρειάζεται αρκετή εργασία ή κάποιο λογισμικό, ικανό να διαχειριστεί με εύκολο τρόπο την επιλεγμένη τοπολογία. Θα μπορούσε να χρησιμοποιηθεί κάποιος έτοιμος router, αλλά τα χρήματα που θα απαιτούνταν θα ήταν πολλά και οι λειτουργίες θα περιοριζόταν σε καθαρά δικτυακές λειτουργίες. Η πρότασή μας αφορά την χρήση ενός SBS (Small Business Server) Server και συγκεκριμένα του Zentyal. Το Zentyal, είναι λογισμικό κατηγορίας ΕΛΛΑΚ (Ελεύθερο Λογισμικό/Λογισμικό Ανοικτού Κώδικα), έχει ήδη χρησιμοποιηθεί σε σχολεία του εξωτερικού (Cambroneiro, 2013; Zentyal authors, 2012) και προσφέρει αρκετά περισσότερες δυνατότητες από έναν απλό router. Άλλωστε το ΕΛΛΑΚ προωθείται ιδιαίτερα από το τμήμα Τεχνικής Στήριξης του Πανελληνίου Σχολικού Δικτύου, για χρήση στα σχολικά εργαστήρια πληροφορικής (Υπηρεσία τεχνικής υποστήριξης πανελληνίου σχολικού δικτύου, 2010).

Ένας απλός υπολογιστής, με μερικές κάρτες δικτύου και εγκατεστημένο το Zentyal, μπορεί να μετατραπεί σε δρομολογητή με δυνατότητες δρομολόγησης, φιλτραρίσματος, τείχους προστασίας, ids/ips (intrusion detection system / intrusion prevention system) κ.α. Περιληπτικά αναφέρουμε τις δυνατότητες του Zentyal (Zentyal official documentation, 2014):

- **Διαχείριση δικτύου:** Μέσω γραφικού περιβάλλοντος μπορούν να διαχωριστούν τα υποδίκτυα, να καθοριστούν κανόνες στο τείχος προστασίας, να εφαρμοστούν πολιτικές αναγνώρισης επιθέσεων και γενικότερα να διευθετηθούν τυπικές διαδικασίες διαχείρισης δικτύου.
- **Traffic Shaping:** Η υπηρεσία θα μπορούσε να μεταφραστεί ως “Υπηρεσία ελέγχου εύρους ζώνης και ταχύτητας” μέσω της οποίας περιορίζεται κατάλληλα το εύρος της εξωτερικής γραμμής που μπορεί να χρησιμοποιήσει το κάθε υποδίκτυο. Μάλιστα είναι δυνατό, το εύρος αυτό να είναι δυναμικό ή/και να αφορά μόνο συγκεκριμένες υπηρεσίες
- **Χρήστες και δικαιώματα:** Παρέχεται η δυνατότητα σε κάθε χρήστη των υπολογιστών του δικτύου να έχει προσωπικό όνομα χρήστη και συνθηματικό και να ανήκει σε μία ή περισσότερες ομάδες. Η μαζική δημιουργία τους είναι ιδιαίτερα εύκολη και σύντομη. Τα διαπιστευτήρια αυτά συνδυάζονται με άλλες υπηρεσίες που παρέχονται όπως διαμοιρασμός φακέλων, captive portal, proxy κ.α.
- **Φιλτράρισμα περιεχομένου:** Ένας Zentyal server μπορεί να λειτουργήσει ως proxy server (απλό ή “διάφανο” -- transparent proxy) με δυνατότητες φιλτραρίσματος περιεχομένου και περιορισμού της ταχύτητας πρόσβασης. Έχει ενσωματωμένο τον Squid Proxy Server και προσφέρει ένα λιτό και εύκολο περιβάλλον διαχείρισης.
- **Απομακρυσμένα Προφίλ:** Μπορεί να αντικαταστήσει πλήρως το Active Directory και να προσφέρει στους χρήστες την δυνατότητα των απομακρυσμένων προφίλ (remote profiles). Πρόκειται για προφίλ που αποθηκεύονται στον server και επιστρέφουν στο χρήστη με κάθε είσοδό του. Πιο απλά οι χρήστες μπορούν να αλλάζουν υπολογιστές και να έχουν διαθέσιμα τα δεδομένα τους και τις ρυθμίσεις τους, μαζί με τυχόν περιορισμούς που τους έχουν επιβληθεί.

- **Διαμοιρασμός φακέλων και συσκευών:** Από μια τέτοια λύση δεν θα μπορούσε να λείπει και η απλή πλέον υπηρεσία του διαμοιρασμού αρχείων και φακέλων. Και εδώ το περιβάλλον διαχείρισης είναι ιδιαίτερα απλό και περιλαμβάνονται λειτουργίες για την εφαρμογή περιορισμών σε ομάδες, χρήστες ή φακέλους.
- **Αντίγραφα ασφαλείας:** Τα αρχεία και οι φάκελοι των χρηστών, όπως και οι ρυθμίσεις του συστήματος μπορούν να αντιγραφούν σε ασφαλείς τοποθεσίες (ή σε εξωτερικό μέσο αποθήκευσης) με πρωτόκολλα όπως FTP, RSYNC, SCP
- **Υπηρεσίες DHCP:** Με την υλοποίηση πολλών υποδικτύων, το modem/router που παρέχει την πρόσβαση στο Internet, δεν είναι δυνατόν να αποδώσει διευθύνσεις σε όλες τις συσκευές όλων των υποδικτύων. Το Zentyal παρέχει την υπηρεσία DHCP για κάθε υποδίκτυο με δυνατότητα καθορισμού του χρόνου απόδοσης και αν απαιτείται με δυνατότητα απόδοσης της ίδιας διεύθυνσης κάθε φορά στην ίδια συσκευή.
- **Υπηρεσίες DNS:** Η υπηρεσία DNS που παρέχεται απαιτείται από το Active Directory αλλά μπορεί να χρησιμοποιηθεί είτε για την ονοματολογία των συσκευών είτε για ανακατεύθυνση συγκεκριμένων σελίδων σε άλλες.
- **Captive Portal:** Το Captive Portal είναι ίσως η σημαντικότερη υπηρεσία για την χρήση ενός ασύρματου δικτύου και μάλιστα ενσωματώνεται με την κεντρική αυθεντικοποίηση των χρηστών. Ο κάθε χρήστης που θα συνδεθεί, για να αποκτήσει πρόσβαση σε κάποια σελίδα του Internet, θα πρέπει να πληκτρολογήσει το όνομα χρήστη και το συνθηματικό του.
- **Vpn:** Η υπηρεσία VPN που παρέχεται, επιτρέπει την ασφαλή απομακρυσμένη σύνδεση μέσω ξεχωριστού υποδικτύου
- **Voip:** Με την υπηρεσία VoIP είναι δυνατόν διάφορες συσκευές να επικοινωνήσουν μεταξύ τους τηλεφωνικά.
- **Anti virus:** Αντιϊκή προστασία στους κοινόχρηστους φακέλους
- **Υπηρεσία Διαμόρφωσης Ταχύτητας Πρόσβασης:** Υπηρεσία με την οποία δίνεται προτεραιότητα πρόσβασης σε συγκεκριμένες συσκευές ή υποδίκτυα.
- **Thin/Fat Clients:** Στις τελευταίες εκδόσεις, το Zentyal προσφέρει την δυνατότητα δημιουργίας και αποστολής Thin και Fat Clients.
- **Άλλες Υπηρεσίες:** Εκτός από τις προηγούμενες βασικές υπηρεσίες παρέχονται υπηρεσίες όπως αποστολή και λήψη εσωτερικών mail, κεντρικό ημερολόγιο, εξυπηρετητής ώρας, εξυπηρετητής ιστοσελίδων κ.α.

Για την υλοποίηση των προηγούμενων υπηρεσιών το Zentyal χρησιμοποιεί τα ακόλουθα λογισμικά ανοιχτού κώδικα:

- Postfix, Dovecot, Roundcube, Sieve, Fetchmail, Spamassassin, ClamAV, Postgrey, Amavisd-new
- OpenLDAP, Heimdal Kerberos, FREERadius
- OpenChange, Zarafa, ejabberd
- OpenVPN, OpenSWAN, PPTPd, xl2tpd
- ISC DHCP, BIND 9, NTPd, NUT
- OpenSSL, Netfilter, Iproute2, Suricata, L7-filter
- Squid, Dansguardian
- Samba4, CUPS

- Duplicity
- Apache, vsftpd

ΣΕΝΑΡΙΟ ΧΡΗΣΗΣ

Σε ένα πιθανό σενάριο χρήσης θα μπορούσαν να χρησιμοποιηθούν όλα τα υποδίκτυα. Σε αυτό το σενάριο θα υπάρχει το εξωτερικό υποδίκτυο, το υποδίκτυο των γραφείων, το υποδίκτυο των εργαστηρίων, τα υποδίκτυα των καθηγητών (ενσύρματο και ασύρματο) και το ασύρματο υποδίκτυο των μαθητών. Στο σενάριο αυτό, οι υπολογιστές έχουν δευτερεύουσα σημασία, αφού δεδομένα και διαπιστευτήρια αποθηκεύονται στον κεντρικό διακομιστή, στο οποίο εφαρμόζονται πολιτικές αντιγράφων ασφαλείας. Το σενάριο χρήσης περιγράφεται αφού έχουν αναφερθεί οι προσφερόμενες υπηρεσίες από το Zentyal έτσι ώστε να είναι εύκολος ο συνδυασμός των υπηρεσιών με τις απαιτήσεις.

ΔΙΑΣΥΝΔΕΣΗ ΥΠΟΔΙΚΤΥΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Καλό θα ήταν όλα τα εργαστήρια να βρίσκονται στο ίδιο υποδίκτυο. Σε περίπτωση ΣΕΚ ή γενικότερα εργαστηρίων διαφορετικών ειδικοτήτων θα μπορούσαν να δημιουργηθούν ομάδες εργαστηρίων όπου κάθε μία θα σχημάτιζε το δικό της υποδίκτυο. Έτσι οι μαθητές θα μπορούσαν να έχουν πρόσβαση στα δεδομένα τους (κεντρικά ή αυτά που 'άφησαν" σε κάποιο εργαστήριο) από οποιοδήποτε άλλο εργαστήριο της ειδικότητας.

Στο υποδίκτυο των γραφείων (της διεύθυνσης και της γραμματείας), δεν θα πρέπει να έχει κανείς άλλος πρόσβαση εκτός από τους υπολογιστές του υποδικτύου. Στο ασύρματο των καθηγητών θα πρέπει να έχουν πρόσβαση μόνον οι καθηγητές και το υποδίκτυο δεν θα πρέπει να έχει επικοινωνία με κανένα άλλο υποδίκτυο (εκτός ίσως των εργαστηρίων). Το ασύρματο υποδίκτυο των μαθητών θα πρέπει να επιτρέπει την πρόσβαση των μαθητών στο Internet μόνο όταν κάτι τέτοιο προβλέπεται και δεν θα πρέπει να επικοινωνεί με κανένα άλλο υποδίκτυο εκτός των εργαστηρίων. Το ενσύρματο υποδίκτυο των εκπαιδευτικών θα πρέπει να είναι προσπελάσιμο μόνο από συσκευές των εκπαιδευτικών. Οι παραπάνω πολιτικές είναι γενικές και θα μπορούσαν να προσαρμοστούν στις εκάστοτε ανάγκες.

Σε αυτή την ενότητα θα πρέπει να αναφερθεί και η τεχνολογία Thin Clients. Όπως έχει γραφεί σε πολλές εργασίες (Διεύθυνση εκπαιδευτικής τεχνολογίας, 2013), η τεχνολογία αυτή επιτρέπει την επαναχρησιμοποίηση παλιών μηχανημάτων για την δημιουργία νέων εργαστηρίων. Το μόνο πρόβλημα είναι το κόστος, αφού το μηχάνημα που θα παίξει το ρόλο του κεντρικού εξυπηρετητή θα πρέπει να είναι ιδιαίτερα ισχυρό. Για υλοποιήσεις Thin Client υπάρχει αρκετή εμπειρία και βιβλιογραφία, οπότε δεν χρειάζεται να αναφερθούμε περισσότερο.

ΧΡΗΣΤΕΣ

Στο πιθανό σενάριο ο κάθε χρήστης (εκπαιδευτικός ή μαθητής) θα έχει προσωπικό λογαριασμό (όνομα χρήστη και συνθηματικό) και θα ανήκει σε μία ή περισσότερες ομάδες. Τα διαπιστευτήριά του θα του επιτρέπουν ή θα του απαγορεύουν την πρόσβαση σε διάφορους πόρους του δικτύου. Τέτοιοι πόροι είναι οι διαμοιρασμένοι φάκελοι, τα αρχεία και οι εκτυπωτές, η πρόσβαση και η ταχύτητα πρόσβασης στο Internet, η πρόσβαση σε δικτυακούς προσωπικούς φακέλους, η σύνδεση σε κάποιον υπολογιστή κ.α.

Ειδικότερα οι εκπαιδευτικοί θα μπορούν να χρησιμοποιούν τους υπολογιστές των γραφείων των καθηγητών και θα έχουν πρόσβαση στους διαμοιρασμένους

φακέλους των καθηγητών, στους προσωπικούς τους φακέλους και στο προσωπικό τους προφίλ. Αυτοί οι αποθηκευτικοί χώροι βρίσκονται στον κεντρικό διακομιστή, οπότε όλοι οι χρήστες, ανεξάρτητα από το υποδίκτυο σύνδεσης, θα μπορούν να έχουν πρόσβαση (με τα κατάλληλα διαπιστευτήρια). Αυτό σημαίνει ότι ανεξάρτητα από το υποδίκτυο σύνδεσης, εκπαιδευτικοί και μαθητές θα μπορούν να προσπελάσουν τα αρχεία τους. Έτσι οι μαθητές θα μπορούν να συνδεθούν στο κάθε εργαστήριο και το προφίλ τους θα μεταφορτώνεται σε κάθε σύνδεση. Τα αρχεία τους και οι εργασίες τους, θα τους ακολουθούν σε κάθε υπολογιστή. Για να είναι εφικτό κάτι τέτοιο θα πρέπει να δημιουργηθούν και να εφαρμοστούν πολιτικές αντιγράφων ασφαλείας. Με την νέα τοπολογία οι καθηγητές θα μπορούν να χρησιμοποιήσουν το Internet μέσα σε οποιαδήποτε αίθουσα, για να παρουσιάσουν κάποια ιστοσελίδα όταν δεν είναι απαραίτητη η ταυτόχρονη περιήγηση των μαθητών, αφήνοντας έτσι το εργαστήριο ελεύθερο να χρησιμοποιηθεί από κάποιον άλλο εκπαιδευτικό, σε μάθημα που απαιτεί την ενεργή συμμετοχή των μαθητών στους υπολογιστές.

Τα γραφεία της διεύθυνσης και της γραμματείας, θα πρέπει να αντιμετωπιστούν με ιδιαίτερη προσοχή. Οι χρήστες εκεί δεν αλλάζουν συχνά και τα διαπιστευτήρια, εκ των πραγμάτων τα γνωρίζουν λίγοι. Όπως όμως κάθε άλλος χρήστης θα πρέπει να έχουν τους δικούς φακέλους στον διακομιστή για τους οποίους θα πρέπει να γίνει ιδιαίτερη μέριμνα όσον αφορά τα αντίγραφα ασφαλείας. Οπότε καλό θα ήταν να δημιουργηθούν μερικοί χρήστες με γενικά ονόματα, τα οποία θα γνωρίζουν κάθε χρόνο ελάχιστοι. Οι διαδικασίες θα εφαρμόζονται κάθε χρόνο σε αυτούς τους χρήστες, ασχέτως του πραγματικού προσώπου που χρησιμοποιεί το μηχάνημα.

ΥΠΗΡΕΣΙΕΣ

Για να υλοποιηθεί το πιθανό σενάριο, οι υποχρεωτικές υπηρεσίες είναι αρκετές. Αρχικά θα πρέπει να υπάρχει η υπηρεσία DHCP για την απόδοση διευθύνσεων IP. Αμέσως μετά θα πρέπει να υπάρχει κατάλληλη υπηρεσία τείχους προστασίας για τον έλεγχο πρόσβασης μεταξύ των υποδικτύων. Επίσης, θα πρέπει να υπάρχει κατάλληλη υπηρεσία, εφάμιλλη του Active Directory για τον κεντροποιημένο έλεγχο διαπιστευτηρίων, για τον διαμοιρασμό αρχείων και εκτυπωτών και για την υλοποίηση των απομακρυσμένων προφίλ. Και επειδή μία από τις απαιτήσεις του Active Directory είναι και η υπηρεσία της ονοματολογίας τομέων, η υπηρεσία DNS κρίνεται απαραίτητη. Δεν θα πρέπει να λείπει η υπηρεσία του proxy server αφού αποτελεί σημαντικό παράγοντα για την σωστή χρήση της εξωτερικής γραμμής (πρόσβαση στο Internet) όπως επίσης, δεν θα πρέπει να λείπει η υπηρεσία ελέγχου εύρους ζώνης και ταχύτητας που θα εφαρμόζεται σε κάθε υποδίκτυο και σε κάθε μηχάνημα. Σημαντική είναι και η υπηρεσία αντιμετώπισης ιών στους διαμοιρασμένους φακέλους.

Επίσης αντίστοιχης σημασίας είναι και η υπηρεσία ασφαλούς απομακρυσμένης πρόσβασης από τους τεχνικούς του σχολικού δικτύου (Γεωργόπουλος & Σιάχος, 2009). Αν και παλαιότερα, ο κάθε διακομιστής είχε συγκεκριμένη διεύθυνση που επέτρεπε την πρόσβαση σε τεχνικούς καθ' όλη την διάρκεια του έτους, τα τελευταία χρόνια η απαίτηση αυτή σχεδόν παραλείπεται πάντα. Όσον αφορά την διαχείριση του δικτύου, δεν πρέπει να παραβλεφθεί η υπηρεσία παρακολούθησης (monitoring) του δικτύου και των άλλων υπηρεσιών.

Τέλος θα ήταν ιδιαίτερα χρήσιμη μια υλοποίηση κατά την οποία δημοφιλείς υπηρεσίες του Internet θα ήταν διαθέσιμες προς πειραματισμό από τους μαθητές. Τέτοιες υπηρεσίες είναι η δημοσίευση ιστοσελίδων, η μεταφορά αρχείων (FTP), η γραμμή εντολών, η δικτυακή τηλεφωνία (VoIP), αποστολή και λήψη email, instant

messaging και άλλες οι οποίες ουσιαστικά αποτελούν εκπαιδευτικά αντικείμενα σε ΕΠΑΛ και ΙΕΚ.

ΑΠΟΤΕΛΕΣΜΑΤΑ ΧΡΗΣΗΣ

Το Zentyal έχει χρησιμοποιηθεί αρκετά σε σχολεία του εξωτερικού και ελάχιστα στη χώρα μας (2ο Ε.Κ. Ανατολικής Αττικής). Εμείς το χρησιμοποιήσαμε σε δύο σχολεία του νομού Γρεβενών ως κεντρικό διακομιστή για χρήση στο εργαστήριο και ως κεντρικό διακομιστή του σχολείου. Τα σχολεία είναι μικρά, εβδομήντα μαθητές στο ένα σχολείο και περίπου διακόσιοι μαθητές στο άλλο, όποτε και τα υποδίκτυα είναι λίγα, το εξωτερικό, του εργαστηρίου, των γραφείων και ένα ή δύο ασύρματα. Με την χρήση του Zentyal καταφέραμε να απομονώσουμε τα υποδίκτυα και να επιτύχουμε τους αρχικούς στόχους.

Η εγκατάσταση του είναι ιδιαίτερα εύκολη, αφού μετά την εισαγωγή του DVD εγκατάστασης και τις απαντήσεις σε μερικές απλές ερωτήσεις, το τελικό αποτέλεσμα είναι σχεδόν το επιθυμητό. Οι παραμετροποιήσεις στους Windows clients είναι ιδιαίτερα εύκολες και για τους GNU/Linux Clients τυπικές (απαιτούνται μερικές αλλαγές σε κάποια αρχεία ρυθμίσεων). Οι απαιτήσεις σε υλικό είναι μικρές και για μικρά σχολεία σχεδόν μηδαμινές. Το γραφικό περιβάλλον διαχείρισης είναι ιδιαίτερα καλαίσθητο, σύγχρονο και εύκολο στην κατανόησή του και την χρήση του.

Ένα μεγάλο πλεονέκτημα του Zentyal είναι η ενοποίηση πολλών λειτουργιών σε ένα λογισμικό, με ενιαίο γραφικό τρόπο διαχείρισης και κεντρικούς μηχανισμούς αυθεντικοποίησης. Ίσως όμως, το πιο ενδιαφέρον χαρακτηριστικό του λογισμικού είναι η ταυτόχρονη χρήση υπολογιστών με εγκατεστημένα λειτουργικά σύστημα Windows και GNU/Linux. Με την ενσωμάτωση του Samba 4, ο εξυπηρετητής μπορεί να λειτουργήσει ως Primary Domain Controller για τους υπολογιστές που έχουν εγκατεστημένα Windows και ως διακομιστής αρχείων και εξυπηρετητής αυθεντικοποίησης για εκείνους που χρησιμοποιούν GNU/Linux. Μάλιστα με την εγκατάσταση του NFS (που δυστυχώς δεν έχει ενσωματωθεί ακόμη), τα απομακρυσμένα προφίλ θα μπορούν να είναι διαθέσιμα και στους χρήστες που συνδέονται από υπολογιστές GNU/Linux.

Όσον αφορά την ασφάλεια, ο διαχωρισμός σε υποδίκτυα μας επέτρεψε να απαγορεύσουμε την πρόσβαση κάθε ασύρματης συσκευής στα γραφεία. Ακόμη και στη περίπτωση που κάποιος εξωτερικός παράγοντας αποκτήσει πρόσβαση στο ασύρματο δίκτυο, δεν θα μπορεί να προσπελάσει υπολογιστές των γραφείων, ούτε να αποκτήσει πρόσβαση το Internet, αφού απαιτούνται επιπλέον διαπιστευτήρια για την επικοινωνία με εξωτερικούς χώρους. Επίσης, με κατάλληλους κανόνες περιορίσαμε σημαντικά την πρόσβαση κάθε άλλης συσκευής στους υπολογιστές όπου είναι αποθηκευμένα τα προσωπικά στοιχεία των μαθητών. Σε κάθε σχολείο, τα γραφεία έχουν προτεραιότητα στην χρήση της εξωτερικής γραμμής λόγω των υπηρεσιών που άρχισαν να χρησιμοποιούνται έντονα φέτος. Τα αντίγραφα ασφαλείας λαμβάνονται καθημερινά και αποθηκεύονται σε εξωτερικές μονάδες. Μαθητές και καθηγητές έχουν πρόσβαση στα δεδομένα τους στον διακομιστή από οποιοδήποτε δίκτυο με την χρήση των διαπιστευτηρίων τους.

Σε γενικές γραμμές, με την χρήση του Zentyal, καταφέραμε να εξαλείψουμε ή να περιορίσουμε αρκετά από τα προβλήματα που αναφέρθηκαν στην αρχή της εργασίας. Το ενδιαφέρον ήταν ότι το κάναμε εύκολα και με μεγάλη υποστήριξη από

τους διευθυντές των σχολείων. Το κόστος και στις δύο περιπτώσεις ήταν ιδιαίτερα μικρό και η ανταπόκριση από εκπαιδευτικούς και μαθητές αρκετά μεγάλη.

ΑΝΑΦΟΡΕΣ

2ο Ε.Κ. Ανατολικής Αττικής. ΕΛΛΑΚ στο 2ο Σχολικό Εργαστηριακό Κέντρο (ΣΕΚ) Αν. Αττικής (Κορωπίου). Ανακτήθηκε στις 20 Ιανουαρίου 2014 από τη διεύθυνση <http://2sek-anatol.att.sch.gr/index.php/2011-03-22-22-06-25/18-2011-06-29-08-11-41>.

Γεωργόπουλος & Σιάχος (2009). Υποέργο 17: «Υποστήριξη Συστημάτων Τεχνικής Στήριξης Σχολικών Εργαστηρίων», Απομακρυσμένη Διαχείριση ΣΕΠΕΗΥ. Τομέας Εκπαιδευτικής Τεχνολογίας, Ε.Α.Ι.Τ.Υ..

Διεύθυνση εκπαιδευτικής τεχνολογίας (2013). Ελεύθερο Λογισμικό/ Λογισμικό Ανοιχτού Κώδικα σε σχολικά εργαστήρια: οδηγός εγκατάστασης & χρήσης *Ubuntu 12.04, LTSP, sch-scripts, erorptes*. Ινστιτούτο τεχνολογίας υπολογιστών και εκδόσεων "Διόφαντος".

Σιάχος (2009). Υποέργο 17: «Υποστήριξη Συστημάτων Τεχνικής Στήριξης Σχολικών Εργαστηρίων», Οδηγίες εγκατάστασης και ρύθμισης διακομιστή μεσολάβησης *Squid*. Τομέας Εκπαιδευτικής Τεχνολογίας, Ε.Α.Ι.Τ.Υ..

Υπηρεσία τεχνικής υποστήριξης πανελλήνιου σχολικού δικτύου (2010). Προώθηση ΕΛ/ΛΑΚ στα Σχολικά Εργαστήρια Πληροφορικής. Ανακτήθηκε στις 15 Ιανουαρίου 2014 από τη διεύθυνση <http://ts.sch.gr/ellak>.

Υπουργείο Εθνικής Παιδείας & Θρησκευμάτων (2004). Περιοδικές εργασίες Τεχνικής Στήριξης στα πληροφοριακά συστήματα των σχολείων. Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών, Τομέας Εκπαιδευτικής Τεχνολογίας.

Marta Cambroner (2013). *How to easily deploy and manage an IT network in a secondary school with Zentyal*. Ανακτήθηκε στις 20 Ιανουαρίου 2014 από τη διεύθυνση <http://blogs.zentyal.org/gueststars/2013/06/05/how-to-easily-deploy-and-manage-an-it-network-in-a-secondary-school-with-zentyal/>.

Zentyal authors (2012). *Aalborg Studenterkursus uses Zentyal as an Office Server, Gateway & Infrastructure Manager*. Ανακτήθηκε στις 20 Ιανουαρίου 2014 από τη διεύθυνση http://www.zentyal.com/wp-content/uploads/2012/08/Aalborg_Zentyal_Use_Case_EN.pdf.

Zentyal authors (2012). *In Aragon, 80 Zentyal servers are deployed within the framework of School 2.0 Program*. Ανακτήθηκε στις 20 Ιανουαρίου 2014 από τη διεύθυνση http://www.zentyal.com/wp-content/uploads/2012/08/School_2_0_Zentyal_Use_Case_EN.pdf.

Zentyal official documentation (2014). *Zentyal 3.3 Official Documentation*. Ανακτήθηκε στις 15 Ιανουαρίου 2014 από τη διεύθυνση <http://doc.zentyal.org/en/>.

Sukhija, S. & Gupta S., (2012). *Wireless Network Security Protocols A Comparative Study*, Volume 2, Issue 1.

Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A., Shrawne, S., (2012). *Vulnerabilities of Wireless Security protocols (WEP and WPA2)*, Volume 1, Issue 2.