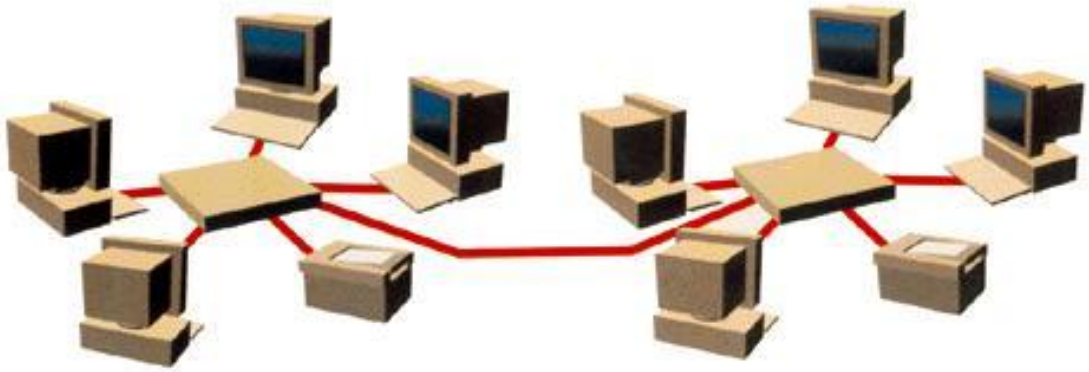
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ

ΤΕΙ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΡΟΕΤΟΙΜΑΣΙΑ ΓΙΑ ΤΗΝ ΑΠΟΚΤΗΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΔΙΑΧΕΙΡΙΣΤΗ ΔΙΚΤΥΩΝ CCNA ΑΝΑΠΤΥΞΗ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΕΝΟΣ VLAN



ΣΠΟΥΔΑΣΤΗΣ: ΠΑΤΣΕΑΣ ΕΥΑΓΓΕΛΟΣ
Εξάμηνο: 16ο, ΑΜ : 8525, Email: patseasv2@gmail.com

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ : ΛΙΑΡΟΚΑΠΗΣ ΔΗΜΗΤΡΙΟΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ 2

ΕΙΣΑΓΩΓΗ 4

ΚΕΦΑΛΑΙΟ 1: ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΥΠΟΛΟΓΙΣΤΩΝ 7

1.1 Οι πιστοποιησεις Πληροφορικης σημερα 7

1.2 Το CCNA 9

1.3 Αναγκη στην αγορα για πιστοποιημενη γνωση δικτυων 10

ΚΕΦΑΛΑΙΟ 2: ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΔΙΚΤΥΩΝ 13

2.1 Δικτυων Υπολογιστων 13

2.2 Ειδη δικτυων 14

2.3 Το πρωτοκολλο OSI 15

2.3.1 ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΠΙΠΕΔΟΥ OSI.....18

2.4 Δικτυακες συσκευες 20

2.4 ΤΟ TCP/IP Μοντελο 26

2.5 Διευθυνσεις IP και υποδικτυωση 27

2.6 Διευθυνσεις IPv6 32

ΚΕΦΑΛΑΙΟ 3: ΔΡΟΜΟΛΟΓΗΣΗ 34

3.1 Τι ειναι δρομολογηση 34

3.2 Στατικη Δρομολογηση 35

3.3 Δυναμικη Δρομολογηση 35

3.4 LINK STATE ΑΛΓΟΡΙΘΜΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ 35

3.5 DISTANCE-VECTOR ΑΛΓΟΡΙΘΜΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ 37

3.6 ΒΑΣΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ..... 37

3.7 ΠΙΝΑΚΕΣ ΔΡΟΜΟΛΟΓΗΣΗΣ 39

3.8 ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ RIP 40

3.9 ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ EIGRP..... 41

3.10 ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ OSPF 44

3.10.1 ΤΥΠΟΙ ΔΡΟΜΟΛΟΓΗΤΩΝ ΤΟΥ OSPF.....**46**

3.11 ACCESS LISTS 49

***ΚΕΦΑΛΑΙΟ 4: ΜΕΤΑΓΩΓΕΙΣ (SWITCHES) ΚΑΙ VLAN* . 51**

4.1 ΜΕΤΑΓΩΓΕΙΣ - SWITCHES 51

4.2 ΔΗΜΙΟΥΡΓΙΑ - ΡΥΘΜΙΣΕΙΣ VLAN..... 53

4.3 ΤΟ VTP..... 56

4.4 ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ..... 56

4.4.1 ΠΡΟΤΥΠΑ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ.....57

***ΚΕΦΑΛΑΙΟ5: ΣΧΕΔΙΑΣΗ ΣΕΝΑΡΙΩΝ ΔΙΚΤΩΝ*..... 65**

5.1 ΔΗΜΙΟΥΡΓΙΑ ΔΙΚΤΥΩΝ ΜΕ ΤΗΝ ΒΟΗΘΕΙΑ ΠΡΟΣΟΜΟΙΩΤΗ 65

5.2 ΕΝΔΕΙΚΤΙΚΕΣ ΕΡΩΤΗΣΕΙΣ ΑΠΟ FINAL TEST CCNA 83

ΣΥΜΠΕΡΑΣΜΑΤΑ ..... .99

ΒΙΒΛΙΟΓΡΑΦΙΑ 1022

ΠΑΡΑΡΤΗΜΑ ΑΣΚΗΣΕΙΣ ΣΤΟ CCNA 1044

ΕΙΣΑΓΩΓΗ

Σήμερα η αγορά εργασίας στο χώρο της πληροφορικής ζητά συνεχώς περισσότερες γνώσεις που να μπορεί κάποιος να τις επιβεβαιώνει στον μελλοντικό εργοδότη. Μάλιστα η σύγχρονη ανταγωνιστική οικονομία πλέον βασίζεται στη γνώση και τη διάχυσή της, και θέτει ως βασική προτεραιότητα για κάθε πολίτη την εκπαίδευση και την απαίτηση βεβαίωσης ότι τελικά κατέχει τις απαιτούμενες δεξιότητες σε ικανοποιητικό βαθμό. Στον τομέα των της Πληροφορικής & Επικοινωνιών αυτό αποτελεί αναγκαίο αφού υπάρχει συνεχής ανάπτυξη και απαιτεί από τους εργαζόμενους γρήγορα και αποτελεσματικά αποτελέσματα.

Πλέον η απόκτηση γνώσεων και δεξιοτήτων και πιστοποίησης αυτών στην Πληροφορικής εξελίσσεται σε πρωταρχικό ανταγωνιστικό πλεονέκτημα του ατόμου και του ανθρώπινου δυναμικού και αποτελεί μάλιστα πολύτιμο επαγγελματικό εργαλείο και εφόδιο, για την εξέλιξη της καριέρας ή της ένταξής του στην αγορά εργασίας.

Στην πληροφορική υπάρχουν πολύ πάρα πολλές πιστοποιήσεις με γνωστότερες αυτές στο χώρο των δικτύων όπως το CCNA , το CCNP το CCNA Security, Microsoft Technology Associate, COMPTIA+, HP ATA, κ.α.

Στη παρούσα πτυχιακή εξετάζουμε την πιστοποίηση CCNA. Το CCNA (CISCO Certified Netword Associate) είναι ουσιαστικά μια πιστοποίηση που περνά από το πιστοποιημένο πρόγραμμα της Ακαδημίας Δικτύων CISCO που παρέχεται από το 1997. Η εκπαίδευση στο CCNA αφορά την γνώση και χρήση των δικτύων υπολογιστών, την χρήση δικτυακών συσκευών, από τους απλούς host που συνδέονται στο δίκτυο, τους ασύρματους και ενσύρματους δρομολογητές (routers), τους μεταγωγείς (switches) καθώς και πληθώρα υποστηρικτικών εξοπλισμών.

Η CISCO έχει αναπτύξει μια σειρά διαλέξεων που παρέχεται σε δικτυακό περιβάλλον και είναι διαθέσιμες μέσω ειδικού περιβάλλοντος και κατάλληλης ηλεκτρονικής τάξης που δίνει την δυνατότητα να μάθει κανείς με ηλεκτρονικό τρόπο. Επίσης στο συγκεκριμένο περιβάλλον της CISCO οι σπουδαστές έχουν την δυνατότητας να

εντοπίσουν περαιτέρω υλικό και προσομοιωτές δικτύων που τους βοηθούν στην εκπαίδευσή τους. Οι ακαδημίες της CISCO παρέχουν ειδικά εξοπλισμένα εργαστήρια με πραγματικές συσκευές ώστε οι φοιτητές να έχουν επιπλέον εξοικείωση με τον δικτυακό εξοπλισμό.

Η διδακτέα ύλη είναι χωρισμένη σε τέσσερις ενότητες που καλύπτουν σημαντικές αρχές δικτύων, όπως δρομολόγηση και μεταγωγή πακέτων σε τοπικά δίκτυα και ασύρματη μετάδοση σε τοπικά δίκτυα. Ακόμα συμπεριλαμβάνονται θέματα που αφορούν πρωτόκολλα και τεχνολογίες που βρίσκει κανείς στα δίκτυα ευρείας ζώνης. Με το επιτυχημένο πέρας των τεσσάρων ενοτήτων οι σπουδαστές έχουν κατακτήσει όλες τις αναγκαίες γνώσεις και δεξιότητες για την επιτυχή απόκτηση της πιστοποίησης CCNA. Όταν ο φοιτητής νιώσει έτοιμος μπορεί να δηλώσει συμμετοχή σε εξετάσεις πιστοποίησης. Η πιστοποίηση CCNA θέτει τις βάσεις μία επιτυχημένη καριέρα, ενώ ταυτόχρονα προσφέρει τις βασικές γνώσεις δικτύων για όλους τους επιστήμονες της πληροφορικής.

Στόχος της πτυχιακής μας είναι η παρουσίαση της ύλης του CCNA και τον τρόπο που μπορεί κάποιος να οδηγηθεί σε πιστοποίηση. Πιο συγκεκριμένα εξετάζεται το πρωτόκολλο TCP-IP που αποτελεί το βασικό πρωτόκολλο που εξετάζει το CCNA , το πρόβλημα της δρομολόγησης καθώς και ο τρόπος και οι αλγόριθμοι που εφαρμόζονται για την μεταφορά μηνυμάτων σε ένα δίκτυο. Στην δρομολόγηση στόχος είναι να βρεθεί η βέλτιστη διαδρομή ώστε ένα μήνυμα να φτάσει όσο το δυνατόν γρηγορότερα στην τελική διεύθυνση του και με τον πιο ασφαλή τρόπο.

Οι συσκευές που εν τέλει αποφασίζουν την διαδρομή που θα ακολουθήσει ένα πακέτο είναι οι ενδιάμεσες με σημαντικότερη τους δρομολογητές . Οι δρομολογητές είναι οι συσκευές που έχουν την δυνατότητας να συνδέσουν δίκτυα μεταξύ τους. Δημιουργούν πίνακες δρομολόγησης που με βάση αυτούς δρομολογούνται τα πακέτα μέχρι τον τελικό προορισμό. Η δρομολόγηση στην ουσία είναι η δημιουργία του πίνακα δρομολόγησης από τον εκάστοτε δρομολογητή.

Σε αυτή την πτυχιακή εργασία ουσιαστικά ασχολούμαστε με τον ορισμό της δρομολόγησης, ποια είναι τα επιμέρους είδη αλλά και τα πρωταρχικά γνωρίσματα της. Συνακόλουθα θα προχωρήσουμε στον ορισμό του αλγορίθμου δρομολόγησης, τις θεμελιώδεις απεικονίσεις που εμφανίζεται ο πίνακας δρομολόγησης, αλλά και τις πρωταρχικές στρατηγικές δρομολόγησης.

Επιπρόσθετα θα ασχοληθούμε με τους βασικούς αλγόριθμους δρομολόγησης και την χρήση τους από τα πρωτόκολλα δρομολόγησης. Ακόμα θα παραθέσουμε τα πρωταρχικά πρωτόκολλα δρομολόγησης στα δίκτυα υπολογιστών, των οποίων η χρήση γίνεται ως επί το πλείστων στα σημερινά δίκτυα.

Επίσης εξετάζουμε τα θέματα των μεταγωγέων (Switches), τον προγραμματισμό τους καθώς και την λειτουργία τους με τον πιο ασφαλή τρόπο για το δίκτυο μας. Ορίζουμε το πώς λειτουργούν τα VLAN και πως χωρίζουμε σε υποδίκτυα ένα δίκτυο.

Στη συνέχεια με την βοήθεια ενός προσομοιωτή δικτυών δημιουργούμε σενάρια δικτύων έτσι ώστε να χρησιμοποιήσουμε όσα αναφέραμε παραπάνω και να δημιουργήσουμε διαφορετικά δίκτυα που εξυπηρετούν διαφορετικές ανάγκες και διαφορετικές τεχνολογίες.

Στο τέλος παραθέτουμε συμπεράσματα που αναφέρονται τόσο στην σύγκριση των πρωτοκόλλων μεταξύ τους όσο και για το πώς ένας επαγγελματίας δικτύων μπορεί να καταλήξει με τον πιο ορθό τρόπο στην πιστοποίηση.

ΚΕΦΑΛΑΙΟ 1: ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΥΠΟΛΟΓΙΣΤΩΝ

1.1 Οι πιστοποιήσεις Πληροφορικής σήμερα

Σήμερα η πιστοποίηση είναι ένα σημαντικό εφόδιο για την αγορά εργασίας. Η πιστοποίηση συνήθως συνοδεύει τον βασικό τίτλο σπουδών από κάποιο ανώτερο οργανισμό και ισχυροποιεί το βιογραφικό κάποιου αφού βεβαιώνει συγκεκριμένες δεξιότητες.

Σήμερα μπορεί κάποιος να πιστοποιήσει φάσμα πιστοποιήσεων σε όλους τους τομείς. Πιο συγκεκριμένα σε διεθνές επίπεδο υπάρχουν πιστοποιήσεις μέσω των οποίων μπορεί κάποιος να αποδείξει τις δεξιότητες και γνώσεις που έχει για κάποιο συγκεκριμένο αντικείμενο.

Ειδικά στο χώρο της πληροφορικής υπάρχουν πιστοποιήσεις σε πολλά διαφορετικά αντικείμενα.

Οι πιστοποιήσεις στην χωρίζονται στους παρακάτω βασικούς τομείς:

- Γενικού Χειρισμού
- Προγραμματισμού
- Δικτύων
- Εφαρμογών

Στον ελληνικό χώρο υπάρχουν φορείς αναγνωρισμένοι από το ελληνικό δημόσιο που πιστοποίηση κυρίως Γενικού Χειρισμού Υπολογιστών αλλά και σε μια ποικιλία διαφορετικών αντικειμένων. Οι αναγνωρισμένοι φορείς από το ελληνικό δημόσιο και συγκεκριμένα από το υπουργείο παιδείας μέσω του φορέα ΕΟΠΠΕΠ είναι οι:

- ACTA

- INFOTEST
- Vellum Global Educatinal Services
- DIPLOMA - Φορέας Πιστοποίησης Ανθρώπινου Δυναμικού
- INFOCERT
- KEY-CERT
- GLOBAL CERT
- I SKILLS
- PeopleCert – ECDL
- UNICERT

Στο χώρο όμως των ειδικών πιστοποιήσεων η εταιρία που συγκεντρώνει το 90% των πιστοποιήσεων σε παγκόσμιο επίπεδο είναι η Pearson VUE.

Η Pearson VUE είναι μια εταιρία πιστοποίησης που ουσιαστικά μονοπωλεί το χώρο των πιστοποιήσεων πληροφορικής διεθνώς. Είναι ο μεγαλύτερος παγκόσμιος οργανισμό πιστοποίησης με πάνω από 5000 εξεταστικά κέντρα σε 165 χώρες. Οι μεγαλύτερες εταιρίες στον κόσμο εμπιστεύονται την Pearson VUE για τις πιστοποιήσεις στα προϊόντα τεχνολογίας τους. Τέτοιες εταιρίες είναι η Cisco, Autodesk, Adobe, Microsoft κ.α. αλλά και σε μια σειρά εκπαιδευτικών οργανισμών με μεγάλη εκπαιδευτική δράση.

Έτσι σήμερα μπορεί κάποιος να πιστοποιηθεί σε αντικείμενα όπως:

C++, JAVA,PHP, Design , Networks , Advanced Networks, Mobile Programming κ.α.

Οι υποψήφιοι όταν θέλουν να εξεταστούν μπορούν μέσα από το διαδίκτυο απλά να ορίσουν μία ημερομηνία, να πληρώσουν με την πιστωτική τους κάρτα και τελικά να δώσουν εξετάσεις.

Στο χώρο των δικτύων η πιστοποίηση που είναι πιο δημοφιλής είναι η πιστοποίηση της CISCO με ονομασία CCNA.

Η πιστοποίηση CCNA αποτελεί ουσιαστικά το διαβατήριο για την εξεύρεση εργασίας στο χώρο των δικτύων αφού εξασφαλίζει στους εργοδότες ότι ο υποψήφιος για εργασία είναι άριστος γνώστης των τεχνολογιών που εφαρμόζονται στα δίκτυα.

1.2 Το CCNA

Στο χώρο των δικτύων, οι πιστοποιήσεις της Cisco θεωρούνται τα πιο ισχυρά εφόδια. Πιο συγκεκριμένα στην αγορά εργασίας στον τομέα της πληροφορικής οι πιστοποιήσεις της CISCO ξεχωρίζουν ανάμεσα σε χιλιάδες πιστοποιήσεις από άλλους φορείς ανά τον κόσμο. Η Cisco μέσω των ακαδημαϊκών προγραμμάτων της, απαιτεί από τους επίσημους συνεργάτες της να απασχολούν τεχνικούς που διαθέτουν μία ή περισσότερες από τις πιστοποιήσεις που παρέχει μαζί με την Pearson VUE. Οι πιστοποιήσεις της Cisco θα έλεγε κανείς ότι αποτελούν πλέον αναγκαιότητα για τους τεχνικούς συστημάτων πληροφορικής και δικτύων.

Σήμερα η πιο δημοφιλή πιστοποίηση της CISCO είναι το λεγόμενο CCNA. Η CISCO ουσιαστικά έχει δημιουργήσει την πιστοποίηση CCNA (Cisco Certified Network Associate) που ουσιαστικά είναι ένα ολόκληρο πρόγραμμα εκπαίδευσης και πιστοποίησης που τελικά εξασφαλίζει ότι ο υποψήφιος για την πιστοποίηση είναι άριστος γνώστης των τεχνολογιών που εφαρμόζονται στα δίκτυα σήμερα.

Σήμερα η φιλοσοφία στον επαγγελματικό χώρο του τομέα των επικοινωνιών που σχετίζεται με την πληροφορική και την εξέλιξη των δικτύων σε μικρές και μεσαίες επιχειρήσεις, απαιτεί το προφίλ του Τεχνικού Δικτύων και Ίντερνετ να είναι εξειδικευμένο.

Με αυτό το CCNA ο υποψήφιος θα κατανοήσει τις λειτουργίες των τοπικών δικτύων. Θα αποκτήσει τη δυνατότητα τόσο να εφαρμόζει και να αναπτύσσει τοπικά δίκτυα σε μια εταιρεία όσο και να μπορεί αποτελεσματικά να διαχειρίζεται αυτά και να τα συντηρεί.

Η Cisco μέσω της πιστοποίηση CCNA αλλά και τον άλλων πιστοποιήσεων διασφαλίζει ότι ο κάτοχός των πιστοποιήσεων έχει όλες τις απαραίτητες γνώσεις για δίκτυα μικρού και μεσαίου μεγέθους, ακόμα και για τμήματα μεγαλύτερων δικτύων. Με την ολοκλήρωση του προγράμματος σπουδών του CCNA, ο κάτοχός του είναι

ικανός να εγκαταστήσει, να διαχειριστεί και να συντηρήσεις τοπικά δίκτυα (LANs), δίκτυα ευρείας περιοχής (WANs), να ορίσει υπηρεσίες στα δίκτυα όπως DNS, DHCP.

1.3 Ανάγκη στην αγορά για πιστοποιημένη γνώση δικτύων

Σήμερα στην αγορά εργασίας υπάρχει μια έντονη κρίση αφού οι θέσεις εργασίας είναι περιορισμένες αλλά ταυτόχρονα οι υποψήφιοι γι' αυτές είναι αρκετοί. Αυτό δυστυχώς συμβαίνει και στις περιπτώσεις των θέσεων πληροφορικής και δικτύων. Παρόλα αυτά μπορεί να ακούγεται λίγο «παράδοξο», στην αγορά εργασίας να επικρατεί αναντιστοιχία ανάμεσα στα υψηλά επίπεδα ανεργίας των πτυχιούχων νέων αλλά και στην ανάγκη και τελικά διαρκή ζήτηση των εργοδοτών για συγκεκριμένες δεξιότητες.

Ακόμα και για όσους έχουν προχωρήσει στην «ανατομία» του προβλήματος και με γνώση, εμπειρία αλλά και με την άποψή τους μπορούν συμβάλλουν στην κατανόηση του φαινομένου.

Μάλιστα σύμφωνα με έρευνα της McKinsey «Education to Employment: Getting Europe's Youth into Work» φαίνεται ότι στην αγορά εργασίας παρουσιάζεται το εξής παράδοξο. Ενώ υπάρχουν θέσεις εργασίας και ταυτόχρονα μεγάλη ανεργία οι θέσεις δεν καλύπτονται. Αυτό γιατί όπως έδειξε η έρευνα το 33% των εργοδοτών που συμμετείχαν στην έρευνα από όλη την Ευρώπη, δήλωσαν ότι δεν μπορούν να βρουν τις κατάλληλες δεξιότητες για να καλύψουν θέσεις εργασίας στελεχών στις επιχειρήσεις τους.

Πιο συγκεκριμένα στην Ελλάδα φαίνεται ότι το ποσοστό αυτό είναι κατά πολύ υψηλότερο και φτάνει το 45%. Μία άλλη έρευνα του ιδρύματος ALBA στην Ελλάδα επιβεβαιώνεται αλλά και επαυξάνει το παραπάνω σε σχέση με την απασχόληση των νέων στη χώρα. Σύμφωνα με την οποία το 53,3% των επιχειρήσεων δηλώνει ότι έχει δυσκολία να βρει νέους υποψηφίους με τις σωστές δεξιότητες και χαρακτηριστικά, όπως και με εργασιακή εμπειρία, παρά το γεγονός ότι η πλειονότητα των άνεργων νέων μας είναι πτυχιούχοι ανώτατης εκπαίδευσης.

Παρόλα αυτά η γνώση και η απόδειξη κατοχής της γνώσης αυτής, θέλει πιστοποίηση όπως οι περισσότεροι φορείς πιστοποίησης τονίζουν καθώς και το υπουργείο Παιδείας στην χώρα μας.

Στο χώρο που ορίζει η Κοινωνία της Πληροφορίας αλλά και Οικονομίας της Γνώσης ορίζονται νέοι κανόνες για μια πιο διευρυμένη αγορά εργασίας. Σήμερα ο χώρος των επιχειρήσεων γίνεται όλο και περισσότερο ανταγωνιστικός και συνεχώς πιο απαιτητικός. Το μεταβαλλόμενο αυτό περιβάλλον επηρεάζει και τις ανάγκες εργασίες από κάθε ανθρώπου ο οποίος επιθυμεί να πρωταγωνιστήσει και να αναδειχθεί. Μάλιστα τον οδηγεί σε ανάλογη και συνεχή εκπαίδευση ώστε τελικά να μπορεί να εξελίσσεται. Ένα όπλο σε αυτή την συνεχόμενη διαδικασία είναι η γνώση αλλά και η απόδειξη ότι γνωρίζει που αυτό το διασφαλίζει η πιστοποίηση.

Μάλιστα ο καιρός που στην Ελλάδα καθένας ήταν ότι δηλώσει φαίνεται να έχει τελειώσει, πλέον αντί της απλής δήλωσης ορίζουμε την πιστοποίηση η οποία παίζει ακριβώς αυτό το ρόλο. Να καλύψει την ανάγκη του να φαίνεται πραγματικά τι γνωρίζει κανείς. Η πιστοποίηση επιβεβαιώνει πλέον ποιος είναι κάποιος και αν αυτό που δηλώνει είναι αυτό που πραγματικά είναι και αυτό ουσιαστικά ορίζεται με την λέξη πιστοποιημένος. Σήμερα οι υποψήφιοι εργαζόμενοι για την αναζήτηση εργασίας ή την διατήρηση της θέση τους, πρέπει να επιδιώξουν επιπρόσθετα πιστοποιητικά σπουδών, που να είναι ποιοτικά δηλαδή να αποδεικνύουν ότι μια απαίτηση σε μία θέση εργασίας είναι γνωστή από τον εργαζόμενο.

Επίσης η πιστοποίηση μπορεί να παίξει σημαντικό ρόλο στην σοβαρή παράμετρο της ανεργίας. Η πιστοποίηση διευκολύνει την είσοδο στην εργασία. Έτσι όταν ζητείται να καλυφθεί μια θέση εργασίας, είναι φυσικό να επιλέγεται πιο εύκολα για την συγκεκριμένη θέση ένας πιστοποιημένος παρά ένας που απλά δηλώνει ότι γνωρίζει. Ταυτόχρονα ένας πιστοποιημένος είναι σε θέση να πετυχαίνει καλύτερη αμοιβή εάν έχει μια σωστή πιστοποίηση που δείχνει ότι γνωρίζει και μπορεί καλύτερα να ανταπεξέλθει σε συγκεκριμένες απαιτήσεις.

Επίσης παλιότερα κάποιος που καταλάμβανε μία θέση εργασίας παρέμενε σε αυτήν μόνιμος για πολλά χρόνια. Η κινητικότητα όμως πλέον είναι μια πραγματικότητα. Έτσι πλέον κάθε δυο – τρία χρόνια, οι εργαζόμενοι αλλάζουν θέση εργασίας και μάλιστα πολλοί αλλάζουν πλήρη προσανατολισμό.

Η πιστοποίηση στην κινητικότητα παίζει πολύ σημαντικό ρόλο.Η πιστοποίηση μάλιστα αποτελεί βασικό πρόσθετο προσόν στο τυχόν πτυχίο που υπάρχει. Δηλαδή κάποιος πιστοποιείται, ανεξάρτητα για ποια πιστοποίηση πρόκειται, πρακτικά πιστοποιεί τα παρακάτω:

- τη γνώση
- τις δεξιότητες
- την εμπειρία
- ειδικά χαρακτηριστικά

Μάλιστα στο ρητορικό ερώτημα «γιατί δεν αρκεί μόνο το πτυχίο;» ουσιαστικά η αγορά γνωρίζει ότι τα πανεπιστήμια που δίνουν πτυχία, παρέχουν μόνο τη απαραίτητη η βασική γνώση. Δηλαδή παρέχουν μόνο τον πρώτο παράγοντα για την επιτυχή επαγγελματική αποκατάσταση.

Το πανεπιστήμιο δίνει πτυχίο, αλλά ο υποψήφιος για εργασία δεν φαίνεται να έχει ούτε δεξιότητες, ούτε εμπειρία, ούτε κάποια ειδικά χαρακτηριστικά για συγκεκριμένες θέσεις. Γι' αυτό και στην Ελλάδα προκύπτει η αναντιστοιχία εκπαίδευσης και απασχόλησης. Η πιστοποίηση ουσιαστικά καλύπτει το συγκεκριμένο κενό. Δηλαδή την σύνδεση της εκπαίδευση με την απασχόληση. Π.χ. σήμερα στην χώρα μας αλλά και στο εξωτερικό όταν ένας φοιτητής τελειώσεις μια σχολή πληροφορικής δεν είναι αμέσως διαθέσιμος να ανταπεξέλθει στις ανάγκες τις αγοράς. Αν λοιπόν μια τράπεζα ζητήσει ένα εργαζόμενο για το εταιρικό δίκτυο τότε πέραν των γνώσεων από την σχολή απαιτούνται δεξιότητες που αφορούν την αρχιτεκτονική δικτύων , ασφάλεια δικτύων και εφαρμογής τους στο τραπεζικό σύστημα. Ο υποψήφιος μπορεί να βεβαιώσεις τις γνώσεις του για τα αιτούμενα από την τράπεζα παίρνοντας τις ανάλογες πιστοποιήσεις.

ΚΕΦΑΛΑΙΟ 2: ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΔΙΚΤΥΩΝ

2.1 Δικτύων Υπολογιστών

Ένα δίκτυο υπολογιστών αποτελεί ένα διασυνδεμένο σύστημα από αυτόνομους ή μη αυτόνομους συνδεδεμένους υπολογιστές. Με την λέξη υπολογιστές θεωρούμε διάφορες τερματικές συσκευές, όπως σταθερούς υπολογιστές, φορητούς υπολογιστές, κινητά τηλέφωνα, εκτυπωτές, κ.α.

Οι τερματικές συσκευές λοιπόν θεωρούνται διασυνδεδεμένες όταν μπορούν να ανταλλάξουν πληροφορίες μεταξύ τους , ενώ αυτόνομες όταν είναι αδύνατον μία συσκευή να ελέγξει τη λειτουργία κάποιας άλλης.

Η μελέτη των δικτύων υπολογιστών επιτυγχάνεται με τις ενδιάμεσες συσκευές. Που η εγκατάσταση και η διαχείριση τους καθορίζει το κλάδο των ειδικών δικτύων Επομένως στον τομέα των επικοινωνιών σαν «Δίκτυο» ονομάζουμε ένα σύστημα που συνδέει κάθε είδους τερματικές συσκευές, είτε αυτές είναι σταθερές είτε κινητές. Οπότε κάθε δίκτυο πρέπει να διαθέτει την κατάλληλη δομή έτσι ώστε να επιτυγχάνεται η επικοινωνία όλων των τερματικών συσκευών που αποτελούν το δίκτυο.

Στην ουσία ένα δίκτυο αποτελείται από ενδιάμεσων συσκευές με σκοπό να μεταφέρουν στον παραλήπτη τα μηνύματα που αποστέλλονται από τις τερματικές συσκευές. Οι τερματικές συσκευές επεξεργάζονται τα πακέτα με κατάλληλο τρόπο ακολουθώντας πρωτόκολλα δρομολόγησης και επαναπροώθησης των πακέτων που υλοποιούνται με τους απαραίτητους αλγόριθμους.

Τελικά το σύνολο των τερματικών συσκευών, και των ενδιάμεσων , σε συνδυασμό με τα πρωτόκολλα δρομολόγησης και επαναπροώθησης αποτελούν το «Δίκτυο» μας.

2.2 Είδη δικτύων

Τα δίκτυα μπορούν να ομαδοποιηθούν σε διάφορες κατηγορίες ανάλογα με τα παρακάτω:

- Το φυσικό μέσο διασύνδεσής, που χαρακτηρίζονται ως «ενσύρματα» ή «ασύρματα».
- Τον τρόπο πρόσβασης, που χαρακτηρίζονται ως «δημόσια» ή «ιδιωτικά» δίκτυα.
- Τον τρόπο σύνδεσης σε σχέση με την γεωγραφική κάλυψη του δικτύου και χαρακτηρίζονται ως «τοπικά» (LAN και WLAN), «προσωπικά» (PAN και WPAN), «μητροπολιτικά» (MAN και WMAN), «ευρείας κάλυψης» (WAN και WWAN).

Ανά γεωγραφική κάλυψη πιο αναλυτικά έχουμε:

- **Τοπικά**

  Τα «τοπικά δίκτυα» ή «LAN» (local area networks) είναι δίκτυα που συνδέουν σχετικά μικρό αριθμό υπολογιστών σε μικρές αποστάσεις, π.χ. υπολογιστές που βρίσκονται σε ένα μικρό χώρο έως υπολογιστές που απέχουν μερικα χιλιόμετρα μεταξύ τους. Χρησιμοποιούνται κυρίως για να συνδέουν υπολογιστές σε γραφεία εταιρειών, και πανεπιστήμια κ.λπ.

- **Μητροπολιτικά**

Ένα «μητροπολιτικό δίκτυο» «MAN» (metropolitan area network) μοιάζει με το τοπικό δίκτυο αλλά έχει μεγαλύτερη εμβέλεια όσον αφορά την απόσταση. Καλύπτει αποστάσεις, από μια ομάδα γειτονικών γραφείων μιας εταιρείας έως μια πόλη.

- **Ευρείας περιοχής**

Τα «δίκτυα ευρείας περιοχής» ή «WAN» (wide area network) καλύπτουν μεγαλύτερες γεωγραφικές αποστάσεις από τα «MAN». Είναι ιδανικά ώστε να καλύπτουν από μια ολόκληρη πόλη έως εκατοντάδες χιλιόμετρα. Μπορούν να συνδέσουν μεγάλο αριθμό τοπικών δικτυών αλλά και ομάδες τοπικών δικτύων. Σε

μεγάλο ποσοστό τα δίκτυα ευρείας περιοχής χρησιμοποιούνται στα τηλεφωνικά δίκτυα ή σε τηλεπικοινωνιακούς δορυφόρους.

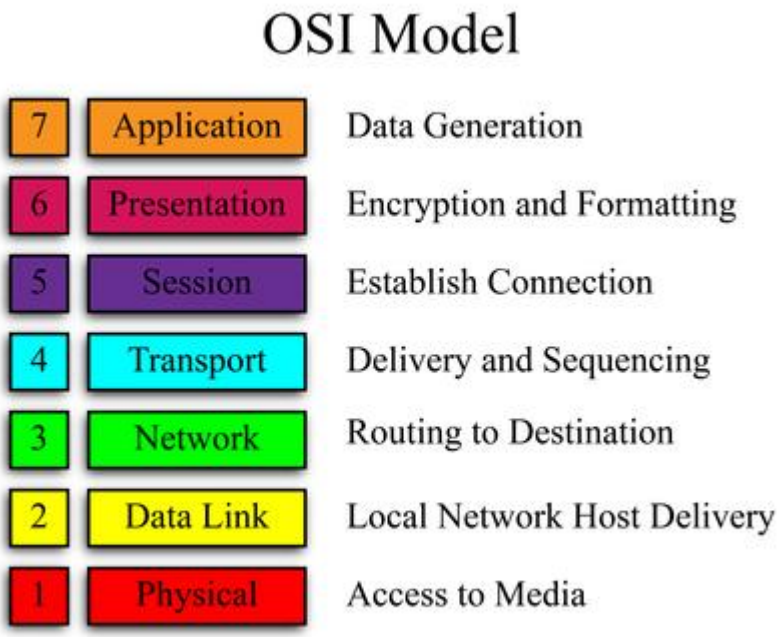
- **Διαδίκτυα**

Το «διαδίκτυο» είναι δίκτυο ευρείας περιοχής που καλύπτουν γεωγραφικές περιοχές μίας ή περισσοτέρων ηπείρων. Αυτό επιτυγχάνεται συνενώνοντας επιμέρους μικρότερα δίκτυα. Σε ένα διαδίκτυο μπορεί να είναι διασυνδεδεμένοι υπολογιστές και δίκτυα που χρησιμοποιούν διαφορετικά λειτουργικά συστήματα και τεχνολογίες . Το Διαδίκτυο (Internet) είναι το μεγαλύτερο τέτοιου είδους δίκτυο.

2.3 Το πρωτόκολλο OSI

Το μοντέλο OSI δίνει την δυνατότητα σε διαφορετικά υπολογιστικά συστήματα να επικοινωνούν μεταξύ τους. Αυτό επιτυγχάνεται διαιρώντας όλες τις απαραίτητες λειτουργίες του κάθε δικτύου υπολογιστών σε επτά επίπεδα, όπου το κάθε επίπεδο έχει διαφορετική λειτουργία χρησιμοποιώντας διαφορετικά πρωτόκολλα που κάνουν συγκεκριμένες λειτουργίες σχετικές με τις ανάγκες του κάθε επιπέδου .

Μία εικόνα του OSI μοντέλου είναι η παρακάτω:



Κάθε επίπεδο χρησιμοποιεί τις λειτουργίες του κατώτερού του επιπέδου, και προσθέτει τα δικά του χαρακτηριστικά που αφορούν τον τρόπο που διαχειρίζεται τα μηνύματα που λαμβάνονται και αποστέλλονται.

Έτσι το κάθε επίπεδο μπορεί να κάνει χρήση ενός καθορισμένου πρωτόκολλου. Τα πρωτόκολλα που χρησιμοποιούνται πραγματοποιούνται είτε σε υλικό είτε σε λογισμικό επίπεδο. Συνήθως τα κατώτερα επίπεδα εξειδικεύονται στο υλικό ενώ τα ανώτερα σε λογισμικό.

Σημαντικό χαρακτηριστικό του μοντέλου OSI είναι η διεπαφη μεταξύ των επιπέδων, η οποία καθορίζει τους κανόνες της διασύνδεση τους. Στην ουσία είναι η συνεργασία μεταξύ των επίπεδων, που πραγματοποιείτε με κάποιο άλλο πρωτόκολλο, αλλα με την προϋπόθεση ότι οι προδιαγραφές του καθενός έχουν εφαρμοστεί σωστά. Αυτές οι προδιαγραφές είναι τυπικά γνωστές ως RFC (Requests for Comments) και αποτελούν πρότυπα του Διεθνούς Οργανισμού Τυποποίησης ISO.

Τελικά το μοντέλο OSI είναι μια ιεραρχική δομή επτά επιπέδων που υποδεικνύει τους κανόνες επικοινωνίας έτσι ώστε και επιτευχθεί η επικοινωνία μεταξύ δυο τερματικών ή ενδιάμεσων συσκευών, ορίζοντας με ακρίβεια τον σκοπό κάθε επιπέδου αλλά και τα απαραίτητα πρωτόκολλα ώστε να επιτευχθεί ο στόχος . Το OSI μοντέλο τυποποιήθηκε ως πρότυπο ISO 7498-1 και θεωρήθηκε ότι θα είναι η βάση στην λειτουργική συνεργασία μεταξύ διάφορων ψηφιακών συσκευών που ήταν διαθέσιμες στην αγορά. Το μοντέλο OSI αναλυτικά περιγράφεται στον παρακάτω πίνακα:

	Μονάδα δεδομένων	**Επίπεδο**	**Λειτουργία**
Λογισμικό	Δεδομένα	7. Εφαρμογών	Παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο
		6. Παρουσίασης	Αναπαράσταση δεδομένων και κρυπτογράφηση
		5. Συνόδου	Έλεγχος του διαλόγου μεταξύ των άκρων της

			επικοινωνίας
	Τμήμα	4. Μεταφοράς	Αξιόπιστη επικοινωνία από άκρο σε άκρο
Υλικό	Πακέτο	3. Δικτύου	Καθορισμός διαδρομών και λογικών διευθύνσεων των κόμβων στα πλαίσια ενός διαδικτύου
	Πλαίσιο	2. Ζεύξης δεδομένων	Φυσική διευθυνσιοδότηση (MAC & LLC)
	Bit	1. Φυσικό	Δυαδική μετάδοση σήματος μέσω του φυσικού μέσου

2.3.1 Περιγραφή των επιπέδων OSI

Επίπεδο 7: Επίπεδο εφαρμογών

Το επίπεδο εφαρμογών ουσιαστικά προσφέρει τον τρόπο πρόσβασης στα δεδομένα που μεταφέρονται από και προς μία εφαρμογή από ένα υπολογιστή σε μία άλλη εφαρμογή σε ένα άλλο υπολογιστή του δικτύου. Ουσιαστικά το συγκεκριμένο επίπεδο κάνει την σύνδεση του χρήστη με την εφαρμογή και ως συνέπεια με το δίκτυο. Στο επίπεδο αυτό επίσης γίνεται η διαχείριση των διάφορων εφαρμογών, π.χ. το ηλεκτρονικό ταχυδρομείο. Το επίπεδο εφαρμογών χρησιμοποιεί μια σειρά πρωτοκόλλων όπως τα HTTP, POP3 , SMTP, DNS, FTP, DHCP κ.α.

Επίπεδο 6: Παρουσίασης

Το επίπεδο παρουσίασης προετοιμάζει και ανασχηματίζει τα δεδομένα μίας εφαρμογής με στόχο να λάβει την τυπική μορφή και να τα προωθήσει στο επίπεδο εφαρμογών. Στο επίπεδο αυτό η κρυπτογράφηση, η συμπίεση και η κωδικοποίηση είναι κάποιες από τις διαδικασίες που περνούν τα δεδομένα έτσι ώστε να πάρουν την σωστή διαμόρφωση και να προωθηθούν στο επίπεδο εφαρμογών. Το επίπεδο

παρουσίασης λοιπόν είναι υπεύθυνο για την μετατροπή αρχείων από κώδικα EBCDIC, σε κώδικα ASCII, σε μορφή XML κ.α..

Επίπεδο 5: Συνόδου

Το επίπεδο συνόδου ελέγχει τις ανταλλαγές δεδομένων μεταξύ δύο υπολογιστών. Διαχειρίζεται τη σύνδεση μεταξύ δυο εφαρμογών, επίσης είναι υπεύθυνο για το άνοιγμα και τον τερματισμό της σύνδεσης. Διαχειρίζεται λειτουργίες FDX ή HDX, και τέλος υποστηρίζει διαδικασίες αποθήκευσης κατάστασης, αναβολής, τερματισμού και επανεκκίνησης έτσι ώστε να επιτευχθεί η ορθή επικοινωνία.

Επίπεδο 4: Μεταφοράς

Στο επίπεδο μεταφοράς ουσιαστικά ορίζεται η μεταφορά των δεδομένων από χρήστη σε χρήστη. Το επίπεδο μεταφοράς στόχο έχει τον έλεγχο και αξιόπιστη επικοινωνία. Πρωταρχικές ευθύνες για να επιτευχθεί αυτό είναι η παρακολούθηση κάθε επικοινωνίας μεταξύ των εφαρμογών του αποστολέα και του παραλήπτη. Επίσης κάνει κατάτμηση των δεδομένων σε πακέτα και διαχειρίζεται κάθε ένα από αυτά. Τέλος αντιλαμβάνεται και προσδιορίζει τις διαφορετικές εφαρμογές. Σήμερα τα πιο συνηθισμένα πρωτοκόλλα μεταφοράς είναι το TCP (Transmission Control Protocol) και το UDP (User Datagram Protoco), καθώς και το SCTP (Stream Control Transmission Protocol) κλπ.

Επίπεδο 3: Δικτύου

Το επίπεδο δικτύου παρέχει υπηρεσίες για την ανταλλαγή των επιμέρους πακέτων δεδομένων μέσω των τερματικών συσκευών (κόμβων) του δικτύου. Για να επιτευχθεί αυτό χρησιμοποιεί τέσσερις βασικές διεργασίες.

- **Την διευθυνσιοδοτηση**
- **Την κατάτμηση**
- **Την δρομολόγηση**
- **Την αποτμηματοποίηση**

Οι δρομολογητές (routers) λειτουργούν στο επίπεδο αυτό· όπου διακινούν τα δεδομένα σε διαφορετικά υποδίκτυα ή δίκτυα. Μάλιστα οι routers αποτελούν και τις βασικές συσκευές στο Internet όπου ουσιαστικά ορίζουν τους κόμβους του διαδικτύου.

Επίπεδο 2: Ζεύξης Δεδομένων

Το επίπεδο ζεύξης δεδομένων παρέχει τις λειτουργίες και διαδικασίες ώστε να επιτευχθεί η μεταφορά δεδομένων στις συσκευές ενός τοπικού δικτύου. Χρησιμοποιεί σαν εργαλείο τις φυσικές διευθύνσεις των συσκευών (MAC), οι οποίες είναι προκαθορισμένες από την κάρτα δικτύου του κάθε τερματικού. Στο επίπεδο ζεύξης δεδομένων το γνωστότερο πρότυπο για τοπικά δίκτυα είναι το Ethernet. Το επίπεδο αυτό σε κάποια πρωτόκολλα όπως το FDDI διαιρείται σε δυο μικρότερα :

- Το επίπεδο ελέγχου πρόσβασης στο μέσο, το υποεπίπεδο MAC (Media Access Control) που υλοποιεί διεργασίες από το πιο κάτω επίπεδο του μοντελου OSI, δηλαδή του φυσικού επιπέδου.
- Το επίπεδο ελέγχου λογικών συνδέσεων, το υποεπίπεδο LLC (Logical Link Control), όπου υλοποιεί διεργασίες από ανώτερο επίπεδο του μοντέλου OSI ανεξάρτητα από το φυσικού επιπέδου.

Στο επίπεδο αυτό χρησιμοποιούνται συσκευές όπως γέφυρες (bridge) και μεταγωγεις (switch).

Επίπεδο 1: Φυσικό

Το φυσικό επίπεδο παρέχει τα μέσα για την μεταφορά τις πληροφορίας μέσα από όλους τους διαφορετικούς τύπους και φυσικές προδιάγραφες του δικτύου. Αυτό το στρώμα δέχεται πακέτα από το επίπεδο ζεύξης δεδομένων και τα κωδικοποιεί ως μια σειρά από δυαδικά ψηφιά (bits), που στην συνέχεια προωθούνται στο φυσικό μέσο και παραλαμβάνονται από ενδιάμεσες ή τερματικές συσκευές. Συσκευές φυσικού επιπέδου είναι οι επαναλήπτες (repeaters), οι κάρτες δικτύου. Οι κυριότερες λειτουργίες του φυσικού επιπέδου είναι:

- Άνοιγμα και κλείσιμο μιας σύνδεσης με μια συσκευής.
- Επίλυση προβλημάτων σε περιπτώσεις (πολυπλεξία), όπου δηλαδή εξυπηρετούνται ταυτόχρονα και αποτελεσματικά πολλοί χρήστες μέσω των ιδίων μέσων του δικτύου, δίνοντας προτεραιότητα πρόσβασης και έλεγχο ροής των πληροφοριών.
- Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων ανάλογα την συσκευή και το μέσω που πρέπει να προσπελάσουν, δηλαδή το πακέτο μπορεί να πάρει την μορφή αναλογικού σήματος αν μεταδίδεται σε χάλκινο καλώδιο και στην συνέχεια να διαμορφωθεί σε δέσμη φωτός για να περάσει από καλώδιο οπτικής ίνας.

2.4 Δικτυακές συσκευές

Σαν δικτυακές Συσκευές ονομάζουμε τις συσκευές εκείνες οι οποίες είναι υπεύθυνες για τον έλεγχο και τη διαχείριση των πόρων του δικτύου.

Είναι αναγκαίο πλέον να υπάρχουν πληθώρα δικτυακών συσκευών λόγω της τεράστιας ανάπτυξης και χρήσης των δικτύων στην καθημερινή μας ζωή, συνεπώς συνέχεια γεννιούνται νέες ανάγκες, όπως για την υποστήριξη όλο και μεγαλύτερου αριθμού χρηστών ή μεγαλύτερες ανάγκες ως προς την ταχύτητα επικοινωνίας και την ασφάλεια του δικτύου κ.α. Με γνώμονα τις ανάγκες δημιουργήθηκαν δικτυακές συσκευές που υλοποιούν τις ανάγκες, την ιεραρχική δομή των δικτύων, την εγκατάσταση αποδοτικών τοπολογιών, την διασύνδεση υποδικτύων κ.α..

Οι πιο γνωστές δικτυακές συσκευές είναι οι παρακάτω :

- Routers
- Switchers
- Gateaways
- Bridges
- Hubs
- Repeaters

Router – Δρομολογητής

Οι δρομολογητές είναι συσκευές οι οποίες είναι υπεύθυνες για την δρομολόγηση των πακέτων μέσα στο δίκτυο, και έχει την δυνατότητα να συνδέσει δυο η περισσότερα δίκτυα μεταξύ τους. Εφόσον δημιουργηθεί κάποια βλάβη ή κάποιος άλλος παράγοντας που θα τροποποιήσει τη τοπολογία, οι δρομολογητές ανακατευθύνουν τα πακέτα δεδομένων ώστε να επιτευχθεί γρηγορότερα και ασφαλέστερα η δρομολόγηση τους στο δίκτυο. Κατά βάση ελέγχουν την αποστολή των πακέτων στο δίκτυο, εξασφαλίζοντας παράλληλα ότι θα φτάσουν στον τελικό παραλήπτη, αποτρέποντας την πρόσβαση άλλων δικτυών λειτουργώντας απαγορευτικά για μη σχετικές πληροφορίες.

Οι δρομολογητές είναι συσκευές που λειτουργούν στο επίπεδο 3 του OSI μοντέλου, και μάλιστα οι νέες σειρές διαθέτουν προστατευτικά τείχη (firewalls) για να εμποδίσουν κακόβουλους χρήστες από το δίκτυο μας .

Σε αυτούς εφαρμόζονται τα πρωτόκολλα δρομολόγησης ορίζοντας τους κανόνες και τις προτεραιότητες που είναι απαραίτητές για την λειτουργεία του δικτύου .

Ουσιαστικά ο τρόπος λειτουργίας ενός δρομολογητή είναι ο εξής :

Ο δρομολογητής λαμβάνοντας ένα μήνυμα πληροφορίας από κάποια ενδιάμεση συσκευή του δικτύου, το οδηγεί σε έναν προορισμό. Το ίδιο το πακέτο παρέχει τις απαραίτητες πληροφορίες για την προώθηση του, ωστόσο ο δρομολογητής είναι υπεύθυνος για το καλύτερο μονοπάτι προς αυτόν τον προορισμό, είτε στέλνοντάς το στον επόμενο router είτε κατευθείαν στον παραλήπτη εφόσον ο δρομολογητής μας συνδέεται άμεσα με αυτόν. Κριτήριο για τον προορισμό είναι οι πίνακες δρομολόγησης που δημιουργεί ο κάθε router με βάση τα αντίστοιχα πρωτόκολλα δρομολόγησης που εκτελούνται σε αυτόν.

Hub – Κατανεμητής καλωδίων

Το Hub είναι μια δικτυακή συσκευή όπου χρησιμοποιείται για να διασυνδέονται οι υπολογιστές σε ένα δίκτυο. Το hub ουσιαστικά λαμβάνει τα σήματα των ηλεκτρονικών υπολογιστών και στη συνέχεια τα ενισχύει και τα αναπαράγει σε όλες τις θύρες του. Υπάρχουν hub 10baseT, που περιλαμβάνονται θύρες στις οποίες κουμπώνουν τα καλώδια του δικτύου με θύρες RJ45 Οι θύρες τους μπορεί να είναι σε αριθμό από 4 (μικρά δίκτυα) έως και 24 συνήθως. Σε μεγαλύτερα δίκτυα μπορούμε να συνδέσουμε πολλά hubs μαζί.

Τα hubs διακρίνονται στις παρακάτω δύο κατηγορίες:

Παθητικά, τα οποία παραλαμβάνουν απλά τα σήματα και τα ξαναστέλνουν σε όλες τις συσκευές του δικτύου

Ενεργητικά που τα παραλαμβάνουν και ενισχύουν το ηλεκτρικό σήμα των εισερχόμενων πακέτων πριν τους διαδώσουν στο δίκτυο.

Έξυπνα, τα οποία είναι ενεργητικά, αλλά μικρότερα σε όγκο, εύκολα αποθηκεύσιμα και τοποθετούνται σε όποια απόσταση εμείς κι αν επιλέξουμε.

Switch –Μεταγωγέας

Οι μεταγωγείς είναι δικτυακές συσκευές με σκοπό τη σύνδεση τερματικών και ενδιάμεσων συσκευών ενός δικτύου. Οι συσκευές αυτές δίνουν τη δυνατότητα στους συνδεδεμένους χρήστες τη ταυτόχρονη αποστολή πληροφοριών στο δίκτυο ,χωρίς να υπάρχουν συγκρούσεις με αποτέλεσμα την γρηγορότερη εκτέλεση εργασιών . Επιπλέον, με τη χρήση των συσκευών αυτών δημιουργείται εξοικονόμηση χώρου δικτύου(bandwidth) αποτρέποντας τα μηνύματα εκπομπής (broadcast) να κατακλύσουν το δίκτυο και παράλληλα ελέγχει τα μηνύματα μεταξύ αποστολέα και παραλήπτη.

Οι μεταγωγεις χωρίζονται σε δύο κατηγορίες :

Unamanageable: ονομάζουμε τους μεταγωγεις που η λειτουργία τους είναι περιορισμένη και αδυνατεί να δώσει δυνατότητες διαχείρισης.

Manageable: Ονομάζονται οι μεταγωγεις που δίνουν αυξημένη δυνατότητα διαχείρισης, όπως ο προγραμματισμός του ανάλογα με τις ανάγκες του δικτύου και ο έλεγχος ροής της κίνησης.

Οι μεταγωγεις είναι συσκευές που λειτουργούν στο επίπεδο 2 του OSI μοντέλου, με αποτέλεσμα να αντιλαμβάνονται τις φυσικές διευθύνσεις (MAC Address) από τις

κάρτες δικτύων όλων των συσκευών του, αποθηκεύοντας τες στη μνήμη, δημιουργώντας τον κατάλληλο πίνακα διευθύνσεων (MAC table).

Υφίστανται δύο τρόποι προσέγγισης για την αντιστοιχία των φυσικών διευθύνσεων με τις θύρες του μεταγωγέα έτσι ώστε να δημιουργηθεί ο πίνακας διευθύνσεων (MAC table) .

Στη πρώτη προσέγγιση χρήσης του MAC table γίνεται μια απλή αντιστοίχιση της θύρας του μεταγωγέα με τη MAC Address του τερματικού, δηλαδή διαβάζει τη MAC Address που συνδέθηκε σε κάποια θύρα του και κάνει την αντιστοίχιση .

Σε μία δεύτερη προσέγγιση κοινής μνήμης, ο έλεγχος στην είσοδο του υλικού αποτυπώνεται σε ένα συγκεκριμένο χώρο μνήμης, και η κάθε θύρα εξόδου αντλεί τη πληροφορία από αυτήν τη μνήμη.

Πλέον, οι μεταγωγεις έχουν αντικαταστήσει με τη πάροδο του χρόνου άλλες δικτυακές συσκευές, όπως είναι οι bridges και οι gateways. Και αυτό γιατί μπορούν να έχουν πολλαπλούς επεξεργαστές με αποτέλεσμα τη καλύτερη απόδοση και λειτουργία του δικτύου ,σε αντίθεση με τους bridges και τις gateways που απαιτούν μεγαλύτερη υπολογιστική ισχύ για να φέρουν εις πέρας το ίδιο αποτέλεσμα με τους μεταγωγείς .

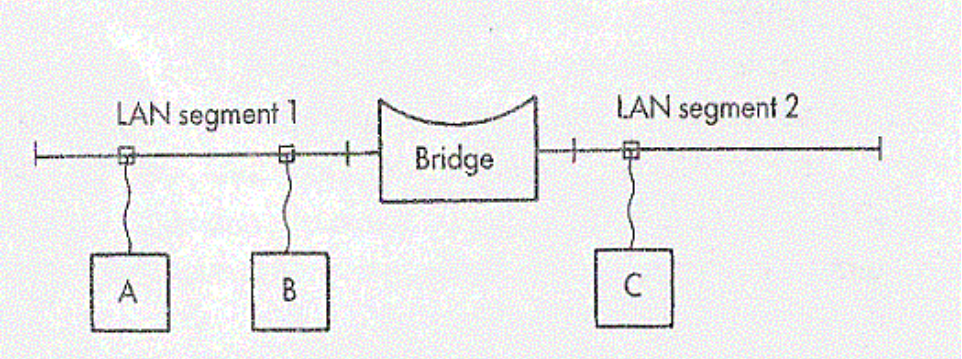
X.25 – Σειριακές συνδέσεις

Το X.25 στην ουσία είναι συσκευές που παρέχουν την δυνατότητα σύνδεση με σειριακές συνδέσεις από απόσταση. Ουσιαστικά είναι η βάση των packet-switching υπηρεσιών για remote επικοινωνίες. Χρησιμοποιούνται σε WANs και δίκτυα επιχειρήσεων.

BRIDGES (ΓΕΦΥΡΕΣ)

Τα γέφυρες είναι συσκευές οι οποίες μπορούν να περνάνε πακέτα από ένα δίκτυο σε ένα άλλο. Κάτι σαν Routers με την διαφορά ότι δρούν στο δεύτερο επίπεδο του μοντέλου OSI και μεταφέρουν απλά από το ένα δίκτυο στο άλλο πακέτα αδιακρίτως

τι υποδίκτυα πιθανά υπάρχουν σε αυτό. Μία συσκευή bridge κάνει τα δίκτυα να φαίνονται ενιαία σε πρωτόκολλα και προγράμματα υψηλότερου επιπέδου. Στην ουσία το bridge είναι μια συσκευή ειδικού σκοπού με δύο Ethernet interfaces, έστω E1 και E2. Όταν το bridge δέχεται ένα πακέτο από το interface E1 το προωθεί στο E2 και το αντίστροφο.



Επίσης μια γέφυρα μπορεί να επιτρέπει πακέτα από έναν κόμβο κάποιου δικτύου να στέλνονται σε έναν κόμβο κάποιου άλλου δικτύου, ενώ, ταυτόχρονα, παραβλέπει οποιοδήποτε πακέτο προορίζεται για το αρχικό δίκτυο (αντί να το περνάει στο άλλο δίκτυο). Οι γέφυρες είναι ανεξάρτητες από τα πρωτόκολλα υψηλότερου επιπέδου, γι' αυτό και μπορεί να χειρίζεται πακέτα, που προέρχονται από αυτά.

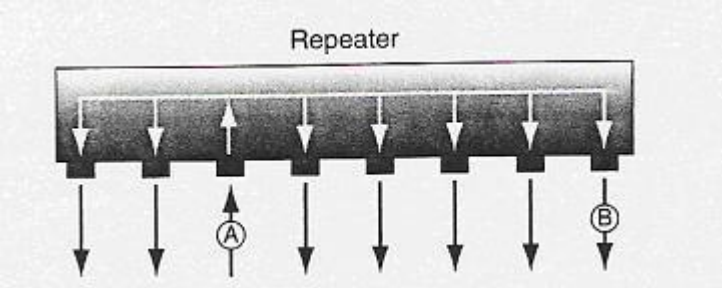
Στα πρωτόκολλα υψηλότερου επίπεδου η παρουσία μίας bridge είναι διαφανής. Αυτό σημαίνει ότι δύο δίκτυα τα οποία συνδέονται με μία bridge αντιμετωπίζονται από πρωτόκολλα ως μέρος του ίδιου λογικού δικτύου. Αυτή η ιδιότητα, κάνει δυνατή την πρόσβαση σε ένα λογικό δίκτυο που είναι κατά πολύ μεγαλύτερο από το μέγιστο επιτρεπτό φυσικό δίκτυο

Repeater

Ο repeater είναι μία συσκευή που λειτουργεί στο πρώτο επίπεδο, δηλαδή το φυσικό επίπεδο του OSI μοντέλο και ουσιαστικά μετακινεί όλα τα πακέτα από ένα τμήμα ενός δικτύου σε κάποιο άλλο. Πρακτικά αναπαράγει και συγχρονίζει και ενισχύει τα ηλεκτρικά σήματα. Στόχος του repeater είναι να επεκτείνει το μήκος του μέσου μετάδοσης στο δίκτυο, πέραν του συνηθισμένου μήκους των καλωδίων. Επίσης Repeater χρησιμοποιείται και στα ασύρματα δίκτυα.

Ένας απλός repeater συνήθως έχει δύο θύρες και στην ουσία ενώνει δύο τμήματα δικτύου. Οι repeaters είναι γενικά παθητικά στοιχεία του δικτύου, καθώς δεν

επηρεάζουν την πληροφορία που δέχονται ούτε αντιλαμβάνονται γεγονότα που συμβαίνουν στο δίκτυο όπως οι συγκρούσεις ή οι συμφορήσεις.



2.4 ΤΟ TCP/IP Μοντέλο

Το TCP/IP είναι ένα σύνολο από συμβάσεις που επιτρέπει στις όλες τις συσκευές ενός δικτύου είτε τερματικές είτε ενδιάμεσες να επικοινωνούν μεταξύ τους παρόλο των τεχνολογικών διαφορών. Ουσιαστικά θέτει τους κανόνες της επικοινωνίας σε ένα δίκτυο .

Το TCP/IP συγκροτείται από τα παρακάτω επίπεδα:

- **Στο φυσικό επίπεδο** καθορίζονται οι φυσικές συνδέσεις, είναι υπεύθυνο για τη μετατροπή του μηνύματος σε μορφή κατάλληλη ώστε να περάσει στο μέσο επικοινωνίας. Δηλαδή μετατρέπει το ψηφιακό σήμα σε αναλογικό έτσι ώστε να περάσει σε ένα αναλογικό μέσο ή σε δέσμη φωτός για να περάσει σε καλώδιο οπτικής ίνας κ.α. Τα μέσα μπορεί να είναι καλώδια, οπτικές ίνες, ασύρματες συνδέσεις, δορυφορικά σήματα κ.α.

- **Το επίπεδο Data Link** είναι υπεύθυνο ώστε να καθορίζει την διευθυνσιοδότηση των συσκευών μέσα σε ένα τοπικό δίκτυο ώστε να είναι εφικτή η ανταλλαγή μηνυμάτων σε συσκευές χαμηλού επιπέδου(Layer 2). Πιο γνωστό είναι το Ethernet στο οποίο κάθε συσκευή του δικτύου αντιστοιχεί μια MAC Address, η οποία κατά βάση είναι μια σειρά χαρακτήρων και αριθμών που προσδιορίζει τις διαφορετικές συσκευές του δικτύου.

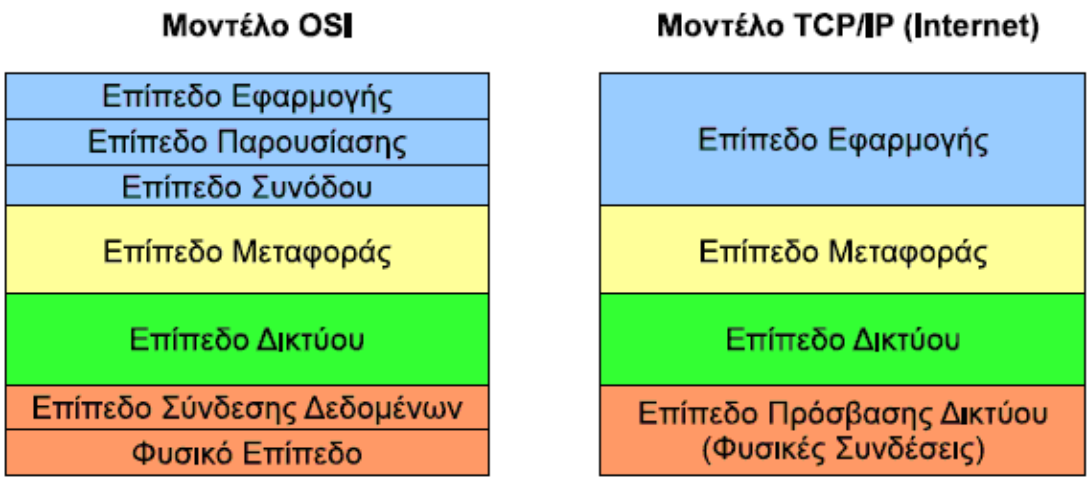
  Επίσης για απομακρυσμένες συνδέσεις με σειριακές γραμμές έχουμε χρήση του πρωτοκόλου HDLC, PPP και Frame Relay.

- **Το επίπεδο Δικτύου** είναι υπεύθυνο για την λογική διευθυνσιοδότηση των πακέτων στο δίκτυο. Αυτό επιτυγχάνεται βασιζόμενο στην αντιστοιχία των διευθύνσεων IP σε συνδυασμό με την μάσκα υποδικτύου καθορίζει ποιες συσκευές ανήκουν στο ίδιο υποδίκτυο και ποιες όχι.

  Ουσιαστικά οι διευθύνσεις IP πληροφορούν το δρομολογητή για τον προορισμό του πακέτου. Αυτός με την σειρά του εντοπίζει την κατάλληλη διαδρομή που πρέπει να ακολουθήσει το πακέτο.

- **Στο επίπεδο των εφαρμογών** οι τερματικές συσκευές αποφασίζουν την κατάληξη των πακέτων, σε ποιες εφαρμογές αντιστοιχούν τα πακέτα και μπαίνουν σε κατάλληλη σειρά.

Χαρακτηριστική της αντιστοίχησης του μοντέλου OSI στο μοντέλο TCP/IP είναι η παρακάτω εικόνα.



2.5 Διευθύνσεις IP και υποδικτύωση

Στο πρωτόκολλο TCP/IP κάθε τερματική συσκευή διαθέτει μια μοναδική διεύθυνση που λέγεται IP.

Μία **διεύθυνση IP** (*Internet Protocol address*), είναι ένας μοναδικός αριθμός που δίνεται στις συσκευές του δικτύου με στόχο τη μεταξύ τους ταυτοποίηση και επικοινωνία σε ένα δίκτυο υπολογιστών. Στην κάθε συσκευή του δικτύου αντιστοιχεί μια και μόνο διεύθυνση. Ουσιαστικά η διεύθυνση IP είναι όπως η αστυνομική

ταυτότητα για τον άνθρωπο, είναι μοναδική και απαραίτητη για την αναγνώριση συσκευών στο δίκτυο. Βέβαια υπάρχει η δυνατότητα μια διεύθυνση IP να "μοιραστεί" σε πολλαπλές συσκευές είτε επειδή αυτές συμπεριλαμβάνονται στο ίδιο υποδίκτυο που στο σύνολο του έχει μια εξωτερική διεύθυνση IP, είτε γιατί διέρχονται από μια ενδιάμεση τερματική συσκευή που ονομάζεται proxy.

Το πρωτόκολλο IP αναλαμβάνει να διοχετεύσει τα μηνύματα πληροφοριών από τους απαιτούμενους κόμβους του δικτύου έως ότου φτάσουν στον τελικό προορισμό. Όλα τα δίκτυα που συνδέονται στο διαδίκτυο αντιλαμβάνονται το πρωτόκολλο IP με αποτέλεσμα την επιτυχή επικοινωνία και την ανταλλαγή των δεδομένων ομοιόμορφα.

Η σύνδεση των δικτύων στο διαδίκτυο(internet) γίνεται μέσω διαδικτυακών συσκευών, τους λεγόμενους δρομολογητές (routers) ή πύλες (gateways). Ένας δρομολογητής ουσιαστικά είναι μια δικτυακή συσκευή που ενώνει είτε δυο είτε παραπάνω δίκτυα, ασχέτως αν είναι ίδιου τύπου ή όχι με αποτέλεσμα να συμπεριλαμβάνεται ταυτόχρονα σε περισσότερα από ένα δίκτυα.

Οι δρομολογητές είναι υπεύθυνοι για την αποστολή πακέτων διάμεσου των υποδικτύων που αποτελούν το internet μέχρι να φτάσουν στον τελικό παραλήπτη.

Μια διεύθυνση IP περιέχει 4 συστοιχίες δεκαδικών αριθμών χωρισμένους με τελείες, λ.χ. ένας υπολογιστής μπορεί να έχει την διεύθυνση 192.168.1.1

Ουσιαστικά μία IP διεύθυνση είναι ένας δυαδικός αριθμός 32-bit που για να γίνει ευκολονόητος, τον χωρίζουμε σε 4 συστοιχίες των 8 bit και εν συνεχεία κάθε συστοιχία αντιστοιχεί στον ανάλογο δεκαδικό αριθμό.

Μια διεύθυνση IP αποτελείται από δύο κομμάτια πληροφορίας:

- Στο πρώτο κομμάτι είναι ο αριθμός δικτύου στο οποίο αντιστοιχεί η κάθε συσκευή.
- Το δεύτερο κομμάτι είναι ο αριθμός των χρηστών. Απαραίτητη προϋπόθεση για να γνωρίζουμε τον αριθμό των χρηστών είναι η μάσκα υποδικτύου (subnet mask). Με τον όρο μάσκα υποδικτύου ονομάζουμε ένα 32 bit δυαδικό αριθμό όπου έχει μονάδες στην περιοχή του δικτύου και μηδέν στην περιοχή των χρηστών Π.χ. μια subnet mask είναι η παρακάτω:

1111111 1111111 00000000 00000000 =255.255.0.0

Συνηθίζεται να γράφουμε μια μάσκα και με ένα απλό αριθμό που είναι ο αριθμός απλά των μονάδων. Π.χ. στην παραπάνω μάσκα είναι το 24.

Έτσι η διεύθυνση 192.168.1.10/24 έχει τμήμα δικτύου το 192.168.1.0 και το 10 στο τέλος είναι οι χρήστες.

Τα δίκτυα που αποτελούν το διαδίκτυο χωρίζονται σε 3 τάξεις (classes) ανάλογα με το μέγεθός τους, δηλ. με βάση το σύνολο των χρηστών τους:

- τάξη A (μεγάλα)
- τάξη B (μεσαία)
- τάξη C (μικρά)

Σε κάθε τάξη έχουμε τα παρακάτω :

και 1*254 (254) μέγιστο αριθμό υπολογιστών ανά δίκτυο. Όπως φαίνεται και στον παρακάτω πίνακα.

Τάξη δικτύου	**Πρώτος αριθμός της διεύθυνσης IP**	**Μάσκα**	**Αριθμός Host**
A	1 έως 126	255.0.0.0	254 x 254 x 254 = 16387064
B	128 έως 191	255.255.0.0	254 x 254 = 64516
C	192 έως 223	255.255.255.0	254

Οποιοδήποτε επιθυμεί να συνδεθεί στο διαδίκτυο λαμβάνει μια IP address από κάποια εταιρεία που έχει ως ασχολία της τον καταμερισμό των διευθύνσεων IP στο διαδίκτυο με σκοπό να βεβαιώνεται ότι πρόκειται για μια και μοναδική.

Σε κάθε δίκτυο ή υποδίκτυο βρίσκουμε κάποιες δεσμευμένες διευθύνσεις, δηλαδή δεν έχουν την δυνατότητα να δοθούν αντίστοιχα σε συσκευές. Και πρόκειται για τις :

- **network address**,στην οποία όλα τα bit που προορίζονται για τους χρήστες είναι 0 (π.χ. η 192.168.1.0 είναι η IP διεύθυνση του δικτύου που περιέχει τον host 192.168.1.5)

- **broadcast address**, στην οποία όλα τα bit που προορίζονται για τα υποδίκτυα είναι 1 (π.χ. η 192.168.1.255 είναι η broadcast διεύθυνση του δικτύου 192.168.1.0)

Οι εναπομείνασες διευθύνσεις έχουν την δυνατότητα να δοθούν στις συσκευές του δικτύου.

Επίσης υπάρχουν ακόμα τρία σύνολα IP διευθύνσεων εντεταλμένα για προσωπική χρήση:

- Class A: 10.0.0.0 έως 10.255.255.255
- Class B: 172.16.0.0 έως 172.31.255.255
- Class C: 192.168.0.0 έως 192.168.255.255

Η μάσκα υποδικτύου παρέχει την δυνατότητα σε μια δικτυακή συσκευή να ξεχωρίζει σε μια IP διεύθυνση ποιο κομμάτι αφορά το δίκτυο και υποδίκτυο και ποιο το κομμάτι των χρηστών. Με τον όρο μάσκα υποδικτύου ονομάζουμε ένα 32 bit δυαδικό αριθμό όπου έχει μονάδες στην περιοχή του δικτύου και μηδέν στην περιοχή των χρηστών. Στον παρακάτω πίνακα διακρίνονται οι default μάσκες ανάλογα με τις κλάσεις.

ΚΛΑΣΗ	DEFAULT MASK (δυαδική μορφή)	DEFAULT MASK
A	11111111.00000000.00000000.00000000	255.0.0.0 ή /8
B	11111111.11111111.00000000.00000000	255.255.0.0 ή /16
C	11111111.11111111.11111111.00000000	255.255.255.0 ή /24

Υποδικτύωση (subnetting)

Μπορούμε να χρησιμοποιήσουμε και ελεύθερα τις μάσκες μας και τα IP ώστε να κάνουμε υποδικτύωση σύμφωνα με τις ανάγκες μας.

Ένα παράδειγμα είναι το παρακάτω:

Έστω ότι έχουμε ένα δίκτυο με βάση την διεύθυνση IP 192.168.0.0 και έχουμε τις παρακάτω απαιτήσεις:

A υποδίκτυο: 20 host

B υποδίκτυο: 60 host

C υποδίκτυο: 20 host

D υποδίκτυο 100 host

Τότε μπορούμε να υποδικτυώσουμε μόνο με τις συγκεκριμένες απαιτήσεις χωρίς να σπαταλούμε διευθύνσεις αν επιλέγαμε την χρήση των τάξεων.

Αρχικά ταξινομούμε τα δίκτυα από το μεγαλύτερο στο μικρότερο αριθμό host και παίρνουμε το πρώτο μεγαλύτερο δυαδικό αριθμό για τον αριθμό των host. Έτσι έχουμε:

Δίκτυο	Host	Αριθμός Διαθέσιμων IP	Αριθμός bit που χρειάζονται για τα host
D	100	128	7
B	60	64	6
A	20	32	5
C	20	32	5

Ο αριθμός των bit που χρειάζονται για τα host μας έχει καθορίσει το μέρος με μηδέν που πρέπει να έχει η subnet mask. Επίσης ξεκινάμε από την αρχική διεύθυνση IP η οποία είναι η διεύθυνση του $1^{ου}$ υποδικτύου και προσθέτοντας κάθε φορά τον αριθμό των διαθέσιμων IP προκύπτουν οι διευθύνσεις IP των άλλων δικτύων.

Έπίσης πρέπει να λάβουμε υπόψη μας ότι σε κάθε δίκτυο έχουμε την διεύθυνση δικτύου και διεύθυνση broadcast (η τελευταία διεύθυνση IP του δικτύου) που δεν μπορούν να διατεθούν σε hosts. Άρα παίρνουμε τον παρακάτω πίνακα:

Δίκτυο	Host	Αριθμός	Subnet Mask	Αριθμός	Net Address	First Address	Last Address	Broadcast

		IP		Διαθέσιμων Host				
D	100	128	255.255.255.128	126	192.168.0.0	192.168.0.1	192.168.0.126	192.168.0.127
B	60	64	255.255.255.192	62	192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
A	20	32	255.255.255.224	30	192.168.0.192	192.168.0.193	192.168.0.222	192.168.0.223
C	20	32	255.255.255.224	30	192.168.0.224	192.168.0.225	192.168.0.254	192.168.0.255

Όταν έχουμε τον παραπάνω πίνακα τότε έχουμε μια πλήρη εικόνα του κάθε υποδικτύου.

2.6 Διευθύνσεις IPv6

Το πρωτόκολλο IPv6 αποτελεί αναθεώρηση του πρωτοκόλλου IPv4. Το IPv6 αναπτύχθηκε από τον οργανισμό Internet Engineering Task Force, (IETF), με στόχο να αντιμετωπίσει το πρόβλημα της εξάντλησης των διευθύνσεων του IPv4.Ο λόγος είναι ότι κάθε συσκευή στο διαδίκτυο αποδίδεται μία Διεύθυνση IP

Όμως οι συσκευές που συνδέονται στο διαδίκτυο αυξάνουν συνεχώς και έτσι, παρουσιάστηκε η ανάγκη περισσοτέρων διευθύνσεων, από αυτές που μπορεί να δώσει το IPv4. Το IPv6 χρησιμοποιεί διευθύνσεις 128 bit, το οποίο επιτρέπει δηλαδή 3.4×10^38 διαφορετικές διευθύνσεις.

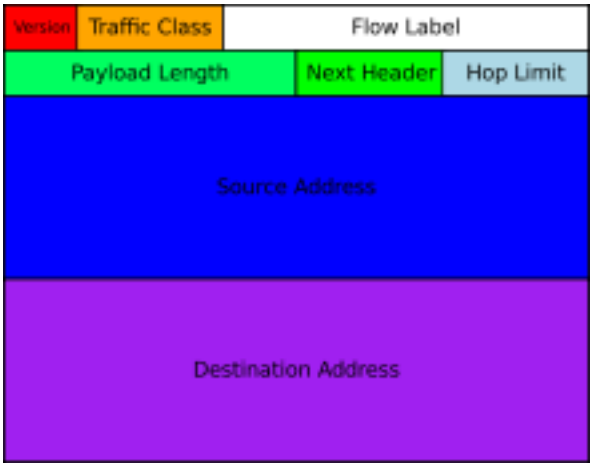
Το πρωτόκολλο IPv6 έχει την δυνατότητα να μπορεί να συνεργαστεί με το IPv4, οπότε το πέρασμα στο IPv6 γίνεται σταδιακά και όχι βίαια. Οι διευθύνσεις IP του πρωτοκόλλου IPv6, απαρτίζονται από 8 ομάδες των τεσσάρων δεκαεξαδικών ψηφίων, χωρισμένων με άνω και κάτω τελεία, π.χ 2001:0ab8:85b3:0042:1000:8a2e:0370:7234.

Ένα πακέτο IPv6 συντίθεται από δυο μέρη. Την επικεφαλίδα και τα δεδομένα, η επικεφαλίδα αποτελείται από ένα σταθερό τμήμα με την μικρότερη λειτουργικότητα που είναι όμως αναγκαία για όλα τα πακέτα και μπορεί να ακολουθείται από εκούσιες επεκτάσεις, που πραγματοποιούν εξειδικευμένα χαρακτηριστικά.

Το σταθερό μέρος της επικεφαλίδας κατέχει τις πρώτες 40 οκτάδες του πακέτου. Η επικεφαλίδα περιέχει διευθύνσεις αφετηρίας και προορισμού, καθώς και το είδος της

διάδοσης, επίσης τον μετρητή αλμάτων, και το είδος των προαιρετικών επιλογών ή των δεδομένων που ακολουθούν την επικεφαλίδα.

Το πεδίο επόμενη επικεφαλίδα (Next Header) πληροφορεί των αποδέκτη πώς να μεταφράσει τα δεδομένα που ακολουθούν την επικεφαλίδα.



Έτσι το IPv6, σε σύγκριση με το IPv4 έχει σαν πλεονέκτημα το μεγαλύτερο χώρος διευθύνσεων. Οι IPv6 διευθύνσεις, χρησιμοποιούν οκτώ ομάδες των τεσσάρων δεκαεξαδικών ψηφίων. Ουσιαστικά μια IPv6 διεύθυνση αναπαρίστανται με οκτώ ομάδες των 16 bits η κάθε μία. Η κάθε ομάδα 16 bits δίνεται σαν δεκαεξαδικός αριθμός με 4 ψηφία και οι ομάδες χωρίζονται με άνω-κάτω τελεία (:).

Π.χ. έχουμε τη διεύθυνση 2001:0ab9:0000:0000:0000:fe00:0041:8080. Επειδή μια διεύθυνση IPv6 είναι αρκετά μεγάλη μπορεί να συντομευτεί με εφαρμογή των παρακάτω κανόνων:

Ένα ή περισσότερα μπροστινά μηδενικά σε οποιαδήποτε από τις οκτώ ομάδες μπορούν να διαγραφούν. Π.χ. αν έχουμε σε μια ομάδα το 0012 συντομεύεται σε 12. Ακόμα αν έχουμε μηδενικές ομάδες (δηλαδή 0000) μπορούν να αντικατασταθούν με διπλή άνω-κάτω τελεία (::).

Π.χ. έχουμε την διεύθυνση:

2001:0ab8:74a2:0000:0000:8a2a:0370:1835.

Τότε γράφεται σαν

2001:ab8:74a3:::8a2e:8a2e:1835

Αν πάλι έχουμε τη διεύθυνση 0000:0000:0000:0000:0000:0000:0000:0001, γράφεται σαν ::1.

ΚΕΦΑΛΑΙΟ 3: ΔΡΟΜΟΛΟΓΗΣΗ

3.1 Τι είναι δρομολόγηση

Ως δρομολόγηση ορίζουμε ουσιαστικά την μεταφορά μηνυμάτων από ένα κόμβο σε έναν άλλο. Από την άλλη μεριά ως κόμβο ορίζουμε κάθε συσκευή που υπάρχει στο δίκτυο μας όπως υπολογιστές, routers, κινητά, tablets, switches, access points κ.α.

Κάθε μήνυμα λοιπόν έχει μία προκαθορισμένη διαδρομή με τον κόμβο πηγή ως αφετηρία και τον κόμβο προορισμού ως σημείο τερματισμού. Τις περισσότερες φορές υπάρχει πλήθος διαδρομών που μπορεί να ακολουθήσει ένα πακέτο για να καταφέρει να φτάσει στον προορισμό του. Οπότε το ζητούμενο είναι να βρούμε την πιο σύντομη διαδρομή, η οποία όμως θα παρέχει και ασφάλεια. Η ανακάλυψη της καλύτερης διαδρομής αποτελεί λοιπόν το αποτέλεσμα της δρομολόγησης.

Σε ένα δίκτυο υπολογιστών το να δρομολογούνται πακέτα ανάμεσα σε κόμβους αποτελεί μία από τις βασικότερες λειτουργίες αυτού του δικτύου. Ένα δίκτυο ως επί το πλείστον χωρίζεται σε υποδίκτυα από όπου τα μηνύματα χρειάζονται περισσότερα βήματα μέχρι να καταλήξουν στον κόμβο προορισμού. Εξαίρεση σε όλα αυτά αποτελούν τα δίκτυα εκπομπής, όμως και πάλι η δρομολόγηση θα γινόταν δύσκολα αν πηγή και προορισμός δεν ανήκαν στο ίδιο δίκτυο.

Η εύρεση της κατάλληλης διαδρομής γίνεται μέσω αλγορίθμων που έχουν αυτό το στόχο, δηλαδή να εντοπίσουν την πιο σύντομη και ασφαλή διαδρομή που θα ακολουθήσουν τα πακέτα.

Τα σημερινά δίκτυα με ποσοστό που αγγίζει το 98% συναντούν τις προδιαγραφές που προσφέρει το μοντέλο TCP-IP.

3.2 Στατική Δρομολόγηση

Η στατική δρομολόγηση μας δίνει την δυνατότητα να προαποφασίσουμε ποιο μονοπάτι θα ακολουθήσει το μήνυμα για να φτάσει στον προορισμό του, με αποτέλεσμα να μην ποικίλει ανάλογα με τα διάφορα χαρακτηριστικά αλλά να είναι αναγκασμένο να ακολουθήσει την διαδρομή που έχει απαιτήσει ο διαχειριστής του δικτύου.

Θα μπορούσαμε να χρησιμοποιήσουμε την στατική δρομολόγηση είτε για την ασφάλεια του πακέτου, όπου ως διαχειριστές έχουμε την δυνατότητα να προκαθορίσουμε την διαδρομή του, είτε σε μικρά δίκτυα στα οποία δεν τίθεται θέμα πολυπλοκότητας, είτε σε περίπτωση που η δρομολόγηση δεν προγραμματίζεται μέσω κάποιου αλγορίθμου αλλά από κάποια συγκεκριμένη λογική του διαχειριστή του δικτύου.

Σε δίκτυα που υπάρχει τόσο στατική, όσο και δυναμική δρομολόγηση, η στατική είναι εκείνη που πάντα προηγείται.

3.3 Δυναμική Δρομολόγηση

Η δυναμική δρομολόγηση πραγματεύεται την αυτόματη κατασκευή του πίνακα δρομολόγησης σε κάθε router. Για να καταστεί αυτό εφικτό, χρησιμοποιούμε διάφορους αλγορίθμους δρομολόγησης που είναι ικανοί να εξερευνήσουν το δίκτυο και να βρουν τις διάφορες διαδρομές που διαθέτει ένα μήνυμα ώστε να ακολουθήσει και να μεταβεί από ένα σημείο του δικτύου σε ένα άλλο.

Ακόμα, αν μια διαδρομή δεν μπορεί να ακολουθηθεί πια, οι κόμβοι είναι αυτοί που θα χαράξουν μια διαφορετική διαδρομή που θα χρησιμοποιηθεί για να φτάσει το πακέτο στο σημείο προορισμού.

Αυτό συνήθως καθίσταται δυνατό μέσω των πρωτοκόλλων δρομολόγησης. Τα πρωτόκολλα χρησιμοποιούν είτε αλγόριθμους διανύσματος απόστασης, είτε αλγόριθμους κατάστασης συνδέσμων, οι οποίοι περιέχουν κάθε αλγόριθμο που υπάρχει στο διαδίκτυο.

3.4 Link State Αλγόριθμοι Δρομολόγησης

Όταν εφαρμόζουμε αλγόριθμους κατάστασης συνδέσμων, η κάθε δικτυακή συσκευή αρχικά δημιουργεί έναν χάρτη του δικτύου με την μορφή γράφου. Για να καταστεί αυτό εφικτό , κάθε δικτυακή συσκευή διαχέει το δίκτυο με δεδομένα

(μηνύματα broadcast) που αφορούν την τοπολογία του δικτύου, κάθε συσκευή διαβάζει τα μηνύματα και αφού έχει συγκεντρώσει όλες τις πληροφορίες που είναι απαραίτητες δημιουργεί τον χάρτη. Με βάση αυτόν τον χάρτη ο δρομολογητής είναι σε θέση να επιλέξει την βέλτιστη διαδρομή από αυτόν προς τους υπόλοιπους δρομολογητές.

Ο αλγόριθμος Dijkstra είναι εκείνος που επιλέγεται ως επί το πλείστον για την εύρεση της συντομότερη διαδρομής.

Με τον όρο 'συντομότερη' δεν εννοούμε απαρέγκλιτα φυσική απόσταση, αλλά οποιοδήποτε κριτήριο, το οποίο μπορεί να διαφέρει από πρωτόκολλο σε πρωτόκολλο. Ανάλογα με το πρωτόκολλο δρομολόγησης είναι πιθανό το κριτήριο απόστασης να τροποποιείται και να πραγματεύεται τη μέση καθυστέρηση μετάδοσης(delay) ή τον αριθμό των αλμάτων που απαιτεί μέχρι να φτάσει στον τελικό παραλήπτη(hop count) ή το εύρος ζώνης(bandwidth) κλπ. Ουσιαστικά, προσμετρώνται (βάσει ενός κριτήριου) οι αποστάσεις από κάθε router προς τους γειτονικούς του.

Ο αλγόριθμος Dijkstra είναι σε θέση να επιλέξει την βέλτιστη διαδρομή με την δημιουργία ενός δέντρου, με τον επιλεγμένο δρομολογητή σαν ρίζα του δέντρου, που μέσα του βρίσκονται όλοι οι υπόλοιποι δρομολογητές του δικτύου. Αρχικά το δέντρο περιέχει μόνο τον εαυτό του. Εν συνεχεία , προσθέτοντας κάθε φορά και από έναν από το σύνολο των δρομολογητών που δεν έχουν προστεθεί στο δέντρο, προσθέτει τον κόμβο που έχει το ελάχιστο κόστος για να προσεγγίσει έναν διπλανό δρομολογητή. Αυτή η διαδικασία θα συνεχιστεί έως ότου όλοι οι κόμβοι να εμπεριέχονται στο δέντρο.

Το γράφημα του δέντρου βοηθά στην κατανόηση όσον αφορά την κατασκευή του πίνακα δρομολόγησης του κάθε router, υποδεικνύοντας το κατάλληλο επόμενο βήμα (hop), ώστε με αφετηρία τον ίδιο να είναι σε θέση να επικοινωνεί με οποιοδήποτε router στο δίκτυο.

3.5 Distance-Vector Αλγόριθμοι Δρομολόγησης

Οι 'αλγόριθμοι διανυσμάτων απόστασης' εκμεταλλεύονται τον αλγόριθμο Bellman-Ford. Αυτή η διαδικασία θέτει το κόστος, σε κάθε μία από τις συνδέσεις μεταξύ των δρομολογητών στο δίκτυο. Οι δρομολογητές αποστέλλουν πακέτα πληροφοριών από ένα σημείο σε ένα άλλο χρησιμοποιώντας τη διαδρομή με το ελάχιστο αθροιστικό κόστος .

Η λειτουργία του αλγορίθμου κρίνεται ως πολύ απλή. Κάθε φορά που αρχίζει ένας κόμβος την λειτουργία του γνωρίζει τους άμεσα συνδεδεμένους με αυτόν κόμβους, καθώς και τον επόμενο κόμβο (hop) και το κόστος που θα χρειαστεί για να τους προσεγγίσει, δεδομένα δηλαδή που είναι απαραίτητα για την δημιουργία του πίνακα δρομολόγησης. Καθήκον του κάθε κόμβου είναι να αποστέλλει στους γειτονικούς κόμβους σε τακτά χρονικά διαστήματα την δική του προσέγγιση όσον αφορά το κόστος που απαιτείται μέχρι και τον τελικό προορισμό .Αφού οι γειτονικοί κόμβοι λάβουν αυτές τις πληροφορίες, είναι πλέον σε θέση να τις αναλύσουν και οτιδήποτε παρουσιάζεται βελτιωμένο σχετικά με αυτά που εκείνοι γνωρίζουν το εναποθέτουν στον δικό τους πίνακα αποστάσεων. Τελικά, όλοι οι δρομολογητές του δικτύου θα μπορούν να βρουν το βέλτιστο επόμενο βήμα (hop) για το σύνολο των προορισμών και το βέλτιστο συνολικό κόστος.

Τα πρωτόκολλα που χρησιμοποιούν τον αλγόριθμο διανυσμάτων απόστασης είναι το RIP και το OSPF.

3.6 Βασικοί Αλγόριθμοι Δρομολόγησης

Ο αλγόριθμος του Dijkstra

Αφορά έναν αλγόριθμο εύρεσης συντομότερων διαδρομών (single-source shortest path problem) από συγκεκριμένη αφετηρία σε έναν (κατευθυνόμενο ή μη) γράφο με μη αρνητικά βάρη στις ακμές. Σε κάθε βήμα ξεχωρίζει την τοπικά βέλτιστη λύση, μέχρις ότου στο τελικό στάδιο προβάλλει μια συνολικά βέλτιστη λύση. Για την σωστή λειτουργία του αλγόριθμου ο γράφος θα πρέπει να περιέχει μόνο θετικές τιμές , σε αντίθετη περίπτωση, δίνει εσφαλμένο αποτέλεσμα. Σε περίπτωση που έχουμε να αντιμετωπίσουμε γράφους οι οποίοι διαθέτουν αρνητικά βάρη στις ακμές, η

καλύτερη λύση θα ήταν να θέσουμε σε ισχύ διαφορετικούς αλγόριθμους, όπως αυτός των Bellman- Ford.

Ο αλγόριθμος του Dijkstra θεωρείται αξιωματικά ως ένας από τους πιο αναγνωρίσιμους και αυτός είναι και ο λόγος που εφαρμόζεται σε πολλά πρωτόκολλα, όπως το OSPF.

Πιο συγκεκριμένα ο αλγόριθμος Dijkstra ακολουθεί τα παρακάτω βήματα:

Βήμα 1. Σημειώνει σε κάθε κόμβο μια ετικέτα απόστασης (d[*]) με τιμή 0 στον αρχικό κόμβο και τιμή άπειρο σε όλους τους υπόλοιπους. Επίσης, σημειώνει μια ετικέτα προηγούμενου κόμβου (prev[*]) και βάζει της την κενή τιμή για όλους τους κόμβους. Η ετικέτα αυτή θεωρείται αναγκαία για να υπολογίσει την τελική διαδρομή που ψάχνει.

Βήμα 2. Σημειώνει όλους τους κόμβους μη-επεξεργασμένους. Ο τρέχων κόμβος είναι ο αρχικός.

Βήμα 3. Για τον τρέχων κόμβο, εξετάζει όλους τους μη-επεξεργασμένους γείτονές του και υπολογίζει το συνολικό άθροισμα απόστασής τους από τον αρχικό κόμβο. Εφόσον η απόσταση δεν είναι μεγαλύτερη από την ετικέτα απόστασης που είχε καταγραφεί, μετατρέπεται στη νέα τιμή που υπολογίστηκε και καταγράφει τον τωρινό κόμβο στην ετικέτα προηγούμενου.

Βήμα 4. Αφού εξετάσει όλους τους γείτονες του τωρινού κόμβου, τότε θα σημειωθεί ότι έχει ήδη επεξεργαστεί. Ο αλγόριθμος δεν θα προχωρήσει σε επανεξέταση ενός κόμβου που έχει επεξεργαστεί στο παρελθόν. Η καταγεγραμμένη απόσταση πλέον θεωρείται η ελάχιστη και δεν θα προβεί σε καμία αλλαγή.

Βήμα 5. Ο κόμβος που θα αναλάβει να τρέξει ο αλγόριθμος θα θεωρηθεί μη-επεξεργασμένος και θα διαθέτει την ελάχιστη απόσταση.

Βήμα 6. Από τη στιγμή που θα έχει γίνει η επεξεργασία όλων των κόμβων, ο αλγόριθμος πρέπει να συνεχίσει στο επόμενο βήμα αλλιώτικα να επιστρέψει στο βήμα 3.

Βήμα 7. Στο τελευταίο βήμα αφού θα ξεκινήσει από τον κόμβο- προορισμό, στη συνέχεια θα προβεί στην εκτύπωση της ετικέτας του προηγούμενου κόμβου.

Belman-Ford ή Ford-Fulkerson Algorithm

Σε περιπτώσεις που ο γράφος εμπεριέχει ακμές με αρνητικά και θετικά βάρη και με σκοπό την εύρεση βέλτιστης διαδρομής από έναν αρχικό κόμβο σε ένα τελικό, χρησιμοποιούμε τον αλγόριθμο Bellman - Ford. Ο αλγόριθμος παρέχει μια λογική τιμή, η οποία μας δείχνει εάν υπάρχει ή όχι ένας αρνητικού προσήμου κύκλος στο γράφο που έχει προσβασιμότητα από τον αρχικό κόμβο. Στην περίπτωση που στο αποτέλεσμα υπάρχει κύκλος αρνητικού βάρους συμπεραίνουμε ότι το πρόβλημα δεν διαθέτει λύση.

Σε αντίθετη περίπτωση εάν δηλαδή δεν εξάγει αρνητικό αποτέλεσμα, τότε ο αλγόριθμος παραθέτει τις βέλτιστες διαδρομές και το αντίστοιχο κόστος.

3.7 Πίνακες δρομολόγησης

Κάθε δικτυακή συσκευή δημιουργεί τον δικό της πίνακα δρομολόγησης ο οποίος αποθηκεύεται στη μνήμη των συσκευών αυτών και παρέχει πληροφορίες για οποιουσδήποτε προορισμούς. Ο πίνακας δρομολόγησης είναι υπεύθυνος να αντιστοιχήσει τις διευθύνσεις IP του παραλήπτη με τις διεπαφές εξόδου (interface) που κατέχει και οι οποίες αντιστοιχούν στην διεύθυνση του επόμενου βήματος.

Μπορεί να καταστεί σαφές ότι είναι αδύνατον οι πίνακες δρομολόγησης κάθε συσκευής να εμπεριέχουν πληροφορίες για κάθε προορισμό του κόσμου. Αρκεί να αντιληφθεί κανείς τον αριθμό των δικτυακών συσκευών που απαρτίζουν το διαδίκτυο για να καταλάβει ότι μία κεντρική διαχείριση θα ήταν αδύνατη, οπότε η κατάτμηση σε μικρότερα δίκτυα αθροίζοντας μαζί και την αρχή περί ιδιωτικής ασφάλειας πληροφοριών μπορεί να θεωρηθεί μονόδρομος. Με λίγα λόγια κάθε συσκευή είναι υπεύθυνη να κάνει μόνο ένα συγκεκριμένο κομμάτι της δουλειάς συλλέγοντας μόνο τοπικές πληροφορίες. Βοήθεια μας προσφέρει το γεγονός ότι οι διευθύνσεις του διαδικτύου κατανέμονται βάσει ιεραρχίας και έχει παρατηρηθεί ότι με αυτό τον τρόπο μπορούμε να εξάγουμε το συμπέρασμα αν ακολουθείται άμεση δρομολόγηση ή όχι. Κατά τον ίδιο τρόπο οι διευθύνσεις που δομούνται ιεραρχικά επιτρέπει να χρησιμοποιούν στους πίνακες δρομολόγησης μόνο το πρόθεμα με αποτέλεσμα να ελαττώνουν σημαντικά το μέγεθος τους. Ουσιαστικά αποτρέπεται η συλλογή λεπτομερειών για τις συσκευές κάθε υποδικτύου, εξαιρουμένων των περιπτώσεων

που οι συσκευές ανήκουν σε ένα δίκτυο με την εκτελούσα την δρομολόγηση συσκευή.

Κάθε δρομολογητής γνωρίζει πληροφορίες μόνο για τον επόμενο κόμβο δρομολόγησης χωρίς να ενδιαφέρεται για τα περαιτέρω βήματα που χρειάζονται μέχρις ότου φτάσουν τα πακέτα στον τελικό παραλήπτη.

3.8 Πρωτόκολλο Δρομολόγησης RIP

Αποστέλλει μηνύματα πληροφορίας που αφορούν την τοπολογία (routing update) κάθε 30 δευτερόλεπτα ή εφόσον υπάρξει μετατροπή στην τοπολογία του δικτύου αποστέλλει μηνύματα με σκοπό να ενημερώσει τους κόμβους του δικτύου για τις τρέχουσες αλλαγές. Το RIP σαν παράμετρο μέτρησης της απόστασης ενεργεί με βάση των αριθμό αλμάτων μεταξύ των κόμβων του δικτύου, δηλαδή μετράει πόσα άλματα θα χρειαστούν ώστε να προσεγγίσει τον τελικό παραλήπτη, έχοντας ως μέγιστο αριθμό τα 15 άλματα.

Συνεπώς η τοπολογία του δικτύου απαγορεύεται να ξεπερνά τα 15 άλματα μέχρι τον τελικό παραλήπτη, ενώ σε αντίθετη περίπτωση θα θεωρηθεί μη προσβάσιμος. Χρησιμοποιεί ένα χρονομετρητή (timeout) ανά 30 δευτερόλεπτα για κάθε διαδρομή που γνωρίζει. Μετά το πέρας αυτού του χρόνου μαρκάρει το μονοπάτι ως μη προσβάσιμο. Αυτό συνεπάγεται ότι το συγκεκριμένο μονοπάτι δεν θα υπάρχει πλέον στους πίνακες δρομολόγησης.

Το πρωτόκολλο RIP κάνει χρήση του αλγόριθμου διανύσματος απόστασης και είναι ιδανικό για να λειτουργήσουν μικρού μεγέθους δίκτυα. Δημιουργεί πίνακες οι οποίοι παρέχουν τα δεδομένα που αφορούν το μονοπάτι και την παράμετρο μέτρησης της απόστασης προς οποιοδήποτε προορισμό.

Τροχοπέδη αποτελεί το γεγονός ότι όσο το δίκτυο αυξάνεται, ο όγκος των πληροφοριών που συχνά ανταλλάσσουν οι δρομολογητές μεταξύ τους αυξάνεται και αυτός με αποτέλεσμα τον περιορισμό του διαθέσιμου εύρους ζώνης και την αύξηση του χρόνου σύγκλισης. Ως χρόνο σύγκλισης ορίζουμε τον χρόνο που απαιτείται έως ότου όλοι οι δρομολογητές να ενημερωθούν για τυχόν αλλαγές στην τοπολογία του δικτύου.

Κάθε φορά που υπάρχουν κάποιες αλλαγές στην τοπολογία του δικτύου ΄΄τρέχει΄΄ ο αλγόριθμος δρομολόγησης και παγώνει η μεταφορά των δεδομένων ανάμεσα στους

δρομολογητές γιατί δεν έχει γνωστοποιηθεί ακόμα σε όλους τους δρομολογητές ποιες είναι αυτές οι αλλαγές.

Οπότε όσο πιο άμεσα γνωστοποιηθούν οι αλλαγές, τόσο πιο άμεσα θα επανέλθει το δίκτυο στην εύρυθμη λειτουργία του.

Υπάρχουν δυο εκδόσεις του πρωτόκολλου RIP:

- η έκδοση RIP v1, στην οποία δεν γίνεται η αποστολή της μάσκας υποδικτύου (subnet mask) μαζί με τους πίνακες δρομολόγησης . Όλα τα δίκτυα πρέπει να έχουν τη προκαθορισμένη μάσκα ανάλογα με την κλάση που ανήκουν. (clasful routing).
- η έκδοση RIP v2, στην οποία αποστέλλονται οι πίνακες δρομολόγησης και ταυτόχρονα η μάσκα υποδικτύου (clasles routing)

Για να ενεργοποιήσουμε Rip σε ένα Router της CISCO κάνουμε τα παρακάτω:

	Command
Step 1	`Router(config)# router rip`
Step 2	`Router(config-router)# network ip-address`

3.9 Πρωτόκολλο Δρομολόγησης EIGRP

Το EIGRP (Enhanced Interior Gateway Routing Protocol) αποτελεί πρωτόκολλο δρομολόγησης δικτύων, που έχει αναπτυχθεί από την εταιρεία Cisco Systems, και βασίζεται στο προγενέστερο πρωτόκολλο IGRP.

Τοποθετείται στην ομάδα των πρωτοκόλλων Διανύσματος απόστασης (Distance Vector), και είναι βελτιωμένο ως προς τον εκμηδενισμό της αστάθειας που δημιουργείται σε ένα δίκτυο όταν μετατρέπεται η τοπολογία του, καθώς και στην καλύτερη διαχείριση του εύρους ζώνης του εκάστοτε δικτύου.

Η πλειονότητα αυτών των δυνατοτήτων συντάσσουν μέρος της σύστασης του αλγορίθμου DUAL, ο οποίος δημιουργήθηκε από την SRI International. Ο αλγόριθμος αυτός βεβαιώνει ότι δεν θα υπάρξουν βρόχοι κατά την διαδικασία της

δρομολόγησης καθώς και την τήρηση εναλλακτικών δρομολογίων για κάθε δίκτυο σε περίπτωση βλάβης των ήδη υπαρχόντων δρομολογίων.

Προτεραιότητα του πρωτοκόλλου EIGRP είναι η επίτευξη της γειτνίασης ανάμεσα στους άμεσα συνδεδεμένους δρομολογητές. Αυτό επιτυγχάνεται διαμέσου μηνυμάτων Hello, τα οποία αποστέλλονται συχνά μεταξύ των γειτονικών δρομολογητών.

Το EIGRP κάνει τις καταχωρήσεις για το υπόλοιπο δίκτυο και την δομή του, σε τρεις λίστες.

- Neighbor Table
- Topology Table
- Route States

Τα tables αυτά, το πρωτόκολλο EIGRP τα καταχωρεί στην μνήμη RAM του router ώστε να μπορεί να έχει γρήγορη και άμεση πρόσβαση του σε αυτά.

- **Neighbor Table**

Κάθε δρομολογητής διατηρεί πακέτα πληροφοριών για τους άμεσους γείτονες. Όταν ανακαλύπτονται καινούργιοι γείτονες, η διεύθυνση και η διεπαφή του γείτονα καταγράφεται. Αυτή η πληροφορία αποθηκεύεται στην βάση πληροφοριών των γειτόνων. Ο πίνακας γειτνίασης διατηρεί αυτές τις εισαγωγές. Όταν ένας γείτονας στέλνει ένα μήνυμα Hello, ενημερώνει για τον χρόνο αναμονής. Ως χρόνο αναμονής ονομάζουμε την χρονική περίοδο που ο δρομολογητής συμπεριφέρεται σε έναν γείτονα σαν προσβάσιμο και λειτουργικό. Αντίθετος, αν ένας δρομολογητής δεν πάρει μήνυμα Hello από έναν γείτονα μέσα στον καθορισμένο χρόνο αναμονής, τότε θεωρεί τον γείτονα ως μη λειτουργικό και ενημερώνει τον αλγόριθμος DUAL για την αλλαγή στην τοπολογία.

Ο πίνακας γειτνίασης περιέχει ακόμα πληροφορίες που απαιτούνται από τον μηχανισμό αξιοπιστίας μεταφοράς. Ο αριθμός ακολουθίας (Sequence number) χρησιμοποιείται για να παρέχει αναγνώριση στα πακέτα δεδομένων. Ο τελευταίος

Sequence number που παραλαμβάνεται από τον γείτονα καταγράφεται με σκοπό να μπορούν να ανιχνευτούν εξωτερικά πακέτα. Μια λίστα μετάδοσης χρησιμοποιείται για να ταξινομεί την προτεραιότητα των πακέτων σε περίπτωση που γίνει αναμετάδοση. Ο χρόνος μέχρι να ολοκληρωθεί η μετάδοση υπολογίζεται και φυλάσσεται στην βάση δεδομένων των γειτόνων για να μπορεί να υπολογιστεί και ο χρόνος που θα χρειαστεί για την αναμετάδοση.

- **Topology Table**

Το topology table παρέχει όλους τους προορισμούς που διαφημίζονται από τους γειτονικούς δρομολογητές. Αλληλοεπιδρώντας με όλες τις εισαγωγές μεταξύ της διεύθυνσης προορισμού και της λίστας των γειτόνων που έχουν διαφημίσει τους προορισμούς. Για κάθε γείτονα καταγράφεται το διαφημιζόμενο απαιτούμενο κόστος (metric). Το metric αποθηκεύεται επίσης στον πίνακα δρομολόγησης του κάθε δρομολογητή. Αν ο γείτονας διαφημίζει αυτόν τον προορισμό πρέπει να χρησιμοποιεί αυτή την διαδρομή για να προωθήσει τα πακέτα. Αυτός είναι ένας σημαντικός κανόνας που τα πρωτόκολλα διανύσματος απόστασης (distance vector) πρέπει να ακολουθούν.

Επίσης , σε αντιστοιχία με τον προορισμό βρίσκεται και το metric που χρησιμοποιεί ο δρομολογητής για να φτιάσει στον προορισμό. Αυτό είναι το άθροισμα του καλύτερου διαφημιζόμενου metric με το κόστος της γραμμής προς αυτόν τον γείτονα. Επομένως αυτό είναι το metric που αποθηκεύει ο δρομολογητής στο πίνακα δρομολόγησης και που διαφημίζει στους υπόλοιπους δρομολογητές.

- **Route States**

Η εισαγωγή του πίνακα τοπολογίας μπορεί να γίνεται μέσω μιας εκ των δύο καταστάσεων. Μία διαδρομή εισέρχεται στην παθητική κατάσταση όταν το router δεν διενεργεί εκ νέου υπολογισμό της διαδρομής. Σε περίπτωση που ο δρομολογητής διενεργήσει εκ νέου υπολογισμό της διαδρομής τότε η διαδρομή θα εισέλθει σε ενεργητική κατάσταση. Όταν έχουμε εφικτούς διαδόχους, μια διαδρομή δεν χρειάζεται ποτέ να εισέλθει σε ενεργητική κατάσταση και αποφεύγει τον υπολογισμό της διαδρομής. Όταν όμως δεν υπάρχουν αυτοί οι εφικτοί διάδοχοι, τότε αναγκαστικά θα προχωρήσει σε εκ νέου υπολογισμό της διαδρομής.

Ο υπολογισμός της διαδρομής ξεκινά με τον δρομολογητή να αποστέλλει ένα μήνυμα ερώτησης σε όλους τους γείτονες του. Οι γειτονικοί δρομολογητές μπορούν να απαντήσουν αν διαθέτουν εφικτούς διαδόχους για τον προορισμό ή διαφορετικά το ερώτημα θα επιστρέψει, γεγονός που υποδεικνύει ότι ενεργεί τον υπολογισμό της διαδρομής. Ενώ βρίσκεται σε ενεργητική κατάσταση, ένας δρομολογητής δεν μπορεί να αλλάξει τον αμέσως επόμενο κόμβο που χρησιμοποιεί για να προωθεί πακέτα. Από τη στιγμή που θα ληφθούν όλες οι απαντήσεις στο συγκεκριμένο ερώτημα, ο προορισμός μπορεί να εισέλθει σε παθητική κατάσταση και να επιλεγεί ο καινούριος διάδοχος.

Για ενεργοποίηση του EIGRP φαίνεται από το παρακάτω παράδειγμα:

```
hostname ROUTER-A!
interface serial 0
 ip address 10.1.1.1 255.255.255.0
 exit
router eigrp 100
 network 10.1.1.0 0.0.0.255
 metric weights 0 2 0 1 0 0
```

3.10 Πρωτόκολλο Δρομολόγησης OSPF

Το OSPF αποτελεί πρωτόκολλο δρομολόγησης εσωτερικής πύλης ακολουθώντας την ιεραρχία και ανάλογα με την κατάσταση που βρίσκεται η εκάστοτε σύνδεση , δρομολογεί τα δίκτυα. Ο αλγόριθμος του Dijkstra, χρησιμοποιείται για να υπολογίσουμε το μονοπάτι μικρότερης διαδρομής, κάνοντας χρήση του κόστους ως μέτρο δρομολόγησης. Κατασκευάζει λοιπόν μία ταμπλέτα πληροφοριών σχετική με

την κατάσταση των συνδέσεων της τοπολογίας του δικτύου που δεν έχει καμία διαφορά στο σύνολο των δρομολογητών.

Το OSPF αποτελεί το πλέον ευρέως γνωστό πρωτόκολλο εσωτερικής πύλης όσον αφορά εκτεταμένα δίκτυα. Έχει την δυνατότητα να τρέχει χωρίς κίνδυνο, κάνοντας χρήση MD5 με σκοπό να επαληθεύσει τους γείτονές του, προτού δημιουργήσει γειτνιάσεις και προτού παραλάβει κάποια διαφήμιση κατάστασης σύνδεσης. Μια πιο καινούρια έκδοση του OSPF, (η OSPFv3), μπορεί επιπλέον να λειτουργήσει και με διευθύνσεις IPv6.

- **Περιοχή Κορμού (backbone area).**

Η περιοχή κορμού είναι υποχρεωμένη να κατασκευάσει τον πυρήνα ενός δικτύου που θα πρέπει όμως να έχει ως βάση του τον OSPF. Στην περιοχή του κορμού είναι επίσης τοποθετημένος ένας δρομολογητής διαμέσου του οποίου γίνεται η διαπεριοχιακή δρομολόγηση όλων των συνδεδεμένων με τον κορμό περιοχών

Σημείωση: Όλες οι περιοχές του OSPF θα πρέπει να συνδέονται με την περιοχή κορμού.

- **Περιοχή στελεχών (Stub Area).**

Μια περιοχή στελεχών είναι μια περιοχή η οποία δεν λαμβάνει εξωτερικές διαδρομές (external routes). Από την άλλη μεριά ως εξωτερικές διαδρομές ορίζουμε τις διαδρομές που φτάνουν στον OSPF μέσω κάποιου άλλου πρωτοκόλλου δρομολόγησης. Συνεπώς οι περιοχές στελεχών πρέπει να βασιστούν σε κάποια προδεδιαγεγραμμένη διαδρομή ώστε να μεταφέρουν την κίνηση σε άλλες διαδρομές έξω από την τωρινή περιοχή.

- **Πλήρως «στελεχωμένη» περιοχή (Totally stubby area – TSA).**

Πλήρως στελεχωμένη θεωρείται η περιοχή που δεν είναι σε θέση να γίνει παραλήπτης διαδρομών συνοψισμού προς κάθε εξωτερική διαδρομή. Η μόνη λύση για εξωτερική δρομολόγηση αποτελεί μια προκαθορισμένη διαδρομή Τύπου- 3LSA που γνωστοποιείται στην περιοχή. Εφόσον υφίσταται μια μοναδική εξωτερική διαδρομή ο δρομολογητής θα είναι αναγκασμένος να πάρει λιγότερες αποφάσεις ως προς την

δρομολόγηση, πράγμα που θα ελαχιστοποιήσει την επεξεργαστική ισχύ του συστήματος.

- **Όχι-τοσο-στελεχωμένη Περιοχή (Not-so-stubby area – NSSA).**

Μια όχι-τόσο-στελεχωμένη περιοχή είναι μια περιοχή στην οποία έχουν την δυνατότητα να εισαχθούν μονοπάτια από αυτόνομα συστήματα και να αποσταλούν στην περιοχή κορμού, αλλά αδυνατεί να εισάγει εξωτερικές διαδρομές από οποιαδήποτε άλλη περιοχή. Η Cisco έχει θέσει σε ισχύ μια δική της προσέγγιση σχετικά με το NSSA, το οποίο παρέχει τα χαρακτηριστικά μιας πλήρως στελεχωμένης περιοχής, με αποτέλεσμα τέτοιες περιοχές να μην μονοπωλούνται από διαδρομές τύπου 3 και 4.

3.10.1 Τύποι Δρομολογητών του OSPF

Το OSPF διαχωρίζει αρκετούς τύπους δρομολογητών. Κάθε δρομολογητής που δουλεύει με το πρωτόκολλο OSPF μπορεί να ομαδοποιηθεί σε αρκετούς από αυτούς τους τύπους.

- Δρομολογητής Ορίων Περιοχής (Area Border Router – ABR)

Ένας δρομολογητής ορίων περιοχής (ABR) μπορεί να επικοινωνεί με πάνω από μια περιοχή OSPF στο δίκτυο κορμού. Συνδέεται σαν μέλος των περιοχών που λαμβάνει χώρα. Ένας ABR δημιουργεί αντίγραφα στη βάση δεδομένων, ένα για κάθε περιοχή.

- Δρομολογητής Ορίων Αυτόνομου Συστήματος (Autonomous System Boundary Router - ASBR)

Ο ASBR έχει την δυνατότητα να επικοινωνεί και να ανταλλάζει πακέτα δεδομένων με δρομολογητές άλλων Αυτόνομων Συστημάτων, καθώς και να συνδεθεί σε πάνω από ένα Αυτόνομα Συστήματα. Οι ASBR συνήθως χρησιμοποιούν πρωτόκολλα όπως το BGP (Border Gateway Protocol). Ουσιαστικά ο ASBR αποστέλλει στο Αυτόνομο Σύστημα που βρίσκεται τα μονοπάτια που του γνωστοποιούν άλλα Αυτόνομα Συστήματα .

- Εσωτερικός Δρομολογητής (Internal Router - IR)

Ως εσωτερικό δρομολογητή μπορούμε να ορίσουμε τον δρομολογητή εκείνον που οι γειτνιάσεις μεταξύ των δρομολογητών ανήκουν στο ίδιο αυτόνομο σύστημα.

- Δρομολογητής Κορμού (Backbone Router - BR)

Ο δρομολογητής κορμού είναι εκείνος του οποίου η διεπαφή συνδέεται στην περιοχή κορμού. Θα μπορούσαμε να πούμε ότι ένας ABR αντιστοιχεί σε έναν BR, χωρίς όμως να είμαστε απόλυτα σίγουροι και για το αντίστροφο.

- Εφεδρικός Ορισμένος Δρομολογητής (Backup Designated Router - BDR)

Ως BDR ορίζουμε τον δρομολογητή που μετατρέπεται σε ορισμένο από την στιγμή κατά την οποία ο τρέχων ορισμένος δρομολογητής παρουσιάσει σφάλμα. Πρόκειται δηλαδή για τον OSPF δρομολογητή με την αμέσως επόμενη υψηλότερη τιμή προτεραιότητας.

- Ορισμένος Δρομολογητής (Designated Router - DR)

Ο ορισμένος δρομολογητής επιλέγεται από το δίκτυο ακολουθώντας την παρακάτω διαδικασία:

Η προτεραιότητα έχει εύρος μονάδων από 1 έως 255 και όσο υψηλότερος είναι ο αριθμός τόσο πιθανότερο είναι ο δρομολογητής να λειτουργήσει ως ορισμένος δρομολογητής ή ως εφεδρικός ορισμένος δρομολογητής, οπότε σε περίπτωση που η τιμή προτεραιότητας ενός δρομολογητή είναι 1, είναι σχεδόν απίθανο να επιλεγεί ως DR ή BDR.

Εφόσον περισσότεροι από ένας δρομολογητές παρουσιάζουν την ίδια, μεγαλύτερη τιμή προτεραιότητας, ως DR θα επιλεγεί εκείνος που διαθέτει το μεγαλύτερο Router ID , δηλαδή την υψηλότερη τιμή λογικής διεύθυνσης ρυθμισμένη στο δρομολογητή.

Στις περισσότερες περιπτώσεις ως BDR θα επιλεγεί ο δρομολογητής που διαθέτει την επόμενη υψηλότερη τιμή προτεραιότητας. Εφόσον στον DR παρουσιαστεί κάποιο σφάλμα, άμεσα αναλαμβάνει ο BDR, ο οποίος μετατρέπεται σε DR, και προχωράμε στην εκλογή του νέου BDR. Ακόμα πρέπει να αναφέρουμε την περίπτωση κατά την οποία συνδέεται αργότερα της εκλογής ένας δρομολογητής με υψηλότερη τιμή

προτεραιότητας από τους υπάρχοντες DR και BDR, δεν θα αναλάβει τη θέση κάποιου αλλά θα αναμένει μέχρι να παρουσιαστεί κάποιο σφάλμα.

Ο DR είναι υπεύθυνος ώστε να ενημερώνει όλους τους δρομολογητές του δικτύου για τυχόν αλλαγές στην τοπολογία, αυτό επιτυγχάνεται κρατώντας ο ίδιος έναν πίνακα αναλυτικής τοπολογίας και σε περίπτωση αλλαγής στο δίκτυο στέλνει τις απαραίτητες πληροφορίες μέσω μηνυμάτων πολυεκπομπής (multicast) στους δρομολογητες που επηρεάζονται από αυτές τις αλλαγές. Έτσι επιτυγχάνεται η ενημέρωση όλων των δρομολογητών χωρίς να στέλνουν συνεχώς μηνύματα μεταξύ τους, και σε συνδυασμό με τα μηνύματα πολυεκπομπής επιτυγχάνουν την μείωση του φόρτου στο δίκτυο.

Το παρακάτω παράδειγμα δείχνει μια πλήρη ρύθμιση του OSPF σε ένα Router CISCO

```
hostname(config)# router ospf 2
hostname(config-router)# network 2.0.0.0 255.0.0.0 area 0
hostname(config-router)# interface inside
hostname(config-interface)# ospf cost 20
hostname(config-interface)# ospf retransmit-interval 15
hostname(config-interface)# ospf transmit-delay 10
hostname(config-interface)# ospf priority 20
hostname(config-interface)# ospf hello-interval 10
hostname(config-interface)# ospf dead-interval 40
hostname(config-interface)# ospf authentication-key cisco
hostname(config-interface)# ospf message-digest-key 1 md5 cisco
hostname(config-interface)# ospf authentication message-digest
```

3.11 Access Lists

Μια Access Control List (ACL) είναι μια λίστα με δικαιώματα που χαρακτηρίζουν κανόνες που πρέπει να διέπονται σε ένα δίκτυο. Η λίστα αυτή προσδιορίζει επακριβώς ποιες ενέργειες μπορούν να εκτελεστούν πάνω στο δίκτυο σε ένα αντικείμενο ,το είδος της εργασίας και από ποιον χρήστη.

Οι Access Control Lists δηλαδή αποτελούν ένα σύνολο κανόνων που ουσιαστικά λένε ποιοι υπολογιστές του δικτύου θα έχουν πρόσβαση σε ποια συγκεκριμένη υπηρεσία ή σε άλλα δίκτυα, ή συσκευές του δικτύου. Οι Access Control Lists κατά κανόνα εφαρμόζονται στους δρομολογητές του δικτύου αλλά και σε servers. Οι λίστες αυτές μας δίνουν την δυνατότητα να φιλτράρουμε τόσο την εισερχόμενη όσο και την εξερχόμενη κίνηση στο δίκτυο μας.

Η χρήση των access-lists στο φιλτράρισμα της IP πληροφορίας έχει συγκεκριμένους στόχους:

- Ελέγχει την μετάδοση των πακέτων σε μια διεπαφή.
- Ελέγχει της πρόσβασης μίας γραμμής εικονικού τερματικού.
- Ελέγχει και περιορίζει το περιεχόμενο της ενημέρωσης κατά την δρομολόγηση των πακέτων.

Οι access-lists χωρίζονται στις λεγόμενες standard και extended. Επίσης υπάρχουν και οι Dynamic Access Lists.

Στις standard access lists ανάλογα με την διεύθυνση προέλευσης και τον κανόνα ελέγχου επιτρέπουν ή αρνούνται πακέτα.

Στις extended access lists έχουμε την δυνατότητα σύμφωνα με τον κανόνα έλεγχο που κάνουν στις διευθύνσεις αλλά και στο είδος πρωτοκόλλου του κάθε πακέτου, επιτρέπουν ή αρνούνται πακέτα.

Οι βασικές εντολές που δίνουμε σε access list είναι οι παρακάτω:

access-list-number	Ο αριθμός access-list. Στις standard list είναι ένας αριθμός από 1 έως 99

deny	Άρνηση στη πρόσβαση εάν οι κανόνες ισχύουν Επιτρέπει τη πρόσβαση εάν οι κανόνες ισχύουν
permit	Η διεύθυνση δικτύου ή συσκευής που εφαρμόζεται ο κανόνας
source	

Παραδείγματα εφαρμογής Access list είναι τα παρακάτω:

access-list 1 permit 100.233.200.5

access-list 1 deny 100.233.200.0 0.0.0.255

access-list 1 permit 100.233.0.0 0.0.255.255

Σε extended list παράδειγμα αποτελεί το παρακάτω:

access-list 101 permit tcp 0.0.0.0 255.255.255.255 100.200.201.0 0.0.0.255 gt 1023

access-list 101 permit tcp 0.0.0.0 255.255.255.255 100.200.201.4 0.0.0.0 eq 25

access-list 101 permit icmp 0.0.0.0 255.255.255.255 100.200.201.0 0.0.0.255

interface ethernet 1

ip access-group 101

ΚΕΦΑΛΑΙΟ 4: ΜΕΤΑΓΩΓΕΙΣ (SWITCHES) ΚΑΙ VLAN

4.1 Μεταγωγείς - Switches

Οι μεταγωγείς είναι δικτυακές συσκευές η οποίες ελέγχουν και αποστέλουν πακέτα δεδομένων μεταξύ των συσκευών δικτύου. Συνήθως λειτουργεί στο δεύτερο επίπεδο του μοντέλου OSI αν και τα νέα μοντέλα μεταγωγέων δίνουν την δυνατότητα λειτουργίας και στο τρίτο επίπεδο. Δίκτυα που λειτουργούν με μεταγωγεις για την επικοινωνία των συσκευών τους, ονομάζονται switched LANs ή όταν λειτουργούν με την τεχνολογία Ethernet, ονομάζονται switched Ethernet LANs..

Στις περιπτώσεις που ένα δίκτυο Ethernet αποτελείται από πολλούς χρήστες, είναι δεδομένο ότι θα υπάρξει διαμάχη των μέσων και συγκρούσεις. Οι συγκρούσεις αυτές αναπτύσσονται όταν περισσότερες από μια συσκευές επιχειρούν να αποστείλουν πληροφορίες στο δίκτυο την ίδια στιγμή.

Ο μεταγωγέας είναι σε θέση να διορθώσει τα περισσότερα προβλήματα μέσω της κατάτμησης των περιοχών εκπομπής, δηλαδή διαχωρίζοντας το δίκτυο σε περισσότερα τμήματα (εικονικά δίκτυα) και με αυτό τον τρόπο τις απαλλάσσει από διαμάχες και συγκρούσεις.

Πλέον οι πλειονότητα των δικτύων δομείται με βάση τα δίκτυα Ethernet και κύριο συστατικό είναι οι μεταγωγείς για Ethernet καθώς πλέον είναι σε θέση να παρέχουν ταχύτητες που φτάνουν τα Gigabits.

Βασικό γνώρισμα του μεταγωγέα αποτελεί το γεγονός ότι όλες οι θύρες του παρέχουν συγκεκριμένο εύρος ζώνης και επιτυγχάνει την μείωση των συγκρούσεων μέσω του διαχωρισμού σε περισσότερα πεδία συγκρούσεων (collision domain).

Όταν δυο σταθμοί θέλουν να συνδεθούν αλλά όμως η θέση τους είναι σε ξεχωριστές πόρτες του μεταγωγέα , το switch είναι αναγκασμένο να ελέγξει τον πίνακα προωθήσεις με σκοπό να ανιχνεύσει τη φυσική διεύθυνση MAC προορισμού καθώς και ποια είναι η κατάλληλη πόρτα για να το στείλει. Με αυτόν τον τρόπο αφού

ανιχνευθεί η καταχώρηση το πακέτο θα προωθηθεί στην σωστή θύρα. Έτσι επιτυγχάνεται η μείωση της κίνησης – συγκρούσεων και αυξάνονται οι επιδόσεις του δικτύου.

Οι μεταγωγείς είναι ικανοί να εργαστούν σε δυο καταστάσεις λειτουργίας:

Store and forward: ελέγχεται το σύνολο του πακέτου και εφόσον ανιχνευθεί ανακολουθία κατά την διαδικασία ελέγχου το πακέτο απορρίπτεται.

Cut-through : ελέγχεται από το πακέτο μόνο η ετικέτα με την πληροφορία που αφορά την φυσική διεύθυνση προορισμού και στην συνέχεια αποστέλλει το πακέτο, κάνοντας την λειτουργία αυτή ταχύτερη αλλά με κόστος στην αξιοπιστία σε σχέση με την Store and forward.

Η γνώση των φυσικών διευθύνσεων MAC και η αντιστοίχισή τους με τις θύρες του μεταγωγέα λύνουν το πρόβλημα του καταιγισμού του δικτύου. Πχ. Εάν σε ένα δίκτυο με 5 τερματικές συσκευές ο Η/Υ Νο 3 θέλει να στείλει μήνυμα στον Η/Υ 5 γνωρίζοντας ο μεταγωγέας την αντιστοίχιση των MAC διευθύνσεων με τις θύρες του, μεταδίδει το πακέτο απευθείας στον Η/Υ 5 χωρίς να καταλύσει το υπόλοιπο δίκτυο με μηνύματα.

Ο μεταγωγέας διαθέτει την ικανότητα να θέτει δικλείδες ασφάλειας στις πόρτες του, αντιστοιχίζοντας συγκεκριμένες φυσικές διευθύνσεις με τις κατάλληλες πόρτες του μεταγωγέα επιτυγχάνοντας τον αποκλεισμό κακόβουλων χρηστών από το δίκτυο μας.

- **Περιοχή συγκρούσεων - Collision Domain**

Ως περιοχή σύγκρουσης ορίζουμε την περιοχή όπου δεν έχουμε την δυνατότητα να αποστείλουμε κατά την ίδια χρονική στιγμή πολλά μηνύματα σε ένα μέσο , αλλά μας επιτρέπει την αποστολή η παραλαβή ενός μοναδικού μηνύματος.

Επομένως όσο περισσότεροι χρήστες υπάρχουν σε μια περιοχή σύγκρουσης , τόσο πιο εύκολο είναι να δημιουργηθούν συγκρούσεις και να μειωθεί η επίδοση του δικτύου. Τα δεδομένα που θα υποστούν σύγκρουση πρέπει να αναμεταδοθούν αυτή την φορά ύστερα από τυχαία χρονική στιγμή ώστε να αποφευχθούν καινούριες συγκρούσεις. Η επίλυση αυτού του προβλήματος είναι η διαιρέσει της περιοχής συγκρούσεων σε περισσότερες, αυτόνομες περιοχές συγκρούσεων.

Οι περιοχές σύγκρουσης που θα δημιουργηθούν θα εμπεριέχουν σαφέστατα λιγότερους χρήστες και αυτός είναι ο λόγος που περιμένουμε λιγότερες συγκρούσεις. Η μεταξύ τους αυτονομία βεβαιώνει την λειτουργία τους κατά την ίδια χρονική στιγμή με την αποφεύγει συγκρούσεων και βελτίωση των επιδόσεων.

Δικτυακές συσκευές που λειτουργούν στο επίπεδο 2 και 3 του μοντέλου OSI όπως οι μεταγωγείς και οι δρομολογητές μας δίνουν την δυνατότητα διαχωρισμού της περιοχής συγκρούσεων.

Η δυνατότητα αυτών των δικτυακών συσκευών βασίζεται στην ικανότητα τους να φιλτράρουν τη διακίνηση των πλαισίων δεδομένων με βάση τις MAC διεύθυνση τους.

Η δρομολόγηση με βάση τις MAC διευθύνσεις ασχολείται απαρέγκλιτα με τις λειτουργίες του επιπέδου 2 με αποτέλεσμα ο διαχωρισμός των περιοχών σύγκρουσης να πραγματοποιείται χρησιμοποιώντας τα switch.

Όσον αφορά το επίπεδο 3 οι δρομολογητές μπορούν να ενεργήσουν και σε αυτό το επίπεδο, συνεπώς ο διαχωρισμός των περιοχών σύγκρουσης είναι εφικτός.

- **Περιοχή εκπομπής - Broadcast Domain**

Ως εκπομπή τομέα ορίζουμε το λογικό εκείνο μέρος ενός δικτύου κατά το οποίο έχουν την δυνατότητα όλοι οι κομβόι να επικοινωνούν μεταξύ τους. Είναι πιθανό κάποια εκπομπή τομέα να βρίσκεται στο εσωτερικό του ίδιου τοπιού δικτύου ή αλλιώς να μεταφέρεται σε άλλα μέρη τοπικών δικτύων.

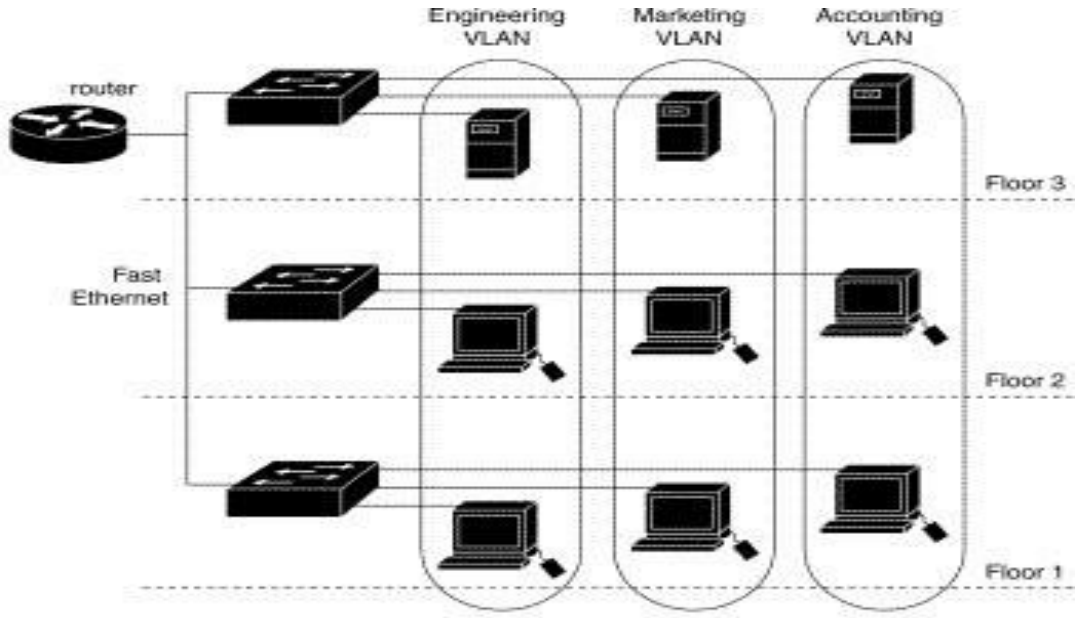
Όλες οι τερματικές συσκευές που συνδέονται με τον ίδιο Ethernet μεταγωγέα αποτελούν μέρος μια συγκεκριμένης εκπομπής τομέα.

4.2 Δημιουργία - ρυθμίσεις VLAN

Όσον αφορά τα τοπικά δίκτυα, ένα βασικό χαρακτηριστικό αποτελεί η περιοχή καθολικής εκπομπής που ονομάζουμε όλους τους κόμβους που έχουν συνδεθεί και υπάρχει η δυνατότητα λήψης του μεταδιδόμενου αυτού μηνύματος.

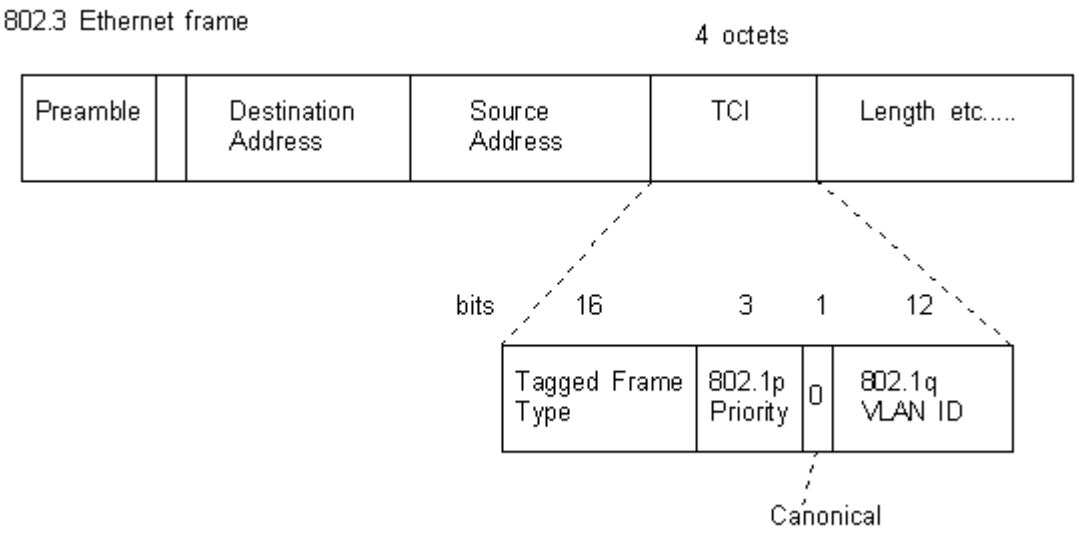
Το ιδεατό τοπικό δίκτυο (virtual LAN) δίνει την δυνατότητα κατασκευής διάφορων αυτόνομων περιοχών καθολικής εκπομπής ανάμεσα σε τερματικές συσκευές χωρίς να

παίζει τον παραμικρό ρόλο η περιοχή τοποθέτησης τους. Ως εκ τούτου, στο συγκεκριμένο μέσο πολλαπλής προσβασιμότητας δίνεται η δυνατότητα κατασκευής πολλών εικονικών δικτύων , σε διαφορετική περίπτωση μπορούμε να έχουμε ένα εικονικό δίκτυο ανάμεσα σε τερματικές συσκευές που συνδέονται σε αυτόνομα και απομακρυσμένα φυσικά μέσα.



Μέσω της κατασκευής εικονικών δικτύων πετυχαίνουμε την κατηγοριοποίηση των τερματικών συσκευών σε παρόμοια λειτουργικά σύνολα, χωρίς να παίζει ρόλο η φυσική θέση των υπολογιστών τους. Το πραγματικό κέρδος αυτής της κατηγοριοποίησης είναι η αύξηση της ασφάλειας από κακόβουλους χρήστες και επίσης ένας φτηνός τρόπος φυσικού διαχωρισμού. Η κατασκευή ενός εικονικού δικτύου καθίσταται δυνατή μέσω του λογισμικού της δικτυακής συσκευής. Με αυτό τον τρόπο η διαδικασία της ανακατασκευής του γίνεται μια πολύ απλή υπόθεση.

Για να γίνει εφικτός ο διαχωρισμός των εικονικών δικτύων, σε κάθε πακέτο προστίθεται μια ετικέτα που δίνει τις απαραίτητες πληροφορίες για το εικονικό δίκτυο που ανήκει καθώς και περεταίρω πληροφορίες (διεύθυνση αποστολέα, διεύθυνση παραλήπτη, τύπος πακέτου, δεδομένα



Το VLAN-ID προσδιορίζει τον αριθμό του εικονικού δικτύου στο όποιο ανήκει το πακέτο. Το εύρος των τιμών που μπορεί να πάρει είναι από 0 έως 4095 όμως επειδή το 0 και το 4095 είναι δεσμευμένες τιμές του πρωτοκόλλου το vlan ID κυμαίνεται από 1 έως 4094. Οι συσκευές δικτύου αναγνωρίζουν το vlan ID για να αναγνωρίσουν σε ποιο εικονικό δίκτυο ανήκει καθώς και για να το επεξεργαστούν ανάλογα.

- **Trunking και access port**

Trunk Port: Είναι μια ειδική λειτουργία που μπορεί να εκχωρηθεί σε μια θύρα, δίνοντας την ικανότητα να μεταφέρει την κυκλοφορία από όλα τα vlans. Μια τέτοια θύρα ονομάζεται trunk θύρα. Ως εκ τούτου, είναι σε θέση να μεταφέρει την κυκλοφορία για πολλά εικονικά δίκτυα στον ίδιο χρόνο, σε αντίθεση με μία θύρα προσβάσεως(access port), η οποία μεταφέρει κίνηση μόνο προς και από ένα συγκεκριμένο εικονικό δίκτυο

Για να προγραμματίσουμε μια θύρα ενός μεταγωγέα να λειτουργήσει ως trunk οι εντολές που χρειάζονται είναι η εξής :

Interface FastEthernet0/1 (οποιαδήποτε θύρα θέλουμε να προγραμματίσουμε)

Switchport mode trunk

Switchport trunk allowed vlan 10, 20, 30 (οποιοδήποτε ονόματα εικονικών δικτύων θέλουμε να περάσουν από την θύρα)

no shutdown

Access Port: είναι μια θύρα με σκοπό να φέρει μόνο την κίνηση που δημιουργείται μόνο από τους χρήστες. Αφήνει ελεύθερη την πληροφορία να περάσει μόνο από πακέτα στα οποία υπάρχει ετικέτα ίδια με το VLAN-ID στο οποίο ανήκει.

Για να προγραμματίσουμε μια θύρα ενός μεταγωγέα να λειτουργήσει ως access οι εντολές που χρειάζονται είναι η εξής :

interface FastEthernet0/1 (οποιαδήποτε θύρα θέλουμε να προγραμματίσουμε)

switchport mode access

switchport access vlan 10 (οποιοδήποτε ονόματα εικονικών δικτύων)

no shutdown

4.3 Το VTP

Το VTP αποτελεί πρωτόκολλο που ασχολείται με μηνύματα επιπέδου 2 και η χρήση του αφορά την κατανομή και ανανέωση πακέτων αναγνώρισης VLAN που έχουν τοποθετηθεί σε ένα δίκτυο μεταγωγής. Η εκάστοτε ρυθμίσεις σε ένα μεταγωγέα που βρίσκεται σε κατάσταση VTP server διαχέονται διαμέσου αυτού σε όλα τα switch που ανήκουν στο δίκτυο με σκοπό να μην είναι αναγκαία η ρύθμιση των δικτύων από τον χρήστη.

Για να προγραμματίσουμε έναν μεταγωγεα σαν vtp server οι εντολές που χρειάζονται είναι η εξής :

Enable
Config term
Vtp domain (domain-name)
Vtp server

4.4 Ασύρματα Δίκτυα

Ως ασύρματο δίκτυο ορίζεται το δίκτυο εκείνο το οποίο μεταδίδεται με ραδιοκύματα. Στα ασύρματα δίκτυα οι πληροφορίες μεταδίδονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα κύματος ανάλογη του ρυθμού μετάδοσης δεδομένων. Επιπλέον σήμερα έχουμε πολύ μεγάλη διάδοση των φορητών συσκευών. Ένα από σημαντικότερα χαρακτηριστικά των σύγχρονων φορητών

συσκευών είναι το μικρό μέγεθος τους σε συνδυασμό με την πολύ μεγάλη υπολογιστική τους ισχύ. Αυτό έχει ως αποτέλεσμα την ραγδαία εξάπλωση τους στην αγορά με αποτέλεσμα οι χρήστες να χρησιμοποιούν όλο και περισσότερο ασύρματα τα δίκτυα.

Έτσι τα ασύρματα δίκτυα βρίσκουν εφαρμογή σε χώρους που η χρήση καλωδίων είναι αδύνατη. Έτσι συναντάμε τα ασύρματα δίκτυα σε επαγγελματικούς χώρους αλλά και χώρους αναψυχής. Ειδικότερα σε γραφεία που είναι απαραίτητο να επικοινωνούν υπολογιστές με περιφερικά όπως για παράδειγμα εκτυπωτές .

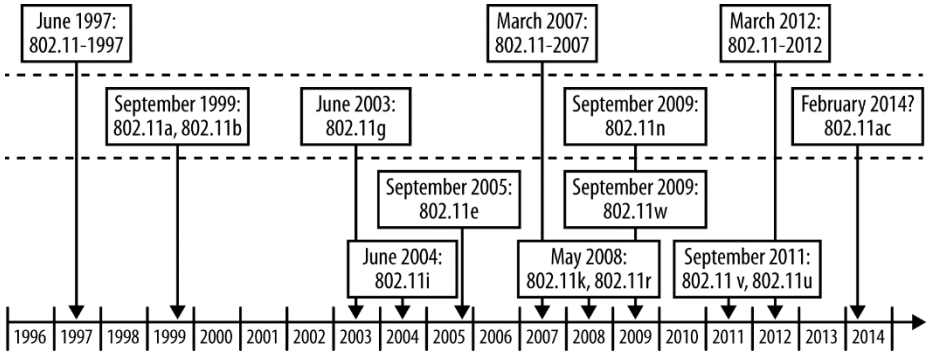
Πρότυπα στα Ασύρματα Δίκτυα

Η σύγχρονη έρευνα οδήγησε σταδιακά στην δημιουργία προτύπων πάνω στα ασύρματα δίκτυα. Πιο συγκεκριμένα σήμερα στο σύνολο των τεχνολογίων των τηλεπικοινωνιών και των ασύρματων δικτύων ακολουθείται το προτύπου 802.11.

Το πρωτόκολλο αυτό επιτρέπει επέκταση της κλασικής δομής LAN των ενσύρματων δικτύων σε ασύρματα και την εύκολη συνεργασία μεταξύ τους. Σήμερα στα ασύρματα δίκτυα έχουμε συνεχώς αυξανόμενη χωρητικότητα καναλιού ετσι ώστε να είναι εφικτό μεγαλύτερος ρυθμός μετάδοσης. Έτσι αναπτύσσονται νέα πρωτόκολλα, πάνω στο 802.11, τα οποία υλοποιούν τις νέες τεχνολογίες.

Τα πιο σημαντικά και γνωστά από αυτά, οι επεκτάσεις του 802.11 όπως 802.11a, 802.11b, 802.11g και το 802.11n και ac. Το πρότυπο που φαίνεται να επεκτείνεται και προβλέπεται να χρησιμοποιηθεί για τα επόμενα χρόνια, είναι το 802.11n, το οποίο πετυχαίνει ρυθμό μετάδοσης δεδομένων έως και 600 Mbit/s, ενώ το 802.11g έχει μέγιστο ρυθμό 54 Mbit/s.

Το πιο πρόσφατο πρωτόκολλο στην οικογένεια 802.11 είναι το 802.11ac, το οποίο αναγνωρίστηκε από την IEEE στις αρχές τους 2014.



Ιστορική Εξέλιξη του Προτύπου 802.11

Σχεδιασμός του 802.11

Κατά τον σχεδιασμό του προτύπου, ορίστηκαν 4 βασικά συστατικά μέρη:

- **Σταθμοί**

Στα ασύρματα δίκτυα αλλά και στα δίκτυα γενικά είναι σχεδιασμένα για την μεταφορά δεδομένων μεταξύ σταθμών. Σαν σταθμοί ονομάζονται οι τελικές συσκευές σε ένα δίκτυο δηλαδή υπολογιστές, κινητά, tables που έχουν διεπαφή ασύρματου δικτύου, και ουσιαστικά την δυνατότητα να συνδέονται σε αυτό. Οι συσκευές αυτές, μπορεί να είναι φορητές, όπως π.χ. ένας φορητός υπολογιστής, αλλά και σταθερές όπως ένας υπολογιστής στο χώρο εργασίας.

- **Σημεία Πρόσβασης (Access Points)**

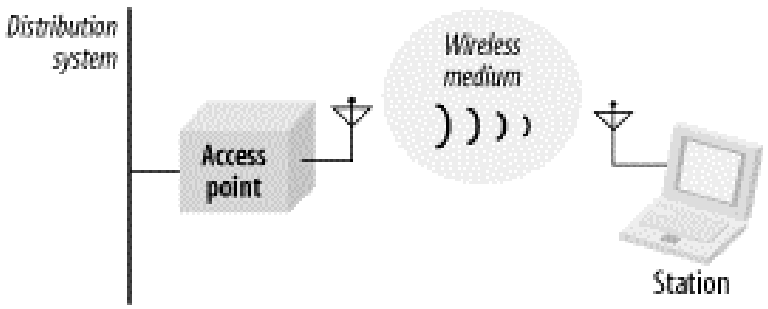
Τα σημεία πρόσβασης είναι συσκευές όπου ουσιαστικά συνδέονται οι σταθμοί και αναλαμβάνουν την μετάδοση της πληροφορίας. Εκεί ουσιαστικά γίνεται η επιλογή με βάση το πλαίσιο του μηνύματος που θα σταλεί η πληροφορία. Τα πλαίσια σε ένα δίκτυο 802.11 πρέπει να μεταβάλλονται σε άλλη μορφη πλαισίου για να αποσταλούν στον υπόλοιπο κόσμο. Την λειτουργία αυτή, με την οποία συνδέεται το ασύρματο δίκτυο στο ενσύρματο δίκτυο και εν συνεχεία στο ευρύτερο δίκτυο, είναι το σημείο πρόσβασης. Η γεφύρωση (bridging) ίσως είναι η σημαντικότερη λειτουργία που επιτελεί.

- **Ασύρματο Μέσο (Wireless Medium)**

Το ασύρματο μέσο είναι ουσιαστικά το αντίστοιχο καλώδιο στα κλασικά ενσύρματα δίκτυα. Για την μεταφορά πλαισίων από συσκευή σε συσκευή, το πρότυπο χρησιμοποιεί κάποιο ασύρματο μέσο. Στα ασύρματα δίκτυα έχουμε ραδιομετάδοση οπότε ανάλογα την συχνότητα επιλογής είναι σαν να έχουμε διαφορετικά φυσικά επίπεδα, για την υποστήριξη του προτύπου 802.11 MAC (Medium Access Control). Για αυτό τον λόγο, έχουν οριστεί φυσικά επίπεδα ραδιοσυχνοτήτων (RF) για την μετάδοση των δεδομένων.

- **Σύστημα Διανομής (Distribution System)**

Το σύστημα διανομής διευκολύνει στην επίτευξη επικοινωνία του ασύρματου δικτύου με τα άλλα δίκτυα. Γενικά τα ασύρματα δίκτυα είναι σχεδιασμένα για την επικοινωνία των υπολογιστών σε ένα χώρο μικρής εμβέλειας. Ένα κλασικό παράδειγμα διανομής, είναι η πρόσβαση στο Internet. Για να επιτύχουμε κάτι τέτοιο αυτό που κάνουμε είναι το σημείο πρόσβασης (Access Point) του ασύρματου δικτύου συνδέεται στο μέσο διανομής ώστε να μπορούν οι συνδεδεμένοι υπολογιστές, να έχουν πρόσβαση στο Internet. Δηλαδή συνδέουμε το access point με ένα δίκτυο καλωδίωσης. Σήμερα το σύστημα διανομής υλοποιείται ως μια συνένωση της μηχανής γεφύρωσης και ένα μέσο διανομής συστήματος, το οποίο αποτελεί το δίκτυο κορμού που χρησιμοποιείται για την αναμετάδοση πλαισίων ανάμεσα των σημείων πρόσβασης. Συχνά ονομάζεται απλά δίκτυο κορμού. Σε όλα σχεδόν τα σημερινά τοπικά δίκτυα, χρησιμοποιείται το Ethernet ως τεχνολογία δικτύου κορμού.



Σύνδεση Access Point με δίκτυο Κορμού

Το πρωταρχικό στοιχείο ενός δικτύου 802.11 είναι το λεγόμενο Βασικό Σύνολο Υπηρεσιών (BSS), που αποτελείται από μία ομάδα σταθμών που επικοινωνούν μεταξύ τους. Η περιοχή όπου είναι δυνατή η επικοινωνία, λέγεται βασική περιοχή υπηρεσιών (Basic Service Area) και προσδιορίζεται κάθε φορά από τα χαρακτηριστικά μετάδοσης. Τα σύνολα αυτά διαιρούνται σε δυο είδη, τα ανεξάρτητα σύνολα και τα σύνολα με υποδομή.

- **Ανεξάρτητα Σύνολα (Independent BSSs)**

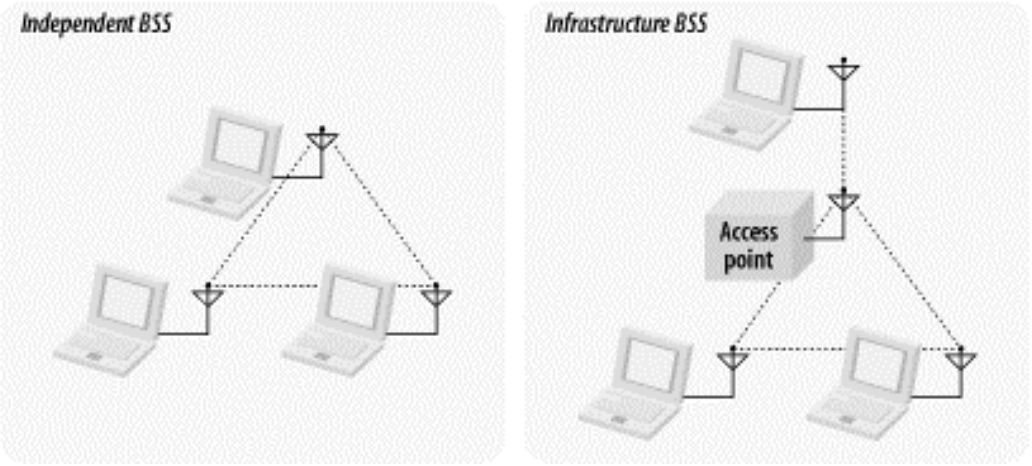
Στο ανεξάρτητο σύνολο, οι σταθμοί επικοινωνούν άμεσα με κάποιο άλλο σταθμό, εφόσον βρίσκεται σε απόσταση κατάλληλη για επικοινωνία. Έχουν μικρή διάρκεια ζωής , μικρό μέγεθος και καθορισμένους σκοπούς δημιουργίας, τα σύνολα αυτά ονομάζονται και ad hoc δίκτυα.

- **Σύνολα με υποδομή (Infrastructure BSSs)**

Τα σύνολα αυτά διαφέρουν από τα προαναφερόμενα στην εμφάνιση του σημείου πρόσβασης. Το σημείο πρόσβασης χρησιμοποιείται για την επικοινωνία στο δίκτυο, συγκαταλέγοντας και την επικοινωνία μεταξύ των σταθμών τους. Αν ένας σταθμός Α θέλει να στείλει ένα πακέτο στον σταθμό Β, όπου και οι δύο εντοπίζονται στο ίδιο δίκτυο, το πακέτο θα διέλθει στην αρχή από το σημείο πρόσβασης και στην συνέχεια στον σταθμό Β. Αυτού του είδους η διάδοση αποσπάει μεγάλο κομμάτι του καναλιού σε σχέση με την άμεση διάδοση του μηνύματος στον παραλήπτη. Η τεχνική αυτή λοιπόν διαθέτει και κάποια προνόμια που παρατίθενται πιο κάτω.

Η απόσταση από το σημείο πρόσβασης είναι εκείνη που ορίζει το σύνολο. Βασική προϋπόθεση είναι οι σταθμοί να εντοπίζονται μέσα στο βελησνεκές του σημείου, χωρίς να υπάρχει περιορισμός στην απόσταση από σταθμό σε σταθμό. Αν επιτρέπαμε την άμεση επικοινωνία θα ήμαστε σε θέση να εξοικονομήσουμε χωρητικότητα του καναλιού, θα επιβαρύναμε όμως όσον αφορά την πολυπλοκότητα του φυσικού επιπέδου, για τον λόγο ότι οι σταθμοί είναι αναγκασμένοι να κρατούν τα δεδομένα των γειτονικών κόμβων μέσα στο δίκτυο.

Ένας τρόπος για την εξοικονόμηση ενέργειας που είναι σημαντική για τους σταθμούς είναι μέσω των σημείων πρόσβασης. Επιτυγχάνεται λοιπόν διότι διαθέτουν την ικανότητα να αναγνωρίζουν την χρονική στιγμή που κάποιος σταθμός διατελεί σε κατάσταση εξοικονόμησης ενέργειας, με αποτέλεσμα να προβαίνουν σε αποθήκευση των πακέτων που προβλέπεται να μεταδώσουν στον εκάστοτε σταθμό και αποστέλλονται μαζικά μετά το πέρας της εξοικονόμησης ενέργειας.



Βασικά είδη δικτύων 802.11

- **Υπηρεσίες**

Οι υπηρεσίες είναι ουσιαστικά διαδικασίες που ορίζει το πρωτόκολλο 802.11 και προσφέρει για την επικοινωνία των συσκευών. Έτσι στην τυποποίηση του προτύπου, καθορίζονται και οι υπηρεσίες που προσφέρει. Οι τρεις είναι υπεύθυνες για την αποστολή πακέτων, ενώ οι άλλες έξι είναι εκείνες που αδειοδοτούν ώστε το δίκτυο να είναι σε θέση να επιτηρεί τους κόμβους αλλά και να αποστέλλει πακέτα.

Οι υπηρεσίες αυτές είναι οι παρακάτω:

- **Διανομή**

Η διανομή είναι η υπηρεσία που χρησιμοποιείται από τους σταθμούς σε ένα δίκτυο με υποδομή με στόχο να επιλεγεί η μεταφορά στο σωστό κόμβο η πληροφορία. Δηλαδή κάθε φορά που θα σταλούν τα δεδομένα. Έτσι όταν ένα πλαίσιο λαμβάνεται από το σημείο πρόσβασης, χρησιμοποιεί την υπηρεσία αυτή για να μεταφέρει το πλαίσιο στον προορισμό του.

- **Ενσωμάτωση**

Η ενσωμάτωση είναι η υπηρεσία σε ένα σύστημα διανομής που πιτρέπει την σύνδεση του συστήματος διανομής σε ένα άλλο δίκτυο που δεν είναι 802.11.

- **Συσχέτιση**

Για να μπορέσει να γίνει η διανομή και να έχουμε μεταφορά των πλαισίων στους σταθμούς πρέπει οι σταθμοί να καταγράφονται ή να συσχετίζονται με σημεία πρόσβασης. Το σύστημα διανομής μπορεί να χρησιμοποιήσει πληροφορίες καταγραφής για να αποφασίσει πιο σημείο πρόσβασης θα χρησιμοποιήσει για κάθε σταθμό. Πρακτικά η συσχέτιση έχει να κάνει με την σύνδεση του σταθμού στο ασύρματο δίκτυο.

- **Επανασυσχέτιση**

Επειδή έχουμε φορητές συσκευές έχουμε και μετακίνηση. Οι σταθμοί λοιπόν είναι αναγκασμένοι να τροποποιήσουν την δύναμη του σήματος τους ή να βρουν ένα έτερο σημείο πρόσβασης για να πραγματοποιήσουν την σύνδεση. Αυτή η διαδικασία συμβαίνει εφόσον το έτερο δίκτυο προσφέρει μεγαλύτερα οφέλη.

- **Αποσυσχέτιση**

Είναι η διαδικασία που ουσιαστικά αποφασίζεται ο τερματισμός μίας συσχέτισης. Όταν καλείται η υπηρεσία αυτή, τα δεδομένα που έχουν καταγραφεί για αυτή την συσχέτιση ενός σταθμού διαγράφονται από το σύστημα διανομής. Ως αποσυσχέτιση ορίζεται η διαδικασία κατά την οποία ένας σταθμός αποσυνδέεται από ένα ασύρματο δίκτυο.

- **Αυθεντικοποίηση**

Αναγκαίο είναι να ταυτοποιηθούν οι σταθμοί. Επειδή λοιπόν το να συνδεθούμε σε κάποιο δίκτυο είναι απλό, πρέπει οι σταθμοί να ταυτοποιούνται, με τη διαδικασία της πιστοποίησης. Η υπηρεσία ταυτοποίησης, παρέχει λειτουργίες πιστοποίησης, με στόχο της εξασφαλίση ότι οι σταθμοί που συνδέονται στο δίκτυο, είναι εξουσιοδοτημένοι να το κάνουν. Ένα εργαλείο επίτευξης αποτελεί ένας κωδικός πρόσβασης για το δίκτυο, με σκοπό να υπάρχει έλεγχος των σταθμών που θα συνδεθούν σε αυτό.

- **Αναίρεση της αυθεντικοποίησης**

Η λειτουργία αυτή είναι υπεύθυνη για να προσδιορίσει πότε φτάνει στο τέλος της η τρέχουσα αυθεντικοποίηση. Πρόκειται για την αντίστροφη διαδικασία από την αυθεντικοποίηση και συμβαίνει για να αποσυσχετίσει τον σταθμό από το δίκτυο.

- **Εμπιστευτικότητα**

Ένα από τα πιο βασικά μειονεκτήματα της ασύρματης επικοινωνίας είναι το πρόβλημα της ασφάλειας αφού η πληροφορία μεταδίδεται ασύρματα και έτσι είναι εύκολο σε κάποιο κακόβουλο χρήστη να την υποκλέψει. Αυτό συμβαίνει γιατί κάθε δίκτυο λαμβάνει και αποστέλλει δεδομένα σε σταθμούς που βρίσκονται μέσα στο βεληνεκές του με συνέπεια την υποβάθμιση της ασφάλειας του ασύρματου δικτύου αφού στην ακτίνα αυτή μπορεί να βρεθεί οποιοσδήποτε. Η υπηρεσία αυτή έχει ως στόχο την προστασία των περιεχομένων των μηνυμάτων, χρησιμοποιώντας διάφορους αλγόριθμους κρυπτογράφησης. Οι πιο γνωστοί αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται στα περισσότερα ασύρματα δίκτυα, είναι οι WEP, TKIP και AES

- **Διάταξη μονάδων δεδομένων υπηρεσίας MAC (MAC Service Data Unit Ordering)**

Η υπηρεσία αυτή είναι υπεύθυνη για την ορθή αποστολή των πακέτων που θα σταλούν στον αποδέκτη, διασφαλίζοντας ελάχιστες απώλειες και τυχόν λάθη των δεδομένων.

- **Έλεγχος Ισχύος Μετάδοσης (Transmit Power Control)**

Ένα ακόμα πολύ μεγάλο πρόβλημα στην ασύρματη επικοινωνία είναι ότι συνήθως οι συσκευές που χρησιμοποιούνται είναι φορητές και μπορεί να βρίσκονται σε χώρους όπου και άλλα δίκτυα παρεμβάλλονται ή υπάρχουν άλλες ραδιοφωνικές εκπομπές και λήψεις. Η υπηρεσία τρέχει λειτουργία εξέτασης της ισχύος που διανέμονται τα πακέτα με σκοπό να αποφύγει μια πιθανή παρέμβαση σε άλλο γειτονικό δίκτυο που θα μπορούσε να υποβαθμίσει την ποιότητα του καναλιού και να διαστρεβλώσει τα πακέτα που θα σταλούν. Σκοπός λοιπόν της υπηρεσίας είναι η ενέργεια μετάδοσης να είναι ίση με αυτή που πρέπει ώστε να γίνει η ορθή αποστολή των πλαισίων αποκλείοντας οποιαδήποτε παρέμβαση και σπατάλη ενέργειας ώστε να υπάρχει εδραίωση του σήματος απέναντι στα άλλα δίκτυα.

- **Δυναμική Επιλογή Συχνότητας (Dynamic Frequency Selection)**

Στα ασύρματα δίκτυα για να μην έχουμε παρεμβολές έχουν οριστεί κανονισμοί που απαιτούν από τα δίκτυα που λειτουργούν στα 5 GHz να διαθέτουν λειτουργία που θα εμποδίζει την παράλληλη εκπομπή ενός ασύρματου δικτύου με άλλα συστήματα ραντάρ, έτσι ώστε να αποτραπούν τυχόν παρεμβολές, με αποτέλεσμα την δυσλειτουργία των συστημάτων. Συγχρόνως η λειτουργία αυτή έχει την ικανότητα να διανέμει ισομερώς τα διαθέσιμα κανάλια για να μην υπάρχουν συγκρούσεις μεταξύ άλλων δικτύων.

ΚΕΦΑΛΑΙΟ 5: ΣΧΕΔΙΑΣΗ ΣΕΝΑΡΙΩΝ ΔΙΚΤΩΝ

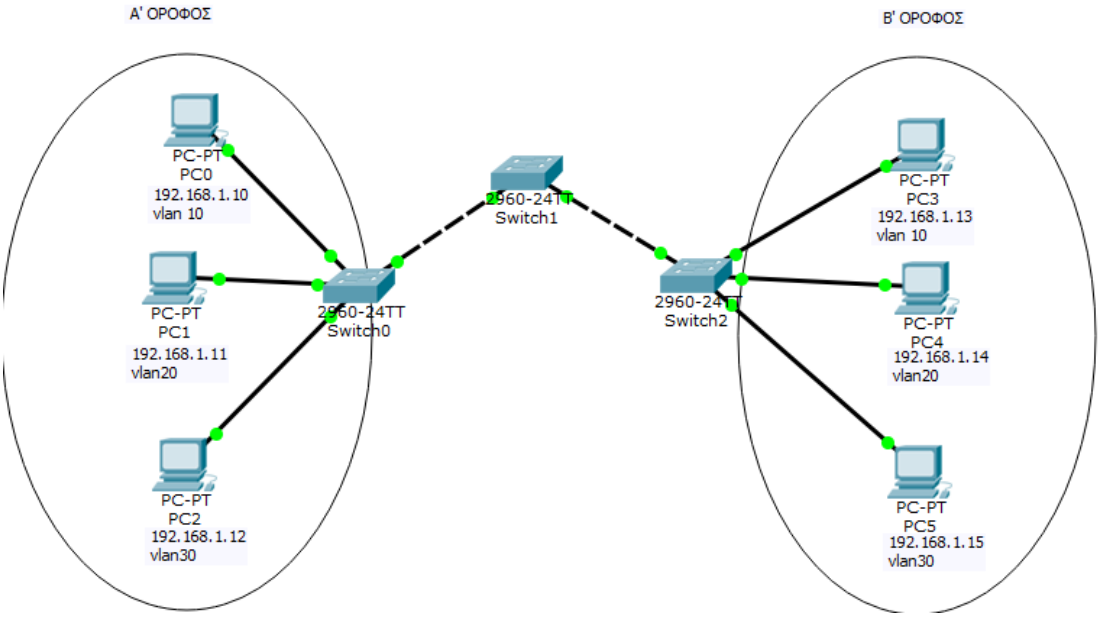
5.1 Δημιουργία δικτύων με την βοήθεια προσομοιωτή

Ένα σημαντικό κομμάτι για την απόκτηση της πιστοποίησης CCNA εκτός από άριστη γνώση σε θεωρητικό επίπεδο, εξίσου σημαντικό είναι και άριστη εφαρμογή τους σε πρακτικό επίπεδο. Ο εξεταζόμενος θα πρέπει να δημιουργεί δίκτυα ανάλογα με τις ανάγκες και τις προδιαγραφές και να εφαρμόζει την θεωρία στο πρακτικό κομμάτι με επιτυχία. Στο κεφάλαιο αυτό θα δημιουργήσουμε κάποια σενάρια δικτύων βασιζόμενα στην παραπάνω θεωρία, θα δούμε αναλυτικά τις εντολές που χρειάζονται για να προγραμματιστούν οι συσκευές των δικτύων μας και τέλος θα δούμε τα αποτελέσματα και θα τα εξηγήσουμε.

ΣΕΝΑΡΙΟ 1

Σε αυτό το σενάριο υπάρχουν τρία switch και έξι υπολογιστές, τρεις από αυτούς βρίσκονται στον Α’ όροφο μιας επιχείρησης και οι υπόλοιποι στον Β’ όροφο.

Βρίσκονται στο ίδιο λογικό δίκτυο (192.168.1.0 /24). Θέλουμε να χωρίσουμε το δίκτυο μας σε τρία εικονικά δίκτυα (VLAN 10- παραγωγή ,20 – λογιστηριο,30 – διοίκηση).



- Βήμα 1: Σχεδιάζουμε το δίκτυο μας στον προσομοιωτή
- Βήμα 2 : Σε κάθε υπολογιστή δίνουμε την διεύθυνση IP και μάσκα υποδικτύου όπως φαίνεται στην παραπάνω εικόνα
- Βήμα 3 : ρυθμίζουμε τους μεταγωγής

Ρυθμίσεις μεταγωγέα (swich 0)

Enable	"μπαίνει στο Privilage Mode"
Config term	"εισαγωγή στο configuration mode"
Vlan 10	"δημιουργια του vlan 10"
Name paragwgh	"ονομάζουμε το vlan 10 ως παραγωγή"
Vlan 20	"δημιουργία του vlan 20"
Name logisthrio	"ονομάζουμε το vlan 20 ως λογιστήριο"
Vlan30	"δημιουργια του vlan 30"
Name dioikhsh	"ονομάζουμε το vlan 30 ως διοίκηση"
interface FastEthernet0/1	" έναρξη του mode για ρύθμιση της θυρας 0/1"
switchport trunk allowed vlan 10,20,	" περνάει τα πακέτα από τα VLAN 10,20,30"
switchport mode trunk	"ρύθμιση της θύρας ως trunk"
interface FastEthernet0/20	" έναρξη του mode για ρύθμιση της θυρας 0/20"
switchport access vlan 10	"περνάει τα πακέτα μόνο από το VLAN 10"
switchport mode access	"ρύθμιση της θύρας ως access"
interface FastEthernet0/21	" έναρξη του mode για ρύθμιση της θύρας 0/21"
switchport access vlan 20	"περνάει τα πακέτα μόνο από το VLAN 20"
switchport mode access	"ρύθμιση της θύρας ως access"
interface FastEthernet0/22	" έναρξη του mode για ρύθμιση της θυρας 0/22"
switchport access vlan 30	"περνάει τα πακετα μονο από το VLAN 30"

switchport mode access “ρύθμιση της θύρας ως access”

Ρυθμίσεις μεταγωγέα (swich 1)

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”
Vlan 10 “δημιουργία του vlan 10”
Name paragwgh “ονομάζουμε το vlan 10 ως παραγωγή”
Vlan 20 “δημιουργία του vlan 20”
Name logisthrio “ ονομάζουμε το vlan 20 ως λογιστήριο”
Vlan30 “δημιουργία του vlan 30”
Name dioikhsh “ονομάζουμε το vlan 30 ως διοίκηση”
interface FastEthernet0/1 “ έναρξη του mode για ρύθμιση της θύρας 0/1”
switchport trunk allowed vlan 10,20,30 “ περνάει τα πακέτα από τα VLAN 10,20,30”
switchport mode trunk “ρύθμιση της θύρας ως trunk”

interface FastEthernet0/2 “ έναρξη του mode για ρύθμιση της θύρας 0/2”
switchport trunk allowed vlan 10,20,30 “ περνάει τα πακέτα από τα VLAN 10,20,30”
switchport mode trunk “ρύθμιση της θύρας ως trunk”

Ρυθμίσεις μεταγωγεα (swich 2)

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”
Vlan 10 “δημιουργία του vlan 10”
Name paragwgh “ονομάζουμε το vlan 10 ως παραγωγή”
Vlan 20 “δημιουργια του vlan 20”
Name logisthrio “ ονομάζουμε το vlan 20 ως λογιστήριο”
Vlan30 “δημιουργία του vlan 30”
Name dioikhsh “ονομάζουμε το vlan 30 ως διοίκηση”
interface FastEthernet0/1 “ έναρξη του mode για ρύθμιση της θύρας 0/1”
switchport trunk allowed vlan 10,20, “ περνάει τα πακετα από τα VLAN 10,20,30”
switchport mode trunk “ρύθμιση της θύρας ως trunk”

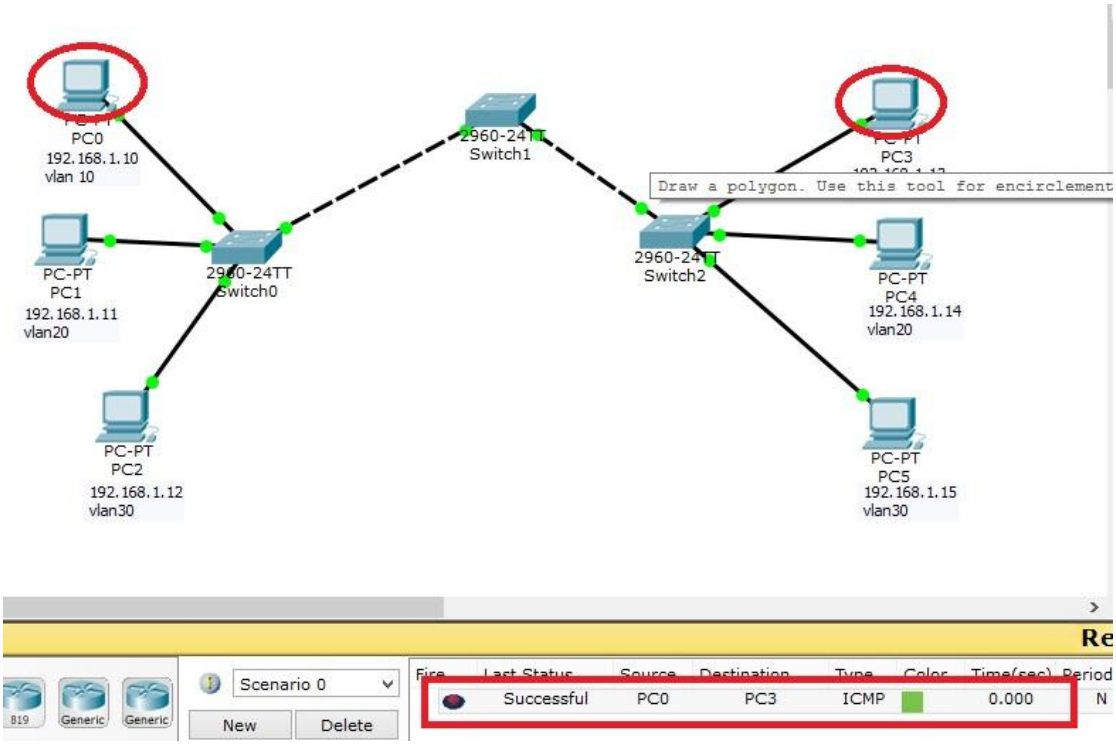
interface FastEthernet0/20 “ έναρξη του mode για ρύθμιση της θύρας 0/20”
switchport access vlan 10 “περνάει τα πακέτα μόνο από το VLAN 10”
switchport mode access “ρύθμιση της θύρας ως access”

interface FastEthernet0/21 “ έναρξη του mode για ρύθμιση της θύρας 0/21”
switchport access vlan 20 “περνάει τα πακέτα μόνο από το VLAN 20”
switchport mode access “ρύθμιση της θύρας ως access”

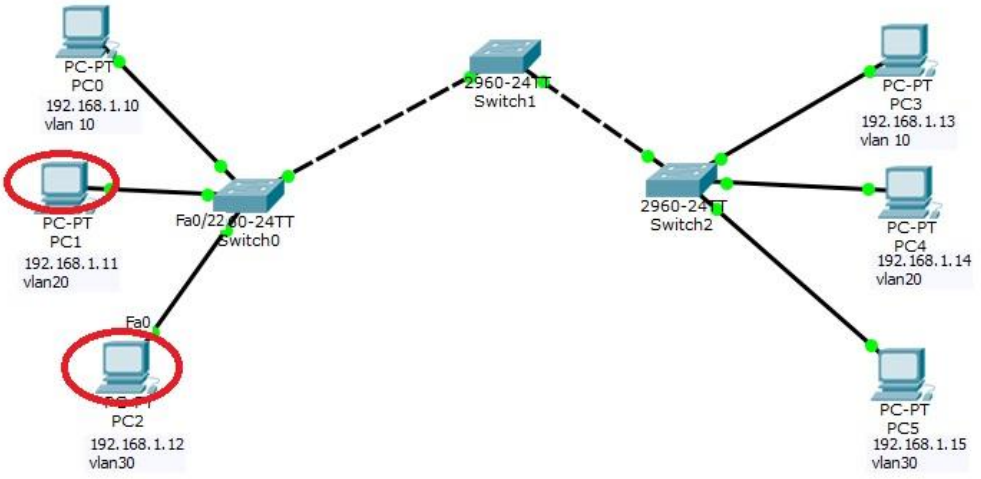
interface FastEthernet0/22 “ έναρξη του mode για ρύθμιση της θύρας 0/22”

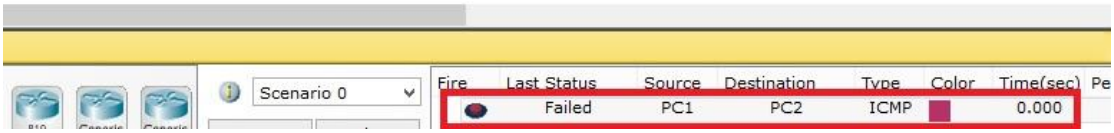
switchport mode access	“ρύθμιση της θύρας ως access”
switchport access vlan 30	“περνάει τα πακέτα μόνο από το VLAN 30”

Κάνοντας τις παραπάνω ρυθμίσεις στους router επιτυγχάνουμε των διαχωρισμό του δικτύου μας σε τρία εικονικά δίκτυα (VLAN 10,20,30) και ενώ κανονικά κάθε υπολογιστής του δικτύου θα έπρεπε να επικοινωνεί με τους υπολοίπους αφού έχουν διευθύνσεις IP του ίδιου δικτύου , αντιθέτως πετύχαμε να διαχωρίσουμε το δίκτυο και κάθε υπολογιστής να επικοινωνεί μόνο με τους υπολογιστές του ίδιου εικονικού δικτύου. Κάνοντας ping από το pc0 στο pc3 που ανήκουν κ οι δυο στο VLAN 10 περιμένουμε να έχουμε επιτυχή επικοινωνία.



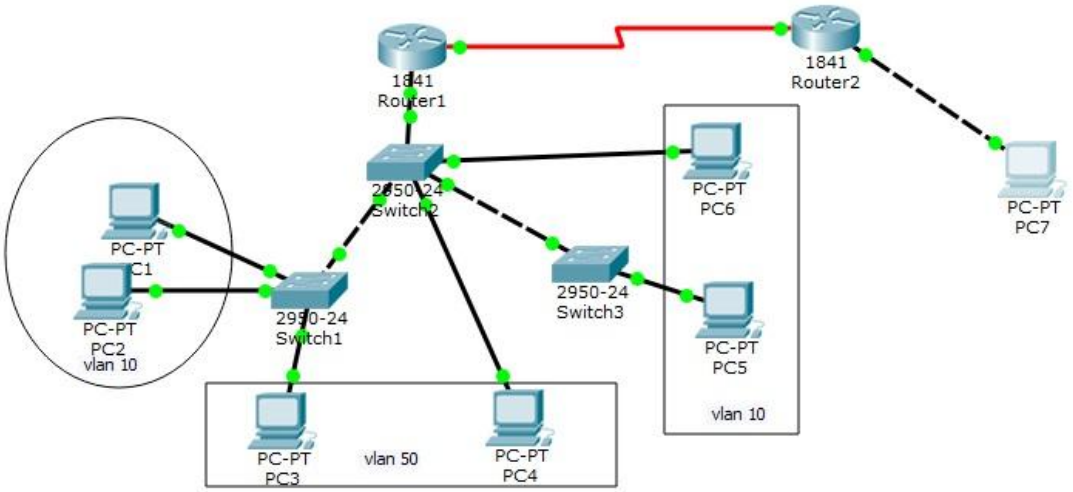
Σε αντίθετη περίπτωση αν κάνουμε ping από το pc1 που ανήκει στο VLAN 20 προς το pc2 που ανήκει στο VLAN 30 αυτό που περιμένουμε να δούμε είναι ανεπιτυχής επικοινωνία.





ΣΕΝΑΡΙΟ 2

Στο σενάριο υπάρχουν τρία switch δυο router και επτά υπολογιστές. Για την καλύτερη απόδοση του δικτύου το χωρίζουμε σε δυο εικονικά δίκτυα το vlan 10 και το vlan 50. Τα PC του VLAN 10 ανήκουν στο δίκτυο 10.0.10.0 και μάσκα υποδικτύου 255.255.255.0, ενώ τα τα PC του VLAN 50 στο δίκτυο 10.0.50.0 και μάσκα υποδικτύου 255.255.255.0.



Ζητούμενο είναι κάθε υπολογιστής να μπορεί να επικοινωνήσει με οποιονδήποτε από τους άλλους υπολογιστές άσχετα αν βρίσκεται σε διαφορετικό VLAN.

- Βήμα 1: Σχεδιάζουμε το δίκτυο μας στον προσομοιωτή.
- Βήμα 2 : Σε κάθε υπολογιστή δίνουμε την διεύθυνση IP και μάσκα υποδικτύου ανάλογα με το εικονικό δίκτυο που ανήκει.
- Βήμα 3 : ρυθμίζουμε τους μεταγωγής .

Ρυθμίσεις μεταγωγέα (swich 1)

Enable	“μπαίνει στο Privilage Mode”
Config term	“εισαγωγή στο configuration mode”
Vlan 10	“δημιουργία του VLAN10”
Name vlan10	“ονομάζουμε το VLAN 10 ως vlan10”
Vlan 50	“δημιουργία του VLAN 50”
Name vlan50	“ονομάζουμε το VLAN 50 ως vlan50”
interface FastEthernet0/1	“ έναρξη του mode για ρύθμιση της θύρας 0/1”
switchport mode trunk	“ρύθμιση της θύρας ως trunk”
switchport trunk allowed vlan 10,50	“ περνάει τα πακέτα από τα VLAN 10,50”
interface FastEthernet0/2	“ έναρξη του mode για ρύθμιση της θύρας 0/2”
switchport mode access	“ρύθμιση της θύρας ως access”
switchport access vlan 10	“περνάει τα πακέτα μόνο από το VLAN 10”
interface FastEthernet0/3	“ έναρξη του mode για ρύθμιση της θύρας 0/3”
switchport mode access	“ρύθμιση της θύρας ως access”
switchport access vlan 10	“περνάει τα πακέτα μόνο από το VLAN 10”

interface FastEthernet0/4	“ έναρξη του mode για ρύθμιση της θύρας 0/4”
switchport mode access	“ρύθμιση της θύρας ως access”
switchport access vlan 50	“περνάει τα πακέτα μόνο από το VLAN 50”

Ρυθμισεις μεταγωγέα (switch 2)

Enable	“μπαίνει στο Privilage Mode”
Config term	“εισαγωγή στο configuration mode”
Vlan 10	“δημιουργία του VLAN10”
Name vlan10	“ονομάζουμε το VLAN 10 ως vlan10”
Vlan 50	“δημιουργία του VLAN 50”
Name vlan50	“ονομάζουμε το VLAN 50 ως vlan50”
interface FastEthernet0/1	“ έναρξη του mode για ρύθμιση της θύρας 0/1”
switchport mode trunk	“ρύθμιση της θύρας ως trunk”
switchport trunk allowed vlan 10,50	“ περνάει τα πακέτα από τα VLAN 10,50”
interface FastEthernet0/2	“ έναρξη του mode για ρύθμιση της θύρας 0/2”
switchport mode trunk	“ρύθμιση της θύρας ως trunk”
switchport trunk allowed vlan 10,50	“ περνάει τα πακέτα από τα VLAN 10,50”
interface FastEthernet0/3	“ έναρξη του mode για ρύθμιση της θύρας 0/3”
switchport mode trunk	“ρύθμιση της θύρας ως trunk”
switchport trunk allowed vlan 10,50	“ περνάει τα πακέτα από τα VLAN 10,50”
interface FastEthernet0/4	“ έναρξη του mode για ρύθμιση της θύρας 0/4”
switchport mode access	“ρύθμιση της θύρας ως access”
switchport access vlan 50	“περνάει τα πακέτα μόνο από το VLAN 50”
interface FastEthernet0/5	“ έναρξη του mode για ρύθμιση της θύρας 0/5”
switchport mode access	“ρύθμιση της θύρας ως access”
switchport access vlan 10	“περνάει τα πακέτα μόνο από το VLAN 10”

Ρυθμισεις μεταγωγέα (switch 3)

Enable	“μπαίνει στο Privilage Mode”
Config term	“εισαγωγή στο configuration mode”
Vlan 10	“δημιουργία του VLAN10”
Name vlan10	“ονομάζουμε το VLAN 10 ως vlan10”
Vlan 50	“δημιουργία του VLAN 50”
Name vlan50	“ονομάζουμε το VLAN 50 ως vlan50”
interface FastEthernet0/1	“ έναρξη του mode για ρύθμιση της θύρας 0/1”
switchport mode trunk	“ρύθμιση της θύρας ως trunk”
switchport trunk allowed vlan 10,50	“ περνάει τα πακέτα από τα VLAN 10,50”
interface FastEthernet0/2	“ έναρξη του mode για ρύθμιση της θύρας 0/2”
switchport mode access	“ρύθμιση της θύρας ως access”

switchport access vlan 10 “περνάει τα πακέτα μόνο από το VLAN 10”

Κάνοντας αυτές τις ρυθμίσεις έχουμε επιτυχή την ομαδοποίηση των υπολογιστών σε δυο εικονικά δίκτυα το VLAN 10 και VLAN 50 όπως φαίνεται στο σχήμα.

- Βήμα 4 :προγραμματίζουμε τους δρομολογητές (router) ώστε να επιτευχθεί η επικοινωνία όλων των υπολογιστών ανεξάρτητα από το εικονικό δίκτυο που ανήκουν.

Οι ρυθμίσεις του δρομολογητή (router 1)

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”

interface FastEthernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”
no shutdown “άνοιγμα του interface”

interface FastEthernet0/0.10 “έναρξη του mode για ρύθμιση της θύρας 0/0.10”
Encapsulation dot1Q 10 “το interface 0/0 να εμπεριέχει και το interface 0/0.10”
ip address 10.0.10.10 255.255.255.0 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0.10”

interface FastEthernet0/0.50 “έναρξη του mode για ρύθμιση της θύρας 0/0.50”
encapsulation dot1Q 50 “το interface 0/0 να εμπεριέχει και το interface 0/0.50”
ip address 10.0.50.10 255.255.255.0 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0.50”

interface Serial0/0/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/0/0
ip address 10.0.20.1 255.255.255.0 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0/0”
clock rate 128000 “ ρύθμιση του ρολογιού για συντονισμό σε serial interface (DCE)”

ip route 10.0.30.0 255.255.255.0 10.0.20.2 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 10.0.30.0/24”

Στη διεπαφή (interface) του router που συνδέσαμε τα switches χρησιμοποιήσαμε δύο subinterfaces δίνοντας στο ένα subinterface, IP από το υποδίκτυο 10.0.10.0 και στο

άλλο από το 10.0.50.0. Τέλος περνάμε στον προγραμματισμό του δρομολογητή (router 2).

Ρυθμίσεις του δρομολογητή (router 2)

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”

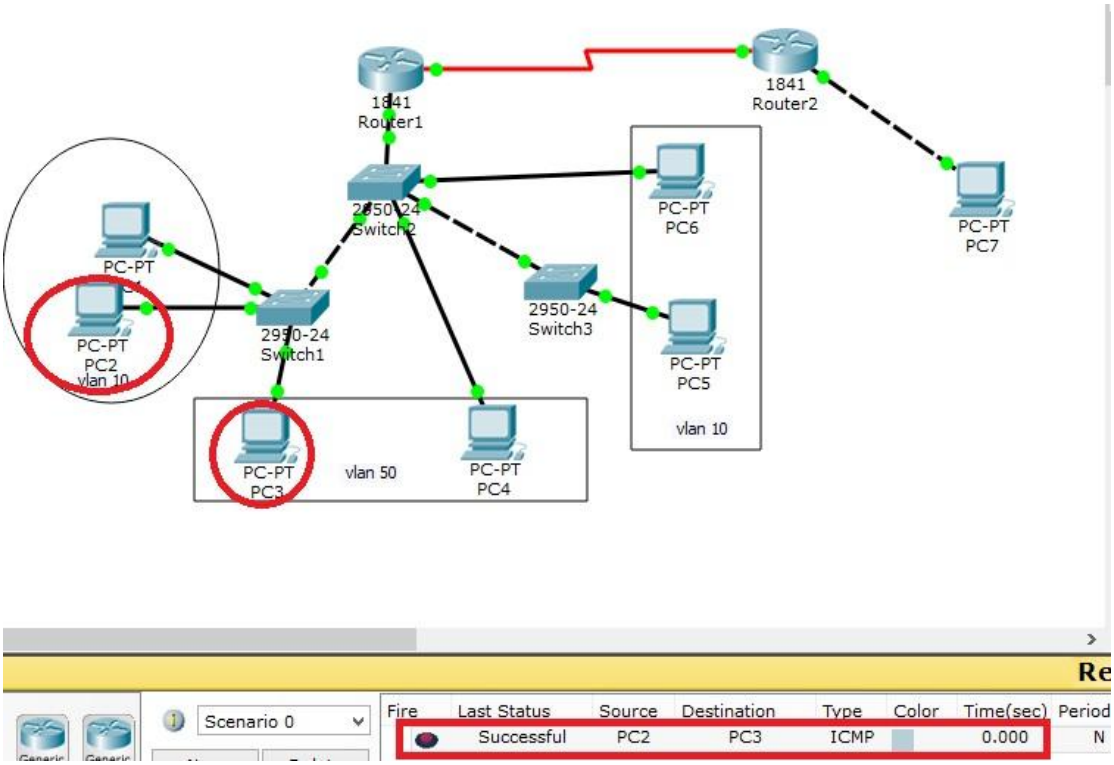
interface FastEthernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”
ip address 10.0.30.10 255.255.255.0“δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0”

interface Serial0/0/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/0/0”
ip address 10.0.20.2 255.255.255.0 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0/0”

ip route 10.0.10.0 255.255.255.0 10.0.20.1 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 10.0.10.0/24”

ip route 10.0.50.0 255.255.255.0 10.0.20.1“στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 10.0.50.0/24”

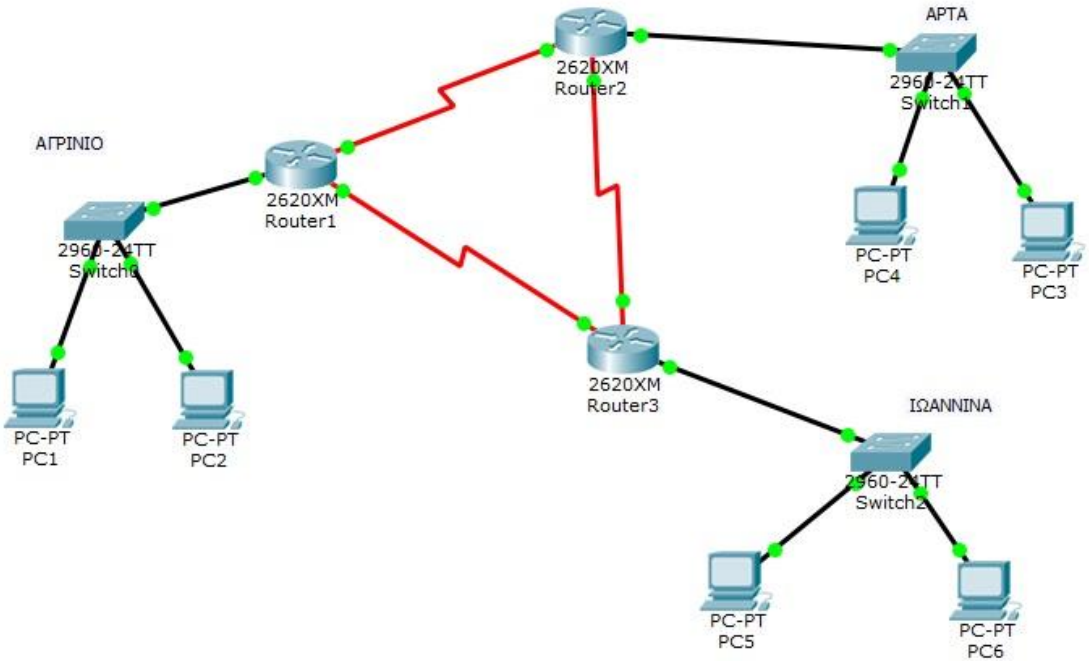
Έτσι επιτυγχάνεται η αμφίδρομη επικοινωνία όλων τον υπολογιστών ανεξάρτητα από το αν βρίσκονται η όχι σε κάποιο εικονικό δίκτυο και σε ποιο.



Όπως φαίνεται και στην παραπάνω εικόνα κάνοντας ping από το pc 2 που ανήκει στο VLAN 10 προς το pc 3 που ανήκει στο VLAN 50 ,το αποτέλεσμα είναι επιτυχία, που σημαίνει ότι οι δυο υπολογιστές επικοινωνούν , που ήταν και το ζητούμενο του σεναρίου.

ΣΕΝΑΡΙΟ 3

Σ’ αυτό το σενάριο μια εταιρία έχει τρία υποκαταστήματα. Θέλουμε να επιτευχθεί η επικοινωνία τους . Κάθε κατάστημα έχει δύο υπολογιστές ένα μεταγωγέα και έναν δρομολογητή Το κατάστημα του Αγρίνιου έχει διεύθυνση βάσης 192.168.1.0/28, το κατάστημα της Άρτας έχει διεύθυνση 192.168.2.0/28, και των Ιωαννίνων την 192.168.3.0/28 .



- Βήμα 1: Σχεδιάζουμε το δίκτυο μας στον προσομοιωτή.
- Βήμα 2 : Σε κάθε υπολογιστή δίνουμε την διεύθυνση IP, μάσκα υποδικτύου και προεπιλεγμένη πύλη ανάλογα σε πιο δίκτυο ανήκει.
- Βήμα 3 : ρυθμίζουμε τους δρομολογητές.

Ρυθμίσεις δρομολογητή (Router Αγρίνιου):

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”

interface FastEthernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”
ip address 192.168.1.14 255.255.255.240 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0”

interface Serial0/0/0 “έναρξη του mode για ρύθμιση της σειριακης θύρας 0/0/0”
ip address 10.10.10.1 255.255.255.252 “δινουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0/0”

interface Serial0/1/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/1/0”
ip address 30.30.30.2 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/1/0”

ip route 192.168.2.0 255.255.255.240 10.10.10.2 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 192.168.2.0 ”

ip route 192.168.3.0 255.255.255.240 30.30.30.1 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 192.168.3.0 ”

Ρυθμίσεις δρομολογητή (router Άρτας):

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”

interface FastEthernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”
ip address 192.168.2.14 255.255.255.240 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0”

interface Serial0/0/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/0/0”
ip address 10.10.10.2 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0/0”

interface Serial0/1/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/1/0”
ip address 20.20.20.1 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/1/0”

ip route 192.168.1.0 255.255.255.240 10.10.10.1 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 192.168.1.0 ”

ip route 192.168.3.0 255.255.255.240 20.20.20.2 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 192.168.3.0 ”

Ρυθμίσεις δρομολογητή (router Ιωαννίνων):

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”

interface FastEthernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”
ip address 192.168.3.14 255.255.255. “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0”

interface Serial0/0/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/0/0”
ip address 20.20.20.2 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0/0”

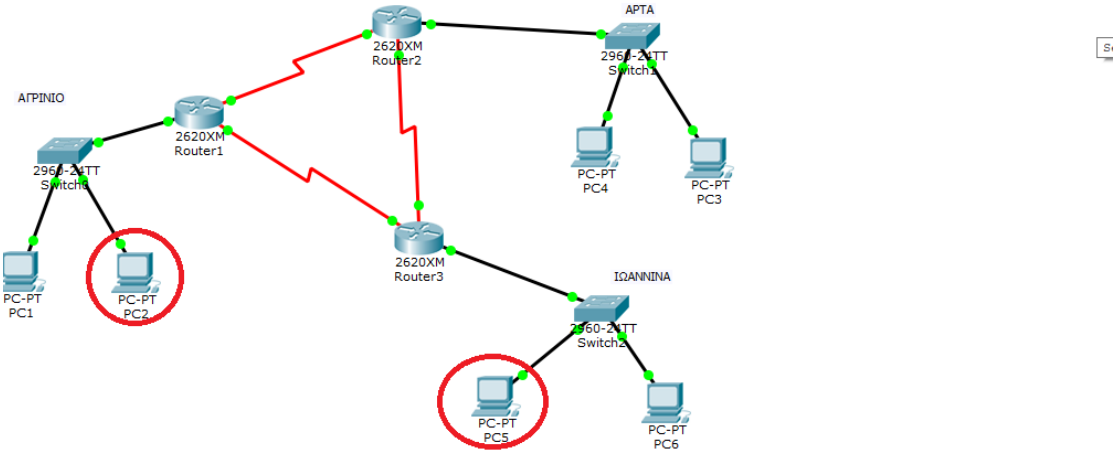
interface Serial0/1/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/1/0”
ip address 30.30.30.1 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/1/0”

interface Serial0/2/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/2/0”
ip address 200.0.0.2 255.255.255.0 “δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/2/0”

ip route 192.168.1.0 255.255.255.240 30.30.30.2 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 192.168.1.0 ”

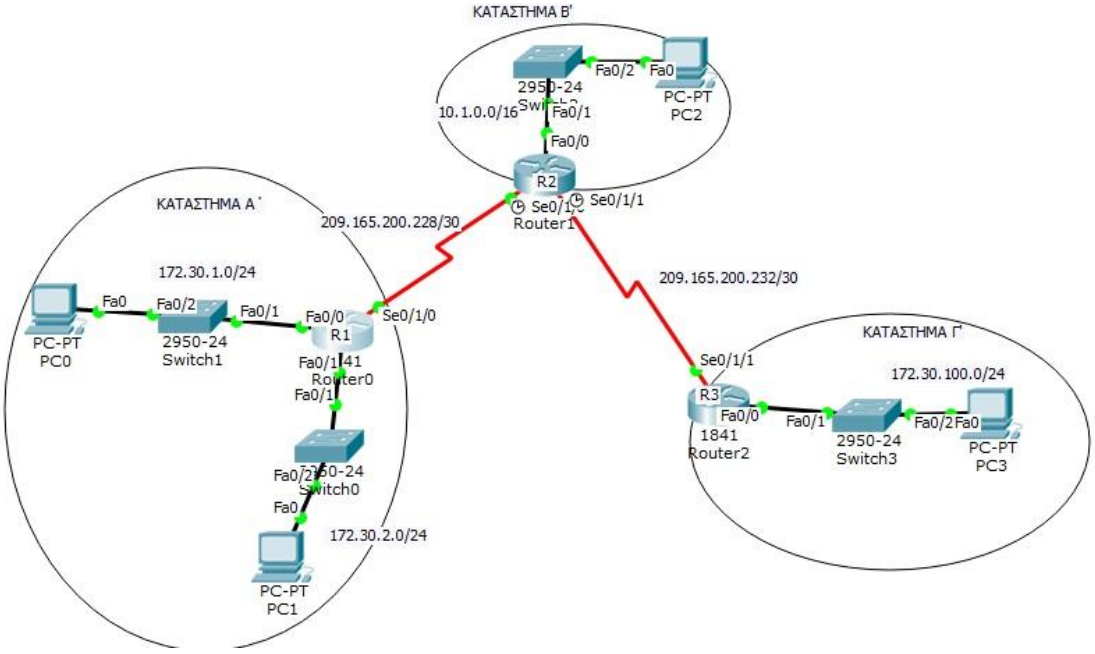
ip route 192.168.2.0 255.255.255.240 20.20.20.1 1 “στατική διαδρομή για την δρομολόγηση των πακέτων που αφορούν το δίκτυο 192.168.2.0 ”

Αφού κάναμε τις απαραίτητες ρυθμίσεις στους δρομολογητές (router) κάνοντας ping από οποιονδήποτε υπολογιστή του δικτύου σε κάποιον άλλο, όπως φαίνεται στην παρακάτω εικόνα, βλέπουμε ότι επικοινωνούν μεταξύ τους, που ήταν και το ζητούμενο του σεναρίου μας .

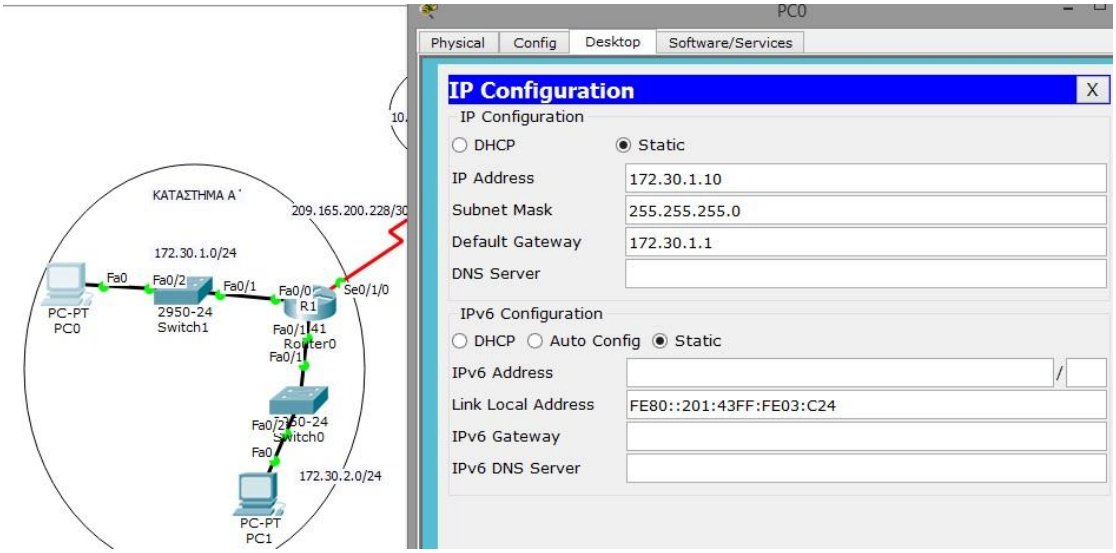


ΣΕΝΑΡΙΟ 4

Σ’ αυτό το σενάριο μια εταιρία έχει τρία υποκαταστήματα. Θέλουμε να επιτευχθεί η επικοινωνία τους με την χρήση ενός δυναμικού πρωτοκόλλου. Το κάθε κατάστημα έχει διαφορετική διεύθυνση βάσης. Το κατάστημα Α’ έχει διεύθυνση βάσης 172.30.1.0/24 και, 172.30.2.0/24 το κατάστημα Β’ έχει διεύθυνση 10.1.0.0/16, και το κατάστημα Γ’ την 172.30.100.0/24. Επίσης οι δρομολογητές συνδέονται με μισθωμένες σειριακές γραμμές, και αποτελούν ένα δικό τους ξεχωριστό δίκτυο με διεύθυνση βάσης το 209.165.200.228/30 και 209.165.200.232/30. Ζητούμενο είναι όλοι οι υπολογιστές να επικοινωνούν μεταξύ τους ανεξάρτητα από το κατάστημα που ανήκουν.



- Βήμα 1: Σχεδιάζουμε το δίκτυο μας στον προσομοιωτή.
- Βήμα 2 : Σε κάθε υπολογιστή δίνουμε την διεύθυνση IP, μάσκα υποδικτύου και προεπιλεγμένη πύλη ανάλογα σε πιο δίκτυο ανήκει. Όπως στην παρακάτω εικόνα για το κατάστημα Α’.



- Βήμα 3 : ρυθμίζουμε τους δρομολογητές.

Ρυθμίσεις δρομολογητή 1(Router 1):

Enable “μπαίνει στο Privilage Mode”
Config term “εισαγωγή στο configuration mode”
interface fastethernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”
ip address 172.30.1.1 255.255.255.0“δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/0”

no shut “ η θύρα 0/0 να παραμείνει ανοιχτεί”
interface fastethernet 0/1 “ έναρξη του mode για ρύθμιση της θύρας 0/1”
ip address 172.30.2.1 255.255.255.0“δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/1”
no shut “ η θύρα 0/1 να παραμείνει ανοιχτεί”
interface serial 0/1/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/1/0”
ip address 209.165.200.230 255.255.255.252“δίνουμε διεύθυνση IP και μάσκα υποδ. Στο 0/1/0”
no shut “ η θύρα 0/1/0 να παραμείνει ανοιχτεί”
router rip “Ο δρομολογητής να ενεργοποιήσει το δυναμικό πρωτόκολλο rip”
version 2 “ να ενεργοποιήσει την εκδοση δυο του rip”
network 172.30.1.0 “να διαφημίσει το δίκτυο 172.30.1.0”

network 172.30.2.0 “να διαφημίσει το δίκτυο 172.30.2.0”

network 209.165.200.228 “να διαφημίσει το δίκτυο 209.165.200.228”

no auto-summary “να μην γίνει αυτόματη σύνοψη των δικτύων”

Ρυθμίσεις δρομολογητή 2 (Router 2):

Enable “μπαίνει στο Privilage Mode”

Config term “εισαγωγή στο configuration mode”

interface fastethernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”

ip address 10.1.0.1 255.255.0 “δίνουμε διεύθυνση IP και μάσκα υποδ. στο 0/0”

no shut “ η θύρα 0/0 να παραμείνει ανοιχτεί ”

interface serial 0/1/0 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/1/0”

ip address 209.165.200.229 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. στο 0/1/0”

no shut “ η θύρα 0/1/0 να παραμείνει ανοιχτεί ”

interface serial 0/1/1 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/1/1”

ip add 209.165.200.233 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. στο 0/1/1”

no shut “ η θύρα 0/1/0 να παραμείνει ανοιχτεί ”

router rip “Ο δρομολογητής να ενεργοποιήσει το δυναμικό πρωτόκολλο rip”

version 2 “ να ενεργοποιήσει την εκδοση δυο του rip”

network 10.1.0.1 “να διαφημίσει το δίκτυο 10.1.0.1”

network 209.165.200.229 “να διαφημίσει το δίκτυο 209.165.200.229”

network 209.165.200.233 “να διαφημίσει το δίκτυο 209.165.200.233”

no auto-summary “να μην γίνει αυτόματη σύνοψη των δικτύων”

Ρυθμίσεις δρομολογητή 3 (Router 3):

Enable “μπαίνει στο Privilage Mode”

Config term “εισαγωγή στο configuration mode”

interface fastethernet0/0 “ έναρξη του mode για ρύθμιση της θύρας 0/0”

ip address 172.30.100.1 255.255.255.0 “δίνουμε διεύθυνση IP και μάσκα υποδ. στο 0/0”

no shut “ η θύρα 0/0 να παραμείνει ανοιχτεί ”

interface serial 0/1/1 “έναρξη του mode για ρύθμιση της σειριακής θύρας 0/1/0”

ip address 209.165.200.234 255.255.255.252 “δίνουμε διεύθυνση IP και μάσκα υποδ. στο 0/1/1”

no shut “ η θύρα 0/1/1 να παραμείνει ανοιχτεί ”

router rip “Ο δρομολογητής να ενεργοποιήσει το δυναμικό πρωτόκολλο rip”

version 2 “ να ενεργοποιήσει την εκδοση δυο του rip”

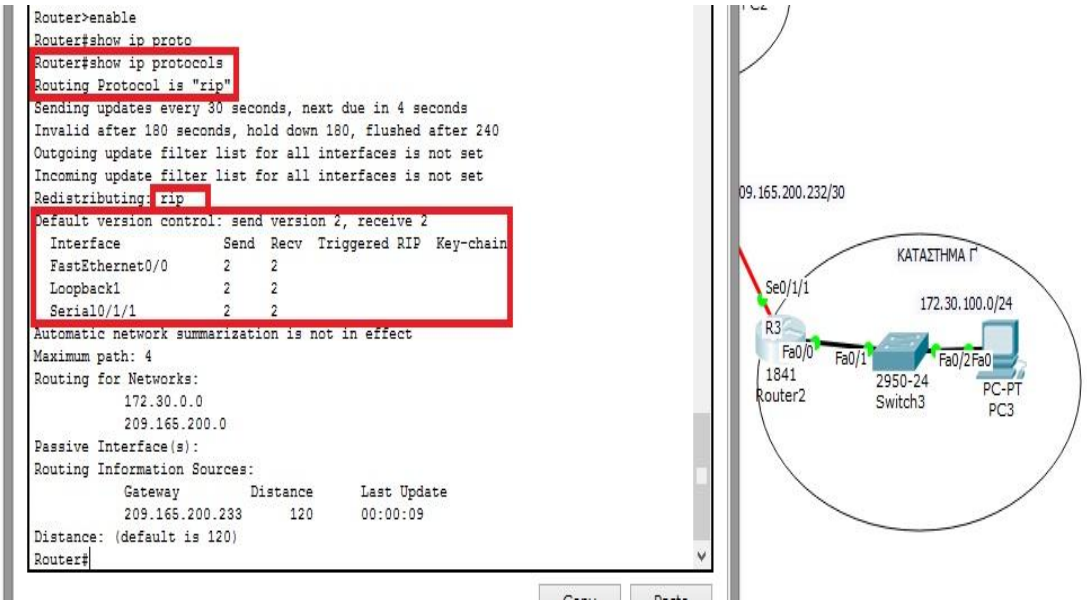
network 172.30.100.0 “να διαφημίσει το δίκτυο 172.30.100.0”

network 172.30.200.17 “να διαφημίσει το δίκτυο 172.30.200.17”

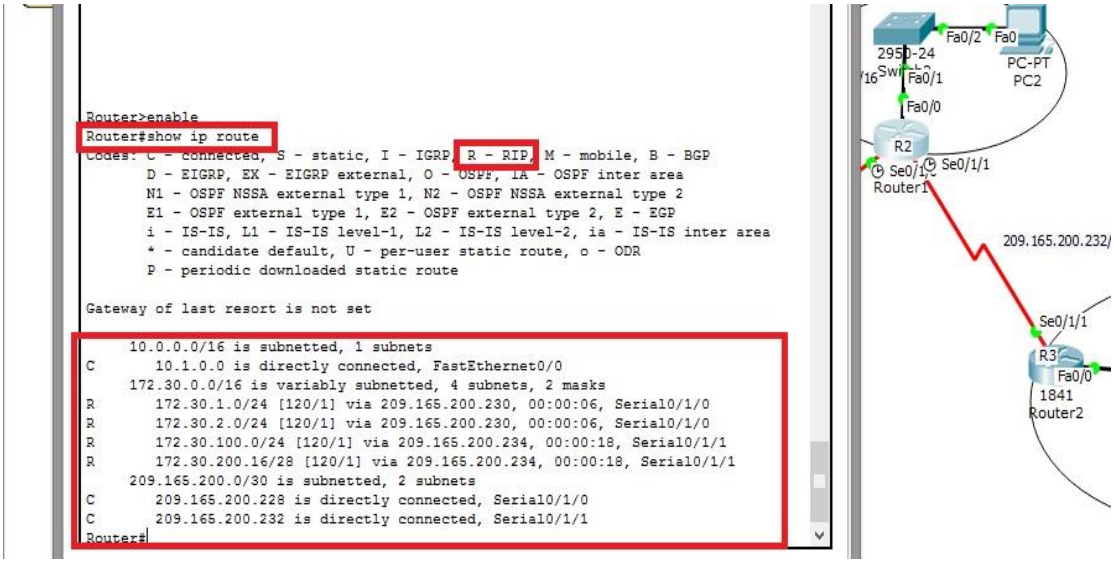
network 209.165.200.232 “να διαφημίσει το δίκτυο 209.165.200.232”

no auto-summary “να μην γίνει αυτόματη σύνοψη των δικτύων”

- Βήμα 4 : Ελέγχουμε αν οι δρομολογητές χρησιμοποιούν το πρωτόκολλο rip2 Με την εντολή **show ip protocols** και αν έχουν ενημερωθεί για όλες τις διαδρομές του δικτύου με την εντολή **show ip route.**

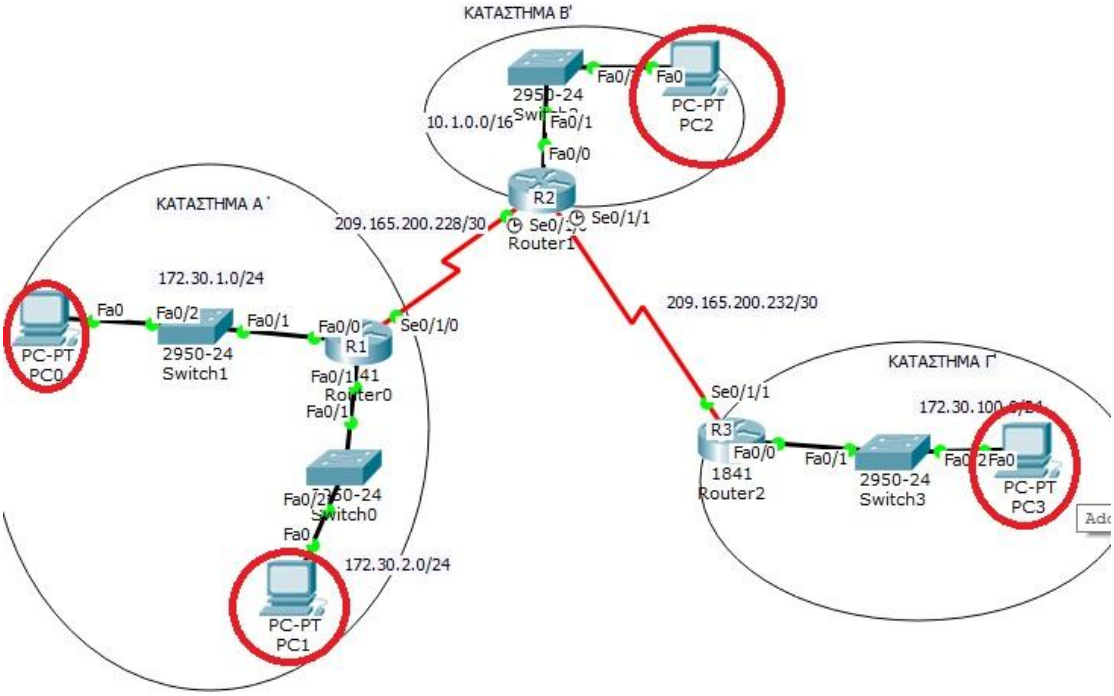


Το αποτέλεσμα της εντολής show ip protocols μας δείχνει ότι ο δρομολογητής χρησιμοποιεί το πρωτόκολλο rip version 2 .



Το αποτέλεσμα της εντολής show ip route μας δείχνει το πίνακα δρομολόγησης του δρομολογητή 2 (router 2) ,ο οποίος είναι ενημερωμένος από το πρωτόκολλο rip με όλες τις πιθανές κατευθύνσεις του δικτύου μας.

- Βήμα 5 : Ελέγχουμε αν ολοι οι υπολογιστες του δικτυου μας επικοινωνουν μεταξυ τους.



Κάνοντας ping από το PC0 προς το PC1,το PC2 και το PC3, όπως φαίνεται στην παραπάνω εικόνα, βλέπουμε ότι επικοινωνούν μεταξύ τους, που ήταν και το ζητούμενο του σεναρίου μας. .

5.2 Ενδεικτικές ερωτήσεις από Final Test CCNA

Παρακάτω παρουσιάζονται μια σειρά από ερωτήσεις που προτείνονται από την CISCO Academy για την επιτυχία κάποιου στο CCNA.

Αξίζει να σημειώσουμε ότι οι Ερωτήσεις είναι πραγματικές ερωτήσεις από πραγματικά Test για την απόκτηση του CCNA. Οι παρακάτω ερωτήσεις προστατεύονται από πνευματικά δικαιώματα της CISCO και μας έχουν δοθεί από επίσημη ακαδημία της CISCO. Παρόλα αυτά είναι ερωτήσεις 3 χρόνων πριν την παράδοση της παρούσας διπλωματικής οπότε και διατίθενται ελεύθερα και από την CISCO.

Οι ερωτήσεις είναι ερωτήσεις αντιστοίχησης, πολλαπλής ή απλής επιλογής.

Ερώτηση 1.

Ποια είναι δύο χαρακτηριστικά του TCP (2 επιλογές)

What are two characteristics of TCP? (Choose two.)

1. αξιοπιστίας μεταφοράς δεδομένων
   data transport reliability
2. καλύτερο καθορισμό διαδρομής
   best path determination
3. ίδρυση, διατήρηση, και περάτωση εικονικών κυκλωμάτων
   establishing, maintaining, and terminating virtual circuits
4. ενθυλάκωση πακέτων σε ένα πλαίσιο δεδομένων με διευθύνσεις πηγής και προορισμού MAC
   encapsulation of packets in a data frame with source and destination MAC addresses

5. Βέλτιστος τρόπος παράδοσης διαγραμμάτων
   best-effort datagram delivery

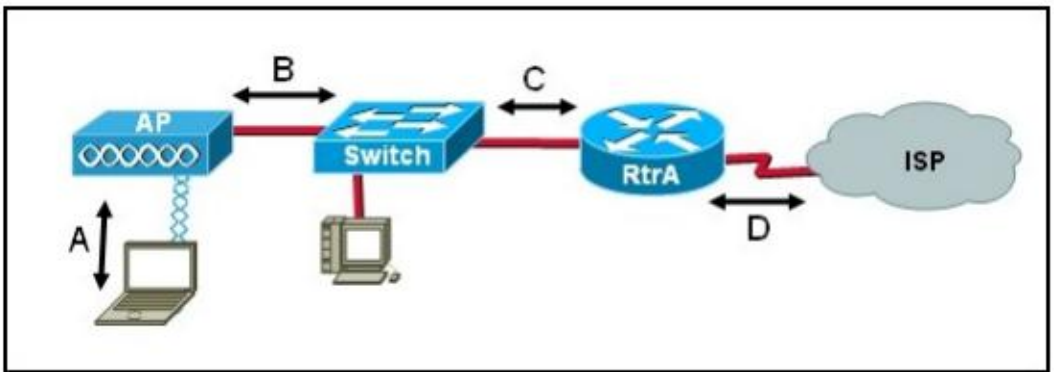
Σωστές απαντήσεις: 1 και 3.

Το TCP εξασφαλίζει την μεταφορά των δεδομένων και ταυτόχρονα στόχο έχει την δημιουργία των λεγόμενων εικονικών κυκλωμάτων για την μεταφορά των δεδομένων. (ενότητα 2.4)

Ερώτηση 2.

Με βάση την παρακάτω εικόνα ποιος τύπος ενθυλάκωσης στο Επίπεδο 2 μπορεί να χρησιμοποιηθεί με στόχο την σύνδεση D με βάση τις παρακάτω ρυθμίσεις στο δρομολογητή ;

Refer to the exhibit. What type of Layer 2 encapsulation will be used for connection D on the basis of this configuration on a newly installed router:




```
RtrA(config)# interface serial0/0/0
RtrA(config-if)# ip address 128.107.0.2 255.255.255.252
RtrA(config-if)# no shutdown
```

1. Ethernet
2. Frame Relay
3. HDLC

4. PPP

Σωστή απάντηση: 3.

Έχουμε σύνδεση από απόσταση με σειριακή γραμμή οπότε έχουμε το πρωτόκολλο. Δεν φαίνεται να υπάρχει ρύθμιση για Frame Relay ή PPP οπότε έχουμε προεπιλογή το HDLC (Ενότητα 2.4)

Ερώτηση 3.

Επίλεξε τρεις επιλογές για το πρωτόκολλο TCP που αφορά το επίπεδο εφαρμογών.

What are three examples of TCP/IP application layer protocols? (Choose three.)

1. ένα τερματικό πρωτόκολλο εξομοίωσης που υποστηρίζει απομακρυσμένες συνδέσεις με διάφορες συσκευές του δικτύου
   a terminal emulation protocol that supports remote console connections with various network devices
2. ένα πρωτόκολλο που δημιουργήθηκε από την IBM που καθιστά ευκολότερο για τους υπολογιστές για να συνδεθείτε σε απομακρυσμένα γραφεία
   a protocol created by IBM that makes it easier for mainframes to connect to remote offices
3. ένα πρωτόκολλο υπεύθυνο για τη μεταφορά ηλεκτρονικού ταχυδρομείου σε δίκτυα TCP / IP και στο Διαδίκτυο
   a protocol responsible for transporting electronic mail on TCP/IP networks and the Internet
4. ένα πρωτόκολλο που ελέγχει τον ρυθμό με τον οποίο τα δεδομένα αποστέλλονται σε άλλο υπολογιστή
   a protocol that controls the rate at which data is sent to another computer
5. ένα πρωτόκολλο που ανταλλάσσει πληροφορίες για τη διαχείριση του δικτύου μεταξύ μιας συσκευής δικτύου και μια κονσόλα διαχείρισης
   a protocol that exchanges network management information between a network device and a management console

6. ένα πρωτόκολλο που διεξάγει δοκιμή της διαδρομής μέσω της οποίας ένα πακέτο ταξιδεύει από την πηγή στον προορισμό
   a protocol that conducts a test of the path through which a packet travels from source to destination

Σωστές απαντήσεις: 1,3,5.

Το επίπεδο εφαρμογών είναι υπεύθυνο για τον τρόπο που μια εφαρμογή θα προετοιμάσει τα πακέτα της προκειμένου να σταλούν μέσω δικτύου. Αφορά τον τελικό προορισμό των πακέτων ή την αρχή μετάδοσης τους. (ενότητα 2.4)

Ερώτηση 4.

Ποιοι είναι τρεις παράγοντες που συμβάλουν στην συμφόρηση ενός Ethernet LAN?

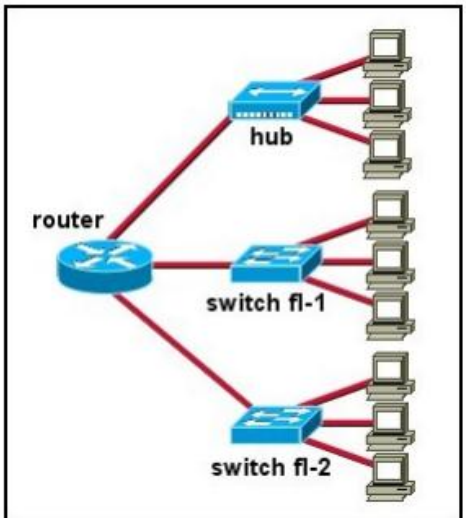
Which three factors contribute to congestion on an Ethernet LAN? (Choose three.)

1. ακατάλληλη τοποθέτηση των servers στο χώρο μιας επιχείρησης
   improper placement of enterprise level servers
2. Προσθήκη τερματικών συσκευών στο φυσικό επίπεδο
   addition of hosts to a physical segment
3. Αντικατάσταση των hum από switches
   replacement of hubs with workgroup switches
4. Αύξηση του bandwidth στα τερματικά με δικτυακές εφαρμογές
   increasing use of bandwidth intensive network applications
5. δημιουργία νέων περιοχών σύγκρουσης χωρίς την προσθήκη δικτυακών συσκευών
   creation of new collision domains without first adding network hosts
6. μετάβαση σε full-duplex Ethernet εντός του LAN
   migration to full-duplex Ethernet within the LAN

Σωστές απαντήσεις: 1,2,4.

Οι παραπάνω παράγοντες επηρεάζουν την συμφόρηση του δικτύου ακόμα κι αν αυτό δεν είναι LAN. (ενότητα 2.2)

Ερώτηση 5.



Με βάση την παραπάνω εικόνα κρίνετε το παρακάτω. Όλες οι πόρτες του switch fl-1 είναι στο Production VLAN και όλες οι πόρτες του switch fl-2 είναι στο Development VLAN. Πόσα broadcast domains και πόσα collision domains υπάρχουν στο δίκτυο (2 επιλογές);

Refer to the exhibit. All ports on switch fl-1 are in the Production VLAN and all ports on switch fl-2 are in the Development VLAN. How many broadcast domains and how many collision domains are in the network? (Choose two.)

1. one broadcast domain
2. three broadcast domains
3. three collision domains
4. five broadcast domains
5. nine collision domains
6. ten collision domains

Σωστές απαντήσεις: 2,5

Ο λόγος είναι ότι έχουμε ουσιαστικά 3 τμήματα στο δίκτυο μας, 1 το VLAN Production και το VLAN Development που σπάει το δίκτυο και δεν αφήνει broadcast μηνύματα από το Hub και 9 collision domains που είναι ουσιαστικά κάθε θύρα από κάθε switch και 1 collision domain από το hub. Ενότητα (4.2,4.1,2.4)

Ερώτηση 6.

Ένας διαχειριστής δικτύων χρειάζεται να ρυθμίσει 3 τοπικά δίκτυα. Τα δίκτυα έχουν τις παρακάτω προδιαγραφές:

Network1 – 500 hosts

Network 2 - 100 hosts

Network 3 - 1000 hosts

Επίλεξε 3 μάσκες δικτύου που μπορούν να χρησιμοποιηθούν για να έχουμε ικανοποίηση των παραπάνω απαιτήσεων.

A network administrator needs to configure three local networks. The networks have these requirements:

Network 1 - 500 hosts

Network 2 - 100 hosts

Network 3 - 1000 hosts

Which three subnet masks will be needed to fulfill these requirements? (Choose three.)

1. 255.255.0.0
2. 255.255.255.0
3. 255.255.254.0
4. 255.255.252.0
5. 255.255.248.0
6. 255.255.255.128
7. 255.255.255.192

Σωστές απαντήσεις: 3,4,6

Οι μάσκες 3,4,5 δίνουν την δυνατότητα 2^9, 2^{10},2^{11} hosts ανά δίκτυο. Ενότητα (2.5)

Ερώτηση 7.

Ποια διεύθυνση από τις παρακάτω είναι διεύθυνση unicast IPv6

Which address is a valid IPv6 unicast address?

1. FE90::1::FFFF
2. FD80::1::1234
3. FE80::1:4545:6578:ABC1
4. FEA0::100::7788:998F
5. FC90::::5678:4251:FFFF

Σωστή απάντηση: 3

Μία unicast IPv6 ξεκινούν με το fe80 και πρέπει να είναι /64 οπότε το 3 είναι σύμφωνο.

(Ενότητα 2.6)

Ερώτηση 8.

Με βάση την διεύθυνση 255.255.224.0 ποιες 3 διευθύνσεις είναι σωστές host addresses

Assuming a subnet mask of 255.255.224.0, which three addresses would be valid host addresses

1. 10.78.103.0
2. 10.67.32.0
3. 10.78.160.0
4. 10.78.48.0
5. 172.55.96.0
6. 172.211.100.0

Σωστές απαντήσεις : 1,4,6

Παίρνουμε κάθε διεύθυνση και την μετατρέπουμε σε δυαδική μορφή όπως και το subnet mask. Μια host διεύθυνση εμφανίζει μονάδες (όχι όμως μόνο μονάδες) στο χώρο όπου η subnet mask έχει 0. (ενότητα 2.5)

Ερώτηση 9.

Τι τύπος διεύθυνσης είναι η διεύθυνση 172.16.134.48/27

What type of IP address is 172.16.134.48/27

1. a useable host address
2. a broadcast address
3. a network address
4. a multicast address
5. a public address

Σωστή απάντηση : 1

Για τον ίδιο λόγο με την προηγούμενη ερώτηση (ενότητα 2.5)

Ερώτηση 10.

Ποιόν πίνακα ο αλγόριθμος EIGRP DUAL χρησιμοποιεί για να υπολογίσει την καλύτερη δρομολόγηση για κάθε router?

What table does the EIGRP DUAL algorithm use to calculate the best route to each destination router?

1. routing table
2. topology table
3. DUAL table
4. MAC table
5. ARP table

Σωστή απάντηση : 2.

Ο EIGRP DUAL χρησιμοποιεί έναν πίνακα topology που με βάση αυτόν υπολογίζει την λεγόμενη βέλτιστη διαδρομή. (ενότητα 3.9)

Ερώτηση 11.

Ποια είναι 2 μέτρα που χρησιμοποιούνται για να αποφευχθούν οι κλειστεί βρόγχοι στην δρομολόγηση στα λεγόμενα distance vector πρωτόκολλα δρομολόγησης

What two measures are used to prevent routing loops in networks that use distance vector routing protocols? (Choose two.)

1. link-state advertisements (LSA)
2. Spanning Tree Protocol
3. shortest path first tree
4. split horizon
5. hold-down timers

Σωστές απαντήσεις : 4,5.

Στους Distance Vectors ρόλο παίζει ο χρόνος και η μέθοδος split horizon για να μην έχουμε loops. (ενότητα 3.5)

Ερώτηση 12.

Τι περιγράφει καλύτερα την διαδικασία των distance vector πρωτοκόλλων δρομολόγησζη;

What best describes the operation of distance vector routing protocols?

1. Χρησιμοποιούν αρίθμηση των hops σαν μοναδικό μέτρο
   They use hop count as their only metric.
2. Στέλνουν ενημέρωση μόνο όταν ένα νέο δίκτυο προστεθεί
   They only send out updates when a new network is added.

3. Στέλνουν τον πίνακα δρομολόγησης στους άμεσα συνδεδεμένους γείτονες
   They send their routing tables to directly connected neighbors.
4. Κατακλύζουν το δίκτυο με μηνύματα ενημέρωσης
   They flood the entire network with routing updates.

Σωστή απάντηση : 3

Πραγματικά σε αυτούς τους αλγόριθμους κάθε κόμβος στέλνει στους γείτονές του τον πίνακα δρομολόγησης του και ανάλογα με το εξεταζόμενο μέτρο υπολογίζεται σε κάθε κόμβο το κατάλληλο μονοπάτι με το μικρότερο μέτρο. (ενότητα 3.5)

Ερώτηση 13.

Ένας router έχει καταχωρήσει το δίκτυο 192.168.168.0 μέσα από static και dynamic routing διαδικασίες. Ποια δρομολόγηση εμφανίζεται στον routing table αν έχουμε πολλαπλές διαδρομές;

A router has learned about network 192.168.168.0 through static and dynamic routing processes. Which route will appear in the routing table for this network if the router has learned multiple routes?

1. D 192.168.168.0/24 [90/2195456] via 192.168.200.1, 00:00:09, FastEthernet0/0
2. 192.168.168.0/24 [110/1012] via 192.168.200.1, 00:00:22, FastEthernet0/0
3. R 192.168.168.0/24 [120/1] via 192.168.200.1, 00:00:17, FastEthernet0/0
4. S 192.168.168.0/24 [1/0] via 192.168.200.1

Σωστή απάντηση : 4

Η στατική δρομολόγηση πάντα υπερισχύει (ενότητα 3.2)

Ερώτηση 14.

Ένας router χρειάζεται να ρυθμιστεί με OSPF στην περιοχή 0. Ποιες είναι 2 σωστές εντολές που υλοποιούν το παραπάνω;

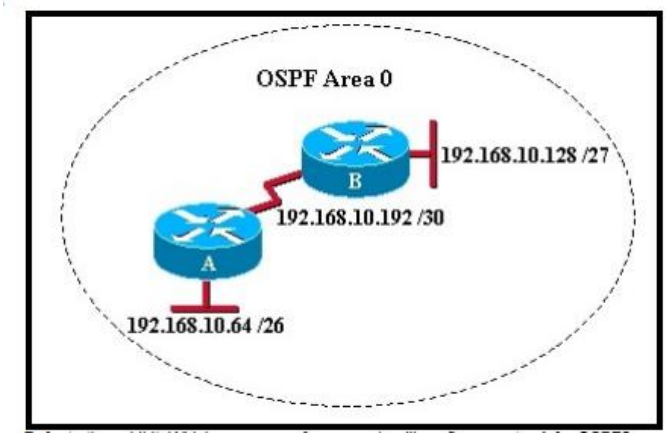
A router needs to be configured to route within OSPF area 0. Which two commands are required to accomplish this? (Choose two.)

1. RouterA(config)# router ospf 0
2. RouterA(config)# router ospf 1
3. RouterA(config-router)# network 192.168.2.0 0.0.0.255 0
4. RouterA(config-router)# network 192.168.2.0 0.0.0.255 area 0
5. RouterA(config-router)# network 192.168.2.0 255.255.255.0 0

Σωστή απάντηση : 2,4

Ορίζουμε ότι θα ρυθμίσουμε στο ospf 1 το δίκτυο 192.168.2.0 με μάσκα 255.255.255.0 στην περιοχή 0.

Ερώτηση 15.



Με βάση την παραπάνω εικόνα ποια σειρά εντολών πρέπει να δώσουμε στον router A για να ρυθμίσουμε το OSPF;

Refer to the exhibit. Which sequence of commands will configure router A for OSPF?

1. router ospf 0
   network 192.168.10.0
   network 192.168.10.192
2. router ospf 0
   network 192.168.10.0

3. router ospf 1
   network 192.168.10.64 0.0.0.63 area 0
   network 192.168.10.192 0.0.0.3 area 0
4. router ospf 1
   network 192.168.10.64 255.255.255.192
   network 192.168.10.192 255.255.255.252
5. router ospf 1
   network 192.168.10.0 area 0

Σωστή απάντηση : 3

Πρέπει κάθε network να ορίζει και την area. (ενότητα 3.10 και 5.1)

Ερώτηση 15.

Σε ποιο ασύρματο πρωτόκολλο εργάζεται ένα δίκτυο περιοχής 2.4 GHz που παρέχει ταχύτητα 54 Mb/s.

Which wireless standard works only in the 2.4 GHz range and provides speeds up to 54 Mb/s?

1. 802.11a
2. 802.11b
3. 802.11g
4. 802.11i
5. 802.11n

Σωστή απάντηση : 3

Το πρωτόκολλο 802.11g είναι το καθιερωμένο πρωτόκολλο για ασύρματα δίκτυα για μικρές εταιρίες και κατοικίες.

Ερώτηση 16

Ποια είναι σειρά γενικά που ακολουθείται σε σχέση με τον τρόπο χρήσης των εκτεταμένων access control lists?

What guideline is generally followed about the placement of extended access control lists

1. Θα πρέπει να τοποθετούνται όσο το δυνατόν πλησιέστερα στην πηγή της οποίας η κυκλοφορία πρέπει να απορριφθεί.
   They should be placed as close as possible to the source of the traffic to be denied.
2. Θα πρέπει να τοποθετούνται όσο το δυνατόν πλησιέστερα προς τον προορισμό της κίνησης που πρέπει αρνηθούμε.
   They should be placed as close as possible to the destination of the traffic to be denied.
3. Θα πρέπει να ορίζονται στην ταχύτερη διαθέσιμη διεπαφή.
   They should be placed on the fastest interface available.
4. Θα πρέπει να τοποθετηθεί σχετικά με τον προορισμό της αντίστοιχης WAN σύνδεσης
   They should be placed on the destination WAN link

Σωστή απάντηση : 1

Οι extended access lists τοποθετούνται στον router που δέχεται την κίνηση με στόχο να μην επιτρέπουμε ή το αντίθετο κίνηση προς το δίκτυο μας από συγκεκριμένους προορισμούς. (ενότητα 3.11)

Ερώτηση 17

Ποια 2 από τις παρακάτω λέξεις χρησιμοποιούνται σε access control list για να αλλάξουν μια wildcard μάσκα ή διεύθυνση σε wildcard mask pair?

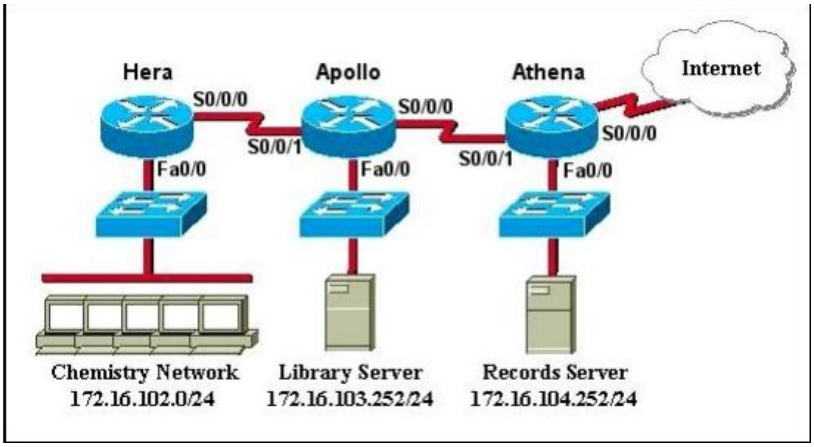
Which two keywords can be used in an access control list to replace a wildcard mask or address and wildcard mask pair? (Choose two.)

1. most
2. host
3. all
4. any
5. some
6. gt

Σωστές απαντήσεις: 2,4

Με τις παραπάνω λέξεις μπορούμε να αναφερθούμε σε ένα host που μπορεί να έχει οποιαδήποτε διεύθυνση ή μάσκα. (ενότητα 3.11)

Ερώτηση 18



Με βάση την παραπάνω εικόνα απαντήστε στο παρακάτω σενάριο: Έχουμε μια access list με το όνομα chemistry_block η οποία αποτρέπει τους χρήστες στο Chemistry δίκτυο και αυτούς από το Internet να έχουν πρόσβαση στον Records Server. Όλοι οι άλλοι χρήστες στο σχολείο έχουν πρόσβαση στον server. Η λίστα περιλαμβάνει τα παρακάτω:

deny 172.16.102.0 0.0.0.255 172.16.104.252 0.0.0.0

permit 172.16.0.0 0.0.255.255 172.16.104.252 0.0.0.0

Ποια είναι η σειρά των εντολών που πρέπει να δοθεί ώστε να έχουμε τα παρακάτω:

Refer to the exhibit. A named access list called chemistry_block has been written to prevent users on the Chemistry Network and public Internet from access to the Records Server. All other users within the school should have access to this server. The list contains the following statements:

deny 172.16.102.0 0.0.0.255 172.16.104.252 0.0.0.0

permit 172.16.0.0 0.0.255.255 172.16.104.252 0.0.0.0

Which command sequence will place this list to meet these requirements?

1. Hera(config)# interface fa0/0
   Hera(config-if)# ip access-group chemistry_block in
2. Hera(config)# interface s0/0/0
   Hera(config-if)# ip access-group chemistry_block out
3. Apollo(config)# interface s0/0/0
   Apollo(config-if)# ip access-group chemistry_block out
4. Apollo(config)# interface s0/0/1
   Apollo(config-if)# ip access-group chemistry_block in
5. Athena(config)# interface s0/0/1
   Athena(config-if)# ip access-group chemistry_block in
6. Athena(config)# interface fa0/0
   Athena(config-if)# ip access-group chemistry_block out

Σωστή απάντηση: 1

Τοποθετούμε τον κανόνα της Action list στον δρομολογητή που βγαίνει η κίνηση ώστε να μην στέλνονται μηνύματα προς το server. (ενότητα 3.11)

Ερώτηση 19

Ποια η διαφορά του RIP v1 και του RIP v2

How do RIP v1 and RIP v2 differ?

Μόνο το RIP v1 παρέχει αυθεντικοποίηση σε κάθε ενημέρωση

1. Only RIP v1 provides authentication in its update.

Μόνο το RIP v1 χρησιμοποιεί το split horizon για να αποτρέψει τους κλειστούς βρόχους.

2. Only RIP v1 uses split horizon to prevent routing loops.

   Μόνο το RIP v2 χρησιμοποιεί 16 άλματα σαν μετρικό για άπειρη απόσταση.

3. Only RIP v2 uses 16 hops as the metric value for infinite distance.

   Μόνο το RIP v2 στέλνει την μάσκα υποδικτύου μαζί με τους πίνακες δρομολόγησης.

4. Only RIP v2 send subnet mask information with its routing updates

Σωστές απαντήσεις: 4

Το πρωτόκολλο RIP v2 με κάθε routing update στέλνει και την μάσκα υποδικτύου καθώς υποστηρίζει classless routing , σε αντίθεση με το RIP v1 το οποίο υποστηρίζει classful routing και αποστέλλει μόνο τους πίνακες δρομολόγησης

Ερώτηση 20

Ποιο είναι το προεπιλεγμένο πρωτόκολλο ενθυλάκωσης στο επίπεδο 2 για συγχρονισμό ενός serial interface στους Cisco δρομολογητές ;

What is the default Layer 2 encapsulation protocol for a synchronous serial interface on a Cisco router?

PPP

HDLC

Frame Relay

CHAP

IEEE 802.1Q

Σωστή απάντηση: 2

Το HDLC είναι ένα αρκετά παλιό πρωτόκολλο και χρησιμοποιείται κατά κόρον για συνδέσεις point-to-point. Θεωρείται το προεπιλεγμένο πρότυπο της CISCO και έχει δημιουργηθεί και υλοποιηθεί από την CISCO. (ενότητα 2.4)

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στόχος της πτυχιακής μας είναι η αποτύπωση της ύλης του CCNA και η σύνδεση της με πρόσθετες γνώσεις δικτύων ώστε τελικά να έχουμε ένα καλύτερο υπόβαθρο από την απλή πρακτική γνώση.

Πιο συγκεκριμένα είδαμε ότι TCP/IP είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων.

Αυτή η συλλογή πρωτοκόλλων, όπως και πολλές άλλες άλλωστε, είναι οργανωμένη σε στρώματα ή επίπεδα (layers). Το καθένα τους απαντά σε συγκεκριμένα προβλήματα μεταφοράς δεδομένων και παρέχει μια καθορισμένη υπηρεσία στα υψηλότερα στρώματα. Τα ανώτερα επίπεδα είναι πιο κοντά στη λογική του χρήστη και εξετάζουν πιο αφηρημένα δεδομένα, στηριζόμενα σε πρωτόκολλα χαμηλότερων στρωμάτων για να μεταφράσουν δεδομένα σε μορφές που μπορούν να διαβιβαστούν με φυσικά μέσα.

Το CCNA εξετάζει την περίπτωση δρομολόγησης στο TCP/IP και πιο συγκεκριμένα περιγράψαμε τα πιο διαδεδομένα πρωτόκολλα δρομολόγησης.

Η δρομολόγηση ουσιαστικά αφορά την δημιουργία των πινάκων δρομολόγησης σε κάθε router.

Αρχικά ορίζουμε τι είναι δρομολόγηση, τα είδη της καθώς και βασικά χαρακτηριστικά της δρομολόγησης. Στην συνέχεια θα ορίσουμε τι είναι ένας αλγόριθμος δρομολόγησης, τις βασικές στρατηγικές δρομολόγησης, και τις βασικότερες μορφές που εξάγεται ο πίνακας δρομολόγησης.

Κάθε πρωτόκολλο εφαρμόζει ένα αλγόριθμο δρομολόγησης μέσω του οποίου προκύπτουν οι σωστοί πίνακες δρομολόγησης ανά περίπτωση.

Για το λόγο αυτό παραθέσαμε τους γνωστότερους αλγόριθμους δρομολόγησης και πως εφαρμόζονται αυτοί στα αντίστοιχα πρωτόκολλα.

Στο παράρτημα που ακολουθεί μετά την βιβλιογραφία δίνονται σειρά ασκήσεων και ερωτήσεων από την εξεταστέα ύλη του CCNA όπως ακριβώς εξετάζονται στο CCNA.

Έτσι κάποιος λύνοντας τις ασκήσεις που δίνονται μπορεί με σιγουριά να γνωρίζει αν είναι ικανός να δώσει εξετάσεις για την απόκτηση του ανάλογου πιστοποιητικού.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α

1. Tanenbaum, Andrew S. [1996] 2000, "Δίκτυα Υπολογιστών", Τρίτη Έκδοση, Πρώτη Ελληνική Έκδοση, Εκδόσεις Παπασωτηρίου, ISBN 960-7510-70-4

2. CCENT ICND1 100-101 Network Simulator, Wendell Odom, Sean Wilkins, Published Oct 16, 2013 by Pearson IT Certification.

3. CCNA Routing and Switching ICND2 200-101 Network Simulator, Download Version,Wendell Odom, Sean Wilkins, Published Nov 22, 2013 by Pearson IT Certification.

4. CCNA Routing and Switching 200-120 Network Simulator, Wendell Odom, Sean Wilkins, Published Dec 19, 2013 by Pearson IT Certification.

5. CCNA Routing and Switching 200-120 Official Cert Guide Library,Wendell Odom, Published May 23, 2013 by Cisco Press.

6. CCNP Routing and Switching ROUTE 300-101 Complete Video Course, Kevin Wallace, Published Oct 27, 2014 by Pearson IT Certification.

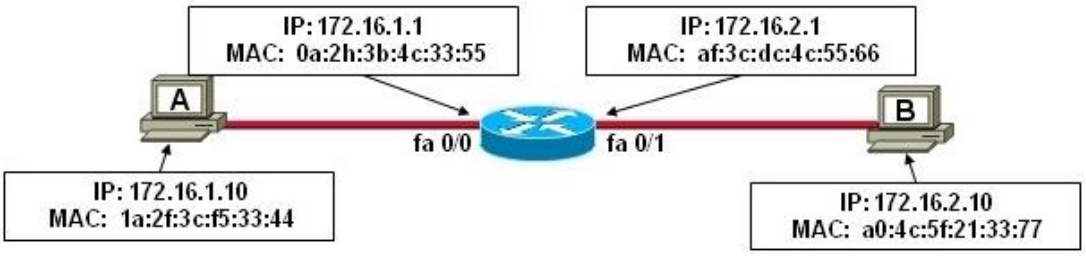
7. CCNP Routing and Switching Foundation Learning Library: (ROUTE 300-101, SWITCH 300-115, TSHOOT 300-135), Diane Teare, Richard Froom, Erum Frahim, Amir Ranjbar, Rick Graziani, Bob Vachon, Published May 15, 2015 by Cisco Press.

8. https://el.wikipedia.org/wiki/Δίκτυο_υπολογιστών, Published ΣΕΠΤ 25, 2015 el.wikipedia.org

ΠΑΡΑΡΤΗΜΑ

ΑΣΚΗΣΕΙΣ ΣΤΟ CCNA

Ενδεικτικό Τεστ CCNA



Questions and Answers CCENT

1. What are two ways that TCP uses the sequence numbers in a segment? (Choose two.)

A. To identify missing segments at the destination

B. To reassemble the segments at the remote location

C. To specify the order in which the segments travel from source to destination

D. To limit the number of segments that can be sent out of an interface at one time

E. To determine if the packet changed during transit

2. Which three statements characterize UDP? (Choose three.)

A. UDP provides connectionless, fast transport of data at Layer 4.

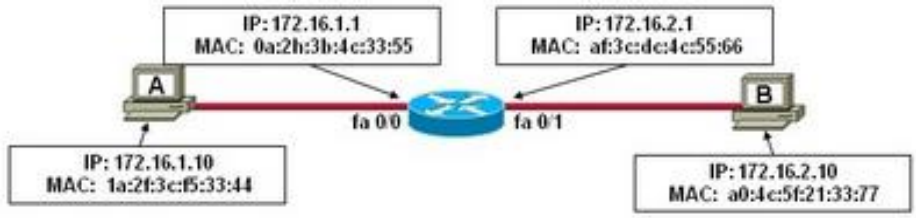
B. UDP provides connection-oriented, fast transport of data at Layer 3.

C. UDP relies on application layer protocols for error detection.

D. UDP works well when an application does not need to guarantee delivery of data.

E. UDP relies on IP for error detection and recovery.

3.



Refer to the exhibit. Host A sends a data packet to host B. What will be the addressing information of the data packet when it reaches host B? A: B: C: D:

A. Image A

B. Image B

C. Image C

D. Image D

4. Which layer of the OSI model defines logical addressing?

A. Application

B. Presentation

C. Session

D. Transport

E. Network

5. Which device connects a local LAN to a geographically separate network?

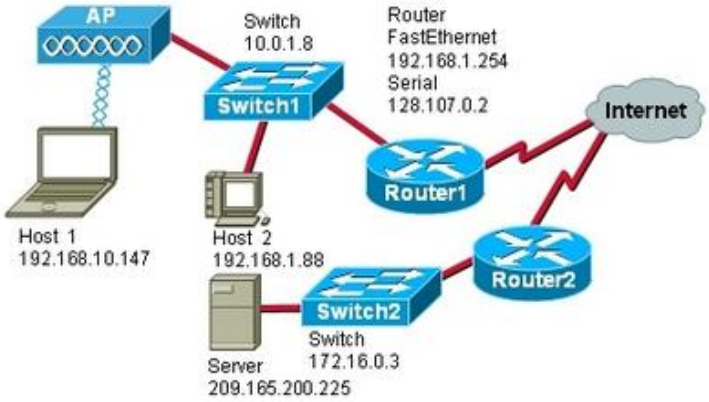
A. Switch

B. Hub

C. Router

D. Bridge

6. Refer to the exhibit. Router1 receives packets addressed as follows: Source IP address: 192.168.1.88Destination IP address: 172.16.0.3Source MAC address: 00-11-12-7a-41-10Destination MAC address: 00-11-5c-cc-a9-c0Source Port: 1464Destination Port: 23 Assuming that Router1 has not been configured with NAT, what will happen to the packets?



A. The packets will be sent to the server because it is a server-based port.

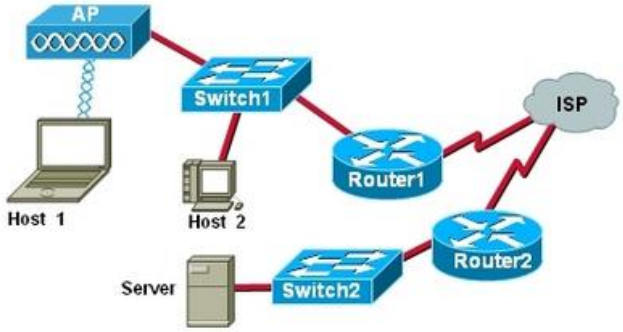
B. The packets will be sent to Switch2 and not leave the switch because the packets are local.

C. The packets will be sent to the laptop host.

D. The packets will be sent to Router1 and dropped because private addresses are not transmitted across the Internet.

E. The packets will be sent to Router2 and dropped because the server is not directly attached.

7. Refer to the exhibit. If host 1 was to send an HTTP request to the web server that connects to Router2, what type of Layer 2 frame would be sent between Router1 and the ISP?



A. A frame with a header that contains the port number of 80

B. A frame with a header and trailer, but no MAC addresses

C. A frame with a header and a trailer that only contains IP addresses

D. A frame with the host 1 MAC address as the source and Router1 MAC address as the destination

E. A frame with the host 1 MAC address as the source and the server MAC address as the destination

8. A company needs to connect an office router to a service provider to access a WAN. What device is needed to connect the router to the ISP if the service provider supplies a T1 line for the connection?

A. A CSU/DSU

B. A cable modem

C. A DSL router

D. A DTE device

E. An SLA device

9. Refer to the exhibit. A technician applies the configuration in the exhibit to an unconfigured router. To verify the configuration, the technician issues the show running-config command in the CLI session with the router. What lines should the technician expect to see in the router output from the show running-config command?

```
Router(config)# service password-encryption
Router(config)# enable secret cisco
Router(config)# enable password class
Router(config)# line console 0
Router(config-line)# password ccna
```

A. Enable password class

line console 0

password ccna

B. Enable secret cisco

enable password class

line console 0

password ccna

C. Enable secret 5 1v0/3$QyQWmJyT7zCa/yaBRasJm0

enable password class

line console 0

password ccna

D. Enable secret cisco

enable password 7 14141E0A1F17

line console 0

password 7 020507550A

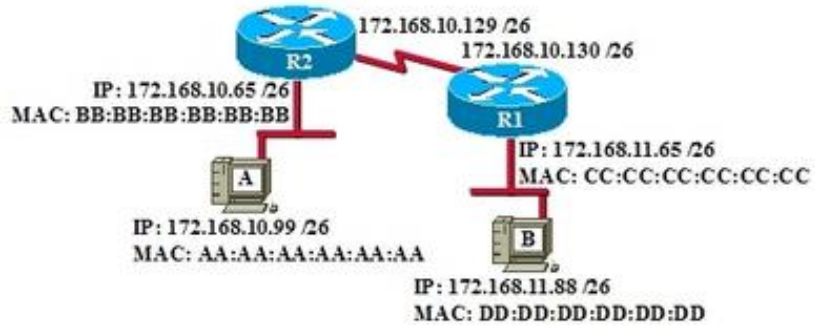
E. Enable secret 5 1v0/3$QyQWmJyT7zCa/yaBRasJm0

enable password 7 14141E0A1F17

line console 0

password 7 020507550A

10. Refer to the exhibit. If host A sends an IP packet to host B, what will the destination address be in the frame when it leaves host A?



A. DD:DD:DD:DD:DD:DD

B. 172.168.10.99

C. CC:CC:CC:CC:CC:CC

D. 172.168.10.65

E. BB:BB:BB:BB:BB:BB

11. Refer to the exhibit. What two facts can be determined from the output of the ping command? (Choose two.)

```
Router1> ping 172.16.101.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.101.2,
Timeout is 2 seconds:
.!!!!
Success rate is 80 percent, round-trip min/avg/max=6/6/6 ms
Router1>
```

A. There was a destination unreachable error.

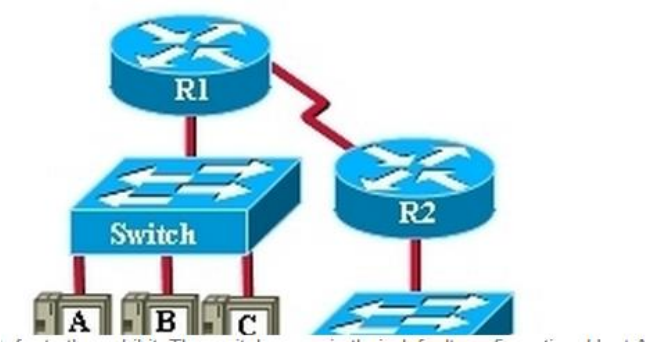
B. The packet type was unknown.

C. One packet timed out.

D. The ping was interrupted.

E. Four packets of data were successfully received.

12. Refer to the exhibit. The switches are in their default configuration. Host A needs to communicate with host D, but host A does not have the MAC address for its default gateway. Which network hosts will receive the ARP request sent by host A?



A. Only host D

B. Only router R1

C. Only hosts A, B, C, and D

D. Only hosts B and C

E. Only hosts B, C, and router R1

13. Refer to the exhibit. Which password will the administrator need to use on this device to enter privileged EXEC mode?

```
Switch> enable
Switch# config terminal
Switch(config)# enable password Cisco
Switch(config)# enable secret cisco
Switch(config)# line con 0
Switch(config-line)# password password
Switch(config-line)# login
Switch(config-line)# end
Switch(config)# line vty 0 15
Switch(config-line)# password class
```

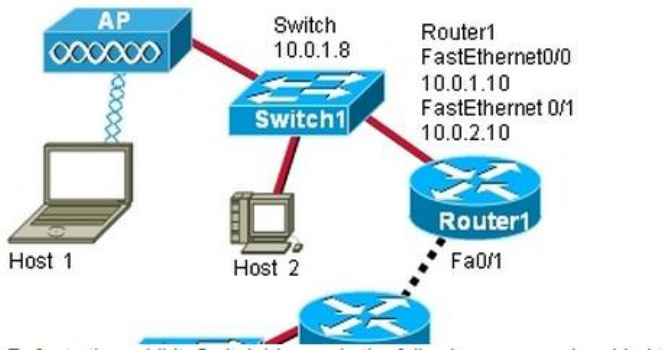
A. Cisco

B. Class

C. Password

D. Cisco

14. Refer to the exhibit. Switch1 has only the following commands added to a default Cisco 2960 configuration: enable secret cisco line vty 0 4 password Kn0ckkn-cK login interface vlan 1 ip address 10.0.1.8 255.255.255.0 no shutdown Assume that routing between networks is functioning properly and that Switch2 has been properly configured for remote access. What would the result be if the telnet 10.0.2.2 command is issued from Switch1 privileged mode?



A. The following prompt would appear:

User Access Verification

Password:

B. Switch2 would return a destination unreachable message to Switch1.

C. Router1 would return a destination unreachable message to Switch1.

D. The packet would be dropped.

15. What caused the following error message to appear? 01:11:12: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/8, putting Fa0/8 in err-disable state 01:11:12: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0011.a0d4.12a0 on port FastEthernet0/8.01:11:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down 01:11:14: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down

A. Another switch was connected to this switch port with the wrong cable.

B. An unauthorized user tried to telnet to the switch through switch port Fa0/8.

C. NAT was enabled on a router, and a private IP address arrived on switch port Fa0/8.

D. A host with an invalid IP address was connected to a switch port that was previously unused.

E. Port security was enabled on the switch port, and an unauthorized connection was made on switch port Fa0/8.

16. When configuring a switch to use SSH for virtual terminal connections, what is the purpose of the crypto key generate rsa command?

A. Show SSH connected hosts

B. Disconnect SSH connected hosts

C. Create a public and private key pair

D. Show active SSH ports on the switch

E. Access the SSH database configuration

17. Which three statements are true about full-duplex operation on an Ethernet network? (Choose three.)

A. There are no collisions in full-duplex mode.

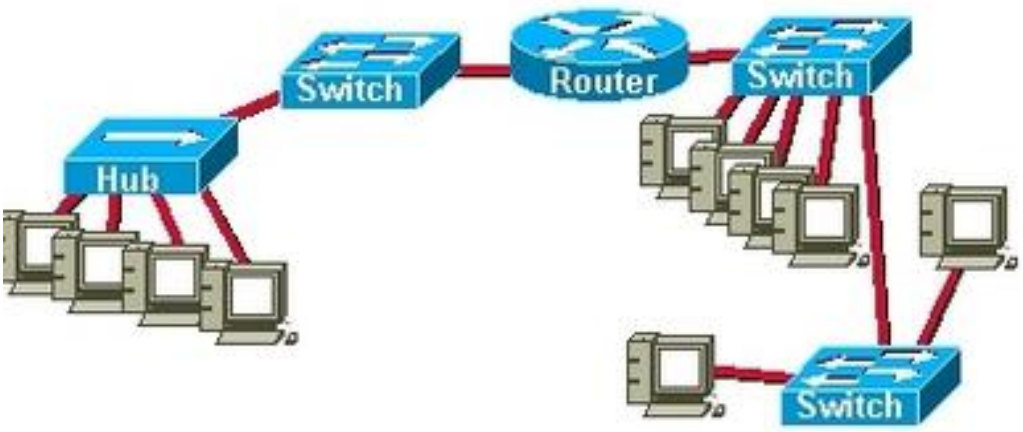
B. A dedicated switch port is required for each node.

C. Hub ports are preconfigured for full-duplex mode.

D. The host network card must detect the availability of the media before transmitting.

E. The host network card and the switch port must both be in full-duplex mode.

18.



A. 1

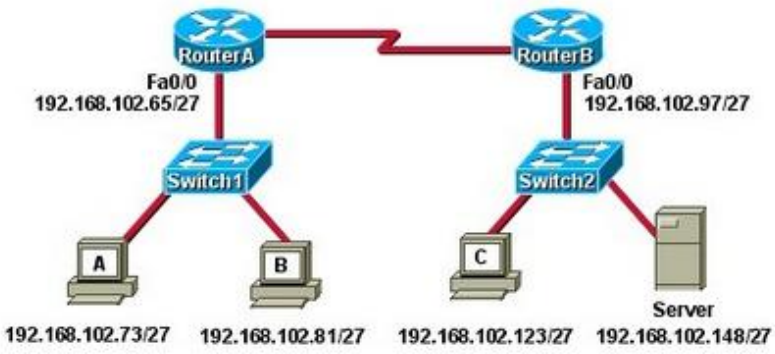
B. 2

C. 3

D. 4

E. 14

20. Refer to the exhibit. The devices have been configured with static IP addresses as shown. All hosts can communicate with each other but none of the hosts can communicate with the server. What is the cause of this problem?



A. The IP address that is assigned to the server is in an incorrect subnet.

B. The IP address that is assigned to the server is a broadcast address.

C. The IP address that is assigned to the server is a network address.

D. The switch to which the server is connected has not been assigned an IP address.

E. The RouterB LAN interface is incorrectly addressed in the RouterA LAN subnet.

21. A network host has the IP address 10.250.206.55/20. How many more network devices can be added to this same subnetwork?

A. 253

B. 509

C. 1021

D. 2045

E. 4093

22. Which type of Network Address Translation allows a host on a public network consistent access to a specified private inside host?

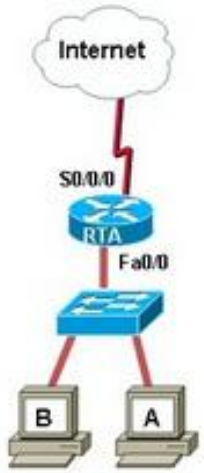
A. Port-based NAT

B. Static NAT

C. Dynamic NAT

D. NAT overload

23. Refer to the exhibit. Which two addresses are "inside global" addresses? (Choose two.)




```
RTA# show running-config
<output omitted>
!
ip subnet-zero
!
interface fastethernet0/0
ip address 192.168.7.1 255.255.255.0
ip nat inside
!
interface serial 0/0/0
ip address 64.100.1.5 255.255.255.252
ip nat outside
!
ip nat pool OUTSIDE 198.133.219.33 198.133.219.62 netmask
255.255.255.224
ip nat inside source list 1 pool OUTSIDE
!
ip route 0.0.0.0 0.0.0.0 64.100.1.6
access-list 1 permit 192.168.7.0 0.0.0.255
```

A. 192.168.7.3

B. 64.100.1.5

C. 198.133.219.35

D. 192.168.7.2

E. 198.133.219.44

24. Which addresses are valid host IP addresses given the subnet mask 255.255.255.248? (Choose three.)

A. 192.168.200.87

B. 194.10.10.104

C. 223.168.210.100

D. 220.100.100.154

E. 196.123.142.190

25. The router receives a packet with the destination address of 172.16.30.79. To which subnetwork does this packet belong?

A. 172.16.30.0/22

B. 172.16.30.64/22

C. 172.16.30.76/22

D. 172.16.28.0/22

E. 172.16.28.56/22

26. Refer to the exhibit. What is the broadcast address for the subnetwork on which host A resides?

A. 10.255.255.255

B. 10.144.255.255

C. 10.149.255.255

D. 10.149.191.255

E. 10.159.255.255

28. What can a network administrator modify on a router to specify the location from which the Cisco IOS loads? (Choose two.)

A. System ROM

B. The startup configuration file

C. The system image file

D. The configuration register value

E. The NVRAM file system

29. Which two items are required for initial configuration of Cisco routers if the IOS command-line interface is used? (Choose two.)

A. A crossover cable

B. A rollover cable

C. An RJ-15 to DB-9 adapter

D. Terminal emulation software

E. Router VTY port

30. Refer to the exhibit. The router named "myhome" has received a frame from the host 192.168.254.7. The contents of this frame are being sent to host 172.16.14.243. What is the Layer 2 destination address of the frame as it leaves the myhome router?

```
myhome# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.14.129           0  0009.1281.18a8  ARPA   Ethernet1
Internet  172.16.14.243           -  0008.a3b6.ce05  ARPA   Ethernet1
Internet  192.168.254.7           1  000a.8a47.e612  ARPA   Ethernet0
Internet  192.168.254.4          33  000d.5609.fbd1  ARPA   Ethernet0
Internet  192.168.254.1           -  0008.a3b6.ce04  ARPA   Ethernet0
Internet  192.168.254.9          12  000f.3d4e.235f  ARPA   Ethernet0
Internet  192.168.254.86         14  0006.2554.b16c  ARPA   Ethernet0
```

A. 0008.a3b6.ce05

B. 0009.1281.18a8

C. 00a.8a47.e612

D. 172.16.14.129

E. 172.16.14.243

31. Refer to the exhibit. What two facts can be determined about the network from the exhibited output? (Choose two.)

```
MontegoBay> show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intrfce   Holdtme   Capability  Platform        Port ID
Negril         Ser 0/1         146          R      2620            Ser 0/1
Lucia          Ser 0/0         175          R      2621            Ser 0/0
MBSwitch       Fas 0/0         155          S I    WS-C2950-2      Fas 0/11
```

A. The MontegoBay router does not have any LAN interfaces configured.

B. The Negril router is connected to the S0/1 interface of the MontegoBay router.

C. There are only four devices in this network.

D. Layer 3 is functioning properly on all routers.

E. Layer 2 is operational on three ports of the MontegoBay router.

32. Which set of commands is used to name a router and save the configuration?

A.

Router(config)# hostname South

South(config)# copy running-config startup-config

B.

Router(config)# hostname South

South(config)# exit

South# copy running-config startup-config

C.

Router(config)# ip host South

South(config)# copy running-config startup-config

D.

Router(config)# ip host South

South(config)# exit

South# copy running-config startup-config

33. Which command is used to create an encrypted password that restricts access to the privileged EXEC mode of a Cisco router?

A. RouterA(config)# encrypted password cisco

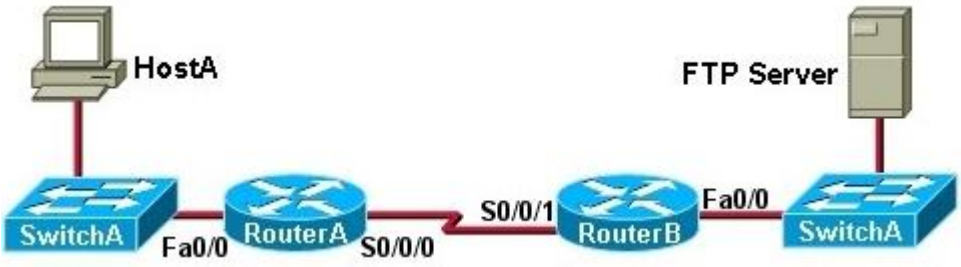
B. RouterA(config)# password encrypted cisco

C. RouterA(config)# enable password cisco

D. RouterA(config)# enable secret cisco

E. RouterA(config)# service-password encryption cisco

34. Refer to the exhibit. A network administrator working at HostA has problems accessing the FTP server. Layer 3 connectivity testing was successful from HostA to the S0/0/1 interface of RouterB. Which set of commands will allow the network administrator to telnet to RouterB to check its status?



A.

RouterB(config)# enable secret class

RouterB(config)# line vty 0 4

RouterB(config-if)# login

B.

RouterB(config)# enable secret class

RouterB(config)# line vty 0

RouterB(config-line)# password cisco

RouterB(config-line)# login

C.

RouterB(config)# enable secret class

RouterB(config)# line aux 0

RouterB(config-line)# password cisco

RouterB(config-line)# login

D.

RouterB(config)# enable secret class

RouterB(config)# line aux 0

RouterB(config-vty)# password cisco

RouterB(config-vty)# login

35. What is the purpose of using SSH to connect to a router?

A. It allows a router to be configured using a graphical interface.

B. It allows a secure remote connection to the router command line interface.

C. It allows the router to be monitored through a network management application.

D. It allows secure transfer of the IOS software image from an unsecure workstation or server.

36. Which two statements describe the command ip route 192.168.7.24 255.255.255.248 192.168.7.9? (Choose two.)

A. A packet that is destined for host 192.168.7.30 will be forwarded to address 192.168.7.9.

B. The address 192.168.7.9 is the destination network for this route.

C. The address 192.168.7.24 is the next-hop router in this command.

D. This command is issued from the interface configuration mode.

E. This command is used to define a static route.

37. Which protocol is described as an enhanced distance vector routing protocol?

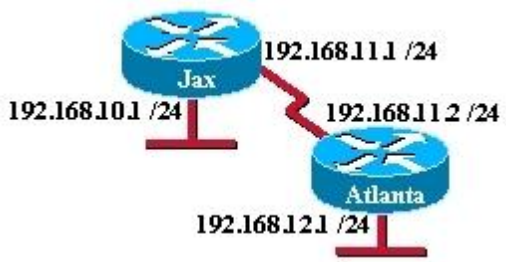
A. RIP v1

B. RIP v2

C. EIGRP

D. OSPF

38. Refer to the exhibit. A network administrator can successfully ping, using IP addresses, between router Jax and router Atlanta. However, when the command telnet Atlanta is entered from the Jax router, the Telnet connection fails. Which two reasons could be the cause of the failure? (Choose two.)



A. The Jax router is not an entry in the host table of the Atlanta router.

B. The Jax router does not have an entry for Atlanta in its host table.

C. The hostname command is not configured correctly on the Atlanta router.

D. The hostname command is not configured correctly on the Jax router.

E. Access to a DNS server is not available.

39. From what two locations can a router load the Cisco IOS during the boot process? (Choose two.)

A. RAM

B. TFTP server

C. NVRAM

D. Setup routine

E. Flash memory

40. Which two statements describe the functions or characteristics of ROM in a router? (Choose two.)

A. Stores routing tables

B. Allows software to be updated without replacing pluggable chips on the motherboard

C. Maintains instructions for POST diagnostics

D. Holds ARP cache

E. Stores bootstrap program

41. Which two statements correctly identify the function of router memory components? (Choose two.)

A. RAM permanently stores the configuration file used during the boot sequence.

B. ROM contains diagnostic self test procedures executed on hardware modules.

C. NVRAM stores a backup copy of the IOS used during the boot sequence.

D. Flash memory does not lose its contents when a router is powered off.

E. Flash contains boot system commands to identify the location of the IOS.

42. Which router component holds the routing table, ARP cache, and running configuration file?

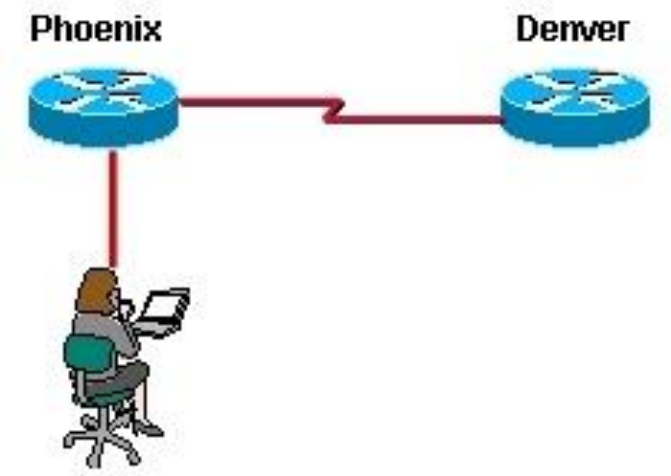
A. RAM

B. Flash

C. NVRAM

D. ROM

43. Refer to the exhibit. A network administrator can ping the Denver router, but gets a 'Password Required but None Set' message when trying to connect remotely via Telnet. Which command or sequence of commands must be applied to the Denver router to allow remote access?



A.

Router(config)# line console 0

Router(config-line)# login

Router(config-line)# password cisco

B.

Router(config)# line vty 0 4

Router(config-line)# login

Router(config-line)# password cisco

C.

Router(config)# line virtual terminal

Router(config-line)# enable login

Router(config-line)# password cisco

D.

Router(config)# line vty 0 4

Router(config-line)# enable secret

Router(config-line)# password cisco

E.

Router(config)# enable secret cisco

45. Which security method uses the Advanced Encryption Standard (AES)?

A. EAP

B. TKIP

C. WEP

D. WPA2

46. What is the purpose of WEP?

A. It encrypts data.

B. It uniquely identifies a wireless network.

C. It coordinates and accepts transmissions from wireless hosts.

D. It provides information about a directly connected Cisco network device.

47. A company has an 802.11b wireless access point installed. Which type of wireless NIC is a valid standards-based one but will not work in this environment?

A. 802.11a

B. 802.11b

C. 802.11g

D. 802.11n

49. A company has a sales team that travels with laptops. On Fridays, the sales members come into assigned cubicles and connect their laptop to the wired network. The company is concerned that unauthorized users could also connect to the network. What can be done to ensure that unauthorized laptops are not connected to the wired network?

A. Implement SSH.

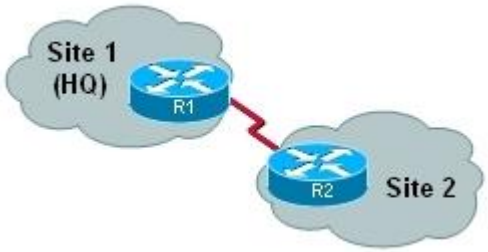
B. Install WEP or WPA.

C. Use switch port security.

D. Clearly label the cubicle network port and the switch port.

E. Configure usernames and passwords on the switch ports assigned to each cubicle.

50. Refer to the exhibit. For security reasons, information about the HQ R1 router model and IP address should not be accessible from the Site 2 R2 router. What security measure should be implemented?



A. Disable CDP on the R1 interface that connects to R2.

B. Disable any routing protocol used between R1 and R2 and install static routes.

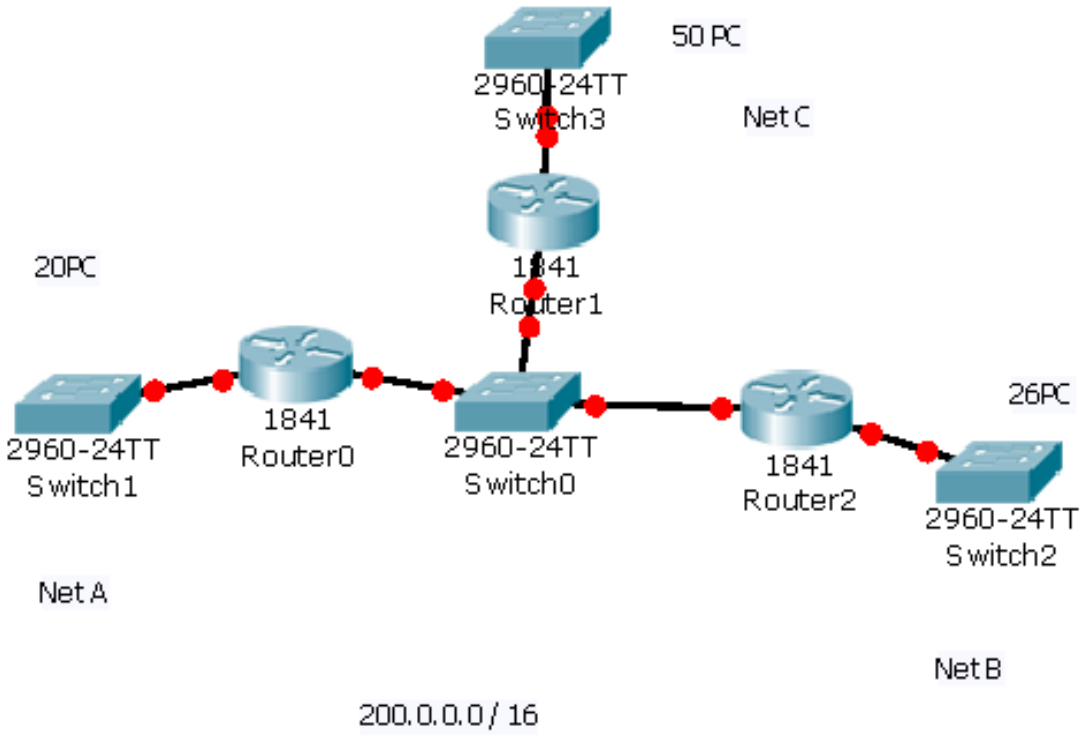
C. Install an IDS between R1 and R2.

D. Install an IPS between R1 and R2.

E. Install a firewall between R1 and R2.

Πρόβλημα 1

Topology Diagram



Task 1

Design the Logical LAN Topology.

Total points: 35

Time: 20 minutes.

Given the IP network 192.168.10.0/25, design an IP addressing scheme that satisfies the following requirements:

Subnet	Number of Hosts
Subnet A	20
Subnet B	26
Subnet C	50
Inter Subnet	3

The all 0s and all 1s subnets are used. No subnet calculators may be used. All work must be shown on the reverse of this Assessment.

Subnet A		
Specification	**Instructor Input**	**Points**
Number of bits in the subnet		(5 points)
IP mask (binary)		
New IP mask (decimal)		
Number of usable hosts per subnet		
IP Subnet		
First IP Host address		
Last IP Host address		

Subnet B		
Specification	**Instructor Input**	**Points**
Number of bits in the subnet		(5 points)
IP mask (binary)		
New IP mask (decimal)		

Number of usable hosts per subnet		
IP Subnet		
First IP Host address		
Last IP Host address		

Subnet C		
Specification	**Instructor Input**	**Points**
Number of bits in the subnet		(5 points)
IP mask (binary)		
New IP mask (decimal)		
Number of usable hosts per subnet		
IP Subnet		
First IP Host address		
Last IP Host address		

Subnet D		
Specification	**Instructor Input**	**Points**
Number of bits in the subnet		(5 points)
IP mask (binary)		
New IP mask (decimal)		

Number of usable hosts per subnet		
IP Subnet		
First IP Host address		
Last IP Host address		

Task2

Use 3 PC for A,B,C Networks and use the first IP addresses of each network.

Task 3

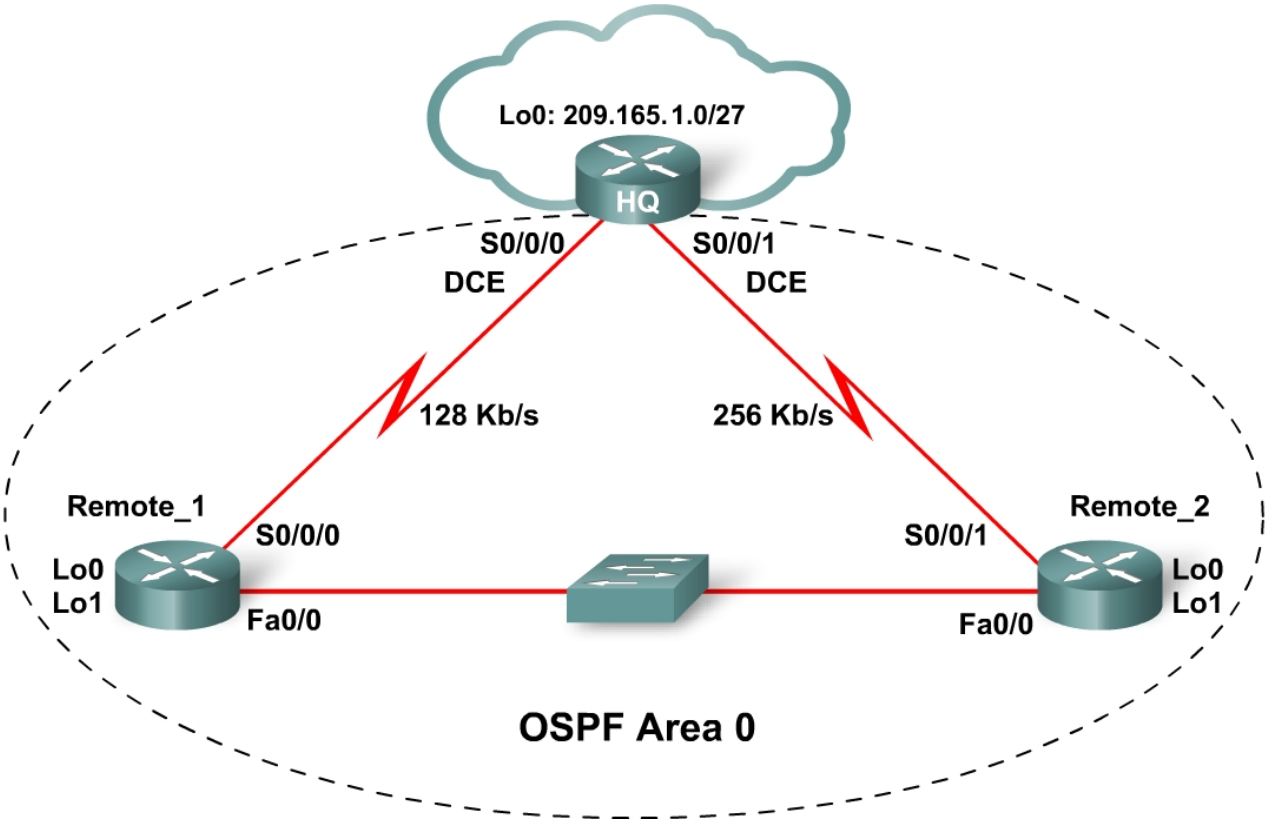
Give the Concole, vty and enable password for each router. Use the words "cisco" and "class" as passwords.

Set Hostname , RtA, RtB, RtC for each router

Set Description for each router using the similar text "Router for A network"

Set static IP router in order to have success ping between every device on the network.

Topology Diagram



Exam Objectives

Completion of this exam requires the following tasks:

- Create an addressing scheme to accommodate the hosts on the network
- Cable and configure the network according to the diagram
- Perform basic router configurations
- Configure the interfaces and serial bandwidths
- Configure OSPF
- Configure OSPF priorities
- Disable OSPF advertisements on LAN interfaces
- Configure and propagate a static default route

Scenario

You are a network engineer for a company. You are assigned the task of interconnecting and creating an addressing scheme for each client's LAN. You must set the OSPF priorities so that the Remote_1 router is the DR and the Remote_2 router is the BDR.

Task 1: Create an Addressing Scheme.

Step 1: Using VLSM, create addressing schemes for all connections. For the interconnecting links, use the 10.0.0.0 network. For each LAN use the 192.168.1.0/24 address space.

Remote_1:

- Lo0: 30 Hosts
- Lo1: 10 Hosts

Remote_2:

- Lo0: 100 Hosts
- Lo1: 10 Hosts

Step 2: Record the appropriate subnet address and mask in Table 1.

Table 1

Device	Interface	IP Address	Subnet Mask
HQ	S0/0/0		
	S0/0/1		
	Lo0		
Remote_1	S0/0/0		
	Fa0/0		
	Lo0		
	Lo1		
Remote_2	S0/0/1		
	Fa0/0		
	Lo0		
	Lo1		

Task 2: Perform Basic Router Configurations.

Step 1 Perform basic configuration of the HQ, Remote_1, and Remote_2 routers. Configure the following:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.
- Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.

Step 2 Configure an EXEC timeout of 15 minutes.

Task 3: Configure the interfaces.

Step 1. Configure and enable the interfaces on all routers.

Task 4: Basic OSPF Configuration.

Step 1 Configure OSPF on each router.

Use Process ID 1 and advertise all directly connected networks in OSPF Area 0. Do not advertise the loopback interface on the HQ router.

Step 2 Verify the OSPF configuration.

Confirm that each router has formed an adjacency with one another and has a path to each network in the topology. Troubleshoot if necessary.

Task 5: Configure the DR / BDR.

Step 1: Configure router Remote_1 to always be the DR. Remote_2 should always be the BDR.

Step 2: Reload the switch to force the OSPF election process.

Step 3: Verify that the OSPF election has occurred.

Confirm that the Remote_1 router is now the DR and that the Remote_2 router is now the BDR. Troubleshoot if necessary.

Task 6: Disable OSPF routing advertisements on the LAN interfaces.

Step 1: Ensure that no OSPF advertisements are being forwarded out of the LAN interfaces.

Task 8: Confirm OSPF Operation.

Step 1: Verify that all networks are present in the routing table. Troubleshoot if necessary

Task 9: Static Default Route

Step 1: Configure a static default route on the HQ router.

Step 2: Propagate the static default route to the other routers in the network.

Step 3: Verify that each router can see the static default route in their routing table. Troubleshoot if necessary

Task 10: Configure OSPF Cost.

Step 1: Set the cost on the Remote_2 FastEthernet link to a value of 1.

Step 2: Set the cost of the Remote_1 FastEthernet to a value of 10.

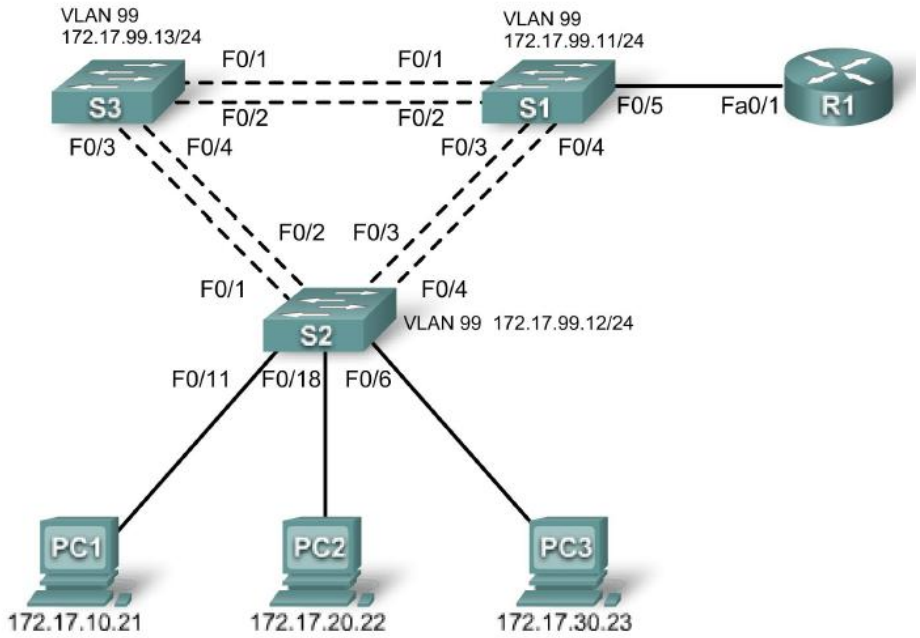
Step 3: Verify the cost in the routing table.

Task 11: Verify Connectivity

Step 1 Ping the loopback interface on the HQ router from the Remote_1 and Remote_2 routers.

Πρόβλημα 3

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	N/A	N/A	N/A
	F0/1.10	172.17.10.1	255.255.255.0	N/A
	F0/1.20	172.17.20.1	255.255.255.0	N/A
	F0/1.30	172.17.30.1	255.255.255.0	N/A
	F0/1.99	172.17.99.1	255.255.255.0	N/A
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN99	172.17.99.12	255.255.255.0	172.17.99.1

Device	Interface	IP Address	Subnet Mask	Default Gateway
S3	VLAN99	172.17.99.13	255.255.255.0	172.17.99.1
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1

Port Assignments

Switch 2

Ports	Assignment	Network
Fa0/1 – 0/4	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Switch 1

Ports	Assignment	Network
Fa0/1 – 0/4	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/5	802.1q Trunks	172.17.99.0 /24

Switch 3

Ports	Assignment	Network
Fa0/1 – 0/4	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the devices.

Step 3: Disable all ports using the shutdown command.

Step 4: Re-enable the active user ports on S2 in access mode.

Task 2: Perform Basic Device Configurations

Configure the S1, S2, and S3 switches according to the following guidelines:

Configure the hostname.

Disable DNS lookup.

Configure an EXEC mode password.

Configure a message-of-the-day banner.

Configure a password for console connections.

Configure synchronous logging.

Configure a password for vty connections.

Task 3: Configure and Activate Network Addresses

Step 1: Configure the Management VLAN interface on S1, S2, and S3.

Step 2: Configure the PC1, PC2, and PC3 Ethernet interfaces.

Task 4: Configure VTP

Step 1: Configure all trunks.

Step 2: Configure S1 as the VTP server, with domain name cisco and password cisco.

Step 3: Configure S2 and S3 as VTP clients, with domain name and password.

Task 5: Configure VLANs

Step 1: Configure the VLANs on the VTP server.

Configure the VLANs in the table below on the VTP server.

VLAN 99 management

VLAN 10 faculty-staff

VLAN 20 students

VLAN 30 guest

Step 2: Verify that the VTP clients are receiving VLAN configurations from the server.

Task 6: Configure STP

Step 1: Configure S1 to always be root.

Step 2: Configure RSTP.

Step 3: Verify that STP is running correctly.

Task 7: Configure Inter-VLAN routing

Step 1: Create a basic configuration on the router.

Step 2: Configure the trunking interface on R1.

Step 3: Verify Inter-VLAN routing.

Ping from each host to every other host.

Task 8: Document the Configurations

On each device, issue the show run command and capture the configurations.