

Αθανάσης Καρούλης
Β' εξάμηνο MIS

Διαδικτυακά Πρωτόκολλα Ροής
(Streaming Protocols)
RTP και RTSP

Β' εργασία στα
Δίκτυα Υπολογιστών

Καθ. Αν. Οικονομίδης

Ιανουάριος 2001

Με την παρούσα εργασία γίνεται μια προσπάθεια να περιγραφεί το υπόβαθρο αλλά και να παρουσιαστούν πρακτικές λύσεις για τη μετάδοση βίντεο και ήχου σε πραγματικό χρόνο μέσω δικτύου υπολογιστών. Στόχος της δεν είναι η εις βάθος ανάλυση του τεχνικού υποβάθρου που κρύβεται πίσω από τους διάφορους τρόπους μετάδοσης, αλλά κυρίως το να προτείνει λύσεις για τις διάφορες ανάγκες αποστολής κινούμενης εικόνας και ήχου σε πραγματικό χρόνο. Ωστόσο κρίνεται απαραίτητη η τεχνική αναφορά έτσι ώστε να μπορούν να δικαιολογηθούν οι διάφορες προτάσεις για τις ανάλογες ανάγκες.

Λέγοντας ανάγκες προσδιορίζουμε γενικά τις διάφορες εκείνες δραστηριότητες οι οποίες κάνουν χρήση της μετάδοσης και θέασης βίντεο σε πραγματικό χρόνο. Όπως γίνεται εύκολα αντιληπτό αυτές οι δραστηριότητες είναι αριθμητικά πάρα πολλές (π.χ. εκπαίδευση από απόσταση, ραδιοφωνικές και τηλεοπτικές εκπομπές, τηλεδιάσκεψη κλπ.) και με διαφορετικές απαιτήσεις η κάθε μια. Ωστόσο μπορούμε γενικά να τις κατατάξουμε σε δύο κατηγορίες:

- α). Σε αυτές που απαιτούν μετάδοση αποθηκευμένου βίντεο.
- β). Σε αυτές που απαιτούν ζωντανή (on the fly) μετάδοση.

Για τη δικτυακή μετάδοσή τους και οι δύο αυτές κατηγορίες χρησιμοποιούν την ίδια τεχνολογία που λέγεται streaming.

Ένας άτυπος ορισμός για το streaming είναι ο εξής: *Streaming είναι ένα ρεύμα σταθερής ή μεταβλητής ροής δεδομένων μεταξύ δύο ή περισσότερων συμβαλλομένων μερών.* Η έννοια του streaming είναι γνωστή και από άλλες εφαρμογές όπως ο αντικειμενοστραφής προγραμματισμός και τα λειτουργικά συστήματα. Η μετάδοση βίντεο ωστόσο μέσω δικτύου υπολογιστών θα ήταν αδύνατο να πραγματοποιηθεί βασισμένη μόνο στο streaming λόγω του ότι το βίντεο είναι ίσως η πιο ογκώδης από άποψη δεδομένων και απαιτητική σε πόρους εφαρμογή. Έτσι επινοήθηκαν διάφορες μέθοδοι συμπίεσης κινούμενης εικόνας και ήχου βασισμένες στη φυσιολογία και την απόκριση των ανθρωπίνων οργάνων και του εγκεφάλου, όπως το ότι η ανθρώπινη όραση μπορεί να

αντιληφθεί περίπου μέχρι 16,7 εκατομμύρια χρώματα, το ότι είναι δύσκολο να γίνουν αντιληπτές οι ποιοτικές διαφορές σε κινούμενη εικόνα με πάνω από δεκαπέντε καρέ το δευτερόλεπτο, ή το ότι η ανθρώπινη ακοή δεν είναι σε θέση να διαχωρίσει τους κοντινούς συχνοτικά ήχους που αλληλοκαλύπτονται. Εκτός αυτών, κάνοντας και χρήση πολύπλοκων μαθηματικών εργαλείων όπως ο διακριτός συνημιτονοειδής μετασχηματισμός (DCT) κατέστη δυνατόν να απομακρύνεται μεγάλη ποσότητα άχρηστων δεδομένων με αποτέλεσμα την συρρίκνωση του βίντεο από άποψη όγκου δεδομένων. Αυτοί οι αλγόριθμοι όμως είναι αρκετά πολύπλοκοι με αποτέλεσμα να είναι αρκετά απαιτητικοί σε υπολογιστικούς πόρους με αντάλλαγμα βέβαια την κατά πολλές τάξεις μεγέθους μικρότερη απαίτηση της δικτυακής μετάδοσης του βίντεο σε εύρος ζώνης (bandwidth), χωρίς ωστόσο να δίνουν ακόμα την δυνατότητα για καλής ποιότητας βίντεο σε δίκτυα με μικρό εύρος ζώνης όπως είναι στο μεγαλύτερο μέρος του το περισσότερο χρησιμοποιούμενο δίκτυο, το Internet.

Κατόπιν τούτων και αφού ορίσαμε τις βάσεις πάνω στις οποίες στηρίζεται η δικτυακή μετάδοση βίντεο σε πραγματικό χρόνο ξεκινάμε την περιήγηση στα ενδότερα αυτής της τεχνολογίας.

Διαδικτυακά Streaming Πρωτόκολλα.

Οι streaming εφαρμογές είναι χτισμένες κατά βάση πάνω στο IP. Είναι φυσιολογικό λοιπόν να χρησιμοποιούνται πρωτόκολλα που να βασίζονται πάνω σε ή να κάνουν χρήση γνωστών πρωτοκόλλων. Για τις απαιτήσεις των εφαρμογών streaming δημιουργήθηκαν ξεχωριστά πρωτόκολλα επικοινωνίας που προσφέρουν καλύτερο έλεγχο και διαχείριση στα δεδομένα των μέσων που μεταφέρουν, με μειωμένο κόστος επιβάρυνσης επικεφαλίδας (*overhead*). Άλλα από αυτά τα πρωτόκολλα είναι τυποποιημένα από διεθνείς οργανισμούς όπως είναι τα RTP (Real Time Protocol), RTCP (Real Time Control Protocol), RTSP (Real Time Streaming Protocol) και multicasting IP (τυποποιημένα από τους Internet Engineering Task Force και Network Working Group) ενώ άλλα από αυτά είναι ξεχωριστές προτάσεις από ιδιωτικές επιχειρήσεις όπως είναι τα PNA και RDT της REAL inc. Τα περισσότερα από αυτά τα πρωτόκολλα βασίζονται πάνω στο γνωστό, μη απαιτήσης σύνδεσης (*connectionless*) και αναξιόπιστο (*unreliable*) πρωτόκολλο UDP (User Datagram Protocol) το οποίο δεν κάνει έλεγχο επαναμετάδοσης των χαμένων πακέτων (Tanenbaum, 1992). Το κύριο πλεονέκτημα αυτής της προσέγγισης είναι η μικρή επιβάρυνση στην επικεφαλίδα (*overhead*) ενώ το μειονέκτημά της είναι ο περιορισμένος έλεγχος που προσφέρει, κάτι όμως που δεν είναι τόσο κρίσιμο για αυτού του είδους τα δεδομένα.

Παρακάτω θα περιγράψουμε τον τρόπο λειτουργίας καθώς και τις υπηρεσίες που προσφέρουν τα πιο διαδεδομένα από αυτά τα πρωτόκολλα χωρίς να υπεισέλθουμε σε περιγραφή των τεχνικών χαρακτηριστικών και της δομής τους.

Το Πρωτόκολλο RTP (Real Time Protocol).

1. Γενική περιγραφή.

Αυτό το πρωτόκολλο που τοποθετείται στο επίπεδο μεταφοράς παρέχει συνεχείς δικτυακές λειτουργίες μεταφοράς, κατάλληλες για εφαρμογές που μεταδίδουν δεδομένα σε πραγματικό χρόνο όπως είναι ο ήχος, το βίντεο και η προσομοίωση δεδομένων πάνω σε multicast¹ (πολλαπλή μετάδοση: Μετάδοση ενός αντιγράφου ιδίων δεδομένων από τον server σε κάθε κλαδί του δικτύου) ή unicast (μετάδοση του stream από τον εξυπηρέτη (server) σε έναν συγκεκριμένο πελάτη (client)) δικτυακές υπηρεσίες. Το RTP δεν καταγράφει την δέσμευση των πόρων και δεν εγγυάται ποιότητα υπηρεσίας - QoS (Quality of Service) - για τις πραγματικού χρόνου υπηρεσίες. Η μεταφορά δεδομένων βελτιώνεται από ένα πρωτόκολλο ελέγχου το RTCP (Real Time Control Protocol) έτσι ώστε να υπάρχει η παρακολούθηση της παράδοσης των δεδομένων με έναν κλιμακούμενο τρόπο ανάλογα με το μέγεθος του multicast δικτύου, και να προσφέρεται κάποιο μικρό ποσοστό ελέγχου καθώς και λειτουργία αναγνώρισης. Τα RTP και RTCP έχουν σχεδιαστεί έτσι ώστε να είναι ανεξάρτητα από τα υποκείμενα² επίπεδα μεταφοράς και δικτύου. Το πρωτόκολλο υποστηρίζει τη χρήση, σε RTP επίπεδο, μικτών και μεταφραστών, έννοιες που θα εξηγηθούν παρακάτω.

2. Αναλυτική περιγραφή.

Υπηρεσίες όπως ο διαλογικός ήχος και βίντεο (interactive audio και video) περιλαμβάνουν την αναγνώριση του τύπου φορτίου (payload type), την αρίθμηση της ακολουθίας δεδομένων (sequence numbering), την τοποθέτηση χρονοσφραγίδων (timestamping) και την παρακολούθηση της παράδοσης των δεδομένων. Οι εφαρμογές τρέχουν τυπικά το RTP πάνω από το UDP έτσι ώστε να χρησιμοποιήσουν τις υπηρεσίες πολυπλεξίας (multiplexing) και αθροίσματος ελέγχου (checksum) που αυτό προσφέρει. Και τα δυο πρωτόκολλα συνεισφέρουν μέρος της λειτουργικότητας του πρωτοκόλλου μεταφοράς. Ωστόσο το RTP μπορεί να χρησιμοποιηθεί και με άλλα κατάλληλα, υποκείμενα πρωτόκολλα δικτύου ή μεταφοράς. Το RTP υποστηρίζει τη μεταφορά δεδομένων σε

¹ Multicast: Σύμφωνα με τον Tannenbaum (1992) ο όρος multicast ορίζεται ως «πολλαπλή αποστολή». Είναι δε υποσύνολο της κατηγορίας δικτύων broadcast δηλ. δικτύων που μεταδίδουν μέσω ενός κοινού καναλιού. Η διαφορά μεταξύ multicast και broadcast δικτύων έγκειται στο ότι τα πρώτα υποστηρίζουν μετάδοση σε ένα υποσύνολο των μηχανημάτων του δικτύου. (βλ. σ. 9 – 11 του βιβλίου Δίκτυα Υπολογιστών).

² Χρησιμοποιείται για την επεξήγηση του underlying δηλ. αυτό που κείται κάτω από κάτι άλλο.

πολλαπλούς προορισμούς χρησιμοποιώντας multicast διανομή αν αυτό παρέχεται από το υποκείμενο δίκτυο.

Να σημειωθεί ότι το RTP δεν προσφέρει κάποιον μηχανισμό που να εγγυάται την έγκαιρη παράδοση ή να προσφέρει άλλη QoS εγγύηση, αλλά βασίζεται αυτές οι λειτουργίες να προσφέρονται από τις υπηρεσίες των κατωτέρων επιπέδων. Επίσης δεν παρέχει εγγύηση για την παράδοση, ούτε εμποδίζει την εκτός χρόνου παράδοση όπως επίσης υποθέτει ότι το υποκείμενο δίκτυο είναι αξιόπιστο και παραδίδει τα πακέτα με τη σωστή σειρά. Οι αριθμοί σειράς που περιέχονται στο RTP επιτρέπουν στον αποδέκτη να επαναδομεί τα σειριοποιημένα πακέτα του μεταδότη, μπορούν όμως να χρησιμοποιηθούν και για τον καθορισμό της σωστής τοποθέτησης ενός πακέτου όπως για παράδειγμα στην αποκωδικοποίηση video όπου δεν είναι απαραίτητη η αποκωδικοποίηση των πακέτων με τη σωστή σειρά.

Το RTP αποτελείται από δυο στενά συνδεδεμένα μέρη:

- A) Το real-time transport protocol (RTP) για την μεταφορά των δεδομένων που έχουν ιδιότητες πραγματικού χρόνου και
- B) Το RTP πρωτόκολλο ελέγχου (RTCP, Real Time Control Protocol) για την παρακολούθηση της ποιότητας υπηρεσιών και την μεταγωγή πληροφοριών σχετικά με τους συμμετέχοντες σε μια διεξαγόμενη συνεδρία. Η τελευταία ιδιότητα του RTCP μπορεί να είναι επαρκής για χαλαρά ελεγχόμενες συνόδους.

Το RTP αντιπροσωπεύει ένα νέου τύπου πρωτόκολλο που ακολουθεί τις αρχές της πλαισίωσης του επιπέδου εφαρμογής και της ολοκληρωμένης επεξεργασίας του επιπέδου (Clark & Tennenhouse, 1990.). Αυτό συνεπάγεται ότι το RTP στοχεύει να είναι προσαρμόσιμο έτσι ώστε να παρέχει τις πληροφορίες που απαιτούνται από μια συγκεκριμένη εφαρμογή και που θα ολοκληρώνεται (εμπεδώνεται) κατά την επεξεργασία της εφαρμογής παρά να υλοποιείται ως ξεχωριστό επίπεδο. Το RTP είναι ένα σχέδιο πρωτοκόλλου που είναι οικειοθελώς ανολοκλήρωτο. Σε αντίθεση με τα συνηθισμένα πρωτόκολλα όπου οι πρόσθετες λειτουργίες μπορούν να διευθετηθούν με την κατασκευή του πρωτοκόλλου έτσι ώστε να είναι πιο γενικό ή την προσθήκη εναλλακτικών μηχανισμών που θα απαιτούν parsing³, το RTP σκοπεύει να προσαρμόζεται με την μετατροπή και / ή την προσθήκη στις επικεφαλίδες (headers) όπου αυτό χρειάζεται.

Για αυτόν το λόγο μια πλήρης περιγραφή του RTP για μια συγκεκριμένη εφαρμογή θα χρειαζόταν συνοδευτικά έγγραφα όπως:

- ◆ Ένα έγγραφο περιγραφής του προφίλ της εφαρμογής που θα καθορίζει τους κωδικούς του τύπου φορτίου και την χαρτογράφηση της μορφής των φορτίων (payload) (όπως για παράδειγμα την κωδικοποίηση των μέσων). Το προφίλ μπορεί ακόμα να καθορίζει τις

³ Parsing: είναι κατά μια έννοια η διερμηνεία κάποιου κώδικα που πρώτα έχει μεταφραστεί σε κάποια ενδιάμεση, κατώτερου επιπέδου μορφή. Για πληροφορίες δείτε Java parsing στο Java tutorial.

επεκτάσεις ή τις διαφοροποιήσεις του RTP που είναι εξειδικευμένες για ξεχωριστής κατηγορίας εφαρμογές. Τυπικά μια εφαρμογή θα λειτουργεί σύμφωνα με ένα μοναδικό προφίλ.

- ◆ Έγγραφα περιγραφής των προδιαγραφών της μορφής του payload τα οποία και θα ορίζουν πώς ένα συγκεκριμένο payload, όπως η κωδικοποίηση ήχου και βίντεο, θα μεταφερθεί μέσω του RTP.

Σχετικά με τις υλοποιήσεις real – time υπηρεσιών και αλγορίθμων καθώς και αποφάσεις για τον σχεδιασμό του RTP μπορούν να βρεθούν στα Schulzrinne (1996) και Schulzrinne et al. (1996).

Μέχρι σήμερα έχουν δημιουργηθεί αρκετές εφαρμογές σύμφωνα με αυτές τις προδιαγραφές. Ωστόσο, το υπάρχον Internet δεν μπορεί να υποστηρίξει ακόμα την πλήρη δυνατή απαίτηση για υπηρεσίες πραγματικού χρόνου. Υπηρεσίες υψηλού εύρους ζώνης που χρησιμοποιούν το RTP, όπως το βίντεο, μπορούν να μειώσουν σημαντικά το QoS άλλων δικτυακών υπηρεσιών.

3. Τυπικά παραδείγματα χρήσης του RTP.

Τα παραδείγματα που ακολουθούν έχουν επιλεγεί έτσι ώστε να επιδειχθούν οι βασικές λειτουργίες των εφαρμογών που κάνουν χρήση του RTP. Σ' αυτά, το RTP είναι υλοποιημένο στην κορυφή των IP και UDP και ακολουθεί τις αρχές που έχουν δημιουργηθεί από τον καθορισμό του προφίλ για audio και video.

3.1. Απλή multicast συνδιάσκεψη μόνο με ήχο (Simple Multicast Audio Conference).

Σ' αυτό το παράδειγμα υποτίθεται ότι γίνεται τηλεδιάσκεψη μόνο με ήχο μεταξύ πολλών μερών χρησιμοποιώντας τις IP multicast υπηρεσίες του Internet για φωνητικές επικοινωνίες. Ο επικεφαλής της συνδιάσκεψης, δεσμεύει ένα σύνολο multicast διευθύνσεων και ένα ζευγάρι θυρών (ports), μέσω ενός μηχανισμού δέσμευσης πόρων. Η μία θύρα χρησιμοποιείται για τα δεδομένα ήχου και η άλλη για τον έλεγχο των πακέτων (προφανώς με το RTCP). Αυτές οι πληροφορίες διεύθυνσης και θυρών διανέμονται στους συμμετέχοντες. Στην περίπτωση που είναι επιθυμητή η μυστικότητα, τα πακέτα δεδομένων και ελέγχου μπορούν να κρυπτογραφηθούν χρησιμοποιώντας κάποια από τις γνωστές μεθόδους κρυπτογράφησης (συνήθως χρησιμοποιείται ο αλγόριθμος DES), στην οποία περίπτωση χρειάζεται να δημιουργηθεί και να διανεμηθεί και το κλειδί της κρυπτογράφησης.

Η εφαρμογή τηλεδιάσκεψης με ήχο (audio conferencing) που χρησιμοποιείται από κάθε συμβαλλόμενο μέρος, στέλνει δεδομένα ήχου σε μικρά κομμάτια, υποθετικά διάρκειας των 20 ms. Σε καθένα από αυτά τα κομμάτια προστίθεται στην αρχή η RTP επικεφαλίδα. Η RTP επικεφαλίδα (header) και τα δεδομένα περιλαμβάνονται διαδοχικά σε κάποιο πακέτο UDP. Η RTP επικεφαλίδα υποδεικνύει ποιος είναι ο τύπος της κωδικοποίησης ήχου (π.χ. PCM, ADPCM, LPC, κλπ.) σε κάθε πακέτο έτσι ώστε οι αποστολείς να μπορούν να αλλάξουν την κωδικοποίηση κατά τη διάρκεια μιας

διάσκεψης, όπως για παράδειγμα στην περίπτωση που πρέπει να προσθέσουν κάποιον νέο συμμετέχοντα που συνδέεται μέσω μιας χαμηλής σε εύρος ζώνης (bandwidth) σύνδεσης, ή στην περίπτωση που πρέπει να αντιδράσει η εφαρμογή λόγω ενδείξεων συμφόρησης του δικτύου.

Το Internet όπως και άλλα δίκτυα μεταγωγής πακέτου, χάνει και επαναδιατάσσει πακέτα κατά διαστήματα και τα καθυστερεί με μεταβλητό χρονικό κόστος. Για να αντιμετωπιστούν αυτά τα προβλήματα η RTP επικεφαλίδα περιέχει πληροφορίες συγχρονισμού και έναν αριθμό σειράς που επιτρέπουν στους αποδέκτες την επαναδόμηση του συγχρονισμού που παράγεται από την πηγή. Στην περίπτωσή μας, τα κομματάκια του ήχου παίζονται πολύ κοντά από το ηχείο του υπολογιστή, κάθε 20 ms. Αυτή η επαναδόμηση του χρονισμού διεξάγεται ξεχωριστά για κάθε πηγή RTP πακέτων που συμμετέχει στην διάσκεψη. Ο αριθμός σειράς μπορεί επίσης να χρησιμοποιηθεί από τον αποδέκτη στον υπολογισμό των χαμένων πακέτων.

Εφόσον τα μέλη της συνδιάσκεψης βγαίνουν ή εισέρχονται κατά τη διάρκεια διεξαγωγής της είναι χρήσιμο να γνωρίζουμε κάθε στιγμή ποιοί συμμετέχουν και πόσο καλά λαμβάνουν τα δεδομένα ήχου. Για αυτόν το σκοπό κάθε οντότητα της εφαρμογής ήχου που χρησιμοποιείται από τους συμμετέχοντες, μεταδίδει περιοδικά στην RTCP θύρα ελέγχου μια αναφορά λήψης και το όνομα του κάθε χρήστη. Η αναφορά λήψης υποδεικνύει πόσο καλά λαμβάνεται ο εκάστοτε ομιλητής και μπορεί να χρησιμοποιηθεί για να ελέγξει τις προσαρμόσιμες κωδικοποιήσεις. Επίσης μπορούν να χρησιμοποιηθούν και άλλες πληροφορίες αναγνώρισης, εκτός του ονόματος χρήστη, αναφορικά με τον έλεγχο των ορίων του εύρους ζώνης.

Ένας συμμετέχων στέλνει ένα RTCP BYE πακέτο όταν αφήνει την συνδιάσκεψη.

3.2. Απλή multicast συνδιάσκεψη με βίντεο και ήχο (Simple Multicast Audio and Video Conference).

Ας εξετάσουμε τώρα την περίπτωση όπου η συνδιάσκεψη γίνεται και με βίντεο. Σ' αυτή την περίπτωση το κάθε μέσο (ήχος, βίντεο) μεταδίδεται ως ξεχωριστή RTP συνεδρία (session) και τα RTCP πακέτα μεταδίδονται για κάθε μέσο χρησιμοποιώντας δύο ξεχωριστά UDP ζεύγη θυρών και/ή multicast διευθύνσεων. Δεν υπάρχει απευθείας σύζευξη μεταξύ των αντικειμένων ήχου και βίντεο στο επίπεδο RTP εκτός του ότι ο συμμετέχων χρήστης και στα δύο αυτά sessions χρησιμοποιεί το ίδιο διακεκριμένο όνομα και για τα δύο RTCP πακέτα που χρησιμοποιούνται για κάθε session, κάτι που οδηγεί στην αντιστοίχιση των δύο αυτών sessions.

Ο λόγος που αντιμετωπίζουμε τα δύο μέσα ως ξεχωριστές συνεδρίες είναι ότι θέλουμε να επιτρέψουμε στους χρήστες να μπορούν να επιλέξουν αν θέλουν να χρησιμοποιήσουν ένα μόνο μέσο (audio ή video) αν όχι και τα δύο ταυτόχρονα. Αυτό είναι χρήσιμο στην περίπτωση που κάποιος συμμετέχων είναι συνδεδεμένος με χαμηλού εύρους ζώνης σύνδεση ή στην περίπτωση όπου υπάρχει φόρτος στο δίκτυο. Παρά αυτόν τον διαχωρισμό είναι δυνατόν να επιτευχθεί

συγχρονισμός μεταξύ ήχου και βίντεο κατά την αναπαραγωγή τους χρησιμοποιώντας πληροφορίες χρονισμού που θα μεταφέρονται μέσω των RTCP πακέτων ξεχωριστά για κάθε μέσο.

3. Μίκτες και μεταφραστές (mixers and translators).

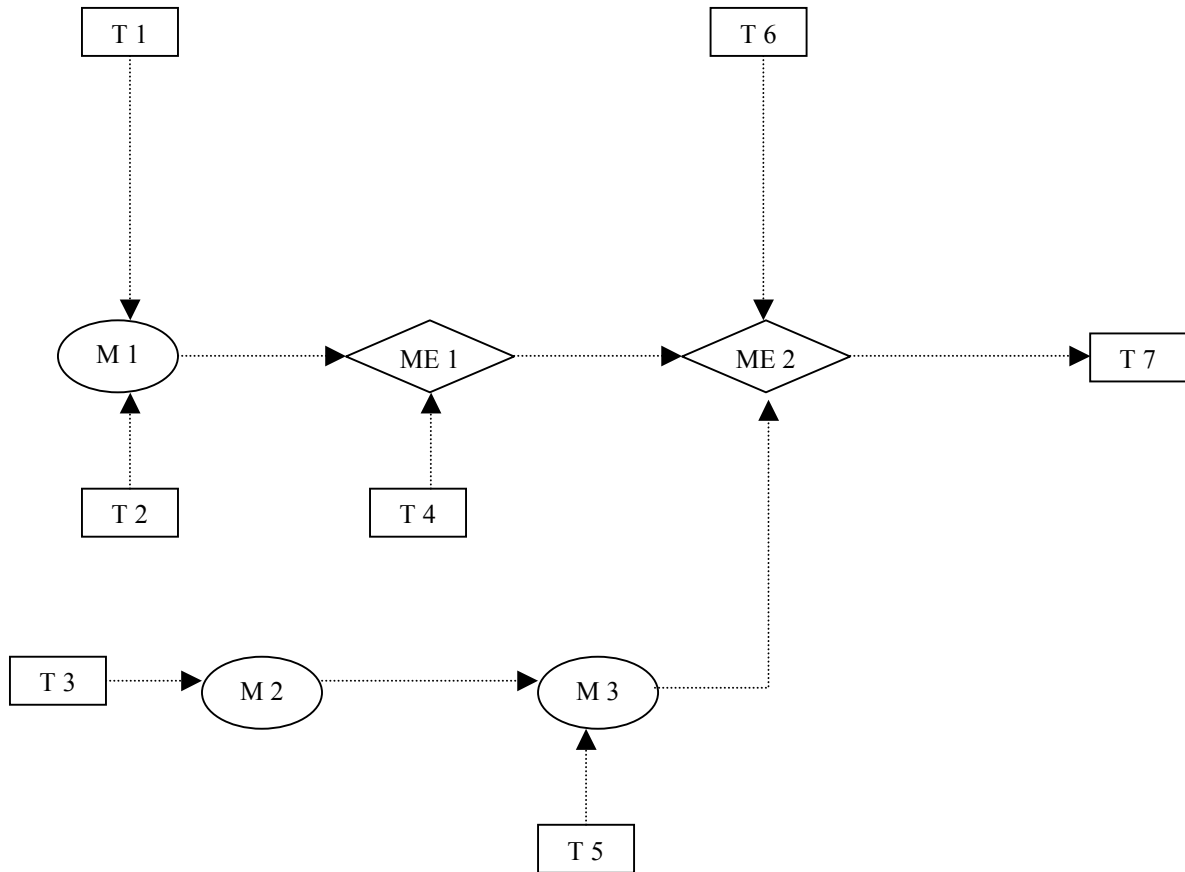
α) Μέχρι τώρα υποθέσαμε ότι όλοι οι συμμετέχοντες θέλουν να λαμβάνουν δεδομένα της ίδιας μορφής κάτι που στην πραγματικότητα δεν συμβαίνει συχνά. Ας υποθέσουμε την περίπτωση όπου κάποια μέρη συνδέονται μέσω χαμηλής ταχύτητας σύνδεσης τη στιγμή που η πλειοψηφία των συμμετεχόντων στη συνδιάσκεψη συνδέονται χρησιμοποιώντας υψηλές ταχύτητες. Σε αντιδιαστολή με το να υποχρεώσουμε τον καθένα στην χρήση χαμηλής ταχύτητας έτσι ώστε όλοι να λαμβάνουν τα ίδια, χαμηλής ποιότητας βίντεο ή ήχου δεδομένα, μπορεί να τοποθετηθεί κοντά στις περιοχές χαμηλού εύρους ένας αναμεταδότης RTP επιπέδου που ονομάζεται μίκτης. Αυτός ο μίκτης επανασυγχρονίζει τα εισερχόμενα πακέτα έτσι ώστε να επαναδομούνται τα σταθερής διάρκειας χρονικά διαστήματα που παράγονται στον αποστολέα (π.χ. στο προηγούμενο παράδειγμα το χρονικό διάστημα ήχου σε κάθε πακέτο ήταν 20 ms). Κατόπιν συγχωνεύει αυτά τα επαναδομημένα ρεύματα (streams) σε ένα ενιαίο ρεύμα, μεταφράζει την κωδικοποίηση σε μια αντίστοιχη χαμηλότερου εύρους (π.χ. PCM, σε MP3) και διαβιβάζει αυτά τα χαμηλού εύρους, ρεύματα κατά μήκος του χαμηλής ταχύτητας δικτύου. Αυτά τα πακέτα μπορούν να μεταδοθούν σε έναν μοναδικό αποδέκτη ή σε πολλαπλούς αποδέκτες σε μια διαφορετική διεύθυνση (multicasting). Η RTP επικεφαλίδα περιέχει τα μέσα για να αναγνωρίζουν οι μίκτες τις πηγές που συνεισφέρουν σε ένα μιξαρισμένο πακέτο έτσι ώστε να μπορεί να παρασχεθεί στους αποδέκτες η σωστή ένδειξη του ομιλητή.

β) Από την άλλη μεριά κάποιοι συμμετέχοντες στην διάσκεψη μπορεί να είναι συνδεδεμένοι με υψηλές ταχύτητες που ωστόσο μπορεί να μην είναι απευθείας προσβάσιμοι μέσω IP multicast. Για παράδειγμα μπορεί να βρίσκονται πίσω από κάποιο φράγμα (firewall) επιπέδου εφαρμογής που να μην επιτρέπει την είσοδο σε οποιοδήποτε IP πακέτο. Για αυτά τα sites ενδέχεται η μίξη να μην είναι απαραίτητη οπότε μπορεί να χρησιμοποιείται ένας άλλου είδους αναμεταδότης RTP επιπέδου που ονομάζεται μεταφραστής (translator). Οι μεταφραστές που τοποθετούνται είναι δύο, ένας σε κάθε μεριά του φράγματος, με αυτόν που βρίσκεται εκτός φράγματος να συγκεντρώνει όλα τα λαμβανόμενα multicast πακέτα στον μεταφραστή που βρίσκεται μέσα στο φράγμα διαμέσου μιας ασφαλούς σύνδεσης μεταξύ τους. Εν συνεχεία ο εσωτερικός μεταφραστής τα ξαναστέλνει ως multicast πακέτα σε ένα multicast σύνολο που είναι όμως περιορισμένο εντός του εσωτερικού, ασφαλούς δικτύου του συγκεκριμένου site.

Οι μεταφραστές και οι μίκτες μπορεί να είναι σχεδιασμένοι για διάφορους σκοπούς. Για παράδειγμα ένας μίκτης βίντεο που μεγεθύνει κάποιες φωτογραφίες συγκεκριμένων ανθρώπων σε ξεχωριστά ρεύματα βίντεο και τα αναμιγνύει σε ένα ρεύμα για να προσομοιώσει κάποια σκηνή

ενός γκρουπ ατόμων. Άλλα παραδείγματα μεταφραστών, περιλαμβάνουν την σύνδεση μεταξύ ενός συνόλου από hosts που «μιλούν» μόνο IP/UDP με ένα σύνολο από hosts που καταλαβαίνουν μόνο ST-II, ή την ανά πακέτο μετάφραση της κωδικοποίησης των ρευμάτων βίντεο από ξεχωριστές πηγές χωρίς συγχρονισμό ή μίξη.

Στο σχήμα που ακολουθεί απεικονίζεται ένα παράδειγμα ενός RTP δικτύου που περιλαμβάνει τερματικά, μίκτες και μεταφραστής.



Εικόνα 1: Παράδειγμα RTP δικτύου που περιέχει τερματικά (T), μίκτες (M) και μεταφραστής (ME).

4. Πολυπλεξία των RTP sessions.

Η πολυπλεξία είναι η τεχνική με την οποία συνενώνονται πολλές γραμμές (κανάλια) χαμηλού εύρους έτσι ώστε να αποτελούν ένα κανάλι μεγάλου εύρους. Τυπικό παράδειγμα είναι η πολυπλεξία τηλεφωνικών συνδιαλέξεων πάνω σε ένα φυσικό κανάλι (Tannenbaum, 1992, σ.111-113, 146-147). Σύμφωνα με τις σχεδιαστικές αρχές της διαχείρισης των ολοκληρωμένων επιπέδων για την αποτελεσματική διαχείριση του πρωτοκόλλου (Clark & Tennenhouse, 1990) πρέπει να ελαχιστοποιείται ο αριθμός των σημείων πολυπλεξίας. Στο RTP η πολυπλεξία παρέχεται από την διεύθυνση μεταφοράς προορισμού (δηλ. η δικτυακή διεύθυνση και ο αριθμός θύρας) που καθορίζουν μια RTP συνεδρία. Για παράδειγμα σε μια τηλεδιάσκεψη που πραγματοποιείται με τα μέσα ήχου και βίντεο, το κάθε μέσο κωδικοποιείται ξεχωριστά και μεταφέρεται σε ξεχωριστές RTP συνεδρίες με την δική του διεύθυνση μεταφοράς προορισμού (destination transport address). Δεν

είναι σκόπιμο ο ήχος και το βίντεο να μεταφερθούν σε μια μοναδική RTP συνεδρία και να αποπολυπλεχθεί με βάση τον τύπο δεδομένων (payload type) ή τα SSRC⁴ πεδία. Οι λόγοι που συμβαίνει αυτό κρίνεται σκόπιμο να μην περιγραφούν στην παρούσα εργασία.

5. Το RTP πρωτόκολλο ελέγχου (RTCP – Real Time Control Protocol).

Το RTP πρωτόκολλο ελέγχου βασίζεται στις περιοδικές μεταδόσεις πακέτων ελέγχου σε όλους τους μετέχοντες σε μια συνεδρία, χρησιμοποιώντας τον ίδιο μηχανισμό διανομής με αυτόν των πακέτων δεδομένων. Το υποκείμενο πρωτόκολλο πρέπει να παρέχει πολυπλεξία των πακέτων δεδομένων και ελέγχου χρησιμοποιώντας για παράδειγμα ξεχωριστό αριθμό θυρών με το UDP. Το RTCP εκτελεί τέσσερις συγκεκριμένες λειτουργίες:

- i. Η κύρια λειτουργία του είναι να παρέχει υποστήριξη στην ποιότητα της διανομής των δεδομένων. Αυτό είναι ένα αναπόσπαστο κομμάτι του ρόλου που διαδραματίζει το RTP ως πρωτόκολλο μεταφοράς και σχετίζεται με τις λειτουργίες ελέγχου της ροής δεδομένων και της συμφόρησης, που υπάρχουν σε άλλα πρωτόκολλα μεταφοράς. Αυτή η υποστήριξη μπορεί να είναι χρήσιμη για τον απευθείας έλεγχο των προσαρμοσίμων κωδικοποιήσεων (Bolot et al., 1994; Busse et al., 1996). Πειραματισμοί με το IP multicasting ωστόσο, έδειξαν ότι είναι το ίδιο κρίσιμη η υποστήριξη της διάγνωσης λαθών της διανομής και από τους αποδέκτες. Η αποστολή υποστηρικτικών αναφορών παράδοσης σε όλους τους αποδέκτες επιτρέπει σε κάποιον που παρακολουθεί προβλήματα να υπολογίσει αν αυτά είναι τοπικά ή ολικά. Επίσης είναι δυνατό για μια οντότητα όπως για παράδειγμα ο παροχέας υπηρεσιών δικτύου χρησιμοποιώντας έναν μηχανισμό διανομής όπως το multicasting IP, να μπορεί να δέχεται πληροφορίες υποστήριξης και να ενεργεί ως ένας έμμεσα εμπλεκόμενος ελεγκτής διάγνωσης δικτυακών προβλημάτων τη στιγμή που σε άλλη περίπτωση δεν εμπλέκεται στην συνεδρία. Αυτή η υποστηρικτική λειτουργία διεκπεραιώνεται από τις RTCP αναφορές αποστολής και λήψης.
- ii. Το RTCP μεταφέρει έναν συνεχή δείκτη στο επίπεδο μεταφοράς για μια πηγή RTP που καλείται κανονικοποιημένο όνομα ή CNAME. Εφόσον υπάρχει περίπτωση να αλλάξει ο δείκτης SSRC αν διαγνωστεί μια σύγκρουση ή αν ένα πρόγραμμα επανεκκινήσει, οι αποδέκτες χρειάζονται τον CNAME ώστε να παρακολουθούν τις κινήσεις του κάθε συμμετέχοντα. Οι αποδέκτες χρειάζονται επίσης τον CNAME για την αντιστοίχιση πολλαπλών streams δεδομένων κάποιου που συμμετέχει σε ένα σύνολο από αντίστοιχες

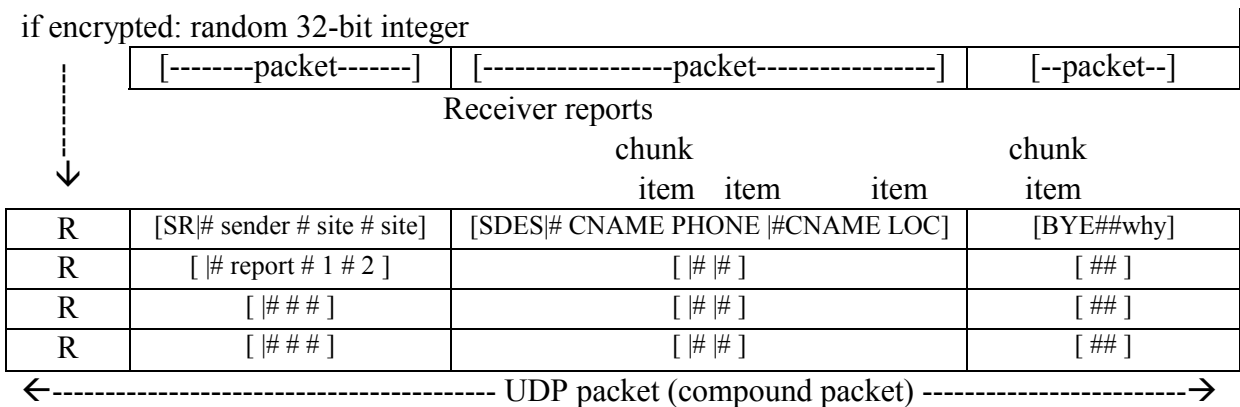
⁴ Synchronization source (SSRC): Η πηγή ενός stream από RTP πακέτα που αναγνωρίζεται από έναν 32-bit αριθμητικό SSRC δείκτη που περιλαμβάνεται μέσα στην RTP επικεφαλίδα έτσι ώστε να μην βασίζεται πάνω στην δικτυακή διεύθυνση.

RTP συνεδρίες, όπως για παράδειγμα ο συγχρονισμός ήχου και βίντεο (που όπως αναφέρθηκε παραπάνω αποτελούν ξεχωριστές RTP sessions).

- iii. Οι προηγούμενες δύο λειτουργίες απαιτούν να στέλνουν όλοι οι συμμετέχοντες RTCP πακέτα και για αυτό πρέπει να ελέγχεται ο ρυθμός αποστολής έτσι ώστε να μπορεί το RTP να επεκταθεί σε μεγάλο αριθμό συμμετεχόντων. Με το να έχουμε τον κάθε συμμετέχοντα να μεταδίδει τα πακέτα ελέγχου του σε όλους τους άλλους δίνεται η δυνατότητα σε καθένα ξεχωριστά να μπορεί να παρατηρεί τον αριθμό των συμμετοχών. Αυτός ο αριθμός χρησιμοποιείται στον υπολογισμό του ρυθμού αποστολής των πακέτων.
- iv. Μια τέταρτη (προαιρετική) λειτουργία είναι η μεταφορά μικρού αριθμού πληροφοριών σχετικά με τη συνεδρία, όπως για παράδειγμα η εμφάνιση στην κονσόλα του χρήστη της ταυτότητας των συνέδρων. Κάτι τέτοιο είναι πιθανότατα χρήσιμο σε «χαλαρά» ελεγχόμενες συνεδρίες όπου οι χρήστες εισέρχονται ή φεύγουν χωρίς να υπάρχει έλεγχος του αν είναι μέλος ή στη διαπραγμάτευση των παραμέτρων σύνδεσης. Το RTCP εξυπηρετεί ως ένα πρακτικό κανάλι για να πλησιάζουμε όλα τα μέλη, αλλά δεν είναι απαραίτητα αναμενόμενη η υποστήριξη όλου του ελέγχου της επικοινωνίας για μια εφαρμογή. Ίσως να χρειάζεται ένα υψηλότερου επιπέδου πρωτόκολλο ελέγχου των συνεδριών για τέτοιες περιπτώσεις.

Οι λειτουργίες 1 – 3 είναι υποχρεωτικές όταν το RTP χρησιμοποιείται σε ένα IP multicast περιβάλλον, ενώ συστήνονται για χρήση σε οποιοδήποτε περιβάλλον.

Στο σχήμα που ακολουθεί απεικονίζεται ένα τυπικό πακέτο RTCP.



Εικόνα 2: Πακέτο RTCP. Το σημείο # σημαίνει SSRC/CSRC (βλέπε υποσημειώσεις που ακολουθούν). SR: Source Report (αναφορά αποστολέα). SDES: Source Description (περιγραφή αποστολέα).

5.1. Το διάστημα μετάδοσης του RTCP (RTCP transmission interval).

Το RTP είναι σχεδιασμένο έτσι ώστε να επιτρέπει στις εφαρμογές να κλιμακώνουν αυτόματα μεγέθη των συνεδριών σε μια ακτίνα που αριθμεί από μερικούς συμμετέχοντες μέχρι χιλιάδες. Σε μια διάσκεψη με μόνο μέσο τη φωνή για παράδειγμα, η κυκλοφορία δεδομένων είναι έμφυτα αυτοπεριοριζόμενη επειδή μόνο ένας ή δύο άνθρωποι θα μιλούν ταυτόχρονα κάθε στιγμή με

αποτέλεσμα ο ρυθμός δεδομένων κάθε σύνδεσης σε μια multicast διανομή να παραμένει σχετικά σταθερός ανεξαρτήτως του αριθμού των συμμετεχόντων. Ωστόσο η κυκλοφορία δεδομένων ελέγχου δεν είναι αυτοπεριοριζόμενη. Αν κάθε συμμετέχων έστελνε αναφορές παραλαβής με σταθερό ρυθμό, η κυκλοφορία δεδομένων ελέγχου θα αυξανόταν γραμμικά με τον αριθμό των μερών. Για αυτό ο ρυθμός πρέπει να μειωθεί.

Για κάθε συνεδρία γίνεται η υπόθεση ότι η κυκλοφορία δεδομένων υπόκειται σε ένα μικτό όριο που ονομάζεται *εύρος ζώνης συνεδρίας (session bandwidth)* που διαιρείται μεταξύ των μελών. Το δίκτυο μπορεί να δεσμεύει και να καθορίζει το όριο αυτού του εύρους είτε μπορεί αυτό να προκύπτει από μια λογική μοιρασιά. Το εύρος ζώνης συνεδρίας μπορεί να επιλεγεί με βάση το κόστος ή την γνώση κάποιας προτεραιότητας του ωφέλιμου δικτυακού εύρους ζώνης για τη συγκεκριμένη συνεδρία. Κατά μια έννοια είναι ανεξάρτητο από την κωδικοποίηση του μέσου αλλά μπορεί να θέσει περιορισμούς στην επιλογή της κωδικοποίησης. Η παράμετρος του εύρους ζώνης συνεδρίας αναμένεται να παρέχεται από κάποια εφαρμογή διαχείρισης συνεδριών, όταν ενεργοποιείται μια εφαρμογή μέσων, αλλά ωστόσο αυτή η εφαρμογή μέσων μπορεί να προκαθορίσει την επιλογή της κωδικοποίησης της συνεδρίας βασιζόμενη στις πληροφορίες για το εύρος ενός και μόνο αποστολέα. Η εφαρμογή αυτή μπορεί επίσης να επιβάλλει τα όρια του εύρους βασισμένη σε multicast κανόνες ή άλλα κριτήρια.

Ο υπολογισμός του εύρους για την κυκλοφορία δεδομένων και ελέγχου περιλαμβάνει πρωτόκολλα μεταφοράς και δικτύου χαμηλού επιπέδου (π.χ. UDP και IP) εφόσον αυτό είναι το μόνο που χρειάζεται να γνωρίζει το σύστημα δέσμευσης πόρων. Επίσης είναι αναμενόμενο από την εφαρμογή να γνωρίζει ποια από αυτά τα πρωτόκολλα χρησιμοποιούνται. Οι επικεφαλίδες του επιπέδου σύνδεσης δεν παίρνουν μέρος σ' αυτούς τους υπολογισμούς μιας και τα πακέτα θα ενθυλακωθούν με διαφορετικές επικεφαλίδες αυτού του επιπέδου κατά τη διάρκεια της μεταφοράς τους.

Η κυκλοφορία ελέγχου είναι αναγκαίο να περιοριστεί σε μικρά και γνωστά ποσοστά του εύρους ζώνης συνεδρίας. Μικρά ποσοστά έτσι ώστε να μην βλάπτεται η κύρια λειτουργία μεταφοράς δεδομένων του πρωτοκόλλου μεταφοράς και γνωστά έτσι ώστε η κυκλοφορία ελέγχου να μπορεί να συμπεριληφθεί στις προδιαγραφές του εύρους που δίνονται σε ένα πρωτόκολλο δέσμευσης πόρων, κάτι που δίνει τη δυνατότητα σε κάθε μέλος να μπορεί να υπολογίσει αυτόνομα το μέρος του εύρους που του αναλογεί. Προτείνεται αυτό το ποσοστό του εύρους ζώνης συνεδρίας που δεσμεύεται για το RTCP να είναι της τάξης του 5%. Ενώ η τιμή αυτή καθώς και άλλων σταθερών δεν παίζει καθοριστικό ρόλο στον υπολογισμό του διαστήματος μετάδοσης, κρίνεται αναγκαίο να χρησιμοποιούνται οι ίδιες τιμές από όλους τους συμβεβλημένους σε μια συνεδρία έτσι ώστε να υπολογίζεται το ίδιο διάστημα μετάδοσης. Για αυτόν το λόγο πρέπει αυτές οι τιμές να είναι δοσμένες σταθερές για κάθε προφίλ εφαρμογής.

5.2. Διατήρηση του αριθμού των μελών μιας συνεδρίας.

Ο υπολογισμός του διαστήματος μετάδοσης ενός RTCP πακέτου εξαρτάται από την εκτίμηση του αριθμού των μελών που συμμετέχουν σε μία συνεδρία. Νέα site προστίθεται σ' αυτόν τον αριθμό όταν γίνουν αντιληπτές οι αιτήσεις τους και δημιουργείται μια καταχώριση για το καθένα για την παρακολούθησή τους. Οι νέες συνδέσεις δεν θεωρούνται αποδεκτές μέχρι να μεταφερθεί ο νέος SSRC (που περιέχει αυτές τις καταχωρίσεις) μέσω της απολαβής πολλαπλών πακέτων που αποστέλλονται από τα νέα μέλη. Επίσης μπορούν να διαγραφούν μέλη από τον πίνακα καταχωρίσεων όταν αποσταλεί ένα RTCP BYE πακέτο που περιλαμβάνει και τον αντίστοιχο SSRC δείκτη.

Αν κάποιο μέλος δεν έχει λάβει κανένα RTP ή RTCP πακέτο από κάποιο site για ένα μικρό αριθμό διαστημάτων RTCP μετάδοσης (συνίσταται 5 διαστήματα), τότε μπορεί να το σημειώσει ως απενεργοποιημένο ή ακόμα και να το διαγράψει εφόσον αυτό δεν έχει καταστεί αποδεκτό. Αυτό προσφέρει κάποια αντίσταση στο χάσιμο των πακέτων. Η συγκεκριμένη διαδικασία απαιτεί όλα τα site να υπολογίζουν σχεδόν την ίδια τιμή για το διάστημα μετάδοσης της RTCP αναφοράς. Άπαξ και ένα site έχει γίνει αποδεκτό και αργότερα σημειωθεί ως απενεργό τότε η κατάστασή του παραμένει ενεργή και εξακολουθεί να συμμετέχει στον συνολικό αριθμό των sites που μοιράζονται το εύρος ζώνης του RTCP για μια περίοδο αρκετά μεγάλη ώστε να μπορεί να επεκτείνει τον τυπικό αριθμό των κατατημήσεων του δικτύου. Αυτό γίνεται σκόπιμα για να αποφευχθεί υπέρογκη κυκλοφορία όταν οι κατατημήσεις επανέρχονται στην αρχική τους κατάσταση που οφείλεται κυρίως στο μικρό διάστημα μετάδοσης της RTCP αναφοράς. Η συνιστώμενη περίοδος αναμονής για την απενεργοποίηση ενός site είναι 30 λεπτά. Ας σημειωθεί ότι αυτή η χρονική περίοδος είναι μεγαλύτερη από το πενταπλάσιο της αναμενόμενης μεγαλύτερης τιμής του διαστήματος μετάδοσης της RTCP αναφοράς, που στην πράξη είναι 2 ως 5 λεπτά.

6. Δέσμευση και χρήση του δείκτη SSRC.

Ο δείκτης SSRC που μεταφέρεται στην RTP επικεφαλίδα και σε πολλά πεδία των RTCP πακέτων είναι ένας τυχαίος 32-μπιτος αριθμός που απαιτείται να είναι ολικά μοναδικός μέσα σε μία συνεδρία RTP. Είναι ζωτικής σημασίας η επιλογή αυτού του αριθμού να γίνεται προσεκτικά, έτσι ώστε τα μέλη που βρίσκονται στο ίδιο δίκτυο ή που ξεκινούν ταυτόχρονα τη συμμετοχή τους σε κάποια συνεδρία, να μην επιλέξουν την ίδια τιμή για αυτόν τον αριθμό. Για αυτόν το λόγο κρίνεται ανεπαρκές να χρησιμοποιηθεί μια τοπική δικτυακή διεύθυνση όπως είναι η IP address.

Εφόσον οι RTP μεταφραστές και μίκτες επιτρέπουν την ενδολειτουργικότητα μεταξύ πολλαπλών δικτύων με διαφορετικά πεδία διευθύνσεων, είναι δυνατόν ο σχεδιασμός δέσμευσης διευθύνσεων μεταξύ δύο διαφορετικών πεδίων να οδηγήσει σε πολύ μεγαλύτερο ρυθμό

συγκρούσεων από ότι θα συνέβαινε με τυχαία δέσμευση. Οι πηγές που τρέχουν σε έναν host θα συγκρούονταν επίσης. Ακόμα δεν θεωρείται συνετό να δημιουργείται ο SSRC δείκτης απλά με την κλήση μιας συνάρτησης παραγωγής τυχαίων αριθμών (randomizer) αν δεν έχει αρχικοποιηθεί προσεκτικά η κατάσταση.

6.1. Πιθανότητα σύγκρουσης.

Εφόσον επιλέγονται τυχαία οι δείκτες είναι πιθανό δύο οι περισσότερες πηγές να επιλέξουν την ίδια τιμή. Η μεγαλύτερη πιθανότητα να συμβεί σύγκρουση προκύπτει όταν όλες οι πηγές ξεκινούν ταυτόχρονα, όπως θα μπορούσε να συμβεί για παράδειγμα στην περίπτωση που ενεργοποιείται αυτόματα κάποιος μηχανισμός διαχείρισης κάποιας συνεδρίας.

Αν N είναι ο αριθμός των πηγών και L το μέγεθος του δείκτη (στην περίπτωσή μας 32-bit) τότε η πιθανότητα δύο πηγές να επιλέξουν ανεξάρτητα την ίδια τιμή δίνεται, προσεγγιστικά για μεγάλο

N , από την μαθηματική εξίσωση $1 - e^{\left(\frac{-N^2}{2^{(L+1)}}\right)}$ (Feller, 1968). Για $N=1000$ η πιθανότητα είναι σχεδόν 10^{-4} . Η τυπική πιθανότητα συμφόρησης είναι πολύ μικρότερη από την πιθανότητα που προκύπτει στη χειρότερη περίπτωση που αναφέρθηκε προηγουμένως.

Όταν μια νέα πηγή λαμβάνει μέρος σε ένα RTP session στο οποίο όλα τα άλλα μέλη έχουν ήδη μοναδικά ορισμένους δείκτες, τότε η πιθανότητα συμφόρησης είναι απλά ένα ποσοστό των αριθμών που έχουν χρησιμοποιηθεί σ' αυτό το διάστημα διευθύνσεων. Σ' αυτή την περίπτωση η πιθανότητα συμφόρησης δίνεται από την μαθηματική εξίσωση $\frac{N}{2^L}$. Για $N=1000$ η πιθανότητα αυτή ισούται με $2 \cdot 10^{-7}$.

Αυτή η πιθανότητα μπορεί να μειωθεί περαιτέρω αν δοθεί η ευκαιρία σε μια νέα πηγή να δεχθεί πακέτα από άλλα μέλη προτού αποστείλει το πρώτο της πακέτο. Αν η νέα πηγή παρακολουθεί τα άλλα μέλη (μέσω του δείκτη SSRC), τότε μπορεί να πιστοποιήσει αν η τιμή του δείκτη της συγκρούεται με οποιαδήποτε τιμή δείκτη από τα πακέτα που έχει λάβει, προτού μεταδώσει το πρώτο της πακέτο. Στην περίπτωση που συγκρούεται ξαναεπιλέγει νέα τιμή.

6.2. Διαχείριση συγκρούσεων και ανίχνευση βρόχων.

Παρόλο που είναι μικρή η πιθανότητα σύγκρουσης του δείκτη SSRC, όλες οι υλοποιήσεις RTP εφαρμογών πρέπει να είναι έτοιμες να ανιχνεύουν συγκρούσεις και να ενεργοποιούνται κατάλληλα για την επίλυσή τους. Αν κάποια πηγή ανακαλύψει, σε οποιαδήποτε στιγμή, ότι ο SSRC δείκτης της είναι ίδιος με κάποιας άλλης πρέπει αμέσως να στείλει ένα RTCP BYE πακέτο για τον παλιό δείκτη και να επιλέξει τυχαία έναν καινούργιο. Αν ένας αποδέκτης ανακαλύψει ότι συγκρούονται δυο άλλες πηγές τότε μπορεί να κρατήσει τα πακέτα της μιας και να απορρίψει τα πακέτα της

άλλης όποτε αυτό είναι δυνατό να ανιχνευτεί. Οι δύο πηγές αναμένεται να αντιμετωπίσουν την σύγκρουση ώστε να μη διαγωνίζεται αυτή η κατάσταση.

Επειδή οι τυχαίοι δείκτες δημιουργούνται έτσι ώστε να είναι μοναδικοί σε όλη την έκταση κάθε RTP session μπορούν επίσης να χρησιμοποιηθούν και για την ανίχνευση βρόχων που να προέρχονται από μίκτες ή μεταφραστές. Ένας βρόχος προκαλεί την επανάληψη των δεδομένων και της πληροφορίας ελέγχου, είτε ως έχει, είτε αναμεμειγμένη όπως φαίνεται στα παραδείγματα που ακολουθούν:

- Ένας μεταφραστής είναι δυνατόν να προωθήσει εσφαλμένα κάποιο πακέτο στο ίδιο multicast σύνολο μελών από το οποίο το παρέλαβε και αυτό συμβαίνει είτε χρησιμοποιείται ένας μεταφραστής είτε μια αλυσίδα από αυτούς. Σ' αυτή την περίπτωση εμφανίζεται το ίδιο πακέτο πολλαπλές φορές, δημιουργούμενο από διαφορετικές δικτυακές πηγές.
- Δύο μεταφραστές που έχουν συνδεθεί λανθασμένα σε παραλληλία όπως για παράδειγμα με τα ίδια σύνολα multicast και στις δύο πλευρές, με αποτέλεσμα και οι δύο να προωθούν τα πακέτα ο ένας στον άλλο. Σ' αυτή την περίπτωση οι μονόδρομοι μεταφραστές θα παρήγαγαν δύο επαναλήψεις των ίδιων πακέτων ενώ οι αμφίδρομοι θα δημιουργούσαν βρόχο.
- Ένας μίκτης μπορεί να κλείσει ένα βρόχο με την αποστολή στον ίδιο προορισμό από όπου παρέλαβε τα πακέτα, είτε με απευθείας αποστολή είτε μέσω ενός άλλου μίκτη ή μεταφραστή. Σε αυτήν την περίπτωση μια πηγή μπορεί να εμφανίζεται και ως SSRC σε ένα πακέτο δεδομένων αλλά και ως CSRC⁵ σε ένα αναμεμειγμένο πακέτο δεδομένων.

Μια πηγή μπορεί να ανακαλύψει ότι τα πακέτα της βρίσκονται σε βρόχο ή ότι συμβαίνει αυτό στα πακέτα μιας άλλης πηγής (έμμεσος βρόχος). Τόσο οι βρόχοι όσο και οι συγκρούσεις καταλήγουν στο να λαμβάνονται πακέτα με τον ίδιο SSRC δείκτη αλλά με διαφορετική διεύθυνση πηγής μεταφοράς που μπορεί να ανήκει είτε στην πηγή που δημιούργησε το πακέτο είτε σε μια ενδιάμεση πηγή. Συμπερασματικά λοιπόν αν μια πηγή αλλάξει την διεύθυνση μεταφοράς της πρέπει επίσης να επιλέξει έναν νέο δείκτη SSRC έτσι ώστε να αποφύγει την ανάδειξή της ως πηγή βρόχου.

Οι βρόχοι ή οι συγκρούσεις που προκύπτουν στην πλευρά κάποιου μεταφραστή ή μίκτη δεν μπορούν να ανιχνευθούν χρησιμοποιώντας την διεύθυνση πηγής μεταφοράς (source transport address) αν όλα τα αντίγραφα των πακέτων διέρχονται διαμέσου του μίκτη ή του μεταφραστή. Για να αντιμετωπιστούν αυτού του είδους οι συγκρούσεις πρέπει να υπάρχει σε μια RTP υλοποίηση ο εξής αλγόριθμος: Να αγνοούνται τα πακέτα κάθε νέας πηγής ή βρόχου που συγκρούονται με

⁵ Contributing source (CSRC): μια πηγή ενός stream από RTP πακέτα που έχει συνεισφέρει στο μικτό stream που παρήχθη από κάποιον RTP mixer. Ο μίκτης εισάγει μια λίστα από τους SSRC δείκτες των πηγών που συνεισέφεραν στη δημιουργία του συγκεκριμένου πακέτου, στην επικεφαλίδα του. Αυτή η λίστα αναφέρεται ως CSRC λίστα.

οποιαδήποτε από τις εγκατεστημένες πηγές. Αντιμετωπίζει τις συγκρούσεις που γίνονται με τον SSRC του κάθε μέλους στέλνοντας ένα RTCP BYE πακέτο για τον παλιό δείκτη που συγκρούεται και να επιλέγει έναν καινούργιο. Ωστόσο όταν η σύγκρουση προέρχεται από βρόχο που δημιουργούν τα πακέτα της ίδιας πηγής τότε ο αλγόριθμος θα επιλέγει νέο δείκτη μόνο μια φορά και θα αγνοεί τα πακέτα του βρόχου. Αυτό γίνεται για να αποφευχθεί η υπερχειλίση των BYE πακέτων.

Ο αλγόριθμος είναι αναγκαίο να διατηρεί έναν πίνακα με καταχωρήσεις για τους δείκτες των πηγών και τις διευθύνσεις μεταφοράς από όπου παρελήφθησαν για πρώτη φορά αυτοί οι δείκτες. Ο κάθε SSRC ή CSRC δείκτης των ληφθέντων πακέτων, εξετάζεται σ' αυτόν τον πίνακα έτσι ώστε να επεξεργαστούμε τις πληροφορίες δεδομένων ή ελέγχου που περιέχουν. Για τα πακέτα ελέγχου χρειάζεται ξεχωριστή εξέταση για κάθε στοιχείο που περιέχει διαφορετικό SSRC. Είναι επίσης σκόπιμο να διατηρείται ένας ξεχωριστός πίνακας με τις source transport addresses των πηγών που βρίσκονται σε σύγκρουση έτσι ώστε να εξιχνιάζονται οι βρόχοι που δημιουργούνται από τα πακέτα του ιδίου μετέχοντα. Να σημειωθεί ότι αυτή η λίστα είναι μικρή σε μέγεθος και συνήθως είναι άδεια. Κάθε στοιχείο αποθηκεύει σ' αυτή τη λίστα την διεύθυνση της πηγής συν το χρόνο που παραλήφθηκε το πιο πρόσφατο πακέτο που συγκρούστηκε. Ένα στοιχείο μπορεί να απομακρυνθεί από τη λίστα όταν δεν έχει παραληφθεί κανένα συγκρούόμενο πακέτο από αυτή την πηγή μέσα σε χρονικό διάστημα που ισοδυναμεί με 10 RTCP διαστήματα μετάδοσης.

7. Ασφάλεια.

Τα πρωτόκολλα χαμηλότερου επιπέδου μπορούν τελικά να προσφέρουν όλες τις υπηρεσίες ασφάλειας που να είναι επιθυμητές για RTP εφαρμογές, συμπεριλαμβάνοντας την πιστοποίηση, την ακεραιότητα και την εμπιστευτικότητα (authentication, integrity and confidentiality). Αυτές οι υπηρεσίες έχουν σχετικά πρόσφατα καθοριστεί για το IP. Άπαξ και επιβεβαιωθεί η ανάγκη για χρήση εμπιστευτικότητας στις αρχικές εφαρμογές βίντεο και ήχου που αναμένεται να χρησιμοποιήσουν το RTP, τότε καθορίζεται στο επόμενο βήμα μια υπηρεσία εμπιστευτικότητας για χρήση με τα RTP και RTCP μέχρι να γίνουν διαθέσιμες αυτές οι υπηρεσίες από τα χαμηλότερα επίπεδα. Η επιβάρυνση που προστίθεται στο πρωτόκολλο από αυτή την υπηρεσία είναι μικρή, οπότε θα είναι μικρό το σφάλμα αν αυτή η υπηρεσία αχρηστευτεί από τις χαμηλότερου επιπέδου υπηρεσίες στο μέλλον.

Αμέσως μετά ακολουθεί μια σύντομη περιγραφή της υπηρεσίας εμπιστευτικότητας μιας και οι άλλες δύο υπηρεσίες δεν υποστηρίζονται ακόμα από το RTP.

8. Εμπιστευτικότητα.

Εμπιστευτικότητα σημαίνει ότι μόνο ο σωστός αποδέκτης μπορεί να αποκωδικοποιήσει τα ληφθέντα πακέτα ενώ για τους άλλους τα πακέτα περιέχουν άχρηστη πληροφορία. Η εμπιστευτικότητα των περιεχομένων επιτυγχάνεται με την κρυπτογράφηση.

Όταν είναι επιθυμητή η κρυπτογράφηση του RTP ή του RTCP, όλες οι οκτάδες που θα ενθυλακωθούν σε ένα μοναδικό, προς μετάδοση, πακέτο χαμηλού επιπέδου, κρυπτογραφούνται ως μοναδική μονάδα. Πριν την κρυπτογράφηση του RTCP προσκολλάται στην μονάδα ένας τυχαίος 32-bit αριθμός έτσι ώστε να αποτραπούν οι επιθέσεις γνωστού κειμένου (plaintext attacks). Για το RTP δεν απαιτείται το συγκεκριμένο πρόθεμα λόγω του ότι τα πεδία αριθμού σειράς και χρόνου αρχικοποιούνται με τυχαία γεννήτρια. Για το RTCP επιτρέπεται ο διαχωρισμός ενός ενιαίου RTCP πακέτου σε δύο χαμηλότερου επιπέδου πακέτα που το ένα θα κρυπτογραφηθεί ενώ το άλλο θα σταλεί ως έχει.

Η ύπαρξη κρυπτογράφησης και το σωστό κλειδί επιβεβαιώνονται από τον αποδέκτη μέσω ελέγχων της επικεφαλίδας ή της εγκυρότητας του φορτίου. Ο προκαθορισμένος αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι ο DES (Balenson, 1993) στην μορφή που κάνει χρήση της CBC (Cipher Block Chaining) τεχνικής όπου το διάνυσμα αρχικοποίησης είναι μηδενικό λόγω του ότι προσφέρονται τυχαίες τιμές από την επικεφαλίδα του RTP ή από το τυχαίο πρόθεμα των ενιαίων RTCP πακέτων (Voydock & Kent, 1983). Οι RTP υλοποιήσεις πρέπει πάντα να υποστηρίζουν αυτήν την τεχνική κρυπτογράφησης ως προεπιλογή έτσι ώστε να υπάρχει ενδοσυνεργασία μεταξύ των εφαρμογών. Αυτή η μέθοδος κρυπτογράφησης έχει επιλεγεί επειδή έχει αποδειχθεί ότι είναι εύκολη και πρακτική στη χρήση με εργαλεία ήχου και βίντεο για λειτουργία τους στο Internet. Μπορούν να χρησιμοποιηθούν δυναμικά και άλλες μέθοδοι κρυπτογράφησης από μέσα που δεν υποστηρίζουν το RTP.

Εναλλακτικά με την κρυπτογράφηση στο RTP επίπεδο που περιγράφηκε αμέσως πρωτύτερα, μπορούν τα προφίλ να καθορίσουν πρόσθετους τύπους φορτίου για κρυπτογραφημένες κωδικοποιήσεις. Αυτές οι κωδικοποιήσεις πρέπει να περιγράφουν πως θα διαχειριστεί το παραγέμισμα (padding) ή άλλα θέματα κρυπτογράφησης. Αυτή η μέθοδος επιτρέπει την κρυπτογράφηση μόνο των δεδομένων ενώ αφήνει τις επικεφαλίδες άθικτες. Κάτι τέτοιο μπορεί να είναι εν μέρει χρήσιμο για συσκευές υλικού που διαχειρίζονται μαζί τόσο την αποκρυπτογράφηση όσο και την αποκωδικοποίηση. (Stubblebine, 1993).

Το σχήμα που ακολουθεί απεικονίζει ένα RTCP πακέτο όπου στην πρώτη περίπτωση είναι κρυπτογραφημένο ενώ στη δεύτερη δεν είναι.



Εικόνα 3: Κρυπτογραφημένα και μη κρυπτογραφημένα RTCP πακέτα.

9. Το RTP πάνω από πρωτόκολλα δικτύου και μεταφοράς.

Σ' αυτήν την παράγραφο περιγράφονται θέματα σχετικά με την μεταφορά των RTP πακέτων μέσα σε συγκεκριμένα πρωτόκολλα δικτύου και μεταφοράς. Για το συγκεκριμένο ζήτημα ισχύουν οι επόμενοι κανόνες εκτός και αν παραμεριστούν από ειδικούς ορισμούς πρωτοκόλλου που βρίσκονται εκτός των προκαθορισμένων προδιαγραφών.

Το RTP βασίζεται στα υποκείμενα πρωτόκολλα για την παροχή αποπολυπλεξίας στα ρεύματα των RTP δεδομένων και RTCP ελέγχων. Το RTP χρησιμοποιεί περιττό αριθμό θυρών για το UDP ή ανάλογα πρωτόκολλα, ενώ το αντίστοιχο RTCP ρεύμα δεδομένων χρησιμοποιεί τον επόμενο **μεγαλύτερο** (περιττό) αριθμό θύρας. Αν μια εφαρμογή είναι εφοδιασμένη με έναν περιττό αριθμό για χρήση του ως RTP θύρα, τότε θα έπρεπε να αντικαταστήσει αυτόν τον αριθμό με τον επόμενο **μικρότερο** περιττό αριθμό.

Τα RTP πακέτα δεδομένων δεν περιέχουν πεδία αναφοράς μήκους ή άλλη σκιαγράφιση και για αυτό το RTP βασίζεται στο πρωτόκολλο που βρίσκεται κάτω από αυτό, για την παροχή ενδείξεων μήκους. Το μέγιστο μέγεθος των RTP πακέτων περιορίζεται μόνο από τα υποκείμενα πρωτόκολλα.

Αν τα RTP πακέτα είναι να μεταφερθούν με κάποιο υποκείμενο πρωτόκολλο που προσφέρει το υπόβαθρο για συνεχή ροή οκτάδων (octets)⁶ παρά μηνυμάτων (πακέτων), πρέπει να οριστεί σαφώς η ενθυλάκωση των RTP πακέτων έτσι ώστε να παρέχεται ένας μηχανισμός πλαισίωσης (framing). Η πλαισίωση είναι επίσης χρήσιμη στην περίπτωση που το υποκείμενο πρωτόκολλο περιέχει παραγέμισμα (padding) με αποτέλεσμα να μη μπορούν να οριστούν οι επεκτάσεις του RTP payload.

Κάποιο προφίλ είναι δυνατόν να καθορίσει κάποια μέθοδο πλαισίωσης που θα χρησιμοποιηθεί ακόμα κι αν το RTP μεταφέρεται με πρωτόκολλα που παρέχουν πλαισίωση. Ο λόγος που μπορεί να γίνει κάτι τέτοιο είναι για να επιτραπεί η μεταφορά πολλαπλών RTP πακέτων σε μία μόνο μονάδα χαμηλότερου πρωτοκόλλου όπως για παράδειγμα ένα UDP πακέτο. Η συγκεκριμένη τεχνική έχει

⁶ Octets: Οκτάδες. Η CCITT (Comité Consultatif International de Telegraphique et Telephonique) ονομάζει τα Bytes octets.

ως αποτέλεσμα την μείωση της επιβάρυνσης της επικεφαλίδας των πακέτων και την απλοποίηση του συγχρονισμού μεταξύ διαφορετικών streams.

Σ' αυτό το σημείο τελειώνει η γενική περιγραφή του πρωτοκόλλου RTP με την ελπίδα ότι καλύψαμε αναλυτικά τα θέματα που αφορούν την απόδοση, τις δυνατότητες και τις λειτουργίες που προσφέρει αυτό το πρωτόκολλο για τη ροή βίντεο και ήχου. Ο αναγνώστης που ενδιαφέρεται για τα τεχνικά χαρακτηριστικά και την δομή του πρωτοκόλλου καθώς και για διάφορους αλγορίθμους υλοποιήσεων του RTP προτρέπεται να ανατρέξει στις αναφορές που επισυνάπτονται στο τέλος.

Το πρωτόκολλο RTSP (Real Time Streaming Protocol)

1. Γενική περιγραφή

Το RTSP είναι ένα πρωτόκολλο επιπέδου εφαρμογής για τη διαχείριση της διανομής δεδομένων που έχουν streaming ιδιότητες. Στις δυνατότητές συγκαταλέγεται το γεγονός ότι παρέχει ένα επεκτάσιμο πλαίσιο ώστε να ενεργοποιεί την ελεγχόμενη, κατά παραγγελία (on demand) διανομή δεδομένων πραγματικού χρόνου όπως είναι το βίντεο και ο ήχος. Οι πηγές των δεδομένων μπορούν να περιέχουν τόσο τροφοδοσία ζωντανών δεδομένων όσο και αποθηκευμένων. Σκοπός του πρωτοκόλλου είναι:

- να διαχειρίζεται πολλαπλές συνεδρίες διανομής δεδομένων
- να παρέχει κάποιο μέσο για την επιλογή των καναλιών διανομής όπως είναι το UDP
- να κάνει multicast των UDP και TCP
- και να παρέχει το μέσο για την επιλογή του μηχανισμού διανομής που βασίζεται πάνω στο RTP.

2. Αναλυτικά οι αιτίες ύπαρξης του πρωτοκόλλου RTSP.

Το RTSP εγκαθιστά και διαχειρίζεται είτε ένα είτε πολλαπλά χρονικά συγχρονισμένα streams συνεχών μέσων όπως είναι ο ήχος και το βίντεο. Τυπικά δεν διανέμει τα συνεχή ρεύματα δεδομένων αυτά καθαυτά, έστω κι αν είναι δυνατή η διαστρωμάτωση των συνεχών ρευμάτων μέσων με ρεύματα ελέγχου. Με άλλα λόγια το RTSP συμπεριφέρεται ως δικτυακό «τηλεκοντρόλ» για τους εξυπηρετές πολυμέσων (multimedia servers).

Δεν υπάρχει καμία ένδειξη για κάποια RTSP σύνδεση, αντιθέτως ο εξυπηρετητής διατηρεί κάποια συνεδρία μαρκαρισμένη μέσω ενός δείκτη. Σε καμία περίπτωση δεν είναι κάποια RTSP συνεδρία στενά δεμένη με κάποια σύνδεση στο επίπεδο μεταφοράς π.χ. μια TCP σύνδεση. Κατά τη διάρκεια μιας RTSP συνεδρίας, μπορεί κάποιος RTSP πελάτης να ξεκινήσει ή να διακόψει πολλές αξιόπιστες συνδέσεις μεταφοράς με τον εξυπηρετητή με σκοπό να διανέμει τις RTSP αιτήσεις. Εναλλακτικά μπορεί να χρησιμοποιήσει ένα πρωτόκολλο μεταφοράς χωρίς σύνδεση (connectionless) όπως είναι το UDP. Τα διαχειριζόμενα από το RTSP ρεύματα ροής μπορούν να χρησιμοποιήσουν το RTP (Schulzrinne, 1996), αλλά η λειτουργία του RTSP δεν εξαρτάται από τον μηχανισμό μεταφοράς που χρησιμοποιείται για την μεταφορά των συνεχών μέσων.

Το πρωτόκολλο έχει σκοπίμως παρόμοια σύνταξη και λειτουργία με το HTTP 1.1 έτσι ώστε οι μηχανισμοί επέκτασης του HTTP να μπορούν να προστεθούν στις περισσότερες περιπτώσεις και στο RTSP (Fielding et al., 1997). Ωστόσο το RTSP διαφέρει από το HTTP σε έναν αριθμό από σημαντικά θέματα:

- i. Το RTSP εισάγει νέες μεθόδους και έχει διαφορετικούς δείκτες πρωτοκόλλου.
- ii. Σε αντιδιαστολή με την άνευ κατάστασης φύση του HTTP σε όλες σχεδόν τις περιπτώσεις, πρέπει ένας RTSP εξυπηρετητής να διατηρεί την κατάστασή του.
- iii. Στο RTSP μπορούν να αποστέλλουν αιτήσεις και ο πελάτης αλλά και ο εξυπηρετητής.
- iv. Τα εκτός ζώνης (ή ομάδας) δεδομένα μεταφέρονται με άλλο πρωτόκολλο. (Ωστόσο υπάρχει μια εξαίρεση σ' αυτό). Το RTSP έχει καθοριστεί να χρησιμοποιεί το ISO 10646 (UTF-8) αντί του ISO 8859-1 που είναι σύμφωνο με τις προσπάθειες για διεθνοποίηση του τωρινού HTML (Yergeau et al., 1997).
- v. Η Request-URI περιέχει πάντοτε την απόλυτη URI. Το HTTP/1.1 λόγω της συμβατότητας προς τα πίσω (backward compatibility) με ένα ιστορικό ατόπημα (Fielding et al., 1997), μεταφέρει μόνο το απόλυτο μονοπάτι στην αίτηση και τοποθετεί το όνομα του ξενιστή (host)⁷ σε ένα ξεχωριστό πεδίο της επικεφαλίδας. Αυτό κάνει ευκολότερο το "virtual hosting", όπου ένας ξενιστής με μοναδική IP διεύθυνση φιλοξενεί πολλές δενδρικές δομές αρχείων (document trees).

3. Λειτουργίες του πρωτοκόλλου.

Το RTSP υποστηρίζει τις εξής λειτουργίες:

a) Ανάκτηση του μέσου από έναν εξυπηρετητή μέσων (media server): ο πελάτης μπορεί να ζητήσει μια περιγραφική παρουσίαση των πληροφοριών μέσω του HTTP ή κάποιας άλλης μεθόδου. Αν η παρουσίαση έχει γίνει multicast, τότε η περιγραφή της περιέχει τις εν δυνάμει multicast διευθύνσεις και θύρες που μπορούν να χρησιμοποιηθούν από τα συνεχή δεδομένα. Αν η παρουσίαση είναι προς αποστολή μόνο στον πελάτη μέσω unicast, τότε ο τελευταίος παρέχει τον προορισμό για λόγους ασφαλείας.

b) Πρόσκληση ενός εξυπηρετητή μέσων σε μια συνδιάσκεψη: ένας εξυπηρετητής μέσων μπορεί να προσκληθεί για να πάρει μέρος σε μια συνδιάσκεψη, είτε για να αναπαράγει κάποιο μέσο (π.χ. βίντεο ή ήχος) στην παρουσίαση, είτε για να καταγράψει ολόκληρα ή μέρος των μέσων μιας παρουσίασης. Αυτή η κατάσταση είναι χρήσιμη σε εφαρμογές κατανεμημένης διδασκαλίας. Πολλά μέλη μιας συνδιάσκεψης μπορούν να κατευθυνθούν αλλού «απλά πατώντας τα πλήκτρα του τηλεχειριστηρίου».

c) Πρόσθεση μέσων σε μία ήδη δημιουργημένη παρουσίαση: είναι χρήσιμο, ειδικότερα για ζωντανές παρουσιάσεις, να μπορεί ένας εξυπηρετητής να πει στον πελάτη σχετικά με το αν έχουν γίνει διαθέσιμα πρόσθετα μέσα.

Οι RTSP αιτήσεις μπορούν να διαχειριστούν από πληρεξούσιους (proxies), τούνελ (tunnels) και caches όπως γίνεται και στην περίπτωση του HTTP/1.1 (Fielding et al., 1997).

4. Ορολογία.

Είναι χρήσιμο για πρακτικούς λόγους, να περιγραφεί η ορολογία που χρησιμοποιείται στην περιγραφή αυτού του πρωτοκόλλου. Πολλοί από τους όρους που θα περιγραφούν μπορεί να μη χρησιμοποιούνται στην παρούσα εργασία, ωστόσο αποτελεί πρόσθετο βοήθημα η γνώση τους. Εκτός των άλλων μπορεί να θεωρηθεί ότι η ορολογία που δίνεται παρακάτω περιγράφει κατά κάποιο τρόπο τις ιδιότητες και την υποστήριξη του πρωτοκόλλου.

➤ **Aggregate control:** είναι η διαχείριση από τον εξυπηρετητή πολλαπλών streams χρησιμοποιώντας μια μοναδική χρονοσειρά (timeline) (κατά πάσα πιθανότητα η πιο ταιριαστή απόδοση του όρου εδώ είναι χρονική κλίμακα). Για τροφοδότηση ήχου ή βίντεο κάτι τέτοιο σημαίνει ότι ο πελάτης μπορεί να εκδώσει ένα μεμονωμένο μήνυμα αναπαραγωγής ή παύσης για να ελέγξει ταυτόχρονα την τροφοδότηση και του ήχου και του βίντεο.

➤ **Conference:** ένα multiparty, multimedia presentation, όπου το multi σημαίνει μεγαλύτερο ή ίσο του ένα. (οι όροι αυτοί προφανώς είναι κατανοητοί καλύτερα ως έχουν παρά αν μεταφραστούν).

➤ **Client:** ο πελάτης ζητά συνεχή δεδομένα μέσω των εξυπηρετητή πολυμέσων.

➤ **Connection:** είναι ένα νοητό κύκλωμα (virtual circuit) στο επίπεδο μεταφοράς που εγκαθίσταται μεταξύ δύο προγραμμάτων για τον σκοπό της επικοινωνίας.

➤ **Container file:** ένα αρχείο που μπορεί να περιέχει πολλαπλά ρεύματα μέσω των οποίων συχνά αποτελούν μια παρουσίαση όταν αναπαράγονται μαζί. Οι RTSP εξυπηρετητές μπορούν να προσφέρουν συνολική διαχείριση (aggregate control) πάνω σε αυτά τα αρχεία παρόλο που το θέμα του container file δεν εμπεδώνεται στο πρωτόκολλο.

➤ **Continuous media:** δεδομένα στα οποία υπάρχει μια χρονική σχέση μεταξύ πηγής και καταναλωτή. Αυτό σημαίνει ότι ο καταναλωτής πρέπει να αναπαράγει την χρονική σχέση που υπήρχε στην πηγή. Τα πιο κοινά παραδείγματα συνεχών μέσων είναι ο ήχος και το βίντεο κίνησης (motion video). Τα συνεχή μέσα μπορούν να είναι είτε πραγματικού χρόνου (ζωντανά, real-time) όπου υπάρχει μια στενή σχέση χρονισμού μεταξύ πηγής και καταναλωτή, είτε streaming (playback, αναπαραγόμενα) όπου η χρονική σχέση είναι πιο χαλαρή.

⁷ Host: Στο βιβλίο «Δίκτυα Υπολογιστών, Δεύτερη Έκδοση» της μετάφρασης του ομώνυμου βιβλίου του Andrew

➤ **Entity:** η πληροφορία που μεταφέρεται ως φορτίο μιας αίτησης ή απόκρισης. Μια οντότητα αποτελείται από μεταπληροφορίες, στη μορφή του πεδίου entity-header, και από περιεχόμενα στη μορφή του entity-body.

➤ **Media initialization:** ειδική αρχικοποίηση των datatype/codec (τύπος δεδομένων και τύπος ή μορφή κωδικοποίησης). Κάτι τέτοιο περιλαμβάνει αντικείμενα όπως χρονισμός (clockrates), πίνακες χρωμάτων, κ.λ.π.. Οποιαδήποτε ανεξάρτητη μεταφοράς πληροφορία απαιτείται από τον πελάτη για αναπαραγωγή κάποιου ρεύματος μέσω, προκύπτει κατά την φάση της αρχικοποίησης του μέσου (media initialization) στην εγκατάσταση του ρεύματος.

➤ **Media parameter:** μια ιδιαίτερη παράμετρος με κάποιο τύπο μέσου που μπορεί να μεταβληθεί πριν ή κατά τη διάρκεια αναπαραγωγής του ρεύματος.

➤ **Media server:** ο εξυπηρετητής που παρέχει υπηρεσίες αναπαραγωγής ή καταγραφής σε ένα ή περισσότερα ρεύματα μέσω. Είναι δυνατό να δημιουργηθούν διαφορετικά ρεύματα μέσω από διαφορετικούς εξυπηρετητές μέσω. Κάποιος εξυπηρετητής μέσω μπορεί να διαμένει στον ίδιο ή και σε διαφορετικό ξενιστή (host) όπως είναι ο web server από όπου ενεργοποιήθηκε η παρουσίαση.

➤ **Media server indirection:** ανακατεύθυνση ενός πελάτη μέσω (media client) σε κάποιον διαφορετικό εξυπηρετητή μέσω.

➤ **(Media) stream:** ένα μοναδικό γεγονός μέσου, π.χ. ένα ρεύμα ήχου ή ένα ρεύμα βίντεο. Όταν χρησιμοποιείται το RTP ένα ρεύμα αποτελείται από όλα τα RTP και RTCP πακέτα που έχουν δημιουργηθεί από κάποια πηγή που συμμετέχει στην RTP συνεδρία. Είναι ισοδύναμο με τον ορισμό ενός DSM-CC stream (ISO/IEC, 1995).

➤ **Message:** η βασική μονάδα της RTSP επικοινωνίας που αποτελείται από μια δομημένη ακολουθία από οκτάδες και που μεταδίδεται μέσω κάποιου connection ή connectionless πρωτοκόλλου.

➤ **Participant:** το μέλος μιας διάσκεψης. Ο μετέχων μπορεί να είναι και μια μηχανή, για παράδειγμα ένας εξυπηρετητής για αναπαραγωγή μέσω.

➤ **Presentation:** ένα σύνολο από ένα ή περισσότερα ρεύματα που παρουσιάζονται στον πελάτη ως μια ολοκληρωμένη τροφοδοσία μέσω, χρησιμοποιώντας μια περιγραφή όπως αυτή ορίζεται αμέσως παρακάτω. Στις περισσότερες περιπτώσεις στο περιβάλλον του RTSP κάτι τέτοιο σημαίνει αθροιστικός έλεγχος (aggregate control) αυτών των ρευμάτων αλλά χωρίς αυτό να είναι και απόλυτο.

➤ **Presentation description:** μια τέτοια περιγραφή παρουσίασης περιέχει πληροφορίες σχετικά με ένα ή περισσότερα ρεύματα μέσα σε μια παρουσίαση. Τέτοιες πληροφορίες μπορεί να είναι οι κωδικοποιήσεις, οι δικτυακές διευθύνσεις και πληροφορίες γύρω από το περιεχόμενο.

Άλλα IETF πρωτόκολλα όπως το SDP (Handley & Jacobson, 1998) χρησιμοποιούν τον όρο συνεδρία (session) για μια ζωντανή παρουσίαση. Η περιγραφή αυτή μπορεί να πάρει πολλές διαφορετικές μορφές που περιέχονται αλλά δεν περιορίζονται από την περιγραφή της μορφής της συνεδρίας στο SDP.

➤ **Response:** είναι μια RTSP απόκριση. Αν εννοείται μια HTTP απόκριση τότε κάτι τέτοιο δηλώνεται ρητά.

➤ **Request:** είναι μια RTSP αίτηση. Αν εννοείται μια HTTP αίτηση τότε κάτι τέτοιο δηλώνεται ρητά.

➤ **RTSP session:** μια ολοκληρωμένη RTSP συναλλαγή (transaction) όπως για παράδειγμα η παρακολούθηση μιας κινηματογραφικής ταινίας. Τυπικά μια συνεδρία αποτελείται από το στήσιμο ενός μηχανισμού μεταφοράς για το συνεχές ρεύμα μέσω από την πλευρά του πελάτη (SETUP), έναρξη του stream με το PLAY ή το RECORD και κλείσιμο του stream με το TEARDOWN. (οι αγγλικές λέξεις με κεφαλαία αποτελούν εντολές του πρωτοκόλλου).

➤ **Transport initialization:** η διαπραγμάτευση των πληροφοριών μεταφοράς (όπως είναι οι αριθμοί των θυρών, το πρωτόκολλο μεταφοράς κλπ.) μεταξύ του πελάτη και του εξυπηρετητή.

5. *Ιδιότητες του πρωτοκόλλου.*

Το RTSP έχει τις εξής ιδιότητες:

✓ **Είναι επεκτάσιμο.** Μπορούν πολύ εύκολα να προστεθούν στο RTSP νέες μέθοδοι και παράμετροι.

✓ **Είναι εύκολο να γίνει μεταγλωττιστεί σε μια ενδιάμεση μορφή και αυτή η μορφή να μεταφράζεται στη συνέχεια από τους κατάλληλους μεταφραστές (parsers).** Το RTSP μπορεί να γίνει parsed από τους συνήθεις HTTP ή MIME parsers.

✓ **Είναι ασφαλές.** Το RTSP επαναχρησιμοποιεί τους μηχανισμούς ασφαλείας του web. Όλοι οι HTTP μηχανισμοί πιστοποίησης (Fielding et al., 1997, Section 11.1.) όπως η βασική ή η συνοπτική (digest) πιστοποίηση (authentication) (Postel, 1980) είναι εφαρμόσιμοι απευθείας.

✓ **Είναι ανεξάρτητο του επιπέδου μεταφοράς.** Το RTSP μπορεί να χρησιμοποιήσει είτε το unreliable datagram protocol (UDP) (RFC 768, Hinden & Partridge, 1990) είτε το reliable datagram protocol (RDP, (RFC 1151, Postel, 1981) δεν είναι πολύ διαδεδομένο), είτε ένα αξιόπιστο stream πρωτόκολλο όπως το TCP (RFC 793, Schulzrinne, 1997).

✓ **Είναι multi-server capable.** Αυτό σημαίνει ότι κάθε ρεύμα μέσω που μετέχει σε μια παρουσίαση μπορεί να παραμένει σε διαφορετικό εξυπηρετητή. Ο πελάτης εγκαθιστά αυτόματα πολλά sessions διαχείρισης, με τους διάφορους εξυπηρετητές μέσω, που εκτελούνται παράλληλα. Ο συγχρονισμός των μέσω εκτελείται στο επίπεδο μεταφοράς.

✓ **Διαχειρίζεται τις συσκευές εγγραφής.** Το πρωτόκολλο μπορεί να διαχειριστεί τόσο τις συσκευές αναπαραγωγής όσο και εγγραφής καθώς και συσκευές που μπορούν να εναλλάσσονται μεταξύ των δύο ρόλων.

✓ **Διαχωρισμός μεταξύ της διαχείρισης του ρεύματος και της έναρξης της διάσκεψης.** Η διαχείριση του ρεύματος έχει χωριστεί από την πρόσκληση κάποιου εξυπηρετητή μέσω σε μια συνδιάσκεψη. Η μόνη απαίτηση που υπάρχει είναι το πρωτόκολλο έναρξης είτε να παρέχει είτε να μπορεί να χρησιμοποιηθεί για να παράγει μοναδικούς δείκτες διάσκεψης. Συγκεκριμένα μπορεί να χρησιμοποιηθεί το SIP ή το H.323 (International Telecommunication Union, 1996) για να προσκληθεί ένας εξυπηρετητής σε κάποια συνδιάσκεψη.

✓ **Είναι κατάλληλο για επαγγελματικές εφαρμογές.** Το RTSP υποστηρίζει ακρίβεια σε επίπεδο πλαισίου (frame) μέσω των SMPTE χρονοσφραγίδων έτσι ώστε να επιτρέπει την απομακρυσμένη ψηφιακή επεξεργασία.

✓ **Χρησιμοποιεί ουδέτερη περιγραφή παρουσίασης.** Το πρωτόκολλο δεν επιβάλλει κάποια συγκεκριμένη μορφή περιγραφής της παρουσίασης ή κάποια ειδική metafile (συνοδευτικό αρχείο συμπληρωματικών πληροφοριών) μορφοποίηση (format) και μπορεί να μεταφέρει τον τύπο της μορφοποίησης που πρόκειται να χρησιμοποιηθεί. Ωστόσο η περιγραφή πρέπει να περιέχει τουλάχιστον μια RTSP URL.

✓ **Είναι proxy και firewall friendly.** Το πρωτόκολλο πρέπει να βρίσκεται σε ετοιμότητα ώστε να διαχειριστεί από τους φράκτες (firewalls) τόσο επιπέδου εφαρμογής όσο και επιπέδου μεταφοράς (McMahon, 1996). Ένας φράκτης πρέπει να μπορεί να κατανοήσει τη SETUP διαδικασία έτσι ώστε να ανοίξει μια «τρύπα» για το UDP ρεύμα μέσω.

✓ **Είναι HTTP friendly.** Το RTSP όντας ευαίσθητο, επαναχρησιμοποιεί τις αρχές που διέπουν το HTTP έτσι ώστε να μπορεί να ξαναχρησιμοποιηθεί η υπάρχουσα υποδομή. Αυτή η υποδομή περιλαμβάνει PICS (Platform for Internet Content Selection) για την αντιστοίχιση ετικετών με το περιεχόμενο (Miller et al., 1996). Ωστόσο το RTSP δεν προσθέτει απλά μεθόδους στο HTTP μιας και η διαχείριση συνεχών μέσω απαιτεί στις περισσότερες περιπτώσεις να βρίσκεται στην πλευρά του εξυπηρετητή.

✓ **Κάνει κατάλληλη διαχείριση του εξυπηρετητή.** Αν ένας πελάτης μπορεί να ξεκινήσει ένα stream τότε πρέπει να έχει επίσης και τη δυνατότητα να το σταματήσει. Οι εξυπηρετητές δεν πρέπει να ξεκινούν ρεύματα συνεχούς ροής δεδομένων προς τους πελάτες κατά τέτοιο τρόπο που να μην δίνεται στους πελάτες η δυνατότητα να τα σταματήσουν.

✓ **Διαπραγματεύσεις μεταφοράς.** Ο πελάτης μπορεί να διαπραγματευτεί κάποια μέθοδο προτού την χρειαστεί πραγματικά για να επεξεργαστεί κάποιο συνεχές ρεύμα μέσω.

✓ **Δυνατότητα διαπραγμάτευσης.** Πρέπει να υπάρχουν κάποιοι σαφείς μηχανισμοί από πλευράς του πελάτη που να καθορίζουν ποιες μέθοδοι δεν θα υλοποιηθούν σε περίπτωση που τα

βασικά χαρακτηριστικά είναι απενεργοποιημένα. Κάτι τέτοιο επιτρέπει στους πελάτες να εμφανίζουν το κατάλληλο user interface. Αν για παράδειγμα δεν επιτρέπεται η αναζήτηση μέσα στην παρουσίαση τότε το GUI (Graphical User Interface) πρέπει να έχει τη δυνατότητα να απενεργοποιήσει την μετακίνηση του ολισθαίνοντα δείκτη θέσης της παρουσίασης.

Σημειώσεις:

1. Μια παλαιότερη απαίτηση ήταν το πρωτόκολλο να έχει δυνατότητες για πολλούς πελάτες (multi-client capabilities). Ωστόσο αποφασίστηκε ότι είναι καλύτερη προσέγγιση να εξασφαλιστεί ότι το πρωτόκολλο είναι εύκολα επεκτάσιμο στο multi-client μοντέλο.

2. Το πρωτόκολλο δεν καταγράφει πώς οι διάφοροι πελάτες διαπραγματεύονται την πρόσβασή τους. Κάτι τέτοιο έχει αφεθεί είτε σε κάποιο «κοινωνικό πρωτόκολλο» είτε σε κάποιον μηχανισμό διαχείρισης διαφορετικού επιπέδου.

6. Η γενική λειτουργία του πρωτοκόλλου.

Κάθε παρουσίαση και κάθε ρεύμα μέσων μπορεί να προσδιοριστεί από μια RTSP URL. Η συνολική παρουσίαση και οι ιδιότητες των μέσων από τα οποία αποτελείται είναι καθορισμένα από το αρχείο περιγραφής. Αυτό το αρχείο μπορεί να αποκτηθεί από τον πελάτη χρησιμοποιώντας το HTTP ή άλλα μέσα όπως το ηλεκτρονικό ταχυδρομείο (email) και μπορεί να μην αποθηκευθεί απαραίτητα στον εξυπηρετητή μέσων. Για να ικανοποιούνται αυτές οι προδιαγραφές θεωρείται ότι η περιγραφή παρουσίασης (presentation description) περιγράφει μία ή περισσότερες παρουσιάσεις, καθεμιά των οποίων διατηρεί έναν κοινό χρονικό άξονα. Θεωρούμε για λόγους απλότητας και χωρίς να επηρεαστεί η γενικότητα ότι η περιγραφή παρουσίασης περιέχει ακριβώς μία τέτοια παρουσίαση.

Μια παρουσίαση μπορεί να περιέχει πολλά ρεύματα μέσων. Το αρχείο περιγραφής της περιέχει τις περιγραφές των ρευμάτων που την συνθέτουν περιλαμβάνοντας και τις κωδικοποιήσεις τους, την γλώσσα καθώς και άλλες παραμέτρους που εξουσιοδοτούν τον πελάτη να διαλέξει τον καταλληλότερο συνδυασμό των μέσων. Μέσα σ' αυτή την περιγραφή παρουσίασης κάθε ρεύματος μέσων, που είναι ξεχωριστά διαχειριζόμενο από το RTSP, προσδιορίζεται από κάποια RTSP URL που οδηγεί στον εξυπηρετητή μέσων που διαχειρίζεται το συγκεκριμένο ρεύμα μέσων και ονομάζει το ρεύμα που είναι αποθηκευμένο σ' αυτόν. Διάφορα ρεύματα μέσων μπορούν να τοποθετηθούν σε διαφορετικούς εξυπηρετητές. Για παράδειγμα τα ρεύματα ήχου και βίντεο μπορούν να χωριστούν σε διάφορους εξυπηρετητές έτσι ώστε να φορτώνονται κατανεμημένα. Εκτός αυτών η περιγραφή απαρτιθμεί της μεθόδους μεταφοράς που έχει τη δυνατότητα να υποστηρίξει ο εξυπηρετητής.

Είναι αναγκαίο να καθοριστούν, εκτός των παραμέτρων των μέσων, και η δικτυακή διεύθυνση προορισμού καθώς και οι θύρες που πρόκειται να χρησιμοποιηθούν. Μπορούμε να διακρίνουμε διάφορους τρόπους λειτουργίας:

➤ *Unicast*: Τα μέσα μεταδίδονται στην πηγή της RTSP αίτησης με τον αριθμό θύρας που επιλέχθηκε από τον πελάτη. Εναλλακτικά, τα μέσα μεταδίδονται με το ίδιο αξιόπιστο ρεύμα όπως και το RTSP.

➤ *Multicast, με τον εξυπηρετητή να επιλέγει την διεύθυνση*: Σ' αυτή την περίπτωση την multicast διεύθυνση και τη θύρα την επιλέγει ο εξυπηρετητής μέσω. Αυτή είναι η τυπική περίπτωση ζωντανής ή σχεδόν media-on-demand μετάδοσης.

➤ *Multicast, όπου ο πελάτης επιλέγει την διεύθυνση*: Αν ο εξυπηρετητής πρόκειται να συμμετάσχει σε μια υπάρχουσα multicast συνδιάσκεψη, η διεύθυνση, η θύρα και το κλειδί κρυπτογράφησης δίνονται από την περιγραφή της συνδιάσκεψης.

7. Καταστάσεις του RTSP.

Το RTSP διαχειρίζεται ένα stream που μπορεί να έχει σταλεί μέσω κάποιου άλλου πρωτοκόλλου ανεξάρτητου από το κανάλι διαχείρισης. Η RTSP διαχείριση, για παράδειγμα, μπορεί να προκύψει σε μια TCP σύνδεση τη στιγμή που τα δεδομένα ρέουν μέσω UDP. Για αυτό η διανομή δεδομένων συνεχίζεται ακόμα κι αν δεν παραλαμβάνονται RTSP αιτήσεις από τον εξυπηρετητή. Επίσης κατά τη διάρκεια ύπαρξής του, ένα ρεύμα μέσω μπορεί να διαχειρίζεται από RTSP αιτήσεις που εκπέμπονται αλυσιδωτά από διαφορετικές TCP συνδέσεις. Για αυτό τον λόγο χρειάζεται να διατηρεί ο εξυπηρετητής την κατάσταση της συνεδρίας έτσι ώστε να είναι σε θέση να συσχετίζει τις RTSP αιτήσεις με το stream. Πολλές μέθοδοι στο RTSP δεν συνεισφέρουν στην κατάσταση.

Στη συνέχεια παρατίθενται οι σημαντικότερες μέθοδοι για τον καθορισμό της δέσμευσης και χρήσης των πόρων του ρεύματος σε έναν εξυπηρετητή.

- **SETUP**: Προκαλεί τον εξυπηρετητή να δεσμεύσει πόρους για ένα stream και να ξεκινήσει μία RTSP συνεδρία.

- **PLAY και RECORD**: Ξεκινά τη μετάδοση δεδομένων ενός stream που δεσμεύτηκε μέσω της κατάστασης SETUP. Η αίτηση PLAY χρησιμοποιείται για την αναπαραγωγή του μέσου ενώ η RECORD για την εγγραφή και αποθήκευσή του.

- **PAUSE**: Σταματά προσωρινά κάποιο stream χωρίς να απελευθερώσει τους πόρους που έχει δεσμεύσει ο εξυπηρετητής για αυτό.

- **TEARDOWN**: Ελευθερώνει τους πόρους που αντιστοιχούν στο stream. Η RTSP συνεδρία σταματά να υπάρχει στον εξυπηρετητή.

Οι RTSP μέθοδοι που συνεισφέρουν στην κατάσταση χρησιμοποιούν το session πεδίο της επικεφαλίδας για την ανίχνευση της RTSP συνεδρίας του οποίου η κατάσταση τελεί υπό διαχείριση. Ο εξυπηρετητής παράγει δείκτες συνεδρίας (session identifiers) σε απόκριση των SETUP αιτήσεων.

8. Σχέση με άλλα πρωτόκολλα.

Στο RTSP υπάρχει μια αλληλοεπικάλυψη ως αναφορά στη λειτουργία του με το HTTP. Μπορεί επίσης να αλληλεπιδρά με το HTTP στο ότι η αρχική σύνδεση με streaming περιεχόμενο πρόκειται να πραγματοποιηθεί μέσω μιας σελίδας του web. Οι προδιαγραφές του πρωτοκόλλου στοχεύουν να επιτρέπουν διάφορα σημεία συναλλαγών μεταξύ ενός εξυπηρετητή web και του εξυπηρετητή μέσων που υλοποιεί το RTSP. Για παράδειγμα να αναφέρουμε ότι η περιγραφή παρουσίασης μπορεί να ανακτηθεί είτε χρησιμοποιώντας RTSP είτε HTTP κάτι που περιορίζει τις παλινδρομήσεις στις περιπτώσεις που βασίζονται σε πλοηγητή ιστοσελίδων (web browser) και ισχύει ακόμα και στην περίπτωση που έχουμε μεμονωμένους (standalone) RTSP εξυπηρετητές και πελάτες που δεν στηρίζονται καθόλου στο HTTP.

Ωστόσο το RTSP διαφέρει ριζικά από το HTTP στο ότι η διανομή δεδομένων πραγματοποιείται με διαφορετικό πρωτόκολλο. Το HTTP είναι ένα ασύμμετρο πρωτόκολλο όπου ο πελάτης δημιουργεί αιτήσεις και ο εξυπηρετητής ανταποκρίνεται σ' αυτές. Στο RTSP μπορούν να δημιουργήσουν αιτήσεις τόσο ο πελάτης μέσω των μέσων όσο και ο εξυπηρετητής μέσω των μέσων. Επίσης οι RTSP αιτήσεις δεν στερούνται κατάστασης (stateless). Έτσι έχουν την δυνατότητα να συνεχίσουν να καθορίζουν παραμέτρους και να διαχειρίζονται κάποιο ρεύμα μέσων για αρκετό χρονικό διάστημα μετά την βεβαίωση της λήψης της αίτησης. Η επαναχρησιμοποίηση της λειτουργικότητας του HTTP έχει πλεονεκτήματα σε τουλάχιστον δύο περιπτώσεις κι αυτές είναι η ασφάλεια και οι proxies. Υπάρχουν σχεδόν οι ίδιες απαιτήσεις και έτσι η δυνατότητα να χρησιμοποιηθεί ο τρόπος που λειτουργεί το HTTP στις caches (ενδιάμεσοι αποθηκευτικοί χώροι), στους proxies και στην πιστοποίηση είναι πολύτιμη.

Παρόλο που τα περισσότερα μέσα πραγματικού χρόνου (real-time media) θα χρησιμοποιήσουν το RTP ως πρωτόκολλο μεταφοράς, το RTSP δεν συνδέεται στενά με αυτό. Το RTSP θεωρεί ότι υπάρχει μια μορφοποίηση περιγραφής παρουσίασης (presentation description format) που μπορεί να εκφράσει τόσο στατικές όσο και προσωρινές ιδιότητες μιας παρουσίασης που περιέχει διάφορα ρεύματα μέσων.

9. Συνδέσεις.

Οι RTSP αιτήσεις μπορούν να μεταδοθούν με διάφορους τρόπους:

- ❖ Να χρησιμοποιούνται για διάφορες συναλλαγές αίτησης-απόκρισης συνεχείς συνδέσεις μεταφοράς.
- ❖ Να χρησιμοποιείται μια σύνδεση ανά συναλλαγή.
- ❖ Να χρησιμοποιείται χωρίς απαίτηση σύνδεσης (connectionless) μορφή σύνδεσης.

Ο τύπος της σύνδεσης μεταφοράς (transport connection) καθορίζεται από την RTSP URL.

Σε αντίθεση με το HTTP, το RTSP επιτρέπει στον εξυπηρετητή να στέλνει αιτήσεις στον πελάτη. Ωστόσο κάτι τέτοιο υποστηρίζεται μόνο από συνεχείς συνδέσεις μιας και ο εξυπηρετητής μέσω δεν έχει σε αντίθετη περίπτωση ασφαλή τρόπο να προσεγγίσει τον πελάτη. Εκτός αυτού είναι και ο μοναδικός τρόπος με τον οποίο οι αιτήσεις από τον εξυπηρετητή μέσω στον πελάτη μπορούν να διαβούν τους φράκτες (firewalls).

9.1. Pipelining.

Ο πελάτης που υποστηρίζει συνεχείς συνδέσεις ή μορφή χωρίς απαίτηση σύνδεσης (*connectionless mode*) μπορεί να διοχετεύσει τις αιτήσεις του χρησιμοποιώντας την τεχνική διασωλήνωσης (*pipeline*) (δηλ. να στείλει πολλαπλές αιτήσεις χωρίς να περιμένει την απόκριση της καθεμιάς). Σε τέτοια περίπτωση ο εξυπηρετητής πρέπει να στείλει τις αποκρίσεις των αιτήσεων κατά την ίδια σειρά με την οποία αυτές παρελήφθησαν.

9.2. Αξιοπιστία και βεβαιώσεις λήψης.

Οι λήψεις των αιτήσεων επιβεβαιώνονται από τον παραλήπτη εκτός κι αν αυτές αποστέλλονται σ' ένα multicast σύνολο. Αν δεν υπάρξει καμιά επιβεβαίωση λήψης τότε ο αποστολέας μπορεί να ξαναστείλει το ίδιο μήνυμα μετά την έλευση κάποιου συγκεκριμένου χρονικού διαστήματος που ισούται με το χρόνο της μεταφοράς του μηνύματος στον προορισμό και της επιστροφής του στον αποστολέα (round-trip time, RTT). Αυτός ο χρόνος εκτιμάται όπως και στο TCP με μια αρχική τιμή των 500 ms (Braden, 1989). Κάποια υλοποίηση μπορεί να αποθηκεύσει προσωρινά την τελευταία μέτρηση του RTT ως την αρχική τιμή για χρήση της σε μελλοντικές συνδέσεις.

Στην περίπτωση που χρησιμοποιείται κάποιο αξιόπιστο πρωτόκολλο μεταφοράς για να μεταφέρει το RTSP δεν πρέπει σε καμία περίπτωση να ξαναμεταδίδονται οι αιτήσεις. Αντί αυτού η RTSP εφαρμογή πρέπει να βασίζεται στην αξιοπιστία που παρέχει το υποκείμενο πρωτόκολλο μεταφοράς.

Αν και το υποκείμενο αξιόπιστο πρωτόκολλο μεταφοράς όπως το TCP αλλά και η RTSP εφαρμογή ξαναμεταδίδουν αιτήσεις, τότε είναι πιθανό κάθε απώλεια πακέτου να προκαλέσει διπλή επαναμετάδοση. Τυπικά ο αποδέκτης δεν είναι σε θέση να εκμεταλλευτεί την επαναμετάδοση του επιπέδου εφαρμογής, μιας και η στοίβα μεταφοράς δε θα παραδώσει αυτήν την επαναμετάδοση προτού φτάσει η πρώτη απόπειρα στον αποδέκτη. Αν η απώλεια του πακέτου οφείλεται σε σύγκρουση τότε οι πολλαπλές επαναμεταδόσεις, σε διαφορετικά επίπεδα, θα χειροτερέψουν την κατάσταση των συγκρούσεων.

Για την αποφυγή του προβλήματος της αμφιβολίας και της επαναμετάδοσης, χρησιμοποιείται η Timestamp επικεφαλίδα (Stevens, 1994, σ. 301). Κάθε αίτηση μεταφέρει έναν αριθμό σειράς στο πεδίο CSeq της επικεφαλίδας, που αυξάνεται κατά ένα για κάθε διακριτή αίτηση που μεταδίδεται.

Αν η αίτηση επαναμεταδοθεί λόγω έλλειψης επιβεβαίωσης λήψης της, τότε πρέπει να φέρει τον αρχικό (αυθεντικό) αριθμό σειράς (δηλ. να μην έχει αυξηθεί αυτός ο αριθμός).

Τα συστήματα που υλοποιούν το RTSP πρέπει να υποστηρίζουν την μεταφορά του RTSP πάνω από το TCP, όπως επίσης πρέπει να υποστηρίζουν το UDP. Ο προκαθορισμένος αριθμός θύρας που χρησιμοποιείται από τον RTSP εξυπηρετητή είναι 554 τόσο για το TCP όσο και στην περίπτωση του UDP.

Κάποιος αριθμός RTSP πακέτων που προορίζεται για τον ίδιο προορισμό είναι δυνατό να πακεταριστεί σε μια μόνο χαμηλότερου επιπέδου PDU ή να ενθυλακωθεί σε ένα TCP stream. Τα RTSP δεδομένα μπορούν να διαστρωματοποιηθούν με RTP και RTCP πακέτα. Σε αντίθεση με το HTTP το RTSP μήνυμα πρέπει να περιέχει μια επικεφαλίδα μεγέθους του περιεχομένου, όποτε υπάρχει μέσα στο μήνυμα κάποιο φορτίο. Διαφορετικά το RTSP πακέτο τελειώνει με μια κενή γραμμή αμέσως μετά την τελευταία επικεφαλίδα του μηνύματος.

Σ' αυτό το σημείο ολοκληρώνεται η γενική περιγραφή του RTSP διότι περαιτέρω εμβάθυνση οδηγεί αναπόφευκτα ανάλυση τεχνικών όρων και λεπτομερειών.

Αναφορές (References)

- (Balenson, 1993) Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", *RFC 1423*, TIS, IAB IRTF PSRG, IETF PEM WG, February 1993.
- (Braden, 1989) Braden, R., "Requirements for Internet Hosts - Application and Support", *STD 3, RFC 1123*, Internet Engineering Task Force, October 1989.
- (Clark & Tennenhouse, 1990) Clark, D. D. and Tennenhouse, D. L. "Architectural considerations for a new generation of protocols," in *SIGCOMM Symposium on Communications Architectures and Protocols*, (Philadelphia, Pennsylvania), pp. 200--208, IEEE, Sept. 1990. *Computer Communications Review*, Vol. 20(4), Sept. 1990.
- (Fielding, 1997) Fielding, R., Gettys, J., Mogul, J., Nielsen, H., and T. Berners-Lee, "Hypertext transfer protocol - HTTP/1.1", *RFC 2068*, January 1997.
- (Schulzrinne, 1997) Schulzrinne, H. "A comprehensive multimedia control architecture for the Internet," in Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV), (St. Louis, Missouri), May 1997.
- (Handley & Jacobson, 1998) Handley, M., and Jacobson, V. "SDP: Session Description Protocol", *RFC 2327*, April 1998.
- (Hinden et al., 1990) Hinden, B. and C. Partridge, "Version 2 of the reliable data protocol (RDP)", *RFC 1151*, April 1990.
- (Busse et al., 1996) Busse, I., Deffner, B. and Schulzrinne, H. "Dynamic QoS control of multimedia applications based on RTP," *Computer Communications*, Jan. 1996.
- (International Telecommunication Union, 1996) International Telecommunication Union, "Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service," Recommendation H.323, Telecommunication Standardization Sector of ITU, Geneva, Switzerland, May 1996.
- (ISO/IEC, 1995) ISO/IEC, "Information technology - generic coding of moving pictures and associated audio information - part 6: extension for digital storage media and control," Draft International Standard ISO 13818-6, International Organization for Standardization ISO/IEC JTC1/SC29/WG11, Geneva, Switzerland, Nov. 1995.
- (Miller et al., 1996) Miller, J. Krauskopf, T. Resnick, P. and Treese, W. "PICS label distribution label syntax and communication protocols," Recommendation REC-PICS-labels-961031, W3C (World Wide Web Consortium), Boston, Massachusetts, Oct. 1996.

- (Bolot et al., 1994) Bolot, J.-C. Turetletti, T. and Wakeman, I. "Scalable feedback control for multicast video distribution in the internet," in *SIGCOMM Symposium on Communications Architectures and Protocols*, (London, England), pp. 58--67, ACM, Aug. 1994.
- (McMahon, 1996) McMahon, P., "GSS-API authentication method for SOCKS version 5", RFC 1961, June 1996.
- (Postel, 1981) Postel, J., "Transmission control protocol", STD 7, RFC 793, September 1981.
- (Stubblebine, 1993) Stubblebine, S. "Security services for multimedia conferencing," in *16th National Computer Security Conference*, (Baltimore, Maryland), pp. 391--395, Sept. 1993.
- (Schulzrinne, 1996) Schulzrinne, H., "RTP profile for audio and video conferences with minimal control", RFC 1890, January 1996.
- (Schulzrinne et al., 1996) Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, "RTP: a transport protocol for real-time applications", RFC 1889, January 1996.
- (Tanenbaum, 1992) Tanenbaum, A. *Δίκτυα Υπολογιστών, Δεύτερη έκδοση*. Prentice-Hall, inc - Παπασωτηρίου, 1992.
- (The Unicode Consortium, 1991) The Unicode Consortium, *The Unicode Standard New York*, New York: Addison-Wesley, 1991.
- (Voydoc & Kent, 1983) Voydock, V. L. and Kent, S. T. "Security mechanisms in high-level network protocols," *ACM Computing Surveys*, vol. 15, pp. 135--171, June 1983.
- (Feller, 1968) Feller, W. *An Introduction to Probability Theory and its Applications*, Volume 1, vol. 1. New York, New York: John Wiley and Sons, third ed., 1968.
- (Stevens, 1994) Stevens, W. R. *TCP/IP illustrated: the implementation*, vol. 2. Reading, Massachusetts: Addison-Wesley, 1994.
- (Yergeau, 1998) Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.