ΤΕΧΝΟΛΟΓΙΚΟ
ΕΚΠΑΙΔΕΥΤΙΚΟ
ΙΔΡΥΜΑ
ΤΕΙ ΗΠΕΙΡΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ (Σ.Δ.Ο.)

ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ Κ' ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ:

« ΤΟ ΠΡΩΤΟΚΟΛΛΟ TCP/IP »

ΣΠΟΥΔΑΣΤΗΣ: ***ΜΑΚΡΟΠΟΥΛΟΣ ΝΙΚΟΛΑΟΣ***

ΕΙΣΗΓΗΤΡΙΑ : ***ΑΝΑΛΥΤΗ ΑΙΚΑΤΕΡΙΝΗ***

ΤΟ ΠΡΩΤΟΚΟΛΛΟ TCP/IP

ΠΕΡΙΕΧΟΜΕΝΑ

1 ΕΙΣΑΓΩΓΗ

Το σημερινό Internet αποτελεί εξέλιξη του **ARPANET**, ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του 60 στις ΗΠΑ.

Τη δεκαετία του '60 στα πανεπιστήμια των ΗΠΑ οι ερευνητές ξεκινούν να πειραματίζονται με τη διασύνδεση απομακρυσμένων υπολογιστών μεταξύ τους. Το δίκτυο **ARPANET** γεννιέται το 1969 με πόρους του προγράμματος ARPA του Υπουργείου Άμυνας, με σκοπό να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς και να αποτελέσει ένα πείραμα για τη μελέτη της αξιόπιστης λειτουργίας των δικτύων. Στην αρχική του μορφή, το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων (packet switching), σύμφωνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε πακέτα και πολλοί χρήστες μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή. Στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας. Κάθε πακέτο θα είχε την πληροφορία που χρειάζονταν για να φτάσει στον προορισμό του, όπου και θα γινόταν η επανασύνθεσή του σε δεδομένα τα οποία μπορούσε να χρησιμοποιήσει ο τελικός χρήστης. Το παραπάνω σύστημα θα επέτρεπε σε υπολογιστές να μοιράζονται δεδομένα και σε ερευνητές να υλοποιήσουν το ηλεκτρονικό ταχυδρομείο.

Τη δεκαετία του '70 και συγκεκριμένα το 1973, ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται Internetting Project (Πρόγραμμα Διαδικτύωσης) προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Στόχος είναι η διασύνδεση πιθανώς ανόμοιων δικτύων και η ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο. Από την έρευνα γεννιέται μια νέα τεχνική, το **Internet Protocol** (**IP**) (Πρωτόκολλο Διαδικτύωσης), από την οποία θα πάρει αργότερα το όνομά του το Internet. Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο IP μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Σε ένα δίκτυο IP όλοι οι υπολογιστές είναι ισοδύναμοι, οπότε τελικά οποιοσδήποτε υπολογιστής του διαδικτύου μπορεί να επικοινωνεί με οποιονδήποτε άλλον. Επίσης, σχεδιάζεται μια άλλη τεχνική για τον έλεγχο της μετάδοσης των δεδομένων, το **Transmission Control Protocol** (**TCP**) (Πρωτόκολλο Ελέγχου Μετάδοσης). Ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (E-mail). Σταδιακά συνδέονται με το ARPANET ιδρύματα από άλλες χώρες, με πρώτα το University College of London (Αγγλία) και το Royal Radar Establishment (Νορβηγία).

Τη δεκαετία του '80 το πρωτόκολλο **TCP/IP** (δηλ. ο συνδυασμός των TCP και IP) αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Η έκδοση του λειτουργικού συστήματος Berkeley UNIX το οποίο περιλαμβάνει το TCP/IP συντελεί στη γρήγορη εξάπλωση της διαδικτύωσης των υπολογιστών. Εκατοντάδες Πανεπιστήμια συνδέουν τους υπολογιστές τους στο ARPANET, το οποίο επιβαρύνεται πολύ και το 1983, χωρίζεται σε δύο τμήματα: στο MILNET (για στρατιωτικές επικοινωνίες) και στο νέο ARPANET (για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση). Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το

NSFNET χρησιμοποιώντας το πρωτόκολλο TCP/IP, προκειμένου να συνδέσει πέντε κέντρα υπερ-υπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του ‘80, όλο και περισσότερες χώρες συνδέονται στο NSFNET (Καναδάς, Γαλλία, Σουηδία, Αυστραλία, Γερμανία, Ιταλία, κ.α.). Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο το οποίο αρχίζει να γίνεται γνωστό σαν **INTERNET** και να εξαπλώνεται με τρομερούς ρυθμούς σε ολόκληρο τον κόσμο. Το 1990, το ARPANET πλέον καταργείται.

Τη δεκαετία του ’90 όλο και περισσότερες χώρες συνδέονται στο NSFNET, μεταξύ των οποίων και η Ελλάδα το 1990. Το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει το **World Wide Web** (**WWW**) (Παγκόσμιο Ιστό) που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη. Παράλληλα, εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Internet (Internet Service Providers - ISP) και προσφέρουν πρόσβαση στο Internet για όλους. Οποιοσδήποτε διαθέτει PC και modem μπορεί να συνδεθεί με το Internet σε τιμές που μειώνονται διαρκώς. Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα. Η ανακάλυψη του WWW σε συνδυασμό με την ευκολία απόκτησης πρόσβασης στο Internet προσέλκυσε έναν μεγάλο αριθμό καινούργιων χρηστών και έφερε την “έκρηξη” που παρακολουθήσαμε τα τελευταία χρόνια. Σήμερα, το μεγαλύτερο μέρος του πληθυσμού της Γης ζει σε χώρες που είναι συνδεδεμένες στο Internet. Παρατηρούμε ότι καθημερινά περιοδικά και εφημερίδες εκδίδονται “on-line” και μας παραπέμπουν στις διευθύνσεις τους, επιχειρήσεις και ιδιώτες φτιάχνουν τις δικές τους σελίδες στο WWW, κλπ. Είναι προφανές ότι το Internet δεν αποτελεί πλέον ένα δίκτυο των φοιτητών και των ερευνητών, αλλά ότι επεκτείνεται και επιδρά στις καθημερινές πρακτικές όλων μας. Ήδη μιλάμε για ηλεκτρονικό εμπόριο, τηλεεργασία, τηλεκπαίδευση, τηλεϊατρική, κλπ. μέσα από το Internet.

1.1 Εισαγωγή στο Internet

Το πλήθος των δικτύων, των μηχανών και των χρηστών που ήταν συνδεδεμένοι στο ARPANET αυξήθηκε ραγδαία μετά την καθιέρωση του TCP/IP ως επίσημου πρωτοκόλλου, την $1^{η}$ Ιανουαρίου του 1983. Όταν διασυνδέθηκαν το NSFNET και το ARPANET η αύξηση έγινε εκθετική. Πολλά περιφερειακά δίκτυα συνδέθηκαν, ενώ έγιναν και συνδέσεις με δίκτυα στον Καναδά, την Ευρώπη και τις χώρες του Ειρηνικού.

Κάπου στα μέσα της δεκαετίας του 1980, ο κόσμος άρχισε να αντιμετωπίζει αυτή τη συλλογή δικτύων σαν ένα διαδίκτυο και αργότερα σαν το Διαδίκτυο ή Internet. Ο συνδετικός ιστός του internet είναι το μοντέλο αναφοράς TCP/IP και η στοίβα πρωτοκόλλων TCP/IP. Το TCP/IP επιτρέπει την παροχή της καθολικής υπηρεσίας και μπορεί να συγκριθεί με την υιοθέτηση ενός κοινού πρωτοκόλλου σηματοδοσίας από όλες τις τηλεφωνικές εταιρείες.

Τι ακριβώς σημαίνει να είναι κανείς συνδεδεμένος στο internet; Ο ορισμός μας είναι ότι μια μηχανή είναι συνδεδεμένη στο internet αν εκτελεί τη στοίβα πρωτοκόλλων TCP/IP, έχει μια διεύθυνση IP και μπορεί να στέλνει πακέτα IP σε όλες τις άλλες μηχανές του internet. Η απλή ικανότητα να μπορεί να στέλνει και να λαμβάνει ηλεκτρονικό ταχυδρομείο δεν είναι αρκετή, αφού το ηλεκτρονικό ταχυδρομείο μπορεί να διακινηθεί μέσω πυλών προς πολλά δίκτυα έξω από το internet. Ωστόσο, το ερώτημα γίνεται κάπως νεφελώδες επειδή εκατομμύρια προσωπικών υπολογιστών μπορούν να καλέσουν ένα φορέα παροχής υπολογιστών internet χρησιμοποιώντας ένα modem, να λάβουν μια προσωρινή διεύθυνση IP, και μετά να στείλουν πακέτα σε άλλους υπολογιστές υπηρεσίας στο internet. Είναι λογικό να θεωρήσουμε ότι αυτές οι μηχανές είναι συνδεδεμένες στο internet για όσο χρονικό διάστημα είναι συνδεδεμένες στο δρομολογητή του φορέα παροχής υπηρεσιών.

Παραδοσιακά το Internet και οι προκάτοχοί του είχαν τέσσερις κύριες εφαρμογές:

1. Ηλεκτρονικό ταχυδρομείο. Η δυνατότητα συγγραφής, αποστολής και λήψης ηλεκτρονικού ταχυδρομείου χρονολογείται από τα πρώτα βήματα του ARPANET και είναι εξαιρετικά δημοφιλής. Πολλοί άνθρωποι λαμβάνουν δεκάδες μηνύματα κάθε μέρα και θεωρούν το ηλεκτρονικό ταχυδρομείο ως την πρωταρχική μέθοδο αλληλεπίδρασης με τον έξω κόσμο, με μεγάλη διαφορά από το τηλέφωνο και το απλό ταχυδρομείο. Σήμερα τα προγράμματα ηλεκτρονικού ταχυδρομείου είναι διαθέσιμα ουσιαστικά σε οποιοδήποτε είδος υπολογιστή.
2. Συζητήσεις. Οι ομάδες συζητήσεων (ή ομάδες ειδήσεων) είναι εξειδικευμένα φόρουμ στα οποία χρήστες με κάποιο κοινό ενδιαφέρον μπορούν να ανταλλάσσουν μηνύματα. Υπάρχουν χιλιάδες ομάδες συζητήσεων που είναι αφιερωμένες σε τεχνικά και μη τεχνικά θέματα, στα οποία συμπεριλαμβάνονται οι υπολογιστές, οι επιστήμες, η ανακάλυψη και η πολιτική. Κάθε ομάδα συζητήσεων έχει τη δική της δεοντολογία, στυλ και συνήθειες και αλίμονο σε όποιον τα παραβιάσει.
3. Τηλεσύνδεση. Χρησιμοποιώντας τα προγράμματα telnet, rlogin και ssh οι χρήστες μπορούν να συνδεθούν από οπουδήποτε στο Internet σε οποιαδήποτε άλλη μηχανή στην οποία διαθέτουν ένα λογαριασμό.
4. Μεταφορά αρχείων. Χρησιμοποιώντας το πρόγραμμα FTP, οι χρήστες μπορούν να αντιγράφουν αρχεία από μια μηχανή του Internet σε μια άλλη. Τεράστιες ποσότητες άρθρων, βάσεων δεδομένων και άλλων πληροφοριών είναι διαθέσιμες με αυτόν τον τρόπο.

Μέχρι και τις αρχές της δεκαετίας του 1990, στο Internet βρίσκονταν κυρίως ακαδημαϊκοί, κρατικοί οργανισμοί και βιομηχανικοί ερευνητές. Μια νέα εφαρμογή, ο Παγκόσμιος Ιστός ή WWW (World Wide Web) άλλαξε τα πάντα και έφερε εκατομμύρια νέους, μη ακαδημαϊκούς, χρήστες στο δίκτυο. Η εφαρμογή αυτή, που εφευρέθηκε από το φυσικό Tim Berners-Lee του CERN, δεν άλλαξε κάποια από τις υπάρχουσες λειτουργίες, αλλά τις έκανε ευκολότερες στη χρήση. Μαζί με το πρόγραμμα φυλλομέτρησης (browser) Mosaic ο Παγκόσμιος Ιστός επέτρεψε σε μια τοποθεσία να δημιουργεί σελίδες πληροφοριών οι οποίες περιέχουν κείμενο, εικόνες, ήχο ακόμη και βίντεο με ενσωματωμένους συνδέσμους σε άλλες σελίδες. Πατώντας σε ένα σύνδεσμο, ο χρήστης μεταφέρεται άμεσα στη σελίδα προς την οποία δείχνει ο σύνδεσμος αυτός. Για παράδειγμα πολλές εταιρείες έχουν μια εισαγωγική σελίδα με καταχωρίσεις που δείχνουν σε άλλες σελίδες με στοιχεία προϊόντων, τιμοκαταλόγους, πωλήσεις, τεχνική υποστήριξη, επικοινωνία με υπαλλήλους, πληροφορίες για τους μετόχους και πολλά άλλα.

Πολλά άλλα είδη σελίδων έχουν εμφανιστεί σε πολύ σύντομο χρονικό διάστημα, όπως χάρτες, πίνακες χρηματιστηριακών στοιχείων, κατάλογοι βιβλιοθηκών, μαγνητοφωνημένα ραδιοφωνικά προγράμματα ακόμη και μια σελίδα με συνδέσμους προς το πλήρες κείμενο πολλών βιβλίων για τα οποία έχουν λήξει τα πνευματικά δικαιώματα. Πολλοί άνθρωποι διαθέτουν επίσης προσωπικές σελίδες.

Μεγάλο μέρος της ανάπτυξης κατά τη δεκαετία του 1990 τροφοδοτήθηκε από εταιρείες που ονομάζονται Φορείς Παροχής Υπηρεσιών Internet ή ISP (Internet Service Provider). Αυτές οι εταιρείες παρέχουν στους οικιακούς χρήστες τη δυνατότητα να καλούν από μια από τις μηχανές τους και να συνδέονται στο Internet, αποκτώντας έτσι πρόσβαση στο ηλεκτρονικό ταχυδρομείο, το WWW και τις άλλες υπηρεσίες του Internet. Οι εταιρείες αυτές στα τέλη της δεκαετίας του 1990 αποκτούσαν δεκάδες εκατομμύρια νέους συνδρομητές κάθε χρόνο, αλλάζοντας εντελώς το χαρακτήρα του δικτύου από έναν ακαδημαϊκό και στρατιωτικό χώρο σε μια υπηρεσία κοινής ωφέλειας, παρόμοια με το τηλεφωνικό σύστημα. Το πλήθος των χρηστών του Internet είναι πια άγνωστο, αλλά είναι σίγουρα της τάξης των εκατοντάδων εκατομμυρίων παγκοσμίως και μάλλον θα φτάσει αρκετά σύντομα το ένα δισεκατομμύριο.

1.2 Εισαγωγή στα πρωτόκολλα Internet

Ένα από τα βασικότερα πρωτόκολλα, τα οποία χρησιμοποιούν οι υπολογιστές για να επικοινωνούν μεταξύ τους, όταν βρίσκονται σε ένα εσωτερικό δίκτυο, ή στο Internet, είναι το πρωτόκολλο TCP/IP.

Ο όρος TCP/IP αντιστοιχεί στις λέξεις Transmission Control Protocol/ Internet Protocol και αποτελεί τη βασική γλώσσα -ή αλλιώς πρωτόκολλο- επικοινωνίας των υπολογιστών στο Internet. Κάθε υπολογιστής, ο οποίος έχει άμεση πρόσβαση στο Internet (ή και σε κάποιο εσωτερικό δίκτυο intranet) διαθέτει εγκατεστημένο ένα αντίγραφο του TCP/IP, για να μπορεί να επικοινωνεί με τους υπόλοιπους. Φανταστείτε το Internet σαν ένα τεράστιο δίκτυο υπολογιστών, στο οποίο όλοι οι υπολογιστές χρειάζονται μια ενιαία γλώσσα, προκειμένου να μπορούν αφενός να στέλνουν αρχεία στους άλλους, αλλά και αφετέρου να μπορούν να αποκωδικοποιούν τα αρχεία, που δέχονται από τους υπόλοιπους. Το πρωτόκολλο TCP/IP αποτελείται από δυο μέρη.

Το υψηλότερο στρώμα διαχειρίζεται τη συγκρότηση οποιουδήποτε μηνύματος, ή αρχείου σε μικρότερα πακέτα πληροφοριών, τα οποία αποστέλλονται από τον υπολογιστή μας στο Internet, για να ανασυγκροτήσει και να τα διαβάσει κάποιος άλλος υπολογιστής, ο οποίος επίσης διαθέτει το ίδιο στρώμα TCP.

Από την άλλη μεριά υπάρχει και το χαμηλότερο στρώμα του πρωτοκόλλου TCP/IP, το Internet Protocol. Στην ουσία, το εν λόγω στρώμα του πρωτοκόλλου είναι υπεύθυνο για τη διαχείριση της διεύθυνσης του κάθε υπολογιστή. Το Internet Protocol ορίζει στον κάθε υπολογιστή και από μια συγκεκριμένη διεύθυνση για να μπορούν να τον βρίσκουν οι υπόλοιποι, ενώ ταυτόχρονα φροντίζει για την αποστολή του κάθε πακέτου πληροφοριών, που στέλνει ο υπολογιστής σας στη σωστή διεύθυνση που του ορίσατε.

Το πρωτόκολλο TCP/IP χρησιμοποιεί ένα επικοινωνιακό μοτίβο, που διαθέτει τη μορφή client/server. Αυτό σημαίνει, πως κάποιος χρήστης υπολογιστή, σε αυτήν την περίπτωση client, καλεί μια υπηρεσία (μια σελίδα στο Internet για παράδειγμα), την οποία του την αποστέλλει ένας άλλος υπολογιστής. Η απλή λογική σύνδεση, που χρησιμοποιεί το πρωτόκολλο, είναι η σύνδεση από σημείο σε σημείο, δηλαδή από τον έναν υπολογιστή του δικτύου στον άλλον. Παρ' όλα αυτά, σε αντίθεση με τη λογική για τις τηλεφωνικές γραμμές, κάθε αίτηση ενός υπολογιστή για κάποια υπηρεσία δεν απαιτεί μια αφοσιωμένη σύνδεση μέχρι την ολοκλήρωση της μεταφοράς της υπηρεσίας. Η πληροφορία για παράδειγμα, η οποία θέλετε να μεταφερθεί στον υπολογιστή σας, μπορεί κατά τη μεταφορά της να περάσει και από άλλους υπολογιστές του δικτύου, χωρίς να χρειάζεται να παραμένετε εσείς μόνιμα συνδεδεμένοι με τον αρχικό υπολογιστή, που σας την παρέχει. Παρ' όλα αυτά, το ίδιο το στρώμα TCP του πρωτοκόλλου παραμένει στον υπολογιστή σας, μέχρι να ανασυγκροτηθούν εκεί οι πληροφορίες, τις οποίες ζητήσατε. Ταυτόχρονα, όλα τα πακέτα των πληροφοριών, που μεταφέρονται από τον έναν υπολογιστή στον άλλον, δεν "ανοίγουν", παρά μόνο όταν φτάσουν στο IP του παραλήπτη, που έχει οριστεί.

Η ελευθερία που προσφέρει ουσιαστικά το πρωτόκολλο TCP/IP, έγκειται στο γεγονός, πως επειδή τα δεδομένα δεν είναι απαραίτητο να μεταφέρονται από την ίδια σταθερή γραμμή ενός δικτύου, συνέχεια ελευθερώνονται γραμμές στο δίκτυο, οι οποίες μπορούν να χρησιμοποιηθούν από άλλους υπολογιστές. Αρκετά από τα πιο γνωστά πρωτόκολλα του Internet, σχετίζονται άμεσα με το πρωτόκολλο TCP/IP. Τα πρωτόκολλα HTTP, FTP συχνά διανέμονται μαζί με το TCP/IP, ως ένα πακέτο για την πρόσβαση στο Internet.

Το πρωτόκολλο TCP/IP, είτε πρόκειται για τη σύνδεση κάποιου υπολογιστή με το Internet, είτε για την επικοινωνία του με άλλους υπολογιστές σε κάποιο εσωτερικό δίκτυο, αποτελεί τον απαραίτητο εκείνο συνδετικό κρίκο, ο οποίος βοηθάει στην επικοινωνία μεταξύ των ηλεκτρονικών υπολογιστών.

1.3 Ορισμός πρωτοκόλλου TCP

Στην καθημερινή μας ζωή, πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν το πώς πρέπει να πραγματοποιηθεί κάποια διαδικασία. Στον κόσμο των δικτύων, πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου. Το πρωτόκολλο είναι αυτό που καθορίζει το πώς διακινούνται τα δεδομένα, το πώς γίνεται ο έλεγχος και ο χειρισμός των λαθών, κλπ. Το Internet δεν είναι ένα απλό δίκτυο, αλλά ένα διαδίκτυο. Χρειάζεται επομένως ένα σύνολο από συμβάσεις που να καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα.

Ακριβώς αυτό το σύνολο συμβάσεων προσφέρει το TCP/IP. Όλοι οι υπολογιστές που είναι συνδεδεμένοι στα χιλιάδες μικρότερα δίκτυα του Internet τρέχουν το πρωτόκολλο TCP/IP κι έτσι μιλούν μια κοινή γλώσσα που τους επιτρέπει να συνεννοούνται παρά τις διαφορές τους. Όμως τι ακριβώς κάνει το TCP/IP ;

Ας υποθέσουμε ότι θέλουμε να μεταφέρουμε δεδομένα από έναν υπολογιστή που είναι συνδεδεμένος στο Internet και βρίσκεται π.χ. στην Αμερική, στο MIT, σε έναν άλλον που είναι επίσης συνδεδεμένος στο Internet και βρίσκεται π.χ. στην Ελλάδα, στο Πανεπιστήμιο Θεσσαλίας. Μεταξύ των δύο υπολογιστών παρεμβάλλεται το "σύννεφο" του Internet, δηλ. ένα πλέγμα από συνδέσεις και ενδιάμεσους υπολογιστές.

Το Internet χρησιμοποιεί την τεχνολογία μεταγωγής πακέτων για τη μεταφορά των δεδομένων: τα δεδομένα κόβονται σε κομμάτια που ονομάζονται πακέτα και σε κάθε πακέτο μπαίνει μια "επικεφαλίδα" με τις διευθύνσεις του υπολογιστή - αποστολέα και του υπολογιστή - παραλήπτη. Σημειώνουμε ότι σε κάθε υπολογιστή του Internet αντιστοιχίζεται μία διεύθυνση που ονομάζεται διεύθυνση IP.

Το πρωτόκολλο IP είναι υπεύθυνο για το πέρασμα του πακέτου από υπολογιστή σε υπολογιστή μέσα από το "σύννεφο" των συνδέσεων. Καθώς το IP δρομολογεί το κάθε πακέτο μέσα στο δίκτυο, προσπαθεί να το παραδώσει, αλλά δεν μπορεί να εγγυηθεί ούτε ότι το πακέτο θα φτάσει στον προορισμό του ούτε ότι τα διάφορα πακέτα που αποτελούν τα αρχικά δεδομένα θα φτάσουν με τη σειρά με την οποία στάλθηκαν ούτε ότι το περιεχόμενο των πακέτων θα φτάσει αναλλοίωτο.

Το TCP προσφέρει ένα αξιόπιστο πρωτόκολλο πάνω από το IP. Εγγυάται ότι τα πακέτα θα παραδοθούν στον προορισμό τους, ότι θα φτάσουν με τη σειρά με την οποία στάλθηκαν και ότι τα περιεχόμενα των πακέτων θα φτάσουν αναλλοίωτα (δηλ. όπως στάλθηκαν). Το TCP δουλεύει ως εξής: το κάθε πακέτο δεδομένων αριθμείται. Ο υπολογιστής - παραλήπτης και ο υπολογιστής - αποστολέας, αλλά όχι οι ενδιάμεσοι υπολογιστές, παρακολουθούν τους αριθμούς των πακέτων και ανταλλάσσουν μεταξύ τους πληροφορίες. Ο παραλήπτης λαμβάνει το πρώτο πακέτο, το δεύτερο, κλπ. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στο δίκτυο είτε χαθεί κάποιο πακέτο κατά τη διάρκεια της μετάδοσης, το ξαναζητάει και ο αποστολέας είναι υπεύθυνος για την αναμετάδοση του. Ο παραλήπτης ελέγχει επίσης αν το περιεχόμενο των πακέτων φτάνει σωστά.

Η μέθοδος αυτή εξασφαλίζει αξιοπιστία και ταχύτητα διότι οι ενδιάμεσοι υπολογιστές δεν εκτελούν ελέγχους.

Τώρα λοιπόν που γνωρίσαμε το TCP/IP μπορούμε να δώσουμε έναν πιο "επίσημο" ορισμό του Internet: ένα δίκτυο αποτελούμενο από δίκτυα υπολογιστών που επικοινωνούν χρησιμοποιώντας το πρωτόκολλο TCP/IP. Όπως θα δούμε παρακάτω, η διαδρομή που ακολουθεί ένα πακέτο μέσα από το "σύννεφο" των συνδέσεων δεν είναι προκαθορισμένη.

Αρχικά, υπάρχει το πρωτόκολλο για το μήνυμα, το οποίο ορίζει το σύνολο των εντολών που μια μηχανή θα στέλνει σε κάποια άλλη, π.χ. εντολές για τον καθορισμό του αποστολέα του μηνύματος, του παραλήπτη και το τέλος του κειμένου του μηνύματος. Το πρωτόκολλο αυτό υποθέτει βέβαια, ότι υπάρχει τρόπος αξιόπιστης επικοινωνίας μεταξύ των δυο υπολογιστών. Το ταχυδρομείο, όπως άλλα πρωτόκολλα εφαρμογών απλά καθορίζει ανά σετ εντολών και μηνυμάτων για αποστολή. Είναι σχεδιασμένο να χρησιμοποιείται μαζί με τα TCP και IP. Το TCP είναι υπεύθυνο για το πέρασμα των εντολών στο άλλο άκρο. Κρατάει λογαριασμό του τι αποστέλλεται και επανεκπέμπει οτιδήποτε δεν πέρασε. Αν ένα μήνυμα είναι πολύ μεγάλο για ένα datagram π.χ. το κείμενο του ταχυδρομείου, το TCP θα το χωρίσει σε πολλαπλά datagrams και θα φροντίσει ώστε να φτάσουν σωστά. Εφόσον αυτές οι λειτουργίες απαιτούνται για πολλές εφαρμογές,

ομαδοποιούνται σε ένα ξεχωριστό πρωτόκολλο αντί να αποτελούν μέρος των προδιαγραφών για την αποστολή ταχυδρομείου.

Μπορούμε να σκεφτούμε ότι το TCP φτιάχνει μια βιβλιοθήκη ρουτινών που οι εφαρμογές μπορούν να χρησιμοποιούν, όταν χρειάζονται, αξιόπιστες επικοινωνίες με άλλο υπολογιστή. Όμοια το TCP καλεί τις υπηρεσίες του IP. Αν και οι υπηρεσίες που παρέχει το TCP απαιτούνται από πολλές εφαρμογές, υπάρχουν ακόμα μερικά είδη εφαρμογών που δεν τις χρειάζονται. Σίγουρα όμως υπάρχουν και υπηρεσίες που απαιτούνται από όλες τις εφαρμογές. Οι υπηρεσίες αυτές ομαδοποιούνται στο IP. Όπως και με το TCP, μπορούμε να σκεφτούμε το IP σαν μια βιβλιοθήκη ρουτινών που καλεί το TCP και που είναι επίσης διαθέσιμη σε εφαρμογές που δεν χρησιμοποιούν το TCP. Η στρατηγική αυτή της οικοδόμησης πολλαπλών επιπέδων του πρωτοκόλλου καλείται "layering". Έτσι, μπορούμε να θεωρήσουμε τα διάφορα προγράμματα εφαρμογών στη θέση του ταχυδρομείου και τα TCP, IP σαν ξεχωριστά επίπεδα, κάθε ένα από τα οποία καλεί τις υπηρεσίες του αμέσως πιο χαμηλού επιπέδου.

Γενικά οι TCP/IP εφαρμογές έχουν τέσσερα επίπεδα: Το TCP/IP είναι βασισμένο στο "catenet model". Το μοντέλο αυτό υποθέτει ότι υπάρχει ένας μεγάλος αριθμός ανεξάρτητων δικτύων συνδεδεμένων μεταξύ τους με gateways. Ο χρήστης πρέπει να μπορεί να προσπελάσει υπολογιστές ή άλλα αγαθά σε οποιοδήποτε από αυτά τα δίκτυα. Τα datagrams περνούν συχνά από δεκάδες διαφορετικά δίκτυα πριν φτάσουν στον τελικό τους προορισμό. Η διαδρομή που χρειάζεται για να επιτευχθεί αυτό, πρέπει να είναι αόρατη στο χρήστη.

Όσον αφορά το χρήστη, το μόνο που χρειάζεται να γνωρίζει για την προσπέλαση ενός άλλου συστήματος είναι η Internet διεύθυνσή του. Αυτή είναι μια διεύθυνση με την εξής μορφή: 128.6.4.194. Στην πραγματικότητα, η διεύθυνση είναι ένας 32-bit αριθμός, αν και γράφεται σαν τέσσερα δεκαδικά ψηφία χωρισμένα μεταξύ τους με μια τελεία, που ο καθένας αντιστοιχεί σε 8 bits της διεύθυνσης. (Για τέτοιες ομάδες των 8 bits χρησιμοποιείται ο όρος "octets". Ο όρος "byte" δεν χρησιμοποιείται, επειδή το TCP/IP υποστηρίζεται από μερικούς υπολογιστές που έχουν μήκος byte διαφορετικό των 8 bits). Γενικά, η δομή της διεύθυνσης δίνει πληροφορίες για το πως θα φτάσουμε στο σύστημα. Για παράδειγμα, το 128.6 είναι το νούμερο του δικτύου που έχει ανατεθεί στο Rutgers University. Το Rutgers χρησιμοποιεί το επόμενο octet, για να δηλώσει σε ποιο από τα Ethernets του πανεπιστημίου γίνεται αναφορά. Για παράδειγμα, 128.6.4 είναι το Ethernet που χρησιμοποιείται από το Computer & Science Dept. Το τελευταίο octet επιτρέπει μέχρι και 254 συστήματα σε κάθε Ethernet.

Φυσικά, αναφερόμαστε συνήθως σε συστήματα, με όνομα, παρά με τη διεύθυνση Internet. Όταν δίνουμε ένα όνομα, το λογισμικό του δικτύου συμβουλεύεται μια βάση δεδομένων και βρίσκει την αντίστοιχη διεύθυνση Internet.

Το TCP/IP είναι χτισμένο με τεχνολογία "χωρίς σύνδεση" (connectionless). Η πληροφορία μεταφέρεται σαν μια ακολουθία datagrams. Το datagram είναι μια ομάδα δεδομένων που στέλνεται σαν ξεχωριστό μήνυμα. Κάθε ένα από τα datagrams, στέλνεται ατομικά μέσω του δικτύου. Αφού επιτευχθεί εγκατάσταση σύνδεσης, η πληροφορία διασπάται σε datagrams, τα οποία αντιμετωπίζονται από το δίκτυο απολύτως ξεχωριστά. Για παράδειγμα, υποθέστε ότι θέλετε να μεταφέρετε ένα αρχείο 15000 octets. Τα περισσότερα δίκτυα δεν μπορούν να χειριστούν ένα datagram 15000 octets. Έτσι, τα πρωτόκολλα θα το διασπάσουν π.χ. σε 30 datagrams

των 500 octets. Κάθε ένα από αυτά τα datagrams θα σταλεί στο άλλο άκρο. Στο σημείο αυτό θα επανασυνδεθούν για να διαμορφώσουν το πρωτότυπο αρχείο των 15000 octets. Όσο όμως τα datagrams αυτά είναι σε μεταφορά, το δίκτυο δεν γνωρίζει ότι υπάρχει κάποια σύνδεση μεταξύ τους. Έτσι, είναι πολύ πιθανόν να φτάσει το datagram 14, πριν το 13. Είναι επίσης πιθανό, ότι κάπου στο δίκτυο θα συμβεί κάποιο λάθος και κάποιο datagram δεν θα περάσει καθόλου. Στην περίπτωση αυτή το datagram πρέπει να σταλεί ξανά.

Σημειώνουμε, ότι οι όροι "datagram" και "packet" φαίνονται να έχουν την ίδια έννοια. Τεχνικά, το datagram είναι ο σωστός όρος που πρέπει να χρησιμοποιείται όταν περιγράφεται το TCP/IP. Το datagram είναι μια μονάδα δεδομένων με την οποία ασχολούνται τα πρωτόκολλα. Το πακέτο είναι κάτι φυσικό, που παρουσιάζεται στο Ethernet ή κάποιο καλώδιο. Στις περισσότερες περιπτώσεις το πακέτο απλώς περιέχει ένα datagram κι έτσι η διαφορά είναι πολύ μικρή. Μπορεί όμως και να διαφέρουν. Όταν το TCP/IP χρησιμοποιείται πάνω η X.25 διεπαφή διασπά τα datagrams σε 128-byte πακέτα. Αυτό δεν το βλέπει το IP, επειδή τα πακέτα συντίθεται ξανά σε ένα datagram στην άλλη άκρη πριν τα επεξεργαστεί το TCP/IP. Έτσι στην περίπτωση αυτή ένα IP datagram θα μεταφέρεται από πολλά πακέτα. Στις περισσότερες περιπτώσεις βέβαια, υπάρχουν αρκετά πλεονεκτήματα στην αποστολή ενός datagram / πακέτο και έτσι οι διακρίσεις τείνουν να εξαλειφθούν.

Υπάρχουν δυο διαφορετικά πρωτόκολλα που χειρίζονται τα TCP/IP datagrams. Το TCP είναι υπεύθυνο για τη διάσπαση του μηνύματος σε datagrams και την επανασύνδεσή τους στο άλλο άκρο επαναστέλλοντας οτιδήποτε έχει χαθεί και ταξινομώντας τα στη σωστή σειρά. Το IP είναι υπεύθυνο για τη δρομολόγηση των datagrams. Ίσως φαίνεται ότι το TCP κάνει όλη τη δουλειά. Στα μικρά δίκτυα, αυτό πράγματι συμβαίνει. Παρ' όλα αυτά στο Internet, το να φτάσει απλώς ένα datagram στον προορισμό του μπορεί να είναι μια δύσκολη δουλειά. Το datagram συνήθως πρέπει να περάσει από πολλά διαφορετικά είδη δικτύων όπου απαιτείται χειρισμός των ασυμβατοτήτων μεταξύ των διαφορετικών μέσων μετάδοσης. Σημειώνουμε ότι η διεπαφή μεταξύ του TCP και IP είναι σχετικά απλό. Το TCP απλά παραδίδει στο IP ένα datagram και τον προορισμό του. Το IP δεν γνωρίζει πως το datagram αυτό συνδέεται με το προηγούμενο ή το επόμενό του.

Μέχρι εδώ έχουμε μιλήσει για τις διευθύνσεις του Internet, αλλά όχι για το πώς κρατιέται λογαριασμός των πολλαπλών συνδέσεων σε ένα σύστημα. Σίγουρα δεν είναι αρκετό να φτάσει ένα datagram στο σωστό προορισμό. Το TCP πρέπει να γνωρίζει ποιας σύνδεσης είναι μέρος, το συγκεκριμένο datagram. Η διαδικασία αυτή αναφέρεται σαν "απόπλεξη" (Demultiplexing). Στην πραγματικότητα, υπάρχουν πολλά επίπεδα απόπλεξης στο TCP/IP. Οι πληροφορίες που χρειάζονται για να γίνει η απόπλεξη αυτή περιέχεται σε μια σειρά επικεφαλίδων (headers). Η επικεφαλίδα είναι απλώς μερικά επιπλέον octets που προσαρτούνται στην αρχή των datagrams από ένα πρωτόκολλο. Αμέσως παρακάτω, φαίνεται πως ακριβώς προσαρτούνται επικεφαλίδες σε ένα μήνυμα που περνά μέσα από ένα τυπικό TCP/IP δίκτυο.

Έστω ότι έχουμε ένα αρχείο που πρέπει να το στείλουμε σε έναν άλλο υπολογιστή:

****

Το TCP χωρίζει το αρχείο σε κομμάτια ώστε να μπορεί να τα χειριστεί (Για να γίνει αυτό πρέπει το TCP να γνωρίζει το μεγαλύτερο μήκος datagram που μπορεί να

χειριστεί το συγκεκριμένο δίκτυο. Στην πραγματικότητα τα TCP στις δύο άκρες δηλώνουν το μεγαλύτερο datagram που μπορούν να χειριστούν και επιλέγεται το μικρότερο από τα δύο).

*** *** *** *** *** *** *** *** *** *** *** ***

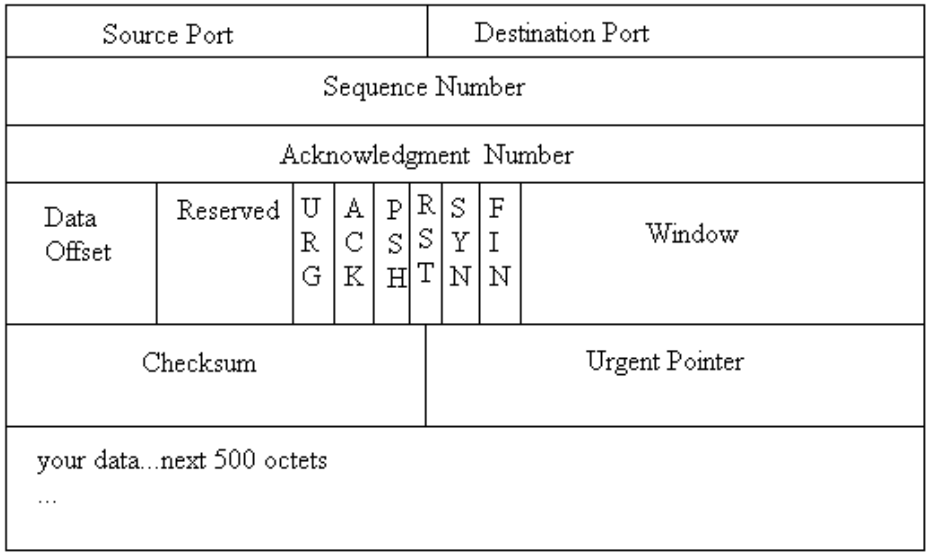
Το TCP βάζει μια επικεφαλίδα στην αρχή του κάθε datagram. Η επικεφαλίδα αυτή περιέχει τουλάχιστον 20 octets, αλλά τα πιο σημαντικά είναι ο αριθμός της πόρτας πηγής και προορισμού και ο αριθμός σειράς (source and destination port number - sequence number) Τα port numbers χρησιμοποιούνται για την ταυτοποίηση των διαφόρων συνδιαλέξεων.

Ας υποθέσουμε ότι 3 διαφορετικοί άνθρωποι μεταφέρουν αρχεία. Το TCP αναθέτει τα port number 1000, 1001, και 1002 στις μεταφορές αυτές. Όταν αποστέλλεται ένα datagram, τα νούμερα αυτά αποτελούν τα source port numbers. Φυσικά το TCP στο άλλο άκρο, έχει αναθέσει ένα δικό του port number για την συνδιάλεξη. Το TCP στο σύστημα αποστολής του αρχείου πρέπει να γνωρίζει το port number που χρησιμοποιείται στο άλλο άκρο, το οποίο και τοποθετεί στο πεδίο πόρτας προορισμού (destination port field). Φυσικά, αν από το άλλο άκρο σταλεί πίσω ένα datagram τα source και destination ports θα αντιστραφούν. Κάθε datagram έχει ένα sequence number. Αυτός ο αριθμός χρησιμοποιείται ώστε το άλλο άκρο να παίρνει τα datagrams στη σωστή σειρά και να εξασφαλίζεται ότι δεν υπάρχουν απώλειες.

Το TCP δεν αριθμεί τα datagrams αλλά τα octets. Έτσι αν υπάρχουν 500 octets δεδομένων σε κάθε datagram, το πρώτο datagram θα έχει αριθμό 0 το δεύτερο 500, το επόμενο 1000 κ.ο.κ. Τέλος, θα αναφερθεί το checksum. Το checksum είναι ένας αριθμός που υπολογίζεται προσθέτοντας όλα τα octets σε ένα datagram. Το αποτέλεσμα μπαίνει στην επικεφαλίδα. Το TCP στο άλλο άκρο υπολογίζει ξανά το checksum. Αν τα δύο checksum δεν συμφωνούν, τότε κάτι έχει συμβεί στο datagram κατά τη διάρκεια της μεταφοράς και απορρίπτεται από το λαμβάνων σύστημα.

Στο παρακάτω σχήμα φαίνεται η τελική μορφή του datagram.

Πίκανας1.



Αν θεωρήσουμε "Τ" τη συντομογραφία της επικεφαλίδας του TCP το αρχείο μας θα έχει τελικά τη μορφή:

Τ*** Τ*** Τ*** Τ*** Τ*** Τ*** Τ*** Τ*** Τ*** Τ***

Σημειώνεται, ότι υπάρχουν κομμάτια της επικεφαλίδας που δεν έχουν περιγραφεί. Γενικά, αυτά έχουν να κάνουν με την διαχείριση της σύνδεσης. Για να εξασφαλιστεί το γεγονός ότι το datagram έχει φτάσει στον προορισμό του, ο λήπτης στέλνει ένα "acknowledgment" (επιβεβαίωση). Αυτό είναι ένα datagram του οποίου το πεδίο "acknowledgment number" είναι συμπληρωμένο.

Για παράδειγμα, στέλνοντας ένα πακέτο με ackn. 1500, σημαίνει ότι έχουν φτάσει όλα τα data έως το octet με νούμερο 1500. Αν ο αποστολέας δεν πάρει acknowledgment μέσα σε ένα συγκεκριμένο χρονικό διάστημα, αποστέλλει ξανά τα δεδομένα. Το πεδίο window χρησιμοποιείται για να ελέγχεται τα πόσα δεδομένα μπορεί να βρίσκονται υπό μεταφορά ταυτόχρονα. Προφανώς, είναι μη πρακτικό να περιμένουμε acknowledgment για κάθε datagram που έχει αποσταλεί για να στείλουμε το επόμενο. Κάτι τέτοιο θα επιβράδυνε πολύ την όλη διαδικασία. Σίγουρα όμως δεν θα μπορούσαμε να στέλναμε συνεχώς δεδομένα διότι ένας γρήγορος αποστολέας θα ξεπερνούσε τη δυνατότητα ενός αργού παραλήπτη να απορροφήσει τα δεδομένα. Έτσι κάθε άκρο δηλώνει πόσα νέα δεδομένα μπορεί να απορροφήσει βάζοντας το νούμερο των octets στο πεδίο "window". Όσο ο υπολογιστής λαμβάνει δεδομένα, το ποσό του χώρου που μένει ελεύθερος στο παράθυρό του μειώνεται. Όταν φτάσει στο μηδέν, ο αποστολέας πρέπει να σταματήσει. Όταν ο λήπτης επεξεργάζεται τα δεδομένα αυξάνει το παράθυρό του, δηλώνοντας ότι είναι έτοιμος να δεχτεί νέα δεδομένα. Συχνά το ίδιο datagram μπορεί να χρησιμοποιηθεί για να επιβεβαιώσει τη λήψη ενός συνόλου δεδομένων και να δώσει την άδεια για επιπρόσθετα νέα δεδομένα. Το πεδίο urgent επιτρέπει στο ένα άκρο να πει στο άλλο να προχωρήσει στην επεξεργασία ενός συγκεκριμένου octet. Είναι επίσης χρήσιμο για το χειρισμό ασύγχρονων γεγονότων π.χ. διακοπή της εξόδου με την πληκτρολόγηση control χαρακτήρα ή άλλης εντολής. Τα άλλα πεδία δεν θα μελετηθούν διότι κάτι τέτοιο ξεφεύγει από τους σκοπούς του κειμένου αυτού.

1.4 Ορισμός πρωτοκόλλου IP

Ένα καλό σημείο για να αρχίσουμε τη μελέτη του επιπέδου δικτύου του Internet είναι η μορφή των ίδιων των αυτοδύναμων πακέτων IP. Το αυτοδύναμο πακέτο IP αποτελείται από ένα κομμάτι κεφαλίδας και ένα κομμάτι κειμένου. Η κεφαλίδα έχει ένα σταθερό τμήμα μεγέθους 20 byte και ένα προαιρετικό τμήμα μεταβλητού μήκους. Μεταδίδεται με σειρά μεγάλου άκρου (big endian): από τα αριστερά προς τα δεξιά, με το σημαντικότερο bit του πεδίου Έκδοση να μεταδίδεται πρώτο. (Οι υπολογιστές SPARC είναι μεγάλου άκρου, οι υπολογιστές Pentium είναι

μικρού άκρου). Στις μηχανές μικρού άκρου, απαιτείται μετατροπή μέσω λογισμικού τόσο κατά τη μετάδοση όσο και κατά τη λήψη.

Το πεδίο Έκδοση (version) δείχνει την έκδοση του πρωτοκόλλου την οποία ακολουθεί το αυτοδύναμο πακέτο. Περιλαμβάνοντας την έκδοση μέσα σε κάθε αυτοδύναμο πακέτο επιτρέπουμε η μετάβαση μεταξύ εκδόσεων να μπορεί να πάρει ακόμα και χρόνια, με μερικές μηχανές να εκτελούν την παλιά έκδοση και άλλες τη νέα. Αυτή τη στιγμή εξελίσσεται μια μετάβαση ανάμεσα στο IPv4 και το IPv6, η οποία έχει ήδη διαρκέσει χρόνια και δεν είναι καθόλου κοντά στην ολοκλήρωση της. Πολλοί μάλιστα πιστεύουν ότι δεν θα συμβεί ποτέ. Παρεμπιπτόντως, σχετικά με την αρίθμηση, το IPv5 ήταν ένα πειραματικό πρωτόκολλο συνεχούς ροής δεδομένων πραγματικού χρόνου, το οποίο δεν χρησιμοποιήθηκε ποτέ ευρέως.

Επειδή το μήκος της κεφαλίδας δεν είναι σταθερό, παρέχεται ένα πεδίο στην κεφαλίδα, το ΜΚΔ (IHL), το οποίο δηλώνει πόσο μεγάλη είναι η κεφαλίδα, σε λέξεις των 32 bit. Η ελάχιστη τιμή είναι 5 και ισχύει όταν δεν υπάρχουν επιλογές. Η μέγιστη τιμή αυτού του 4μπιτου πεδίου είναι 15, γεγονός που περιορίζει την κεφαλίδα σε 60 byte και κατά συνέπεια το πεδίο Επιλογές (options) σε 40 byte. Για μερικές επιλογές, όπως αυτή που καταγράφει το δρομολόγιο που ακολούθησε ένα πακέτο, τα 40 byte είναι πάρα πολύ λίγα και έτσι αυτή η επιλογή είναι σχεδόν άχρηστη.

Το πεδίο Τύπος υπηρεσίας (type of service) είναι ένα από τα πεδία που έχουν αλλάξει (ελαφρώς) νόημα με τα χρόνια. Προοριζόταν και ακόμη προορίζεται για να κάνει διάκριση ανάμεσα σε διαφορετικές τάξεις υπηρεσιών. Είναι πιθανοί διάφοροι συνδυασμοί αξιοπιστίας και ταχύτητας. Για την ψηφιοποιημένη φωνή η γρήγορη παράδοση είναι καλύτερη από την ορθή παράδοση. Για τη μεταφορά αρχείων η μετάδοση χωρίς σφάλματα είναι πιο σημαντική από τη γρήγορη μετάδοση.

Αρχικά, αυτό το 6μπιτο πεδίο περιείχε (από τα αριστερά προς τα δεξιά), ένα πεδίο τριών bit Προτεραιότητα (precedence) και τρεις σημαίες, τις Κ, Δ και Α. Το πεδίο Προτεραιότητα ήταν ένα επίπεδο προτεραιότητας από 0 (κανονική) έως 7 (πακέτο ελέγχου δικτύου). Τα τρία bit σημαίας επέτρεπαν στον υπολογιστή υπηρεσίας να προσδιορίζει για ποιο πράγμα ενδιαφερόταν περισσότερο από το σύνολο {Καθυστέρηση, Διεκπεραίωση, Αξιοπιστία} (Delay, Throughput, Reliability). Θεωρητικά, αυτά τα πεδία επέτρεπαν στους δρομολογητές να κάνουν επιλογές ανάμεσα σε, για παράδειγμα, μια δορυφορική γραμμή με υψηλό εύρος ζώνης και υψηλή καθυστέρηση ή μια μισθωμένη γραμμή με χαμηλό εύρος ζώνης και χαμηλή καθυστέρηση. Στην πράξη, οι τρέχοντες δρομολογητές συχνά παραβλέπουν εντελώς το πεδίο Τύπος υπηρεσίας.

Τελικά η IETF τα παράτησε και άλλαξε ελαφρώς το πεδίο, έτσι ώστε να εξυπηρετεί τις διαφοροποιημένες υπηρεσίας. Έξι από τα bit χρησιμοποιούνται για να δείξουν σε ποια από τις τάξεις υπηρεσίας που αναφέραμε νωρίτερα ανήκει κάθε πακέτο. Οι τάξεις αυτές περιλαμβάνουν τέσσερις προτεραιότητες ουρών, τρεις προτεραιότητες απόρριψης, και τις κληρονομημένες τάξεις.

Το Συνολικό μήκος (total length) περιλαμβάνει όλα τα περιεχόμενα μέσα στο αυτοδύναμο πακέτο- και την κεφαλίδα και τα δεδομένα. Το μέγιστο μήκος είναι 65.535 byte. Προς το παρόν αυτό το άνω όριο είναι ανεκτό, αλλά στα μελλοντικά δίκτυα ταχύτητας gigabit θα χρειαστούν μεγαλύτερα αυτοδύναμα πακέτα.

Το πεδίο Αναγνωριστικό (identification) χρειάζεται για να επιτρέπει στον υπολογιστή υπηρεσίας προορισμού να προσδιορίζει σε ποιο αυτοδύναμο πακέτο

ανήκει το θραύσμα που μόλις έφθασε. Όλα τα θραύσματα ενός αυτοδύναμου πακέτου περιέχουν την ίδια τιμή στο πεδίο Αναγνωριστικό.

Στη συνέχεια έχουμε ένα μη χρησιμοποιούμενο bit και μετά ακολουθούν δύο πεδία του 1 bit. Το πεδίο ΟΚ σημαίνει Όχι Κατακερματισμός (DF, don't fragment). Είναι μια διαταγή προς τους δρομολογητές να μην κατακερματίσουν το αυτοδύναμο πακέτο, επειδή ο προορισμός δεν είναι σε θέση να συναρμολογήσει ξανά όλα τα τμήματα του πακέτου. Για παράδειγμα, όταν ξεκινά ένας υπολογιστής , η ROM του μπορεί να ζητήσει να του αποσταλεί μια εικόνα της μνήμης σε ένα μόνο αυτοδύναμο πακέτο. Σημειώνοντας το αυτοδύναμο πακέτο με το bit ΟΚ, ο αποστολέας ξέρει ότι το πακέτο θα φτάσει ενιαίο- ακόμα και αν αυτό σημαίνει ότι το αυτοδύναμο πακέτο θα πρέπει να αποφύγει ένα δίκτυο μικρών πακέτων το οποίο βρίσκεται στην καλύτερη διαδρομή και κατά συνέπεια θα ακολουθήσει ένα μη βέλτιστο δρομολόγιο. Όλες οι μηχανές απαιτείται να δέχονται θραύσματα μήκους 576 byte ή μικρότερα.

Το πεδίο ΠΘ σημαίνει Περισσότερα Θραύσματα (MF, more fragments). Όλα τα θραύσματα εκτός από το τελευταίο έχουν ενεργοποιημένο αυτό το bit. Αυτό απαιτείται έτσι ώστε να γνωρίζουμε πότε έχουν φτάσει όλα τα θραύσματα ενός αυτοδύναμου πακέτου.

Η Σχετική απόσταση θραύσματος (fragment offset) δείχνει που βρίσκεται αυτό το θραύσμα στο τρέχον αυτοδύναμο πακέτο. Όλα τα θραύσματα εκτός από το τελευταίο ενός αυτοδύναμου πακέτου θα πρέπει να είναι πολλαπλάσια των 8 byte, που είναι το στοιχειώδες μέγεθος των θραυσμάτων. Αφού παρέχονται 13 bit, έχουμε ένα μέγιστο όριο 8192 θραυσμάτων ανά αυτοδύναμο πακέτο, γεγονός που δίνει μέγιστο μήκος αυτοδύναμου πακέτου ίσο με 65.536 byte, ένα byte περισσότερο απ' ό,τι το πεδίο Συνολικό μήκος.

Το πεδίο Χρόνος ζωής (time to live) είναι ένας μετρητής που χρησιμοποιείται για τον περιορισμό της ζωής των πακέτων. Υποτίθεται ότι μετρά το χρόνο σε δευτερόλεπτα, επιτρέποντας μέγιστο χρόνο ζωής ίσο με 255 sec. Θα πρέπει να μειώνεται σε κάθε άλμα, και υποτίθεται ότι θα μειώνεται πολλές φορές όταν το πακέτο βρίσκεται για πολλή ώρα στην ουρά ενός δρομολογητή. Στην πράξη απλώς μετρά άλματα. Όταν φτάσει στο μηδέν, το πακέτο απορρίπτεται και επιστρέφεται στον αποστολέα ένα πακέτο προειδοποίησης. Αυτό το χαρακτηριστικό αποτρέπει τα αυτοδύναμα πακέτα από το να περιπλανούνται για πάντα – κάτι που θα μπορούσε να συμβεί αν τύχαινε να αλλοιωθούν οι πίνακες δρομολόγησης.

Όταν το επίπεδο δικτύου συναρμολογήσει ένα πλήρες αυτοδύναμο πακέτο, πρέπει να ξέρει τι να το κάνει. Το πεδίο Πρωτόκολλο (protocol) λέει σε ποια διεργασία επιπέδου μεταφοράς να το δώσει. Μία πιθανότητα είναι το TCP, υπάρχει όμως και το UDP, καθώς και άλλα πρωτόκολλα. Η αρίθμηση των πρωτοκόλλων είναι κοινή σε ολόκληρο το Internet.

Το Άθροισμα ελέγχου κεφαλίδας (header checksum) επαληθεύει μόνο την κεφαλίδα. Αυτό το άθροισμα ελέγχου είναι χρήσιμο για την ανίχνευση σφαλμάτων που παράγονται από προβληματικές λέξεις μνήμης μέσα σε ένα δρομολογητή. Ο αλγόριθμος είναι να αθροίζονται όλες οι μισές λέξεις των 16 bit καθώς φτάνουν, χρησιμοποιώντας αριθμητική συμπληρώματος ως προς ένα, και μετά να παίρνουμε το συμπλήρωμα ως προς ένα του αποτελέσματος. Για τις ανάγκες του αλγόριθμου αυτού, το Άθροισμα ελέγχου κεφαλίδας θεωρείται μηδενικό κατά την άφιξη. Ο αλγόριθμος αυτός είναι πιο ανθεκτικός από τη χρήση μιας απλής πρόσθεσης. Σημειώνουμε ότι το Άθροισμα ελέγχου κεφαλίδας πρέπει να υπολογίζεται ξανά σε

κάθε άλμα επειδή αλλάζει πάντα ένα τουλάχιστον πεδίο (το πεδίο χρόνος ζωής), μπορούν όμως να χρησιμοποιηθούν κάποια κόλπα για επιτάχυνση του υπολογισμού.

Η Διεύθυνση προέλευσης (source address) και η Διεύθυνση προορισμού (destination address) δείχνουν τον αριθμό δικτύου και τον αριθμό υπολογιστή υπηρεσίας. Το πεδίο Επιλογές (options) σχεδιάστηκε για να παρέχει έναν τρόπο διαφυγής ο οποίος θα επιτρέπει σε επόμενες εκδόσεις του πρωτοκόλλου να περιέχουν πληροφορίες που δεν υπήρχαν στην αρχική σχεδίαση, θα δίνει στους ερευνητές τη δυνατότητα να δοκιμάζουν νέες ιδέες, και θα αποφεύγει την εκχώρηση bit κεφαλίδας για πληροφορίες που χρειάζονται σπάνια. Οι επιλογές έχουν μεταβλητό μήκος. Κάθε επιλογή αρχίζει με έναν κωδικό 1 byte που προσδιορίζει την επιλογή. Μερικές επιλογές ακολουθούνται από ένα πεδίο μήκους επιλογής με μέγεθος 1 byte,και στη συνέχεια ακολουθούν ένα ή περισσότερα byte δεδομένων. Το πεδίο Επιλογές συμπληρώνεται σε πολλαπλάσια των τεσσάρων byte. Αρχικά είχαν οριστεί πέντε επιλογές, αλλά σήμερα έχουν οριστεί και μερικές νέες.

Η επιλογή Ασφάλεια (security) δηλώνει πόσο μυστικές είναι οι πληροφορίες. Θεωρητικά ένας στρατιωτικός δρομολογητής μπορεί να χρησιμοποιήσει αυτό το πεδίο για να προσδιορίσει ότι δεν πρέπει να γίνει δρομολόγηση μέσω ορισμένων χωρών που θεωρούνται ‘κακές’ από το στρατό. Στην πράξη όλοι οι δρομολογητές το παραβλέπουν, έτσι η μόνη πρακτική χρησιμότητά του είναι να βοηθά τους κατασκόπους να εντοπίζουν πιο εύκολα τις σημαντικές πληροφορίες.

Η επιλογή Αυστηρή δρομολόγηση προέλευσης (strict source routing) προσδιορίζει την πλήρη διαδρομή από την προέλευση ως τον προορισμό, με τη μορφή μιας ακολουθίας διευθύνσεων IP. Το αυτοδύναμο πακέτο θα πρέπει να ακολουθήσει αυτή ακριβώς τη διαδρομή. Η επιλογή αυτή είναι ιδιαίτερα χρήσιμη για τους διαχειριστές των συστημάτων, έτσι ώστε να στέλνουν πακέτα έκτακτης ανάγκης όταν παραμορφώνονται οι πίνακες δρομολόγησης, ή να μπορούν να εκτελούν χρονομετρήσεις.

Η επιλογή Χαλαρή δρομολόγηση προέλευσης (loose source routing) απαιτεί να περάσει το πακέτο από τη λίστα προσδιοριζόμενων δρομολογητών, με τη σειρά που καθορίζονται, αν και μπορεί να περάσει και από άλλους δρομολογητές στη διαδρομή. Κανονικά η επιλογή αυτή θα περιέχει λίγους μόνο δρομολογητές, με στόχο να επιβάλει τη χρήση μιας συγκεκριμένης διαδρομής. Για παράδειγμα, για να εξαναγκαστεί ένα πακέτο που πηγαίνει από το Λονδίνο στο Σύδνεϋ να κινηθεί δυτικά αντί ανατολικά, αυτή η επιλογή μπορεί να προσδιορίζει δρομολογητές στη Νέα Υόρκη, το Λος Άντζελες, και τη Χονολουλού. Η επιλογή αυτή είναι πιο χρήσιμη όταν πολιτικοί ή οικονομικοί λόγοι επιβάλουν τη χρήση ή την αποφυγή ορισμένων χωρών.

Η επιλογή Καταγραφή δρομολογίου (record route) ζητά από τους δρομολογητές που υπάρχουν κατά μήκος της διαδρομής να επισυνάπτουν τη διεύθυνση IP τους στο πεδίο των επιλογών. Αυτό επιτρέπει στους διαχειριστές των συστημάτων να εντοπίζουν σφάλματα στον αλγόριθμο δρομολόγησης (‘Γιατί τα πακέτα από το Χιούστον στο Ντάλας επισκέπτονται πρώτα το Τόκιο;’).Όταν εγκαταστάθηκε αρχικά το ARPANET κανένα πακέτο δεν διέσχιζε ποτέ περισσότερους από εννιά δρομολογητές, έτσι 40 byte επιλογών ήταν υπερεπαρκή. Όπως αναφέραμε προηγουμένως, τώρα πια είναι πολύ λίγα.

Τέλος, η επιλογή Χρονοσφραγίδα (timestamp) μοιάζει με την επιλογή Καταγραφή δρομολογίου, με τη διαφορά ότι, εκτός από την καταγραφή της 32μπιτης διεύθυνσης IP, κάθε δρομολογητής θα πρέπει επίσης να καταγράφει και μια 32μπιτη χρονοσφραγίδα. Και αυτή η επιλογή χρησιμεύει κυρίως για τον εντοπισμό σφαλμάτων στους αλγόριθμους δρομολόγησης. Το TCP στέλνει καθένα από τα datagrams στο IP. Πρέπει βέβαια να πληροφορήσει το IP για την Internet διεύθυνση του υπολογιστή στο άλλο άκρο. Σημειώνουμε ότι η διεύθυνση αυτή είναι η μόνη που ενδιαφέρει το IP. Το IP δεν ενδιαφέρεται για το τι περιέχει το datagram ή η επικεφαλίδα TCP. Η δουλειά του IP είναι απλά να εξασφαλίσει το μονοπάτι ώστε το datagram να φτάσει στο άλλο άκρο. Το IP προσθέτει τις δικές του επικεφαλίδες ώστε το datagram να προωθηθεί από άλλα ενδιάμεσα συστήματα. Η επικεφαλίδα αυτή περιέχει βασικά τις Internet διευθύνσεις του συστήματος πηγής και προορισμού (32 bits π.χ. 128.6.4.194), τον αριθμό πρωτοκόλλου και ένα ακόμη checksum. Η Internet διεύθυνση είναι απλά η διεύθυνση της μηχανής που στέλνει τα δεδομένα. (Είναι απαραίτητη ώστε το άλλο άκρο να γνωρίζει από που ήρθε το datagram). Η διεύθυνση προορισμού είναι η διεύθυνση στην οποία θέλουμε να φτάσουν τα δεδομένα. (Είναι απαραίτητη ώστε τα ενδιάμεσα συστήματα να γνωρίζουν που πρέπει να πάει το datagram). Ο αριθμός πρωτοκόλλου πληροφορεί το IP στο άλλο άκρο ότι πρέπει να στείλει το datagram στο TCP. (Μπορεί να υπάρχουν και άλλα πρωτόκολλα εκτός του TCP που χρησιμοποιούν το IP οπότε το IP πρέπει να πληροφορηθεί σε ποιο πρωτόκολλο θα στείλει το datagram). Τέλος, το checksum επιτρέπει στο IP στο άλλο άκρο, να επαληθεύσει ότι το header δεν καταστράφηκε κατά τη μετάδοση. Σημειώνουμε, ότι το TCP και το IP έχουν διαφορετικά checksums. Το IP πρέπει να μπορεί να εξακριβώσει ότι η επικεφαλίδα δεν καταστράφηκε, αλλιώς υπάρχει περίπτωση να στείλει ένα μήνυμα σε λάθος μέρος. Όταν το IP προσαρτήσει την επικεφαλίδα του, το μήνυμα θα δείχνει όπως παρακάτω:

Πίνακας 2.

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td>Time to Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">TCP Header, then your data...</td></tr>
</table>

Αν συμβολίσουμε την επικεφαλίδα του IP με I, το αρχείο θα έχει τη μορφή:

IT*** IT*** IT*** IT*** IT*** IT*** IT*** IT*** IT*** IT***

Και εδώ, η επικεφαλίδα αποτελείται από μερικά επιπλέον πεδία στα οποία δεν έχουμε αναφερθεί. Τα περισσότερα από αυτά ξεφεύγουν από το σκοπό του κειμένου. Τα πεδία "flags" και "fragment effect" χρησιμοποιούνται όταν ένα datagram πρέπει να χωριστεί σε κομμάτια. Αυτό μπορεί να συμβεί όταν τα datagrams προωθούνται σε ένα δίκτυο, το οποίο δεν μπορεί να χειριστεί τόσο μεγάλα datagrams. Το πεδίο "time to live" περιέχει έναν αριθμό που μειώνεται κάθε φορά που ένα datagram περνά μέσα από ένα σύστημα. Όταν γίνεται 0, το datagram εξαλείφεται. Αυτό γίνεται σε περίπτωση που για κάποιο λόγο εμφανιστεί βρόγχος μέσα στο δίκτυο. Κάτι τέτοιο είναι βέβαια απίθανο, αλλά τα καλά σχεδιασμένα δίκτυα είναι φτιαγμένα ώστε να μπορούν να αντιμετωπίσουν και απίθανες καταστάσεις. Στο σημείο αυτό αναφέρεται, ότι είναι πιθανόν να μην χρειαστούν περισσότερες επικεφαλίδες. Εαν ο υπολογιστής σας συνδέεται απευθείας μέσω τηλεφωνικής γραμμής με τον υπολογιστή προορισμού, μπορεί να στείλει απευθείας τα datagrams στη γραμμή (αν και στην πραγματικότητα θα έπρεπε να χρησιμοποιείται ένα σύγχρονο πρωτόκολλο σαν το HDLC, όπου θα πρόσθετε τουλάχιστον λίγα octets στην αρχή και το τέλος).

2 ΜΟΝΤΕΛΑ ΑΝΑΦΟΡΑΣ

Έχοντας ορίσει τα πρωτόκολλα TCP και IP, στις επόμενες ενότητες θα μελετήσουμε κάποιες σημαντικές αρχιτεκτονικές δικτύων, το μοντέλο αναφοράς TCP/IP, το μοντέλο αναφοράς UDP και το μοντέλο αναφοράς OSI.

2.1 ΠΡΩΤΟΚΟΛΛΑ ΤΥΠΟΥ TCP/IP

2.1.1 Μοντέλο αναφοράς TCP/IP

Το μοντέλο αναφοράς αυτό χρησιμοποιείται στο παγκόσμιο Internet. Η ικανότητα διασύνδεσης πολλών δικτύων με διαφανή τρόπο, η ικανότητα του δικτύου να επιβιώνει από απώλειες στο υλικό του υποδικτύου χωρίς να τερματίζονται οι υπάρχουσες συνδέσεις και η δυνατότητα χρήσης εφαρμογών με ριζικά διαφορετικές απαιτήσεις, από μεταφορά αρχείων έως μετάδοση ομιλίας σε πραγματικό χρόνο, οδήγησαν στη σχεδίαση μιας αρχιτεκτονικής γνωστή ως Μοντέλο Αναφοράς TCP/IP χρησιμοποιώντας το όνομα των δύο βασικών πρωτοκόλλων.

Το επίπεδο διαδικτύου

Επιλέχθηκε ένα δίκτυο μεταγωγής πακέτων που βασίζεται σε ένα ασυνδεσμικό επίπεδο διαδικτύου, που ονομάζεται επίπεδο διαδικτύου και είναι ο ακρογωνιαίος λίθος ολόκληρης της αρχιτεκτονικής. Η δουλειά του είναι να επιτρέπει στους υπολογιστές υπηρεσίας να εισάγουν τα πακέτα τους σε οποιοδήποτε δίκτυο και αυτά να ταξιδεύουν ανεξάρτητα προς τον προορισμό τους. Τα πακέτα μπορεί να φτάσουν ακόμη και με διαφορετική σειρά από αυτή που στάλθηκαν. Στην περίπτωση αυτή είναι δουλειά των ανώτερων επιπέδων να αναδιατάξουν τα πακέτα, εάν είναι επιθυμητή η παράδοση των πακέτων με τη σειρά. Το επίπεδο διαδικτύου ορίζει μια επίσημη μορφή για τα πακέτα και ένα επίσημο πρωτόκολλο που ονομάζεται Πρωτόκολλο Διαδικτύου ή IP και σκοπός του είναι να παραδίδει τα πακέτα IP εκεί όπου προορίζονται. Συνεπώς βασικό μέλημα είναι η δρομολόγηση των πακέτων και η αποφυγή συμφόρησης.

Το επίπεδο μεταφοράς

Το επίπεδο που βρίσκεται πάνω από το επίπεδο διαδικτύου ονομάζεται επίπεδο μεταφοράς. Έχει σχεδιαστεί για να επιτρέπει στις ομότιμες οντότητες στους υπολογιστές υπηρεσίας προέλευσης και προορισμού να συνομιλούν. Έχουν οριστεί

δύο πρωτόκολλα μεταφοράς από άκρου εις άκρο. Το πρώτο, το Πρωτόκολλο Ελέγχου Μετάδοσης ή TCP, είναι ένα αξιόπιστο συνδεσμοστρεφές πρωτόκολλο, το οποίο επιτρέπει σε μια ροή byte που προέρχεται από μια μηχανή να παραδίδεται χωρίς σφάλματα σε οποιαδήποτε άλλη μηχανή στο διαδίκτυο. Το πρωτόκολλο τεμαχίζει την εισερχόμενη ροή byte σε διακριτά μηνύματα και μεταβιβάζει το καθένα από αυτά στο επίπεδο διαδικτύου. Στον προορισμό, η διεργασία-παραλήπτης του TCP ανασυναρμολογεί τα μηνύματα που λαμβάνει σε μια ροή εξόδου. Το TCP χειρίζεται επίσης και τον έλεγχο ροής, εξασφαλίζοντας ότι ένας γρήγορος αποστολέας δε θα μπορεί να κατακλείσει ένα αργό παραλήπτη με περισσότερα μηνύματα από όσα μπορεί αυτός να χειριστεί.

Το δεύτερο πρωτόκολλο στο επίπεδο αυτό, είναι το Πρωτόκολλο Αυτοδύναμων Πακέτων ή UDP, είναι ένα αναξιόπιστο ασυνδεσμικό πρωτόκολλο το οποίο προορίζεται για εφαρμογές που δε χρειάζονται τη παράδοση των πακέτων με τη σωστή σειρά ή τον έλεγχο ροής του TCP, αφού επιθυμούν να παρέχουν δικούς τους μηχανισμούς. Περισσότερα όμως για το πρωτόκολλο αυτό θα δούμε σε επόμενη παράγραφο.

Το επίπεδο εφαρμογών

Πάνω από το επίπεδο μεταφοράς είναι το επίπεδο εφαρμογών. Αυτό περιέχει όλα τα πρωτόκολλα ανώτερου επιπέδου. Στην αρχή σε αυτά περιλαμβάνονταν το εικονικό τερματικό (TELNET), η μεταφορά αρχείων (FTP), και το ηλεκτρονικό ταχυδρομείο. Το πρωτόκολλο μεταφοράς αρχείων παρέχει ένα τρόπο αποτελεσματικής μεταφοράς δεδομένων από μηχανή σε μηχανή. Το ηλεκτρονικό ταχυδρομείο αρχικά ήταν ένα είδος μεταφοράς αρχείων, αργότερα όμως ένα εξειδικευμένο πρωτόκολλο (SMTP) γι’ αυτό. Με τα χρόνια προστέθηκαν πολλά ακόμα πρωτόκολλα, εκτός από τα προαναφερθέντα: το Σύστημα Ονομάτων Περιοχών (DNS) για την αντιστοίχηση των ονομάτων των υπολογιστών υπηρεσίας στις διευθύνσεις δικτύου τους, το NNTP, το πρωτόκολλο για τη μετάδοση των άρθρων των ομάδων συζητήσεων του USENET, και το HTTP, το πρωτόκολλο για την προσκόμιση σελίδων στον Παγκόσμιο Ιστό, καθώς και πολλά άλλα.

Το επίπεδο διασύνδεσης μεταξύ υπολογιστή υπηρεσίας και δικτύου

Κάτω από το επίπεδο διαδικτύου έχουμε ένα μεγάλο κενό. Το μοντέλο αναφοράς TCP/IP δε λέει και πολλά για το τι συμβαίνει εκεί, αλλά απλώς παρατηρεί ότι ο υπολογιστής υπηρεσίας πρέπει να συνδέεται με το δίκτυο χρησιμοποιώντας κάποιο πρωτόκολλο έτσι ώστε να μπορεί να στέλνει πακέτα IP. Το πρωτόκολλο αυτό δεν προσδιορίζεται και διαφέρει από υπολογιστή σε υπολογιστή και από δίκτυο σε δίκτυο.

2.1.2 Μοντέλο αναφοράς UDP

Όπως προαναφέρθηκε, επιπλέον του TCP, υπάρχει ένα ακόμη πρωτόκολλο επιπέδου μεταφοράς που είναι συνηθισμένο ως μέρος του μοντέλου TCP/IP: το πρωτόκολλο αυτόνομων πακέτων χρήστη (User Datagram Protocol - UDP). Το UDP παρέχει μία υπηρεσία χωρίς σύνδεση για διαδικασίες επιπέδου εφαρμογής. Έτσι, το UDP είναι βασικά μία μη αξιόπιστη υπηρεσία. Η παράδοση και η προστασία από αντίγραφα δεν είναι εξασφαλισμένες. Ωστόσο, αυτό μειώνει την επιβάρυνση του πρωτοκόλλου και μπορεί να είναι επαρκές σε αρκετές περιπτώσεις.

Η δύναμη της προσέγγισης με σύνδεση είναι εμφανής. Επιτρέπει χαρακτηριστικά σχετικά με τη σύνδεση όπως ο έλεγχος ροής, ο έλεγχος σφαλμάτων και η διατεταγμένη παράδοση. Ωστόσο, σε μερικά περιβάλλοντα είναι περισσότερο κατάλληλη η υπηρεσία χωρίς σύνδεση. Σε χαμηλότερα στρώματα (διαδικτύου, δικτύου), η υπηρεσία χωρίς σύνδεση είναι περισσότερο εύρωστη. Επίσης, αντιπροσωπεύει έναν ‘‘ελάχιστο κοινό παρανομαστή’’ υπηρεσίας που αναμένεται σε υψηλότερα στρώματα. Επιπλέον, ακόμη και στο στρώμα μεταφοράς και άνω υπάρχει δικαιολογία για την ύπαρξη μίας υπηρεσίας χωρίς σύνδεση. Υπάρχουν περιπτώσεις στις οποίες η επιβάρυνση από την αποκατάσταση σύνδεσης και την υποστήριξη είναι αδικαιολόγητη ή ακόμη και αντιπαραγωγική. Μερικά παραδείγματα είναι τα παρακάτω:

- Εσωτερική συλλογή δεδομένων: περιλαμβάνει την περιοδική ενεργή ή παθητική δειγματοληψία πηγών δεδομένων, όπως αισθητήρες και αυτόματες αυτοδιαγνωστικές αναφορές από εξοπλισμό ασφαλείας ή συνιστώσες δικτύου. Σε μία κατάσταση παρακολούθησης πραγματικού χρόνου, η απώλεια μίας τυχαίας μονάδας δεδομένων δε θα προκαλέσει καταπόνηση, επειδή η επόμενη αναφορά θα φτάσει σύντομα.
- Εξωτερική διασπορά δεδομένων: περιλαμβάνει μηνύματα ευρείας εκπομπής σε χρήστες δικτύου, την ανακοίνωση ενός νέου κόμβου ή την αλλαγή της διεύθυνσης μίας υπηρεσίας, καθώς και τη διανομή τιμών χρονομέτρου πραγματικού χρόνου.
- Αίτηση-απόκριση: εφαρμογές στις οποίες μία υπηρεσία συναλλαγής από έναν κοινό server σε έναν αριθμό από κατανεμημένους χρήστες TS για τους οποίους είναι τυπική μία ακολουθία αίτησης-απόκρισης. Η χρήση της υπηρεσίας ρυθμίζεται στο στρώμα εφαρμογής και συνδέσεις χαμηλότερου επιπέδου είναι συχνά άσκοπες και δυσκίνητες.
- Εφαρμογές πραγματικού χρόνου: όπως φωνή και τηλεμετρία, περιλαμβάνοντας ένα βαθμό απόρριψης και/ή απαίτησης μετάδοσης πραγματικού χρόνου. Αυτές δεν πρέπει να έχουν λειτουργίες σύνδεσης όπως και η αναμετάδοση.

Έτσι, υπάρχει ένα μέρος στο στρώμα μεταφοράς τόσο για υπηρεσία με σύνδεση όσο και για υπηρεσία χωρίς σύνδεση.

Το UDP κάθεται πάνω από το IP. Επειδή είναι χωρίς σύνδεση, το UDP έχει πολύ λίγα να κάνει. Ουσιαστικά, προσθέτει μία δυνατότητα διευθυνσιοδότησης θυρών στο IP. Η επικεφαλίδα περιλαμβάνει μία θύρα πηγής και μία θύρα προορισμού. Το πεδίο μήκους περιέχει το μήκος ολόκληρου του τεμαχίου UDP, περιλαμβάνοντας την επικεφαλίδα και τα δεδομένα. Το άθροισμα ελέγχου είναι ο

ίδιος αλγόριθμος που χρησιμοποιείται για το TCP και το IP. Για το UDP, το άθροισμα ελέγχου εφαρμόζεται σε ολόκληρο το τεμάχιο UDP κατά τη διάρκεια του υπολογισμού και η οποία είναι η ίδια η ψευδοεπικεφαλίδα που χρησιμοποιείται για το TCP. Εάν ανιχνευθεί ένα σφάλμα, το τεμάχιο απορρίπτεται και δε λαμβάνεται επιπλέον ενέργεια.

Το πεδίο αθροίσματος ελέγχου στο UDP είναι προαιρετικό. Εάν δε χρησιμοποιείται, τίθεται στο μηδέν. Ωστόσο, πρέπει να επισημανθεί ότι το άθροισμα ελέγχου IP εφαρμόζεται μόνο στη κεφαλίδα IP και όχι στο πεδίο δεδομένων, το οποίο σε αυτή τη περίπτωση αποτελείται από την επικεφαλίδα UDP και τα δεδομένα χρήστη. Έτσι, εάν δεν εκτελείται υπολογισμός αθροίσματος ελέγχου από το UDP, τότε δε γίνεται έλεγχος για τα δεδομένα χρήστη.

2.2 Μοντέλο αναφοράς OSI

Το μοντέλο αναφοράς OSI βασίζεται σε μια πρόταση που αναπτύχθηκε από το Διεθνή Οργανισμό Τυποποίησης ως ένα πρώτο βήμα για τη διεθνή τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα επίπεδα των δικτύων. Το μοντέλο αυτό ονομάζεται Μοντέλο Αναφοράς ISO OSI, όπου OSI σημαίνει Διασύνδεση Ανοικτών Συστημάτων, επειδή ασχολείται με τη διασύνδεση ανοικτών συστημάτων – δηλαδή συστημάτων που είναι ανοικτά στην επικοινωνία με άλλα συστήματα. Για λόγους συντομίας θα το λέμε απλά μοντέλο OSI.

Το μοντέλο OSI έχει επτά επίπεδα. Οι αρχές που εφαρμόστηκαν για να καταλήξουμε σε αυτά τα επτά επίπεδα μπορούν να συνοψιστούν ως εξής:

1. Όπου χρειάζεται μια διαφορετική λογική αφαίρεση πρέπει να δημιουργείται ένα επίπεδο.
2. Κάθε επίπεδο πρέπει να εκτελεί μια σαφώς καθορισμένη λειτουργία.
3. Η λειτουργία κάθε επιπέδου πρέπει να επιλέγεται με στόχο τον καθορισμό διεθνώς τυποποιημένων πρωτοκόλλων.
4. Τα σύνορα των επιπέδων πρέπει να επιλέγονται έτσι ώστε να ελαχιστοποιείται η ροή των πληροφοριών μέσω της διασύνδεσης των επιπέδων.
5. Το πλήθος των επιπέδων πρέπει να είναι αρκετά μεγάλο έτσι ώστε να μη χρειάζεται να ανακατεύονται χωρίς λόγο διαφορετικές λειτουργίες στο ίδιο επίπεδο, και ταυτόχρονα αρκετά μικρό έτσι ώστε η αρχιτεκτονική να μη γίνεται άβολη.

Στη συνέχεια παρατίθεται ένας πίνακας με τα επτά επίπεδα του OSI με μια σύντομη περιγραφή του κάθε επιπέδου.

Πίνακας 3.Τα επίπεδα του OSI

Εφαρμογών	
Παρέχει στους χρήστες πρόσβαση στο περιβάλλον του OSI, όπως επίσης κατανεμημένες υπηρεσίες πληροφόρησης.	

Παρουσίασης

Παρέχει ανεξαρτησία στις διαδικασίες της εφαρμογής από διαφορές στην αναπαράσταση (σύνταξη) των δεδομένων.

Συνδιάλεξης

Παρέχει τη δομή ελέγχου για επικοινωνία μεταξύ των εφαρμογών. Αποκαθιστά, διαχειρίζεται και τερματίζει συνδέσεις (συνδιαλέξεις) μεταξύ συνεργατικών εφαρμογών.

Μεταφοράς

Παρέχει αξιόπιστη, διαφανή μεταφορά δεδομένων μεταξύ τερματικών σημείων. Παρέχει από άκρο σε άκρο ανάκτηση από σφάλματα και έλεγχο ροής.

Δικτύου

Παρέχει ανεξαρτησία στα ανώτερα επίπεδα από τη μετάδοση δεδομένων και τις τεχνολογίες μεταγωγής που χρησιμοποιούνται για τη σύνδεση συστημάτων. Είναι υπεύθυνο για την αποκατάσταση, τη συντήρηση και τον τερματισμό συνδέσεων.

Συνδέσμου μετάδοσης δεδομένων

Παρέχει αξιόπιστη μεταφορά της πληροφορίας μέσω της φυσικής σύνδεσης. Στέλνει μπλοκ (πλαίσια) με τον απαραίτητο συγχρονισμό, έλεγχο σφαλμάτων και έλεγχο ροής.

Φυσικό

Σχετίζεται με τη μετάδοση μη δομημένης σειράς bit μέσω του φυσικού μέσου. Ασχολείται με τα μηχανικά, ηλεκτρικά, λειτουργικά και διαδικαστικά χαρακτηριστικά για την πρόσβαση στο φυσικό μέσο.

Θα εξετάσουμε παρακάτω λεπτομερέστερα κάθε επίπεδο του μοντέλου με τη σειρά, ξεκινώντας από το κατώτατο επίπεδο. Σημειώνουμε ότι το μοντέλο OSI δεν αποτελεί από μόνο του μια αρχιτεκτονική δικτύου, επειδή δεν προσδιορίζει τις ακριβείς υπηρεσίες και πρωτόκολλα που πρέπει να χρησιμοποιούνται σε κάθε επίπεδο. Το μοντέλο απλώς ορίζει τι πρέπει να κάνει το κάθε επίπεδο. Ο οργανισμός ISO έχει δημιουργήσει όμως και πρότυπα για όλα τα επίπεδα, αν και αυτά δεν αποτελούν μέρος του μοντέλου αναφοράς. Το καθένα από τα πρωτόκολλα αυτά έχει δημοσιευτεί ως ξεχωριστό διεθνές πρότυπο.

Το φυσικό επίπεδο

Το φυσικό επίπεδο ασχολείται με τη μετάδοση ανεπεξέργαστων δυαδικών ψηφίων μέσω ενός καναλιού επικοινωνίας. Τα ζητήματα σχεδίασης σχετίζονται με την εξασφάλιση του ότι, όταν η μία πλευρά στέλνει το bit 1, αυτό θα λαμβάνεται από την άλλη πλευρά ως bit 1 και όχι ως bit 0. Τυπικά ερωτήματα στο επίπεδο αυτό είναι πόσα Volt πρέπει να χρησιμοποιούνται για την αναπαράσταση του 1 και πόσα για το 0, πόσα νανοδευτερόλεπτα διαρκεί ένα bit, κατά πόσον θα μπορεί να γίνεται η μετάδοση ταυτόχρονα και προς τις δύο κατευθύνσεις, πώς εγκαθιδρύεται η αρχική σύνδεση και πώς τερματίζεται όταν τελειώσουν και οι δύο πλευρές, πόσους ακροδέκτες έχει ο συζευκτήρας του δικτύου και σε τι χρησιμεύει ο κάθε ακροδέκτης. Το φυσικό επίπεδο έχει τέσσερα σημαντικά χαρακτηριστικά:

- Μηχανικό: Σχετίζεται με τις φυσικές ιδιότητες της διεπαφής σε ένα μέσο μετάδοσης. Τυπικά, η προδιαγραφή είναι μια υποδοχή που ενώνει έναν ή περισσότερους αγωγούς σημάτων, που ονομάζονται κυκλώματα.
- Ηλεκτρικό: Σχετίζεται με την αναπαράσταση των bit (π.χ. σε σχέση με τα επίπεδα τάσης ρεύματος) και το ρυθμό μετάδοσης δεδομένων (bit).
- Λειτουργικό: Καθορίζει τις λειτουργίες που εκτελούνται από ανεξάρτητα κυκλώματα της φυσικής διεπαφής ανάμεσα σε ένα σύστημα και στο μέσο μετάδοσης.
- Διαδικαστικό: Καθορίζει την ακολουθία γεγονότων κατά τα οποία σειρές από bit ανταλλάσσονται μέσω ενός φυσικού μέσου.

Το επίπεδο συνδέσμου μετάδοσης δεδομένων

Το κύριο καθήκον του επιπέδου συνδέσμου μετάδοσης δεδομένων είναι να μετασχηματίζει μια υπηρεσία μετάδοσης ανεπεξέργαστων δεδομένων σε μια γραμμή η οποία να φαίνεται στο επίπεδο δικτύου ότι δεν έχει τον κίνδυνο μη εντοπισμένων σφαλμάτων μετάδοσης. Ο στόχος αυτός επιτυγχάνεται με το να βάζουμε τον αποστολέα να τεμαχίζει τα δεδομένα εισόδου σε πλαίσια δεδομένων (data frames) –

με τυπικό μέγεθος λίγες εκατοντάδες ή χιλιάδες byte – και να μεταδίδει τα πλαίσια με τη σειρά. Αν η υπηρεσία είναι αξιόπιστη, ο παραλήπτης επιβεβαιώνει την ορθή λήψη κάθε πλαισίου επιστρέφοντας ένα πλαίσιο επιβεβαίωσης (acknowledgment frame).

Ένα άλλο πρόβλημα που παρουσιάζεται στο επίπεδο συνδέσμου μετάδοσης δεδομένων (καθώς και στα περισσότερα ανώτερα επίπεδα) είναι το πώς μπορεί να αποτραπεί ένας γρήγορος αποστολέας από το να κατακλύσει με δεδομένα έναν αργό παραλήπτη. Συχνά απαιτείται κάποιος μηχανισμός ρύθμισης της κυκλοφορίας, έτσι ώστε ο αποστολέας να μαθαίνει πόσο χώρο προσωρινής αποθήκευσης διαθέτει ανά πάσα στιγμή ο παραλήπτης. Πολλές φορές οι μηχανισμοί ρύθμισης της κυκλοφορίας και διαχείρισης των σφαλμάτων είναι ενοποιημένοι.

Στα δίκτυα εκπομπής υπάρχει άλλο ένα ζήτημα στο επίπεδο συνδέσμου μετάδοσης δεδομένων: πώς θα ελέγχεται η πρόσβαση στο κοινόχρηστο κανάλι. Με αυτό το πρόβλημα ασχολείται ένα ειδικό υποεπίπεδο του συνδέσμου μετάδοσης δεδομένων, το υποεπίπεδο ελέγχου προσπέλασης μέσων.

Το επίπεδο δικτύου

Το επίπεδο δικτύου παρέχει υπηρεσίες για τη μεταφορά πληροφορίας ανάμεσα σε τερματικά συστήματα ενός τηλεπικοινωνιακού δικτύου. Απαλλάσσει τα υψηλότερα επίπεδα από την ανάγκη να γνωρίζουν οτιδήποτε σχετικά με την υποκείμενη μετάδοση δεδομένων και τις τεχνολογίες μεταγωγής που χρησιμοποιούνται για να συνδέουν συστήματα. Σε αυτό το επίπεδο ο υπολογιστής εμπλέκεται σε ένα διάλογο με το δίκτυο για να καθορίσει τη διεύθυνση προορισμού και να ζητήσει συγκεκριμένες υπηρεσίες δικτύου, όπως προτεραιότητα.

Ένα βασικό ζήτημα σχεδίασης είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την προέλευση προς τον προορισμό τους. Τα δρομολόγια μπορεί να βασίζονται σε στατικούς πίνακες οι οποίοι είναι ‘‘προσηλωμένοι’’ στο δίκτυο και μεταβάλλονται σπάνια. Μπορεί επίσης να προσδιορίζονται στην αρχή κάθε συνομιλίας – για παράδειγμα, στην αρχή μιας περιόδου εργασίας τερματικού (δηλαδή όταν πραγματοποιείται μια σύνδεση σε κάποια απομακρυσμένη μηχανή). Τέλος, μπορεί να είναι εντελώς δυναμικά, δηλαδή να καθορίζονται εκ νέου για κάθε πακέτο, έτσι ώστε να αντανακλούν το τρέχον φορτίο του δικτύου.

Αν υπάρχουν πάρα πολλά πακέτα στο υποδίκτυο την ίδια χρονική στιγμή, θα αρχίσουν να ‘‘παρεμποδίζουν’’ το ένα το άλλο, δημιουργώντας συμφόρηση. Ο έλεγχος της συμφόρησης ανήκει και αυτός στο επίπεδο δικτύου. Γενικότερα, η παρεχόμενη ποιότητα υπηρεσιών (καθυστέρηση, χρόνος διέλευσης, παραμόρφωση χρονισμού, κ.λ.π.) είναι επίσης θέμα του επίπεδου δικτύου.

Όταν ένα πακέτο πρέπει να ταξιδέψει από ένα δίκτυο σε κάποιο άλλο προκειμένου να φτάσει στον προορισμό του, μπορεί να εμφανιστούν πολλά προβλήματα. Η διευθυνσιοδότηση που χρησιμοποιείται από το δεύτερο δίκτυο μπορεί να διαφέρει από εκείνη του πρώτου. Το δεύτερο δίκτυο μπορεί να μη δεχτεί καθόλου το πακέτο, αν αυτό είναι πολύ μεγάλο. Μπορεί ακόμα να διαφέρουν τα πρωτόκολλα και ούτω καθεξής. Είναι θέμα του επιπέδου δικτύου να ξεπεράσει όλα αυτά τα προβλήματα, επιτρέποντας έτσι τη διασύνδεση ετερογενών δικτύων.

Υπάρχει ένα φάσμα από ενδιάμεσες υπηρεσίες επικοινωνιών που μπορεί να διαχειριστεί το επίπεδο δικτύου. Στην ακραία περίπτωση, όπου υπάρχει άμεση point-to-point σύνδεση ανάμεσα σε σταθμούς, μπορεί να μην υπάρχει η ανάγκη για επίπεδο δικτύου επειδή το επίπεδο συνδέσμου μετάδοσης δεδομένων μπορεί να εκτελέσει την αναγκαία λειτουργία της διαχείρισης της σύνδεσης.

Έπειτα τα συστήματα μπορεί να είναι συνδεδεμένα σε ένα δίκτυο μεταγωγής κυκλώματος ή ένα δίκτυο μεταγωγής πακέτου. Στην αρχιτεκτονική OSI τα τρία χαμηλότερα επίπεδα εμπλέκονται στη σύναψη και επικοινωνία με το δίκτυο. Τα πακέτα που δημιουργούνται από το τερματικό σύστημα μεταβιβάζονται μέσα από έναν ή περισσότερους κόμβους δικτύου που δρουν ως αναμεταδότες ανάμεσα σε δύο τερματικά συστήματα. Οι κόμβοι του δικτύου υλοποιούν τα επίπεδα 1 έως 3. Το στρώμα 3 στον κόμβο εκτελεί μία λειτουργία μεταγωγής και δρομολόγησης. Εσωτερικά στον κόμβο υπάρχουν δύο επίπεδα συνδέσμου μετάδοσης δεδομένων και δύο φυσικά επίπεδα, ανταποκρινόμενα στις συνδέσεις με τα δύο τερματικά συστήματα. Κάθε επίπεδο συνδέσμου μετάδοσης δεδομένων (και φυσικό) λειτουργεί ξεχωριστά για να παράσχει υπηρεσία στο επίπεδο δικτύου μέσω της αντίστοιχης σύνδεσης. Τα τέσσερα υψηλότερα επίπεδα είναι πρωτόκολλα ‘‘από-άκρο-σε-άκρο’’ (end-to-end) ανάμεσα στα συνδεδεμένα τερματικά συστήματα.

Στην άλλη ακραία περίπτωση δύο τερματικά συστήματα που επιθυμούν να επικοινωνήσουν μπορεί να μην είναι καν συνδεδεμένα στο ίδιο δίκτυο. Άντ’ αυτού, είναι συνδεδεμένα σε δίκτυα έτσι ώστε άμεσα ή έμμεσα είναι συνδεδεμένα το ένα με το άλλο. Αυτή η περίπτωση απαιτεί τη χρήση κάποιου είδους τεχνικής διαδικτύωσης.

Το επίπεδο μεταφοράς

Η βασική λειτουργία του επιπέδου μεταφοράς είναι να δέχεται δεδομένα από το ανώτερο επίπεδο, να τα διασπά αν χρειάζεται σε μικρότερες μονάδες να τα μεταβιβάζει στο επίπεδο δικτύου και να εξασφαλίζει ότι τα δεδομένα παραδίδονται απαλλαγμένα από σφάλματα, στη σωστή σειρά, χωρίς απώλειες ή πολλαπλά αντίγραφα. Επιπρόσθετα, όλα αυτά πρέπει να γίνονται με αποδοτικό τρόπο και έτσι ώστε να απομονώνονται τα ανώτερα επίπεδα από τις αναπόφευκτες τεχνολογικές αλλαγές που προκύπτουν στο χρησιμοποιούμενο υλικό.

Επιπλέον, το επίπεδο μεταφοράς καθορίζει τον τύπο της υπηρεσίας που θα παρέχεται στο επίπεδο συνδιάλεξης και, τελικά, στους χρήστες του δικτύου. Ο πιο δημοφιλής τύπος σύνδεσης στο επίπεδο μεταφοράς είναι ένα απαλλαγμένο από σφάλματα κανάλι από σημείο σε σημείο, το οποίο παραδίδει μηνύματα ή byte με τη σειρά που στάλθηκαν. Άλλα πιθανά είδη υπηρεσίας μεταφοράς είναι η μεταφορά μεμονωμένων μηνυμάτων χωρίς εγγυήσεις για τη σειρά μετάδοσής τους και η εκπομπή μηνυμάτων σε πολλαπλούς προορισμούς. Ο τύπος της υπηρεσίας καθορίζεται όταν εγκαθιδρύεται η σύνδεση.

Το επίπεδο μεταφοράς είναι ένα πραγματικό επίπεδο ‘‘απ’ άκρου εις άκρο’’ (end-to-end), δηλαδή από την προέλευση έως τον προορισμό. Με άλλα λόγια, ένα πρόγραμμα στη μηχανή προέλευσης πραγματοποιεί ‘‘συνομιλία’’ με ένα παρόμοιο πρόγραμμα στη μηχανή προορισμού, χρησιμοποιώντας τις κεφαλίδες των μηνυμάτων και τα μηνύματα ελέγχου. Στα κατώτερα επίπεδα τα πρωτόκολλα λειτουργούν

ανάμεσα σε κάθε μηχανή και τους άμεσους γείτονές της και όχι ανάμεσα στις ακραίες μηχανές προέλευσης και προορισμού όπου ενδιαμέσως μπορεί να υπάρχουν πολλοί δρομολογητές.

Το επίπεδο συνδιάλεξης

Τα τέσσερα χαμηλότερα επίπεδα του μοντέλου OSI παρέχουν τα μέσα για την αξιόπιστη ανταλλαγή των δεδομένων και μπορεί να παρέχουν διάφορες επιλογές ποιότητας υπηρεσίας. Για πολλές εφαρμογές η βασική υπηρεσία είναι ανεπαρκής. Για παράδειγμα, μία εφαρμογή απομακρυσμένης πρόσβασης τερματικού μπορεί να απαιτεί ημιαμφίδρομο (half-duplex) διάλογο. Μία εφαρμογή επεξεργασίας συναλλαγών μπορεί να απαιτεί σημεία ελέγχου στη ροή μεταφοράς δεδομένων που να επιτρέπουν τη δημιουργία αντιγράφων (backup) και ανάκτηση της πληροφορίας. Μία εφαρμογή επεξεργασίας μηνυμάτων μπορεί να απαιτεί την ικανότητα να διακόπτεται ένας διάλογος για να προετοιμαστεί ένα νέο μέρος ενός μηνύματος και αργότερα να συνεχιστεί ο διάλογος από το σημείο που διακόπηκε.

Όλες αυτές οι δυνατότητες θα μπορούσαν να ενσωματωθούν σε συγκεκριμένες εφαρμογές στο έβδομο επίπεδο. Ωστόσο, επειδή αυτοί οι τύποι εργαλείων δόμησης διαλόγου έχουν ευρεία εφαρμογή, είναι λογικό να τους οργανώσουμε σε ένα ξεχωριστό επίπεδο: το επίπεδο συνδιάλεξης.

Το επίπεδο συνδιάλεξης παρέχει το μηχανισμό για τον έλεγχο του διαλόγου ανάμεσα σε εφαρμογές και τερματικά συστήματα. Σε πολλές περιπτώσεις θα υπάρχει μικρή ή καθόλου ανάγκη για υπηρεσίες επιπέδου συνδιάλεξης, όμως σε μερικές εφαρμογές χρησιμοποιούνται τέτοιες υπηρεσίες. Οι κυριότερες υπηρεσίες που θα παρέχονται από το επίπεδο συνδιάλεξης περιλαμβάνουν τις ακόλουθες:

- Τρόπος διαλόγου: Αυτός μπορεί να είναι δύο κατευθύνσεων ταυτόχρονα (full-duplex) ή αμφίδρομος εναλλασσόμενος (half-duplex).
- Έλεγχος διαλόγου (dialog control): Η παρακολούθηση του ποιος έχει σειρά να μεταδώσει.
- Διαχείριση σκυτάλης (token management): Η αποτροπή των δύο πλευρών από το να επιχειρήσουν ταυτόχρονα την εκτέλεση της ίδιας κρίσιμης λειτουργίας.
- Ομαδοποίηση: Η ροή των δεδομένων μπορεί να σημειωθεί έτσι ώστε να καθορίζονται ομάδες δεδομένων. Για παράδειγμα, αν ένα κατάστημα λιανικής μεταδίδει δεδομένα πωλήσεων σε ένα περιφερειακό γραφείο, τα δεδομένα μπορεί να είναι σημειωμένα με στόχο να υποδεικνύουν το τέλος των δεδομένων πωλήσεων για κάθε τμήμα. Αυτό θα έδινε σήμα στον host υπολογιστή να σταματήσει να υπολογίζει το σύνολο γι’ αυτό το τμήμα και να αρχίσει να τρέχει νέο σύνολο για το επόμενο τμήμα.
- Ανάκτηση ή Συγχρονισμός: Το επίπεδο συνδιάλεξης μπορεί να παρέχει ένα μηχανισμό με σημεία ελέγχου έτσι ώστε, αν συμβεί κάποιου είδους βλάβη ανάμεσα στα σημεία ελέγχου η οντότητα συνδιάλεξης να μπορεί να αναμεταδώσει όλα τα δεδομένα από το τελευταίο σημείο ελέγχου.

Το επίπεδο παρουσίασης

Το επίπεδο παρουσίασης καθορίζει τη μορφή των δεδομένων που πρόκειται να ανταλλαγούν ανάμεσα στις εφαρμογές και προσφέρει στα προγράμματα εφαρμογών ένα σύνολο υπηρεσιών μετασχηματισμού δεδομένων. Το επίπεδο παρουσίασης καθορίζει τη σύνταξη που χρησιμοποιείται ανάμεσα στις οντότητες εφαρμογών και προνοεί για την επιλογή και ακολούθως την μετατροπή της αναπαράσταση που χρησιμοποιείται. Παραδείγματα συγκεκριμένων υπηρεσιών που μπορούν να εκτελεστούν σε αυτό το επίπεδο περιλαμβάνουν τη συμπίεση και τη κρυπτογράφηση δεδομένων.

Το επίπεδο εφαρμογών

Το επίπεδο εφαρμογών παρέχει το μέσο ώστε τα προγράμματα εφαρμογών να έχουν πρόσβαση στο περιβάλλον του OSI. Αυτό το επίπεδο περιλαμβάνει διαχειριστικές λειτουργίες, γενικά χρήσιμους μηχανισμούς για την υποστήριξη κατανεμημένων εφαρμογών και περιέχει μια ποικιλία πρωτοκόλλων που απαιτούνται συχνά από τους χρήστες. Ένα ευρέως χρησιμοποιούμενο πρωτόκολλο εφαρμογής είναι το Πρωτόκολλο Υπερ-κειμένου ή HTTP (HyperText Transfer Protocol), το οποίο είναι η βάση του Παγκόσμιου Ιστού. Όταν ένα πρόγραμμα φυλλομέτρησης (browser) χρειάζεται μια ιστοσελίδα, στέλνει το όνομα της επιθυμητής σελίδας στο διακομιστή χρησιμοποιώντας το πρωτόκολλο HTTP. Ο διακομιστής επιστρέφει στη συνέχεια τη σελίδα. Άλλα πρωτόκολλα εφαρμογών χρησιμοποιούνται για τη μεταφορά αρχείων, το ηλεκτρονικό ταχυδρομείο, τη πρόσβαση σε απομακρυσμένους υπολογιστές και τις ομάδες ειδήσεων δικτύου.

2.3 Σύγκριση των μοντέλων αναφοράς OSI και TCP/IP

Τα μοντέλα αναφοράς OSI και TCP/IP έχουν πολλά κοινά σημεία. Και τα δύο βασίζονται στην έννοια μιας στοίβας από ανεξάρτητα πρωτόκολλα. Επιπλέον, η λειτουργικότητα των επιπέδων είναι σε χονδρικές τιμές παρόμοια. Για παράδειγμα, και στα δύο μοντέλα τα επίπεδα μέχρι το επίπεδο μεταφοράς χρησιμεύουν στην παροχή μιας ανεξάρτητης από το δίκτυο υπηρεσίας μεταφοράς απ᾽ άκρου εις άκρο, για τις διεργασίες που επιθυμούν να επικοινωνήσουν. Τα επίπεδα αυτά αποτελούν τον παροχέα της υπηρεσίας μεταφοράς. Επιπλέον, και στα δύο μοντέλα τα επίπεδα που βρίσκονται πάνω από το επίπεδο μεταφοράς είναι χρήστες της υπηρεσίας μεταφοράς και είναι προσανατολισμένα προς τις εφαρμογές.

Παρά τις θεμελιώδεις αυτές ομοιότητες, τα δύο μοντέλα έχουν και πολλές διαφορές. Στην ενότητα αυτή θα εστιάσουμε στις βασικές διαφορές ανάμεσα στα δύο μοντέλα αναφοράς. Είναι σημαντικό να σημειώσουμε ότι εδώ συγκρίνουμε τα μοντέλα αναφοράς και όχι τις αντίστοιχες στοίβες πρωτοκόλλων.

Στο επίκεντρο του μοντέλου OSI βρίσκονται τρεις έννοιες:

1. Υπηρεσίες.
2. Διασυνδέσεις.
3. Πρωτόκολλα.

Η μεγαλύτερη συνεισφορά του μοντέλου OSI είναι πιθανότατα το ότι έκανε σαφή τη διάκριση ανάμεσα στις τρεις αυτές έννοιες. Κάθε επίπεδο υλοποιεί κάποιες υπηρεσίες για το επίπεδο που βρίσκεται πάνω από αυτό. Ο ορισμός της υπηρεσίας λέει τι κάνει το επίπεδο, όχι πώς γίνεται η προσπέλασή του από τα ανώτερα επίπεδα ή πως δουλεύει. Καθορίζει λοιπόν τη σημασιολογία του επιπέδου.

Η διασύνδεση ενός επιπέδου λέει στις διεργασίες που βρίσκονται πάνω από αυτό πώς να το προσπελάσουν. Προσδιορίζει ποιες είναι οι παράμετροι και ποια αποτελέσματα πρέπει να αναμένονται. Ούτε η διασύνδεση λέει τίποτα σχετικά με τον τρόπο εσωτερικής λειτουργίας του επιπέδου.

Τέλος, τα ομότιμα πρωτόκολλα που χρησιμοποιούνται σε ένα επίπεδο είναι δουλειά του επιπέδου και μόνο. Το επίπεδο μπορεί να χρησιμοποιήσει όποια πρωτόκολλα θέλει, αρκεί να κάνει τη δουλειά του (δηλαδή να παρέχει τις κατάλληλες υπηρεσίες). Μπορεί ακόμη να αλλάξει πρωτόκολλα κατά βούληση, χωρίς να επηρεάσει το λογισμικό στα ανώτερα επίπεδα.

Οι ιδέες αυτές ταιριάζουν απόλυτα στις σύγχρονες απόψεις του αντικειμενοστρεφούς προγραμματισμού. Ένα αντικείμενο, όπως και ένα επίπεδο, διαθέτει ένα σύνολο μεθόδων (πράξεων) τις οποίες μπορούν να καλέσουν οι διεργασίες που βρίσκονται εκτός του αντικειμένου. Η σημασιολογία αυτών των μεθόδων καθορίζει το σύνολο των υπηρεσιών που προσφέρονται από το αντικείμενο. Οι παράμετροι και τα αποτελέσματα των μεθόδων αποτελούν τη διασύνδεση του αντικειμένου. Ο κώδικας που βρίσκεται μέσα στο αντικείμενο είναι το πρωτόκολλό του και δεν είναι ορατός ούτε έχει κάποια σημασία έξω από το αντικείμενο.

Το μοντέλο TCP/IP αρχικά δεν έκανε σαφή διάκριση ανάμεσα στις υπηρεσίες, τις διασυνδέσεις και τα πρωτόκολλα, αν και κάποιοι προσπάθησαν να το μετασκευάσουν εκ των υστέρων για να το κάνουν να μοιάζει με το μοντέλο OSI. Για παράδειγμα, οι μόνες πραγματικές υπηρεσίες που παρέχονται από το επίπεδο διαδικτύου είναι οι ΑΠΟΣΤΟΛΗ ΠΑΚΕΤΟΥ IP (send IP packet) και ΛΗΨΗ ΠΑΚΕΤΟΥ IP (receive IP packet).

Κατά συνέπεια τα πρωτόκολλα στο μοντέλο OSI είναι ‘‘καλύτερα κρυμμένα’’ απ’ ότι στο μοντέλο TCP/IP και μπορούν να αντικατασταθούν σχετικά εύκολα όποτε αλλάζει η τεχνολογία. Η δυνατότητα πραγματοποίησης τέτοιων αλλαγών είναι ένας από τους βασικούς σκοπούς για τους οποίους δημιουργήθηκαν εξαρχής πρωτόκολλα δομημένα σε επίπεδα.

Το μοντέλο αναφοράς ISO επινοήθηκε πριν σχεδιαστούν τα αντίστοιχα πρωτόκολλα. Αυτή η χρονική διαδοχή σημαίνει ότι το μοντέλο δεν ήταν ‘‘προκατειλημμένο’’ υπέρ κάποιου συνόλου πρωτοκόλλων, γεγονός που έκανε το μοντέλο ιδιαίτερα γενικό. Το μειονέκτημα αυτής της χρονικής διαδοχής είναι ότι οι

σχεδιαστές δεν είχαν μεγάλη πείρα με το αντικείμενο, οπότε δεν είχαν και τόσο καλή ιδέα σχετικά με τις λειτουργίες που έπρεπε να βάλουν σε κάθε επίπεδο.

Για παράδειγμα, το επίπεδο συνδέσμου μετάδοσης δεδομένων αρχικά χειριζόταν μόνο δίκτυα από σημείο σε σημείο. Όταν εμφανίστηκαν τα δίκτυα εκπομπής, χρειάστηκε να προστεθεί πρόχειρα ένα καινούριο υποεπίπεδο στο μοντέλο. Όταν άρχισαν να κατασκευάζονται πραγματικά δίκτυα με βάση το μοντέλο OSI και τα υπάρχοντα πρωτόκολλα, ανακαλύφθηκε ότι τα δίκτυα αυτά δεν ικανοποιούσαν τις προδιαγραφές των υπηρεσιών, οπότε χρειάστηκε να προστεθούν υποεπίπεδα σύγκλισης στο μοντέλο ώστε να υπάρχει κάποιος τρόπος γεφύρωσης των διαφορών. Τέλος, η επιτροπή σχεδίασης αρχικά ανέμενε ότι κάθε χώρα θα έχει μόνο ένα δίκτυο, το οποίο θα λειτουργούσε με ευθύνη του κράτους και θα χρησιμοποιούσε τα πρωτόκολλα OSI, έτσι δεν υπήρχε πρόβλεψη για δικτύωση. Τα πράγματα όμως δεν εξελίχθηκαν έτσι.

Στο TCP/IP ίσχυε το αντίθετο: πρώτα εμφανίστηκαν τα πρωτόκολλα, ενώ το μοντέλο ήταν στην πραγματικότητα μια απλή περιγραφή των υπαρχόντων πρωτοκόλλων. Δεν υπήρχε πρόβλημα ταιριάσματος των πρωτοκόλλων με το μοντέλο. Το ταίριασμα ήταν τέλειο. Το μόνο πρόβλημα ήταν ότι το μοντέλο δεν ταίριαζε με οποιεσδήποτε άλλες στοίβες πρωτοκόλλων. Κατά συνέπεια, δεν ήταν ιδιαίτερα χρήσιμο για την περιγραφή άλλων δικτύων που δε βασίζονται στο TCP/IP.

Μια προφανής διαφορά ανάμεσα στα δύο μοντέλα είναι το πλήθος των επιπέδων: το μοντέλο OSI έχει επτά επίπεδα ενώ το TCP/IP έχει τέσσερα επίπεδα. Και τα δύο έχουν επίπεδα (δια)δικτύου, μεταφοράς και εφαρμογών, όμως τα άλλα επίπεδα είναι διαφορετικά.

Μια άλλη διαφορά είναι στο θέμα ασυνδεσμικής έναντι της συνδεσμοστραφούς επικοινωνίας. Το μοντέλο OSI υποστηρίζει και ασυνδεσμική και συνδεσμοστρεφή επικοινωνία στο επίπεδο δικτύου, αλλά υποστηρίζει μόνο συνδεσμοστρεφή επικοινωνία στο επίπεδο μεταφοράς, εκεί όπου έχει πραγματικά σημασία (αφού το επίπεδο μεταφοράς είναι ορατό στους χρήστες). Το μοντέλο TCP/IP έχει μόνο ένα τρόπο λειτουργίας στο επίπεδο δικτύου (ασυνδεσμικό) αλλά υποστηρίζει και τους δύο τρόπους λειτουργίας στο επίπεδο μεταφοράς, αφήνοντας την επιλογή στους χρήστες. Αυτή η επιλογή είναι ιδιαίτερα σημαντική για τα απλά πρωτόκολλα αίτησης-απάντησης.

2.4 Κριτική του μοντέλου αναφοράς TCP/IP

Το μοντέλο και τα πρωτόκολλα του TCP/IP έχουν τα προβλήματά τους. Καταρχήν, το μοντέλο δεν κάνει επαρκή διάκριση ανάμεσα στις έννοιες της υπηρεσίας, της διασύνδεσης και του πρωτοκόλλου. Οι ορθές πρακτικές κατασκευής λογισμικού απαιτούν τη διάκριση ανάμεσα στις προδιαγραφές και την υλοποίηση, όπως γίνεται πολύ προσεκτικά στο OSI αλλά όχι στο TCP/IP. Κατά συνέπεια, το μοντέλο TCP/IP δεν είναι και πολύ καλός οδηγός για τη σχεδίαση νέων δικτύων με χρήση νέων τεχνολογιών.

Δεύτερον, το μοντέλο TCP/IP δεν είναι καθόλου γενικό και είναι ακατάλληλο για την περιγραφή οποιασδήποτε στοίβας πρωτοκόλλων εκτός από αυτής του TCP/IP. Για παράδειγμα, το να προσπαθήσουμε να χρησιμοποιήσουμε το μοντέλο TCP/IP για να περιγράψουμε το Bluetooth είναι εντελώς αδύνατο.

Τρίτον, το επίπεδο διασύνδεσης μεταξύ υπολογιστή υπηρεσίας και δικτύου δεν είναι ‘‘πραγματικό επίπεδο’’ με τη συνηθισμένη έννοια του όρου, όπως αυτός χρησιμοποιείται στα πρωτόκολλα που δομούνται σε επίπεδα. Είναι μια διασύνδεση (ανάμεσα στα επίπεδα δικτύου και συνδέσμου μετάδοσης δεδομένων). Η διάκριση ανάμεσα στη διασύνδεση και το επίπεδο είναι κρίσιμη και δεν πρέπει να είμαστε πρόχειροι με τέτοια θέματα.

Τέταρτον, το μοντέλο TCP/IP δε διακρίνει (και ούτε καν αναφέρει) το φυσικό επίπεδο και το επίπεδο συνδέσμου μετάδοσης δεδομένων. Τα επίπεδα αυτά είναι εντελώς διαφορετικά. Το φυσικό επίπεδο ασχολείται με τα χαρακτηριστικά μετάδοσης των χάλκινων συρμάτων, των οπτικών ινών και των ασύρματων επικοινωνιών. Η δουλειά του επιπέδου συνδέσμου μετάδοσης δεδομένων είναι να οριοθετεί την αρχή και το τέλος των πλαισίων και να τα μεταφέρει από τη μια πλευρά στην άλλη με τον επιθυμητό βαθμό αξιοπιστίας. Ένα σωστό μοντέλο πρέπει να περιλαμβάνει χωριστά το κάθε ένα από αυτά τα επίπεδα. Το μοντέλο TCP/IP δεν κάνει κάτι τέτοιο.

Τέλος, αν και τα πρωτόκολλα IP και TCP σχεδιάστηκαν προσεκτικά και υλοποιήθηκαν καλά, πολλά από τα άλλα πρωτόκολλα ήταν προχειροφτιαγμένα και πολλές φορές υλοποιήθηκαν από ομάδες μεταπτυχιακών φοιτητών που τα τροποποιούσαν μέχρι να βαρεθούν. Οι υλοποιήσεις των πρωτοκόλλων αυτών στη συνέχεια διανέμονταν δωρεάν, γεγονός που οδήγησε στο να εδραιωθούν βαθιά και έτσι να είναι δύσκολο να αντικατασταθούν. Μερικά από αυτά είναι κάπως πιο ενοχλητικά. Για παράδειγμα, το πρωτόκολλο εικονικού τερματικού, το TELNET, σχεδιάστηκε για ένα μηχανικό τερματικό Teletype που εμφάνιζε δέκα χαρακτήρες ανά δευτερόλεπτο. Δε γνωρίζει τίποτα για τις διασυνδέσεις με το χρήστη μέσω γραφικών και τα ποντίκια. Ωστόσο, 25 χρόνια αργότερα, εξακολουθεί να χρησιμοποιείται ευρύτατα.

Συνοψίζοντας, παρά τα προβλήματά του, το μοντέλο OSI (εκτός από τα επίπεδα διασύνδεσης και παρουσίασης) έχει αποδειχθεί εξαιρετικά χρήσιμο για την ανάλυση των δικτύων υπολογιστών. Σε αντίθεση, τα πρωτόκολλα OSI δεν έχουν γίνει δημοφιλή. Το αντίστροφο ισχύει για το TCP/IP: το μοντέλο στη πράξη είναι ανύπαρκτο, αλλά τα πρωτόκολλα χρησιμοποιούνται ευρύτατα.

3 Φιλοσοφία του TCP

3.1 Στοιχεία του συστήματος Internetwork

Το περιβάλλον Internetwork αποτελείται από τους hosts που συνδέονται με τα δίκτυα που διασυνδέονται στη συνέχεια μέσω των πυλών.

Υποτίθεται εδώ ότι τα δίκτυα μπορούν να είναι είτε τοπικά δίκτυα (π.χ., το ETHERNET) είτε μεγάλα δίκτυα (π.χ., ARPANET), αλλά σε κάθε περίπτωση είναι βασισμένα στην τεχνολογία εναλλακτικής μετάδοσης πακέτου πληροφοριών. Οι ενεργοί πράκτορες που παράγουν και καταναλώνουν τα μηνύματα είναι διεργασίες. Τα διάφορα επίπεδα πρωτοκόλλων στα δίκτυα, τις πύλες, και τους hosts υποστηρίζουν ένα interprocess σύστημα επικοινωνιών που παρέχει τη διπλής κατεύθυνσης ροή στοιχείων στις λογικές συνδέσεις μεταξύ των ports διεργασίας.

Ο όρος πακέτου χρησιμοποιείται γενικά εδώ για να σημάνει τα δεδομένα μιας συναλλαγής μεταξύ ενός host και ενός δικτύου του.

Το σχήμα των φραγμών στοιχείων που ανταλλάσσονται μέσα σε ένα δίκτυο γενικά δεν θα είναι υπόθεση μας. Οι hosts είναι υπολογιστές που συνδέονται με ένα δίκτυο, και από την άποψη του δικτύου επικοινωνίας, είναι οι πηγές και οι προορισμοί των πακέτων. Οι διεργασίες αντιμετωπίζονται ως ενεργά δεδομένα στους hosts υπολογιστές (σύμφωνα με τον αρκετά κοινό καθορισμό μιας διεργασίας ως πρόγραμμα στην εκτέλεση). Ακόμη και τα τερματικά και τα αρχεία ή άλλες I/O συσκευές αντιμετωπίζονται σαν να επικοινωνούν το ένα με το άλλο μέσω της χρήσης των διεργασιών. Κατά συνέπεια, όλη η επικοινωνία αντιμετωπίζεται ως inter-process επικοινωνία.

Δεδομένου ότι μια διεργασία μπορεί να χρειάζεται να διακρίνει μεταξύ διάφορων καναλιών επικοινωνίας μεταξύ της ίδιας και μιας άλλης διεργασίας (ή των διεργασιών), φανταζόμαστε ότι κάθε διεργασία μπορεί να έχει διάφορα ports μέσω των οποίων επικοινωνεί με τα ports άλλων διεργασιών.

3.2 Μοντέλο λειτουργίας

Οι διεργασίες διαβιβάζουν τα στοιχεία καλώντας το TCP και διαβάζοντας τους buffers των στοιχείων ως επιχειρήματα.

Το TCP συσκευάζει τα στοιχεία από αυτούς τους buffers σε τμήματα και καλεί την ενότητα Διαδικτύου για να διαβιβάσει κάθε τμήμα στο TCP προορισμού. Το λαμβάνον TCP τοποθετεί τα στοιχεία από ένα τμήμα στον buffer του λαμβάνοντα χρήστη και ειδοποιεί το λαμβάνοντα χρήστη. Τα TCPs περιλαμβάνουν τις πληροφορίες ελέγχου στα τμήματα που χρησιμοποιούν για να εξασφαλίσουν αξιόπιστη διαταγμένη μετάδοση στοιχείων. Το πρότυπο της επικοινωνίας Διαδικτύου

είναι ότι υπάρχει μια ενότητα πρωτοκόλλου Διαδικτύου που συνδέεται με κάθε TCP που παρέχει μια διεπαφή στο τοπικό δίκτυο.

Αυτά τα πακέτα τμημάτων TCP του Internet εισάγουν διαγράμματα δεδομένων και τα δρομολογούν σε ένα προορισμό στο Internet ή μια ενδιάμεση πύλη.

Για να διαβιβαστεί το διάγραμμα δεδομένων μέσω του τοπικού δικτύου, ενσωματώνεται σε ένα τοπικό πακέτο δικτύων. Οι διακόπτες πακέτων μπορούν να εκτελέσουν τον τεμαχισμό, η άλλες διεργασίες για να επιτύχουν την παράδοση του τοπικού πακέτου στην ενότητα Διαδικτύου προορισμού.

Σε μια πύλη μεταξύ των δικτύων, το διάγραμμα δεδομένων Διαδικτύου είναι "ξετυλιγμένο" από το τοπικό πακέτο του και εξετάζεται για να καθοριστεί μέσω ποιου δικτύου το διάγραμμα δεδομένων Διαδικτύου πρέπει να ταξιδέψει έπειτα. Το διάγραμμα δεδομένων Διαδικτύου είναι έπειτα "τυλιγμένο" σε ένα τοπικό πακέτο κατάλληλο στο επόμενο δίκτυο και καθοδηγούμενο προς την επόμενη πύλη, ή τον τελικό προορισμό.

Μια πύλη επιτρέπεται να χωρίσει ένα διάγραμμα δεδομένων Διαδικτύου σε μικρότερα τεμάχια διαγραμμάτων δεδομένων Διαδικτύου εάν αυτό είναι απαραίτητο για τη μετάδοση μέσω του επόμενου δικτύου. Για να το κάνει αυτό, η πύλη παράγει ένα σύνολο διαγραμμάτων δεδομένων Διαδικτύου, κάθε ένα από τα οποία φέρει ένα τεμάχιο. Τα τεμάχια μπορούν να σπάσουν περαιτέρω σε μικρότερα τεμάχια στις επόμενες πύλες. Το σχήμα τεμαχίων των διαγραμμάτων δεδομένων Διαδικτύου σχεδιάζεται έτσι ώστε η ενότητα Διαδικτύου προορισμού να μπορεί να συγκεντρώσει εκ νέου τα τεμάχια στα διαγράμματα δεδομένων Διαδικτύου. Μια ενότητα Διαδικτύου προορισμού ξετυλίγει το τμήμα από το διάγραμμα δεδομένων (μετά από την εκ νέου συγκέντρωση του διαγράμματος δεδομένων, εάν είναι απαραίτητο) και το περνά στο TCP προορισμού.

Αυτό το απλό πρότυπο της λειτουργίας παρουσιάζει πολλές λεπτομέρειες. Ένα σημαντικό χαρακτηριστικό γνώρισμα είναι ο τύπος υπηρεσίας. Παρέχει τις πληροφορίες στην πύλη (ή την ενότητα Διαδικτύου) που οδηγούν στην επιλογή των παραμέτρων υπηρεσιών που χρησιμοποιούνται για να διασχίσει το επόμενο δίκτυο. Συμπεριλαμβανόμενες στον τύπο υπηρεσίας, οι πληροφορίες είναι η προτεραιότητα του διαγράμματος δεδομένων. Τα διαγράμματα δεδομένων μπορούν επίσης να φέρουν τις πληροφορίες ασφάλειας για να επιτρέψουν τον host και τις πύλες που λειτουργούν στα πολλαπλής στάθμης ασφαλή περιβάλλοντα να διαχωρίσουν κατάλληλα τα διαγράμματα δεδομένων για τις εκτιμήσεις ασφάλειας.

3.3 Περιβάλλον

Το TCP υποτίθεται ότι είναι μια ενότητα σε ένα λειτουργικό σύστημα .Οι χρήστες έχουν πρόσβαση στο TCP όπως θα είχαν πρόσβαση στο σύστημα αρχείων. Το TCP μπορεί να καλέσει άλλες λειτουργίες λειτουργικών συστημάτων, παραδείγματος χάριν, για να διαχειριστεί τις δομές δεδομένων. Η πραγματική διεπαφή στο δίκτυο υποτίθεται ότι ελέγχεται από μια ενότητα οδηγών συσκευών. Το TCP δεν καλεί τον οδηγό συσκευών δικτύων άμεσα, αλλά μάλλον καλεί την ενότητα πρωτοκόλλου διαγραμμάτων δεδομένων Διαδικτύου που μπορεί στη συνέχεια να καλέσει τον οδηγό

συσκευών. Οι μηχανισμοί του TCP δεν αποκλείουν την εφαρμογή του TCP σε έναν front-end επεξεργαστή. Εντούτοις, σε μια τέτοια εφαρμογή, ένα πρωτόκολλο host-to-front-end πρέπει να παρέχει τη λειτουργία για να υποστηρίξει τον τύπο διεπαφής TCP- χρήστη που περιγράφεται στο παρόν έγγραφο.

3.4 Διεπαφές

Η διεπαφή TCP-χρήστη παρέχει για τις κλήσεις που γίνονται από το χρήστη στο TCP για άνοιγμα η κλείσιμο μιας σύνδεσης, για ΝΑ ΣΤΕΙΛΕΙ ή ΝΑ ΛΑΒΕΙ δεδομένα, η για να λάβει την ΚΑΤΑΣΤΑΣΗ για μια σύνδεση. Αυτές οι κλήσεις είναι όπως άλλες κλήσεις από τα προγράμματα χρηστών στο λειτουργικό σύστημα, παραδείγματος χάριν, οι κλήσεις για άνοιγμα αρχείου, διάβασμα από ένα αρχείο, και κλείσιμο ενός αρχείου. Η διεπαφή Διαδικτύου TCP παρέχει τις κλήσεις για να στείλει και να λάβει τα διαγράμματα δεδομένων που απευθύνονται στις ενότητες TCP στους hosts οπουδήποτε στο σύστημα Διαδικτύου. Αυτές οι κλήσεις έχουν τις παραμέτρους για τη διαβίβαση της διεύθυνσης, του τύπου υπηρεσίας, της προτεραιότητας, της ασφάλειας, και άλλων πληροφοριών ελέγχου.

3.5 Αξιόπιστη επικοινωνία

Ένα κανάλι στοιχείων που στέλνονται σε μια σύνδεση TCP παραδίδεται αξιόπιστα και διατεταγμένα για τον προορισμό. Η μετάδοση γίνεται αξιόπιστη μέσω της χρήσης των αριθμών ακολουθίας και των acknowledgments (επιβεβαίωση λήψης). Εννοιολογικά, κάθε octet των στοιχείων προσδιορίζεται από έναν αριθμό ακολουθίας. Ο αριθμός ακολουθίας του πρώτου octet των στοιχείων σε ένα τμήμα διαβιβάζεται με εκείνο το τμήμα και καλείται αριθμός ακολουθίας τμήματος. Τα τμήματα φέρουν επίσης έναν αριθμό αναγνώρισης που είναι ο αριθμός ακολουθίας των επόμενων αναμενόμενων στοιχείων octet των μεταδόσεων στην αντίστροφη κατεύθυνση. Όταν το TCP διαβιβάζει ένα τμήμα που περιέχει τα στοιχεία, βάζει ένα αντίγραφο σε μια σειρά αναμονής αναμετάδοσης και αρχίζει ένα χρονόμετρο. Όταν η επιβεβαίωση λήψης για εκείνο το στοιχείο παραλαμβάνεται, το τμήμα διαγράφεται από τη σειρά αναμονής. Εάν η επιβεβαίωση λήψης δεν παραληφθεί πριν από την εκπνοή του χρόνου του χρονομέτρου, το τμήμα αναμεταδίδεται. Μια επιβεβαίωση λήψης από το TCP δεν εγγυάται ότι το στοιχείο έχει παραδοθεί στον τελικό χρήστη, αλλά μόνο ότι το λαμβάνον TCP έχει πάρει την ευθύνη να το κάνει αυτό. Για να διαχειριστεί τη ροή των στοιχείων μεταξύ TCPs, υιοθετείται ένας μηχανισμός ελέγχου ροής. Το λαμβάνον TCP εκθέτει ένα "παράθυρο" στο TCP αποστολής. Αυτό το παράθυρο διευκρινίζει τον αριθμό octets, αρχίζοντας από τον αριθμό αναγνώρισης, τον οποίο το λαμβάνον TCP είναι αυτήν την περίοδο έτοιμο να λάβει.

3.6 Μετάδοση στοιχείων

Τα στοιχεία που ρέουν σε μια σύνδεση μπορούν να θεωρηθούν ως κανάλι των octets. Ο αποστέλλων χρήστης δείχνει σε κάθε κλήση SEND εάν τα στοιχεία σε εκείνη την κλήση (και οποιεσδήποτε preceeding κλήσεις) πρέπει να ωθηθούν κατευθείαν στο λαμβάνοντα χρήστη με τη ρύθμιση της PUSH FLAG. Ένα TCP αποστολής επιτρέπεται να συλλέξει τα στοιχεία από τον αποστέλλοντα χρήστη και να στείλει αυτά τα στοιχεία ως τμήματα για μεγαλύτερη ευκολία, έως ότου επισημανθεί η λειτουργία ώθησης. Κατόπιν αυτού πρέπει να σταλούν όλα τα unsent στοιχεία(τα στοιχεία που δεν έχουν σταλεί ακόμα). Όταν ένα λαμβάνον TCP βλέπει τη push flag, δεν πρέπει να περιμένει περισσότερα στοιχεία από το TCP αποστολής πριν περαστούν τα στοιχεία στη λαμβάνουσα διεργασία. Δεν υπάρχει καμία υποχρεωτική σχέση μεταξύ των λειτουργιών ώθησης και των ορίων τμήματος. Τα στοιχεία σε οποιοδήποτε ιδιαίτερο τμήμα μπορούν να είναι το αποτέλεσμα μιας μοναδικής κλήσης SEND ή πολλαπλών κλήσεων SEND. Ο σκοπός της λειτουργίας ώθησης και της PUSH FLAG είναι να ωθηθούν τα στοιχεία κατευθείαν από τον αποστέλλοντα χρήστη στο λαμβάνοντα χρήστη. Δεν παρέχεται υπηρεσία αρχείων. Υπάρχει μια σύζευξη μεταξύ της λειτουργίας ώθησης και της χρήσης των buffers των στοιχείων που διασχίζουν τη διεπαφή TCP/ χρήστη. Κάθε φορά που συνδέεται μια PUSH FLAG με τα στοιχεία που τοποθετούνται στο λαμβάνοντα buffer του χρήστη, ο buffer επιστρέφεται στο χρήστη για επεξεργασία ακόμα κι αν δεν έχει γεμίσει. Εάν το στοιχείο φθάνει και υπάρχει αφθονία στον buffer του χρήστη, προτού να φανεί μια PUSH, περνά στις μονάδες μεγέθους buffers.

Το TCP παρέχει επίσης μέσα για τη διαβίβαση των δεδομένων στο δέκτη που σε κάποιο σημείο στα δεδομένα, στο κανάλι από το οποίο ο δέκτης διαβάζει αυτή την περίοδο υπάρχει επείγον δεδομένο. Το TCP δεν προσπαθεί να καθορίσει τι κάνει ο χρήστης συγκεκριμένα για τα εκκρεμή επείγοντα δεδομένα, αλλά η γενική έννοια είναι ότι η λαμβάνουσα διεργασία παίρνει μέτρα για να υποβληθούν σε επεξεργασία τα επείγοντα δεδομένα γρήγορα.

3.7 Καθιέρωση και κλείσιμο σύνδεσης

Για να αναγνωρίσει τα χωριστά κανάλια στοιχείων που ένα TCP μπορεί να χειριστεί, το TCP παρέχει έναν αναγνωριστή ports.Δεδομένου ότι οι αναγνωριστές των ports επιλέγονται ανεξάρτητα από κάθε TCP, δεν μπορούν να είναι μοναδικοί. Για να παρέχουμε τις μοναδικές διευθύνσεις μέσα σε κάθε TCP, συνδέουμε μια διεύθυνση Διαδικτύου που προσδιορίζει το TCP με έναν αναγνωριστή ports για να δημιουργήσουμε μια socket που θα είναι μοναδική σε όλα τα δίκτυα που συνδέονται. Μια σύνδεση καθορίζεται πλήρως από το ζευγάρι των sockets στις άκρες. Μια τοπική socket μπορεί να συμμετέχει σε πολλές συνδέσεις στις διαφορετικές ξένες sockets. Μια σύνδεση μπορεί να χρησιμοποιηθεί για να μεταφέρει τα δεδομένα και στις δύο κατευθύνσεις, δηλαδή είναι "full duplex".

Τα TCPs είναι ελεύθερα να συνδέσουν τα ports με τις διεργασίες με οποιοδήποτε τρόπο επιλέξουν. Εντούτοις, διάφορες βασικές έννοιες είναι απαραίτητες σε οποιαδήποτε εφαρμογή. Πρέπει να υπάρξουν γνωστά sockets που το TCP συνδέει μόνο με τις "κατάλληλες" διεργασίες με μερικά μέσα. Προβλέπουμε ότι οι διεργασίες μπορούν "να είναι κύριοι" κάποιων ports, και ότι οι διεργασίες μπορούν να αρχίσουν τις συνδέσεις μόνο στους ports αυτούς που κατέχουν. (Τα μέσα για την ιδιοκτησία είναι ένα τοπικό ζήτημα, αλλά προβλέπουμε μια εντολή χρήστη αιτήματος port , ή μια μέθοδο μοναδικής κατανομής ομάδας ports σε μια δεδομένη διεργασία, π.χ., με την ένωση κομματιών υψηλής διαταγής ενός ονόματος port με μια δεδομένη διεργασία.)

Μια σύνδεση προσδιορίζεται στην κλήση OPEN από το τοπικό port και τα ξένα sockets. Σε αντάλλαγμα, το TCP παρέχει ένα (σύντομο) τοπικό όνομα σύνδεσης με το οποίο ο χρήστης αναφέρεται στη σύνδεση στις επόμενες κλήσεις. Υπάρχουν διάφορα πράγματα που πρέπει να αναφερθούν για μια σύνδεση. Για να αποθηκεύσουμε αυτές τις πληροφορίες φανταζόμαστε ότι υπάρχει μια δομή δεδομένων αποκαλούμενη φραγμό (μπλοκ) ελέγχου μετάδοσης (tcb). Μια στρατηγική εφαρμογής θα είχε το όνομα τοπικής σύνδεσης σαν δείκτη στο tcb για αυτήν την σύνδεση. Η κλήση OPEN επίσης καθορίζει εάν η εγκαθίδρυση σύνδεσης πρόκειται να ακολουθηθεί ενεργά, ή να αναμένει παθητικά.

Ένα παθητικό αίτημα OPEN σημαίνει ότι η διεργασία προτιμά να δεχτεί τα εισερχόμενα αιτήματα σύνδεσης παρά την προσπάθεια να ξεκινήσει μια σύνδεση. Συχνά η διεργασία που ζητά ένα παθητικό OPEN θα δεχτεί ένα αίτημα σύνδεσης από οποιοδήποτε επισκέπτη. Σε αυτήν την περίπτωση χρησιμοποιείται ένα ξένο socket όλων των μηδενικών για να δηλώσει μια απροσδιόριστη socket. Οι απροσδιόριστες ξένες sockets επιτρέπονται μόνο σε παθητικά OPENs. Μια διεργασία υπηρεσιών που επιθυμεί να παρέχει τις υπηρεσίες για άλλες άγνωστες διεργασίες θα εκδίδει ένα παθητικό αίτημα OPEN με μια απροσδιόριστη ξένη socket. Κατόπιν θα μπορούσε να γίνει μια σύνδεση με οποιαδήποτε διεργασία που ζήτησε σύνδεση σε αυτήν την τοπική socket. Θα βοηθούσε εάν αυτή η τοπική socket ήταν γνωστή για να συνδεθεί με αυτήν την υπηρεσία.

Οι γνώστες sockets είναι ένας κατάλληλος μηχανισμός για a priori σύνδεση μιας διεύθυνσης socket με μια τυποποιημένη υπηρεσία. Παραδείγματος χάριν, η διεργασία "Telnet-Server"είναι μόνιμα ορισμένη σε μια ειδική socket, και άλλες sockets προορίζονται για τη μεταφορά αρχείων, πρόσβαση τερματικού σε απομακρυσμένους υπολογιστές, τη γεννήτρια κειμένων, Echoer, και τις sink processes (τα τελευταία τρία είναι για δοκιμαστικούς λόγους). Μια διεύθυνση socket μπορεί να διατηρηθεί για την πρόσβαση σε μια "Look-Up" υπηρεσία, η οποία θα επέστρεφε τη συγκεκριμένη socket εκεί οπού μια πρόσφατα δημιουργημένη υπηρεσία θα παρεχόταν. Η έννοια μιας γνωστής sockets είναι μέρος της προδιαγραφής TCP, αλλά η ανάθεση των sockets στις υπηρεσίες είναι έξω από αυτήν την προδιαγραφή.

Οι διεργασίες μπορούν να εκδώσουν ενεργητικά OPENs από άλλες διεργασίες και να ενημερωθούν από το TCP όταν καθιερωθούν οι συνδέσεις. Δύο διεργασίες που διανέμουν ενεργά OPENs η μια στην άλλη συγχρόνως θα συνδεθούν σωστά. Αυτή η ευελιξία είναι κρίσιμη για την υποστήριξη του διανεμημένου υπολογισμού οπού οι συνιστώσες ενεργούν ασύγχρονα ο ένας όσον αφορά τον άλλον.

Υπάρχουν δυο κύριες περιπτώσεις για το ταίριασμα sockets στα τοπικά παθητικά OPENs και ξένα ενεργά OPENs. Στην πρώτη περίπτωση, το τοπικά παθητικό OPEN έχει διευκρινίσει πλήρως την ξένη socket. Σε αυτήν την περίπτωση,

η αντιστοιχία πρέπει να είναι ακριβής. Στη δεύτερη περίπτωση, το τοπικό παθητικό OPENs έχει αφήσει την ξένη socket απροσδιόριστη. Σε αυτήν την περίπτωση, οποιαδήποτε ξένη socket είναι αποδεκτή εφ' όσον ταιριάζουν οι τοπικές sockets. Άλλες δυνατότητες περιλαμβάνουν τις μερικώς περιορισμένες αντιστοιχίες.

Εάν υπάρχουν διάφορα εκκρεμή παθητικά OPENs (που καταγράφονται σε TCPs) με την ίδια τοπική socket, ένα ξένο ενεργό OPEN θα αντιστοιχηθεί σε ένα tcb με τη συγκεκριμένη ξένη socket στο ξένο ενεργό OPEN, εάν ένα τέτοιο tcb υπάρξει , πριν επιλεγεί tcb με μια απροσδιόριστη ξένη socket. Οι διεργασίες για να εγκαταστήσουν τις συνδέσεις χρησιμοποιούν τη συγχρονισμένη σημαία ελέγχου (SYN) και περιλαμβάνουν μια ανταλλαγή τριών μηνυμάτων. Αυτή η ανταλλαγή έχει διάρκεια όσο ένα three-way hand shake.

Μια σύνδεση αρχίζει από τα ‘ραντεβού’ άφιξης ενός τμήματος που περιέχει ένα SYN και μια waiting tcb είσοδο που καθεμία δημιουργείται από μια εντολή χρήστη OPEN. Το ταίριασμα των τοπικών και ξένων sockets καθορίζει πότε μια σύνδεση έχει αρχίσει. Η σύνδεση εγκαθιδρύεται όταν συγχρονιστούν οι αριθμοί ακολουθίας και στις δύο κατευθύνσεις. Το κλείσιμο μιας σύνδεσης περιλαμβάνει επίσης την ανταλλαγή των τμημάτων, φέρνοντας σε αυτήν την περίπτωση τη σημαία ελέγχου FIN.

3.8 Προτεραιότητα και ασφάλεια

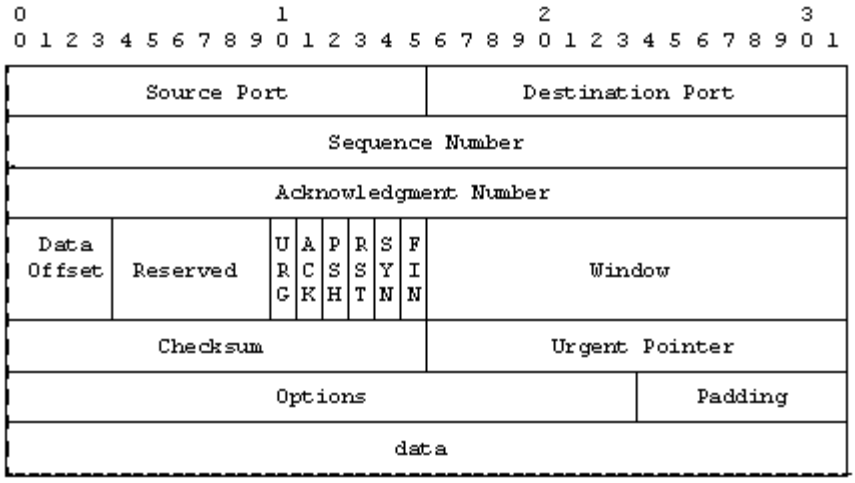
Το TCP χρησιμοποιεί τον τύπο πρωτοκόλλου Διαδικτύου τομέα υπηρεσιών και επιλογής ασφάλειας για να παρασχεθεί η προτεραιότητα και η ασφάλεια ανά βάση σύνδεσης στους χρήστες TCP. Δεν λειτουργούν απαραιτήτως όλες οι ενότητες TCP σε ένα πολλαπλής στάθμης ασφαλές περιβάλλον. Μερικές μπορούν να περιοριστούν μόνο στην αταξινόμητη χρήση και άλλες μπορούν να λειτουργήσουν μόνο σε ένα επίπεδο και διαμέρισμα ασφάλειας. Συνεπώς, μερικές εφαρμογές TCP και υπηρεσίες μπορούν να περιοριστούν σε ένα υποσύνολο της πολλαπλής στάθμης ασφαλούς περίπτωσης. Οι ενότητες TCP που λειτουργούν σε ένα πολλαπλής στάθμης ασφαλές περιβάλλον πρέπει να χαρακτηρίσουν κατάλληλα τα εξερχόμενα τμήματα, ανάλογα με την ασφάλεια, το διαμέρισμα, και την προτεραιότητα. Τέτοιες ενότητες TCP πρέπει επίσης να παρέχουν στους χρήστες ή τα πρωτόκολλα πιο υψηλού επιπέδου όπως Telnet ή THP, μια διεπαφή που τους επιτρέπει να διευκρινίσουν το επιθυμητό επίπεδο όσον αφορά το διαμέρισμα, την προτεραιότητα και ασφάλεια των συνδέσεων.

4 Λειτουργική Προδιαγραφή

4.1 Σχήμα επιγραφών - Κεφαλίδα

Τα τμήματα TCP στέλνονται ως διαγράμματα δεδομένων Διαδικτύου. Η κεφαλίδα του πρωτοκόλλου Διαδικτύου φέρει διάφορους τομείς πληροφοριών, συμπεριλαμβανομένων των πηγών και του προορισμού των διευθύνσεων του host. Μια κεφαλίδα TCP ακολουθεί την κεφαλίδα Διαδικτύου, που παρέχει πληροφορίες συγκεκριμένα στο πρωτόκολλο TCP. Αυτός ο διαχωρισμός επιτρέπει την ύπαρξη των επιπέδων των host πρωτοκόλλων εκτός από το TCP.

Πίνακας 4.Σχήμα επιγραφών TCP



Port πηγής: 16 bits

Ο αριθμός port πηγής.

Port προορισμού: 16 bits

Ο αριθμός port προορισμού.

Αριθμός ακολουθίας : 32 bits

Ο αριθμός ακολουθίας του πρώτου octet των δεδομένων σε αυτό το τμήμα (εκτός όταν το SYN είναι παρόν). Εάν το SYN είναι παρόν ο αριθμός ακολουθίας είναι ο αρχικός αριθμός ακολουθίας (ISN) και τα πρώτα octet δεδομένων είναι ISN+1.

Αριθμός αναγνώρισης :32 bits

Εάν το bit ελέγχου ACK τίθεται, αυτός ο τομέας περιέχει την τιμή του επόμενου αριθμού ακολουθίας που ο αποστολέας του τμήματος αναμένει να λάβει. Μόλις καθιερωθεί μια σύνδεση αυτό στέλνεται πάντα.

Data Offset: 4 bits

Ο αριθμός των 32 bits λέξεων στην κεφαλίδα TCP. Αυτό δείχνει από που αρχίζουν τα στοιχεία. Η κεφαλίδα TCP (ακόμη και των συμπεριλαμβανομένων επιλογών) είναι ένας ακέραιος αριθμός μήκους 32 bits.

Διατηρημένα : 6 bits

Διατηρημένα για μελλοντική χρήση. Πρέπει να είναι μηδέν.

Bits ελέγχου: 6 bits (από αριστερά προς τα δεξιά):

URG: Πεδίο επείγων δεικτών σημαντικό

ACK: Πεδίο αναγνώρισης σημαντικό

PSH: Συνάρτηση push

RST: Επανεκκίνηση σύνδεσης

SYN: Συγχρονισμός αριθμών ακολουθίας

FIN: Όχι άλλα στοιχεία από τον αποστολέα

Window: 16 bits

Ο αριθμός των 8 στοιχείων, που αρχίζουν με αυτό που υποδεικνύεται στο πεδίο αναγνώρισης όπου ο αποστολέας αυτού του τμήματος είναι πρόθυμος να δεχτεί.

Checksum: 16 bits

Το πεδίο checksum είναι το 16 bit συμπλήρωμα ως προς ένα του αθροίσματος όλων των λέξεων 16 bit στην κεφαλίδα και στο κείμενο. Εάν ένα τμήμα περιέχει έναν περιττό αριθμό κεφαλίδας και κειμένου των octets για να είναι checksummed, το τελευταίο octet είναι γεμισμένη από δεξιά με μηδενικά για να διαμορφωθεί μια λέξη 16 bit για checksum λόγους. Το pad δεν διαβιβάζεται ως κομμάτι του τμήματος. Υπολογίζοντας το checksum, ο ίδιος ο checksum τομέας αντικαθίσταται με μηδενικά.

Το ckecksum καλύπτει επίσης μια ψευδο-κεφαλίδα 96 bits που προτάσσεται εννοιολογικά στην κεφαλίδα TCP. Αυτή η ψευδο-κεφαλίδα περιέχει τη διεύθυνση πηγής, τη διεύθυνση προορισμού, το πρωτόκολλο, και το μήκος του TCP. Αυτό δίνει προστασία στο TCP ενάντια στην πιθανότητα κάποια τμήματα να χαθούν. Αυτές οι πληροφορίες φέρονται στο πρωτόκολλο Διαδικτύου και μεταφέρονται πέρα από το TCP/ διεπαφή δικτύων στα επιχειρήματα ή τα αποτελέσματα των κλήσεων από το TCP για την IP.

Πίνακας 5.

Source Address		
Destination Address		
zero	PTCL	TCP Length

Το μήκος του TCP είναι το μήκος της κεφαλίδας TCP συν το μήκος των δεδομένων του octet (αυτό δεν είναι μια ρητά διαβιβασθείσα ποσότητα, αλλά υπολογίζεται), και δε μετρά τις 12 octets της ψευδο-κεφαλίδας.

Επείγων δείκτης :16 bits

Αυτός ο τομέας επικοινωνεί με την τρέχουσα τιμή του επείγοντος δείκτη ως θετικό offset από τον αριθμό ακολουθίας σε αυτό το τμήμα. Ο επείγων δείκτης δείχνει τον αριθμό ακολουθίας του octet ακολουθώντας τα επείγοντα δεδομένα. Αυτό το πεδίο ερμηνεύεται μόνο στα τμήματα που έχει τεθεί το URG bit ελέγχου.

Επιλογές: μεταβλητή

Οι επιλογές μπορούν να καταλάβουν το διάστημα στο τέλος της κεφαλίδας TCP και είναι πολλαπλάσια των 8 bits στο μήκος. Όλες οι επιλογές συμπεριλαμβάνονται στο checksum. Μια επιλογή μπορεί να αρχίσει σε οποιοδήποτε όριο του octet. Υπάρχουν δύο περιπτώσεις για το σχήμα μιας επιλογής:

Περίπτωση 1: Μοναδικό octet επιλογής ανά είδος.

Περίπτωση 2: Ένα octet επιλογής ανά είδος, ένα octet επιλογής ανά μήκος και τα πραγματικά octets επιλογής ανά δεδομένα.

Η επιλογή-μήκους μετρά τις δύο octets της επιλογής-είδους και της επιλογής-μήκους καθώς επίσης και της επιλογής-δεδομένων οκτάδων.

Σημειώνουμε ότι ο κατάλογος επιλογών μπορεί να είναι συντομότερος από ό,τι υπονοεί το πεδίο offset των δεδομένων. Το περιεχόμενο της κεφαλίδας πέρα από την επιλογή End-Of-Option πρέπει να είναι header padding (δηλ., μηδέν).

Ένα TCP πρέπει να εφαρμόσει όλες τις επιλογές.

Οι πρόσφατα καθορισμένες επιλογές περιλαμβάνουν (είδος που υποδεικνύεται σε οκταδικό):

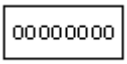
Πίνακας 6.

Kind	Length	Meaning
0	-	End of option list.
1	-	No-Operation.
2	4	Maximum Segment Size.

Συγκεκριμένοι ορισμοί επιλογής

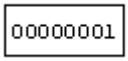
Τέλος του καταλόγου επιλογής

Kind=0



Αυτός ο κώδικας επιλογής δείχνει το τέλος του καταλόγου επιλογής. Αυτό μπορεί να μη συμπέσει με το τέλος της κεφαλίδας TCP σύμφωνα με τον τομέα offset δεδομένων. Αυτό χρησιμοποιείται στο τέλος όλων των επιλογών, όχι στο τέλος κάθε επιλογής, και χρειάζεται μόνο να χρησιμοποιηθεί εάν το τέλος των επιλογών δε θα μπορούσε διαφορετικά να συμπέσει με το τέλος της κεφαλίδας TCP.

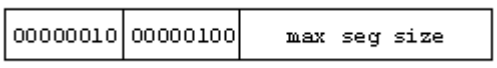
Καμία λειτουργία



Kind=1

Αυτός ο κώδικας επιλογής μπορεί να χρησιμοποιηθεί μεταξύ των επιλογών, παραδείγματος χάριν, να ευθυγραμμίσει την αρχή της επόμενης επιλογής σε ένα όριο λέξης. Δεν υπάρχει καμία εγγύηση ότι οι αποστολείς θα χρησιμοποιήσουν αυτήν την επιλογή, έτσι οι δέκτες πρέπει να προετοιμαστούν για να επεξεργαστούν τις επιλογές ακόμα κι αν δεν αρχίζουν με ένα όριο λέξης.

Μέγιστο μέγεθος τμήματος



Kind=2 Length=4

Μέγιστο μέγεθος τμήματος επιλογής δεδομένων : 16 bits

Εάν αυτή η επιλογή είναι παρούσα, τότε επικοινωνεί με το μέγιστο μέγεθος λαμβανόμενου τμήματος στο TCP το οποίο στέλνει αυτό το τμήμα. Αυτό το πεδίο

πρέπει μόνο να σταλεί στο αρχικό αίτημα σύνδεσης (δηλ. στα τμήματα με το bit ελέγχου SYN καθορισμένο). Εάν αυτή η επιλογή δεν χρησιμοποιείται, οποιοδήποτε μέγεθος τμήματος επιτρέπεται.

Padding: μεταβλητό

Η κεφαλίδα padding TCP χρησιμοποιείται για να εξασφαλίσει ότι η κεφαλίδα TCP τελειώνει και το δεδομένο αρχίζει σε ένα 32 bit όριο. Το padding αποτελείται από μηδενικά.

4.2 Εγκατάσταση σύνδεσης

Η “three-way handshake” είναι η διαδικασία που χρησιμοποιείται για να εγκατασταθεί μια σύνδεση. Αυτή η διαδικασία κανονικά κινείται από ένα TCP και αποκρίνεται από ένα άλλο TCP. Η διαδικασία λειτουργεί επίσης εάν δυο TCP κινούν ταυτόχρονα τη διαδικασία. Όταν η ταυτόχρονη προσπάθεια εμφανίζεται, κάθε TCP λαμβάνει ένα τμήμα "SYN" που δεν φέρνει καμία αναγνώριση αφότου έχει στείλει ένα "SYN". Φυσικά, η άφιξη ενός παλαιού διπλού τμήματος "SYN" μπορεί ενδεχομένως να το κάνει να εμφανιστεί, στον παραλήπτη, ότι μια ταυτόχρονη έναρξη σύνδεσης είναι υπό εξέλιξη.

Διάφορα παραδείγματα της έναρξης σύνδεσης ακολουθούν. Αν και αυτά τα παραδείγματα δεν παρουσιάζουν συγχρονισμό σύνδεσης χρησιμοποιώντας τμήματα μεταφοράς δεδομένων, αυτό είναι τέλεια νόμιμο, εφ' όσον δεν παραδίδει το λαμβάνον TCP τα δεδομένα στο χρήστη έως ότου γίνει σαφές ότι τα δεδομένα είναι έγκυρα (δηλ. τα στοιχεία πρέπει να αποθηκευθούν στο δέκτη έως ότου φθάσει η σύνδεση στην καθιερωμένη κατάσταση). Η “three-way handshake” μειώνει τη δυνατότητα των ψεύτικων συνδέσεων. Είναι η εφαρμογή μιας ανταλλαγής μεταξύ μνήμης και μηνυμάτων για να παρέχει τις πληροφορίες για αυτόν τον έλεγχο. Η απλούστερη three-way handshake παρουσιάζεται στο σχήμα 7 κατωτέρω. Οι αριθμοί πρέπει να ερμηνευθούν με τον ακόλουθο τρόπο. Κάθε γραμμή είναι αριθμημένη για λόγους αναφοράς. Τα δεξιά βέλη (-->) δείχνουν την αναχώρηση ενός τμήματος TCP από το TCP A στο TCP B, ή την άφιξη ενός τμήματος στο B από το A. Τα αριστερά βέλη (<- -), δείχνουν την αντιστροφή. Η έλλειψη (...) δείχνει ένα τμήμα που είναι ακόμα στο δίκτυο (καθυστερημένο). Ένα "XXX" δείχνει ένα τμήμα που χάνεται ή απορρίπτεται. Τα σχόλια εμφανίζονται σε παρένθεση. Οι καταστάσεις του TCP αντιπροσωπεύουν την κατάσταση μετά από την αναχώρηση ή την άφιξη του τμήματος (τα περιεχόμενα αυτά παρουσιάζονται στο κέντρο κάθε γραμμής). Τα περιεχόμενα του τμήματος παρουσιάζονται με σύντομη μορφή, με τον αριθμό ακολουθίας, τα flags ελέγχου, και το πεδίο ACK. Άλλα πεδία όπως το παράθυρο, οι διευθύνσεις, τα μήκη, και το κείμενο έχουν αφεθεί εκτός για χάρη σαφήνειας.

Πίνακας 7. Βασική 3-way χειραψία για το συγχρονισμό σύνδεσης

	TCP A		TCP B
1.	CLOSED		LISTEN
2.	SYN-SENT	--> <SEQ=100><CTL=SYN>	--> SYN-RECEIVED
3.	ESTABLISHED	<-- <SEQ=300><ACK=101><CTL=SYN,ACK>	<-- SYN-RECEIVED
4.	ESTABLISHED	--> <SEQ=101><ACK=301><CTL=ACK>	--> ESTABLISHED
5.	ESTABLISHED	--> <SEQ=101><ACK=301><CTL=ACK><DATA>	--> ESTABLISHED

Στη γραμμή 2 του πίνακα 7, το TCP A αρχίζει με την αποστολή ενός τμήματος SYN που δείχνει ότι θα χρησιμοποιήσει τους αριθμούς ακολουθίας αρχίζοντας από τον αριθμό ακολουθίας 100. Στη γραμμή 3, το TCP B στέλνει ένα SYN και αναγνωρίζει το SYN που έλαβε από το TCP A. Σημειώνουμε ότι ο τομέας αναγνώρισης που δείχνει το TCP B αναμένει τώρα να ακούσει την ακολουθία 101, αναγνωρίζοντας το SYN που κατέλαβε την ακολουθία 100. Στη γραμμή 4, το TCP A αποκρίνεται με ένα κενό τμήμα που περιέχει ένα ACK για το SYN του TCP B και στη γραμμή 5, το TCP A στέλνει μερικά δεδομένα. Σημειώνουμε ότι ο αριθμός ακολουθίας του τμήματος στη γραμμή 5 είναι ο ίδιος όπως στη γραμμή 4 επειδή το ACK δεν καταλαμβάνει το διάστημα αριθμού ακολουθίας.

Η ταυτόχρονη έναρξη είναι μόνο ελαφρώς πιο σύνθετη, όπως παρουσιάζεται στον πίνακα 8. Κάθε TCP κάνει κύκλους από το CLOSE στο SYN-SENT στο SYN-RECEIVED και στο ESTABLISHED.

Πίνακας 8.Ταυτόχρονος συγχρονισμός σύνδεσης

```
      TCP A
TCP B

  1.  CLOSED
CLOSED

  2.  SYN-SENT     --> <SEQ=100><CTL=SYN>
...

  3.  SYN-RECEIVED <-- <SEQ=300><CTL=SYN>              <-
- SYN-SENT

  4.               ... <SEQ=100><CTL=SYN>              --> SYN
RECEIVED

  5.  SYN-RECEIVED --> <SEQ=100><ACK=301><CTL=SYN,ACK>
...
```

```
  6.  ESTABLISHED  <-- <SEQ=300><ACK=101><CTL=SYN,ACK> <-- SYN
RECEIVED

  7.                ... <SEQ=101><ACK=301><CTL=ACK>      --
>ESTABLISHED
```

Ο κύριος λόγος για την three way handshake είναι να αποτραπούν οι παλιές διπλές ενάρξεις σύνδεσης από πρόκληση σύγχυσης. Για να αντιμετωπιστεί αυτό, ένα ειδικό μήνυμα ελέγχου, reset, έχει επινοηθεί. Εάν το λαμβανόμενο TCP είναι σε μια μη-συγχρονισμένη κατάσταση (δηλ., SYN-SENT, SYN-RECEIVED), επιστρέφει στην κατάσταση LISTEN λαμβάνοντας ένα αποδεκτό reset. Εάν το TCP είναι σε μια από τις συγχρονισμένες καταστάσεις (ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT), αποβάλλει τη σύνδεση και ενημερώνει το χρήστη του. Συζητάμε αυτήν την τελευταία περίπτωση κάτω από τις half-open συνδέσεις κατωτέρω.

Πίνακας 9.Αποκατάσταση από παλαιό διπλό SYN

```
      TCP A
TCP B

  1.  CLOSED
LISTEN

  2.  SYN-SENT    --> <SEQ=100><CTL=SYN>
...

  3.  (duplicate) ... <SEQ=90><CTL=SYN>               --> SYN
RECEIVED

  4.  SYN-SENT    <-- <SEQ=300><ACK=91><CTL=SYN,ACK>  <-- SYN
RECEIVED

  5.  SYN-SENT    --> <SEQ=91><CTL=RST>                --
> LISTEN

  6.                ... <SEQ=100><CTL=SYN>              --> SYN
RECEIVED
```

```
  7.  SYN-SENT    <-- <SEQ=400><ACK=101><CTL=SYN,ACK>  <-- SYN
RECEIVED

  8.  ESTABLISHED --> <SEQ=101><ACK=401><CTL=ACK>      -->
ESTABLISHED
```

Σαν απλό παράδειγμα της αποκατάστασης από τα παλαιά αντίγραφα, εξετάζουμε το σχήμα 9. Στη γραμμή 3, ένα παλιό διπλό SYN φθάνει στο TCP B. Το TCP B δεν μπορεί να πει ότι αυτό είναι ένα παλιό αντίγραφο, έτσι αποκρίνεται κανονικά (γραμμή 4). Το TCP A ανιχνεύει ότι το πεδίο ACK είναι ανακριβές και επιστρέφει ένα RST (reset) με το πεδίο SEQ του που επιλέγεται για να καταστήσει το τμήμα πιστευτό. Το TCP B, στη λήψη του RST, επιστρέφει στην κατάσταση LISTEN. Όταν το αρχικό SYN τελικά φθάνει στη γραμμή 6, ο συγχρονισμός προχωρά κανονικά. Εάν το SYN στη γραμμή 6 είχε φθάσει πριν από το RST, μια πιο σύνθετη ανταλλαγή μπορεί να είχε εμφανιστεί με το RST να έχει σταλεί και στις δύο κατευθύνσεις.

Half-Open συνδέσεις και άλλες ανωμαλίες

Μια καθιερωμένη σύνδεση λέγεται “half-open” εάν ένα από τα TCPs έχει κλείσει ή έχει αποβάλει τη σύνδεση στο τέλος του χωρίς τη γνώση του άλλου, ή εάν οι δύο άκρες της σύνδεσης έχουν γίνει μη συγχρονισμένες εξ’αιτίας μιας συντριβής που οδήγησε στην απώλεια μνήμης. Τέτοιες συνδέσεις θα γίνουν αυτόματα reset εάν γίνει προσπάθεια να σταλούν τα στοιχεία σε καθεμία κατεύθυνση. Εντούτοις, οι half-open συνδέσεις αναμένονται να είναι ασυνήθιστες, και η διαδικασία αποκατάστασης περιλαμβάνεται ελάχιστα.

Εάν στην πλευρά A η σύνδεση δεν υπάρχει πλέον, μια προσπάθεια από το χρήστη στην πλευρά B να στείλει οποιαδήποτε δεδομένα θα οδηγήσει στο TCP πλευράς B που λαμβάνει ένα μήνυμα ελέγχου reset. Ένα τέτοιο μήνυμα δείχνει στο TCP της πλευράς B ότι κάτι είναι λάθος, και αναμένεται να αποβάλει τη σύνδεση. Υποθέτουμε ότι δυο διεργασίες χρήστη A και B επικοινωνούν ο ένας με τον άλλο όταν εμφανίζεται μια συντριβή προκαλώντας απώλεια μνήμης στο TCP του A. Ανάλογα με το λειτουργικό σύστημα που υποστηρίζει το TCP του A, είναι πιθανό ότι κάποιος μηχανισμός αποκατάστασης λάθους υπάρχει. Όταν το TCP είναι ενεργό πάλι, το A είναι πιθανό να αρχίσει πάλι από την αρχή ή από ένα σημείο αποκατάστασης. Κατά συνέπεια, το A θα προσπαθήσει πιθανώς να ΑΝΟΙΞΕΙ τη σύνδεση πάλι ή να προσπαθήσει να ΣΤΕΙΛΕΙ στη σύνδεση που θεωρεί ανοικτή. Στην τελευταία περίπτωση, λαμβάνει το μήνυμα λάθους "σύνδεση μη ανοικτή" από το τοπικό TCP (του A). Σε μία προσπάθεια να εγκατασταθεί η σύνδεση, το TCP του A θα στείλει ένα τμήμα που περιέχει SYN. Αυτό το σενάριο οδηγεί στο παράδειγμα που παρουσιάζεται στο σχήμα 10. Αφού το TCP A συντρίβει, ο χρήστης προσπαθεί να ανοίξει πάλι τη σύνδεση. Το TCP B, στο μεταξύ, νομίζει ότι η σύνδεση είναι ανοικτή.

Πίνακας 10.Ανακάλυψη μισάνοιχτης σύνδεσης

```
      TCP A                                                TCP B

  1.  (CRASH)                                  (send
300,receive 100)

  2.  CLOSED
ESTABLISHED

  3.  SYN-SENT --> <SEQ=400><CTL=SYN>                  -->
(??)

  4.  (!!)     <-- <SEQ=300><ACK=100><CTL=ACK>     <--
ESTABLISHED

  5.  SYN-SENT --> <SEQ=100><CTL=RST>                  -->
(Abort!!)

  6.  SYN-SENT
CLOSED

  7.  SYN-SENT --> <SEQ=400><CTL=SYN>                  -->
```

Όταν το SYN φθάσει στη γραμμή 3, το TCP B, που είναι σε συγχρονισμένη κατάσταση, και το εισερχόμενο τμήμα εκτός από το window, ανταποκρίνεται με μια αναγνώριση που προσδιορίζει ποια ακολουθία αναμένει έπειτα να ακούσει (ACK 100). Το TCP A βλέπει ότι αυτό το τμήμα δεν αναγνωρίζει τίποτα απ'ότι έστειλε και όντας μη συγχρονισμένο στέλνει ένα reset (RST) επειδή έχει ανιχνεύσει μια μισάνοιχτη σύνδεση. Το TCP B αποβάλλει στη γραμμή 5. Το TCP A θα συνεχίσει να προσπαθεί να εγκαταστήσει τη σύνδεση, το πρόβλημα περιορίζεται τώρα στη βασική 3-way shake του σχήματος 7.

Μια ενδιαφέρουσα εναλλακτική περίπτωση εμφανίζεται όταν καταστρέφεται το TCP A και το TCP B προσπαθεί να στείλει δεδομένα σ'αυτό νομίζοντας ότι υπάρχει ακόμα η συγχρονισμένη σύνδεση. Αυτό διευκρινίζεται στο σχήμα 11. Σε αυτήν την περίπτωση, τα δεδομένα που φθάνουν στο TCP A από το TCP B (γραμμή 2) είναι μη αποδεκτά επειδή καμία τέτοια σύνδεση δεν υπάρχει, έτσι το TCP A στέλνει ένα RST. Το RST γίνεται αποδεκτό, έτσι το TCP B το επεξεργάζεται και αποβάλλει τη σύνδεση.

Πίνακας 11.Η ενεργός πλευρά προκαλεί τη μισάνοιχτη ανακάλυψη σύνδεσης

```
   TCP A                                                  TCP
B

  1.  (CRASH)                                        (send
300,receive 100)

  2.  (??)    <-- <SEQ=300><ACK=100><DATA=10><CTL=ACK> <--
ESTABLISHED

  3.          --> <SEQ=100><CTL=RST>                   --
> (ABORT!!)
```

Στο σχήμα 12, βρίσκουμε τα δυο TCPs A και B με παθητικές συνδέσεις να περιμένουν SYN. Μια παλιά διπλή άφιξη στο TCP B (γραμμή 2) ενεργοποιεί τη πλευρά B. Ένα SYN-ACK επιστρέφεται (γραμμή 3) και προκαλεί το TCP A να παράγει ένα RST (το ACK στη γραμμή 3 δεν είναι αποδεκτό). Το TCP B δέχεται το reset και επιστρέφει στην παθητική του LISTEN κατάσταση.

Πίνακας 12. Παλιό διπλό SYN αρχίζει ένα reset σε δυο παθητικά sockets

```
    TCP A                                                TCP B

  1.  LISTEN
LISTEN

  2.       ... <SEQ=Z><CTL=SYN>                -->  SYN-
RECEIVED

  3.  (??) <-- <SEQ=X><ACK=Z+1><CTL=SYN,ACK>   <--  SYN-
RECEIVED

  4.       --> <SEQ=Z+1><CTL=RST>              -->  (return to
LISTEN!)

  5.  LISTEN
LISTEN
```

Ποικίλες άλλες περιπτώσεις είναι δυνατές, οι οποίες αποτελούνται από τους ακόλουθους κανόνες για την παραγωγή RST και την επεξεργασία.

Παραγωγή reset

Κατά γενικό κανόνα, reset (RST) πρέπει να σταλεί όποτε ένα τμήμα φθάνει που δεν προορίζεται προφανώς για την τρέχουσα σύνδεση. Ένα reset δεν πρέπει να στέλνεται εάν δεν είναι σαφές ότι αυτό πρέπει να συμβεί.

Υπάρχουν τρεις ομάδες καταστάσεων:

1. Εάν η σύνδεση δεν υπάρχει (CLOSED) τότε ένα reset στέλνεται σαν απάντηση σε οποιοδήποτε εισερχόμενο σήμα εκτός από ένα άλλο reset. Ειδικότερα, SYNs που απευθύνονται σε μια ανύπαρκτη σύνδεση απορρίπτονται σε κάθε περίπτωση. Εάν το εισερχόμενο τμήμα έχει ένα πεδίο ACK, το reset παίρνει τον αριθμό ακολουθίας του από το πεδίο ACK του τμήματος, διαφορετικά το reset έχει τον αριθμό ακολουθίας μηδέν και το πεδίο ACK τίθεται στο άθροισμα του αριθμού ακολουθίας και του μήκους τμήματος του εισερχόμενου τμήματος. Η σύνδεση παραμένει στην κατάσταση CLOSED.
2. Εάν η σύνδεση είναι σε οποιαδήποτε μη-συγχρονισμένη κατάσταση (LISTEN, SYN-SENT, SYN-RECEIVED), και το εισερχόμενο τμήμα αναγνωρίζει κάτι που δεν έχει σταλεί ακόμα (το τμήμα φέρνει ένα μη αποδεκτό ACK), ή εάν ένα εισερχόμενο τμήμα έχει ένα επίπεδο ασφαλείας ή ένα compartment που δεν ταιριάζει ακριβώς με το επίπεδο και το compartment που ζητούνται για τη σύνδεση, στέλνεται ένα reset. Εάν το SYN μας δεν έχει αναγνωριστεί και το επίπεδο προτεραιότητας του εισερχόμενου τμήματος είναι πιο υψηλό από το επίπεδο προτεραιότητας που ζητείται έπειτα είτε βελτιώνουμε το τοπικό επίπεδο προτεραιότητας (εάν επιτρέπεται από το χρήστη και το σύστημα) ή στέλνουμε ένα reset, ή εάν το επίπεδο προτεραιότητας του εισερχόμενου τμήματος είναι χαμηλότερο από το επίπεδο προτεραιότητας που ζητείται έπειτα συνεχίζουμε σαν να ταίριαξε ακριβώς η προτεραιότητα (εάν το μακρινό TCP δεν μπορεί να βελτιώσει το επίπεδο προτεραιότητας στην αντιστοιχία του δικού μας αυτό θα ανιχνευθεί στο επόμενο τμήμα που θα σταλεί, και η σύνδεση θα τερματίσει έπειτα). Εάν το SYN μας έχει αναγνωριστεί (ίσως σε αυτό το εισερχόμενο τμήμα) το επίπεδο προτεραιότητας του εισερχόμενου τμήματος πρέπει να ταιριάξει με το τοπικό επίπεδο προτεραιότητας ακριβώς, εάν όχι ένα reset πρέπει να σταλεί. Εάν το εισερχόμενο τμήμα έχει ένα πεδίο ACK, το reset παίρνει τον αριθμό ακολουθίας του από το πεδίο ACK του τμήματος, διαφορετικά το reset έχει τον αριθμό ακολουθίας μηδέν και το πεδίο ACK τίθεται στο άθροισμα του αριθμού ακολουθίας και του μήκους τμήματος του εισερχόμενου τμήματος. Η σύνδεση παραμένει στην ίδια κατάσταση.
3. Εάν η σύνδεση είναι σε συγχρονισμένη κατάσταση (ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT), οποιοδήποτε μη αποδεκτό τμήμα (εκτός του αριθμού ακολουθίας του window ή μη-αποδεκτό αριθμό acknowledgement) πρέπει να αποσπάσει μόνο ένα κενό τμήμα αναγνώρισης που περιέχει τον τρέχοντα αριθμό αποστολής-ακολουθίας και μια αναγνώριση που δείχνει τον επόμενο αριθμό ακολουθίας

που αναμένεται να παραληφθεί, και η σύνδεση παραμένει στην ίδια κατάσταση. Εάν ένα εισερχόμενο τμήμα έχει επίπεδο ασφάλειας, ή το compartment, ή προτεραιότητα που δεν ταιριάζει ακριβώς με το επίπεδο, και compartment, και την προτεραιότητα που ζητείται για τη σύνδεση, ένα reset στέλνεται και η σύνδεση πηγαίνει στην κατάσταση CLOSED. Το reset παίρνει τον αριθμό ακολουθίας του από το πεδίο ACK του εισερχόμενου τμήματος.

Επεξεργασία reset

Σε όλες τις καταστάσεις εκτός από την SYN-SENT, όλα τα reset τμήματα (RST) επικυρώνονται με τον έλεγχο των πεδίων SEQ. Ένα reset ισχύει εάν ο αριθμός ακολουθίας του είναι στο window. Στην κατάσταση SYN-SENT (ένα RST παραλαμβάνεται σαν απάντηση σε ένα αρχικό SYN), το RST είναι αποδεκτό εάν το πεδίο ACK αναγνωρίζει το SYN. Ο αποδέκτης ενός RST το επικυρώνει αρχικά, και αλλάζει έπειτα κατάσταση. Εάν ο αποδέκτης ήταν στην κατάσταση LISTEN, το αγνοεί. Εάν ο αποδέκτης ήταν στην κατάσταση SYN-RECEIVED και ήταν προηγουμένως στην κατάσταση LISTEN, κατόπιν ο αποδέκτης επιστρέφει στην κατάσταση LISTEN, διαφορετικά αποβάλλει τη σύνδεση και πηγαίνει στην κατάσταση CLOSED. Εάν ο αποδέκτης ήταν σε οποιαδήποτε άλλη κατάσταση, αποβάλλει τη σύνδεση, συμβουλεύει το χρήστη και πηγαίνει στην κατάσταση CLOSED.

4.3 Κλείσιμο σύνδεσης

CLOSE είναι μία λειτουργία που σημαίνει ότι "δεν έχω άλλα στοιχεία να στείλω". Η έννοια του κλεισίματος μια πλήρους-διπλής σύνδεσης υπόκειται στη διφορούμενη ερμηνεία, φυσικά, δεδομένου ότι μπορεί να μην είναι προφανές πώς να μεταχειριστεί τη λαμβάνουσα πλευρά της σύνδεσης. Έχουμε επιλέξει να μεταχειριστούμε την κατάσταση CLOSE σαν μία μονής κατεύθυνσης κατάσταση. Ο χρήστης που κάνει CLOSE μπορεί να συνεχίσει ΝΑ ΛΑΜΒΑΝΕΙ έως ότου ειδοποιηθεί ότι η άλλη πλευρά ΕΧΕΙ ΚΛΕΙΣΕΙ επίσης. Κατά συνέπεια, ένα πρόγραμμα θα μπορούσε να αρχίσει διάφορα SENDs ακολουθούμενα από ένα CLOSE, και να συνεχίσει έπειτα ΝΑ ΛΑΜΒΑΝΕΙ μέχρι να του επισημανθεί ότι ένα RECEIVE απέτυχε επειδή η άλλη πλευρά ΕΧΕΙ ΚΛΕΙΣΕΙ. Υποθέτουμε ότι το TCP θα ειδοποιήσει έναν χρήστη, ακόμα κι αν κανένα RECEIVE δεν είναι σημαντικό, ότι η άλλη πλευρά έχει κλείσει, έτσι ο χρήστης μπορεί να ολοκληρώσει την πλευρά του επιτυχημένα. Ένα TCP θα παραδώσει αξιόπιστα όλους τους SENT buffers προτού η σύνδεση γίνει CLOSED έτσι ώστε ένας χρήστης που δεν αναμένει κανένα στοιχείο να επιστραφεί χρειάζεται μόνο να 'ακούσει' ότι η σύνδεση έγινε CLOSED επιτυχώς για να ξέρει ότι όλα τα δεδομένα του παραλήφθηκαν από το προοριζόμενο TCP. Οι χρήστες πρέπει να συνεχίσουν να διαβάζουν τις συνδέσεις που κλείνουν για αποστολή έως ότου το TCP δε δέχεται άλλα στοιχεία.

Υπάρχουν ουσιαστικά τρεις περιπτώσεις:

1) Ο χρήστης αρχίζει λέγοντας στο TCP ΝΑ ΚΛΕΙΣΕΙ τη σύνδεση

2) Το μακρινό TCP αρχίζει με την αποστολή ενός σήματος ελέγχου FIN

3) Και οι δύο χρήστες ΚΛΕΙΝΟΥΝ ταυτόχρονα

Περίπτωση 1: Ο τοπικός χρήστης αρχίζει το κλείσιμο

Σε αυτήν την περίπτωση, ένα τμήμα FIN μπορεί να κατασκευαστεί και να τοποθετηθεί στην εξερχόμενη σειρά αναμονής τμήματος. Κανένα περαιτέρω SEND από το χρήστη δεν θα γίνει αποδεκτό από το TCP, και μπαίνει στην κατάσταση FIN-WAIT-1. Τα RECEIVEs επιτρέπονται σε αυτήν την κατάσταση. Όλα τα τμήματα προηγούνται και συμπεριλαμβανομένου του FIN θα αναμεταδοθούν μέχρι να γίνουν acknowledged. Όταν το άλλο TCP αναγνωρίσει το FIN και στείλει ένα δικό του FIN, το πρώτο TCP μπορεί να κάνει ACK αυτό το FIN. Σημειώνουμε ότι ένα TCP που λαμβάνει ένα FIN θα κάνει ACK αλλά δε θα στείλει το FIN του έως ότου ο χρήστης του ΕΧΕΙ ΚΛΕΙΣΕΙ τη σύνδεση επίσης.

Περίπτωση 2: Το TCP λαμβάνει ένα FIN από το δίκτυο

Εάν ένα εκούσιο FIN φτάσει από το δίκτυο, το λαμβάνον TCP μπορεί να το κάνει ACK και να πει στο χρήστη ότι η σύνδεση κλείνει. Ο χρήστης θα αποκριθεί με ένα CLOSE, επάνω στον οποίο το TCP μπορεί να στείλει ένα FIN στο άλλο TCP αφού σταλούν οποιαδήποτε υπόλοιπα δεδομένα. Το TCP τότε περιμένει έως ότου αναγνωριστεί το FIN του όπου και διαγράφει τη σύνδεση. Εάν ένα ACK δεν είναι προσεχές, αφότου ο χρήστης διακόψει τη σύνδεση αποβάλλεται και ο χρήστης ενημερώνεται.

Περίπτωση 3 : και οι δύο χρήστες κλείνουν ταυτόχρονα

Ένα ταυτόχρονο CLOSE από τους χρήστες και στις δύο άκρες μιας σύνδεσης αναγκάζει τα τμήματα FIN να ανταλλαχθούν. Όταν όλα τα τμήματα που προηγούνται των FINs υποβληθούν σε επεξεργασία και αναγνωριστούν, κάθε TCP μπορεί να κάνει ACK το FIN που έχει λάβει. Και οι δύο, επάνω στη λήψη αυτών των ACKs, θα διαγράψουν τη σύνδεση.

Πίνακας 13. Κανονική ακολουθία κλεισίματος μιας σύνδεσης

```
      TCP A
TCP B

  1.  ESTABLISHED
ESTABLISHED

  2.  (Close)
      FIN-WAIT-1  --> <SEQ=100><ACK=300><CTL=FIN,ACK>  --
> CLOSE-WAIT

  3.  FIN-WAIT-2  <-- <SEQ=300><ACK=101><CTL=ACK>      <-
- CLOSE-WAIT
```

```
  4.
(Close)
      TIME-WAIT   <-- <SEQ=300><ACK=101><CTL=FIN,ACK>  <-
- LAST-ACK

  5.  TIME-WAIT   --> <SEQ=101><ACK=301><CTL=ACK>      --
> CLOSED

  6.  (2 MSL)
      CLOSED
```

Πίνακας 14. Ταυτόχρονη ακολουθία κλεισίματος μιας σύνδεσης

```
      TCP A
TCP B

  1.  ESTABLISHED
ESTABLISHED

  2.  (Close)
(Close)
      FIN-WAIT-1  --> <SEQ=100><ACK=300><CTL=FIN,ACK>
... FIN-WAIT-1
                  <-- <SEQ=300><ACK=100><CTL=FIN,ACK>  <-
-
                  ... <SEQ=100><ACK=300><CTL=FIN,ACK>  --
>

  3.  CLOSING     --> <SEQ=101><ACK=301><CTL=ACK>
... CLOSING
                  <-- <SEQ=301><ACK=101><CTL=ACK>      <-
-
                  ... <SEQ=101><ACK=301><CTL=ACK>      --
>

  4.  TIME-WAIT
TIME-WAIT
      (2 MSL)
(2 MSL)
      CLOSED
CLOSED
```

4.4 Προτεραιότητα και ασφάλεια

Η πρόθεση είναι ότι η σύνδεση επιτρέπεται μόνο μεταξύ των ports που λειτουργούν με ακριβώς την ίδια ασφάλεια και compartment τιμές και στο υψηλότερο επίπεδο προτεραιότητας που ζητείται από τα δύο ports. Οι παράμετροι προτεραιότητας και ασφάλειας που χρησιμοποιούνται στο TCP είναι ακριβώς εκείνες που καθορίζονται στο πρωτόκολλο Διαδικτύου (IP). Σε όλη αυτήν την προδιαγραφή του TCP ο όρος "ασφάλεια/ compartment" προορίζεται να δείξει τις παραμέτρους ασφάλειας που χρησιμοποιούνται στο IP συμπεριλαμβανομένης της ασφάλειας, του compartment, της ομάδας χρηστών, και του διαχειριζόμενου περιορισμού.

Μια προσπάθεια σύνδεσης με τις κακώς συνδυασμένες τιμές ασφάλειας/ compartments ή μια χαμηλότερη τιμή προτεραιότητας πρέπει να απορριφθεί με την αποστολή ενός reset. Η απόρριψη μιας σύνδεσης λόγω μιας πάρα πολύ χαμηλής προτεραιότητας εμφανίζεται μόνο αφότου έχει παραληφθεί μια αναγνώριση του SYN.

Σημειώνουμε ότι οι ενότητες TCP που λειτουργούν μόνο στην προκαθορισμένη τιμή της προτεραιότητας θα πρέπει ακόμα να ελέγξουν την προτεραιότητα των εισερχόμενων τμημάτων και να βελτιώσουν ενδεχομένως το επίπεδο προτεραιότητας που χρησιμοποιούν στη σύνδεση.

Οι παράμετροι ασφάλειας μπορούν να χρησιμοποιηθούν ακόμη και σε ένα μη-ασφαλές περιβάλλον (οι τιμές θα έδειχναν τα αταξινόμητα δεδομένα), κατά συνέπεια οι hosts στα μη-ασφαλή περιβάλλοντα πρέπει να προετοιμαστούν να λάβουν τις παραμέτρους ασφάλειας, αν και δε χρειάζεται να τις στείλουν.

4.5 Μετάδοση στοιχείων

Μόλις καθιερωθεί η σύνδεση τα δεδομένα επικοινωνούν με την ανταλλαγή των τμημάτων. Επειδή τα τμήματα μπορούν να χαθούν λόγω των λαθών (checksum αποτυχία δοκιμής), ή της συμφόρησης δικτύου, το TCP χρησιμοποιεί την αναμετάδοση (μετά από μια διακοπή) για να εξασφαλίσει παράδοση κάθε τμήματος. Τα διπλά τμήματα μπορεί να φτάσουν λόγω του δικτύου ή της αναμετάδοσης TCP. Το TCP εκτελεί ορισμένες δοκιμές στους αριθμούς ακολουθίας και στους αριθμούς acknowledgement στα τμήματα για να ελέγξει την αποδοχή τους.

Ο αποστολέας των δεδομένων παρακολουθεί τη διαδρομή του επόμενου αριθμού ακολουθίας για να τη χρησιμοποιήσει στη μεταβλητή SND.NXT. Ο αποδέκτης των δεδομένων παρακολουθεί τη διαδρομή του επόμενου αριθμού ακολουθίας που αναμένει στη μεταβλητή RCV. NXT. Ο αποστολέας των δεδομένων παρακολουθεί τη διαδρομή του παλαιότερου μη αναγνωρισμένου αριθμού ακολουθίας στη μεταβλητή SND. UNA. Εάν η ροή δεδομένων είναι στιγμιαία μη απασχολημένη και όλα τα δεδομένα που στέλνονται έχουν αναγνωριστεί τότε οι τρεις μεταβλητές θα είναι ίσες.

Όταν ο αποστολέας δημιουργεί ένα τμήμα και το διαβιβάζει ο αποστολέας προωθεί τη SND. NXT. Όταν ο αποδέκτης δέχεται ένα τμήμα προωθεί τη RCV. NXT και στέλνει μια αναγνώριση. Όταν ο αποστολέας δεδομένων λαμβάνει μια αναγνώριση προωθεί τη SND.UNA. Ο βαθμός στον οποίο οι τιμές αυτών των μεταβλητών διαφέρουν είναι ένα μέτρο της καθυστέρησης στην επικοινωνία. Το ποσό από το οποίο οι μεταβλητές είναι προηγμένες είναι το μήκος των δεδομένων στο τμήμα. Σημειώνουμε ότι στην κατάσταση ESTABLISHED πρέπει να φέρουν όλα τα τμήματα τις τρέχουσες πληροφορίες αναγνώρισης.

Η CLOSE κλήση των χρηστών υπονοεί μια λειτουργία push, όπως το flag ελέγχου FIN σε ένα εισερχόμενο τμήμα.

Διακοπή αναμετάδοσης

Λόγω της μεταβλητότητας των δικτύων που συνθέτουν ένα σύστημα internetwork και το ευρύ φάσμα των χρήσεων των συνδέσεων TCP η διακοπή αναμετάδοσης πρέπει να καθοριστεί δυναμικά. Μια διαδικασία καθορισμού μιας διακοπής αναμετάδοσης δίνεται εδώ ως απεικόνιση.

Ένα παράδειγμα διαδικασίας διακοπής αναμετάδοσης

Μετρώντας την παρερχόμενη περίοδο μεταξύ της αποστολής ενός octet δεδομένων με έναν ιδιαίτερο αριθμό ακολουθίας και της λήψης μιας αναγνώρισης που καλύπτει εκείνο τον αριθμό ακολουθίας (τα τμήματα που στέλνονται δεν είναι απαραίτητο να ταιριάζουν με τα λαμβανόμενα τμήματα). Αυτός ο υπολογισμένος παρερχόμενος χρόνος είναι ο Round Trip Time (RTT). Έπειτα υπολογίζουμε έναν Smoothed Round Trip Time (SRTT) όπως:

SRTT = (ALPHA * SRTT) + ((1-ALPHA) * RTT)

και βασιζόμενοι σε αυτό, υπολογίζουμε τη διακοπή αναμετάδοσης (RTO) όπως:

RTO = min[UBOUND, max[LBOUND, (BETA*SRTT)]]

όπου UBOUND είναι ένα άνω όριο της διακοπής (π.χ., 1 λεπτό), LBOUND είναι ένα κάτω όριο της διακοπής (π.χ., 1 δεύτερο), ALPHA είναι ένας ομαλός παράγοντας (π.χ. από 0.8 ως 0.9), και BETA είναι ένας παράγοντας διαφοράς καθυστέρησης (π.χ. 1.3 έως 2.0).

Η επικοινωνία των επειγουσών πληροφοριών

Ο στόχος του επείγοντος μηχανισμού TCP είναι να επιτραπεί στον στέλνοντα χρήστη να υποκινήσει το λαμβάνοντα χρήστη να δεχτεί μερικά επείγοντα δεδομένα και να επιτραπεί στο λαμβανόμενο TCP να δείξει στο λαμβάνοντα χρήστη πότε όλα τα πρόσφατα γνωστά επείγοντα δεδομένα λήφθηκαν από το χρήστη.

Αυτός ο μηχανισμός επιτρέπει σε ένα σημείο στο κανάλι δεδομένων να σχεδιασθεί ως το τέλος των επειγουσών πληροφοριών. Όποτε αυτό το σημείο προηγείται του λαμβανόμενου αριθμού ακολουθίας (RCV. NXT) στο λαμβάνον TCP, αυτό το TCP πρέπει να πει στο χρήστη να πάει στην "επείγουσα κατάσταση" όταν ο λαμβανόμενος αριθμός ακολουθίας προφθάνει τον επείγοντα δείκτη, το TCP πρέπει να πει στο χρήστη να πάει στην “κανονική κατάσταση”. Εάν ο επείγων δείκτης ενημερώνεται ενώ ο χρήστης είναι στον "επείγοντα τρόπο", η ενημέρωση θα είναι αόρατη στο χρήστη.

Η μέθοδος χρησιμοποιεί έναν επείγοντα τομέα που φέρει όλα τα διαβιβασθέντα τμήματα. Το flag ελέγχου URG δείχνει ότι ο επείγων τομέας είναι σημαντικός και πρέπει να προστεθεί στον αριθμό ακολουθίας τμήματος για να παραγάγει τον επείγοντα δείκτη. Η απουσία αυτού του flag δείχνει ότι δεν υπάρχει κανένα επείγον σημαντικό δεδομένο. Για να στείλει μια επείγουσα ένδειξη ο χρήστης πρέπει επίσης να στείλει τουλάχιστον ένα octet δεδομένων. Εάν ο αποστέλλων χρήστης δείχνει επίσης ένα push, ενισχύεται η έγκαιρη παράδοση των επειγουσών πληροφοριών στη διαδικασία προορισμού.

Διαχείριση window

Το παράθυρο που στέλνεται σε κάθε τμήμα δείχνει τη σειρά των αριθμών ακολουθίας που ο αποστολέας του παραθύρου (ο δέκτης δεδομένων) είναι αυτήν την περίοδο έτοιμος να δεχτεί. Υπάρχει μια υπόθεση ότι αυτό συσχετίζεται με το διαθέσιμο σήμερα διάστημα buffer δεδομένων για αυτήν την σύνδεση. Η ένδειξη ενός μεγάλου παραθύρου ενθαρρύνει τις μεταδόσεις. Εάν περισσότερα δεδομένα φθάσουν από όσα μπορούν να γίνουν αποδεκτά, θα απορριφθούν. Αυτό θα οδηγήσει στις υπερβολικές αναμεταδόσεις, προσθέτοντας μη απαραίτητο φορτίο στο δίκτυο και στα TCPs. Η ένδειξη ενός μικρού παραθύρου μπορεί να περιορίσει τη διαβίβαση δεδομένων στο σημείο της εισαγωγής μιας καθυστέρησης round trip μεταξύ κάθε νέου διαβιβασθέντος τμήματος.

Οι παρεχόμενοι μηχανισμοί επιτρέπουν σε ένα TCP να διαφημίσει ένα μεγάλο παράθυρο και να διαφημίσει στη συνέχεια ένα πολύ μικρότερο παράθυρο χωρίς να έχει αποδεχτεί τόσα πολλά δεδομένα. Αυτό, λέγεται “shrinking the window” . Η αρχή ευρωστίας υπαγορεύει ότι τα TCPs δεν θα στενέψουν το window τα ίδια, αλλά θα προετοιμαστούν για τέτοια συμπεριφορά εκ μέρους άλλων TCPs. Το αποστέλλων TCP πρέπει να προετοιμαστεί να δεχτεί από το χρήστη και να στείλει τουλάχιστον ένα octet των νέων δεδομένων ακόμα κι αν το παράθυρο αποστολής είναι μηδέν. Το αποστέλλων TCP πρέπει να αναμεταδίδει τακτικά στο λαμβάνον TCP ακόμα και όταν το παράθυρο είναι μηδέν. Δύο λεπτά συστήνονται για το διάστημα αναμετάδοσης όταν το παράθυρο είναι μηδέν. Αυτή η αναμετάδοση είναι ουσιαστική για να εγγυηθεί ότι όταν έχει καθένα TCP ένα μηδέν παράθυρο η επαναλειτουργία του παραθύρου θα αναφερθεί αξιόπιστα στο άλλο. Όταν το λαμβάνον TCP έχει ένα μηδέν παράθυρο και φτάνει ένα τμήμα, πρέπει ακόμη να στείλει μια αναγνώριση που παρουσιάζει τον επόμενο αναμενόμενο αριθμό ακολουθίας και το τρέχον παράθυρό του (μηδέν). Το αποστέλλων TCP συσκευάζει τα δεδομένα που διαβιβάζονται στα τμήματα που εγκαθιστούν το τρέχον παράθυρο, και μπορεί να ξαναπακετάρει τα τμήματα στη σειρά αναμονής αναμετάδοσης. Τέτοιο ξαναπακετάρισμα δεν απαιτείται, αλλά μπορεί να φανεί χρήσιμο.

Σε μια σύνδεση με μονόδρομη ροή δεδομένων, οι πληροφορίες παραθύρων θα φέρουν τμήματα αναγνώρισης που όλα θα έχουν τον ίδιο αριθμό ακολουθίας έτσι δε θα υπάρξει κανένας τρόπος να αναδιαταχθούν πάλι εάν φτάσουν εκτός σειράς. Αυτό δεν είναι σοβαρό πρόβλημα, αλλά θα επιτρέψει στις πληροφορίες παραθύρων να είναι περιστασιακά προσωρινά βασισμένες στις παλιές αναφορές από το δέκτη δεδομένων. Ένας καθαρισμός για να αποφευχθεί αυτό το πρόβλημα είναι να ενεργήσει στις πληροφορίες παραθύρων από τα τμήματα που φέρουν τον υψηλότερο αριθμό αναγνώρισης (αυτά είναι τμήματα με ίσο αριθμό αναγνώρισης ή μεγαλύτερο από τον υψηλότερο προηγουμένως λαμβανόμενο). Η διοικητική διαδικασία παραθύρων έχει σημαντική επιρροή στην απόδοση επικοινωνίας.

Προτάσεις διαχείρισης του Window

Η διάθεση ενός πολύ μικρού παραθύρου αναγκάζει τα δεδομένα να διαβιβαστούν σε πολλά μικρά τμήματα όταν επιτυγχάνεται καλύτερη απόδοση χρησιμοποιώντας λιγότερα μεγάλα τμήματα. Μια πρόταση για αποφυγή μικρών παραθύρων είναι ο δέκτης να αναβάλει την ενημέρωση ενός παραθύρου έως ότου η πρόσθετη κατανομή γίνει τουλάχιστον X % της μέγιστης κατανομής πιθανής για τη σύνδεση (όπου το X να είναι από 20 έως 40). Μια άλλη πρόταση για τον αποστολέα είναι να αποφεύγει να στέλνει μικρά τμήματα περιμένοντας έως ότου το window γίνει αρκετά μεγάλο πριν να στείλει τα δεδομένα. Εάν ο χρήστης επισημαίνει μια push λειτουργία έπειτα τα δεδομένα πρέπει να σταλούν ακόμα κι αν είναι ένα μικρό τμήμα.

Σημειώνουμε ότι οι acknowledgements δεν πρέπει να καθυστερήσουν αλλιώς οι περιττές αναμεταδόσεις θα έχουν αποτέλεσμα. Μια στρατηγική θα ήταν να σταλεί μια αναγνώριση όταν φθάνει ένα μικρό τμήμα (με έξω ενημέρωση στις πληροφορίες παραθύρων), και έπειτα να σταλεί μια άλλη αναγνώριση με νέες πληροφορίες παραθύρων όταν το παράθυρο είναι μεγαλύτερο. Το τμήμα που στέλνεται για να εξετάσει ένα μηδέν παράθυρο μπορεί επίσης να αρχίσει ένα χωρισμό των διαβιβασθέντων δεδομένων σε όλο και μικρότερα τμήματα. Εάν ένα τμήμα περιέχει ένα ενιαίο octet δεδομένων που στέλνεται για να εξετάσει ένα μηδέν παράθυρο γίνεται αποδεκτό, καταναλώνει ένα octet του window που είναι τώρα διαθέσιμο. Εάν το αποστέλλων TCP στείλει απλώς τόσο πολύ όσο μπορεί όποτε το παράθυρο είναι μη μηδενικό, τα διαβιβασθέντα δεδομένα θα διασπαστούν σε εναλλασσόμενα μεγάλα και μικρά τμήματα.

Καθώς ο χρόνος περνάει, οι περιστασιακές διακοπές στο δέκτη καθιστούν την κατανομή παραθύρων διαθέσιμη και ως αποτέλεσμα θα έχει το σπάσιμο των μεγάλων τμημάτων σε ένα μικρό και όχι τόσο αρκετά μεγάλο ζευγάρι. Μετά από λίγο η μετάδοση δεδομένων θα γίνεται κυρίως στα μικρά τμήματα. Η πρόταση εδώ είναι οι εφαρμογές TCP να προσπαθήσουν ενεργά να συνδυάσουν τις μικρές κατανομές παραθύρων στα μεγαλύτερα παράθυρα, δεδομένου ότι οι μηχανισμοί για το παράθυρο τείνουν να οδηγήσουν σε πολλά μικρά παράθυρα στις απλούστερες απασχολημένες εφαρμογές.

4.6 Διεπαφές

Υπάρχουν φυσικά δύο διεπαφές που μας αφορούν : η διεπαφή χρήστη/ TCP και η διεπαφή TCP/ χαμηλότερο επίπεδο. Για την περίπτωση που το χαμηλότερο επίπεδο είναι IP σημειώνουμε μερικές από τις τιμές παραμέτρου που τα TCPs μπορεί να χρησιμοποιήσουν.

Διεπαφή χρήστη/ TCP

Η ακόλουθη λειτουργική περιγραφή των εντολών χρηστών στο TCP είναι, στην καλύτερη περίπτωση, πλασματική, δεδομένου ότι κάθε λειτουργικό σύστημα θα έχει διαφορετικές εγκαταστάσεις. Συνεπώς, πρέπει να προειδοποιήσουμε τους αναγνώστες ότι οι διαφορετικές εφαρμογές TCP μπορούν να έχουν διαφορετικές διεπαφές χρήστη. Εντούτοις, όλα τα TCPs πρέπει να παρέχουν ένα ορισμένο ελάχιστο σύνολο υπηρεσιών για να εγγυηθούν ότι όλες οι εφαρμογές TCP μπορούν να υποστηρίξουν την ίδια ιεραρχία πρωτοκόλλου. Αυτό το τμήμα διευκρινίζει τις λειτουργικές διεπαφές που απαιτούνται από όλες τις εφαρμογές TCP.

Εντολές χρηστών TCP

Τα εξής τμήματα χαρακτηρίζουν λειτουργικά μια διεπαφή χρήστη/ TCP. Η σημείωση χρησιμοποιούμενη είναι παρόμοια με τις περισσότερες διαδικασίες ή κλήσεις συνάρτησης στις γλώσσες υψηλού επιπέδου, αλλά αυτή η χρήση δεν προορίζεται να αποκλείσει τις κλήσεις υπηρεσιών τύπων trap (π.χ., SVCs, UUOs, EMTs). Οι εντολές χρηστών που περιγράφονται κατωτέρω διευκρινίζουν τις βασικές λειτουργίες που το TCP πρέπει να εκτελέσει για να υποστηρίξει την ενδοδιεργασιακή επικοινωνία. Οι μεμονωμένες εφαρμογές πρέπει να καθορίσουν το ακριβές σχήμα τους, και μπορούν να παρέχουν συνδυασμούς ή υποσύνολα των βασικών λειτουργιών στις ενιαίες κλήσεις. Ειδικότερα, μερικές εφαρμογές μπορούν να επιθυμήσουν ΝΑ ΑΝΟΙΞΟΥΝ αυτόματα μια σύνδεση στο πρώτο SEND ή RECEIVE από το χρήστη για μια δεδομένη σύνδεση.

Στην παροχή των ενδοδιεργασιακών εγκαταστάσεων επικοινωνίας, το TCP πρέπει όχι μόνο να δεχτεί τις εντολές, αλλά πρέπει επίσης να επιστρέψει τις πληροφορίες στις διεργασίες που εξυπηρετεί. Το τελευταίο αποτελείται από:

(α) γενικές πληροφορίες για μια σύνδεση (π.χ. διακοπές, μακρινό κλείσιμο, δέσμευση του απροσδιόριστου ξένου socket).

(β) απαντήσεις στις συγκεκριμένες εντολές χρηστών που δείχνουν επιτυχία ή στους διάφορους τύπους αποτυχιών.

Open

Σχήμα: OPEN (τοπικό port, ξένο socket, ενεργό /παθητικό [διακοπή]
[προτεραιότητα] [ασφάλεια /compartments] [επιλογές]) -> τοπικό όνομα σύνδεσης.

Υποθέτουμε ότι το τοπικό TCP γνωρίζει την ταυτότητα των διαδικασιών που εξυπηρετεί και θα ελέγξει την αρχή της διαδικασίας για να χρησιμοποιήσει τη σύνδεση που διευκρινίζεται. Ανάλογα με την εφαρμογή του TCP, το τοπικό δίκτυο και τα προσδιοριστικά του TCP για τη διεύθυνση πηγής είτε θα παρασχεθούν από το TCP είτε το χαμηλότερο επίπεδο πρωτοκόλλου (π.χ. IP). Αυτές οι εκτιμήσεις είναι το αποτέλεσμα της ανησυχίας για την ασφάλεια, μέχρι το σημείο που κανένα TCP να μην είναι σε θέση να μεταμφιεστεί σαν ένα άλλο ένα, και τα λοιπά. Ομοίως, καμία διαδικασία δεν μπορεί να μεταμφιεστεί σαν άλλη χωρίς τη συνεργία του TCP.

Εάν το ενεργό/ παθητικό flag τίθεται στο παθητικό, κατόπιν αυτό είναι μια κλήση για να ΑΚΟΥΣΕΙ μια εισερχόμενη σύνδεση. Ένα παθητικό άνοιγμα μπορεί να έχει είτε ένα πλήρως διευκρινισμένο socket για να περιμένει μια ιδιαίτερη σύνδεση είτε ένα απροσδιόριστο socket να περιμένει οποιαδήποτε κλήση. Μια πλήρως διευκρινισμένη παθητική κλήση μπορεί να γίνει ενεργή από την επόμενη εκτέλεση ενός SEND. Ένας φραγμός ελέγχου μετάδοσης (TCB) δημιουργείται και γεμίζει μερικώς με τα δεδομένα από τις ΑΝΟΙΚΤΕΣ παραμέτρους εντολής. Σε μια ενεργό ΑΝΟΙΚΤΗ εντολή, το TCP θα αρχίσει τη διαδικασία για να συγχρονίζει (δηλ., να καθιερώσει) τη σύνδεση αμέσως. Η διακοπή επιτρέπει στον επισκέπτη να οργανώσει μια διακοπή για όλα τα δεδομένα που υποβάλλονται στο TCP. Εάν τα δεδομένα δεν παραδίδονται επιτυχώς στον προορισμό εντός της περιόδου διακοπής, το TCP θα αποβάλει τη σύνδεση. Η παρούσα σφαιρική προεπιλογή είναι πέντε λεπτά. Το TCP ή κάποιο συστατικό του λειτουργικού συστήματος θα ελέγξει την αρχή χρηστών για να ανοίξει μια σύνδεση με τη διευκρινισμένη προτεραιότητα ή την ασφάλεια/ compartment. Η απουσία προτεραιότητας ή η προδιαγραφή ασφάλειας/compartment στην ΑΝΟΙΚΤΗ κλήση δείχνει ότι οι προκαθορισμένες τιμές πρέπει να χρησιμοποιηθούν. Το TCP θα δεχτεί τα εισερχόμενα αιτήματα ότι ταιριάζουν μόνο εάν η πληροφορία ασφάλειας/ compartments είναι ακριβώς οι ίδιες και μόνο εάν η προτεραιότητα είναι ίση ή υψηλότερη από την προτεραιότητα που ζητείται στην ΑΝΟΙΚΤΗ κλήση.

Η προτεραιότητα για τη σύνδεση είναι η υψηλότερη των τιμών που ζητούνται στην ΑΝΟΙΚΤΗ κλήση και παραλαμβάνεται από το εισερχόμενο αίτημα, και είναι σταθερή σε εκείνη την τιμή για τη ζωή της σύνδεσης. Οι εφαρμοστές μπορεί να θελήσουν να δώσουν στο χρήστη τον έλεγχο αυτής της διαπραγμάτευσης προτεραιότητας. Παραδείγματος χάριν, ο χρήστης να έχει την άδεια για να διευκρινίσει ότι η προτεραιότητα πρέπει ακριβώς να αντιστοιχηθεί, ή ότι οποιαδήποτε προσπάθεια να αυξηθεί η προτεραιότητα να επιβεβαιώνεται από το χρήστη. Ένα τοπικό όνομα σύνδεσης θα επιστραφεί στο χρήστη από το TCP. Το τοπικό όνομα σύνδεσης μπορεί έπειτα να χρησιμοποιηθεί ως όρος short hand για τη σύνδεση που καθορίζεται από το ζευγάρι < τοπικό socket, ξένο socket > .

SEND

Σχήμα: SEND (τοπικό όνομα σύνδεσης, διεύθυνση buffer, αρίθμηση byte, σημαία PUSH, ΕΠΕΙΓΟΥΣΑ σημαία [διάλειμμα])

Αυτή η κλήση αναγκάζει τα δεδομένα που περιλαμβάνονται στον υποδεδειγμένο buffer χρηστών να σταλούν στην υποδεδειγμένη σύνδεση. Εάν η σύνδεση δεν έχει ανοιχτεί, το SEND θεωρείται λάθος. Μερικές εφαρμογές μπορεί να επιτρέπουν στους χρήστες ΝΑ ΣΤΕΙΛΟΥΝ πρώτα, οπότε σ'αυτή την περίπτωση,

αυτόματα ένα OPEN θα γινόταν. Εάν η καλούμενη διεργασία δεν είναι εξουσιοδοτημένη να χρησιμοποιήσει αυτήν την σύνδεση, επιστρέφεται ένα λάθος.

Εάν τεθεί η PUSH flag, τα δεδομένα πρέπει να διαβιβαστούν αμέσως στον αποδέκτη και το bit PUSH θα τεθεί στο τελευταίο τμήμα του TCP που δημιουργείται από τον buffer. Εάν η PUSH flag δεν έχει τεθεί, τα δεδομένα μπορούν να συνδυαστούν με τα δεδομένα από τα επόμενα SENDs για την αποδοτικότητα μετάδοσης. Εάν τίθεται η επείγον flag, τα τμήματα που στέλνονται στο προορισμένο TCP θα θέσουν τον επείγοντα δείκτη. Το λαμβάνον TCP θα επισημάνει την επείγουσα κατάσταση στη λαμβάνουσα διεργασία εάν ο επείγων δείκτης δείξει ότι τα δεδομένα που προηγούνται του επείγοντος δείκτη δεν έχουν καταναλωθεί με τη λαμβάνουσα διαδικασία.

Ο σκοπός του σήματος επείγον είναι να υποκινηθεί ο δέκτης για να επεξεργαστεί τα επείγοντα δεδομένα και να δείξει στο δέκτη πότε θα παραληφθούν όλα τα πρόσφατα γνωστά επείγοντα δεδομένα. Ο αριθμός των σταλμένων επειγόντων TCP σημάτων του χρήστη δε θα είναι απαραιτήτως ίσος με τον αριθμό των φορών που ο λαμβάνων χρήστης θα ενημερωθεί για την παρουσία επειγόντων δεδομένων.

Εάν κανένα ξένο socket δε διευκρινίστηκε στο OPEN, αλλά η σύνδεση έχει καθιερωθεί (π.χ. επειδή μια σύνδεση LISTENing έχει γίνει συγκεκριμένη εξ'αιτίας ενός ξένου τμήματος που έφτασε για το τοπικό socket), κατόπιν ο οριζόμενος buffer στέλνεται στο υπονοούμενο ξένο socket. Οι χρήστες που χρησιμοποιούν το OPEN με ένα απροσδιόριστο ξένο socket μπορούν να χρησιμοποιήσουν το SEND χωρίς πάντα ρητά να ξέρουν την ξένη διεύθυνση του socket. Εντούτοις, εάν ένα SEND επιχειρηθεί προτού το ξένο socket να διευκρινιστεί, θα επιστραφεί ένα λάθος. Οι χρήστες μπορούν να χρησιμοποιήσουν την κλήση STATUS για να καθορίσουν την κατάσταση της σύνδεσης. Σε μερικές εφαρμογές το TCP μπορεί να ειδοποιήσει το χρήστη όταν ένα απροσδιόριστο socket είναι συνδεδεμένο.

Εάν μια διακοπή διευκρινίζεται, το τρέχον διάλειμμα χρηστών για αυτήν τη σύνδεση αλλάζει στη νέα. Στην απλούστερη εφαρμογή, το SEND δεν θα επέστρεφε τον έλεγχο στη διαδικασία αποστολής έως ότου είτε η μετάδοση ολοκληρωνόταν ή η διακοπή είχε παρέλθει. Εντούτοις, αυτή η απλή μέθοδος υπόκειται και στα αδιέξοδα (παραδείγματος χάριν, και οι δύο πλευρές της σύνδεσης να προσπαθήσουν να κάνουν SENDs πρίν κάνουν οποιοδήποτε RECEIVE) και προσφέρει κακή απόδοση, έτσι δεν συστήνεται. Μια περιπλοκότερη εφαρμογή θα επέστρεφε αμέσως για να επιτρέψει στη διεργασία να τρέξει ταυτόχρονα με το δίκτυο I/O, και, επιπλέον, να επιτρέψει πολλαπλά SENDs να είναι υπό εξέλιξη. Πολλαπλά SENDs εξυπηρετούνται σύμφωνα με την πολιτική 'αυτός που έρχεται πρώτος, εξυπηρετείται πρώτος' , έτσι το TCP θα τοποθετήσει στη σειρά εκείνα που δεν μπορεί να συντηρήσει αμέσως.

Έχουμε υποθέσει σιωπηρά μια ασύγχρονη διεπαφή χρήστη στην οποία ένα SEND αποσπά αργότερα κάποιο είδος σήματος ή ψευδο-διακόπτουμε το TCP από την εξυπηρέτηση. Μια εναλλακτική λύση είναι να επιστραφεί μια απάντηση αμέσως. Παραδείγματος χάριν, τα SENDs να επιστρέψουν μια άμεση τοπική αναγνώριση, ακόμα κι αν το τμήμα που εστάλη δεν ήταν αναγνωρισμένο από το απόμακρο TCP. Θα μπορούσαμε αισιόδοξα να υποθέσουμε την ενδεχόμενη επιτυχία. Εάν κάνουμε λάθος, η σύνδεση θα κλείσει οπωσδήποτε λόγω της διακοπής. Στις εφαρμογές αυτού του είδους (σύγχρονου), θα υπάρχουν ακόμα μερικά ασύγχρονα σήματα, αλλά αυτά έχουν να κάνουν με τη σύνδεση, και όχι με τα συγκεκριμένα τμήματα ή τους buffers. Για τη διαδικασία διάκρισης μεταξύ των ενδείξεων λάθους ή επιτυχίας για διαφορετικά SENDs, είναι αρμόζον για τη διεύθυνση του buffer να επιστραφεί μαζί

με την κωδικοποιημένη απάντηση στο SEND αίτημα. Τα σήματα από το TCP στο χρήστη συζητούνται κατωτέρω, δείχνοντας τις πληροφορίες που πρέπει να επιστραφούν στην καλούμενη διεργασία.

RECEIVE

Σχήμα: RECEIVE (τοπικό όνομα σύνδεσης, διεύθυνση buffer, αρίθμηση byte) -> αρίθμηση byte, επείγον flag, push flag

Αυτή η εντολή διαθέτει έναν λαμβάνοντα buffer που συνδέεται με τη διευκρινισμένη σύνδεση. Εάν κανένα OPEN δεν προηγείται αυτής της εντολής ή η καλούμενη διεργασία δεν εξουσιοδοτείται να χρησιμοποιήσει αυτήν την σύνδεση, επιστρέφεται ένα λάθος.

Στην απλούστερη εφαρμογή, ο έλεγχος δε θα επέστρεφε στο καλούμενο πρόγραμμα έως ότου είτε γέμιζε ο buffer, ή κάποιο λάθος εμφανιζόταν, αλλά αυτό το σχέδιο υπόκειται ιδιαίτερα στα αδιέξοδα. Μια πιο περίπλοκη εφαρμογή θα επέτρεπε σε διάφορα RECEIVEs να γίνονταν αμέσως εκκρεμή. Αυτά θα γέμιζαν καθώς τα τμήματα έφθαναν. Αυτή η στρατηγική επιτρέπει την αύξηση της ρυθμαπόδοσης με το κόστος ενός πιο επιμελημένου σχεδίου (ενδεχομένως ασύγχρονου) να δηλωθεί το καλούμενο πρόγραμμα ότι μια PUSH έχει φανεί ή ένας buffer είναι γεμάτος. Εάν αρκετά δεδομένα φθάσουν για να γεμίσουν τον buffer πριν να φανεί μια PUSH, το flag push δε θα τεθεί σαν απάντηση στο RECEIVE. Ο buffer θα γεμίσει με όσο δυνατόν περισσότερα δεδομένα μπορεί να κρατήσει. Εάν μια PUSH εμφανιστεί προτού να γεμίσει ο buffer, ο buffer θα επιστραφεί μερικώς γεμάτος και η PUSH θα ενεργοποιηθεί.

Εάν υπάρχει επείγον δεδομένο ο χρήστης θα έχει ενημερωθεί μόλις φτάσει μέσω ενός σήματος TCP-σε-χρήστη. Ο λαμβάνον χρήστης πρέπει να είναι σε "επείγουσα κατάσταση". Εάν το επείγον flag είναι ανοικτό, το πρόσθετο επείγον δεδομένο παραμένει. Εάν το επείγον flag είναι κλειστό, αυτή η κλήση ΠΟΥ ΛΑΜΒΑΝΕΙ έχει επιστρέψει όλα τα επείγοντα δεδομένα, και ο χρήστης μπορεί τώρα να αφήσει το "επείγοντα τρόπο". Σημειώνουμε ότι τα δεδομένα μετά από τον επείγοντα δείκτη (μη-επείγοντα δεδομένα) δεν μπορούν να παραδοθούν στο χρήστη στον ίδιο buffer με τα επείγοντα δεδομένα εκτός αν το όριο είναι σαφώς μαρκαρισμένο για το χρήστη. Για να γίνει διάκριση μεταξύ διάφορων σημαντικών RECEIVEs και για να φροντίσει την περίπτωση που ένας buffer δε γεμίζει εντελώς, ο επιστρεφόμενος κώδικας συνοδεύεται από έναν δείκτη buffer και από μια αρίθμηση byte που δείχνουν το πραγματικό μήκος των λαμβανόμενων δεδομένων. Οι εναλλακτικές εφαρμογές του RECEIVE ίσως να έχουν το TCP να διαθέτει αποθήκευση buffer, ή το TCP να μοιραστεί έναν buffer δαχτυλίου με το χρήστη.

Close

Σχήμα: CLOSE (τοπικό όνομα σύνδεσης)

Αυτή η εντολή προκαλεί τη συγκεκριμένη σύνδεση να κλείσει. Εάν η σύνδεση δεν είναι ανοικτή ή η καλούμενη διεργασία δεν είναι εξουσιοδοτημένη να χρησιμοποιήσει αυτήν την σύνδεση, επιστρέφεται ένα λάθος. Το κλείσιμο των συνδέσεων είναι μια λειτουργία κατά την οποία σημαντικά SENDs θα διαβιβαστούν

(και θα ξαναδιαβιβασθούν), όπως ο έλεγχος ροής επιτρέπει, έως ότου έχουν εξυπηρετηθεί όλες. Κατά συνέπεια, πρέπει να είναι αποδεκτό να κάνουν διάφορες SEND κλήσεις, που ακολουθούνται από ένα CLOSE, και να αναμείνουν όλα τα δεδομένα να σταλούν στον προορισμό. Πρέπει επίσης να είναι σαφές ότι οι χρήστες πρέπει να συνεχίσουν ΝΑ ΛΑΜΒΑΝΟΥΝ στο ΚΛΕΙΣΙΜΟ των συνδέσεων, δεδομένου ότι η άλλη πλευρά μπορεί να προσπαθεί να διαβιβάσει τα τελευταία δεδομένα της. Κατά συνέπεια, CLOSE σημαίνει "δεν έχω άλλα να στείλω" αλλά δεν σημαίνει ότι "δεν θα λάβω άλλα.". Μπορεί να συμβεί (εάν το πρωτόκολλο επιπέδων χρηστών δεν θεωρείται καλά εξετασμένο) το γεγονός ότι η πλευρά κλεισίματος είναι ανίκανη να ξεφορτωθεί όλα τα δεδομένα της πριν τελειώσει ο χρόνος. Σε αυτό το γεγονός, το CLOSE μετατρέπεται σε ABORT, και το TCP κλεισίματος σταματά.

Ο χρήστης μπορεί ΝΑ ΚΛΕΙΣΕΙ τη σύνδεση οποιαδήποτε στιγμή με δική του πρωτοβουλία, ή σε απάντηση στις διάφορες υπαγορεύσεις από το TCP (π.χ. μακρινό κλείσιμο εκτελεσμένο, υπερβαίνουσα διακοπή μετάδοσης, προορισμός απρόσιτος). Επειδή το κλείσιμο μιας σύνδεσης απαιτεί την επικοινωνία με το ξένο TCP, οι συνδέσεις μπορούν να παραμείνουν στην κατάσταση κλεισίματος για σύντομο χρόνο. Οι προσπάθειες να ανοιχτεί πάλι η σύνδεση πριν από την απάντηση του TCP στην εντολή CLOSE θα οδηγήσουν σε λάθος απαντήσεις. Το κλείσιμο επίσης υπονοεί τη συνάρτηση push.

Κατάσταση

Σχήμα: ΚΑΤΑΣΤΑΣΗ (τοπικό όνομα σύνδεσης) -> δεδομένα κατάστασης

Αυτή είναι μια εξαρτώμενη εντολή χρηστών και θα μπορούσε να αποκλειστεί χωρίς δυσμενή συνέπεια. Οι πληροφορίες επιστρεφόμενες θα προέρχονταν τυπικά από το TCB που συνδέεται με τη σύνδεση. Αυτή η εντολή επιστρέφει ένα σύνολο δεδομένων που περιέχει τις ακόλουθες πληροφορίες:

τοπικό socket,

ξένο socket,

τοπικό όνομα σύνδεσης,

λαμβανόμενο window,

σταλμένο window,

κατάσταση σύνδεσης,

αριθμός buffers που αναμένουν την αναγνώριση,

αριθμός buffers εν αναμονή της παραλαβής,

επείγουσα κατάσταση,

προτεραιότητα,

ασφάλεια/ compartment

και διακοπή μετάδοσης.

Ανάλογα με την κατάσταση της σύνδεσης, ή η ίδια η εφαρμογή, μερικές από αυτές τις πληροφορίες μπορεί να μην είναι διαθέσιμες ή σημαντικές. Εάν η καλούμενη διεργασία δεν εξουσιοδοτείται για να χρησιμοποιήσει αυτήν την σύνδεση,

επιστρέφεται ένα λάθος. Αυτό αποτρέπει τις αναρμόδιες διεργασίες από τη λήψη πληροφοριών για μια σύνδεση.

ABORT

Σχήμα: ABORT (τοπικό όνομα σύνδεσης)

Αυτή η εντολή προκαλεί όλο εκκρεμή SENDs και RECEIVEs για να αποβληθούν, το TCB που αφαιρείται, και ένα ειδικό μήνυμα reset που στέλνεται στο TCP στην άλλη πλευρά της σύνδεσης. Ανάλογα με την εφαρμογή, οι χρήστες μπορούν να λάβουν ενδείξεις αποβολής για κάθε εκκρεμές SEND ή RECEIVE, ή μπορούν απλά να λάβουν μια αποβολή –αναγνώριση.

Μηνύματα TCP-σε-χρήστη

Υποτίθεται ότι το περιβάλλον του λειτουργικού συστήματος παρέχει μέσα για το TCP ασύγχρονα το πρόγραμμα χρηστών. Όταν το TCP επισημαίνει ένα πρόγραμμα χρηστών, ορισμένες πληροφορίες περνούν στο χρήστη. Συχνά στην προδιαγραφή οι πληροφορίες θα είναι ένα μήνυμα λάθους. Σε άλλες περιπτώσεις θα υπάρξουν πληροφορίες σχετικά με την ολοκλήρωση της επεξεργασίας ενός SEND ή RECEIVE ή άλλης κλήσης χρηστών.

Παρέχονται οι ακόλουθες πληροφορίες :

Τοπικό όνομα σύνδεσης	πάντα
String απάντησης	πάντα
Η διεύθυνση buffer	στέλνει & λαμβάνει
Η αρίθμηση byte (αρίθμηση λαμβανόμενων byte)	λαμβάνει
Push flag	λαμβάνει
Επείγον flag	λαμβάνει

Διεπαφή TCP/χαμηλού επίπεδου

Το TCP καλεί ένα χαμηλότερου επιπέδου πρωτόκολλο για να στείλει και να λάβει τις πληροφορίες πέρα από ένα δίκτυο. Μια περίπτωση είναι αυτή του συστήματος ARPAS internetwork όπου η χαμηλότερη ενότητα επιπέδων είναι το πρωτόκολλο Διαδικτύου (IP). Εάν το χαμηλότερο επίπεδο πρωτοκόλλου είναι IP παρέχει τα επιχειρήματα για έναν τύπο υπηρεσίας και για έναν χρόνο ζωής. Το TCP χρησιμοποιεί τις ακόλουθες τοποθετήσεις για αυτές τις παραμέτρους:

Τύπος υπηρεσίας = προτεραιότητα: ρουτίνα, καθυστέρηση: κανονική, ρυθμαπόδοση: κανονική, αξιοπιστία: κανονική ή 00000000.

Χρόνος ζωής = ένα λεπτό, ή 00111100.

Σημειώνουμε ότι η υποτιθέμενη μέγιστη διάρκεια ζωής τμήματος είναι δύο λεπτά. Εδώ ζητάμε ρητά να καταστραφεί ένα τμήμα εάν δεν μπορεί να παραδοθεί από το σύστημα Διαδικτύου μέσα σε ένα λεπτό.

Εάν το χαμηλότερο επίπεδο είναι IP (ή άλλο πρωτόκολλο που παρέχει αυτό το χαρακτηριστικό γνώρισμα) και χρησιμοποιείται δρομολόγηση πηγής, η διεπαφή πρέπει να επιτρέψει στις πληροφορίες διαδρομών να μεταβιβαστούν. Αυτό είναι ιδιαίτερα σημαντικό έτσι ώστε οι διευθύνσεις πηγής και προορισμού που χρησιμοποιείται checksum TCP είναι η αρχική πηγή και ο τελευταίος προορισμός. Είναι επίσης σημαντικό να συντηρηθεί η διαδρομή επιστροφής για να απαντήσει στα αιτήματα σύνδεσης. Οποιοδήποτε χαμηλότερου επιπέδου πρωτόκολλο θα πρέπει να παρέχει τη διεύθυνση πηγής, τη διεύθυνση προορισμού, και τα πεδία πρωτοκόλλου, και κάποιο τρόπο να αποφασιστεί το "μήκος του TCP", για να παρέχει τη λειτουργική ισοδύναμη υπηρεσία του IP και για να χρησιμοποιηθεί checksum TCP.

5 Internet Protocol (IP)

Το πρωτόκολλο Διαδικτύου σχεδιάζεται για τη χρήση στα διασυνδεόμενα συστήματα των packet-switched δικτύων επικοινωνίας υπολογιστών. Ένα τέτοιο σύστημα έχει κληθεί "catenet". Το πρωτόκολλο Διαδικτύου παρέχει τη διαβίβαση των φραγμών αποκαλούμενων datagrams από τις πηγές στους προορισμούς, όπου οι πηγές και οι προορισμοί είναι οι hosts που προσδιορίζονται από τις σταθερού μήκους διευθύνσεις. Επιτρέπει επίσης τον τεμαχισμό και την επανασυναρμολόγηση των μακριών datagrams, εάν είναι απαραίτητο, για τη μετάδοση μέσω των δικτύων "μικρών πακέτων".

Το πρωτόκολλο Διαδικτύου είναι συγκεκριμένα περιορισμένο στο πεδίο για να παρέχει τις απαραίτητες λειτουργίες ώστε να παραδώσουν πακέτα bits από μια πηγή σε έναν προορισμό ενός διασυνδεόμενου συστήματος δικτύων. Δεν υπάρχει κανένας μηχανισμός για να αυξήσει την αξιοπιστία των end-to-end δεδομένων, αλληλουχίας, ελέγχου ροής ή άλλες υπηρεσίες που βρίσκονται συνήθως στα host to host πρωτόκολλα. Το πρωτόκολλο Διαδικτύου μπορεί να κεφαλαιοποιήσει στις υπηρεσίες των δικτύων υποστήριξης του για να παρέχει τους διάφορους τύπους και ιδιότητες της υπηρεσίας.

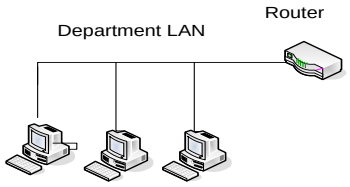
Αυτό το πρωτόκολλο καλείται από τα host to host πρωτόκολλα σε ένα περιβάλλον Διαδικτύου. Αυτό το πρωτόκολλο καλεί τα τοπικά πρωτόκολλα δικτύων για να μεταφέρουν το internet datagram στον επόμενο gateway ή host προορισμό. Παραδείγματος χάριν, μια ενότητα TCP θα καλούσε την ενότητα Διαδικτύου για να πάρει ένα τμήμα TCP (συμπεριλαμβανομένων του TCP header και των δεδομένων των χρηστών) ως αναλογία δεδομένων ενός internet datagram. Η ενότητα TCP θα παρείχε τις διευθύνσεις και άλλες παραμέτρους στην header Διαδικτύου στην ενότητα Διαδικτύου ως επιχειρήματα της κλήσης. Η ενότητα Διαδικτύου θα δημιουργούσε έπειτα ένα internet datagram και θα καλούσε την τοπική διεπαφή δικτύου για να διαβιβάσει το datagram.

5.1 Δίκτυο των χαμηλότερων πλειοδοτών

Το πρωτόκολλο Διαδικτύου αναπτύχθηκε για να δημιουργήσει ένα δίκτυο των δικτύων (το "Διαδίκτυο"). Οι μεμονωμένες μηχανές συνδέονται αρχικά με το τοπικό LAN (Ethernet). Το TCP/ IP μοιράζεται το LAN με άλλες χρήσεις. Μια συσκευή παρέχει τη σύνδεση TCP/IP μεταξύ του LAN και του υπόλοιπου κόσμου.

Για να εξασφαλίσει ότι όλοι οι τύποι συστημάτων από όλους τους προμηθευτές μπορούν να επικοινωνήσουν, το TCP/IP είναι απολύτως τυποποιημένο στο LAN. Εντούτοις, τα μεγαλύτερα δίκτυα βασισμένα στις μεγάλες αποστάσεις και τις τηλεφωνικές γραμμές είναι πιο πτητικά. Στις ΗΠΑ, πολλές μεγάλες εταιρίες θα επιθυμούσαν να επαναχρησιμοποιήσουν τα μεγάλα εσωτερικά δίκτυα βασισμένα στο SNA της IBM. Στην Ευρώπη, οι εθνικές τηλεφωνικές επιχειρήσεις τυποποιούν παραδοσιακά στη X.25. Εντούτοις, η ξαφνική έκρηξη των μικροεπεξεργαστών υψηλής ταχύτητας, των οπτικών ινών, και των ψηφιακών τηλεφωνικών συστημάτων

έχει δημιουργήσει μια έκρηξη των νέων επιλογών: ISDN, FDDI, τρόπος ασύγχρονης μεταφοράς (ATM). Οι νέες τεχνολογίες προκύπτουν και γίνονται ξεπερασμένες μέσα σε μερικά έτη. Με τις επιχειρήσεις καλωδιακής τηλεόρασης και τηλεφώνων που ανταγωνίζονται για να χτίσουν την εθνική λωρίδα ταχείας κυκλοφορίας πληροφοριών, κανένα πρότυπο δεν μπορεί να κυβερνήσει τις αστικού, εθνικού ή παγκόσμιου επιπέδου επικοινωνίες.



Το αρχικό σχέδιο του TCP/IP ως δίκτυο των δικτύων εγκαθίσταται ωραία μέσα στην τρέχουσα τεχνολογική αβεβαιότητα. Τα δεδομένα TCP/IP μπορούν να σταλούν κατά μήκος ενός LAN, ή μπορούν να μεταφερθούν μέσα σε ένα εσωτερικό εταιρικό δίκτυο SNA. Επιπλέον, οι μηχανές που συνδέονται με οποιαδήποτε από αυτά τα δίκτυα μπορούν να επικοινωνήσουν με οποιοδήποτε άλλο δίκτυο μέσω των gateways που παρέχονται από τον προμηθευτή δικτύων.

5.2 IP Addressing

Κάθε υπολογιστής υπηρεσίας και δρομολογητής στο Internet έχει μια διεύθυνση IP, η οποία κωδικοποιεί τον αριθμό δικτύου και τον αριθμό υπολογιστή υπηρεσίας. Ο συνδυασμός είναι μοναδικός : η ιδέα είναι ότι δύο διαφορετικές μηχανές στο Internet δε θα έχουν ποτέ την ίδια διεύθυνση IP. Όλες οι διευθύνσεις IP έχουν μήκος 32 bit, και χρησιμοποιούνται στα πεδία *Διεύθυνση προέλευσης* και *Διεύθυνση προορισμού* των πακέτων IP. Είναι σημαντικό να σημειώσουμε ότι η διεύθυνση IP δεν αναφέρεται ουσιαστικά σε έναν υπολογιστή υπηρεσίας. Στην πραγματικότητα αναφέρεται σε μια διασύνδεση δικτύου- έτσι, αν κάποιος υπολογιστής υπηρεσίας συνδέεται σε δύο δίκτυα, θα πρέπει να έχει δύο διευθύνσεις IP. Ωστόσο, στην πράξη οι περισσότεροι υπολογιστές βρίσκονται σε ένα μόνο δίκτυο και έτσι έχουν μόνο μία διεύθυνση IP.

Για πολλές δεκαετίες οι διευθύνσεις IP διαιρούνταν σε πέντε κατηγορίες. Αυτή η κατανομή ονομάζεται πλέον ταξική διευθυνσιοδότηση (classful addressing). Δε χρησιμοποιείται πια, αλλά είναι ακόμα συχνές οι αναφορές σε αυτή στη βιβλιογραφία.

Οι μορφές των τάξεων A, B, C επιτρέπουν αντίστοιχα μέχρι 128 δίκτυα με 16.777.214 υπολογιστές υπηρεσίας το καθένα, 16.384 δίκτυα με μέχρι 65.534 υπολογιστές και 2.097.152 δίκτυα (για παράδειγμα LAN) με μέχρι 254 υπολογιστές υπηρεσίας το καθένα (αν και ορισμένες διευθύνσεις έχουν ειδική χρήση). Οι κλάσεις D και E χρησιμοποιούνται για αιδικούς σκοπούς.

Το εύρος των κλάσεων είναι:

Class A: 1.0.0.0 – 127.255.255.255

Class B: 128.0.0.0 – 191.255.255.255

Class C: 192.0.0.0 – 223.255.255.255

Class D: 224.0.0.0 – 239.255.255.255

Class E: 240.0.0.0 – 255.255.255.255

Υποστηρίζεται και η πολυδιανομή, στην οποία ένα αυτοδύναμο πακέτο κατευθύνεται σε πολλούς υπολογιστές υπηρεσίας. Οι διευθύνσεις που αρχίζουν με 1111 είναι δεσμευμένες για μελλοντική χρήσης. Αυτή τη στιγμή περισσότερα από 500.000 δίκτυα συνδέονται στο Internet, και ο αριθμός αυτός μεγαλώνει κάθε χρόνο. Τους αριθμούς δικτύων τους διαχειρίζεται μια μη κερδοσκοπική εταιρία που ονομάζεται Εταιρία Internet για Εκχωρημένα Ονόματα και Αριθμούς ή ICANN, με στόχο να αποφεύγονται οι διενέξεις. Με τη σειρά της, η ICANN έχει μεταβιβάσει περιοχές του χώρου διευθύνσεων σε διάφορες περιφερειακές αρχές, οι οποίες παρέχουν διευθύνσεις IP στους ISP και τις άλλες εταιρείες.

Οι διευθύνσεις δικτύου, οι οποίες είναι 32μπιτοι αριθμοί, συνήθως γράφονται σε δεκαδική γραφή με τελείες (dotted decimal notation). Στη μορφή αυτή, το καθένα από τα 4 byte γράφεται σε δεκαδική μορφή, με τιμές από 0 έως 255. Για παράδειγμα, η 32μπιτη δεκαεξαδική διεύθυνση C0290614 γράφεται ως 192.41.6.20. Η χαμηλότερη διεύθυνση IP είναι η 0.0.0.0, ενώ η υψηλότερη είναι η 255.255.255.255.

Οι τιμές 0 και -1 (όλα τα ψηφία 1) έχουν ειδικές σημασίες. Η τιμή 0 σημαίνει “ αυτό το δίκτυο” ή “αυτός ο υπολογιστής υπηρεσίας”. Η τιμή -1 χρησιμοποιείται ως διεύθυνση εκπομπής, και σημαίνει “ όλοι οι υπολογιστές στο συγκεκριμένο δίκτυο’’.

Υπάρχουν πειραματικές και ελεύθερα διαθέσιμες διευθύνσεις που δεν χρησιμοποιούνται για δρομολόγηση παρα μόνο σαν εσωτερικές διευθύνσεις δικτύου:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Η διεύθυνση IP 0.0.0.0 χρησιμοποιείται από τους υπολογιστές υπηρεσίας κατά την εκκίνησή τους. Οι διευθύνσεις IP με τιμή 0 ως αριθμό δικτύου αναφέρονται στο τρέχον δίκτυο. Οι διευθύνσεις αυτές επιτρέπουν στις μηχανές να αναφέρονται στο δίκτυό τους χωρίς να ξέρουν τον αριθμό του (θα πρέπει όμως να ξέρουν την τάξη του, ώστε να γνωρίζουν πόσα 0 να συμπεριλάβουν). Η διεύθυνση που αποτελείται μόνο από 1 επιτρέπει εκπομπή στο τοπικό δίκτυο, συνήθως ένα δίκτυο LAN. Οι διευθύνσεις με έναν κανονικό αριθμό δικτύου και μόνο ψηφία 1 στο πεδίο του υπολογιστή υπηρεσίας επιτρέπουν στις μηχανές να στέλνουν πακέτα εκπομπής σε απομακρυσμένα LAN οπουδήποτε στο Internet (αν και πολλοί διαχειριστές δικτύου απενεργοποιούν αυτή τη λειτουργία). Τέλος, όλες οι διευθύνσεις της μορφής 127.xx.xx.xx είναι δεσμευμένες για έλεγχο ανατροφοδότησης (loopback). Τα πακέτα που στέλνονται σε αυτή τη διεύθυνση

δεν τοποθετούνται στο καλώδιο, γίνεται τοπική επεξεργασία τους και αντιμετωπίζονται σαν εισερχόμενα πακέτα. Αυτό επιτρέπει σε πακέτα να στέλνονται στο τοπικό δίκτυο χωρίς ο αποστολέας να γνωρίζει τον αριθμό του. Κάθε τεχνολογία έχει τη σύμβασή της για τη διαβίβαση των μηνυμάτων μεταξύ δύο μηχανών μέσα στο ίδιο δίκτυο. Σε ένα LAN, τα μηνύματα στέλνονται μεταξύ των μηχανών με την παροχή του μοναδικού προσδιοριστικού των 6 byte (η διεύθυνση "MAC"). Σε ένα δίκτυο SNA, κάθε μηχανή έχει λογικές μονάδες με τη δική τους διεύθυνση δικτύου. Τα DECNET, Appletalk και Novell IPX έχουν ένα σχέδιο για την ανάθεση αριθμών σε κάθε τοπικό δίκτυο και σε κάθε τερματικό σταθμό που συνδέεται με το δίκτυο.

Πάνω από αυτές τις τοπικές ή συγκεκριμένες διευθύνσεις δικτύου, το TCP/IP ορίζει έναν μοναδικό αριθμό σε κάθε τερματικό σταθμό στον κόσμο. Αυτός ο "αριθμός IP" είναι μια τιμή τεσσάρων byte που, από σύμβαση, εκφράζεται με τη μετατροπή κάθε byte σε έναν δεκαδικό αριθμό (0 έως 255) και χωρίζοντας τα bytes με μια περίοδο. Παραδείγματος χάριν, ο PC Lube and Tune server είναι 130.132.59.234. Μία οργάνωση αρχίζει με την αποστολή ηλεκτρονικού ταχυδρομείου στο Hostmaster@INTERNIC.NET ζητώντας την ανάθεση ενός αριθμού δικτύου. Είναι ακόμα δυνατό για τον καθένα σχεδόν να πάρει ανάθεση ενός αριθμού για ένα μικρό δίκτυο "κλάσης C" στο οποίο τα 3 πρώτα bytes προσδιορίζουν το δίκτυο και το τελευταίο byte προσδιορίζει το μεμονωμένο υπολογιστή. Ο συντάκτης ακολούθησε αυτήν την διαδικασία και του ορίστηκαν οι αριθμοί 192.35.91.* για ένα δίκτυο υπολογιστών στο σπίτι του. Μεγαλύτερες οργανώσεις μπορούν να πάρουν ένα δίκτυο "κλάσης B" όπου τα 2 πρώτα bytes προσδιορίζουν το δίκτυο και τα τελευταία δύο bytes προσδιορίζουν το καθένα μέχρι 64 χιλιάδες μεμονωμένων τερματικών σταθμών. Το δίκτυο κλάσης B του Yale είναι 130.132, έτσι όλοι οι υπολογιστές με IP 130.132. *. * συνδέονται μέσω Yale.H οργάνωση συνδέεται έπειτα με το Διαδίκτυο μέσω ενός από μια δωδεκάδα περιφερειακών ή ειδικευμένων προμηθευτών δικτύου. Στον προμηθευτή δικτύων δίνεται ο αριθμός δικτύου συνδρομητών και το προσθέτει στη διαμόρφωση δρομολόγησης στις δικές του μηχανές του και σε άλλες, άλλων σημαντικών προμηθευτών δικτύου. Δεν υπάρχει κανένας μαθηματικός τύπος που μεταφράζει τους αριθμούς 192.35.91 ή 130.132 ‘στο πανεπιστήμιο Yale’ ή στο ‘New Haven, CT’. Οι μηχανές που διαχειρίζονται τα μεγάλα περιφερειακά δίκτυα ή τους κεντρικούς δρομολογητές Διαδικτύου διοικούμενους από το Εθνικό Ίδρυμα Επιστήμης μπορούν μόνο να εντοπίσουν αυτά τα δίκτυα με το να ανατρέξουν για κάθε αριθμό δικτύου σε έναν πίνακα. Υπάρχουν ενδεχομένως χιλιάδες δίκτυα κλάσης B, και εκατομμύρια δικτύων κλάσης C, αλλά οι δαπάνες για μνήμη υπολογιστών είναι χαμηλές, έτσι οι πίνακες είναι σε λογικά επίπεδα. Πελάτες που συνδέονται με το Διαδίκτυο, ακόμη και πελάτες τόσο μεγάλοι όσο η IBM, δε χρειάζεται να διατηρήσουν οποιεσδήποτε πληροφορίες για άλλα δίκτυα. Στέλνουν όλα τα εξωτερικά δεδομένα στον περιφερειακό μεταφορέα στα οποία προσυπογράφουν, και ο περιφερειακός μεταφορέας διατηρεί τους πίνακες και κάνει την κατάλληλη δρομολόγηση.

Υπάρχουν τρία επίπεδα γνώσης TCP/IP. Εκείνοι που διαχειρίζονται ένα περιφερειακό ή εθνικό δίκτυο πρέπει να σχεδιάσουν ένα σύστημα με μεγάλων αποστάσεων τηλεφωνικές γραμμές, συσκευών δρομολόγησης, και πολύ μεγάλων αρχείων διαμόρφωσης. Πρέπει να ξέρουν τους αριθμούς IP και τις φυσικές θέσεις χιλιάδων συνδρομητών δικτύων. Πρέπει επίσης να έχουν μια επίσημη στρατηγική οργάνων ελέγχου δικτύων για να ανιχνεύουν τα προβλήματα και να ανταποκρίνονται γρήγορα.

Κάθε μεγάλη επιχείρηση ή πανεπιστήμιο που προσυπογράφει στο Διαδίκτυο πρέπει να έχει ένα ενδιάμεσο επίπεδο οργάνωσης δικτύου και πείρας. Οι μισοί από μια

δωδεκάδα δρομολογητών μπορούν να διαμορφωθούν, έτσι ώστε να συνδέσουν αρκετές δωδεκάδες υπηρεσιακών LANs σε διάφορα κτίρια. Όλη η κυκλοφορία έξω από την οργάνωση θα καθοδηγούνταν τυπικά σε μια ενιαία σύνδεση σε έναν περιφερειακό προμηθευτή δικτύου. Εντούτοις, ο τελικός χρήστης μπορεί να εγκαταστήσει το TCP/IP σε έναν προσωπικό υπολογιστή χωρίς οποιαδήποτε γνώση είτε του εταιρικού είτε περιφερειακού δικτύου. Τρία κομμάτια πληροφοριών απαιτούνται:

1. η διεύθυνση IP που ορίζεται σε αυτόν τον προσωπικό υπολογιστή
2. το μέρος της διεύθυνσης IP (subnet mask) που διακρίνει άλλες μηχανές στο ίδιο LAN (τα μηνύματα μπορούν να σταλούν σε αυτά άμεσα) από τις μηχανές σε άλλα τμήματα ή αλλού στον κόσμο (που στέλνονται σε μια μηχανή δρομολογητών)
3. η διεύθυνση IP της μηχανής δρομολογητή που συνδέει αυτό το LAN με τον υπόλοιπο κόσμο.

Στην περίπτωση του server PCLT, η διεύθυνση IP είναι 130.132.59.234. Δεδομένου ότι τα πρώτα τρία bytes υποδεικνύουν αυτό το τμήμα, μια subnet mask ορίζεται ως 255.255.255.0 (255 είναι η μεγαλύτερη τιμή byte και αντιπροσωπεύει τον αριθμό με όλα τα bits ανεστραμμένα). Είναι μια σύμβαση του Yale ότι ο δρομολογητής για κάθε τμήμα έχει αριθμό σταθμού 1 μέσα στο δίκτυο τμημάτων. Επομένως ο δρομολογητής PCLT είναι 130.132.59.1. Κατά συνέπεια ο server PCLT διαμορφώνεται με τις τιμές:

- Η διεύθυνση IP μου: 130.132.59.234
- Subnet mask: 255.255.255.0
- δρομολογητής προεπιλογής: 130.132.59.1

Η subnet mask λέει στον server ότι οποιαδήποτε άλλη μηχανή με μία διεύθυνση IP που αρχίζει από 130.132.59.* είναι στο ίδιο LAN, έτσι τα μηνύματα στέλνονται σε αυτήν άμεσα. Οποιαδήποτε διεύθυνση IP που αρχίζει με μια διαφορετική τιμή προσεγγίζεται έμμεσα με την αποστολή του μηνύματος μέσω του δρομολογητή στο 130.132.59.1 (που είναι στο υπηρεσιακό LAN).

5.3 Δρομολόγηση

Το IP υποθέτει ότι ένα σύστημα είναι προσαρτημένο σε κάποιο τοπικό δίκτυο. Υποθέτουμε ότι το σύστημα μπορεί να στείλει datagrams σε ένα οποιοδήποτε άλλο σύστημα του δικτύου του. Το πρόβλημα δημιουργείται όταν ένα σύστημα πρέπει να στείλει datagram σε σύστημα που ανήκει σε διαφορετικό δίκτυο. Το πρόβλημα αυτό χειρίζονται τα gateways. Το gateway είναι ένα σύστημα που συνδέει ένα δίκτυο με ένα ή περισσότερα άλλα δίκτυα. Τα gateways είναι συνήθως κανονικοί υπολογιστές που έχουν περισσότερες από μια διεπαφές δικτύου. Για παράδειγμα, έχουμε μια μηχανή Unix που έχει δυο διαφορετικές Ethernet διεπαφές. Η μηχανή αυτή είναι έστω συνδεδεμένη με τα δίκτυα 128.6.4 και 128.6.3. Η μηχανή μπορεί να παίξει το ρόλο ενός gateway για τα δυο δίκτυα. Το s/w της μηχανής αυτής πρέπει

να φροντίζει ώστε να μπορούν να προωθηθούν datagrams από το ένα δίκτυο στο άλλο.
Έτσι, αν μια μηχανή του δικτύου 128.6.4 στείλει ένα datagram στο gateway και το datagram απευθύνεται σε μια μηχανή στο δίκτυο 128.6.3, το gateway θα προωθήσει το datagram στον προορισμό του. Τα μεγάλα κέντρα επικοινωνιών έχουν συχνά gateways, για να συνδέουν έναν αριθμό διαφορετικών δικτύων.

Η δρομολόγηση στο IP βασίζεται ολοκληρωτικά στο νούμερο του δικτύου που υπάρχει στη διεύθυνση προορισμού. Κάθε υπολογιστής διαθέτει ένα πίνακα αριθμών των δικτύων. Για κάθε αριθμό δικτύου είναι καταχωρημένο και ένα gateway. Αυτό είναι το gateway που θα χρησιμοποιηθεί ώστε να έχουμε πρόσβαση στο συγκεκριμένο δίκτυο.
Όταν ένας υπολογιστής θέλει να στείλει ένα datagram ελέγχει πρώτα αν η διεύθυνση προορισμού ανήκει σε σύστημα που βρίσκεται στο τοπικό δίκτυο. Αν ναι, το datagram στέλνεται απευθείας. Αλλιώς, το σύστημα περιμένει να βρει μια καταχώρηση για το δίκτυο στο οποίο βρίσκεται το σύστημα με τη συγκεκριμένη διεύθυνση. Το datagram στέλνεται τότε στο gateway που υπάρχει στην αντίστοιχη καταχώρηση. Ο πίνακας αυτός μπορεί να γίνει αρκετά μεγάλος. Ειδικά τώρα, που το Internet περιέχει τώρα αρκετές εκατοντάδες διαφορετικά δίκτυα. Έτσι, έχουν αναπτυχθεί πολλές στρατηγικές για τη μείωση του μεγέθους του πίνακα δρομολογήσεων. Μια στρατηγική είναι η χρησιμοποίηση default δρόμων. Συχνά, υπάρχει μόνο ένα gateway σε ένα δίκτυο που μπορεί για παράδειγμα να συνδέει ένα τοπικό Ethernet σε ένα ευρύτερο δίκτυο ενός πανεπιστημίου. Στην περίπτωση αυτή, δεν απαιτείται ξεχωριστή καταχώρηση για κάθε δίκτυο στον κόσμο. Δηλώνουμε απλά το gateway αυτό σαν default. Όταν δεν υπάρχει κάποιος καθορισμένος δρόμος για ένα datagram, το datagram στέλνεται στο default gateway. Default gateway μπορεί επίσης να χρησιμοποιηθεί ακόμα κι όταν υπάρχουν περισσότερα gateways σε ένα δίκτυο. Έχει προβλεφθεί η αποστολή μηνυμάτων από τα gateways, του τύπου δεν είμαι το καλύτερο gateway - χρησιμοποιήστε καλύτερα το τάδε (τα μηνύματα αυτά αποστέλλονται μέσω του ICMP). Τα περισσότερα s/w δικτύων έχουν σχεδιαστεί ώστε να χρησιμοποιούν αυτά τα μηνύματα και να προσθέτουν καταχωρήσεις στους πίνακες δρομολόγησής τους. Ας υποθέσουμε ότι το δίκτυο 128.6.4 έχει δυο gateways, τα 128.6.4.59 και 128.6.4.1. Το 128.6.4.59 οδηγεί σε διάφορα άλλα εσωτερικά δίκτυα του Rutgers. Το 128.6.4.1 οδηγεί στο NSFnet. Ας υποθέσουμε ότι έχουμε θέσει σαν default gateway το 128.6.4.59 και δεν υπάρχουν άλλες καταχωρήσεις στον πίνακα δρομολογήσεων. Τι θα συμβεί όταν χρειαστεί να στείλουμε ένα datagram στο MIT; Το MIT είναι το δίκτυο 18. Εφόσον δεν υπάρχει καταχώρηση για το δίκτυο 18 το datagram θα σταλεί στο default 128.6.4.59.
Φυσικά, το gateway αυτό είναι λάθος για την περίπτωση. Έτσι, το datagram θα προωθηθεί στο 128.6.4.1. Θα σταλεί όμως πίσω ένα σφάλμα που θα λέει: για να φτάσεις στο δίκτυο 18, χρησιμοποίησε το 128.6.4.1. Το s/w του δικτύου λοιπόν θα προσθέσει μια καταχώρηση στον πίνακα δρομολογήσεων. Οποιοδήποτε μελλοντικό datagram προς το MIT θα πάει απευθείας στο 128.6.4.1.
Οι περισσότεροι ειδικοί στο IP συνιστούν ότι οι μεμονωμένοι υπολογιστές δεν πρέπει να προσπαθούν να κρατούν πληροφορίες για όλο το δίκτυο. Αντί γι αυτό θα πρέπει να ξεκινούν με τα default gateways και να αφήνουν τα gateways να βρίσκουν τους καλύτερους δρόμους, όπως μόλις περιγράφηκε. Βέβαια, δεν έχουμε μιλήσει ακόμα με πιο τρόπο προσδιορίζονται οι καλύτεροι δρόμοι. Για να γίνει αυτό χρειάζεται κάποιο πρωτόκολλο δρομολόγησης. Το πρωτόκολλο αυτό είναι μια τεχνική ώστε τα gateways να μπορούν να εντοπίζουν το ένα το άλλο και να είναι ενημερωμένα για τον καλύτερο τρόπο που υπάρχει ώστε να προσπελαστεί το καθένα από αυτά.

Το πρωτόκολλο IP είναι υπεύθυνο για το πέρασμα ενός πακέτου δεδομένων από υπολογιστή σε υπολογιστή. Όλα τα δίκτυα που συνδέονται στο Internet "καταλαβαίνουν" τη γλώσσα IP κι έτσι μπορούν να συνεννοούνται και να ανταλλάσσουν δεδομένα με ομοιόμορφο τρόπο.

Τα δίκτυα του Internet συνδέονται μεταξύ τους με ειδικούς υπολογιστές που ονομάζονται δρομολογητές (routers) ή πύλες (gateways). Ένας router είναι λοιπόν ένας υπολογιστής που συνδέει δύο ή περισσότερα δίκτυα (που μπορεί να είναι διαφορετικού τύπου) και έτσι ανήκει σε δύο ή περισσότερα δίκτυα ταυτόχρονα.

Η δουλειά των routers είναι να δρομολογούν τα πακέτα των δεδομένων μέσα από τα διάφορα δίκτυα που αποτελούν το Internet μέχρις ότου τα επιδώσουν στον προορισμό τους. Ας δούμε πώς γίνεται αυτό:

Ας θεωρήσουμε πάλι ότι ένας υπολογιστής που βρίσκεται κάπου στο Internet θέλει να στείλει δεδομένα σε κάποιον άλλον υπολογιστή. Τα δεδομένα κόβονται σε πακέτα και το IP που εκτελείται στον υπολογιστή - αποστολέα ετοιμάζεται να στείλει το κάθε πακέτο. Εισάγει λοιπόν στην επικεφαλίδα του πακέτου τις IP διευθύνσεις του αποστολέα και του παραλήπτη και κατόπιν, βάσει των διευθύνσεων αυτών, ελέγχει αν ο παραλήπτης βρίσκεται στο ίδιο δίκτυο με τον αποστολέα. Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη χωρίς να χρειαστεί να διαβεί τα όρια του δικτύου. Εάν όχι, προωθείται στον router που είναι συνδεμένος με το δίκτυο. Ο router με τη σειρά του ελέγχει αν ο παραλήπτης βρίσκεται σε κάποιο από τα υπόλοιπα δίκτυα με τα οποία είναι συνδεδεμένος. Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη στο δίκτυο αυτό. Εάν όχι, το πακέτο προωθείται στον επόμενο router, κ.ο.κ. μέχρις ότου το πακέτο προωθηθεί τελικά στον router που είναι συνδεδεμένος στο ίδιο δίκτυο με τον παραλήπτη. Το πακέτο μπορεί έτσι να περάσει από πολλούς routers μέχρις ότου φτάσει στον προορισμό του. Οι routers διατηρούν πίνακες που προσδιορίζουν την κατεύθυνση που πρέπει να πάρει ένα πακέτο προκειμένου να φτάσει στον προορισμό του. Βάσει αυτών των πινάκων αποφασίζουν ποιος θα είναι ο επόμενος router στον οποίο θα πρέπει να προωθήσουν το πακέτο. Κάθε φορά, το πακέτο μετακινείται όλο και πιο κοντά προς τον προορισμό του έως ότου τελικά τον φτάσει. Ένα μεγάλο πλεονέκτημα αυτής της μεθόδου είναι ότι η διαδρομή που ακολουθεί ένα πακέτο δεν είναι προκαθορισμένη, αλλά επιλέγεται δυναμικά. Έτσι, οι routers μπορούν να επιλέγουν εναλλακτικούς δρόμους για ένα πακέτο σε περίπτωση που μια συγκεκριμένη σύνδεση του δικτύου παρουσιάζει πρόβλημα και βρίσκεται προσωρινά σε αχρηστία.

5.4 Υποδίκτυα

Όπως έχουμε δει, όλοι οι υπολογιστές υπηρεσίας σε ένα δίκτυο πρέπει να έχουν τον ίδιο αριθμό δικτύου. Αυτή η ιδιότητα της διευθυνσιοδότησης του IP μπορεί να προκαλέσει προβλήματα καθώς μεγαλώνουν τα δίκτυα. Για παράδειγμα, φανταστείτε ένα πανεπιστήμιο που ξεκίνησε με ένα δίκτυο τάξης Β το οποίο το χρησιμοποιούσε το Τμήμα Επιστήμης Υπολογιστών για τους υπολογιστές του δικτύου Ethernet του. Ένα χρόνο αργότερα το Τμήμα Ηλεκτρολόγων Μηχανικών θέλησε να μπει στο Internet, έτσι αγόρασε έναν επαναλήπτη για να επεκτείνει το υπάρχον Ethernet μέχρι το δικό του κτίριο. Καθώς περνούσε ο χρόνος, πολλά άλλα τμήματα απέκτησαν

υπολογιστές και γρήγορα έφτασαν στο όριο των τεσσάρων επαναληπτών ανά Ethernet. Απαιτήθηκε λοιπόν μια διαφορετική οργάνωση.

Η προμήθεια μιας δεύτερης διεύθυνσης δικτύων θα ήταν δύσκολη, επειδή οι διευθύνσεις δικτύου είναι σπάνιες και το πανεπιστήμιο είχε ήδη διευθύνσεις για περισσότερους από 60.000 υπολογιστές υπηρεσίας. Το πρόβλημα είναι ο κανόνας ότι μία διεύθυνση τάξης A, B ή C αναφέρεται σε ένα δίκτυο και όχι σε μια συλλογή LAN. Καθώς όλο και περισσότεροι οργανισμοί αντιμετώπιζαν αυτήν την κατάσταση, έγινε μια μικρή αλλαγή στο σύστημα διευθυνσιοδότησης για να λυθεί αυτό το πρόβλημα.

Η λύση είναι να επιτρέπεται η διάσπαση ενός δικτύου σε πολλά τμήματα για εσωτερική χρήση, ενώ για τον έξω κόσμο θα λειτουργεί ακόμα σαν να ήταν ένα μόνο δίκτυο. Ένα τυπικό σύγχρονο δίκτυο πανεπιστημιούπολης μπορεί να μοιάζει με αυτό της Εικόνας 5-57, με έναν κύριο δρομολογητή συνδεδεμένο σε έναν ISP ή ένα περιφερειακό δίκτυο και πολυάριθμα δίκτυα Ethernet απλωμένα στην πανεπιστημιούπολη σε διάφορα τμήματα. Καθένα από τα δίκτυα Ethernet έχει το δικό του δρομολογητή που είναι συνδεδεμένος στον κύριο δρομολογητή (πιθανόν μέσω ενός δικτύου σπονδυλικής στήλης LAN, αν και η φύση της διασύνδεσης των δρομολογητών δεν έχει σημασία εδώ) .

Στην ορολογία του Internet, τα τμήματα του δικτύου (σε αυτή την περίπτωση, τα δίκτυα Ethernet) ονομάζονται υποδίκτυα (subnets). Η χρήση αυτού του όρου συγκρούεται με τον όρο ‘υποδίκτυο’ που σημαίνει το σύνολο όλων των δρομολογητών και γραμμών επικοινωνίας σε ένα δίκτυο.

Όταν φτάνει ένα πακέτο στον κύριο δρομολογητή, πώς γνωρίζει αυτός σε ποιο υποδίκτυο (Ethernet) να το παραδώσει; Ένας τρόπος θα ήταν να έχουμε έναν πίνακα με 65.536 καταχωρίσεις στο δρομολογητή, ο οποίος να δείχνει ποιο δρομολογητή πρέπει να χρησιμοποιήσει για κάθε υπολογιστή υπηρεσίας της πανεπιστημιούπολης . Η ιδέα αυτή θα μπορούσε να λειτουργήσει, αλλά θα απαιτούσε έναν πολύ μεγάλο πίνακα στον κύριο δρομολογητή καθώς και πολλή χειρονακτική συντήρηση κατά την προσθήκη, μετακίνηση, ή κατάργηση υπολογιστών υπηρεσίας.

Επινοήθηκε λοιπόν μια διαφορετική μέθοδος. Αντί να έχουμε μια μόνο διεύθυνση τάξης B με 14 bit για τον αριθμό δικτύου και 16 bit για τον αριθμό υπολογιστή υπηρεσίας, μερικά bit αφαιρούνται από τον αριθμό υπολογιστή υπηρεσίας για τη δημιουργία ενός αριθμού υποδικτύου. Για παράδειγμα, αν το πανεπιστήμιο έχει 35 τμήματα, θα μπορούσε να χρησιμοποιήσει έναν αριθμό υποδικτύου των 6 bit και έναν αριθμό υπολογιστή υπηρεσίας των 10 bit, επιτρέποντας μέχρι 64 δίκτυα Ethernet που το καθένα τους θα έχει μέχρι 1022 υπολογιστές υπηρεσίας (οι τιμές 0 και -1 δεν είναι διαθέσιμες, όπως αναφέραμε προηγουμένως). Αυτή η διάσπαση θα μπορούσε αργότερα να αλλάξει αν αποδεικνυόταν ότι ήταν λανθασμένη.

Για την υλοποίηση των υποδικτύων, ο κύριος δρομολογητής χρειάζεται μια μάσκα υποδικτύου (subnet mask) η οποία θα δείχνει τον τρόπο διάσπασης ανάμεσα στον αριθμό δικτύου και υποδικτύου και τον αριθμό υπολογιστή υπηρεσίας. Οι μάσκες υποδικτύου γράφονται και αυτές με δεκαδική γραφή με τελείες, με την προσθήκη μιας καθέτου (slash) η οποία ακολουθείται από το πλήθος των bit που υπάρχουν στο τμήμα δικτύου και υποδικτύου.

Έξω από το δίκτυο τα υποδίκτυα δεν είναι ορατά, έτσι η δημιουργία ενός νέου υποδικτύου δεν απαιτεί να έρθουμε σε επαφή με την ICANN ή να τροποποιήσουμε

κάποιες εξωτερικές βάσεις δεδομένων. Στο παράδειγμα αυτό, το πρώτο υποδίκτυο θα μπορούσε να χρησιμοποιεί διευθύνσεις που αρχίζουν με την 130.50.4.1, το δεύτερο υποδίκτυο θα μπορούσε να αρχίζει στη διεύθυνση 130.50.8.1, το τρίτο υποδίκτυο θα μπορούσε να ξεκινά στη διεύθυνση 130.50.12.1, και ούτω καθεξής. Για να κατανοήσουμε γιατί στα υποδίκτυα μετράμε ανά τέσσερα, παρατηρούμε ότι οι αντίστοιχες δυαδικές διευθύνσεις είναι οι ακόλουθες:

Υποδίκτυο 0: 10000010 00110010 000001|00 00000001

Υποδίκτυο 1: 10000010 00110010 000010|00 00000001

Υποδίκτυο 2: 10000010 00110010 000011|00 00000001

Η κατακόρυφη γραμμή (|) δείχνει το όριο ανάμεσα στον αριθμό υποδικτύου και τον αριθμό υπολογιστή υπηρεσίας. Στα αριστερά της βρίσκεται ο 6μπιτος αριθμός υποδικτύου, ενώ στα δεξιά της ακολουθεί ο 10μπιτος αριθμός υπολογιστή υπηρεσίας.

Για να κατανοήσουμε πώς δουλεύουν τα υποδίκτυα, είναι απαραίτητο να εξηγήσουμε πώς γίνεται η επεξεργασία των πακέτων IP σε ένα δρομολογητή. Κάθε δρομολογητής έχει έναν πίνακα που παραθέτει κάποιο πλήθος διευθύνσεων IP με τη μορφή (δίκτυο, 0) και κάποιο πλήθος διευθύνσεων IP με τη μορφή (αυτό το δίκτυο, υπολογιστής υπηρεσίας). Το πρώτο είδος καταχωρίσεων δείχνει πώς φτάνουμε σε απομακρυσμένα δίκτυα. Το δεύτερο είδος δείχνει πώς φτάνουμε σε τοπικούς υπολογιστές υπηρεσίας. Με κάθε καταχώριση συσχετίζεται η διασύνδεση δικτύου που χρησιμοποιείται για να φτάσουμε στον προορισμό, καθώς και μερικές άλλες πληροφορίες.

Όταν φτάνει ένα πακέτο IP, η διεύθυνση προορισμού του αναζητείται στον πίνακα δρομολόγησης. Αν το πακέτο προορίζεται για ένα απομακρυσμένο δίκτυο, προωθείται στον επόμενο δρομολογητή μέσω της διασύνδεσης που δίνεται στον πίνακα. Αν προορίζεται για έναν τοπικό υπολογιστή υπηρεσίας (με άλλα λόγια, βρίσκεται στο LAN του δρομολογητή), στέλνεται απευθείας στον προορισμό. Αν το δίκτυο δεν υπάρχει, το πακέτο προωθείται σε έναν προεπιλεγμένο δρομολογητή που διαθέτει πιο εκτενείς πίνακες. Αυτός ο αλγόριθμος σημαίνει ότι κάθε δρομολογητής χρειάζεται να παρακολουθεί μόνο τα άλλα δίκτυα και τους τοπικούς υπολογιστές υπηρεσίας και όχι ζεύγη της μορφής (δίκτυο, υπολογιστής υπηρεσίας), γεγονός που μειώνει σημαντικά το μέγεθος του πίνακα δρομολόγησης.

Όταν χρησιμοποιούνται υποδίκτυα οι πίνακες δρομολόγησης αλλάζουν, με την προσθήκη καταχωρίσεων της μορφής (αυτό το δίκτυο, υποδίκτυο, 0) και (αυτό το δίκτυο, αυτό το υποδίκτυο, υπολογιστής υπηρεσίας). Έτσι, ένας δρομολογητής στο υποδίκτυο k γνωρίζει πώς να φτάσει σε όλα τα άλλα υποδίκτυα καθώς και πώς να φτάσει σε όλους τους υπολογιστές υπηρεσίας στο υποδίκτυο k. Δε χρειάζεται να γνωρίζει λεπτομέρειες για υπολογιστές υπηρεσίας σε άλλα υποδίκτυα. Στην πραγματικότητα, το μόνο που πρέπει να αλλάξει είναι ότι ο κάθε δρομολογητής θα εκτελεί ένα λογικό AND με τη μάσκα του υποδικτύου, έτσι ώστε να ξεφορτωθεί τον αριθμό υπολογιστή υπηρεσίας και να αναζητήσει τη διεύθυνση που προκύπτει στους πίνακες του (αφού καθορίσει σε ποια τάξη δικτύου ανήκει).

Για παράδειγμα, ένα πακέτο με διεύθυνση προορισμού 130.50.15.6 που φτάνει στον κύριο δρομολογητή περνά από AND με τη μάσκα υποδικτύου 255.255.252.0/22, και δίνει αποτέλεσμα τη διεύθυνση 130.50.12.0. Η διεύθυνση αυτή αναζητείται στους πίνακες δρομολόγησης, ώστε να βρούμε ποια γραμμή εξόδου θα πρέπει να χρησιμοποιηθεί για να φτάσουμε στο δρομολογητή για το υποδίκτυο 3. Έτσι τα υποδίκτυα μειώνουν το χώρο των πινάκων στους δρομολογητές, δημιουργώντας μια

ιεραρχία τριών επιπέδων που αποτελείται από το δίκτυο, το υποδίκτυο και τον υπολογιστή υπηρεσίας.

Οι προκαθορισμένες μάσκες υποδικτύου είναι:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

5.5 Φορητό IP

Πολλοί χρήστες του Internet έχουν φορητούς υπολογιστές και θέλουν να παραμείνουν συνδεδεμένοι στο Internet όταν επισκέπτονται μια απομακρυσμένη τοποθεσία του Internet , και ακόμα και κατά την διαδρομή τους μέχρι εκεί. Δυστυχώς το σύστημα διευθυνσιοδότησης του IP κάνει τη λειτουργία μακριά από την οικεία θέση πιο εύκολη στην περιγραφή παρά στην υλοποίηση.

Ο πραγματικός ένοχος είναι το σύστημα διευθυνσιοδότησης. Κάθε διεύθυνση IP περιέχει έναν αριθμό δικτύου και έναν αριθμό υπολογιστή υπηρεσίας. Για παράδειγμα, φανταστείτε τη μηχανή με διεύθυνση IP 160.80.40.20/16. Το 160.80 προσδιορίζει τον αριθμό δικτύου (8272 σε δεκαδικό σύστημα), ενώ το 40.20 είναι ο αριθμός υπολογιστή υπηρεσίας (10260 σε δεκαδικό σύστημα) . Οι δρομολογητές σε ολόκληρο τον κόσμο έχουν πίνακες δρομολόγησης οι οποίοι λένε ποια γραμμή πρέπει να χρησιμοποιηθεί για να πάμε στο δίκτυο 160.80. Όποτε φτάνει ένα πακέτο με διεύθυνση IP προορισμού της μορφής 160.80.xxx.yyy , φεύγει από την αντίστοιχη γραμμή.

Αν ξαφνικά η μηχανή που έχει τη διεύθυνση αυτή μεταφερθεί σε κάποια απομακρυσμένη τοποθεσία ,τα πακέτα της θα συνεχίσουν να δρομολογούνται στο οικείο της LAN (η δρομολογητή). Ο ιδιοκτήτης δεν θα λαμβάνει πια ηλεκτρονικό ταχυδρομείο, ούτε τίποτα άλλο. Η απόδοση μιας νέας διεύθυνσης IP στη μηχανή, η οποία θα αντιστοιχεί στη νέα της θέση, δεν είναι ελκυστική λύση επειδή μεγάλο πλήθος ανθρώπων, προγραμμάτων και βάσεων δεδομένων θα πρέπει να πληροφορηθούν την αλλαγή αυτή.

Μια άλλη επιλογή είναι να χρησιμοποιούν οι δρομολογητές ολόκληρες τις διευθύνσεις IP για τη δρομολόγηση και όχι μόνο το τμήμα του δικτύου. Ωστόσο η στρατηγική αυτή θα απαιτούσε κάθε δρομολογητής να έχει εκατομμύρια καταχωρίσεις στους πίνακες του, με αστρονομικό κόστος για το Internet.

Όταν ο κόσμος άρχισε να απαιτεί τη δυνατότητα να συνδέει τους φορητούς υπολογιστές του στο Internet όπου κι αν βρίσκεται, η IETF δημιούργησε μια Ομάδα Εργασίας για να βρει μια λύση. Η Ομάδα Εργασίας έθεσε σύντομα έναν αριθμό στόχων που θεωρούνταν επιθυμητοί για οποιαδήποτε λύση. Οι βασικοί στόχοι ήταν:

1. Κάθε κινητός υπολογιστής υπηρεσίας θα έπρεπε να είναι σε θέση να χρησιμοποιεί οπουδήποτε την οικεία του διεύθυνση IP.

2. Δεν επιτρέπονταν αλλαγές λογισμικού στους σταθερούς υπολογιστές υπηρεσίας.

3. Δεν επιτρέπονταν αλλαγές στο λογισμικό και τους πίνακες των δρομολογητών.

4. Τα περισσότερα πακέτα για τους κινητούς υπολογιστές υπηρεσίας δεν θα έπρεπε να κάνουν παρακάμψεις στο δρόμο.

5. Δεν θα έπρεπε να υπάρχει επιβάρυνση όταν ένας κινητός υπολογιστής υπηρεσίας βρισκόταν στην οικεία του θέση.

Κάθε τοποθεσία που θέλει να επιτρέπει στους χρηστές της να "περιπλανιούνται" πρέπει να εγκαταστήσει έναν οικείο πράκτορα. Κάθε υπηρεσία που θέλει να επιτρέπει επισκέπτες πρέπει να εγκαταστήσει έναν ξένο πράκτορα. Όταν ένας κινητός υπολογιστής υπηρεσίας εμφανιστεί σε μια ξένη τοποθεσία, επικοινωνεί με τον εκεί ξένο πράκτορα και εγγράφεται σ'αυτόν. Ο ξένος πράκτορας επικοινωνεί τότε με τον οικείο πράκτορα του χρηστή δίνοντας του μια διεύθυνση επιμέλειας (care-of address) συνήθως τη διεύθυνση IP του ίδιου του ξένου πράκτορα.

Όταν φτάνει ένα πακέτο στο οικείο LAN του χρηστή, σταματάει σε κάποιο δρομολογητή συνδεδεμένο στο LAN. Ο δρομολογητής προσπαθεί τότε να εντοπίσει τον υπολογιστή υπηρεσίας με το συνηθισμένο τρόπο, εκπέμποντας ένα πακέτο ARP που ρωτάει για παράδειγμα: Ποια είναι η διεύθυνση Ethernet του υπολογιστή 160.80.40.20 ; Ο οικείος πράκτορας αποκρίνεται σε αυτή την ερώτηση δίνοντας τη δική του διεύθυνση Ethernet. Ο δρομολογητής στέλνει τότε τα πακέτα 160.80.40.20 στον οικείο πράκτορα. Αυτός με τη σειρά του, τα διοχετεύει μέσω σήραγγας στη διεύθυνση επιμέλειας, ενθυλακώνοντας τα στο πεδίο ωφέλιμου φορτίου ενός πακέτου IP το οποίο έχει τη διεύθυνση του ξένου πράκτορα. Ο ξένος πράκτορας στη συνέχεια τα εξάγει και τα παραδίδει στη διεύθυνση συνδέσμου μετάδοσης δεδομένων του κινητού υπολογιστή υπηρεσίας. Επιπλέον, ο οικείος πράκτορας δίνει τη διεύθυνση επιμέλειας στον αποστολέα έτσι ώστε τα μελλοντικά πακέτα να μπορούν να διοχετευτούν μέσω σήραγγας απευθείας στον ξένο πράκτορα. Η λύση αυτή ικανοποιεί όλες τις απαιτήσεις.

Τη στιγμή που θα μετακινηθεί ο κινητός υπολογιστής υπηρεσίας, ο δρομολογητής μάλλον θα έχει στην κρυφή του μνήμη τη διεύθυνση Ethernet του υπολογιστή (που σε λίγο δεν θα είναι έγκυρη). Η αντικατάσταση αυτής της διεύθυνσης Ethernet με εκείνη του οικείου πράκτορα γίνεται με μια διαδικασία που ονομάζεται αναίτιο ARP. Αυτό είναι ένα ειδικό αυτόκλητο μήνυμα προς τον δρομολογητή που τον κάνει να ενημερώσει μια καταχώριση στην κρυφή του μνήμη, στην περίπτωση αυτή τη διεύθυνση του κινητού υπολογιστή υπηρεσίας που πρόκειται να φύγει. Όταν αργότερα επιστρέψει ο κινητός υπολογιστής υπηρεσίας, χρησιμοποιείται το ίδιο κόλπο για ενημερωθεί ξανά η κρυφή μνήμη του δρομολογητή. Τίποτα στη σχεδίαση αυτή δεν αποτρέπει έναν κινητό υπολογιστή υπηρεσίας από το να είναι ξένος πράκτορας του εαυτού του, αλλά η προσέγγιση αυτή λειτουργεί μόνο όταν ο κινητός υπολογιστής υπηρεσίας (στο ρόλο του ξένου πράκτορα) είναι λογικά συνδεδεμένος στο Internet στην τρέχουσα τοποθεσία του. Επιπλέον , ο κινητός υπολογιστής υπηρεσίας θα πρέπει να μπορεί να αποκτήσει μια

(προσωρινή) διεύθυνση επιμέλειας IP για να τη χρησιμοποιήσει. Αυτή η διεύθυνση IP θα πρέπει να ανήκει στο LAN στο οποίο είναι συνδεδεμένος τη δεδομένη στιγμή.

Η λύση της ITEM για τους κινητούς υπολογιστές υπηρεσίας λύνει και πλήθος άλλων προβλημάτων που δεν έχουμε αναφέρει μέχρι στιγμής. Για παράδειγμα, πως εντοπίζονται οι πράκτορες; Η λύση είναι να εκπέμπει κάθε πράκτορας περιοδικά τη διεύθυνση του και τον τύπο των υπηρεσιών που προτίθεται να παρέχει (για παράδειγμα οικείος, ξένος, και τα δυο). Όταν ένας κινητός υπολογιστής υπηρεσίας φτάσει κάπου, μπορεί να εκπέμψει ένα πακέτο που να ανακοινώνει την άφιξη του, ελπίζοντας ότι ο τοπικός ξένος πράκτορας θα απαντήσει σε αυτό. Ένα άλλο ζήτημα είναι η ασφάλεια. Όταν ένας οικείος πράκτορας λάβει ένα μήνυμα που του ζητά να προωθήσει όλα τα πακέτα ενός χρηστή σε κάποια διεύθυνση IP, καλό είναι να μην συμμορφωθεί αν δεν πειστεί ότι η πηγή της αίτησης αυτής είναι ο συγκεκριμένος χρηστής και όχι κάποιος που προσπαθεί να τον υποδυθεί. Για το σκοπό αυτό χρησιμοποιούνται κρυπτογραφικά πρωτοκολλά πιστοποίησης ταυτότητας. Ένα τελευταίο σημείο σχετίζεται με τα επίπεδα κινητικότητας. Φανταστείτε ένα αεροπλάνο με ένα Ethernet αεροσκάφους που χρησιμοποιείται από τους υπολογιστές πλοήγησης και οργάνων έλεγχου. Στο Ethernet αυτό υπάρχει ένας τυπικός δρομολογητής που μιλάει με το ενσύρματο Ethernet στο έδαφος μέσω μιας γραμμής ραδιοκυμάτων. Μια μέρα, κάποιος από το τμήμα μάρκετινγκ έχει την ιδέα να εγκαταστήσει συζευκτήρες Ethernet σε όλους τους βραχίονες των καθισμάτων, έτσι ώστε να μπορούν να συνδεθούν και οι επιβάτες που έχουν φορητούς υπολογιστές. Τώρα έχουμε δυο επίπεδα κινητικότητας: οι υπολογιστές του ίδιου του αεροσκάφους, οι οποίοι είναι στατικοί σε σχέση με το Ethernet και οι υπολογιστές των επιβατών οι οποίοι είναι κινητοί σε σχέση με αυτό. Επιπλέον, ο δρομολογητής του αεροσκάφους είναι κινητός σε σχέση με τους δρομολογητές στο έδαφος. Η ύπαρξη κινητών χρηστών σε σχέση με ένα σύστημα το οποίο είναι το ίδιο κινητό, μπορεί να αντιμετωπιστεί με χρήση αναδρομικής διοχέτευσης σε σήραγγα.

5.6 IPv6

Μια από τις ελλείψεις της σημερινής έκδοσης του πρωτοκόλλου Internet (IPv4) είναι ότι δεν παρέχει επαρκή αριθμό διευθύνσεων, δεδομένου ότι σχεδιάστηκε πολύ πριν από την ανάπτυξη του Παγκόσμιου Ιστού (World-Wide-Web) και των κινητών επικοινωνιών και, ως εκ τούτου, δεν μπορεί να καλύψει τις ανάγκες των τελευταίων αυτών τεχνολογιών. Επιπλέον η δυσκολία στη διαχείριση, η μη αποδοτική δρομολόγηση, θέματα ασφαλείας και η δυσκολία στην ταυτόχρονη χρήση περισσότερων της μιας προσθηκών του Ipv4 (QoS, IPsec, MobileIP κτλ.) κάνουν επιτακτική την ανάγκη μετάβασης στο IPv6.

Ένα από τα βασικά πλεονεκτήματα του νέου πρωτοκόλλου είναι η επίλυση του προβλήματος του περιορισμένου αριθμού διευθύνσεων IP. Το νέο πρωτόκολλο καθιστά δυνατό έναν σχεδόν απεριόριστο αριθμό διευθύνσεων (2128) ικανό για να καλύψει τις μελλοντικές ανάγκες ανάπτυξης του Internet παγκοσμίως, μεταξύ άλλων της μεγάλης αύξησης του αριθμού των συσκευών συνεχούς σύνδεσης και άλλων συσκευών συνδεδεμένων με το Internet, όπως τα κινητά τηλέφωνα, τα συστήματα πλοήγησης αυτοκινήτων και οι οικιακές συσκευές. Το νέο πρωτόκολλο περιλαμβάνει επίσης βελτιώσεις που κάνουν το Internet ταχύτερο, περισσότερο ευέλικτο και ασφαλές και προσαρμοσμένο στις σημερινές και μελλοντικές ανάγκες του Internet.

Επίσης το Ipv6 προσφέρει τη δυνατότητα απλοποίησης της επικεφαλίδας, καλύτερη υποστήριξη επιλογών και επεκτάσεων στη στάνταρ επικεφαλίδα.

Οι διευθύνσεις IPv6 είναι 128μπιτα προσδιοριστικά για τις διεπαφές και τα σύνολα διεπαφών. Υπάρχουν τρεις τύποι διευθύνσεων:

Unicast: Ένα προσδιοριστικό για μια ενιαία διεπαφή. Ένα πακέτο που στέλνεται σε μια διεύθυνση unicast παραδίδεται στη διεπαφή που προσδιορίζεται από εκείνη την διεύθυνση.

Anycast: Ένα προσδιοριστικό για ένα σύνολο διεπαφών (χαρακτηριστικά που ανήκουν στους διαφορετικούς κόμβους). Ένα πακέτο που στέλνεται σε μια διεύθυνση anycast παραδίδεται σε μια από τις διεπαφές που προσδιορίζονται από από εκείνη την διεύθυνση (η "κοντινότερη", σύμφωνα με το μέτρο των πρωτοκόλλων δρομολόγησης της απόστασης).

Η βασική IPv6 επικεφαλίδα είναι απλοποιημένη σε σχέση με το IPv4 και άρα βοηθά στη μείωση του κόστους δρομολόγησης για κάθε πακέτο και του κόστους σε εύρος ζώνης που καταναλώνει η επικεφαλίδα, έχει σταθερό μήκος και οι δρομολογητές έχουν καλύτερη απόδοση για τέτοιες επικεφαλίδες. Τα προαιρετικά πεδία υποστηρίζονται σε ξεχωριστές επικεφαλίδες. Αυτό διευκολύνει την απόδοση της απλής δρομολόγησης, αφού δεν χρειάζεται κάθε δρομολογητής να επεξεργαστεί αυτά τα πεδία, αν κάτι τέτοιο δεν είναι αναγκαίο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Books

Stallings William, 2004, Seventh Edition. *Data and Computer Communications.* Prentice Hall.

Stallings William, 1998, First Edition. *High-speed Networks TCP/IP and ATM design principles.* Prentice Hall.

John C. B. Le Gates, "TCP/IP and Related Protocolos", New York, McGraw-Hill, 1996.

Tanenbaum Andrew, 2003, Fourth Edition. *Δίκτυα Υπολογιστών.* Κλειδάριθμος.

Tanenbaum A.S., Δίκτυα Υπολογιστών, Δεύτερη Έκδοση, Prentice Hall, για την ελληνική έκδοση Παπασωτηρίου.

Comer E.D., Internetworking with TCP/IP Volume I, Principles, Protocols and Architecture, 2nd edition, Prentice Hall,N.J., 1991.

Comer D.E., "Interworking with TCP/IP" , Prentice Hall, 1995.

Rose M.T., The Open Book, A Practical Perspective on OSI, Prentice Hall, 1990.

Information processing systems – Open System Interconnection – Systems Management: Alarm reporting Function – International Organization for standardization – International Standard 10164-4, December 1992.

Dinesh Verma, "Supporting Service Level Agreements on IP Networks", Prentice Hall, 2001.

Stallings William, "High-speed Networks TCP/IP and ATM design principles", First Edition Prentice Hall, 2001.

RFCs

RFC1180, A TCP/IP Tutorial

RFC793, Transmision Control Protocol

RFC791, Internet Protocol

RFC2373, IP version 6 Addressing Architecture