

Κανονισμός λειτουργίας ασύρματων τοπικών δικτύων Wireless Local Area Networks (WLANs) στους χώρους του Τ.Ε.Ι. Σερρών¹

1. ΕΙΣΑΓΩΓΗ

Τα ασύρματα δίκτυα προσφέρουν τη δυνατότητα σύνδεσης στο Internet (συνήθως φορητών) υπολογιστών και συσκευών χωρίς τη χρήση καλωδίου δικτύου. Απαραίτητες προϋποθέσεις είναι να διαθέτει ο υπολογιστής κάρτα ασύρματης δικτύωσης και να βρίσκεται εντός της εμβέλειας ενός από τα σημεία πρόσβασης (Access Points) του δικτύου. Καθώς όμως το μέσο μετάδοσης δεν είναι χωροταξικά ελεγχόμενο, προκύπτουν θέματα στη χρήση ασύρματων υπηρεσιών που δεν υφίστανται στις ενσύρματες εκδοχές τους.

Το παρόν κείμενο εξειδικεύει το κανονιστικό πλαίσιο και τις προδιαγραφές που πρέπει να τηρούν οι μονάδες του ΤΕΙ Σερρών σε ό,τι αφορά στη δημιουργία και χρήση ασύρματων τοπικών δικτύων (Wireless Local Area Networks – WLAN) εντός του ιδρύματος. Τα WLANs αυτά στο πλαίσιο του παρόντος κειμένου διακρίνονται σε δύο κατηγορίες:

1. «WLAN υποδομής» (infrastructure) που λειτουργεί ως δίκτυο πρόσβασης εντός του ΤΕΙ για κοινόχρηστες υπηρεσίες, εντός του βεληνεκούς του οποίου παρέχεται επίσημα δικτυακή πρόσβαση σε τερματικά (laptops, PDAs, κλπ.) διερχόμενων εγγεγραμμένων χρηστών.

2. WLAN για προσωπική χρήση» (π.χ. ασύρματη διασύνδεση καταχωρημένου Η/Υ χρήστη με laptops, PDA, κινητό τηλέφωνο, κλπ). Η λειτουργία τέτοιων δικτύων πρέπει να αποφεύγεται και η έγκριση εγκατάστασής τους θα πρέπει να γίνεται μόνο μετά από απόφαση του Συμβουλίου του ΤΕΙ έπειτα από εισήγηση της Επιτροπής Κέντρου Υποστήριξης Τεχνολογιών Επικοινωνιών και Πληροφορικής (ΕΚΥΤΕΠ) του ΤΕΙΣ. Σε κάθε περίπτωση ένα τέτοιο δίκτυο δεν θα πρέπει να παρέχει πρόσβαση σε περισσότερους από τέσσερις (4) χρήστες, τα ονόματα των οποίων θα δηλώνονται εκ των προτέρων στο ΚΛΔ.

¹ Αριθμ. Απόφασης 423/27/3-9-2009 του Συμβουλίου του Τ.Ε.Ι. Σερρών

2. ΑΡΧΕΣ

Ο Κανονισμός Λειτουργίας Δικτύου του ΤΕΙΣ (ο υφιστάμενος ή κάθε μελλοντικός) εφαρμόζεται και για τα ασύρματα τοπικά δίκτυα, τα οποία θεωρούνται τμήμα το Δικτύου Δεδομένων του ΤΕΙ. Επιπλέον, το παρόν κανονιστικό πλαίσιο βασίζεται σε τρεις αρχές ευρείας αποδοχής. Οι ασύρματες υπηρεσίες του ΤΕΙΣ θα πρέπει να έχουν κατάλληλες προδιαγραφές ώστε να επιτυγχάνεται:

1. προστασία των χρηστών της υπηρεσίας από υποκλοπή των στοιχείων πιστοποίησής τους (username, password) ή των δεδομένων της επικοινωνίας τους.
2. προστασία του δικτύου δεδομένων του ΤΕΙΣ και του Internet από μη εξουσιοδοτημένη χρήση, σύμφωνα με α) τον Κανονισμό Λειτουργίας Δικτύου και β) τις υποχρεώσεις του ΤΕΙΣ έναντι τρίτων, π.χ. Κανονισμός Χρήσης Εθνικού Δικτύου Έρευνας και Τεχνολογίας (ΕΔΕΤ).
3. πιστοποιημένη παροχή ασύρματης δικτυακής πρόσβασης σε όσο το δυνατόν περισσότερα μέλη της ακαδημαϊκής κοινότητας.

Η ευθύνη λειτουργίας των «Ασύρματων WLAN για προσωπική χρήση» βαρύνει τους τελικούς χρήστες που τα εγκαθιστούν για προσωπική τους εξυπηρέτηση. Είναι ευθύνη των ίδιων των χρηστών προσωπικών WLANs να προστατεύονται από υποκλοπές, ενώ οι ίδιοι είναι υπόλογοι να εξασφαλίσουν την προστασία του δικτύου δεδομένων και του Διαδικτύου από κακή χρήση του προσωπικού WLAN.

Απαγορεύεται η παροχή ασύρματης πρόσβασης σε πάνω από τέσσερα (4) διαφορετικά μέλη του ΤΕΙ Σερρών μέσω προσωπικού WLAN. Σε αυτή την περίπτωση απαιτείται να ακολουθούνται οι προβλεπόμενες διαδικασίες για δημιουργία ασύρματης υποδομής.

Η ευθύνη λειτουργίας «Ασύρματων WLANs υποδομής» βαρύνει τους επίσημους διαχειριστές των υποδομών αυτών και υπόκειται σε κανόνες που καθορίζουν μεταξύ άλλων το ελάχιστο αποδεκτό επίπεδο παρεχόμενης προστασίας όπως προδιαγράφεται στις επόμενες ενότητες.

Η ευθύνη χρήσης κάθε δικτύου βαρύνει αποκλειστικά τον χρήστη.

3. ΠΛΑΙΣΙΟ ΠΑΡΟΧΗΣ

3.1 Ασφάλεια

Σε ένα μέρος ενδέχεται να είναι διαθέσιμα πολλά ασύρματα δίκτυα (νησίδες), οπότε ο χρήστης καλείται να διαλέξει σε ποιο θα συνδεθεί. Τα δεδομένα του χρήστη διακινούνται με ασφάλεια, μόνον εφόσον αυτός συνδεθεί σε επίσημα αναγνωρισμένη- πιστοποιημένη από το ΚΛΔ υποδομή ασύρματης πρόσβασης στο δίκτυο του ΤΕΙΣ. Άρα, ο χρήστης θα πρέπει να μπορεί με εύκολο τρόπο να επιβεβαιώσει εάν πρόκειται να συνδεθεί σε αυθεντική ασύρματη υποδομή του ΤΕΙΣ, και όχι σε ασύρματο εξοπλισμό κάποιου πιθανώς κακόβουλου διαχειριστή (rogue wireless access points) ο οποίος, μεταξύ άλλων, θα μπορούσε να υποκλέψει ή να παραποιήσει τη δικτυακή κίνηση του υπολογιστή του χρήστη.

Η ανάγκη για προστασία του δικτύου δεδομένων του ΤΕΣΙ από μη εξουσιοδοτημένη χρήση επιβάλλει την πιστοποίηση της ταυτότητας του χρήστη από την υποδομή ασύρματης πρόσβασης. Συνεπώς, **απαγορεύεται** η διάθεση «ανοιχτών» δικτύων (στα οποία συνδέεται οποιοσδήποτε χωρίς κανέναν έλεγχο), ή δικτύων με ανεπαρκή μηχανισμό πιστοποίησης (κοινόχρηστο κωδικό πρόσβασης pass-phrase).

Τέλος, η χρήση ισχυρής κρυπτογράφησης από την υποδομή, στα τρέχοντα διεθνώς αποδεκτά επίπεδα, διαβεβαιώνει τον κάθε χρήστη ότι πιθανότατα τα δεδομένα του που μεταδίδονται στο ασύρματο μέσο δεν μπορούν να τύχουν υποκλοπής.

3.2 Δικαιούχοι

Η πρόσβαση στο ασύρματο δίκτυο (νησίδα) θα πρέπει να παρέχεται μόνο:

1. σε μέλη της Ακαδημαϊκής κοινότητας (μέλη ΕΠ, προσωπικό, σπουδαστές, κλπ).
2. σε μέλη ακαδημαϊκών ιδρυμάτων που επισκέπτονται το ΤΕΙΣ τα οποία συμμετέχουν στη διεθνή υποδομή πρόσβασης EduRoam (<http://www.eduroam.org/>), όταν συμβληθεί το ΤΕΙ Σερρών μέσω του ΕΔΕΤ.

Η ακαδημαϊκή φύση και οι γενικές αρχές που διέπουν το Δίκτυο Δεδομένων του ΤΕΙΣ, επιτάσσουν κάθε ασύρματη υποδομή να είναι προσβάσιμη από οποιαδήποτε

μέλος του ΤΕΙΣ ή ιδρύματος EduRoam βρεθεί μέσα στο βεληνεκές της. Απαραίτητη προϋπόθεση για να συνδεθεί κάποιος δικαιούχος σε ασύρματο δίκτυο του ΤΕΙΣ είναι να μπορεί να ταυτοποιηθεί και να εξουσιοδοτηθεί η πρόσβασή του μέσω της κεντρικής υποδομής Radius/TACACS του Τ.Ε.Ι.Σ. που διαχειρίζεται το ΚΛΔ. Τέτοιοι είναι τελικοί χρήστες που:

- ή διαθέτουν λογαριασμό χρήστη στο ΚΛΔ,
- ή διαθέτουν λογαριασμό σε ίδρυμα που μπορεί να πιστοποιείται μέσω της διεθνούς υποδομής EduRoam
- διαθέτουν λογαριασμό σε τμήμα που συμμετέχει στην κεντρική υπηρεσία Radius.

Ειδικά για τους σπουδαστές του Ιδρύματος, λόγω του πλήθους τους, τίθεται περιορισμός χρόνου πρόσβασης στις δύο (2) ώρες ανά ημέρα (24ωρο) ώστε το δίκτυο να μπορεί να εξυπηρετήσει όλους τους ενδιαφερόμενους χρήστες.

Επισκέπτες που συμμετέχουν σε ημερίδες, συνέδρια κλπ μπορούν να έχουν προσωρινή πρόσβαση (“guest access”) στη διάρκεια της εκδήλωσης, κατόπιν συνεννόησης με το ΚΛΔ για ειδικά στοιχεία προσωρινής πρόσβασης.

Σε κάθε περίπτωση, η χρήση του δικτύου πρέπει να γίνεται για ακαδημαϊκές και ερευνητικές δραστηριότητες και μόνον. Απαγορεύεται ρητά η οποιασδήποτε μορφής έξω-ακαδημαϊκή και εμπορική δραστηριότητα (με ή χωρίς αμοιβή). Για κάθε παραβίαση των όρων χρήσης του δικτύου υπεύθυνος είναι ο χρήστης που παραβαίνει τον κανονισμό. Για λόγους απόδοσης ευθυνών κατά την πρόσβαση στο ασύρματο δίκτυο του Ιδρύματος καταγράφονται στοιχεία όπως το κωδικό όνομα (username) του χρήστη, η ημερομηνία, η ώρα πρόσβασης και η διάρκεια της σύνδεσης καθώς η IP διεύθυνση με την οποία έγινε η πρόσβαση. Τα στοιχεία αυτά τηρούνται σε ασφαλή βάση δεδομένων στην οποία πρόσβαση έχει μόνο εξουσιοδοτημένο προσωπικό του ΚΛΔ.

Η χρήση του ασύρματου δικτύου του ΤΕΙ Σερρών προϋποθέτει την αυτόματη και ανεπιφύλακτη αποδοχή των όρων τόσο του παρόντος κανονισμού όσο και του Κανονισμού Λειτουργίας του Δικτύου Δεδομένων του ΤΕΙ Σερρών.

3.3 Γεωγραφική Κάλυψη

Η κάλυψη των ασύρματων τοπικών δικτύων πρέπει να περιορίζεται γεωγραφικά αποκλειστικά εντός των χώρων του ΤΕΙ Σερρών. Πιο συγκεκριμένα θα πρέπει η περιοχή που καλύπτει το access point να περιορίζεται στον χώρο τον οποίο έχει σχεδιαστεί να καλύπτει (π.χ. μέσα σε ένα αμφιθέατρο). Για το λόγο αυτό θα πρέπει να γίνεται προσεκτική μελέτη και επιλογή στο σημείο τοποθέτησης του κάθε σημείου πρόσβασης (Access Point) καθώς και της αντίστοιχης ισχύος εκπομπής. Προσωπικά ασύρματα δίκτυα θα πρέπει να καλύπτουν ένα σχετικά μικρό ενιαίο χώρο (γραφείο, εργαστήριο).

4. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

4.1 Συχνότητες

Η πρόσβαση των χρηστών στο ασύρματο δίκτυο του ΤΕΙΣ γίνεται στην περιοχή 2,4 GHz, όπου δεν απαιτείται Εκχώρηση Ραδιοσυχνότητας για την λειτουργία Σταθμών Ραδιοεπικοινωνιών, οι οποίοι πληρούν τις προϋποθέσεις (απόφαση ΕΕΤΤ 254/72, ΦΕΚ 895/Β/1672002/άρθρο 5) να εκπέμπουν και λαμβάνουν στην περιοχή ραδιοσυχνοτήτων 2.400 - 2.483,5 MHz (ISM band), να χρησιμοποιούν τεχνολογία διασποράς φάσματος (Spread Spectrum) και να είναι πλήρως συμβατοί με το εναρμονισμένο πρότυπο EN 300 328 του ETSI (<http://www.etsi.org>).

Επίσης, σύμφωνα με την ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων - <http://www.eett.gr>) για τις συσκευές μικρής εμβέλειας χρησιμοποιούμενες για τοπικά ραδιοδίκτυα οι οποίες λειτουργούν στην ζώνη ραδιοσυχνοτήτων 2.400 – 2.483,5 MHz (απαίτηση διεπαφής ραδιοεξοπλισμού 201), την απόφαση της Ευρωπαϊκής Επιτροπής Ραδιοεπικοινωνιών ERC/DEC(01)07 και τη σύσταση της Ευρωπαϊκής Επιτροπής Ραδιοεπικοινωνιών ERC/REC 70-03, **ορίζεται** σαν μέγιστο όριο ισχύς εκπομπής τα 100 mW e.i.r.p. (μέση ισοδύναμη ιστροπικά ακτινοβολούμενη ισχύς). Στη φασματική διεύρυνση με αναπήδηση συχνότητας η μέγιστη πυκνότητα ισχύος φάσματος περιορίζεται σε -10 dBW/100 kHz, ενώ σε άλλες μορφές φασματικής διεύρυνσης συμπεριλαμβανόμενης αυτής της άμεσης ακολουθίας, η μέγιστη πυκνότητα ισχύος φάσματος περιορίζεται σε -20 dBW / 1 MHz.

4.2 Εξοπλισμός

Με το Προεδρικό Διάταγμα 44/2002 (ΦΕΚ 44/Α/7-3-2002) «Ραδιοεξοπλισμός και τηλεπικοινωνιακός τερματικός εξοπλισμός και αμοιβαία αναγνώριση της συμμόρφωσης των εξοπλισμών αυτών. Προσαρμογή της ελληνικής νομοθεσίας στην οδηγία 99/5/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 9 Μαρτίου 1999», ρυθμίζεται η διάθεση στην αγορά και χρήση του τηλεπικοινωνιακού εξοπλισμού. Οι ουσιώδεις απαιτήσεις ως προς τις οποίες θα πρέπει σύμφωνα με το παραπάνω Π.Δ. να συμμορφώνεται κάθε προϊόν τηλεπικοινωνιακού εξοπλισμού αφορούν (άρθρο 3 του Π.Δ.) α) στην προστασία της υγείας και ασφάλειας του χρήστη

ή τρίτου, συμπεριλαμβανομένων των απαιτήσεων ασφαλείας σύμφωνα με την ΚΥΑ 470/1985 όπως τροποποιήθηκε από την ΚΥΑ Β 6467/608/88 που εναρμονίζουν στην ελληνική νομοθεσία την οδηγία 73/23/ΕΟΚ, εξαιρουμένης της επιβολής κατώτατου ορίου τάσης, β) στην προστασία για την ηλεκτρομαγνητική συμβατότητα, σύμφωνα με την ΚΥΑ 94649/8682/93 που μεταφέρει στην ελληνική νομοθεσία την οδηγία 89/336/ΕΟΚ όπως τροποποιήθηκε με τις οδηγίες 92/31/ΕΟΚ και 93/68/ΕΟΚ, και γ) στον ραδιοεξοπλισμό, για τον οποίο ισχύει ότι θα πρέπει να κατασκευάζεται έτσι ώστε να χρησιμοποιείται αποτελεσματικά το φάσμα που έχει παραχωρηθεί σε επίγειες ή δορυφορικές ραδιοεπικοινωνίες και τους τροχιακούς πόρους και να αποφεύγονται οι επιβλαβείς παρεμβολές.

Τις παραπάνω προδιαγραφές εκτός από τον εξοπλισμό υποδομής πρέπει να καλύπτουν και οι συσκευές των χρηστών.

4.3 Λειτουργικές απαιτήσεις

Σύμφωνα με τις παραπάνω αρχές του κανονισμού, κρίνεται απαραίτητο πέρα από την κάλυψη των προδιαγραφών του εξοπλισμού, να τηρούνται και οι εξής όροι λειτουργίας από τους διαχειριστές της ασύρματης υποδομής νησίδων:

Εάν το WLAN προσφέρει πρόσβαση με οποιοδήποτε τρόπο στο Δίκτυο Δεδομένων ΤΕΙΣ, θα πρέπει:

- Να υποστηρίζει πιστοποίηση χρηστών προτού δοθεί πρόσβαση στο LAN με χρήση πρωτοκόλλου IEEE 802.1x και επικοινωνία με επίσημο εξυπηρετητή Radius μονάδος του ΤΕΙΣ για πιστοποίηση των χρηστών. Ο εν λόγω radius server υποχρεωτικά θα πρέπει να εντάσσεται στην ιεραρχία του ΤΕΙΣ και να λειτουργεί ως μεταγωγός (relaying proxy). Η δυνατότητα του τελικού χρήστη να επιβεβαιώσει ότι η πρόσβασή του γίνεται σε εξουσιοδοτημένο-αναγνωρισμένο από το ΤΕΙΣ εξοπλισμό μπορεί να γίνεται με χρήση ψηφιακού πιστοποιητικού εξυπηρετητή υπογεγραμμένο από την Αρχή Πιστοποίησης ΤΕΙΣ και τοποθετημένο στον Radius εξυπηρετητή. Η χρήση του πιστοποιητικού επιβάλλει την υποστήριξη των πρωτοκόλλων EAP/TLS ή EAP/TTLS.

- Να επιβάλλεται κρυπτογράφηση στο κανάλι επικοινωνίας μεταξύ του Wireless Access Point και του Radius server, με τεχνικές tunneling (IPSec VPN, ελεγχόμενου VLAN ή αντιστοίχου μηχανισμού) και αντίστοιχα μεταξύ του Radius server και κάποιου πιθανώς εξωτερικού μηχανισμού ταυτοποίησης (LDAP ή MySQL server).
- Να επιβάλλεται κρυπτογράφηση στο κανάλι επικοινωνίας μεταξύ του Wireless Access Point και του υπολογιστή του χρήστη. Προτείνεται το WPA σύμφωνα με το IEEE 802.11i.
- Να τηρείται από τους διαχειριστές της υπηρεσίας αρχείο καταγραφής πρόσβασης (accounting logs) από όπου θα προκύπτει η ταυτότητα του χρήστη και ο ακριβής χρόνος σύνδεσής του. Η διάρκεια και οι συνθήκες φύλαξης και εξουσιοδοτημένης πρόσβασης των στοιχείων του αρχείου πρέπει να είναι σύμφωνα με την ισχύουσα νομοθεσία.
- Να υποστηρίζεται συνεργασία του 802.1x authentication με την διεθνή υποδομή EduRoam για υπηρεσίες προς επισκέπτες στο ΤΕΙΣ.

Σημειώνεται ότι, δεν είναι επιθυμητή η χρήση κρυπτογράφησης με το πρωτόκολλο WEP του προτύπου IEEE 802.11, καθώς το WEP πλέον θεωρείται πεπαλαιωμένο και ανασφαλές.

5. ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΚΑΙΡΟΠΟΙΗΣΗΣ ΤΟΥ ΠΑΡΟΝΤΟΣ ΚΑΝΟΝΙΣΜΟΥ

Ο κανονισμός λειτουργίας ασύρματων τοπικών δικτύων του ΤΕΙΣ μπορεί να επικαιροποιηθεί εφόσον υπάρξει ανάγκη που προκύπτει είτε από αλλαγή τεχνολογίας, είτε από προσθήκη νέων υπηρεσιών, είτε από αλλαγή πολιτικής στη χρήση του δικτύου.

Η επικαιροποίηση του κανονισμού γίνεται με απόφαση του Συμβουλίου του ΤΕΙΣ έπειτα από σχετική εισήγηση του ΚΥΤΕΠ του ΤΕΙ Σερρών.

ΓΛΩΣΣΑΡΙΟ ΟΡΩΝ

- Access Point: Σημείο πρόσβασης ασύρματης δικτύωσης
- WLAN: Wireless Local Area Network – Ασύρματο τοπικό δίκτυο
- AAI: Authentication Authorization Infrastructure – Υποδομή αυθεντικοποίησης εξουσιοδότησης
- e.i.r.p. – Equivalent isotropically radiated power: Μέση ισοδύναμη ισοτροπικά ακτινοβολούμενη ισχύς
- ETSI: European Telecommunications Standards Institute
- IEEE: Institute of Electrical and Electronics Engineers
- WEP: Wired Equivalent Privacy
- WAP2: Wi-Fi Protected Access
- EAP: Extensible Authentication Protocol
- TLS: Transport Layer Security
- TTLS: Tunneled Transport Layer Security
- PEAP: Protected Extensible Authentication Protocol
- EduRoam: Διεθνής συνεργασία πιστοποίησης χρηστών Ακαδημαϊκών - Ερευνητικών ιδρυμάτων. <http://www.eduroam.org>.