19 Γιατί παίρνουμε μόνο ένα μικρό ποσοστό από τη διαφημιζόμενη ταχύτητα στο 4G;

Μετά το τέλος αυτού του κεφαλαίου, θα θεωρείτε τον εαυτό σας τυχερό που παίρνει έστω ένα μικρό ποσοστό από την διαφημιζόμενη ταχύτητα. Πού πήγε όμως το υπόλοιπο;

19.1 Μία Σύντομη Απάντηση

Κατ' αρχάς, οι όροι 3G και 4G δεν είναι απόλυτα σαφείς. Υπάρχει μία τεχνολογία η οποία ακολουθεί τον οργανισμό προτυποποίησης 3GPP η οποία ονομάζεται UMTS ή WCDMA, και μία άλλη τεχνολογία η οποία ακολουθεί το πρότυπο 3GPP2 και ονομάζεται CDMA2000. Κάθε μία από αυτές έχει πολλές διαφορετικές εκδόσεις μεταξύ του 2G και του 3G, οι οποίες συχνά αποκαλούνται 2.5G, όπως τα EDGE, EVDO κτλ. Για το 4G η κύρια τεχνολογία καλείται Long Term Evolution (LTE) με παραλλαγές όπως τις LTE light και LTE advanced. Μία άλλη ανταγωνιστική τεχνολογία είναι το WiMAX. Μερικοί αναφέρονται ακόμη και στις προηγμένες εκδόσεις του 3G, όπως το HSPA+ ως 4G. Όλα αυτά έχουν δημιουργήσει σύγχυση στο μυαλό του καταναλωτή όσον αφορά στο ποια είναι η πραγματική τεχνολογία 3G και ποια είναι η πραγματική τεχνολογία 4G.

Θα έχετε πιθανόν διαβάσει ότι η ταχύτητα λήψης της τεχνολογίας για στατικούς χρήστες θα έπρεπε να είναι 7,2 Mbps. Αλλά όταν προσπαθείτε να μεταφορτώσετε ένα συνημμένο αρχείο ηλεκτρονικού ταχυδρομείου, μεγέθους 3MB, αυτό μπορεί συνήθως να διαρκέσει έως και ενάμιση λεπτό. Η ταχύτητα λήψης που λαμβάνετε είναι 267 Kbps, η οποία είναι το 3,7% από αυτή που αναμένατε. Ποιος πήρε το υπόλοιπο 96%;

Πολλές χώρες κινούνται προς το LTE. Χρησιμοποιείται ένα μεγάλο εύρος τεχνικών το οποίο αυξάνει τη φασματική απόδοση, η οποία ορίζεται ως ο αριθμός των bit ανά δευτερόλεπτο τα οποία μπορεί να υποστηρίξει κάθε Hz του εύρους ζώνης. Αυτές συμπεριλαμβάνουν τις OFDM και MIMO, όπως αναφέρθηκε στο τέλος του προηγούμενου κεφαλαίου, και το διαχωρισμό μίας μεγάλης κυψέλης σε μικρότερες. Αλλά η διαπερατότητα που παρατηρεί ο χρήστης στο 4G, αν και αρκετά μεγαλύτερη από αυτή του 3G, είναι ακόμα πολύ μικρότερη από τις διαφημιζόμενες τιμές, οι οποίες ακούμε ότι είναι στη περιοχή των 300 Mbps. Γιατί συμβαίνει αυτό;

Υπάρχουν δύο βασικοί λόγοι: μη ιδανικές συνθήκες δικτύου και οι επιβαρύνσεις. Πολλά τμήματα του ασύρματου δικτύου παρουσιάζουν μη ιδανικές συνθήκες συμπεριλαμβανόμενων του δικτύου εναέριας μετάδοσης καθώς και του ενσύρματου δικτύου. Επιπλέον, τα δίκτυα, όπως και οι ζωές μας, κυριαρχούνται από επιβαρύνσεις, όπως η επιβάρυνση του δικτύου διαχείρισης με τη μορφή των bit έλεγχου των πακέτων ή ακολουθιών ελέγχου στα πρωτόκολλα.

Αυτό το κεφάλαιο είναι κατά κάποιο τρόπο η «επιβάρυνση» αυτού του βιβλίου: δεν υπάρχουν άλλα περαιτέρω πιο «βαθιά» μηνύματα εκτός από τη σημασία των επικεφαλίδων: η δικτύωση δεν αφορά μόνο τη βελτιστοποίηση των μετρικών απόδοσης όπως της διαπερατότητας, αλλά συμπεριλαμβάνει και το αναπόφευκτο κόστος της διαχείρισης του δικτύου.

Ας δούμε κάποιες λεπτομέρειες σχετικά με τρεις σημαντικές παραμέτρους μείωσης της ταχύτητας, ή, πιο εύστοχα, της μείωσης της ωφέλιμης διαπερατότητας μεταξύ του πομπού και του δέκτη σε μία συνεδρία. Η ωφέλιμη διαπερατότητα που ορίζεται ως ο αριθμός των bit των πραγματικών δεδομένων της εφαρμογής που ελήφθησαν δια του χρόνου που απαιτείται για να περάσουν τα δεδομένα. Αυτό είναι τι πραγματικά "αισθάνεστε" ότι παίρνετε ως υπηρεσία αλλά αυτό δεν είναι αυτό που διαφημίζεται είτε αυτό που μετράνε τα τεστ ταχύτητας.

19.1.1 Εναέριο δίκτυο

1. *Κανάλι μετάδοσης*: Τα ασύρματα κανάλια μετάδοσης υποφέρουν από διάφορους τύπους υποβάθμισης, συμπεριλαμβανομένης της απώλειας μονοπατιού (όπου η ισχύς του σήματος εξασθενεί όσο αυξάνεται η απόσταση στο μέσο μετάδοσης), της σκίασης (λόγω της παρεμβολής αντικειμένων) και της πολυβηματικής εξασθένησης (κάθε σήμα ανακλάται σε διαφορετικά αντικείμενα και λαμβάνεται από το δέκτη από διαφορετικά μονοπάτια). Ένας χρήστης που στέκεται στο όριο της κυψέλης, μακριά από το σταθμό βάσης και αποκλεισμένος από πολλά κτήρια θα λάβει μικρότερο ρυθμό από έναν άλλο που στέκεται ακριβώς κάτω από το σταθμό βάσης. Αυτοί οι παράγοντες επηρεάζουν ακόμα και αν υπάρχει μόνο ένας χρήστης σε ολόκληρο τον κόσμο.
2. *Παρεμβολή:* Υπάρχουν επίσης πολλοί χρήστες, οι οποίοι και αλληλεπιδρούν μεταξύ τους. Όπως αναφέρεται στο Κεφάλαιο 1, αν υπάρχουν λίγες αλλά ισχυρές παρεμβολές ή αν οι παρεμβολές είναι αδύναμες αλλά υπάρχουν πολλές στον αριθμό, τότε το λαμβανόμενο SIR θα είναι χαμηλό. Σε κάποιο σημείο, θα είναι τόσο χαμηλό ώστε η τάξη της διαμόρφωσης να πρέπει να υποβαθμιστεί και ο ρυθμός μετάδοσης να μειωθεί, έτσι ώστε ο δέκτης να μπορεί να αποκωδικοποιήσει με ακρίβεια. Όπως είδαμε στο Κεφάλαιο 1, ένα τυπικό παράδειγμα του προβλήματος είναι το αποκαλούμενο

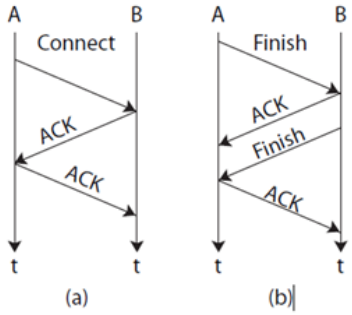
πρόβλημα του εγγύς-μακράν. Ακόμα και ο έλεγχος της ισχύος δεν μπορεί να επιλύσει εξ' ολοκλήρου αυτό το πρόβλημα.

19.1.2 Ενσύρματο Δίκτυο

Μπορεί να υπάρχουν περισσότερες από δέκα συνδέσεις οι οποίες διασχίζονται από το σταθμό βάσης προς τον πραγματικό προορισμό στην άλλη πλευρά μίας ασύρματης συνεδρίας, ας πούμε μίας λήψης ροής YouTube. Η συνεδρία πρώτα διασχίζει το δίκτυο ασύρματης πρόσβασης, έπειτα το δίκτυο κορμού της κινητής τηλεφωνίας, το οποίο επίσης ανήκει στον πάροχο κινητών επικοινωνιών, στη συνέχεια πιθανόν διασχίζει το δίκτυο ενός παρόχου απομακρυσμένων συνδέσεων, έπειτα ενδεχομένως συνεχίζει μέσω πολλών άλλων ISP που συνθέτουν το υπόλοιπο του Διαδικτύου και, τέλος, το δίκτυο του κέντρου δεδομένων της Google.

1. *Ζεύξεις*: Η κίνηση που δημιουργεί ο κάθε χρήστης ανταγωνίζεται με την αντίστοιχη των άλλων χρηστών στις συνδέσεις πίσω από την εναέρια διεπαφή του δικτύου κινητής τηλεφωνίας. Όπως εξηγείται με περισσότερες λεπτομέρειες στην επόμενη ενότητα, πολλά από τα ασύρματα δίκτυα έχουν το μεγαλύτερο μέρος των ζεύξεών τους υλοποιημένο με ενσύρματα δίκτυα. Συμβαίνει κυκλοφοριακή συμφόρηση σε αυτές τις συνδέσεις και η προκύπτουσα ουρά αναμονής μειώνει τη διαπερατότητα. Επιπρόσθετα, υπάρχει καθυστέρηση διάδοσης που οφείλεται στις αποστάσεις που διανύονται. Μία αύξηση στην καθυστέρηση μειώνει τη διαπερατότητα, δεδομένου ότι η διαπερατότητα ορίζεται ως ο αριθμός των bit που μπορούν να μεταδοθούν από την πηγή προς τον προορισμό ανά δευτερόλεπτο.
2. *Κόμβοι*: Αυτές οι ζεύξεις ενώνονται μέσω κόμβων διαφόρων ειδών: πυλών, μεταγωγών, δρομολογητών, εξυπηρετητών κτλ. Ορισμένοι από αυτούς, όπως οι δρομολογητές, αποθηκεύουν τα πακέτα ενώ περιμένουν τις εξερχόμενες συνδέσεις να ετοιμαστούν, αυξάνοντας έτσι το χρόνο καθυστέρησης των πακέτων. Άλλοι κόμβοι, όπως οι εξυπηρετητές, έχουν περιορισμούς επεξεργαστικής ισχύος και μπορεί να προκαλέσουν πολύ μεγάλη συμφόρηση όταν ευρίσκονται σε πολύ μεγάλη ζήτηση. Για παράδειγμα, ένας δημοφιλής εξυπηρετητής ιστού ή ένας εξυπηρετητής βίντεο μπορεί να γίνουν τόσο κορεσμένοι ώστε να μην μπορούν να επεξεργαστούν όλες τις αιτήσεις. Αυτό δεν έχει να κάνει τίποτε με το υπόλοιπο δίκτυο παρά μόνο με τον εξυπηρετητή που δεν μπορεί να διαχειριστεί τη ζήτηση. Παρόλα αυτά μειώνεται η απόδοση της συνεδρίας.

Με σχόλια [C1]: Μηπως είναι ¨λ¨ογω αυτών;»



Σχήμα 19.1 *(*a*) Εγκαθίδρυση συνεδρίας μέσω τριών βημάτων και (*b*) κατάργηση επικοινωνίας μέσω τεσσάρων βημάτων στο TCP. (*a*) Όταν ο Α αρχικοποιεί μία επικοινωνία με τον Β, ο Β στέλνει μία επιβεβαίωση (acknowledgement), και ο Α επιβεβαιώνει την επιβεβαίωση ώστε να ξέρει ο Β ότι ο Α γνωρίζει ότι η επικοινωνία έχει εγκαθιδρυθεί. (*b*) Όταν ο Α ξεκινά την παύση της επικοινωνίας, ο Β πρώτα το επιβεβαιώνει. Αμέσως μετά τα ο Β στέλνει μήνυμα κατάργησης της σύνδεσης, καθώς οι συνδέσεις του TCP είναι αμφίδρομες: ότι ο Α δεν έχει άλλα μηνύματα για τον Β δεν σημαίνει ότι ο Β δεν έχει άλλα μηνύματα για τον Α.*

19.1.3 Πρωτόκολλα

1. *Σημασιολογία πρωτόκολλου:* Πολλές λειτουργίες απαιτούν αλληλουχίες μεταγωγής μηνυμάτων. Για παράδειγμα, στο TCP κάθε συνεδρία χρειάζεται να εγκατασταθεί και να απεγκατασταθεί μέσω τριμερούς χειραψίας και αντίστοιχα τεσσάρων μηνυμάτων τερματισμού. Αυτή η διαδικασία απεικονίζεται στο Σχήμα 19.1. Γιατί όμως ο σχεδιαστής του πρωτοκόλλου του δικτύου έκανε τον κόπο να δημιουργήσει μία τόσο περίπλοκη διαδικασία προκειμένου απλά να εγκαθιδρύσει μία συνεδρία και έπειτα να την τερματίσει; Λοιπόν, γιατί με αυτό τον τρόπο, για την εγκαθίδρυση της επικοινωνίας, τόσο ο πομπός όσο και ο δέκτης γνωρίζουν ότι υπάρχει και ότι ο άλλος το γνωρίζει επίσης. Όσον αφορά τη διαδικασία απεγκαθίδρυσης με τέσσερα μηνύματα που στέλνει ο ένας στον άλλο, διασφαλίζεται ότι δεν υπάρχει ημιτελής επικοινωνία σε καμία από τις δύο κατευθύνσεις σε μία πλήρως αμφίδρομη επικοινωνία (για παράδειγμα σε ένα αμφίδρομο μονοπάτι όπου και οι δύο μπορούν να στέλνουν ταυτόχρονα). Προφανώς, για μικρότερες συνεδρίες, η επιβάρυνση καταλαμβάνει το μεγαλύτερο μέρος

του διαθέσιμου εύρους που έχουμε στη διάθεσή μας, αφήνοντας μικρότερο μέρος για τα ωφέλιμα δεδομένα της εφαρμογής.

2. *Επικεφαλίδα πακέτου:* Όπως εξηγείται στο Κεφάλαιο 13, κάθε επίπεδο προσθέτει μία επικεφαλίδα προκειμένου να μεταφέρει πληροφορίες ελέγχου, όπως τη διεύθυνση, τον αριθμό έκδοσης του πρωτοκόλλου, την ποιότητα της υπηρεσίας, τον έλεγχο σφαλμάτων, κτλ. Αυτές οι επικεφαλίδες επίσης αφήνουν κάποιο χώρο για να είναι ευέλικτο σε μελλοντική χρήση. Αυτές οι επικεφαλίδες επιβαρύνουν το δίκτυο, ιδιαίτερα αν το ωφέλιμο φορτίο του πακέτου είναι μικρό και το ποσοστό του φορτίου των επικεφαλίδων γίνεται μεγαλύτερο. Κάποια πρωτόκολλα επίσης καθορίζουν επίσης ένα όριο κατακερματισμού πακέτων, με αποτέλεσμα μεγαλύτερα πακέτα να διαιρούνται σε μικρότερα αυξάνοντας το μέγεθος των επικεφαλίδων ακόμη περισσότερο.

3. *Επίπεδο ελέγχου σηματοδοσίας:* Σκεφτείτε ένα δίκτυο αεροπορικών μεταφορών. Η πραγματική κίνηση των ανθρώπων και των αποσκευών υλοποιείται από τα αεροπλάνα που μετακινούνται από αεροδρόμιο σε αεροδρόμιο ακολουθώντας συγκεκριμένες διαδρομές. Αλλά η απόφαση δρομολόγησης και πολλά άλλα σήματα ελέγχου διασχίζουν εντελώς διαφορετικά δίκτυα, ενδεχομένως το Διαδίκτυο ή το τηλεφωνικό δίκτυο. Το επίπεδο δεδομένων χωρίζεται από το επίπεδο ελέγχου. Στο Διαδίκτυο, η πραγματική κίνηση των ροών δεδομένων γίνεται μέσω των καναλιών δεδομένων (τα οποία αποτελούν λογικές οντότητες παρά φυσικές), ενώ τα σήματα ελέγχου μεταδίδονται μέσω των καναλιών ελέγχου. Αυτά τα κανάλια σηματοδοσίας αντλούν τους διαθέσιμους πόρους από τη μετάδοση δεδομένων και τις δεσμεύουν για τα σήματα ελέγχου. Ενώ οι περισσότεροι αντιλαμβάνονται τη σημαντικότητα των καναλιών μετάδοσης δεδομένων, εξίσου σημαντικά είναι και τα κανάλια ελέγχου. Στα πρότυπα του 3G και του 4G, έχουν γίνει πολύ μεγάλες προσπάθειες να σχεδιαστούν τα κανάλια ελέγχου κατάλληλα. Μερικές φορές όμως διαστασιοποιούνται μικρά με αποτέλεσμα να προκαλείται επιπλέον καθυστέρηση και περαιτέρω μείωση της επίδοσης. Άλλες φορές διαστασιοποιούνται πολύ μεγάλα, καταναλώνοντας, χωρίς να απαιτείται, μεγάλα ποσά από τη συνολική χωρητικότητα μειώνοντας έτσι την διαπερατότητα.

Σε γενικές γραμμές, υπάρχουν πέντε κύριες λειτουργίες διαχείρισης δικτύου:

- Επίδοση: παρακολουθεί, συλλέγει και αναλύει μετρικές απόδοσης.
- Παραμετροποίηση: ανανεώνει το σχεδιασμό των παραμέτρων των επιλογέων ελέγχου σε διαφορετικά πρωτόκολλα.

- Χρέωση: διατηρεί τα δεδομένα που απαιτούνται για τον προσδιορισμό της χρέωσης κάθε χρήστη, π.χ. όταν ο χρήστης χρησιμοποιεί το δίκτυο με χρονοχρέωση.
- Διαχείριση βλάβης: παρακολουθεί συνεχώς προκειμένου να δει αν κάποια σύνδεση είτε κάποιος κόμβος καταρρεύσει και στη συνέχεια περιορίζει, επισκευάζει και κάνει τη διάγνωση των αρχικών αιτιών που την προκάλεσαν.
- Ασφάλεια: πιστοποιεί, διατηρεί την ακεραιότητα και ελέγχει την εμπιστευτικότητα.

Τα μηνύματα γι αυτές τις λειτουργίες κάποιες φορές χρησιμοποιούν κοινά κανάλια με αυτά των δεδομένων (εσωτερικός έλεγχος), και άλλες φορές αφιερωμένα κανάλια ελέγχου (εξωτερικός έλεγχος). Συλλογικά, αποτελούν το επίπεδο ελέγχου. Παράδειγμα πρωτοκόλλου που εκτελεί τις λειτουργίες της διαχείρισης δικτύου είναι το Πρωτόκολλο Απλής Διαχείρισης Δικτύου (SNMP: Simple Network Management Protocol) για το Διαδίκτυο.

19.2 Μία Εκτενής Απάντηση

Η ταχύτητα της ασύρματης (ή της ενσύρματης) σύνδεσής σας στο Διαδίκτυο δεν είναι ένας αριθμός, αλλά πολλοί αριθμοί που εξαρτώνται από τις απαντήσεις στις παρακάτω τέσσερις ερωτήσεις.

Πρώτα, σε ποιο επίπεδο μετριέται η ταχύτητα; Αυτή είναι συχνά η πρωταρχική αιτία σύγχυσης σχετικά με τα αποτελέσματα των δοκιμών ταχύτητας. Για παράδειγμα, οι οργανισμοί ασύρματης τυποποίησης αναφέρονται συχνά στην ταχύτητα στο φυσικό επίπεδο, ενώ οι χρήστες βιώνουν άμεσα την ταχύτητα στο επίπεδο εφαρμογής. Ανάλογα με το επίπεδο που μιλάμε, αλλάζει το μέρος του ενσύρματου δικτύου και του πρωτοκόλλου που εμπλέκεται. Όσο περισσότερες συνδέσεις τρέχουν στο ενσύρματο δίκτυο, τόσο μεγαλώνουν και οι πιθανότητες να συμβεί συμφόρηση. Όσο πιο πολλά πρωτόκολλα εμπλέκονται τόσο αυξάνεται η επιβάρυνση.

Στο Κεφάλαιο 17, είδαμε κάποια από τα βασικά πρωτόκολλα τα οποία χρησιμοποιούνται σε κάθε επίπεδο. Σε ένα άλλο παράδειγμα, στο LTE, το επίπεδο ζεύξης (που είναι το δεύτερο επίπεδο) αποτελείται από τρία επίπεδα, το καθένα με τη δική του επικεφαλίδα:

- επίπεδο MAC: Έλεγχος πρόσβασης στο μέσο. Διαχειρίζεται την πολύπλεξη των δεδομένων διαφορετικών λογικών καναλιών και αποφασίζει τον τρόπο με τον οποίο θα χρονο-προγραμματιστούν τα πακέτα.
- επίπεδο RLC: Έλεγχος ραδιοζεύξης. Ελέγχει τον κατακερματισμό και την επανασυναρμολόγηση των πακέτων για να επιτύχει το μέγεθος των πακέ-

των που μπορεί εύκολα να μεταδοθεί μέσω της ραδιοζεύξης. Επίσης ελέγχει την επανεκπομπή των χαμένων πακέτων.

- επίπεδο PDCP: Πρωτόκολλο σύγκλισης πακέτων δεδομένων. Επεξεργάζεται τις διαδικασίες συμπίεσης της επικεφαλίδας, την ασφάλεια και τη διαπομπή.

Δεύτερον, σε ποιο σημείο μετριέται η ταχύτητα; Υπάρχει εξάρτηση από την τοποθεσία των δύο τερματικών στην οποία μετριέται η ταχύτητα, τα διαφορετικά κομμάτια του δικτύου οπισθοζεύξης (backhaul) και τα διαφορετικά πρωτόκολλα τα οποία περιλαμβάνει. Αυτό που καθορίζει την τιμή της δοκιμής ταχύτητας είναι πάντα η πιο αδύναμη σύνδεση. Για παράδειγμα, στην κινητή τηλεφωνία, η ταχύτητα συχνά μετριέται ανάμεσα σε μία κινητή συσκευή και στο σταθμό βάσης του κεντρικού δικτύου. Αλλά όπως βλέπουμε στο Σχήμα 19.2, ο σταθμός βάσης επικοινωνεί με διάφορες πύλες πριν φτάσει στον κορμό του Διαδικτύου και τελικά να κατευθυνθεί προς το άλλο τερματικό, π.χ. σε μία άλλη κινητή συσκευή ή σε ένα εξυπηρετητή. Η ταχύτητα που μετριέται είναι διαφορετική σε κάθε ένα από τους προορισμούς κατά μήκος αυτής της διαδρομής. Αν η δοκιμή ταχύτητας είναι μεταξύ του κινητού τηλεφώνου και του σταθμού βάσης αυτά που περιλαμβάνονται είναι το πρωτόκολλο φυσικού επιπέδου ασύρματης ζεύξης και το επίπεδο ζεύξης. Αν πάλι η ταχύτητα που κάνουμε τη δοκιμή είναι ανάμεσα στο κινητό και τον εξυπηρετητή μέσων, τότε αυτά που σχετίζονται είναι το κεντρικό backhaul, το δίκτυο κορμού IP και, ακόμη και η συμφόρηση στην οποία θα βρίσκεται ο εξυπηρετητής μέσων. Έτσι σε αυτή την περίπτωση θα έχουμε τα πρωτόκολλα του επίπεδου δικτύου, του επίπεδου μεταφοράς και του επίπεδου εφαρμογής.

Τρίτον, σε ποια χρονική στιγμή μετριέται η ταχύτητα; Σε διαφορετικές χρονικές στιγμές της ημέρας, παρατηρούνται διαφορετικά επίπεδα συμφόρησης τόσο στο μέσο επικοινωνίας όσο και στο backhaul. Το επίπεδο της κίνησης σε διαφορετικές ώρες της ημέρας αποτελεί ένα συχνά επαναλαμβανόμενο μοτίβο ιδιαίτερα σε ό,τι αφορά τα υψηλά επίπεδα συνάθροισης. Μεγαλύτερη δραστηριότητα του χρήστη μεταφράζεται στην εκπομπή περισσοτέρων bit, τα οποία προκαλούνται από:

- Παρεμβολές (μία πολλαπλασιαστική συμπεριφορά) όπως είδαμε στο Κεφάλαιο 1: $x/y \geq s$ όπου το s είναι κάποια τιμή στόχος για το SIR.
- Συμφόρηση (μία προσθετική συμπεριφορά) όπως στο Κεφάλαιο 14: $x + y \leq c$ όπου το c είναι κάποιο όριο χωρητικότητας.
- Σύγκρουση (μία δυαδική συμπεριφορά) όπως στο Κεφάλαιο 18: $x, y \in \{0,1\}$ αν οι συνεδρίες x, και y δεν μπορούν να μεταδώσουν την ίδια χρονική στιγμή χωρίς να έχουμε σύγκρουση.

Τέταρτον, σε ποια εφαρμογή μετριέται η ταχύτητα; Αυτό έχει σημασία για δύο λόγους. (1) Διαφορετικές μορφές κίνησης χρησιμοποιούν διαφορετικά είδη πρω-

τοκόλλων, κάποια τα οποία έχουν μεγαλύτερη επιβάρυνση σε σχέση με άλλα. Για παράδειγμα, τα γραπτά μηνύματα καταλαμβάνουν μικρό ποσοστό της κίνησης του καναλιού δεδομένων αλλά απαιτούν περισσότερη πληροφορία ελέγχου. Η λήψη ενός ηλεκτρονικού μηνύματος και η κίνηση ιστού είναι λιγότερο απαιτητικές ως προς την επιβάρυνση σε σύγκριση με υπηρεσίες VoIP και τηλεδιάσκεψης. (2) Οι προσδοκίες του χρήστη και η συνάρτηση χρησιμότητάς του διαφέρουν πολύ για διαφορετικές εφαρμογές. Τα διαδραστικά παιχνίδια έχουν πολύ αυστηρές απαιτήσεις τόσο σε καθυστερήσεις όσο και στις μεταβολές τους, ενώ η λήψη αρχείων δεν έχει. Άλλες εφαρμογές μπορούν να ανεχθούν μεγαλύτερη καθυστέρηση επικοινωνίας αν η διαπερατότητα από τη στιγμή της εκκίνησης είναι σταθερά υψηλή. Άλλες εφαρμογές είναι πιο ευαίσθητες σε μεταβολές του χρόνου, αλλά μπορούν να αποδώσουν σε μεταβολές διαπερατότητας με άνεση. Κάθε αντικειμενική μέτρηση της ταχύτητας πρέπει να μεταφραστεί στην υποκειμενική εμπειρία του χρήστη.

19.3 Παραδείγματα

Θα παρουσιάσουμε παρακάτω λίγα αριθμητικά παραδείγματα μη ιδανικών συνθηκών δικτύου, πριν μεταφερθούμε σε μία περαιτέρω συζήτηση για τις επιβαρύνσεις των πρωτοκόλλων στο Προχωρημένο Υλικό.

19.3.1 Παράδειγμα εναέριας μετάδοσης

Παρακάτω ακολουθεί ένα παράδειγμα LTE 4G. Η διαπερατότητα στο φυσικό επίπεδο και αποκλειστικά για μετάδοση μέσω αέρα, μπορεί να υπολογιστεί όπως θα περιγραφεί παρακάτω.

Για κάθε υπο-πλαίσιο δεδομένων (μία μονάδα χρόνου η οποία διαρκεί 1 ms), μετράμε πόσα bit στάλθηκαν. Το φυσικό επίπεδο του LTE βασίζεται στη διαμόρφωση OFDM, διαιρώντας το φάσμα σε μπλοκ και χρησιμοποιώντας επεξεργασία σήματος σε κάθε ένα από αυτά. Ο αριθμός των bit που εκπέμπονται είναι ίσος με τον (α) αριθμό των συμβόλων σε κάθε μπλοκ συχνοτήτων πολλαπλασιασμένο επί (β) τον αριθμό των μπλοκ, μετά πολλαπλασιασμένο με (γ) τον αριθμό των bit σε κάθε σύμβολο και μετά πολλαπλασιασμένο (δ) με την ενίσχυση της κωδικοποίησης και το κέρδος των πολλαπλών κεραιών.

Για το (α) παραπάνω, ο αριθμός των συμβόλων είναι (α_1) το γινόμενο του αριθμού των συμβόλων ανά φέρουσα επί (α_2) τον αριθμό των φερουσών ανά μπλοκ συχνοτήτων με (α_3) αφαιρεμένη την επιβάρυνση.

Γι αυτό, έχουμε τον παρακάτω τύπο που υπολογίζει τα bit που στέλνονται σε κάθε υπο-πλαίσιο:

$$\begin{aligned}\Sigma\acute{\upsilon}\mu\beta o\lambda\alpha/\phi\acute{\varepsilon}\rho ou\sigma\alpha - \varepsilon\pi\iota\beta\acute{\alpha}\rho\upsilon\nu\sigma\eta\ \varepsilon\lambda\acute{\varepsilon}\gamma\chi ou \\ \times\ \alpha\rho\iota\theta\mu\acute{o}\ \phi\varepsilon\rho ou\sigma\acute{\omega}\nu\ \alpha\nu\acute{\alpha}\ \mu\pi\lambda o\kappa\ \sigma\upsilon\chi\nu o\tau\acute{\eta}\tau\omega\nu \\ -\ \acute{\alpha}\nu\omega\ \varepsilon\kappa\tau\acute{\iota}\mu\eta\sigma\eta\ \tau\varepsilon\pi\iota\beta\acute{\alpha}\rho\upsilon\nu\sigma\eta\varsigma\ \tau ou\ \kappa\alpha\nu\alpha\lambda\iota o\acute{\upsilon}\ \times \frac{bit}{\sigma\acute{\upsilon}\mu\beta o\lambda o} \\ \times\ \pi\lambda\acute{\eta}\theta o\varsigma\ \tau\omega\nu\ \mu\pi\lambda o\kappa\ \sigma\upsilon\chi\nu o\tau\acute{\eta}\tau\omega\nu \\ \times\ \kappa\acute{\varepsilon}\rho\delta o\varsigma\ \kappa\omega\delta\iota\kappa o\pi o\acute{\iota}\eta\sigma\eta\varsigma\kappa\alpha\iota\ \pi o\lambda\lambda\alpha\pi\lambda\acute{\omega}\nu\ \kappa\varepsilon\rho\alpha\iota\acute{\omega}\nu.\end{aligned}$$

Ποιες είναι οι αριθμητικές τιμές των παραπάνω παραγόντων;

- Σύμβολα ανά φέρουσα: Συνήθως είναι 12-14 στο LTE.
- Επιβάρυνση/ φέρουσα: τουλάχιστον 1 αλλά κάποιες φορές 2 ή 3 σύμβολα ανά φέρουσα σε ένα υπο-πλαίσιο για τον έλεγχο της σηματοδοσίας.
- Φέρουσες/μπλοκ συχνοτήτων: συνήθως 12 φέρουσες ανά μπλοκ συχνότητας πλάτους 180kHz.
- Εκτίμηση της επιβάρυνσης του καναλιού ανά μπλοκ συχνοτήτων: το μέγεθος των επικεφαλίδων που χρησιμοποιούνται για την αποστολή πιλοτικών συμβόλων για την εκτίμηση του καναλιού είναι συνήθως 20 σύμβολα για συστήματα πολλαπλών κεραιών τύπου 4 x 4.
- Bit/ Σύμβολο: αυτό εξαρτάται από τη διαμόρφωση, το λαμβανόμενο λόγο Σήματος προς Παρεμβολή (SIR) και τη δυνατότητα του αποκωδικοποιητή. Ιδανικά μπορεί να είναι 6 για το LTE, χρησιμοποιώντας διαμόρφωση $2^6 = 64$ QAM. Συνήθως είναι 4, χρησιμοποιώντας το μικρότερης δύναμης $2^4 = 16$ QAM διαμόρφωση όταν η κατάσταση του καναλιού δεν είναι αρκετά καλή (π.χ όταν υπάρχει σκίαση, εξασθένηση, ή η απόσταση από το σταθμό εκπομπής είναι μεγάλη). Εάν το κανάλι είναι σε ακόμη χειρότερη κατάσταση, τότε ο αριθμός αυτός μπορεί να γίνει 2.
- Αριθμός των μπλοκ συχνοτήτων: Ας υποθέσουμε ότι μπορούμε να χρησιμοποιήσουμε όλη την ζώνη των 20 MHz ενός καναλιού LTE, με 1MHz σε κάθε πλευρά για λόγους προστασίας. Επειδή κάθε μπλοκ συχνοτήτων στην OFDM έχει πλάτος 180 kHz έχουμε 100 μπλοκ. Στην πραγματικότητα, η αμφίδρομη επικοινωνία πραγματοποιείται είτε με διπλή διαίρεση συχνότητας (FDD- Frequency Division Duplex) οπότε έχουμε 10MHz δηλαδή 50 μπλοκ ή με διπλή διαίρεση χρόνου (TDD- Time Devision Duplex) οπότε έχουμε διαθέσιμο το 40% του χρόνου για την ανοδική ζεύξη και το 60% του χρόνου για την καθοδική ζεύξη.
- Ρυθμός κωδικοποίησης: Ο ρυθμός κωδικοποίησης του καναλιού είναι η επιβάρυνση λόγω της κωδικοποίησης του καναλιού που προσθέτει πλεονασμό για να προστατέψει τα εκπεμπόμενα bit από το θόρυβο του καναλιού. Όσο υψηλότερος είναι ο ρυθμός κωδικοποίησης τόσο λιγότερος πλε-

ονασμός προστίθεται. Ιδανικά, θέλουμε να είναι κοντά στο 1 αλλά μπορεί να είναι χαμηλότερο για συγκεκριμένες κωδικοποιήσεις. Όσο υψηλότερη προστασία χρειάζεται και όσο λιγότερο αποδοτική είναι η κωδικοποίηση, τόσο χαμηλώνει η τιμή αυτής της μεταβλητής.

- Κέρδος πολλαπλών κεραιών: ιδανικά σε ένα σύστημα κεραιών 4 x 4 η μεταβλητή αυτή θα πρέπει να είναι 4. Αλλά λόγω του περιορισμού του αριθμού των συσκευών (κάποιες φορές είναι δυνατό να εγκατασταθούν μόνο 2 κεραίες) και λόγω της παρεμβολής των καναλιών στον χώρο (όπου οι κεραίες είναι πολύ κοντά η μία στην άλλη, τα σήματα που λαμβάνονται δεν χρησιμοποιούν πολύ διαφορετικά κανάλια) πολύ συχνά αυτή η μεταβλητή έχει την τιμή 2.

Άρα, ο αριθμός των bit που εκπέμπονται σε 1 ms στην καλύτερη περίπτωση θα είναι:

$$[(14-1)\times 12-10]\times 6\times 100\times 0{,}9\times 4=315.360\ bit,$$

το οποίο μεταφράζεται σε 315.360/0,001= 315 Mbps. Θα ήταν πράγματι εντυπωσιακό αν θα μπορούσαμε να έχουμε αυτή τη χρήσιμη διαπερατότητα όλη την ώρα.

Στην πραγματικότητα το πιο πιθανό σενάριο είναι:

$$[(12-2)\times 12-20]\times 4\times 50\times 0{,}7\times 2=28.000\ bit,$$

το οποίο μεταφράζεται σε 28.000/0,001= 28 Mbps, δηλαδή περίπου το 8,8% της αρχικής εκτίμησης.

Εάν μετρηθούν η επανεκπομπή και η επιβάρυνση του επιπέδου MAC: το PDCP έχει επικεφαλίδα 3,5 byte συν τον αριθμό ακολουθίας, το RLC έχει επικεφαλίδα 5,5 byte συν τον αριθμό ακολουθίας, το MAC έχει επικεφαλίδα 1 byte και CRC 3 byte, και υπάρχει τουλάχιστον άλλος ένα λόγος απώλειας της χρήσιμης διαπερατότητας 0,9, ρίχνοντας τον ρυθμό στα περίπου 25Mbps.

Τα παραπάνω περιλαμβάνουν μόνο την υποβάθμιση του φυσικού επιπέδου και την επιβάρυνση του επιπέδου MAC. Είναι ήδη μικρότερο του 8% της ιδανικής περίπτωσης. Αν σε όλα αυτά προσμετρήσουμε την αλληλεπίδραση μεταξύ των χρηστών και των ανώτερων επιπέδων και τη συμφόρηση του δικτύου backhaul η διαπερατότητα του δικτύου μπορεί να πέσει κατά ένα παράγοντα 2-5.

Τώρα, τα 5-10 Mbps σε μία κινητή συσκευή είναι μία αρκετά εντυπωσιακή ταχύτητα και μπορεί να καταστήσει δυνατές πολλές ενεργές εφαρμογές, συμπεριλαμβανομένων των μέσης ποιότητας ροών βίντεο. Η εμπειρία των χρηστών δεν είναι κακή, ειδικά όταν η διαπερατότητα του WiFi στις οικίες των περισσότερων ανθρώπων είναι σήμερα μόνον περίπου 5-20Mbps, καθώς περιορίζεται από την ταχύτητα του 802.11b ή από την ταχύτητα της πύλης του δικτύου backhaul). Αλλά δεν

θα πρέπει να εκπλαγείτε αν δεν «αισθανθείτε» την ταχύτητα των 300Mbps στο έξυπνο κινητό σας τεχνολογίας LTE.

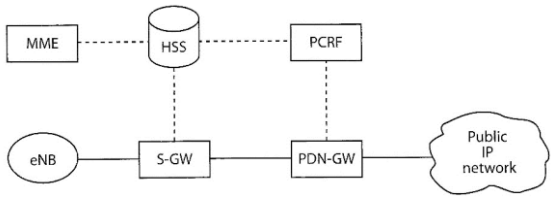
19.3.2 Παραδείγματα οπισθοζεύξης

Το δίκτυο backhaul της κινητής τηλεφωνίας αποτελείται από κάποιες ζεύξεις (π.χ μικροκυμματικές συνδέσεις, οπτικές ζεύξεις ελεύθερου χώρου, δορυφορικές ζεύξεις) που συνδέουν την ασύρματη ζεύξη με το υπόλοιπο από άκρο σε άκρο σύστημα όπως φαίνεται στο Σχήμα 19.2, έπειτα με το κύριο δίκτυο κινητής τηλεφωνίας και μετέπειτα με το δημόσιο δίκτυο IP. Έτσι πολλοί παράγοντες μπορεί να μειώσουν τη χρήσιμη διαπερατότητα. Θα δούμε μόνον τρία παραδείγματα σχετικά με το TCP.

(1) Όπως είδαμε στο Κεφάλαιο 14, η διαπερατότητα του TCP μπορεί να υπολογιστεί ως εξής:

$$Διαπερατότητα\ TCP = Μέγεθος\ παραθύρου\ TCP/RTT,$$

όπου το RTT είναι ο χρόνος μετ' επιστροφής (Round Trip Time). Το μέγιστο μέγεθος παραθύρου είναι $2^{16} - 1 = 65535$ byte λόγω του ό,τι το παράθυρο του δέκτη στην επικεφαλίδα του TCP είναι 16 bit. Ο λόγος ύπαρξης του παραθύρου του δέκτη είναι για να αποτρέψει το πρόβλημα επικοινωνίας μεταξύ ενός γρήγορου πομπού και ενός αργού δέκτη.



Σχήμα 19.2. *Τα κύρια μέρη του πυρήνα του εξελικτικού πακέτου στο LTE: η εναέρια μετάδοση (μεταξύ της συσκευής του τελικού χρήστη και του BS ονομάζεται eNB στο LTE), το δημόσιο δίκτυο IP και το υπόλοιπο ενσύρματο δίκτυο που είναι το κύριο δίκτυο της κινητής τηλεφωνίας. Οι συμπαγείς γραμμές αντιπροσωπεύουν τις φυσικές συνδέσεις με τη ζεύζη μεταξύ του τηλεφώνου και του BS να είναι η μόνη ασύρματη ζεύξη. Οι διακεκομμένες γραμμές αντιπροσωπεύουν τους διαύλους του επίπεδου ελέγχου. Ο BS διέρχεται μέσα από πύλες διαφόρων επιπέδων στο δίκτυο της κινητής τηλεφωνίας πριν φτάσει στο δημόσιο δίκτυο IP.*

Υποθέστε ότι είστε συνδεδεμένοι με μία σύνδεση 1Gbps και ότι εκπέμπετε ένα αρχείο σε έναν προορισμό με καθυστέρηση 100 ms. Σε αυτή την περίπτωση η μέγιστη διαπερατότητα TCP που μπορεί να επιτευχθεί είναι:

$$65535 \times 8/0.1 \approx 5{,}24 \text{ Mbps}.$$

Παρόλο που είμαστε συνδεδεμένοι με μία ζεύξη Ethernet του 1Gbps, δεν θα πρέπει να περιμένουμε παραπάνω από 5,24 Mbps ενώ μεταφέρουμε το αρχείο, δεδομένου του μεγέθους του παραθύρου του TCP και του RTT.

(2) Στην πράξη το TCP μπορεί να μην φτάσει στο μέγιστο μέγεθος παραθύρου λόγω του μηχανισμού ελέγχου της συμφόρησης που αποτρέπει τον αποστολέα από το να υπερφορτώσει το δίκτυο. Το παράθυρο TCP είναι το min{παράθυρο συμφόρησης, παράθυρο δέκτη}.

Το παράθυρο συμφόρησης μειώνεται όταν ανιχνευτεί συμφόρηση μέσα στο δίκτυο, π.χ. μία απώλεια πακέτου. Η διαπερατότητα του TCP για ζεύξεις μακρινών αποστάσεων μπορεί να υπολογιστεί όπως παρακάτω, όπως είχαμε δει και σε μία άσκηση στο Κεφάλαιο 14:

$$\text{διαπερατότητα TCP} \leq \text{MSS}/\left(\text{RTT} * \sqrt{\text{p}}\right),$$

όπου το MSS είναι το μέγιστο μέγεθος του τμήματος (σταθερό για το πρωτόκολλο TCP/IP, συνήθως 1460 byte), και p ο ρυθμός απώλειας των πακέτων. Ας υποθέσουμε ότι έχουμε ένα υψηλό ρυθμό απώλειας πακέτων 0,1%, το οποίο μας δίνει το παρακάτω άνω όριο για τη διαπερατότητα:

$$1460 * 8/(0.1 * \sqrt{0.001} \approx 3{,}63\text{Mbps}.$$

(3) Τελευταία, ας δούμε το πρόβλημα των εκρήξεων δεδομένων (flash crowds), π.χ. τη μεγάλη επισκεψιμότητα σε έναν δημοφιλή εξυπηρετητή ιστού την ίδια χρονική στιγμή. Η εφαρμογή του εξυπηρετητή μπορεί να μην είναι σε θέση να δημιουργήσει δεδομένα αρκετά γρήγορα λόγω της συμφόρησης (στη CPU, στη μνήμη ή στο εύρος του δικτύου). Για παράδειγμα, ο πομπός μπορεί να γράψει λίγα δεδομένα, προκαλώντας την ενεργοποίηση του αλγόριθμου Nagle που καθυστερεί την αποστολή δεδομένων. Στην ουσία συνδυάζει τα μικρά πακέτα πληροφοριών σε μεγάλα για να πετύχει την καλύτερη αξιοποίηση του δικτύου, αλλά αυξάνεται η καθυστέρηση. Αυτή είναι μία απαραίτητη υποχώρηση για να μπορέσουμε να ελέγξουμε την επιβάρυνση και να τη μειώσουμε, αλλά με κόστος, την αύξηση της καθυστέρησης.

Αν υποθέσουμε ότι για τους παραπάνω λόγους, χρειάζονται 4 RTT για έναν εξυπηρετητή για να στείλει δεδομένα 1 MSS. Η ενεργή διαπερατότητα γίνεται πολύ μικρή:

$$1400 * 8/(0{,}1 * 4) \approx 29{,}2\ kbps.$$

Αυτό ίσως εξηγεί γιατί χρειάζεται αρκετή ώρα για να εμφανιστεί μία απλή ιστοσελίδα στο φυλλομετρητή. Αν η συμφόρηση στον εξυπηρετητή είναι όπως αναφέρουμε παραπάνω, δεν έχει σημασία αν το κινητό μας είναι συνδεδεμένο σε δίκτυο LTE 4G ή στο παλιό GSM 2G.

Αυτή είναι μία τυπική ανταλλαγή στη διαχείριση της επιβάρυνσης μέσω της συνάθροισης πλαισίων: ίσως καταφέρετε να μειώσετε το ποσόν της επιβάρυνσης αλλά σε βάρος της αύξησης της καθυστέρησης. Μία παρόμοια υποχώρηση γίνεται με τις συγκεντρωτικές επιβεβαιώσεις. Αν χαθεί μία συγκεντρωτική επιβεβαίωση τότε ο αποστολέας θα ξαναστείλει όλα τα πακέτα που δεν έλαβαν επιβεβαίωση, ένα φαινόμενο που μοιάζει με την απώλεια πλαισίων στη GOP στο Κεφάλαιο 17.

19.4 Προχωρημένο Υλικό

Θα ασχοληθούμε πιο αναλυτικά με τις επιβαρύνσεις του πρωτοκόλλου ελέγχου σε αυτή την ενότητα: με τρεις περιπτώσεις διαχείρισης του κεντρικού δικτύου κινητής τηλεφωνίας, με την υποστήριξη της κινητικότητας, και με την τοπική μεταγωγή. Σε μία άσκηση θα διερευνήσουμε την επιβάρυνση που σχετίζεται με την ασφάλεια των δικτύων.

19.4.1 Δίκτυο κορμού κινητής τηλεφωνίας

Ένα ασύρματο δίκτυο, κινητό ή WiFi, στην πραγματικότητα αποτελείται κυρίως από ενσύρματες ζεύξεις. Συνήθως, μόνο η σύνδεση της συσκευής του τελικού χρήστη με το σταθμό βάσης (ή το σημείο πρόσβασης του WiFi) είναι ασύρματη. Αν ο προορισμός είναι μία άλλη ασύρματη συσκευή τότε θα υπάρχει και άλλο ένα κομμάτι ασύρματης επικοινωνίας, αλλιώς όλη η υπόλοιπη επικοινωνία θα ήταν ενσύρματη. Πώς, λοιπόν, φτάνει η κίνηση από το σταθμό βάσης μέσω του υπόλοιπου Διαδικτύου στον προορισμό της;

Ένα πακέτο μεταφέρεται μέσω δύο σκελών από ενσύρματα δίκτυα.

- Πρώτο είναι το βασικό δίκτυο κορμού της κινητής τηλεφωνίας, το οποίο μεταφέρει την κίνηση από το σταθμό βάσης μέσω ενός συνόλου εξυπηρετητών και ζεύξεων, προσεκτικά σχεδιασμένου και διαχειριζόμενου από τον πάροχο κινητής τηλεφωνίας.
- Μετά υπάρχει το δημόσιο δίκτυο IP το οποίο διευθύνεται από έναν ή περισσότερους παρόχους.

Έχουμε ήδη δει κάποια χαρακτηριστικά των δημοσίων δικτύων IP στα Κεφάλαια 13 και 14, και τώρα αναλύουμε τα δίκτυα κορμού κινητής τηλεφωνίας. Θα συζητήσουμε μόνο για ένα πολύ μικρό κλάσμα αυτού του δικτύου το οποίο θα μας επιτρέψει να καταλάβουμε πότε θα αυξηθεί η επιβάρυνση και το οποίο θα οδηγήσει στη συζήτηση για τη διαχείριση των δικτύων και τη διαχείριση της κινητικότητας.

Και γιατί χρειαζόμαστε ένα δίκτυο κορμού για να υποστηρίξουμε τη μετάδοση μέσω αέρα ενός ασύρματου δικτύου; Αυτό γίνεται γιατί υπάρχουν περισσότερες διαδικασίες από την αποστολή και τη λήψη «μηνυμάτων» μέσω του αέρα. Για πα-

ράδειγμα, χρειάζονται μερικά συστήματα το οποία είναι υπεύθυνα για τη χρέωση, την υποστήριξη της κινητικότητας των χρηστών, την καταγραφή της κίνησης του δικτύου, την παροχή της ποιότητας Υπηρεσίας (QoS) και την εξασφάλιση της διαλειτουργικότητας μεταξύ διαφορετικών τύπων και γενιών δικτύων.

Κάθε γενιά προτύπων δικτύων κινητής τηλεφωνίας έχει διαφορετικό δίκτυο κορμού. Για το LTE 4G, αυτό αποκαλείται εξελίξιμο δίκτυο κορμού πακέτων (Evolvable Packet Core (EPC)). Το αρχικό σημείο του EPC είναι ο σταθμός βάσης (που λέγεται eNB (evolvable Node B)) και ο συσχετιζόμενος ελεγκτής (όπως το κινητό κέντρο μεταγωγής (Mobile Switching Center (MSC)) στο 3G και στο τωρινό πρότυπο της κίνησης φωνής στο LTE). Το τελικό σημείο είναι ένας δρομολογητής IP. Ενδιάμεσα παρεμβάλλονται μερικές άλλες συσκευές:

- Υλικό: Υπάρχουν πολλαπλές πύλες γεμάτες με εξυπηρετητές και μεταγωγείς. Οι δύο κύριες είναι οι πύλες εξυπηρέτησης (Serving Gateways S-GW) και η πύλη δικτύου πακέτων δεδομένων (P-GW).
- Λογισμικό: Υπάρχει ένα σύνολο προγραμμάτων που είναι υπεύθυνα για τους λογαριασμούς, τις χρεώσεις, την καταγραφή και τις ρυθμίσεις, την πολυμεσική επεξεργασία σήματος, την υποστήριξη της φορητότητας, την ασφάλεια και την ιδιωτικότητα, τη ρύθμιση του QoS, και την κατανομή των διευθύνσεων IP.
- Έλεγχος Καναλιών: Μερικές φορές ο έλεγχος σηματοδοσίας εκτελείται μαζί με τα πραγματικά δεδομένα, ενώ κάποιες φορές πάνω σε ειδικά κανάλια τα οποία ονομάζονται κανάλια ελέγχου.

Όπως φαίνεται στο Σχήμα 19.2, τα βασικά λογικά τμήματα του EPC περιλαμβάνουν τα παρακάτω:

- PCRF (Policy Control and charging Rule Function): Έλεγχος πολιτικής και λειτουργία κανόνων χρέωσης. Είναι υπεύθυνο για τη λήψη αποφάσεων σχετικά με τις πολιτικές ελέγχου, π.χ. πιστοποίηση για τη διαφοροποίηση της ποιότητας της εξυπηρέτησης.
- MME (Mobility Management Entity): Οντότητα Διαχείρισης Κινητικότητας. Ελέγχει τη σηματοδοσία μεταξύ των συσκευών των χρηστών κα των EPC.
- HSS (Home Subscriber Server): Οικείος Εξυπηρετητής Συνδρομητών. Αυτή είναι μία βάση δεδομένων για να υποστηρίζει την κινητικότητα που θα αναλυθεί αργότερα. Είναι παρόμοιο με τον Οικείο Καταχωρητή Θέσης (Home Location Register: HLR) των προηγούμενων γενιών κινητής τηλεφωνίας.

- S-GW (). Μετράει τον αριθμό των byte για λόγους χρέωσης. Χρησιμοποιείται ως άγκυρα τοπικής κινητικότητας, καθώς γίνεται ενταμίευση δεδομένων όταν ο MME μπαίνει σε λειτουργία διαπομπής. Επίσης, επικοινωνεί με διάφορα πρότυπα του 3G, όπως το UMTS και το GPRS, για ευκολότερη ενσωμάτωση. Λειτουργεί στο επίπεδο ζεύξης.
- P-GW (PDN Gateway). Κατανέμει τις διευθύνσεις IP, ελέγχει την ποιότητα εξυπηρέτησης και επιβάλλει άλλους κανόνες του PCRF. Επίσης, επικοινωνεί με άλλα πρότυπα του 3G ή του 4G όπως το CDMA2000 και το WiMAX.

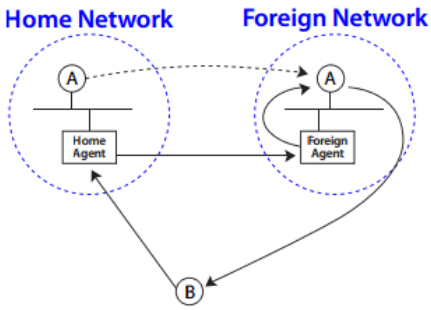
19.4.2 Διαχείριση κινητικότητας: κινητό IP και διαπομπή

Η διεύθυνση IP μίας συσκευής ή ένας αριθμός τηλεφώνου αποτελεί ένα τύπο μίας μοναδικής ταυτότητας (ID). Για τις κινητές συσκευές, όμως, το πρόβλημα είναι ότι το ID πρέπει να αποσυνδεθεί από μία σταθερή περιοχή. Όταν ένας φορητός υπολογιστής μετακινείται μέσα σε ένα κτήριο, μπορεί να επικοινωνούμε με διαφορετικό AP. Όταν μετακινούμαστε, ο σταθμός βάσης που μας εξυπηρετεί αλλάζει όποτε το κανάλι μεταξύ ενός νέου σταθμού βάσης και των χρηστών είναι καλύτερο απ' ό,τι μεταξύ των χρηστών και του ήδη υπάρχοντος. Όταν το αεροπλάνο προσγειώνεται και ξανανοίγουμε το iPhone, όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα φωνητικά μηνύματα πρέπει να βρουν τη νέα τοποθεσία μας.

Οι παραπάνω τρεις περιπτώσεις έχουν διαφορετικές ταχύτητες κινητικότητας και διαφορετικό ρυθμό αλλαγής χωρικής κάλυψης σε μία τοποθεσία, αλλά όλες χρειάζεται να φροντίσουν τη διαχείριση της κινητικότητας. Το κλειδί για όλες τις λύσεις είναι να υπάρχει μία "άγκυρα", ένα σημείο όπου όλοι οι υπόλοιποι να μπορούν να μας "φτάσουν" όπου και αν είμαστε, δηλαδή αυτό το σημείο να μας παρακολουθεί. Αυτό είναι παρόμοιο με το εξής σενάριο: μία συμμαθήτρια μας από το δημοτικό θέλει να μας βρει αφού έχουμε μετακομίσει σε μία άλλη πόλη για το Πανεπιστήμιο. Μπορεί να έρθει σε επαφή με το πατρικό μας σπίτι, δηλαδή τον "οικείο πράκτορα", θεωρώντας ότι οι γονείς μας θα ξέρουν πώς να έρθουν σε επαφή με τη φοιτητική εστία στην οποία μένουμε, που είναι ο "ξένος πράκτορας", και έτσι να μας βρει.

Θεωρήστε μία συσκευή Α με σταθερή διεύθυνση IP και ένα οικείο δίκτυο. Υπάρχει ο **οικείος πράκτορας** στο δίκτυο. Όταν η συσκευή μετακινείται σε ένα ξένο δίκτυο ως επισκέπτης, ο οικείος πράκτορας έρχεται σε επαφή με έναν άλλο πράκτορα που είναι υπεύθυνος στο να φροντίζει τους επισκέπτες. Ανακοινώνει σ' αυτόν τον ξένο πράκτορα την σταθερή του διεύθυνση IP καθώς και το ID του. Τότε ο ξένος **πράκτορας** θα ενημερώσει τον οικείο ότι η συσκευή Α αποτελεί μέρος του δικτύου του.

Τώρα όταν κάποιος, έστω ο Bob, θέλει να στείλει ένα μήνυμα στη συσκευή Α, το μήνυμα φτάνει στον οικείο πράκτορα. Ο Bob δεν ξέρει πού πραγματικά βρίσκεται η συσκευή, ξέρει όμως ότι ο οικείος πράκτορας το γνωρίζει. Ο οικείος πράκτορας ελέγχει έναν πίνακα που ταιριάζει τη διεύθυνση IP της συσκευής με το ID του τωρινού ξένου πράκτορα, έρχεται σε επαφή με τον ξένο πράκτορα και προωθεί το μήνυμα. Ο ξένος πράκτορας προωθεί, στη συνέχεια, το μήνυμα στη συσκευή. Αυτή η διαδικασία της **έμμεσης προώθησης** φαίνεται στο Σχήμα 19.3. Αν η συσκευή συνεχίσει να κινείται, ο πρώτος ξένος πράκτορας γίνεται η **"άγκυρα" ξένος πράκτορας** και συνεχίζει να προωθεί πακέτα προς τα εμπρός.



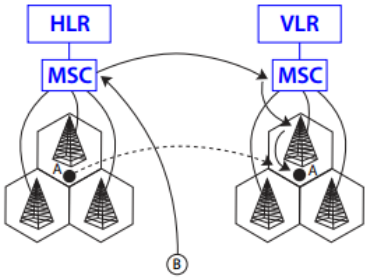
Σχήμα 19.3 *Έμμεση προώθηση για υποστήριξη κινητικότητας. Η συσκευή Α μετακινήθηκε από την τοποθεσία στα αριστερά, δηλαδή το οικείο δίκτυο (Home Network), σε μία νέα τοποθεσία στα δεξιά, στο ξένο δίκτυο (Foreign Network). Ο ξένος πράκτορας (Foreign Agent) ενημερώνει τον οικείο πράκτορα (Home Agent). Έτσι, όταν μία άλλη συσκευή Β καλέσει την Α, η Β έρχεται σε επαφή με τον οικείο πράκτορα ο οποίος προωθεί την κλήση στον ξένο πράκτορα και ο οποίος με τη σειρά του προωθεί την κλήση στη συσκευή Α. Μετά από αυτή την αρχικοποίηση, γίνεται απλούστερο για την Α να επικοινωνήσει με την Β.*

Προσθέτοντας τη διεύθυνση του ξένου πράκτορα στο μήνυμα, γίνεται ξεκάθαρη η πορεία που θα ακολουθήσει το μήνυμα. Αν θέλουμε να το κάνουμε εντελώς διάφανο στη συσκευή Α, ο οικείος πράκτορας μπορεί να ενθυλακώσει το πραγματικό μήνυμα και να το προωθήσει μέσω του ξένου πράκτορα, ο οποίος τότε μπορεί να αφαιρέσει την ενθυλάκωση.

Η αρχή του να έχουμε έναν οικείο πράκτορα σαν τη μόνιμη διεύθυνση "άγκυρα" και έναν συνεχιζόμενα ενημερωμένο ξένο πράκτορα είναι η ιδέα-κλειδί πίσω από πρωτόκολλα κινητού IP και της διαδικασίες διαπομπής στα κινητά δίκτυα.

Το Σχήμα 19.4 δείχνει τη διαδικασία διαπομπής στα δίκτυα 3G. Κάθε κινητό τηλέφωνο έχει μία εγγραφή στη βάση δεδομένων της μόνιμης διεύθυνσης, η οποία ονομάζεται οικείος καταχωρητής θέσης (**Home Location Register (HLR)).** Όταν μετακινείται σε ξένα δίκτυα, η διεύθυνση καταχωρίζεται σε ένα δυναμικό καταχωρητή θέσης επισκεπτών **(Visitor Location Register (VLR))**. Η διαδικασία αυτή στη συνέχεια ακολουθεί την παραπάνω μέθοδο έμμεσης προώθησης, Σχήμα 19.3. Στα πρότυπα 4G LTE, μέχρι το καλοκαίρι του 2012, η υποστήριξη κινητικότητας για τη φωνή και τα δεδομένα ακολουθεί δύο διαφορετικές διαδικασίες, αλλά η κύρια ιδέα της υποστήριξης κινητικότητας παραμένει η ίδια.

Όσον αφορά την πραγματική κατανομή πόρων για τη διαπομπή, εξαρτάται από το εάν το τηλέφωνο κινείται πέρα από τα όρια ενός MSC ή όχι. Κάθε MSC ελέγχει πολλαπλούς σταθμούς βάσης. Αν κινείται πέρα σε ένα διαφορετικό BS αλλά ακόμη στο ίδιο MSC, το MSC μπορεί να διαχειριστεί τη διαπομπή. Αν περάσει σε νέο MSC, όπως φαίνεται στο Σχήμα 19.5, τότε τη στιγμή που ο τωρινός σταθμός βάσης εντοπίσει ότι το SIR είναι χαμηλό και χρειάζεται διαπομπή, ζητάει από το MSC του να ενημερώσει ένα γειτονικό MSC,το οποίο με τη σειρά του ζητά στο σωστό BS να ετοιμαστεί για διαπομπή και να διαθέσει τους απαραίτητους ασύρματους πόρους. Τότε το σήμα "έτοιμος να φύγω" στέλνεται στον τωρινό σταθμό βάσης, ο οποίος "λέει" στο τηλέφωνο να μεταφερθεί στο νέο BS.



Σχήμα 19.4*.Μεταπομπή σε ασύρματα κυψελωτά δίκτυα με έμμεση προώθηση. Οι συμπαγείς μη κατευθυνόμενες ζεύξεις δείχνουν τις συνδέσεις μεταξύ του MSC και των BSs. Η διακεκομμένη γραμμή δείχνει την κίνηση του τηλεφώνου Α από τη μία κυψέλη στην άλλη, η οποία ελέγχεται από ένα διαφορετικό MSC. Οι συμπαγείς κατευθυνόμενες γραμμές αντιπροσωπεύουν το μονοπάτι επικοινωνίας από κάποιον που καλεί ο Β, πρώτα στο MSC στο οικείο δίκτυο του Α, στη συνέχεια στο MSC του δικτύου που επισκέπτεται ο Α και τελικά στο Α .*

19.4.3 Επιβάρυνση στη μεταγωγή και τη δρομολόγηση

Στο Κεφάλαιο 13, μιλήσαμε για τη δρομολόγηση τη βασισμένη σε διευθύνσεις IP. Αλλά η κάρτα δικτύου μίας συσκευής αναγνωρίζει μόνο διευθύνσεις MAC. Σε αντίθεση με τα 32 bit του IP (π.χ. 64.125.8.15), κάθε διεύθυνση MAC είναι των 48 bit, ένας αριθμός κωδικοποιημένος στο υλικό, που συχνά εκφράζεται στον τύπο των 6 τμημάτων από 8 bit το καθένα (π.χ. 00-09-8D-32-B2-21).

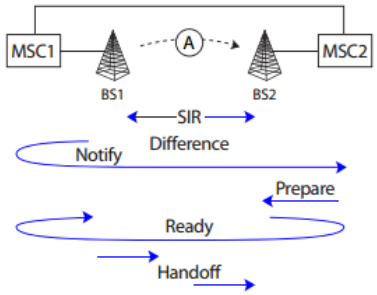
Όταν μιλήσαμε για τη δυναμική ανάθεση των διευθύνσεων IP μέσω του DHCP στο Κεφάλαιο 13, παραλείψαμε τις λεπτομέρειες του πώς γίνεται αυτό όταν μία συσκευή δεν έχει ούτε την αρχική διεύθυνση IP (αυτό είναι ακριβώς που πρέπει να γίνει μέσω DHCP) ούτε τη διεύθυνση IP του προορισμού της (δεν γνωρίζει πού βρίσκεται ο τοπικός εξυπηρετητής DHCP). Τώρα τα παρουσιάζουμε εν συντομία, για να τονίσουμε ότι στα κατανεμημένα πρωτόκολλα πληρώνουμε ένα τίμημα.

Αρχικά, το DHCP λαμβάνει μία διεύθυνση MAC και επιστρέφει μία διεύθυνση IP, μαζί με άλλες πληροφορίες σχετικές με το τοπικό δίκτυο, όπως τον εξυπηρετητή DNS και το δρομολογητή εξόδου. Η δυναμική διεύθυνση IP «μισθώνεται» για μία συγκεκριμένη χρονική περίοδο πριν να πρέπει να ανανεωθεί. Αυτό είναι ένα παράδειγμα προσωρινής κατάστασης (**soft state).**

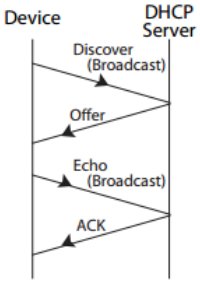
Σε μία προσωρινή κατάσταση, η διαμόρφωση πρέπει περιοδικά να ανανεώνεται. Αν όχι, διαγράφεται, δηλαδή η κατάσταση εξαφανίζεται εκτός και αν έχουν δοθεί διαφορετικές οδηγίες.

Σε αντίθεση, στη μόνιμη κατάσταση (**hard state)**, η διαμόρφωση παραμένει εκεί μέχρις ότου κληθεί μία σαφής εντολή απεγκατάστασης. Η κατάσταση παραμένει ίδια εκτός και αν έχουν δοθεί διαφορετικές οδηγίες. Πολλά πρωτόκολλα στο διαδίκτυο χρησιμοποιούν την προσωρινή κατάσταση επειδή υπάρχει το ρίσκο του να αφήνονται αιωρούμενες καταστάσεις όταν χάνονται πακέτα ελέγχου στο δίκτυο.

Αυτό είναι παρόμοιο με τις κινητές συσκευές που χρησιμοποιούν την προσωρινή κατάσταση για να κρατήσουν την κατάσταση: εκτός και αν χρησιμοποιήσετε το τηλέφωνο πριν τελειώσει ο μετρητής χρόνου, αυτό θα μπει σε κατάσταση αναμονής για εξοικονόμηση ενέργειας.



Σχήμα 19.5*.Μεταπομπή σε ασύρματα κυψελωτά δίκτυα με δέσμευση πόρων. Όταν το τηλέφωνο Α κινείται σε ένα σημείο μεταξύ του BS1 και του BS2,και εντοπίζει ότι το ληφθέν SIR από το BS2 ξεκινά να είναι καλύτερο από αυτό στο BS1,εισάγει μία μεταπομπή. Το MSC1 ειδοποιεί το MSC2, το οποίο ζητά ένα σωστό BS να προετοιμάσει τους απαραίτητους ασύρματους πόρους, τότε ειδοποιεί το MSC1 ότι το BS2 είναι έτοιμο να λάβει το Α. Τέλος, το MSC1 ειδοποιείς το BS1 να αφήσει το Α να μεταβιβαστεί στο BS2.*



Σχήμα 19.6. *Η βασική επιβάρυνση του πρωτοκόλλου που σχετίζεται με μία συσκευή που συνδέεται με έναν εξυπηρετητή DHCP, ώστε να ανακτηθεί η δυναμική διεύθυνση IP από τον εξυπηρετητή. Παρουσιάζεται η αρχή του "όταν αμφισβητείς, φώναξε", καθώς όταν η συσκευή ξεκινά μεταδίδει ένα μήνυμα καθολικής εκπομπής για να ανακαλύψει τους εξυπηρετητές DHCP που μπορεί να φτάσει και μετά να επιλέξει ένα.*

Τώρα, ας επιστρέψουμε στο DHCP. Πώς όμως μία νέα συσκευή σε ένα τοπικό δίκτυο γνωρίζει πώς να έλθει σε επικοινωνία με τον εξυπηρετητή DHCP; Δεν το γνωρίζει. Έτσι στέλνει ένα μήνυμα **καθολικής μετάδοσης** του τύπου "ανακάλυψη του DHCP εξυπηρετητή" για να λύσει αυτό το πρόβλημα στην εκκίνηση. Μερικά μέσα επικοινωνίας, όπως η ασύρματη, είναι εγγενώς καθολικοί μεταδότες από τη φύση τους. Μετά, ο κάθε εξυπηρετητής DHCP που ακούει αυτό το μήνυμα, στέλνει ένα μήνυμα "προσφορά DHCP" (περιλαμβάνει μία διεύθυνση IP, ένα ID του εξυπηρετητή DNS, ένα ID του δρομολογητή εξόδου και το χρόνο μίσθωσης). Η συσκευή τότε αναμεταδίδει μία ηχώ των παραμέτρων του εξυπηρετητή DHCP που διαλέγει. Τέλος, ο επιλεγμένος εξυπηρετητής DHCP καταλαβαίνει ότι έχει επιλεγεί και στέλνει ένα μήνυμα επιβεβαίωσης. Αυτή η διαδικασία φαίνεται στο Σχήμα 19.6.

Δεν έχουμε τελειώσει ακόμη. Η δεύτερη δοκιμασία μας είναι να καθορίσουμε το πώς θα παραδοθεί ένα μήνυμα στο προσαρμογέα του δικτύου της συσκευής προορισμού. Αυτό απαιτεί τη βοήθεια ενός άλλου μεταφραστή: του πρωτοκόλλου ανάλυσης διευθύνσεων (Address Resolution Protocol **(ARP)).** Είναι το αντίθετο από το DHCP: δεδομένης μίας διεύθυνσης IP, το ARP δίνει τη διεύθυνση MAC.

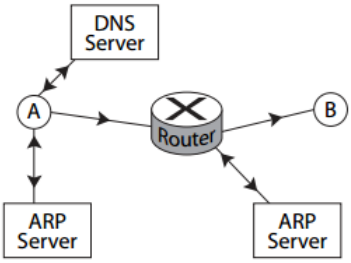
Υποθέτουμε ότι το Α (έστω ένα iPhone) θέλει να επικοινωνήσει με το Β (π.χ. με τον εξυπηρετητή www.bbc.com). Για να απλοποιήσουμε τη ροή, υποθέτουμε ότι το Β είναι συνδεδεμένο με το Α μόνο μέσω ενός δρομολογητή εξόδου.

Πρώτα, το Α παίρνει τη διεύθυνση IP του Β μέσω του DNS (όπως είπαμε στο Κεφάλαιο 13). Τώρα, το Α πρέπει να μεταφράσει τη διεύθυνση IP του προορισμού σε διεύθυνση MAC, εφόσον αυτή τη διεύθυνση "καταλαβαίνουν" οι οδηγοί των συσκευών. Για να το επιτύχουμε αυτό, πρώτα το Α παίρνει τη διεύθυνση MAC του δρομολογητή εξόδου, από το ARP (ξέρει ήδη τη διεύθυνση IP του δρομολογητή από τον εξυπηρετητή DHCP, όπως φαίνεται στο Σχήμα 19.6). Αυτό εδραιώνει ένα μονοπάτι επικοινωνίας μεταξύ του Α και του δρομολογητή. Η συσκευή Α ενθυλακώνει το πακέτο IP σε ένα πλαίσιο MAC. Όταν το λάβει, ο δρομολογητής εξάγει το πακέτο IP από το πλαίσιο MAC και διαβάζει τη διεύθυνση IP του προορισμού. Τώρα, ο δρομολογητής παίρνει τη διεύθυνση MAC του Β, από αυτή τη διεύθυνση IP από άλλο ARP και μπορεί και το στέλνει στο Β. Η παραπάνω διαδικασία φαίνεται στο Σχήμα 19.7.

Και στα δύο Σχήματα 19.6 και 19.7 χρησιμοποιούνται 1 εξυπηρετητής DHCP, 1 εξυπηρετητής DNS και 2 εξυπηρετητές ARP, καθώς και πολλοί γύροι από μηνύματα ελέγχου για τη σηματοδοσία. Όλες αυτές οι επιβαρύνσεις καταναλώνουν χωρητικότητα και προκαλούν καθυστέρηση, μειώνοντας έτσι τη χρήσιμη διαπερατότητα.

Τα παραπάνω πρωτόκολλα ίσως φαίνονται ιδιαίτερα πολύπλοκα. Αν θέλουμε όμως να έχουμε κατανεμημένο συντονισμό σε μία αρχιτεκτονική με επίπεδα, κάποια

μεταφορά μηνυμάτων μεταξύ των στοιχείων του δικτύου είναι το τίμημα που πρέπει να πληρώσουμε.



Σχήμα 19.7*.Η συσκευή "πηγή" με ένα προσαρμογέα δικτύου Α θέλει να φτάσει στην συσκευή "προορισμό" με έναν προσαρμογέα δικτύου Β. Πρώτα πρέπει να έρθει σε επαφή με τον εξυπηρετητή DNS για να λάβει τη διεύθυνση IP του Β. Μετά πρέπει να μεταφράσει τη διεύθυνση IP σε διεύθυνση MAC, την οποία μπορεί να διαβάσει ο οδηγός της συσκευής. Στη συνέχεια, ο δρομολογητής εξόδου διαβάζει τη διεύθυνση IP του Β από το πακέτο του Α, παίρνει τη διεύθυνση MAC του Β από έναν άλλο εξυπηρετητή ARP και, τέλος, βρίσκει έναν τρόπο να επικοινωνεί με το Β .*

Σύνοψη

Πλαίσιο 19 Η ταχύτητα προσφέρεται σε διάφορες γεύσεις

Μία μετάδοση σε ένα κυψελωτό δίκτυο διασχίζει όχι μόνο τον αέρα, αλλά επίσης το δίκτυο κορμού και το δημόσιο Διαδίκτυο. Η χρήσιμη διαπερατότητα στο επίπεδο εφαρμογής συχνά περιορίζεται από τις μη ιδεατές συνθήκες των πολλών κόμβων και ζεύξεων κατά μήκος των μονοπατιών από το ένα άκρο στο άλλο και από τις αναπόφευκτες επιβαρύνσεις στην κατασκευή των πακέτων, των μηνυμάτων ελέγχου και των διαδικασιών των πρωτοκόλλων. Τα αποτελέσματα των δοκιμών ταχυτήτων εξαρτώνται από παράγοντες οι οποίοι δίνονται περιληπτικά από το «ποιο επίπεδο, πού, πότε και γιατί».

Περαιτέρω Μελέτη

Η επίδραση των μη ιδεατών συνθηκών στη διαπερατότητα του επιπέδου εφαρμογής και οι επιβαρύνσεις των δικτυακών πρωτοκόλλων είναι σχετικά λίγο εξερευνημένες περιοχές στις ακαδημαϊκές δημοσιεύσεις.

1. Μία διάσημη συζήτηση για τη διαχείριση δικτύων είναι αυτή για την αρχή του από άκρο σε άκρο, η οποία ξεκίνησε με την ακόλουθη κλασική εργασία:

   J. H. Saltzer, D. P. Reed, and D. D. Clark, "End to end arguments in system design," Proceedings of IEEE International Conference on Distributed Computing Systems, 1981.

2. Στην ασύρματη πλευρά, υπάρχουν πολύ λίγα καλογραμμένα συγγράμματα τα οποία να εστιάζουν στο κυψελωτά δίκτυα κορμού, σχετικά ως προς την εκτεταμένα καλυμμένη περιοχή της εναέριας μετάδοσης. Το ακόλουθο πρόσφατο βιβλίο είναι ένα από τα λίγα:

   M. Olsson, S. Sultanan, S. Rommer, L. Frid, and C. Mulligan, SAE and the Evolved Packet Core, Academic Press, 2009.

3. Ένα κλασικό μεταπτυχιακό εγχειρίδιο για τα δίκτυα δεδομένων από είκοσι χρόνια πριν ακόμη και σήμερα περιέχει μερικά μηνύματα-κλειδιά για τη μελέτη των σημερινών δικτύων.

   D. P. Bertsekas and R. Gallager, Data Networks, 2nd Ed., Prentice Hall, 1992.

4. Αυτό είναι ένα ενδιαφέρον βιβλίο το οποίο συζητά τους υποκείμενους λόγους και ιστορικά ανέκδοτα γιατί τα πρωτόκολλα του Διαδικτύου λειτουργούν με τον τρόπο με τον οποίο λειτουργούν σήμερα:

   J. Day, Patterns in network architecture: A return to fundamentals, Prentice Hall, 2008.

5. Αυτό είναι ένα πρόσφατο βιβλίο το οποίο έχει γραφεί με βάση την πρακτική, εστιάζοντας στην πραγματική πρακτική του σχεδιασμού και της διαχείρισης ενός παγκόσμιου δικτύου.

   G. K. Cambron, Engineering and Operation in Global Network, 2012.

Με σχόλια [C2]: Λείπει ο εκδότης.

Ασκήσεις

19.1 *Η επιβάρυνση του RTS/CTS**

Στην ενότητα των παραδειγμάτων του Κεφαλαίου 18, εκτιμήσαμε το T_s του 802.11g στα 54 Mbps για την περίπτωση που το RTS/CTS έχει απενεργοποιηθεί. Εδώ εκτιμούμε το T_s για την άλλη περίπτωση. Δεδομένου ότι το RTS/CTS έχει

ενεργοποιηθεί, μία επιτυχής μετάδοση αποτελείται από μία ακολουθία [πλαίσιο RTS] + [πλαίσιο CTS] + SIFS + [πλαίσιο δεδομένων] + SIFS + [πλαίσιο ACK] + DIFS. Η μόνη προσθήκη είναι η χειραψία RTS/CTS η οποία συμβαίνει πριν τη μετάδοση των δεδομένων.

Σας δίνετε επίσης ότι (1) ο χρόνος που καταναλώνεται για τη μετάδοση ενός πλαισίου RTS είναι 23,25μs, και (2) ο χρόνος που καταναλώνεται για τη μετάδοση ενός πλαισίου CTS είναι 22,37μs.

(α) Εάν $L = 8192$ bit, υπολογίστε το T_s για την περίπτωση που είναι ενεργοποιημένο το RTS/CTS και για την περίπτωση που είναι απενεργοποιημένο. Υπολογίστε την τελική διαπερατότητα ως προς το L/T_s.

(β) Εάν $L = 320$ bit, υπολογίστε τα T_s και L/T_s πάλι και για τις δύο περιπτώσεις.

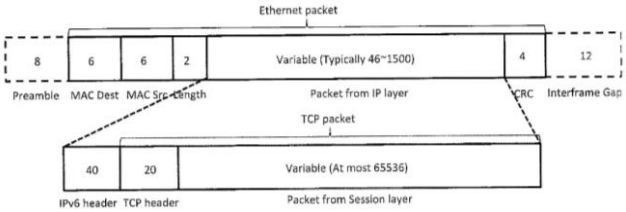
(γ) Στα περισσότερα οικιακά δίκτυα, το RTS/CTS είναι απενεργοποιημένο. Μπορείτε να δείτε το γιατί από τα αποτελέσματα του (α) και του (β);

19.2 *Επιβάρυνση επικεφαλίδων* *

Μία τυπική δομή ενός πακέτου Ethernet φαίνεται στο Σχήμα 19.8. Παρακάτω εξηγούνται οι όροι που χρησιμοποιούνται.

- Πρόθεμα (Preamble): Χρησιμοποιεί 64 bit για να συγχρονίζεται με τη συχνότητα του σήματος πριν γίνει η αποστολή των πραγματικών δεδομένων.
- Προορισμός/Πηγή MAC (Dest/Src): Καταγράφει τις διευθύνσεις MAC του προορισμού και της πηγής κάθε πακέτου και η κάθε μία είναι μεγέθους 6 byte.
- Μήκος (Length): Ορίζει το μήκος του πακέτου IP χρησιμοποιώντας 2 byte.
- Ακολουθία ελέγχου πλαισίου (Frame Check Sequence): Περιέχει έναν έλεγχο κυκλικού πλεονάσματος των 32 bit ο οποίος κάνει δυνατή την ανίχνευση παραποιημένων δεδομένων μέσα σε ένα πακέτο.
- Ενδοπλαισιακό Κενό (Interframe gap): Μετά την αποστολή ενός πακέτου, οι μεταδότες επιβάλλεται να στέλνουν ένα σύνολο από 96 bit τα οποία δηλώνουν μία κατάσταση «άεργης γραμμής» πριν στείλουν το επόμενο πακέτο.
- Επικεφαλίδα IPv6: συνολικά 40 byte.
- Επικεφαλίδα TCP: συνολικά 20 byte.

Ποιο είναι το ποσοστό του ρυθμού δεδομένων του φορτίου εάν στέλνουμε ένα πακέτο των 250 byte;



Σχήμα 19.8. *Δομή πακέτου στο IEEE 802.3 (το μήκος σε byte)*

19.3 *Η διαπερατότητα της φάσης αργής εκκίνησης****

Όπως αναφέραμε στο Κεφάλαιο 14, το TCP ξεκινάει με ένα μικρό παράθυρο συμφόρησης, το οποίο στην αρχή τίθεται ίσο με 1 MSS και υλοποιεί την φάση αργής εκκίνησης (slow start). Το παράθυρο συμφόρησης αυξάνεται πολλαπλασιαστικά, δηλαδή σε 2MSS, 4MSS, 8MSS, …., για κάθε χρόνο μετ' επιστροφής μέχρι να φτάσει το όριο της αργής εκκίνησης και εισέλθει στη φάση της αποφυγής συμφόρησης. Υποθέστε ότι ανοίγετε ένα εξυπηρετητή ιστού και προσπαθείτε να μεταφορτώσετε μία ιστοσελίδα των 70MSS.

(α) Υποθέτοντας ότι δεν υπάρχει απώλεια πακέτων, πόσες RTT απαιτούνται για να μεταφορτώσετε τη σελίδα; Θυμηθείτε να προσθέσετε ένα RTT για να εγκαταστήσετε τη σύνδεση.

(β) Εάν το RTT=100 ms ποια είναι η μέση διαπερατότητα σε kbps; Μπορείτε να δείτε την επίδραση της αργής εκκίνησης στη διαπερατότητα μίας συνεδρίας αργής εκκίνησης;

19.4 *Εναλλακτικές στην έμμεση προώθηση* **

Η ενότητα 19.4.2 ανέφερε τη διαδικασία της έμμεσης προώθησης στη διαχείριση της κινητικότητας. Μπορείτε να προτείνετε μία άλλη μέθοδο προώθησης;

19.5 *Επιβάρυνση σχετιζόμενη με την ασφάλεια* ***

Δεν είχαμε την ευκαιρία, μέχρι τώρα, να μιλήσουμε για τη δικτυακή ασφάλεια, ένα σημαντικό αντικείμενο με πολλά βιβλία να τη διαπραγματεύονται. Υπάρχουν πολλές έννοιες στη λέξη «ασφάλεια», και πολλές διάσημες μέθοδοι για να διασφαλίσουν ή να σπάσουν την ασφάλεια σε ένα δίκτυο. Θα παρουσιάσουμε απλά τα βασικά βήματα τα οποία απαιτούνται για να διασφαλιστεί η εμπιστευτικότητα στο πρωτόκολλο ασφαλούς πυρήνα (Secure Shell (SSH)), το οποίο είναι ένα πρωτόκολλο ασφάλειας στο επίπεδο εφαρμογής το οποίο χρησιμοποιείται συχνά στην απομακρυσμένη πρόσβαση για να διασφαλίσει ότι ο εξυπηρετητής είναι ο σωστός, ο πελάτης αυτός που ισχυρίζεται ό,τι είναι και η επικοινωνία μεταξύ πελάτη και

εξυπηρετητή είναι εμπιστευτική. Στη διαδρομή αυτή, θα δούμε το πόση επιβάρυνση σχετίζεται με την παροχή ασφαλούς υπηρεσίας SSH.

Υπάρχουν πάμπολλα βιβλία και εργασίες για την κρυπτογράφηση κειμένων. Στην άσκηση αυτή, θα χρειαστούμε την έννοια της κρυπτογραφίας δημοσίας κλείδας. Αυτή βασίζεται στις μαθηματικές πράξεις που είναι εύκολες να υπολογιστούν στη μία κατεύθυνση αλλά πολύ δύσκολο το αντίστροφο, π.χ. ο πολλαπλασιασμός δύο πρώτων αριθμών είναι εύκολος, αλλά η παραγοντοποίηση ενός μεγάλου αριθμού σε δύο μεγάλους πρώτους αριθμούς είναι πολύ δύσκολη. Αυτό δίνει τη δυνατότητα να δημιουργηθούν ένα ζεύγος κλειδιών: ένα δημόσιο κλειδί κρυπτογράφησης (γνωστό σε οποιονδήποτε θέλει να στείλει ένα μήνυμα, ας πούμε στην Alice) και ένα ιδιωτικό κλειδί αποκρυπτογράφησης (γνωστό μόνον σε όσους επιτρέπεται να αποκρυπτογραφήσουν το αρχικό μήνυμα).

Τώρα θεωρήστε ότι ένας πελάτης προσπαθεί να συνδεθεί απομακρυσμένα σε ένα εξυπηρετητή. Εάν είστε ο εφευρέτης ενός πρωτοκόλλου ασφαλούς απομακρυσμένης πρόσβασης το οποίο χρησιμοποιεί δημόσιες και ιδιωτικές κλείδες, ποια είναι τα βήματα τα οποία θα σχεδιάζατε; Ποια θα ήταν η μεγαλύτερη τρωτότητα του σχεδίου σας;