Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μελέτη και Υλοποίηση ενός Σύγχρονου Δικτύου Δεδομένων με Έμφαση στη Μετάδοση Φωνής (VoIP)**
Ονοματεπώνυμο Φοιτητή	**Δημήτριος Καλδής**
Πατρώνυμο	**Ιωάννης**
Αριθμός Μητρώου	**ΜΠΠΛ/ 08065**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**

Ημερομηνία Παράδοσης: **Δεκέμβριος 2011**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης Καθηγητής	Χαράλαμπος Κωνσταντόπουλος Λέκτορας	Δημήτριος Βέργαδος Λέκτορας

Περίληψη

Η νέα γενιά τηλεφωνικών κέντρων ταυτίζεται με τον όρο Voice over Internet Protocol (VoIP). Ο όρος αυτός έχει συσχετιστεί πλέον με ένα σύνολο πρωτοκόλλων, τεχνολογιών και υπηρεσιών οι οποίες υλοποιούνται κάτω από μια κοινή πλατφόρμα. Ο στόχος των νέων τηλεφωνικών κέντρων επικεντρώνεται στην αύξηση της παραγωγικότητας μιας εταιρίας. Οι τηλεφωνικές υποδομές σήμερα μετατρέπονται σε εργαλείο ανάπτυξης και βελτίωσης της απόδοσης των εργαζομένων. Το τηλεφωνικό κέντρο έως και πριν λίγο καιρό αποτελούσε απλά μια μηχανή που γνωρίζει καλά να δρομολογεί την τηλεπικοινωνιακή κίνηση και να εξυπηρετεί συγκεκριμένες ανάγκες για υπηρεσίες φωνητικής επικοινωνίας. Με την πάροδο του χρόνου η ανάγκη για επικοινωνία άλλαξε. Ο τρόπος με τον οποίο επικοινωνεί η ανθρωπότητα σήμερα έχει αλλάξει δραστικά σε σχέση με την τελευταία δεκαετία. Η μορφή της μεταλλάχτηκε μαζί με τη συνήθεια και την ανάγκη να βελτιωθεί η επικοινωνία σε επίπεδο διαχείρισης χρόνου, κόστους, ταχύτητας και ελευθερίας από το συμβατικό γραφείο. Το τηλέφωνο, το ηλεκτρονικό ταχυδρομείο, το φαξ και ο τηλεφωνητής ακολουθούν πάντα το χρήστη όπου και αν βρίσκεται. Τα κοινωνικά δίκτυα αποτελούν αναπόσπαστο κομμάτι των κινητών συσκευών. Τα «πανέξυπνα» πλέον τηλεφωνικά κέντρα γνωρίζουν που βρίσκεται ο χρήστης, σε ποια συσκευή θέλει να λαμβάνει τις κλήσεις του, αλλά και τον υποστηρίζουν να οργανώνει το χρόνο του εκτελώντας για παράδειγμα μια τηλεδιάσκεψη αντί να πραγματοποιήσει ένα ταξίδι. Είναι γεγονός πως οι τεχνολογίες που πλαισιώνουν ένα τέτοιο τηλεπικοινωνιακό εργαλείο το καθιστούν ιδιαίτερα φιλικό προς το χρήστη. Το νόμισμα όμως έχει δυο όψεις. Σε επίπεδο κατασκευής, υλοποίησης και εγκατάστασης τα πράγματα αλλάζουν δραστικά, καθώς ένας τόσο πολύπλοκος μηχανισμός εγκυμονεί κινδύνους. Η φαινομενικά απλή ρύθμιση του κέντρου δε θα επιφέρει την παραμετροποίηση που θα το διασφαλίσει αλλά ούτε και το συνδυασμό των ρυθμίσεων που θα το κάνει να λειτουργεί απρόσκοπτα. Σεβόμενοι τις τεχνολογίες που κρύβονται πίσω από αυτόν τον περίπλοκο μηχανισμό πρέπει οι διαδικασίες παραμετροποίησης να στοχεύουν στην ασφαλή λειτουργία ενός τέτοιου περίτεχνου συστήματος το οποίο είναι διασυνδεδεμένο με το διαδίκτυο.

Abstract

The new generation of Telephone Centers coincides with the term Voice over Internet Protocol (VoIP) term. This term is associated with broad range of protocols, technologies and services that are implemented under a common platform. The aim of all new generation of Telephone Centers focuses on increasing productivity in businesses. Telephone infrastructure is rapidly transforming to tools capable of increasing and optimizing employee's performance. Until recently, the telephone center was just a "clever" machine capable of routing telephone conversations and to serve certain common voice communication tasks. As time and technology advanced, communication needs changed rapidly. The way that humanity communicates today changed dramatically compared to last decade. The form of communication transformed along with common business habits and the necessity to improve all communications in terms of time management, costs, speed and freedom from a conventional office. The telephone device, electronic mail, fax and answering machine serve users wherever they are. The social networks are an integral part of all modern mobile devices. Not only do "Smart" telephone centers know the location of a user and his preferred device to receive calls but also support him to organize his time by setting up a teleconference, instead of taking a long trip to an actual meeting. It's a fact that all the technologies that surround such a telecommunication tool render it very user friendly. However every coin has two faces. The construction, implementation, and installation standards are radically changing as such this complex mechanism can hide risks. A seemingly common setting on a telephone center does not guarantee risk free operation. In respect to all these technologies that lay behind such a complex mechanism, which is nowadays connected to the internet, all configuration procedures must target to a problem free and secure operation.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1ο

1. Φωνή μέσω IP

1.1 Πραγματοποίηση Κλήσεων Μέσω του Ιστού

1.1.1 Γενικά

Παραδοσιακά, για τη μεταφορά κυκλοφορίας δεδομένων φωνής χρησιμοποιούνταν συνδέσεις μεταγωγής μέσω κυκλωμάτων. Οι εταιρικοί πελάτες οι οποίοι είχαν ανάγκη από πολλές τηλεφωνικές γραμμές εγκαθιστούσαν ιδιωτικά τηλεφωνικά κέντρα (Private Branch eXchange, PBX) και δίκτυα φωνής. Αυτά τα παραδοσιακά δίκτυα συνήθως ήταν αποκλειστικά, κλειστά συστήματα, ακριβά στη συντήρηση, την αναβάθμιση και την επεκτασή τους.

Η VoIP τεχνολογία παρέχει υπηρεσίες φωνής όπως τηλεφωνία, δρομολόγηση κλήσεων και φωνητικό ταχυδρομείο χρησιμοποιώντας το δίκτυο δεδομένων. Έτσι τόσο τα δίκτυα δεδομένων όσο και τα δίκτυα φωνής μπορούν να συγκλίνουν σε ένα μόνο δίκτυο IP, παρέχοντας τη δυνατότητα συνδυασμού υπολογιστικών εφαρμογών με υπηρεσίες τηλεφωνίας. Η σύγκλιση αυτή προσφέρει πλεονεκτήματα τόσο στους χρήστες όσο και στην ίδια την εταιρία:

- Μειώνεται το κόστος και η πολυπλοκότητα αφού υπάρχει μόνο ένα δίκτυο που χρειάζεται διαχείριση.
- Επειδή οι τηλεφωνικοί αριθμοί παρέχονται μέσω λογισμικού και όχι μέσω συσκευών, διευκολύνεται η μετακίνηση και η προσθήκη υπαλλήλων στην επιχείρηση.
- Μειώνονται οι χρεώσεις από υπεραστικές κλήσεις διότι εξυπηρετούνται από το εταιρικό δίκτυο.
- Ένα νούμερο επικοινωνίας για το προσωπικό της εταιρίας ανεξαρτήτως συσκευής (κινητό, σταθερό) ή τοποθεσίας.
- Συσκευές διπλής λειτουργίας που επιτρέπουν στους εργαζομένους τη μετάβαση από δίκτυο κινητής τηλεφωνίας σε ασύρματο δίκτυο δεδομένων χωρίς να χάσουν τις συνδέσεις τους.
- Οι ενοποιημένες επικοινωνίες συντελούν στην μείωση ή εξάλειψη των καθυστερήσεων και δυσχερειών που συνδέονται με την αναζήτηση και σύνδεση με σημαντικές επαφές[1].
- Διατηρείται για τον χρήστη μια συνεχόμενη ροή σκέψης και πράξης ανάμεσα στις συσκευές επικοινωνίας.
- Οι εργαζόμενοι είναι διαθέσιμοι και παραγωγικοί οπουδήποτε και αν βρίσκονται μέσω του δικτύου της εταιρίας, βελτιώνοντας έτσι το προφίλ της εταιρίας μιας και οι πελάτες μπορούν να καλούν απλά ένα εταιρικό τηλέφωνο για να έρχονται σε επαφή με τον εκπρόσωπο.

[1]Με βάση μια έρευνα της εταιρίας τηλεπικοινωνιών Avaya περισσότεροι από το 64% των εργαζομένων μεταφέρουν πάνω από μια συσκευή επικοινωνίας, παρόλα αυτά περίπου το 40% αυτών απαντούν ότι περισσότερες από τέσσερεις με πέντε φορές την εβδομάδα λαμβάνουν κάποιο σημαντικό μήνυμα με καθυστέρηση. Το 34% των οποίον δήλωσαν ότι έχασαν ευκαιρίες για κάποια πώληση ή συνεργασία επειδή δεν μπόρεσαν να επικοινωνήσουν μαζί τους όταν χρειάστηκε.

- Ένα ενοποιημένο mail box χωρίς πλέον να χρειάζεται να ελέγχει κανείς ξεχωριστά το mail box του κινητού και του γραφείου καθώς και επιπλέον υπηρεσίες όπως βίντεοδιάσκεψη και κινητικότητα.
- Απρόσκοπτη λειτουργία ανεξάρτητα εάν το δίκτυο, η συσκευή ή ο χώρος επηρεαστεί από φυσική καταστροφή ή δυσλειτουργία.
- Μείωση των επιχειρηματικών κινδύνων που σχετίζονται με ιούς και λοιπές απειλές ασφαλείας.

1.1.2 Ενοποίηση Επικοινωνιών

Η έννοια των ενοποιημένων επικοινωνιών αναφέρεται σε ένα σύνολο συγκλινουσών υπηρεσιών επικοινωνίας, όπως φωνή, φωνητικές συνδιασκέψεις, βίντεοδιασκέψεις, φωνητικό ταχυδρομείο και άλλα.

Κάθε δίκτυο ενοποιημένων επικοινωνιών μπορεί να διαχωριστεί σε τέσσερα διαφορετικά επίπεδα:

Επίπεδο πελάτη: Στο επίπεδο αυτό ανήκουν οι συσκευές με τις όποιες έρχεται σε επαφή και αλληλεπιδρά ο πελάτης-χρήστης. Για παράδειγμα IP τηλέφωνα, υπολογιστές με εγκατεστημένο ή όχι λογισμικό τηλεφώνου (softphone), συσκευές PDA και κάθε είδους IP εξοπλισμός για βίντεοδιάσκεψη. Οι συσκευές στο επίπεδο αυτό είναι υπεύθυνες για τη μετατροπή του ήχου σε ψηφιακή μορφή (και το αντίστροφο). Αυτό επιτυγχάνεται με την ψηφιακή επεξεργασία σήματος των δειγμάτων του ήχου που λαμβάνονται από τα ακουστικά. Ένα σημαντικό πρόβλημα που υπήρξε με τις IP τηλεφωνικές συσκευές ήταν η ανάγκη για μόνιμη παροχή ρεύματος. Αυτό ξεπεράστηκε με τη χρήση μεταγωγέων Power over Ethernet, δηλαδή ο μεταγωγέας στον οποίο συνδέεται η τηλεφωνική συσκευή παρέχει και ρεύμα μέσα από το Ethernet καλώδιο.

Επίπεδο υποδομής: Το επίπεδο αυτό περιλαμβάνει τις παραδοσιακές συσκευές δικτύου όπως δρομολογητές, μεταγωγείς και πύλες δικτύου (gateways). Ο ρόλος του επιπέδου αυτού ειδικά σε εφαρμογές πραγματικού χρόνου, όπως η μετάδοση φωνής, είναι πολύ κρίσιμος διότι τυχόν καθυστερήσεις ή απώλειες πακέτων θα έχουν σαν αποτέλεσμα την κακή μετάδοση του ήχου στον παραλήπτη. Έτσι για να μπορεί η IP τηλεφωνία να θεωρείται ποιοτικά αντάξια της παραδοσιακής θα πρέπει ο συνολικός σχεδιασμός του δικτύου για υψηλή διαθεσιμότητα και η κατάλληλη εφαρμογή τεχνικών Ποιότητας Υπηρεσιών (Quality of Service) να πραγματοποιούνται με μεγάλη προσοχή.

Οι πύλες είναι υπεύθυνες για τη γεφύρωση των PSTN δικτύων με τα δίκτυα ενοποιημένων επικοινωνιών. Επιπλέον χρησιμοποιούνται για να ενώσουν μεταξύ τους απομακρυσμένα PBX δημιουργώντας «σήραγγες» επικοινωνίας.

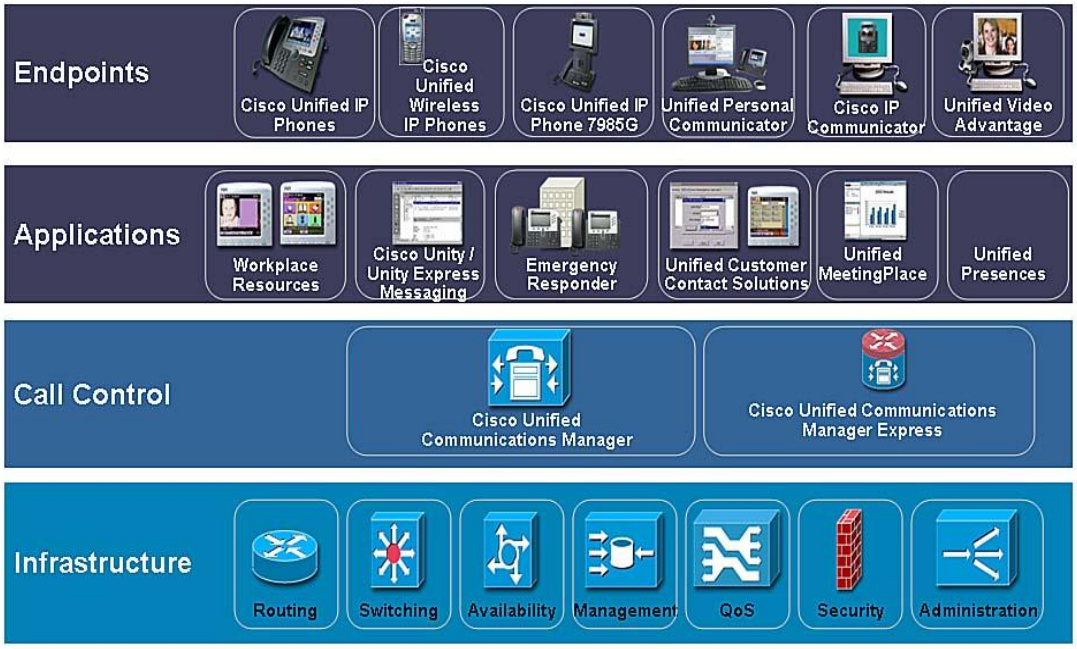
Επίπεδο επεξεργασίας κλήσεων: Στο επίπεδο αυτό πραγματοποιείται ο έλεγχος των κλήσεων μέσω του λογισμικού διαχείρισης κλήσεων (Call Manager). Ο Call Manager χαρακτηρίζεται ως η «καρδιά» του επιπέδου αυτού διότι αντικαθιστά το PBX ενός εταιρικού τηλεφωνικού δικτύου ή το ψηφιακό κέντρο ενός PSTN δικτύου. Πέρα από την παροχή συνδεσιμότητας, σηματοδοσίας και ελέγχου συσκευών, ο Call Manager εκτελεί λειτουργίες διαχείρισης, συντήρησης και μέριμνας για το δίκτυο.

Όταν κάποιος πραγματοποιήσει μια κλήση σε έναν αριθμό, το λογισμικό διαχείρισης κλήσεων αναζητά τον αριθμό, προκαλεί το κουδούνισμα του τηλεφώνου και αναπαράγει τον ήχο κλήσης στο ακουστικό του πομπού. Όταν ο δέκτης σηκώσει το ακουστικό, ο Call Manager σταματά να συμμετέχει αφού πλέον τα δυο τηλέφωνα επικοινωνούν απευθείας.

Στις ενοποιημένες υπηρεσίες, το λογισμικό διαχείρισης κλήσεων παρέχει και λειτουργίες Call Admission Control (CAC). Έτσι όταν ένας χρήστης που βρίσκεται σε ένα υποκατάστημα πραγματοποιήσει μια κλήση σε ένα άλλο υποκατάστημα, ο Call Manager πρέπει να ελέγξει αν υπάρχει το απαιτούμενο εύρος ζώνης στη WAN ζεύξη που πρόκειται να εξυπηρετήσει την κλήση. Αν υπάρχει, ο Call Manager θα προωθήσει την κλήση μέσω αυτής, σε διαφορετική περίπτωση συνδυαστικά με το σχήμα αριθμοδότησης (dial plan) της εταιρίας ίσως να προωθήσει την κλήση μέσω του PSTN δικτύου. Επομένως είναι σημαντικό οι λειτουργίες CAC και το dial plan να συνεργάζονται άριστα ώστε να επιτυγχάνεται η βέλτιστη δρομολόγηση των κλήσεων μέσα στο δίκτυο.

Επίπεδο εφαρμογών: Ορισμένες από τις εφαρμογές που προέκυψαν μετά τη σύγκληση των δικτύων φωνής και δεδομένων είναι: Η φορητότητα αριθμών τηλεφώνου, δηλαδή οι χρήστες μπορούν να χρησιμοποιούν οποιαδήποτε εταιρική τηλεφωνική συσκευή με το δικό τους αριθμό. Η συγχώνευση δεδομένων φωνής, ηλεκτρονικού ταχυδρομείου και φαξ σε έναν και μόνο κουβά «εισερχομένων». Η δυνατότητα αναγνώρισης ομιλίας σε συνδυασμό με κανόνες χειρισμού κλήσεων. Ενοποίηση εφαρμογών πελατών όπως Enterprise Resource Planning (ERP), Customer Relationship Management ή Marketing (CRM[2]) και διαχείριση αποθεμάτων κ.α. Επίσης προσφέρονται όλες οι λειτουργίες της παραδοσιακής τηλεφωνίας, όπως η προώθηση και η φραγή κλήσεων κ.α.

Εικόνα 1-1: Βασικά Επίπεδα Δικτύου Ενοποιημένων Επικοινωνιών

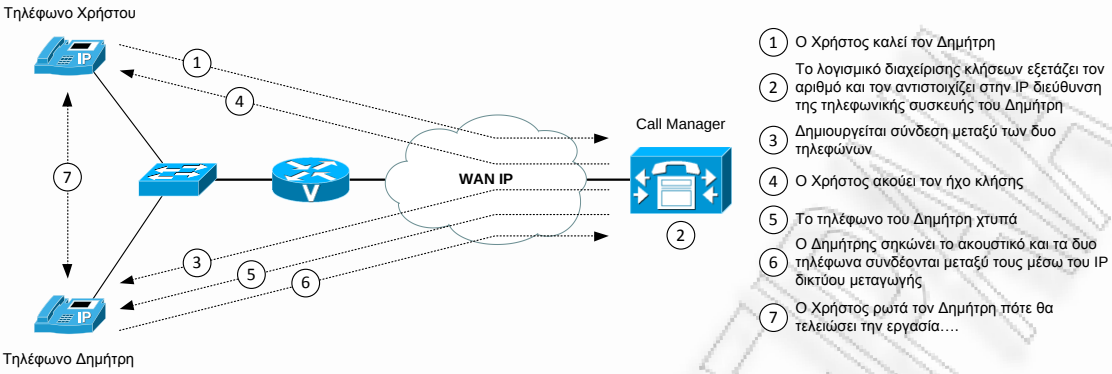


[53]

Στην επόμενη εικόνα γίνονται ξεκάθαρα τα βήματα που απαιτούνται για την πραγματοποίηση μιας κλήσης μεταξύ δυο IP τηλεφωνικών συσκευών. Το παράδειγμα έχει βασιστεί στην υπόθεση ότι η επεξεργασία κλήσεων γίνεται συγκεντρωτικά σε κεντρική θέση του δικτύου. Στην περίπτωση κατανεμημένης επεξεργασίας κλήσεων τα βήματα διαφοροποιούνται ελαφρώς, όπως επίσης διαφοροποίηση θα έχουμε και στην περίπτωση όπου η κλήση δεν πραγματοποιηθεί τελικά προς IP τηλέφωνο ή υπάρξει συμφόρηση στο εσωτερικό δίκτυο όπου τότε πιθανών να εξυπηρετηθεί μέσω μιας PSTN πύλης.

[2] Η σύνδεση του τηλεφωνικού κέντρου με το σύστημα διαχείρισης πελατειακών σχέσεων (CRM) μιας επιχείρησης, βοηθάει ώστε κάθε φορά που ένας πελάτης καλεί, οι εργαζόμενοι αυτόματα βλέπουν στο τηλέφωνο ή τον υπολογιστή τους ένα pop-up παράθυρο με όλες τις απαραίτητες πληροφορίες του πελάτη.

Εικόνα 1-2: Πραγματοποίηση Κλήσης Μεταξύ IP Τηλεφώνων

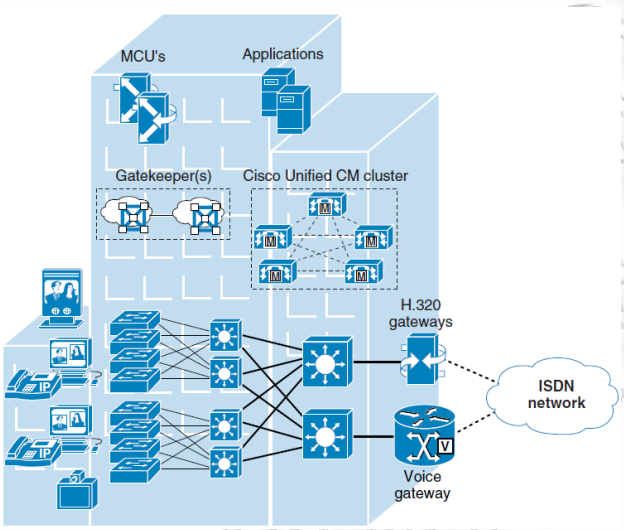


1.1.3 Μοντέλα Ανάπτυξης Ενοποιημένων Επικοινωνιών

Υπάρχουν τρία βασικά μοντέλα ανάπτυξης των ενοποιημένων επικοινωνιών:

- **Σε μια τοποθεσία**: Η επεξεργασία των κλήσεων υλοποιείται σε μια μόνο τοποθεσία και από ένα μέσο επεξεργασίας.

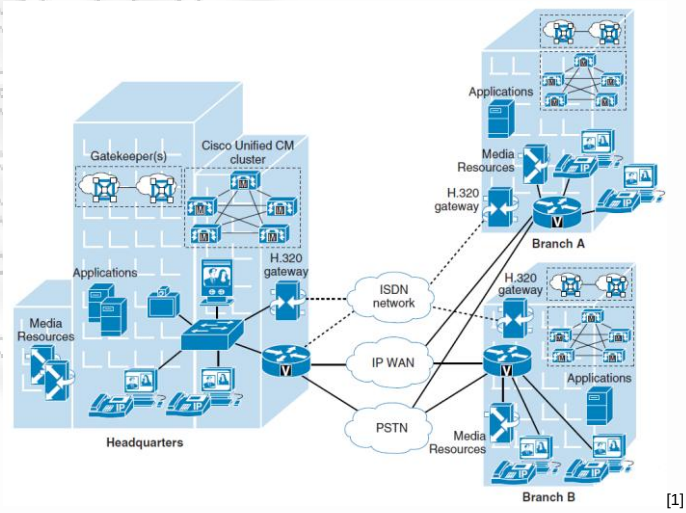
Εικόνα 1-3: Μονός Σταθμότοπος - Μοντέλο Ανάπτυξης



[1]

- **Σε πολλές τοποθεσίες με κατανεμημένη επεξεργασία κλήσεων**: Η επεξεργασία των κλήσεων πραγματοποιείται σε κάθε διαφορετικό σταθμότοπο (σε πολλές θέσεις της εταιρίας) όπου και απαιτείται να υπάρχει εξοπλισμός επεξεργασίας κλήσεων και χειρισμού φωνητικών μηνυμάτων. Παρόλα αυτά, συνολικά ο εξοπλισμός και οι πόροι του δικτύου λειτουργούν σαν ένα ενιαίο σύστημα. Η δρομολόγηση των κλήσεων πραγματοποιείται μέσω του IP WAN της εταιρίας, με εξαίρεση περιπτώσεις πιθανής βλάβης ή φόρτου του εταιρικού δικτύου όπου τότε οι κλήσεις εξυπηρετούνται μέσω του PSTN δικτύου. Η εφαρμογή του μοντέλου αυτού ενδείκνυται σε περιπτώσεις συγχώνευσης εταιριών ή σε περιπτώσεις σταδιακής αντικατάστασης των παλαιών τηλεφωνικών κέντρων με VoIP από τα υποκαταστήματα μιας εταιρίας.

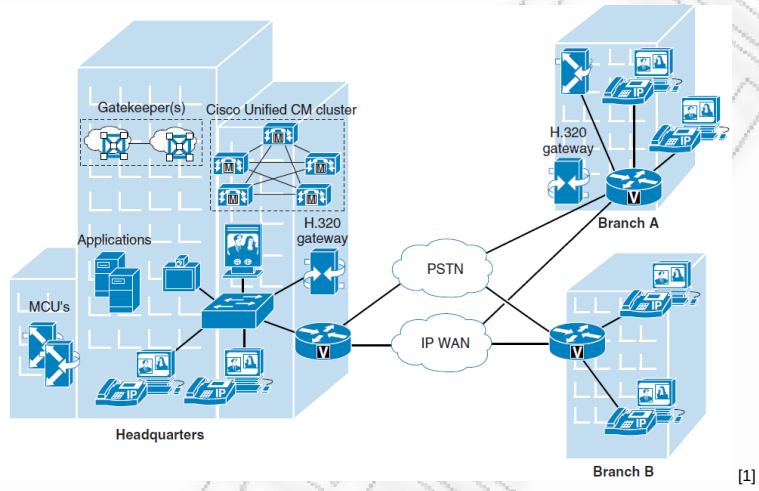
Εικόνα 1-4: Πολυσταθμοτοπικό Δίκτυο με Κατανεμημένη Επεξεργασία Κλήσεων - Μοντέλο Ανάπτυξης



[1]

- **Σε πολλές τοποθεσίες με συγκεντρωτική επεξεργασία κλήσεων:** Η επεξεργασία των κλήσεων πραγματοποιείται συγκεντρωτικά σε ένα και μόνο κεντρικό σταθμότοπο όπου και απαιτείται να υπάρχει εξοπλισμός επεξεργασίας κλήσεων και χειρισμού φωνητικών μηνυμάτων. Οι απομακρυσμένες τοποθεσίες περιέχουν μόνο τον βασικό εξοπλισμό όπως δρομολογητές, μεταγωγείς, πύλες και IP τηλέφωνα. Η δρομολόγηση των κλήσεων πραγματοποιείται μέσω του IP WAN της εταιρίας, με εξαίρεση περιπτώσεις πιθανής βλάβης ή φόρτου του εταιρικού δικτύου όπου τότε οι κλήσεις εξυπηρετούνται μέσω του PSTN δικτύου. Στα θετικά του συγκεντρωτικού μοντέλου συγκαταλέγονται η ευκολότερη διαχείριση, η ευκολότερη αντιμετώπιση πιθανών προβλημάτων και ο λιγότερος απαιτούμενος εξοπλισμός.

Εικόνα 1-5: Πολυσταθμοτοπικό Δίκτυο με Συγκεντρωτική Επεξεργασία Κλήσεων - Μοντέλο Ανάπτυξης



[1]

1.2 Κινητικότητα IP Συσκευής

Στον CallManager, ένα υποκατάστημα ή ένα κεντρικό κατάστημα προσδιορίζονται χρησιμοποιώντας διάφορες παραμέτρους, όπως: τοποθεσίες, περιοχές, μετάφραση αριθμού κλήσης. Τα IP τηλέφωνα που βρίσκονται σε ένα συγκεκριμένο υποκατάστημα έχουν προγραμματιστεί στατικά με συγκεκριμένες ρυθμίσεις ώστε να προσδιορίζουν τη θέση τους. Ο CallManager χρησιμοποιεί αυτές τις ρυθμίσεις για τη σωστή εγκατάσταση κλήσεων, δρομολόγηση των κλήσεων και ούτω καθεξής. Ωστόσο, όταν κινητά τηλέφωνα σαν τα Cisco IP Communicator ή Cisco Unified Wireless IP Phones μετακινούνται από τη φυσική τους θέση σε μια απομακρυσμένη τοποθεσία, διατηρούν τις αρχικές στατικές ρυθμίσεις. Έτσι ο CallManager χρησιμοποιεί αυτές τις ρυθμίσεις τηλεφώνων στη νέα τοποθεσία. Η κατάσταση αυτή είναι ανεπιθύμητη διότι μπορεί να προκαλέσει προβλήματα κατά τη δρομολόγηση των κλήσεων, την επιλογή codec, την επιλογή πόρων πολυμέσων, καθώς και σε άλλες λειτουργίες επεξεργασίας κλήσεων.

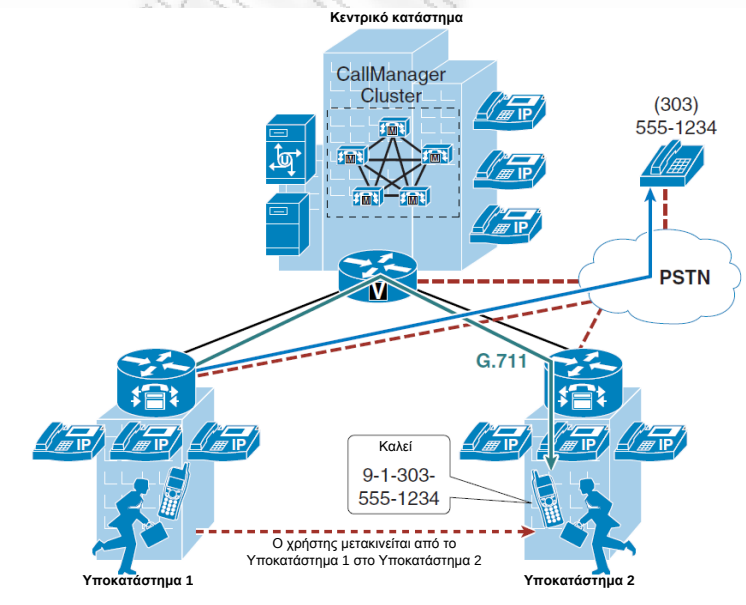
Η έκδοση 4.2 του Cisco Unified CallManager εισάγει ένα νέο χαρακτηριστικό που ονομάζεται «κινητικότητα συσκευής» (Device Mobility). Το χαρακτηριστικό αυτό δίνει τη δυνατότητα στο πρόγραμμα διαχείρισης κλήσεων να διαπιστώσει αν το IP τηλέφωνο βρίσκεται στη φυσική του θέση ή σε τοποθεσία περιαγωγής. Αυτό γίνεται με τη βοήθεια των υποδικτύων που μαρτυρούν την ακριβή θέση του τηλεφώνου. Με την ενεργοποίηση της κινητικότητας συσκευής μέσα σε μια συστάδα (cluster), οι κινητοί χρήστες μπορούν να μεταφέρονται από μια περιοχή σε μια άλλη αποκτώντας τις ρυθμίσεις που απαιτεί κάθε σταθμότοπος. Εν συνεχεία ο CallManager χρησιμοποιεί τις δυναμικά κατανεμημένες ρυθμίσεις για τη δρομολόγηση κλήσεων, επιλογή codec, επιλογή πόρων και ούτω καθεξής.

Στην Εικόνα 1-5 απεικονίζεται ένα υποθετικό δίκτυο όπου στο κεντρικό κατάστημα υπάρχει συστάδα από Cisco Unified CallManager των οποίων η έκδοση είναι η 4.1 ή και παλαιότερη. Το συγκρότημα διαθέτει δυο απομακρυσμένες τοποθεσίες, το Υποκατάστημα 1 και το Υποκατάστημα 2. Όλες οι κλήσεις που πραγματοποιούνται εντός του ίδιου σταθμότοπου χρησιμοποιούν τον G.711 VoCodec, ενώ όλες οι διασταθμοτοπικές κλήσεις (κλήσεις δια μέσου IP WAN) τον G.729. Κάθε περιοχή έχει μια πύλη PSTN για εξωτερικές κλήσεις.

Όταν ένας χρήστης από το Υποκατάστημα 1 μετακινείται προς το Υποκατάστημα 2 και καλεί έναν PSTN χρήστη σε μια πόλη, συμβαίνουν τα ακόλουθα:

1. Ο CallManager (πρόγραμμα διαχείρισης κλήσεων) δε γνωρίζει ότι ο χρήστης μετακινείται από το πρώτο στο δεύτερο υποκατάστημα. Μια εξερχόμενη κλήση στέλνεται μέσω WAN στην πύλη του Υποκαταστήματος 1 και μετά έξω στο PSTN δίκτυο. Έτσι ο κινητός χρήστης συνεχίζει να χρησιμοποιεί την πύλη του Υποκαταστήματος 1 για όλες τις PSTN κλήσεις.
2. Ο κινητός χρήστης και η πύλη του Υποκαταστήματος 1 είναι στην ίδια περιοχή (region) και θέση (location) για τον Cisco Unified CallManager. Ο έλεγχος αποδοχής κλήσεων (CAC) πραγματοποιείται μόνο για συσκευές που βρίσκονται σε διαφορετικές θέσεις, επιπλέον γνωρίζουμε ότι μια κλήση εντός της ίδιας περιοχής χρησιμοποιεί τον G.711 VoCodec. Έτσι, η κλήση μέσω του IP WAN προς την πύλη του Υποκαταστήματος 1 χρησιμοποιεί τον G.711 και δεν παρακολουθείται από το Cisco Unified CallManager για έλεγχο αποδοχής κλήσεων (CAC). Αυτή η συμπεριφορά μπορεί να οδηγήσει σε υπερκάλυψη του εύρους ζώνης του IP WAN αν όλες οι απομακρυσμένες ζεύξεις είναι χαμηλής ταχύτητας.
3. Ο κινητός χρήστης προσθέτει και άλλους χρήστες στη συνομιλία (teleconference) από το Υποκατάστημα 2. Επειδή ο κινητός χρήστης χρησιμοποιεί πόρους από το Υποκατάστημα 1, ως εκ τούτου όλα τα ρεύματα της τηλεφωνικής διάσκεψης περνάνε από το IP WAN.

Εικόνα 1-6: Κινητικότητα Συσκευής - Υποθετικό Σενάριο



[1]

1.2.1 Χαρακτηριστικό «Κινητικότητα Συσκευής»

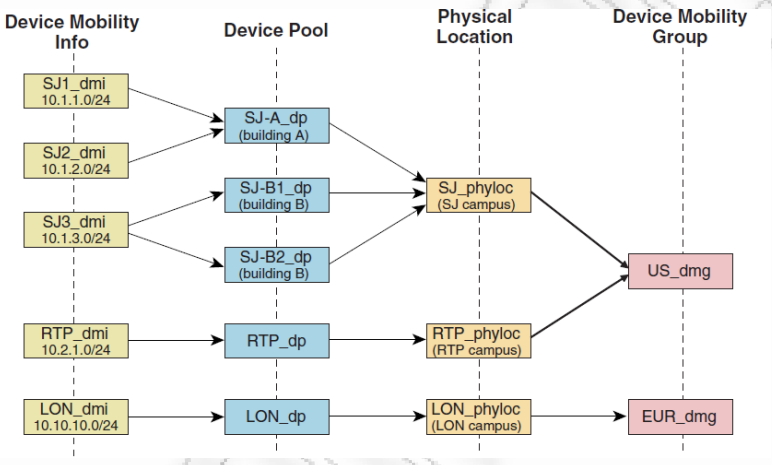
Ο Cisco Unified CallManager 4.2 εισάγει το χαρακτηριστικό γνώρισμα «Κινητικότητα Συσκευής», το οποίο βοηθά στην επίλυση των προβλημάτων που αναφέρθηκαν παραπάνω.

Σε αυτή την ενότητα θα περιγραφεί, εν συντομία, πώς λειτουργεί αυτό το χαρακτηριστικό.

Μερικοί από τους νέους όρους που εισάγονται στον Cisco Unified CallManager 4.2 και σχετίζονται με το χαρακτηριστικό αυτό είναι:

- **Device Mobility Info**: Καθορίζει τα IP υποδίκτυα και συνδέει τις ομάδες συσκευών (Device pools) με αυτά.
- **Physical Location**: Καθορίζει τη φυσική τοποθεσία μιας ομάδας συσκευών. Με άλλα λόγια, το στοιχείο αυτό καθορίζει τη γεωγραφική θέση των IP τηλεφώνων και άλλων συσκευών που συνδέονται με την ομάδα συσκευών (για παράδειγμα στο επόμενο σχήμα, όλα τα IP τηλέφωνα στο San Jose, καθορίζονται από τη φυσική τοποθεσία SJ_phyloc).
- **Device Mobility Group**: Ορίζει μια λογική ομάδα τοποθεσιών με παρόμοια πρότυπα κλήσης (για παράδειγμα στο επόμενο σχήμα, US_dmg και EUR_dmg).

Εικόνα 1-7: Σχέση Συστατικών του Χαρακτηριστικού «Κινητικότητα Συσκευής»

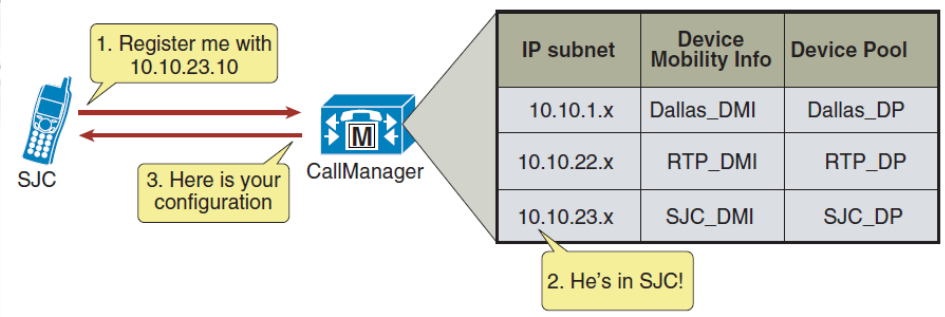


[1]

Στη συνέχεια περιγράφεται πώς ο Cisco Unified CallManager αποδίδει μια ομάδα συσκευών (device pool) σε ένα IP τηλέφωνο που ανήκει σε ένα IP υποδίκτυο.

1. Το IP τηλέφωνο προσπαθεί να εγγραφεί στον Cisco Unified CallManager αποστέλλοντας την IP διεύθυνσή του μέσω ενός Skinny Client Control Protocol (SCCP) μηνύματος εγγραφής.
2. Ο Cisco Unified CallManager παραλαμβάνει την πληροφορία του IP υποδικτύου της συσκευής και την αντιστοιχίζει με το υποδίκτυο που έχει ρυθμιστεί στο Device Mobility Info.
3. Αν το υποδίκτυο προσαρμοστεί, ο Cisco Unified CallManager παρέχει στη συσκευή νέες ρυθμίσεις που βασίζονται στις ρυθμίσεις της ομάδας συσκευών (device pool).

Εικόνα 1-8: Διαδικασία Εγγραφής Τηλεφώνου



[1]

Ο CallManager για να φιλοξενήσει την «κινητικότητα συσκευής» προσθέτει νέες παραμέτρους για τη ρύθμιση της ομάδας συσκευών (device pool).

Αυτές οι παράμετροι είναι οι ακόλουθες δυο βασικές κατηγορίες:

- **Ρυθμίσεις Περιαγωγής**: Οι παράμετροι στο πλαίσιο αυτών των ρυθμίσεων θα παρακάμπτουν τις ρυθμίσεις του επιπέδου συσκευής όταν η συσκευή βρίσκεται σε περιαγωγή εντός ή εκτός του Devise Mobility Group.

  Οι παράμετροι που περιλαμβάνονται στις εν λόγω ρυθμίσεις είναι:

  — Date/time Group Region

  — Media Resource Group List

  — Location

  — Network Locale

  — Survivable Remote Site Telephony (SRST)

  — Reference Physical Location

  — Device Mobility Group

Οι παραπάνω ρυθμίσεις πρωτίστως βοηθούν στην επίτευξη του κατάλληλου ελέγχου αποδοχής κλήσεων και στην επιλογή codec φωνής. Αυτό διότι οι ρυθμίσεις θέσης (Location) και περιοχής (Region) χρησιμοποιούνται βάσει της περιαγώμενης ομάδας συσκευών (roaming device pool) της συσκευής.

Επίσης ενημερώνουν τη λίστα ομάδων πόρων πολυμέσων (media resource group list - MRGL) ώστε να χρησιμοποιούνται οι κατάλληλοι πόροι πολυμέσων για μουσική κατά την αναμονή, διάσκεψη, διακωδικοποίηση (transcoding) και ούτω καθεξής έτσι ώστε να αξιοποιείται αποδοτικά το δίκτυο.

Μέσα από τις ρυθμίσεις της κατηγορίας αυτής ενημερώνεται επίσης η Survivable Remote Site Telephony (SRST) πύλη. Οι κινητοί χρήστες εγγράφονται σε διαφορετική SRST πύλη κατά την περιαγωγή. Αυτή η εγγραφή μπορεί να επηρεάσει τη συμπεριφορά της κλήσης όταν τα περιαγώμενα τηλέφωνα είναι σε λειτουργία SRST.

- **Ρυθμίσεις Κινητικότητας Συσκευής:** Οι παράμετροι στο πλαίσιο αυτών των ρυθμίσεων θα παρακάμπτουν τις ρυθμίσεις του επιπέδου συσκευής μόνο όταν η συσκευή βρίσκεται σε περιαγωγή εντός του Devise Mobility Group.

  Οι παράμετροι που περιλαμβάνονται στις εν λόγω ρυθμίσεις είναι:

  — Device Mobility CSS

  — AAR CSS

  — AAR Group

Όπως προαναφέρθηκε το Device Mobility Group, ορίζει μια λογική ομάδα τοποθεσιών με παρόμοια πρότυπα κλήσης (για παράδειγμα, οι περιοχές που έχουν τους ίδιους κωδικούς πρόσβασης PSTN κοκ). Με αυτή την κατευθυντήρια γραμμή, όλες οι τοποθεσίες διαθέτουν παρόμοια πρότυπα κλήσης στις «ρυθμίσεις-τοποθεσίας» της υπηρεσίας Calling Search Space.

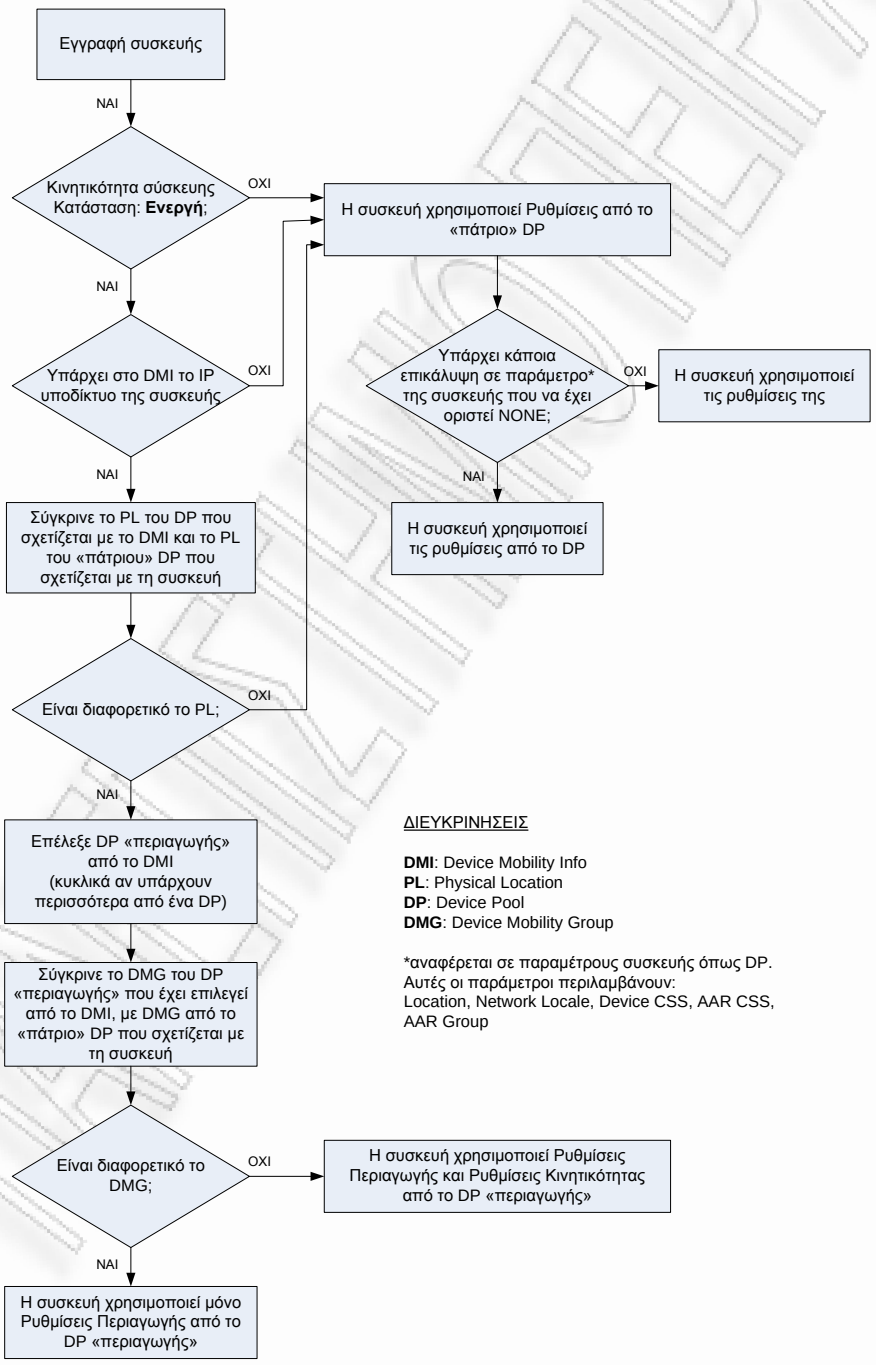
Οι παράμετροι αυτοί επηρεάζουν το σχέδιο επιλογής κλήσης διότι η λειτουργία Calling Search Space υπαγορεύει τα σχέδια για την επίτευξη εξερχομένων κλήσεων ή τις συσκευές που μπορεί να επιτευχθεί. Ένας χρήστης σε περιαγωγή εντός του Device Mobility Group μπορεί να διατηρήσει τον τρόπο με τον όποιο πραγματοποιεί κλήσεις ακόμα και μετά τη λήψη ενός νέου Calling Search Space. Ενώ ένας χρήστης σε περιαγωγή εκτός του Device Mobility Group διατηρεί τον τρόπο με τον όποιο πραγματοποιεί κλήσεις διότι χρησιμοποιεί το «πάτριο» Calling Search Space.

Ωστόσο, εάν το Device Mobility Group ορίζεται από περιοχές-τομείς που έχουν διαφορετικά πρότυπα κλήσης (για παράδειγμα, περιοχές που έχουν διαφορετικούς PSTN κωδικούς πρόσβασης), τότε ένας χρήστης σε περιαγωγή εντός του Device Mobility Group δεν μπορεί να διατηρήσει τον ίδιο τρόπο πραγματοποίησης κλήσεων σε όλες τις τοποθεσίες.

Άρα μετά τη λήψη ενός νέου Calling Search Space ο χρήστης θα είναι αναγκασμένος να καλεί διαφορετικά ψηφία ανάλογα με τις περιοχές, γεγονός που θα του προκαλέσει σύγχυση.

Το επόμενο διάγραμμα ροής αντιπροσωπεύει τη λειτουργία της δυνατότητας: «Κινητικότητα Συσκευής».

Εικόνα 1-9: Κινητικότητα Συσκευής – Διάγραμμα Ροής Διαδικασίας

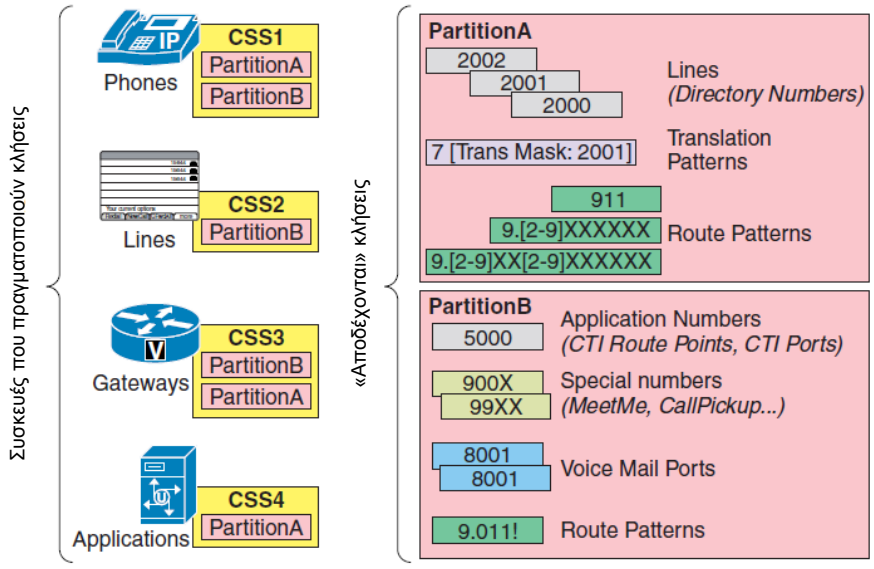


Partitions και Calling Search Spaces

Ένα Partition αποτελεί μια λογική ομαδοποίηση αριθμών καταλόγου (Directory Numbers-DNs) και διαγραμμάτων δρομολόγησης με ομοειδή χαρακτηριστικά προσβασιμότητας. Οι συσκευές που τοπικά τοποθετούνται σε Partitions περιέχουν DNs και διαγράμματα δρομολόγησης. Αυτές οι οντότητες σχετίζονται με τα DNs που οι χρήστες καλούν. Για απλοποίηση των Partitions συνήθως δηλώνουν τα χαρακτηριστικά τους, όπως «NYLongDistancePT», «NY911PT» κοκ.

Ένα calling search space αποτελεί μια λίστα από Partitions που οι χρήστες μπορούν να ανατρέξουν πριν τους επιτραπεί να κάνουν μια κλήση. Τα calling search space καθορίζουν τα Partitions , τα οποία οι συσκευές κλήσεις, συμπεριλαμβανομένων IP τηλέφωνων, soft phones και gateways, μπορούν να ανατρέξουν όταν επιχειρούν να ολοκληρώσουν μια κλήση.

Εικόνα 1-10: Partitions και Calling Search Spaces



[1]

Όπως έχει ήδη αναφερθεί τα calling search space καθορίζουν τα Partitions, τα οποία οι συσκευές μπορούν να ανατρέξουν όταν επιχειρούν να ολοκληρώσουν μια κλήση. Για παράδειγμα, υποθέτουμε ότι ένα calling search space με όνομα «Executive- Ανώτατο» περιέχει 4 Partitions: NYLongDistance - μακράς αποστάσεως, NYInternational - διεθνές, NYLocalCall - τοπική κλήση και NY911. Υποθέτουμε ότι ένα άλλο calling search space με όνομα «Guest- Επισκέπτης» περιέχει 2 Partitions: NY911 και NYLocalCall- τοπική κλήση.

Αν υποθέσουμε πως ένα IP τηλέφωνο βρίσκεται στο "Executive" CSS, όταν κάποιος επιχειρήσει να πραγματοποίησει μια κλήση, τότε η αναζήτηση γίνεται στα Partitions "NYLongDistance," "NYInternationalCall," "NYLocalCall," και "NY911". Ως εκ τούτου οι χρήστες που καλούν από το νούμερο αυτό μπορούν να κάνουν διεθνείς κλήσεις, μακρινές και τοπικές κλήσεις και κλήσεις στο 911. Αντίστοιχα αν είναι συνδεδεμένο με το "Guest" CSS, τότε η αναζήτηση γίνεται μόνο στα partitions "NYLocalCall" και "NY911" και κατά συνέπεια αν ο χρήστης επιχειρήσει να πραγματοποιήσει μια διεθνή κλήση, δε θα γίνει ταυτοποίηση-σύνδεση με αποτέλεσμα να μην μπορεί να ολοκληρωθεί.

Αυτοματοποιημένη Εναλλακτική Δρομολόγηση

Όταν το IP δίκτυο δεν έχει αρκετό διαθέσιμο εύρος ζώνης για την επεξεργασία μιας κλήσης, ο CallManager χρησιμοποιεί το μηχανισμό ελέγχου αποδοχής κλήσης (CAC) για να καθορίσει τι θα κάνει με την κλήση. Γενικά ανάλογα με τη ρύθμιση που έχει επιλεγεί, ο CallManager εκτελεί μια από παρακάτω ενέργειες:

1. Αστοχία κλήσης, ο καλών ακούει το χαρακτηριστικό τόνο κατειλημμένης γραμμής και βλέπει το μήνυμα Bandwidth Unavailable στην οθόνη. Σε περίπτωση βίντεο-κλήσης, γίνεται επανάκληση άλλα ως ήχο-κλήση.
2. Χρήση της Αυτοματοποιημένης Εναλλακτικής Δρομολόγησης (Automated Alternate Routing, AAR) για την αλλαγή πορείας της κλήσης μέσω μιας εναλλακτικής διαδρομής, όπως μια πύλη PSTN.

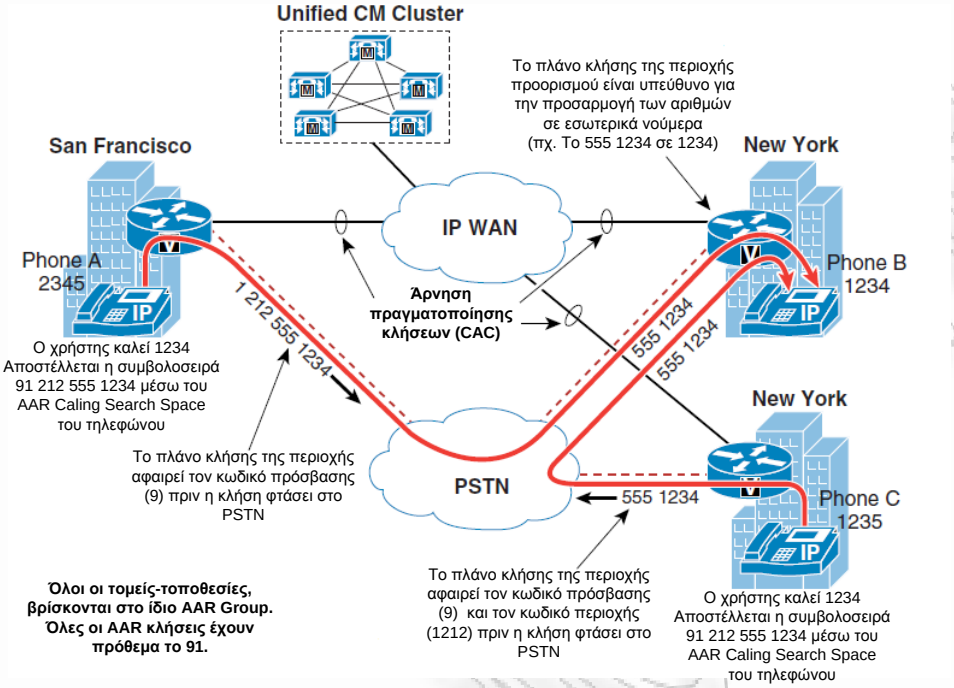
Για να είναι εφικτή η χρήση της AAR δυνατότητας για φωνή και βίντεο, πρέπει η συσκευή αυτού που πραγματοποιεί την κλήση και η συσκευή του καλούμενου να είναι μέλη μιας AAR ομάδας, επίσης απαιτείται να έχει οριστεί μια μάσκα εξωτερικού αριθμού κλήσεως για την καλούμενη συσκευή. Η μάσκα εξωτερικού αριθμού κλήσης τηλεφώνου ορίζει ολόκληρη την έγκυρη E.164 διεύθυνση για το εσωτερικό του καλούμενου χρήστη. Επίσης η ομάδα AAR ορίζει τι ψηφία πρέπει να προηγούνται της μάσκας της καλούμενης συσκευής προκειμένου η κλήση να δρομολογηθεί με επιτυχία μέσω του PSTN δικτύου καθώς καθορίζει ποια πύλη θα χρησιμοποιηθεί για την αναδρομολογημένη κλήση. Για αυτούς ακριβώς τους λόγους οι συσκευές δεν επιτρέπεται να ανήκουν σε περισσότερες από μια AAR ομάδες. Ως εκ τούτου, πρέπει να γίνεται πολύ προσεκτικά η κατασκευή των AAR groups και AAR Calling Search Spaces για να εξασφαλισθεί πως σε κάθε AAR κλήση προηγούνται τα σωστά ψηφία και χρησιμοποιείται το σωστό CSS.

Για παράδειγμα, ας υποθέσουμε ότι ο Α χρήστης βρίσκεται στην San Jose AAR ομάδα και ο Β χρήστης στην San Francisco AAR ομάδα. Το εσωτερικό νούμερο του Β χρήστη είναι το 51212 και η μάσκα εξωτερικού αριθμού κλήσης είναι ο αριθμός 6505551212. Επίσης έχει οριστεί πως τα ψηφία που πρέπει να προηγούνται για κλήσεις μεταξύ των δυο AAR ομάδων, δηλαδή μεταξύ San Francisco AAR group και San Jose AAR group είναι τα 9 και 1. Έτσι, αν ο Α χρήστης πληκτρολογήσει 51212 και δεν υπάρχει το απαραίτητο εύρος ζώνης στο IP WAN για να εξυπηρετήσει την κλήση μεταξύ των δυο τοποθεσιών, ο Cisco Unified CallManager θα χρησιμοποιήσει τη μάσκα του Β χρήστη, δηλαδή τον αριθμό 6505551212 με το πρόθεμα 91 και θα πραγματοποιήσει μια νέα κλήση στον αριθμό 916505551212 χρησιμοποιώντας τη δυνατότητα AAR CSS για το χρήστη Α.

Τοποθεσίες που βρίσκονται στην Ίδια Τοπική Περιοχή Κλήσης

Σε ορισμένες περιπτώσεις, η AAR συμβολοσειρά κλήσης απαιτείται να τροποποιηθεί τοπικά για να καταστεί δυνατή μια τοπική κλήση. Για παράδειγμα, ας υποθέσουμε δυο διαφορετικές περιοχές στην NY που μοιράζονται τον ίδιο κωδικό περιοχής 212 (βλ Εικόνα 1-10). Σε αυτή την περίπτωση ένας αριθμός που καλείται ως 91 212 5555 1234 θα πρέπει να μετατραπεί σε 9 5555 1234. Η μετατροπή αυτή πραγματοποιείται καλύτερα με ένα μοντέλο μετάφρασης όπου αφαιρεί τα ψηφία πριν την τελεία και εν συνεχεία προσθέτει το 9, πχ το 91212.555XXXX μεταφράζεται σε 9555XXXX. Αυτό το πρότυπο μετάφρασης-κανόνας, πρέπει να τοποθετηθεί μόνο στο AAR CSS της Νέας Υόρκης. Αντίθετα το San Francisco χρειάζεται ολόκληρη τη συμβολοσειρά 91 212 5555 1234 για να καλέσει τον ίδιο προορισμό στη Νέα Υόρκη οπότε ο παραπάνω κανόνας δεν πρέπει να προστεθεί στο AAR CSS του. Επίσης το παραπάνω μοντέλο μετάφρασης πρέπει να καταχωρηθεί και στο σχέδιο κλήσης της Νέας Υόρκης για την παροχή κατάλληλης δρομολόγησης των τοπικών προσβάσιμων αριθμών που καλούνται ως υπεραστικά. Έτσι το σχέδιο κλήσης στη Νέα Υόρκη είναι υπεύθυνο για την αποδοχή της συμβολοσειράς 9 555 1234 ως έγκυρης και τη μετατροπή της σε 555 1234 πριν την αποστολή της κλήσης στο PSTN.

Εικόνα 1-11: Πραγματοποίηση AAR Κλήσεων Μεταξύ Περιοχών



[1]

Κεφάλαιο 2ο

2. Τηλεπικοινωνιακή Κίνηση

2.1 Ανάλυση Τηλεπικοινωνιακής Κίνησης

2.1.1 Γενικά

Τα δίκτυα είτε φωνής είτε δεδομένων σχεδιάζονται γύρω από διαφορετικές μεταβλητές. Δυο από τους πιο βασικούς παράγοντες που πρέπει να ληφθούν υπόψη κατά το σχεδιασμό δικτύων είναι η υπηρεσία και η τιμή. Η υπηρεσία-εξυπηρέτηση είναι βασική για να συντηρείται η ικανοποίηση του πελάτη, ενώ η τιμή είναι ένας παράγοντας για τη συντήρηση του κέρδους. Ένας τρόπος για να επιτευχτεί η ποιοτική υπηρεσία και η συγκράτηση του κόστους των δικτύων, είναι η βελτιστοποίηση της χρήσης των κυκλωμάτων. Στο κεφάλαιο αυτό γίνεται αναφορά στις διαφορετικές τεχνικές σχεδιασμού, καθώς και στη μεθοδολογία για ακριβή μέτρηση του φορτίου κίνησης στα ευαίσθητα IP δίκτυα φωνής. Επιπλέον αναλύονται τα βασικά μοντέλα κίνησης, τα εργαλεία υπολογισμού φορτίου κίνησης, ο τρόπος χρήσης των πινάκων πιθανοτήτων καθώς και ο τρόπος επιλογής δρομολογητή για κάθε κόμβο του δικτύου με βάση το μέγιστο φορτίο κίνησης που πρέπει να εξυπηρετεί. Όλα τα παραπάνω έχουν σαν μοναδικό στόχο το σχεδιασμό ισχυρών και αποτελεσματικών δικτύων φωνής.

2.1.2 Βασική θεωρία Τηλεπικοινωνιακής Κίνησης

Οι σχεδιαστές δικτύων χρειάζονται ένα τρόπο σωστής μέτρησης της χωρητικότητας δικτύων λόγω της αύξησης των απαιτήσεων. Η θεωρία της τηλεπικοινωνιακής κίνησης δίνει τη δυνατότητα στους σχεδιαστές δικτύων να κάνουν υποθέσεις για τα δίκτυα βασιζόμενοι στην εμπειρία του παρελθόντος. Ως κίνηση ορίζεται είτε το μέγεθος της δραστηριότητας ενός κυκλώματος, είτε ο αριθμός των μηνυμάτων που διαχειρίζεται ένας τηλεπικοινωνιακός μεταγωγέας σε ένα συγκεκριμένο χρονικό διάστημα. Η κίνηση περιλαμβάνει τη σχέση μεταξύ προσπαθειών κλήσης σε έναν ευαίσθητο τηλεπικοινωνιακό εξοπλισμό με την ταχύτητα που αυτές οι κλήσεις ολοκληρώνονται. Η ανάλυση της κίνησης δίνει τη δυνατότητα να καθοριστεί το εύρος ζώνης που χρειάζεται στα κυκλώματα δεδομένων και φωνής. Ο υπολογισμός της κίνησης αναφέρεται σε θέματα εξυπηρέτησης δίνοντας τη δυνατότητα καθορισμού ποιότητας εξυπηρέτησης ή πιθανότητα συμφόρησης. Ένα ορθά σχεδιασμένο δίκτυο έχει χαμηλή πιθανότητα συμφόρησης τηλεπικοινωνιακής κίνησης και μεγάλο βαθμό εξυπηρέτησης, που σημαίνει ότι η εξυπηρέτηση μεγαλώνει και το κόστος μειώνεται. Κατά την ανάλυση της κίνησης πρέπει να ληφθούν διαφορετικοί παράγοντες υπόψη, οι πιο σημαντικοί παράγοντες είναι οι ακόλουθοι:

- Φορτίο κίνησης (Traffic load)
- Βαθμός εξυπηρέτησης (Grade of Service)
- Τύποι κίνησης (Traffic types)
- Δειγματοληπτικές μέθοδοι (Sampling methods)

Φυσικά και άλλοι παράγοντες μπορεί να επηρεάσουν τα αποτελέσματα των υπολογισμών της ανάλυσης, αλλά οι παραπάνω είναι οι βασικότεροι.

2.1.3 Υπολογισμός Φορτίου Κίνησης

Στη θεωρία της κίνησης υπολογίζεται το φορτίο κίνησης. Ως φορτίο κίνησης (traffic load) ορίζεται η συνολική διάρκεια όλων των κλήσεων εντός ενός χρονικού διαστήματος που λαμβάνεται ως μονάδα. Οι μονάδες μέτρησης βασίζονται στον Μέσο Χρόνο Διάρκειας Κλήσης (Average Hold Time, AHT). Ο AHT ορίζεται ως ο συνολικός χρόνος όλων των κλήσεων που πραγματοποιούνται σε συγκεκριμένο χρονικό διάστημα προς το συνολικό αριθμό των κλήσεων στο συγκεκριμένο χρονικό διάστημα. Για παράδειγμα:

$$\frac{\text{3976 sec (συνολικός χρόνος όλων των κλήσεων)}}{\text{23 κλήσεις}} = \text{172.87 sec κάθε κλήση = AHT}$$

Οι δυο κύριες μονάδες μέτρησης που χρησιμοποιούνται σήμερα για το φορτίο κίνησης είναι οι ακόλουθες:

- Erlangs
- Centum Call Seconds (CCS)

Το 1918 ο A.K. Erlang ανέπτυξε τύπους που με την χρήση τους μπορούσε να προβλέψει την τυχαία παραγόμενη εισερχόμενη τηλεπικοινωνιακή κίνηση. Το Erlang (η μέτρηση της τηλεφωνικής κίνησης) ονομάστηκε προς τιμήν του. Ένα Erlang ορίζεται ως 3600 sec κλήσεων στο ίδιο κύκλωμα ή αρκετό φορτίο κίνησης ώστε να διατηρηθεί ένα κύκλωμα απασχολημένο για μια ώρα.

$$\text{Traffic Load(erl)} = \frac{\text{total holding time (sec)}}{3600} = \frac{\text{number of calls x AHT}}{3600}$$

Για παράδειγμα:

$$\frac{\text{23 calls x 172.87 AHT}}{3600} = \text{1.104 Erlangs}$$

Το CCS βασίζεται στα 100 sec κλήσεων στο ίδιο κύκλωμα. Οι μεταγωγείς φωνής γενικά μετρούν το μέγεθος του φορτίου κίνησης σε CCS.

$$\text{Traffic Load(CCS)} = \frac{\text{total holding time (sec)}}{100} = \frac{\text{number of calls x AHT}}{100}$$

Για παράδειγμα:

$$\frac{\text{23 calls x 172.87 AHT}}{100} = \text{39.76 CCS}$$

Ποιο μέγεθος επιλέγεται, καθορίζεται από τον εκάστοτε εξοπλισμό και τη μονάδα που χρησιμοποιεί αυτός. Πολλοί μεταγωγείς χρησιμοποιούν το CCS γιατί είναι ευκολότερο να δουλεύεις με αυξητικό βήμα των 100 παρά των 3600. Και οι δυο μετρήσεις αναγνωρίζονται σαν πρότυπα. Από τις ανωτέρω σχέσεις συμπεραίνουμε ότι η σχέση μεταξύ Erlang και CCS είναι:

$$\text{1 Erlangs = 36 CCS}$$

Όπως ήδη έχει αναφερθεί για να οριστεί η κίνηση σε Erlangs αρκεί να ληφθούν τα συνολικά δευτερόλεπτα κλήσεων σε μια ώρα και να διαιρεθούν με 3600 sec. Επιπλέον υπάρχει η δυνατότητα να χρησιμοποιηθεί ο μέσος όρος διαφορετικών χρονικών περιόδων. Αυτοί οι μέσοι όροι επιτρέπουν τη χρήση περισσοτέρων δειγμάτων από χρονικές περιόδους για τον καθορισμό της σωστής κίνησης.

2.1.4 Κίνηση σε Ώρα Αιχμής (Busy Hour Traffic)

Συνήθως ο υπολογισμός της κίνησης πραγματοποιείται κατά την ώρα αιχμής, διότι τότε φαίνεται το μέγιστο φορτίο που δύναται να υποστηρίξει το δίκτυο. Η μέτρηση αυτή δίνει τη μονάδα μέτρησης που συχνά αναφέρεται ως *Κίνηση σε Ώρα Αιχμής* (Busy Hour Traffic, BHT). Κάποιες φορές δεν μπορεί να γίνει ακριβής δειγματοληψία ή υπάρχει μόνο εκτίμηση των καθημερινά ληφθεισών κλήσεων. Σε αυτή την περίπτωση συνήθως γίνονται υποθέσεις σχετικά με το επιχειρησιακό περιβάλλον, όπως ο μέσος αριθμός των κλήσεων ανά ημέρα και το AHT. Σε ένα πρότυπο επιχειρησιακό περιβάλλον κατά τη διάρκεια ώρας αιχμής σε μια μέρα, πραγματοποιείται το 15-20% της ημερήσιας τηλεπικοινωνιακής κίνησης. Γενικά κατά τους υπολογισμούς της ώρας (μέγιστης) αιχμής χρησιμοποιείται το 17% της ημερήσιας κίνησης. Σε πολλά επιχειρησιακά περιβάλλοντα, ένας αποδεκτός μέσος χρόνος διάρκειας κλήσης (AHT) θεωρείται τα 180-210 sec. Αυτοί οι υπολογισμοί μπορούν να χρησιμοποιηθούν σε περίπτωση καθορισμού απαιτήσεων trunking[3] χωρίς να υπάρχουν ολοκληρωμένα δεδομένα.

2.1.5 Μετρήσεις Χωρητικότητας Δικτύου

Πολλές είναι οι μονάδες μέτρησης όπου μπορούν να χρησιμοποιηθούν με σκοπό τη μέτρηση της χωρητικότητας ενός δικτύου. Για παράδειγμα:

- Απόπειρες κλήσης στην ώρα αιχμής (Busy Hour Call Attempts, BHCA)
- Περαιωμένες κλήσεις στην ώρα αιχμής (Busy Hour Call Completions, BHCC)
- Κλήσεις ανά δευτερόλεπτο (Calls per seconds, CPS)

Όλοι αυτοί οι δείκτες είναι βασισμένοι στον αριθμό των κλήσεων. Οι δείκτες αυτοί περιγράφουν τη χωρητικότητα του δικτύου αλλά ουσιαστικά είναι ασήμαντοι για την ανάλυση της κίνησης γιατί δεν συνυπολογίζουν την ώρα αναμονής της κλήσης. Οι δείκτες αυτοί πρέπει να χρησιμοποιηθούν συνδυαστικά με τον AHT για να υπολογιστεί ένα BHT που μπορεί να χρησιμοποιηθεί για την ανάλυση της κίνησης.

2.1.6 Βαθμός Εξυπηρέτησης (GoS)

Όταν υπάρχει συμφόρηση και η εισερχόμενη κλήση μπλοκάρεται και εγκαταλείπει το σύστημα, τότε αυτό καλείται σύστημα απωλειών (loss or non delay system). Αν όμως η κλήση μπορεί να αναμένει έως ότου πραγματοποιηθεί σύνδεση, τότε αυτό καλείται σύστημα αναμονής (waiting or delay system). Το ποσοστό των κλήσεων που χάνονται ή καθυστερούν να διεκπεραιωθούν λόγω συμφόρησης είναι ένας δείκτης της ποιότητας εξυπηρέτησης που παρέχεται από το τηλεπικοινωνιακό σύστημα ή την υπηρεσία (service), όπως λέμε. Καλείται βαθμός εξυπηρέτησης (Grade of Service, GoS ή Percent Blockage).

Για ένα σύστημα απωλειών ο βαθμός εξυπηρέτησης ορίζεται ως εξής:

$$GoS = \frac{\text{Συνολικός Αριθμός Χαμένων Κλησεών}}{\text{Συνολικός Αριθμός Προσφερθεισών Κλησεών}} = \frac{\text{Κίνηση που Χάθηκε}}{\text{Κίνηση που Προσφέρθηκε}}$$

Βάσει του ορισμού προκύπτει ότι ο βαθμός εξυπηρέτησης είναι μικρότερος ή ίσος της μονάδας. Όσο μεγαλύτερος είναι ο βαθμός εξυπηρέτησης, τόσο χειρότερο είναι το σύστημα.

Συνεπώς λέγοντας βαθμό εξυπηρέτησης εννοούμε την πιθανότητα που υπάρχει να μπλοκαριστούν οι κλήσεις κατά την προσπάθεια να καταλάβουν το κύκλωμα. Γράφεται ως P.xx

[3] Ο όρος trunk χρησιμοποιείται από τους τηλεπικοινωνιακούς μηχανικούς για να περιγράψουν κάθε ποσότητα που μπορεί να εξυπηρετήσει (διεκπεραιώσει) μια κλήση. Trunk, μπορεί να είναι ένα διεθνές κύκλωμα μήκους χιλιάδων χιλιομέτρων, ή ένα σύρμα λίγων μέτρων μεταξύ δυο διακοπτών ενός τηλεφωνικού κέντρου. Η διάταξη των trunks και των διακοπτών (switches) ενός τηλεφωνικού κέντρου καλείται trucking.

βαθμός συμφόρησης, όπου xx είναι το ποσοστό των κλήσεων που μπλοκάρονται σε ένα σύστημα κίνησης. Για παράδειγμα για εγκαταστάσεις κίνησης που απαιτούν P.01 GoS ορίζεται ως 1% πιθανότητα των κλήσεων να μπλοκαριστούν στις εγκαταστάσεις. Ένα P.00 GoS, σπάνια απαιτείται και σπάνια συμβαίνει. Αυτό γιατί για να υπάρχει 100% σιγουριά ότι δεν θα υπάρχει συμφόρηση, πρέπει να σχεδιαστεί ένα δίκτυο όπου η αναλογία χρήστη κυκλώματος να είναι 1:1. Όλοι σχεδόν οι τύποι υπολογισμού κίνησης υποθέτουν άπειρο αριθμό κλήσεων.

2.1.7 Τύποι Κίνησης

Ο τηλεπικοινωνιακός εξοπλισμός της προσφερόμενης κίνησης μπορεί να χρησιμοποιηθεί για την καταγραφή των δεδομένων. Δυστυχώς περισσότερα από τα δείγματα βασίζονται στη διεκπεραιωμένη κίνηση (carried traffic) και όχι στο προσφερόμενο φορτίο κίνησης. Διεκπεραιωμένη κίνηση είναι η κίνηση η οποία εξυπηρετείται από τον τηλεπικοινωνιακό εξοπλισμό, ενώ η προσφερόμενη κίνηση (offered traffic) είναι οι πραγματικές προσπάθειες κλήσης σε ένα σύστημα. Η διαφορά των δυο παραπάνω καλείται απώλειες (traffic lost) και μπορεί να δημιουργήσει ανακρίβειες στους υπολογισμούς. Όσο μεγαλύτερος είναι ο βαθμός συμφόρησης τόσο μεγαλύτερη είναι η διαφορά μεταξύ προσφερόμενης και διεκπεραιωμένης κίνησης. Μπορεί να χρησιμοποιηθεί η παρακάτω φόρμουλα για τον υπολογισμό προσφερόμενου από διεκπεραιωμένο φορτίου:

$$\text{Offered Load} = \frac{\text{Caried Load}}{\text{1-Blocking Factor}}$$

οπου:

Offered Load: Προσφερόμενο Φορτίο

Caried Load: Διεκπεραιωμένο Φορτίο

Blocking Factor: Βαθμός Συμφόρησης

Δυστυχώς αυτή η φόρμουλα δεν λαμβάνει υπόψη τις προσπάθειες επανάκλησης όταν η κλήση απορριφθεί. Μπορεί να χρησιμοποιηθεί η παρακάτω σχέση για να υπολογιστεί και η προσπάθεια επανάκλησης:

$$\text{Offerd Load} = \text{Caried Load} \times \text{Offered Load Adjustment Factors (OAF)}$$

με

$$\text{OAF} = \frac{\text{1.0-(R x Blocking Factor)}}{\text{1.0-Blocking Factor}}$$

Όπου το R ορίζει το ποσοστό της πιθανότητας να υπάρξει επανάκληση, πχ R=0.6 για 60% ποσοστό επανάκλησης.

Η ακριβής ανάλυση της κίνησης, βασίζεται επίσης στην ακρίβεια των δειγματοληπτικών μεθόδων. Οι παρακάτω παράγοντες είναι ορισμένοι από αυτούς που επηρεάζουν το φορτίο κίνησης:

- Καθημερινές σε σύγκριση με Σαββατοκύριακα
- Αργίες
- Τύπος κίνησης
- Φερόμενο σε σύγκριση με Προσφερόμενο φορτίο
- Περίοδος δειγματοληψίας
- Σύνολο δειγμάτων
- Σταθερότητα δειγματοληπτικής περιόδου

Η θεωρία πιθανοτήτων δηλώνει ότι για να εκτιμηθεί σωστά η δικτυακή κίνηση φωνής, θα πρέπει μέσα στο δειγματοληπτικό διάστημα να υπάρχουν τουλάχιστον 30 ώρες αιχμής. Αν και αυτό είναι ένα καλό σημείο εκκίνησης, υπάρχουν και άλλες μεταβλητές που μπορούν να παραποιήσουν την ακρίβεια των δειγμάτων. Για παράδειγμα, δε μπορεί να παρθούν τα 30 υψηλοτέρα δείγματα μέσα από ένα σύνολο 32 δειγμάτων και να θεωρηθεί ότι υπάρχει ακριβής εικόνα. Για να υπάρξουν ακριβή αποτελέσματα, πρέπει να ληφθούν όσο το δυνατόν περισσότερα δείγματα του προσφερόμενου φορτίου. Εναλλακτικά αν λαμβάνονται δείγματα όλο το χρόνο, τα αποτελέσματα ανά έτος για το φορτίο κίνησης μπορεί να είναι ασύμμετρα, δηλαδή να παρατηρείται μείωση ή αύξηση του φορτίου. Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU-T) προβαίνει σε συστάσεις για το πώς πρέπει να λαμβάνονται δείγματα από ένα δίκτυο στη σωστή διάσταση.

Η ITU-T συνιστά σε ένα δημόσιο τηλεφωνικό δίκτυο μεταγωγής (PSTN), η δειγματοληπτική περίοδος πρέπει να είναι ίση με 60 λεπτά ή / και 15 λεπτά. Τα διαστήματα αυτά είναι σημαντικά διότι συνοψίζουν την ένταση της κίνησης κατά τη διάρκεια μιας χρονικής περιόδου. Αν λαμβάνονται μετρήσεις κατά τη διάρκεια της ημέρας, μπορεί να προσδιοριστεί η ώρα μέγιστης κίνησης σε κάθε δεδομένη ημέρα. Υπάρχουν δυο συνιστάμενοι τρόποι για τον προσδιορισμό ημερήσιας μέγιστης κίνησης, όπως παρακάτω:

- **Ημερήσια Περίοδος Αιχμής** (Daily Peak Period, DPP), καταγράφει το μεγαλύτερο όγκο κίνησης που μετράται κατά τη διάρκεια μιας ημέρας. Η μέθοδος αυτή απαιτεί συνεχείς μετρήσεις και τυπικά χρησιμοποιείται σε περιβάλλοντα όπου η ώρα αιχμής μπορεί να διαφέρει από μέρα σε μέρα.
- **Ημερήσια Μέτρηση σε Σταθερά Διαστήματα** (Fixed Daily Measurement Interval, FDMI), απαιτεί μετρήσεις μόνο κατά τη διάρκεια των προκαθορισμένων περιόδων αιχμής. Χρησιμοποιείται όταν το πρότυπο κίνησης είναι κάπως προβλέψιμο και οι περίοδοι αιχμής συμβαίνουν σε τακτά χρονικά διαστήματα. Σε επιχειρησιακά περιβάλλοντα οι χρονικές περίοδοι αιχμής της κίνησης είναι γύρω στις 10:00 π.μ. με 11:00 π.μ. και 2:00 μ.μ. με 3:00 μ.μ.

Στο παράδειγμα του Πίνακα 2-1 χρησιμοποιείται FDMI δειγματοληψία. Συμπεραίνουμε πως η ώρα με το υψηλότερο φορτίο κίνησης είναι 10:00 π.μ. και το συνολικό φορτίο κίνησης είναι 60.6 Erlangs.

Πίνακας 2-1: Υπολογισμός Συνολικού Φορτίου με Χρήση FDMI Δειγματοληψίας

Ώρα	Δευτέρα	Τρίτη	Τετάρτη	Πέμπτη	Παρασκευή	Συνολικό Φορτίο
9:00 π.μ.	12.7	11.5	10.8	11.0	8.6	54.6
10:00 π.μ.	12.6	11.8	12.5	12.2	11.5	*60.6*
11:00 π.μ.	11.1	11.3	11.6	12.0	12.3	58.3
12:00 μ.μ.	9.2	8.4	8.9	9.3	9.4	45.2
13.00 μ.μ.	10.1	10.3	10.2	10.6	9.8	51.0
14.00 μ.μ.	12.4	12.2	11.7	11.9	11.0	59.2
15.00 μ.μ.	9.8	11.2	12.6	10.5	11.6	55.7
16.00 μ.μ.	10.1	11.1	10.8	10.5	10.2	52.7

Στο παράδειγμα του Πίνακα 2-2 για τον υπολογισμό του συνολικού φορτίου κίνησης χρησιμοποιείται DPP δειγματοληψία.

Πίνακας 2-2: Υπολογισμός Συνολικού Φορτίου με Χρήση DPP Δειγματοληψίας

	Δευτέρα	Τρίτη	Τετάρτη	Πέμπτη	Παρασκευή	Συνολικό Φορτίο
Κίνηση Αιχμής	12.7	12.2	12.5	12.2	12.3	61.9
Ώρα Κίνησης Αιχμής	9:00 π.μ.	2:00 μ.μ.	10:00 π.μ.	10:00 π.μ.	11:00 π.μ.	

Επίσης υπάρχει η δυνατότητα να τμηματοποιηθεί η ημερήσια μέτρηση σε ομάδες με ίδια στατιστική συμπεριφορά. Σύμφωνα με την ITU-T οι ομάδες αυτές ορίζονται ως: *εργάσιμες*,

σαββατοκύριακα και *ειδικές ετήσιες εξαιρέσεις*. Η ομαδοποίηση των μετρήσεων που έχουν την ίδια στατιστική συμπεριφορά καθίσταται σημαντική διότι ημέρες με εξαιρετικά υψηλό ημερήσιο όγκο κλήσεων (πχ όπως η μέρα των Χριστουγέννων) μπορεί να παραποιήσουν τα αποτελέσματα.

Η σύσταση E.492 της ITU-T περιλαμβάνει οδηγίες για τον καθορισμό της κανονικής και υψηλής έντασης φορτίου κίνησης για το μήνα. Ορίζει ως κανονική ένταση φορτίου κίνησης για το μήνα, την τέταρτη υψηλότερη ημερήσια κίνηση αιχμής. Ενώ, επιλέγοντας τη δεύτερη υψηλότερη μέτρηση του μήνα, θα έχει ως αποτέλεσμα την υψηλή ένταση φορτίου κίνησης. Το αποτέλεσμα επιτρέπει τον υπολογισμό του αναμενόμενου μηνιαίου φορτίου κίνησης.

2.1.8 Κριτήρια Επιλογής Μοντέλου Κίνησης

Γνωρίζοντας πλέον ποιες μετρήσεις είναι απαραίτητες, το επόμενο στάδιο είναι ο καθορισμός του τρόπου χρήσης τους. Συνεπώς πρέπει να επιλεγεί το κατάλληλο μοντέλο κίνησης. Τα βασικά χαρακτηριστικά που επηρεάζουν την επιλογή του κατάλληλου μοντέλου είναι:

- Διαγράμματα Άφιξης Κλήσεων
- Φραγμένες Κλήσεις
- Αριθμός Πηγών
- Διάρκεια Κλήσης

Διαγράμματα Άφιξης Κλήσεων

Το πρώτο βήμα στην επιλογή του κατάλληλου μοντέλου κίνησης είναι ο καθορισμός του τρόπου άφιξης κλήσεων. Τα διαγράμματα άφιξης κλήσεων είναι σημαντικά στην επιλογή του μοντέλου κίνησης διότι διαφορετικά διαγράμματα άφιξης επηρεάζουν ανάλογα τα μέσα κίνησης.

Τα τρία κύρια διαγράμματα άφιξης κλήσεων είναι τα ακόλουθα και περιγράφονται στις επόμενες ενότητες:

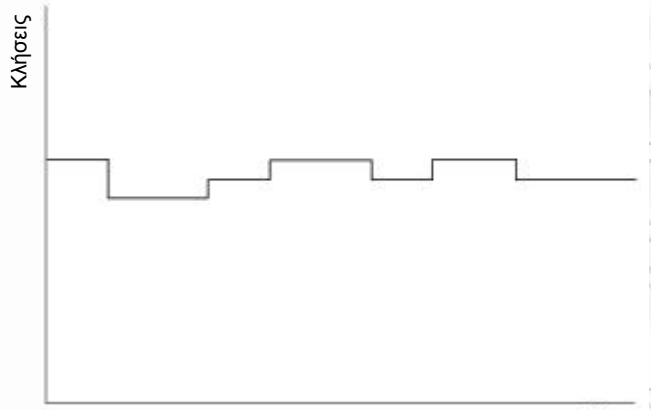
1. Διάγραμμα Ομαλής Άφιξης Κλήσεων
2. Διάγραμμα Υπερμεταβαλλόμενης Άφιξης Κλήσεων
3. Διάγραμμα Τυχαίας Άφιξης Κλήσεων

Διάγραμμα Ομαλής Άφιξης Κλήσεων

Ένα ομαλό ή υπό-εκθετικό διάγραμμα κίνησης εμφανίζεται όταν δεν υπάρχει ένα μεγάλο ποσό μεταβολής στην κίνηση. Η διάρκεια κλήσης και οι διαφιξιακοί χρόνοι μεταξύ των κλήσεων είναι στοιχεία προβλέψιμα, επιτρέποντας να προβλεφθεί η κίνηση σε κάθε δεδομένη περίσταση. Για παράδειγμα, υποθέτουμε ότι πρέπει να σχεδιαστεί ένα δίκτυο φωνής για μια εταιρία telemarketing όπου έχει μεγάλο εξερχόμενο φορτίο κίνησης διότι οι υπάλληλοι περνάνε όλη τη μέρα στο τηλέφωνο. Επιπλέον υποθέστε ότι σε διάστημα μιας ώρας θα μπορούσαν να πραγματοποιηθούν τριάντα (30) διαδοχικές κλήσεις των δυο (2) λεπτών η κάθε μια. Επομένως θα πρέπει για το χειρισμό των κλήσεων, να διατεθεί ένα κύκλωμα (trunk) για μια ώρα.

Για μια ομαλή άφιξη κλήσεων, ένα γράφημα των κλήσεων, συναρτήσει του χρόνου, μπορεί να μοιάζει με την Εικόνα 2-1.

Εικόνα 2-1: Διάγραμμα Ομαλής Άφιξης Κλήσεων



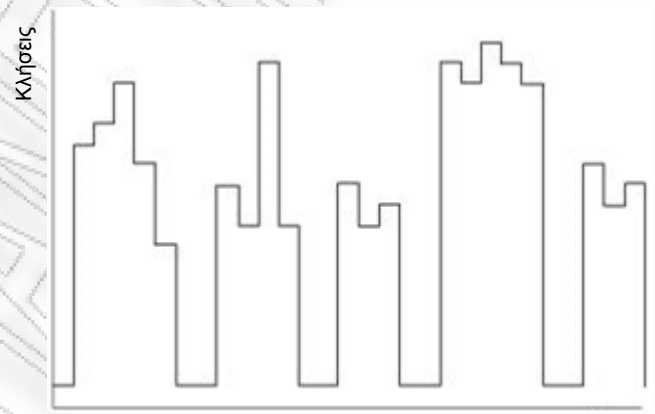
[3]

Διάγραμμα Υπερμεταβαλλόμενης Άφιξης Κλήσεων

Ένα διάγραμμα υπερμεταβαλλόμενης κίνησης έχει μεγάλες μεταβολές στην κίνηση σε σχέση με το μέσο όρο. Αυτό το μοντέλο άφιξης κλήσεων είναι γνωστό και ως υπέρ-εκθετικό μοντέλο άφιξης. Αποδεικνύει γιατί δεν είναι καλή ιδέα να συμπεριληφθούν ημέρες όπως τα Χριστούγεννα ή μια γιορτή κατά τη μελέτη της κίνησης. Μπορεί να υπάρξουν φορές που για να διαχειριστεί αυτό το πρότυπο κίνησης, θα χρειαστεί να αλλαχθούν οι ζευκτικές ομάδες. Ωστόσο, σε γενικές γραμμές, για τη σωστή διαχείριση της κίνησης αυτής και ιδιαίτερα σε ώρες αιχμής, απαιτείται να διατεθούν αρκετοί πόροι. Παράδειγμα για την ταυτόχρονη διαχείριση 30 κλήσεων απαιτούνται 30 trunks ή μια E1.

Για μια υπερμεταβαλλόμενη άφιξη κλήσεων, ένα γράφημα των κλήσεων συναρτήσει του χρόνου μπορεί να μοιάζει με την Εικόνα 2-2.

Εικόνα 2-2: Διάγραμμα Υπερμεταβαλλόμενης Άφιξης Κλήσεων



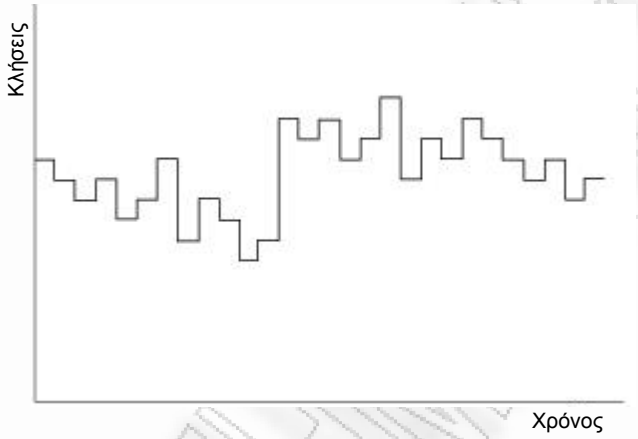
[3]

Διάγραμμα Τυχαίας Άφιξης Κλήσεων

Το διάγραμμα τυχαίας άφιξης κλήσεων είναι ακριβώς «τυχαίο». Είναι επίσης γνωστό και ως Poisson ή εκθετική κατανομή. Ο Poisson ήταν ο πρώτος μαθηματικός που όρισε αυτού του είδους την κατανομή. Διάγραμμα τυχαίας κίνησης συμβαίνει σε περίπτωση που υπάρχουν πολλές κλήσεις, όπου κάθε μια παράγει ένα μικρό κομμάτι της κυκλοφορίας. Γενικά αυτού του είδους η κίνηση συναντάται σε περιβάλλον PBX. Ο αριθμός των κυκλωμάτων που απαιτούνται σε αυτήν την κατάσταση συνήθως ποικίλει μεταξύ ένα (1) έως τριάντα (30) κυκλωμάτων.

Για μια τυχαία άφιξη κλήσεων, ένα γράφημα των κλήσεων συναρτήσει του χρόνου μπορεί να μοιάζει με την Εικόνα 2-3.

Εικόνα 2-3: Διάγραμμα Τυχαίας Άφιξης Κλήσεων



[3]

Φραγμένες Κλήσεις

Μια κλήση χαρακτηρίζεται «φραγμένη» όταν δεν εξυπηρετείται άμεσα. Οι κλήσεις θεωρούνται φραγμένες αν δρομολογούνται ξανά σε άλλη ζευκτική ομάδα (trunk group), τοποθετούνται σε μια ουρά αναμονής ή αναπαράγεται ένας ήχος ή ανακοίνωση. Η φύση των φραγμένων κλήσεων καθορίζει το μοντέλο που θα επιλεγεί διότι επηρεάζει το φορτίο κίνησης.

Οι βασικοί τύποι φραγμένων κλήσεων είναι οι ακόλουθοι:

- **Lost Calls Held** (LCH), αυτές οι φραγμένες κλήσεις χάθηκαν, δε θα πραγματοποιηθούν ποτέ ξανά.
- **Lost Calls Delayed** (LCD), αυτές οι φραγμένες κλήσεις παραμένουν στο σύστημα έως ότου οι εγκαταστάσεις είναι διαθέσιμες να εξυπηρετήσουν την κλήση.
- **Lost Calls Cleared** (LCC), αυτές οι φραγμένες κλήσεις «εκκαθαρίζονται» από το σύστημα, που σημαίνει ότι όταν μπλοκάρεται ο καλών, η κλήση δρομολογείται κάπου αλλού (κυρίως σε άλλες ευαίσθητες εγκαταστάσεις κίνησης).
- **Lost Calls Retried** (LCR), η LCR υποθέτει ότι μόλις μια κλήση αποκλειστεί, ένα ποσοστό από τους αποκλεισμένους καλούντες προσπαθούν ξανά όσες φορές χρειαστεί έως ότου εξυπηρετηθούν. Το μοντέλο LCR είναι ένα παράγωγο του LCC και χρησιμοποιείται στο Extended Erlang B μοντέλο.

Πλήθος Πηγών

Το πλήθος πηγών των κλήσεων έχει επίσης σχέση με το τι μοντέλο κίνησης θα επιλεγεί. Για παράδειγμα, αν υπάρχει μόνο μια πηγή και μια γραμμή (trunk), η πιθανότητα αποκλεισμού της

κλήσης είναι μηδέν. Καθώς ο αριθμός των πηγών αυξάνει, η πιθανότητα αποκλεισμού γίνεται υψηλότερη. Ο αριθμός των πηγών μπαίνει στο παιχνίδι όταν πρόκειται για PBX μικρού μεγέθους, όπου μπορεί να χρησιμοποιηθεί ένας μικρός αριθμός γραμμών και να φτάσει στον καθορισμένο βαθμό εξυπηρέτησης (GoS).

Μερικές φορές υπάρχει μια σημαντική διαφορά μεταξύ σχεδιασμού για άπειρο σε σχέση με το σχεδιασμό για μικρό αριθμό πηγών. Στο επόμενο παράδειγμα δε θα σταθούμε στον τρόπο υπολογισμού των τιμών του πίνακα. Ο πίνακας συγκρίνει το ποσό της κίνησης που απαιτείται από το σύστημα για την μεταφορά της κίνησης σε erlangs, με το ποσό των πιθανών πηγών της προσφερόμενης κίνησης. Υποθέτουμε ότι ο αριθμός των γραμμών (trunks) παραμένει σταθερός και ίσος με δέκα για .01 GoS.

Πίνακας 2-3: Κατανομή Poisson με 10 Γραμμές και P.01

Αριθμός Πηγών	Χωρητικότητα Κίνησης (erlangs)
Άπειρος	4.13
100	4.26
75	4.35
50	4.51
25	4.84
20	5.08
15	5.64
13	6.03
11	6.95
10	10

Μόνο 4.13 erlangs μεταφέρονται αν υπάρχει ένας άπειρος αριθμός πηγών. Ο λόγος για αυτό το φαινόμενο είναι ότι όταν ο αριθμός πηγών αυξάνεται, η πιθανότητα για ευρύτερη διανομή των κλήσεων στους χρόνους άφιξης και η διάρκεια κλήσεων αυξάνονται. Ενώ όταν ο αριθμός πηγών μειώνεται, η πιθανότητα να μεταφερθεί-εξυπηρετηθεί η κίνηση αυξάνεται. Στην τελική ακραία κατάσταση το σύστημα υποστηρίζει δέκα (10) erlangs και υπάρχουν μόνο δέκα πηγές. Συνεπώς διαστασιοποιώντας το PBX σε ένα απομακρυσμένο υποκατάστημα, μπορούν να καλυφθούν οι απαιτούμενες ανάγκες χρησιμοποιώντας λιγότερες γραμμές και προσφέροντας το ίδιο GoS.

Διάρκεια Κλήσης

Ορισμένα μοντέλα κίνησης λαμβάνουν υπόψη τη χρονική διάρκεια των κλήσεων. Αντίθετα τα περισσότερα δεν τη λαμβάνουν υπόψη κατά τους υπολογισμούς και αυτό διότι θεωρούν τους χρόνους συγκράτησης εκθετικούς. Γενικά, οι κλήσεις έχουν μικρούς και όχι μεγάλους χρόνους συγκράτησης. Γεγονός που σημαίνει ότι υπάρχουν φορές που οι χρόνοι συγκράτησης έχουν αρνητική εκθετική κατανομή.

2.1.9 Επιλογή Μοντέλου Κίνησης

Αφού έχει προσδιοριστεί το μοντέλο άφιξης κλήσεων, οι φραγμένες κλήσεις, ο αριθμός πηγών και η διάρκεια των κλήσεων, εν συνεχεία μπορεί να επιλεγεί το κατάλληλο μοντέλο κίνησης για το αντίστοιχο περιβάλλον. Ωστόσο κανένα μοντέλο κίνησης δεν μπορεί να ταιριάξει ακριβώς στις πραγματικές καταστάσεις αλλά κατά την επιλογή λαμβάνεται υπόψη ο μέσος όρος κάθε κατάστασης. Υπάρχουν πολλά διαφορετικά μοντέλα κίνησης. Το κλειδί είναι να βρεθεί το μοντέλο που ταιριάζει καλύτερα σε κάθε περιβάλλον. Μια σύγκριση των χαρακτηριστικών κάθε μοντέλου παρουσιάζεται στον Πίνακα 2-4.

Τα μοντέλα κίνησης με την ευρύτερη υιοθέτηση είναι τα: Erlang B, Extended Erlang B και Erlang C. Άλλα λιγότερο υιοθετημένα μοντέλα είναι τα: Engset, EART/EARC και Neal-Wilkerson.

Πίνακας 2-4: Σύγκριση Μοντέλων Κίνησης

Μοντέλο Κίνησης	Αριθμός Πηγών	Διάγραμμα Άφιξης	Μετακύλυση Φραγμένων Κλήσεων	Χρόνος Συγκράτησης
Poisson	Άπειρος	Τυχαίο	Συγκράτηση	Εκθετικός
Erlang B	Άπειρος	Τυχαίο	Αναδρομολόγηση	Εκθετικός
Extended Erlang B	Άπειρος	Τυχαίο	Επανάκληση	Εκθετικός
Erlang C	Άπειρος	Τυχαίο	Αναμονή	Εκθετικός
Engset	Πεπερασμένος	Ομαλό	Αναδρομολόγηση	Εκθετικός
EART/EARC	Άπειρος	Υπερμεταβαλόμενο	Αναδρομολόγηση	Εκθετικός
Neal-Wilkerson	Άπειρος	Υπερμεταβαλόμενο	Συγκράτηση	Εκθετικός
Crommelin	Άπειρος	Τυχαίο	Αναμονή	Σταθερός
Binomial	Πεπερασμένος	Τυχαίο	Συγκράτηση	Εκθετικός
Delay	Πεπερασμένος	Τυχαίο	Αναμονή	Εκθετικός

Erlang B Μοντέλο Κίνησης

Το Erlang B μοντέλο βασίζεται στις παρακάτω υποθέσεις:

- Άπειρος αριθμός πηγών
- Τυχαίο διάγραμμα άφιξης κλήσεων
- Οι φραγμένες κλήσεις αναδρομολογούνται
- Εκθετική κατανομή διάρκειας κλήσεων

Το μοντέλο Erlang B χρησιμοποιείται όταν οι φραγμένες κλήσεις αναδρομολογούνται που σημαίνει ότι δεν γυρνάνε πίσω στην αρχική ζευκτική ομάδα. Το μοντέλο προϋποθέτει τυχαίο διάγραμμα άφιξης κλήσεων. Αυτός που καλεί κάνει μια προσπάθεια και αν η κλήση μπλοκαριστεί τότε αναδρομολογείται. Το Erlang B μοντέλο χρησιμοποιείται για πρώτης προσπάθειας ζευκτικές ομάδες (trunk groups) όπου δεν λαμβάνεται υπόψη ο βαθμός επανάκλησης διότι οι κλήσεις επαναδρομολογούνται ή αναμένονται πολύ λίγες μπλοκαρισμένες.

Η επόμενη σχέση παρέχει τη φόρμουλα που χρησιμοποιείται για τον υπολογισμό του Erlang B μοντέλου κίνησης:

$$B(c,a)=\frac{\frac{a^c}{c!}}{\sum_{k=0}^{c}\frac{a^k}{k!}}$$

Όπου:

B(c,a): Η πιθανότητα αποκλεισμού της κλήσης

c: Ο αριθμός των κυκλωμάτων

α: Το φορτίο κίνησης

Παράδειγμα χρήσης του Erlang B μοντέλου: Χρειάζεται να επαναπροσδιοριστούν οι ζευκτικές ομάδες που εξυπηρετούν τις εξερχόμενες υπεραστικές κλήσεις διότι παρατηρείται συμφόρηση τις ώρες αιχμής. Τα στατιστικά του μεταγωγέα δηλώνουν ότι η ζευκτική ομάδα προσφέρει 17 Erlang κίνησης κατά την ώρα αιχμής. Είναι επιθυμητό να έχουμε χαμηλό βαθμό συμφόρησης ώστε να σχεδιαστεί αυτό για λιγότερο από 1% φραγή κλήσεων.

Λύση: Μελετώντας τους Erlang B πίνακες (βλ. Παράρτημα Β) συμπεραίνουμε ότι για 17 Erlang κίνησης με GoS 0.64 χρειάζονται 27 κυκλώματα για να διαχειριστούν το φορτίο.

Extended Erlang B Μοντέλο Κίνησης

Το Extended Erlang B μοντέλο βασίζεται στις παρακάτω υποθέσεις:

- Άπειρος αριθμός πηγών
- Τυχαίο διάγραμμα άφιξης κλήσεων
- Επανάκληση μετά από φραγή
- Εκθετική κατανομή διάρκειας κλήσεων

Το Extended Erlang B μοντέλο είναι σχεδιασμένο να λαμβάνει υπόψη του τις προσπάθειες επανάκλησης που πραγματοποιούνται με συγκεκριμένο ρυθμό. Το μοντέλο υποθέτει τυχαίο διάγραμμα άφιξης κλήσεων. Αυτοί που καλούν και μπλοκάρονται κάνουν πολλαπλές προσπάθειες επανάκλησης και δεν επιτρέπεται η υπερφόρτωση. Το Extended Erlang B χρησιμοποιείται για αυτοδύναμες ζευκτικές ομάδες.

Παράδειγμα χρήσης του Extended Erlang B μοντέλου: Ζητείται ο απαιτούμενος αριθμός κυκλωμάτων για κλήση εξυπηρετητή πρόσβασης. Είναι γνωστό ότι λαμβάνουμε 28 Erlang κίνησης κατά την ώρα αιχμής και ότι το αποδεκτό ποσοστό φραγής είναι 5%. Επίσης αναμένεται ότι το 50% των χρηστών θα πραγματοποιήσουν άμεση επανάκληση.

Λύση: Μελετώντας τους Extended Erlang B πίνακες, παρατηρείται ότι για την εξυπηρέτηση 28 Erlang κίνησης με πιθανότητα επανάκλησης 50% και 4% ποσοστό φραγής, απαιτούνται 35 κυκλώματα.

Erlang C Μοντέλο Κίνησης

Το Erlang C μοντέλο βασίζεται στις παρακάτω υποθέσεις:

- Άπειρος αριθμός πηγών
- Τυχαίο διάγραμμα άφιξης κλήσεων
- Οι φραγμένες κλήσεις μπαίνουν σε αναμονή
- Εκθετική κατανομή διάρκειας κλήσεων

Το Erlang C μοντέλο βασίζεται στη θεωρία ουρών. Το μοντέλο αυτό προϋποθέτει ένα τυχαίο μοτίβο άφιξης κλήσεων, ο καλών πραγματοποιεί μια κλήση η οποία διατηρείται σε μια ουρά αναμονής έως ότου ολοκληρωθεί. Το Erlang C μοντέλο εφαρμόζεται συχνά για τον υπολογισμό των πρακτόρων που απαιτούνται σε ένα σύστημα αυτόματης διανομής κλήσεων (Automatic Call Distributor). Επίσης μπορεί να χρησιμοποιηθεί για τον προσδιορισμό του εύρους ζώνης σε κυκλώματα μεταφοράς δεδομένων, αλλά δε χαρακτηρίζεται ως η καλύτερη επιλογή μοντέλου για το σκοπό αυτό. Στο μοντέλο Erlang C, απαραίτητη πληροφορία είναι ο αριθμός των κλήσεων ή πακέτων στην ώρα αιχμής, η μέση διάρκεια κλήσης ή το μέγεθος του πακέτου καθώς και η αναμενόμενη καθυστέρηση σε δευτερόλεπτα. Η επόμενη σχέση παρέχει τη φόρμουλα που χρησιμοποιείται για τον υπολογισμό του Erlang C μοντέλου κίνησης:

$$C(c,a)=\frac{\frac{a^c c}{c!\ c-a}}{\sum_{k=0}^{c-1}\frac{a^k}{k!}+\frac{a^c c}{c!\ c-a}}$$

Όπου:

C(c,a) είναι η πιθανότητα καθυστέρησης

c είναι ο αριθμός των κυκλωμάτων

α είναι το φορτίο κίνησης

Παράδειγμα χρήσης του Erlang C μοντέλου για Φωνή: Αναμένουμε ότι ένα τηλεφωνικό κέντρο θα δεχθεί περίπου 600 κλήσεις διάρκειας περίπου 3 λεπτών και ότι κάθε αντιπρόσωπος για 20 δευτερόλεπτα μετά το πέρας της συνομιλίας δε θα μπορεί να απαντήσει λόγω δουλειάς. Επιθυμητός μέσος χρόνος αναμονής στην ουρά είναι τα 10 δευτερόλεπτα.

Λύση: Υπολογισμός του αναμενόμενου φορτίου κίνησης: Είναι γνωστό ότι πραγματοποιούνται περίπου 600 κλήσεις διάρκειας 3 λεπτών η κάθε μια. Σε αυτό το χρόνο πρέπει να προστεθούν τα 20 sec που ο αντιπρόσωπος δεν απαντά. Τα επιπλέον 20 δευτερόλεπτα είναι μέρος του ποσού του χρόνου που απαιτείται για την εξυπηρέτηση μιας κλήσης, όπως φαίνεται στην επόμενη φόρμουλα:

$$\frac{600 \text{ calls} * (180+20) \text{ seconds AHT}}{3600} = 33.33 \text{ Erlang κίνησης}$$

Ο συντελεστής καθυστέρησης υπολογίζεται διαιρώντας τον αναμενόμενο χρόνο καθυστέρησης με το AHT, ως εξής:

$$\frac{10 \text{ sec (delay)}}{200 \text{ sec (AHT)}} = 0.05 \text{ delay factor}$$

Παράδειγμα χρήσης του Erlang C μοντέλου για Δεδομένα: Απαιτείται να σχεδιαστεί η δικτυακή σύνδεση κορμού μεταξύ δυο δρομολογητών. Αναμένονται 600 πακέτα ανά δευτερόλεπτο (pps), με 200 bytes ανά πακέτο, δηλαδή 1600 bits ανά πακέτο. Πολλαπλασιάζοντας 600 pps με 1600 bpp υπολογίζεται το ύψους του απαιτούμενου εύρους ζώνης ίσο με 960000 bps. Επιπλέον είναι γνωστό ότι υπάρχει η δυνατότητα αγοράς κυκλωμάτων που είναι πολλαπλάσια των 64,000 bps, το απαραίτητο ποσό δεδομένων για να διατηρηθεί το κύκλωμα απασχολημένο για 1 δευτερόλεπτο. Πόσα κυκλώματα απαιτούνται ώστε η καθυστέρηση να κρατηθεί κάτω των 10 ms;

Λύση: Υπολογισμός του φορτίου κίνησης:

$$\frac{960,000bps}{64,000bps} = 15 \; Erlangs$$

Υπολογισμός του μέσου χρόνου μετάδοσης πακέτου:

$$\frac{1600 \text{ bits per packet}}{64000 \text{ bits per sec}} = 0.025 \text{ sec} = 25 \text{ msec}$$

Ο συντελεστής καθυστέρησης υπολογίζεται διαιρώντας τον χρόνο καθυστέρησης με το χρόνο μετάδοσης πακέτου, ως εξής:

$$\frac{10 \text{ msec (delay)}}{25 \text{ msec (ATT)}} = 0.4 \text{ delay factor}$$

Μελετώντας τους Erlang C πίνακες, παρατηρείται ότι για φορτίο κίνησης 15.47 Erlang και συντελεστή καθυστέρησης (delay factor) 0.4, απαιτούνται 17 κυκλώματα για να εξυπηρετήσουν το φορτίο κίνησης. Κατά τον παραπάνω υπολογισμό θεωρήθηκε ότι στο κύκλωμα δεν υπήρχαν απώλειες πακέτων.

Engset

Το Engset μοντέλο βασίζεται στις παρακάτω υποθέσεις:

- Πεπερασμένος αριθμός πηγών
- Ομαλή καμπύλη άφιξης κλήσεων
- Οι φραγμένες κλήσεις αναδρομολογούνται από το σύστημα
- Εκθετική κατανομή διάρκειας κλήσεων

Γενικά το μοντέλο Engset χρησιμοποιείται σε περιβάλλοντα όπου είναι εύκολο να υποτεθεί πως ένας πεπερασμένος αριθμός πηγών χρησιμοποιεί μια ζευκτική ομάδα. Γνωρίζοντας τον αριθμό των πηγών, μπορεί να διατηρηθεί υψηλός ο βαθμός εξυπηρέτησης. Η χρήση του μοντέλου Engset συναντάται περισσότερο στα δίκτυα κινητών επικοινωνιών GSM

Poisson

Το μοντέλο Poisson βασίζεται στις παρακάτω υποθέσεις:

- Άπειρος αριθμός πηγών
- Τυχαίο διάγραμμα άφιξης κλήσεων
- Συγκράτηση φραγμένων κλήσεων
- Εκθετική κατανομή διάρκειας κλήσεων

Στο μοντέλο Poisson, οι φραγμένες κλήσεις συγκρατούνται έως ότου γίνει διαθέσιμο το κύκλωμα. Το μοντέλο αυτό προϋποθέτει ένα τυχαίο μοτίβο άφιξης κλήσεων, ο καλών κάνει μόνο μια προσπάθεια να πραγματοποιήσει την κλήση και αν αυτή δεν εξυπηρετηθεί τότε χάνεται. Το μοντέλο Poisson συνήθως χρησιμοποιείται για υπερδιαστασιολόγηση (overengineering) αυτοδύναμων ζευκτικών ομάδων.

Ο τύπος που ακολουθεί χρησιμοποιείται για τον υπολογισμό του μοντέλου κίνησης Poisson:

$$P(c,a) = 1 - e^{-a} \sum_{k=0}^{c-1} \frac{a^k}{k!}$$

Όπου:

P(c,a) είναι η πιθανότητα αποκλισμού της κλήσης

e είναι η φυσική βάση log

c είναι ο αριθμός των κυκλωμάτων

α είναι το φορτίο κίνησης

Παράδειγμα χρήσης του μοντέλου κίνησης Poisson: Απαιτείται ο σχεδιασμός μιας νέας ζευκτικής ομάδας που θα εξυπηρετεί μόνο το νέο γραφείο μιας εταιρίας και πρέπει να καθοριστούν πόσες γραμμές είναι απαραίτητες για το σκοπό αυτό. Αναμένεται πως το γραφείο θα πραγματοποιεί και θα δέχεται περίπου 300 κλήσεις την ήμερα με ΑΗΤ τα 4 λεπτά. Ο στόχος είναι P.01 GoS ή 1% ρυθμός φραγής. Κάνοντας συντηρητική προσέγγιση, να υποτεθεί πως το 20% των κλήσεων συμβαίνει κατά την διάρκεια της ώρας αιχμής.

Λύση: Ο υπολογισμός της κίνησης στην ώρα αιχμής γίνεται όπως παρακάτω:

300 κλήσεις * 20% = 60 κλήσεις κατά τη διάρκεια της ώρας αιχμής

$$\frac{\text{60 κλήσεις * 240 ΑΗΤ}}{3600} = \text{4 erlangs κίνησης κατά τη διάρκεια της ώρας αιχμής}$$

Μελετώντας τους πίνακες Poisson παρατηρείται ότι για 4 Erlang κίνησης με ρυθμό φραγής 0.81% (αρκετά κοντά στο 1%), χρειάζονται 10 κυκλώματα για να διαχειριστούν το φορτίο κίνησης. Το αποτέλεσμα αυτό μπορεί να ελεγχθεί με τη βοήθεια του τύπου Poisson ως εξής:

$$P(10,4) = 1 - e^{-4}\sum_{k=0}^{10-1}\frac{4^k}{k!} = 1 - e^{-4}(1 + 4 + \frac{16}{2} + \frac{64}{6} + \frac{256}{24} + \ldots) \approx 0.00813$$

2.2 Ανάλυση Τηλεπικοινωνιακής Κίνησης σε VoIP Δίκτυα

Για την ανάλυση της τηλεπικοινωνιακής κίνησης και τον υπολογισμό του απαιτούμενου εύρους ζώνης των WAN ζεύξεων ενός VoIP δικτύου, μπορεί να χρησιμοποιηθεί η ίδια μεθοδολογία που περιγράφτηκε παραπάνω. Ωστόσο υπάρχουν κάποιες επιπλέον παράμετροι οι οποίες πρέπει να ληφθούν υπόψη κατά τον ακριβή καθορισμό του εύρους ζώνης.

Οι παράμετροι που παρουσιάζονται στη συνέχεια είναι αυτοί που επηρεάζουν το εύρος ζώνης των VoIP δικτύων:

- Κωδικοαποκωδικευτές Φωνής (Voice Codecs)
- Δείγματα (Samples)
- Ανίχνευση Φωνητικής Δραστηριότητας (Voice Activity Detection)
- Συμπίεση Κεφαλίδας RTP (RTP Header Compression)
- Δισημειακή ζεύξη σε σύγκριση με σημείο προς σημεία ζεύξη (Point-to-Point versus Point-to-Multipoint)

2.2.1 Κωδικοαποκωδικευτές Φωνής

Πολλοί είναι οι Codecs φωνής που χρησιμοποιούνται στην IP τηλεφωνεία. Όλοι έχουν διαφορετικούς δυφιορρυθμούς (bit rates) και πολυπλοκότητα. Ορισμένα πρότυπα κωδικοαποκωδικευτών φωνής είναι τα: G.711, G.729, G.726, G.723.1 και G.728. Όλοι οι δρομολογητές Cisco που υποστηρίζουν μετάδοση φωνής υποστηρίζουν ορισμένα ή και όλα τα πρότυπα αυτά.

Οι Codecs επηρεάζουν το εύρος ζώνης διότι καθορίζουν το μέγεθος του ωφέλιμου φορτίου των πακέτων που μεταφέρονται πάνω από IP σε κάθε κλήση. Οι πύλες φωνής (voice gateways), δίνουν τη δυνατότητα διάρθρωσης του μεγέθους ωφέλιμου φορτίου για τον έλεγχο του εύρους ζώνης. Αυξάνοντας το μέγεθος του ωφέλιμου φορτίου, μειώνεται ο συνολικός αριθμός των προς αποστολή πακέτων, μειώνοντας έτσι το απαιτούμενο εύρος ζώνης από τη μείωση του αριθμού των επικεφαλίδων που χρειάζονται για την πραγματοποίηση της κλήσης.

2.2.2 Δείγματα

Ο αριθμός των δειγμάτων ανά πακέτο είναι ένας άλλος παράγοντας που θα καθορίσει το εύρος ζώνης μιας φωνητικής κλήσης. Ο Codec ορίζει το μέγεθος του δείγματος αλλά ο συνολικός αριθμός δειγμάτων που τοποθετούνται σε ένα πακέτο επηρεάζει τον αριθμό των πακέτων που στέλνονται κάθε δευτερόλεπτο. Συνεπώς, ο αριθμός των δειγμάτων που περιλαμβάνονται σε ένα πακέτο επηρεάζει το συνολικό εύρος ζώνης μιας κλήσης. Για παράδειγμα στο πρότυπο G.711 10-ms, το κάθε δείγμα είναι 80 bytes.

Μια κλήση με μόνο ένα δείγμα ανά πακέτο θα αποφέρει τα ακόλουθα:

80 bytes + 20 bytes (IP) + 12 bytes (UDP) + 8 bytes (RTP) = 120 bytes ανά πακέτο

$$120 \text{ bytes per packet} * 100 \text{ pps} = \frac{12000 * 8 \text{ bits}}{1000} = 96 \text{ Kbps ανά κλήση}$$

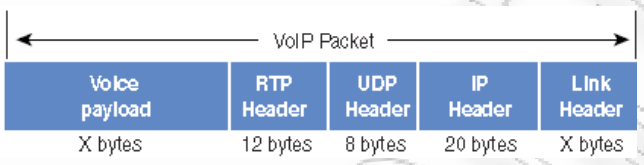
Η ίδια κλήση αλλά με δυο δείγματα ανά πακέτο θα αποφέρει τα εξής:

(80 bytes * 2 samples) + 20 bytes (IP) + 12 bytes (UDP) + 8 bytes (RTP) = 200 bytes ανά πακέτο

$$200 \text{ bytes per packet} * 50 \text{ pps} = \frac{10000 * 8 \text{ bits}}{1000} = 80 \text{ Kbps ανά κλήση}$$

Σημείωση: Στους παραπάνω υπολογισμούς δε συμπεριλήφθηκαν οι επικεφαλίδες του Layer-2.

Εικόνα 2-4: Τυπικό VoIP Πακέτο



[1]

Τα αποτελέσματα δείχνουν ότι υπάρχει μια διαφορά 16 kbps μεταξύ των δυο κλήσεων. Με την αλλαγή του αριθμού δειγμάτων ανά πακέτο, σίγουρα μπορεί να μεταβληθεί το ποσό του εύρους ζώνης που χρησιμοποιεί κάθε κλήση, αλλά υπάρχει ένα αντάλλαγμα. Καθώς μεγαλώνει ο αριθμός δειγμάτων ανά πακέτο, αυξάνεται και η καθυστέρηση κάθε κλήσης. Οι DSP πόροι που χειρίζονται κάθε κλήση πρέπει να αποθηκεύουν τα δείγματα (προσωρινά) για μεγαλύτερο χρονικό διάστημα. Αυτό είναι κάτι που πρέπει να ληφθεί υπόψη κατά τη σχεδίαση ενός δικτύου φωνής.

2.2.3 Ανίχνευση Φωνητικής Δραστηριότητας

Οι τυπικές συνομιλίες φωνής μπορεί να περιέχουν 35% με 50% σιωπή. Στα παραδοσιακά δίκτυα φωνής, όλες οι κλήσεις ομιλίας χρησιμοποιούν σταθερό εύρος ζώνης ίσο με 64 kbps ανεξάρτητα από το πόσο μεγάλο μέρος της συζήτησης είναι ομιλία και πόσο σιωπή. Στα VoIP δίκτυα, όλη η συνομιλία και η σιωπή μετατρέπεται σε πακέτα. Η Ανίχνευση Φωνητικής Δραστηριότητας (Voice Activity Detection, VAD) στέλνει RTP πακέτα μόνο όταν ανιχνεύεται φωνή. Για τον υπολογισμό του VoIP εύρους ζώνης, υποθέτουμε πως η ύπαρξη ανίχνευσης φωνής το μειώνει κατά 35%. Παρά το γεγονός ότι η τιμή αυτή μπορεί να είναι μικρότερη από την πραγματική μείωση, παρέχει μια συντηρητική εκτίμηση που λαμβάνει υπόψη τις διαφορετικές διαλέκτους και τα γλωσσικά πρότυπα. Υπάρχουν Codecs που περιλαμβάνουν μια ενσωματωμένη λειτουργία VAD, αλλά κατά τα άλλα έχουν ίδιες επιδόσεις αντίστοιχα.

2.2.4 Συμπίεση Κεφαλίδας RTP

Όλα τα πακέτα VoIP έχουν δυο συνιστώσες: δείγματα φωνής και IP/UDP/RTP επικεφαλίδες. Αν και τα δείγματα συμπιέζονται από την ψηφιακή επεξεργασία σήματος (DSP) και διαφέρουν σε μέγεθος ανάλογα με τον επιλεγμένο Codec, οι κεφαλίδες είναι πάντα σταθερές 40 bytes. Συγκρίνοντας τα 20 bytes δειγμάτων φωνής σε μια κλήση που χρησιμοποιεί τον προεπιλεγμένο G.729, γίνεται αντιληπτό πως οι κεφαλίδες δημιουργούν σημαντική επιβάρυνση. Με τη χρήση του RTP Header Compresion (cRTP), το οποίο χρησιμοποιείται σε μια ζεύξη-προς-ζεύξη βάση, αυτές οι κεφαλίδες μπορούν να συμπιεστούν σε 2 ή 4 bytes. Αυτή η συμπίεση μπορεί να απελευθερώσει σημαντικό εύρος ζώνης. Για παράδειγμα μια κλήση με χρησιμοποιούμενο codec G.729 χωρίς cRTP καταναλώνει 24 kbps, ενώ με ενεργοποιημένη cRTP μόλις 12 kbps.

Ο επιλεγμένος Codec, ο αριθμός δειγμάτων ανά πακέτο, τα VAD και cRTP είναι αυτά που επηρεάζουν με τον ένα ή τον άλλο τρόπο το εύρος ζώνης μιας κλήσης. Σε κάθε περίπτωση υπάρχει ένας συμβιβασμός μεταξύ ποιότητας φωνής και εύρους ζώνης (bandwidth).

Στον επόμενο πίνακα παρουσιάζεται το απαιτούμενο εύρος ζώνης για διάφορα σενάρια. Η απόδοση λόγω Ανίχνευσης Φωνητικής Δραστηριότητας (VAD) θεωρείται ότι είναι ίση με 50%. Επίσης ο πίνακας παραθέτει τα αποτελέσματα μεγέθους ωφέλιμου φορτίου σχετικά με τις απαιτήσεις εύρους ζώνης των διαφόρων codecs.

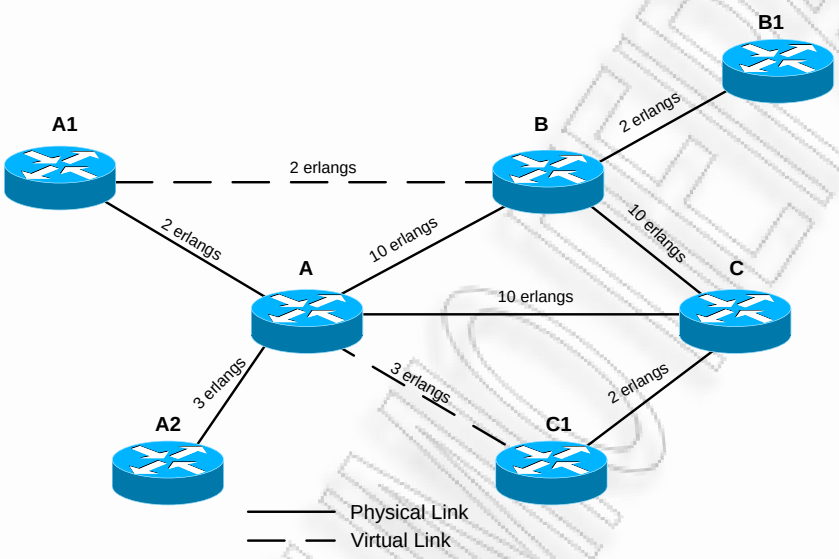
Πίνακας 2-5: Voice Codec Χαρακτηριστικά

Algorithm	Voice BW (kb/s)	Frame Size (bytes)	Cisco Payload (bytes)	Packets per Second	IP/UDP/RTP Header (bytes)	CRTP Header (bytes)	L2	Layer 2 Header (bytes)	Total Bandwidth (kb/s) No VAD	Total Bandwidth (kb/s) With VAD
G.711	64	80	160	50	40	—	Ether	14	85.6	42.8
G.711	64	80	160	50	—	2	Ether	14	70.4	35.2
G.711	64	80	160	50	40	—	PPP	6	82.4	41.2
G.711	64	80	160	50	—	2	PPP	6	67.2	33.6
G.711	64	80	160	50	40	—	FR	4	81.6	40.8
G.711	64	80	160	50	—	2	FR	4	66.4	33.2
G.711	64	80	80	100	40	—	Ether	14	107.2	53.6
G.711	64	80	80	100	—	2	Ether	14	76.8	38.4
G.711	64	80	80	100	40	—	PPP	6	100.8	50.4
G.711	64	80	80	100	—	2	PPP	6	70.4	35.2
G.711	64	80	80	100	40	—	FR	4	99.2	49.6
G.711	64	80	80	100	—	2	FR	4	68.8	34.4
G.729	8	10	20	50	40	—	Ether	14	29.6	14.8
G.729	8	10	20	50	—	2	Ether	14	14.4	7.2
G.729	8	10	20	50	40	—	PPP	6	26.4	13.2
G.729	8	10	20	50	—	2	PPP	6	11.2	5.6
G.729	8	10	20	50	40	—	FR	4	25.6	12.8
G.729	8	10	20	50	—	2	FR	4	10.4	5.2
G.729	8	10	30	33	40	—	Ether	14	22.4	11.2
G.729	8	10	30	33	—	2	Ether	14	12.3	6.1
G.729	8	10	30	33	40	—	PPP	6	20.3	10.1
G.729	8	10	30	33	—	2	PPP	6	10.1	5.1
G.729	8	10	30	33	40	—	FR	4	19.7	9.9
G.729	8	10	30	33	—	2	FR	4	9.6	4.8
G.723.1	6.3	30	30	26	40	—	Ether	14	17.6	8.8
G.723.1	6.3	30	30	26	—	2	Ether	14	9.7	4.8
G.723.1	6.3	30	30	26	40	—	PPP	6	16.0	8.0
G.723.1	6.3	30	30	26	—	2	PPP	6	8.0	4.0
G.723.1	6.3	30	30	26	40	—	FR	4	15.5	7.8
G.723.1	6.3	30	30	26	—	2	FR	4	7.6	3.8
G.723.1	5.3	30	30	22	40	—	Ether	14	14.8	7.4
G.723.1	5.3	30	30	22	—	2	Ether	14	8.1	4.1
G.723.1	5.3	30	30	22	40	—	PPP	6	13.4	6.7
G.723.1	5.3	30	30	22	—	2	PPP	6	6.7	3.4
G.723.1	5.3	30	30	22	40	—	FR	4	13.1	6.5
G.723.1	5.3	30	30	22	—	2	FR	4	6.4	3.2

2.2.5 Point-to-Point έναντι Point-to-Multipoint

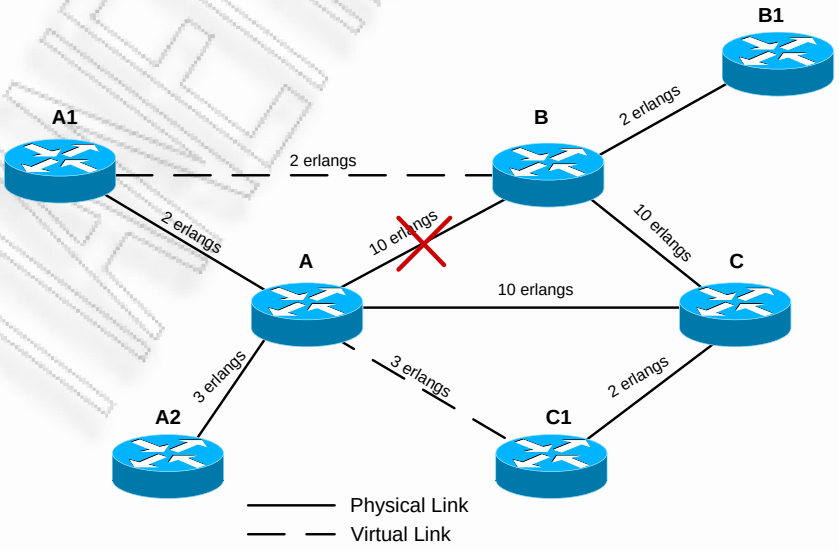
Επειδή τα PSTN κυκλώματα χτίστηκαν ως point-to-point συνδέσεις και τα VoIP δίκτυα βασικά είναι point-to-multipoint, θα πρέπει να εξεταστεί η κατεύθυνση της κίνησης και να ομαδοποιηθεί ανάλογα. Αυτή η ομαδοποίηση αποτελεί έναν από τους σημαντικότερους παράγοντες που ορίζουν το εύρος ζώνης σε εφεδρικές συνδέσεις.

Εικόνα 2-5: Κατάλληλη Λειτουργική Τοπολογία



Οι point-to-point συνδέσεις δε θα χρειαστούν μεγαλύτερο εύρος ζώνης από τον αριθμό των φωνητικών κλήσεων που εισάγονται προς και από τις PSTN συνδέσεις. Αν μια από αυτές τις συνδέσεις χαθεί, θα πρέπει να έχει διασφαλιστεί ότι οι εφεδρικές συνδέσεις θα έχουν την ικανότητα να εξυπηρετήσουν την αυξημένη κίνηση. Στο επόμενο σχήμα, η WAN σύνδεση μεταξύ των κόμβων A και B είναι εκτός λειτουργίας. Συνεπώς θα υπάρχει αυξημένη κυκλοφορία μεταξύ των κόμβων A και C, καθώς και C και B. Αυτή η πρόσθετη κίνηση θα απαιτεί από τις συγκεκριμένες ζεύξεις να είναι σχεδιασμένες έτσι ώστε να μπορούν να χειριστούν το πρόσθετο φορτίο.

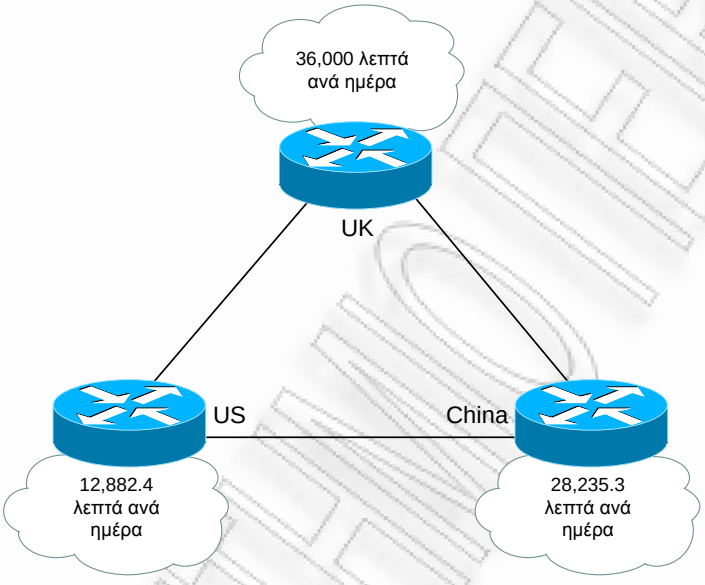
Εικόνα 2-6: Τοπολογία με Ζεύξη Εκτός Λειτουργίας



2.2.6 Από Άκρο σε Άκρο Ανάλυση Κίνησης

Με τη βοήθεια των πινάκων κίνησης, η διαδικασία υπολογισμού των κυκλωμάτων που απαιτούνται για την εξυπηρέτηση της κίνησης γίνεται πολύ απλή. Επιπλέον με τον καθορισμό του αριθμού των κλήσεων από την PSTN πλευρά γίνεται επίσης εύκολος ο υπολογισμός του απαιτούμενου εύρους ζώνης (bandwidth) για το IP σκέλος της κλήσης. Δυστυχώς, το να συσχετιστούν οι παράγοντες αυτοί μαζί τελικά μπορεί να είναι ένα ζήτημα. Στο επόμενο σχήμα παρουσιάζεται η τοπολογία του δικτύου που θα αναλύσουμε την κίνηση.

Εικόνα 2-7: Τοπολογία Παραδείγματος



Μια εταιρία όπως παρουσιάζεται και στο σχήμα, έχει γραφεία στις ΗΠΑ, την Κίνα και το Ηνωμένο Βασίλειο. Επειδή η κύρια έδρα είναι στη Βρετανία, έχουν αγοραστεί μισθωμένες γραμμές από τη Βρετανία προς ΗΠΑ και Κίνα. Το μεγαλύτερο μέρος τις κίνησης πηγαίνει από το Ηνωμένο Βασίλειο προς τις ΗΠΑ ή την Κίνα και ένα μικρότερο μέρος φορτίου κίνησης διέρχεται μεταξύ Κίνας και ΗΠΑ. Το αρχείο καταγραφής κλήσεων δίνει τα ακόλουθα στατιστικά:

- ✓ Ηνωμένο Βασίλειο: 36,000.0 λεπτά ομιλίας ανά ημέρα
- ✓ ΗΠΑ: 12,882.4 λεπτά ομιλίας ανά ημέρα
- ✓ Κίνα: 28,235.3 λεπτά ομιλίας ανά ημέρα

Σε αυτό το δίκτυο, γίνονται οι ακόλουθες υποθέσης:

- Η κίνηση σε κάθε κόμβο έχει τυχαίο διάγραμμα άφιξης
- Εκθετική κατανομή διάρκειας κλήσεων
- Οι φραγμένες κλήσεις αναδρομολογούνται από το σύστημα
- Υπάρχει άπειρος αριθμός πηγών

Οι παραπάνω υποθέσεις παραπέμπουν στη χρήση του Erlang B μοντέλου για την ταξινόμηση των ζευκτικών ομάδων με το PSTN. Το απαιτούμενο GoS για κάθε ζευκτική ομάδα ορίζεται ίσο με P.01.

Ο υπολογισμός του φορτίου κίνησης για τις PSTN ζεύξεις σε κάθε κόμβο γίνεται ως εξής:

$$\text{Ηνωμένο Βασίλειο} = (36{,}000 \text{ λεπτά ανά ημέρα})*17\% = \frac{6{,}120 \text{ λεπτά ανά ημέρα}}{60} = 102 \text{ BHT}$$

$$\text{ΗΠΑ} = (12{,}882.4 \text{ λεπτά ανά ημέρα})*17\% = \frac{2{,}190 \text{ λεπτά ανά ημέρα}}{60} = 36.5 \text{ BHT}$$

$$\text{Κίνα} = (28{,}235.3 \text{ λεπτά ανά ημέρα})*17\% = \frac{4{,}800 \text{ λεπτά ανά ημέρα}}{60} = 80 \text{ BHT}$$

Ουσιαστικά τα παραπάνω αποτελέσματα είναι αυτά που δίνουν τον αριθμό των κυκλωμάτων που απαιτούνται για τις PSTN συνδέσεις σε κάθε κόμβο. Έτσι, έχοντας ένα χρησιμοποιήσιμο αριθμό κίνησης και ανατρέχοντας στους πίνακες, επιλέγεται ο πλησιέστερος αριθμός που ταιριάζει.

Για το Ηνωμένο Βασίλειο τα 102 BHT με P.01 GoS αποδεικνύουν την ανάγκη ενός συνόλου από 120 DS0s για να υποστηρίξουν αυτό το φορτίο.

Από τους πίνακες γίνεται φανερό ότι για να εξυπηρετηθούν 36,108 erlangs φορτίου κίνησης με πιθανότητα αποκλεισμού P.01, απαιτούνται 48 κυκλώματα. Επειδή το BHT που υπολογίστηκε για τις ΗΠΑ είναι 36.5 erlangs, μπορεί να παρατηρηθεί ένα μεγαλύτερο ποσοστό φραγής κλήσεων από P.01. Από τον τύπο Erlang B υπολογίζεται πως το ποσοστό αυτό είναι περίπου ίσο με P.01139.

Αντίστοιχα για την Κίνα έχει υπολογιστεί BHT ίσο με 80 erlangs. Οι Erlang B πίνακες δείχνουν πως υπάρχουν δυο δυνατές επιλογές. Συγκεκριμένα για 80,303 erlangs BHT με P.01 GoS απαιτούνται 96 κυκλώματα. Επειδή τα κυκλώματα ταξινομούνται σε ομάδες των 24 (T1) ή 30 (E1) όταν δουλεύουν με ψηφιακές φέρουσες, πρέπει να γίνει επιλογή μεταξύ 4 T1s ή 4 E1. Η επιλογή τεσσάρων T1 (96 κυκλώματα) είναι υπερβολική για το ποσό της κίνησης που θα εξυπηρετηθεί, αλλά δυστυχώς η επιλογή τριών T1 (72 κυκλώματα) θα αυξήσει το ποσοστό των κλήσεων που δε θα εξυπηρετούνται.

Αφού πλέον είναι γνωστός ο αριθμός των απαιτούμενων PSTN κυκλωμάτων, πρέπει να καθοριστεί σημείο-προς-σημείο το εύρος ζώνης στα κυκλώματα αυτά. Επειδή το ποσό της κίνησης που απαιτείται στο IP σκέλος προσδιορίζεται από το ποσό της κίνησης που υπάρχει στο PSTN σκέλος, μπορεί να συσχετισθούν άμεσα τα DS-0s με το απαιτούμενο εύρος ζώνης.

Το πρώτο βήμα είναι η επιλογή του κατάλληλου codec. Ο G.729 είναι ο πιο δημοφιλής διότι παρέχει υψηλή ποιότητα φωνής για το ποσό της συμπίεσης που παρέχει.

Μια κλήση με G.729 χρησιμοποιεί το ακόλουθο εύρος ζώνης:

- ✓ 26.4 kbps ανά κλήση ολόρρυθμο (full rate) με κεφαλίδες
- ✓ 11.2 kbps ανά κλήση με VAD
- ✓ 9.6 kbps ανά κλήση με cRTP
- ✓ 6.3 kbps ανά κλήση με cRTP και VAD

Συνεπώς, το απαιτούμενο εύρος ζώνης για τη σύνδεση μεταξύ Ηνωμένου Βασιλείου και Κίνας έχει ως εξής:

- Full Rate: 96 DS0s * 26.4 Kbps = 2.534 Mbps
- VAD: 96 DS0s * 11.2 Kbps = 1.075 Mbps
- cRTP: 96 DS0s * 17.2 Kbps = 1.651 Mbps
- VAD & cRTP: 96 DS0s * 7.3 Kbps = 700.8 Kbps

Το απαιτούμενο εύρος ζώνης για τη σύνδεση μεταξύ Ην. Βασιλείου και ΗΠΑ έχει ως εξής:

- Full Rate: 48 DS0s * 26.4 Kbps = 1.267 Mbps

- VAD: 48 DS0s * 11.2 Kbps = 537.6 Kbps
- cRTP: 48 DS0s * 17.2 Kbps = 825.6 Kbps
- VAD & cRTP: 48 DS0s * 7.3 Kbps = 350.4 Kbps

Όπως είναι φανερό οι παράμετροι VAD και cRTP έχουν σημαντική επίπτωση στο απαιτούμενο εύρος ζώνης των WAN ζεύξεων.

2.2.7 Εργαλεία Υπολογισμού Εύρους Ζώνης

Ο υπολογισμός του απαιτούμενου εύρους ζώνης για έναν συγκεκριμένο αριθμό VoIP κλήσεων μπορεί να υπολογιστεί πολύ εύκολα με την βοήθεια εργαλείων. Ένα από αυτά είναι και το ***Voice Codec Bandwidth Calculator*** που είναι διαθέσιμο από τη Cisco και βρίσκεται στη διεύθυνση: http://tools.cisco.com/Support/VBC/do/CodecCalc1.do (απαιτείται εγγραφή).

Για τον υπολογισμό με βάση το εργαλείο αυτό απαιτούνται οι ακόλουθες παράμετροι:

1. ***Codec*** (πχ G711, G729 κτλ)
2. ***Voice Protocol*** (πρωτόκολλο μεταφοράς φωνής, πχ VoATM, VoFR, VoIP)
3. ***Number of Calls*** (μέγιστος αριθμός ταυτόχρονων φωνητικών κλήσεων, πχ 5)
4. ***Voice Payload Size*** (μέγεθος του Voice Payload[4], πχ 80,160, 240)
5. ***Media Access*** (Layer-2 πρωτόκολλο στη διεπαφή διασύνδεσης πχ Ethernet, ATM, Frame-Relay κ.α.)
6. ***Tunnel/Security/Misc*** (επιπρόσθετες επιβαρύνσεις, πχ λόγο χρήσης IPSec, VPN κ.α.)

Έτσι εάν για παράδειγμα επιθυμούμε να υπολογίσουμε το απαιτούμενο εύρος ζώνης για την πραγματοποίηση 5 VoIP συνομιλιών με παραμέτρους αυτές της Εικόνας 2-8, δηλαδή με χρήση του G.711 Codec, Voice Payload ίσο με 160 bytes (δηλαδή το default) και το Ethernet ως Layer-2 πρωτόκολλο στη διεπαφή διασύνδεσης, τότε από τα αποτελέσματα (Εικόνα 2-9) του εργαλείου *Voice Codec Bandwidth Calculator* πληροφορούμαστε πως απαιτούνται 457,8 Kbps μαζί με τις επιβαρύνσεις (συνυπολογίζονται 5% επιπρόσθετες επιβαρύνσεις ανά κλήση λόγω σηματοδοσίας).

Στις Εικόνες 2-8, 2-9 παρουσιάζονται αναλυτικά όλες οι παράμετροι επιλογής καθώς και τα αποτελέσματα για δυο παραδείγματα, ένα με χρήση του Codec G.711 και ένα με χρήση του G.729:

Εικόνα 2-8: Voice Codec Bandwidth Calculator-Παράμετροι Επιλογής

Παράδειγμα 1ο

Your Selections	
Codec:	g711_All_Variants
Voice Payload Size:	160 bytes
Voice Protocol:	VoIP
Compression:	Not Applicable
Media Access:	Ethernet
Tunnel/Security /Misc:	None
Number of Calls:	5

Παράδειγμα 2ο

Your Selections	
Codec:	g729_All_Variants
Voice Payload Size:	20 bytes
Voice Protocol:	VoIP
Compression:	Not Applicable
Media Access:	Ethernet
Tunnel/Security /Misc:	None
Number of Calls:	5

[4] Το φορτίο φωνής (voice payload) αναπαριστά τον αριθμό των bytes από το δείγμα (ή τα δείγματα) φωνής που περιέχει κάθε πακέτο. Κάθε δείγμα φωνής, ανάλογα με το είδος της κωδικοποίησης που χρησιμοποιεί, έχει διαφορετικό μήκος π.χ. στην περίπτωση του G.711 ένα δείγμα φωνής έχει μέγεθος 80 bytes ενώ μπορεί να περιέχονται ένα ή περισσότερα δείγματα φωνής σε ένα πακέτο. Για παράδειγμα φορτίο φωνής 80, 160 ή 240 bytes σημαίνει ένα, δύο ή τρία δείγματα φωνής κωδικοποιημένα κατά G.711.

Εικόνα 2-9: Voice Codec Bandwidth Calculator-Στοιχεία Μετά την Επεξεργασία

Παράδειγμα 1ο

Codec Information		
Codec Bit Rate	64 kbps	= (Codec Sample Size * 8) / (Codec Sample Interval)
Codec Sample Size	80 bytes	size of each individual codec sample
Codec Sample Interval	10 msec	the time it takes for a single sample
Bandwith Per Call (VoIP)		
Voice Packets Per Second	50	(Codec Bit Rate / Voice Payload Size)
Bandwidth Per Call (RTP Only)	87.2 kbps	(Total Packet Size(bits))* (Packets Per Second)
5% Additional Overhead	4.36 kbps	5% additional overhead per call to accomodate bandwidth for signaling (for example: RTCP/H225/H245 messages on H.323 networks).
Bandwith Per Call + 5.0% Additional Overhead	91.56 kbps	Overhead + Bandwidth Per call
Total Bandwith Required (VoIP)		
Bandwidth Used for All Calls (RTP Only)	436 kbps	(Bandwidth per Call) * (Number of Calls)
Total Bandwidth (including Overhead)	457.8 kbps	Same as above + 5.0% Overhead
Packet Size Calculation		
Total Packet Size	218 bytes	Entire Packet Size
Voice Payload Size	160 bytes	Size of the Codec Samples per packet
Layer2 Overhead	18 bytes	Layer2 Overhead including CRC
IP Header Overhead	20 bytes	IP Overhead in bytes
UDP Header Overhead	8 bytes	UDP Overhead in bytes
RTP Header Overhead	12 bytes	RTP Overhead in bytes

What if the Voice Payload Size changed (VoIP)				
Voice Payload Size (Bytes)	Packets per Second	Bandwidth per Call (kbps) including 5% Overhead	Bandwidth Difference from Reference (kbps)	Delay Difference (msec)
80.0	100	115.92	-24.36	-10
160	50	91.56	Reference	Reference
240.0	33.333	83.44	8.12	10

Παράδειγμα 2ο

Codec Information		
Codec Bit Rate	8 kbps	= (Codec Sample Size * 8) / (Codec Sample Interval)
Codec Sample Size	10 bytes	size of each individual codec sample
Codec Sample Interval	10 msec	the time it takes for a single sample
Bandwith Per Call (VoIP)		
Voice Packets Per Second	50	(Codec Bit Rate / Voice Payload Size)
Bandwidth Per Call (RTP Only)	31.2 kbps	(Total Packet Size(bits))* (Packets Per Second)
5% Additional Overhead	1.56 kbps	5% additional overhead per call to accomodate bandwidth for signaling (for example: RTCP/H225/H245 messages on H.323 networks).
Bandwith Per Call + 5.0% Additional Overhead	32.76 kbps	Overhead + Bandwidth Per call
Total Bandwith Required (VoIP)		
Bandwidth Used for All Calls (RTP Only)	156 kbps	(Bandwidth per Call) * (Number of Calls)
Total Bandwidth (including Overhead)	163.8 kbps	Same as above + 5.0% Overhead
Packet Size Calculation		
Total Packet Size	78 bytes	Entire Packet Size
Voice Payload Size	20 bytes	Size of the Codec Samples per packet
Layer2 Overhead	18 bytes	Layer2 Overhead including CRC
IP Header Overhead	20 bytes	IP Overhead in bytes
UDP Header Overhead	8 bytes	UDP Overhead in bytes
RTP Header Overhead	12 bytes	RTP Overhead in bytes

What if the Voice Payload Size changed (VoIP)				
Voice Payload Size (Bytes)	Packets per Second	Bandwidth per Call (kbps) including 5% Overhead	Bandwidth Difference from Reference (kbps)	Delay Difference (msec)
10.0	100	57.12	-24.36	-10
20	50	32.76	Reference	Reference
30.0	33.333	24.64	8.12	10
40.0	25	20.58	12.18	20
50.0	20	18.144	14.616	30
60.0	16.667	16.52	16.24	40
70.0	14.286	15.36	17.4	50
80.0	12.5	14.49	18.27	60
90.0	11.111	13.813	18.947	70
100.0	10	13.272	19.488	80
110.0	9.091	12.829	19.931	90
120.0	8.333	12.46	20.3	100
130.0	7.692	12.148	20.612	110
140.0	7.143	11.88	20.88	120
150.0	6.667	11.648	21.112	130
160.0	6.25	11.445	21.315	140
170.0	5.882	11.266	21.494	150
180.0	5.556	11.107	21.653	160
190.0	5.263	10.964	21.796	170
200.0	5	10.836	21.924	180
210.0	4.762	10.72	22.04	190
220.0	4.545	10.615	22.145	200
230.0	4.348	10.518	22.242	210
240.0	4.167	10.43	22.33	220

Εκτός από την πληροφορία για το απαιτούμενο συνολικό εύρος ζώνης, δίνονται επιπρόσθετες πληροφορίες για τον Codec που έχει επιλεγεί, το εύρος ζώνης για κάθε VoIP κλήση, καθώς και το μέγεθος του VoIP πακέτου και των τμημάτων του. Επιπλέον πληροφορούμαστε πώς επηρεάζεται το εύρος ζώνης σε περίπτωση αλλαγής του Voice Payload. Στο πρώτο παράδειγμά μας αν το Voice Payload επιλεγεί ίσο με 80 bytes, τότε το απαιτούμενο εύρος ζώνης ανά VoIP κλήση, άρα και το συνολικό, αυξάνονται, ενώ στην περίπτωση όπου επιλεγεί ίσο με 240 bytes μειώνονται.

2.2.8 Διεκπεραιωτική Ικανότητα Δρομολογητή και Μέγιστο Φορτίο Κίνησης

Στις προηγούμενες ενότητες αναλύθηκε η διαδικασία υπολογισμού του απαιτούμενου εύρους ζώνης για την πραγματοποίηση συγκεκριμένου αριθμού VoIP κλήσεων. Θεωρώντας πως ο παραπάνω υπολογισμός έχει γίνει και πως το απαιτούμενο εύρος ζώνης είναι εφικτό να εξυπηρετηθεί από την ζεύξη, πώς είμαστε σίγουροι ότι αυτό το μέγιστο φορτίο κίνησης θα εξυπηρετηθεί και από τον εκάστοτε δρομολογητή; Με την αύξηση των ταυτόχρονων κλήσεων αυξάνεται και ο αριθμός των πακέτων φωνής που πρέπει να εξυπηρετηθούν από τους δρομολογητές του δικτύου. Ως εκ τούτου, ένας άλλος παράγοντας που πρέπει να ληφθεί υπόψη τόσο κατά το σχεδιασμό του δικτύου όσο και κατά τον προγραμματισμό δρομολόγησης της κίνησης μέσα σε αυτό, είναι η διεκπεραιωτική ικανότητα του κάθε δρομολογητή.

Παρατηρώντας τα φύλλα δεδομένων (βλ. Παράρτημα Α), εύκολα μπορεί να γίνει κατανοητό πως κάθε δρομολογητής έχει διαφορετική διεκπεραιωτική ικανότητα ανάλογα με τον αριθμό πακέτων που μπορεί να εξυπηρετεί ανά δευτερόλεπτο. Για παράδειγμα αν επιλεγεί ο δρομολογητής Cisco 2610, με ενεργοποίηση[5] της επιλογής γρήγορης προώθησης πακέτων (Cisco Express Forwarding, CEF), μπορεί να εξυπηρετήσει έως 15,000 πακέτα το δευτερόλεπτο (pps). Όμως κάθε VoIP κλήση απαιτεί δυο συνδέσεις και κάθε πακέτο υπολογίζεται δυο φόρες από τον δρομολογητή (μια φορά στη θύρα εισόδου και μια στη θύρα εξόδου), άρα συνολικά το ίδιο πακέτο μετράται 2x2=4 φορές. Συνεπώς, εάν για τη μετάδοση της φωνής χρησιμοποιείται ο G.711 Codec με *Codec Bit Rate* 64 Kbps και *Codec Sample Interval* 10 msec, κάθε VoIP κλήση για να εξυπηρετηθεί θα απαιτεί από τον δρομολογητή να διεκπεραιώσει 50 πακέτα το δευτερόλεπτο:

$$\text{Voice Packets Per Sec} = \frac{\text{Codec Bit Rate}}{\text{Voice Payload Size}} = \frac{64000 \text{ bps}}{160*8 \text{ bits}} = 50$$

Ως εκ τούτου, ο μέγιστος αριθμός κλήσεων που δύναται να εξυπηρετήσει ο συγκεκριμένος δρομολογητής (Cisco 2610), θεωρώντας ότι εξυπηρετεί μόνο πακέτα φωνής, θα είναι:

$$\frac{15000 \text{ pps}}{50 \text{ pps} * 4} = 75 \text{ Calls/Sec}$$

Επομένως ο δρομολογητής αυτός, μπορεί να εξυπηρετήσει ένα σχετικά χαμηλό αριθμό ταυτόχρονων τηλεφωνικών συνδιαλέξεων και κατά συνέπεια θα επιλεγεί για ένα δίκτυο με σχετικά χαμηλό φορτίο κίνησης. Αντίστοιχα υπάρχουν δρομολογητές όπως ο Cisco 12000, όπου είναι ικανός να εξυπηρετεί άριστα μεγάλο αριθμό φορτίου κίνησης σε ένα κεντρικό σημείο του δικτύου.

Όπως ήδη έχει αναφερθεί, είναι σημαντικό κατά την ανάλυση του φορτίου κίνησης, να συνυπολογίζεται και ένα επιπρόσθετο φορτίο που μπορεί να προκύψει για κάποιο χρονικό διάστημα λόγο μιας πιθανής βλάβης, πχ σε μια άλλη ζεύξη του δικτύου. Η μέριμνα αυτή, σε συνδυασμό με την κατάλληλη επιλογή και το σωστό προγραμματισμό των δικτυακών συσκευών, αποτελούν τα βασικά συστατικά για την υλοποίηση ισχυρών και αποτελεσματικών δικτύων φωνής.

[5] Με την εντολή: Router(config)# **ip cef**

Κεφάλαιο 3ο

3. Ποιότητα Υπηρεσίας

3.1 Γενικά

3.1.1 Σύγκλιση Δικτύων και QoS

Παραδοσιακά, τα δίκτυα υπολογιστών χρησιμοποιούνταν μόνο για εφαρμογές δεδομένων και υπηρεσίες αποθήκευσης αρχείων. Ένα σύγχρονο επιχειρησιακό δίκτυο συνεχίζει να αποτελεί τον κορμό των επικοινωνιών αλλά επιπρόσθετα υποστηρίζει υπηρεσίες μετάδοσης φωνής, βίντεο υψηλής ποιότητας και γενικά δυνατότητα συνδιασκέψεων και συνεργασίας μέσω του διαδικτύου.

Η σύγκλιση των δικτύων, όπως ήταν αναμενόμενο επέφερε επιπρόσθετες ανάγκες σε εύρος ζώνης και γενικά σε πόρους. Όμως τα δίκτυα διαθέτουν πεπερασμένο σύνολο πόρων όσων αφορά το εύρος ζώνης, το πλήθος των πακέτων που μπορούν να εξυπηρετήσουν, καθώς και τη ταχύτητα εξυπηρέτησης. Για το λόγο αυτό κρίνεται αναγκαία η ύπαρξη μηχανισμών υπεύθυνων για τη διαχείριση των πόρων και την εξασφάλιση υψηλού επιπέδου υπηρεσιών προκειμένου να επιτρέπεται η συνύπαρξη πολλών εφαρμογών.

Όμως, κάθε εφαρμογή έχει διαφορετικές απαιτήσεις και ως εκ τούτου πρέπει να αντιμετωπίζεται με διαφορετικό τρόπο. Για παράδειγμα, υπάρχουν εφαρμογές πραγματικού χρόνου (VoIP, βίντεο μέσω IP), που κρίνονται πολύ ευαίσθητες στις καθυστερήσεις μετάδοσης και εφαρμογές, όπως η μετάδοση ενός email, όπου δεν παρουσιάζουν τόση μεγάλη ευαισθησία. Έτσι όταν το δίκτυο δεν μπορεί να αναγνωρίσει τον τύπο της εφαρμογής και κατά συνέπεια τις απαιτήσεις της, θα αντιμετωπίζει όλες τις εφαρμογές με ίδιο και όχι με διαφοροποιημένο τρόπο. Αυτό ενδέχεται να προκαλέσει κακή ποιότητα στη μετάδοση φωνής και γενικά μη αποδεκτές υπηρεσίες.

Συνεπώς το δίκτυο πρέπει να έχει την «ευφυΐα» να μπορεί να προσδιορίζει τις ανάγκες κάθε εφαρμογής, ώστε να παρέχει αντίστοιχα τις κατάλληλες διαφοροποιημένες υπηρεσίες. Η **Ποιότητα Υπηρεσίας** (Quality of Service, QoS) είναι ένα σύνολο δυνατοτήτων που έχουν σχεδιαστεί με σκοπό την εξασφάλιση της αξιόπιστης και έγκαιρης παράδοσης των «ευαίσθητων» στην καθυστέρηση πακέτων «πραγματικού χρόνου» μέσω ενός IP δικτύου. Σε αντίθεση με τα αρχεία δεδομένων, τα οποία μπορούν να κατακερματίζονται, εν συνεχεία να στέλνονται με τυχαία σειρά και τέλος να ανασυνθέτονται στο άκρο προορισμού, τα πακέτα φωνής πρέπει να παραδίδονται με ελάχιστες καθυστερήσεις και στη σωστή σειρά. Το QoS λοιπόν αναφέρεται στην απόδοση του δικτύου, η οποία όμως εκφράζεται από την ποιότητα του ήχου μιας τηλεφωνικής κλήσης ή την διαθεσιμότητα σημαντικών δεδομένων. Επιτρέπει σε διαφορετικούς τύπους εφαρμογών να ανταγωνίζονται για τους πόρους του δικτύου και ανάλογα με τον τύπο να παρέχονται διαφοροποιημένες υπηρεσίες οι οποίες θα δίνουν προτεραιότητα στις κρίσιμες εφαρμογές.

Το σύνολο δυνατοτήτων του QoS περιλαμβάνει, μηχανισμούς διαχείρισης του παρεχόμενου από το δίκτυο εύρους ζώνης, τον καθορισμό προτεραιότητας πακέτων, καθώς και αλγορίθμους προγραμματισμού εκπομπής πακέτων. Επιπλέον παρέχει προστασία στο δίκτυο μετριάζοντας την επίδραση DoS επιθέσεων που προκαλούν τα λογισμικά σκουληκιών. Τέλος είναι σημαντικό να διευκρινιστεί, πως το QoS δε δύναται να δώσει λύσεις σε όλα τα προβλήματα. Για παράδειγμα, δεν είναι σχεδιασμένο να αντιμετωπίζει ένα λάθος υλοποιημένο δίκτυο με ελάχιστους πόρους ή την αδυναμία μιας εφαρμογής να υποστηρίζει QoS τεχνικές.

3.1.2 Ενοποιημένες Επικοινωνίες και QoS

Όπως ήδη έχει αναφερθεί, κάθε εφαρμογή έχει διαφορετικές απαιτήσεις. Ως εκ τούτου, σε ένα ενοποιημένο περιβάλλον επικοινωνίας για να είναι λειτουργικά αποδεκτές οι εφαρμογές και ειδικά οι «πραγματικού χρόνου», πρέπει σε συγκεκριμένους παράγοντες που διαμορφώνουν και επηρεάζουν το τελικό αποτέλεσμα να καθοριστούν αυστηρά όρια.

Οι αλληλοεξαρτώμενοι παράγοντες, οι οποίοι επηρεάζουν την ποιότητα μιας εφαρμογής «πραγματικού χρόνου» και κατά συνέπεια και την αποτελεσματικότητα ενός ενοποιημένου δικτύου, αναφέρονται στη συνέχεια:

- Η **απώλεια** (loss) πακέτων, εκφράζει το ποσοστό των πακέτων που απορρίπτονται και δεν εξυπηρετούνται. Συνήθως είναι ανάλογη της διαθεσιμότητας του δικτύου. Έτσι σε ένα δίκτυο υψηλής διαθεσιμότητας το ποσοστό αυτό πρέπει να είναι μικρότερο του 1%, ενώ υπάρχουν εφαρμογές ενοποιημένων επικοινωνιών όπως η τηλεπαρουσία, όπου απαιτούν σχεδόν μηδενική απώλεια.
- Η **καθυστέρηση** (Latency), εκφράζει το χρόνο που χρειάζεται ένα πακέτο για να μεταφερθεί από την πηγή στον προορισμό. Στην περίπτωση της φωνής, η καθυστέρηση εκφράζει το χρόνο που χρειάζεται για να ταξιδέψει από το στόμα του ομιλητή έως το αυτί του ακροατή. Η καθυστέρηση δημιουργείται από μόνιμους (πχ συριακή διάταξη, κρυπτογράφηση) αλλά και από μεταβλητούς (συμφόρηση δικτύου) παράγοντες. Σύμφωνα με την ITU η τιμή καθυστέρησης μιας κατεύθυνσης (one-way) δε πρέπει να ξεπερνά τα 150 msec.
- Η **μεταβλητότητα καθυστέρησης** (jitter). Υποθέτουμε πως ο χρόνος καθυστέρησης ενός πακέτου για τη μεταφορά του από την πηγή στον προορισμό είναι 100 msec, ενώ αντίστοιχα ο χρόνος καθυστέρησης του επόμενου (διαδοχικού) πακέτου είναι 120 msec, η διαφορά αυτή στην καθυστέρηση (120-100=20 msec) ορίζεται ως jitter. Για την εξομάλυνση των χρόνων άφιξης των πακέτων, χρησιμοποιείται ένας προσωρινός ενδιάμεσος καταχωρητής (jitter buffer) με συγκεκριμένα όρια. Σύμφωνα με την ITU η μεταβλητότητα καθυστέρησης δε θα πρέπει να ξεπερνάει τα 20 msec.

Για την αξιολόγηση της ποιότητας σε εφαρμογές πραγματικού χρόνου, έχει καθιερωθεί το πρότυπο MOS (Mean Opinion Score, Μέσο Αποτέλεσμα Κοινής Γνώμης), βάσει του οποίου η βαθμολόγηση της ποιότητας καθορίζεται ως εξής:

Πίνακας 3-1: Mean Opinion Score-MOS

MOS	Ποιότητα	Περιγραφή Κατάστασης
1	Κακή	Πολύ ενοχλητική
2	Ανεπαρκής	Κάπως ενοχλητική
3	Μέτρια	Ελαφρώς ενοχλητική
4	Υψηλή	Αντιληπτά προβλήματα αλλά όχι ενοχλητική
5	Εξαιρετική	Δεν υπάρχουν αντιληπτά προβλήματα

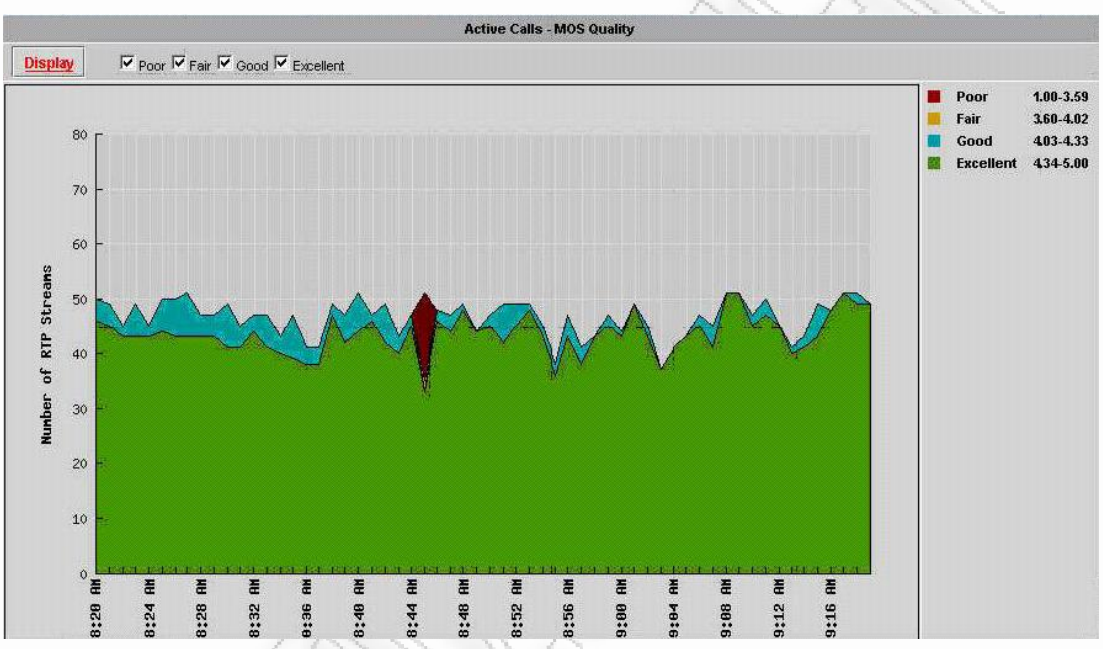
Όσο η βαθμολογία πλησιάζει το 5, τόσο καλύτερη είναι η ποιότητα. Συνήθως ο στόχος κατά το σχεδιασμό ενός δικτύου είναι η επίτευξη μιας MOS τιμής από 4,2 έως 4,7. Το «Εξαιρετικό» 5 αποφεύγεται, διότι για την επιτευξή του απαιτείται μεγάλη επεξεργαστική ισχύ (CPU) και υψηλό εύρος ζώνης που κοστίζουν. Έτσι και αλλιώς έχει διαπιστωθεί πως οι περισσότεροι χρήστες δε θα αντιληφθούν καμία διαφορά στην ποιότητα αν το MOS από 4,7 γίνει 5.

Σε ένα σύγχρονο επιχειρησιακό δίκτυο χρησιμοποιούνται εργαλεία με στόχο τη συνεχή παρακολούθηση και διόρθωση της ποιότητας φωνής. Τα εργαλεία αυτά λαμβάνουν υπόψη τους όλους τους παράγοντες που επηρεάζουν την ποιότητα και υπολογίζουν σε πραγματικό χρόνο (ακόμα και κατά τη διάρκεια της κλήσης) τον δείκτη MOS. Ένα τέτοιο εργαλείο είναι το NAM

(Network Analysis Module) της Cisco, το οποίο προκειμένου να αξιολογήσει την ποιότητα επικοινωνίας εντοπίζει και παρακολουθεί τα RTP ρεύματα. Αρχικά εξετάζει την κεφαλίδα του πακέτου και προσδιορίζει αν πρόκειται για RTP. Αν ναι, ελέγχει αν το πακέτο ανήκει σε μια νέα ή υπάρχουσα RTP ροη. Εν συνεχεία και αφού το πακέτο έχει συνδεθεί με μια ροή, αποστέλλεται στη διαδικασία MOS για ανάλυση της ποιότητας. Η διαδικασία MOS εκτελεί υπολογισμούς και σε πραγματικό χρόνο υπολογίζει τους παράγοντες: jitter, απώλεια και καθυστέρηση. Βάση αυτών των αποτελεσμάτων και της ITU-T σύστασης G.107 υπολογίζεται η τιμή MOS ανά λεπτό της ημέρας. Συνεπώς δίνεται στους διαχειριστές του δικτύου συνεχής ενημέρωση για την παρεχόμενη ποιότητα και ως εκ τούτου η δυνατότητα για άμεση παρέμβαση και επίλυση πιθανών προβλημάτων.

Στην Εικόνα 3-1 παρουσιάζεται ο αριθμός των ενεργών κλήσεων και ο δείκτης MOS στη διάρκεια του χρόνου.

Εικόνα 3-1: Ενεργές Κλήσεις – MOS Ποιότητα



[13]

3.1.3 Ο Βασικός Άξονας για Εφαρμογή QoS

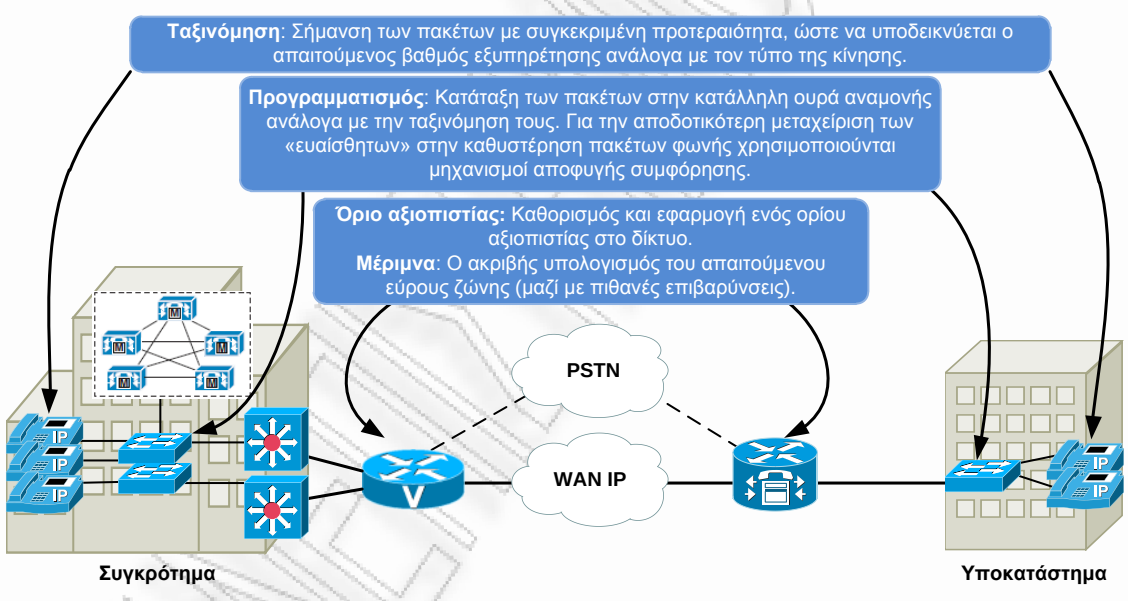
Στην προηγούμενη ενότητα αναφέρθησαν οι παράγοντες εκείνοι που επιδρούν αρνητικά στο τελικό παρεχόμενο επίπεδο υπηρεσιών ενός ενοποιημένου δικτύου. Η ελαχιστοποίηση, αν όχι και η εξάλειψη αυτών των αρνητικών παραγόντων επιτυγχάνεται με το QoS. Όμως για να εφαρμοστεί σωστά το QoS απαιτούνται τρία βασικά βήματα:

- Η **μέριμνα** (provisioning), είναι η διαδικασία μέσω της οποίας διασφαλίζεται η διαθεσιμότητα του απαιτούμενου εύρους ζώνης για κάθε τύπο κίνησης. Κατά τον υπολογισμό του απαιτούμενου εύρους ζώνης κρίνεται σκόπιμο να λαμβάνονται υπόψη όχι μόνο οι παρούσες ανάγκες αλλά και πιθανές μελλοντικές. Μια πιθανή κατανομή του εύρους ζώνης απεικονίζεται στην Εικόνα 3-2, χωρίς βέβαια να σημαίνει ότι αυτά τα ποσοστά θα είναι ο κανόνας εφαρμογής σε όλα τα δίκτυα.
- Η **ταξινόμηση** (classification), είναι η διαδικασία σήμανσης των πακέτων που εκφράζει το επίπεδο εξυπηρέτησης που απαιτούν από το δίκτυο. Η ταξινόμηση μπορεί να γίνει σε διάφορα σημεία του δικτύου από συσκευές Layer-2 ή Layer-3 καθώς και στις τελικές συσκευές (IP τηλέφωνα) αν το υποστηρίζουν. Ως εκ τούτου, σε ένα ενοποιημένο περιβάλλον τα πακέτα φωνής θα χαρακτηρίζονται ως κρίσιμα και θα σηματοδοτούνται για προνομιακή μεταχείριση και άμεση εξυπηρέτηση.

Εικόνα 3-2: Ενδεικτική Κατανομή του Εύρους Ζώνης Βάσει του Τύπου Κίνησης

- Ο **προγραμματισμός** (scheduling), αφορά τη διαδικασία ένταξης των πακέτων σε μια από τις ουρές αναμονής. Έχει σκοπό την αποδοτικότερη μεταχείριση των «ευαίσθητων» πακέτων φωνής και στηρίζεται στη σήμανση που ήδη έχουν αποκτήσει τα πακέτα κατά τη διαδικασία ταξινόμησης.

Εικόνα 3-3: Εφαρμογή QoS - Βασικός Άξονας



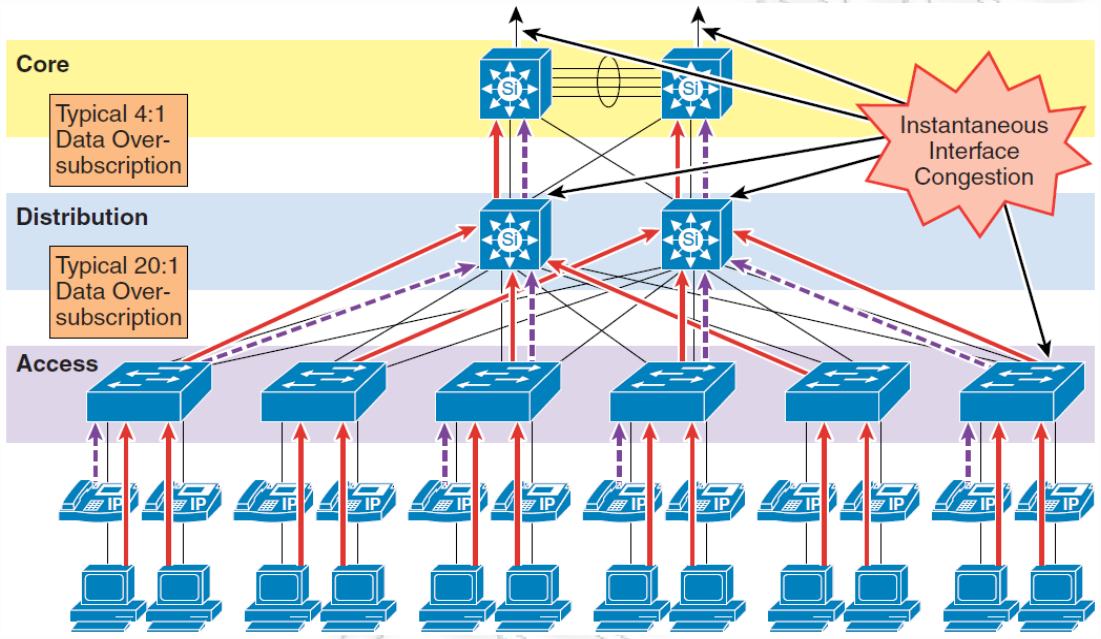
Εκτός από τα παραπάνω βήματα εξασφάλισης του QoS, υπάρχουν μηχανισμοί οι οποίοι σχετίζονται με τη χωρητικότητα της ζεύξης και εφαρμόζονται σε περιπτώσεις όπου το εύρος ζώνης είναι μικρότερο ή ίσο με 768 Kbps. Τέτοιοι μηχανισμοί είναι: Ο μηχανισμός *Διαμόρφωσης Κυκλοφορίας* (Traffic Shaping), ο μηχανισμός *Κατακερματισμού και Παρεμβολής Συνδέσμου* (Link Fragmentation and Interleaving, LFI) και ο μηχανισμός *Συμπίεσης Κεφαλίδας* (Compressed Real-Time Transport Protocol, cRTP).

Στη συνέχεια του κεφαλαίου θα γίνει αναλυτική παρουσίαση όλων των απαραίτητων QoS μηχανισμών που απαιτείται να εφαρμόζονται σε ένα Τοπικό (LAN) ή Ευρείας Περιοχής (WAN) Δίκτυο, καθώς και ο τρόπος υλοποίησής τους.

3.2 Ποιότητα Υπηρεσίας σε Τοπικό Δίκτυο

Μέχρι πρόσφατα, η ποιότητα υπηρεσίας δεν ήταν πρόβλημα σε ένα επιχειρησιακό δίκτυο λόγω της ασύγχρονης φύσης των δεδομένων κίνησης και της ικανότητας των δικτυακών συσκευών να ανέχονται την υπερχείλιση του ενδιάμεσου καταχωρητή (buffer) και την απώλεια πακέτων. Ωστόσο, ο ερχομός νέων εφαρμογών φωνής και βίντεο με ευαισθησία στην απώλεια πακέτων και στις καθυστερήσεις, έθεσε τους καταχωρητές και το εύρος ζώνης να είναι το βασικό θέμα για την παροχή ποιότητας υπηρεσίας.

Εικόνα 3-4: Υπερπροσφορά Κίνησης Δεδομένων σε LAN



[1]

Αυτή η υπερπροσφορά σε συνδυασμό με τον επιμέρους όγκο κυκλοφορίας από τις συσωρευτικές επιπτώσεις των πολλαπλών ανεξάρτητων πηγών, μπορεί να οδηγήσει σε ακαριαίες συγκρούσεις στη διεπαφή εξόδου προκαλώντας έτσι πρόσθετες απορρίψεις πακέτων κατά την προσπάθειά τους να εισέλθουν στην προσωρινή μνήμη (buffer) εξόδου.

Εφαρμογές όπως η κοινή χρήση αρχείων (τόσο peer-to-peer όσο και server-based), απομακρυσμένη δικτυακή αποθήκευση (remote network storage), δημιουργία αντιγράφων ασφαλείας μέσω δικτύου και emails με μεγάλα συνημμένα αρχεία μπορούν να δημιουργήσουν συνθήκες συμφόρησης στο δίκτυο για μεγάλη διάρκεια. Μερικές από τις αρνητικές συνέπειες των επιθέσεων από ιούς είναι η δημιουργία τεράστιου όγκου κίνησης για το δίκτυο με αποτέλεσμα την αύξηση της συμφόρησης. Συνεπώς η μη ύπαρξη πολιτικής διαχείρισης της προσωρινής μνήμης θα έχει σαν αποτέλεσμα την απώλεια, την καθυστέρηση και το jitter.

Επιπλέον, αρνητική επίδραση μπορεί να προκαλέσει μια πιθανή αλλαγή της τοπολογίας του δικτύου. Για παράδειγμα εάν ένας μεταγωγέας αποτύχει, θα έχει σαν αποτέλεσμα όλες οι ροές να αναδρομολογηθούν μέσα από τους εναπομείναντες μεταγωγείς. Πριν από την αποτυχία ο μηχανισμός εξισορρόπησης φορτίου μοίραζε το φορτίο μεταξύ των μεταγωγέων, αλλά μετά το πρόβλημα όλες οι ροές συγκεντρώνονται σε λιγότερους μεταγωγείς, ενδεχομένως προκαλώντας στην έξοδο επιβάρυνση που υπό κανονικές συνθήκες δε θα εμφανιζόταν.

Για εφαρμογές όπως η φωνή, αυτή η απώλεια πακέτων καθώς και η καθυστέρηση για τους λόγους που αναφέρθηκαν, δημιουργούν σοβαρή υποβάθμιση της ποιότητας. Ως εκ τούτου τα QoS εργαλεία κρίνονται απαραίτητα για τη διαχείριση του φορτίου, την ελαχιστοποίηση: των χαμένων πακέτων, της καθυστέρησης και του Jitter.

Οι επόμενοι μηχανισμοί QoS απαιτούνται από άκρο σε άκρο στο δίκτυο για τη διαχείριση της κίνησης και την εξασφάλιση της ποιότητας φωνής:

1. **Ταξινόμηση Κίνησης (Traffic Classification)**

Αφορά τη σήμανση των πακέτων με συγκεκριμένη προτεραιότητα που υποδηλώνει την απαίτηση για την κατηγορία της υπηρεσίας (Class of Service-CoS) από το δίκτυο. Το σημείο στο οποίο γίνεται ο έλεγχος αν ένα πακέτο είναι μαρκαρισμένο σαν αξιόπιστο ή όχι, θεωρείται το όριο εμπιστοσύνης. Η εμπιστοσύνη συνήθως επεκτείνεται σε συσκευές φωνής (τηλέφωνα), σε αντίθεση με τις συσκευές δεδομένων που δεν επεκτείνεται (ηλεκτρονικοί υπολογιστές).

2. **Ουρά αναμονής - Προγραμματισμός**

Περιλαμβάνει την ανάθεση των πακέτων σε μια από τις πολλές ουρές αναμονής με βάση την κατηγοριοποίηση (ταξινόμηση) που έγινε προηγουμένως για την ταχεία επεξεργασία σε όλο το δίκτυο.

3. **Παροχή Εύρους Ζώνης (Bandwidth provisioning)**

Περιλαμβάνει πληροφορίες για το σωστό υπολογισμό του απαιτούμενου εύρους ζώνης για όλες τις εφαρμογές συν στοιχεία επιβάρυνσης.

Στη συνέχεια γίνεται αναλυτική αναφορά αυτών των μηχανισμών QoS σε ένα επιχειρησιακό συγκρότημα.

3.2.1 Ταξινόμηση Κίνησης

Είναι πάντα ένα αναπόσπαστο κομμάτι της αρχιτεκτονικής σχεδιασμού δικτύων, που έχει σαν στόχο να ταξινομεί-χαρακτηρίζει την κίνηση όσο το δυνατόν πιο κοντά στην άκρη του δικτύου. Η ταξινόμηση της κίνησης είναι ένα κριτήριο εισόδου για την πρόσβαση στις διάφορες ουρές αναμονής που χρησιμοποιούνται στις διεπαφές. Το IP τηλέφωνο ταξινομεί την κίνηση σηματοδοσίας ελέγχου και τα RTP ρεύματα φωνής στην πηγή, με βάση τις τιμές που παρουσιάζονται στον παρακάτω πίνακα. Υπό αυτήν τη μορφή, το IP τηλέφωνο μπορεί και πρέπει να ταξινομήσει την κίνηση. Ο πίνακας που ακολουθεί απαριθμεί τις απαιτήσεις ταξινόμησης της κίνησης σε μια υποδομή ενός LAN.

Πίνακας 3-2: Οδηγός Ταξινόμησης Κίνησης για Διάφορους Τύπους Δικτυακής Κίνησης

	Layer-3 Ταξινόμηση			**Layer-2 Ταξινόμηση**
Εφαρμογή	**IP Precedence (IPP)**	**Per-Hop Behavior (PHB)**	**Differentiated Services Code Point (DSCP)**	**Class of Service (CoS)**
Routing	6	CS6	48	6
Voice Real-Time Transport Protocol (RTP)	5	EF	46	5
Videoconferencing	4	AF41	34	4
Streaming video	4	CS4	32	4
Call signalling	3	CS3 AF31 (παλαιότερα)	24 26 (παλαιότερα)	3
Transactional data	2	AF21	18	2
Network management	2	CS2	16	2
Scavenger	1	CS1	8	1
Best effort	0	0	0	0

Ταξινόμηση Κίνησης για Βιντεοτηλεφωνία

Οι βασικές κατηγορίες για την IP Βίντεο-Τηλεφωνία είναι οι ακόλουθες:

- Η φωνή ταξινομείται με CoS 5 (IPP 5, PHB EF, ή DSCP 46).
- Η βίντεο διάσκεψη ταξινομείται με CoS 4 (IPP 4, PHB AF41, ή DSCP 34).

Η σηματοδοσία κλήσης για φωνή και βίντεο-διάσκεψη σήμερα ταξινομείται με CoS 3 (IPP 3, PHB CS3, ή DSCP 24) σε αντίθεση με παλαιότερα όπου οι τιμές ταξινόμησης ήταν οι PHB AF31 ή DSCP 26. Η Cisco συστήνει ιδιαίτερα αυτές τις ταξινομήσεις ως καλύτερες πρακτικές σε ένα Cisco ενοποιημένο δίκτυο επικοινωνιών.

Το τμήμα φωνής μιας κλήσης μπορεί να ταξινομηθεί με τον έναν από τους δύο τρόπους, ανάλογα με τον υπό εξέλιξη τύπο κλήσης. Ένα τηλεφώνημα φωνής θα ταξινομούσε τα μέσα ως CoS 5 (IPP 5 ή PHB EF), ενώ το ακουστικό κανάλι μιας βίντεο-διάσκεψης θα ταξινομούσε τα μέσα ως CoS 4 (IPP 4 ή PHB AF41). Όλα τα τηλεοπτικά προϊόντα τηλεφωνίας της Cisco εμμένουν στα εταιρικά πρότυπα βασικών QoS γραμμών, όπου απαιτούν τα ακουστικά και τηλεοπτικά κανάλια μιας κλήσης με εικόνα και ήχο να χαρακτηρίζονται με CoS 4 (IPP 4 ή PHB AF41).

Λαμβάνοντας υπόψη τις συνιστώμενες κατηγορίες ταξινόμησης, το πρώτο βήμα είναι να αποφασιστεί που θα ταξινομηθούν τα πακέτα (δηλαδή που η συσκευή θα χαρακτηρίσει πρώτα την κίνηση με την QoS ταξινόμηση της). Ουσιαστικά υπάρχουν δυο σημεία στα οποία μπορεί να γίνει η ταξινόμηση της κίνησης: Στα ακροσημεία, δηλαδή στις συσκευές (τηλέφωνα, βίντεο-τηλέφωνα) ή όταν αυτά δεν είναι ικανά ή αξιόπιστα στους δρομολογητές και μεταγωγείς του δικτύου.

Προτού συνεχίσουμε με τους υπόλοιπους QoS μηχανισμούς, οι οποίοι πρέπει να εφαρμόζονται σε ένα επιχειρησιακό δίκτυο LAN, κρίνεται σκόπιμο να διευκρινίσουμε σε τι αναφέρεται κάθε τάξη κίνησης που συναντήσαμε στον προηγούμενο πίνακα. Επιπλέον θα γίνει αναφορά στον τρόπο με τον οποίο αποτρέπονται DoS κακόβουλες επιθέσεις μέσω της τάξης Scavenger.

Interactive-Video: Η Τάξη αυτή αναφέρεται σε IP Video-Conferencing κίνηση.

Streaming Video: Η Τάξη αυτή αναφέρεται στην κίνηση που γεννά κάθε unicast ή multicast μονοκατευθυντική μετάδοση video.

Voice: Η Τάξη αυτή αναφέρεται μόνο στην κίνηση φωνής και δεν περιλαμβάνει την κίνηση σηματοδοσίας (Call-Signaling).

Transactional Data: Η Τάξη αυτή αναφέρεται σε κίνηση που δημιουργείται από διαδραστικές εφαρμογές χρήστη (user-interactive), όπως database access, transaction services, interactive messaging, και προτιμώμενες υπηρεσίες δεδομένων.

Mission-Critical: Η Τάξη αυτή προορίζεται ως ένα υποσύνολο των εφαρμογών της Transactional Data τάξης, με σκοπό τη βελτιστοποίηση των επιχειρησιακών στόχων.

Bulk Data: Η Τάξη αυτή αναφέρεται στην κίνηση μη-διαδραστικών εφαρμογών που «τρέχουν» στο παρασκήνιο, όπως: λειτουργία backup, μεταφορά μεγάλων αρχείων, συγχρονισμός βάσεων.

IP Routing: Η Τάξη αυτή προορίζεται για την κίνηση που δημιουργείται από τα IP πρωτόκολλα δρομολόγησης όπως το BGP το OSPF και άλλα.

Call-Signaling: Η Τάξη αυτή προορίζεται για την κίνηση σηματοδοσίας Φωνής και/ή Βίντεο, όπως Skinny, SIP και H.323 κτλ.

Network Management: Η Τάξη αυτή, προορίζεται για την κίνηση που δημιουργείται από τα πρωτόκολλα ελέγχου, όπως SNMP, Syslog, DNS κτλ.

Best Effort: Η Τάξη αυτή καλείται επίσης και default.

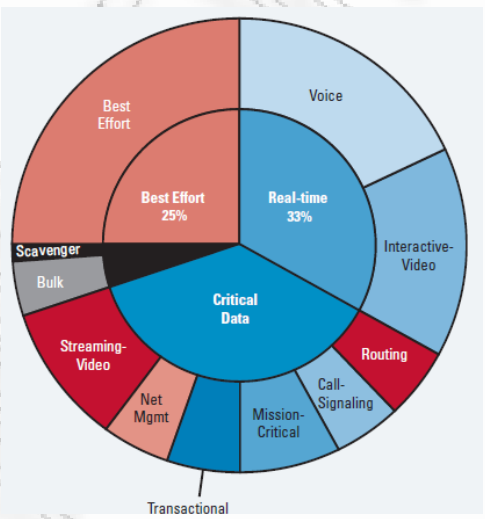
Στρατηγική QoS για Μείωση Κακόβουλων Επιθέσεων Μέσω της Τάξης Κίνησης Scavenger

Οι επιθέσεις DoS μέσω λογισμικών σκουληκιών (worm) αυξάνονται εκθετικά σε συχνότητα, πολυπλοκότητα και επικινδυνότητα. Τα εργαλεία QoS και ο σωστός στρατηγικός σχεδιασμός μπορούν να μετριάσουν την επίδρασή τους και να κρατήσουν τις κρίσιμες εφαρμογές διαθέσιμες κατά τη διάρκεια των DoS επιθέσεων.

Μια τέτοια στρατηγική, ονομαζόμενη ως Ποιότητα Υπηρεσίας μέσω της Τάξης Scavenger[6], χρησιμοποιεί μια τακτική προσέγγιση δυο βημάτων για να παρέχει πρώτου και δεύτερου επιπέδου ανίχνευση ανωμαλίας και αντίδραση στην παραγόμενη DoS/worm κίνηση.

Εικόνα 3-5: Ταξινόμηση Κίνησης

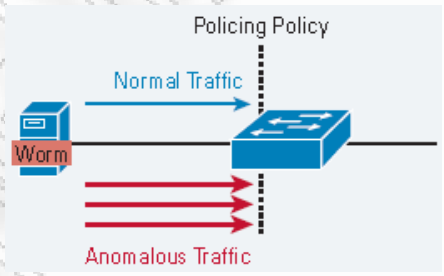
Application	L3 Classification PHB	DSCP
Routing	CS6	48
Voice	EF	46
Interactive-Video	AF41	34
Streaming Video	CS4	32
Mission-Critical	AF31	26
Call-Signaling	CS3	24
Transactional Data	AF21	18
Network Mgmt	CS2	16
Bulk Data	AF11	10
Scavenger	CS1	8
Best Effort	0	0



[44]

Το πρώτο βήμα της στρατηγικής Scavenger είναι ο καθορισμός του προφίλ εφαρμογών, ώστε να μπορεί να γίνει ξεκάθαρο ποια κίνηση είναι κανονική και ποια «ανώμαλη» (σε ένα διάστημα εμπιστοσύνης 95%).

Εικόνα 3-6: Καθορισμός κανονικής και ανώμαλης κίνησης

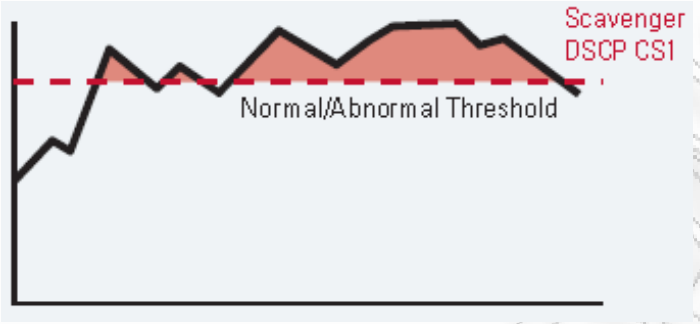


[44]

Η κίνηση που υπερβαίνει αυτό το κανονικό ρυθμό θα είναι υπαγόμενη στη πρώτου επιπέδου ανίχνευση ανωμαλίας. Συγκεκριμένα: η κίνηση που υπερβαίνει θα χαρακτηριστεί ως Scavenger (DSCP=8, CS1). Εδώ πρέπει να σημειώσουμε ότι η ανώμαλη κίνηση δεν απορρίπτεται ούτε τιμωρείται, απλά χαρακτηρίζεται ξανά.

[6] Βασίζεται στο Internet 2. Το Internet 2 είναι το πιο προηγμένο δίκτυο Internet των ΗΠΑ και του κόσμου. Υλοποιείται από μια κοινοπραξία περισσότερων από 170 πανεπιστημίων τα οποία σε στενή συνεργασία με τη βιομηχανία και την κυβέρνηση δημιουργούν το «Διαδίκτυο του μέλλοντος».

Εικόνα 3-7: Μόνο η Κίνηση που Υπερβαίνει το Κανονικό/Ανώμαλο Κατώφλι Επαναχαρακτηρίζεται ως Scavenger.

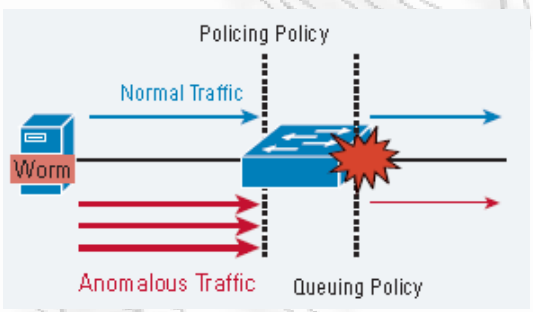


[44]

Οι πολιτικές αστυνόμευσης που εφαρμόζονται στα σημεία πρόσβασης ενός επιχειρησιακού δικτύου συνδέονται με τις πολιτικές αναμονής που εξυπηρετούν την Scavenger τάξη κίνησης. Οι πολιτικές αναμονής συμπλέκονται μόνο όταν οι ενεργές ζεύξεις είναι κορεσμένες. Επομένως, μόνο αν κορεστούν οι ενεργές ζεύξεις θα αρχίσει η απόρριψη πακέτων κίνησης.

Η ανώμαλη κίνηση που προηγουμένως χαρακτηρίστηκε ως Scavenger, απορρίπτεται πολύ επιθετικά και μόνο όταν όλοι οι άλλοι τύποι κίνησης έχουν πλήρως εξυπηρετηθεί.

Εικόνα 3-8: Επιθετική Απόρριψη Ανώμαλης Κίνησης



[44]

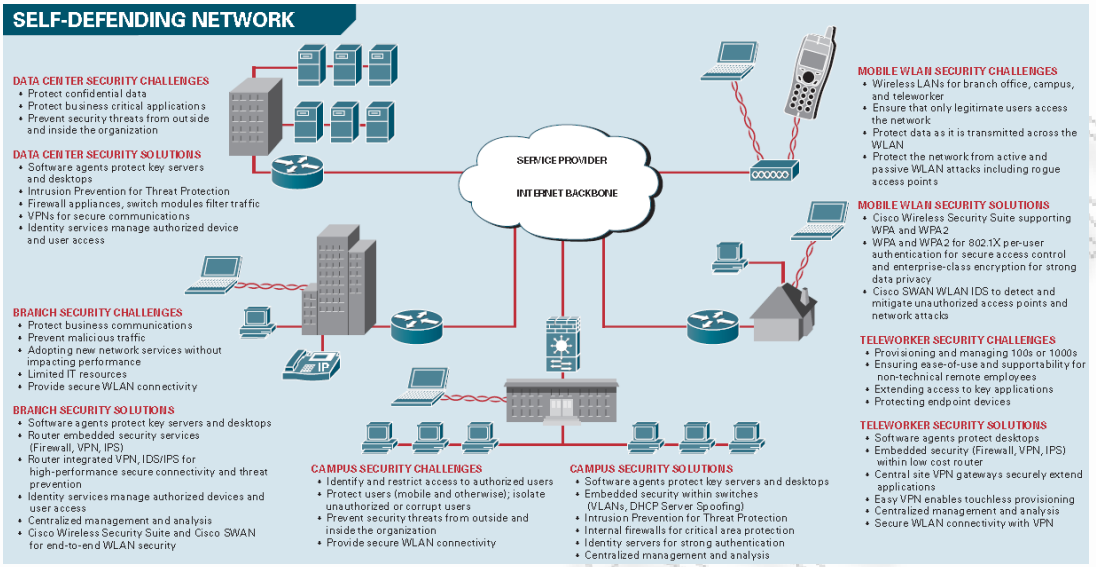
Ένα σημείο κλειδί αυτής της στρατηγικής είναι ότι νόμιμες κυκλοφοριακές ροές που υπερβαίνουν προσωρινά το κατώφλι δεν τιμωρούνται από τη Scavenger τάξη. Μόνο συνεχή, «ανώμαλα» ρεύματα που παράγονται ταυτόχρονα από πολλαπλούς hosts (ιδιαίτερα ενδεικτικό των επιθέσεων DoS/worm) υπόκεινται σε επιθετική απόρριψη και τέτοια διακοπή εμφανίζεται μόνο μετά από την εξυπηρέτηση όλης της νόμιμης κίνησης.

Οι ενεργές ζεύξεις ενός Campus δεν είναι τα μόνα σημεία στην υποδομή δικτύου όπου μπορεί να εμφανιστεί συμφόρηση. Τυπικά οι WAN και VPN ζεύξεις είναι οι πρώτες που υπόκεινται σε συμφόρηση. Επομένως, η ουρά αναμονής για την κίνηση της Scavenger τάξης, πρέπει να ενεργοποιείται σε όλες τις δικτυακές συσκευές με συγκεκριμένο τρόπο (σύμφωνα με τις δυνατότητες του hardware).

Πριν τεθεί παραγωγικά η ανάπτυξη ενός δικτύου πρέπει να δοκιμαστούν λεπτομερώς οι πολιτικές QoS. Είναι σημαντικό να τονιστεί ότι η εφαρμογή της τεχνικής Scavenger μετριάζει μόνο ένα μέρος των επιδράσεων από ορισμένους τύπους επιθέσεων DoS/worm και δεν εκμηδενίζει τον κίνδυνο.

Η Τάξη Scavenger για παροχή QoS, είναι ένα τμήμα μιας περιεκτικής στρατηγικής της Cisco που αφορά την ασφάλεια ενοποιημένων δικτύων και ονομάζεται Self-Defending Networks (SDN). Η SDN στρατηγική δεν αποτελεί αντικείμενο της παρούσας εργασίας και για αυτό δε θα επεκταθούμε σε λεπτομερείς αναλύσεις, παρά μόνο σε μια γενική εικόνα όπως παρουσιάζεται στη συνέχεια:

Εικόνα 3-9: Self-Defending Network



[45]

3.2.2 Ουρά Αναμονής

Αφότου τα πακέτα έχουν χαρακτηριστεί με την κατάλληλη ετικέτα στο Layer-2 (CoS) και Layer-3 (DSCP ή PHB), είναι σημαντικό να παραμετροποιηθεί το δίκτυο ώστε να κατατάσσει τα πακέτα στην κατάλληλη ουρά αναμονής με βάση την ταξινόμησή τους και κατά συνέπεια να παρέχεται σε κάθε τάξη κίνησης η κατάλληλη υπηρεσία. Με ενεργοποιημένο το QoS στις δικτυακές συσκευές Layer-2 και Layer-3 μπορεί να παραμετροποιηθεί όλη η κίνηση φωνής ώστε να καταταγεί σε ξεχωριστές ουρές αναμονής, εξαλείφοντας έτσι την πιθανότητα απόρριψης πακέτων φωνής.

Παρότι σε ένα επιχειρησιακό δίκτυο υπάρχουν εργαλεία διαχείρισης που μπορούν να δείξουν αν αυτό είναι κορεσμένο ή όχι, απαιτούνται ακόμα και QoS εργαλεία για να εξασφαλίζουν την ποιότητα φωνής. Τα εργαλεία διαχείρισης δικτύου παρουσιάζουν μόνο τη μέση συμφόρηση πάνω σε ένα χρονικό δείγμα. Ενώ αυτός ο μέσος όρος είναι χρήσιμος, δεν παρουσιάζει τις αιχμές συμφόρησης σε μια διεπαφή.

3.2.3 Παροχή Εύρους Ζώνης

Σε ένα τοπικό επιχειρησιακό δίκτυο, απαιτείται προσεκτικός προγραμματισμός της υποδομής έτσι ώστε το διαθέσιμο εύρος ζώνης να είναι πάντα αρκετά υψηλότερο από το απαιτούμενο και αυτό για να μην προκαλείται καμία συμφόρηση. Η επιπλέον προσθήκη του φορτίου κίνησης φωνής επάνω σε ένα συγκριμένο δίκτυο δεν αντιπροσωπεύει μια σημαντική αύξηση στο γενικό φορτίο. Ο υπολογισμός του παρεχόμενου εύρους ζώνης συνεχίζει να βασίζεται στις απαιτήσεις της κίνησης δεδομένων. Ο σχεδιαστικός στόχος είναι να αποφευχθεί η εκτενής κυκλοφοριακή συμφόρηση δεδομένων σε οποιαδήποτε σύνδεση όπου θα εξυπηρετεί εφαρμογές πραγματικού χρόνου. Η αντιπαράθεση των απαιτήσεων εύρους ζώνης μιας φωνητικής κλήσης G.711 (περίπου 86 Kbps) με το εύρος ζώνης μιας FastEthernet σύνδεσης (100 Mbps) δείχνει ότι η φωνή δεν είναι μια πηγή κίνησης που προκαλεί τη συμφόρηση στο δίκτυο αλλά μάλλον είναι μια προστατευμένη από το δίκτυο κίνηση.

3.3 Ποιότητα Υπηρεσίας σε Δίκτυο Ευρείας Περιοχής

Πριν τα δεδομένα φωνής διατεθούν σε ένα δίκτυο, είναι σημαντικό πρώτα απ` όλα να εξασφαλιστεί ότι υπάρχει επαρκές εύρος ζώνης για όλες τις απαραίτητες εφαρμογές. Μόλις

παρασχεθεί το εύρος ζώνης, το επόμενο βήμα είναι να διαμορφωθεί σε όλες τις διεπαφές (Interface) μια ουρά προτεραιότητας για τη κίνηση φωνής. Αυτή η ουρά είναι απαραίτητη ώστε να μειώθει το Jitter και η απώλεια πακέτων που θα προκληθούν από μια πιθανή έξαρση της κίνησης και κατά συνέπεια την υπερφόρτωση του ενδιάμεσου καταχωρητή (buffer). Αυτή η απαραίτητη σειρά είναι παρόμοια με αυτήν για την υποδομή ενος τοπικού LAN που έγινε αναφορά στην προηγούμενη ενότητα.

Μετά, το WAN απαιτεί (τυπικά) κάποιους επιπρόσθετους μηχανισμούς, όπως η «Διαμόρφωση Κίνησης» ώστε να εξασφαλιστεί ότι στις WAN ζεύξεις δεν αποστέλλεται περισσότερη κίνηση από αυτή που μπορούν να διαχειριστούν, γεγονός το οποίο θα μπορούσε να προκαλέσει απώλεια πακέτων.

Τέλος, για τις ζεύξεις χαμηλής ταχύτητας ενός WAN υπάρχουν συγκεκριμένες τεχνικές εφαρμογής όπως ο μηχανισμός Link Fragmentation and Interleaving (LFI), όπου χρησιμοποιείται για να αποτρέψει την απαράδεκτη αναμονή που προκαλείται σε μια ουρά διεπαφής όταν μεγάλα πακέτα βρεθούν μπροστά από τα πακέτα φωνής.

Ο στόχος αυτών των QoS μηχανισμών είναι να εξασφαλίζουν την αξιόπιστη και υψηλής ποιότητας μετάδοση φωνής μέσω της μείωσης της καθυστέρησης, της απώλειας πακέτων, και την εξάλειψη του Jitter. Ο ακόλουθος πίνακας απαριθμεί τα απαιτούμενα QoS χαρακτηριστικά και εργαλεία ώστε να επιτευχθεί ο προαναφερθείς στόχος.

Πίνακας 3-3: Απαιτούμενα QoS Χαρακτηριστικά και Εργαλεία για την Υποστήριξη της IP Τηλεφωνίας για Κάθε WAN Τεχνολογία και Ταχύτητα Σύνδεσης

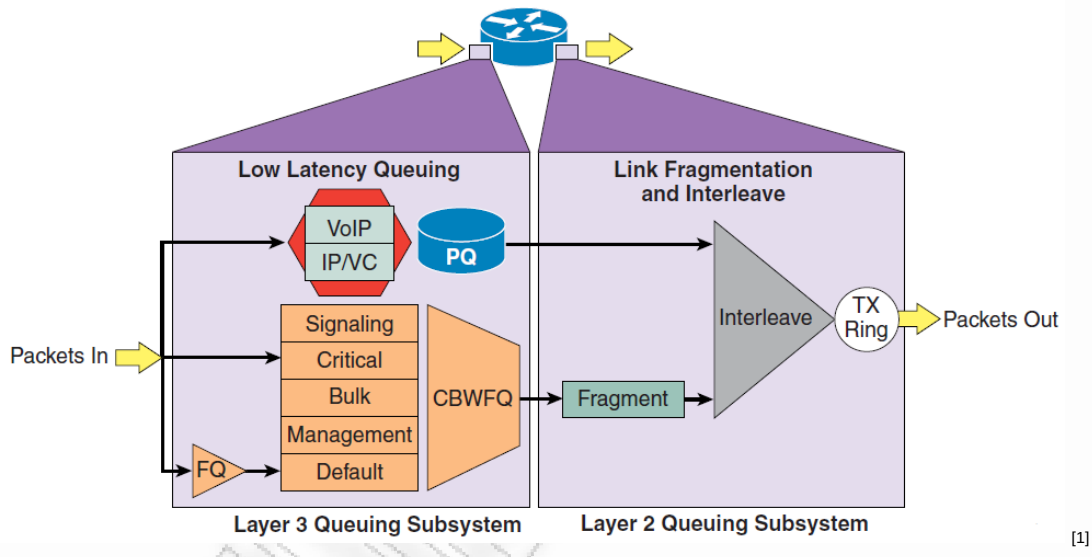
Τεχνολογία WAN	56 Kbps ≤ Ταχύτητα Ζεύξης ≤ 768 Kbps	Ταχύτητα Ζεύξης ≻ 768 Kbps
Leased Lines	1. Multilink Point-to-Point Protocol (MLP) 2. Link Fragmentation and Interleaving(LFI) 3. Low Latency Queuing (LLQ) 4. Optional: Compressed Real-Time Transport Protocol (cRTP)	1. LLQ
Frame Relay (FR)	1. Traffic Shaping 2. LFI (FRF.12) 3. LLQ 4. Προαιρετικά: cRTP 5. Προαιρετικά: Voice-Adaptive Traffic Shaping (VATS) 6. Προαιρετικά: Voice-Adaptive Fragmentation (VAF)	1. Traffic Shaping 2. LLQ 3. Προαιρετικά: VATS
Asynchronous Transfer Mode (ATM)	1. Αλλαγές στο TX-ring buffer 2. MLP over ATM 3. MLP LFI 4. LLQ 5. Προαιρετικά: cRTP (απαιτεί MLP)	1. Αλλαγές στο TX-ring buffer 2. LLQ
Frame Relay and ATM Service Inter-Working (SIW)	1. Αλλαγές στο TX-ring buffer 2. MLP over ATM and FR 3. MLP LFI 4. LLQ 5. Προαιρετικά: cRTP (απαιτεί MLP)	1. Αλλαγές στο TX-ring buffer 2. MLP over ATM and FR 3. LLQ
Multiprotocol Label Switching (MPLS)	1. Όμοια με παραπάνω, ακολουθώντας τη τεχνολογία διεπαφής	1. Όμοια με παραπάνω, ακολουθώντας τη τεχνολογία διεπαφής

Στις ακόλουθες ενότητες περιγράφονται ορισμένες από τις σημαντικότερες τεχνικές που εφαρμόζονται κατά το σχεδιασμό και την υλοποίηση ενός Δικτύου Ευρείας Περιοχής που υποστηρίζει και μετάδοση φωνής.

3.3.1 Προτεραιότητα Κίνησης

Επιλέγοντας ανάμεσα στα πολλά διαθέσιμα σχήματα προτεραιότητας, τα σημαντικότερα που πρέπει να ληφθούν υπόψη σε ένα WAN είναι ο τύπος της κίνησης και ο τύπος της επικοινωνίας. Για πολλαπλής υπηρεσίας κίνηση πάνω σε ένα IP WAN, η Cisco προτείνει εφαρμογή Low-Latency Queuing (LLQ) σε όλους τους συνδέσμους. Η μέθοδος αυτή υποστηρίζει μέχρι και 64 τάξεις κίνησης, με την ικανότητα να καθορίζει, για παράδειγμα, εφαρμογή ουράς προτεραιότητας για φωνή και διαδραστικά Video, το ελάχιστο bandwidth μέσω του αλγορίθμου CBWFQ για την κίνηση ελέγχου φωνής, το επιπρόσθετο ελάχιστο bandwidth μέσω του αλγορίθμου WFQ για σημαντικά δεδομένα και μια προκαθορισμένα best-effort ουρά για όλους τους άλλους τύπους κίνησης. Στην Εικόνα 3-10 φαίνεται ένα παράδειγμα σχήματος προτεραιότητας.

Εικόνα 3-10: Βελτιστοποιημένη Ουρά Αναμονής για VoIP πάνω από το WAN



[1]

Η Tx-Ring είναι μια τελική FIFO ουρά, υπεύθυνη για να συγκρατεί τα πλαίσια που πρέπει να διαβιβάζονται αμέσως από τη φυσική διεπαφή. Εξασφαλίζει πως ένα πλαίσιο θα είναι πάντα διαθέσιμο όταν η διεπαφή θα επιθυμεί να διαβιβάσει την κυκλοφορία και κατά συνέπεια έτσι επιτυγχάνεται η μέγιστη χρήση της γραμμής μετάδοσης. Το μέγεθος της Tx-Ring εξαρτάται από το υλικό και τον αλγόριθμο αναμονής που έχει διαμορφωθεί στην εκάστοτε διεπαφή. Σε ορισμένες πλατφόρμες/διεπαφές οι Tx-Ring πρέπει να είναι συντονισμένες ώστε να αποφεύγονται ανεπιθύμητες καθυστερήσεις/Jitter από αυτές.

Η Cisco συνιστά τα ακόλουθα κριτήρια προτεραιότητας για LLQ:

- Το κριτήριο για να ενταχθεί ένα πακέτο φωνής σε ουρά προτεραιότητας (PQ) είναι: α) η τιμή του Differentiated Services Code Point (DSCP) να είναι ίση με 46 ή β) μια EF per-hop Behavior (PHB) τιμή.
- Το κριτήριο για να ενταχθούν τα πακέτα *Video συνομιλίας* σε ουρά προτεραιότητας είναι α) η τιμή του Differentiated Services Code Point (DSCP) να είναι ίση με 34 ή β) PHB τιμή ίση με AF41. Παρόλα αυτά εξαιτίας του μεγαλύτερου μεγέθους των πακέτων της κίνησης των Video, αυτά τα πακέτα πρέπει να μπουν σε ουρά προτεραιότητας μόνο για WAN συνδέσμους που είναι ταχύτεροι των 768 Kbps. Σε ταχύτητες συνδέσμων (Link) που είναι χαμηλότερες της τιμής 768 Kbps απαιτείται ο τεμαχισμός των πακέτων

πριν την μετάδοση τους. Όμως όπως φαίνεται και στην παραπάνω εικόνα τα πακέτα που μπαίνουν σε ουρά προτεραιότητας (PQ) δεν τεμαχίζονται, γεγονός που μπορεί να αναγκάσει σε καθυστέρηση τα μικρότερα πακέτα φωνής που θα βρεθούν πίσω από τα μεγαλύτερα πακέτα Video. Συνεπώς, σε ζεύξεις με ταχύτητα μικρότερη ή ίση των 768 Kbps, η κίνηση των Video συνδιαλέξεων πρέπει να τοποθετείται σε ξεχωριστή CBWFQ.

- Όταν υπάρχει συμφόρηση σε WAN συνδέσμους, είναι δυνατόν να διακοπούν τα πρωτόκολλα ελέγχου φωνής, εξαλείφοντας την ικανότητα των IP τηλεφώνων να ολοκληρώσουν κλήσεις. Έτσι τα πρωτόκολλα ελέγχου φωνής H.323, MGCP, και SCCP (Skinny Client Control Protocol), απαιτούν τη δική τους Τάξη. Το αρχικό κριτήριο για αυτήν την ουρά είναι μια DSCP τιμή ίση με 24 ή μια PHB τιμή ίση με CS3.

  Παρατήρηση: Η Cisco έχει αρχίσει να αλλάζει την τιμή των πρωτοκόλλων ελέγχου φωνής από DSCP 26 (PHB AF31) σε DSCP 24 (PHB CS3). Παρόλα αυτά πολλά προϊόντα ακόμα χαρακτηρίζουν την κίνηση σηματοδοσίας με DSCP 26 (PHB AF31), επομένως στο μεσοδιάστημα η Cisco συνιστά να χρησιμοποιούνται ταυτόχρονα τόσο το AF31 όσο και το CS3.

- Σε ορισμένες περιπτώσεις, συγκεκριμένη κίνηση δεδομένων μπορεί να απαιτήσει καλύτερη μεταχείριση από την best-effort. Η κίνηση αυτή αφορά σημαντικά δεδομένα και τοποθετείται σε μια ή περισσότερες ουρές προτεραιότητας που έχουν το απαιτούμενο ποσό εύρους ζώνης. Το σχήμα προτεραιότητας σε αυτή την τάξη ακολουθεί τη λογική First-In-First-Out (FIFO) με το ελάχιστο μεριζόμενο εύρος ζώνης, ενώ η κίνηση που υπερβαίνει το προπαραμετροποιημένο όριο εύρους ζώνης τοποθετείται στην προκαθορισμένη ουρά. Το αρχικό κριτήριο για αυτή την ουρά μπορεί να είναι ο TCP αριθμός πόρτας (port number), μια Layer 3 διεύθυνση ή μια DSCP/PHB τιμή.

- Όλη η υπολειπόμενη κίνηση μπορεί να τοποθετηθεί σε μια προκαθορισμένη ουρά για best-effort μεταχείριση. Αν καθοριστεί η λέξη κλειδί **fair**, ο αλγόριθμος προτεραιότητας θα γίνει FQ.

Τεχνικές για Ζεύξεις Μικρού Εύρους Ζώνης

Οι ακόλουθες τεχνικές βελτιώνουν την ποιότητα και την αποτελεσματικότητα των WAN ζεύξεων χαμηλής ταχύτητας.

3.3.2 Μηχανισμός Συμπίεσης Κεφαλίδας

Η αποδοτικότητα μιας ζεύξης δικτύου μπορεί να αυξηθεί με τη χρησιμοποίηση του cRTP πρωτοκόλλου. Αυτό το πρωτόκολλο συμπιέζει μια 40 byte IP, UDP και RTP κεφαλίδα σε περίπου δύο έως τέσσερα bytes. Η χρήση του cRTP ενδείκνυται σε μια συγκεκριμένη ζεύξη μόνο εάν η τελευταία ικανοποιεί όλους τους ακόλουθους όρους:

1. Η κίνηση της φωνής αντιπροσωπεύει περισσότερο από το 33% του φορτίου στη συγκεκριμένη ζεύξη.
2. Η ζεύξη χρησιμοποιεί έναν codec με χαμηλό δυφιορρυθμό (bit-rate), πχ ο G.729.
3. Καμία άλλη εφαρμογή πραγματικού χρόνου (πχ τηλεοπτική σύσκεψη) δε χρησιμοποιεί την ίδια ζεύξη.

Εάν η ζεύξη αποτύχει να ικανοποιήσει οποιονδήποτε από τους προηγούμενους όρους, τότε το cRTP δεν είναι αποτελεσματικό και δεν πρέπει να χρησιμοποιηθεί στη συγκεκριμένη ζεύξη. Μια άλλη σημαντική παράμετρος που πρέπει να εξεταστεί, διότι επηρεάζεται αρνητικά από διαδικασίες συμπίεσης και αποσυμπίεσης, είναι η απαιτούμενη CPU του Router. Να σημειωθεί ότι η συμπίεση εφαρμόζεται ως τελικό βήμα προτού να φτάσει ένα πακέτο στη διεπαφή εξόδου του δρομολογητή, δηλαδή μετά από την εφαρμογή LLQ και αφού ήδη έχει ταξινομηθεί η κίνηση.

Από την έκδοση Cisco IOS 12.(2)2T και μετά υπάρχει ο μηχανισμός ανατροφοδότησης του LLQ που επιτρέπει στο bandwidth της τάξης φωνής να διαμορφωθεί βασισμένο στη συμπιεσμένη τιμή του πακέτου, κάτι που δεν συνέβαινε στις προγενέστερες εκδόσεις με αποτέλεσμα το LLQ να αγνοεί το συμπιεσμένο εύρος ζώνης (compressed bandwidth) και κατά συνέπεια το εύρος ζώνης της κλάσης που εξυπηρετεί την κίνηση φωνής να υπολογίζεται χωρίς την παράμετρο αυτή.

Στον επόμενο πίνακα παρουσιάζονται οι διαφορές στον υπολογισμό εύρους ζώνης της κλάσης που εξυπηρετεί την κίνηση φωνής, με και χωρίς ανατροφοδότηση του LLQ όπως έγινε αναφορά παραπάνω. Για το παράδειγμα υποθέτουμε μια ζεύξη 512 kbps με χρήση του codec G.729 και απαίτηση πραγματοποίησης 10 κλήσεων.

Πίνακας 3-4: LLQ Απαιτήσεις Εύρους Ζώνης Τάξης Κίνησης Φωνής για 10 Κλήσεις, 512 Kbps Εύρος Ζώνης Ζεύξης και Χρήση του G.729 Codec.

Cisco IOS Release	Με cRTP όχι διαμορφωμένο	Με cRTP διαμορφωμένο
Προγενέστερες από 12.2(2)T	240 Kbps	240 Kbps
12.2(2)T και μεταγενέστερες	240 Kbps	100 Kbps

Πρέπει να σημειωθεί ότι για τον υπολογισμό των τιμών του πίνακα θεωρήθηκαν τα ακόλουθα: 24 kbps για μη cRTP G.729 κλήσεις και 10 kbps για cRTP G.729 κλήσεις. Αυτά τα νούμερα εύρους ζώνης βασίζονται μόνο στο voice payload και τις IP/UDP/RTP κεφαλίδες και δεν λαμβάνουν υπόψη την επιβάρυνση κεφαλίδων του Layer 2, κάτι που στην πράξη πρέπει να συνυπολογιστεί βασισμένο στον τύπο της επιλεγμένης ζεύξης. Πρέπει επίσης να σημειωθεί ότι από την έκδοση Cisco IOS 12.2(13)T και μετά, το cRTP μπορεί να διαμορφωθεί ως τμήμα της τάξης φωνής. Αυτή η επιλογή επιτρέπει στο cRTP να καθοριστεί μέσα σε μια τάξη, που συνδέεται με μια εφαρμογή ανταλλαγής στοιχείων μέσω μιας πολιτικής υπηρεσιών. Αυτό το νέο χαρακτηριστικό γνώρισμα παρέχει τις στατιστικές συμπίεσης και την κατάσταση του εύρους ζώνης μέσω της εντολής ***show policy interface*** η οποία μπορεί να είναι πολύ χρήσιμη στον καθορισμό του ποσοστού που παρέχεται σε μια υπηρεσία πολιτικής τάξης μιας διεπαφής.

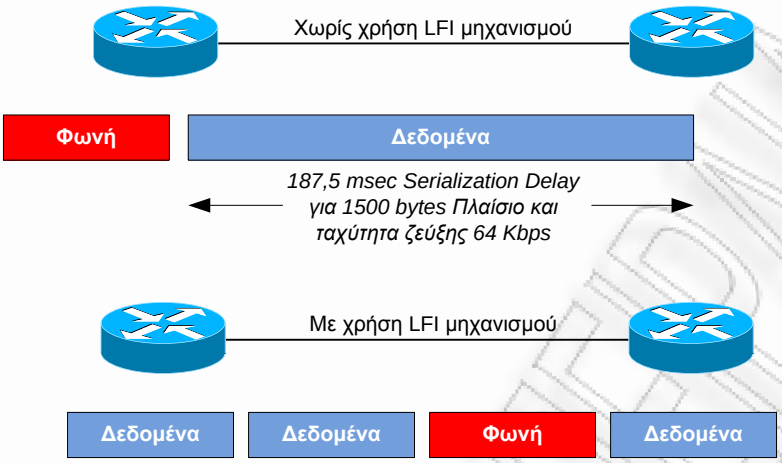
3.3.3 Κατακερματισμός και Παρεμβολή Συνδέσμου

Σε ζεύξεις χαμηλής ταχύτητας (μικρότερη από 768 Kbps), η χρήση του μηχανισμού LFI κρίνεται απαραίτητη για επίτευξη αποδεκτής ποιότητας φωνής. Αυτή η τεχνική περιορίζει το Jitter που προκαλείται από την παρεμπόδιση της κίνησης φωνής όταν βρεθεί πίσω από μεγάλα πλαίσια δεδομένων όπως παρουσιάζεται και σχηματικά στη συνέχεια. Οι δύο τεχνικές που υπάρχουν για αυτό το λόγο είναι: η Multilink Point-to-Point Protocol (MLP) LFI (για Leased Lines και ATM) και η FRF.12 για το Frame Relay.

Για να γίνει περισσότερο κατανοητή η αξία του LFI μηχανισμού ας υποθέσουμε πως ένα «άτυχο» πακέτο φωνής περιμένει να εξυπηρετηθεί πίσω από ένα μεγάλο πακέτο δεδομένων. Το πακέτο δεδομένων μπορεί να είναι σε μέγεθος, το πολύ ίσο με την MTU (Maximum Transmission Unit, Μέγιστη Μονάδα Μετάδοσης) τιμή. Έτσι για μια ζεύξη με ταχύτητα 64 Kbps και ένα πακέτο δεδομένων MTU τιμής ίση με 1500 bytes θα έχουμε:

$$\text{Serialization Delay} = \frac{\text{Frame Size}}{\text{Link Speed}} = \frac{1500 * 8 \text{ bits}}{64000 \text{ bits/sec}} = 187{,}5 \text{ msec}$$

Εικόνα 3-11: Κατακερματισμός και Παρεμβολή Συνδέσμου



Ως εκ τούτου, στο προηγούμενο σενάριο ένα VoIP πακέτο μπορεί να χρειαστεί να περιμένει έως και 187,5 msec πριν να μπορεί να σταλεί. Όμως, όπως ήδη έχει αναφερθεί, κάθε εφαρμογή έχει τα δικά της χαρακτηριστικά που καθορίζουν τις ανοχές της σε καθυστέρηση, μεταβλητότητα καθυστέρησης (Jitter) και απώλεια πακέτων. Για να χαρακτηριστεί μια VoIP κλήση «υψηλής ποιότητας», θα πρέπει οι από άκρο σε άκρο καθυστερήσεις να μη ξεπερνούν τα 150 msec, το Jitter να είναι έως 20 msec και η απώλεια πακέτων μικρότερη από το 1%. Συνεπώς, η 187,5 msec καθυστέρηση συριακής διάταξης (serialization delay) δεν μπορεί να είναι αποδεκτή και πρέπει να μειωθεί.

Απαιτείται λοιπόν ένας μηχανισμός που να εξασφαλίζει ότι ο χρόνος μετάδοσης κάθε μονάδας δε θα ξεπερνά τα 10 msec. Έτσι, οποιοδήποτε πακέτο απαιτεί να δημιουργήσει καθυστέρηση συριακής διάταξης μεγαλύτερη από την επιτρεπτή και κατά συνέπεια να δημιουργήσει μεγάλη καθυστέρηση στα «ευαίσθητα» ως προς το χρόνο παράδοσης πακέτα, χωρίζεται σε 10 msec τεμάχια. Ένα 10 msec τεμάχιο ή τμήμα είναι ο αριθμός των bytes που μπορούν να σταλούν πάνω από τη συγκεκριμένη ζεύξη σε χρόνο 10 msec και υπολογίζεται ως εξής:

$$\text{Fragmentation Size} = \frac{0{,}01\ \text{sec} * 64000\ \text{bits/sec}}{8\ \text{bits/byte}} = 80\ \text{bytes}$$

Συνεπώς, σε ζεύξεις χαμηλής ταχύτητας όπου το 10 msec τεμάχιο είναι μικρότερο από την MTU, ο κατακερματισμός κρίνεται απαραίτητος. Βέβαια ο κατακερματισμός από μόνος του είναι ανεπαρκής και αυτό διότι αν ένα VoIP πακέτο πρέπει να περιμένει να αποσταλεί μετά από όλα τα δημιουργούμενα τεμάχια, τότε η καθυστέρησή του θα συνεχίσει να κυμαίνεται σε μη αποδεκτά επίπεδα. Για το λόγο αυτό η παρεμβολή (interleaving) περιλαμβάνει διαδικασίες «περίπλεξης» πακέτων που είναι «ευαίσθητα» ως προς το χρόνο παράδοσής τους στην αλληλουχία των κατακερματισμένων πακέτων δεδομένων.

Πρέπει να σημειωθεί πως το μέγεθος του κατακερματισμένου πακέτου δεν πρέπει ποτέ να είναι μικρότερο από το μέγεθος του VoIP πακέτου. Επίσης είναι σημαντικό να σημειωθεί πως ποτέ δεν πρέπει να κατακερματίζονται τα VoIP πακέτα και αυτό διότι μπορεί να επηρεαστεί αρνητικά η ποιότητα.

Στον επόμενο πίνακα παρουσιάζονται τα συνιστώμενα μεγέθη τεμαχίων για διάφορες ταχύτητες ζεύξης με βάση τον κανόνα των 10 msec.

Πίνακας 3-5: Ταχύτητα Ζεύξης και Μέγεθος Τεμαχίου

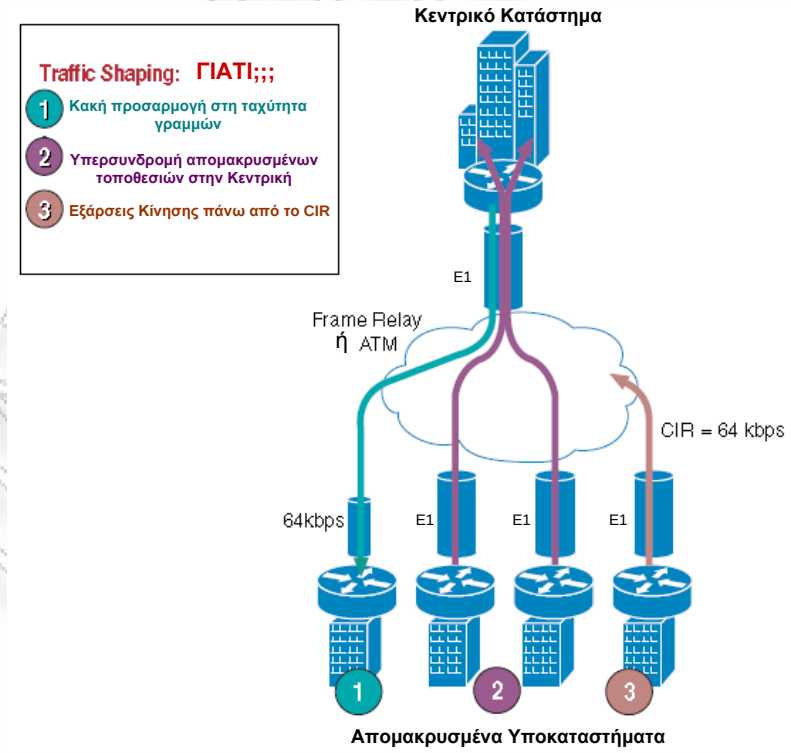
Ταχύτητα Ζεύξης (Kbps)	Μέγεθος Τεμαχίου (bytes)
56	70
64	80
128	160
256	320
512	640
768	960
1024	1280
1536	1920 (δεν συνιστάται τεμαχισμός διότι το μέγεθος του τεμαχίου προκύπτει μεγαλύτερο από την MTU)

3.3.4 Μορφοποίηση Κίνησης

Η μορφοποίηση της κίνησης απαιτείται για την πολλαπλή πρόσβαση μέσων μη πολυεκπομπής (non-broadcast) σαν το ATM και το Frame Relay, όπου η φυσική ταχύτητα πρόσβασης ποικίλλει μεταξύ δύο ακροσημείων (endpoints) και διάφορα δίκτυα υποκαταστημάτων αθροίζονται τυπικά σε μια ενιαία διεπαφή στον δρομολογητή του κεντρικού καταστήματος. Το ακόλουθο σχήμα επεξηγεί τους κύριους λόγους για τους οποίους απαιτείται κατά τη μεταφορά της φωνής και των δεδομένων μέσα σε ένα IP WAN η εφαρμογή του μηχανισμού Traffic Shaping.

Στο επόμενο σχήμα παρουσιάζονται τρία διαφορετικά σενάρια:

Εικόνα 3-12: Traffic Shaping με Frame Relay και ATM



[1]

Κακή Προσαρμογή στη Ταχύτητα Γραμμών

Τυπικά μια διεπαφή ενός δρομολογητή που βρίσκεται στο κεντρικό κατάστημα και συνδέεται με την αντίστοιχη διεπαφή ενός δρομολογητή σε ένα απομακρυσμένο υποκατάστημα, υποστηρίζει υψηλές ταχύτητες (όπως E1 και μεγαλύτερες). Στην περίπτωση που η αντίστοιχη διεπαφή στο υποκατάστημα δεν υποστηρίζει ίση ταχύτητα μεταφοράς δεδομένων αλλά αρκετά μικρότερη (για παράδειγμα 64 kbps), μπορεί να μειώσει σημαντικά την ταχύτητα μεταφοράς δεδομένων της γραμμής. Αυτό διότι αν τα δεδομένα αποστέλλονται από τον κεντρικό κόμβο σε έναν απομακρυσμένο κόμβο, χαμηλής ταχύτητας, τότε στη διεπαφή του απομακρυσμένου σημείου μπορεί να υπάρξει συμφόρηση με αποτέλεσμα την υποβίβαση της απόδοσης και την παροχή κακής ποιότητας φωνής.

Η υλοποίηση του Traffic Shaping πρέπει να εφαρμόζεται στη διεπαφή εξόδου του κεντρικού δρομολογητή και όχι στη διεπαφή εισόδου του απομακρυσμένου (που δεν υποστηρίζει υψηλές ταχύτητες μεταφοράς δεδομένων). Αυτό διότι στην αντίθετη περίπτωση θα χάνονται πακέτα από την υπερχείλιση της ουράς στη διεπαφή εισόδου του απομακρυσμένου δρομολογητή.

Υπερσυνδρομή Απομακρυσμένων Τοποθεσιών στην Κεντρική Τοποθεσία

Είναι κοινή πρακτική στα δίκτυα Frame Relay ή ATM, να συναθροίζονται πολλά απομακρυσμένα σημεία (υποκαταστήματα) σε ένα ενιαίο κεντρικό κόμβο (κεντρικό κατάστημα). Παραδείγματος χάριν, μπορεί να υπάρξουν πολλά υποκαταστήματα που συνδέονται με το WAN με μια διεπαφή E1 όμως το κεντρικό σημείο να έχει μόνο μια ενιαία διεπαφή E1. Καθώς αυτή η παραμετροποίηση επιτρέπει την ανάπτυξη ώστε να επωφεληθεί από την τεχνική της «στατιστικής πολυπλεξίας» (statistical multiplexing), η διεπαφή του κεντρικού δρομολογητή μπορεί να υπερφορτωθεί κατά τη διάρκεια ενός πιθανού καταιγισμού κίνησης, υποβιβάζοντας κατά συνέπεια την ποιότητα φωνής.

Στατιστική πολυπλεξία

Στα δίκτυα με Σύγχρονο Τρόπο Μεταγωγής (Synchronous Transfer Mode – STM, βασίζεται στην μεταγωγή κυκλωμάτων και στη σύγχρονη πολύπλεξη, ενώ ο ATM τρόπος βασίζεται σε μεταγωγή πακέτων και σε ασύγχρονη πολύπλεξη) εμφανίζεται ένα πρόβλημα απόδοσης, το πρόβλημα του αχρησιμοποίητου πακέτου. Όταν εγκαθίσταται μια σύνδεση STM, το ποσοστό των πόρων του δικτύου που αφιερώνεται στη σύνδεση παραμένει σταθερό ανεξάρτητα του βαθμού χρησιμοποίησής της. Έτσι ένα μεγάλο ποσοστό του διαθέσιμου εύρους ζώνης παραμένει αχρησιμοποίητο.

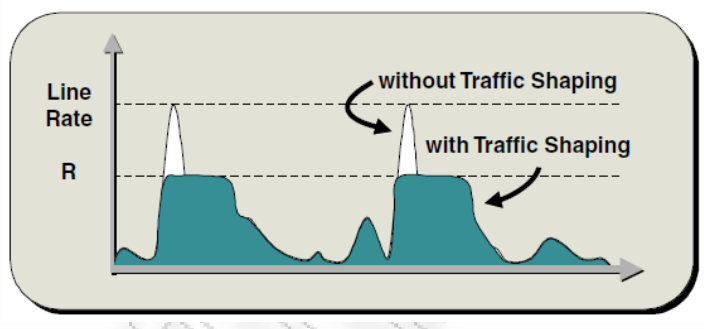
Στο ATM γίνεται μια προσπάθεια να λυθεί το πρόβλημα με την τεχνική που ονομάζεται στατιστική πολυπλεξία. Σύμφωνα με αυτήν, πολλές συνδέσεις μπορούν να μοιράζονται ταυτόχρονα το ίδιο μέσο μετάδοσης, σύμφωνα πάντα με τα ιδιαίτερα χαρακτηριστικά κάθε σύνδεσης. Με άλλα λόγια, εάν πολλές συνδέσεις δεδομένων έχουν χαρακτηριστικά ριπής (burst), δηλαδή ο λόγος του μέγιστου ρυθμού μεταγωγής προς τον μέσο ρυθμό είναι αρκετά μεγάλος (π.χ. 10:1), τότε είναι αρκετά πιθανό αυτές να μπορούν να μοιράζονται το ίδιο διαθέσιμο εύρος με την στατιστικά μικρή πιθανότητα ότι δε θα συμβεί ταυτόχρονη εκπομπή πακέτου από όλες τις συνδέσεις. Ακόμα και αν συμβεί κάτι τέτοιο, θα πρέπει να υπάρχει η πρόβλεψη κάποιου χώρου προσωρινής αποθήκευσης των πακέτων (buffer) έτσι ώστε να μην υπάρχουν απώλειες. Η στατιστική πολυπλεξία επιτυγχάνει το άθροισμα των απαιτήσεων των επιμέρους συνδέσεων σε εύρος ζώνης σε ορισμένες περιπτώσεις, και κάτω από αυστηρές προϋποθέσεις υπερβαίνει το προκαθορισμένο εύρος ζώνης του φυσικού μέσου μετάδοσης. Αυτό ήταν μέχρι πρότινος αδύνατο με τα δίκτυα STM και αποτελεί το κύριο σημείο διαφοροποίησης του ATM.

Εξάρσεις Κίνησης

Μια άλλη κοινή παραμετροποίηση είναι να επιτρέπονται εξάρσεις κίνησης πάνω από το Δεσμευμένο Ρυθμό Πληροφορίας (Committed Information Rate, CIR), ο οποίος αντιπροσωπεύει το ρυθμό με τον οποίο ο φορέας παροχής υπηρεσιών έχει εγγυηθεί να μεταφέρει την κίνηση μέσω του δικτύου του χωρίς απώλειες και καθυστερήσεις. Παραδείγματος χάριν, σε μια απομακρυσμένη τοποθεσία, στη διεπαφή E1 να έχει οριστεί CIR μόνο 64 kbps. Τότε όταν περισσότερα από 64 kbps κίνησης στέλνονται μέσω WAN, ο φορέας παροχής υπηρεσιών χαρακτηρίζει την πρόσθετη κυκλοφορία ως «νόμιμη απόρριψη (discard eligible)». Συνεπώς εάν υπάρξει συμφόρηση στο δίκτυο του φορέα, η κίνηση αυτή θα απορριφθεί αφού δε θα αφορά την ταξινομημένη, προκαλώντας ενδεχομένως αρνητικά αποτελέσματα στην ποιότητα φωνής.

Ο μηχανισμός Traffic Shaping παρέχει μια λύση σε αυτά τα ζητήματα με τον περιορισμό της αποστελλόμενης κίνησης μέσω διεπαφής με ένα ρυθμό χαμηλότερο από το *Ρυθμό Γραμμής* (Line Rate), εξασφαλίζοντας κατά συνέπεια ότι καμία συμφόρηση δε θα εμφανίζεται. Η Εικόνα 3-13 που ακολουθεί επεξηγεί το μηχανισμό με ένα γενικό παράδειγμα, όπου το **R** είναι ο ρυθμός με εφαρμοσμένη τη διαμόρφωση κίνησης.

Εικόνα 3-13: Ο Μηχανισμός Traffic Shaping



[1]

3.3.5 Πρωτόκολλο Δέσμευσης Πόρων

Το Πρωτόκολλο Δέσμευσης Πόρων (Resource Reservation Protocol, RSVP) είναι το πρώτο σημαντικό βιομηχανικό πρότυπο που δυναμικά καθιερώνει εξαρχής το QoS μέσα σε ένα ετερογενές δίκτυο. Το RSVP που τρέχει πάνω σε IP, εισήχθη αρχικά από τον IETF στο RFC 2205 και επιτρέπει σε μια εφαρμογή να διατηρεί δυναμικά το δικτυακό εύρος ζώνης. Χρησιμοποιώντας το RSVP, οι εφαρμογές μπορούν να ζητήσουν ένα ορισμένο επίπεδο QoS για μια ροή δεδομένων μέσω ενός δικτύου. Λόγω της κατανεμημένης και δυναμικής φύσης του, το RSVP είναι σε θέση να διατηρεί το εύρος ζώνης πέρα από οποιαδήποτε τοπολογία δικτύων, επομένως μπορεί να χρησιμοποιηθεί για να παρέχει τοπολογικά ενημερωμένο έλεγχο αποδοχής κλήσεων για φωνή και βίντεο κλήσεις.

Βασικές Αρχές

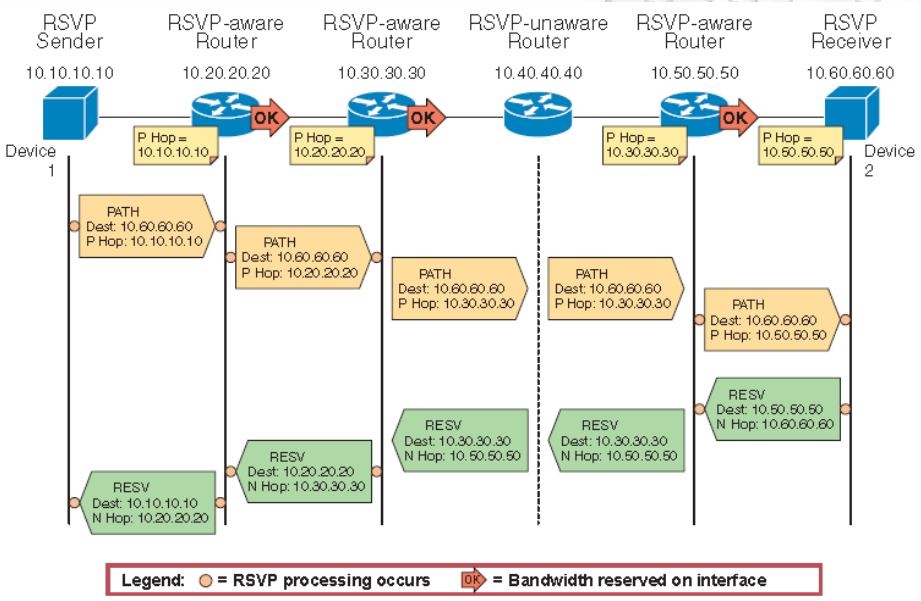
Το RSVP με τον καθορισμό μηνυμάτων σηματοδοσίας που ανταλλάσσονται μεταξύ των συσκευών πηγής και προορισμού καθώς και των ενδιάμεσων κόμβων (routers) κατά μήκος της διαδρομής, προβαίνει σε δέσμευση πόρων για μια συγκεκριμένη ροή δεδομένων. Τα RSVP μηνύματα σηματοδοσίας είναι πακέτα IP με καθορισμένο αριθμό πρωτοκόλλου κεφαλίδας το 46. Στη συνέχεια δρομολογούνται μέσω του δικτύου σύμφωνα με τα υπάρχοντα πρωτόκολλα δρομολόγησης.

Στην πορεία δεν απαιτείται όλοι οι routers να υποστηρίξουν το RSVP επειδή το πρωτόκολλο σχεδιάστηκε για να λειτουργεί με διαφανή τρόπο στους μη ενημερωμένους RSVP κόμβους. Σε κάθε δρομολογητή με ενεργοποιημένο το RSVP η διαδικασία RSVP διακόπτει τα μηνύματα σηματοδοσίας και αλληλεπιδρά με το διαχειριστή QoS για τις διεπαφές του

δρομολογητή που περιλαμβάνονται στη ροή δεδομένων προκειμένου «να διατηρηθούν» οι πόροι. Όταν οι διαθέσιμοι πόροι δεν είναι αρκετοί για τη ροή δεδομένων οπουδήποτε κατά μήκος της διαδρομής, οι δρομολογητές επισημαίνουν την αποτυχία πίσω στην εφαρμογή που δημιούργησε το αίτημα δέσμευσης.

Ο τρόπος λειτουργίας του Πρωτόκολλου Δέσμευσης Πόρων μπορεί να γίνει κατανοητός με τη χρήση του παρακάτω παραδείγματος. Σε αυτό το διάγραμμα, μια εφαρμογή επιθυμεί να δεσμεύσει πόρους δικτύου για ένα ρεύμα δεδομένων που ρέει από τη συσκευή 1, της οποίας η IP διεύθυνση είναι η 10.10.10.10, στη συσκευή 2, της οποίας η IP διεύθυνση είναι η 10.60.60.60.

Εικόνα 3-14: Παράδειγμα Δέσμευσης Πόρων



[1]

Τα ακόλουθα βήματα περιγράφουν τη διαδικασία RSVP-σήμανσης για το παράδειγμα του σχήματος:

1. Η εφαρμογή που βρίσκεται στη Συσκευή 1 δημιουργεί ένα RSVP μήνυμα αποκαλούμενο PATH (Διαδρομή), το οποίο αποστέλλεται στην ίδια IP διεύθυνση προορισμού με τη ροή δεδομένων για την οποία ζητείται μια δέσμευση (δηλαδή το 10.60.60.60) και με την επιλογή "router alert" που ενεργοποιείται στην IP κεφαλίδα. Το μήνυμα PATH περιέχει, μεταξύ άλλων, τα ακόλουθα αντικείμενα:

   - Το αντικείμενο «session» (συνόδου), που αποτελείται από τη διεύθυνση προορισμού IP, τον αριθμό πρωτοκόλλου και το UDP/TCP port, το οποίο χρησιμοποιείται για να προσδιορίσει τη ροή δεδομένων στους δρομολογητές που έχουνε διαμορφωθεί να υποστηρίζουν το RSVP πρωτόκολλο (RSVP-enabled routers).
   - Το αντικείμενο «sender Tspec» (Traffic specification, προδιαγραφή κίνησης), το οποίο χαρακτηρίζει τη ροή δεδομένων για την οποία ζητείται μια δέσμευση. Αυτό μεταφράζεται χαρακτηριστικά σε ένα μοντέλο κουβά κουπονιών (token bucket) που ορίζει ένα ρυθμό δεδομένων και ένα μέγεθος ριπής (ή μέγεθος κουβά).
   - Το αντικείμενο «P Hop» (Previous Hop, Προηγούμενο Άλμα), το οποίο περιέχει την IP διεύθυνση της διεπαφής του router που επεξεργάστηκε τελευταία το PATH μήνυμα. Σε αυτό το παράδειγμα, «P Hop» τέθηκε αρχικά ο 10.10.10.10 από τη Συσκευή 1.

2. Μέσω της επιλογής "router alert", το Path μήνυμα αναχαιτίζεται από τη CPU του RSVP-aware router (10.20.20.20), ο οποίος το στέλνει στη RSVP διαδικασία. Το RSVP δημιουργεί ένα path state (κατάσταση διαδρομής) για αυτή τη ροή δεδομένων που αποθηκεύει τις τιμές της συνόδου του αποστολέα Tspec, και των αντικειμένων P Hop που περιλαμβάνονται στο μήνυμα Path. Στη συνέχεια διαβιβάζει το μήνυμα προς τα κάτω, αφού έχει αντικαταστήσει την «P Hop» αξία με τη διεύθυνση IP της εξερχόμενης διεπαφής του (10.20.20.20).
3. Ομοίως, το Path μήνυμα αναχαιτίζεται από την CPU του ακόλουθου RSVP-aware router, που προσδιορίζεται στο σχήμα ως 10.30.30.30. Αφού δημιουργήσει το path state και αλλάξει την «P Hop» αξία σε 10.30.30.30, ο router διαβιβάζει το μήνυμα προς τα κάτω.
4. Το Path μήνυμα φθάνει τώρα στο RSVP-unaware router που προσδιορίζεται στο σχήμα ως 10.40.40.40. Επειδή το RSVP δεν είναι ενεργοποιημένο σε αυτόν τον router, καθοδηγεί ακριβώς αυτό το μήνυμα σύμφωνα με τα υπάρχοντα πρωτόκολλα δρομολόγησης όπως οποιοδήποτε άλλο πακέτο IP, χωρίς οποιαδήποτε πρόσθετη επεξεργασία και χωρίς καμία αλλαγή στο περιεχόμενο των μηνυμάτων.
5. Επομένως, το Path message φτάνει στο RSVP-aware router που προσδιορίζεται ως 10.50.50.50, ο οποίος επεξεργάζεται το μήνυμα, δημιουργεί το αντίστοιχο path state, και διαβιβάζει το μήνυμα προς τα κάτω. Πρέπει να επισημανθεί ότι το «P Hop» που καταγράφεται από αυτόν τον router περιέχει ακόμα την IP διεύθυνση του τελευταίου RSVP-aware router κατά μήκος του network path δηλαδή την 10.30.30.30.
6. Ο RSVP δέκτης στη Συσκευή 2 λαμβάνει το Path message με «P Hop» τιμή την 10.50.50.50 και μπορεί τώρα να αρχίσει την πραγματική διαφύλαξη με τη δημιουργία ενός μηνύματος αποκαλούμενου Resv. Για αυτόν τον λόγο, το RSVP είναι γνωστό ως receiver-initiated protocol. Το μήνυμα Resv φέρνει το αίτημα διαφύλαξης τμήμα προς, τμήμα (hop-by-hop) από το δέκτη στον αποστολέα κατά μήκος της αντίστροφης πορειας της ροής δεδομένων για τη σύνοδο. Σε κάθε hop η διεύθυνση προορισμού IP του μηνύματος Resv είναι η διεύθυνση IP του προηγούμενου hop κόμβου που λαμβάνεται από το path state. Ως εκ τούτου, σε αυτήν την περίπτωση η Συσκευή 2 στέλνει το μήνυμα Resv με IP διεύθυνση προορισμού την 10.50.50.50. Το μήνυμα Resv περιέχει, μεταξύ άλλων, τα ακόλουθα αντικείμενα:
   - Το αντικείμενο «session» (συνόδου), το οποίο χρησιμοποιείται για να προσδιορίσει τη ροή δεδομένων.
   - Το αντικείμενο "N Hop" (Next Hop-Επόμενο Άλμα) το οποίο περιέχει τη διεύθυνση IP του κόμβου που παρήγαγε το μήνυμα. Σε αυτό το παράδειγμα, «N Hop» ορίστηκε αρχικά η IP 10.60.60.60 από τη Συσκευή 2.
7. Όταν ο RSVP-aware router 10.50.50.50 λαμβάνει το μήνυμα Resv για αυτή τη ροή δεδομένων, το συγκρίνει με τις πληροφορίες του path state χρησιμοποιώντας το λαμβανόμενο αντικείμενο συνόδου και ελέγχει εάν το αίτημα δέσμευσης μπορεί να γίνει αποδεκτό βάσει των ακόλουθων κριτηρίων:
   - *Έλεγχος πολιτικής*: Επιτρέπεται αυτός ο χρήστης ή/και η εφαρμογή να κάνει αυτό το αίτημα διαφύλαξης;
   - *Έλεγχος αποδοχής*: Υπάρχουν αρκετοί πόροι (bandwidth) διαθέσιμοι στη σχετική εξερχόμενη διεπαφή για να προσαρμόσουν αυτό το αίτημα δέσμευσης;
8. Σε αυτήν την περίπτωση, γίνεται η υπόθεση ότι και η πολιτική και ο έλεγχος αποδοχής είναι επιτυχείς στο 10.50.50.50, που σημαίνει ότι το bandwidth που παρέχεται από το Tspec στο path state για αυτή τη σύνοδο είναι δεσμευμένο στην εξερχόμενη διεπαφή (στην ίδια κατεύθυνση με τη ροή δεδομένων, η οποία είναι από τη συσκευή 1 στη συσκευή 2) και ένα αντίστοιχο «reservation state» δημιουργείται. Τώρα ο router 10.50.50.50 μπορεί να στείλει ένα μήνυμα δέσμευσης (Resv) στη IP διεύθυνση προορισμού η οποία είναι αποθηκευμένη στο «P Hop», όπου για αυτή τη σύνοδο είναι η 10.30.30.30. Το αντικείμενο «N Hop» ενημερώνεται επίσης με την αξία του 10.50.50.50.

9. Το μήνυμα Resv διέρχεται τώρα μέσω του 10.40.40.40 RSVP-unaware router και ο οποίος το καθοδηγεί προς τον προορισμό 10.30.30.30 όπως οποιοδήποτε άλλο IP πακέτο. Αυτός ο μηχανισμός επιτρέπει την ενεργοποίηση του RSVP signaling και μέσω ενός ετερογενούς δικτύου όπου μερικοί κόμβοι δεν υποστηρίζουν το RSVP.
10. Ο RSVP-aware router που προσδιορίζεται ως 10.30.30.30 λαμβάνει το μήνυμα Resv και το επεξεργάζεται σύμφωνα με τους μηχανισμούς που περιγράφονται στα βήματα 7 και 8. Υποθέτοντας ότι η πολιτική και ο έλεγχος αποδοχής είναι επιτυχείς και σε αυτό το hop, το bandwidth δεσμεύεται στην εξερχόμενη διεπαφή και ένα Resv μήνυμα στέλνεται στο προηγούμενο Hop (10.20.20.20).
11. Μετά από μια παρόμοια διαδικασία μέσα στο router που προσδιορίζεται ως 10.20.20.20, το Resv φθάνει τελικά στο RSVP αποστολέα, Συσκευή 1. Αυτό δείχνει στην αιτούμενη εφαρμογή ότι μια συνολική δέσμευση έχει καθιδρυθεί και ότι το bandwidth έχει τεθεί κατά μέρος για αυτήν την ροή δεδομένων σε όλους τους RSVP-routers του δικτύου.

Αυτό το παράδειγμα περιγράφει πώς τα δύο κύρια RSVP μηνύματα σηματοδοσίας, Path και Resv, υπάρχουν μέσα στο δίκτυο για να καθιερώσουν τις δεσμεύσεις. Επιπλέον, καθορίζονται διάφορα άλλα μηνύματα στο πρότυπο RSVP με σκοπό να εξετάσουν τις καταστάσεις λάθους, τις αποτυχίες δέσμευσης και την απελευθέρωση των πόρων. Συγκεκριμένα το μήνυμα ResvErr χρησιμοποιείται κατά την αποτυχία των σημάτων να δεσμεύσουν τους απαιτούμενους πόρους λόγω είτε του ελέγχου πολιτικής είτε του ελέγχου αποδοχής κάπου κατά μήκος του δικτύου. Εάν π.χ., στο παραπάνω σχήμα ο έλεγχος αποδοχής είχε αποτύχει στον κόμβο 10.50.50.50, αυτός ο κόμβος θα είχε στείλει ένα μήνυμα ResvErr πίσω στη Συσκευή 2, διευκρινίζοντας την αιτία της αποτυχίας και ενημερώνοντας την εφαρμογή.

Μια άλλη σημαντική πτυχή του πρωτοκόλλου RSVP είναι ότι υιοθετεί μια soft-state προσέγγιση, που σημαίνει ότι για κάθε σύνοδο τόσο το path state όσο και το reservation state κατά μήκος του δικτύου πρέπει να ανανεώνεται περιοδικά μέσω της εφαρμογής αποστέλλοντας πανομοιότυπα Path και Resv μηνύματα. Εάν ένας router δε λαμβάνει μηνύματα ανανέωσης για μια δεδομένη σύνοδο για μια ορισμένη χρονική περίοδο, διαγράφει την αντίστοιχη κατάσταση και απελευθερώνει τους πόρους που είχαν δεσμευθεί. Αυτό επιτρέπει στο RSVP να αντιδρά δυναμικά στις αλλαγές της τοπολογίας ενός δικτύου ή τις αλλαγές δρομολόγησης λόγω των αποτυχιών στις δεσμεύσεις. Οι δεσμεύσεις αρχίζουν απλά με τις νέες διαδρομές που καθορίζονται από το πρωτόκολλο δρομολόγησης και κατά συνέπεια οι δεσμεύσεις των παλαιών διαδρομών σταματούν και τελικά διαγράφονται.

3.3.6 RSVP και QoS σε Δρομολογητές ενός WAN

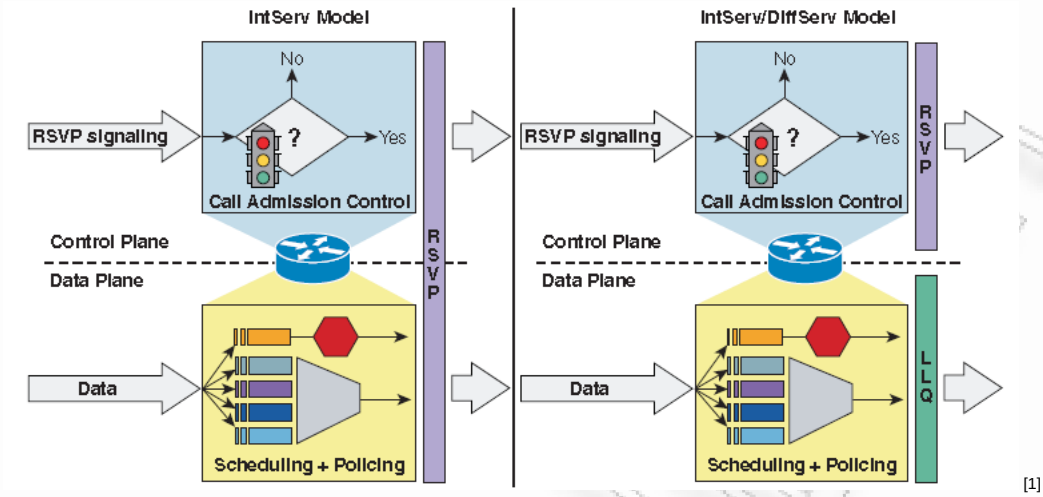
Το Πρωτόκολλο Δέσμευσης Πόρων (RSVP) υποστηρίζεται από τους Cisco δρομολογητές εδώ και πολλά χρόνια. Η ενεργοποίηση του σε ένα δρομολογητή και ο καθορισμός του μέγιστου ποσού εύρους ζώνης που μπορεί να ελέγξει επιτυγχάνεται με την ακόλουθη εντολή:

ip rsvp bandwidth [*interface-kbps*] [*single-flow-kbps*]

Όπου η παράμετρος *interface-kbps* καθορίζει το ανώτατο όριο του εύρους ζώνης που το RSVP μπορεί να δεσμεύσει στη δεδομένη διεπαφή, ενώ η παράμετρος *single-flow-kbps* καθορίζει το ανώτατο όριο εύρους ζώνης για κάθε μεμονωμένη δέσμευση (έτσι ώστε να απορρίπτονται οι ροές που απαιτούν να δεσμεύσουν υψηλότερο ποσό εύρους ζώνης ακόμα και αν αυτό υπάρχει διαθέσιμο).

Στους Cisco δρομολογητές, το RSVP μπορεί να λειτουργήσει με βάση τα δυο ακόλουθα διαφορετικά μοντέλα: το Integrated Services (IntServ) μοντέλο που περιγράφεται από το RFC 2210 και το Integrated Services/Differentiated Services (IntServ/DiffServ) μοντέλο, που περιγράφεται απο το RFC 2998. Στη συνέχεια παρουσιάζονται σχηματικά τα δυο μοντέλα:

Εικόνα 3-15: IntServ και IntServ/DiffServ Μοντέλα



[1]

3.3.7 Το IntServ Μοντέλο

Όπως παρουσιάζεται στην αριστερή πλευρά του παραπάνω σχήματος, το RSVP στο πρότυπο IntServ περιλαμβάνει και το Πλάνο Ελέγχου (Control Plane) και το Πλάνο Δεδομένων (Data Plane). Στο πλάνο ελέγχου, το RSVP αποδέχεται ή απορρίπτει το αίτημα δέσμευσης. Το πλάνο δεδομένων, ταξινομεί τα πακέτα ανάλογα με την περιγραφή της κίνησης που περιλαμβάνεται στα μηνύματα RSVP και τα τοποθετεί στην κατάλληλη ουρά αναμονής.

Η ταξινόμηση που εκτελεί το RSVP είναι βασισμένη στο 5-πλειαδικό που αποτελείται από την IP διεύθυνση πηγής, από το port της πηγής, την IP διεύθυνση προορισμού, το port προορισμού και τον αριθμό πρωτοκόλλου. Σε αυτό το μοντέλο, όλα τα πακέτα δεδομένων που διέρχονται μέσω του router πρέπει να φιλτραριστούν από το RSVP έτσι ώστε αυτό να ελέγξει το 5-πλειαδικό και να ψάξει μια αντιστοιχία μεταξύ των καθιερωμένων δεσμεύσεων. Εάν βρεθεί μια αντιστοιχία, τα πακέτα ελέγχονται και προγραμματίζονται από το RSVP με βάση τα χαρακτηριστικά της δεσμευμένης κίνησης.

Όπως φαίνεται στο επόμενο σχήμα, όταν συνδυάζεται το πρότυπο IntServ με τη Low Latency Queuing (LLQ), το διαθέσιμο προς χρήση εύρος ζώνης διαιρείται μεταξύ του RSVP και των προκαθορισμένων LLQ ουρών αναμονής. Το RSVP ελέγχει τα κριτήρια εισόδου στο δεσμευμένο RSVP εύρος ζώνης, ενώ οι χάρτες πολιτικής (policy maps) ελέγχουν τα κριτήρια εισόδου για τις προκαθορισμένες ουρές αναμονής.

Για να εφαρμοστεί το πρότυπο λειτουργίας IntServ σε έναν Cisco router, απαιτείται στη διεπαφή η χρήση των ακόλουθων εντολών διαμόρφωσης:

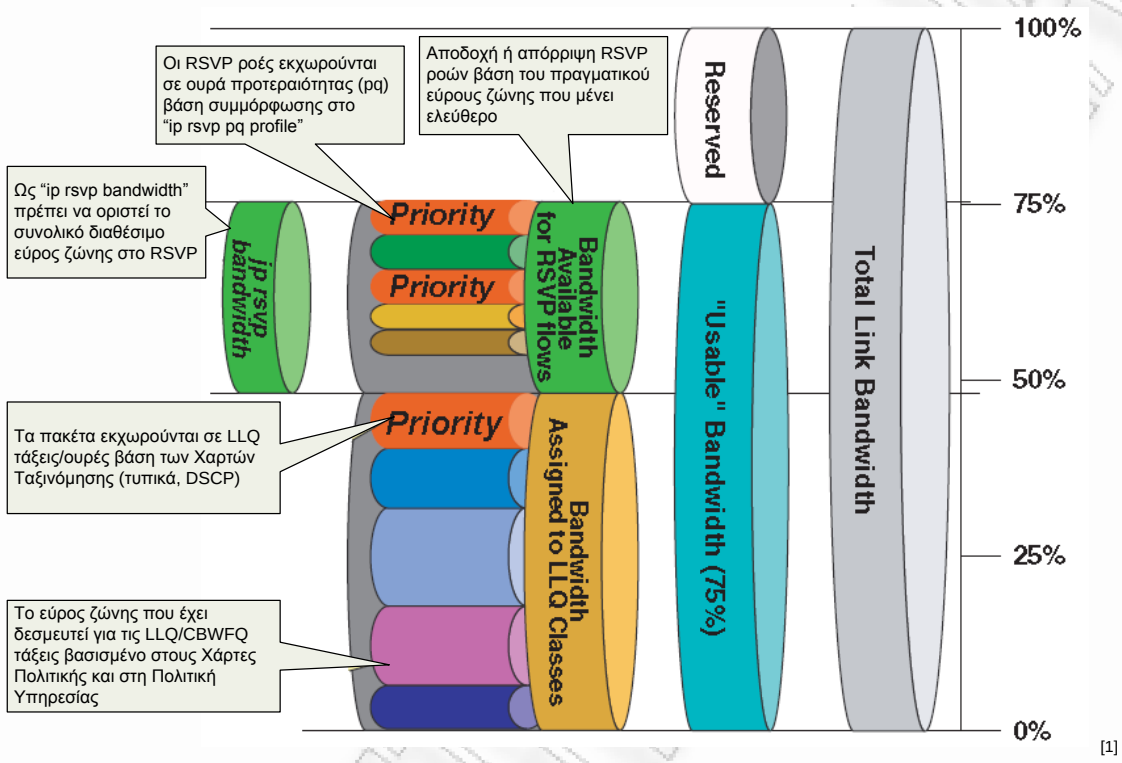
ip rsvp resource-provider wfq [interface]

no ip rsvp data-packet classification

Όταν αυτές οι εντολές είναι ενεργές, το RSVP αναγνωρίζει ή απορρίπτει τις νέες δεσμεύσεις όχι μόνο με βάση το ανώτερο όριο του εύρους ζώνης που καθορίζεται μέσα από την εντολή ***ip rsvp bandwidth***, αλλά με βάση τους πραγματικά διαθέσιμους πόρους. Παραδείγματος χάριν, εάν υπάρχουν τάξεις LLQ με δηλωμένο εύρος ζώνης, αυτό το ποσό αφαιρείται από το εύρος ζώνης που μπορεί να διατεθεί στις RSVP δεσμεύσεις. Ενώ οι LLQ τάξεις μοιράζουν στατικά το εύρος ζώνης στον παραμετροποιημένο χρόνο, το RSVP δε διαθέτει οποιοδήποτε ποσό έως ότου λάβει ένα αίτημα δέσμευσης. Επομένως, είναι σημαντικό να εξασφαλιστεί ότι ένα κατάλληλο ποσοστό του διαθέσιμου εύρους ζώνης στη διεπαφή δεν διατίθεται στις LLQ τάξεις, έτσι ώστε να μείνει ελεύθερο προς χρήση από το RSVP όταν ληφθούν οι αιτήσεις δεσμεύσεις.

Επειδή το συνολικό μέγιστο εύρος ζώνης που μπορεί να οριστεί στους μηχανισμούς QoS για μια ζεύξη είναι ίσο με το 75% της ταχύτητας ζεύξης, εάν απαιτηθεί διατήρηση του 33% του εύρους ζώνης μιας ζεύξης για τις RSVP εκχωρημένες ροές, θα πρέπει να καθοριστεί ότι το διαθέσιμο εύρος ζώνης για τις LLQ Τάξεις δε θα υπερβαίνει το (75 - 33) = 42% του συνολικού.

Εικόνα 3-16: Συνδυασμός IntServ Μοντέλου με LLQ



[1]

Επιπλέον είναι δυνατό να καθοριστεί ένας μηχανισμός για το RSVP που να το καθοδήγεί αν πρέπει ή όχι να τοποθετηθούν οι ροές στην ουρά προτεραιότητας (PQ). Αυτό επιτυγχάνεται με τη χρησιμοποίηση της ακόλουθης εντολής:

ip rsvp pq-profile [*r* [*b* [*p-to-r*]]]

Το RSVP χρησιμοποιεί τις παραμέτρους r, b, και p-to-r για να καθορίσει εάν η ροή που χρησιμοποιείται είναι μια ροή φωνής που χρειάζεται μεταχείριση ουράς προτεραιότητας (PQ). Αυτές οι παράμετροι αντιπροσωπεύουν:

- *r* = το μέσο ρυθμό κίνησης σε bytes ανά δευτερόλεπτο
- *b* = τη μέγιστη ριπή μιας ροής σε bytes
- *p-to-r* = το λόγο του μέγιστου ρυθμού προς το μέσο ρυθμό, που εκφράζεται ως ποσοστό.

Εάν οι παραπάνω τιμές κίνησης (οι οποίες καθορίζονται από τα μηνύματα RSVP) για μια συγκεκριμένη ροή, είναι μικρότερες ή ίσες προς τις αντίστοιχες παραμέτρους που έχουν εκχωρηθεί στην εντολή, τότε το RSVP θα κατευθύνει τη ροή στην ουρά προτεραιότητας (PQ). Στην περίπτωση που καμία παράμετρος δεν έχει καθοριστεί, οι ακόλουθες προεπιλεγμένες τιμές αντιπροσωπεύουν την πλειοψηφία του συνήθως χρησιμοποιούμενου codec φωνής (G.711):

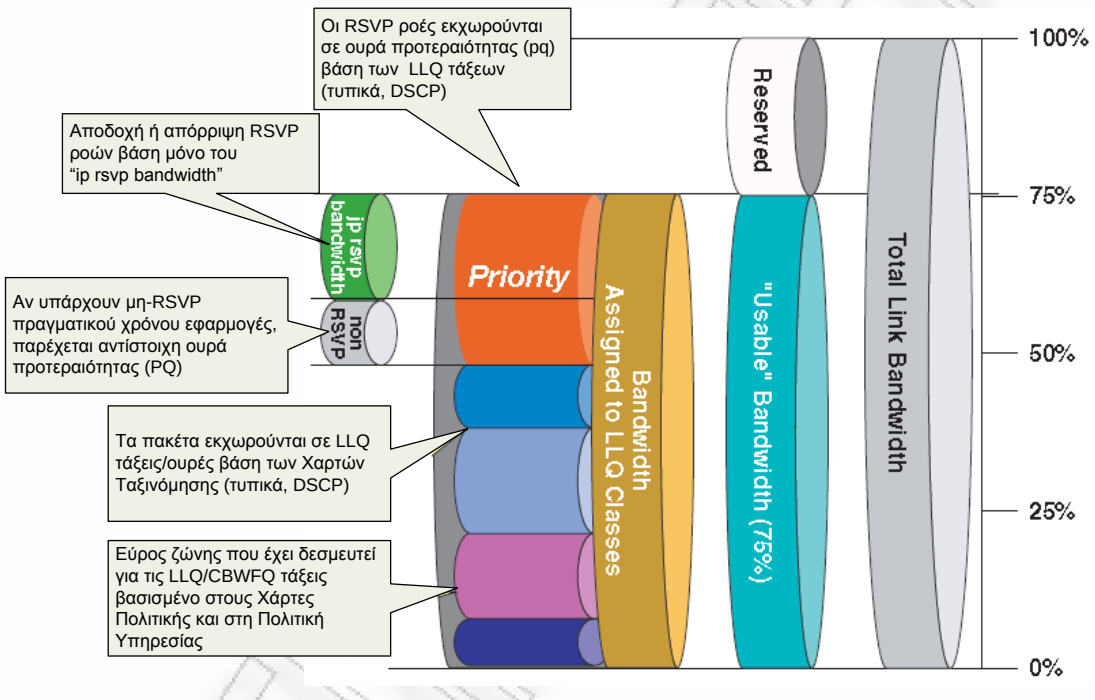
- *r* = 12288 bytes ανά δευτερόλεπτο
- *b* = 592 bytes
- *p-to-r* = 110%

3.3.8 Το IntServ/DiffServ Μοντέλο

Όπως παρουσιάζεται στη δεξιά πλευρά του σχήματος, το RSVP στο πρότυπο IntServ/DiffServ περιλαμβάνει μόνο το πλάνο ελέγχου. Αυτό σημαίνει ότι η λειτουργία ελέγχου αποδοχής κλήσεων (Call Admission Control) είναι ξεχωριστή από τις λειτουργίες χρονοπρογραμματισμού (scheduling) και αστυνόμευσης (policing). Για τις λειτουργίες αυτές υπεύθυνος είναι ο αλγόριθμος LLQ που βασίζεται στους προκαθορισμένους χάρτες τάξης, χάρτες πολιτικής και την πολιτική υπηρεσίας.

Συνεπώς με το IntServ/DiffServ μοντέλο, είναι δυνατό να προστεθεί ο RSVP έλεγχος αποδοχής κλήσεων σε ένα δίκτυο που χρησιμοποιεί ήδη μια διαφοροποιημένη QoS προσέγγιση υπηρεσιών. Το RSVP δέχεται ή απορρίπτει τις κλήσεις βάσει ενός προκαθορισμένου ποσού εύρους ζώνης, αλλά ο πραγματικός σχεδιασμός είναι βασισμένος στα προϋπάρχοντα LLQ κριτήρια όπως η DSCP τιμή κάθε πακέτου.

Εικόνα 3-17: Καταμερισμός LLQ Εύρους Ζώνης με RSVP



[1]

Όπως φαίνεται στο παραπάνω σχήμα, ολόκληρο το διαθέσιμο εύρος ζώνης (75% της ταχύτητας ζεύξης) μπορεί να εκχωρηθεί στις LLQ τάξεις. Οι χάρτες πολιτικής καθορίζουν την κίνηση που εκχωρείται σε κάθε ουρά αναμονής. Το RSVP διαμορφώνεται ώστε να αποδέχεται ροές με μέγιστο εύρος ζώνης ίσο με αυτό που έχει καθοριστεί για την κίνηση προτεραιότητας. Πρέπει όμως να ληφθεί υπόψη ότι το RSVP σε αυτό το πρότυπο δε ρυθμίζει το χρονοπρογραμματισμό, συνεπώς οποιαδήποτε αποδεκτή από το RSVP κίνηση, η οποία ξεπερνά την προκαθορισμένη ουρά προτεραιότητας (PQ), μπορεί να απορριφθεί ή και να επαναπροσδιοριστεί ώστε να εξυπηρετηθεί από άλλη ουρά χαμηλότερης προτεραιότητας.

Αν όλες οι εφαρμογές που στέλνουν κίνηση προτεραιότητας είναι RSVP-enabled, τότε μπορεί να παραμετροποιηθεί το RSVP εύρος ζώνης, ώστε να αντιστοιχηθεί με το μέγεθος της ουράς προτεραιότητας. Εάν αντιθέτως υπάρχουν εφαρμογές μη-RSVP που πρέπει επίσης να στείλουν κίνηση προτεραιότητας (όπως ο Cisco Unified CallManager ή ένας gatekeeper), τότε όπως φαίνεται και στο σχήμα, η ουρά προτεραιότητας διαιρείται σε κίνηση προτεραιότητας που ελέγχεται από τους μη-RSVP μηχανισμούς και κίνηση προτεραιότητας που ελέγχεται από το RSVP. Οι συνδυασμένοι μηχανισμοί ελέγχου αποδοχής μη-RSVP και RSVP δεν πρέπει να χρησιμοποιήσουν περισσότερο εύρος ζώνης από το διατιθέμενο, ώστε να εξασφαλιστεί ότι η ουρά προτεραιότητας δε θα υπερφορτωθεί ποτέ.

Για χρήση του πρότυπου λειτουργίας IntServ/DiffServ σε έναν router της Cisco, απαιτείται να εφαρμοστούν στη διεπαφή οι ακόλουθες εντολές:

ip rsvp resource-provider none

ip rsvp data-packet classification none

Μετά την εφαρμογή των εντολών, το RSVP δέχεται ή απορρίπτει τις νέες δεσμεύσεις μόνο με βάση του άνω ορίου του καθορισμένου εύρους ζώνης (με την εντολή **ip rsvp bandwidth**) και ανεξάρτητα από τους πραγματικά διαθέσιμους πόρους στη διεπαφή. Μόλις γίνουν αποδεκτές οι RSVP ροές υπόκεινται στους ίδιους κανόνες σχεδιασμού όπως όλη η άλλη μη-RSVP κίνηση (π.χ. κλάση LLQ και χάρτες πολιτικής). Επομένως, είναι σημαντικό να εξασφαλιστεί ότι η RSVP-enabled κίνηση είναι χαρακτηρισμένη με την κατάλληλη DSCP τιμή και ότι το εύρος ζώνης των ουρών PQ ή CBWFQ αντιστοίχως είναι αρκετό για να προσαρμόσει και τη RSVP-enabled κίνηση αλλά και όλη την άλλη κίνηση.

Σε αυτό το λειτουργικό πρότυπο, η εντολή **ip rsvp pq-profile** είναι ανενεργή επειδή το RSVP δεν ελέγχει τη λειτουργία χρονοπρογραμματισμού.

Σήμερα γίνεται χρήση του IntServ/DiffServ μοντέλου αλλά κάτω από συγκεκριμένες συνθήκες και με μεγάλη προσοχή κατά την εφαρμογή του:

1. Η Cisco προτείνει τη χρήση του μοντέλου IntServ/DiffServ εάν καθεμία των ακόλουθων δηλώσεων είναι αληθινή:
   - Η μόνη κίνηση που προορίζεται για την Ουρά Προτεραιότητας (PQ) στις διεπαφές να είναι RSVP-enabled κίνηση.
   - Όλη η μη-RSVP κίνηση που προορίζεται για την PQ μπορεί να περιοριστεί σε ένα συγκεκριμένο ποσό από έναν εκτός ζώνης CAC μηχανισμό (όπως ο Cisco Unified CallManager ή ένας gatekeeper).
2. Εάν όλη η κίνηση προτεραιότητας είναι RSVP-enabled, η τιμή που ορίζεται στην εντολή **ip rsvp bandwidth** και την εντολή **priority** πρέπει να ταιριάξει μόλις ληφθούν υπόψη και οι Layer 2 επιβαρύνσεις.
3. Αν το RSVP είναι ενεργοποιημένο σε μια ή περισσότερες διεπαφές ενός router, πρέπει επίσης να ενεργοποιηθεί σε όλες τις διεπαφές μέσω των οποίων αναμένεται RSVP signaling ώστε να εξασφαλιστεί ότι τα RSVP μηνύματα δε θα διακοπούν.
4. Απαιτείται η ενεργοποίηση του RSVP σε όλα τα πιθανά σημεία συμφόρησης του WAN, συμπεριλαμβανομένων των ζεύξεων διαφορετικής ταχύτητας.

3.4 Ποιότητα Υπηρεσίας στην Πράξη

3.4.1 Ταξινόμηση Πλαισίων και Πακέτων για Παροχή QoS

Όπως ήδη έχει γίνει κατανοητό, με τη χρήση μηχανισμών QoS μπορούμε να κατηγοριοποιούμε τη δικτυακή κίνηση για να παρέχουμε προνομιακή μεταχείριση σε συγκεκριμένους τύπους κίνησης εις βάρος φυσικά άλλων. Χωρίς τη χρήση μηχανισμών QoS, η δικτυακή συσκευή υπεύθυνη για την προώθηση των πακέτων, παρέχει την καλύτερη δυνατή εξυπηρέτηση ανεξάρτητα από τον τύπο και το μέγεθος των πακέτων. Τα πακέτα στέλνονται χωρίς καμία εγγύηση όσον αφορά την αξιοπιστία της αποστολής και το χρόνο άφιξης στον προορισμό. Συνεπώς, σε περιπτώσεις δικτυακής κίνησης πραγματικού χρόνου όπως της IP τηλεφωνίας, η χρήση QoS μηχανισμών κρίνεται επιβεβλημένη.

Τα δίκτυα λειτουργούν με τέτοιο τρόπο ώστε όλη η δικτυακή κίνηση να έχει την ίδια προτεραιότητα, με αποτέλεσμα σε περιπτώσεις συμφόρησης όλη η κίνηση να έχει ίσες πιθανότητες μη αποστολής προς τον παραλήπτη. Όταν ενεργοποιούμε μηχανισμούς QoS σε ένα δίκτυο, μπορούμε να επιλέξουμε συγκεκριμένο τύπο δικτυακής κίνησης, να του δώσουμε συγκεκριμένη προτεραιότητα με βάση την σπουδαιότητα του και να χρησιμοποιήσουμε

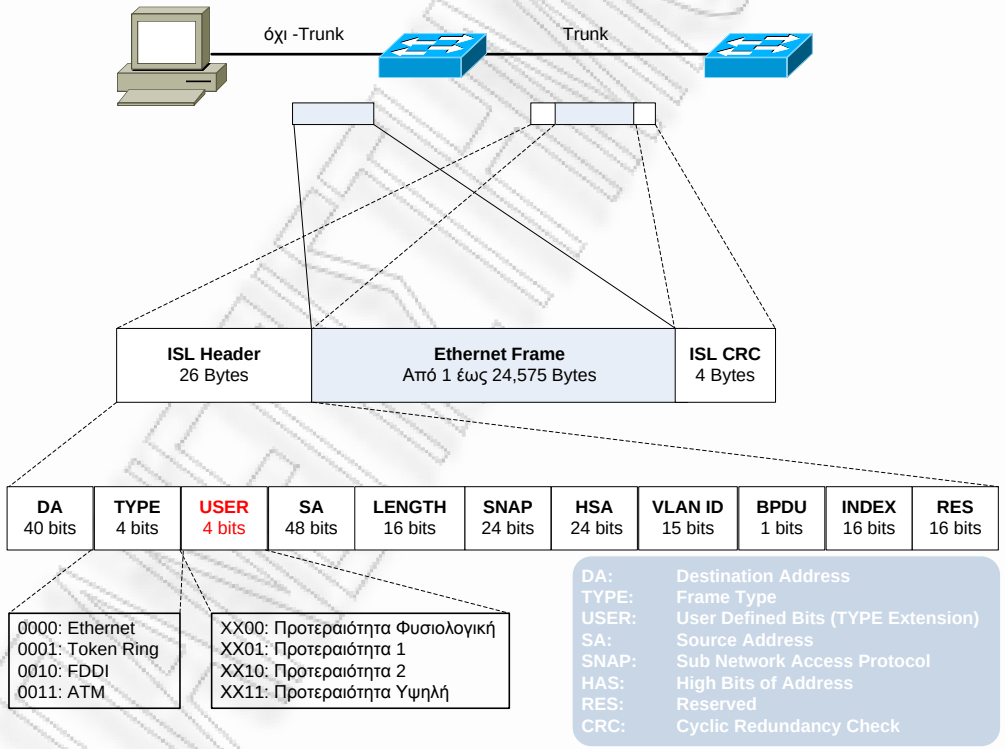
μηχανισμούς διαχείρισης και αποφυγής της συμφόρησης. Έτσι, παρέχοντας προνομιακή μεταχείριση σε συγκεκριμένους τύπους κίνησης κάνουμε τη ροή των δεδομένων προβλέψιμη και τη χρήση του εύρους ζώνης μιας γραμμής διασύνδεσης πιο αποδοτική.

Η εφαρμογή μηχανισμών QoS βασίζεται στην αρχιτεκτονική **DiffServ** (Differentiated Services, Διαφοροποιημένες Υπηρεσίες) ένα εξελισσόμενο πρότυπο της IETF. Η προσέγγιση αυτή είναι γνωστή και ως ποιότητα υπηρεσιών **βασισμένη σε τάξεις** (class-based), σε αντιδιαστολή με το πρότυπο Ολοκληρωμένων Υπηρεσιών (IntServ) που βασίζεται σε ροές (flow-based). Οι διαφοροποιημένες υπηρεσίες μπορούν να υλοποιηθούν τοπικά σε κάθε δρομολογητή, χωρίς να απαιτείται εκ των προτέρων διευθέτηση και χωρίς να εμπλέκεται ολόκληρη η διαδρομή. Κατά συνέπεια για την υλοποίηση και εφαρμογή DS πρέπει να οριστεί ένα σύνολο τάξεων υπηρεσιών (κατηγοριοποίηση) με αντίστοιχους κανόνες προώθησης.

Στην πράξη η κατηγοριοποίηση «μεταφέρεται» στην κεφαλίδα ενός IP πακέτου, χρησιμοποιώντας 6 bits από το πεδίο ToS Layer-3, ή μπορεί να εμπεριέχεται σε ένα πλαίσιο Layer-2:

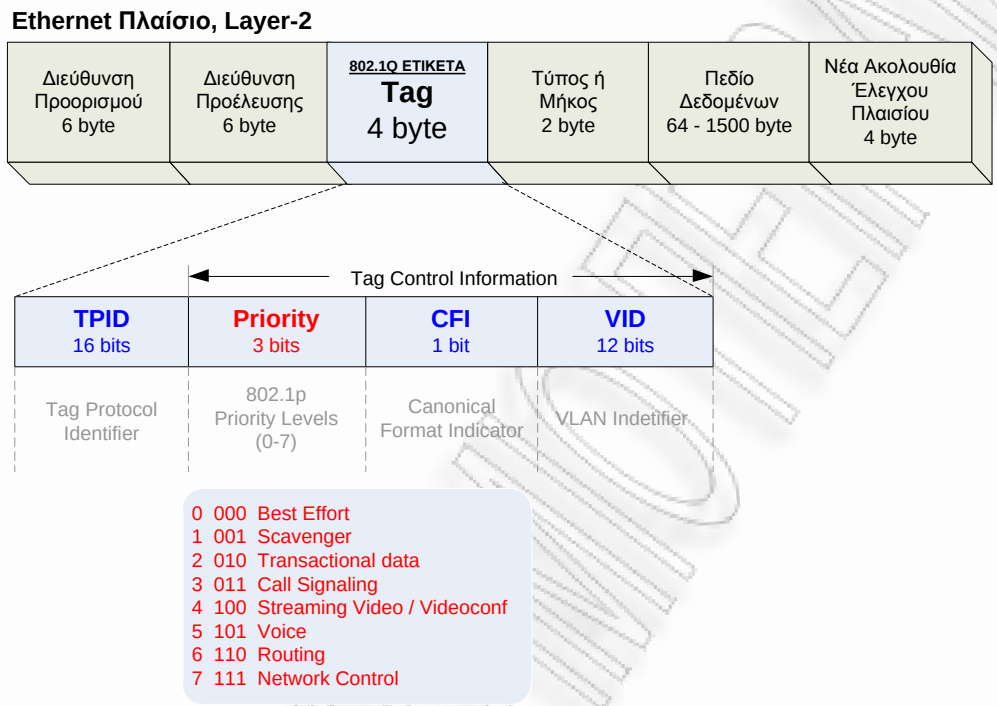
- Η κατηγοριοποίηση σε πλαίσια Layer-2, επιτυγχάνεται μόνο στις παρακάτω περιπτώσεις:
  - Σε κεφαλίδες ISL (Inter Switch Link) που έχουν ένα 1-byte πεδίο χρήστη (User) το οποίο μπορεί να μεταφέρει την Class of Service (CoS) πληροφορία στα 2 τελευταία bits του πεδίου. Τονίζεται ότι σε θύρες που έχουν προγραμματιστεί ως Layer 2 ISL trunks, όλη η κίνηση είναι ενθυλακωμένη σε ISL πλαίσια. Όσα αναφέρθησαν παρουσιάζονται σχηματικά στη συνέχεια:

Εικόνα 3-18: Layer-2 Ταξινόμηση ISL Πλαισίων για Παροχή QoS



— Σε κεφαλίδες 802.1Q που έχουν ένα πεδίο 2-byte το οποίο ονομάζεται Tag Control Information και μεταφέρει τη βαθμίδα του CoS. Με τα 3 bits του πεδίου Priority ορίζονται επτά (7) επίπεδα προτεραιότητας. Τονίζεται ότι σε θύρες που έχουν προγραμματιστεί ως Layer 2 802.1Q trunks όλη η κίνηση είναι ενθυλακωμένη σε 802.1Q πλαίσια. Όσα αναφέρθησαν παρουσιάζονται σχηματικά στη συνέχεια:

Εικόνα 3-19: Layer-2 Ταξινόμηση 802.1Q Πλαισίων για Παροχή QoS

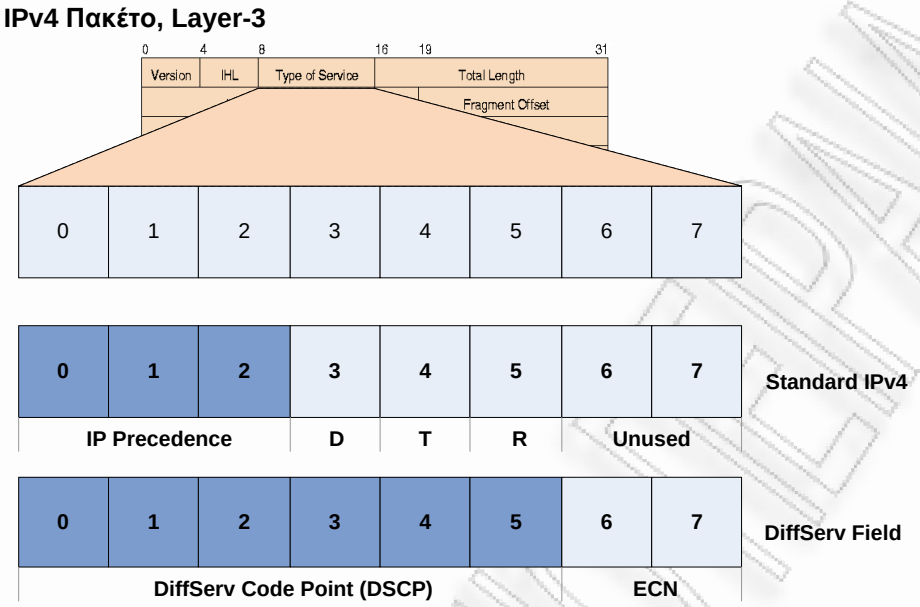


Πρέπει να σημειωθεί ότι η κατηγοριοποίηση με βάση το IEEE 802.1Q πρότυπο είναι ευρέως διαδεδομένη διότι υποστηρίζεται από όλους τους κατασκευαστές Layer 2 συσκευών, σε αντίθεση με την ISL που υποστηρίζεται από ένα μέρος κατασκευαστών.

- Η κατηγοριοποίηση σε πακέτα Layer-3 επιτυγχάνεται στις παρακάτω περιπτώσεις:
  - — Τα πακέτα Layer-3 μπορούν να μεταφέρουν την κατηγοριοποίηση μέσω της τιμής του IP precedence ή
  - — Μέσω της τιμής του DSCP (Differentiated Services Code Point).

    Η τιμή του IP Precedence μπορεί να διαφοροποιείται μεταξύ των τιμών 0 και 7, ενώ η τιμή του DSCP μεταξύ 0 και 63.

Εικόνα 3-20: Layer-3 Ταξινόμηση Πακέτων για Παροχή QoS



Όπως διακρίνεται και στο παραπάνω σχήμα, στο Standard IPv4 η κατηγοριοποίηση των πακέτων μεταφέρεται μέσω της τιμής IP Precedence δηλαδή μέσω των 3 σημαντικότερων bits (bits:0-2). Ενώ τα bits 3, 4 και 5 προσδιορίζουν: Delay (Καθυστέρηση), Throughput (Διεκπεραιωτικότητα) και Reliability (Αξιοπιστία) αντίστοιχα. Επίσης τα bits 6 και 7 δεν χρησιμοποιούνται.

Πίνακας 3-6: Τα 8 bits του ToS στο Standard IPv4

Bits 0-2:	IP Precedence	
Bit 3:	0=Normal Delay	1=Low Delay
Bit 4:	0=Normal Throughput	1=High Throughput
Bit 5:	0=Normal Reliability	1=High Reliability
Bits 6-7:	Δεσμευμένα για μελλοντική χρήση	

Αντίστοιχα όταν η κατηγοριοποίηση των πακέτων μεταφέρεται μέσω του DiffServ πεδίου απαιτούνται 6 bits (DSCP) και κατά συνέπεια δημιουργούνται 2^6 = 64 διαφορετικές τάξεις. Σε αυτή την περίπτωση τα δυο τελευταία bits δεν μένουν αχρησιμοποίητα όπως πριν αλλά τώρα χρησιμοποιούνται για την επιλογή ECN (Explicit Congestion Notification, Ρητή ειδοποίηση συμφόρησης), κατά την οποία ένας δρομολογητής δεν απορρίπτει το πακέτο αλλά το μαρκάρει υπονοώντας εμμέσως το επίπεδο συμφόρησης.

Πίνακας 3-7: Τα 8 bits του ToS στο DiffServ Πεδίο

Bits 0-5:	DSCP (Differentiated Services Code Point)
Bit :6-7	ECN (Explicit Congestion Notification)

Η προεπιλεγμένη DSCP τιμή είναι η 000 000, ενώ οι επιλεγμένες DSCP τάξεις έχουν τιμές που τα τρία τελευταία τους bits συμβαδίζουν με τα αντίστοιχα των IP Precedence τιμών. Κατά τη μετατροπή μιας IPP τιμής σε DSCP τιμή ταιριάζουν τα τρία σημαντικότερα bits. Με άλλα λόγια το IPP 101 (5) ταιριάζει με το DSCP **101 000**.

Όλες οι δικτυακές συσκευές οι οποίες συνδέονται με το Internet βασίζονται στην πληροφορία CoS ώστε να παρέχουν την ίδια υπηρεσία προώθησης σε πακέτα με την ίδια τάξη και διαφοροποιημένη υπηρεσία προώθησης σε πακέτα με διαφορετική τάξη. Τα σημεία προσδιορισμού της τάξεως ενός πακέτου είναι τα τερματικά ή οι μεταγωγείς ή οι δρομολογητές κατά μήκος μια διαδρομής και βασίζονται είτε σε κάποια πολιτική που ήδη εφαρμόζεται είτε με τον λεπτομερή έλεγχο του πακέτου σε αυτά τα σημεία είτε και με τα δύο. Ο λεπτομερής έλεγχος ενός πακέτου συνήθως πραγματοποιείται στις συσκευές που βρίσκονται στην άκρη ενός δικτύου. Οι διάφοροι δρομολογητές και μεταγωγείς κατά μήκος μιας διαδρομής χρησιμοποιούν επίσης την CoS πληροφορία ώστε να περιορίσουν το ποσοστό των πόρων που κατανέμονται για μια συγκεκριμένη κλάση.

Τι συμβαίνει όμως όταν τα πακέτα κινούνται ανάμεσα σε υποδίκτυα που ελέγχονται από διαφορετικούς φορείς και οι οποίοι δεν έρχονται σε συνεννόηση για την επιλογή των τάξεων υπηρεσιών;

Για το λόγο αυτό η IETF για συγκεκριμένες DSCP σημάνσεις, έχει καθορίσει ειδικές λέξεις κλειδιά που καλούνται **PHB** (**Per-Hop Behavior**, **Συμπεριφορά Ανά Άλμα**). Στην ουσία η IETF έχει καθορίσει τάξεις υπηρεσιών που να είναι ανεξάρτητες από το δίκτυο και αναλαμβάνουν την προώθηση κάθε πακέτου.

Η απλούστερη PHB τάξη είναι η **EF** (**Expedited Forwarding**, **Εσπευσμένη Προώθηση**). Η αντίστοιχη σήμανση για την EF τάξη έχει καθοριστεί η DSCP 46. Η λογική πίσω από την Εσπευσμένη Προώθηση είναι ότι υπάρχουν δυο τάξεις υπηρεσιών: η απλή και η εσπευσμένη. Στα εσπευσμένα πακέτα, όπως πακέτα φωνής, δίνεται προτεραιότητα και μπορούν να διασχίσουν το δίκτυο ανεμπόδιστα, σε αντίθεση με τα πακέτα της απλής τάξης που έρχονται σε δεύτερη μοίρα.

Μια δεύτερη μέθοδος διαχείρισης των τάξεων υπηρεσιών είναι η **AF** (**Assured Forwarding**, **Εξασφαλισμένη Προώθηση**). Στη συγκεκριμένη μέθοδο δημιουργούνται συνολικά 12 AFxy τάξεις και αυτό διότι ορίζονται x=4 τάξεις προτεραιότητας με τους αντίστοιχους πόρους, όπου για τα πακέτα κάθε μιας από τις 4 τάξεις υπάρχουν y=3 πιθανότητες απόρριψης σε περίπτωση συμφόρησης: Χαμηλή, Μεσαία και Υψηλή. Όλες οι AF τάξεις με τις αντίστοιχες DSCP τιμές παρουσιάζονται στον πίνακα που ακολουθεί:

Πίνακας 3-8: AF Τάξεις, Αντίστοιχες DSCP Τιμές

Απόρριψη	**Τάξη 1η**	**Τάξη 2η**	**Τάξη 3η**	**Τάξη 4η**
Χαμηλή	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Μεσαία	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Υψηλή	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

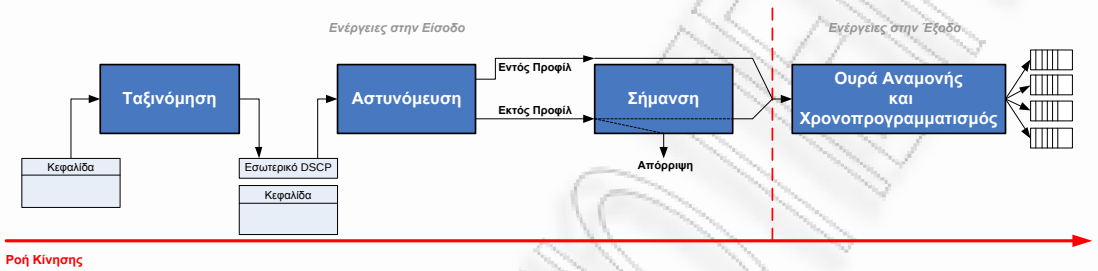
Δυο επιπλέον καθορισμένες PHB συμπεριφορές είναι η **BE** (**Best Effort**, **Βέλτιστη Προσπάθεια**), με αντίστοιχη DSCP τιμή την DSCP 0. Καθώς και η **CS** (**Class Selector**, **Επιλογέας Τάξης**). Στη συγκεκριμένη μέθοδο δημιουργούνται συνολικά 7 CSx τάξεις όπου το «x» αντιστοιχεί στις IP Precedence τιμές (1-7). Οι αντίστοιχες DSCP τιμές είναι οι: DSCP 8, 16, 24, 32, 40, 48 και 56.

3.4.2 Βασικό Μοντέλο Υλοποίησης QoS

Για την υλοποίηση QoS, κάθε μεταγωγέας πρέπει να ξεχωρίζει ένα πακέτο από τα άλλα, να απονέμει «ετικέτες» ώστε να καθορίζεται ο τύπος του QoS, να διασφαλίζει ότι τα πακέτα συμμορφώνονται με τυχόν πολιτικές χρήσης της γραμμής διασύνδεσης και να παρέχει διαφοροποιημένη μεταχείριση (ουρές και χρονοδιάγραμμα αποστολής) σε όλες τις περιπτώσεις όπου υφίσταται μεγάλος ανταγωνισμός για τη χρήση των πόρων του δικτύου.

Στην Εικόνα 3-21 απεικονίζεται το βασικό QoS μοντέλο. Οι ενέργειες που γίνονται στην θύρα εισόδου μιας δικτυακής συσκευής αφορούν την ταξινόμηση, την εφαρμογή ή όχι πολιτικής (αστυνόμευση), τη σήμανση του πακέτου, την τοποθέτηση σε ουρά και τέλος τον προγραμματισμό αποστολής.

Εικόνα 3-21: Βασικό Μοντέλο Υλοποίησης QoS



Δράσεις στην εισερχόμενη θύρα:

- Η ταξινόμηση ενός πακέτου και η τοποθέτησή του σε μια ξεχωριστή διαδρομή συνδέεται με την QoS ετικέτα. Ο μεταγωγέας διαβάζει την CoS ή την DSCP πληροφορία σε ένα πακέτο και τη συνδυάζει με τον ορισμό μιας ετικέτας QoS για να διαφοροποιήσει το ένα είδος κίνησης από ένα άλλο. Η QoS ετικέτα χρησιμοποιείται για την αναγνώριση όλων των μελλοντικά εισερχόμενων πακέτων και των ενεργειών που πρέπει να γίνουν σε πακέτα αυτού του τύπου.
- Η εφαρμογή ή όχι πολιτικής καθορίζει κατά πόσον ένα πακέτο ανήκει σε κάποια κατηγορία και ελέγχει το ρυθμό εισόδου/εξόδου. Ο μηχανισμός αυτός περιορίζει ή αυξάνει τον ρυθμό χρήσης μιας διεπαφής (interface).
- Η σήμανση χρησιμοποιεί τα στοιχεία από την εφαρμογή της πολιτικής και ενεργεί ανάλογα. Το πακέτο, εφόσον ανήκει σε κάποια πολιτική, προωθείται με/χωρίς αλλαγές σηματοδότησης ή απορρίπτεται.
- Ο μηχανισμός τοποθέτησης σε ουρά αποτιμά την ετικέτα QoS και τις τιμές DSCP και CoS ενός πακέτου για να επιλέξει σε ποια ουρά εισόδου θα το τοποθετήσει.
- Ο προγραμματισμός αποστολής βασίζεται σε μηχανισμούς όπως Shaped Round Robin (SRR) και Weighted Round Robin (WRR).

Δράσεις στην εξερχόμενη θύρα:

- Ο μηχανισμός τοποθέτησης σε ουρά αποτιμά την ετικέτα QoS και τις τιμές DSCP και CoS ενός πακέτου για να επιλέξει σε ποια ουρά εξόδου θα το τοποθετήσει.
- Ο προγραμματισμός αποστολής βασίζεται σε μηχανισμούς όπως Shaped Round Robin (SRR) και Weighted Round Robin (WRR).

3.4.3 Ταξινόμηση

Ταξινόμηση είναι η διαδικασία του διαχωρισμού ενός τύπου δικτυακής κίνησης από κάποιον άλλο ελέγχοντας τα πεδία μέσα στα πακέτα. Η ταξινόμηση ενεργοποιείται μόνο εφόσον έχει ενεργοποιηθεί πρώτα το QoS στη συσκευή. Εξ ορισμού το QoS είναι απενεργοποιημένο στις καινούργιες συσκευές οπότε δεν πραγματοποιείται ταξινόμηση πακέτων.

Κατά τη διάρκεια της ταξινόμησης, ο μεταγωγέας εξετάζει τα πακέτα και τους απονέμει μια QoS ετικέτα. Αυτή η ετικέτα αναγνωρίζει όλες τις ενέργειες που πρέπει να γίνουν στα συγκεκριμένα πακέτα και από ποια ουρά τα πακέτα αυτά έχουν αποσταλεί. Η τιμή της QoS ετικέτας καθορίζεται από τις τιμές DSCP και CoS που έχουν ήδη τα πακέτα. Κατόπιν ο μεταγωγέας αποφασίζει τις ενέργειες σχετικά με την ουρά στην οποία θα τοποθετηθούν και το χρονικό προσδιορισμό αποστολής (scheduling).

Ο διαχειριστής του μεταγωγέα μπορεί να καθορίσει ποια πεδία μέσα στο πακέτο θα χρησιμοποιεί για την ταξινόμηση του πακέτου.

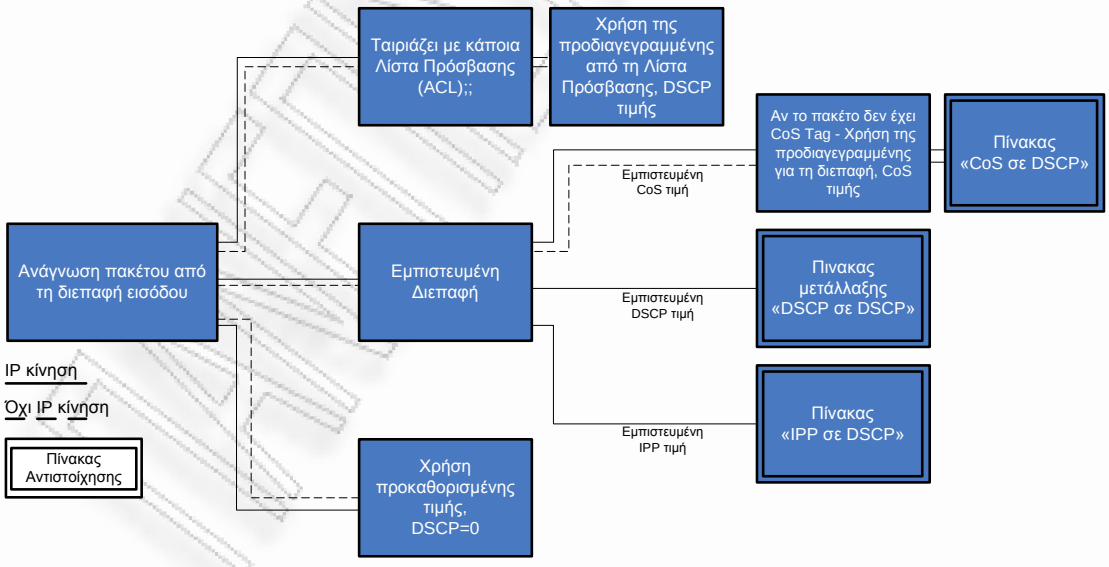
Για κίνηση, η οποία δεν αφορά IP πακέτα (Layer-2):

- Χρήση της τιμής DSCP στο εισερχόμενο πακέτο.
- Χρήση της τιμής DSCP ή της τιμής IP precedence του εισερχόμενου πακέτου.
- Γίνεται ταξινόμηση με βάση κάποια δηλωμένη MAC λίστα πρόσβασης Layer-2.

Για κίνηση, η οποία αφορά IP πακέτα (Layer-3):

- Χρήση της τιμής DSCP στο εισερχόμενο πακέτο.
- Χρήση της τιμής DSCP ή της τιμής IP precedence του εισερχόμενου πακέτου.
- Χρήση της τιμής CoS που φέρει το εισερχόμενο πακέτο.
- Γίνεται ταξινόμηση με βάση κάποια δηλωμένη IP λίστα πρόσβασης Layer-3.

Εικόνα 3-22: Ταξινόμηση



3.4.4 Ταξινόμηση Βασισμένη σε Λίστες Πρόσβασης (QoS ACLs)

Μπορούμε να χρησιμοποιήσουμε στάνταρ ή εκτεταμένες (extended) IP λίστες πρόσβασης ή λίστες πρόσβασης επιπέδου 2 (MAC) για να καθορίσουμε μία ομάδα από πακέτα με τα ίδια χαρακτηριστικά (τάξη). Σε περιεχόμενο που αφορά QoS οι εντολές permit (επιτρέπω) και deny (απαγορεύω) έχουν διαφορετική έννοια από τις κλασικές λίστες πρόσβασης επιπέδου ασφαλούς πρόσβασης (security ACLs).

- Αν υπάρχει αντιστοίχιση με εντολή permit, η προκαθορισμένη δράση για το QoS εφαρμόζεται.
- Αν υπάρχει αντιστοίχιση με εντολή deny, η τρέχουσα γραμμή ACL παρακάμπτεται και εξετάζεται η επόμενη γραμμή ACL.
- Αν δεν υπάρχει καμία αντιστοίχιση του πακέτου με κάποια εντολή permit στις τρέχουσες ACLs, καμία επεξεργασία QoS δεν γίνεται στο πακέτο και ο μεταγωγέας προωθεί το πακέτο στον καλύτερο δυνατό χρόνο.
- Αν πολλαπλές λίστες εφαρμόζονται σε κάποιο interface, η αναζήτηση σταματά στην πρώτη λίστα όπου γίνεται αντιστοίχιση της εντολής permit με το πακέτο και ξεκινά η επεξεργασία του QoS.

Εφόσον η τάξη της κίνησης έχει προσδιοριστεί με τις λίστες πρόσβασης, τότε έχουμε τη δυνατότητα να εφαρμόσουμε κάποια πολιτική. Μια πολιτική μπορεί να εμπεριέχει πολλαπλές κλάσεις στις οποίες εφαρμόζονται διαφορετικές δράσεις. Μία πολιτική μπορεί να περιέχει εντολές για κατηγοριοποίηση της κλάσης ως συγκεκριμένη ομάδα κίνησης ή για περιορισμό του εύρους ζώνης (bandwidth) που θα χρησιμοποιεί. Κατόπιν αυτή η πολιτική εφαρμόζεται σε κάποιο interface και ενεργοποιείται.

Η δημιουργία των λιστών πρόσβασης για την ταξινόμηση της IP κίνησης γίνεται χρησιμοποιώντας την εντολή **access-list**, ενώ για την κίνηση επιπέδου 2 (non-IP) χρησιμοποιούμε την εντολή **mac access-list extended**.

3.4.5 Ταξινόμηση Βασισμένη σε Χάρτες Ταξινόμησης και Χάρτες Πολιτικής

Ο χάρτης ταξινόμησης (class map) είναι ένας μηχανισμός που χρησιμοποιείται για να ονοματίσουμε μια συγκεκριμένη ροή κίνησης και να την απομονώσουμε από όλη την υπόλοιπη κίνηση. Ο χάρτης ταξινόμησης καθορίζει τα κριτήρια επιλογής κάποιας συγκεκριμένης κίνησης. Τα κριτήρια αυτά περιλαμβάνουν την ταύτιση με κάποια λίστα πρόσβασης ή την ταύτιση με κάποιες συγκεκριμένες λίστες τιμών DSCP ή IP precedence.

Ο χάρτης πολιτικής (policy map) καθορίζει σε ποια κλάση κίνησης θα δράσουμε. Οι δράσεις αυτές είναι:

- Χρήση και προώθηση των υπαρχουσών τιμών CoS, DSCP ή IP precedence.
- Εφαρμογή συγκεκριμένης τιμής DSCP ή IP precedence στην τάξη κίνησης.
- Καθορισμός περιορισμού στο εύρος ζώνης που θα χρησιμοποιηθεί από την κλάση.
- Για να εφαρμοστεί ο χάρτης πολιτικής πρέπει να εφαρμοστεί πρώτα σε κάποιο interface.

3.4.6 Εφαρμογή Αστυνόμευσης και Σήμανσης

Αμέσως μετά την ταξινόμηση ενός πακέτου και αφού του έχει αποδοθεί DSCP ετικέτα ξεκινά η διαδικασία εφαρμογής αστυνόμευσης (policing) και σήμανσης του πακέτου (marking).

Η εφαρμογή αστυνόμευσης καθορίζει τα όρια στο εύρος ζώνης (bandwidth) που μπορεί να χρησιμοποιεί ένα είδος κίνησης. Πακέτα τα οποία ξεπερνούν το όριο χαρακτηρίζονται ως ότι

«εκτός προφίλ» ή «αιρετικά». Κάθε μηχανισμός εφαρμογής αστυνόμευσης αποφασίζει για κάθε πακέτο ξεχωριστά εάν είναι εκτός προφίλ και καθορίζει τις ενέργειες που πρέπει να γίνουν στο πακέτο.

Αυτές οι ενέργειες πραγματοποιούνται από τον μηχανισμό σήμανσης (marker) και περιλαμβάνουν:

- Προώθηση πακέτου χωρίς αλλαγές και τροποποιήσεις.
- Απόρριψη πακέτου.
- Τροποποίηση της τιμής DSCP που φέρει το πακέτο και προώθηση.

Τροποποιημένα πακέτα χρησιμοποιούν τις ίδιες ουρές με τα αυθεντικά πακέτα (με QoS ετικέτα) για να αποφεύγονται προβλήματα συγχρονισμού στη ροή των πακέτων.

Η εφαρμογή της αστυνόμευσης γίνεται μόνο σε φυσικές πόρτες μίας συσκευής. Μετά τον καθορισμό του χάρτη πολιτικής και τις ενέργειες που θα γίνονται σε κάθε περίπτωση, συσχετίζουμε την αστυνόμευση με το εισερχόμενο interface χρησιμοποιώντας την εντολή **service-policy**.

3.4.7 Εφαρμογή Αστυνόμευσης σε Φυσικές Πόρτες

Υπάρχει η δυνατότητα δημιουργίας διαφορετικών μηχανισμών εφαρμογής αστυνόμευσης σε φυσικές πόρτες ενός μεταγωγέα ή δρομολογητή:

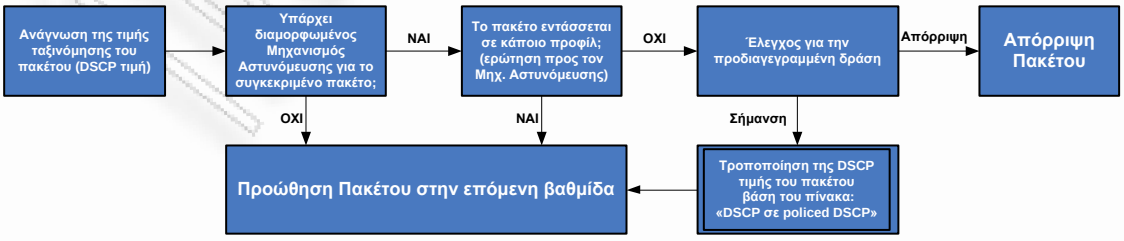
- Ξεχωριστό QoS: καθορίζει τα όρια εύρους ζώνης που διευκρινίζονται στον policer χωριστά για κάθε αντίστοιχη κατηγορία κίνησης. Η διαμόρφωση αυτού του τύπου policer μέσα σε ένα χάρτη πολιτικής γίνεται με τη χρησιμοποίηση της εντολής **police**.
- Συνολικό QoS: εφαρμόζει τα όρια εύρους ζώνης που διευκρινίζονται σε ένα συνολικό policer συσσωρευτικά σε όλες τις αντιστοιχημένες κυκλοφοριακές ροές. Η παραμετροποίηση συνολικής αστυνόμευσης μέσα στο χάρτη πολιτικής γίνεται μέσω της εντολής **police aggregate**. Μπορούμε επίσης να διευκρινίσουμε τα όρια του εύρους ζώνης για τον policer με τη χρήση της εντολής **mls qos aggregate-policer**.

Η εφαρμογή πολιτικής χρησιμοποιεί τον αλγόριθμο Κουβά Κουπονιών. Κάθε φορά που ένα πακέτο παραλαμβάνεται από το μεταγωγέα, ένα κουπόνι προστίθεται στον κουβά. Ο κουβάς έχει μια τρύπα και διαρρέει κουπόνια σε ένα ποσοστό που διευκρινίζεται ως μέσο ποσοστό κυκλοφορίας σε bits ανά δευτερόλεπτο. Κάθε φορά που ένα κουπόνι προστίθεται στον κουβά ο μεταγωγέας ελέγχει εάν υπάρχει αρκετός χώρος. Εάν δεν υπάρχει αρκετός χώρος, το πακέτο χαρακτηρίζεται ως εκτός προφίλ, και λαμβάνονται οι ανάλογες ενέργειες (απόρριψη πακέτου ή τροποποίηση).

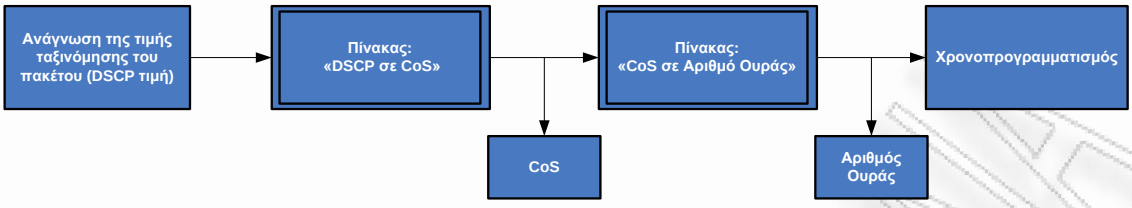
Το πόσο γρήγορα γεμίζει ο κουβάς εξαρτάται από το βάθος του (burst-byte), το ποσοστό στο οποίο τα κουπόνια αφαιρούνται (ποσοστό-bps) και τη διάρκεια της ροής η οποία είναι πάνω από το μέσο ποσοστό.

Στη συνέχεια παρουσιάζονται διαγραμματικά οι διαδικασίες αστυνόμευσης και σήμανσης ενός πακέτου (Εικόνα 3-23), καθώς και οι ενέργειες που εφαρμόζονται στην έξοδο (Εικόνα 3-24):

Εικόνα 3-23: Αστυνόμευση και Σήμανση



Εικόνα 3-24: Ουρά Αναμονής και Χρονοπρογραμματισμός



3.4.8 Πίνακες Αντιστοίχησης

Πίνακας «CoS σε DSCP»

Οι προεπιλεγμένες τιμές του πίνακα αντιστοίχησης εμφανίζονται στη συνέχεια.

Πίνακας 3-9: Προεπιλεγμένες τιμές πίνακα «CoS σε DSCP»

CoS τιμές	0	1	2	3	4	5	6	7
DSCP τιμές	0	8	16	24	32	40	48	56

Υπάρχει η δυνατότητα τροποποίησης των τιμών αυτών και κατά συνέπεια ο καθορισμός νέων DSCP τιμών για όλες τις CoS τιμές. Για παράδειγμα με την ακόλουθη εντολή, τα περιεχόμενα του πίνακα τροποποιούνται όπως παρουσιάζονται στον Πίνακα 3-10:

mls qos map cos-dscp 10 15 20 25 30 35 40 45

Πίνακας 3-10: Τροποποιημένες τιμές πίνακα «CoS σε DSCP»

CoS τιμές	0	1	2	3	4	5	6	7
DSCP τιμές	10	15	20	25	30	35	40	45

Πίνακας Μετάλλαξης «DSCP σε DSCP»

Οι προεπιλεγμένες τιμές αντιστοίχησης του πίνακα είναι 1:1. Υπάρχει η δυνατότητα να αλλάξουν τα περιεχόμενα και να καθοριστούν νέες DSCP τιμές για όλες τις παλαιές. Κάθε διεπαφή (interface) έχει το δικό της πίνακα μετάλλαξης. Έτσι, για παράδειγμα αν επιθυμούμε για όσα πακέτα καταφθάνουν στη διεπαφή GigabitEthernet0/1 με DSCP τιμή από 0 έως και 7 να μεταλλάσσεται στην QoS ετικέτα τους η DSCP τιμή σε 0 (μηδέν) και όσα καταφθάνουν με DSCP τιμή από 8 έως και 13 να μεταλλάσσεται στην QoS ετικέτα τους η DSCP τιμή σε 10, απαιτούνται οι ακόλουθες εντολές παραμετροποίησης:

```
Router(config)# mls qos map dscp-mutation OurMap1 1 2 3 4 5 6 7 to 0
Router(config)# mls qos map dscp-mutation OurMap1 8 9 10 11 12 13 to 10
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# mls qos trust dscp
Router(config-if)# mls qos dscp-mutation OurMap1
```

Πίνακας «IP Precedence σε DSCP»

Οι προεπιλεγμένες τιμές του «IP Precedence σε DSCP» πίνακα είναι ίδιες με του «CoS σε DSCP» πίνακα. Η τροποποίηση των τιμών αυτών και κατά συνέπεια ο ορισμός νέων DSCP τιμών για όλες τις IPP τιμές γίνεται ως ακολούθως:

```
Router(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
```

Πίνακας «DSCP σε policed DSCP»

Η προεπιλεγμένη αντιστοίχηση είναι 1:1. Η τροποποίηση των τιμών αυτών και κατά συνέπεια ο ορισμός νέων DSCP τιμών για όλες τις παλαιές DSCP τιμές γίνεται όπως στο ακόλουθο παράδειγμα όπου αντικαθίστανται οι τιμές 50-57 με 0:

```
Router(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
```

Πίνακας «DSCP σε CoS»

Οι προεπιλεγμένες τιμές του πίνακα αντιστοίχησης εμφανίζονται στη συνέχεια.

Πίνακας 3-11: Προεπιλεγμένες τιμές πίνακα «DSCP σε CoS»

DSCP τιμές	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS τιμές	0	1	2	3	4	5	6	7

Υπάρχει η δυνατότητα τροποποίησης των τιμών αυτών και κατά συνέπεια ο ορισμός νέων CoS τιμών για όλες τις DSCP τιμές. Για παράδειγμα με την ακόλουθη εντολή:

```
Router(config)# mls qos map dscp-cos 8 16 24 32 40 to 0
```

Πίνακας «CoS σε Αριθμό Ουράς»

Οι προεπιλεγμένες τιμές του πίνακα αντιστοίχησης εμφανίζονται στη συνέχεια.

Πίνακας 3-12: Προεπιλεγμένες τιμές πίνακα «CoS σε Αριθμό Ουράς»

User Priority (CoS)	**Ουρά**
0, 1	1
2, 3	2
4, 5	3
6, 7	4

Σε περίπτωση που οι προεπιλεγμένες αυτές τιμές δε συμβαδίζουν με το πρότυπο IEEE 802.1Q (βλ. Πίνακα 3-13), μπορούν να παραμετροποιηθούν.

Πίνακας 3-13: Προτεινόμενη Αντιστοίχιση CoS σε Αριθμό Ουράς Εξόδου

	Αριθμός διαθέσιμων Τάξεων κίνησης (Ουρές Εξόδου)							
CoS	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0	0	0	0	1	1	1	1	2
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1
3	0	0	0	1	1	2	2	3
4	0	1	1	2	2	3	3	4
5	0	1	1	2	3	4	4	5
6	0	1	2	3	4	5	5	6
7	0	1	2	3	4	5	6	7

Συνεπώς στην περίπτωση που απαιτούνται τέσσερεις ουρές εξόδου σε μια διεπαφή, με βάση τον παραπάνω πίνακα και κατά συνέπεια με βάση το πρότυπο 802.1Q, απαιτείται η ακόλουθη παραμετροποίηση:

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# wrr-queue cos-map 1 1 2
Router(config-if)# wrr-queue cos-map 2 0 3
Router(config-if)# wrr-queue cos-map 3 4 5
Router(config-if)# wrr-queue cos-map 4 6 7
```

3.4.9 Σταθμισμένη Δίκαιη Αναμονή Βασισμένη σε Τάξεις (CBWFQ)

Προεπισκόπηση

Ο αλγόριθμος προγραμματισμού εκπομπής πακέτων CBWFQ (Σταθμισμένη δίκαιη αναμονή βασισμένη σε Τάξεις) είναι επέκταση του αλγορίθμου WFQ (Σταθμισμένη δίκαιη αναμονή-ουρά) και παρέχει υποστήριξη στη χρήση των καθορισμένων τάξεων κίνησης. Για την εφαρμογή του αλγορίθμου CBWFQ, πρέπει να οριστούν οι τάξεις κίνησης με βάση τα κριτήρια προσαρμογής των συμπεριλαμβανομένων πρωτοκόλλων, λίστες ελέγχου πρόσβασης (ACLs) και διεπαφές εισόδου. Τα πακέτα που πληρούν τις προδιαγραφές προσαρμογής για μια τάξη αποτελούν κίνηση της τάξης αυτής.

Όταν μια τάξη οριστεί σύμφωνα με τα κριτήρια, ακολούθως θα λάβει χαρακτηριστικά. Ο χαρακτηρισμός μιας τάξης γίνεται με τον ορισμό του εύρους ζώνης, το βάρος στάθμισης και το μέγιστο όριο πακέτων. Το εύρος ζώνης που έχει ανατεθεί σε μια τάξη είναι το εγγυημένο εύρος ζώνης που παραχωρείται στην τάξη κατά τη διάρκεια της συμφόρησης. Επίσης μπορεί να καθοριστεί το όριο ουράς της τάξης αυτής που είναι ο μέγιστος αριθμός πακέτων που επιτρέπεται να συσσωρεύονται στην ουρά για την τάξη αυτή. Συνεπώς τα πακέτα που ανήκουν σε μια τάξη υπόκεινται στα όρια εύρους ζώνης και ουράς της τάξης αυτής.

Όταν μια ουρά προτεραιότητας φτάσει στο προπαραμετροποιημένο όριο, τότε με το να εισέλθουν σε αυτή επιπρόσθετα πακέτα θα προκληθεί απόρριψη tail drop ή packet drop, ανάλογα πώς έχει παραμετροποιηθεί η πολιτική της Τάξης.

Tail Drop χρησιμοποιείται για CBWFQ τάξεις, εκτός αν διακριτά η τάξη έχει παραμετροποιηθεί να χρησιμοποιεί ως μέθοδο αποφυγής συμφόρησης τον αλγόριθμο Weighted Random Early Detection (WRED) για την απόρριψη των πακέτων. Στην περίπτωση που χρησιμοποιείται WRED packet drop αντί για tail drop για μια ή περισσότερες τάξεις σε έναν χάρτη πολιτικής, πρέπει να επιβεβαιώνεται ότι δεν έχει παραμετροποιηθεί για τη διεπαφή (interface), στην οποία επισυνάπτεται η πολιτική υπηρεσίας, ο αλγόριθμος WRED.

Αν η προεπιλεγμένη κλάση (default class) διαρθρωθεί με την εντολή ***bandwidth*** *policy-map class*, όλη η μη ταξινομημένη κίνηση θα ενταχθεί σε μια ενιαία ουρά με δεδομένη μεταχείριση σύμφωνα με το παραμετροποιημένο εύρος ζώνης. Αν η προεπιλεγμένη κλάση διαρθρωθεί με την εντολή ***fair-queue***, όλη η μη ταξινομημένη κίνηση κατατάσσεται σε ροή με best-effort μεταχείριση. Αν η προεπιλεγμένη κλάση δεν παραμετροποιηθεί, τότε έχει προεπιλεγεί η κίνηση που δεν ταιριάζει με καμία από τις προγραμματισμένες υπάρχουσες κλάσεις να κατατάσσεται σε ροή με best-effort μεταχείριση. Μόλις ένα πακέτο ταξινομηθεί, εφαρμόζονται όλοι οι πρότυποι μηχανισμοί που μπορούν να χρησιμοποιηθούν για τη διαφοροποίηση των υπηρεσιών κλάσεων.

Λέγοντας ταξινόμηση ροών γίνεται αναφορά στο πρότυπο WFQ. Δηλαδή τα πακέτα με την ίδια IP διεύθυνση προέλευσης, IP διεύθυνση προορισμού, TCP ή UDP πόρτα πηγής ή πόρτα προορισμό TCP ή UDP ταξινομούνται στην ίδια ροη. Το πρότυπο WFQ διαθέτει ίδιο μερίδιο του εύρους ζώνης για κάθε ροή - ίδια στάθμιση και για το λόγο αυτό καλείται επίσης «δίκαιη ουρά» (fair queue).

Για το CBWFQ, το οποίο είναι επέκταση του προτύπου WFQ, το βάρος στάθμισης που ορίζεται για την κλάση, εκφράζει και το βάρος κάθε πακέτου που ανήκει σε αυτή. Τα πακέτα που

φτάνουν στη διεπαφή εξόδου, κατατάσσονται σύμφωνα με τα κριτήρια που ταιριάζουν στα φίλτρα που έχουν καθοριστεί και έτσι κάθε πακέτο σταθμίζεται κατάλληλα. Η στάθμιση κάθε πακέτου καθορίζεται από το εύρος ζώνης που έχει ορίσει ο χρήστης να διατίθεται σε κάθε κλάση. Υπό αυτή την έννοια και η στάθμιση μιας κλάσης ορίζεται από το χρήστη.

Μετά τη στάθμιση, το πακέτο πάει και τοποθετείται στη κατάλληλη ουρά κλάσης. Ο CBWFQ χρησιμοποιεί τα βάρη, δηλαδή τη στάθμιση των πακέτων για να διασφαλίσει ότι η ουρά κλάσης εξυπηρετείται δίκαια.

Η διαμόρφωση μιας πολιτικής τάξεων (class policy) – *δηλαδή η διαμόρφωση του CBWFQ αλγορίθμου* – περιλαμβάνει τα ακόλουθα τρία βήματα:

1. Καθορισμός τάξεων κίνησης, ώστε να δημιουργηθεί πολιτική ταξινόμησης (χάρτες ταξινόμησης-class maps)

   Η διαδικασία αυτή καθορίζει πόσα είδη πακέτων θα πρέπει να διαφοροποιηθούν μεταξύ τους.

2. Συσχέτιση των πολιτικών (δηλαδή χαρακτηριστικά τάξεων) με κάθε τάξη κίνησης (χάρτες πολιτικής – policy maps).

   Αυτή η διαδικασία προϋποθέτει διαμόρφωση των πολιτικών που εφαρμόζονται στα πακέτα που ανήκουν σε μια από τις τάξεις που έχουν ήδη οριστεί, μέσω ενός χάρτη ταξινόμησης (class map). Για τη διαδικασία αυτή πρέπει να οριστεί ένας χάρτης πολιτικής (policy map) που καθορίζει την πολιτική για κάθε τάξη κίνησης.

3. Σύνδεση πολιτικών με τη διεπαφή (υπηρεσία πολιτικών-service policies)

   Αυτή η διαδικασία απαιτεί να συσχετιστεί ένας ήδη υπάρχων χάρτης πολιτικής (policy map) ή υπηρεσία πολιτικής (service policy), με μια διεπαφή (interface) ώστε να εφαρμοστεί το συγκεκριμένο σύνολο πολιτικών για τον καθορισμό της συγκεκριμένης διεπαφής.

Οφέλη

Ο CBWFQ αλγόριθμος επιτρέπει τον ακριβή προσδιορισμό του εύρους ζώνης που θα διατεθεί σε κάθε συγκεκριμένη τάξη κίνησης. Λαμβάνοντας υπόψη το διαθέσιμο εύρος ζώνης στη διεπαφή, μπορούν να διαμορφωθούν έως και 64 τάξεις καθώς και η μεταξύ τους κατανομή ελέγχου, γεγονός που δεν μπορεί να συμβεί με τη δίκαιη ουρά WFQ.

Η δίκαιη ουρά, που βασίζεται σε ροές, για να ταξινομήσει την κίνηση εφαρμόζει βάρη στάθμισης για κάθε συνομιλία και υπολογίζει το διαθέσιμο εύρος ζώνης για κάθε μια. Αυτά τα βάρη ταξινόμησης της κίνησης, εξαρτώνται και περιορίζονται από τα επτά IP Precedence επίπεδα.

Περιορισμοί

Η διαμόρφωση του CBWFQ σε μια φυσική διεπαφή είναι δυνατή μόνο αν η διεπαφή είναι στην προκαθορισμένη κατάσταση ουράς. Για τη σειριακή διεπαφή E1 (2048 Mbps) η προκαθορισμένη κατάσταση είναι ο αλγόριθμος WFQ, ενώ άλλες διεπαφές χρησιμοποιούν FIFO σαν προκαθορισμένη κατάσταση. Η ενεργοποίηση της λειτουργιάς CBWFQ αντικαθιστά την αρχική WFQ, ενώ αντίθετα σε ένα ATM PVC δεν συμβαίνει το ίδιο.

Πριν γίνει η παραμετροποίηση σε μια κλάση ενός χάρτη πολιτικής, ότι για τη WRED λειτουργία θα χρησιμοποιεί packet drop αντί tail drop, θα πρέπει πρώτα να έχει επιβεβαιωθεί ότι δεν έχει διαμορφωθεί WRED λειτουργία στη διεπαφή όπου θα εφαρμοστεί αυτή η υπηρεσία πολιτικής.

3.4.10 Διαμόρφωση Class Map

Κάθε class-map περιέχει προσαρμοσμένα κριτήρια (συνθήκες ελέγχου) όπως: λίστες πρόσβασης ή διεπαφή εισόδου ή το πρωτόκολλο, βάσει των οποίων ένα πακέτο ελέγχεται έτσι ώστε να καθοριστεί αν ανήκει ή όχι σε μια συγκεκριμένη τάξη κίνησης. Ο στόχος είναι η δημιουργία μιας αποτελεσματικής τάξης της οποίας η πολιτική μπορεί να καθοριστεί σε έναν ή και περισσότερους χάρτες (policy maps).

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# class-map class-map-name`	Καθορίζει το όνομα του class-map

2	`Router(config-cmap)# match access-group {access-group | name access-group-name}`
	
	ή
	
	`Router(config-cmap)# match input-interface interface-name`
	
	ή
	
	`Router(config-cmap)# match protocol protocol`
		Καθορίζει το όνομα της **ACL** της οποίας τα περιεχόμενα πακέτα ελέγχονται για να διαπιστωθεί εάν ανήκουν στη τάξη.
		
		Καθορίζει το όνομα της **διεπαφής εισόδου** που χρησιμοποιείται σαν κριτήριο προσαρμογής κατά το οποίο τα πακέτα ελέγχονται για να διαπιστωθεί εάν ανήκουν στη τάξη.
		
		Καθορίζει το **πρωτόκολλο** που χρησιμοποιείται σαν κριτήριο προσαρμογής κατά το οποίο τα πακέτα ελέγχονται για να διαπιστωθεί εάν ανήκουν στη τάξη.

Παράδειγμα διαμόρφωσης class-map

Στο ακόλουθο παράδειγμα θα δημιουργηθούν δυο access-lists με ονόματα 101 και 102 στις οποίες θα καθοριστούν τα κριτήρια προσαρμογής. Για την πρώτη class-map που θα ονομαστεί class1, η ACL 101 θα χρησιμοποιηθεί ως κριτήριο προσαρμογής. Όμοια η ACL 102 για τη δεύτερη τάξη που δημιουργείται με όνομα class2. Κατά συνέπεια τα πακέτα θα ελέγχονται με βάση αυτές τις ACLs για να διαπιστωθεί αν ανήκουν στην τάξη.

```
Router(config)# access-list 101 permit udp host 10.10.10.10 host 10.10.10.20 range 16384 20000
Router(config)# access-list 102 permit udp host 10.10.10.10 host 10.10.10.20 range 53000 56000
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config-cmap)# class-map class2
Router(config-cmap)# match access-group 102
Router(config-cmap)# exit
```

3.4.11 Διαμόρφωση Class Policy σε Policy Map

Η διαμόρφωση ενός χάρτη πολιτικής (policy map) και η δημιουργία πολιτικών τάξης (class policies) συνθέτουν την υπηρεσία πολιτικής (service policy). Χρησιμοποιείται πρώτα η εντολή **policy-map** για τον καθορισμό του ονόματος και εν συνεχεία μια ή και περισσότερες από τις εντολές που ακολουθούν, για τον προγραμματισμό πολιτικής για την πρότυπη-τυπική τάξη (standard class) ή την προκαθορισμένη τάξη (default class):

- **Class**
- **Bandwidth**
- **Fair-queue (μόνο για class-default class)**
- **Queue-limit ή random-detect**

Για να διαμορφωθεί η πολιτική τάξης, μπορεί να χρησιμοποιηθεί μια ή και περισσότερες από τις εντολές της λίστας. Για παράδειγμα, σε μια τάξη μπορεί να καθοριστεί το bandwidth ενώ σε μια δεύτερη τάξη μπορεί να καθοριστεί και το bandwidth αλλά και το queue limit.

Η προκαθορισμένη τάξη (class default-class) του χάρτη πολιτικής (policy map), είναι η τάξη στην οποία κατευθύνεται η κίνηση που δεν πλήροι τα κριτήρια προσαρμογής των άλλων τάξεων, των οποίων η πολιτική καθορίζεται στο συγκεκριμένο χάρτη πολιτικής.

Όπως έχει αναφερθεί υπάρχει η δυνατότητα να δημιουργηθούν έως 64 τάξεις με τις πολιτικές τους. Ωστόσο, το συνολικό εύρος ζώνης που διατίθεται για όλες τις τάξεις δεν πρέπει να υπερβαίνει το 75% του συνολικού διαθέσιμου στη διεπαφή. Το υπόλοιπο 25% χρησιμοποιείται για έλεγχο και κίνηση δρομολόγησης (η παράκαμψη του 75%, μπορεί να επιτευχθεί με την εντολή **max-reserved bandwidth**). Αν δεν είναι όλο το εύρος ζώνης κατανεμημένο, το υπόλοιπο κατανέμεται αναλογικά μεταξύ των τάξεων με βάση το παραμετροποιημένο εύρος ζώνης τους.

3.4.12 Διαμόρφωση Class Policy με χρήση Tail Drop

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# policy-map policy-map`	Καθορίζει το όνομα του policy-map
2	`Router(config-pmap)# class class-name`	Καθορίζει το όνομα της τάξης που περιλαμβάνεται στο service policy.

3	`Router(config-pmap-c)# bandwidth {bandwidth-kbps | remaining percent percentage | percent percentage}`
	
	ή
	
	`Router(config-pmap-c)# priority {bandwidth-kbps | percent percentage}`
		Καθορίζει το ποσό του εύρους ζώνης που θα διατεθεί στη τάξη. Το διατιθέμενο εύρος ζώνης θα πρέπει να μπορεί να υποστηρίζει και τις επιβαρύνσεις του Layer 2.
		
		Διατηρεί μια αυστηρή ουρά προτεραιότητας (PQ) για την CBWFQ κίνηση.

4	`Router(config-pmap-c)# queue-limit number-of-packets`	Καθορίζει το μέγιστο αριθμό πακέτων που μπορούν να ενταχθούν στην ουρά για τη κλάση. Παίρνει τιμές από 16 έως 16384, αλλά εξαρτάται από την πλατφόρμα και την έκδοση του IOS. Η προκαθορισμένη τιμή είναι 64.

Για διαμόρφωση πολιτικής σε περισσότερες από μια τάξεις στον ίδιο χάρτη πολιτικής, αρκεί η επανάληψη των βημάτων 2 έως 4. Σημειώνεται ότι επειδή το σύνολο των εντολών χρησιμοποιεί την εντολή queue-limit, ο χάρτης πολιτικής χρησιμοποιεί tail drop (δηλαδή απορρίπτει το τελευταίο πακέτο) και όχι WRED packet drop.

Η εντολή bandwidth

Ο καθορισμός του εύρους ζώνης που θα διατίθεται σε μια συγκεκριμένη τάξη διαμορφώνεται με την εντολή **bandwidth** (Βήμα 3).

```
Router(config-pmap-c)# bandwidth {bandwidth-kbps | remaining percent percentage | percent percentage}
```

Αντίθετα η κατάργηση του διατιθέμενου εύρους ζώνης επιτυγχάνεται με τη χρήση της εντολής **no bandwidth**.

Στη συνέχεια γίνεται συντακτική ανάλυση της εντολής:

bandwidth-kbps	Το ποσό του εύρους ζώνης σε kbps, που θα διατεθεί για τη τάξη. Η τιμή ποικίλει ανάλογα με τη διεπαφή και τη πλατφόρμα που χρησιμοποιείται.
remaining percent *percentage*	Καθορίζει το ποσοστό του εγγυημένου εύρους ζώνης που θα εξαρτάται από το σχετικό ποσοστό του διαθέσιμου εύρους ζώνης. Το ποσοστό μπορεί να είναι ένας αριθμός από 1 έως 100.
percent *percentage*	Καθορίζει το ποσοστό του εγγυημένου εύρους ζώνης που θα εξαρτάται από το απόλυτο ποσοστό του διαθέσιμου εύρους ζώνης. Το ποσοστό μπορεί να είναι ένας αριθμός από 1 έως 100.

Παράδειγμα χρήσης της εντολής bandwidth σε CBWFQ

Στο ακόλουθο παράδειγμα θα δημιουργηθεί ένα policy map με δυο τάξεις: με την εντολή bandwidth θα καθοριστεί το εγγυημένο εύρος ζώνης για κάθε τάξη (50% για την πρώτη και 25% για τη δεύτερη), καθώς και ο μέγιστος αριθμός πακέτων που μπορούν να ενταχθούν στην ουρά της πρώτης τάξης. Στη συνέχεια θα εφαρμοστεί η πολιτική στη διεπαφή serial3/2/1.

```
Router(config)# policy-map policy1

Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# queue-limit 30
Router(config-pmap-c)# exit

Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth percent 25
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

Το τελευταίο στάδιο του παραδείγματος είναι η εφαρμογή της υπηρεσίας πολιτικής (service policy) και η ενεργοποίηση του CBWFQ αλγορίθμου στη διεπαφή (interface). Για να συμβεί αυτό θα χρησιμοποιηθεί η ακόλουθη εντολή:

```
Router(config-if)# service-policy output policy-map
```

Συνεπώς η συνέχεια του παραδείγματος θα είναι η ακόλουθη:

```
Router(config)# interface serial3/2/1
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

Η εντολή priority

Για να δοθεί προτεραιότητα στην κίνηση μιας τάξης, που ανήκει σε ένα χάρτη πολιτικής, χρησιμοποιείται η εντολή **priority** (Βήμα 3).

```
Router(config-pmap-c)# priority {bandwidth-kbps | percent percentage}
```

Αντίθετα η κατάργηση της προτεραιότητας αυτής επιτυγχάνεται με τη χρήση της εντολής **no priority**.

```
Router(config-pmap-c)# no priority {bandwidth-kbps | percent percentage}
```

Στη συνέχεια γίνεται συντακτική ανάλυση της εντολής:

bandwidth-kbps	Εγγυημένο επιτρεπτό εύρος ζώνης σε kbps για την κίνηση προτεραιότητας. Η τιμή ποικίλει ανάλογα με τη διεπαφή και τη πλατφόρμα που χρησιμοποιείται. Πέρα από το εγγυημένο εύρος ζώνης, η υπόλοιπη κίνηση μπορεί να απορριφτεί σε περίπτωση συμφόρησης. Η τιμή πρέπει να είναι μεταξύ 8 και 2.000.000 kbps.
percent	Καθορίζει ότι το ποσό του εγγυημένου εύρους ζώνης θα εξαρτάται από το ποσοστό του διαθέσιμου εύρους ζώνης.
percentage	Το συνολικό ποσοστό του διαθέσιμου εύρους ζώνης για μια τάξη προτεραιότητας μπορεί να λάβει τιμές από 1 έως 100.

Με τη διατήρηση αυστηρής ουράς προτεραιότητας (PQ) για τη CBWFQ κίνηση, διαμορφώνεται ο μηχανισμός Low Latency Queuing (LLQ). Η PQ επιτρέπει στα ευαίσθητα στην καθυστέρηση δεδομένα φωνής να ενταχθούν μέσα σε ουρά και να αποσταλούν πριν από τα δεδομένα των υπολοίπων τάξεων. Μια παρόμοια εντολή είναι η **ip rtp priority**, η οποία δίνει τη δυνατότητα να ορίζεται προτεραιότητα ροών με βάση μόνο τον UDP αριθμό θύρας. Δεν είναι διαθέσιμη για τα ATM PVCs.

Οι εντολές **bandwidth** και **priority** δεν μπορεί να χρησιμοποιηθούν στην ίδια τάξη ενός χάρτη πολιτικής. Ωστόσο μπορούν να χρησιμοποιηθούν σε διαφορετικές τάξεις που ανήκουν στον ίδιο χάρτη πολιτικής.

Μέσα σε ένα χάρτη πολιτικής, μπορούν να δοθούν μια ή και περισσότερες καταστάσεις προτεραιότητας τάξεων. Όταν πολλές τάξεις μέσα σε ένα ενιαίο χάρτη πολιτικής καθοριστούν σαν τάξεις προτεραιότητας, τότε όλη η κίνηση των τάξεων αυτών μπαίνει σε μια ενιαία ουρά προτεραιότητας.

Παράδειγμα χρήσης της εντολής priority

Στο επόμενο παράδειγμα θα καθοριστεί PQ με εγγυημένο εύρος ζώνης τα 50 kbps για την τάξη voice του χάρτη πολιτικής policy1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
```

3.4.13 Διαμόρφωση Class Policy με Χρήση WRED Packet Drop

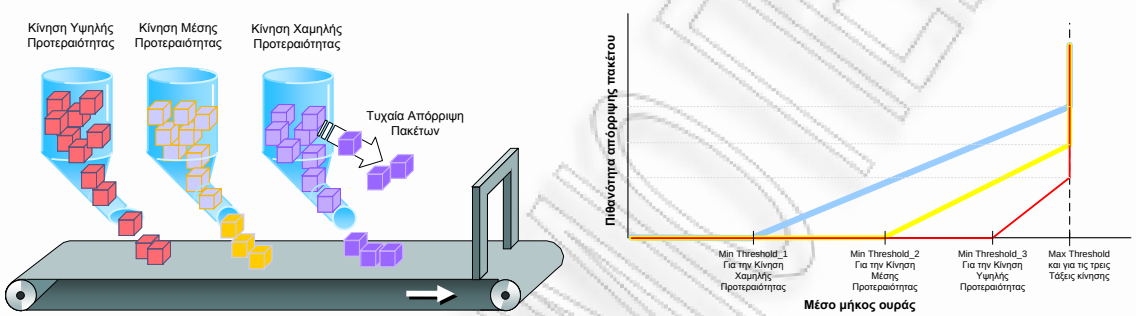
Σε προγενέστερη ενότητα έγινε ανάλυση της Tail Drop διαδικασίας απόρριψης πακέτων. Ένα τέτοιο σχήμα στην πράξη έχει πάρα πολλά προβλήματα, με κυριότερα τη μειωμένη απόδοση, την αυξημένη αδικία, τον καθολικό συγχρονισμό των ροών και τον μη διαχωρισμό της κίνησης δεδομένων σε τάξεις. Για να αντιμετωπίσουμε αυτά τα προβλήματα υλοποιούμε πολιτικές Ενεργούς Διαχείρισης Ουράς (Active Queue Management), βάσει των οποίων διαχειριζόμαστε τα πακέτα στους καταχωριτές με σκοπό την αποφυγή των προαναφερθέντων προβλημάτων. Οι δυο κύριες μέθοδοι υλοποίησης Ενεργούς Διαχείρισης Ουράς είναι η Απόρριψη Πακέτων (Packet Drop) και ο Χρονοπρογραμματισμός (Scheduling).

Ο αλγόριθμος RED (Random Early Detection / Drop, Τυχαία Πρώιμη Ανίχνευση / Απόρριψη) βασίζεται στη λογική της τυχαίας απόρριψης πακέτων, με σκοπό την αύξηση δικαιοσύνης και τη μείωση απόρριψης ριπής, αφού έτσι χάνονται πακέτα από διάφορες ροές. Έτσι κατά τη λειτουργία του θέτει δυο κατώφλια ως προς το μέγεθος της ουράς: το Ελάχιστο Κατώφλι (Minimum Threshold) και το Μέγιστο Κατώφλι (Maximum Threshold), καθώς και μια πιθανότητα MPD (Mark Probability Denominator). Κάθε φορά που εισέρχεται ένα πακέτο, ο αλγόριθμος RED υπολογίζει αν θα το απορρίψει ή όχι με βάση τη σχέση του μέσου μήκους ουράς με τα κατώφλια και την πιθανότητα απόρριψης.

Η ανάγκη παροχής ποιότητας υπηρεσίας βασισμένης σε τάξεις κίνησης, οδήγησε στην μετεξέλιξη του αλγορίθμου RED σε WRED (Weighted RED, Σταθμισμένο RED). Ο WRED επιτυγχάνει να αντιμετωπίζει διαφορετικά κάθε τάξη κίνησης, εισάγοντας τα αντίστοιχα Max και Min Threshold για κάθε μια. Αυτό σημαίνει ότι για κάθε επίπεδο προτεραιότητας (Τάξη) ορίζεται ξεχωριστό Μέγιστο και Ελάχιστο Κατώφλι και κατά συνέπεια εφαρμόζεται διαφορετικό προφίλ απόρριψης ανάλογα με τον τύπο κίνησης. Γενικά ο WRED απορρίπτει πακέτα επιλεκτικά με βάση το IP Precedence. Έτσι τα πακέτα υψηλής προτεραιότητας είναι λιγότερο πιθανό να απορριφθούν σε σχέση με πακέτα χαμηλής προτεραιότητας.

Στο επόμενο σχήμα παρουσιάζεται ένα σενάριο WRED απόρριψης πακέτων. Έχουν οριστεί τρεις Τάξεις κίνησης με Χαμηλή, Μεσαία και Υψηλή προτεραιότητα. Κατά συνέπεια εφαρμόζεται διαφορετικό προφίλ απόρριψης καθορίζοντας τρεις διαφορετικές τιμές Min Threshold (Min Threshold_1, Min Threshold_2 και Min Threshold_3) και μια κοινή τιμή Max Threshold.

Εικόνα 3-25: Διαδικασία WRED Απόρριψης Πακέτων



Είναι φανερό πως υπάρχουν τρεις διαφορετικές συμπεριφορές απόρριψης αφού ισχύει ότι $\text{MinThreshold}\_1 \prec \text{MinThreshold}\_2 \prec \text{MinThreshold}\_3$ και κατά συνέπεια το μέσο μήκος ουράς για την κίνηση Χαμηλής Προτεραιότητας θα προσεγγίσει συντομότερα την αντίστοιχη Min Threshold τιμή του (Min Threshold_1) απ ότι το μέσο μήκος ουράς της Μεσαίας και Υψηλής Προτεραιότητας. Συνεπώς σε κάθε περίπτωση συμφόρησης τη μεγαλύτερη πιθανότητα απόρριψης την έχουν τα πακέτα που ανήκουν στην τάξη με τη χαμηλότερη προτεραιότητα.

Η διαμόρφωση του WRED αλγορίθμου κρίνεται απαραίτητη σε κάθε διεπαφή εξόδου που αναμένεται συμφόρηση. Κυρίως προτείνεται η εφαρμογή του σε δρομολογητές επιπέδου πυρήνα, ενώ οι δρομολογητές πρόσβασης έχουν την υποχρέωση να εκχωρούν το IP Precedence στα εισερχόμενα στο δίκτυο πακέτα, βάσει του οποίου ο WRED αντιμετωπίζει τα διαφορετικά είδη κίνησης.

Στη συνέχεια παρουσιάζεται βήμα προς βήμα η διαδικασία εφαρμογής του WRED αλγορίθμου σε έναν δρομολογητή Cisco.

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# policy-map policy-map`	Καθορίζει το όνομα του policy-map
2	`Router(config-pmap)# class class-name`	Καθορίζει το όνομα της τάξης που δημιουργείται και περιλαμβάνεται στο service policy.

3	`Router(config-pmap-c)# bandwidth bandwidth-kbps`
	ή
	`Router(config-pmap-c)# priority {bandwidth-kbps | percent percentage}`
		Καθορίζει το ποσό του εύρους ζώνης που θα διατεθεί στη τάξη. Το διατιθέμενο εύρος ζώνης θα πρέπει να μπορεί να υποστηρίζει και τις επιβαρύνσεις του Layer 2.
		Διατηρεί μια αυστηρή ουρά προτεραιότητας (PQ) για την CBWFQ κίνηση.

Βήμα	Εντολή	Επεξήγηση
4	`Router(config-pmap-c)# **random-detect**`	Ενεργοποιεί τη WRED διαδικασία. Η πολιτική τάξης απορρίπτει πακέτα με χρήση WRED αντί tail drop.

5	`Router(config-pmap-c)# **random-detect exponential-weighting-constant** *exponent*`
	
	και/ή
	
	`Router(config-pmap-c)# **random-detect precedence** *precedence min-threshold max-threshold mark-prob-denominator*`
		Διαμορφώνει το συντελεστή εκθετικού βάρους που χρησιμοποιείται κατά τον υπολογισμό του μέσου μεγέθους ουράς.
		
		Ρυθμίζει τις παραμέτρους του WRED με ένα συγκεκριμένο IP Precedence. Η εντολή πρέπει να επαναλαμβάνεται για κάθε Precedence.

Για διαμόρφωση πολιτικής σε περισσότερες από μια τάξεις στον ίδιο χάρτη πολιτικής, αρκεί η επανάληψη των βημάτων 2 έως 5. Σημειώνεται ότι το σύνολο των εντολών χρησιμοποιεί WRED packet drop και όχι tail drop.

Το μέσο μέγεθος ουράς βασίζεται στον προηγούμενο μέσο όρο και στο τρέχον μέγεθος της ουράς. Ο τύπος υπολογισμού είναι ο ακόλουθος:

$$\text{average}=[\text{old\_average}*(1-\frac{1}{2^n})]+(\text{current\_queue\_size}*\frac{1}{2^n})$$

Όπου το *n* είναι συντελεστής εκθετικού βάρους. Παίρνει τιμές απο1 έως 16, με προκαθορισμένη τιμή το 9.

Για μεγάλες τιμές του *n*, αυξάνεται η βαρύτητα του προηγούμενου μέσου όρου. Το μέσο μέγεθος ουράς είναι απίθανο να αλλάξει πολύ γρήγορα, αποφεύγοντας δραστική ταλάντευση στο μέγεθος. Βέβαια για πολύ υψηλές τιμές του *n*, η διαδικασία WRED θα είναι σαν να έχει τεθεί εκτός λειτουργίας.

Για χαμηλές τιμές του *n*, το μέσο μέγεθος ουράς πλησιάζει στενά το τρέχον μέγεθος ουράς. Το μέσο μέγεθος ουράς που προκύπτει κυμαίνεται ανάλογα με τις αλλαγές των επιπέδων κυκλοφορίας.

Πιθανότητα απόρριψης πακέτου

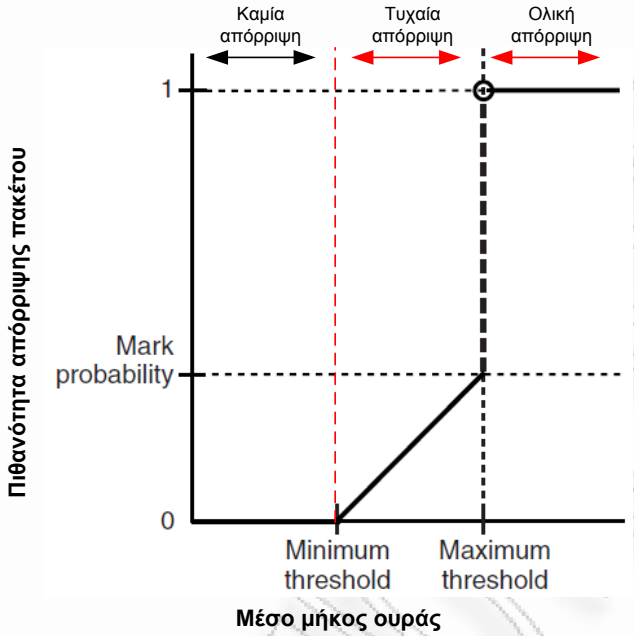
Η πιθανότητα απόρριψης πακέτου βασίζεται στο minimum threshold (ελάχιστο κατώφλι), maximum threshold (μέγιστο κατώφλι) και στον παρονομαστή mark probability (σημείο πιθανότητας).

Όταν το μέσο μέγεθος ουράς είναι πάνω από το ελάχιστο κατώφλι, τότε η διαδικασία RED ξεκινά να απορρίπτει πακέτα. Το ποσοστό απόρριψης πακέτων αυξάνεται γραμμικά όσο το μέσο μέγεθος ουράς αυξάνεται και έως ότου να φτάσει το μέγιστο κατώφλι.

Ο παρονομαστής mark probability (mark-prob-denominator) είναι το κλάσμα των πακέτων που απορρίφθηκαν όταν το μέσο μέγεθος ουράς είναι στο μέγιστο κατώφλι. Για παράδειγμα, αν ο παρονομαστής είναι 512 σημαίνει ότι απορρίπτεται ένα ανά 512 πακέτα και ενώ το μέσο μέγεθος ουράς είναι στο μέγιστο κατώφλι.

Μόλις το μέσο μέγεθος ουράς ξεπεράσει το μέγιστο κατώφλι, όλα τα πακέτα απορρίπτονται.

Εικόνα 3-26: Πιθανότητα WRED Απόρριψης Πακέτου



Η εντολή random-detect precedence

Όπως ήδη έχει αναφερθεί η ρύθμιση των WRED παραμέτρων με ένα συγκεκριμένο IP Precedence επιτυγχάνεται με την ακόλουθη εντολή:

`random-detect precedence` *`precedence min-threshold max-threshold mark-prob-denominator`*

Ενώ με την ακόλουθη εντολή επιστρέφουν οι παράμετροι στην προκαθορισμένη τιμή ανάλογα με το IP Precedence:

`no random-detect precedence` *`precedence min-threshold max-threshold mark-prob-denominator`*

Στη συνέχεια γίνεται συντακτική ανάλυση της εντολής:

precedence	Ο αριθμός IP Precedence. Η τιμή κυμαίνεται από 0 έως και 7
min-threshold	Το ελάχιστο κατώφλι του αριθμού πακέτων. Η τιμή κυμαίνεται από 1 έως 4096. Όταν το μέσο μέγεθος ουράς φτάσει αυτό τον αριθμό, ο WRED ξεκινάει την απόρριψη πακέτων ανάλογα με το καθορισμένο IP Precedence. Η προκαθορισμένη τιμή εξαρτάται από το επιλεγμένο IP Precedence. Για παράδειγμα το min-threshold για IP Precedence ισο με το 0, αντιστοιχεί στο μισό του max-threshold. Στη συνέχεια θα δοθεί η λίστα με τις προκαθορισμένες τιμές του min-threshold ανά IP Precedence.
max-threshold	Το μέγιστο κατώφλι του αριθμού πακέτων. Η τιμή κυμαίνεται από min-threshold έως 4096. Όταν το μέσο μέγεθος ουράς φτάσει αυτό τον αριθμό, ο WRED ξεκινάει την απόρριψη όλων των πακέτων με το καθορισμένο IP Precedence.
mark-prob-denominator	Είναι το κλάσμα των πακέτων που απορρίφθηκαν όταν το μέσο μέγεθος ουράς είναι στο μέγιστο κατώφλι. Για παράδειγμα, αν ο παρονομαστής είναι 512, σημαίνει ότι απορρίπτεται ένα ανά 512 πακέτα και ενώ το μέσο μέγεθος ουράς είναι στο max-threshold. Η τιμή του κυμαίνεται από 1 έως 65536 με προκαθορισμένη τιμή το 10 (απορρίπτεται ένα πακέτο ανά 10 στο max-threshold).

Πίνακας 3-14: Προκαθορισμένες Τιμές της Παραμέτρου Minimum Threshold του WRED

IP Precedence (IP Προτεραιότητα)	**Τιμή Minimum Threshold (κλάσμα Buffer εξόδου)**
0	9/18 (1/2)
1	10/18 (5/9)
2	11/18
3	12/18 (2/3)
4	13/18
5	14/18 (7/9)
6	15/18 (5/6)
7	16/18 (8/9)

Η εντολή random-detect dscp

Όμοια με την παραπάνω εντολή και η ρύθμιση των WRED παραμέτρων με μια συγκεκριμένη DSCP τιμή επιτυγχάνεται με την ακόλουθη εντολή:

random-detect dscp *dscp-value min-threshold max-threshold [max-prob-denominator]*

Ενώ με την ακόλουθη εντολή επιστρέφουν οι παράμετροι στην προκαθορισμένη τιμή ανάλογα με τη DSCP τιμή.

no random-detect dscp *dscp-value min-threshold max-threshold [max-prob-denominator]*

Στη συνέχεια γίνεται συντακτική ανάλυση της εντολής:

dscp-value	Η DSCP τιμή. Κυμαίνεται από 0 έως και 63 ή μπορεί να είναι μια από τις ακόλουθες λέξεις κλειδιά: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5,cs6, cs7, ef και rsvp.
min-threshold	Το ελάχιστο κατώφλι του αριθμού πακέτων. Η τιμή κυμαίνεται από 1 έως 4096. Όταν το μέσο μέγεθος ουράς φτάσει αυτό τον αριθμό, ο WRED ξεκινάει την τυχαία απόρριψη πακέτων ανάλογα με τη καθορισμένη DSCP τιμή.
max-threshold	Το μέγιστο κατώφλι του αριθμού πακέτων. Η τιμή κυμαίνεται από min-threshold έως 4096. Όταν το μέσο μέγεθος ουράς ξεπεράσει αυτόν τον αριθμό, ο WRED ξεκινάει την απόρριψη όλων των πακέτων με την καθορισμένη DSCP τιμή.
max-prob-denominator	(Προαιρετικό) Εκφράζει το κλάσμα των πακέτων που απορρίπτονται όταν το μέσο μέγεθος ουράς είναι στο μέγιστο κατώφλι. Για παράδειγμα, αν ο παρονομαστής είναι 512, σημαίνει ότι απορρίπτεται ένα ανά 512 πακέτα και ενώ το μέσο μέγεθος ουράς είναι στο max-threshold. Η τιμή του κυμαίνεται από 1 έως 65536 με προκαθορισμένη τιμή το 10 (απορρίπτεται ένα πακέτο ανά 10 στο max-threshold).

Πίνακας 3-15: Προκαθορισμένες dscp Τιμές (PHB τιμές)

DSCP	Minimum Threshold	Maximum Threshold	Mark Probability
af11	32	40	1/10
af12	28	40	1/10
af13	24	40	1/10
af21	32	40	1/10
af22	28	40	1/10
af23	24	40	1/10
af31	32	40	1/10
af32	28	40	1/10
af33	24	40	1/10
af41	32	40	1/10
af42	28	40	1/10
af43	24	40	1/10
cs1	22	40	1/10
cs2	21	40	1/10
cs3	26	40	1/10
cs4	28	40	1/10
cs5	30	40	1/10
cs6	32	40	1/10
cs7	34	40	1/10
ef	36	40	1/10
rsvp	36	40	1/10
default	20	40	1/10

Στον παραπάνω πίνακα παρατηρούμε ότι οι af (assured forwarding, εξασφαλισμένη προώθηση) τιμές χωρίζονται σε τέσσερεις κατηγορίες ως εξής: af1x (υψηλή προτεραιότητα), af2x, af3x, af4x (χαμηλή προτεραιότητα), όπου το «x» δηλώνει τα τρία επίπεδα απόρριψης (τρεις πιθανότητες απόρριψης): Χαμηλό (1), Μεσαίο (2) και Υψηλό (3). Στο Χαμηλό (1) επίπεδο απόρριψης τα πακέτα παραμένουν στην ενδιάμεση μνήμη για μεγάλο χρονικό διάστημα, ενώ στο Υψηλό (3) επίπεδο απόρριψης τα πακέτα εάν δεν μπορούν να εξυπηρετηθούν απορρίπτονται αμέσως. Συνδυαζόμενοι οι δυο αυτοί παράγοντες ορίζουν δώδεκα af τάξεις υπηρεσιών.

Στο αντίστοιχο παράρτημα (Γ) της εργασίας παρατίθεται αναλυτικός πίνακας με τις 64 προκαθορισμένες random-detect dscp τιμές.

Παράδειγμα

Στο ακόλουθο παράδειγμα ενεργοποιείται ο αλγόριθμος WRED έτσι ώστε να χρησιμοποιεί DSCP τιμή την af22.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 256
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp af22 28 40 10
Router(config-if)# service-policy output p1
```

3.4.14 Tail Drop ή WRED

Όπως είδαμε μπορεί να καθοριστεί μια πολιτική τάξης (class policy) που να χρησιμοποιεί είτε tail drop με τη χρήση της εντολής **queue-limit** είτε Weighted Random Early Detection (WRED) με τη χρήση της εντολής **random-detect**. Κατά τη χρήση είτε tail drop είτε WRED υπογραμμίζονται τα ακόλουθα σημεία:

- Οι εντολές **queue-limit** και **random-detect** δεν μπορούν να χρησιμοποιηθούν στο ίδιο class policy, αλλά μπορούν να χρησιμοποιηθούν σε δύο διαφορετικά class policy που ανήκουν στο ίδιο policy map.
- Η εντολή bandwidth μπορεί να διαμορφωθεί όταν σε ένα class policy χρησιμοποιείται είτε η εντολή queue-limit είτε η εντολή random-detect. Η εντολή bandwidth καθορίζει το μέγεθος εύρους ζώνης που διατίθεται για την κλάση.
- Για την προκαθορισμένη default class μπορεί να διαμορφωθεί η εντολή fair-queue (class-default). Η εντολή fair-queue καθορίζει τον αριθμό των δυναμικών ουρών αναμονής για την default class. Η εντολή fair-queue μπορεί να χρησιμοποιηθεί στο ίδιο class policy είτε με την εντολή queue-limit είτε με την random-detect. Δεν μπορεί να χρησιμοποιηθεί με την εντολή bandwidth.

3.4.15 Διαμόρφωση Πολιτικής στην Class-Default Τάξη

Η τάξη class-default χρησιμοποιείται για να ταξινομήσει κίνηση που δεν εμπίπτει σε μια από τις καθορισμένες τάξεις. Μόλις ένα πακέτο ταξινομείται ισχύουν όλοι οι προκαθορισμένοι μηχανισμοί που μπορούν να χρησιμοποιηθούν για τη χρήση διαφοροποιημένων υπηρεσιών. Η τάξη class-default στην πραγματικότητα έχει δημιουργηθεί κατά τη διαμόρφωση του χάρτη πολιτικής, αλλά πρέπει να παραμετροποιηθεί. Από προεπιλογή, στην τάξη class-default έχει καθοριστεί να παρέχει υποστήριξη ο (flow-based) WFQ αλγόριθμος. Ωστόσο η υποστήριξη αυτή αλλάζει όταν διαμορφωθεί η default τάξη με την εντολή bandwidth.

Στη συνέχεια παρουσιάζεται πώς μπορεί να διαμορφωθεί η class-default ώστε να χρησιμοποιεί tail drop.

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# policy-map` *policy-map*	Καθορίζει το όνομα του policy-map
2	`Router(config-pmap)# class class-default` *default-class-name*	Καθορίζει το όνομα της default τάξης που δημιουργείται και περιλαμβάνεται στο service policy.
3	`Router(config-pmap-c)# bandwidth` *bandwidth-kbps* ή `Router(config-pmap-c)# fair-queue` [number-of-dynamic-queues]	Καθορίζει το ποσό του εύρους ζώνης που θα διατεθεί στην τάξη. Το διατιθέμενο εύρος ζώνης θα πρέπει να μπορεί να υποστηρίζει και τις επιβαρύνσεις του Layer 2. Καθορίζει τον αριθμό των δυναμικών ουρών που θα διατεθούν για χρήση,

		από τη flow-based WFQ διαδικασία που εκτελείται στη default τάξη. Ο αριθμός των δυναμικών ουρών εξαρτάται από το bandwidth της διεπαφής, όπως φαίνεται στον επόμενο πίνακα.
4	`Router(config-pmap-c)# **queue-limit** *number-of-packets*`	Καθορίζει το μέγιστο αριθμό πακέτων που μπορούν να ενταχθούν στην ουρά για τη default τάξη.

Ο επόμενος πίνακας καταγράφει τον προεπιλεγμένο αριθμό δυναμικών ουρών που θα διατεθούν για χρήση από τους αλγόριθμους WFQ και CBWFQ, όταν ενεργοποιηθούν σε μια διεπαφή.

Πίνακας 3-16: Προκαθορισμένος Αριθμός Δυναμικών Ουρών ως Συνάρτηση του Εύρους Ζώνης στη Διεπαφή.

Περιοχή Εύρους Ζώνης (Bandwidth Range)	Αριθμός Δυναμικών Ουρών
$64kbps \geq BR$	16
$64kbps \prec BR \leq 128kbps$	32
$128kbps \prec BR \leq 256kbps$	64
$256kbps \prec BR \leq 512kbps$	128
$512kbps \prec BR$	256

Ενώ για να διαμορφωθεί η τάξη class-default ώστε να χρησιμοποιεί WRED packet drop απαιτούνται τα ακόλουθα βήματα.

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# **policy-map** *policy-map*`	Καθορίζει το όνομα του policy-map
2	`Router(config-pmap)# **class class-default** *default-class-name*`	Καθορίζει το όνομα της default τάξης που δημιουργείται και περιλαμβάνεται στο service policy.

3	`Router(config-pmap-c)# **bandwidth** *bandwidth-kbps*`
	
	ή
	
	`Router(config-pmap-c)# **fair-queue** [number-of-dynamic-queues]`
		Καθορίζει το ποσό του εύρους ζώνης που θα διατεθεί στη τάξη. Το διατιθέμενο εύρος ζώνης θα πρέπει να μπορεί να υποστηρίζει και τις επιβαρύνσεις του Layer 2.
		
		Καθορίζει τον αριθμό των δυναμικών ουρών που θα διατεθούν για χρήση, από τη flow-based WFQ διαδικασία που εκτελείται στη default τάξη. Ο αριθμός των δυναμικών ουρών εξαρτάται από το bandwidth της διεπαφής, όπως φαίνεται στον επόμενο πίνακα.

4	`Router(config-pmap-c)# **random-detect**`	Ενεργοποιεί τη WRED διαδικασία. Η πολιτική τάξης απορρίπτει πακέτα με χρήση WRED αντί tail drop.

5	`Router(config-pmap-c)# **random-detect exponential-weighting-constant** *exponent*`
	
	και/ή
	
	`Router(config-pmap-c)# **random-detect precedence** *precedence min-threshold max-threshold mark-prob-denominator*`
		Διαμορφώνει το συντελεστή εκθετικού βάρους που χρησιμοποιείται κατά τον υπολογισμό του μέσου μεγέθους ουράς.
		
		Ρυθμίζει τις παραμέτρους του WRED με ένα συγκεκριμένο IP Precedence. Η εντολή πρέπει να επαναλαμβάνεται για κάθε Precedence.

Παράδειγμα CBWFQ με χρήση WRED Packet Drop

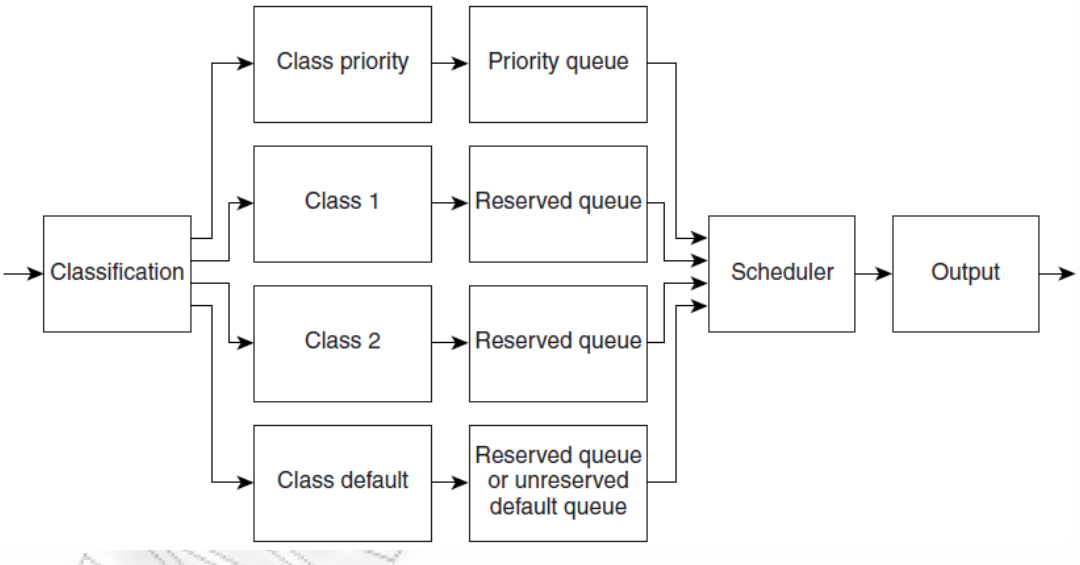
Στο παράδειγμα αυτό θα καθοριστεί μια τάξη με όνομα class1 και στη συνέχεια θα καθοριστεί το όνομα της διεπαφής εισόδου που χρησιμοποιείται σαν κριτήριο προσαρμογής, κατά το οποίο τα πακέτα ελέγχονται για να διαπιστωθεί εάν ανήκουν στην τάξη. (Με άλλα λόγια θα λέγαμε ότι ελέγχονται τα πακέτα που περνάνε από τη διεπαφή εισόδου FastEthernet0/1 αν ανήκουν στη class1). Εν συνεχεία θα οριστεί ένα policy-map με όνομα policy1, το οποίο θα περιέχει τις προδιαγραφές πολιτικής για την τάξη class1, η οποία θα παραμετροποιηθεί για χρήση WRED Packet Drop. Τέλος θα εφαρμοστεί η πολιτική policy1 στη διεπαφή serial0/0.

```
Router(config)# class-map class1
Router(config-cmap)# match input-interface FastEthernet0/1

Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# random-detect

Router(config)# interface serial0/0
Router(config-if)# service-policy output policy1
```

Παράδειγμα διαμόρφωσης LLQ

Έχει ήδη αναφερθεί πως με τη διατήρηση αυστηρής ουράς προτεραιότητας (PQ) για τη CBWFQ κίνηση, διαμορφώνεται ο μηχανισμός Low Latency Queuing (LLQ). Για να γίνει αυτό περισσότερο κατανοητό στη συνέχεια θα παρουσιαστεί ο τρόπος με τον οποίο μπορεί να υλοποιηθεί ο μηχανισμός LLQ.

Εικόνα 3-27: Διαδικασία LLQ



[33]

Στο παραπάνω σχήμα φαίνεται ότι μετά από την ταξινόμηση της κίνησης στη διεπαφή, δημιουργούνται τέσσερεις τάξεις: μια υψηλής προτεραιότητας (Class priority), δυο με δεσμευμένο εύρος ζώνης (Class 1 και Class 2) και η default τάξη (Class default). Η κίνηση της τάξης υψηλής προτεραιότητας τοποθετείται σε μια ουρά προτεραιότητας (PQ), η κίνηση κάθε τάξης με εγγυημένο εύρος ζώνης τοποθετείται σε μια ουρά που εξασφαλίζει εγγυημένο εύρος ζώνης, ενώ η κίνηση της default τάξης μπορεί να τοποθετηθεί σε ουρά που εξασφαλίζει ή όχι εύρος ζώνης. Ο Scheduler βασίζεται στον WFQ αλγόριθμο δίνοντας έτσι σε κάθε ουρά την αντίστοιχη προτεραιότητα.

```
Router(config)# access-list 100 permit udp any any range 16384 32000  #UDP Ports χρήση από VoIP
Router(config)# access-list 100 permit tcp any any eq 1720  #TCP Port για H.323 signaling traffic
Router(config)# access-list 101 permit tcp any any eq 80  #TCP Port για web traffic
Router(config)# access-list 102 permit tcp any any eq 23  #TCP Port για Telnet traffic

Router(config)# class-map voip
Router(config-cmap)# match access-group 100
Router(config)# class-map data1
Router(config-cmap)# match access-group 101
Router(config)# class-map data2
Router(config-cmap)# match access-group 102

Router(config)# policy-map llq
Router(config-pmap)# class voip
Router(config-pmap-c)# priority 32          # Priority Queue για την κίνηση της τάξης voip
Router(config-pmap)# class data1
Router(config-pmap-c)# bandwidth 64         # Reserved queue για την κίνηση της τάξης data1
Router(config-pmap)# class data2
Router(config-pmap-c)# bandwidth 32         # Reserved queue για την κίνηση της τάξης data2
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue           # Fair queue για την κίνηση της τάξης default

Router(config)# interface Serial1/0
Router(config-if)# bandwidth 256            # Συνολικό εύρος ζώνης στη διεπαφή Serial1/0
Router(config-if)# service-policy output llq
```

3.4.16 Αστυνόμευση (Policing)

Η παρακολούθηση της κίνησης ονομάζεται **αστυνόμευση κίνησης** (traffic policing). Σε αντίθεση με τη μορφοποίηση κίνησης (traffic shaping), η αστυνόμευση παίρνει μια ειδική δράση για τη κίνηση εκτός προφίλ πάνω από μια καθορισμένη τιμή. Συνήθως η απόφαση για τη κίνηση που υπερβαίνει μια ορισμένη τιμή είναι η απόρριψη. Ωστόσο, επιτρέπονται και άλλες ενέργειες όπως είναι η εμπιστοσύνη και η σήμανση.

Η αστυνόμευση μπορεί να αποδειχθεί πολύπλοκη διαδικασία. Ουσιαστικά το δίκτυο πρέπει με τη χρήση κατάλληλου αλγορίθμου να επιβεβαιώνει ότι δεν στέλνονται περισσότερα πακέτα ή byte απ όσα επιτρέπονται. Η λειτουργία «αστυνόμευση κίνησης» επιτυγχάνεται με τον **αλγόριθμο κουβά κουπονιών** (token bucket algorithm). Στον αλγόριθμο αυτό ο τρύπιος κουβάς παράγει κουπόνια με ρυθμό ένα κουπόνι ανά ΔΤ sec, ο μετρητής αυξάνεται κάθε ΔΤ και μειώνεται κάθε φορά που στέλνεται ένα πακέτο. Όταν ο μετρητής πάρει τιμή ίση με μηδέν δεν μπορούν να σταλθούν πακέτα. Στη παραλλαγή μέτρησης σε byte, ο μετρητής αυξάνει κατά *K* byte κάθε ΔΤ sec και μειώνεται κατά τόσα byte όσα το μήκος του πακέτου που στέλνεται. Ουσιαστικά επιτρέπει ριπές αλλά μέχρι ένα ορισμένο μέγιστο μήκος.

Ο υπολογισμός της διάρκειας ριπής μέγιστου ρυθμού μετάδοσης πραγματοποιείται ως εξής: Αν ονομάσουμε τη διάρκεια της ριπής *S* sec, τη χωρητικότητα του κουβά κουπονιών *C* byte, το ρυθμό άφιξης κουπονιών *ρ* byte/sec και το μέγιστο ρυθμό εξόδου *M* byte/sec, συμπεραίνουμε ότι μια ριπή εξόδου περιέχει το πολύ (*C+ρ*S*) byte. Επίσης ο αριθμός των byte σε μια ριπή μέγιστης ταχύτητας μήκους *S* sec είναι ίσος με *M*S*. Συνεπώς ισχύει ότι:

$$C + \rho S = MS \Rightarrow S = \frac{C}{M - \rho},\ \gamma\iota\alpha\ \rho \prec \mathrm{M}$$

Η εντολή police

Η διαμόρφωση «αστυνόμευσης κίνησης» σε έναν Cisco router επιτυγχάνεται με την εντολή **police**. Ενώ η κατάργησή της από τον προγραμματισμό της συσκευής επιτυγχάνεται με την εντολή **no police** όπως παρακάτω.

```
police bps [burst-normal] [burst-max] conform-action action exceed-action action
[violate-action action]
```

```
no police bps [burst-normal] [burst-max] conform-action action exceed-action action
[violate-action action]
```

Στη συνέχεια γίνεται συντακτική ανάλυση της εντολής:

bps	Μέσος ρυθμός, σε bps. Αποδεκτές τιμές από 8000 έως 200000000.
burst-normal	(Προαιρετικό) Φυσιολογικό μέγεθος ριπής, σε bytes. Αποδεκτές τιμές από 1000 έως 51200000. Προκαθορισμένη τιμή 1500.
burst-max	(Προαιρετικό) Μέγιστο μέγεθος ριπής, σε bytes. Αποδεκτές τιμές από 1000 έως 51200000. Προκαθορισμένη τιμή ανάλογα την πλατφόρμα.
conform-action	Καθορίζει τη δράση που εφαρμόζεται στο πακέτο όταν συμμορφώνεται με το όριο ρυθμού.
exceed-action	Καθορίζει τη δράση που εφαρμόζεται στο πακέτο όταν υπερβαίνει το όριο ρυθμού.
violate-action	(Προαιρετικό) Καθορίζει τη δράση που εφαρμόζεται στο πακέτο όταν παραβιάζει το Φυσιολογικό και Μέγιστο μέγεθος ριπής.
action	Δράσεις που εφαρμόζονται στο πακέτο. Καθορίζονται ακολούθως: • **drop** – Απόρριψη πακέτου. • **set-cos-transmit** *value* – ορίζει τιμή COS για το πακέτο και το στέλνει. • **set-dscp-transmit** *value* – ορίζει τιμή DSCP για το πακέτο και το στέλνει με τη νέα τιμή. • **set-prec-transmit** *value* - ορίζει τιμή IP Precedence για το πακέτο και το στέλνει με τη νέα τιμή. • **transmit** – Μεταδίδει αμετάβλητο το πακέτο.

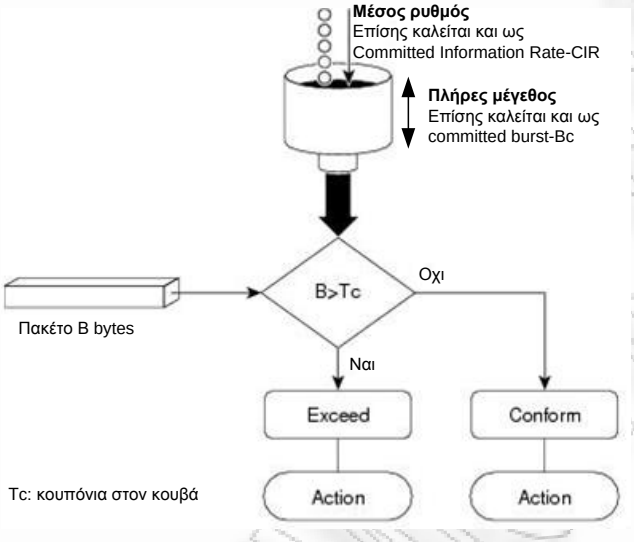
Μπορούν να οριστούν έως τέσσερεις δράσεις ταυτόχρονα, αλλά δεν πρέπει να είναι συγκρουόμενες μεταξύ τους, π.χ. οι **conform-action transmit** και **conform-action drop**.

Όπως ήδη έχει αναφερθεί, η λειτουργία «αστυνόμευση κίνησης» επιτυγχάνεται με τον **αλγόριθμο κουβά κουπονιών** (token bucket algorithm). Στο λειτουργικό σύστημα της Cisco υποστηρίζονται δυο τύποι του αλγορίθμου αυτού: Ο αλγόριθμος με μονό κουβά κουπονιών (single-token bucket) και ο αλγόριθμος με διπλό κουβά κουπονιών (tow-token bucket). Ο πρώτος χρησιμοποιείται όταν η επιλογή **violate-action** δεν προσδιορίζεται, ενώ ο δεύτερος χρησιμοποιείται όταν η επιλογή **violate-action** προσδιορίζεται.

3.4.17 Αλγόριθμος Κουβά Κουπονιών με Ένα Κουβά

Ο conform bucket (κουβάς συμμόρφωσης) έχει οριστεί αρχικά σε πλήρες μέγεθος (το πλήρες μέγεθος είναι ο αριθμός των bytes που προσδιορίζεται σαν «Φυσιολογικό μέγεθος ριπής»)

Εικόνα 3-28: Αλγόριθμος Κουβά Κουπονιών με ένα Κουβά



[57]

Όταν ένα πακέτο συγκεκριμένου μεγέθους (για παράδειγμα B bytes) φτάνει σε συγκεκριμένο χρόνο (χρόνος T) συμβαίνουν οι ακόλουθες ενέργειες:

- Ενημερώνονται τα κουπόνια στον conform bucket. Αν η προηγουμένη άφιξη πακέτου ήταν τη χρονική στιγμή T1 και η τρέχουσα ώρα είναι T, τότε ο κουβάς ενημερώνεται με την αντίστοιχη (T-T1) αξία σε bytes βασισμένη στο ρυθμό άφιξης κουπονιών.

  Ο τρόπος υπολογισμού του ρυθμού άφιξης κουπονιών παρουσιάζεται στη συνέχεια:

  $$\textit{ρυθμός άφιξης κουπονιών σε bytes} = [(\mathrm{T}-\mathrm{T1})(\mathrm{sec}) * \textit{Μέσο ρυθμό } (bps)] * \frac{1byte}{8bits}$$

  Για παράδειγμα αν ο μέσος ρυθμός αστυνόμευσης είναι 512000 bps και ο τυπικός χρόνος πλήρους διαδρομής είναι 1.5 sec, στο χρονικό διάστημα αυτό θα υπάρξει άφιξη κουπονιών ίση με 1.5*512000*(1/8)=96000 byte.

- Αν ο αριθμός των bytes που υπάρχουν στον conform bucket είναι περισσότερα ή ίσα με το μέγεθος του πακέτου, το πακέτο «συμμορφώνεται» και η αντίστοιχη δράση συμμόρφωσης (conform-action) εφαρμόζεται σε αυτό. Συνεπώς B bytes μετακινούνται από τον conform bucket και η δράση συμμόρφωσης ολοκληρώνεται για το πακέτο.

- Αν ο αριθμός των bytes που υπάρχουν στον conform bucket (μετά την αφαίρεση των B Bytes του πακέτου) είναι μικρότερος από μηδέν τότε η αντίστοιχη δράση υπέρβασης (exceed-action) εφαρμόζεται στο πακέτο.

Παράδειγμα υλοποίησης Αλγόριθμου Κουβά Κουπονιών με ένα Κουβά Κουπονιών

Το ακόλουθο παράδειγμα δείχνει πώς καθορίζεται η τάξη κίνησης (με τη χρήση της εντολής **class-map**) και πώς συνδέονται τα κριτήρια προσαρμογής από την τάξη κίνησης με την αστυνόμευση της κίνησης, η οποία έχει διαμορφωθεί στην υπηρεσία πολιτικής (με τη χρήση της εντολής **policy-map**). Στη συνέχεια χρησιμοποιείται η εντολή **service-policy** για να επισυναφτούν οι υπηρεσίες πολιτικής στη διεπαφή.

Σε αυτό το συγκεκριμένο παράδειγμα, η κίνηση αστυνόμευσης έχει καθοριστεί με μέσο ρυθμό τα 8000 bps και φυσιολογικό μέγεθος ριπής τα 1000 bytes για όλα τα πακέτα που εξέρχονται από τη διεπαφή fastethernet 0/0.

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

Αρχικά ο conform bucket έχει οριστεί σε πλήρες μέγεθος ίσο με 1000 bytes. Αν ένα πακέτο 450 bytes φτάσει στον μηχανισμό αστυνόμευσης, το πακέτο συμμορφώνεται διότι υπάρχουν αρκετά ελεύθερα bytes, δηλαδή αρκετά κουπόνια στον κουβά. Άρα το πακέτο αποστέλλεται (conform-action transmit) και κατά συνέπεια αφαιρούνται 450 byte από τον κουβά (άρα απομένουν 550 bytes).

Αν το επόμενο πακέτο φτάσει 0.25 sec αργότερα, στον κουβά κουπονιών θα προστεθούν (0.25*8000)/8=250 bytes, άρα συνολικά θα υπάρχουν 550+250=800 bytes. Αν το πακέτο αυτό είναι 900 bytes, τότε θα «υπερβαίνει» διότι στον κουβά υπάρχουν μόνο 800 bytes με αποτέλεσμα να εφαρμόζεται σε αυτό δράση απόρριψης (exceed-action drop).

3.4.18 Αλγόριθμος Κουβά Κουπονιών με Δυο Κουβάδες και ένα Ρυθμό

Ο αλγόριθμος με διπλό κουβά κουπονιών χρησιμοποιείται όταν στην εντολή **police** προσδιορίζεται η επιλογή **violate-action**.

Ο conform bucket (που είναι ο πρώτος κουβάς) έχει οριστεί αρχικά σε πλήρες μέγεθος (το πλήρες μέγεθος είναι ο αριθμός των bytes που προσδιορίζεται σαν «Φυσιολογικό μέγεθος ριπής»)

Ο exceed bucket (που είναι ο δεύτερος κουβάς) έχει οριστεί αρχικά σε πλήρες μέγεθος (το πλήρες μέγεθος για το δεύτερο κουβά είναι ο αριθμός των bytes που προσδιορίζεται σαν «Μέγιστο μέγεθος ριπής»).

Τα κουπόνια και στους δυο κουβάδες ενημερώνονται βάσει του ρυθμού άφιξης κουπονιών ή δεσμευμένου ρυθμού πληροφορίας (Committed Information Rate-CIR).

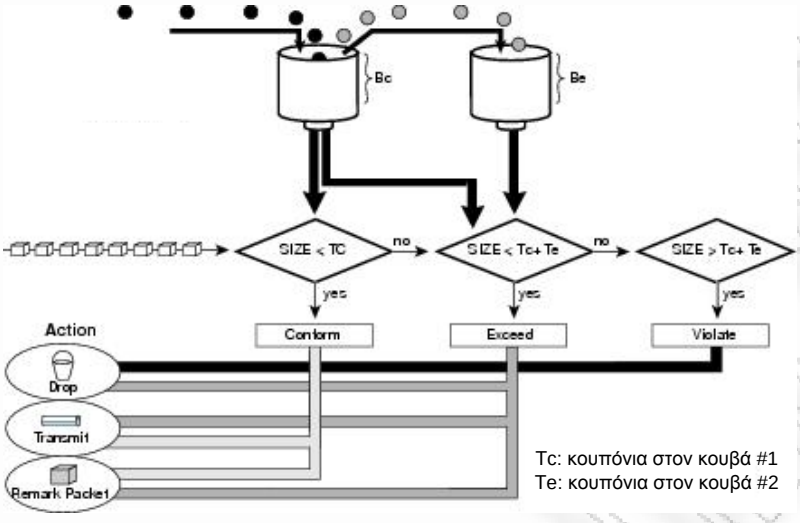
Όταν ένα πακέτο, συγκεκριμένου μεγέθους (για παράδειγμα B bytes), φτάνει σε συγκεκριμένο χρόνο (χρόνος T), συμβαίνουν οι ακόλουθες ενέργειες:

- Ενημερώνονται τα κουπόνια στον conform bucket. Αν η προηγουμένη άφιξη πακέτου ήταν τη χρονική στιγμή T1 και η τρέχουσα ώρα είναι T, τότε ο κουβάς ενημερώνεται με την αντίστοιχη (T-T1) αξία σε bytes βασισμένη στο ρυθμό άφιξης κουπονιών. Αν με την προσθήκη των κουπονιών υπερχειλίσει ο πρώτος κουβάς, τότε τα πλεονάζοντα κουπόνια τοποθετούνται στο δεύτερο κουβά.

  Ο τρόπος υπολογισμού του ρυθμού άφιξης κουπονιών παρουσιάζεται στη συνέχεια:

$$\textit{ρυθμός άφιξης κουπονιών σε bytes} = [(\mathrm{T}-\mathrm{T1})(\mathrm{sec}) * \textit{Μέσο ρυθμό (bps)}] * \frac{1byte}{8bits}$$

Εικόνα 3-29: Αλγόριθμος Κουβά Κουπονιών με Δυο Κουβάδες Κουπονιών



[55]

- Αν ο αριθμός των bytes που υπάρχουν στον conform bucket είναι περισσότερα ή ίσα με το μέγεθος του πακέτου, το πακέτο «συμμορφώνεται» και η αντίστοιχη δράση συμμόρφωσης (conform-action) εφαρμόζεται σε αυτό. Συνεπώς B bytes μετακινούνται από τον conform bucket και η δράση συμμόρφωσης ολοκληρώνεται για το πακέτο. Ο δεύτερος κουβάς παραμένει αμετάβλητος σε αυτό το σενάριο.
- Αν ο αριθμός των bytes στον conform bucket (πρώτος κουβάς) είναι μικρότερος από το μέγεθος του πακέτου, τότε ο δεύτερος κουβάς κουπονιών ελέγχεται από το πακέτο για bytes. Αν ο αριθμός των bytes στον exceed bucket είναι μεγαλύτερος ή ίσος με B (μέγεθος πακέτου), η αντίστοιχη exceed δράση εφαρμόζεται και B bytes αφαιρούνται από το δεύτερο κουβά κουπονιών. Δε μετακινούνται bytes προς τον πρώτο κουβά.
- Αν ο αριθμός των bytes στον exceed bucket είναι μικρότερος από το μέγεθος του πακέτου, το πακέτο παραβιάζει το ρυθμό και η αντίστοιχη δράση (violate-action) εφαρμόζεται στο πακέτο. Η δράση για το πακέτο έχει ολοκληρωθεί.

Παράδειγμα υλοποίησης Αλγόριθμου Κουβά Κουπονιών με Δυο Κουβάδες

Σε αυτό το συγκεκριμένο παράδειγμα, η κίνηση αστυνόμευσης έχει καθοριστεί με μέσο ρυθμό τα 8000 bps, φυσιολογικό μέγεθος ριπής (normal burst size) τα 1000 byte και υπερβάλλον μέγεθος ριπής (excess burst size) 1000 bytes, για όλα τα πακέτα που εξέρχονται από τη διεπαφή fastethernet 0/0.

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-dscp-transmit 26 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

Αρχικά ο conform bucket έχει οριστεί σε πλήρες μέγεθος ίσο με 1000 bytes. Αν ένα πακέτο 450 bytes φτάσει στον μηχανισμό αστυνόμευσης, τότε αυτό «συμμορφώνεται» διότι υπάρχουν αρκετά ελεύθερα bytes, δηλαδή αρκετά κουπόνια στον κουβά. Άρα το πακέτο αποστέλλεται (conform-action transmit) και κατά συνέπεια αφαιρούνται 450 bytes από τον κουβά (άρα απομένουν 550 bytes).

Αν το επόμενο πακέτο φτάσει 0.25 sec αργότερα, στον πρώτο κουβά κουπονιών θα προστεθούν (0.25*8000)/8=250 bytes, άρα συνολικά θα υπάρχουν 550+250=800 bytes. Αν το πακέτο αυτό είναι 900 bytes θα έχει σαν αποτέλεσμα τη μη «συμμόρφωσή» του διότι στον conform bucket υπάρχουν μόνο 800 bytes.

Ο exceed bucket, ο οποίος έχει οριστεί αρχικά σε πλήρες μέγεθος (όπως καθορίζεται από το υπερβάλλον μέγεθος ριπής) ίσο με 1000 bytes, ελέγχεται για διαθέσιμα bytes. Επειδή υπάρχουν αρκετά διαθέσιμα bytes στο δεύτερο κουβά κουπονιών, εφαρμόζεται η exceed δράση (ορίζει τιμή DSCP ίση με 26 για το πακέτο και το στέλνει με τη νέα τιμή), αφαιρούνται 900 bytes από τον κουβά και κατά συνέπεια απομένουν 100 bytes σε αυτόν.

Αν το επόμενο πακέτο φτάσει 0.40 sec αργότερα, θα προστεθούν στους κουβάδες κουπονιών (0.40*8000)/8=400 bytes. Ως εκ τούτου ο conform bucket θα έχει τώρα 800+200=1000 bytes (δηλαδή περιέχει το μέγιστο αριθμό κουπονιών που επιτρέπεται να υπάρχουν στον πρώτο κουβά) και τα υπόλοιπα πλεονάζοντα 200 bytes τοποθετούνται στο δεύτερο κουβά. Μετά την προσθήκη των υπερχειλισμένων κουπονιών στον exceed bucket, ο συνολικός αριθμός τους θα είναι 100+200=300 bytes.

Αν το μέγεθος του πακέτου που φθάνει είναι 1000 bytes, το πακέτο «συμμορφώνεται» διότι υπάρχουν αρκετά διαθέσιμα bytes στον πρώτο κουβά κουπονιών. Η conform δράση εφαρμόζεται στο πακέτο (conform-action transmit) και 1000 bytes αφαιρούνται από τον πρώτο κουβά (αφήνοντας 0 bytes).

Αν το επόμενο πακέτο φτάσει 0.20 sec αργότερα, θα προστεθούν στον πρώτο κουβά κουπονιών (0.20*8000)/8=200 bytes. Ως εκ τούτου ο conform bucket έχει 200 bytes. Αν το μέγεθος του πακέτου που φθάνει είναι 400 bytes, το πακέτο δε συμμορφώνεται (conform) διότι στον πρώτο κουβά υπάρχουν διαθέσιμα μόνο 200 bytes. Ομοίως, το πακέτο δεν υπερβαίνει (exceed) διότι μόνο 300 bytes είναι διαθέσιμα στον exceed bucket. Ως εκ τούτου το πακέτο «παραβιάζει» και η δράση παραβίασης εφαρμόζεται σε αυτό (violate-action drop).

3.4.19 Αλγόριθμος Κουβά Κουπονιών με Δυο Κουβάδες και Δυο Ρυθμούς

Η διαμόρφωση «αστυνόμευσης κίνησης» σε έναν Cisco router όταν υφίστανται δυο ρυθμοί, ο committed information rate (CIR) και ο peak information rate (PIR) επιτυγχάνεται με την εντολή **police**. Ενώ η κατάργησή της από τον προγραμματισμό της συσκευής επιτυγχάνεται με την εντολή **no police** όπως παρακάτω.

```
police cir cir [bc conform-burst] [pir pir] [be peak-burst] [conform-action action
[exceed-action action [violate-action action]]]

no police cir
```

Στη συνέχεια γίνεται συντακτική ανάλυση της εντολής:

cir	Δεσμευμένος ρυθμός πληροφορίας (Committed information rate-CIR), με τον οποίο ο πρώτος κουβάς κουπονιών ενημερώνεται.
cir	Προσδιορίζει την τιμή CIR σε bps. Αποδεκτές τιμές από 8000 έως 200000000.
bc	(Προαιρετικό) Μέγεθος συμμορφωμένης ριπής (conform burst) που χρησιμοποιείται από τον πρώτο κουβά για αστυνόμευση.
conform-burst	(Προαιρετικό) Προσδιορίζει την τιμή bc σε bytes. Αποδεκτές τιμές από 1000 έως 51200000.
pir	(Προαιρετικό) Μέγιστος ρυθμός πληροφορίας (Peak information rate-PIR), με τον οποίο ο δεύτερος κουβάς κουπονιών ενημερώνεται.
pir	(Προαιρετικό) Προσδιορίζει την τιμή PIR σε bps. Αποδεκτές τιμές από 8000 έως 200000000.

be	(Προαιρετικό) Μέγεθος ακραίας ριπής (Peak burst) που χρησιμοποιείται από το δεύτερο κουβά για αστυνόμευση.
peak-burst	(Προαιρετικό) Προσδιορίζει την τιμή be σε bytes. Αποδεκτές τιμές: Το μέγεθος ποικίλει ανάλογα με τη διεπαφή και την πλατφόρμα.
conform-action	(Προαιρετικό) Καθορίζει τη δράση που εφαρμόζεται στο πακέτο όταν αυτό συμμορφώνεται με τα CIR και PIR.
exceed-action	(Προαιρετικό) Καθορίζει τη δράση που εφαρμόζεται στο πακέτο όταν αυτό συμμορφώνεται με το PIR αλλά όχι με το CIR.
violate-action	(Προαιρετικό) Καθορίζει τη δράση που εφαρμόζεται στο πακέτο όταν αυτό υπερβαίνει το PIR.
action	Δράσεις που εφαρμόζονται στο πακέτο. Καθορίζονται ακολούθως: • **drop** – Απόρριψη πακέτου. • **set-cos-transmit** *value* – ορίζει τιμή COS για το πακέτο και το στέλνει. • **set-dscp-transmit** *value* – ορίζει τιμή DSCP για το πακέτο και το στέλνει με τη νέα τιμή. • **set-prec-transmit** *value* - ορίζει τιμή IP Precedence για το πακέτο και το στέλνει με τη νέα τιμή. • **transmit** – Μεταδίδει αμετάβλητο το πακέτο.

Διαμορφωση Προτεραιοτητας με Ρητη Τιμη Ρυθμου Αστυνομευσης

Όταν διαμορφώνεται μια τάξη προτεραιότητας με ρητή τιμή ρυθμού αστυνόμευσης, η κίνηση περιορίζεται στο ρυθμό αστυνόμευσης ανεξάρτητα από τις συνθήκες συμφόρησης. Με άλλα λόγια ακόμα και αν υπάρχει διαθέσιμο εύρος ζώνης, η κίνηση προτεραιότητας δεν μπορεί να υπερβαίνει τον προκαθορισμένο ρυθμό αστυνόμευσης που ρητά έχει καθοριστεί.

Στο ακόλουθο παράδειγμα η κίνηση προτεραιότητας περιορίζεται σε δεσμευμένο ρυθμό ίσο με 1000 kbps ανεξάρτητα από τις συνθήκες συμφόρησης στο δίκτυο:

```
Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police cir 1000000 conform-action transmit exceed-action drop
```

Όπως έχουμε δει, για την αστυνόμευση της κίνησης δυο ανεξάρτητων ρυθμών χρησιμοποιούνται δυο κουβάδες κουπονιών (T_c και T_p). Στη συνέχεια παρουσιάζονται ορισμένα σημαντικά σημεία:

Κουβάδες Κουπονιών

- Ο T_c κουβάς κουπονιών ενημερώνεται με βάση το Δεσμευμένο Ρυθμό Πληροφορίας (CIR) κάθε στιγμή που ένα πακέτο φτάνει προς έλεγχο. Τα περιεχόμενα του T_c κουβά κουπονιών μπορεί να είναι το πολύ ίσα με την τιμή B_c.
- Ο T_p κουβάς κουπονιών ενημερώνεται με βάση το Μέγιστο Ρυθμό Πληροφορίας (PIR) κάθε στιγμή που ένα πακέτο φτάνει προς έλεγχο. Τα περιεχόμενα του T_p κουβά κουπονιών μπορεί να είναι το πολύ ίσα με την τιμή B_e.

Ενημέρωση Κουβάδων

Το ακόλουθο σενάριο παρουσιάζει πώς ενημερώνονται οι κουβάδες κουπονιών:

Έστω ότι τη χρονική στιγμή t φτάνει ένα πακέτο B Bytes. Και ότι το τελευταίο πακέτο έχει φτάσει τη χρονική στιγμή t_1. Τα CIR και PIR τη χρονική στιγμή t εκπροσωπούνται από τις Tc(t) και Tp(t) αντίστοιχα. Με βάση το παραπάνω σενάριο οι κουβάδες ενημερώνονται ως ακολούθως:

$$Tc(t) = \min(CIR * (t - t_1) + Tc(t_1),\ Bc)$$
$$Tp(t) = \min(PIR * (t - t_1) + Tp(t_1),\ Be)$$

Σήμανση Κίνησης

Ένα πακέτο κατά τον έλεγχο μπορεί να σημανθεί με «συμμόρφωση», «υπέρβαση» ή «παραβίαση» του προκαθορισμένου ρυθμού. Στη συνέχεια περιγράφεται πώς επιτυγχάνεται η σήμανση ενός πακέτου B Bytes:

- Αν B>Tp(t), το πακέτο σηματοδοτείται με ένδειξη «παραβίασης» του προκαθορισμένου ρυθμού.
- Αν B>Tc(t), το πακέτο σηματοδοτείται με ένδειξη «υπέρβασης» του προκαθορισμένου ρυθμού και ο Tp(t) κουβάς κουπονιών ενημερώνεται ως ακολούθως:

  $$Tp(t) = Tp(t) - B$$

  Αλλιώς, το πακέτο χαρακτηρίζεται με «συμμόρφωση» στον προκαθορισμένο ρυθμό και οι δυο κουβάδες κουπονιών ενημερώνονται ως εξής:

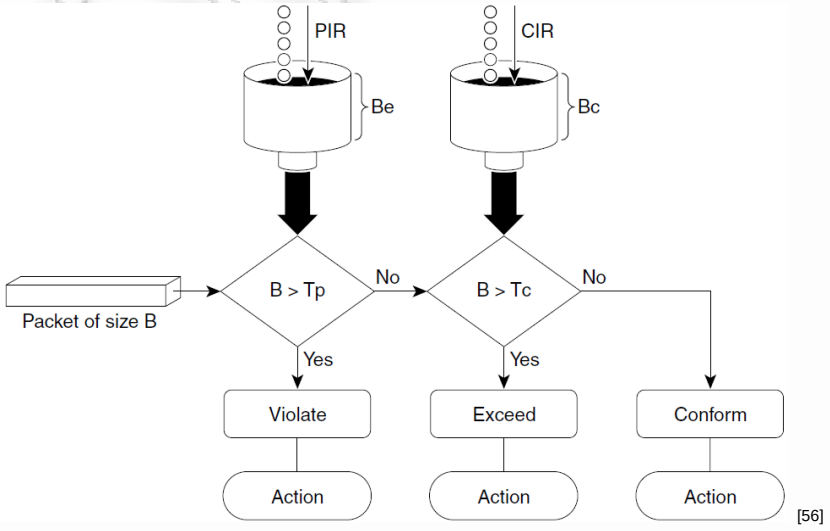
  $$Tp(t) = Tp(t) - B$$
  $$Tc(t) = Tc(t) - B$$

Για παράδειγμα αν το CIR είναι 100 kbps και το PIR είναι 200 kbps και μια ροή δεδομένων με ρυθμό 250 kbps φτάσει στον έλεγχο, το πακέτο θα πρέπει να φέρει την ακόλουθη σήμανση:

- 100 kbps θα χαρακτηριστούν με «συμμόρφωση» προς το ρυθμό.
- 100 kbps θα χαρακτηριστούν με «υπέρβαση» προς το ρυθμό.
- 50 kbps θα χαρακτηριστούν με «παραβίαση» προς το ρυθμό.

Στο επόμενο σχήμα παρουσιάζεται σχηματικά η διαδικασία σήμανσης ενός πακέτου καθώς και πως εφαρμόζεται η αντίστοιχη δράση σε αυτό.

Εικόνα 3-30: Αλγόριθμος Κουβά Κουπονιών με Δυο Κουβάδες Κουπονιών και Δυο Ρυθμούς



[56]

Παράδειγμα υλοποίησης Αλγόριθμου Κουβά Κουπονιών με Δυο Κουβάδες και Δυο Ρυθμούς.

Στο παρακάτω παράδειγμα έχει διαμορφωθεί η εφαρμογή αστυνόμευσης σε μια τάξη για περιορισμό της κίνησης με ένα μέσο δεσμευμένο ρυθμό τα 500 kbps και μέγιστο ρυθμό το 1 Mbps.

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action transmit
exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
```

3.4.20 Aggregate Policer

Μέχρι τώρα η εφαρμογή της αστυνόμευσης πραγματοποιείται ανά διεπαφή (Individual policer). Υπάρχει η δυνατότητα να εφαρμοστεί συγκεντρωτικά σε μια ομάδα διεπαφών με τη βοήθεια της εντολής ***mls qos aggregate-policer***. Για παράδειγμα, ο ορισμός ενός ***aggregate-policer*** για τον περιορισμό της συνολικής κίνησης μιας ομάδας διεπαφών έως 75 Mbps, θα έχει ως αποτέλεσμα, η ομάδα των διεπαφών να μπορεί να επιτύχει μόνο 75 Mbps μεταξύ όλων των μελών.

Ο ορισμός ενός aggregate-policer για χρήση σε χάρτες πολιτικής πραγματοποιείται με την εντολή **mls qos aggregate-policer**. Ενώ η κατάργηση της από τον προγραμματισμό της συσκευής επιτυγχάνεται με την εντολή **no mls qos aggregate-policer** όπως παρακάτω:

```
mls qos aggregate-policer name rate-bps [normal-burst-bytes [maximum-burst-bytes | pir
peak-rate-bps | action-type action]]

no mls qos aggregate-policer name
```

Στη συνέχεια γίνεται συντακτική ανάλυση της εντολής:

name	Το όνομα του aggregate policer.
rate-bps	Μέγιστος αριθμός bits ανά sec. Αποδεκτές τιμές από 32000 έως 10000000000.
normal-burst-bytes	(Προαιρετικό) Φυσιολογικό μέγεθος ριπής, σε bytes. Αποδεκτές τιμές από 1000 έως 31250000.
maximum-burst-bytes	(Προαιρετικό) Μέγιστο μέγεθος ριπής, σε bytes. Αποδεκτές τιμές από 1000 έως 31250000 (αν εισαχθεί τιμή, πρέπει να οριστεί ίση με το *normal-burst-bytes*).
pir *peak-rate-bps*	(Προαιρετικό) Μέγιστος ρυθμός πληροφορίας (Peak information rate-PIR). Αποδεκτές τιμές από 32000 έως 10000000000. Προκαθορισμένα είναι ίσο με το CIR.
action-type action	Δράσεις που εφαρμόζονται. Καθορίζονται ακολούθως: **conform-action** – δράση που εφαρμόζεται όταν ο ρυθμός δεν «υπερβαίνει»: • **drop** – Απόρριψη πακέτου. • **set-cos-transmit** *value* – ορίζει τιμή COS για το πακέτο

	και το στέλνει. • **set-dscp-transmit** *value* – ορίζει τιμή DSCP για το πακέτο και το στέλνει με τη νέα τιμή. • **set-prec-transmit** *value* - ορίζει τιμή IP Precedence για το πακέτο και το στέλνει με τη νέα τιμή. • **transmit** – Μεταδίδει αμετάβλητο το πακέτο. **exceed-action** – δράση που εφαρμόζεται όταν οι QoS τιμές «υπερβαίνουν»: • **drop** – Απόρριψη πακέτου. • **set-dscp-transmit** *value* – ορίζει τιμή DSCP για το πακέτο και το στέλνει με τη νέα τιμή. • **transmit** – Μεταδίδει αμετάβλητο το πακέτο. **violate-action** – δράση που εφαρμόζεται όταν οι QoS τιμές «παραβιάζουν»: • **drop** – Απόρριψη πακέτου. • **set-dscp-transmit** *value* – ορίζει τιμή DSCP για το πακέτο και το στέλνει με τη νέα τιμή. • **transmit** – Μεταδίδει αμετάβλητο το πακέτο.

3.4.21 Σήμανση (Marking)

Στο ακόλουθο παράδειγμα θα γίνει κατανοητός ο τρόπος διαμόρφωσης σήμανσης της κίνησης βασισμένη στη τιμή του DSCP.

```
Router(config)# access-list 100 permit udp any any range 16384 32000  ! UDP Ports για VoIP
Router(config)# access-list 100 permit tcp any any eq 1720      ! TCP Port 1720 για H.323 κίνηση σηματοδοσίας
Router(config)# access-list 101 permit tcp any any eq 80        ! TCP Port 80 για web traffic

Router(config)# class-map voip
Router(config-cmap)# match access-group 100
Router(config)# class-map webtraffic
Router(config-cmap)# match access-group 101

Router(config)# policy-map dscp_marking
Router(config-pmap)# class voip
Router(config-pmap-c)# set ip dscp 46  ! EF Class
Router(config-pmap)# class webtraffic
Router(config-pmap-c)# set ip dscp 26  ! AF Class

Router(config)# interface Ethernet0/0
Router(config-if)# service-policy input dscp_marking
```

Σε αυτό το παράδειγμα όλη η κίνηση που φτάνει στη διεπαφή Ethernet0/0 ελέγχεται και ταξινομείται με βάση τα class-map voip και webtraffic. Ο χάρτης πολιτικής dscp_marking ορίζει τιμή DSCP ίση με 46 (101110 για EF) για την τάξη voip και 26 (011010 για AF3) για τη τάξη webtrafic.

Γενικά για τη διαμόρφωση σήμανσης ως μέλος ενός policy-map, μπορεί να χρησιμοποιηθεί μια από τις ακόλουθες εντολές, ανάλογα με την εφαρμογή:

set ip dscp ip-dscp-value

set ip precedence ip-precedence-value

set cos *cos-value*

όπου είναι:

ip-dscp-value	Η τιμή IP DSCP. Κυμαίνεται από 0 έως και 63
ip-precedence-value	Ο αριθμός IP Precedence. Κυμαίνεται από 0 έως και 7
cos-value	Η τιμή CoS Layer 2, IEEE 802.1Q. Κυμαίνεται από 0 έως και 7

Το προηγούμενο παράδειγμα μπορεί να μετατραπεί ως ακολούθως με χρήση της τιμής IP Precedence:

```
Router(config)# access-list 100 permit udp any any range 16384 32000
Router(config)# access-list 100 permit tcp any any eq 1720
Router(config)# access-list 101 permit tcp any any eq 80

Router(config)# class-map voip
Router(config-cmap)# match access-group 100
Router(config)# class-map webtraffic
Router(config-cmap)# match access-group 101

Router(config)# policy-map IPP_marking
Router(config-pmap)# class voip
Router(config-pmap-c)# set ip precedence 5
Router(config-pmap)# class webtraffic
Router(config-pmap-c)# set ip precedence 3

Router(config)# interface Ethernet0/0
Router(config-if)# service-policy input IPP_marking
```

3.4.22 Μορφοποίηση Κίνησης

Η «μορφοποίηση» χρησιμοποιείται για την εξομάλυνση της κίνησης από την πλευρά του διακομηστή, με επίτευξη περιορισμού του άνω ορίου του εύρους ζώνης. Για παράδειγμα, σε μια τοπολογία δικτύου ο κορμός του δικτύου έχει συνήθως διασυνδέσεις υψηλής χωρητικότητας (π.χ. E1) ενώ οι περιφερειακές διασυνδέσεις έχουν συγκριτικά χαμηλό εύρος ζώνης (π.χ. 384 kbps). Σ' αυτή την περίπτωση είναι πιθανό η κίνηση που προέρχεται από μια κεντρική διασύνδεση του δικτύου να υπερχειλίσει τις χαμηλής χωρητικότητας διασυνδέσεις στα άκρα (υποκαταστήματα). Η μορφοποίηση, λοιπόν, είναι ένας καλός τρόπος ώστε να «συντονιστεί» η κυκλοφορία των πακέτων στα 384 kbps και να αποφευχθεί έτσι η υπερχείλιση. Τα πλεονάζοντα πακέτα που προκύπτουν από τη διαδικασία μορφοποίησης αποθηκεύονται σε περιοχή προσωρινής αποθήκευσης και εκπέμπονται αργότερα, διατηρώντας την ομαλή ροή της κυκλοφορίας.

Η αστυνόμευση (policing) όπως ήδη έχει αναφερθεί, είναι μια παρεμφερής διαδικασία, παρόλα αυτά διαφέρει σημαντικά σε ένα σημείο: τα πακέτα υπερχείλισης δεν αποθηκεύονται αλλά απορρίπτονται.

Στη συνέχεια θα γίνει κατανοητός ο τρόπος διαμόρφωσης του μηχανισμού «Traffic Shaping» σε έναν Cisco δρομολογητή. Θα αναφερθούν οι διαδικασίες εφαρμογής Generic Traffic Shaping-GTS[7] και Class-Based Shaping.

[7] GTS δεν υποστηρίζεται σε ISDN διεπαφές.

3.4.23 Generic Traffic Shaping

Η εφαρμογή GTS στην εξερχόμενη κίνηση μιας διεπαφής επιτυγχάνεται με την ακόλουθη εντολή:

```
traffic-shape rate bit-rate [burst-size[excess-burst-size]]
```

Η εφαρμογή GTS στην εξερχόμενη κίνηση μιας λίστας πρόσβασης επιτυγχάνεται με την ακόλουθη διαδικασία:

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# access-list access-list-number`	Αναθέτει την κίνηση σε μια λίστα πρόσβασης.
2	`Router(config)# interface interface-type interface-number`	Καθορίζει τον τύπο και το όνομα της διεπαφής.
3	`Router(config-if)# traffic-shape group access-list bit-rate [burst-size[excess-burst-size]]`	Διαμορφώνει τη μορφοποίηση της εξερχόμενης κίνησης σε μια διεπαφή για την καθορισμένη λίστα πρόσβασης.

Παράδειγμα ενεργοποίησης GTS σε διεπαφή

Στο ακόλουθο παράδειγμα παρουσιάζεται ο τρόπος παραμετροποίησης για επίτευξη μορφοποίησης της κίνησης σε δυο διεπαφές ενός δρομολογητή. Η διεπαφή Ethernet0 διαμορφώνεται ώστε να περιορίζει τη UDP κίνηση στο 1 Mbps, ενώ η διεπαφή Ethernet1 διαμορφώνεται ώστε να περιορίζει τη συνολική εξερχόμενη κίνηση στα 5 Mbps.

```
Router(config)# access-list 101 permit udp any any

Router(config)# interface Ethernet0
Router(config-if)# traffic-shape group 101 1000000 125000 125000

Router(config)# interface Ethernet1
Router(config-if)# traffic-shape rate 5000000 625000 625000
```

Τα αποτελέσματα της παραπάνω διαμόρφωσης στο δρομολογητή μπορούν να γίνουν ορατά με τις ακόλουθες εντολές παρακολούθησης:

```
Router(config-if)# show traffic-shape
```

```
Interface   Ethernet0

       Access Target    Byte   Sustain   Excess    Interval  Increment    Adapt
VC     List   Rate      Limit  bits/int  bits/int  (ms)      (bytes)      Active
-      101    1000000   31250  125000    125000    125       15625        -

Interface   Ethernet1

       Access Target    Byte   Sustain   Excess    Interval  Increment    Adapt
VC     List   Rate      Limit  bits/int  bits/int  (ms)      (bytes)      Active
-             5000000   156250 625000    625000    125       78125          –
```

Ο δρομολογητής εσωτερικά υπολογίζει τις παραπάνω τιμές ως εξής:

Για παράδειγμα στο Interface Ethernet1 ισχύει:

$$Target\ Rate = CIR = 5000000bps$$

$$Sustain = Bc = 625000bits$$

$$Excess = Be = 625000bits$$

$$Byte\ Limit = Bc + Be = \frac{625000}{8} + \frac{625000}{8} = 156250Byte$$

$$Interval = Tc = \frac{Bc}{CIR} = \frac{625000bits}{5000000\,bits/\sec} = 125ms$$

$$Increment = Tc * CIR = 0{,}125\sec * 5000000\,bit/\sec = 625000bits = 78125Bytes$$

```
Router(config-if)# show traffic-shape statistics
```

I/F	Access List	Queue Depth	Packets	Bytes	Packets Delayed	Bytes Delayed	Shaping Active
Et0	101	0	2	180	0	0	no
Et1		0	0	0	0	0	no

3.4.24 Class-Based Shaping

Για επίτευξη Μορφοποίησης Βάσει Τάξεως εξυπηρέτησης της κίνησης, απαιτούνται τα ακόλουθα βήματα εντολών:

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# policy-map policy-map`	Καθορίζει το όνομα του χάρτη πολιτικής που πρέπει να δημιουργηθεί ή να τροποποιηθεί.
2	`Router(config)# class-map class-map-name`	Καθορίζει το όνομα του class-map.
3	`Router(config-pmap-c)# shape {average | peak} cir [bc] [be]`	Καθορίζει το μέσο ή ακραίο ρυθμό μορφοποίησης.
4	`Router(config-pmap-c)# shape max-buffers number-of-buffers`	Καθορίζει το μέγιστο αριθμό ενταμιευτών (buffers) που επιτρέπονται στις ουρές.

Παράδειγμα Class-Based Shaping

Το ακόλουθο παράδειγμα ορίζει μια τάξη c1 , η οποία έχει ρυθμιστεί για μορφοποίηση της κίνησης στα 384 kbps, με φυσιολογικό μέγεθος ριπής 15440 bits.

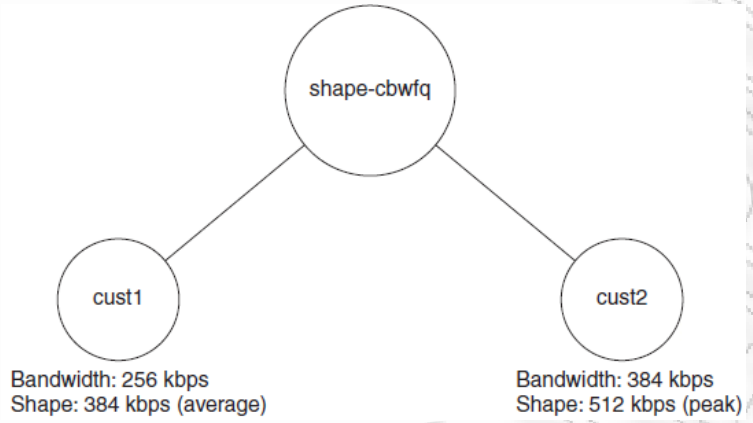
```
Router(config)# policy-map shape
Router(config-pmap)# class c1
Router(config-pmap-c)# shape average 384000 15440
Router(config-pmap-c)# configure terminal
Router(config)# interface Serial 3/3
Router(config-if)# service out shape
```

Παράδειγμα υλοποίησης CBWFQ σε σύζευξη με GTS

Για το ακόλουθο παράδειγμα, εφαρμόζεται στη διεπαφή ο αλγόριθμος προγραμματισμού εκπομπής πακέτων CBWFQ και η κίνηση μορφοποιείται πριν μπει στην ουρά του CBWFQ. Καθορίζονται δυο τάξεις, εκ των οποίων η πρώτη καλείται cust1 και είναι υπεύθυνη για τη διασφάλιση εύρους ζώνης 256 kbps και τη μορφοποίηση της εξόδου στα 384 kbps. Ενώ η δεύτερη τάξη καλείται cust2 και είναι υπεύθυνη για τη διασφάλιση εύρους ζώνης ίσο με 384 kbps. Στην περίπτωση που υπάρχει αρκετό διαθέσιμο εύρος ζώνης στη διεπαφή η τάξη μπορεί να επιτύχει διεκπεραιωτική ικανότητα έως 512 kbps.

Στη συνέχεια παρουσιάζεται σχηματικά το παράδειγμα.

Εικόνα 3-31: CBWFQ σε Σύζευξη με GTS



[5]

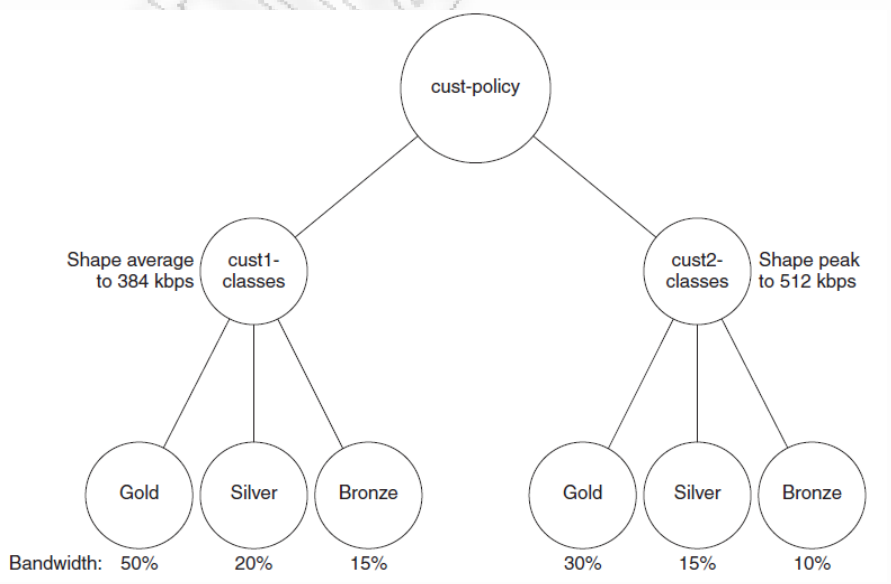
Οι εντολές που απαιτούνται για τη διαμόρφωση του παραδείγματος είναι οι ακόλουθες:

```
Router(config)# policy-map shape-cbwfq
Router(config-pmap)# class cust1
Router(config-pmap-c)# shape average 384000
Router(config-pmap-c)# bandwidth 256
Router(config-pmap)# class cust2
Router(config-pmap-c)# shape peak 512000
Router(config-pmap-c)# bandwidth 384
Router(config-pmap-c)# configure terminal
Router(config)# interface Serial 3/3
Router(config-if)# service out shape-cbwfq
```

Παράδειγμα υλοποίησης CBWFQ μέσα σε GTS

Στη συνέχεια παρουσιάζεται σχηματικά το παράδειγμα που θα υλοποιηθεί:

Εικόνα 3-32: Υλοποίησης CBWFQ Μέσα σε GTS



[5]

Από το σχήμα γίνεται φανερό πως πρέπει να διαμορφωθούν ιεραρχικά οι χάρτες πολιτικής και να υλοποιηθεί CBWFQ διαμόρφωση μέσα σε GTS.

Οι εντολές που απαιτούνται για τη διαμόρφωση του παραδείγματος είναι οι ακόλουθες:

Διαμόρφωση cust1-classes

```
Router(config)# policy-map cust1-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 15
```

Διαμόρφωση cust2-classes

```
Router(config)# policy-map cust2-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 15
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 10
```

Διαμόρφωση Customer Policy και χαρακτηριστικών QoS

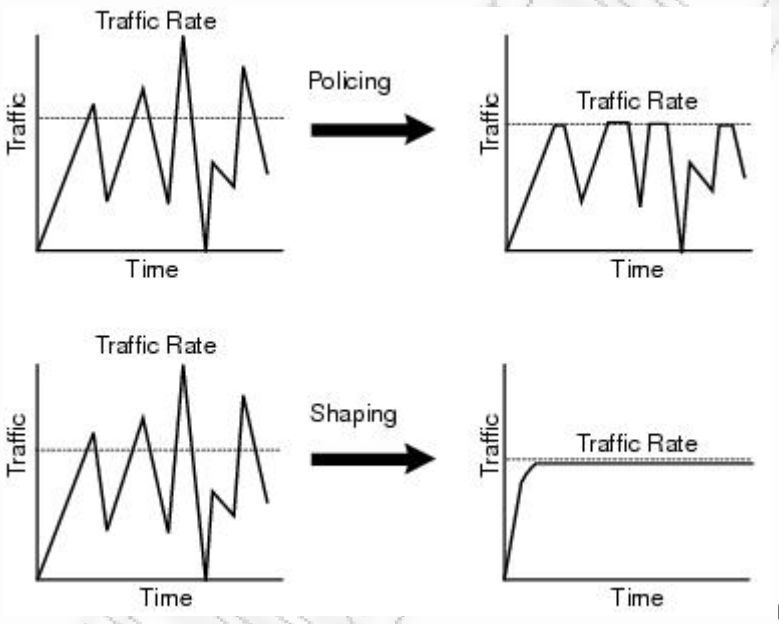
```
Router(config)# policy-map cust-policy
Router(config-pmap)# class cust1
Router(config-pmap-c)# shape average 384000
Router(config-pmap-c)# service-policy cust1-classes
Router(config-pmap)# class cust2
Router(config-pmap-c)# shape peak 512000
Router(config-pmap-c)# service-policy cust2-classes
Router(config-pmap-c)# interface Serial 3/2
Router(config-if)# service out cust-policy
```

3.4.25 Σύγκριση Αστυνόμευσης – Μορφοποίησης

Το ακόλουθο διάγραμμα παρουσιάζει τις σημαντικές διαφορές μεταξύ των μεθόδων Αστυνόμευσης και Μορφοποίησης της κίνησης.

Στην αστυνόμευση όταν ο ρυθμός κίνησης φτάσει το διαμορφωμένο μέγιστο ρυθμό, η κίνηση που υπερβαίνει το ρυθμό αυτό απορρίπτεται ή σηματοδοτείται ξανά. Αυτό, καθώς και το γεγονός ότι κατά την αστυνόμευση διαδίδονται ριπές κίνησης, έχει σαν αποτέλεσμα εξόδου την πριονωτή μορφή του διαγράμματος κίνησης. Σε αντίθεση με την αστυνόμευση, η μορφοποίηση διατηρεί τα περίσσια πακέτα σε μια ουρά (γεγονός που προϋποθέτει την ύπαρξη αρκετής μνήμης) και προγραμματίζει την μετέπειτα μετάδοσή τους φυσικά με κάποια χρονική επιβάρυνση. Αυτή η λειτουργία προγραμματισμού επιτρέπει την οργάνωση της μορφοποίησης μέσα σε διαφορετικές ουρές. Το αποτέλεσμα της μορφοποίησης είναι η εξομάλυνση του ρυθμού εξόδου των πακέτων όπως παρουσιάζεται στη συνέχεια.

Εικόνα 3-33: Σύγκριση Αστυνόμευσης – Μορφοποίησης



[55]

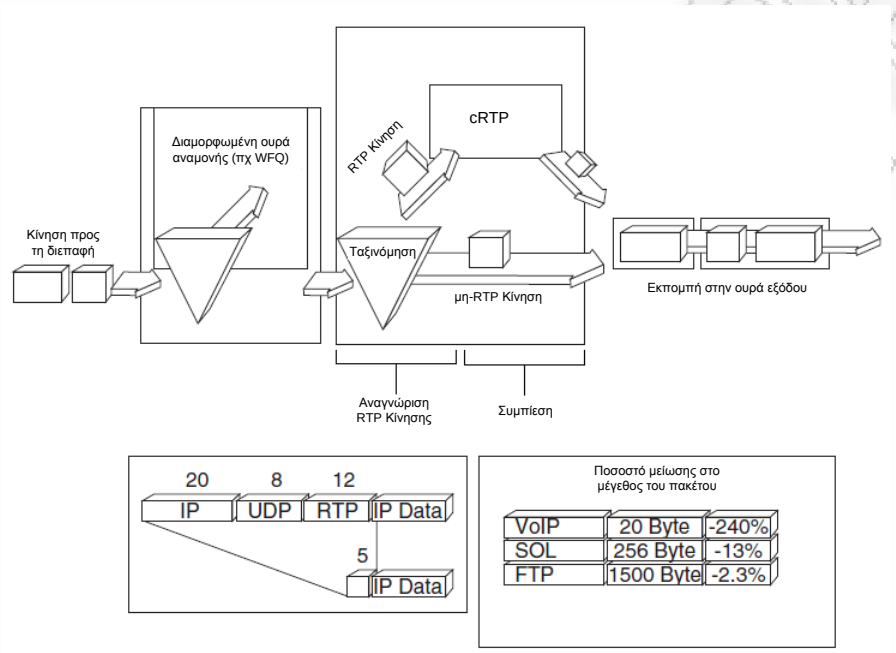
Μια επιπλέον σημαντική διαφορά και κατά συνέπεια κριτήριο επιλογής είναι ότι η αστυνόμευση μπορεί να εφαρμοστεί σε μια διεπαφή εισερχόμενης αλλά και εξερχόμενης κίνησης, σε αντίθεση με τη μορφοποίηση που μπορεί να εφαρμοστεί μόνο σε διεπαφή εξερχόμενης κίνησης.

3.4.26 Μηχανισμός Συμπίεσης Κεφαλίδας cRTP

Η παραμετροποίηση του cRTP σε έναν δρομολόγητή επιτυγχάνεται με την εντολή ***ip rtp header-compression*** όταν αφορά σειριακή διεπαφή ή με την εντολή ***frame-relay ip rtp header-compression*** όταν αφορά Frame Relay υποδιεπαφή.

Στη συνέχεια παρουσιάζεται γραφικά ο μηχανισμός συμπίεσης κεφαλίδας, cRTP:

Εικόνα 3-34: Μηχανισμός Συμπίεσης Κεφαλίδας cRTP



[33]

Επειδή η διαδικασία συμπίεσης επιβαρύνει την CPU του δρομολογητή, μπορεί να παραμετροποιηθεί ο συνολικός αριθμός RTP ή/και TCP συνδέσεων όπου πραγματοποιείται συμπίεση κεφαλίδας με τις ακόλουθες αντίστοιχες εντολές:

Πίνακας 3-17: Εντολές Καθορισμού Συνολικού Αριθμού RTP, TCP Συνδέσεων όπου Μπορεί να Πραγματοποιείται Συμπίεση Κεφαλίδας σε μια Διεπαφή.

Εντολή	Επεξήγηση
`Router(config-if)# ip rtp compression-connections number`	Καθορίζει το συνολικό αριθμό RTP συνδέσεων όπου πραγματοποιείται συμπίεση κεφαλίδας, σε μια διεπαφή.
`Router(config-if)# ip tcp compression-connections number`	Καθορίζει το συνολικό αριθμό TCP συνδέσεων όπου πραγματοποιείται συμπίεση κεφαλίδας, σε μια διεπαφή.

Από προεπιλογή, σε Frame Relay ενθυλάκωση έχει καθοριστεί να μπορούν να πραγματοποιούνται έως και 256 cTCP συνδέσεις. Η μέγιστη τιμή είναι προκαθορισμένη και δεν επιτρέπεται η παραμετροποίησή της. Αντίθετα η παραμετροποίηση αυτή, επιτρέπεται σε PPP ή High-Level Data Link Control (HDLC) ενθυλάκωση. Συγκεκριμένα, από προεπιλογή ισχύει ότι η μέγιστη τιμή είναι 32 cTCP και 32 cRTP (16 κλήσεις) όπου μπορούν να αυξηθούν έως τη μέγιστη τιμή 256 cTCP και 1000 cRTP αντίστοιχα σε μια διεπαφή.

3.4.27 Κατακερματισμός και Παρεμβολή Συνδέσμου

Όπως είδη έχει αναφερθεί, οι δύο τεχνικές που εφαρμόζονται για την υλοποίηση του μηχανισμού είναι:

1. Multilink Point-to-Point Protocol (MLP) Link Fragmentation and Interleaving (LFI) για Leased Lines και ATM.
2. Frame Relay Fragmentation (FRF.12) για Frame Relay.

Παράδειγμα υλοποίησης:

Στο παράδειγμα που ακολουθεί θα γίνει εφαρμογή της πρώτης τεχνικής υλοποίησης που αναφέρθηκε. Σε point-to-point συριακές συνδέσεις πρώτα απαιτείται η ενεργοποίηση του MLP (*ppp multilink*). Έπειτα πρέπει να καθοριστεί σε msec το μέγεθος κατακερματισμού των τεμαχίων (*ppp multilink fragment-delay 10*). Υπενθυμίζεται ότι ένα 10 msec τεμάχιο ή τμήμα είναι ο αριθμός των bytes που μπορούν να σταλούν πάνω από τη συγκεκριμένη ζεύξη σε χρόνο 10 msec. Τέλος απαιτείται να ενεργοποιηθεί η Παρεμβολή Συνδέσμου (interleave) στη multilink διεπαφή (*ppp multilink interleave*). Κατά αυτόν τον τρόπο επιτυγχάνεται ο κατακερματισμός των πακέτων στο ένα άκρο της σύνδεσης και η συγκέντρωσή τους στο άλλο άκρο. Είναι δυνατό να συνδυάζονται πολλές συνδέσεις και να ενεργούν ως ένας μεγάλος εικονικός σωλήνας-ζεύξη.

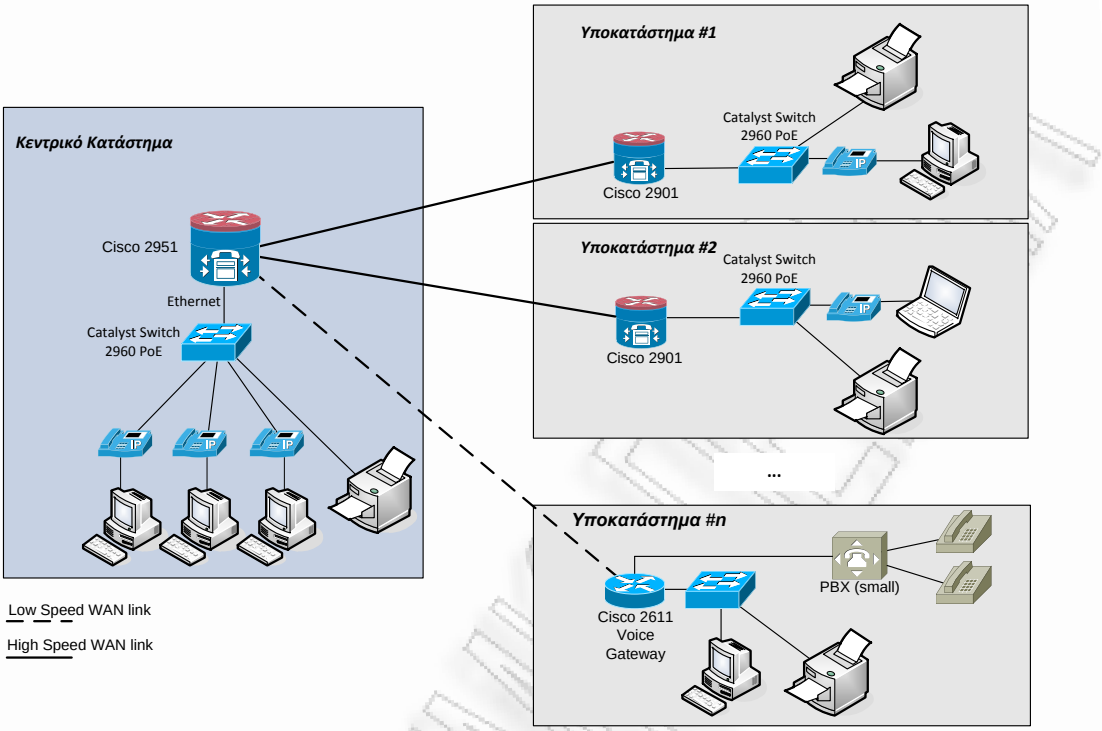
```
Router> enable
Router# configure terminal
Router(config)# interface Multilink1
Router(config-if)# ip address 10.1.1.1 255.255.255.252
Router(config-if)# bandwidth 256
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink fragment-delay 10
Router(config-if)# ppp multilink interleave
Router(config-if)# exit
Router(config)# multilink-group 1
```

3.4.28 Παράδειγμα Διαμόρφωσης QoS για VoIP πάνω από PPP WAN Ζεύξεις

Για το παράδειγμα υποθέτουμε πως μια εταιρία θέλει να εντάξει στο τηλεπικοινωνιακό της δίκτυο μια νέα μικρή εταιρία την οποία αγόρασε πρόσφατα. Όπως απεικονίζεται και στην Εικόνα 3-32 η διασύνδεση του νέου υποκαταστήματος (#**n**) με το κεντρικό μπορεί να γίνει δυστυχώς μόνο μέσω μιας ζεύξης χαμηλής ταχύτητας (πχ υποθέτουμε 64 Kbps). Μια από τις τηλεπικοινωνιακές απαιτήσεις είναι η μετάδοση φωνής πάνω από τη ζεύξη. Ως εκ τούτου θα πρέπει να εφαρμοστούν όλες οι κατάλληλες τεχνικές που θα προστατεύουν τα «ευαίσθητα» πακέτα ώστε να εξασφαλιστεί η ποιοτική επικοινωνία μεταξύ των συνομιλητών.

Στο παράδειγμα της επόμενης σελίδας φαίνεται η διαδικασία υλοποίησης όλων αυτών των απαραίτητων QoS χαρακτηριστικών:

Εικόνα 3-35: Σχήμα Παραδείγματος, VoIP over PPP WAN Ζεύξη Χαμηλής Ταχύτητας



Εντολές	Περιγραφή

`class-map voip`
` match ip precedence 5`
!
	Δημιουργία της Τάξης *voip*, για τα «ευαίσθητα» πακέτα φωνής που είναι χαρακτηρισμένα με: ip precedence 5.

`class-map webtraffic`
` match ip precedence 3`
!
	Δημιουργία της Τάξης *webtraffic* για τα πακέτα της διαδικτυακής κίνησης που είναι χαρακτηρισμένα με: ip precedence 3.

`policy-map llq`
` class voip`
`  priority 64`
` class webtraffic`
`  bandwidth 64`
` class class-default`
`  fair-queue`
!
	Δημιουργία πολιτικής: Στην κίνηση φωνής δίνεται αυστηρή προτεραιότητα (PQ) με εγγυημένο εύρος ζώνης 64 Kbps σε περίπτωση συμφόρησης, ενώ για τη διαδικτυακή κίνηση καθορίζεται το ποσό του εύρους ζώνης που μπορεί να διατεθεί ίσο με 64 Kbps. Όλη η άλλη κίνηση μοιράζεται το υπόλοιπο εύρος ζώνης.

`interface Serial1/0`
` bandwidth 256`
` encapsulation ppp`
` no fair-queue`
` ppp multilink`
` multilink-group 1`
!
	Ένταξη της σειριακής διεπαφής (*Serial1/0*) στην πολυζευκτική διεπαφή της ομάδας 1 (*multilink-group 1*).
	Παρατήρηση: Για ταχύτητες ζεύξης μεγαλύτερες από 1.2 Mbps, δεν απαιτείται εφαρμογή Multilink PPP LFI και cRTP. Σε αυτή την περίπτωση οι δηλώσεις *ip address* και *service-policy* πάνε κάτω από τη διαμόρφωση του *serial interface*.

`interface Multilink1`
` ip address 10.1.1.1 255.255.255.252`
` bandwidth 256`
!
	Διαμόρφωση Multilink PPP LFI για ζεύξη χαμηλής ταχύτητας.

`ip rtp header-compression iphc-format`
`ip tcp header-compression iphc-format`
!
	Διαμόρφωση του cRTP μηχανισμού με σκοπό τη μείωση του απαιτούμενου εύρους ζώνης για κάθε φωνητική κλήση.

`ppp multilink` ` ppp multilink fragment-delay 10`	Το μέγεθος κατακερματισμού τεμαχίων ορίζεται ίσο με 10 msec.
` ppp multilink interleave`	Ενεργοποίηση της Παρεμβολής Συνδέσμου (interleave)

`multilink-group 1`
` service-policy output llq`
!
	Εφαρμογή της llq πολιτικής (υπεύθυνη να εξυπηρετεί κατάλληλα την εξερχόμενη κίνηση) στην πολυζευκτική διεπαφή (multilink interface).

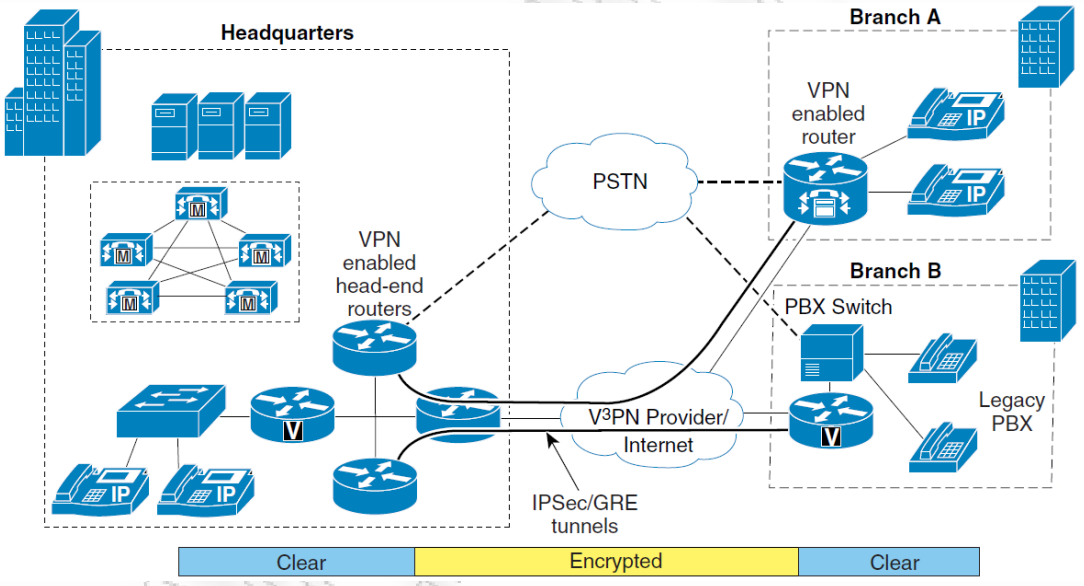
3.5 Σχεδιασμός QoS για IPsec VPNs

3.5.1 Εισαγωγή

Με τη βοήθεια των IPsec VPNs επιτυγχάνεται ο διαχωρισμός του δικτύου και το απόρρητο μέσω της κρυπτογράφησης. Τα IPsec VPNs που δημιουργούνται μέσω του Provider/Internet καλύπτουν από σημείο προς σημείο την ασφαλή επικοινωνία μέσω Layer-3 κρυπτογραφημένων σηράγγων (tunnels). Η διαδικασία της Κρυπτογράφησης, Αποκρυπτογράφησης υλοποιείται στα τελικά σημεία της σήραγγας και η προστατευμένη κίνηση διαβιβάζεται σε όλο το δίκτυο παρέχοντας έτσι μεγαλύτερο επίπεδο ασφάλειας στις φωνητικές συνομιλίες.

Από την Εικόνα 3-36 γίνεται φανερό πως το βασικό μοντέλο ανάπτυξης μένει αμετάβλητο, με τη μόνη διαφορά ότι η σύνδεση της κεντρικής τοποθεσίας με τα υποκαταστήματα υλοποιείται μέσω VPN σηράγγων. Έτσι η κίνηση σηματοδοσίας (όπως το H.323) και η κίνηση φωνής στέλνεται κρυπτογραφημένη μέσω της VPN (IPSec/GRE) σήραγγας στο πρόγραμμα διαχείρισης κλήσεων που βρίσκεται στο κεντρικό κατάστημα. Ωστόσο, ούτε τα IP τηλέφωνα, ούτε το πρόγραμμα διαχείρισης κλήσεων, ούτε οι φωνητικές εφαρμογές, όπως για παράδειγμα ένας διακομηστής φωνητικού ταχυδρομείου, γνωρίζουν ούτε και πρέπει να γνωρίζουν ότι η πληροφορία τους θα μεταφερθεί κρυπτογραφημένη μέσω VPN σηράγγων.

Εικόνα 3-36: IP Τηλεφωνία μέσω VPN



[4]

Όμως η διαδικασία της κρυπτογράφησης μέσω VPN σηράγγων, δημιουργεί ορισμένες νέες παραμέτρους όπου μπορούν να επηρεάσουν την ποιότητα της επικοινωνίας. Τα βασικά QoS ζητήματα που σχετίζονται με τα IPsec VPNs αναφέρονται στη συνέχεια:

1. Το επιπλέον εύρος ζώνης που απαιτείται για την IPsec κρυπτογράφηση (encryption) και πιστοποίηση (authentication).
2. Η απαιτούμενη οριακή χρονική τιμή καθυστέρησης σε κάθε σημείο όπου πραγματοποιείται κρυπτογράφηση ή αποκρυπτογράφηση.
3. Προστασία από επιθέσεις επανάληψης (Anti-Replay).

3.5.2 IPsec Επιβαρύνσεις Εύρους Ζώνης

Κατά το σχεδιασμό και την υλοποίηση QoS πολιτικών είναι απαραίτητο να λαμβάνεται υπόψη το επιπλέον εύρος ζώνης που απαιτείται για την κρυπτογράφηση και πιστοποίηση ενός πακέτου. Η επιβάρυνση αυτή κρίνεται ιδιαίτερα σημαντική στη VoIP τηλεφωνία, όπου όπως θα γίνει φανερό και στη συνέχεια, θα μπορούσε ακόμα και να διπλασιάσει το μέγεθος ενός πακέτου φωνής G.729.

Στο Layer-3 ο ρυθμός μετάδοσης δεδομένων για μια VoIP κλήση με χρήση του G.729 (50 pps) είναι 24 Kbps. Η χρήση του IP Generic Routing Encapsulation (GRE[8]) επιβαρύνει κάθε πακέτο κατά 24 bytes, ενώ η χρήση IPsec Encapsulating Security Payload (ESP[9]) προσθέτει άλλα 52 bytes αντίστοιχα. Η συνδυασμένη πρόσθετη επιβάρυνση αυξάνει τον ρυθμό από 24 Kbps (καθαρή φωνή) σε 56 Kbps (IPSec ESP Tunnel mode encrypted voice).

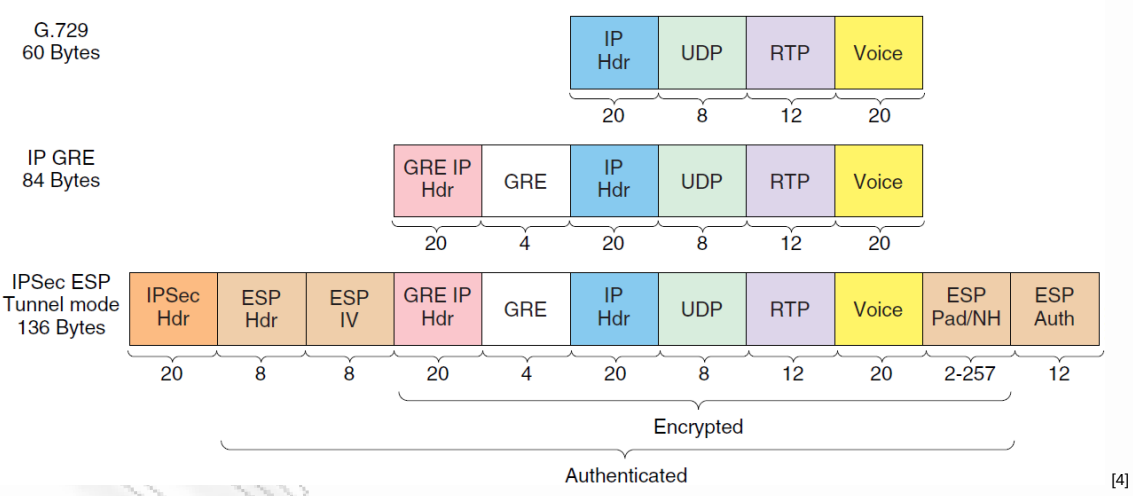
Ο υπολογισμός παρουσιάζεται συνοπτικά στη συνέχεα:

60 bytes ανά πακέτο (G.729 voice)
24 bytes ανά πακέτο (επιβάρυνση IP GRE)
\+ 52 bytes ανά πακέτο (επιβάρυνση IPsec ESP)
= 136 bytes ανά πακέτο
× 8 bits ανά byte
= 1088 bits ανά πακέτο
× 50 πακέτα ανά sec
=54.400 bps = 54.4 Kbps

Συνεπώς κατά την κρυπτογράφηση μιας G.729 κλήσης δημιουργείται πρόσθετη επιβάρυνση ίση με 227%.

Στην επόμενη εικόνα παρουσιάζεται η ανατομία ενός IPsec-Κρυπτογραφημένου πακέτου φωνής (G.729):

Εικόνα 3-37: Ανατομία IPsec-Κρυπτογραφημένου VoIP (G.729) πακέτου



[4]

Πρέπει να σημειωθεί πως αυτές οι καταχωρίσεις εύρους ζώνης προκύπτουν μόνο από τις Layer-3 απαιτήσεις και δεν περιλαμβάνουν τις Layer-2 επιβαρύνσεις. Ως εκ τούτου, η Layer-

[8] Η χρήση IPSec με GRE σήραγγες είναι απαραίτητη όταν απαιτείται IP Multicast.
[9] Το IPSec μπορεί να παρέχει κρυπτογράφηση στο επίπεδο δικτύου με: α. Το Authentication Header (AH) που παρέχει πιστοποίηση δεδομένων και προστασία από επιθέσεις επανάληψης. Και β. Το Encapsulation Security Payload (ESP) που παρέχει πιστοποίηση δεδομένων, εμπιστευτικότητα και προστασία από επιθέσεις επανάληψης.

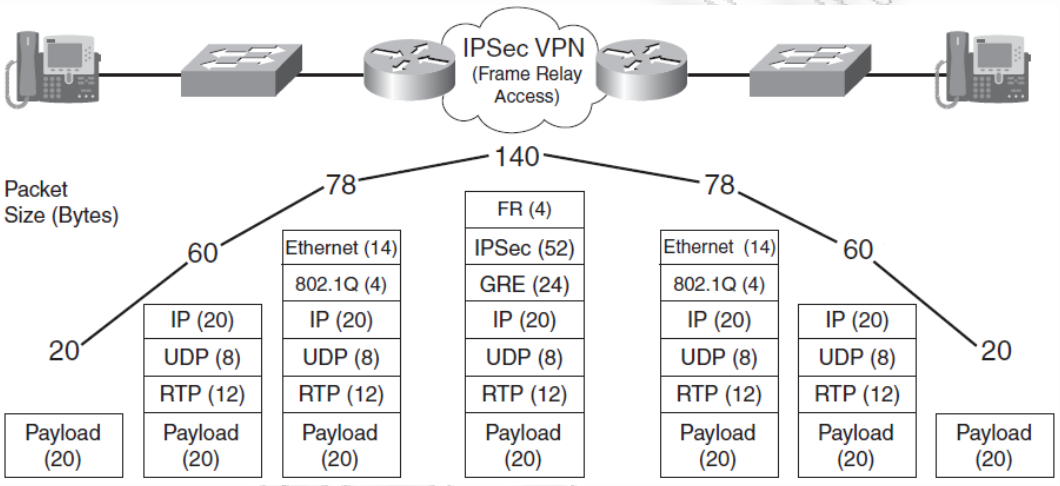
2 επιβάρυνση πρέπει να προστεθεί στην κορυφή των Layer-3 απαιτήσεων εύρους ζώνης για παροχή LLQ και CBWFQ. Στην Εικόνα 3-38 φαίνεται πρώτα η προσθήκη και έπειτα η αφαίρεση των Ethernet (Ethernet + 802.1Q ζεύξης) και Frame Relay επιβαρύνσεων.

Οι βασικές τιμές Layer-2 επιβάρυνσης παρουσιάζονται στον πίνακα που ακολουθεί:

Πίνακας 3-18: Layer-2 Επιβάρυνση Ενθυλάκωσης

Layer-2 Ενθυλάκωση	Επιβάρυνση
Ethernet	14 bytes (+ 4 για 802.1Q)
Frame Relay	4 bytes (+ 4 για FRF.12)
MLP	10 bytes (+ 3 για MLP LFI)
ATM	5 bytes ανά 53-byte cell + cell padding
PPP, HDLC	4 bytes

Εικόνα 3-38: Μεταβολές Μεγέθους (bytes) ενός G.729 IPsec-Encrypted Πακέτου



[43]

Ως εκ τούτου, ο τρόπος υπολογισμού της επιβάρυνσης, συμπεριλαμβανομένης και αυτής του Layer-2, παρουσιάζεται μέσω του επόμενου παραδείγματος. Υποτίθεται ότι θα πραγματοποιείται μια VoIP (G.729) κλήση, κρυπτογραφημένη μέσω μιας αργής σύνδεσης (≤768 Kbps, Frame Relay Link), όπου απαιτείται FRF.12 Κατακερματισμός και Παρεμβολή Συνδέσμου (LFI).

60 bytes ανά πακέτο (G.729 voice)
24 bytes ανά πακέτο (επιβάρυνση IP GRE)
52 bytes ανά πακέτο (επιβάρυνση IPsec ESP)
4 bytes ανά πακέτο (επιβάρυνση FR)
\+ 4 bytes ανά πακέτο (επιβάρυνση FRF.12)
= 144 bytes ανά πακέτο
× 8 bits ανά byte
= 1152 bits ανά πακέτο
× 50 πακέτα ανά sec
=57.600 bps ≃ 58 Kbps

Εν ολίγοις, σε IPsec-Encrypted εφαρμογές είναι σημαντικό πάντα να συνυπολογίζονται οι Layer-2 επιβαρύνσεις για τον ακριβή υπολογισμό παροχής εύρους ζώνης.

Όπως φαίνεται στον Πίνακα 3-19, το ποσοστό των LLQ απαιτήσεων για μια κρυπτογραφημένη κλήση φωνής σε ζεύξεις χαμηλής χωρητικότητας όπως 64, 128 και 256 Kbps, υπερβαίνει το συνιστώμενο όριο του 33%. Συνεπώς οι επιχειρήσεις που επιθυμούν κρυπτογραφημένες κλήσεις φωνής πάνω από ζεύξεις χαμηλής χωρητικότητας θα πρέπει να αναγνωρίζουν και τις επιπτώσεις στην κυκλοφορία των υπολοίπων δεδομένων που διέρχονται από αυτές τις συνδέσεις. Στην περίπτωση όπου αυτό δε μπορεί να γίνει αποδεκτό, συνιστάται να αυξηθεί η χωρητικότητα των γραμμών μεταφοράς έτσι ώστε οι κρυπτογραφημένες κλήσεις να υπάγονται στον κανόνα του 33% και κατά συνέπεια να μην δημιουργούνται σοβαρές καθυστερήσεις στα δεδομένα εφαρμογών όπως πριν.

Πίνακας 3-19: Μέγιστος Αριθμός Κρυπτογραφημένων Κλήσεων Φωνής (G.729) ανά Ταχύτητα Ζεύξης

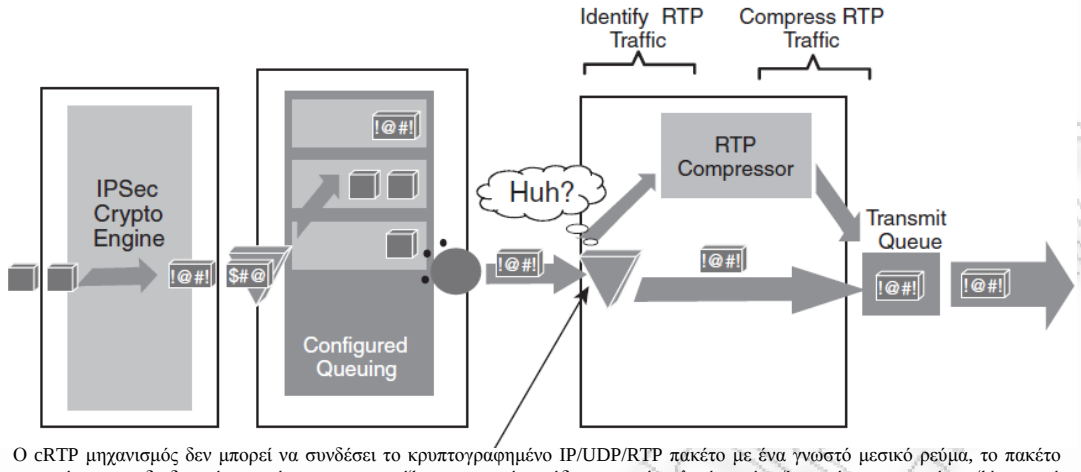
Ταχύτητα Ζεύξης (Kbps)	Μέγιστος Αριθμός Κλήσεων Φωνής (G.729)	LLQ Εύρος Ζώνης (Kbps)	LLQ Εύρος Ζώνης (ποσοστό)
64 (FRF.12)	1 (58 Kbps)	58	91%
128 (FRF.12)	1 (58 Kbps)	58	46%
256 (FRF.12)	2 (58 Kbps)	116	46%
512 (FRF.12)	3 (58 Kbps)	174	34%
768 (FRF.12)	4 (58 Kbps)	232	31%
1024	6 (56 Kbps)	336	33%
1536	9 (56 Kbps)	504	33%
2048	12 (56 Kbps)	672	33%

Κατά τον υπολογισμό του απαιτούμενου εύρους ζώνης για ένα υποκατάστημα, θεωρούμε τον μέγιστο αριθμό των ταυτόχρονων κλήσεων που μπορούν να διατρέχουν το IPsec VPN κατά τις περιόδους αιχμής. Αυτό ποικίλει ανάλογα με τη μορφή της εργασίας των υπαλλήλων, για παράδειγμα το τμήμα μηχανογράφησης αναμένεται να πραγματοποιήσει λιγότερες κλήσεις από το τμήμα πωλήσεων. Μια τυπική αναλογία ατόμων που κάνουν κλήση σε σχέση με το συνολικό αριθμό είναι ένα προς έξι (1:6), δηλαδή ανά έξι άτομα το ένα πραγματοποιεί κλήση. Αυτό βέβαια μπορεί να αλλάζει και να κυμανθεί σε 1:4 ή 1:10 ανάλογα με τη διεκπεραίωση των εργασιών. Με βάση τα παραπάνω αλλά και τον Πίνακα 3-19, μια ζεύξη με Line Rate 512 Kbps μπορεί να υποστηρίξει από 12 έως και 30 άτομα. Όπως σε κάθε τοπολογία έτσι και εδώ, πολύ σημαντικός είναι ο τρόπος διαχείρισης του μηχανισμού CAC, ο οποίος πρέπει να ανταποκρίνεται σωστά στις QoS πολιτικές που έχουν αναπτυχτεί με βάση το πλαίσιο υποδομής του δικτύου.

3.5.3 Ασυμβατότητα IPSec με cRTP

Οι σημαντικές επιβαρύνσεις που προκαλεί στο εύρος ζώνης η διαδικασία κρυπτογράφησης, οδήγησε πολλούς διαχειριστές να εξετάσουν τη χρήση της τεχνικής IP RTP συμπίεσης κεφαλίδας με σκοπό την αντιστάθμιση των παραπάνω επιβαρύνσεων. Ωστόσο ένας από τους περιοριστικούς όρους της κρυπτογράφησης είναι ότι τα βασικά τμήματα του αρχικού IP πακέτου δεν είναι πλέον αναγνώσιμα. Κατά συνέπεια το IPsec με το cRTP είναι δυο εκ φύσεως ασύμβατα πρότυπα μιας και η αρχική IP/UDP/RTP κεφαλίδα είναι ήδη κρυπτογραφημένη τη στιγμή που ο cRTP μηχανισμός καλείται να εκτελέσει τη συμπίεση. Ως εκ τούτου, επειδή ο cRTP μηχανισμός δεν μπορεί να συνδέσει το κρυπτογραφημένο IP/UDP/RTP πακέτο με ένα γνωστό μεσικό ρεύμα, το πακέτο παρακάμπτει τη διαδικασία συμπίεσης και συνεχίζει στην ουρά μετάδοσης χωρίς τελικά καμία εξοικονόμηση στο εύρος ζώνης από τον cRTP μηχανισμό.

Εικόνα 3-39: Ασυμβατότητα IPsec με cRTP



Ο cRTP μηχανισμός δεν μπορεί να συνδέσει το κρυπτογραφημένο IP/UDP/RTP πακέτο με ένα γνωστό μεσικό ρεύμα, το πακέτο παρακάμπτει τη διαδικασία συμπίεσης και συνεχίζει στην ουρά μετάδοσης χωρίς τελικά καμία εξοικονόμηση στο εύρος ζώνης από τον cRTP μηχανισμό.

[43]

Μια επιπλέον σημαντική διαφορά που επιδεινώνει περαιτέρω την ασυμβατότητα είναι ότι το cRTP πρότυπο λειτουργεί σε μια βάση σημείο-προς-σημείο, ενώ το IPsec μπορεί να επεκταθεί σε πολλαπλά ενδιάμεσα (Layer-3) σημεία.

Παρότι γίνονται πολλές προσπάθειες για επίτευξη συνεργασίας των δυο αυτών προτύπων, έως σήμερα που γράφεται αυτή η εργασία δεν έχει καταστεί ακόμη εφικτό.

3.5.4 Προ-Κατακερματισμός

Όταν ένα μη κρυπτογραφημένο πακέτο είναι σχεδόν ίσο με την Μέγιστη Μονάδα Μετάδοσης (MTU) της ζεύξης, τότε μετά την κρυπτογράφησή του, λόγω των πρόσθετων επιβαρύνσεων υπάρχει η πιθανότητα το πακέτο να υπερβεί την MTU τιμή. Αυτό θα έχει ως αποτέλεσμα τον κατακερματισμό του πακέτου μετά την κρυπτογράφηση και αντίστοιχα την αναγκαστική επανασυναρμολόγησή του πριν την αποκρυπτογράφηση από το δρομολογητή δέκτη.

Η Cisco για την αντιμετώπιση της παραπάνω κατάστασης σε IPSec VPNs εισήγαγε ένα νέο χαρακτηριστικό που το ονόμασε Προ-κατακερματισμό (Prefragmentation) με το οποίο επιτυγχάνει να αυξάνει την απόδοση του δρομολογητή δέκτη. Η λειτουργία αυτή επιτρέπει στον δρομολογητή αποστολέα να προβλέπει το μέγεθος που θα έχει το πακέτο μετά την κρυπτογράφησή του για IPSec ασφαλή μετάδοση. Έτσι, αν το προβλεπόμενο μέγεθος του πακέτου είναι μεγαλύτερο από την MTU τιμή, το πακέτο κατακερματίζεται πριν κρυπτογραφηθεί. Ως εκ τούτου, ο δρομολογητής δέκτης απαλλάσσεται από τη λειτουργία επανασυναρμολόγησης που ήταν αναγκασμένος να πράττει πριν από την αποκρυπτογράφηση, απελευθερώνοντας έτσι πόρους και συμβάλλοντας στη συνολική αύξηση της διεκπεραιωτικότητας.

Η λειτουργία προ-κατακερματισμού για IPSec VPNs είναι από προεπιλογή ενεργοποιημένη σε όλους τους δρομολογητές Cisco που υποστηρίζουν VPN και έχουν IOS Release την 12.2 (13) T ή νεότερη.

3.5.5 Αύξηση Προϋπολογίσιμης Καθυστέρησης

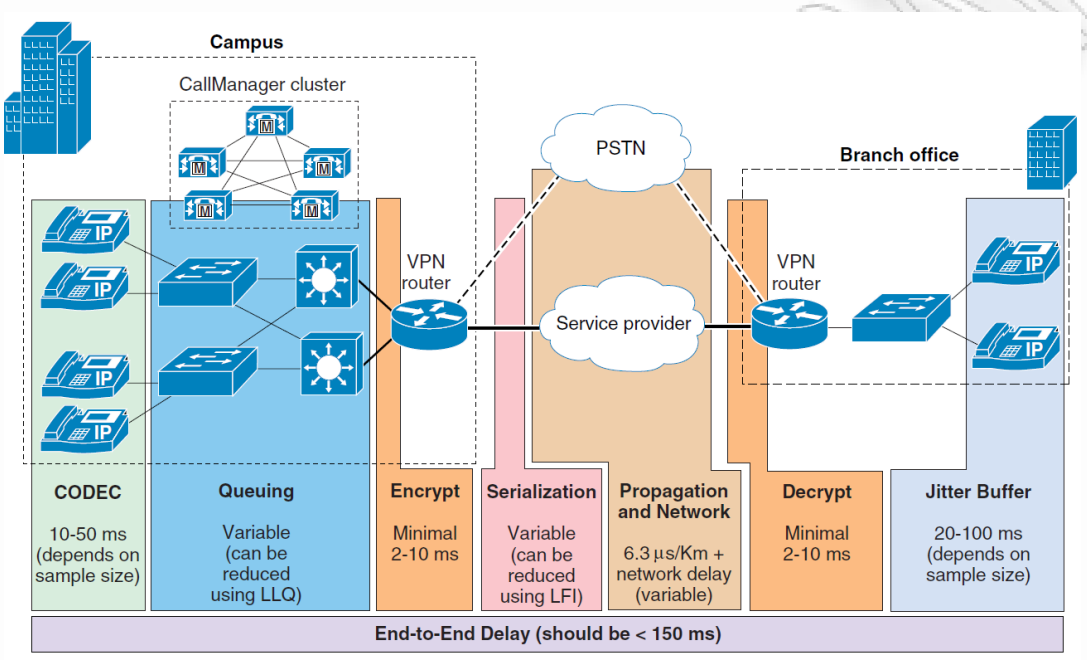
Όπως ήδη έχει αναφερθεί, ο προϋπολογισμός της καθυστέρησης για την IP Τηλεφωνία περιλαμβάνει σταθερές και μεταβλητές παραμέτρους. Κατά την ITU η μέγιστη τιμή καθυστέρησης μιας κατεύθυνσης (one-way) είναι 150 msec. Ωστόσο σε μια IPsec VPN ανάπτυξη, πρέπει να συνυπολογισθούν δυο επιπλέον στοιχεία καθυστέρησης:

1. Η καθυστέρηση λόγω κρυπτογράφησης στο αρχικό σημείο της IPsec VPN σήραγγας.

2. Η καθυστέρηση λόγω αποκρυπτογράφησης στο τελικό σημείο της IPsec VPN σήραγγας.

Έχει υπολογιστεί πως στις περισσότερες περιπτώσεις η πρόσθετη καθυστέρηση που προκαλούν οι διαδικασίες Κρυπτογράφησης/Αποκρυπτογράφησης κυμαίνεται από 4 έως 10 msec (συνδυαστικά). Στη συνέχεια παρουσιάζονται σχηματικά όλες οι αυξητικές καθυστερήσεις σε μια IPsec VPN ανάπτυξη:

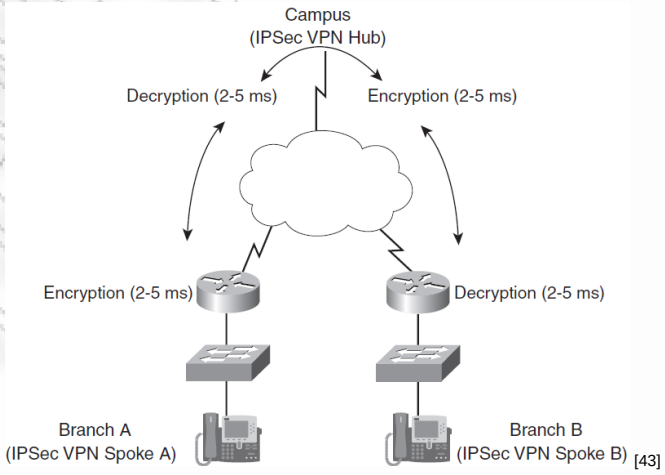
Εικόνα 3-40: Παράγοντες Καθυστέρησης σε IPsec VPN ανάπτυξη



[4]

Κατά το σχεδιασμό, μια συντηρητική εκτίμηση θα είναι 10 msec καθυστέρηση για την κρυπτογράφηση και 10 msec για την αποκρυπτογράφηση. Μια τέτοια καθυστέρηση αρχικά μπορεί να μη φαίνεται σημαντική, δυστυχώς κάτι τέτοιο δεν ισχύει ειδικά όταν πρόκειται για πραγματοποίηση φωνητικής κλήσης μεταξύ δυο συνομιλητών που βρίσκονται σε διαφορετικά υποκαταστήματα. Σε αυτή την περίπτωση οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης μπορεί να συμβούν παραπάνω από μια φορά ανάλογα με τη λογική τοπολογία του VPN. Αυτό φαίνεται στην επόμενη εικόνα:

Εικόνα 3-41: Πολλαπλές Καθυστερήσεις Κρυπτογράφησης/Αποκρυπτογράφησης Μεταξύ IPsec VPNs

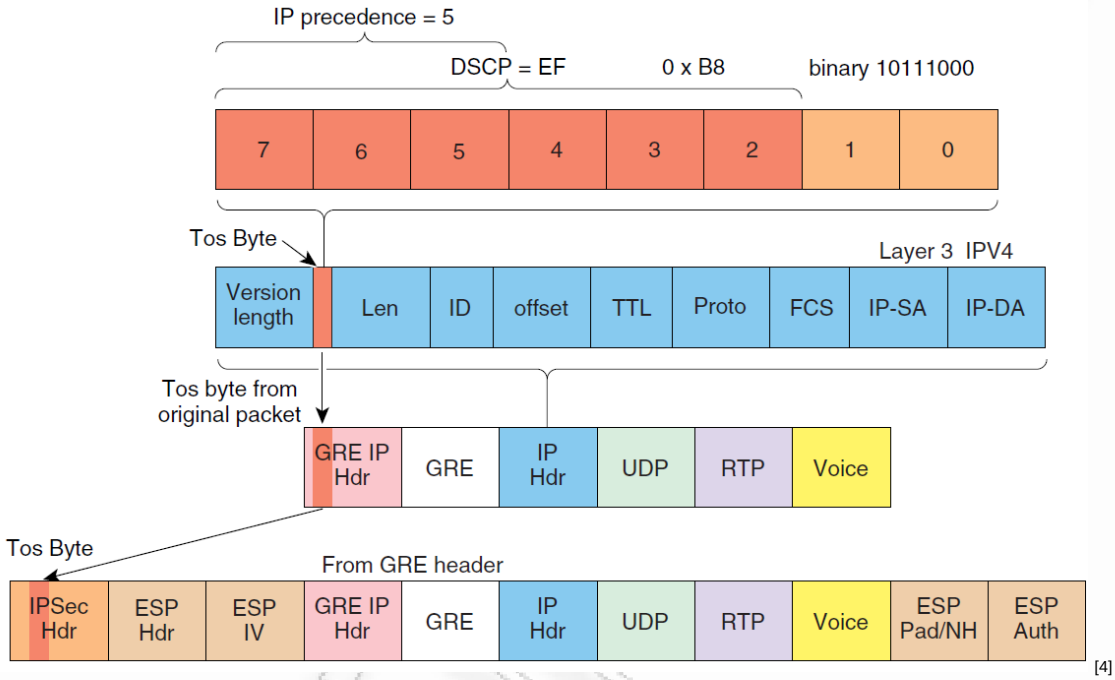


[43]

3.5.6 Διάσωση του ToS Byte

Όπως ήδη έχει αναφερθεί, η ταξινόμηση των πακέτων πραγματοποιείται βάσει της DSCP σήμανσης που υπάρχει στο ToS Byte του εκάστοτε πακέτου. Ωστόσο, μετά την κρυπτογράφηση ενός πακέτου η συγκεκριμένη πληροφορία δεν μπορεί να είναι διαθέσιμη από τους QoS μηχανισμούς. Για την υπερπήδηση αυτού του δυσάρεστου εμποδίου, ενδογενώς το πρωτόκολλο IPsec παρέχει τη δυνατότητα διατήρησης της πληροφορίας που εμπεριέχεται στο ToS Byte αντιγράφοντάς το από την αρχική IP κεφαλίδα.

Εικόνα 3-42: Διάσωση του ToS Byte



[4]

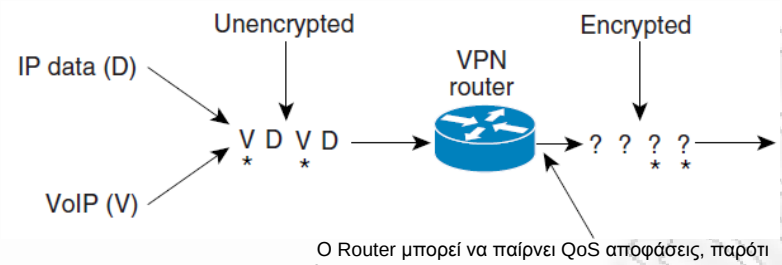
Όπως φαίνεται και στην Εικόνα 3-42 οι αρχικές τιμές του ToS Byte αντιγράφονται πρώτα από την αρχική IP κεφαλίδα και προστίθενται στην GRE, εν συνεχεία αντιγράφονται πάλι και προστίθενται στη IPsec κεφαλίδα χωρίς να υποστούν καμία αλλοίωση.

Η διαδικασία αυτή αντισταθμίζει το γεγονός ότι η αρχική IP κεφαλίδα (συμπεριλαμβανομένου και του ToS Byte) είναι στην πραγματικότητα μη αναγνώσιμη λόγω της κρυπτογράφησης και επιτρέπει στους QoS μηχανισμούς να επεξεργαστούν το πακέτο όπως κάθε άλλο. Επιπρόσθετα, μέσω αυτής της διαδικασίας υπογραμμίζεται η σημασία της διασφάλισης πως η κίνηση πρέπει να χαρακτηρίζεται σωστά (σε Layer-3) πριν κρυπτογραφηθεί.

3.5.7 QoS Προ-Ταξινόμηση (Pre-Classify)

Η Pre-Classify διαδικασία συχνά συγχέεται με τη *Διάσωση του ToS Byte* που αναλύθηκε στην προηγούμενη παράγραφο. Ωστόσο είναι μια λειτουργία που προσφέρει το IOS της Cisco για την επίτευξη κατηγοριοποίησης των κρυπτογραφημένων πακέτων κίνησης όπου η ταξινόμησή τους δεν γίνεται με βάση την DSCP πληροφορία του ToS Byte, αλλά με βάση διαφορετικά κριτήρια όπως η IP διεύθυνση πηγής/προορισμού, οι αριθμοί θύρας πηγής/προορισμού και τα Layer-4 πρωτόκολλα. Επειδή όλες οι παραπάνω πληροφορίες εμπεριέχονται κρυπτογραφημένες στα πεδία της κεφαλίδας του κάθε πακέτου, δεν είναι δυνατό από τους QoS μηχανισμούς να πραγματοποιηθεί ταξινόμηση με βάση τα κριτήρια αυτά. Η Εικόνα 3-43 απεικονίζει το QoS χαρακτηριστικό σε υψηλό επίπεδο:

Εικόνα 3-43: Pre-Classify Χαρακτηριστικό

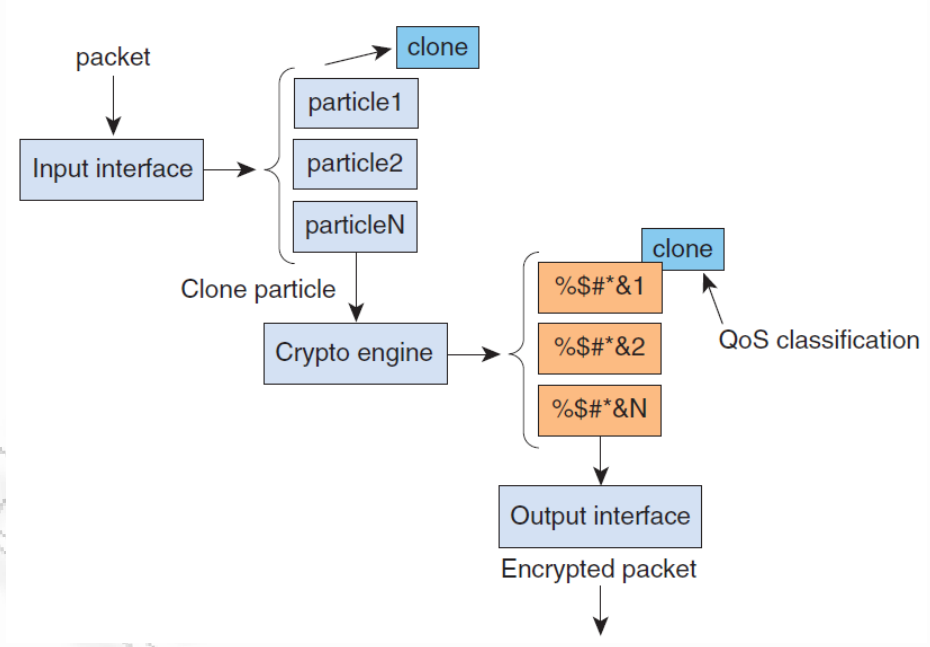


[4]

Μια λύση στο παραπάνω εμπόδιο είναι η δημιουργία ενός κλώνου της αρχικής κεφαλίδας πριν την κρυπτογράφηση του πακέτου. Έπειτα η μηχανή κρυπτογράφησης κρυπτογραφεί το πακέτο, ο κλώνος συσχετίζεται με το νέο κρυπτογραφημένο πακέτο που εν συνεχεία αποστέλλεται στη διεπαφή εξόδου. Στη διεπαφή εξόδου όλες οι QoS αποφάσεις που βασίζονται στις προαναφερθείσες πληροφορίες κεφαλίδας (εκτός του ToS Byte που έχει διασωθεί) μπορούν να πραγματοποιηθούν χρησιμοποιώντας για συσχέτιση με τις λίστες πρόσβασης τις πληροφορίες που εμπεριέχονται στους κλώνους. Συνεπώς με αυτό τον τρόπο μπορεί να παρασχεθεί ταξινόμηση ακόμα και σε κρυπτογραφημένα πακέτα.

Ένα λεπτό σημείο που πρέπει να διευκρινιστεί σχετικά με τη Pre-Classify λειτουργία είναι ότι μπορεί να εφαρμοστεί μόνο σε διεπαφές εξόδου δρομολογητών που υποστηρίζουν κρυπτογράφηση. Τα πεδία που διατηρούνται από τη Pre-Classify διαδικασία δεν είναι διαθέσιμα σε κανέναν μεταγενέστερο δρομολογητή μιας και ο κλώνος ποτέ δεν εγκαταλείπει τον δρομολογητή στον οποίο δημιουργήθηκε και εκτελεί την κρυπτογράφηση, διασφαλίζοντας έτσι την ακεραιότητα και την ασφάλεια της IPSec VPN σήραγγας. Η διαδικασία απεικονίζεται και περιγράφεται στη συνέχεια:

Εικόνα 3-44: Pre-Classify Λειτουργική Διαδικασία



[4]

Τα ακόλουθα βήματα συνοψίζουν τη διαδικασία Προ-Ταξινόμησης του QoS όπως αυτή παρουσιάζεται στην Εικόνα 3-44:

1. Ένα πακέτο εισέρχεται στο interface εισόδου και αποθηκεύεται σε τμήματα μέσα σε κάποια συγκεκριμένη ομάδα

2. Όταν το πακέτο ταιριάξει με ένα κρυπτογραφημένο πίνακα του interface, προωθείται στην μηχανή Crypto.
3. Σαν μέρος της διαδικασίας μετάδοσης της μηχανής κρύπτο, ένα πιστό αντίγραφο (clone) τμήματος συμπεριλαμβανομένου και της IP κεφαλίδας δημιουργείται και συσχετίζεται με τη δομή των δεδομένων του πακέτου
4. Η μηχανή κρυπτογράφησης κρυπτογραφεί το αρχικό πακέτο και τοποθετεί το κωδικοποιημένο κείμενο στα νέα τμήματα συσχετίζοντας τα αρχικά τμήματα με τα νέα.
5. Αν στο εξερχόμενο interface δεν υπάρχει συμφόρηση, το κρυπτογραφημένο πακέτο απλά μεταδίδεται.

Αν υπάρχει συμφόρηση και πρέπει να τοποθετηθεί σε ουρά QoS, η ταξινόμηση ενεργεί πάνω στα μη κρυπτογραφημένα πιστά αντίγραφα έτσι ώστε να γίνει το ταίριασμα με το πρωτόκολλο, την IP διεύθυνση (αποστολέα/παραλήπτη) και τον αριθμό θύρας (port number).

Η Pre-Classify διαδικασία συνιστάται να είναι ενεργοποιημένη πάντα ακόμα και αν η ταξινόμηση γίνεται μόνο με βάση το ToS Byte. Δοκιμές έχουν δείξει πως η ενεργοποίηση της Pre-Classify διαδικασίας βελτιώνει ελαφρώς την απόδοση της κάρτας κρυπτογράφησης (hardware).

Η εντολή εφαρμογής της Pre-Classify διαδικασίας σε μια διεπαφή ενός δρομολογητή που υποστηρίζει κρυπτογράφηση, παρουσιάζεται στη συνέχεια:

```
Router(config-if)# qos pre-classify
```

3.5.8 Προστασία από Επιθέσεις Επανάληψης (Anti-Replay)

Το IPSec προσφέρει ενδογενή μηχανισμό για πληροφόρηση ακεραιότητας έτσι ώστε να εξακριβώνεται εάν ένα μεμονωμένο πακέτο αναμεταδίδεται από υποκλοπέα ή όχι. Αυτή η διαδικασία καλείται ακεραιότητα χωρίς σύνδεση (connectionless integrity). Επιπλέον το IPsec παρέχει μερική ακεραιότητα ακολουθίας (sequence integrity) με σκοπό την αποτροπή άφιξης διπλών πακέτων. Οι έννοιες αυτές περιγράφονται αναλυτικά στο RFC 2401, «Αρχιτεκτονική Ασφαλείας για το Πρωτόκολλο Διαδικτύου ».

Όταν μέσω μιας δράσης μετασχηματισμού διαμορφώνεται ESP πιστοποίηση (**esp-sha-hmac**) σε μια IPsec σύνδεση, τότε το IPsec άκρο του δέκτη, ελέγχει αν τα πακέτα παραλαμβάνονται μόνο μια φορά. Επειδή δυο IPsec άκρα μπορούν να στείλουν εκατομμύρια πακέτα, υλοποιείται ένα κυλιόμενο παράθυρο χωρητικότητας *N*=64 πακέτων για να δεσμεύει το ποσό μνήμης που απαιτείται ώστε να ελεγχθεί η παραλαβή των πακέτων του άκρου. Τα πακέτα μπορούν να φθάσουν εκτός σειράς, αλλά για να γίνουν αποδεκτά πρέπει να παραληφθούν στα πλαίσια του παραθύρου. Ενώ εάν φτάσουν πάρα πολύ αργά (έξω από το παράθυρο), τότε απορρίπτονται.

Η λειτουργία του Anti-Replay παραθύρου είναι η ακόλουθη:

1. Ο αποστολέας ανά ασφαλή σύνδεση εκχωρεί στα κρυπτογραφημένα πακέτα έναν μοναδικό αριθμό ακολουθίας (κάθε πακέτο λαμβάνει έναν μοναδικό αύξοντα αριθμό):
2. Ο δέκτης διατηρεί ένα κυλιόμενο παράθυρο χωρητικότητας *N*=64 πακέτων, η δεξιά άκρη του οποίου περιλαμβάνει τον υψηλότερο αριθμό της ακολουθίας (*X*), ενώ η αριστερή τον μικρότερο (*X-N+1*). Επιπλέον, διατηρείται μια μεταβλητή η οποία «θυμάται» αν στο τρέχον παράθυρο (από *X-N+1* έως *X*) κάθε πακέτο παραλήφτηκε ή όχι.
3. Ο δέκτης αξιολογεί το λαμβανόμενο αριθμό ακολουθίας του κάθε πακέτου ως εξής:
    - Αν ο αριθμός ακολουθίας του λαμβανόμενου πακέτου εμπίπτει μέσα στο παράθυρο και το πακέτο δεν έχει παραληφθεί προηγουμένως, τότε αυτό γίνεται αποδεκτό και χαρακτηρίζεται με «λήψη».

— Αν ο αριθμός ακολουθίας του λαμβανόμενου πακέτου εμπίπτει μέσα στο παράθυρο και το πακέτο έχει παραληφθεί προηγουμένως, τότε αυτό απορρίπτεται και ο μετρητής λάθους επανάληψης αυξάνεται.

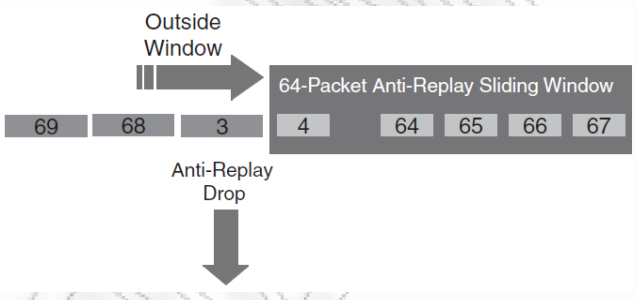
— Αν ο αριθμός ακολουθίας του λαμβανόμενου πακέτου είναι μεγαλύτερος από τον υψηλότερο αριθμό ακολουθίας που υπάρχει στο παράθυρο, τότε το πακέτο γίνεται αποδεκτό, χαρακτηρίζεται με «λήψη» και το κυλιόμενο παράθυρο κινείται «προς τα δεξιά».

— Αν ο αριθμός ακολουθίας του λαμβανόμενου πακέτου είναι μικρότερος από την χαμηλότερη τιμή ακολουθίας στο παράθυρο, τότε το πακέτο απορρίπτεται και ο μετρητής λάθους επανάληψης αυξάνεται.

Σε μια συγκλίνουσα IPSec εφαρμογή με ενεργοποιημένο το QoS, τα πακέτα χαμηλής προτεραιότητας καθυστερούν περισσότερο έτσι ώστε να δίνεται η δυνατότητα στα αντίστοιχα υψηλής προτεραιότητας να απολαμβάνουν προνομιακή μεταχείριση. Ως εκ τούτου, υπάρχει η πιθανότητα λόγω μεγάλης καθυστέρησης από την QoS διαδικασία ιεράρχησης, ορισμένα πακέτα παρ` ότι είναι «νόμιμα» να απορριφτούν από τον μηχανισμό ως Anti-Replay λάθη.

Η Εικόνα 3-45 παρέχει μια απεικόνιση της λειτουργίας. Σε αυτό το παράδειγμα τα πακέτα φωνής 4 έως 67 έχουν παραληφθεί, το πακέτο δεδομένων με αριθμό 3 καταφθάνει με καθυστέρηση και γι` αυτό απορρίπτεται και εν συνεχεία διαβιβάζεται το πακέτο φωνής με αριθμό 68. Όταν η Anti-Replay λογική καλείται να επεξεργαστεί το πακέτο 3, το απορρίπτει διότι είναι έξω από την αριστερή άκρη του κυλιόμενου παραθύρου. Τα πακέτα μπορούν να παραλαμβάνονται και εκτός σειράς αλλά πρέπει να εμπίπτουν μέσα στο παράθυρο για να γίνουν αποδεκτά.

Εικόνα 3-45: Anti-Replay Λειτουργία



[43]

Οι Anti-Replay απορρίψεις πακέτων μπορούν να εξαλειφτούν με την υλοποίηση ενός ξεκάθαρου IPSec σχεδιασμού δημιουργώντας ανεξάρτητες σχέσεις ασφαλείας για φωνή και δεδομένα. Τα πακέτα φωνής και δεδομένων πρέπει να προσαρμόζονται σε ξεχωριστή γραμμή της λίστας πρόσβασης του χάρτη κρυπτογράφησης. Αυτό υλοποιείται πολύ εύκολα εάν στα IP τηλέφωνα δίνονται διαφορετικές (διαφορετικού εύρους) IP διευθύνσεις απ` ότι στους σταθμούς εργασίας.

Για μια εφαρμογή που βασίζεται στο TCP, η απόρριψη ενός πακέτου είτε από την Anti-Replay λειτουργία είτε από την πολιτική υπηρεσιών που εφαρμόζεται σε μια διεπαφή εξόδου σε περίπτωση συμφόρησης δεν έχει καμία διαφορά. Στο TCP πρωτόκολλο μπορεί να υπάρχει ενσωματωμένος μηχανισμός ελέγχου ροής, αλλά δεν μπορεί να αντιληφθεί γιατί ένα πακέτο απορρίφτηκε. Ωστόσο, από πλευράς δικτύων είναι αποδοτικότερο να απορριφτεί το πακέτο πριν σταλεί μέσω μιας ζεύξης παρά πρώτα να αποσταλεί και εν συνεχεία να απορριφτεί από τον Anti-Replay μηχανισμό του παραλήπτη.

Έχει διαπιστωθεί πως οι Anti-Replay απορρίψεις πακέτων σε IPSec VPN ζεύξεις όπου παρατηρείται συμφόρηση, είναι της τάξεως του 1 με 1.5%. Αντίθετα οι απορρίψεις από την εφαρμογή πολιτικής στις διεπαφές εξόδου είναι πολύ λιγότερες. Συνεπώς ο Anti-Replay μηχανισμός λειτουργεί περισσότερο επιθετικά. Ο λόγος που συμβαίνει αυτό θα αναλυθεί στη συνέχεια.

Εξ ορισμού, κάθε CBWFQ τάξη λαμβάνει μια ουρά αναμονής με ένα μήκος 64 πακέτων. Από την άλλη πλευρά στο IPSec άκρο του δέκτη υπάρχει ένα ενιαίο παράθυρο 64 πακέτων (ανά ασφαλή σύνδεση), το οποίο πρέπει να επεξεργαστεί όλα τα πακέτα (όλο το εύρος ζώνης) από τις LLQ και CBWFQ τάξεις. Συνεπώς, ο κακός συνδυασμός στο μέγεθος των ουρών αναμονής της διεπαφής εξόδου του αποστολέα έναντι του σχετικά μικρού μεγέθους του Anti-Replay παραθύρου έχουν σαν αποτέλεσμα την προαναφερθείσα διαφορά επιθετικότητας.

Υπάρχει η δυνατότητα βελτίωσης του σεναρίου μειώνοντας τον παράγοντα *max_threshold* σε κάθε ουρά αναμονής της πολιτικής υπηρεσιών που εφαρμόζεται στη διεπαφή εξόδου του αποστολέα. Κατά αυτό τον τρόπο η πολιτική υπηρεσιών γίνεται επιθετικότερη στην απόρριψη αφού δίνει δυνατότητα αποθήκευσης σε λιγότερα πακέτα και με μειωμένους χρόνους αναμονής. Εκτενής εργαστηριακή δοκιμή έχει δείξει πως ο κατάλληλος συντονισμός στο ανώτατο όριο ουρών αναμονής μπορεί να μειώσει τον αριθμό των Anti-Replay απορρίψεων από 1% σε λιγότερο από 0,1%.

Μια εναλλακτική διαδικασία μείωσης των Anti-Replay απορρίψεων είναι η αύξηση του αριθμού των πακέτων (*N*) που μπορεί να παρακολουθεί μέσω του κυλιόμενου παραθύρου ο δέκτης. Η μεταβολή αυτή δεν προκαλεί καμία επίπτωση στη διεκπεραιωτικότητα και την ασφάλεια. Οι επιπτώσεις στη μνήμη είναι ασήμαντες μιας και απαιτούνται επιπλέον μόνο 128 bytes ανά εισερχόμενη IPSec SA (Security Association, Ασφαλή Σύνδεση) ώστε να αποθηκευτεί ο αριθμός ακολουθίας στο δρομολογητή δέκτη.

Η καθολική μεταβολή του αριθμού *N* (αποδεκτές τιμές: 64, 128, 256, 512, ή 1024) μπορεί να διαμορφωθεί μέσω της εντολής:

crypto ipsec security-association replay window-size [N]

Δε θα έχει καμία αξία η μεταβολή αυτή εάν πρώτα έχει απενεργοποιηθεί ο Anti-Replay έλεγχος:

crypto ipsec security-association replay disable

Η ενεργοποίηση του ελέγχου και η επαναφορά του *N* στην προεπιλεγμένη τιμή (*N=64*) γίνεται μέσω της εντολής:

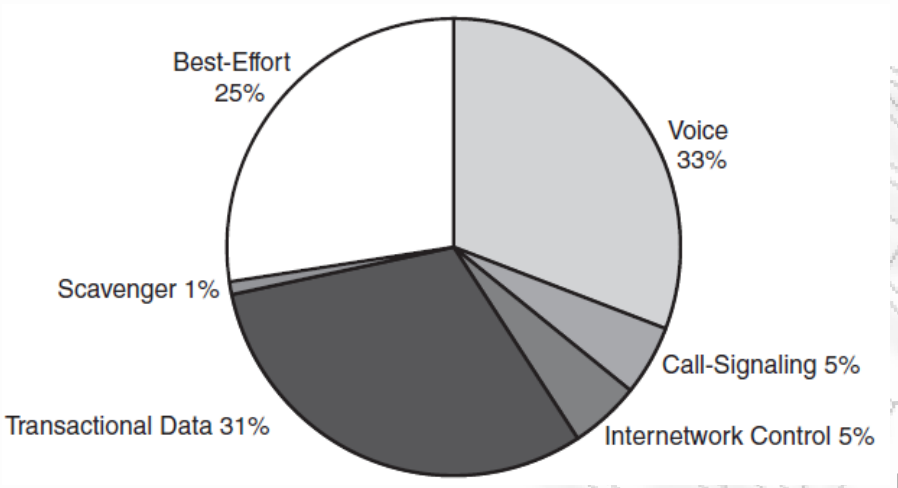
no crypto ipsec security-association replay disable

3.5.9 V3PN Μοντέλο 6-Τάξεων Κίνησης

Στη συνέχεια παρουσιάζεται ο τρόπος διαμόρφωσης ενός V3PN μοντέλου, 6-κλάσεων κίνησης το οποίο είναι κατάλληλο για ταχύτητες ζεύξης έως 2 Mbps (τεχνικά θα έπρεπε να ονομάζεται V2PN, διότι το μοντέλο 6-κλάσεων δεν υποστηρίζει πάνω από IPSec VPN την κίνηση Video). Οι διάφοροι τύποι κίνησης, καθώς και το ποσοστό εύρους ζώνης που τους αναλογεί απεικονίζονται στην Εικόνα 3-45.

Το λειτουργικό της Cisco διαθέτει έναν εσωτερικό μηχανισμό με ονομασία PAK_Priority, με σκοπό την προστασία της κίνησης ελέγχου (control traffic) όπως οι πίνακες δρομολόγησης (routing tables). Ο μηχανισμός PAK_Priority είναι υπεύθυνος ώστε να χαρακτηρίζει τα πρωτόκολλα ελέγχου με DSCP CS6, κάτι που δυστυχώς έως και σήμερα δεν υποστηρίζει για τα IPSec πρωτόκολλα ελέγχου, όπως είναι το ISAKMP (UDP θύρα 500). Για αυτό το λόγο στο επόμενο παράδειγμα θα χρησιμοποιηθεί ρητή κλάση για την κίνηση ελέγχου συμπεριλαμβανομένων και των IPSec πρωτοκόλλων ελέγχου.

Εικόνα 3-46: V3PN Μοντέλο 6 Τάξεων Κίνησης



[43]

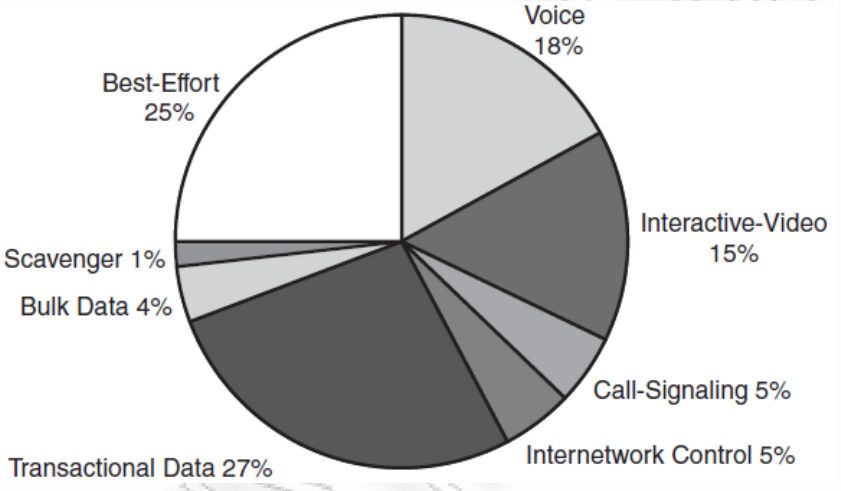
```
!
class-map match-all VOICE
match ip dscp ef                                ! VoIP
class-map match-any CALL-SIGNALING
match ip dscp cs3                               ! Call-Signaling (Παλαιό)
match ip dscp af31                              ! Call-Signaling (Νέο)
class-map match-any INTERNETWORK-CONTROL
match ip dscp cs6                               ! IP Routing
match access-group name IKE                     ! Αναφορές ISAKMP ACL
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21 af22                         ! Transactional-Data
class-map match-all SCAVENGER
match ip dscp cs1                               ! Scavenger

!
!
policy-map SIX-CLASS-V3PN-EDGE
class VOICE
priority percent 33                             ! Το VoIP παίρνει το 33% του BW, LLQ
class CALL-SIGNALING
bandwidth percent 5                             ! Call-Signaling
class INTERNETWORK-CONTROL
bandwidth percent 5                             ! Control Plane
class TRANSACTIONAL-DATA
bandwidth percent 31                            ! Transactional-Data
queue-limit 20                                  ! Προαιρετικό:Anti-Replay συντονισμός
class SCAVENGER
bandwidth percent 1                             ! Η Scavenger τάξη έχει τεθεί σε αναμονή
queue-limit 1                                   ! Προαιρετικό:Anti-Replay συντονισμός
class class-default
bandwidth percent 25                            ! Εξασφαλισμένο BW για Best Effort
queue-limit 16                                  ! Προαιρετικό:Anti-Replay συντονισμός
!
!
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp          ! ISAKMP ACL
!
```

3.5.10 V3PN Μοντέλο 8-Τάξεων Κίνησης

Το μοντέλο αυτό ενδείκνυται για γραμμές με ταχύτητα διασύνδεσης από 3Mbps και πάνω. Ωστόσο δεν πρέπει να ξεχνάμε ότι ο καταμερισμός φορτίου σε πολλές φυσικές διεπαφές (μέσω GRE σηράγγων) επιδεινώνει τις Anti-Replay απορρίψεις. Ως εκ τούτου είναι πιθανό να απαιτείται η χρήση μόνο μιας φυσικής διεπαφής ώστε να αποφευχθεί η παραπάνω κατάσταση. Ένας επιπρόσθετος παράγοντας που πρέπει να εξετάζεται είναι οι απαιτήσεις του εκάστοτε δρομολογητή. Υπάρχουν πλατφόρμες δρομολογητών όπως οι 2691, 3700 και 7200, όπου σε υψηλές ταχύτητες μεταφοράς δεδομένων απαιτούν να εκτελούν και κρυπτογράφηση.

Στο μοντέλο αυτό σε σχέση με το προηγούμενο προστίθενται δυο νέες τάξεις, μια για διαδραστικό βίντεο (Interactive Video) και μια για μαζική μεταφορά δεδομένων (Bulk Data). Μια άλλη διαφοροποίηση είναι το παρεχόμενο ποσοστό εύρους ζώνης για κάθε τάξη κίνησης καθώς και οι αντίστοιχοι *queue-limit* αριθμοί που αντανακλούν τη σχετική προτεραιότητα της εφαρμογής. Το V3PN μοντέλο 8-ταξεων απεικονίζεται στη συνέχεια:

Εικόνα 3-47: V3PN Μοντέλο 8 Τάξεων Κίνησης



[43]

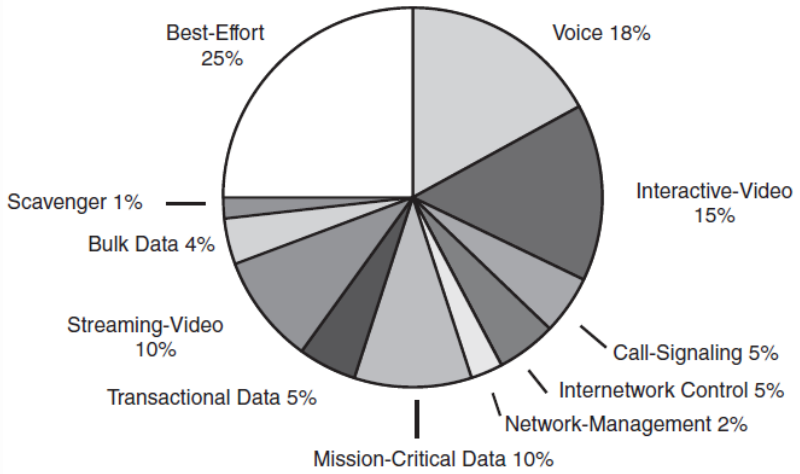
```
!
class-map match-all VOICE
match ip dscp ef                          ! VoIP
class-map match-all INTERACTIVE-VIDEO
match ip dscp af41 af42                   ! Interactive-Video
class-map match-any CALL-SIGNALING
match ip dscp cs3                         ! Call-Signaling (Παλαιό)
match ip dscp af31                        ! Call-Signaling (Νέο)
class-map match-any INTERNETWORK-CONTROL
match ip dscp cs6                         ! IP Routing
match access-group name IKE               ! Αναφορές ISAKMP ACL
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21 af22                   ! Transactional-Data
class-map match-all BULK-DATA
match ip dscp af11 af12                   ! Bulk Data
class-map match-all SCAVENGER
match ip dscp cs1                         ! Scavenger
!
policy-map EIGHT-CLASS-V3PN-EDGE
class VOICE
priority percent 18                       ! Το VoIP παίρνει το 18% του BW, LLQ
class INTERACTIVE-VIDEO
priority percent 15                       ! Παίρνει το 15%,LLQ
class CALL-SIGNALING
bandwidth percent 5                       ! Call-Signaling
class INTERNETWORK-CONTROL
bandwidth percent 5                       ! Control Plane
```

```
class TRANSACTIONAL-DATA
bandwidth percent 27                    ! Transactional-Data
queue-limit 18                          ! Προαιρετικό:Anti-Replay συντονισμός
class BULK-DATA
bandwidth percent 4                     ! Bulk-Data
queue-limit 3                           ! Προαιρετικό:Anti-Replay συντονισμός
SCAVENGER
bandwidth percent 1                     ! Η Scavenger τάξη έχει τεθεί σε αναμονή
queue-limit 1                           ! Προαιρετικό:Anti-Replay συντονισμός
class class-default
bandwidth percent 25                    ! Εξασφαλισμένο BW για Best Effort
queue-limit 16                          ! Προαιρετικό:Anti-Replay συντονισμός
!
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp  ! ISAKMP ACL
```

3.5.11 V3PN Μοντέλο 11-Τάξεων Κίνησης

Με βάση το προηγούμενο μοντέλο προστίθενται άλλες τρεις τάξεις: Network-Management, Mission-Critical Data και Streaming Video. Όπως και το προηγούμενο έτσι και αυτό ενδείκνυται για γραμμές με ταχύτητα διασύνδεσης από 3Mbps και πάνω, επιπλέον ισχύουν οι ίδιες παρατηρήσεις σχετικά με τον κατακερματισμό φορτίου και τις Anti-Replay απορρίψεις. Το V3PN μοντέλο 11-ταξεων απεικονίζεται στη συνέχεια:

Εικόνα 3-48: V3PN Μοντέλο 11 Τάξεων Κίνησης



[43]

```
!
class-map match-all VOICE
match ip dscp ef                        ! VoIP
class-map match-all INTERACTIVE-VIDEO
match ip dscp af41 af42                 ! Interactive-Video
class-map match-any CALL-SIGNALING
match ip dscp cs3                       ! Call-Signaling (Παλαιό)
match ip dscp af31                      ! Call-Signaling (Νέο)
class-map match-any INTERNETWORK-CONTROL
match ip dscp cs6                       ! IP Routing
match access-group name IKE             ! Αναφορές ISAKMP ACL
class-map match-all NET-MGMT
match ip dscp cs2                       ! Network Management
class-map match-all MISSION-CRITICAL-DATA
match ip dscp 25                        ! MC Data
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21 af22                 ! Transactional Data
class-map match-all STREAMING-VIDEO
match ip dscp cs4                       ! Streaming Video
class-map match-all BULK-DATA
match ip dscp af11 af12                 ! Bulk Data
class-map match-all SCAVENGER
```

```
match ip dscp cs1                          ! Scavenger
!
!
policy-map QOSBASELINE-V3PN-EDGE
class VOICE
priority percent 18                        ! Το VoIP παίρνει το 18% του BW, LLQ
class INTERACTIVE-VIDEO
priority percent 15                        ! Παίρνει το 15%,LLQ
class CALL-SIGNALING
bandwidth percent 5                        ! Call-Signaling
class INTERNETWORK-CONTROL
bandwidth percent 5                        ! Control Plane
class NET-MGMT
bandwidth percent 2                        ! Network Management
class MISSION-CRITICAL-DATA
bandwidth percent 10                       ! Mission-Critical Data
queue-limit 6                              ! Προαιρετικό:Anti-Replay συντονισμός
class TRANSACTIONAL-DATA
bandwidth percent 5                        ! Transactional-Data
queue-limit 3                              ! Προαιρετικό:Anti-Replay συντονισμός
class STREAMING-VIDEO
bandwidth percent 10                       ! Streaming-Video
queue-limit 6                              ! Προαιρετικό:Anti-Replay συντονισμός
class BULK-DATA
bandwidth percent 4                        ! Bulk-Data
queue-limit 3                              ! Προαιρετικό:Anti-Replay συντονισμός
class SCAVENGER
bandwidth percent 1                        ! Η Scavenger τάξη έχει τεθεί σε αναμονή
queue-limit 1                              ! Προαιρετικό:Anti-Replay συντονισμός
class class-default
bandwidth percent 25                       ! Εξασφαλισμένο BW για Best Effort
queue-limit 16                             ! Προαιρετικό:Anti-Replay συντονισμός
!
!
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp     ! ISAKMP ACL
!
```

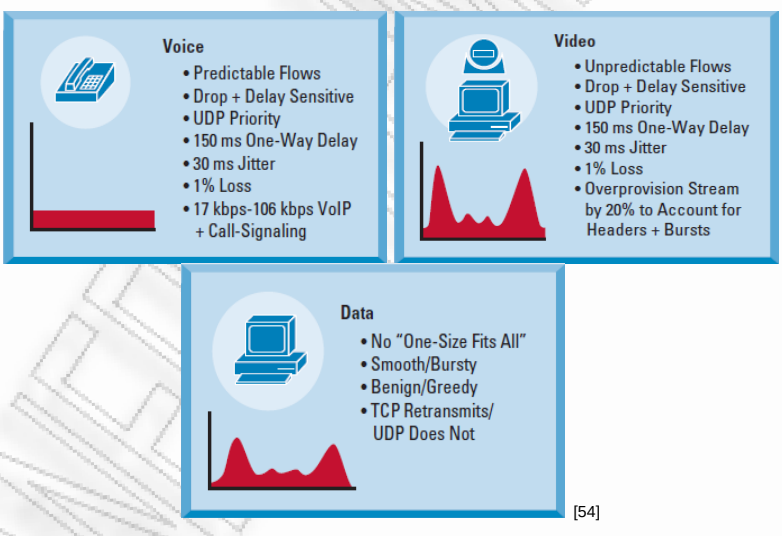
3.6 Σύνοψη - Βέλτιστες Πρακτικές

Θέλοντας να κάνουμε μια γενική σύνοψη όλων όσων έχουν αναφερθεί σε αυτό το κεφάλαιο, θα συμπεραίναμε πως για την επιτυχημένη εφαρμογή Ποιότητας Υπηρεσίας σε ένα επιχειρησιακό δίκτυο απαιτούνται τρεις βασικές φάσεις υλοποίησης:

1. Ο καθορισμός των στρατηγικών επιχειρησιακών στόχων όπου πρέπει να επιτευχθούν μέσω του QoS, όπος:
   - Απαιτείται μετάδοση μόνο φωνής (VoIP) ή και video;
   - Αν ναι, απαιτείται video-conferencing ή streaming video;
   - Θα υπάρχουν εφαρμογές κρίσιμης μετάδοσης; Αν ναι, ποιες είναι αυτές;
   - Μήπως η επιχείρηση επιθυμεί τη φίμωση ορισμένων τύπων κίνησης; Αν ναι, ποιοι είναι αυτοί;
   - Η επιχείρηση επιθυμεί να χρησιμοποιήσει τα QoS εργαλεία για άμβλυνση των κακόβουλων επιθέσεων;
   - Πόσες κατηγορίες (τάξεις) κίνησης απαιτούνται για την κάλυψη των επιχειρηματικών στόχων;
2. Η ανάλυση του παρεχόμενου επιπέδου υπηρεσιών για κάθε τύπο κίνησης.

Στην Εικόνα παρουσιάζονται τα διαφορετικά χαρακτηριστικά μεταξύ της κίνησης για Φωνή, Βίντεο και Δεδομένα.

Εικόνα 3-49: Χαρακτηριστικά Κίνησης Φωνής, Βίντεο και Δεδομένων



[54]

3. Ο σχεδιασμός, η υλοποίηση και ο έλεγχος των QoS πολιτικών.

Η Ταξινόμηση, η Σήμανση και η Αστυνόμευση της κίνησης πρέπει να υλοποιείται όσο το δυνατόν πιο κοντά στην πηγή της κίνησης, ακολουθώντας τα στάνταρτ Διαφοροποιημένων Υπηρεσιών (Differentiated-Services), όπως παρουσιάζονται στα RFC 2474, 2475, 2597, 2698, και 3246.

Πριν δοθεί σε παραγωγική διαδικασία το δίκτυο, απαιτείται η διεξοδική δοκιμή των υλοποιημένων πολιτικών. Μια επιτυχής πρώτη λειτουργική έναρξη ακολουθείται από τη συνεχή παρακολούθηση των επιπέδων υπηρεσιών με σκοπό την κατάλληλη προσαρμογή και τον συντονισμό των QoS πολιτικών όπου απαιτείται.

Δεδομένου ότι οι επιχειρησιακές ανάγκες αλλάζουν, υπάρχει η πιθανότητα επαναπροσδιορισμού των αρχικών στόχων, γεγονός που μπορεί να επιφέρει την ανάγκη για εκ νέου σχεδιασμό, υλοποίηση και έλεγχο των QoS πολιτικών.

Κεφάλαιο 4ο

4. Υλοποίηση Δικτύου Δεδομένων για Μετάδοση Φωνής

4.1 Γενικά

Η κατάλληλη επιλογή της δικτυακής υποδομής, θα δώσει στην εταιρεία τη δυνατότητα να αναπτύξει ένα ενιαίο, απόλυτα ιδιωτικό δίκτυο διασύνδεσης με τα υποκαταστήματά της ώστε να υποστηρίξει τόσο τις έως σήμερα γνωστές συμβατικές υπηρεσίες μετάδοσης πληροφοριών όσο και τις νέες ηλεκτρονικές υπηρεσίες (μετάδοση φωνής και εικόνας) που εκμεταλλεύονται την δυνατότητα που παρέχει το διαδίκτυο για διάδοση των υπηρεσιών αυτών στον τελικό χρήστη.

Η τεχνολογική υποδομή που παρουσιάζεται βασίζεται καθολικά στην τεχνολογία δικτύων IP, μειώνοντας ως αποτέλεσμα τα κόστη εκμετάλλευσης, αποσβένοντας ταχύτατα το αρχικό κόστος όποιας επένδυσης και προστατεύοντας την επένδυση αυτή χωρίς την παραμικρή υποχώρηση στην ποιότητα των υπηρεσιών. Αυτό συνεπάγεται την ενσωμάτωση της τηλεφωνίας στο IP δίκτυο δεδομένων αποφεύγοντας τα ακριβά κόστη τηλεφωνικών κλήσεων και τα κόστη για αγορά, εγκατάσταση, διαχείριση και συντήρηση ξεχωριστού εξοπλισμού τηλεφωνικών κέντρων.

Για την ποιότητα των υπηρεσιών ιδιαίτερη έμφαση πρέπει να δοθεί σε θέματα που σχετίζονται με την ασφάλεια δικτύου, τις υψηλές ταχύτητες επικοινωνίας πακέτων φωνής και δεδομένων, την κεντρικοποιημένη διαχείριση, την υψηλή διαθεσιμότητα. Σε επόμενη παράγραφο δίνονται οι σχεδιαστικές κατευθύνσεις όπως αυτές διέπουν την παρούσα μελέτη.

4.2 Σχεδιαστικές Κατευθύνσεις

Σε κάθε περίπτωση δημιουργίας ενός νέου σύγχρονου τηλεπικοινωνιακού δικτύου, η ορθή κατεύθυνση που οδηγεί τον σχεδιασμό του, πρέπει να στοχεύει στην ποιοτική διαφοροποίηση και αριστοποίηση των υπηρεσιών, που αυτό θα προσφέρει και που συνεπάγεται την αύξηση της αποδοτικότητας. Η σχεδίαση λοιπόν του προτεινόμενου δικτύου βασίζεται κυρίως στην ποιότητα της τελικής λύσης , η οποία με τη σειρά της μεταφέρει την ποιότητα των υπηρεσιών της στον τελικό χρήστη, με τη χρήση των τελευταίων τεχνολογιών της εταιρείας Cisco που κατέχει το μεγαλύτερο μερίδιο αγοράς Internet και με διαπιστωμένη τη λειτουργικότητα τους σε IP περιβάλλοντα.

Η ποιότητα της τελικής λύσης με τεχνολογία Cisco μπορεί να αναλυθεί στις εξής επιμέρους συνιστώσες:

- Την αυξημένη ασφάλεια σε όλα τα επίπεδα του δικτύου. Το γεγονός αυτό επιβάλλεται λόγω της εκπληκτικής αύξησης της χρήσης του Internet καθώς, με την εκθετική αύξηση των χρηστών, αυξάνεται εκθετικά και ο κίνδυνος εξωτερικών προσβολών του εσωτερικού δικτύου γεγονός που επιβεβαιώνεται καθημερινά. Επιπλέον σε έναν ευαίσθητο χώρο, όπως π.χ. αυτός των τραπεζικών συναλλαγών, είναι πρωτευούσης σημασίας να μην αμφισβητηθεί ποτέ η ασφάλεια και η ακεραιότητα των συναλλαγών.
- Την ελαστικότητα του δικτύου να προσφέρει ανεμπόδιστα τις υπηρεσίες σε στιγμές αύξησης του φόρτου του. Αυτό προϋποθέτει την αύξηση της ταχύτητας του δικτύου κορμού στην τάξη των εκατοντάδων Mbps, για την αποτελεσματική υποστήριξη των αυξημένων αναγκών των χρηστών και των προηγμένων υπηρεσιών σε όλη την έκταση του δικτύου.
- Την υλοποίηση ενός τοπικού δικτύου ιεραρχικά δομημένου σε επίπεδα κορμού (core), διανομής (distribution) και πρόσβασης (access).

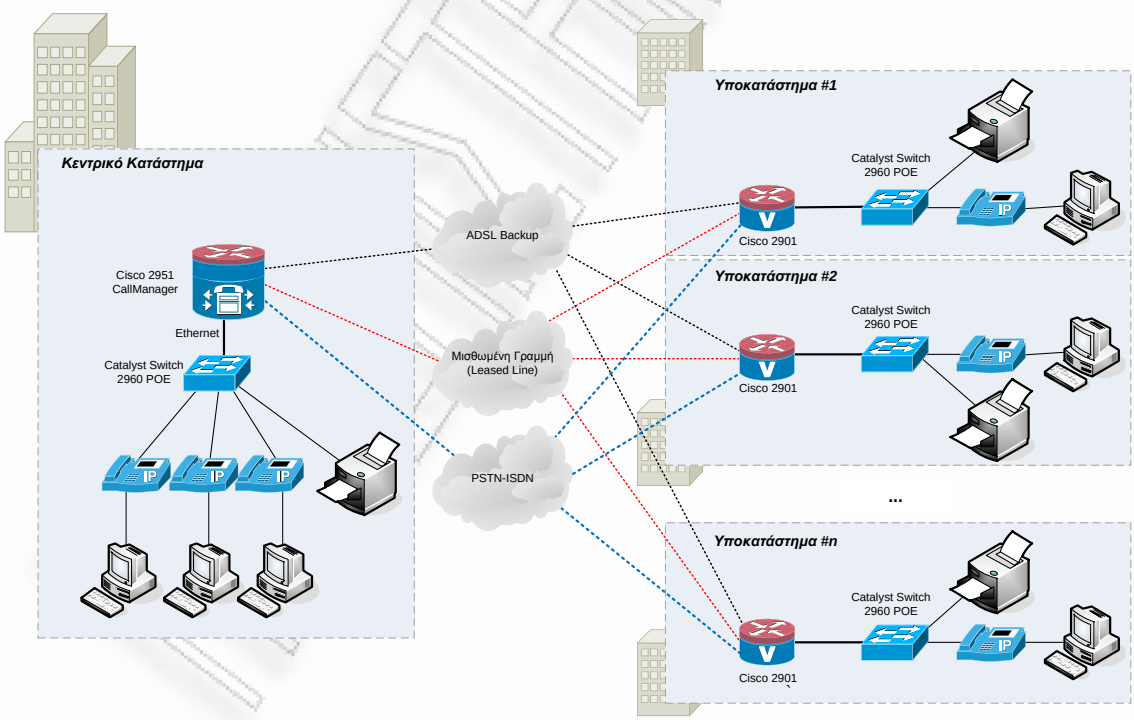
- Την επεκτασιμότητά του και την προστασία της επένδυσης ώστε μελλοντικά να μπορεί να ικανοποιήσει μεγαλύτερο αριθμό χρηστών ή να ενσωματώσει στο δίκτυο συνεργατών περισσότερα υποκαταστήματα ή και να ενσωματώσει και να αφομοιώσει νέες τεχνολογίες.
- Την ανοχή και αδιάλειπτη παροχή των υπηρεσιών σε βλάβες που σχετίζονται με τη δικτυακή υποδομή και με τις τηλεπικοινωνιακές γραμμές διασύνδεσης.
- Την όσο το δυνατόν καλύτερη διαχείριση και έλεγχο του δικτύου από κάποιο κεντρικό σημείο. Η δυνατότητα βέλτιστης διαχείρισης συμβάλλει στην ποιοτική διαφοροποίηση των παρεχομένων υπηρεσιών καθώς νέοι χρήστες μπορούν να εισάγονται στο σύστημα χωρίς να διακόπτουν την λειτουργία του ενώ επίσης τυχόν αδυναμίες του δικτύου μπορούν να εντοπίζονται και να αφαιρούνται βελτιώνοντας την απόδοση του δικτύου.

Υπερθεματίζοντας, ξεκινά η περιγραφή της προτεινόμενης σχεδίασης του δικτύου στις επόμενες παραγράφους.

Η λύση περιλαμβάνει τα εξής (βλ. Εικόνα 4-1):

1. Κεντρική σύνδεση με τον πάροχο Internet και PSTN τηλεφωνίας (πχ ΟΤΕ).
2. Εφαρμογή ολοκληρωμένης πολιτικής ασφάλειας και προστασίας της επικοινωνίας δεδομένων με τη χρήση συσκευών firewall.
3. Δημιουργία ενός δικτύου intranet που να περιλαμβάνει τα υποκαταστήματα της εταιρείας. Σε πρώτη φάση θα συμπεριλαμβάνονται δεκαέξι (16) υποκαταστήματα.
4. Υλοποίηση της υποδομής στο τοπικό δίκτυο για πιο γρήγορες και αξιόπιστες υπηρεσίες.
5. Την υλοποίηση ενοποιημένου δικτύου φωνής δεδομένων με την χρήση IP τηλεφωνίας.

Εικόνα 4-1: Συνοπτική Παρουσίαση Προτεινόμενου Δικτύου

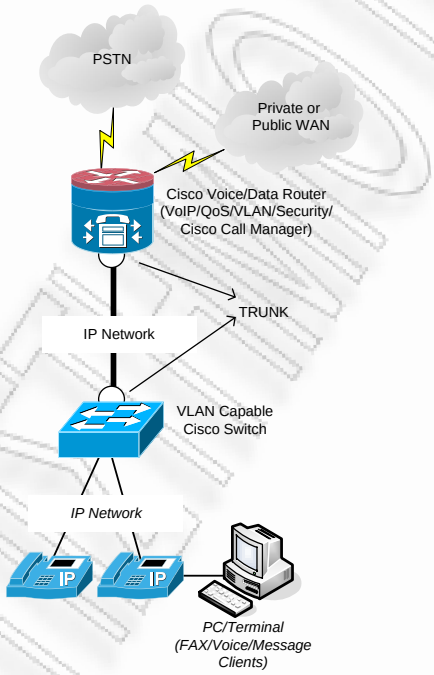


4.2.1 Cisco Unified Communications

Η ολοκληρωμένη πρόταση που προσφέρεται από την Cisco για τη μετάδοση τηλεφωνικών υπηρεσιών μέσω ενός TCP/IP δικτύου, ονομάζεται Cisco Unified Communications. Η λύση αυτή αποτελεί ουσιαστικά ένα τηλεφωνικό κέντρο (Public Branch Exchange, PBX) που χρησιμοποιεί το πρωτόκολλο IP για τη μετάδοση φωνής.

Η διαχείριση των κλήσεων γίνεται μέσω του λογισμικού πακέτου Cisco Unified Communication Manager, το οποίο είτε είναι εγκατεστημένο σε έναν εξυπηρετητή Windows Server ή βρίσκεται προ-εγκατεστημένο ως τμήμα του λειτουργικού συστήματος ενός Voice Router (π.χ. σειρά Cisco 2900 και 3900). Οι τηλεφωνικές συσκευές των τελικών χρηστών (ονομάζονται Cisco IP Phone) συνδέονται απευθείας στο δίκτυο δεδομένων μέσω του προτύπου 10/100Base-T και η ποιότητα των υπηρεσιών που προσφέρουν είναι εφάμιλλη με αυτή των συμβατικών τηλεφωνικών συσκευών. Τέλος, η διασύνδεση των χρηστών με το δημόσιο τηλεφωνικό δίκτυο ή με τα ήδη υπάρχοντα ιδιωτικά τηλεφωνικά κέντρα, γίνεται μέσω των ιδίων των Voice routers ή μέσω διασυνδέσεων προς άλλα PBXs.

Εικόνα 4-2: Cisco Communications Network



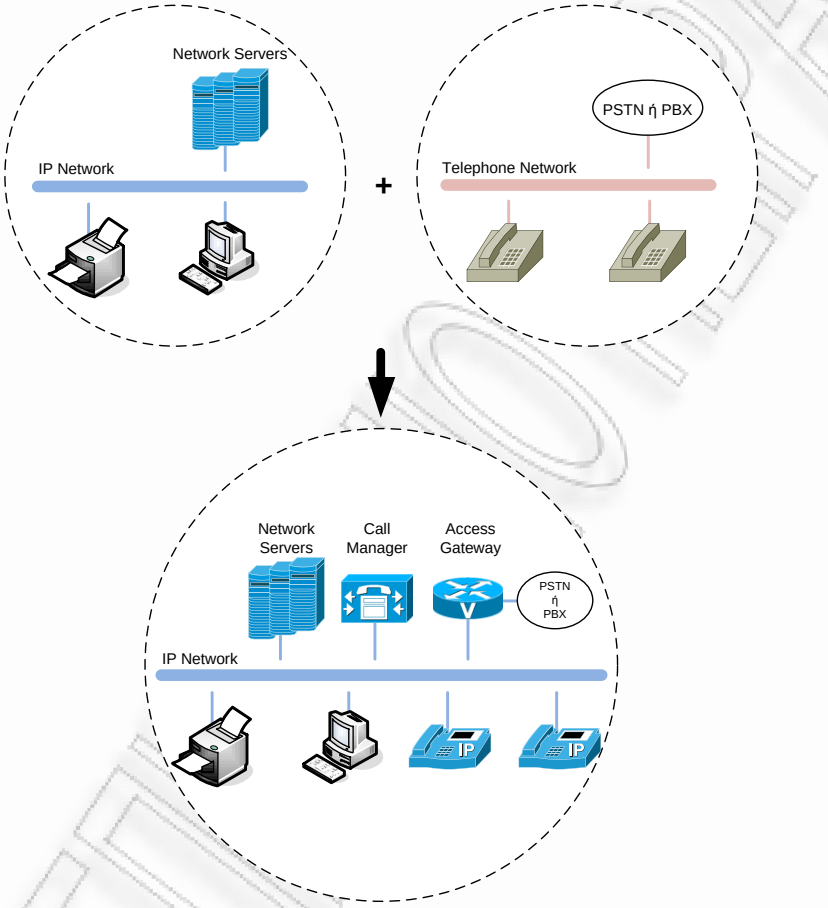
4.2.2 Απαιτήσεις για την Εφαρμογή

Η προτεινόμενη λύση λειτουργεί σε οποιοδήποτε τύπο δικτύου TCP/IP, που βασίζεται σε καλωδίωση συνεστραμμένων καλωδίων (twisted pair) κατηγορίας 4 ή καλύτερο και συνδέσμους τύπου RJ-45, κάτι που επιτρέπει τη σύνδεση των IP τηλεφωνικών συσκευών στην υπάρχουσα δικτυακή καλωδίωση.

4.2.3 Τα Δομικά Στοιχεία του Δικτύου Cisco Unified Communications

Όπως ήδη έχει αναφερθεί, με την πρόταση «Cisco Unified Communications» καλύπτεται η ανάγκη ενοποίησης του τηλεφωνικού δικτύου και του δικτύου δεδομένων. Έτσι όπως απεικονίζεται και στην Εικόνα 4-3, η παραδοσιακή μορφή, στην οποία υπάρχουν δυο διαφορετικά δίκτυα, απλοποιείται σε μια ενοποιημένη μορφή.

Εικόνα 4-3: Ενοποίηση IP και Τηλεφωνικού Δικτύου



Η αρχιτεκτονική αυτή εξυπηρετεί τα εξής:

- ✓ Λειτουργία των τηλεφωνικών υπηρεσιών μέσω του TCP/IP δικτύου χωρίς τη μείωση της απόδοσής του.
- ✓ Την πλήρη συνεργασία με τα υπάρχοντα τηλεφωνικά κέντρα και το Δημόσιο Δίκτυο Τηλεφωνίας (ΟΤΕ).
- ✓ Δια-λειτουργικότητα με τα προϊόντα (λογισμικού και συσκευών) που βασίζονται στο πρωτόκολλο Η.323.
- ✓ Παροχή ποιότητας ήχου ψηφιακού επιπέδου.

4.2.4 Υποστηριζόμενα Πρότυπα

Τα προσφερόμενα προϊόντα υποστηρίζουν τα απαιτούμενα πρότυπα και πρωτόκολλα H.323,SIP, PRI ISDN, Windows Telephony API, G.711, G.723, H.225, H.245, TCP/IP, UDP/IP, DHCP, DNS και IEEE 802.3.

H.323, SIP: Ο εξοπλισμός της Cisco είναι συμβατός με τα πρότυπα των IP επικοινωνιών, H.323 και SIP. Αυτό επιτρέπει στα προϊόντα, όπως το Cisco IP Phone, να επικοινωνούν με συσκευές συμβατές με τα πρότυπα αυτά.

Επίπεδο Ζεύξης Δεδομένων: Οι προσφερόμενες συσκευές χρησιμοποιούν το πρότυπο IEEE 802.3, 100Base-T Ethernet για τη σύνδεση στο IP δίκτυο.

ISDN Συμβατότητα (Q.931, Q.921): Χρησιμοποιείται σηματοδοσία για τον έλεγχο των κλήσεων που ακολουθεί το πρότυπο PRI ISDN των παραδοσιακών ψηφιακών τηλεφωνικών δικτύων μεταγωγής κυκλώματος. Επιτυγχάνεται έτσι η διασυνδεσιμότητα και η αλληλεπίδραση των τοπικών τηλεφωνικών κέντρων με τους παρόχους τηλεφωνικών υπηρεσιών και οποιοδήποτε ISDN δικτύου.

TAPI (Windows Telephony Application Programmer's Interface): Η αρχιτεκτονική Cisco Unified Communications περιλαμβάνει ένα προσαρμοστικό TAPI, που καλείται "Cisco-IP PBX Service Provider". Το προσαρμοστικό αυτό επιτρέπει την υλοποίηση εφαρμογών όπως voice mail και αυτόματη διανομή των κλήσεων.

4.2.5 Προτεινόμενη Ανάπτυξη με Συγκεντρωτική Διαχείριση Κλήσεων

Η τεχνική ανάπτυξης που ακολουθείται στηρίζεται στη συγκεντρωτική διαχείριση των κλήσεων που προέρχονται τόσο από τον κεντρικό κόμβο όσο και από τα υποκαταστήματα. Ως εκ τούτου, όπως απεικονίζεται και στην Εικόνα 4-1, σε ένα δρομολογητή του κεντρικού καταστήματος υπάρχει προ-εγκατεστημένος ένας Communication Manager υπεύθυνος για την επεξεργασία και διαχείριση των κλήσεων όλου του δικτύου.

Το κυριότερο πλεονέκτημα της ανάπτυξης αυτής, είναι η ικανότητα κεντρικής διαχείρισης των κλήσεων πράγμα που μειώνει τον απαιτούμενο εξοπλισμό στα περιφερειακά υποκαταστήματα. Ως συνακόλουθο, δεν απαιτείται επιπλέον φόρτος διαχείρισης σε κάθε σημείο χωριστά. Επιπλέον, πέρα από τη σύνδεση των υποκαταστημάτων μέσω του δικτύου ευρείας περιοχής (WAN) υπάρχει και ADSL εφεδρική διασύνδεση των υποκαταστημάτων με το κεντρικό. Έτσι σε περίπτωση αστοχίας της WAN σύνδεσης, επιτυγχάνεται η εξασφάλιση της προσφοράς των υπηρεσιών του δικτύου μέσω των ADSL γραμμών. Το γεγονός αυτό αυξάνει τη διαθεσιμότητα και αξιοπιστία των προσφερόμενων υπηρεσιών.

Το λογισμικό «Cisco Unified Communications Manager», αποτελεί τον εξυπηρετητή (server) της λύσης «Cisco Unified Communications Network». Είναι μια εφαρμογή client/server που ελέγχει τη διαδικασία και τη δρομολόγηση των κλήσεων καθώς και τα χαρακτηριστικά των συσκευών (IP Phone, Gateways). Η βάση δεδομένων που περιέχει τις πληροφορίες παραμετροποίησης των συσκευών μπορεί να βρίσκεται τόσο στον ίδιο εξυπηρετητή είτε σε διαφορετικό. Η διαχείριση της βάσης δεδομένων γίνεται μέσω γραφικού interface που χρησιμοποιεί έναν φιλομετρητή (IE, Mozilla, κτλ), με αποτέλεσμα να γίνεται αν απαιτείται και απομακρυσμένα.

Κάθε IP τηλέφωνο πρώτα πρέπει να εγγράφεται στο λογισμικό διαχείρισης κλήσεων ώστε το τελευταίο να του παρέχει χαρακτηριστικά τηλεφωνίας όπως συγκράτηση κλήσεων, μεταφορά, μεταβίβαση, φραγή, καθώς και δημιουργία αναλυτικών αρχείων κλήσεων κατάλληλα για χρέωση. Βέβαια ανάλογα με την αντίστοιχη έκδοση μεταβάλλονται οι δυνατότητες και οι παρεχόμενες υπηρεσίες. Στη συνέχεια ακολουθεί ο Πίνακας 4-1, στον οποίο αναφέρονται όλες οι έως τώρα εκδόσεις του Cisco Call Manager καθώς και τα βασικά πλεονεκτήματα κάθε έκδοσης.

Πίνακας 4-1: Προσφερόμενες Εκδόσεις του Cisco Call Manager

Μοντέλο	Αριθμός εργαζομένων	Βασικά πλεονεκτήματα
Cisco Unified Communications 500 Series	5-50	✓ Σχεδιασμένο για να συνεργάζεται με υπάρχουσες εφαρμογές παραγωγικότητας μέσω της επιφάνειας εργασίας και προγράμματα διαχείρισης πελατειακών σχέσεων ✓ Ενοποιείται με το Cisco Unified Communications Manager Express ✓ Διαθέσιμο ως εφαρμογή ενός διακομιστή
Cisco Unified Communications Manager Express	Έως 240	✓ Προεγκατεστημένο στους Cisco Integrated Services Routers ✓ Εύκολη σύνδεση σε γραφείο χρησιμοποιώντας το Cisco Unified Communications Manager
Cisco Unified Communications Manager Business Edition	Έως 500	✓ Υποστηρίζει καινοτόμες τηλεφωνικές εφαρμογές ✓ Υποστηρίζει επικοινωνίες φωνής και φορητότητα σε έναν μόνο διακομιστή ✓ Λειτουργεί σε πέντε τοποθεσίες
Cisco Unified Communications Manager	Από 150 έως 40000 (σε Cluster)	✓ Πλήθος δυνατοτήτων επέκτασης για να προσαρμόζεται στις αυξανόμενες ανάγκες της επιχείρησής ✓ Υποστηρίζει καινοτόμες τηλεφωνικές εφαρμογές ✓ Διαθέσιμο ως εφαρμογή single-server ✓ Συνεργασία με διακομιστές τρίτων κατασκευαστών ή με τον διακομιστή Cisco 7800 Series Media Convergence Server

Αναλυτικότερα ορισμένες από τις λειτουργίες του λογισμικού Cisco Call Manager αναφέρονται στη συνέχεια:

- **Αυτόματη επιλογή του καταλαμβανόμενου από την κλήση εύρους** (Automatic Bandwidth Selection). Η λειτουργία αυτή επιτρέπει τον καθορισμό του καταλαμβανόμενου εύρους μεταξύ συσκευών που ανήκουν σε καθορισμένες περιοχές. Έτσι η τηλεφωνική κλήση μεταξύ απομακρυσμένων περιοχών μπορεί να συμπιεστεί (π.χ. σε 8 Kbps), ενώ η κλήση μεταξύ συσκευών που ανήκουν στην ίδια περιοχή μπορεί να χρησιμοποιεί όλο το διαθέσιμο εύρος του καναλιού (π.χ. 64 Kbps).
- **Αυτόματη εγκατάσταση του IP τηλεφώνου** (Automatic Phone Installation). Παρέχεται η δυνατότητα της εγκατάστασης και της αρχικής παραμετροποίησης των IP τηλεφωνικών συσκευών κατά την σύνδεσή τους στο δίκτυο.
- **Αυτόματη μετακίνηση των συσκευών** (Automatic Phone Moves). Η λειτουργία αυτή επιτρέπει την μεταφορά των συσκευών σε οποιοδήποτε σημείο του δικτύου χωρίς αλλαγή των παραμέτρων. Αυτό είναι εφικτό γιατί όλες οι πληροφορίες διευθυνσιοδότησης της συσκευής αποθηκεύονται στη flash μνήμη της συσκευής.
- **Λεπτομερή Αρχεία Κλήσεων** (Call Detail Records). Η λειτουργία αυτή παρέχει λεπτομερές ιστορικό για κάθε εισερχόμενη και εξερχόμενη κλήση.

- **Υπηρεσία DHCP των Cisco IP Phone**. Οι τηλεφωνικές συσκευές Cisco IP Phone, υποστηρίζουν το πρωτόκολλο Dynamic Host Configuration Protocol (DHCP). Με τον τρόπο αυτό είναι δυνατή η αυτόματη διευθυνσιοδότηση των τηλεφωνικών συσκευών.
- **Προγραμματισμός κλήσεων** (Dial Plan). Το πακέτο Cisco CallManager παρέχει πολλές δυνατότητες στον προγραμματισμό των κλήσεων και στη δρομολόγησή τους. Για παράδειγμα μπορεί να γίνει δρομολόγηση των κλήσεων προς τις πύλες θέτοντας ως κριτήριο τους αριθμούς της κλήσης ή το είδος της κλήσης (εσωτερική, υπεραστική ή διεθνής).
- **Φραγή κλήσεων** (Call Blocking). Παρέχεται η δυνατότητα απαγόρευσης εξερχόμενων κλήσεων προς συγκεκριμένους αριθμούς ή ομάδες αριθμών. Όταν γίνεται μια κλήση προς ένα απαγορευμένο αριθμό, η κλήση αυτή δεν δρομολογείται.
- **Κωδικοί Πρόσβασης Φορέων** (Carrier Access Codes). Παρέχεται η δυνατότητα προγραμματισμού της δρομολόγησης των κλήσεων σε εξωτερικά τηλεφωνικά δίκτυα, ανάλογα με τον κωδικό πρόσβασης του εξωτερικού φορέα.
- **Κωδικός Πρόσβασης Κλήσης** (Dial Access Code). Μια κλήση μπορεί να δρομολογηθεί σε προεπιλεγμένους προορισμούς ανάλογα με τον κωδικό πρόσβασης που προηγείται του αριθμού της κλήσης. Για παράδειγμα, για εξωτερικές κλήσεις, προηγείται ο αριθμός 9.
- **Προγραμματισμός Ιδιωτικής Αριθμοδότησης** (Private Numbering Plan). Η οργάνωση της αριθμοδότησης μπορεί να γίνει είτε αυτόνομα είτε σύμφωνα με την υπάρχουσα αριθμοδότηση. Οι αριθμοί των εσωτερικών τηλεφώνων, μπορούν να κυμαίνονται μεταξύ 1 και 23 ψηφίων.
- **Διεπιλογή** (Direct Inward dialing, Direct Outward). Παρέχεται η δυνατότητα απ' ευθείας κλήσης του εσωτερικού τηλεφωνικού αριθμού από το δημόσιο δίκτυο.
- **Αναφορές Γεγονότων** (Event logging and reports). Γίνεται καταγραφή των γεγονότων λειτουργίας του λογισμικού CallManager σε κατάλληλο βοηθητικό πακέτο λογισμικού (Event Viewer). Οι καταγραφές αυτές μπορούν να χρησιμοποιηθούν για την παρακολούθηση της σωστής λειτουργίας του συστήματος.
- **External voice messaging (VM)/automated attendant (AA)/interactive voice rensponse system (IVR)**. Είναι δυνατή η σύνδεση εξωτερικών συστημάτων για την παροχή: Μηνυμάτων Φωνής (Voice messaging), Εκτροπής κλήσεων σε επιλεγμένους σταθμούς και Δυνατότητες IVR (interactive voice response system).
- **Υποστήριξη IP Precedence bit για τα IP τηλέφωνα και τις Πύλες της Cisco**.Τα πακέτα φωνής που προέρχονται από τις IP τηλεφωνικές συσκευές και τις Πύλες της εταιρίας Cisco, μπορούν να αποκτήσουν προτεραιότητα κατά την επεξεργασία τους από τους δρομολογητές της Cisco.
- **Φορητότητα Αριθμού**.Το χαρακτηριστικό αυτό επιτρέπει την τοποθέτηση της τηλεφωνικής συσκευής σε οποιοδήποτε σημείο του δικτύου, χωρίς την αλλαγή του τηλεφωνικού αριθμού.

4.2.6 Πύλες Πρόσβασης (Access Gateway)

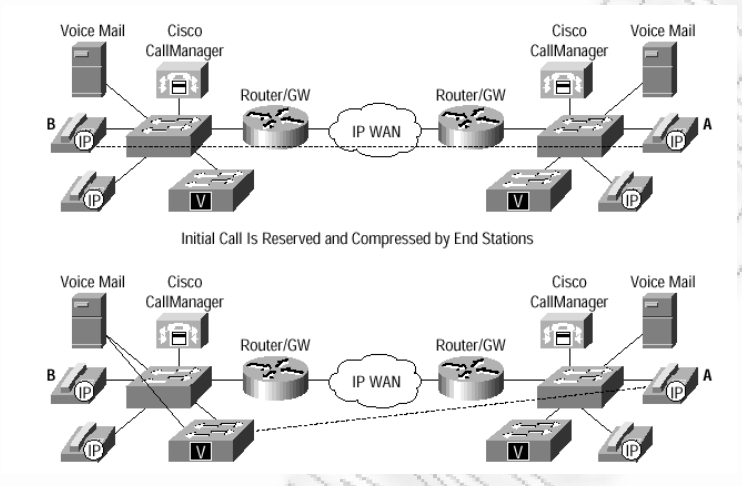
Οι πύλες πρόσβασης συνδέουν τα συμβατά με το πρωτόκολλο H.323 τερματικά, με συσκευές που είναι συνδεδεμένες με άλλα δίκτυα όπως PSTN και ISDN. Οι συσκευές αυτές μετατρέπουν τη σηματοδοσία και το πακέτο δεδομένων σε μορφή που υποστηρίζεται από το νέο δίκτυο. Δύο H.323 τερματικά επικοινωνούν χωρίς τη μεσολάβηση κάποιας πύλης πρόσβασης.

Βάσει του προτεινόμενου μοντέλου, στο κεντρικό κατάστημα, η λειτουργία αυτή υλοποιείται με τη χρήση της κάρτας με κωδικό **HWIC-2CE1T1-PRI** όπου καταλαμβάνει ένα WIC slot του δρομολογητή σε συνδυασμό με Cisco IOS IP Plus Feature Set που εγκαθίσταται στον Cisco 2951.

Επιπλέον η κάρτα είναι υπεύθυνη για:

- Τη μετατροπή μεταξύ διαφορετικών κωδικοποιήσεων (Transcoding). Υποστηρίζει τα σημαντικότερα πρότυπα όπως G.711, G.729a και G.723 που είναι και τα πιο ευρέως χρησιμοποιούμενα στην IP τηλεφωνία. Τα πρότυπα αυτά ορίζουν τον τρόπο δειγματοληψίας κατά την ψηφιοποίηση του αναλογικού σήματος φωνής. Έτσι επιτρέπει την επικοινωνία μεταξύ συσκευών που υποστηρίζουν διαφορετικά πρότυπα ψηφιοποίησης φωνής.

Εικόνα 4-4: Transcoding

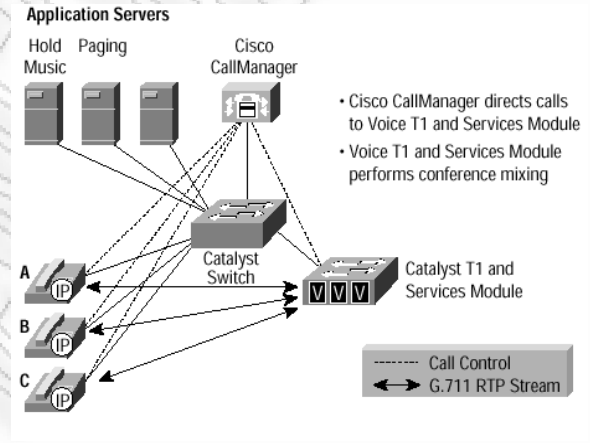


[3]

Στο υποθετικό σενάριο της Εικόνας 4-4, τα τερματικά Α και Β υποστηρίζουν επικοινωνία με συμπιεσμένο ψηφιακό σήμα φωνής. Έτσι είναι δυνατή η απευθείας επικοινωνία μεταξύ τους. Έστω ότι το τερματικό Β για κάποιο λόγο δεν απαντά στην κλήση από το Α. Τότε η κλήση προωθείται σε ένα σύστημα Voice Mail που δεν υποστηρίζει συμπίεση φωνής. Η επικοινωνία επιτυγχάνεται και το μήνυμα αποθηκεύεται καθώς η κάρτα αναλαμβάνει τη μετατροπή από το ένα πρότυπο κωδικοποίησης στο άλλο.

- Τη λειτουργία συνδιάσκεψης, μέσω της οποίας εγκαθίσταται συνομιλία μεταξύ περισσοτέρων των 2 συνομιλητών. Η λειτουργία αυτή παρουσιάζεται στην Εικόνα 4-5.

Εικόνα 4-5: Λειτουργία Συνδιάσκεψης



[3]

Το Β IP τηλέφωνο συνδιασκέπτεται με τα Α και C. Ο Call Manager κατευθύνει τα τρία κανάλια φωνής στην κάρτα. Η κάρτα εν συνεχεία γεφυρώνει τα τρία κανάλια φωνής υποστηρίζοντας με τον τρόπο αυτό τη συνδιάσκεψη μεταξύ των 3 τερματικών. Ο συνδυασμός των δύο παραπάνω χαρακτηριστικών επιτρέπει σε τερματικά που υποστηρίζουν διαφορετικά πρότυπα αποκωδικοποίησης να συμμετέχουν σε συνδιασκέψεις.

4.3 Κεντρικός Κόμβος - Περιγραφή Υποδομής

4.3.1 Διασύνδεση με το Internet και τους Περιφερικούς Κόμβους

Για τη σύνδεση με το Internet και την τηλεπικοινωνιακή διασύνδεση (φωνή/δεδομένα) των υποκαταστημάτων προτείνεται ένας δρομολογητής Cisco 2951 ο οποίος έχει πέραν της μίας WAN συνδέσεις προς υποκαταστήματα και μια σύνδεση στο LAN της εταιρείας.

Οι δρομολογητές αυτοί διακρίνονται για τις υψηλές επιδόσεις, την ευελιξία, την πολυσυλλεκτικότητα των υπηρεσιών που υποστηρίζουν, την επεκτασιμότητά τους και την υψηλή πυκνότητα θυρών. Υπάρχει μεγάλη ποικιλία από 70 διαφορετικές διαθέσιμες Service Modules (SM) και WIC κάρτες, γεγονός που δίνει πολύ μεγάλη ευελιξία, καθώς υπάρχουν τελικά αναρίθμητοι συνδυασμοί πλήρους διάρθρωσης. Καθώς έχουν αρθρωτή pay-as-you-grow αρχιτεκτονική, είναι κατάλληλοι για να καλύπτουν τις ανάγκες μιας επιχείρησης καθώς αυτές μεγαλώνουν. Ενδεικτικά αναφέρεται ότι ο Cisco 2951 μπορεί να υποστηρίξει έως 24 σύγχρονες ή 96 ασύγχρονες σειριακές συνδέσεις, μέχρι 8 συνδέσεις ISDN PRI, 24 ISDN BRI, επιπλέον μπορεί να στεγάσει εσωτερικά έως 120 ψηφιακά μόντεμ για εξυπηρέτηση κλήσεων φωνής ή/και δεδομένων. Το λογισμικό του είναι βασισμένο στην κοινή πλατφόρμα λογισμικού των δρομολογητών της Cisco, το Cisco IOS για την οικογένεια 2900. Διαθέτει κεντρικό επεξεργαστή αρχιτεκτονικής multi-core και έχει τη δυνατότητα να εκτελεί περίπλοκους αλγορίθμους δρομολόγησης πακέτων με υψηλή διεκπεραιωτική ικανότητα.

Εικόνα 4-6: Ο Δρομολογητής Cisco 2951

[23]

Οι δρομολογητές Cisco 2951 είναι αρθρωτής αρχιτεκτονικής καθώς διαθέτουν δύο υποδοχές για κάρτες NM (Network Modules) και 4 υποδοχές για WIC κάρτες. Ανάλογα με την επιλογή των καρτών μπορούν να χρησιμοποιηθούν σε εφαρμογές όπως για:

- Ασφαλή πρόσβαση στο Internet και στο Intranet.
- Ολοκλήρωση υπηρεσιών φωνής/δεδομένων/βίντεο.
- Υπηρεσίες πρόσβασης από PSTN και ISDN δίκτυα.
- Δημιουργία Virtual Private Networks (VPNs) μέσω IPSec.
- Δρομολόγηση ιδεατών υποδικτύων (VLANs).
- Υποστήριξη HSRP (Hot standby routing protocol).
- Υποστήριξη QoS.
- Δρομολόγηση καναλιών φωνής μέσα από το δίκτυο δεδομένων με προφανές όφελος στο κόστος τηλεφωνικών συνδιαλέξεων.

Το πανίσχυρο λειτουργικό σύστημα Cisco IOS είναι υπεύθυνο για το άριστο και πλούσιο σε λειτουργίες υπόβαθρο της συσκευής καθώς και για τις εξαιρετικές επιδόσεις της.

Μερικά από τα χαρακτηριστικά του είναι:

- Ενσωματωμένες λειτουργίες, πρωτόκολλα και υπηρεσίες αναφορικά με τη μετάδοση φωνής.
- Εξειδικευμένα DSP (Digital Signal Processor) κυκλώματα νέας γενιάς.
- Ενσωμάτωση του συστήματος Cisco Unified Communication Manager Express το οποίο είναι το υπεύθυνο λογισμικό για τον προγραμματισμό, τη δρομολόγηση και τη διαχείριση όλων των στοιχείων που ολοκληρώνουν ένα VoIP δίκτυο, καθώς επίσης και για την επεξεργασία των κλήσεων.
- Υποστήριξη SIP (session initiation protocol) πρωτοκόλλου.
- Υποστήριξη Voice Activity Detection (VAD), το οποίο ανιχνεύει την ύπαρξη «σιωπής» κατά τη διάρκεια μια συνδιάλεξης, ώστε τα πακέτα που μεταφέρονται να περιέχουν μόνο φωνή.
- Υποστήριξη συμπίεσης Real Time Protocol (cRTP).
- Υποστήριξη voicemail.
- Ολοκληρωμένο σύστημα firewall, intrusion detection και content filtering.
- Ενσωματωμένο σύστημα AAA (Authentication, Authorization, Accounting).
- Υποστηριζόμενα πρωτόκολλα: IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
- Υποστηριζόμενα πρωτόκολλα ενθυλάκωσης (encapsulation): Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE) και ATM.
- Υποστηριζόμενα πρωτόκολλα διαχείρισης δικτυακής κίνησης: QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR) και Network-Based Advanced Routing (NBAR).

4.3.2 Προτεινόμενη Διάρθρωση του Κεντρικού Δρομολογητή

Ο κεντρικός δρομολογητής **Cisco 2951**, περιλαμβάνει σασί, τροφοδοτικό AC, 3 ενσωματωμένες κάρτες υποδοχής τύπου Ethernet, έως 8 ελεύθερες υποδοχές για κάρτες επέκτασης, λογισμικό Cisco IOS, 512 MB μνήμη τύπου DRAM, 256MB μνήμη τύπου Flash.

Οι κάρτες επέκτασης που θα χρησιμοποιηθούν στον κεντρικό router είναι:

1. **SM-NM-ADPTR**

Η προσφερόμενη κάρτα ανήκει στην οικογένεια των καρτών NM (Network Modules). Οι κάρτες της οικογένειας αυτής διαθέτουν δύο θέσεις για την τοποθέτηση θυγατρικών καρτών. Οι θυγατρικές κάρτες υποστηρίζουν μία μεγάλη ποικιλία από interface και πρωτόκολλα επικοινωνίας αυξάνοντας την ευελιξία ανάπτυξης. Επιπλέον, η ευελιξία αυτή προσαυξάνεται

από το γεγονός ότι στην ίδια μητρική NM κάρτα μπορούν να φιλοξενηθούν διαφορετικού τύπου θυγατρικές κάρτες. Έτσι προσαυξάνεται η ικανότητα διασύνδεσης του δρομολογητή.

Εικόνα 4-7: Η κάρτα SM-NM-ADPTR

[23]

2. HWIC-2CE1T1-PRI Cisco Channelized T1/E1 and ISDN PRI Module

Η συγκεκριμένη κάρτα θα χρησιμοποιηθεί για τη διασύνδεση με τον ΟΤΕ και την υποστήριξη VoIP στο δίκτυο. Η κάρτα HWIC-2CE1T1-PRI διαθέτει δύο θύρες που υποστηρίζουν channelized E1 επικοινωνία. Υποστηρίζει έως 2 E1 διασυνδέσεις με τον τηλεπικοινωνιακό πάροχο για απόδοση έως και 60 ταυτόχρονων καναλιών φωνής. Η επιλογή δικτύου (E1 ή T1) γίνεται μέσω software. Διαθέτει ολοκληρωμένο σύστημα CSU/DSU καθιστώντας μη αναγκαία την ύπαρξη εξωτερικού modem για τη διασύνδεση. Υποστηρίζει E1 διασύνδεση και συμμορφώνεται με τα στάνταρντ G.703 και G.704.

Εικόνα 4-8: Η Κάρτα HWIC-2CE1T1 για Διασύνδεση με τον Τηλεπικοινωνιακό Πάροχο

[23]

3. HWIC-4T, 4-Port Serial High-Speed WAN Interface Card

Η κάρτα HWIC-4T θα είναι υπεύθυνη για τη διασύνδεση του κεντρικού με τα υποκαταστήματα. Υποστηρίζει σειριακές συνδέσεις μέσω μισθωμένων κυκλωμάτων και βασίζεται στην ύπαρξη κατάλληλου modem, το οποίο παρέχεται από τον πάροχο της γραμμής. Οι κάρτες αυτές υποστηρίζουν ταχύτητες έως 8Mbps ανά πόρτα. Ο τύπος της διεπαφής (interface) επικοινωνίας καθορίζεται από τον τύπο του καλωδίου προσαρμογής που συνδέεται στην θύρα της κάρτας.

Εικόνα 4-9: Η Κάρτα HWIC-4T για Διασύνδεση Κεντρικού με Υποκαταστήματα Μέσω Μισθωμένων Γραμμών

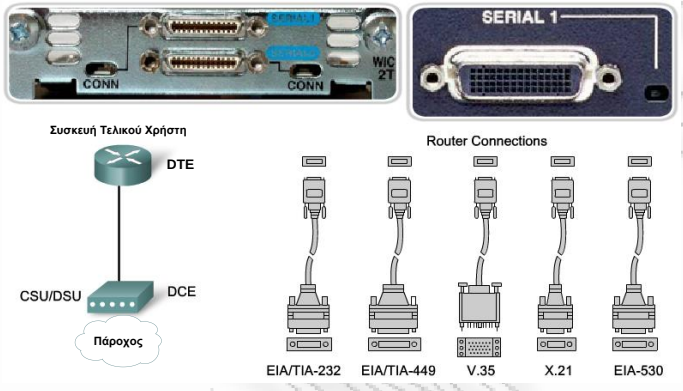
[23]

Τα υποστηριζόμενα interface είναι τα V.35, X.21, RS-232, RS-449, RS-530 και καθορίζονται από τα παρακάτω καλώδια σύνδεσης:

- ✓ CAB-SS-V35 MT/FC
- ✓ CAB-SS-232 MT/FC
- ✓ CAB-SS-449 MT/FC
- ✓ CAB-SS_X21 MT/FC
- ✓ CAB-SS-530 MT

Ο τύπος του interface αλλάζει με απλή σύνδεση του αντίστοιχου καλωδίου προσαρμογής χωρίς να απαιτείται αλλαγή ή τοποθέτηση άλλης κάρτας.

Εικόνα 4-10: Πρότυπα Σειριακών Συνδέσεων Φυσικού Επιπέδου[10]



4. HWIC-1ADSL, 1-port ADSL

Η κάρτα HWIC-1ADSL θα χρησιμοποιηθεί σε περίπτωση όπου η μισθωμένη σύνδεση του κεντρικού με κάποιο από τα υποκαταστήματα διακοπεί και χρειάζεται εναλλακτική πρόσβαση (backup[11]). Υποστηρίζει το πρότυπο Annex A για διασύνδεση μέσω απλής τηλεφωνικής σύνδεσης (PSTN). Προσφέρει υψηλές ταχύτητες διασύνδεσης μέχρι 12Mbps downstream και 1Mbps upstream καθώς υποστηρίζει το πρότυπο ADSL2.

Μια δεύτερη όμοια κάρτα HWIC-1ADSL θα χρησιμοποιηθεί για τη σύνδεση του κεντρικού κόμβου με το Internet και την παροχή υπηρεσιών δεδομένων (http,dns,ftp,mail κλπ.) προς το εσωτερικό δίκτυο.

Εικόνα 4-11: Η Κάρτα HWIC-1ADSL για Διασύνδεση με ADSL-ISP

[23]

[10] DTE: Data Terminal Equipment, DCE: Data Circuit-Terminal Equipment (π.χ. ένα modem)

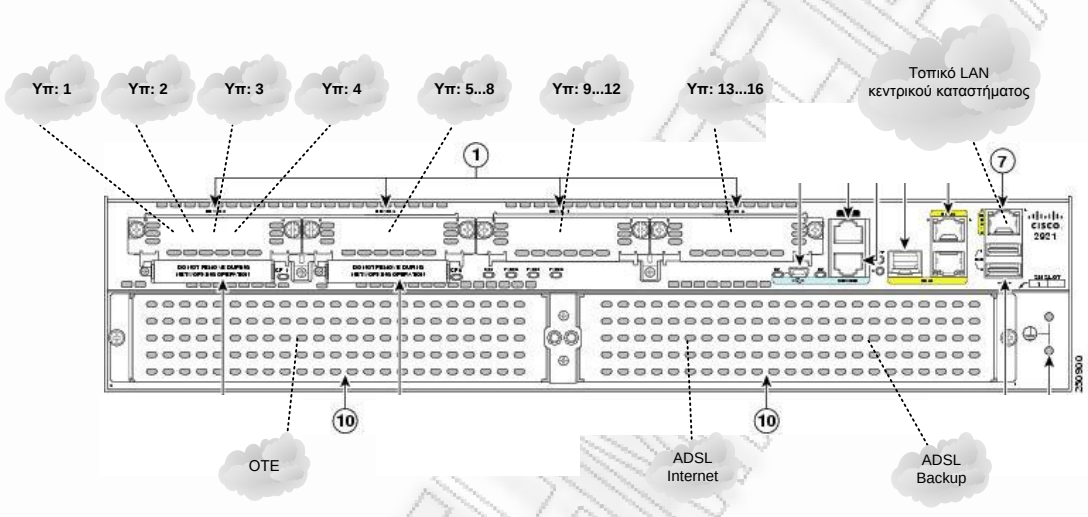
[11] Για να δρομολογηθεί η κίνηση από την εναλλακτική διαδρομή, απαιτείται στο interface της μισθωμένης γραμμής να καθοριστεί το όνομα του backup interface καθώς και ο χρόνος αναμονής πριν τη δρομολόγηση.
backup interface *<όνομα backup διεπαφής>*
backup delay 0 *<χρονική διάρκεια αναμονής>*

Συνοπτικά ο κεντρικός Router θα διαθέτει:

- ✓ **4 x 4 HWIC-4T** για τη σύνδεση έως 16 απομακρυσμένων υποκαταστημάτων μέσω μισθωμένων γραμμών
- ✓ **1 x HWIC-2CE1T1-PRI** για τη διασύνδεση του δικτύου με το τηλεφωνικό δίκτυο ΟΤΕ ή άλλου παρόχου.
- ✓ **2 x HWIC-1ADSL** για τη σύνδεση με το internet και την backup διασύνδεση με τα υποκαταστήματα.

Και η τελική μορφή που θα έχει απεικονίζεται στη συνέχεια:

Εικόνα 4-12: Προτεινόμενη Διάρθρωση του Κεντρικού Δρομολογητή



Θέση 1: WIC slots - 4 HWIC-4T για διασύνδεση με υποκαταστήματα
Θέση 10: NM slots με αντάπτορα SM-NM-ADPTR
- Αριστερά: HWIC-2CE1T1-PRI για σύνδεση με την υποδομή του ΟΤΕ
- Δεξιά: 2 x HWIC-1ADSL για σύνδεση Internet και Backup προς υποκαταστήματα

Θέση 7: Ethernet port – Gigabit διασύνδεση με τοπικό δίκτυο

4.3.3 Σύστημα Διασύνδεσης Τοπικών Χρηστών

Ο μεταγωγέας (switch) που θα χρησιμοποιηθεί για τη διασύνδεση των συστημάτων και των χρηστών στο τοπικό δίκτυο LAN του κεντρικού καταστήματος είναι ο Cisco Catalyst 2960-48PST-L της σειράς Catalyst 2960.

Εικόνα 4-13: Διασύνδεσης Τοπικών Χρηστών - Cisco Catalyst 2960

[24]

Η οικογένεια μεταγωγέων 2960 της εταιρείας Cisco αποτελείται από τα προϊόντα 2960-12, 2960-24, 2960-48. Οι συσκευές αυτές διαθέτουν 12, 24 και 48 θύρες 10BaseT/100BaseTX/1000BaseTx αντίστοιχα και επιπλέον από 2 ή 4 υποδοχές uplinks για τη διασύνδεση τους με άλλα συστήματα (routers, switches). Η προτεινόμενη συσκευή με κωδικό 2960-48PST-L διαθέτει 48 θύρες που υποστηρίζουν Gigabit Ethernet και power over Ethernet (POE) και 2 uplinks.

Τα μέλη της οικογένειας 2960 αποτελούν υψηλής απόδοσης μεταγωγείς με μεγάλη ευκολία στη διαχείριση και ευελιξία στις σχεδιάσεις-αναπτύξεις δικτύων. Διαθέτουν στάνταρ 16 Gbps χωρητικότητα διαύλου και η ταχύτητα διόδευσης πακέτων μπορεί να φτάσει τα 10.1 Mpps. Είναι διαχειρίσιμοι τόσο με τη χρήση του πρωτοκόλλου SNMP όσο και μέσω Telnet ή μέσω ενσωματωμένου περιβάλλοντος διαχείρισης. Τα κυριότερα χαρακτηριστικά τους είναι τα εξής

- ✓ Διαθέτουν 12, 24 ή 48 θύρες 10/100/1000 ανάλογα με το μοντέλο. Διαθέτουν έως 4 ενσωματωμένες θύρες uplink. Τα SFP (small factor port) μπορούν να χρησιμοποιηθούν είτε ως uplinks προς τον κορμό του δικτύου είτε για την ανάπτυξη διατάξεων μεταγωγέων σε ακολουθιακή τοπολογία, τοπολογία αστέρα, στοίβα κ.λπ..
- ✓ Υποστήριξη του πρωτοκόλλου Gigabit Ethernet IEEE 802.3z.
- ✓ Υποστήριξη των 1000BaseSX, 1000BaseLX/LH και 1000BaseZX φυσικών interface.
- ✓ Δίαυλο χωρητικότητας 16 Gbps.
- ✓ Κλιμακούμενη, ανάλογα με τον αριθμό των θυρών, ταχύτητα μεταγωγής που φτάνει τα 10 Mpps.
- ✓ Υποστήριξη full-duplex λειτουργίας σε όλες τις θύρες.
- ✓ Δυνατότητα ομαδοποίησης θυρών με χρήση των τεχνολογιών fast EtherChannel και Gigabit EtherChannel δίνοντας έτσι έως 8 Bbps bandwidth σε συνδέσεις μεταξύ μεταγωγέων, δρομολογητών ή/και εξυπηρετητών.
- ✓ Απομόνωση θυρών που εμφανίζουν συγκρούσεις ή δυσλειτουργία.
- ✓ Υποστήριξη VLANs σε όλες τις θύρες.
- ✓ Υποστήριξη πρωτοκόλλου STP (IEEE 802.1D).
- ✓ Υποστήριξη STP ανά VLAN (STP per VLAN).
- ✓ Υποστήριξη των πρωτοκόλλων IEEE 802.1Q και ISL.
- ✓ Υποστήριξη του πρωτοκόλλου IEEE 802.1p σε συνδυασμό με 2 ουρές προτεραιότητας. Η υποστήριξη του πρωτοκόλλου IEEE 802.1p τα καθιστά ιδανικά για την ανάπτυξη εφαρμογών IP τηλεφωνίας. Σύμφωνα με το πρωτόκολλο αυτό δημιουργούνται ουρές εξυπηρέτησης με διαφορετικές προτεραιότητες. Τα πακέτα πληροφορίας με την υψηλότερη προτεραιότητα εξυπηρετούνται πρώτα, εξασφαλίζοντας την ποιότητα επικοινωνίας των κρίσιμων εφαρμογών. Έτσι, ακολουθώντας το πρότυπο αυτό, εφαρμογές VoIP αποκτούν μεγαλύτερη προτεραιότητα σε σχέση με εφαρμογές μη κρίσιμες, όπως για παράδειγμα, FTP ή από web browsing.
- ✓ Διαχείριση μέσω SNMP, Telnet.
- ✓ Υποστήριξη RMON, TFTP, NTP, ARP.
- ✓ Περιορισμό στην πρόσβαση σε κάθε θύρα σε επίπεδο MAC διεύθυνσης.
- ✓ Προστασία διαχείρισης με password.
- ✓ Υποστήριξη Power over Ethernet (PoE). Ο μεταγωγέας Catalyst 2960, διαθέτει την ικανότητα τροφοδοσίας συσκευών με DC ρεύμα. Πιο συγκεκριμένα, η τροφοδοσία ισχύος γίνεται μέσω του καλωδίου σύνδεσης της τερματικής συσκευής (πχ. IP Phone) με τον μεταγωγέα. Εφόσον η συνδεόμενη συσκευή έχει την ικανότητα τροφοδοσίας μέσω καλωδίου UTP (π.χ. Cisco 7900 family IP phones) τότε μπορεί να τροφοδοτηθεί με ηλεκτρική ισχύ απευθείας από τον μεταγωγέα.

4.4 Περιφεριακοί Κόμβοι - Περιγραφή Υποδομής

4.4.1 Διασύνδεση με το Internet και τον Κεντρικό Κόμβο

Για τη διασύνδεση των υποκαταστημάτων με τον κεντρικό κόμβο και τις υπηρεσίες φωνής δεδομένων, προτείνεται ο δρομολογητής Cisco 2901. Ανήκει στην ίδια οικογένεια με τον Cisco 2951 με τη μόνη διαφορά ότι δέχεται χαμηλότερο αριθμό καρτών.

Η διάρθρωση κάθε δρομολογητή μπορεί να είναι διαφορετική ανάλογα με τις ανάγκες του αντίστοιχου υποκαταστήματος. Παραδείγματος χάριν, σε ένα υποκατάστημα με μικρό αριθμό υπαλλήλων και ως εκ τούτου και μικρό φορτίο τηλεπικοινωνιακής κίνησης, ίσως να μην κριθεί απαραίτητη η απευθείας διασύνδεση με το PSTN δίκτυο. Σε αυτή την περίπτωση στο δρομολογητή του συγκεκριμένου υποκαταστήματος, δεν απαιτείται η εγκατάσταση της HWIC-2CE1T1-PRI κάρτας μιας και όλη η κίνηση θα δρομολογείται από και προς το κεντρικό κατάστημα.

Εικόνα 4-14: Ο δρομολογητής Cisco 2901

[24]

4.4.2 Προτεινόμενη Διάρθρωση Δρομολογητή Υποκαταστήματος

Περιλαμβάνει σασί, τροφοδοτικό AC, 2 ενσωματωμένες κάρτες υποδοχής τύπου Ethernet, έως 4 ελεύθερες υποδοχές για κάρτες επέκτασης (WIC), λογισμικό Cisco IOS, 512 MB μνήμη τύπου DRAM, 256MB μνήμη τύπου Flash.

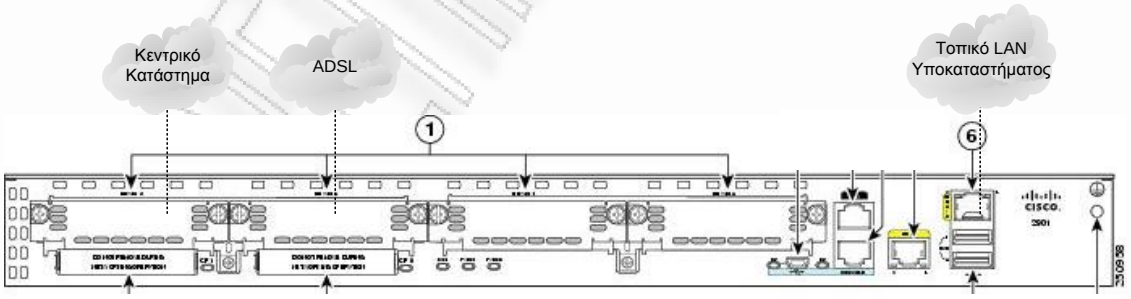
Συνοπτικά ο Router θα διαθέτει:

1 x 1 HWIC-4T για τη διασύνδεση με το κεντρικό κατάστημα μέσω μισθωμένης γραμμής.

1 x HWIC-1ADSL για την backup διασύνδεση με το κεντρικό κατάστημα.

Η μορφή που θα έχει ο Router είναι η εξής:

Εικόνα 4-15: Προτεινόμενη Διάρθρωση Δρομολογητή Υποκαταστήματος



Θέση 1: WIC slots - Αριστερά: 1 x HWIC-1T για διασύνδεση με κεντρικό κατάστημα
Δεξιά: HWIC-1ADSL για σύνδεση backup προς κεντρικό καταστήματα
Θέση 6: Ethernet port – Gigabit διασύνδεση με τοπικό δίκτυο

4.4.3 Σύστημα Διασύνδεσης Τοπικών Χρηστών Υποκαταστήματος

Ο μεταγωγέας (switch) που θα χρησιμοποιηθεί για τη διασύνδεση των συστημάτων και των χρηστών στο τοπικό δίκτυο ενός υποκαταστήματος, θα είναι ίδιος με αυτόν του κεντρικού. Με τη διαφορά ότι σε υποκαταστήματα με μικρό αριθμό υπαλλήλων άρα μικρή ανάγκη σε ports μπορεί για λόγους οικονομίας να μη χρησιμοποιηθεί ο 2960-48, αλλά ο 2960-24 ή ακόμα και ο 2960-12 με 24 και 12 πόρτες αντίστοιχα.

4.5 Παραμετροποίηση Συσκευών

4.5.1 Βέλτιστη Διαχείριση Δικτύου μέσω VLANs

Τα Virtual LANs (VLANs) αποτελούν μία ριζική αλλαγή στον τρόπο με τον οποίο σχεδιάζονται και διαχειρίζονται τα παραδοσιακά LAN καθώς δίνουν λύση σε προβλήματα που σχετίζονται με μετακινήσεις, προσθέσεις και αλλαγές χρηστών στο δίκτυο, συμβάλλουν στη διαχείριση, την ασφάλεια, τον έλεγχο, και την καλύτερη κατανομή των πόρων του δικτύου.

Η τεχνολογία VLAN επιτρέπει στους διαχειριστές των δικτύων να ομαδοποιήσουν κάποιες θύρες ενός switch και τους χρήστες που είναι συνδεδεμένοι σε αυτές, σε λογικά οργανωμένες ομάδες. Ο διαχωρισμός μπορεί να γίνει με βάση το αν π.χ. οι χρήστες αυτοί χρησιμοποιούν τα ίδια προγράμματα ή τις ίδιες εφαρμογές. Οι διασυνδεδεμένοι χρήστες μπορεί να ανήκουν στο ίδιο switch ή σε διαφορετικά switch. Με τον τρόπο αυτό τα VLANs μπορούν να ορισθούν μέσα στο ίδιο κτίριο, να συνδέουν διαφορετικά κτίρια ή ακόμη και WANs μεταξύ τους. Για παράδειγμα, μπορεί οι υπάλληλοι του τμήματος πιστωτικών καρτών να βρίσκονται σε διαφορετικά κτίρια και ταυτόχρονα όλοι μαζί να ανήκουν στο ίδιο VLAN και να μοιράζονται τον ίδιο server όπου βρίσκεται μια data-base ή μια εφαρμογή ή κάποιες άλλες ομάδες που σχεδιάζουν τραπεζικά προϊόντα να μοιράζονται έναν server που τρέχει κάποια εφαρμογή CRM.

Έτσι για να συνδεθεί κάποιος χρήστης στον server δεν είναι απαραίτητο να υπάρχει φυσική σύνδεση στο ίδιο switch που συνδέεται ο server παρά σε οποιοδήποτε switch όπου ανήκει στο ίδιο VLAN με τον εξυπηρετητή. Με αυτόν τον τρόπο γίνεται προφανής η απαλοιφή του κόστους για νέα καλωδίωση και η ευχέρεια στη μετακίνηση των χρηστών.

4.5.2 Ασφάλεια μέσω VLANs

Ένα από τα σημαντικά χαρακτηριστικά των VLANs είναι ότι παρέχουν αυξημένη ασφάλεια. Οι χρήστες είναι χωρισμένοι σε ομάδες, οι οποίες ανήκουν σε διαφορετικά VLANs και έτσι δεν μπορούν να έχουν πρόσβαση σε άλλες ομάδες χρηστών, δεδομένου ότι το κάθε VLAN αποτελεί μία κλειστή, λογικά προσδιορισμένη ομάδα. Επίσης, δεδομένου ότι τα VLANs είναι λογικές μονάδες που συμπεριφέρονται ως φυσικά απομονωμένες οντότητες, η επικοινωνία μεταξύ τους γίνεται μέσω δρομολογητών (routers). Έτσι, όλος ο έλεγχος και το φιλτράρισμα της επικοινωνίας μεταξύ των διαφόρων VLANs μπορεί να γίνει χρησιμοποιώντας τις λειτουργίες που παρέχουν οι routers (access lists, filtering).

4.5.3 Κατανομή των Πόρων με Έλεγχο του Broadcast Traffic

Όπως η χρήση των Ethernet switches υλοποιεί την απομόνωση των συσκευών που είναι συνδεδεμένες στο δίκτυο σε διαφορετικά collision domains, επιτυγχάνοντας με αυτόν τον τρόπο την προώθηση σε μία πόρτα του δικτύου μόνο της απαραίτητης κίνησης, έτσι και με τον ορισμό των VLANs στο switch, παρέχεται επιπλέον διαχωρισμός των περιοχών αυτών στα διαφορετικά λογικά δίκτυα (Virtual LANs). Το κάθε VLAN είναι ένας ξεχωριστός διασυνδεδεμένος τομέας (bridging domain) και όλη η κίνηση broadcast/multicast περιέχεται μέσα σε αυτό. Εάν δεν γίνει σωστή διαχείριση της κίνησης broadcast τότε υπάρχει η πιθανότητα να έχουμε μείωση της απόδοσης του δικτύου.

Με τη χρήση των VLANs αυτό μπορεί να αποφευχθεί, διότι η κίνηση Broadcast του ενός VLAN δεν μεταδίδεται εκτός του VLAN αυτού. Κατ΄ αυτόν τον τρόπο έχουμε καλύτερη διαχείριση του bandwidth και αποφυγή προβλημάτων υπερφόρτισης του δικτύου από broadcast πληροφορία.

4.5.4 Αρχική Παραμετροποίηση Κεντρικού Δρομολογητή

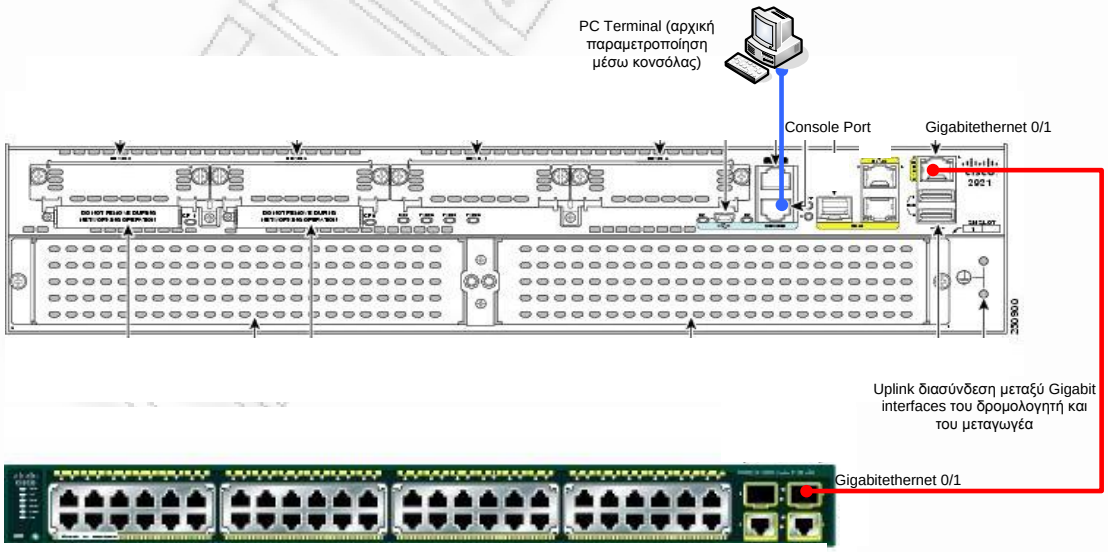
Το δίκτυό μας αποτελείται από δύο κύριες δικτυακές συσκευές. Τον μεταγωγέα (switch) Catalyst 2960-48 PST και το δρομολογητή (router) Cisco 2951. Η δημιουργία των VLANs θα ξεκινήσει από το δρομολογητή, ο οποίος θα είναι υπεύθυνος για τη δρομολόγηση της δικτυακής κίνησης μεταξύ διαφορετικών VLAN. Θα ορισθούν τα χαρακτηριστικά των VLANs όπως:

1. Ονομασία
2. Δίκτυο IP που θα χρησιμοποιηθεί
3. Διεύθυνση IP
4. Το είδος του trunking protocol που θα χρησιμοποιηθεί. Το trunking protocol είναι υπεύθυνο για τη σωστή δρομολόγηση των πακέτων μεταξύ δυο διαφορετικών VLANs

Πριν ξεκινήσουμε με την παραμετροποίηση των VLANs, θα παραμετροποιήσουμε κάποια βασικά στοιχεία που έχουν να κάνουν με την ταυτότητα της συσκευής και τη θέση της στο δίκτυο. Αφού συνδεθούμε με καλώδιο κονσόλας στον δρομολογητή (βλ Εικονα), μέσω της εφαρμογής HyperTerminal των Windows, δίνουμε τις πρώτες εντολές (μετά τη σύνδεση, τον διαχειριστή τον υποδέχεται το μήνυμα ***Router>***) :

Βήμα	Εντολή	Επεξήγηση
1	`Router> enable` `Router# configure terminal`	Είσοδος σε configuration mode (κατάσταση παραμετροποίησης)
2	`Router(config)# hostname Kentriko`	Καθορισμός ονόματος συσκευής
3	`Kentriko(config)# enable secret p@ssw0rd`	Καθορισμός κωδικού ασφαλείας για είσοδο σε configuration mode
4	`Kentriko(config)# no ip domain-lookup`	Απενεργοποίηση ελέγχου μετάφρασης άγνωστων εντολών (τυπογραφικά λάθη) σε IP διευθύνσεις

Εικόνα 4-16: Διασύνδεση Δρομολογητή - Μεταγωγέα



4.5.5 Παραμετροποίησης της IP Διεύθυνσης Δρομολογητή

Βήμα	Εντολή	Επεξήγηση
1	`Kentriko(config)# interface gigabitethernet 0/1`	Είσοδος για παραμετροποίηση του gigabit interface
2	`Kentriko(config-if)# ip address 192.168.1.1 255.255.255.0`	Δήλωση IP διεύθυνσης δρομολογητή η οποία θα χρησιμοποιηθεί σαν διαχειριστική διεύθυνση του δρομολογητή και σαν πύλη εξόδου του κεντρικού δικτύου προς το WAN
3	`Kentriko(config-if)# no shutdown`	Ενεργοποίηση του interface
4	`Kentriko(config-if)# exit`	Έξοδος από την παραμετροποίηση του interface

4.5.6 Ενεργοποίηση Απομακρυσμένης Πρόσβασης στο Δρομολογητή Μέσω Telnet

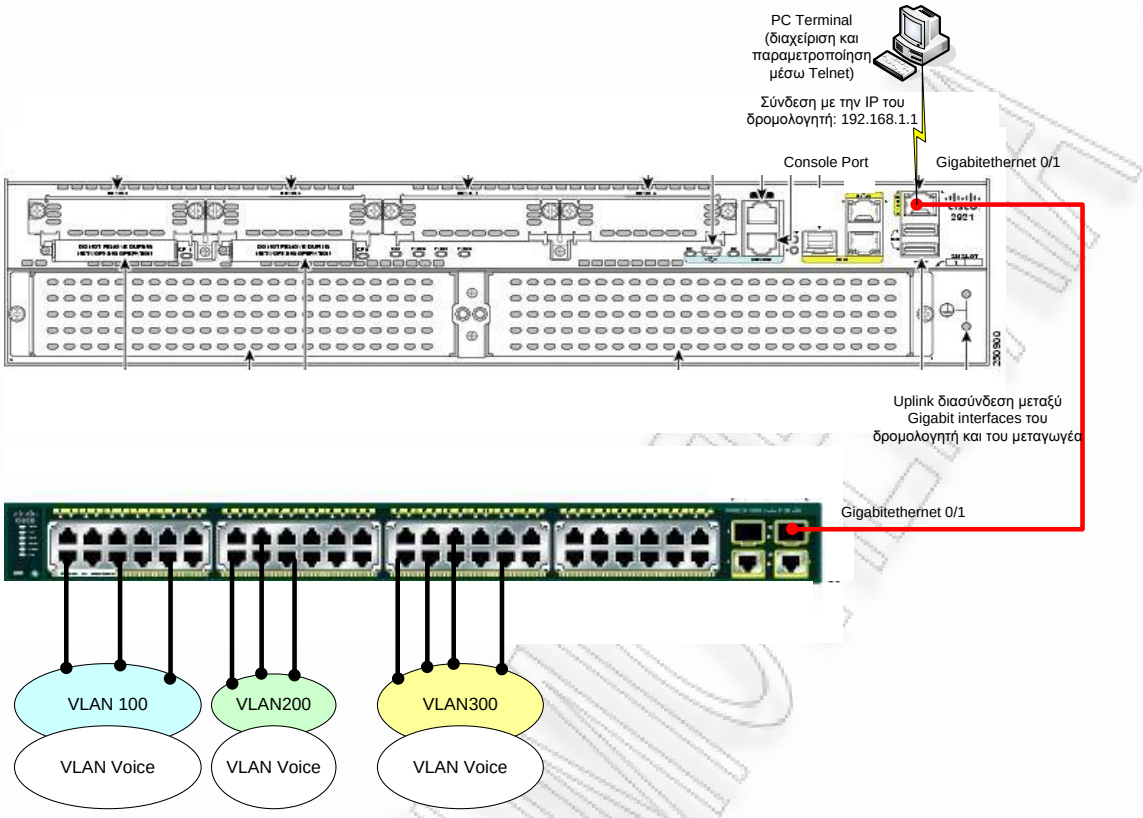
Βήμα	Εντολή	Επεξήγηση
1	`Kentriko(config)# password p@ssw0rd`	Ορισμός κωδικού πρόσβασης
2	`Kentriko(config-line)# login`	Ενεργοποίηση ελέγχου κωδικού κατά την πρόσβαση
3	`Kentriko(config-line)# line vty 0 4`	Καθορισμός και ενεργοποίηση απομακρυσμένης πρόσβασης
4	`Kentriko(config-line)# password pass`	Ορισμός κωδικού πρόσβασης μόνο για telnet
5	`Kentriko(config-line)# login`	Ενεργοποίηση ελέγχου κωδικού κατά την πρόσβαση με telnet
6	`Kentriko(config-line)# end`	Έξοδος από την παραμετροποίηση γραμμών πρόσβασης

4.5.7 Καθορισμός Παραμέτρων στον Κεντρικό Δρομολογητή

Τα VLANs που θα δημιουργηθούν θα είναι δύο (2) τύπων, data και voice. Η Cisco διαχωρίζει, όπως έχουμε προαναφέρει, τη δικτυακή κίνηση σε data traffic και σε real-time traffic που περιλαμβάνει τη μετάδοση της φωνης (VoIP). Με αυτό τον τρόπο η φωνή χρησιμοποιεί αποκλειστικό κανάλι για τη διαχείριση και τη μετάδοση, απομονωμένο από όλη την κίνηση data και σε απόλυτη προτεραιότητα από οποιαδήποτε άλλη μορφή μετάδοσης. Γι' αυτό το λόγο τα VLANs κατά τη Cisco διαχωρίζονται σε DATA και VOICE VLANs, παρέχοντας παράλληλα τη δυνατότητα ορισμού και των 2 τύπων VLANs σε καθένα από τα interfaces του μεταγωγέα όπως φαίνεται από το προηγούμενο σχήμα.

Η παραμετροποίηση περιλαμβάνει τη δημιουργία sub-interfaces στο κεντρικό interface διασύνδεσης με το δίκτυο (gigabitethernet 0/1) και, ο ορισμός του πρωτόκολλου υπεύθυνου για τη διαχείριση και μετάδοση της δικτυακής κίνησης ανάμεσα στα διαφορετικά VLANs (επικοινωνία μεταξύ voice και data vlans απαγορεύεται εξ' ορισμού). Το πρωτόκολλο αυτό ονομάζεται trunking protocol και η Cisco υποστηρίζει τα εξής, 802.1q (γενική υλοποίηση) και ISL (υλοποιείται μόνο από τη Cisco). Στο δίκτυό μας θα χρησιμοποιήσουμε το ISL. Η δημιουργία sub-interfaces στον κεντρικό δρομολογητή είναι ο μόνος τρόπος ώστε να επιτευχθεί δρομολόγηση μεταξύ διαφορετικών VLANs (intervlan routing), δρομολόγηση δηλαδή σε επίπεδο Layer 3. Οι μεταγωγείς ως γνωστών είναι Layer 2 συσκευές και δεν έχουν δυνατότητα routing. Κατά αυτόν τον τρόπο ο μεταγωγέας (layer2) χρησιμοποιεί, αναγκαστικά, έναν εξωτερικό δρομολογητή για την δρομολόγηση των πακέτων μεταξύ θυρών του ίδιου μεταγωγέα που ανήκουν σε διαφορετικά VLAN.

Εικόνα 4-17: Διασύνδεση Δρομολογητή – Μεταγωγέα και Απεικόνιση VLANs



4.5.8 Παραμετροποίηση Sub-Interfaces και VLANs στον Κεντρικό Δρομολογητή

Βήμα	Εντολή	Επεξήγηση
1	`Kentriko (config)# interface gigabitethernet 0/1.1`	Είσοδος για παραμετροποίηση gigabit interface και ενεργοποίηση sub-interface (1.1).
2	`Kentriko (config-subif)# encapsulation ISL 1`	Ενεργοποίηση πρωτοκόλλου για το default vlan 1 το οποίο είναι το διαχειριστικό VLAN και είναι απαραίτητο σε όλες τις υλοποιήσεις. Μόνο management πληροφορία μεταφέρεται στο VLAN 1.
3	`Kentriko (config-subif)# ip address 192.168.1.1 255.255.255.0`	Δήλωση IP διεύθυνσης για το VLAN 1 η οποία είναι ίδια με τη management
4	`Kentriko(config)# interface gigabitethernet 0/1.2`	Είσοδος για ενεργοποίηση sub-interface (1.2)
5	`Kentriko (config-subif)# encapsulation ISL 100`	Ενεργοποίηση πρωτοκόλλου για το πρώτο data VLAN
6	`Kentriko (config-subif)#ip address 192.168.10.1 255.255.255.0`	Δήλωση IP διεύθυνσης για το data VLAN 100
7	`Kentriko(config)# interface gigabitethernet 0/1.3`	Είσοδος για ενεργοποίηση sub-interface (1.3)

Βήμα	Εντολή	Επεξήγηση
8	`Kentriko (config-subif)# encapsulation ISL 200`	Ενεργοποίηση πρωτοκόλλου για το δεύτερο data VLAN
9	`Kentriko (config-subif)#ip address 192.168.20.1 255.255.255.0`	Δήλωση IP διεύθυνσης για το data VLAN 200
10	`Kentriko(config)# interface gigabitethernet 0/1.4`	Είσοδος για ενεργοποίηση sub-interface (1.4)
11	`Kentriko (config-subif)# encapsulation ISL 300`	Ενεργοποίηση πρωτοκόλλου για το τρίτο data VLAN
12	`Kentriko (config-subif)#ip address 192.168.30.1 255.255.255.0`	Δήλωση IP διεύθυνσης για το data VLAN 300
13	`Kentriko(config)# interface gigabitethernet 0/1.5`	Είσοδος για ενεργοποίηση sub-interface (1.5)
14	`Kentriko (config-subif)# encapsulation ISL 400`	Ενεργοποίηση πρωτοκόλλου για το voice VLAN
15	`Kentriko (config-subif)#ip address 10.90.100.1 255.255.255.0`	Δήλωση IP διεύθυνσης για το voice VLAN 400

Οι IP διευθύνσεις που έχουν δηλωθεί στα sub-interfaces θα χρησιμοποιηθούν ως προεπιλεγμένες πύλες (default gateway) για τα υπόλοιπα στοιχεία του δικτύου που ανήκουν σε κάποιο από τα δηλωμένα VLAN (π.χ. συσκευή στο VLAN 200 θα χρησιμοποιεί ως default gateway την ip 192.168.20.1).

4.5.9 Αρχική Παραμετροποίηση Μεταγωγέα

Όπως και με το δρομολογητή, θα ξεκινήσουμε από κάποια βασικά στοιχεία που έχουν να κάνουν με την ταυτότητα της συσκευής και τη θέση της στο δίκτυο. Αφού συνδεθούμε με καλώδιο κονσόλας στο μεταγωγέα μέσω της εφαρμογής HyperTerminal των Windows, δίνουμε τις πρώτες εντολές (μετά τη σύνδεση, τον διαχειριστή τον υποδέχεται το μήνυμα ***Switch>***):

Βήμα	Εντολή	Επεξήγηση
1	`Switch> enable` `Switch# configure terminal`	Είσοδος σε configuration mode (κατάσταση παραμετροποίησης)
2	`Switch(config)# hostname Kentrikosw` `Kentrikosw(config)#`	Καθορισμός ονόματος συσκευής
3	`Kentrikosw(config)# enable secret p@ssw0rd`	Καθορισμός κωδικού ασφαλείας για είσοδο σε configuration mode

4.5.10 Παραμετροποίησης της IP Διεύθυνσης Μεταγωγέα

Βήμα	Εντολή	Επεξήγηση
1	`Kentrikosw(config)# interface vlan1` `Kentrikosw(config-if)#`	Είσοδος για παραμετροποίηση του Vlan 1. Το switch πρέπει να ανήκει στο ίδιο management VLAN με το δρομολογητή
2	`Kentrikosw(config-if)# ip address 192.168.1.2 255.255.255.0`	Δήλωση IP διεύθυνσης, η οποία θα χρησιμοποιηθεί σαν διαχειριστική διεύθυνση του μεταγωγέα
3	`Kentrikosw(config-if)# no shutdown`	Ενεργοποίηση του interface

4.5.11 Ενεργοποίηση Απομακρυσμένης Πρόσβασης στον Μεταγωγέα μέσω Telnet

Βήμα	Εντολή	Επεξήγηση
1	`Kentrikosw(config)# password p@ssw0rd` `Kentrikosw(config-line)#`	Ορισμός κωδικού πρόσβασης
2	`Kentrikosw(config-line)# login`	Ενεργοποίηση ελέγχου κωδικού κατά την πρόσβαση
3	`Kentrikosw(config-line)# line vty 0 4`	Καθορισμός και ενεργοποίηση απομακρυσμένης πρόσβασης
4	`Kentrikosw(config-line)# password pass`	Ορισμός κωδικού πρόσβασης μόνο για telnet
5	`Kentrikosw(config-line)# login`	Ενεργοποίηση ελέγχου κωδικού κατά την πρόσβαση με telnet

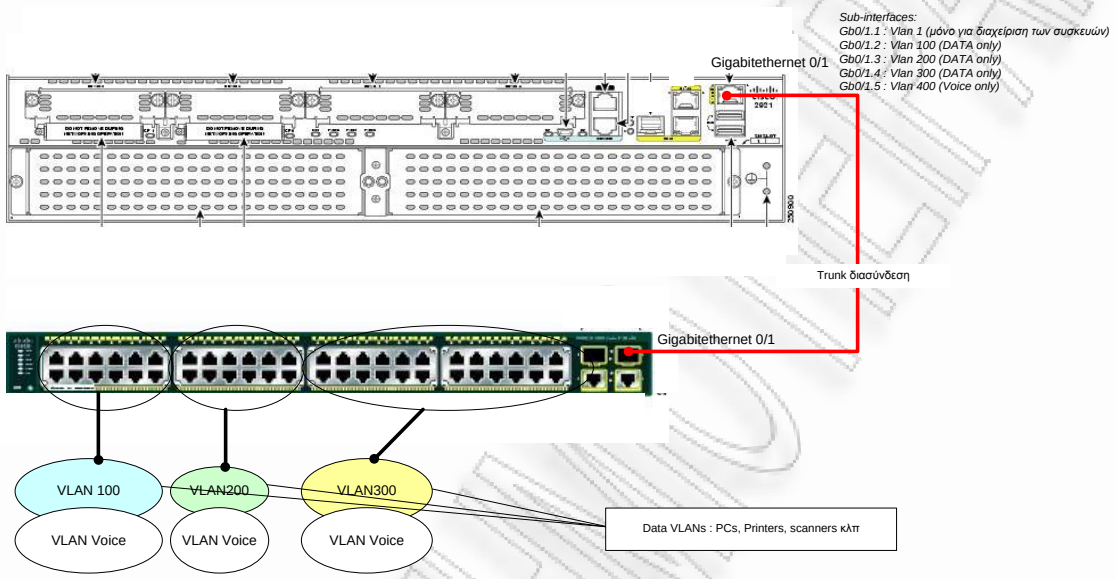
4.5.12 Παραμετροποίηση VLANs στον Μεταγωγέα

Βήμα	Εντολή	Επεξήγηση
1	`Kentrikosw (config)#ip default gateway 192.168.1.1`	Δήλωση προεπιλεγμένης πύλης (ο δρομολογητής)
2	`Kentrikosw (config)#exit`	Έξοδος από το configuration του interface
3	`Kentrikosw# vlan database`	Είσοδος στο μηχανισμό δημιουργίας και διαχείρισης των VLANs
4	`Kentrikosw(vlan)# vtp server`	Ενεργοποίηση VTP προτοκόλλου (υπεύθυνο διαχείρισης των VLANs)
5	`Kentrikosw(vlan)#vlan 100` *VLAN 100 added:* *Name: VLAN0100*	Πρόσθεση νέου data vlan με ονομασία 100, ίδιο με το όνομα που έχει δηλωθεί στο δρομολογητή. Για την intervlan κίνηση υπεύθυνο θα είναι το interface gb0/1.2 του δρομολογητή
6	`Kentrikosw(vlan)#vlan 200` *VLAN 200 added:* *Name: VLAN0200*	Πρόσθεση νέου data vlan με ονομασία 200, ίδιο με το όνομα που έχει δηλωθεί στο δρομολογητή. Για την intervlan κίνηση υπεύθυνο θα είναι το interface gb0/1.3 του δρομολογητή
7	`Kentrikosw(vlan)#vlan 300` *VLAN 300 added:* *Name: VLAN0300*	Πρόσθεση νέου data vlan με ονομασία 300, ίδιο με το όνομα που έχει δηλωθεί στο δρομολογητή. Για την intervlan κίνηση υπεύθυνο θα είναι το interface gb0/1.4 του δρομολογητή
8	`Kentrikosw(vlan)#vlan 400` *VLAN 400 added:* *Name: VLAN0400*	Πρόσθεση του voice vlan με ονομασία 400, ίδιο με το όνομα που έχει δηλωθεί στο δρομολογητή. Για την intervlan κίνηση υπεύθυνο θα είναι το interface gb0/1.5 του δρομολογητή
9	`Kentrikosw(vlan)#exit` *APPLY completed.* *Exiting....*	Έξοδος από το σύστημα διαχείρισης VLANs

4.5.13 Ενεργοποίηση Trunk Διασύνδεσης Μεταγωγέα με Δρομολογητή

Όλη η πληροφορία αναφορικά με τη διαχείριση μεταξύ των διαφορετικών VLANs και η αντίστοιχη δικτυακή κίνηση διοχετεύεται μέσω των trunk θυρών. Στην περίπτωσή μας ο μόνος τρόπος έτσι ώστε να μεταφέρεται η δικτυακή κίνηση από το ένα VLAN στο άλλο, είναι μέσω της trunk θύρας, της σύνδεσης δηλαδή μεταξύ μεταγωγέα και δρομολογητή.

Εικόνα 4-18: Ενεργοποίηση Trunk Διασύνδεσης Μεταξύ Μεταγωγέα και Δρομολογητή



Ως trunk πόρτα στο δρομολογητή έχουμε θέσει την Gigabitethernet0/1 και έχουμε δηλώσει και τα απαραίτητα sub-interfaces που θα ορισθούν για την intervlan δρομολόγηση. Έτσι λοιπόν στο μεταγωγέα θα έχουμε:

Βήμα	Εντολή	Επεξήγηση
1	`Kentrikosw(config)#interface gigabitethernet 0/1`	Είσοδος στο interface για παραμετροποίηση
2	`Kentrikosw(config-if)# switchport mode trunk`	Δήλωση ότι η συγκεκριμένα θύρα θα λειτουργεί ως trunk
3	`Kentrikosw(config-if)# switchport trunk encapsulation isl`	Υπεύθυνο πρωτόκολλο θα είναι το ISL
4	`Kentrikosw(config-if)# switchport trunk allowed vlan all`	Όλα τα VLANs έχουν πρόσβαση στην trunk διασύνδεση

4.5.14 Προγραμματισμός Θυρών Πρόσβασης Μεταγωγέα και Ένταξη σε VLAN

Κάθε θύρα εισόδου θα προγραμματισθεί έτσι ώστε να ανήκει σε κάποιο απο τα δηλωμένα DATA Vlans (100,200 ή 300) **και** ταυτόχρονα στο VOICE Vlan (400). Τα IP Phones έχουν εσωτερικό Ethernet switch, που επιτρέπει τη σύνδεση της τηλεφωνικής συσκευής και ενός υπολογιστή στην ίδια θύρα ενός μεταγωγέα.

Η δικτυακή κίνηση μεταξύ των διαφορετικών vlans επιτρέπεται εξ ορισμού. Υπάρχει όμως η δυνατότητα περιορισμού ή και απαγόρευση της κίνησης μεταξύ διαφορετικών VLANs με τη χρήση λιστών πρόσβασης (access-lists), τις οποίες θα δούμε παρακάτω. Έτσι στα τερματικά που είναι συνδεδεμένα στο vlan 100 μπορούμε να απαγορεύσουμε ή να περιορίσουμε την σύνδεση σε τερματικά ή υπηρεσίες, οι οποίες είναι συνδεδεμένες στο vlan 200.

Βήμα	Εντολή	Επεξήγηση
1	`Kentrikosw(config)#interface range fastethernet 0/1 – 12`	Παραμετροποίηση πολλαπλών interfaces
2	`Kentrikosw(config-if)# switchport access vlan 100`	Ένταξη των πρώτων 12 interfaces στο DATA vlan 100
3	`Kentrikosw(config-if)# switchport voice vlan 400`	Ένταξη των πρώτων 12 interfaces στο Voice vlan 400
4	`Kentrikosw(config)#interface range fastethernet 0/13 – 24`	Παραμετροποίηση πολλαπλών interfaces
5	`Kentrikosw(config-if)# switchport access vlan 200`	Ένταξη των επόμενων 12 interfaces στο DATA vlan 200
6	`Kentrikosw(config-if)# switchport voice vlan 400`	Ένταξη των επόμενων 12 interfaces στο Voice vlan 400
7	`Kentrikosw(config)#interface range fastethernet 0/25 – 48`	Παραμετροποίηση πολλαπλών interfaces
8	`Kentrikosw(config-if)# switchport access vlan 300`	Ένταξη των υπόλοιπων interfaces στο DATA vlan 300
9	`Kentrikosw(config-if)# switchport voice vlan 400`	Ένταξη υπόλοιπων interfaces στο Voice vlan 400

4.5.15 Ενεργοποίηση Αυτόματης Διευθυνσιοδότησης Συσκευών (DHCP)

Οι μεταγωγείς Catalyst 2960 προσφέρουν δυνατότητα απόδοσης IP διευθύνσεων και λοιπών στοιχείων IP παραμετροποίησης σε τερματικά και PCs μέσω της ενσωματωμένης λειτουργίας DHCP (Dynamic Host Configuration Protocol). Με αυτό τον τρόπο αποφεύγουμε τις χειροκίνητες διαδικασίες παραμετροποίησης ή την εγκατάσταση ξεχωριστού server που θα υλοποιεί αυτή τη διαδικασία

Βήμα	Εντολή	Επεξήγηση
1	`Kentrikosw(config)# ip dhcp pool VLAN100`	Δήλωση του πρώτο pool διευθύνσεων που θα αποδοθεί στα τερματικά που θα συνδεθούν στο VLAN 100
2	`Kentrikosw(config-dhcp)#network 192.168.10.0 255.255.255.0`	Το δίκτυο από το οποίο θα γίνει απόδοση IP διεύθυνσης προς το τερματικό
3	`Kentrikosw(config-dhcp)# default-router 192.168.10.1`	Ο default router που θα χρησιμοποιηθεί από το τερματικό δεν είναι άλλο από το gigabit interface 0/1.2 που έχει δηλωθεί στον δρομολογητή
4	`Kentrikosw(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.100`	Περιορισμός των προς απόδοση διευθύνσεων. Στα τερματικά θα δίνονται IPs πάνω από την 192.168.10.101
5	`Kentrikosw(config)# ip dhcp pool VLAN200`	Δήλωση του δεύτερου pool διευθύνσεων που θα αποδοθεί στα τερματικά που θα συνδεθούν στο VLAN 100
6	`Kentrikosw(config-dhcp)#network 192.168.20.0 255.255.255.0`	Το δίκτυο από το οποίο θα γίνει απόδοση IP διεύθυνσης προς το τερματικό
7	`Kentrikosw(config-dhcp)# default-router 192.168.20.1`	Ο default router που θα χρησιμοποιηθεί από το τερματικό δεν είναι άλλο από το gigabit interface 0/1.3 που έχει δηλωθεί στον δρομολογητή

Βήμα	Εντολή	Επεξήγηση
8	`Kentrikosw(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.100`	Περιορισμός των προς απόδοση διευθύνσεων. Στα τερματικά θα δίνονται IPs πάνω από την 192.168.20.101
9	`Kentrikosw(config)# ip dhcp pool VLAN300`	Δήλωση του τρίτου pool διευθύνσεων που θα αποδοθεί στα τερματικά που θα συνδεθούν στο VLAN 100
10	`Kentrikosw(config-dhcp)#network 192.168.30.0 255.255.255.0`	Το δίκτυο από το οποίο θα γίνει απόδοση IP διεύθυνσης προς το τερματικό
11	`Kentrikosw(config-dhcp)# default-router 192.168.30.1`	Ο default router που θα χρησιμοποιηθεί από το τερματικό δεν είναι άλλο από το gigabit interface 0/1.4 που έχει δηλωθεί στον δρομολογητή
12	`Kentrikosw(config)# ip dhcp excluded-address 192.168.30.1 192.168.30.100`	Περιορισμός των προς απόδοση διευθύνσεων. Στα τερματικά θα δίνονται IPs πάνω από την 192.168.30.101
13	`Kentrikosw(config)# ip dhcp pool VLAN400`	Δήλωση του pool διευθύνσεων που θα αποδοθεί στα IP phone που θα συνδεθούν στο VLAN 400
14	`Kentrikosw(config-dhcp)#network 10.90.100.0 255.255.255.0`	Το δίκτυο από το οποίο θα γίνει απόδοση IP διεύθυνσης προς το IP phone
15	`Kentrikosw(config-dhcp)# default-router 10.90.100.1`	Ο default router που θα χρησιμοποιηθεί από το IP phone που δεν είναι άλλο από το gigabit interface 0/1.5που έχει δηλωθεί στον δρομολογητή
16	`Kentrikosw(config)# ip dhcp excluded-address 10.90.100.1 10.90.100.100`	Περιορισμός των προς απόδοση διευθύνσεων. Στα IP phone θα δίνονται IPs πάνω από την 10.90.100.101

4.5.16 Ενεργοποίηση Auto-QoS

Με το QoS παρέχεται προνομιακή διαχείριση προς συγκεκριμένους τύπους δικτυακής κίνησης εις βάρος κάποιον άλλων. Στην περίπτωσή μας η κίνηση VoIP πρέπει πάντα να έχει την απόλυτη προτεραιότητα στην αναμετάδοση. Χωρίς την ενεργοποίηση του QoS στον μεταγωγέα, η συσκευή καταβάλει την καλύτερη δυνατή προσπάθεια να εξυπηρετήσει κάθε εισερχόμενο πακέτο (FIFO), ανεξαρτήτως από το περιεχόμενο, το μέγεθος, τον τύπο ή τον «χαρακτηρισμό» ο οποίος έχει αποτυπωθεί στο πακέτο σε κάποια προηγούμενη δικτυακή συσκευή (συνήθως στην αφετηρία) κατά τη διαδρομή του. Η Cisco στην υλοποίησή της για QoS, στις δικτυακές της συσκευές, έχει εισάγει την τεχνολογία AutoQoS, η οποία έχει απλουστεύσει την ανάπτυξη και την ενεργοποίηση QoS υπηρεσιών. Το AutoQoS κάνει υποθέσεις σχετικά με την τοπολογία και το είδος των συσκευών και υπηρεσιών που συμμετέχουν σε αυτό και αυτόματα αναγνωρίζει και κατηγοριοποιεί τις διαφορετικές ροές κίνησης και ανάλογα χρησιμοποιεί τις εισερχόμενες και εξερχόμενες ουρές. Εξ ορισμού το QoS είναι απενεργοποιημένο στις συσκευές Cisco.

Όταν ενεργοποιούμε το QoS, αυτό αυτόματα κατηγοριοποιεί την κίνηση βασιζόμενο στον τύπο της κίνησης και την επικεφαλίδα των εισερχόμενων πακέτων. Ο μεταγωγέας χρησιμοποιεί το αποτέλεσμα της κατηγοριοποίησης για να επιλέξει και να τοποθετήσει το πακέτο στην ανάλογη εξερχόμενη ουρά.

Χρησιμοποιούμε τις εντολές του AutoQoS για να δηλώσουμε σε ποιες πόρτες έχουμε συνδεδεμένα IP τηλέφωνα ή για να δηλώσουμε θύρες, οι οποίες δέχονται έγκυρη κίνηση (μέσω κάποιου uplink).

Οι ενέργειες του AutoQoS κατά την πρώτη ενεργοποίηση είναι:

1. Αναζήτηση για την παρουσία ή όχι IP Cisco τηλεφώνων
2. Παραμετροποίηση της κατηγοριοποίησης του QoS
3. Παραμετροποίηση εξερχόμενων ουρών

Στην περίπτωσή μας υποθέτουμε ότι σε όλες τις θύρες πρόσβασης του κεντρικού μεταγωγέα θα συνδεθούν IP τηλέφωνα (μέσω του ενσωματωμένου switch θα συνδέονται και τερματικά των χρηστών) και η uplink σύνδεση με το δρομολογητή είναι μια έγκυρη πηγή εισερχόμενης κίνησης.

Βήμα	Εντολή	Επεξήγηση
1	`Kentrikosw(config)# interface range fastethernet 0/1 48`	Είσοδος για μαζική παραμετροποίηση όλων των θυρών πρόσβασης
2	`Kentrikosw(config-if)# auto qos voip cisco-phone`	Ενεργοποίηση auto QoS σε όλες τις θύρες πρόσβασης. Δήλωση ότι θα συνδεθούν Cisco IP τηλέφωνα.
3	`Kentrikosw(config)# interface gigabitethernet 0/1`	Παραμετροποίηση της Uplink interface σύνδεσης με το δρομολογητή Cisco 2951
4	`Kentrikosw(config-if)# auto qos voip trust`	Ενεργοποίηση auto QoS στην uplink θύρα διασύνδεσης με το δρομολογητή Δήλωση ότι Cisco δρομολογητής είναι συνδεδεμένος σε αυτή και πρέπει ο μηχανισμός QoS να εμπιστεύεται το «μαρκάρισμα» των εισερχομένων.

4.5.17 Περιορισμός Πρόσβασης Μεταξύ Διαφορετικών VLANs με Λίστες Πρόσβασης

Η δυνατότητα περιορισμού ή/και απαγόρευσης της επικοινωνίας μεταξύ χρηστών από διαφορετικά VLANs επιτυγχάνεται με την χρήση λιστών ελέγχου πρόσβασης. Οι access-list δίνουν τη δυνατότητα στον διαχειριστή να περιορίσει τη πρόσβαση χρηστών σε υπηρεσίες ή σε συστήματα τα οποία βρίσκονται σε διαφορετικά VLANs. Ο προγραμματισμός και ένταξη των λιστών πρόσβασης γίνεται μόνο στο δρομολογητή, ο οποίος είναι υπεύθυνος για τη δρομολόγηση των διαφορετικών VLANs.

Υπάρχουν δυο γενικοί τύποι λιστών πρόσβασης:

1. **Τυπικές λίστες πρόσβασης** (standard access lists): οι οποίες ελέγχουν τη διεύθυνση προέλευσης των πακέτων που μπορούν να δρομολογηθούν. Το αποτέλεσμα του ελέγχου καθορίζει αν θα επιτραπεί ή όχι η έξοδος των πακέτων για ολόκληρη την γκάμα πρωτοκόλλων, με βάση την IP διεύθυνση προέλευσης του δικτύου, του υποδικτύου ή του υπολογιστή.
2. **Εκτεταμένες λίστες πρόσβασης** (extended access lists): οι οποίες ελέγχουν τη διεύθυνση προέλευσης αλλά και προορισμού των πακέτων. Επιπλέον μπορούν να πραγματοποιούν έλεγχο για συγκεκριμένα πρωτόκολλα, αριθμούς θυρών και άλλες παραμέτρους, κάτι που προσφέρει στους διαχειριστές μεγαλύτερη ευελιξία.

Οι λίστες πρόσβασης μπορούν να χρησιμοποιηθούν με τους εξής δυο τρόπους:

1. **Λίστες πρόσβασης εισόδου** (inbound access lists): τα εισερχόμενα πακέτα υποβάλλονται σε επεξεργασία πριν δρομολογηθούν σε μια διασύνδεση εξόδου. Σε περίπτωση όπου το πακέτο πρόκειται να απορριφτεί από τους ελέγχους φιλτραρίσματος, μια λίστα πρόσβασης εισόδου δεν προκαλεί επιβάρυνση λόγο

αναζητήσεων στον πίνακα δρομολόγησης. Ως εκ τούτου θεωρείται περισσότερο αποδοτική σε σχέση με μια λίστα πρόσβασης εξόδου.

2. **Λίστες πρόσβασης εξόδου** (outbound access lists): τα εισερχόμενα πακέτα δρομολογούνται στη διασύνδεση εξόδου και υποβάλλονται σε επεξεργασία μέσω της λίστας πρόσβασης εξόδου πριν από τη μεταδοσή τους.

Οι λίστες πρόσβασης εκφράζουν το σύνολο των κανόνων που επιτρέπουν περαιτέρω έλεγχο σε πακέτα τα οποία εισέρχονται σε διεπαφές εισόδου, αναμεταδίδονται μέσω του δρομολογητή και εξέρχονται από τις διεπαφές εξόδου του δρομολογητή. Αντίθετα σε πακέτα που προέρχονται από τον ίδιο το δρομολογητή, όπως π.χ. ενημερώσεις δρομολόγησης, οι λίστες πρόσβασης δεν έχουν καμία επίδραση. Συνεπώς οι λίστες πρόσβασης είναι οι εντολές που καθορίζουν τις συνθήκες για το πώς θα χειριστεί ο δρομολογητής τη ροή της κίνησης μέσω συγκεκριμένων διεπαφών (interface).

Στην πράξη, μια γενική προσέγγιση για διευθέτηση λιστών πρόσβασης χωρίζεται σε δυο τμήματα:

1. Η λίστα πρόσβασης περιέχει καθολικές προτάσεις που χρησιμοποιούνται στον προσδιορισμό πακέτων. Αυτές οι λίστες δημιουργούνται με την εντολή **access-list**.
2. Η εντολή διευθέτησης **ip access-group** ενεργοποιεί μια IP λίστα πρόσβασης (υπάρχουν και οι mac λίστες πρόσβασης, Layer-2) σε μια διεπαφή.

Η επόμενη σύνταξη παρουσιάζει τη γενική μορφή της εντολής **access-list**:

```
Router(config)# access-list αριθμός λίστας πρόσβασης {permit | deny}  {συνθήκες ελέγχου}
```

Όταν καθορίζεται ένας *αριθμός λίστας πρόσβασης* από 1 έως 99 ή από 1300 έως 1999, δίνεται η οδηγία στο δρομολογητή για δημιουργία τυπικής λίστας πρόσβασης. Όμοια, για αριθμούς από 100 έως 199 ή από 2000 έως 2699 δίνεται η οδηγία για δημιουργία εκτεταμένης λίστας πρόσβασης.

Ο όρος **permit** ή **deny** δείχνει τον τρόπο που το IOS θα χειριστεί τα πακέτα που ικανοποιούν τις *συνθήκες ελέγχου*. Η εντολή **permit** σημαίνει ότι στο πακέτο θα επιτραπεί να περάσει μέσα από τις διασυνδέσεις στις οποίες εφαρμόζεται η λίστα, ενώ η εντολή **deny** σημαίνει ότι ο δρομολογητής θα απορρίψει το πακέτο.

Οι *συνθήκες ελέγχου* μπορεί να περιέχουν στην απλούστερη περίπτωση π.χ. μόνο μια διεύθυνση προέλευσης αλλά και να επεκταθούν συμπεριλαμβάνοντας πολλές συνθήκες (εκτεταμένες λίστες).

Η επόμενη σύνταξη παρουσιάζει τη γενική μορφή της εντολής {*πρωτόκολλο*} **access-group**, με την οποία εφαρμόζεται μια λίστα πρόσβασης σε μια διεπαφή:

```
Router(config-if)# {πρωτόκολλο} access-group αριθμός λίστας πρόσβασης {in | out}
```

Με το **in | out** μπορεί να επιλεγεί αν η λίστα ελέγχου πρόσβασης θα εφαρμόζεται ως φίλτρο εισόδου ή φίλτρο εξόδου. Αν δεν καθοριστεί τίποτα από τα δυο, ως προεπιλογή είναι το out. Για παράδειγμα, η εφαρμογή της εντολής **ip access-group 1** ενεργοποιεί την IP λίστα πρόσβασης με αριθμό 1 ως φίλτρο εξόδου σε μια διεπαφή.

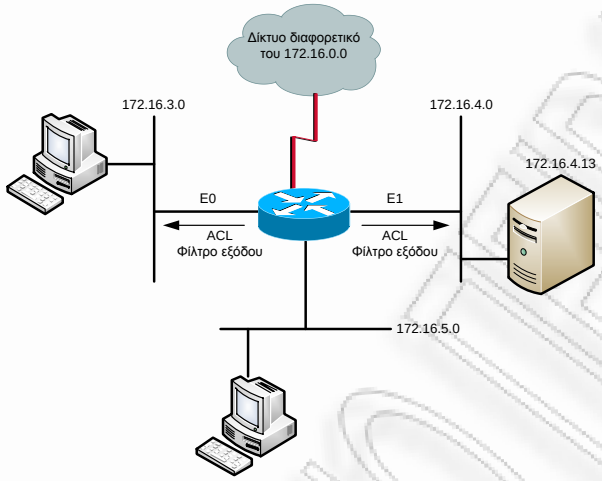
Συνολικά οι παραπάνω εντολές για διευθέτηση τυπικών λιστών πρόσβασης IP θα είναι:

```
Router(config)# access-list αριθμός λίστας πρόσβασης {permit | deny}
      ip διεύθυνση προέλευσης [μάσκα μπαλαντέρ]

Router(config)# interface serial 0

Router(config-if)# ip access-group αριθμός λίστας πρόσβασης {in | out}
```

Η *μάσκα μπαλαντέρ* ορίζει για ποια bit του πεδίου διεύθυνσης θα γίνεται έλεγχος ταύτισης. Η προεπιλεγμένη μάσκα είναι η 0.0.0.0 (ταύτιση σε όλα τα bit). Ένα bit μάσκας μπαλαντέρ με τιμή 0 ερμηνεύεται ως: «έλεγξε την αντίστοιχη τιμή bit», ενώ ένα bit μάσκας μπαλαντέρ με τιμή 1 ερμηνεύεται ως: «μην ελέγξεις την αντίστοιχη τιμή bit».

Παράδειγμα: Με βάση όσα είπαμε παραπάνω, ας υποθέσουμε πως θέλουμε να διευθετήσουμε μια λίστα πρόσβασης, η οποία θα μπλοκάρει όλη την κίνηση που δεν προέρχεται από το δίκτυο 172.16.0.0 (βλ. Εικόνα 4-19).

Εικόνα 4-19: Τυπική Λίστα που Μπλοκάρει την Κίνηση που είναι Διαφορετική του Δικτύου 172.16.0.0




```
Router(config)# access-list 1 permit 172.16.0.0 0.0.255.255
Router(config)# interface E0
Router(config-if)# ip access-group 1 out
Router(config)# interface E1
Router(config-if)# ip access-group 1 out
```

Όπου:

- ✓ Το 1 είναι ο αριθμός της λίστας πρόσβασης που δείχνει ότι πρόκειται για μια τυπική λίστα.
- ✓ Η παράμετρος **permit** δηλώνει ότι η κίνηση που ταυτίζεται με συγκεκριμένες παραμέτρους θα προωθηθεί.
- ✓ Η IP **172.16.0.0** είναι η διεύθυνση όπου μαζί με τη μάσκα **0.0.255.255** θα χρησιμοποιηθεί για τον προσδιορισμό του δικτύου προέλευσης.
- ✓ Η παράμετρος **ip access-group 1 out** συνδέει τη λίστα πρόσβασης στις διεπαφές E0 και E1 ως φίλτρο εξόδου.

Για διευθέτηση εκτεταμένης λίστας και εφαρμογής της σε μια διεπαφή απαιτείται η ακόλουθη σειρά εντολών:

```
Router(config)# access-list αριθμός λίστας πρόσβασης {permit | deny}
       πρωτόκολλο διεύθυνση-προέλευσης μπαλαντέρ-προέλευσης [θύρα τελεστή]
       διεύθυνση-προορισμού μπαλαντέρ-προορισμού [θύρα τελεστή]
       [established] [log]
Router(config)# interface serial 0
Router(config-if)# ip access-group αριθμός λίστας πρόσβασης {in | out}
```

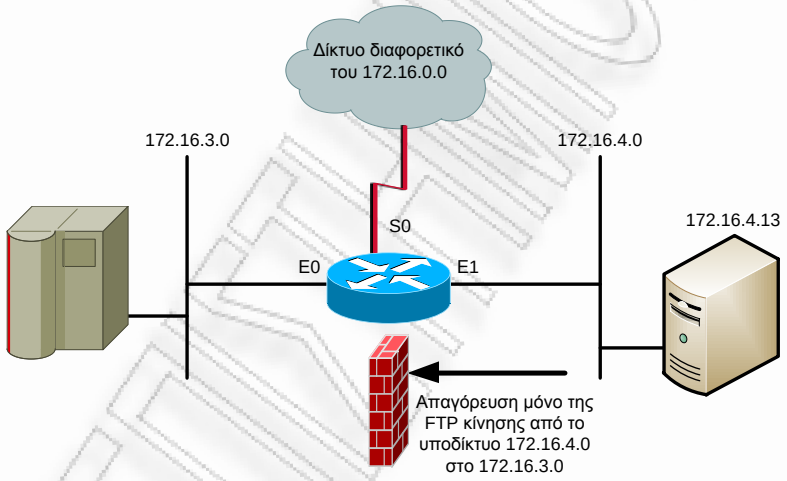
Όπου:

- ✓ Ο αριθμός λίστας πρόσβασης προσδιορίζει τη λίστα με έναν αριθμό από 100 έως 199 ή από 2000 έως 2699.

- ✓ Η παράμετρος **permit | deny** δείχνει αν αυτή η καταχώριση θα επιτρέπει ή θα μπλοκάρει την καθοριζόμενη κίνηση.
- ✓ Το *πρωτόκολλο* μπορεί να είναι IP,TCP,UDP,ICMP,GRE ή IGRP.
- ✓ Η *προέλευση* και ο *προορισμός* προσδιορίζουν IP διευθύνσεις προέλευσης και προορισμού.
- ✓ Ο *μπαλαντέρ-προέλευσης* και *μπαλαντέρ-προορισμού* προσδιορίζουν τη μάσκα μπαλαντέρ.
- ✓ Η επιλογή *θύρα τελεστή* αποτελείται από τη σύντμηση lt (less than - μικρότερο από), gt (greater than – μεγαλύτερο από), eq (equal to – ίσο με), ή neq (not equal to – διάφορο από) και έναν αριθμό θύρας πρωτοκόλλου.
- ✓ Η παράμετρος **established** χρησιμοποιείται μόνο για τα εισερχόμενα πακέτα TCP. Αυτό επιτρέπει τη διέλευση της TCP κίνησης αν το πακέτο χρησιμοποιεί μια λειτουργική σύνδεση (π.χ. αν είναι ενεργοποιημένα τα bit επιβεβαίωσης ACK).
- ✓ Με την παράμετρο **log** στέλνεται ένα μήνυμα ημερολογίου στην κονσόλα.

Παράδειγμα: Δημιουργία εκτεταμένης λίστας πρόσβασης που μπλοκάρει την FTP κίνηση από ένα συγκεκριμένο δίκτυο (βλ. Εικόνα 4-20).

Εικόνα 4-20: Εκτεταμένη Λίστα Πρόσβασης που Μπλοκάρει την FTP Κίνηση από Συγκεκριμένο Δίκτυο



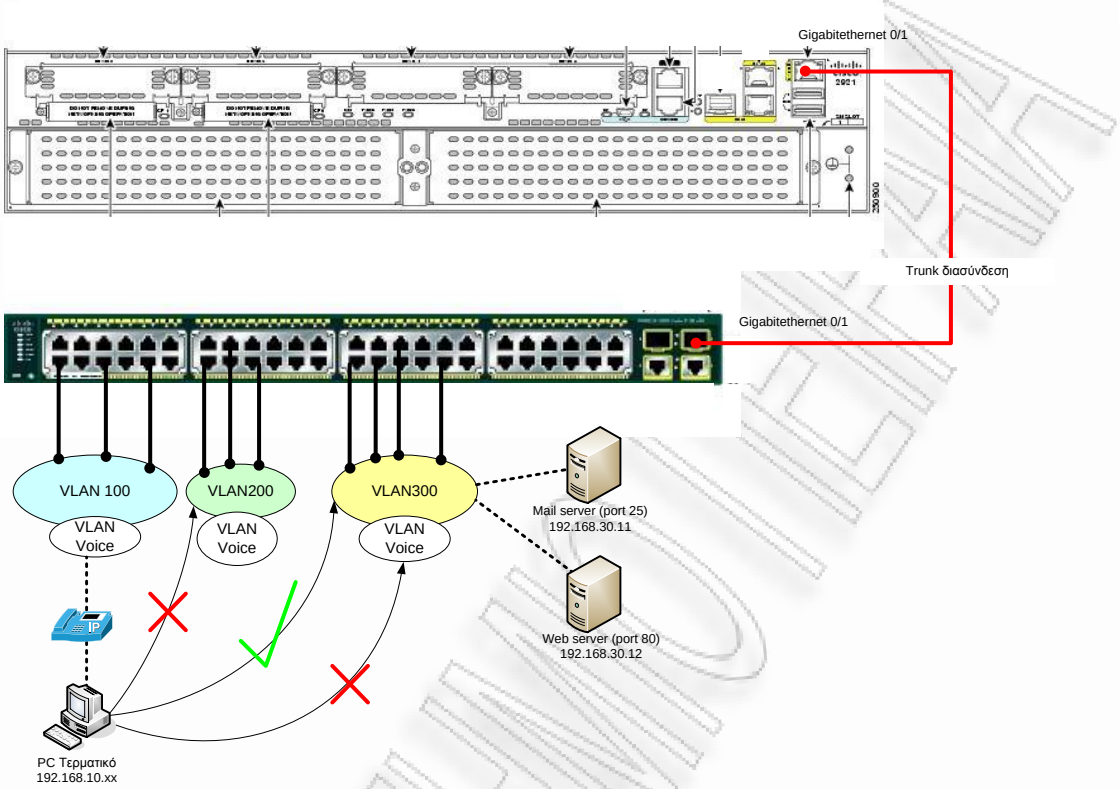

```
Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
Router(config)# access-list 101 permit ip any any
Router(config)# interface E1
Router(config-if)# ip access-group 101 in
```

Το **eq 21** και **eq 20** καθορίζουν αντίστοιχα τον αριθμό θύρας για το FTP και τον αριθμό θύρας για τα δεδομένα FTP.

Παράδειγμα: Θεωρούμε ένα υποθετικό σενάριο, όπου οι χρήστες του Vlan 100:

1. Απαγορεύεται να συνδεθούν στο VLAN 200.
2. Έχουν πρόσβαση μόνο στον mail server και στον web server (VLAN 300).
3. Απαγορεύεται η πρόσβαση σε συστήματα ip phones του VLAN 400.

Εικόνα 4-21: Περιορισμός Πρόσβασης Μεταξύ Διαφορετικών VLANs με Λίστες Πρόσβασης



Βήμα	Εντολή	Επεξήγηση
1	`Kentriko# configuration terminal`	Είσοδος σε configuration mode (κατάσταση παραμετροποίησης)
2	`Kentriko(conf)#ip access-list extended to-vlan100`	Δήλωση ονόματος (to-vlan100) πρώτης λίστας πρόσβασης. Ακολουθούν οι προτάσεις περιορισμού.
3	`Kentriko(conf ext-nacl)# deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255`	Απαγόρευση πρόσβασης όλων των στοιχείων από το δίκτυο vlan 100 στο δίκτυο vlan 200 για όλα τα πρωτόκολλα και τις υπηρεσίες
4	`Kentriko(conf ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 host 192.168.30.11 equal smtp`	Δυνατότητα πρόσβασης όλων των στοιχείων από το δίκτυο vlan 100 στο δίκτυο vlan 300 στον server 192.168.30.11 μόνο για υπηρεσίες email
5	`Kentriko(conf ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 host 192.168.30.12 equal 80`	Δυνατότητα πρόσβασης όλων των στοιχείων από το δίκτυο vlan 100 στο δίκτυο vlan 300 στον server 192.168.30.12 μόνο για υπηρεσίες web και http
6	`Kentriko(conf ext-nacl)# deny ip 192.168.10.0 0.0.0.255 10.90.100.0 0.0.0.255`	Απαγόρευση πρόσβασης όλων των στοιχείων από το δίκτυο vlan 100 στο δίκτυο vlan 400 (voice) για όλα τα πρωτόκολλα και τις υπηρεσίες
7	`Kentriko(conf)# interface gigabitinternet 0/1.2`	Είσοδος στο κατάλληλο interface για αντιστοίχηση της λίστας πρόσβασης
8	`Kentriko(conf-if)# ip access-group to-vlan100 out`	Αντιστοίχηση access-list με το interface

Στο προηγούμενο παράδειγμα διευθετήθηκε μια λίστα πρόσβασης όπου για τον προσδιορισμό της χρησιμοποιήθηκε αλφαριθμητικό στη θέση του αριθμού. Η Cisco μετά την έκδοση 11.2 του IOS εισήγαγε τη δυνατότητα προσδιορισμού τυπικών και εκτεταμένων λιστών πρόσβασης IP με χρήση ονόματος αντί αριθμητικής αναπαράστασης. Οι λίστες αυτές ονομάζονται «**Επώνυμες λίστες πρόσβασης IP**» και σε αντίθεση με τις αριθμητικές, επιτρέπουν την τροποποίηση μεμονωμένων καταχωρίσεων χωρίς να απαιτείται πρώτα η διαγράφη τους. Η τοποθέτηση των νέων στοιχείων πρέπει να γίνεται πάντα στο τέλος της λίστας. Στις αριθμητικές λίστες για να πραγματοποιηθεί μια τροποποίηση, ο διαχειριστής πρέπει πρώτα να διαγράψει ολόκληρη τη λίστα (χρησιμοποιώντας πριν από τη συνθήκη τη λέξη **no**) και έπειτα να τη διαμορφώσει από την αρχή.

Για διευθέτηση επώνυμης λίστας IP και εφαρμογής της σε μια διεπαφή απαιτείται η ακόλουθη σειρά εντολών:

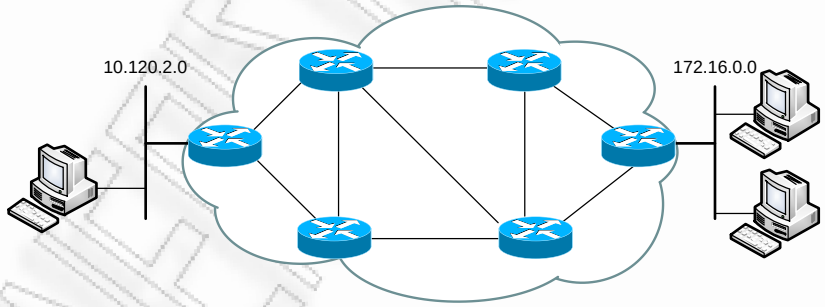
```
Router(config)# ip access-list {standard | extended} όνομα
Router(config {std- | ext-}nacl)# access-list {permit | deny} {συνθήκες ελέγχου}
Router(config)# interface όνομα διεπαφής
Router(config-if)# ip access-group όνομα {in | out}
```

Διευκρινιστικά αναφέρουμε πως δεν μπορεί να έχουν το ίδιο όνομα επώνυμες λίστες διαφορετικών τύπων (standard, extended).

4.5.18 Δρομολόγηση

Για να μπορέσει ένας δρομολογητής να στείλει ένα πακέτο από ένα δίκτυο σε ένα άλλο δίκτυο, πρέπει πρώτα να προσδιορίσει τη διαδρομή που θα ακολουθήσει το πακέτο. Γενικά, δρομολόγηση (Routing) καλείται η διαδικασία κατά την οποία ένα στοιχείο φτάνει από μια θέση σε μια άλλη. Για παράδειγμα, στην επόμενη εικόνα για να επικοινωνήσει ένας host του υποδικτύου 10.120.2.0 με έναν host του υποδικτύου 172.16.0.0, οι δρομολογητές που βρίσκονται ανάμεσά τους πρέπει να επιλέγουν και να διατηρούν τις διαδρομές.

Εικόνα 4-22: Περιγραφή Δρομολόγησης



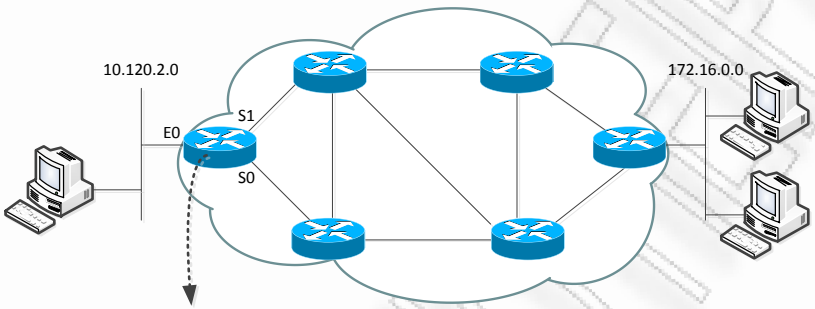
Ένας δρομολογητής για να μπορεί να δρομολογεί πακέτα, θα πρέπει:

1. **Να γνωρίζει τη διεύθυνση προορισμού**: Σε ποια διεύθυνση πρέπει να πάει το πακέτο; Γι' αυτό υπεύθυνος είναι ο host.
2. **Να αναγνωρίζει προελεύσεις πληροφοριών**: Από πού μαθαίνει ο δρομολογητής τις διαδρομές προς έναν καθορισμένο προορισμό, δυναμικά από άλλους δρομολογητές ή στατικά από τον διαχειριστή;
3. **Να ανακαλύπτει πιθανά δρομολόγια:** Ποιές είναι οι αρχικές πιθανές διαδρομές προς τους προορισμούς;
4. **Να επιλέγει τα καλύτερα δρομολόγια**: Ποια είναι η καλύτερη διαδρομή προς τον προορισμό; Πρέπει να γίνεται εξισορρόπηση φορτίων από το δρομολογητή μεταξύ αυτής της διαδρομής και άλλων εξίσου ή λιγότερο βέλτιστων διαδρομών;

5. **Να ελέγχει και να διατηρεί τις πληροφορίες δρομολόγησης**: Οι πληροφορίες δρομολόγησης τοποθετούνται στον πίνακα δρομολόγησης (routing table). Είναι ο πίνακας δρομολόγησης ενημερωμένος;

Ο πίνακας δρομολόγησης είναι ο πληροφοριοδότης του δρομολογητή για τα δίκτυα. Αν το δίκτυο προορισμού συνδέεται απευθείας με το δρομολογητή, αυτός γνωρίζει ήδη ποια διεπαφή θα χρησιμοποιήσει για την προώθηση των πακέτων. Αν όμως τα δίκτυα προορισμού δε συνδέονται απευθείας, τότε ο δρομολογητής πρέπει να ενημερωθεί και να υπολογίσει το καλύτερο δρομολόγιο που θα χρησιμοποιήσει. Ο τρόπος, με τον οποίο ένας δρομολογητής δημιουργεί τον πίνακα δρομολόγησης, απεικονίζεται στη συνέχεια (Εικόνα 4-23).

Εικόνα 4-23: Πίνακας Δρομολόγησης



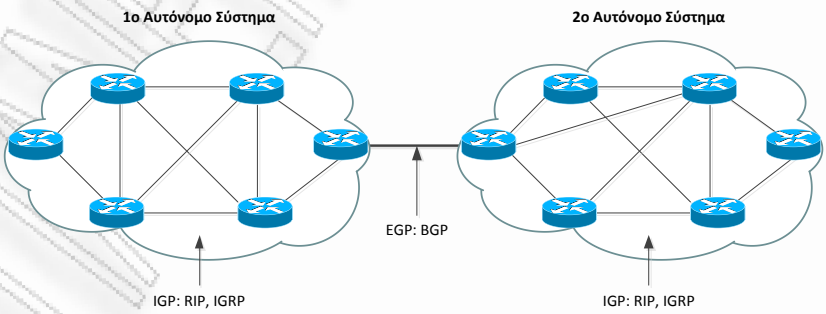
Πρωτόκολλο Δικτύου	Δίκτυο προορισμού	Διεπαφή εξόδου
Πληροφορία από απευθείας σύνδεση	10.120.2.0	E0
Πληροφορία από ενημέρωση	172.16.0.0	S0

Ο πίνακας δρομολόγησης δημιουργείται με έναν από τους ακόλουθους δυο τρόπους:

1. Από το διαχειριστή του δικτύου διευθετώντας τις κατάλληλες εντολές δρομολόγησης με το χέρι.
2. Μέσω δυναμικών διεργασιών που εκτελούνται στο δίκτυο, οι οποίες εξαρτώνται από το επιλεγμένο πρωτόκολλο δυναμικής δρομολόγησης (επιπέδου δικτύου). Το πρωτόκολλο αυτό ορίζει το σύνολο των κανόνων που χρησιμοποιούνται από ένα δρομολογητή όταν αυτός επικοινωνεί με γειτονικούς, καθορίζει τις διαδρομές δρομολόγησης και συντηρεί τους πίνακες.

Οι δυο κύριοι τύποι πρωτοκόλλων δυναμικής δρομολόγησης είναι οι IGP και EGP όπως απεικονίζονται στην Εικόνα 4-24.

Εικόνα 4-24: IGP και EGP Πρωτόκολλα Δυναμικής Δρομολόγησης



- Τα **IGP** (Interior Gateway Protocols, Πρωτόκολλα Εσωτερικών Πυλών) πρωτόκολλα χρησιμοποιούνται για την ανταλλαγή πληροφοριών δρομολόγησης μέσα σε ένα αυτόνομο σύστημα[12].
- Τα **EGP** (Exterior Gateway Protocols, Πρωτόκολλα Εξωτερικών Πυλών) πρωτόκολλα χρησιμοποιούνται για την ανταλλαγή πληροφοριών δρομολόγησης μεταξύ αυτόνομων συστημάτων.

Διευθέτηση Στατικής Δρομολόγησης

Κατά την υλοποίηση του δικτύου μας, επιλέγουμε η δρομολόγηση να διευθετηθεί στατικά. Τα στατικά δρομολόγια ορίζονται από το διαχειριστή και καθορίζουν την IP διεύθυνση του επόμενου hop μιας διαδρομής, την οποία θα ακολουθήσουν τα πακέτα. Σε κάθε δρομολογητή πρέπει να διευθετηθεί ο πίνακας δρομολόγησης ο οποίος θα παρέχει πληροφορίες για τα στατικά δρομολόγια συμπεριλαμβανομένου και ενός ειδικού τύπου στατικού δρομολογίου που καλείται «πύλη έσχατης ανάγκης[13]». Η χρήση στατικής δρομολόγησης δεν επιβαρύνει το δίκτυο με πληροφορίες δρομολόγησης όπως θα συνέβαινε με τη χρήση κάποιου πρωτοκόλλου δυναμικής δρομολόγησης, αλλά μια πιθανή αλλαγή στην τοπολογία του δικτύου επιφορτίζει τον διαχειριστή με την υποχρέωση να ενημερώνει «με το χέρι» όλους τους δρομολογητές.

Η διευθέτηση στατικής δρομολόγησης υλοποιείται με την επόμενη εντολή στην καθολική κατάσταση:

```
Router(config)# ip route δίκτυο [μάσκα] {διεύθυνση | διασύνδεση} [απόσταση] [permanent]
```

Όπου:

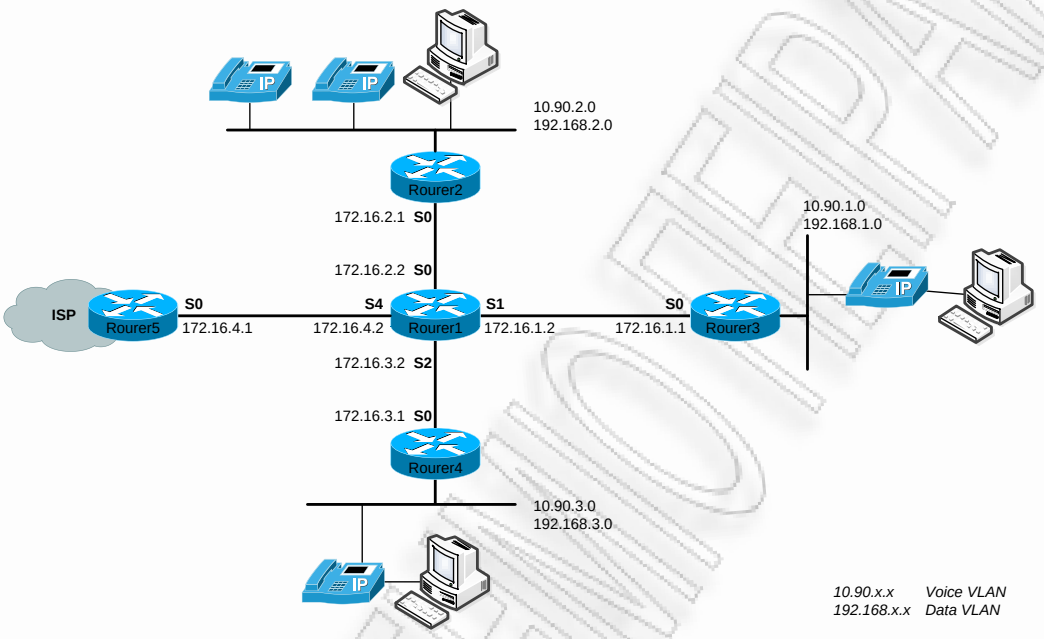
- ✓ *Δίκτυο* είναι το δίκτυο ή υποδίκτυο προορισμού.
- ✓ *Μάσκα* είναι η μάσκα του υποδικτύου.
- ✓ *Διεύθυνση* είναι η IP διεύθυνση του next-hop router.
- ✓ *Διασύνδεση* είναι το όνομα της διεπαφής μέσω της οποίας θα δρομολογηθεί το πακέτο για να φτάσει στο δίκτυο προορισμού.
- ✓ *Απόσταση* είναι μια προαιρετική παράμετρος που ορίζει τη διαχειριστική απόσταση. Προκαθορισμένη τιμή για ένα στατικό δρομολόγιο είναι η τιμή 1.
- ✓ **Permanent** είναι μια προαιρετική παράμετρος μέσω της οποίας καθορίζεται η μη αφαίρεση του δρομολογίου ακόμα και σε περίπτωση που κλείσει η διασύνδεση.

[12] Αυτόνομο Σύστημα (Α.Σ.) καλείται μια συλλογή δικτύων με κοινή περιοχή διαχείρισης. Ο IANA (Internet Assigned Number Authority) είναι υπεύθυνος για την αριθμοδότησης κάθε Α.Σ.

[13] Η «*πύλη έσχατης ανάγκης*» είναι ένας ειδικός τύπος στατικού δρομολογίου που χρησιμοποιείται σε περιπτώσεις όπου δεν είναι γνωστό το δρομολόγιο από μια προέλευση σε έναν προορισμό ή όταν ο πίνακας δρομολόγησης δεν μπορεί να αποθηκεύσει όλες τις απαραίτητες πληροφορίες για τα πιθανά δρομολόγια.

Ας υποθέσουμε το σενάριο που παρουσιάζεται στην Εικόνα 4-25, ο Router1 βρίσκεται στο κεντρικό κατάστημα και συνδέεται μέσω σειριακών διεπαφών με τους δρομολογητές των υποκαταστημάτων (Router2,3,4), καθώς και με τον ISP (Router5). Ο καθορισμός των στατικών δρομολογίων που πρέπει να διευθετηθούν σε κάθε δρομολογητή του δικτύου ώστε να επιτυγχάνεται η δρομολόγηση της κίνησης μεταξύ των υποδικτύων αλλά και από/προς τον ISP παρουσιάζεται στη συνέχεια.

Εικόνα 4-25: Παράδειγμα Στατικής Δρομολόγησης



Διευθέτηση πίνακα δρομολόγησης στον Router1:

Βήμα	Εντολή	Επεξήγηση
1	`Router1(config)# ip route 192.168.1.0 255.255.255.0 172.16.1.1`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.1.0/24 (Data)
2	`Router1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.1`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.2.0/24 (Data)
3	`Router1(config)# ip route 192.168.3.0 255.255.255.0 172.16.3.1`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.3.0/24 (Data)
4	`Router1(config)# ip route 10.90.1.0 255.255.255.0 172.16.1.1`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.1.0 /24 (Voice)
5	`Router1(config)# ip route 10.90.2.0 255.255.255.0 172.16.2.1`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.2.0 /24 (Voice)
6	`Router1(config)# ip route 10.90.3.0 255.255.255.0 172.16.3.1`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.3.0 /24 (Voice)
7	`Router1(config)# ip route 0.0.0.0 0.0.0.0 172.16.4.1`	Ο Router1 πρέπει να δρομολογεί την κίνηση σε ένα μη προσδιορισμένο δίκτυο. Το **0.0.0.0** καθοδηγεί τη δρομολόγηση σε μη γνωστά δίκτυα, όπου με τη χρήση της ειδικής μάσκας **0.0.0.0**, μετατρέπεται σε «πύλη έσχατης ανάγκης». Το **172.16.4.1** καθορίζει την IP του next-hop router.

Διευθέτηση πίνακα δρομολόγησης στον Router2:

Βήμα	Εντολή	Επεξήγηση
1	`Router2(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.1.0/24 (Data)
2	`Router2(config)# ip route 192.168.3.0 255.255.255.0 172.16.2.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.3.0/24 (Data)
3	`Router2(config)# ip route 10.90.1.0 255.255.255.0 172.16.2.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.1.0 /24 (Voice)
4	`Router2(config)# ip route 10.90.3.0 255.255.255.0 172.16.2.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.3.0 /24 (Voice)
5	`Router2(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2`	Ο Router2 πρέπει να δρομολογεί την κίνηση σε ένα μη προσδιορισμένο δίκτυο. Το **0.0.0.0** καθοδηγεί τη δρομολόγηση σε μη γνωστά δίκτυα, όπου με τη χρήση της ειδικής μάσκας **0.0.0.0**, μετατρέπεται σε «πύλη έσχατης ανάγκης». Το **172.16.2.2** καθορίζει την IP διεύθυνση του next-hop router που θα χρησιμοποιηθεί για την προώθηση πακέτων.

Διευθέτηση πίνακα δρομολόγησης στον Router3:

Βήμα	Εντολή	Επεξήγηση
1	`Router3(config)# ip route 192.168.2.0 255.255.255.0 172.16.1.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.2.0/24 (Data)
2	`Router3(config)# ip route 192.168.3.0 255.255.255.0 172.16.1.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.3.0/24 (Data)
3	`Router3(config)# ip route 10.90.2.0 255.255.255.0 172.16.1.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.2.0 /24 (Voice)
4	`Router3(config)# ip route 10.90.3.0 255.255.255.0 172.16.1.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.3.0 /24 (Voice)
5	`Router3(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.2`	Ο Router3 πρέπει να δρομολογεί την κίνηση σε ένα μη προσδιορισμένο δίκτυο. Το **0.0.0.0** καθοδηγεί τη δρομολόγηση σε μη γνωστά δίκτυα, όπου με τη χρήση της ειδικής μάσκας **0.0.0.0**, μετατρέπεται σε «πύλη έσχατης ανάγκης». Το **172.16.1.2** καθορίζει την IP διεύθυνση του next-hop router που θα χρησιμοποιηθεί για την προώθηση πακέτων.

Διευθέτηση πίνακα δρομολόγησης στον Router4:

Βήμα	Εντολή	Επεξήγηση
1	`Router4(config)# ip route 192.168.1.0 255.255.255.0 172.16.3.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.1.0/24 (Data)
2	`Router4(config)# ip route 192.168.2.0 255.255.255.0 S0`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 192.168.2.0/24 (Data), με δήλωση της διεπαφής μέσω της οποίας θα δρομολογηθούν τα πακέτα
3	`Router4(config)# ip route 10.90.1.0 255.255.255.0 172.16.3.2`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.1.0 /24 (Voice)
4	`Router4(config)# ip route 10.90.2.0 255.255.255.0 S0`	Καθορισμός στατικού δρομολογίου για το υποδίκτυο προορισμού 10.90.2.0 /24 (Voice), με δήλωση της διεπαφής μέσω της οποίας θα δρομολογηθούν τα πακέτα.
5	`Router4(config)# ip route 0.0.0.0 0.0.0.0 172.16.3.2`	Ο Router4 πρέπει να δρομολογεί την κίνηση σε ένα μη προσδιορισμένο δίκτυο. Το **0.0.0.0** καθοδηγεί τη δρομολόγηση σε μη γνωστά δίκτυα, όπου με τη χρήση της ειδικής μάσκας **0.0.0.0**, μετατρέπεται σε «πύλη έσχατης ανάγκης». Το **172.16.3.2** καθορίζει την IP διεύθυνση του next-hop router που θα χρησιμοποιηθεί για την προώθηση πακέτων.

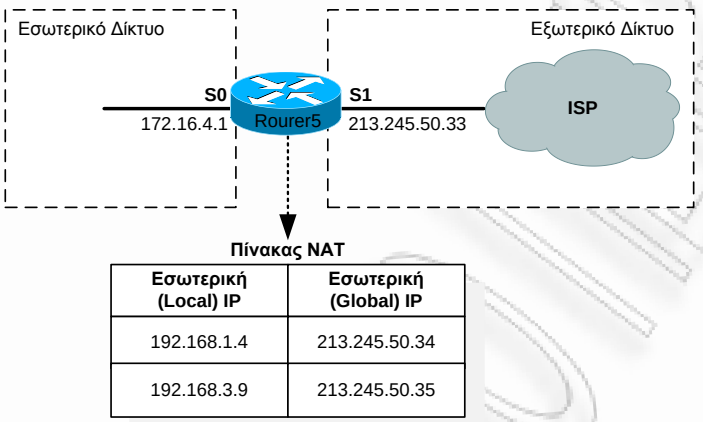
Διευθέτηση πίνακα δρομολόγησης στον Router5:

Βήμα	Εντολή	Επεξήγηση
1	`Router5(config)# ip route 192.168.0.0 255.255.0.0 172.16.4.2`	Καθορισμός στατικού δρομολογίου για τα υποδίκτυα προορισμού 192.168.0.0/16 (Data)
2	`Router5(config)# ip route 10.90.0.0 255.255.255.0 172.16.4.2`	Καθορισμός στατικού δρομολογίου για τα υποδίκτυα προορισμού 10.90.0.0 /16 (Voice)

4.5.19 Διασύνδεση με το Διαδίκτυο - Μετάφραση Εσωτερικών Διευθύνσεων

Έχουμε ήδη αναφέρει, πως η σύνδεση του κεντρικού κόμβου με το Internet και την παροχή υπηρεσιών δεδομένων διαδικτύου (http,dns,ftp,mail κλπ.) στο εσωτερικό δίκτυο θα πραγματοποιηθεί μέσω μιας HWIC-1ADSL κάρτας που έχει τοποθετηθεί στον κεντρικό δρομολογητή. Με βάση την Εικόνα 4-25, υπεύθυνος γι αυτή τη διασύνδεση είναι ο Router5. Μια συνέχεια του προηγούμενου παραδείγματος απεικονίζεται στην Εικόνα 4-26.

Εικόνα 4-26: Μετάφραση IP Διευθύνσεων[14]



Εσωτερική (Local) IP	Εσωτερική (Global) IP
192.168.1.4	213.245.50.34
192.168.3.9	213.245.50.35

Ο μηχανισμός NAT (Network Address Translation, Μετάφραση Διευθύνσεων Δικτύου), επιτρέπει στις επιχειρήσεις όπου δε χρησιμοποιούν πολιτική δημόσιας διευθυνσιοδότησης να συνδέονται στο διαδίκτυο μέσω της μετάφρασης των ιδιωτικών IP διευθύνσεών τους σε δηλωμένες παγκόσμια μοναδικές IP διευθύνσεις. Αυτό επιτρέπει τη χρήση του ίδιου εύρους IP διευθύνσεων σε πολλά intranets και επιπλέον διαφυλάσσει περισσότερο το απόρρητο των δικτύων μη αποκαλύπτοντας τις εσωτερικές IPs σε εξωτερικά δίκτυα.

Στην Εικόνα 4-26 παρουσιάζεται η μετάφραση δυο εσωτερικών IP διευθύνσεων αντίστοιχα σε δυο εξωτερικές IP διευθύνσεις. Τις τελευταίες, συνήθως, τις παρέχει στον πελάτη ο ISP σε συνεργασία φυσικά με την αρχή διευθυνσιοδότησης IANA. Ας θεωρήσουμε πως ο ISP μάς παρέχει ένα 16-αρι[15] δίκτυο εξωτερικών IP διευθύνσεων (συνήθως δίνεται στον εκάστοτε πελάτη μια «δεξαμενή» των 8 ή 16 ή 32 ή 64 μοναδικών IP διευθύνσεων). Συνεπώς, με βάση όσα έχουμε αναφέρει έως τώρα, επικοινωνία με τον «έξω κόσμο» θα μπορούν να έχουν μόνο 13 εσωτερικές IP διευθύνσεις (μια χρησιμοποιείται ως IP της σειριακής διεπαφής S1, μια ως δήλωση δικτύου και μια IP broadcast), γεγονός που σε δίκτυα με εκατοντάδες χρήστες δεν μπορεί να θεωρηθεί ικανοποιητικό.

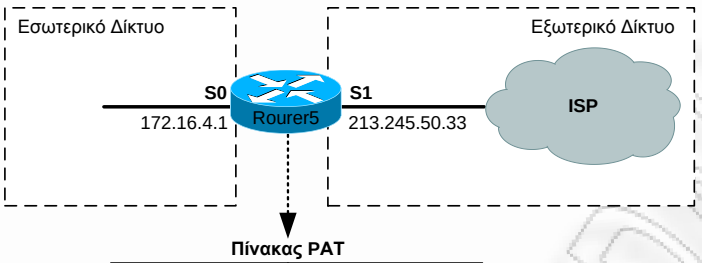
Η αντιμετώπιση αυτής της ανεπιθύμητης κατάστασης γίνεται μέσω του «TCP overloading» ή όπως διαφορετικά λέγεται «στατικό PAT[16]», μέσω του οποίου μεταφράζονται πολλές εσωτερικές IP διευθύνσεις σε μια (ή λίγες) εξωτερική, με τη χρήση μοναδικών αριθμών θυρών στην καθολική IP διεύθυνση η οποία θα αντιπροσωπεύει τις εσωτερικές IP διευθύνσεις στον έξω κόσμο (στο παράδειγμα μας είναι η **213.245.50.33**).

[14] *Εσωτερικό Δίκτυο* (inside network) είναι το σύνολο των δικτύων στα οποία γίνεται μετάφραση, ενώ το *Εξωτερικό Δίκτυο* (outside network) αναφέρεται σε όλες τις άλλες διευθύνσεις.

[15] IP Address: *213.245.50.32*, Subnet Mask: *255.255.255.240*, Host/Network:*14*, Broadcast Addr.: *213.245.50.47.*

[16] PAT: Port Address Translation, Μετάφραση Διευθύνσεων Θυρών

Εικόνα 4-27: Μετάφραση Διευθύνσεων Θυρών

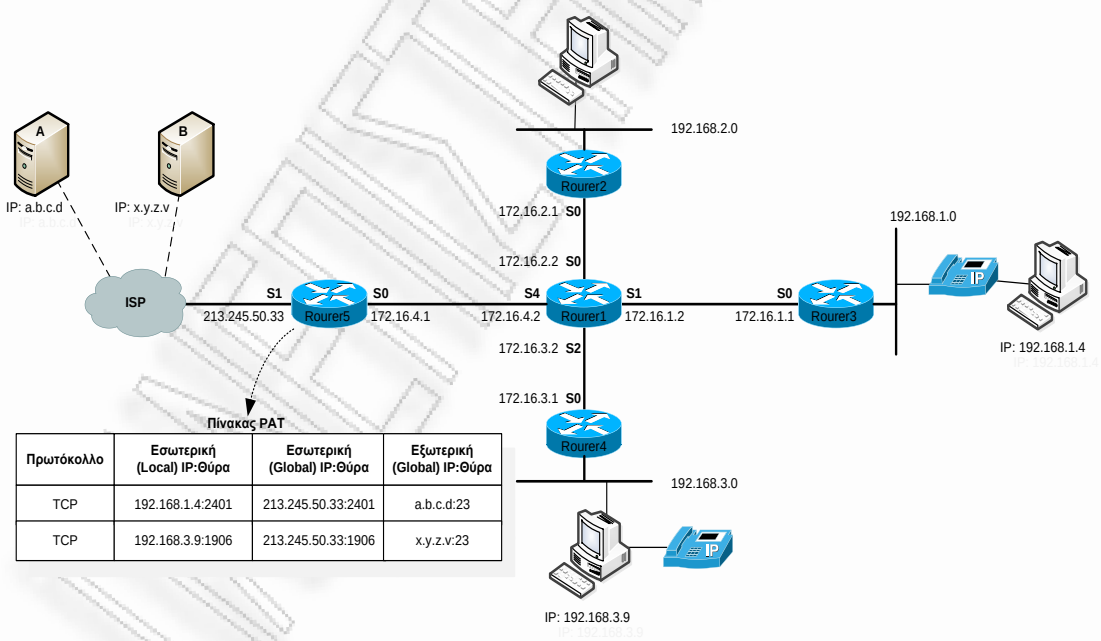


Πίνακας PAT

Εσωτερική (Local) IP	Εσωτερική (Global) IP
192.168.1.4:2401	213.245.50.33:2401
192.168.3.9:1906	213.245.50.33:1906

Στην Εικόνα 4-27 παρουσιάζεται το προηγούμενο παράδειγμα αλλά με χρήση PAT. Τώρα οι δυο εσωτερικές IP διευθύνσεις μεταφράζονται μοναδικά, χρησιμοποιώντας την ίδια καθολική IP διεύθυνση 213.245.50.33 αλλά διαφορετικές θύρες. Κατά αυτόν τον τρόπο και σε συνδυασμό με το γεγονός ότι η θύρα εκφράζεται με έναν 16-bit αριθμό, οι εσωτερικές διευθύνσεις που θεωρητικά μπορούν να μεταφρασθούν με τη χρήση μόνο μιας εξωτερικής διεύθυνσης, είναι 2^{16}=65536 (ομάδες θυρών: 0-511, 512-1023, ή 1024-65535). Μετά τη διευθέτηση στατικού PAT, ο δρομολογητής διατηρεί πολλές πληροφορίες από τα πρωτοκόλλα υψηλοτέρων επιπέδων, όπως αριθμούς θυρών, TCP ή UDP, ώστε να τις χρησιμοποιήσει κατά την αντίστροφη διαδικασία, δηλαδή για τη μετάφραση της εξωτερικής καθολικής διεύθυνσης στη σωστή εσωτερική.

Εικόνα 4-28: Στατικό PAT



Οι αριθμοί θυρών λειτουργούν ως διαφοροποίητές, τόσο ο υπολογιστής **A** όσο και ο **B** πιστεύουν ότι συνομιλούν με ένα μόνο υπολογιστή με IP διεύθυνση την 213.245.50.33. Στην πραγματικότητα όμως, όπως φαίνεται και στην Εικόνα 4-28, επικοινωνούν με περισσότερους του ενός διαφορετικούς υπολογιστές.

Διευθέτηση TCP Overloading

Βήμα	Εντολή	Επεξήγηση
1	Router5(config)# **access-list** 1 **permit** 192.168.1.0 0.0.0.255 Router5(config)# **access-list** 1 **permit** 192.168.2.0 0.0.0.255 Router5(config)# **access-list** 1 **permit** 192.168.3.0 0.0.0.255	Καθορισμός μιας τυπικής λίστας πρόσβασης, που θα καθορίζει ποιες από τις διευθύνσεις του εσωτερικού δικτύου επιτρέπεται να μεταφρασθούν.
2	Router(config)# **ip nat inside source list** *αριθμός λίστας πρόσβασης* **interface** *διεπαφή* **overload** Συνέχεια παραδείγματος: Router5(config)# **ip nat inside source list** 1 **interface** S1 **overload**	Παραμετροποίηση δυναμικής μετάφρασης προέλευσης, καθορίζοντας τον αριθμό λίστας πρόσβασης από το Βήμα 1, καθώς και ποια διεπαφή θα χρησιμοποιείται σαν διεύθυνση υπερφόρτωσης (overload). Στο παράδειγμά μας ο αριθμός ACL=**1** και διεπαφή **S1** (Εικόνα 4-28).
3	Router5(config)# interface S0 Router5(config-if)# **ip nat inside** Router5(config-if)# exit Router5(config)#	Καθορισμός της διεπαφής **S0** ως διεπαφή διασύνδεσης με το εσωτερικό δίκτυο για μετάφραση NAT.
4	Router5(config)# interface S1 Router5(config-if)# **description** to-ISP Router5(config-if)# **ip nat outside** Router5(config-if)# exit Router5(config)#	Καθορισμός της διεπαφής **S1** ως διεπαφή διασύνδεσης με το εξωτερικό δίκτυο για μετάφραση NAT.

Συνεπώς, περιγράφοντας το μηχανισμό μετάφρασης διευθύνσεων θυρών, θα λέγαμε ότι η διαδικασία NAT *από το εσωτερικό προς το εξωτερικό* δίκτυο του παραδείγματος ακολουθεί τα εξής βήματα:

1. Το εισερχόμενο πακέτο μεταφέρεται στον πίνακα του δρομολογητή και προσδιορίζεται το επόμενο hop.
2. Με βάση τις καθορισμένες προτάσεις NAT δημιουργείται μια διεύθυνση προέλευσης.
3. Ο δρομολογητής ενθυλακώνει το πακέτο και το στέλνει από τη διεπαφή S1.

Ενώ η διαδικασία NAT *από το εξωτερικό προς το εσωτερικό δίκτυο* του παραδείγματος ακολουθεί τα εξής βήματα:

1. Αναλύονται οι προτάσεις NAT, ο δρομολογητής αναζητεί μια υπάρχουσα μετάφραση και προσδιορίζει την κατάλληλη διεύθυνση προορισμού.
2. Με τη βοήθεια του πίνακα προσδιορίζεται η διασύνδεση του επόμενου hop για το πακέτο.
3. Το πακέτο ενθυλακώνεται και στέλνεται στη διεπαφή S0.

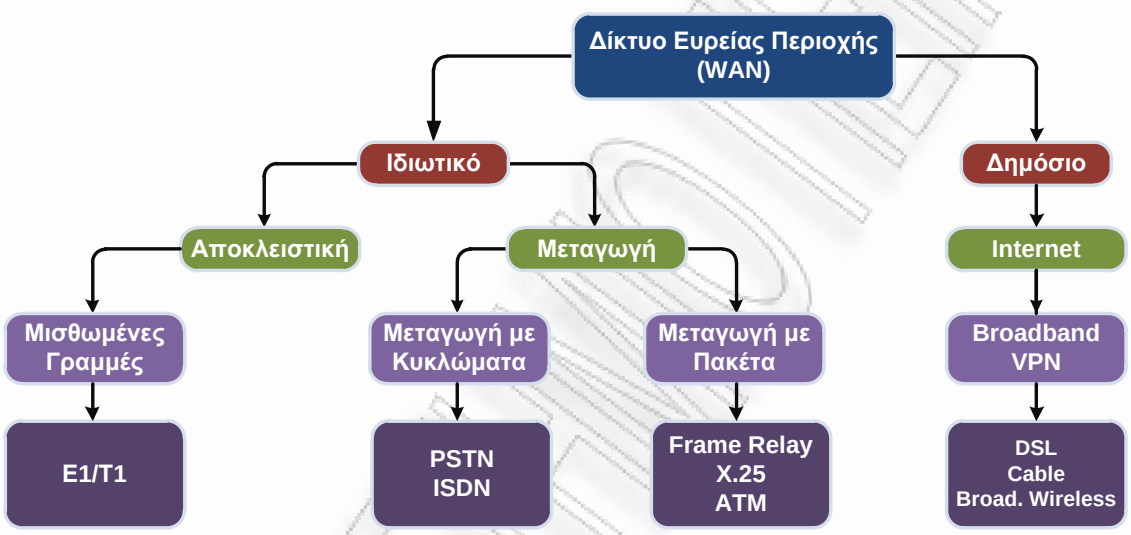
Η προβολή και επιβεβαίωση της μετάφρασης IP διευθύνσεων δικτύου πραγματοποιείται μέσω των εντολών (σε κατάσταση EXEC): α. ***show ip nat translations***, η οποία εμφανίζει τις ενεργές μεταφράσεις και β. ***show ip nat statistics***, η οποία εμφανίζει στατιστικά στοιχεία των μεταφράσεων. Η εντολή ***clear ip nat translation*** αφαιρεί όλες τις καταχωρήσεις δυναμικής μετάφρασης από τον πίνακα NAT.

4.5.20 Διασύνδεση WAN

Ένα Δίκτυο Ευρείας Περιοχής, σε αντίθεση με ένα Τοπικό Δίκτυο, χρησιμοποιεί συνδέσεις δεδομένων σε μια ευρεία γεωγραφική περιοχή. Οι επιχειρήσεις που εδρεύουν σε πολλές διαφορετικές γεωγραφικές τοποθεσίες μισθώνουν (από τους παρόχους) και διευθετούν WAN διασυνδέσεις μεταξύ των καταστημάτων τους ώστε να επιτυγχάνεται ανταλλαγή πληροφοριών μεταξύ αυτών. Οι απαιτήσεις της εκάστοτε σύνδεσης διαφέρουν ανάλογα με τις ανάγκες των εφαρμογών που πρόκειται να εξυπηρετηθούν καθώς και από το κόστος.

Παρότι υπάρχουν πολλές επιλογές για τη δημιουργία μιας WAN διασύνδεσης, η τελική επιλογή εξαρτάται πάντα από τις παρεχόμενες, σε κάθε γεωγραφική τοποθεσία, υπηρεσίες. Στην Εικόνα 4-29, παρουσιάζονται οι βασικές επιλογές διασύνδεσης:

Εικόνα 4-29: Επιλογή WAN Διασύνδεσης



Μια **Μισθωμένη Γραμμή** (leased line) καλείται επίσης και σύνδεση point-to-point, παρέχει μια προεγκατεστημένη, αποκλειστική για τον πελάτη διαδρομή επικοινωνίας μεταξύ δυο διαφορετικών γεωγραφικών σημείων. Οι μισθωμένες γραμμές είναι δαπανηρές αλλά με εγγυημένη διαθεσιμότητα του εύρους ζώνης και μεγάλη ασφάλεια. Συνήθως υλοποιούνται σε σύγχρονες σειριακές συνδέσεις με πολύ υψηλές ταχύτητες που φτάνουν έως 45 Mbps.

Η **Μεταγωγή με Κυκλώματα** (circuit-switched) είναι μια μέθοδος μεταγωγής WAN στην οποία κατά τη διάρκεια μιας κλήσης πρέπει να υπάρχει μια αποκλειστική διαδρομή μέσω κυκλωμάτων μεταξύ αποστολέα και παραλήπτη. Οι διαδρομές αυτές παραμένουν σταθερές κατά τη διάρκεια της κλήσης αλλά δεν είναι απαραίτητο οι επόμενες κλήσεις να χρησιμοποιήσουν την ίδια διαδρομή. Συνήθως η μεταγωγή με κυκλώματα χρησιμοποιείται για παροχή υπηρεσιών τηλεφωνίας (PSTN ή ISDN) καθώς και σε WAN συνδέσεις με απαίτηση για περιστασιακή χρήση (π.χ. Backup links). Η υλοποίησή τους γίνεται με τη χρήση μιας ασύγχρονης συριακής σύνδεσης στο δρομολογητή, ο οποίος είναι συνδεδεμένος σε ένα modem.

Η **Μεταγωγή με Πακέτα** (packet-switched) είναι μια μέθοδος μεταγωγής WAN μέσω της οποίας, για τη μεταφορά πακέτων από μια προέλευση σε ένα προορισμό μέσα από ένα δίκτυο παρόχου, οι δικτυακές συσκευές μοιράζονται ένα point-to-point ή point-to-multipoint σύνδεσμο. Για τη μεταγωγή πακέτων τα διαδίκτυα χρησιμοποιούν μόνιμα εικονικά κυκλώματα (PVC, Permanent Virtual Circuits) ή εικονικά κυκλώματα μεταγωγής (SVC, Switched Virtual Circuits) που παρέχουν από άκρο σε άκρο σύνδεση. Οι κεφαλίδες των πακέτων συνήθως παρέχουν την πληροφορία προορισμού. Οι υπηρεσίες που παρέχει η μεταγωγή με πακέτα,

είναι εφάμιλλες με αυτές των μισθωμένων γραμμών. Το κόστος είναι χαμηλότερο και αυτό οφείλεται στο γεγονός ότι ενώ υπάρχει μια αποκλειστική ποσότητα εύρους ζώνης μεταξύ του παρόχου και του πελάτη, μέσα στο «σύννεφο» του παρόχου το εύρος ζώνης μοιράζεται και σε άλλους πελάτες. Υλοποιούνται σε σύγχρονες σειριακές συνδέσεις.

Όμοια με τη μεταγωγή με πακέτα λειτουργεί και η **Μεταγωγή με Κελιά** (cell-switched). Αντί για πακέτα μεταβλητού μήκους, τα δεδομένα διαιρούνται σε κελιά σταθερού μήκους (53 bytes) και έπειτα μεταφέρονται μέσω εικονικών κυκλωμάτων. Ένα χαρακτηριστικό παράδειγμα μεταγωγής με κελιά είναι το ATM. Οι ταχύτητες διασύνδεσης με χρήση καλωδίων χαλκού φτάνουν τα 45 Mbps, ενώ με τη χρήση οπτικών ινών αγγίζουν τα 10 Gbps. Εκτός από τη μεγάλη ταχύτητα η μεταγωγή με κελιά παρέχει προσαρμογή πολυμέσων (φωνή, βίντεο) και καλύτερη Ποιότητα Υπηρεσίας (QoS).

Ο φθηνότερος αλλά και λιγότερο ασφαλής τρόπος WAN διασύνδεσης είναι μέσω του **Internet**. Λόγο του χαμηλού κόστους, αλλά και της μεγάλης γεωγραφικής εξάπλωσης της υπηρεσίας, τα τελευταία χρόνια έχει καθιερωθεί ως ελκυστική επιλογή. Στην κατεύθυνση αυτή θετικά συμβάλουν και οι διαθέσιμες τεχνικές κρυπτογράφησης IPsec/VPNs (δες 3.5) που μπορούν να υλοποιηθούν μέσω του Internet ώστε να παρέχουν από σημείο σε σημείο την ασφαλή επικοινωνία μέσω Layer-3 κρυπτογραφημένων σηράγγων. Η διαδικασία της κρυπτογράφησης - αποκρυπτογράφησης υλοποιείται στα τελικά σημεία της σήραγγας και η προστατευμένη κίνηση διαβιβάζεται σε όλο το δίκτυο παρέχοντας έτσι μεγαλύτερο επίπεδο ασφάλειας. Οι ταχύτητες διασύνδεσης φτάνουν 24 Mbps (Download) χωρίς εγγυημένη διαθεσιμότητα.

Ανάλογα λοιπόν με τις ανάγκες κάθε επιχείρησης, τα χαρακτηριστικά των διατιθέμενων στην ενδιαφέρουσα γεωγραφική περιοχή διασυνδέσεων WAN αλλά και το κόστος «ενοικίασης» της γραμμής από τον πάροχο ολοκληρώνεται η διαδικασία επιλογής. Όπως ήδη έχουμε αναφέρει και στις σχεδιαστικές κατευθύνσεις υλοποίησης του δικτύου μας, για τη διασύνδεση των υποκαταστημάτων με τον κεντρικό κόμβο θα χρησιμοποιηθούν μισθωμένες γραμμές. Για αυτό το λόγο έχει επιλεγεί να τοποθετηθεί στους κεντρικούς δρομολογητές η κάρτα HWIC-4T (βλ. Εικόνα 4-9) όπου υποστηρίζει σύγχρονες σειριακές συνδέσεις.

Βάσει της επιλεγμένης διάρθρωσης του δρομολογητή και κατά προέκταση του τύπου των διεπαφών (Serial, ADSL, ISDN κ.α.) που υπάρχουν σε αυτόν, μεταβάλλονται οι υποστηριζόμενοι τύποι Layer-2 ενθυλάκωσης. Όσον αφορά τις σειριακές διεπαφές οι δρομολογητές Cisco υποστηρίζουν HDLC, PPP και FR. Κάτι που μπορεί να απεικονιστεί δίνοντας στη σειριακή διεπαφή την εντολή ***encapsulation ?***, όπως παρουσιάζεται στη συνέχεια για τη διεπαφή *S0/0/0* (η έξοδος μπορεί να διαφέρει ανάλογα με την έκδοση του IOS που τρέχει στον δρομολογητή):

```
Router(config)#configuration terminal
Router(config)# interface S0/0/0
Router(config-if)# encapsulation ?
        atm-dxi          ATM-DXI encapsulation
        frame-relay      Frame Relay networks
        hdlc             Serial HDLC synchronous
        lapb             LAPB (X.25 Level 2)
        ppp              Point-to-Point protocol
        x25              X.25
```

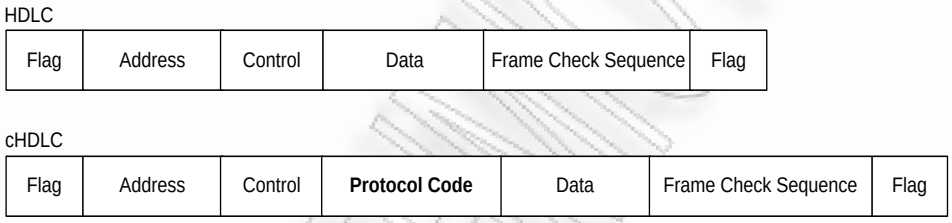
Πρέπει να διευκρινίσουμε πως αν είχαμε άλλους τύπους διεπαφών στο δρομολογητή θα είχαμε και διαφορετικές επιλογές ενθυλάκωσης σαν αποτέλεσμα.

Διευθέτηση HDLC Ενθυλάκωσης

Το HDLC (High-Level Data Link Control, Έλεγχος Συνδέσμου Υψηλού Επιπέδου) αποτελεί μια μέθοδο ενθυλάκωσης δεδομένων σε σύγχρονους σειριακούς συνδέσμους η οποία χρησιμοποιεί χαρακτήρες και άθροισμα ελέγχου πλαισίων. Το HDLC είναι ένα πρωτόκολλο Layer 2 και χρησιμοποιείται συχνά σε ζεύξεις point-to-point. Αρχικά υλοποιήθηκε για τη μεταφορά χαρακτήρων μεταξύ «χαζών» τερματικών σε απομακρυσμένα δίκτυα. Το HDLC σε μια ζεύξη δεν μπορεί να υποστηρίξει εγγενώς πολλά πρωτόκολλα και αυτό διότι δεν υπάρχει τυποποιημένη μέθοδος που να καθορίζει ποιο πρωτόκολλο μεταφέρει.

Η ανάγκη προσπέλασης του παραπάνω μειονεκτήματος, οδήγησε τη Cisco στη δημιουργία μιας αποκλειστικής έκδοσης του HDLC που το ονόμασε cHDLC. Τα πλαίσια του cHDLC χρησιμοποιούν ένα πεδίο που ενεργεί ως πεδίο πρωτοκόλλου, επιτυγχάνοντας έτσι τη δυνατότητα κοινής χρήσης του ίδιου σειριακού συνδέσμου από πολλά πρωτόκολλα. Το cHDLC είναι ο προεπιλεγμένος τύπος ενθυλάκωσης μόνο μεταξύ δρομολογητών Cisco όπου μπορούν να αναγνωρίζουν και ερμηνεύουν το συγκεκριμένο τύπο πλαισίων. Στην Εικόνα 4-30 παρουσιάζεται η μορφή των HDLC και cHDLC πλαισίων. Στο cHDLC πλαίσιο διακρίνεται το πεδίο **Protocol Code** που είναι υπεύθυνο για τον καθορισμό του τύπου πρωτοκόλλου που ενθυλακώνεται μέσα στο πλαίσιο.

Εικόνα 4-30: Μορφή Πλαισίων HDLC και cHDLC



Οι σύγχρονες σειριακές συνδέσεις από προεπιλογή χρησιμοποιούν τη μέθοδο cHDLC. Σε περίπτωση όμως που αυτό έχει αλλάξει από κάποια προγενέστερη παραμετροποίηση η διαδικασία διευθέτησης cHDLC ενθυλάκωσης υλοποιείται με την εντολή ***encapsulation hdlc*** όπως παρουσιάζεται στη συνέχεια:

```
Router#configuration terminal
Router(config)# interface S0/0/0
Router(config-if)# encapsulation hdlc
```

Το cHDLC λοιπόν, είναι ένα Layer-2 πρωτόκολλο που χρησιμοποιείται σε μισθωμένες γραμμές μεταξύ δυο συσκευών Cisco όπου μπορούν να ερμηνεύουν το συγκεκριμένο τύπο πλαισίων. Για την επικοινωνία συσκευών που δεν υποστηρίζουν το cHDLC, ως μέθοδος ενθυλάκωσης ενδείκνυται το πρωτόκολλο PPP.

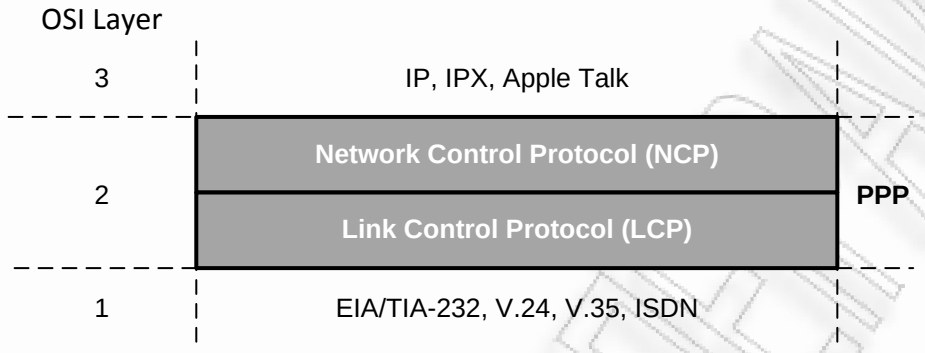
PPP Ενθυλάκωση

Το PPP περιγράφεται από τα έγραφα RFC1661, RFC1932 και RFC1332. Μπορεί να διευθετηθεί σε διεπαφές τύπου όπως:

- ✓ Ασύγχρονες σειριακές
- ✓ Σύγχρονες σειριακές
- ✓ ISDN
- ✓ HSSI (High Speed Serial Interface, Συριακή διασύνδεση Υψηλής Ταχύτητας)

Το PPP είναι ένα πρωτόκολλο επιπέδου ζεύξης δεδομένων, με υψηλά βελτιωμένη λειτουργική αξία λόγω της χρήσης δύο υποεπιπέδων, των NCP και LCP όπως απεικονίζονται στη συνέχεια (Εικόνα 4-31).

Εικόνα 4-31: PPP Υποεπίπεδα



Το PPP για να μπορεί να υποστηρίζει και να ενθυλακώνει πολλά πρωτόκολλα Layer-3, χρησιμοποιεί το **NCP** (Network Control Protocol, Πρωτόκολλο Ελέγχου Δικτύου). Το PPP μεταφέρει πακέτα από πολλά πρωτόκολλα επιπέδου δικτύου σε στοιχεία NCP. Πρόκειται για πεδία που περιέχουν τυποποιημένη πληροφορία με τον κωδικό του πρωτοκόλλου που ενθυλακώνει το PPP.

Επιπλέον, το PPP χρησιμοποιεί τις **LCP** (Link Control Protocol, Πρωτόκολλο Ελέγχου Συνδέσμου) επιλογές κυρίως στη διαπραγμάτευση και τον έλεγχο πλαισίων για την υλοποίηση των μηχανισμών ελέγχου της point-to-point ζεύξης που καθορίζει ο διαχειριστής για τη σύνδεση. Ο Πίνακας 4-2 παρουσιάζει τις λειτουργικές επιλογές του LCP.

Πίνακας 4-2: Επιλογές Διευθέτησης LCP

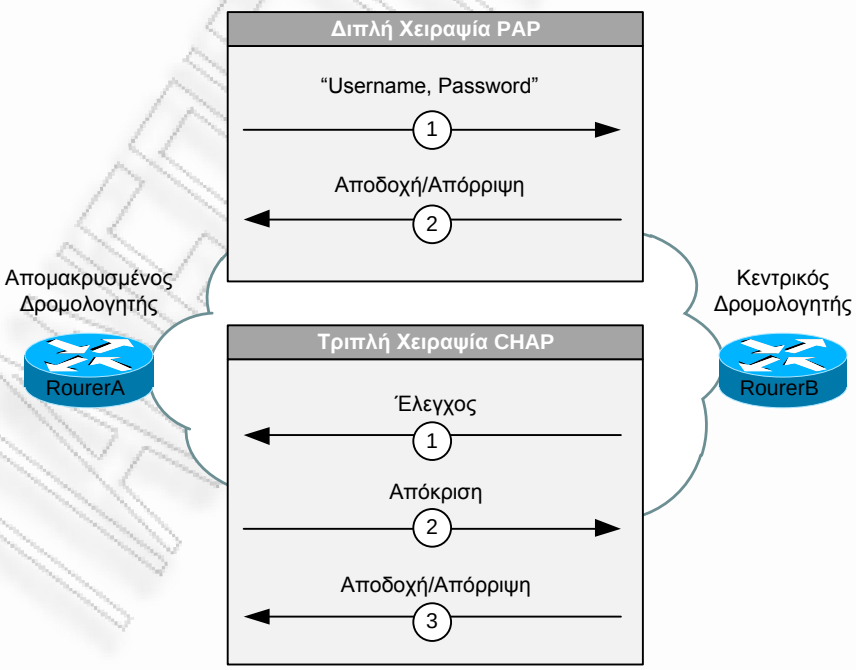
Επιλογή LCP	**Πρωτόκολλο**	**Λειτουργία**
Εντοπισμός σφαλμάτων (Error detection)	Magic Number Quality	Οι μηχανισμοί εντοπισμού σφαλμάτων επιτρέπουν σε μια διεργασία να εντοπίσει προβληματικές καταστάσεις. Οι επιλογές Magic Number και Quality βοηθούν στην εξασφάλιση της ποιότητας των ζεύξεων.
Multilink	Multilink PPP	Επιτρέπει τη χρήση πολλών διασυνδέσεων PPP που έχουν τον ίδιο προορισμό, για την εξισορρόπηση του φορτίου.
Συμπίεση (Compression)	Stacker Predictor	Με την επιλογή συμπίεσης, μειώνονται τα προς αποστολή δεδομένα αφού τα πλαίσια συμπιέζονται πριν την αποστολή τους και αποσυμπιέζονται από την πλευρά του παραλήπτη. Επιτυγχάνοντας έτσι αύξηση της διεκπεραιωτικής ικανότητας της PPP ζεύξης.
Πιστοποίηση (Authentication)	PAP CHAP	Οι επιλογές πιστοποίησης, απαιτούν από την καλούσα πλευρά της ζεύξης κατά την προσπάθεια σύνδεσής της, να εισάγει πληροφορίες με τις οποίες θα αποδεικνύει τη νόμιμη άδεια σύνδεσης. Είναι ιδιαίτερα χρήσιμες σε συνδέσεις μέσω τηλεφώνου που χρησιμοποιούν το PPP ως μέθοδο ενθυλάκωσης.

Για την αποκατάσταση PPP σύνδεσης μεταξύ των συσκευών απαιτούνται τρεις φάσεις οι οποίες περιγράφονται στη συνέχεια:

Εικόνα 4-32: Αποκατάσταση PPP Σύνδεσης

1. Στη **Φάση δημιουργίας συνδέσμου**, κάθε συσκευή στέλνει πακέτα LCP προκειμένου να ξεκινήσει η διαδικασία διαπραγμάτευσης μεταξύ των συσκευών. Τα LCP πακέτα περιέχουν ένα πεδίο *Επιλογής Διευθέτησης* που επιτρέπει στις συσκευές να διαπραγματεύονται τη χρήση επιλογών όπως αυτών που αναφέρονται στον Πίνακας 4-2.
2. Η **Φάση πιστοποίησης** είναι προαιρετική. Ως εκ τούτου, μετά την πιθανή επιλογή πρωτοκόλλου πιστοποίησης PAP ή CHAP, ξεκινά η επιλεγμένη διαδικασία πιστοποίησης.
3. Στη **Φάση πρωτοκόλλου επιπέδου δικτύου**, οι συσκευές στέλνουν NCP πακέτα προκειμένου να διευθετήσουν ένα ή και περισσότερα πρωτόκολλα Layer-3. Μόλις συμβεί αυτό κάθε ένα από τα επιλεγμένα πρωτόκολλα έχει τη δυνατότητα αποστολής πακέτων μέσω της WAN ζεύξης.

Εικόνα 4-33: Πιστοποίηση PAP και CHAP



Η πιστοποίηση είναι μια επιλογή αρκετά χρήσιμη ειδικά σε συνδέσεις μέσω τηλεφώνου όπου δεν υπάρχει εκ των προτέρων καμία εγγύηση για το ποιος θα προσπαθήσει να συνδεθεί με το δρομολογητή. Κατά την υλοποίηση PPP πιστοποίησης δύναται να χρησιμοποιηθούν δυο πρωτόκολλα, το PAP και το CHAP, με το δεύτερο να θεωρείται ασφαλέστερο.

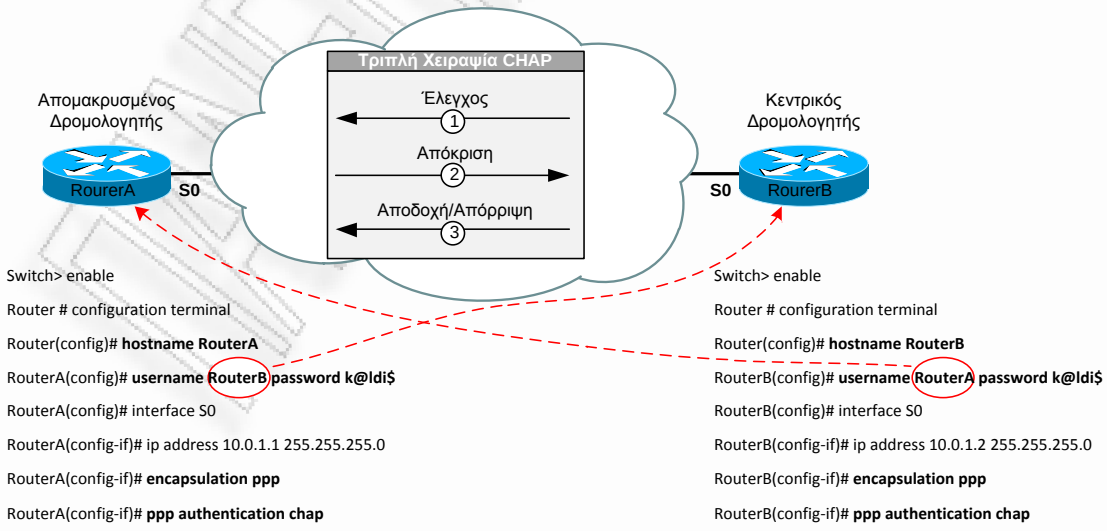
Το PAP δε θεωρείται ισχυρό πρωτόκολλο πιστοποίησης. Επεμβαίνει μόνο κατά την αρχική δημιουργία της σύνδεσης και βασίζεται στον προσδιορισμό της ταυτότητας ενός απομακρυσμένου κόμβου με τη χρήση της «διπλής χειραψίας» (βλ. Εικόνα 4-33). Μετά την ολοκλήρωση της φάσης δημιουργίας συνδέσμου (1η φάση) ο **απομακρυσμένος** δρομολογητής στέλνει συνεχώς ζεύγη username και password έως ότου ολοκληρωθεί η σύνδεση με αποδοχή ή διακοπεί η σύνδεση με απόρριψη. Κατά την πιστοποίηση PAP αυτός που έχει τον έλεγχο συγχρονισμού για την πραγματοποίηση σύνδεσης είναι ο απομακρυσμένος κόμβος. Το password στέλνεται χωρίς απόκρυψη μέσω της ζεύξης και δεν παρέχεται καμία προστασία από επιθέσεις επανάληψης.

Αντίθετα με το PAP, το CHAP δεν επεμβαίνει μόνο κατά την αρχική σύνδεση αλλά και σε τακτά χρονικά διαστήματα, μετά την αποκατάστασή της, ώστε να επαληθεύει συνέχεια την ταυτότητα μέσω «τριπλής χειραψίας» (βλ. Εικόνα 4-33). Μετά την ολοκλήρωση της φάσης δημιουργίας συνδέσμου (1η φάση), ο **κεντρικός** δρομολογητής στέλνει στον απομακρυσμένο κόμβο ένα μήνυμα «επαλήθευσης». Ο τελευταίος απαντά με μια τιμή που υπολογίζεται μέσω μιας μονόδρομης συνάρτησης κατατεμαχισμού (συνήθως χρησιμοποιείται η MD5 που βασίζεται στο κοινό username και σε ένα «μήνυμα επαλήθευσης»). Ο κεντρικός δρομολογητής, αφού έχει ολοκληρώσει τους δικούς του υπολογισμούς, αναμένει μια συγκεκριμένη τιμή κατατεμαχισμού. Αν ο απομακρυσμένος τού στείλει την αναμενόμενη τιμή τότε η σύνδεση παραμένει ενεργή, διαφορετικά διακόπτεται ακαριαία. Το CHAP παρέχει προστασία από επιθέσεις επανάληψης.

Διευθέτηση Ενθυλάκωσης PPP και Πιστοποίησης CHAP

Στο παράδειγμα της Εικόνα 4-34, παρουσιάζεται η διαδικασία διευθέτησης ενθυλάκωσης PPP και πιστοποίησης CHAP. Οι εντολές πιστοποίησης εφαρμόζονται και στους δυο δρομολογητές αφού εκατέρωθεν πρέπει και να πιστοποιήσουν και να πιστοποιηθούν. Το username καθώς και το password που στέλνει ο κάθε δρομολογητής πρέπει να ταιριάζουν με αυτά που έχουν καθοριστεί (μέσω της εντολής: Router(config)# **username** *όνομα* **password** *κωδικός-πρόσβασης*) στον «απέναντι» δρομολογητή. Δηλαδή, όπως απεικονίζεται και στο παράδειγμα, σαν *όνομα χρήστη* CHAP για τον ένα δρομολογητή ορίζουμε το hostname του απέναντι δρομολογητή. Επίσης ο *κωδικός-πρόσβασης* και στους δυο δρομολογητές πρέπει να είναι ο ίδιος.

Εικόνα 4-34: Διευθέτηση Ενθυλάκωσης PPP και Πιστοποίησης CHAP



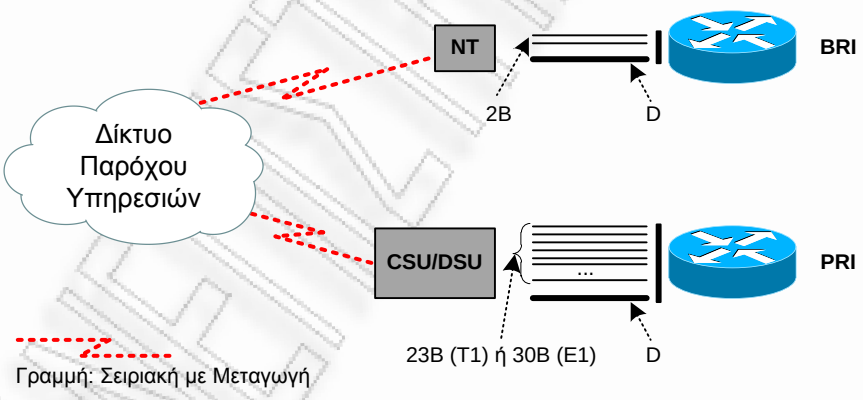
4.5.21 Διασύνδεση με Τηλεπικοινωνιακό Πάροχο Υπηρεσιών

Για την ολοκλήρωση μη ενδοεταιρικών κλήσεων, δηλαδή κλήσεων από και προς τηλεφωνικούς αριθμούς που δεν ανήκουν στο αριθμοδοτικό πλάνο της εταιρίας, απαιτείται η διασύνδεση της τελευταίας με έναν (ή και περισσότερους) πάροχο τηλεφωνίας, όπως είναι ο ΟΤΕ η HOL κ.α. Η διασύνδεση με τον πάροχο μπορεί να γίνει σε ένα ή και περισσότερα σημεία του WAN δικτύου ανάλογα με τις ανάγκες και την πολιτική της εκάστοτε εταιρίας.

Για παράδειγμα, η εταιρία του υποθετικού σεναρίου που υλοποιούμε έχει 16 σημεία παρουσίας σε όλη την Ελλάδα. Στην περίπτωσή μας, επιλέγουμε να υπάρχει μόνο ένα κεντρικό σημείο διασύνδεσης (μέσω PRI ISDN) με τον πάροχο (π.χ. στο κεντρικό κατάστημα της Αθήνας). Μια εξερχόμενη κλήση που θα πραγματοποιηθεί από ένα περιφεριακό κατάστημα (π.χ. της Καλαμάτας), για να εξυπηρετηθεί πρέπει πρώτα να δρομολογηθεί μέσω του WAN της εταιρίας προς τον κεντρικό κόμβο και έπειτα από εκεί προς τον τελικό προορισμό μέσω του παρόχου υπηρεσιών. Στη περίπτωση αυτή παρατηρείται αναστάτωση όταν τηλέφωνα περιφεριακών καταστημάτων καλούν αριθμούς άμεσης ανάγκης (π.χ. 199 ή 100), αφού οι κλήσεις δεν μπορούν να κατευθυνθούν στους κατά τόπους σταθμούς. Η αντιμετώπιση αυτού του προβλήματος μπορεί να επιτευχτεί αν σε κάθε περιφεριακό κατάστημα εγκατασταθεί μια BRI γραμμή και επιπροσθέτως παραμετροποιηθεί κατάλληλα το πλάνο ελέγχου κλήσεων, ώστε να δρομολογεί προς την BRI πύλη όλες τις κλήσεις άμεσης ανάγκης που πραγματοποιούνται από τοπικά εσωτερικά τηλέφωνα. Ένα δεύτερο όφελος που προσφέρει η παραπάνω επιλογή είναι ότι τα εσωτερικά τηλέφωνα των περιφεριακών καταστημάτων, δύναται να αποκτήσουν και τοπική αριθμοδότηση (π.χ. για την Καλαμάτα: 27210…..). Μέσα από κατάλληλα διαμορφωμένους πίνακες αντιστοίχησης στο πλάνο ελέγχου, οι κλήσεις προς αριθμούς με τοπική αριθμοδότηση εξυπηρετούνται από συγκεκριμένα εσωτερικά τοπικά τηλέφωνα.

Όπως ήδη έχουμε αναφέρει, οι δυο πρότυπες μέθοδοι πρόσβασης που καθορίζει το ISDN είναι οι BRI και PRI όπως παρουσιάζονται στην Εικόνα 4-35.

Εικόνα 4-35: Μέθοδοι Πρόσβασης ISDN



1. Η **BRI** (Basic Rate Interface, Διασύνδεση Βασικού Ρυθμού) διασύνδεση αποτελείται από δυο κανάλια **B** (Bearer, Φέροντα) 64 Kbps και ένα κανάλι **D** 16 Kbps. Τα κανάλια B χρησιμοποιούνται για τη μετάδοση ψηφιοποιημένων σημάτων ομιλίας, ενώ το κανάλι D χρησιμοποιείται για την έναρξη της κλήσης, τη σηματοδοσία και τον τερματισμό της κλήσης. Η κυκλοφορία που διέρχεται από το κανάλι D βασίζεται στο Layer-2 πρωτόκολλο LAPD (το LAPD βασίζεται στο HDLC). Στους επιλεγμένους για το δίκτυο μας δρομολογητές 2951 και 2901 υπάρχουν αντίστοιχα 16 και 8 BRI διαθέσιμες διασυνδέσεις.
2. Η **PRI** (Primary Rate Interface, Διασύνδεση Πρωτεύοντος Ρυθμού) διασύνδεση, μέσω της τεχνολογίας **T1**, παρέχει 23 κανάλια **B** 64 Kbps και ένα κανάλι **D** 64 Kbps. Στην Ευρώπη αλλά και σε πολλά άλλα σημεία του κόσμου χρησιμοποιείται η τεχνολογία **E1**, μέσω της οποίας η PRI διασύνδεση παρέχει 30 κανάλια **B** 64 Kbps και ένα κανάλι **D** 64

Kbps. Για μια διασύνδεση PRI, αν η επιλεγμένη στον δρομολογητή κάρτα έχει ενσωματωμένο εξοπλισμό CSU/DSU, απαιτείται μόνο μια απευθείας σύνδεση με τον πάροχο, διαφορετικά πρέπει να παρεμβάλλεται ο εξοπλισμός CSU/DSU (Channel Service Unit/Data Service Unit, Μονάδα Εξυπηρέτησης Δεδομένων/Μονάδα Εξυπηρέτησης Καναλιού). Η κάρτα HWIC-2CE1T1 (βλ. Εικόνα 4-8), διαθέτει ολοκληρωμένο σύστημα CSU/DSU καθιστώντας μη αναγκαία την ύπαρξη εξωτερικού modem για τη διασύνδεση.

Ενεργοποίηση PRI ISDN Διασύνδεσης

Προκειμένου να ενεργοποιηθεί μια PRI ISDN διασύνδεση ακολουθούμε τα επόμενα βήματα διευθέτησης:

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# isdn switch-type` *switch-type* Παράδειγμα: `Router(config)# isdn switch-type primary-net5`	Καθορισμός του τύπου μεταγωγέα, με βάση τη *switch-type* τιμή που χρησιμοποιεί ο πάροχος υπηρεσιών (βλ. Πίνακας 4-3).
2	`Router(config)# controller {t1 | e1}` slot/port Παράδειγμα: `Router(config)# controller e1 1/0`	Εισαγωγή στον controller και επιλογή του τύπου της PRI διασύνδεσης (T1 ή E1).

3	`Router(config-controller)# framing {sf | esf | crc4 | no-crc4}`
	Παράδειγμα:
	`Router(config-controller)# framing crc4`
		Καθορισμός του τύπου πλαισίων που θα χρησιμοποιεί ο πάροχος για την επικοινωνία μέσω της γραμμής. Ο τύπος δίνεται στον πελάτη από τον πάροχο και μπορεί να είναι για T1: **SF** (Super Frame, Υπερπλαίσιο) ή **ESF** (Extended SF, Εκτεταμένο Υπερπλαίσιο) και για E1: **CRC4** (Cyclic Redundancy Check 4, Κυκλικός Έλεγχος Πλεονασμού) ή χωρίς Κυκλικό Έλεγχο Πλεονασμού (no-CRC4)

4	`Router(config-controller)# clocking {line | internal | loop-timed}`
	Παράδειγμα:
	`Router(config-controller)# clocking line`
		Καθορισμός προέλευσης χρονισμού. Από προεπιλογή είναι η γραμμή του παρόχου (line).

5	`Router(config-controller)# linecode {ami | b8zs | hdb3}`
	Παράδειγμα:
	`Router(config-controller)# linecode hdb3`
		Ρύθμιση σηματοδότησης κωδικού γραμμής. Έγκυρες τιμές για:
		T1: **ami** (προεπιλεγμένη) ή **b8zs**
		E1: **hdb3**

6	`Router(config-controller)# pri-group timeslots {1-24 | 1-31}`
	Παράδειγμα:
	`Router(config-controller)# pri-group timeslots 1-31`
	`Router(config-controller)# exit`
		Καθορίζει ότι ο ελεγκτής θα λειτουργεί σαν PRI και προσθέτει το κατάλληλο εύρος χρονοθυρίδων ανάλογα με τον τύπο:
		T1: **1-24**, E1: **1-31**

7	`Router(config)# interface serial` slot/port:23 ή `Router(config)# interface serial` slot/port:15 Παράδειγμα: `Router(config)# interface serial 1/0:15`	Μετά τη δημιουργία των χρονοθυρίδων (Βήμα 6), ο δρομολογητής δημιουργεί αυτόματα τη διασύνδεση του καναλιού D, όπου είναι η σειριακή διεπαφή: Για T1: **slot/port:23** Για E1: **slot/port:15** Εισαγωγή στη σειριακή διεπαφή 1/0:15
8	`Router(config-if)# isdn incoming-voice voice`	Ενεργοποιεί την εισερχόμενη κίνηση φωνής (ενεργεί ως το κανάλι D) για να εξασφαλίσει τον τόνο κλήσης.

Πίνακας 4-3: Τύποι Μεταγωγέων PRI ISDN

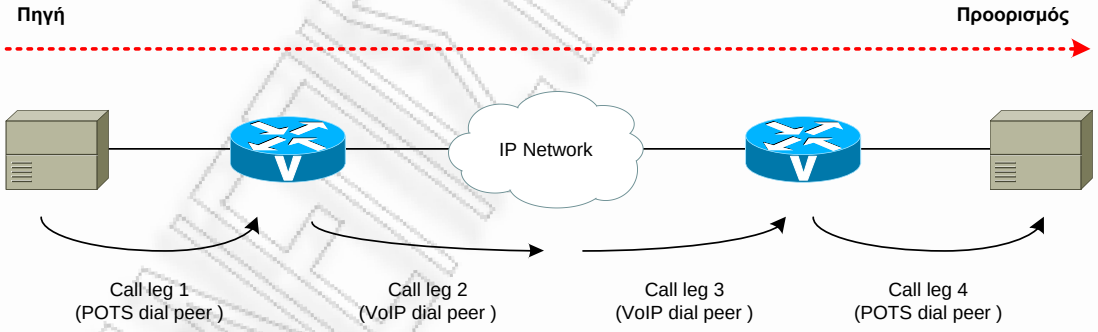
Τιμή: *switch-type*	Περιγραφή
primary-5ess	Μεταγωγείς AT&Τα (ΗΠΑ)
primary-dms100	NT (Nortel Northern Telecom) DMS-100 (Βόρεια Αμερική)
primary-ni1	National ISDN-1 (Βόρεια Αμερική)
primary-net5	Τύπος Μεταγωγέων για Net3 στο Ηνωμένο Βασίλειο, Ευρώπη και Αυστραλία
primary-ntt	Μεταγωγείς ISDN NTT (Ιαπωνία)

4.5.22 Πλάνο Ελέγχου Κλήσεων

Όταν ένας χρήστης τηλεφώνου θέλει να καλέσει ένα συγκεκριμένο προορισμό πληκτρολογεί πρώτα το νούμερο κλήσης και έπειτα περιμένει να ακούσει το συνομιλητή του. Ανάλογα με τον προορισμό, αλλάζει το σχήμα της αριθμοσειράς που πληκτρολογεί. Συγκεκριμένα για κλήσεις εσωτερικού πληκτρολογεί 10 ψηφία (area-code + subscriber-code), ενώ για διεθνείς κλήσεις πληκτρολογεί 14 ψηφία (00 + country-code + area-code + subscriber-code). Υπεύθυνο για τη μετάφραση και δρομολόγηση της κλήσης είναι το τηλεφωνικό κέντρο και πιο συγκεκριμένα το πλάνο ελέγχου κλήσεων που έχει διευθετηθεί στο εκάστοτε τηλεφωνικό κέντρο.

Το κλειδί για την υλοποίηση ενός πλάνου ελέγχου (dial plan) κλήσεων και την παροχή υπηρεσιών φωνής μέσω IP δικτύου είναι η διαμόρφωση dial peers. Τα dial peers χρησιμοποιούνται για την αναγνώριση των τελικών συσκευών πηγής και προορισμού καθώς και για τον καθορισμό των χαρακτηριστικών (π.χ. Voicecodec) που χρησιμοποιούνται σε κάθε σκέλος κλήσης (call leg) της σύνδεσης.

Εικόνα 4-36: Dial Peer - Call Legs



Ένα dial peer σχετίζεται με κάθε σκέλος κλήσης (call leg): Τα χαρακτηριστικά που δύναται να οριστούν μέσα σε κάθε dial peer ώστε να εφαρμοστούν σε κάθε call leg είναι ο codec, το QoS, το VAD και ο ρυθμός για υπηρεσία Fax. Ανάλογα με το σκέλος κλήσης κάθε κλήση μπορεί να προγραμματιστεί για δρομολόγηση με έναν από τους δυο ακόλουθους τρόπους:

1. **POTS-Dial Peer**, που καθορίζει τα χαρακτηριστικά μιας παραδοσιακής σύνδεσης με το δίκτυο τηλεφωνίας. Το Plain Old Telephone System - Dial Peer αντιστοιχίζει μια αριθμοσειρά σε μια συγκεκριμένη θύρα φωνής (voive port) του τοπικού δρομολογητή, όπου συνήθως συνδέεται στο τοπικό δίκτυο τηλεφωνίας ή σε ένα PBX ή σε ένα αναλογικό τηλέφωνο (FXS).

2. **VoIP-Dial Peer**, που καθορίζει τα χαρακτηριστικά μιας σύνδεσης μέσω του IP δικτύου. Το VoIP-Dial Peer αντιστοιχίζει μια αριθμοσειρά σε μια απομακρυσμένη συσκευή δικτύου, όπως ο δρομολογητής προορισμού που συνδέεται με την απομακρυσμένη τηλεφωνική συσκευή προορισμού.

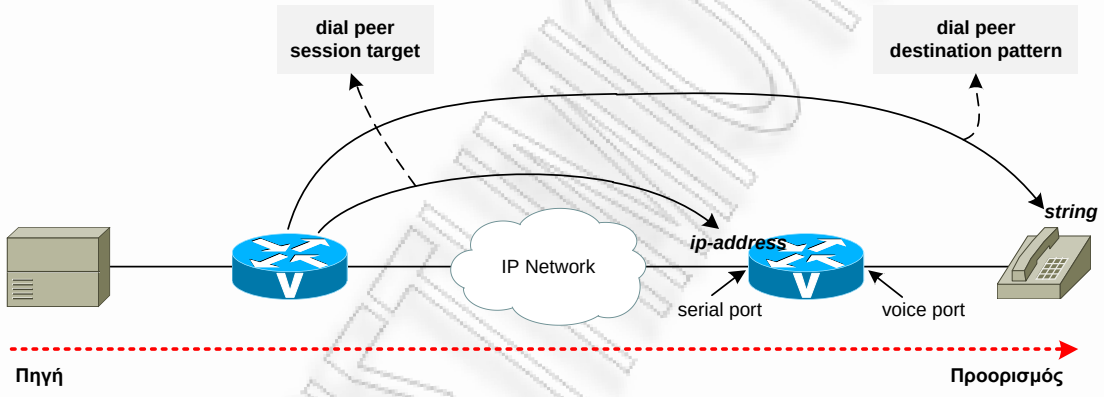
Session Target και Destination Pattern

Το session target (σύνοδος στόχου) είναι η IP διεύθυνση (ip-address) δικτύου του απομακρυσμένου δρομολογητή στον οποίο θέλουμε να αποσταλεί μια κλήση όταν συμφωνεί με ένα τοπικό dial peer. Δηλαδή αντιπροσωπεύει τη διαδρομή προς τον απομακρυσμένο δρομολογητή, στον οποίο είναι συνδεδεμένο το τηλέφωνο προορισμού. Εξ ορισμού, κάθε VoIP dial peer χρησιμοποιεί την εντολή διευθέτησης session target.

Για τα εξερχόμενα (outbound) dial peers, το destination pattern (σχήμα προορισμού) είναι ο αριθμός (*string*) της απομακρυσμένης τηλεφωνικής συσκευής που θέλουμε να καλέσουμε. Εξ ορισμού, κάθε POTS dial peer χρησιμοποιεί την εντολή διευθέτησης destination pattern.

Στην Εικόνα 4-37 παρουσιάζεται ο συσχετισμός μεταξύ session target και destination pattern.

Εικόνα 4-37: Συσχετισμός Μεταξύ Session Target και Destination Pattern



Διευθέτηση Dial Peer και Session Targets

Ο προγραμματισμός ενός session target υλοποιείται όπως παρακάτω:

Βήμα	Εντολή	Επεξήγηση
1	`Router(config)# dial-peer voice` *number* {**voip** | **vofr** | **voatm**} Παράδειγμα: `Router(config)# dial-peer voice 864 voip`	Εισαγωγή στην κατάσταση διαμόρφωσης dial peers και καθορισμός ενός voip dial peer (π.χ. με αριθμό 864). Αποδεκτές τιμές για την παράμετρο "*number*" 1 έως 2147483647.
2	`Router(config-dialpeer)# session-target ipv4:`*ip-address* Παράδειγμα: `Router(config-dialpeer)# session-target ipv4:10.45.44.43`	Καθορίζει την IP διεύθυνση του next-hop router δικτύου φωνής και τη συσχετίζει με το dial peer

Διευθέτηση Dial Peer και Destination Patterns

Ο προγραμματισμός ενός session target υλοποιείται όπως παρακάτω:

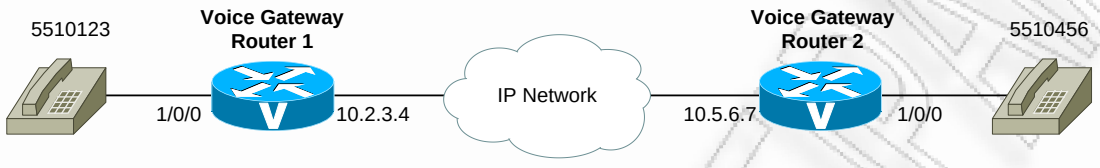
Βήμα	Εντολή	Επεξήγηση
1	Router(config)# **dial-peer voice** *number* **{pots | voip | vofr | voatm}** Παράδειγμα: Router(config)# dial-peer voice 123 voip	Εισαγωγή στην κατάσταση διαμόρφωσης dial peers και καθορισμός ενός voip dial peer (π.χ. με αριθμό 864). Αποδεκτές τιμές για την παράμετρο "*number*" 1 έως 2147483647.
2	Router(config-dialpeer)# **destination-pattern [+]** *string* **[T]** Παράδειγμα: Router(config-dialpeer)# destination-pattern 5510527	Ταιριάζει τα ψηφία του αριθμού που έχουν κληθεί και τα συσχετίζει με το dial peer. Το *string* μπορεί να είναι μια αριθμοσειρά με βάση το πρότυπο E.164. Το κεφαλαίο **T** συμβολίζει τον «interdigit timeout». Αν βρίσκεται στο τέλος της αριθμοσειράς τότε ο δρομολογητής συλλέγει τα ψηφία έως ότου λήξει το χρονικό περιθώριο που έχει καθοριστεί μεταξύ της πληκτρολόγησης των αριθμών (10 sec είναι το default) ή μέχρι να πληκτρολογηθεί ο χαρακτήρας τερματισμού (#).

Υπάρχουν και άλλοι παράμετροι που μπορούν να καθοριστούν μέσα στο dial peer, όπως για παράδειγμα οι:

Εντολή	Επεξήγηση
Router(config-dialpeer)# **forword-digits** {**num-digit | all |extra**}	Καθορίζει τη μέθοδο προώθησης των ψηφίων που θα χρησιμοποιήσει ο dial peer
Router(config-dialpeer)# **max-conn** *number*	Καθορίζει τις μέγιστες επιτρεπτές συνδέσεις από και προς τον dial peer
Router(config-dialpeer)# **preference** *value*	Καθορίζει το βαθμό προτεραιότητας. Όσο μικρότερη η τιμή value τόσο μεγαλύτερη η προτεραιότητα.
Router(config-dialpeer)# **prefix** *string*	Καθορίζει το πρόθεμα που θα βάλει μπροστά από την αριθμοσειρά το dial peer προτού το στείλει στην τηλεφωνική θύρα. Αποδεκτές τιμές για την παράμετρο *string:* 0-9 και το κόμμα (,) που εισάγει 1 sec καθυστέρηση.
Router(config-dialpeer)# **codec** { g711alaw | g711ulaw |g729br8 |…} [*bytes*]	Σε ένα voip dial peer, καθορίζει τον codec που θα χρησιμοποιηθεί για την κωδικοποίηση της φωνής. Η προαιρετική παράμετρος *bytes* καθορίζει το voice payload size.
Router(config-dialpeer)# **port** *string*	Σε ένα pots dial peer, καθορίζει τη θύρα φωνής. Π.χ. **port 1/0:0**

Παράδειγμα: Στη συνέχεια παρουσιάζεται ένα παράδειγμα διευθέτησης δρομολόγησης κλήσεων μεταξύ δυο αναλογικών τηλεφώνων που συνδέονται σε διαφορετικούς Voice Gateway Routers. Όλα τα πακέτα του ωφέλιμου φορτίου φωνής των VoIP κλήσεων που προσαρμόζονται με τα **dial-peer voice 10 voip** και **dial-peer voice 20 voip**, ορίζεται πως θα χαρακτηρίζονται με IP Precedence 5[17] και επιπλέων για την κωδικοποίηση θα χρησιμοποιείται ο g711ulaw codec.

Εικόνα 4-38: Παράδειγμα Δρομολόγησης Κλήσεων Μεταξύ Αναλογικών Τηλεφώνων



Διευθέτηση Voice Gateway Router 1	**Διευθέτηση Voice Gateway Router 2**
voice-port 1/0/0 ! dial-peer voice 1 pots destination-pattern 5510123 port 1/0/0 ! dial-peer voice 10 voip destination-pattern 5510456 session target ipv4:10.5.6.7 ip precedence 5 codec g711ulaw	voice-port 1/0/0 ! dial-peer voice 2 pots destination-pattern 5510456 port 1/0/0 ! dial-peer voice 20 voip destination-pattern 5510123 session target ipv4:10.2.3.4 ip precedence 5 codec g711ulaw

Το παραπάνω παράδειγμα μπορεί να μετατραπεί ώστε να υπάρχει η δυνατότητα χρήσης δυο codec φωνής. Σε κάθε codec δίνεται διαφορετικός βαθμός προτεραιότητας (preference).

Διευθέτηση Voice Gateway Router 1	**Διευθέτηση Voice Gateway Router 2**
voice class codec 1 codec preference 1 g729r8 codec preference 2 g711ulaw ! voice-port 1/0/0 ! voice-port 1/0/1 ! dial-peer voice 1 pots destination-pattern 5510123 port 1/0/0 ! dial-peer voice 2 voip destination-pattern 5510456 voice-class codec 1 session target ipv4:10.5.6.7 ip precedence 5	voice class codec 1 codec preference 1 g729r8 codec preference 2 g711ulaw ! voice-port 1/0/0 ! voice-port 1/0/1 ! dial-peer voice 1 pots destination-pattern 5510456 port 1/0/0 ! dial-peer voice 2 voip destination-pattern 5510123 voice-class codec 1 session target ipv4:10.2.3.4 ip precedence 5

[17] Μέθοδος Ταξινόμησης και Σήμανσης με τη χρήση Dial Peers.

Παράδειγμα: Ακολουθεί ένα παράδειγμα διευθέτησης για υποστήριξη επικοινωνίας συσκευών fax με χρήση του πρωτοκόλλου T.38.

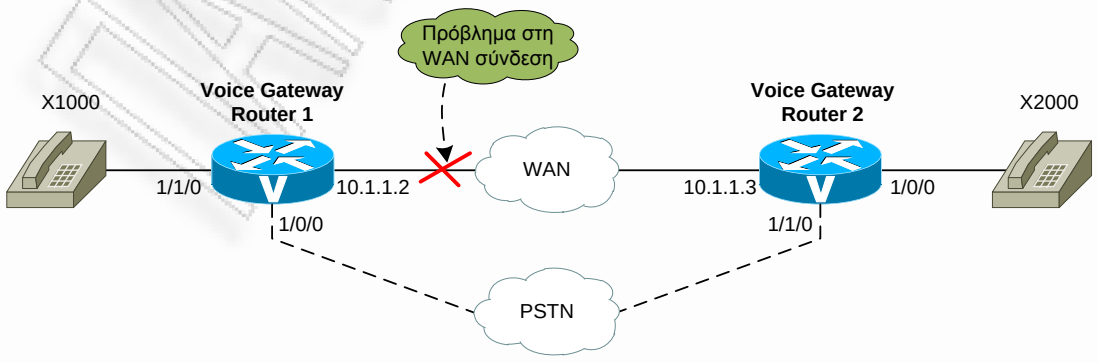
Εικόνα 4-39: Επικοινωνία Συσκευών Fax Μέσω T.38

Διευθέτηση Voice Gateway Router 1	Διευθέτηση Voice Gateway Router 2
voice-port 1/0/0 ! voice-port 1/0/1 ! dial-peer voice 1 pots destination-pattern 5510123 port 1/0/0 ! dial-peer voice 2 voip destination-pattern 5510456 session target ipv4:10.5.6.7 codec g711ulaw fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco fax rate voice	voice-port 1/0/0 ! voice-port 1/0/1 ! dial-peer voice 1 pots destination-pattern 5510456 port 1/0/0 ! dial-peer voice 2 voip destination-pattern 5510123 voice-class codec 1 session target ipv4:10.2.3.4 codec g711ulaw fax protocol t38 ls-redundancy 0 hs-redundancy 0 fax rate voice

Παράδειγμα: Υπάρχουν περιπτώσεις όπου οι κλήσεις πρέπει να αναδρομολογούνται αυτόματα μέσω μιας εναλλακτικής διαδρομής. Στο παράδειγμα της Εικόνα 4-40 παρουσιάζεται μια ανάλογη περίπτωση. Η κύρια WAN ζεύξη, μέσω της οποίας εξυπηρετείται όλη η κίνηση, ξαφνικά αντιμετωπίζει πρόβλημα και σταματά να λειτουργεί. Από το εσωτερικό τηλέφωνο 1000 που είναι συνδεδεμένο στον VGR1, πραγματοποιείται μια κλήση με προορισμό το εσωτερικό τηλέφωνο 2000 που συνδέεται στον VGR2. Η κλήση επειδή δεν μπορεί να εξυπηρετηθεί μέσω της WAN ζεύξης, όπου είναι η πρώτη επιλογή δρομολόγησης (preference 1), θα αναδρομολογηθεί αυτόματα μέσω του PSTN δικτύου (preference 2) με την ανάλογη χρέωση φυσικά. Πριν σταλεί η κλήση στη θύρα φωνής του PSTN, απαιτείται το εσωτερικό τετραψήφιο νούμερο να μετατραπεί στο εθνικό δεκαψήφιο ώστε το PSTN να μπορεί να το μεταφράσει σωστά και κατά επέκταση να το δρομολογήσει στο σωστό προορισμό.

Επίσης, πρέπει να προβλεφτεί και η αντίστροφη περίπτωση. Δηλαδή η μετατροπή σε εσωτερικό τετραψήφιο αριθμό (π.χ. 2000), της συμβολοσειράς που στέλνει το PSTN στον VGR που εξυπηρετεί το τηλέφωνο προορισμού (π.χ. 2105512000). Το δεκαψήφιο εθνικό νούμερο πρέπει να μετατρέπεται αυτόματα σε τετραψήφιο εσωτερικό ώστε ο VGR να το μεταφράσει σωστά και κατά επέκταση να το δρομολογήσει στο σωστό εσωτερικό.

Εικόνα 4-40: Αυτόματη Αναδρομολόγηση Κλήσεων Μέσω Εναλλακτικής Διαδρομής

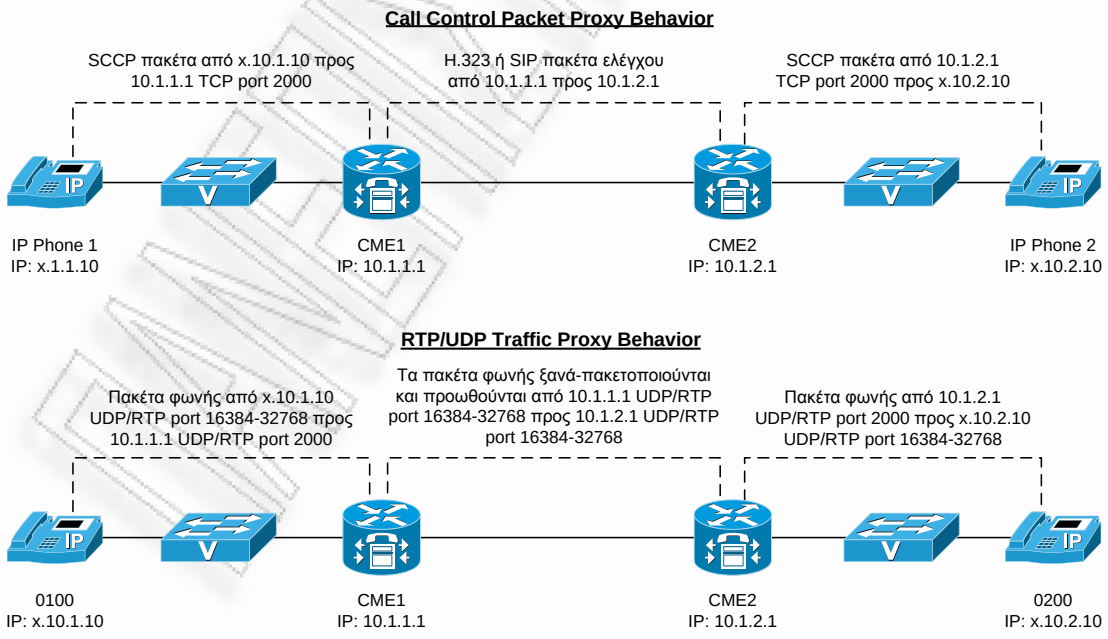


Στη συνέχεια παρουσιάζονται τα σχετικά αρχεία διευθέτησης για το παραπάνω σενάριο:

Διευθέτηση Voice Gateway Router 1	**Διευθέτηση Voice Gateway Router 2**
translation-rule 12 Rule 1 ^2 2105512 ! translation-rule 11 Rule 1 ^2105511 1 ! voice-port 1/0/0 translate called 11 ! voice-port 1/0/1 ! voice-port 1/1/0 ! voice-port 1/1/1 ! dial-peer cor custom ! dial-peer voice 1 pots destination-pattern 1000 port 1/1/0 ! dial-peer voice 2000 voip preference 1 destination-pattern 2000 session target ipv4:10.1.1.3 ! dial-peer voice 20 pots preference 2 destination-pattern 2000 translate-outgoing called 12 port 1/0/0 forward-digits all	translation-rule 11 Rule 1 ^1 2105511 ! translation-rule 12 Rule 1 ^2105512 2 ! voice-port 1/0/0 ! voice-port 1/0/1 ! voice-port 1/1/0 translate called 12 ! voice-port 1/1/1 ! dial-peer cor custom ! dial-peer voice 1 pots destination-pattern 2000 port 1/0/0 ! dial-peer voice 1000 voip preference 1 destination-pattern 1000 session target ipv4:10.1.1.2 ! dial-peer voice 10 pots preference 2 destination-pattern 1000 translate-outgoing called 11 port 1/1/0 forward-digits all

Παράδειγμα: Στην επόμενη εικόνα παρουσιάζεται μια απλή τοπολογία με δυο κόμβους και χρήση του H.323 πρωτοκόλλου. Όταν πραγματοποιείται μια κλήση μεταξύ δυο τηλεφώνων που δεν είναι εγγεγραμμένα στον ίδιο CME, ο τελευταίος θα πρέπει να αναγνωρίζει ότι το τηλέφωνο προορισμού δεν ανήκει σε αυτόν και εν συνεχεία να δρομολογεί την κλήση στο δεύτερο CME.

Εικόνα 4-41: Ροή VoIP Κλήσης Μεταξύ Δυο Cisco Unified CME



Στη συνέχεια ακολουθούν τα σχετικά αρχεία διευθέτησης του παραδείγματος:

Διευθέτηση CME1	**Διευθέτηση CME2**

`dial-peer voice 200 voip`
`  destination-pattern 02..`
`  session target 10.1.2.1`
`  dtmf-relay h245-alphanumeric`
`  codec g729r8`
`  no vad`
`telephony-service`
`ip source-address 10.1.1.1 port 2000`
	`dial-peer voice 100 voip`
	`  destination-pattern 01..`
	`  session target 10.1.1.1`
	`  dtmf-relay h245-alphanumeric`
	`  codec g729r8`
	`  no vad`
	`telephony-service`
	`ip source-address 10.1.2.1 port 2000`

Παράδειγμα: Όπως ήδη έχουμε αναφέρει, υπεύθυνος για την επεξεργασία και διαχείριση των κλήσεων στο δίκτυο είναι ο Call Manager. Επίσης στην παράγραφο 1.1.3 αναφερθήκαμε στα μοντέλα ανάπτυξης ενοποιημένων υπηρεσιών και είδαμε πως η επεξεργασία κλήσεων μπορεί να γίνεται είτε κεντρικά είτε κατανεμημένα με τη χρήση ξεχωριστού προγράμματος διαχείρισης κλήσεων σε κάθε LAN. Στο παράδειγμα της Εικόνας 4-42 επιλέγουμε η επεξεργασία να γίνεται κατανεμημένα από έναν τοπικό Call Manager Express (βλ. Πίνακας 4-1: Προσφερόμενες Εκδόσεις του Cisco Call Manager) κάθε υποδικτύου. Για την αποκατάσταση επικοινωνίας μεταξύ των CME χρησιμοποιείται το H.323[18] πρωτόκολλο σηματοδοσίας.

Στα πλαίσια του παραδείγματος, θεωρούμε ότι υπάρχουν τρία συνδεδεμένα υποκαταστήματα με τον κεντρικό κόμβο, των οποίων τα εσωτερικά τηλέφωνα λαμβάνουν αριθμοδότηση από συγκεκριμένο εύρος.

Πίνακας 4-4: Αριθμοδότηση Εσωτερικών Τηλεφώνων ανά CME

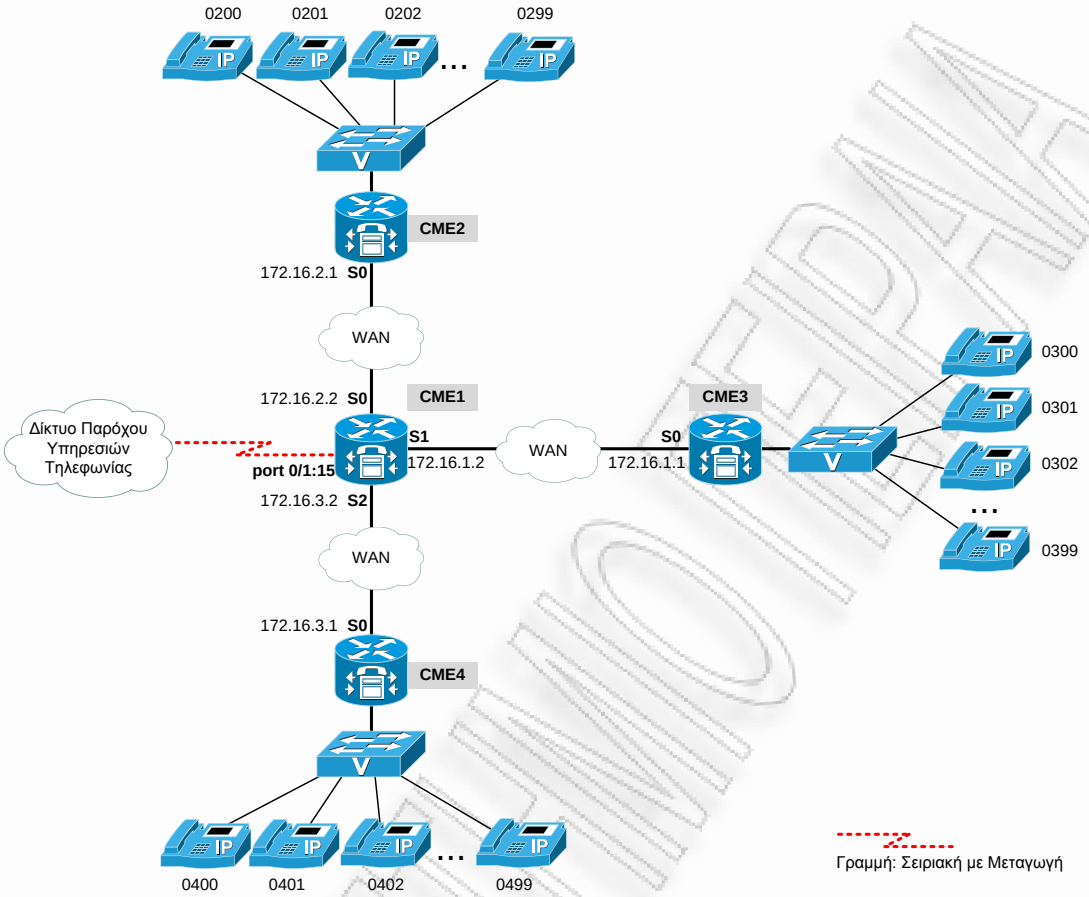
CME	Αριθμοδότηση
2	από 0200 έως 0299 (100 εσωτερικά νούμερα)
3	από 0300 έως 0399 (100 εσωτερικά νούμερα)
4	από 0400 έως 0499 (100 εσωτερικά νούμερα)

Επιπρόσθετα, η εταιρία μελετώντας τις παρούσες αλλά και μελλοντικές ανάγκες της, έχει ζητήσει και έχει πάρει από τον πάροχο τηλεφωνίας 1000 διεθνή νούμερα (E.164), από 2105510000 έως 2105510999.

Για τις εισερχόμενες κλήσεις ο πάροχος έχει ενημερώσει το διαχειριστή πως θα στέλνει τα τέσσερα τελευταία νούμερα του αριθμού. Π.χ. αν ένα μη εταιρικό τηλέφωνο καλέσει το 2105510280, ο πάροχος στέλνει το τετραψήφιο 0280, όπου ο CME1 μπορεί να το μεταφράσει και να το δρομολογήσει στον CME2 και αυτός με τη σειρά του στην εσωτερική τηλεφωνική συσκευή του χρήστη. Αν για κάποιο λόγο τα εσωτερικά νούμερα δε σχετίζονται με το δεκαψήφιο, όπως συμβαίνει στο παράδειγμά μας, τότε πρέπει να δημιουργηθούν πίνακες αντιστοίχισης. Π.χ. με την εντολή διευθέτησης: *num-exp 0280 5555*, επιτυγχάνεται η παραπάνω κλήση να κτυπάει στο εσωτερικό 5555 (για τα εσωτερικά νούμερα μπορούμε να επιλέξουμε αριθμοδότηση της αρεσκείας μας, αλλά πάντα προσπαθούμε να έχει μια λογική αντιστοιχία με το δεκαψήφιο ώστε να αποφεύγουμε όσο το δυνατόν τη χρήση πινάκων αντιστοίχισης).

[18] Τα dial peers χρησιμοποιούν εξ' ορισμού το H.323 signaling protocol. Υπάρχει η δυνατότητα διευθέτησης dial peers με χρήση και άλλων πρωτοκόλλων σηματοδοσίας όπως τα SIPv2 και MGCP.

Εικόνα 4-42: Πλάνο Ελέγχου Κλήσεων - Παράδειγμα



Απαιτείται να διευθετηθεί το πλάνο ελέγχου κλήσεων, έτσι ώστε:

- ✓ Να εξυπηρετούνται οι ενδοεταιρικές κλήσεις μεταξύ των sites της εταιρίας με χρήση του τετραψήφιου εσωτερικού αλλά και με χρήση του δεκαψήφιου (E.164).
- ✓ Να εξυπηρετούνται οι εξερχόμενες κλήσεις από όλα τα τηλέφωνα της εταιρίας προς όλους τους σταθερούς προορισμούς στην Ελλάδα (2xxxxxxxxx), ακόμα και αν πληκτρολογηθεί το πρόθεμα 0030 (00 + country-code).
- ✓ Για την κωδικοποίηση της φωνής πρέπει να χρησιμοποιηθούν οι codecs g729r8 και g711ulaw με την αντίστοιχη σειρά προτεραιότητας.

Στη συνέχεια ακολουθούν τα σχετικά αρχεία διευθέτησης του παραδείγματος[19]:

Διευθέτηση CME1

```
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
translation-rule 10
 Rule 1 ^2105510 0
!
voice service voip
 allow-connections h323 to h323
 dial-peer voice 200 voip
  destination-pattern 02..
  translate-outgoing called 10
  voice-class codec 1
  session target ipv4:172.16.2.1
!
 dial-peer voice 300 voip
  destination-pattern 03..
  translate-outgoing called 10
  voice-class codec 1
  session target ipv4:172.16.1.1
!
 dial-peer voice 400 voip
  destination-pattern 04..
  translate-outgoing called 10
  voice-class codec 1
  session target ipv4:172.16.3.1
!
 dial-peer voice 2 pots
  destination-pattern 2.........
  port 0/1:15
  forward-digits all
!
num-exp 00302......... 2.........
```

Διευθέτηση CME2

```
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
translation-rule 10
 Rule 1 ^2105510 0
!
dial-peer voice 300 voip
 destination-pattern 03..
 translate-outgoing called 10
 voice-class codec 1
 session target ipv4:172.16.1.2
!
dial-peer voice 400 voip
 destination-pattern 04..
 translate-outgoing called 10
 voice-class codec 1
 session target ipv4:172.16.1.2
!
dial-peer voice 2 voip
 destination-pattern 2.........
 voice-class codec 1
 session target ipv4:172.16.1.2
!
num-exp 00302......... 2.........
```

Διευθέτηση CME3

```
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
translation-rule 10
 Rule 1 ^2105510 0
!
dial-peer voice 200 voip
 destination-pattern 02..
 translate-outgoing called 10
 voice-class codec 1
 session target ipv4:172.16.1.2
!
dial-peer voice 400 voip
 destination-pattern 04..
 translate-outgoing called 10
 voice-class codec 1
 session target ipv4:172.16.1.2
!
dial-peer voice 2 voip
 destination-pattern 2.........
 voice-class codec 1
 session target ipv4:172.16.1.2
!
num-exp 00302......... 2.........
```

Διευθέτηση CME4

```
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
!
translation-rule 10
 Rule 1 ^2105510 0
!
dial-peer voice 300 voip
 destination-pattern 03..
 translate-outgoing called 10
 voice-class codec 1
 session target ipv4:172.16.3.2
!
dial-peer voice 200 voip
 destination-pattern 02..
 translate-outgoing called 10
 voice-class codec 1
 session target ipv4:172.16.3.2
!
dial-peer voice 2 voip
 destination-pattern 2.........
 voice-class codec 1
 session target ipv4:172.16.3.2
!
num-exp 00302......... 2.........
```

Μέσα από το γραφικό περιβάλλων διαχείρισης του Cisco Unified CallManager, δύναται να υλοποιηθούν Dial Plan επιλογές όπως AAR Group, Application Dial Rules, Route Filter, Translation Pattern, External Route Plan και Route Plan Report.

[19] Η τελεία (.) λειτουργεί ως «μπαλαντέρ» και συμβολίζει ένα οποιοδήποτε αριθμητικό ψηφίο από το 0 έως το 9.

Ο Ρόλος του H.323 Gatekeeper

Ο πρωταρχικός ρόλος ενός H.323 Gatekeeper, είναι να παράσχει μια αναζήτηση μετατροπής μεταξύ ενός τηλεφωνικού αριθμού και μιας IP διεύθυνσης. Στην ουσία, η υπηρεσία αυτή συγκεντρώνει το πλάνο ελέγχου σε ένα μόνο κεντρικό σημείο, αποφεύγοντας έτσι τη διαμόρφωση πλάνου ελέγχου σε κάθε κόμβο. Η χρήση ενός H.323 Gatekeeper διευκολύνει σημαντικά τη διαχείριση ενός μεγάλου δικτύου και επιπρόσθετα παρέχει υπηρεσίες CAC (Call Admission Control).

Συνεπώς τα dial peers του προηγούμενου παραδείγματος που εξυπηρετούν το πλάνο ελέγχου των ενδοεταιρικών κλήσεων, θα μετατραπούν ως εξής[20]:

Cisco Unified CME1

```
dial-peer voice 234 voip
   destination-pattern 0[234]..
   session target ras
   no vad
```

Cisco Unified CME2

```
dial-peer voice 34 voip
   destination-pattern 0[34]..
   session target ras
   no vad
```

Cisco Unified CME3

```
dial-peer voice 24 voip
   destination-pattern 0[24]..
   session target ras
   no vad
```

Cisco Unified CME4

```
dial-peer voice 23 voip
   destination-pattern 0[23]..
   session target ras
   no vad
```

Για να συνδεθεί και να συνεργάζεται π.χ. ο CME4 με έναν H.323 Gatekeeper που έχει IP διεύθυνση την 172.16.10.1, απαιτούνται οι ακόλουθες εντολές διαμόρφωσης στη σειριακή διεπαφή S0 του CME4:

```
CME4(config)# interface S0
CME4(config-if)# ip address 172.16.3.1 255.255.0.0
CME4(config-if)# h323-gateway voip interface
CME4(config-if)# h323-gateway voip id gk ipaddr 172.16.10.1 1719
CME4(config-if)# h323-gateway voip h323-id cme4
CME4(config-if)# h323-gateway voip tech-prefix 1#
CME4(config-if)# h323-gateway voip bind srcaddr 172.16.3.1
```

Από ένα VoIP dial peer, η αναφορά στον Gatekeeper πραγματοποιείται με τη βοήθεια του πρωτοκόλλου **ras** (μέσω της εντολής **session target ras**) και όχι με τη χρήση της IP διεύθυνσης (session target ipv4: *ip address*).

Στις περισσότερες περιπτώσεις, ο H.323 gatekeeper λαμβάνει την αντιστοιχία *Αριθμός τηλεφώνου-IP διεύθυνση,* μέσω ενός μηνύματος εγγραφής που αποστέλλει ο CME στον οποίο πραγματοποιείται η εγγραφή του τηλεφώνου. Ουσιαστικά το μήνυμα εγγραφής λέει: «*είμαι π.χ. ο h323-gateway voip h323-id cme4 και στην IP x.x.x.x έχω τον αριθμό τηλεφώνου Y*». Ο

[20] Το [ ] δηλώνει μια λίστα με εναλλακτικές τιμές, δηλαδή το 0[23].. δηλώνει 02.. , 03..

gatekeeper καταγράφει όλες αυτές τις πληροφορίες σε μια βάση δεδομένων η οποία περιέχει όλες τις τρέχουσες θέσεις όλων των τηλεφωνικών αριθμών στο δίκτυο.

Πίνακας 4-5: Αρίθμηση Θυρών στον Cisco Unified CME για VoIP Υπηρεσίες

Protocol	Port Numbers	Port Type
H.225 (call signaling)	1720	TCP
SIP	5060	UDP/TCP
RTP	16384 εως 32768	UDP (dynamic)
RTP (LAN)	2000	UDP
SCCP	2000	TCP
H.245	11000 εως 11999	TCP (dynamic)
H.225 RAS	1719	UDP
Unicast GK Discovery	1718	UDP
Multicast GK Discovery	223.0.1.4	UDP

5. Συμπεράσματα - Περίληψη

Στα πλαίσια αυτής της μεταπτυχιακής διατριβής αναπτύχτηκε η βασική μεθοδολογία για το σχεδιασμό και την υλοποίηση ενός ενοποιημένου δικτύου επικοινωνιών με έμφαση στη μετάδοση φωνής. Κατά την ανάπτυξη έγινε προσπάθεια, όπου ήταν δυνατόν, οι θεωρητικές αναφορές να ακολουθούνται από πρακτικά παραδείγματα υλοποίησης, έτσι ώστε να καταστεί ξεκάθαρη η αντίστοιχη φάση παραμετροποίησης.

Είναι σχεδόν σίγουρο πως αν το έργο αυτό υλοποιούνταν στην πράξη, θα προέκυπταν επιπλέον παράμετροι οι οποίες δεν ήταν δυνατόν να μας απασχολήσουν σε επίπεδο εργασίας. Τέτοια παραδείγματα είναι η λεπτομερής καταγραφή των πραγματικών αναγκών, η επιλογή κατάλληλα διαμορφωμένων και ασφαλών χώρων (computer room) για τη φιλοξενία του ενεργού εξοπλισμού, η χωροταξική και καλωδιακή δόμηση, το κόστος αγοράς του εξοπλισμού που μπορεί να αποδειχτεί απαγορευτικό για την εταιρία με αποτέλεσμα την ανατροπή όλου του πλάνου υλοποίησης και πιθανή τελικά προμήθεια εξοπλισμού χαμηλότερου κόστους και δυνατοτήτων κ.α.

Η βασική γραμμή λοιπόν για την υλοποίηση ενός ενοποιημένου δικτύου υπηρεσιών απαιτεί πρώτα και κύρια τη λεπτομερή καταγραφή των σημερινών αλλά και πιθανά μελλοντικών αναγκών. Μπορεί να ακούγεται εύκολη διαδικασία αλλά στην πράξη χρειάζεται μεγάλη προσοχή και προνοητικότητα διότι επηρεάζει τα επόμενα στάδια υλοποίησης και κατά συνέπεια το τελικό αποτέλεσμα.

Στη συνέχεια πρέπει να ακολουθήσει η διαστασιολόγηση και επιλογή των οντοτήτων του έργου βάσει των παραπάνω καταγεγραμμένων αναγκών. Η επιλογή των συσκευών πρέπει να γίνεται με βάση τόσο τον τύπο υπηρεσιών, που έχει επιλεγεί να υλοποιηθούν στο ενοποιημένο δίκτυο, όσο και με βάση τη μέγιστη διεκπεραιωτική ικανότητα που απαιτείται να έχουν αυτές ώστε να παρέχουν αδιάλειπτα και χωρίς προβληματισμό υπηρεσίες. Επιπρόσθετα απαιτείται ο υπολογισμός του μέγιστου φορτίου κίνησης που πρέπει να εξυπηρετείται από τις γραμμές μεταφοράς του IP δικτύου, ώστε να προσφέρεται ο μέγιστος ή ο προκαθορισμένα αποδεκτός βαθμός εξυπηρέτησης.

Πολύ σημαντική, όσον αφορά την εγγυημένη διαθεσιμότητα, την ασφάλεια και το κόστος, είναι η επιλογή των WAN ζεύξεων μέσω των οποίων επικοινωνούν τα απομακρυσμένα σημεία της εταιρίας. Οι μισθωμένες γραμμές παρέχουν υψηλή ασφάλεια και εγγυημένη διαθεσιμότητα αλλά με μεγάλο κόστος συντήρησης. Αντίθετα η επιλογή σύνδεσης μέσω Internet είναι φτηνή αλλά όχι τόσο ασφαλής. Βεβαίως έχουν αναπτυχτεί τεχνικές, όπως η δημιουργία IPsec VPNs, μέσω των οποίων επιτυγχάνεται ο διαχωρισμός του δικτύου και το απόρρητο μέσω της κρυπτογράφησης. Τα IPsec VPNs που δημιουργούνται μέσω του Internet καλύπτουν από σημείο προς σημείο την ασφαλή επικοινωνία παρέχοντας έτσι μεγαλύτερο επίπεδο ασφάλειας.

Η σύγκλιση των δικτύων επέφερε επιπρόσθετες ανάγκες σε εύρος ζώνης και γενικά σε πόρους. Όμως τα δίκτυα διαθέτουν πεπερασμένο σύνολο πόρων, όσον αφορά το εύρος ζώνης, το πλήθος των πακέτων που μπορούν να εξυπηρετήσουν καθώς και την ταχύτητα εξυπηρέτησης. Για το λόγο αυτό κρίνεται αναγκαία η ύπαρξη μηχανισμών υπεύθυνων για τη διαχείριση των πόρων και την εξασφάλιση υψηλού επιπέδου υπηρεσιών προκειμένου να επιτρέπεται η συνύπαρξη πολλών εφαρμογών.

Όμως, όπως έχουμε αναφέρει, κάθε εφαρμογή έχει διαφορετικές απαιτήσεις και ως εκ τούτου πρέπει να αντιμετωπίζεται με διαφορετικό τρόπο. Για παράδειγμα οι εφαρμογές πραγματικού χρόνου, όπως είναι η IP τηλεφωνία, κρίνονται πολύ ευαίσθητες στις καθυστερήσεις μετάδοσης, ενώ υπάρχουν εφαρμογές όπως η μεταφορά ενός αρχείου μέσω FTP σύνδεσης, όπου δεν παρουσιάζουν τόση μεγάλη ευαισθησία στον παράγοντα καθυστέρηση. Συνεπώς, όταν το δίκτυο δεν μπορεί να αναγνωρίσει τον τύπο της εφαρμογής και κατά συνέπεια τις απαιτήσεις της, θα αντιμετωπίζει όλες τις εφαρμογές με ίδιο και όχι με διαφοροποιημένο τρόπο. Αυτό ενδέχεται να προκαλέσει κακή ποιότητα στη μετάδοση δεδομένων εφαρμογών πραγματικού χρόνου και γενικά μη αποδεκτές υπηρεσίες. Συνεπώς το

δίκτυο πρέπει να έχει την «ευφυΐα» να μπορεί να προσδιορίζει τις ανάγκες κάθε εφαρμογής, ώστε να παρέχει αντίστοιχα τις κατάλληλες διαφοροποιημένες υπηρεσίες.

Η «ευφυΐα» έρχεται μέσα από την υλοποίηση μηχανισμών Ποιότητας Υπηρεσίας. Το QoS είναι ένα σύνολο δυνατοτήτων που έχουν σχεδιαστεί με σκοπό την εξασφάλιση της αξιόπιστης και έγκαιρης παράδοσης των «ευαίσθητων» στην καθυστέρηση πακέτων «πραγματικού χρόνου» μέσω ενός IP δικτύου. Όμως για να λαμβάνουν τα κρίσιμα πακέτα προνομιακή μεταχείριση, πρέπει να κατέχουν ένα «εισιτήριο προνομιακής θέσης» που θα υποδεικνύει τον απαιτούμενο βαθμό εξυπηρέτησης.

Ο χαρακτηρισμός των πακέτων μπορεί να γίνει σε διάφορα σημεία του δικτύου από συσκευές Layer-2 (CoS) ή Layer-3 (DSCP, IPP, PHB) καθώς και από τις τελικές συσκευές αν το υποστηρίζουν. Αφού λοιπόν το πακέτο έχει λάβει QoS χαρακτηρισμό, ο μηχανισμός αστυνόμευσης καθορίζει κατά πόσο αυτό ανήκει σε μια κατηγορία κίνησης και έπειτα εφαρμόζονται στο πακέτο οι δράσεις που προβλέπει η προκαθορισμένη πολιτική για αυτή την κατηγορία. Εν συνεχεία τα πακέτα τοποθετούνται στην κατάλληλη ουρά αναμονής και αποστέλλονται βάσει του αλγόριθμου προγραμματισμού εκπομπής πακέτων.

Ο σύγχρονος τρόπος προγραμματισμού και διαχείρισης ενός δικτύου απαιτεί τη χρήση Virtual LANs. Τα VLANs αποτελούν μία ριζική αλλαγή στον τρόπο με τον οποίο σχεδιάζονται και διαχειρίζονται τα παραδοσιακά LAN καθώς δίνουν λύση σε προβλήματα που σχετίζονται με μετακινήσεις, προσθέσεις και αλλαγές χρηστών στο δίκτυο, συμβάλλουν στη διαχείριση, την ασφάλεια, τον έλεγχο, και την καλύτερη κατανομή των πόρων του δικτύου. Ως εκ τούτου, σε ένα δίκτυο ενοποιημένων υπηρεσιών είναι απαραίτητη η δημιουργία Data και Voice VLANs. Ο παραπάνω διαχωρισμός σε συνδυασμό με τη χρήση λιστών πρόσβασης (ACLs), είναι μια δεύτερη μέθοδος κατηγοριοποίησης της κίνησης.

Υπάρχουν QoS μηχανισμοί που εφαρμόζονται σε ένα τοπικό δίκτυο καθώς και επιπρόσθετοι μηχανισμοί που έχουν σχεδιαστεί να υλοποιούνται σε δίκτυα ευρείας περιοχής όπως π.χ. σε ζεύξεις που συνδέουν απομακρυσμένα σημεία του δικτύου και είναι χαμηλού εύρους ζώνης. Το σύνολο δυνατοτήτων του QoS περιλαμβάνει, μηχανισμούς διαχείρισης του παρεχόμενου από το δίκτυο εύρους ζώνης, τον καθορισμό προτεραιότητας πακέτων καθώς και αλγόριθμους προγραμματισμού εκπομπής πακέτων. Επιπλέον παρέχει προστασία στο δίκτυο μετριάζοντας την επίδραση DoS επιθέσεων που προκαλούν τα λογισμικά σκουληκιών. Τέλος είναι σημαντικό να διευκρινιστεί, πως το QoS δε δύναται να δώσει λύσεις σε όλα τα προβλήματα. Για παράδειγμα, δεν είναι σχεδιασμένο να αντιμετωπίζει ένα λάθος υλοποιημένο δίκτυο με ελάχιστους πόρους ή την αδυναμία μιας εφαρμογής να υποστηρίζει QoS τεχνικές.

Ανάλογα με το επιλεγμένο μοντέλο ανάπτυξης, η επεξεργασία των κλήσεων μπορεί να πραγματοποιείται είτε συγκεντρωτικά είτε κατανεμημένα. Στη πρώτη περίπτωση απαιτείται η ύπαρξη ενός μόνο Call Manager, ενώ στη δεύτερη συνήθως εγκαθίσταται ένας Call Manager Express σε κάθε σταθμότοπο. Παρόλα αυτά, συνολικά ο εξοπλισμός και οι πόροι του δικτύου λειτουργούν σαν ένα ενιαίο σύστημα. Η δρομολόγηση των κλήσεων πραγματοποιείται μέσω του IP WAN της εταιρίας, με εξαίρεση περιπτώσεις πιθανής βλάβης ή φόρτου του εταιρικού δικτύου όπου τότε οι κλήσεις εξυπηρετούνται μέσω του PSTN δικτύου.

Το λογισμικό διαχείρισης κλήσεων, πέρα από την παροχή συνδεσιμότητας, σηματοδοσίας και ελέγχου συσκευών, εκτελεί λειτουργίες διαχείρισης, συντήρησης και μέριμνας για το δίκτυο. Στις ενοποιημένες υπηρεσίες αυτός που παρέχει Call Admission Control υπηρεσίες είναι ο Call Manager. Ως εκ τούτου όταν γίνεται προσπάθεια επικοινωνίας μεταξύ δυο συσκευών που δε βρίσκονται στο ίδιο υποκατάστημα, ο Call Manager πρώτα ελέγχει αν υπάρχει το απαιτούμενο εύρος ζώνης στη WAN ζεύξη, η οποία πρόκειται να εξυπηρετήσει την κλήση και αν υπάρχει, τότε και μόνο δρομολογεί την κλήση μέσω αυτής. Σε διαφορετική περίπτωση συνδυαστικά με το dial plan της εταιρίας ίσως να αναδρομολογήσει την κλήση μέσω του PSTN δικτύου με την ανάλογη φυσικά χρέωση. Επομένως είναι σημαντικό οι λειτουργίες CAC και το dial plan να συνεργάζονται άριστα ώστε να επιτυγχάνεται η βέλτιστη δρομολόγηση των κλήσεων μέσα στο δίκτυο.

Στην ενότητα 1.1.2 αναφερθήκαμε στα τέσσερα βασικά επίπεδα τα οποία συνθέτουν ένα δίκτυο ενοποιημένων επικοινωνιών. Έως τώρα, ουσιαστικά, έχουμε επικεντρωθεί στην ανάλυση και υλοποίηση των δυο πρώτων επιπέδων, δηλαδή στα Επίπεδα Υποδομής και Επεξεργασίας Κλήσεων. Τα επίπεδα αυτά είναι η βάση πάνω στην οποία υλοποιούνται τα Επίπεδα Εφαρμογών και Πελάτη.

Για να μπορεί μια επιχείρηση να λειτουργεί και να αναπτύσσεται, οι υπάλληλοι πρέπει να έχουν τη δυνατότητα να επικοινωνούν με άλλους υπαλλήλους, προμηθευτές, πελάτες και άλλες επιχειρήσεις μέσω ενός ετερογενούς συνόλου μέσων επικοινωνίας, στο οποίο περιλαμβάνονται:

- ✓ Φωνή
- ✓ Φωνή μέσω φορητών συσκευών
- ✓ Φωνητικό ταχυδρομείο
- ✓ Ηλεκτρονικό ταχυδρομείο
- ✓ Συνδιασκέψεις
- ✓ Βίντεοδιασκέψεις
- ✓ Συνδιασκέψεις μέσω του ιστού
- ✓ Ανταλλαγή άμεσων μηνυμάτων, κ.α.

Πρέπει να υπάρχει δυνατότητα επικοινωνίας ανεξάρτητα από το αν οι υπάλληλοι βρίσκονται στο δικό τους ή κάποιο άλλο γραφείο, στο δρόμο ή στο σπίτι. Όταν δεν παρέχεται μια ολοκληρωμένη λύση οι διάφορες μορφές επικοινωνίας μπορεί να αποδειχθούν ανεπαρκείς. Αυτή η αναποτελεσματικότητα μπορεί να οδηγήσει σε μειωμένη παραγωγικότητα, πιο δαπανηρές επιχειρηματικές συναλλαγές και χαμένες ευκαιρίες.

Η λύση των ενοποιημένων επικοινωνιών παρέχει ένα σύνολο υπηρεσιών επικοινωνίας οι οποίες, όταν ενσωματώνονται στο κατάλληλο σύστημα, επιτρέπουν την απρόσκοπτη σύνδεση διαφορετικών τύπων επικοινωνίας. Το σύστημα δίνει τη δυνατότητα στους υπαλλήλους να χρησιμοποιούν αυτά τα εργαλεία από ένα γραφείο, το σπίτι ή ακόμα και ταξιδεύοντας. Βελτιώνει τις πιθανότητες επαφής με άλλα άτομα, μειώνοντας τις αποτυχημένες προσπάθειες επικοινωνίας. Για παράδειγμα, μέσα από τα προγράμματα τηλεπαρουσίας και ανταλλαγής άμεσων μηνυμάτων, μπορούμε να διαπιστώσουμε αν κάποιος είναι διαθέσιμος, να δούμε το προτεινόμενο ή το τρέχον μέσο επικοινωνίας του και να τον καλέσουμε.

Επιπλέον οι χρήστες μπορούν να ειδοποιούνται για εισερχόμενες κλήσεις μέσω αναδυόμενων μηνυμάτων, ενώ με την ενσωμάτωση του εταιρικού καταλόγου και ενός CRM συστήματος έχουν ολοκληρωμένη πληροφόρηση για αυτόν που τους καλεί. Η χρήση μιας μόνο θέσης «εισερχομένων» για κάθε είδους επικοινωνία, επιτρέπει στους χρήστες να εξετάζουν εύκολα το ιστορικό και να απαντούν με έναν από τους πολλούς τρόπους επικοινωνίας.

Ως εκ τούτου, για την ολοκλήρωση ενός συστήματος ενοποιημένων επικοινωνιών η μελλοντική υλοποίηση των επιπέδων Εφαρμογών και Πελάτη κρίνεται απαραίτητη. Ο Cisco Unified Call Manager (CUCM) έχει ένα εξελιγμένο και αξιόπιστο γραφικό περιβάλλον μέσω του οποίου μπορεί να πραγματοποιηθεί η διαδικασία προσθήκης και παραμετροποίησης των νέων συσκευών καθώς και η υλοποίηση ενός ετερογενούς συνόλου μέσων επικοινωνίας.

Παράρτημα Α

Portable Product Sheets – Routing Performance

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
801,805	1,000			0.51	15-Apr-07
806			7,000	3.58	30-Apr-04
830			8,500	4.35	5-Jul-06
850			10,000	5.12	No
860			25,000	12.80	No
870			25,000	12.80	No
880			50,000	25.60	No
890			100,000	51.20	No
14xx	600	0.3072	4,000	2.05	31-Aug-00
160x(-R)	600	0.3072	4,000	2.05	28-Feb-03
1701	1,700	0.8704	12,000	6.14	27-Mar-07
1710	1,300	0.6656	7,000	3.58	30-Jul-04
1711-1712	1,700	0.8704	13,500	6.91	27-Mar-07
1720	1,400	0.7168	8,500	4.35	1-Aug-03
1721	1,700	0.8704	12,000	6.14	27-Mar-07
1750	1,400	0.7168	8,500	4.35	31-May-02
1751	1,500	0.768	12,000	6.14	27-Mar-07
1760	1,700	0.8704	16,00	8.19	27-Mar-07
ISR 1801-1812			70,000	35.84	No
ISR 1841			75,000	38.40	No
ISR 1861			146,142	74.82	No
ISR G2 1941			299,000	153.08	No
2500	800	0.4096	4,400	2.25	30-Apr-02
261X	1,500	0.768	15,000	7.68	26-Apr-03

[25]

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
262X	1,500	0.768	25,000	12.80	26-Apr-03
265X	2,000	1.024	37,000	18.94	26-Apr-03
261X(XM)	1,500	0.768	20,000	10.24	27-Mar-07
262X(XM)	1,500	0.768	30,000	15.36	27-Mar-07
265X(XM)	2,000	1.024	40,000	20.48	27-Mar-07
2691	7,400	3.7888	70,000	35.84	27-Mar-07
ISR 2801	3,000	1.536	90,000	46.08	No
ISR 2811	3,000	1.536	120,000	61.44	No
ISR 2821	11,500	5.888	170,000	87.04	No
ISR 2851	15,000	7.68	220,000	112.64	No
3620	2,000	1.024	20,000 – 40,000	10 - 20	31-Dec-03
ISR G2 2901			327,000	167.42	No
ISR G2 2911			353,000	180.73	No
ISR G2 2921			480,000	245.76	No
ISR G2 2951			580,000	296.96	No
3640/3640A	4,000	2.048	50,000 – 70,000	25.6 – 36	31-Dec-03
3660	12,000	6.144	100 - 120,000	51.2 – 61.4	31-Dec-03
3631	4,000	2.048	50 – 70,000	25.6 – 36	2-Aug-04
3725			100 – 120,000	51.2 – 61.4	27-Mar-07
3745			225 – 250,000	115.2 – 128	27-Mar-07
MC3810	2,000	1.024	8,000	4.10	14-Dec-01
MC3810-V3	3,000	1.536	15,000	7.68	13-Dec-02
ISR 3825	25,000	12.8	350,000	179.20	No
ISR 3845	35,000	17.92	500,000	256.00	No
ISR G2 3925			833,000	426.49	No
ISR G2 3945			982,000	502.78	No
IAD2400	3,000	1.536	15,000	7.68	No
4000	1,800	0.9216	14,000	7.17	10-Jul-98
4500	3,500	1.792	45,000	23.04	25-Nov-00
4700	4,600	2.3552	75,000	38.40	25-Nov-00
7120	13,000	6.656	175,000	89.60	30-Nov-01
7140	20,000	10.24	300,000	153.60	30-Nov-01
7200-NPE100	7,000	3.584	100,000	51.20	30-Apr-00
7200-NPE150	10,000	5.12	150,000	76.80	30-Apr-00
7200-NPE175	9,000	4.608	177,848	91.06	15-Jul-00
7200-NPE200	13,000	6.656	200,000	102.40	1-Jan-02
7200-NPE225	13,000	6.656	233,170	119.38	23-Jul-07
7200-NPE300	20,000	10.24	353,000	180.74	31-Dec-01
7200-NPE400	20,000	10.24	420,000	215.04	No
7200-NPE-G1	79,000	40.448	1,018,000	521.22	No
7200-NPE-G2			2,000,000	1,024.00	No
7200-NSE-1	20,000	10.24	300,000(RP)	153.6	2-Mar-04
7304-NSE-100			3,500,000(PXF) 450,000(RP)	1,792 230.4	31-Mar-08

[25]

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
7304-NSE-150			3,500,000(PXF) 800,000(RP)	1,792 409.6	No
7304-NPE-G100			1,099,000	562.69	No
7301	79,000	40.448	1,018,000	521.22	No
7401	20,000	10.24	300,000 (Also has PXF)	153.6	30-Dec-04
7000-RP	2,500	1.28	30,000	15.36	31-Jul-97
7500-RSP2	5,000	2.56	220,000	112.64	16-Feb-03
7500-RSP4/4+	8,000	4.096	345,000	176.64	15-Dec-07
7500-RSP8	22,000	11.264	470,000	240.64	15-Dec-07
7500-RSP16	29,000	14.848	530,000	271.36	15-Dec-07
7500-VIP2/40	Punts to RSP[1]		60,000 – 95,000	30.7 – 48.6	30-Apr-04
7500-VIP2/50	Punts to RSP[1]		90,000 – 140,000	46.1 – 71.7	15-May-03
7500-VIP4/50	Punts to RSP[1]		90,000 – 140,000	46.1 – 71.7	15-Dec-07
7500-VIP4/80	Punts to RSP[1]		140,000 – 210,000	71.7 – 107.5	15-Dec-07
7500-VIP6/80	Punts to RSP[1]		140,000 – 219,000	71.7 – 112.1	15-Dec-07
7600-MSFC2(Sup2)	20,000 (500,000 for software-switched CEF)	10.24 (256.00)	30,000,000 for central forwarding of non-DFC traffic - 15,000,000 for central forwarding on non-DFC traffic with classic line cards[2]	15,360.00 or 7,680.00	1-Mar-07
7600-MSFC2A(Sup32)			15,000,000[2]	7,680.00	No
7600-MSFC3(Sup720)	20,000 (500,000 for software switched CEF)	10.24 (256.00)	30,000,000 for central forwarding of non-DFC traffic – 15,000,000 for central forwarding on non-DFC traffic with classic line cards[2]	15,360.00 or 7,680.00	No
7600-CEF256			15,000,000 per slot[2]	7,680.00	No
7600-dCEF256 (6816)			24,000,000 per slot[2]	12,288.00	No
7600-dCEF720(6724)			24,000,000 per slot[2]	12,288.00	No
7600-dCEF720(67xx)			48,000,000 per slot[2]	24,576.00	No
(ASR1002-F)-ESP2.5			4,420,000	2,263.04	No
ASR1000-ESP5			8,840,000	4,526.08	No
ASR1000-ESP10			17,690,000	9,057.28	No
ASR1000-ESP20			25,430,000	13,020.16	No
10000-PRE1			2,800,000 (Also has 2xPXF)	1,433.60	17-Aug-06
10000-PRE2			6,200,000 (Also has a 4xPXF)	3,174.40	1-Jan-10
10000-PRE3			9,500,000 (Also has a 4xPXF)	4,864.00	No
10000-PRE4			10,000,000(Also has a 4xPXF)	5,120.00	No
10720	50,000	25.6	2,000,000 (Also has a 2xPXF)	1,024.00	No
12000 (Engine 0)			400,000	622.00	No
12000 (Engine 1)			700,000	2,500.00	No
12000 (Engine 2)			4,000,000	2,500.00	No
12000 (Engine 3)			4,000,000	2,500.00	No
12000 (Engine 4/4+)			25,000,000	10,000.00	No

[25]

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
12000 (Engine 5)			16,000,000	10,000.00	No
12000 (Engine 6)			50,000,000	20,000.00	No
CRS-1 LC			80,000,000	40,960.00	No

[25]

Cisco Integrated Services Routers Generation 2

	Cisco 3945E	Cisco 3925E	Cisco 3945	Cisco 3925	Cisco 2951	Cisco 2921	Cisco 2911	Cisco 2901	Cisco 1941 and 1941W	Cisco 1921
Form Factor	3 rack units (3RU)	3RU	3RU	3RU	2RU	2RU	2RU	1RU	2RU	1RU
Integrated WAN Ports	4 GE(2 SFP)	4 GE (2 SFP)	3 GE (2 SFP)	3 GE (2 SFP)	3 GE (1 SFP)	3 GE (1 SFP)	3 GE	2 GE	2 GE	2 GE
Interface Slots (EHWIC)	3	3	4	4	4	4	4	4	2	2
Service Module Slots	4	2	4	2	2	1	1	0	0	0
ISM Slots	0	0	1	1	1	1	1	1	1	0
PVDM Slots	3	3	4	4	3	3	2	2	0	0
USB Ports (v2.0)	2	2	2	2	2	2	2	2	2	1
Default/Max Flash	256MB/4GB	256 MB/4GB	256 MB/4 GB	256 MB/4 GB	256 MB/4 GB	256 MB/4 GB	256 MB/4 GB	256 MB/4 GB		256 MB/256 MB
Default/Max SDRAM	1 GB/4 GB**	1 GB/4 GB**	1 GB/4 GB**	1 GB/4 GB**	512 MB/2.5 GB	512 MB/2.5 GB	512 MB/2.5 GB			512MB/512MB
Modular LAN Switchports (with optional POE)	98*	74 *	98*	74 *	50*	50*	24*	16*	11*	9*
Advanced Security	**Enabled via Security License for Universal IOS Image. IPS and Content Filtering needs additional subscription licenses**									
Stateful Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Onboard Hardware VPN Acceleration (DES, 3DES, AES)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intrusion prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Content filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Unified Communication	**Enabled via Unified Communications License for Universal IOS Image. CCME/SRST support through separate feature licenses**									
Local conferencing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	–	–
Voice and Video DSP support	PVDM3 and PVDM2	PVDM3 and PVDM2	PVDM3 and PVDM2	PVDM3 and PVDM2	PVDM3 and PVDM2	PVDM3 and PVDM2	PVDM3 and PVDM2	PVDM3 and PVDM2	–	–
Survivable Remote Site Telephony (SRST)	Up to 1500	Up to 1350	Up to 1200	Up to 730	Up to 250	Up to 100	Up to 50	Up to 35	–	–
Cisco Unified Communications Manager Express	Up to 450	Up to 400	Up to 350***	Up to 250***	Up to 150	Up to 100	Up to 50	Up to 35	–	–
Cisco Unity™ Express (network module [NM], service module [SM], or ISM)	32 ports; 500 mailboxes	32 ports; 500 mailboxes	32 ports; 500 mailboxes	32 ports; 500 mailboxes	32 ports; 500 mailboxes	32 ports; 500 mailboxes	32 ports; 500 mailboxes	10 ports; 100 mailboxes	–	–
Session Initiartion Protocol (SIP) sessions	2500	2000	1000	800	600	400	200	100	–	–
Digital voice support	Up to 660	Up to 420	Up to 720	Up to 480	Up to 400	Up to 240	Up to 150	Up to 100	–	–
Maximum voice support for analog and Basic Rate Interface (BRI)	Foreign exchange station (FXS): 108 Foreign exchange office (FXO): 60 BRI: 38	FXS: 60 FXO: 36 BRI: 22	FXS: 112 FXO: 64 BRI: 40	FXS: 64 FXO: 40 BRI: 24	FXS 40 FXO 28 BRI 16	FXS: 40 FXO: 28 BRI: 16	FXS: 40 FXO: 28 BRI: 16	FXS: 16 FXO: 16 BRI: 8	–	–

*LAN Switching counts for the Cisco 2911 through Cisco 3945 and Cisco 3945E routers based on latest generation of switch service modules
** Up to 2 GB available for use; upgrade to 4 GB available in future
*** Scales to documented phone support in 15.0.1 rebuild

[52]

Παράρτημα Β

Erlang B Traffic Model

Circuits	Grade of Service													
	0.001	0.002	0.003	0.004	0.005	0.01	0.02	0.03	0.04	0.05	0.1	0.2	0.3	0.4
21	10.1071	10.7922	11.2383	11.5792	11.8586	12.8366	14.0350	14.8835	15.5782	16.1858	18.6493	22.8457	27.3164	32.7920
22	10.8120	11.5250	11.9883	12.3428	12.6342	13.6506	14.8940	15.7776	16.5000	17.1311	19.6904	24.0625	28.7246	34.4609
23	11.5239	12.2644	12.7459	13.1130	13.4162	14.4691	15.7592	16.6744	17.4241	18.0782	20.7343	25.2798	30.1426	36.1172
24	12.2432	13.0107	13.5088	13.8896	14.2031	15.2944	16.6289	17.5752	18.3516	19.0283	21.7793	26.4961	31.5469	37.7578
25	12.9684	13.7627	14.2792	14.6729	14.9963	16.1240	17.5034	18.4814	19.2841	19.9829	22.8302	27.7100	32.9590	39.4287
26	13.6998	14.5211	15.0535	15.4597	15.7946	16.9578	18.3812	19.3921	20.2173	20.9409	23.8799	28.9326	34.3789	41.0820
27	14.4377	15.2847	15.8335	16.2537	16.5965	17.7962	19.2645	20.3027	21.1564	21.9012	24.9368	30.1641	35.7935	42.7412
28	15.1809	16.0533	16.6199	17.0505	17.4043	18.6399	20.1489	21.2188	22.0972	22.8662	25.9902	31.3838	37.2012	44.4063
29	15.9302	16.8276	17.4090	17.8524	18.2170	19.4861	21.0385	22.1394	23.0421	23.8315	27.0494	32.6108	38.6289	46.0488
30	16.6827	17.6056	18.2025	18.6584	19.0338	20.3357	21.9305	23.0603	23.9868	24.7998	28.1104	33.8379	40.0342	47.7246
31	17.4413	18.3873	19.0023	19.4696	19.8537	21.1895	22.8262	23.9841	24.9377	25.7703	29.1685	35.0566	41.4443	49.3760
32	18.2041	19.1748	19.8037	20.2832	20.6768	22.0469	23.7227	24.9141	25.8887	26.7422	30.2344	36.2891	42.8750	51.0313
33	18.9714	19.9654	20.6099	21.1003	21.5032	22.9070	24.6251	25.8417	26.8407	27.7189	31.3000	37.5198	44.2793	52.6904
34	19.7413	20.7603	21.4202	21.9224	22.3353	23.7714	25.5291	26.7742	27.7993	28.6958	32.3647	38.7480	45.7041	54.3535
35	20.5164	21.5588	22.2328	22.7466	23.1685	24.6371	26.4337	27.7090	28.7579	29.6765	33.4277	39.9731	47.1338	56.0205
36	21.2959	22.3594	23.0493	23.5745	24.0051	25.5059	27.3428	28.6436	29.7158	30.6563	34.4971	41.2031	48.5508	57.6914
37	22.0771	23.1645	23.8680	24.4055	24.8458	26.3770	28.2513	29.5837	30.6768	31.6388	35.5682	42.4380	49.9717	59.3301
38	22.8629	23.9727	24.6917	25.2390	25.6878	27.2522	29.1633	30.5225	31.6404	32.6191	36.6362	43.6777	51.3965	61.0078
39	23.6514	24.7844	25.5176	26.0746	26.5328	28.1265	30.0784	31.4661	32.6063	33.6061	37.7146	44.9033	52.8062	62.6895
40	24.4434	25.5981	26.3452	26.9141	27.3804	29.0063	30.9961	32.4097	33.5742	34.5947	38.7842	46.1328	54.2188	64.3359

[3]

Table A-1. Erlang B

Circuits	Grade of Service													
	0.001	0.002	0.003	0.004	0.005	0.01	0.02	0.03	0.04	0.05	0.1	0.2	0.3	0.4
41	25.2384	26.4145	27.1765	27.7546	28.2300	29.8867	31.9136	33.3550	34.5387	35.5797	39.8589	47.3662	55.6543	65.9844
42	26.0359	27.2344	28.0085	28.5994	29.0826	30.7694	32.8330	34.3044	35.5093	36.5706	40.9336	48.6035	57.0527	67.6758
43	26.8369	28.0560	28.8447	29.4457	29.9378	31.6542	33.7565	35.2524	36.4807	37.5620	42.0079	49.8447	58.4951	69.3291
44	27.6396	28.8804	29.6833	30.2943	30.7952	32.5408	34.6812	36.2012	37.4526	38.5537	43.0869	51.0791	59.8984	70.9844
45	28.4464	29.7070	30.5228	31.1449	31.6544	33.4314	35.6067	37.1530	38.4274	39.5453	44.1595	52.3169	61.3257	72.6416
46	29.2540	30.5370	31.3667	31.9984	32.5164	34.3203	36.5327	38.1050	39.4021	40.5420	45.2363	53.5469	62.7559	74.3008
47	30.0649	31.3687	32.2121	32.8518	33.3796	35.2127	37.4589	39.0596	40.3792	41.5381	46.3173	54.7798	64.1660	75.9619
48	30.8774	32.2017	33.0586	33.7090	34.2451	36.1084	38.3906	40.0137	41.3555	42.5332	47.3965	56.0156	65.6016	77.6250
49	31.6927	33.0385	33.9058	34.5698	35.1111	37.0012	39.3220	40.9729	42.3337	43.5330	48.4736	57.2544	67.0161	79.2900
50	32.5104	33.8745	34.7580	35.4294	35.9802	37.8998	40.2527	41.9312	43.3136	44.5313	49.5605	58.4961	68.4570	80.9570
51	33.3302	34.7154	35.6104	36.2921	36.8508	38.7979	41.1885	42.8881	44.2950	45.5277	50.6389	59.7407	69.8760	82.6260
52	34.1520	35.5564	36.4641	37.1560	37.7241	39.6982	42.1230	43.8496	45.2747	46.5283	51.7207	60.9756	71.2969	84.2969
53	34.9753	36.4003	37.3206	38.0226	38.5968	40.6008	43.0560	44.8093	46.2585	47.5331	52.8059	62.2129	72.7197	85.9697
54	35.8017	37.2453	38.1797	38.8883	39.4717	41.5020	43.9937	45.7734	47.2401	48.5354	53.8879	63.4526	74.1445	87.6445
55	36.6292	38.0928	39.0378	39.7595	40.3503	42.4081	44.9326	46.7352	48.2257	49.5349	54.9731	64.6948	75.5713	89.2676
56	37.4592	38.9409	39.8997	40.6294	41.2275	43.3125	45.8726	47.7012	49.2119	50.5381	56.0547	65.9258	77.0000	90.9453
57	38.2899	39.7911	40.7617	41.5010	42.1064	44.2216	46.8135	48.6643	50.1951	51.5449	57.1392	67.1726	78.4028	92.6250
58	39.1227	40.6432	41.6273	42.3743	42.9885	45.1284	47.7551	49.6313	51.1819	52.5483	58.2266	68.4077	79.8350	94.2500
59	39.9575	41.4970	42.4927	43.2489	43.8719	46.0361	48.6973	50.5987	52.1724	53.5552	59.3097	69.6592	81.2402	95.9326
60	40.7941	42.3523	43.3594	44.1248	44.7546	46.9482	49.6436	51.5662	53.1592	54.5654	60.3955	70.8984	82.6758	97.6172

Circuits	Grade of Service													
	0.001	0.002	0.003	0.004	0.005	0.01	0.02	0.03	0.04	0.05	0.1	0.2	0.3	0.4
72	50.9436	52.7168	53.8638	54.7383	55.4546	57.9551	61.0313	63.2417	65.0742	66.6914	73.4590	85.7813	99.7734	117.5625
90	66.4810	68.5547	69.8950	70.9140	71.7517	74.6823	78.3051	80.9143	83.0786	85.0122	93.1421	108.1714	125.4199	147.5684
96	71.7275	73.8926	75.2930	76.3623	77.2383	80.3027	84.0996	86.8359	89.1152	91.1367	99.7148	115.6406	133.9688	157.5000
120	92.9626	95.4822	97.1118	98.3569	99.3787	102.9602	107.4170	110.6470	113.3496	115.7666	126.0645	145.5469	168.2227	197.4609
144	114.5127	117.3560	119.2017	120.6079	121.7637	125.8286	130.9043	134.6045	137.7158	140.5020	152.5078	175.4648	202.5000	237.5156
150	119.9387	122.8638	124.7543	126.2009	127.3911	131.5704	136.7981	140.6158	143.8202	146.7041	159.1187	182.9590	211.0840	247.4121
168	136.2949	139.4480	141.4885	143.0522	144.3340	148.8560	154.5161	158.6689	162.1758	165.3135	178.9717	205.4063	236.7422	277.4297
180	147.2607	150.5566	152.6935	154.3304	155.6763	160.4114	166.3660	170.7385	174.4299	177.7478	192.2168	220.3857	253.8281	297.4219
192	158.2646	161.7012	163.9336	165.6387	167.0449	171.9961	178.2305	182.8125	186.7031	190.1953	205.4766	235.3594	271.0313	317.4375
210	174.8419	178.4821	180.8533	182.6605	184.1537	189.4153	196.0675	200.9637	205.1294	208.8849	225.3552	257.8345	296.7480	347.4023
216	180.3812	184.0924	186.5017	188.3474	189.8701	195.2358	202.0188	207.0220	211.2803	215.1167	231.9785	265.3594	305.2266	357.3281
240	202.6208	206.5942	209.1797	211.1572	212.7905	218.5547	225.8643	231.2842	235.8984	240.0879	258.5449	295.3125	339.6094	397.5000
264	224.9656	229.1873	231.9386	234.0454	235.7856	241.9409	249.7720	255.5889	260.5518	265.0635	285.1084	325.2305	373.8281	437.2500
270	230.5646	234.8492	237.6425	239.7766	241.5482	247.7939	255.7452	261.6696	266.7371	271.3184	291.7529	332.7539	382.3242	447.4512
288	247.3989	251.8682	254.7773	257.0098	258.8467	265.3770	273.7090	279.9316	285.2402	290.0918	311.6602	355.2188	408.0938	477.2813
300	258.6456	263.2324	266.2170	268.5059	270.4010	277.1210	285.6995	292.1082	297.6013	302.6001	324.9756	370.2393	425.2441	497.4609
312	269.9103	274.6139	277.6750	280.0269	281.9692	288.8723	297.6987	304.2876	309.9624	315.1230	338.2412	385.2012	442.4063	517.3594
330	286.8416	291.7108	294.8932	297.3303	299.3445	306.5149	315.6995	322.5879	328.5095	333.9075	358.1982	407.6660	468.0908	547.2070
336	292.4927	297.4248	300.6343	303.1055	305.1460	312.4058	321.7061	328.6992	334.6875	340.1836	364.8340	415.2422	476.6016	557.1563
360	315.1318	320.2844	323.6462	326.2280	328.3704	335.9729	345.7507	353.1006	359.4507	365.2515	391.4648	445.1660	510.8203	597.3047

Extended Erlang B Traffic Model με 50% πιθανότητα επανάκλησης

Circuits	Grade of Service													
	0.001	0.002	0.003	0.004	0.005	0.01	0.02	0.03	0.04	0.05	0.1	0.2	0.3	0.4
35	20.5067	21.5375	22.1997	22.7017	23.1097	24.5132	26.1688	27.2925	28.1812	28.9331	31.7615	35.9827	40.0586	44.8267
36	21.2849	22.3374	23.0142	23.5272	23.9458	25.3784	27.0681	28.2173	29.1226	29.8894	32.7744	37.0898	41.2734	46.1602
37	22.0659	23.1408	23.8330	24.3558	24.7826	26.2460	27.9691	29.1411	30.0648	30.8484	33.7932	38.2014	42.4741	47.4785
38	22.8513	23.9495	24.6545	25.1880	25.6240	27.1154	28.8734	30.0679	31.0095	31.8074	34.8086	39.3081	43.6777	48.8174
39	23.6395	24.7594	25.4783	26.0222	26.4673	27.9860	29.7784	30.9948	31.9541	32.7682	35.8246	40.4187	44.8843	50.1401
40	24.4312	25.5725	26.3062	26.8604	27.3120	28.8623	30.6860	31.9238	32.9004	33.7305	36.8457	41.5283	46.0938	51.4648
41	25.2259	26.3882	27.1352	27.6995	28.1600	29.7365	31.5958	32.8571	33.8505	34.6938	37.8669	42.6416	47.3062	52.8115
42	26.0231	27.2062	27.9675	28.5417	29.0109	30.6156	32.5049	33.7892	34.8018	35.6580	38.8879	43.7534	48.5112	54.1406
43	26.8225	28.0272	28.8014	29.3867	29.8643	31.4968	33.4179	34.7223	35.7511	36.6224	39.9083	44.8582	49.7188	55.4717
44	27.6262	28.8508	29.6390	30.2339	30.7200	32.3796	34.3320	35.6587	36.7061	37.5923	40.9331	45.9766	50.9287	56.8047
45	28.4312	29.6782	30.4788	31.0831	31.5761	33.2639	35.2496	36.5955	37.6611	38.5593	41.9568	47.0874	52.1411	58.1177
46	29.2399	30.5062	31.3190	31.9338	32.4350	34.1490	36.1677	37.5350	38.6160	39.5313	42.9790	48.2012	53.3447	59.4541
47	30.0491	31.3372	32.1633	32.7873	33.2964	35.0377	37.0859	38.4744	39.5702	40.4996	44.0051	49.3121	54.5503	60.7925
48	30.8628	32.1694	33.0088	33.6416	34.1602	35.9268	38.0068	39.4160	40.5293	41.4727	45.0293	50.4258	55.7578	62.1094
49	31.6777	33.0056	33.8565	34.4995	35.0244	36.8188	38.9272	40.3568	41.4873	42.4443	46.0571	51.5361	56.9673	63.4512
50	32.4951	33.8409	34.7046	35.3577	35.8917	37.7106	39.8499	41.3025	42.4469	43.4174	47.0825	52.6489	58.1787	64.7705
51	33.3147	34.6796	35.5574	36.2205	36.7590	38.6049	40.7745	42.2468	43.4079	44.3947	48.1113	53.7642	59.3921	66.1157
52	34.1361	35.5215	36.4102	37.0814	37.6289	39.5015	41.7009	43.1926	44.3701	45.3667	49.1372	54.8818	60.6074	67.4375
53	34.9592	36.3631	37.2656	37.9449	38.5013	40.3970	42.6290	44.1397	45.3334	46.3427	50.1663	55.9955	61.8118	68.7603
54	35.7836	37.2074	38.1220	38.8125	39.3728	41.2960	43.5553	45.0879	46.2975	47.3225	51.1919	57.1113	63.0176	70.1104

[3]

Παράρτημα Γ

Προκαθορισμένες random-detect dscp τιμές για WRED απόρριψη πακέτου

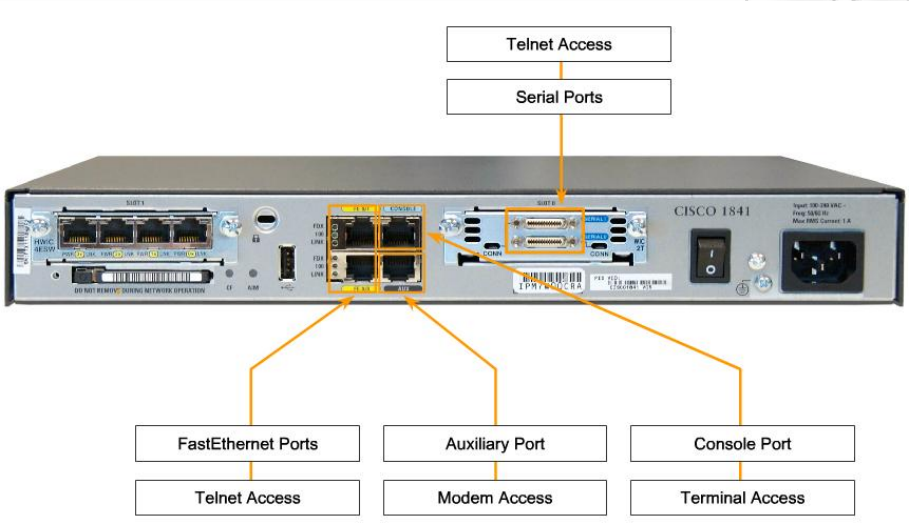
DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
0 (0)	20	40	1/10
1	22	40	1/10
2	24	40	1/10
3	26	40	1/10
4	28	40	1/10
5	30	40	1/10
6	32	40	1/10
7	34	40	1/10
8 (1)	22	40	1/10
9	22	40	1/10
10	24	40	1/10
11	26	40	1/10
12	28	40	1/10
13	30	40	1/10
14	32	40	1/10
15	34	40	1/10
16 (2)	24	40	1/10
17	22	40	1/10
18	24	40	1/10
19	26	40	1/10
20	28	40	1/10
21	30	40	1/10
22	32	40	1/10
23	34	40	1/10
24 (3)	26	40	1/10
25	22	40	1/10
26	24	40	1/10
27	26	40	1/10
28	28	40	1/10
29	30	40	1/10
30	32	40	1/10

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
31	34	40	1/10
32 (4)	28	40	1/10
33	22	40	1/10
34	24	40	1/10
35	26	40	1/10
36	28	40	1/10
37	30	40	1/10
38	32	40	1/10
39	34	40	1/10
40 (5)	30	40	1/10
41	22	40	1/10
42	24	40	1/10
43	26	40	1/10
44	28	40	1/10
45	30	40	1/10
46	36	40	1/10
47	34	40	1/10
48 (6)	32	40	1/10
49	22	40	1/10
50	24	40	1/10
51	26	40	1/10
52	28	40	1/10
53	30	40	1/10
54	32	40	1/10
55	34	40	1/10
56 (7)	34	40	1/10
57	22	40	1/10
58	24	40	1/10
59	26	40	1/10
60	28	40	1/10
61	30	40	1/10
62	32	40	1/10
63	34	40	1/10
rsvp	36	40	1/10

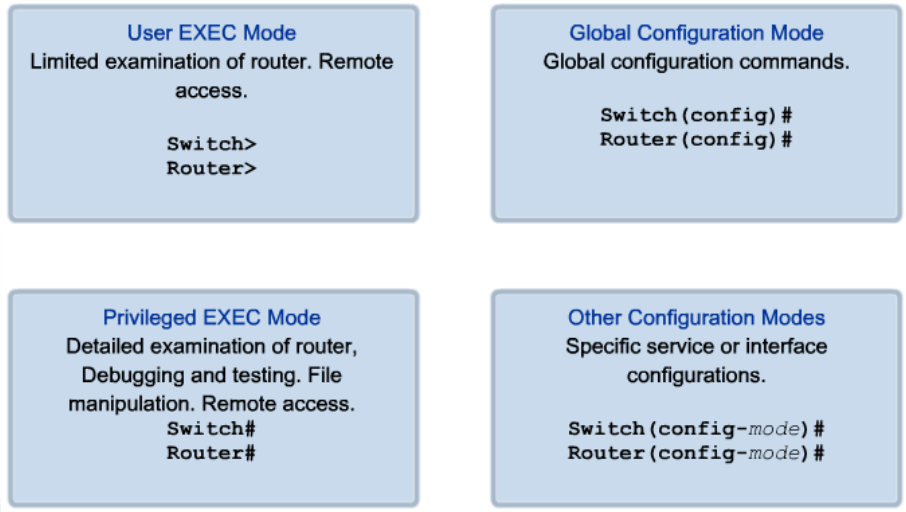
Παράρτημα Δ[21]

Cisco IOS - Βασικές Έννοιες

Επιλογές πρόσβασης στο Cisco IOS (Internetwork Operating System)

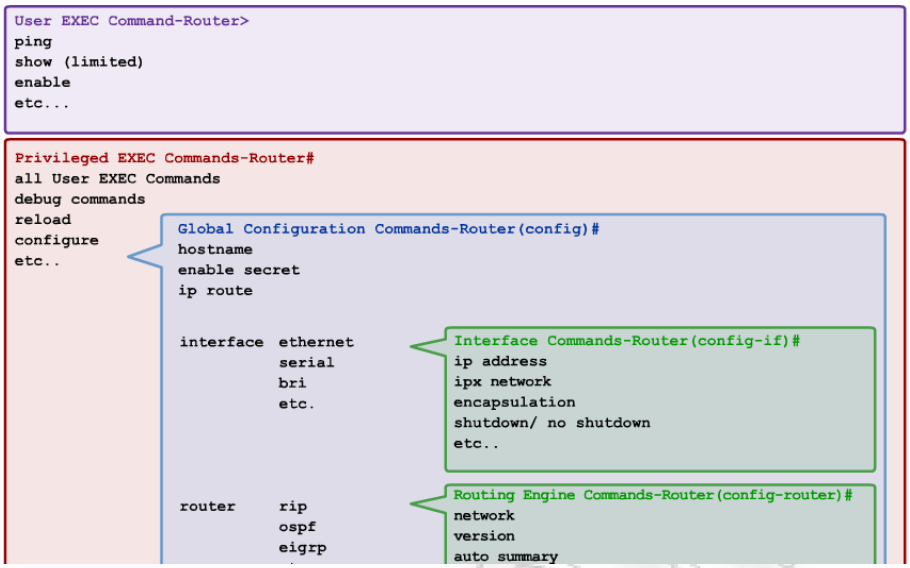


Αρχικές καταστάσεις παραμετροποίησης στο Cisco IOS

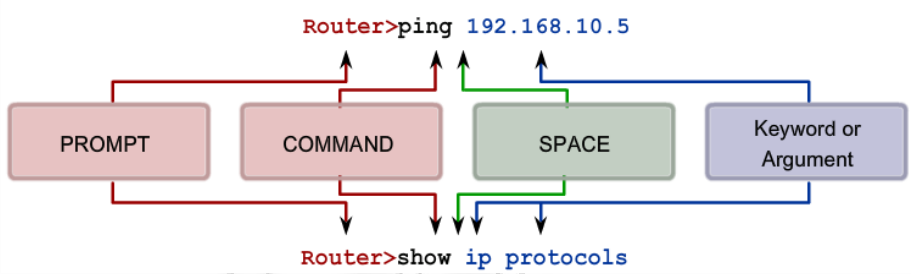


[21] Οι εικόνες στο Παράρτημα Δ είναι PrtScn από το CCNA Exploration 4.0 (Cisco Networking Academy)

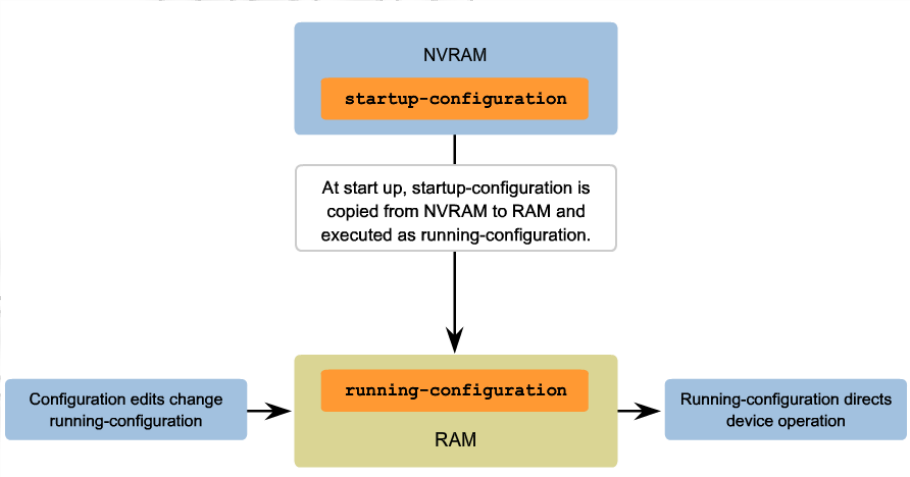
Ιεράρχηση καταστάσεων παραμετροποίησης



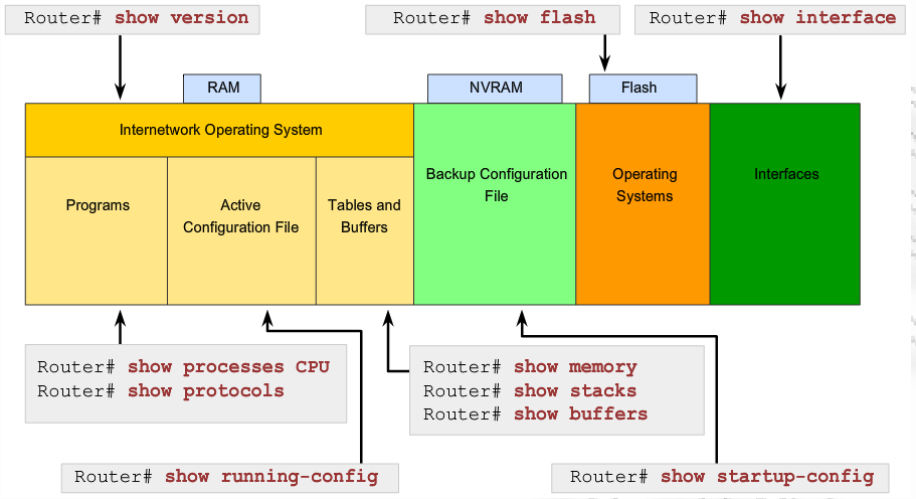
Βασική δομή εντολών του Cisco IOS



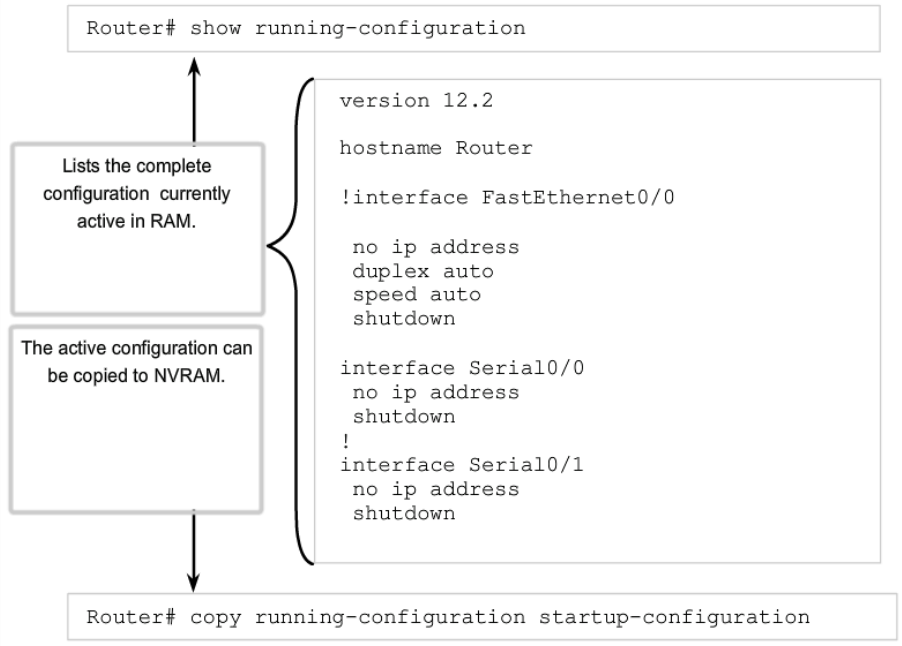
Αρχείο διάρθρωσης (Configuration Files)



Προβολή πληροφοριών μέσω Show Commands



Έλεγχος του αρχείου διάρθρωσης (Configuration File)



Βιβλιογραφία – Πηγές από το Διαδίκτυο

[1] *"Cisco Unified Communications Solution Reference Network Design*", Cisco Press, USA, October 2008.

[2] "*Cisco Unified Contact Center Enterprise Solution Reference Network Design*", Cisco Press, October 2010.

[3] *"Jonathan Davidson, Tina Fox, "Deploying Cisco over IP Solutions*", Cisco Press, USA, 2000.

[4] "*Voice and Video Enabled IPSec VPN Solution Reference Network Design*", Cisco Press, USA, January 2004.

[5] "*Cisco IOS Quality of Service Solutions Configuration Guide*", Cisco Press, USA, November 2009.

[6] "*Cisco IOS IP Service Level Agreements (SLAs) Configuration Guid",* Cisco Press, USA, August 2005.

[7] "*Traffic Analysis for Voice over IP*", Cisco Press, May 2007.

[8] Text Part Number: OL-18712-01 , "*Cisco 2900 and 3900 Series Hardware Installation*", Cisco Press, USA, 2010.

[9] "*Cisco IOS Quality of Service Solutions Command Reference",* Cisco Press, USA, December 2010.

[10] *"Cisco Unified Communications Manager Express System Administrator Guide",* Cisco Press, USA, Noveber 2010.

[11] *"Catalyst 2960 Switch Software Configuration Guide"* , Cisco Press, USA, Noveber 2008.

[12] *"Enterprice QoS Solution Reference Network Design Guide",* Cisco Press, USA, November 2005.

[13] White Paper, *"Monitoring VoIP with Cisco Network Analysis Module"*, Cisco Press, USA, October 2009.

[14] Todd Lammle, "*Cisco Certified Network Associate Study Guide*", Sixth Edition, Wiley Publishing, Indianapolis, 2007.

[15] "*Cisco IOS Dial Services Configuration Guide*", Cisco Press, USA, November 2005.

[16] Jim Doherthy, Neil Anderson, Paul Maggiora, "*Cisco Networking Simplified*", 2nd Edition, Cisco Press, USA 2008.

[17] Steve McQuerry, "*Interconnection Cisco Network Devices*", Second Edition, Cisco Press, USA 2004.

[18] Δουληγέρης Χρήστος, "*Σύγχρονα Τηλεπικοινωνιακά και Δικτυακά Πρωτόκολλα*", Εκδοσεις Νηρηίδες, Αθήνα 2004.

[19] Βενιέρης Ιάκωβος Στ., "*Δίκτυα Ευρείας Ζώνης*", 2η Έκδοση, Εκδόσεις Τζιόλα, Θεσσαλονίκη 2007.

[20] Λογοθέτης Μιχαήλ Δ., "*Θεωρία Τηλεπικοινωνιακής Κινήσεως και Εφαρμογές*", Εκδόσεις Παπασωτηρίου, Αθήνα 2001.

[21] James F. Kurose, Keith W. Ross, "*Δικτύωση Υπολογιστών Προσέγγιση από Πάνω προς τα* Κάτω", 4η Έκδοση, Εκδόσεις Γκιούρδας, Αθήνα 2009.

[22] Andrew S. Tanenbaum, "*Δίκτυα Υπολογιστών*", 4η Αμερικάνικη Έκδοση, Εκδόσεις Κλειδάριθμος, Αθήνα 2008.

[23] *"Cisco 2900 Series Integrated Services Routers"*
http://www.cisco.com/en/US/products/ps10537/index.html

[24] "*Cisco Catalyst 2960 Series Switches*"
http://www.cisco.com/en/US/products/ps6406/index.html

[25] "*Portable Product Sheets – Routing Performance*"
http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf

[26] "*Voice Design and Implementation Guide*"
http://www.cisco.com/en/US/customer/tech/tk1077/technologies_tech_note09186a0080094a8b.shtml#intro

[27] "*Configuring Voice VLAN*"
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see/configuration/guide/swvoip.pdf

[28] "*Configuring QoS*"
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see/configuration/guide/swqos.pdf

[29] "*Cisco CallManager System Guide*"
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/4_0_1/ccmsys/accm.pdf

[30] "*Understanding Delay in Packet Voice Networks*"
http://www.cisco.com/application/pdf/paws/5125/delay-details.pdf

[31] "*GRE over IPSec with EIGRP to Route Through a Hub and Multiple Remote Sites Configuration Example*"
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008009438e.shtml

[32] "*QoS in Layer 2 Networks with Cisco Catalyst 3550*"
http://www.cesnet.cz/doc/techzpravy/2003/l2qos/l2qos.pdf

[33] "*Quality of Service for Voice over IP"*
http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html

[34] "*Low Latency Queueing"*
http://www.cisco.com/en/US/docs/ios/12_0t/12_0t7/feature/guide/pqcbwfq.html

[35] "*Distributed WRED*"
http://www.cisco.com/en/US/docs/ios/11_1/feature/guide/WRED.html

[36] "*Class-Based Weighted Fair Queueing*"

http://www710.univlyon1.fr/~ogluck/Cours/Supports/L3IF_RE/CNA/CISCO1721/cbwfq.pdf

[37] "*Implementing Quality of Service Policies with DSCP*"
http://www.cisco.com/application/pdf/paws/10103/dscpvalues.pdf

[38] "*VoIP over PPP Links with Quality of Service (LLQ / IP RTP Priority, LFI, cRTP)"*
http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094660.shtml

[39] "*Cisco Secure SRST Configuration Example*"
http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_configuration_example09186a0080509462.shtml

[40] "*Sizing Call Center Resources*"
http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/ipcc_enterprise/srnd/7x/c7resrcs.html

[41] "*Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting*"
http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

[42] "*Select Your Product or Technology*"
http://www.cisco.com/cisco/web/psa/default.html?mode=tech

[43] "*IPSec VPN QoS Design*"
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/IPSecQoS.html

[44] "*Scavenger-Class QoS Strategy for DoS/Worm Attack Mitigaton*"
http://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd80295ac7.pdf

[45] "*Cisco Self-Deferending Networks*"
http://www.extraxi.com/PDFs/PostSDN1.pdf

[46] "*Codec Bandwidth Calculator*",
http://tools.cisco.com/Support/VBC/do/CodecCalc1.do

[47] *"Understanding the Basic Networking Functions, Components and Signaling Protocols in VoIP Networks*",
http://www.1stadvance.com/docs/voip/Juniper_voip.pdf

[48] *"Call Admission Control and Traffic Engineering of VoIP",*
http://140.192.40.4:8001/~imad/voip/YuJ-CallAdmin.pdf

[49] *"Dial Peer Overview",*
http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_ovrvw.html

[50] *"Dial Peer Features and Configuration",*
http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_confg.html

[51] *"Βάση Τηλεπικοινωνιακών Όρων",*
http://www.moto-teleterm.gr/search_gr.asp

[52] *"Cisco Integrated Services Routers Generation 2",*
http://www.cisco.com/en/US/prod/collateral/routers/ps10538/aag_c45_556315.pdf

[53] *"Cisco Unified Communications Manager Architecture",*
http://www.networkworld.com/subnets/cisco/072808-ch1-cisco-unified-comm-manager.html

[54] *"QoS BEST-PRACTICES",*
http://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd80295aa1.pdf

[55] *"User Guide for Cisco Security Manager 4.1",*
http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/CSMUserGuide_wrapper.html

[56] "*Policing Traffic*",
http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qpolce.html

[57] "*Configuring Modular Quality of Service Packet Classification on Cisco IOS*",
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.2/qos/configuration/guide/qc32cong.html

να πέσεις επιτρέπεται…

να σηκωθείς επιβάλλεται…