



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ &
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Μελέτη Μηχανισμών Ελέγχου Αποδοχής Ροών βασισμένων σε μετρήσεις»

Αναστάσιος Α. Ζαφειρόπουλος

Επιβλέπων: Βασίλειος Μάγκλαρης
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 14^η Ιουλίου 2004.

.....
Β.Μάγκλαρης
Καθηγητής Ε.Μ.Π

.....
Ε.Συκάς
Καθηγητής Ε.Μ.Π

.....
Δ.Καλογεράς
Ερευνητής

.....

Αναστάσιος Α. Ζαφειρόπουλος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π

Copyright © Αναστάσιος Α. Ζαφειρόπουλος, 2004

Με επιφύλαξη παντός δικαιώματος. All rights reserved. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της παρούσας διπλωματικής εργασίας, κ. Β. Μάγκλαρη, ο οποίος μου έδωσε την ευκαιρία να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα. Επίσης, θα ήθελα να ευχαριστήσω ιδιαίτερα τον υποψήφιο διδάκτορα κ. Αθ. Λιακόπουλο, ο οποίος με συνεχές ενδιαφέρον κατεύθυνε και ενέπνευσε την όλη πορεία αυτής της εργασίας και συνέβαλε αποφασιστικά στην τελική της διαμόρφωση.

Περίληψη

Ο σκοπός της διπλωματικής εργασίας ήταν η μελέτη του μηχανισμού ελέγχου αποδοχής ροών (Measurement Based Admission Control), η εφαρμογή του οποίου γίνεται στον κεντρικό δρομολογητή ενός δικτύου (core router). Ο μηχανισμός αυτός έχει ως στόχο να βελτιώσει την χρησιμοποίηση των γραμμών του δικτύου (link utilization), να μειώσει τον ρυθμό απωλειών πακέτων (packet loss rate) και να δώσει τη δυνατότητα για παροχή εγγυήσεων σε ροές που το επιζητούν, σχετικά με το χρησιμοποιούμενο εύρος ζώνης (bandwidth) και την καθυστέρηση (delay).

Συγκεκριμένα, από τη μελέτη των υπαρχόντων αλγορίθμων ελέγχου αποδοχής ροών, διαπιστώθηκε ότι δεν παρουσιάζονται σημαντικές διαφορές ως προς τα αποτελέσματα για τα χαρακτηριστικά της κίνησης που αναφέραμε προηγουμένως. Επομένως προχωρήσαμε στην πρόταση ενός νέου αλγόριθμου, ο οποίος βασίζεται στον χρωματισμό των πακέτων πριν αυτά εισέλθουν στο δίκτυο (ανάλογα με την εκάστοτε κατάσταση των γραμμών του δικτύου) και στην αποδοχή ή απόρριψη των νέων ροών από τον κεντρικό δρομολογητή (core router), με βάση τον χρωματισμό των πακέτων.

Αναλυτικότερα, στο 1^ο κεφάλαιο γίνεται μια εισαγωγή σχετικά με το τι είναι Ποιότητα Υπηρεσίας, γιατί είναι αναγκαία, ποιες είναι οι Αρχιτεκτονικές που έχουν αναπτυχθεί για παροχή Ποιότητας Υπηρεσίας, καθώς και ποια είναι η συνεισφορά της εργασίας μας. Στο 2^ο κεφάλαιο, αναφέρονται τα κύρια χαρακτηριστικά που θα πρέπει κάποιος να λάβει υπόψη του, κατά τον σχεδιασμό της Αρχιτεκτονικής παροχής Ποιότητας Υπηρεσίας. Στο 3^ο κεφάλαιο, εξετάζονται η Αρχιτεκτονική Ενοποιημένων Υπηρεσιών, το Πρωτόκολλο Δέσμευσης Πόρων, η Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών, οι Υπηρεσίες που παρέχονται από αυτή και γίνεται μία σύγκριση μεταξύ των δύο Αρχιτεκτονικών που αναφέρθηκαν προηγουμένως. Στο 4^ο κεφάλαιο εξετάζονται οι μηχανισμοί ταξινόμησης, ελέγχου κίνησης, διαχείρισης ουρών, χρονοδρομολόγησης και οι μηχανισμοί ελέγχου αποδοχής ροών. Για τους τελευταίους αναπτύσσονται και αλγόριθμοι που τους υλοποιούν. Στο 5^ο κεφάλαιο περιγράφεται το πρόβλημα που αντιμετωπίστηκε, η τοπολογία του δικτύου που αναπτύχθηκε, και τα χαρακτηριστικά των πηγών κίνησης που χρησιμοποιήθηκαν. Τέλος, Στο 6^ο κεφάλαιο παρουσιάζονται τα αποτελέσματα που πήραμε από τις προσομοιώσεις και τα συμπεράσματα που βγάλαμε.

Για τη διερεύνηση των παραπάνω αναπτύχθηκαν μοντέλα προσομοίωσης με τη χρήση του εργαλείου προσομοίωσης NS (Network Simulator). Η σχεδίαση και παραμετροποίηση των πειραμάτων επιδιώχθηκε να είναι όσο το δυνατόν πιο αντιπροσωπευτική για υπάρχοντα IP δίκτυα.

Λέξεις Κλειδιά

Ποιότητα Υπηρεσίας, Αρχιτεκτονική Ενοποιημένων Υπηρεσιών, Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών, Αλγόριθμοι Ελέγχου Αποδοχής Ροής, χρωματισμός πακέτων.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευχαριστίες.....	2
Περίληψη.....	3
1. Εισαγωγή.....	7
2. Απαιτήσεις για ποιότητα υπηρεσίας στο διαδίκτυο.....	10
2.1. Εξυπηρέτηση απαιτητικών εφαρμογών.....	10
2.2. Κλιμάκωση.....	11
2.3. Εύκολη διαχείριση και παρακολούθηση χρήσης πόρων.....	12
2.4. Διαφορετικές υλοποιήσεις και λειτουργικά συστήματα.....	12
3. Αρχιτεκτονικές και υπηρεσίες QoS.....	14
3.1. Ενοποιημένες Υπηρεσίες (Integrated Services, Intserv).....	14
3.1.1. Η Κλάση Ελεγχόμενου Φορτίου (Controlled Load Service).....	17
3.1.2. Η Κλάση Εγγυημένης Υπηρεσίας (Guaranteed Service).....	18
3.2. Πρωτόκολλο Δέσμευσης πόρων (Resource Reservation Protocol, RSVP). 19	
3.3. Πλεονεκτήματα του μοντέλου IntServ-RSVP.....	22
3.4. Μειονεκτήματα του μοντέλου Intserv-RSVP.....	23
3.5. Διαφοροποιημένες υπηρεσίες (Differentiated Services).....	24
3.5.1. Βασικές αρχές Διαφοροποιημένων Υπηρεσιών.....	25
3.5.2. Δομή του πεδίου DS.....	29
3.5.3. Μηχανισμοί προώθησης πακέτων, Λειτουργίες δρομολόγησης.....	30
3.5.4. Υπηρεσίες που παρέχονται από την Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών (DiffServ-Based Υπηρεσίες).....	32
3.5.4.1. EF-based υπηρεσίες (expedited forwarding).....	32
3.5.4.2. AF-based υπηρεσίες (assured forwarding).....	34
3.5.5. Δυνατότητα Κλιμάκωσης.....	36
3.6. Ενοποιημένες Υπηρεσίες πάνω από δίκτυα Διαφοροποιημένων Υπηρεσιών.....	38
3.7. Σύγκριση των IntServ και DiffServ αρχιτεκτονικών.....	42
4. Μηχανισμοί για την υλοποίηση QoS αρχιτεκτονικών.....	45
4.1. Μηχανισμοί Διαχείρισης πακέτων.....	45
4.1.1. Ταξινόνηση (Classification).....	46
4.1.1.1. BA ταξινόμηση (IP Precedence/ToS και DSCP).....	47
4.1.1.2. IPv4 MF ταξινόμηση.....	48
4.1.2. Ρύθμιση της κίνησης (Traffic Conditioning).....	49
4.1.2.1. Αλγόριθμοι διαρρέοντος δοχείου (Token και leaky bucket).....	50
4.1.3. Διαχείριση Ουρών (Queue Management).....	51
4.1.3.1. Αλγόριθμοι διαχείρισης ουρών για αποφυγή συμφόρησης.....	53
4.1.3.2. Τυχαία Έγκαιρη Ανίχνευση (Random Early Detection, RED).....	55
4.1.4. Χρονοδρομολόγηση (Scheduling).....	56
4.1.4.1. First-in, First-out (FIFO) Queueing.....	57
4.1.4.2. Priority Queueing (PQ).....	58
4.1.4.3. Fair Queueing (FQ).....	59
4.1.4.4. Weighted Fair Queueing.....	60
4.2. Μηχανισμοί Ελέγχου (Control Path Μηχανισμοί).....	62
4.2.1. Έλεγχος απόδοσης (admission control).....	62
4.2.1.1. Έλεγχος Αποδοχής βασισμένος σε μετρήσεις (Measurement-based Admission Control).....	63
4.2.1.2. Measurement-based admission control algorithms (MBACs).....	64
5. Πρόβλημα.....	70

5.1.	Προσέγγιση – Αντιμετώπιση του προβλήματος	70
5.2.	Τοπολογία του δικτύου	72
5.3.	Χαρακτηριστικά των πηγών κίνησης (traffic sources)	72
6.	Προσομοιώσεις και αποτελέσματα	74
6.1.	Προσομοιώσεις χωρίς την εφαρμογή του MBAC μοντέλου	74
6.1.1.	Χρησιμοποίηση TCP πηγών	74
6.1.2.	Χρησιμοποίηση TCP και BE πηγών	77
6.1.3.	Χρησιμοποίηση TCP, UDP και BE πηγών	80
6.2.	1η Προσομοίωση με εφαρμογή του MBAC μοντέλου	84
6.3.	2η προσομοίωση με εφαρμογή του MBAC μοντέλου	94
6.4.	Σύγκριση των αλγορίθμων MS_EF και Color MBAC μέσα από προσομοιώσεις	108
7.	Συμπεράσματα	112
	ΒΙΒΛΙΟΓΡΑΦΙΑ	113
8.	Παράρτημα	115
8.1.	Παράρτημα Α – Όρια απόδοσης	115
8.2.	Παράρτημα Β – Συμπεριφορά του πρωτοκόλλου TCP RENO	120

1. Εισαγωγή

Μέχρι πριν μερικά χρόνια, το Διαδίκτυο (Internet) χρησιμοποιούταν για την μεταφορά πληροφοριών μεταξύ απομακρυσμένων σημείων, αλλά χωρίς να παρέχονται εγγυήσεις από το δίκτυο, τόσο για το χρόνο μεταφοράς της πληροφορίας, όσο και για την πιθανότητα απώλειάς της, λόγω της συμφόρησης στις γραμμές. Η απομακρυσμένη πρόσβαση σε τερματικά, η μεταφορά αρχείων και η ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), ήταν από τις πιο δημοφιλείς εφαρμογές, για τις οποίες η μέθοδος μεταγωγής πακέτων (κάθε πακέτο προωθείται ανεξάρτητα από τα άλλα προς τον προορισμό του) δούλευε ικανοποιητικά. Όμως η ραγδαία εξάπλωση του Διαδικτύου τα τελευταία χρόνια τροφοδότησε και συνεχίζει να τροφοδοτεί την ανάπτυξη προηγμένων εφαρμογών πραγματικού χρόνου (real time), που επιθυμούν να το χρησιμοποιήσουν σαν μέσο μεταφοράς των δεδομένων τους. Τα συστήματα τηλεδιάσκεψης (videoconference), η τηλεφωνία πάνω από IP (Voice over IP), το ηλεκτρονικό εμπόριο (e-commerce), αποτελούν εφαρμογές, με απαιτήσεις σε αξιοπιστία και ποιότητα κατά τη μεταφορά της πληροφορίας.

Η οικογένεια πρωτοκόλλων TCP/IP, με την οποία είναι χτισμένο το Διαδίκτυο, δεν παρέχει την ποιότητα υπηρεσίας (Quality of Service) που χρειάζονται οι νέες εφαρμογές για να λειτουργήσουν ικανοποιητικά. Συγκεκριμένα, η υπηρεσία Βέλτιστης Προσπάθειας (Best Effort) που παρέχει ο αρχικός σχεδιασμός του Διαδικτύου, επιτρέπει στις απ' άκρο σ' άκρο (end-to-end) καθυστερήσεις ενός πακέτου να αυξηθούν απεριόριστα, εξαιτίας του φαινομένου της συμφόρησης. Εφαρμογές πραγματικού χρόνου, όπως π.χ. εφαρμογές μεταφοράς ήχου ή κινούμενης εικόνας (video) απαιτούν καλύτερη QoS από το Διαδίκτυο. Για να είναι λοιπόν σε θέση ένας Πάροχος Δικτυακών Υπηρεσιών (ISP), να παρέχει τις παραπάνω υπηρεσίες στους Πελάτες του, χρειάζεται ένα δίκτυο με δυνατότητες να διασφαλίζει εγγυήσεις κατά την μεταφορά της κίνησης.

Η Ποιότητα Υπηρεσίας (QoS) αναφέρεται στην ικανότητα που έχει ένα δίκτυο να παρέχει όσο το δυνατόν καλύτερη εξυπηρέτηση στη κίνηση του δικτύου. Συγκεκριμένα, παρέχει στην κίνηση που εξυπηρετείται από το δίκτυο καλύτερη και πιο προβλέψιμη μετάδοση με το να :

- Ελέγχει το διαθέσιμο εύρος ζώνης στις γραμμές διάδοσης.

- Μειώνει την πιθανότητα των απωλειών πακέτων.
- Αποφεύγει τη συμφόρηση του δικτύου και διαχειρίζεται αποδοτικά τους πόρους του.
- Διαχωρίζει την κίνηση σε διαφορετικές κλάσεις, παρέχοντας έτσι διαφορετικές εγγυήσεις κατά τη μεταφορά.

Η Ποιότητα Υπηρεσίας (QoS) εξυπηρετεί με διαφορετικό τρόπο τις ροές που δημιουργούνται. Αυτό γίνεται με το να αυξάνει την προτεραιότητα κάποιας ροής ή με το να μειώνει τη προτεραιότητα κάποιας άλλης. Σημαντικό είναι το γεγονός ότι με το να παρέχουμε προτεραιότητα σε κάποιες ροές, δεν σημαίνει ότι αναγκάζουμε τις υπόλοιπες να απορριφθούν. Ως ροή ορίζουμε τα πακέτα που ανταλλάσσονται μεταξύ δύο συγκεκριμένων κόμβων πηγής (source node) και προορισμού (destination node), με συγκεκριμένες IP διευθύνσεις και θύρες ο καθένας.

Οι δύο αρχιτεκτονικές ποιότητας υπηρεσίας που έχουν οριστεί από την Internet Engineering Task Force (IETF) για να εξυπηρετήσουν τις νέες εφαρμογές είναι η Αρχιτεκτονική Ενοποιημένων Υπηρεσιών (Integrated Service Architecture, IntServ) και η Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών (Differentiated Service Framework, DiffServ) . Η καταγεγραμμένη εμπειρία δείχνει πως δεν είναι εφικτή αλλά ούτε και αποτελεσματική η υιοθέτηση μίας μόνο ενιαίας αρχιτεκτονικής σε όλο το εύρος του Διαδικτύου, το οποίο αποτελείται από διαφορετικές διαχειριστικές περιοχές. Αντίθετα, προκύπτει πως η υιοθέτηση διαφορετικών αρχιτεκτονικών σε διάφορα τμήματα, τα οποία διασυνδέονται με καθορισμένο τρόπο έχει σημαντικά πλεονεκτήματα. Εξάλλου η μελέτη και ανάπτυξη ενός σχήματος για παροχή QoS, όσον αφορά τα ανώτερα επίπεδα από αυτό του δικτύου, είναι άρρηκτα συνδεδεμένη με την ανάπτυξη μηχανισμών διαχείρισης της χωρητικότητας των συνδέσμων και ελέγχου ή χρέωσης της κατανάλωσης των πόρων του δικτύου από τους πελάτες.

Σήμερα, στο δίκτυα μεταγωγής πακέτου IP, κάθε δρομολογητής ο οποίος παρεμβάλλεται στη διαδρομή ενός πακέτου IP δεν κάνει τίποτα περισσότερο από το να προωθεί το πακέτο προς τον προορισμό του, με βάση την διεύθυνση προορισμού. Αν σε ένα δρομολογητή, η ουρά εξόδου είναι συμφορημένη, ορισμένα πακέτα απορρίπτονται χωρίς διάκριση μεταξύ κίνησης χαμηλής και υψηλής προτεραιότητας. Αυτό είναι γνωστό σαν υπηρεσία Βέλτιστης Προσπάθειας (best-effort). Για τη σωστή λειτουργία τους, πολλές προηγμένες εφαρμογές απαιτούν εγγύηση του ελάχιστου εύρους ζώνης και της μέγιστης καθυστέρησης πακέτου (latency), εγγυήσεις τις οποίες τα δίκτυα βέλτιστης προσπάθειας δεν είναι δυνατόν να παρέχουν. Για παράδειγμα,

απομακρυσμένα εργαλεία αλληλεπίδρασης (interactive) έχουν συνήθως απαιτήσεις που πηγάζουν από ιδιότητες των ανθρώπινων αισθήσεων, έχοντας έτσι αυστηρές απαιτήσεις σε εύρος ζώνης και καθυστέρηση πακέτου. Η αποτυχία να υλοποιηθούν οι παραπάνω απαιτήσεις, οδηγεί σε λανθασμένη λειτουργία της εφαρμογής.

Στην εργασία αυτή αναφερόμαστε σε μια δομή δικτύου που συνδυάζει την Αρχιτεκτονική Ενοποιημένων Υπηρεσιών με την Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών. Το βασικό αντικείμενο ενασχόλησής μας εστιάζεται στη μελέτη Αλγορίθμων Ελέγχου Αποδοχής Ροών (Measurement Based Admission Control Algorithms). Με τη χρησιμοποίηση των αλγορίθμων αυτών, προσπαθούμε να επιτύχουμε όσο το δυνατόν καλύτερη χρησιμοποίηση (utilization) των γραμμών μας, μικρότερο ποσοστό απωλειών πακέτων (packet loss rate), καθώς και αποδοτική διαμοίραση των πόρων του δικτύου στις ροές που γίνονται αποδεκτές. Αρχικά, μελετώντας τη συμπεριφορά ήδη υπάρχοντων αλγορίθμων και κάνοντας διάφορες προσομοιώσεις, παίρνουμε παρόμοια αποτελέσματα, όσον αφορά τα στοιχεία που αναφέραμε παραπάνω. Στη συνέχεια υλοποιούμε έναν νέο μηχανισμό, ο οποίος βασίζεται στον χρωματισμό των πακέτων πριν αυτά εισέλθουν στο δίκτυο και στην εφαρμογή ενός καινούριου αλγορίθμου αποδοχής ροών (Color MBAC) στους εσωτερικούς δρομολογητές. Με τον νέο αυτό μηχανισμό, κάθε φορά που θέλουμε να κάνουμε έλεγχο για την αποδοχή ή όχι μιας νέας ροής, γνωρίζουμε πέραν του μέσου ρυθμού μετάδοσης κάθε ροής, το ποσοστό των πακέτων που αντιστοιχούνται σε ρυθμό μετάδοσης μεγαλύτερο του μέσου, το ποσοστό των πακέτων που αντιστοιχούνται σε ρυθμό μετάδοσης μεγαλύτερο του μετρούμενου και το ποσοστό των πακέτων που αντιστοιχούνται σε ρυθμό μετάδοσης μικρότερο του μετρούμενου. Επομένως, έχουμε στη διάθεσή μας περισσότερη πληροφορία για την κατάσταση στην οποία βρίσκεται η γραμμή μας και μπορούμε να κάνουμε καλύτερη εκτίμηση για το αν μια νέα ροή μπορεί να γίνει αποδεκτή ή όχι.

2. Απαιτήσεις για ποιότητα υπηρεσίας στο διαδίκτυο

Μεγάλο μέρος της έρευνας για το Διαδίκτυο στρέφεται στο να εντοπιστούν και να προδιαγραφούν οι απαιτήσεις ώστε νέα πρωτόκολλα και υλοποιήσεις να βελτιώσουν την Ποιότητα Υπηρεσίας που υπάρχει σήμερα. Επομένως μια λύση, η οποία θα επέτρεπε την παροχή Ποιότητας Υπηρεσίας στο Διαδίκτυο, θα έπρεπε:

- Να εξυπηρετεί προηγμένες εφαρμογές.
- Να μπορεί να εφαρμοστεί σε ευρεία κλίμακα και να είναι κλιμακούμενη (scalable).
- Να διευκολύνει τη διαχείριση του δικτύου.
- Να επιτρέπει τη διαλειτουργικότητα μεταξύ διαφορετικών υλοποιήσεων τόσο σε επίπεδο εξοπλισμού όσο και σε επίπεδο δικτύων.
- Να μπορεί να υποστηριχτεί από διαφορετικά λειτουργικά συστήματα.

Στη συνέχεια δίνονται διάφορες λεπτομέρειες για τις παραπάνω απαιτήσεις.

2.1. Εξυπηρέτηση απαιτητικών εφαρμογών

Η συνήθης απάντηση των προγραμματιστών στην ερώτηση «τι Ποιότητα Υπηρεσίας χρειάζονται από το δίκτυο», είναι ότι χρειάζονται όσο περισσότερο εύρος ζώνης γίνεται, ελάχιστη καθυστέρηση και διακύμανση καθυστέρησης (jitter) και τις μικρότερες κατά το δυνατόν απώλειες πακέτων. Η απάντηση αυτή, αν και κοινότυπη, είναι αποτέλεσμα της σημερινής πραγματικότητας, η οποία αναγκάζει τους προγραμματιστές δικτυακών εφαρμογών να γράφουν εφαρμογές, που να προσαρμόζονται σε μεγάλα εύρη ρυθμού διέλευσης πακέτων (throughput). Δηλαδή η βασική τους μέριμνα είναι να φτιάχνουν εφαρμογές, τέτοιες ώστε να λειτουργούν σωστά και προβλέψιμα κάτω από τις αντίξοες συνθήκες συμφόρησης, που δημιουργούνται στο Διαδίκτυο.

Για να υποστηριχθεί η ανάπτυξη προχωρημένων δικτυακών εφαρμογών, τα κύρια πρωτόκολλα του στρώματος μεταφοράς του Διαδικτύου, με πρώτο το TCP, σχεδιάστηκαν και βελτιστοποιήθηκαν κατά τέτοιο τρόπο, ώστε να ελαττώνουν την κίνηση που παράγουν στην περίπτωση συμφόρησης και φυσικά να την μεγιστοποιούν στην περίπτωση απουσίας συμφόρησης και διάθεσης εύρους ζώνης. Στη σημερινή υλοποίηση του Διαδικτύου, κάθε νέα σύνδεση γίνεται πάντοτε δεκτή και ποτέ ένα

δίκτυο βέλτιστης προσπάθειας δεν αρνείται την εξυπηρέτησή της. Με αυτόν τον τρόπο κάθε νέα σύνδεση επιβαρύνει την επίδοση των ήδη εγκατεστημένων συνδέσεων, δίνοντας την εντύπωση στον χρήστη ότι ένα δίκτυο βέλτιστης προσπάθειας δεν είναι ποτέ πλήρως κατειλημμένο, αντίθετα με αυτό που συμβαίνει στα συνήθη τηλεφωνικά δίκτυα.

Σε αντίθεση με το κλασσικό Διαδίκτυο, ένας χρήστης δικτύου που υποστηρίζει Ποιότητα Υπηρεσίας αντιλαμβάνεται ένα μοντέλο υπηρεσίας παρόμοιο με αυτό ενός τηλεφωνικού δικτύου. Έτσι, σε πρώτη φάση λαμβάνει χώρα μια διαδικασία παρόμοια με αυτή της εγκατάστασης κλήσης, όπου ο χρήστης προσπαθεί να αρχικοποιήσει μια σύνδεση και να δεσμεύσει τους απαραίτητους πόρους. Υποθέτοντας ότι η κλήση έχει γίνει δεκτή, ο χρήστης έχει στη διάθεσή του ένα καθαρό τηλεπικοινωνιακό διάυλο. Στην αντίθετη περίπτωση, ο χρήστης λαμβάνει ένα σήμα κατειλημμένου, που τον ειδοποιεί ότι η αίτησή του για σύνδεση με τη συγκεκριμένη ποιότητα δεν έγινε δεκτή. Οι μελέτες διάφορων ερευνητικών κέντρων πάνω στο θέμα των δικτυακών απαιτήσεων των εφαρμογών οδήγησε σε κάποια συμπεράσματα για τις παραμέτρους κίνησης, αλλά ακόμη το πεδίο είναι ανοιχτό για περαιτέρω έρευνα ώστε τα αποτελέσματα να είναι πιο συγκεκριμένα. Το κύριο θέμα των απαιτήσεων για Ποιότητα Υπηρεσίας είναι η διασφάλιση (assurance) ορισμένων παραμέτρων κίνησης. Από τις παραμέτρους κίνησης αυτές που αναφέρονται συχνότερα είναι το εύρος ζώνης και η καθυστέρηση. Προβλέπεται ότι για τις εφαρμογές που θα αναπτυχθούν στο κοντινό μέλλον θα είναι απαραίτητο εύρος ζώνης μερικών megabits ανά δευτερόλεπτο (<10Mbps) και καθυστέρηση που θα κυμαίνεται μεταξύ 30 και 500ms. Μερικές εφαρμογές απαιτούν επίσης αυστηρά όρια για τη διακύμανση καθυστέρησης, αλλά οι απαιτήσεις αυτές συνήθως μπορούν να αντιμετωπιστούν με ενταμιευτές εγκατεστημένους στους παραλήπτες των πακέτων.

2.2. Κλιμάκωση

Μία από τις μεγαλύτερες προκλήσεις στο σχεδιασμό του Διαδικτύου είναι η παροχή ποιότητας υπηρεσίας από άκρη σε άκρη για μεγάλο αριθμό ενεργών συνδέσεων και παράλληλα η διασφάλιση της βέλτιστης εκμετάλλευσης των πόρων του Διαδικτύου από τις εφαρμογές. Ο αριθμός των χρηστών που απαιτούν QoS αυξάνεται συνεχώς ,

με αποτέλεσμα να απαιτείται μεγάλος όγκος πληροφορίας για την κατάσταση κάθε ροής πακέτων και μεγάλη υπολογιστική ισχύ από τις μηχανές προώθησής τους. Το πρόβλημα γίνεται πιο έντονο στα σημεία συγκέντρωσης της κίνησης του δικτύου, όπως είναι οι δρομολογητές πηρύνα (core routers) του Διαδικτύου, που είναι αναγκασμένοι να προωθούν χιλιάδες ροές με υψηλές ταχύτητες μετάδοσης. Το Πρωτόκολλο Δέσμευσης Πόρων (Resource Reservation Protocol, RSVP), αποτελεί μια λύση για το παραπάνω πρόβλημα, η οποία όμως έχει αποδειχθεί πως δεν μπορεί να κλιμακωθεί.

2.3. Εύκολη διαχείριση και παρακολούθηση χρήσης πόρων

Όπως σε κάθε δίκτυο με περιορισμένους πόρους, έτσι και στο Διαδίκτυο, απαιτούνται μηχανισμοί για τη σωστή διαχείριση και χρέωσή τους. Οι μηχανισμοί αυτοί πρέπει να λειτουργούν με αποδοτικό τρόπο ώστε να δίνουν στους τελικούς χρήστες όλα όσα υπόσχεται ένα ικανό δίκτυο Ποιότητας Υπηρεσίας, χωρίς να δημιουργούνται επιπρόσθετα προβλήματα στο σχεδιασμό του δικτύου και στη διαχείρισή του (από τηλεπικοινωνιακής άποψης). Επίσης οι μηχανισμοί αυτοί θα επιτρέπουν ένα ελαστικό σετ από πολιτικές και θα αποτρέπουν προσπάθειες εξαπάτησης από πλευράς χρηστών των υπηρεσιών Ποιότητας Υπηρεσίας του δικτύου.

Η παρεχόμενη Ποιότητα Υπηρεσίας κατά πάσα πιθανότητα θα χρεώνεται ανάλογα. Για αυτό το λόγο θα πρέπει να δίνεται η δυνατότητα και στους τελικούς χρήστες αλλά και στους λειτουργούς των δικτύων να μετρούν και να ελέγχουν την απόδοση του δικτύου και των παρεχόμενων υπηρεσιών. Η ανάγκη για παρακολούθηση του δικτύου προϋποθέτει όχι μόνο την ύπαρξη εργαλείων παρακολούθησης, αλλά και γνώση για το τι πρέπει να παρακολουθείται.

2.4. Διαφορετικές υλοποιήσεις και λειτουργικά συστήματα

Κάθε προσπάθεια και προτεινόμενη λύση για Ποιότητα Υπηρεσίας στο Internet οφείλει να επιτρέπει την ύπαρξη πολλαπλών υλοποιήσεων των βασικών λειτουργικών οντοτήτων (προωθητές πακέτων, ταξινομητές πακέτων, έλεγχος αποδοχής), που θα μπορούν όμως να συνεργάζονται μεταξύ τους.

Διαλειτουργικότητα σε επίπεδο υλικού : Η ανάπτυξη τόσο λογισμικού όσο και υλικού για την καλύτερη Ποιότητα Υπηρεσίας στο Διαδίκτυο κάνουν επιτακτική την ανάγκη για νέα πρωτόκολλα. Η παραπάνω ανάγκη οδηγεί στην τυποποίηση (standard) και ένας από τους φορείς που δραστηριοποιείται έντονα πάνω σε αυτό το θέμα είναι η IETF. Σήμερα βλέπουμε ότι οι κατασκευαστές όχι μόνο προσπαθούν να ακολουθήσουν πιστά τα πρότυπα της IETF αλλά και να συμβάλλουν σε αυτά.

Διαλειτουργικότητα διαφορετικών – ανομοιογενών δικτύων: Μεταξύ διαφορετικών δικτύων μπορούμε να ανοίξουμε ένα κανάλι ροών μέσω σηματοδότησης και να ορίσουμε μέσω ειδικών πρωτοκόλλων την Ποιότητα Υπηρεσίας. Με αυτά τα πρωτόκολλα γίνονται οι διαπραγματεύσεις μεταξύ αυτόνομων δικτύων σύμφωνα με τις απαιτήσεις που έχουμε όσον αφορά την Ποιότητα Υπηρεσίας. Όλα αυτά κάνουν επιτακτική την ανάγκη για τη δημιουργία προτύπων ώστε να βοηθηθεί η επικοινωνία και η διαπραγμάτευση μεταξύ ξένων δικτύων.

Υποστήριξη από λειτουργικά συστήματα : Τα τερματικά συστήματα (hosts) πρέπει να είναι σε θέση να εγκαθιστούν αιτήσεις Ποιότητας Υπηρεσίας για τις ροές τους. Τα τερματικά συστήματα πρέπει να είναι σε θέση να ορίζουν κατάλληλα στο δίκτυο, τους εαυτούς τους ή τους χρήστες, με αντικειμενικό σκοπό την εξακρίβωση της γνησιότητας του χρήστη (authentication), την εξουσιοδότηση (authorization) και τον λογιστικό έλεγχο (accounting). Επιπλέον, για την παροχή αληθινής Ποιότητας Υπηρεσίας από άκρη σε άκρη στο δίκτυο, τα λειτουργικά συστήματα θα πρέπει να υποστηρίζουν ροές που απαιτούν Ποιότητα Υπηρεσίας. Αυτού του είδους η πραγματικού χρόνου λειτουργικότητα (real-time functionality) δεν υπάρχει στα περισσότερα σημερινά τερματικά συστήματα, με αποτέλεσμα τα πακέτα να είναι δυνατό να υποστούν συμφόρηση λόγω της στοίβας δικτύου στο λειτουργικό σύστημα, της μνήμης του συστήματος ή του χρόνου επεξεργασίας.

3. Αρχιτεκτονικές και υπηρεσίες QoS

Στη συνέχεια γίνεται μια καταγραφή των αρχιτεκτονικών που έχουν σχεδιαστεί για την παροχή Ποιότητας Υπηρεσίας σε δίκτυα IP. Για κάθε μία από τις αρχιτεκτονικές αυτές παρουσιάζουμε και τις υπηρεσίες με βάση τις οποίες παρέχει QoS.

3.1. Ενοποιημένες Υπηρεσίες (Integrated Services, Intserv)

Όπως είναι γνωστό, τα δίκτυα που βασίζονται στο πρωτόκολλο IP είναι δίκτυα μεταγωγής πακέτου και ως εκ τούτου δεν μπορούν να εξυπηρετήσουν εφαρμογές που απαιτούν συγκεκριμένη Ποιότητα Υπηρεσίας. Αυτό οφείλεται στο γεγονός ότι οι δρομολογητές του Διαδικτύου δεν γνωρίζουν αν τα πακέτα που δρομολογούν ανήκουν σε κάποια χρονικά ευαίσθητη υπηρεσία όπως είναι η φωνή ή αν προέρχονται από πηγές οι οποίες δεν θέτουν στο δίκτυο κανένα περιορισμό ως προς το χρόνο παράδοσης, όπως είναι η μεταφορά αρχείων και το ηλεκτρονικό ταχυδρομείο.

Η ανάπτυξη των ενοποιημένων υπηρεσιών ήταν μία μεγάλη πρόκληση για την κοινότητα του Διαδικτύου. Χρησιμοποιούμε τον όρο Ενοποιημένες Υπηρεσίες για ένα μοντέλο παροχής υπηρεσιών δικτύου, που περιλαμβάνει, εκτός από υπηρεσίες βέλτιστης προσπάθειας (best-effort), υπηρεσίες πραγματικού χρόνου και έλεγχο του διαμοιρασμού των συνδέσμων. Η φιλοσοφία του μοντέλου παροχής υπηρεσιών Ενοποιημένων Υπηρεσιών, έχει να κάνει με τη δέσμευση πόρων και τη διατήρηση πληροφορίας για αυτή, σε κάθε δρομολογητή του δικτύου από τον οποίο πρόκειται να περάσει η κίνηση μιας ροής για την οποία δεσμεύονται οι πόροι. Το επίτευγμα των Ενοποιημένων Υπηρεσιών είναι ότι διατηρούν το μοντέλο μεταγωγής πακέτων πάνω στο οποίο έχει χτιστεί το Διαδίκτυο και παράλληλα επιτρέπουν τη δέσμευση πόρων για εφαρμογές πραγματικού χρόνου.

Στην Αρχιτεκτονική των Ενοποιημένων Υπηρεσιών ένας αριθμός από πρωτόκολλα και μηχανισμούς χρησιμοποιείται για αποκλειστική δέσμευση πόρων. Για να είμαστε βέβαιοι για τη σωστή απόδοση πόρων, πρέπει πριν αρχίσουν να μεταδίδονται τα πακέτα της κάθε ροής να γίνει ένας έλεγχος κατά μήκος του μονοπατιού απ' όπου θα περάσει η συγκεκριμένη ροή, για το αν οι πόροι αυτοί είναι παντού διαθέσιμοι. Ο

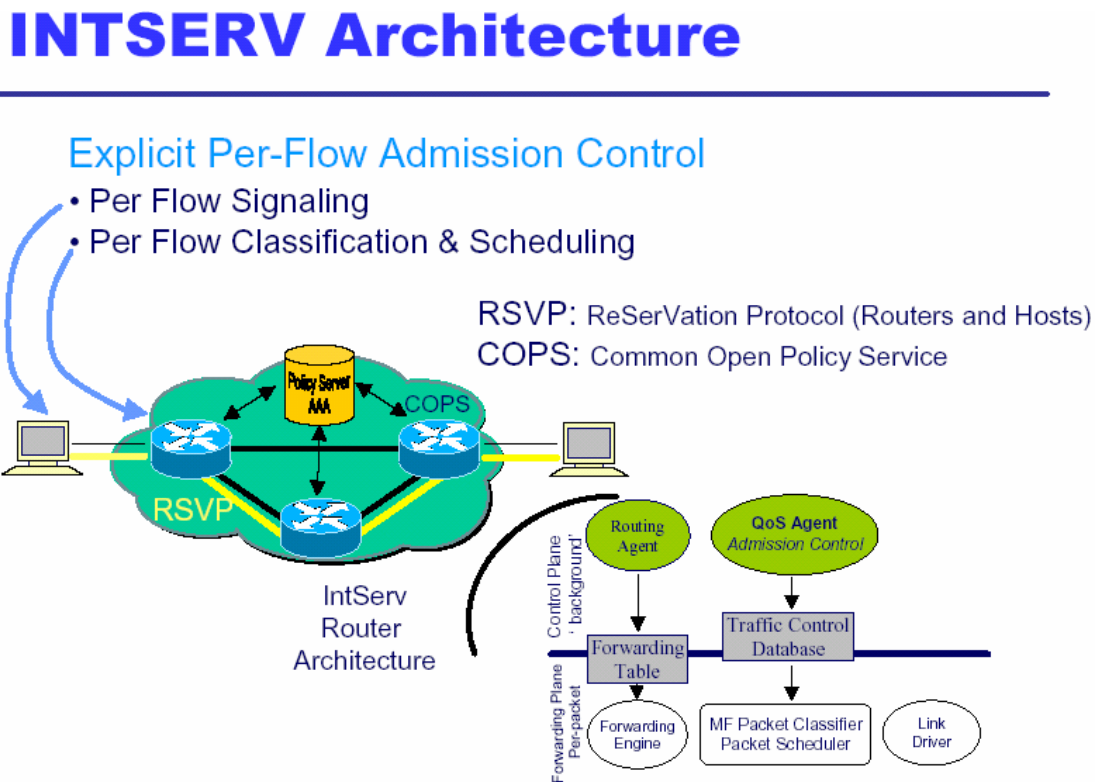
εκάστοτε πομπός, αρχικά ενημερώνει το δίκτυο με τα χαρακτηριστικά και τον παραλήπτη της ροής που θέλει να εγκαταστήσει. Το δίκτυο αποδέχεται την καινούρια ροή μόνο αν υπάρχουν επαρκείς πόροι για να ικανοποιήσουν τις απαιτήσεις της ροής. Αν η δέσμευση πραγματοποιηθεί τότε η εφαρμογή μπορεί να αρχίσει και να στέλνει πακέτα.

Σύμφωνα με την Αρχιτεκτονική Ενοποιημένων Υπηρεσιών η κύρια ποιότητα υπηρεσίας που πρέπει να παρέχεται είναι η διαφορά στην ανά πακέτο καθυστέρηση (per packet delay, jitter), και ιδιαίτερα η μέγιστη τιμή αυτής της διαφοράς. Και αυτό γιατί ο χρόνος παραλαβής των πακέτων (time of delivery) είναι από τους πιο σημαντικούς παράγοντες στις εφαρμογές πραγματικού χρόνου.

Οι Ενοποιημένες Υπηρεσίες αποτελούνται από τέσσερα λειτουργικά μέρη:

- Το πρωτόκολλο σηματοδότησης (π.χ. RSVP),
- Τη διαδικασία ελέγχου αποδοχής κλήσης,
- Τη διαδικασία διαχωρισμού της κυκλοφορίας ανά ροή
- Τη διαδικασία χρονοπρογραμματισμού αποστολής κίνησης

Στο παρακάτω σχήμα παρουσιάζεται το μοντέλο Αρχιτεκτονικής Ενοποιημένων Υπηρεσιών, με τα λειτουργικά του μέρη:



Η μονάδα επεξεργασίας σηματοδότησης (1^ο λειτουργικό μέρος) λαμβάνει αιτήσεις από το χρήστη για εγκατάσταση νέων ροών ή κατάργηση παλαιών και τις προωθεί στις

άλλες εσωτερικές μονάδες του δρομολογητή. Κατά συνέπεια η μονάδα επεξεργασίας σηματοδοσίας υλοποιεί το πρωτόκολλο σηματοδοσίας, που στην περίπτωση των Ενοποιημένων Υπηρεσιών Διαδικτύου είναι το Πρωτόκολλο Δέσμευσης Πόρων (Resource Reservation Protocol, RSVP).

Η μονάδα αποδοχής κλήσης (2^ο λειτουργικό μέρος) αποφασίζει αν μια νέα αίτηση εγκατάστασης ροής μπορεί να γίνει αποδεκτή ή όχι. Συνήθως αυτός ο έλεγχος γίνεται σε δύο φάσεις. Στην πρώτη φάση ελέγχεται αν ο χρήστης που ζητάει να γίνει η συγκεκριμένη δέσμευση έχει και την ανάλογη άδεια (Policy Control). Στη δεύτερη φάση συγκρίνονται οι παράμετροι της κίνησης της νέας ροής με τους διαθέσιμους πόρους του δρομολογητή. Η αίτηση γίνεται αποδεκτή μόνο αν ο χρήστης έχει το δικαίωμα να κάνει τη συγκεκριμένη δέσμευση και εφόσον υπάρχουν οι ανάλογοι πόροι στο σύστημα. Σε αυτήν την περίπτωση ενημερώνεται και η τοπική βάση δεδομένων στην οποία φυλάσσονται οι ενεργές ροές με τις παραμέτρους κίνησής τους.

Η μονάδα αναγνώρισης ροής (3^ο λειτουργικό μέρος) αναλαμβάνει να βρίσκει τη ροή στην οποία ανήκει κάθε εισερχόμενο πακέτο και να το τοποθετεί στην αντίστοιχη ουρά του χρονοδρομολογητή πακέτων. Η εύρεση της ροής στην οποία ανήκει ένα συγκεκριμένο πακέτο γίνεται βάση της διεύθυνσης προορισμού, της διεύθυνσης πηγής, της θύρας πηγής (source port number), της θύρας προορισμού (destination port number) καθώς και του ενδείκτη πρωτοκόλλου μεταφοράς (Protocol ID). Αν ένα πακέτο δεν ανήκει σε καμία ενεργή ροή, τότε αυτό αντιμετωπίζεται ως πακέτο κλάσης βέλτιστης προσπάθειας (φυσικά τα πακέτα της κλάσης βέλτιστης προσπάθειας αντιμετωπίζουν χειρότερη συμπεριφορά σε σχέση με τα πακέτα των υπόλοιπων κλάσεων).

Η μονάδα χρονοδρομολόγησης πακέτων (4^ο λειτουργικό μέρος) διατηρεί μια ξεχωριστή ουρά πακέτων για κάθε ενεργή ροή. Η λειτουργία της χωρίζεται σε δύο φάσεις. Αρχικά για κάθε μια ροή ελέγχεται κατά πόσο είναι σύμφωνη με το αρχικό προφίλ κίνησης που είχε ζητήσει από το δίκτυο. Πακέτα που δεν είναι σύμφωνα με το αρχικό προφίλ κίνησης απορρίπτονται. Στη συνέχεια η μονάδα χρονοδρομολόγησης αδειάζει μία μία τις ουρές πακέτων εξυπηρετώντας πρώτη εκείνη με τη μεγαλύτερη προτεραιότητα.

Μέσα στο μοντέλο Ενοποιημένων Υπηρεσιών Διαδικτύου (Internet integrated Services, IntServ) ορίζονται πολλαπλές κατηγορίες τηλεπικοινωνιακής κίνησης (traffic classes), οι οποίες έχουν διαφορετικές απαιτήσεις από το δίκτυο, όσον αφορά

την Ποιότητα Υπηρεσίας. Έτσι πέραν της υπάρχουσας Κλάσης Βέλτιστης Προσπάθειας (Best Effort Service) ορίζονται δύο νέες κατηγορίες κίνησης: η Κλάση Ελεγχόμενου Φορτίου (Controlled Load Service) και η Κλάση Εγγυημένης Υπηρεσίας (Guaranteed Service).

3.1.1. Η Κλάση Ελεγχόμενου Φορτίου (Controlled Load Service)

Η Κλάση Ελεγχόμενου Φορτίου παρέχει σχεδόν την ίδια Ποιότητα Υπηρεσίας τόσο κάτω από συνθήκες υπερφόρτωσης δικτύου όσο και κάτω από συνθήκες ελαφριάς κίνησης στο δίκτυο. Η βασική διαφορά σε σχέση με την υπάρχουσα Κλάση Βέλτιστης Προσπάθειας του Διαδικτύου είναι ότι η αύξηση της τηλεπικοινωνιακής κίνησης μέσα στο δίκτυο δεν επιδεινώνει την Ποιότητα Υπηρεσίας των ροών που υπόκεινται στη Κλάση Ελεγχόμενου Φορτίου. Αντίθετα, μια ροή που υπόκειται στην Κλάση Βέλτιστης Προσπάθειας θα υπόκειντο σε συνεχή και σταδιακή χειροτέρευση της προσφερόμενης Ποιότητας Υπηρεσίας με την αύξηση του φόρτου του δικτύου.

Η κατηγορία Ελεγχόμενου Φορτίου είναι κατάλληλη για υπηρεσίες πολυμέσων, οι οποίες μπορούν να ανεχθούν μικρές απώλειες πακέτων και μικρές καθυστερήσεις, αρκεί αυτό να γίνεται μέσα σε ένα λογικό πλαίσιο. Για παράδειγμα, η υπηρεσία κινούμενης εικόνας κατά απαίτηση (Video On Demand) θα μπορούσε να χρησιμοποιήσει τη συγκεκριμένη κλάση, αρκεί το τερματικό του δέκτη να είχε το κατάλληλο μέγεθος ενταμιευτή, ώστε να μπορεί να κρατήσει ψηφιακά δεδομένα, το χρονικό μήκος των οποίων πρέπει να είναι μεγαλύτερο από τη μέγιστη καθυστέρηση που μπορεί να εισάγει το δίκτυο. Μια τέτοιου είδους υπηρεσία πολυμέσων πραγματικού χρόνου ονομάζεται προσαρμοζόμενη υπηρεσία πραγματικού χρόνου (adaptive real-time application). Αντίθετα, για την υπηρεσία μετάδοσης φωνής μεταξύ δύο συνομιλητών, όπου η μέγιστη διαφορά φάσης δεν πρέπει να είναι μεγαλύτερη των 125ms, η κατηγορία ελεγχόμενου φορτίου είναι ακατάλληλη. Ακόμη η κλάση ελεγχόμενου φορτίου είναι κατάλληλη και για «ελαστικές εφαρμογές» (δηλαδή εφαρμογές που δεν έχουν ιδιαίτερες απαιτήσεις ποιότητας πέρα από τη μέση από άκρο σε άκρο καθυστέρηση, π.χ. e-mail, FTP κ.τ.λ.).

Μια εφαρμογή πολυμέσων, που θέλει να χρησιμοποιήσει την υπηρεσία Ελεγχόμενου Φορτίου, πρέπει πάντοτε να στέλνει στο δίκτυο μια περιγραφή των χαρακτηριστικών της κίνησης που παράγει. Αν μια αίτηση για μια νέα ροή Ελεγχόμενου Φορτίου γίνει

αποδεκτή από το δίκτυο, τότε οι δρομολογητές του δικτύου δεσμεύοντας τους κατάλληλους πόρους, διασφαλίζουν ότι τα πακέτα της συγκεκριμένης ροής θα απολαμβάνουν την ίδια Ποιότητα Υπηρεσίας με ροές που ανήκουν στη Κλάση Βέλτιστης Προσπάθειας σε συνθήκες χαμηλού φόρτου.

3.1.2. Η Κλάση Εγγυημένης Υπηρεσίας (Guaranteed Service)

Τα πακέτα μιας ροής που υπόκεινται στη Κλάση Εγγυημένης Υπηρεσίας φθάνουν στον προορισμό τους μέσα σε ένα προκαθορισμένο χρονικό διάστημα, ενώ παράλληλα δεν πρόκειται να απορριφθούν λόγω υπερχείλισης των ενταμιευτών στους δρομολογητές του δικτύου. Τα παραπάνω βέβαια ισχύουν εφόσον η πηγή της συγκεκριμένης ροής στέλνει πακέτα στο δίκτυο σύμφωνα με τις παραμέτρους κίνησης που έχουν συμφωνηθεί με το δίκτυο. Ωστόσο, η Κλάση Εγγυημένης Υπηρεσίας δεν ελέγχει την ελάχιστη ή τη μέση καθυστέρηση μιας ροής, ούτε ελαχιστοποιεί τη διακύμανση της μέσης χρονικής απόστασης μεταξύ διαδοχικών πακέτων της συγκεκριμένης ροής (jitter). Η Κλάση Εγγυημένης Υπηρεσίας προορίζεται για υπηρεσίες πολυμέσων με αυστηρότατες απαιτήσεις όσον αφορά το χρόνο παράδοσης των ψηφιακών δεδομένων. Τέτοιες εφαρμογές είναι ορισμένες εφαρμογές μεταφοράς ήχου ή κινούμενης εικόνας, όπου το μέγεθος των ενταμιευτών στους αποκωδικοποιητές είναι σταθερό και μικρό και έτσι κάθε καθυστερημένο πακέτο απορρίπτεται.

Επομένως, για να κάνει χρήση της υπηρεσίας GRS, μια εφαρμογή παρέχει περιγραφή της αναμενόμενης κίνησης που πρόκειται να διοχετεύσει στο δίκτυο (προφίλ) και το δίκτυο με τη σειρά του υπολογίζει και επιστρέφει την από άκρο σε άκρο εγγύηση καθυστέρησης που μπορεί να εγγυηθεί. Εάν η εγγύηση αυτή είναι ανεκτή από την εφαρμογή, η μετάδοση μπορεί να ξεκινήσει, αλλιώς η εφαρμογή έχει τη δυνατότητα να προσαρμόσει τα χαρακτηριστικά της κίνησής της, να επαναδιατυπώσει αίτηση μετάδοσης και να περιμένει νέα εκτίμηση για την εγγύηση της από άκρο σε άκρο καθυστέρησης από το δίκτυο.

Το μοντέλο Ενοποιημένων Υπηρεσιών του Διαδικτύου διαχωρίζει το πρωτόκολλο που χρησιμοποιείται για μεταφορά αιτήσεων δέσμευσης πόρων δικτύου από το μηχανισμό ελέγχου και περιγραφής της κίνησης του χρήστη (QoS control) . Στη συνέχεια περιγράφουμε το Πρωτόκολλο Δέσμευσης Πόρων.

3.2. Πρωτόκολλο Δέσμευσης πόρων (Resource Reservation Protocol, RSVP)

Το Πρωτόκολλο Δέσμευσης πόρων (RSVP) είναι ένα πρωτόκολλο σηματοδοσίας που ορίστηκε από την IETF. Σύμφωνα με αυτό μπορούν να δεσμευθούν πόροι για κάποιες ροές κίνησης, δηλαδή να ανατεθούν προτεραιότητες, να δεσμευθεί χώρος ενταμίευσης και εύρος ζώνης, σε όλους τους ενδιάμεσους δρομολογητές και μεταγωγείς κίνησης κατά μήκος ενός μονοπατιού του δικτύου. Χρησιμοποιώντας μια σύνδεση για τη σηματοδοσία διαφορετική από τη σύνδεση για τη ροή κίνησης της πληροφορίας μια λαμβάνουσα εφαρμογή στέλνει μια αίτηση δέσμευσης πόρων μέσω του πρωτοκόλλου RSVP. Το πρωτόκολλο RSVP μπορεί να λειτουργήσει τόσο για συνδέσεις από σημείο σε σημείο όσο και για συνδέσεις από σημείο προς πολλά σημεία διαδίδοντας τις αιτήσεις δέσμευσης πόρων σε όλους τους δρομολογητές στα μονοπάτια από τα οποία θα περάσει η ροή κίνησης της πληροφορίας. Αυτό σημαίνει ότι διαφορετικοί δέκτες της ίδιας συνόδου μπορούν να ζητήσουν διαφορετική ποιότητα υπηρεσίας (αυτή είναι και μια χαρακτηριστική διαφορά του πρωτοκόλλου αυτού από αντίστοιχα πρωτόκολλα σηματοδοσίας που έχουν αναπτυχθεί για δίκτυα μεταγωγής κυκλώματος). Η δυνατότητα αυτή παρέχεται είτε γιατί δεν έχουν όλοι οι δέκτες την ίδια δικτυακή υποδομή (π.χ ένας δέκτης μπορεί να λαμβάνει μέρος σε μια υπηρεσία τηλεδιάσκεψης μέσω ενός απλού modem στα 56kbps ενώ ένας άλλος να είναι συνδεδεμένος σε ένα LAN των 10Mbps), είτε γιατί δεν επιθυμούν όλοι να επιβαρυνθούν οικονομικά το ίδιο.

Ένα επιπλέον χαρακτηριστικό του πρωτοκόλλου RSVP είναι η υποστήριξη δυναμικής μεταβολής της Ποιότητας υπηρεσίας μιας δεδομένης ροής πακέτων. Ανά πάσα στιγμή ο κάθε δέκτης μπορεί να μεταβάλλει τις παραμέτρους Ποιότητας Υπηρεσίας μιας ροής χωρίς να είναι απαραίτητο να γίνει πρώτα προσωρινή κατάργησή της και εκ νέου επανεγκατάστασή της. Ένα άλλο μοναδικό χαρακτηριστικό που συναντάμε στο RSVP είναι ότι η δέσμευση των πόρων του δικτύου γίνονται από το δέκτη της πληροφορίας και όχι τον πομπό. Μάλιστα, ο δέκτης της πληροφορίας μπορεί να ζητήσει από το δίκτυο να δεσμευτούν λιγότεροι πόροι απ' ότι ορίζεται στο προφίλ κίνησης του πομπού. Αυτό είναι απαραίτητο για

την υποστήριξη ετερογενών συνδέσεων μέσα στην ίδια σύνοδο. Ακόμη, το γεγονός ότι η δέσμευση πόρων γίνεται από το δέκτη της πληροφορίας διευκολύνει την ύπαρξη συνόδων με πολύ μεγάλο αριθμό μελών.

Το πρωτόκολλο RSVP τοποθετείται ακριβώς πάνω από το πρωτόκολλο IP στη στοίβα πρωτοκόλλου TCP/IP καταλαμβάνοντας τη θέση πρωτοκόλλου μεταφοράς. Ωστόσο, το RSVP παρέχει υπηρεσίες επιπέδου συνόδου εφόσον δε μεταφέρει δεδομένα εφαρμογής. Η δέσμευση πόρων γίνεται από τον δέκτη της πληροφορίας και όχι από τον πομπό. Πάντως, για να μπορέσει ο δέκτης να δεσμεύσει πόρους του δικτύου θα πρέπει να ξέρει τα χαρακτηριστικά της κίνησης (μέσο και μέγιστο εύρος ζώνης, μέγιστη χρονική καθυστέρηση κ.λ.π.) που πρόκειται να αρχίσει να λαμβάνει. Γι' αυτό το λόγο, προτού ο δέκτης κάνει οποιαδήποτε ενέργεια για δέσμευση πόρων, ο πομπός στέλνει ένα ειδικό μήνυμα, ονομαζόμενο PATH message, με σκοπό να ενημερώσει το δέκτη και τους ενδιάμεσους δρομολογητές, για τα χαρακτηριστικά της κίνησης που πρόκειται να αρχίσει να εκπέμπει. Το μήνυμα PATH, μέχρι να φτάσει στο δέκτη (η στους δέκτες αν η διεύθυνση προορισμού είναι διεύθυνση πολλαπλών περιορισμών, multicast IP address) περνάει μέσα από έναν ή περισσότερους δρομολογητές. Κάθε ενδιάμεσος δρομολογητής που λαμβάνει ένα μήνυμα PATH ελέγχει αρχικά αν είναι έγκυρο ή όχι το περιεχόμενό του. Αν κατά τη διάρκεια επεξεργασίας του μηνύματος διαπιστωθεί κάποιο λάθος, τότε ο ενδιάμεσος δρομολογητής στέλνει ένα ειδικό μήνυμα λάθους στον πομπό ώστε να γίνουν οι κατάλληλες ενέργειες. Αν το περιεχόμενο του μηνύματος PATH είναι έγκυρο, τότε αυτό φυλάσσεται σε μια τοπική βάση δεδομένων, τίθεται ο χρονιστής επανεκκίνησης για τη συγκεκριμένη ροή και τέλος αποστέλλεται στον επόμενο δρομολογητή.

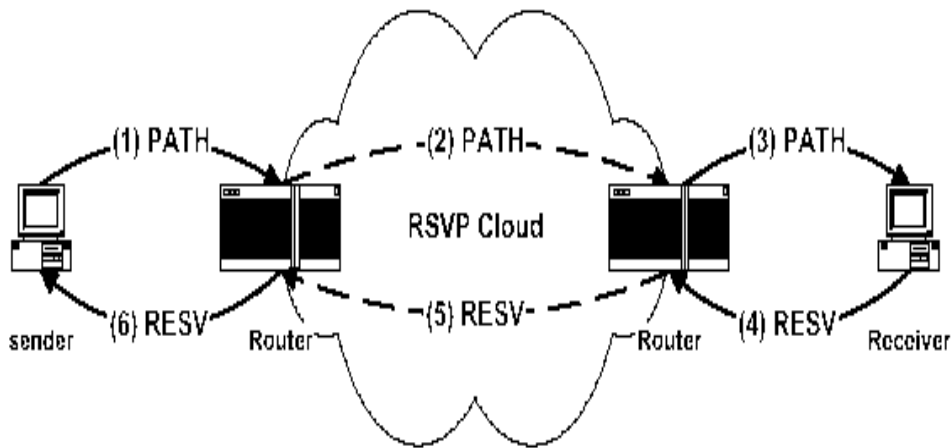
Ο λόγος που οι ενδιάμεσοι δρομολογητές αποθηκεύουν τα περιεχόμενα των μηνυμάτων PATH είναι ο εξής: για κάθε μήνυμα PATH ένας δρομολογητής δέχεται μία ή περισσότερες αιτήσεις για δέσμευση εσωτερικών πόρων (RESV message). Αν κάποια στιγμή ο πομπός αποφασίσει να σταματήσει να στέλνει δεδομένα, τότε όλοι οι ενδιάμεσοι δρομολογητές θα πρέπει να καταργήσουν αυτομάτως και όλες τις δεσμεύσεις πόρων που έχουν γίνει για τη συγκεκριμένη ροή πακέτων. Επιπλέον ο χρονιστής τίθεται για τη διασφάλιση της σωστής λειτουργίας του δικτύου: αν για χρονικό διάστημα ίσο με την περίοδο του χρονιστή, ο ενδιάμεσος δρομολογητής δε λάβει μήνυμα ανανέωσης από τον πομπό της πληροφορίας, τότε το δίκτυο θεωρεί ότι ο πομπός της πληροφορίας σταμάτησε να εκπέμπει κίνηση στο δίκτυο και άρα όλες οι συσχετιζόμενες δεσμεύσεις πρέπει να καταργηθούν. Μηνύματα ανανέωσης είναι

υποχρεωμένοι να στέλνουν τόσο οι πομποί όσο και οι δέκτες σε τακτά χρονικά διαστήματα, μικρότερα των αντίστοιχων χρονιστών που τίθενται στους ενδιάμεσους δρομολογητές.

Όταν το μήνυμα PATH περάσει μέσα από όλους τους ενδιάμεσους δρομολογητές και φτάσει τελικά στο δέκτη (ή στους δέκτες) της πληροφορίας, τότε αυτός στέλνει στο δίκτυο το κατάλληλο μήνυμα RSVP, που ονομάζεται RESV message, για τη δέσμευση των αντίστοιχων πόρων. Το μήνυμα RESV περιέχει τους πόρους που θέλει ο συγκεκριμένος δέκτης να δεσμεύσει από το δίκτυο για τη ροή πακέτων που περιγράφεται από το μήνυμα PATH που έλαβε. Είναι αρκετά πιθανό το εύρος ζώνης που ζητάει ένας δέκτης να δεσμεύσει από το δίκτυο να είναι μικρότερο από την αντίστοιχη τιμή που υπάρχει στο μήνυμα PATH. (σχήμα)

Η επεξεργασία του μηνύματος RESV στους ενδιάμεσους δρομολογητές περιλαμβάνει δύο ελέγχους. Ο πρώτος έλεγχος αποσκοπεί στην εξακρίβωση της ταυτότητας του δέκτη αλλά και στο αν του παρέχεται το δικαίωμα να κάνει τη συγκεκριμένη δέσμευση πόρων από το δίκτυο (Policy Control). Ο δεύτερος έλεγχος αποσκοπεί στο να εξακριβωθεί αν υπάρχουν αρκετοί διαθέσιμοι εσωτερικοί πόροι για την εξυπηρέτηση της συγκεκριμένης δέσμευσης (Flow Admission Control). Αν έστω και ένας από τους δύο ελέγχους αποτύχει, στέλνεται το κατάλληλο μήνυμα λάθους (RESV_ERR) στο δέκτη που ζήτησε να γίνει η συγκεκριμένη δέσμευση. Στην αντίθετη περίπτωση ενημερώνεται η μονάδα χρονοδρομολόγησης πακέτων του δρομολογητή για τη νέα ροή και το μήνυμα RESV αποστέλλεται στον επόμενο δρομολογητή.

Όπως έχει ήδη αναφερθεί, το ίδιο μήνυμα PATH μπορεί να κατευθύνεται σε περισσότερους από ένα δέκτες. Σε αυτήν την περίπτωση κάθε ένας δέκτης θα απαντήσει στέλνοντας ένα μήνυμα RESV, οι παράμετροι του οποίου, όσον αφορά το εύρος ζώνης που επιθυμεί να δεσμεύσει από το δίκτυο, μπορεί να διαφέρουν από τις παραμέτρους των μηνυμάτων RESV των υπόλοιπων δεκτών. Κατά συνέπεια, θα υπάρξουν κάποιοι δρομολογητές οι οποίοι θα δεχθούν περισσότερα από ένα μηνύματα RESV για το ίδιο μήνυμα PATH (σημείο συγχώνευσης). Σε αυτήν την περίπτωση ο δρομολογητής θα στείλει στον επόμενο δρομολογητή ένα μόνο μήνυμα RESV του οποίου η τιμή για το εύρος ζώνης που πρέπει να δεσμευθεί θα είναι η μεγαλύτερη από τα μηνύματα RESV που έλαβε ο συγκεκριμένος δρομολογητής και έγιναν αποδεκτά.



Τα επίπεδα υπηρεσίας που υποστηρίζει το πρωτόκολλο RSVP είναι:

- Η Εγγυημένη (Guaranteed) Κλάση Ποιότητας Υπηρεσίας που εξασφαλίζει το εύρος ζώνης για τη ροή των πακέτων της πληροφορίας χωρίς απώλειες και με εγγύηση για τη μέγιστη καθυστέρηση που θα αντιμετωπίσουν τα πακέτα της ροής κίνησης μέχρι τον προορισμό τους.
- Η Προβλεπόμενη (Predictive) Κλάση Ποιότητας Υπηρεσίας που εξασφαλίζει το εύρος ζώνης για τη ροή των πακέτων της πληροφορίας χωρίς απώλειες. Δεν παρέχει καμιά εγγύηση για τη μέγιστη καθυστέρηση των πακέτων της ροής κίνησης μέχρι τον προορισμό τους.
- Η Κλάση Ποιότητας Υπηρεσίας Ελεγχόμενου Φορτίου (Controlled Load) που εξασφαλίζει αντιμετώπιση στα πακέτα μιας ροής κίνησης, όμοια με αυτή που θα είχαν από το δίκτυο αν ήταν ελαφρώς φορτωμένο με κίνηση. Δεν παρέχονται εγγυήσεις όσον αφορά το εύρος ζώνης και την καθυστέρηση.
- Η Κλάση Ποιότητας Υπηρεσίας Βέλτιστης Προσπάθειας (Best Effort) που συνεπάγεται ότι το δίκτυο θα προσπαθήσει να μεταδώσει την πληροφορία, αλλά δεν παρέχει καμιά εγγύηση γι' αυτό.

3.3. Πλεονεκτήματα του μοντέλου IntServ-RSVP

Η αρχιτεκτονική που προέρχεται από τις Ενοποιημένες Υπηρεσίες (Integrated Services, IntServ) έχει έναν αριθμό από οφέλη. Πρώτα απ' όλα, το μοντέλο σχεδιάστηκε για να παρέχει απόλυτη εγγύηση υπηρεσίας. Η συμπεριφορά του

μοντέλου προδιαγράφηκε με αρκετή λεπτομέρεια ώστε να επιτρέπει στους πελάτες RSVP (RSVP clients) να προδιαγράψουν κάθε κατηγορία υπηρεσίας λεπτομερώς. Επειδή το RSVP «τρέχει» σε κάθε δρομολογητή από την πηγή έως τον προορισμό, κάθε ροή μπορεί να παρακολουθηθεί ώστε να αποτραπεί η κατανάλωση περισσότερων πόρων από αυτούς που αρχικά είχαν ζητηθεί, δεσμευθεί και προφανώς πληρωθεί.

Ένα άλλο όφελος του RSVP είναι ότι χρησιμοποιεί τα ήδη υπάρχοντα πρωτόκολλα δρομολόγησης ώστε να ορίσει το μονοπάτι της ροής μεταξύ της πηγής και του προορισμού. Περιοδικά επαναμεταδίδονται τα μηνύματα PATH και RESV και το πρωτόκολλο μπορεί και αντιδρά στην αλλαγή της τοπολογίας του δικτύου. Ακριβώς αυτά τα ανανεωμένα PATH και RESV μπορούν να χρησιμοποιηθούν για να αλλάξουν το μονοπάτι της δεσμευμένης ροής. Η απώλεια αυτών των μηνυμάτων μπορεί να βοηθήσει επίσης στη διαπίστωση ότι ο αποστολέας ή ο παραλήπτης δεν είναι πλέον ενεργός. Όταν ο δρομολογητής ανακαλύψει αυτήν την απώλεια, αποδεσμεύει τους πόρους που σχετίζονται με τη συγκεκριμένη δέσμευση.

Ένας από τους πρωταρχικούς σκοπούς των Ενοποιημένων Υπηρεσιών ήταν να παρέχει Ποιότητα Υπηρεσίας (Quality of Service, QoS) που να δουλεύει για πηγές από μία πηγή σε έναν προορισμό (unicast) και από μία πηγή σε πολλαπλούς προορισμούς (multicast). Το πρωτόκολλο RSVP σχεδιάστηκε έτσι ώστε να επιτρέπει στα μηνύματα PATH να αναγνωρίζουν όλα τα τερματικά σημεία μιας ροής πολλαπλών προορισμών και να στέλνουν το μήνυμα PATH σε κάθε αποδέκτη. Επίσης, επιτρέπει στα μηνύματα RESV από κάθε αποδέκτη να μπορούν να συνδυάζονται σε μία μόνο αίτηση στα σημεία του δικτύου όπου ροή πολλαπλών προορισμών θα έστελνε την ίδια ροή σε δύο διαφορετικά κανάλια.

3.4. Μειονεκτήματα του μοντέλου Intserv-RSVP

Ως η κυριότερη αδυναμία του μοντέλου Ενοποιημένων Υπηρεσιών (IntServ) μπορεί να θεωρηθεί το γεγονός ότι οι στόχοι που θέτει είναι πολύ φιλόδοξοι. Η απαίτηση όλοι οι δρομολογητές να παίρνουν μέρος στη δέσμευση των πόρων είναι μια διαδικασία η οποία επιβάλλει στον κάθε δρομολογητή να αποθηκεύει και να συντηρεί μεγάλο όγκο πληροφορίας και να έχει μεγάλη υπολογιστική ισχύ. Αυτό το μοντέλο

δεν είναι πρακτικά χρησιμοποιήσιμο για ροές που διαρκούν λίγο γιατί το τίμημα για τη δέσμευση των πόρων είναι μεγαλύτερο ακόμα και από την επεξεργασία όλων των πακέτων της ροής. Πρέπει να τονιστεί ότι το μεγαλύτερο ποσοστό της κίνησης στο Διαδίκτυο αποτελείται από ροές μικρής διάρκειας. Έτσι, σε περιπτώσεις που απαιτείται έστω και ελάχιστη Ποιότητα Υπηρεσίας (QoS) από ροές μικρής διάρκειας, το μοντέλο Ενοποιημένων Υπηρεσιών (IntServ) θα απαιτούσε πολύ κόπο (από πλευράς δικτύου) σε σχέση με το αποτέλεσμα.

Το μοντέλο Ενοποιημένων Υπηρεσιών απαιτεί ένα μεγάλο όγκο πληροφορίας για την κατάσταση της ροής. Η κατάσταση περιλαμβάνει πληροφορία για τον προσδιορισμό της ταυτότητας της ροής και των πόρων που καταναλώνει. Επίσης πρέπει να υπάρχει η δυνατότητα αστυνόμευσης και προγραμματισμού της κίνησης σύμφωνα με τις υποχρεώσεις που προκύπτουν από την προκαθορισμένη δέσμευση πόρων. Ο πηρύνας του δικτύου θα μπορούσε να περιέχει εκατομμύρια τέτοιες συνδέσεις. Χειροτερεύοντας ακόμα το σενάριο, αν η τοπολογία του δικτύου άλλαζε, όλες αυτές οι συνδέσεις θα έπρεπε να διαπραγματευτούν ξανά ταυτοχρόνως. Όλα αυτά καθιστούν σχεδόν αδύνατη την εφαρμογή του RSVP σε μεγάλη κλίμακα.

3.5. Διαφοροποιημένες υπηρεσίες (Differentiated Services)

Το μοντέλο Διαφοροποιημένων Υπηρεσιών (Differentiated Services, DiffServ) είναι μία τεχνολογία που ορίστηκε από την IETF προτείνοντας μια επεκτάσιμη λύση (δεν χρειάζεται η ανά ροή διατήρηση πληροφοριών σε κάθε κόμβο του δικτύου) για την εισαγωγή Ποιότητας Υπηρεσίας στο Διαδίκτυο. Η Αρχιτεκτονική Διαφοροποιημένων υπηρεσιών αναπτύχθηκε προς απάντηση στην ανάγκη για δημιουργία απλών μεθόδων που θα παρέχουν διαφορετικά επίπεδα υπηρεσίας στην κίνηση ενός δικτύου, καθώς και για την υποστήριξη ποικίλων νέων εφαρμογών και συγκεκριμένων απαιτήσεων. Η αρχιτεκτονική αυτή διαφέρει από την αντίστοιχη των Ενοποιημένων Υπηρεσιών στην όλη φιλοσοφία.

Οι Διαφοροποιημένες Υπηρεσίες ελαχιστοποιούν τη σηματοδότηση και επικεντρώνονται σε συσσωρευμένες ροές (aggregate) και Συμπεριφορές Προώθησης Ανά Κόμβο (Per-Hop Behaviour, PHB), που εφαρμόζονται σε σύνολο κλάσεων κίνησης μέσα στο δίκτυο. Οι ροές ταξινομούνται ανάλογα με προκαθορισμένους

κανόνες, έτσι ώστε πολλές ροές εφαρμογών να συγκεντρώνονται σε ένα περιορισμένο σύνολο κλάσεων ροών. Το μυστικό είναι ο συνδυασμός μικρού αριθμού απλών χειρισμών συλλογικών πακέτων με ένα μεγαλύτερο αριθμό πολιτικών ανά ροή για την παροχή μιας ευρείας και εύκαμπτης περιοχής υπηρεσιών. Το πλήθος των ροών, που απαιτούν συγκεκριμένη Ποιότητα Υπηρεσίας, συγκεντρώνονται σε διαφορετικές κλάσεις ανάλογα με το επίπεδο ποιότητας που ζητούν. Το πλήθος των διαφορετικών κλάσεων διατηρείται μικρό και η κάθε κλάση έχει διαφορετική μεταχείριση από το δίκτυο. Με αυτόν τον τρόπο το δίκτυο Διαφοροποιημένων Υπηρεσιών (Differentiated Services, DiffServ) δεν χρειάζεται να κάνει δέσμευση πόρων και δεν είναι αναγκασμένο να αναγνωρίζει κάθε σύνδεση ξεχωριστά και να κρατά μεγάλο όγκο πληροφορίας για τις συνδέσεις. Αυτό αποτελεί και το μεγαλύτερο πλεονέκτημα της αρχιτεκτονικής DiffServ έναντι του μοντέλου IntServ/RSVP, αφού μπορεί εύκολα να κλιμακωθεί.

3.5.1. Βασικές αρχές Διαφοροποιημένων Υπηρεσιών

Η Αρχιτεκτονική Ενοποιημένων Υπηρεσιών και το μοντέλο Βέλτιστης Προσπάθειας αντιπροσωπεύουν δύο ακραίες καταστάσεις στο φάσμα της δέσμευσης των πόρων ενός δικτύου. Από τη μία πλευρά το μοντέλο Βέλτιστης Προσπάθειας βασίζεται στην ανά πακέτο μετάδοση (per packet basis) ενώ οι Ενοποιημένες Υπηρεσίες εξετάζουν κάθε ροή που δημιουργείται. Η Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών κινείται κάπου ενδιάμεσα σε αυτά τα δύο άκρα. Προσπαθεί να προχωρήσει ένα βήμα μπροστά από το μοντέλο Βέλτιστης Προσπάθειας, δηλαδή να παρέχει υπηρεσίες καλύτερες από τις «best-effort». Επιτυγχάνει να λύσει το πρόβλημα της επεκτασιμότητας με τον προσδιορισμό ενός μικρού αριθμού απλών, διαφοροποιημένων χειρισμών προώθησης πακέτων (differentiated packet forwarding treatments), γνωστών με το όνομα Συμπεριφορά Προώθησης Ανά-Κόμβο (Per-Hop Behavior, PHB). Μεμονωμένα δικτυακά στοιχεία υλοποιούν τις Συμπεριφορές Προώθησης Ανά-Κόμβο με μια πληθώρα μηχανισμών και κανόνων αναμονής και εξυπηρέτησης (queueing disciplines). Η ουσία των Διαφοροποιημένων Υπηρεσιών είναι ο συνδυασμός αυτών των Συμπεριφορών Προώθησης Ανά-Κόμβο με προσεκτικά ρυθμισμένους μηχανισμούς πολιτικών κίνησης στα άκρα του δικτύου για την παροχή διάφορων υπηρεσιών. Επιβάλλοντας λειτουργίες ελέγχου πολιτικών στα

άκρα και παρέχοντας απλή μεταχείριση συσσωρευμένων δεδομένων στον πυρήνα του δικτύου, μπορούν να διασφαλιστούν νέες υπηρεσίες IP χωρίς υπερβολική αποθήκευση πληροφορίας κατάστασης ή ακριβών αποφάσεων προώθησης στους δρομολογητές του δικτύου πυρήνα.

Κάθε πακέτο που εισέρχεται στο δίκτυο Διαφοροποιημένων Υπηρεσιών μαρκάρεται με ένα Κωδικό Σημείο Διαφοροποιημένων Υπηρεσιών (DiffServ Code Point, DSCP) σε ένα καινούριο πεδίο της επικεφαλίδας IP, το πεδίο DS, για να δηλώσει ποια Συμπεριφορά Προώθησης Ανά-Κόμβο πρέπει να λάβει το πακέτο. Όλα τα πακέτα με το ίδιο DSCP ανήκουν σε μία συσσωρευμένη συμπεριφορά (behavior aggregate) και λαμβάνουν την ίδια μεταχείριση PHB, ανεξάρτητα από τη μικρο-ροή στην οποία ανήκουν.

Παρακάτω παρουσιάζουμε ορισμένα βασικά χαρακτηριστικά των διαφοροποιημένων υπηρεσιών:

- Έχουμε δέσμευση πόρων για συγκεκριμένες κλάσεις που αντιπροσωπεύουν aggregate κίνηση και όχι για κάθε ροή ξεχωριστά. Η απόδοση που θα έχει η κίνηση της κάθε ροής εξαρτάται από την προτεραιότητα της κλάσης στην οποία ανήκει και από το συνολική κίνηση που διαχειρίζεται η συγκεκριμένη κλάση εκείνη τη χρονική στιγμή και όχι από τη δέσμευση πόρων ανά ροή(κάτι το οποίο μπορούσε να οδηγήσει σε δεκάδες χιλιάδες δεσμεύσεις σε ένα μεγάλο δίκτυο).
- Η αστυνόμευση και το σημάδεμα ανά ροή γίνονται στους ακραίους δρομολογητές (στον πρώτο δρομολογητή εμπιστοσύνης, το δρομολογητή πρόσβασης, που συναντά η κίνηση από τον αποστολέα). Μετά από αυτόν το δρομολογητή, κάθε ροή Διαφοροποιημένων Υπηρεσιών αναμιγνύεται με άλλες ροές με παρόμοια χαρακτηριστικά και απαιτήσεις. Σαν αποτέλεσμα αυτής της διαδικασίας είναι η δημιουργία κλάσεων ροών. Όλες οι διαδικασίες προώθησης και αστυνόμευσης στους εσωτερικούς δρομολογητές γίνεται πλέον στο επίπεδο των κλάσεων. Ένα πρόσθετο πλεονέκτημα αυτής της προσέγγισης είναι ότι απλοποιεί και τις επιχειρησιακές σχέσεις μεταξύ διαφορετικών Παρόχων Υπηρεσιών Διαδικτύου(Internet Service provider, ISP), ώστε να μπορούν να συνεργαστούν με αποδοτικό τρόπο και να δημιουργήσουν υπηρεσίες από άκρη σε άκρη που διασχίζουν διαφορετικά δίκτυα.
- Ορισμός υπηρεσιών προώθησης και όχι απ' άκρο σε άκρο υπηρεσιών. Κάθε κλάση προώθησης αντιπροσωπεύει μία πολιτική μεταχείρισης και όχι μια υπηρεσία. Οι υπηρεσίες, ωστόσο μπορούν να δημιουργηθούν με το συνδυασμό

κλάσεων προώθησης (forwarding classes) και ελέγχου απόδοσης (admission control). Πακέτα διαφορετικών κλάσεων έχουν διαφορετικές προτεραιότητες και φυσικά αντιμετωπίζονται με διαφορετικό τρόπο. Κατά συνέπεια, οι δρομολογητές κάνουν διάκριση των πακέτων βάσει της κλάσης στην οποία ανήκουν και όχι βάσει της ροής. Επειδή δε, ο αριθμός των διαφοροποιημένων κλάσεων που μπορεί να υπάρχουν σε ένα δίκτυο μεταγωγής πακέτου είναι γενικά μικρός και ανεξάρτητος του αριθμού των χρηστών που εξυπηρετεί το δίκτυο (σε αντίθεση με τις ενεργές ροές), η αρχιτεκτονική των Διαφοροποιημένων Υπηρεσιών είναι επεκτάσιμη. Η κλάση ενός πακέτου (δηλαδή σε ποια διαφοροποιημένη υπηρεσία ανήκει) καθορίζεται από την τιμή του πεδίου DiffServ Code Point(DSCP) που βρίσκεται στην επικεφαλίδα του.

➤ Εγγύηση Ποιότητας Υπηρεσίας μέσω provisioning και όχι μέσω δέσμευσης πόρων. Η Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών παρέχει επιβεβαίωση χρήσης των πόρων του δικτύου μέσα από συνδυασμό provisioning και προτεραιοτήτων, με το να παρέχει πόρους στις κλάσεις προώθησης και να ελέγχει το ποσοστό της κίνησης αυτών των κλάσεων. Ουσιαστικά δημιουργεί διάφορα επίπεδα υπηρεσιών και επιβεβαίωσης χρήσης πόρων, χωρίς όμως να δίνει απόλυτες εγγυήσεις για χρήση εύρους ζώνης ή για καθυστερήσεις, ξεχωριστά σε κάθε ροή.

➤ Έμφαση σε σύνολο απλών Συμφωνιών Επιπέδου Υπηρεσίας (Service Level Agreements, SLAs) και όχι σε δυναμική σηματοδότηση. Όπως και στα συμβόλαια που αφορούν κάθε ροή ξεχωριστά έτσι και εδώ τα συμβόλαια χαρακτηρίζονται από ορισμένες ιδιότητες (profiles). Εφαρμόζοντας με αυστηρότητα τα συμβόλαια κίνησης των ομαδοποιημένων ροών και εξασφαλίζοντας ότι καινούριες συνδέσεις που θα επηρέαζαν αρνητικά την απόδοση του δικτύου δε θα γίνονται δεκτές, το μοντέλο Διαφοροποιημένων Υπηρεσιών εξασφαλίζει μια καλά ορισμένη υπηρεσία από άκρη σε άκρη για μια αλυσίδα διασυνδεδεμένων δικτύων. Τα συμβόλαια αυτά αφορούν κίνηση μεταξύ των ορίων ξένων δικτύων και αποτελούνται από ένα σύνολο απλών Συμφωνιών Επιπέδου Υπηρεσίας. Κάτι τέτοιο είναι πολύ κοντά και στη σημερινή πραγματικότητα και το γεγονός αυτό βοηθά στην ευκολότερη κατανόηση και αποδοχή του. Ένα SLA μπορεί να είναι στατικό ή δυναμικό. Για τα στατικά SLAs η διαπραγμάτευση μεταξύ του πελάτη και του ISP γίνεται ανά μεγάλα χρονικά διαστήματα, για παράδειγμα μηνιαίως ή ετησίως. Οι πελάτες με

δυναμικά SLAs πρέπει να χρησιμοποιούν κάποιο πρωτόκολλο σηματοδότησης (π.χ. RSVP), προκειμένου να ζητούν άλλες υπηρεσίες κατά βούληση.

➤ Εφαρμογή σε ένα αυτόνομο σύστημα και όχι σε ολόκληρο το δίκτυο. Η ανάπτυξη των διαφοροποιημένων υπηρεσιών στο Διαδίκτυο μπορεί να είναι διακριτή. Κλάσεις προώθησης μπορούν να οριστούν μόνο για ένα αυτόνομο σύστημα (domain), και μεταξύ διαφορετικών αυτόνομων συστημάτων οι πάροχοι υπηρεσιών θα πρέπει απλά να κάνουν συμφωνίες για το πώς ο καθένας από αυτούς θα διαχειρίζεται την κίνηση. Αυτό δεν μπορεί να συμβεί στην Αρχιτεκτονική Ενοποιημένων Υπηρεσιών, διότι αν η δέσμευση πόρων για μια ροή αποτύχει σε κάποιο συγκεκριμένο κομμάτι του δικτύου, τότε η ροή απορρίπτεται.

Προηγουμένως αναφέραμε ότι η κλάση ενός πακέτου καθορίζεται από την τιμή του πεδίου DSCP που βρίσκεται στην επικεφαλίδα του. Κατά συνέπεια, όταν ένας χρήστης κάνει χρήση μιας χρονικά ευαίσθητης υπηρεσίας, όπως είναι η μεταφορά φωνής, δεν έχει παρά να σημαδέψει τα πακέτα του με τέτοιο τρόπο ώστε αυτά να τύχουν και της ανάλογης αντιμετώπισης από το δίκτυο. Εναλλακτικά, η ταξινόμηση των πακέτων ενός χρήστη μπορεί να γίνεται στον πρώτο δρομολογητή με τον οποίο συνδέεται άμεσα ο συγκεκριμένος χρήστης. Σε αυτήν την περίπτωση χρειάζεται να προδιαγραφούν τα κριτήρια για την ταξινόμηση των πακέτων π.χ. όλα τα πακέτα με ένα συγκεκριμένο αριθμό θύρας (port number) που χρησιμοποιείται από μια εφαρμογή μεταφοράς φωνής, να ταξινομούνται στη κλάση μέγιστης προτεραιότητας. Αυτή η λύση είναι η προτιμότερη γιατί δεν χρειάζεται να γίνει καμία αλλαγή στη στοίβα πρωτοκόλλου των τερματικών. Ωστόσο, η Αρχιτεκτονική των Διαφοροποιημένων Υπηρεσιών δεν περιορίζεται αποκλειστικά στον τελικό χρήστη για την ταξινόμηση των πακέτων που στέλνει στο δίκτυο. Είναι φανερό ότι σε μια τέτοια περίπτωση κάθε χρήστης θα σημάδευε όλα τα πακέτα του ως πακέτα μέγιστης προτεραιότητας και κατά συνέπεια το τελικό αποτέλεσμα θα ήταν το ίδιο με την παρούσα κατάσταση. Για αυτό το λόγο η Αρχιτεκτονική των Διαφοροποιημένων Υπηρεσιών προσθέτει επιπλέον λειτουργίες στους δρομολογητές που βρίσκονται στα άκρα του δικτύου, όπου το φορτίο είναι σχετικά μικρό, οι οποίοι αποσκοπούν στον έλεγχο της κίνησης που εισάγει ένας χρήστης στο δίκτυο. Αν ένας συνδρομητής εισάγει περισσότερη κίνηση για μια συγκεκριμένη κλάση από αυτή που του αναλογεί, τότε η επιπλέον κίνηση είτε απορρίπτεται είτε υποβιβάζεται σε μια άλλη κλάση χαμηλότερης προτεραιότητας. Συνοψίζοντας, οι βασικές αρχές της Αρχιτεκτονικής των Διαφοροποιημένων Υπηρεσιών είναι:

- Περιορισμός της πολυπλοκότητας στον πυρήνα του δικτύου έτσι ώστε να είναι όσο το δυνατόν πιο επεκτάσιμο.
- Τοποθέτηση εργασιών (έλεγχος κίνησης, χρέωση κ.λ.π) που είναι απαραίτητες για τη σωστή λειτουργία του δικτύου.

Στη συνέχεια θα δοθεί η περιγραφή της λειτουργίας ενός δικτύου μεταγωγής πακέτου το οποίο υποστηρίζει την Αρχιτεκτονική των Διαφοροποιημένων Υπηρεσιών. Πέραν της κλάσης Βέλτιστης Προσπάθειας, το δίκτυο υποστηρίζει δύο επιπλέον Διαφοροποιημένες Υπηρεσίες: την Εξαιρετική (premium) και την Εγγυημένη (assured). Η Εξαιρετική κλάση (premium) υλοποιεί μια υπηρεσία που έχει συγκεκριμένο μέγιστο εύρος ζώνης (peak bandwidth), ασήμαντη αναμονή στις ουρές των δρομολογητών, δεν δανείζεται εύρος ζώνης από άλλες υπηρεσίες και μπορεί να υλοποιηθεί αρκετά εύκολα. Αυτή η κλάση είναι κατάλληλη για εμπορικές εφαρμογές που δεν έχουν μεγάλη εκρηκτικότητα αλλά είναι αρκετά ευαίσθητες στις χρονικές καθυστερήσεις (π.χ. φωνή, video). Από την άλλη μεριά, η Εγγυημένη υπηρεσία (assured) έχει χρονικές καθυστερήσεις παρόμοιες με αυτές που έχει η υπηρεσία βέλτιστης προσπάθειας όταν το δίκτυο είναι χωρίς υψηλό φορτίο. Ροές πακέτων που χρησιμοποιούν την εγγυημένη υπηρεσία μπορούν να δανείζονται εύρος ζώνης από άλλες κλάσεις χαμηλότερης προτεραιότητας (ή και από κλάσεις υψηλότερης προτεραιότητας όταν αυτές έχουν μικρή κίνηση) όταν αυτό είναι απαραίτητο. Για αυτό το λόγο η συγκεκριμένη υπηρεσία είναι κατάλληλη για εφαρμογές μη πραγματικού χρόνου με υψηλή εκρηκτικότητα (π.χ. World Wide Web). Η υιοθέτηση των δύο παραπάνω υπηρεσιών στο ίδιο δίκτυο έχει μερικά επιπλέον οφέλη. Καταρχήν, η Εξαιρετική Κλάση κάνει σπατάλη στη δέσμευση των πόρων του δικτύου (αφού η δέσμευση των πόρων του δικτύου γίνεται με μόνο μία παράμετρο που είναι το μέγιστο εύρος ζώνης). Ωστόσο, λόγω της ύπαρξης επιπλέον κλάσεων στο δίκτυο, το εύρος ζώνης που δεν χρησιμοποιείται από την εξαιρετική κλάση μπορεί να δανειστεί στην Κλάση Εγγυημένης Υπηρεσίας.

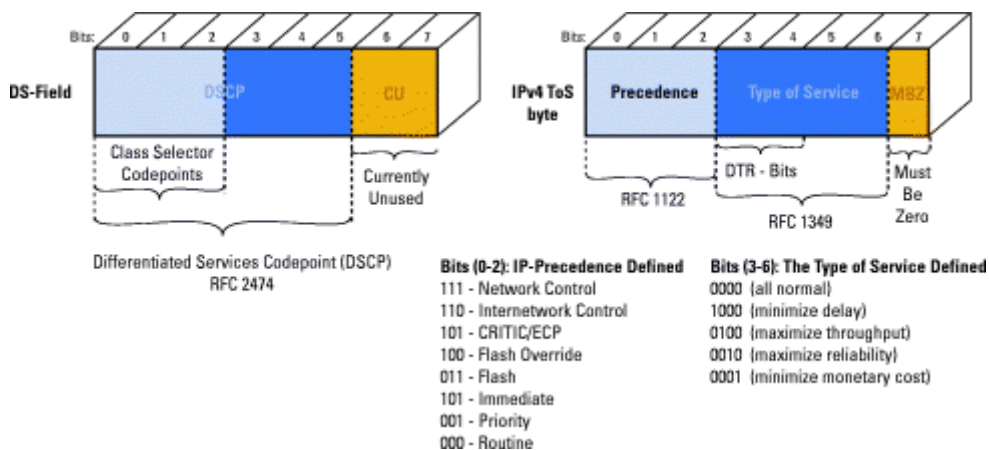
3.5.2. Δομή του πεδίου DS

Όπως αναφέραμε παραπάνω, DSCP είναι η κωδική τιμή που ανατίθεται στα πακέτα και υποδηλώνει την PHB που του αναλογεί. Η τιμή αυτή, ανατίθεται σε ένα συγκεκριμένο πεδίο του πακέτου το DS πεδίο. Το πεδίο αυτό καλύπτει ένα byte, και

αντιστοιχίζεται στο TOS byte του IPv4, ή στο Traffic Class Octet του IPv6. Η DSCP τιμή, ανατίθεται στα 6 πιο σημαντικά bits του DS πεδίου. Η αντιστοιχία μεταξύ των DSCP και των PHB αφορά το διαχειριστή του δικτύου. Κάθε DSCP τιμή πρέπει να αντιστοιχίζεται σε κάποια PHB, ενώ πρέπει να ορίζεται μια default DSCP τιμή για όλα τα πακέτα που διέρχονται στο δίκτυο Διαφοροποιημένων Υπηρεσιών. Τα πακέτα που εισέρχονται στο δίκτυο, και είναι μαρκαρισμένα με μια άγνωστη DSCP τιμή, πρέπει να προωθούνται με την καθορισμένη συμπεριφορά που ορίζει το δίκτυο. Οποιοσδήποτε ενδιαμέσος κόμβος, μπορεί να αλλάξει την τιμή που αναγράφεται στο DS πεδίο ενός πακέτου, εφόσον αυτό απαιτείται για την παροχή κάποιας υπηρεσίας. Πρόδρομος του DS πεδίου, θεωρείται το πεδίο IP Precedence (IP Prec). Το πεδίο αυτό αποτελείται από 3 bit, και χρησιμοποιείται για έλεγχο ροής στο δίκτυο, δρομολόγηση, και κάποια επίπεδα προνομίων (privileges).

Κάποια στιγμή, το IPv4 TOS octet, ορίστηκε ξανά, και επεκτάθηκε από τα 3 bits του IP Prec, στα 6 bits του DSCP. Προκειμένου να διατηρηθεί η συμβατότητα μεταξύ των δύο ορισμών, ορίστηκαν κάποιες ειδικές τιμές για το DSCP οι οποίες αναγνωρίζονται από συστήματα που υποστηρίζουν μόνο το σχήμα με το IP Prec. Αυτές οι τιμές έχουν τη μορφή 'xyz000', όπου x, y, z παίρνουν τιμές 0 ή 1. Οι τιμές αυτές ονομάζονται Class Selector Codepoints. Αν κάποιο πακέτο δεν μπορεί να αντιστοιχηθεί σε καμία PHB, τότε του αναθέτουμε ένα default PHB codepoint που είναι το <000000>.

Παρακάτω φαίνονται η δομή του πεδίου DS και η δομή του IPv4 TOS byte:



3.5.3. Μηχανισμοί προώθησης πακέτων, Λειτουργίες δρομολόγησης

Οι απαραίτητες λειτουργίες για την εφαρμογή των SLAs στα πακέτα των διαφόρων ροών κίνησης, υλοποιούνται στους δρομολογητές του DiffServ δικτύου από τις εξής οντότητες: τον Packet Classifier, τον Meter, τον Marker και τον Traffic Conditioner.

➤ Packet Classifier, είναι υπεύθυνος για την επεξεργασία ενός ή περισσότερων πεδίων του πακέτου προκειμένου να το μεταχειριστεί σύμφωνα με το SLA της ροής κίνησης στην οποία ανήκει. Ο packet classifier ξεχωρίζει μία εισερχόμενη ροή πακέτων σε πολλαπλά groups με βάση κάποιους προκαθορισμένους κανόνες. Υπάρχουν δυο τύποι Classifiers. Ο Bandwidth Aggregate (BA) Classifier διαχωρίζει την κίνηση στο επίπεδο ομαδοποιημένων ροών κίνησης με βάση το πεδίο DS των πακέτων της κυκλοφορίας. Ο Multi-Field (MF) Classifier διαχωρίζει την κίνηση, με βάση την τιμή ενός συνδυασμού πεδίων της επικεφαλίδας του πακέτου (διεύθυνση πηγής και προορισμού, πεδίο DS, θύρα πομπού, θύρα δέκτη) προκειμένου να βρει τη ροή στην οποία ανήκει κάθε πακέτο.

➤ Ο Marker σημαδεύει τα ασημάδευτα πακέτα (το πεδίο DS) ανάλογα με τη ροή κίνησης στην οποία ανήκουν ή τα σημαδεμένα πακέτα σύμφωνα με την τιμή του DSCP που έχουν ήδη (σε περίπτωση αντιστοίχισης μεταξύ DSCP από τον διαχειριστή του δικτύου ή όπως ορίζει η πολιτική που ακολουθείται τοπικά). Με αυτή τη λειτουργία τα πακέτα μαρκάρονται ως πακέτα εξαιρετικής (premium) ή εγγυημένης (assured) κλάσης ανάλογα με την κλάση της ροής που ανήκει το συγκεκριμένο πακέτο. Αυτό βέβαια γίνεται μόνο για πακέτα που έχουν περάσει επιτυχώς τη λειτουργία ελέγχου. Σε αντίθετη περίπτωση το πακέτο είτε απορρίπτεται είτε δε μαρκάρεται καθόλου, οπότε στη συνέχεια μεταχειρίζεται ως πακέτο της κλάσης βέλτιστης προσπάθειας.

➤ Ο Meter συλλέγει στοιχεία για την κυκλοφορία σε κάθε PHB και άλλα στατιστικά στοιχεία για την κίνηση. Ο μετρητής εξετάζει το προφίλ της κίνησης για κάθε κατηγορία πακέτων και το συγκρίνει με κάποια συμφωνηθέντα χαρακτηριστικά έτσι ώστε αν ακολουθείται από marker να γίνεται διάκριση των πακέτων σε δύο ή περισσότερα επίπεδα «νομιμότητας» ενώ όταν ακολουθείται από shaper ή dropper να εφαρμόζεται μορφοποίηση ή απόρριψη της «μη νόμιμης» κίνησης

➤ Ο Traffic Conditioner εφαρμόζει σε κάθε πακέτο μιας ροής κίνησης τη PHB που του αντιστοιχεί. Συχνά περιλαμβάνει τις λειτουργίες του meter και του marker, αλλά οι κυρίως λειτουργίες που επιτελεί είναι επιλογή της ουράς εξυπηρέτησης για τα εισερχόμενα πακέτα, καθώς και λειτουργίες μορφοποίησης και απόρριψης

πακέτων (shaper-dropper) ανά ροή κίνησης ή σε επίπεδο ομαδοποιημένων ροών προκειμένου να συμμορφώνεται η κίνηση με τους όρους του SLA που έχει επιλεχθεί και με τη συνολική χωρητικότητα ανά PHB.

3.5.4. Υπηρεσίες που παρέχονται από την Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών (DiffServ-Based Υπηρεσίες)

Η επιλογή και ο ορισμός παραμέτρων για τον προσδιορισμό της QoS που δίνει ένα δίκτυο μέσα από διάφορες υπηρεσίες, έχει αποτελέσει αντικείμενο της IETF, καθώς και άλλων προσπαθειών οι οποίες φαίνεται να συγκλίνουν σε ένα κοινά αποδεκτό σύνολο. Πρόκειται για τις παραμέτρους

- Καθυστέρηση.
- IP Packet Delay Variation (IPDV) ή jitter.
- Χωρητικότητα.
- Απώλεια πακέτων.

Οι προϋποθέσεις για τον ορισμό μιας QoS υπηρεσίας βάση των παραπάνω τεσσάρων παραμέτρων είναι :

- Σταθερή λειτουργία του φυσικού επιπέδου και του επιπέδου σύνδεσης δεδομένων.
- Bit error rate $\leq 10^{-12}$.
- Αξιοπιστία του εξοπλισμού.
- Επιλογή του MTU για την αποφυγή κατακερματισμού των πακέτων.
- Overprovisioning χαρακτήρας του δικτύου (όπως θα αναλυθεί και στη συνέχεια, η εξασφάλιση ντετερμινιστικών εγγυήσεων ποιότητας προϋποθέτει ότι ο ρυθμός άφιξης της κίνησης είναι μικρότερος από το ρυθμό εξυπηρέτησής της).

3.5.4.1. EF-based υπηρεσίες (expedited forwarding)

Σε αυτή την παράγραφο, παρουσιάζουμε την EF PHB, η οποία μπορεί να χρησιμοποιηθεί για συνθήκες χαμηλών απωλειών, χαμηλής καθυστέρησης και για παροχή εγγυημένων υπηρεσιών (assured bandwidth services). Η EF PHB είχε αρχικά προταθεί για να χαρακτηρίσει μια τεχνική προώθησης, όμοια με αυτήν της ουράς απλής προτεραιότητας (simple priority queueing). Όμως, σήμερα η EF PHB έχει οριστεί σαν μια τεχνική προώθησης για μια συνολική κλάση υπηρεσίας (aggregate

traffic), όπου ο ρυθμός αναχώρησης πακέτων της συγκεκριμένης κλάσης από κάθε κόμβο που βασίζεται στις διαφοροποιημένες υπηρεσίες (DS node) πρέπει να είναι ίσος ή να ξεπερνά ένα προκαθορισμένο ρυθμό. Η EF κίνηση πρέπει να ξεπερνάει αυτόν τον ρυθμό ανεξάρτητα από την υπόλοιπη κίνηση του δικτύου. Στην EF PHB έχει ανατεθεί το codeword <101110>.

Οι EF-based υπηρεσίες βρίσκουν εφαρμογή σε εφαρμογές πραγματικού χρόνου ευαίσθητες στο jitter ή/και τις απώλειες πακέτων (έχουν ήδη αναφερθεί ως «μη ανεκτικές») που απαιτούν εγγυήσεις χωρητικότητας.

Ο ορισμός τους βασίζεται:

- στον καθορισμό της διεπαφής μεταξύ DiffServ domains έτσι ώστε να εμφανίζει και αυτό συμπεριφορά EF PHB
- στον περιορισμό της χωρητικότητας που αφιερώνεται στην υπηρεσία για να αποφευχθεί αποκλεισμός της best-effort κίνησης
- σε μια αρχικά στατική ρύθμιση των δικτυακών συσκευών για την παροχή της (αποφυγή χρήσης πρωτοκόλλου σηματοδότησης)
- στην εξασφάλιση και συνεχή μέτρηση των QoS παραμέτρων που επιτυγχάνονται κατά τη λειτουργία της
- στην ελαχιστοποίηση των χρησιμοποιούμενων μηχανισμών ανά κόμβο

Διάφοροι τύποι μηχανισμών χρονοδρομολόγησης ουρών μπορούν να χρησιμοποιηθούν για να υλοποιήσουν την EF PHB. Μία απλή προσέγγιση είναι η υλοποίηση σχήματος δρομολόγησης προτεραιότητας (priority-queueing scheme) με τον αλγόριθμο του διαρρέοντος δοχείου (token bucket algorithm). Η ουρά για την κίνηση EF πρέπει να έχει την υψηλότερη προτεραιότητα στο σύστημα, έτσι ώστε να διατηρηθούν οι ιδιότητες της EF μεταχείρισης. Ο token bucket είναι εκεί για να περιορίσει το συνολικό ποσοστό της EF κίνησης, έτσι ώστε η υπόλοιπη κίνηση να μην είναι καταπιεσμένη από τις εκρήξεις της EF κίνησης.

Ένας άλλος τρόπος για να υλοποιήσουμε την EF PHB είναι να χρησιμοποιήσουμε τον αλγόριθμο δίκαιης αναμονής με βάρη (Weighted Fair Queuing – WFQ) και να διαμορφώσουμε τα βάρη με τέτοιο τρόπο ώστε η EF κίνηση να έχει σχετική προτεραιότητα. Σε μια τυπική εφαρμογή των WFQ αλγορίθμων, το βάρος είναι ανάλογο με το εύρος ζώνης που αποδίδεται (rate-proportional allocation). Για παράδειγμα, αν στις ροές A και B έχουν χορηγηθεί 1Mbits/sec και 2Mbits/sec αντίστοιχα, τότε τα βάρη για τις ροές A και B σε ένα σύστημα WFQ πρέπει να έχουν μία αναλογία της τάξης του 1/2. Για μία γραμμή (link) με χωρητικότητα 3Mbits/sec ή

περισσότερο, οι ροές A και B θα λάβουν κατ' ελάχιστο εύρος ζώνης της τάξης του 1Mbits/sec και 2Mbits/sec αντίστοιχα. Ωστόσο ο WFQ αλγόριθμος δεν απαιτεί υποχρεωτικά αναλογική απόδοση του διαθέσιμου εύρους ζώνης. Στη πραγματικότητα η μη αναλογική απόδοση, αν και λιγότερο γνωστή, μπορεί να χρησιμοποιηθεί για να παρέχει ελεγχόμενη προτεραιότητα (controlled allocation at fine granularity). Ας υποθέσουμε ότι αναθέτουμε και στις δύο ροές βάρος ίσο με ένα, δηλαδή μια αναλογία 1/1. Δεδομένου ότι οι υπόλοιπες συνθήκες παραμένουν οι ίδιες, χορηγείται από 1,5Mbit/sec σε κάθε μία ροή. Αν οι ροές A και B συνεχίσουν να στέλνουν με ρυθμό 1Mbit/sec και 2 Mbit/sec πάνω από τη γραμμή των 3 Mbit/sec, τότε θα λάβουν εύρος ζώνης 1 Mbit/sec και 2 Mbit/sec αντίστοιχα. Η μόνη διαφορά θα είναι ότι η ροή A θα υπόκειται σε μικρότερη καθυστέρηση από την ροή B. Με άλλα λόγια, η καθυστέρηση ουράς αλλάζει (queuing delay) ενώ η χορήγηση εύρους ζώνης παραμένει η ίδια. Ο λόγος για το παραπάνω είναι ότι ο αλγόριθμος δίκαιης κατανομής με βάρη είναι συντηρητικός. Δηλαδή, το περισσευούμενο εύρος ζώνης από τη ροή A δεν σπαταλιέται, αλλά παραχωρείται στη ροή B. Συνεπώς, όσο το συνολικό ποσοστό κίνησης είναι μέσα στα όρια της γραμμής, τότε η χορήγηση εύρους ζώνης παραμένει η ίδια.

Πάντως είναι δυνατό να υλοποιήσουμε μηχανισμούς ουρών απλής προτεραιότητας με μη αναλογική χορήγηση bandwidth στους αλγόριθμους WFQ. Μπορούμε πολύ απλά να αναθέσουμε ένα μεγάλο βάρος στις ουρές που μεταφέρει κίνηση υψηλής προτεραιότητας. Όπως και στη υλοποίηση της EF με απλή προτεραιότητα, η ουρά η οποία έχει το μεγαλύτερο βάρος θα πρέπει να είναι περιορισμένη έτσι ώστε να μην καταπιέζει την υπόλοιπη κίνηση.

3.5.4.2. AF-based υπηρεσίες (assured forwarding)

Πρόκειται για υπηρεσίες που βασίζονται στην Assured Forwarding PHB. Έχουν ως στόχο να εξασφαλίσουν την εξυπηρέτηση των πακέτων μιας ροής η οποία συμμορφώνεται σε ένα συμφωνηθέντα ρυθμό με πολύ μεγάλη πιθανότητα, ενώ υποστηρίζουν την κίνηση που ξεφεύγει από το συμφωνηθέν προφίλ με μικρότερη πιθανότητα εξυπηρέτησης των πακέτων. Παραμένει αντικείμενο διερεύνησης και πειραματισμών το κατά πόσο είναι εφικτό να δοθούν πραγματικές εγγυήσεις ελάχιστου ρυθμού μετάδοσης σε επιμέρους ροές ανεξάρτητα από το βαθμό

aggregation τους στον κορμό ενός DiffServ domain, την συμπεριφορά τους κλπ. Οι βασικοί κανόνες του AF PHB σύμφωνα με τους οποίους πρέπει να «χτίζονται» οι AF-based υπηρεσίες είναι:

- Δεν πρέπει να γίνεται συνένωση των ροών δύο διαφορετικών AF κλάσεων.
- Σε κάθε AF κλάση πρέπει να παραχωρείται συγκεκριμένη ποσότητα πόρων (η οποία πρέπει να μπορεί να ρυθμιστεί) και η κλάση πρέπει να επιτυγχάνει τον προκαθορισμένο ρυθμό της τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα.
- Η πιθανότητα εξυπηρέτησης ενός πακέτου πρέπει να είναι αντιστρόφως ανάλογη της drop precedence τιμής του (δηλ. της προτεραιότητας εξυπηρέτησής του).
- Κάθε κόμβος πρέπει να δέχεται πακέτα και των τριών επιπέδων precedence ενώ πρέπει να τα εξυπηρετεί με τουλάχιστον δύο διαφορετικά επίπεδα προτεραιότητας.
- Κάθε κόμβος θα πρέπει να μην αλλάζει την σειρά των πακέτων που ανήκουν στην ίδια ροή και στην ίδια AF κλάση.

Ουσιαστικά δηλαδή, οι AF υπηρεσίες ορίζουν τέσσερις Κλάσεις Προώθησης (forwarding classes) και σε καθεμία κλάση τρεις drop precedences. Σε κάθε μία Κλάση Ισοδύναμης Προώθησης χορηγείται ένας ελάχιστος αριθμός buffers και εύρους ζώνης. Οι πελάτες μπορούν να εγγραφούν στις υπηρεσίες AF και τότε τα πακέτα τους θα σηματοδοτούν με τα αντίστοιχα AF DSCPs.

Οι τρεις προτεραιότητες απόρριψης σε κάθε forwarding class χρησιμοποιούνται για την επιλογή των πακέτων τα οποία θα απορριφθούν κατά τη διάρκεια συμφόρησης. Όταν AF πακέτα μιας συγκεκριμένης κλάσης προώθησης ξεπερνούν ένα συγκεκριμένο κατώφλι, τότε αρχικά απορρίπτονται τα πακέτα με τη μεγαλύτερη προτεραιότητα απόρριψης και στη συνέχεια αυτά με τη χαμηλότερη προτεραιότητα. Οι προτεραιότητες αυτές είναι μοναδικές για κάθε κλάση προώθησης AF. Για παράδειγμα, όταν ένας DS κόμβος αρχίζει να απορρίπτει πακέτα με τη μεγαλύτερη προτεραιότητα σε μία κλάση, τα πακέτα σε άλλες κλάσεις πιθανόν να μην υπόκεινται σε καμία απολύτως απόρριψη. Οι απορρίψεις συμβαίνουν μόνο σε εκείνες τις κλάσεις στις οποίες η κίνηση ξεπερνά τους δεσμευμένους πόρους τους. Ένας DS κόμβος πρέπει να υλοποιεί και τις τέσσερις AF κλάσεις.

Για κάθε AF κλάση το ελάχιστο ποσό των πόρων προώθησης (buffers και bandwidth) που της έχουν χορηγηθεί πρέπει να είναι διαμορφώσιμο. Παρόλο που το AF standard δεν ορίζει πως το διαθέσιμο εύρος ζώνης που περισσεύει από αυτό που χορηγείται για

τις ελάχιστες απαιτήσεις θα μοιραστεί, η κάθε υλοποίηση θα πρέπει να ορίζει έναν συγκεκριμένο αλγόριθμο για απόδοση εύρους ζώνης. Μέσα σε μία AF κλάση, η Διαφοροποιημένη Υπηρεσία πρέπει να προωθεί τα πακέτα σε συμφωνία με τις προτεραιότητες απόρριψής τους. Ένας DS κόμβος μπορεί να αναδιατάσσει πακέτα από διαφορετικές AF κλάσεις, αλλά όχι πακέτα με διαφορετικές προτεραιότητες απόρριψης στην ίδια κλάση. Τα συνιστώμενα coderpoints για τις AF υπηρεσίες φαίνονται στο παρακάτω σχήμα:

Τα πρώτα 3 bits του DS πεδίου κωδικοποιούν την εκάστοτε κλάση και τα επόμενα δύο τις προτεραιότητες απόρριψης. Οι AF κλάσεις πολλές φορές παρουσιάζονται στη μορφή AFxy, όπου το x παριστάνει την κλάση προώθησης και το y την προτεραιότητα απόρριψης μέσα στην κλάση προώθησης.

Ένα πρόβλημα των AF-based υπηρεσιών, που αποτελεί και γενικότερο πρόβλημα των DiffServ υπηρεσιών είναι ότι είναι «sender-oriented» και κατ' επέκταση δεν δίνουν τη δυνατότητα να ορίσει ο παραλήπτης την ποιότητα της κίνησης που λαμβάνει. Στην ειδική περίπτωση που ο παραλήπτης θέλει να λαμβάνει κίνηση με ένα συγκεκριμένο ρυθμό αυτό δεν είναι πάντα εφικτό γιατί το aggregate που φτάνει στο χρήστη ενδέχεται να προέρχεται από διαφορετικά σημεία εισόδου στο DiffServ domain και είναι δύσκολο να συγκριθεί/μετρηθεί με ένα ενιαίο συμβόλαιο. Στα πλαίσια των AF-based υπηρεσιών δεν παρέχονται αυστηρές εγγυήσεις καθυστέρησης/jitter γιατί για να γίνει αυτό θα πρέπει να αναιρεθεί η δυνατότητα που δίνεται στα aggregates να καταλαμβάνουν πόρους πέραν των συμφωνηθέντων όταν αυτοί είναι διαθέσιμοι. Ωστόσο το τελευταίο δεν αποτελεί πρόβλημα γιατί στο σημείο αυτό υπάρχει συμπληρωματικότητα των AF-based υπηρεσιών με τις EF-based υπηρεσίες.

3.5.5. Δυνατότητα Κλιμάκωσης

Η Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών από την αρχή έχει σχεδιαστεί έτσι ώστε να μπορεί εύκολα να κλιμακωθεί και έχει δύο επίπεδα.

Αποδοχή μεγάλου αριθμού συνδέσεων: Οι δρομολογητές πυρήνα που βρίσκονται στο εσωτερικό ενός δικτύου (core routers) πρέπει να ασχολούνται και να προωθούν χιλιάδες συνδέσεις, μην έχοντας έτσι τη δυνατότητα, για πρακτικούς λόγους, να ασχολούνται και με άλλες διαδικασίες. Στις διαφοροποιημένες υπηρεσίες έχει γίνει προσπάθεια να απομακρυνθεί η όποια πολυπλοκότητα από αυτούς τους

δρομολογητές και να μεταφερθεί στους δρομολογητές απόληξης (edge routers), όπου οι απαιτήσεις σε ταχύτητα προώθησης είναι μικρότερες, όπως επίσης και ο αριθμός των ροών που πρέπει να εξυπηρετηθούν. Οι δρομολογητές αυτοί μπορούν να διαθέσουν την απαραίτητη υπολογιστική ισχύ για να ικανοποιήσουν τις διαδικασίες διαφοροποιημένων υπηρεσιών.

Υψηλές ταχύτητες: Όσο θα υπάρχει η ανάγκη να κρατηθούν οι συμπεριφορές προώθησης ανά κόμβο απλές, έτσι ώστε οι ομαδοποιημένες ροές να εξυπηρετούνται με μεγάλες ταχύτητες, τόσο μεγαλύτερη θα είναι η ανάγκη και για πιο γρήγορη εξυπηρέτηση των ξεχωριστών ροών. Αυτό συνήθως ισχύει στην πράξη, όπου η αύξηση του διαθέσιμου εύρους ζώνης δημιουργεί την ψευδαίσθηση ότι είναι και απεριόριστο. Έτσι δημιουργείται ένα είδος θετικής ανάδρασης που εμπνέει νέα είδη εφαρμογών με ακόμη σκληρότερες τηλεπικοινωνιακές απαιτήσεις. Όταν τέτοιες εφαρμογές γίνουν πραγματικότητα αργά ή γρήγορα θα φέρουν και πάλι τη συμφόρηση στο δίκτυο, οπότε θα γίνει ακόμη πιο επιτακτική η ανάγκη για μηχανισμούς Ποιότητας Υπηρεσίας ικανούς να αποδίδουν με μεγάλες ταχύτητες, ακόμη και τέτοιες απαιτήσεις σε ποιότητα υπηρεσίας. Η προσπάθεια που γίνεται να πάει η πολυπλοκότητα όσο πιο κοντά γίνεται στο χρήστη και έξω από το δίκτυο, δίνει την καλύτερη προοπτική για να επιτευχθούν υψηλές ταχύτητες προώθησης πολλών ροών.

Εύκολη διαχείριση: Το μοντέλο της Αρχιτεκτονικής Διαφοροποιημένων Υπηρεσιών επιτρέπει στους παροχείς του δικτύου να ορίσουν οι ίδιοι τον τρόπο με τον οποίο θα διαχειρίζονται τα δίκτυά τους. Αυτό με την προϋπόθεση ότι η διαχείριση θα είναι τέτοια που θα φροντίζει για την τήρηση συμβολαίων κίνησης με άλλα συνεργαζόμενα δίκτυα. Οι εσωτερικές πολιτικές και διαδικασίες παίζουν καθοριστικό ρόλο και στον τρόπο διαχείρισης του δικτύου, γι' αυτό υπάρχει η απαίτηση από κάθε δίκτυο να μπορεί να έχει το δικό του ξεχωριστό τρόπο ιδιαίτερα όταν περιλαμβάνει και τελικούς χρήστες. Η παροχή Ποιότητας Υπηρεσίας από τα δίκτυα, αναπόφευκτα θα δημιουργήσει και την ανάγκη για έλεγχο της πρόσβασης σε αυτά, σύμφωνα πάντα με την ισχύουσα πολιτική των διαχειριστών τους.

Παρακολούθηση χρήσης πόρων: Οι Διαφοροποιημένες Υπηρεσίες επιτρέπουν συμφωνηθέντα προφίλ υπηρεσιών Ποιότητας Υπηρεσίας να μπορούν να συγκριθούν με καλά ορισμένα μέτρα απόδοσης δικτύων (IP performance metrics). Ακόμη και απλοί χρήστες εφοδιασμένοι με τα κατάλληλα εργαλεία παρακολούθησης θα μπορούν να ελέγχουν κατά πόσο αυτό που τους προσφέρει το δίκτυο είναι το

συμφωνηθέν, για το οποίο προφανώς πληρώνουν. Με τον ίδιο τρόπο θα μπορούσε να γίνει έλεγχος και στα σύνορα των δικτύων. Τέτοια εργαλεία παρακολούθησης μπορούν να φανούν χρήσιμα ακόμη και στο σχεδιασμό, στη σωστή διαστασιολόγηση και αντιμετώπιση διάφορων τεχνικών δυσκολιών και προβλημάτων ενός δικτύου. Μια καλή συνέπεια του σχεδιασμού των διαφοροποιημένων υπηρεσιών είναι ότι πολλά δεδομένα για μετρήσεις μπορούν να εξαχθούν από τους ταξινομητές πακέτων και τους μηχανισμούς αστυνόμευσης.

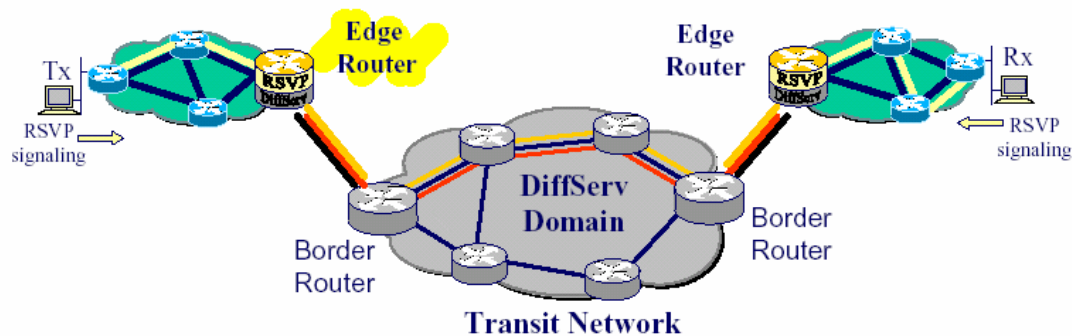
Πολλαπλές υλοποιήσεις: Η διαλειτουργικότητα των στοιχείων του δικτύου βασισμένη στην τυποποίηση βασικών λειτουργιών ήταν από τις πρωταρχικές σχεδιαστικές αρχές των διαφοροποιημένων υπηρεσιών. Η IETF προς το παρόν έχει εντοπίσει τη δουλειά της στην παραγωγή προτύπων για τις συμπεριφορές προώθησης ανά κόμβο και πως αυτές θα κωδικοποιούνται στις επικεφαλίδες των πακέτων IP. Αυτό προσφέρει τη δυνατότητα διαλειτουργικότητας στο κατώτερο επίπεδο. Συνεργασία μεταξύ ξένων δικτύων θα επιτευχθεί με την τυποποίηση καθολικών Συμπεριφορών Προώθησης Ανά Κόμβο και δημιουργία απλών διμερών SLAs, που η συνένωσή τους θα οδηγήσει στη δημιουργία Ενοποιημένων Υπηρεσιών.

3.6. Ενοποιημένες Υπηρεσίες πάνω από δίκτυα Διαφοροποιημένων Υπηρεσιών

Στην αρχιτεκτονική αυτή, παρέχεται Ποιότητα Υπηρεσίας απ' άκρο σ' άκρο, με την εφαρμογή του μοντέλου Ενοποιημένων Υπηρεσιών κατά μήκος ενός δικτύου που περιλαμβάνει ένα ή περισσότερα δίκτυα Διαφοροποιημένων Υπηρεσιών. Χρησιμοποιείται δηλαδή η Αρχιτεκτονική Ενοποιημένων Υπηρεσιών στα περιβάλλοντα διαχειριζόμενων δικτύων του αποστολέα και του παραλήπτη κίνησης, και η Αρχιτεκτονική Διαφοροποιημένων Υπηρεσιών στα ενδιάμεσα διαχειριζόμενα περιβάλλοντα. Σύμφωνα με την αρχιτεκτονική αυτή, για τη δέσμευση των πόρων στα περιβάλλοντα διαχειριζόμενων δικτύων του αποστολέα και του παραλήπτη κίνησης, χρησιμοποιείται η σηματοδότηση του πρωτοκόλλου RSVP. Τα DiffServ τμήματα, μπορεί (χωρίς να είναι απαραίτητο) να συμμετέχουν στη σηματοδότηση του RSVP, για λόγους βελτιστοποίησης της δέσμευσης πόρων, και προκειμένου να συμμετέχουν στον έλεγχο αποδοχής των αιτήσεων.

Από τη σκοπιά του δικτύου Ενοποιημένων Υπηρεσιών, τα τμήματα Διαφοροποιημένων Υπηρεσιών αντιμετωπίζονται σαν εικονικοί σύνδεσμοι που συνδέουν τους κόμβους Ενοποιημένων Υπηρεσιών και δρομολογητές. Στις DiffServ περιοχές του δικτύου, οι δρομολογητές εφαρμόζουν συγκεκριμένες PHBs (Per Hop Behaviors). Η συνολική ποσότητα κίνησης που γίνεται αποδεκτή στο DiffServ δίκτυο και που λαμβάνει μια συγκεκριμένη PHB, μπορεί να περιοριστεί με την εφαρμογή πολιτικών στις άκρες του δικτύου. Σαν αποτέλεσμα όλων αυτών, οι DiffServ περιοχές μπορούν να υποστηρίξουν τις υπηρεσίες τύπου IntServ που ζητούνται. Στο επόμενο σχήμα παρουσιάζεται η αρχιτεκτονική ενός τέτοιου δικτύου:

Interoperation IntServ/DiffServ



Παρακάτω αναφέρονται τα βασικά στοιχεία που υλοποιούν την αρχιτεκτονική αυτή, και η λειτουργικότητα του καθενός:

- Οι ακραίοι κόμβοι (hosts) οι οποίοι δημιουργούν τη σηματοδότηση του RSVP ζητώντας Ποιότητα Υπηρεσίας εκ' μέρους των εφαρμογών. Οι κόμβοι αυτοί μπορεί να διαθέτουν την ικανότητα και για άλλες λειτουργίες, όπως το μαρκάρισμα του DSCP πεδίου των πακέτων, και την μορφοποίηση της κίνησης στις παραμέτρους που θέτει το συμβόλαιο κίνησης. Συνήθως πάντως, οι λειτουργίες αυτές εκτελούνται στον πρώτο IntServ δρομολογητή από τη μεριά του αποστολέα της κίνησης.
- Οι ακραίοι δρομολογητές των IntServ δικτύων, που επικοινωνούν απ' ευθείας με κάποιο DiffServ δίκτυο. Η λειτουργικότητά τους εξαρτάται από τη γενικότερη υλοποίηση του δικτύου. Αν το DiffServ τμήμα του δικτύου με το οποίο επικοινωνούν, δεν υποστηρίζει RSVP, τότε οι δρομολογητές αυτοί εκτελούν έλεγχο αποδοχής (admission control) για το DiffServ δίκτυο. Επεξεργάζονται τα μηνύματα σηματοδότησης του RSVP, και παίρνουν τις αποφάσεις αποδοχής

στηριζόμενοι σε στοιχεία για την διαθεσιμότητα των πόρων του DiffServ δικτύου, και σε καθορισμένες πολιτικές. Αν αντίθετα το DiffServ τμήμα υποστηρίζει RSVP, τότε ο κόμβος λαμβάνει μόνο τοπικές αποφάσεις αποδοχής των αιτήσεων, στηριζόμενος σε στοιχεία για τη διαθεσιμότητα των πόρων του δρομολογητή, και με βάση πάντα τις καθορισμένες πολιτικές.

➤ Οι ακραίοι δρομολογητές των DiffServ δικτύων, που επικοινωνούν απ' ευθείας με κάποιο IntServ δίκτυο. Όπως και προηγουμένως, η λειτουργικότητά τους εξαρτάται από τη γενικότερη υλοποίηση του δικτύου. Έτσι, αν το DiffServ δίκτυο στο οποίο ανήκουν δεν υποστηρίζει RSVP, τότε οι δρομολογητές αυτοί λειτουργούν σαν συνηθισμένοι DiffServ δρομολογητές. Σαν τέτοιοι η κύρια λειτουργία τους είναι να εξυπηρετούν τα πακέτα που λαμβάνουν, με βάση το επίπεδο υπηρεσίας που προσδιορίζεται από το DSCP πεδίο τους. Από την άλλη, αν το DiffServ δίκτυο υποστηρίζει RSVP, οι δρομολογητές αυτοί συμμετέχουν στη σηματοδότηση του RSVP, και λαμβάνουν τις αποφάσεις αποδοχής των αιτήσεων, εκ μέρους του DiffServ δικτύου.

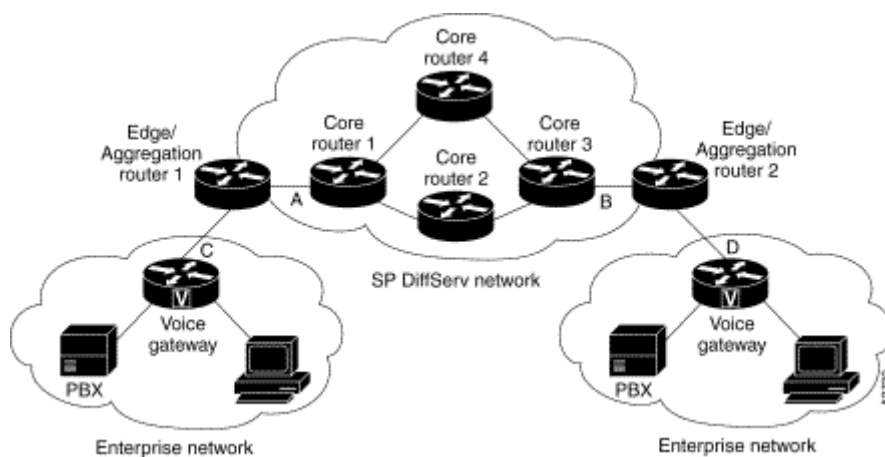
Οι αιτήσεις για IntServ υπηρεσία πρέπει να αντιστοιχίζονται με τις δυνατότητες εξυπηρέτησης της DiffServ περιοχής του δικτύου. Η αντιστοίχιση αυτή περιλαμβάνει την επιλογή της κατάλληλης PHB που εξυπηρετεί την αίτηση, την εφαρμογή κατάλληλης πολιτικής στα άκρα του DiffServ δικτύου (μορφοποίηση, αλλαγή του DSCP πεδίου), και έλεγχο αποδοχής κλήσης που λαμβάνει υπ' όψιν την διαθεσιμότητα των πόρων στο DiffServ δίκτυο.

Η αντιστοίχιση των IntServ αιτήσεων σε κάποια συγκεκριμένη PHB, μπορεί να γίνεται στατικά, με τον εκ των προτέρων καθορισμό των PHB που αντιστοιχεί σε κάθε IntServ υπηρεσία, είτε δυναμικά. Η δυναμική αντιστοίχιση γίνεται από τον διαχειριστή του DiffServ δικτύου, ο οποίος για λόγους πολιτικής μπορεί να παρακάμψει τις προκαθορισμένες αντιστοιχίσεις και να επιλέξει κάποια διαφορετική. Σε περίπτωση που το μαρκάρισμα των πακέτων (DSCP πεδίο) γίνεται έξω από το DiffServ δίκτυο, τότε ο κόμβος που εκτελεί το μαρκάρισμα πρέπει να ενημερωθεί για την νέα τιμή DSCP. Αυτό γίνεται συνήθως με RSVP.

Ο έλεγχος αποδοχής κλήσης γίνεται συνήθως με τη βοήθεια αντιπροσώπων του δικτύου (γνωστοί ως "oracle"), οι οποίοι έχουν ικανή γνώση της διαθεσιμότητας των πόρων και της τοπολογίας του δικτύου για να κάνουν τον έλεγχο. Μια άλλη προσέγγιση (για κόμβους DiffServ που υποστηρίζουν RSVP) είναι να ενημερώνονται

οι IntServ κόμβοι για τις αλλαγές στη διαθεσιμότητα των πόρων του DiffServ δικτύου με την αποστολή RSVP μηνυμάτων.

Στο παράδειγμα που φαίνεται παρακάτω, η κίνηση μεταξύ των δύο enterprise δικτύων, περνάει από ένα DiffServ δίκτυο κάποιου SP. Κάθε enterprise δίκτυο έχει ένα voice gateway, ο οποίος συνδέεται με ένα ακραίο δρομολογητή (Edge/Aggregation router) του DiffServ δικτύου.



Η κίνηση μεταξύ των δύο enterprise δικτύων, περνάει από ένα DiffServ δίκτυο κάποιου SP

Οι Voice gateways υποστηρίζουν RSVP, και κρατάνε πληροφορίες για κάθε ροή ξεχωριστά. Οι λειτουργίες της κατάταξης, του μαρκαρίσματος και του χρονοπρογραμματισμού των πακέτων, γίνονται επίσης ανά ροή πληροφορίας (per-flow). Οι ακραίοι (Edge) κόμβοι υποστηρίζουν RSVP στις διεπαφές C και D οι οποίες τους συνδέουν με τους gateways. Οι κόμβοι αυτοί χρησιμοποιούν το RSVP για την πραγματοποίηση ελέγχου αποδοχής κλήσης στις διεπαφές που τους συνδέουν με τους Core routers 1 και 3. Οι Core routers με τη σειρά τους δεν υποστηρίζουν RSVP, αλλά προωθούν τα RSVP μηνύματα σαν απλά πακέτα. Οι δρομολογητές αυτοί, υλοποιούν μια συγκεκριμένη PHB, για όλες τις ομαδοποιημένες ροές κίνησης που φέρουν την ίδια DSCP τιμή.

Οι Voice gateways, αναγνωρίζουν τα πακέτα που λαμβάνουν, και θέτουν την κατάλληλη DSCP τιμή σε καθένα. Εφόσον η αίτηση μιας ροής για ποιότητα υπηρεσίας περάσει με επιτυχία από τον έλεγχο αποδοχής κλήσης, τα πακέτα της ανατίθενται στην αντίστοιχη κλάση υπηρεσίας, στους ακραίους κόμβους του DiffServ δικτύου.

3.7. Σύγκριση των IntServ και DiffServ αρχιτεκτονικών

Οι αρχιτεκτονικές IntServ και Diffserv παρουσιάζουν η καθεμία ορισμένα πλεονεκτήματα και μειονεκτήματα, τα οποία παρουσιάζουμε παρακάτω:

- Στην αρχιτεκτονική IntServ είναι γνωστή η κατάσταση των ροών κίνησης (state-based) κάθε στιγμή, με αποτέλεσμα να υπάρχει μεγαλύτερη ακρίβεια και λεπτομέρεια όσον αφορά στην ανταπόκριση προς τις αιτήσεις για ποιότητα υπηρεσίας. Αντίθετα η αρχιτεκτονική DiffServ δεν απαιτεί γνώση της κατάστασης (state-less) των ροών κίνησης, με αποτέλεσμα να είναι απαραίτητη η σηματοδότηση μεταξύ της εφαρμογής και του δικτύου, για παροχή ποιότητας υπηρεσίας.

Στην πρώτη περίπτωση οι απαιτήσεις πόρων (υπολογιστική ισχύς και κατανάλωση μνήμης) για την διαχείριση της κατάστασης κάθε σύνδεσης στους δρομολογητές αυξάνει σε απόλυτη αναλογία με τον αριθμό των ροών που χρειάζεται να εξυπηρετηθούν, επηρεάζοντας δυσμενώς την επίδοση των δρομολογητών. Στη δεύτερη περίπτωση, όταν το δίκτυο δεν μπορεί να παρέχει την ποιότητα υπηρεσίας που του ζητήθηκε δεν ενημερώνει την εφαρμογή, οπότε μένει στις δυνατότητές της να αναγνωρίσει ότι δεν παρέχεται η ποιότητα υπηρεσίας που επιθυμεί (αυτό δίνει στην αρχιτεκτονική DiffServ μεγάλη επεκτασιμότητα). Δημιουργείται ένας βαθμός συμβιβασμού των απαιτήσεων για ποιότητα υπηρεσίας, αφού η απόκριση στις αιτήσεις ποιότητας υπηρεσίας δεν θα είναι ακριβώς αυτή που ζητούν οι εφαρμογές, εφόσον η ποιότητα υπηρεσίας προσφέρεται σε συνολική κίνηση και όχι σε κίνηση ανά ροή (per flow).

Ένα άλλο γνώρισμα στην παροχή ποιότητας υπηρεσίας στο Διαδίκτυο, είναι αν οι αιτήσεις πραγματοποιούνται σε επίπεδο εφαρμογής (application layer) ή αποτελούν μια επιλογή του επιπέδου μεταφοράς (transport layer). Η σημαντική διαφορά μεταξύ των δύο αυτών προσεγγίσεων είναι το γεγονός, ότι στη πρώτη η εφαρμογή πρέπει να γνωρίζει πως να διαχειριστεί την διεπιφάνεια πρωτοκόλλου εφαρμογής (Application Protocol Interface – API) που παρέχεται κάθε φορά ώστε να έχει τη δυνατότητα να αιτείται ποιότητα υπηρεσίας από το δίκτυο. Στη δεύτερη προσέγγιση η εφαρμογή δεν χρειάζεται να γνωρίζει με ποιο τρόπο παρέχεται ποιότητα υπηρεσίας από το δίκτυο σε αυτή αφού αυτό καθορίζεται στο επίπεδο μεταφοράς (transport layer). Το

μειονέκτημα αυτής της προσέγγισης είναι ότι η εφαρμογή δεν μπορεί να ανταλλάξει χρήσιμες πληροφορίες με το δίκτυο, οι οποίες μπορεί να είναι απαραίτητες και για τους δύο.

- Στην περίπτωση των IntServ ακολουθείται η πρώτη προσέγγιση, αφού η εφαρμογή πρέπει να καθίσταται ικανή να παρέχει στο τμήμα της αρχιτεκτονικής που είναι υπεύθυνο για την δέσμευση πόρων, ένα προφίλ με τις απαιτήσεις κίνησης. Από την άλλη μεριά στην περίπτωση των DiffServ δεν προβλέπεται επικοινωνία μεταξύ της εφαρμογής και του δικτύου, οπότε και προτιμάται η δεύτερη προσέγγιση, η οποία δεν απαιτεί αλλαγές στις εφαρμογές για την επιλογή των προφίλ υπηρεσιών που προσφέρεται από την αρχιτεκτονική DiffServ.

Στην πρώτη περίπτωση η εφαρμογή θα πρέπει να είναι ενήμερη για την κατάσταση δέσμευσης πόρων (reservation state) στο δίκτυο ώστε στην περίπτωση που δεν ισχύει πια η δέσμευση να μπορεί να το γνωρίζει. Στη δεύτερη περίπτωση είτε η εφαρμογή είναι ενήμερη είτε όχι για τα προφίλ υπηρεσίας, δεν υπάρχει κανένα επίπεδο ασφαλείας για την εφαρμογή σε ένα τέτοιο μοντέλο. Πιο συγκεκριμένα αν το δίκτυο βρίσκεται σε κατάσταση υψηλού φόρτου, η εφαρμογή δεν ειδοποιείται για αυτή τη κατάσταση και φυσικά δεν είναι σε θέση να γνωρίζει ποτέ ότι η ποιότητα υπηρεσίας που ζήτησε δεν παρέχεται από το δίκτυο.

- Μία άλλη διαφορά μεταξύ των δύο αρχιτεκτονικών που μελετάμε είναι ότι στην αρχιτεκτονική DiffServ προσφέρεται μόνο ένας περιορισμένος αριθμός κλάσεων ποιότητας υπηρεσίας που προσδιορίζονται από την τιμή του πεδίου DS των πακέτων. Αντίθετα στις IntServ ο πελάτης μπορεί να ζητήσει απεριόριστο αριθμό διαφορετικών μεταχειρίσεων για κάθε ροή κίνησής του.

Η χρήση του IntServ μοντέλου σε DiffServ δίκτυα, προσφέρει υπό προϋποθέσεις κάποια πλεονεκτήματα, καθώς προσφέρει την επεκτασιμότητα του DiffServ μοντέλου ενώ ταυτόχρονα παρέχει εγγυήσεις ποιότητας υπηρεσίας σε επίπεδο ροών κίνησης. Για να δουλέψει το μοντέλο όμως πρέπει να πληρούνται μια σειρά από προϋποθέσεις. Κατ' αρχήν, το DiffServ δίκτυο πρέπει να μπορεί να υποστηρίξει τις IntServ υπηρεσίες, με την αντιστοίχησή τους σε κατάλληλα PHB. Επίσης, πρέπει να μπορεί να προσφέρει ικανή πληροφορία στο μη-DiffServ δίκτυο, σχετικά με την διαθεσιμότητα των πόρων του, προκειμένου να πραγματοποιείται ο έλεγχος αποδοχής κλήσης. Τέλος, το DiffServ δίκτυο, πρέπει να επιτρέπει τη διέλευση των RSVP μηνυμάτων με τρόπο που να μπορούν να ανακτηθούν στην έξοδο του δικτύου. Έτσι

προκειμένου να δουλέψει το μοντέλο αυτό, απαιτείται επιπλέον εργασία στους παρακάτω τομείς:

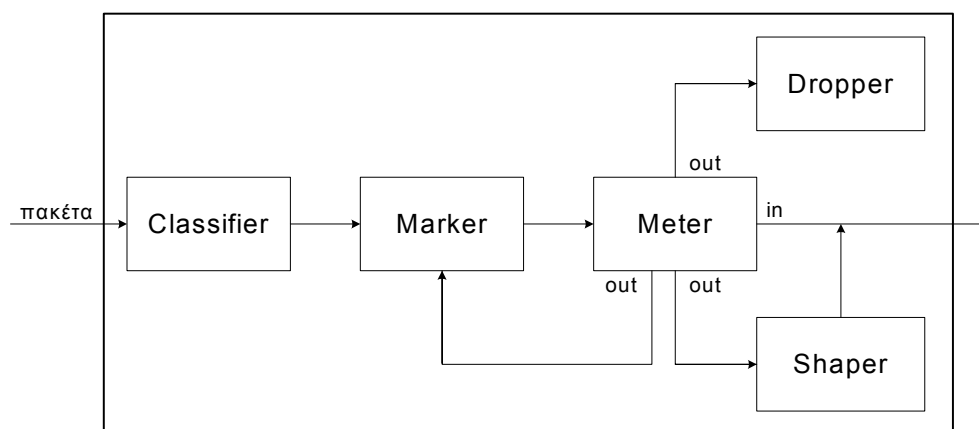
- Αντιστοίχιση των υπηρεσιών τύπου IntServ, με υπηρεσίες που μπορούν να παρασχεθούν από DiffServ δίκτυα.
- Προσδιορισμός της λειτουργικότητας που πρέπει να διαθέτουν τα στοιχεία του DiffServ δικτύου για την υποστήριξη της RSVP σηματοδότησης.
- Προσδιορισμός μηχανισμών για τον αποδοτικό και δυναμικό προσδιορισμό των εκάστοτε διαθέσιμων πόρων του DiffServ δικτύου.

4. Μηχανισμοί για την υλοποίηση QoS αρχιτεκτονικών

Πολύ σημαντικός παράγοντας για την καλή λειτουργία των σύγχρονων IP δικτύων είναι η ενεργοποίηση διαφόρων μηχανισμών διαχείρισης και εξυπηρέτησης της κίνησης στους δρομολογητές. Μια μεγάλη κατηγορία αυτών των μηχανισμών ονομάζονται μηχανισμοί διαχείρισης πακέτων (data path μηχανισμοί) και εφαρμόζονται στα πακέτα που διακινούνται σε ένα IP δίκτυο προκειμένου να αποδοθούν σε αυτά διαφορετικά επίπεδα υπηρεσίας.

4.1. Μηχανισμοί Διαχείρισης πακέτων

Στο παρακάτω διάγραμμα παρουσιάζουμε τους βασικούς μηχανισμούς διαχείρισης πακέτων (για τους οποίους έχουμε μιλήσει περιληπτικά προηγουμένως) με τη σειρά με την οποία τα πακέτα υπόκεινται στην επεξεργασία καθενός από τους μηχανισμούς και την αλληλεπίδραση των μηχανισμών αυτών μεταξύ τους. Φυσικά η διαδικασία ενεργοποίησης των μηχανισμών μπορεί να αλλάξει (π.χ. ο shaper να προηγείται του meter), ανάλογα με την περίπτωση και τις προδιαγραφές των υπηρεσιών τις οποίες υποστηρίζουν οι μηχανισμοί. Στη συνέχεια εξετάζουμε έναν προς ένα τους μηχανισμούς αυτούς.



4.1.1. Ταξινόνηση (Classification)

Ο μηχανισμός ταξινόμησης των πακέτων που υλοποιεί ένας δρομολογητής επηρεάζει την κλίμακα με την οποία μπορεί να απομονώσει διαφορετικούς τύπους κίνησης και να παρέχει υπηρεσίες σε αυτές. Η διαφοροποίηση της κίνησης στην εξυπηρέτηση από μια QoS υποδομή μπορεί να είναι είτε σε επίπεδο microflow (ροών) είτε σε επίπεδο aggregate. Στην πράξη, η ταξινόμηση ενός πακέτου είναι συνάρτηση τόσο της πληροφορίας που περιλαμβάνεται στην επικεφαλίδα του πακέτου όσο και στην «τοπολογική» πληροφορία που προκύπτει ανάλογα με το interface στο οποίο το πακέτο εμφανίζεται. Ανεξάρτητα από το ποια πεδία χρησιμοποιούνται για την ταξινόμηση των πακέτων, ο μηχανισμός ταξινόμησης πρέπει να είναι γρήγορος αρκετά για να παρακολουθεί τον ρυθμό άφιξης πακέτων.

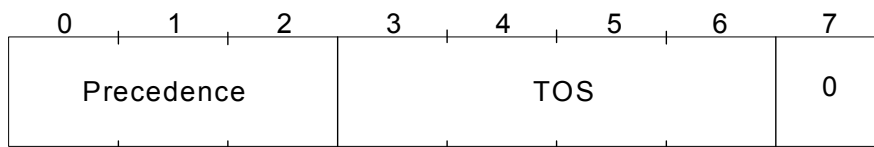
Μια ροή ορίζεται μονοσήμαντα από μια πεντάδα (IP δν/ση πηγής, αριθμός port πηγής, IP δν/ση προορισμού, αριθμός port προορισμού, πρωτόκολλο {TCP, UDP}), δηλαδή μια εξέταση περισσότερων του ενός πεδίων από το header κάθε IP πακέτου στο επίπεδο μεταφοράς. Η διαδικασία αυτή για την ταξινόμηση πακέτων απαιτεί επεξεργαστική ισχύ και χρησιμοποιείται σε περιπτώσεις που η ταξινόμηση πακέτων ανά ροή είναι απαραίτητη. Οι περιπτώσεις αυτές αφορούν QoS αρχιτεκτονικές που παρέχουν εγγυήσεις ποιότητας ανά ροή (π.χ. IntServ) καθώς και την αρχιτεκτονική DiffServ σύμφωνα με την οποία απαιτείται διεξοδική ταξινόμηση των πακέτων στα σημεία εισόδου της κίνησης σε ένα DiffServ-enabled domain (DS domain) εξετάζοντας περισσότερα του ενός πεδία της επικεφαλίδας των IP πακέτων. Στην τελευταία περίπτωση, αυτή η μέθοδος ταξινόμησης πακέτων αναφέρεται ως Multifield (MF) classification.

Αν η ταξινόμηση έχει ως στόχο την διάκριση των πακέτων σε σύνολα ροών, δηλ. aggregates υπάρχει θεωρητικά μεγάλη ποικιλία κριτηρίων για την διαφοροποίηση ενός υποσυνόλου ροών από ένα ευρύτερο σύνολο και το σχηματισμό ενός aggregate. Έτσι είναι δυνατόν ένα aggregate να ορίζεται με ένα ή περισσότερα από τα στοιχεία της πεντάδας που προαναφέρθηκε (π.χ. το (*,*,*,*, TCP) είναι ένα aggregate από TCP ροές). Στην πράξη, όταν ο σχεδιαστής ενός δικτύου γνωρίζει ότι χρειάζεται έναν μηχανισμό διαφοροποίησης όλων των πακέτων σε ένα μικρό αριθμό κλάσεων, η πιο αποδοτική λύση είναι η χρήση ενός σταθερού πεδίου στην επικεφαλίδα των πακέτων ο οποίος θα δηλώνει την κλάση όπου ανήκει το καθένα από αυτά. Έτσι καθώς το

πακέτο διατρέχει το δίκτυο, σε κάθε δρομολογητή ο μηχανισμός ταξινόμησης κάνει bit-wise σύγκριση με το πεδίο αυτό της επικεφαλίδας του IP πακέτου η οποία είναι πολύ πιο γρήγορη και καταναλώνει λιγότερη επεξεργαστική ισχύ από την MF ταξινόμηση. Στην περίπτωση της DiffServ αρχιτεκτονικής, αυτή η μέθοδος διάκρισης μεταξύ πακέτων αναφέρεται ως Behaviour Aggregate (BA) classification γιατί ακριβώς διαχωρίζει τα πακέτα σε aggregates. Στις ενότητες που ακολουθούν περιγράφονται τα πεδία βάση των οποίων γίνεται η κατηγοριοποίηση των πακέτων που φτάνουν σε ένα interface εισόδου ενός δρομολογητή.

4.1.1.1. BA ταξινόμηση (IP Precedence/ToS και DSCP)

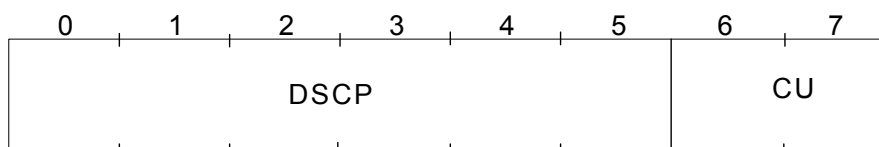
Τα IPv4 πακέτα περιέχουν στην επικεφαλίδα τους μια οκτάδα από bits (ToS octet) η οποία επιτρέπει BA ταξινόμηση.



Το ToS octet του IPv4 header

Αρχικά τα τρία πρώτα bits ορίστηκαν προκειμένου να αναπαριστούν την σχετική προτεραιότητα κάθε πακέτου, επιτρέποντας έτσι 2^3 διαφορετικά επίπεδα προτεραιότητας. Τα επόμενα τέσσερα bits δηλώνουν το επιθυμητό είδος δρομολόγησης/προώθησης των πακέτων (π.χ. ελαχιστοποίηση καθυστέρησης, μεγιστοποίηση ρυθμού μετάδοσης, μεγιστοποίηση αξιοπιστίας, ελαχιστοποίηση κόστους και κανονική εξυπηρέτηση). Αντίστοιχο πεδίο υπάρχει και για τα IPv6 πακέτα.

Πρόσφατα το IPv4 ToS octet ορίστηκε να περιλαμβάνει στα 6 πιο σημαντικά bits του το DiffServ Code Point (DSCP), το οποίο ορίζει 2^6 διαφορετικούς συνδυασμούς διαχείρισης στις ουρές και χρονοδρομολόγησης για τα IP πακέτα.



Η IPv4 επικεφαλίδα σύμφωνα με την DiffServ αρχιτεκτονική (CU=Currently Unused)

Μαζί με τον ορισμό του DiffServ πεδίου για το IPv4 ορίζεται και το αντίστοιχο TC octet για το IPv6

4.1.1.2. IPv4 MF ταξινόμηση

Στην επόμενη εικόνα φαίνονται τα πεδία της επικεφαλίδας ενός IP πακέτου που χρησιμοποιούνται για MF ταξινόμηση. Υπάρχουν δύο επίπεδα πολυπλοκότητας για έναν MF classifier:

- αυτό της εξέτασης των πεδίων που φαίνονται στην παρακάτω εικόνα και αθροιστικά αποτελούνται από 104 bits και
- αυτό των κανόνων ταξινόμησης που εφαρμόζονται σε πολλαπλές ροές ταυτόχρονα και εκφράζονται είτε σαν μοναδικές τιμές (exact-match classifier) είτε σαν διαστήματα τιμών των πεδίων ταξινόμησης (π.χ. ο κανόνας «Πρωτόκολλο=TCP» ή ο κανόνας «IP source addresses between 128.90.80.20 and 129.0.0.0») (range-matching classifier).

Ένας περιορισμός της MF ταξινόμησης είναι ότι IPv4 πακέτα που έχουν διασπαστεί περιέχουν τις TCP/UDP port τιμές μόνο στο πρώτο απόσπασμα οπότε ο MF classifier μπορεί να μην εντοπίσει για όλα τα αποσπάσματα ενός πακέτου την απαιτούμενη πληροφορία για την ταξινόμησή τους. Το πρόβλημα αυτό δεν υπάρχει στην περίπτωση του ToS/DiffServ byte το οποίο αντιγράφεται σε κάθε απόσπασμα ενός πακέτου.



Τα πεδία της επικεφαλίδας ενός IP πακέτου που χρησιμοποιούνται για MF ταξινόμηση.

4.1.2. Ρύθμιση της κίνησης (Traffic Conditioning)

Σε αυτήν τη παράγραφο περιγράφουμε μηχανισμούς ρύθμισης της κίνησης του δικτύου, που έχουν ως σκοπό την επιτέλεση των λειτουργιών του μαρκαρίσματος (marker), της μέτρησης (meter) και της μορφοποίησης των πακέτων που εισέρχονται στο δίκτυο. Η αλληλουχία των πακέτων μιας σύνδεσης, όπως αυτή εμφανίζεται στο σημείο πρόσβασης στο δίκτυο μπορεί να εμφανίζεται αλλοιωμένη σε σχέση με τις προσυμφωνημένες παραμέτρους κίνησης. Η αλλοίωση μπορεί να οφείλεται στον χρήστη ή σε άλλους παράγοντες όπως π.χ. στην παρεμβολή ενός τοπικού δικτύου χρήστη. Για να αποφευχθεί η προσήμανση ή η απόρριψη πακέτων που ανήκουν σε σύμμορφους χρήστες εισάγεται η λειτουργία της μορφοποίησης κίνησης. Πριν το σημείο πρόσβασης στο δίκτυο η ροή των πακέτων διαμορφώνεται κατά τέτοιο τρόπο, ώστε οι μετρήσεις που επιτελούνται στα πακέτα από τις συσκευές αστυνόμευσης να βρίσκονται σε συμφωνία με τις τιμές του συμβολαίου κίνησης. Παρόλο που η μορφοποίηση κίνησης αναφέρεται ως προαιρετική στις συστάσεις, στην πραγματικότητα είναι απόλυτα αναγκαία όταν υπάρχει συγκέντρωση κίνησης πολλαπλών πηγών πριν το σημείο πρόσβασης στο κυρίως δίκτυο. Επίσης ένα δίκτυο μπορεί να χρησιμοποιεί μορφοποίηση όταν μεταφέρει μια ροή πακέτων σε ένα άλλο δίκτυο, με σκοπό να ικανοποιηθούν οι συνθήκες ρυθμού του συμβολαίου κίνησης από δίκτυο σε δίκτυο, ή με σκοπό να εξασφαλίσει ότι η εφαρμογή που τρέχει στο τερματικό του λαμβάνοντα χρήστη, θα λειτουργήσει με αποδεκτό τρόπο.

Ουσιαστικά με τους μηχανισμούς που αναφέρουμε παραπάνω είναι εφικτός ο ορισμός των υπηρεσιών οι οποίες παρέχονται σε κάθε ροή με ένα συγκεκριμένο προφίλ από τη στιγμή που τα πακέτα της θα εισέλθουν στο domain. Υπάρχει όμως και η δυνατότητα ορισμού υπηρεσιών που καθορίζονται από τον παραλήπτη της κίνησης και στην περίπτωση αυτή ο μετρητής του προφίλ της κίνησης εγκαθίσταται στον παραλήπτη. Η δυνατότητα αυτή παρέχεται μόνο στις περιπτώσεις όπου κάθε δρομολογητής στο εσωτερικό του domain υποστηρίζει την Explicit Congestion Notification (ECN) λειτουργικότητα, σύμφωνα με την οποία τίθεται το ECN bit σε κάθε διερχόμενο πακέτο εάν ανιχνευτεί συμφόρηση. Όταν τα πακέτα φτάσουν στον παραλήπτη, υπόκεινται σε μέτρηση για το κατά πόσο υπακούουν στο προφίλ της ροής στην οποία ανήκουν. Εάν είναι νόμιμα, τότε αγνοείται η τιμή του ECN bit τους, αλλιώς το ECN bit αντιγράφεται στα ack πακέτα τα οποία φτάνοντας στον αποστολέα

αποτελούν ένδειξη για τη μείωση του ρυθμού μετάδοσης. Δεδομένου ότι έχουν επικρατήσει στην πλειοψηφία των περιπτώσεων και προσφέρουν καλύτερο έλεγχο της συμφόρησης, οι μηχανισμοί ελέγχου των χαρακτηριστικών της κίνησης που παρατίθενται στις επόμενες ενότητες εφαρμόζονται στην είσοδο της κίνησης σε ένα domain, είναι δηλαδή βασισμένοι στον αποστολέα. Ωστόσο ακόμα και σε αυτή την περίπτωση υπάρχει ένα σημαντικό μειονέκτημα: οι μηχανισμοί αυτοί δεν έχουν γνώση του RTT ή άλλων εγγενών χαρακτηριστικών των ροών με αποτέλεσμα να δημιουργούνται διακρίσεις μεταξύ ροών. Στην ιδανική περίπτωση οι μηχανισμοί για τον έλεγχο του προφίλ της κίνησης είναι εγκατεστημένοι και λειτουργούν μέσα στους hosts, έτσι ώστε να αλληλεπιδρούν με το TCP, να λειτουργούν βάση των ιδιαίτερων χαρακτηριστικών κάθε ροής και να ελαχιστοποιείται π.χ. η απόρριψη πακέτων.

4.1.2.1. Αλγόριθμοι διαρρέοντος δοχείου (Token και leaky bucket)

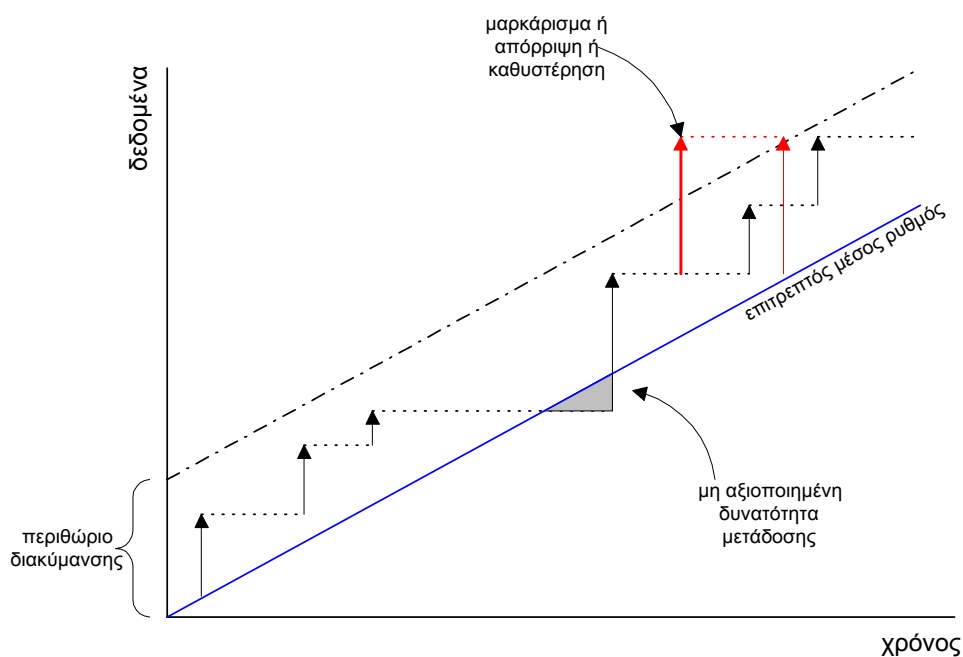
Οι πιο απλοί μηχανισμοί ελέγχου της κίνησης μιας ροής που διακρίνει τα πακέτα της σε In και Out ανάλογα με το αν υπακούουν ή όχι σε ένα προκαθορισμένο προφίλ είναι αυτοί των leaky και token bucket. Οι δύο αυτοί αλγόριθμοι έχουν ως στόχο την επιβολή ενός μέσου ρυθμού μετάδοσης σε μια ροή επιτρέποντας εκρηκτικότητα μικρής διάρκειας.

Ο μεν leaky bucket καθορίζει αυστηρά τον ρυθμό διοχέτευσης των πακέτων στο δίκτυο επιτρέποντας την συσσώρευση τους μέχρι ενός συγκεκριμένου ποσού πακέτων, αν ο ρυθμός άφιξης τους είναι μεγαλύτερος από τον ρυθμό αποχώρησης. Μπορεί να θεωρηθεί σαν μια δεξαμενή από την οποία τα πακέτα εξέρχονται με σταθερό ρυθμό, εισέρχονται με οποιοδήποτε ρυθμό και αν χρειάζεται και υπάρχει χώρος αποθηκεύονται προσωρινά. Αλλιώς τα πακέτα μαρκάρονται σαν Out (εκτός του νόμιμου προφίλ κίνησης) ή σαν πακέτα κλάσης εξυπηρέτησης με μικρότερη προτεραιότητα ή απορρίπτονται.

Ο token bucket καθορίζει το μέσο ρυθμό εισαγωγής των πακέτων στο δίκτυο χωρίς να εμποδίζει διακυμάνσεις στον στιγμιαίο ρυθμό μετάδοσης. Επιτρέπει εκρήξεις συγκεκριμένου μεγέθους, το οποίο ελέγχεται με το μέγιστο πλήθος tokens (b) που μπορούν να συσσωρευτούν και να χρησιμοποιηθούν για την αποστολή μιας

ακολουθίας πακέτων. Η δημιουργία tokens γίνεται με ρυθμό ίσο με το μέσο ρυθμό μετάδοσης που επιβάλλει ο token bucket (r) και όσο αυτά δεν χρησιμοποιούνται για την εξυπηρέτηση πακέτων συσσωρεύονται μέχρι το μέγιστο πλήθος b . Τα πακέτα για τα οποία δεν υπάρχουν διαθέσιμα tokens κατά την άφιξή τους θεωρούνται εκτός του νόμιμου προφίλ κίνησης οπότε μαρκάρονται σαν Out ή σαν πακέτα κλάσης εξυπηρέτησης με μικρότερη προτεραιότητα ή απορρίπτονται.

Στην παρακάτω εικόνα φαίνεται σχηματικά η ανοχή απόκλισης από τον επιτρεπτό μέσο ρυθμό που επιτρέπει ο αλγόριθμος token bucket.



4.1.3. Διαχείριση Ουρών (Queue Management)

Η διαχείριση ουρών χωρίζεται σε δύο κατηγορίες ανάλογα με τον σκοπό τον οποίο υπηρετεί. Στην διαχείριση που αφορά την αποφυγή της συμφόρησης (congestion avoidance) και στην διαχείριση που αφορά την αντιμετώπιση της συμφόρησης (congestion control). Επίσης, οι ροές κίνησης στο Διαδίκτυο μπορούν να χωριστούν στις TCP-συμβατές ροές, δηλαδή ροές που προσαρμόζουν το ρυθμό εκπομπής πακέτων σε περίπτωση συμφόρησης και στις μη TCP-συμβατές ροές που δεν ανήκουν στην παραπάνω κατηγορία. Ως γνωστό, η μεγάλη διάδοση και επιτυχία του Διαδικτύου οφείλεται στο μηχανισμό του TCP. Επειδή το TCP μειώνει το ρυθμό

εκπομπής πακέτων σε κατάσταση συμφόρησης, ένας μεγάλος αριθμός από TCP συνδέσεις μπορεί να μοιραστεί το εύρος ζώνης μιας συμφορημένης διασύνδεσης. Αντίθετα, για τις μη-TCP συμβατές ροές, κυρίως εφαρμογές UDP, δεν υπάρχουν μηχανισμοί αποφυγής συμφόρησης ή όσοι υπάρχουν είναι ανεπαρκείς.

Πιο συγκεκριμένα, οι αλγόριθμοι αποφυγής συμφόρησης (congestion avoidance) αφορούν τις TCP-συμβατές ροές και υλοποιούνται με την απόρριψη πακέτων πριν επέλθει η πλήρωση των ουρών, έτσι ώστε οι πηγές πακέτων να ανταποκριθούν στη συμφόρηση χωρίς να έχει προηγηθεί η υπερχειλίση των αντίστοιχων ουρών. Η προσέγγιση αυτή καλείται ενεργή διαχείριση ουρών (active queue management). Με την υιοθέτηση της παραπάνω προσέγγισης, οι δρομολογητές θα έχουν τη δυνατότητα να ελέγχουν πότε και πόσα πακέτα θα χαθούν στη συνέχεια. Οι αλγόριθμοι αντιμετώπισης συμφόρησης (congestion control) λαμβάνουν χώρα όταν επέλθει η συμφόρηση (συμπλήρωση ενταμιευτή με πακέτα) και αποσκοπούν στην εξασφάλιση ενός όσο το δυνατό μικρότερου ρυθμού απόρριψης πακέτων. Οι αλγόριθμοι αυτοί είναι ιδιαίτερα σημαντικοί για τις μη TCP-συμβατές ροές για τις οποίες, όπως έχουμε ήδη αναφέρει, δεν υπάρχει δυνατότητα προσαρμογής σε περίπτωση συμφόρησης. Στη σπουδαιότητα των αλγορίθμων αντιμετώπισης συμφόρησης συντείνει η μεγάλη έξαρση των εφαρμογών πολυμέσων με υψηλές απαιτήσεις σε εύρος ζώνης και μικρές ανοχές στις χρονικές καθυστερήσεις.

Ο διαχειριστής ουρών είναι υπεύθυνος για την εγκαθίδρυση και τη συντήρηση των διάφορων ουρών και γενικότερα για συμπεριφορά των ουρών ενός δρομολογητή. Αυτή η ευθύνη αναλύεται σε έξι βασικές δραστηριότητες:

- προσθήκη ενός πακέτου σε μία ουρά (που καθορίζεται από τις πληροφορίες που αφορούν το πακέτο, όπως αυτές καθορίστηκαν στο στάδιο της κατηγοριοποίησης), εάν βέβαια η ουρά δεν είναι γεμάτη.
- απόρριψη ενός πακέτου, εάν η σχετική ουρά είναι γεμάτη.
- αφαίρεση ενός πακέτου όταν αυτό ζητηθεί από τον χρονοδρομολογητή για μετάδοση πάνω από τη γραμμή.
- προαιρετική παρακολούθηση της πληρότητας των ουρών (δηλαδή του αριθμού των πακέτων σε κάθε ουρά) και η προκαταβολική ενεργοποίηση ενός από τα παρακάτω βήματα για να διατηρηθεί η πληρότητα των ουρών σε χαμηλά επίπεδα:

- αφαίρεση και απόρριψη ενός πακέτου (ή απόφαση να μην προστεθεί, και άρα να απορριφθεί, ένα πακέτο) όταν η ουρά είναι (ή έχει αρχίσει να γίνεται) σχεδόν πλήρης (γεμάτη).
- μαρκάρισμα ενός πακέτου, όταν η ουρά έχει αρχίσει να γίνεται σχεδόν πλήρης.

4.1.3.1. Αλγόριθμοι διαχείρισης ουρών για αποφυγή συμφόρησης

Ο πρωταρχικός σκοπός των αλγορίθμων αποφυγής συμφόρησης σε ένα δρομολογητή είναι η ανίχνευση της επερχόμενης συμφόρησης. Ένας αλγόριθμος αποφυγής συμφόρησης πρέπει να διατηρεί το δίκτυο σε κατάσταση χαμηλών καθυστερήσεων και υψηλών ρυθμών εξυπηρέτησης. Συνεπώς, το μέσο μήκος των ουρών θα πρέπει να διατηρείται μικρό, αλλά θα πρέπει να επιτρέπονται οι διακυμάνσεις στο πραγματικό μήκος των ουρών λόγω της εκρηκτικότητας της κίνησης και των παροδικών συμφορήσεων.

Η μείωση της πληρότητας των ουρών απαιτεί κάποιο μηχανισμό ανάδρασης για την αποφυγή της συμφόρησης στα πρωτόκολλα του επιπέδου μεταφοράς (που δημιουργούν τις ροές που διέρχονται από την ουρά). Καθώς μέχρι να αρχίσουν να αντιδρούν τα πρωτόκολλα μεσολαβεί κάποιος χρόνος, η διαχείριση ουρών πρέπει να διακρίνει ανάμεσα σε δύο διαφορετικούς τύπους συμφόρησης:

- παροδική συμφόρηση (transient congestion), που διαρκεί λιγότερο από το χρόνο αντίδρασης των πρωτοκόλλων αποφυγής συμφόρησης και προκαλείται από μικρές εξάρσεις της κίνησης και εξομαλύνεται γρήγορα.
- μακροπρόθεσμη συμφόρηση (long-term congestion), που προκαλείται από το ρυθμό (στη σταθερή κατάσταση) των ροών που διέρχονται από την ουρά.

Είναι φανερό η διαχείριση ουρών ασχολείται κυρίως με το δεύτερο τύπο συμφόρησης. Προκειμένου να αποφεύγεται αυτού του είδους η συμφόρηση και να διατηρείται χαμηλά η μέση πληρότητα των ουρών, ο διαχειριστής ουρών πρέπει να ανατροφοδοτεί τα πρωτόκολλα του επιπέδου μεταφοράς συνεχώς με πληροφορίες

(κυρίως αρνητικές) για την παρατηρούμενη συμφόρηση. Αυτό γίνεται με το σημάδεμα και την απόρριψη των πακέτων. Το σημάδεμα των πακέτων απαιτεί από τα πρωτόκολλα του επιπέδου μεταφοράς να αντιδρούν στην παραλαβή σηματοδομένων πακέτων με ενεργοποίηση μηχανισμών αποφυγής συμφόρησης. Πρακτικά, στα IP δίκτυα προτιμάται η απόρριψη γιατί το πρωτόκολλο TCP αντιδρά στην απώλεια πακέτων με ενεργοποίηση του μηχανισμού του για την αποφυγή συμφόρησης. Επίσης η απόρριψη πακέτων έχει τα πλεονέκτημα μειώνει άμεσα το φόρτο κυκλοφορίας.

Παρόλο που η απόρριψη πακέτων είναι η προτιμώμενη σήμερα ενέργεια για την πληροφόρηση των πρωτοκόλλων του επιπέδου μεταφοράς για καταστάσεις συμφόρησης, γίνεται σχεδιασμός και εφαρμογή και μη-καταστροφικών μεθόδων σηματοδότησης (δηλαδή μεθόδων που δεν απορρίπτουν πακέτα). Αυτό γίνεται διότι η απόρριψη πακέτων ουσιαστικά είναι κατασπατάληση πόρων (αυτών που χρησιμοποιήθηκαν για να φτάσει το πακέτο μέχρι το δρομολογητή που το απορρίπτει). Επομένως, ενδείξεις συμφόρησης που αποφεύγουν την κατασπατάληση αυτή είναι ελκυστικές. Μία τέτοια πολύ γνωστή μέθοδος είναι η Ρητή Ειδοποίηση για Συμφόρηση (Explicit Congestion Notification – ECN), η οποία περιγράφεται στο RFC 2481. Τα δύο αχρησιμοποίητα bits (CU) του πεδίου DSCP επαναπροσδιορίζονται ως τα bits ECN Capable Transport (ECT) και Congestion Experienced (CE). Ένα πρωτόκολλο του επιπέδου μεταφοράς θέτει το ECT bit στα πακέτα που αποστέλλει όταν γνωρίζει ότι τα και δύο άκρα της ροής μπορούν να κατανοήσουν το νόημα του CE bit. Εάν δεν παρατηρηθεί συμφόρηση το ECT bit αγνοείται από τον εκάστοτε δρομολογητή. Εάν όμως κάποιος δρομολογητής επιθυμεί να ειδοποιήσει για κατάσταση συμφόρησης, τότε έχει δύο επιλογές:

- Εάν το ECT bit έχει τιμή 1, τότε θέτει το CE bit.
- Εάν το ECT bit έχει τιμή 0, τότε απορρίπτει το πακέτο.

Έτσι, τα πρωτόκολλα του επιπέδου μεταφοράς που κατανοούν το μηχανισμό του ECN, λαμβάνουν την σχετική ειδοποίηση με μη-καταστροφικό τρόπο, ενώ τα πρωτόκολλα που δεν το κατανοούν αντιλαμβάνονται την κατάσταση συμφόρησης από την απόρριψη του πακέτου. Από τα παραπάνω βέβαια μπορούμε να συμπεράνουμε ότι η ρητή ειδοποίηση για συμφόρηση λειτουργεί καλά μόνο σε περιπτώσεις μακροπρόθεσμης συμφόρησης. Σε περιπτώσεις παροδικής συμφόρησης μπορεί να λειτουργήσει αρνητικά μειώνοντας την απόδοση του δικτύου.

Αρκετοί αλγόριθμοι έχουν προταθεί κατά καιρούς για την αποφυγή συμφόρησης στο Διαδίκτυο όπως ο DECbit, ο αλγόριθμος Τυχαίας Έγκαιρης Απόρριψης (Early

Random Drop, ERD) και ο αλγόριθμος Τυχαίας Έγκαιρης Ανίχνευσης (Random Early Detection, RED), ο οποίος θεωρείται ως ο επικρατέστερος. Ο DECbit χρησιμοποιεί ένα bit ως ένδειξη συμφόρησης (congestion indication bit) στην επικεφαλίδα των πακέτων για να παρέχει πληροφορίες σχετικά με τη συμφόρηση στο δίκτυο. Για τους δρομολογητές που χρησιμοποιούν τον αλγόριθμο DECbit, το επίπεδο μεταφοράς (transport layer) θα πρέπει να υπολογίζει το ποσοστό των πακέτων που έχουν το bit συμφόρησης ίσο με 1. Ο εν λόγω αλγόριθμος δεν ευνοεί τις ροές που παρουσιάζουν εκρηκτικότητα. Με τον αλγόριθμο ERD, εάν το μήκος της ουράς ξεπερνάει ένα προκαθορισμένο επίπεδο (drop level), τότε ο δρομολογητής απορρίπτει κάθε εισερχόμενο πακέτο με σταθερή πιθανότητα (drop probability). Τα αποτελέσματα που δίνονται αποδεικνύουν ότι ο αλγόριθμος ERD δεν επιτυγχάνει τον έλεγχο των ροών με κακή συμπεριφορά. Τέλος, οι δρομολογητές που υιοθετούν τον αλγόριθμο RED διατηρούν το μέσο μήκος της ουράς μικρό και ταυτόχρονα έχουν τη δυνατότητα να εξυπηρετήσουν περιστασιακές αποστολές πακέτων με ριπές. Όταν το μέσο μήκος ουράς έχει ξεπεράσει το προκαθορισμένο όριο, οι RED δρομολογητές απορρίπτουν τυχαία πακέτα, έτσι ώστε οι ροές TCP να μειώνουν το ρυθμό εκπομπής σε διαφορετικές χρονικές στιγμές. Με αυτόν τον τρόπο αποφεύγεται ο συγχρονισμένος περιορισμός ρυθμών εκπομπής των ροών και ο ρυθμός εξυπηρέτησης διατηρείται υψηλός. Αντίθετα με τον DECbit, ο RED δεν ζημιώνει τις ροές που παρουσιάζουν εκρηκτικότητα και δεν έχει απαιτήσεις από το επίπεδο μεταφοράς. Επιπλέον, ενώ στον ERD υπάρχει αδυναμία ελέγχου των ροών με κακή συμπεριφορά (misbehaving), στον RED η πιθανότητα μείωσης του ρυθμού εκπομπής πακέτων μιας σύνδεσης καθορίζεται από το διατιθέμενο για τη σύνδεση ποσοστό εύρους ζώνης.

4.1.3.2. Τυχαία Έγκαιρη Ανίχνευση (Random Early Detection, RED)

Ένας δρομολογητής RED υπολογίζει το μέσο μήκος ουράς και όταν αυτό ξεπεράσει ένα προκαθορισμένο όριο, απορρίπτει κάθε εισερχόμενο πακέτο με πιθανότητα που μεταβάλλεται συναρτήσει του μέσου μήκους της ουράς. Το μέσο μήκος ουράς υπολογίζεται χρησιμοποιώντας ένα κατωδιαβατό φίλτρο με εκθετική μεταβολή (Exponentially Weighted Moving Average-EWMA) έτσι ώστε να επιτρέπει

πρόσκαιρες ριπές πακέτων στο δρομολογητή. Στην περίπτωση συνεχούς συμφόρησης στο δρομολογητή, το μέσο μήκος ουράς θα είναι μεγάλο καθώς και η πιθανότητα απόρριψης. Η μεγάλη πιθανότητα απόρριψης θα επιτρέπει την ανίχνευση καθώς και τον έλεγχο της συμφόρησης.

Οι παράμετροι του αλγορίθμου RED είναι οι εξής: \min_{th} , \max_{th} και P_{max} . Στο παρακάτω σχήμα ο άξονας x είναι το μέσο μήκος ουράς, το οποίο υπολογίζεται με την άφιξη κάθε πακέτου, όπως αναφέρθηκε παραπάνω, από το στιγμιαίο μήκος ουράς, χρησιμοποιώντας το φίλτρο EWMA. Ο άξονας y συμβολίζει την πιθανότητα απόρριψης εισερχόμενου πακέτου. Στον αλγόριθμο RED διακρίνουμε τρεις καταστάσεις ανάλογα με την τιμή του μέσου μήκους ουράς, δηλαδή τα διαστήματα $[0, \min_{th})$, $[\min_{th}, \max_{th})$, και $[\max_{th}, \infty)$, τις οποίες ονομάζουμε αντίστοιχα ομαλή λειτουργία, αποφυγή συμφόρησης και έλεγχος συμφόρησης αντίστοιχα. Κατά τη διάρκεια της ομαλής λειτουργίας, όταν το μέσο μήκος ουράς είναι χαμηλότερο από \min_{th} , ο δρομολογητής δεν απορρίπτει κανένα πακέτο. Όταν το μέσο μήκος ουράς είναι μεταξύ των δύο ορίων, ο δρομολογητής λειτουργεί σε κατάσταση αποφυγής συμφόρησης και με κάθε απόρριψη πακέτου ειδοποιείται το επίπεδο μεταφοράς να μειώσει το ρυθμό εκπομπής πακέτων. Για αυτό το λόγο η πιθανότητα απόρριψης είναι συνήθως μικρή με μέγιστη τιμή τη P_{max} . Όταν το μέσο μήκος ουράς είναι μεγαλύτερο από \max_{th} , ο δρομολογητής απορρίπτει κάθε εισερχόμενο πακέτο προκειμένου να διατηρήσει μικρό το μήκος της ουράς.

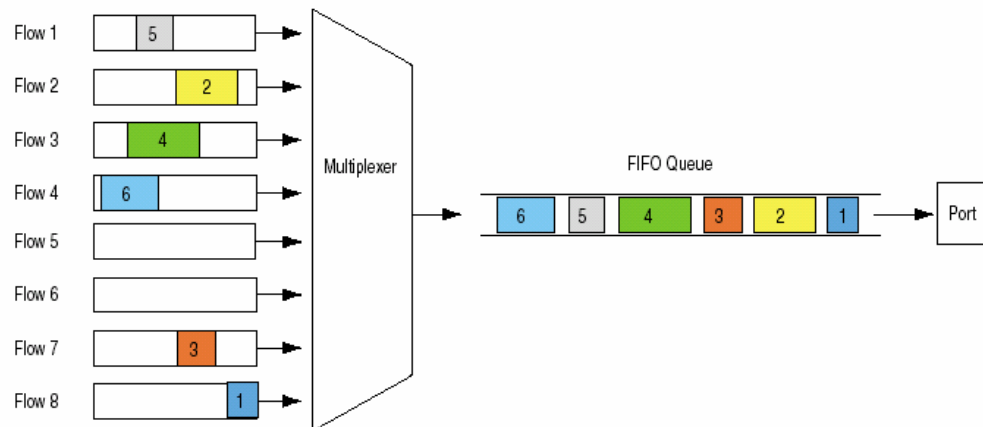
4.1.4. Χρονοδρομολόγηση (Scheduling)

Η βασική λειτουργία της χρονοδρομολόγησης είναι η επιλογή του επόμενου πακέτου που θα μεταδοθεί, καθώς και ο καθορισμός του χρόνου που θα συμβεί αυτό. Δηλαδή, η χρονοδρομολόγηση καθορίζει τα χρονικά χαρακτηριστικά των αναχωρήσεων των πακέτων από την έξοδο μίας ουράς. Στους μοντέρνους δρομολογητές ο χρονοδρομολογητής για κάθε γραμμή εξόδου συσχετίζεται με περισσότερες από μία ουρές και διαμοιράζει τη χρήση της γραμμής ανάμεσα σε αυτές. Όμως επειδή το κάθε πακέτο τοποθετείται σε κάποια συγκεκριμένη ουρά ανάλογα με την κλάση κίνησης στην οποία ανήκει, είναι επακόλουθο ότι ο χρονοδρομολογητής επιβάλλει τη σχετική προτεραιότητα, τα όρια της καθυστέρησης και την κατανομή του εύρους ζώνης των διαφόρων κλάσεων κίνησης που έχουμε θεσπίσει στο δίκτυό μας.

Συγκεκριμένα, ο χρονοδρομολογητής εξασφαλίζει ότι σε κάθε ροή θα δοθεί επαρκές εύρος ζώνης, εγγυάται μία μέγιστη καθυστέρηση (delay) για κάθε πακέτο καθώς και το ότι η διαφορά στην καθυστέρηση εξυπηρέτηση δύο συνεχόμενων πακέτων (jitter) δεν θα ξεπερνά κάποιο όριο. Επιπλέον μεριμνά για τη δίκαιη κατανομή του πλεονάζοντος εύρους ζώνης μεταξύ των ενεργών ροών, όταν δεν υπάρχει συμφόρηση. Στη συνέχεια περιγράφονται ορισμένοι από τους πιο συχνά χρησιμοποιούμενους αλγόριθμους χρονοδρομολόγησης.

4.1.4.1. First-in, First-out (FIFO) Queueing

Στον αλγόριθμο χρονοδρομολόγησης First-in, First-out (FIFO) όλα τα πακέτα υπόκεινται στην ίδια μεταχείριση αφού τοποθετούνται σε μια απλή ουρά και στη συνέχεια εξυπηρετούνται με την ίδια σειρά με την οποία τοποθετήθηκαν στην ουρά (όπως φαίνεται και στο παρακάτω σχήμα).



Ο αλγόριθμος χρονοδρομολόγησης FIFO έχει τα παρακάτω πλεονεκτήματα:

- Επιβαρύνει το δίκτυο με πολύ μικρό υπολογιστικό φόρτο.
- Η συμπεριφορά του είναι προβλέψιμη-τα πακέτα δεν αναδιατάσσονται και η μέγιστη καθυστέρηση καθορίζεται από το μέγιστο μήκος της ουράς.
- Όσο το μήκος της ουράς παραμένει μικρό, ο αλγόριθμος FIFO παρέχει ορθή χρήση των πόρων του δικτύου χωρίς να επηρεάζει σημαντικά την καθυστέρηση που εισάγεται από κάθε κόμβο.

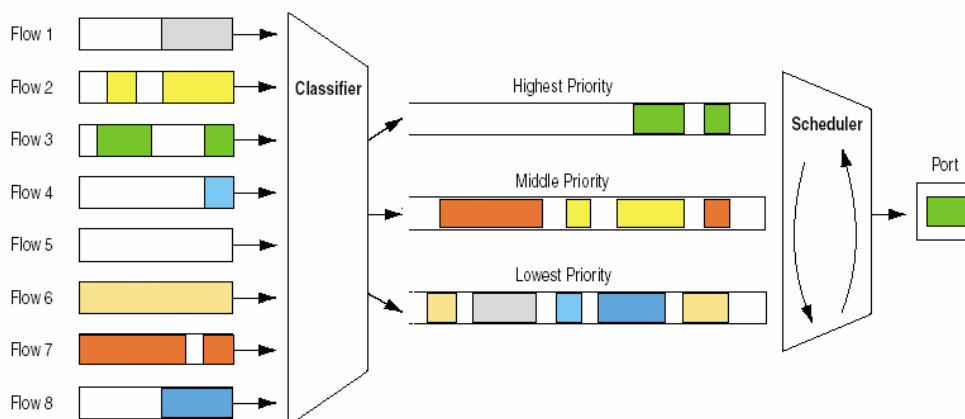
Ο αλγόριθμος χρονοδρομολόγησης FIFO έχει τα παρακάτω μειονεκτήματα:

- Δεν επιτρέπει στους δρομολογητές να οργανώνουν buffered πακέτα και επομένως να εξυπηρετούν μια κλάση διαφορετικά από τις άλλες.

- Μεταχειρίζεται όλες τις ροές ισοδύναμα, με αποτέλεσμα η μέση καθυστέρηση στην ουρά για όλες τις ροές να αυξάνεται όσο αυξάνεται η συμφόρηση. Ο αλγόριθμος FIFO μπορεί να οδηγήσει σε αυξημένη καθυστέρηση, jitter και απώλειες σε εφαρμογές πραγματικού χρόνου.
- Κατά την διάρκεια των περιόδων συμφόρησης, ο αλγόριθμος FIFO δίνει προτεραιότητα στις ροές UDP έναντι στις TCP. Και αυτό γιατί όταν υπάρχουν απώλειες πακέτων που οφείλονται στη συμφόρηση, οι TCP ροές μειώνουν τον ρυθμό εκπομπής τους, αλλά οι UDP ροές συνεχίζουν να στέλνουν με τον ίδιο ρυθμό.
- Μία εκρηκτική ροή μπορεί να καταναλώσει το σύνολο του buffer space μιας FIFO ουράς, κάτι που οδηγεί όλες τις υπόλοιπες ροές να μην μπορούν να εξυπηρετηθούν μέχρις ότου η εκρηκτική ροή να εξυπηρετηθεί πλήρως. Αυτό μπορεί να οδηγήσει σε αυξημένες καθυστερήσεις, jitter και απώλειες πακέτων όλες τις υπόλοιπες ροές.

4.1.4.2. Priority Queueing (PQ)

Ο αλγόριθμος PQ αποτελεί τη βάση των αλγορίθμων χρονοδρομολόγησης που έχουν σχεδιαστεί για να παρέχουν μια σχετικά απλή μέθοδο υποστήριξης διαφοροποιημένων υπηρεσιών. Στον κλασικό PQ αλγόριθμο, τα πακέτα αρχικά κατηγοριοποιούνται από το σύστημα και στη συνέχεια τοποθετούνται σε διαφορετικές ουρές προτεραιότητας. Τα πακέτα δρομολογούνται από την κεφαλή μιας δοσμένης ουράς μόνο εάν οι ουρές μεγαλύτερης προτεραιότητας είναι άδειες. Μέσα σε καθεμία από τις ουρές αυτές, τα πακέτα προωθούνται με βάση τον αλγόριθμο FIFO, όπως φαίνεται στο παρακάτω σχήμα.



Ο αλγόριθμος χρονοδρομολόγησης PQ έχει τα παρακάτω πλεονεκτήματα:

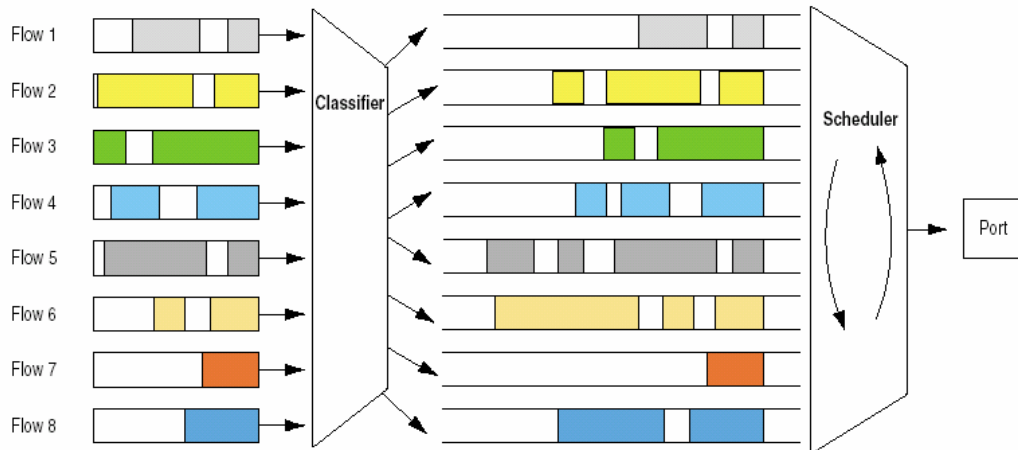
- Επιβαρύνει το δίκτυο με πολύ μικρό υπολογιστικό φόρτο. Επιβαρύνει το δίκτυο με μικρό υπολογιστικό φόρτο, συγκρινόμενος με άλλους χρησιμοποιούμενους αλγόριθμους.
- Επιτρέπει στους δρομολογητές να οργανώνουν buffered πακέτα, και έτσι να εξυπηρετούν συγκεκριμένες κλάσεις υπηρεσίας. Για παράδειγμα, μπορούμε να θέσουμε προτεραιότητες, τέτοιες ώστε οι υπηρεσίες πραγματικού χρόνου να έχουν προτεραιότητα απέναντι στις υπόλοιπες υπηρεσίες.

Ο αλγόριθμος χρονοδρομολόγησης PQ έχει τα παρακάτω μειονεκτήματα:

- Αν το ποσό της κίνησης υψηλής προτεραιότητας δεν ελέγχεται στα άκρα του δικτύου, τότε η κίνηση χαμηλής προτεραιότητας μπορεί να υποστεί υψηλές καθυστερήσεις.
- Αν το ποσό της κίνησης υψηλής προτεραιότητας γίνει πολύ μεγάλο, τότε η κίνηση χαμηλής προτεραιότητας μπορεί να απορριφθεί. Αν αυτό συμβεί, τότε είναι πιθανό λόγω του συνδυασμού των απωλειών των πακέτων, της αυξημένης καθυστέρησης και της επαναμετάδοσης από τα τερματικά να οδηγηθούμε σε πλήρη έλλειψη πόρων για την κίνηση χαμηλής προτεραιότητας.
- Μία κακώς συμπεριφερόμενη ροή υψηλής προτεραιότητας μπορεί να αυξήσει σημαντικά την καθυστέρηση και το jitter που θα υποστούν οι υπόλοιπες ροές της ίδιας κατηγορίας.

4.1.4.3. Fair Queueing (FQ)

Ο αλγόριθμος FQ αποτελεί την θεμελίωση μιας κλάσης αλγορίθμων χρονοδρομολόγησης που σχεδιάστηκαν για να βεβαιώσουν ότι κάθε ροή έχει δίκαιη πρόσβαση στους πόρους του δικτύου και να εμποδίσουν μία εκρηκτική ροή από τα να καταναλώνει περισσότερο εύρος ζώνης από αυτό που τις αναλογεί. Στον αλγόριθμο FQ, τα πακέτα κατηγοριοποιούνται σε ροές μέσα στο σύστημα, και στη συνέχεια οι ουρές αυτές εξυπηρετούν ένα πακέτο τη φορά βάσει του round-robin αλγορίθμου (οι άδειες ροές αγνοούνται).



Το πρωταρχικό όφελος του αλγορίθμου FQ είναι ότι μια εκρηκτική ή κακώς συμπεριφερόμενη ροή δεν υποβαθμίζει την ποιότητα υπηρεσίας που λαμβάνουν οι υπόλοιπες ροές, αφού κάθε ροή είναι απομονωμένη στην δική της ουρά. Αν μια ροή προσπαθεί να καταναλώσει παραπάνω εύρος ζώνης από αυτό που της αναλογεί, τότε επηρεάζεται μόνο η αντίστοιχη ουρά, έτσι ώστε να μην υπάρχει καμία επίδραση στην επίδοση των υπόλοιπων ροών.

Ο αλγόριθμος χρονοδρομολόγησης FQ έχει όμως και κάποια μειονεκτήματα:

- Ο αλγόριθμος FQ υλοποιείται μόνο σε λογισμικό και όχι σε υλικό, κάτι το οποίο περιορίζει την εφαρμογή του σε διεπαφές χαμηλών ταχυτήτων στα άκρα του δικτύου.
- Το αντικείμενο του συγκεκριμένου αλγορίθμου αφορά την απόδοση του ίδιου εύρους ζώνης σε όλες τις ροές και δεν μπορεί να υποστηρίξει ροές που ζητούν διαφορετικό εύρος ζώνης.
- Ο αλγόριθμος είναι ευαίσθητος στην σειρά αφίξεων των πακέτων. Αν το πακέτο φθάσει στην ουρά αμέσως μετά από το πέρασμα του αλγορίθμου round-robin από τη συγκεκριμένη ουρά, τότε το πακέτο πρέπει να περιμένει στην ουρά έως ότου όλες οι άλλες ουρές να έχουν εξυπηρετηθεί.

4.1.4.4. Weighted Fair Queueing

Ο αλγόριθμος WFQ υποστηρίζει ροές με διαφορετικές απαιτήσεις σε εύρος ζώνης με το να αντιστοιχεί σε κάθε ουρά ένα βάρος, το οποίο αντανακλά το διαφορετικό ποσοστό που έχει η συγκεκριμένη ουρά στη χρήση της εξωτερικής γραμμής. Ακόμη υποστηρίζει πακέτα μεταβλητού μήκους, έτσι ώστε στις ροές με μεγαλύτερα πακέτα

να μην ανατίθεται περισσότερο εύρος ζώνης από ότι σε ροές με μικρότερα πακέτα. Η υποστήριξη όμως της δίκαιης απονομής bandwidth κατά την προώθηση πακέτων μεταβλητού μήκους αυξάνει την υπολογιστική πολυπλοκότητα αυτού του αλγορίθμου.

Η βασική ιδέα του αλγορίθμου WFQ βασίζεται σε αυτή των προγραμματισμών πακέτων Generalized Processor Sharing (GPS) και έχει ως εξής: ένα «βάρος» ϕ_i συσχετίζεται με κάθε ροή κίνησης $i, i=1, \dots, N$, και το εύρος ζώνης του μέσου πρόσβασης μοιράζεται μεταξύ των ενεργών ροών ανάλογα με τα «βάρη» τους. Με άλλα λόγια εάν C είναι η ταχύτητα του μέσου πρόσβασης, τότε κάθε ροή i εξασφαλίζει ένα ελάχιστο ρυθμό εξυπηρέτησης ίσο με $(\phi_i / \sum_{j=1}^N \phi_j) * C, i=1, \dots, N$. Σε

κάποιες χρονικές στιγμές είναι πολύ πιθανό κάποιες από τις ενεργές ροές να μην έχουν αποθηκευμένα πακέτα που να αναμένουν να αποσταλούν στο μέσο πρόσβασης. Αυτό μεταφράζεται σε διαθέσιμο εύρος ζώνης του μέσου πρόσβασης το οποίο είναι δυνατό να μοιραστεί μεταξύ των υπερφορτωμένων ενεργών ροών σε πλήρη αναλογία προς τα αντίστοιχα «βάρη» τους. Όσο μεγαλύτερο είναι το «βάρος» μιας ροής τόσο μεγαλύτερο είναι και το ελάχιστο δεσμευμένο εύρος ζώνης για τη συγκεκριμένη ροή κίνησης και τόσο μεγαλύτερη είναι και η προτεραιότητα εξυπηρέτησής της.

Ο αλγόριθμος WFQ έχει δύο σημαντικά πλεονεκτήματα:

- Εγγυάται ένα ελάχιστο επίπεδο εύρους ζώνης για κάθε κλάση υπηρεσίας ανεξάρτητα από την συμπεριφορά των άλλων κλάσεων.
- Όταν συνδυάζεται με τεχνικές traffic conditioning στα άκρα του δικτύου, ο αλγόριθμος εγγυάται μια δίκαιη κατανομή του εύρους ζώνης σε κάθε κλάση υπηρεσίας, καθώς και τη μέγιστη καθυστέρηση που μπορούν να υποστούν τα πακέτα.

Ο αλγόριθμος χρονοδρομολόγησης WFQ έχει όμως και κάποια μειονεκτήματα:

- Ο αλγόριθμος WFQ υλοποιείται μόνο σε λογισμικό και όχι σε υλικό, κάτι το οποίο περιορίζει την εφαρμογή του σε διεπαφές χαμηλών ταχυτήτων στα άκρα του δικτύου.
- Λόγω της δημιουργίας κλάσεων υπηρεσίας με συσσωρευμένες ροές (aggregated service classes), αν μια ροή μιας κλάσης υπηρεσίας δεν συμπεριφέρεται σωστά, τότε θα επηρεάσει και τις υπόλοιπες ροές που ανήκουν στην ίδια κλάση υπηρεσίας.

- Ο αλγόριθμος WFQ έχει υψηλή πολυπλοκότητα, με αποτέλεσμα να μην είναι επεκτάσιμος στο να υποστηρίξει πολλές κλάσεις υπηρεσίας σε διεπαφές υψηλών ταχυτήτων (high-speed interfaces).

4.2. Μηχανισμοί Ελέγχου (Control Path Μηχανισμοί)

4.2.1. Έλεγχος απόδοσης (admission control)

Μία από τις μεγαλύτερες προκλήσεις του ελέγχου απόδοσης για την παροχή ποιότητας υπηρεσίας σε δίκτυα IP (Admission Control for IP QoS) είναι η σωστή και αποδοτική διαμοίραση των πηγών του δικτύου ανάμεσα στις ροές που γίνονται αποδεκτές από το δίκτυο. Οι παραδοσιακοί αλγόριθμοι αποδοχής ελέγχου (γνωστοί ως parameter-based admission control) βασίζονται σε στατιστικά μοντέλα που εξετάζουν την κάθε μία ροή χωριστά (M/M/1, M/D/1, M/M/n). Τα μοντέλα αυτά καθορίζουν τις παραμέτρους που περιγράφουν τα χαρακτηριστικά της κίνησης της κάθε ροής. Οι παράμετροι αυτοί στη συνέχεια χρησιμοποιούνται από τις ροές για να υπολογίσουν το ποσοστό των πόρων που χρειάζονται. Το δίκτυο στη συνέχεια χρησιμοποιεί αυτούς τους υπολογισμούς για να αποδεχτεί ή να απορρίψει ροές, ανάλογα με την διαθεσιμότητα ή όχι των ζητούμενων πόρων.

Όμως, το πρόβλημα με αυτή τη προσέγγιση είναι ότι είναι συχνά πολύ δύσκολο για εφαρμογές να συνεργαστούν με μοντέλα τα οποία περιγράφουν με ακρίβεια τις παραμέτρους τους, όσον αφορά την κίνηση. Αυτή η προσέγγιση αποτελεί μεγαλύτερη πρόκληση στα IP δίκτυα, όπου το μεγαλύτερο ποσοστό της κίνησης σε τέτοια δίκτυα είναι ετερογενής κίνηση. Έτσι, προκειμένου να παρέχουμε εγγυημένες υπηρεσίες (όταν αυτές αποδοθούν), οι ροές πρέπει να παρέχουν a priori εκτιμήσεις που να αντιπροσωπεύουν το σενάριο χειρότερης συμπεριφοράς. Αυτό προκαλεί την δέσμευση παραπάνω πόρων από τις αληθινά χρησιμοποιούμενες με αποτέλεσμα τη χαμηλή χρησιμοποίηση του δικτύου (low network utilization). Η χρησιμοποίηση αυτή είναι ακόμη πιο χαμηλή αν οι ροές είναι εκρηκτικές.

4.2.1.1. Έλεγχος Απόδοχής βασισμένος σε μετρήσεις (Measurement-based Admission Control)

Ο έλεγχος απόδοσης βασισμένος σε μετρήσεις (MBAC) είναι μια εναλλακτική πρόταση απέναντι στον έλεγχο απόδοσης βασισμένο σε παραμέτρους (parameter-based admission control), του οποίου οι αποφάσεις βασίζονται στον υπολογισμό των παραμέτρων κίνησης που γίνονται με βάση μετρήσεις της τωρινής κυκλοφορίας. Κάθε MBAC έχει δύο συνιστώσες :

- Μία διαδικασία μετρήσεων για τον υπολογισμό του τωρινού φορτίου του δικτύου και
- έναν αλγόριθμο που χρησιμοποιεί τον υπολογισμό του φορτίου για να παίρνει αποφάσεις αποδοχής.

Φυσικά, οι μετρήσεις της κίνησης δεν είναι πάντα κατάλληλοι παράγοντες για την πρόβλεψη της μελλοντικής συμπεριφοράς, και η προσέγγιση που βασίζεται σε measurement-based μηχανισμούς μπορεί να οδηγήσει σε περιστασιακές απώλειες πακέτων ή σε καθυστερήσεις που ξεπερνούν τα επιθυμητά επίπεδα. Κατά τον σχεδιασμό ενός αλγορίθμου MBAC πρέπει να δοθεί μια παράμετρος, η οποία θα υπολογίζει ακριβώς το επίπεδο των υπηρεσιών που θα αποτυγχάνουν και επιπλέον να επιτευχθεί η καλύτερη δυνατή χρησιμοποίηση (utilization) δεδομένου του επιπέδου των απωλειών.

Οι προτεινόμενοι αλγόριθμοι παρόλο που έχουν παρόμοια πλεονεκτήματα, διαφέρουν σε τέσσερα σημαντικά σημεία.

- Ορισμένοι βασίζονται σε αυστηρές μαθηματικές θεωρίες και σχέσεις, ενώ άλλοι είναι ad-hoc (έχουν έλλειψη ενός θεωρητικού υποβάθρου).
- Οι εξισώσεις που χρησιμοποιεί ο καθένας για να παίρνει αποφάσεις διαφέρουν σε αρκετά σημεία μεταξύ τους.
- Ενώ όλοι οι αλγόριθμοι έχουν μια παράμετρο που μεταβάλλει το επίπεδο της απόδοσης και της χρησιμοποίησης του δικτύου (με το να κάνει τον αλγόριθμο περισσότερο ή λιγότερο επιθετικό), μερικοί αλγόριθμοι προσπαθούν να ρυθμίσουν αυτήν την παράμετρο και να την χρησιμοποιούν για έναν ακριβή υπολογισμό της απόδοσης του δικτύου, ενώ άλλοι δεν αφήνουν αυτή την παράμετρο αμετάβλητη.

➤ Οι διαδικασίες μετρήσεων που χρησιμοποιούνται για τον υπολογισμό του φορτίου του δικτύου διαφέρουν αρκετά μεταξύ τους. Ποικίλουν, από τον υπολογισμό του φορτίου μέσω απλής δειγματοληψίας, έως την εύρεση του εκθετικού μέσου όρου και τον υπολογισμό βασισμένο στο μέσο όρο, αλλά και στη διακύμανση του μετρούμενου φορτίου(measured load).

Επομένως, ο χώρος των αλγορίθμων ελέγχου αποδοχής ροών, βασισμένων σε μετρήσεις που γίνονται στο δίκτυο (measurement-based admission control algorithms) γίνεται όλο και πιο δημοφιλής.

4.2.1.2. Measurement-based admission control algorithms (MBACs)

Σε αυτήν την παράγραφο, εξετάζουμε ένα ευρύ, αλλά όχι πλήρες, δείγμα των υπαρχόντων MBACs. Ο κάθε αλγόριθμος έχει δύο συνιστώσες : μια διαδικασία μετρήσεων η οποία παράγει έναν υπολογισμό του φόρτου του δικτύου, και ένα αλγόριθμο αποφάσεων, ο οποίος χρησιμοποιεί το υπολογιζόμενο φορτίο για να παίρνει αποφάσεις ελέγχου αποδοχής κλήσεων.

a) Measured Sum (MS) και Measured Sum EF (Expedited Forwarding)

Ορίζουμε ως μ το εύρος ζώνης(link bandwidth) της γραμμής, r^a το ποσοστό του εύρους που δεσμεύεται από τη ροή a και \hat{u} το μετρούμενο φορτίο της τωρινής κυκλοφορίας. Τότε ο αλγόριθμος Measured Sum αποδέχεται την ροή a στο δίκτυο που εξετάζουμε αν ισχύει η ακόλουθη συνθήκη : $\hat{u} + r^a < c \cdot \mu$, όπου $0 < c < 1$ και c είναι μια σταθερά που ορίζει τη μέγιστη χρησιμοποίηση που θέλουμε να έχουμε στο δίκτυό μας. Ο ίδιος τύπος ισχύει και για τον αλγόριθμο Measured Sum EF, με τη διαφορά ότι τώρα μετράμε μόνο την EF κίνηση. Όταν η χρησιμοποίηση το δικτύου πλησιάζει το 100%, τότε η διακύμανση στην καθυστέρηση των πακέτων μεγαλώνει και ο αλγόριθμος παίρνει λάθος αποφάσεις αποδοχής. Επομένως με τη χρησιμοποίηση του c , το δίκτυο παραμένει σε καθεστώς επιθυμητής χρησιμοποίησης του διαθέσιμου εύρους ζώνης.

b) Hoeffding Bounds (HB)

Αυτός ο αλγόριθμος υπολογίζει το ισοδύναμο εύρος ζώνης C , βασισμένος σε Hoeffding bounds, των ροών μιας σύνδεσης. Ορίζουμε ως πιθανότητα $C(\epsilon)$ την πιθανότητα το απαιτούμενο εύρος ζώνης από όλες τις ροές να ξεπερνά το ϵ ,

υποθέτοντας ότι οι ροές έχουν μέγιστο ρυθμό μετάδοσης p . Το C δίνεται από την

$$\text{σχέση : } \widehat{C}_H(\widehat{v}, \{p_i\}, \varepsilon) = \widehat{v} + \sqrt{\frac{1}{2} \cdot (\ln(1/\varepsilon) \sum_i (p_i)^2)}, \text{ όπου } \widehat{v} \text{ είναι ο μέσος μετρούμενος}$$

ρυθμός άφιξης της τωρινής κυκλοφορίας. Η ροή a γίνεται αποδεκτή αν ισχύει η ακόλουθη συνθήκη : $\widehat{C}_H + p^a \leq \mu$, όπου p^a είναι ο μέγιστος ρυθμός της ροής a , και μ είναι το εύρος ζώνης της γραμμής. Ο τωρινός μέσος ρυθμός άφιξης ενημερώνεται και γίνεται : $\widehat{v}' = \widehat{v} + p^a$.

Εδώ πρέπει να αναφέρουμε ότι στους παραπάνω αλγόριθμους υποθέτουμε την ύπαρξη κάποιου πρωτοκόλλου σηματοδοσίας (όπως για παράδειγμα το RSVP), το οποίο χρησιμοποιείται από τις ροές για την απαίτηση αποδοχής ποιότητας υπηρεσίας (QoS).

Περιοχή αποδοχής (Acceptance Region) :

Αν θεωρήσουμε ως a και p το μέσο και μέγιστο ρυθμό αντίστοιχα μιας ON/OFF πηγής, τότε το ισοδύναμο εύρος ζώνης (C) της πηγής μπορεί να υπολογιστεί από την

$$\text{ακόλουθη εξίσωση : } C(s) = \frac{1}{s} \cdot \log\left[1 + \frac{a}{p} \cdot (e^{s \cdot p} - 1)\right], \text{ όπου } s > 0. \text{ Τότε μπορούμε να}$$

σχεδιάσουμε μια καμπύλη ισοδύναμου εύρους ζώνης παριστάνοντας τον μέσο ρυθμό στον άξονα x και το ισοδύναμο εύρος ζώνης που προκύπτει στον άξονα y . Ένα γραμμικό όριο μπορεί να υπολογιστεί σε διάφορα σημεία αυτής της καμπύλης σαν την εφαπτομένη στα σημεία αυτά : $c + a \cdot \widehat{v} \leq \mu$, όπου το c μας δείχνει την θέση και το a την κλίση της εφαπτομένης. Αυτό το γραμμικό όριο μπορεί τότε να χρησιμοποιηθεί σαν ένας MBAC. Δύο MBAC, ο καθένας βασισμένος σε μια διαφορετική εφαπτομένη της καμπύλης του ισοδύναμου εύρους ζώνης, παρουσιάζονται παρακάτω :

c) Tangent at peak (TP) :

Ο αλγόριθμος αυτός χρησιμοποιεί την εφαπτομένη στο μέγιστο της καμπύλης του ισοδύναμου εύρους ζώνης, το οποίο υπολογίζεται με χρήση Chernoff Bounds. Εδώ ισχύει : $n \cdot p \cdot (1 - e^{-s \cdot p}) + e^{-s \cdot p} \cdot \widehat{v} \leq \mu$, όπου n είναι ο αριθμός των ροών που έχουν γίνει αποδεκτές. Επομένως μια καινούρια ροή γίνεται αποδεκτή μόνο αν ισχύει η παραπάνω σχέση.

d) Tangent at Origin (TO)

Ο αλγόριθμος αυτός χρησιμοποιεί την εφαπτομένη στο αρχικό σημείο της καμπύλης του ισοδύναμου εύρους ζώνης, το οποίο υπολογίζεται με χρήση Chernoff Bounds. Σε

αυτήν την περίπτωση μια νέα ροή γίνεται αποδεκτή μόνο αν ικανοποιείται η ακόλουθη εξίσωση : $e^{s \cdot p} \cdot \hat{v} \leq \mu$. Και οι δύο παραπάνω αλγόριθμοι χρησιμοποιούν μια διαδικασία μετρήσεων βασισμένη στη δειγματοληψία.

e) Measure CAC (MC)

Ο MBAC αλγόριθμος αυτός βασίζεται στη θεωρία των μεγάλων αποκλίσεων (large deviation theory). Αποδέχεται μια καινούρια ροή αν το άθροισμα του μέγιστου ρυθμού της ροής και του υπολογιζόμενου εύρους ζώνης των χρησιμοποιούμενων ροών είναι μικρότερο από το εύρος ζώνης της γραμμής. Υπολογίζει τον φόρτο της υπάρχουσας κίνησης l (βάση της διαδικασίας αφίξεων, με είσοδο το ζητούμενο ρυθμό απωλειών), και η συνθήκη για την αποδοχή ροής είναι η $p + l \leq C$ όπου p : ο μέγιστος ρυθμός ροής.

f) Αλγόριθμος MBAC με Aggregate Traffic Envelopes (TE)

Ο αλγόριθμος αυτός αναφέρεται σε δίκτυα που υποστηρίζουν πολλές κλάσεις υπηρεσίας και οι οποίες μοιράζονται το διαθέσιμο εύρος ζώνης. Αναπτύσσει μία νέα θεωρητική μέθοδο βασισμένη σε συσσωρευμένη κίνηση όπως περιγράφουμε παρακάτω. Κάνουμε μετρήσεις για την προσέγγιση του προφίλ κίνησης χειρότερης περίπτωσης για κάθε aggregate και κάνουμε χρήση της μέσης τιμής και της απόκλισης του (μαζί με το ζητούμενο ρυθμό απωλειών σαν παράμετρο εισόδου) στον αλγόριθμο απόφασης. Βάση συγκεκριμένων συνθηκών εξετάζεται η αποδοχή ή όχι μιας ροής βάσει ενός schedulability test (εξασφαλίζει ότι δεν θα καθυστερήσει ένα πακέτο πέραν των ορίων του λόγω παραμονής στον buffer), ενός stability test (ο μέσος ρυθμός του aggregate σε ένα χρονικό διάστημα είναι μικρότερος της διαθέσιμης χωρητικότητας) και ενός loss probability test (φράσσει τον αριθμό των απολεσθέντων πακέτων).

Παρατηρώντας τις αποδόσεις των παραπάνω αλγορίθμων σε διάφορες προσομοιώσεις που έχουν πραγματοποιηθεί, βλέπουμε ότι δεν υπάρχουν ουσιαστικές διαφορές, όσον αφορά το ρυθμό απωλειών πακέτων ή τον αριθμό των ροών που γίνονται αποδεκτές από το δίκτυο. Οι πιο απλοί αλγόριθμοι παρουσιάζουν τα ίδια αποτελέσματα όσον αφορά την απόδοση του δικτύου με τους πολύπλοκους αλγορίθμους που βασίζονται σε σύνθετες μαθηματικές σχέσεις. Επομένως, θεωρούμε ότι για να επιτύχουμε καλύτερα αποτελέσματα πρέπει να υλοποιήσουμε έναν αλγόριθμο που να χρησιμοποιεί παρόμοιους μηχανισμούς μετρήσεων με τους παραπάνω αλγορίθμους,

αλλά να μας παρέχει περισσότερη πληροφορία για τις ροές που βρίσκονται αυτή τη στιγμή στο δίκτυο, οπότε και παρουσιάζουμε τον παρακάτω αλγόριθμο.

g) Αλγόριθμος MBAC με χρωματισμό πακέτων (Color MBAC)

Στον αλγόριθμο αυτό διαιρούμε κάθε ροή σε ένα αριθμό στρώματων. Ανάλογα με τον τωρινό και το μέσο ρυθμό μετάδοσης της συγκεκριμένης ροής, κάθε πακέτο μαρκάρεται (η «χρωματίζεται») από το κόμβο εισόδου του στο δίκτυο με μία ετικέτα που δηλώνει το στρώμα στο οποίο ανήκει (ή το «χρώμα»).

Τα πακέτα χρωματίζονται στα άκρα του δικτύου, ενώ ο έλεγχος για αποδοχή ή απόρριψη των πακέτων γίνεται στους εσωτερικούς δρομολογητές. Όταν μια ροή φτάνει στα άκρα του δικτύου, ο ρυθμός της υπολογίζεται από μια σχέση που βασίζεται στους χρόνους άφιξης των πακέτων. Ο ακραίος δρομολογητής τότε, διαιρεί τη ροή σε στρώματα, αντιστοιχώντας σε κάθε στρώμα έναν αριθμό, τον οποίο εμείς αποκαλούμε «χρώμα». Τα στρώματα με τα διάφορα χρώματα έχουν ως σκοπό να σημειώνουν την διαφορά ανάμεσα στον τωρινό ρυθμό της ροής και στο μέσο ρυθμό της. Τα στρώματα χρωμάτων παρέχουν μία δομή για ελεγχόμενη απόρριψη πακέτων στο δίκτυό μας στην περίπτωση που έχουμε συμφόρηση. Εσωτερικά στο δίκτυο, πολυπλέκονται διάφορες ροές. Δεδομένου ότι οι εσωτερικοί δρομολογητές (core routers) δεν κάνουν έλεγχο ανά ροή, δεν μπορούν να διακρίνουν πακέτα ανά ροή. Αυτοί οι δρομολογητές επιτυγχάνουν έλεγχο απόδοσης βασισμένοι σε MBAC μηχανισμούς. Μετράνε τον ρυθμό των πακέτων διαφορετικών χρωμάτων, καθώς και τον συνολικό ρυθμό μετάδοσης. Όταν η συνολική κίνηση ξεπερνά το ποσοστό που έχουμε ορίσει ως threshold, τότε οι δρομολογητές αυτοί απορρίπτουν πακέτα προκειμένου να μειώσουν το φορτίο του δικτύου. Οι απορρίψεις ξεκινούν με πακέτα των οποίων το χρώμα αντιστοιχεί σε υψηλή τιμή.

Υπολογισμός του ρυθμού άφιξης πακέτων μιας ροής: Ο υπολογιζόμενος ρυθμός της

ροής i βρίσκεται από τον τύπο:
$$R_i^{new} = (1 - a) * \frac{l_i^k}{T_i^k} + e^{\left(\frac{-T_i^k}{K}\right)} \cdot R_i^{old}$$
, όπου

t_i^k είναι ο χρόνος άφιξης του k -ου πακέτου της i ροής, l_i^k είναι το μέγεθος του k -ου πακέτου της i ροής, $T_i^k = t_i^k - t_i^{k-1}$ είναι ο χρόνος που μεσολαβεί ανάμεσα στις αφίξεις δύο πακέτων, και K είναι μια σταθερά (100-500 msec). Στην περίπτωση που έχουμε ροές με σταθερό μέγεθος πακέτων τότε το a μπορεί να είναι απλά μια σταθερά

($0 < \alpha < 1$), διαφορετικά για καλύτερη σύγκλιση μπορούμε να χρησιμοποιήσουμε τον εκθετικό όρο $a = e^{-\frac{T_i^k}{K}}$. Και αυτό γιατί με τον όρο $e^{-\frac{T_i^k}{K}}$, ο υπολογιζόμενος ρυθμός θα συγκλίνει ασυμπτωτικά στον πραγματικό ρυθμό, με αποτέλεσμα να μπορούμε να φράξουμε το ποσοστό της υπηρεσίας που θα μείνει αχρησιμοποίητη.

Σημαντικό ρόλο στην όλη διαδικασία διαδραματίζει και η επιλογή του K . Ενώ μία μικρή τιμή του K αυξάνει την ανταπόκριση του συστήματος στις απότομες μεταβολές του ρυθμού των ροών, ένα μεγαλύτερο K φιλτράρει καλύτερα το θόρυβο και κάνει το σύστημα πιο σταθερό. Ακόμη, το K θα πρέπει να είναι τόσο μεγάλο ώστε ο εκτιμημένος ρυθμός, υπολογισμένος στα άκρα του δικτύου, να παραμένει ακριβής ακόμη και όταν ένα πακέτο έχει περάσει από πολλές συνδέσεις (links). Και αυτό γιατί η διαφορετική καθυστέρηση που υφίσταται κάθε πακέτο (delay-jitter) αλλάζει τον στιγμιαίο ρυθμό άφιξης των πακέτων, κάτι που μπορεί να οδηγήσει σε μία αυξανόμενη αντίφαση ανάμεσα στον υπολογιζόμενο ρυθμό και στον πραγματικό ρυθμό. Για να εξουδετερώσουμε αυτό το αποτέλεσμα, το K πρέπει να είναι μία τάξη μεγέθους μεγαλύτερο από την διαφορά στην καθυστέρηση των πακέτων (delay-jitter) που υφίσταται μια ροή. Επίσης, το K δεν πρέπει να είναι μεγαλύτερο από τη μέση διάρκεια μιας ροής. Βασισμένοι στους παραπάνω περιορισμούς, μια κατάλληλη τιμή για το K θα ήταν αυτή μεταξύ των 100 και 500ms.

Σε κάθε πακέτο αντιστοιχίζουμε ένα χρώμα με βάση μια πιθανότητα, η οποία αποφασίζεται με βάση των τον τωρινό ρυθμό της ροής.

Απόδοση Χρωμάτων (Color Assignment)

➤ Αν ο τωρινός ρυθμός της ροής R_t είναι μεγαλύτερος από τον μέσο όρο του ρυθμού της ροής R_{aver} , $R_t \geq R_{aver} = [R_t - y]$, όπου y είναι μια θετική τιμή, τότε τα πακέτα που βρίσκονται πάνω από τον μέσο όρο μαρκάρονται ως κόκκινα, ενώ όλα τα υπόλοιπα πακέτα μαρκάρονται ως μπλε. Ισχύει :

$$Pr_{red} = \frac{y}{R_t} = \frac{R_t - R_{aver}}{R_t}$$

$$Pr_{blue} = 1 - Pr_{red} = 1 - \frac{y}{R_t} = 1 - \frac{R_t - R_{aver}}{R_t} = \frac{R_{aver}}{R_t}$$

➤ Αν ο τωρινός ρυθμός της ροής R_t είναι μικρότερος από τον μέσο όρο του ρυθμού της ροής R_{aver} , $R_t \leq R_{aver} = [R_{aver} - x]$, όπου x είναι μια θετική τιμή, τότε τα πακέτα που βρίσκονται πάνω από τον R_t μαρκάρονται ως πράσινα, ενώ όλα τα υπόλοιπα πακέτα μαρκάρονται ως μπλε. Ισχύει :

$$\Pr_{green} = \frac{x}{R_t} = \frac{R_{aver} - R_t}{R_t}$$

$$\Pr_{blue} = 1 - \Pr_{green} = 1 - \frac{x}{R_t} = 1 - \frac{R_{aver} - R_t}{R_t} = \frac{2 \cdot R_t - R_{aver}}{R_t}$$

Μετρήσεις βασισμένες στον Color MBAC:

Ισχύει ότι:

$$\begin{aligned} R_{measured} &= \sum(\text{flows_with_red_packets}) + \sum(\text{flows_with_green_packets}) = \\ &= \sum(R_{aver,red} + y) + \sum(R_{aver,green} - x) = \\ &= \sum(R_{aver,red} + R_{aver,blue} + R_{aver,green}) + \sum y - \sum x \Rightarrow \\ &\Rightarrow R_{reserved} = R_{measured} - \sum y + \sum x \end{aligned}$$

5. Πρόβλημα

Το ζήτημα που αντιμετωπίζεται στην εργασία αυτή είναι η εύρεση ενός βέλτιστου μοντέλου ελέγχου αποδοχής ροών (MBAC Model), που εφαρμόζεται σε ένα IP δίκτυο, προκειμένου να μπορέσουμε να δώσουμε στον τελικό χρήστη, όσο το δυνατόν καλύτερη ποιότητα υπηρεσίας με βάση τα χαρακτηριστικά που αυτός ζητάει. Απώτερος σκοπός είναι:

- η κατανόηση της λειτουργίας των μηχανισμών που εκτελούνται στα πειράματα,
- η σύγκριση των αποτελεσμάτων που πήραμε από το μοντέλο που αναπτύξαμε με αντίστοιχα μοντέλα που προυπήρχαν,
- η εξαγωγή χρήσιμων συμπερασμάτων σχετικά με το ποια χαρακτηριστικά της κίνησης είναι αυτά που επηρεάζουν περισσότερο την απόδοση ενός μοντέλου ελέγχου αποδοχής ροών.

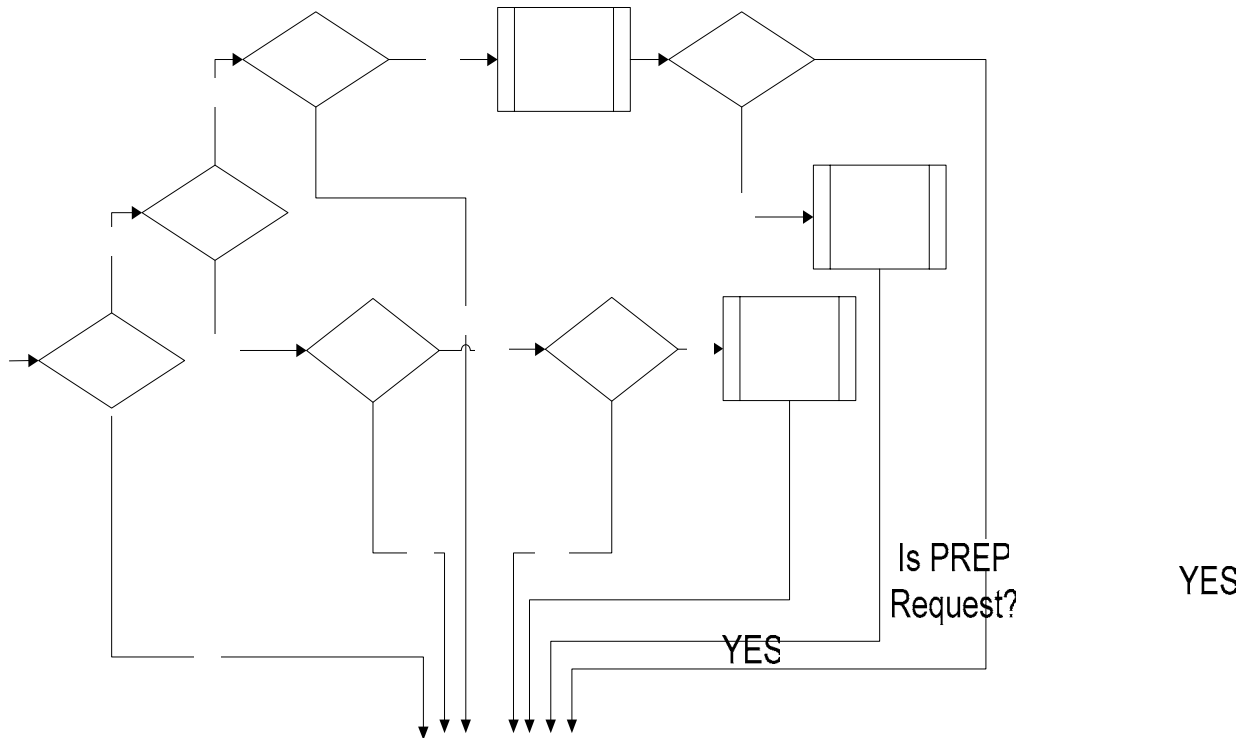
5.1. Προσέγγιση – Αντιμετώπιση του προβλήματος

Όπως έχουμε αναφέρει προηγουμένως, το μοντέλο MBAC, είναι ένα μοντέλο παροχής Ποιότητας Υπηρεσίας που βασίζεται κυρίως στην Αρχιτεκτονική Ενοποιημένων Υπηρεσιών. Σύμφωνα με αυτό, όλοι οι δρομολογητές του δικτύου είναι υποχρεωμένοι να κρατούν πληροφορίες για κάθε ροή που δημιουργείται και παραμένει ενεργή, και παράλληλα να ελέγχουν αν η κίνηση της εκάστοτε ροής είναι σύμμορφη με το προφίλ κίνησης που έχει οριστεί για αυτήν. Επομένως, έχουμε αυξημένη καθυστέρηση των πακέτων καθώς και υψηλή πολυπλοκότητα των δρομολογητών.

Λαμβάνοντας υπόψη τα παραπάνω, προτείνεται μία νέα τοπολογία δικτύου, η οποία συνδυάζει τα χαρακτηριστικά των Αρχιτεκτονικών Ενοποιημένων και Διαφοροποιημένων Υπηρεσιών. Στην περίπτωση αυτή, οι μόνοι δρομολογητές, οι οποίοι κρατάνε πληροφορίες ανά ροή είναι οι ακραίοι δρομολογητές του δικτύου (edge routers), ενώ οι εσωτερικοί δρομολογητές (core routers), απλά προωθούν τα πακέτα. Ο έλεγχος για την αποδοχή ή όχι μιας νέας ροής γίνεται στους εσωτερικούς δρομολογητές, με βάση όμως τις πληροφορίες που έχουν για τη συνολική κίνηση της γραμμής τη στιγμή που έρχεται η καινούρια ροή. Πριν την είσοδο των πακέτων στους

ακραίους δρομολογητές επιτελείται χρωματισμός τους, με βάση την απόδοση χρωμάτων του αλγορίθμου Color MBAC.

Στο παρακάτω σχήμα παρουσιάζεται η διαδικασία με την οποία υλοποιείται ο έλεγχος αποδοχής ροών, βασισμένος στον χρωματισμό πακέτων (Color MBAC).



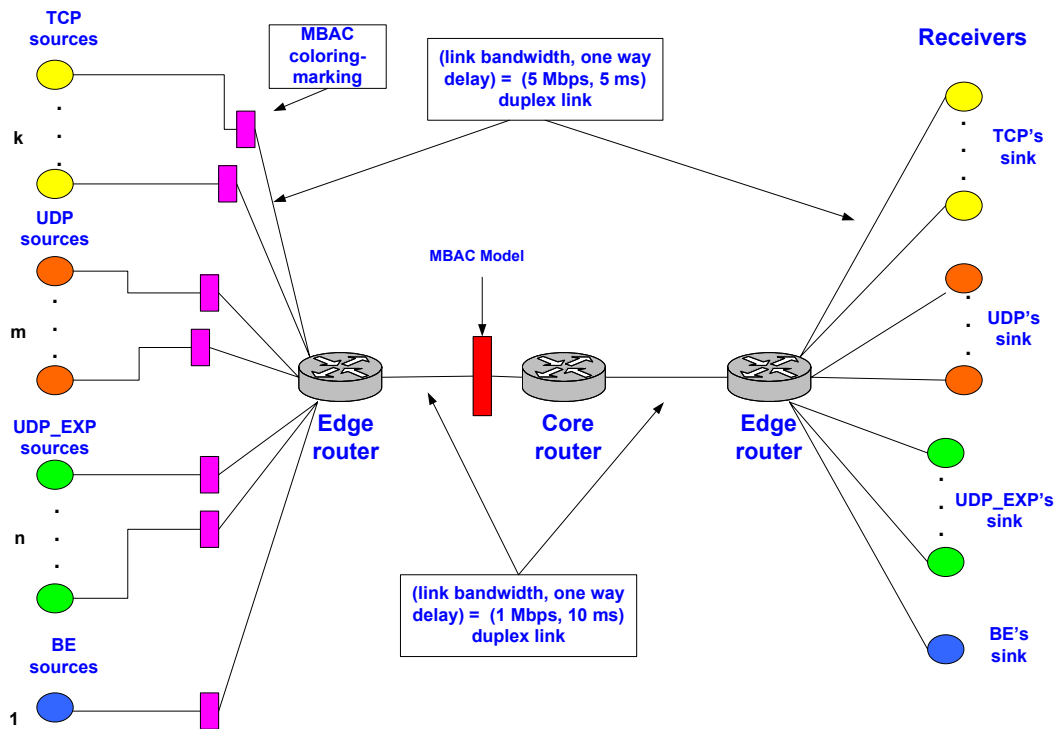
Εκτελείται η ακόλουθη διαδικασία:

- έλεγχος ότι ο αλγόριθμος Color MBAC είναι ενεργοποιημένος
- πρόκειται για μήνυμα σηματοδότησης {PREP (Path Resource Estimation Protocol) message}
- πρόκειται για αίτηση για μια νέα ροή
- εκτέλεση του αλγορίθμου Color MBAC
- επιτυχές αποτέλεσμα → αποδοχή ροής

Αν το αποτέλεσμα δεν είναι επιτυχές, τότε προσθέτουμε τον PREP header, ότι ο έλεγχος αποδοχής της ροής έδωσε αρνητικό αποτέλεσμα. Αν πάλι το μήνυμα σηματοδότησης, δεν περιείχε αίτηση για μια νέα ροή, τότε αυτό απλά προωθείται.

5.2. Τοπολογία του δικτύου

Η τοπολογία του δικτύου που χρησιμοποιούμε για να κάνουμε τις προσομοιώσεις φαίνεται στο παρακάτω σχήμα:



Η τοπολογία αυτή έχει ως στόχο την μελέτη της κίνησης γραμμών κορμού, δηλαδή γραμμών που μεταφέρουν κίνηση που προκύπτει από την συνάθροιση των ροών (aggregate traffic) που παράγουν οι πηγές.

5.3. Χαρακτηριστικά των πηγών κίνησης (traffic sources)

Η κίνηση που διοχετεύεται προς το δίκτυο ανήκει στις παρακάτω δύο κατηγορίες:

- Η κίνηση υψηλής προτεραιότητας που ονομάζεται Gold και δημιουργήθηκε κατά τέτοιο τρόπο ώστε να προσομοιώνει εφαρμογές που έχουν αυστηρές απαιτήσεις σε μετρικές ποιότητας προκειμένου να εξυπηρετηθούν αποτελεσματικά (στην περίπτωσή μας αποτελεί το 80% της συνολικής κίνησης).

- Η κίνηση συνηθισμένης προτεραιότητας, που αναφέρεται ως Best Effort (BE), η οποία έχει τα χαρακτηριστικά της best effort IP κίνησης (στην περίπτωσή μας αποτελεί το 20% της συνολικής κίνησης).

Οι πηγές κίνησης που χρησιμοποιούμε στις προσομοιώσεις μας είναι οι παρακάτω:

- Πηγές TCP: Το είδος αυτό της κίνησης εισέρχεται για να κάνει πιο ρεαλιστική τη συνολικά μεταφερόμενη κίνηση από τις γραμμές κορμού. Η TCP κίνηση κάθε πηγής μπορεί να είναι CBR (κάθε ροή που δημιουργείται μεταδίδει με ένα σταθερό ρυθμό, αν δε υπάρχει συμφόρηση), ή EXP (κάθε ροή που δημιουργείται μεταδίδει με έναν ρυθμό που μεταβάλλεται εκθετικά γύρω από μια μέση τιμή, αν δεν υπάρχει συμφόρηση).
- Πηγές UDP και UDP_EXP: Στην περίπτωση αυτή έχουμε συνεχή παροχή κίνησης προς το δίκτυο, ανεξάρτητα από την κατάσταση στην οποία βρίσκονται οι γραμμές κορμού, σχετικά με την χρησιμοποίησή τους (link utilization) και τον ρυθμό απωλειών πακέτων (packet loss rate). Οι πηγές UDP μεταδίδουν με σταθερό (CBR) ή μεταβλητό (VBR) ρυθμό, ενώ οι πηγές UDP_EXP μεταδίδουν με έναν ρυθμό που μεταβάλλεται εκθετικά γύρω από μια μέση τιμή.
- Πηγές BE: Οι πηγές αυτές παράγουν κίνηση χαμηλής προτεραιότητας, δηλαδή κίνηση που θα μεταδοθεί μόνο αν οι γραμμές δεν είναι συμφορημένες. Η χρησιμοποίησή τους όμως είναι απαραίτητη, διότι μας δίνουν την δυνατότητα να πραγματοποιούμε προσομοιώσεις κάτω από καθεστώς υψηλής χρησιμοποίησης του δικτύου.

6. Προσομοιώσεις και αποτελέσματα

Στη συνέχεια παρουσιάζονται οι προσομοιώσεις που πραγματοποιήθηκαν με το ns(network simulator), στην τοπολογία δικτύου που αναφέρθηκε παραπάνω. Αρχικά παρουσιάζουμε κάποιες προσομοιώσεις που έγιναν χωρίς την εφαρμογή του MBAC μοντέλου και σχολιάζουμε τα αποτελέσματα που παίρνουμε.

6.1. Προσομοιώσεις χωρίς την εφαρμογή του MBAC μοντέλου

6.1.1. Χρησιμοποίηση TCP πηγών

Στην προσομοίωση αυτή έχουμε κίνηση που παράγεται από 17 TCP πηγές, με τα χαρακτηριστικά που φαίνονται στον παρακάτω πίνακα:

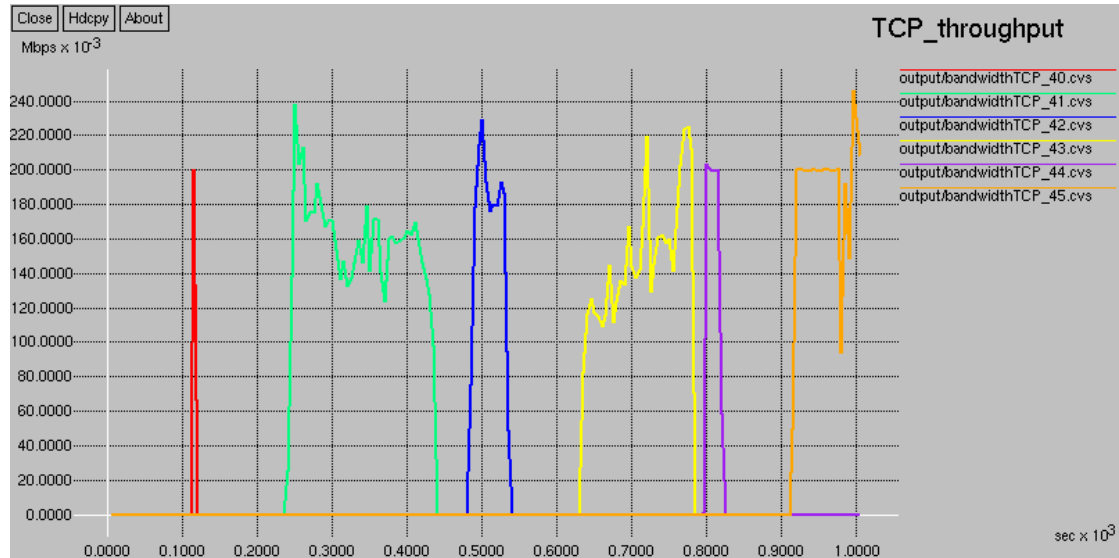
TCP πηγές	17	Link bandwidth	2 Mbps
Αριθμός ροών ανά πηγή	15	Link one way delay	10 ms
TCP Rate	200 Kbps(CBR)	Initialization period	200 sec
TCP packet size	460 bytes	Time of simulation	1000 sec

Εκτελώντας το παραπάνω πείραμα πήραμε τα εξής αποτελέσματα,

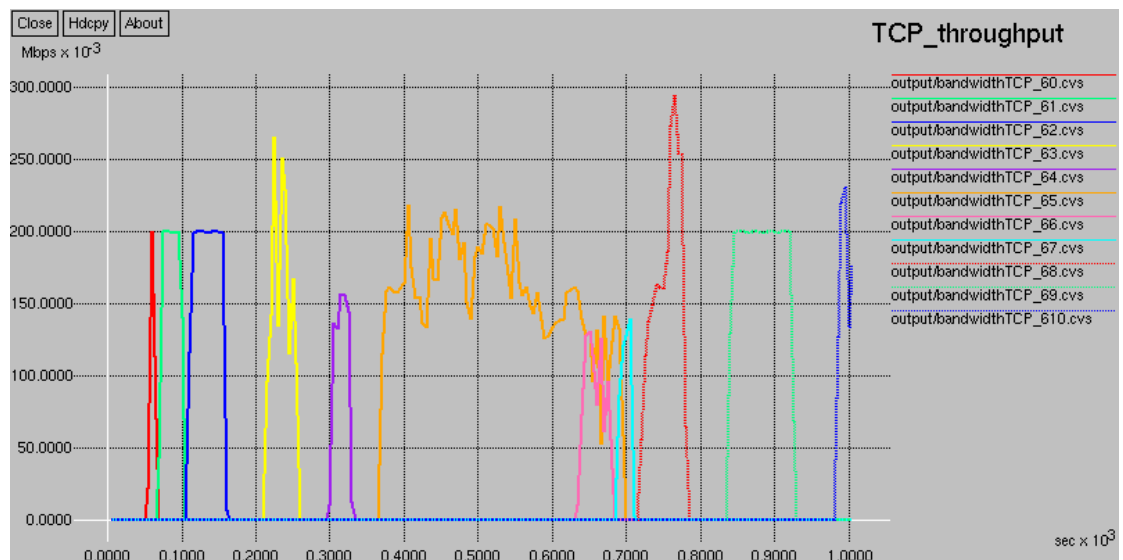
Link Utilisation	78%	Bad connections	50
Excellent Connections	39	Worst connections	8
Good Connections	15	Total number of packets	855137

όπου ως excellent connections, good connections, bad connections και worst connections, ορίζουμε τις συνδέσεις εκείνες όπου έχουν ποσοστό απωλειών πακέτων στα διαστήματα (0, 0,01]%, (0,01, 1]%, (1, 3]%, και (3, 100]%, αντίστοιχα. Επιπλέον, παρακάτω παρατίθενται τα διαγράμματα της απόδοσης της γραμμής και δύο ενδεικτικών TCP ροών συναρτήσει του χρόνου, καθώς και το διάγραμμα των ενεργών ροών συναρτήσει του χρόνου:

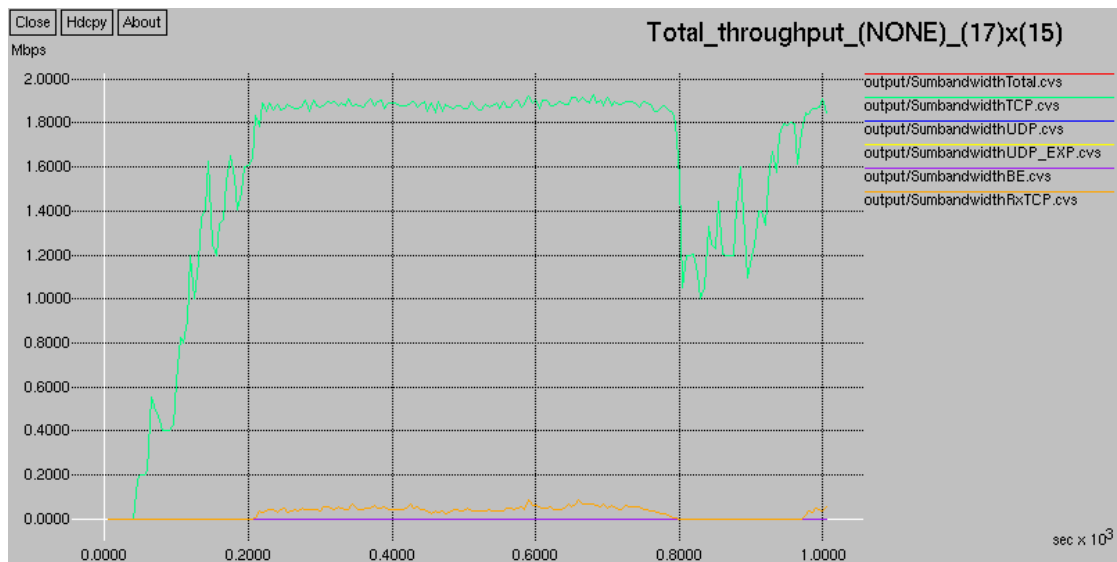
Διάγραμμα απόδοσης (throughput) TCP ροής:



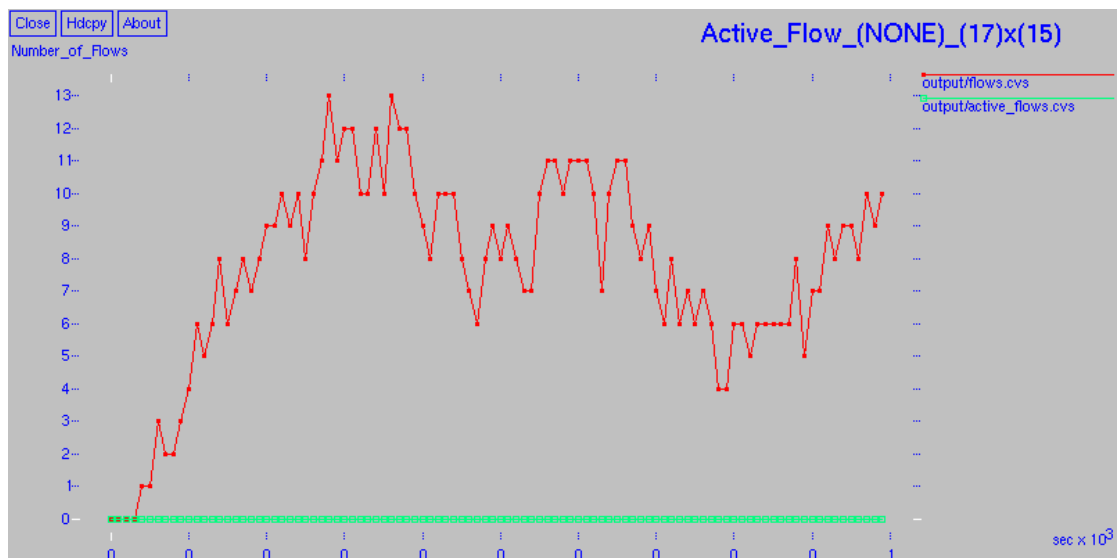
Διάγραμμα απόδοσης (throughput) TCP ροής:



Διάγραμμα απόδοσης (throughput) όλων των ροών:



Διάγραμμα των ενεργών ροών (active flows):



Τα παραπάνω γραφήματα, επιβεβαιώνουν τα αποτελέσματα του προηγούμενου πίνακα σχετικά με τις απώλειες πακέτων. Παρατηρούμε ότι οι TCP ροές που δημιουργούνται, δεν καταφέρνουν να μεταδώσουν με τον ρυθμό που τους αναλογεί. Και αυτό γιατί ανιχνεύουν συμφόρηση στο δίκτυο, με αποτέλεσμα να μεταβάλλουν ανάλογα και το παράθυρο με το οποίο στέλνουν πακέτα (σε αυτό το γεγονός οφείλονται οι αυξομειώσεις στα γραφήματα των TCP ροών). Οποιαδήποτε ροή δημιουργείται, προσπαθεί να μεταδώσει πακέτα, ανεξάρτητα από την κατάσταση της γραμμής, αφού δεν εφαρμόζεται έλεγχος αποδοχής ροών. Στο 3^ο γράφημα παρουσιάζεται η συνολική απόδοση της γραμμής (total throughput). Παρατηρούμε, ότι μετά την αρχικοποίηση, στο δίκτυο παρουσιάζεται συμφόρηση καθώς και επαναμετάδοση σημαντικού ποσοστού πακέτων.

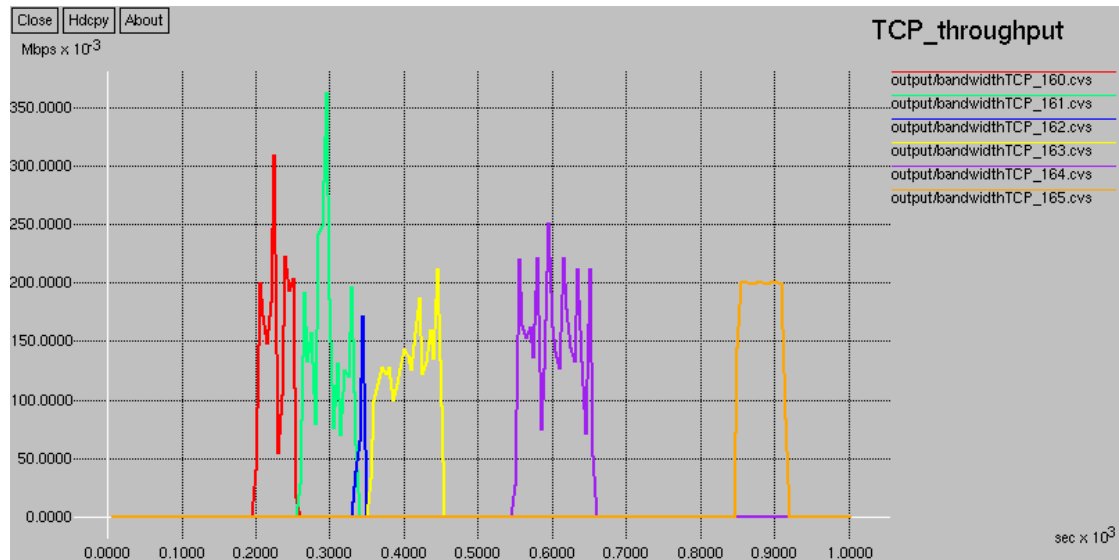
6.1.2. Χρησιμοποίηση TCP και BE πηγών

Στην περίπτωση αυτή κάνουμε την ίδια προσομοίωση με την προηγούμενη, με την διαφορά ότι χρησιμοποιούμε και μία BE πηγή με ρυθμό μετάδοσης 2.3 Mbps. Εκτελώντας το παραπάνω πείραμα πήραμε τα εξής αποτελέσματα:

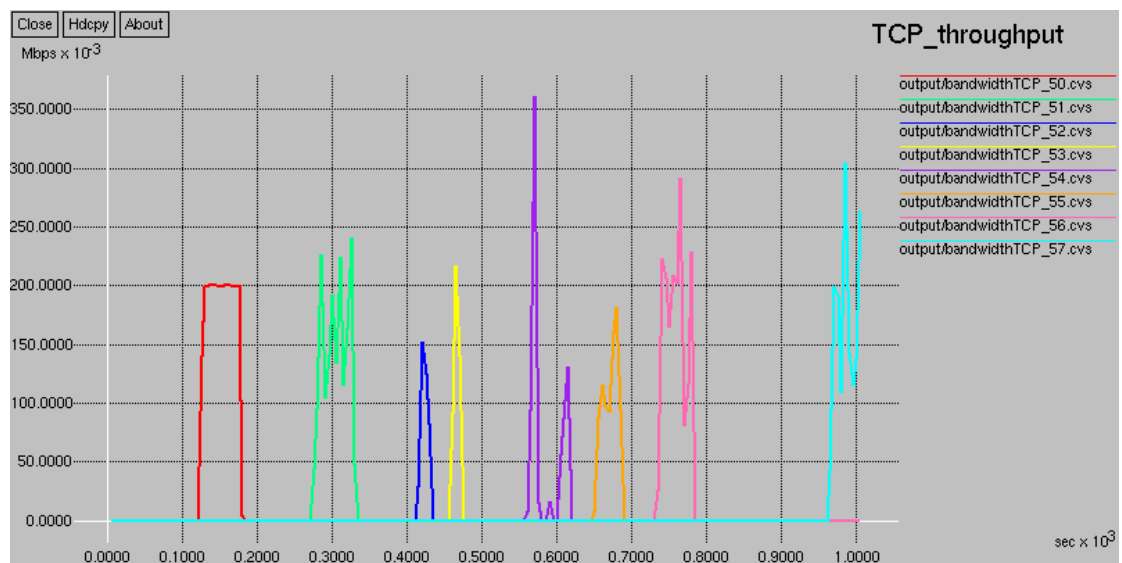
Link Utilisation	93,11	Bad connections	52
Excellent Connections	38	Worst connections	5
Good Connections	17	Total number of packets	1237914

Παρατηρούμε, ότι η κατάσταση σχετικά με τις συνδέσεις που δημιουργούνται χειροτερεύει ελαφρώς, κάτι που είναι λογικό αφού υπάρχει επιπλέον κίνηση στο δίκτυο. Επιπλέον, λόγω της συνεχούς μετάδοσης πακέτων, η χρησιμοποίηση της γραμμής ανεβαίνει αισθητά. Παρακάτω παρατίθενται τα διαγράμματα της απόδοσης της γραμμής, της BE κίνησης και δύο ενδεικτικών TCP ροών συναρτήσει του χρόνου, καθώς και το διάγραμμα των ενεργών ροών συναρτήσει του χρόνου:

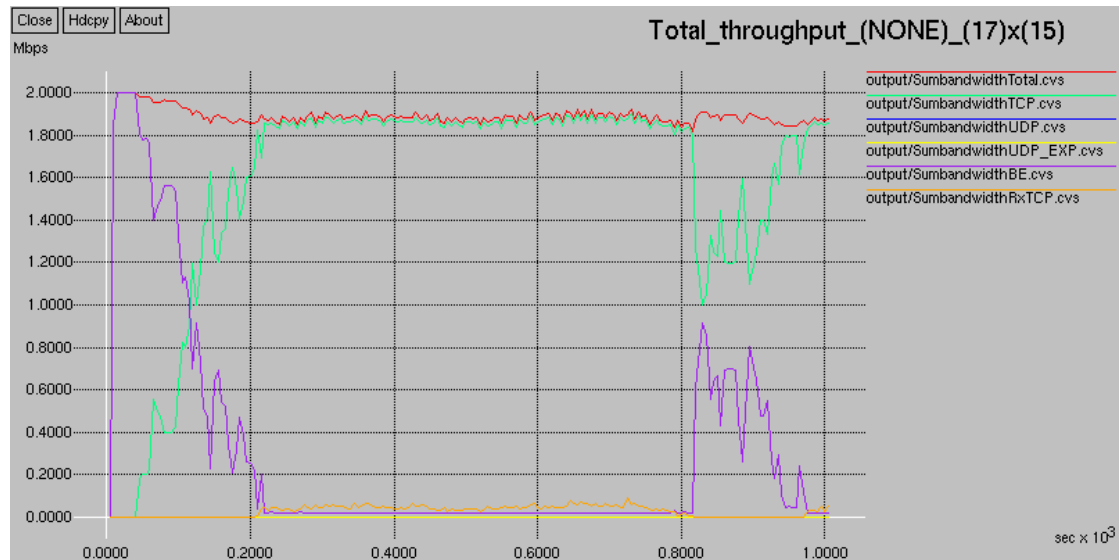
Διάγραμμα απόδοσης (throughput) TCP ροής:



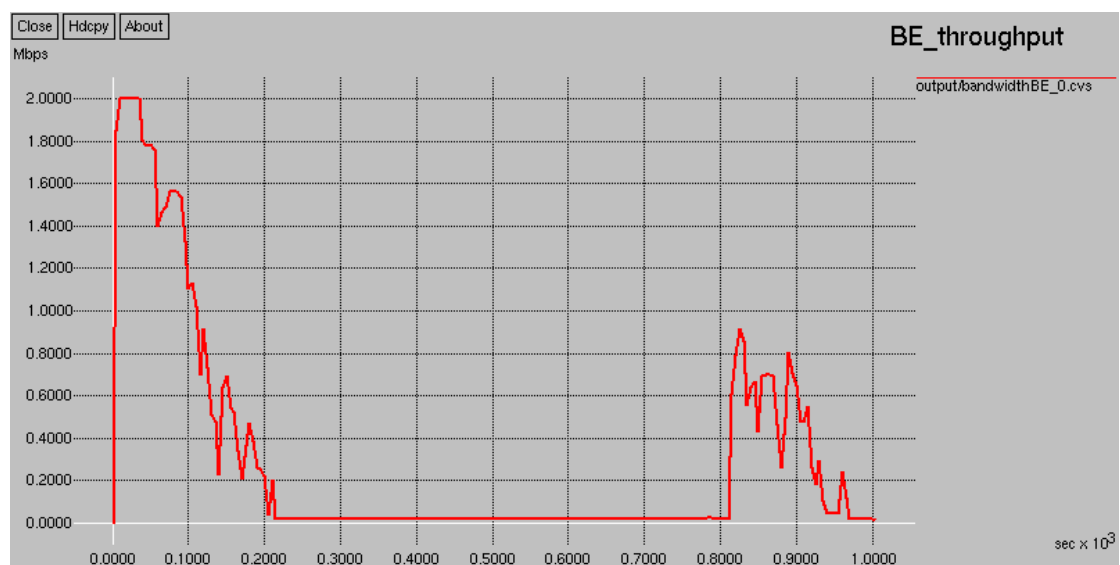
Διάγραμμα απόδοσης (throughput) TCP ροής:



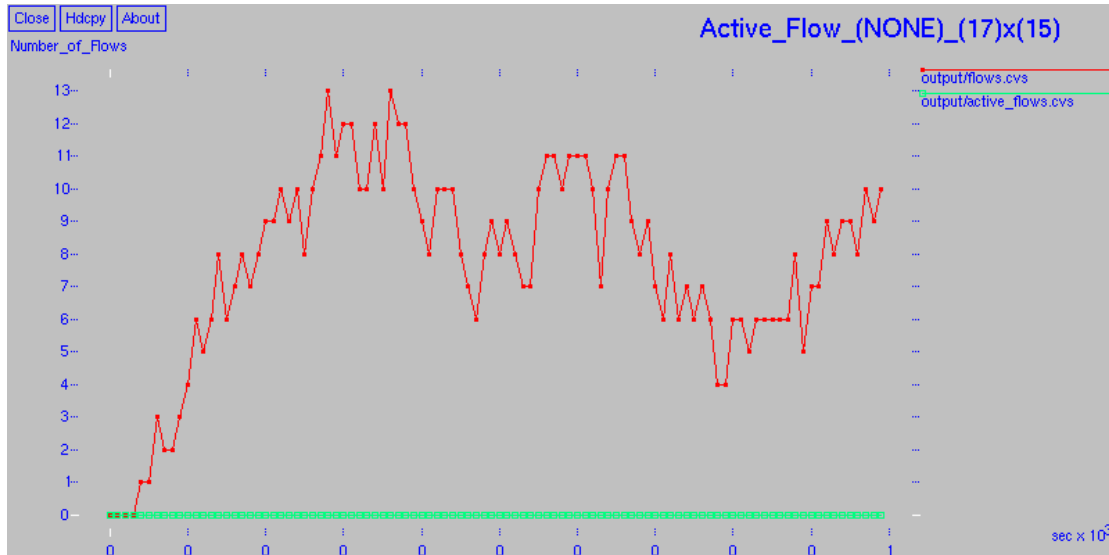
Διάγραμμα απόδοσης (throughput) όλων των ροών:



Διάγραμμα απόδοσης (throughput) της BE κίνησης:



Διάγραμμα των ενεργών ροών (active flows):



Και σε αυτήν την περίπτωση, τα συμπεράσματα συμπίπτουν με την προηγούμενη, με την διαφορά ότι, η BE κίνηση καλύπτει το αχρησιμοποίητο εύρος ζώνης της γραμμής, που αφήνουν οι TCP ροές.

6.1.3. Χρησιμοποίηση TCP, UDP και BE πηγών

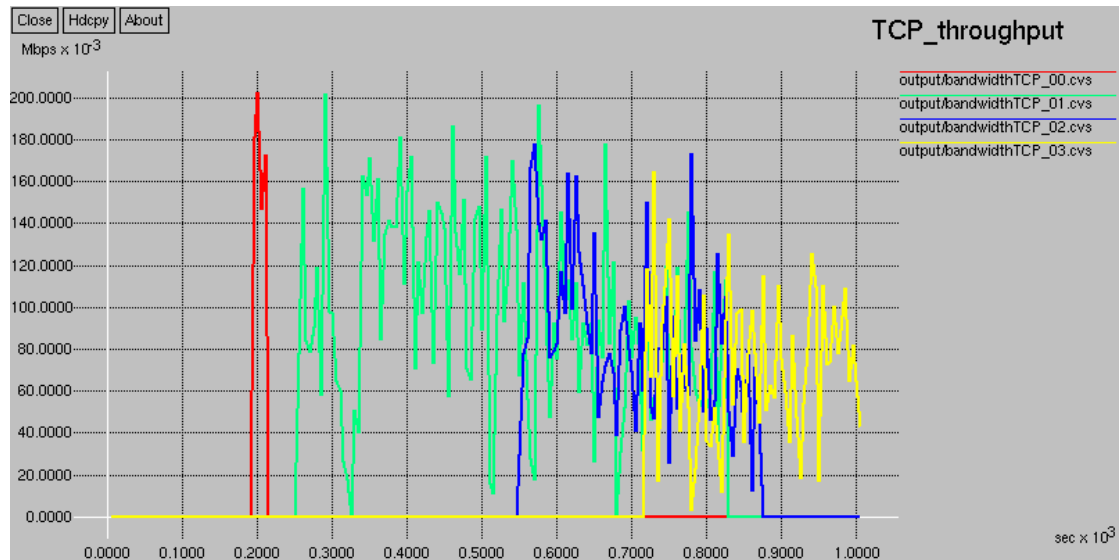
Στην περίπτωση αυτή κάνουμε την ίδια προσομοίωση με την προηγούμενη, με την διαφορά ότι χρησιμοποιούμε επιπλέον 2 UDP πηγές με ρυθμό μετάδοσης 150 Kbps έκαστη. Εκτελώντας το παραπάνω πείραμα πήραμε τα εξής αποτελέσματα;

Link Utilisation	95,63	Bad connections	14
Excellent Connections	13	Worst connections	82
Good Connections	3	Total number of packets	1355278

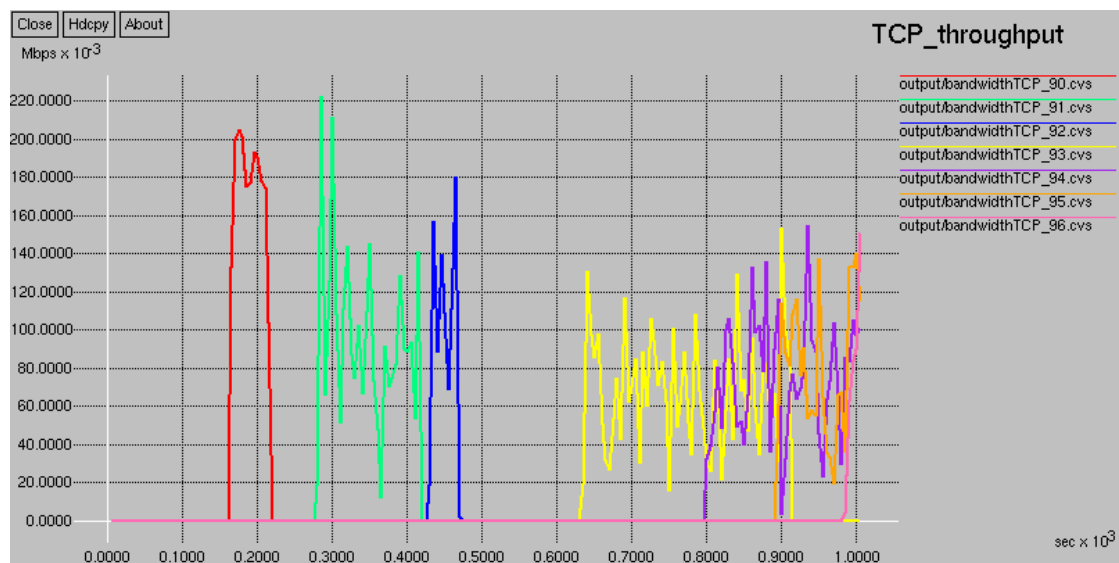
Παρατηρούμε, ότι σε αυτήν την περίπτωση, η κατάσταση με τις συνδέσεις που δημιουργούνται χειροτερεύει δραματικά. Το αίτιο για αυτά τα αποτελέσματα, είναι η χρησιμοποίηση των UDP ροών, που μεταδίδουν συνεχώς με τον καθορισμένο ρυθμό τους, χωρίς να ενδιαφέρονται για το αν υπάρχει συμφόρηση στο δίκτυο. Επιπλέον,

όλες οι TCP ροές που δημιουργούνται προσπαθούν να μεταδώσουν πακέτα, ενώ όταν υπάρχει διαθέσιμο εύρος ζώνης, μεταδίδει και η BE ροή. Παρακάτω παρατίθενται τα διαγράμματα της απόδοσης της γραμμής, της BE κίνησης, των UDP ροών και δύο ενδεικτικών TCP ροών συναρτήσει του χρόνου, καθώς και το διάγραμμα των ενεργών ροών συναρτήσει του χρόνου:

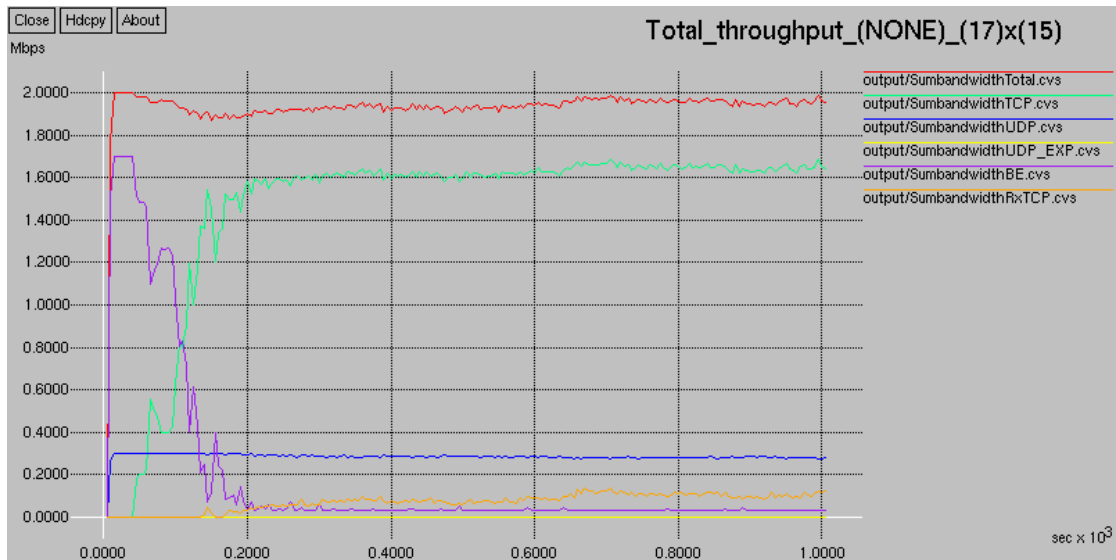
Διάγραμμα απόδοσης (throughput) TCP ροής:



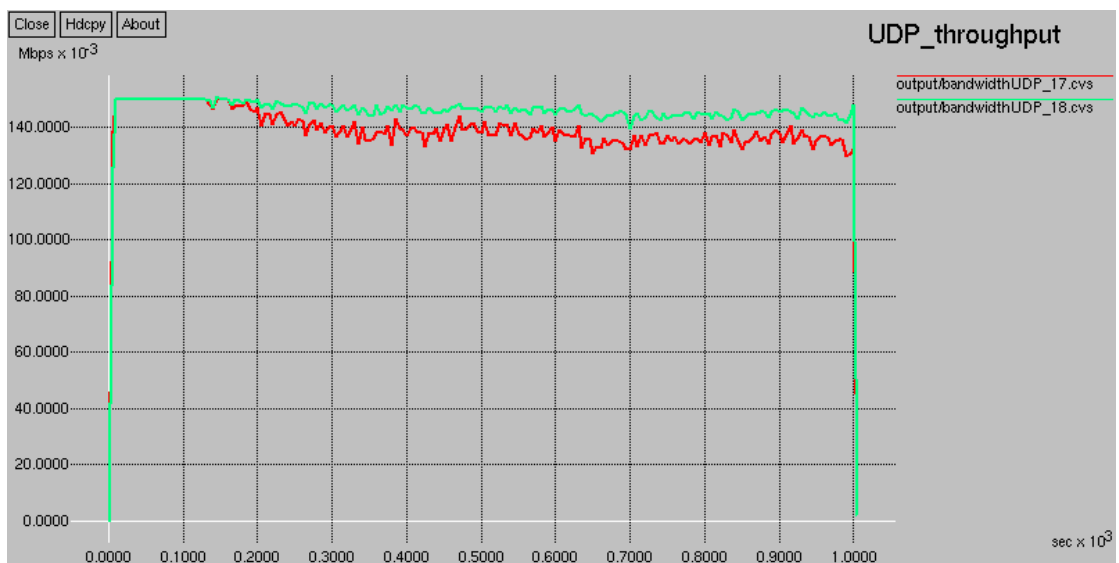
Διάγραμμα απόδοσης (throughput) TCP ροής:



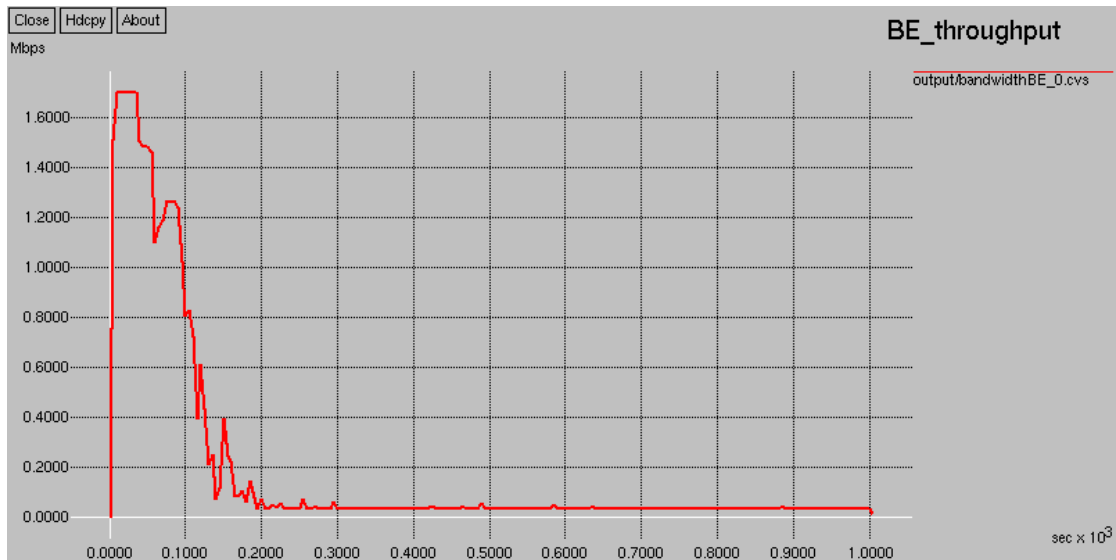
Διάγραμμα απόδοσης (throughput) όλων των ροών:



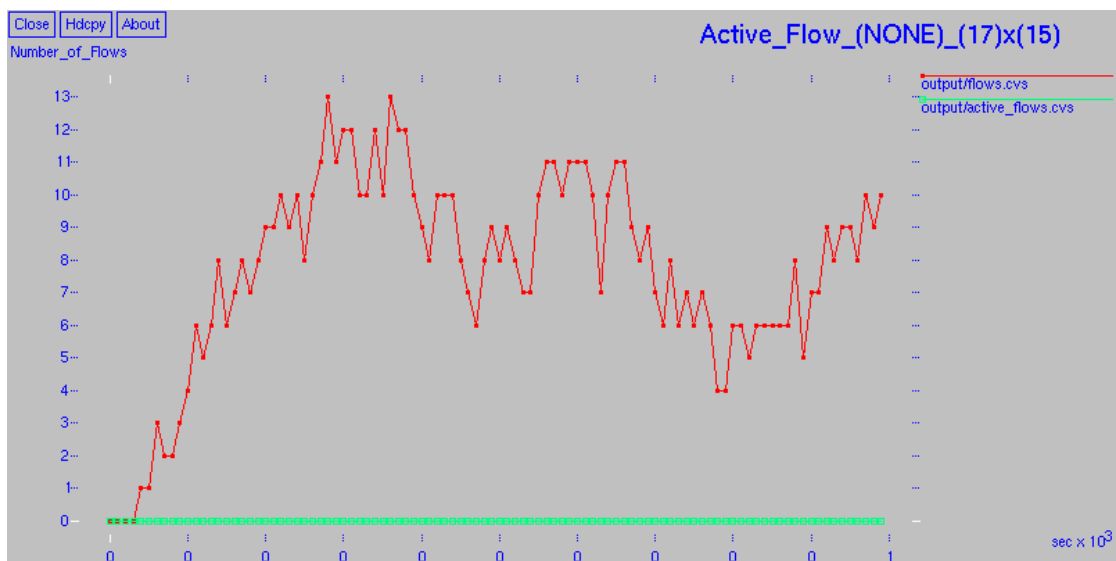
Διάγραμμα απόδοσης (throughput) όλων των UDP ροών:



Διάγραμμα απόδοσης (throughput) της BE κίνησης:



Διάγραμμα των ενεργών ροών (active flows):



Παρατηρούμε, ότι οι μεταβολές στον ρυθμό μετάδοσης των TCP πηγών είναι περισσότερες και πιο έντονες, κάτι που είναι λογικό, αφού 0,3 Mbps της γραμμής καταλαμβάνονται επί μονίμου βάσεως από τις UDP πηγές. Ακόμη, αρκετές TCP πηγές μεταδίδουν σε ρυθμό αισθητά μικρότερο από τον προκαθορισμένο. ΒΕ κίνηση, υπάρχει μόνο στο πρώτο διάστημα, όπου δεν έχουν ενεργοποιηθεί αρκετές TCP ροές. Επομένως, από τα τρία παραπάνω πειράματα, εξάγουμε το συμπέρασμα ότι είναι αναγκαία η εισαγωγή ενός μοντέλου ελέγχου αποδοχής ροών, έτσι ώστε, όταν υπάρχει συμφόρηση, οι νέες ροές να μην γίνονται αποδεκτές. Με αυτό τον τρόπο θα υπάρχει η δυνατότητα παροχής αξιόλογης ποιότητας υπηρεσίας στις υπάρχουσες ροές, κάτι το οποίο θα οδηγήσει σε εξομάλυνση της συμφόρησης και θα δώσει τη δυνατότητα στις καινούριες ροές να γίνουν αποδεκτές.

6.2. 1η Προσομοίωση με εφαρμογή του MBAC μοντέλου

Στις επόμενες προσομοιώσεις εφαρμόζουμε έλεγχο αποδοχής ροών με τον αλγόριθμο Color MBAC. Σε κάθε ένα από τα πειράματα, θεωρούμε ότι έχουμε ως εισόδους τα παρακάτω στοιχεία:

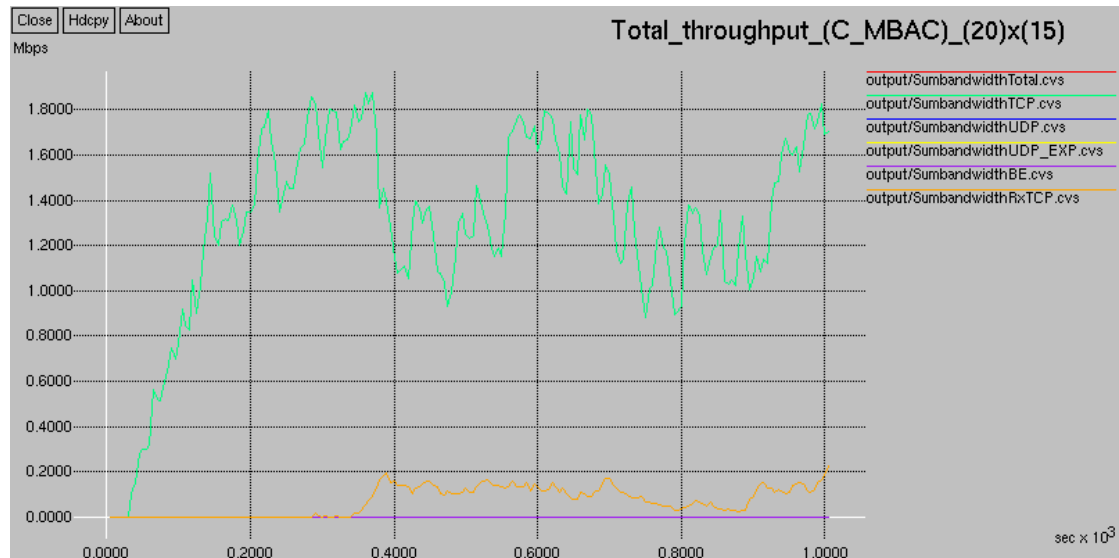
TCP πηγές	20	Link bandwidth	2 Mbps
Αριθμός ροών ανά πηγή	15	Link one way delay	10 ms
TCP Rate	150 Kbps(CBR)	Initialization period	200 sec
TCP packet size	460 bytes	Time of simulation	1000 sec

Αυτό που μεταβάλλεται κάθε φορά είναι το κατώφλι (threshold) για την χρησιμοποίηση του δικτύου. Εκτελούμε το ίδιο πείραμα για τιμές κατωφλίου 0.99, 0.98, 0.97, 0.95, 0.9, 0.85, 0.8, 0.75, 0.7, 0.65, 0.6, 0.55, 0.5, και κάθε φορά εξετάζουμε τις ροές που δημιουργούνται. Από τα αποτελέσματα παρατηρούμε ότι για τιμές του κατωφλίου από 0.97 και κάτω, όσες ροές γίνονται αποδεκτές, εξυπηρετούνται άριστα, δηλαδή δεν έχουμε καθόλου απώλειες πακέτων. Παρακάτω παρουσιάζουμε τα γραφήματα (για κάποιες ενδεικτικές, από τις παραπάνω τιμές) της

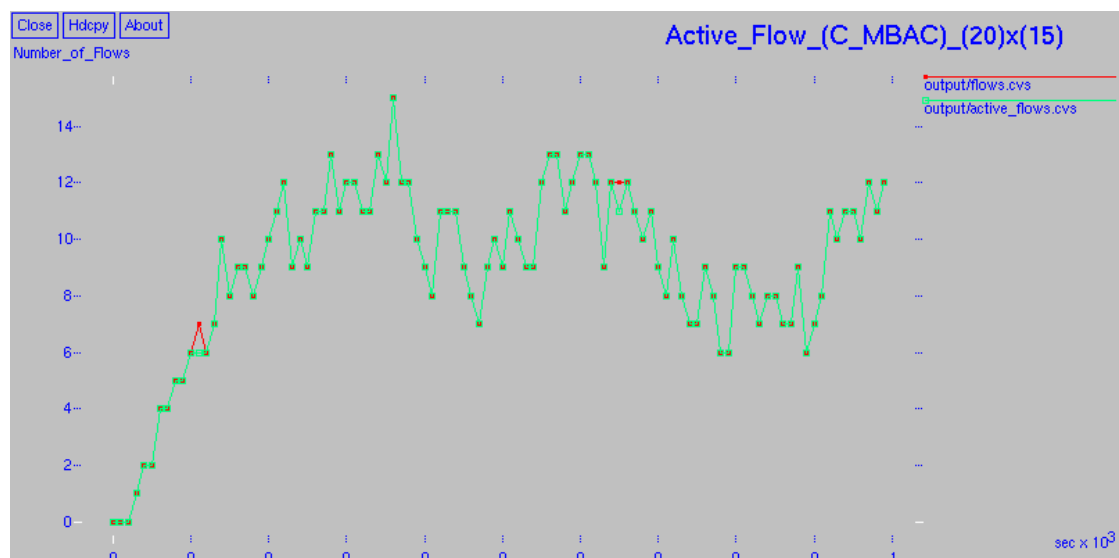
απόδοσης της γραμμής, του αριθμού των ροών που δημιουργούνται και του αριθμού των ροών που είναι ενεργές, συναρτήσει του χρόνου.

➤ Threshold = 0.99

Στην περίπτωση αυτή γίνονται αποδεκτές 133 ροές, απορρίπτονται μηδέν και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 63,5924 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

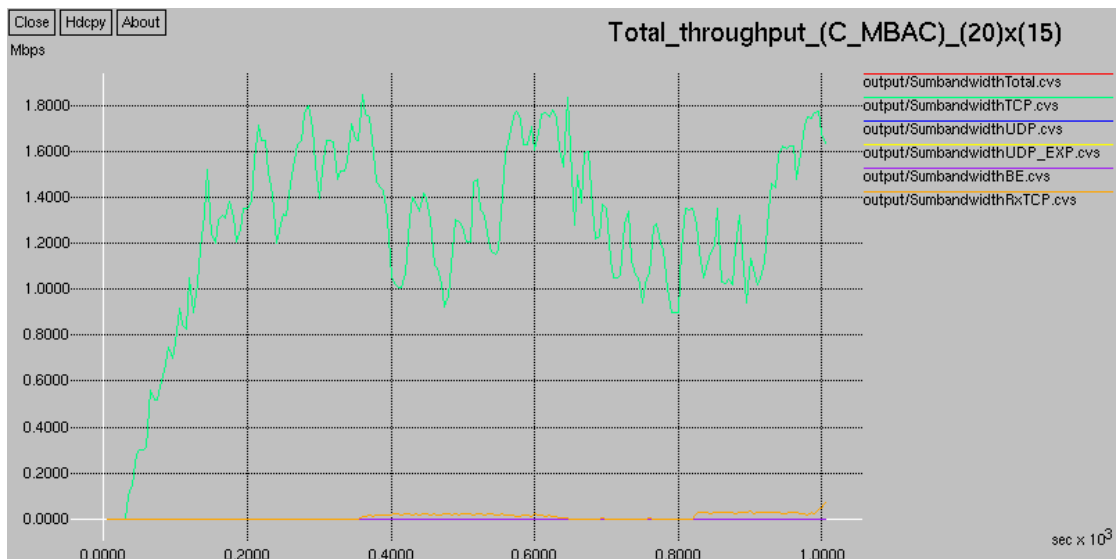


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:

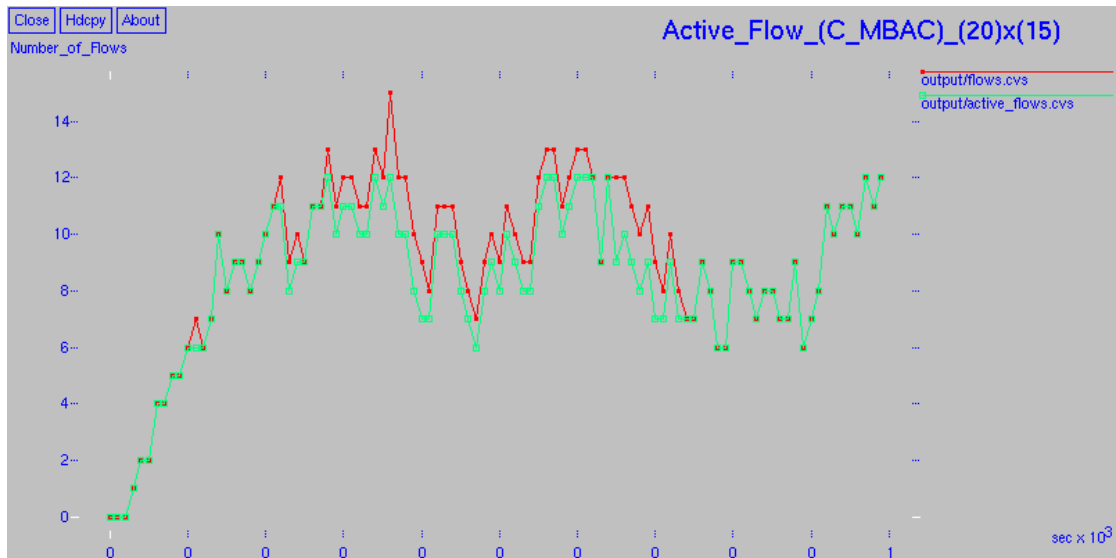


➤ Threshold = 0.98

Στην περίπτωση αυτή γίνονται αποδεκτές 126 ροές, απορρίπτονται 7 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 61,9611 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

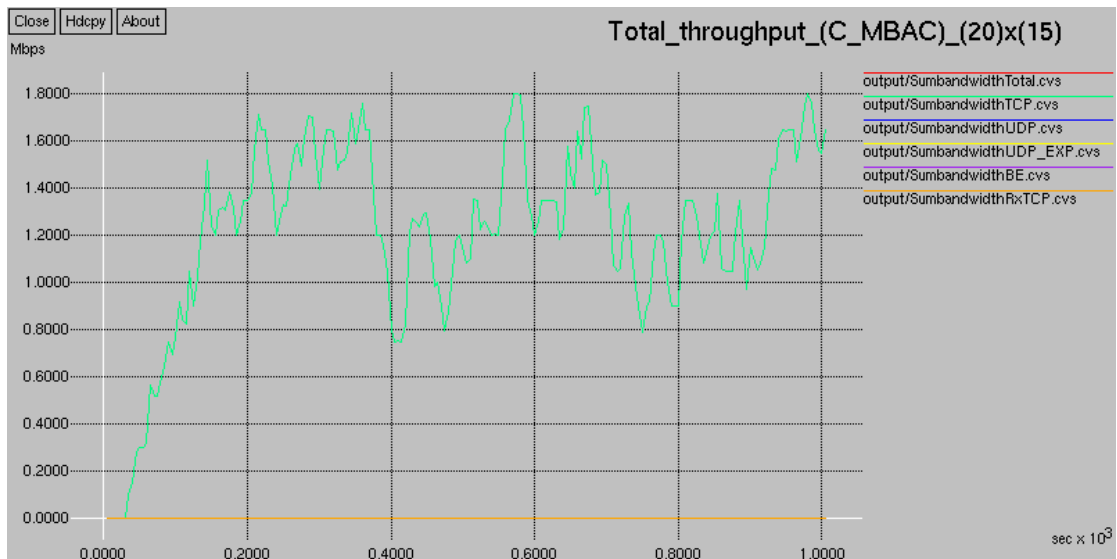


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:

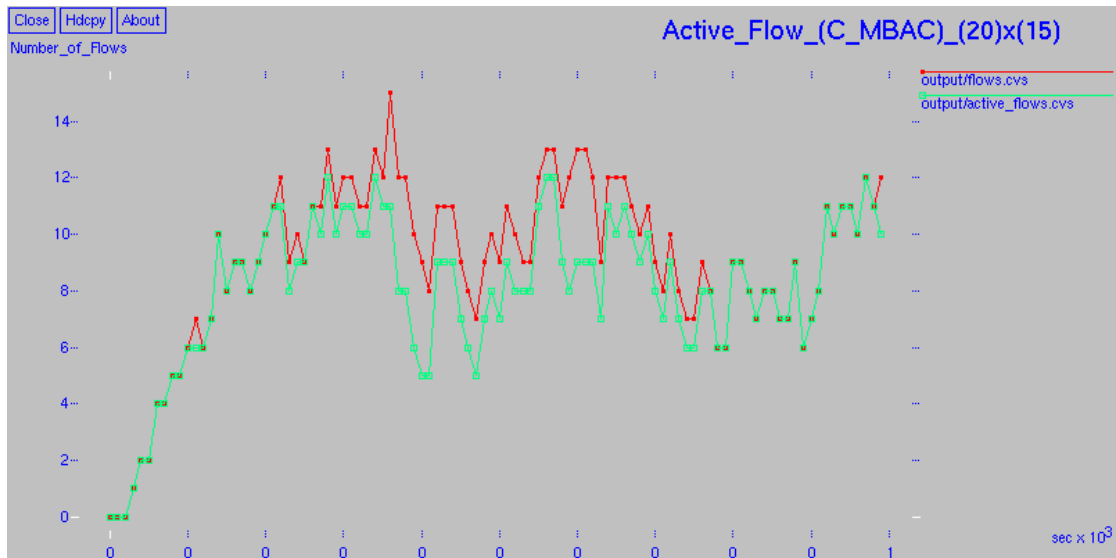


➤ Threshold = 0.97

Στην περίπτωση αυτή γίνονται αποδεκτές 123 ροές, απορρίπτονται 10 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 59,8127 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

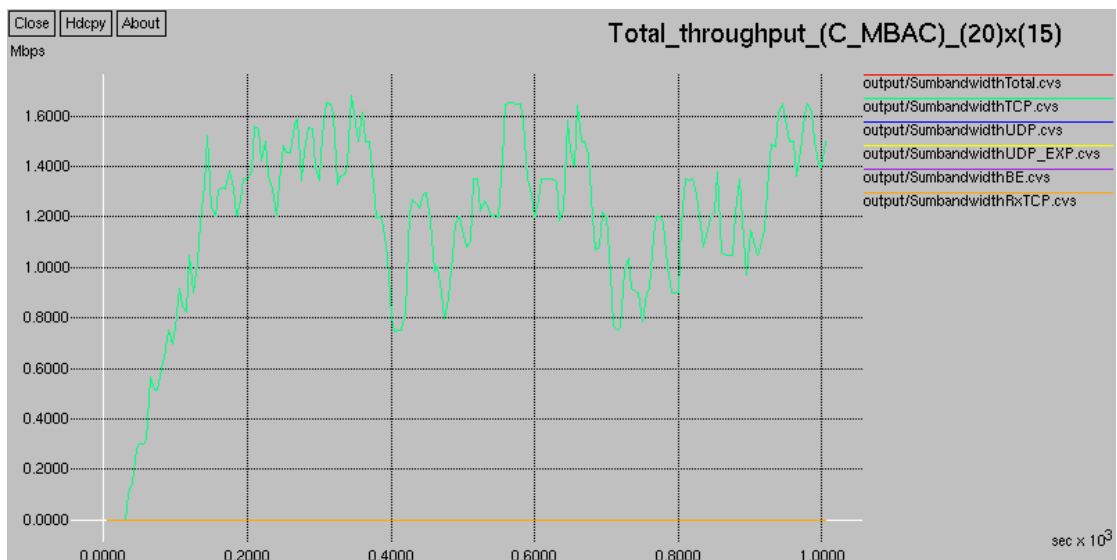


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:

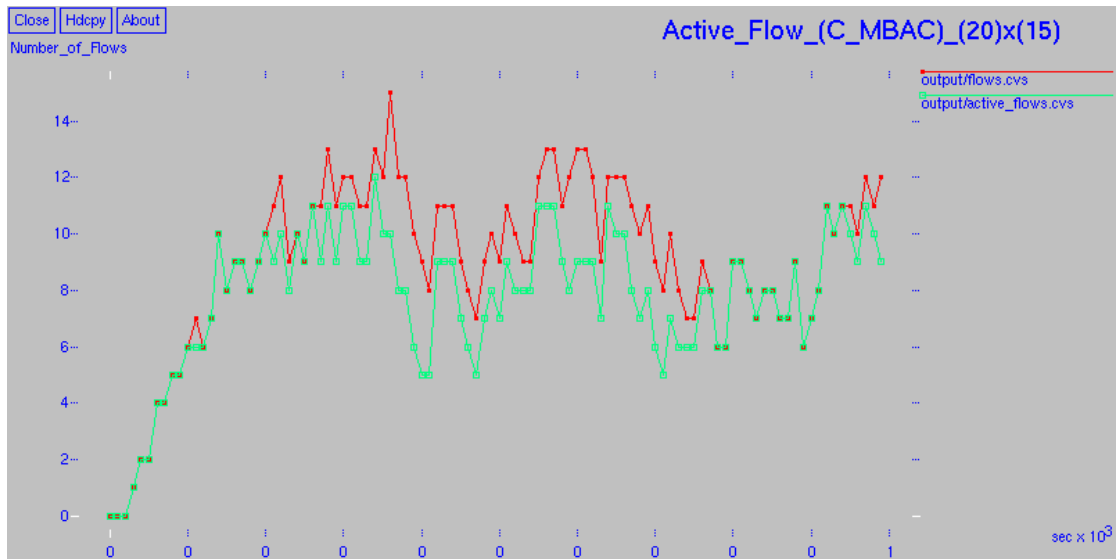


➤ Threshold = 0.9

Στην περίπτωση αυτή γίνονται αποδεκτές 115 ροές, απορρίπτονται 18 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 57,6733 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

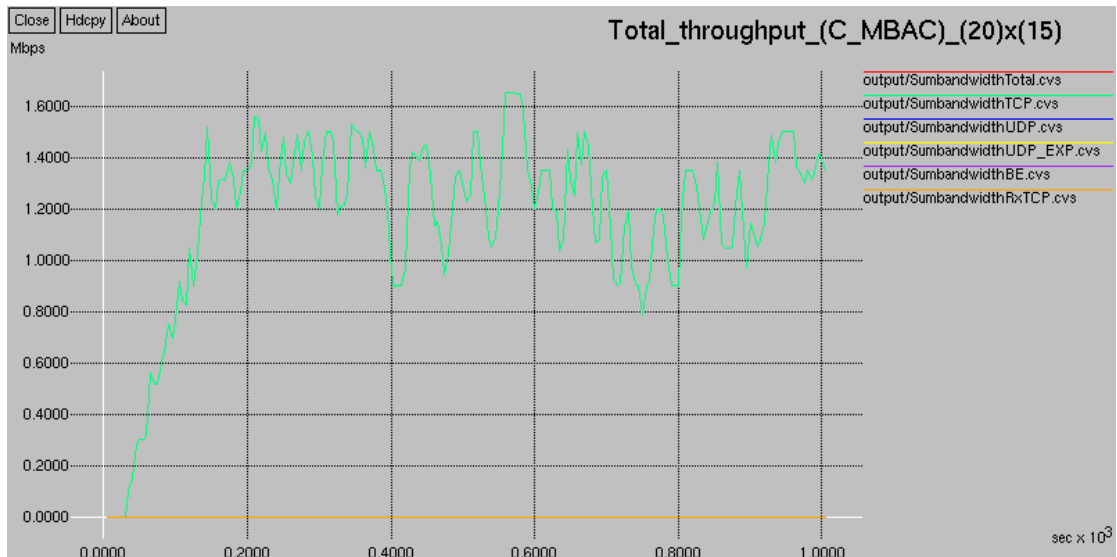


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:

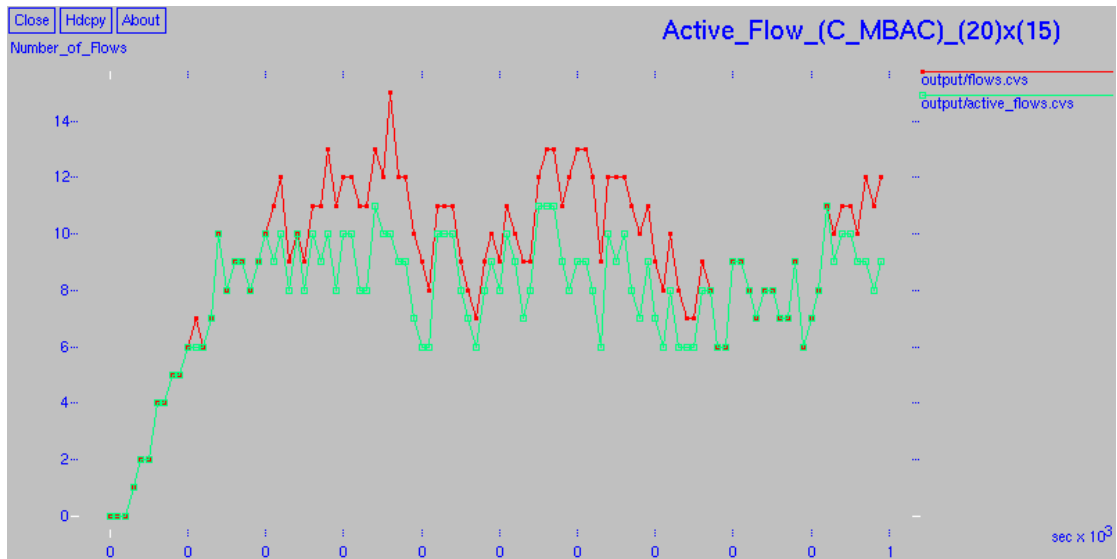


➤ Threshold = 0.85

Στην περίπτωση αυτή γίνονται αποδεκτές 111 ροές, απορρίπτονται 22 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 57,5968 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

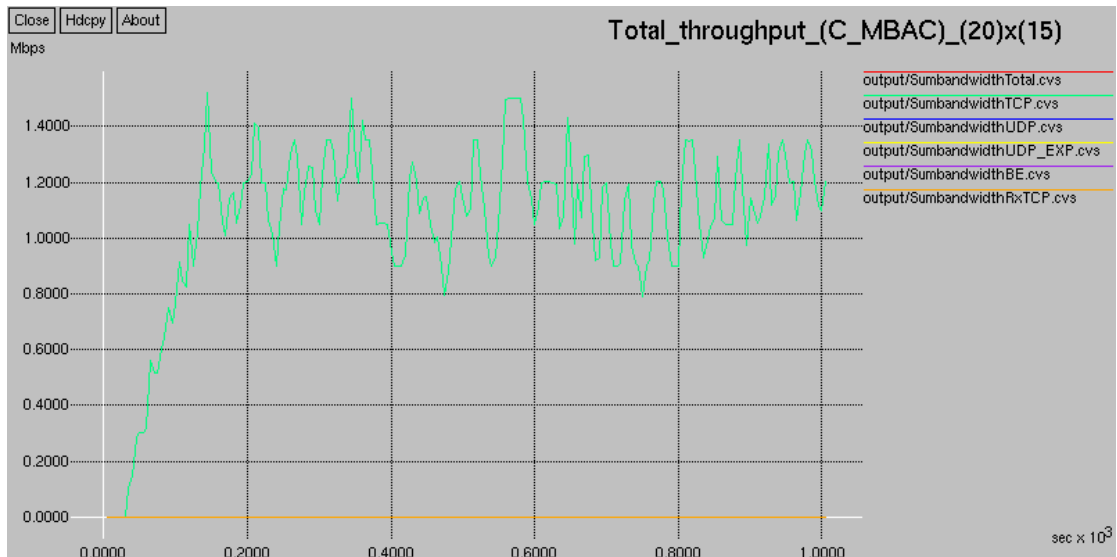


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:

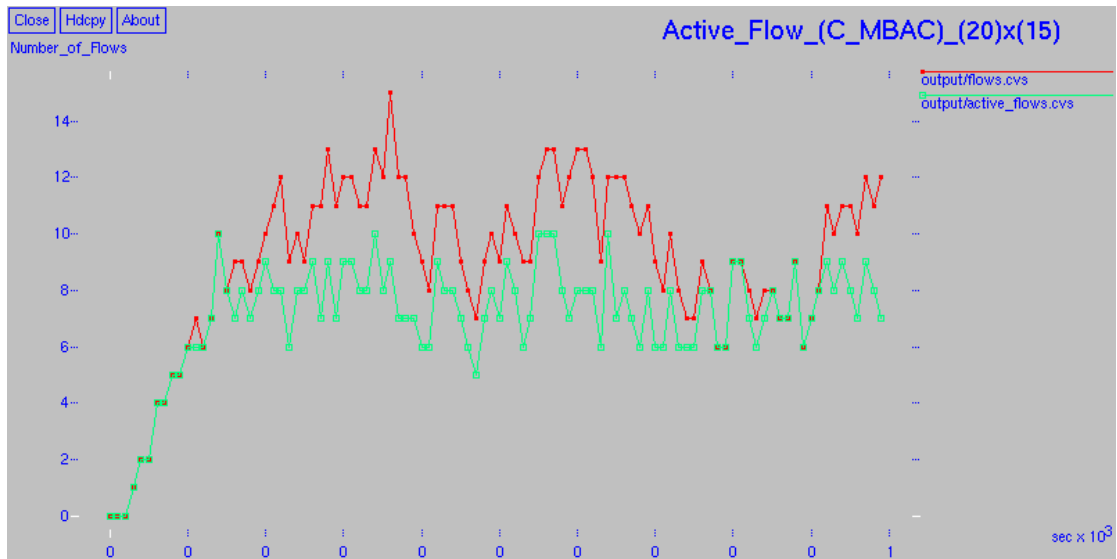


➤ Threshold = 0.75

Στην περίπτωση αυτή γίνονται αποδεκτές 104 ροές, απορρίπτονται 29 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 52,422 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

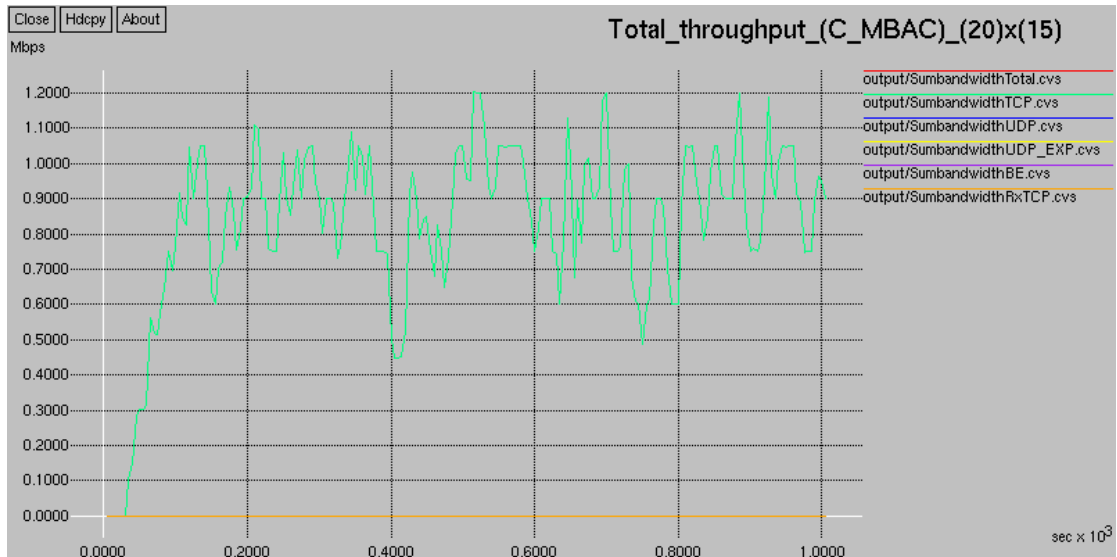


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:

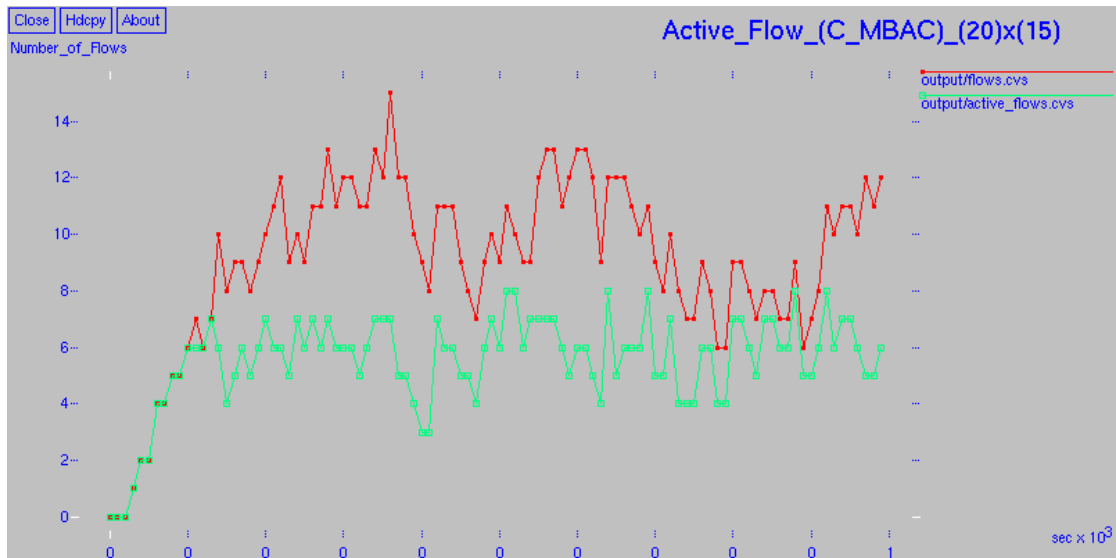


➤ Threshold = 0.6

Στην περίπτωση αυτή γίνονται αποδεκτές 86 ροές, απορρίπτονται 47 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 40,9192 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

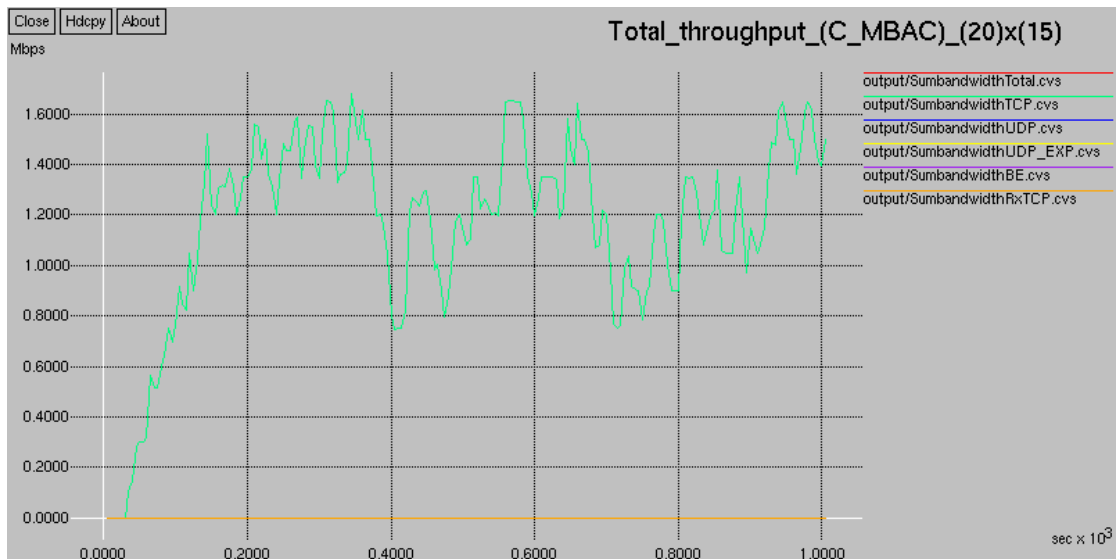


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:

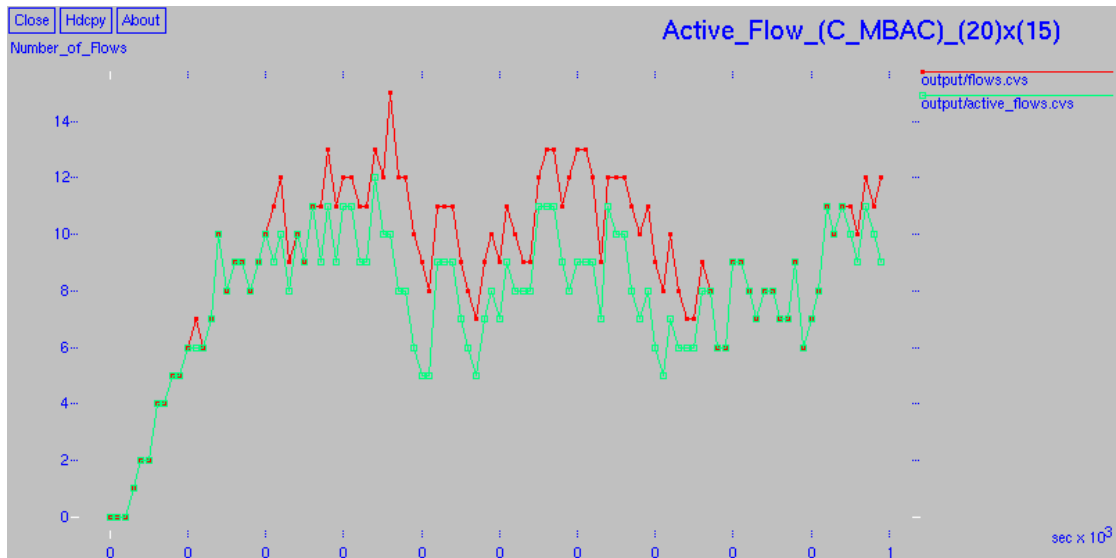


➤ Threshold = 0.5

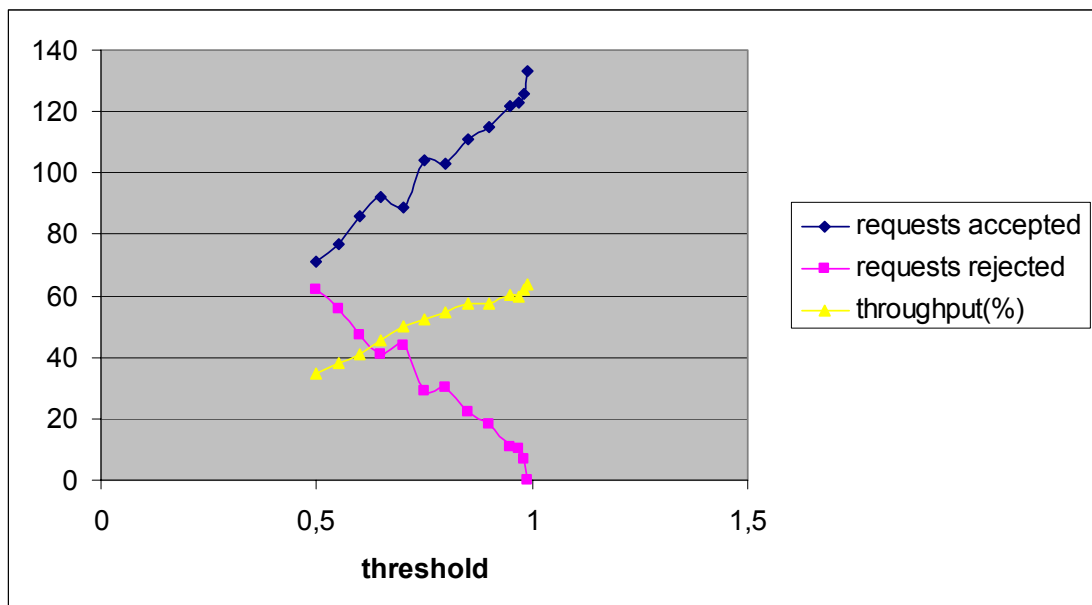
Στην περίπτωση αυτή γίνονται αποδεκτές 71 ροές, απορρίπτονται 62 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 34,7385 %. Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:



Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



Στη συνέχεια παρουσιάζουμε ένα διάγραμμα με τις ροές που έγιναν αποδεκτές, τις ροές που απορρίφθηκαν και την χρησιμοποίηση του δικτύου για διαφορετικές τιμές του κατώφλιου:



Από τα παραπάνω διαγράμματα, συμπεραίνουμε ότι καθώς μειώνεται το κατώφλι, μειώνεται και ο αριθμός των ροών που γίνονται αποδεκτές (με αποτέλεσμα να μειώνεται και ο αριθμός των ενεργών ροών) και αυξάνεται ο αριθμός των ροών που απορρίπτονται. Παράλληλα μειώνεται η μέγιστη απόδοση (throughput) της γραμμής.

6.3. 2η προσομοίωση με εφαρμογή του MBAC μοντέλου

Στις επόμενες προσομοιώσεις εφαρμόζουμε έλεγχο αποδοχής ροών με τον αλγόριθμο Color MBAC. Σε κάθε ένα από τα πειράματα, θεωρούμε ότι έχουμε ως εισόδους τα παρακάτω στοιχεία:

Link threshold	0.93	Link bandwidth	1,5 Mbps
Αριθμός ροών ανά πηγή	15	Link one way delay	10 ms
TCP Rate	170 Kbps(CBR)	Initialization period	200 sec
TCP packet size	460 bytes	Time of simulation	1000 sec

Αυτό που μεταβάλλεται κάθε φορά είναι το ο αριθμός των TCP πηγών. Εκτελούμε το ίδιο πείραμα για τιμές 15, 16, 17, 18, 19 και 20, και κάθε φορά εξετάζουμε τις ροές που δημιουργούνται, όσον αφορά τις απώλειες πακέτων. Σκοπός αυτής της προσομοίωσης είναι να μελετηθεί η επίδραση που έχει η σταδιακή αύξηση του αριθμού των πηγών, στη συμπεριφορά των δημιουργούμενων ροών. Η αρχική τιμή που έχουμε επιλέξει (αριθμός πηγών 15), αντιστοιχεί σε πολύ μικρό ποσοστό απωλειών πακέτων. Στην προσομοίωση αυτή, έχουμε επιλέξει μια υψηλή τιμή για το threshold, που σε συνδυασμό με τον ρυθμό μετάδοσης των ροών, θα δώσει απώλειες πακέτων. Στην περίπτωση αυτή, η απόδοση του ελέγχου αποδοχής ροών δεν είναι η επιθυμητή. Συνεχίζει όμως, να παρέχει καλύτερα αποτελέσματα από αυτά που θα παίρναμε αν απουσίαζε.

Παρακάτω, παρουσιάζουμε τα γραφήματα της απόδοσης της γραμμής, του αριθμού των ροών που δημιουργούνται, του αριθμού των ροών που είναι ενεργές και ένα διάγραμμα με την απόδοση ανά χρώμα πακέτων, συναρτήσει του χρόνου. Το τελευταίο διάγραμμα, είναι αυτό, που κάθε στιγμή μας δίνει την επιπλέον πληροφορία (αριθμός πακέτων που ξεπερνούν / υπολείπονται του μέσου ρυθμού της ροής) για την κατάσταση των ροών στον αλγόριθμο Color MBAC.

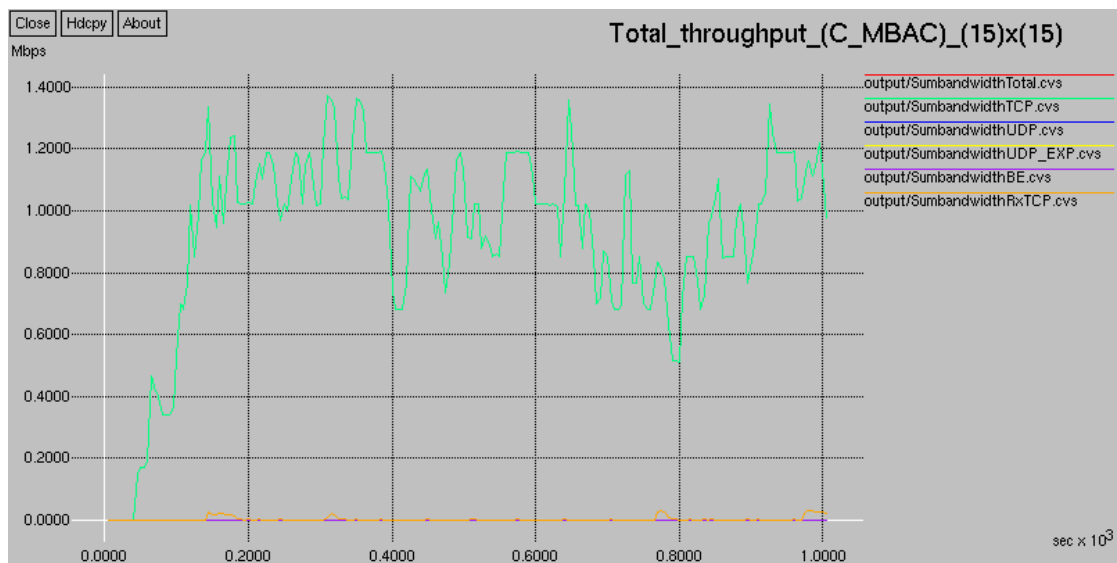
➤ Αριθμός TCP πηγών = 15

Στην περίπτωση αυτή, όπως αναφέραμε, έχουμε πολύ μικρές απώλειες πακέτων. Παρατηρούμε ότι γίνονται αποδεκτές 78 ροές, απορρίπτονται 23 και η

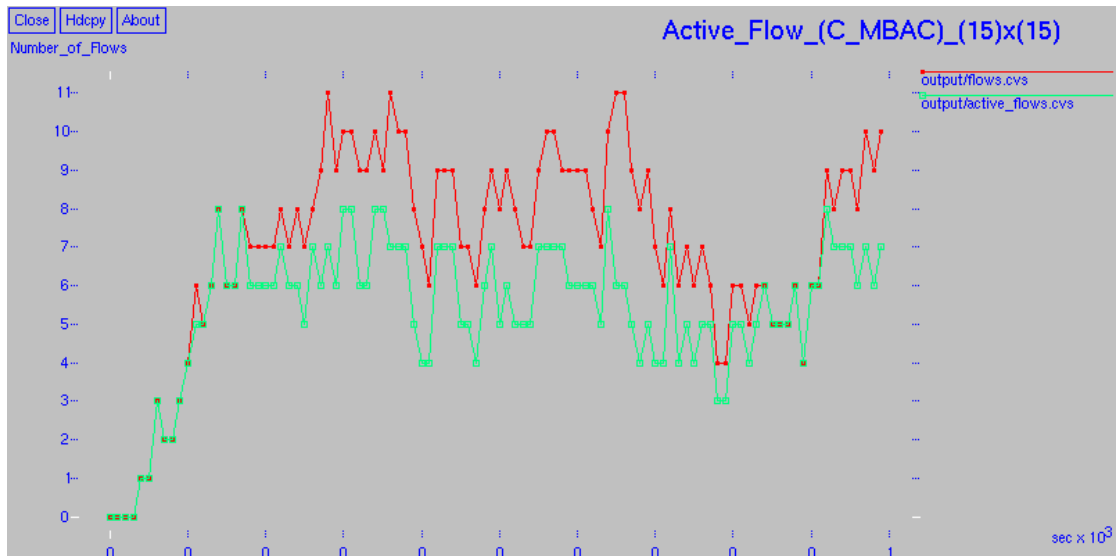
χρησιμοποίηση του δικτύου είναι Link Utilisation = 60,5890 %. Ακόμη παίρνουμε τα εξής αποτελέσματα σε σχέση με την συμπεριφορά των ροών:

Excellent Connections	74
Good Connections	0
Bad connections	0
Worst connections	4

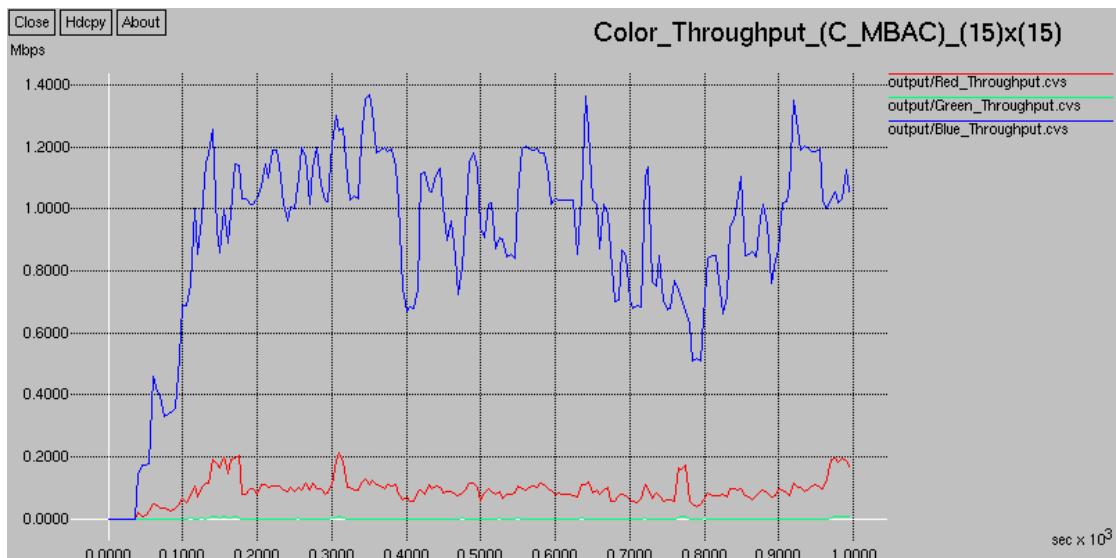
Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:



Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



Επιπλέον, παραθέτουμε και το γράφημα με την απόδοση για κάθε διαφορετικό χρώμα πακέτων:

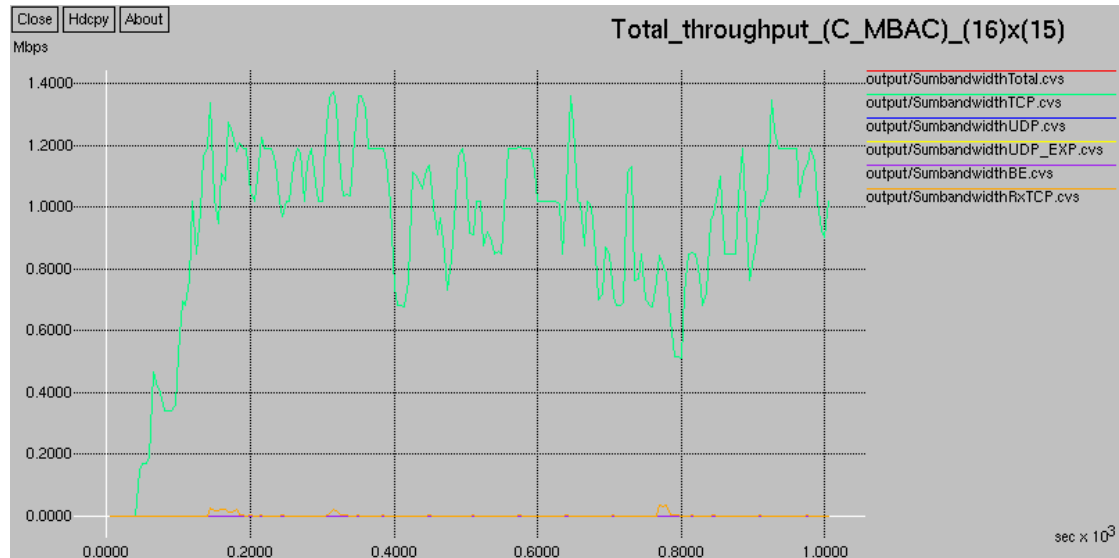


➤ Αριθμός TCP πηγών = 16

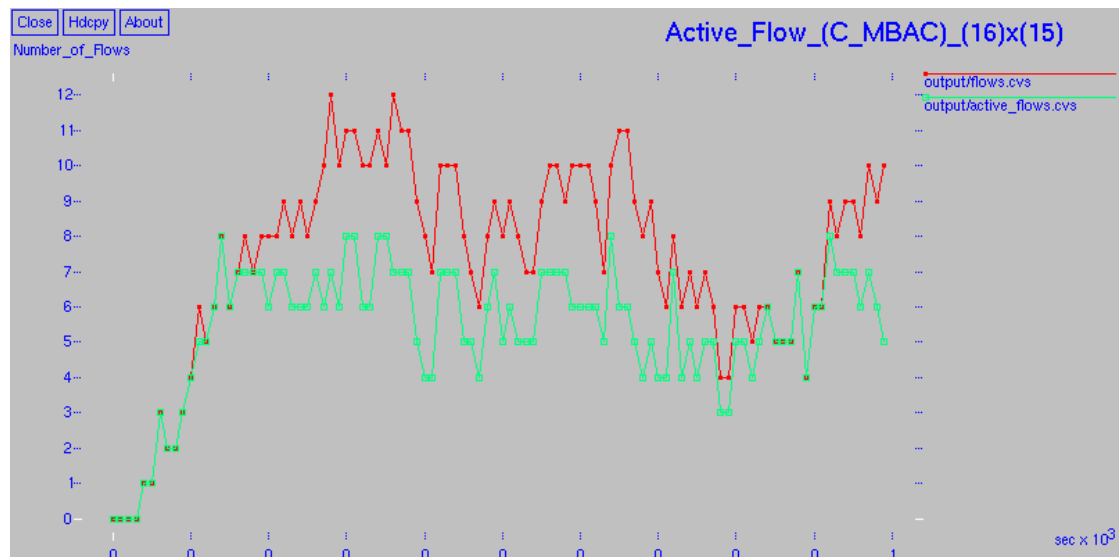
Στην περίπτωση αυτή, όπως αναφέραμε, έχουμε πολύ μικρές απώλειες πακέτων. Παρατηρούμε ότι γίνονται αποδεκτές 77 ροές, απορρίπτονται 29 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 61,0286 %. Ακόμη παίρνουμε τα εξής αποτελέσματα σε σχέση με την συμπεριφορά των ροών:

Excellent Connections	74
Good Connections	0
Bad connections	0

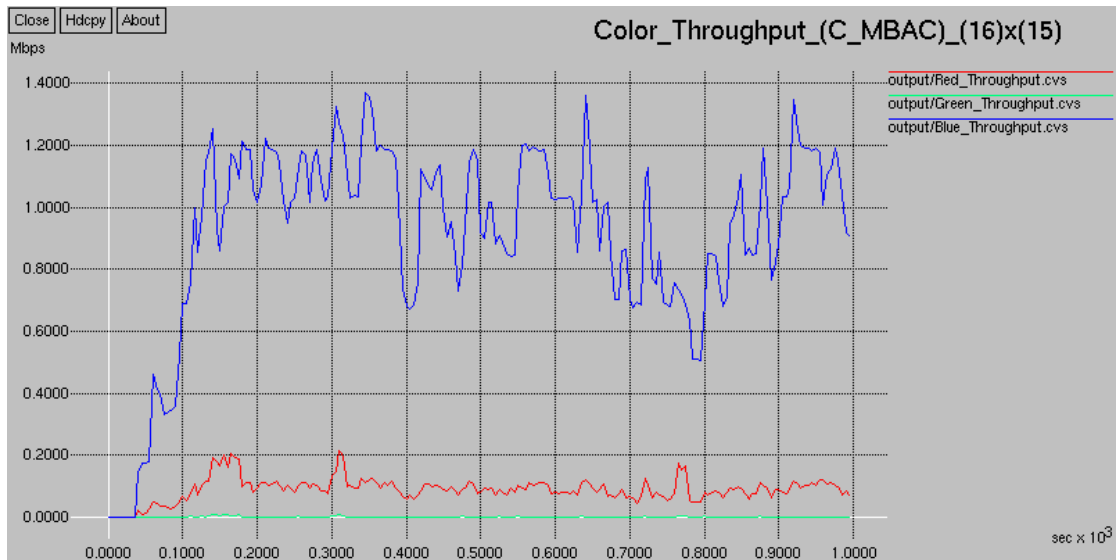
Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:



Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



Επιπλέον, παραθέτουμε και το γράφημα με την απόδοση για κάθε διαφορετικό χρώμα πακέτων:

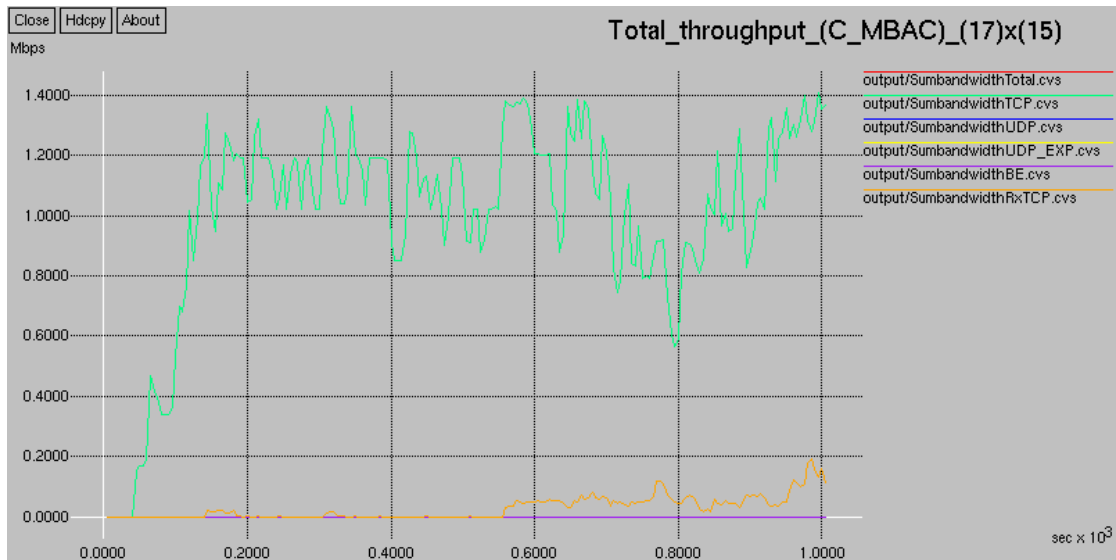


➤ Αριθμός TCP πηγών = 17

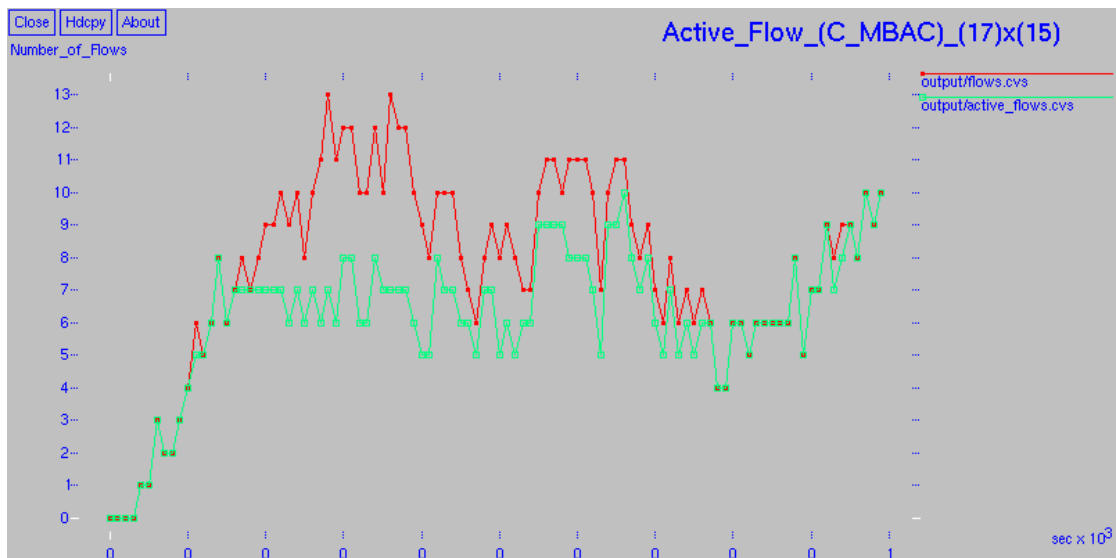
Στην περίπτωση αυτή, όπως αναφέραμε, έχουμε πολύ μικρές απώλειες πακέτων. Παρατηρούμε ότι γίνονται αποδεκτές 89 ροές, απορρίπτονται 23 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 65,8504 %. Ακόμη παίρνουμε τα εξής αποτελέσματα σε σχέση με την συμπεριφορά των ροών:

Excellent Connections	59
Good Connections	4
Bad connections	1
Worst connections	25

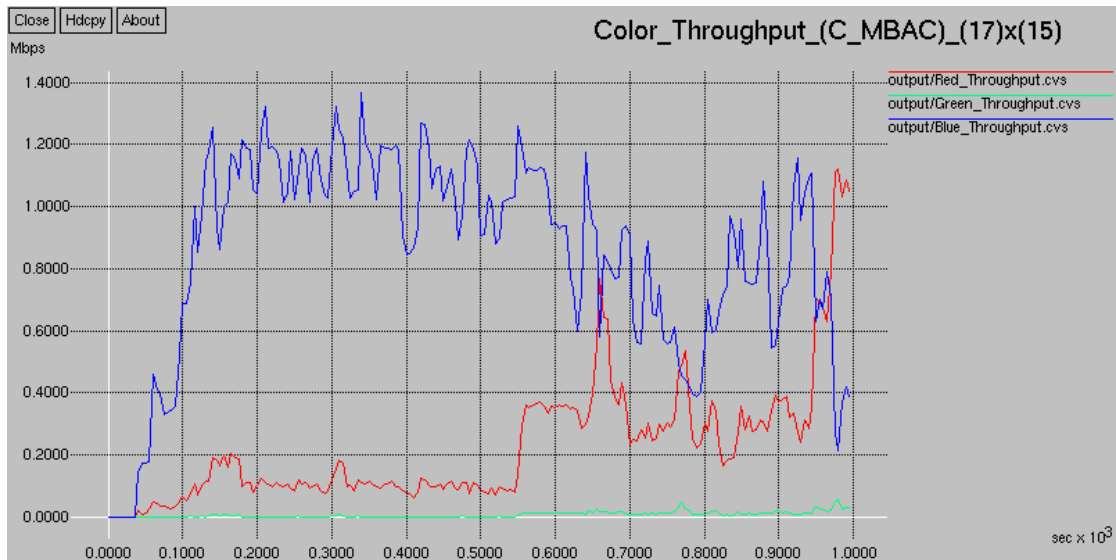
Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:



Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



Επιπλέον, παραθέτουμε και το γράφημα με την απόδοση για κάθε διαφορετικό χρώμα πακέτων:

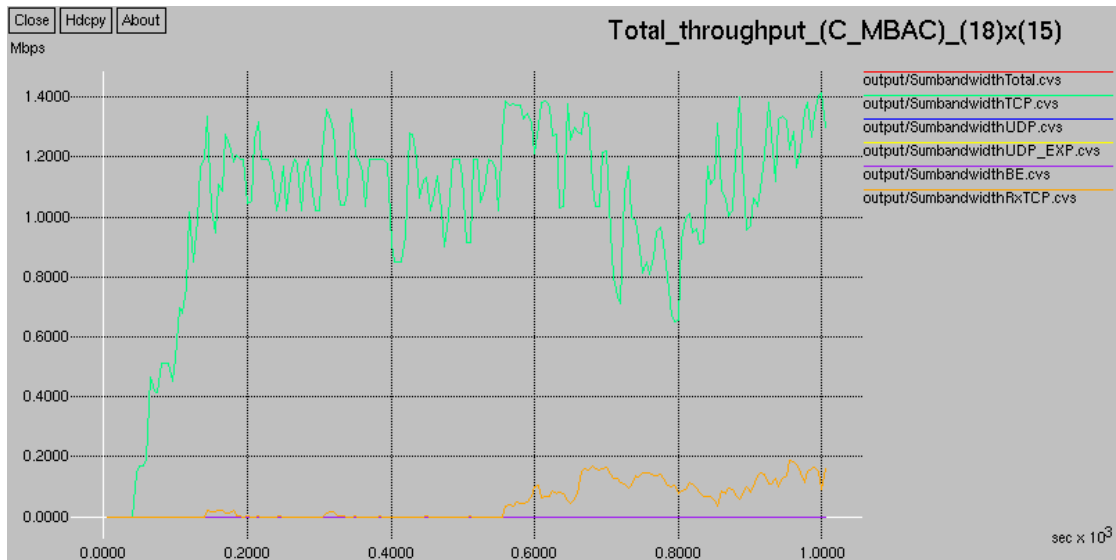


➤ Αριθμός TCP πηγών = 18

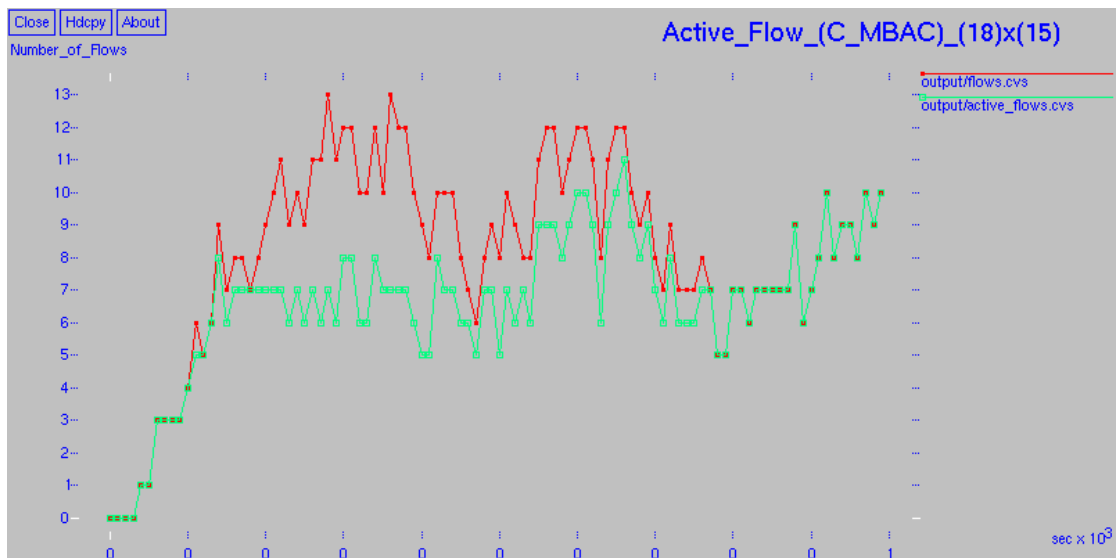
Στην περίπτωση αυτή, όπως αναφέραμε, έχουμε πολύ μικρές απώλειες πακέτων. Παρατηρούμε ότι γίνονται αποδεκτές 97 ροές, απορρίπτονται 24 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 67,7223%. Ακόμη παίρνουμε τα εξής αποτελέσματα σε σχέση με την συμπεριφορά των ροών:

Excellent Connections	51
Good Connections	1
Bad connections	4
Worst connections	41

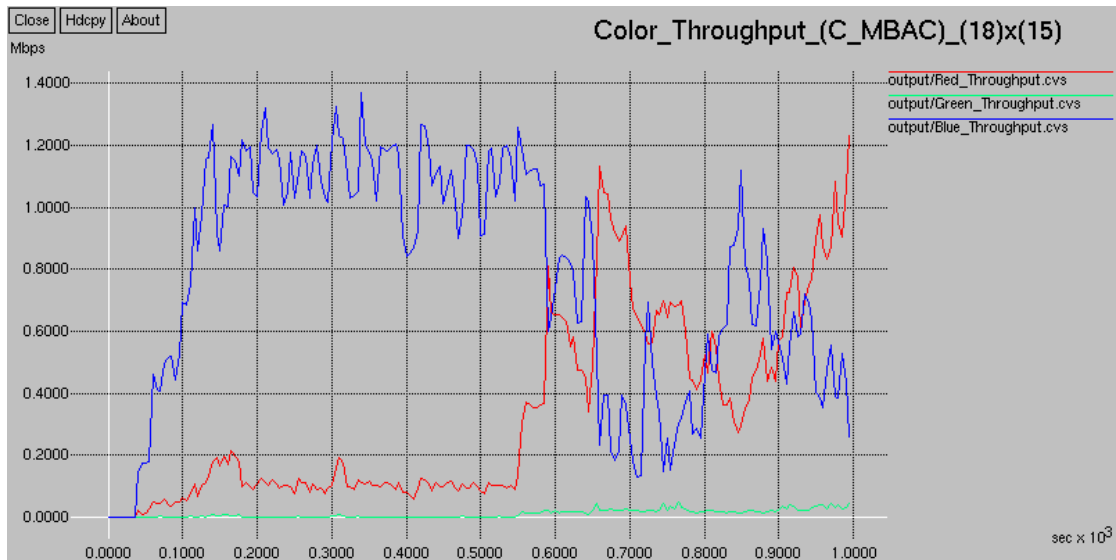
Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσσει του χρόνου:



Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



Επιπλέον, παραθέτουμε και το γράφημα με την απόδοση για κάθε διαφορετικό χρώμα πακέτων:

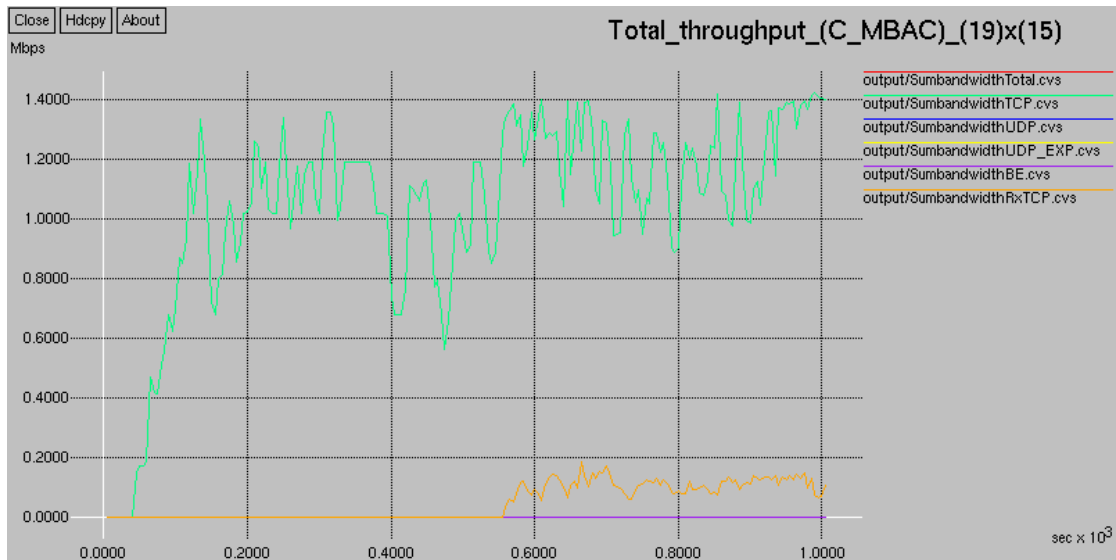


➤ Αριθμός TCP πηγών = 19

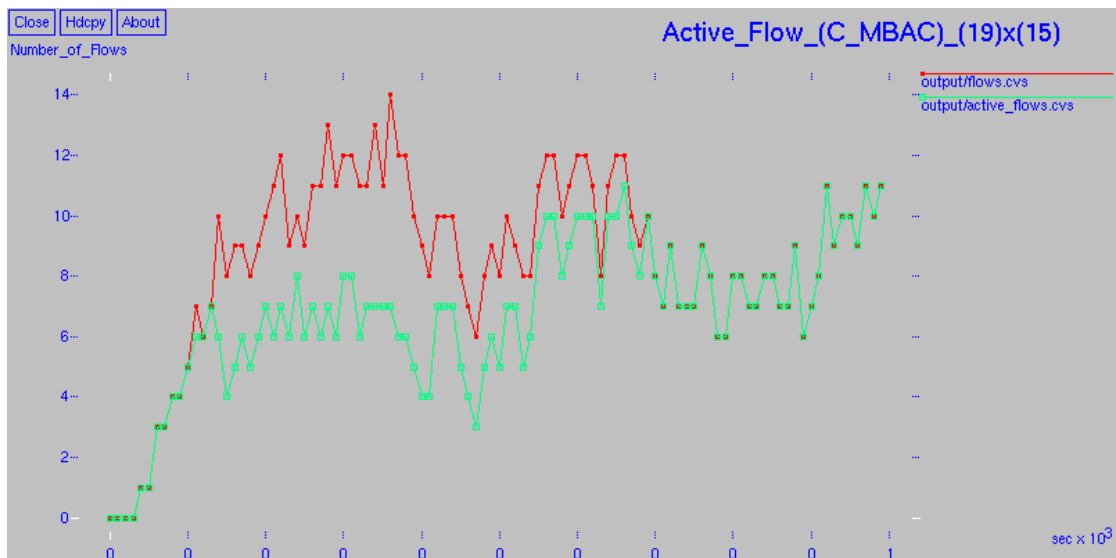
Στην περίπτωση αυτή, όπως αναφέραμε, έχουμε πολύ μικρές απώλειες πακέτων. Παρατηρούμε ότι γίνονται αποδεκτές 105 ροές, απορρίπτονται 21 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 68,1561 %. Ακόμη παίρνουμε τα εξής αποτελέσματα σε σχέση με την συμπεριφορά των ροών:

Excellent Connections	60
Good Connections	2
Bad connections	5
Worst connections	38

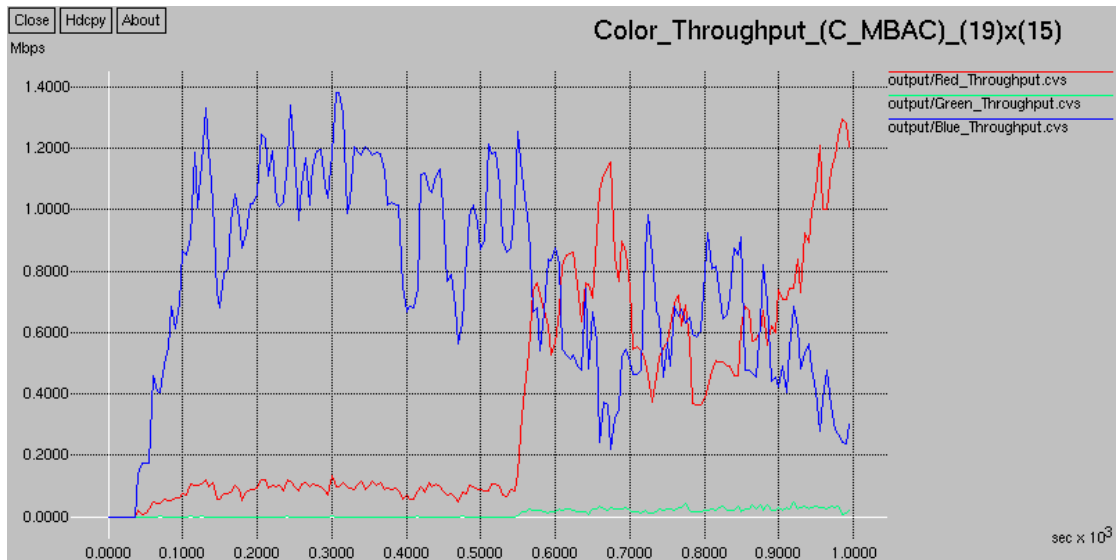
Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:



Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



Επιπλέον, παραθέτουμε και το γράφημα με την απόδοση για κάθε διαφορετικό χρώμα πακέτων:

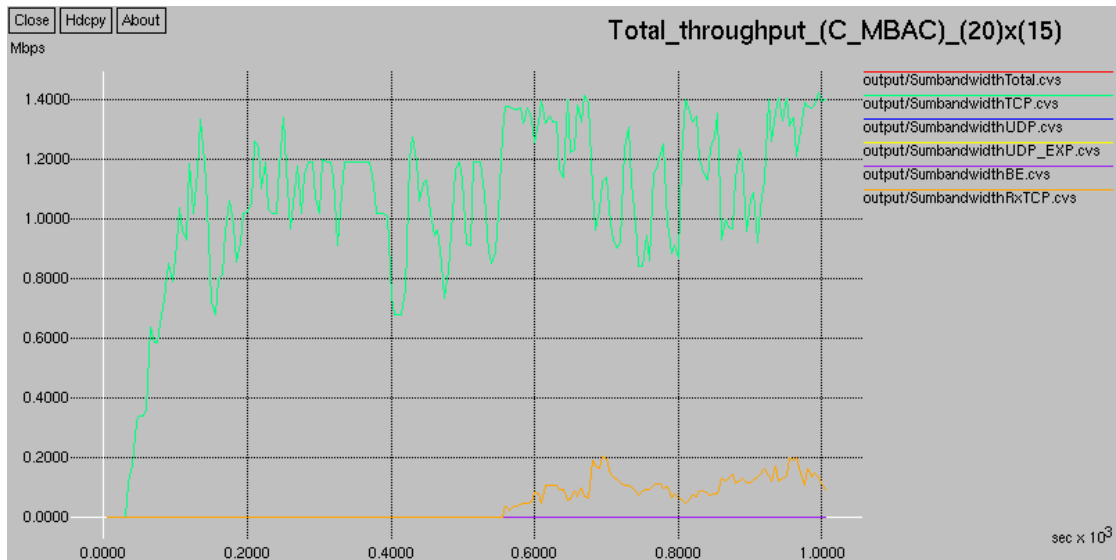


➤ Αριθμός TCP πηγών = 20

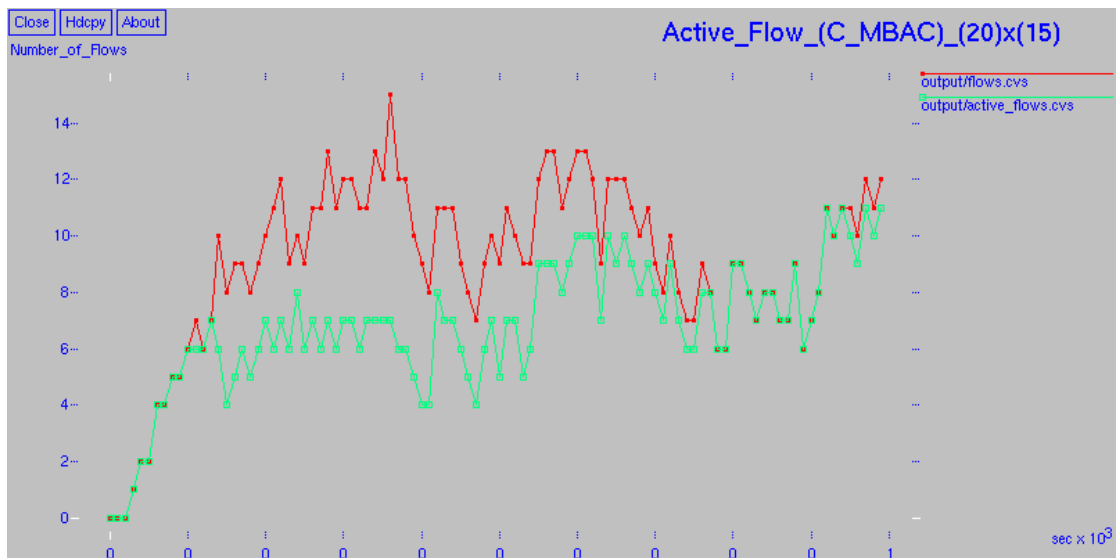
Στην περίπτωση αυτή, όπως αναφέραμε, έχουμε πολύ μικρές απώλειες πακέτων. Παρατηρούμε ότι γίνονται αποδεκτές 105 ροές, απορρίπτονται 27 και η χρησιμοποίηση του δικτύου είναι Link Utilisation = 68,8857 %. Ακόμη παίρνουμε τα εξής αποτελέσματα σε σχέση με την συμπεριφορά των ροών:

Excellent Connections	56
Good Connections	5
Bad connections	1
Worst connections	42

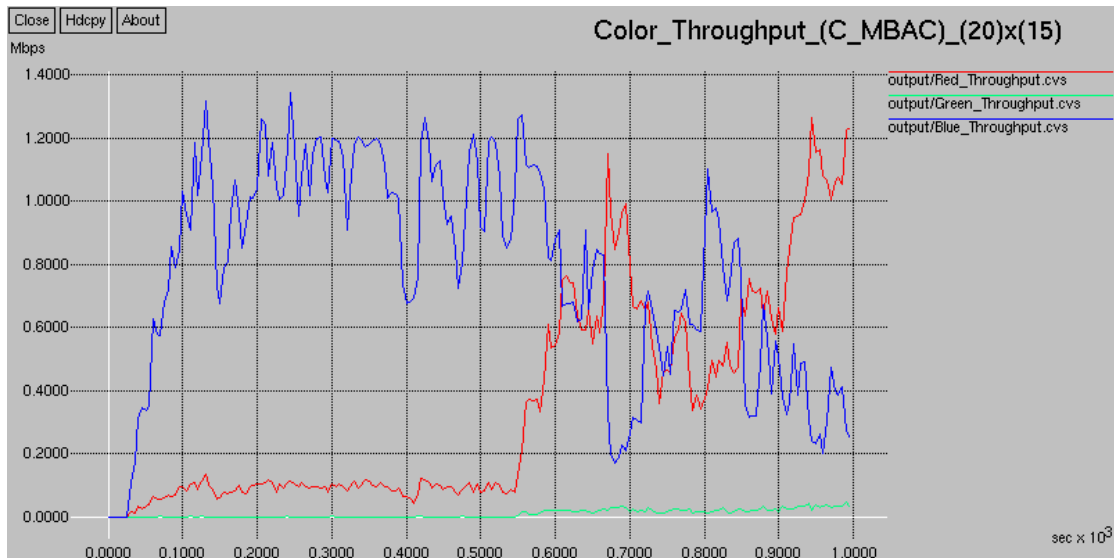
Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσσει του χρόνου:



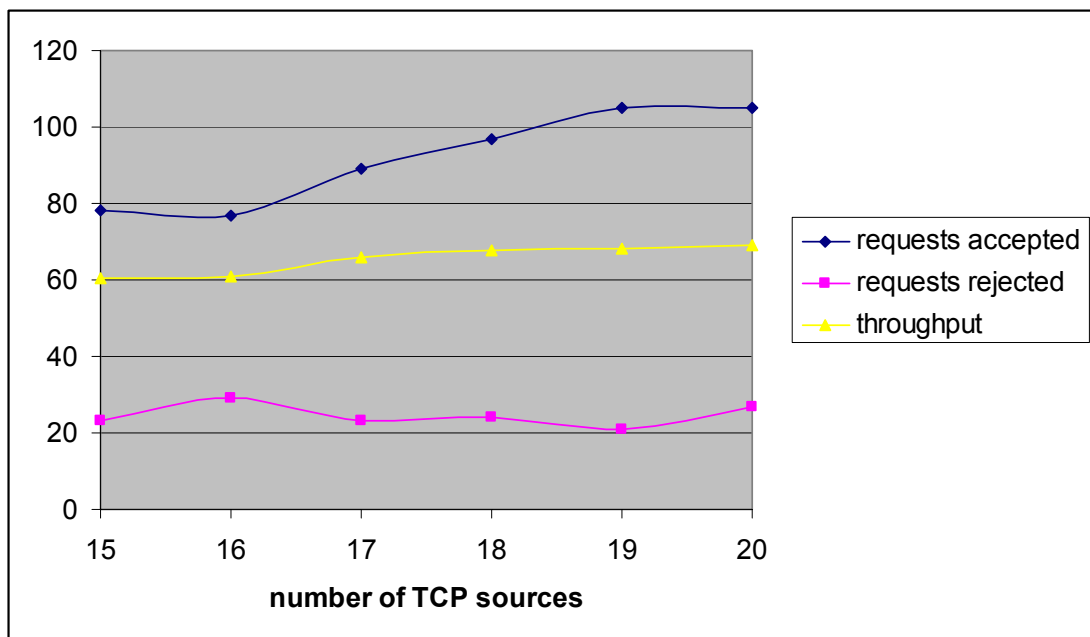
Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



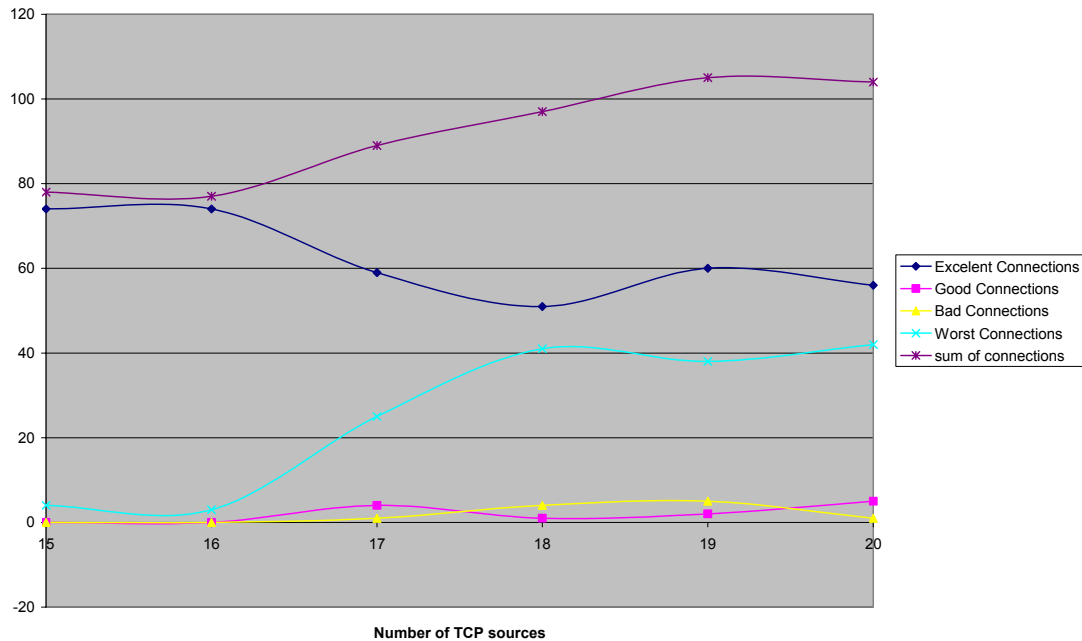
Επιπλέον, παραθέτουμε και το γράφημα με την απόδοση για κάθε διαφορετικό χρώμα πακέτων:



Στο επόμενο γράφημα, παρουσιάζουμε τις ροές που έγιναν αποδεκτές, τις ροές που απορρίφθηκαν και την χρησιμοποίηση του δικτύου για διαφορετικές τιμές των χρησιμοποιούμενων πηγών:



Στο επόμενο γράφημα, παρουσιάζουμε τον τρόπο με τον οποίο μεταβάλλεται η κατανομή των ροών, όσον αφορά τις απώλειες πακέτων, συναρτήσει του αριθμού των χρησιμοποιούμενων πηγών:



Από τα δύο παραπάνω γραφήματα, συμπεραίνουμε ότι καθώς αυξάνεται ο αριθμός των χρησιμοποιούμενων πηγών, αυξάνονται οι ροές που γίνονται αποδεκτές, οι συνολικές ροές που δημιουργούνται και η απόδοση της γραμμής, ενώ οι ροές που απορρίπτονται παρουσιάζουν διακυμάνσεις. Όσον αφορά τις ροές που δημιουργούνται, παρατηρούμε, ότι καθώς αυξάνονται οι πηγές, η συμπεριφορά των ροών χειροτερεύει σε μεγάλο βαθμό. Ενώ οι ροές που χαρακτηρίζονται από καλή και μέτρια συμπεριφορά δεν παρουσιάζουν μεγάλες μεταβολές, υπάρχει μεγάλη αύξηση των ροών με την χειρότερη συμπεριφορά και σημαντική μείωση των ροών με τέλεια συμπεριφορά.

Ένα άλλο συμπέρασμα που εξάγουμε, είναι ότι με την αύξηση του αριθμού των χρησιμοποιούμενων πηγών, έχουμε αύξηση της κίνησης κόκκινων πακέτων και μείωση της κίνησης μπλε πακέτων. Αυτό οφείλεται στην συμπεριφορά του πρωτοκόλλου TCP όταν υπάρχουν απώλειες πακέτων (βλέπε παράρτημα). Η απότομη μείωση του παραθύρου του πρωτοκόλλου TCP, έχει ως αποτέλεσμα την εκθετική αύξηση στις μεταδόσεις πακέτων μετά από μια απώλεια (μετάδοση πολλών διαδοχικών πακέτων), με αποτέλεσμα ο στιγμιαίος ρυθμός της κάθε ροής να ξεπερνά τον μέσο και να έχουμε κόκκινο χρωματισμό πακέτων.

6.4. Σύγκριση των αλγορίθμων MS_EF και Color MBAC μέσα από προσομοιώσεις

Στο πείραμα αυτό γίνεται μια προσπάθεια για σύγκριση των αλγορίθμων MS_EF και Color MBAC, μέσα από τρεις προσομοιώσεις (στην καθεμία έχουμε διαφορετικά χαρακτηριστικά για τις πηγές κίνησης).

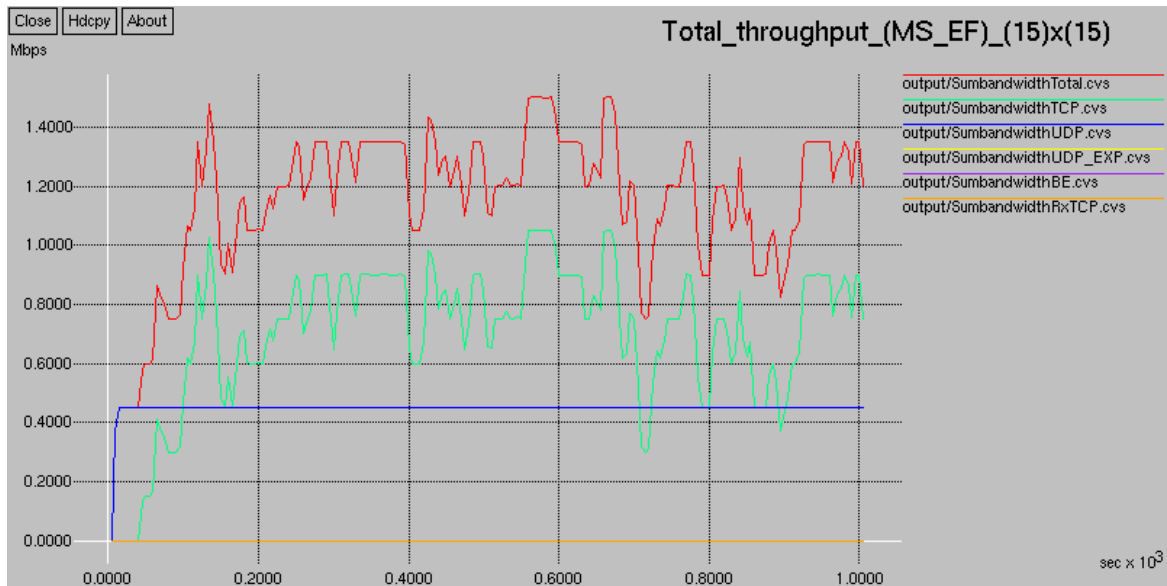
Στην 1^η περίπτωση έχουμε τα παρακάτω χαρακτηριστικά για τις πηγές:

TCP πηγές	15	Link bandwidth	2 Mbps
Αριθμός ροών ανά πηγή	15	Link one way delay	10 ms
TCP Rate	150 Kbps(CBR)	Initialization period	200 sec
TCP packet size	460 bytes	Time of simulation	1000 sec
UDP πηγές	3	threshold	0.8
UDP Rate	150 Kbps(CBR)	BE πηγές	0

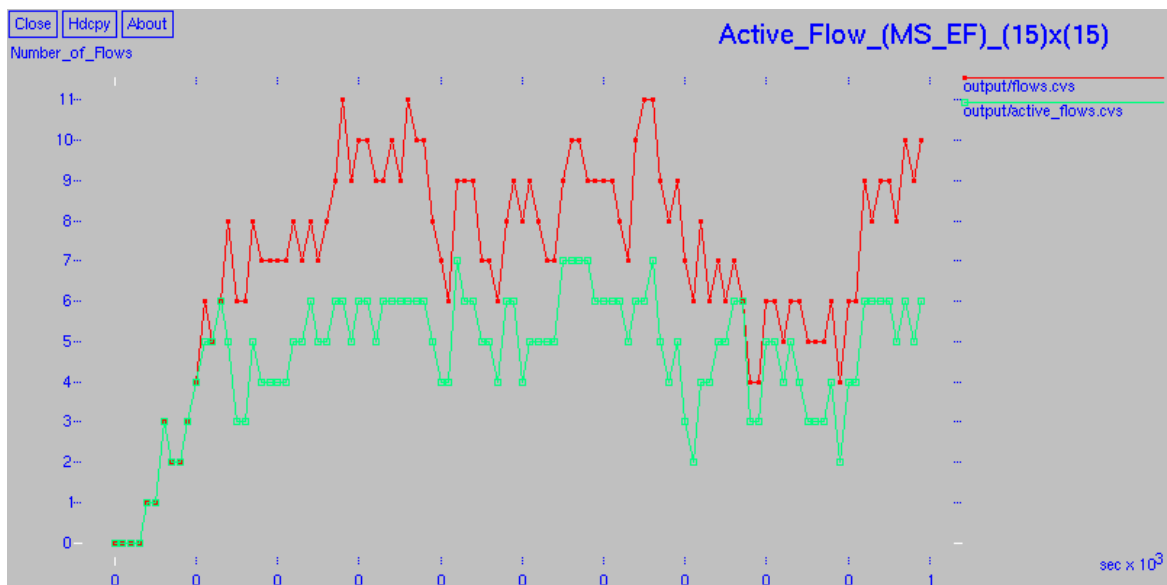
Εκτελώντας την προσομοίωση με τον αλγόριθμο MS_EF, βλέπουμε ότι γίνονται αποδεκτές 71 ροές, ενώ απορρίπτονται 31. Η απόδοση της γραμμής (throughput) είναι 56,8489%, ενώ σχετικά με την συμπεριφορά των ροών έχουμε:

Excellent Connections	71
Good Connections	0
Bad connections	0
Worst connections	0

Παρακάτω παραθέτουμε το γράφημα της χρησιμοποίησης της γραμμής συναρτήσει του χρόνου:

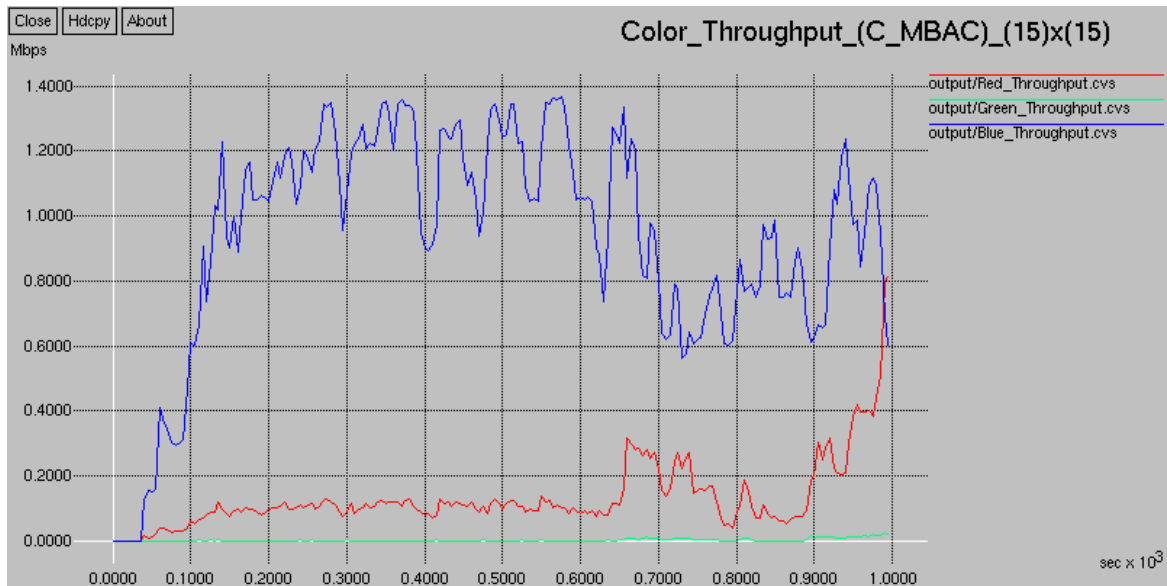


Στη συνέχεια παραθέτουμε και το γράφημα των ενεργών, καθώς και των συνολικών (οι ροές που θα υπήρχαν αν δεν είχαμε έλεγχο αποδοχής) ροών που δημιουργούνται συναρτήσει του χρόνου:



Εκτελώντας την προσομοίωση με τον αλγόριθμο Color MBAC, βλέπουμε ότι γίνονται αποδεκτές 94 ροές, ενώ απορρίπτονται 7. Η απόδοση της γραμμής (throughput) είναι 70,6721%, ενώ σχετικά με την συμπεριφορά των ροών έχουμε:

Excellent Connections	81
Good Connections	0
Bad connections	3



Συγκεντρωτικά, τα αποτελέσματα που παραθέσαμε προηγουμένως, φαίνονται στον επόμενο πίνακα:

Αλγόριθμος	MS_EF	Color MBAC
Αποδεκτές Ροές	71	94
Μη Αποδεκτές Ροές	31	7
Throughput(%bandwidth)	56.64	70.67
Excellent Connections	71	81
Good Connections	0	0
Bad Connections	0	3
Worst Connections	0	10

Παρατηρούμε, ότι ο αλγόριθμος Color MBAC, παρουσιάζει καλύτερα αποτελέσματα από τον MS_EF, δεδομένου ότι αποδέχεται μεγαλύτερο αριθμό ροών, οι συνδέσεις με τέλεια χαρακτηριστικά είναι περισσότερες και η απόδοση της γραμμής μεγαλύτερη. Επιπλέον, από τα διαγράμματα των ενεργών ροών, βλέπουμε ότι κάθε χρονική στιγμή, ο αριθμός των ενεργών ροών είναι μεγαλύτερος κατά την εφαρμογή του Color MBAC.

7. Συμπεράσματα

Στην εργασία αυτή, παρουσιάζονται οι μηχανισμοί που έχουν υλοποιηθεί, για την εφαρμογή ελέγχου αποδοχής ροών βασισμένων σε μετρήσεις, και προτείνεται η εφαρμογή ενός νέου μηχανισμού που βασίζεται στον χρωματισμό των πακέτων στον ακραίο δρομολογητή που συναντούν, και στον έλεγχο για την αποδοχή ή όχι μιας νέας ροής στους κεντρικούς δρομολογητές του δικτύου (με βάση τον χρωματισμό που έχει γίνει, Color MBAC).

Μετά από προσομοιώσεις που έγιναν με το εργαλείο προσομοίωσης Network Simulator (NS), καταλήξαμε στα ακόλουθα συμπεράσματα:

- Ο μηχανισμός Color MBAC μπορεί να χρησιμοποιηθεί για την αποφυγή της συμφόρησης στις γραμμές διασύνδεσης.
- Η χρήση των μηχανισμών MBAC διατηρεί σταθερό τον αριθμό των ροών που είναι ενεργές στο δίκτυο.
- Η χρήση ακατάλληλης τιμής για την μεταβλητή κατωφλιού για το μηχανισμό Color MBAC, μπορεί να οδηγήσει σε χαμηλή χρησιμοποίηση του δικτύου ή σε στιγμιαία συμφόρηση των γραμμών διασύνδεσης.
- Ο μηχανισμός Color MBAC βελτιώνει κατά ένα μικρό ποσοστό τα αποτελέσματα που εξάγουμε, σχετικά με τον αριθμό των ροών που γίνονται αποδεκτές ή απορρίπτονται, καθώς και με τη χρησιμοποίηση της γραμμής μας.

BIBΛΙΟΓΡΑΦΙΑ

- [1] Zheng Wang, “Internet QoS, Architectures and Mechanisms for Quality of Service”, 2001.
- [2] Jingyu Qiu and Edward W. Knightly, Member, IEEE, “Measurement-Based Admission Control with Aggregate Traffic Envelopes”, April 2001.
- [3] Lee Breslaw, Sugih Jamin and Scott Shenker, “Comments on the Performance of Measurement-Based Admission Control Algorithms”, 2000.
- [4] Sugih Jamin and Scott Shenker, “Measurement-Based Admission Control Algorithms for Controlled-load Service: A Structural Examination”, April 1997.
- [5] Sugih Jamin, Scott J. Shenker and Peter B. Danzig, “Comparison of Measurement-based Admission Control Algorithms for Controlled-Load Service”.
- [6] Sugih Jamin, Peter B. Danzig, Scott Shenker and Lixia Zhang, “A Measurement-based Admission Control Algorithm for Integrated Services Packet networks (Extended Version), December 13, 1995.
- [7] Yaw Opoku, JinSoo Park, Todd J. Eshler and Kevin P. Flanagan, Bradley Department of Electrical and Computer Engineering, “Admission Control for IP Quality of Service”.
- [8] Raquel Hill and HT Kung, “A Diff-Serv Admission Control Scheme”, Division of Engineering and Applied Science, Harvard University, Proceedings of IEEE Globecom 2001, November 2001.
- [9] Mansour J. Karam and Fouad A. Tobagi, “Rate And Queue Controlled Random Drop (RQRD): A Buffer Management Scheme for Internet Routers”.
- [10] Jani Lakkakorpi, Nokia Research Center, “Simple measurement-based admission control for DiffServ access networks”.
- [11] Ion Stoica, Scott Shenker and Hui Zhang, “Core-Stateless Fair Queueing: Achieving Approximately Fair Bandwidth Allocations in High Speed Networks”, June 1998.
- [12] Zhiruo Cao, Zheng Wang and Ellen Zegura, “Rainbow Fair Queueing: Fair Bandwidth Sharing Without Per-Flow State”.
- [13] Cisco Systems, “Quality of Service Networking”.

- [14] Z Turanyi, A. Veres and A. Olah, Ericsson, Traffic Analysis and Network Performance Laboratory, “A family of measurement-based admission control algorithms”.
- [15] Tal Anker, Roi Cohen, Danny Dovel and Yoram Singer, “PrFQ: Probabilistic Fair Queueing”.
- [16] Cisco Systems, “DiffServ- The Scalable End-to-End Qos Model”, 2001.
- [17] White Paper, “Quality of Service for applications over IP VPNs”, October 2003.
- [18] White Paper, “Quality of service (QoS) in High Priority Applications”.
- [19] Cisco systems, “QoS in an AVVID-Enabled Wide-Area Network”.
- [20] Chuck Semeria, “Supporting Differentiated Service Classes: Queue Scheduling Disciplines”.
- [21] Marconi Communications, “Quality of Service Internetworking: Ethernet and ATM Solutions”, November 2000.
- [22] Cisco Systems, “Quality of Service Overview”.
- [23] M. Allman, V. Paxson and W. Stevens, “TCP Congestion Control”, April 1999.
- [24] Matt Mathis, Jeff Semke, Jamshid Mahdavi and Kevin Lahey, “The Rate-Halving Algorithm for TCP Congestion Control”, June 1999.
- [25] Jitendra Padhye, Victor Firoiu, Don Towsley, Jim Kurose, “Modeling TCP Throughput: A Simple Model and its Empirical Validation”.
- [26] C. Pandit and S. Meyn, “Robust Measurement-Based Admission Control Using Markov’s Theory of Canonical Distributions”, October 11, 2003.
- [27] Ιάκωβος Στ. Βενιέρης, Αναπληρωτής Καθηγητής Ε.Μ.Π, “Δίκτυα Ευρείας Ζώνης”, 2003.
- [28]] Ιάκωβος Στ. Βενιέρης, Αναπληρωτής Καθηγητής Ε.Μ.Π, “Τεχνολογίες Διαδικτύου”, 2003.

8. Παράρτημα

8.1. Παράρτημα Α – Όρια απόδοσης

Το λήμμα 1 μας δίνει το άνω όριο για την επιπλέον υπηρεσία (από αυτή που της αναλογεί) που λαμβάνει μια ροή, η οποία δεν παρουσιάζει καμία απώλεια κατά τη διάρκεια ενός διαστήματος $[t', t'']$, δηλαδή ισχύει $r(t) \leq w \cdot a^u, \forall t \in [t', t'']$. Στην σχέση αυτή $r(t)$ είναι ο υπολογιζόμενος ρυθμός μετάδοσης της ροής αυτής, a^u ο κανονικοποιημένος ρυθμός δικαιοσύνης για κάθε ροή στη συγκεκριμένη γραμμή (link) όπου βρισκόμαστε και w το βάρος (weight) που αποδίδουμε στη συγκεκριμένη ροή. Το λήμμα 2 μας δίνει ένα παρόμοιο αποτέλεσμα στην περίπτωση όπου $r(t) \geq w \cdot a^u, \forall t \in [t', t'']$. Τελικά, το θεώρημα 1 μας δίνει το άνω όριο για την επιπλέον υπηρεσία που λαμβάνεται από μια ροή κατά τη διάρκεια ενός τυχαίου χρονικού διαστήματος.

Λήμμα 1

Θεωρούμε μια γραμμή με ένα κανονικοποιημένο ρυθμό δικαιοσύνης a^u , και μια ροή με βάρος w . Η επιπλέον υπηρεσία που αποδέχεται η ροή κατά τη διάρκεια ενός διαστήματος $I = [t', t'']$, όταν ο υπολογιζόμενος ρυθμός μετάδοσης της ροής είναι μικρότερος ή ίσος με το ρυθμό r_a (όπου $r_a = a^u \cdot w$), $r(t) \leq r_a \forall t \in I$, είναι άνω φραγμένη από την τιμή $r_a \cdot K + l_{\max}$, όπου l_{\max} παριστάνει το μέγιστο μέγεθος ενός πακέτου.

Απόδειξη: Χωρίς απώλεια της γενικότητας υποθέτουμε ότι ακριβώς n πακέτα της ροής λαμβάνονται κατά τη διάρκεια του διαστήματος I . Ορίζουμε ως $t_i \in I, (1 \leq i \leq n)$ το χρόνο άφιξης του i -στού πακέτου και ως l_i το μέγεθός του. Σύμφωνα με την εξίσωση του αλγορίθμου MBAC (measurement based admission control) που μελετάμε, θα έχουμε ότι :

$$r_i = \left(1 - e^{-\frac{T_i}{K}}\right) \cdot \frac{l_i}{T_i} + e^{-\frac{T_i}{K}} \cdot r_{i-1} \quad (1)$$

Όπου $T_i = t_i - t_{i-1}$ και r_0 αντιπροσωπεύει τον αρχικά υπολογισμένο ρυθμό. Αν $r_0 > 0$, τότε το t_0 θεωρείται ότι παίρνει την τιμή του χρόνου όπου είχε ληφθεί το τελευταίο πακέτο πριν το t^* . Διαφορετικά, αν $r_0 = 0$, τότε υποθέτουμε ότι $t_0 = -\infty$. Όσο ισχύει $r_i \leq r_a$ ($1 \leq i \leq n$), θεωρούμε ότι όλα τα πακέτα προωθούνται και συνεπώς ο συνολικός αριθμός των bits που στέλνονται κατά τη διάρκεια του διαστήματος I είναι $\sum_{i=1}^n l_i$. Επομένως, το πρόβλημά μας μπορεί να ξαναδιατυπωθεί στη μορφή: $\max(\sum_{i=1}^n l_i)$ (2), δεδομένου ότι $r_i \leq r_a$ ($1 \leq i \leq n$).

Από την εξίσωση (1) συνεπάγεται ότι: $l_i = \frac{r_i - r_{i-1} \cdot e^{-\frac{T_i}{K}}}{1 - e^{-\frac{T_i}{K}}} \cdot T_i, 2 \leq i \leq n$ (2)

Σημειώνουμε ότι η παραπάνω εξίσωση δεν ισχύει για $i=1$, δεδομένου ότι $T_1 = \infty$ για $r_0 = 0$.

Στη συνέχεια ορίζουμε: $F(r_1, r_2, \dots, r_n) = \sum_{i=1}^n l_i, 2 \leq i < n$.

Παίρνοντας την μερική παράγωγο της παραπάνω συνάρτησης ως προς r_i έχουμε ότι:

$$\frac{\partial F(r_1, r_2, \dots, r_n)}{\partial r_i} = \frac{T_i}{1 - e^{-\frac{T_i}{K}}} - \frac{T_{i+1} e^{-\frac{T_{i+1}}{K}}}{1 - e^{-\frac{T_{i+1}}{K}}}, 2 \leq i < n.$$

Δεδομένου ότι ισχύει $\frac{x}{1 - e^{-x}} \geq 1$ και $\frac{x \cdot e^{-x}}{1 - e^{-x}} \leq 1$ για $\forall x \geq 0$, έχουμε ότι:

$$\frac{\partial F(r_1, r_2, \dots, r_n)}{\partial r_i} \geq 0, 2 \leq i < n.$$

Επιπλέον έχουμε $\frac{\partial F(r_1, r_2, \dots, r_n)}{\partial r_n} = \frac{T_n}{1 - e^{-\frac{T_n}{K}}} > 0$.

Συνεπώς (έχουμε αύξουσα συνάρτηση) η συνάρτηση $F(r_1, r_2, \dots, r_n) = \sum_{i=1}^n l_i, 2 \leq i < n$ μεγιστοποιείται όταν καθένα από τα ορίσματά της παίρνει τη μέγιστή του τιμή, που στην περίπτωσή μας είναι η r_a .

Έτσι η εξίσωση (2) μεγιστοποιείται όταν

$$l_i = \frac{r_i - r_{i-1} \cdot e^{-\frac{T_i}{K}}}{1 - e^{-\frac{T_i}{K}}} \cdot T_i = \frac{r_a - r_a \cdot e^{-\frac{T_i}{K}}}{1 - e^{-\frac{T_i}{K}}} \cdot T_i = r_a \cdot T_i, 2 \leq i \leq n$$

$$\sum_{i=1}^n l_i = l_1 + l_2 + \sum_{i=3}^n l_i$$

$$\begin{aligned} \text{Άρα έχουμε ότι : } &\leq l_{\max} + K \cdot r_a + \sum_{i=3}^n r_a \cdot T_i \\ &\leq l_{\max} + K \cdot r_a + (t'' - t') \cdot r_a \end{aligned}$$

Αφού όμως $(t'' - t') \cdot r_a$ είναι η υπηρεσία την οποία η ροή πρέπει να δεχθεί κατά τη διάρκεια του διαστήματος I, συνεπάγεται ότι η επιπλέον υπηρεσία είναι φραγμένη από το $l_{\max} + K \cdot r_a$.

Λήμμα 2

Θεωρούμε μια γραμμή με κανονικοποιημένο ρυθμό δικαιοσύνης a^u , και μια ροή με βάρος w , η οποία στέλνει με έναν ρυθμό όχι μεγαλύτερο από R , όπου $R > r_a$. Στη συνέχεια θεωρούμε ένα διάστημα $I = [t', t'')$ τέτοιο ώστε το t' να αντιπροσωπεύει το χρόνο ακριβώς μετά την άφιξη ενός πακέτου, κατά τη διάρκεια του οποίου ο υπολογιζόμενος ρυθμός r να μην είναι ποτέ μικρότερος από r_a , $r(t) \geq r_a, \forall t \in I$. Τότε, η επιπλέον υπηρεσία που λαμβάνεται από τη ροή κατά τη διάρκεια του χρονικού διαστήματος I είναι άνω φραγμένη από τη σχέση: $r_a \cdot K \cdot \ln\left(\frac{R}{r}\right)$, όπου $r_a = a^u \cdot w$.

Απόδειξη: Η απόδειξη είναι παρόμοια με αυτή του προηγούμενου λήμματος. Ξανά, υποθέτουμε ότι κατά τη διάρκεια του διαστήματος I η ροή στέλνει ακριβώς n πακέτα. Ομοίως, αφήνουμε ως t_i την άφιξη του i -στού πακέτου και ως l_i το μέγεθός του. Με αυτές τις υποθέσεις, όταν ο υπολογιζόμενος ρυθμός είναι μεγαλύτερος από r_a , τότε το i -στό πακέτο προωθείται με πιθανότητα $\frac{r_a}{r_i}$ και το πρόβλημα μπορεί να

ξαναδιατυπωθεί ως την εύρεση του: $\max(\sum_{i=1}^n l_i \frac{r_a}{r_i})$, (3) για τις τιμές $r_a \leq r_i \leq R$,

$1 \leq i \leq n$.

$$\frac{l_i}{r_i} = \frac{r_i - r_{i-1} \cdot e^{-\frac{T_i}{K}}}{r_i(1 - e^{-\frac{T_i}{K}})} \cdot T_i$$

Από την εξίσωση (1) έχουμε ότι:

$$= T_i + (1 - \frac{r_{i-1}}{r_i}) \cdot \frac{e^{-\frac{T_i}{K}}}{1 - e^{-\frac{T_i}{K}}} \cdot T_i, \quad 1 \leq i \leq n. \quad (4)$$

Εδώ σημειώνουμε, ότι σε αντίθεση με την αντίστοιχη σχέση (2) που είχαμε στο προηγούμενο λήμμα, η εξίσωση (3) ισχύει και όταν $i=1$. Και αυτό γιατί είμαστε βέβαιοι ότι έχει παραληφθεί τουλάχιστον ένα πακέτο πριν το t' και συνεπώς το T_i είναι καλά ορισμένο. Για να είμαστε πιο ακριβείς, από την υπόθεση έχουμε ότι $T_1 = t_1 - t_0 = t_1 - t'$. Υποθέτοντας ότι οι χρόνοι άφιξης των πακέτων είναι fixed, η

σχέση (3) ισοδυναμεί με την: $\max(\sum_{i=1}^n (1 - \frac{r_{i-1}}{r_i}) \cdot \beta_i)$, όπου $\beta_i = \frac{e^{-\frac{T_i}{K}} \cdot T_i}{(1 - e^{-\frac{T_i}{K}})}$.

Επιπλέον, υποθέτοντας ότι $K \gg T_i (1 \leq i \leq n)$, παίρνουμε ότι $\beta_i \cong K$, και η εξίσωση

(3) μεταβαίνει στην $\max \sum_{i=1}^n (1 - \frac{r_{i-1}}{r_i})$.

Δεδομένου ότι ο αριθμητικός μέσος είναι πάντα μεγαλύτερος ή ίσος από τον

γεωμετρικό μέσο, έχουμε ότι

$$\sum_{i=1}^n (1 - \frac{r_{i-1}}{r_i}) \leq n - n \cdot (\prod_{i=1}^n \frac{r_{i-1}}{r_i})^{\frac{1}{n}} \quad (5), \quad \text{όπου η τελευταία}$$

$$= n \cdot (1 - (\frac{r_0}{r_n})^{\frac{1}{n}}) \leq n(1 - (\frac{r_a}{R})^{\frac{1}{n}})$$

ανισότητα συνοδεύεται από την υπόθεση ότι $r_a \leq r_i \leq R, (1 \leq i \leq n)$.

Επιπλέον, μπορεί εύκολα να αποδειχθεί ότι $k(1 - (\frac{r_a}{R})^{\frac{1}{k}}) \leq \ln(\frac{R}{r_a}), \forall k \geq 1$. Για την

ακρίβεια, πρώτα δείχνουμε ότι $\ln(x) \geq 1 - \frac{1}{x}, \forall x \geq 1$, και μετά απλά αντικαθιστούμε

το x με $x = (\frac{R}{r_a})^{\frac{1}{k}}$. Επομένως η εξίσωση (5) μεταβαίνει στην $\sum_{i=1}^n (1 - \frac{r_{i-1}}{r_i}) \leq \ln \frac{R}{r_a}$ (6).

Τελικά με χρήση των εξισώσεων (4) και (6) καταλήγουμε στη σχέση

$$\sum_{i=1}^n l_i \cdot \frac{r_a}{r_i} \leq r_a \cdot \sum_{i=1}^n T_i + r_a \cdot K \cdot \ln(\frac{R}{r_a}) \leq r_a (t'' - t') + r_a \cdot K \cdot \ln \frac{R}{r_a} .$$

Δεδομένου ότι το $(t'' - t') \cdot r_a$ αντιπροσωπεύει ακριβώς τον αριθμό των bits που η ροή δικαιούται να στείλει κατά τη διάρκεια του διαστήματος I , το λήμμα αποδεικνύεται.

Θεώρημα 1

Θεωρούμε μια γραμμή με κανονικοποιημένο ρυθμό δικαιοσύνης a^u , και μια ροή με βάρος w . Τότε, η επιπλέον υπηρεσία που θα λάβει η ροή με βάρος w , η οποία στέλνει σε έναν ρυθμό όχι μεγαλύτερο από R είναι άνω φραγμένη από τη σχέση:

$$r_a \cdot K \cdot (1 + \ln \frac{R}{r_a}) + l_{\max}, \text{ όπου } r_a = a^u \cdot w, \text{ και } l_{\max} \text{ αντιπροσωπεύει το μέγιστο μέγεθος}$$

του πακέτου.

Απόδειξη: Υποθέτουμε ότι η ροή μας ενεργοποιείται για πρώτη φορά τη χρονική στιγμή t_0 . Αν t_1 είναι η χρονική στιγμή όπου ο υπολογιζόμενος ρυθμός ξεπερνάει για πρώτη φορά την τιμή $r_a, r(t_1) > r_a$ και $r(t) \leq r_a, \forall t < t_1$. Αν η χρονική στιγμή t_1 δεν υπάρχει, τότε σύμφωνα με το λήμμα 1 η επιπλέον υπηρεσία που λαμβάνεται από τη ροή είναι φραγμένη από την τιμή $r_a \cdot K$, κάτι που αποτελεί και απόδειξη για αυτήν την περίπτωση. Στη συνέχεια θεωρούμε ότι η χρονική στιγμή t_1 υφίσταται.

Παρακάτω, δείχνουμε ότι η επιπλέον υπηρεσία που λαμβάνει η ροή μεγιστοποιείται όταν $r(t) \geq r_a, \forall t > t_1$. Υποθέτουμε ότι υπάρχει ένα διάστημα $I' = [t', t''] \subset I$, τέτοιο ώστε $t' \geq t_1$, και $r(t) < r_a, \forall t \in I'$. Προχωρώντας με τον ίδιο τρόπο σε κάθε υποδιάστημα I' στο οποίο ο υπολογιζόμενος ρυθμός είναι μικρότερος από r_a ,

υποθέτουμε πως έχουμε μια νέα διαδικασία άφιξης, υπό την οποία η ροή δέχεται επιπλέον υπηρεσία. Όμως τότε, σύμφωνα με το λήμμα 2, η επιπλέον υπηρεσία που λαμβάνεται από τη ροή μετά τη χρονική στιγμή t_1 είναι φραγμένη από τη σχέση:

$$r_a \cdot K \cdot \ln \frac{R}{r_a} \quad (7).$$

Ομοίως από το λήμμα 1 συνεπάγεται ότι η επιπλέον υπηρεσία που λαμβάνεται από τη ροή κατά τη διάρκεια του διαστήματος $[t_0, t_1)$ είναι άνω φραγμένη από τη σχέση:

$$r_a \cdot K + l_{\max} \quad (8),$$

και συνεπώς συνεπώς συνδυάζοντας τις σχέσεις (7) και (8) παίρνουμε ότι η συνολική επιπλέον υπηρεσία είναι φραγμένη από τη σχέση:

$$r_a \cdot K \cdot \left(1 + \ln \frac{R}{r_a}\right) + l_{\max}.$$

8.2. Παράρτημα Β – Συμπεριφορά του πρωτοκόλλου TCP RENO

Ένα σημαντικό ποσοστό της σημερινής κίνησης του Internet, συμπεριλαμβανομένου του WWW (HTTP), του email (SMTP), της μεταφοράς αρχείων (FTP), και της απομακρυσμένης πρόσβασης (telnet), μεταφέρεται πάνω από το πρωτόκολλο μεταφοράς TCP. Παραδοσιακά, οι εξομοιώσεις και οι μετρήσεις αποτελούσαν τα εργαλεία για την εξέταση της απόδοσης του πρωτοκόλλου TCP. Ωστόσο, πρόσφατα, αρκετές προσπάθειες κατευθύνονται στον αναλυτικό χαρακτηρισμό της απόδοσης (throughput) των μηχανισμών ελέγχου συμφόρησης του TCP, ως συνάρτηση του ποσοστού απωλειών πακέτων (packet loss) και του round trip delay. Το μοντέλο αυτό, περικλείει όχι μόνο τη συμπεριφορά του μηχανισμού γρήγορης επαναμετάδοσης του TCP (fast retransmit mechanism), αλλά και τα αποτελέσματα που φέρει ο μηχανισμός λήξης χρόνου (timeout mechanism) στην απόδοση (throughput). Από συγκρίσεις που έχουν γίνει ανάμεσα σε αυτό και σε άλλα μοντέλα, συμπεραίνουμε ότι το μοντέλο αυτό είναι ικανό να προβλέψει την απόδοση (TCP throughput) με μεγαλύτερη ακρίβεια, καθώς και να χρησιμοποιηθεί πάνω από μια αρκετούς διαφορετικούς ρυθμούς απωλειών.

Ανάπτυξη του μοντέλου όσον αφορά τον έλεγχο συμφόρησης

Το TCP είναι ένα πρωτόκολλο, το οποίο μπορεί να υιοθετήσει σύνθετη συμπεριφορά, ειδικότερα στα πλαίσια του σημερινού Διαδικτύου, όπου οι συνθήκες κίνησης μπορεί να είναι από μόνες τους αρκετά πολύπλοκες. Παρακάτω, εστιάζουμε την προσοχή μας στους μηχανισμούς αποφυγής συμφόρησης του TCP και στις επιδράσεις τους στην απόδοση (throughput), λαμβάνοντας υπόψη την εξάρτηση της αποφυγής συμφόρησης στα ACK πακέτα, τον τρόπο με τον οποίο η απώλεια πακέτων γνωστοποιείται (είτε με διπλή ανίχνευση ACK πακέτου και γρήγορη επαναμετάδοση, είτε με λήξη του διαθέσιμου χρόνου), περιοριζόμενοι από το μέγεθος παραθύρου του παραλήπτη (receiver window size), και τον average round trip time (RTT). Το μοντέλο μας εστιάζεται στους μηχανισμούς αποφυγής συμφόρησης του TCP, όπου το μέγεθος παραθύρου W του πρωτοκόλλου TCP, αυξάνεται κατά την τιμή $1/W$, κάθε φορά που έρχεται ένα ACK πακέτο. Αντιθέτως, το μέγεθος παραθύρου μειώνεται κάθε φορά που ανιχνεύεται η απώλεια ενός πακέτου, με το ποσοστό της μείωσης να καθορίζεται από το αν η απώλεια πακέτου οφείλεται σε λήψη διπλών ACK πακέτων, ή στη λήξη του διαθέσιμου χρόνου.

Μοντελοποιούμε τον μηχανισμό αποφυγής συμφόρησης του πρωτοκόλλου IP, με βάση διαδικασίες που επαναλαμβάνονται, όπως φαίνεται παρακάτω. Ένας γύρος ξεκινάει με την συνεχόμενη μετάδοση W πακέτων, όπου W είναι το τωρινό μέγεθος παραθύρου. Όταν όλα τα πακέτα αυτού του γύρου αποσταλούν, τότε δεν αποστέλλονται άλλα πακέτα μέχρι την λήψη του πρώτου ACK πακέτου, που αναφέρεται στα προηγούμενα W . Η λήψη αυτού του ACK πακέτου, σηματοδοτεί το τέλος του προηγούμενου γύρου και την έναρξη ενός καινούριου. Στο μοντέλο αυτό, η διάρκεια ενός γύρου είναι ίση με το round trip time, και υποθέτουμε πως είναι ανεξάρτητη από το μέγεθος παραθύρου. Ακόμη, υποθέτουμε πως ο χρόνος που απαιτείται για να αποσταλούν τα πακέτα ενός παραθύρου είναι μικρότερος από το round trip time.

Κατά την εκκίνηση του επόμενου γύρου, αποστέλλονται W' νέα πακέτα, όπου W' είναι το νέο μέγεθος παραθύρου. Έστω b ο αριθμός των πακέτων που επιβεβαιώνεται ότι στάλθηκαν σωστά με την λήψη ενός ACK (συνήθως $b=2$). Αν κατά τον πρώτο γύρο στάλθηκαν W πακέτα και όλα επαληθεύθηκαν σωστά, τότε λήφθηκαν W/b ACKs. Δεδομένου ότι το κάθε πακέτο ACK αυξάνει το μέγεθος παραθύρου κατά $1/W$, τότε το μέγεθος παραθύρου κατά την εκκίνηση του δεύτερου γύρου είναι $W' = W + \frac{1}{b}$. Επομένως, εφόσον δεν υπάρχει συμφόρηση και δεν έχουμε

απώλειες πακέτων, το μέγεθος παραθύρου αυξάνεται γραμμικά συναρτήσει του χρόνου, με ρυθμό $1/b$ πακέτα ανά round trip time. Αν όμως δεν έχουμε επιβεβαίωση όλων των πακέτων τότε ανάλογα με την αιτία που την προκάλεσε λειτουργούμε ανάλογα:

➤ Αν έχουμε λήψη τεσσάρων ACKs με τον ίδιο αριθμό πακέτου, τότε μειώνουμε το μέγεθος του παραθύρου στο μισό ($W' = \left\lceil \frac{W}{2} \right\rceil$) και συνεχίζουμε όπως προηγουμένως.

Αν έχουμε λήξη του χρόνου αναμονής (timeout), τότε θέτουμε το μέγεθος παραθύρου ίσο με ένα ($W=1$) και συνεχίζουμε όπως προηγουμένως. Εφόσον όμως, παρατηρηθεί εκ νέου λήξη του χρόνου αναμονής, πριν μεταδοθεί το καινούριο πακέτο, τότε ο χρόνος αυτός διπλασιάζεται.