ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

«ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΧΕΙΡΙΣΗ ΥΠΗΡΕΣΙΩΝ QUALITY OF SERVICE»

ΔΗΜΗΤΡΙΟΣ Ν. ΠΡΙΜΠΑΣ
Α.Μ.: 308

ΠΑΤΡΑ 2008

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

«ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΧΕΙΡΙΣΗ ΥΠΗΡΕΣΙΩΝ QUALITY OF SERVICE»

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

Χρήστος Μπούρας, Αναπληρωτής Καθηγητής

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

Εμμανουήλ Βαρβαρίγος, Καθηγητής

Ιωάννης Γαροφαλάκης, Αναπληρωτής Καθηγητής

Χρήστος Μπούρας, Αναπληρωτής Καθηγητής

ΕΠΤΑΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

Γεώργιος Αλεξίου, Καθηγητής

Εμμανουήλ Βαρβαρίγος, Καθηγητής

Κυριάκος Βλάχος, Επίκουρος Καθηγητής

Ιωάννης Γαροφαλάκης, Αναπληρωτής Καθηγητής

Σπυρίδων Λυκοθανάσης, Καθηγητής

Χρήστος Μπούρας, Αναπληρωτής Καθηγητής

Δημήτριος Χριστοδουλάκης, Καθηγητής

Στην οικογένειά μου.

ΠΕΡΙΛΗΨΗ

Η συνεχής εξέλιξη των δικτύων που βασίζονται στο IP πρωτόκολλο και η ευρύτατη διάδοση και χρήση τους τα τελευταία χρόνια σε ολόκληρο τον κόσμο καθοδηγεί την ανάγκη για την ανάπτυξη νέων τεχνολογιών και την αναβάθμιση των υπαρχόντων, προκειμένου να καλυφθούν οι συνεχώς μεταβαλλόμενες τάσεις και ανάγκες. Δύο από τις βασικότερες εξελίξεις που σχετίζονται με το επίπεδο του IP πρωτοκόλλου είναι η δυνατότητα για την παροχή εγγυήσεων ποιότητας (Quality of Service) σε τμήμα της συνολικής κίνησης που διακινείται μέσα από τα IP δίκτυα, καθώς και η ανάγκη αναβάθμισης του IPv4 πρωτοκόλλου προκειμένου (κυρίως) να εξαλειφθεί το πρόβλημα της φειδωλής διάθεσης μοναδικών και οικουμενικά δρομολογήσιμων διευθύνσεων, καθώς και να βελτιωθούν άλλες δευτερεύουσες ατέλειες του IPv4.

Κεντρικό αντικείμενο αυτής της Διδακτορικής Διατριβής αποτελεί η μελέτη των τεχνολογιών για παροχή Quality of Service καθώς και η ανάπτυξη μηχανισμών και αλγορίθμων για την αποδοτική διαχείριση των πόρων, τον όσο το δυνατόν δίκαιο καταμερισμό της ποιότητας υπηρεσίας, καθώς και τη δυνατότητα συνεργασίας και διαλειτουργικότητας μεταξύ διαφορετικών αυτόνομων δικτυακών τμημάτων με αυτοματοποιημένο τρόπο (χωρίς δηλαδή να χρειάζεται η παρέμβαση ενός ανθρώπου διαχειριστή στις περισσότερες περιπτώσεις). Για το σκοπό αυτό έχουν προταθεί διάφορες προσεγγίσεις, οι οποίες μελετώνται στην εργασία αυτή, ενώ προτείνονται αλγόριθμοι και μηχανισμοί για τη βελτίωση της λειτουργίας και της απόδοσής τους. Επίσης, από το RFC 2638 της IETF έχει οριστεί η μονάδα του Bandwidth Broker που διαχειρίζεται συνολικά υπηρεσίες QoS σε ένα domain. Οι Bandwidth Brokers χρειάζεται να εγκαθιδρύσουν σχέσεις περιορισμένης εμπιστοσύνης με τις αντίστοιχες μονάδες στα γειτονικά domains, αντίθετα με άλλες αρχιτεκτονικές που απαιτούν τον καθορισμό των χαρακτηριστικών μιας ροής στους δρομολογητές κατά μήκος του από άκρο σε άκρο μονοπατιού. Επομένως η αρχιτεκτονική του Bandwidth Broker δίνει τη δυνατότητα να κρατηθεί η πληροφορία στο επίπεδο του διαχειριστικού domain, αντί να πρέπει να κρατηθεί σε κάθε δρομολογητή, και η DiffServ αρχιτεκτονική δίνει τη δυνατότητα να περιοριστεί η πληροφορία αυτή μόνο για τους ακραίους δρομολογητές κάθε domain.

Στα πλαίσια της διδακτορικής αυτής διατριβής μελετήθηκε η αρχιτεκτονική DiffServ σε επίπεδο μηχανισμών χρησιμοποιώντας εργαλεία εξομοίωσης (NS-2 simulator) καθώς και πραγματικό δίκτυο ευρείας κλίμακας. Το IPv4 πρωτόκολλο έχει τη δυνατότητα υλοποίησης μηχανισμών QoS στο επίπεδο δικτύου με τη χρήση του πεδίου TOS (Type Of Service). Το IPv6 επεκτείνει και βελτιώνει την ιδέα αυτή, παρέχοντας δύο νέα πεδία στην στάνταρ επικεφαλίδα, τα Traffic Class και Flow Label, τα οποία μπορούν να χρησιμοποιηθούν προς αυτήν την κατεύθυνση. Το αποτέλεσμα ήταν ο σχεδιασμός μιας ομάδας υπηρεσιών QoS (απόλυτης προτεραιότητας σε IP κίνηση, εγγυημένου εύρους ζώνης για L2 συνδέσεις μέσω ιδεατών δικτύων καθώς και κίνησης χαμηλής προτεραιότητας). Ο σχεδιασμός αυτός ολοκληρώθηκε με την υλοποίηση μιας πλήρους εφαρμογής bandwidth broker (κεντρικοποιημένη αρχιτεκτονική) που εκτελεί τις ακόλουθες εργασίες: μοντελοποίηση δικτύου, εφαρμογή του μοντέλου διαστασιολόγησης στην τρέχουσα κατάσταση, αποδοχή κλήσης QoS αιτημάτων, παραγωγή παραμέτρων ρύθμισης για τις δικτυακές συσκευές, παρακολούθηση λειτουργίας QoS στο δίκτυο, επικοινωνία με αντίστοιχους bandwidth brokers σε γειτονικά domains και πλήρη διαχείριση των αιτημάτων QoS. Επιπλέον, δεδομένου ότι οι ανάγκες των εφαρμογών για QoS αυξάνονται, πρέπει να δίνεται μεγαλύτερη ευελιξία μια QoS σηματοδοσία. Για το λόγο αυτό μελετήθηκε και υλοποιήθηκε μια εφαρμογή αυτόματης σηματοδοσίας χρησιμοποιώντας το ευρέως γνωστό πρωτόκολλο δρομολόγησης BGP. Το αποτέλεσμα είναι να επιτυγχάνεται δυναμική σηματοδοσία για QoS σε ένα δίκτυο μέσω μιας διεπαφής που βασίζεται σε Web service ή σε μια Βάση Δεδομένων. Το σύνολο της εργασίας αυτής δοκιμάστηκε και εφαρμόστηκε στο Εθνικό Δίκτυο Έρευνας & Τεχνολογίας και είναι διαθέσιμο σε αντίστοιχα ερευνητικά εθνικά δίκτυα.

Επιπλέον, μια σημαντική παράμετρος της υποστήριξης QoS μηχανισμών από άκρο σε άκρο είναι η συνεργασία μεταξύ διαφορετικών αυτόνομων τμημάτων (domains) που απαιτείται προκειμένου η κίνηση να υφίσταται προνομιακή μεταχείριση καθ' όλη τη διαδρομή της και να της παρέχονται οι αναγκαίες εγγυήσεις ποιότητας. Η διαπραγμάτευση της συνεργασίας αυτής είναι σαφές ότι πρέπει να είναι όσο το δυνατόν αυτοματοποιημένη για να μπορούν τέτοιου είδους υπηρεσίες να γνωρίσουν ευρύτερη διάδοση. Ο υλοποιημένος bandwidth broker επεκτάθηκε ώστε μέσω Web service διεπαφών να «συνομιλεί» με αντίστοιχους άλλων domains.

Παράλληλα, στα πλαίσια της εργασίας αυτής ασχοληθήκαμε επίσης με κατανεμημένες αρχιτεκτονικές bandwidth broker όπου έγιναν υλοποιήσεις σε επίπεδο εξομοίωσης. Αρχικά υλοποιήθηκαν ή επεκτάθηκαν οι υλοποιήσεις των μηχανισμών QoS στον εξομοιωτή και δημιουργήθηκε και δοκιμάστηκαν QoS σενάρια. Στη συνέχεια υλοποιήθηκαν παραλλαγές bandwidth broker που ακολουθούσαν

κεντρικοποιημένες και κατανεμημένες αρχιτεκτονικές. Στόχος της μελέτης ήταν να μελετηθεί το trade-off στη λειτουργία τους και να συσχετιστεί με τις εκάστοτε δικτυακές συνθήκες. Στην κατανεμημένη λειτουργία εξαρτάται σημαντικά από την τοπολογία του δικτύου, από την διαμόρφωση του bandwidth broker πάνω στη τοπολογία και από την κατανομή QoS αιτημάτων. Για το τελευταίο μελετήθηκε ένας αλγόριθμος προσαρμογής ενός κατανεμημένου bandwidth broker ώστε να επιλέγεται η βέλτιστη διαμόρφωσή του στο δίκτυο (με βάση τις συνθήκες δικτύου) με στόχο την ταχύτερη απόκριση. Τέλος, στα πλαίσια της εργασίας αυτής διερευνήθηκε το θέμα της «inter domain» δρομολόγησης σε μια πλήρη τοπολογία ανεξάρτητων – αυτόνομων domains για την εξεύρεση του βέλτιστου μονοπατιού που ικανοποιεί τις QoS απαιτήσεις. Ειδικότερα, μελετήθηκαν διάφορα μοντέλα και δοκιμάστηκαν πειραματικά σε επίπεδο εξομοίωσης, δίνοντας έμφαση σε θέματα αυτονομίας διαχείρισης στο εσωτερικό κάθε ανεξάρτητου domain και στην τήρηση των SLAs μεταξύ γειτονικών domains.

EXECUTIVE SUMMARY

The main goal of this dissertation is the study of the provisioning of Quality of Service guarantees to part of the total traffic traversing IP networks. The study is focused on both IPv4 and IPv6 protocol, as IPv6 overcome the limitation that IPv4 has introduced. Also goal of this dissertation is the development of mechanisms and algorithms for the effective administration of resources, the best possible fairness in distributing the quality of service, and the possibility of cooperation and interoperability between different domains in an automated way (without the need for human intervention in most cases). For this reason, a number of approaches have been proposed related to Bandwidth Brokers. These approaches are studied in this dissertation, while new algorithms and mechanisms are proposed for the improvement of their operation and performance.

IPv4 was capable of supporting QoS mechanisms at the network layer using the TOS field (Type of Service). IPv6 advances and improves on this idea, by supplying two new fields in the standard header, called Traffic Class and Flow Label, which can be used for this purpose. The usage of these fields, as well as the usage of IPv6 is still at an early stage. However, while IPv6 comes to the foreground and becomes mature enough to replace the dominant IPv4, it is especially interesting to investigate the way that IPv6 QoS capabilities are practically going to be exploited.

An important parameter for supporting end-to-end QoS mechanisms is the interaction between multiple domains so that the designated traffic is subjected to preferential treatment along the whole path. The negotiation of this interaction clearly has to be as much automated as possible, if such services are to be widely supported.

For this reason, RFC 2638 from IETF has defined the Bandwidth Broker entity. According to the RFC definition, it controls the network load by accepting or rejecting requests for specific bandwidth with QoS guarantees. Bandwidth Brokers only need to establish relationships of limited trust with their peers in adjacent domains, unlike schemes that require the setting of flow specifications in routers throughout an end-to-end path. In practical technical terms, the Bandwidth Broker architecture makes it possible to keep state on an administrative domain basis, rather than at every router and the service definitions of Premium and Assured service make it possible to confine per flow state to just the leaf routers.

In the framework of this dissertation we studied a full QoS framework, including priority and assured bandwidth services for Greek Research and Technology Network. In addition, we studied and implemented a bandwidth broker that manages these services in the above network and it also communicate with adjacent domains (like Geant, the Pan-European Academic Network), providing end-to-end provisioning. The implemented bandwidth broker is based on open source tools and belongs to Grnet's production services portfolio. Finally, it is available for use to other Research networks as well as the experience from the development.

Additionally, we studied distributed architectures of bandwidth brokers using simulation tools. We implemented some enhancements on NS-2 simulator in order to have all the necessary tools for QoS tests and measurements. Next, we simulated and compared distributed and centralized models, focusing on the trade-off in their operation related to the network conditions. In distributed architectures, the operation is highly affected by topology and the distribution of service's requests. Therefore, we studied an algorithm that adapts the distributed bandwidth broker according to several conditions, by changing the location of the main base station and the overall configuration. Finally, we studied several models for the inter-domain routing in a topology with many independent autonomous systems, aiming at investigate the best routing path that provides the QoS guarantees while the autonomous systems keeps the privacy and the SLAs in their domains.

ΠΡΟΛΟΓΟΣ

Πριν την παρουσίαση των αποτελεσμάτων της παρούσας διδακτορικής διατριβής, αισθάνομαι την υποχρέωση να ευχαριστήσω ορισμένους από τους ανθρώπους που γνώρισα, συνεργάστηκα μαζί τους και έπαιξαν πολύ σημαντικό ρόλο στην πραγματοποίησή της.

Πρώτο από όλους τον επιβλέποντα της διδακτορικής διατριβής, Αναπληρωτή Καθηγητή Χρήστο Μπούρα που αποτέλεσε τον καθοδηγητή μου σε όλα τα στάδια της διδακτορικής διατριβής, δίνοντάς μου ευκαιρίες να γίνω καλύτερος τόσο ακαδημαϊκά όσο και σαν άνθρωπος. Με στήριξε και με βοήθησε σε διάφορα επίπεδα, σαν καθηγητής προς μαθητή στο Πανεπιστήμιο, σαν διευθυντής προς υπάλληλο στα πλαίσια της συνεργασίας μας στην Ερευνητική Μονάδα 6 του Ερευνητικού Ακαδημαϊκού Ινστιτούτου Τεχνολογίας Υπολογιστών (ΕΑΙΤΥ) αλλά κυρίως σαν φίλος προς φίλο. Του εύχομαι να είναι καλά και πάντα επιτυχίες, προσωπικές και επαγγελματικές.

Στη συνέχεια τα μέλη της τριμελούς επιτροπής, τον Καθηγητή Μάνο Βαρβαρίγο και τον Αναπληρωτή Καθηγητή Γιάννη Γαροφαλάκη, εξαιρετικούς δάσκαλους με βαρύνουσα άποψη και κύρος, για την καθοδήγησή τους και την υποστήριξή τους στην ολοκλήρωση αυτής της διδακτορικής διατριβής.

Επίσης τα μέλη της επταμελούς επιτροπής για την ουσιαστική συνδρομή τους στην ολοκλήρωση αυτής της διδακτορικής διατριβής: τον Καθηγητή Σπυρίδων Λυκοθανάση, τον Καθηγητή Δημήτριο Χριστοδουλάκη, τον Καθηγητή Γεώργιο Αλεξίου και τον Επίκουρο Καθηγητή Κυριάκο Βλάχο .

Στη συνέχεια ευχαριστώ, όλους τους συναδέλφους και συνεργάτες μου στα πλαίσια της συμμετοχής μου στο Εργαστήριο Κατανεμημένων Συστημάτων & Τηλεματικής του ΤΜΗΥΠ και στην Ερευνητική Μονάδα 6 του ΕΑΙΤΥ. Ιδιαίτερη μνεία οφείλω να κάνω για τους φίλους Κώστα Στάμο, Βαγγέλη Ιγγλέση, Λεωνίδα και Βασίλη Πουλόπουλο, Αποστόλη Γκάμα καθώς και τον Αντώνη Αλεξίου.

Ευγνωμοσύνη εκφράζω για την συμβολή των γονέων μου και του αδερφού μου, σε αυτή την προσπάθεια αλλά και για όλα όσα έχουν κάνει για εμένα.

Πάτρα, Μάρτιος 2008

Δημήτρης Πρίμπας

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

ΕΙΣΑΓΩΓΗ

Η συνεχής εξέλιξη των δικτύων που βασίζονται στο IP πρωτόκολλο και η ευρύτατη διάδοση και χρήση τους τα τελευταία χρόνια σε ολόκληρο τον κόσμο καθοδηγεί την ανάγκη για την ανάπτυξη νέων τεχνολογιών και την αναβάθμιση των υπαρχόντων, προκειμένου να καλυφθούν οι συνεχώς μεταβαλλόμενες τάσεις και ανάγκες. Δύο από τις βασικότερες εξελίξεις που σχετίζονται με το επίπεδο του IP πρωτοκόλλου είναι η δυνατότητα για την παροχή εγγυήσεων ποιότητας (Quality of Service) σε τμήμα της συνολικής κίνησης που διακινείται μέσα από τα IP δίκτυα, καθώς και η ανάγκη αναβάθμισης του IPv4 πρωτοκόλλου προκειμένου (κυρίως) να εξαλειφθεί το πρόβλημα της φειδωλής διάθεσης μοναδικών και οικουμενικά δρομολογήσιμων διευθύνσεων, καθώς και να βελτιωθούν άλλες δευτερεύουσες ατέλειες του IPv4.

Κεντρικό αντικείμενο αυτής της Διδακτορικής Διατριβής αποτελεί η μελέτη των τεχνολογιών για παροχή Quality of Service καθώς και η ανάπτυξη μηχανισμών και αλγορίθμων για την αποδοτική διαχείριση των πόρων, τον όσο το δυνατόν δίκαιο καταμερισμό της ποιότητας υπηρεσίας, καθώς και τη δυνατότητα συνεργασίας και διαλειτουργικότητας μεταξύ διαφορετικών αυτόνομων δικτυακών τμημάτων με αυτοματοποιημένο τρόπο (χωρίς δηλαδή να χρειάζεται η παρέμβαση ενός ανθρώπου διαχειριστή στις περισσότερες περιπτώσεις). Για το σκοπό αυτό έχουν προταθεί διάφορες προσεγγίσεις, οι οποίες μελετώνται στην εργασία αυτή, ενώ προτείνονται αλγόριθμοι και μηχανισμοί για τη βελτίωση της λειτουργίας και της απόδοσής τους. Επίσης, από το RFC 2638 της IETF έχει οριστεί η μονάδα του Bandwidth Broker που διαχειρίζεται συνολικά υπηρεσίες QoS σε ένα domain. Οι Bandwidth Brokers χρειάζεται να εγκαθιδρύσουν σχέσεις περιορισμένης εμπιστοσύνης με τις αντίστοιχες μονάδες στα γειτονικά domains, αντίθετα με άλλες αρχιτεκτονικές που απαιτούν τον καθορισμό των χαρακτηριστικών μιας ροής στους δρομολογητές κατά μήκος του από άκρο σε άκρο μονοπατιού. Επομένως η αρχιτεκτονική του Bandwidth Broker δίνει τη δυνατότητα να κρατηθεί η πληροφορία στο επίπεδο του διαχειριστικού domain, αντί να πρέπει να κρατηθεί σε κάθε δρομολογητή, και η DiffServ αρχιτεκτονική δίνει τη δυνατότητα να περιοριστεί η πληροφορία αυτή μόνο για τους ακραίους δρομολογητές κάθε domain.

Στα πλαίσια της διδακτορικής αυτής διατριβής μελετήθηκε η αρχιτεκτονική DiffServ σε επίπεδο μηχανισμών χρησιμοποιώντας εργαλεία εξομοίωσης (NS-2 simulator) καθώς και πραγματικό δίκτυο ευρείας κλίμακας. Το IPv4 πρωτόκολλο έχει τη δυνατότητα υλοποίησης μηχανισμών QoS στο επίπεδο δικτύου με τη χρήση του πεδίου TOS (Type Of Service). Το IPv6 επεκτείνει και βελτιώνει την ιδέα αυτή, παρέχοντας δύο νέα πεδία στην στάνταρ επικεφαλίδα, τα Traffic Class και Flow Label, τα οποία μπορούν να χρησιμοποιηθούν προς αυτήν την κατεύθυνση. Το αποτέλεσμα ήταν ο σχεδιασμός μιας ομάδας υπηρεσιών QoS (απόλυτης προτεραιότητας σε IP κίνηση, εγγυημένου εύρους ζώνης για L2 συνδέσεις μέσω ιδεατών δικτύων καθώς και κίνησης χαμηλής προτεραιότητας). Ο σχεδιασμός αυτός ολοκληρώθηκε με την υλοποίηση μιας πλήρους εφαρμογής bandwidth broker (κεντρικοποιημένη αρχιτεκτονική) που εκτελεί τις ακόλουθες εργασίες: μοντελοποίηση δικτύου, εφαρμογή του μοντέλου διαστασιολόγησης στην τρέχουσα κατάσταση, αποδοχή κλήσης QoS αιτημάτων, παραγωγή παραμέτρων ρύθμισης για τις δικτυακές συσκευές, παρακολούθηση λειτουργίας QoS στο δίκτυο, επικοινωνία με αντίστοιχους bandwidth brokers σε γειτονικά domains και πλήρη διαχείριση των

αιτημάτων QoS. Επιπλέον, δεδομένου ότι οι ανάγκες των εφαρμογών για QoS αυξάνονται, πρέπει να δίνεται μεγαλύτερη ευελιξία μια QoS σηματοδοσία. Για το λόγο αυτό μελετήθηκε και υλοποιήθηκε μια εφαρμογή αυτόματης σηματοδοσίας χρησιμοποιώντας το ευρέως γνωστό πρωτόκολλο δρομολόγησης BGP. Το αποτέλεσμα είναι να επιτυγχάνεται δυναμική σηματοδοσία για QoS σε ένα δίκτυο μέσω μιας διεπαφής που βασίζεται σε Web service ή σε μια Βάση Δεδομένων. Το σύνολο της εργασίας αυτής δοκιμάστηκε και εφαρμόστηκε στο Εθνικό Δίκτυο Έρευνας & Τεχνολογίας και είναι διαθέσιμο σε αντίστοιχα ερευνητικά εθνικά δίκτυα.

Επιπλέον, μια σημαντική παράμετρος της υποστήριξης QoS μηχανισμών από άκρο σε άκρο είναι η συνεργασία μεταξύ διαφορετικών αυτόνομων τμημάτων (domains) που απαιτείται προκειμένου η κίνηση να υφίσταται προνομιακή μεταχείριση καθ' όλη τη διαδρομή της και να της παρέχονται οι αναγκαίες εγγυήσεις ποιότητας. Η διαπραγμάτευση της συνεργασίας αυτής είναι σαφές ότι πρέπει να είναι όσο το δυνατόν αυτοματοποιημένη για να μπορούν τέτοιου είδους υπηρεσίες να γνωρίσουν ευρύτερη διάδοση. Ο υλοποιημένος bandwidth broker επεκτάθηκε ώστε μέσω Web service διεπαφών να «συνομιλεί» με αντίστοιχους άλλων domains.

Παράλληλα, στα πλαίσια της εργασίας αυτής ασχοληθήκαμε επίσης με κατανεμημένες αρχιτεκτονικές bandwidth broker όπου έγιναν υλοποιήσεις σε επίπεδο εξομοίωσης. Αρχικά υλοποιήθηκαν ή επεκτάθηκαν οι υλοποιήσεις των μηχανισμών QoS στον εξομοιωτή και δημιουργήθηκε και δοκιμάστηκαν QoS σενάρια. Στη συνέχεια υλοποιήθηκαν παραλλαγές bandwidth broker που ακολουθούσαν κεντρικοποιημένες και κατανεμημένες αρχιτεκτονικές. Στόχος της μελέτης ήταν να μελετηθεί το trade-off στη λειτουργία τους και να συσχετιστεί με τις εκάστοτε δικτυακές συνθήκες. Στην κατανεμημένη λειτουργία εξαρτάται σημαντικά από την τοπολογία του δικτύου, από την διαμόρφωση του bandwidth broker πάνω στη τοπολογία και από την κατανομή QoS αιτημάτων. Για το τελευταίο μελετήθηκε ένας αλγόριθμος προσαρμογής ενός κατανεμημένου bandwidth broker ώστε να επιλέγεται η βέλτιστη διαμόρφωσή του στο δίκτυο (με βάση τις συνθήκες δικτύου) με στόχο την ταχύτερη απόκριση. Τέλος, στα πλαίσια της εργασίας αυτής διερευνήθηκε το θέμα της «inter domain» δρομολόγησης σε μια πλήρη τοπολογία ανεξάρτητων – αυτόνομων domains για την εξεύρεση του βέλτιστου μονοπατιού που ικανοποιεί τις QoS απαιτήσεις. Ειδικότερα , μελετήθηκαν διάφορα μοντέλα και δοκιμάστηκαν πειραματικά σε επίπεδο εξομοίωσης, δίνοντας έμφαση σε θέματα αυτονομίας διαχείρισης στο εσωτερικό κάθε ανεξάρτητου domain και στην τήρηση των SLAs μεταξύ γειτονικών domains.

Η εργασία δομείται σε κεφάλαια ως εξής:

- Στο Κεφάλαιο 2 παρουσιάζονται οι τεχνολογίες στις οποίες βασίστηκε η έρευνα αυτής της διδακτορικής διατριβής, δηλαδή οι μηχανισμοί για την παροχή Ποιότητας Υπηρεσίας (QoS) στο επίπεδο 3 του Internet, με έμφαση στην ευρέως χρησιμοποιούμενη αρχιτεκτονική DiffServ, και το πρωτόκολλο IPv6.
- Στο Κεφάλαιο 3 περιγράφεται η αρχιτεκτονική των Bandwidth Brokers για την αυτοματοποιημένη παροχή υπηρεσιών QoS από άκρο σε άκρο, καθώς και τα πρωτόκολλα που έχουν προταθεί για την υλοποίηση του signaling (σηματοδότησης) μεταξύ Bandwidth Brokers και δικτυακών συσκευών.
- Στο Κεφάλαιο 4 εξετάζεται το κατά πόσο οι τεχνολογίες QoS μπορούν να αποδώσουν αποτελεσματικά σε επίπεδο παραγωγής, και παρουσιάζεται ο

αναλυτικός σχεδιασμός των QoS υπηρεσιών για το δίκτυο παραγωγής του ΕΔΕΤ που χρησιμοποιήθηκε ως βάση για τη μελέτη μας.

- Στο κεφάλαιο 5 περιγράφεται ο σχεδιασμός και υλοποίηση ενός κεντρικοποιημένου bandwidth broker για την αυτόματη διαχείριση των υπηρεσιών QoS στο δίκτυο του ΕΔΕΤ και την διασύνδεση με άλλα αυτόνομα (ανεξάρτητα domains)
- Στο κεφάλαιο 6 περιγράφεται η αλληλεπίδραση και οι αλλαγές που επιφέρει η είσοδος του πρωτοκόλλου IPv6 στις QoS υπηρεσίες. Παρουσιάζονται πειραματικά αποτελέσματα από την υλοποίηση QoS υπηρεσίας σε δίκτυο διπλής στοίβας (το οποίο δηλαδή υποστηρίζει μεταφορά κίνησης πάνω από IPv4 και IPv6) στο δίκτυο του ΕΔΕΤ καθώς και πειράματα σε native IPv6. Τέλος, γίνεται αναφορά στις επεκτάσεις του υλοποιημένου bandwidth broker προκειμένου α διαχειρίζεται και υπηρεσίες IPv6 QoS.
- Στο κεφάλαιο 7 παρουσιάζεται η μελέτη και δοκιμή σε περιβάλλον εξομοίωσης (με χρήση του NS-2) διαφόρων μοντέλων bandwidth broker με έμφαση σε κατανεμημένες αρχιτεκτονικές. Γίνεται μελέτη και σύγκριση μεταξύ τους καθώς επίσης αναδεικνύονται διάφορα σημεία που χρήζουν βελτίωσης και προτείνονται μέθοδοι βελτιστοποίησης τόσο για ταχύτερη απόδοση των κατανεμημένων αρχιτεκτονικών μέσω αλγορίθμων επιλογής θέσης του βασικού agent όσο και για ταχύτερη και αποδοτικότερη interdomain λειτουργία.
- Στο Κεφάλαιο 8 ανακεφαλαιώνονται συνοπτικά τα συμπεράσματα από την παρούσα διδακτορική διατριβή.
- Στο Κεφάλαιο 9 παρουσιάζονται οι ανοιχτοί τομείς έρευνας στο σχετικό αντικείμενο και η σχεδιαζόμενη μελλοντική μας εργασία πάνω σε αυτό.
- Στο Παράρτημα Ι παρουσιάζονται αλφαβητικά η βιβλιογραφία και οι δικτυακοί τόποι που αναφέρονται στην διδακτορική διατριβή. Οι αναφορές στην βιβλιογραφία και τους δικτυακούς τόπους ενσωματώνονται στο κείμενο μέσα σε αγκύλες ([ ]).
- Στο Παράρτημα ΙΙ παρουσιάζονται τα ακρωνύμια τα οποία χρησιμοποιούνται σε αυτή τη διδακτορική διατριβή για την διευκόλυνση του αναγνώστη.
- Στο Παράρτημα ΙΙΙ παρουσιάζεται το γλωσσάριο ξενικών όρων οι οποίοι χρησιμοποιούνται σε αυτή τη διδακτορική διατριβή για την διευκόλυνση του αναγνώστη.

Στην συνέχεια παρουσιάζονται τα άρθρα που δημοσιεύτηκαν, στα πλαίσια της παρούσας διατριβής, σε διεθνή περιοδικά και συνέδρια.

ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΠΕΡΙΟΔΙΚΑ

[1] “Architectures and Performance Evaluation of Bandwidth Brokers”, International Journal of Network Management, Wiley InterScience, C. Bouras, D. Primpas, 2008 (to appear)

[2] “QoS experiences in native IPv6 networks”, International Journal of Network Management, Wiley InterScience, A. Liakopoulos, D. Kalogeras, V. Maglaris, D. Primpas, C. Bouras, 2008 (to appear)

[3] “IPv6 Deployment: Real Time Applications and QoS Aspects”, Computer Communications Journal, Elsevier Science, C. Bouras, A. Gkamas, D. Primpas, K. Stamos, 2006, Vol. 29, No. 9, pp. 1393 - 1401

[4] “Performance Evaluation of the Impact of Quality of Service mechanisms in an IPv6 network for IPv6 - capable real time applications”, Journal of Network and Systems Management, Kluwer Academic Publishers, Volume 12, Issue 4, C. Bouras, A. Gkamas, D. Primpas, K. Stamos, December 2004, pp. 463 – 483

ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΣΥΝΕΔΡΙΑ

[1] “Framework for Dynamic and On - Demand QoS to Videoconference Session”, The 2007 International Conference on Multimedia Systems and Applications (MSA07), Las Vegas, Nevada, USA, C. Bouras, A. Gkamas, D. Primpas, 25 - 28 June 2007

[2] “AMPS - ANStool: Interoperability of automated tools for the provisioning of QoS services”, TERENA Networking Conference 2007, Lyngby, Denmark, C. Bouras, V. Haniotakis, D. Primpas, K. Stamos, A. Varvitsiotis, 21 - 24 May 2007

[3] “Pathfinding architectures for interdomain Bandwidth Broker operation”,14th IEEE International Conference on Networks, Singapore, C. Bouras, D. Primpas, 13 - 15 September 2006, pp. 21 – 26

[4] "Techniques for DiffServ - based QoS in Hierarchically Federated MAN Networks - the GRNET Case" A. Varvitsiotis, V. Siris, D. Primpas, G. Fotiadis, A. Liakopoulos, C. Bouras, The 14th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN 2005), Chania. Island of Crete, Greece, September 18 - 21 2005

[5] "QoS experiences in native IPv6 GRNET and 6NET networks" A. Liakopoulos, D. Kalogeras, V. Maglaris, D. Primpas, C. Bouras, The 2005 International Conference on Telecommunication Systems – Modeling and Analysis, Dallas, TX, USA, 17 - 20 November 2005, pp. 284 – 292

[6] “Enhancing ns-2 with DiffServ QoS features”, 10th International Communications and Networking Simulation Symposium (CNS 07), Norfolk Marriott Waterside, Norfolk, VA, USA, C. Bouras, D. Primpas, K. Stamos, 25 - 29 March 2007

[7] “Using the ns-2 simulation environment to implement and evaluate Bandwidth Broker models”, 2nd Conference on Next Generation Internet Design and Engineering (NGI 2006), Valencia, C. Bouras, I. Pappas, D. Primpas, K. Stamos, 3 - 5 April 2006, pp. 285 – 291

[8] “Investigating Bandwidth Broker's inter-domain operation for dynamic and automatic end to end provisioning”, Sixth International Network Conference, Plymouth, UK, C. Bouras, D. Primpas, 11 - 14 July 2006

[9] "An admission control and deployment optimization algorithm for an implemented distributed Bandwidth Broker in a simulation environment" C. Bouras, D. Primpas, 4th International Conference on Networking – ICN 2005, Reunion Island, France, April 17 -21 2005, pp. 766 – 773

[10] "A host selection model for a distributed bandwidth broker" C. Bouras, D. Primpas, Third International Working Conference on Performance Modelling and Evaluation of Heterogeneous Networks, Ilkley, West Yorkshire, UK, July 18 - 20 2005

[11] "QoS issues in the Research and Academic Networks: The case of GRnet" C. Bouras, A. Karaliotas, M. Oikonomakos, M. Paraskevas, D. Primpas, C. Sintoris, Industrial Conference on Multi-Provider QoS/SLA Internetworking (MPQSI 2005), Tahiti, French Polynesia, October 23 - 28 2005

[12] "IPv6 QoS Testing on Dual Stack Networks", The Second International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications (AAA-IDEA 2006), Pisa, Italy, C. Bouras, D. Primpas, K. Stamos, 10 October 2006

[13] "QoS issues in a large - scale IPv6 network" C. Bouras, K. Stamos, D. Primpas, 2005 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS' 05), Philadelpia, Pennsylvania, USA, 23 - 28 July 2005, pp. 406 – 415

[14] "Design and implementation of a Bandwidth Broker in a simulation environment" C. Bouras, D. Primpas, K. Stamos, N. Stathis, 7th International Symposium on Communications Interworking - INTERWORKING 2004, Ottawa, Canada, November 29 - December 1 2004

[15] "Quality of Service aspects in an Ipv6 domain" C. Bouras, A. Gkamas, D. Primpas, K. Stamos, 2004 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 04), San Jose, California, USA, July 25 - 29 2004

[16] "Enhancing the DiffServ Architecture of a Simulation Environment", Sixth IEEE International Workshop on Distributed Simulation and Real Time Applications, Fort Worth, USA, C. Bouras, D. Primpas, A. Sevasti, 11 - 13 October 2002, pp. 108 – 118

[17] "Implemention issues of Managed Bandwidth Service: The case of GRNET" C. Bouras, D. Primpas, International Conference on High Speed Networks(ICHSN 2005), Montreal, Canada, 14 - 17 August 2005, pp. 293 - 298

ΚΕΦΑΛΑΙΟ 2: Η ΕΝΝΟΙΑ «QUALITY OF SERVICE»

Η ΕΝΝΟΙΑ «QUALITY OF SERVICE»

2.1 ΕΙΣΑΓΩΓΗ

Σε ένα πραγματικό IP δίκτυο [1][2], η βασική υπηρεσία που προσφέρεται είναι η υπηρεσία best effort (καλύτερης προσπάθειας). Σύμφωνα με αυτή κάθε πακέτο που φτάνει σε ένα δρομολογητή δέχεται την ακόλουθη επεξεργασία:

- Αρχικά γίνεται έλεγχος για το που θα σταλεί το πακέτο που μόλις έφτασε.
- Στη συνέχεια το πακέτο στέλνεται στη γραμμή εξόδου για το επόμενο hop. Εάν δεν είναι δυνατό το πακέτο να σταλεί άμεσα αυτό αποθηκεύεται προσωρινά σε μια ουρά εξόδου.
- Εάν η ουρά αυτή είναι γεμάτη το πακέτο απορρίπτεται. Σε περίπτωση που όταν φτάσει το πακέτο η ουρά περιέχει ήδη άλλα πακέτα τότε το πακέτο αυτό δέχεται επιπλέον καθυστέρηση σύμφωνα με το χρόνο που απαιτείται ώστε τα παλιότερα πακέτα να φύγουν από την ουρά.

Ουσιαστικά στην best effort υπηρεσία όλα τα πακέτα αντιμετωπίζονται όμοια και δεν υπάρχουν εγγυήσεις, διαφοροποιήσεις ή προσπάθεια επιβολής δικαιοσύνης. Εντούτοις το δίκτυο προσπαθεί να προωθήσει όσο περισσότερη κίνηση μπορεί με «λογική» ποιότητα. Στο δίκτυο πολλές φορές παρουσιάζεται το φαινόμενο της συμφόρησης, που ουσιαστικά συμβαίνει όταν ένας δρομολογητής αποθηκεύει πακέτα σε μια ουρά εξόδου, γεγονός που συμβαίνει όταν λαμβάνει περισσότερα πακέτα από αυτά που μπορεί να μεταδώσει. Στη διάρκεια της περιόδου συμφόρησης είναι λογικό τα πακέτα να δέχονται μεγαλύτερη καθυστέρηση ενώ όταν η ουρά εξόδου γεμίσει, τότε αυτά απορρίπτονται.

Ωστόσο υπάρχουν εφαρμογές που απαιτούν ορισμένες εγγυήσεις (κυρίως σε καθυστέρηση και απόρριψη πακέτων) όπως οι εφαρμογές Voice over IP (VoIP - IP τηλεφωνία) και Videoconference (τηλεδιάσκεψη). Αυτές προκειμένου να πετύχουν τις εγγυήσεις ποιότητας που εξασφαλίζουν τη σωστή λειτουργία τους πρέπει να βρίσκουν στο δίκτυο άδειες ή σχεδόν άδειες ουρές, γεγονός που για να συμβεί πρέπει να υπάρξουν μηχανισμοί που θα το διασφαλίσουν.

Ένας τρόπος προκειμένου να υπάρξει παροχή εγγυήσεων σε κάποια κίνηση είναι η διαχείριση ορισμένων πακέτων διαφορετικά έναντι των υπολοίπων. Στο σημείο αυτό ουσιαστικά εισέρχεται η έννοια της ποιότητας υπηρεσίας (Quality of Service) [3]. Ένας ορισμός της είναι: «**η ικανότητα ενός στοιχείου του δικτύου να παρέχει ένα επίπεδο διαβεβαίωσης (εγγύησης) σε ένα υποσύνολο κίνησης ότι οι απαιτήσεις υπηρεσίας της μπορεί να επιτευχθούν με συγκεκριμένη (πολύ μεγάλη) πιθανότητα**». Ουσιαστικά οι μηχανισμοί του Quality of Service δεν παρέχουν μεγαλύτερη χωρητικότητα στο δίκτυο ή κάτι παρόμοιο, αλλά απλώς κάνουν καλύτερη διαχείριση του δικτύου ώστε να χρησιμοποιείται πιο αποδοτικά και σύμφωνα με τις απαιτήσεις των εφαρμογών

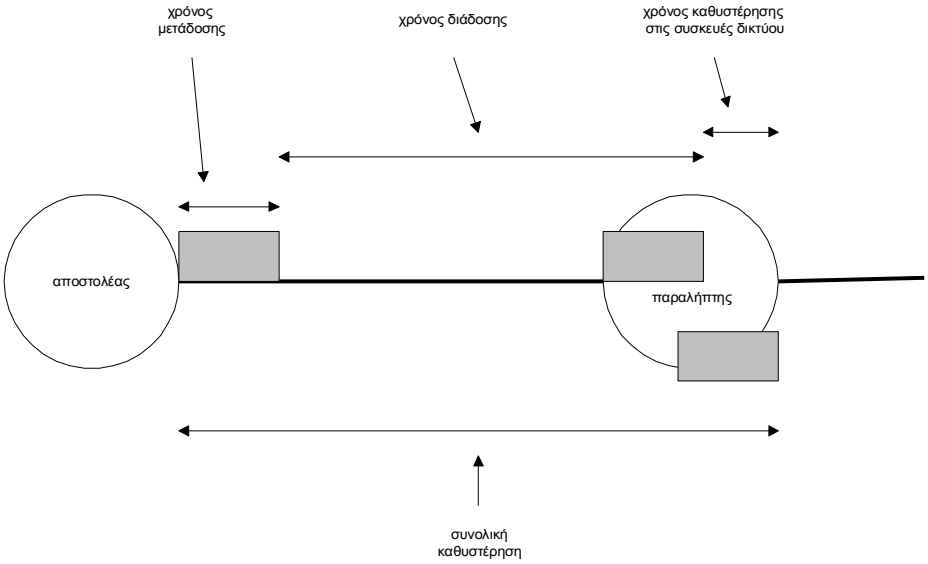
2.2 ΜΕΤΡΙΚΕΣ ΠΟΙΌΤΗΤΑΣ

Οι μετρικές που ενδιαφέρουν τις εφαρμογές που ζητούν ποιότητα υπηρεσίας στην εξυπηρέτηση τους είναι γενικά 4 και περιγράφονται αμέσως παρακάτω. Η σημαντικότερη μετρική που ενδιαφέρει και επηρεάζει τις εφαρμογές είναι η χωρητικότητα (bandwidth), που ορίζεται ως το πλήθος των δεδομένων, σε bits per second, που μεταδίδονται από ένα χρήστη στον άλλο. Το bandwidth χαρακτηρίζεται από 4 μεγέθη που είναι:

- Το μέγιστο μέγεθος καταιγισμού (maximum burst size), δηλαδή ο μέγιστος αριθμός πακέτων που μπορούν να βρεθούν στην ουρά του δρομολογητή χωρίς να απορριφθούν. Μία εφαρμογή που κατά τα άλλα συμπεριφέρεται μέσα στα προκαθορισμένα όρια, μπορεί για διάφορους λόγους να στείλει κάποια χρονική στιγμή δεδομένα με ρυθμό καταιγισμού.
- Η μέγιστη χωρητικότητα (peak bandwidth), δηλαδή η ανώτατη επιτρεπόμενη τιμή της χωρητικότητας που επιτρέπεται μία ροή να διατηρήσει σταθερή.
- Η ελάχιστη εγγυημένη χωρητικότητα (minimum guaranteed bandwidth)
- Η μέση χωρητικότητα (average bandwidth), δηλαδή η μέση τιμή της χωρητικότητας που υπολογίζεται διαιρώντας τον αριθμό των bytes που μεταδόθηκαν προς το συγκεκριμένο χρονικό διάστημα.

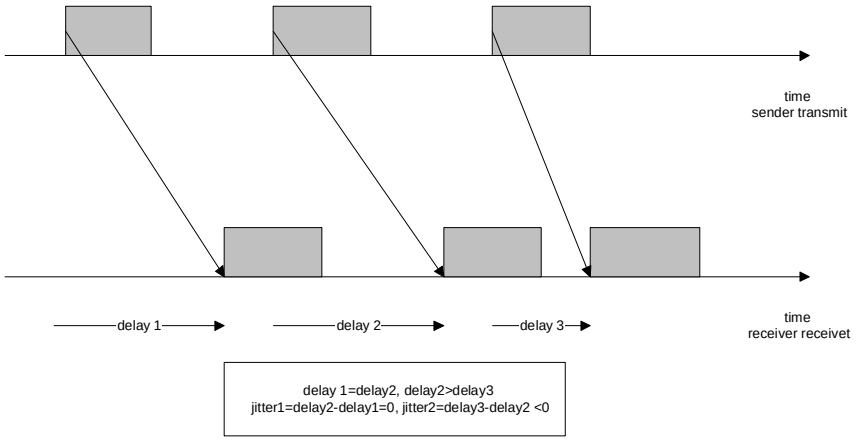
Η δεύτερη μετρική που ενδιαφέρει σχεδόν όλες τις εφαρμογές είναι η καθυστέρηση (delay), που ορίζεται ως ο χρόνος μεταξύ της μετάδοσης του πρώτου bit ενός IP πακέτου και της λήψης του τελευταίου bit αυτού του πακέτου από τον παραλήπτη. Ουσιαστικά η συνολική αυτή καθυστέρηση ισούται με το άθροισμα των καθυστερήσεων σε κάθε τμήμα του δικτύου. Η καθυστέρηση σε κάθε τμήμα του δικτύου είναι 3 ειδών και συγκεκριμένα:

- Χρόνος μετάδοσης, είναι δηλαδή ο χρόνος που απαιτείται για την τοποθέτηση πάνω σε μια γραμμή μετάδοσης όλων των bit του πακέτου και είναι ανάλογος της ταχύτητας της γραμμής
- Χρόνος διάδοσης, είναι ο χρόνος από τη μετάδοση του πρώτου (ή του τελευταίου bit του πακέτου) και τη λήψη αυτού του bit από τον παραλήπτη. Ο χρόνος αυτός εξαρτάται από την τεχνολογία μετάδοσης και την απόσταση.
- Χρόνος καθυστέρησης στις συσκευές του δικτύου. Η καθυστέρηση αυτή εισάγεται στα σημεία που λαμβάνουν πληροφορία και είναι ο χρόνος από τη λήψη τους μέχρι η πληροφορία να μεταδοθεί στην επόμενη συσκευή. Ο χρόνος αυτός αποτελείται από το χρόνο επεξεργασίας και το χρόνο που η πληροφορία παραμένει στην ουρά.



Εικόνα 1: Τα είδη της καθυστέρησης και η συνολική

Η επόμενη μετρική που χαρακτηρίζει την ποιότητα υπηρεσίας είναι το jitter (IP packet delay variation). Ουσιαστικά, το jitter αναφέρεται σε ζεύγη πακέτων και είναι η διαφορά μεταξύ της καθυστέρησης του πρώτου πακέτου από το δεύτερο. Όπως φαίνεται και από το Σχήμα 1, το jitter μεταξύ των πακέτων 1 και 2 ισούται με delay2-delay1 και μεταξύ των πακέτων 2 και 3 με delay3-delay2 αντίστοιχα. Πολλές εφαρμογές απαιτούν να έχουν ένα άνω όριο για το jitter προκειμένου η απόδοσή τους να είναι καλή.



Εικόνα 2: Η μετρική ποιότητας jitter

Τέλος, μια μετρική που ενδιαφέρει πολλές εφαρμογές είναι η απώλεια πακέτων (packet loss) και είναι ουσιαστικά το ποσοστό των πακέτων που μεταδόθηκαν από την πηγή και δεν λήφθηκαν από τον παραλήπτη ή παραλήφθηκαν με λάθη. Η απώλεια πακέτων προκαλείται είτε από απώλεια κάποιου link (συνδέσμου του δικτύου), είτε εξαιτίας προβλημάτων στη ρύθμιση των συσκευών του δικτύου είτε τέλος από συμφόρηση στο δίκτυο. Γενικά η επίδραση της απώλειας πακέτων στις εφαρμογές μπορεί να είναι καταστροφική υποβαθμίζοντας την απόδοσή τους. Επίσης σε πολλές εφαρμογές ενδεχόμενη αποστολή ξανά ενός χαμένου πακέτου δεν έχει

καμιά απολύτως σημασία και αντιθέτως δυσχεραίνει την λειτουργία της εφαρμογής παρά την βοηθά. Ένα παράδειγμα τέτοιας εφαρμογής είναι η τηλεδιάσκεψη.

2.3 ΤΥΠΟΙ QoS

2.3.1 Μηχανισμοί για QoS στο φυσικό επίπεδο

Το φυσικό επίπεδο αποτελείται από τη φυσική καλωδίωση και το μέσο μετάδοσης στο ίδιο το δίκτυο. Η δοκιμασμένη τακτική της κατασκευής διαφοροποιημένων μεταξύ τους φυσικών μονοπατιών σε ένα δίκτυο είναι μια πρώτη προσπάθεια για την παροχή διαφοροποιημένων επιπέδων υπηρεσιών. Σε ορισμένες περιπτώσεις διαφορετικά μονοπάτια κατασκευάζονται κυρίως για χρήση από το επίπεδο δικτύου, παρέχοντας διαθεσιμότητα επιπλέον links στις περιπτώσεις που το πρωτεύων φυσικό μονοπάτι χαθεί για κάποιο λόγο. Ωστόσο, πολλές φορές η χρήση όλου του διαθέσιμου εύρους ζώνης τόσο από το πρωτεύων όσο και από τα εναλλακτικά (backup) μονοπάτια φαίνεται ελκυστική. Στις περιπτώσεις αυτές βέβαια υπάρχει ο κίνδυνος η απόδοση να γίνει προβληματική. Ειδικότερα, αυτό μπορεί να παρατηρηθεί αν ένα αυθαίρετο τμήμα της κίνησης του δικτύου χρησιμοποιήσει το χαμηλής καθυστέρησης, μεγάλου εύρους ζώνης μονοπάτι και το υπόλοιπο τμήμα της κίνησης επιλέξει ένα backup μονοπάτι το οποίο μπορεί να έχει διαφορετικά χαρακτηριστικά εύρους ζώνης και καθυστέρησης. Μια τέτοια ρύθμιση οδηγεί σε μειωμένη αξιοπιστία και αυξημένο jitter, εκτός εάν το πρωτόκολλο δρομολόγησης έχει σχεδιαστεί προσεκτικά έτσι ώστε να σταθεροποιεί την τμηματοποίηση της κίνησης μεταξύ των δύο μονοπατιών.

2.3.2 Διαφοροποίηση φυσικών μονοπατιών

Παρ' όλο που η εισαγωγή επιπλέον φυσικών μονοπατιών σε ένα δίκτυο γίνεται συνήθως προκειμένου να εξασφαλιστεί backup μέσω πλεονασμού (redundancy), μπορεί επίσης να χρησιμοποιηθεί για την παροχή διαφοροποιημένων μεταξύ τους υπηρεσιών στις περιπτώσεις όπου τα διαθέσιμα μονοπάτια έχουν διαφορετικά χαρακτηριστικά.

Για παράδειγμα, η κίνηση καλύτερης προσπάθειας μπορεί να διοχετευτεί από τις συσκευές του επιπέδου δικτύου (δρομολογητές) στο μονοπάτι χαμηλότερης ταχύτητας, ενώ η κίνηση υψηλότερης προτεραιότητας (QoS) μπορεί να προωθηθεί στο μονοπάτι υψηλότερης ταχύτητας. Εναλλακτικά, το παραπάνω σενάριο μπορεί να υλοποιηθεί με ένα δορυφορικό μονοπάτι που συνοδεύεται από ένα γρηγορότερο επίγειο μονοπάτι μέσω καλωδίων. Η κυκλοφορία καλύτερης προσπάθειας διοχετεύεται μέσω του μεγαλύτερης καθυστέρησης δορυφορικού μονοπατιού, ενώ η κίνηση υψηλότερης προτεραιότητας δρομολογείται μέσω του συστήματος επίγειων καλωδίων. Η παραπάνω προσέγγιση είναι πρωτόγονη και έχει πολλά μειονεκτήματα.

2.3.3 Μηχανισμοί για QoS στο επίπεδο σύνδεσης

Η διαφοροποίηση στις υπηρεσίες που παρέχονται μέσω της κυκλοφορίας στα δίκτυα, επιτυγχάνεται κυρίως μέσω μηχανισμών στο επίπεδο σύνδεσης και πιο συγκεκριμένα με τη χρήση της τεχνολογίας ATM στα WANs.

Το ATM [2] είναι μια από τις τεχνολογίες μετάδοσης που παρέχουν ταχύτητες μετάδοσης δεδομένων μεγαλύτερες των 34Mbps. Εκτός από τους υψηλής ταχύτητας ρυθμούς bits, το ATM παρέχει ένα πολύπλοκο υποσύνολο από μηχανισμούς διαχείρισης της κυκλοφορίας, αποκατάστασης Virtual Circuits (VCs) και συσχετισμού των παραμέτρων για QoS με τα VCs αυτά. Ωστόσο αυτοί οι μηχανισμοί QoS μεταδόσεων δεν χρησιμοποιούνται από την πλειοψηφία των οργανισμών που χρησιμοποιούν το ATM σαν εργαλείο μετάδοσης δεδομένων για Internet δίκτυα. Το ATM χρησιμοποιείται κυρίως λόγω των μεγάλων ταχυτήτων μετάδοσης που υποστηρίζει και της ευελιξίας για πολύπλεξη που παρέχεται στις διάφορες ATM υλοποιήσεις.

2.4 Η ΕΙΣΟΔΟΣ ΤΟΥ MPLS

Το MPLS [27][37][56] αποτελεί μια εξελισσόμενη τεχνολογία η οποία μετατρέπει την αρχιτεκτονική της IP δρομολόγησης ενοποιώντας τη λειτουργικότητα των επιπέδων IP και σύνδεσης δεδομένων με στόχο τη βελτίωση της απόδοσης της προώθησης των IP πακέτων και την υποστήριξη εξελιγμένων χαρακτηριστικών του IP επιπέδου. Όταν συνδυάζεται με τα υπάρχοντα IP δίκτυα προσφέρει αξιοπιστία, ποιότητα υπηρεσίας, και χαρακτηριστικά προώθησης προσανατολισμένης στη σύνδεση των τεχνολογιών μεταγωγής δευτέρου επιπέδου, ενώ ταυτόχρονα διατηρεί την ευελιξία και τη δυνατότητα κλιμάκωσης της δρομολόγησης τρίτου επιπέδου.

Το MPLS διαφέρει σημαντικά από τις hop-by-hop μεθόδους επεξεργασίας των παραδοσιακών δικτύων. Στην παραδοσιακή IP δρομολόγηση, κάθε δρομολογητής παίρνει μια απόφαση προώθησης βασιζόμενος σε ολόκληρη την IP επικεφαλίδα και στη γνώση του δρομολογητή σχετικά με την τοπολογία του δικτύου. Αυτός ο μηχανισμός είναι αρκετά ανεπαρκής. Καθώς κάθε δρομολογητής γνωρίζει την τοπολογία του δικτύου, ένας ακραίος δρομολογητής μπορεί όχι μόνο να καθορίσει το επόμενο hop, αλλά και το μεθεπόμενο. Στην πραγματικότητα, ο ακραίος δρομολογητής θα μπορούσε να καθορίσει ολόκληρο το μονοπάτι. Το MPLS στηρίζεται σε αυτήν την αρχή χρησιμοποιώντας μια μικρή, σταθερού μήκους, εύκολα επεξεργάσιμη «ετικέτα» (20-bit) που καθορίζει το επόμενο hop δρομολογητή.

Το MPLS δεν ελέγχεται από τις εφαρμογές και δεν έχει κανένα στοιχείο πρωτοκόλλου τελικού host. Σε αντίθεση με τα άλλα πρωτόκολλα, το MPLS ανήκει μόνο στους δρομολογητές. Επιπλέον, το MPLS είναι ανεξάρτητο από τα πρωτόκολλα (multi-protocol), κι έτσι μπορεί να χρησιμοποιηθεί και με άλλα δικτυακά πρωτόκολλα εκτός από το IP (ATM, PPP, Frame-Relay, Ethernet και token ring) ή ακόμα και πάνω από το επίπεδο σύνδεσης δεδομένων. Συνδυάζει τη τεχνολογία μεταγωγής δευτέρου επιπέδου με τις δικτυακές υπηρεσίες τρίτου επιπέδου, ενώ παράλληλα μειώνει την πολυπλοκότητα και τα λειτουργικά κόστη.

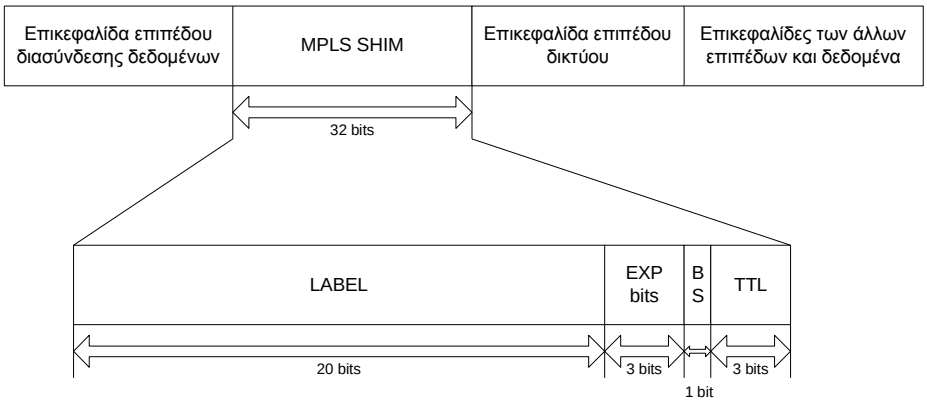
Αποτελεί μια τεχνολογία κλειδί για τα δίκτυα κορμού. Δίνει στους παροχείς υπηρεσιών τη δυνατότητα να προσφέρουν διαφοροποιημένες IP υπηρεσίες από άκρη σε άκρη απαιτώντας ταυτόχρονα απλούστερη διαμόρφωση και διαχείριση τόσο για τους παροχείς υπηρεσιών όσο και για τους πελάτες. Το MPLS δεν αντικαθιστά την IP δρομολόγηση, αλλά μπορεί να λειτουργήσει παράλληλα με υπάρχουσες και μελλοντικές τεχνολογίες δρομολόγησης με στόχο την προώθηση δεδομένων με υψηλή ταχύτητα και τη δέσμευση του εύρους ζώνης για ροές κυκλοφορίας με διαφορετικές απαιτήσεις.

Η σημασία του MPLS εγγυάται στο γεγονός ότι δίνει στα σύγχρονα δίκτυα τη δυνατότητα να αντιμετωπίσουν τις μεγάλες προκλήσεις που συναντούν στα ακόλουθα πεδία:

- Λειτουργικότητα: Παράδειγμα αποτελεί η ρητή δρομολόγηση (explicit routing)
- Κλιμάκωση (Scalability)
- Εξέλιξη: Δυνατότητα αλλαγής και επέκτασης των δικτύων αποφεύγοντας τη μεγάλη αποδιοργάνωση ή διακοπή τους.
- Ολοκλήρωση

Το MPLS είναι μια τεχνολογία που χρησιμοποιεί προώθηση που βασίζεται σε ετικέτες. Στο σημείο εισόδου, τα εισερχόμενα πακέτα επεξεργάζονται και επιλέγονται ετικέτες οι οποίες και εφαρμόζονται σε αυτά. Το δίκτυο κορμού απλά διαβάζει τις ετικέτες, εφαρμόζει τις κατάλληλες υπηρεσίες, και προωθεί τα πακέτα βάση της ετικέτας. Η αναλυτική επεξεργασία, η κατηγοριοποίηση και το 'φιλτράρισμα' λαμβάνουν χώρα μόνο μια φορά, στο σημείο εισόδου. Στο σημείο εξόδου, οι ετικέτες αφαιρούνται και τα πακέτα προωθούνται στον τελικό προορισμό τους.

Η ετικέτα είναι μια μικρή, σταθερού μήκους επικεφαλίδα (32-bit) που χρησιμοποιείται για την προώθηση των πακέτων. Η διάταξη της επικεφαλίδας εξαρτάται από τα χαρακτηριστικά του δικτύου. Στα ATM δίκτυα, η ετικέτα τοποθετείται εντός της virtual channel identifier/virtual path identifier (VCI/VPI) επικεφαλίδας του cell. Στο δίκτυο κορμού, οι δρομολογητές διαβάζουν μόνο την ετικέτα και όχι όλη την επικεφαλίδα του πακέτου. Ένα στοιχείο-κλειδί για τη διαβάθμιση του MPLS είναι ότι οι ετικέτες έχουν μόνο τοπική σημασία. Η διάταξη της MPLS ετικέτας φαίνεται παρακάτω.



Εικόνα 3: Η MPLS επικεφαλίδα

Η 32-bit MPLS ετικέτα τοποθετείται μετά την επικεφαλίδα του δευτέρου επιπέδου και πριν την IP επικεφαλίδα. Περιλαμβάνει τα ακόλουθα πεδία:

- Το πεδίο Label (20-bits) περιλαμβάνει την πραγματική τιμή του MPLS label.
- Το πεδίο CoS (3-bits) μπορεί να επηρεάσει τους αλγορίθμους χρονοδρομολόγησης και απόρριψης που εφαρμόζονται στο πακέτο καθώς αυτό μεταδίδεται μέσα στο δίκτυο. Ουσιαστικά αφορά λειτουργίες σχετικές με τις κλάσεις ποιότητας υπηρεσίας.
- Το πεδίο Stack (1-bit) υποστηρίζει μια ιεραρχική στοίβα ετικετών.

- Το πεδίο TTL (time-to-live) (8-bits) παρέχει τη συμβατική IP TTL λειτουργικότητα.

Ένα από τα σημαντικότερα πλεονεκτήματα του MPLS είναι το γεγονός ότι αποτελεί μια υλοποίηση βασισμένη σε πρότυπα της τεχνολογίας μεταγωγής ετικέτας. Η ανάπτυξη των προτύπων οδηγεί σε ένα ανοιχτό περιβάλλον όπου πολλαπλά προϊόντα διαφόρων κατασκευαστών μπορούν να συνυπάρξουν. Το MPLS αναμένεται να τύχει ευρείας βιομηχανικής υποστήριξης, αντικαθιστώντας εν τέλει τις υπάρχουσες λύσεις.

Τα σημαντικότερα πλεονεκτήματα του MPLS για τα σημερινά δίκτυα συνοψίζονται στα παρακάτω:

- Υποστήριξη πολλαπλών πρωτοκόλλων. Το MPLS μπορεί να υποστηρίξει πολλαπλά πρωτοκόλλα αφού οι κλάσεις ισοδύναμης προώθησης (FECs) μπορούν να βασίζονται σε πρωτόκολλα επιπέδου δικτύου και σε πληροφορίες που σχετίζονται με πρωτόκολλα δρομολόγησης. Αν και η αρχική προσπάθεια τυποποίησης του MPLS εστιάστηκε στα IPv4 και IPv6, η ομάδα εργασίας για το MPLS στοχεύει να επεκτείνει την υποστήριξη σε πρωτόκολλα επιπέδου δικτύου όπως τα IPX, AppleTalk, DECnet και CLNP.

- Ανεξαρτησία επιπέδου διασύνδεσης δεδομένων. Το MPLS προορίζεται για συνεργασία με κάθε τεχνολογία επιπέδου διασύνδεσης, όπως το ATM, το Frame Relay, το Packet-over-SONSET, το Ethernet (όλους τους τύπους, όπως το Gigabit Ethernet, κ.ά.), το Token Ring και το FDDI. Εντούτοις, οι ετικέτες για FEC ταξινόμηση σε καθεμιά από αυτές τις περιπτώσεις είναι εξαρτώμενες από το επίπεδο διασύνδεσης δεδομένων που επιλέγεται κάθε φορά.

- Αυξημένη απόδοση. Το MPLS καθιστά ικανή την υψηλότερη απόδοση λόγω της απλοποιημένης προώθησης πακέτων και των αποφάσεων μεταγωγής. Οι δρομολογητές που βασίζονται στο MPLS μπορούν να υλοποιήσουν δυνατότητες αναζήτησης και προώθησης χρησιμοποιώντας hardware τεχνικές.

- Ρητή δρομολόγηση. Ένα από τα σημαντικότερα χαρακτηριστικά του MPLS είναι η υποστήριξη ρητών διαδρομών. Μολονότι αυτό είναι παρόμοιο με την IP δρομολόγηση προέλευσης (source routing), το πλεονέκτημα του MPLS είναι ότι δεν υπάρχει η επιβάρυνση της επεξεργασίας των επικεφαλίδων για κάθε πακέτο. Επιπρόσθετα, οι ρητές διαδρομές παρέχουν επίσης κάποια από τη λειτουργικότητα που χρειάζεται για έλεγχο κυκλοφορίας, δρομολόγηση με βάση απαιτήσεις για ποιότητα υπηρεσίας κ.λπ.

- Εξέλιξη. Το MPLS έχει το πλεονέκτημα του διαχωρισμού των λειτουργιών ελέγχου και προώθησης. Κάθε τμήμα μπορεί να αναπτυχθεί και να εξελιχθεί χωρίς να επηρεάζει το άλλο, γεγονός που καθιστά την εξέλιξη των δικτύων πιο εύκολη, με λιγότερο κόστος, και λιγότερο ευάλωτη σε λάθη. Επίσης, προσφέρει «μεταφορά» και υποστήριξη των λειτουργιών QoS του επιπέδου 3 ώστε να επιτυγχάνεται ομοιογένεια ανεξαρτήτως των πρωτοκόλλων χαμηλότερων επιπέδων.

- Έλεγχος κυκλοφορίας. Ο έλεγχος κυκλοφορίας αναφέρεται στην διαδικασία της επιλογής των μονοπατιών για την κυκλοφορία των δεδομένων ώστε να εξισορροπηθεί ο φόρτος της κυκλοφορίας σε διάφορες συνδέσεις, δρομολογητές, και μεταγωγείς μέσα στο δίκτυο. Αυτό έχει ολοένα αυξανόμενη σπουδαιότητα εξαιτίας της αστραπιαίας ανάπτυξης του Internet και την αντίστοιχη απαίτηση για εύρος ζώνης.

Παράλληλα, το MPLS διαθέτει ορισμένα εγγενή πλεονεκτήματα σε ότι αφορά τον έλεγχο κυκλοφορίας:

- Τα ρητά μονοπάτια μεταγωγής ετικέτας μπορούν να συσχετίζονται με κάποια από τις πολλές ιδιότητες κυκλοφορίας που υπάρχουν στο MPLS για την υποστήριξη διαφορετικών τύπων κυκλοφορίας.
- Οι βασικές λειτουργίες όπως η δημιουργία, ενεργοποίηση, απενεργοποίηση, μεταβολή ιδιοτήτων, επανα-δρομολόγηση και καταστροφή γραμμής κυκλοφορίας μπορούν να εκτελεστούν σε ένα ρητό μονοπάτι μεταγωγής ετικέτας.
- Η ροή δεδομένων από οποιοδήποτε κόμβο εισόδου σε οποιοδήποτε κόμβο εξόδου μπορούν να προσδιοριστούν αυτόνομα. Κάτι τέτοιο παρέχει ένα σαφή μηχανισμό για τη μέτρηση της ροής κυκλοφορίας μεταξύ ζεύγους κόμβων εισόδου-εξόδου και γι' αυτό ικανοποιεί τις υπολογιστικές απαιτήσεις του ελέγχου κυκλοφορίας.
- Συνάθροιση ροών. Κανονικά, όταν πρέπει να συσσωρευτούν πολλαπλές ροές δεδομένων για προώθηση σε ένα μονοπάτι μεταγωγής, απαιτείται επεξεργασία τόσο στο επίπεδο διασύνδεσης δεδομένων όσο και στο επίπεδο δικτύου. Στο MPLS, εντούτοις, μπορεί να χρησιμοποιηθεί ο μηχανισμός στοίβας ετικετών για να εκτελεστεί η συνάθροιση μόνο εντός του δευτέρου επιπέδου. Η κορυφαία ετικέτα της στοίβας ετικετών του MPLS χρησιμοποιείται για τη μεταγωγή πακέτων κατά μήκος του LSP. Το υπόλοιπο της στοίβας ετικετών εξαρτάται από την εφαρμογή και θα μπορούσε να χρησιμοποιηθεί για τη μεταγωγή πακέτων στην είσοδο και στην έξοδο του LSP. Τα ιδιωτικά ιδεατά δίκτυα (VPNs) είναι μια από τις εφαρμογές που χρησιμοποιεί ο μηχανισμός της στοίβας ετικετών.
- Η επεκτασιμότητα της δρομολόγησης του επιπέδου δικτύου. Μια από τις βασικές απαιτήσεις που ελήφθησαν υπόψη στον σχεδιασμό του MPLS ήταν να επιτευχθεί μια καλύτερη και αποτελεσματικότερη μεταφορά των πακέτων δεδομένων των υπαρχόντων IP δικτύων. Σήμερα, ένας αριθμός από τα υπάρχοντα IP δίκτυα αναβαθμίζονται με ATM για αυξημένη απόδοση. Εντούτοις, επειδή αυτό συνεπάγεται ένα μοντέλο επικάλυψης, ανακύπτουν προβλήματα επεκτασιμότητας, απόδοσης δικτύου και επιβαρύνσεις στη διαχείριση. Συνδυάζοντας τις γνώσεις για τη δρομολόγηση στο τρίτο επίπεδο με την ικανότητα της ATM μεταγωγής σε ATM συσκευές πετυχαίνεται μια καλύτερη λύση. Σε αυτό το μοντέλο, δεν υπάρχει η επιβάρυνση της δημιουργίας ελέγχου του VC και της συντήρησής του, το πλήθος των γειτονικών συνδέσεων είναι μικρότερο και οι πίνακες δρομολόγησης είναι μικρότεροι σε μέγεθος.

2.5 ΜΗΧΑΝΙΣΜΟΙ ΓΙΑ QoS ΣΤΑ ΕΠΙΠΕΔΑ ΔΙΚΤΥΟΥ ΚΑΙ ΜΕΤΑΦΟΡΑΣ

Στο μεγαλύτερο τμήμα του Διαδικτύου ο βασικός φορέας υπηρεσιών είναι η οικογένεια πρωτοκόλλων TCP/IP και το καθολικά κοινό πρωτόκολλο είναι το IP. Η χρήση του πρωτοκόλλου αυτού για την εφαρμογή μηχανισμών QoS, φαίνεται να οδηγεί σε μια μεγαλύτερη πιθανότητα για την επιτυχή παροχή πραγματικής ποιότητας υπηρεσίας αφού η εφαρμογή, διαχείριση και αντιμετώπιση λαθών μπορούν να γίνουν πάνω σε μια κοινή βάση.

Συμβαίνει επίσης η τεχνολογία αυτή του IP να λειτουργεί πάνω σε μια από άκρο σε άκρο φιλοσοφία, χρησιμοποιώντας ένα μηχανισμό σηματοδοσίας που εκτείνεται σε

όλο το δίκτυο με ομοιόμορφο τρόπο. Το IP είναι η υπηρεσία από άκρου σε άκρο μεταφοράς στις περισσότερες περιπτώσεις, οπότε παρ' όλο που όπως φάνηκε στις προηγούμενες παραγράφους είναι δυνατόν να υλοποιηθούν QoS υπηρεσίες στα κατώτερα επίπεδα της στοίβας πρωτοκόλλων, οι υπηρεσίες αυτές καλύπτουν μόνο ένα τμήμα του από άκρο σε άκρο μονοπατιού δεδομένων. Αυτές οι ατελείς προσπάθειες συχνά υποβαθμίζονται από την αλλοίωση της σηματοδοσίας, η οποία προκαλείται από τα τμήματα του από άκρο σε άκρο μονοπατιού που δεν καλύπτονται από την QoS υπηρεσία, οπότε το συνολικό αποτέλεσμα μιας μη-καθολικής QoS δομής είναι γενικά μη ικανοποιητικό.

Όταν το από άκρο σε άκρο μονοπάτι δεν αποτελείται από ένα ομοιογενές επίπεδο διασύνδεσης δεδομένων, κάθε προσπάθεια για την παροχή διαφοροποιημένων υπηρεσιών μέσα στα πλαίσια μιας συγκεκριμένης τεχνολογίας του επιπέδου διασύνδεσης δεν θα έχει τα αναμενόμενα αποτελέσματα. Στο Διαδίκτυο για παράδειγμα, ένα IP πακέτο μπορεί να διανύσει οποιοδήποτε αριθμό από ανομοιογενή μονοπάτια του επιπέδου διασύνδεσης, κάθε ένα από τα οποία μπορεί να χρησιμοποιεί χαρακτηριστικά που εγγενώς παρέχουν μεθόδους για την παροχή διαφοροποίησης της κίνησης. Ωστόσο το πακέτο μπορεί επίσης να διανύσει συνδέσμους του δικτύου που δεν μπορούν να παρέχουν κανενός είδους διαφοροποίηση υπηρεσιών στο επίπεδο διασύνδεσης, όποτε η παροχή QoS καθίσταται ανεπαρκής.

Το συμπέρασμα είναι ότι κανενός είδους μηχανισμός στα επίπεδα μεταφοράς και δικτύου δεν μπορεί να προσφέρει τη δυνατότητα για διαφοροποίηση υπηρεσιών σε όλα τα είδη ροής δεδομένων και ότι ένα QoS δίκτυο πρέπει να αναπτύσσει έναν αριθμό από μηχανισμούς για την αντιμετώπιση του μεγάλου εύρους απαιτήσεων των χρηστών. Η IETF (Internet Engineering Task Force) έχει προτείνει διάφορα μοντέλα και μηχανισμούς για την επίτευξη QoS. Τα πιο σημαντικά μοντέλα είναι :

- Integrated services με χρήση του Resource Reservation Protocol (RSVP) [15][43][99]. Στην περίπτωση αυτή πραγματοποιείται κράτηση πόρων (resource reservation), όπου οι πόροι του δικτύου διατίθενται με βάση τις ανάγκες των εφαρμογών. Πιο συγκεκριμένα για κάθε πελάτη (η συνένωση πελατών) που επιθυμεί κάποια ποιότητα υπηρεσίας γίνεται στο δίκτυο κράτηση πόρων ώστε να εξυπηρετούνται οι ανάγκες του.
- Differentiated Service Architecture (DS) [47][98]. Στην περίπτωση αυτή γίνεται διάκριση των πακέτων και παρέχεται προτεραιότητα σε ορισμένα από αυτά. Η κίνηση του δικτύου διαχωρίζεται και οι πόροι διανέμονται δίκαια με βάση τα κριτήρια αστυνόμευσης και διαχείρισης του bandwidth. Προκειμένου να επιτευχθεί ποιότητα στην υπηρεσία, οι διαχωρισμοί (classifications) που έχουν μεγαλύτερες απαιτήσεις απολαμβάνουν προνομιακή μεταχείριση από το δίκτυο.

2.5.1 Η αρχιτεκτονική Integrated Service (IntServ)

Ο οργανισμός Internet Engineering Task Force (IETF), ανταποκρινόμενος στην απαίτηση για ανάπτυξη ολοκληρωμένων υπηρεσιών στο Διαδίκτυο, προχώρησε στην ανάπτυξη της αρχιτεκτονικής Ολοκληρωμένων Υπηρεσιών (Integrated Services architecture ή εν συντομία IntServ). Η αρχιτεκτονική IntServ σχεδιάστηκε αρχικά για να παρέχει ένα σύνολο προεκτάσεων στο παραδοσιακό μοντέλο μετάδοσης «καλύτερης προσπάθειας» (best effort) του Διαδικτύου. Στόχος της ήταν να παρέχει κάποια ιδιαίτερη μεταχείριση σε ορισμένους τύπους κυκλοφορίας / κίνησης και να

παρέχει ένα μηχανισμό στις εφαρμογές ώστε αυτές να έχουν τη δυνατότητα να επιλέξουν ανάμεσα σε πολλά επίπεδα υπηρεσιών μετάδοσης.

Η βασική ιδέα της αρχιτεκτονικής IntServ είναι ότι δεν απαιτείται να τροποποιηθεί η βασική υποκείμενη αρχιτεκτονική του Διαδικτύου, αλλά αρκεί να προστεθούν κάποιες προεκτάσεις που θα παρέχουν υπηρεσίες πέρα από την παραδοσιακή υπηρεσία «καλύτερης προσπάθειας» (best effort). Η ομάδα εργασίας του μοντέλου IntServ έχει εστιάσει στους εξής στόχους:

Στον ξεκάθαρο καθορισμό των υπηρεσιών που θα παρέχονται. Δηλαδή στον καθορισμό και την τεκμηρίωση αυτού του νέου και βελτιωμένου μοντέλου υπηρεσιών του Διαδικτύου.

Στον καθορισμό των υπηρεσιών στο επίπεδο της εφαρμογής, του χρονοπρογραμματισμού των δρομολογητών του Διαδικτύου σχετικά με την δέσμευση των δικτυακών πόρων, και των διασυνδέσεων των δρομολογητών μεταξύ τους (Link Layer).

Στην ανάπτυξη απαιτήσεων εγκυρότητας στους δρομολογητές του Διαδικτύου για να εξασφαλίζεται η παροχή της κατάλληλης υπηρεσίας. Το Διαδίκτυο θα συνεχίσει να περιέχει ένα ετερογενές σύνολο δρομολογητών, να τρέχει διάφορα πρωτόκολλα δρομολόγησης και να χρησιμοποιεί διαφορετικούς αλγορίθμους δρομολόγησης. Για αυτό η ομάδα εργασίας πρέπει να θέσει κάποιες απαιτήσεις στους δρομολογητές που θα εξασφαλίζουν ότι το Διαδίκτυο μπορεί να υποστηρίξει το νέο μοντέλο υπηρεσιών.

Ο όρος εγγύηση ποιότητας υπηρεσίας (Quality of Service – QoS) στο περιβάλλον του IntServ αναφέρεται στη φύση της υπηρεσίας μετάδοσης πακέτων που παρέχεται από το δίκτυο, όπως αυτή χαρακτηρίζεται από παραμέτρους όπως το εύρος ζώνης, η καθυστέρηση μετάδοσης πακέτων και ο ρυθμός απώλειας πακέτων. Κόμβος του δικτύου θεωρείται κάθε συνιστώσα του δικτύου που χειρίζεται πακέτα δεδομένων και έχει τη δυνατότητα επιβολής ελέγχου ποιότητας υπηρεσίας στα δεδομένα που ρέουν διαμέσου της. Στους κόμβους συμπεριλαμβάνονται οι δρομολογητές, τα τελικά συστήματα και τα υποδίκτυα. Ένας IntServ - capable κόμβος είναι ένας κόμβος του δικτύου που μπορεί να παρέχει μία ή περισσότερες υπηρεσίες του μοντέλου IntServ. Ένας IntServ - aware κόμβος είναι ένας κόμβος του δικτύου που υποστηρίζει τις συγκεκριμένες διασυνδέσεις που απαιτούνται από το μοντέλο αλλά που δε μπορεί να παρέχει τη ζητούμενη υπηρεσία. Παρόλο που ένας IntServ - aware κόμβος δε μπορεί να παρέχει καμία από τις υπηρεσίες QoS, μπορεί απλά να κατανοεί τις παραμέτρους της ζητούμενης υπηρεσίας και να απαντάει αρνητικά σε αυτές τις αιτήσεις.

Σημαντικό ρόλο στο μοντέλο IntServ παίζει η έννοια του ελέγχου των πόρων. Οι πόροι του δικτύου (π.χ. εύρος ζώνης) πρέπει να ελέγχονται ώστε να επιτευχθεί το επιθυμητό επίπεδο ποιότητα υπηρεσίας. Μια θεμελιώδης αρχή του μοντέλου IntServ είναι ότι η κυκλοφορία που διαχειρίζεται από αυτό το μοντέλο πρέπει να υπόκειται σε μηχανισμούς ελέγχου αποδοχής. Επίσης, εκτός από τον έλεγχο αποδοχής, το μοντέλο IntServ φροντίζει για ένα μηχανισμό δέσμευσης πόρων. Οι εφαρμογές πραγματικού χρόνου δε μπορούν να ικανοποιηθούν χωρίς εγγυήσεις πόρων, και οι εγγυήσεις πόρων δε μπορούν να γίνουν χωρίς δέσμευση πόρων. Για την υλοποίηση αυτού του μηχανισμού δέσμευσης πόρων χρησιμοποιείται ένα πρωτόκολλο, όπως το RSVP (Resource Reservation Setup Protocol). Σκοπός του πρωτοκόλλου αυτού είναι να αποτελεί το μέσο καθορισμού των πόρων του δικτύου που απαιτούνται για την επίτευξη της απαιτούμενης ποιότητας υπηρεσίας. Η λογική του RSVP είναι πως πρέπει κατά μήκος όλης της διαδρομής που ακολουθούν τα πακέτα, να γίνουν

δεσμεύσεις πόρων σύμφωνα με τις ανάγκες της κάθε εφαρμογής. Η διαδικασία δέσμευσης πόρων είναι ακολουθιακή και ο πρώτος δρομολογητής στέλνει κατάλληλο μήνυμα στον επόμενο όπου ζητά δέσμευση πόρων. Η διαδικασία αυτή εξελίσσεται μέχρι να φτάσει στον παραλήπτη, ο οποίος τότε στέλνει στην αντίθετη διαδρομή επιβεβαιώσεις κράτησης. Οι IntServ υπηρεσίες που έχουν προταθεί έως σήμερα είναι η Guaranteed, που είναι η πλησιέστερη δυνατή στα αφιερωμένα ιδεατά κυκλώματα (dedicated virtual circuits) και η Controlled Load που είναι ισοδύναμη με την υπηρεσία καλύτερης προσπάθειας σε συνθήκες έλλειψης φόρτου.

2.5.1.1 Το πρωτόκολλο RSVP

Το RSVP (Resource ReSerVation Protocol) πρωτόκολλο [15] αποτελεί μέρος μιας ευρύτερης προσπάθειας να αξιοποιηθεί η υπάρχουσα υποδομή του Διαδικτύου προσφέροντας υποστήριξη για QoS (Quality of Service) στις υπηρεσίες. Το πρωτόκολλο RSVP χρησιμοποιείται από ένα κόμβο-χρήστη προκειμένου να απαιτήσει από το δίκτυο συγκεκριμένη ποιότητα για ροή δεδομένων συγκεκριμένων εφαρμογών. Το RSVP χρησιμοποιείται από δρομολογητές ώστε αυτοί να μεταφέρουν τις συγκεκριμένες QoS απαιτήσεις σε όλους τους κόμβους του μονοπατιού της ροής των δεδομένων αλλά και να εξασφαλίσουν ότι όντως αυτές οι συγκεκριμένες απαιτήσεις πληρούνται.

Το RSVP αποτελεί ένα πρωτόκολλο για multicasting και unicasting σηματοδότηση το οποίο σχεδιάστηκε για την εγκατάσταση και την συντήρηση σταθμών πληροφοριών σε κάθε δρομολογητή που βρίσκεται στο μονοπάτι μετάδοσης δεδομένων, κατά την μετάδοση δεδομένων. Το RSVP επιτρέπει στον παραλήπτη να ζητήσει μία ορισμένη από άκρο σε άκρο ποιότητα υπηρεσίας. Οι εφαρμογές πραγματικού χρόνου χρησιμοποιούν το RSVP για να δεσμεύσουν τους απαραίτητους πόρους στους δρομολογητές κατά μήκος του μονοπατιού μετάδοσης, έτσι ώστε να είναι διαθέσιμη η απαιτούμενη χωρητικότητα όταν λάβει χώρα η μετάδοση των πολυμεσικών δεδομένων. Κατά συνέπεια, το RSVP είναι ένα πρωτόκολλο ελέγχου δικτύου που καθιστά τις διαδικτυακές εφαρμογές ικανές να αποκτήσουν QoS χαρακτηριστικά. Το RSVP καταλαμβάνει τη θέση ενός πρωτοκόλλου μεταφοράς στο μοντέλο OSI των 7 επιπέδων, παρόλο που το ίδιο το RSVP δεν μεταφέρει τα δεδομένα.

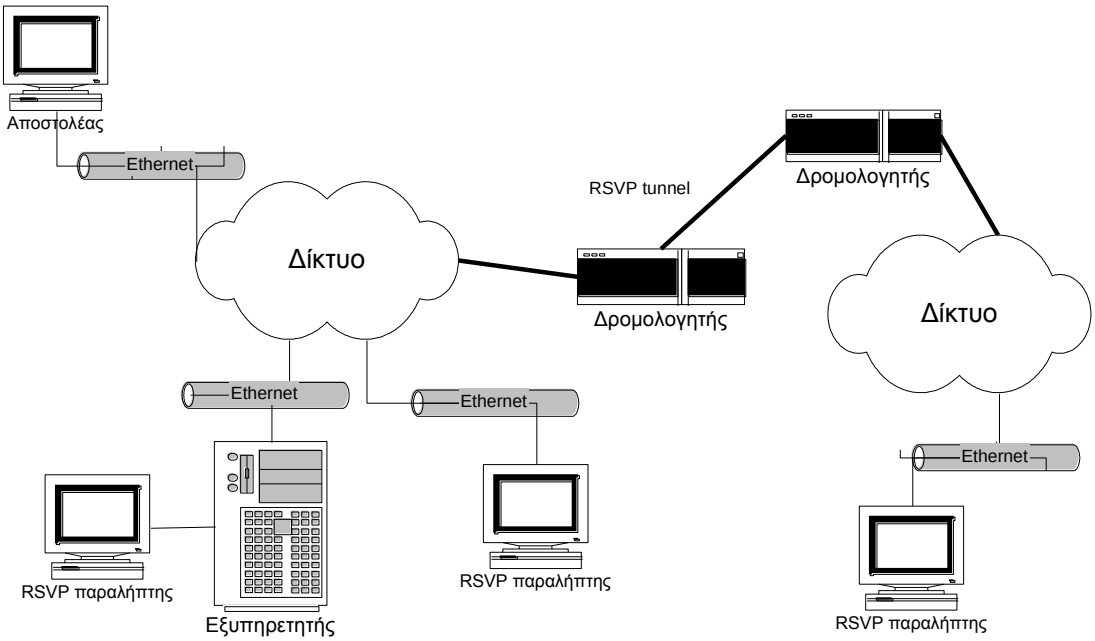
Για τη μετάδοση δεδομένων πολυμέσων πάνω από ένα δίκτυο είναι αναγκαίο να ικανοποιούνται τρία βασικά χαρακτηριστικά :

1. Η μεταφορά των δεδομένων να γίνεται με όσο το δυνατό πιο γρήγορο τρόπο.
2. Να παρέχεται δυνατότητα multicasting.
3. Να υπάρχει δυνατότητα για εξασφάλιση στην μεταφορά των δεδομένων με βάση τις απαιτήσεις που έχει ορίσει εκ των προτέρων ο χρήστης.

Τα δεδομένα πολυμέσων είναι μεγάλα σε όγκο και επομένως αποδοτικοί μηχανισμοί αποστολής τέτοιων δεδομένων πρέπει να παρέχονται. Το RSVP δείχνει περισσότερο ενδιαφέρον στη διατήρηση των παρεχόμενων πόρων και δεν μπορεί να επέμβει στη δρομολόγηση των δεδομένων που έχουν αποσταλεί.

Η 1η έκδοση του RSVP καθορίζεται από το RFC 2205 και η IETF (Internet Engineering Task Force) έχει καταλήξει στην καθιέρωση των τεχνικών προδιαγραφών του πρωτοκόλλου σαν ένα Internet Proposed Standard. Το RSVP προέκυψε από τη συνεργασία μίας ομάδας ερευνητικών κέντρων: Xerox, Palo Alto

Research Center (PARK), MIT, και του Information Sciences Institute of University California (ISI).

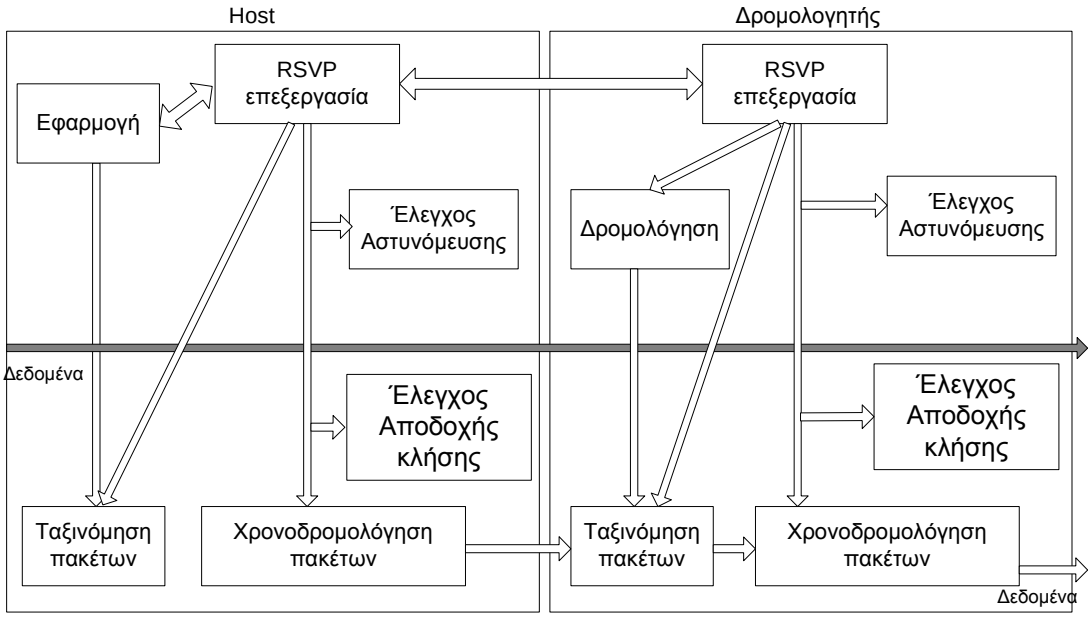


Εικόνα 4: Δικτυακό σχεδιάγραμμα συστημάτων που χρησιμοποιούν RSVP

Η παροχή του QoS στο RSVP, υλοποιείται για μια συγκεκριμένη ροή δεδομένων με μηχανισμούς ελέγχου κυκλοφορίας. Αυτοί οι μηχανισμοί περιλαμβάνουν τους παρακάτω μηχανισμούς:

- Admission Control (Έλεγχος αποδοχής): Ο μηχανισμός admission control αποφασίζει αν ο κόμβος μπορεί να ικανοποιήσει το απαιτούμενο QoS.
- Policy Control (Έλεγχος πολιτικής): Ο μηχανισμός policy control αποφασίζει αν ο χρήστης έχει την άδεια (π.χ. αν είναι διαχειριστής του δικτύου) να κάνει την δέσμευση.
- Packet Scheduler (Χρονοδρομολογητής πακέτων): Ο packet scheduler καθορίζει τη κλάση του QoS, και πιθανόν τη δρομολόγηση, για κάθε πακέτο. Ο packet scheduler είναι αυτός που επιτυγχάνει το επιθυμητό επίπεδο QoS.
- Packet Classifier (Ταξινομητής πακέτων): Ο packet classifier καθορίζει την κλάση QoS για κάθε πακέτο.

Οι μηχανισμοί του RSVP πρωτοκόλλου παρέχουν τη δυνατότητα δημιουργίας και συντήρησης κατανεμημένης δέσμευσης κατά μήκος ενός μεγάλου αριθμού multicast και unicast μονοπατιών. Το RSVP μεταφέρει και χειρίζεται τις παραμέτρους του QoS και του policy control σαν απλά δεδομένα μεταφέροντας τα στις αντίστοιχες ρουτίνες (modules) του μηχανισμού για επεξεργασία. Καθώς είναι πολύ πιθανό, η συμμετοχή σε μια multicast ομάδα να αλλάζει με τη πάροδο κάποιου χρονικού διαστήματος, το RSVP υποστηρίζει, αν αυτό είναι επιθυμητό, την αποστολή περιοδικών μηνυμάτων προκειμένου να συντηρήσει την κατάσταση σε όλα τα δεσμευμένα μονοπάτια.



Εικόνα 5: Σχηματική αναπαράσταση αρχιτεκτονικής του RSVP

Το RSVP πρωτόκολλο έχει τα παρακάτω χαρακτηριστικά:

- Η ροή δεδομένων στο RSVP είναι μονής κατεύθυνσης. Το πρωτόκολλο διαχωρίζει τους αποστολείς από τους παραλήπτες. Παρόλο που σε πολλές περιπτώσεις ο αποστολέας μπορεί να είναι και παραλήπτης, το RSVP δεσμεύει πόρους μόνο προς τη μία κατεύθυνση.
- Το RSVP υποστηρίζει και multicast και unicast και προσαρμόζεται στις συνεχείς αλλαγές ενός δυναμικού περιβάλλοντος. Δηλαδή, επιτρέπεται η δυναμική σύνδεση και αποσύνδεση παραληπτών σε multicast σύνοδο. Παρέχει μια πληθώρα μοντέλων και "μορφών" (styles) ώστε να εξυπηρετεί μια μεγάλη ποικιλία εφαρμογών.
- Το RSVP είναι προσανατολισμένο προς τον αποδέκτη (receiver-oriented) και μπορεί να χειριστεί διαφορετικές κατηγορίες παραληπτών. Ο κάθε παραλήπτης είναι υπεύθυνος για να διαλέξει το δικό του επίπεδο QoS. Ο αποστολέας διαχωρίζει την κίνηση σε ξεχωριστές ροές, μία για κάθε διαφορετικό επίπεδο QoS.
- Το RSVP είναι συμπληρωματικό του IP ελέγχοντας τον τρόπο με τον οποίο το IP μεταδίδει τα πακέτα του. Προορίζεται κυρίως για έλεγχο των δεδομένων που αποστέλλονται και όχι για μεταφορά δεδομένων. Είναι αναγκαίο να υπάρχει ενημέρωση για τους διαθέσιμους πόρους πριν γίνουν αλλαγές στην δρομολόγηση.
- Χρησιμοποιώντας το RSVP ένας αποστολέας δε γνωρίζει ποιοι παραλαμβάνουν τα δεδομένα που αποστέλλει.
- Το RSVP έχει καλή συμβατότητα. Τρέχει πάνω από IPv4 και IPv6. Επίσης, λειτουργεί ακόμα και όταν ένας δρομολογητής στο μονοπάτι ροής δεδομένων δεν το υποστηρίζει με την χρήση τεχνικής tunneling (απλά τα RSVP μηνύματα "περνάνε" χωρίς να υπόκεινται σε επεξεργασία).

2.5.1.2 Τρόπος λειτουργίας του RSVP

Για να εγκαθιδρύσουμε μια RSVP multicast σύνοδο πρώτα "ενώνεται" ο παραλήπτης με τη multicast ομάδα η οποία ορίζεται από μια IP διεύθυνση προορισμού κάνοντας χρήση του πρωτοκόλλου Internet Group-Membership Protocol (IGMP). Στην περίπτωση μιας unicast συνοδού, η unicast δρομολόγηση εξυπηρετεί τη λειτουργία του IGMP. Αφότου ο παραλήπτης συμμετέχει στην ομάδα, ένας δυνητικός αποστολέας αρχίζει να στέλνει RSVP μηνύματα μονοπατιού στην IP διεύθυνση προορισμού. Όταν η εφαρμογή, η οποία λαμβάνει τα μηνύματα, δέχεται ένα μήνυμα μονοπατιού αρχίζει να στέλνει κατάλληλα μηνύματα αίτησης-δέσμευσης καθορίζοντας τους επιθυμητούς περιγραφείς ροής που χρησιμοποιούν το RSVP. Αφού η εφαρμογή αποστολέας δεχτεί ένα μήνυμα αίτησης-δέσμευσης, ο αποστολέας ξεκινάει να στέλνει πακέτα δεδομένων.

Όταν μία εφαρμογή απαιτεί μία συγκεκριμένη ποιότητα υπηρεσίας, χρησιμοποιεί το πρωτόκολλο αυτό για να στείλει την απαίτηση της σε όλους τους δρομολογητές κατά μήκος του μονοπατιού μετάδοσης. Αν δεσμευτούν οι κατάλληλοι πόροι, το RSVP είναι υπεύθυνο για διατήρηση των πόρων αυτών.

Το policy control καθορίζει αν ο χρήστης έχει το δικαίωμα να δεσμεύσει πόρους. Στο μέλλον, η διαδικασία αυτή θα περιλαμβάνει έλεγχο ταυτότητας, έλεγχο πρόσβασης και χρέωση. Το admission control ελέγχει τους πόρους και αποφασίζει για το αν ο κόμβος έχει αρκετούς πόρους για να υποστηρίξει την απαιτούμενη ποιότητα υπηρεσίας (QoS).

Το RSVP daemon (το πρόγραμμα που τρέχει στον κόμβο και υλοποιεί το RSVP πρωτόκολλο) πραγματοποιεί ελέγχους με βάση τις δύο αυτές διαδικασίες. Αν κάποιος από τους δύο ελέγχους αποτύχει, το RSVP πρόγραμμα επιστρέφει ένα error notification στην εφαρμογή που έκανε την αίτηση. Αν και οι δύο έλεγχοι είναι επιτυχημένοι, το RSVP daemon θέτει παραμέτρους στον packet classifier και στον packet scheduler έτσι ώστε να επιτευχθεί η ζητούμενη ποιότητα. Ο packet classifier καθορίζει την κλάση QoS για κάθε πακέτο και ο packet scheduler καθορίζει τη μετάδοση των πακέτων με στόχο την επίτευξη της ζητούμενης QoS για κάθε ροή.

Το RSVP daemon επικοινωνεί επίσης με τη διαδικασία δρομολόγησης, για τον καθορισμό του μονοπατιού το οποίο θα ακολουθήσουν οι αιτήσεις δέσμευσης. Η δέσμευση γίνεται μέσω δύο τύπων μηνυμάτων του RSVP, τα PATH και τα RESV μηνύματα.

Τα PATH μηνύματα στέλνονται ανά τακτά χρονικά διαστήματα από τον αποστολέα στους παραλήπτες και περιλαμβάνουν το προφίλ των δεδομένων (data format, source address, source port) και άλλα χαρακτηριστικά για τη μεταφορά τους. Την πληροφορία αυτή χρησιμοποιούν οι παραλήπτες για να βρουν το αντίστροφο μονοπάτι προς τον αποστολέα και να προσδιορίσουν τους πόρους που πρέπει να δεσμευτούν.

Τα RESV μηνύματα δημιουργούνται από τους παραλήπτες και περιέχουν παραμέτρους για τη δέσμευση στις οποίες περιλαμβάνονται οι flow spec και filter spec. Η παράμετρος filter spec ορίζει ποια πακέτα πρέπει να χρησιμοποιηθούν από τον packet classifier. Η παράμετρος flow spec χρησιμοποιείται από τον packet scheduler. Τα RESV μηνύματα ακολουθούν το ακριβώς αντίθετο μονοπάτι των PATH μηνυμάτων.

Η δέσμευση που κάνει στους δρομολογητές το RSVP καλείται soft states. Το RSVP daemon πρέπει ανά τακτά χρονικά διαστήματα να ανανεώνει τα μηνύματα έτσι ώστε να διατηρούνται οι δεσμευμένοι πόροι. Το γεγονός όμως αυτό καθιστά πιο εύκολες τις αλλαγές που είναι δυνατό να προκύψουν σε ένα δυναμικό περιβάλλον.

Οι αιτήσεις για δέσμευση αρχικοποιούνται από τους παραλήπτες. Δε χρειάζεται όλες οι αιτήσεις να ταξιδέψουν όλη τη διαδρομή μέχρι τον αποστολέα. Αντί γι' αυτό, οι ροές που συναντώνται σε κάποιο κόμβο και κατευθύνονται στον ίδιο αποστολέα ενώνονται σε μία ροή, ενώνοντας και τις απαιτήσεις τους σε πόρους.

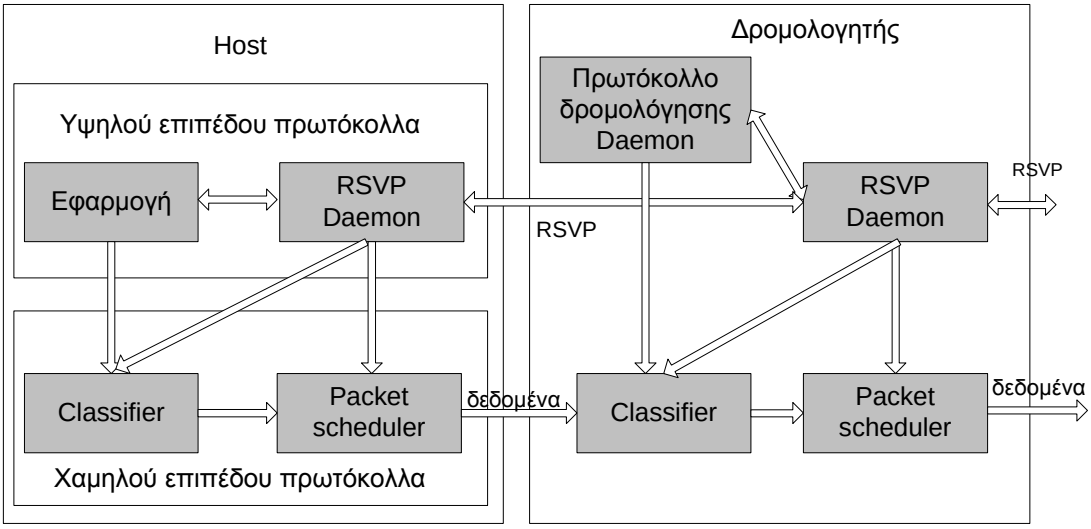
Το χαρακτηριστικό αυτό είναι και το πιο βασικό πλεονέκτημα του RSVP, που καλείται scalability (δυνατότητα κλιμάκωσης). Ένας μεγάλος αριθμός χρηστών μπορεί να ενωθεί σε ένα multicast group χωρίς αυτό να αυξάνει σημαντικά το φόρτο του δικτύου.

Η αποστολή των παραμέτρων δέσμευσης (reservation parameters) είναι μια διαδικασία διαφορετική από αυτή του προσδιορισμού των παραμέτρων αυτών. Το RSVP είναι υπεύθυνο μόνο για την αποστολή των παραμέτρων αυτών.

Ο τρόπος με τον οποίο το RSVP προσθέτει ή απομακρύνει παραλήπτες από μια multicast σύνοδο είναι ο ίδιος τρόπος σύνδεσης με αυτόν που παρέχει το IP-multicast. Δηλαδή, κάποιος που θέλει να παρακολουθήσει τη σύνοδο μπορεί να ζητήσει να συνδεθεί. Στην περίπτωση αυτή, ο παραλήπτης προστίθεται σε μία λίστα από παραλήπτες που ήδη παρακολουθούν τη σύνοδο αυτή. Ο αποστολέας διαδίδει ένα κατάλληλο μήνυμα στο οποίο περιγράφονται οι απαιτήσεις σε πόρους. Μόλις ένας κόμβος πάρει ένα τέτοιο μήνυμα πρέπει να απαντήσει με ένα αντίστοιχο μήνυμα. Έτσι, επιτυγχάνεται μία σύνδεση. Σε περίπτωση που κάποιος θέλει να αποχωρίσει από τη σύνοδο μπορεί απλά να το κάνει στέλνοντας ένα κατάλληλο μήνυμα. Το μήνυμα μπορεί να σταλεί είτε από το παραλήπτη που θέλει να φύγει είτε από τον αποστολέα που θέλει να "διώξει" κάποιον παραλήπτη.

Ένα άλλο χαρακτηριστικό είναι η δυνατότητα διαπραγμάτευσης του παρεχόμενου επιπέδου εξυπηρέτησης από πολλαπλούς αποστολείς σε πολλαπλούς παραλήπτες. Το RSVP δίνει τη δυνατότητα σε ένα παραλήπτη να διατηρήσει μόνο ένα σύνολο από πόρους που μπορεί να χρησιμοποιηθεί από πολλούς αποστολείς. Ο παραλήπτης προσδιορίζει ποια πακέτα και από ποιους παραλήπτες θα "πάρει". Με το τρόπο αυτό, οι παραλήπτες μπορούν να "μεταπηδήσουν" από μία ροή δεδομένων σε μία άλλη.

Το RSVP δεν μπορεί να υποστηρίξει εγγυημένο επίπεδο υπηρεσιών αφού δεν υπάρχει κάποια σύνδεση ανάμεσα στο τρόπο δρομολόγησης, τη δέσμευση πόρων και τη μεταφορά των δεδομένων. Το RSVP, λόγω της δυνατότητας για μεταπήδηση από μία ροή σε κάποια άλλη, είναι ιδανικό για εφαρμογές που κάνουν μετάδοση δεδομένων σε πολλούς χρήστες, τους οποίους δε γνωρίζουν ούτε πόσοι είναι ούτε που είναι.



Εικόνα 6: Αλληλουχία γεγονότων δέσμευσης πόρων με χρήση RSVP

2.5.1.2.1 Ροές Δεδομένων

Οι RSVP ροές δεδομένων χαρακτηρίζονται γενικά από συνόδους πάνω στις οποίες ρέουν πακέτα δεδομένων. Μια σύνοδος είναι ένα σύνολο από ροές δεδομένων unicast ή multicast και το RSVP διαχειρίζεται την κάθε σύνοδο ανεξάρτητα.

Η τριάδα Destination Address, Protocol ID και Destination Port καθορίζει ουσιαστικά μια σύνοδο. Η Destination Address, όπως αναφέραμε μπορεί να είναι είτε μια multicast είτε μια unicast διεύθυνση, ενώ η τελευταία παράμετρος μπορεί να είναι η διεύθυνση μιας UDP ή TCP πόρτας ή ακόμα και μια πληροφορία που απευθύνεται σε κάποιο παραπάνω επίπεδο (στο επίπεδο μεταφοράς ή και στο επίπεδο εφαρμογής ακόμα).

Το RSVP υποστηρίζει τρεις τύπους κυκλοφορίας: καλύτερης προσπάθειας, ευαίσθητος σε ρυθμό και ευαίσθητος σε καθυστέρηση. Ο τύπος της υπηρεσίας ροής δεδομένων που χρησιμοποιείται για να υποστηρίξει αυτούς τους τύπους κυκλοφορίας εξαρτάται από το υλοποιημένο QoS.

Κάθε RSVP αποστολέας και παραλήπτης αντιστοιχεί σε ένα μοναδικό κόμβο-χρήστη του Διαδικτύου. Ένας απλός κόμβος-χρήστης, ωστόσο, μπορεί να περιέχει πολλαπλούς λογικούς αποστολείς και παραλήπτες, διακεκριμένους από διαφορετικές θύρες (ports).

2.5.1.2.2 Το Μοντέλο Δέσμευσης

Ένα στοιχειώδες αίτημα δέσμευσης του RSVP αποτελείται από μια προδιαγραφή ροής (flowspec) και από μια προδιαγραφή φίλτρου (filespec). Όταν φτάνει σε κάποιο κόμβο, το αίτημα ενεργοποιεί τις ακόλουθες διαδικασίες:

- Πραγματοποιεί μια δέσμευση σε μια σύνδεση (link). Το αίτημα περνάει για επεξεργασία από το admission και το policy control. Αν το αίτημα αποτύχει σε ένα από τους δύο ελέγχους, το αίτημα απορρίπτεται και στέλνεται μήνυμα λάθους στον αποστολέα. Αν περάσει τη φάση του ελέγχου ο κόμβος δίνει εντολή στο packet classifier να επιλέξει τα πακέτα δεδομένων όπως καθορίζονται από το

filespec και επικοινωνεί με το επίπεδο σύνδεσης ώστε να πάρει και το επιθυμητό QoS που ορίζεται από το flowspec.

- Το αίτημα προωθείται προς τους κατάλληλους deamons. Το αίτημα που προωθείται από ένα κόμβο μπορεί να διαφέρει από αυτό που έλαβε για δύο λόγους: Ο μηχανισμός ελέγχου κυκλοφορίας μπορεί να τροποποιεί το flowspec, καθώς επίσης και γιατί οι δεσμεύσεις από διαφορετικά "παρακλάδια" του multicast δέντρου προς τον ίδιο αποστολέα θα πρέπει να συγχωνεύονται καθώς η δέσμευση θα "κατευθύνεται" προς αυτόν.

Θα πρέπει να σημειωθεί επίσης ότι όταν ένας παραλήπτης απευθύνει ένα αίτημα δέσμευσης, μπορεί επίσης να ζητήσει ένα μήνυμα επιβεβαίωσης ότι το αίτημά του αυτό εγκαταστάθηκε στο δίκτυο. Η επιβεβαίωση αυτή όμως θα είναι μια αρκετά ισχυρή ένδειξη και όχι μια απόλυτη εγγύηση. Τέλος αξίζει να αναφερθεί ότι ένα επιτυχές αίτημα δέσμευσης προωθείται μέσα στο multicast δέντρο έως ότου συναντήσει μια υπάρχουσα δέσμευση που να είναι ίση ή μεγαλύτερη από τη δική του. Όπως είναι φυσικό, τότε, το αίτημα δεν προωθείται παραπέρα καθώς το υπόλοιπο του μονοπατιού έχει λάβει ήδη την επιθυμητή δέσμευση.

Ένα σημείο στο οποίο αξίζει να σταθούμε αποτελεί η παρατήρηση ότι η διαδικασία δέσμευσης είναι ενός περάσματος (one pass): κάθε κόμβος στο μονοπάτι είτε αποδέχεται είτε απορρίπτει το αίτημα. Αυτό όμως το μοντέλο δεν παρέχει έναν εύκολο τρόπο να γίνει γνωστό το αποτέλεσμα της υπηρεσίας από άκρο σε άκρο, γι' αυτό το RSVP προσφέρει επιπροσθέτως την δυνατότητα του OPWA (One Pass With Advertising). Με αυτή την υπηρεσία στέλνονται στους κόμβους πακέτα ελέγχου που μαζεύουν πληροφορία η οποία επιστρέφεται στους παραλήπτες και αξιοποιείται για τη διάγνωση του υπάρχοντος QoS από άκρο σε άκρο και τη δυναμική προσαρμογή των αιτημάτων δέσμευσης.

2.5.1.2.3 Μορφές δέσμευσης (Reservation Styles)

Ένα αίτημα δέσμευσης περιλαμβάνει ένα σύνολο επιλογών το οποίο ονομάζεται και μορφή δέσμευσης (reservation style). Το RSVP υποστηρίζει δύο βασικές κατηγορίες μορφών δέσμευσης: μεμονωμένες και διαμοιραζόμενες δεσμεύσεις. Οι μεμονωμένες δεσμεύσεις εγκαθιστούν μια ροή για κάθε σχετικό αποστολέα σε κάθε σύνολο. Μια διαμοιραζόμενη δέσμευση χρησιμοποιείται από ένα σύνολο αποστολέων οι οποίοι δεν παρεμβάλλονται μεταξύ τους. Ο Πίνακας 1 περιγράφει όλους τους υποστηριζόμενους από το πρωτόκολλο συνδυασμούς στυλ / εμβέλειας δέσμευσης.

Εμβέλεια	Κρατήσεις	
	Μεμονωμένη	Διαμοιραζόμενη
Ρητή	Στυλ Fixed Filter (FF)	Στυλ ρητώς διαμοιραζόμενο Shared Explicit (SE)
Μεταβαλλόμενη (wildcard)	Μη ορισμένο	Στυλ Wildcard Filter (WF)

Πίνακας 1: Συνδυασμοί στύλ/ εμβέλειας δέσμευσης

- Wildcard-Filter (WF)

Το Wildcard-Filter στυλ ορίζει διαμοιραζόμενη κράτηση με Wildcard εμβέλεια. Με μια κράτηση στυλ WF, δημιουργείται μια απλή κράτηση στην οποία αναμειγνύονται ροές από όλους τους αποστολείς. Μπορούμε να φανταστούμε τις κρατήσεις σαν μία διαμοιραζόμενη σωλήνα της οποίας το μέγεθος είναι το μεγαλύτερο των απαιτήσεων πόρων γι' αυτή τη σύνδεση από όλους του παραλήπτες, ανεξάρτητα από τον αριθμό των αποστολέων.

- Fixed-Filter (FF)

Το στυλ Fixed-Filter ορίζει μια μεμονωμένη κράτηση με ρητή εμβέλεια. Με μια κράτηση FF στυλ, δημιουργείται μια μεμονωμένη αίτηση κράτησης για πακέτα δεδομένων από συγκεκριμένο αποστολέα. Η εμβέλεια της κράτησης καθορίζεται από μια συγκεκριμένη λίστα αποστολέων. Η συνολική κράτηση σε μια σύνδεση για δεδομένη σύνοδο είναι το άθροισμα όλων των FF κρατήσεων για όλους τους αποστολείς. Τις FF κρατήσεις τις ζητούν διαφορετικοί παραλήπτες αλλά επιλέγουν τον ίδιο αποστολέα, ωστόσο, πρέπει να αναμειχθούν προκειμένου να διαμοιραστούν μια απλή κράτηση σε ένα δεδομένο κόμβο.

- Shared-Explicit (SE)

Το στυλ κράτησης SE ορίζει ένα περιβάλλον διαμοιραζόμενης κράτησης με μια ρητή εμβέλεια κράτησης. Το SE στυλ δημιουργεί μια απλή κράτηση στην οποία αναμιγνύονται ροές από όλους τους αποστολείς. Όπως στην περίπτωση της FF κράτησης, το σύνολο των αποστολέων (και κατά συνέπεια η εμβέλεια) ορίζεται ρητά από τον παραλήπτη που κάνει την κράτηση.

2.5.1.2.4 Rsvp Soft State

Στο περιβάλλον ενός RSVP, μια Soft State κατάσταση αναφέρεται σε κατάσταση δρομολογητών και τερματικών κόμβων οι οποίοι μπορούν να ενημερωθούν από ορισμένα RSVP μηνύματα. Το χαρακτηριστικό της Soft State κατάστασης είναι ότι επιτρέπει σε ένα RSVP δίκτυο να υποστηρίξει δυναμικές αλλαγές στη ομάδα μελών και να προσαρμοστεί σε αλλαγές δρομολόγησης. Γενικά, η Soft State κατάσταση υποστηρίζεται από ένα RSVP based δίκτυο ικανοποιώντας τις δικτυακές αλλαγές χωρίς προσφυγή στα τερματικά σημεία, σε αντίθεση με μια αρχιτεκτονική μεταγωγής κυκλώματος στην οποία το τερματικό σημείο εγκαθιστά μια κλήση και, σε περίπτωση αποτυχίας, εγκαθιστά μια νέα κλήση.

Οι μηχανισμοί του RSVP πρωτοκόλλου παρέχουν μια γενική διευκόλυνση στη δημιουργία και συντήρηση μιας κατανεμημένης κατάστασης κράτησης κατά μήκος του πλέγματος multicast και unicast μονοπατιών μετάδοσης.

Για να συντηρήσει μια κατάσταση κράτησης, το RSVP ανιχνεύει μια Soft State κατάσταση στους κόμβους-χρήστες και κόμβους δρομολόγησης. Η RSVP Soft State κατάσταση δημιουργείται και περιοδικά ανανεώνεται από μηνύματα μονοπατιού και αιτήσεων κράτησης. Η κατάσταση διαγράφεται αν δε φτάσει κάποιο μήνυμα ανανέωσης πριν τη λήξη του χρονικού διαστήματος καθαρισμού. Η Soft State κατάσταση μπορεί επίσης να διαγραφεί σαν αποτέλεσμα ενός ρητού καταιγιστικού μηνύματος. Το RSVP σαρώνει περιοδικά την Soft State κατάσταση για να χτίσει και να προωθήσει μηνύματα ανανέωσης μονοπατιών και αιτήσεων κράτησης. Όταν μια διαδρομή αλλάζει, το επόμενο μήνυμα μονοπατιού αρχικοποιεί την κατάσταση μονοπατιού στο νέο μονοπάτι. Μελλοντικά μηνύματα αιτήσεων κράτησης εγκαθιστούν μια κατάσταση κράτησης.

2.5.1.2.5 RSVP tunneling

Είναι αδύνατο να χρησιμοποιήσουμε το RSVP ή οποιοδήποτε καινούριο πρωτόκολλο την ίδια στιγμή σε όλο το Διαδίκτυο. Στην πραγματικότητα το RSVP μπορεί να μη χρησιμοποιηθεί ποτέ παντού. Για αυτό και πρέπει να εξασφαλισθεί η σωστή λειτουργία του πρωτοκόλλου ακόμα και όταν δύο RSVP δρομολογητές ενώνονται μέσω ενός τυχαίου συνόλου δρομολογητών που δεν υποστηρίζουν το RSVP πρωτόκολλο. Ένα ενδιάμεσο σύνολο δρομολογητών που δεν υποστηρίζει RSVP είναι αδύνατο να πετύχει δέσμευση πόρων, οπότε δεν είναι δυνατό να δοθούν εγγυήσεις για τις παρεχόμενες υπηρεσίες. Αν ωστόσο, ένα τέτοιο σύνολο έχει αρκετή επιπλέον χωρητικότητα, μπορεί να παρέχει αποδεκτές και χρήσιμες υπηρεσίες πραγματικού χρόνου.

Για να υποστηριχτεί η σύνδεση RSVP δικτύων μέσω δικτύων που δεν υποστηρίζουν το RSVP πρωτόκολλο, το RSVP παρέχει την δυνατότητα tunneling, το οποίο πραγματοποιείται αυτόματα μέσα σε μη-RSVP δίκτυα. Το tunneling απαιτεί από όλους τους δρομολογητές (RSVP και μη-RSVP) να προωθούν τα μηνύματα μονοπατιού (path messages) προς την διεύθυνση προορισμού χρησιμοποιώντας έναν τοπικό πίνακα δρομολόγησης. Όταν ένα τέτοιο μήνυμα διασχίζει ένα μη-RSVP δίκτυο, τα αντίγραφα του μηνύματος φέρουν την IP διεύθυνση του τελευταίου RSVP δρομολογητή που συνάντησαν στην πορεία τους. Τα μηνύματα αίτησης-δέσμευσης (reservation-request) προωθούνται, ακολουθώντας πορεία αντίθετη με αυτή της ροής δεδομένων, προς τον επόμενο RSVP δρομολογητή δηλαδή σε αυτόν του οποίου την διεύθυνση φέρουν τα μηνύματα μονοπατιού.

Υπάρχουν δύο επιχειρήματα για την υποστήριξη της υλοποίησης του tunneling σε ένα RSVP περιβάλλον. Πρώτον, το RSVP θα χρησιμοποιηθεί σποραδικά και όχι καθολικά Είναι απίθανο όλα τα δίκτυα και οι δρομολογητές του Διαδικτύου να υποστηρίξουν το RSVP πρωτόκολλο, οπότε θα υπάρχει η ανάγκη για το tunneling. Δεύτερον, το tunneling μπορεί να γίνει πιο αποτελεσματικό, αν υλοποιηθεί έλεγχος της συμφόρησης σε καταστάσεις υψηλού φόρτου κυκλοφορίας.

Η σποραδική εφαρμογή σημαίνει ότι μερικά τμήματα του δικτύου θα το υλοποιήσουν πριν από άλλα. Αν προκειμένου να έχουμε αποδεκτές και χρήσιμες υπηρεσίες πραγματικού χρόνου το RSVP απαιτείται σε όλο το μήκος μιας διαδρομής, τότε κέρδος μπορεί να επιτευχθεί μόνο με τη σχεδόν καθολική εφαρμογή του πρωτοκόλλου, η οποία όμως είναι αδύνατη εκτός και αν πρώιμη εφαρμογή δώσει πολύ ενθαρρυντικά αποτελέσματα.

2.5.2 Η αρχιτεκτονική Differentiated Services (DiffServ)

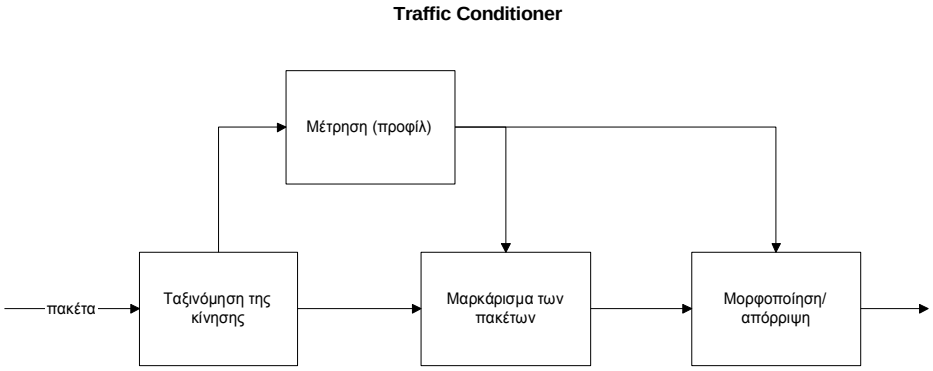
Προκειμένου να υλοποιηθεί μια υπηρεσία παροχής ποιότητας υπηρεσίας στο επίπεδο δικτύου και ειδικότερα ποιότητα υπηρεσίας με τη μέθοδο DiffServ, απαιτείται να λειτουργήσουν στο δίκτυο μια σειρά από μηχανισμούς. Αυτοί ενεργούν πάνω στις ροές και αναλυτικά είναι οι ακόλουθοι.

- Ταξινόμηση των πακέτων (packet classification). Ο μηχανισμός αυτός ταξινομεί τα πακέτα που φτάνουν σε ένα κόμβο σε ροές ή συνενώσεις ροών ώστε στη συνέχεια αυτά να εξυπηρετηθούν κατάλληλα.
- Μαρκάρισμα (marking) των πακέτων. Με το μηχανισμό αυτό τα πακέτα μαρκάρονται ανάλογα με την κλάση στην οποία ανήκουν (προέκυψε από τον

προηγούμενο μηχανισμό) είτε με βάση άλλα κριτήρια όπως τα χαρακτηριστικά της κίνησης που παρουσιάζουν κλπ.

- Μέτρηση (metering) της κίνησης. Στην προκειμένη περίπτωση ο μηχανισμός αυτός ελέγχει το προφίλ της κίνησης που δέχεται και το συγκρίνει με το προσυμφωνηθέν προφίλ κίνησης όπως προκύπτει από το SLA που έχει υπογράψει με τον διαχειριστή του δικτύου. Στη συνέχεια ο μηχανισμός αυτός διαχωρίζει τα πακέτα σε έναν αριθμό κατηγοριών (ανάλογα αν βρίσκονται στα νόμιμα πλαίσια ή όχι). Ο αριθμός των κατηγοριών αυτών εξαρτάται από τη συμφωνία που έχει γίνει με το πάροχο όπου επίσης καθορίζεται η μεταχείριση που θα έχουν τα πακέτα όλων των κατηγοριών.
- Μηχανισμός μορφοποίησης (shaping) της κίνησης όπου τροποποιούνται τα χαρακτηριστικά της κίνησης που έλαβε ο κόμβος (δρομολογητής). Επίσης αντί του μηχανισμού αυτού μπορεί να υπάρχει μηχανισμός απόρριψης (dropping) των πακέτων.

Γενικά η σειρά με τη οποία συνήθως αυτοί χρησιμοποιούνται είναι και η σειρά με την οποία παρουσιάστηκαν. Πρέπει στο σημείο αυτό να αναφέρουμε ότι είναι επίσης δυνατό οι μηχανισμοί μαρκαρίσματος και μέτρησης του προφίλ της κίνησης να εμφανίζονται αντίστροφα, δηλαδή πρώτα μέτρηση του προφίλ της κίνησης και ύστερα με βάση αυτό το κριτήριο μαρκάρισμα των πακέτων. Επίσης μετά από τη διαδικασία μέτρησης του προφίλ, σε ορισμένες «κατηγορίες» πακέτων (και κυρίως στα νόμιμα πακέτα) συνήθως δεν εφαρμόζεται κανένας περαιτέρω μηχανισμός και εισάγονται έτσι στο δίκτυο.



Εικόνα 7: Οι βασικοί μηχανισμοί και η σειρά με την οποία εκτελούνται

Στο σημείο αυτό είναι αναγκαίο να τονιστεί πως όλοι οι παραπάνω μηχανισμοί και λειτουργικότητες εφαρμόζονται στους συνοριακούς κόμβους (edge routers) σε ένα DiffServ enabled domain. Αντίθετα, στους ενδιάμεσους κόμβους (core routers) η DiffServ αρχιτεκτονική προσδιορίζει πως οι παραπάνω μηχανισμοί δεν έχουν καμία εφαρμογή.

Η αρχιτεκτονική DiffServ γενικά αποτελεί το πιο δυναμικό σημείο για την παροχή υπηρεσιών QoS. Η λογική της είναι να αναγνωρίζει κάποιες ροές πακέτων και να τις διαχειρίζεται προνομιακά έναντι των υπολοίπων. Γενικά έχουν προταθεί 2 είδη DiffServ υπηρεσιών (per hop behaviors) που περιγράφονται παρακάτω. Με τον όρο per hop behavior καλείται η «συμπεριφορά προώθησης» (forwarding behavior) που εφαρμόζεται στα πακέτα σε κάθε κόμβο του DiffServ domain.

- Expedited Forwarding (EF) [4]. Σε αυτή την κατηγορία υπηρεσιών στόχο αποτελεί η ελαχιστοποίηση της καθυστέρησης και της διακύμανσης καθυστέρησης (jitter) ενώ παράλληλα στοχεύει ώστε να παρέχει ποιότητα υπηρεσίας στον υψηλότερο βαθμό. Τα πακέτα που υπερβαίνουν το προφίλ της κίνησης που έχει συμφωνηθεί ότι θα εισάγει ο χρήστης (στο SLA που υπογράφηκε) απορρίπτονται. Γενικά οι υπηρεσίες αυτής της κατηγορίες εξομοιώνουν τη λειτουργία μιας εικονικής μισθωμένης γραμμής.
- Assured Forwarding (AF) [5]. Η κατηγορία αυτή διαθέτει το πολύ 4 κλάσεις εξυπηρέτησης και το πολύ 3 επίπεδα απόρριψης για κάθε κλάση. Η AF κίνηση που υπερβαίνει τα χαρακτηριστικά διανέμεται με όχι τόσο μεγάλη πιθανότητα όσο η εντός προφίλ κίνηση, γεγονός που σημαίνει ότι μπορεί να υποβιβάζεται αλλά δεν σημαίνει απαραίτητα ότι απορρίπτεται.

2.5.2.1 Ταξινόμηση της κίνησης

Η ταξινόμηση της κίνησης είναι το πρώτο σημείο στο οποίο βασίζεται η παροχή ποιότητας υπηρεσίας στην εξυπηρέτηση των πακέτων και για το λόγο αυτό αποτελεί ιδιαίτερα σημαντικό παράγοντα. Η ταξινόμηση των πακέτων προκειμένου να εξυπηρετηθούν κατάλληλα σε ένα δίκτυο που υποστηρίζει QoS γίνεται είτε σε επίπεδο ροών, είτε σε επίπεδο συνενώσεων ροών (aggregates). Η διαδικασία αυτή γίνεται κυρίως με τον έλεγχο της επικεφαλίδας κάθε πακέτου και την άντληση από εκεί κάποιας πληροφορίας με βάση την οποία γίνεται η ταξινόμηση. Γενικά ο μηχανισμός αυτός απαιτείται να είναι πολύ γρήγορος, ακολουθώντας το ρυθμό άφιξης των πακέτων, και ιδιαίτερα ακριβής.

Θεωρητικά οι ροές χαρακτηρίζονται από μια πεντάδα που αποτελείται από:

- Την IP διεύθυνση του αποστολέα
- Τον αριθμό port του αποστολέα
- Την IP διεύθυνση του παραλήπτη
- Τον αριθμό port του παραλήπτη
- Το πρωτόκολλο που χρησιμοποιείται.

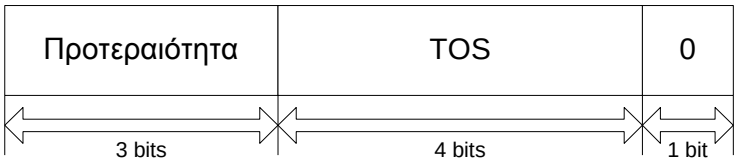
Κάνοντας τελικά ταξινόμηση ανά ροή με βάση αυτή την πεντάδα είναι μια διαδικασία αρκετά δύσκολη παρότι όλα αυτά τα πεδία υπάρχουν στην IP επικεφαλίδα (στο σημείο αυτό να σημειώσουμε ότι όλοι αυτοί οι μηχανισμοί λειτουργούν στο επίπεδο δικτύου του OSI μοντέλου). Η δυσκολία έγκειται στο γεγονός ότι απαιτείται η διαδικασία της ταξινόμησης να γίνεται άμεσα και συνεπώς ο έλεγχος τόσων πεδίων απαιτεί μεγάλη επεξεργαστική ισχύ. Η μέθοδος αυτή της ταξινόμησης εφαρμόζεται μόνο όταν θέλουμε απαραιτήτως να κάνουμε ταξινόμηση με βάση ξεχωριστές ροές όπως θέλουμε να κάνουμε πολλές φορές στην DiffServ αρχιτεκτονική στα σημεία εισόδου της κίνησης σε DiffServ enabled domains. Τέλος αυτή η μέθοδος ονομάζεται Multifield classification.

Αντίθετα στην περίπτωση όπου επιθυμούμε να κάνουμε ταξινόμηση σε συνενώσεις ροών τότε αρκεί να χρησιμοποιηθεί ένας συνδυασμός των παραπάνω πεδίων της πεντάδας που χαρακτηρίζει μια ροή, ή ακόμη και ένα μόνο πεδίο. Η περίπτωση αυτή είναι πιο εύκολη να γίνει και μπορεί τελικά να πραγματοποιείται ταχύτατα σε σύγκριση με τον έλεγχο όλης της πεντάδας.

Στην πραγματικότητα ισχύει πως η ταξινόμηση των πακέτων επιθυμούμε να γίνει σε έναν περιορισμένο αριθμό κατηγοριών (κλάσεων) και συνεπώς αρκεί να χρησιμοποιηθεί ένα σταθερό πεδίο στην επικεφαλίδα των πακέτων. Η μέθοδος αυτή είναι σαφώς απλούστερη και πιο αποδοτική. Στην περίπτωση της DiffServ αρχιτεκτονικής ονομάζεται behaviour aggregate classification και πρέπει να παρατηρήσουμε ότι η ταξινόμηση που επιτυγχάνει είναι σε επίπεδο συνενώσεων ροών (aggregates).

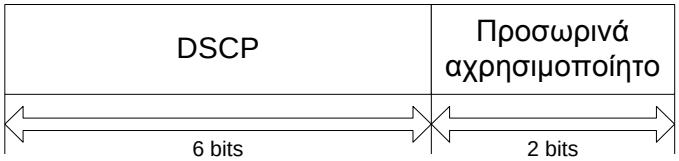
2.5.2.1.1 Ταξινόμηση με βάση την IPv4 επικεφαλίδα

Η ταξινόμηση πραγματοποιείται χρησιμοποιώντας μια οκτάδα από bits που υπάρχει την επικεφαλίδα των IPv4 πακέτων και η οποία ονομάζεται TOS octet. Σε αυτή τα τρία πρώτα πακέτα δηλώνουν την προτεραιότητα κάθε πακέτου και συνεπώς υπάρχουν 8 διαφορετικές κλάσεις προτεραιότητας. Τα επόμενα 4 bits χαρακτηρίζουν το είδος της υπηρεσίας που επιθυμεί η εφαρμογή, δηλαδή ελαχιστοποίηση της καθυστέρησης, η ελαχιστοποίηση της απώλειας πακέτων κλπ.



Εικόνα 8: Το TOS octet της IPv4 επικεφαλίδας

Ακόμη, αργότερα καθορίστηκε στο TOS octet τα 6 πιο σημαντικά bits να αναπαριστούν το DiffServ Code Point το οποίο ουσιαστικά δημιουργεί 64 δυνατές συνδυασμούς για τη διαχείριση ουρών και χρονοδρομολόγησης των IP πακέτων. Τέλος να αναφέρουμε πως αντίστοιχο πεδίο έχει οριστεί και για το πρωτόκολλο IPv6.

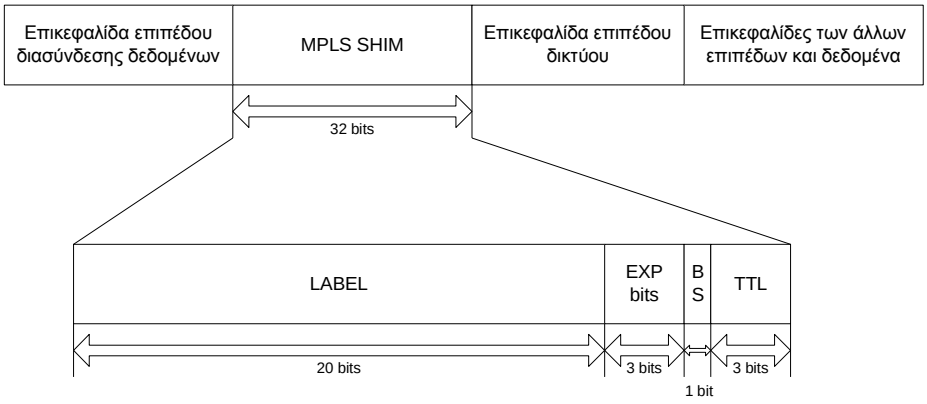


2.5.2.1.2 Ταξινόμηση με βάση την IPv6 επικεφαλίδα

Ομοίως στο IPv6 [52] έχει οριστεί αντίστοιχο πεδίο για μαρκάρισμα κίνησης προκειμένου να δεχτεί ποιότητα εξυπηρέτησης. Ένα από τα πεδία της επικεφαλίδας ονομάζεται Traffic Class (Τάξη Κυκλοφορίας) και έχει μήκος 8 bits. Το πεδίο αυτό περιέχει το πεδίο DSCP (Differentiated Code Point) όπως το αντίστοιχο type of service του IPv4 και χρησιμοποιείται για μαρκάρισμα πακέτων προκειμένου να ανήκουν σε κάποια κλάση υπηρεσίας. Επίσης, το IPv6 πρωτόκολλο έχει εισάγει και ένα νέο πεδίο που ονομάζεται Flow Label (Ετικέτα Ροής) και έχει μήκος 20 bit. Αυτό χρησιμοποιείται για να γνωστοποιεί ποια πακέτα ανήκουν σε μια συγκεκριμένη ροή. Ένας κόμβος μπορεί να είναι η αφετηρία για πάνω από μια ροές ταυτόχρονα. Γι αυτό η ετικέτα ροής σε συνδυασμό με τη διεύθυνση της αφετηρίας μπορούν να αναγνωρίσουν μονοσήμαντα μια ροή. Γενικά πάντως μέχρι σήμερα δεν έχει μοντελοποιηθεί πλήρως η χρήση του.

2.5.2.1.3 Ταξινόμηση με βάση την MPLS επικεφαλίδα

Το MPLS [56] αποτελεί ένα σύγχρονο και δυναμικό πρωτόκολλο που ανήκει μεταξύ του επιπέδου 2 και του επιπέδου 3 του ISO/OSI μοντέλου. Το πρωτόκολλο αυτό τοποθετεί μια δική του επικεφαλίδα στα πακέτα (κάτω από την IP επικεφαλίδα) και προωθεί τα πακέτα με βάση τις πληροφορίες της ετικέτας αυτής. Συνεπώς, για να υποστηριχτεί Ποιότητα Υπηρεσίας σε MPLS δίκτυα είναι απαραίτητο το μαρκάρισμα (classification) να γίνεται στην MPLS επικεφαλίδα.



Εικόνα 9: Η MPLS επικεφαλίδα

Η MPLS επικεφαλίδα περιλαμβάνει το πεδίο EXP (experimental), με μήκος 3 bits που χρησιμοποιείται για να καθοριστεί ο τύπος της μεταχείρισης. Ιδιαίτερη σημασία βέβαια πρέπει να δίνεται σε περιπτώσεις όπου πακέτα έχουν μαρκαρισμένο το DSCP πεδίο στο IP επίπεδο και εισέλθουν σε ένα MPLS domain όπου η μεταγωγή γίνεται με έλεγχο της MPLS επικεφαλίδας αγνοώντας την IP επικεφαλίδα. Στο σημείο αυτό σχεδόν όλες οι εταιρίες παροχής δικτυακού εξοπλισμού έχουν προβλέψει και όταν ένα IP πακέτο εισέρχεται σε ένα MPLS domain αντιγράφουν στο πεδίο EXP τα IP Precedence bits, δηλαδή τα 3 πιο σημαντικά bits του DSCP πεδίου. Βέβαια υπάρχει και η πρόβλεψη να μπορεί ο διαχειριστής του δικτύου να μαρκάρει το πεδίο αυτό με άλλη τιμή (άσχετη με την τιμή του IP Precedence). Τέλος πρέπει να σημειωθεί ότι επειδή το EXP πεδίο έχει μήκος 3 bits, μόνο 8 διαφορετικές κλάσεις μπορούν να υποστηριχτούν σε ένα MPLS δίκτυο.

2.5.2.2 Μηχανισμοί μαρκαρίσματος, μέτρησης της κίνησης, μορφοποίησης και απόρριψης πακέτων

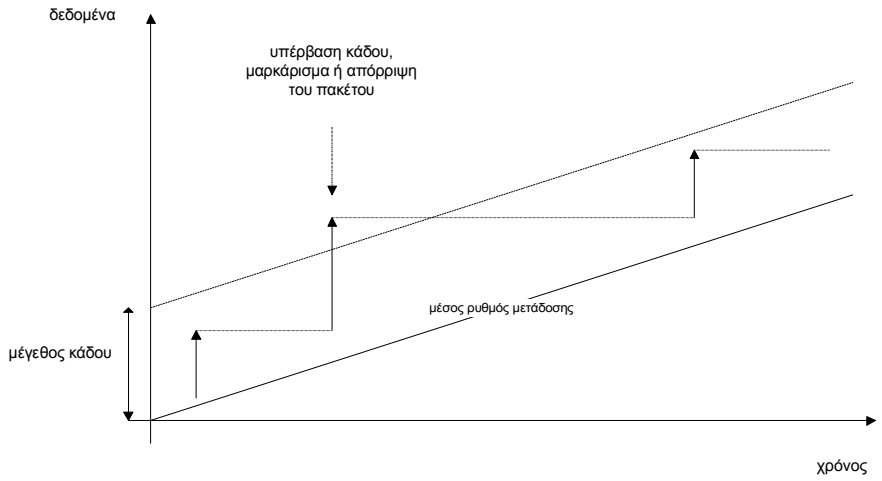
Γενικά οι μηχανισμοί μαρκαρίσματος των πακέτων, μέτρησης του προφίλ της κίνησης και μορφοποίησης ή απόρριψης της κίνησης ονομάζονται όλοι μαζί μηχανισμοί ελέγχου της κίνησης (traffic conditioning). Συνήθως οι μηχανισμοί αυτοί εφαρμόζονται στον αποστολέα, στα σημεία εισόδου της κίνησης σε κάποιο domain. Εντούτοις, έχει αναφερθεί πως μπορεί ο μηχανισμός μέτρησης να βρίσκεται στον παραλήπτη με ορισμένες βέβαια προϋποθέσεις. Για να είναι αυτό εφικτό απαιτείται από το δίκτυο να υποστηρίζει σε όλους τους δρομολογητές του την λειτουργικότητα του ECN (Explicit Congestion Notification) που είναι μια λειτουργία ελέγχου συμφόρησης. Στην πράξη το ECN είναι ένα bit στην επικεφαλίδα των πακέτων που τίθεται στην τιμή 1 όταν ανιχνεύσει στο δίκτυο συμφόρηση. Με τον τρόπο αυτό ενημερώνονται οι υπόλοιποι κόμβοι από τους οποίους περνά το συγκεκριμένο πακέτο πως σε κάποιο σημείο στο δίκτυο παρατηρήθηκε συμφόρηση.

Οι μηχανισμοί ελέγχου της κίνησης που παρουσιάζουμε στις επόμενες παραγράφους της ενότητας υποθέτουν πως το μαρκάρισμα και η μέτρηση των πακέτων γίνεται στα σημεία εισόδου στο δίκτυο.

2.5.2.2.1 Αλγόριθμοι Token Bucket και Leaky Bucket

Ένας απλός μηχανισμός για τον έλεγχο της κίνησης, που διαχωρίζει τα πακέτα σε 2 κατηγορίες, σε αυτά που είναι εντός προφίλ και αντίστροφα σε όσα είναι εκτός προφίλ είναι η εφαρμογή κάποιου από τους αλγορίθμους token ή leaky bucket. Η λειτουργία τους βασίζεται στην ίδια λογική αλλά επιτυγχάνουν διαφορετικά αποτελέσματα όπως θα παρουσιαστούν αμέσως.

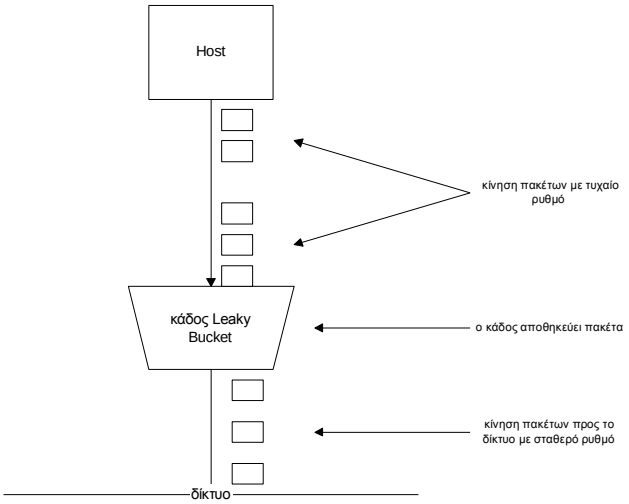
Ο αλγόριθμος token bucket καθορίζει 2 μεταβλητές, το μέσο ρυθμό αποστολής πακέτων r και το μέγιστο μέγεθος του κάδου b. Σε αυτόν παράγονται tokens με ρυθμό ίσο με το μέσο ρυθμό που καθορίστηκε, και αν αυτά δεν χρησιμοποιούνται συσσωρεύονται στο κάδο μέχρι το πολύ b. Όταν φτάσει ένα πακέτο, αν υπάρχει ελεύθερο token, τότε θεωρείται ότι το token ανατίθεται στο πακέτο αυτό και το πακέτο χαρακτηρίζεται σαν εντός προφίλ. Αντίθετα αν φτάσει ένα πακέτο και δεν υπάρχει ελεύθερο token, τότε το πακέτο μαρκάρεται ως εκτός προφίλ έτσι ώστε αργότερα να δεχτεί ανάλογη μεταχείριση, όπως εξυπηρέτηση με ελάχιστη ποιότητα ή ακόμη και απόρριψη ανάλογα με το SLA [23] που έχει υπογραφεί. Συμπερασματικά λοιπόν ο αλγόριθμος token bucket καθορίζει το μέσο ρυθμό μετάδοσης και επομένως επιτρέπει διακυμάνσεις του στιγμιαίου ρυθμού. Επίσης ο ρόλος του κάδου, που έχει μέγιστο μέγεθος b, είναι ιδιαίτερα σημαντικός αφού επιτρέπει να μαρκάρονται σαν κίνηση εντός προφίλ, εκρήξεις που δεν ξεπερνούν όμως την τιμή b.



Εικόνα 10: Η λειτουργία του μηχανισμού token bucket

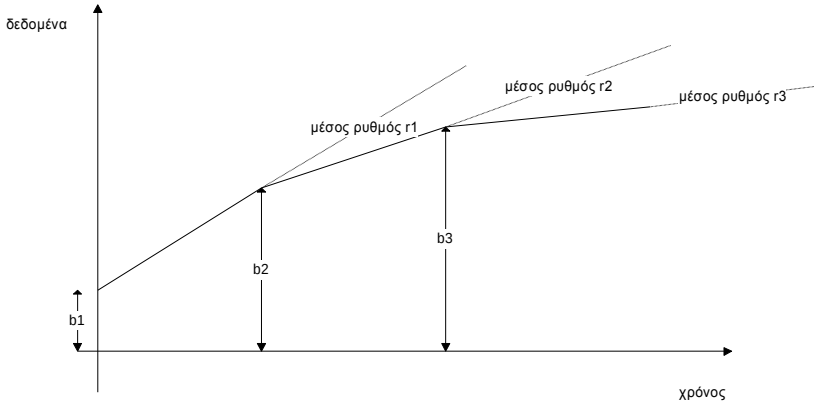
Παρόμοιος σε φιλοσοφία είναι και ο αλγόριθμος leaky bucket που καθορίζει αυστηρά το ρυθμό εξόδου των πακέτων από τον κάδο και είσοδό τους στο δίκτυο. Αν ο ρυθμός με τον οποίο καταφθάνουν τα πακέτα στον κάδο είναι μεγαλύτερος από τον ρυθμό με τον οποίο αυτά εξέρχονται από αυτόν, τότε συσσωρεύονται, μέχρι όμως μια τιμή που αποτελεί και το μέγιστο μέγεθος του κάδου. Ουσιαστικά λοιπόν ο αλγόριθμος αυτός οδηγεί τα πακέτα να εξέρχονται με σταθερό ρυθμό από τον κάδο και επιτρέπει αυτά να συσσωρεύονται στον κάδο εφόσον βέβαια υπάρχει διαθέσιμος χώρος. Τα πακέτα αυτά θεωρούνται ως νόμιμα (εντός προφίλ), ενώ αντίθετα όσα δεν εισέρχονται στον

κάδο μαρκάρονται ως εκτός προφίλ και χειρίζονται σύμφωνα με ότι προβλέπει η συμφωνία που έχει υπογραφεί. Συμπερασματικά ο αλγόριθμος leaky bucket αποτελεί έναν πολύ καλό αλγόριθμο μορφοποίησης της κίνησης αφού σταθεροποιεί το ρυθμό μετάδοσης των πακέτων εξαλείφοντας εκρήξεις.



Εικόνα 11: Η λειτουργία του μηχανισμού leaky bucket

Επίσης προκειμένου να επιτευχθεί ο έλεγχος της κίνησης σε περισσότερα από 2 επίπεδα τότε μπορεί να χρησιμοποιηθεί κάποιος από τους παραπάνω αλγορίθμους διαδοχικά [7][8]. Έτσι τα πακέτα κατηγοριοποιούνται σε περισσότερα επίπεδα και μπορούν στη συνέχεια τα πακέτα κάθε επιπέδου να μαρκάρονται και να εξυπηρετούνται ξεχωριστά.



Εικόνα 12: Ένας μηχανισμός κατηγοριοποίησης της κίνησης σε 3 επίπεδα

2.5.2.3 Αστυνόμευση (policing) της κίνησης

Η λειτουργία αυτή πραγματοποιείται επίσης στα σημεία εισόδου της κίνησης σε ένα DiffServ domain. Η αστυνόμευση έχει την έννοια του ελέγχου της κίνησης με βάση ένα συγκεκριμένο προφίλ που έχει συμφωνηθεί και στη συνέχεια τη λήψη συγκεκριμένων αποφάσεων για τον χειρισμό της κίνησης που ξεφεύγει από το συμφωνηθέν προφίλ. Οι αποφάσεις αυτές μπορεί να είναι είτε μαρκάρισμα των πακέτων σε μικρότερη κλάση εξυπηρέτησης, να εξυπηρετηθούν χωρίς εγγυημένη ποιότητα ή τέλος στη χειρότερη περίπτωση να απορριφθούν. Στο σημείο αυτό πρέπει

να σημειωθεί πως οι αποφάσεις αυτές επίσης έχουν συμφωνηθεί εκ των προτέρων μεταξύ του πελάτη και του διαχειριστή του δικτύου (SLA). Τα κριτήρια αστυνόμευσης που χρησιμοποιούνται μπορεί να είναι με βάση τη χρονική στιγμή στη διάρκεια της μέρας, βάση της πηγής και του προορισμού ή γενικότερα με βάση κάθε δεδομένο της κίνησης.

Παράλληλα η λειτουργία της μορφοποίησης της κίνησης που περιγράφηκε προηγουμένως επιτυγχάνει να διαμορφώνει την κίνηση εξαλείφοντας εκρήξεις. Επίσης μπορεί να προβλεφθεί τα πακέτα που κανονικά απορρίπτονται (πακέτα εκτός προφίλ) να αποθηκεύονται προσωρινά και να διοχετεύονται αργότερα στο δίκτυο αφού πλέον έχει εξομαλυνθεί η εκρηκτικότητα της μετάδοσής τους. Επομένως είναι δυνατό οι μηχανισμοί αστυνόμευσης και μορφοποίησης της κίνησης να χρησιμοποιηθούν συνδυασμένα ώστε ένα μέρος των πακέτων που θεωρούνται εκτός προφίλ από τον μηχανισμό αστυνόμευσης να μορφοποιείται και να μεταδίδεται. Γενικά το πεδίο αυτό είναι ανοικτό και μπορούν να παρουσιαστούν διάφοροι μηχανισμοί που συνδυάζουν μηχανισμούς αστυνόμευσης και μορφοποίησης.

2.5.2.4 Διαχείριση ουρών (Queue management)

Το θέμα της διαχείρισης των ουρών αποτελεί ένα σημαντικό και κρίσιμο ζήτημα για το διαχειριστή του δικτύου προκειμένου να είναι σε θέση να προσφέρει ποιότητα υπηρεσίας στις διάφορες ροές όπως έχει συμφωνήσει. Επίσης η διαχείριση των ουρών είναι μια βασική προϋπόθεση για τη λειτουργία του μηχανισμού της χρονοδρομολόγησης που θα περιγράψουμε στην επόμενη ενότητα. Προκειμένου το δίκτυο να ικανοποιήσει όλες τις εγγυήσεις παροχής ποιότητας υπηρεσίας πρέπει να χειρίζεται τα πακέτα κάθε κλάσης ποιότητας σε ξεχωριστή ουρά ώστε να μπορεί να εφαρμόζει τον κατάλληλο μηχανισμό χρονοδρομολόγησης. Σε αντίθετη περίπτωση δεν είναι δυνατό ο μηχανισμός χρονοδρομολόγησης να διαχωρίσει τις διαφορετικές κλάσεις ποιότητας και να προσφέρει επομένως τις κατάλληλες εγγυήσεις στις αντίστοιχες ροές. Πιο αναλυτικά, αναφέροντας ένα παράδειγμα, αν δεν γίνει διαχωρισμός των κλάσεων ποιότητας σε διαφορετικές ουρές, θα συσσωρεύονται στην ίδια ουρά ροές με διαφορετικές απαιτήσεις με αποτέλεσμα είτε πακέτα να απορρίπτονται (αν γεμίσει η ουρά) είτε να παρουσιάζεται μεγάλη καθυστέρηση. Συνέπεια όλων αυτών είναι το δίκτυο να μην μπορεί να παρέχει τις καλύτερες εγγυήσεις και αντίστοιχα η απόδοση που επιτυγχάνουν οι εφαρμογές των πελατών να υποβαθμίζεται σημαντικά.

Οι κατεξοχήν λειτουργίες του διαχειριστή των ουρών παρουσιάζονται αμέσως παρακάτω και επιγραμματικά συνοψίζονται στην σωστή λειτουργία των ουρών και στη χρήση μηχανισμών για τον έλεγχο τους.

- Είσοδος ενός πακέτου στη σωστή ουρά με βάση τη κατηγοριοποίηση του πακέτου από τον αντίστοιχο μηχανισμό.
- Απόρριψη ενός πακέτου στην περίπτωση που η ουρά που πρέπει να εισαχθεί είναι γεμάτη.
- Απομάκρυνση ενός πακέτου από την κορυφή της ουράς όταν το ζητήσει ο χρονοδρομολογητής προκειμένου να μεταδοθεί στον επόμενο κόμβο.
- Έλεγχος της κατάστασης της ουράς, δηλαδή της μέσης πληρότητάς της και ανάληψη πρωτοβουλιών ανάλογα με αυτή την τιμή, με στόχο τη διατήρηση της

μέσης πληρότητας σε χαμηλά επίπεδα. Οι πρωτοβουλίες που μπορεί να αναλάβει είναι οι ακόλουθες:

- Αφαίρεση ενός πακέτου από την ουρά και απόρριψή του στην περίπτωση που η ουρά έχει αρχίσει να γεμίζει.
- Μαρκάρισμα ενός πακέτου όταν η ουρά παρουσιάζει μεγάλη πληρότητα (ECN).

Γενικά λοιπόν παρατηρείται ότι εκτός από τις κλασικές λειτουργίες υποδοχής και αποχώρησης ενός πακέτου, ο διαχειριστής μιας ουράς ενδιαφέρεται και την αποδοτική λειτουργίας της που εξασφαλίζεται κυρίως μέσα από τη διατήρηση σε χαμηλά επίπεδα της μέσης πληρότητάς της. Αυτό δικαιολογείται από το γεγονός ότι διατηρώντας χαμηλά τη μέση πληρότητα τότε οι ουρές μπορούν να απορροφούν εύκολα εκρήξεις της κίνησης. Αντίθετα, αν η μέση πληρότητα ήταν υψηλή τότε πλήθος πακέτων κατά τη διάρκεια εκρήξεων θα απορρίπτονταν. Επίσης η μικρή πληρότητα μιας ουράς συνεπάγεται πως η μέση καθυστέρηση εξυπηρέτησης θα παραμένει χαμηλή, γεγονός που είναι ιδιαίτερα επιθυμητό.

Το θέμα της διαχείρισης των ουρών γίνεται ακόμα επιτακτικότερο και πιο κρίσιμο ειδικά σε καταστάσεις συμφόρησης του δικτύου όπου πρέπει πλέον οι ουρές να αντιδράσουν σωστά και άμεσα. Το κυριότερο πρόβλημα είναι πως να προσδιοριστούν συγκεκριμένες στρατηγικές αποφάσεις για την ανάληψη δράσεων. Μια από αυτές τις αποφάσεις είναι πότε αποφασίζεται να απορρίπτονται πακέτα, δηλαδή αν απορρίπτονται πακέτα μόλις φτάσουν στην ουρά ή επιτρέπεται να απορρίπτονται πακέτα που βρίσκονται μέσα στην ουρά προκειμένου να εξυπηρετηθούν άλλα μεγαλύτερης προτεραιότητας. Επίσης κρίσιμη απόφαση είναι με βάση ποια κριτήρια και πληροφορίες απορρίπτονται τα πακέτα, αφού μπορεί να κρατούνται γενικές πληροφορίες για όλη την κίνηση ή αντίθετα για κάθε είδος κίνησης ξεχωριστά.

Συμπερασματικά, οι παραπάνω στρατηγικές αποφάσεις για τη λειτουργία της διαχείρισης ουρών επηρεάζουν άμεσα την απόδοση των ίδιων των ουρών και κατ' επέκταση όλου του δικτύου. Γενικό στόχο αποτελεί η δίκαια διαχείριση των ουρών για όλες τις κλάσεις ποιότητας χωρίς σε καμία περίπτωση να παραβούμε τις συμφωνίες που έχουν υπογραφεί με τους πελάτες του δικτύου.

Επιστρέφοντας στο θέμα της συμφόρησης πρέπει να τονιστεί πως η ύπαρξη συμφόρησης στο δίκτυο συνεπάγεται και αύξηση του μέσου μεγέθους των ουρών. Για την αποφυγή της συμφόρησης υπάρχουν συγκεκριμένοι μηχανισμοί από το πρωτόκολλο TCP [18] στο επίπεδο μεταφοράς σύμφωνα με το OSI μοντέλο. Παράλληλα με αυτούς, οι διαχειριστές έχουν αναπτύξει και δικούς τους μηχανισμούς που θα παρουσιαστούν παρακάτω. Γενικά οι μηχανισμοί αυτοί προσπαθούν να βελτιώσουν το πρόβλημα της συμφόρησης που παρατηρείται στο δίκτυο και οφείλεται σε αποστολή πακέτων με ρυθμό υψηλότερο από αυτό που μπορεί να αντιμετωπίσει το δίκτυο και δεν οφείλεται σε μικροεκρήξεις παροδικού χαρακτήρα. Οι μηχανισμοί που μπορεί να χρησιμοποιήσει ο διαχειριστής του δικτύου είναι:

- Απόρριψη των πακέτων. Ο μηχανισμός αυτός έχει διπλό αποτέλεσμα καθώς αφενός μειώνει άμεσα το φόρτο του δικτύου και αφετέρου ενημερώνει άμεσα το πρωτόκολλο TCP για συμφόρηση. Αυτό επιτυγχάνεται αφού το TCP θεωρεί ότι κάθε απώλεια πακέτου οφείλεται σε συμφόρηση και στη συνέχεια ενεργοποιεί αυτόματα το μηχανισμό του για την αποφυγή συμφόρησης.

- Μαρκάρισμα των πακέτων. Η δεύτερη αυτή μέθοδος είναι λιγότερο καταστροφική από την πρώτη αφού δεν απορρίπτει πακέτα αλλά και λιγότερο άμεση αφού το δίκτυο δεν «αποφορτίζετε» άμεσα.

Στη συνέχεια περιγράφονται τεχνικές και μηχανισμοί που ανήκουν στη δεύτερη κατηγορία.

2.5.2.4.1 Explicit Congestion Notification (ECN)

Η μέθοδος αυτή στηρίζεται στα 2 αχρησιμοποίητα bits του πεδίου DSCP (DiffServ Code Point), τα οποία πλέον ονομάζονται ECN Capable Transport (ECT) και Congestion Experienced (CE) αντίστοιχα [12]. Αυτός ο μηχανισμός ελέγχεται από τα πρωτόκολλα του επιπέδου μεταφοράς και η λειτουργία του είναι απλή. Τα 2 αυτά bits επιτελούν συγκεκριμένες λειτουργίες:

- Το bit ECT τίθεται στην τιμή 1 αν τα άκρα μιας ροής που μεταδίδεται κατανοούν την λειτουργία του bit CE και κατ' επέκταση του όλου αυτού μηχανισμού.
- Το bit CE τίθεται στην τιμή 1 όταν κάποιος δρομολογητής επιθυμεί να ειδοποιήσει για συμφόρηση και το bit ECT είναι ενεργοποιημένο.

Συνεπώς σε κάθε πακέτο το ECT είναι 1 όταν και οι 2 άκρες της ροής κατανοούν τη λειτουργία του μηχανισμού. Κάθε δρομολογητής αν θέλει να ειδοποιήσει για συμφόρηση θέτει το CE στην τιμή 1 αν το ECT είναι ενεργοποιημένο αλλιώς απορρίπτει το πακέτο. Ουσιαστικά με τη μέθοδο αυτή ειδοποιούνται τα πρωτόκολλα με μη καταστροφικό τρόπο αν κατανοούν τη μέθοδο αυτή και σε αντίθετη περίπτωση (δεν καταλαβαίνουν τη μέθοδο) κατανοούν τη συμφόρηση από την απόρριψη του πακέτου. Ένα κρίσιμο σημείο στη μέθοδο αυτή είναι πότε ο δρομολογητής αποφασίζει να ειδοποιήσει για συμφόρηση, αφού σε περιπτώσεις παροδικής συμφόρησης λόγω μικροεκρήξεων της κίνησης, δεν είναι αποδοτικό να ειδοποιείται το πρωτόκολλο καθώς τότε θα υποβαθμιστεί η απόδοση του δικτύου χωρίς λόγο.

2.5.2.4.2 Μηχανισμός RED (Random Early Detection)

Ένας δεύτερος μηχανισμός που ειδοποιεί τα πρωτόκολλα για ενδεχόμενη συμφόρηση είναι ο RED. Στους μηχανισμούς αποφυγής συμφόρησης σημαντικό πρόβλημα αποτελεί ο καθορισμός πότε θα αποστέλλεται ειδοποίηση για συμφόρηση και πόσο έντονη αυτή θα είναι. Παράλληλα το θέμα αυτό σχετίζεται και με την διαμόρφωση των ουρών, πως έχουν δηλαδή οριστεί ώστε να είναι ξεχωριστές για κάθε ροή ή επιτρέπεται aggregates να περνούν από την ίδια ουρά.

Με το θέμα αυτό ασχολήθηκε για αρκετά χρόνια η IRTF (Internet Research Task Force) που κατέληξε να προτείνει τον μηχανισμό RED ο οποίος στέλνει ειδοποιήσεις για συμφόρηση τυχαία και η συχνότητα με την αυτές στέλνονται εξαρτάται από τη μέση πληρότητα της ουράς. Βασική παράμετρος με βάση την οποία αποφασίζει ο μηχανισμός αυτός είναι η μέση πληρότητα της ουράς. Ο τρόπος με τον οποίο ειδοποιεί τα πρωτόκολλα για συμφόρηση είναι έμμεσος καθώς αυτό γίνεται με απόρριψη πακέτων. Σε κάθε ουρά που εφαρμόζεται ο RED ορίζονται τρία μεγέθη:

- Το min threshold
- Το max threshold
- Το max possibility

Έτσι ο μηχανισμός λειτουργεί ως εξής:

- Εάν η μέση πληρότητα είναι μικρότερη από την τιμή min_threshold τότε όλα τα πακέτα διέρχονται κανονικά και δεν έχουμε καμία απόρριψη.
- Εάν η μέση πληρότητα είναι μεγαλύτερη από την τιμή min_threshold και μικρότερη από την τιμή max_threshold τότε η πιθανότητα απόρριψης αυξάνει γραμμικά από 0 έως την τιμή max_possibility.
- Τέλος αν η μέση πληρότητα ξεπερνά την τιμή του max_threshold, τότε όλα τα πακέτα απορρίπτονται.

Οι τρεις αυτές καταστάσεις στις οποίες μπορεί να βρίσκεται μια ουρά ονομάζονται αντίστοιχα κανονική, αποφυγής συμφόρησης και ελέγχου συμφόρησης. Κρίσιμο παράγοντα για τη λειτουργία του αλγορίθμου αποτελεί η σωστή εκτίμηση της μέσης πληρότητας της ουράς. Αυτή υπολογίζεται κάθε φορά που ένα πακέτο εισέρχεται στην ουρά, και ο υπολογισμός της γίνεται με τη χρήση ενός κατωπερατού φίλτρου. Επίσης ο RED έχει προβλέψει και την περίπτωση όπου να μεσολαβήσει μεγάλο χρονικό διάστημα μεταξύ 2 απορρίψεων πακέτων και εν τω μεταξύ να έχει παρουσιαστεί συμφόρηση. Αυτό μπορεί να παρατηρηθεί εξαιτίας του γεγονότος ότι η απόρριψη πακέτων γίνεται πιθανοτικά. Λύση σε αυτό το θέμα δίνει ένας μετρητής που χρησιμοποιείται και μετρά τον αριθμό των πακέτων που πέρασαν από την ουρά χωρίς απόρριψη. Έτσι η πιθανότητα απόρριψης πολλαπλασιάζεται τώρα και με την ποσότητα 1/1-c όπου c ο μετρητής αυτός.

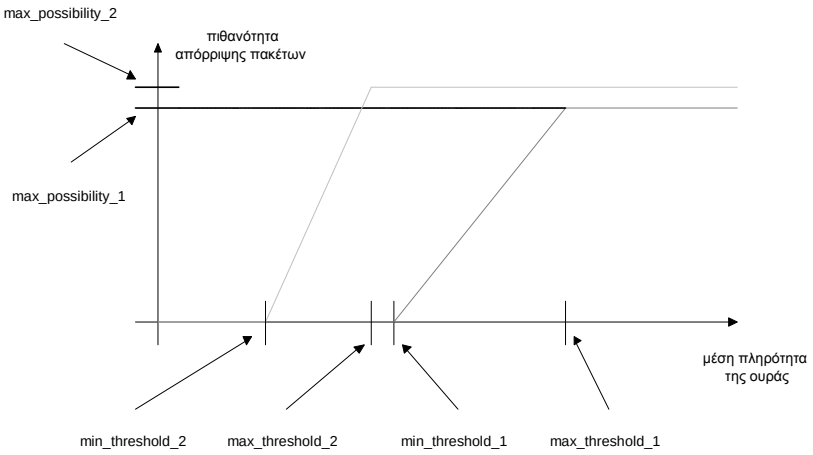
Γενικά ο μηχανισμός αυτός είναι ιδιαίτερα αποδοτικός, αλλά παρουσιάζει σημαντική δυσκολία στη ρύθμιση των παραμέτρων του. Το σημείο που πρέπει να τονιστεί είναι ότι απαιτείται να επιτρέπει να περνούν μικροεκρήξεις χωρίς απόρριψη πακέτων, ενώ αντίθετα θα πρέπει να αντιδρά άμεσα σε περιπτώσεις παρατεταμένης αύξησης της μέσης πληρότητας της ουράς. Τέλος προκειμένου να είναι πραγματικά αποδοτικός ο αλγόριθμος πρέπει πραγματικά να απορρίπτει πακέτα (άρα και να ειδοποιεί για συμφόρηση) από τις ροές που δημιουργούν το πρόβλημα.

Στη συνέχεια παρουσιάστηκαν διάφορες παραλλαγές του RED που προσπαθούσαν να εξαλείψουν ορισμένα μειονεκτήματα του. Τέτοιες ήταν ο Adaptive και ο Flow RED. Πάντως κυριότερη παραλλαγή του αποτελεί ο Weighted RED που περιγράφεται στην επόμενη ενότητα.

2.5.2.4.3 Μηχανισμός Weighted RED

Ο Weighted RED αποτελεί μια σημαντική παραλλαγή του κλασσικού RED μηχανισμού αφού επιτρέπει να συμπεριφέρεται η ουρά με διαφορετικό τρόπο (εφαρμόζοντας διαφορετικά κριτήρια) στα πακέτα μιας ροής. Στην πραγματικότητα δίνει τη δυνατότητα να μεταχειρίζεται τα πακέτα της ίδιας ροής με διαφορετικό τρόπο μεταξύ τους ανάλογα βέβαια με κάποιο κριτήριο.

Ο μηχανισμός αυτός λειτουργεί όπως ο απλός RED με τη διαφορά ότι σε αυτόν ορίζονται περισσότερες τριάδες μεταβλητών (Min_threshold, max_threshold, max_possibility), ίσες σε αριθμό με τον αριθμό των διαφορετικών τρόπων χειρισμού πακέτων που ζητείται. Ένα παράδειγμα αποτελεί να οριστούν 2 επίπεδα τιμών, με το δεύτερο αυστηρότερο από το πρώτο και να διαχειρίζονται με βάση το πρώτο τα πακέτα που καταφθάνουν κανονικά στην ουρά, ενώ αντίθετα με το δεύτερο επίπεδο τιμών τα πακέτα που είχαν μαρκαριστεί εκτός προφίλ σε προηγούμενο δρομολογητή.



Εικόνα 13: Η λειτουργία του μηχανισμού Weighted RED

2.5.2.5 Χρονοδρομολόγηση

Το επόμενο σημαντικό ζήτημα στη προσπάθεια ενός δικτύου να παρέχει εγγυήσεις ποιότητας είναι το θέμα της χρονοδρομολόγησης. Αναλύοντας της έννοια αυτή, σημαίνει ο τρόπος με τον οποίο χειρίζεται το δίκτυο τις ουρές, δηλαδή ποια ουρά στέλνει δεδομένα και για πόσο χρόνο. Ουσιαστικά ο μηχανισμός αυτός έχει στην διάθεσή του το σύνολο των ουρών που έχει ένας δρομολογητής και αποφασίζει με ποια σειρά θα μεταδώσουν πακέτα και για πόσο διάστημα η καθεμία.

Ο ρόλος του χρονοδρομολογητή είναι ιδιαίτερα κρίσιμος για ένα δίκτυο όταν επιθυμεί να προσφέρει και να παρέχει εγγυήσεις ποιότητας. Αυτό δικαιολογείται από το γεγονός ότι η λειτουργία του δρομολογητή καθορίζει την καθυστέρηση σε κάθε ουρά και τον τρόπο που διαμοιράζεται η γραμμή μετάδοσης μεταξύ των ουρών. Στην πραγματικότητα ο μηχανισμός του χρονοδρομολογητή είναι αυτός που καθορίζει το είδος της ποιότητας που παρέχει το δίκτυο. Οι παράμετροι αναλυτικά που μπορεί και επηρεάζει είναι:

- Η χωρητικότητα κάθε ροής, αφού μπορεί και ελέγχει κάθε πότε η ροή αυτή θα μεταδίδει.
- Την καθυστέρηση κάθε ροής, αφού ελέγχει όπως αναφέρθηκε παραπάνω το ρυθμό με τον οποίο κάθε ροή μεταδίδει, άρα καθορίζει και το χρονικό διάστημα που τα πακέτα παραμένουν στην ουρά.
- Επίσης ο χρονοδρομολογητής καθορίζει και το jitter, που είναι η διαφορά στην καθυστέρηση μεταξύ 2 διαδοχικών πακέτων.

Γενικά λοιπόν αυτοί είναι οι κύριοι παράμετροι που μπορεί να επηρεάσει ο χρονοδρομολογητής και συνεπώς προδιαγράφει την ποιότητα υπηρεσίας που μπορεί να παρέχει το δίκτυο. Επομένως εξαιτίας της σπουδαιότητας του μηχανισμού αυτού και του γεγονότος ότι οι μηχανισμοί χρονοδρομολόγησης που υπάρχουν είναι αρκετοί, είναι αναγκαίο η επιλογή του καταλληλότερου να γίνεται προσεκτικά και με βάση ορισμένα κριτήρια. Είναι απαραίτητο στην επιλογή του μηχανισμού χρονοδρομολόγησης να ελέγχεται πρώτα το είδος των εγγυήσεων που παρέχει και ο βαθμός επιτυχίας του, έτσι ώστε να ταιριάζει απόλυτα στη φύση των εφαρμογών που θα υποστηρίξει.

2.5.2.5.1 FIFO

Ο πρώτος μηχανισμός χρονοδρομολόγησης είναι ο λεγόμενος FIFO [1] και είναι ο παλαιότερος που υπάρχει. Ο μηχανισμός αυτός υποθέτει ότι υπάρχει μόνο 1 ουρά και η λογική του είναι ότι εξέρχεται από την ουρά το πρώτο πακέτο που μπήκε, δηλαδή κάθε φορά το παλαιότερο πακέτο μέσα στην ουρά. Ο μηχανισμός αυτός όπως γίνεται σαφές αντιμετωπίζει όλα τα πακέτα όμοια και δεν χρησιμοποιεί καμία έννοια προτεραιότητας.

Ο μηχανισμός αυτός έχει ως πλεονέκτημά του μόνο την απλότητα του και μπορεί να βρει εφαρμογή σε περιπτώσεις γραμμών μετάδοσης πολύ μεγάλης ταχύτητας όπου δεν υπάρχει καθόλου συμφόρηση, και ειδικότερα όταν η χρησιμοποίηση της γραμμής είναι πολύ χαμηλή. Αντιθέτως σε περιπτώσεις συμφόρησης έχει πολύ κακή απόδοση. Επίσης αντίστοιχα κακή απόδοση παρουσιάζει και στις περιπτώσεις όπου υπάρχουν εφαρμογές με καταιγισμούς που μπορεί να καταλαμβάνουν όλη την ουρά και να απορρίπτονται πακέτα άλλων εφαρμογών. Γενικά ο μηχανισμός αυτός είναι απλός και δεν ενδείκνυται για δρομολογητές που πρέπει να παρέχουν εγγυήσεις ποιότητας.

2.5.2.5.2 Priority Queueing (PQ)

Ένας δεύτερος μηχανισμός χρονοδρομολόγησης είναι ο Priority Queueing [3] ο οποίος σε αντίθεση με το μηχανισμό FIFO επιτρέπει διαφορετικές προτεραιότητες και μπορεί να χειριστεί πλήθος ουρών. Η λογική του είναι ότι μια ουρά έχει αυστηρή προτεραιότητα και πάντοτε εξυπηρετείται όταν έχει πακέτα σε βάρος των υπολοίπων ουρών. Ουσιαστικά λοιπόν ο μηχανισμός αυτός συμπεριφέρεται προνομιακά στην ουρά υψηλής προτεραιότητας αφού πάντοτε εκείνη μεταδίδει άμεσα και υποβαθμίζει τις υπόλοιπες.

Στην πράξη, τα πακέτα ανάλογα με την ταξινόμηση που έχουν δεχτεί εισέρχονται στην αντίστοιχη ουρά. Τότε ο PQ ελέγχει πάντοτε τις ουρές με τη σειρά, αρχίζοντας από την ουρά μεγαλύτερης προτεραιότητας και προχωρώντας προς την ουρά μικρότερης προτεραιότητας έως ότου βρει μια ουρά που έχει πακέτο και το μεταδίδει. Στη συνέχεια επαναλαμβάνει ξανά την ίδια διαδικασία.

Ο μηχανισμός αυτός εισάγει στο δίκτυο ένα είδος αδικίας καθώς ανάλογα με το ρυθμό που καταφτάνουν πακέτα στην ουρά υψηλής προτεραιότητας, μπορεί οι άλλες ουρές είτε να εξυπηρετούνται ελάχιστα είτε ακόμη και καθόλου. Το τελευταίο μπορεί να συμβεί αν ο ρυθμός με τον οποίο εισέρχονται πακέτα στην ουρά υψηλής προτεραιότητας ισούται με το ρυθμό μετάδοσης πάνω στο link. Αυτό μπορεί να διορθωθεί είτε με αστυνόμευση, είτε εφαρμόζοντας μορφοποίηση στην κίνηση υψηλής προτεραιότητας σε κάποιο προηγούμενο σημείο της διαδρομής.

Επικεντρώνοντας τώρα στα θετικά σημεία αυτού του μηχανισμού πρέπει να αναφερθεί ότι μπορεί και προσφέρει πολύ χαμηλή καθυστέρηση στα πακέτα που ανήκουν στην ουρά υψηλής προτεραιότητας. Σε αυτή την περίπτωση αν η ουρά αυτή δεν έχει πακέτα, μόλις θα φτάσει ένα, τότε θα περιμένει μέχρι να μεταδοθεί το πακέτο που μεταδίδεται εκείνη τη στιγμή. Στη περίπτωση που η ουρά έχει πακέτα θα περιμένει μέχρι να σταλούν τα προηγούμενα, κάτι που εξαρτάται από το μέγεθος αυτών και το bandwidth του link.

2.5.2.5.3 Modified Deficit Round Robin (M-DRR)

Στη συνέχεια ένας άλλος μηχανισμός χρονοδρομολόγησης, με πολλές επιλογές χρήσης και ιδιαίτερα αποδοτικός είναι ο M-DRR [94]. Αυτός στηρίζεται στη λογική του Deficit Round Robin (DRR) [13][65] και του Round Robin (RR), όπου κρίνεται σκόπιμο να περιγραφούν εν συντομία. Ο Round Robin αλγόριθμος χειρίζεται όλες τις ουρές όμοια και τις ελέγχει κυκλικά. Σε όποια βρει πακέτο στην αναμονή το μεταδίδει και συνεχίζει τον κυκλικό έλεγχο. Η μέθοδος συνεπώς αυτή έχει το μειονέκτημα ότι δεν μπορεί να παρέχει εγγυήσεις για την καθυστέρηση. Η μέθοδος DRR αποτελεί μια παραλλαγή της απλής μεθόδου Round Robin, όπου τώρα οι ουρές ελέγχονται ξανά κυκλικά αλλά προσπαθούν να διατηρούν σταθερό το μέσο ρυθμό μετάδοσης. Αυτό επιτυγχάνεται με την ακόλουθη τεχνική, σε κάθε ουρά ορίζονται 2 ποσότητες, το κβάντο Q και το έλλειμμα D. Το κβάντο είναι ο μέγιστος αριθμός bytes που μπορεί να μεταδώσει η ουρά κάθε φορά. Αν μεταδώσει λιγότερα τότε η διαφορά αποθηκεύεται στο έλλειμμα και προστίθεται στην μέγιστη τιμή bytes που θα μεταδώσει την αμέσως επόμενη φορά.

Ο μηχανισμός M-DRR λειτουργεί ουσιαστικά όπως ο DRR με τη διαφορά ότι εισάγει και μια ουρά προτεραιότητας ώστε να επιτυγχάνει χαμηλή καθυστέρηση. Οι υπόλοιπες ουρές εξυπηρετούνται με τη σειρά σύμφωνα με τον μηχανισμό DRR και η ουρά προτεραιότητας είτε εξυπηρετείται εναλλάξ με τις άλλες είτε κατά απόλυτη προτεραιότητα. Υπάρχουν 2 παραλλαγές του M-DRR όπου το σημείο που διαφέρουν είναι πόσο συχνά εξυπηρετείται η ουρά προτεραιότητας. Αναλυτικότερα αυτές είναι:

- Alternate Priority. Στη μέθοδο αυτή η ουρά προτεραιότητας εξυπηρετείται εκ περιτροπής με τις υπόλοιπες ουρές, οι οποίες εξυπηρετούνται με τη σειρά. Για παράδειγμα, εξυπηρετείται η ουρά προτεραιότητας, ύστερα η πρώτη από τις άλλες, μετά πάλι η ουρά προτεραιότητας, ύστερα η δεύτερη κοκ.
- Strict Priority. Αντίθετα στη μέθοδο αυτή η ουρά προτεραιότητας εξυπηρετείται κατά απόλυτη προτεραιότητα για όσο διάστημα έχει πακέτα προς μετάδοση. Όταν δεν έχει, εξυπηρετούνται οι υπόλοιπες σύμφωνα με τον DRR μηχανισμό.

Γενικά λοιπόν η μέθοδος Modified-Deficit Round Robin είναι ευέλικτη και αποδοτική μόνο όμως σε περιπτώσεις όπου δεν υπάρχει μεγάλη συμφόρηση. Γι' αυτό ακριβώς το λόγο προτείνεται να χρησιμοποιείται παράλληλα με ένα μηχανισμό διαχείρισης ουρών που προλαμβάνει τη συμφόρηση, όπως αυτοί που περιγράφηκαν στην προηγούμενη ενότητα

2.5.2.5.4 Fair Queueing – Weighted Fair Queueing

Η μέθοδος Fair Queueing [3] θεωρείται ως μια καλή παραλλαγή της μεθόδου Round Robin, όπου πλέον ο στόχος είναι να εξυπηρετεί όλες τις ουρές με τέτοιο τρόπο ώστε να ικανοποιείται μακροπρόθεσμα ο στόχος για ίσο μέσο εύρος ζώνης. Το ιδανικό για να ικανοποιηθεί ο στόχος είναι αν γινόταν η διαμοίραση σε επίπεδο bit (θα έστελνε η κάθε ουρά για σταθερό χρόνο 1/N, ιδανική διαμοίραση χρόνου), οπότε μπορούσε να μετέδιδε από συγκεκριμένο αριθμό bits από κάθε ουρά, επιτυγχάνοντας πλέον ίσο μέσο εύρος ζώνης. Όμως επειδή η χρονοδρομολόγηση γίνεται σε επίπεδο πακέτου, το αποτέλεσμα είναι πλέον προσεγγιστικό και μακροπρόθεσμο. Ουσιαστικά, η μέθοδος αυτή χρονοδρομολογεί τις μεταδόσεις πακέτων από τις ουρές με την σειρά με τη σειρά με την οποία θα είχαν καταφτάσει στο άλλο άκρο της γραμμής μετάδοσης αν είχε χρησιμοποιηθεί ο ιδανικός χρονοδρομολογητής διαμοίρασης χρόνου. Η μέθοδος Fair Queueing έχει 2 συγκεκριμένα μειονεκτήματα:

- Για να επιτύχει το στόχο της αυτή η μέθοδος χρονοδρομολόγησης πρέπει να σημαδεύει τα πακέτα και να υπολογίζει τον αναμενόμενο χρόνο αναχώρησής τους. Όμως, οι υπολογισμοί αυτοί είναι αρκετοί και χρονοβόροι με αποτέλεσμα τελικά να γίνονται προσεγγιστικά, γεγονός που οδηγεί σε βραχυπρόθεσμες αδικίες μερικές φορές.
- Η μέθοδος Fair Queueing είναι σχεδιασμένη να εφαρμόζεται στη περίπτωση ξεχωριστών ουρών για κάθε ροή προκειμένου να επιτυγχάνει να μην επηρεάζεται κάθε ροή από την ύπαρξη της άλλης. Η λογική αυτή όμως δεν μπορεί να λειτουργήσει με το μοντέλο της συγκέντρωσης ροών (aggregate classes).

Μια σημαντική παραλλαγή της Fair Queueing μεθόδου αποτελεί η μέθοδος Weighted Fair Queueing. Στόχος της μεθόδου αυτής είναι να αποδίδει βάρη σε κάθε ουρά επιτρέποντας να διαφοροποιείται το μέσο εύρο ζώνης που κάθε μια αντιλαμβάνεται. Αν για παράδειγμα υπάρχουν N ουρές με πακέτα προς μετάδοση τότε κάθε ουρά M εξυπηρετείται έτσι ώστε να λαμβάνει ποσοστό WM από το συνολικό ρυθμό της γραμμής. Σε περίπτωση που κάποιες από τις ουρές είναι άδειες τότε το επιπλέον εύρος ζώνης (που θα έπαιρναν οι ουρές αυτές) μοιράζεται αναλογικά στις υπόλοιπες ουρές με βάση πάντοτε τα βάρη τους.

2.5.3 EF-based υπηρεσίες

Οι υπηρεσίες EF-based [4] έχουν σαν στόχο να προσομοιώσουν τις εικονικές μισθωμένες γραμμές για την εξυπηρέτηση κίνησης που προέρχεται από συνένωση ροών, όπως προκύπτει από την εφαρμογή των μηχανισμών ταξινόμησης και μαρκαρίσματος. Οι υπηρεσίες αυτές απευθύνονται σε εφαρμογές πραγματικού χρόνου ευαίσθητες στο jitter και στην απώλεια πακέτων που απαιτούν εγγυήσεις χωρητικότητας. Ο ορισμός τους βασίζεται στα ακόλουθα σημεία:

- Στον καθορισμό της διεπαφής μεταξύ DiffServ domains έτσι ώστε και αυτό να εμφανίζει συμπεριφορά EF-based.
- Στον περιορισμό της χωρητικότητας που αφιερώνεται στην υπηρεσία για να αποφευχθεί αποκλεισμός της best effort κίνησης
- Σε μια αρχική στατική ρύθμιση των δικτυακών συσκευών για την παροχή της υπηρεσίας.
- Στην ελαχιστοποίηση των μηχανισμών που χρησιμοποιούνται ανά κόμβο.

Τα παραπάνω σημεία αποτελούν ένα συνοπτικό ορισμό των EF-based υπηρεσιών. Μια από αυτές είναι η IP Premium [10][21][61][102] και παρέχεται σε συνενώσεις IP κίνησης. Οι μηχανισμοί που απαιτούνται για την υλοποίηση της είναι αρχικά ένας μηχανισμός αποδοχής κλήσης, όπου συνήθως η αποδοχή κλήσης γίνεται με βάση τα SLAs. Επίσης απαιτείται ένας μηχανισμός ταξινόμησης σε συνενώσεις όπου γίνεται με βάση τις διευθύνσεις πηγής και προορισμού. Σύμφωνα με τον ορισμό της IP Premium υπηρεσίας αν τα πακέτα περιέχουν διευθύνσεις που εξυπηρετούνται από την υπηρεσία αυτή εντάσσονται στο aggregate της κίνησης στο interface εισόδου του router. Στην συνέχεια και αφού απομακρυνόμαστε από την πηγή η ταξινόμηση γίνεται αποκλειστικά με βάση το DSCP στην επικεφαλίδα του πακέτου. Η τιμή για το DSCP που συνιστάται για την υπηρεσία IP Premium είναι η τιμή 101110. Τέλος αν εμφανίζονται κοντά στην πηγή τους πακέτα να περιέχουν το IP premium DSCP αλλά μη συμβατό ζεύγος πηγής προορισμού απορρίπτονται σαν μη νόμιμα.

Η συνένωση IP Premium ροής που μπαίνει σε ένα DiffServ domain αρχικά υπόκειται σε μηχανισμό αστυνόμευσης. Αν η ροή βρίσκεται στο domain του χρήστη, τότε η αστυνόμευση γίνεται με βάση ένα token bucket και τις παραμέτρους του SLA μεταξύ του χρήστη και του δικτύου του πρόσβασης. Επίσης σε αυτό το σημείο ο χρήστης μπορεί να μορφοποιήσει και την κίνηση του αφού η υπηρεσία αυτή δεν επιτρέπει μορφοποίηση σε άλλο σημείο του δικτύου. Η διαδικασία της μορφοποίησης θεωρείται σημαντική καθώς οι buffers στις δικτυακές συσκευές κατά μήκος του μονοπατιού που ακολουθείται είναι περιορισμένοι με αποτέλεσμα αν δεν έχει μορφοποιηθεί επαρκώς η κίνηση, τότε αυτοί να γεμίζουν και πακέτα να απορρίπτονται. Μια πρόταση που έχει παρουσιαστεί είναι να γίνεται μορφοποίηση από την ίδια την πηγή.

Επίσης, στον ορισμό της IP Premium υπηρεσίας αναφέρεται ότι ο μηχανισμός αστυνόμευσης πρέπει να στηρίζεται σε ένα token bucket με βάθος μερικά πακέτα και χωρητικότητα ελαφρά μεγαλύτερη από αυτή που εγγυάται η υπηρεσία. Αυτό έχει σαν αποτέλεσμα να μπορούν να απορροφώνται και κάποιες μικρές αλλοιώσεις στα χαρακτηριστικά της κίνησης. Επειδή αποτελεί στόχο η ελαχιστοποίηση των μηχανισμών που χρησιμοποιούνται ανά κόμβο έχει προταθεί η αστυνόμευση να γίνεται μόνο στους κόμβους εισόδου σε DiffServ domains. Επίσης αυτό μπορεί να αποφευχθεί αν η κίνηση προέρχεται από κάποιο άλλο «έμπιστο» domain.

Για την υλοποίηση της IP Premium υπηρεσίας είναι απαραίτητο να χρησιμοποιείται αυστηρή κατά προτεραιότητα χρονοδρομολόγηση προκειμένου να επιτυγχάνεται η ελάχιστη δυνατή καθυστέρηση των πακέτων των IP συνενώσεων. Επίσης η υπηρεσία αυτή δεν απαιτεί μηχανισμούς διαχείρισης ουρών αφού προφανώς έχουν πολύ μικρό μήκος. Τέλος απαραίτητοι θεωρούνται οι μηχανισμοί διάδοσης των κανόνων εφαρμογής της υπηρεσίας και οι μηχανισμοί παρακολούθησης και καταγραφής της λειτουργίας της υπηρεσίας.

Μια δεύτερη υπηρεσία EF-based είναι η λεγόμενη QBone Premium η οποία ορίστηκε από τη ομάδα QBone του Internet2. Η υπηρεσία αυτή έχει σαν στόχο την παροχή εγγυήσεων χωρητικότητας χωρίς απώλειες πακέτων, με την ελάχιστη δυνατή καθυστέρηση και jitter σε κίνηση με περιορισμένο μέγιστο ρυθμό που διατρέχει πολλαπλά domains. Σε αυτή την υπηρεσία κρίσιμος παράγοντας αποτελεί επίσης η χρονοδρομολόγηση των πακέτων όπου πρέπει να είναι αυστηρής προτεραιότητας. Η πηγή καθορίζει 2 παραμέτρους, το μέγιστο ρυθμό και το μέγιστο μέγεθος έκρηξης και όταν η κίνηση ξεπερνά αυτό το προφίλ τότε τα πακέτα απορρίπτονται στο σημείο εισόδου που διαπιστώνεται η παράβαση.

Επικεντρώνοντας το ενδιαφέρον στις διαφορές της QBone Premium υπηρεσίας σε σχέση με την IP Premium διαπιστώνεται ότι η κυριότερη διαφορά τους είναι το γεγονός ότι η QBone Premium απαιτεί οι συνοριακοί κόμβοι ενός domain να υποστηρίζουν την μορφοποίηση της συνένωσης ροών που εξέρχονται από αυτούς.

Γενικά όλες οι υπηρεσίες που βασίζονται στο μοντέλο DiffServ και επομένως και η IP Premium παρουσιάζουν μια σημαντική δυσκολία που συνίσταται στη μελέτη και ανάλυση της ποιότητας υπηρεσίας που παρέχουν. Όπως είναι γνωστό αφορούν συνενώσεις ροών που η μορφή και τα χαρακτηριστικά τους δεν μπορούν να προσεγγιστούν εύκολα, ενώ επίσης δέχονται και αλλοίωση από τα IP δίκτυα. Συνεπώς για να υλοποιηθεί μια τέτοια υπηρεσία πρέπει εκτός από τον καθορισμό των παραμέτρων που αναφέρθηκαν παραπάνω, να ακολουθηθεί και μια πειραματική διαδικασία σε συνθήκες πραγματικής λειτουργίας προκειμένου να ρυθμιστούν όλες οι παράμετροι του δικτύου και να προκύψει το αναμενόμενο αποτέλεσμα.

Συνολικά, έχουν παρουσιαστεί διάφορες έρευνες για την απόδοση των παραπάνω υπηρεσιών. Τα σημεία τα οποία εξετάζονται είναι η επίδραση του μεγέθους της ουράς στην οποία εισέρχονται τα EF πακέτα, του αλγόριθμου δρομολόγησης και του μεγέθους των πακέτων. Παράλληλα ελέγχεται η επίδραση της ύπαρξης ή όχι best–effort κίνησης στην εγγυημένη, από την EF-based υπηρεσία, ποιότητα. Από τη διερεύνηση προέκυψε ότι όσο αφορά τη χρονοδρομολόγηση, η χρήση ουράς προτεραιότητας δίνει για κάθε μέγεθος πακέτου την ελάχιστη καθυστέρηση. Επίσης οι αλγόριθμοι Priority Queueing (PQ) και Weighted Fair Queueing (WFQ) παρουσιάζουν παρόμοιες μέσες τιμές για το jitter ενώ ο PQ ενδεχομένως να ελαχιστοποιεί το jitter σε σχέση με τον WFQ μόνο στην περίπτωση που ο WFQ έχει αριθμό ουρών μεγαλύτερο από 2. Τα συμπεράσματα αυτά επαληθεύτηκαν και στην περίπτωση όπου υπήρχε και best-effort κίνηση. Ορισμένες επιπλέον παρατηρήσεις είναι ότι η μέση καθυστέρηση φαίνεται να αυξάνεται γραμμικά με την αύξηση του μεγέθους του πακέτου, ενώ η αύξηση παρουσιάζεται περισσότερο απότομη με την απουσία best –effort κίνησης. Στη συνέχεια επικεντρώνοντας στο jitter παρουσιάζεται κατά την απουσία best effort κίνησης να αυξάνεται γραμμικά ενώ με την παρουσία της παρουσιάζει μεταβολές χωρίς να ακολουθεί συγκεκριμένη μορφή.

Τέλος, έχουν πραγματοποιηθεί μελέτες με μια σειρά πειραμάτων για την απόδοση που αντιλαμβάνεται η EF κίνηση κατά μήκος ενός DiffServ domain όπου υπάρχουν πολλά σημεία συγκέντρωσης ροών και επομένως πιθανά σημεία συμφόρησης. Τα βασικά συμπεράσματα είναι ότι η καθυστέρηση από άκρο σε άκρο είναι ανάλογη του αριθμού των σημείων που παρουσιάζουν συμφόρηση στη διαδρομή των πακέτων από την πηγή στον προορισμό. Παράλληλα οι καθυστερήσεις των EF πακέτων οφείλονται κυρίως στην καθυστέρηση στις ουρές. Επίσης η συνένωση πολλών ροών οδηγεί στην αύξηση της καθυστέρησης και του jitter και ιδίως στη δεύτερη περίπτωση η επίδραση του βαθμού συνένωσης είναι αντιστρόφως ανάλογη του μεγέθους των EF πακέτων. Παράλληλα jitter εμφανίζεται ακόμη και στις περιπτώσεις όπου δεν έχουμε best effort κίνηση αλλά υπάρχουν συνενώσεις EF κίνησης. Το γεγονός αυτό μάλλον οφείλεται στη συγκέντρωση πακέτων στις ουρές της EF κίνησης καθώς απομακρυνόμαστε από ην είσοδο του DiffServ domain.

Ανακεφαλαιώνοντας λοιπόν, στην υλοποίηση EF-based υπηρεσιών πρέπει να δοθεί ιδιαίτερη προσοχή για την εξάλειψη των παρενεργειών στην απόδοση εξαιτίας της δημιουργίας συνενώσεων καθώς η EF κίνηση διατρέχει ένα DiffServ enabled domain. Για να επιτευχθεί αυτό πρέπει να διατηρείται το φορτίο σε χαμηλά επίπεδα προκειμένου να μπορεί το δίκτυο να απορροφά τις εκρήξεις χωρίς επιβάρυνση της απόδοσης. Συνεπώς η σωστή υλοποίηση μιας EF-based υπηρεσίας πρέπει να επιτυγχάνει 2 πράγματα:

- Να έχουν ρυθμιστεί οι buffers να έχουν τόσες θέσεις ώστε να απορροφούν τις εκρήξεις και συνάμα
- Το μέγεθος των buffers να μην προκαλεί αύξηση της καθυστέρησης από άκρο σε άκρο λόγω παρατεταμένης παραμονής σε αυτούς πακέτων.

Επίσης σημαντικό παράγοντα αποτελεί και ο αλγόριθμος χρονοδρομολόγησης που θα επιλεγεί, όπου φαίνεται να υπερτερεί ο αλγόριθμος PQ έναντι του WFQ με βάση τις παραμέτρους ποιότητας. Όμως παρατηρήθηκε ότι σε μετρήσεις σε σχέση με την διασύνδεση πολλών κόμβων τους οποίους διατρέχουν οι συνενώσεις EF ροών, ο WFQ επιτυγχάνει μικρότερες εκρήξεις για τις διάφορες συνενώσεις. Μια πρόταση που έχει διατυπωθεί είναι η χρησιμοποίηση priority queueing σε συνδυασμό με μορφοποίηση της κίνησης στα κατάλληλα σημεία του δικτύου.

2.5.4 AF based Υπηρεσίες

Οι υπηρεσίες αυτές βασίζονται στην Assured Forwarding PHB [5] και στόχο τους αποτελεί να εγγυηθούν την εξυπηρέτηση μιας ροής που εναρμονίζεται με το συμφωνηθέν προφίλ με πολύ μεγάλη πιθανότητα και αντίστοιχα κίνηση που βρίσκεται εκτός προφίλ με μικρότερη πιθανότητα. Γενικά οι υπηρεσίες αυτές βρίσκονται σε πρώιμο στάδιο και αποτελεί θέμα διερεύνησης ο ακριβής καθορισμός τους και η λεπτομερειακή μελέτη της απόδοσης που μπορεί να επιτύχουν. Οι γενικοί κανόνες του AF PHB που χρησιμοποιούνται προκειμένου να οριστούν οι υπηρεσίες αυτές είναι οι ακόλουθοι:

- Δεν πρέπει να γίνεται συνένωση των ροών 2 διαφορετικών AF κλάσεων.
- Σε κάθε κλάση πρέπει να παρέχεται συγκεκριμένη ποσότητα πόρων και η κλάση πρέπει να επιτυγχάνει το ρυθμό της τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα.
- Η πιθανότητα εξυπηρέτησης ενός πακέτου πρέπει να είναι αντιστρόφως ανάλογη της προτεραιότητας εξυπηρέτησής του.
- Κάθε κόμβος πρέπει να δέχεται πακέτα και των όλων των επιπέδων προτεραιότητας και πρέπει να τα εξυπηρετεί με τουλάχιστον 2 διαφορετικά επίπεδα προτεραιότητας.
- Κάθε κόμβος πρέπει να διατηρεί αναλλοίωτη τη σειρά των πακέτων που ανήκουν στην ίδια ροή και στην ίδια κλάση AF.

Για να εφαρμοστεί μια AF-based υπηρεσία, στο σημείο εισόδου του domain γίνεται πρώτα σύγκριση του πραγματικού aggregate κίνησης με τα προκαθορισμένα και συμφωνημένα χαρακτηριστικά που θα έπρεπε να έχει. Έτσι η κίνηση εντός προφίλ μαρκάρεται με προτεραιότητα 1 (πράσινα πακέτα), κίνηση εκτός προφίλ αλλά εντός ενός ορίου σαν προτεραιότητας 2 (κίτρινα πακέτα) και τέλος η υπόλοιπη σαν προτεραιότητας 3 (κόκκινα πακέτα). Η διαδικασία αυτή συνήθως γίνεται με τη χρήση 2 συνεχόμενων leaky buckets που λειτουργούν όμως και σαν μορφοποιητές. Στη συνέχεια μέσα στο δίκτυο κάθε AF κλάση διαχειρίζεται διαφορετικά όσο αφορά το θέμα της απόρριψης πακέτων από τους μηχανισμούς διαχείρισης ουρών.

Μια πρώτη παρατήρηση για τις AF-based υπηρεσίες είναι ότι παρουσιάζουν ορατή βελτίωση στην ποιότητα εξυπηρέτησης μόνο στην περίπτωση που το δίκτυο βρίσκεται σε συμφόρηση. Επίσης ένα μειονέκτημα τους είναι το γεγονός ότι είναι προσανατολισμένες στους αποστολείς και όχι στους παραλήπτες. Έτσι, στην ειδική περίπτωση που ο παραλήπτης πρέπει να λαμβάνει πληροφορία με συγκεκριμένο ρυθμό, αυτό δεν είναι εφικτό διότι η συνένωση ροών που φτάνουν στον παραλήπτη μπορεί να προέρχονται από διαφορετικά σημεία εισόδου στο DiffServ domain.

Γενικά οι AF-based υπηρεσίες δεν παρέχουν συγκεκριμένες εγγυήσεις για την καθυστέρηση και το jitter, αφού κάτι τέτοιο αναιρεί τη δυνατότητα που έχουν οι συνενώσεις ροών να καταλαμβάνουν περισσότερους πόρους από όσους συμφωνήθηκαν, αν αυτοί είναι διαθέσιμοι. Συγκεκριμένα για την παροχή εγγυήσεων από τις AF-based υπηρεσίες ισχύουν:

- Για την εξασφάλιση χωρητικότητας σε over-provisioned δίκτυα (δίκτυα όπου έχουν γίνει κρατήσεις για περισσότερους πόρους από όσους είναι πραγματικά διαθέσιμοι, με την εκτίμηση ότι δεν θα χρησιμοποιηθεί η υπηρεσία από όλους τους πελάτες ταυτόχρονα στο όριο) είναι εφικτή η εγγύηση ρυθμού που αφορά

όμως μόνο την βασική πρόσβαση στους πόρους του δικτύου και όχι στην παροχή εγγυήσεων για χωρητικότητα που μπορεί να είναι αδιάθετη.

- Η πιθανότητα απόρριψης πακέτων μπορεί να είναι εγγυημένη μόνο όταν πρόκειται για SLAs μεταξύ 2 domains ενώ είναι δύσκολο και χρειάζεται ιδιαίτερη προσοχή η εγγύηση της από άκρο σε άκρο πιθανότητας απόρριψης.
- Τέλος για την καθυστέρηση ισχύουν ακριβώς τα ίδια όπως και στην περίπτωση της απόρριψης πακέτων.

Μια παραλλαγή των AF-based υπηρεσιών είναι οι Assured Data όπου χρησιμοποιούνται AF PHB και PDB όχι για τη διασφάλιση του ρυθμού αλλά για την διασφάλιση μετάδοσης συγκεκριμένων πακέτων. Για παράδειγμα ο μηδενισμός της πιθανότητας απόρριψης πράσινων πακέτων.

2.6 SERVICE LEVEL AGREEMENTS (SLA)

Στα σύγχρονα δίκτυα για να λειτουργούν ικανοποιητικά οι προηγμένες υπηρεσίες Quality of Service εμφανίζεται συχνά η ανάγκη εγγυημένης απόδοσης του δικτύου και εγγυημένης τιμής για ορισμένες παραμέτρους του δικτύου. Έτσι όταν συμφωνείται η παροχή και λήψη δικτυακών υπηρεσιών καθορίζονται και αντίστοιχες προδιαγραφές για το επίπεδο ποιότητας των προσφερομένων και λαμβανομένων υπηρεσιών.

Ο καθορισμός κατάλληλων προδιαγραφών για το επίπεδο λαμβανομένων υπηρεσιών είναι γενικότερα ένας πολύ καθοριστικός παράγοντας για την επιτυχημένη λήψη δικτυακών υπηρεσιών από εξωτερικούς παρόχους. Για το απλό παράδειγμα της διασύνδεσης με το Διαδίκτυο, είναι πολύ σημαντικό οι προδιαγραφές να καθορίζουν την ελάχιστη εγγυημένη χωρητικότητα της διασύνδεσης (που έχει επίπτωση στην ταχύτητα), τη διαθεσιμότητα της διασύνδεσης, και άλλες παραμέτρους που επιδρούν στο χρόνο απόκρισης των δικτυακών εφαρμογών, ώστε οι χρήστες να μην αντιμετωπίζουν συνεχή και μεγάλα προβλήματα.

Με τις προδιαγραφές για το επίπεδο των υπηρεσιών, ο αγοραστής των υπηρεσιών καθορίζει τα αποτελέσματα που θέλει να έχει, αλλά δεν καθορίζει τον τρόπο με τον οποίο ο προμηθευτής (πάροχος) της υπηρεσίας θα λειτουργεί την υπηρεσία. Οι προδιαγραφές του επιπέδου υπηρεσιών παίζουν δύο σημαντικούς ρόλους: εξασφαλίζουν την ευθύνη από πλευρά παρόχου και καθορίζουν το αντίτιμο για την παρεχόμενη υπηρεσία.

Οι προδιαγραφές επηρεάζουν επίσης και το κόστος παροχής των υπηρεσιών. Αγοραστές που επιθυμούν πολύ υψηλά επίπεδα υπηρεσιών δημιουργούν μεγαλύτερες ανάγκες σε πόρους του πάροχου και επομένως αυξάνουν το κόστος των υπηρεσιών. Για τους παραπάνω λόγους ο καθορισμός προδιαγραφών για το επίπεδο των υπηρεσιών είναι πολύ σημαντικός.

Ειδικότερα για τις υπηρεσίες QoS, τα SLAs που συντάσσονται αφορούν κύρια σε 2 παράγοντες:

1. Στη διαθεσιμότητα της υπηρεσίας στο δίκτυο. Τυπικές τιμές είναι της τάξης 95-99% στην ομαλή λειτουργία του δικτύου.
2. Στο ποσοστό κίνησης που ένας πάροχος μπορεί να χρησιμοποιήσει τις υπηρεσίες QoS. Το τελευταίο έχει εφαρμογή στις υπηρεσίες απόλυτης προτεραιότητας

(κύρια στις EF based υπηρεσίες), όπου ο πάροχος εφαρμόζει και αυστηρή αστυνόμευση στο συμφωνηθέν όριο.

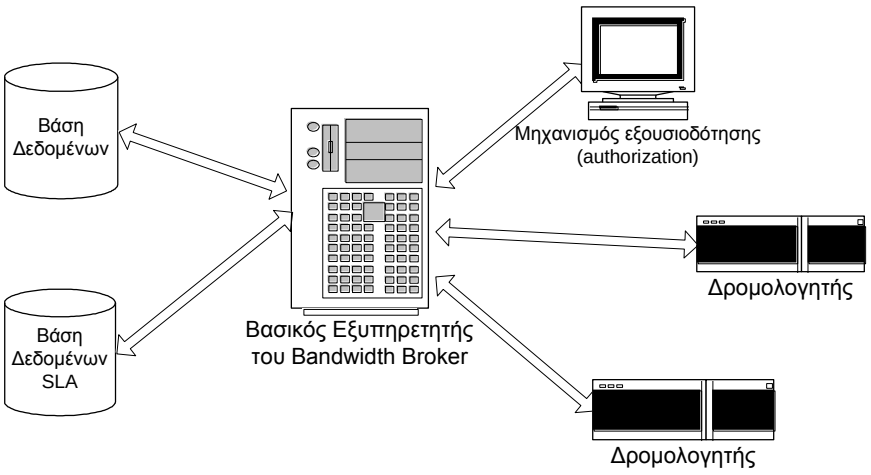
Γενικά, η υλοποίηση ενός αυστηρού SLA είναι μια πολύπλοκη διαδικασία και απαιτεί εξειδικευμένα βήματα αφού ένα SLA αποτελεί ένα εξειδικευμένο νομικό κείμενο με ευαίσθητες τεχνολογικές παραμέτρους.

ΚΕΦΑΛΑΙΟ 3: BANDWIDTH BROKERS

BANDWIDTH BROKERS

Η παροχή υπηρεσιών Ποιότητας Εξυπηρέτησης σε ένα σύγχρονο δίκτυο είναι αρκετά δύσκολη προσπάθεια καθώς απαιτεί την εμπλοκή πολλών ατόμων για την αποδοχή των αιτημάτων παροχής της υπηρεσίας και την αντίστοιχη διαμόρφωση του δικτύου. Η διαδικασία αυτή έχει γίνει προσπάθεια να αυτοματοποιηθεί σε μεγάλο βαθμό με την δημιουργία ενός ολοκληρωμένου συστήματος που λέγεται «Bandwidth Broker».

Ένας bandwidth broker αποτελείται από πολλές οντότητες που συνεργάζονται μεταξύ τους. Αρχικά, ο bandwidth broker έχει μια πλήρη καταγραφή του δικτύου και πρόσβαση στα SLAs που έχουν υλοποιηθεί στο δίκτυο. Επίσης, διατηρεί όλη την τοπολογία καθώς και τους δια-συνδεδεμένους φορείς που μπορούν να χρησιμοποιούν μια υπηρεσία QoS. Στη συνέχεια, ο bandwidth broker έχει κατάλληλες διεπαφές για καταγραφή αιτημάτων τα οποία και επεξεργάζεται με την εκτέλεση αλγορίθμων ελέγχου αποδοχής (admission control). Η λειτουργία των αλγορίθμων αυτών είναι να ελέγχουν τα αποθηκευμένα στοιχεία στη βάση δεδομένων και να αποκρίνονται αν το κάθε αίτημα μπορεί να γίνει αποδεκτό. Στη συνέχεια ο bandwidth broker αποθηκεύει στην βάση δεδομένων του τα αιτήματα και τις απαντήσεις τους και ξεκινά την διαδικασία για ενημέρωση των δρομολογητών ώστε τα αποδεκτά αιτήματα να εξυπηρετηθούν. Η επικοινωνία μεταξύ του Bandwidth broker server και των δρομολογητών γίνεται συνήθως μέσω ειδικού σκοπού διεπαφών (interfaces).



Εικόνα 14: Η βασική αρχιτεκτονική ενός Bandwidth Broker

Η λειτουργία ενός bandwidth broker σε ένα σύγχρονο δίκτυο αποτελεί ένα πολύ σημαντικό αυτοματοποιημένο εργαλείο διαχείρισης. Η επιτυχία στην δημιουργία ενός τέτοιου μηχανισμού έγκειται κυρίως στο πόσο έξυπνα είναι σχεδιασμένο ώστε να μπορεί να λειτουργεί και να παρακολουθεί τη λειτουργία του δικτύου αυτόματα όσο και να υποστηρίζει πολλαπλά SLAs τα οποία μπορούν να μεταβάλλονται. Επίσης, πολύ σημαντικό ζήτημα αποτελεί η δυνατότητα διασύνδεσής του με αντίστοιχους bandwidth brokers που λειτουργούν σε γειτονικά διαχειριστικά τμήματά του.

3.1 Η ΛΕΙΤΟΥΡΓΙΑ ΕΝΟΣ BANDWIDTH BROKER

Ένας Bandwidth Broker [53] διαχειρίζεται τους πόρους που βρίσκονται μέσα σε ένα συγκεκριμένο domain σύμφωνα με τις προδιαγραφές υπηρεσίας (Service Level Specifications-SLS) που έχουν συμφωνηθεί μέσα σε αυτό το domain. Οι προδιαγραφές υπηρεσίας είναι μια μετάφραση του συμβολαίου υπηρεσίας (Service Level Agreement-SLA) στην κατάλληλη πληροφορία η οποία είναι αναγκαία για την κατανομή και την παροχή των πόρων των δικτυακών συσκευών και ειδικά στα άκρα του domain, σε links που το συνδέουν με γειτονικά domains. Ο Bandwidth Broker είναι επίσης υπεύθυνος για τη διαχείριση της inter-domain επικοινωνίας, με Bandwidth Brokers γειτονικών δικτύων, ώστε να συντονίζονται οι προδιαγραφές υπηρεσίας κατά μήκος των ορίων όλων των domains.

Ο Bandwidth Broker συγκεντρώνει και παρακολουθεί την κατάσταση των πόρων που βρίσκονται εντός του δικού του domain και στις ακμές που συνδέουν αυτό το domain με τα γειτονικά domains. Αυτή η πληροφορία μαζί με την πληροφορία αστυνόμευσης (από την policy rules data base) χρησιμοποιείται για αποφάσεις αποδοχής κλήσης αιτημάτων για Ποιότητα Υπηρεσίας στο δίκτυο. Ο διαχειριστής αστυνόμευσης (policy manager), αν υπάρχει, επιβεβαιώνει τέτοια αιτήματα χρησιμοποιώντας τους κανόνες αστυνόμευσης, ελέγχοντας αν υπάρχουν συγκρούσεις με υπάρχοντα αιτήματα, λαμβάνοντας μέτρα ώστε να εκχωρούνται πόροι για συγκεκριμένες υπηρεσίες κλπ. Ο Bandwidth Broker χρησιμοποιεί την πληροφορία της κατάστασης του δικτύου και για να επιβεβαιώνει ότι όντως υπάρχουν διαθέσιμοι πόροι στο δίκτυο ώστε να εξυπηρετηθούν αιτήματα. Αυτή η πληροφορία μπορεί να λαμβάνεται απευθείας από τον Bandwidth Broker δια μέσου ενός interface με τον policy manager, ή ο Bandwidth Broker μπορεί να την διατηρεί σε μια βάση δεδομένων που την χρησιμοποιεί από κοινού με τον policy manager.

Κατά μήκος των ορίων των domains, οι προδιαγραφές υπηρεσίας μπορούν να είναι στη βάση συνενώσεων ροών, όπου οι συνενώσεις ροών γίνονται χρησιμοποιώντας ένα συγκεκριμένο πεδίο μαρκαρίσματος, όπως για παράδειγμα το DiffServ codepoint(DSCP). Μέσα σε ένα domain μπορούν να κατανέμονται πόροι σε ανεξάρτητες ροές χρησιμοποιώντας αιτήματα κατανομής πόρων (Resource Allocation Requests-RARs). Είναι ευθύνη του Bandwidth Broker να συντονίζει την κατανομή και την παροχή των πόρων του δικτύου στις συνενώσεις ροών που εισέρχονται ή εξέρχονται από το δικό του domain όταν δέχεται RARs.

Αιτήματα κατανομής πόρων (RAR – Resource Allocation Requests) στέλνονται στον Bandwidth Broker από τους χρήστες της υπηρεσίας ζητώντας τη χρήση των πόρων που παρέχονται μέσα σε ένα domain για μια συγκεκριμένη υπηρεσία. Το RAR περιέχει τον προορισμό της κίνησης για την οποία έγινε το αίτημα και ο Bandwidth Broker ελέγχει για το συγκεκριμένο προορισμό εάν η κίνηση είναι τοπική (εάν και ο προορισμός βρίσκεται εντός του domain που καλύπτει ο Bandwidth Broker) ή αν η κίνηση είναι προς κάποιο άλλο domain (εάν ο προορισμός βρίσκεται εκτός του domain που καλύπτει ο Bandwidth Broker). Πολλά RARs μπορούν να αντιστοιχίζονται σε ένα μοναδικό SLA. Όταν οι πόροι που καθορίζονται σε ένα SLS έχουν διανεμηθεί πλήρως σε υπάρχοντα RARs και ληφθεί ένα νέο RAR για τον ίδιο προορισμό, το RAR θα πρέπει να απορριφθεί ή το SLA θα πρέπει να επαναδιαπραγματευτεί.

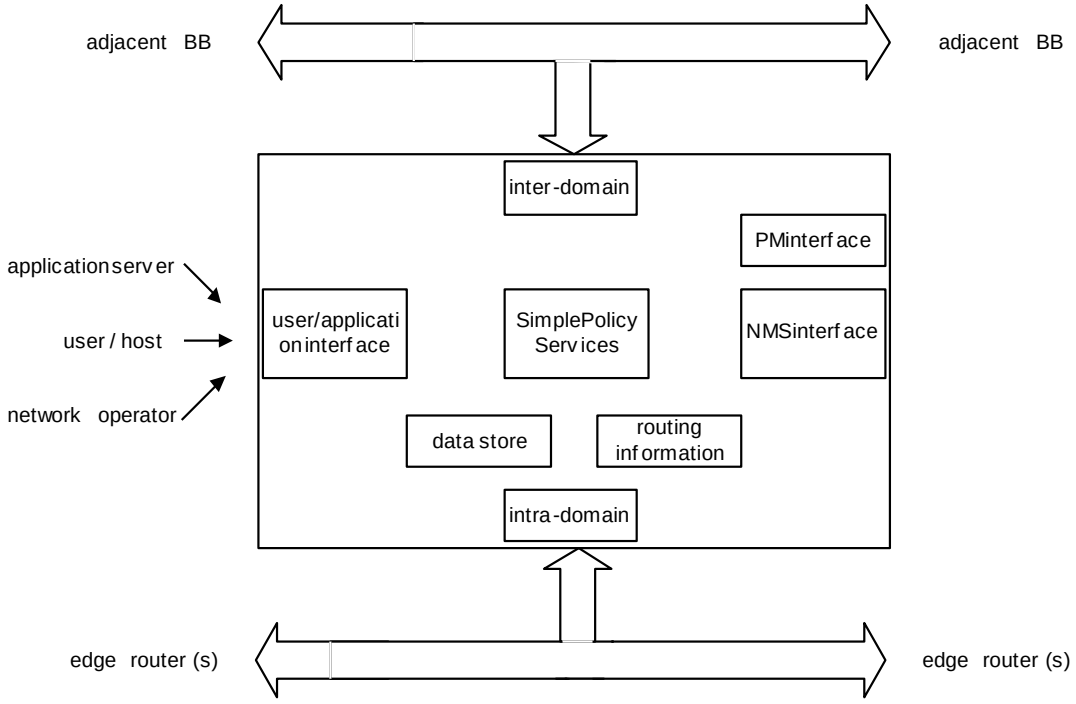
Της υλοποίησης ενός Bandwidth Broker προηγείται ο σχεδιασμός των τύπων QoS υπηρεσιών που θα υποστηρίζονται μέσα στο domain και από τον Bandwidth Broker,

η υλοποίηση των υπηρεσιών και των modules του bandwidth broker και στη συνέχεια ο σχεδιασμός της αντιστοίχησής τους με τις υπηρεσίες των γειτονικών domains.

3.2 ΤΑ MODULES ΕΝΟΣ BANDWIDTH BROKER

Ένας Bandwidth Broker έχει τις ακόλουθες λειτουργικές μονάδες:

- Το interface χρήστη / εφαρμογών (user/application interface)
- Το inter-domain interface
- Το intra-domain interface
- Το interface πινάκων δρομολόγησης (routing table interface)
- Το interface διαχείρισης της αστυνόμευσης (policy manager interface)
- Το interface διαχείρισης δικτύου (network management interface)
- Την αποθήκη δεδομένων (data repository)



Εικόνα 15: Τα modules ενός Bandwidth Broker

3.2.1 Interface χρήστη / εφαρμογών

Το user/application interface αποτελείται από τα παρακάτω τμήματα:

- Το GUI, έτσι ώστε ο χειριστής του δικτύου να μπορεί να:
  - διαχειρίζεται την αποθήκη δεδομένων χρησιμοποιώντας απλές εντολές
  - εισάγει απλούς κανόνες αστυνόμευσης στο σύστημα
  - εισάγει χειροκίνητα στο σύστημα αιτήματα για bandwidth προς τον Bandwidth Broker

- στέλνει ερωτήματα στον Bandwidth Broker για υπάρχουσες δεσμεύσεις υπηρεσιών, την παροχή πόρων και άλλα.
- ανταποκρίνεται στον χειριστή με σφάλματα και άλλα.

- Το User interface, το οποίο χρησιμοποιείται ώστε:
  - Οι εφαρμογές των χρηστών να μπορούν απευθείας να στείλουν αιτήματα για bandwidth στον Bandwidth Broker
  - Οι χρήστες να μπορούν να στέλνουν ερωτήματα στον Bandwidth Broker για τις υπάρχουσες δεσμεύσεις υπηρεσιών που τους έχουν χορηγηθεί. Απαιτείται ασφάλεια έτσι ώστε να μην είναι δυνατό κάποιος χρήστης να δει τις δεσμεύσεις εφαρμογών άλλων χρηστών
  - Να υπάρχουν μηχανισμοί που να ανταποκρίνονται στον χρήστη ή στην εφαρμογή
  - Ως προς το interface χρήστη, μπορεί να χρησιμοποιηθεί το ίδιο GUI όπως και αυτό του χειριστή δικτύου. Για τις εφαρμογές απαιτείται η ύπαρξη ενός πρωτοκόλλου ή καλύτερα ένα Web Service.

3.2.2 Inter-Domain interface

Το inter-domain interface έχει τη μορφή ενός πρωτοκόλλου αιτήματος-επιβεβαίωσης. Οι Bandwidth Brokers που επιθυμούν να επικοινωνήσουν χρειάζεται αρχικά να εγκαταστήσουν συνδέσεις μεταξύ των ζευγών των γειτονικών Bandwidth Brokers και στη συνέχεια χρησιμοποιώντας αυτές τις συνδέσεις να ανταλλάξουν τα RARs. Οι συνδέσεις μεταξύ των Bandwidth Brokers γίνονται πάντα κατά ζεύγη και είναι και προς τις δύο κατευθύνσεις (και οι δύο Bandwidth Brokers μπορούν να ζητήσουν πόρους ο ένας από τον άλλο). Παρόλα αυτά, τα SLAs είναι προς μια κατεύθυνση (δηλαδή χρειάζεται να εγκατασταθούν δύο SLAs, ένα προς κάθε κατεύθυνση).

Τα στάδια κατά τη λειτουργία του πρωτοκόλλου είναι:

- Αρχικό Configuration: Το module αυτό φορτώνει τοπική πληροφορία για το configuration καθώς ξεκινά
- Αρχικοποίηση Σύνδεσης: Μετά το ξεκίνημα, οι Bandwidth Brokers εγκαθιστούν συνδέσεις με τους γειτονικούς Bandwidth Brokers
- Έναρξη Υπηρεσίας: Οι συνδεδεμένοι Bandwidth Brokers ανταλλάσσουν αιτήματα για υπηρεσίες για τις οποίες έχουν συμφωνηθεί στα SLAs
- Κατανομή Πόρων: Οι Bandwidth Brokers ζητούν πόρους και απαντούν σε αιτήματα κατανομής πόρων.

Εκτός από τα παραπάνω μπορεί να υποστηρίζεται επιπρόσθετες δυνατότητες όπως η διαπραγμάτευση, διαχείριση και συντήρηση πόρων. Επίσης είναι σημαντικό να υπάρχει υποδομή τέτοια ώστε ο Bandwidth Broker να ανέχεται σφάλματα του συστήματος όπως το να διακόπτεται η λειτουργία κάποιου ανεξάρτητου Bandwidth Broker ή μια σύνδεση μεταξύ δύο Bandwidth Brokers.

3.2.2.1 Αρχικό Configuration

Ο καθορισμός μιας υπηρεσίας μεταξύ δύο domains και των αρχικών διαθέσιμων πόρων που θα υποστηρίζουν αυτήν την υπηρεσία δεν ορίζεται με επικοινωνία μεταξύ των Bandwidth Brokers. Εξάλλου, ο καθορισμός των πόρων, άλλων παραμέτρων όπως τα DS code points, η PHB μεταχείριση και η κίνηση εκτός του προφίλ (out-of-profile traffic) πρέπει να συμφωνηθούν πριν ξεκινήσει η inter-domain επικοινωνία.

Όλοι οι Bandwidth Brokers θα πρέπει να έχουν πρόσβαση στις ακόλουθες πληροφορίες που αφορούν τις inter-domain και τις intra-domain συνδέσεις των routers που βρίσκονται στα όρια του κάθε domain:

- Μέγιστη διαθεσιμότητα πόρων ανά υπηρεσία
- Πληροφορία για τη διαστασιολόγηση και το σχεδιασμό κάθε Υπηρεσίας
- Αντιστοίχηση Υπηρεσίας – PHB
- Αντιστοίχηση Υπηρεσίας – DSCP
- SLA ID
- Μεθόδους σηματοδότησης οι οποίοι είναι επιτρεπτοί από το SLA

3.2.2.2 Αρχικοποίηση Σύνδεσης

Πριν ξεκινήσουν οποιεσδήποτε υπηρεσίες μεταξύ δύο domains, οι Bandwidth Brokers χρειάζεται να συνδεθούν ώστε να εξασφαλιστεί η επικοινωνία. Κατά τη διάρκεια αυτής της διαδικασίας αρχικοποίησης, ο Bandwidth Broker διαβιβάζει:

- τα AS που βρίσκονται στο δικό του domain
- τη διεύθυνση – το id του Bandwidth Broker ο οποίος πρόκειται να στείλει αίτημα
- τη λίστα των γειτονικών του Bandwidth Brokers

Όλες αυτές οι πληροφορίες είναι υποχρεωτικές. Σε ένα περιβάλλον όπου υπάρχουν περισσότεροι Bandwidth Brokers από έναν, δύο domains μπορούν να έχουν πολλαπλές συνδέσεις μεταξύ τους. Αυτό προσφέρει πλεονασμό σε περίπτωση κάποιας βλάβης.

3.2.2.3 Διαχείριση Υπηρεσιών

Οι Bandwidth Brokers είναι υπεύθυνοι για τη διαχείριση των υπηρεσιών οι οποίες είναι διαθέσιμες στους πελάτες μέσω του inter-domain και του intra-domain interface. Οι υπηρεσίες έχουν συμφωνηθεί σε SLAs και έχουν οριστεί οι αντίστοιχες προδιαγραφές υπηρεσίας SLSs. Οι λειτουργίες για τη διαχείριση των SLSs περιλαμβάνουν:

- Έναρξη της Υπηρεσίας (υποχρεωτικό)

Πριν από την έναρξη μιας υπηρεσίας μεταξύ δύο domains, οι peer Bandwidth Brokers πρέπει να διαμορφωθούν με ένα συνεπή τρόπο όσον αφορά τη διμερή συμφωνία για αυτή την υπηρεσία. Όλοι οι πόροι που είναι αναγκαίοι για την υποστήριξη της υπηρεσίας θα πρέπει να παρέχονται και να κατακρατούνται σε κάθε τοπικό domain. Όταν οριστούν οι πόροι που διαχειρίζεται ο κάθε Bandwidth Broker, μπορούν να δημιουργηθούν μηνύματα αιτημάτων για την έναρξη υπηρεσίας (Service Setup

Requests - SSR). Το SSR μήνυμα είναι ένας απλός μηχανισμός ώστε ένας Bandwidth Broker να επιβεβαιώσει το SLA μεταξύ αυτού και κάποιου άλλου Bandwidth Broker και να επιβεβαιώσει στον άλλο ότι υπάρχουν οι αναγκαίοι πόροι ώστε να τηρηθεί το SLA.

Ένα SSR μήνυμα μπορεί να ξεκινήσει με διάφορους τρόπους:

- Με εντολή του διαχειριστή δικτύου
- Αυτοματοποιημένα με την εκκίνηση του συστήματος ή την επανεκκίνηση

Ο παραλήπτης Bandwidth Broker θα ελέγξει τη συνέπεια όσον αφορά το SLS με την πληροφορία που έχει αποθηκεύσει στη δικιά του βάση δεδομένων. Αν υπάρχει συνέπεια, ο Bandwidth Broker απαντά με ένα μήνυμα Απάντησης Εκκίνησης (Set up Answer - SA). Κάθε Bandwidth Broker πρέπει να ελέγχει ότι όλοι οι πόροι είναι ενεργοί ή διατεθειμένοι σε υπηρεσίες. Η κατάσταση των πόρων πρέπει να ανανεώνεται κάθε φορά που εγκρίνεται ένα SA. Πρέπει εδώ να σημειωθεί ότι η υπηρεσία δεν είναι συμμετρική.

- Αναβολή της Υπηρεσίας (υποχρεωτικό)

Εάν ένα SLA τερματιστεί, η υπηρεσία πρέπει να αναβληθεί. Το μήνυμα Αναβολής Υπηρεσίας (Service Cancellation - SC μπορεί να ξεκινήσει από μια εντολή ενός διαχειριστή δικτύου ή μπορεί να ενεργοποιηθεί σε κάποια ημερομηνία λήξης. Ένα SC ελέγχεται για συνέπεια κατά τη λήψη και στέλνεται η Απάντηση Αναβολής (Cancellation Answer - CA). Το CA περιέχει τα ίδια πεδία με το SC. Όταν στέλνεται το CA, ο Bandwidth Broker ανανεώνει την κατάσταση όλων των πόρων που είχαν κατακρατηθεί για τη συγκεκριμένη υπηρεσία. Επειδή από τη φύση της μια υπηρεσία είναι προς μια κατεύθυνση, μια υπηρεσία μπορεί να αναβάλλεται στην κατεύθυνση από τον Χ στον Υ ενώ παραμένει ενεργή από τον Υ στον Χ.

- Επαναδιαπραγμάτευση της Υπηρεσίας (προαιρετικό)

Ένα SLA μπορεί να επιτρέπει στον Bandwidth Broker να επανα-διαπραγματεύεται μια υπάρχουσα υπηρεσία. Αυτό επιτυγχάνεται με ένα μήνυμα Επαναδιαπραγμάτευσης Υπηρεσίας (Service Renegotiate - SR). Τα SR μηνύματα μπορούν να δημιουργηθούν είτε χειροκίνητα από τον διαχειριστή ενός δικτύου είτε αυτόματα από τον Bandwidth Broker όταν η κίνηση που λαμβάνει την υπηρεσία υπερβαίνει ένα κατώφλι. Αν χρειάζεται να προστεθούν επιπρόσθετοι πόροι για κάποια υπηρεσία, η κατάσταση των νέων πόρων που διατέθηκαν πρέπει να ενημερωθεί στην βάση δεδομένων του Bandwidth Broker.

Το SR εγκρίνεται από ένα SA μήνυμα. Μετά την έγκριση οι επιπρόσθετοι πόροι έχουν προστεθεί και στα δύο domains και η υπηρεσία είναι έτοιμη για χρήση. Και οι δύο Bandwidth Brokers χρειάζεται να ανανεώσουν τις παραμέτρους αστυνόμευσης και τα προφίλ κίνησης στους routers που βρίσκονται στα domain τους.

3.2.2.4 Κατανομή Πόρων

Αφού ολοκληρωθεί η αρχική διαδικασία εκκίνησης της υπηρεσίας, η υπηρεσία είναι διαθέσιμη αλλά δεν έχει ακόμα κατανεμηθεί σε συγκεκριμένες ροές. Ο Bandwidth Broker δεν πρέπει να επιτρέψει στη διαθέσιμη υπηρεσία να χρησιμοποιηθεί έως ότου λάβει RARs για την υπηρεσία μέσα από το domain και SLS μεταξύ των domains.

Τα RAR αιτήματα μέσα σε ένα domain επιτρέπουν σε ένα χρήστη η διαχειριστή δικτύου να ζητήσει πόρους από τον Bandwidth Broker. Τα RARs επίσης επιτρέπουν

στον Bandwidth Broker μέσα σε ένα domain να καταγράφει την πραγματική ποσότητα μιας διαθέσιμης υπηρεσίας που έχει διανεμηθεί σε κίνηση μέσα στο domain, και βασισμένος σε αυτό να παίρνει αποφάσεις αποδοχής (admission control).

Η κατανομή πόρων περιλαμβάνει μηνύματα αιτήματος και απόκρισης, τα RARs και RAA αντίστοιχα. Τα RARs και RAAs χρησιμοποιούνται και στο intra-domain interface. Το Resource Allocation Request περιλαμβάνει τα παρακάτω πεδία αλλά πιθανόν και άλλα αναλόγως του σχεδιασμού και των απαιτήσεων των QoS υπηρεσιών που διαχειρίζεται:

- RAR_ID
- DS_egress_router_ID
- DSCP (πιθανόν να είναι περισσότερα από ένα)
- DSCP για τα downstream domains (ένα ανά DSCP)
- Παράμετροι όπως: διεύθυνση αποστολέα, διεύθυνση προορισμού, πρωτόκολλα, αριθμοί των ports, πληροφορία για το προφίλ, παράμετροι διαπραγμάτευσης

3.2.2.5 Διατήρηση της σύνδεσης

Το πρωτόκολλο το οποίο υλοποιεί το inter-domain interface, εκτός από την ανταλλαγή μηνυμάτων που αφορούν κατακράτηση πόρων, θα πρέπει να υποστηρίζει και ένα σύνολο λειτουργιών διατήρησης της σύνδεσης. Αυτές οι λειτουργίες περιλαμβάνουν:

1. Το πρωτόκολλο θα μπορούσε να χρησιμοποιεί ένα ήδη υπάρχον connection oriented transport πρωτόκολλο, όπως το TCP
2. Διαδικασία Keep Alive
3. Ένα μηχανισμό που να αντιμετωπίζει επιτυχώς κάποιο σταμάτημα ή βλάβη κάποιου Bandwidth Broker και τη διακοπή της επικοινωνίας μεταξύ Bandwidth Brokers. Θέματα που θα πρέπει να προσεχτούν είναι :
    - Ένας Bandwidth Broker που ξαναρχίζει να λειτουργεί πρέπει να ξανακατασκευάζει την κατάστασή του.
    - Ένας Bandwidth Broker που πρόσφατα ξανάρχισε να λειτουργεί χρειάζεται να ενημερώσει τους γειτονικούς Bandwidth Brokers για την κατάστασή του.
    - Ένας Bandwidth Broker που πρόσφατα ξανάρχισε να λειτουργεί είναι υπεύθυνος για το συγχρονισμό και τις επαναδιαπραγματεύσεις με τους γειτονικούς Bandwidth Brokers για τις υπηρεσίες και την κατανομή των πόρων.
4. Το interface θα πρέπει να περιλαμβάνει timers οι οποίοι να λήγουν στην περίπτωση χαμένων ή καθυστερημένων απαντήσεων.
5. Απαιτείται να υπάρχει μια προκαθορισμένη συμπεριφορά που να αφορά τη διαχείριση μη προσδοκώμενων μηνυμάτων (π.χ. απαντήσεις χωρίς να έχει γίνει κάποιο αίτημα) και μη προσδοκώμενες παράμετροι σε μηνύματα

3.2.2.6 Το πρωτόκολλο SIBBS

Το interdomain πρωτόκολλο που έχει προταθεί τελευταία ονομάζεται SIBBS (Simple Interdomain Bandwidth Broker Signalling) [105].Το πρωτόκολλο αποτελείται από ένα απλό πρωτόκολλο αίτησης-απάντησης ανάμεσα στους γειτονικούς bandwidth brokers και έχει ως αποστολή να μεταφέρει την απαραίτητη πληροφορία για την αίτηση μια υπηρεσίας γενικά. Το πρωτόκολλο είναι sender-oriented και αναμένεται στο μέλλον να επεκταθεί για να γίνει (προαιρετικά) receiver-oriented.

Το πρωτόκολλο SIBBS αποτελεί πρόταση ως ένα νέο QoS πρωτόκολλο σηματοδότησης που θα χρησιμοποιηθεί σε ερωτήσεις και απαντήσεις απλών συναθροιστικών αιτημάτων υπηρεσίας. Τα γειτονικά domain τα οποία ελέγχονται από τους bandwidth brokers πρέπει να είναι DiffServ (differentiated service). Αυτό που ορίζει το πρωτόκολλο είναι οι διεπαφές σηματοδότησης(signaling interfaces) ανάμεσα στα γειτονικά domains και όχι οι λεπτομέρειες των SLA και τα μέσα διαχείρισης των δικτυακών πόρων του εκάστοτε domain. Άλλωστε θα υπάρξει σημαντική ποικιλία των υλοποιήσεων και των στρατηγικών διαχείρισης πόρων πίσω από την ομοιόμορφη διεπαφή σηματοδότησης. Το πρωτόκολλο αυτό λοιπόν αλληλοσυνδέεται καλά με τις end-to-end δυνατότητες σηματοδότησης των hosts και είναι αρκετά απλό για την διευκόλυνση γρήγορης υλοποίησης ενώ παραμένει αρκετά εύκαμπτο για να υποστηρίξει μελλοντική βελτιστοποίηση απόδοσης και επέκταση πρωτοκόλλου.

3.2.3 Intra-Domain Interface

Το intra-domain interface είναι το interface που χρησιμοποιείται για την επικοινωνία του Bandwidth Broker με τους routers που βρίσκονται στο τοπικό του domain ώστε να κατανέμονται κατάλληλα οι πόροι αυτού του domain. Το intra-domain interface υλοποιείται σαν μια αυτοματοποιημένη διαδικασία. Κάθε αυτοματοποιημένη διαδικασία πρέπει να βασίζεται στους μηχανισμούς του router για configuration, όπως αυτοί παρέχονται από τους κατασκευαστές. Οι κυριότεροι από αυτούς τους μηχανισμούς είναι οι:

- Το πρωτόκολλο COPS (Common Open Policy Service)
- Το πρωτόκολλο SNMP (Simple Network Management Protocol)
- Το πρωτόκολλο telnet

Γενικά, το intra-domain interface θα πρέπει να επιτρέπει στον Bandwidth Broker να διαχειρίζεται τις QoS υπηρεσίες (κύρια DiffServ based) σε κάθε router που δρομολογεί πακέτα στο domain. Αυτό θα πρέπει υποχρεωτικά να περιλαμβάνει τους ακραίους routers αλλά μπορεί να περιλαμβάνει και άλλους routers που δεν βρίσκονται στα άκρα του domain. Η διαχείριση ενός DiffServ router περιλαμβάνει το configuration και τον έλεγχο των διάφορων Traffic Conditioning παραμέτρων σε κάθε interface ενός router.

3.2.4 Routing Interface

Όταν γίνεται η επεξεργασία ενός αιτήματος για bandwidth, ο Bandwidth Broker χρειάζεται να έχει πρόσβαση στην πληροφορία δρομολόγησης στο δίκτυο. Ο βαθμός αναγκαιότητας και η ποσότητα της πληροφορίας δρομολόγησης εξαρτάται από την

διαστασιολόγηση του δικτύου και των QoS υπηρεσιών. Συνήθως χρησιμοποιείται ώστε να ληφθούν οι αποφάσεις του ελέγχου αποδοχής και επίσης να παραχθούν αυτόματα οι παράμετροι αστυνόμευσης για κάθε νέο αίτημα. Ο Bandwidth Broker χρειάζεται να γνωρίζει πληροφορία τόσο για την inter-domain όσο και για την intra-domain δρομολόγηση.

3.2.5 Policy Manager Interface & Network Manager Interface

Το Policy Manager interface χρησιμοποιείται για να παρέχει πλήρη έλεγχο αποδοχής. Υλοποιεί τον συντονισμό των συμβολαίων υπηρεσίας και των πόρων του δικτύου. Επίσης, με αυτό το interface παρέχονται οι AAA λειτουργίες.

Το Network Manager interface χρησιμοποιείται για το συντονισμό και την παρακολούθηση του δικτύου. Η ύπαρξη ενός Network Manager interface είναι απαραίτητη αλλά σε πολλές περιπτώσεις αυτά υλοποιούνται εκτός του bandwidth broker και ο τελευταίος απλά χρησιμοποιεί την αποθηκευμένη πληροφορία.

3.3 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ BANDWIDTH BROKER

Στην ενότητα αυτή παρουσιάζονται προτεινόμενες αρχιτεκτονικές από τη σχετική βιβλιογραφία για το σχεδιασμό Bandwidth Brokers. Σκοπός είναι να παρουσιαστούν τα πλεονεκτήματα και τα μειονεκτήματα των διαφόρων στρατηγικών για το σχεδιασμό ενός Bandwidth Broker. Πολλοί ερευνητές έχουν δουλέψει σε αυτή την περιοχή παράγοντας διάφορες λύσεις, κάθε μία από τις οποίες είναι δυνητικά κατάλληλη για κάποιες καταστάσεις και αδύναμη για άλλες.

	University of Kansas	**MIPTel**	**QBone**	**UCLA**	**Υλοποίηση στον NS-2 του CEID**
Αρχιτεκτονική	Κεντρικοποιημένη	Κεντρικοποιημένη	Κεντρικοποιημένη, αλλά μπορεί να επεκταθεί για κατανεμημένη	Κατανεμημένη	Κατανεμημένη
Έλεγχος αποδοχής	Διατηρεί και χρησιμοποιεί βάση δεδομένων με πολιτικές (policy database)	Προκαθορισμένο όριο στο εύρος ζώνης	Πίνακας απαιτήσεων κίνησης (traffic demand matrix)	Αποδοχή αν δεν παραβιάζεται το SLA	Περιορίζεται από το διαθέσιμο εύρος ζώνης
Πίνακας δρομολόγησης	Όχι	Ναι	Ναι	Ναι	Όχι
Ασφάλεια	Μη καθορισμένη	Μη καθορισμένη	Μη καθορισμένη	Μη καθορισμένη	Μη καθορισμένη
Ευρωστία (Robustness) / Επανάκαμψη από αστοχίες	Μη καθορισμένη	Μη καθορισμένη	Επανάκαμψη από τις πιο κοινές αστοχίες	Επανάκαμψη από τις πιο κοινές αστοχίες	Μη καθορισμένη

	University of Kansas	**MIPTel**	**QBone**	**UCLA**	**Υλοποίηση στον NS-2 του CEID**
Inter-domain interface	TCP sockets για Linux δρομολογητές / Telnet αυτοματοποιημένο script για Cisco δρομολογητές	Εξειδικευμένο πρωτόκολλο	Εξειδικευμένο πρωτόκολλο	Εξειδικευμένο πρωτόκολλο	TCP
Intra-domain interface	TCP sockets για Linux δρομολογητές / αυτοματοποιημένο script για Cisco δρομολογητές	Εξειδικευμένο πρωτόκολλο	COPS / SNMP / Telnet	COPS	TCP
Interface με το χρήστη	Web-based GUI	Ανταλλαγή μηνυμάτων	GUI, Host/Χρήστης, Server / Gateway Interface	Web-based GUI (PHP)	–

Πίνακας 2: Σύγκριση διαφόρων αρχιτεκτονικών Bandwidth Broker

Μερικές από τις αρχιτεκτονικές που συγκρίνει ο Πίνακας 2 έχουν υλοποιηθεί, όπως οι αρχιτεκτονικές του University of Kansas, του QBONE και του UCLA, ενώ άλλες είναι θεωρητικές ή σε φάση σχεδιασμού και αξιολόγησης. Ο πίνακας καταδεικνύει τη γκάμα χαρακτηριστικών των προτεινόμενων και υλοποιημένων αρχιτεκτονικών Bandwidth Broker που μπορεί να βρει κανείς στην τρέχουσα βιβλιογραφία. Πρέπει επίσης να σημειωθεί ότι όπως δείχνει και ο πίνακας, οι κατανεμημένες αρχιτεκτονικές δεν είναι τόσο συνηθισμένες όσο οι κεντρικοποιημένες.

Οι περισσότερες εργασίες προτείνουν Bandwidth Brokers που αποτελούνται από μία κεντρική μονάδα που ασχολείται με λειτουργίες όπως έλεγχο αποδοχής, inter-domain επικοινωνία, διατήρηση ενός interface με τον πίνακα δρομολόγησης, σύνδεση στους δρομολογητές του δικτύου και αποστολή των κατάλληλων παραμέτρων διαμόρφωσης.

Προκειμένου να ξεπεράσουν τα προβλήματα κλιμάκωσης που σχετίζονται με το μοντέλο του κεντρικοποιημένου Bandwidth Broker και να αποφύγουν να έχουν τον Bandwidth Broker ως το σημείο "μποτιλιαρίσματος" (bottleneck) ενώ το δίκτυο το ίδιο υπο-χρησιμοποιείται, έχουν προταθεί και κατανεμημένες αρχιτεκτονικές Bandwidth Broker. Αυτές αποτελούνται από έναν κεντρικό Bandwidth Broker (cBB) και έναν αριθμό από περιφερειακούς Bandwidth Broker (eBB) στο διαχειριστικό τμήμα. Υπάρχουν δύο επίπεδα που αντιπροσωπεύουν τις καταστάσεις QoS, οι link level και path level. Η ιδέα είναι να διατηρούνται βάσεις δεδομένων με πληροφορία σχετική με τις κρατήσεις στο επίπεδο του συνδέσμου και στο επίπεδο του μονοπατιού. Η πληροφορία για τη βάση δεδομένων στο επίπεδο του μονοπατιού (path level database) εξάγεται από την κατάσταση της βάσης δεδομένων στο επίπεδο του συνδέσμου (link QoS database). Αν και η κατάσταση της βάσης δεδομένων στο επίπεδο συνδέσμου διατηρείται μόνο από τον cBB, κάθε eBB διατηρεί ένα αμοιβαία διακριτό υποσύνολο της κατάστασης της βάσης δεδομένων σε επίπεδο μονοπατιού,

και μπορεί επομένως να χειριστεί το φόρτο του ελέγχου αποδοχής για τα σχετικά μονοπάτια. Οι συγγραφείς προτείνουν σε αυτό το σημείο έναν αριθμό από παραλλαγές για το χειρισμό των αιτημάτων ελέγχου αποδοχής, ανάλογα με το αν θα γίνουν αποδεκτά ή όχι.

Συγκρίνοντας τις κατανεμημένες αρχιτεκτονικές με το κεντρικοποιημένο μοντέλο, παρατηρούμε ότι ενώ οι κατανεμημένες αρχιτεκτονικές προσφέρουν πλεονεκτήματα κλιμάκωσης σε σχέση με το κεντρικοποιημένο μοντέλο, παρέχουν κατώτερη διαχείριση πόρων και εισάγουν σπατάλη εύρους ζώνης κατά μήκος των μονοπατιών. Επιπλέον, αν η βάση δεδομένων στο επίπεδο συνδέσμου χρειάζεται να προσπελαύνεται συχνά, η υπολογιστική επιβάρυνση μπορεί να αυξηθεί και να καταστεί αντιπαραγωγική.

Ένα άλλο σημαντικό σημείο σύγκρισης είναι ότι η ευρωστία της κάθε λύσης και η συμπεριφορά της σε απροσδόκητες ή μη επιθυμητές καταστάσεις. Οι αστοχίες σε ένα δικτυακό στοιχείο (κόμβο/μηχάνημα/διεργασία) μπορούν να κατηγοριοποιηθούν ως εξής:

- Το στοιχείο δεν λειτουργεί καθόλου.
- Το στοιχείο λειτουργεί λανθασμένα και στέλνει μη αναμενόμενα και άγνωστα μηνύματα στους κόμβους με τους οποίους επικοινωνεί.
- Το στοιχείο έχει καταληφθεί από κακόβουλη οντότητα (για παράδειγμα έναν ιό) και εμφανίζεται να στέλνει έγκυρα μηνύματα αλλά δεν υπακούει στην κατάλληλη συμπεριφορά και προσπαθεί να υποβαθμίσει, να φθείρει ή να σταματήσει εντελώς την κανονική λειτουργία της αρχιτεκτονικής.

Οι τελευταίες δύο κατηγορίες λέγονται και "Βυζαντινές (Byzantine) συμπεριφορές και μπορούν να συνοψιστούν ως καταστάσεις όπου το στοιχείο λειτουργεί με αυθαίρετο τρόπο, και όχι σύμφωνα με τον αλγόριθμο που θα έπρεπε να ακολουθήσει.

Σε αυτό το σημείο εμφανίζεται μία ακόμα εξισορρόπηση (trade-off) μεταξύ των κεντρικοποιημένων και των κατανεμημένων κατηγοριών αρχιτεκτονικών. Μία κατανεμημένη αρχιτεκτονική μπορεί να σχεδιαστεί με τέτοιο τρόπο ώστε να επιτυγχάνει καλύτερη ευρωστία και ανοχή για κάποιες μονάδες του Bandwidth Broker που έχουν αστοχήσει, ενώ μια κεντρικοποιημένη αρχιτεκτονική έχει ένα μόνο σημείο από το οποίο εξαρτάται η σωστή λειτουργία της (single point of failure). Από την άλλη μεριά είναι ευκολότερο να ασφαλιστεί και να προστατευθεί μία μόνο μονάδα Bandwidth Broker, απ' ότι είναι να φυλαχτεί και να εξετάζεται εξονυχιστικά η λειτουργία πολλαπλών μονάδων που αποτελούν μια κατανεμημένη αρχιτεκτονική Bandwidth Broker.

Επιπλέον, μία κατανεμημένη αρχιτεκτονική πρέπει επίσης να λάβει υπόψη της το θέμα της συνοχής μεταξύ των στοιχείων που αποτελούν τον Bandwidth Broker. Αυτό ισχύει ακόμα και σε κάποιες περιπτώσεις ενός απλού Bandwidth Broker, όπου προκειμένου να αυξηθεί η ευρωστία, εισάγονται επιπρόσθετες αναπληρωματικές (backup) μονάδες (όπως ένας Bandwidth Broker που αντιγράφει τη λειτουργία του βασικού).

Πρέπει ακόμα να ληφθεί υπόψη ότι τα σχετικά πλεονεκτήματα και μειονεκτήματα των αρχιτεκτονικών επηρεάζονται από το περιβάλλον όπου χρησιμοποιούνται. Εφόσον η πρώτη κατηγορία βλαβών (πλήρης παύση λειτουργίας του στοιχείου) ανακαλύπτονται συνήθως πολύ ευκολότερα και είναι πιο "επιθυμητές" σε σχέση με τα υπόλοιπα είδη βλαβών, εάν η αρχιτεκτονική του Bandwidth Broker υλοποιείται

και χρησιμοποιείται σε ένα περιβάλλον όπου τέτοιες βλάβες μπορούν να αποκλειστούν, οι σχετικές ανησυχίες δεν χρειάζεται φυσιολογικά να ληφθούν υπόψη.

ΚΕΦΑΛΑΙΟ 4: ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ QOS ΥΠΗΡΕΣΙΩΝ ΣΕ WAN

ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ QOS ΥΠΗΡΕΣΙΩΝ ΓΙΑ WAN ΔΙΚΤΥΟ

Η υπηρεσία QoS έχει ως σκοπό να δημιουργήσει, να συντηρήσει και να διαχειριστεί μηχανισμούς στον κορμό και στην περιφέρεια του δικτύου οι οποίοι θα μπορούν να εξασφαλίζουν εγγυήσεις στην απόδοση του δικτύου για συγκεκριμένες κλάσεις κίνησης. Χρήστες της υπηρεσίας θα είναι οι φορείς που διασυνδέονται στο δίκτυο. Οι εγγυήσεις ποιότητας που παρέχει η υπηρεσία έχουν να κάνουν κυρίως με την διασφάλιση ορισμένης χωρητικότητας πάνω στις συνδέσεις πρόσβασης και κορμού του δικτύου. Δευτερευόντως, πλέον της διασφάλισης ορισμένης χωρητικότητας, η υπηρεσία QoS προσπαθεί να εξασφαλίσει άνω όρια στις τιμές της καθυστέρησης μετάδοσης (delay) και στο jitter.

Η εξασφάλιση συγκεκριμένου εύρους ζώνης παρέχεται είτε μεταξύ δύο ορισμένων σημείων του δικτύου είτε μεταξύ ενός σημείου και του «δικτύου». Το εύρος ζώνης που διατίθεται για την παροχή υπηρεσιών ποιότητας υπηρεσίας θα είναι ποσοστό του συνολικού διαθέσιμου εύρους ζώνης στις συνδέσεις του δικτύου και σίγουρα δεν θα ξεπερνάει ένα άνω όριο το οποίο προκύπτει από την μελέτη διαστασιολόγησης του δικτύου.

Το δίκτυο στοχεύει να παρέχει τις ακόλουθες υπηρεσίες, υιοθετώντας της αρχιτεκτονική DiffServ:

- IP Premium. Η κίνηση που υπάγεται σε αυτήν την υπηρεσία εξυπηρετείται με προτεραιότητα έναντι όλων των άλλων ακολουθώντας της EF PHB της DiffServ αρχιτεκτονικής. Με άλλα λόγια, τα πακέτα της IPP υπηρεσίας διαδίδονται στο δίκτυο χωρίς συμφόρηση ανεξάρτητα από το φόρτο κίνησης που οφείλεται στις υπόλοιπες δυο κλάσεις υπηρεσίας QoS. Έτσι η καθυστέρηση διάδοσης και το ποσοστό αποτυχημένων μεταδόσεων των πακέτων αυτών μπορούν να διατηρηθούν σε χαμηλά επίπεδα για τα οποία μάλιστα παρέχεται και εγγύηση μη παραβίασης. Η υπηρεσία αυτή παρέχεται κατόπιν αιτήματος χρήσης και διακρίνεται σε 3 υποκλάσεις:
    1. IP Premium. Χρησιμοποιείται μεταξύ δύο άκρων του δικτύου και εξασφαλίζει πως ένα μέρος της κίνησης που θα ανταλλάσσεται μεταξύ των σημείων αυτών εξυπηρετείται κατά προτεραιότητα από το δίκτυο. Προφανώς ο ορισμός της κίνησης γίνεται με την χρήση μιας Access List (ACL) και με μαρκάρισμα της κίνησης από τον φορέα ή εναλλακτικά από το δίκτυο αν ο φορέας δεν έχει τέτοια δυνατότητα.
    2. IP Premium Transparent. Αυτή η κλάση κίνησης λειτουργεί με τον ίδιο τρόπο με την κλάση IP Premium με την διαφορά πως το δεύτερο άκρο θα είναι πάντα το interface διασύνδεσης του δικτύου με τον upstream provider. Η υπηρεσία αυτή, ενώ μέσα στο δίκτυο λαμβάνει εξυπηρέτηση άμεσης προώθησης (Priority) εντούτοις στο δίκτυο του upstream provider μεταχειρίζεται ως BestEffort.
    3. IP Premium VoIP. Η κλάση αυτή στοχεύει στην παροχή προτεραιότητας στην VoIP κίνηση σε όλο το δίκτυο. Τα αιτήματα χρήσης της υπηρεσίας αυτής ορίζουν μόνο 1 άκρο (τον φορέα που αιτείται) και ο προορισμός της μπορεί να είναι οποιοσδήποτε άλλος φορέας. Οι χρήσεις της κλάσης αυτής

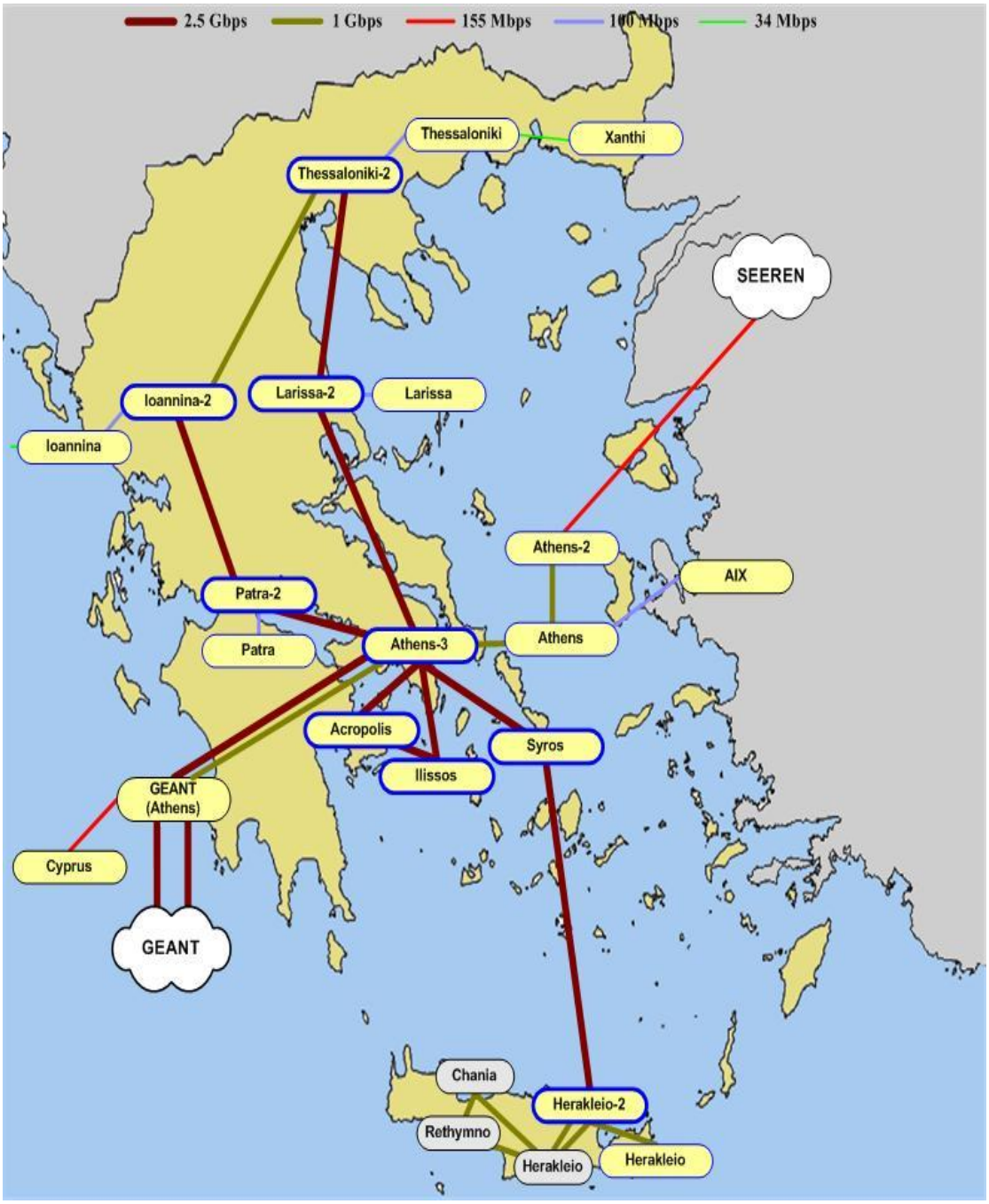
μπορεί να επεκταθούν και πέρα του VoIP, αλλά γενικά απαιτεί ειδικούς επιπλέον μηχανισμούς admission control ώστε να μην παραβιάζετε η διαστασιολόγηση.

- Managed Bandwidth Service. Η υπηρεσία αυτή στοχεύει ώστε να εξασφαλίζει εγγυήσεις σε εύρος ζώνης για νοητά κυκλώματα point-to-point μεταξύ αυθαίρετων σημείων του δικτύου. Η υπηρεσία αυτή παρέχεται κατόπιν αιτήματος χρήσης.
- Best Effort. Για την κίνηση που ανήκει σε αυτήν την κλάση υπηρεσίας δεν παρέχεται καμία εγγύηση όσον αφορά στο επίπεδο εξυπηρέτησης. Το δίκτυο δεν διαθέτει πόρους ή προτεραιότητα για την κίνηση αυτή και για αυτό η προώθησή της στο δίκτυο εξαρτάται από τη σταθερότητα της δρομολόγησης, το φόρτο κίνησης και τη διαθεσιμότητα του δικτύου. Επειδή ακριβώς δεν απαιτείται κάποια ιδιαίτερη μεταχείριση των πακέτων που ανήκουν στην BE κλάση υπηρεσίας, δεν χρειάζεται να ακολουθηθεί οποιαδήποτε διαδικασία κράτησης.
- Less Than Best Effort (LBE). Σε αυτήν την κλάση υπηρεσίας αντιστοιχίζεται η κίνηση χαμηλής προτεραιότητας η οποία αξιοποιεί το ποσό του εύρους ζώνης που μένει ελεύθερο από τις άλλες κλάσεις. Κατά βάση, η κίνηση αυτή είναι μεγάλου όγκου η οποία όμως δεν χρειάζεται να μεταδοθεί μέσα σε κάποιο συγκεκριμένο χρονικό πλαίσιο (ερευνητικού χαρακτήρα κτλ.) και για αυτό δεν επηρεάζει την κίνηση των IPP και BE, απλά κάνει χρήση των πόρων που αυτές αφήνουν ανεκμετάλλευτο. Σε περίπτωση συμφόρησης στο δίκτυο τα LBE πακέτα είναι τα πρώτα που απορρίπτονται.

Προκειμένου να είναι δυνατή η παροχή διασφαλίσεων στο ποσό του εύρους ζώνης, την καθυστέρηση και το jitter που λαμβάνουν συγκεκριμένες κλάσεις κίνησης στο δίκτυο έπρεπε να εφαρμοστούν συγκεκριμένες τεχνικές στους δρομολογητές του δικτύου. Η τεχνική υλοποίηση κινείται σε 3 άξονες:

1. Τον ορισμό του τρόπου χαρακτηρισμού της κίνησης (marking schema) και την περιφρούρηση του δικτύου.
2. Την διαστασιολόγηση του δικτύου για την παροχή της υπηρεσίας QoS, η οποία ορίζει τα άνω όρια του δεσμευμένου εύρους ζώνης στο δίκτυο.
3. Τις τεχνικές χειρισμού ουρών στους δρομολογητές προκειμένου να υλοποιηθεί η υπηρεσία.

Στο σημείο αυτό πρέπει να αναφέρουμε πως η μελέτη, ο σχεδιασμός και η υλοποίηση έχει εφαρμοστεί στο δίκτυο του ΕΔΕΤ [96] που είναι και το case study (Εικόνα 16).



Εικόνα 16: το δίκτυο κορμού του ΕΔΕΤ, case study της μελέτης

4.1 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΙΝΗΣΗΣ

Ο χαρακτηρισμός της κίνησης η οποία θα λαμβάνει ιδιαίτερη εξυπηρέτηση από το δίκτυο γίνεται με χρήση του DSCP πεδίου στην επικεφαλίδα του IP πακέτου. Αντίστοιχα μέσα σε ένα MPLS domain, ο διαχωρισμός της κίνησης γίνεται με χρήση του EXP πεδίου στην επικεφαλίδα του MPLS.

Βασικός στόχος της υλοποίησης μιας υπηρεσίας QoS σε ένα δίκτυο είναι οι κλάσεις όσο και το σχήμα μαρκαρίσματος να είναι πλήρως συμβατό με αυτό των γειτονικών μιας και τα δίκτυα λειτουργούν συνήθως σε ιεραρχίες (hierarchical federations). Για

το σκοπό αυτό χρησιμοποιούνται και οι προτάσεις – προτυποποιήσεις που είχαν προκύψει από το SEQUIN.

Ο χαρακτηρισμός γίνεται περιμετρικά στο δίκτυο (στα σημεία εισόδου της κίνησης), όπου με την ενεργοποίηση κατάλληλων μηχανισμών γίνεται και η περιφρούρηση του δικτύου από «παράνομη QoS κίνηση». Ο Πίνακας 3 παρουσιάζει τις τιμές στο πεδίο DSCP της IP επικεφαλίδας που χρησιμοποιούνται.

RFC 2474 DSCP bits						Δεκαδική τιμή	Περιγραφή
3 MS bits			3 LS Bits				
1	0	1	1	1	0	46	IP Premium (IPP)
1	0	1	0	0	0	40	IP Premium Transparent (IPPT)
0	0	0	0	0	0	0	Best Effort (BE)
0	0	1	0	0	0	8	Less than Best Effort (LBE)
0	0	0	1	1	0	6	Downgraded Premium-Discard Eligible (DP/DE), μεταχειριζόμενη ως best effort
1	0	1	1	1	1	47	IP Premium VoIP (IPPV) (source only aware)
Όλες οι υπόλοιπες τιμές							Best Effort (BE)

Πίνακας 3: Σχήμα μαρκαρίσματος με βάση το πεδίο DSCP

Σε κάθε interface εισόδου της κίνησης στο δίκτυο γίνονται οι ακόλουθες ενέργειες:

- Έλεγχος για IP Premium κίνηση σύμφωνα με τα υποβληθέντα αιτήματα χρήσης. Η κίνηση που ανήκει σε κάθε αίτημα περιγράφεται από ένα traffic class που δηλώνεται σε μορφή μιας extended ACL σε λογικό AND με το μαρκάρισμα ή όχι της κίνησης (με κατάλληλη τιμή στο DSCP). Τα πακέτα που περνούν το φίλτρο αυτό ελέγχονται (αστυνομεύονται) για το κατά πόσο σέβονται το συμφωνημένο προφίλ κίνησης. Η αστυνόμευση πραγματοποιείται με τη χρήση token bucket αλγορίθμου. Τα πακέτα που συμμορφώνονται μαρκάρονται με την κατάλληλη τιμή στο DSCP πεδίο, ενώ όσα πακέτα το παραβιάζουν ξαναμαρκάρονται ως DP/DE (για την περίπτωση της υποκλάσης IP Premium) και ως BE για τις άλλες 2 υποκλάσεις.
- Έλεγχος άλλης μαρκαρισμένης κίνησης με τιμές στο πεδίο DSCP που αντιστοιχούν σε κλάσεις της IP Premium και για την οποία δεν έχουν υποβληθεί αιτήματα χρήσης. Τέτοια κίνηση ξαναμαρκάρεται σε BE (DSCP 0).

Στο σημείο αυτό πρέπει να τονιστεί πως οι υπόλοιπες τιμές DSCP (πλην όσων αναφέρει ο Πίνακας 3) παραμένουν αναλλοίωτες και απλά τα πακέτα λαμβάνουν μεταχείριση ως BE. Η επιλογή αυτή αποσκοπεί ώστε αν ένας φορέας χρησιμοποιεί το συγκεκριμένο δίκτυο ως transit για να συνδέσει δικά του υποδίκτυα να μπορεί να έχει επιλογές μαρκαρίσματος για εσωτερικές ανάγκες.

Επιπλέον, δεδομένου ότι το δίκτυο είναι MPLS enabled (στο σύνολό του ή σε τμήμα του), στο σημείο εισόδου στο MPLS domain γίνεται αντιγραφή των 3 πιο σημαντικών bits του πεδίου DSCP στο πεδίο MPLS EXP. Από την αντιστοίχηση είναι προφανές ότι οι κλάσεις IPP, IPPT και IPPB του IP domain αντιστοιχίζονται στην κλάση IPP του MPLS domain, οι κλάσεις DP/DE και BE του IP domain αντιστοιχίζονται στην κλάση BE του MPLS domain και η κλάση LBE αντιστοιχίζεται στην κλάση LBE του MPLS domain. Στην αντίστροφη κατεύθυνση (κατά την έξοδο από το MPLS domain προς το IP domain) αποκαθίστανται οι τιμές DSCP των αρχικών πακέτων με την αφαίρεση (popping) των MPLS labels. Λόγω της λειτουργίας του penultimate hop popping (στην MPLS τεχνολογία), κάθε τελικός δρομολογητής του δικτύου θα χειρίζεται πακέτα με βάση το πεδίο DSCP.

4.2 ΔΙΑΣΤΑΣΙΟΛΟΓΗΣΗ ΔΙΚΤΥΟΥ

Γενικά το πρόβλημα της διαστασιολόγησης της IP κίνησης προτεραιότητας σε ένα δίκτυο είναι ένα πρόβλημα βελτιστοποίησης λαμβάνοντας υπόψη κόστη σε κάθε σύνδεσμο. Όταν στον υπολογισμό εντάσσονται και μετρικές όπως η καθυστέρηση και το jitter τότε το πρόβλημα καταλήγει σε NP-complete και η λύση του βασίζεται πλέον σε ευριστικές μεθόδους. Γενικά στην βιβλιογραφία υπάρχουν εργασίες ερευνητών που προσεγγίζουν το πρόβλημα αυτό [20][22][40]. Στην περίπτωση της μελέτης μας χρησιμοποιήθηκε η προσέγγιση που δεν θεωρεί ως προαπαιτούμενο την γνώση του πίνακα δρομολόγησης μεταξύ πηγής και προορισμού. Αντίθετα, υπολογίζει την δεσμευμένη χωρητικότητα (στην χειρότερη περίπτωση), άσχετα με την πολιτική δρομολόγησης. Το σημαντικότερο χαρακτηριστικό της προσέγγισης αυτής είναι πως με αστυνόμευση στα άκρα του δικτύου και καθολική υλοποίηση ουρών προτεραιότητας, η αποδοχή κλήσης βασίζεται πλέον σε υπολογισμούς των δεσμεύσεων στα interface πρόσβασης του δικτύου.

Επιπλέον, με δεδομένη την κατάταξη της κίνησης σε ουρές προτεραιότητας και σε ουρές κανονικής εξυπηρέτησης, η διαστασιολόγηση ανάγεται στον υπολογισμό της μέγιστης κίνησης προτεραιότητας a_l σε κάθε γραμμή l στο σύνολο L των γραμμών κορμού, $0 < a_l < 1$. Διατηρώντας την τιμή a_l κάτω από ένα συγκεκριμένο όριο (περίπου 25% της ταχύτητας της γραμμής), δημιουργούνται αντίστοιχα οι συνθήκες για εγγύηση ελάχιστης καθυστέρησης και jitter στην «Premium» κίνηση. Ο μόνος τρόπος περιορισμού της μετρικής a_l στις γραμμές κορμού είναι η καθολική χρήση μηχανισμών αυστηρής αστυνόμευσης στην περίμετρο του δικτύου για έλεγχο της Premium κίνησης που εισάγεται. Συνεπώς, η διαστασιολόγηση του δικτύου διαιρείται σε:

1. Καθορισμό μιας ποσότητας Premium εύρους ζώνης για κάθε access γραμμή στο δίκτυο
2. απεικόνιση της παραπάνω ποσότητας σε πολιτική αστυνόμευσης και εφαρμογή της σε κάθε access interface στην περίμετρο του δικτύου.

Ο Πίνακας 4 παρουσιάζει την κατάτμηση . Η κατάτμηση αυτή είναι λειτουργική για την παρούσα κατάσταση (εύρος ζώνης συνδέσεων δικτύου κορμού και πρόσβασης) του ΕΔΕΤ και χρησιμοποιήθηκε επίσης για την εξαγωγή συμπερασμάτων για την αποτελεσματικότητα / ορθότητα των αλγορίθμων που παρουσιάζονται. Αν μελλοντικά γίνει σημαντική αναβάθμιση του εύρους ζώνης των γραμμών πρόσβασης μεγάλου αριθμού φορέων του ΕΔΕΤ, ενδεχομένως να απαιτηθεί να αλλάξουν τα ποσοστά αυτά. Για παράδειγμα, αν η αύξηση αυτή του εύρους ζώνης των γραμμών

πρόσβασης δεν ακολουθηθεί από κατάλληλη αύξηση του εύρους ζώνης των γραμμών κορμού, θα απαιτηθεί μείωση των παρακάτω ποσοστών.

Ταχύτητα Πρόσβασης	**Ποσοστό Gold Κίνησης**
>= 30 Mbps	5%
10 Mbps - 30 Mbps	10%
2 Mbps – 10 Mbps (DSL φορείς)	15%
<= 2 Mbps	20%

Πίνακας 4: κατάτμηση γραμμών πρόσβασης με βάση τη διαστασιολόγηση

Βήμα 1: Υπολογισμός του μέγιστου ρυθμού της Premium κίνησης που διέρχεται από έναν δρομολογητή προς και από το ΕΔΕΤ, I και O

Είσοδος

Ταχύτητα των συνδέσμων πρόσβασης και του ποσοστού αυτών που έχει δεσμευθεί για Premium κίνηση.

S: σύνολο όλων των δρομολογητών

Έξοδος

I(s): μέγιστος ρυθμός της Premium κίνησης που διέρχεται από τον δρομολογητή s με κατεύθυνση από τον φορέα αφετηρίας προς το ΕΔΕΤ

O(d): μέγιστος ρυθμός της Premium κίνησης που διέρχεται από τον δρομολογητή d με κατεύθυνση από το ΕΔΕΤ προς τον φορέα προορισμού

Παρατηρήσεις

Τα I,O μπορεί να υπολογιστούν εύκολα από τις ταχύτητες πρόσβασης των φορέων και του ποσοστού που έχει δεσμευθεί για την Premium κίνηση. Αν σε έναν δρομολογητή s υπάρχουν εξυπηρετητές που είναι πηγές Premium κίνησης (π.χ. εξυπηρετητές video-on-demand) τότε αυτό μπορεί να οδηγήσει σε τιμή του I(s) μεγαλύτερη από O(s). Θα ισχύει I(s)=O(s) αν σε όλους τους συνδέσμους πρόσβασης του δρομολογητή s το ποσοστό της Premium κίνησης στις δύο κατευθύνσεις είναι το ίδιο.

Το σύνολο S μπορεί να περιλαμβάνει μόνο τους δρομολογητές του ΕΔΕΤ2, ή και τους δρομολογητές του ΕΔΕΤ1. Στην δεύτερη περίπτωση ο αλγόριθμος υπολογίζει και το εύρος ζώνης για την Premium κίνηση στους συνδέσμους μεταξύ δρομολογητών του ΕΔΕΤ1 και του ΕΔΕΤ2.

Βήμα 2: Υπολογισμός των BI και BO

Είσοδος

I(s): μέγιστος ρυθμός της Premium κίνησης που διέρχεται από τον δρομολογητή s με κατεύθυνση από τον φορέα αφετηρίας προς το ΕΔΕΤ

O(d): μέγιστος ρυθμός της Premium κίνησης που διέρχεται από τον δρομολογητή d με κατεύθυνση από το ΕΔΕΤ προς τον φορέα προορισμού

G: γράφος που περιγράφει την τοπολογία του δικτύου

L: σύνολο όλων των συνδέσμων

S: σύνολο όλων των δρομολογητών

Έξοδος

BI(I): Το άθροισμα των I(s) για τα οποία υπάρχει δρομολογητής προορισμού d για το οποίο ο σύνδεσμος I ανήκει στο R(s,d), που είναι το σύνολο των συνδέσμων που ανήκουν στο μονοπάτι από τον δρομολογητή s προς τον δρομολογητή d.

BO(I): Το άθροισμα των O(d) για τα οποία υπάρχει δρομολογητής προορισμού d για το οποίο ο σύνδεσμος I ανήκει στο R(s,d).

Αλγόριθμος

R=DIJSTRA_SHORTEST_PATH(G) % R(s,d): σύνολο συνδέσμων που ανήκουν στο μονοπάτι από τον δρομολογητή s προς τον δρομολογητή d.

```
For all l in L {
        BI(l)=0
        BO(l)=0
}
For all s in S {
        For all l in L {
                If d exists such that l in R(s,d) then
                        BI(l) += I(s)
        }
}
For all d in S {
        For all l in L {
                If s exists such that l in R(s,d) then
                        BO(l) += O(d)
        }
}
```

Βήμα 3: Υπολογισμός του B_bound(l), εύρος ζώνης στο σύνδεσμο l που απαιτείται για την Premium υπηρεσία.

Είσοδος

BI(I): Το άθροισμα των I(s) για τα οποία υπάρχει δρομολογητής προορισμού d για το οποίο ο σύνδεσμος I ανήκει στο R(s,d).

BO(I): Το άθροισμα των O(d) για τα οποία υπάρχει δρομολογητής προορισμού d για το οποίο ο σύνδεσμος I ανήκει στο R(s,d).

L: σύνολο όλων των συνδέσμων

Έξοδος

B_bound(l): εύρος ζώνης στο σύνδεσμο l που απαιτείται για την Premium υπηρεσία.

Αλγόριθμος

```
For all l in L {
        B_bound(l) = min{BI(l), BO(l)}
}
```

Στη συνέχεια θα περιγράψουμε την επέκταση του αλγορίθμου ώστε να λαμβάνονται υπόψη στον υπολογισμό των άνω φραγμάτων πιθανά link failures. Όταν έχουμε κάποιο link failure τότε οι δρομολογητές που εξυπηρετούνται από το συγκεκριμένο link θα πρέπει να δρομολογήσουν την κίνηση τους από κάπου αλλού. Όταν το link failure συμβαίνει στην άκρη του δικτύου σε σύνδεσμο που δεν ανήκει σε κάποιο βρόγχο τότε τα bandwidth reservations που υπολογίζονται βάσει του αλγορίθμου δεν θα αλλάξουν αφού η κίνηση που πέρναγε από το προβληματικό link δεν μπορεί να δρομολογηθεί από αλλού. Συνεπώς ο νέος αλγόριθμος αρκεί να λάβει υπόψη μόνο τα links που βρίσκονται σε βρόγχο.

Στον νέο αλγόριθμο χρησιμοποιείται επιπλέον η έννοια του βρόγχου (loop) v, που είναι το σύνολο των συνδέσμων που δημιουργούν τον βρόγχο. Ορίζουμε επίσης το σύνολο των βρόγχων που περιέχει το δίκτυο μας V={v}. Επίσης ορίζουμε το V*={l: l in V}. Έτσι, πρέπει να εντοπιστούν τα links τα οποία ανήκουν σε βρόγχο και να γίνουν και πάλι οι δεσμεύσεις πόρων θεωρώντας ότι έχουμε link failure σε καθένα από τα links.

Αλγόριθμος

```
B_bound_lf(l) = 0 for all l in L
While exist l in V* such that l not processed {
    For all v in V {
        If exists l in v such that l not processed {
            Mark l as ‘down’
            Mark l as processed
        }
    }

    Run algorithm output is B_bound(l)
    B_bound_lf(l)=max{B_bound_lf(l),B_bound(l)}
```

}

Στον παρακάτω πίνακα (Πίνακας 5) φαίνονται τα αποτελέσματα εφαρμογής του αλγορίθμου στο δίκτυο του ΕΔΕΤ. Στην πρώτη και δεύτερη στήλη σημειώνεται ο σύνδεσμος και στην τρίτη η δέσμευση πόρων (worse case with link failures). Τέλος, η τέταρτη στήλη παρουσιάζει το μέγιστο ποσοστό της χωρητικότητας κάθε γραμμή κορμού που μπορεί να δεσμευθεί για κίνηση IP Premium και MBS.

Γραμμή Κορμού		**Maximum Premium Traffic (Kbps)**	**Ποσοστό της χωρητικότητας (%)**
Άκρο Α	**Άκρο Β**		
athens-3.grnet.gr	acropolis.grnet.gr	660.397	26,42%
athens-3.grnet.gr	ilissos-1.grnet.gr	660.397	26,42%
athens-3.grnet.gr	patra-2.grnet.gr	873.101	34,92%
athens-3.grnet.gr	larissa-2.grnet.gr	873.101	34,92%
athens-3.grnet.gr	syros.grnet.gr	250.503	10,02%
athens-3.grnet.gr	athens-1.grnet.gr	18.348	1,83%
acropolis.grnet.gr	ilissos-1.grnet.gr	405.249	16,21%
thessaloniki.grnet.gr	thessaloniki-2.grnet.gr	5.999	0,60%
patra.grnet.gr	patra-2.grnet.gr	2.763	2,76%
heraklio.grnet.gr	heraklio-2.grnet.gr	307	0,03%
ioannina.grnet.gr	ioannina-2.grnet.gr	409	0,04%
larissa.grnet.gr	larissa-2.grnet.gr	2.409	2,41%
xanthi.grnet.gr	xanthi-2.grnet.gr	921	0,092%
thessaloniki-2.grnet.gr	ioannina-2.grnet.gr	569.929	56,99%
thessaloniki-2.grnet.gr	larissa-2.grnet.gr	720.692	28,83%
thessaloniki-2.grnet.gr	xanthi-2.grnet.gr	101.521	10,15%
patra-2.grnet.gr	ioannina-2.grnet.gr	670.338	26,81%
heraklio-2.grnet.gr	syros.grnet.gr	200.503	8,02%

Πίνακας 5: Αποτελέσματα αλγορίθμου διαστασιολόγησης

4.3 ΧΡΟΝΟΔΡΟΜΟΛΟΓΗΣΗ ΣΤΟ ΔΙΚΤΥΟ

Ο σχεδιασμός της υπηρεσίας ορίζει ότι το μαρκάρισμα των πακέτων θα γίνεται στα σημεία εισόδου (στην περίμετρο του δικτύου), από το ΕΔΕΤ ή από το συνδεδεμένο φορέα. Η κλάση κίνησης που περιγράφει ένα αίτημα χρήσης της υπηρεσίας αποτελείται από μια ACL, όπου δηλώνεται η πηγή και ο προορισμός καθώς και από μια δήλωση αν η κίνηση έρχεται μαρκαρισμένη ή όχι. Αυτή η επιλογή παρέχει μια

ευελιξία δήλωσης της κίνησης καθώς αυτή μπορεί να γίνει με IP διευθύνσεις, πρωτόκολλα, ports, τιμές DSCP μαρκαρίσματος ή διάφορους λογικούς συνδυασμούς των παραπάνω.

Ο μηχανισμός της αστυνόμευσης της κίνησης εφαρμόζεται ώστε να προστατεύεται το δίκτυο από πλεονάζουσα (παράνομη) κίνηση χαρακτηρισμένη ως premium. Με δεδομένο το σχήμα διαστασιολόγησης, αρκεί η αστυνόμευση της κίνησης να γίνει περιμετρικά και όχι στο κορμό του δικτύου. Επιπλέον, μας αρκεί η αστυνόμευση να γίνεται στην κατεύθυνση εισόδου προς το δίκτυο (και όχι στην εξερχόμενη κίνηση). Η κίνηση που παραβιάζει το συμφωνηθέν προφίλ μεταξύ ΕΔΕΤ και συνδεόμενου φορέα, απορρίπτεται ή μαρκάρεται ως best-effort, ανάλογα με την επιθυμία του κάθε φορέα, όπως αποτυπώνεται στο αίτημα χρήσης. Η αστυνόμευση γίνεται με χρήση του Token Bucket αλγορίθμου, ρυθμισμένου να αστυνομεύει την κίνηση σε ρυθμό CIR (Committed Information Rate), ίσο με τον ζητούμενο ρυθμό από το φορέα και με βάθος (depth) ίσο με 2 φορές το μέγιστο πλαίσιο μετάδοσης (MTU). Καθώς στις γραμμές πρόσβασης το MTU είναι 9000bytes, το depth ισούται με 18000bytes. Αυτή η επιλογή έχει δοκιμαστεί και για UDP κίνηση παρέχει ιδανική αστυνόμευση. Στην περίπτωση TCP κίνησης, το αποτέλεσμα είναι πολύ καλό αλλά αυτό εξαρτάται και από άλλους παράγοντες όπως το TCP window και ο βαθμός συνάθροισης (aggregation).

Για την υλοποίηση ουρών, ακολουθώντας τις οδηγίες του SEQUIN, επιλέξαμε να υλοποιήσουμε ένα μοντέλο όπου θα εφαρμόζεται πολιτική ουρών σε όλα τα interfaces εξόδου (πρόσβασης και κορμού) και δεν θα εφαρμόζεται στα interface εισόδου. Η υλοποίηση της πολιτικής έγινε με χρήση του μηχανισμού Modified Deficit Round-Robin (MDRR) [3][88][94] ή Class Based Weighted Fair Queuing (CBWFQ) [88], ανάλογα με την πλατφόρμα εξοπλισμού (η σειρά Cisco 12000 υποστηρίζει μόνο MDRR, ενώ η σειρά Cisco 7200 series μόνο CBWFQ).

Χρησιμοποιώντας της ουρά απόλυτης προτεραιότητας του MDRR (σε strict priority mode) ή του CBWFQ, η premium κίνηση απολαμβάνει απόλυτη προτεραιότητα σε όλο το δίκτυο. Μια δεύτερη ουρά με πολύ μικρό βάρος (δέσμευση 1%) έχει ενεργοποιηθεί για τις ανάγκες της LBE υπηρεσίας. Τέλος, για την Best Effort κίνηση γίνεται χρήση μιας κλασική ουράς FCFS (First Come First Served). Τέλος, να σημειωθεί πως στις γραμμές κορμού, η κατηγοριοποίηση της κίνησης σε κλάσεις και ουρές γίνεται βάσει του DSCP και του MPLS EXP, εξαιτίας του penultimate hop popping του MPLS [25][37][56][58].

4.4 ΥΛΟΠΟΙΗΣΗ MBS ΥΠΗΡΕΣΙΑΣ

Η υπηρεσία απευθύνεται σε φορείς που επιθυμούν συνδέσεις εγγυημένου εύρους ζώνης με άλλον φορέα και οι οποίες δεν θα είναι πολύ μικρής διάρκειας. Η υπηρεσία αυτή θα παρέχεται σε όλους τους φορείς του δικτύου του ΕΔΕΤ που το επιθυμούν σε επίπεδο 2 (Layer-2) και θα δημιουργούνται traffic engineering tunnels κατά μήκος του backbone δικτύου για κάθε αίτημα της υπηρεσίας. Η τεχνική υλοποίηση της υπηρεσίας θα γίνεται ως εξής:

- Δημιουργείται ένα traffic engineering tunnel μεταξύ των PE δρομολογητών, δηλαδή μεταξύ των ακραίων δρομολογητών του δικτύου του ΕΔΕΤ. Το tunnel αυτό δρομολογείται αρχικά βάσει της κανονικής δρομολόγησης που εφαρμόζεται στο δίκτυο του ΕΔΕΤ και όταν παρουσιαστούν προβλήματα συμφόρησης θα ρυθμίζεται ώστε να ακολουθεί εναλλακτικά μονοπάτια καθώς το δίκτυο του

ΕΔΕΤ2 διαθέτει εναλλακτικές διαδρομές. Η ρύθμιση θα γίνεται ώστε το tunnel να ακολουθεί την εναλλακτική διαδρομή από αυτή που ορίζουν τα βάρη δρομολόγησης και θα ρυθμίζεται το path με explicit τρόπο για το κάθε tunnel.

- Η δρομολόγηση μέσω του tunnel ορίζεται ώστε σε περίπτωση απώλειας αυτού να υπάρχει επαναδρομολόγηση της κίνησης.
- Η κίνηση που εισάγεται μέσα στο tunnel μαρκάρεται στον PE δρομολογητή (στο interface όπου συνδέεται ο φορέας) με την τιμή 5 στο Experimental πεδίο του MPLS. Η τιμή αυτή είναι όμοια με το μαρκάρισμα της IP Premium υπηρεσίας και η προώθηση στο δίκτυο του ΕΔΕΤ πραγματοποιείται δίνοντας στην κίνηση πολύ υψηλή προτεραιότητα με χρήση του MDRR μηχανισμού χρονοδρομολόγησης.
- Στους P δρομολογητές (που είναι όλοι οι εσωτερικοί στο μονοπάτι της MBS σύνδεσης) δεν απαιτείται κάποια διαμόρφωση, απλά να είναι MPLS enabled και επίσης να έχουν διαμορφωμένο τον MDRR μηχανισμό και τις ουρές του, όπως ορίζεται από την QoS υπηρεσία και περιγράφεται και παρακάτω στο κείμενο.
- Στην πλευρά του πελάτη που επιθυμεί την χρήση της υπηρεσίας, πρέπει αυτός να συνδέεται στους δρομολογητές του ΕΔΕΤ2 με τεχνολογία Ethernet. Ειδικότερα ο πελάτης δημιουργεί ένα VLAN για την κίνηση που επιθυμεί να δρομολογείται μέσω της κάθε MBS σύνδεσης (dot1q encapsulation). Ο ακραίος δρομολογητής του ΕΔΕΤ που συνδέεται το sub-interface (VLAN) κάνει αστυνόμευση της κίνησης σε όλη την εισερχόμενη κίνηση με ρυθμό ίσο με το εύρος ζώνης που ο φορέας έχει ζητήσει και έχει γίνει αποδεκτό. Στη συνέχεια, τα πακέτα που συμμορφώνονται στο προφίλ αυτό κίνησης μαρκάρονται με τιμή 5 (EXP field). Όλη η κίνηση μεταξύ των 2 ακραίων VLANs δρομολογείται μέσω του tunnel που έχει κατασκευαστεί μεταξύ των PE δρομολογητών. Αντίθετα, τα πακέτα που παραβιάζουν το παραπάνω προφίλ αστυνόμευσης θα απορρίπτονται. Στο σημείο αυτό είναι σημαντικό να τονιστεί πως η αστυνόμευση τόσο για την υπηρεσία QoS όσο και για την υπηρεσία MBS θα εφαρμόζεται ανεξάρτητα σε κάθε αίτημα, όπου αυτό είναι τεχνικά εφικτό, και όχι συγκεντρωτικά στα αιτήματα κάθε φορέα καθώς στην τελευταία περίπτωση θα δημιουργούνταν προβλήματα δικαιοσύνης. Το μαρκάρισμα των MPLS πλέον frames γίνεται στο 1ο label και μόλις εισαχθεί η κίνηση στο TE tunnel τότε το μαρκάρισμα μεταφέρεται σε όλα τα MPLS labels. Με αυτό τον τρόπο, το τελευταίο MPLS label που χρησιμοποιείται για την προώθηση της κίνησης είναι μαρκαρισμένο και συνεπώς σε κάθε δρομολογητή του ΕΔΕΤ εισάγεται στην ουρά υψηλής προτεραιότητας. Στο άλλο άκρο της σύνδεσης θα δημιουργείται ένα νέο VLAN προς τον φορέα προορισμού με αντίστοιχες ρυθμίσεις. Στο σημείο αυτό να σημειωθεί πως η υπηρεσία MBS εγγυάται εύρος ζώνης, σε συγκεκριμένη κίνηση (που έχει γίνει αποδεκτή), κατά μήκος των γραμμών κορμού του ΕΔΕΤ. Επίσης, στις γραμμές πρόσβασης των φορέων στο δίκτυο του ΕΔΕΤ εγγυάται εύρος ζώνης μόνο στην κατεύθυνση από το ΕΔΕΤ προς το φορέα.. Αντίθετα, στην κατεύθυνση από το φορέα προς τον δρομολογητή του ΕΔΕΤ που αυτός συνδέεται, είναι στην ευθύνη του φορέα να ενεργοποιήσει όποιους κατάλληλους μηχανισμούς διαθέτει ανάλογα με τον εξοπλισμό του. Συνολικά η περίπτωση αυτή αφορά φορείς που έχουν συνδεθεί στο δίκτυο του ΕΔΕΤ2 με τεχνολογία Gigabit Ethernet. Επίσης, πρέπει να αναφερθεί πως η σύνδεση των VLANs και η δρομολόγηση της κίνησης μέσω του TE tunnel γίνεται χρησιμοποιώντας την τεχνολογία AToM, όπου συνδέονται τα 2 ακραία VLAN (με το ίδιο VC) και η κίνηση δρομολογείται με τα χαρακτηριστικά ενός pseudowire class. Το pseudowire class ακολουθεί τα χαρακτηριστικά του

Traffic engineering tunnel. Η χρήση της τεχνολογίας AToM προφανώς εισάγει τους περιορισμούς που έχει και στην υπηρεσία MBS. Ειδικότερα, η τεχνολογία AToM και συνεπώς η υπηρεσία MBS δεν διατίθεται για σύνδεση φορέων που συνδέονται στον ίδιο PE δρομολογητή του ΕΔΕΤ. Το τελευταίο αντιμετωπίζεται με χρήση της τεχνικής local switching.

Στην περίπτωση της MBS υπηρεσίας υπάρχει αστυνόμευση της κίνησης στα άκρα (στους ακραίους δρομολογητές του ΕΔΕΤ, που είναι οι PE στην τοπολογία που περιγράφηκε παραπάνω). Η αστυνόμευση γίνεται σε επίπεδο VLAN στο interface όπου συνδέεται ο φορέας και για την κίνηση που κατευθύνεται προς το δίκτυο του ΕΔΕΤ. Η διαδικασία της αστυνόμευσης συνοδεύεται από αντίστοιχο μαρκάρισμα της κίνησης ώστε στο δίκτυο κορμού του ΕΔΕΤ να δέχεται προνομιακή μεταχείριση από τον MDRR μηχανισμό που έχει διαμορφωθεί σε όλους τους δρομολογητές κορμού σύμφωνα με την QoS υπηρεσία.

4.5 ΔΥΝΑΜΙΚΗ ΣΗΜΑΤΟΔΟΣΙΑ ΣΕ CONTROL PLANE ΓΙΑ ΠΑΡΟΧΗ QoS ΣΕ RTS ΚΙΝΗΣΗ

Η υπηρεσία RTS παρέχει point-to-point και multipoint βιντεοσυνδιαλέξεις (βασισμένες στο H323 πρωτόκολλο) μεταξύ των συνδεδεμένων ινστιτούτων του ΕΔΕΤ. Αρχικά, η κίνηση του videoconference ταξινομούταν σαν best effort κίνηση. Όταν ένα συνδεδεμένο ινστιτούτο θέλει να έχει μια υπηρεσία βιντεοσυνδιάλεξης με συγκεκριμένες εγγυήσεις QoS, το ινστιτούτο πρέπει να κάνει μια αίτηση στο εργαλείο ANS provisioning και οι διαχειριστές του ΕΔΕΤ πρέπει να ρυθμίσουν χειροκίνητα τους ακραίους δρομολογητές του ΕΔΕΤ ώστε να παρέχουν εγγυήσεις QoS στην υπηρεσία videoconference. Εναλλακτικά, ένα ινστιτούτο μπορεί να κάνει μια μόνιμη αίτηση για συνόδους βιντεοσυνδιαλέξεων, δεσμεύοντας μόνιμα κάποιους πόρους(βλέπε Σχήμα 1). Σε αυτή την αίτηση το συνδεδεμένο ινστιτούτο πρέπει να δηλώσει τις διευθύνσεις IP των σταθμών που συμμετέχουν στις συνόδους RTS και τις παραμέτρους Ποιότητας Υπηρεσίας που χρειάζονται (εύρος ζώνης, περίοδος χρόνου). Σε περίπτωση που οι διευθύνσεις IP αλλάξουν, ενημερωμένες αιτήσεις πρέπει να υποβληθούν.

Για να ξεπεραστούν οι παραπάνω περιορισμοί αποφασίσαμε να χρησιμοποιήσουμε QPPB (QoS Policy Propagation via BGP) [94] για τη διάδοση των παραμέτρων QoS πάνω από πρωτόκολλο δρομολόγησης BGP. Η βασική διαφορά με την κανονική διαδικασία είναι το γεγονός ότι το δίκτυο μπορεί αυτόνομα να βρει τους σταθμούς που συμμετέχουν στη σύνοδο RTS και μπορεί να λάβει εγγυήσεις QoS και να διαδώσει αυτές τις πληροφορίες σε όλους τους δρομολογητές. Η έρευνα των συμμετεχόντων στο videoconference γίνεται με μια καινούρια μονάδα λογισμικού που επικοινωνεί με την MCU και αποθηκεύει τις διευθύνσεις IP των συνδεδεμένων σταθμών σε μια βάση. Το λογισμικό αυτό αποθηκεύει στη βάση μόνο τις διευθύνσεις IP των σταθμών που έχουν την κατάλληλη δικαιοδοσία για να λάβουν εγγυήσεις QoS.

Στη συνέχεια, χρησιμοποιείται μια τροποποιημένη έκδοση του software router Quagga [106] που έχει eBGP(external BGP) peers με όλους τους δρομολογητές του δικτύου. Η τροποποιημένη έκδοση του Quagga διαβάζει τις διευθύνσεις IP που είναι αποθηκευμένες στη βάση δεδομένων και τις διαφημίζει μέσω BGP σε όλους τους δρομολογητές του δικτύου του ΕΔΕΤ στην κατάλληλη κοινότητα BGP που υποδεικνύει τις IP διευθύνσεις που πρέπει να λάβουν εγγυήσεις Ποιότητας Υπηρεσίας.

Το «κλειδί» σε αυτή την περίπτωση είναι ότι ο software router διαφημίζει ένα σύνολο από IP διευθύνσεις που ανήκουν σε άλλα Αυτόνομα Συστήματα. Αυτή η επιλογή έγινε έτσι ώστε να ελαχιστοποιηθεί η συνολική διαχειριστική προσπάθεια και με σκοπό να υπάρχει πλήρως αυτοματοποιημένη υπηρεσία. Έτσι, το Quagga χρειάζεται μια πρόσθετη μονάδα (την μονάδα εύρεσης μονοπατιού) που είναι ικανή να αναγνωρίσει και να θέσει το σωστό next hop για κάθε διεύθυνση IP που είναι συνδεδεμένη με την υπηρεσία RTS. Το next hop σε αυτή την περίπτωση πρέπει να είναι η κατάλληλη διασύνδεση εξόδου από το backbone δίκτυο του ΕΔΕΤ προς το ίδρυμα στο οποίο ανήκει η διεύθυνση IP. Γενικά, αυτή η μονάδα είναι σχετικά απαιτητική αφού πρέπει να λάβει υπόψη της διάφορες παραμέτρους όπως multihoming, multisiting κ.α. Στην περίπτωσή μας, αυτή η μονάδα επωφελείται από την υλοποίηση του MPLS στο δίκτυο και λειτουργεί σε 2 βήματα. Αρχικά, βρίσκει μέσω MPLS labeling pool, το άκρο του δρομολογητή του ΕΔΕΤ στο οποίο είναι συνδεδεμένο το ίδρυμα. Στη συνέχεια, στέλνει ερώτημα στο δρομολογητή (για το next hop για την IP διεύθυνση) και απαντά με την πραγματική διασύνδεση εξόδου από το δίκτυο του ΕΔΕΤ. Υπό αυτήν την έννοια, οι διευθύνσεις IP που συμμετέχουν σε μια σύνοδο βιντεοσυνδιάλεξης διαφημίζονται ξεχωριστά (μέσω μιας ιδιωτικής κοινότητας BGP) σε ένα δίκτυο μέσα από το τροποποιημένο Quagga που λειτουργεί σαν "route injector". Στη συνέχεια, χρησιμοποιώντας την τεχνική QPPB μπορούμε να αναθέσουμε σε αυτή την κοινότητα ειδικές ιδιότητες για τα χαρακτηριστικά QoS.

Λεπτομερώς, η υλοποίηση δουλεύει ως εξής:

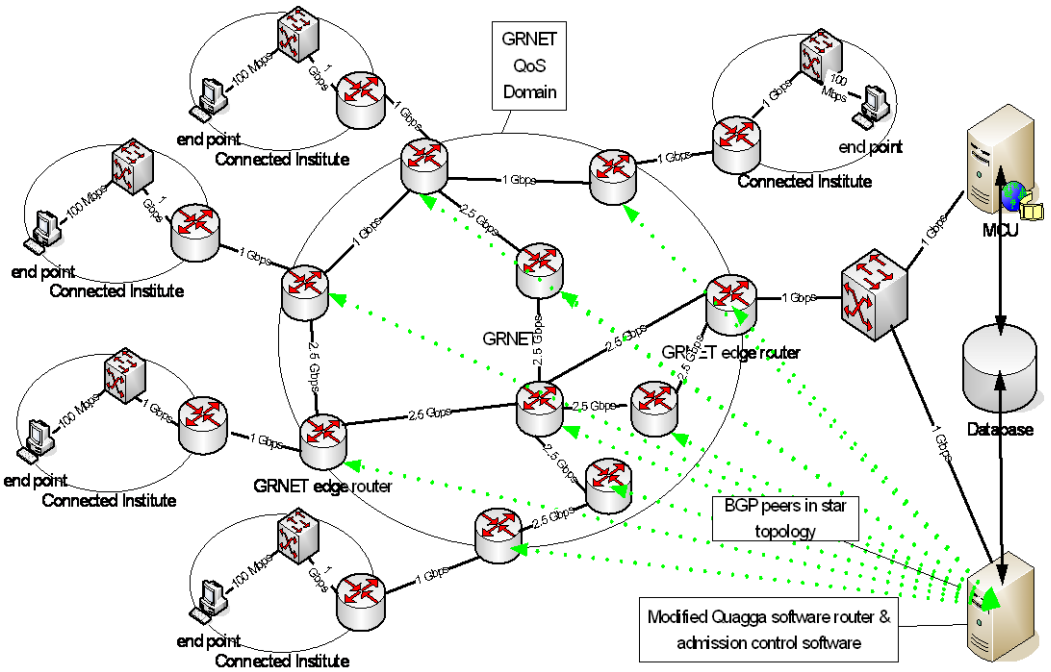
- Ο υλοποιημένος έλεγχος εισόδου σε λογισμικό παρακολουθεί την MCU και περιοδικά ανανεώνει (προσθέτει ή αφαιρεί) την βάση με τις διευθύνσεις IP των συνδεδεμένων σταθμών που έχουν την κατάλληλη δικαιοδοσία να λάβουν εγγυήσεις QoS.
- Το τροποποιημένο λογισμικό Quagga παρακολουθεί την βάση περιοδικά για πρόσθεση ή αφαίρεση των IP διευθύνσεων. Στην περίπτωση που μια νέα IP διεύθυνση έχει προστεθεί στη βάση δεδομένων, το Quagga καθορίζει το κατάλληλο next hop χρησιμοποιώντας τη μονάδα pathfinding και διαφημίζει αυτή την IP διεύθυνση στην κατάλληλη ιδιωτική BGP κοινότητα σε όλους τους BGP peers. Στην περίπτωση που μια IP διεύθυνση έχει αφαιρεθεί από την βάση, ο δρομολογητής quagga σταματά να διαφημίζει αυτή την IP διεύθυνση σε όλους τους BGP peers.
- Ο ακραίος δρομολογητής του ΕΔΕΤ μαρκάρει την κίνηση βασισμένος στην προκαθορισμένη κοινότητα BGP έτσι ώστε να παρέχει εγγυήσεις QoS στην κίνηση από τα συνδεδεμένα ιδρύματα προς την MCU. Η όλη λειτουργία γίνεται σε 2 βήματα. Αρχικά, μέσω QPPB signaling (βασισμένο στην πηγή), ο δρομολογητής φτιάχνει τοπικής εμβέλειας (στο δρομολογητή μόνο) μαρκάρισμα, χρησιμοποιώντας το χαρακτηριστικό qos-group [94]. Στη συνέχεια όλα τα μαρκαρισμένα πακέτα σε κάθε εισερχόμενη διασύνδεση (από ένα ίδρυμα που κατευθύνονται προς το σύστημα MCU) κατηγοριοποιούνται και ακολουθούν μια συγκεκριμένη πολιτική σε ξεχωριστή κλάση. Αυτή η κλάση έχει δημιουργηθεί για κίνηση RTS μόνο και το προφίλ πολιτικής που εφαρμόζεται, έχει αποφασιστεί με το συνδεδεμένο ίδρυμα (συνήθως, το συνδεδεμένο ίδρυμα ζητά ένα συγκεκριμένο προφίλ που είναι επίσης συμβατό με τη διαστασιολόγηση QoS του ΕΔΕΤ). Όλα τα κατάλληλα πακέτα μαρκάρονται σαν κίνηση IP Premium (με DSCP 46) και στέλνονται στο δίκτυο. Τα πλεονάζοντα πακέτα απορρίπτονται. Η λειτουργία 2 βημάτων είναι απαραίτητη εξαιτίας του γεγονότος ότι το QPPB signaling είναι

ενήμερο μόνο για την πηγή ή μόνο για τον προορισμό και στην περίπτωσή μας χρειαζόμαστε να είναι ενήμερο και για την πηγή και για τον προορισμό.

- Ο ακραίος δρομολογητής του ΕΔΕΤ που είναι συνδεδεμένος με την MCU δουλεύει προς την αντίθετη κατεύθυνση και μαρκάρει την κίνηση βασιζόμενος στην προκαθορισμένη BGP κοινότητα έτσι ώστε να παρέχει εγγυήσεις QoS στην κίνηση από την MCU στα συνδεδεμένα ιδρύματα. Το μαρκάρισμα γίνεται μέσω QPPB signaling σε destination based mode.

Στον πυρήνα του δικτύου του ΕΔΕΤ, δεν υπάρχει ανάγκη για καμία αλλαγή αφού το πλαίσιο QoS έχει αρχικά υλοποιηθεί (υπάρχουν ενεργοποιημένες ουρές σε όλες τις διασυνδέσεις εισόδου). Επιπρόσθετα, η πολιτική και το μαρκάρισμα των άκρων (η ξεχωριστή RTS κλάση για κάθε διασύνδεση) έχει υλοποιηθεί μια φορά και δεν υπάρχει ανάγκη για αλλαγές, εκτός και αν ένα ίδρυμα ζητήσει να αλλάξει το προφίλ κίνησής του (το εύρος ζώνης που θέλει να χρησιμοποιήσει για υπηρεσίες videoconference).

Συνεπώς, η ενοποίηση όλων των μονάδων και της σωστής αρχικής ρύθμισης QoS του δικτύου παρέχουν ένα πλήρως δυναμικό πλαίσιο που αναγνωρίζει τους συνδεδεμένους σταθμούς στις υπηρεσίες RTS και χρησιμοποιώντας ρυθμίσεις QPPB και QoS, παρέχει τις κατάλληλες εγγυήσεις QoS σε όλο το δίκτυο.



Εικόνα 17: Δυναμική Σηματοδοσία σε Control Plane

Ένα πολύ κρίσιμο σημείο που παρουσιάστηκε στην υλοποίηση είναι το γεγονός πως το BGP peering που γίνεται έχει σαν αποτέλεσμα ο προορισμός να ανακοινώνει IP διευθύνσεις άλλων φορέων. Συνεπώς, σε κάθε τέτοιο /32 route που διαφημίζει το zebra, θα πρέπει ως next-hop να εμφανίζεται το πραγματικό next-hop (δηλαδή η IP διεύθυνση του interface εισόδου της κίνησης στο δίκτυο). Για το λόγο αυτό πρέπει να υλοποιηθεί ένα module που να υλοποιεί λειτουργικότητα pathfinding και με παράμετρο ένα /32 route να βρίσκει το πραγματικό interface εισόδου της κίνησης στο δίκτυο. Το τελευταίο είναι πολύ σημαντικό να υλοποιείται σε real-time καθώς σε

διαφορετική περίπτωση θα υπάρχει πρόβλημα με τις περιπτώσεις multi-homing & multi-siting.

Για να αξιολογήσουμε την προσέγγιση, υλοποιήσαμε τα παραπάνω στο δίκτυο κορμού του ΕΔΕΤ. Συγκεκριμένα, ο τροποποιημένος δρομολογητής quagga απέκτησε BGP peers όλους τους δρομολογητές του δικτύου (9 δρομολογητές) και έγιναν οι κατάλληλες ρυθμίσεις QoS στην περίμετρο του δικτύου.

Class-map: cm_rts_qos (match-all) (10645969/7)

391873 packets, 253275711 bytes

Match: qos-group 1 (13756610)

Match: access-group 199 (15174802)

police: 1024000 bps, 9000 limit, 9000 extended limit conformed **391873** packets, 253275711 bytes actions: set-dscp-transmit ef, exceeded 0 packets, 0 bytes; actions: set-dscp-transmit default

Εικόνα 18: CLI στατιστικά στην κατεύθυνση 'χρήστης προς MCU'

Επίσης, το λογισμικό ελέγχου εισόδου ενεργοποιήθηκε και η υλοποίηση χρησιμοποιήθηκε πειραματικά σε διάφορες βιντεοσυνδιαλέξεις (με διάρκεια 2 ωρών). Κατά τη διάρκεια αυτών των τεστ, η σταθερότητα και οι κατάλληλες ρυθμίσεις μετρήθηκαν χρησιμοποιώντας μετρητές του CLI (Εικόνα 18 & Εικόνα 19) και παρακολούθηση του BGP. Η ιδέα του αυτόματου QoS έδωσε άρτιο αποτέλεσμα, αφού η πολιτική QoS διαδόθηκε σε όλα τα στοιχεία του δικτύου και η κίνηση videoconference ταξινομήθηκε σαν IP Premium. Το επόμενο σετ δοκιμών είχε ως σκοπό να μετρήσει την απόδοση QoS στο δίκτυο για κίνηση videoconference χρησιμοποιώντας αυτή την προσέγγιση. Επίσης έγινε μια σύγκριση με την κλασική προσέγγιση best effort.

Class-map: ip_premium_out (match-any) (3447969/1)

659862 packets, 323954552 bytes

Match: ip dscp 46 (1941986)

Match: ip dscp 47 (1941730)

Match: ip dscp 40 (1939426)

Match: mpls experimental 5 (392754)

Priority

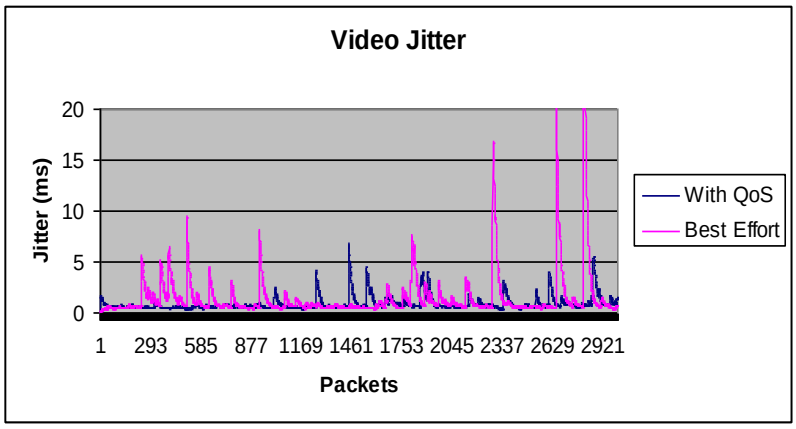
police: cir 20%, burst 250 ms, extended burst 250 ms 200000000 bps, 6250000 limit, 6250000 extended limit conformed **659862** packets, 323954552 bytes; actions: transmit, exceeded 0 packets, 0 bytes; actions: drop conformed 0 bps, exceed 0 bps

Εικόνα 19: CLI στατιστικά στην κατεύθυνση 'MCU προς χρήστη'

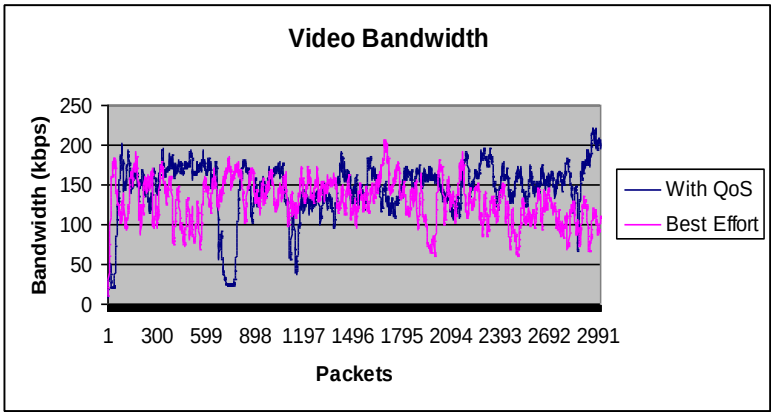
Επομένως, μια βιντεοσυνδιάλεξη εγκαταστάθηκε ανάμεσα σε διάφορα μέρη του δικτύου χρησιμοποιώντας την κεντρική MCU. Σε αυτή την περίπτωση, μετρήσαμε και λάβαμε την απόδοση σε ένα ακραίο σημείο. Κατά τη διάρκεια της βιντεοσυνδιάλεξης μετράμε τις ακόλουθες παραμέτρους που είναι σημαντικές για τις συνόδους videoconference:

- Bandwidth/Throughput: Κατά τη διάρκεια του πειράματος, μετράμε το φόρτο video και ήχου (χωρίς την καθυστέρηση των επικεφαλίδων) των χρησιμοποιούμενων ροών RTP. Εξαιτίας του γεγονότος ότι ο ήχος και το βίντεο μεταδίδονται σε διαφορετικές RTP ροές κάνουμε διαφορετικές μετρήσεις για τα δεδομένα ήχου και βίντεο.
- Packet loss: Κατά τη διάρκεια του πειράματος, μετράμε τα πακέτα που χάνονται στις ροές RTP ήχου και εικόνας. Το packet loss είναι μια σημαντική παράμετρος QoS για σύνοδο videoconference και ακόμα και μια μικρή παράμετρος packet loss μπορεί να επηρεάσει σημαντικά την ποιότητα videoconference.
- Delta: Κατά τη διάρκεια του πειράματος, μετρήσαμε την παράμετρο delta στις RTP ροές και ήχου και εικόνας. Η παράμετρος delta είναι η διαφορά καθυστέρησης μονής κατεύθυνσης 2 διαδοχικών πακέτων μεταδιδόμενων σε μια RTP ροή και χρησιμοποιείται στον υπολογισμό διακύμανσης καθυστέρησης(jitter). Η παράμετρος δέλτα είναι μια υπόδειξη της διακύμανσης στην καθυστέρηση κατά τη διάρκεια της μετάδοσης πολυμεσικών δεδομένων.
- Jitter(διακύμανση καθυστέρησης): Κατά τη διάρκεια του πειράματος, μετράμε τη διακύμανση καθυστέρησης στις RTP ροές ήχου και βίντεο. Το jitter είναι σημαντική παράμετρος QoS για συνόδους videoconference και επηρεάζει (μεταξύ άλλων χαρακτηριστικών) και τη διαδραστικότητα μια συνόδου βιντεοσυνδιάλεξης.

Μετράμε τις παραπάνω παραμέτρους και στην κατεύθυνση από end point προς MCU και στην αντίστροφη (MCU προς end point). Τα επόμενα σχήματα δείχνουν διαγράμματα που συγκρίνουν μια σύνοδο videoconference best effort και μια σύνοδο videoconference με ενεργοποιημένη Ποιότητα Υπηρεσίας. Παρουσιάζουμε το jitter, delta και τα διαγράμματα throughput κατά τη διάρκεια μετάδοσης video από ένα συμμετέχοντα προς την MCU. Παρουσιάζουμε επίσης ένα διάγραμμα όσον αφορά την διακύμανση καθυστέρησης του ήχου από την MCU σε 1 συμμετέχοντα). Τα άλλα διαγράμματα (video από MCU και ήχος από/προς MCU) δείχνουν τα ίδια αποτελέσματα.

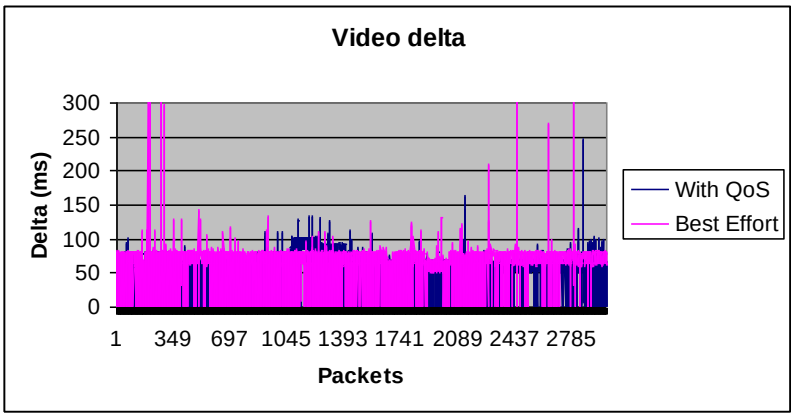


Εικόνα 20: Video Jitter

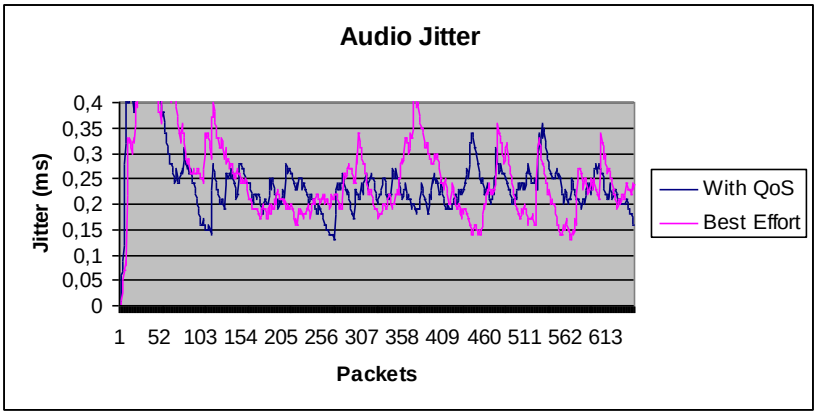


Εικόνα 21: Video Bandwidth

Όπως μπορεί να δει κάποιος στα επόμενα διαγράμματα (Εικόνα 20, Εικόνα 21 και Εικόνα 22 όσον αφορά τη μετάδοση video) υπάρχει σημαντική μείωση της διακύμανσης καθυστέρησης κατά τη διάρκεια videoconference με ενεργοποιημένο QoS σε σύγκριση με το best effort videoconference. Αυτή η υπόθεση αντικατοπτρίζει επίσης και τη μέση τιμή του jitter (QoS-enabled videconference 0,87 ms και best effort videoconference 1,51 ms) και τη μέγιστη τιμή jitter (QoS-enabled videoconference: 6,91ms και best effort videoconference: 38,55ms).
Όσον αφορά την παράμετρο δέλτα, οι σύνοδοι videoconference που είναι QoS-enabled με τις best effort έχουν παρόμοια απόδοση με τις QoS-enabled να έχουν λιγότερα peaks όπως μπορεί να δει κανείς στην Εικόνα 22. Αυτό φαίνεται επίσης και στη μέση τιμή (QoS-enabled videoconference: 33,96ms και best effort videoconference: 34,78ms) της παραμέτρου δέλτα.
Ομοίως το μέσο throughput είναι καλύτερο για QoS-enabled videoconference (QoS-enabled videoconference: 145kbps και best effort videoconference : 130 kbps). Επιπλέον, και τα QoS-enabled και τα best effort videoconference δεν έχασαν κανένα πακέτο κατά τη διάρκεια των πειραμάτων.



Εικόνα 22: Video Delta



Εικόνα 23: Audio Jitter

Όπως μπορεί κανείς να δει στην Εικόνα 23 (jitter ήχου από MCU προς συμμετέχοντα), τα QoS-enabled videoconferences έχουν παρόμοια απόδοση με τα best effort με τα QoS-enabled να έχουν λιγότερες αυξομειώσεις.
Συνεπώς, υπάρχει βελτιωμένη απόδοση για τις συνόδους videoconference με τον αυτοματοποιημένο μηχανισμό QoS όπως αυτός υλοποιήθηκε. Συγκεκριμένα το βελτιωμένο jitter κατά τη διάρκεια των QoS-enabled videoconference είναι σημαντικό εξαιτίας του γεγονότος ότι η διακύμανση καθυστέρησης επηρεάζει σημαντικά την ποιότητα του videoconference. Όσον αφορά το throughput η βελτίωση είναι σχετικά μικρή αλλά αυτό εξηγείται εξαιτίας του γεγονότος ότι το δίκτυο κορμού και το δίκτυο πρόσβασης (στο περιβάλλον που έγινε το τεστ) είναι υψηλής ταχύτητας και χωρίς συμφόρηση (στη χειρότερη περίπτωση οι δικτυακοί πόροι χρησιμοποιούνται κατά 50%). Έτσι, δεν περιμέναμε διαφορές στο packet loss. Τελικά, αναμέναμε και μετρήσαμε καλύτερα αποτελέσματα στο jitter επειδή η κίνηση videoconference εξυπηρετείται από ουρές υψηλής προτεραιότητας.

ΚΕΦΑΛΑΙΟ 5: ΥΛΟΠΟΙΗΣΗ BANDWIDTH BROKER ΔΙΑΧΕΙΡΙΣΗΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ QoS

ΥΛΟΠΟΙΗΣΗ BANDWIDTH BROKER ΔΙΑΧΕΙΡΙΣΗΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ QoS

5.1 ΥΛΟΠΟΙΗΣΗ BANDWIDTH BROKER ΔΙΑΧΕΙΡΙΣΗΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Το πιο σημαντικό στοιχείο για την λειτουργία ενός QoS framework είναι η διαχείριση του που πρέπει να είναι όσο πιο αυτοματοποιημένη γίνεται. Για το σκοπό αυτό, υλοποιήσαμε ένα διαχειριστικό εργαλείο (που ονομάζεται ANStool) με έναν αριθμό από δυνατότητες. Τα βασικά χαρακτηριστικά του είναι πως είναι αρθρωτό, βασίζεται σε standards (XML, Web Services) και δεν είναι συσχετισμένο με τεχνολογία και κατασκευαστή. Συνεπώς, μπορεί να υιοθετηθεί και από άλλα domains πλην του Ελληνικού ΕΔΕΤ.

Το διαχειριστικό εργαλείο διαθέτει 3 επίπεδα πρόσβασης:

1. Το επίπεδο χρήστη όπου μπορεί κάθε φορέας να κάνει αιτήματα χρήσης των υπηρεσιών, με άκρο το δικό του φορέα

2. Το επίπεδο των διαχειριστών του δικτύου, που βλέπουν όλα τα υποβληθέντα αιτήματα και το απαραίτητο configuration που πρέπει να υλοποιηθεί για το καθένα.

3. Το επίπεδο του διαχειριστή του εργαλείου.

5.1.1 Network Management Interface

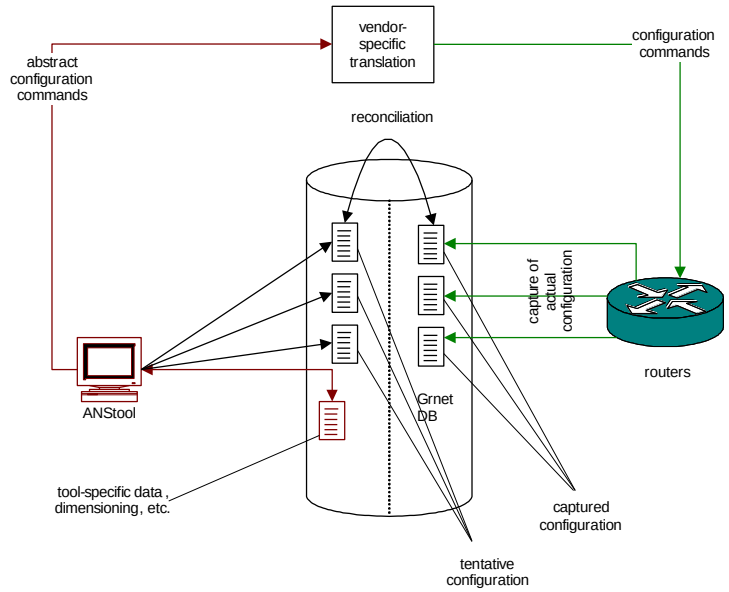
Το ANStool [97] είναι κατασκευασμένο γύρω από μια κεντρική Βάση Δεδομένων η οποία αποθηκεύει όλων των ειδών την πληροφορία διαχείρισης, συμπεριλαμβανομένου της τοπολογίας, πληροφορία για κάθε υπηρεσία, πληροφορία διαχείρισης, στοιχεία επικοινωνίας των συνδεόμενων φορέων και trouble tickets από το σύστημα παρακολούθησης και εξυπηρέτησης του ΕΔΕΤ.

Η πιο σημαντική πληροφορία στη Βάση Δεδομένων είναι η τοπολογία δικτύου. Διατηρούμε 2 διακριτά (μη συσχετισμένα) σύνολα πληροφοριών σχετικά με το δίκτυο, το πρώτο αναπαριστά το δίκτυο όπως το αντιλαμβάνονται τα L3 devices (routers) και το δεύτερο όπως το αντιλαμβάνονται τα L2 devices (switches). Αξίζει να σημειωθεί πως η layer-3 τοπολογία περιλαμβάνει και στοιχεία layer 2 (για παράδειγμα layer-2 router sub-interfaces, VLAN ids, κλπ), αλλά δεν έχει πλήρη εικόνα της layer 2 τοπολογίας.

Στην layer 3 τοπολογία, ένας δρομολογητής μοντελοποιείται σαν μια συσκευή που βρίσκεται σε μια φυσική τοποθεσία και έχει μια IP διεύθυνση για διαχείριση. Σε κάθε δρομολογητή είναι συσχετισμένα πληθώρα από φυσικά interfaces διασύνδεσης, όπου το καθένα μοντελοποιεί το τύπο του Interface (Gigabit Ethernet, Packet over SONET/SDH, ATM, κλπ) και άλλες πληροφορίες επιπέδου 1 όπως το MTU, το bandwidth της γραμμής μετάδοσης και τη δυνατότητα υποστήριξης πολλαπλών λογικών interfaces.

Ένα λογικό interface είναι ισοδύναμο με ένα layer 2 interface ή sub-interface. Κάθε λογικό interface είναι συσχετισμένο με το φυσικό interface στο οποίο ανήκει, και το οποίο φυσικό μπορεί να έχει πληθώρα λογικών interface. Σε αυτό το επίπεδο, η πληροφορία που αποθηκεύεται περιλαμβάνει layer-2 addressing για κάθε interface, (για παράδειγμα VLAN id, ATM VP/VC id). Επιπλέον, αποθηκεύεται και πληροφορία για το bandwidth ανεξαρτήτως αν η τεχνολογία του χαμηλότερου επιπέδου επιτρέπει καταμερισμό του bandwidth. Σε περίπτωση που δεν το επιτρέπει, τότε μεταφράζουμε το bandwidth που του έχει αποδοθεί σε shaping στην κατεύθυνση εξόδου. Τέλος, τα interface επιπέδου δικτύου μοντελοποιούν layer-3 πληροφορία όπως IP διεύθυνση, network mask, IP level MTU και επιπλέον διατηρούνται διαφορετικοί πίνακες για κάθε πρωτόκολλο επιπέδου δικτύου (IPv4, IPv6 κλπ). Αξίζει να σημειωθεί πως όλα τα interface επιπέδου δικτύου δεν διατηρούν πληροφορία σχετικά με bandwidth και συνεπώς όλοι οι αλγόριθμοι και οι συσχετίσεις λειτουργούν πάνω σε λογικά interfaces.

Η αποθήκευση και συντήρηση όλης αυτής της πληροφορίας γίνεται μέσω αυτόματων scripts που τα ονομάζουμε topology discovery. Αυτά επισκέπτονται τους δρομολογητές και διαβάζουν την απαραίτητη πληροφορία, την οποία στη συνέχεια (με το κατάλληλο business logic) την αποθηκεύουν στη βάση δεδομένων. Εκτός από πληροφορία τοπολογίας, η βάση δεδομένων περιέχει επιπλέον πίνακες σχετικούς με την QoS διαστασιολόγηση και την κατάσταση του ANStool. Ένα πολύ σημαντικό σημείο είναι το γεγονός πως έχει δημιουργηθεί discovery script που επισκέπτεται όλους τους δρομολογητές και διαβάζει όλο το υλοποιημένο QoS configuration και το αποθηκεύει στη βάση δεδομένων. Αυτή η πληροφορία τροφοδοτεί ένα "reconciliation" module στο ANStool που συγκρίνει την κατάσταση στο δίκτυο με την ιδεατή κατάσταση με βάση το ANStool και παράγει σε πραγματικό χρόνο ένα report με πιθανά λάθη. Με τη βοήθεια αυτού, είμαστε σε θέση να καλύπτουμε άμεσα προβλήματα λάθους configuration ή ξεχασμένων ή ελλειπών εντολών.



Εικόνα 24: Γενική αρχιτεκτονική

5.1.2 Interface χρήστη

Από το interface αυτό ο χρήστη έχει τις ακόλουθες επιλογές:

- Δημιουργία αιτήματος
- Περιγραφή υπηρεσίας
- Προβολή αιτημάτων
- Προβολή του εγχειρίδιου χρήστη

5.1.2.1 Δημιουργία αιτήματος

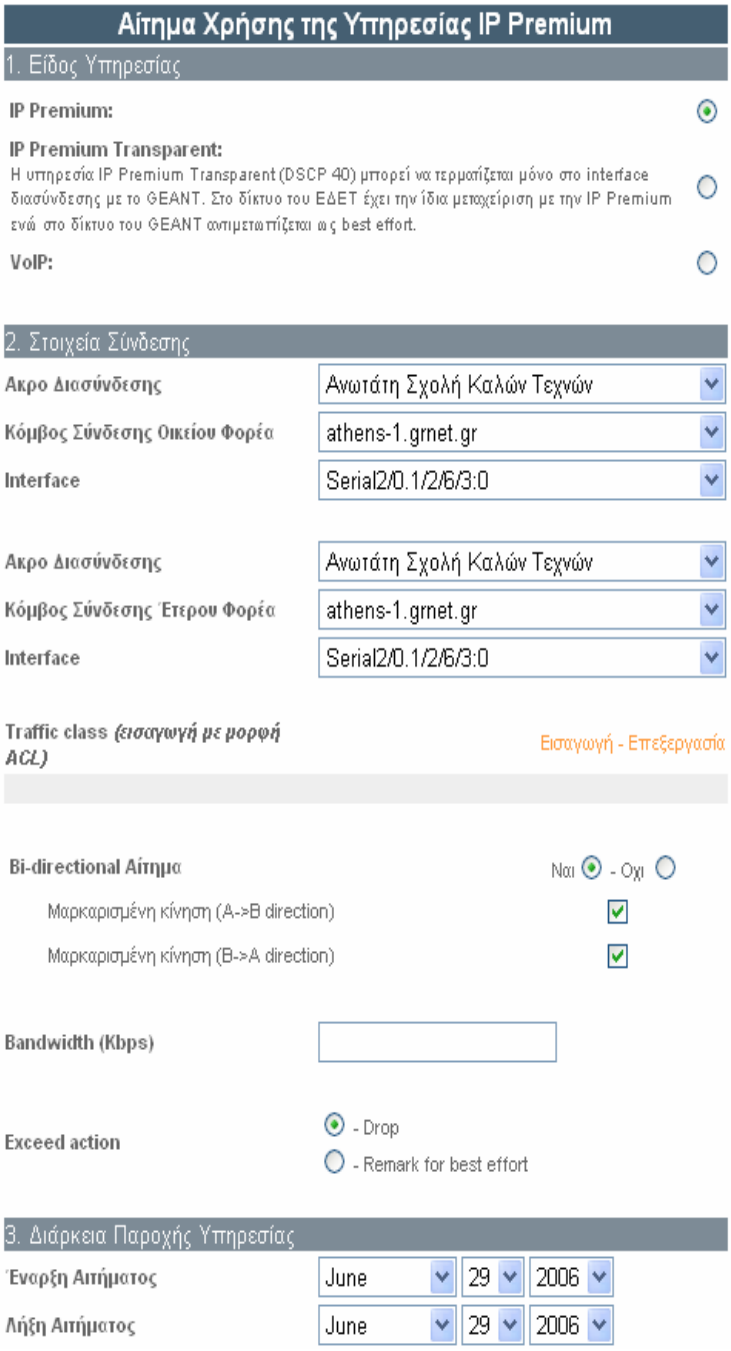
Κάθε φορέας που θέλει να υποβάλει ένα νέο αίτημα χρήσης της υπηρεσίας, καλείται να επιλέξει την επιλογή «Δημιουργία αιτήματος» στην ενότητα αυτή. Στη συνέχεια εμφανίζεται μια φόρμα (Εικόνα 25) που ο χρήστης προσδιορίζει τα στοιχεία του αιτήματος.

Αρχικά, ο χρήστης καλείται να επιλέξει το είδος της υπηρεσίας IP Premium που επιθυμεί να χρησιμοποιήσει. Στη συνέχεια ο χρήστης επιλέγει τα άκρα χρήσης της υπηρεσίας. Ειδικότερα για το οικείο άκρο προσδιορίζει το access interface του φορέα του που επιθυμεί την υπηρεσία. Η επιλογή γίνεται με τον προσδιορισμό του κόμβου σύνδεσης στο ΕΔΕΤ και του αντίστοιχου interface. Στη συνέχεια ο χρήστης επιλέγει το έτερο άκρο με προσδιορισμό του ονόματος του φορέα, του κόμβου σύνδεσης και του interface. Σε περίπτωση χρήσης της υπηρεσίας IP Premium Transparent, τότε το έτερο άκρο ρυθμίζεται και κλειδώνεται αυτόματα στο φορέα GEANT. Επίσης, στην περίπτωση αιτήματος χρήσης της υπηρεσίας IP Premium VoIP, τότε το έτερο άκρο είναι απενεργοποιημένο.

Ακολούθως, ο χρήστης καλείται να ορίσει μια σειρά από παραμέτρους για το QoS αίτημά του:

- Αν το αίτημα είναι διπλής ή μονής κατεύθυνσης (ισχύει μόνο για Ip Premium αιτήματα)
- Αν ο φορέας θα στέλνει την κίνηση μαρκαρισμένη (με βάση τις τιμές DSCP που ορίζει το ΕΔΕΤ). Αυτή η επιλογή ορίζεται για κάθε κατεύθυνση.
- Το ρυθμό της κίνησης που θα χρησιμοποιήσει την υπηρεσία IP Premium
- Δήλωση αν κίνηση που υπερβαίνει τον παραπάνω ρυθμό θα απορρίπτεται ή θα μαρκάρεται σαν best effort από το ΕΔΕΤ.

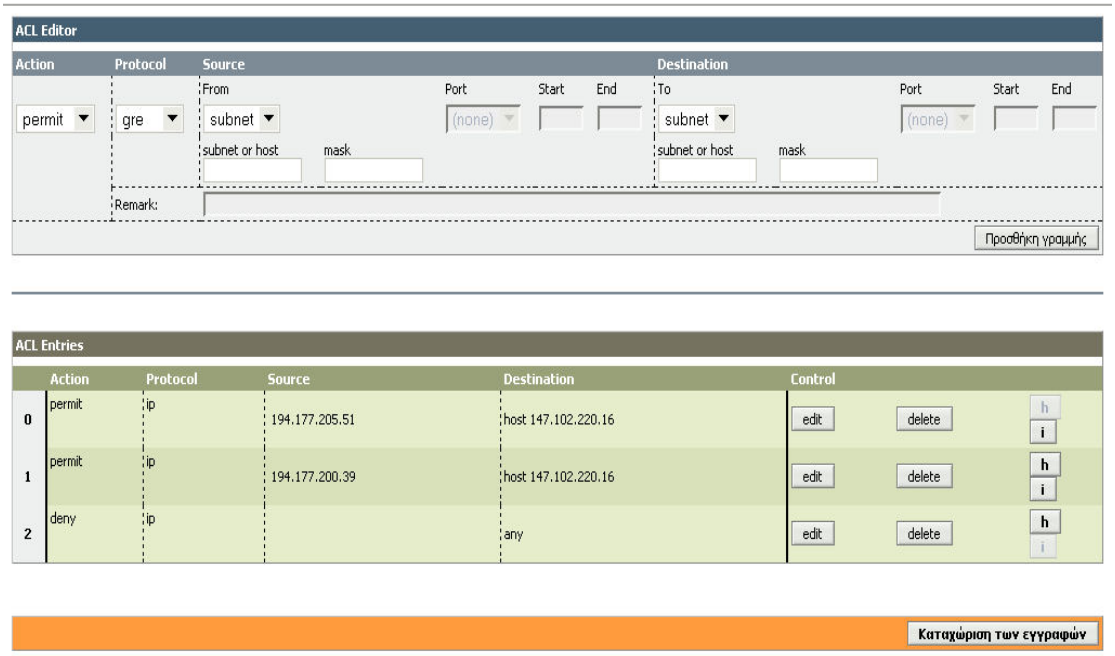
Στο σημείο αυτό πρέπει να τονιστεί πως το ΕΔΕΤ κάνει αυστηρή αστυνόμευση της κίνησης κάθε αιτήματος στον αιτούμενο ρυθμό και σε περίπτωση παραβίασης του, τότε τα επιπλέον πακέτα δέχονται την μεταχείριση που έχει ορίσει ο αιτών παραπάνω (απόρριψη ή επαναμαρκάρισμα σε best effort).



Εικόνα 25: φόρμα υποβολής αιτήματος

Βασικά χαρακτηριστικό που πρέπει να έχει κάθε αίτημα χρήσης της υπηρεσίας IP Premium είναι η εισαγωγή του traffic class που περιγράφει την κίνηση που θα δεχτεί την προνομιακή μεταχείριση. Το traffic class δηλώνεται σε μορφή μιας extended ACL, μέσω ενός υλοποιημένου ACL wizard (βλέπε Εικόνα 26) που είναι προσβάσιμος από την φόρμα υποβολής του αιτήματος (στην επιλογή «Εισαγωγή - Επεξεργασία»).

Η ACL αυτή έχει την έννοια του φιλτραρίσματος και ελέγχου της κίνησης στο interface εισόδου στο ΕΔΕΤ και πρέπει να δηλώνεται όπως ακριβώς θα εφαρμόζεται εκεί.



Εικόνα 26: ACL wizard

Τέλος, ο χρήστης δηλώνει την χρονική διάρκεια που επιθυμεί το αίτημά του να είναι ενεργό, όπως επίσης και ότι σημειώσεις αυτός κρίνει πως θέλει να γνωστοποιήσει στο ΕΔΕΤ. Στη συνέχεια υποβάλλοντας το αίτημα, το διαχειριστικό εργαλείο ελέγχει τα στοιχεία και με βάση τη διαστασιολόγηση και τα υπόλοιπα υποβληθέντα αιτήματα, αποκρίνεται αν αυτό μπορεί να ικανοποιηθεί. Η απόκριση βασίζεται στο γεγονός αν υπάρχει διαθέσιμο εύρος ζώνης στα access interfaces των φορέων (άκρων του αιτήματος) για χρήση από την υπηρεσία. Σε περίπτωση θετικής απάντησης τότε το αίτημα υποβάλλεται σε έλεγχο αποδοχής από το έτερο άκρο σύνδεσης (ισχύει μόνο για τα IP Premium αιτήματα). Στη συνέχεια, το υποβληθέν αίτημα υλοποιείται από το ΕΔΕΤ και ο φορέας ενημερώνεται για την πορεία υλοποίησης. Ο χρόνος απόκρισης σε αιτήματα είναι τουλάχιστον 24 ώρες από την στιγμή υποβολής και θετικής αποδοχής.

5.1.2.2 Προβολή αιτημάτων

Ο χρήστης χρησιμοποιώντας την επιλογή «Προβολή αιτημάτων» στην ενότητα της IP Premium υπηρεσίας μπορεί να δει όλα τα αιτήματα που έχει υποβάλει ο φορέας που εκπροσωπεί.

Η αναλυτική περιγραφή περιλαμβάνει:

- Το είδος της υπηρεσίας που ζητήθηκε (IP Premium, IP Premium Transparent, IP Premium VoIP
- Τα άκρα του αιτήματος (όνομα φορέα και οι δρομολογητές σύνδεσης στο ΕΔΕΤ)
- Το traffic class που προσδιορίζει την κίνηση που θα δεχτεί προνομιακή μεταχείριση
- Την επιλογή του χρήστη αν το αίτημα θα είναι για κίνηση μονής ή διπλής κατεύθυνσης

- Τις επιλογές του χρήστη αν η κίνηση για κάθε κατεύθυνση θα είναι μαρκαρισμένη από το φορέα ή αλλιώς θα την μαρκάρει το ΕΔΕΤ στο Interface εισόδου
- Το αιτούμενο bandwidth (profile της κίνησης του αιτήματος)
- Τη χρονική διάρκεια του αιτήματος
- Την κατάσταση του αιτήματος

Στην αναλυτική περιγραφή του κάθε αιτήματος, ο χρήστης έχει επίσης διαθέσιμες 2 επιλογές:

- Τροποποίηση αιτήματος. Ο χρήστης οδηγείται σε μια φόρμα με συμπληρωμένα τα αρχικά στοιχεία, και τα οποία μπορεί να τροποποιήσει (πλην του είδους της υπηρεσίας και των άκρων).
- Διαγραφή αιτήματος. Σε αυτή την περίπτωση το αίτημα διαγράφεται (αν έχει υποβληθεί αλλά ακόμη δεν είναι ενεργό) ή ολοκληρώνεται άμεσα και αφαιρείται το αντίστοιχο configuration από το δίκτυο αν είναι ήδη σε ισχύ.

5.1.2.3 Περιγραφή υπηρεσίας

Χρησιμοποιώντας την επιλογή «Περιγραφή υπηρεσίας» στο μενού της IP Premium υπηρεσίας, ο χρήστης βλέπει μια συνοπτική τεχνική περιγραφή της. Ειδικότερα επεξηγούνται τα είδη της υπηρεσίας (IP Premium, IP Premium Transparent, IP Premium VoIP), οι τιμές μαρκαρίσματος στο DSCP πεδίο καθώς και κάποια στοιχεία επικοινωνίας για περαιτέρω πληροφορίες.

5.1.3 Intradomain και Policy-manager interface

Παράλληλα, το διαχειριστικό εργαλείο διαθέτει μια σειρά από λειτουργικότητες που είναι διαθέσιμες στους διαχειριστές των υπηρεσιών όπως και στην ομάδα διαχείρισης των δρομολογητών. Η επιπλέον αυτή λειτουργικότητα είναι διαθέσιμη κύρια μέσα από επιλογές στο δεξιό μενού που είναι ορατές και προσβάσιμες μόνο στους διαχειριστές, αλλά και από επιλογές που ενεργοποιούνται σε άλλες σελίδες μόνο για τους διαχειριστές. Αυτή η λειτουργικότητα περιλαμβάνει:

- Δυνατότητα προβολής και επεξεργασίας / τροποποίησης της διαστασιολόγησης,
- Δυνατότητα προβολής για τις τρέχουσες δεσμεύσεις από ενεργά αιτήματα στα access interfaces όλων των φορέων,
- Δυνατότητα προβολής και ελέγχου του QoS configuration σε κάθε κόμβο.
- Αυτοματοποιημένη παραγωγή του configuration για κάθε αίτημα

5.1.3.1.1 Διαστασιολόγηση δικτύου

Η δυνατότητα προβολής και επεξεργασίας της διαστασιολόγησης είναι διαθέσιμη από την επιλογή «Διαστασιολόγηση δικτύου» στο δεξιό μενού. Ειδικότερα οι διαχειριστές μπορούν:

- να δούνε την τρέχουσα διαστασιολόγηση στις γραμμές πρόσβασης, ανά συνδεόμενο φορέα (Εικόνα 27), και αν επιθυμούν να επεξεργαστούν και να

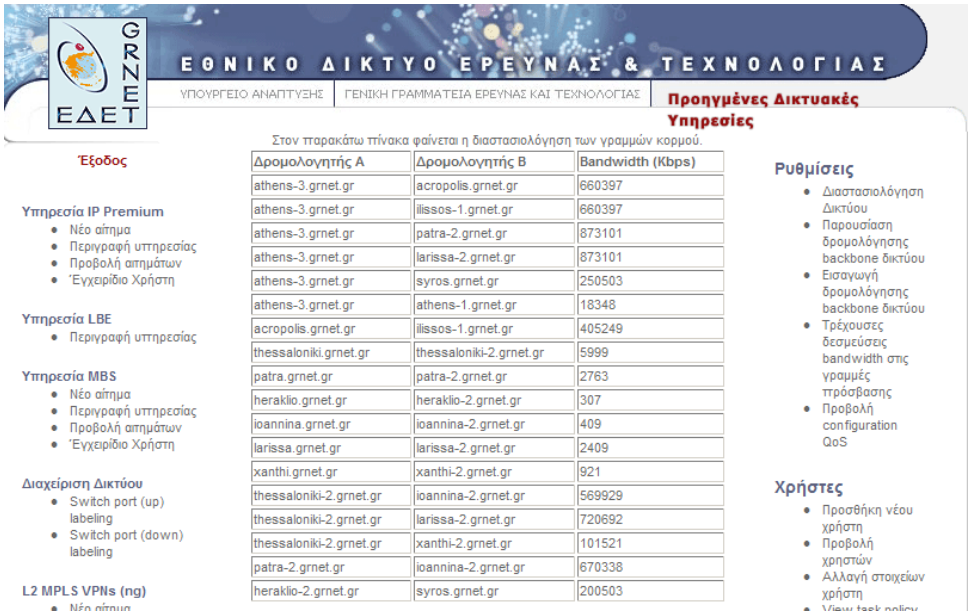
τροποποιήσουν τις σχετικές δεσμεύσεις πατώντας στη σχετική επιλογή πάνω από τον πίνακα και διαλέγοντας το σχετικό κόμβο (Εικόνα 28)

Επιπλέον, κάθε βράδυ εκτελείται ένα module, το οποίο ανανεώνει αυτόματα τη διαστασιολόγηση στις access γραμμές Η χρησιμότητα αυτού του module είναι μεγάλη σε περίπτωση που εισάγονται ή τροποποιούνται γραμμές πρόσβασης των φορέων.

Εικόνα 27: Διαστασιολόγηση γραμμών πρόσβασης

Εικόνα 28: Επεξεργασία διαστασιολόγησης γραμμών πρόσβασης

- να δούνε την τρέχουσα διαστασιολόγηση στις γραμμές κορμού (Εικόνα 29)



Εικόνα 29: Διαστασιολόγηση στις γραμμές κορμού

- να ελέγξουν τη διαστασιολόγηση και να δούνε αν υπάρχει παραβίαση της (Εικόνα 30), όπως για παράδειγμα αν κάποια ενεργά αιτήματα ξεπερνούν την τρέχουσα

διαστασιολόγηση (αυτό μπορεί να συμβεί αν μετά την έγκριση αιτημάτων μειωθεί η διαστασιολόγηση της γραμμής πρόσβασης ενός φορέα).

Εικόνα 30: Έλεγχος διαστασιολόγησης (με ορισμένα σφάλματα)

Εικόνα 31: Τρέχουσες δεσμεύσεις στις γραμμές πρόσβασης

5.1.3.1.2 Τρέχουσες δεσμεύσεις στις γραμμές πρόσβασης

Η δυνατότητα προβολής των δεσμεύσεων από ενεργά αιτήματα στα access interfaces όλων των φορέων είναι διαθέσιμη από την επιλογή «Τρέχουσες δεσμεύσεις bandwidth στις γραμμές πρόσβασης» στο δεξιό μενού. Με την επιλογή αυτή, οι

διαχειριστές μπορούνε να δούνε όλες τις τρέχουσες δεσμεύσεις bandwidth, καθώς και την μέγιστη διαστασιολόγηση σε κάθε γραμμής πρόσβασης, ανά φορέα (Εικόνα 31).

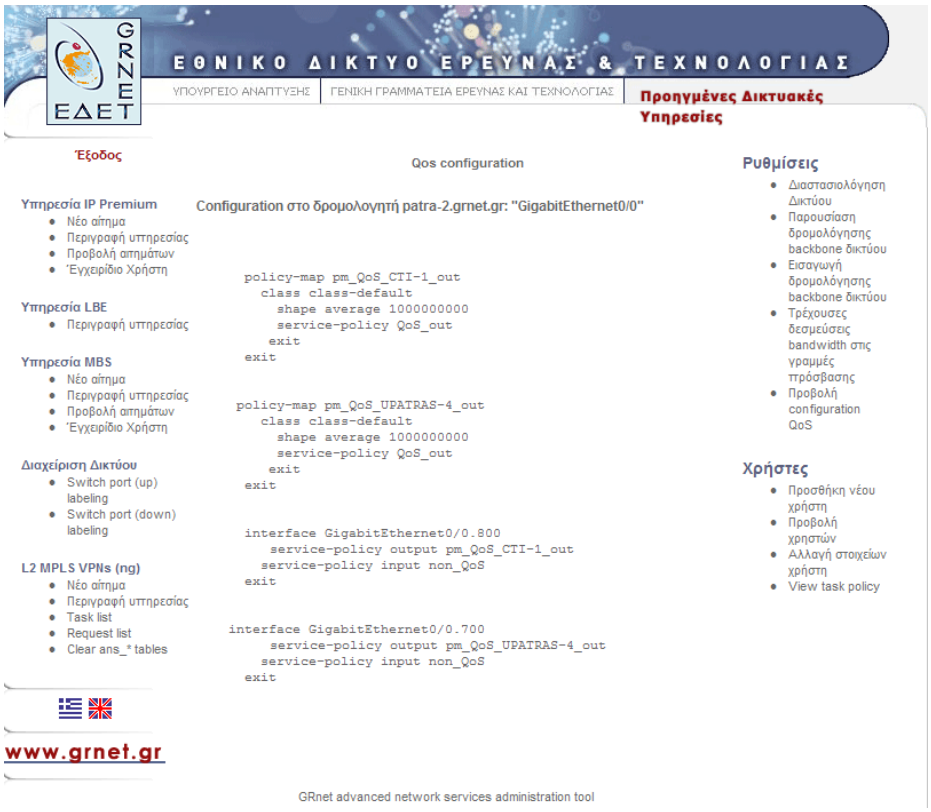
5.1.3.1.3 Προβολή και έλεγχος του QoS configuration

Η δυνατότητα προβολής και ελέγχου του QoS configuration είναι διαθέσιμη από την επιλογή «Προβολή configuration QoS» στο δεξιό μενού. Ειδικότερα οι διαχειριστές μπορούν:

- Να προβάλουν το QoS configuration για κάθε δρομολογητή και κάθε interface σε όλο το δίκτυο

  Η παραγωγή του QoS configuration είναι αυτοματοποιημένη. Η λειτουργικότητα αυτή παράγει δυναμικά το configuration για την ενεργοποίηση των ουρών και shaping σε όλα τα output access interfaces του δικτύου του ΕΔΕΤ (physical ή logical), όπως και το configuration στα input interfaces ανάλογα με τα αιτήματα και το σταθερό configuration για αποτροπή «παράνομα» μαρκαρισμένης κίνησης. Η λειτουργικότητα αυτή είναι ιδιαίτερα χρήσιμη όταν ενεργοποιούνται νέα interfaces στο δίκτυο ή γίνονται αλλαγές σε υπάρχοντα. Ένα χαρακτηριστικό παράδειγμα φαίνεται στην Εικόνα 32 και στην Εικόνα 33.

Εικόνα 32: Επιλογή interface σε κάθε δρομολογητή



Εικόνα 33: Παράδειγμα παραγόμενου configuration για κάποιο interface

- Να ελέγξουν την ορθή εφαρμογή του QoS configuration για κάθε δρομολογητή και κάθε interface, σε όλο το δίκτυο

  Η λειτουργικότητα αυτή είναι ιδιαίτερα χρήσιμη καθώς εντοπίζονται πιθανά σφάλματα ή/και αλλαγές (που μπορεί, για παράδειγμα, να έγιναν δοκιμαστικά και να μην ανακλήθηκαν) οι οποίες μπορούν δυνητικά να επιφέρουν προβλήματα στην ορθή παροχή QoS από το δίκτυο (Εικόνα 34). Οι εντοπιζόμενες διαφοροποιήσεις από το QoS configuration, δεν αντιστοιχούν όλες σε σφάλματα, καθώς υπάρχουν περιπτώσεις, που λόγω περιορισμών από τους δρομολογητές και τις κάρτες δεν είναι δυνατή η εφαρμογή του κανονικού QoS configuration και εφαρμόζεται κάποιο διαφοροποιημένο (Οι περιπτώσεις αυτές είναι γνωστές και δεν προκαλούν προβλήματα στην παροχή QoS στο δίκτυο, αλλά στο module αυτό παρουσιάζονται για λόγους ορθότητας και καλύτερης τεκμηρίωσης).

  Για την υλοποίηση της παραπάνω λειτουργικότητας, το ANStool, μέσω ενός αυτοματοποιημένου script (discovery module) διαβάζει το configuration από τους δρομολογητές και ανανεώνει την κατάσταση της ΒΔ. Στη συνέχεια, στο διαχειριστικό εργαλείο υλοποιήθηκε ένα ειδικό module που συγκρίνει το QoS configuration στο δίκτυο με το «θεωρητικό» όπως παράγεται από το εργαλείο και τα υλοποιημένα αιτήματα στο δίκτυο με όσα θα έπρεπε να έχουν υλοποιηθεί με βάση το εργαλείο. Οι έλεγχοι που αυτό το module ελέγχου υλοποιεί είναι οι ακόλουθοι:

  - Έλεγχος αιτημάτων που περιλαμβάνει:
    - Έλεγχος ορθού policing στον αιτούμενο ρυθμό
    - Έλεγχος ορθής υλοποίησης του exceed action

- Έλεγχος σωστής αντιστοίχησης του αιτήματος με την ACL του αιτήματος
- Έλεγχος ορθότητας του class-map (να περιλαμβάνει την ACL και match ip dscp αν ο φορέας μαρκάρει την κίνησή του)

- Έλεγχος ύπαρξης του σταθερού non_QoS configuration στα interfaces που δεν έχουν ενεργό κάποιο αίτημα.
- Έλεγχος του output configuration σε κάθε access interface
- Έλεγχος ορθότητας των παραμέτρων shaping στα output interfaces.
- Έλεγχος του QoS configuration στις γραμμές κορμού του δικτύου.

Η λειτουργία του discovery module είναι περιοδική και έχει ρυθμιστεί να εκτελείται καθημερινά. Το module ελέγχου εκτελείται κάθε φορά που ο διαχειριστής χρησιμοποιεί τη σχετική επιλογή ελέγχου του QoS configuration.

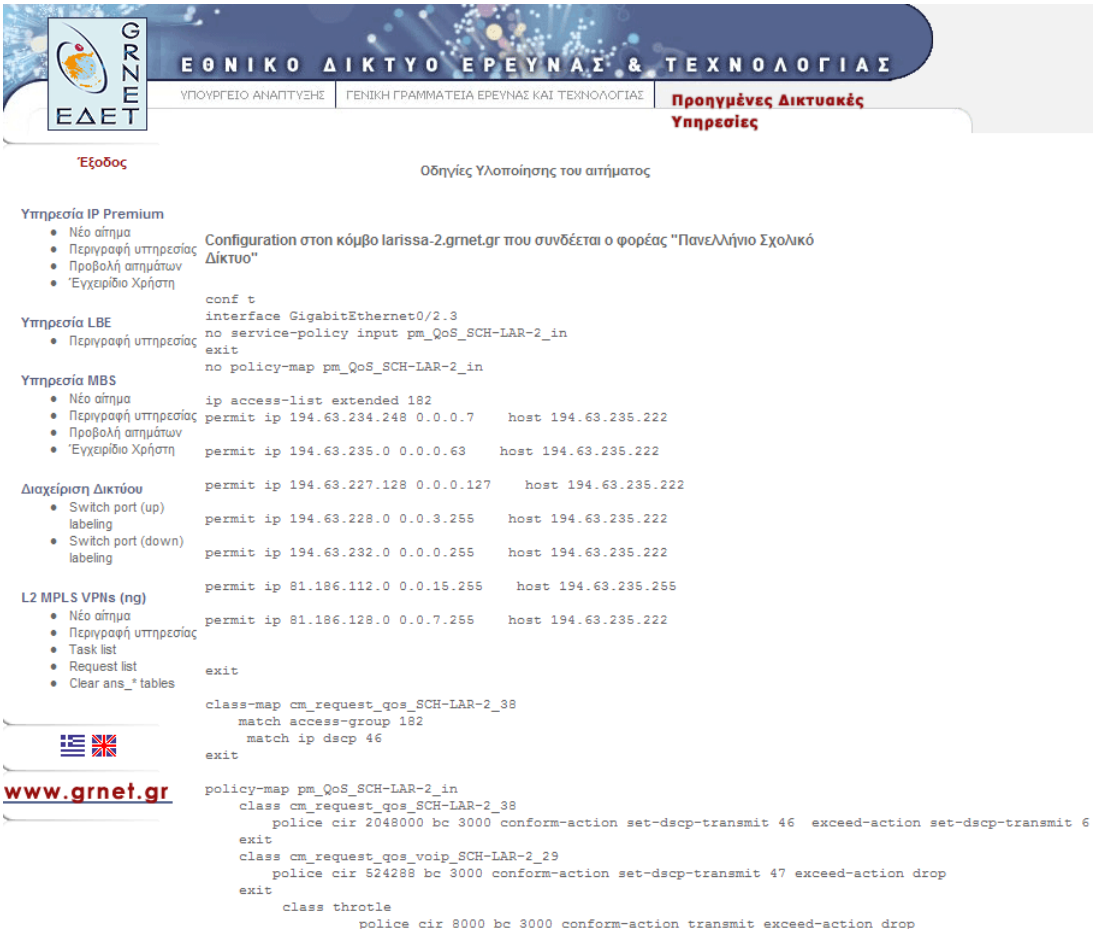
Εικόνα 34: Έλεγχος QoS configuration

5.1.3.1.4 Αυτοματοποιημένη παραγωγή του configuration για κάθε αίτημα

Η δυνατότητα αυτοματοποιημένης παραγωγής του configuration για την ικανοποίηση κάθε αιτήματος είναι διαθέσιμη μέσω της σελίδας αναλυτικής παρουσίασης κάθε αιτήματος. Στη σελίδα αυτή για τους διαχειριστές της υπηρεσίας είναι ενεργοποιημένη η πρόσθετη επιλογή «Οδηγίες υλοποίησης». Η επιλογή αυτή

παράγει το configuration που πρέπει να εφαρμοστεί στα interfaces σύνδεσης λαμβάνοντας υπόψη του όλα τα υπόλοιπα ενεργά αιτήματα των interfaces αυτών. Ένα χαρακτηριστικό παράδειγμα παρουσιάζεται στην Εικόνα 35.

Μάλιστα στην παραπάνω σελίδα αναλυτικής παρουσίασης κάθε αιτήματος γίνεται αυτοματοποιημένη ενημέρωση για την ενεργοποίηση ή την κατάργηση αιτημάτων, (με αυτόματη αλλαγή της κατάστασης του εκάστοτε αιτήματος), ώστε οι διαχειριστές να προβαίνουν στις κατάλληλες ενέργειες κάθε φορά κλπ.



Εικόνα 35: Αυτόματη παραγωγή του configuration για κάθε αίτημα

5.1.4 InterDomain interface

Το ANStool [97] υποστηρίζει διαχείριση σε ένα single managed δίκτυο, όμως οι ανάγκες επιβάλουν συνεργατική διαχείριση σε επίπεδο ιεραρχικών federations. Για το σκοπό αυτό έχει υλοποιηθεί η υποδομή για τη διασύνδεση του ANStool με το διαχειριστικό εργαλείο του Geant (AMPS) [93], βασισμένη σε standards (XML) και πρότυπα (Web Services).

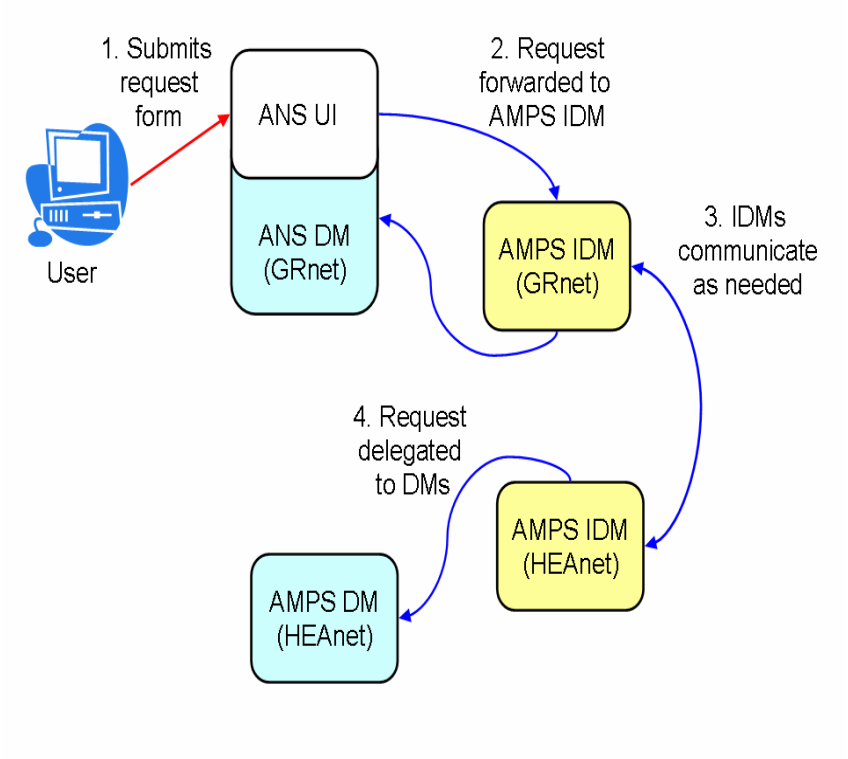
Οι λειτουργικότητες που έχουν υλοποιηθεί είναι οι εξής:

- Αυτόματη υποβολή αιτήματος που σαν έτερο άκρο διασύνδεσης έχει σημείο στον Ευρωπαϊκό χώρο, στην ιεραρχία του AMPS για επεξεργασία. Το ANStool έχει

συνδεθεί με το AMPS ώστε να λαμβάνει και να επεξεργάζεται τα αιτήματα που αφορούν το domain του ΕΔΕΤ

- Υλοποίηση λειτουργιών cancel και query για αιτήματα με παν-ευρωπαϊκή εμβέλεια που ένα τμήμα τους είναι στο domain του ΕΔΕΤ.

Συνολικά η δράση αυτή είναι ακόμη πιλοτική και θα συντηρείται σε αυτή τη μορφή έως ότου το εργαλείο του AMPS περάσει πλήρως σε κατάσταση υπηρεσίας παραγωγής.

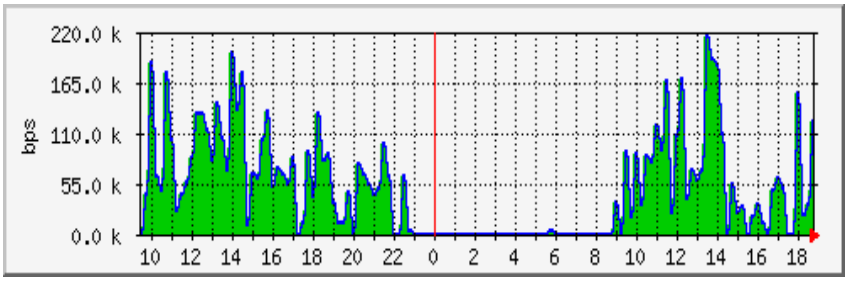


Εικόνα 36: ANStool interdomain

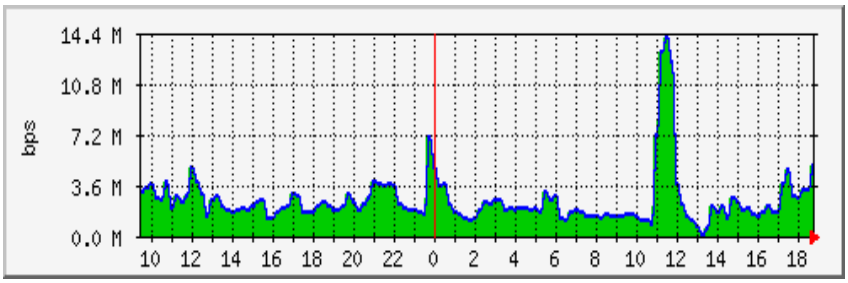
5.2 ΑΠΟΤΕΛΕΣΜΑΤΑ ΧΡΗΣΗΣ

Το ANStool βρίσκεται σε λειτουργία από τον Γενάρη του 2006 (και από τότε αναβαθμίζεται διαρκώς), όπως και η υπηρεσίες QoS ανήκουν στις υπηρεσίες παραγωγής του ΕΔΕΤ από τον Οκτώβρη του 2006. Όλο αυτό το διάστημα, 25 αιτήματα μόνιμου χαρακτήρα (SDA και SADU) έχουν υποβληθεί και εξυπηρετηθεί μέσω του ANSTool. Επίσης, στο ίδιο διάστημα έχουν υποβληθεί και πληθώρα αιτημάτων με μικρή όμως διάρκεια, συνήθως για τις ανάγκες διαφόρων projects.

Αναλυτικά γραφήματα καθυστέρησης και jitter δεν είναι διαθέσιμα για το δίκτυο παραγωγής, παρόλα αυτά υπάρχουν μετρήσεις QoS bandwidth με χρήση MRTG. Η Εικόνα 37 δείχνει την IP Premium κίνηση που κατευθύνεται προς το Πανεπιστήμιο Αθηνών και προέρχεται από VoIP κλήσεις, ενώ η Εικόνα 38 δείχνει την LBE κίνηση σε μια γραμμή κορμού στο MAN της Αθήνας.



Εικόνα 37: IP premium κίνηση στο Παν. Αθηνών



Εικόνα 38: LBE κίνηση στο MAN της Αθήνας

ΚΕΦΑΛΑΙΟ 6: ΕΠΕΚΤΑΣΗ QOS ΥΠΗΡΕΣΙΩΝ ΣΕ IPV6 ΠΕΡΙΒΑΛΛΟΝ

ΕΠΕΚΤΑΣΗ QOS ΥΠΗΡΕΣΙΩΝ ΣΕ IPV6 ΠΕΡΙΒΑΛΛΟΝ

6.1 ΕΙΣΑΓΩΓΗ

Η εξάπλωση του πρωτοκόλλου IPv6 αναμένεται να είναι ραγδαία τα επόμενα χρόνια καθώς αντιμετωπίζει μια σειρά από προβλήματα που υπάρχουν σήμερα με την χρήση του πρωτοκόλλου IPv4. Το IPv6 περιγράφεται στο RFC 2460 και σε σχέση με το παλιότερο πρωτόκολλο προσφέρει:

- Διευρυμένο χώρο διευθύνσεων από 32 σε 128 bits
- Απλοποίηση της επικεφαλίδας
- Καλύτερη υποστήριξη επιλογών και επεκτάσεων στην στάνταρ επικεφαλίδα
- Δυνατότητα μαρκαρίσματος των ροών κίνησης (Flow Label)
- Δυνατότητες για ασφάλεια (Authentication και Privacy)

Οι αλλαγές από το IPv4 στο IPv6 μπορούν να συνοψισθούν στις παρακάτω κατηγορίες:

- Εκτεταμένη δυνατότητα διευθυνσιοδότησης: Το IPv6 αυξάνει το μέγεθος της IP διεύθυνσης από 32 σε 128 bits, προσφέροντας δυνατότητες για περισσότερα επίπεδα διευθυνσιοδότησης, "ανεξάντλητο" χώρο διευθύνσεων και απλούστερη διαδικασία απόδοσης των διευθύνσεων (autoconfiguration). Η διαβαθμισιμότητα της δρομολόγησης multicast έχει βελτιωθεί, προσθέτοντας το πεδίο scope στη διεύθυνση που πληροφορεί το δρομολογητή για την περιοχή των host που "ακούνε" (π.χ. LAN, WAN, Internet).
- Απλοποιημένη επικεφαλίδα: Ορισμένα πεδία του IPv4 απουσιάζουν από το IPv6 ή έχουν γίνει προαιρετικά. Αυτό βοηθά στη μείωση του κόστους δρομολόγησης για κάθε πακέτο και του κόστους σε εύρος ζώνης που καταναλώνει η επικεφαλίδα. Η επικεφαλίδα, επίσης, έχει σταθερό μήκος, και οι δρομολογητές έχουν καλύτερη απόδοση για τέτοιες επικεφαλίδες.
- Βελτιωμένη υποστήριξη για επεκτάσεις και επιλογές της επικεφαλίδας: Το IPv6 διαθέτει υποστήριξη προαιρετικών πεδίων σε ξεχωριστές επικεφαλίδες. Αυτό διευκολύνει την απόδοση της απλής δρομολόγησης, αφού δεν χρειάζεται κάθε δρομολογητής να επεξεργαστεί αυτά τα πεδία, αν κάτι τέτοιο δεν είναι αναγκαίο.
- Έλεγχος ροής στο επίπεδο IP: Μια καινούρια λειτουργία έχει προστεθεί που κατηγοριοποιεί τα πακέτα ενός αποστολέα σε μια συγκεκριμένη ροή (flow) με βάση το πεδίο flow label. Αυτή η ροή μπορεί να αντιμετωπιστεί με κάποιο ειδικό τρόπο (π.χ. μια ροή δεδομένων live streaming video)
- Ασφάλεια στο επίπεδο IP: Το IPv6 προσφέρει, μέσω των επικεφαλίδων επέκτασης, ασφάλεια και απόκρυψη δεδομένων.

Στα δίκτυα που χρησιμοποιούν πλέον το πρωτόκολλο IPv6 μπορούν θεωρητικά να εφαρμοστούν τεχνικές που ακολουθούν την IntServ και DiffServ αρχιτεκτονική. Ειδικότερα για την DiffServ αρχιτεκτονική που έχει και την μεγαλύτερη δυναμική,

στο πρωτόκολλο IPv6 έχει ήδη προβλεφθεί το πεδίο Traffic Class όπου περιέχεται το πεδίο DSCP για μαρκάρισμα των ροών σε κλάσεις. Επίσης, έχει εισαχθεί ένα νέο πεδίο που ονομάζεται flow label και ο στόχος του είναι να διαχωρίζει την κίνηση σε επίπεδο ροών. Ο διαχωρισμός αυτός μπορεί να συμβάλει στην παροχή εξειδικευμένων υπηρεσιών ποιότητας υπηρεσίας, γεγονός που μελετάται σήμερα από μια ειδική ομάδα ερευνητών. Ειδικότερα, οι προδιαγραφές του πεδίου Flow Label της επικεφαλίδας του IPv6 και οι ελάχιστες απαιτήσεις για την πηγή και τους ενδιάμεσους κόμβους αναλύονται στο RFC 3697 [54].

6.2 ΜΕΛΕΤΗ ΑΠΟΔΟΤΙΚΟΤΗΤΑΣ ΜΗΧΑΝΙΣΜΩΝ ΣΕ IPv6 ΚΙΝΗΣΗ

Για να προχωρήσουμε στην επέκταση των QoS υπηρεσιών ώστε να λειτουργούν και σε IPv6 κίνηση, πραγματοποιήσαμε μελέτη υποστήριξης και απόδοσης των QoS μηχανισμών στο δίκτυο. Ειδικότερα, διακρίναμε τους δρομολογητές του δικτύου στις 2 παρακάτω κατηγορίες:

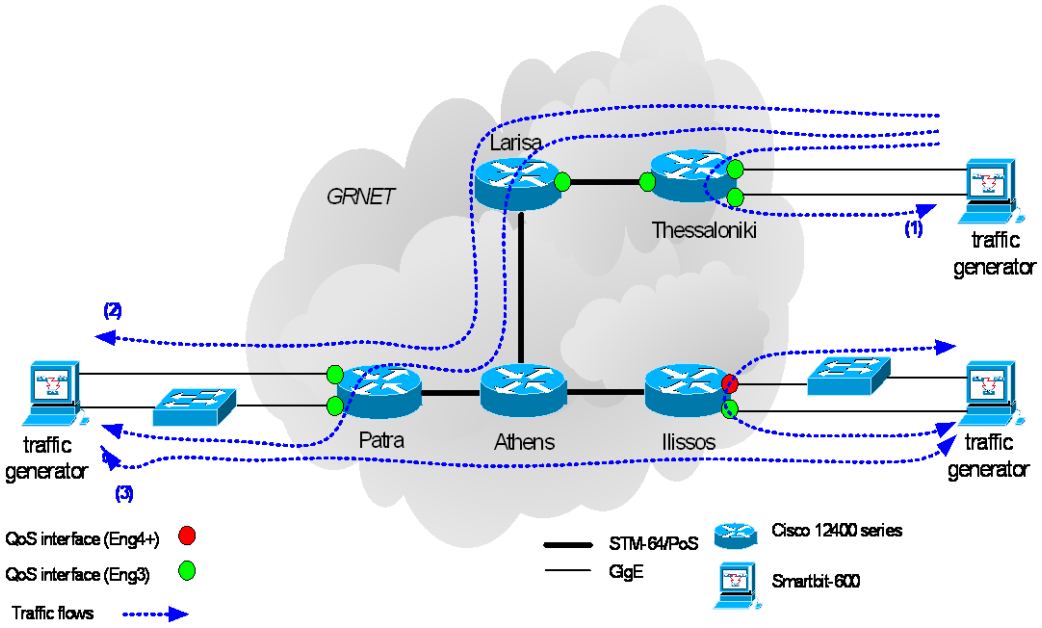
- Εξοπλισμός με hardware based IPv6 switching
- Εξοπλισμός με software based IPv6 switching

Οι δοκιμές που πραγματοποιήθηκαν αφορούσαν την δοκιμή και αξιολόγηση των ακόλουθων παραμέτρων:

- Υποστήριξη μηχανισμών χαρακτηρισμού και μαρκαρίσματος της κίνησης
- Επίδραση της κίνησης στο CPU load
- Δοκιμή ικανότητας switching των interfaces
- Μελέτη packet loss και throughput σε κίνηση μέσω ουρών απόλυτης προτεραιότητας

6.2.1 Δοκιμές σε εξοπλισμό με hardware based IPv6 switching

Η πρώτη σειρά tests αφορούσε τη διερεύνηση μηχανισμών classification και ACLs. Το Smartbit traffic generator παρήγαγε IPv6 κίνηση 100Mbps προς συγκεκριμένη IP διεύθυνση. Δοκιμάστηκαν επιτυχώς ACLs στο Input Interface των φυσικών θυρών όπως και στο output λογικών θυρών. Στη συνέχεια δοκιμάστηκε ο μηχανισμός αστυνόμευσης με επιτυχία όπως και ο μηχανισμός shaping. Κατά την δοκιμή shaping, το smartbit παρήγαγε bursty κίνηση με μέσο ρυθμό 400Mbps και γινόταν shaping στο output interface στα 200Mbps. Τα αποτελέσματα απέδειξαν πως το latency ήταν 443 msec και το μέγιστο latency ήταν 9 φορές μεγαλύτερο από το μέσο. Σε περίπτωση μη ενεργοποίησης shaping, η μέγιστη τιμή του latency ήταν 5,5 φορές μεγαλύτερη από τη μέση τιμή (που είναι 236 μsec). Συνεπώς ορθώς προκύπτει πως ο μηχανισμός shaping εισάγει ένα σημαντικό latency, όπως αναμενόταν.



Εικόνα 39: Η τοπολογία δοκιμών

Η επόμενη σειρά πειραμάτων στόχευε να διερευνήσει τον αντίκτυπο στο CPU load των δρομολογητών όταν κάνουν IPv6 switching σε gigabit ταχύτητες. Σε αυτή την περίπτωση δημιουργήθηκαν 2 ροές (διπλής κατεύθυνσης) στον δρομολογητή patra-2.grnet.gr. Αρχικά δοκιμάστηκε IPv4 μόνο κίνηση και για διάστημα 30 λεπτών όπου δεν παρουσιάστηκε αύξηση στο CPU load (ήταν περίπου στο 11%). Στη συνέχεια η κίνηση που περνούσε ήταν μίξη IPv4 και IPv6 και στη συνέχεια δοκιμάστηκε μόνο IPv6 κίνηση. Οι μετρήσεις έδειξαν πως δεν παρουσιάστηκε καμία αύξηση στο CPU load. Παράλληλα, στη σειρά των πειραμάτων που έγιναν στον δρομολογητή patra-2 παρατηρήθηκε πρόβλημα στα IPv6 BGP sessions όταν το Interface ήταν συμφορημένο. Το πρόβλημα αυτό ήταν περιορισμένο στα συγκεκριμένα interfaces, ενώ σε όλα τα υπόλοιπα (που δρομολογούσαν κίνηση παραγωγής) δεν υπήρχε κανένα απολύτως πρόβλημα. Το γεγονός αυτό προέκυψε επειδή η IPv6 control κίνηση δεν είναι προστατευμένη στις εσωτερικές CPU ουρές σε αντίθεση με την IPv4.

Στη συνέχεια έγιναν δοκιμές με Best Effort IPv4 και IPv6 κίνηση και τα αποτελέσματα έδειξαν ακριβώς ίδιο packet loss για IPv4 και IPv6. Το γεγονός πως παρατηρήθηκε packet loss σε ρυθμό κίνησης ίσο με 1Gbps οφείλεται στο ότι οι κάρτες πρόσβασης δεν υποστηρίζουν συνολικά line rate switching (γνωστό από τις προδιαγραφές τους). Σε αυτές τις κάρτες παρουσιάστηκε packet loss 13,88% και για IPv4 και για IPv6 κίνηση όταν δεχόταν κίνηση με ρυθμό 1Gbps.

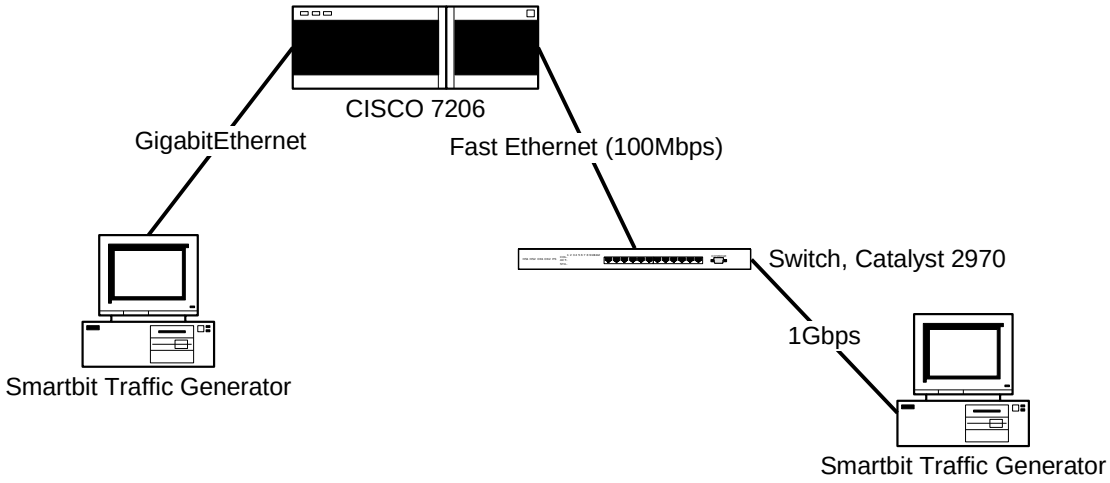
Στη συνέχεια των δοκιμών ενεργοποιήθηκαν ουρές προτεραιότητας στο testbed (σε όλα τα output interfaces), με στόχο να διερευνήσουμε την απόδοσή τους με IPv6 κίνηση. Τα Smartbits δημιουργούσαν κίνηση όπου το 2% ήταν μαρκαρισμένη ως IP Premium και το υπόλοιπο ήταν Best effort. Τα πειράματα ξεκινούσαν με κίνηση από 100Mbps και έφτανε στο 1Gbps (με βήματα των 150Mbps). Τελικά υπήρχε μηδενικό packet loss για την IPv6 Premium κίνηση. Ομοίως, ελέγχοντας και το latency της κίνησης προκύπτει πως για όσο δεν υπάρχει packet loss, δηλαδή μέχρι 850Mbps όπως υπάρχει στο specification της κάρτας και αποδείχτηκε και πειραματικά, το latency για IP Premium και BE είναι το ίδιο και ιδιαίτερα χαμηλό. Όταν υπάρχει packet loss, τότε το latency της Premium κίνησης είναι 20 φορές μεγαλύτερο από πριν αλλά και 100 φορές μικρότερο από ότι στην BE.

Συμπερασματικά λοιπόν, ο εξοπλισμός που υποστηρίζει hardware based IPv6 switching μπορεί να υποστηρίξει υπηρεσίες QoS για την κίνηση IPv6 το ίδιο καλά όσο για την κίνηση IPv4. Η υποστήριξη λειτουργιών είναι άριστη σε επίπεδο φυσικής και λογικής θύρας και οι κάρτες πρόσβασης υποστηρίζουν ρυθμό κίνησης μέχρι 850Mbps (γνωστό από το specification και επιβεβαιώθηκε και πειραματικά). Οι κάρτες παρουσίασαν ένα πρόβλημα στα BGP sessions των interfaces που έχουν μεγάλη συμφόρηση από δρομολόγηση IPv6 κίνησης, αλλά αυτό δεν αναμένεται να προβληματίσει έντονα τη συνολική λειτουργία δεδομένου πως η συνολική IPv6 κίνηση στο δίκτυο δεν αναμένεται τα επόμενα χρόνια να δημιουργεί συνθήκες έντονου κορεσμού.

6.2.2 Δοκιμές σε εξοπλισμό με software based IPv6 switching

Στη συνέχεια έγιναν αντίστοιχα πειράματα στις πλατφόρμες που υλοποιούν software based IPv6 switching με στόχο να συλλέγουν συμπεράσματα για την απόδοση τους.

```
R7206#show version
Cisco IOS Software, 7200 Software (C7200-IS-M), Version 12.3(14)T1, RELEASE SOFT
WARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 31-Mar-05 08:04 by yiyan
```

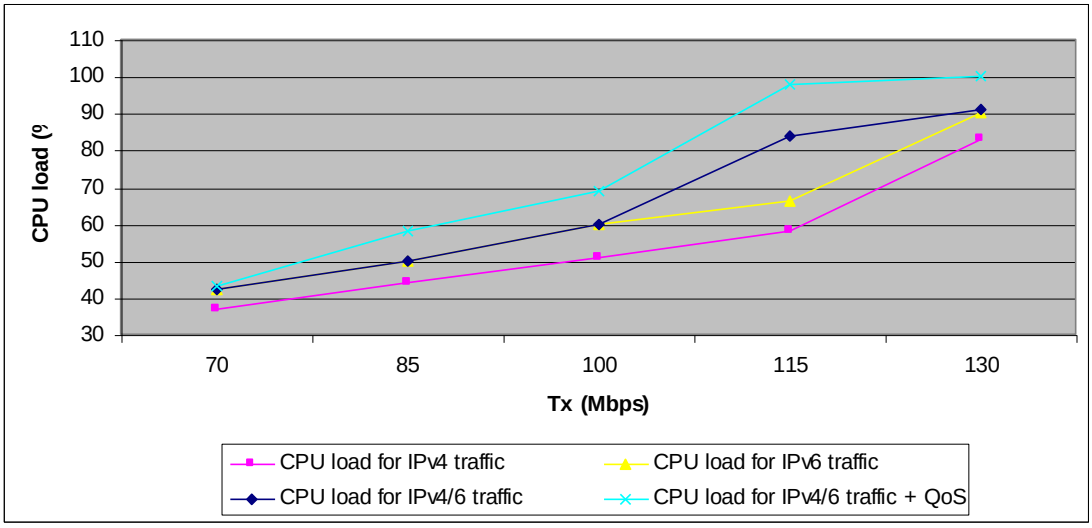


Εικόνα 40: Η τοπολογία δοκιμών για τις software based πλατφόρμες

Η πειραματική διαδικασία περιέχει διάφορα στάδια και αρχικά εκτελέστηκαν δοκιμές προκειμένου να διερευνηθεί η διαφορά στη διαχείριση IPv4 και IPv6 κίνησης. Ειδικότερα, η πρώτη σειρά πειραμάτων περιλάμβανε την δημιουργία κίνησης από το Smartbit με ρυθμό 70Mbps έως 130 Mbps και βήμα 15 Mbps. Το σενάριο αυτό εκτελέστηκε 4 φορές όπου στην πρώτη η κίνηση ήταν IPv4 μόνο, στη δεύτερη IPv6 μόνο και στη τρίτη ήταν μίξη IPv4 και IPv6 σε αναλογία 50-50. Στην τέταρτη είχε

ενεργοποιηθεί το κλασικό QoS configuration (ουρές προτεραιότητας στο output του FastEthernet 2/0) και η κίνηση ήταν ξανά μίξη IPv4 και IPv6 best effort σε αναλογία 50-50. Στις δοκιμές αυτές μετρήθηκε το throughput της κίνησης και το CPU load του δρομολογητή. Η μέτρηση του CPU load γινόταν στο τέλος κάθε πειράματος συγκεντρώνοντας πληροφορίες από το CLI (CPU 5sec average). Όλα τα πειράματα εκτελέστηκαν με μέγεθος πακέτου 512 bytes.

Το αποτέλεσμα των δοκιμών ήταν πως packet loss εμφανίστηκε όταν η παραγόμενη κίνηση ξεπερνούσε τα 100Mbps και δεν παρουσιάστηκε καμία διαφοροποίηση μεταξύ IPv4 και IPv6. Αυτό σημαίνει πως οι δρομολογητές αυτοί έχουν τη δυνατότητα line rate switching ως προς το fastethernet interface. Αντίστοιχο συμπέρασμα για Gigabit ταχύτητες δεν μπορούμε να εξάγουμε καθώς ο δρομολογητής είχε μόνο 1 Gigabit Ethernet port. Παράλληλα, αξιοσημείωτα είναι τα αποτελέσματα σχετικά με το CPU load. Ειδικότερα, στην περίπτωση ύπαρξης IPv6 κίνησης παρουσιάζεται αύξηση του CPU load κατά 5-9%. Επίσης, στο τελευταίο πείραμα που είχε ενεργοποιηθεί και QoS configuration παρουσιάστηκε το shell να είναι κολλημένο όταν η παραγόμενη κίνηση από το Smartbit ήταν 130 Mbps.



Εικόνα 41: CPU load

Στη συνέχεια δοκιμάστηκε ένα δεύτερο σενάριο που στόχευε να διερευνήσει τη συμπεριφορά του δρομολογητή σε κίνηση με διάφορα μεγέθη πακέτων. Ειδικότερα, το Smartbit παρήγαγε κίνηση 85Mbps για 10sec, στη συνέχεια την αύξανε σε 100Mbps για άλλα 10 sec και τέλος γινόταν 115 Mbps για άλλα 10 sec. Το σενάριο αυτό εκτελέστηκε σε επαναλήψεις όπου το μέγεθος των πακέτων της κίνησης ήταν από 128 bytes έως 1408 bytes με βήμα 128. Οι δοκιμές αυτές έγιναν 3 φορές, όπου αρχικά υπήρχε IPv4 μόνο κίνηση, τη δεύτερη IPv6 μόνο και την τρίτη υπήρχε μίξη IPv4 και IPv6 σε αναλογία 50-50. Ένα πολύ ενδιαφέρον αποτέλεσμα προέκυψε στην περίπτωση που η κίνηση παραγόταν σε πακέτα των 128 bytes. Τότε ο δρομολογητής παρουσίαζε μια ασυνήθιστη και ασταθή συμπεριφορά μόλις ο φόρτος κίνησης προσέγγιζε την χωρητικότητα του interface (100Mbps). Στην περίπτωση της IPv4 κίνησης, όταν ο φόρτος που παρήγαγε το Smartbit ήταν 100Mbps υπήρχαν ελάχιστα drops και το CPU load του δρομολογητή ήταν πολύ υψηλό. Στη συνέχεια, μόλις ο φόρτος γινόταν 115 Mbps, ο δρομολογητής γινόταν εξαιρετικά ασταθής, όλα τα πακέτα απορρίπτονταν και χρειαζόταν περίπου 10 sec από τη στιγμή που σταματούσε η παραγωγή κίνησης για να επανέλθει σε φυσιολογική λειτουργία. Το φαινόμενο

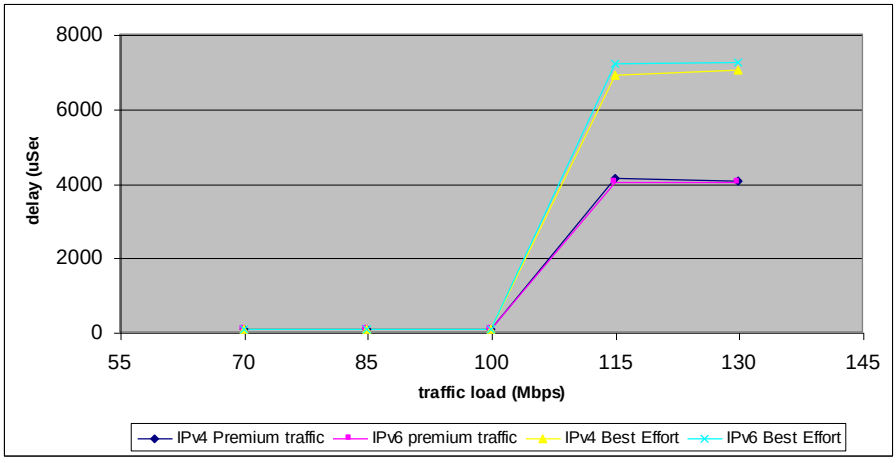
αυτό παρουσιαζόταν σε πολύ μεγαλύτερη έκταση όταν ο δρομολογητής είχε να μεταγάγει IPv6 κίνηση, καθώς το packet loss όταν ο φόρτος ήταν 100Mbps ήταν 14,8%. Αυτή η συμπεριφορά επαναλήφθηκε και όταν η κίνηση ήταν μίξη IPv4 και IPv6. Τέλος πρέπει να σημειώσουμε πως στην περίπτωση αυτή το packet loss ήταν κατανεμημένο το ίδιο σε IPv4 και IPv6 κίνηση.

Στην πραγματικότητα, η κατάσταση αυτή (πακέτα μικρού μεγέθους – 128 bytes) χαρακτηρίζεται σαν DoS attack και οι software based πλατφόρμες είναι ευάλωτες σε τέτοιες επιθέσεις. Η διαφοροποίηση όμως που παρουσιάζεται στη συμπεριφορά ανάλογα με το είδος της κίνησης (στο IPv6 παρουσιάζεται μεγαλύτερο packet loss σε κίνηση 100Mbps) δεν μπορεί να εξηγηθεί. Προφανώς άπτεται του εσωτερικού σχεδιασμού και της λειτουργίας των software modules του δρομολογητή. Τέλος πρέπει να σημειωθεί πως για μεγέθη πακέτων μεγαλύτερα ή ίσα των 256 bytes η συμπεριφορά του δρομολογητή είναι υποδειγματική.

packet size (bytes)	Packet loss (%)								
	IPv4 traffic (Mbps)			IPv6 traffic (Mbps)			IPv4 and IPv6 traffic (Mbps)		
	85	100	115	85	100	115	85	100	115
128	0	0,17	100	0	14,83	100	0	14,99	100
256	0	0	12,55	0	0	12,55	0	0	12,55
384	0	0	12,62	0	0	12,61	0	0	12,62
512	0	0	12,66	0	0	12,66	0	0	12,66

Πίνακας 6: Αποτελέσματα πειραμάτων για διάφορα μεγέθη πακέτων

Στη συνέχεια εκτελέστηκαν διάφορα πειράματα με στόχο να διερευνήσουν τους βασικούς QoS μηχανισμούς. Ειδικότερα δοκιμάστηκαν επιτυχώς κατηγοριοποίηση της κίνησης με βάση το DSCP πεδίο του traffic class, μαρκάρισμα του DSCP πεδίου και τέλος αστυνόμευση με χρήση token bucket αλγορίθμου. Επίσης, δοκιμάστηκε επιτυχώς QoS configuration για ενεργοποίηση priority ουράς στο output ενός interface και γενικά ο μηχανισμός CBWFQ για διαχείριση ουρών που υποστηρίζει ο δρομολογητής δούλεψε απροβλημάτιστα.



Εικόνα 42: Αποτέλεσμα μέσου delay σε QoS enabled interfaces

Ένα τυπικό παράδειγμα παρουσιάζεται στην Εικόνα 42, όπου είναι το αποτέλεσμα του delay που μετρήθηκε δοκιμάζοντας το ακόλουθο σενάριο: το Smartbit παρήγαγε IPv4 και IPv6 κίνηση (σε αναλογία 50-50) και ο φόρτος κίνησης ήταν από 70 Mbps

έως 130 Mbps με βήμα 15 Mbps. Από τα πακέτα αυτά, το 5% των IPv4 και το 5% των IPv6 ήταν μαρκαρισμένα με DSCP 46. Το αποτέλεσμα είναι πώς όσο η κίνηση δεν ξεπερνούσε την χωρητικότητα του interface (100Mbps) το μέσο delay ήταν ίδιο και σε απόλυτη τιμή πολύ μικρό τόσο για την Premium όσο και για την best effort κίνηση. Μόλις το interface βρέθηκε σε κατάσταση σημαντικής συμφόρησης, τότε το delay της premium κίνησης αυξήθηκε σημαντικά αλλά το προστάτεψε η ουρά προτεραιότητας και ήταν τελικά το μισό συγκρινόμενο με το delay της best effort κίνησης. Επίσης, η Premium κίνηση παρουσίαζε μηδενικό packet loss ενώ η best effort σημαντικό. Τέλος, πρέπει να σημειωθεί πως στην τελευταία επανάληψη του σεναρίου που ο φόρτος κίνησης ήταν 130 Mbps το shell του δρομολογητή ήταν κολλημένο.

Η επόμενη σειρά πειραμάτων αφορούσε τη δοκιμή και χρήση του πεδίου flow label για πιο εξειδικευμένη κατηγοριοποίηση. Ο μόνος πιθανός τρόπος χρήσης του πεδίου flow label είναι μέσω IPv6 access lists καθώς δεν είναι διαθέσιμο σαν matching κριτήριο σε άλλους μηχανισμούς. Η χρήση αυτή του flow label μέσω ACL επιτρέπει την κατηγοριοποίηση της κίνησης με κριτήρια (source address AND destination address AND DSCP AND flow label), με αποτέλεσμα να μπορούμε να επιτύχουμε ανεξάρτητη αστυνόμευση σε ροές παρά απλά σε συνενώσεις ροών όπως στο IPv4. Συνεπώς, με τον τρόπο αυτό μπορούμε να έχουμε πιο εξειδικευμένη αστυνόμευση με τη χρήση του επιπλέον κριτηρίου (flow label) γεγονός που μπορεί να αποδειχθεί ιδιαίτερα σημαντική για ειδικές απαιτητικές εφαρμογές όπως για παράδειγμα VoIP. Από την άλλη πλευρά, η χρήση του flow label πρέπει να γίνεται πολύ προσεκτικά και πρέπει να ακολουθεί τις οδηγίες που περιγράφονται στο σχετικό RFC. Είναι απαραίτητο να υπάρχει ένας κεντρικός μηχανισμός που θα αναθέτει τιμές στο flow label. Επίσης το εύρος τιμών που θα χρησιμοποιείται θα είναι ισχυρό μόνο στο εσωτερικό του ΕΔΕΤ καθώς δεν υπάρχει ακόμη κάποια προτυποποίηση ή καταμερισμός του χώρου.

Τέλος, ένα επιπλέον σενάριο που δοκιμάστηκε επιτυχώς ήταν ο διαχωρισμός της IPv4 και IPv6 κίνησης στο output και η εισαγωγή τους σε διαφορετικές ουρές προτεραιότητας.

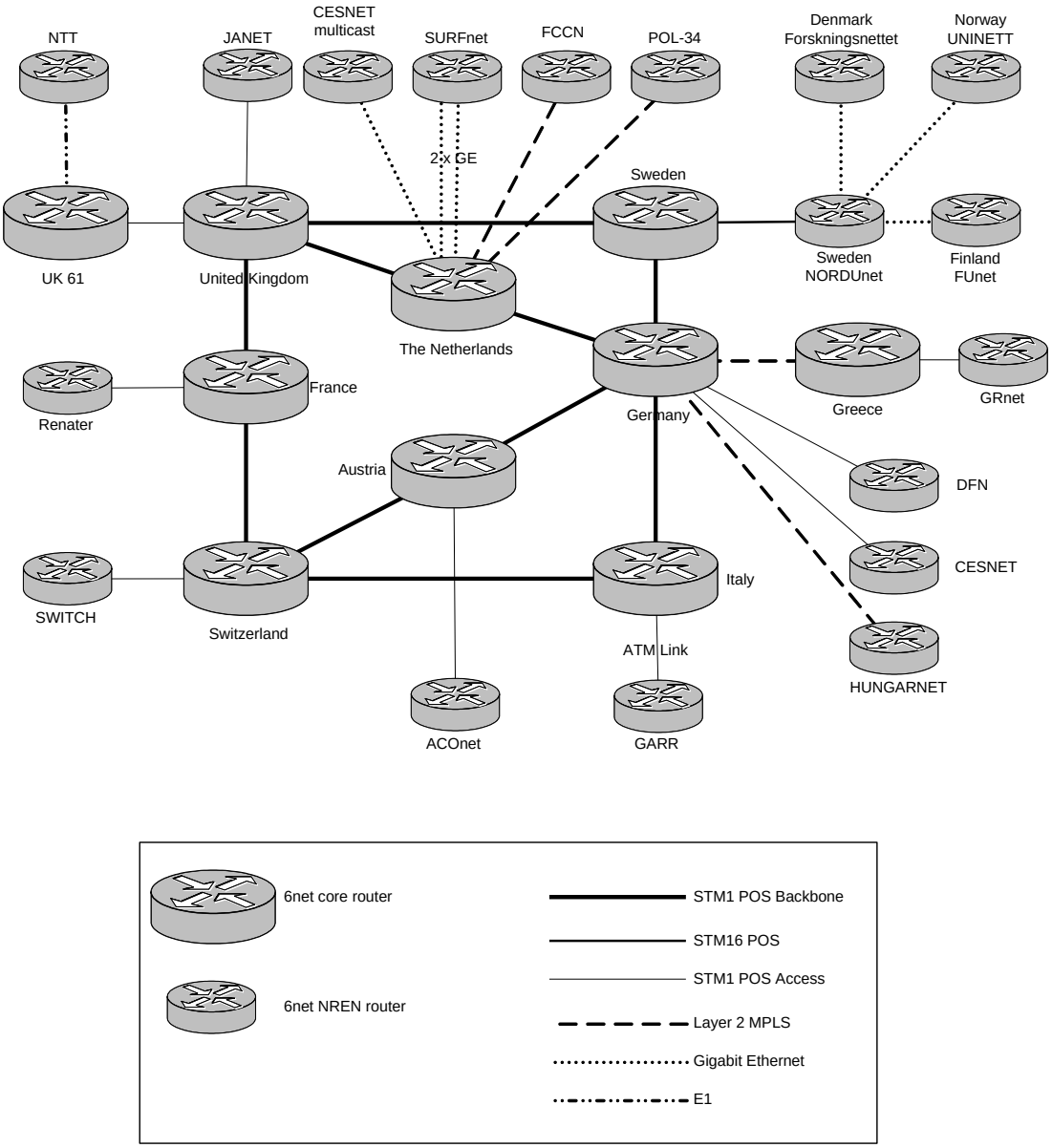
Συμπερασματικά, τα αποτελέσματα από τις δοκιμές συνοψίζονται στα ακόλουθα σημεία:

- Η υποστήριξη IPv6 switching στα μηχανήματα αυτά τα επιβαρύνει ελαφρώς όσον αφορά το CPU load.
- Οι fast Ethernet κάρτες υποστηρίζουν line rate switching τόσο για IPv4 και IPv6 κίνηση. Μόνη παραφωνία αποτελεί η δοκιμή κίνησης με πακέτα πολύ μικρού μεγέθους (π.χ. 128 bytes), όπου ο δρομολογητής επιβαρύνεται σημαντικά και η απόκρισή του γίνεται πολύ κακή. Επιπλέον, όταν ο φόρτος της κίνησης αυτής είναι ίσος ή μεγαλύτερος των 100Mbps (χωρητικότητα του FastEthernet), τότε ο δρομολογητής γίνεται εντελώς ασταθής και αρνείται κάθε υπηρεσία.
- Οι βασικοί QoS μηχανισμοί υποστηρίζονται αποδοτικά τόσο για IPv4 όσο και για IPv6 κίνηση χωρίς κάποια σημαντική διαφοροποίηση μεταξύ τους.
- Η χρήση του πεδίου flow label δοκιμάστηκε επιτυχώς σε σενάρια εξειδικευμένου classification για εφαρμογή ανεξάρτητου policing. Η χρήση του πεδίου flow label είναι δυνατή μόνο μέσω IPv6 ACL καθώς δεν διατίθεται σαν matching κριτήριο σε class-maps. Η χρήση του στο μέλλον ίσως είναι σημαντική, αλλά ακόμη η

προτυποποίησή του είναι ελλιπής καθώς υπάρχει απλά ένα γενικό RFC με βασικές οδηγίες χρήσης, επαναχρησιμοποίησης τιμών και ασφάλειας.

6.2.3 Πειράματα σε δίκτυο native IPv6 only

Στην ενότητα αυτή περιγράφεται η υλοποίηση και η δοκιμή μιας αντίστοιχης QoS υπηρεσίας αλλά αυτή τη φορά σε IPv6 δίκτυο μεγάλης κλίμακας (που αποτελεί μια μίξη δρομολογητών που εκτελούν IPv6 switching software & hardware based). Η υπηρεσία είναι και πάλι βασισμένη στην αρχιτεκτονική DiffServ (expedited forwarding) και παρέχει αυστηρές προτεραιότητες στα πακέτα που παράγονται από εφαρμογές πραγματικού χρόνου.

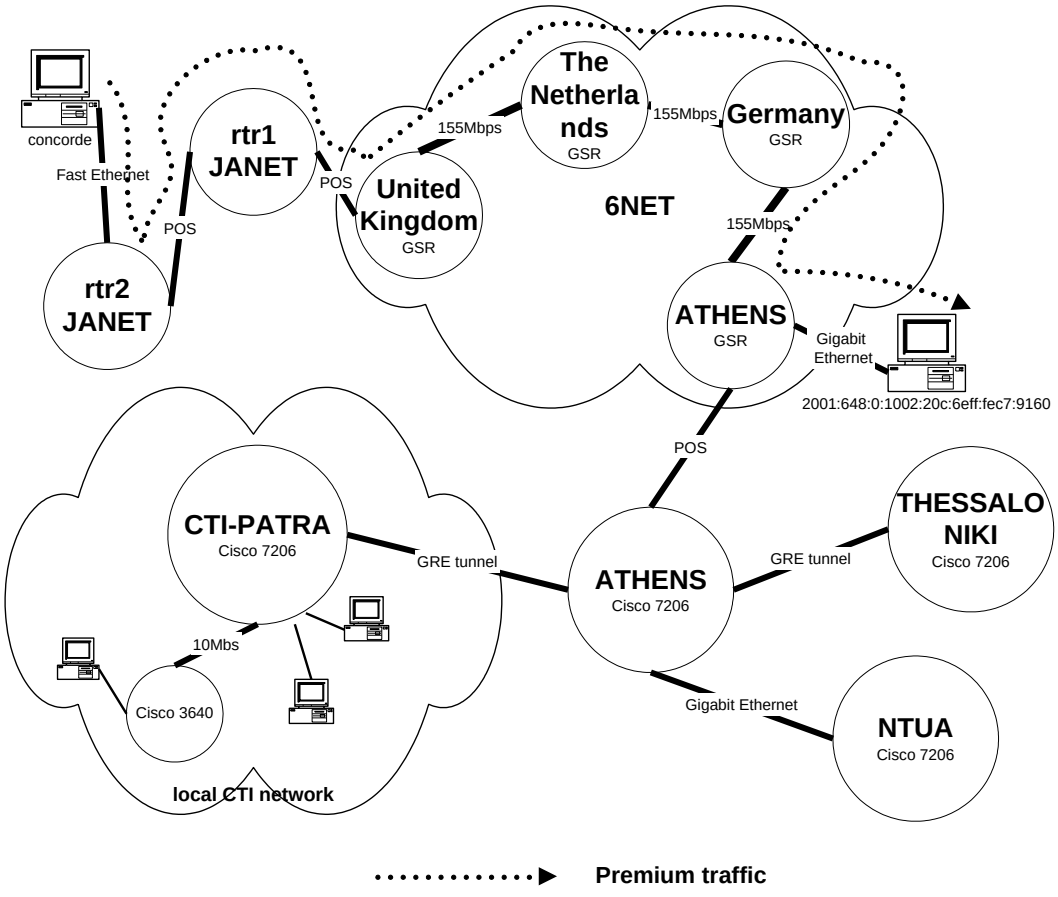


Εικόνα 43: Το backbone δίκτυο του 6NET

Η υπηρεσία εφαρμόστηκε στο backbone του πανευρωπαϊκού δικτύου 6NET, το οποίο φαίνεται στην Εικόνα 43 [91]. Επίσης η Εικόνα 44 παρουσιάζει με μεγαλύτερη

λεπτομέρεια το τμήμα του testbed που χρησιμοποιήθηκε για τα πειράματα. Η QoS υπηρεσία λειτουργούσε με το να κατηγοριοποιεί τα πακέτα που ανήκουν σε καθορισμένες εφαρμογές (τυπικά εφαρμογές πραγματικού χρόνου) και να χρησιμοποιεί μια ουρά προτεραιότητας "priority queue" για αυτά. Το υπόλοιπο της κίνησης στους δρομολογητές μεταχειρίζεται ως συνήθως με την best–effort υπηρεσία.

Η υπηρεσία υλοποιήθηκε με το μηχανισμό Modified Deficit Round Robin (MDRR) και ακολουθεί την τυπική DiffServ αρχιτεκτονική. Για τα πειραματικά σενάρια χρησιμοποιήθηκε η γεννήτρια τεχνητής κίνησης Iperf. Η κίνηση παρασκηνίου (background) κατηγοριοποιήθηκε με τιμή για το πεδίο DSCP 0 (default) και μεταχειρίζεται ως best-effort. Επιπλέον εισαγάγαμε κίνηση προσκηνίου (foreground) που προσομοιώνει μία συνάθροιση (aggregate) κίνησης πραγματικού χρόνου. Η κίνηση αυτή ανάλογα με το πείραμα, ήταν είτε TCP είτε UDP, είτε ένα μείγμα τεχνητά παραγόμενης UDP κίνησης και RTP κίνησης που παρήγαγε μια εφαρμογή βασισμένη στη βιβλιοθήκη OpenH323, η οποία έχει γίνει συμβατή με το IPv6. Στις δικτυακές συσκευές εφαρμόστηκε ένας μηχανισμός μαρκαρίσματος προκειμένου να μαρκάρει τη background και τη foreground κίνηση. Συγκεκριμένα η background και η foreground κίνηση διαχωρίζονται με διαφορετικές access lists και μαρκάρονται με διαφορετικές DSCP τιμές, οι οποίες είναι αντίστοιχα η default (0) και η προκαθορισμένη τιμή για expedited forwarding (46). Τα output interfaces των δικτυακών συσκευών διαμορφώθηκαν ώστε να στέλνουν τα μαρκαρισμένα με DSCP 46 πακέτα με αυστηρή προτεραιότητα.



Εικόνα 44: Testbed μεγάλης κλίμακας

Το μαρκάρισμα των πακέτων γινόταν στο επίπεδο πρόσβασης (access) και η κίνηση με προτεραιότητα αστυνομευόταν στο 5% του συνολικού διαθέσιμου bandwidth, το οποίο αντιστοιχούσε σε περίπου 7.5Mbps για τα core links που είχαν συνολική χωρητικότητα 155Mbps στο φυσικό επίπεδο.

Για τους σκοπούς των πειραμάτων χρησιμοποιήθηκαν 3 PCs τοποθετημένα σε διάφορα σημεία στο δίκτυο. Η IP Premium κίνηση στο foreground παραγόταν από το Ηνωμένο Βασίλειο (δίκτυο JANET), δρομολογείτο μέσω Ολλανδίας και, και λαμβανόταν στην Ελλάδα. Επιπλέον, στα πειράματα όπου απαιτείτο η δημιουργία τεχνητής κίνησης background, ένα κατάλληλο PC-γεννήτρια κίνησης στην Ολλανδία έστελνε την παραγόμενη κίνηση μέσω Γερμανίας στην Ελλάδα.

Η μέτρηση των μετρικών για το δίκτυο και την απόδοση της υπηρεσίας γινόταν με τα εργαλεία στατιστικών του Iperf για την τεχνητή κίνηση που παρήγαγε. Τα στατιστικά παράγονταν στο server instance του Iperf traffic [100] και συμπεριελάμβαναν το μέσο throughput (ρυθμαπόδοση – ρυθμός μετάδοσης κίνησης) και τη μέση διακύμανση καθυστέρησης (jitter) για την UDP κίνηση, καθώς και το μέσο throughput για την TCP κίνηση. Το Iperf υπολογίζει το jitter χρησιμοποιώντας τον ορισμό του RFC 3550 που ορίζει το jitter ως εξής:

$$J_i = J_{i-1} + (| D(i-1,i) | - J_{i-1}) / 16$$

όπου D(i,j) είναι η διαφορά του διαστήματος μεταξύ δύο διαδοχικών αφίξεων πακέτων στον αποδέκτη από το διάστημα μεταξύ δύο διαδοχικών πακέτων στον αποστολέα, και ορίζεται ως

$$D(i,j) = (R_j – R_i) – (S_j – S_i)$$

Ένα άλλο εργαλείο ήταν τα στατιστικά από το RTCP τα οποία παρείχε το εργαλείο τηλεδιάσκεψης που χρησιμοποιήθηκε ως εφαρμογή πραγματικού χρόνου, καθώς και τέλος τα αποτελέσματα από το Ethereal Network Protocol Analyzer που έπιανε όλα τα πακέτα στον αποδέκτη και μας παρείχε γραφικές αναπαραστάσεις του throughput.

Με την υποδομή αυτή δοκιμάσαμε αρχικά τους μηχανισμούς προτεραιότητας (prioritization) και κατηγοριοποίησης (classification), κατόπιν πραγματοποιήσαμε πιο περίπλοκες δοκιμές και τέλος εφαρμόσαμε όλους τους μηχανισμούς ταυτόχρονα δοκιμάζοντας την QoS με πραγματικού χρόνου δεδομένα.

6.2.3.1 Διερεύνηση του μηχανισμού prioritization

Ο μηχανισμός κατηγοριοποίησης (classification) υλοποιήθηκε με access lists και δημιουργώντας μια κλάση αστυνόμευσης (policing class) στο input interface του δρομολογητή. Ανάλογα με την ipv6 access list στην οποία ανήκουν τα πακέτα, η policy class αναθέτει τις τιμές DSCP: ef (46) για τη foreground κίνηση και default (0) για τη background. Κατόπιν, στο output interface του δρομολογητή, ορίστηκε μια δεύτερη policy class που δίνει αυστηρή προτεραιότητα στα πακέτα που έχουν μαρκαριστεί με την κατάλληλη DSCP τιμή για EF.

Σε πρώτο στάδιο επιβεβαιώθηκε η ορθή λειτουργία των μηχανισμών μαρκαρίσματος (marking), αστυνόμευσης (policing) και διαμόρφωσης (shaping), και κατόπιν πραγματοποιήθηκαν ένας αριθμός από σενάρια που συμπεριελάμβαναν ταυτόχρονη UDP και TCP background κίνηση, ενώ η foreground κίνηση εναλλασσόταν μεταξύ των 2 αυτών πρωτοκόλλων. Προκειμένου να επιβεβαιωθεί ότι το μαρκάρισμα με την DSCP τιμή 46 (IP Premium traffic) οδηγούσε όντως σε προνομιακή μεταχείριση της κίνησης, προκαλέσαμε τεχνητή συμφόρηση στο δίκτυο με την εισαγωγή 200 Mbps

background UDP κίνησης. Όπως δείχνει ο Πίνακας 7, ενώ η γενική κίνηση είχε πολύ μεγάλες απώλειες (περίπου τα μισά μεταδιδόμενα πακέτα της background κίνησης χάνονταν), η IP Premium μαρκαρισμένη κίνηση διαπερνούσε άνετα το δίκτυο παρά τη συμφόρηση χωρίς καθόλου απώλειες.

	Throughput (Mbps)	**Jitter (ms)**	**Ποσοστό απώλειας πακέτων (%)**
UDP foreground	5.11	4.1780	0.082
UDP background	105.00	0.1430	49.000

Πίνακας 7: Σύγκριση premium με best-effort κίνηση σε συνθήκες συμφόρησης

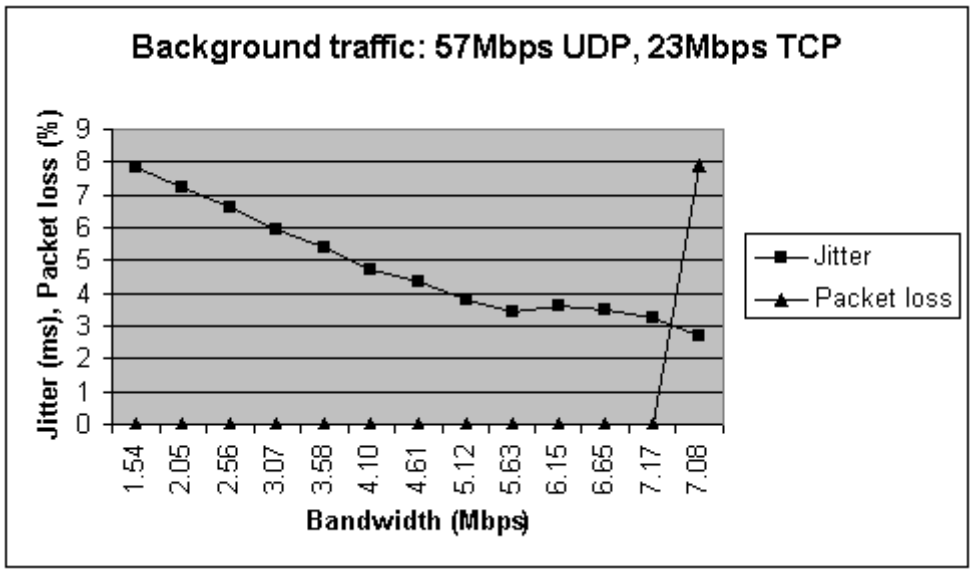
6.2.3.2 Σενάρια μεγάλης κλίμακας

Ο Πίνακας 8 δείχνει τις προδιαγραφές για κάθε σενάριο. Έχουν σχεδιαστεί ώστε να διερευνηθεί η αποδοτικότητα και τα χαρακτηριστικά των υλοποιημένων QoS μηχανισμών προκειμένου να υπάρχει μετρήσιμη βελτίωση σε διάφορους τύπους κίνησης που έχει μαρκαριστεί ως premium κίνηση. Για την όσο το δυνατόν ακριβέστερη προσομοίωση πραγματικών δικτυακών συνθηκών, τα σενάρια περιλαμβάνουν συνδυασμούς UDP, TCP ή και των δύο τύπων κίνησης στο background (best-effort κίνηση). Η αναλογία είναι 30% TCP και 70% UDP, προκειμένου να προσομοιωθεί ένα πραγματικό περιβάλλον με μεγάλο αριθμό UDP εφαρμογών με μεγάλη κατανάλωση bandwidth, και έναν επίσης σημαντικό αριθμό TCP εφαρμογών (όπως web browsing).

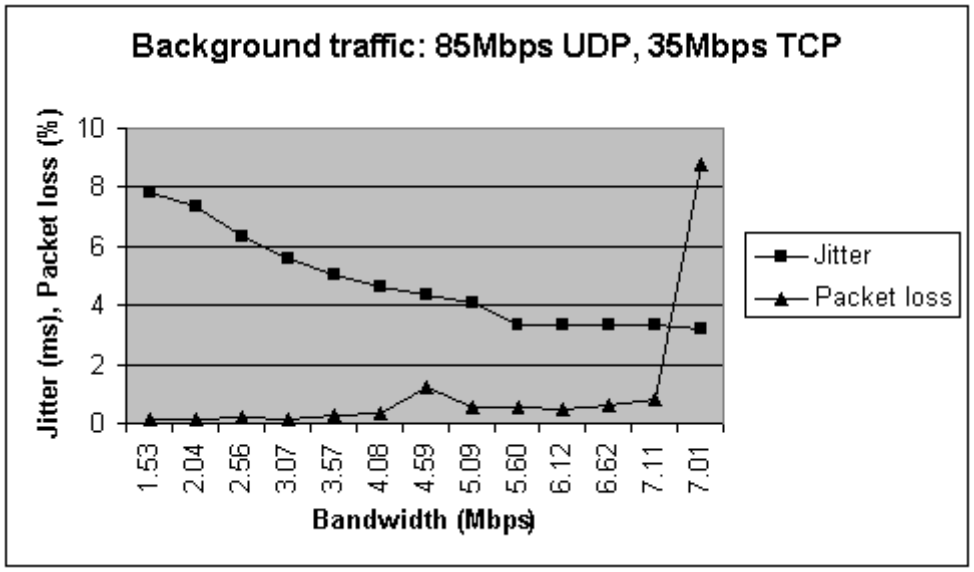
Σενάριο	**Background**	**Foreground**
1	50Mbps (30% TCP- 70% UDP)	UDP traffic (1.5Mbps)
2	50Mbps (30% TCP- 70% UDP)	TCP traffic (1.5Mbps)
3	80Mbps (30% TCP- 70% UDP)	UDP traffic (1.5Mbps)
4	80Mbps (30% TCP- 70% UDP)	TCP traffic (1.5Mbps)
5	120Mbps (30% TCP- 70% UDP)	UDP traffic (1.5Mbps)
6	120Mbps (30% TCP- 70% UDP)	TCP traffic (1.5Mbps)
7	80Mbps (30% TCP- 70% UDP)	UDP traffic >1.5Mbps)
8	80Mbps (30% TCP- 70% UDP)	TCP traffic > 1.5Mbps)
9	120Mbps (30% TCP- 70% UDP)	UDP traffic > 1.5Mbps)
10	120Mbps (30% TCP- 70% UDP)	TCP traffic > 1.5Mbps)

Πίνακας 8: Σενάρια μεγάλης κλίμακας

Τα αποτελέσματα από τα σενάρια 7 και 9 τα οποία αποτελούνται από πολλαπλές δοκιμές, παρουσιάζονται γραφικά στις Εικόνα 45 και Εικόνα 46 αντίστοιχα.



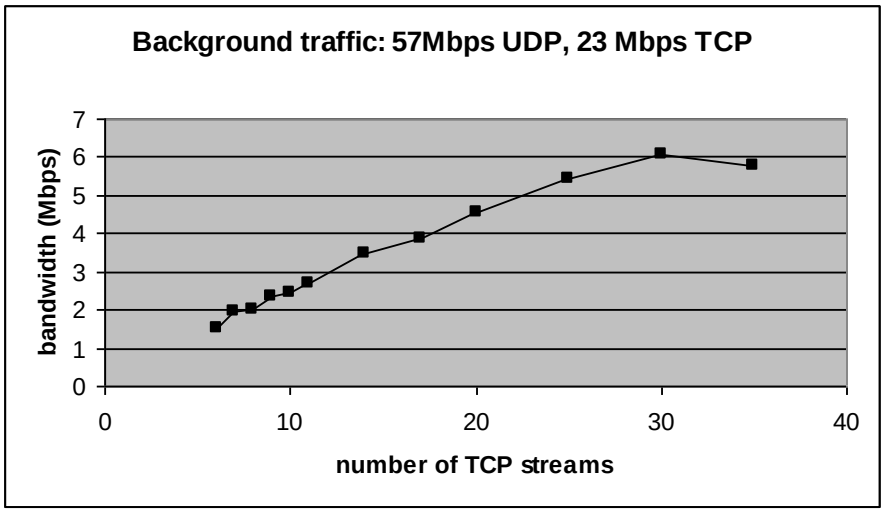
Εικόνα 45: UDP foreground με 80Mbps background κίνηση



Εικόνα 46: UDP foreground με 120Mbps background κίνηση

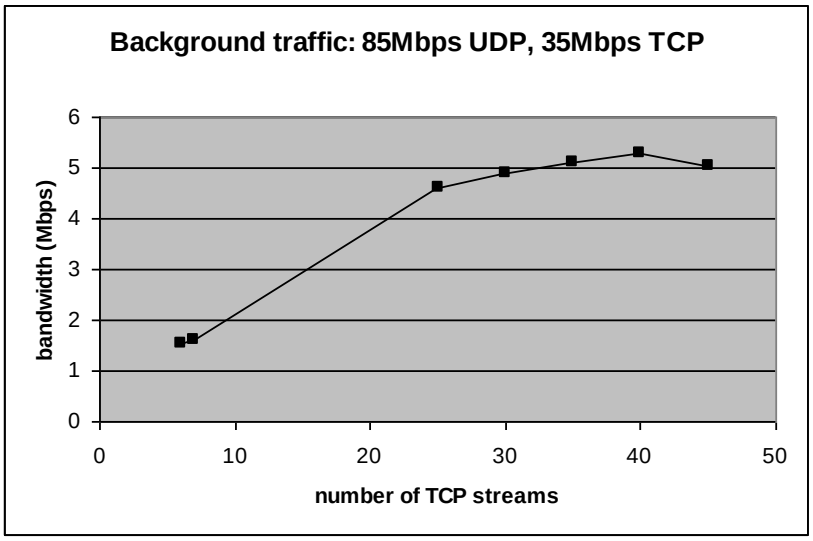
Στις Εικόνα 45 και Εικόνα 46 φαίνεται η αποδοτικότητα του μηχανισμού αστυνόμευσης, ο οποίος εφαρμόστηκε στο input interface για την premium κίνηση. Η διαμόρφωση του μηχανισμού αστυνόμευσης έγινε χρησιμοποιώντας την επιλογή της πλήρους απόρριψης τυχόν επιπλέον πακέτων (αντί της εναλλακτικής επιλογής που θα ήταν τα επιπλέον πακέτα να μεταχειρίζονται ως best-effort κίνηση). Επομένως, μόλις η foreground κίνηση ξεπερνούσε το αποδοθέν σε αυτήν bandwidth (5% του συνολικά διαθέσιμου bandwidth ή περίπου 7.5 Mbps στο φυσικό επίπεδο), οι απώλειες πακέτων αυξάνονταν δραματικά. Η επιλογή αυτή είναι πιο κατάλληλη για εφαρμογές πραγματικού χρόνου, καθώς για αυτόν τον τύπο εφαρμογής ο κατάλληλος συγχρονισμός στην λήψη των πακέτων είναι πιο σημαντικός από την καθυστερημένη παράδοση. Σε τέτοια περίπτωση, τα καθυστερημένα πακέτα είναι άχρηστα εάν η σχετική πληροφορία έπρεπε να είχε ήδη παρουσιαστεί στον χρήστη.

Μία άλλη ενδιαφέρουσα παρατήρηση είναι ότι το jitter για τη foreground κίνηση αυξάνει σταθερά καθώς αυξάνεται ο ρυθμός μετάδοσης. Αυτό εξηγείται αν ληφθεί υπόψη ο τρόπος υπολογισμού του jitter. Ένας υψηλότερος ρυθμός μετάδοσης οδηγεί τα πακέτα να φτάνουν στον προορισμό πιο κοντά το ένα στο άλλο, και άρα οι διαφοροποιήσεις στο χρόνο μεταξύ αφίξεων είναι μικρότερες (επομένως οι διαφορές αυτές μπορούν να γίνουν σταθερές αν ζυγιστούν με τους χρόνους μεταξύ διαδοχικών αφίξεων πακέτων).



Εικόνα 47: TCP foreground με 80Mbps background κίνηση

Στις Εικόνα 47 και Εικόνα 48 συνοψίζονται τα αποτελέσματα για την TCP foreground κίνηση για τα σενάρια 8 και 10 αντίστοιχα, όπου αυξανόταν σταδιακά ο ρυθμός μετάδοσης για την TCP foreground κίνηση. Όταν ο ρυθμός μετάδοσης πλησίασε στο κατώφλι του δοθέντος bandwidth, ο ρυθμός μετάδοσης δεν μπορούσε πλέον να αυξηθεί, εφόσον ο μηχανισμός αστυνόμευσης απέρριπτε τα επιπλέον πακέτα και ο μηχανισμός αποφυγής συμφόρησης του TCP χρησιμοποιούσε την πληροφορία αυτή για να μειώσει το ρυθμό μετάδοσης.



Εικόνα 48: TCP foreground με 120Mbps background κίνηση

6.3 ΑΠΑΡΑΙΤΗΤΕΣ ΕΠΕΚΤΑΣΕΙΣ ΤΟΥ BANDWIDTH BROKER ΓΙΑ ΥΠΟΣΤΗΡΙΞΗ IPv6 QoS

Από τα παραπάνω πειράματα – δοκιμές των QoS μηχανισμών για IPv6 κίνηση είναι προφανές πως μπορούν να υποστηριχτούν οι παραπάνω υπηρεσίες και για IPv6 κίνηση. Προκειμένου όμως να επιτευχθεί αυτό πρέπει να γίνουν οι ακόλουθες αλλαγές:

- Το μαρκάρισμα στην IPv6 κίνηση πρέπει να γίνει με βάση το πεδίο "Traffic Class-TC
- Η περιγραφή του traffic class για κάθε αίτημα IP premium υπηρεσίας πρέπει να βασίζεται σε ipv6 extended ACL
- Αν υποστηριχτούν IP Premium αιτήματα που το traffic class περιέχει μίξη IPv4 και IPv6 κίνησης τότε απαιτούνται πολλαπλές περιγραφές traffic class
- Στο network management interface πρέπει να γίνει πλήρης μοντελοποίηση των γραμμών που μεταφέρουν IPv6 κίνηση. Επιπλέον απαιτείται συσχέτιση των interfaces στη Βάση Δεδομένων με IPv4 only, IPv6 only ή και τα 2.
- Στο interface χρήστη απαιτείται κατάλληλη αλλαγή της φόρμας υποβολής αιτήματος ώστε να διακρίνεται αν ο χρήστης υποβάλει IPv4 QoS αίτημα ή IPv6 ή μεικτό αίτημα.
- Στον policy manager απαιτείται ενσωμάτωση αλλαγών στο configuration ώστε να παράγεται αυτόματα και για τα IPv6 QoS αιτήματα. Επιπλέον χρειάζεται και κατάλληλη αλλαγή του μηχανισμού ελέγχου του υλοποιημένου configuration (όπως αποθηκεύεται στο network management interface) και αντιστοίχησή του με τα ενεργά αιτήματα της υπηρεσίας.

ΚΕΦΑΛΑΙΟ 7: ΜΕΛΕΤΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ BANDWIDTH BROKER ΜΕ ΕΞΟΜΟΙΩΣΗ

ΜΕΛΕΤΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΜΗΧΑΝΙΣΜΩΝ BANDWIDTH BROKER ΜΕ ΕΞΟΜΟΙΩΣΗ

7.1 ΕΙΣΑΓΩΓΗ

Προκειμένου να αξιολογηθεί πειραματικά η συμπεριφορά των προτεινόμενων μηχανισμών χρησιμοποιήσαμε δύο συστήματα προσομοίωσης. Το ένα είναι ο γνωστός δικτυακός προσομοιωτής ns-2, ο οποίος χρησιμοποιήθηκε για την πιο ρεαλιστική μελέτη των αρχιτεκτονικών σε επίπεδο πακέτων. Το δεύτερο σύστημα (το οποίο μελετάται στο επόμενο κεφάλαιο) αποτελεί αλγοριθμικές εξομοιώσεις σε Java. Είναι γρήγορο και αποδοτικό, αλλά μένει σε υψηλό επίπεδο μελέτης των μηχανισμών, για αυτό και τα πειράματα συμπληρώθηκαν με την υλοποίηση των αντίστοιχων λειτουργικοτήτων στα πλαίσια του ns-2. Το περιβάλλον του ns-2 υλοποιήθηκε και έτρεξε σε ένα μηχάνημα βασισμένο σε αρχιτεκτονική Intel PC με λειτουργικό σύστημα Linux, 256 MB κύριας μνήμης (RAM) και επεξεργαστή Pentium III, ο οποίος λειτουργεί στα 700MHz.

7.2 Ο ΕΞΟΜΟΙΩΤΗΣ NS-2

Η υλοποίηση του Bandwidth Broker έγινε στον προσομοιωτή Network Simulator ns-2 [107]. Ο ns-2 είναι ένας προσομοιωτής ανοιχτού κώδικα. Ο ns ξεκίνησε το 1989 ως μια παραλλαγή του Real network simulator και το 1995 η ανάπτυξή του υποστηρίχτηκε από την DARPA μέσα από το έργο VINT. Το VINT είναι ένα έργο στο οποίο συνεργάζονται οι εταιρίες USC/ISI, Xerox PARC, LBNL και το πανεπιστήμιο Berkeley της California. Σήμερα η υποστήριξη του ns γίνεται από την DARPA μέσα από το SAMAN και από την NSF μέσα από το CONSER. Ο ns βγαίνει σε διάφορες εκδόσεις για διάφορα λειτουργικά συστήματα όπως τα FreeBSD, Linux, SunOS, Solaris και Windows. Η τελευταία του έκδοση είναι η 2.29.

Ο ns-2 είναι ένα πολύ ισχυρό περιβάλλον εξομοίωσης το οποίο μπορεί να εξομοιώσει πολλά είδη δικτύων, όπως ασύρματα και δορυφορικά δίκτυα. Ένας χρήστης μπορεί να ορίζει τυχαίες τοπολογίες δικτύων που αποτελούνται από κόμβους και συνδέσμους. Στη συνέχεια μπορεί να αναθέτει εφαρμογές σε κάθε κόμβο καθώς και ουρές για τους συνδέσμους. Ένας ερευνητής μπορεί να χρησιμοποιήσει τον ns-2 ώστε να σχεδιάσει νέα πρωτόκολλα, να ελέγξει την συμπεριφορά και την απόδοσή τους και να τα συγκρίνει με τα ήδη υπάρχοντα πρωτόκολλα. Ο ns-2 μπορεί να χρησιμοποιηθεί και για εκπαιδευτικούς σκοπούς διότι μπορεί να "οπτικοποιήσει" τα δίκτυα και τις συμπεριφορές των πρωτοκόλλων, όπως για παράδειγμα του TCP ή του UDP, σαν animations.

Ο ns-2 έχει γραφτεί σε C++ και χρησιμοποιεί την OTcl σαν γλώσσα εντολών και ρύθμισης των παραμέτρων. Ο ns-2 υποστηρίζει πάρα πολλά δικτυακά πρωτόκολλα, όπως τα TCP και UDP, πολλές πηγές κίνησης όπως FTP, Telnet, Web, CBR (Constant Bit Rate) και VBR (Variable Bit Rate), μηχανισμούς διαχείρισης ουρών όπως τους RED, DropTail και CBQ, αλγορίθμους δρομολόγησης όπως τους Dijkstra και Bellman-Ford. Επίσης, ο ns-2 υποστηρίζει σφάλματα της λειτουργίας του δικτύου, όπως ντετερμινιστικές και πιθανοτικές απώλειες πακέτων καθώς και link

failures. Ο ns-2 είναι ένας event-driven προσομοιωτής που δέχεται σαν είσοδο tcl scripts και τα εκτελεί. Η έξοδος μπορεί να έχει διάφορες μορφές, ακόμα και γραφική αναπαράσταση του δικτύου. Μια κοινή έξοδος μπορεί να είναι αρχεία τα οποία περιγράφουν με πληρότητα την κίνηση σε ένα σύνδεσμο ή την κατάσταση σε μια ουρά. Με την μετα-επεξεργασία αυτών των αρχείων μπορούν να υπολογιστούν ποσότητες όπως το throughput ή το jitter της κίνησης.

Η έκδοση του ns που χρησιμοποιήθηκε ήταν η ns-allinone-2.26. Αυτή η έκδοση περιείχε τον ns, έκδοση 2.26, τη γλώσσα OTcl καθώς και μερικά ακόμα πακέτα που προσθέτουν λειτουργικότητα. Τα σημαντικότερα από αυτά είναι:

- Το πακέτο nam. Το πακέτο nam δίνει τη δυνατότητα γραφικής αναπαράστασης του δικτύου και των πακέτων που μεταφέρονται μέσα σε αυτό.
- Το πακέτο xgraph. Αυτό το πακέτο χρησιμοποιείται για τη δημιουργία γραφικών παραστάσεων και είναι πολύ χρήσιμο κατά τη μετα-επεξεργασία της εξόδου. Για παράδειγμα μπορεί να αναπαραστήσει το throughput μιας εφαρμογής.
- Τη γλώσσα Perl. Η Perl μπορεί να χρησιμοποιηθεί για την περιγραφή πειραμάτων στον ns-2.
- Το πακέτο tcl-debug που χρησιμοποιείται για debugging.
- Τα πακέτα gt-itm και sgb. Το πακέτο gt-itm χρησιμοποιείται για τη δημιουργία διαφόρων τοπολογιών δικτύων. Το πακέτο sgb χρησιμοποιείται για τη μετατροπή της εξόδου του gt-itm σε μορφή συμβατή με αυτήν των τοπολογιών ns-2.
- Το πακέτο CWeb χρησιμοποιείται για τη δημιουργία ευανάγνωστων C και C++ προγραμμάτων.
- Το πακέτο Zlib χρησιμοποιείται για συμπίεση αρχείων.

Κατά την υλοποίηση του Bandwidth Broker χρησιμοποιήθηκε ιδιαίτερα το πακέτο diffserv του ns-2. Αυτό το πακέτο παρέχει αρκετούς DiffServ μηχανισμούς. Η DiffServ λειτουργία στον ns-2 μπορεί να υποστηρίξει τέσσερις κλάσεις κίνησης κάθε μία από τις οποίες έχει τρεις προτεραιότητες απόρριψης. Τα πακέτα που ανήκουν σε κάποια κλάση τοποθετούνται στην αντίστοιχη φυσική RED ουρά η οποία περιέχει τρεις ιδεατές ουρές, μία για κάθε προτεραιότητα απόρριψης. Το diffserv πακέτο του ns υλοποιεί τρεις κύριες λειτουργίες:

- Αστυνόμευση (policing)
- Λειτουργίες των edge routers, δηλαδή μαρκάρισμα (marking) των πακέτων
- Λειτουργίες των core routers, δηλαδή έλεγχο των code points των πακέτων και κατάλληλη προώθησή τους

Το πακέτο diffserv διαθέτει την κλάση dsREDQueue η οποία χρησιμοποιείται για τη δημιουργία και την διαχείριση ουρών που διαθέτουν τον μηχανισμό RED. Οι κλάσεις edgeQueue και coreQueue κληρονομούν την κλάση dsREDQueue και αντιστοιχούν στις ουρές των edge και core routers. Η αστυνόμευση υλοποιείται στην κλάση dsPolicy. Η αστυνόμευση γίνεται με βάση το ζεύγος πηγής-προορισμού. Όλες οι ροές που διαθέτουν κοινό ζεύγος πηγής προορισμού συνενώνονται σε ένα traffic aggregate. Για κάθε διαφορετικό traffic aggregate ορίζεται ένας τύπος αστυνόμευσης, οι παράμετροι του τύπου αστυνόμευσης καθώς και ένα μοναδικό code point. Οι μηχανισμοί αστυνόμευσης που έχουν υλοποιηθεί είναι οι:

- Time Sliding Window with 2 Color Marking
- Time Sliding Window with 3 Color Marking
- Token Bucket
- Single Rate Three Color Marker
- Two Rate Three Color Marker

Όλοι οι παραπάνω μηχανισμοί χρησιμοποιούν έναν αριθμό από προτεραιότητες απόρριψης και μια σειρά παραμέτρων όπως η μέγιστη επιτρεπτή συχνότητα μετάδοσης και το μέγιστο μέγεθος καταιγισμού.

Όσον αφορά τη χρονοδρομολόγηση στις ουρές, ο ns-2 διαθέτει τους μηχανισμούς Priority Queueing, Round Robin, Weighted Round Robin, Weighted Interleaved Round Robin και Deficit Round Robin. Ο προεπιλεγμένος μηχανισμός είναι ο Round Robin.

Ο προσομοιωτής ns-2 ανανεώνεται πολύ συχνά και πολλοί άνθρωποι σε όλο τον κόσμο τον υποστηρίζουν είτε με το να διορθώνουν bugs είτε με το να γράφουν νέο κώδικα που προσθέτει λειτουργικότητα στον ns-2. Η επιστημονική κοινότητα τον χρησιμοποιεί ευρύτατα καθώς είναι ένα πολύ ισχυρό και εύκολο στη χρήση περιβάλλον εξομοίωσης.

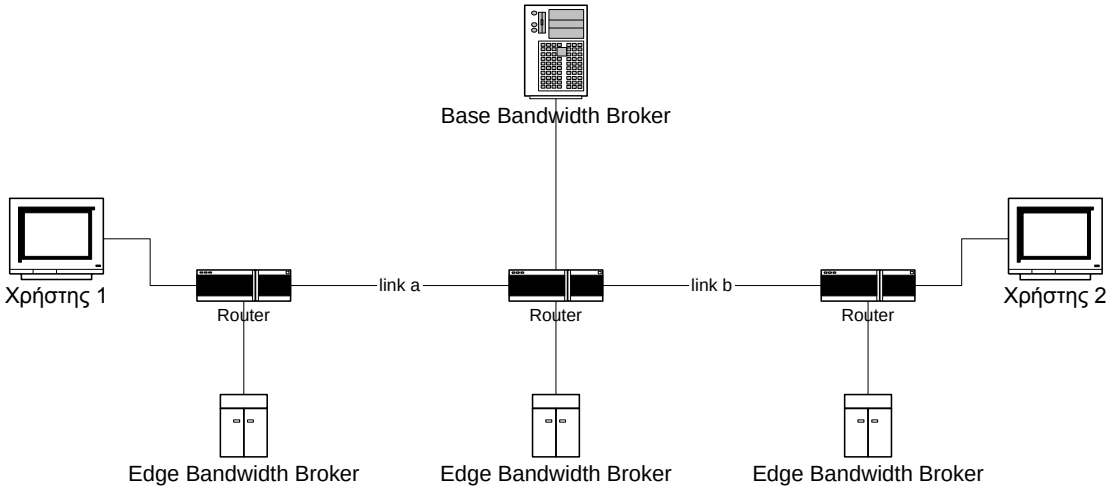
7.3 Η ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΤΩΝ BANDWIDTH BROKER

Οι bandwidth broker που υλοποιήθηκαν στηρίζονται σε agents, τον base bandwidth broker και τον edge bandwidth broker. Σε κάθε κόμβο του δικτύου ανατίθεται ένας edge bandwidth broker. Ο base bandwidth broker ανατίθεται μόνο σε έναν κόμβο. Σε αυτόν τον κόμβο μπορεί να τρέχει και κάποιος edge bandwidth broker ή μπορεί να είναι ένας επιπλέον κόμβος ο οποίος να συνδέεται με όλους τους άλλους κόμβους του δικτύου.

Τέσσερις διαφορετικοί bandwidth brokers υλοποιήθηκαν:

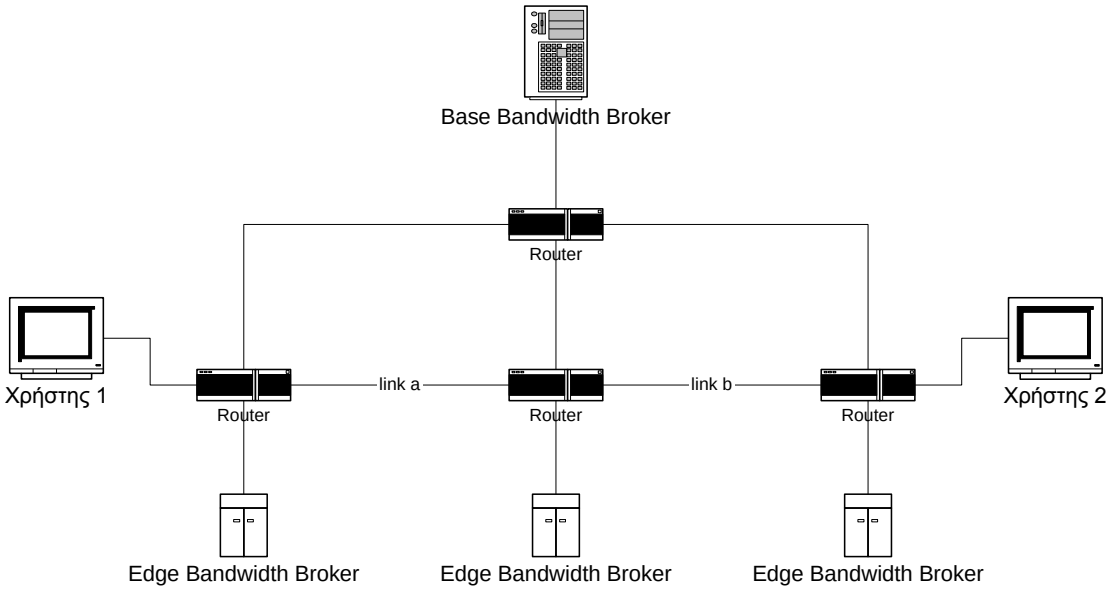
- Serial Distributed Bandwidth Broker model (SDBB model)
- Parallel Distributed Bandwidth Broker model (PDBB model)
- Centralized Bandwidth Broker model (CBB model)
- Centralized Fault-tolerant Bandwidth Broker model (CFBB model)

Ο base bandwidth broker εκτελεί διαφορετική λειτουργία ανάλογα με το μοντέλο ενώ ο edge bandwidth broker είναι κοινός σε όλα τα μοντέλα.



Εικόνα 49: Το δίκτυο αποτελείται από τρεις κόμβους, σε κάθε έναν ανατίθεται και ένας Edge Bandwidth Broker και σε οποιοδήποτε από αυτούς τους κόμβους μπορεί να τοποθετηθεί και ο Base Bandwidth Broker

Τα κοινά στοιχεία των base bandwidth broker είναι ότι όλοι, ανεξαρτήτως αρχιτεκτονικής, συνδέονται με όλους τους edge bandwidth brokers. Η λειτουργία του συστήματος γίνεται με χρήση μηνυμάτων τα οποία πάντα αποστέλλονται είτε από κάποιον edge bandwidth broker προς τον base bandwidth broker, είτε από τον base bandwidth broker προς κάποιον από τους edge bandwidth brokers. Ποτέ δηλαδή δεν επικοινωνούν δύο edge bandwidth brokers στέλνοντας μηνύματα μεταξύ τους. Στην επικοινωνία πάντα παρεμβάλλεται ο base bandwidth broker.



Εικόνα 50: Σε κάθε κόμβο τρέχει ένας Edge Bandwidth Broker ενώ έχει προστεθεί και ένας επιπλέον κόμβος (ο ανώτερος κόμβος) στον οποίο τρέχει ο Base Bandwidth Broker.

Η λειτουργία του συστήματος ξεκινά όταν κάποιος από τους edge bandwidth brokers κάνει ένα αίτημα ζητώντας εγγυημένο bandwidth x bytes για ένα συγκεκριμένο

χρονικό διάστημα από τον κόμβο στον οποίο τρέχει ως κάποιον άλλο κόμβο του δικτύου.

Εάν ο base bandwidth broker εξυπηρετεί εκείνη τη στιγμή κάποιο άλλο αίτημα θα έχουμε διαφορετική αντιμετώπιση ανάλογα με την αρχιτεκτονική.

Στο CBB και στο CFBB μοντέλο στέλνει απάντηση ειδοποίησης μη διαθεσιμότητας στον συγκεκριμένο edge bandwidth broker. Αλλιώς, ξεκινά την εξυπηρέτηση του αιτήματος. Επειδή όμως η απόκριση των base agents ήταν άμεση ανεξαρτήτως του αριθμού των αιτημάτων που έφταναν, προέκυψε η περίπτωση απόρριψης αιτημάτων σε πολύ μικρό ποσοστό.

Αντίθετα στο SDBB και στο PDBB μοντέλο επειδή η απόρριψη ήταν μεγάλη λόγω μη διαθεσιμότητας του Base agent, υλοποιήθηκε ένα buffer στο οποίο αποθηκεύονται με σειριακό τρόπο τα αιτήματα που δεν μπορούσαν να εξυπηρετηθούν. Μόλις το αίτημα έβγαινε από το buffer , ελέγχονταν αν η έναρξη του αιτήματος δεν είχε έρθει ακόμη και αν δεν είχε έρθει όντως, ο base το επεξεργάζονταν. Διαφορετικά απορρίπτονταν.

Όταν ο base bandwidth broker εξυπηρετεί ένα αίτημα, ελέγχει αν υπάρχει διαθέσιμο bandwidth από τον κόμβο στον οποίο τρέχει ο edge bandwidth broker που έκανε το αίτημα μέχρι τον άλλο τελικό κόμβο για το συγκεκριμένο χρονικό διάστημα.

Ανάλογα με το μοντέλο η πληροφορία για το διαθέσιμο bandwidth βρίσκεται είτε στους edge είτε στους ίδιους τους base agents

Στα SDBB, PDBB και CFBB μοντέλα κάθε edge bandwidth broker διατηρεί πληροφορία για το διαθέσιμο bandwidth μεταξύ του κόμβου στον οποίο τρέχει και όλων των γειτονικών του κόμβων. Ο base bandwidth broker βρίσκει από τα routing tables το next hop n_1 από τον κόμβο n_0 που έκανε το αίτημα ως τον άλλο τελικό κόμβο n_k.

Στο πρώτο μοντέλο, στέλνει ερώτημα στον edge bandwidth broker που τρέχει στον κόμβο n_0 για το αν υπάρχει διαθέσιμο bandwidth μεταξύ των κόμβων n_0 και n_1. Αν η απάντηση είναι θετική, ο base bandwidth broker υπολογίζει το next hop n_2 από τον n_1 ως τον n_k και στέλνει στον n_1 ερώτημα για το αν υπάρχει διαθέσιμο bandwidth μεταξύ των κόμβων n_1 και n_2. Αν όλες οι απαντήσεις είναι θετικές, αυτή η διαδικασία συνεχίζεται ως ότου φτάσουμε στον κόμβο n_k. Αυτό θα σημαίνει ότι το διαθέσιμο bandwidth από τον n_0 ως τον n_k υπάρχει. Ο base bandwidth broker τότε θα στείλει θετική απάντηση στον edge bandwidth broker που έκανε αρχικά το αίτημα. Η διαδικασία θα ολοκληρωθεί με την αποστολή από τον base bandwidth broker μηνυμάτων προς όλους τους edge bandwidth brokers που βρίσκονται στο μονοπάτι $n_0,n_1,\ldots,n_k$ τα οποία θα τους ειδοποιούν να μειώσουν το διαθέσιμο bandwidth κατά x bytes στα links τα οποία βρίσκονται στο μονοπάτι. Στην περίπτωση που κάποιος από τους edge bandwidth brokers στείλει αρνητική απάντηση διότι δεν υπάρχει διαθέσιμο bandwidth σε κάποιο link, ο base bandwidth broker στέλνει αρνητική απάντηση στον κόμβο από τον οποίο έγινε το αρχικό αίτημα και η διαδικασία τελειώνει εκεί.

Στο PDBB μοντέλο η ερώτηση στους edge agents γίνεται ταυτόχρονα σε όλους. Αν στείλει κάποιος αρνητική απάντηση καθώς ο base agent περιμένει τις απαντήσεις, τότε η επεξεργασία του αιτήματος σταματά, στέλνεται αρνητική απάντηση στον αιτούντα και συνεχίζει την επεξεργασία του επόμενου αιτήματος. Διαφορετικά αν παίρνει θετικές απαντήσεις, περιμένει να του απαντήσουν όλοι οι agents τους οποίους ρώτησε. Αν λάβει από όλους θετική απάντηση ακολουθείται η διαδικασία που έγινε και παραπάνω.

Στο CFBB μοντέλο η πληροφορία είναι αποθηκευμένη και στα δύο σημεία, στους edge agents και στο ίδιο τον base agent. Όταν έρχεται το αίτημα, ο base agent ρωτά την βάση του και αν πάρει θετική απάντηση, αλλάζει τα δεδομένα της, αλλάζει και τα δεδομένα στους edge agents και στέλνει θετική απάντηση στον αιτούντα. Εάν πάρει αρνητική απάντηση, απλά την στέλνει πίσω στον αιτούντα.

Τέλος στο CBB μοντέλο όλη η πληροφορία βρίσκεται στο base agent. Όταν παίρνει ένα αίτημα ρωτά τη βάση του, που έχει όλη την πληροφορία για την κατάσταση του δικτύου που ελέγχει. Αν πάρει θετική απάντηση, αλλάζει τα δεδομένα της βάση του και στέλνει θετική απάντηση στον αιτούντα ενώ διαφορετικά στέλνει αρνητική και προχωρά στην επεξεργασία του επόμενου αιτήματος.

Η κατανομή των πόρων ώστε να παρέχονται εγγυήσεις για το bandwidth γίνεται χρησιμοποιώντας την DiffServ αρχιτεκτονική. Ο base bandwidth broker όταν στέλνει στον edge bandwidth broker μια θετική απάντηση, στο ίδιο μήνυμα στέλνει και το DSCP που πρέπει να φέρουν τα πακέτα της εφαρμογής η οποία θα χρησιμοποιεί το δεσμευμένο bandwidth. Προηγουμένως έχει κάνει configure όλους τους δρομολογητές του δικτύου ώστε να προσφέρουν εγγυήσεις στην εφαρμογή που έκανε το αίτημα για το ζητούμενο bandwidth, με βάση το DSCP.

7.4 ΟΙ AGENTS BBEDGE, BBBASE, CENTRALBBBASE, DISTRIBUTEDBBBASE

Οι agents base bandwidth broker και edge bandwidth broker οι οποίοι αναφέρθηκαν στην περιγραφή της λειτουργίας του συστήματος υλοποιήθηκαν με τα ονόματα BBbase, CentralBBbase, DistributedBBbase και BBedge αντίστοιχα.

Η κλάση BBbaseAgent κληρονομεί τις ιδιότητες της κλάσης Agent. Η κλάση BBbaseAgent έχει τρεις public συναρτήσεις-μέλη και μια protected μεταβλητή-μέλος. Συγκεκριμένα ορίζονται:

- ο constructor της κλάσης
- η συνάρτηση-μέλος command που χρησιμοποιείται για να μπορούν να δοθούν στον agent εντολές μέσω tcl
- η συνάρτηση-μέλος recv χρησιμοποιείται για να καθοριστεί η διαδικασία που θα ακολουθηθεί με την παραλαβή του κάθε πακέτου
- η δυαδική μεταβλητή-μέλος available που χρησιμοποιείται για να δείξει εάν ο base bandwidth broker είναι διαθέσιμος ή εξυπηρετεί ήδη κάποιο αίτημα για bandwidth
- η δυαδική μεταβλητή-μέλος cur_dscp χρησιμοποιείται για να διατηρεί ο base bandwidth broker πληροφορία για το τρέχον διαθέσιμο DSCP που θα ανατεθεί σε κάποια ροή μετά από μια θετική απάντηση από τον έλεγχο αποδοχής.

Όταν δημιουργείται ένας BBbaseAgent χρειάζεται η μεταβλητή-μέλος available να γίνει TRUE αφού ο BBbaseAgent είναι αρχικά διαθέσιμος. Η άλλη μεταβλητή-μέλος cur_dscp χρειάζεται να γίνει 2 αφού αυτό είναι το αρχικό διαθέσιμο DSCP. Αυτές οι αναθέσεις γίνονται στον constructor της κλάσης.

Και η κλάση BBedgeAgent κληρονομεί τις ιδιότητες της κλάσης Agent. Η κλάση BBedgeAgent έχει τέσσερις public συναρτήσεις-μέλη και μια protected μεταβλητή-μέλος. Συγκεκριμένα, ορίζονται:

- ο constructor της κλάσης
- η συνάρτηση-μέλος command χρησιμοποιείται για να μπορούν να δοθούν στον agent εντολές μέσω tcl
- η συνάρτηση-μέλος recv χρησιμοποιείται για να καθοριστεί η διαδικασία που θα ακολουθηθεί με την παραλαβή του κάθε πακέτου
- η συνάρτηση sendto η οποία χρησιμοποιείται για την αποστολή αιτήματος για bandwidth
- η μεταβλητή-μέλος nghbr_list χρησιμοποιείται για να διατηρείται σε κάθε BBedgeAgent πληροφορία για το διαθέσιμο bandwidth μεταξύ του κόμβου στον οποίο τρέχει ο BBedgeAgent και των γειτονικών του κόμβων
- η συνάρτηση inform χρησιμοποιείται για την εισαγωγή της πληροφορίας για την κατάσταση του δικτύου στο χρόνο μηδέν για τα CBB και CFBB μοντέλα.

Η κλάση CentralBBbaseAgent κληρονομεί τις ιδιότητες της κλάσης BBbaseAgent. Η κλάση CentralBBbaseAgent έχει τρεις public συναρτήσεις-μέλη και μια protected μεταβλητή-μέλος. Συγκεκριμένα ορίζονται:

- ο constructor της κλάσης
- η συνάρτηση-μέλος recv χρησιμοποιείται για να καθοριστεί η διαδικασία που θα ακολουθηθεί με την παραλαβή του κάθε πακέτου
- οι υπόλοιπες μεταβλητές κληρονομούνται

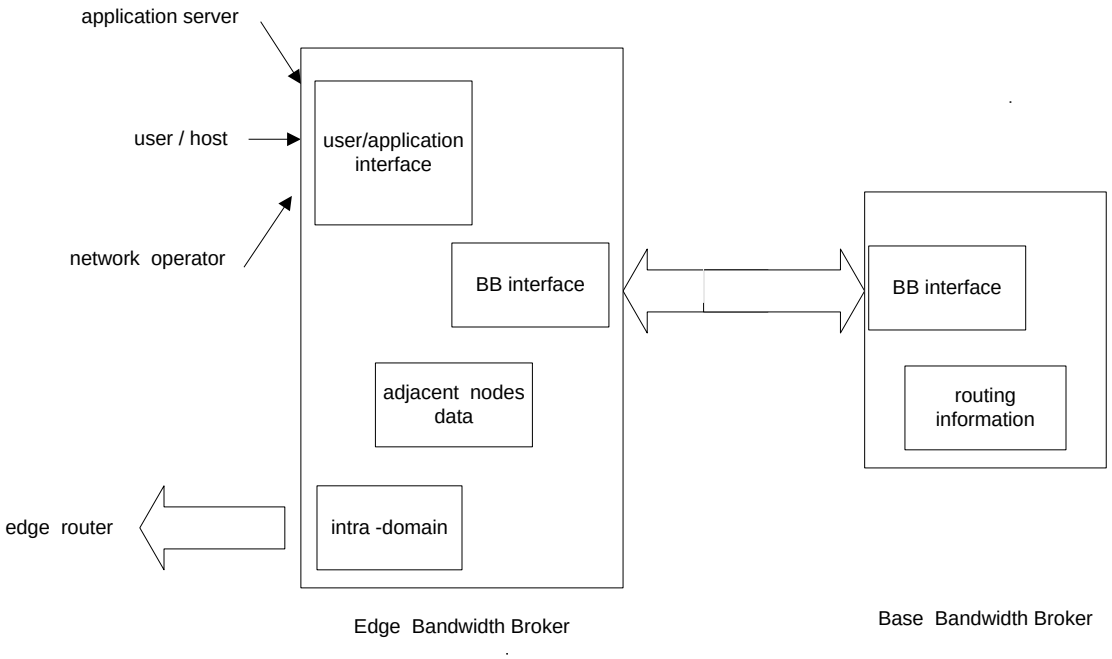
Η κλάση DistributedBBbaseAgent κληρονομεί τις ιδιότητες της κλάσης BBbaseAgent. Η κλάση CentralBBbaseAgent έχει τρεις public συναρτήσεις-μέλη και μια protected μεταβλητή-μέλος. Συγκεκριμένα ορίζονται:

- ο constructor της κλάσης
- η συνάρτηση-μέλος recv χρησιμοποιείται για να καθοριστεί η διαδικασία που θα ακολουθηθεί με την παραλαβή του κάθε πακέτου
- οι υπόλοιπες μεταβλητές κληρονομούνται

Όταν ορίζεται στον ns ένας νέος agent, χρειάζεται να καθοριστεί ο τύπος των πακέτων που θα διαχειρίζεται. Τα πακέτα που διαχειρίζονται οι BBedgeAgent και BBbaseAgent, CentralBBbaseAgent, DistributedBBbaseAgent είναι δύο νέοι τύποι πακέτων, τα πακέτα BBB και BBE, που δημιουργήθηκαν για να εξυπηρετήσουν τη λειτουργικότητα του bandwidth broker.

7.5 Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ BANDWIDTH BROKER

Η γενικότερη αρχιτεκτονική των bandwidth broker που υλοποιήθηκαν εμφανίζεται στην Εικόνα 51.



Εικόνα 51: Η αρχιτεκτονική του bandwidth broker που υλοποιήθηκε

Όπως αναφέρθηκε, οι bandwidth broker που υλοποιήθηκαν αποτελούνται από τον κεντρικό base bandwidth broker και τους κατανεμημένους edge bandwidth brokers. Όπως φαίνεται στο παραπάνω σχήμα, ο base bandwidth broker αποτελείται από δύο λειτουργικές μονάδες. Αυτές είναι:

- Το BB interface
- Το routing information interface

Ο edge bandwidth broker αποτελείται από τέσσερις λειτουργικές μονάδες. Αυτές είναι:

- Το user/application interface
- Το BB interface
- Το intra-domain interface
- Το adjacent nodes interface

Στη συνέχεια θα αναλύσουμε τη λειτουργία του κάθε interface.

7.5.1 BB Interface

Ολόκληρη η λειτουργία των bandwidth broker βασίζεται στο BB interface. Το BB interface είναι το πρωτόκολλο επικοινωνίας μεταξύ των διαφορετικών base bandwidth broker και κάποιου edge bandwidth broker.

Δημιουργήθηκαν δύο τύποι πακέτων για το BB interface, ο τύπος BBE και ο τύπος BBB. Οι διαφορετικοί base bandwidth broker agents δημιουργούν BBB πακέτα και λαμβάνουν BBE πακέτα. Οι edge bandwidth broker agents δημιουργούν BBE πακέτα και λαμβάνουν BBB πακέτα. Και οι δύο τύποι πακέτων έχουν την ίδια επικεφαλίδα, δηλαδή οι επικεφαλίδες και των δύο τύπων αποτελούνται από ακριβώς τα ίδια πεδία. Η δημιουργία όμως δύο τύπων πακέτων και όχι ενός επιτρέπει την τοποθέτηση σε

κάποιον κόμβο τόσο ενός base bandwidth broker agent όσο και ενός edge bandwidth broker agent. Με αυτόν τον τρόπο δεν απαιτείται ένας επιπλέον κόμβος για την τοποθέτηση του κεντρικού Bandwidth Broker. Το μέγεθος των πακέτων BBE και BBB καθορίστηκε να είναι 64 bytes. Επίσης, στα BBE και BBB πακέτα όλη η πληροφορία που είναι απαραίτητη για τη λειτουργία του BB interface βρίσκεται στην επικεφαλίδα των πακέτων. Δηλαδή τα πακέτα δεν περιλαμβάνουν δεδομένα.

Στον ns για να δημιουργηθεί ένας τύπος πακέτου χρειάζεται να δηλωθεί η επικεφαλίδα του. Η επικεφαλίδα του BBE (ομοίως και του BBB) πακέτου ορίστηκε να έχει τα πεδία :

- type
- answer
- bndw_request
- sender
- endnode
- hop_num
- DSCP
- Start_time
- Stop_time
- status

Ας αναλύσουμε τώρα το κάθε πεδίο της επικεφαλίδας, δηλαδή τι εκφράζει, και από ποιον καθορίζεται.

Το πεδίο type της επικεφαλίδας καθορίζει τον τύπο του πακέτου. Έχουν οριστεί οι ακόλουθοι τύποι:

- Ο τύπος REQUEST δηλώνει πακέτο αιτήματος για bandwidth. Πακέτα τύπου REQUEST στέλνονται τόσο από κάποιον από τους edge bandwidth broker agents όταν στέλνει ένα αρχικό αίτημα για bandwidth όσο και από τον base bandwidth broker agent κατά την εξυπηρέτηση του αιτήματος στον έλεγχο αποδοχής.
- Ο τύπος ANSWER δηλώνει πακέτο απάντησης σε κάποιο αίτημα. Πακέτα τύπου ANSWER στέλνονται τόσο από τον base bandwidth broker agent όσο και από κάποιον από τους edge bandwidth broker agents.
- Ο τύπος FIX_BWD δηλώνει πακέτο εντολής μείωσης του διαθέσιμου bandwidth σε κάποιο link. Πακέτα τύπου FIX_BWD στέλνονται μόνο από τον base bandwidth broker agent.
- Ο τύπος UNAVAILABLE δηλώνει μη διαθεσιμότητα του bandwidth broker. Πακέτα τύπου UNAVAILABLE στέλνονται μόνο από τον base bandwidth broker agent.
- Ο τύπος DISTR_QUESTION δηλώνει το τύπο πακέτου που στέλνει ο DistributedBBbase στο BBedge για το αν υπάρχει το διαθέσιμο bandwidth
- Ο τύπος DISTR_ANSWER δηλώνει το τύπο πακέτου με το οποίο απαντά ο BBedge στον DistributedBBbase για το αν όντως υπάρχει το διαθέσιμο bandwidth

- Ο τύπος CENTR_QUESTION δηλώνει το τύπο πακέτου που στέλνει ο CentralBBbase στο BBedge για το αν υπάρχει το διαθέσιμο bandwidth
- Ο τύπος CENTR_ANSWER δηλώνει το τύπο πακέτου με το οποίο απαντά ο BBedge στον CentralBBbase για το αν όντως υπάρχει το διαθέσιμο bandwidth

Το πεδίο answer της επικεφαλίδας καθορίζει την απάντηση σε κάποιο αίτημα για bandwidth. Το συγκεκριμένο πεδίο χρησιμοποιείται μόνο στα πακέτα τύπου ANSWER. Η απάντηση μπορεί να είναι είτε θετική είτε αρνητική. Για τους υπόλοιπους τύπους πακέτων η τιμή στο συγκεκριμένο πεδίο δεν έχει καμία σημασία.

Το πεδίο bndw_request της επικεφαλίδας καθορίζει το ζητούμενο bandwidth όταν το πακέτο είναι τύπου REQUEST ή ANSWER. Στην περίπτωση πακέτου τύπου FIX_BWD το συγκεκριμένο πεδίο καθορίζει την μείωση του διαθέσιμου bandwidth σε κάποιο link. Για τους υπόλοιπους τύπους πακέτων η τιμή στο συγκεκριμένο πεδίο δεν έχει καμία σημασία.

Το πεδίο sender της επικεφαλίδας καθορίζει την διεύθυνση του κόμβου ο οποίος αρχικά δημιούργησε το αίτημα. Αρχικά συμπληρώνεται από τον edge bandwidth broker που στέλνει το αρχικό αίτημα και στη συνέχεια αντιγράφεται σε όλες τις επικεφαλίδες των μηνυμάτων που στέλνονται κατά τον έλεγχο αποδοχής.

Σε πακέτα τύπου REQUEST το πεδίο endnode της επικεφαλίδας καθορίζει τη διεύθυνση του τελικού κόμβου. Σε πακέτα τύπου FIX_BWD το συγκεκριμένο πεδίο χρησιμοποιείται για να καθορίσει ένα link. Δηλαδή σε πακέτα τύπου FIX_BWD το πεδίο endnode πρέπει να είναι ένας κόμβος γειτονικός με τον κόμβο στον οποίο στέλνεται το πακέτο ενώ σε πακέτα τύπου REQUEST μπορεί να είναι οποιοσδήποτε κόμβος του δικτύου.

Το πεδίο hop_num καθορίζει τον αριθμό των hops που το αίτημα έχει επισκεφτεί εκτός του base bandwidth broker agent. Κάθε edge bandwidth broker που δέχεται ένα αίτημα κατά τον έλεγχο αποδοχής, αυξάνει την τιμή στο συγκεκριμένο πεδίο κατά μία μονάδα.

Όταν ένα αίτημα για bandwidth γίνει δεκτό, ανατίθεται στην εφαρμογή που έκανε το αίτημα ένα μοναδικό DSCP. Για αυτό απαιτείται το πεδίο DSCP στην επικεφαλίδα των πακέτων BBE και BBB. Το πεδίο DSCP το συμπληρώνει μόνο ο base bandwidth broker.

Τα πεδία start_time και stop_time περιλαμβάνουν το χρόνο έναρξης και λήξης του αιτήματος για bandwidth.

Το πεδίο status εκφράζει την κατάσταση στην οποία βρίσκεται ένας κόμβος.

7.5.2 Routing Information

Ο base bandwidth broker, όταν δέχεται ένα αίτημα για bandwidth θα πρέπει ή να το προωθήσει σε όλους τους edge bandwidth brokers που βρίσκονται στο μονοπάτι πηγής-προορισμού ή να ρωτήσει τη βάση δεδομένων του για την απαιτούμενη πληροφορία. Και στις δύο περιπτώσεις απαιτείται λοιπόν να γνωρίζουν οι base agents όλους τους κόμβους που βρίσκονται στο μονοπάτι. Συγκεκριμένα, αρχικά υπολογίζεται ο επόμενος κόμβος n_1 από τον κόμβο που προήλθε το μήνυμα, στη συνέχεια ο επόμενος κόμβος n_2 από τον n_1 και ούτω καθεξής μέχρι να φτάσουμε στον προορισμό.

Αυτή η διαδικασία εύρεσης του επόμενου κόμβου γίνεται με το να προσπελαύνει ο base bandwidth broker τους πίνακες δρομολόγησης. Συγκεκριμένα χρησιμοποιούνται διαδοχικά οι εντολές ***compute-routes***, ***get-routelogic*** και ***lookup.*** Στη συνέχεια παρουσιάζουμε συνοπτικά αυτές τις εντολές.

compute-routes

Η παραπάνω εντολή υπολογίζει από την τοπολογία του δικτύου την πληροφορία για το next hop για κάθε κόμβο του δικτύου. Στη συνέχεια δημιουργεί τα routing tables.

get-routelogic

Με αυτήν την εντολή μπορούμε να χειριστούμε τα routing tables και να λάβουμε πληροφορία από αυτά. Χρειάζεται λοιπόν να έχουν υπολογιστεί τα routing tables, άρα να έχει εκτελεστεί η εντολή compute-routes.

lookup <srcid> <destid>

Αφού έχει εκτελεστεί η εντολή get-routelogic, η εντολή lookup επιστρέφει το id του επόμενου κόμβου από το <srcid> ως το <destid>.

Και οι τρεις παραπάνω εντολές είναι της γλώσσας tcl. Όταν χρειάζεται ένα πρόγραμμα που είναι γραμμένο σε C++ να χρησιμοποιήσει tcl εντολές μπορεί να το κάνει με χρήση των *εντολών* ***Tcl::instance()***, ***tcl.evalc tcl.evalf*** και ***tcl.result()***.

7.5.3 Adjacent Nodes Interface

Το adjacent nodes interface χρησιμοποιείται για να διατηρεί ο κάθε edge bandwidth broker πληροφορία για το διαθέσιμο bandwidth στα links που συνδέουν τον κόμβο πάνω στον οποίο τρέχει με τους γειτονικούς του κόμβους.

Ο κάθε edge bandwidth broker χρειάζεται να γνωρίζει ποιοι είναι οι γειτονικοί του edge bandwidth brokers. Επίσης, για κάθε γειτονικό edge bandwidth broker χρειάζεται να γνωρίζει πόσο είναι το διαθέσιμο bandwidth στο αντίστοιχο link. Για τη διαχείριση του bandwidth σε κάθε link δημιουργήθηκε η δομή *neighbor*. Η δομή neighbor αποτελείται από ένα node-id και από το διαθέσιμο bandwidth. Ακόμα, δημιουργήθηκε η μεταβλητή-μέλος *nghbr_list* σε κάθε edge bandwidth broker. Η *nghbr_list* είναι μια λίστα από δομές neighbor. Για κάθε γειτονικό κόμβο δημιουργείται μια δομή neighbor και καθορίζεται το node-id του γειτονικού κόμβου καθώς και το διαθέσιμο bandwidth στο link προς αυτόν τον γειτονικό κόμβο. Στη συνέχεια γίνεται η καταχώρηση της δομής στη λίστα nghbr_list. Με αυτόν τον τρόπο κάθε edge bandwidth broker διατηρεί πληροφορία για το bandwidth σε κάθε link μεταξύ του κόμβου στον οποίο έχει τοποθετηθεί και των γειτονικών κόμβων.

Για να μπορεί ο χρήστης να έχει πρόσβαση στο adjacent nodes interface δημιουργήθηκε η tcl εντολή ***set_bndw***. Η εντολή συντάσσεται ως:

BBedgeAgent set_bndw *node_id bandwidth start_time stop_time*

όπου *BBedgeAgent* κάποιος edge bandwidth broker που τρέχει σε κάποιον κόμβο n1, *node_id* το node-id κάποιου κόμβου n_2 γειτονικού του n_1 , *bandwidth* το bandwidth που θα διαχειρίζεται ο bandwidth broker στο link n_1-n_2 και start_time- stop_time το χρονικό διάστημα για το οποίο θέλουμε το bandwidth.

Στα SDBB, PDBB μοντέλα όταν προωθείται ένα αίτημα από τον base bandwidth broker σε κάποιον edge bandwidth broker που βρίσκεται στο μονοπάτι, ουσιαστικά ο

edge bandwidth broker ερωτάται για το εάν υπάρχει διαθέσιμο bandwidth στο link που οδηγεί στον επόμενο κόμβο. Ο έλεγχος γίνεται με το να αναζητείται στη λίστα *nghbr_list* η εγγραφή *neighbor* της οποίας το node-id ισούται με το node-id του επόμενου κόμβου. Στη συνέχεια γίνεται έλεγχος εάν το bandwidth στη συγκεκριμένη εγγραφή είναι μεγαλύτερο από το αιτούμενο bandwidth για το συγκεκριμένο χρονικό διάστημα. Εάν τελικά το αίτημα γίνει δεκτό, ο base bandwidth broker ενημερώνει για το γεγονός όλους τους edge bandwidth brokers που βρίσκονται στο μονοπάτι. Αφού ειδοποιηθεί, ο κάθε edge bandwidth broker αναζητεί και πάλι στη λίστα *nghbr_list* την εγγραφή *neighbor* της οποίας το node-id ισούται με το node-id του επόμενου κόμβου και μειώνει το bandwidth στη συγκεκριμένη εγγραφή τόσο όσο είναι το bandwidth του αιτήματος για το συγκεκριμένο χρονικό διάστημα.

Στα CBB/CFBB μοντέλα όλες οι λίστες *nghbr_list* όλων των κόμβων του δικτύου βρίσκονται στους base agents. Η αναζήτηση γίνεται με ακριβώς των ίδιο τρόπο μόνο που δεν γίνεται μέσω δικτύου αλλά τοπικά. Εάν τελικά το αίτημα γίνει δεκτό, ο base bandwidth broker ενημερώνει για το γεγονός την τοπική του βάση δεδομένων. Ειδικά στο CFBB μοντέλο, έχουμε και ενημέρωση της βάσης δεδομένων που βρίσκεται στους Edges.

Υπάρχουν πολλά πλεονεκτήματα με το να διαθέτει κάθε edge bandwidth broker τη δική του λίστα *nghbr_list*. Το σημαντικότερο είναι ότι για κάθε link σε ένα μονοπάτι, το διαθέσιμο bandwidth μπορεί να έχει διαφορετική τιμή. Επίσης, στην περίπτωση που ένα duplex link αποτελείται από δύο simplex links, δηλαδή στην περίπτωση που το link αποτελείται από δύο links μιας κατεύθυνσης, μπορεί να οριστεί διαφορετικό διαθέσιμο bandwidth για τη μια κατεύθυνση και διαφορετικό για την άλλη. Αυτό θα σημαίνει ότι για δύο γειτονικούς edge bandwidth brokers, το bandwidth στην εγγραφή neighbor του πρώτου για τον δεύτερο δεν είναι απαραίτητα ίσο με το bandwidth στην εγγραφή neighbor του δεύτερου για τον πρώτο διότι το διαθέσιμο bandwidth σε κάθε ένα από τα δύο simplex links μπορεί να διαφέρει.

7.5.4 User/Application Interface

Το ανώτερο επίπεδο στην αρχιτεκτονική του bandwidth broker που υλοποιήθηκε είναι το user/application interface. Το user/application interface είναι το interface που χρησιμοποιείται για την επικοινωνία του χρήστη με το σύστημα του bandwidth broker. Όταν ένας χρήστης επιθυμεί να χρησιμοποιήσει ένα μέρος των δικτυακών πόρων με εγγυήσεις για το bandwidth, μπορεί να χρησιμοποιήσει το user/application interface για να κάνει ένα αίτημα στον bandwidth broker. Επίσης, όταν ο bandwidth broker ολοκληρώσει τη διαδικασία του ελέγχου αποδοχής του αιτήματος (και στην περίπτωση θετικής απάντησης ολοκληρώσει και την κατανομή των πόρων) χρησιμοποιεί το user/application interface ώστε να δηλώσει την απάντηση στον χρήστη.

Το user/application interface υλοποιήθηκε σε Tcl. Τα αιτήματα για bandwidth στέλνονται πάντα από κάποιον Edge bandwidth broker agent. Έτσι δημιουργήθηκε η Tcl εντολή ***sendto***. Η εντολή συντάσσεται ως:

BBedgeAgent *sendto* node_id bandwidth *start_time stop_time*

όπου *BBedgeAgent* κάποιος edge bandwidth broker που τρέχει σε κάποιον κόμβο n1, *node_id* το node-id κάποιου κόμβου n2 , *bandwidth* το αιτούμενο bandwidth που ζητά

ο BBedgeAgent από τον κόμβο n1 ως τον κόμβο n2 και start_time-stop_time το χρονικό διάστημα για το οποίο επιθυμούμε το bandwidth.

Όταν ο edge bandwidth broker ο οποίος έστειλε ένα αίτημα λάβει απάντηση, τη διαβιβάζει στην εφαρμογή που ζήτησε το εγγυημένο bandwidth. Αυτό γίνεται με την Tcl συνάρτηση **recv** του edge bandwidth broker που επιστρέφει την απάντηση στην εφαρμογή. Σε περίπτωση θετικής απάντησης επιστρέφεται και το DSCP που έχει ανατεθεί στη συγκεκριμένη κίνηση του χρήστη. Από εκεί και πέρα είναι θέμα της εφαρμογής το πώς θα μεταχειριστεί το εγγυημένο bandwidth που της παραχωρήθηκε. Παρόλα αυτά, για να έχει τις εγγυήσεις ποιότητας που ζήτησε, η εφαρμογή χρειάζεται να μαρκάρει όλα τα πακέτα της με το DSCP που της επιστράφηκε.

7.5.5 Intra Domain Interface

Το intra-domain interface χρησιμοποιείται από τους edge bandwidth brokers για την κατανομή των πόρων του δικτύου. Όταν ολοκληρωθεί ο έλεγχος αποδοχής ενός αιτήματος για bandwidth, στην περίπτωση που το αίτημα γίνει δεκτό απαιτείται να γίνει η κατάλληλη κατανομή των πόρων του δικτύου. Η κατανομή των πόρων έχει τρεις κύριους στόχους:

- Να παρέχεται στην εφαρμογή που έστειλε το αίτημα το εγγυημένο bandwidth που ζήτησε και έγινε δεκτό από τον bandwidth broker.
- Στην περίπτωση που η συγκεκριμένη εφαρμογή αποπειραθεί να στείλει στο δίκτυο κίνηση που να απαιτεί ελαφρώς περισσότερο bandwidth από αυτό που της έχει ανατεθεί, αυτό να γίνεται ομαλά χωρίς απώλειες πακέτων.
- Στην περίπτωση που η συγκεκριμένη εφαρμογή αποπειραθεί να στείλει στο δίκτυο κίνηση που να απαιτεί αρκετά περισσότερο bandwidth από αυτό που της έχει ανατεθεί, τα πακέτα της πλεονάζουσας κίνησης να απορρίπτονται από τους routers του δικτύου.

Η λειτουργία της κατανομής πόρων αρχίζει μόλις γίνει δεκτό ένα αίτημα για bandwidth. Εκείνη τη στιγμή ο edge bandwidth broker χρησιμοποιεί το intra-domain interface για να κάνει configure τους routers ώστε να ικανοποιούν κατάλληλα το αίτημα. Όλη η διαδικασία κατανομής των πόρων γίνεται μέσα στην Tcl συνάρτηση recv που αναφέρθηκε και στο user/application interface.

Για τη χρονοδρομολόγηση σε όλες τις ουρές έχουν επιλεγεί οι ουρές προτεραιοτήτων. Έτσι, ορίζονται δύο φυσικές ουρές εκ των οποίων η μία θα εξυπηρετεί την κίνηση των εφαρμογών που έχουν πάρει την έγκριση από τον bandwidth broker και έχουν εξασφαλισμένο bandwidth και η άλλη ουρά θα εξυπηρετεί όλη την υπόλοιπη κίνηση. Η πρώτη φυσική ουρά αποτελείται από δύο ιδεατές ουρές (virtual queues). Στον ns, όταν χρησιμοποιούνται ουρές προτεραιοτήτων για τη χρονοδρομολόγηση στις ουρές, μπορεί να ρυθμιστεί συγκεκριμένα το μέγιστο bandwidth που θα εξυπηρετείται από κάθε φυσική ουρά (π.χ. ότι η φυσική ουρά 0 θα εξυπηρετεί το πολύ 1Mbps). Αντίστοιχα, για την Weighted Round Robin χρονοδρομολόγηση ή την Modified Deficit Round Robin το μέγιστο bandwidth που θα εξυπηρετεί η κάθε ουρά δεν ρυθμίζεται συγκεκριμένα αλλά σχετικά με τις υπόλοιπες ουρές. Σε κάθε ουρά ανατίθεται ένα βάρος και όσο μεγαλύτερο βάρος έχει μια ουρά σε σχέση με μια άλλη τόσο περισσότερο εξυπηρετείται σε κάθε κύκλο.

Στην υλοποίηση θεωρούμε ότι η κίνηση στην οποία παρέχεται εξασφαλισμένο bandwidth εξυπηρετείται από τη φυσική ουρά 0 και η υπόλοιπη κίνηση από τη φυσική ουρά 1. Εδώ απαιτείται να γίνει ορθά η κατανομή των βαρών ή το μέγιστο bandwidth που θα εξυπηρετεί η κάθε ουρά (ανάλογα με το μηχανισμό χρονοδρομολόγησης) ώστε το bandwidth που θα εξυπηρετεί ή ουρά 0 να είναι ίσο με το bandwidth που διαχειρίζεται ο bandwidth broker στο συγκεκριμένο link, όπως καθορίζεται από τη συνάρτηση *set_bndw*.

Το DSCP της κίνησης που δεν έχει εξασφαλίσει bandwidth από τον bandwidth broker είναι το 0. Το DSCP των πακέτων BBB και BBE είναι το 1. Τα DSCPs των ροών που έχουν εξασφαλίσει bandwidth από τον bandwidth broker είναι τα 2-255. Η επιλογή της ουράς στην οποία τοποθετείται κάθε πακέτο γίνεται με βάση το DSCP της επικεφαλίδας του. Συγκεκριμένα, τα πακέτα με DSCP 0 τοποθετείται στην φυσική ουρά 1. Τα πακέτα με DSCP 1 τοποθετούνται στην ιδεατή ουρά 0 της φυσικής ουράς 0. Τα πακέτα με DSCP 2-255 τοποθετούνται στην ιδεατή ουρά 1 της φυσικής ουράς 0. Ο καθορισμός των ουρών στις οποίες τοποθετούνται τα πακέτα με DSCP 0 και 1 γίνεται από την αρχή της λειτουργίας του συστήματος. Αρχικά δεν έχει ανατεθεί κανένα από τα DSCPs 2-255 σε κάποια εφαρμογή και δεν προβλέπεται η τοποθέτηση πακέτων που φέρουν κάποιο από αυτά τα DSCPs σε κάποια ουρά.

Όταν ολοκληρωθεί ένας έλεγχος αποδοχής κάποιου αιτήματος με επιτυχία, δηλαδή το αίτημα γίνει δεκτό, αρχικά καθορίζεται το DSCP που θα χρησιμοποιεί η εφαρμογή που έκανε το αίτημα. Ο καθορισμός αυτού του DSCP γίνεται από τον base bandwidth broker. Ο base bandwidth broker διαθέτει την μεταβλητή-μέλος *cur_dscp* η τιμή της οποίας ανά πάσα στιγμή εκφράζει το επόμενο διαθέσιμο DSCP που θα ανατεθεί σε εφαρμογές των οποίων τα αιτήματα έγιναν δεκτά. Το αρχικό διαθέσιμο DSCP είναι 2 και μετά από κάθε ανάθεση αυξάνεται κατά 1. Συνεπώς μπορούν να υπάρχουν 254 διαφορετικές συνενώσεις ροών και η διαφοροποίηση τους θα γίνεται με βάση το DSCP.

Όταν υπολογιστεί το DSCP που θα χρησιμοποιεί μια εφαρμογή, επιστρέφεται με το μήνυμα θετικής απάντησης στον edge bandwidth broker ο οποίος έστειλε το αίτημα και από αυτόν μέσω της Tcl συνάρτησης *recv* στην εφαρμογή που θα το χρησιμοποιεί. Από εκεί και μετά είναι ευθύνη της εφαρμογής να μαρκάρει τα πακέτα της με το συγκεκριμένο DSCP.

Στη συνάρτηση recv γίνονται configure και όλοι οι δρομολογητές του δικτύου ώστε να εξυπηρετούν κατάλληλα τα πακέτα που φέρουν το συγκεκριμένο DSCP. Σε κάθε ουρά του δικτύου κορμού καθορίζεται ότι τα πακέτα με το συγκεκριμένο DSCP θα τοποθετούνται στην ιδεατή ουρά 1 της φυσικής ουράς 0. Επίσης, καθορίζεται η αστυνόμευση που θα γίνεται στα πακέτα με το συγκεκριμένο DSCP. Ως μηχανισμός αστυνόμευσης έχει οριστεί ο Token Bucket (κουβάς με κουπόνι). Η αστυνόμευση γίνεται σε όλους τους κόμβους του δικτύου. Ο μηχανισμός Token Bucket, έχει δύο σημαντικές παραμέτρους, το μέσο επιτρεπτό bandwidth σε bps και το μέγεθος του κάδου σε bytes. Το μέσο επιτρεπτό bandwidth συνήθως είναι λίγο μεγαλύτερο από το bandwidth που είχε ζητηθεί από τον bandwidth broker. Αυτό συμβαίνει για να μην χάνονται πακέτα μιας ροής όταν ο ρυθμός τους υπερβαίνει κατά ένα μικρό ποσοστό το προκαθορισμένο προφίλ.

Όλες οι ροές που έχουν διασφαλίσει εγγυημένο bandwidth καθώς και τα πακέτα του intra-domain πρωτοκόλλου τοποθετούνται πάντα στη φυσική ουρά 0. Τα πακέτα του intra-domain πρωτοκόλλου τοποθετούνται στην ιδεατή ουρά 0 της φυσικής ουράς 0 ενώ τα άλλα πακέτα στην ιδεατή ουρά 1 της φυσικής ουράς 0. Ο λόγος που τα πακέτα

του intra-domain πρωτοκόλλου τοποθετούνται σε διαφορετική ιδεατή ουρά από τα υπόλοιπα πακέτα είναι ότι απαιτείται ιδιαίτερη προσοχή ώστε να μην χάνονται τέτοια πακέτα, καθώς απώλεια BBB ή BBE πακέτων μπορεί να οδηγήσει σε μη ορθή λειτουργία του πρωτοκόλλου. Ο ns δίνει τη δυνατότητα ανάθεσης σε κάθε ιδεατή ουρά της μέγιστης πιθανότητας απόρριψης πακέτων. Αν λοιπόν ανατεθεί σχεδόν μηδενική πιθανότητα απόρριψης πακέτων στην ιδεατή ουρά 1 της φυσικής ουράς 0, διασφαλίζεται ότι πολύ σπάνια θα χαθούν πακέτα του intra-domain πρωτοκόλλου, ακόμα και σε περιπτώσεις συμφόρησης του δικτύου.

7.6 ΥΛΟΠΟΙΗΣΗ BANDWIDTH BROKER

Στην παράγραφο αυτή θα γίνει μια περιγραφή των Bandwidth Broker που αναπτύχθηκαν, υλοποιήθηκαν και δοκιμάστηκαν στον ns-2. Όπως έχει ήδη αναφερθεί τα μοντέλα αυτά είναι:

- Serial Distributed Bandwidth Broker model (SDBB model)
- Parallel Distributed Bandwidth Broker model (PDBB model)
- Centralized Bandwidth Broker model (CBB model)
- Centralized Fault-tolerant Bandwidth Broker model (CFBB model)

Σε κάθε υλοποίηση υπάρχουν δύο είδη agents, ο Edge Bandwidth Broker (BBedgeAgent) και ο Base Bandwidth Broker (BBbaseAgent). Ένας agent στον ns-2 είναι ένα σημείο όπου τα πακέτα καταναλώνονται και κατασκευάζονται χρησιμοποιώντας ένα συγκεκριμένο πρωτόκολλο. Ένας BBedge agent είναι ένα απλό module τοποθετημένο σε κάθε κόμβο (router) του δικτύου που αναπαριστά ένα client (ένας χρήστης ή μια εφαρμογή) και έχει ως λειτουργία το να στέλνει αιτήματα για κίνηση με συγκεκριμένο profile για μια συγκεκριμένη χρονική περίοδο. Ένα τέτοιο αίτημα λαμβάνεται από τον BBbase agent, που αναπαριστά έναν server, και προστίθεται σαν ένα αίτημα με συγκεκριμένες παραμέτρους (sender, end node, bandwidth, time limit και status, που στο στάδιο αυτό μαρκάρεται ως pending) στην τοπική βάση δεδομένων. Όταν τελειώνει η επεξεργασία του αιτήματος, το status του αιτήματος αλλάζει ανάλογα με το αποτέλεσμα της επεξεργασίας, είτε “satisfied” είτε “rejected”. Η απάντηση μετά στέλνεται πίσω στον BBedge agent.

Ένα άλλο κοινό στοιχείο των BBbase agents για όλα τα μοντέλα είναι το buffer για τα αιτήματα. Οι BBbase agents επεξεργάζονται ένα αίτημα τη φορά ώστε εάν δύο αιτήματα φτάσουν κοντινά το ένα με το άλλο, το πρώτο πρόκειται να ικανοποιηθεί και το άλλο πρόκειται να προστεθεί σε ένα buffer που υπάρχει στους BBbase agents. Εάν ένα αίτημα φτάσει και το buffer είναι άδειο, το αίτημα θα ικανοποιηθεί αμέσως. Διαφορετικά, εάν το buffer εμπεριέχει προηγούμενα αιτήματα αλλά δεν είναι ακόμα γεμάτο, το αίτημα θα προστεθεί στο τέλος του buffer με σκοπό να επεξεργαστεί στο μέλλον. Τελικά, εάν το buffer είναι γεμάτο, το αίτημα απορρίπτεται. Το μήκος του buffer μπορούμε να το διαμορφώσουμε οι ίδιοι και είναι ένα σημείο έρευνας για την αποτελεσματική λειτουργία του bandwidth broker.

Παρόλο που η δομή των BBedge agents είναι ίδια και για τα τέσσερα μοντέλα που έχουν υλοποιηθεί, κάθε ένα λειτουργεί με τον τρόπο του, όταν διάφορα πακέτα λαμβάνονται κατά τη διάρκεια της εξομοίωσης. Οι διαφορές ανάμεσα στις τέσσερις αρχιτεκτονικές έχουν κυρίως να κάνουν κυρίως με τη δομή και τη συμπεριφορά των υλοποιημένων πρωτοκόλλων. Τα διάφορα μοντέλα χρησιμοποιούν μεθόδους για να

επεξεργαστούν τα αιτήματα (admission control) και να αποθηκεύσουν την απαραίτητη πληροφορία. Οι μέθοδοι επεξεργασίας αιτημάτων περιγράφονται λεπτομερώς στη συνέχεια ενώ το υπόλοιπο κομμάτι αφορά την αποθήκευση της πληροφορίας.

Τα SDBB και PDBB μοντέλα αποθηκεύουν την πληροφορία σχετικά με την κατάσταση της κάθε σύνδεσης (δεσμευμένο bandwidth για τα υπάρχοντα αιτήματα, ελεύθερο bandwidth) στους αντίστοιχους BBedge agents. Αντίθετα, το CBB μοντέλο αποθηκεύει την πληροφορία στον BBbase agent και το CFBB μοντέλο αποθηκεύει την πληροφορία τόσο στους BBedge agents όσο και στον BBbase agent. Το format της πληροφορίας αυτής είναι το παρακάτω: ας πάρουμε για παράδειγμα τον κόμβο 1 που είναι συνδεδεμένος με τον κόμβο 2 και τον κόμβο 2 που είναι συνδεδεμένος με τον κόμβο 1. Η σχετική πληροφορία για τον κόμβο ένα είναι ότι "Το διαθέσιμο bandwidth από τον κόμβο 1 στον κόμβο 2 είναι b για την χρονική περίοδο t_2-t_1" όπου t_2, t_1 είναι σημεία στο χρόνο και b το bandwidth που προκύπτει. Η σχετική πληροφορία για τον κόμβο 2 είναι ότι "το διαθέσιμο bandwidth από τον κόμβο 2 στον κόμβο 1 είναι b' για την χρονική περίοδο t_2'-t_1' ", όπου t_2', t_1' είναι σημεία στο χρόνο και b' το bandwidth. Στο δικό μας μοντέλο εξομοίωσης κάνουμε την υπόθεση ότι b'=b, t_2'=t_2 και t_1=t_1' ανάμεσα στους δύο κόμβους, με άλλα λόγια ότι όλα τα αιτήματα και οι δεσμεύσεις είναι bidirectional. Για τα CBB και CFBB μοντέλα, η τοπική βάση δεδομένων του BBbase agent, έχει για κάθε κόμβο που ελέγχει, ολόκληρη την πληροφορία του διαθέσιμου bandwidth για κάθε σύνδεση που έχει με ένα γειτονικό κόμβο για όλες τις χρονικές στιγμές.

7.6.1 Περιγραφή των υλοποιημένων μοντέλων

Σε κάθε ένα από τα υλοποιημένα μοντέλα, χρησιμοποιούμε διαφορετικό μοντέλο επικοινωνίας με σκοπό την ολοκλήρωση της επεξεργασίας των αιτημάτων. Σκοπός μας είναι να εξομοιώσουμε, όσο ακριβές γίνεται, ένα δίκτυο που ελέγχεται από ένα Bandwidth Broker. Η επικοινωνία ανάμεσα στο BBbase και στον BBedge agent επιτυγχάνεται με τη χρήση μηνυμάτων που στέλνονται συνέχεια είτε από ένα BBedge σε ένα BBbase είτε από έναν BBbase σε έναν BBedge agent. Δύο BBedge agents δεν επικοινωνούν ποτέ με το να στέλνουν μηνύματα ο ένας στον άλλο, αφού ο BBbase agent πάντα μεσολαβεί στην επικοινωνία.

Για το SDBB μοντέλο η επεξεργασία παρουσιάζεται στη συνέχεια. Στο μοντέλο αυτό, όλη η πληροφορία σχετικά με την κατάσταση των γραμμών όσον αφορά το διαθέσιμο bandwidth αποθηκεύεται τοπικά στους BBedge agents, όπως έχει ήδη αναφερθεί. Στην αρχή, ο BBedge στέλνει ένα αίτημα για bandwidth στον BBbase agent. Όταν ο BBbase agent λαμβάνει το αίτημα, αποθηκεύει την διεύθυνση του αποστολέα. Μετά χρησιμοποιώντας μια tcl εντολή του ns-2 περιβάλλοντος προσομοίωσης ("lookup"), βρίσκει τον γειτονικό κόμβο του αποστολέα αιτήματος. Συγκεκριμένα, με την εισαγωγή του κόμβου έναρξης και λήξης της επιθυμητής διαδρομής, ο ns-2 χρησιμοποιεί το OSFP πρωτόκολλο για να βρει το πιο σύντομο μονοπάτι ανάμεσα στους δύο αυτούς κόμβους και μετά επιστρέφει στον χρήστη τον πρώτο κόμβο της διαδρομής αυτής που βρίσκεται δίπλα στον αποστολέα αιτήματος. Έτσι, αρχικά, ο BBbase στέλνει ένα πακέτο στον BBedge agent που ξεκίνησε το αίτημα για bandwidth, ρωτώντας τον για το κατά πόσο υπάρχει διαθέσιμο bandwidth από τον εαυτό του μέχρι τον επόμενο γειτονικό κόμβο. Εάν ο BBbase λάβει μια θετική απάντηση από τον πρώτο BBedge agent της διαδρομής, τότε ο BBbase ρωτά τον γείτονα του πρώτου κόμβου για bandwidth και πάει λέγοντας, μέχρι ο BBbase λάβει

μια αρνητική ενέργεια, στην οποία περίπτωση σταματά την επεξεργασία του αιτήματος, στέλνει αρνητική απάντηση στον αποστολέα του αιτήματος και συνεχίζει με το επόμενο αίτημα, ή μέχρι ο BBbase λάβει θετικές απαντήσεις από όλους τους κόμβους που βρίσκονται στη διαδρομή του αιτήματος, περίπτωση στην οποία ο BBbase στέλνει θετική απάντηση στον αποστολέα του αιτήματος και από ένα πακέτο σε κάθε κόμβο που βρίσκεται πάνω στη διαδρομή του αιτήματος, με σκοπό να ανανεώσει την πληροφορία τους σχετικά με τη διαθεσιμότητα του bandwidth. Μετά από αυτό, ο BBbase συνεχίζει στην επεξεργασία του επόμενου αιτήματος (εάν υπάρχει). Μια θετική απάντηση σημαίνει ότι ο BBbase agent επιτρέπει στον αποστολέα του αιτήματος να χρησιμοποιήσει το bandwidth που ζητήθηκε δίνοντας εγγυήσεις σχετικά με την δέσμευση των απαιτούμενων πόρων και μια αρνητική απάντηση σημαίνει ότι το αίτημα απορρίφθηκε λόγω έλλειψης bandwidth.

Το PDBB μοντέλο, παρόμοια με το SDBB μοντέλο, αποθηκεύει και αυτό την πληροφορία στους BBedge agents αλλά έχει διαφορετικό τρόπο απόκτησης της πληροφορίας αυτής στην πορεία επεξεργασίας ενός αιτήματος. Όταν το αίτημα φτάνει, ο BBbase agent στέλνει ένα πακέτο σε κάθε ένα από τους κόμβους που βρίσκονται στη διαδρομή του αιτήματος ρωτώντας τους για bandwidth σε μια συγκεκριμένη χρονική περίοδο. Εάν λάβει έστω και μια αρνητική απάντηση, δεν περιμένει για οποιαδήποτε άλλη απάντηση από τους BBedge agents, αλλά σταματά την επεξεργασία του αιτήματος, στέλνει μια αρνητική απάντηση στον αποστολέα του αιτήματος και συνεχίζει στο επόμενο αίτημα. Εάν ο BBbase agent συνεχίζει να παίρνει θετικές απαντήσεις από τους κόμβους, περιμένει να απαντήσουν όλοι οι κόμβοι στη ερώτησή του. Εάν όλοι οι κόμβοι έχουν απαντήσει θετικά, τότε το υπόλοιπο μέρος της επεξεργασίας του αιτήματος είναι πανομοιότυπο με το SDBB μοντέλο. Η κύρια διαφορά από τον SDBB είναι επομένως ότι τώρα ο BBbase agent δεν ρωτάει σειριακά τους κόμβους, αλλά παράλληλα (ένα είδος πλημμύρας των μηνυμάτων ερώτησης) και περιμένει μέχρι όλοι οι BBedge agents απαντήσουν. Το PDBB μοντέλο στοχεύει στη μείωση των χρόνων απόκρισης των αιτημάτων σε σχέση με το SDBB μοντέλο με την παραλληλοποίηση των ερωτήσεων πάνω στο δίκτυο.

Το CBB μοντέλο είναι ένα κεντρικοποιημένο μοντέλο σε σχέση με την κατανεμημένη φύση των προηγούμενων μοντέλων. Ο BBbase agent αποθηκεύει όλη την πληροφορία σχετικά με την κατάσταση και την διαθεσιμότητα των γραμμών σε μια τοπική βάση δεδομένων, την οποία λαμβάνει υπόψη με σκοπό να επεξεργαστεί ένα αίτημα. Έτσι ο χρόνος απόκρισης μειώνεται με την μείωση της διαδικτυακής επικοινωνίας, αλλά το CBB μοντέλο μείωσε και την ανεκτικότητα εξαιτίας της εξάρτησής του από έναν μόνον κόμβο.

Το CFBB μοντέλο συνδυάζει τα πλεονεκτήματα του CBB μοντέλου και προσθέτει πλεονασμό πληροφορίας με σκοπό την αύξηση της ανεκτικότητας σε αποτυχίες κόμβων. Τα δεδομένα που αφορούν την κατάσταση των γραμμών και την διαθεσιμότητα αποθηκεύονται και στους BBedge και στους BBbase agents. Ένα αίτημα επεξεργάζεται όπως ακριβώς και στο CBB μοντέλο, αλλά με το που έχουμε μια θετική απάντηση, ο BBbase agent όχι μόνο ενημερώνει την τοπική βάση δεδομένων του, αλλά και επίσης στέλνει ένα πακέτο σε κάθε κόμβο της διαδρομής του αιτήματος με σκοπό την ενημέρωση της σχετικής τους πληροφορίας. Η πληροφορία αυτή δεν μπορεί να αποκτηθεί κατά την διάρκεια της επεξεργασίας του αιτήματος, αλλά μπορεί να χρησιμοποιηθεί στην περίπτωση μιας αποτυχίας στον κόμβο που φιλοξενεί τον BBbase agent. Ένας άλλος κόμβος μπορεί μετά να τρέξει ένα νέο BBbase agent ο οποίος γίνεται ενήμερος για την κατάσταση του δικτύου από όλους τους BBedge agents(ο καθένας στέλνει ένα απλό μήνυμα στο νέο BBbase agent

με την σχετική πληροφορία) σχετικά με την διαθεσιμότητα του bandwidth και τις υπάρχουσες δεσμεύσεις. Το μειονέκτημα για το CFBB μοντέλο είναι η παραγωγή κάποιου επιπλέον φόρτου στο δίκτυο σε σχέση με το CBB μοντέλο.

7.7 ΠΕΙΡΑΜΑΤΙΚΗ ΑΞΙΟΛΟΓΗΣΗ

Όλα τα πειράματα στον ns γράφονται σε Tcl και απαιτείται να έχουν μια συγκεκριμένη δομή ώστε να μπορέσει ο προσομοιωτής να τα εκτελέσει.

Αρχικά χρειάζεται να οριστεί η τοπολογία του δικτύου. Ορίζονται αρχικά οι κόμβοι από τους οποίους αποτελείται το δίκτυο και στη συνέχεια τα links που τους συνδέουν. Τα links μπορούν να είναι simplex links ή duplex links, ανάλογα αν επιθυμούμε η κατεύθυνση της κίνησης μέσα από αυτά να είναι μονόδρομη ή αμφίδρομη αντίστοιχα. Οι σημαντικότερες παράμετροι κατά τη δημιουργία του κάθε link είναι το μέγιστο bandwidth σε bits per second, η καθυστέρηση μετάδοσης σε second ή milliseconds και το είδος της ουράς, για παράδειγμα droptail, dsRed/edge κλπ. Μετά την τοπολογία του δικτύου γίνονται configure οι ουρές των links ώστε να μπορέσουν να εξυπηρετήσουν την DiffServ αρχιτεκτονική, αν βέβαια αυτό κρίνεται απαραίτητο. Σε κάθε ουρά, ορίζεται ο μηχανισμός χρονοδρομολόγησης, ο αριθμός των φυσικών και των ιδεατών ουρών, οι αντιστοιχίσεις του κάθε DSCP με την αντίστοιχη φυσική και ιδεατή ουρά, για κάθε DSCP ο μηχανισμός αστυνόμευσης με τις παραμέτρους του (όπως το μέγιστο επιτρεπτό bandwidth και το μέγιστο μέγεθος καταιγισμού), και για κάθε ιδεατή ουρά η πιθανότητα απόρριψης πακέτων που βρίσκονται σε αυτήν.

Στο τελευταίο μέρος του tcl script που καθορίζει το πείραμα δηλώνονται όλες οι λειτουργίες που θα συμβούν και η χρονική στιγμή την οποία θα συμβεί η καθεμία.

Σε γενικές γραμμές η παραπάνω μεθοδολογία ακολουθείται κατά τη δημιουργία ενός Tcl πειράματος στον ns. Όταν χρησιμοποιείται η υλοποίηση του bandwidth broker απαιτείται να γίνουν ορισμένες διευκρινήσεις επιπλέον. Συγκεκριμένα, σε κάθε ουρά ο αριθμός των ιδεατών και των φυσικών ουρών χρειάζεται να οριστεί ως 2. Η φυσική ουρά 1 θα χρησιμοποιείται για την εξυπηρέτηση της κίνησης που δεν έχει διασφαλίσει εγγυημένο bandwidth παίρνοντας την έγκριση από τον bandwidth broker. Τα πακέτα αυτής της κίνησης χρειάζεται να μαρκάρονται ώστε να έχουν DSCP 0. Χρειάζεται λοιπόν να γίνει αντιστοίχηση του DSCP 0 με τη φυσική ουρά 1. Όμοια, η φυσική ουρά 0 θα χρησιμοποιείται από την κίνηση που έχει διασφαλίσει εγγυημένο bandwidth. Χρειάζεται δηλαδή να γίνει αντιστοίχηση των πακέτων που χρησιμοποιούνται στο BB interface πρωτόκολλο , δηλαδή του DSCP 1, με τη φυσική ουρά 0 και την ιδεατή ουρά 0.

Σε κάθε κόμβο του δικτύου χρειάζεται να ανατεθεί ένας BBedge agent και σε έναν μοναδικό κόμβο πρέπει να ανατεθεί ένας BBbase agent. Όλοι οι BBedge agents χρειάζεται να συνδεθούν με τον BBbase agent. Επίσης, απαιτείται για κάθε link να χρησιμοποιηθεί η εντολή set_bndw ώστε να δημιουργηθούν σε όλους τους BBedge agents οι λίστες nghbr_list και, κατά συνέπεια, να καθοριστεί το bandwidth που θα διαχειρίζεται ο bandwidth broker σε όλο το εύρος του δικτύου.

Στο Tcl αρχείο χρειάζεται να δημιουργηθεί και η συνάρτηση recv του BBedge. Η συνάρτηση recv δέχεται έξι ορίσματα:

- τη διεύθυνση του κόμβου προορισμού
- την απάντηση στο αίτημα (θετική ή αρνητική)

- το DSCP που θα πρέπει να χρησιμοποιεί η εφαρμογή (σε περίπτωση θετικής απάντησης)
- το bandwidth που ζητήθηκε
- ο χρόνος έναρξης του αιτήματος
- ο χρόνος λήξης του αιτήματος

Στη συνάρτηση recv θα πρέπει:

- Να ελέγχεται αν η απάντηση είναι θετική η αρνητική.
- Να καθορίζεται η λειτουργία του συστήματος σε περίπτωση θετικής απάντησης. Αυτή η λειτουργία θα πρέπει κυρίως να περιλαμβάνει το μηχανισμό κατανομής πόρων ώστε να μπορεί να εξυπηρετηθεί η κίνηση της εφαρμογής που έστειλε το αίτημα. Μετά την κατανομή των πόρων μπορεί να ξεκινά η δημιουργία των πακέτων της νέας κίνησης, τα οποία απαιτείται να μαρκάρονται με το συγκεκριμένο DSCP.
- Να καθορίζεται η λειτουργία του συστήματος σε περίπτωση αρνητικής απάντησης. Για παράδειγμα, σε περίπτωση αρνητικής απάντησης μπορεί να στέλνει ο BBedge ένα νέο αίτημα στον bandwidth broker.

Στο τελευταίο τμήμα του tcl script μπορούν οι BBedge agents να στέλνουν αιτήματα στον BBbase agent χρησιμοποιώντας την εντολή sendto.

Η απόδοση των Bandwidth Broker models συγκρίθηκε σε ένα αριθμό από διαφορετικές δικτυακές τοπολογίες χρησιμοποιώντας διαφορετικά κριτήρια και μετρικές. Μία σημαντική μετρική είναι το ποσοστό των θετικών απαντήσεων (τα αιτήματα που έγιναν αποδεκτά) σε σχέση με τον συνολικό αριθμό από τα αιτήματα που έχουν υποβληθεί για κάθε πείραμα. Επίσης μελετήσαμε τον χρόνο απόκρισης (το χρόνο από την στιγμή που ένα αίτημα υποβάλλεται μέχρι τη στιγμή που ο BBbase agent απαντά είτε με το να δεχθεί το αίτημα είτε να το απορρίψει) καθώς και το φόρτο δικτύου εξαιτίας το μηνυμάτων ελέγχου που ανταλλάσσονται μεταξύ BBbase και BBedge agents.

Τα αιτήματα στα πειράματα μας παρήχθησαν τυχαία από ένα ns-2 tcl script που χρησιμοποιούσε την μεταβλητή variable για να καθορίσει τον αριθμό των αιτημάτων που θα παραχθούν. Οι παράμετροι για κάθε αίτημα παράγονταν τυχαία μέσα στα κατάλληλα διαστήματα (όσον αφορά τη συνολική διάρκεια κάθε πειράματος, το συνολικά διαθέσιμο bandwidth, το ελάχιστο και το μέγιστο που μπορούσε να ζητήσει ένα αίτημα) για κάθε σενάριο που θέλαμε να προσομοιώσουμε. Έγινε η παραδοχή στα σενάρια που τρέξαμε ότι ένα αίτημα ήταν υποχρεωμένο να καθορίσει μία σταθερή τιμή για το bandwidth για μια συγκεκριμένη χρονική διάρκεια (δεν υπήρχε δηλαδή η δυνατότητα καθορισμού μεταβλητού μέγιστου ρυθμού bandwidth). Τα αιτήματα είχαν συγκεκριμένα χρονικά όρια όσο αφορά τη διάρκειά τους (χρόνος λήξης μείον χρόνος έναρξης), πολύ μικρότερο όριο από την συνολική διάρκεια του κάθε πειράματος, με σκοπό να αντισταθμίσουμε οποιεσδήποτε επιρροές έναρξης.

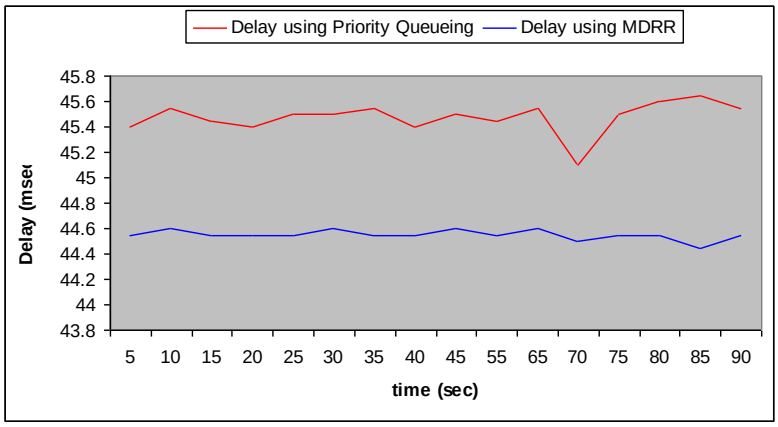
Η τυχαιότητα εξασφαλίστηκε από την χρήση της κλάσης RNG του ns-2, η οποία περιέχει μια υλοποίηση της πολλαπλής συνδυασμένης αναδρομικής γεννήτριας MRG32k3a. Η γεννήτρια MRG32k3a παρέχει 1.8×10^{19} ανεξάρτητες ροές τυχαίων αριθμών, κάθε μία από τις οποίες αποτελείται από 2.3×10^{15} υπο-ροές. Κάθε υπο-ροή έχει μια περίοδο (δηλαδή πλήθος τυχαίων αριθμών προτού επαναληφθούν) ίση με 7.6×10^{22}. Η περίοδος συνολικά της γεννήτριας είναι επομένως 3.1×10^{57}, πολύ

παραπάνω από αρκετή για να παράγουμε τυχαιότητα για τους σκοπούς μας. Πιο συγκεκριμένα, η γεννήτρια τυχαίων αριθμών παρήγαγε τιμές που ανατίθεντο σε κάθε ένα από τα χαρακτηριστικά ενός νέου αιτήματος. Αν ο τυχαίος συνδυασμός των χαρακτηριστικών δεν ήταν έγκυρος (αν για παράδειγμα ο χρόνος εκκίνησης ήταν υστερότερος του χρόνου λήξης της κράτησης) το αίτημα αγνοείτο σαν να μην είχε ποτέ δημιουργηθεί. Διαφορετικά αποστελλόταν από τον κόμβο στον Bandwidth Broker για εξέταση.

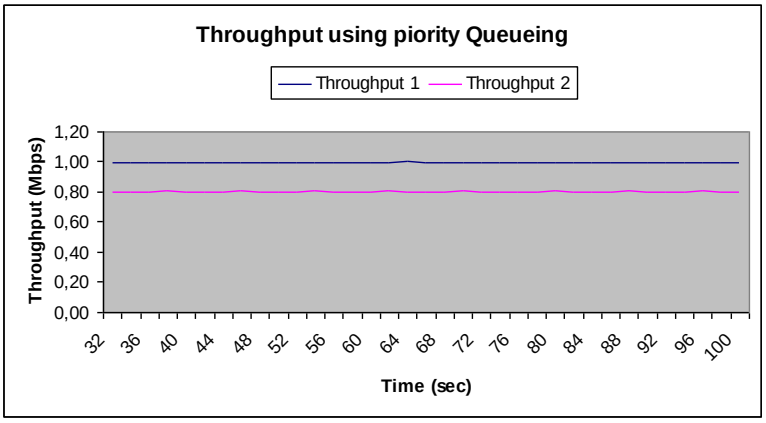
7.7.1 Εξετάζοντας και επικυρώνοντας την υπηρεσία QoS.

Ο bandwidth broker, όπως αναφέρθηκε πιο πάνω, έχει ρυθμιστεί να διαχειρίζεται την υπηρεσία QoS IP Premium. Η υπηρεσία χρησιμοποιεί την προτεραιότητα με ουρά(Queueing) ή τον αλγόριθμο MDRR(Modified Deficit Round Robin) σε κατάσταση αυστηρής προτεραιότητας και μηχανισμούς scheduling ουράς. Ο μηχανισμός ουράς με προτεραιότητα(Priority Queueing) μπορεί να παρέχει προτεραιότητες χρησιμοποιώντας μια ουρά προτεραιότητας ενώ άλλα πακέτα εξυπηρετούνται με την προεπιλεγμένη εξυπηρέτηση ουράς (First Come, First Served) όταν η ουρά προτεραιότητας είναι αδρανής. Ο MDRR είναι ένας πιο καινούριος αλγόριθμος scheduling που επιτρέπει τη ρύθμιση πολλών ουρών. Σε κατάσταση αυστηρής προτεραιότητας (strict priority mode) ο MDRR μπορεί να παρέχει απόλυτη προτεραιότητα στα πακέτα μιας μόνης ουράς, ενώ οι άλλες ουρές λειτουργούν εκ περιτροπής (round robin) μόνο όταν η ουρά προτεραιότητας είναι άδεια. Η διάρκεια εξυπηρέτησης κάθε ουράς ρυθμίζεται από συγκεκριμένες ιδιότητες(αποκαλούμενες κβάντο (quantum) και έλλειμμα (deficit)).

Στη συνέχεια, έγιναν δοκιμές επικύρωσης του Bandwidth broker στα υλοποιημένα μοντέλα όπου 2 πηγές έκαναν αίτηση για 1Mbps και 800Kbps αντίστοιχα. Συγκρίνοντας τα αποτελέσματα από τα πειράματα (Εικόνα 52) είναι προφανές ότι ο bandwidth broker διαχειρίζεται την υπηρεσία IP Premium πολύ καλά, είτε με MDRR είτε με τον μηχανισμό ουράς προτεραιότητας. Ο συνολικός όγκος(throughput) των εγκεκριμένων ροών ήταν ιδανικός και η καθυστέρηση ήταν υπερβολικά μικρή και στις 2 περιπτώσεις Priority Queuing έναντι MDRR. Η μόνη αξιοσημείωτη διαφορά είναι ότι η καθυστέρηση είναι λίγο μικρότερη όταν η υπηρεσία IP Premium παρέχεται χρησιμοποιώντας μηχανισμό MDRR. Τελικά, αφού ο μηχανισμός MDRR φαίνεται πιο ισχυρός και παρέχει μικρότερη καθυστέρηση από το Priority Queuing, αποφασίσαμε να χρησιμοποιήσουμε το μηχανισμό MDRR στις επόμενες εξομοιώσεις.



Delay (in msec)

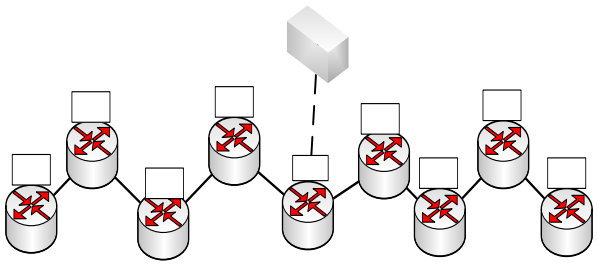


Συνολικό throughput

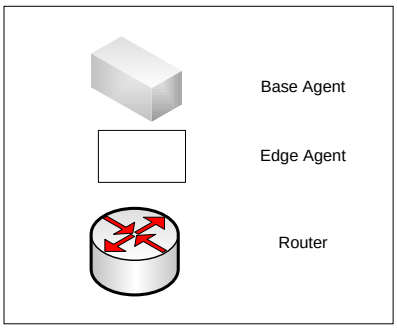
Εικόνα 52: Throughput και καθυστέρηση χρησιμοποιώντας Priority Queuing

7.7.2 Μελετώντας τις επιρροές του μεγέθους του buffer

Στο πρώτο μας πείραμα, μελετήσαμε πως οι απαιτήσεις για buffer του BBbase agent επηρεάζουν την ολική απόδοση και πιο συγκεκριμένα πως οι απαιτήσεις αυτές σχετίζονται με το ποσοστό των αιτημάτων που έγιναν αποδεκτά. Εξετάσαμε μόνο τα SDBB και PDBB μοντέλα αφού είναι τα μόνα που πρέπει να χρησιμοποιήσουν το δίκτυο για να ολοκληρώσουν την επεξεργασία ενός αιτήματος, ενώ τα κεντρικοποιημένα μοντέλα (CBB, CFBB) εκτελούν την επεξεργασία ενός αιτήματος εσωτερικά με αποτέλεσμα πιο γρήγορα και για αυτό έχουν πολύ μικρότερη ανάγκη για buffer. Η τοπολογία δικτύου που χρησιμοποιήθηκε για αυτό το πείραμα ήταν μία τοπολογία σε σειρά, με τον BBbase Agent τοποθετημένο στο κέντρο της τοπολογίας όπως φαίνεται στην Εικόνα 53.

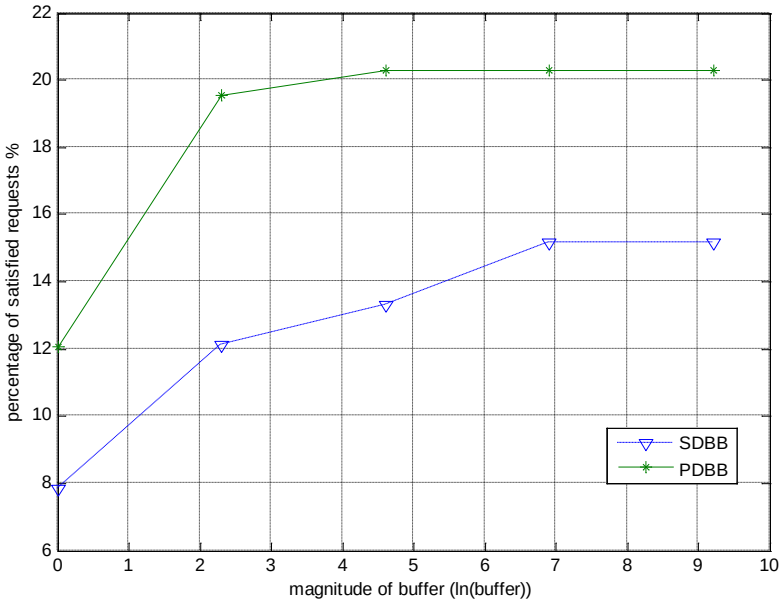


Εικόνα 53: Σειριακή τοπολογία



Εικόνα 54: Επεξήγηση συμβόλων

Ο buffer των αιτημάτων για τα SDBB και τα PDBB μοντέλα αποθηκεύει αιτήματα που δεν μπορούν να επεξεργαστούν αμέσως. Εάν ο χρόνος έναρξης του αιτήματος έχει περάσει και το αίτημα δεν έχει επεξεργαστεί, τότε το αίτημα απορρίπτεται.



Εικόνα 55: Ποσοστό αποδοχής vs μέγεθος του buffer (1ms καθυστέρηση γραμμής)

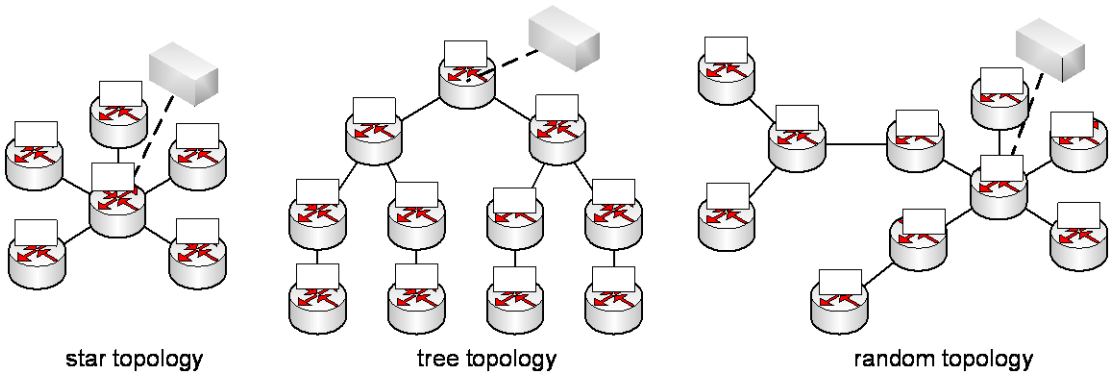
Ο οριζόντιος άξονας στην Εικόνα 55 απεικονίζει το μέγεθος του buffer σε λογαριθμική (ln) κλίμακα και ο κάθετος άξονας μετράει το ποσοστό των αιτημάτων

που έχουν γίνει αποδεκτά. Όταν δεν υπάρχει buffer (μηδενικό μέγεθος), υπάρχει μεγάλη αστοχία απόδοσης, ειδικά για το SDBB μοντέλο, αλλά χρησιμοποιώντας ένα buffer μεγέθους δέκα ή μεγαλύτερο, οι αρνητικές συνέπειες μειώνονται σημαντικά. Για το PDBB μοντέλο, αυτό σημαίνει ότι με την τοποθέτηση ενός πολύ μικρού buffer στους agents, κανένα αίτημα δεν χάνεται λόγω μη διαθεσιμότητας. Αυτό το συμπέρασμα μπορεί επίσης να ενισχυθεί από το γεγονός ότι σε παρόμοια πειράματα, τα CBB και CFBB μοντέλα επίσης παρουσιάζουν παρόμοια επίδοση (20% αιτήματα που έχουν ικανοποιηθεί). Για το SDBB μοντέλο, παρόλο που το buffer βελτιώνει την κατάσταση, η απόδοση ποτέ δεν φτάνει το ποσοστό απόδοσης των υπόλοιπων μοντέλων, εξαιτίας της γραμμικής και για αυτό αργής φύσης του SDBB μοντέλου. Ακόμα και αν το buffer πρακτικά γίνει άπειρο (για παράδειγμα, κανένα αίτημα δεν απορρίπτεται εξαιτίας της έλλειψης buffer space), η αργή λειτουργία του SDBB αναγκάζει πολλά αιτήματα να απορρίπτονται απλώς επειδή ο χρόνος έναρξης του αιτήματος έχει λήξει λόγω του χρόνου που πήρε στα αιτήματα για να εξεταστούν.

Οι γραμμές στο δίκτυο εξομοιώθηκαν με latency 1ms, που είναι ένας τυπικός αριθμός για μη τοπικά δίκτυα. Μεγαλύτερες τιμές καθυστέρησης θα είχαν, όπως φαίνεται από τα παραπάνω αποτελέσματα, καταστρεπτικές συνέπειες στην απόδοση του SDBB.

7.7.3 Αποτίμηση των αρχιτεκτονικών με τη χρήση διαφορετικών τοπολογιών

Για το κύριο σύνολο των πειραμάτων μας χρησιμοποιήσαμε έναν αριθμό από διαφορετικές τοπολογίες σε συνδυασμό με τη βασική τοπολογία. Οι υπόλοιπες τοπολογίες φαίνονται στην Εικόνα 56, και σχεδιάστηκαν έτσι ώστε όσα περισσότερα χαρακτηριστικά τοπολογίας δικτύου γίνεται, να συμπεριληφθούν και να ληφθούν υπόψη. Για παράδειγμα, ενώ η τοπολογία αστέρα ελαχιστοποιεί την απόσταση μεταξύ των BBbase και των BBedge agents, η τοπολογία δέντρου και η σειριακή τοπολογία την αυξάνουν και μεγεθύνουν την συνέπειά της στην απόδοση του Bandwidth Broker. Η τοπολογία δέντρου ξεχωρίζει κυρίως από την σειριακή (που είναι και αυτή τυπικά ένα δέντρο) στο ότι η σειριακή έχει τα πιο πιθανά bottlenecks από οποιαδήποτε άλλη τοπολογία, αφού τα περισσότερα αιτήματα πιθανότατα πρόκειται να ζητήσουν μέρος από τους πόρους των μεσαίων γραμμών. Τέλος, η τυχαία τοπολογία συνδυάζει χαρακτηριστικά και από τις τοπολογίες αστέρα, δέντρου και τη σειριακή τοπολογία με σκοπό να έχει ένα πιο ισορροπημένο σύνολο από αποτελέσματα. Για όλα τα πειράματα, εκτός και αν τονιστεί διαφορετικά, το latency των γραμμών ορίστηκε ίσο με 1ms.



Εικόνα 56: Επιπλέον τοπολογίες που χρησιμοποιήθηκαν για τα πειράματα

7.7.3.1 Overhead δικτύου

Ο Πίνακας 9 συνοψίζει το overhead δικτύου που προκαλείται από κάθε Bandwidth Broker μοντέλο για κάθε μία τοπολογία, υπολογισμένο από το μέσο αριθμό πακέτων που ανταλλάσσονται για κάθε αίτημα.

Εξαιτίας της κατανεμημένης φύσης τους, υπάρχει περισσότερο overhead δικτύου για τους SDBB, PDBB σε σύγκριση με τα CBB και CFBB μοντέλα, ειδικά για την σειριακή τοπολογία και για την τοπολογία δέντρου. Η διαφορά αυτή μειώνεται σημαντικά για την τοπολογία αστέρα, επειδή η τοπολογία αστέρα ταιριάζει περισσότερο στους υλοποιημένους αλγορίθμους των SDBB και PDBB μοντέλων. Σε όλες τις περιπτώσεις, το CFBB μοντέλο παρουσιάζει τη μέση εναλλακτική οδό για τα SDBB/PDBB και CBB μοντέλα.

Επίσης, αυτά τα πειράματα δείχνουν ότι το ολικό overhead δικτύου επηρεάζεται από την τοπολογία και από την θέση του BBbase agent συνδυαζόμενο από την κατανομή των QoS αιτημάτων κατά μήκος των δικτυακών κόμβων. Είναι ένα ήδη γνωστό πρόβλημα που αντιμετωπίζεται με τη μελέτη της τοπολογίας, την κατανομή της χρήσης QoS και γι' αυτό συστήνεται η εφαρμογή μιας περιοδικής βέλτιστης επιλογής του κόμβου που θα φιλοξενήσει των BBbase agent.

Μοντέλο \ Τοπολογία	**Σειριακή (Serial)**	**Αστέρα (Star)**	**Δέντρου (Tree)**	**Τυχαία (Random)**
SDBB	7.65	4.76	7.39	5.99
PDBB	9.68	4.92	9.92	6.61
CBB	2.01	1.70	1.94	1.90
CFBB	3.66	2.44	3.63	3.01

Πίνακας 9: Overhead δικτύου (μέσος όρος αριθμών πακέτου ανά αίτημα)

7.7.3.2 Ρυθμός αποδοχής αιτημάτων

Ο Πίνακας 10 δείχνει το ποσοστό αποδοχής ανά μοντέλο για κάθε τοπολογία. Όλα τα μοντέλα επωφελούνται από την τοπολογία αστέρα και παράγουν καλύτερα αποτελέσματα. Ο λόγος είναι ότι οι γραμμές είναι κατά μέσο όρο λιγότερο φορτωμένες στην τοπολογία αστέρα από ότι στις υπόλοιπες τοπολογίες, όπου εμφανίζονται γραμμές με bottleneck.

Μοντέλο \ Τοπολογία	**Σειριακή (Serial)**	**Αστέρα (Star)**	**Δέντρου (Tree)**	**Τυχαία (Random)**
SDBB	0.1514	0.2216	0.1699	0.2012
PDBB	0.2029	0.2227	0.2171	0.2130
CBB	0.2035	0.2259	0.2088	0.2106
CFBB	0.2060	0.2323	0.2083	0.2118

Πίνακας 10: Ρυθμός αποδοχής (ρυθμός αποδοχής των αιτημάτων που υποβλήθηκαν)

Γενικά οι διαφορές μεταξύ των μοντέλων είναι μάλλον μικρές, εκτός από το SDBB μοντέλο το οποίο, ειδικά για τοπολογίες με μεγαλύτερες κατά μέσο όρο αποστάσεις, παρουσιάζει σημαντικά χειρότερη συμπεριφορά από τα υπόλοιπα μοντέλα. Οι μεγάλες του καθυστερήσεις που παρουσιάζει στην απάντηση των αιτημάτων προκαλούν σε πολλά από αυτά, να έχουν λήξει την χρονική στιγμή που οδηγούνται προς επεξεργασία. Αυτό φαίνεται και από τον μέσο όρο των χρόνων απόκρισης που παρέχονται στον Πίνακας 12. Κατά την διάρκεια των πειραμάτων μας, αποφασίσαμε να ερευνήσουμε το κατά πόσο το να εξαναγκάσουμε τους χρήστες να υποβάλλουν αιτήματα με ένα ελάχιστο όριο στο advance time (μια ελάχιστη χρονική περίοδο από τη στιγμή που ένα αίτημα υποβλήθηκε στη στιγμή στην οποία οι ζητούμενοι πόροι πρέπει να δεσμευτούν) θα βοηθούσε το SDBB να ξεπεράσει το πρόβλημα του περιορισμένου ρυθμού αποδοχής αιτημάτων. Παρόλα αυτά, εξαιτίας των μεγάλων χρόνων απόκρισης σε σύγκριση με τα άλλα μοντέλα, ο ρυθμός άφιξης των αιτημάτων στο SDBB buffer είναι μεγαλύτερος από τον ρυθμό επεξεργασίας (με δεδομένο ένα σταθερό ρυθμό εισερχομένων αιτημάτων, όπως στα πειράματά μας). Γι' αυτό, το SDBB μοντέλο πάντα σταδιακά θα αποτυγχάνει να επεξεργαστεί κάποια αιτήματα έγκαιρα (πριν τη χρονική στιγμή που η κράτησή τους θα ξεκινούσε).

Εξαιτίας της έλλειψης πιθανών bottleneck γραμμών, η τοπολογία αστέρα επιτρέπει το μεγαλύτερο ποσοστό αιτημάτων που θα γίνουν αποδεκτά. Από τη στιγμή που γενικά η τοπολογία πρόκειται να είναι σταθερή και η μόνη ρεαλιστική επιλογή πρόκειται να γίνει ανάμεσα στα Bandwidth Broker μοντέλα, ο Πίνακας 10 προτείνει ότι για μια τυχαία τοπολογία το SDBB μοντέλο είναι το μόνο που φαίνεται μη αποδοτικό, ενώ τα υπόλοιπα παρουσιάζουν παρόμοια συμπεριφορά, που υπονοεί ότι αυτή είναι μάλλον η καλύτερη συμπεριφορά που μπορεί κανείς να περιμένει, στερούμενος τη χρήση τη χρήση πιο πολύπλοκων admission control αλγορίθμων ή πιο πολύπλοκης τοποθέτησης του BBbase agent.

Με σκοπό την περαιτέρω μελέτη της επίδρασης του latency, επαναλάβαμε τα πειράματα για τα SDBB/PDBB μοντέλα με latency 10ms. Τέτοιο latency θα μπορούσε να εξομοιώσει έναν Bandwidth Broker που λειτουργεί σε ένα domain που καλύπτει απομακρυσμένες περιοχές, όπως για παράδειγμα ένα εθνικό δίκτυο. Όπως μπορούμε να δούμε από τα αποτελέσματα που παρουσιάζει ο Πίνακας 11, αυτή η αύξηση του latency έχει επιβλαβείς συνέπειες στην απόδοση των κατανεμημένων μοντέλων. Αυτό μας οδηγεί στο συμπέρασμα ότι για Bandwidth Brokers που λειτουργούν σε domain ευρείας περιοχής, η κεντρικοποιημένη προσέγγιση έχει το πλεονέκτημα απέναντι στην κατανεμημένη, τουλάχιστον όσο αφορά τις διαδικασίες που αφορούν το admission control που χρησιμοποιήθηκαν από τα μοντέλα που περιγράφηκαν.

Μοντέλο \ Τοπολογία	**Σειριακή (Serial)**	**Αστέρα (Star)**	**Δέντρου (Tree)**	**Τυχαία (Random)**
SDBB	0.0201	0.1263	0.0265	0.0366
PDBB	0.0515	0.2099	0.0714	0.0861

Πίνακας 11: Ρυθμός αποδοχής για latency 10ms

7.7.3.3 Η απόκριση χρόνου των μοντέλων

Ο Πίνακας 12 παρουσιάζει τους κατά μέσο όρο χρόνους απόκρισης για όλα τα μοντέλα σε εξεταζόμενες τοπολογίες. Οι χρόνοι απόκρισης για το SDBB μοντέλο

είναι τάξεις μεγέθους μεγαλύτεροι από τους υπόλοιπους, που εξηγεί την κατώτερη απόδοση στην μέτρηση που έγινε για το ρυθμό αποδοχής και εκφράζει την ακαταλληλότητα που έχει ως μοντέλο για όλες τις περιπτώσεις με εξαίρεση τις πιο βολικές (για παράδειγμα, τοπολογία αστέρα).

Μοντέλο \ Τοπολογία	**Σειριακή (Serial)**	**Αστέρα (Star)**	**Δέντρου (Tree)**	**Τυχαία (Random)**
SDBB	1919	4.077	1325	314.3
PDBB	22.19	2.520	9.382	6.041
CBB	5.502	1.597	4.097	2.879
CFBB	5.502	1.597	4.097	2.879

Πίνακας 12: Χρόνος απόκρισης σε msec (ο μέσος χρόνος που πέρασε μέχρι τη στιγμή που η απάντηση επιστρέφει στο αποστολέα αιτήματος)

Με σκοπό την καλύτερη κατανόηση της ακριβούς επίδρασης των αριθμών που παρουσιάζει ο Πίνακας 12, υπολογίσαμε επίσης την τυπική απόκλιση (standard deviation) των χρόνων απόκρισης, την οποία παρουσιάζει ο Πίνακας 13. Τα αποτελέσματα αυτά δείχνουν ότι οι χρόνοι απόκρισης του SDBB όχι μόνο είναι πολύ μεγαλύτεροι από τους υπόλοιπους των άλλων μοντέλων κατά μέσο όρο, αλλά επίσης έχουν πολύ μεγαλύτερη διακύμανση. Σε όλες τις περιπτώσεις, τα CBB και CFBB μοντέλα είναι πανομοιότυπα όπως αναμένεται, από τη στιγμή που οι διαδικασίες επεξεργασίας αιτημάτων είναι ακριβώς ίδιες.

Μοντέλο \ Τοπολογία	**Σειριακή (Serial)**	**Αστέρα (Star)**	**Δέντρου (Tree)**	**Τυχαία (Random)**
SDBB	757	2.180	591.7	224.1
PDBB	19.83	1.485	6.404	4.726
CBB	2.576	0.8128	2.176	1.770
CFBB	2.576	0.8128	2.176	1.770

Πίνακας 13: Τυπική απόκλιση του χρόνου απόκρισης (10^{-3})

Η κοντινή γειτνίαση των κόμβων στον BBbase agent στην τοπολογία αστέρα ευνοεί το PDBB κατανεμημένο μοντέλο, γεγονός που μειώνει τη διαφορά με τα CBB/CFBB κεντρικοποιημένα μοντέλα. Αλλά και για τις υπόλοιπες τοπολογίες ο χρόνος απόκρισης παραμένει το πολύ 2-4 φορές μεγαλύτερος από το χρόνο των CBB\CFBB μοντέλων, που μπορεί να είναι μια λογική εξισορρόπηση για τα κατανεμημένα πλεονεκτήματα του PDBB μοντέλου.

7.8 ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ ΤΟΥ BANDWIDTH BROKER

Εξετάζοντας τον αλγόριθμο αποδοχής, ένα πιθανό μειονέκτημα είναι ότι οι αποφάσεις για μια αίτηση που έχει γίνει σε ένα δοθέντα χρόνο περιλαμβάνουν το μονοπάτι δρομολόγησης. Το τελευταίο μπορεί να προκαλέσει μερικές απορρίψεις αιτήσεων, σε περίπτωση που οι δικτυακοί πόροι δεν έχουν κρατηθεί με ένα ισορροπημένο τρόπο έτσι ώστε να επιτρέπουν ελεύθερους πόρους σε όλες τις συνδέσεις αν αυτό είναι

πιθανό λαμβάνοντας υπόψη εναλλακτικά μονοπάτια. Αυτό το πρόβλημα μπορεί να λυθεί τρέχοντας ένα αλγόριθμο βελτιστοποίησης όταν το δίκτυο πλησιάζει μη ισορροπημένες καταστάσεις (για παράδειγμα όταν δεσμευμένοι πόροι σε μια σύνδεση ξεπερνούν ένα συγκεκριμένο κατώφλι ~ 80% των διαθέσιμων πόρων). Αυτός ο αλγόριθμος βελτιστοποίησης μπορεί να τρέχει περιοδικά, να ξαναρυθμίζει κάποιες αιτήσεις που έγιναν δεκτές χρησιμοποιώντας εναλλακτικά μονοπάτια με τις ίδιες εγγυήσεις και να εξετάζει ξανά τις απορριπτέες αιτήσεις. Ένας τέτοιος αλγόριθμος βελτιστοποίησης θα πρέπει να χρησιμοποιεί χαρακτηριστικά traffic engineering με τη χρήση MPLS και άλλων προχωρημένων μηχανισμών που έχουν προταθεί [77].

7.8.1 Ένα μοντέλο επιλογής κόμβου Bandwidth Broker

Ένα άλλο σημαντικό σημείο στη λειτουργία του κατανεμημένου bandwidth broker είναι να αποφασίσει ποιος κόμβος θα φιλοξενήσει τον bandwidth broker agent. Πολλές ερευνητικές ομάδες έχουν ασχοληθεί με το θέμα της βέλτιστης τοποθέτησης κρίσιμων εφαρμογών στο δίκτυο [82]. Όσον αφορά τον bandwidth broker, το πρόβλημα αυτό είναι πιο πολύπλοκο εξ' αιτίας του γεγονότος ότι η χρήση του δεν είναι τυποποιημένη και εξαρτάται από τις εγκαταστάσεις του χρήστη.

Προσπαθήσαμε να προσεγγίζουμε το πρόβλημα εξετάζοντας ένα μοντέλο επιλογής κόμβου που εξετάζει τους κόμβους, τις γειτονικές συνδέσεις και προσπαθεί να βρει τον καλύτερο κόμβο για να τοποθετήσει τον base bandwidth broker. Με άλλα λόγια, το πρόβλημα είναι να βρεθεί η ρίζα του γραφήματος, όπου η ρίζα είναι ο πιο σημαντικός κόμβος στο δίκτυο και έτσι τα περισσότερα πακέτα για τη λειτουργία του bandwidth broker θα τον φτάσουν γρήγορα. Το προτεινόμενο μοντέλο χωρίζεται σε 2 φάσεις και πρέπει να τρέχει σειριακά.

Φάση 1

Η φάση 1 προσπαθεί να αξιολογήσει τη σημαντικότητα του κάθε κόμβου στο δίκτυο και τελικά αναθέτει ένα βάρος σε όλους τους κόμβους.

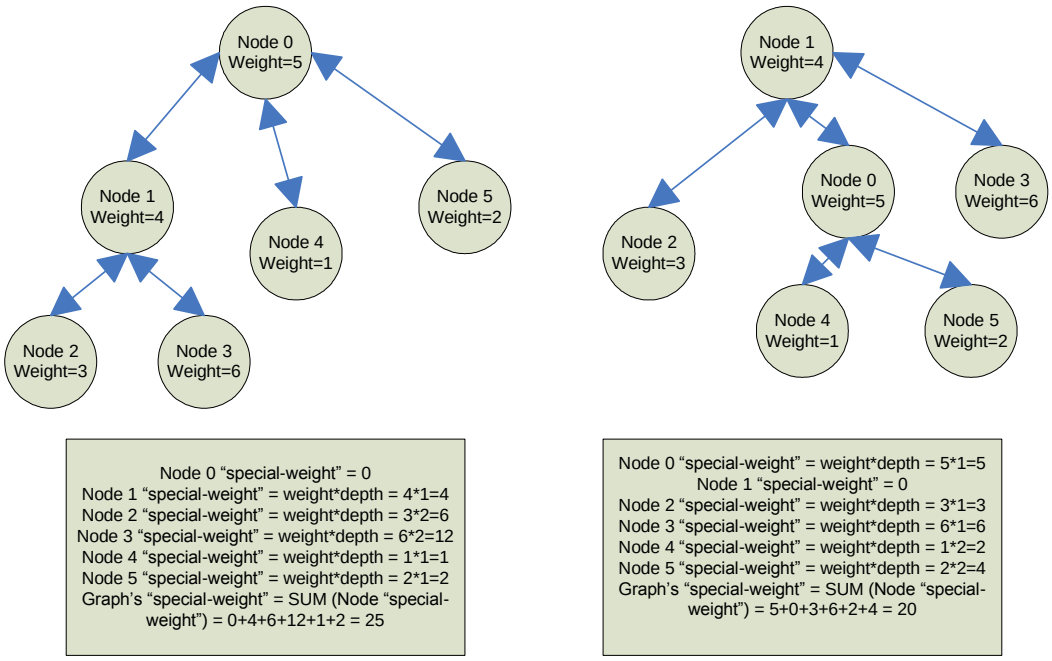
Η αξιολόγηση βασίζεται στα παρακάτω κριτήρια.

- Στον αριθμό των διεπαφών πρόσβασης(access interfaces) σε αυτό τον κόμβο και την αντίστοιχη κίνηση που αυτές οι διεπαφές εισάγουν στο δίκτυο.
- Στην ωριμότητα και στις δυνατότητες του εξοπλισμού του κόμβου να χειριστεί την κίνηση.
- Στο ρόλο του κόμβου στο σχήμα δρομολόγησης. Το κριτήριο σχετίζεται με τη δικτυακή τοπολογία και δείχνει πόσο σημαντικό είναι ο κόμβος στη λειτουργία του δικτύου (για παράδειγμα, σε μια τοπολογία αστέρα, η ρίζα είναι ο κρίσιμος κόμβος).
- Σημείο διασύνδεσης(interconnection point). Τελικά, ένας κόμβος έχει ένα σημαντικό ρόλο αν είναι το σημείο διασύνδεσης με ένα μεγαλύτερο δίκτυο κορμού και αποτελεί ιεραρχική ομοσπονδία.

Φάση 2

Στη φάση 2, για κάθε κόμβο, δημιουργούμε το γράφημα δρομολόγησης που σημαίνει ότι τοποθετούμε κάθε κόμβο σαν ρίζα και δημιουργούμε όλα τα μονοπάτια σε όλους

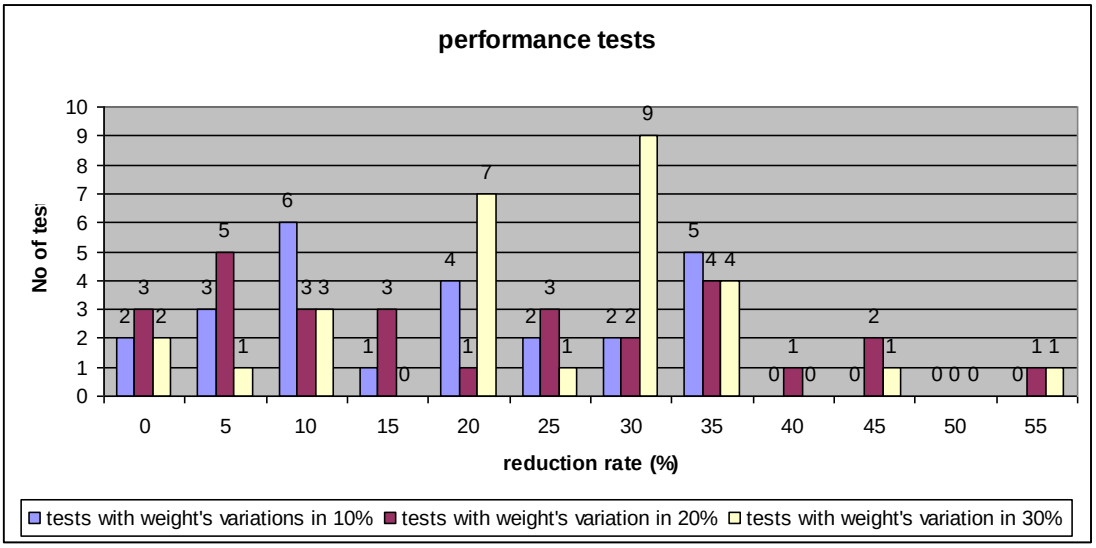
τους άλλους κόμβους, χρησιμοποιώντας το τρέχον δικτυακό σχήμα δρομολόγησης. Άρα, υπάρχουν N γραφήματα (όπου N είναι ο αριθμός των κόμβων στο δίκτυο) και πρέπει να εξεταστεί. Τότε, για κάθε γράφημα, υπολογίζουμε το συνολικό κόστος που μορφοποιείται σαν το άθροισμα του κόστους για κάθε κόμβο να επικοινωνήσει με τη ρίζα. Αυτό το επικοινωνιακό κόστος προκύπτει από το βάρος του κόμβου πολλαπλασιασμένο με το βάθος του στο γράφημα. Τέλος, το πρόβλημα είναι να βρούμε το γράφημα με το ελάχιστο συνολικό κόστος.



Εικόνα 57: Οι καλύτερες 2 τοποθεσίες για τον κόμβο BBbase

Στη συνέχεια προσπαθήσαμε να εξομοιώσουμε το παραπάνω μοντέλο και να μετρήσουμε την ακρίβειά του. Η ιδέα της εξομοίωσης ήταν να βρούμε τις καλύτερες 2 τοποθεσίες για τον base bandwidth broker σε μια δεδομένη δικτυακή τοπολογία και στις 2 αυτές περιπτώσεις να γίνουν τυχαίες αιτήσεις σχετικά με τα βάρη τους. Μετρήσαμε τον χρόνο εκτέλεσης, με την υπόθεση ότι επηρεάζεται κυρίως από την μετάδοση πακέτων. Πρώτα, υπολογίσαμε το ποσοστό επιτυχίας επιλογής του κατάλληλου κόμβου για base bandwidth broker, όπως αυτό καθορίζεται από το χρόνο εκτέλεσης (σημαίνει ότι μετρήσαμε για κάθε αίτηση αν ο επιλεγμένος κόμβος ή ο εναλλακτικός (2η επιλογή) είναι πιο αποδοτικός). Η εξομοίωση έγινε με 50 επαναλήψεις από 100 τυχαίες αιτήσεις και το αποτέλεσμα δείχνει ότι το ποσοστό επιτυχίας (σε σύγκριση με το μείζον υποψήφιο κόμβο) ήταν μεταξύ 90 και 96%.

Στη συνέχεια προσπαθήσαμε να δούμε πόσο ελαστικό είναι το μοντέλο σύμφωνα με τα κριτήρια. Το σύνολο των τεστ έγινε με 30 επαναλήψεις από 100 τυχαίες αιτήσεις, ενώ χρησιμοποιούσαμε 10%,20% και 30% διακύμανση στα βάρη των κόμβων. Σε αυτή την περίπτωση, παρατηρήσαμε ότι η μέση μείωση του χρόνου εκτέλεσης που μετρήσαμε (του καλύτερου κόμβου από τον υποψήφιο) είναι 8.2%, 22% και 26% για διακύμανση βαρών 10%, 20% και 30% αντίστοιχα. Επίσης, η Εικόνα 58 δείχνει την κατανομή της μείωσης του χρόνου εκτέλεσης. Άρα, το μοντέλο φαίνεται να βελτιώνει την απόδοση του μοντέλου PDDB, που είναι ανεκτικό στον υπολογισμό βαρών.



Εικόνα 58: η κατανομή της μείωσης του χρόνου εκτέλεσης μεταξύ βέλτιστης επιλογής υποψηφίου κόμβου

7.9 ΛΕΙΤΟΥΡΓΙΑ INTERDOMAIN

Γενικά, ένας bandwidth broker πρέπει να μπορεί να επικοινωνεί με γειτονικά domains που δουλεύουν σε μια ιεραρχία ή σύνδεση ομότιμων(peer connection), έτσι ώστε να εξυπηρετηθούν αιτήσεις για υπηρεσίες QoS από άκρο σε άκρο. Σε αυτή την περίπτωση, ειδικό provisioning και επικοινωνία απαιτείται έτσι ώστε να επιτευχθεί η απαραίτητη συνεργασία (inter-working). Αλλά το θέμα με τη μεγαλύτερη πρόκληση είναι η διερεύνηση το μονοπατιού από το domain πηγής στο domain προορισμού. Ένας bandwidth broker πρέπει να υπολογίσει το «καλύτερο» μονοπάτι από την πηγή στον προορισμό διαμέσου ενδιάμεσων domains, λαμβάνοντας υπόψη και τα πιθανά SLAs μεταξύ domains. Το μονοπάτι πρέπει τελικά να ακολουθηθεί, χρησιμοποιώντας traffic engineering μηχανισμούς. Πολλοί ερευνητές έχουν μελετήσει θέματα traffic engineering σε intra-domain και inter-domain λειτουργία των bandwidth brokers[75][76][77][79]. Σε αυτό το τμήμα της εργασίας, συζητάμε 2 μοντέλα που προσεγγίζουν traffic engineering(εύρεση μονοπατιού(pathfinding)) από άκρο σε άκρο σε λειτουργία interdomain.

7.9.1 Προσεγγίσεις με εύρεση μονοπατιού

7.9.1.1 Κεντροποιημένο μοντέλο εύρεσης μονοπατιού

Το πρώτο καλείται κεντρικοποιημένο και σύμφωνα με αυτό το μοντέλο, η απόφαση για τη δρομολόγηση της αίτησης, συγκεκριμένα στα domains και στα εσωτερικά μονοπάτια που η κίνηση θα διασχίσει για να φτάσει το domain προορισμού γίνεται από το domain πηγής. Για να πάρει αυτή την απόφαση, ένα κεντρικό σύστημα provisioning είναι απαραίτητο, που θα διατηρεί την τοπολογία, το peering (τα SLA μεταξύ ISPs) και τεχνολογικές πληροφορίες. Συγκεκριμένα, τα domains που παίρνουν μέρος σε αυτό το μοντέλο, ανακοινώνουν την τοπολογία τους και την κατάσταση

πόρων σε ένα κοινό δικτυακό πληροφοριακό σύστημα (NIS) που χρησιμοποιείται για τη λειτουργία του bandwidth broker. Όλα τα domains πρέπει να διατηρούν τις σχετικές πληροφορίες σε αυτό το σύστημα συγχρονισμένες. Αλλιώς, ο bandwidth broker θα δουλεύει με μη-έγκυρα δεδομένα και μπορεί να οδηγήσει σε λανθασμένα μονοπάτια και κρατήσεις. Η υλοποίηση τέτοιων συστημάτων είναι ανοικτό θέμα και πολλές προσεγγίσεις έχουν παρουσιαστεί [76][77][78].

Αφού έχει σταλεί μια αίτηση, το domain πηγής «κάνει ερωτήσεις» ρωτώντας για τους αιτούμενους πόρους στα μονοπάτια. Ακολουθεί τη διαδικασία σειριακά μέχρι να βρει όλα τα μονοπάτι από την πηγή στον προορισμό που έχουν οι αιτούμενοι πόροι. Στη συνέχεια αποφασίζει ποιο μονοπάτι είναι το καλύτερο, σύμφωνα με κριτήρια που έχουν καθοριστεί στην πολιτική του bandwidth broker. Τα κριτήρια θα πρέπει να καθορίζονται από τα domains και πρέπει να υποδεικνύουν το κόστος που έχουν για να παρέχουν τους πόρους.

Το κεντρικοποιημένο μοντέλο εύρεσης μονοπατιού μπορεί να παραλληλιστεί με τη λειτουργία RSVP-Traffic engineering πρωτόκολλο σε ένα μόνο διαχειριζόμενο domain [76]. Το RSVP-TE σε ένα ενεργό MPLS domain παρέχει στο δίκτυο πόρους και δίνει μονοπάτια Label Switched (που μπορούν να χρησιμοποιήσουν τους πόρους) χρησιμοποιώντας ποικίλα κριτήρια επιλογής στην περίπτωση πολλών υποψήφιων μονοπατιών. Γενικά είναι κοντά στο κεντρικοποιημένο μοντέλο εύρεσης μονοπατιού αλλά δεν εφαρμόζεται, αφού το μοντέλο interdomain διασχίζει ανεξάρτητα τα διαχειριζόμενα δίκτυα και έτσι η λειτουργία από άκρο σε άκρο ενός RSVP-TE δεν είναι δυνατή. Επίσης, το RSVP-TE λειτουργεί μόνο κατά το χρόνο εκτέλεσης των δικτυακών συσκευών και η λειτουργία δεν μπορεί να εξαχθεί για χρήση σε offline ή συμπληρωματικά εργαλεία. Επιπλέον, η ίδια λειτουργία μπορεί να επιτευχθεί μέσω άλλων προσεγγίσεων που έχουν προταθεί [76], αλλά έχουν και πάλι τον περιορισμό ότι χάνεται η ελευθερία του κάθε domain(αφού ανακοινώνει την τοπική του πολιτική) ή χρειάζεται κοινούς δικτυακούς μηχανισμούς που δεν μπορούν να εφαρμοστούν ανεξάρτητα σε διαχειριζόμενα δίκτυα.

7.9.1.2 Κατανεμημένο μοντέλο εύρεσης μονοπατιού

Το δεύτερο μοντέλο είναι «από ομότιμο σε ομότιμο» και σε αυτή την περίπτωση η υπηρεσία εύρεσης μονοπατιού του domain πηγής προωθεί τις αιτήσεις που έχουν προορισμό σε άλλο domain σε κάθε γειτονικό domain, υπό την προϋπόθεση ότι υπάρχουν διαθέσιμοι πόροι από την πηγή στα αντίστοιχα σημεία εξόδου. Στη συνέχεια, κάθε domain που λαμβάνει μήνυμα ελέγχει αν είναι το domain προορισμού ή ένα ενδιάμεσο. Στην περίπτωση ενδιάμεσου domain, ο εξυπηρετητής bandwidth broker ελέγχει αν μπορεί να εγγυηθεί τους αιτούμενους πόρους από το σημείο εισόδου στο σημείο εξόδου σε όλα τα άλλα domain που έχει σύνδεση. Αν υπάρχουν οι απαραίτητοι πόροι, τότε το μήνυμα εκπέμπεται στο επόμενο domain. Για να αποφευχθούν οι βρόχοι, όταν ένα domain λαμβάνει μια αίτηση, ελέγχει τον συνδυασμό του αριθμού ακολουθίας της αίτησης και του σημείου εισόδου του domain που το έλαβε. Αν αυτός ο συνδυασμός έχει ήδη επεξεργαστεί, το domain απορρίπτει την αίτηση. Όταν φτάσει στο domain προορισμού ο εξυπηρετητής bandwidth broker αυτού του domain ελέγχει τους αιτούμενους πόρους από το σημείο εισόδου που έλαβε το μήνυμα μέχρι τον προορισμό. Αυτή η διαδικασία επαναλαμβάνεται και τελικά όλες οι πιθανές διαδρομές ανάμεσα στην πηγή και στον προορισμό βρίσκονται και δηλώνονται στο domain πηγής. Τότε, το domain πηγής αποφασίζει την καλύτερη δρομολόγηση σύμφωνα με συγκεκριμένα κριτήρια που

έχουν καθοριστεί στο μοντέλο εύρεσης μονοπατιού. Σε περίπτωση που δεν υπάρχουν μονοπάτια με τους αιτούμενους πόρους λόγω περιορισμών του SLA, το μοντέλο μπορεί να ζητήσει κάποια επαναδιαπραγμάτευση του SLA μεταξύ των domains και να πάρει μια τελική απόφαση, Επίσης, σε περίπτωση που ο προορισμός δεν μπορεί να προσεγγιστεί λόγω βλάβης του δικτύου, το module μπορεί να βρεθεί σε αδιέξοδο, αφού δεν υπάρχουν μονοπάτια επιστροφής, ούτε απορριπτέα εξαιτίας ανεπαρκών πόρων. Έτσι το module πρέπει να έχει ένα χρονιστή λήξης και σε περίπτωση που λήξει μια περίοδος, το module υποθέτει ότι ο προορισμός δεν μπορεί να προσεγγιστεί.

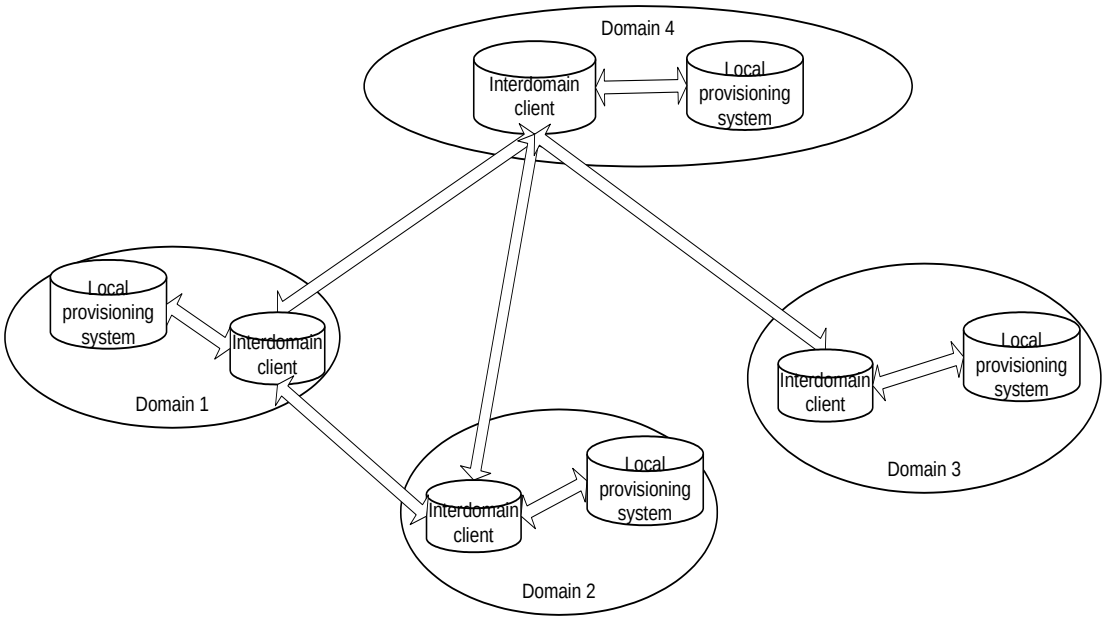
Η πολυπλοκότητα αυτού του κατανεμημένου module εύρεσης μονοπατιού είναι μεγάλη και η απόδοσή του εξαρτάται από την τρέχουσα τοπολογία μεταξύ των domains όπου το module εφαρμόζεται. Στην πραγματικότητα, το πρόβλημα στηρίζεται στην Αναζήτηση κατά Εύρος (BFS) σε ένα γράφημα, όπου μορφοποιείται σε κάθε αίτημα και χρησιμοποιεί σαν ρίζα το domain πηγής [84]. Η χρονική πολυπλοκότητα του αλγορίθμου BFS είναι ανάλογη του αριθμού των κορυφών συν τον αριθμό των ακμών στα γραφήματα που διασχίζει.

Επιπρόσθετα, ένα πολύ σημαντικό θέμα σε όλη την λειτουργία του κατανεμημένου μοντέλου είναι ο ορισμός κριτηρίων που πρέπει να εφαρμοστούν στα επιλεγμένα μονοπάτια (αν το μοντέλο παρέχει περισσότερα από ένα(έτσι ώστε να αποφασίσει ποιο είναι το καλύτερο. Το προτεινόμενο μοντέλο χρησιμοποιεί ένα συνδυασμό από κριτήρια που είναι τα ελάχιστα hops, η ελάχιστη εκπλήρωση του SLA και το συνολικό κόστος του μονοπατιού. Το συνολικό κόστος είναι το άθροισμα από τα κόστη όλων των domain στο μονοπάτι. Πρέπει να είναι χρονικά ανεξάρτητο έτσι ώστε να μην περιπλέκει περισσότερο την διαδικασία υπολογισμού μονοπατιού. Ο σκοπός αυτού του τύπου είναι να αποφασίσει το βέλτιστο μονοπάτι από τα διαθέσιμα ενώ κάνει εξισορρόπηση φόρτου (load balancing) και έχει μικρό κόστος σύμφωνα με την εγκατάσταση του domain. Το μοντέλο, όπως έχει περιγραφεί, υποθέτει συμμετρικό SLA στη μετάδοση και στη λήψη μεταξύ των domain, αλλά λειτουργεί και με ασύμμετρα SLA.

Για να υλοποιηθεί αυτό το μοντέλο, πρέπει κάθε domain να έχει την ελευθερία να χρησιμοποιήσει οποιοδήποτε εργαλείο provisioning για το δίκτυο του ανοικτού κώδικα ή ιδιωτικό. Οι μόνες απαιτήσεις είναι η υλοποίηση όλου του module που θα παρέχει το συγχρονισμό της λειτουργίας και μια κοινή μορφή των δεδομένων που παρέχει κάθε domain. Επιπρόσθετα, αυτή η μορφή προτείνεται να βασίζεται σε XML αφού το module εύρεσης μονοπατιού μπορεί να λειτουργήσει χρησιμοποιώντας web services. Ένα παράδειγμα XML μηνύματος για την κατανεμημένη εύρεση μονοπατιού παρουσιάζεται στην Εικόνα 59. Επιπλέον, η Εικόνα 60 περιγράφει την αρχιτεκτονική του μοντέλου σε περιβάλλον interdomain.

```
<pathfinding-message>
  <request-sequence-number>DATA</request-sequence-number>
  <domain>DATA</domain>
  <ingress_point>DATA</ingress_point>
  <outgress_point>DATA</outgress_point>
  <resources>DATA</resources>
  <cost>DATA<cost>
  <destination_reached>YES/NO</destination_reached>
  <other-domain-data>DATA</other-domain-data>
</pathfinding- message >
```

Εικόνα 59: Παράδειγμα XML μηνύματος για το module εύρεσης μονοπατιού



Εικόνα 60: Μια interdomain προσέγγιση κατανεμημένης εύρεσης μονοπατιού

7.9.1.3 Σύγκριση

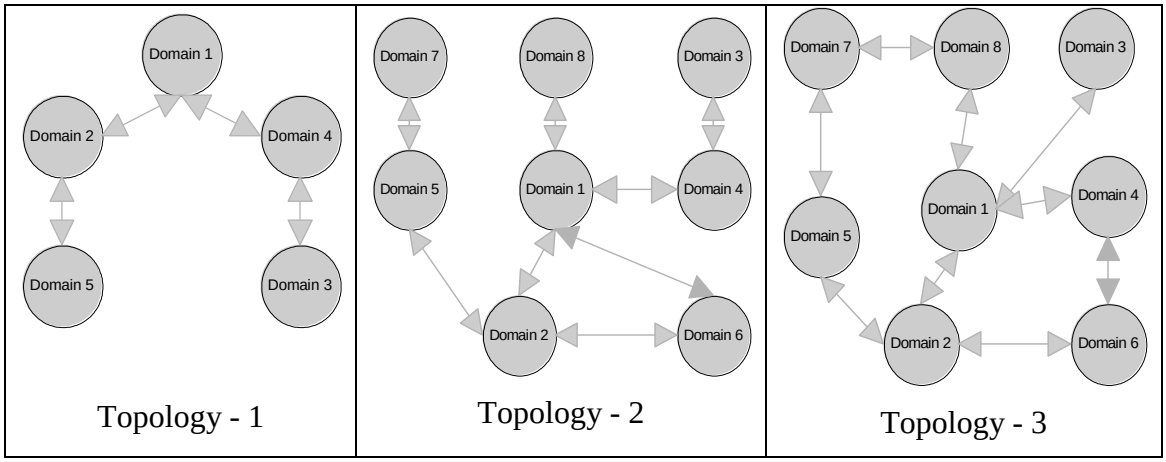
Και τα 2 μοντέλο (κεντρικοποιημένο και κατανεμημένο) χρειάζονται ενημερωμένες πληροφορίες για την κατάσταση του δικτύου και την πολιτική του. Ο πρώτος αλγόριθμος απαιτεί κάθε domain να ανακοινώνει αυτήν την πληροφορία κεντρικά, όπου όλα τα άλλα domain «ρωτούν» το κεντρικό σύστημα έτσι ώστε να επεξεργάζεται inter-domain αιτήματα. Ο δεύτερος αλγόριθμος αφαιρεί αυτό το βήμα (ανακοίνωση της κατάστασης του δικτύου και λειτουργία), καθορίζοντας ότι ο εξυπηρετητής του bandwidth broker κάθε domain πρέπει να απαντά για τα πιθανά μονοπάτια με διαθέσιμους πόρους. Έτσι η λειτουργία κάθε δικτύου παραμένει εσωτερική και κάθε αίτηση που μπορεί να περάσει υπόκειται σε επεξεργασία από τον bandwidth broker του domain μόνο. Από την άλλη, ο δεύτερος αλγόριθμος έχει μεγαλύτερη πολυπλοκότητα και επίσης χρειάζεται περισσότερο χρόνο να απαντήσει σε μια αίτηση αφού όλα τα πιθανά μονοπάτια θα πρέπει να ελεγχθούν μέσα από μια αναζήτηση που μοιάζει με BFS ρωτώντας τους bandwidth brokers των domain. Έτσι, ο χρόνος απόκρισης του module εύρεσης μονοπατιού περιλαμβάνει την καθυστέρηση μετάδοσης των αιτήσεων για εύρεση μονοπατιού ανάμεσα στους bandwidth broker των domain και το χρόνο εκτέλεσης τοπικά σε κάθε domain. Ο πρώτος αλγόριθμος έχει ένα μεγάλο πλεονέκτημα σε αυτό το θέμα, αφού όλη η πληροφορία για όλα τα domain και τη λειτουργία τους είναι αποθηκευμένη τοπικά σε μια βάση δεδομένων και άρα όλα τα εναλλακτικά μονοπάτια δρομολόγησης μπορούν να βρεθούν ψάχνοντας το καινούριο γράφημα που παράγεται προσθέτοντας την τοπολογία όλων των domain, τους διαθέσιμους πόρους καθώς και τα SLA μεταξύ γειτονικών domain.

Συμπερασματικά, ο πρώτος αλγόριθμος έχει καλύτερο χρόνο απόκρισης αλλά χρειάζεται να ανακοινώσει εσωτερικές πληροφορίες περιοδικά ώστε να κρατήσει το καθολικό «σύστημα provisioning» ενημερωμένο. Αυτή η απαίτηση εισάγει πληθώρα προβλημάτων ασφάλειας και κλιμάκωσης, κάτι που κάνει αυτή τη λύση ανέφικτη. Ο δεύτερος αλγόριθμος φυλάει αυτή την εσωτερική πληροφορία κρυμμένη αλλά η διαδικασία κάθε αίτησης δεσμεύει όλους τους bandwidth broker όλων των εμπλεκόμενων domain. Αφού αυτή η λειτουργία πρέπει να υλοποιηθεί σε

ανεξάρτητους διαχειριστικά κόμβους, το δεύτερο μοντέλο (κατανεμημένο) είναι πιο κατάλληλο λόγω του γεγονότος ότι κρατά την ανεξαρτησία της διαχείρισης και της τοπικής πολιτικής σε ένα domain.

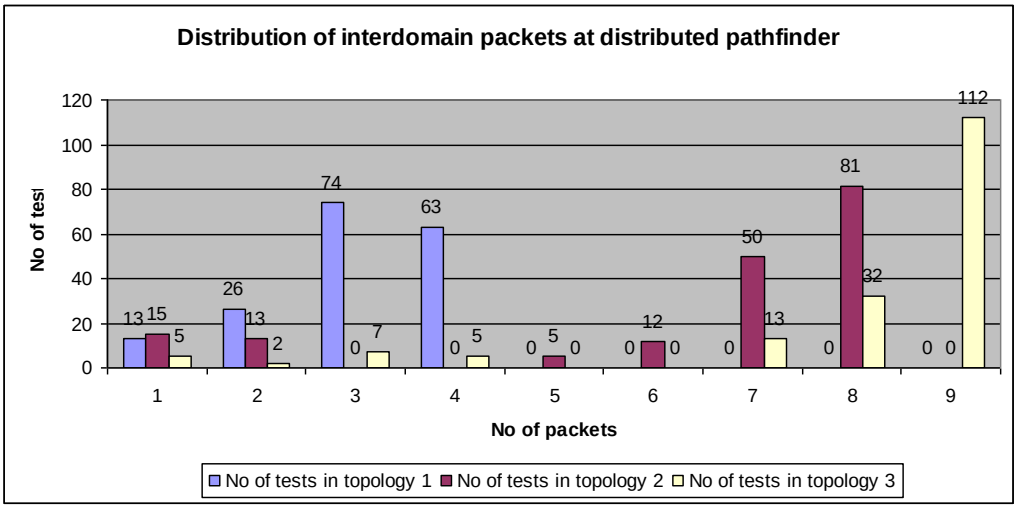
7.9.2 Εξομοίωση εύρεσης μονοπατιών

Για να μελετήσουμε περισσότερο το module κατανεμημένης εύρεσης μονοπατιών, εξομοιώσαμε την λειτουργία και εκτελέσαμε το μοντέλο χρησιμοποιώντας 170 τυχαίες αιτήσεις μεταξύ των domain στις 3 τοπολογίες που παρουσιάζονται στην Εικόνα 61. Οι μετρήσεις που προσπαθήσαμε να πάρουμε είναι τα ανταλλαγμένα "interdomain" πακέτα ανά αίτηση, όπως υποδεικνύει ο συνολικός χρόνος απόκρισης, που χρησιμοποιεί την υπόθεση ότι ο χρόνος απόκρισης κάθε bandwidth broker κάθε domain είναι περίπου ίδια. Σύμφωνα με τα αποτελέσματα (βλέπε Σχήμα 9), ο αριθμός των πακέτων που χρειάζεται να ανταλλάξει το module εύρεσης μονοπατιών είναι σχετικά μικρός και εξαρτάται από τη συνολική τοπολογία και την τοποθεσία στην τοπολογία της πηγής και του προορισμού σε κάθε αίτηση. Το σχήμα παρουσιάζει τα ανταλλαγμένα πακέτα μεταξύ των domain και όχι των εσωτερικών πακέτων σε κάθε domain(αν υπάρχουν), αφού εξαρτάται στην υπηρεσία provisioning που κάθε domain πρέπει να επιλέξει για να χρησιμοποιήσει. Μετά το module εύρεσης μονοπατιών, ο αλγόριθμος επιστρέφει τα διαθέσιμα μονοπάτια που φτάνουν το domain προορισμού (και τα χαρακτηριστικά τους), περιμένοντας για την τελική απόφαση για το προτιμητέο μονοπάτι που θα παραχθεί μετά τη ρύθμιση των κριτηρίων εύρεσης μονοπατιού. Η συνολική διαδικασία αίτησης θα τελειώσει όταν το κατάλληλο μονοπάτι έχει επιλεχθεί και τα σχετικά domain έχουν πληροφορηθεί να κρατήσουν τους πόρους και να κάνουν τις απαραίτητες ρυθμίσεις στις δικτυακές συσκευές.



Εικόνα 61: Οι εξομοιωμένες domain τοπολογίες

Συγκρίνοντας τα αποτελέσματα για τα απαραίτητα πακέτα (επικοινωνία0 για εύρεση μονοπατιού σε 3 τοπολογίες, παρατηρούμε ότι ο μέσος αριθμός πακέτων που ανταλλάσσονται αυξάνει αναλογικά με την πολυπλοκότητα της τοπολογίας (και συγκεκριμένα όταν περιέχει πολλές συνδέσεις που οδηγούν σε κύκλους). Το αποτέλεσμα αυτό ήταν αναμενόμενο εξαιτίας του γεγονότος ότι το κατανεμημένο module εύρεσης μονοπατιού βασίζεται στον αλγόριθμο BFS.



Εικόνα 62: Η κατανομή των ανταλλασσόμενων πακέτων για το module εύρεσης μονοπατιού

ΚΕΦΑΛΑΙΟ 8: ΣΥΜΠΕΡΑΣΜΑΤΑ

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην διδακτορική αυτή διατριβή εξετάστηκε η αυτοματοποιημένη παροχή ποιότητας υπηρεσίας σε σύγχρονα δίκτυα δεδομένων. Μελετήσαμε ακόμα την ανάπτυξη μηχανισμών και αλγορίθμων για την αποδοτική διαχείριση των πόρων, τον όσο το δυνατόν δίκαιο καταμερισμό της ποιότητας υπηρεσίας, καθώς και τη δυνατότητα συνεργασίας και διαλειτουργικότητας μεταξύ διαφορετικών αυτόνομων δικτυακών τμημάτων με αυτοματοποιημένο τρόπο (χωρίς δηλαδή να χρειάζεται η παρέμβαση ενός ανθρώπου διαχειριστή στις περισσότερες περιπτώσεις). Αναλύθηκαν διάφορες προσεγγίσεις που έχουν προταθεί όσον αφορά bandwidth brokers, ενώ προτάθηκαν αλγόριθμοι και μηχανισμοί για τη βελτίωση της λειτουργίας και της απόδοσής τους.

Η σημασία της υποστήριξης Ποιότητας Υπηρεσίας (QoS) για IP κίνηση καταδεικνύεται από το γεγονός ότι όλο και περισσότερες συσκευές αποκτούν ικανοποιητική επεξεργαστική ισχύ και διασυνδέονται στο διαδίκτυο διακινώντας όγκο πληροφορίας με ετερογενή χαρακτηριστικά και ανάγκες ποιότητας. Η ανάγκη αυτή για υποστήριξη ποιότητας υπηρεσίας γίνεται επιτακτικότερη για IPv6 κίνηση, δεδομένου ότι το πρωτόκολλο IPv6 συνυπάρχει και αντικαθιστά σιγά σιγά το IPv4, επιλύοντας το πρόβλημα των περιορισμένων διευθύνσεων. Παράλληλα οι ευρυζωνικές τεχνολογίες προσεγγίζουν τον τελικό χρήστη, και σε συνδυασμό με την εμφάνιση εφαρμογών όλο και πιο απαιτητικών από άποψη δικτυακών πόρων καθίσταται επίσης αναγκαία η υποστήριξη κάποιου είδους Ποιότητας Υπηρεσίας.

Οι δοκιμές που διεξαγάγαμε, σε πραγματικό περιβάλλον και με ρεαλιστική κίνηση, μας οδηγούν στο συμπέρασμα ότι οι σημαντικότεροι κατασκευαστές δικτυακού εξοπλισμού υποστηρίζουν σε ικανοποιητικό βαθμό μηχανισμούς QoS και συγκεκριμένα την ανάπτυξη DiffServ αρχιτεκτονικών πάνω από δίκτυα διπλής στοίβας (με ταυτόχρονη υποστήριξη IPv4 και IPv6). Το IPv6 εισάγει μια σταθερή, αλλά ελαφρά μεγαλύτερη επικεφαλίδα, η οποία οδηγεί στην εμφάνιση μιας μικρής επιπλέον επιβάρυνσης. Αυτό σε συνδυασμό με τον διαφορετικό ενδεχομένως τρόπο υλοποίησης των σχετικών μηχανισμών από τους κατασκευαστές δικτυακού εξοπλισμού όσον αφορά το IPv6, μας δίνει σε ορισμένες περιπτώσεις ελαφρά διαφορετική συμπεριφορά σε σχέση με το IPv4. Παρόλα αυτά, οι QoS υπηρεσίες υποστηρίζονται σε ικανοποιητικό βαθμό ώστε να μπορεί να θεωρηθεί αρκετά ώριμη για υλοποίηση QoS πάνω από IPv6 υπηρεσιών παραγωγής.

Στην παρούσα εργασία έγινε ένας ολοκληρωμένος σχεδιασμός υπηρεσιών QoS που εστιαζόταν στο Εθνικό Δίκτυο Έρευνας και Τεχνολογίας που διασυνδέει τα ακαδημαϊκά και ερευνητικά κέντρα της χώρας καλύπτοντας τις ανάγκες τους για διασύνδεση και ποιότητα υπηρεσίας είτε μεταξύ τους είτε με το εξωτερικό διαμέσου του Πανευρωπαϊκού Ακαδημαϊκού Δικτύου Geant2. Οι υλοποιημένες υπηρεσίες είναι οι IP Premium (με τις υποπεριπτώσεις της), η LBE και η MBS. Οι παραπάνω υπηρεσίες σχεδιάστηκαν, μελετήθηκαν και αξιολογήθηκαν στο δίκτυο, όπου επιβεβαιώθηκε η ορθότητα και η καλή απόδοσή τους. Επίσης, ο σχεδιασμός τους ήταν τέτοιος που ήταν απόλυτα συμβατές και διαλειτουργικές με τις αντίστοιχες του Geant2.

Στην παρούσα εργασία κάναμε επίσης μια ανασκόπηση των υπαρχόντων προτάσεων και αρχιτεκτονικών για την αυτοματοποιημένη παροχή εγγυήσεων ποιότητας υπηρεσίας. Διάφοροι οργανισμοί όπως οι ETSI, MSF, IETF έχουν προτείνει αρχιτεκτονικές που προσεγγίζουν την ιδέα του Bandwidth Broker. Μία σειρά επίσης

από ερευνητικά έργα ασχολούνται με το αντικείμενο αυτό και ερευνούν την παροχή εγγυημένης χωρητικότητας (στο επίπεδο 2) ή εγγυήσεις ποιότητας στο επίπεδο 3. Επίσης εξετάζουν σε ρεαλιστικές συνθήκες τη δυνατότητα αυτοματοποιημένης διαχείρισης των διαθέσιμων πόρων και τις δυνατότητες συνεργασίας μεταξύ πολλαπλών domains. Η σχετική εργασία στους Bandwidth Brokers καλύπτει πολλών ειδών αρχιτεκτονικές, με κεντρικοποιημένα και κατανεμημένα μοντέλα λειτουργίας μέσα σε ένα domain, οι οποίες υποστηρίζουν άμεσα ή προκαταβολικά αιτήματα από χρήστες ή εφαρμογές. Ο έλεγχος αποδοχής είναι ένα από τα σημαντικότερα θέματα που αντιμετωπίζεται με διάφορες τεχνικές και μπορεί να υλοποιηθεί με απλές ή περισσότερο πολύπλοκες δομές δεδομένων για καλύτερη διαχείριση της μνήμης και πιο αποδοτική λειτουργία.

Στα πλαίσια της εργασίας μας, σχεδιάστηκε και υλοποιήθηκε ένας bandwidth broker που αποσκοπούσε στην μοντελοποίηση και διαχείριση των QoS υπηρεσιών που σχεδιάστηκαν στο δίκτυο του ΕΔΕΤ. Ο bandwidth broker βασίστηκε σε κεντρικοποιημένη αρχιτεκτονική και εκτελεί τις ακόλουθες εργασίες: μοντελοποίηση δικτύου, εφαρμογή του μοντέλου διαστασιολόγησης στην τρέχουσα κατάσταση, αποδοχή κλήσης QoS αιτημάτων, παραγωγή παραμέτρων ρύθμισης για τις δικτυακές συσκευές, παρακολούθηση λειτουργίας QoS στο δίκτυο, επικοινωνία με αντίστοιχους bandwidth brokers σε γειτονικά domains και πλήρη διαχείριση των αιτημάτων QoS. Επιπλέον, δεδομένου ότι οι ανάγκες των εφαρμογών για QoS αυξάνονται, πρέπει να δίνεται μεγαλύτερη ευελιξία μια QoS σηματοδοσία. Για το λόγο αυτό στα πλαίσια της εργασίας αυτής μελετήθηκε και υλοποιήθηκε μια εφαρμογή αυτόματης σηματοδοσίας χρησιμοποιώντας το ευρέως γνωστό πρωτόκολλο δρομολόγησης BGP. Το αποτέλεσμα είναι να επιτυγχάνεται δυναμική σηματοδοσία για αυτόματη παροχή ποιότητας υπηρεσίας σε ένα δίκτυο μέσω μιας διεπαφής που βασίζεται σε Web service ή σε μια Βάση Δεδομένων. Ο bandwidth broker αυτός σχεδιάστηκε να «επικοινωνεί» με τους αντίστοιχους των άλλων Ευρωπαϊκών χωρών και του Geant, αποτελώντας το $1^{ο}$ χρονικά σε λειτουργία σύστημα καθώς και το $1^{ο}$ διαλειτουργικό σύστημα με τα αναπτυσσόμενα στο Geant.

Επίσης, στα πλαίσια της εργασίας μας μελετήθηκαν θεωρητικά και υλοποιήθηκαν σε προσομοιωτές και αξιολογήθηκαν σε συγκριτικά πειράματα μιας σειρά από QoS μηχανισμούς στη βάση της αρχιτεκτονικής DiffServ. Στη συνέχεια, μελετήθηκαν κατανεμημένες αρχιτεκτονικές bandwidth broker όπου έγιναν υλοποιήσεις σε επίπεδο εξομοίωσης. Αρχικά υλοποιήθηκαν ή επεκτάθηκαν οι υλοποιήσεις των μηχανισμών QoS στον εξομοιωτή και δημιουργήθηκε και δοκιμάστηκαν QoS σενάρια. Στη συνέχεια υλοποιήθηκαν παραλλαγές bandwidth broker που ακολουθούσαν κεντρικοποιημένες και κατανεμημένες αρχιτεκτονικές. Στόχος της μελέτης ήταν να μελετηθεί το trade-off στη λειτουργία τους και να συσχετιστεί με τις εκάστοτε δικτυακές συνθήκες. Οι πειραματικές αξιολογήσεις κατέδειξαν πως στις κατανεμημένες αρχιτεκτονικές, η λειτουργία και απόδοση του bandwidth broker εξαρτάται σημαντικά από την τοπολογία του δικτύου, από την διαμόρφωση - διάρθρωση του bandwidth broker πάνω στη τοπολογία και από την κατανομή των υποβληθέντων QoS αιτημάτων. Με αφορμή το παραπάνω συμπέρασμα, στα πλαίσια της εργασίας αυτής μελετήθηκε ένας αλγόριθμος προσαρμογής ενός κατανεμημένου bandwidth broker ώστε να επιλέγεται η βέλτιστη διαμόρφωσή του στο δίκτυο (με βάση τις συνθήκες δικτύου) με στόχο την ταχύτερη απόκριση - απόδοση.

Εξετάστηκε ακόμα ο τρόπος επέκτασης της λειτουργίας σε επίπεδο πολλαπλών αυτόνομων δικτυακών τμημάτων (domains), ο οποίος απαιτεί την κατάλληλη σηματοδότηση και ανταλλαγή πληροφορίας για τη συνεργασία των αντίστοιχων

μονάδων διαφορετικών domains. Ένα βασικό κριτήριο διαπιστώθηκε πως είναι το πώς θα γίνει η δρομολόγηση για την από άκρο σε άκρο κράτηση. Η από άκρο σε άκρο δρομολόγηση που απαιτεί πλήρη γνώση της εσωτερικής τοπολογίας κάθε domain είναι μια αποδοτική αλλά όχι πρακτικά εφικτή λύση. Ακόμα και αν οι διαχειριστές των domain είναι διατεθειμένοι να μοιραστούν τέτοια πληροφορία, η ανανέωση και η χρήση της γίνεται μια πολύπλοκη διαδικασία. Για το σκοπό αυτό μελετήθηκαν 2 μοντέλα και δοκιμάστηκαν πειραματικά σε επίπεδο εξομοίωσης, δίνοντας έμφαση σε θέματα αυτονομίας διαχείρισης στο εσωτερικό κάθε ανεξάρτητου domain και στην τήρηση των SLAs μεταξύ γειτονικών domains. Το πρώτο μοντέλο βασιζόταν σε ένα κεντρικό σύστημα provisioning όπου όλα τα domains ανακοίνωναν υποχρεωτικά πληροφορίες λειτουργίας τους. Το δεύτερο μοντέλο ήταν ένα peer-peer μοντέλο μεταξύ ομότιμων οντοτήτων όπου με ανταλλαγή πολλαπλών signaling πακέτων και χρήση αναζήτησης παρόμοιας με BFS προσπαθεί να εξάγει τα δυνατά μονοπάτια και να αποφασίσει λαμβάνοντας υπόψη διάφορες παραμέτρους όπως κόστος, SLAs κλπ. Η απόδοση του μοντέλου αυτού που προτάθηκε, μελετήθηκε πειραματικά μέσω ενός προγράμματος εξομοίωσης.

Το περιβάλλον υλοποίησης που αναπτύχθηκε ειδικά για τους σκοπούς της αξιολόγησης των αλγορίθμων στα πλαίσια της εργασίας αυτής μας έδωσε τη δυνατότητα να εξετάσουμε τους εναλλακτικούς αλγορίθμους σε ένα αρκετά υψηλό (αφαιρετικό) επίπεδο, απομονώνοντας τις σχετικές με την χαμηλότερου επιπέδου υλοποίηση λεπτομέρειες. Επίσης η υλοποίησή του έγινε έχοντας ως πρωταρχικό στόχο την ευκολία χρησιμοποίησης και υλοποίησης αλγορίθμων, με αποτέλεσμα την εύκολη και ευέλικτη δοκιμή, τροποποίηση και αρχική αξιολόγηση των προτεινόμενων και των υπαρχόντων αλγορίθμων.

Η υλοποίηση των αλγορίθμων στο περιβάλλον προσομοίωσης ns-2 έδωσε τη δυνατότητα για ακόμα καλύτερη και βαθύτερη αξιολόγηση, προσομοιώνοντας ένα πλήρες δικτυακό περιβάλλον σε επίπεδο πακέτων. Ο προσομοιωτής ns-2 διαθέτει ευρεία υποστήριξη καθώς είναι το πιο συχνά χρησιμοποιούμενο εργαλείο δικτυακής προσομοίωσης στην ερευνητική κοινότητα, και διαθέτει μεγάλη ποικιλία από προσθήκες για την προσομοίωση διαφόρων ειδών δικτύων, τεχνολογιών και περιβαλλόντων. Αυτό κάνει τον προσομοιωτή ns-2 ένα ελκυστικό περιβάλλον για τη δοκιμή δικτυακών τεχνολογιών και αρχιτεκτονικών πριν τη δοκιμή τους σε πραγματικές συνθήκες. Σχετικά με τον εξομοιωτή NS-2, αναπτύξαμε και λειτουργικότητα που δεν υπήρχε στις τρέχουσες διανομές (για αλγορίθμους ή μηχανισμούς QoS) που έχουν αποδοθεί προς χρήση στην ακαδημαϊκή κοινότητα μέσω patches που διατίθενται από την ιστοσελίδα του εργαστηρίου και της ιστοσελίδας του NS.

Όσον αφορά την κατανομή των λειτουργικοτήτων του Bandwidth Broker, καταλήξαμε στο ότι η κατανεμημένη αρχιτεκτονική μπορεί να προσφέρει έναν αριθμό από πλεονεκτήματα σε σχέση με την κεντρικοποιημένη προσέγγιση. Επιπλέον, η κατανομή των μονάδων του Bandwidth Broker βοηθά το δίκτυο να αντιμετωπίσει έναν αριθμό από προβλήματα και αστοχίες διαφόρων βαθμών σοβαρότητας.

Οι ιδέες και οι προτάσεις που εξετάστηκαν στα πλαίσια αυτής της διδακτορικής διατριβής έχουν χρησιμοποιηθεί σαν βάση για την ερευνητική εργασία άλλων ομάδων οι οποίες δοκιμάζουν τα αντίστοιχα μοντέλα για είδη δικτύων όπως τα ασύρματα δίκτυα, με την αυξημένη ανάγκη εγγυήσεων ποιότητας και το δυνητικά μεγάλο αριθμό χρηστών που μπορούν να κάνουν χρήση της υπηρεσίας.

Ακόμα, το ενδιαφέρον για σχετικές αρχιτεκτονικές είναι έντονο σε μια σειρά από ερευνητικά προγράμματα που διερευνούν τη δυνατότητα αυτοματοποιημένης παροχής εγγυήσεων ποιότητας υπηρεσίας σε μεγάλο δυνητικά αριθμό χρηστών για συνδέσεις από άκρο σε άκρο που διασχίζουν πολλαπλά αυτόνομα δικτυακά τμήματα. Τα πλέον σχετικά με το αντικείμενο της εργασίας παρουσιάστηκαν στα πλαίσια της διατριβής αυτής, ενώ ελπίζουμε πως και η παρούσα εργασία θα συνεισφέρει στην περαιτέρω ερευνητική δραστηριότητα στον τομέα αυτό.

ΚΕΦΑΛΑΙΟ 9: ΜΕΛΛΟΝΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΛΟΝΤΙΚΗ ΕΡΓΑΣΙΑ

Η έντονη ερευνητική δραστηριότητα που αναπτύσσεται στους τομείς της αυτοματοποιημένης παροχής από άκρο σε άκρο Ποιότητας Υπηρεσίας (QoS) στο επίπεδο 3 αλλά και σε χαμηλότερο επίπεδο, δημιουργεί μια σειρά από ενδιαφέροντα πιθανά θέματα μελλοντικής εργασίας και ερευνητικής αναζήτησης στους τομείς που εξετάστηκαν στα πλαίσια της συγκεκριμένης διδακτορικής διατριβής. Το έντονο ερευνητικό ενδιαφέρον αποδεικνύεται από το πλήθος των σχετικών ακαδημαϊκών και ερευνητικών δραστηριοτήτων που διεξάγονται στο σχετικό αντικείμενο.

Βασικό πεδίο έρευνας αποτελεί σήμερα η εξασφάλιση της επικοινωνίας μεταξύ πολλαπλών, ετερογενών αυτόνομων δικτυακών τμημάτων ώστε να παρουσιάζεται μια συνεχής και ολοκληρωμένη εικόνα της υπηρεσίας στο χρήστη. Η έννοια του Bandwidth Broker είναι κεντρική όσον αφορά την περίπτωση των υπηρεσιών επιπέδου 3 (επίπεδο δικτύου), ενώ οι επεκτάσεις της έννοιας μπορούν να καλύψουν και γενικότερες περιπτώσεις υπηρεσιών που δεν περιορίζονται στην υποστήριξη μηχανισμών QoS στο επίπεδο 3.

Στην κατεύθυνση των θεμάτων που διαπραγματεύτηκαν στη διδακτορική αυτή διατριβή, υπάρχουν μια σειρά από συγκεκριμένα θέματα που σκοπεύουμε να διερευνήσουμε περαιτέρω, και τα οποία αναφέρονται σε συντομία παρακάτω. Ειδικότερα, θα εστιάσουμε στην επέκταση της μελέτης των αρχιτεκτονικών Bandwidth Broker για interdomain επικοινωνία, με έμφαση στην επιλογή κατάλληλων μονοπατιών και επαναφοράς από αστοχίες μέσω μεγαλύτερης κλίμακας προσομοιώσεων. Επίσης θα μελετήσουμε θέματα σχετικά με τη διασφάλιση της ορθής λειτουργίας του Bandwidth Broker, με τη δυνατότητα προστασίας από προβληματικές μονάδες του Bandwidth Broker, από μη «υπάκουους» clients καθώς και από χαμένα ή αλλοιωμένα μηνύματα κατά τη μετάδοσή τους στο δίκτυο.

Επιπλέον, με την ταχεία εισβολή των οπτικών δικτύων, η διαμορφωμένη τάση είναι οι υπηρεσίες QoS να μεταφέρονται ή να επεκτείνονται με υπηρεσίες χαμηλότερου επιπέδου (δυναμικά lightpaths κλπ) και για το σκοπό αυτό σχεδιάζονται και υλοποιούνται τέτοιο αυτόματοι μηχανισμοί. Επίσης, οι υπάρχουσες υπηρεσίες θα επεκταθούν με επόμενης γενιάς control plane μηχανισμούς. Για το σκοπό αυτό, αντικείμενο μελλοντικής εργασίας είναι η μελέτη των σχετικών μηχανισμών επόμενης γενιάς (που περιγράφουμε συνοπτικά παρακάτω) σε συνδυασμό με τις υπάρχουσες αρχιτεκτονικές bandwidth broker για το σχεδιασμό αποδοτικότερων υπηρεσιών QoS και βέλτιστης διαχείρισης.

9.1 ΕΠΟΜΕΝΗΣ ΓΕΝΙΑΣ ΜΗΧΑΝΙΣΜΟΙ ΟΠΤΙΚΩΝ ΔΙΚΤΥΩΝ

Η ITU-T αναπτύσσει δύο μοντέλα για οπτικά control-plane ανεξάρτητα πρωτοκόλλου, τα Automatic Switched Transport Network (G.ASTN) και Automatic Switched Optical Network (G.ASON). Το G.ASTN περιγράφει τις ανεξάρτητες από τεχνολογία απαιτήσεις επιπέδου δικτύου του control-plane για αυτόματης μεταγωγής δίκτυα μεταφοράς, ενώ το G.ASON περιγράφει την αρχιτεκτονική για αυτόματης μεταγωγής οπτικά δίκτυα. Καθώς είναι ανεξάρτητα πρωτοκόλλου, το Generalized

Multiprotocol Label Switching (GMPLS) και άλλα πρωτόκολλα μπορούν να ταιριάξουν μέσα στο πλαίσιο αυτό.

Η IETF έχει ορίσει μια ευρεία γκάμα από πρωτόκολλα για το GMPLS. Το GMPLS επεκτείνει τα δοκιμασμένα πρωτόκολλα σηματοδότησης και δρομολόγησης του MPLS στα οπτικά δίκτυα και επιτρέπει τη δυναμική διαλειτουργικότητα control-plane για SDH/SONET, wavelength, fibre και port-switched δικτυακά στοιχεία, δηλαδή δικτυακά στοιχεία που κάνουν μεταγωγή όχι σε επίπεδο πακέτου αλλά και στα παρακάτω επίπεδα του δικτύου. Το πρότυπο προτείνει ένα ενοποιημένο οπτικό control plane μεταξύ των διαφόρων αυτών στοιχείων που θα επιτρέπουν στους παροχείς υπηρεσιών να δημιουργούν, διαχειρίζονται και επιβλέπουν υπηρεσίες από άκρο σε άκρο.

9.1.1 G-MPLS

Η αρχιτεκτονική G-MPLS [85][86][87] αποτελεί τη γενίκευση του MPLS ενώ σε μερικές περιπτώσεις μπορεί να διαφέρει ελαφρώς από το MPLS. Η αρχιτεκτονική αυτή καλύπτει τα βασικά στοιχεία κατασκευής που χρειάζονται για ένα συνεπές επίπεδο ελέγχου για πολλαπλά επίπεδα μεταγωγής. Η αρχιτεκτονική αυτή χωρίζει το επίπεδο ελέγχου από το επίπεδο προώθησης. Επίσης χωρίζει σε δύο μέρη το επίπεδο ελέγχου σε επίπεδο σηματοδότησης (signaling) που περιλαμβάνει τα πρωτόκολλα σηματοδότησης και το επίπεδο δρομολόγησης που περιλαμβάνει τα πρωτόκολλα δρομολόγησης.

Το GMPLS διαφέρει από το παραδοσιακό MPLS στο ότι υποστηρίζει πολλαπλούς τύπους μεταγωγής, δηλαδή παρέχει επιπλέον υποστήριξη για TDM, λάμδα και fiber μεταγωγή. Η υποστήριξη επιπλέον τύπων μεταγωγής έχει οδηγήσει το GMPLS στο να επεκτείνει συγκεκριμένες βασικές λειτουργίες του παραδοσιακού MPLS και σε μερικές περιπτώσεις να προσθέσει λειτουργικότητα. Οι αλλαγές αυτές και οι προσθήκες έχουν επίδραση στις βασικές ιδιότητες των LSPs: το πως τα labels ζητούνται και επικοινωνούν, η μη κατευθυνόμενη φύση των LSP, το πως τα λάθη διαδίδονται και το πως η πληροφορία παρέχεται για το συγχρονισμό των ingress και egress LSR.

Η MPLS αρχιτεκτονική ορίστηκε για να υποστηρίζει τα δεδομένα που προωθούνται με βάση ένα label. Ένα κύκλωμα μπορεί να εγκατασταθεί μόνο μεταξύ, ή διαμέσου, interfaces του ιδίου τύπου. Ανάλογα με τη συγκεκριμένη τεχνολογία που χρησιμοποιείται για κάθε interface, διαφορετικά ονόματα κυκλωμάτων μπορούν να χρησιμοποιηθούν, για παράδειγμα SDH κύκλωμα, οπτική γραμμή, light-path και άλλα. Στα πλαίσια του GMPLS, όλα αυτά τα κυκλώματα αναφέρονται με ένα κοινό όνομα: Label Switched Path (LSP).

Η ιδέα του εμφωλευμένου LSP (LSP μέσα σε LSP), ήδη διαθέσιμη στο παραδοσιακό MPLS, διευκολύνει τη δημιουργία μια ιεραρχίας προώθησης, για παράδειγμα μια ιεραρχία από LSP. Η ιεραρχία αυτή μπορεί να συμβεί στο ίδιο interface ή μεταξύ διαφορετικών interfaces. Η εμφώλευση μπορεί να συμβεί και μεταξύ διαφορετικών τύπων από interfaces.

Το GMPLS επίπεδο ελέγχου φτιάχνεται από διάφορα blocks. Αυτά τα κατασκευαστικά blocks στηρίζονται σε γνωστά πρωτόκολλα σηματοδότησης και δρομολόγησης που έχουν επεκταθεί ή/και αλλαχθεί για να υποστηριχτεί το GMPLS.

Μόνο ένα νέο πρωτόκολλο χρειάζεται για να υποστηριχθούν οι λειτουργίες του, ένα πρωτόκολλο σηματοδότησης για τη διαχείριση γραμμών (LMP).

Βασικά το GMPLS στηρίζεται στις επεκτάσεις του Traffic Engineering (TE) που αφορούν το MPLS. Αυτό διότι οι περισσότερες τεχνολογίες που μπορούν να χρησιμοποιηθούν κάτω από το επίπεδο των Packet Switch Capable interfaces απαιτούν traffic engineering.

Επεκτάσεις στα παραδοσιακά πρωτόκολλα και στους παραδοσιακούς αλγορίθμους δρομολόγησης χρειάζονται για την ομοιόμορφη κωδικοποίηση και μεταφορά ΤΕ πληροφορίας γραμμής ενώ για την σηματοδότηση απαιτούνται σαφείς διαδρομές. Επίσης η σηματοδότηση πρέπει να είναι τώρα ικανή για μεταφορά των απαιτούμενων παραμέτρων για τα κυκλώματα (LSP), όπως το bandwidth, ο τύπος του σήματος, η επιθυμητή προστασία και/ή αποκατάσταση, η θέση στη συγκεκριμένη πολύπλεξη καθώς και άλλοι παράμετροι.

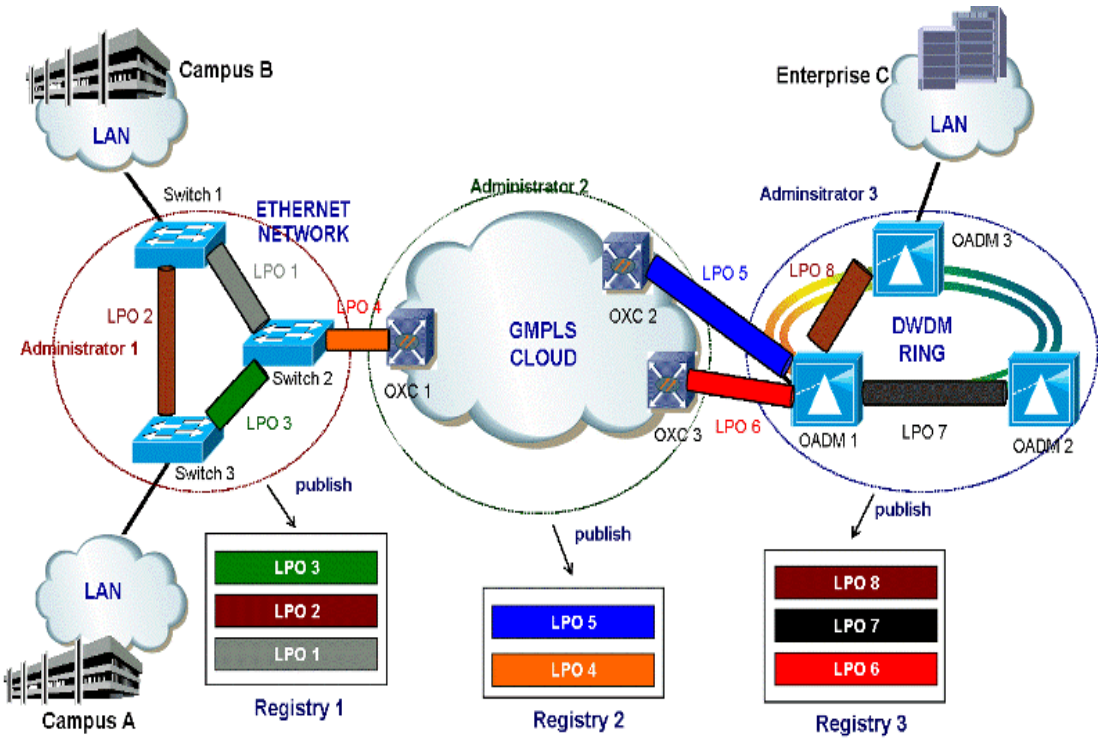
Το GMPLS επεκτείνει δύο πρωτόκολλα σηματοδότησης τα RSVP-TE [RFC3209] και CR-LDP [RFC3212]. Παρόλα αυτά το GMPLS δεν καθορίζει ποιο από αυτά πρέπει να χρησιμοποιηθεί. Οι κατασκευαστές θα ορίσουν την λύση ανάλογα με τα ενδιαφέροντά τους. Επίσης επεκτείνει δύο παραδοσιακά intra-domain link-state πρωτόκολλα δρομολόγησης, τα OSPF-TE και IS-IS-TE [29].

9.1.2 UCLP

Το έργο UCLP (User Controlled LightPath Provisioning) [108] χρηματοδοτείται από το CANARIE, το Καναδικό NREN, και τη Cisco Canada. Το UCLP software επιτρέπει σε τελικούς χρήστες (ανθρώπους ή εφαρμογές) να μεταχειρίζονται τους δικτυακούς πόρους ως αντικείμενα software και να παρέχουν και διαμορφώνουν lightpaths μέσα σε ένα domain ή μεταξύ πολλαπλών, ανεξάρτητα διαχειριζόμενων, domains. Οι χρήστες μπορούν επίσης να ενώσουν ή διαχωρίσουν lightpaths και να παραδώσουν τον έλεγχο και τη διαχείριση των μεγαλύτερων ή μικρότερων αυτών τμημάτων σε άλλους χρήστες. Το UCLP είναι σχεδιασμένο ώστε να δίνει τη δυνατότητα στους χρήστες να δημιουργούν το δικό τους προσανατολισμένο στην εφαρμογή IP δίκτυο, ειδικά για την υποστήριξη υψηλών απαιτήσεων εφαρμογών e-science και grid. Αυτά τα δίκτυα μπορούν να επαναδιαμορφωθούν από τον τελικό χρήστη και δεν απαιτείται η μεσολάβηση του διαχειριστή του οπτικού δικτύου.

Μέσω του UCLP οι χρήστες (ερευνητικά ινστιτούτα, κυβερνητικές υπηρεσίες, νοσοκομεία) θα μπορούν να ελέγχουν από άκρο σε άκρο lightpaths όπως WDM lambdas ή SONET STS κανάλια. Το σύστημα επιτρέπει γρήγορη παροχή δικτυακών πόρων και αυξάνει το σύνολο των διαθέσιμων lightpaths πέρα από αυτό που παρέχεται από έναν πάροχο.

Το UCLP ενσωματώνει τη λειτουργικότητα ενός grooming agent (πράκτορας συνένωσης που συνενώνει τα διακριτά κανάλια σε έναν πελάτη μέσα στο ίδιο OCX), ενός switch agent (πράκτορα μεταγωγής) και ενός signaling control plane agent (πράκτορα σηματοδότησης control plane) ανά πελάτη. Οι signalling control plane agents μέσα στο ίδιο UCLP σύστημα μπορούν να χρησιμοποιήσουν διαφορετικές τεχνολογίες και πρωτόκολλα.



Εικόνα 63: Αρχιτεκτονική UCLP

Οι λειτουργίες του UCLP βασίζονται σημαντικά στην έννοια των Lightpath Objects (LPOs). Κάθε LPO είναι μια αφηρημένη αναπαράσταση ενός lightpath (με όρους bandwidth και θεμάτων πολιτικής) που ελέγχεται και ανήκει σε έναν χρήστη. Οι Root LPOs καταγράφονται στο UCLP σύστημα από κάθε διαχειριστή domain και οι LPOs μπορούν να καθοριστούν αναπαριστώντας υποσύνολα του εύρους ζώνης και των πολιτικών των γονικών τους LPO. Ο ορισμός του root LPOs στο περιβάλλον του UCLP επιτρέπει τη δυναμική εύρεση της τοπολογίας. Ένα σύνθετο (compound) LPO από άκρο σε άκρο αντιπροσωπεύει μία συνένωση από LPOs.

Το UCLP παρέχει την εξής λειτουργικότητα:

- Μίσθωση / διαφήμιση lightpaths
- Διαμοίραση (partitioning) lightpaths
- Συνένωση lightpaths
- Εγκαθίδρυση lightpaths από άκρο σε άκρο
- Δημιουργία root lightpaths
- Διαχείριση λογαριασμών χρηστών.

9.1.3 DRAGON

Το έργο Dynamic Resource Allocation via GMPLS Optical Networks (DRAGON) [109] χρηματοδοτείται από τον οργανισμό National Science Foundation (NSF) των ΗΠΑ και είναι μια συνεργασία μεταξύ των παρακάτω οργανισμών: Mid-Atlantic Crossroads (MAX), University of Southern California (USC) Information Sciences Institute (ISI) και George Mason University (GMU).

Στόχοι του DRAGON είναι η ανάπτυξη υποδομών, τεχνολογιών και software για την παροχή αφιερωμένων (dedicated) μονοπατιών μεταξύ ετερογενών δικτυακών τεχνολογιών. Η εργασία των ανθρώπων του έργου εστιάζεται στη δυνατότητα δυναμικής παροχής των μονοπατιών έπειτα από αιτήματα από εφαρμογές, σε inter-domain επίπεδο και με την απαραίτητη AAA υποδομή.

Σκοπός του DRAGON είναι να αναπτυχθεί ένα οπτικό δίκτυο κορμού που να λειτουργεί GMPLS, με εξοπλισμό μεταγωγής που να ενεργεί ως Label Switching Routers (LSRs) και ο οποίος θα παρέχει ντετερμινιστικά δικτυακούς πόρους σε επίπεδο πακέτου, lambda, και οπτικής ίνας. Στο δίκτυο υποδομής θα έχουν πρόσβαση πειραματικά δίκτυα από τους συνεργαζόμενους οργανισμούς (Experimental Networks - ExNets) τα οποία θα παρέχουν στο DRAGON ένα περιβάλλον πολλαπλών domain και θα είναι αντιπροσωπευτικά των δικτυακών τεχνολογιών που πρέπει να διαχειριστούν σε ένα πραγματικό από άκρο σε άκρο περιβάλλον.

Σημαντικό τμήμα του έργου είναι η ανάπτυξη των απαραίτητων τμημάτων software για την επίλυση ανοιχτών ζητημάτων σε σχέση με το GMPLS καθώς και πρακτικών ζητημάτων για την από άκρο σε άκρο επικοινωνία. Η αρχιτεκτονική του DRAGON περιλαμβάνει έναν Network Aware Resource Broker (NARB) ο οποίος ανταλλάσει πληροφορία με τα πρωτόκολλα δρομολόγησης Interior Gateway Protocol/Exterior Gateway Protocol (IGP/EGP) για τη διαφήμιση inter-domain δυνατοτήτων για τις υπηρεσίες, κάνει τον υπολογισμό inter-domain μονοπατιών, ανάθεση πόρων, χρονοδρομολόγηση, σηματοδότηση καθώς και πιστοποίηση/χρέωση για τις ζητηθείσες δικτυακές υπηρεσίες. Η αρχιτεκτονική της λειτουργίας του NARB ενσωματώνει προηγμένες υπηρεσίες από το πρόγραμμα NSF Middleware Initiative (NMI), ειδικά για θέματα ασφάλειας και προηγμένη χρονοδρομολόγηση. Το software που αναπτύσσεται από το DRAGON θα χρησιμοποιηθεί επίσης από το έργο BRUW.

ΠΑΡΑΡΤΗΜΑ Ι: ΑΝΑΦΟΡΕΣ

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Δίκτυα Υπολογιστών, Τρίτη Έκδοση, Andrew Tanenbaum

[2] Εισαγωγή στις νέες τεχνολογίες επικοινωνιών, Ανδρέας Πομπόρτσης, εκδόσεις Α. Τζιόλα Ε.

[3] S. Vegesna, 'IP Quality of Service: the complete resource for understanding and deploying IP quality of service for Cisco networks', Cisco Press, 2001

[4] V. Jacobson, K. Nicholsm K.Poduri, "An Expedited Forwarding PHB", RFC 2598, June 1999

[5] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, 1999

[6] J. Heinanen, R. Guerin, "A single rate three color marker", RFC 2697, September 1999

[7] J. Heinanen, R. Guerin, "A Two Rate Three Color Marker", RFC 2698, September 1999

[8] W. Fang, N. Seddigh, "A Time Sliding Window Three Color Marker (TSWTCM)," RFC 2859, June 2000

[9] C Bouras, M. Campanella, M. Przybylski, A. Sevasti "QoS and SLA aspects across multiple management domains: The SEQUIN approach" (http://www.elsevier.com/locate/future). Future Generation Computer Systems 19 (2003) 313-326

[10] Chahed T. "IP QoS Parameters", private communication to TF-NGN November 2000

[11] J.Wroclawski, "Specification of the Controlled-Load Network Element Service", RFC 2211, September 1997

[12] K.Ramakrishman and S.Floyd, "A proposal to Add Explicit Congestion Notification (ECN) to IP", RFC 2481, January 1999

[13] M.Shreedhar and G.Varghese, "Efficient Fair Queueing Using Deficit Round Robin", Proceedings of ACM SIGCOMM 95, October 1995

[14] E.Hahne and R.Gallager, "Round Robin Scheduling for Fair Flow Control in Data Communication Networks", IEEE International Conference on Communications, June 1986

[15] RFC 2205, R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification", IETF.

[16] RFC 1890, H. Shculzrinne, S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", IETF.

[17] RFC 792, J. Postel, "Internet Control Message Protocol", IETF.

[18] RFC 793, J. Postel, "Transmission Control Protocol", IETF.

[19] M. Campanella, Implementation Architecture specification for the Premium IP service", Deliverable D2.1-Addendum 1, SEQUIN Project (IST-1999-20841)

[20] N.Seddigh, B.Nandy, J.Heinanen, "An Asured Rate Per-Domain Behaviour for Differentiated services", Internet Draft (draft-ietf-diffserv-pdb-ar-00.txt), 2000

[21] Marking for QoS improvements I.Yeom and A.L.N. Reddy

[22] A Measurement-based Admission Control Algorithm for Integrated Service Packet Networks (Extended Version) Sugih Jamin, Peter B. Danzig Scott J. Shenker, and Lixia Zhang

[23] Service Level Agreement Trading for the Differentiated Services Architecture George Fankhauser, David Schweikert, Bernhard Plattner

[24] B. Nandy, N. Seddigh, P. Pieda, "DiffServ's Assured Forwarding PHB What Assurance does the costumer Have ? ," The 9th International Workshop on Network and Operating Systems support for Digital Audio and Video (NOSSDAV'99), New Jersey, June 1999

[25] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, "Requirements for Traffic Engineering Over MPLS", RFC 2702, September 1999

[26] E. Rosen, Y.Rekhter, "BGP/MPLS VPNs", RFC 2547, March 1999

[27] "Advanced MPLS Design and Implementation", Vivek Alwin, CISCO PRESS, ISBN 158705020X

[28] Deliverable D9.5 "Proposal and implementation plan of the migration of current MBS", Geant's Report, Work Package 8

[29] "Traffic Engineering Extensions to OSPF", Dave katz, Derek Yeung, internet draft (draft-katz-yeung-ospf-traffic-00.txt) 1999

[30] "Management Bandwidth Service on MPLS domain", C. Bouras, V. kapoulas, D. Primpas, 17th IEEE International Workshop on Communications Quality & Reliability, CQR-2003, Kiawah Island, South Carolina, USA

[31] RFC 2815 "Integrated Service Mappings on IEEE 802 Networks" M. Seaman, A. Smith, E. Crawley, J. Wroclawski, May 2000

[32] "Class-Based Weighted Fair Queueing", CISCO Documentation

[33] Deliverable D9.5 "Proposal and implementation plan of the migration of current MBS", Geant's Report, Work Package 8

[34] Deliverable D9.12 Service specification for the proposal and implementation plan for the migration of current MBS, Geant's Report, Work Package 8

[35] C. Dovrolis, D. Stiliadis and P. Ramanathan, "Proportional Differentiated Services: Delay Differentiation and Packet Scheduling", in proceedings of ACM SIGCOMM '99 Conference, Boston, USA, 1999

[36] S. McCanne and S. Floyd, "ns Network Simulator", available at: http://www.isi.edu/nsnam/ns/

[37] RFC 3031 "MultiProtocol Label Switching Architecture" E. Rosen, A. Viswanathan, R. Callon, January 2001

[38] RFC 2328 "OSPF Version 2" J. Moy, April 1998

[39] RFC 3209 "RSVP-TE: Extensions to RSVP for LSP Tunnels" D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow December 2001

[40] J Kielthy, R. Frisby, M O Foghlu "An Initial investigation into QoS provisioning in a DiffServ domain" Telecommunication System Software Group 2003 (http://www.tssg.org)

[41] S. Josset, C. Bouras, A. Gkamas, K. Stamos, "Adding IPv6 support to H323: Gnomemeeting/openH323 port", 11th International Conference on Software Telecommunications and Computer Networks (SoftCOM 2003), Croatia, Italy, October 7-10 2003, pp. 458-462

[42] Internet Protocol, Version 6 (IPv6) Specification - RFC 2460

[43] RFC 2212, "Specification of the Guaranteed Quality of Service", S.Shenker, R.Guerin, September 1997

[44] RFC 1889, RTP: A Transport Protocol for Real-Time Applications, H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson January 1996

[45] D.Clark and W.Feng. "Explicit allocation of the best effort packet delivery service". IEEE/ACM Transactions on Networking, 6(4):362-374, 1998

[46] Service Level Agreement Trading for the Differentiated Services Architecture George Fankhauser, David Schweikert, Bernhard Plattner

[47] RFC 3086, Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification, K. Nichols, B. Carpenter April 2001

[48] RFC 2905 "AAA Authorization Application Examples", J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, August 2000

[49] "6NET Deliverable D.4.4.2v2. (2005). Report in QoS Tests, 2nd version", IST Programme (IST-2001-32603).

[50] G. Almes, S. Kalidindi, M. Zekauskas. (1999). "A One-way Delay Metric for IPPM", IETF RFC2679.

[51] G. Almes, S. Kalidindi, M. Zekauskas. (1999). "A One-way Packet Loss Metric for IPPM", IETF RFC2680.

[52] S. Deering, R. Hinden. (1998). "Intenet Protocol, Version 6 (IPv6)", RFC2460.

[53] K. Nichols, V. Jacobson, L.Zhang. (1999). "A Two-bit Differentiated Services Architecture for the Internet", IETF RFC2638.

[54] J.Rayahalme et al. (2004). "IPv6 Flow Label Specification", RFC3697.

[55] R. Roth et al. (2003). "IP QoS Across Multiple Management Domains: Practical Experiences for the Pan-European Experiments", IEEE Communications Magazine, Vol. 41, No 1.

[56] RFC 3270, "Multi-Protocol Label Switching (MPLS), Support of Differentiated Services", F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J. Heinanen, May 2002

[57] IEEE, "802.1D: IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Bridges", IEEE Std 802.1D-2004, (http://standards.ieee.org/getieee802/download/802.1D-2004.pdf).

[58] P. Trimintzios, I. Andrikopoulos, G. Pavlou, P. Flegkas, D. Griffin, P. Georgatsos, D. Goderis, Y. T'Joens, L. Georgiadis, C. Jacquenet, R. Egan, “A Management and Control Architecture for Providing IP Differentiated Services in MPLS-based Networks”, IEEE Communications, special issue in IP-Oriented Operations and Management, Vol. 39, No. 5, pp. 80-88, IEEE, May 2001

[59] A. Liakopoulos, B. Maglaris, C. Bouras, A. Sevasti, "Providing and verifying advanced IP services in hierarchical DiffServ networks - the case of GEANT", International Journal of Communication Systems, Wiley InterScience, 2004, pp. 321 - 336

[60] Przemyslaw Jaskola, Krzysztof Malinowski “Two methods of optimal Bandwidth allocation in TCP/IP networks with QoS differentiation”, 2004 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS’ 04), San Jose, California, USA, July 25 - 29 2004

[61] SEQUIN: “Service Quality across Independently Managed Networks”, IST Project IST-1999-20841, (http://www.dante.net/sequin/)

[62] C. Bouras, M. Campanella, A. Sevasth, "SLA definition for the provision of an EF-based service", 16th International Workshop on Communications Quality & Reliability (CQR 2002), Okinawa, Japan, May 14-16 2002, pp. 17-21

[63] Howarth M. et al., “Provisioning for Interdomain Quality of Service: The MESCAL Approach”, IEEE Comm., Vol. 43, No 6, June 2005.

[64] Roth R. et al., “IP QoS Across Multiple Management Domains: Practical Experiences for the Pan-European Experiments”, IEEE Comm., Vol. 41, No 1, January 2003

[65] M. Shreedhar and G. Varghese, “Efficient Fair Queuing using Deficit Round Robin”, in Proc. SIGCOMM ’95, Cambridge, USA, 1995.

[66] P. Trimintzios, T. Bauge, G. Pavlou, L. Georgiadis, P. Flegkas, R.Egan, “Quality of Service Provisioning for Supporting Premium Services in IP Networks”, Proc. IEEE Globecom 2002, Taipei, TW, Vol. 3, pp.2473-2477, IEEE, November 2002.

[67] K. Wu and D. S. Reeves, “Capacity Planning of DiffServ Networks with Best-Effort and Expedited Forwarding Traffic”, Telecommunication Systems, Vol. 25, No. 3-4, pp. 193-207, March-April 2004.

[68] C. Filsfils and J. Evans, “Engineering a multiservice IP backbone to support tight SLAs”, Computer Networks, vol 40, pp. 131-148, 2002

[69] V.A. Siris and G. Fotiadis, “Network Dimensioning Based on Percentage of Access Link Capacity Carrying Premium Traffic”. In Proc. of ICC 2006

[70] F. Yergeau, T. Bray, J. Paoli, C. M. Sperberg-McQueen and E. Maler, “Extensible Markup Language (XML) 1.0 (3rd Edition)”, W3C, Feb 2004, (http://www.w3.org/TR/2004/REC-xml-20040204/).

[71] E. Christensen, F. Curbera, G. Meredith and S. Weerawarana, “Web Services Description Language (WSDL) 1.1”, W3C TR, Mar 2001, (http://www.w3.org/TR/wsdl/).

[72] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, “RSVP-TE: Extensions to RSVP for LSP Tunnels”, IETF RFC 3209, December 2001

[73] Manzoor Hashmani and Mikio Yoshida "ENICOM's Bandwidth Broker", Saint 2001 Workshops, pp 213-220, Jan 8-12, 2001, San Diego, USA

[74] J. Ogawa, A. Terzis, S. Tsui, L. Wang, L. Zhang. “A Prototype Implementation of the Two-Tier Architecture for Differentiated Services”, RTAS99 Vancouver, Canada

[75] S. Sohail, S. Jha, “The Survey of Bandwidth Broker”, Technical Report UNSW CSE TR 0206, School of Computer Science and Engineering, University of New South Wales, Sydney 2052, Australia, May 2002

[76] H. A. Mantar, I. Okumus, S. J. Chapin, and J. Hwang, "A Scalable Model for Inter-Bandwidth-Broker Resource Reservation and Provisioning," the IEEE Journal on Selected Areas in Communications, Vol. 22, No. 10, December 2004

[77] Junseok Hwang, Rajesh Revuru “Inter-Domain Diffserv Dynamic Provisioning and Interconnection Peering Study Using Bandwidth Management Point - A Simulation Evaluation” The 2003 International Conference on Information Systems and Engineering

[78] I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, “Adaptive Multipath Routing for Dynamic Traffic Engineering,” in IEEE Globecom, (San Francisco), Nov 2003.

[79] I. Okumus, J. Hwang, S. J. Chapin, and H. Mantar, "Inter-Domain Traffic Engineering on a Bandwidth Broker Supported Diffserv Internet," Applied Telecommunication Symposium (ATS '03), part of the Advanced Simulation Technologies Conference 2003 (ASTC'03).

[80] Z. Zhang, Z. Duan, Y. Hou, “On Scalable Design of Bandwidth Brokers”, IEICE Trans. Communications, Vol. E84-B, No.8 August 2001

[81] C. Bouras, K. Stamos, “An Adaptive Admission Control Algorithm for Bandwidth Brokers”, 3rd IEEE International Symposium on Network Computing and Applications (NCA04), Cambridge, MA, USA, August 30 - September 1 2004

[82] Lili Qiu; Padmanabhan, V.N.; Voelker, G.M, "On the placement of Web server replicas," INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE Volume 3, 22-26 April 2001 Page(s):1587 - 1596 vol.3.

[83] Przemyslaw Jaskola, Krzysztof Malinowski “Two methods of optimal Bandwidth allocation in TCP/IP networks with QoS differentiation”, 2004 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS’ 04), San Jose, California, USA, July 25 - 29 2004

[84] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0262032937. Section 22.3: Depth-first search, pp.540–549

[85] E. Mannie, IETF RFC 3945, “Generalized Multi-Protocol Label Switching (GMPLS) Architecture”, October 2004.

[86] L. Berger, IETF RFC 3471, “Generalized Multi-Protocol Label Switching (GMPLS) Signalling Functional Description”, January 2003.

[87] L. Berger, IETF RFC 3473, “Generalized Multi-Protocol Label Switching (GMPLS) Signalling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions”, January 2003.

WEB SITES

[88] Cisco 12000 Series Internet Router: Frequently Asked Questions, http://www.cisco.com/warp/public/63/gsrfaq_11085.shtml

[89] RSVP ReSerVation Protocol: http:// www.isi.edu/div7/rsvp/rsvp.html

[90] R. Wielicki, "ns-2 ad-ons page", found at: http://thenut.eti.pg.gda.pl/~rafalw/wfq/

[91] "6NET – Large Scale IPv6 Pilot Network", IST Programme (IST-2001-32603), http://www.6net.org.

[92] http://www.ethereal.com

[93] http://www.geant.net

[94] http://www.cisco.com

[95] http://www.juniper.net

[96] http://www.grnet.gr

[97] http://anstool.grnet.gr

[98] http://www.ietf.org/html.charters/OLD/diffserv-charter.html

[99] http://www.ietf.org/html.charters/intserv-charter.html

[100] http://dast.nlanr.net/Projects/Iperf/

[101] Service Assurance Agent (SAA)", Cisco Systems Inc., http://www.cisco.com.

[102] EUQoS Project, (http://www.euqos.org/index.php).

[103] GN2 project (http://www.geant2.net)

[104] SEQUIN: 'Service Quality across Independently Managed Networks', IST Project IST-1999-20841, (http://www.dante.net/sequin/)

[105] Qbone Signaling Design Team, http://qbone.internet2.edu/bb/

[106] Quagga Routing Suite - http://www.quagga.net/

[107] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/

[108] UCLP Project, http://www.canarie.ca/canet4/uclp/uclp_software.html

[109] Dragon Project, http://dragon.east.isi.edu

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΑΚΡΩΝΥΜΑ

ΑΚΡΩΝΥΜΙΑ

Ακρώνυμο	Επεξήγηση
6PE	IPv6 Provider Edge Router over MPLS
AAC	Adaptive admission control
AACR	Adaptive admission control with resubmissions
ABK	Address Based Keys
AF	Assured Forwarding
AH	Authentication Header
AIIH	Assignment of IPv4-global addresses to IPv6 Hosts
ALG	Application Level Gateway
API	Application Programming Interface
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
bps	bits per second
CIDR	Classless Inter-Domain Routing
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DoS	Denial of Service
DRR	Deficit Round Robin
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSTM	Dual Stack Transition Mechanism
DTI	Dynamic Tunnelling Interface
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
EGP	External Gateway Protocol

Ακρώνυμο	Επεξήγηση
ESP	Encapsulating Security Payload
EUI	Extended Unique Identifier
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocol
ICF	Internet Connection Firewall
ICV	Integrity Check Value
IGMP	Internet Group Membership Protocol
IGP	Interior Gateway Protocol
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IntServ	Integrated Services
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internet Packet Exchange
IRC	Internet Relay Chat
ISI	Information Sciences Institute, University of Southern California School of Engineering
ISP	Internet Service Provider
Kbps	Kilobits per second
LAN	Local Area Networks
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
MAC address	Medium Access Control
MAC (στην κρυπτογραφία)	Message Authentication Code
Mbps	Megabits per second
MD5	Message Digest 5

Ακρώνυμο	Επεξήγηση
MDRR	Modified Deficit Round Robin
MIT	Massachusetts Institute of Technology
MP-BGP	Multi-Protocol Border Gateway Protocol
MPLS	Multi-Protocol Label Switching
MRTG	Multi Router Traffic Grapher
MTU	Maximum Transfer Unit
NAT	Network Address Translation
NAT-PT	Network Address Translation – Protocol Translation
NBMA	Non-Broadcast Multiple Access
NLA ID	Next-Level Aggregation Identifier
NSAP	Network Service Access Point
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PARK	Palo Alto Research Center
PBAC	Price-based admission control without adaptation
PDA	Personal Digital Assistant
PESQ	Perceptual Evaluation of Speech Quality
PHB	Per-Hop Behavior
PKI	Public Key Infrastructure
POP	Post Office Protocol
PPP	Point to Point Protocol
PQ	Priority Queuing
QoS	Quality of Service
RFC	Request For Comments
RH	Routing Header
RIP	Routing Information Protocol
RIPE	Réseaux IP Européens
RR	Round Robin
RSVP	Resource Reservation Protocol
RTCP	Real-Time Control Protocol
RTP	Real Time Protocol

Ακρώνυμο	Επεξήγηση
SA	Security Association
SAC	Simple admission control
SHA	Secure Hash Algorithm
SHTTP	Secure HyperText Transport Protocol
SIT	Simple Internet Transition
SLA	Service Level Agreement
SLA ID	Site-Level Aggregation Identifier
SMTP	Simple Mail Transfer Protocol
SPI	Security Parameter Index
TCP	Transmission Control Protocol
TLA ID	Top-Level Aggregation Identifier
TOS	Type Of Service
TTL	Time To Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Networks
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
XNS	Xerox Network System

ΠΑΡΑΡΤΗΜΑ ΙΙΙ: ΓΛΩΣΣΑΡΙΟ

ΓΛΩΣΣΑΡΙΟ

Όρος	Επεξήγηση
Acknowledgement	Επιβεβαίωση/αναγνώριση
Address	Διεύθυνση
Admission control	Έλεγχος αποδοχής
Agent	Πράκτορας – η οντότητα που εκτελεί μια λειτουργία εκ μέρους μιας άλλης
Aggregation	Συνάθροιση
Authentication	Πιστοποίηση
Authorization	Εξουσιοδότηση
Automatic	Αυτόματος – διαδικασία που δεν απαιτεί τη μεσολάβηση ανθρώπου/διαχειριστή
Backbone	Δίκτυο κορμού
Balancing	Εξισορρόπηση
Bandwidth	Εύρος ζώνης, καθορίζει το ποσό της πληροφορίας που μπορεί να μεταδοθεί από έναν δικτυακό σύνδεσμο στη μονάδα του χρόνου
Best effort	Καλύτερης προσπάθειας – μετάδοση πακέτων χωρίς εγγυήσεις για τον τρόπο και την ποιότητα της μετάδοσης
Binding	Δέσιμο – ο συνδυασμός της οικείας (home) διεύθυνσης ενός κινητού κόμβου με την προσωρινή (care-of) διεύθυνση και τη χρονική διάρκεια εγκυρότητας του συνδυασμού
Bit	Δυαδικό ψηφίο
Broadcast	Ευρεία αναμετάδοση
Broker	Μεσίτης/διαμεσολαβητής για μία υπηρεσία
Byte	Μία οκτάδα δυαδικών ψηφίων
Care-of	Η προσωρινή διεύθυνση που αποκτά ένας κινητός κόμβος όταν βρίσκεται σε ένα ξένο υποδίκτυο
Case study	Συγκεκριμένη μελέτη
Class	Κλάση/κατηγορία
Client	Πελάτης – το μηχάνημα/πρόγραμμα/διεργασία που ζητάει μια υπηρεσία από έναν εξυπηρετητή (server)
Compatible	Συμβατός

Όρος	Επεξήγηση
Confidentiality	Εμπιστευτικότητα
Configuration	Ρύθμιση / Διαμόρφωση
Cookie	Είδος κουπονιού που κρατάει πληροφορία
Core	Πυρήνας/κεντρικός
Data	Δεδομένα
Database	Βάση δεδομένων
Debugging	Αποσφαλμάτωση κώδικα
Default	Προεπιλεγμένος
Delay	Καθυστέρηση – ο χρόνος που απαιτείται για να μεταδοθεί ένα πακέτο
Denial of Service	Επίθεση με σκοπό το υπολογιστικό σύστημα που δέχεται την επίθεση να αδυνατεί να εξυπηρετήσει τους κανονικούς του χρήστες
Deprecate	Αποδοκιμάσιμος – ένα χαρακτηριστικό ενός πρωτοκόλλου/προτύπου το οποίο μπορεί ακόμα να χρησιμοποιηθεί, αλλά προτείνεται να μην χρησιμοποιείται (πιθανώς γιατί σε επόμενη έκδοση του πρωτοκόλλου/προτύπου θα καταργηθεί)
Destination	Προορισμός
Domain	Αυτόνομο σύστημα (σύνολο από κόμβους) σε ένα δίκτυο, που συνήθως διαχειρίζεται από μία οντότητα
Dual stack	Διπλής στοίβας (ένας σταθμός που υποστηρίζει IPv4 και IPv6)
Edge-to-edge	Από-άκρο-σε-άκρο ενός διαχειριστικού τμήματος (domain)
Encapsulation	Ενθυλάκωση
Encryption	Απόκρυψη/Κωδικοποίηση
End-to-end	Από-άκρο-σε-άκρο μιας σύνδεσης
Error	Σφάλμα/λάθος
Feedback	Ανατροφοδότηση
Firewall	Ρυθμιστής της δικτυακής κίνησης μεταξύ δικτύων / υπολογιστικών συστημάτων
Flag	Σημαία – ένα bit που ανάλογα με την τιμή 0 ή 1 που παίρνει σηματοδοτεί κάτι
Flow	Ροή
Forwarding	Προώθηση πακέτων

Όρος	Επεξήγηση
Fragment	Κομμάτι από διασπασμένο πακέτο
Gateway	Πύλη
Global	Οικουμενικός
Hardware	Υλικό ενός υπολογιστικού συστήματος
Hash function	Μαθηματική διαδικασία που δημιουργεί μία σύνοψη συγκεκριμένου μεγέθους ενός μηνύματος, η οποία δεν μπορεί εύκολα να χρησιμοποιηθεί για την ανάκτηση του αρχικού μηνύματος χωρίς τον βοηθητικό αλγόριθμο hashing
Header	Επικεφαλίδα
Home	Οικείος
Hop	Βήμα σε ένα δικτυακό μονοπάτι
Host	Σταθμός
Identifier	Αναγνωριστικό
Index	Δείκτης που καθορίζει την τρέχουσα θέση επεξεργασίας για ένα σύνολο
Integrity	Ακεραιότητα
Interface	Διεπαφή – Ένα δικτυακό interface είναι το σημείο επαφής ενός κόμβου με έναν δικτυακό σύνδεσμο (link)
Internet	Διαδίκτυο
Jitter	Διακύμανση καθυστέρησης μεταξύ των αφίξεων διαδοχικών πακέτων
Jumbo	Πολύ μεγάλο
Kernel	Πυρήνας λειτουργικού συστήματος
Label	Ετικέτα
Laptop	Φορητός υπολογιστής
Latency	Καθυστέρηση μετάδοσης
Layer	Επίπεδο
Length	Μήκος
Library	Βιβλιοθήκη
Link	Δικτυακός σύνδεσμος
Load	Φόρτος
Local	Τοπικός
Management	Διαχείριση

Όρος	Επεξήγηση
Manual	Χειροκίνητος – διαδικασία που απαιτεί τη μεσολάβηση ενός ανθρώπου/διαχειριστή
Marking	Μαρκάρισμα
Metering	Μέτρηση
Mobile	Κινητός
Native IPv6	Γνήσιος – υποστήριξη του IPv6 πρωτοκόλλου χωρίς τη χρήση κάποιου μεταβατικού μηχανισμού
Network	Δίκτυο
Node	Κόμβος
Offset	Αριθμός που δείχνει τη μετατόπιση σε σχέση με κάποιο σημείο αναφοράς
Optimization	Βελτιστοποίηση
Option	Επιλογή
Overhead	Επιβάρυνση
Packet	Πακέτο – ένα σύνολο από bits που μεταδίδονται μαζί στο δίκτυο
Padding	Συμπλήρωμα που χρησιμοποιείται στα πεδία της επικεφαλίδας ενός πακέτου ώστε αυτά να στοιχίζονται κατάλληλα (συνήθως σε μία δύναμη του 2)
Path	Δικτυακό μονοπάτι
Payload	Ωφέλιμο φορτίο
Port	Θύρα
Prefix	Πρόθεμα
Process	Διεργασία
Protocol	Πρωτόκολλο
Provider	Παροχέας
Proxy	Αντιπρόσωπος – μία οντότητα που εκτελεί μια διαδικασία εκ μέρους μιας άλλης και της μεταδίδει το αποτέλεσμα
Quality of Service	Ποιότητα Υπηρεσίας
Refresh	Ανανέωση
Relay	Αναμεταδότης
Reply	Απάντηση
Request	Αίτημα
Reserved	Δεσμευμένο

Όρος	Επεξήγηση
Robustness	Ευρωστία
Router	Δρομολογητής
Security	Ασφάλεια
Segment	Τεμάχιο
Server	Εξυπηρετητής – το μηχάνημα/πρόγραμμα/διεργασία που παρέχει μια υπηρεσία σε έναν πελάτη (client)
Session	Σύνοδος
Shaping	Μορφοποίηση
Single point of failure	Ένα σημείο ενός συστήματος το οποίο αν αποτύχει παρασύρει ολόκληρο το σύστημα («αχίλλειος πτέρνα»)
Site	Χρησιμοποιείται για να προσδιορίσει έναν οργανισμό ή μία τοποθεσία στα πλαίσια ενός ευρύτερου δικτύου, αν και ο ακριβής ορισμός αλλάζει ανάλογα με τον τρόπο χρήσης του όρου
Socket	Μηχανισμός δικτυακής επικοινωνίας, αντιπροσωπεύει τη δομή στην οποία γράφονται και από την οποία ανακτώνται τα δεδομένα που μεταδίδονται μέσω του δικτύου
Software	Λογισμικό που εκτελείται σε ένα υπολογιστικό σύστημα
Source	Αφετηρία / Πηγή
Spoofing	Προσπάθεια εξαπάτησης με το να υποκρίνεται ο θύτης ότι είναι κάποιος άλλος
Stack	Στοίβα
Standard	Πρότυπο
Stateful	Μηχανισμός/πρωτόκολλο που λειτουργεί κρατώντας μνήμη προηγούμενης κατάστασης
Stateless	Μηχανισμός/πρωτόκολλο που λειτουργεί μη κρατώντας μνήμη προηγούμενης κατάστασης, οπότε κάθε ενέργεια είναι ανεξάρτητη
Streaming	Μετάδοση πακέτων πάνω από δίκτυο τα οποία επεξεργάζονται καθώς καταφθάνουν με σκοπό την πραγματικού χρόνου μετάδοση πολυμέσων
Subnet	Υποδίκτυο
Throughput	Απόδοση – το ποσό της πληροφορίας που επιτυγχάνεται να παραχθεί στη μονάδα του χρόνου
Timeout	Χρόνος λήξης

Όρος	Επεξήγηση
Traffic	Δικτυακή κίνηση
Translation	Μετάφραση
Tunnel	Σήραγγα
Update	Ενημέρωση/ανανέωση
Valid	Έγκυρος
Version	Έκδοση
Well-known	Ευρέως γνωστό – ένα χαρακτηριστικό που μπορεί να θεωρηθεί ότι θα το γνωρίζουν όλες οι οντότητες με τις οποίες θα υπάρξει αλληλεπίδραση
Wireless	Ασύρματη σύνδεση