ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΚΑΒΑΖΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΔΙΕΥΘΥΝΣΙΟΔΟΤΗΣΗ IP

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

INTERNET PROTOCOL version 6 (IPv6)

ΚΕΦΑΛΑΙΟ 2

ΑΝΑΦΟΡΑ ΣΤΟ TCP/IP

ΚΕΦΑΛΑΙΟ 3

ΣΤΑΤΙΚΗ ΔΡΟΜΟΛΟΓΗΣΗ

ΚΕΦΑΛΑΙΟ 4

ΔΥΝΑΜΙΚΗ ΔΡΟΜΟΛΟΓΗΣΗ

ΚΕΦΑΛΑΙΟ 1
INTERNET PROTOCOL version 6

ΕΙΣΑΓΩΓΗ

Τα πρωτόκολλα Διαδικτύου είναι τα δημοφιλέστερα παγκοσμίως πρωτόκολλα ανοικτών-συστημάτων επειδή μπορούν να χρησιμοποιηθούν για να επικοινωνήσουν με κάθε είδους διασυνδεόμενων δικτύων και είναι εξίσου καλά για LAN και WAN επικοινωνίες. Τα πρωτόκολλα Διαδικτύου αποτελούνται από μια ακολουθία των πρωτοκόλλων επικοινωνίας, εκ των οποίων ευρύτερα διαδεδομένα είναι το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το πρωτόκολλο Διαδικτύου (IP). Η ακολουθία πρωτοκόλλου Διαδικτύου όχι μόνο περιλαμβάνει τα πρωτόκολλα χαμηλού-στρώματος (όπως το TCP και η IP), αλλά διευκρινίζει επίσης τις κοινές εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο και τη μεταφορά αρχείων.

Τα πρωτόκολλα Διαδικτύου αναπτύχθηκαν αρχικά στα μέσα της δεκαετίας του '70, όταν η Defense Advanced Research Projects Agency (DARPA) ενδιαφέρθηκε για την καθιέρωση ενός packet-switched δικτύου που θα διευκόλυνε την επικοινωνία μεταξύ των ανόμοιων συγκροτημάτων ηλεκτρονικών υπολογιστών στα ερευνητικά ιδρύματα. Με το στόχο την ετερογενής συνδετικότητα, η DARPA χρηματοδότησε την έρευνα του πανεπιστημίου του Στάνφορντ, Beranek, και Newman (BBN). Το αποτέλεσμα αυτής της προσπάθειας ανάπτυξης ήταν η ακολουθία πρωτοκόλλου Διαδικτύου, που ολοκληρώθηκε προς το τέλος της δεκαετίας του '70. Το TCP/IP αργότερα περιλήφθηκε με το Unix διανομής λογισμικού του Μπέρκλευ και έχει γίνει από τότε το ίδρυμα στο οποίο το Διαδίκτυο και το World Wide Web (WWW) είναι βασισμένα.

Η τεκμηρίωση των πρωτοκόλλων Διαδικτύου (συμπεριλαμβανομένων των νέων ή αναθεωρημένων πρωτοκόλλων) και οι πολιτικές διευκρινίζονται στις τεχνικές εκθέσεις, αποκαλούμενο, αίτημα για σχόλια (RFCs), τα οποία δημοσιεύονται και έπειτα αναθεωρημένα αναλύονται από την κοινότητα Διαδικτύου και έπειτα δημοσιεύονται στο νέο RFCs.

(INTERNET PROTOCOL-IP)

Το Internet πρωτόκολλο (Internet Protocol—IP) μπόρεσε να συνδέσει εκατομμύρια υπολογιστών και να φέρει μία καινούργια πραγματικότητα στην παροχή πρόσβασης στην πληροφορία. Το IP αναπτύχθηκε πριν είκοσι χρόνια σαν το πρωτόκολλο του network επιπέδου της αρχιτεκτονικής του Διαδικτύου (Internet) και μαζί με το πρωτόκολλο του transport επιπέδου TCP (Transmission Control Protocol) δημιούργησαν την οικογένεια πρωτοκόλλων TCP/IP. Στην αρχή το TCP/IP χρησιμοποιήθηκε για την διασύνδεση των διαφορετικών υπολογιστικών συστημάτων που χρησιμοποιούσε η κυβέρνηση των Η.Π.Α αλλά λόγω της εξαιρετικής του δύναμης εξαπλώθηκε παγκοσμίως νικώντας τις άλλες δικτυακές κατευθύνσεις και τεχνολογίες όπως: OSI, SNA, DECnet, NETware, κ.α. Το IP λοιπόν έγινε η βάση της δημιουργίας πάρα πολλών client-server ή peer-to-peer εφαρμογών εκμεταλεύοντας έτσι την δυνατότητα της δικτυακής σύνδεσης.

Η μεγάλη όμως ανάπτυξη του Διαδικτύου (Internet), που καλείται να εξυπηρετήσει δισεκατομμύρια χρηστών, καθώς και οι απαιτήσεις των νέων δικτυακών εφαρμογών δεν μπορούν να αντιμετωπισθούν από το IPv4, το οποίο και αποτελεί το υπάρχον IP.

Αυτό είναι λογικό γιατί δεν ήταν δυνατό στο σχεδιασμό του IPv4 να προέβλεπαν αυτήν την αλματώδη εξέλιξη που θα είχε ο δικτυακός χώρος. Η αδυναμία λοιπόν του IPv4 να ακολουθήσει τις εξελίξεις ώθησε τον οργανισμό IETF(Internet Engineering Task Force), στις 25 Ιουλίου του 1994 σ'ένα συνέδριο στο Τορόντο, να προτείνει το IP της επόμενης γενιάς, δηλαδή το Ipng (Next Generation Internet Protocol—RFC1752). Η πρόταση αυτή εγκρίθηκε από Internet Engineering Steering Group και από τις 17 Νοεμβρίου 1994 αποτελεί προτεινόμενο πρότυπο(Proposed Standard).

Mobility

Το επίσημο όνομά του IPv6 είναι (Internet Protocol version 6) και έρχεται να δώσει λύση στο εμφανή πρόβλημα της έλλειψης διευθύνσεων που παρουσιάζει το IPv4 και όχι μόνο, γιατί λόγω του βελτιωμένου σχεδιασμού του καθορίζει μία ομάδα από υπηρεσίες όπως ασφάλεια, υψηλή απόδοση, εύκολη διευθέτηση(configuration), δημιουργώντας με αυτό το τρόπο ένα πιο αξιόπιστο δίκτυο με λιγότερο διαχειριστικό βάρος.

Όμως η πραγματική πρόκληση για το IPv6 είναι για το εάν θα επιτύχει να "δέσει" το περιβάλλον του επερχόμενου δικτύου όπου εκτός από τους συμβατικούς υπολογιστές θα αποτελείται από χιλιάδες άλλες συσκευές όπως προσωπικοί επεξεργαστές δεδομένων μεγέθους παλάμης (palmtop personal data assistants-PDA), υβριδικά κινητά τηλέφωνα με υπολογιστικές δυνατότητες καθώς και από φωτοτυπικά μηχανήματα ενός γραφείου έως και συσκευές που χρησιμοποιούνται στην κουζίνα ενός σπιτιού.

Η επιτυχία του IPv6 θα βασιστεί όμως και στη δυνατότητα του να εντάξει το παλιό στο καινούργιο. Είναι γνωστό το μέγεθος που έχει ήδη το Διαδίκτυο και η μετάβαση από το IPv4 στο IPv6 δεν είναι απλή υπόθεση αλλά απαιτεί σωστή στρατηγική έτσι ώστε να παραμείνει αδιάλειπτη και αποδοτική η λειτουργία του Διαδικτύου.

Μετάβαση

Σίγουρα η τεχνολογία του IPv6 έχει να προσφέρει πολλά στο χώρο των δικτύων και να εξελίξει το Διαδίκτυο δίνοντας του εφόδια ώστε να αντιμετωπίσει τις μελλοντικές προκλήσεις. Η μεγαλύτερη όμως πρόκληση για την επιτυχή εφαρμογή του IPv6 είναι η μετάβαση του Διαδικτύου από το IPv4 στο νέο πρωτόκολλο. Το μεγάλο μέγεθος του Διαδικτύου όπου περιέχει εκατομμύρια δικτυακών συσκευών καθιστά βέβαιο ότι η μετάβαση δεν πρόκειται να πραγματοποιηθεί μέσα σε μια νύκτα αλλά θα υπάρχει μια μακρά περίοδος συνύπαρξης του IPv4 με το IPv6.

Με αυτή τη λογική ενέργησε το IETF δίνοντας την δυνατότητα στους διαχειριστές δικτύων να πραγματοποιήσουν με ελαστικότητα την αναβάθμιση των δικτύων τους. Η ελαστικότητα έγκειται στο ότι δεν είναι απαραίτητη η άμεση και ολοκληρωμένη αναβάθμιση ολόκληρων πληθυσμών στο νέο πρωτόκολλο γιατί είναι δεδομένη η συνλειτουργία των IPv4 και IPv6 και δεν υπάρχει το πρόβλημα της απομόνωσης ή του μεγάλου χρόνου μη λειτουργίας. Όμως κατά την αναβάθμιση σε πολλούς δρομολογητές ή hosts θα πρέπει να κρατούνται και οι λειτουργίες του IPv4 (downward compatibility) για την επικοινωνία με τους δικτυακούς χώρους όπου δεν έχει πραγματοποιηθεί η μετάβαση.

Για να επιτύχουν λοιπόν οι παραπάνω στόχοι της μετάβασης έχει γίνει σοβαρός σχεδιασμός στο IPv6 το οποίο βασίζεται σε μηχανισμούς όπως Hosts και δρομολογητές που υποστηρίζουν και τα δύο πρωτόκολλα IPv4 και IPv6 (dual-stack), και πραγματοποίηση σήραγγας (tunnelling) του IPv6 διαμέσου IPv4. Παρακάτω ακολουθεί η παρουσίαση του IPv6 πρωτοκόλλου στους τομείς της διευθυνσιοδότησης, απόδοσης και ασφάλειας.

Διευθυνσιοδότηση

Το IPv6 χρησιμοποιεί ένα σχήμα διευθυνσιοδότησης μεγέθους 128-bit. Το μέγεθος των διευθύνσεων που παράγονται είναι τόσο μεγάλο ώστε είναι δυνατό ο κάθε κάτοικος αυτού του πλανήτη να έχει τόσες διευθύνσεις για το δίκτυο του όσες το τωρινό Διαδίκτυο.

Το βασικότερο όμως δεν είναι η δημιουργία ενός σχήματος διευθυνσιοδότησης που θα παράγει πολλές σε αριθμό διευθύνσεις όσο η κατανομή των διευθύνσεων αυτών. Το IPv6 κατανέμει τις διευθύνσεις με ιεραρχικό τρόπο αποφεύγοντας έτσι τα προβλήματα του IPv4 όπου και

παραγόταν υπέρογκη πληροφορία για τη δρομολόγηση πάνω στα συστήματα και διευθύνσεις έμεναν αχρησιμοποίητες.
Οι τάξεις των διευθύνσεων στο IPv6 απευθύνονται καλύτερα στους χρήστες απ' ότι στο IPv4. Υπάρχουν βασικά τρεις κατηγορίες δικτυακών χρηστών: αυτοί που χρησιμοποιούν το δίκτυο ενός οργανισμού και μέσω αυτού και το Διαδίκτυο, αυτοί που χρησιμοποιούν μόνο το δίκτυο του οργανισμού με πιθανότητα να χρησιμοποιήσουν το Διαδίκτυο στο μέλλον και χρήστες που συνδέονται στο Διαδίκτυο διαμέσου τηλεφωνικών γραμμών.
Για την καλύτερη εξυπηρέτηση αυτών των δικτυακών χρηστών το IPv6 παρέχει τρεις τύπους διευθύνσεων, τις unicast, τις multicast και τις anycast.

Μοντέλο Διευθυνσιοδότησης

Από τις αρχές τις δεκαετίας του 1990 άρχισε να γίνεται αντιληπτό ότι το Internet σύντομα θα αντιμετώπιζε τρία βασικά προβλήματα στον τομέα της Διευθυνσιοδότησης:

1. Εξάντληση των διευθύνσεων δικτύων τάξεως B (Class B)
2. Αύξηση του μεγέθους των πινάκων δρομολόγησης (routing tables) πέρα από τα όρια του σημερινού λογισμικού, υλικού και ανθρώπινου δυναμικού.
3. Ολοκληρωτική εξάντληση των IP διευθύνσεων, μήκους 32-bit (2^{32} διευθύνσεις) που παρέχει η τρέχουσα έκδοση του IP (IPv4) σήμερα.

Τα προβλήματα στην αρχιτεκτονική Διευθυνσιοδότηση του IPv6

Ο διαχωρισμός των διευθύνσεων σε τάξεις δικτύων (A.B.C).

Από τον πίνακα 1, μπορούμε να δούμε ότι οι υπάρχουσες τάξεις (A,B,C) δικτύων δεν ικανοποιούν τις απαιτήσεις σε διευθύνσεις, των σημερινών δικτύων. Τα δίκτυα μεσαίου μεγέθους τα οποία περιλαμβάνουν πάνω από 254 μηχανές και έχουν σαφώς λιγότερες από 65.534, αποτελούν ένα χαρακτηριστικό παράδειγμα. Ένα μεσαίου μεγέθους δίκτυο που απαιτεί 500 έως 1000 διευθύνσεις, υποχρεωτικά χρησιμοποιεί διευθύνσεις τάξης B. Σαν αποτέλεσμα έχουμε την σπατάλη 64.000 περίπου διευθύνσεων ή 98.5% των διευθύνσεων ενός δικτύου τάξεως B. Αντίστοιχες απώλειες υπάρχουν στα μεγάλα και πολύ μικρά δίκτυα με αποτέλεσμα την γρηγορότερη εξάντληση των διευθύνσεων.

Τάξη δικτύου	Αριθμός δικτύων / Τάξη	Αριθμός μηχανών (host) / δίκτυο
Τάξη A	125	16.777.214
Τάξη B	16.320	65.534
Τάξη C	2.080.800	254

Πίνακας.1 Κατηγορίες δικτύων στο IPv6

Επίπεδος χώρος διευθυνσιοδότησης. Με τον όρο Επίπεδο χώρο εννοούμε ότι δεν υπάρχει κάποια συγκεκριμένη ιεραρχία στην απόδοση των διευθύνσεων που να μας επιτρέπει να συμπεράνουμε οτιδήποτε για την πραγματική θέση ενός δικτύου γνωρίζοντας μόνο την διεύθυνση του.

Η αρχιτεκτονική της διευθυνσιοδότησης του IPv6

Οι σχεδιαστές του IPv6 φρόντισαν ώστε να είναι απαλλαγμένο από τα προβλήματα που παρουσίαζε στην διευθυνσιοδότηση το IPv4. Είναι σημαντικό να υπενθυμίσουμε ότι μια διεύθυνση χαρακτηρίζει ένα interface μιας μηχανής και όχι την ίδια την μηχανή. Η αρχιτεκτονική της διευθυνσιοδότησης του IPv6 αποτελείται από τα εξής βασικά σημεία.

Μεγαλύτερος χώρος διευθυνσιοδότησης

Ενώ το μήκος των διευθύνσεων μόλις τετραπλασιάζεται (από 32 σε 128 bits) η αύξηση του χώρου των διευθύνσεων ακουμπάει το απίστευτο νούμερο των 2^{96} φορές τον χώρο του IPv4 (2^{32})=4.294.967.296 διευθύνσεις).
Ο συνολικός αριθμός των διευθύνσεων που υποστηρίζει το IPv6 είναι:
2^{128}=340.282.366.920.938.463.463.374.607.431.768.211.456 διευθύνσεις.

Στα πραγματικά δίκτυα, λόγο της ιεραρχίας που απαιτείται για την απόδοση και δρομολόγηση των διευθύνσεων μειώνεται η αποδοτικότητα της χρήσης και περιορίζεται ο αριθμός των διευθύνσεων που μπορούν να χρησιμοποιηθούν.

Ο Christian Huitema μετά από ανάλυση της αποδοτικότητας των τηλεφωνικών δικτύων της Γαλλίας και της Αμερικής, του σημερινού Intertnet με το IPv4 και άλλων κατέληξε ότι από τις διευθύνσεις των 128-bit μόνο 8×10^{17} έως 2×10^{33} διευθύνσεις μπορούν να χρησιμοποιηθούν υποθέτοντας απόδοση στα ίδια επίπεδα με τις άλλες αρχιτεκτονικές διευθυνσιοδότησης. Ακόμα και σε αυτή την περίπτωση έχουμε αναλογία διευθύνσεων/m^2 ίση με 1.564 διευθύνσεις στην πρώτη και 3.911.873.538.269.506.102 στην δεύτερη περίπτωση, μεγέθη που φαίνονται για το άμεσο μέλλον να είναι υπεραρκετά.

Νέος Τρόπος γραφής διευθύνσεων

Ο τετραπλασιασμός του μήκους σε bit των διευθύνσεων κάνει δύσκολη την γραφή τους με δεκαδικούς αριθμούς. Η νέα μορφή γραφής χρησιμοποιεί δεκαεξαδικούς αριθμούς και έχει την ακόλουθη μορφή:
Διεύθυνση IPv6 : x:x:x:x:x:x:x:x
όπου x ένας δεκαεξαδικός αριθμός μήκους 16-bit
π.χ. FEDC:BA98:7654:3210:FFDA:1A98:4512:24A2
1080:0:0:0:8:800:200C:417A
Για την περίπτωση που υπάρχουν πολλά x=0 είναι δυνατό να παραληφθούν.
Για παράδειγμα οι διευθύνσεις:
1080:0:0:0:8:800:200C:417A
1A34:0:0:0:342D:0:0:13DF
Γράφονται για συντομία:
1080::8:800:200C:417A
1A34::342D:0:0:13DF
Παρατηρήστε ότι η συντομογραφία :: δεν μπορεί να χρησιμοποιηθεί πάνω από μια φορά.

Τέλος υπάρχει μια ειδική γραφή που μπορεί να φανεί χρήσιμη σε μια ειδική κατηγορία διευθύνσεων που θα παρουσιάσουμε σε επόμενη παράγραφο είναι η ακόλουθη:
διεύθυνση IPv6 με ενσωματωμένη IPv4 διεύθυνση : x:x:x:x:x:x.d.d.d.d όπου x ένας δεκαεξαδικός αριθμός μήκους 16-bit και d.d.d.d μια διεύθυνση IPv4.
Για παράδειγμα : 0:0:0:0:0:0:143.233.241.250

Τύποι διευθύνσεων του IPv6

Στο IPv6 υπάρχουν τρεις βασικές κατηγορίες διευθύνσεων και τρεις ειδικές κατηγορίες. Στον πίνακα 2 φαίνεται ο καταμερισμός του χώρου διευθυνσιοδότησης σε αυτές της κατηγορίες και το μέγεθος τους ως προς το συνολικό χώρο.

Κατανομή διευθύνσεων	Πρόθεμα Μορφής (Δυαδικό)	Κομμάτι του χώρου διευθυνσιοδότησης
Παρακρατημένο	0000 0000	1/256
Ελεύθερο	0000 0001	1/256
Παρακρατημένο για NSAP διευθύνσεις	0000 001	1/128
Παρακρατημένο για IPX διευθύνσεις	0000 010	1/128
Ελεύθερο	0000 011	1/128

Ελεύθερο	0000 1	1/32
Ελεύθερο	0001	1/16
Αθροίσιμες Global Unicast Διευθύνσεις	001	1/8
Ελεύθερο	010	1/8
Ελεύθερο	011	1/8
Ελεύθερο	100	1/8
Ελεύθερο	101	1/8
Ελεύθερο	110	1/8
Ελεύθερο	1110	1/16
Ελεύθερο	1111 0	1/32
Ελεύθερο	1111 10	1/64
Ελεύθερο	1111 110	1/128
Ελεύθερο	1111 1110 0	1/512
Τοπικής σύνδεσης Unicast διευθύνσεις	1111 1110 10	1/1024
Τοπικού Δικτύου Unicast διευθύνσεις	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Πίνακας 2.
Καταμερισμός του χώρου διευθυνσιοδότησης ανά κατηγορία.

Ο διαχωρισμός των κατηγοριών γίνεται από το πρόθεμα όπως φαίνεται στον πίνακα 2. Το πρόθεμα αυτό ονομάζεται πρόθεμα μορφής (Format Prefix ή FP). Αξίζει να παρατηρήσουμε ότι μόνο το 15% του συνολικού χώρου έχει αποδοθεί σε κάποιες κατηγορίες ενώ το υπόλοιπο 85% είναι διαθέσιμο για επέκταση κάποιον κατηγοριών όταν χρειαστεί ή για την δημιουργία καινούργιων ανάλογα με τις ανάγκες που θα προκύψουν.

Οι βασικές κατηγορίες διευθύνσεων του IPv6

Unicast διευθύνσεις:
Είναι ο πιο ευρέως χρησιμοποιούμενος τύπος διευθύνσεων. Μια διεύθυνση τύπου unicast χαρακτηρίζει μονοσήμαντα ένα και μόνο ένα interface κάποιας μηχανής. Δηλαδή εάν ζητήσουμε να επικοινωνήσουμε με αυτή την διεύθυνση θα επικοινωνούμε μόνο με μία μηχανή, αυτήν στην οποία ανήκει τον interface που έχει αυτή την διεύθυνση.
Στον πίνακα 2 μπορούμε να δούμε ότι υπάρχουν τρείς περιοχές που χαρακτηρίζονται ως Unicast:

Αθροίσιμες Global Unicast Διευθύνσεις

Είναι Unicast διευθύνσεις οι οποίες μπορούν να χρησιμοποιηθούν για επικοινωνία στο Internet.

Τοπικής σύνδεσης Unicast διευθύνσεις

Τοπικής εμβέλειας διευθύνσεις, η βασικότερη χρήση τους είναι η επικοινωνία κατά την εκκίνηση μιας μηχανής με τον εξυπηρέτη (server) για την διαδικασία ης αυτόματης ρύθμισης της μηχανής (Autoconfiguration).

Τοπικού Δικτύου Unicast διευθύνσεις

Οι διευθύνσεις αυτές έχουν παρακρατηθεί για χρησιμοποίηση από ιδιωτικά δίκτυα που δεν είναι ακόμη συνδεμένα με το Internet και μπορούν να χρησιμοποιηθούν ελεύθερα από κάθε τέτοιο δίκτυο.

Η μορφή που έχουν οι διευθύνσεις τύπου unicast θα παρουσιασθεί σε επόμενη παράγραφο όπου και αναλύεται η ιεραρχία διευθυνσιοδότησης που χρησιμοποιεί το IPv6.

Multicast διευθύνσεις:
Μία διεύθυνση τύπου multicast χαρακτηρίζει ουσιαστικά μια ολόκληρη ομάδα από interfaces. Ένα πακέτο πληροφορίας με προορισμό μια τέτοια διεύθυνση θα παραδοθεί σε όλα τα interfaces. Οι εφαρμογές πολυμέσων χρησιμοποιούν κατά κόρο τέτοιες διευθύνσεις. Π.Χ : εφαρμογές τηλεδιάσκεψης, μετάδοση ραδιοφωνικών και τηλεοπτικών προγραμμάτων μέσω του Internet.
Σε αυτό το σημείο πρέπει να πούμε ότι το IPv6 καταργεί την έννοια των διευθύνσεων broadcast αφού τις θεωρεί υπο-περίπτωση των multicast.

Κατηγορία παρακρατημένων (Reserved) διευθύνσεων του IPv6

Η μη καθορισμένη διεύθυνση:
Η διεύθυνση 0:0:0:0:0:0:0:0 ονομάζεται μη καθορισμένη και δηλώνει την έλλειψη διεύθυνσης.

Η διεύθυνση Loopback:

Είναι η διεύθυνση 0:0:0:0:0:0:0:1 και χρησιμοποιείτε από το λειτουργικό όλων των μηχανών για διάφορες λειτουργίες.
IPv6 Addresses with Embedded IPv4 Addresses

Αυτές οι διευθύνσεις επινοήθηκαν για να βοηθήσουν στη μετάβαση από το IPv4 στο IPv6 και έχουν την γενική μορφή 0:0:0:0:0:0:IPv4 διεύθυνση.
π.χ. 0:0:0:0:0:0:143.233.241.250

Ιεραρχία διευθυνσιοδότησης

Το IPv6 στο θέμα της διευθυνσιοδότησης παρουσιάζει ένα μεγάλο πλεονέκτημα συγκριτικά με το IPv4, έχει σχεδιαστεί για ιεραρχημένη διευθυνσιοδότηση και CIDR. Οι δύο βασικότερες δομές ιεραρχίας (μέχρι στιγμής) στην απόδοση διευθύνσεων στο IPv6 είναι:
Μορφή διευθύνσεων κατανομής ανά παροχέα Internet (Provider-Based Unicast Address Format)

Είναι ιεραρχία αντίστοιχη με αυτή που χρησιμοποιείται στο IPv4 σήμερα. Στο σχήμα που ακολουθεί φαίνονται τα επίπεδα ιεραρχίας που είναι κωδικοποιημένα στην διεύθυνση (Registry, παροχέας, πελάτης).

Μήκος σε bits	3 bits	n bits	m bits	o bits	125-n-m-o bits
περιεχόμενο	Format Prefix	Registry ID	provider ID	subscriber ID	intra-subscriber

Σχήμα 1.
Μορφή διευθύνσεων κατανομής ανά παροχέα Internet.

Η μορφή αυτή έχει αντικατασταθεί από την μορφή που παρουσιάζουμε στην συνέχεια. Αθροίσιμη Μορφή διευθύνων (Aggregatable Global Unicast Address Format)

Αυτή η μορφή ιεραρχίας εμπεριέχει και την ιεραρχία ανά παροχέα ενώ πάει ένα βήμα παραπέρα θεωρώντας ότι θα υπάρχουν σημεία στα οποία θα συναντώνται ομάδες παροχέων τα οποία και ονομάζει αθροιστές κορυφαίου επιπέδου. Εάν λοιπόν οι παροχείς πάρουν το χώρο διευθύνσεων τους από

αυτούς έχουμε ακόμα μεγαλύτερη οικονομία στον αριθμό των διαδρομών που θα πρέπει να ανακοινώνονται.

Μήκος σε bits	3 bits	13 bits	32 bits	16 bits	64 bits
περιεχόμενο	Format Prefix	TLA ID	NLA ID	SLA ID	interface ID

Σχήμα 2. Αθροίσιμη Μορφή διευθύνσεων

Απόδοση

Η δικτυακή απόδοση έχει άμεση σχέση με την δρομολόγηση των πακέτων. Το ποσό της πληροφορίας που παράγεται συνεχώς αυξάνει και σε αυτό συντελούν και οι νέου είδους εφαρμογές. Οι ταχύτητες όμως που υποστηρίζουν τα LANs και τα WANs αυξάνουν και αυτές και έτσι οι λειτουργίες επεξεργασίας και προώθησης των IP πακέτων από τους δρομολογητές θα πρέπει να γίνονται ακόμα ταχύτερα.

Με αυτή τη λογική το IPv6 περιέχει λιγότερα πεδία στη κεφαλή (header) του πακέτου απ'ότι το IPv4 και εισάγει την χρήση των επεκτάσεων των κεφαλών οι οποίες βρίσκονται μεταξύ της IPv6 κεφαλής και της κεφαλής του transport επιπέδου. Η ταχύτητα λοιπόν επεξεργασίας και προώθησης του πακέτου από τους δρομολογητές αυξάνει γιατί οι περισσότερες από τις επεκτάσεις των κεφαλών δεν εξετάζονται από τους ενδιάμεσους δρομολογητές, οι οποίοι έχουν να επεξεργάσουν μόνο σταθερού μήκους IPv6 κεφαλές απλοποιώντας κατά πολύ την επεξεργασία και προώθηση.
Επίσης ο φόρτος στους ενδιάμεσους δρομολογητές μειώνεται περισσότερο αφού την διαδικασία τεμαχισμού (fragmentation) και ανασχηματισμού (reassembly) των πακέτων αναλαμβάνουν οι επικοινωνούντες hosts.

Η απόδοση με το IPv6 βελτιώνεται με την χρήση του πεδίου της κεφαλής flow label, όπου κατορθώνεται να ζητηθούν συγκεκριμένες απαιτήσεις από τους δρομολογητές για κάποια διαδρομή. Οι απαιτήσεις σχετίζονται με την προτεραιότητα, τη καθυστέρηση ή το εύρος ζώνης (bandwidth) που ζητούν κάποιες εφαρμογές όπως αυτές που μεταδίδουν video κ.α

Αύξηση της απόδοσης με το IPv6

Η αύξηση της απόδοσης στο IPv6 έχει δύο βασικές κατευθύνσεις:

1. Πρόβλεψη για Εγγυημένη ποιότητα εξυπηρέτησης από το δίκτυο Q.o.S.

Η απαίτηση για Q.o.S. είναι μια απαίτηση που εμφανίζεται κυρίως λόγο των νέων δικτυακών εφαρμογών πολυμέσων. Οι εφαρμογές αυτές στις περισσότερες περιπτώσεις περιλαμβάνουν εικόνα, ήχο, και αλληλεπίδραση ανάμεσα στους συμμετέχοντες, γεγονός που απαιτεί επικοινωνία πραγματικού χρόνου (real time). Η ιδιαιτερότητα αυτή μεταφράζεται σε σχέση με το δίκτυο σε δύο πράγματα:

Ο όγκος των πληροφοριών είναι μεγάλος και στο μεγαλύτερο μέρος τους έχουν ένα σταθερό ρυθμό bit κατά την διάρκεια της μετάδοσης (Constant Bit Rate -CBR).

Η ποιότητα του αποτελέσματος επηρεάζεται σε πολύ μεγάλο βαθμό από την καθυστέρηση που κατά περίπτωση μπορεί να υπάρχει στην μεταφορά την πληροφορίας.

Αυτά τα δύο βασικά σημεία κάνουν πολύ δύσκολη την χρησιμοποίηση των εφαρμογών αυτών στο σημερινό Internet με το IPv4 το οποίο δεν είχε σχεδιαστεί για μεταφορά πληροφορίας πραγματικού χρόνου. Τέτοιου τύπου εφαρμογές είναι επιθυμητό να χρησιμοποιούν κανάλια με μικρή καθυστέρηση και εάν είναι δυνατό μεγάλου bandwidth, αλλά κανάλια που εισάγουν μεγάλη καθυστέρηση είναι άσχημη επιλογή ανεξάρτητος του bandwidth που παρέχουν.

Στο IPv6 αναπτύσσονται ειδικοί μηχανισμοί για να εξυπηρετήσουν την νέα αυτή ανάγκη. Η ανάπτυξη όμως της δυνατότητας Q.o.S. είναι αυτή τη στιγμή η πιο πειραματική από όλες τις άλλες δυνατότητες που παρέχει το IPv6.

2. Βελτιωμένη εσωτερική σχεδίαση του πρωτοκόλλου.

Η επιλογή για σχεδίαση του πρωτοκόλλου IPv6 από την αρχή και όχι απλά εξελίσσοντας τον κώδικα που είδη είναι γραμμένος για το IPv4 παρέχει πλεονεκτήματα και στον τομέα της απόδοσης του IPv6.

Εγγυημένη Ποιότητας Εξυπηρέτησης από το Δίκτυο - Q.o.S.

Το IPv6 λαμβάνει υπόψη τις νέες απαιτήσεις των σύγχρονων εφαρμογών και περιλαμβάνει ειδικές τεχνικές για την επίτευξη της ποιότητας εξυπηρέτησης που επιθυμεί η εκάστοτε εφαρμογή.
Το θεμέλιο του Q.o.S. μπαίνει στην επικεφαλίδα του IPv6 με τα δύο πεδία Priority και Flow Label που φαίνονται στο σχήμα 1.

Επίπεδα Προτεραιότητας (Priority Level)

Το IPv6 χωρίζει την πληροφορία την οποία προωθεί σε κατηγορίες με αντίστοιχες απαιτήσεις για ποιότητα εξυπηρέτησης - προτεραιότητα (Priority).

Τα επίπεδα προτεραιότητας χωρίζονται σε δύο βασικές κατηγορίες:

Πληροφορίες που έχουν μηχανισμούς αποτροπής κορεσμού του δικτύου (congestion-controlled traffic) και περιγράφονται στον πίνακα που ακολουθεί.

Προτεραιότητα	Τύπος πληροφορίας
0	μη χαρακτηρισμένη πληροφορία
1	"filler" traffic (π.χ., netnews)
2	Μη παρακολουθούμενη μεταφορά μεγάλης ποσότητας δεδομένων (π.χ. email)
3	μελλοντική χρήση
4	Παρακολουθούμενη μεταφορά μεγάλης ποσότητας δεδομένων (π.χ.., FTP, NFS)
5	μελλοντική χρήση
6	Αλληλεπιδραστική πληροφορία (π.χ telnet, X Windows)
7	Πληροφορία ελέγχου του Internet (π.χ. πρωτόκολλα δρομολόγησης, SNMP)

Πληροφορίες που δεν έχουν μηχανισμούς αποτροπής κορεσμού του δικτύου (non-congestion-controlled traffic).

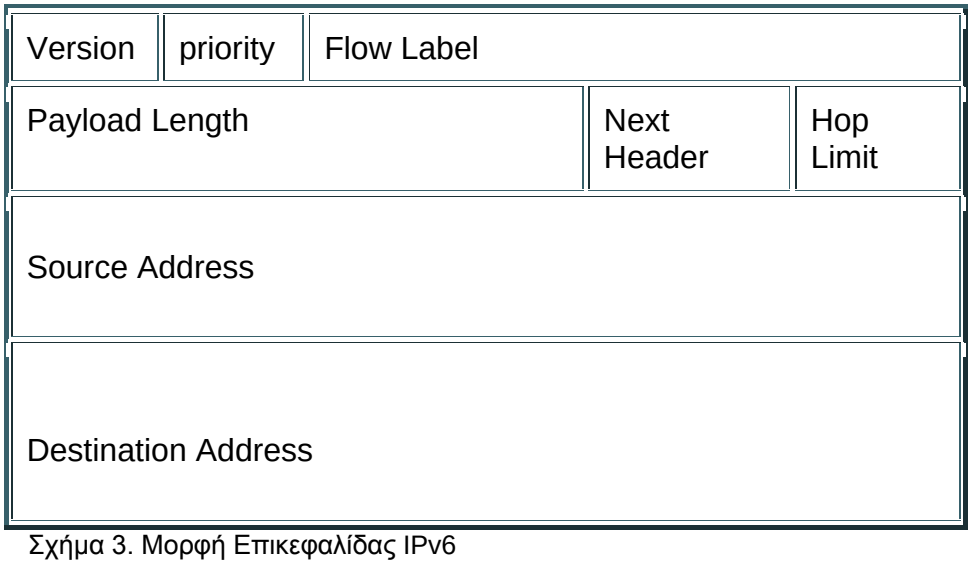
Αυτού του είδους η πληροφορία έχει αριθμούς προτεραιότητας από 8-15. Η μικρότερη προτεραιότητα θα πρέπει να χρησιμοποιείτε για πληροφορία που η απώλεια της θα επηρεάσει λιγότερο σε περίπτωση κορεσμού του δικτύου (π.χ. υψηλής ποιότητας εικόνα). Αντίστοιχα η μεγαλύτερη θα πρέπει να χρησιμοποιείτε για πιο απαραίτητη πληροφορία όπως χαμηλής ποιότητας ήχος.

Ροές Πληροφοριών (Flows)

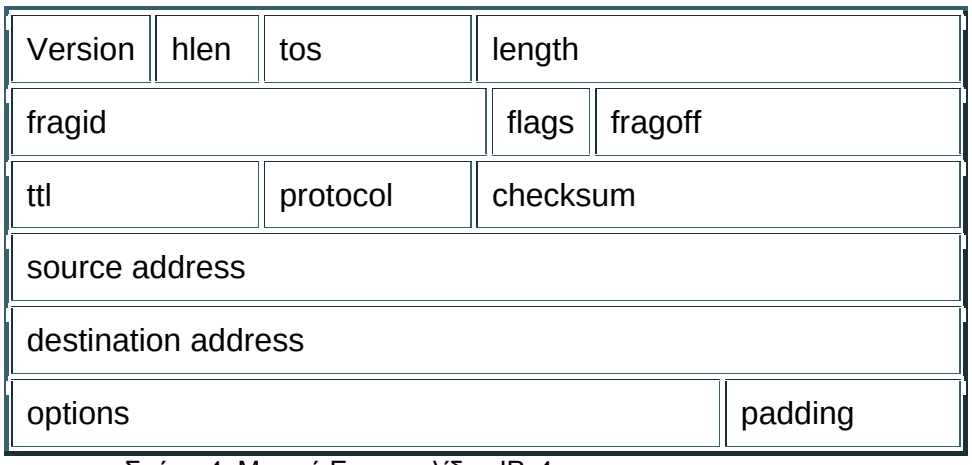
Το IPv6 εισάγει την έννοια της ροής πληροφορίας, θεωρώντας ότι τα πακέτα της πληροφορίας ρέουν μέσα από ένα ιδεατό κανάλι. Οι δρομολογητές που αποτελούν αυτό το ιδεατό κανάλι έχουν φροντίσει με κάποιο μηχανισμό να παρακρατήσουν τους απαραίτητους πόρους για την εξυπηρέτηση της ροής. Επιπλέον οι απαραίτητοι υπολογισμοί για την προώθηση κάθε πακέτου που ανήκει σε μια ροή γίνονται μόνο για το πρώτο πακέτο της πληροφορίας και εφαρμόζονται σε κάθε πακέτο της ίδιας ροής , γλιτώνοντας έτσι υπολογιστική ισχύς στον δρομολογητή και μειώνοντας σημαντικά την καθυστέρηση δρομολόγησης του πακέτου.
Η αναγνώριση της ροής στην οποία ανήκει το πακέτο επιτυγχάνεται με το πεδίο Flow Label της επικεφαλίδας του IPv6.

Βελτίωση στην εσωτερική σχεδίαση του IPv6

Η εμπειρία που έχει αποκτηθεί από την πολύχρονη χρήση και βελτίωση του IPv4 οδήγησαν στην απόρριψη χαρακτηριστικών που αποδείχτηκαν μη αποδοτικά ή δεν χρειάζονταν πλέον. Αυτές οι αλλαγές φαίνονται καθαρά στην καινούργια μορφή της επικεφαλίδας του IPv6 η οποία φαίνεται στο σχήμα 3:



Σχήμα 3. Μορφή Επικεφαλίδας IPv6



Σχήμα 4. Μορφή Επικεφαλίδας IPv4

Πεδίο Επικεφαλίδας	Μήκος (bit)	Σύντομη περιγραφή
Version	4	Αριθμός έκδοσης του IP (6)
Priority	4	Προτεραιότητα πακέτου
Flow Label	24	Αναγνωριστικό ροής
Payload Length	16	Μήκος της μεταφερόμενης πληροφορίας που ακολουθεί την επικεφαλίδα.
Next Header	8	Ο τύπος της επικεφαλίδας που ακολουθεί μετά την επικεφαλίδα του IPv6
Hop Limit	8	Μέγιστος αριθμός δρομολογητών που επιτρέπεται να περάσει το πακέτο πριν απορριφθεί.
Source Address	128	Διεύθυνση αποστολέα
Destination Address	128	Διεύθυνση παραλήπτη.

Πίνακας 5 Πεδία της επικεφαλίδας του IPv6

Συγκρίνοντας την επικεφαλίδα του IPv6 με την επικεφαλίδα του IPv4 στο σχήμα 4αμέσως παρατηρούμε την απλοποίηση που έχει γίνει στην μορφή της επικεφαλίδας κρατώντας μόνο τις άκρως απαραίτητες πληροφορίες. Σαν αποτέλεσμα έχουμε διπλάσιο μήκος σε bit της επικεφαλίδας του IPv6 σε σχέση με το IPv4 παρόλο που το μέγεθος των διευθύνσεων έχει τετραπλασιαστεί. Η επιλογές πλέον προστίθονται σαν επιπλέον επικεφαλίδες που ακολουθούν την επικεφαλίδα του IPv6 όταν αυτές χρειάζονται.

Οι σχεδιαστές για να μειώσουν τον χρόνο που ένας δρομολογητής χρειάζεται για να επεξεργαστεί ένα πακέτο φρόντισαν ώστε :

Οι δρομολογητές να χρειάζεται να επεξεργαστούν το πολύ μια επιπλέον επιλογή ενώ οι υπόλοιπες να ελέγχονται μόνο από τον παραλήπτη του πακέτου.
Το πακέτο πρέπει να ξεκινάει από τον αποστολέα με κατάλληλο μέγεθος ώστε να είναι δυνατή η μετάδοση του, από όλες της τεχνολογίες δικτύου που πρόκειται να συναντήσει στην πορεία του, χρησιμοποιώντας την τεχνική αναζήτησης της μέγιστης δυνατής μονάδας πληροφορίας (Path MTU Discovery).
Τέλος η δυνατότητα μεγάλων IP πακέτων (Jumbograms) που επιτρέπει το μεγέθους του IP πακέτου να ξεπεράσει το όριο των 65Kb που θέτει το IPv4 επιτρέπει την καλύτερη εκμετάλλευση των νέων τεχνολογιών δικτύων υψηλών ταχυτήτων όπως ATM, GigaBit Ethernet, κ.α.

Ασφάλεια

Η ανάπτυξη και η εκτεταμένη χρήση του Διαδικτύου έφερε καινούργιες απαιτήσεις από τους χρήστες οι οποίοι ζητούν οι συναλλαγές τους και η πρόσβαση στις πηγές τους να γίνονται με ασφάλεια.
Το IPv4 δεν είχε χαρακτηριστικά που θα μπορούσαν να χρησιμοποιηθούν στην ασφάλεια των δικτύων και έτσι η προσπάθεια είχε κατευθυνθεί στη χρήση μεθόδων που βασίζονται στο network επίπεδο.
Το IPv6 όμως παρέχει εγγενής δυνατότητες για παροχή ασφάλειας οι οποίες βασίζονται στις προσαρμοστικές επεκτάσεις της κεφαλής του IPv6 πακέτου. Η επέκταση της πιστοποίησης (authentication header extension) εξασφαλίζει ότι όντως το πακέτο έρχεται από τον host που δείχνει η διεύθυνση της πηγής. Αυτή η πιστοποίηση είναι σημαντική στη προστασία έναντι των εισβολέων, οι οποίοι ρυθμίζουν ένα host να παράγει πακέτα με πλαστή διεύθυνση πηγής. Αυτή η μεταμφίεση μπορεί να ξεγελάσει (IP spoofing) ένα εξυπηρέτη και να υπάρξει παράτυπη πρόσβαση σε πολύτιμα δεδομένα ή σε κρίσιμες δικτυακές λειτουργίες. Σύμφωνα με στατιστικές έρευνες αυτού του είδους το “ξεγέλασμα” (IP spoofing) ενός εξυπηρετητή είναι από τους πιο συνηθισμένους τρόπους εισβολής και δεν υπάρχει εγγενής τρόπος από το IPv4 να ελέγξει εάν το πακέτο έρχεται από εκεί που το ίδιο αναφέρει. Η σημερινή αντιμετώπιση αυτού του προβλήματος γίνεται με τους “Firewalls” η χρήση των οποίων παρουσιάζει μία σειρά από προβλήματα όπως μείωση στην απόδοση, περιοριστική δικτυακή πολιτική και περιορισμένη διασύνδεση με το Διαδίκτυο.
Μία άλλη διαδεδομένη παγίδα στο Διαδίκτυο είναι οι αναλυτές της κυκλοφορίας της πληροφορίας (sniffers) οι οποίοι λαθραία παρακολουθούν τη πληροφορία που διέρχεται στο δίκτυο. Με αυτό το τρόπο μπορούν να γίνουν γνωστά εμπορικά μυστικά, αριθμοί τραπεζικών λογαριασμών και “πλαστικών” καρτών, συνθηματικά (passwords) καθώς και άλλα πολύτιμα δεδομένα.
Το IPv6 παρέχει και σε αυτό το πρόβλημα εγγενή λύση μέσω της επέκτασης για κρυπτογράφηση της κεφαλής του IPv6 πακέτου όπου διαμέσου κλειδιών κρυπτογράφησης γίνεται κρυπτογράφηση του περιεχομένου (payload) του

πακέτου. Η χρήση των επεκτάσεων ασφαλείας μπορεί να γίνει απ'ευθείας μεταξύ δύο hosts ή σε συνδυασμό με μία πύλη ασφαλείας (security gateway) η οποία και προσθέτει ένα βαθμό περισσότερης ασφάλειας.

Ασφάλεια στο IPv6

Στο IPv6 η ασφάλεια βασίζεται αποκλειστικά στο επίπεδο IP (IP level Security), δηλαδή όλες οι διαδικασίες ασφάλειας έχουν σκοπό την προστασία του IP πακέτου από κάθε είδος επίθεσης κατά την πορεία του μέσα από το δίκτυο. Η ασφάλεια στο επίπεδο IP μπορεί να παρέχει τις εξής δυνατότητες:

Πιστοποίηση (Authentication)

Πιστοποίηση είναι η ικανότητα να γνωρίσουμε ότι τα δεδομένα που παραλήφθηκαν είναι αυτά που έστειλε ο αποστολέας και ότι ο αποστολέας είναι αυτός που ισχυρίζεται.

Ακεραιότητα πληροφορίας (Integrity)

Η ακεραιότητα της πληροφορίας είναι η δυνατότητα να ανιχνεύεται οποιαδήποτε αλλαγή της πληροφορίας στην ενδιάμεση διαδρομή από τον αποστολέα στον παραλήπτη.

Απόρρητο της πληροφορίας (Confidentiallity)

Το απόρρητο της πληροφορίας είναι η δυνατότητα να είναι διαθέσιμη σε κατανοητή μορφή μόνο από τους πραγματικούς παραλήπτες. Με αυτό τον τρόπο είναι σχεδόν αδιάφορο ποιοι μπορούν να υποκλέψουν την πληροφορία κατά την διάρκεια της πορείας της προς τον τελικό προορισμό της .

Απόδειξη αποστολής δεδομένων από τον αποστολέα (Non-repudiation)

Με αυτή την δυνατότητα είναι αδύνατο να αρνηθεί ένας αποστολέας το γεγονός της αποστολής των δεδομένων. Η δυνατότητα αυτή είναι διαθέσιμη μόνο όταν χρησιμοποιείται ένας ασύμμετρος αλγόριθμος κρυπτογράφησης. Η ασφάλεια σε επίπεδο IP και σαν συνέπεια η ασφάλεια που παρέχει το IPv6. δεν μπορεί να καλύψει όλες τις περιπτώσεις επιθέσεων. Μια τέτοια περίπτωση είναι η περίπτωση της ανάλυσης της ροής της πληροφορίας (traffic analysis). Η ανάλυση αυτή μπορεί να παρέχει χρήσιμες πληροφορίες για έναν πιθανό εισβολέα, όπως η συχνότητα ανταλλαγής πληροφοριών των μηχανισμών ασφαλείας, το μέγεθος των πακέτων ή ακόμα και ο τύπος της πληροφορίας που κάποιος χρήστης αναζητεί στο Internet.

Μηχανισμοί ασφάλειας του IPv6

Το IPv6 χρησιμοποιεί δύο βασικούς μηχανισμούς για να παρέχει τις υπηρεσίες ασφάλειας που αναφέρθηκαν στην προηγούμενη παράγραφο. Οι μηχανισμοί αυτοί είναι :

IP Authentication Header
IP Encapsulating Security Payload

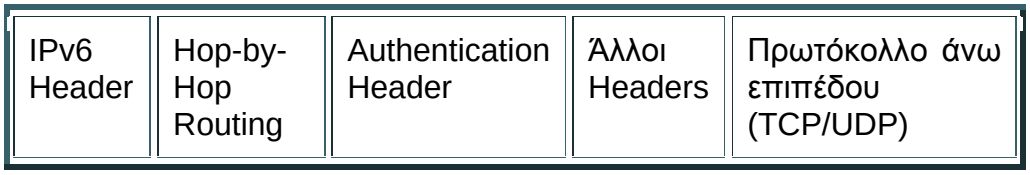
Οι δύο αυτοί μηχανισμοί βασίζονται κυρίως σε εξωτερικούς μηχανισμούς κρυπτογράφησης για να παρέχουν ασφάλεια. Να σημειώσουμε ότι η κρυπτογράφηση χρησιμοποιεί κάποια κλειδιά η διαχείριση των οποίων είναι ένα πολύ σημαντικό θέμα. Ο κυρίως λόγος είναι ότι η διαχείριση δεν είναι στενά συνδεδεμένη με την δομή και λειτουργία του IPv6 και μπορεί να αλλάξει στο μέλλον χωρίς απαραίτητα να επηρεάσει το IP.

IP Authentication Header

Ο μηχανισμός του IP authentication Header μπορεί να παρέχει τις εξής δυνατότητες ασφάλειας:

- Πιστοποίηση (Authentication).
- Ακεραιότητας την πληροφορίας (Integrity).

Απόδειξη αποστολής δεδομένων από τον αποστολέα (Non-repudiation).
Ο μηχανισμός αυτός στο IPv6 προστίθεται σαν μια έξτρα επικεφαλίδα όπως φαίνεται και στο Σχήμα 6. Η κύρια πληροφορία που υπάρχει στην επικεφαλίδα αυτή είναι ένα νούμερο το οποίο είναι το αποτέλεσμα της εφαρμογής του χρησιμοποιούμενου αλγόριθμου κρυπτογράφησης σε όλο το πακέτο.



Σχήμα 6. Μορφή IP πακέτου με Authentication Header

IP Encapsulating security Payload (ESP)

Ο μηχανισμός του IP Encapsulating security Payload μπορεί να παρέχει τις εξής δυνατότητες ασφάλειας:

- Ακεραιότητας την πληροφορίας (Intergrity).
- Απόρρητο της πληροφορίας (Confidentiality)
- Απόδειξη αποστολής δεδομένων από τον αποστολέα (Non-repudiation).

Η λειτουργία αυτού του μηχανισμού βασίζεται στην κρυπτογράφηση της προς μετάδοσης πληροφορίας. Με αυτό τον τρόπο μόνο ο παραλήπτης που έχει στην κατοχή του το κατάλληλο κλειδί μπορεί να αποκρυπτογραφήσει την πληροφορία. Η γενική μορφή ενός πακέτου IP που χρησιμοποιεί την λειτουργία IP Encapsulating security Payload φαίνεται στο Σχήμα 7
.

<-- Μη κρυπτογραφημένα -->		<-- Κρυπτογραφημένα -->	
IP Header	Άλλη IP Headers	ESP Header	Encrypted Data

Σχήμα 7. Μορφή IP πακέτου με IP Encapsulating security Payload

Ο μηχανισμός του ESP μπορεί να χρησιμοποιηθεί με δύο τρόπους:

1. Εφαρμογή σε Transport επίπεδο.

   Σε αυτή την περίπτωση η κρυπτογραφημένη πληροφορία περιέχει μόνο το πακέτο του επιπέδου μεταφοράς (Transport TCP/UDP). Δηλαδή την επικεφαλίδα του επιπέδου Transport και τα δεδομένα του χρήστη. Σαν αποτέλεσμα δεν έχουμε προστασία των IP Headers.

2. Εφαρμογή σε Tunnel επίπεδο.

   Σε αυτή την περίπτωση γίνεται κρυπτογράφηση ολόκληρου του IP πακέτου. Ο τρόπος αυτός χρήσης είναι ιδιαίτερα χρήσιμος για την δημιουργία VPN’s

Εφαρμογή των μηχανισμών ασφαλείας

Οι μηχανισμοί ασφάλειας του IP μπορούν να εφαρμοστούν σε παραλλαγές που επιτρέπουν την συμμετοχή μηχανών που δεν έχουν στη στοίβα τους, υποστήριξη για τους μηχανισμούς αυτούς. Οι τρεις δυνατές περιπτώσεις περιγράφονται στην συνέχεια.

- **Σταθμός εργασίας με Σταθμό εργασίας**
  Σε αυτή την περίπτωση έχουμε επικοινωνία μεταξύ δύο υπολογιστών, που έχουν και οι δύο την ικανότητα να χρησιμοποιήσουν τους μηχανισμού ασφαλείας.

- **Δρομολογητής/ Πύλη Ασφάλειας με Σταθμό εργασίας**
  Ο ένας από τους δύο host είναι διαθέτει μηχανισμού ασφαλείας. Ο άλλος host βρίσκεται σε κάποιο δίκτυο στο οποίο όλοι οι host θεωρούνται έμπιστοι μεταξύ τους και ένα gateway αναλαμβάνει να διασφαλίσει την ασφάλεια των επικοινωνιών με τον υπόλοιπο κόσμο εκτός του εσωτερικού δικτύου.

- **Δρομολογητής/ Πύλη Ασφάλειας με Δρομολογητή/ Πύλη Ασφάλειας**
  Τέλος έχουμε την περίπτωση δύο δικτύων που εμπιστεύονται όλους τους host που το καθένα περιλαμβάνει και επιθυμούν μιλήσουν μεταξύ τους εξασφαλίζοντας ασφάλεια από το υπόλοιπο δύκτιο. Ουσιαστικά αυτή η περίπτωση απεικονίζει ένα VPN. Εδώ βρίσκει εφαρμογή το Tunnel επίπεδο λειτουργίας της μεθόδου IP Encapsulating security Payload του IPv6.

Το κόστος της αυξημένης ασφάλειας σε απόδοση

Η αύξηση της ασφάλειας αυξάνει τον υπολογιστικό φόρτο για κάθε πακέτο που δημιουργείται. Σαν αποτέλεσμα αυξάνεται η καθυστέρηση μετάδοσης της πληροφορίας. Ειδικά για την περίπτωση IP Encapsulating Security Payload η μείωση της απόδοσης του δικτύου μπορεί να είναι ιδιαίτερα αισθητή. Η μείωση αυτή της απόδοσης περιορίζεται μόνο στις μηχανές που συμμετέχουν στους μηχανισμούς ασφαλείας και δεν επηρεάζει τους ενδιάμεσους δρομολογητές όταν δεν συμμετέχουν στον μηχανισμό.

ΚΕΦΑΛΑΙΟ 2
ΑΝΑΦΟΡΑ ΣΤΟ TCP/IP

Εισαγωγή

Ο σκοπός αυτού του κεφαλαίου είναι να εξεταστούν οι λεπτομέρειες των πρωτοκόλλων που επιτρέπουν, έλεγχο, ή συμβολή στη δρομολόγηση του TCP/ IP, όχι για να κάνει μια σε βάθος μελέτη της ακολουθίας πρωτοκόλλου TCP/IP.

Η σύλληψη της ιδέας στις αρχές της δεκαετίας του '70 από τον Vint Cerf και Bob Kahn, το TCP/IP και η σε στρώσεις αρχιτεκτονική του πρωτοκόλλου προηγείται χρονικώς του προτύπου αναφοράς της OSI του ISO. Μια συνοπτική αναθεώρηση των στρωμάτων TCP/IP θα είναι χρήσιμη στην κατανόηση πώς συσχετίζονται οι διάφορες λειτουργίες και υπηρεσίες που εξετάζονται σε αυτό το κεφάλαιο.

Τα στρώματα πρωτοκόλλου TCP / IP

Το σχήμα 2.1 παρουσιάζει μια ακολουθία του πρωτοκόλλου TCP/IP σε σχέση με το πρότυπο αναφοράς της OSI. Το στρώμα διεπαφών δικτύων, που αντιστοιχεί στα στρώματα φυσικό και συνδέσεων δεδομένων στην OSI, δεν είναι πραγματικά μέρος της προδιαγραφής. Εντούτοις, έχει γίνει ένα de facto στρώμα είτε όπως φαίνεται στο σχήμα 2.1 είτε ως χωριστά στρώματα, φυσικό και συνδέσεων δεδομένων. Περιγράφεται σε αυτό το τμήμα από την άποψη της OSI στα στρώματα φυσικό και συνδέσεων δεδομένων.

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>APPLICATION</td><td rowspan="3">APPLICATION</td></tr>
<tr><td>PRESENTATION</td></tr>
<tr><td>SESSION</td></tr>
<tr><td>TRANSPORT</td><td>HOST-TO-HOST</td></tr>
<tr><td>NETWORK</td><td>INTERNET</td></tr>
</table>

DATA LINK	NETWORK INTERFACE
PHYSICAL	

Σχήμα 2.1
Η ακολουθία πρωτοκόλλου TCP/IP

Το φυσικό στρώμα περιέχει τα πρωτόκολλα σχετικά με το φυσικό μέσο στο οποίο το TCP/IP θα επικοινωνεί. Επίσημα, τα πρωτόκολλα αυτού του στρώματος εμπίπτουν σε τέσσερις κατηγορίες που περιγράφουν μαζί όλες τις πτυχές των φυσικών μέσων:

- Τα ηλεκτρικά / οπτικά πρωτόκολλα περιγράφουν τα χαρακτηριστικά σημάτων όπως η τάση ή τα φωτονιακά επίπεδα, συγχρονισμός bit, κωδικοποίηση και μορφή σημάτων.
- Τα μηχανικά πρωτόκολλα είναι προδιαγραφές όπως οι διαστάσεις ενός συνδετήρα ή το μεταλλικό περίβλημα ενός καλωδίου.
- Τα λειτουργικά πρωτόκολλα περιγράφουν τι κάτι κάνει. Παραδείγματος χάριν, “Request to Send” είναι η λειτουργική περιγραφή της καρφίτσας 4 ενός συνδετήρα EIA-232-D.
- Τα διαδικαστικά πρωτόκολλα περιγράφουν πώς κάτι γίνεται. Παραδείγματος χάριν, ένα δυαδικό 1 αντιπροσωπεύεται σε έναν αγωγό EIA-232-D ως τάση πιο αρνητική από -3 βολτ.

Το στρώμα συνδέσεων δεδομένων περιέχει τα πρωτόκολλα που ελέγχουν το φυσικό στρώμα: πώς το μέσο προσεγγίζεται και μοιράζεται, πώς οι συσκευές στο μέσο προσδιορίζονται και πώς το δεδομένο είναι πλαισιωμένο πριν να διαβιβαστεί επάνω στο μέσο. Τα παραδείγματα των πρωτοκόλλων συνδέσεων δεδομένων είναι IEEE 802.3/Ethernet, IEEE 802.5/Token Ring, and FDDI.

Το στρώμα Διαδικτύου, που αντιστοιχεί στο στρώμα δικτύων της OSI, είναι πρώτιστα αρμόδιο για τη διευκόλυνση της δρομολόγησης των δεδομένων στα λογικά μονοπάτια του internetwork, με τον καθορισμό ενός σχήματος πακέτων και ενός σχήματος εξέτασης.

Το host-to-host στρώμα, αντιστοιχίζεται στο στρώμα μεταφορών της OSI, διευκρινίζει τα πρωτόκολλα που ελέγχουν το στρώμα Διαδικτύου, όπως το

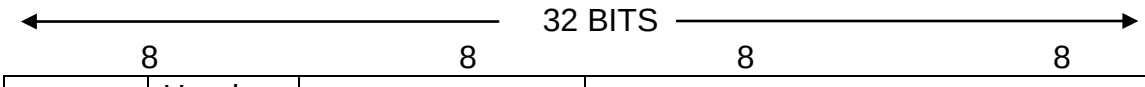
στρώμα συνδέσεων δεδομένων ελέγχει το φυσικό στρώμα. Και τα δύο, host-to-host και τα στρώματα συνδέσεων δεδομένων μπορούν να καθορίσουν τέτοιους μηχανισμούς όπως τον έλεγχο ροής και λάθους. Η διαφορά είναι ότι ενώ τα πρωτόκολλα συνδέσεων δεδομένων ελέγχουν την κυκλοφορία στη σύνδεση δεδομένων — το φυσικό μέσο συνδέει δύο συσκευές — το στρώμα μεταφορών ελέγχει την κυκλοφορία στη λογική σύνδεση — η end-to-end σύνδεση δύο συσκευών των οποίων η λογική σύνδεση διαπερνά μια σειρά συνδέσεων σύνδεση δύο συσκευών των οποίων η λογική σύνδεση διαπερνά τη σειρά συνδέσεων δεδομένων.

Το στρώμα εφαρμογής αντιστοιχεί στα στρώματα της OSI, συνδιάλεξης, παρουσίασης και εφαρμογής. Αν και μερικά πρωτόκολλα δρομολόγησης όπως BGP και RIP κατοικούν σε αυτό το στρώμα, τις πιο κοινές υπηρεσίες του στρώματος εφαρμογής παρέχουν οι διεπαφές από τις οποίες οι εφαρμογές χρηστών έχουν πρόσβαση στο δίκτυο.

Μια λειτουργία κοινή για την ακολουθία πρωτοκόλλου του σχήματος 2.1 και οποιωνδήποτε άλλων ακολουθιών πρωτοκόλλου πολυπλεξίας μεταξύ των στρωμάτων. Πολλές εφαρμογές μπορούν να χρησιμοποιήσουν μια υπηρεσία host-to-host layer και πολλές υπηρεσίες host-to-host layer μπορούν να χρησιμοποιήσουν το στρώμα Διαδικτύου. Πολλαπλάσιες ακολουθίες πρωτοκόλλου (IP, IPX, AppleTalk, παραδείγματος χάριν) μπορούν να μοιραστούν μια φυσική σύνδεση μέσω των κοινών πρωτοκόλλων συνδέσεων δεδομένων.

Η κεφαλή πακέτων IP

Το σχήμα 2.2 παρουσιάζει το σχήμα της κεφαλής πακέτων IP, που διευκρινίζεται σε RFC 791. Οι περισσότεροι τομείς σε αυτό το πακέτο έχουν κάποια σημασία στη δρομολόγηση.



Version	Header Length	Type of Service		Total length			
Identifier				Flags	Fragmented Offset		
Time to Live		Protocol		Header Checksum			
Source Address							
Destination Address							
Options							Padding

Σχήμα 2.2
Το πρωτόκολλο πακέτων IP.

Η έκδοση προσδιορίζει την έκδοση IP στην οποία το πακέτο ανήκει. Αυτός ο τομέας τεσσάρων-bit θέτεται συνήθως στο δυαδικό 0100, έκδοση 4 (IPv4) είναι σε συνεχή, κοινή χρήση. Μια νεώτερη έκδοση του πρωτοκόλλου, όχι ακόμα τόσο διαδεδομένο, είναι έκδοση 6 (IPv6), μερικές φορές καλούμενο "next-generation IP" (IPng). Όλοι οι τωρινοί ορισμένοι αριθμοί έκδοσης μπορούν να φανούν στον πίνακα 2.1, μαζί με μερικά από τα σχετικά RFCs. Όλες οι εκδόσεις εκτός από 4 και 6 (στηριγμένες σε μια προηγούμενη πρόταση αποκαλούμενη απλό πρωτόκολλο Διαδικτύου, ή SIP, που το οποίο έφερε επίσης έναν αριθμό έκδοσης 6) τώρα υπάρχουν μόνο ως "πολιτισμός" και θα αφεθούν στον περίεργο να διαβάσει τα αναφερόμενα RFCs.

Το μήκος κεφαλών είναι ένας τομέας τεσσάρων bit που λέει, όπως το όνομα υπονοεί, το μήκος της κεφαλής IP. Ο λόγος που αυτός ο τομέας συμπεριλαμβάνεται είναι ότι ο τομέας επιλογών (περιγράφεται αργότερα στο κεφάλαιο) μπορεί να ποικίλει στο μέγεθος. Το ελάχιστο μήκος της κεφαλής IP είναι 20 οχτάδες και οι επιλογές μπορούν να αυξήσουν αυτό το μέγεθος μέχρι ένα μέγιστο 24 οχτάδων. Αυτός ο τομέας περιγράφει το μήκος της κεφαλής από την άποψη των τριανταδυάμπιτων λέξεων — πέντε για το ελάχιστο μέγεθος 160-bit και έξι για το μέγιστο.

Πίνακας 2.1
Αριθμοί έκδοσης IP.

Number	Version	RFC
0	Reserved	
1-3	Unassigned	
4	Internet Protocol (IP)	791
5	ST Datagram Mode	1190
6	Simple Internet Protocol (SIP)	
6	IPng	1883
7	TP/IX	1475
8	P Internet Protocol (PIP)	1621
9	TCP and UDP over Bigger	1347
10-14	Addresses(TUBA)	
15	Unassigned	
	Reserved	

Τύπος υπηρεσίας (TOS) είναι ένας οκτώ-bit τομέας που μπορεί να χρησιμοποιηθεί για τη διευκρίνιση του ειδικού χειρισμού του πακέτου. Αυτός ο τομέας μπορεί πραγματικά να χωριστεί σε δύο υποκατηγορίες: Προτεραιότητα και TOS. Η προτεραιότητα θέτει μια προτεραιότητα για το πακέτο, ο τρόπος που ένα πακέτο μπορεί να σταλεί τη νύχτα, δύο ημερών παράδοση, ή γενική ενημέρωση. Το TOS επιτρέπει την επιλογή μιας υπηρεσίας παράδοσης από την άποψη της ρυθμοαπόδοσης, της καθυστέρησης, της αξιοπιστίας, και του νομισματικού κόστους. Αν και αυτός ο τομέας δεν χρησιμοποιείται συνήθως (όλα τα bit τείθονται συνήθως μηδέν), πρόωρες προδιαγραφές του Open Shortest Path First (OSPF) πρωτόκολλο αποκαλούνται για δρομολόγηση TOS. Επίσης, τα κομμάτια προτεραιότητας χρησιμοποιούνται περιστασιακά στην ποιότητα των εφαρμογών υπηρεσιών (QoS).

Το συνολικό μήκος είναι ένας δεκαέξι-bit τομέας που διευκρινίζει το συνολικό μήκος του πακέτου, συμπεριλαμβανομένης της κεφαλής, σε οχτάδες. Με την αφαίρεση του μήκους κεφαλής, ο δέκτης μπορεί να καθορίσει ότι το μέγεθος των δεδομένων του πακέτου είναι pay-load. Επειδή ο μεγαλύτερος δεκαδικός αριθμός που μπορεί να περιγραφεί με 16 bit είναι 65.535, το μέγιστο πιθανό μέγεθος ενός πακέτου IP είναι 65.535 οχτάδες.

Το προσδιοριστικό είναι ένας δεκαέξι-bit τομέας που χρησιμοποιείται από κοινού με τους τομείς: σημαίες και το τεμάχιο μετατόπισης για τον τεμαχισμό

ενός πακέτου. Τα πακέτα πρέπει να τεμαχιστούν σε μικρότερα πακέτα εάν το αρχικό μήκος υπερβαίνει τη Μέγιστη Μονάδα Μετάδοσης (MTU) μιας σύνδεσης δεδομένων μέσω της οποίας περνούν. Παραδείγματος χάριν, εξετάστε ένα πακέτο 5.000-byte που ταξιδεύει μέσω ενός internetwork. Αντιμετωπίζει μια σύνδεση δεδομένων της οποίας το MTU είναι 1.500 byte — δηλαδή το πλαίσιο μπορεί να περιέχει ένα μέγιστο μέγεθος πακέτων 1.500 byte. Ο δρομολογητής που τοποθετεί το πακέτο επάνω σε αυτήν την σύνδεση δεδομένων πρέπει πρώτα να τεμαχίσει το πακέτο σε κομμάτια λιγότερα από 1.500 οχτάδες, το κάθε ένα. Ο δρομολογητής χαρακτηρίζει έπειτα κάθε τεμάχιο, με τον ίδιο αριθμό στον τομέα προσδιοριστικών έτσι ώστε μια λαμβάνουσα συσκευή μπορεί να προσδιορίσει τα τεμάχια που πηγαίνουν από κοινού.

Οι σημαίες είναι ένας τομέας τριών-bit στον οποίο το πρώτο bit είναι αχρησιμοποίητο. Το δεύτερο είναι το Μη Τεμαχισμένο (DF) bit. Όταν στο DF κομμάτι τίθεται το ένα, ένας δρομολογητής δεν μπορεί να τεμαχίσει το πακέτο. Εάν το πακέτο δεν μπορεί να διαβιβαστεί χωρίς τεμαχισμό, ο δρομολογητής ρίχνει το πακέτο και στέλνει ένα μήνυμα λάθους στην πηγή. Αυτή η λειτουργία επιτρέπει τη δοκιμή MTUs σε ένα internetwork. Το df bit μπορεί να τεθεί χρησιμοποιώντας τη χρησιμότητα του Extended Ping στους δρομολογητές Cisco.

Το τρίτο bit είναι το bit των Περισσότερων Τεμαχίων (MF). Όταν ένας δρομολογητής τεμαχίζει ένα πακέτο, θέτει το bit MF σε ένα, σε όλο εκτός από το τελευταίο τεμάχιο έτσι ώστε ο δέκτης να ξέρει για να συνεχίζει τα τεμάχια έως ότου αντιμετωπίζει ένα τεμάχιο με MF=0.

Η μετατόπιση τεμαχίων είναι ένας τομέας 13-bit που διευκρινίζει τη μετατόπιση, σε μονάδες οκτώ οχτάδων, από την αρχή της κεφαλής στην αρχή του τεμαχίου. Επειδή τα τεμάχια δεν μπορούν πάντα να φθάνουν με σειρά, ο τομέας μετατόπισης τεμαχίου επιτρέπει στα κομμάτια να συγκεντρωθούν εκ νέου στη σωστή σειρά.

Σημειώστε ότι εάν ένα τεμάχιο χάνεται κατά τη διάρκεια μιας μετάδοσης, ολόκληρο το πακέτο πρέπει να ξανασταλθεί στο ίδιο σημείο στο internetwork. Επομένως, οι επιρρεπείς σε λάθη συνδέσεις δεδομένων θα μπορούσαν να προκαλέσουν μια δυσανάλογη καθυστέρηση. Και εάν ένα τεμάχιο χάνεται

λόγω της συμφόρησης η αναμετάδοση ολόκληρης της σειράς τεμαχίων μπορεί να αυξήσει τη συμφόρηση.

Time to live (TTL) είναι ένας οκτώ-bit τομέας που θα τεθεί με έναν ορισμένο αριθμό όταν παράγεται αρχικά το πακέτο. Καθώς το πακέτο περνά από δρομολογητή σε δρομολογητή, κάθε δρομολογητής μειώνει αυτόν τον αριθμό. Εάν ο αριθμός φθάσει σε μηδέν, το πακέτο θα απορριφθεί και ένα μήνυμα λάθους θα σταλεί στην πηγή. Αυτή η διαδικασία αποτρέπει τα "χαμένα" πακέτα από το να περιπλανούνται ατέλειωτα μέσα στο internetwork.
Όπως αρχικά συλλαμβάνεται, το TTL διευκρινίστηκε σε δευτερόλεπτα, εάν ένα πακέτο καθυστερούσε περισσότερο από ένα δευτερόλεπτο σε έναν δρομολογητή, ο δρομολογητής θα ρύθμιζε το TTL αναλόγως. Εντούτοις, αυτή η προσέγγιση είναι δύσκολο να εφαρμοστεί και υποστηρίζεται σπάνια. Οι περισσότεροι δρομολογητές μειώνουν απλά το TTL κατά ένα, όποια και αν είναι η πραγματική καθυστέρηση, έτσι το TTL είναι πραγματικά a hop count. Η συνιστώμενη προεπιλογή TTL είναι 64, αν και οι τιμές όπως 15 και 32 δεν είναι ασυνήθιστες.
Μερικές ανιχνευτικές λειτουργίες , όπως η εντολή trace της Cisco, χρησιμοποιούν τον τομέα TTL. Εάν στο δρομολογητή δοθεί η εντολή να ανιχνεύσει τη διαδρομή σε μια διεύθυνση οικοδεσποτών όπως 10.11.12.13, ο δρομολογητής θα στείλει τρία πακέτα με το TTL καθορισμένο σε ένα, ο πρώτος δρομολογητής θα το μειώσει αυτό σε μηδέν, θα ρίξει τα πακέτα, και θα στείλει μηνύματα λάθους στην πηγή. Με την ανάγνωση της διεύθυνσης προέλευσης των μηνυμάτων λάθους, ο πρώτος δρομολογητής της πορεία είναι τώρα γνωστός. Τα επόμενα τρία πακέτα θα σταλούν με ένα TTL δύο. Ο πρώτος δρομολογητής θα το μειώσει σε ένα, ο δεύτερος σε μηδέν, και ένα μήνυμα λάθους παραλαμβάνεται από το δεύτερο δρομολογητή. Το τρίτο σύνολο έχει ένα TTL τρία, και ούτω καθ'εξής, μέχρι να βρεθεί ο προορισμός. Όλοι οι δρομολογητές κατά μήκος της πορείας internetwork θα έχουν προσδιοριστεί.
Το πρωτόκολλο είναι ένας οκτώ-bit τομέας που δίνει τη "διεύθυνση," ή τον αριθμό πρωτοκόλλου, του host-to-host ή πρωτόκολλο στρώματος μεταφορών για το οποίο οι πληροφορίες του πακέτου προορίζονται. Ο πίνακας 2.2

παρουσιάζει μερικά από τα πιο κοινά των 100 διαφορετικών αριθμών πρωτοκόλλου που ορίζονται αυτήν την περίοδο.

Πίνακας 2.2 Μερικοί - γνωστοί αριθμοί πρωτοκόλλου.

Protocol Number	Host-to-Host Layer Protocol
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
3	Gateway to Gateway Protocol (GGP)
4	IP in IP
6	Transmission Control Protocol (TCP)
8	Exterior Gateway Protocol (EGP)
17	User Datagram Protocol (UDP)
35	Inter-Domain Policy Routing Protocol (IDPR)
45	Inter-Domain Routing Protocol (IDRP)

Η κεφαλή Checksum είναι ο τομέας διορθώσεων λάθους για την κεφαλή IP. Το Checksum δεν υπολογίζεται για encapsulated data, τα UDP, TCP και ICMP έχουν τα δικά τους checksums για να το κάνουν αυτό. Ο τομέας περιέχει έναν 16-bit checksum συμπληρώματός κάποιου, που υπολογίζεται από το δημιουργό του πακέτου. Ο δέκτης θα υπολογίσει πάλι το άθροισμα ενός 16-bit συμπληρώματός κάποιου, συμπεριλαμβανομένου του αρχικού checksum. Εάν κανένα λάθος δεν έχει εμφανιστεί κατά τη διάρκεια των δρομολογιών του πακέτου, το προκύπτον checksum θα γίνει όλο ένα. Θυμηθείτε ότι κάθε δρομολογητής μειώνει το TTL, επομένως, το checksum πρέπει να υπολογιστεί εκ νέου σε κάθε δρομολογητή.

Οι διευθύνσεις πηγής και προορισμού είναι οι 32-bit διευθύνσεις IP του δημιουργού του πακέτου και του προορισμού του πακέτου. Το σχήμα των διευθύνσεων IP καλύπτεται στο επόμενο τμήμα, "διευθύνσεις IP."

Οι επιλογές είναι ένας τομέας μεταβλητού-μήκους και όπως το όνομα υπονοεί, είναι προαιρετικές. Ένα διάστημα προστίθεται στην κεφαλή των πακέτων για να περιέχει είτε τις πληροφορίες πηγής είτε για άλλους δρομολογητές για να εισαγάγει τις πληροφορίες, οι επιλογές χρησιμοποιούνται πρώτιστα για τη δοκιμή. Οι πολύ συχνά χρησιμοποιημένες επιλογές ακολουθούν.

- Χαλαρή δρομολόγηση πηγής, στην οποία μια σειρά διευθύνσεων IP για τις διεπαφές του δρομολογητή παρατίθεται. Το πακέτο πρέπει να περάσει μέσω κάθε μιας από αυτές τις διευθύνσεις, αν και πολλαπλά βήματα μπορούν να γίνουν μεταξύ των διευθύνσεων.

- Ακριβής δρομολόγηση πηγής, όπου πάλι μια σειρά από διευθύνσεις του δρομολογητή παρατίθενται. Αντίθετα από τη χαλαρή δρομολόγηση πηγής, το πακέτο πρέπει να ακολουθήσει τη διαδρομή ακριβώς. Εάν το επόμενο βήμα δεν είναι η επόμενη διεύθυνση στον κατάλογο, ένα λάθος εμφανίζεται.
- Η διαδρομή αρχείων παρέχει χώρο για κάθε δρομολογητή για να εισαγάγει τη διεύθυνση της εξερχόμενης διεπαφής του καθώς το πακέτο μεταφέρεται, έτσι ώστε ένα αρχείο διατηρείται από κάθε δρομολογητή που το πακέτο διέρχεται.
  Η διαδρομή αρχείων παρέχει μια λειτουργία παρόμοια με το μονοπάτι εκτός από ότι οι εξερχόμενες διεπαφές και στην πορεία στον προορισμό και στην επιστροφής πορεία καταγράφονται.

- Timestamp είναι μια επιλογή παρόμοια με τη διαδρομή αρχείων μόνο που κάθε δρομολογητής εισάγει επίσης timestamp — το πακέτο όχι μόνο κρατά τη διαδρομή όπου ήταν αλλά και αρχεία όταν ήταν εκεί.

Padding εξασφαλίζει ότι οι κεφαλές τελειώνουν σε ένα 32-bit όριο με την προσθήκη μηδενικών μετά από τον τομέα επιλογής μέχρι ένα πολλαπλάσιο του 32 να επιτευχθεί.

IP διευθύνσεις

Οι διευθύνσεις IP είναι 32 bit, όπως όλες οι διευθύνσεις στο επίπεδο του δικτύου, έχουν ένα κομμάτι για το δίκτυο και ένα κομμάτι για τους οικοδεσπότες. Το κομμάτι του δικτύου προσδιορίζει μεμονωμένα τη σύνδεση δεδομένων (δηλαδή το δίκτυο) και είναι κοινή για όλες τις συσκευές που συνδέονται με το δίκτυο. Το κομμάτι των οικοδεσποτών προσδιορίζει μεμονωμένα μια ιδιαίτερη συσκευή που συνδέεται με το δίκτυο.

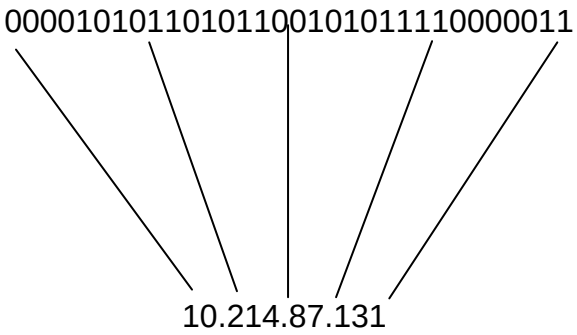
Υπάρχουν διάφοροι τρόποι να αντιπροσωπευθούν τα 32 bit μιας διεύθυνσης IP. Παραδείγματος χάριν, η 32-bit διεύθυνση IP

00001010110101100101011110000011

θα μπορούσε να αντιπροσωπευθεί στο δεκαδικό ως 181,819,267.

Το δυαδικό σχήμα είναι δυσκίνητο και το δεκαδικό σχήμα είναι χρονοβόρο να υπολογίσει. Ένα καλύτερο σχήμα παρουσιάζεται στην εικόνα 2.3.
Τα 32 bit της διεύθυνσης περιλαμβάνουν τέσσερις οχτάδες, κάθε μια από τις οποίες μπορεί να αντιπροσωπευθεί με έναν δεκαδικό αριθμό μεταξύ 0 και 255, με τελείες μεταξύ των δεκαδικών αντιπροσωπεύσεων. Στην εικόνα, η διεύθυνση 32-bit καταγράφεται σε μια δεκαδική αντιπροσώπευση.
Μια σημαντική διαφορά που πρέπει να προσέχουμε κατά την εργασία με διευθύνσεις IP είναι ότι το δεκαδικό είναι ένας εύκολος τρόπος για τους ανθρώπους να διαβάσουν και να γράψουν τις διευθύνσεις IP. Πάντα να θυμόσαστε ότι ο δρομολογητής δεν διαβάζει μια διεύθυνση από την άποψη τεσσάρων οχτάδων, αλλά, ο δρομολογητής βλέπει μια δυαδική σειρά 32 bit. Πολλές παγίδες μπορούν να αποφευχθούν εάν έχουμε αυτό το γεγονός σταθερά υπόψη.

Εικόνα 2.3
Το δεκαδικό σχήμα είναι ένας κατάλληλος τρόπος να γραφτούν οι διευθύνσεις IP, αλλά δεν πρέπει να συγχεθεί με αυτά που ο δρομολογητής (ή οικοδεσπότης) βλέπει —μια 32-bit σειρά.



Πιθανώς το πιο διακριτικό χαρακτηριστικό των διευθύνσεων IP είναι ότι αντίθετα με άλλες διευθύνσεις στο επίπεδο δικτύου, τα τμήματα δίκτυο και

οικοδεσπότης μπορούν να ποικίλουν στο μέγεθος μέσα στα 32 bit όρια. Δηλαδή το τμήμα δικτύου μπορεί να λάβει τα περισσότερα από τα 32 bit ή το τμήμα του οικοδεσπότη ή να διαιρέσουν τα κομμάτια εξίσου. Τα πρωτόκολλα, όπως NetWare και AppleTalk, σχεδιάστηκαν για τη χρήση στα σχετικά μικρά internetworks, και κατά συνέπεια οι διευθύνσεις τους στο επίπεδο δικτύου έχουν του καθορισμένου μήκους τμήματα δικτύων και οικοδεσποτών. Αυτή η ρύθμιση καθιστά βεβαίως τη ζωή ευκολότερη, μια λαμβάνουσα συσκευή ξέρει να διαβάζει ορισμένα bits στη διεύθυνση, για να βρει το μέρος δικτύων, και το υπόλοιπο είναι διεύθυνση οικοδεσποτών.
Το TCP/IP, εντούτοις, σχεδιάστηκε από την αρχή για να είναι αρκετά εύκαμπτο να χρησιμοποιηθεί σε οποιοδήποτε internetwork, από το πιο μικρό έως το πιο μεγάλο. Αυτή η ευελιξία καθιστά τις διευθύνσεις IP δυσκολότερες στη διαχείριση.

Ο κανόνας της πρώτης οχτάδας

Μπορεί να ειπωθεί ότι υπάρχουν τρία μεγέθη των internetworks όπως μετριούνται από τον αριθμό οικοδεσποτών: μεγάλος, μέσος, και μικρός.

- Τα μεγάλα internetworks, εξ ορισμού, έχουν έναν τεράστιο αριθμό οικοδεσποτών. Σχετικά, λίγα μεγάλα internetworks υπάρχουν.
- Τα μικρά internetworks είναι ακριβώς το αντίθετο. Το καθένα είναι μικρό επειδή έχει έναν μικρό αριθμό οικοδεσποτών. Ένας τεράστιος αριθμός μικρών internetworks υπάρχει.
- Τα μεσαία internetworks είναι ακριβώς αυτό: ένας μέσος αριθμός τους (σε σχέση με τα μεγάλα και τα μικρά) και ένας μέσος αριθμός οικοδεσποτών σε καθένας από αυτά.

Αυτό το υψηλό επίπεδο απαιτεί τρεις τύπους –κατηγορίες- διεύθυνσης δικτύων για τα τρία μεγέθη των internetworks. Οι διευθύνσεις για τα μεγάλα internetworks πρέπει να είναι ικανές να απευθυνθούν σε πολλούς οικοδεσπότες, αλλά επειδή είναι λίγα τα μεγάλα internetworks, μόνο μερικές μεγάλων δικτύων οι διευθύνσεις απαιτούνται.

Η κατάσταση αντιστρέφεται για τα μικρά internetworks. Επειδή υπάρχουν πολλά μικρά internetworks, ένας μεγάλος αριθμός διευθύνσεων μικρών-δικτύων απαιτείται. Αλλά επειδή ένα μικρό internetwork έχει έναν μικρό αριθμό οικοδεσποτών, κάθε μια από τις πολλές διευθύνσεις δικτύων απαιτεί μόνο μερικές διευθύνσεις οικοδεσποτών.
Για τα μέσου μεγέθους internetworks, ένας μέσος αριθμός διευθύνσεων δικτύων και ένας μέσος αριθμός διευθύνσεων οικοδεσποτών θα είναι διαθέσιμος για κάθε διεύθυνση δικτύων.
Το σχήμα 2.4 επιδεικνύει πώς τα τμήματα δικτύων και οικοδεσποτών των διευθύνσεων IP είναι επάνω για αυτές τις τρεις κατηγορίες.

Εικόνα 2.4
Διαμόρφωση των διευθύνσεων IP στις κατηγορίες A, B και C.

Class A:	N	H	H	H
Class B:	N	N	H	H
Class C:	N	N	N	H

Τα μεγάλα, μεσαία και μικρά δίκτυα περιέγραψαν ως εδώ το χάρτη για να απευθυνθούν στις κατηγορίες ως εξής:

- Οι διευθύνσεις IP κατηγορίας A είναι για τα μεγάλα internetworks. Το πρώτη οχτάδα είναι το κομμάτι του δικτύου, και οι τελευταίες τρεις οχτάδες είναι το κομμάτι οικοδεσποτών. Μόνο 256 αριθμοί είναι διαθέσιμοι στο 8-bit μέρος δικτύων, αλλά 224 ή 16.777.216 αριθμοί είναι διαθέσιμοι στο μέρος οικοδεσποτών για κάθε μια από εκείνες τις διευθύνσεις δικτύων.
- Οι διευθύνσεις κατηγορίας B είναι για τα μεσαίου μεγέθους internetworks. Οι πρώτες δύο οχτάδες είναι το κομμάτι του δικτύου και οι τελευταίες δύο οχτάδες είναι το κομμάτι οικοδεσποτών. Υπάρχουν 216 ή 65.536 διαθέσιμοι αριθμοί στο μέρος του δικτύου και ένας ίσος αριθμός στο μέρος οικοδεσποτών.

- Οι διευθύνσεις κατηγορίας C είναι ακριβώς το αντίθετο της κατηγορίας A. Οι πρώτες τρεις οχτάδες είναι το κομμάτι του δικτύου και η τελευταία οχτάδα είναι το κομμάτι οικοδεσποτών.

Επειδή όλες οι διευθύνσεις IP είναι 32-bit δυαδικές σειρές, ένας τρόπος για να ξεχωρίζει την κατηγορία στην οποία μια ιδιαίτερη διεύθυνση ανήκει, είναι απαραίτητος. Ο κανόνας της πρώτης οχτάδας, που διευκρινίζεται στο σχήμα 2.5, παρέχει τα μέσα να γίνει μια τέτοια διάκριση και μπορεί να περιγραφεί ως εξής:

- Για τις διευθύνσεις κατηγορίας A, το πρώτο bit της πρώτης οχτάδας — δηλαδή το πιο αριστερό bit ολόκληρης της 32-bit σειράς —θέτεται πάντα μηδέν. Επομένως, μπορούμε να βρούμε τους ελάχιστους και μέγιστους αριθμούς στην κατηγορία A με τη ρύθμιση όλων των υπόλοιπων bit στην πρώτη οχτάδα σε μηδέν (για το ελάχιστο) και το ένα (για το μέγιστο). Αυτή η δράση οδηγεί στους δεκαδικούς αριθμούς 0 και 127 με μερικές εξαιρέσεις: 0 είναι δεσμευμένο ως τμήμα της διεύθυνσης προεπιλογής και 127 είναι δεσμευμένο για τις εσωτερικές διευθύνσεις loopback. Αυτό αφήνει 1 μέχρι 126, οποιαδήποτε διεύθυνση IP της οποίας τη πρώτη οχτάδα είναι μεταξύ 1 και 126, είναι μια διεύθυνση κατηγορίας A.

- Οι διευθύνσεις κατηγορίας B πάντα θέτουν το πιο αριστερό bit τους ένα και το δεύτερο bit καθορισμένο μηδέν. Πάλι βρίσκοντας τον ελάχιστο και μέγιστο αριθμό της πρώτης οχτάδας με τη ρύθμιση όλων των υπόλοιπων bits σε μηδέν και έπειτα σε ένα. Βλέπουμε στο σχήμα 2.5 ότι οποιαδήποτε διεύθυνση της οποίας η πρώτη οχτάδα είναι στη δεκαδική σειρά 128 μέχρι 191 είναι μια διεύθυνση κατηγορίας B.

- Στις διευθύνσεις κατηγορίας C, στα πρώτα δύο bit τίθενται το ένα και στο τρίτο bit τίθεται μηδέν. Το αποτέλεσμα είναι μια πρώτη οχτάδα από 192 μέχρι 223.

ΚΑΝΟΝΑΣ	ΕΛΑΧΙΣΤΑ ΚΑΙ ΜΕΓΙΣΤΑ	ΔΕΚΑΔΙΚΟ ΕΥΡΟΣ
Class A: Το πρώτο bit πάντα 0.	00000000 = 0 01111111 =127	1 -126* *0 and 127 are reserved
Class B: Τα δυο πρώτα bits πάντα 10.	10000000 = 128 10111111 -191	128- 191
Class C: Τα τρία πρώτα bits πάντα 110.	11000000 = 192 11011111 =223	192-223

Σχήμα 2.5
Ο κανόνας πρώτης οχτάδας.

Μέχρι τώρα η εξέταση IP δεν φαίνεται τόσο δύσκολη. Ένας δρομολογητής ή ένας οικοδεσπότης θα μπορούσε εύκολα να καθορίσει το μέρος του δικτύου μιας διεύθυνσης IP με τη χρησιμοποίηση του κανόνα της πρώτης οχτάδας. Εάν το πρώτο bit είναι 0, κατόπιν διαβάστε τα πρώτα οκτώ bits για να βρείτε τη διεύθυνση δικτύου. Εάν τα πρώτα δύο bits είναι 10, κατόπιν διαβάστε τα πρώτα 16 bits, και εάν τα πρώτα τρία bits είναι 110, κατόπιν διαβάστε 24 bits για να πάρετε τη διεύθυνση δικτύου. Δυστυχώς, τα πράγματα δεν είναι τόσο εύκολα.

Μάσκες διευθύνσεων

Η διεύθυνση για μια ολόκληρη σύνδεση δεδομένων —μια μη συγκεκριμένου οικοδεσπότη διεύθυνση δικτύων—αντιπροσωπεύεται από το τμήμα δικτύου μιας διεύθυνσης IP, με όλα τα bits οικοδεσποτών καθορισμένα σε μηδέν. Παραδείγματος χάριν, το InterNIC, το σώμα που διαχειρίζεται τις διευθύνσεις IP, μπορεί να ορίσει σε έναν υποψήφιο μια διεύθυνση 172.21.0.0.
Αυτή η διεύθυνση είναι μια διεύθυνση κατηγορίας Β επειδή το 172 είναι μεταξύ 128 και 191, έτσι οι τελευταίες δύο οχτάδες αποτελούν τα bits οικοδεσποτών. Παρατηρούμε ότι είναι όλοι μηδέν. Τα πρώτα 16 bits : (172.21.) ορίζονται,

αλλά οι ιδιοκτήτες διευθύνσεων είναι ελεύθεροι να κάνουν οτιδήποτε θέλουν με τα κομμάτια οικοδεσποτών.
Σε κάθε συσκευή ή διεπαφή θα οριστεί μια μοναδική, συγκεκριμένη οικοδεσπότης διεύθυνση όπως 172.21.35.17. Η συσκευή, είτε ένας οικοδεσπότης είτε ένας δρομολογητής, πρέπει προφανώς να ξέρει τη διεύθυνσή της, αλλά πρέπει επίσης να είναι σε θέση να καθορίσει το δίκτυο στο οποίο ανήκει— σε αυτήν την περίπτωση, 172.21.0.0.
Αυτός ο στόχος ολοκληρώνεται με τη βοήθεια μιας μάσκας διευθύνσεων. Η μάσκα διευθύνσεων είναι μια 32-bit σειρά, ένα bit για κάθε bit της διεύθυνσης IP. Σαν 32-bit σειρά, η μάσκα μπορεί να αντιπροσωπευθεί με το δεκαδικό σχήμα ακριβώς όπως μια διεύθυνση IP. Αυτή η αντιπροσώπευση τείνει να είναι ένας φραγμός για μερικούς αρχάριους. Αν και η μάσκα διευθύνσεων μπορεί να γραφτεί στο δεκαδικό, δεν είναι μια διεύθυνση. Ο πίνακας 2.3 παρουσιάζει τυποποιημένες μάσκες διευθύνσεων για τις τρεις κατηγορίες διεύθυνσης IP.

Πίνακας 2.3 Μάσκες διευθύνσεων για τις κατηγορίες A, B και C διευθύνσεων δικτύων.

Κατηγορία	**Μάσκα**	**Δεκαδικό**
A	11111111000000000000000000000000	255.0.0.0
B	11111111111111110000000000000000	255.255.0.0
C	11111111111111111111111100000000	255.255.255.0

Για κάθε bit της διεύθυνσης IP, η συσκευή εκτελεί μια Boolean (λογική) AND λειτουργία με το αντίστοιχο bit της μάσκας διευθύνσεων. Η λειτουργία AND μπορεί να δηλωθεί ως εξής:

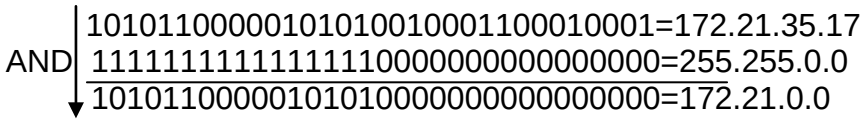
Συγκρίνετε δύο bits και παράγετε ένα αποτέλεσμα. Το αποτέλεσμα θα είναι ένα εάν και μόνο εάν και τα δύο bits είναι ένα. Εάν καθένα ή και τα δύο bits είναι μηδέν, το αποτέλεσμα θα είναι μηδέν.

Το σχήμα 2.6 επιδεικνύει πώς, για μια δεδομένη διεύθυνση IP, η μάσκα διευθύνσεων χρησιμοποιείται για να καθορίσει τη διεύθυνση δικτύων. Η μάσκα έχει ένα, ένα σε κάθε θέση bit που αντιστοιχεί σε ένα bit δικτύων της διεύθυνσης και ένα μηδέν σε κάθε θέση bit που αντιστοιχεί σε ένα bit

οικοδεσποτών. Επειδή 172.21.35.17 είναι μια διεύθυνση κατηγορίας B, η μάσκα πρέπει να θέσει τις πρώτες δύο οχτάδες όλα σε ένα και τις τελευταίες δύο οχτάδες, το μέρος οικοδεσποτών, όλα σε μηδενικά. Όπως ο πίνακας 2.3 παρουσιάζει, αυτή η μάσκα μπορεί να αντιπροσωπευθεί στο δεκαδικό ως 255.255.0.0.

Σχήμα 2.6

0 AND 0 = 0
0 AND 1 = 0
1 AND 0 = 0
1 AND 1 = 1



Ένα λογικό AND εκτελείται στη διεύθυνση IP και τη μάσκα του για κάθε θέση bit, το αποτέλεσμα παρουσιάζεται στο σχήμα 2.6. Στο αποτέλεσμα, κάθε bit δικτύου επαναλαμβάνεται και όλα τα bits οικοδεσποτών γίνονται μηδενικά. Έτσι με την ανάθεση μιας διεύθυνσης 172.21.35.17 και μιας μάσκας 255.255.0.0 σε μια διεπαφή, η συσκευή ξέρει ότι η διεπαφή ανήκει στο δίκτυο 172.21.0.0. Θέτοντας AND σε μια διεύθυνση IP και τη μάσκα διευθύνσεών του, αποκαλύπτουν πάντα τη διεύθυνση δικτύων.

Υποδίκτυα και υποδίκτυα μάσκας

Για να ολοκληρωθεί η δρομολόγηση, κάθε σύνδεση δεδομένων (δίκτυο) πρέπει να έχει μια μοναδική διεύθυνση. Επιπλέον, κάθε οικοδεσπότης σε εκείνη την σύνδεση δεδομένων πρέπει να έχει μια διεύθυνση που να το προσδιορίζει ως μέλος του δικτύου και το διακρίνει από οποιοδήποτε άλλο οικοδεσπότη σε εκείνο το δίκτυο.
Όπως καθορίζεται μέχρι τώρα, μια ενιαία διεύθυνση κατηγορίας A, B, ή C μπορεί να χρησιμοποιηθεί μόνο σε μια ενιαία σύνδεση δεδομένων. Για να σχεδιάσουν ένα internetwork, χωριστές διευθύνσεις πρέπει να χρησιμοποιηθούν για κάθε σύνδεση δεδομένων έτσι ώστε εκείνα τα δίκτυα είναι μοναδικά ευπροσδιόριστα. Εάν μια χωριστή διεύθυνση κατηγορίας A, B,

ή C ορίστηκε σε κάθε σύνδεση δεδομένων, λιγότερο από 17 εκατομμύρια συνδέσεις δεδομένων θα μπορούσαν να εξεταστούν προτού να εξαντληθούν όλες οι διευθύνσεις IP.Αυτή η προσέγγιση είναι προφανώς μη πρακτική, όπως είναι το γεγονός ότι για να αξιοποιήσουν πλήρως το διάστημα διευθύνσεων οικοδεσποτών στο προηγούμενο παράδειγμα, περισσότερες από 65.000 συσκευές θα έπρεπε να τοποθετηθούν στη σύνδεση δεδομένων 172.21.0.0!

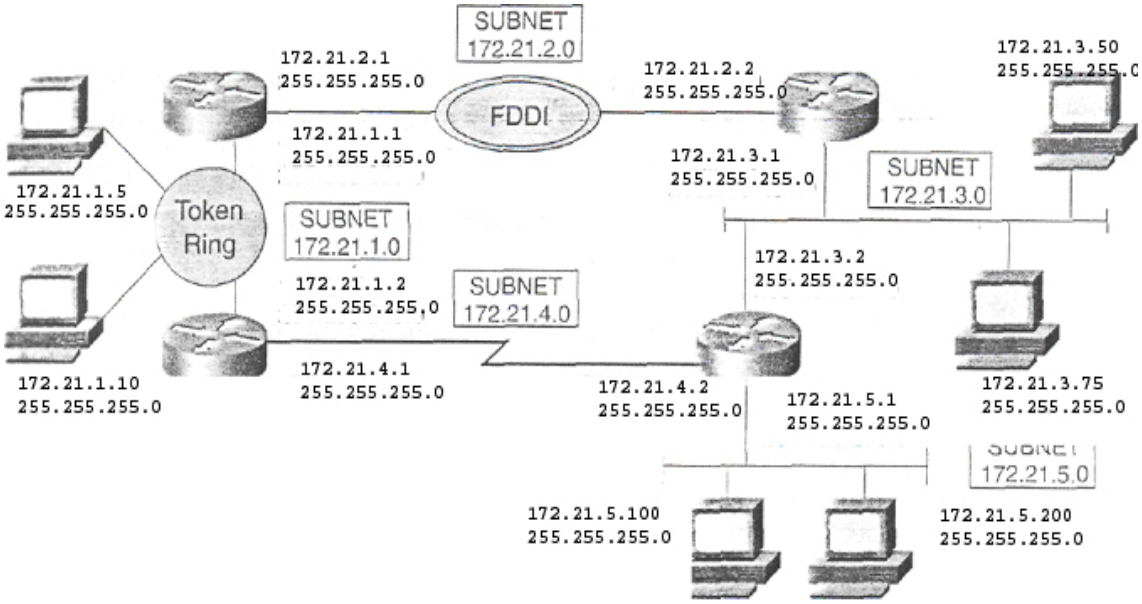
Ο μόνος τρόπος να γίνουν οι διευθύνσεις κατηγορίας A, B, C πρακτικές είναι με τη διαίρεση κάθε σημαντικής διεύθυνσης, όπως 172.21.0.0, σε διευθύνσεις υποδικτύων. Θυμηθείτε δυο πράγματα:

- Το τμήμα οικοδεσποτών μιας διεύθυνσης μπορεί να χρησιμοποιηθεί όπως επιθυμείτε.
- Το τμήμα δικτύου μιας διεύθυνσης IP καθορίζεται από τη μάσκα διευθύνσεων που ορίζεται σε εκείνη την διεπαφή.

Το σχήμα 2.7 παρουσιάζει ένα internetwork στο οποίο η σημαντικότερη διεύθυνση 172.21.0.0 κατηγορίας B έχει οριστεί. Πέντε συνδέσεις δεδομένων διασυνδέουν τους δρομολογητές, καθένας των οποίων απαιτεί μια διεύθυνση δικτύου. Υπό τις παρούσες συνθήκες, 172.21.0.0 θα έπρεπε να οριστεί σε μια ενιαία σύνδεση δεδομένων και έπειτα τέσσερις περισσότερες διευθύνσεις θα έπρεπε να ζητηθούν για τις άλλες τέσσερις συνδέσεις δεδομένων. Παρατηρήστε τι έγινε στο σχήμα 2.7. Η μάσκα διευθύνσεων δεν είναι μια τυποποιημένη δεκαεξάμπιτη μάσκα για τις διευθύνσεις κατηγορίας B, η μάσκα έχει επεκταθεί άλλα οκτώ bits έτσι ώστε τα πρώτα 24 bits της IP ερμηνεύονται ως bits δικτύου. Με άλλα λόγια, στους δρομολογητές και στους οικοδεσπότες έχει δοθεί μια μάσκα που τους αναγκάζει να διαβάσουν τα πρώτα οκτώ bits οικοδεσποτών ως τμήμα της διεύθυνσης δικτύου. Το αποτέλεσμα είναι ότι η σημαντικότερη διεύθυνση δικτύου ισχύει για το ολόκληρο internetwork, και κάθε σύνδεση δεδομένων έχει γίνει ένα υποδίκτυο. Ένα υποδίκτυο είναι ένα υποσύνολο ενός σημαντικού διαστήματος διευθύνσεων κατηγορίας A, B, C. Η διεύθυνση IP έχει τώρα τρία μέρη: το μέρος δικτύου, το μέρος υποδικτύου και το μέρος οικοδεσποτών. Η μάσκα διευθύνσεων είναι τώρα μια μάσκα

υποδικτύου, ή μια μάσκα που είναι πιο μεγάλη από την τυποποιημένη μάσκα διευθύνσεων.

ΔΙΚΤΥΟ : 172.21.0.0
ΜΑΣΚΑ ΥΠΟΔΙΚΤΥΟΥ : 255.255.255.0



Σχήμα 2.7
Οι μάσκες υποδικτύου επιτρέπουν μια διεύθυνση του δικτύου να χρησιμοποιείται σε μια πολλαπλή σύνδεση δεδομένων, δανειζόμενη μερικά bits του οικοδεσπότη για να τα χρησιμοποιήσει ως bits υποδικτύου.

Οι δυο πρώτες οχτάδες της διεύθυνσης θα είναι πάντα 172.21, αλλά η τρίτη οχτάδα — τα της οποίας bits είναι τώρα bits υποδικτύου αντί των bits οικοδεσποτών — μπορεί να κυμανθεί από 0 έως 255. Το internetwork στο σχήμα 2.6 έχει τα υποδίκτυα 1 ..2 ..3 ..4, και 5 (172.21.1.0 μέχρι 172.21.5.0). Μέχρι 256 υποδίκτυα μπορούν να οριστούν κάτω από την ενιαία διεύθυνση κατηγορίας B, χρησιμοποιώντας τη μάσκα που παρουσιάζεται.
Δυο λεπτομέρειες που πρέπει να προσεχθούν.
Κατ' αρχάς, δεν υποστηρίζουν όλα τα πρωτόκολλα δρομολόγησης τις διευθύνσεις υποδικτύου στις οποίες τα bits υποδικτύου είναι όλα μηδενικά ή όλα ένα. Ο λόγος είναι ότι αυτά τα πρωτόκολλα, αποκαλούμενα classful πρωτόκολλα, δεν μπορούν να διαφοροποιηθούν μεταξύ ενός όλου-μηδενικά υποδικτύου και του κύριου αριθμού του δικτύου. Επιπλέον, τα classful πρωτόκολλα δρομολόγησης δεν μπορούν να διαφοροποιήσουν μια

διεύθυνση broadcast στο υποδίκτυο όλα-ένα από μια διεύθυνση broadcast όλα-υποδίκτυα.

Κατά δεύτερον έχουμε να κάνουμε με τη λεκτική περιγραφή των υποδικτύων και των μασκών τους. Διασπάζοντας την τρίτη οχτάδα της διεύθυνσης κατηγορίας Β, όπως γίνεται στο σχήμα 2.7, είναι πολύ κοινό, επίσης κοινό ακούγεται ότι οι άνθρωποι περιγράφουν ένα τέτοιο σχέδιο υποδικτύου ως "χρησιμοποίηση μιας μάσκας κατηγορίας C με μια διεύθυνση κατηγορίας Β, " ή " μια διεύθυνση κατηγορίας Β σε μια κατηγορία C. " Και οι δύο περιγραφές κάνουν λάθος! Τέτοιες περιγραφές οδηγούν συχνά σε παρανοήσεις για το σχέδιο υποδικτύου ή σε μια φτωχή κατανόηση. Ο κατάλληλος τρόπος να περιγραφεί το σχέδιο διάσπασης του σχήματος 2.6 είναι είτε ως "διεύθυνση κατηγορίας Β με 8 bits," είτε ως "διεύθυνση κατηγορίας Β με μια μάσκα 24-bits."

Η μάσκα υποδικτύου μπορεί να αντιπροσωπευθεί σε οποιαδήποτε από τα τρία σχήματα —δεκαδικό, δυαδικό και δεκαεξαδικό — όπως φαίνεται στο σχήμα 2.8. το δεκαδικό είναι ακόμα το πιο κοινό σχήμα, αν και το σχήμα του δυαδικού γίνεται όλο και περισσότερο δημοφιλές. Έναντι του δεκαδικού, το δυαδικό είναι ευκολότερο να γραφεί (η διεύθυνση ακολουθείται από μια μπροστινή κάθετο και τον αριθμό bits που είναι καλυμμένα για το μέρος δικτύων).

Επιπλέον, το δυαδικό είναι περιγραφικότερο αυτών που η μάσκα κάνει πραγματικά και επομένως αποφεύγει τον τύπο σημασιολογικών παρανοήσεων που περιγράφονται στην προηγούμενη παράγραφο. Πολλά συστήματα Unix χρησιμοποιούν το δεκαεξαδικό σχήμα.

ΔΕΚΑΔΙΚΟ

255.255.255.0

ΔΥΑΔΙΚΟ

172.21.0.0/24

ΔΕΚΑΕΞΑΔΙΚΟ

0xFFFFFF00

Σχήμα 2.8
Η μάσκα υποδικτύου στο σχήμα 2.7 μπορεί να αντιπροσωπευθεί με τρία διαφορετικά σχήματα.

Σχεδιασμός των υποδικτύων

Όπως καθιερώνεται στο προηγούμενο τμήμα, τα bits υποδικτύου δεν μπορούν να είναι όλα μηδενικά ή όλα ένα στα classful περιβάλλοντα. Επιπλέον, μια διεύθυνση οικοδεσποτών IP δεν μπορεί να θέσει όλα τα bits οικοδεσποτών της σε μηδέν — αυτή η ρύθμιση είναι διατηρημένη για το δρομολογητή διευθύνσεων για να αντιπροσωπεύσει το δίκτυο ή τον ίδιο. Και τα bits οικοδεσποτών δεν μπορούν να τεθούν όλα σε ένα, δεδομένου ότι αυτή η ρύθμιση είναι η διεύθυνση broadcast. Αυτοί οι περιορισμοί ισχύουν για τα bits οικοδεσποτών χωρίς τις εξαιρέσεις και είναι αφετηρίες για το σχεδιασμό των υποδικτύων. Πέρα από αυτές τις αφετηρίες, οι σχεδιαστές δικτύων πρέπει να επιλέξουν το πιο κατάλληλο σχέδιο διάσπασης από την άποψη του ταιριάσματος του διαστήματος διευθύνσεων στις λεπτομέρειες ενός internetwork.

Κατά σχεδιασμό των υποδικτύων και των μασκών τους, τον αριθμό διαθέσιμων υποδικτύων κάτω από μια σημαντική διεύθυνση δικτύου και ο αριθμός διαθέσιμων οικοδεσποτών σε κάθε υποδίκτυο και οι δύο υπολογίζονται με τον ίδιο τύπο: $2^n - 2$, όπου το n είναι ο αριθμός bits στο υποδίκτυο ή το διάστημα οικοδεσποτών και 2 αφαιρούνται για να αποτελέσουν τις μη διαθέσιμες όλα - μηδενικά και όλα -ένα διευθύνσεις. Παραδείγματος χάριν, λαμβάνοντας υπόψη μια διεύθυνση κατηγορίας A 10.0.0.0, μια μάσκα υποδικτύου 10.0.0.0/16 (255.255.0.0) σημαίνει ότι το οκτάμπιτο διάστημα υποδικτύου θα παραγάγει $2^8 - 2 = 254$ διαθέσιμα υποδίκτυα και $2^{16} - 2 = 65.534$ διευθύνσεις οικοδεσποτών διαθέσιμες σε κάθε ένα από εκείνα τα υποδίκτυα. Αφ' ετέρου, μια μάσκα 10.0.0.0 / 24 (255.255.255.0) σημαίνει ότι ένα δεκαεξάμπιτο διάστημα υποδικτύου παράγει 65.534 υποδίκτυα και ένα οκτάμπιτο διάστημα οικοδεσποτών παράγει 254 διευθύνσεις οικοδεσποτών για κάθε υποδίκτυο.

Τα ακόλουθα βήματα χρησιμοποιούνται για τη διάσπαση μιας διεύθυνσης IP:

- Καθορίστε πόσα υποδίκτυα απαιτούνται και πόσοι οικοδεσπότες ανά υποδίκτυο απαιτούνται.

- Χρησιμοποιήστε τον τύπο 2^n -2 για να καθορίσετε τον αριθμό bits του υποδικτύου και τον αριθμό bits οικοδεσποτών που θα ικανοποιήσουν τις απαιτήσεις που καθιερώνονται στο βήμα 1. Εάν οι πολλαπλάσιες μάσκες υποδικτύου μπορούν να ικανοποιήσουν τις απαιτήσεις, επιλέξτε αυτή που θα ταιριάζει καλύτερα στις μελλοντικές ανάγκες. Παραδείγματος χάριν, εάν το internetwork είναι πιο πιθανό να αυξηθεί με την προσθήκη των υποδικτύων, επιλέξτε περισσότερα bits υποδικτύου, εάν το internetwork είναι πιο πιθανό να αυξηθεί με την προσθήκη των οικοδεσποτών στα υπάρχοντα υποδίκτυα, επιλέξτε περισσότερα bits οικοδεσποτών. Αποφύγετε ένα σχέδιο στο οποίο είτε όλα τα υποδίκτυα είτε οι διευθύνσεις οικοδεσποτών μέσα στα υποδίκτυα θα καταναλωθούν αμέσως, μην αφήνοντας κάποιο περιθώριο για μελλοντική αύξηση.

- Εργαζόμενοι στο δυαδικό, καθορίστε όλους τους διαθέσιμους συνδυασμούς bits στο διάστημα υποδικτύου, σε κάθε περίπτωση, θέστε όλα τα bits οικοδεσποτών σε μηδέν. Μετατρέψτε τις προκύπτουσες διευθύνσεις υποδικτύου στο δεκαδικό. Αυτές είναι οι διευθύνσεις υποδικτύου.

- Για κάθε διεύθυνση υποδικτύου, πάλι που λειτουργεί στο δυαδικό, γράψτε όλους τους πιθανούς συνδυασμούς bits για το διάστημα οικοδεσποτών χωρίς αλλαγή των bits υποδικτύου. Μετατρέψτε τα αποτελέσματα στο δεκαδικό. Αυτές είναι οι διευθύνσεις οικοδεσποτών διαθέσιμες για κάθε υποδίκτυο.

Σπάσιμο του ορίου οχτάδας

Στα παραδείγματα που δίνονται μέχρι τώρα, τα διαστήματα υποδικτύου έχουν πέσει στα όρια της οχτάδας. Αυτή η ρύθμιση είναι όχι πάντα η πρακτικότερη ή αποδοτική επιλογή. Τι εάν, παραδείγματος χάριν, χρειάζεστε υποδίκτυο για μια διεύθυνση κατηγορίας Β σε 500 συνδέσεις δεδομένων, κάθε μια με ένα μέγιστο 100 οικοδεσποτών; Αυτή η απαίτηση καλύπτεται εύκολα, αλλά μόνο με τη χρησιμοποίηση εννέα bits στον τομέα υποδικτύου: 2^9- 2 = 510 διαθέσιμα υποδίκτυα, αφήνοντας επτά bits για τον τομέα οικοδεσποτών, και

2^7-2 = 126 διαθέσιμοι οικοδεσπότες ανά υποδίκτυο. Κανένας άλλος συνδυασμός bits δεν θα ικανοποιήσει αυτήν την απαίτηση.

Διάσπαση μιας μάσκα υποδικτύου

Η ανάγκη προκύπτει συχνά για "να τεμαχίσει" μια δεδομένη διεύθυνση και μια μάσκα οικοδεσποτών, για να προσδιορίσει συνήθως το υποδίκτυο στο οποίο ανήκει. Παραδείγματος χάριν, εάν μια διεύθυνση πρόκειται να διαμορφωθεί σε μια διεπαφή, μια ορθή πρακτική είναι αρχικά να ελέγξει ότι η διεύθυνση ισχύει για το υποδίκτυο με το οποίο το υποδίκτυο συνδέεται.
Χρησιμοποιήστε τον ακόλουθο αντίστροφο-μηχανισμό βημάτων σε μια διεύθυνση IP:

1. Γράψτε τη δεδομένη μάσκα υποδικτύου στο δυαδικό.
2. Γράψτε τη διεύθυνση οικοδεσποτών IP στο δυαδικό.
3. Γνωρίζοντας τη κατηγορία της διεύθυνσης οικοδεσποτών, τα bits υποδικτύου της μάσκας πρέπει να είναι προφανή. Χρησιμοποιώντας τα bits μασκών ως οδηγό, σχεδιάστε μια γραμμή μεταξύ του τελευταίου bit δικτύου και του πρώτου bit υποδικτύου της διεύθυνσης. Σχεδιάστε μια άλλη γραμμή μεταξύ του τελευταίου bit υποδικτύου και του πρώτου bit δικτύου.
4. Γράψτε τα bits δικτύου και υποδικτύου της διεύθυνσης, ρυθμίστε όλα τα bits οικοδεσποτών σε μηδέν. Το αποτέλεσμα είναι η διεύθυνση του υποδικτύου
   στο οποίο η διεύθυνση οικοδεσποτών ανήκει.
5. Πάλι γράψτε τα bits δικτύου και υποδικτύου της διεύθυνσης, αυτή τη φορά θέτοντας όλα τα bits οικοδεσποτών σε ένα. Το αποτέλεσμα είναι η διεύθυνση broadcast του υποδικτύου .
6. Ξέροντας ότι η διεύθυνση υποδικτύου είναι η πρώτη διεύθυνση στην ακολουθία και ότι η διεύθυνση broadcast είναι η τελευταία διεύθυνση στην ακολουθία, επίσης ξέρετε ότι όλες οι διευθύνσεις μεταξύ αυτών των δύο είναι έγκυρες διευθύνσεις οικοδεσποτών.

Το σχήμα 2.9 παρουσιάζει αυτά τα βήματα που εφαρμόζονται σε 172.30.0.141/25. Η διεύθυνση είναι κατηγορίας B, έτσι είναι γνωστό ότι τα

πρώτα 16 bits είναι τα bits του δικτύου, επομένως, τα τελευταία εννέα bits της μάσκας των 25-bits χαρακτηρίζει το διάστημα υποδικτύου. Η διεύθυνση υποδικτύου είναι 172.30.0.128, και η διεύθυνση broadcast είναι 172.30.0.255. Ξέροντας ότι οι έγκυρες διευθύνσεις οικοδεσποτών για το υποδίκτυο είναι οριακές από αυτές τις δύο διευθύνσεις, καθορίζεται ότι οι διευθύνσεις οικοδεσποτών για το υποδίκτυο 172.30.0.128 είναι 172.30.0.129 μέχρι 172.30.0.254.

Διάφορα πράγματα, για αυτό το παράδειγμα, τείνουν να ενοχλήσουν τα άτομα που είναι νέοι στη διάσπαση. Μερικοί ενοχλούνται από την τρίτη οχτάδα της διεύθυνσης, όπου είναι όλα μηδενικά. Μερικοί ενοχλούνται από το μοναδικό bit υποδικτύου στην τελευταία οχτάδα. Μερικοί σκέφτονται ότι η διεύθυνση broadcast φαίνεται ύποπτα άκυρη. Όλα αυτά τα δύσκολα συναισθήματα προκύπτουν από την ανάγνωση των διευθύνσεων στο δεκαδικό. Όταν οι διευθύνσεις και η μάσκα φαίνονται στο δυαδικό, αυτές οι υποψίες μετριάζονται και όλα φαίνονται να είναι νόμιμα, η μάσκα θέτει ένα εννέα-bits υποδίκτυο—όλα από την τρίτη οχτάδα, και το πρώτο bit από την τέταρτη οχτάδα. Το δίδαγμα της ιστορίας είναι ότι εάν όλα είναι γνωστά για να είναι σωστά στο δυαδικό, μην ανησυχήστε εάν στο δεκαδικό η αντιπροσώπευση φαίνεται αστεία.

172.30.0.141/25

(1) Γράψε μάσκα υποδικτύου :	11111111111111111111111110000000 = 255.255.255.128
(2) Γράψε διεύθυνση IP :	10101100000111100000000010001101 = 172.30.0.141

(3) Μάρκαρε το διάστημα	11111111111111111111111110000000 = 255.255.255.128
του υποδικτύου	10101100000111100000000010001101 = 172.30.0.141

Διαχώρισε τα	11111111111111111111111110000000 = 255.255.255.128
	10101100000111100000000010001101 = 172.30.0.141
(4) διεύθυνση υποδικτύου	10101100000111100000000010000000 = 172.30.0.128
(5) διεύθυνση broadcast	10101100000111100000000011111111 =172.30.0.255

(6) Οι έγκυρες διευθύνσεις οικοδεσποτών για αυτό το υποδίκτυο είναι 172.30.0.129 – 172.30.0.254

Σχήμα 2.9
Δοσμένης μιας διεύθυνσης IP και μιας μάσκας υποδικτύου, ακολουθήστε αυτά τα βήματα για να βρείτε το υποδίκτυο, το broadcast και την διεύθυνση οικοδεσποτών.

ARP

Ξέρουμε ότι οι δρομολογητές περνούν τα πακέτα μέσα από μια λογική πορεία, που αποτελείται από τις πολλαπλάσιες συνδέσεις δεδομένων, διαβάζοντας και τοποθετώντας τις διευθύνσεις δικτύων στα πακέτα. Τα πακέτα περνούν στις μεμονωμένες συνδέσεις δεδομένων με την τοποθέτηση των πακέτων στα πλαίσια, τα οποία χρησιμοποιούν προσδιοριστικά συνδέσεων δεδομένων (διευθύνσεις της MAC, παραδείγματος χάριν) για να φτάσουν το πλαίσιο από την πηγή στον προορισμό στη σύνδεση. Ένα από τα σημαντικότερα θέματα αυτής της εργασίας αφορά τους μηχανισμούς από τους οποίους οι δρομολογητές ανακαλύπτουν και μοιράζονται τις πληροφορίες για τις διευθύνσεις δικτύων έτσι ώστε η δρομολόγηση μπορεί να πραγματοποιηθεί. Ομοίως, οι συσκευές σε μια σύνδεση δεδομένων χρειάζονται έναν τρόπο να ανακαλύψουν τα προσδιοριστικά συνδέσεων δεδομένων των γειτόνων τους έτσι ώστε τα πλαίσια να μπορούν να διαβιβαστούν στο σωστό προορισμό. Διάφοροι μηχανισμοί μπορούν να παρέχουν αυτές τις πληροφορίες, η IP χρησιμοποιεί το Address Resolution Protocol (ARP), περιγεγραμμένο στο RFC 826. Μια συσκευή που πρέπει να ανακαλύψει το προσδιοριστικό συνδέσεων δεδομένων μιας άλλης συσκευής θα δημιουργήσει ένα arp πακέτο αιτήματος. Αυτό το αίτημα περιέχει τη διεύθυνση IP της συσκευής (ο στόχος) και το προσδιοριστικό της διεύθυνσης IP και των συνδέσεων δεδομένων (διεύθυνση της MAC) της συσκευής υποβάλλοντας το αίτημα (ο αποστολέας). Το arp πακέτο αιτήματος είναι έπειτα τοποθετημένο σε ένα πλαίσιο με τη διεύθυνση της MAC του αποστολέα ως πηγή και μια διεύθυνση broadcast για τον προορισμό. Η broadcast μετάδοση σημαίνει ότι όλες οι συσκευές στη σύνδεση δεδομένων θα λάβουν το πλαίσιο και θα εξετάσουν το τοποθετημένο πακέτο. Όλες οι συσκευές εκτός από το στόχο θα αναγνωρίσουν ότι το πακέτο δεν είναι για αυτούς και θα ρίξουν το πακέτο. Ο στόχος θα στείλει μια arp απάντηση στη διεύθυνση προέλευσης, που παρέχει τη διεύθυνση της MAC του.

Proxy ARP

Μερικές φορές αποκαλείται promiscuous arp και περιγράφεται σε RFCs 925 και 1027, proxy arp είναι μια μέθοδος με την οποία οι δρομολογητές μπορούν να κατασταθούν διαθέσιμοι στους οικοδεσπότες. Παραδείγματος χάριν, ένας οικοδεσπότης 192.168.12.5/24 πρέπει να στείλει ένα πακέτο σε 192.168.20.101/24, αλλά δεν διαμορφώνεται με τις πληροφορίες πυλών προεπιλογής και επομένως δεν ξέρει πώς να φθάσει σε έναν δρομολογητή. Μπορεί να εκδώσει ένα arp αίτημα για 192.168.20.101, ο τοπικός δρομολογητής, που λαμβάνει το αίτημα και που ξέρει πώς να φθάσει στο δίκτυο 192.168.20.0, θα εκδώσει μια arp απάντηση με το προσδιοριστικό συνδέσεων δεδομένων του στον τομέα διευθύνσεων υλικού. Στην πραγματικότητα, ο δρομολογητής έχει εξαπατήσει τον τοπικό οικοδεσπότη στη σκέψη ότι η διεπαφή του δρομολογητή είναι η διεπαφή 192.168.20.101. Όλα τα πακέτα που προορίζονται για εκείνη την διεύθυνση θα σταλούν στο δρομολογητή.

Άνευ λόγου ARP

Ένας οικοδεσπότης μπορεί περιστασιακά να εκδώσει ένα arp αίτημα με τη διεύθυνση IP του ως διεύθυνση στόχων. Αυτά τα arp αιτήματα, γνωστά ως gratuitous ARPs έχουν δύο χρήσεις:

- Άνευ λόγου arp μπορεί να χρησιμοποιηθεί για ελέγχους για διπλή διεύθυνση. Μια συσκευή που εκδίδει ένα arp αίτημα με τη δική της διεύθυνση IP ως στόχο και λαμβάνει μια arp απάντηση από μια άλλη συσκευή ξέρει ότι η διεύθυνση είναι ένα αντίγραφο.
- Άνευ λόγου arp μπορεί να χρησιμοποιηθεί για να διαφημίσει ένα νέο προσδιοριστικό σύνδεσης δεδομένων. Αυτή η χρήση εκμεταλλεύεται το γεγονός ότι όταν λαμβάνει μια συσκευή ένα arp αίτημα για μια διεύθυνση IP που είναι ήδη της arp cache, η cache θα ενημερωθεί με τη νέα διεύθυνση υλικού του αποστολέα.

Πολλές εφαρμογές IP δεν χρησιμοποιούν άνευ λόγου arp, αλλά πρέπει να γνωρίζετε την ύπαρξή του.

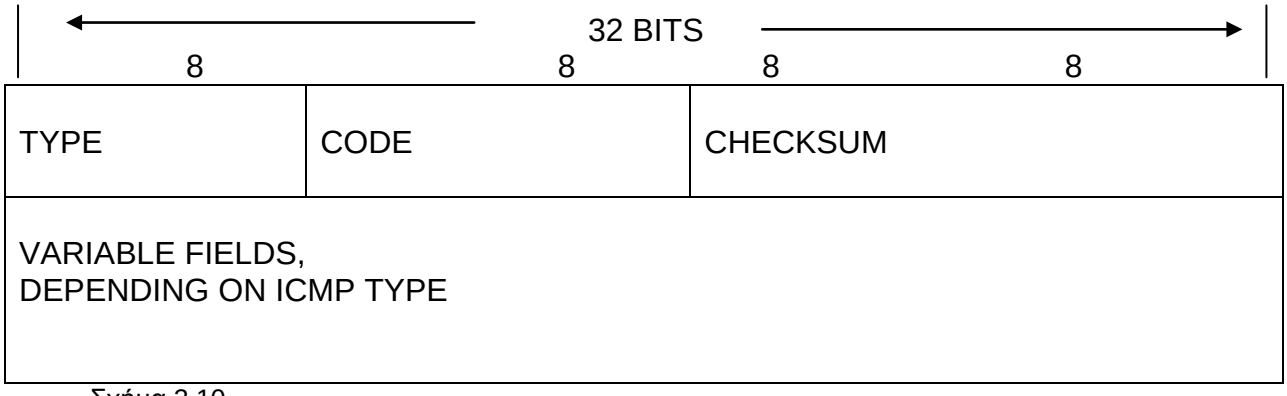
Αντίστροφο ARP

Αντί της χαρτογράφησης μιας διεύθυνσης υλικού σε μια γνωστή διεύθυνση IP, το αντίστροφο arp (RARP) χαρτογραφεί μια διεύθυνση IP σε μια γνωστή διεύθυνση υλικού. Μερικές συσκευές, όπως οι diskless τερματικοί σταθμοί, μπορούν να μην ξέρουν τη διεύθυνση IP τους, στο ξεκίνημα. Το RARP μπορεί να προγραμματιστεί σε firmware σε αυτές τις συσκευές, επιτρέποντας να εκδώσουν ένα arp αίτημα που έχει burned-in τη διεύθυνση υλικού τους. Η απάντηση από τον διακομιστή RARP θα προμηθεύσει την κατάλληλη IP διεύθυνση.

Το RARP κατά ένα μεγάλο μέρος αντικαθίσταται από το πρωτόκολλο Bootstrap (BOOTP) και της επέκτασής του το δυναμικό πρωτόκολλο διαμόρφωσης οικοδεσποτών (DHCP), όπου και τα δύο μπορούν να παρέχουν περισσότερες πληροφορίες από τη διεύθυνση IP, και το οποίο, αντίθετα από το RARP, μπορεί να καθοδηγηθεί από την τοπική σύνδεση δεδομένων.

ICMP

Το πρωτόκολλο ελέγχου μηνυμάτων Διαδικτύου, ή ICMP, που περιγράφεται σε RFC 792, διευκρινίζει ποικίλα μηνύματα των οποίων κοινός σκοπός είναι να ρυθμιστεί το internetwork. Τα μηνύματα ICMP μπορούν να ταξινομηθούν είτε ως μηνύματα λάθους είτε ως ερωτήσεις και απαντήσεις. Το σχήμα 2.10 παρουσιάζει το γενικό σχήμα πακέτων ICMP.



Σχήμα 2.10
Το πακέτο κεφαλής icmp περιλαμβάνει : type field code field checksum.

ΤΟ ΣΤΡΩΜΑ HOST-TO-HOST

Το επίπεδο host-to-host του TCP/IP πρωτοκόλλου ορθώς διατυπωμένο. Όπου το στρώμα διαδικτύου είναι αρμόδιο για τις λογικές πορείες μεταξύ των δικτύων, το στρώμα host-to-host είναι αρμόδιο για την πλήρη λογική πορεία μεταξύ δύο οικοδεσποτών σε ανόμοια δίκτυα. Από μια άλλη άποψη, το στρώμα host-to-host είναι μια διεπαφή στα χαμηλότερα στρώματα της ακολουθίας πρωτοκόλλου, που ελευθερώνει τις εφαρμογές από οποιαδήποτε ανησυχία για το πώς τα δεδομένα τους παραδίδονται πραγματικά.
Κάτι ανάλογο σε αυτήν την υπηρεσία είναι ένα εταιρικό mailroom. Ένα πακέτο μπορεί να δοθεί στο mailroom με τις ανάγκες που εκφράζονται για την παράδοσή του (γενική παράδοση, ολονύκτια). Το πρόσωπο που υποβάλλει το αίτημα παράδοσης δεν είναι ανάγκη να ξέρει, και δεν ενδιαφέρεται πιθανώς, για τις πραγματικές λειτουργίες της παράδοσης του πακέτου. Οι άνθρωποι του mailroom θα κανονίσουν για την κατάλληλη υπηρεσία για να ικανοποιήσουν τις απαιτήσεις παράδοσης.
Οι δύο αρχικές υπηρεσίες που προσφέρονται από το στρώμα host-to-host είναι το TCP και UDP.

TCP

Το πρωτόκολλο ελέγχου μετάδοσης, το TCP, περιγράφεται στο RFC 793, παρέχει στις εφαρμογές μια αξιόπιστη, με προσανατολισμένη-σύνδεση υπηρεσία. Με άλλα λόγια, το TCP παρέχει μια σύνδεση από σημείο σε σημείο.
Οι από σημείο σε σημείο συνδέσεις έχουν δύο χαρακτηριστικά:

- Έχουν μόνο μια πορεία για τον προορισμό. Ένα πακέτο μπαίνει στο ένα άκρο της σύνδεσης και δεν μπορεί να χαθεί, επειδή η μόνη θέση για να πάει είναι το άλλο άκρο της σύνδεσης.
- Τα πακέτα φθάνουν με την ίδια σειρά με την οποία στέλνονται.

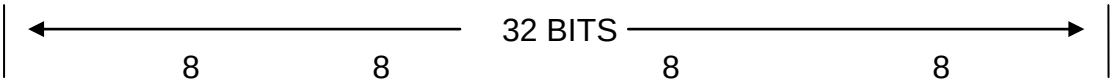
Το TCP παρέχει μια από σημείο σε σημείο σύνδεση, αν και στην πραγματικότητα δεν υπάρχει καμία τέτοια σύνδεση. Το στρώμα TCP του

διαδικτύου χρησιμοποιεί μια υπηρεσία παράδοσης πακέτων χωρίς σύνδεση. Το ανάλογο αυτού είναι η ταχυδρομική υπηρεσία. Εάν ένας σωρός από επιστολές δίνεται στο μεταφορέα ταχυδρομείου για την παράδοση, δεν υπάρχει καμία εγγύηση ότι οι επιστολές θα φθάσουν συσσωρευμένα με την ίδια σειρά, ή ότι όλες θα φθάσουν την ίδια ημέρα, ή ότι πράγματι θα φθάσουν. Η ταχυδρομική υπηρεσία δεσμεύει μόνο στην καταβολή καλύτερης προσπάθειάς της να παραδώσει τις επιστολές.
Παρομοίως, το στρώμα διαδικτύου δεν εγγυάται ότι όλα τα πακέτα θα πάρουν την ίδια διαδρομή, και επομένως δεν υπάρχει καμία εγγύηση ότι θα φθάσουν με την ίδια σειρά και χρόνο που στάλθηκαν, ή ότι πράγματι θα φθάσουν.
Αφ'ετέρου, ένα τηλεφώνημα είναι μια υπηρεσία προσανατολισμένη προς τη σύνδεση. Τα στοιχεία πρέπει να φθάσουν διαδοχικά και αξιόπιστα, ή αλλιώς είναι άχρηστα. Όπως ένα τηλεφώνημα, το TCP πρέπει πρώτα να εγκαταστήσει μια σύνδεση, κατόπιν να μεταφέρει τα δεδομένα, και έπειτα να εκτελέσει την αποσύνδεση όταν η μεταφορά δεδομένων έχει ολοκληρωθεί.
Το TCP χρησιμοποιεί τρεις θεμελιώδεις μηχανισμούς για να ολοκληρώσει μια υπηρεσία προσανατολισμένη προς τη σύνδεση πάνω από μια χωρίς σύνδεση υπηρεσία:

- Τα πακέτα ονομάζονται με αριθμούς ακολουθίας έτσι ώστε η λήψη της υπηρεσίας TCP να μπορεί να βάλει σε σωστή σειρά τα πακέτα πριν τα παραδώσει στην εφαρμογή προορισμού.
- Το TCP χρησιμοποιεί ένα σύστημα acknowledgments, checksums και timers για να παρέχει αξιοπιστία. Ένας δέκτης μπορεί να ειδοποιήσει έναν αποστολέα πότε αναγνωρίζει ότι ένα πακέτο σε μια ακολουθία έχει αποτύχει να φθάσει ή έχει λάθη, ή ένας αποστολέας μπορεί να υποθέσει ότι ένα πακέτο δεν έχει φθάσει εάν ο δέκτης δεν στείλει ένα acknowledgment μέσα σε ένα ορισμένο χρονικό διάστημα μετά από τη μετάδοση. Και στις δύο περιπτώσεις, ο αποστολέας θα στείλει εκ νέου το πακέτο.
- Το TCP χρησιμοποιεί έναν μηχανισμό αποκαλούμενο windowing για να ρυθμίσει τη ροή των πακέτων, το windowing μειώνει τις πιθανότητες τα πακέτα να πέφτουν από τους πλήρεις buffers στο δέκτη.

Το TCP συνδέει μια κεφαλή στο στρώμα αίτησης δεδομένων, η κεφαλή περιέχει τομείς για τους αριθμούς ακολουθίας και άλλες πληροφορίες απαραίτητες για τους μηχανισμούς καθώς επίσης και τομείς για τις διευθύνσεις αποκαλούμενες port numbers, οι οποίοι προσδιορίζουν τις αιτήσεις πηγής και προορισμού των δεδομένων. Το δεδομένο αίτησης με τη συνημμένη κεφαλή TCP είναι έπειτα τοποθετημένο μέσα σε ένα πακέτο IP για την παράδοση. Το σχήμα 1.11 παρουσιάζει τους τομείς της κεφαλής TCP.
Το port πηγής και προορισμού είναι δεκαεξάμπιτοι τομείς που διευκρινίζουν τις αιτήσεις πηγής και προορισμού για τα δεδομένα. Όπως άλλοι αριθμοί που χρησιμοποιούνται από το TCP/IP, RFC 1700 περιγράφει όλους τους αριθμούς port σε κοινή χρήση ή όχι. Ένας αριθμός port για μια αίτηση, όταν συνδέεται με τη διεύθυνση IP του οικοδεσπότη που η αίτηση βρίσκεται, καλείται υποδοχή(socket). Μια υποδοχή προσδιορίζει μεμονωμένα κάθε αίτηση σε ένα internetwork.

Ο αριθμός ακολουθίας(sequence number) είναι ένας τριανταδυάμπιτος αριθμός που προσδιορίζει σε ποια ροή δεδομένων του αποστολέα ταιριάζουν τα δεδομένα.



SOURCE PORT			DESTINATION PORT
SEQUENCE NUMBER			
ACKNOWLEDGMENT NUMBER			
HLEN	RESERVED (6 BITS)	FLAGS (6 BITS)	WINDOW SIZE
CHECKSUM			URGENT POINTER
OPTIONS AND PADDING			

Σχήμα 2.11
Το σχήμα της κεφαλής του TCP.

Παραδείγματος χάριν, εάν ο αριθμός ακολουθίας ενός τμήματος είναι 1343 και το τμήμα περιέχει 512 οχτάδες από δεδομένα, το επόμενο τμήμα πρέπει να έχει έναν αριθμό ακολουθίας 1343 + 512 + 1 = 1856.
Ο αριθμός αναγνώρισης είναι ένας τριανταδυάμπιτος τομέας που προσδιορίζει τον αριθμό ακολουθίας, η πηγή έπειτα αναμένει να λάβει από τον προορισμό. Εάν ένας οικοδεσπότης λάβει έναν αριθμό αναγνώρισης που ταιριάζει με τον επόμενο αριθμό ακολουθίας σκοπεύει να το στείλει (ή το έχει στείλει) ξέροντας όχι μόνο ότι τα πακέτα έχουν χαθεί αλλά και που τα πακέτα έχουν χαθεί.
Το μήκος κεφαλών, αποκαλούμενο μερικές φορές offset δεδομένων, είναι ένας τομέας τεσσάρων-bits που δείχνει το μήκος της κεφαλής σε τριανταδυάμπιτες λέξεις. Αυτός ο τομέας είναι απαραίτητος για να προσδιορίσει την αρχή των δεδομένων επειδή ο τομέας των επιλογών είναι μεταβλητός.

Ο reserved τομέας είναι έξι bits, τα οποία είναι πάντα μηδέν.
Οι σημαίες(flags) είναι έξι σημαίες 1-bits που χρησιμοποιούνται για τη ροή δεδομένων και τον έλεγχο της σύνδεσης. Οι σημαίες είναι Urgent (URG), Acknowledgment (ACK), Push (PSH), Reset (RST), Synchronize (SYN), and Final (FIN).
Το μέγεθος παραθύρων είναι ένας δεκαεξάμπιτος τομέας που χρησιμοποιείται για τον έλεγχο ροής. Διευκρινίζει τον αριθμό οχτάδων, αρχίζοντας από την οχτάδα που υποδεικνύεται από τον αριθμό αναγνώρισης, τον οποίο ο αποστολέας του τμήματος θα δεχτεί από το peer του στην άλλη άκρη της σύνδεσης προτού να πρέπει το peer να σταματήσει και να περιμένει μια αναγνώριση.
Το Checksum είναι 16 bits, καλύπτοντας και την κεφαλή και τα δεδομένα των στοιχείων, επιτρέποντας την ανίχνευση λάθους.
Το Urgent Pointer χρησιμοποιείται μόνο όταν τίθεται η σημαία URG. Ο δεκαεξάμπιτος αριθμός προστίθεται στον αριθμό ακολουθίας για να δείξει το τέλος των επειγόντων δεδομένων.
Οι επιλογές, όπως το όνομα υπονοεί, διευκρινίζουν τις επιλογές που απαιτούνται με τη διαδικασία TCP του αποστολέα. Η συνηθισμένη χρησιμοποιούμενη επιλογή είναι μέγιστο μέγεθος τμήματος, το οποίο

ενημερώνει το δέκτη για το μεγαλύτερο τμήμα που ο αποστολέας είναι πρόθυμος να δεχτεί. Το υπόλοιπο του τομέα είναι γεμισμένο με μηδενικά για να εξασφαλίσει ότι το μήκος των κεφαλών είναι ένα πολλαπλάσιο 32 οχτάδων.

UDP

Το πρωτόκολλο διαγραμμάτων δεδομένων χρηστών, ή UDP, που περιγράφεται σε RFC 768, παρέχει μια υπηρεσία παράδοσης πακέτων χωρίς σύνδεση. Με την πρώτη ματιά, μπορεί να φανεί αμφισβητήσιμο ότι οποιαδήποτε αίτηση θα προτιμούσε μια αναξιόπιστη παράδοση μέσω του προσανατολισμένου προς τη σύνδεση TCP. Το πλεονέκτημα του UDP, εντούτοις, είναι ότι κανένας χρόνος δεν ξοδεύεται οργανώνοντας μια σύνδεση, απλά στέλνεται το δεδομένο. Οι αιτήσεις που στέλνουν σύντομα καταιγιστικά δεδομένα αντιλαμβάνονται ένα πλεονέκτημα απόδοσης χρησιμοποιώντας UDP αντί για το TCP.
Το σχήμα 2.12 παρουσιάζει ένα άλλο πλεονέκτημα του UDP: μια πολύ μικρότερη κεφαλή από το TCP. Οι τομείς source και destination port είναι οι ίδιοι όπως είναι και στην κεφαλή TCP, το μήκος UDP δείχνει το μήκος ολόκληρου του τμήματος σε οχτάδες. Το Checksum καλύπτει ολόκληρο το τμήμα, αλλά αντίθετα από το TCP, το checksum εδώ είναι προαιρετικό, όταν κανένα checksum δεν χρησιμοποιείται, ο τομέας ορίζεται σε όλα μηδενικά.

32 BITS

8 | 8	8 | 8
SOURCE PORT	DESTINATION PORT
UDP LENGTH	CHECKSUM

Σχήμα 2.12
Το σχήμα κεφαλών UDP

Η εστίαση αυτού του κεφαλαίου ήταν κατά ένα μεγάλο μέρος στους μηχανισμούς από τους οποίους το στρώμα διαδικτύου μιας συσκευής (ή

στρώμα δικτύων της OSI) προσδιορίζεται και πώς χαρτογραφείται στο στρώμα διεπαφών δικτύων (ή συνδέσεων δεδομένων της OSI). Οι λειτουργίες στρώματος Διαδικτύου που είναι σημαντικές στη δρομολόγηση εξετάστηκαν επίσης. Το ακόλουθο κεφάλαιο εξετάζει τη λειτουργία δρομολόγησης και τις πληροφορίες που ένας δρομολογητής απαιτεί για να εκτελέσει αυτή τη λειτουργία.

ΚΕΦΑΛΑΙΟ 3
ΣΤΑΤΙΚΗ ΔΡΟΜΟΛΟΓΗΣΗ

Εισαγωγή

Μια σημαντική παρατήρηση από το κεφάλαιο, "TCP/IP," είναι ότι τα στρώματα σύνδεση δεδομένων/φυσικό, και τα στρώματα μεταφοράς/δικτύου, όπως καθορίζονται από το πρότυπο της OSI, εκτελούν πολύ παρόμοια καθήκοντα: Παρέχουν τα μέσα για την μεταφορά δεδομένων από την πηγή σε έναν προορισμό μέσα από κάποια πορεία. Η διαφορά είναι ότι τα στρώματα σύνδεση δεδομένων/φυσικό παρέχει τις επικοινωνίες μέσα από μια φυσική πορεία, ενώ αντιθέτως τα στρώματα μεταφοράς/δικτύου παρέχουν τις επικοινωνίες μέσα από μια λογική ή εικονική πορεία φτιαγμένη από μια σειρά συνδέσεων δεδομένων.
Περαιτέρω, το προηγούμενο κεφάλαιο έδειξε ότι για να πραγματοποιηθούν οι επικοινωνίες μέσα από μια φυσική πορεία, συγκεκριμένες πληροφορίες για τα προσδιοριστικά και encapsulations συνδέσεων δεδομένων πρέπει να αποκτιέται και να αποθηκεύεται σε μια βάση δεδομένων όπως Arp cache. Ομοίως, οι πληροφορίες που τα στρώματα μεταφοράς/δικτύου απαιτούν για να κάνουν την εργασία τους πρέπει επίσης να αποκτηθούν και να αποθηκευτούν. Αυτές οι πληροφορίες αποθηκεύονται στον πίνακα διαδρομών, επίσης γνωστό ως βάση δεδομένων αποστολής.
Αυτό το κεφάλαιο εξετάζει ποιο είδος πληροφοριών απαιτείται για να καθοδηγήσει ένα πακέτο, πώς αυτές οι πληροφορίες αποθηκεύονται στον πίνακα διαδρομών, πώς να εισαγάγει τις πληροφορίες στη βάση δεδομένων, και μερικές τεχνικές για την δημιουργία ενός δρομολογημένου internetwork με την εισαγωγή των κατάλληλων πληροφοριών μέσα στους πίνακες διαδρομών των κατάλληλων δρομολογητών.

Ο πίνακας διαδρομών

Για να καταλάβουμε το είδος πληροφοριών που υπάρχουν στον πίνακα διαδρομών, είναι χρήσιμο να ξεκινήσουμε με μια εξέταση του τι είναι αυτό που συμβαίνει όταν ένα πλαισιωμένο πακέτο φθάνει σε μια από τις διεπαφές ενός

δρομολογητή. Το προσδιοριστικό σύνδεσης δεδομένων στον τομέα διευθύνσεων προορισμού του πλαισίου εξετάζεται. Εάν περιέχει είτε το προσδιοριστικό της διεπαφής του δρομολογητή είτε ένα προσδιοριστικό broadcast μετάδοσης, ο δρομολογητής αφαιρεί το πλαίσιο και περνά το εσωκλειόμενο πακέτο στο στρώμα δικτύου. Στο στρώμα δικτύου, η διεύθυνση προορισμού του πακέτου εξετάζεται. Εάν η διεύθυνση προορισμού είναι είτε η διεύθυνση IP της διεπαφής του δρομολογητή είτε μια διεύθυνση broadcast μετάδοσης όλο-οικοδεσποτών, ο τομέας πρωτοκόλλου του πακέτου εξετάζεται και το εσωκλειόμενο στοιχείο στέλνεται στην κατάλληλη εσωτερική διαδικασία.

Οποιεσδήποτε άλλες διευθύνσεις προορισμού καλούν για δρομολόγηση. Η διεύθυνση μπορεί να είναι για έναν οικοδεσπότη σε ένα άλλο δίκτυο με το οποίο ο δρομολογητής είναι συνδεμένος (συμπεριλαμβανομένης της διεπαφής δρομολογητών που συνδέεται με εκείνο το δίκτυο) ή για έναν οικοδεσπότη σε ένα δίκτυο όχι άμεσα συνδεμένο με το δρομολογητή. Η διεύθυνση μπορεί επίσης να είναι μια κατευθυνόμενη broadcast μετάδοση, στην οποία υπάρχει μια ευδιάκριτη διεύθυνση δικτύου ή υποδικτύου, και τα υπόλοιπα bits οικοδεσποτών είναι όλα ένα. Αυτές οι διευθύνσεις είναι επίσης δρομολογήσιμες.

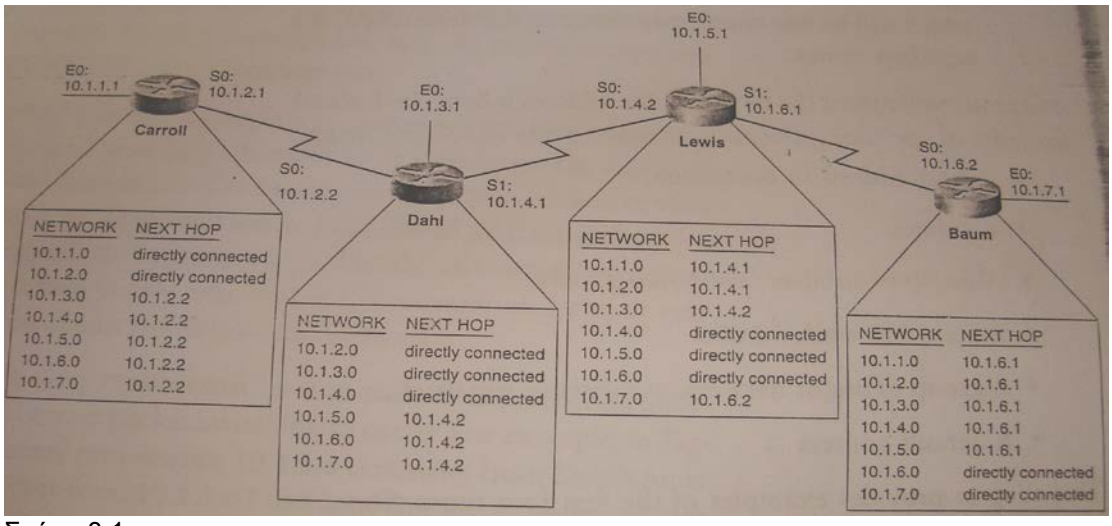
Εάν το πακέτο πρόκειται να δρομολογηθεί, ο δρομολογητής θα κάνει ένα lookup στον πίνακα διαδρομών για να αποκτήσει τη σωστή διαδρομή. Τουλάχιστον, κάθε είσοδος διαδρομών στη βάση δεδομένων πρέπει να περιέχει δύο στοιχεία:

- Μια διεύθυνση προορισμού. Αυτή είναι η διεύθυνση του δικτύου που ο δρομολογητής μπορεί να φθάσει. Όπως αυτό το κεφάλαιο εξηγεί, ο δρομολογητής μπορεί να έχει περισσότερες από μια διαδρομές στην ίδια διεύθυνση και/ ή μια ομάδα υποδικτύων με ίδιων ή διαφορετικών μηκών που ομαδοποιούνται κάτω από την ίδια σημαντική διεύθυνση δικτύων IP.
- Ένας δείκτης στον προορισμό. Αυτός ο δείκτης είτε δείχνει ότι το δίκτυο προορισμού συνδέεται άμεσα στο δρομολογητή ή δείχνει τη διεύθυνση άλλου δρομολογητή σε ένα άμεσα συνδεδεμένο δίκτυο. Αυτός ο δρομολογητής, που θα είναι ένα hop δρομολογητή πιο κοντά στον προορισμό, είναι ένας δρομολογητής επόμενου-hop.

Ο δρομολογητής θα ταιριάξει με την πιο συγκεκριμένη διεύθυνση που μπορεί. Κατά μειούμενη σειρά κατά την ιδιομορφία, η διεύθυνση μπορεί να είναι μια από τις ακόλουθες:

- Μια διεύθυνση οικοδεσποτών (*μια διαδρομή οικοδεσποτών*)
- ένα υποδίκτυο
- Μια ομάδα υποδικτύων (*μια συνοπτική διαδρομή*)
- ένας σημαντικός αριθμός δικτύων
- Μια ομάδα σημαντικών αριθμών δικτύων (*ένα supernet*)
- Μια διεύθυνση προεπιλογής

Εάν η διεύθυνση προορισμού του πακέτου δεν μπορεί να αντιστοιχηθεί με καμία εισαγωγή του πίνακα διαδρομών, το πακέτο πέφτει και ένα μήνυμα ICMP απρόσιτου προορισμού στέλνεται στη διεύθυνση προέλευσης.
Το σχήμα 3.1 παρουσιάζει ένα απλό internetwork και τις καταχωρήσεις του πίνακα διαδρομών που απαιτούνται από κάθε δρομολογητή.



Σχήμα 3.1
Η ελάχιστη πληροφορία που χρειάζεται για τα δεδομένα κάθε δρομολογητής αποτελείται από τον προορισμό δικτύων και τους δείκτες σε αυτά τα δίκτυα.

Εάν ο δρομολογητής Carroll στο σχήμα 3.1 λάβει ένα πακέτο με μια διεύθυνση προέλευσης 10.1.1.97 και μια διεύθυνση προορισμού 10.1.7.35, ένα lookup στον πίνακα διαδρομών καθορίζει ότι η καλύτερη αντιστοιχία για τη διεύθυνση προορισμού είναι το υποδίκτυο 10.1.7.0, εφικτό μέσω της

διεύθυνσης next-hop 10.1.2.2, στη διεπαφή S0.Το πακέτο στέλνεται σε αυτόν τον επόμενο δρομολογητή (Dahl), που κάνει ένα lookup στον πίνακά του και βλέπει ότι το δίκτυο 10.1.7.0 είναι εφικτό μέσω της διεύθυνσης next-hop 10.1.4.2, έξω διεπαφή S1. Η διαδικασία συνεχίζεται έως ότου φθάσει το πακέτο στο δρομολογητή Baum. Αυτός ο δρομολογητής, που λαμβάνει το πακέτο στη διεπαφή του S0, κάνει ένα lookup και βλέπει ότι ο προορισμός είναι σε ένα από τα άμεσα συνδεδεμένα δίκτυά του, έξω E0. Η δρομολόγηση ολοκληρώθηκε, και το πακέτο παραδόθηκε στον οικοδεσπότη 10.1.7.35 στη σύνδεση Ethernet.

Η διαδικασία δρομολόγησης, όπως εξηγείται, υποθέτει ότι ο δρομολογητής μπορεί να ταιριάξει τις απαριθμημένες διευθύνσεις next-hop στις διεπαφές του. Παραδείγματος χάριν, ο δρομολογητής Dahl πρέπει να ξέρει ότι η διεύθυνση Lewis 10.1.4.2 είναι εφικτή μέσω της διεπαφής S1. Ο Dahl ξέρει από τη διεύθυνση IP και τη μάσκα υποδικτύου που ορίζονται στο S1 ότι το S1 συνδέεται άμεσα με το υποδίκτυο 10.1.4.0. Έπειτα ξέρει ότι 10.1.4.2, ένα μέλος του ίδιου υποδικτύου, πρέπει να συνδεθεί με το ίδιο δίκτυο.

Παρατηρήστε ότι κάθε δρομολογητής πρέπει να έχει σταθερές και ακριβής πληροφορίες για να εξασφαλιστεί η σωστή ανταλλαγή πακέτων.

Παραδείγματος χάριν, στο σχήμα 3.1 μια είσοδος για το δίκτυο 10.1.1.0 λείπει από τον πίνακα διαδρομών Dahl. Ένα πακέτο από 10.1.1.97 στο 10.1.7.35 θα παραδοθεί, αλλά όταν στέλνεται μια απάντηση από 10.1.7.35 στο 10.1.1.97, το πακέτο περνά από Baum σε Lewis σε Dahl. Το Dahl κάνει ένα lookup και διαπιστώνει ότι δεν έχει καμία είσοδο για το υποδίκτυο 10.1.1.0, έτσι το πακέτο απορρίπτεται, και ένα απρόσιτο μήνυμα προορισμού ICMP στέλνεται στον οικοδεσπότη 10.1.7.35.

Το σχήμα 3.2 παρουσιάζει τον πραγματικό πίνακα διαδρομών Cisco από το δρομολογητή Lewis του σχήματος 3.1. Η εντολή για την εξέταση του πίνακα διαδρομών IP ενός δρομολογητή Cisco είναι **show ip route**.

```
Lewis#show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP,
       D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area,
       N1 – OSPF NSSA external type 1, N2 – ospf nssa external type 2,
       E1 – OSPF external type 1, E2 – ospf external type 2, E – EGP,
       i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate default,
       U – per-user staticroute, 0 – ODR
```

```
Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 7 subnets
S       10.1.3.0[1/0] via 10.1.4.1
S       10.1.2.0[1/0] via 10.1.4.1
S       10.1.1.0[1/0] via 10.1.4.1
S       10.1.7.0[1/0] via 10.1.6.2
C       10.1.6.0 is directly connected, Serial1
C       10.1.5.0 is directly connected, Ethernet0
C       10.1.4.0 is directly connected, Serial0
Lewis#
```

Σχήμα 3.2
Ο πίνακας διαδρομών Cisco για το δρομολογητή Lewis του σχήματος 3.1.

Εξετάστε το περιεχόμενο αυτής της βάσης δεδομένων και να το συγκρίνετε με το γενικό πίνακα που παρουσιάζεται για το Lewis στο σχήμα 3.1. Ένα κλειδί στην κορυφή του πίνακα εξηγεί τα γράμματα κάτω από την αριστερή πλευρά του πίνακα. Αυτά τα γράμματα δείχνουν πώς κάθε είσοδος διαδρομών μαθεύτηκε, στο σχήμα 3.2 όλες οι διαδρομές κολλιούνται με το C για "directly connected," είτε το S για "static entry." Η δήλωση "gateway of last resort is not set" αναφέρεται σε μια προεπιλεγμένη διαδρομή. Στην κορυφή του πίνακα είναι μια δήλωση που δείχνει ότι ο πίνακας διαδρομών ξέρει για επτά υποδίκτυα της σημαντικότερης διεύθυνσης 10.0.0.0 δικτύων, με μια μάσκα 24-bits. Για κάθε μια από τις επτά καταχωρήσεις διαδρομών, το υποδίκτυο προορισμού παρουσιάζεται, για τις καταχωρήσεις που δεν συνδέονται άμεσα — διαδρομές για τις οποίες το πακέτο πρέπει να διαβιβαστεί σε έναν δρομολογητή next-hop— μια πλειάδα κατηγοριών [administrative distance/metric] για αυτή την διαδρομή.
Metric, είναι ένας τρόπος για τις διαδρομές που εκτιμώνται από την προτίμηση — χαμηλότερο metric, "μικρότερη" η διαδρομή. Παρατηρήστε ότι οι στατικές διαδρομές που παρουσιάζονται στο σχήμα 3.2 έχουν ένα metric 0. Τέλος, είτε η διεύθυνση της άμεσα συνδεδεμένης διεπαφής του next-hop δρομολογητή είτε της διεπαφής με τις οποίες ο προορισμός συνδέεται παρουσιάζεται.

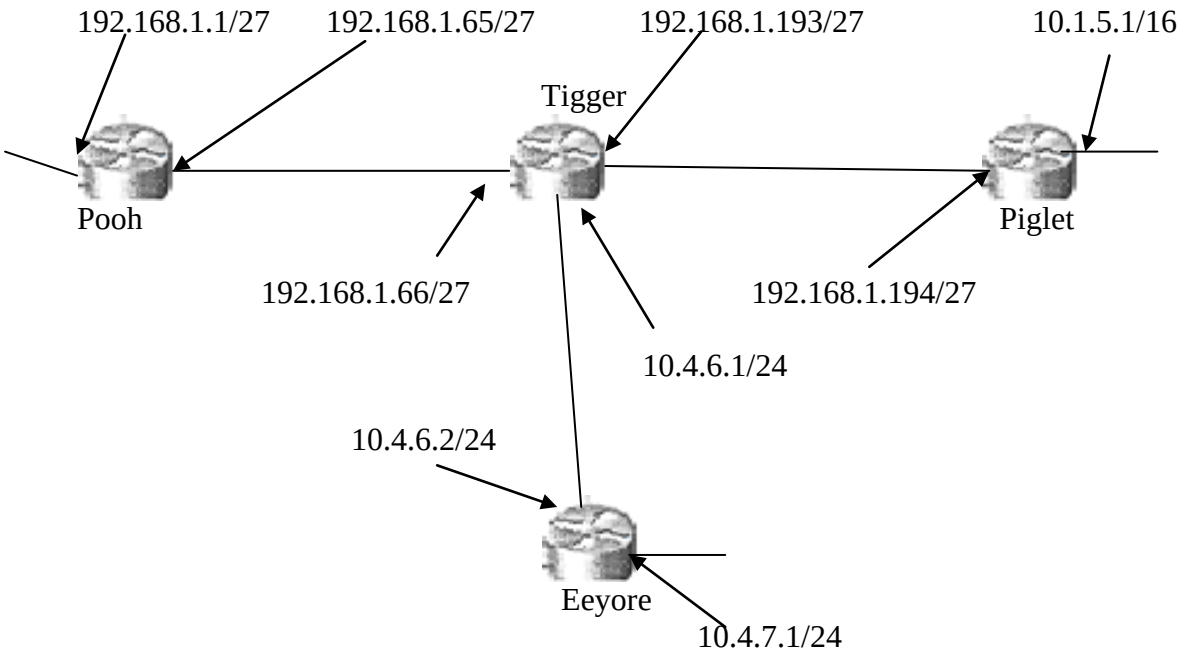
ΔΙΑΜΟΡΦΩΝΟΝΤΑΣ ΣΤΑΤΙΚΕΣ ΔΙΑΔΡΟΜΕΣ

Ο πίνακας διαδρομών αποκτά τις πληροφορίες με δύο τρόπους. Οι πληροφορίες μπορούν να εισαχθούν με το χέρι, με τη βοήθεια μιας στατικής εισόδου διαδρομών, ή αυτόματα από ένα από τα διάφορα συστήματα αυτόματης ανακάλυψης και διανομής πληροφοριών γνωστές όπως dynamic routing protocols.

Πιο επικεντρωμένα, η στατική δρομολόγηση προτιμάται σε σχέση με τη δυναμική δρομολόγηση σε ορισμένες περιστάσεις. Όπως με οποιαδήποτε διαδικασία, όσο πιο αυτόματο αυτό είναι, τόσο λιγότερο έλεγχο έχουμε πάνω σε αυτό. Αν και η δυναμική (αυτόματη) δρομολόγηση απαιτεί πολύ λιγότερη ανθρώπινη επέμβαση, η στατική δρομολόγηση επιτρέπει τον πολύ ακριβή έλεγχο συμπεριφοράς δρομολόγησης ενός internetwork. Η τιμή που καταβάλλεται για αυτήν την ακρίβεια είναι η ανάγκη του χειρωνακτικού επανασχηματισμού οποτεδήποτε αλλάζει η τοπολογία του δικτύου.

Case Study: Απλές στατικές διαδρομές

Το σχήμα 3.3 παρουσιάζει ένα internetwork με τέσσερις δρομολογητές και έξι δίκτυα. Παρατηρήστε ότι τα υποδίκτυα του δικτύου 10.0.0.0 είναι διακεκομμένα, εκεί υπάρχει ένα διαφορετικό σημαντικό υποδίκτυο δικτύων (192.168.1.192, στη σύνδεση Tigger-to-piglet) που χωρίζει 10.1.0.0 από τα άλλα 10.0.0.0 υποδίκτυα. Τα υποδίκτυα 10.0.0.0 είναι επίσης μεταβλητά —οι μάσκες υποδικτύου δεν είναι συνεπή σε όλο το internetwork. Τελικά, η διεύθυνση υποδικτύου της σύνδεσης Ethernet Pooh είναι ένα όλο-μηδενικά υποδίκτυο.



Σχήμα 3.3
Πρωτοκόλλα δρομολόγησης όπως RIP και IGRP δεν μπορούν εύκολα να δρομολογήσουν αυτό το μη συνεχές, πολλαπλά διασπασμένο internetwork, αλλά η στατική δρομολόγηση μπορεί.

Η διαδικασία για μια στατική δρομολόγηση ενός internetwork έχει τρία βήματα:

1. Για κάθε σύνδεση δεδομένων μέσα στο internetwork, προσδιορίστε όλες τις διευθύνσεις (υποδίκτυο ή δίκτυο).

2. Για κάθε δρομολογητή, προσδιορίστε όλες τις συνδέσεις δεδομένων που συνδέονται όχι άμεσα με εκείνο τον δρομολογητή.

3. Για κάθε δρομολογητή, γράψτε μια δήλωση διαδρομών για κάθε σύνδεση δεδομένων όχι άμεσα συνδεμένη με αυτόν.

Γράφοντας δηλώσεις διαδρομών για τις άμεσα συνδεδεμένες συνδέσεις δεδομένων ενός δρομολογητή είναι περιττές, επειδή οι διευθύνσεις και οι μάσκες που διαμορφώνονται στις διεπαφές του δρομολογητή κάνουν εκείνα τα δίκτυα να καταγράφονται στον πίνακα διαδρομών του.

Παραδείγματος χάριν, το internetwork στο σχήμα 3.3 έχει έξι υποδίκτυα:

- 10.1.0.0/16
- 10.4.6.0/24
- 10.4.7.0/24
- 192.168.1.192/27
- 192.168.1.64/27

- 192.168.1.0/27

Για να διαμορφώσουν τις στατικές διαδρομές για το Piglet, τα υποδίκτυα που δεν συνδέονται άμεσα προσδιορίζονται ως εξής:

- 10.4.6.0/24
- 10.4.7.0/24
- 192.168.1.64/27
- 192.168.1.0/27

Αυτά είναι τα υποδίκτυα για τα οποία οι στατικές διαδρομές πρέπει να γραφτούν. Οι εντολές για την είσοδο των στατικών διαδρομών του Piglet είναι οι ακόλουθες:

Piglet(config)# **ip route 192.168.1.0 255.255.255.224 192.168.1.193**
Piglet(config)# **ip route 192.168.1.64 255.255.255.224 192.168.1.193**
Piglet(config}# **ip route 10.4.6.0 255.255.255.3 192.168.1.193**
Piglet(config)# **ip route 10.4.7.0 255.255.255.0 192.168.1.193**

Ακολουθώντας τα ίδια βήματα, οι καταχωρήσεις διαδρομών για τους άλλους 3 δρομολογητές είναι:

Pooh(config)# **ip route 192.168.1.192 255.255.255.224 192.168.1.66**
Pooh(config)# **ip route 10.1.0.0 255.255.0.0 192.168.1.66**
Pooh(config}# **ip route 10.4.6.0 255.255.255.0 192.168.1.66**
Pooh(config)# **ip route 10.4.7.3 255.255.255.0 192.168.1.66**
Tigger(config)# **ip route 192.168.1.0 255.255.255.224 192.168.1.65**
Tigger(config)# **ip route 10.1.0.0 255.255.0.0 192.168.1.194**
Tigger(config)# **ip route 10.4.7.0 255.255.255.0 10.4.6.2**
Eeyore(config)# **ip route 192.168.1.0 255.255.255.224 10.4.6.1**
Eeyore(config)# **ip route 192.168.1.64 255.255.255.224 10.4.6.1**
Eeyore(config}# **ip route 192.168.1.92 255.255.255.224 10.4.6.1**
Eeyore(config)# **ip route 10.1.0.0 255.255.0.0 10.4.6.1**

Οι εντολές δρομολόγησης διαβάζονται εύκολα εάν ο αναγνώστης θυμάται ότι κάθε εντολή περιγράφει μια είσοδο στον πίνακα διαδρομών. Η εντολή είναι ip route, ακολουθούμενη από τη διεύθυνση που εισάγεται στον πίνακα, μια μάσκα για τον καθορισμό του τμήματος δικτύου της διεύθυνσης, και η διεύθυνση της άμεσα συνδεδεμένης διεπαφής του δρομολογητή next-hop. Μια εναλλακτική εντολή διαμόρφωσης για τις στατικές διαδρομές διευκρινίζει τη διεπαφή από την οποία ένα δίκτυο επιτυγχάνεται αντί της διεύθυνσης του δρομολογητή next-hop. Παραδείγματος χάριν, οι καταχωρήσεις διαδρομών για Tigger θα μπορούσαν να είναι οι ακόλουθες:

Tigger(config)# **ip route 192.168.1.0 255.255.255.224 S0**
Tigger{config)# **ip route 10.1.0.0 255.255.0.0 E0**
Tigger(config)# **ip route 10.4.7.0 255.255.255.0 S1**

```
Tigger#show ip route
Gateway of last resort is not set
   10.0.0.0  is  variably  subnetted, 3 subnets, 2 masks
C    10.4.6.0   255.255.255.0   is  directly  connected, Serial1
S    10.4.7.0   255.255.255.0  [1/0] via 10.4.6.2
S    10.1.0.0   255.255.0.0  [1/0] via 192.168.1.194
   192.168.1.0  255.255.255.224 is subnetted, 3 subnets
C    192.168.1.64 is directly connected, Serial0
S    192.168.1.0 [1/0] via 192.168.1.65
C    192.168.1.192 is directly connected, Ethernet0
Tigger#
```

```
Tigger#show ip route
Gateway of last resort is not set
    10.0.0.0 is variably subnetted. 3 subnets, 2 .masks
C     10.4.6.0 255.255.255.0 is directly connected, Serial1
S    10.4.7.0 255.255.255.0 is directly connected, Serial1
S     10.1.0.0 255.255.0.0 is directly connected, Ethernet0
    192.168.1.0 255.255.255.224 is subnetted, 3 subnets
C    192.168.1.64 is directly connected, Serial0
S    192.168.1.0 is directly connected, Serial0
C    192.168.1.192 is directly connected, Ethernet0
Tigger#
```

Σχήμα 3.4
Ο πρώτος πίνακας δρομολόγησης είναι αποτέλεσμα των καταχωρήσεων της στατικής δρομολόγησης δείχνοντας στον δρομολογητή next-hop. Ο δεύτερος πίνακας είναι αποτέλεσμα που δείχνει στην διεπαφή ένα πακέτο που πρέπει να βγει για να φτάσει στο δίκτυο προορισμού

Case Study: Συνοπτικές διαδρομές

Μια συνοπτική διαδρομή είναι μια διεύθυνση που καλύπτει αρκετές ακόμα συγκεκριμένες διευθύνσεις σε έναν πίνακα διαδρομών. Είναι μάσκα διεύθυνσης που χρησιμοποιείται με μια είσοδο διαδρομής που καθιστά τις στατικές διαδρομές τόσο εύκαμπτες, χρησιμοποιώντας μια κατάλληλη μάσκα διευθύνσεων, είναι μερικές φορές δυνατό να δημιουργηθεί μια ενιαία συνοπτική διαδρομή για διάφορες διευθύνσεις προορισμού. Παραδείγματος χάριν, το προηγούμενο case study χρησιμοποιεί μια χωριστή είσοδο για κάθε σύνδεση δεδομένων. Η μάσκα κάθε εισόδου αντιστοιχεί στη μάσκα διευθύνσεων που χρησιμοποιείται στις διεπαφές συσκευών που συνδέονται

με εκείνη την σύνδεση δεδομένων. Εξετάζοντας πάλι το σχήμα 3.3, μπορείτε να δείτε ότι τα υποδίκτυα 10.4.6.0/24 και 10.4.7.0/24 θα μπορούσαν να διευκρινιστούν στο Piglet με μια ενιαία είσοδο 10.4.0.0/16, εφικτή μέσω Tigger. Επιπλέον, τα υποδίκτυα 192.168.1.0/27 και 192.168.1.64/27 θα μπορούσαν να λογαριαστούν στον πίνακα διαδρομών του με μια ενιαία είσοδο που δείχνει 192.168.1.0/24, επίσης εφικτό μέσω Tigger. Αυτές οι δύο καταχωρήσεις διαδρομών, 10.4.0.0/16 και 192.16.1.0/24, είναι συνοπτικές διαδρομές.
Χρησιμοποιώντας τις συνοπτικές διαδρομές, οι στατικές καταχωρήσεις διαδρομών του Piglet είναι:

Piglet(config)# **ip route 192.168.1.0 255.255.255.0 192.168.1.193**
Piglet(config)# **ip route 10.4.0.0 255.255.0.0 192.168.1.193**

Όλα τα υποδίκτυα του δικτύου 10.0.0.0 είναι εφικτά από Pooh μέσω Tigger, έτσι μια ενιαία είσοδος σε εκείνη την σημαντική διεύθυνση δικτύων και μια αντίστοιχη μάσκα είναι όλα αυτά που απαιτούνται:

Pooh(config)# **ip route 192.168.1.192 255.255.255.224 192.168.1.66**
Pooh(config)# **ip route 10.0.0.0 255.0.0.0 192.168.1.66**

Από Eeyore, όλες οι διευθύνσεις προορισμού αρχίζοντας με 192 είναι εφικτές μέσω Tigger. Η ενιαία είσοδος διαδρομών δεν είναι απαραίτητο να διευκρινίσει όλα τα bits διευθύνσεων της κατηγορίας C:

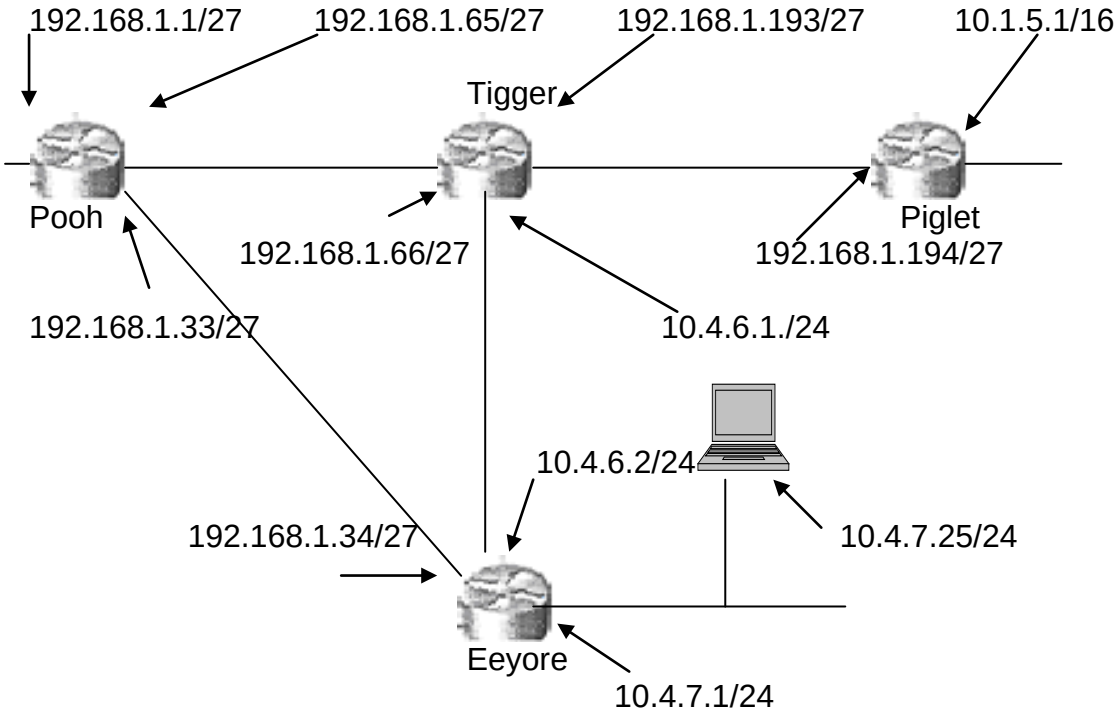
Eeyore(config)# **ip route 192.0.0.0 255.0.0.0 10.4.6.1**
Eeyore(config)# **ip route 10.1.0.0 255.255.0.0 10.4.6.1**

Με τη σύνοψη μιας ομάδας υποδικτύων ή ακόμα και σημαντικών δικτύων, ο αριθμός καταχωρήσεων στατικών διαδρομών μπορεί να μειωθεί δραστικά — σε αυτό το παράδειγμα, περισσότερο από το ένα τρίτο. Εντούτοις, προσοχή πρέπει να δίνεται κατά τη σύνοψη των διευθύνσεων, όταν γίνεται ανακριβώς, απροσδόκητες συμπεριφορές δρομολόγησης μπορεί να εμφανιστούν.

Case Study: Εναλλακτικές δρομολογήσεις

Στο σχήμα 3.5, μια νέα σύνδεση έχει προστεθεί μεταξύ Pooh και Eeyore. Όλα τα πακέτα από Pooh στα 10.0.0.0 δίκτυα θα πάρουν αυτήν την νέα πορεία με εξαίρεση τα πακέτα που προορίζονται για τον οικοδεσπότη 10.4.7.25, μια πολιτική δηλώνοντας ότι η κυκλοφορία προς αυτόν τον οικοδεσπότη πρέπει να περάσει από το Tigger. Οι στατικές εντολές διαδρομών σε Pooh θα είναι:

Pooh(config)# **ip route 192.168.1.192 255.255.255.224 192.168.1.66**
Pooh(config)# **ip route 10.0.3.0 255.0.0.0 192.168.1.34**
Pooh(config)# **ip route 10.4.7.25 255.255.255.255 192.168.1.66**



Σχήμα 3.5
Μια πιο άμεση διαδρομή από Pooh στα 10.4.0.0 υποδίκτυα έχει προστεθεί στο internetwork.

Οι πρώτες δύο καταχωρήσεις διαδρομών είναι οι ίδιες όπως πριν εκτός από το ότι η δεύτερη πορεία δείχνει τώρα τη νέα διεπαφή 192.168.1.34 Eeyore. Η τρίτη είσοδος είναι μια διαδρομή οικοδεσποτών, δείχνοντας τον ενιαίο οικοδεσπότη 10.4.7.25 και το κάνει εφικτό με τον καθορισμό της μάσκας διευθύνσεων σε όλα ένα. Παρατηρήστε ότι αντίθετα από την είσοδο για τα άλλα 10.0.0.0 υποδίκτυα, αυτή η διαδρομή οικοδεσποτών δείχνει τη διεπαφή του Tigger 192.168.1.66. Η λειτουργία διόρθωσης debug ip packet ανοίγεται

σε Pooh (σχήμα 3.6) για να παρατηρήσει τις πορείες των πακέτων που παίρνει από το δρομολογητή ως αποτέλεσμα των νέων καταχωρήσεων διαδρομών. Ένα πακέτο στέλνεται από έναν οικοδεσπότη 192.168.1.15 στον οικοδεσπότη 10.4.7.25. Τα δυο πρώτα διορθώνουν τα μηνύματα παγίδων, δείχνουν ότι το πακέτο καθοδηγείται από τη διεπαφή E0 στο δρομολογητή next-hop 192.168.1.66 (Tigger) στην έξω διεπαφή S0, όπως απαιτείται και ότι το πακέτο απάντησης παραλήφθηκε στο S0 και δρομολογήθηκε στον οικοδεσπότη 192.168.1.15 έξω E0.

```
Pooh#debug ip packet
IP packet debugging is on
Pooh#
IP: s=192.168.1.15 (Ethernet0), d=10.4.7.25 (Serial0), g=192.168.1.66,
forward
IP: s=10.4.7.25 (Serial), d=192.168.1.15 (Ethernet0), g=192.168.1.15,
forward
Pooh#
IP: s=192.168.1.15 (Ethernet0), d=10.4.7.100 (Serial1), g=192.168.1.34,
forward
IP: s=10.4.7.100 (Serial0), d=192.168.1.15 (Ethernet0), g=192.168.1.15,
forward
Pooh#
```

Σχήμα 3.6
Η εμφάνιση πιστοποιεί ότι οι νέες είσοδοι στον Pooh δουλεύουν σωστά.

Έπειτα ένα πακέτο στέλνεται από τον οικοδεσπότη 192.168.1.15 στον οικοδεσπότη 10.4.7.100. Τα πακέτα που προορίζονται για οποιοδήποτε οικοδεσπότη σε 10.0.0.0 υποδίκτυα, εκτός από τον οικοδεσπότη 10.4.7.25, πρέπει να καθοδηγηθούν μέσα από τη νέα σύνδεση με τη διεπαφή Eeyore 192.186.1.34. Το τρίτο μήνυμα διόρθωσης ελέγχει ότι αυτό πράγματι συμβαίνει. Εντούτοις, το τέταρτο μήνυμα παρουσιάζει κάτι που μπορεί αρχικά να είναι εκπληκτικό. Η απάντηση από 10.4.7.100 στο 192.168.1.15 έφθασε στη διεπαφή Pooh S0 από Tigger. Θυμηθείτε ότι οι καταχωρήσεις διαδρομών στους άλλους δρομολογητές δεν έχουν αλλάξει από το αρχικό παράδειγμα. Αυτό το αποτέλεσμα μπορεί ή δεν μπορεί να επιδιωχτεί, αλλά επεξηγεί δύο χαρακτηριστικά των στατικών διαδρομών. Πρώτον, εάν η τοπολογία του internetwork αλλάξει, οι δρομολογητές που απαιτούνται να ξέρουν για εκείνες

τις αλλαγές πρέπει να μετατραπούν, και δεύτερον, οι στατικές διαδρομές μπορούν να χρησιμοποιηθούν για να δημιουργήσουν πολύ συγκεκριμένη συμπεριφορά δρομολόγησης.
Μια τελική παρατήρηση για αυτό το παράδειγμα είναι ότι τα πακέτα που δρομολογούνται από το Pooh στο υποδίκτυο 10.1.5.0 παίρνουν μια λιγότερο-από-βέλτιστη διαδρομή, από Pooh σε Eeyore σε Tigger αντί άμεσα από Pooh σε Tigger. Μια αποδοτικότερη διαμόρφωση είναι:

Pooh(config)# **ip route 192.168.1.192 255.255.255.224 192.168.1.66**
Pooh(config}# **ip route 10.0.0.0 255.0.0.0 192.168.1.34**
Pooh{config)# **ip route 10.1.0.0 255.255.0.0 192.168.1.66**
Pooh(config)# **ip route 10.4.7.25 255.255.255.255 192.168.1.66**

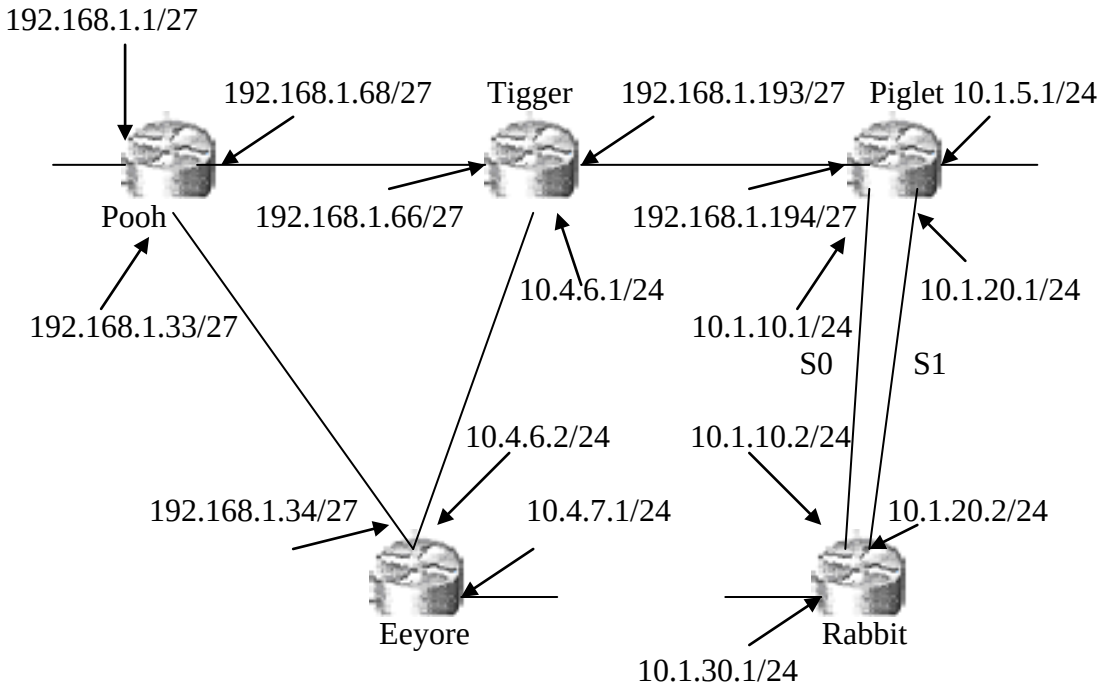
Η τρίτη είσοδος θα στείλει τώρα όλα τα πακέτα για το υποδίκτυο 10.1.5.0 άμεσα σε Tigger.

Case Study: Floating Static Routes

Αντίθετα από άλλες στατικές διαδρομές, μια floating στατική διαδρομή δεν εισάγεται μόνιμα στον πίνακα διαδρομών, εμφανίζεται μόνο κάτω από την ειδική περίσταση της αποτυχίας μιας περισσότερο-προτιμημένης διαδρομής. Στο σχήμα 3.7, ένας νέος δρομολογητής (Rabbit) συνδέεται με το Piglet μέσω αντίστοιχων Serial 0 διεπαφών τους, αλλά μια νέα σύνδεση έχει προστεθεί μεταξύ των δύο Serial 1 διεπαφών. Αυτή η δεύτερη σύνδεση έχει προστεθεί για πλεονασμό: Εάν η αρχική σύνδεση 10.1.10.0 αποτυγχάνει, οι floating στατικές διαδρομές θα κατευθύνουν την κυκλοφορία μέσα από την εφεδρική σύνδεση 10.1.20.0. Επιπλέον, η μάσκα στη διεπαφή Ethernet του Piglet έχει αλλάξει από 10.1.5.1/16 σε 10.1.5.1/24. Αυτή η αλλαγή επιτρέπει την ενιαία είσοδο διαδρομών σε Tigger

ip route 10.1.0.0 255.255.0.0 192.168.1.194

για να δείξει όχι μόνο 10.1.5.0 αλλά και όλα τα νέα υποδίκτυα που χρησιμοποιούνται σε συνδυασμό με το νέο δρομολογητή.



Σχήμα 3.7
Ένας νέος δρομολογητής έχει συνδεθεί στον Piglet. Δυο συνδέσεις χρησιμοποιούνται, μια για την κύρια σύνδεση και μια εφεδρική.

Για να δημιουργήσουν την floating στατική διαδρομή, οι καταχωρήσεις διαδρομών του Piglet είναι οι ακόλουθες:

ip route 192.168.1.0 255.255.255.0 192.168.1.193
ip route 10.4.0.0 255.255.0.0 192.168.1.193
ip route 10.1.30.0 255.255.255.0 10.1.10.1
ip route 10.1.30.0 255.255.255.0 10.1.20.1 50

Και - οι καταχωρήσεις διαδρομών του Rabbit είναι:

ip route 10.4.0.0 255.255.0.0 10.1.10.1
ip route 10.4.0.0 255.255.0.0 10.1.20.1 50
ip route 10.1.5.0 255.255.255.0 10.1.10.1
ip route 10.1.5.0 255.255.255.0 10.1.20.1 50
ip route 192.168.0.0 255.255.0.0 10.1.10.1
ip route 192.168.0.0 255.255.0.0 10.1.20.1 50

Δύο καταχωρήσεις στο Piglet δείχνουν στο δίκτυο 10.1.30.0 του Rabbit, το ένα διευκρινίζει μια διεύθυνση next-hop της διεπαφής του Rabbit S0, και η άλλη διευκρινίζει μια διεύθυνση next-hop της διεπαφής του Rabbit S1. Το Rabbit έχει παρόμοιες διπλές καταχωρήσεις για κάθε διαδρομή.

Παρατηρήστε ότι όλες οι στατικές διαδρομές που χρησιμοποιούν τα υποδίκτυα της 10.1.20.0 ακολουθούνται από 50. Αυτός ο αριθμός διευκρινίζει μια administrative distance, η οποία είναι ένα μέτρο προτίμησης, όταν οι διπλές πορείες στο ίδιο δίκτυο είναι γνωστές, ο δρομολογητής θα προτιμήσει την πορεία με το χαμηλότερο administrative distance. Στην αρχή αυτή η ιδέα ακούγεται σαν ένα metric, εντούτοις, ένα metric διευκρινίζει τη προτίμηση μιας διαδρομής, εκτιμώντας ότι μια administrative distance διευκρινίζει τη προτίμηση μέσα από τη διαδρομή όπου ανακαλύφθηκε. Παραδείγματος χάριν, οι στατικές διαδρομές που δείχνουν μια next-hop διεύθυνση έχουν μια administrative distance 1, και οι στατικές διαδρομές που παραπέμπουν μια διεπαφή εξόδων έχουν μια administrative distance 0. Εάν δύο στατικές διαδρομές δείξουν τον ίδιο προορισμό, αλλά κάποια παραπέμπει σε μια next-hop διεύθυνση και κάποια παραπέμπει σε μια διεπαφή εξόδων, τα τελευταία —με τη χαμηλότερη administrative distance —θα προτιμηθούν. Με την αύξηση των administrative distances των στατικών διαδρομών που διαπερνούν το υποδίκτυο 10.1.20.0 σε 50, γίνονται λιγότερο προτιμημένες από τις διαδρομές που διαπερνούν το υποδίκτυο 10.1.10.0.

Case Study: Load Sharing

Το πρόβλημα με τη διαμόρφωση που χρησιμοποιείται στο προηγούμενο τμήμα είναι ότι κάτω από τις κανονικές περιστάσεις η δεύτερη σύνδεση δεν χρησιμοποιείται ποτέ. Το εύρος ζώνης που είναι διαθέσιμο στη σύνδεση σπαταλιέται. Load sharing, επίσης γνωστό όπως load balancing, επιτρέπει στους δρομολογητές να εκμεταλλευθούν τις πολλαπλάσιες πορείες στον ίδιο προορισμό με την αποστολή των πακέτων σε όλες τις διαθέσιμες διαδρομές. Load sharing μπορεί να έχει ίσο κόστος ή άνισο κόστος, όπου το κόστος είναι ένας γενικός όρος που αναφέρεται σε οποιοδήποτε metric (ενδεχομένως) συνδέεται με τη διαδρομή.

- Το ίσο-κόστος load sharing διανέμει την κυκλοφορία εξίσου μεταξύ των πολλαπλάσιων πορειών με τα ίσα metric.

- Το άνισο-κόστος load sharing διανέμει τα πακέτα μεταξύ των πολλαπλάσιων πορειών με διαφορετικά metrics. Η κυκλοφορία διανέμεται αντιστρόφως ανάλογα προς το κόστος των διαδρομών. Δηλαδή στις πορείες με το χαμηλότερο κόστος ορίζεται περισσότερη κυκλοφορία, και στις πορείες με το υψηλότερο κόστος ορίζεται λιγότερη κυκλοφορία.

Μερικά πρωτόκολλα δρομολόγησης υποστηρίζουν και ίσο-κόστος και άνισο-κόστος load sharing, εκτιμώντας ότι άλλοι υποστηρίζουν μόνο το ίσο κόστος. Οι στατικές διαδρομές, που δεν έχουν κανέναν metric, υποστηρίζουν μόνο ίσο-κόστος load sharing. Για να διαμορφώσουν τις παράλληλες συνδέσεις στο σχήμα 3.7 για load sharing χρησιμοποιώντας τις στατικές διαδρομές, οι καταχωρήσεις διαδρομών του Piglet είναι:

ip route 192.168.1.0 255.255.255.0 192.168.1.193
ip route 10.4.0.0 255.255.0.0 192.168.1.193
ip route 10.1.30.0 255.255.255.0 10.1.10.1
ip route 10.1.30.0 255.255.255.0 10.1.20.1

Οι καταχωρήσεις διαδρομών του Rabbit είναι:

ip route 10.4.0.0 255.255.0.0 10.1.10.1
ip route 10.4.0.0 255.255.0.0 10.1.20.1
ip route 10.1.5.0 255.255.255.0 10.1.10.1
ip route 10.1,5.0 255.255.255.0 10.1.20.1
ip route 192.168.0.0 255.255.0.0 10.1.10.1
ip route 192.168.0.0 255.255.0.0 10.1.20.1

Αυτές οι καταχωρήσεις χρησιμοποιήθηκαν επίσης στο προηγούμενο τμήμα των floating στατικών διαδρομών, μόνο που οι δυο συνδέσεις τώρα χρησιμοποιούν την προεπιλεγμένη administrative distance 1.
Load sharing είναι επίσης είτε ανά προορισμό είτε ανά πακέτο.

Ανά προορισμό Load Sharing and Fast Switching

Ανά φορτίο προορισμού η εξισορρόπηση διανέμει το φορτίο σύμφωνα με τη διεύθυνση προορισμού. Λαμβάνοντας υπόψη δύο πορείες στο ίδιο δίκτυο, όλα τα πακέτα για έναν προορισμό στο δίκτυο μπορούν να ταξιδέψουν πέρα από την πρώτη πορεία, όλα τα πακέτα για έναν δεύτερο προορισμό στο ίδιο δίκτυο μπορεί να ταξιδέψει πέρα από τη δεύτερη πορεία, όλα τα πακέτα για έναν τρίτο προορισμό μπορούν πάλι να σταλθούν πέρα από την πρώτη πορεία, και ου το καθ' εξής. Η γρήγορη μετατροπή λειτουργεί ως εξής: Όταν ένας δρομολογητής μεταστρέφει το πρώτο πακέτο σε έναν ιδιαίτερο προορισμό, ένα lookup στον πίνακα διαδρομών εκτελείται και μια διεπαφή εξόδων επιλέγεται. Οι απαραίτητες πληροφορίες της σύνδεσης δεδομένων για να πλαισιώσουν το πακέτο για την επιλεγμένη διεπαφή ανακτώνται (από τη arp cache, παραδείγματος χάριν), και το πακέτο διαβιβάζεται. Η ανακτημένη διαδρομή και οι πληροφορίες της σύνδεσης δεδομένων έπειτα εισάγονται σε μια γρήγορης μετατροπής cache, και καθώς τα επόμενα πακέτα στον ίδιο προορισμό εισάγονται στον δρομολογητή, οι πληροφορίες στη γρήγορη cache επιτρέπουν στο δρομολογητή να μεταστρέψει αμέσως το πακέτο χωρίς να εκτελέσει ένα άλλο lookup στον πίνακα διαδρομών και Arp cache. Ενώ ο χρόνος αλλαγής και η χρησιμοποίηση επεξεργαστών μειώνονται, η γρήγορη μετατροπή σημαίνει ότι όλα τα πακέτα σε έναν συγκεκριμένο προορισμό καθοδηγούνται έξω από την ίδια διεπαφή. Όταν υπάρχει ένα πακέτο που απευθύνεται σε έναν διαφορετικό οικοδεσπότη στο ίδιο δίκτυο μπαίνει στο δρομολογητή και σε μια εναλλακτική διαδρομή, ο δρομολογητής μπορεί να στείλει όλα τα πακέτα για εκείνο τον προορισμό στην εναλλακτική διαδρομή. Επομένως, το καλύτερο που μπορεί να κάνει ο δρομολογητής είναι να ισορροπήσει την κυκλοφορία στην ανά προορισμού βάση.

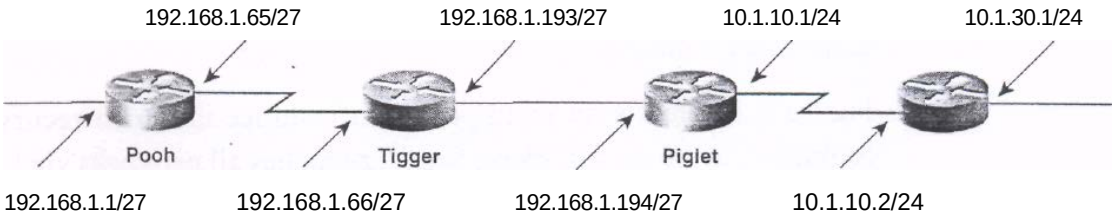
Ανά πακέτο Load Sharing and Process Switching

Ανά πακέτο load sharing σημαίνει ότι ένα πακέτο στέλνεται σε έναν προορισμό μέσω μιας σύνδεσης, το επόμενο πακέτο στέλνεται στον ίδιο προορισμό μέσα από την επόμενη σύνδεση και ου το καθ' εξής, λαμβάνοντας υπόψη τις πορείες ίσου-κόστους. Εάν οι πορείες είναι άνισου κόστους, η load balancing μπορεί να είναι ένα πακέτο πέρα από τη σύνδεση υψηλού-κόστους για κάθε τρία πακέτα πέρα από τη χαμηλότερου κόστους σύνδεση, ή κάποια άλλη αναλογία στηριζόμενη επάνω στην αναλογία των δαπανών. Οι δρομολογητές Cisco θα κάνουν ανά πακέτο load balancing όταν είναι process switching. Το process switching απλά σημαίνει ότι για κάθε πακέτο, ο δρομολογητής εκτελεί ένα lookup στον πίνακα διαδρομών, επιλέγει μια διεπαφή, και ανατρέχει έπειτα στις πληροφορίες συνδέσεων δεδομένων. Επειδή κάθε απόφαση δρομολόγησης είναι ανεξάρτητη για κάθε πακέτο, όλα τα πακέτα στον ίδιο προορισμό δεν αναγκάζονται να χρησιμοποιήσουν την ίδια διεπαφή. Για να ενεργοποιήσετε το process switching σε μια διεπαφή, χρησιμοποιήστε την εντολή no ip route-cache.

Case Study: Recursive Table Lookups

Όλες οι καταχωρήσεις διαδρομών δεν πρέπει απαραιτήτως να δείξουν το δρομολογητή next-hop. Το σχήμα 3.8 παρουσιάζει την απλουστευμένη έκδοση του internetwork του σχήματος 3.7. Σε αυτό το internetwork, το Pooh διαμορφώνεται με:

ip route 10.1.30.0 255.255.255.0 10.1.10.2
ip route 10.1.10.0 255.255.255.0 192.168.1.194
ip route 192.168.1.192 255.255.255.224 192.168.1.66

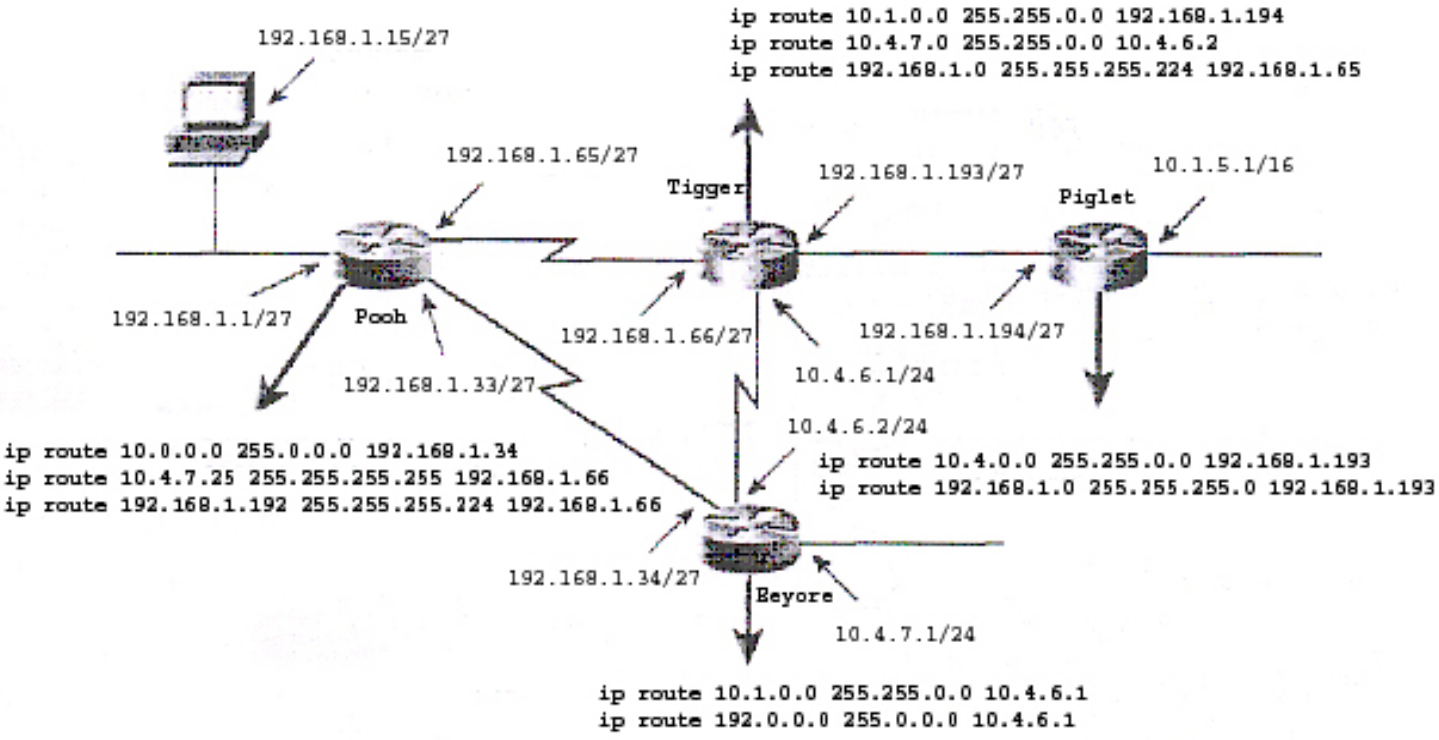


Σχήμα 3.8
Για να φτάσει το δίκτυο 10.1.30.0, ο Pooh πρέπει να εκτελέσει τρία lookups στους πίνακες των δρομολογητών.

Εάν το Pooh πρέπει να στείλει ένα πακέτο στον οικοδεσπότη της 10.1.30.25, θα εξετάσει τον πίνακα διαδρομών του και διαπιστώνει ότι το υποδίκτυο είναι εφικτό μέσω 10.1.10.2. Επειδή αυτή η διεύθυνση δεν είναι σε ένα άμεσα συνδεδεμένο δίκτυο, το Pooh πρέπει πάλι να συμβουλευθεί τον πίνακα για να διαπιστώσει ότι το δίκτυο 10.1.10.0 είναι εφικτό μέσω 192.168.1.194. Αυτό το υποδίκτυο δεν είναι επίσης άμεσα συνδεδεμένο και έτσι ένα τρίτο lookup στον πίνακα απαιτείται. Το Pooh θα διαπιστώσει ότι το 192.168.1.192 είναι εφικτό μέσω 192.168.1.66, το οποίο είναι σε ένα άμεσα συνδεδεμένο υποδίκτυο. Το πακέτο μπορεί τώρα να διαβιβαστεί. Επειδή κάθε lookup του πίνακα κοστίζει σε χρόνο επεξεργασίας, κάτω από κανονικές συνθήκες αναγκάζεται ο δρομολογητής να εκτελέσει πολλαπλά κάτι που είναι μια φτωχή απόφαση σχεδιασμού. Η γρήγορη μετατροπή μειώνει σημαντικά αυτά τα δυσμενή αποτελέσματα με τον περιορισμό των επαναλαμβανόμενων lookups στο πρώτο πακέτο σε κάθε προορισμό, αλλά μια αιτιολόγηση πρέπει ακόμα να προσδιοριστεί πριν χρησιμοποιεί ένα τέτοιο σχέδιο.

Case Study: Tracing a Failed Route

Το σχήμα 3.9 παρουσιάζει ένα προηγούμενο διαμορφωμένο internetwork, με τις σχετικές στατικές διαδρομές κάθε δρομολογητή. Ένα πρόβλημα έχει ανακαλυφθεί. Οι συσκευές στο υποδίκτυο 192.168.1.0/27, που συνδέεται με τη διεπαφή Ethernet Pooh, μπορούν να επικοινωνήσουν με τις συσκευές στο υποδίκτυο 10.1.0.0/16 μια χαρά. Εντούτοις, όταν στέλνεται ένα ping από το ίδιο το Pooh στο υποδίκτυο 10.1.0.0/16, το ping αποτυγχάνει (σχήμα 3.10). Αυτό φαίνεται παράξενο. Εάν τα πακέτα που καθοδηγούνται από Pooh φθάνουν επιτυχώς στους προορισμούς τους, γιατί πακέτα που δημιουργούνται από τον ίδιο δρομολογητή αποτυγχάνουν;



Σχήμα 3.9
Τα πακέτα από το υποδίκτυο 192.168.1.0/27 στο υποδίκτυο 10.1.0.0/16 δρομολογούνται σωστά, αλλά ο Pooh δεν μπορεί να κάνει ping σε καμία συσκευή στο 10.1.0.0/16

Η εξέταση αυτού του προβλήματος απαιτεί την ανίχνευση της διαδρομής του ping. Κατ' αρχάς, ο πίνακας διαδρομών Pooh εξετάζεται (σχήμα 3.11). Η διεύθυνση προορισμού των 10.1.5.1 ταιριάζει με την είσοδο διαδρομών για 10.0.0.0/8, που (σύμφωνα με τον πίνακα) επιτυγχάνεται μέσω του next-hop 192.168.1.34 —μια από τις διεπαφές Eeyore.

Έπειτα ο πίνακας διαδρομών για Eeyore πρέπει να εξεταστεί (σχήμα 3.12). Η διεύθυνση προορισμού 10.1.5.1 ταιριάζει με την είσοδο 10.1.0.0/16, με μια διεύθυνση next-hop 10.4.6.1. Αυτή η διεύθυνση είναι μια από τις διεπαφές Tigger.

```
C:\WINDOWS>ping 10.1.5.1
Pinging 10.1.5.1 with 32 bytes of data:

Reply from 10.1.5.1:   bytes=32  time=22ms  TTL=253
Reply from 10.1.5.1:   bytes=32  time=22ms  TTL=253
Reply from 10.1.5.1:   bytes=32  time=22ms  TTL=253
Reply from 10.1.5.1:   bytes=32  time=22ms  TTL=253
```

```
Pooh#ping 10.1.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoechoes to 10.1.5.1, timeout is 2 seconds:
….
Success rate is 0 percent (0/5)
Pooh#
```

Σχήμα 3.10
Μια συσκευή στο υποδίκτυο 192.168.1.0/27 κάνει επιτυχημένο ping στη διεπαφή του Piglet, αλλά το ping από Pooh αποτυγχάνει.

```
Pooh#show ip route
Codes C- connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP
D – EIGRP, EX – EIGRP external, o – OSPF, IA – OSPF inter area
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
I – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate default
Gateway of last resort is not set
   10.0.0.0 is variably subnetted, 2 subnets, 2 masks
S     10.0.0.0 255.0.0.0 [1/0] via 192.168.1.34
S     10.4.7.25 255.255.255.255 [1/0] via 192.168.1.66
   192.168.1.0 255.255.255.224. is subnetted, 4 subnets
C     192.168.1.64 is directly connected, Serial0
C     192.168.1.32 is directly connected, Serial1
C     192.168.1.0 is directly connected, Ethernet0
C     192.168.1.192 [1/0] via 192.168.1.66
Pooh#
```

Σχήμα 3.11
Ένα πακέτο με διεύθυνση προορισμού 10.1.5.1 ταιριάζει για 10.0.0.0/8 και θα σταλεί με τον δρομολογητή next-hop στο 192.168.1.34.

Το σχήμα 3.13 παρουσιάζει τον πίνακα διαδρομών Tigger. Η διεύθυνση προορισμού ταιριάζει με την είσοδο 10.1.0.0/16 και θα διαβιβαστεί σε 192.168.1.194, η οποία είναι στο Piglet.

```
Eeyore#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP
       D - EIGRP, EX - EIGRP external, 0 - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,* - candidate default
Gateway of last resort is not set
10.0.0.0 is variably subnetted, 3 subnets, 2 masks
C        10.4.6.0 255.255.255.0 is directly connected, Serial1
C        10.4.7.0 255.255.255.0 is directly connected, Ethernet0
S         10.1.0.0 255.255.0.3 [1/0] via 10.4.5.1
192.168.1.0 255.255.255.224 is subnetted, 1 subnets
C        192.168.1.32 is directly connected, Serial0
S         192.0.0.0 255.0.0.0 [1/0] via 10.4.6.1
Eeyore#
```

Σχήμα 3.12
10.1.5.1 ταιριάζει με την είσοδό για 10.1.0.0/16 και θα διαβιβαστεί στο 10.4.6.1.

```
Tigger#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        E1 - OSPF external type 1 , E2 - OSPF external type 2, E - EGP
        I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,* - candidate default
Gateway of last resort is not set
10.0.0.0 is variably subnetted, 3 subnets, 2 masks
C        10.4.6.0 255.255.255.0 is directly connected, Serial1
S           10.4.7.0 255.255.255.0 [1/0] via 10.4.6.2
S         10.1.0.0 255.255.0.0 [1/0] via 192.168.1.194
      192.168.1.0 255.255.255.224 is subnetted, 3 subnets
C        192.168.1.64 is directly connected, Serial0
S         192.168.1.0 [1/0] via 192.168.1.65
C        192.168.1.192 is directly connected, Ethernet0
Tigger#
```

Σχήμα 3.13
10.1.5.1 ταιριάζει με την είσοδο για 10.1.0.0/16 και θα διαβιβαστεί στο 192.1658.1.194.

Ο πίνακας διαδρομών του Piglet (σχήμα 3.14) αποκαλύπτει ότι το δίκτυο, 10.1.0.0, συνδέεται άμεσα. Με άλλα λόγια, το πακέτο έχει φθάσει. Η διεύθυνση 10.1.5.1 είναι η διεπαφή του Piglet σε εκείνο το δίκτυο. Επειδή η πορεία στη διεύθυνση ελέγχθηκε μόλις και είναι καλή, μπορούμε να υποθέσουμε ότι τα πακέτα ICMP από Pooh έχουν φθάσει στον προορισμό.

```
Piglet#show ip route
Codes:  C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP
        D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
        E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
        I – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * - candidate default

Gateway of last resort is not set
```

```
     10.0.0.0 255.255.0.0 is subnetted, 2 subnets
C       10.1.0.0 is directly connected, Ethernet1
S       10.4.0.0 [1/0] via 192.168.1.193
     192.168.1.0 is variably subnneted, 2 subnets, 2 masks
S       192.168.1.0 255.255.255.0 [1/0] via 192.168.1.193
C       192.168.1.192 255.255.255.224 is directly connected, Ethernet0
Piglet#
```

Σχήμα 3.14
Το δίκτυο προορισμού, 10.1.0.0, είναι απευθείας συνδεδεμένο στο Piglet.

Το επόμενο βήμα είναι να ανιχνευθεί η πορεία των αποκριμένων πακέτων απάντησης ICMP. Για να ανιχνευθεί αυτή η πορεία, πρέπει να ξέρετε τη διεύθυνση προέλευσης του πακέτου— αυτή η διεύθυνση θα είναι η διεύθυνση προορισμού του πακέτου απάντησης. Η διεύθυνση προέλευσης ενός πακέτου που προέρχεται από έναν δρομολογητή είναι η διεύθυνση της διεπαφής από την οποία το πακέτο διαβιβάστηκε. Σε αυτό το παράδειγμα, το Pooh διαβίβασε αρχικά το πακέτο στο 192.168.1.34. Το σχήμα 3.9 δείχνει ότι η διεύθυνση προέλευσης αυτού του πακέτου είναι 192.168.1.33. Έτσι αυτή η διεύθυνση είναι η διεύθυνση προορισμού στην οποία το Piglet θα στείλει την απάντηση. Αναφερόμενος πάλι στον πίνακα διαδρομών του Piglet στο σχήμα 3.14, 192.168.1.33 θα ταιριάξει με την είσοδο για 192.168.1.0/24 και θα διαβιβαστεί σε 192.168.1.193, η οποία είναι άλλη μια διεπαφή του Tigger. Μια αναθεώρηση του πίνακα διαδρομών του Tigger στο σχήμα 3.13 αρχικά προτείνει ότι υπάρχει μια είσοδος για 192.168.1.0. Συγκρίνετε τις καταχωρήσεις στον πίνακα διαδρομών του Tigger για τα 10.0.0.0 υποδίκτυα με εκείνες των 192.168.1.0 υποδικτύων. Ο τίτλος για τα πρώτα λέει ότι 10.0.0.0 είναι μεταβλητά: με άλλα λόγια, η στατική διαδρομή του Tigger στο υποδίκτυο 10.4.7.0 χρησιμοποιεί μια μάσκα 24-bits, και η στατική διαδρομή στο υποδίκτυο 10.1.0.0 χρησιμοποιεί μια 16-bits μάσκα. Ο πίνακας καταγράφει τη σωστή μάσκα σε κάθε υποδίκτυο.

Ο τίτλος για 192.168.1.0 είναι διαφορετικός. Αυτός ο τίτλος δηλώνει ότι το Tigger ξέρει για τρία υποδίκτυα του 192.168.1.0 και ότι όλα έχουν μια μάσκα 255.255.255.224. Αυτή η μάσκα θα χρησιμοποιηθεί στη διεύθυνση προορισμού 192.168.1.33 για να παραγάγει ένα δίκτυο προορισμού 192.168.1.32/27. Ο πίνακας διαδρομών έχει καταχωρήσεις για 192.168.1.64/27, 192.168.1.0/27, και 192.168.1.192/27. Δεν υπάρχει καμία

είσοδος για 192.168.1.32/27, έτσι ο δρομολογητής δεν ξέρει πώς να φθάσει σε αυτό το υποδίκτυο. Το πρόβλημα, έπειτα, είναι ότι το πακέτο απάντησης ICMP πέφτει στο Tigger. Μια λύση είναι να δημιουργηθεί μια άλλη στατική είσοδος διαδρομών για το δίκτυο 192.168.1.32, με μια μάσκα 255.255.255.224 και δείχνοντας σε ένα next-hop είτε 192.168.1.65 είτε 10.4.6.2. Μια άλλη λύση θα ήταν να αλλαχτεί η μάσκα στην υπάρχουσα στατική είσοδο διαδρομών για 192.168.1.0 από 255.255.255.224 σε 255.255.255.0. Το ήθος αυτής της ιστορίας είναι ότι όταν επισημαίνετε μια διαδρομή, πρέπει να εξετάσετε την πλήρη διαδικασία επικοινωνίας. Ελέγξτε όχι μόνο ότι η πορεία σε έναν προορισμό είναι καλή αλλά και ότι η επιστροφή είναι καλή.

ΚΕΦΑΛΑΙΟ 4
ΔΥΝΑΜΙΚΗ ΔΡΟΜΟΛΟΓΗΣΗ

Εισαγωγή

Το τελευταίο κεφάλαιο εξήγησε τι ένας δρομολογητής πρέπει να ξέρει για να μεταστρέφει σωστά τα πακέτα στους αντίστοιχους προορισμούς τους και πώς εκείνες οι πληροφορίες τίθενται στον πίνακα διαδρομών με το χέρι. Αυτό το κεφάλαιο επιδεικνύει πώς οι δρομολογητές μπορούν να ανακαλύψουν αυτές τις πληροφορίες αυτόματα και να μοιραστούν εκείνες τις πληροφορίες με άλλους δρομολογητές μέσω των δυναμικών πρωτοκόλλων δρομολόγησης. Ένα πρωτόκολλο δρομολόγησης είναι η γλώσσα που ένας δρομολογητής μιλά με άλλους δρομολογητές προκειμένου να μοιραστούν οι πληροφορίες, για τη προσπελασιμότητα και τη κατάσταση των δικτύων. Τα δυναμικά πρωτόκολλα δρομολόγησης όχι μόνο εκτελούν αυτά τα προσδιοριστικά μονοπάτια και τις ενημερώσεις του πίνακα διαδρομών αλλά επίσης καθορίζουν την επόμενη-καλύτερη πορεία εάν η καλύτερη πορεία σε έναν προορισμό γίνεται ακατάλληλη προς χρήση. Η ικανότητα να αντισταθμιστούν οι αλλαγές τοπολογίας είναι τα σημαντικότερα πλεονεκτήματα που προσφέρει η δυναμική δρομολόγηση πέρα από τη στατική δρομολόγηση. Προφανώς για να συμβούν οι επικοινωνίες, οι πληροφοριοδότες πρέπει να μιλήσουν την ίδια γλώσσα. Υπάρχουν οκτώ σημαντικά πρωτόκολλα δρομολόγησης IP από τα οποία έχει να επιλέξει, εάν ένας δρομολογητής μιλά RIP και άλλος μιλά OSPF, δεν μπορούν να μοιραστούν τις πληροφορίες δρομολόγησης επειδή δεν μιλούν την ίδια γλώσσα.

ΒΑΣΙΚΑ ΠΡΩΤΟΚΟΛΛΟΥ ΔΡΟΜΟΛΟΓΗΣΗΣ

Όλα τα δυναμικά πρωτόκολλα δρομολόγησης χτίζονται γύρω από έναν αλγόριθμο. Γενικά, ένας *αλγόριθμος* είναι μια βαθμιαία διαδικασία για την επίλυση ενός προβλήματος. Ένας αλγόριθμος δρομολόγησης πρέπει, τουλάχιστον, να διευκρινίσει τα ακόλουθα:

- Μια διαδικασία για τις πληροφορίες προσπελασιμότητας για δίκτυα σε άλλους δρομολογητές
- Μια διαδικασία για τις πληροφορίες προσπελασιμότητας από άλλους

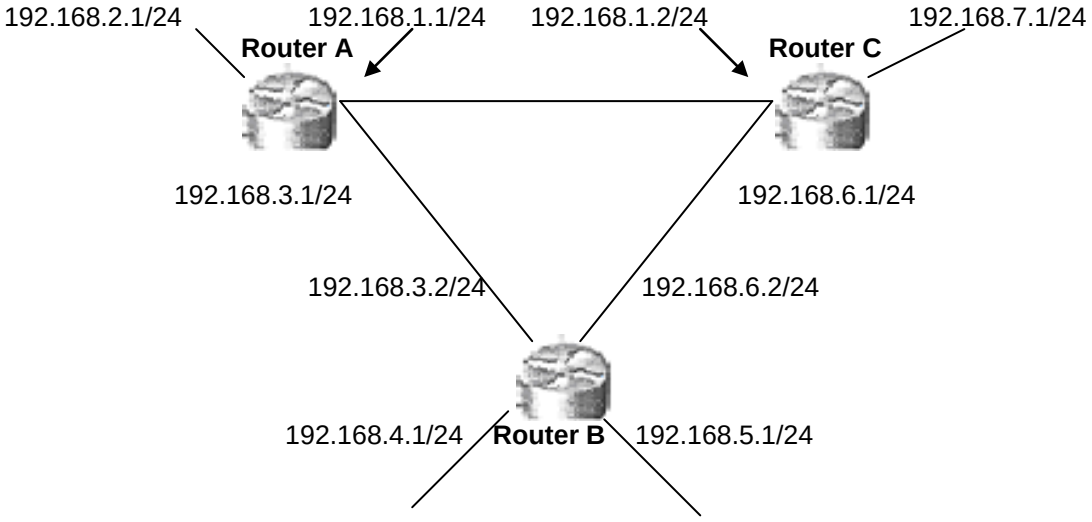
δρομολογητές

- Μια διαδικασία για τις βέλτιστες διαδρομές καθορισμού βασισμένες πληροφορίες προσπελασιμότητας που έχει και για να καταγράψει αυτές τις πληροφορίες μέσα σε έναν πίνακα διαδρομών
- Μια διαδικασία για αντίδραση, αποζημίωση και γνωστοποίηση των αλλαγών τοπολογίας σε ένα internetwork.

Μερικά ζητήματα κοινά για οποιοδήποτε πρωτόκολλο δρομολόγησης είναι καθορισμός πορειών, metrics, σύγκλιση, και load balancing.

Καθορισμός πορειών

Όλα τα δίκτυα μέσα σε ένα internetwork πρέπει να συνδεθούν με έναν δρομολογητή, και οπουδήποτε ένας δρομολογητής έχει μια διεπαφή στο δίκτυο αυτή η διεπαφή πρέπει να έχει μια διεύθυνση στο δίκτυο. Αυτή η διεύθυνση είναι το αρχικό σημείο για τις πληροφορίες προσπελασιμότητας. Το σχήμα 4.1 παρουσιάζει ένα απλό τριών-δρομολογητών internetwork. Ο δρομολογητής A ξέρει για τα δίκτυα 192.168.1.0, 192.168.2.0 και 192.168.3.0 επειδή έχει τις διεπαφές σε εκείνα τα δίκτυα με τις αντίστοιχες διευθύνσεις και τις κατάλληλες μάσκες διευθύνσεων. Επιπλέον, ο δρομολογητής B ξέρει για 192.168.3.0, 192.168.4.0, 192.168.5.0 και 192.186.6.0, ο δρομολογητής C ξέρει για 192.168.6.0, 192.168.7.0 και 198.168.1.0. Κάθε διεπαφή εφαρμόζει τη σύνδεση δεδομένων και τα φυσικά πρωτόκολλα του δικτύου με το οποίο είναι συνδεμένο, έτσι ο δρομολογητής ξέρει επίσης την κατάσταση του δικτύου (πάνω ή κάτω).



Σχήμα 4.1
κάθε δρομολογητής ξέρει για τα απευθείας συνδεδεμένα σε αυτόν δίκτυα από τις καθορισμένες διευθύνσεις και μάσκες.

Με την πρώτη ματιά, η διαδικασία ανταλλαγής πληροφοριών φαίνεται απλή. Δείτε το δρομολογητή Α:

1. Ο δρομολογητής Α εξετάζει τις διευθύνσεις IP και τις σχετικές μάσκες του και συνάγει ότι είναι συνδεμένο με τα δίκτυα 192.168.1.0, 192.186.2.0, και 192.168.3.0.
2. Ο δρομολογητής Α εισάγει αυτά τα δίκτυα στον πίνακα διαδρομών του, μαζί με κάποιο είδος σημαίας που δείχνει ότι τα δίκτυα συνδέονται άμεσα.
3. Ο δρομολογητής Α τοποθετεί τις πληροφορίες σε ένα πακέτο: Τα "άμεσα συνδεδεμένα δίκτυά μου είναι 192.168.1.0. 192.186.2.0,και 192.168.3.0."
4. Ο δρομολογητής Α διαβιβάζει τα αντίγραφα από αυτά τα πακέτα πληροφοριών διαδρομής, ή *αναπροσαρμογές δρομολόγησης,* στους δρομολογητές Β και C.
5. Οι δρομολογητές Β και C, που έχουν εκτελέσει τα ίδια βήματα, έχουν στείλει τις αναπροσαρμογές με τα άμεσα συνδεδεμένα δίκτυά τους στο Α. Ο δρομολογητής Α εισάγει τις λαμβανόμενες πληροφορίες στον πίνακα διαδρομών του, μαζί με τη διεύθυνση προέλευσης του δρομολογητή που έστειλε το πακέτο αναπροσαρμογών. Ο δρομολογητής Α ξέρει τώρα για όλα τα δίκτυα, και ξέρει τις διευθύνσεις των δρομολογητών με τους οποίους είναι συνδεμένοι.

Αυτή η διαδικασία φαίνεται αρκετά απλή. Έτσι, γιατί τα πρωτόκολλα δρομολόγησης είναι πιο περίπλοκα από αυτό; Εξετάστε πάλι το σχήμα 4.1.

- Τι θα έπρεπε να έκανε ο δρομολογητής Α με τις αναπροσαρμογές από το Β και το C αφότου έχει καταγράψει τις πληροφορίες στον πίνακα διαδρομών; Έπρεπε, παραδείγματος χάριν, να περάσει το

πακέτο πληροφοριών δρομολόγησης του B στο C και το πακέτο του C στο B;

- Εάν ο δρομολογητής A δεν διαβιβάζει τις αναπροσαρμογές, η ανταλλαγή πληροφοριών μπορεί να μην είναι πλήρης. Παραδείγματος χάριν, εάν η σύνδεση μεταξύ του B και του C δεν υπάρχει, αυτοί οι δύο δρομολογητές δεν θα γνωρίζουν ο ένας για τα δίκτυα του άλλου. Ο δρομολογητής A πρέπει να διαβιβάσει τις πληροφορίες αναπροσαρμογών, αλλά αυτό το βήμα ανοίγει ολόκληρο ένα νέο σύνολο προβλημάτων.
- Εάν ο δρομολογητής A ακούσει για το δίκτυο 192.168.4.0 και από τους δύο δρομολογητές B και C, ποιος δρομολογητής πρέπει να χρησιμοποιηθεί για να φθάσει σε εκείνο το δίκτυο; Είναι και οι δύο έγκυροι; Ποια μια είναι η καλύτερη πορεία;
- Ποιος μηχανισμός θα χρησιμοποιηθεί για να εξασφαλίσει ότι όλοι οι δρομολογητές λαμβάνουν όλες τις πληροφορίες δρομολόγησης ενώ αποτρέπουν την αναπροσαρμογή των πακέτων από το να γυρνούν αδιάκοπα μέσα στο internetwork;
- Οι δρομολογητές μοιράζονται ορισμένα άμεσα συνδεδεμένα δίκτυα (192.168.1.0, 192.168.3.0, και 192.168.6.0). Πρέπει οι δρομολογητές να διαφημίσουν αυτά τα δίκτυα;

Αυτές οι ερωτήσεις είναι σχεδόν τόσο απλοϊκές όσο η προηγούμενη προκαταρκτική εξήγηση της δρομολόγησης των πρωτοκόλλων, αλλά πρέπει να σας δώσουν μια αίσθηση για μερικά από τα ζητήματα που συμβάλλουν στην πολυπλοκότητα των πρωτοκόλλων.

Metrics

Όταν υπάρχουν πολλαπλάσιες διαδρομές στον ίδιο προορισμό, ένας δρομολογητής πρέπει να έχει έναν μηχανισμό για την καλύτερη πορεία. Ένα *metric* είναι μια μεταβλητή που ορίζεται στις διαδρομές ως μέσο για να τους ταξινομήσει από το καλύτερο στο χειρότερο ή από το προτιμημένο στο ελάχιστα προτιμημένο. Εξετάστε το ακόλουθο παράδειγμα, γιατί τα metrics απαιτούνται. Υποθέτοντας ότι η ανταλλαγή πληροφοριών έχει εμφανιστεί

κατάλληλα στο internetwork του σχήματος 4.1, ο δρομολογητής Α έχει έναν πίνακα διαδρομών που μοιάζει με τον πίνακα 4.1.

Πίνακας 4.1
Ένας στοιχειώδης πίνακας δρομολόγησης για τον δρομολογητή Α της εικόνας 3.1.

Network	**Next-Hop Router**
192.168.1.0	Direct connected
192.168.2.0	Direct connected
192.168.3.0	Direct connected
192.168.4.0	B, C
192.168.5.0	B, C
192.168.6.0	B, C
192.168.7.0	B, C

Αυτός ο πίνακας διαδρομών λέει ότι τα πρώτα τρία δίκτυα συνδέονται άμεσα και ότι καμία δρομολόγηση δεν απαιτείται από το δρομολογητή Α για να φθάσει σε αυτά, το οποίο είναι σωστό. Τα τελευταία τέσσερα δίκτυα, σύμφωνα με αυτόν τον πίνακα, μπορούν να επιτευχθούν μέσω του δρομολογητή Β ή του δρομολογητή C. Αυτή η πληροφορία είναι επίσης σωστή. Αλλά εάν το δίκτυο 192.168.7.0 μπορεί να επιτευχθεί μέσω είτε του δρομολογητή Β είτε του δρομολογητή C, ποια πορεία είναι η προτιμητέα; Τα metrics απαιτούνται για να ταξινομήσουν τις εναλλακτικές λύσεις. Τα διαφορετικά πρωτόκολλα δρομολόγησης χρησιμοποιούν διαφορετικά, και μερικές φορές πολλαπλάσια, metrics. Παραδείγματος χάριν, το RIP καθορίζει τη "καλύτερη" διαδρομή ως αυτήν με το λιγότερο αριθμό hops δρομολογητών, το IGRP καθορίζει τη "καλύτερη" διαδρομή βασισμένη σε έναν συνδυασμό του χαμηλότερου εύρους ζώνης κατά μήκος της διαδρομής και τη συνολική καθυστέρηση της διαδρομής. Τα επόμενα τμήματα παρέχουν τους βασικούς ορισμούς αυτών και άλλων συνήθως χρησιμοποιημένων metrics.

Hop Count

Ένα metric μέτρησης βημάτων απλά μετράει τα βήματα του δρομολογητή. Παραδείγματος χάριν, από το δρομολογητή A είναι 1 βήμα για το δίκτυο 192.168.5.0 εάν τα πακέτα στέλνονται στη διεπαφή 192.168.3.1 (μέσω δρομολογητή B) και 2 βήματα εάν τα πακέτα στέλνονται στο 192.168.1.1 (μέσω των δρομολογητών C και B). Υποθέτοντας hop count είναι το μόνο εφαρμοσμένο metric, η καλύτερη διαδρομή είναι αυτή με τα λιγότερα βήματα, σε αυτήν την περίπτωση, A-B. Αλλά είναι η σύνδεση A-B πραγματικά η καλύτερη πορεία; Εάν η σύνδεση A-B είναι DS-0 σύνδεση και οι συνδέσεις C-B είναι T-l συνδέσεις, η διαδρομή 2 βημάτων μπορεί πραγματικά να είναι καλύτερη, επειδή το εύρος ζώνης διαδραματίζει έναν ρόλο στο πόσο αποτελεσματικά η κυκλοφορία ταξιδεύει μέσα στο δίκτυο.

Εύρος ζώνης

Ένα εύρος ζώνης metric θα επέλεγε μια πορεία υψηλού-εύρους ζώνης πέρα από μια σύνδεση χαμηλού-εύρους ζώνης. Εντούτοις, το εύρος ζώνης από μόνο του μπορεί ακόμα να μην είναι ένα καλό metric. Και τι εάν το ένα ή και οι δυο από τις T-1 συνδέσεις φορτώνεται βαριά με άλλη κυκλοφορία και τη σύνδεση 56K φορτώνεται ελαφριά; Ή τι εάν η σύνδεση υψηλού-εύρους ζώνης έχει επίσης μια υψηλότερη – καθυστέρηση;

Load

Αυτό το metric απεικονίζει το ποσό κυκλοφορίας που χρησιμοποιεί η σύνδεση κατά μήκος της πορείας. Η καλύτερη πορεία είναι αυτή με το χαμηλότερο φορτίο.

Αντίθετα από την αρίθμηση βημάτων και το εύρος ζώνης, το φορτίο σε μια διαδρομή αλλάζει, και επομένως το metric θα αλλάξει. Προσοχή πρέπει να ληφθεί εδώ. Εάν το metric αλλάζει πολύ συχνά, route flapping— η συχνή αλλαγή των προτιμώμενων πορειών— μπορεί να εμφανιστεί. Τα route flaps μπορούν να έχουν δυσμενή αποτελέσματα στην ΚΜΕ του

δρομολογητή, το εύρος ζώνης των συνδέσεων δεδομένων, και τη γενική σταθερότητα του δικτύου.

Καθυστέρηση

Η καθυστέρηση είναι ένα μέτρο χρόνου, που χρειάζεται ένα πακέτο για να διασχίσει μια διαδρομή. Ένα πρωτόκολλο δρομολόγησης που χρησιμοποιεί την καθυστέρηση ως metric θα επέλεγε την πορεία με τη λιγότερη καθυστέρηση ως καλύτερη πορεία. Μπορούν να υπάρξουν πολλοί τρόποι να μετρηθεί η καθυστέρηση. Η καθυστέρηση μπορεί να λάβει υπόψη όχι μόνο την καθυστέρηση των συνδέσεων κατά μήκος της διαδρομής αλλά και τέτοιους παράγοντες όπως τη λανθάνουσα κατάσταση δρομολογητών και την καθυστέρηση αναμονής. Αφ' ετέρου, η καθυστέρηση μιας διαδρομής μπορεί να μη μετρηθεί καθόλου, μπορεί να είναι ένα ποσό των στατικών ποσοτήτων καθορισμένο για κάθε διεπαφή κατά μήκος της πορείας. Κάθε μεμονωμένη ποσότητα καθυστέρησης θα ήταν μια εκτίμηση βασισμένη στον τύπο σύνδεσης με τον οποίο η διεπαφή συνδέεται.

Αξιοπιστία

Η *αξιοπιστία* μετρά την πιθανότητα ότι η σύνδεση θα αποτύχει με κάποιο τρόπο και μπορεί να είναι είτε μεταβλητή είτε σταθερή. Τα παραδείγματα των μεταβλητής-αξιοπιστίας metrics είναι ο αριθμός χρόνων που μια σύνδεση έχει αποτύχει ή ο αριθμός λαθών που έχει λάβει εντός ενός ορισμένου χρονικού διαστήματος. Σταθερής- αξιοπιστίας metrics είναι βασισμένα σε γνωστές ιδιότητες μιας σύνδεσης όπως καθορίζεται από το διοικητή δικτύων. Η πορεία με την υψηλότερη αξιοπιστία θα επιλεγόταν ως καλύτερη.

Κόστος

Αυτό το metric διαμορφώνεται από έναν διοικητή δικτύων για να απεικονίσει περισσότερες - ή λιγότερες-προτιμημένες διαδρομές. Το κόστος μπορεί να καθοριστεί από οποιοδήποτε χαρακτηριστικό πολιτικής ή συνδέσεων ή μπορεί να απεικονίσει την αυθαίρετη κρίση του διοικητή

δικτύων. Ο όρος κόστος χρησιμοποιείται συχνά ως γενικός όρος κατά την ομιλία για τις επιλογές διαδρομών. Παραδείγματος χάριν, ‘Το RIP επιλέγει την πορεία χαμηλού-κόστους βασισμένη στην αρίθμηση βημάτων.’ Ένας άλλος γενικός όρος είναι *ο πιο σύντομος,* όπως "το RIP επιλέγει την κοντύτερη πορεία βασισμένη στην αρίθμηση βημάτων." Όταν χρησιμοποιείται σε αυτό το πλαίσιο, καθένα από τα *χαμηλότερο -κόστος* (ή *υψηλότερο - κόστος)* και *κοντύτερο* (ή *μακρύτερο)* αναφέρονται σε μια άποψη πρωτοκόλλου δρομολόγησης των πορειών με βάση τα συγκεκριμένα metrics.

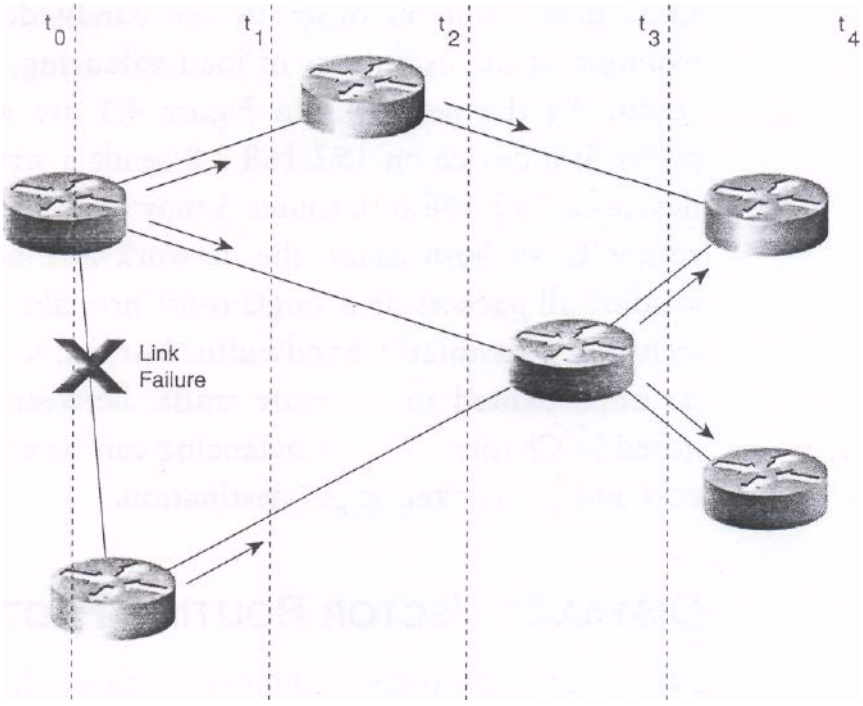
Σύγκλιση

Ένα δυναμικό πρωτόκολλο δρομολόγησης πρέπει να περιλάβει ένα σύνολο διαδικασιών για έναν δρομολογητή για να ενημερώσει άλλους δρομολογητές για τα άμεσα συνδεδεμένα δίκτυά του, για να λάβει και να επεξεργαστεί τις ίδιες πληροφορίες από άλλους δρομολογητές, και για να περάσει κατά μήκος τις πληροφορίες που λαμβάνει από άλλους δρομολογητές. Περαιτέρω, ένα πρωτόκολλο δρομολόγησης πρέπει να καθορίσει ένα metric από το οποίο οι καλύτερες πορείες μπορούν να καθοριστούν. Περαιτέρω κριτήρια για τη δρομολόγηση των πρωτοκόλλων είναι ότι οι πληροφορίες προσπελασιμότητας στους πίνακες διαδρομών όλων των δρομολογητών στο internetwork πρέπει να είναι συνεπείς. Εάν ο δρομολογητής A στο σχήμα 4.1 καθορίσει ότι η καλύτερη πορεία για το δίκτυο 192.168.5.0 είναι μέσω του δρομολογητή C και εάν ο δρομολογητής C καθορίσει ότι η καλύτερη πορεία για το ίδιο δίκτυο είναι μέσω του δρομολογητή A, ο δρομολογητής A θα στείλει τα πακέτα που προορίζονται για 192.168.5.0 στο C, το C θα τα στείλει πίσω στο A, το A θα τα στείλει πάλι στο C, και ου το καθ’ εξής. Αυτή η συνεχής κυκλική κυκλοφορία μεταξύ δύο ή περισσότερων προορισμών αναφέρεται ως *βρόχος δρομολόγησης*.

Η διαδικασία που φέρνει όλους τους πίνακες διαδρομών σε μια κατάσταση σταθερότητας καλείται σύγκλιση. Ο χρόνος που χρειάζεται για την ανταλλαγή πληροφοριών μέσα σε ένα internetwork και για όλους τους δρομολογητές για να υπολογίσουν τις καλύτερες πορείες λέγεται χρόνος

σύγκλισης. Το σχήμα 4.2 παρουσιάζει ένα internetwork που έχει συγκλίνει, αλλά τώρα μια αλλαγή τοπολογίας έχει εμφανιστεί. Η σύνδεση μεταξύ των δύο πιο-αριστερών δρομολογητών έχει αποτύχει, και οι δύο δρομολογητές, που συνδέονται άμεσα, ξέρουν για την αποτυχία από το πρωτόκολλο συνδέσεων δεδομένων και προχωρούν να ενημερώσουν τους γείτονές τους για μη διαθέσιμη σύνδεση. Οι γείτονες ενημερώνουν τους πίνακες διαδρομών τους αναλόγως και ενημερώνουν τους γείτονές τους, και η διαδικασία συνεχίζεται έως ότου ξέρουν όλοι οι δρομολογητές περί της αλλαγής.

CONVERGENCE TIME



Σχήμα 4.2
Η επαναφορά μετά από μια αλλαγή τοπολογίας χρειάζεται χρόνο. Καθώς το internetwork είναι σε κατάσταση μη σύγκλισης, οι δρομολογητές είναι επιρρεπείς σε κακές πληροφορίες δρομολόγησης.

Παρατηρήστε ότι στο χρόνο t_2 οι τρεις πιο-αριστεροί δρομολογητές ξέρουν για την αλλαγή τοπολογίας αλλά οι τρεις πιο-δεξιοί δρομολογητές δεν έχει ακούσει ακόμα για τις αλλαγές. Αυτοί οι τρεις έχουν τις παλαιές πληροφορίες και θα συνεχίσουν να μεταστρέφουν τα πακέτα αναλόγως. Είναι κατά τη διάρκεια αυτού του ενδιάμεσου χρόνου, όταν το internetwork είναι σε μια κατάσταση μη σύγκλισης, όπου τα λάθη δρομολόγησης

μπορούν να εμφανιστούν. Επομένως ο χρόνος σύγκλισης είναι ένας σημαντικός παράγοντας σε οποιοδήποτε πρωτόκολλο δρομολόγησης. Όσο γρηγορότερα ένα δίκτυο κάνει την σύγκλισή του μετά από μια αλλαγή τοπολογίας, τόσο καλύτερα.

Load Balancing

Ανακλώντας το κεφάλαιο 3, "στατική δρομολόγηση," που load balancing είναι η πρακτική της διανομής της κυκλοφορίας μεταξύ των πολλαπλάσιων πορειών στον ίδιο προορισμό προκειμένου να χρησιμοποιηθεί το εύρος ζώνης αποτελεσματικά. Σαν παράδειγμα της χρησιμότητας της load balancing, εξετάστε το σχήμα 4.1 πάλι. Όλα τα δίκτυα στο σχήμα 4.1 είναι εφικτά από δύο πορείες. Εάν μια συσκευή στο 192.168.2.0 στέλνει ένα stream πακέτων σε μια συσκευή στο 192.168.6.0, ο δρομολογητής A μπορεί να τα στείλει όλα μέσω του δρομολογητή B ή του δρομολογητή C. Και στις δύο περιπτώσεις, το δίκτυο είναι 1 βήμα μακριά. Εντούτοις, η αποστολή όλων των πακέτων σε μια ενιαία διαδρομή δεν είναι πιθανώς η αποδοτικότερη χρήση του διαθέσιμου εύρους ζώνης. Άντ' αυτού, load balancing πρέπει να εφαρμοστεί για να εναλλάξει την κυκλοφορία μεταξύ των δύο πορειών. Όπως σημειώνεται στο κεφάλαιο 3, load balancing μπορεί να είναι ίσου κόστους ή άνισου κόστους και ανά πακέτο ή ανά προορισμό.

DISTANCE VECTOR ROUTING PROTOCOLS

Τα περισσότερα πρωτόκολλα δρομολόγησης περιέρχονται στη μια από τις δύο κατηγορίες: διάνυσμα απόστασης ή κατάσταση συνδέσεων. Τα βασικά των διανυσματικών πρωτοκόλλων δρομολόγησης απόστασης εξετάζονται εδώ, το επόμενο τμήμα καλύπτει τα πρωτόκολλα κατάσταση δρομολόγησης συνδέσεων. Οι διανυσματικοί αλγόριθμοι απόστασης είναι βασισμένοι στην εργασία που έγινε από R.E. Bellman, L.R. Ford, και D.R. Fulkerson και για αυτόν τον λόγο περιστασιακά αναφέρεται ως Bellman-Ford ή Ford-Fulkerson αλγόριθμος. Το όνομα διάνυσμα απόστασης

προέρχεται από το γεγονός ότι οι διαδρομές διαφημίζονται ως διανύσματα (απόσταση, κατεύθυνση), όπου η απόσταση καθορίζεται από την άποψη ενός metric και η κατεύθυνση καθορίζεται από την άποψη του δρομολογητή next-hop. Παραδείγματος χάριν, " Ο προορισμός Α είναι μια απόσταση 5 βημάτων μακριά, στην κατεύθυνση του δρομολογητή next-hop Χ." Όπως αυτή η δήλωση υπονοεί, κάθε δρομολογητής μαθαίνει τις διαδρομές από τους γειτονικούς δρομολογητές και διαφημίζουν έπειτα τις διαδρομές. Επειδή κάθε δρομολογητής εξαρτάται από τους γείτονές του για τις πληροφορίες, τις οποίες οι γείτονες μπορεί στη συνέχεια να είχαν μάθει από τους γείτονές τους, και τα λοιπά, η διανυσματική δρομολόγηση απόστασης μερικές φορές περιπαικτικά αναφέρεται ως "δρομολόγηση από τη φήμη."

Τα διανυσματικά πρωτόκολλα δρομολόγησης απόστασης περιλαμβάνουν τα ακόλουθα:

- *Routing Information Protocol (RIP) for IP*
- *Xerox Networking System's XNS RIP*
- *Novell's IPX RIP*
- *Cisco's Internet Gateway Routing Protocol (IGRP)*
- *DEC's DNA Phase IV*
- *AppleTalk's Routing Table Maintenance Protocol (RTMP)*

Κοινά χαρακτηριστικά

Ένα τυπικό διανυσματικό πρωτόκολλο δρομολόγησης απόστασης χρησιμοποιεί έναν αλγόριθμο δρομολόγησης στον οποίο οι δρομολογητές στέλνουν περιοδικά τις αναπροσαρμογές δρομολόγησης σε όλους τους γείτονες με broadcast ολόκληρων των πινάκων διαδρομών τους. Η προηγούμενη δήλωση περιέχει πολλές πληροφορίες. Τα ακόλουθα τμήματα το εξετάζουν λεπτομερέστερα.

Περιοδικές αναπροσαρμογές

Οι *περιοδικές αναπροσαρμογές* σημαίνουν ότι στο τέλος ενός ορισμένου χρονικού διαστήματος, οι αναπροσαρμογές θα διαβιβαστούν. Αυτή η περίοδος κυμαίνεται χαρακτηριστικά από 10 δευτερόλεπτα για AppleTalk's RTMP ως 90 δευτερόλεπτα για IGRP Cisco. Το ζήτημα εδώ, είναι το γεγονός ότι εάν οι αναπροσαρμογές στέλνονται πάρα πολύ συχνά, συμφόρηση μπορεί να εμφανιστεί, εάν οι αναπροσαρμογές στέλνονται πάρα πολύ σπάνια, ο χρόνος σύγκλισης μπορεί να είναι απαράδεκτα υψηλός.

Γείτονες

Στα πλαίσια των δρομολογητών, *οι γείτονες*, πάντα σημαίνουν δρομολογητές που μοιράζονται μια κοινή σύνδεση δεδομένων. Ένα διανυσματικό πρωτόκολλο δρομολόγησης απόστασης στέλνει τις αναπροσαρμογές του στους γειτονικούς δρομολογητές και εξαρτάται από αυτούς για να περάσει τις πληροφορίες αναπροσαρμογών προς στους γείτονές τους. Για αυτόν τον λόγο, η διανυσματική δρομολόγηση απόστασης λέγεται ότι χρησιμοποιεί βήμα-βήμα τις αναπροσαρμογές.

Broadcast Αναπροσαρμογές

Όταν ένας δρομολογητής γίνεται αρχικά ενεργός σε ένα δίκτυο, πώς βρίσκει άλλους δρομολογητές και πώς αναγγέλλει την παρουσία του; Διάφορες μέθοδοι είναι διαθέσιμες. Ο απλούστερος τρόπος είναι να στείλει τις αναπροσαρμογές στη broadcast διεύθυνση (στην περίπτωση της IP, 255.255.255.255). Οι γειτονικοί δρομολογητές που χρησιμοποιούν το ίδιο πρωτόκολλο δρομολόγησης θα αντιληφθούν το broadcast και θα λάβουν τα κατάλληλα μέτρα. Οι οικοδεσπότες και άλλες συσκευές, αδιάφοροι στις αναπροσαρμογές δρομολόγησης απλά θα ρίξουν τα πακέτα.

Πλήρης Αναπροσαρμογές πινάκων διαδρομών

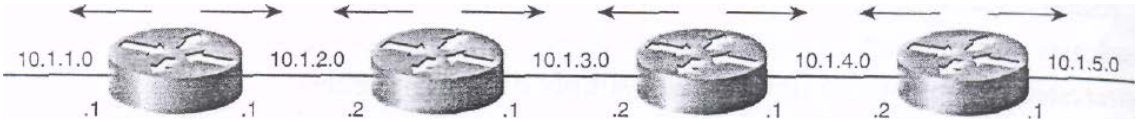
Τα περισσότερα διανυσματικά πρωτόκολλα δρομολόγησης απόστασης υιοθετούν την πολύ απλή μέθοδο της αφήγησης όλων γειτόνων τους που ξέρουν, με broadcasting ολόκληρου του πίνακα διαδρομών τους, με μερικές εξαιρέσεις που καλύπτονται στα ακόλουθα τμήματα. Οι γείτονες που λαμβάνουν αυτές τις αναπροσαρμογές καθαρίζουν τις πληροφορίες που χρειάζονται και απορρίπτουν όλα τα άλλα.

Δρομολόγηση από τη φήμη

Το σχήμα 4.3 παρουσιάζει έναν αλγόριθμο διανυσματικής απόστασης σε δράση. Σε αυτό το παράδειγμα, το metric είναι αρίθμηση βημάτων. Στο χρόνο t_0, οι δρομολογητές A μέσω του D μόλις έγιναν ενεργοί. Εξετάζοντας τους πίνακες διαδρομών πέρα από την κορυφαία σειρά, στο t_0 οι μόνες πληροφορίες που οποιοσδήποτε από τους τέσσερις δρομολογητές έχει είναι τα άμεσα συνδεδεμένα δίκτυά τους. Οι πίνακες προσδιορίζουν αυτά τα δίκτυα και δείχνουν ότι συνδέονται άμεσα με την κατοχή κανενός δρομολογητή next-hop και με την κατοχή μιας αρίθμησης βημάτων 0. Κάθε ένας από τους τέσσερις δρομολογητές θα broadcast αυτές τις πληροφορίες για όλες τις συνδέσεις.

Στο χρόνο t_1, οι πρώτες αναπροσαρμογές έχουν παραληφθεί και έχουν υποβληθεί σε επεξεργασία από τους δρομολογητές. Εξετάστε τον πίνακα δρομολογητών A στο t_1. Η αναπροσαρμογή δρομολογητών B στο δρομολογητή A είπε ότι ο δρομολογητής B μπορεί να φθάσει στα δίκτυα 10.1.2.0 και 10.1.3.0 και οι δύο 0 βήματα μακριά. Εάν τα δίκτυα είναι 0 βήματα από το B, πρέπει να είναι 1 βήμα από το A. Ο δρομολογητής A αύξησε την αρίθμηση βημάτων κατά 1 και έπειτα εξέτασε τον πίνακα διαδρομών του. Ήξερε ήδη για 10.1.2.0 και η αρίθμηση βημάτων (0) ήταν λιγότερη από την αρίθμηση βημάτων που διαφήμισε ο B (1), έτσι ο A δεν έλαβε υπόψη εκείνες τις πληροφορίες. Το δίκτυο 10.1.3.0 ήταν νέες πληροφορίες, εντούτοις, ο A εισήγαγε αυτό στον πίνακα διαδρομών. Η διεύθυνση προέλευσης του πακέτου αναπροσαρμογών ήταν η διεπαφή του

δρομολογητή B (10.1.2.2) έτσι ώστε οι πληροφορίες να εισάγονται μαζί με την υπολογισμένη αρίθμηση βημάτων.



	Router A			Router B			Router C			Router D		
	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS
T0	10.1.1.0	- -	0	10.1.2.0	- -	0	10.1.3.0	--	0	10.1.4.0	--	0
	10.1.2.0	- -	0	10.1.3.0	- -	0	10.1.4.0	--	0	10.1.5.0	--	0
	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS
T1	10.1.1.0	- -	0	10.1.2.0	- -	0	10.1.3.0	--	0	10.1.4.0	--	0
	10.1.2.0	- -	0	10.1.3.0	- -	0	10.1.4.0	--	0	10.1.5.0	--	0
	10.1.3.0	10.1.2.2	1	10.1.1.0	10.1.2.1	1	10.1.2.0	10.1.3.1	1	10.1.3.0	10.1.4.1	1
				10.1.4.0	10.1.3.2	1	10.1.5.0	10.1.4.2	1			
	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS
T2	10.1.1.0	--	0	10.1.2.0	- -	0	10.1.3.0	--	0	10.1.4.0	- -	0
	10.1.2.0	--	0	10.1.3.0	- -	0	10.1.4.0	--	0	10.1.5.0	- -	0
	10.1.3.0	10.1.2.2	1	10.1.1.0	10.1.2.1	1	10.1.2.0	10.1.3.1	1	10.1.3.0	10.1.4.1	1
	10.1.4.0	10.1.2.2	2	10.1.4.0	10.1.3.2	1	10.1.5.0	10.1.4.2	1	10.1.2.0	10.1.4.1	2
				10.1.5.0	10.1.3.2	2	10.1.1.0	10.1.3.1	2			
	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS	NET	VIA	HOPS
T3	10.1.1.0	--	0	10.1.2.0	- -	0	10.1.3.0	--	0	10.1.4.0	- -	0
	10.1.2.0	--	0	10.1.3.0	- -	0	10.1.4.0	--	0	10.1.5.0	- -	0
	10.1.3.0	10.1.2.2	1	10.1.1.0	10.1.2.1	1	10.1.2.0	10.1.3.1	1	10.1.3.0	10.1.4.1	1
	10.1.4.0	10.1.2.2	2	10.1.4.0	10.1.3.2	1	10.1.5.0	10.1.4.2	1	10.1.2.0	10.1.4.1	2
	10.1.5.0	10.1.2.2	3	10.1.5.0	10.1.3.2	2	10.1.1.0	10.1.3.1	2	10.1.1.0	10.1.4.1	3

Σχήμα 4.3
Τα πρωτόκολλα διανυσματικής απόστασης συγκλίνουν βήμα-βήμα.

Παρατηρήστε ότι οι άλλοι δρομολογητές εκτέλεσαν παρόμοιες διαδικασίες στον ίδιο χρόνο t_1. Ο δρομολογητής C, παραδείγματος χάριν, δεν έλαβε υπόψη τις πληροφορίες για 10.1.3.0 από το B και 10.1.4.0 από το C αλλά εισήγαγε τις πληροφορίες για 10.1.2.0, εφικτό μέσω της διεύθυνσης διεπαφών B 10.1.3.1 και 10.1.5.0, εφικτό μέσω της διεπαφής C 10.1.4.2. Και τα δύο δίκτυα υπολογίστηκαν ως 1 βήμα μακριά.

Στο χρόνο t_2, η περίοδος αναπροσαρμογών έχει λήξει πάλι και ένα άλλο σύνολο αναπροσαρμογών είναι broadcast. Ο δρομολογητής B έστειλε τον πιο πρόσφατο πίνακά του ο δρομολογητής A αύξησε πάλι τις

διαφημισμένες αριθμήσεις βημάτων του B από 1 και τα σύγκρινε. Οι πληροφορίες για 10.1.2.0 απορρίπτονται πάλι για τον ίδιο λόγο όπως πριν. 10.1.3.0 είναι ήδη γνωστό, και η αρίθμηση βημάτων δεν έχει αλλάξει, έτσι οι πληροφορίες απορρίπτονται επίσης. 10.1.4.0 είναι νέες πληροφορίες και εισάγονται στον πίνακα διαδρομών.

Το δίκτυο συγκλίνει στο χρόνο t_3. Κάθε δρομολογητής ξέρει για κάθε δίκτυο, τη διεύθυνση του δρομολογητή next-hop για κάθε δίκτυο, και την απόσταση των βημάτων σε κάθε δίκτυο.

Οι διανυσματικοί αλγόριθμοι απόστασης παρέχουν τα οδικά σημάδια στα δίκτυα. Παρέχουν την κατεύθυνση και την απόσταση, αλλά καμία λεπτομέρεια, για αυτό που βρίσκεται κατά μήκος της διαδρομής και είναι τρωτοί στην τυχαία ή σκόπιμη εσφαλμένη κατεύθυνση. Παρακάτω είναι μερικές από τις δυσκολίες και τους καθαρισμούς που συνδέονται με τους διανυσματικούς αλγορίθμους απόστασης.

Χρονόμετρα ακύρωσης διαδρομών

Τώρα που το internetwork στο σχήμα 4.3 έχει συγκλίνει πλήρως , πώς θα χειριστεί την επαναφορά όταν αλλάζει κάποιο μέρος της τοπολογίας; Εάν το δίκτυο 10.1.5.0 ‘πέσει’, η απάντηση είναι αρκετά απλή —ο δρομολογητής D, στην επόμενη σχεδιασμένη αναπροσαρμογή του, σημαιοστολίζει το δίκτυο ως απρόσιτο και περνά τις πληροφορίες εμπρός.

Αλλά ακόμη και αν, αντί για 10.1.5.0 πηγαίνοντας κάτω, ο δρομολογητής D αποτυγχάνει; Οι δρομολογητές A, B και C έχουν ακόμα τις καταχωρήσεις στους πίνακες διαδρομών τους για 10.1.5.0, οι πληροφορίες δεν ισχύουν πλέον, αλλά δεν υπάρχει κανένας δρομολογητής για να τους ενημερώσει για αυτό το γεγονός. Θα διαβιβάσουν εν αγνοία τα πακέτα σε έναν απρόσιτο προορισμό — μια μαύρη τρύπα έχει ανοίξει στο internetwork. Αυτό το πρόβλημα αντιμετωπίζεται με τη ρύθμιση ενός χρονομέτρου ακύρωσης διαδρομών για κάθε είσοδο στον πίνακα διαδρομών. Παραδείγματος χάριν, όταν ο δρομολογητής C πρώτα ακούει για 10.1.5.0 και εισάγει τις πληροφορίες

στον πίνακα δρομολογητών του, ο C βάζει ένα χρονόμετρο για εκείνη η διαδρομή. Τακτικά σε κάθε αναπροσαρμογή προγραμμάτων από το δρομολογητή D, το C απορρίπτει την ήδη- γνωστή πληροφορία της αναπροσαρμογής για 10.1.5.0 όπως περιγράφεται "στη δρομολόγηση από φήμη. Αλλά αφού ο C κάνει έτσι, επαναρυθμίζει το χρόνο σε εκείνη την διαδρομή. Εάν ο δρομολογητής D πηγαίνει κάτω, ο C δεν θα ακούσει πλέον τις αναπροσαρμογές για το 10.1.5.0. Ο χρόνος θα λήξει, ο C θα σημαιοστολίσει τη διαδρομή ως απρόσιτη και θα περάσει τις πληροφορίες εμπρός στην επόμενη αναπροσαρμογή. Οι χαρακτηριστικές περίοδοι για τη σειρά διαλειμμάτων είναι από τρεις έως έξι περιόδους αναπροσαρμογών. Ένας δρομολογητής δεν θα ήθελε να ακυρώσει μια διαδρομή αφού έχει χαθεί η ενιαία αναπροσαρμογή, επειδή αυτό το γεγονός μπορεί να είναι το αποτέλεσμα από ένα αλλοιωμένο ή χαμένο πακέτο ή κάποιο είδος καθυστέρησης δικτύων. Συγχρόνως, εάν η περίοδος είναι πάρα πολύ μεγάλη, η επαναφορά θα είναι χαρακτηριστικά αργή.

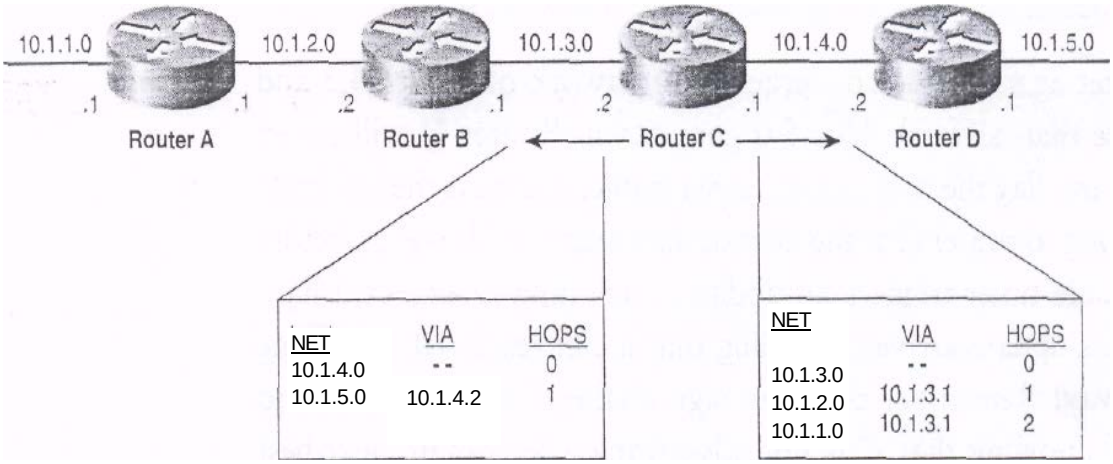
Σύμφωνα με το διανυσματικό αλγόριθμο απόστασης, δεδομένου ό,τι έχει περιγραφεί μέχρι τώρα, σε κάθε περίοδο αναπροσαρμογών κάθε δρομολογητής κάνει αναμετάδοση ολόκληρο τον πίνακα διαδρομών του σε κάθε γείτονα. Αλλά είναι αυτό πραγματικά απαραίτητο; Κάθε δίκτυο που είναι γνωστό από το δρομολογητή A στο σχήμα 4.3, με μια αρίθμηση βημάτων υψηλότερη από 0, έχει μαθευτεί από το δρομολογητή B. Η ίδια αίσθηση το προτείνει για το δρομολογητή A για να broadcast τα δίκτυα που έχει μάθει από το δρομολογητή B πίσω στο δρομολογητή B είναι χάσιμο πόρων. Προφανώς, ο B ήδη γνωρίζει για αυτά τα δίκτυα. Μια διαδρομή που δείχνει πίσω στο δρομολογητή από τον οποίο τα πακέτα έχουν ληφθεί καλείται *αντίστροφη διαδρομή. Ο διασπασμένος ορίζοντας* είναι μια τεχνική για τις αντίστροφες διαδρομές μεταξύ δύο δρομολογητών. Εκτός από την μη σπατάλη των πόρων, υπάρχει ένας σημαντικότερος λόγος για μην στέλνονται πληροφορίες προσπελασιμότητας πίσω στο δρομολογητή από τον οποίο οι πληροφορίες μαθεύτηκαν. Η σημαντικότερη λειτουργία ενός δυναμικού πρωτοκόλλου δρομολόγησης είναι να ανιχνευθούν και να αντισταθμιστούν οι αλλαγές τοπολογίας — εάν η καλύτερη πορεία σε ένα

δίκτυο γίνεται απρόσιτη, το πρωτόκολλο πρέπει να ψάξει μια επόμενη - καλύτερη πορεία.

Εξετάστε για ακόμη μία φορά την σύγκλιση του internetwork του σχήματος 4.3 και υποθέστε ότι το δίκτυο 10.1.5.0 'πέφτει'.
Ο δρομολογητής D θα ανιχνεύσει την αποτυχία, θα σημαιοστολίσει το δίκτυο ως απρόσιτο, και περνά τις πληροφορίες εμπρός, στο δρομολογητή C στο επόμενο διάστημα αναπροσαρμογών. Εντούτοις, πριν από την αναπροσαρμογή του D το χρονόμετρο προκαλεί μια αναπροσαρμογή, κάτι απροσδόκητο συμβαίνει. Η αναπροσαρμογή του C φθάνει, υποστηρίζοντας ότι μπορεί να φθάσει το 10.1.5.0, ένας βήμα μακριά! Ο δρομολογητής D δεν γνωρίζει εάν ο C δεν διαφημίζει μια νόμιμη καλύτερη-επόμενη πορεία. Θα αυξήσει την αρίθμηση βημάτων και θα κάνει μια είσοδο μέσα στον πίνακα διαδρομών του που δείχνει ότι 10.1.5.0 είναι εφικτό μέσω της διεπαφής του δρομολογητή C 10.1.4.1, ακριβώς 2 βήματα μακριά. Τώρα ένα πακέτο με μια διεύθυνση προορισμού 10.1.5.3 φθάνει στο δρομολογητή C. Ο C συμβουλεύεται τον πίνακα διαδρομών του και διαβιβάζει το πακέτο στο D. Ο D συμβουλεύεται τον πίνακα διαδρομών του και διαβιβάζει το πακέτο στο C, ο C το διαβιβάζει πίσω στο D, *έπ' άπειρον.* Ένας βρόχος δρομολόγησης έχει εμφανιστεί.

Η εφαρμογή του διασπασμένου ορίζοντα αποτρέπει τη δυνατότητα ενός τέτοιου βρόχου δρομολόγησης. Υπάρχουν δύο κατηγορίες διασπασμένου ορίζοντα: απλός διασπασμένος ορίζοντας και διασπασμένος ορίζοντας με τη δηλητηριασμένη αντιστροφή. Ο κανόνας για τον απλό διασπασμένο ορίζοντα είναι, Κατά την αποστολή ενημερώσεων από μια ιδιαίτερη διεπαφή, δεν περιλαμβάνει τα δίκτυα που μαθεύτηκαν από τις αναπροσαρμογές που παραλήφθηκαν σε εκείνη την διεπαφή. Οι δρομολογητές στο σχήμα 4.4 εφαρμόζουν τον απλό διασπασμένο ορίζοντα. Ο δρομολογητής C στέλνει μια αναπροσαρμογή στο δρομολογητή D για τα δίκτυα 10.1.1.0, 10.1.2.0.1 και 10.1.3.0. Τα δίκτυα 10.1.4.0 και 10.1.5.0 δεν συμπεριλαμβάνονται επειδή μαθεύτηκαν από το δρομολογητή D. Επιπλέον, οι αναπροσαρμογές στο δρομολογητή

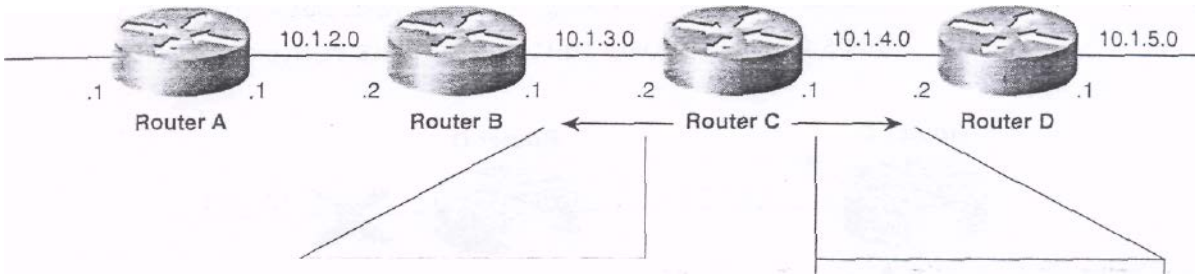
Β περιλαμβάνουν 10.1.4.0 και 10.1.5.0 με καμία αναφορά σε 10.1.1.0, 10.1.2.0 και 10.1.3.0.



Σχήμα 4.4
Ο απλός διασπασμένος ορίζοντας δεν διαφημίζει διαδρομές πίσω στους γείτονες από όπου οι διαδρομές μαθεύτηκαν.

Ο απλός διασπασμένος ορίζοντας δουλεύει με την καταστολή των πληροφοριών. Ο διασπασμένος ορίζοντας με τη δηλητηριασμένη αντιστροφή είναι μια τροποποίηση που παρέχει πιο θετικότερες πληροφορίες. Ο κανόνας για το διασπασμένο ορίζοντα με τη δηλητηριασμένη αντιστροφή είναι, κατά την αποστολή ενημερώσεων από μια ιδιαίτερη διεπαφή, υποδεικνύει οποιαδήποτε δίκτυα μαθεύτηκαν από τις αναπροσαρμογές που παραλήφθηκαν σε εκείνη την διεπαφή ως απρόσιτα.

Στο σενάριο του σχήματος 4.4, ο δρομολογητής C θα διαφήμιζε στην πραγματικότητα 10.1.4.0 και 10.1.5.0 στο δρομολογητή D, αλλά το δίκτυο θα χαρακτηριζόταν όπως απρόσιτο. Το σχήμα 4.5 παρουσιάζει πως θα έμοιαζαν οι πίνακες διαδρομών από το C στο B και D. Παρατηρήστε ότι μια διαδρομή είναι χαρακτηρισμένη ως απρόσιτη με τη ρύθμιση του metric στο άπειρο, με άλλα λόγια, το δίκτυο είναι μια άπειρη απόσταση μακριά.



NET	VIA	HOPS
10.1.3.0	--	inf
10.1.4.0		0
10.1.2.0	10.1.3.1	inf
10.1.5.0	10.1.4.2	1
10.1.1.0	10.1.3.1	inf

NET	VIA	HOPS
10.1.3.0	- -	0
10.1.4.0	- -	inf
10.1.2.0	10.1.3.1	1
10.1.5.0	10.1.4.2	inf
10.1.1.0	10.1.3.1	2

Σχήμα 4.5
Ο διασπασμένος ορίζοντας με δηλητηριασμένες αντίστροφες διαφημίσεις αντιστρέφει διαδρομές αλλά με ένα άφταστο metric.

Ο διασπασμένος ορίζοντας με τη δηλητηριασμένη αντιστροφή θεωρείται ασφαλέστερος και ισχυρότερος από τον απλό διασπασμένο ορίζοντα που —κάποιες "κακές ειδήσεις είναι καλύτερες από καμία είδηση". Παραδείγματος χάριν, υποθέστε ότι ο δρομολογητής B στο σχήμα 4.5 λαμβάνει αλλοιωμένες πληροφορίες αναγκάζοντας να θεωρήσει ότι το υποδίκτυο 10.1.1.0 είναι εφικτό μέσω του δρομολογητή C. Ο απλός διασπασμένος ορίζοντας δεν θα έκανε τίποτα για να διορθώσει αυτήν την εσφαλμένη εκτίμηση, ενώ μια δηλητηριασμένη αντίστροφη αναπροσαρμογή από το δρομολογητή C αμέσως σταματά τον πιθανό βρόχο. Για αυτόν τον λόγο, πιο σύγχρονες εφαρμογές διανυσματικής απόστασης χρησιμοποιούν διασπασμένο ορίζοντα με τη δηλητηριασμένη αντιστροφή. Η ανταλλαγή είναι ότι τα πακέτα αναπροσαρμογών δρομολόγησης είναι μεγαλύτερα, το οποίο μπορεί να επιδεινώσει οποιαδήποτε προβλήματα συμφόρησης σε μια σύνδεση.

Triggered Updates

Οι *προκαλούμενες αναπροσαρμογές* γνωστές επίσης ως *αναπροσαρμογές λάμψης*, είναι πολύ απλές: Εάν ένα metric αλλάξει για καλύτερα ή για χειρότερα, ένας δρομολογητής θα στείλει αμέσως μια αναπροσαρμογή χωρίς να περιμένει να λήξει το χρονόμετρο αναπροσαρμογών του. Το

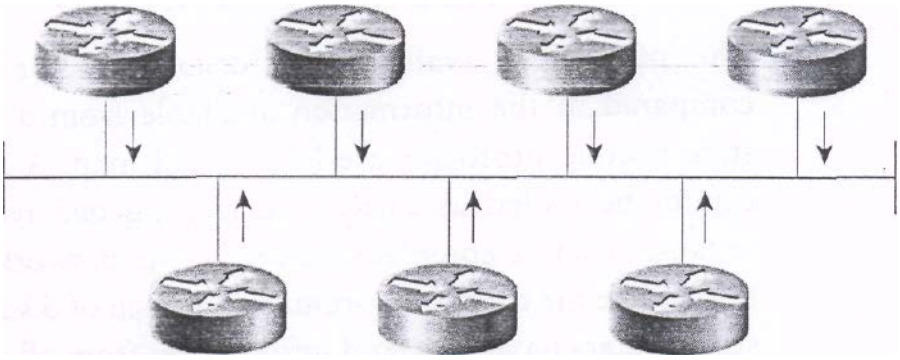
Reconvergence θα εμφανιστεί πολύ γρηγορότερα από το εάν κάθε δρομολογητής έπρεπε να περιμένει τις τακτικά σχεδιασμένες αναπροσαρμογές και το πρόβλημα στο άπειρο περιορίζεται πολύ, αν και δεν αποβάλλεται πλήρως. Οι κανονικές αναπροσαρμογές μπορούν ακόμα να εμφανιστούν μαζί με τις προκαλούμενες αναπροσαρμογές. Κατά συνέπεια ένας δρομολογητής να λάβει κακές πληροφορίες για μια διαδρομή από έναν όχι-ακόμα- Reconverged δρομολογητή αφού έχει λάβει τις σωστές πληροφορίες από μια προκαλούμενη αναπροσαρμογή. Μια τέτοια κατάσταση δείχνει ότι τα λάθη σύγχυσης και δρομολόγησης μπορούν ακόμα να εμφανιστούν ενώ ένα internetwork κάνει επαναφορά, αλλά προκαλούμενες αναπροσαρμογές θα βοηθήσουν να διορθωθούν τα πράγματα έξω, γρηγορότερα. Ένας περαιτέρω καθαρισμός είναι να περιληφθούν στην αναπροσαρμογή μόνο τα δίκτυα που το προκάλεσαν πραγματικά, παρά ολόκληρος ο πίνακας διαδρομών. Αυτή η τεχνική μειώνει το χρόνο επεξεργασίας και τον αντίκτυπο στο εύρος ζώνης δικτύων.

Holddown Timers

Οι προκαλούμενες αναπροσαρμογές προσθέτουν ανταπόκριση σε ένα reconverging internetwork. *Τα holddown χρονόμετρα* εισάγουν ένα ορισμένο ποσό σκεπτικισμού για να μειώσουν την αποδοχή των πληροφοριών κακής δρομολόγησης. Εάν η απόσταση σε έναν προορισμό αυξάνεται (παραδείγματος χάριν, οι αυξήσεις αρίθμησης βημάτων από 2 σε 4), ο δρομολογητής θέτει ένα holddown χρονόμετρο για εκείνη την διαδρομή. Μέχρι να λήξει το χρονόμετρο, ο δρομολογητής δεν θα δεχτεί οποιεσδήποτε νέες αναπροσαρμογές για τη διαδρομή. Προφανώς, μια ανταλλαγή περιλαμβάνεται εδώ. Η πιθανότητα των πληροφοριών κακής δρομολόγησης που παίρνουν σε έναν πίνακα μειώνεται αλλά εις βάρος του χρόνου επαναφοράς. Όπως και άλλα χρονόμετρα, το holddown χρονόμετρο πρέπει να τεθεί με προσοχή. Εάν η holddown περίοδος είναι πάρα πολύ μικρή, θα είναι ατελέσφορη, και εάν είναι πάρα πολύ μακριά, η κανονική δρομολόγηση θα επηρεαστεί αρνητικά.

Ασύγχρονες αναπροσαρμογές

Το σχήμα 4.6 παρουσιάζει μια ομάδα δρομολογητών που συνδέονται με μια σπονδυλική στήλη Ethernet. Οι δρομολογητές δεν πρέπει να αναμεταδίδουν τις αναπροσαρμογές τους συγχρόνως, εάν το κάνουν, τα πακέτα αναπροσαρμογών θα συγκρουστούν. Ακόμη, αυτή η κατάσταση είναι ακριβώς, τι μπορεί να συμβεί όταν διάφοροι δρομολογητές μοιράζονται το broadcast δίκτυο. Οι καθυστερήσεις συστημάτων σχετίζονται με τις αναπροσαρμογές επεξεργασίας στους δρομολογητές που τείνουν να αναγκάσουν τα χρονόμετρα αναπροσαρμογών για να γίνουν συγχρονισμένα. Δεδομένου ότι μερικοί δρομολογητές γίνονται συγχρονισμένοι, οι συγκρούσεις θα αρχίσουν να εμφανίζονται, να προαγάγουν τη συμβολή στις καθυστερήσεις των συστημάτων, και τελικά όλοι οι δρομολογητές που μοιράζονται το broadcast δίκτυο μπορούν να γίνουν συγχρονισμένοι.



Σχήμα 4.6
Εάν τα ενημερωμένα χρονόμετρα συγχρονιστούν, συγκρούσεις μπορεί να προκύψουν.

Οι ασύγχρονες αναπροσαρμογές μπορούν να διατηρηθούν με τη μια από δύο μεθόδους:

- Το χρονόμετρο αναπροσαρμογών κάθε δρομολογητή είναι ανεξάρτητο από την επεξεργασία δρομολόγησης
  και, επομένως, δεν επηρεάζεται με την επεξεργασία των φορτίων στο δρομολογητή.

- Ένας μικρός τυχαίος χρόνος, ή *ο συγχρονισμός jitter,* προστίθεται σε κάθε περίοδο αναπροσαρμογών όπως ένα offset.

Εάν οι δρομολογητές εφαρμόζουν τη μέθοδο άκαμπτων, σύστημα-ανεξάρτητων χρονομέτρων, τότε όλοι οι δρομολογητές που μοιράζονται ένα broadcast δίκτυο πρέπει να παρουσιαστούν on-line σε μια τυχαία μόδα. Η εκ νέου αναχώρηση της ολόκληρης ομάδας δρομολογητών ταυτόχρονα, θα μπορούσε να οδηγήσει σε όλα τα χρονόμετρα να προσπαθούν να ενημερωθούν συγχρόνως. Η προσθήκη του τυχαίου, στην περίοδο αναπροσαρμογών είναι αποτελεσματική εάν η μεταβλητή είναι αρκετά μεγάλη αναλογικά προς τον αριθμό δρομολογητών που μοιράζονται το broadcast δίκτυο.

LINK STATE ROUTING PROTOCOLS

Οι πληροφορίες που είναι διαθέσιμες σε έναν διανυσματικό δρομολογητή απόστασης έχουν συγκριθεί με τις πληροφορίες που είναι διαθέσιμες από ένα οδικό σημάδι. Link state routing protocols είναι όπως ένας οδικός χάρτης. A link state router δεν μπορεί να πιαστεί κορόιδο παίρνοντας εύκολα κακές αποφάσεις δρομολόγησης, επειδή έχει μια πλήρη εικόνα του δικτύου. Ο λόγος είναι ότι αντίθετα από την δρομολόγηση-από-φήμη προσέγγιση του διανύσματος απόστασης, link state routers έχουν τις από πρώτο χέρι πληροφορίες από όλους τους peer δρομολογητές. Κάθε δρομολογητής δημιουργεί πληροφορίες για τον εαυτό του, για τις άμεσα συνδεδεμένες συνδέσεις του και την κατάσταση εκείνων των συνδέσεων (ως εκ τούτου το όνομα). Αυτές οι πληροφορίες περνούν από δρομολογητή σε δρομολογητή, κάθε δρομολογητής κάνει ένα αντίγραφο από αυτό, αλλά ποτέ δεν το αλλάζει. Ο τελευταίος στόχος είναι ότι κάθε δρομολογητής έχει τις ίδιες πληροφορίες για το internetwork, και κάθε δρομολογητής θα υπολογίσει ανεξάρτητα τις καλύτερες πορείες του.

Link state protocols, μερικές φορές αποκαλούνται *shortest path first ή distributed database πρωτόκολλα*, δημιουργημένα γύρω από έναν πολύ-γνωστό αλγόριθμο από τη θεωρία γραφικών παραστάσεων, E. W.

Dijkstra’a ένας πιο σύντομος αλγόριθμος πορειών. Παραδείγματα από link state routing protocols είναι:

- Open Shortest Path First (OSPF) for IP
- The ISO's Intermediate System to Intermediate System (IS-IS) for CLNS and IP
- DEC'S DNA Phase V
- Novell's NetWare Link Services Protocol (NLSP)

Αν και τα link state protocols θεωρούνται πιο σύνθετα από τα διανυσματικά πρωτόκολλα απόστασης, η βασική λειτουργία δεν είναι καθόλου σύνθετη:

1. Κάθε δρομολογητής καθιερώνει μια σχέση με κάθε έναν από τους γείτονές του.
2. Κάθε δρομολογητής στέλνει *link state advertisements* (LSAs), μερικές φορές αποκαλούνται link state packets (LSPs), σε κάθε γείτονα. Ένα LSA παράγεται για κάθε μια από τις συνδέσεις του δρομολογητή, που προσδιορίζουν τη σύνδεση, την κατάσταση της σύνδεσης, το κόστος metric της διεπαφής του δρομολογητή στη σύνδεση, και οποιουσδήποτε γείτονες που μπορούν να συνδεθούν με τη σύνδεση. Κάθε γείτονας που λαμβάνει μια διαφήμιση διαβιβάζει στη συνέχεια (πλημμύρες) τη διαφήμιση στους γείτονές του.
3. Κάθε δρομολογητής αποθηκεύει ένα αντίγραφο όλου του LSAs που έχει δει στη βάση δεδομένων. Εάν όλα δουλεύουν καλά, οι βάσεις δεδομένων σε όλους τους δρομολογητές πρέπει να είναι ίδιες.
4. Η ολοκληρωμένη *topological database*, αποκαλούμενη επίσης *link state database*, περιγράφει μια γραφική παράσταση του internetwork. Χρησιμοποιώντας τον αλγόριθμο Dijkstra, κάθε δρομολογητής υπολογίζει την κοντύτερη πορεία σε κάθε δίκτυο και εισάγει αυτές τις πληροφορίες στον πίνακα διαδρομών.

Γείτονες

Η ανακάλυψη γειτόνων είναι το πρώτο βήμα ώστε ένα δίκτυο να ‘σηκωθεί’ και να ‘τρέξει’. Σύμφωνα με τη φιλική ορολογία γειτόνων, ένα hello πρωτόκολλο χρησιμοποιείται για αυτό το βήμα. Το πρωτόκολλο θα καθορίσει ένα hello σχήμα πακέτων και μια διαδικασία για τα πακέτα και τις πληροφορίες που τα πακέτα περιέχουν. Τουλάχιστον, το hello πακέτο περιέχει μια *ταυτότητα δρομολογητών* και τη διεύθυνση του δικτύου όπου το πακέτο στέλνεται. Η ταυτότητα δρομολογητών είναι κάτι από το οποίο ο δρομολογητής που δημιουργεί το πακέτο μπορεί να διακριθεί μεμονωμένα από όλους τους άλλους δρομολογητές, παραδείγματος χάριν, μια διεύθυνση IP από μια από τις διεπαφές του δρομολογητή. Άλλοι τομείς του πακέτου μπορούν να φέρουν μια μάσκα υποδικτύου, Hello διαστήματα, μια καθορισμένη μέγιστη περίοδος που ο δρομολογητής θα περιμένει να ακούσει Hello πριν κηρύσσει το γείτονα "νεκρό," έναν περιγραφέα του τύπου κυκλωμάτων, και τις σημαίες για να βοηθήσει να φέρει επάνω τους γείτονες. Όταν δύο δρομολογητές ανακαλύψουν ο ένας τον άλλον ως γείτονες, περνούν από μια διαδικασία συγχρονισμού των βάσεων δεδομένων τους, στις οποίες ανταλλάσσουν και επαληθεύουν τις πληροφορίες έως ότου οι βάσεις δεδομένων τους να είναι ίδιες. Για να εκτελέσουν αυτόν τον συγχρονισμό των βάσεων δεδομένων, οι γείτονες πρέπει να είναι *παρακείμενοι* —δηλαδή πρέπει να συμφωνήσουν σχετικά με ορισμένες πρωτοκόλλου συγκεκριμένες - παραμέτρους όπως τα χρονόμετρα και η υποστήριξη των προαιρετικών ικανοτήτων. Με τη χρησιμοποίηση Hello πακέτων για να χτίσουν τις γειτνιάσεις, τα link state protocols μπορούν να ανταλλάξουν τις πληροφορίες σε μια ελεγχόμενη μόδα. Αντιπαραβάλετε αυτήν την προσέγγιση με το διάνυσμα απόστασης, το οποίο broadcasts απλά τις αναπροσαρμογές από οποιαδήποτε διεπαφή που διαμορφώνεται για εκείνο το πρωτόκολλο δρομολόγησης. Εάν τα Hellos δεν λαμβάνουν νέα από έναν παρακείμενο γείτονα μέσα σε έναν ορισμένο καθιερωμένο χρόνο, ο γείτονας θεωρείται απρόσιτος και η επικοινωνία είναι σπασμένη. Ένα χαρακτηριστικό διάστημα για την ανταλλαγή Hello πακέτων είναι 10 δευτερόλεπτα, και μια χαρακτηριστική νεκρή περίοδος είναι τέσσερις φορές αυτή.

Link State Flooding

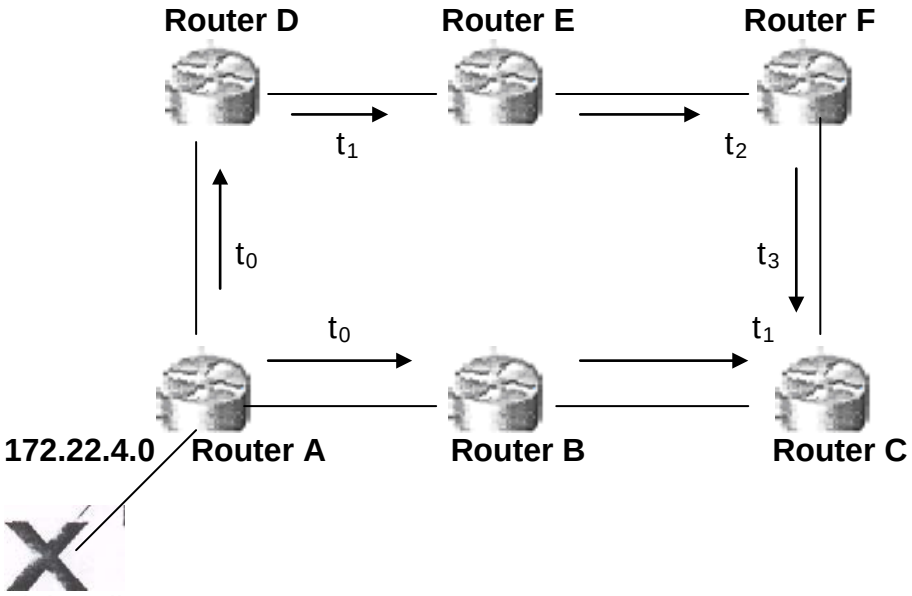
Αφότου καθιερώνονται οι γείτονες, οι δρομολογητές μπορούν να αρχίσουν να στέλνουν LSAs. Όπως ο όρος *πλημμύρα* υπονοεί, οι διαφημίσεις στέλνονται σε κάθε γείτονα. Στη συνέχεια, κάθε λαμβανόμενο LSA αντιγράφεται και διαβιβάζεται σε κάθε γείτονα εκτός από αυτόν που έστειλε το LSA. Αυτή η διαδικασία είναι η πηγή από ένα από τα πλεονεκτήματα του link state επί του διανύσματος απόστασης. Τα LSAs διαβιβάζονται σχεδόν αμέσως, εκτιμώντας ότι το διάνυσμα απόστασης πρέπει να τρέξει τον αλγόριθμό του και να ενημερώσει τον πίνακα διαδρομών του πριν οι αναπροσαρμογές δρομολόγησης, ακόμη και οι προκαλούμενες, μπορούν να διαβιβαστούν. Κατά συνέπεια, τα link state πρωτόκολλα συγκλίνουν πολύ γρηγορότερα από τα διανυσματικά πρωτόκολλα απόστασης όταν αλλάζει η τοπολογία. Η διαδικασία της πλημμύρας είναι το πιο περίπλοκο κομμάτι ενός link state πρωτοκόλλου. Υπάρχουν διάφοροι τρόποι να κατασταθεί η πλημμύρα αποδοτικότερη και πιο αξιόπιστη, όπως η χρησιμοποίηση μονής και πολλαπλής διανομής διευθύνσεις, checksums και θετικά acknowledgments. Δύο διαδικασίες, είναι σημαντικές στην διαδικασία πλημμύρας: sequencing και aging.

Αριθμοί ακολουθίας

Μια δυσκολία με την πλημμύρα, όπως περιγράφεται μέχρι τώρα, είναι ότι όταν λάβουν όλοι οι δρομολογητές όλα τα LSAs, η πλημμύρα πρέπει να σταματήσει. Μια time-to-live αξία στα πακέτα θα μπορούσε απλά να στηριχθεί για να λήξει, αλλά είναι μετά βίας αποδοτικό να επιτραπεί LSAs για να περιπλανηθεί το internetwork έως ότου λήγουν. Πάρτε το internetwork στο σχήμα 4.7. Το υποδίκτυο 172.22.4.0 στο δρομολογητή A έχει αποτύχει, και ο A έχει πλημμυρίσει ένα LSA στους γείτονές του B και D, που διαφημίζουν τη νέα κατάσταση της σύνδεσης. B και D πλημμυρίζουν τους γείτονές τους, και τα λοιπά.

Δείτε μετά αυτό που συμβαίνει στο δρομολογητή C. Ένα LSA φθάνει από το δρομολογητή B στο χρόνο t^1, εισάγεται στην τοπολογική βάση δεδομένων του C και διαβιβάζεται στο δρομολογητή F. Σε χρόνο t_3, ένα

άλλο αντίγραφο του ίδιου LSA φθάνει από τη μακριά διαδρομή A-D-E-F-C. Ο δρομολογητής C βλέπει ότι έχει ήδη το LSA στη βάση δεδομένων του και η ερώτηση είναι, εάν διαβιβάσει ο C, αυτό το LSA στο δρομολογητή B. Η απάντηση είναι όχι, επειδή ο B έχει λάβει ήδη τη διαφήμιση. Ο δρομολογητής C το ξέρει αυτό, επειδή ο αριθμός ακολουθίας του LSA που έλαβε από το δρομολογητή F είναι ο ίδιος με τον αριθμό ακολουθίας του LSA που έλαβε νωρίτερα από το δρομολογητή B.



Σχήμα 4.7
Όταν μια αλλαγή τοπολογίας συμβεί, τα LSA θα διαφημίσουν την αλλαγή σε ολόκληρο το internetwork.

Όταν ο δρομολογητής A έστειλε το LSA, περιέλαβε έναν ίδιο αριθμό ακολουθίας σε κάθε αντίγραφο. Αυτός ο αριθμός ακολουθίας καταγράφεται στις τοπολογικές βάσεις δεδομένων των δρομολογητών μαζί με το υπόλοιπο του LSA, όταν ένας δρομολογητής λαμβάνει ένα LSA που είναι ήδη στη βάση δεδομένων και ο αριθμός ακολουθίας είναι ο ίδιος, οι λαμβανόμενες πληροφορίες απορρίπτονται. Εάν οι πληροφορίες είναι ίδιες αλλά ο αριθμός ακολουθίας είναι μεγαλύτερος, οι λαμβανόμενες πληροφορίες και ο νέος αριθμός ακολουθίας εισάγονται στη βάση δεδομένων και το LSA είναι πλημμυρισμένο. Κατ' αυτό τον τρόπο, η πλημμύρα μειώνεται όταν δουν όλοι οι δρομολογητές ένα αντίγραφο του πιο πρόσφατου LSA. Όπως περιγράφεται μέχρι τώρα, φαίνεται ότι οι

δρομολογητές θα μπορούσαν μόνο να ελέγξουν ότι οι link state βάσεις δεδομένων τους περιέχουν το ίδιο LSA με το πρόσφατα λαμβανόμενο LSA και κάνουν μια πλημμύρα/απόρριψη της απόφασης βασισμένοι σε εκείνες τις πληροφορίες, χωρίς ανάγκη ενός αριθμού ακολουθίας. Αλλά φανταστείτε ότι αμέσως μετά την αποτυχία του δικτύου 172.22.4.0 του σχήματος 4.7, επανήλθε. Ο δρομολογητής A μπορεί να στείλει ένα LSA που διαφημίζει το δίκτυο ως κάτω, με έναν αριθμό ακολουθίας 166, κατόπιν στέλνει ένα νέο LSA που αναγγέλλει το ίδιο δίκτυο ως επάνω, με έναν αριθμό ακολουθίας 167. Ο δρομολογητής C λαμβάνει το κάτω LSA και έπειτα το επάνω LSA από την πορεία A-B-C, αλλά έπειτα λαμβάνει καθυστερημένα το κάτω LSA από την πορεία A-D-E-F-C. Χωρίς τους αριθμούς ακολουθίας, ο C δεν ξέρει εάν πρέπει ή όχι να πιστέψει το καθυστερημένο LSA που δείχνει κάτω. Με τους αριθμούς ακολουθίας, η βάση δεδομένων του C θα δείξει ότι οι πληροφορίες από το δρομολογητή A έχουν έναν αριθμό ακολουθίας 167, το τελευταίο LSA έχει έναν αριθμό ακολουθίας 166 και επομένως αναγνωρίζεται ως παλαιά πληροφορία και απορρίπτεται. Επειδή οι αριθμοί ακολουθίας φέρονται σε έναν καθορισμένο τομέα μέσα στο LSA, οι αριθμοί πρέπει να δεσμεύσουν κάποιο ανώτερο. Τι θα γίνει όταν αυτός ο ανώτερος αριθμός ακολουθίας χρησιμοποιηθεί;

Linear Sequence Number Spaces

Μια προσέγγιση είναι να χρησιμοποιηθεί ένα γραμμικό διάστημα αριθμού ακολουθίας τόσο μεγάλο που θα είναι απίθανο το ανώτερο όριο να επιτευχθεί ποτέ. Εάν, παραδείγματος χάριν, ένας τριανταδυάμπιτος τομέας χρησιμοποιείται, υπάρχουν 2^{32} = 4.294.967.296 διαθέσιμοι αριθμοί ακολουθίας αρχίζοντας από μηδέν. Ακόμα κι αν ένας δρομολογητής δημιουργούσε ένα νέο link state πακέτο κάθε 10 δευτερόλεπτα, θα διαρκούσε περίπου 1361 έτη για να εξαντλήσει τον ανεφοδιασμό αριθμού ακολουθίας, πολύ λίγοι δρομολογητές αναμένονται να διαρκέσουν τόσο πολύ. Σε αυτόν τον ατελή κόσμο, δυστυχώς, οι δυσλειτουργίες εμφανίζονται. Εάν μια διαδικασία δρομολόγησης link state κατά κάποιο τρόπο ξεμείνει από τους αριθμούς ακολουθίας, πρέπει να

κλείσει και να μείνει κάτω για μεγάλο χρονικό διάστημα μέχρι το LSA του να παλιώσει στις βάσεις δεδομένων πριν αρχίσει ξανά στο χαμηλότερο αριθμό ακολουθίας (δείτε το τμήμα "Aging" αργότερα σε αυτό το κεφάλαιο).

Μια πιο κοινή δυσκολία παρουσιάζεται κατά τη διάρκεια των καινούριων ξεκινημάτων των δρομολογητών. Εάν ο δρομολογητής Α ξανά ξεκινήσει, πιθανώς δεν θα θυμάται κανέναν αριθμό ακολουθίας που χρησιμοποίησε τελευταία και πρέπει να αρχίσει πάλι, για παράδειγμα, από ένα. Αλλά εάν οι γείτονές του έχουν ακόμα τους προηγούμενους αριθμούς ακολουθίας του δρομολογητή Α στις βάσεις δεδομένων τους, οι χαμηλότεροι αριθμοί ακολουθίας θα ερμηνευθούν ως παλαιότεροι αριθμοί ακολουθίας και θα αγνοηθούν. Πάλι, η διαδικασία δρομολόγησης πρέπει να μείνει κάτω έως ότου γεράσουν όλα παλαιά LSAs από το internetwork. Δεδομένου ότι μια μέγιστη ηλικία μπορεί να είναι μια ώρα ή περισσότερο, αυτή η λύση δεν είναι πολύ ελκυστική. Μια καλύτερη λύση είναι να προστεθεί ένας νέος κανόνας στην πλημμυρίζοντα συμπεριφορά που περιγράφεται ως εδώ: Εάν ένας δρομολογητής που ξανά ξεκινάει διανέμει σε έναν γείτονα ένα LSA με έναν αριθμό ακολουθίας που εμφανίζεται να είναι παλαιότερος από τον αποθηκευμένο αριθμό ακολουθίας του γείτονα, ο γείτονας θα στείλει το αποθηκευμένο LSA του και τον αριθμό ακολουθίας πίσω στο δρομολογητή. Ο δρομολογητής θα μάθει έτσι τον αριθμό ακολουθίας που χρησιμοποιούσε προτού να ξανά ξεκινήσει και θα μπορέσει να ρυθμίσει αναλόγως. Προσοχή πρέπει να ληφθεί, εντούτοις, ότι ο τελευταίος-χρησιμοποιημένος αριθμός ακολουθίας δεν ήταν κοντά στο μέγιστο, διαφορετικά, αυτός ο δρομολογητής θα πρέπει απλά να ξανά ξεκινήσει πάλι. Ένας κανόνας πρέπει να τεθεί περιορίζοντας το "άλμα" που ο δρομολογητής μπορεί να κάνει στη σειρά των αριθμών — παραδείγματος χάριν, ένας κανόνας μπορεί να πει ότι οι αριθμοί ακολουθίας δεν μπορούν κάνετε μια ενιαία αύξηση περισσότερη του ενός και μισού του συνολικού διαστήματος των αριθμών ακολουθίας. (Οι πραγματικοί τύποι είναι πιο σύνθετοι από αυτό το παράδειγμα, λαμβάνοντας υπόψη τους περιορισμούς ηλικίας.) Το IS-IS χρησιμοποιεί ένα τριανταδυάμπιτο γραμμικό διάστημα αριθμών ακολουθίας.

Κυκλικά διαστήματα αριθμών ακολουθίας

Μια άλλη προσέγγιση είναι να χρησιμοποιηθεί ένα κυκλικό διάστημα αριθμών ακολουθίας, όπου οι αριθμοί "τυλίγουν "— που σημαίνει, σε ένα διάστημα 32-bit - ο αριθμός που ακολουθεί το 4.294.967.295 είναι το 0. Οι δυσλειτουργίες μπορούν να προκαλέσουν ενδιαφέροντα διλήμματα εδώ, επίσης.

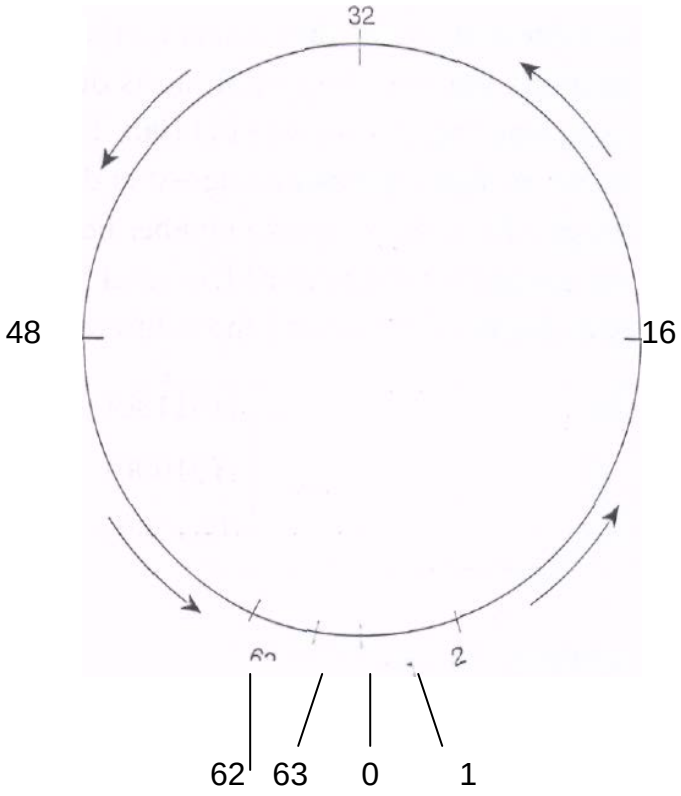
Η κυκλική αρίθμηση ακολουθίας δημιουργεί ένα παράλογο κομμάτι. Εάν το X είναι οποιοσδήποτε αριθμός μεταξύ 1 και 4.294.967.295 συμπεριλαμβανόντων, τότε 0 < X < 0. Αυτή η κατάσταση μπορεί να ρυθμιστεί σε καλώς συμπεριφερόμενα internetworks με τη βεβαίωση δύο κανόνων για όταν ένας αριθμός ακολουθίας είναι μεγαλύτερος από ή μικρότερος από έναν άλλο αριθμό ακολουθίας. Έχοντας ένα διάστημα αριθμών ακολουθίας *n* και δύο αριθμούς ακολουθίας *a* και *b*, το *a* θεωρείται πιο πρόσφατος σε καθεμία από τις ακόλουθες καταστάσεις:

- a > b, *και* (a - b) < n/2
- a < b, *και* (b - a) > n/2

Χάριν της απλότητας, πάρτε ένα διάστημα αριθμού ακολουθίας έξι bit, που παρουσιάζεται στο σχήμα 4.8:

$n = 2^6 = 64$, άρα $n/2 = 32$.

Σχήμα 4.8
Ένα εξάμπιτο κυκλικό διάστημα διευθύνσεων.



Λαμβάνοντας υπόψη δύο αριθμούς ακολουθίας 48 και 18, ο 48 είναι πιο πρόσφατος, από τον κανόνα (1):

48>18 και (48-18)=30, και 30 < 32.

Λαμβάνοντας υπόψη δύο αριθμούς ακολουθίας 3 και 48, ο 3 είναι πιο πρόσφατος, από τον κανόνα (2):

3<48 και (48 - 3) = 45, και 45 > 32.

Λαμβάνοντας υπόψη δύο αριθμούς ακολουθίας 3 και 18, ο 18 είναι πιο πρόσφατος, από τον κανόνα (1):

18 > 3 και (18 - 3) = 15, και 15<32.

Έτσι οι κανόνες φαίνονται να επιβάλλουν την κυκλικότητα.

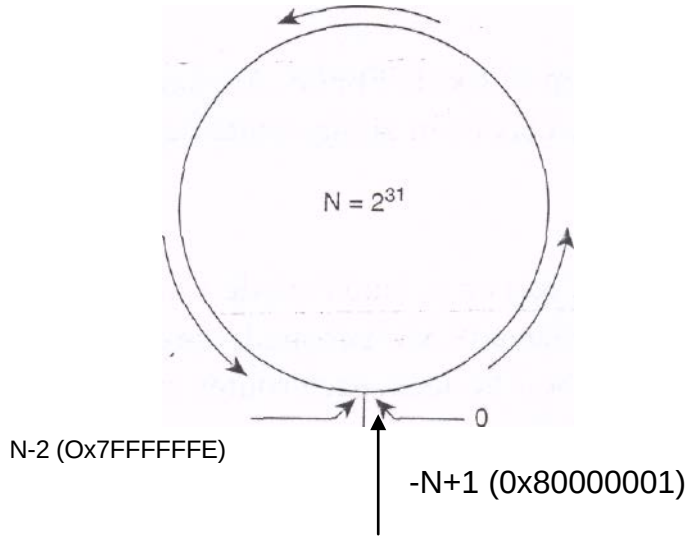
Lollipop-Shaped Sequence Number Spaces

Lollipop-shaped διάστημα αριθμών ακολουθίας είναι ένα υβρίδιο των γραμμικών και κυκλικών διαστημάτων αριθμού ακολουθίας, εάν το σκεφτείτε, ένα lollipop έχει ένα γραμμικό και ένα κυκλικό συστατικό. Το πρόβλημα με τα κυκλικά διαστήματα είναι ότι δεν υπάρχει κανένας αριθμός μικρότερος από όλους τους άλλους αριθμούς. Το πρόβλημα με τα γραμμικά διαστήματα είναι ότι δεν είναι —καλά —κυκλικά. Δηλαδή, το σύνολο των αριθμών ακολουθίας είναι πεπερασμένο. Όταν ο δρομολογητής Α ξανά ξεκινήσει, αυτό θα ήταν καλό να αρχίσει με έναν αριθμό *a* που είναι μικρότερος από όλους τους άλλους αριθμούς. Οι γείτονες θα αναγνωρίσουν αυτόν τον αριθμό για αυτό που είναι και εάν έχουν έναν αριθμό προ-καινούριου ξεκινήματος *b* στις βάσεις δεδομένων τους από το δρομολογητή Α, μπορούν να στείλουν αυτόν τον αριθμό στο δρομολογητή Α και ο δρομολογητής Α, θα πηδήσει σε εκείνον τον αριθμό ακολουθίας. Ο δρομολογητής Α μπορεί να είναι σε θέση να στείλει περισσότερα από ένα LSA πριν ακούσει για τον αριθμό ακολουθίας που χρησιμοποιούσε πριν ξανά ξεκινήσει. Επομένως, είναι σημαντικό να υπάρξουν αρκετοί αριθμοί καινούριου ξεκινήματος έτσι ώστε ο Α να μην να τους χρησιμοποιήσει όλους προτού να τον ενημερώσουν οι γείτονες είτε για τον προηγουμένως χρησιμοποιούμενο αριθμό είτε τις προηγουμένως χρησιμοποιημένες ηλικίες αριθμού από όλες τις βάσεις δεδομένων. Αυτοί οι κυκλικοί αριθμοί επανεκκίνησης όταν έχουν χρησιμοποιηθεί, ή αφού ένας γείτονας έχει δώσει έναν αριθμό ακολουθίας στον οποίο ο Α μπορεί να πηδήσει, ο Α εισάγει ένα κυκλικό διάστημα αριθμών.

Ένας τρόπος να σχεδιαστεί ένα διάστημα διευθύνσεων lollipop είναι να χρησιμοποιηθούν οι υπογεγραμμένοι αριθμοί ακολουθίας, όπου - $K < 0 < K$. Οι αρνητικοί αριθμοί που μετρούν επάνω το – *K* μέχρι το 1 και οι θετικοί αριθμοί από το 0 ως *το K* είναι το κυκλικό διάστημα. Οι κανόνες του Perlman για τους αριθμούς ακολουθίας είναι ως εξής. Λαμβάνοντας υπόψη δύο αριθμούς *α* και *b* και ένας αριθμός ακολουθίας διαστήματος n*, το b* είναι πιο πρόσφατο από εάν και μόνο εάν:

1. $a < 0$ και $a < b$, ή
2. $a > 0$, $a < b$, και $(b - a) < n/2$, ή
3. $a > 0$, $b > 0$, $a > b$, και $(a - b) > n/2$.

Το σχήμα 3.9 δείχνει μια εφαρμογή του lollipop-shaped διαστήματος αριθμών ακολουθίας. Ένας τριανταδυάμπιτος υπογεγραμμένος αριθμός διαστήματος N χρησιμοποιείται, παράγοντας 2^{31} θετικούς αριθμούς και 2^{31} αρνητικούς αριθμούς. - N (-2^{31} , ή 0x80000000) και N- 1(2^{31} - 1, ή 0x 7FFFFFFF) δεν χρησιμοποιούνται. Ένας δρομολογητής που έρχεται on-line θα αρχίσει τους αριθμούς ακολουθίας του από -N + 1 (0x80000001) και θα το αυξήσει μέχρι το μηδέν, όταν έχει εισαγάγει το κυκλικό διάστημα αριθμού. Όταν η ακολουθία φθάνει στο N - 2 (0x7FFFFFFE), τα περικαλύμματα ακολουθίας γίνονται πάλι μηδέν (πάλι, η N-1 είναι αχρησιμοποίητη). Έπειτα, υποθέστε τα καινούρια ξεκινήματα δρομολογητών. Ο αριθμός ακολουθίας του τελευταίου LSA που στέλνεται πριν από το καινούριο ξεκίνημα είναι 0x00005de3 (μέρος του κυκλικού διαστήματος ακολουθίας). Δεδομένου ότι συγχρονίζει τη βάση δεδομένων του με το γείτονά του μετά από το καινούριο ξεκίνημα, ο δρομολογητής στέλνει ένα LSA με έναν αριθμό ακολουθίας 0x80000001 (-N+ 1) . Ο γείτονας εξετάζει τη βάση δεδομένων του και βρίσκει το LSA προ-καινούριου ξεκινήματος με έναν αριθμό ακολουθίας 0x00005de3. Ο γείτονας στέλνει αυτό το LSA στον καινούριο δρομολογητή, λέγοντας ουσιαστικά, "Αυτό είναι από τότε που φύγατε."



Σχήμα 4.9
Ένα lollipop-shaped διάστημα αριθμών ακολουθίας.

Ο καινούριος δρομολογητής καταγράφει έπειτα το LSA με το θετικό αριθμό ακολουθίας. Εάν πρέπει να στείλει ένα νέο αντίγραφο του LSA σε κάποια στιγμή στο μέλλον, ο νέος αριθμός ακολουθίας θα είναι 0x00005de6.

Τα διαστήματα ακολουθίας Lollipop χρησιμοποιήθηκαν με την αρχική έκδοση OSPF, OSPFvl (RFC 1131). Αν και η χρήση των υπογεγραμμένων αριθμών ήταν μια βελτίωση πέρα από το γραμμικό διάστημα αριθμού, το κυκλικό μέρος βρέθηκε να είναι τρωτό στις ίδιες ασάφειες ως ένα καθαρό κυκλικό διάστημα. Η επέκταση του OSPFvl ποτέ δεν προχώρησε πέρα από το πειραματικό στάδιο. Η τρέχουσα έκδοση OSPF, OSPFv2 (αρχικά εξειδικευμένη στο RFC 1247) υιοθετεί τα καλύτερα χαρακτηριστικά γνωρίσματα των διαστημάτων γραμμικού και lollipop αριθμού ακολουθίας. Χρησιμοποιεί ένα υπογεγραμμένο διάστημα αριθμού όπως τους αριθμούς ακολουθίας lollipop, αρχίζοντας με 0x80000001. Εντούτοις, όταν ο αριθμός ακολουθίας γίνεται θετικός, το διάστημα ακολουθίας συνεχίζει να είναι γραμμικό έως ότου φθάνει στο μέγιστο 0x7FFFFFFF. Σε αυτό το σημείο η διαδικασία OSPF πρέπει να ξεπλύνει το LSA από όλες τις link state βάσεις δεδομένων πριν ξανά ξεκινήσει.

Aging

Το σχήμα LSA πρέπει να περιλάβει έναν τομέα για την ηλικία της διαφήμισης. Όταν ένα LSA δημιουργείται, ο δρομολογητής θέτει αυτόν τον τομέα σε μηδέν. Δεδομένου ότι το πακέτο είναι πλημμυρισμένο, κάθε δρομολογητής αυξάνει την ηλικία της διαφήμισης. Αυτή η διαδικασία προσθέτει ένα άλλο στρώμα στην αξιοπιστία της διαδικασίας πλημμύρας. Το πρωτόκολλο καθορίζει μια μέγιστη διαφοράς ηλικίας (MaxAgeDiff) τιμή για το internetwork. Ένας δρομολογητής μπορεί να λάβει πολλαπλάσια αντίγραφα του ίδιου LSA με τους ίδιους αριθμούς ακολουθίας αλλά με διαφορετικές ηλικίες. Εάν η διαφορά στις ηλικίες είναι χαμηλότερη από το MaxAgeDiff, υποτίθεται ότι η διαφορά ηλικίας ήταν το αποτέλεσμα των κανονικών καθυστερήσεων του δικτύου, το αρχικό LSA διατηρείται στη βάση

δεδομένων και το νεώτερο LSA (με τη μεγαλύτερη ηλικία) δεν είναι πλημμυρισμένο. Εάν η διαφορά είναι μεγαλύτερη από την MaXAgeDiff τιμή, υποτίθεται ότι μια ανωμαλία έχει εμφανιστεί στο internetwork στο οποίο ένα νέο LSA εστάλη χωρίς αύξηση του αριθμού ακολουθίας. Σε αυτήν την περίπτωση, το νεώτερο LSA θα καταγραφεί και το πακέτο θα πλημμυρίσει. Μια χαρακτηριστική MaxAgeDiff τιμή είναι 15 λεπτά (που χρησιμοποιούνται από OSPF).

Η ηλικία ενός LSA συνεχίζει να αυξάνεται καθώς βρίσκεται σε μια link state βάση δεδομένων. Εάν η ηλικία για ένα link state αρχείο αυξάνεται μέχρι κάποια μέγιστη ηλικία (MaxAge) - πάλι καθορισμένη από το συγκεκριμένο πρωτόκολλο δρομολόγησης - το LSA, με τον τομέα ηλικίας καθορισμένο με την MaxAge τιμή, πλημμυρίζεται σε όλους τους γείτονες και το αρχείο διαγράφεται από τις βάσεις δεδομένων.

Εάν το LSA πρόκειται να ξεπλυθεί από όλες τις βάσεις δεδομένων όταν επιτυγχάνεται η MaxAge, πρέπει να υπάρξει ένας μηχανισμός για να επικυρώσει περιοδικά το LSA και να επαναριθμήσει το χρονόμετρό του προτού να επιτευχθεί η MaxAge. Ένας χρόνος ανανέωσης link state καθορίζεται (LSRefeshTime), όταν αυτός ο χρόνος λήξει, ένας δρομολογητής πλημμυρίζει ένα νέο LSA σε όλους τους γείτονές του, οι οποίοι θα επαναριθμήσουν την ηλικία των αρχείων που στάλθηκαν από τον δρομολογητή στη νέα λαμβανόμενη ηλικία. Το OSPF καθορίζει ένα MaxAge 1 ώρας και ένα LSRefreshTime 30 λεπτών.

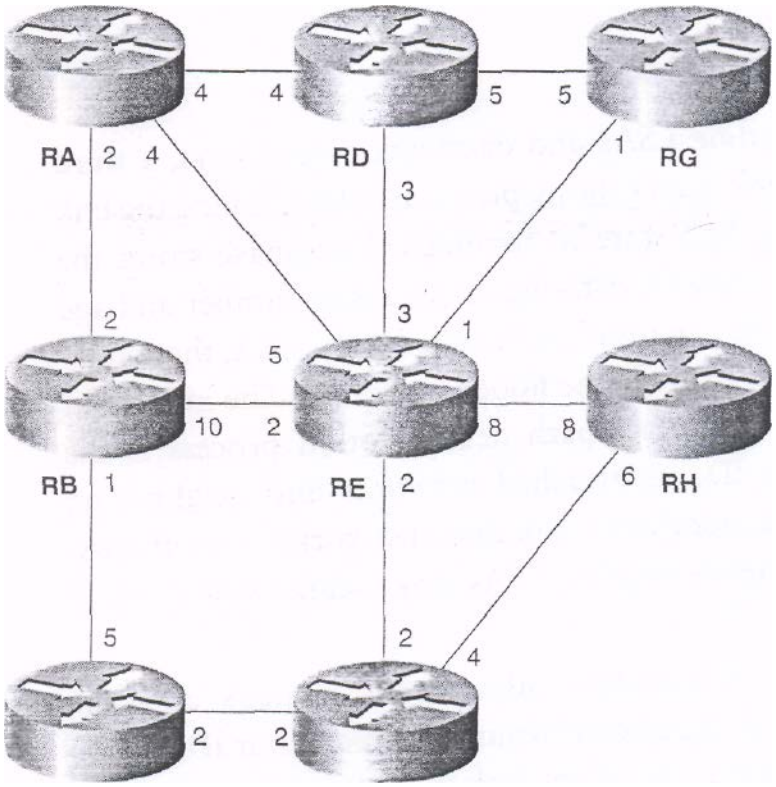
The Link State Database

Εκτός από την πλημμύρα LSAs και την ανακάλυψη των γειτόνων, ένας τρίτος σημαντικός στόχος του πρωτοκόλλου δρομολόγησης link state καθιερώνει την link state βάση δεδομένων. Το link state ή η τοπολογική βάση δεδομένων αποθηκεύει το LSAs ως μια σειρά αρχείων. Αν και ένας αριθμός ακολουθίας και μια ηλικία και ενδεχομένως άλλες πληροφορίες συμπεριλαμβάνονται στο LSA, αυτές οι μεταβλητές υπάρχουν κυρίως για να διαχειριστούν την διαδικασία πλημμύρας. Οι σημαντικές πληροφορίες για

την πιο σύντομη διαδικασία προσδιορισμού πορειών είναι η ταυτότητα του δρομολογητή διαφήμισης, τα συνημμένα δίκτυα και οι γειτονικοί δρομολογητές του και το κόστος που συνδέεται με εκείνα τα δίκτυα ή γείτονες. Όπως η προηγούμενη πρόταση υπονοεί, τα LSAs μπορεί να περιλάβουν δύο τύπους γενικών πληροφοριών:

- Οι πληροφορίες συνδέσεων δρομολογητών διαφημίζουν τους παρακείμενους γείτονες ενός δρομολογητή με μια τριπλέτα (ταυτότητας δρομολογητών, ταυτότητας γειτόνων, κόστος), όπου το κόστος είναι το κόστος της σύνδεσης με το γείτονα.
- Οι πληροφορίες δικτύων στελεχών διαφημίζουν τα άμεσα συνδεδεμένα δίκτυα στελεχών ενός δρομολογητή (δίκτυα χωρίς γείτονες) με μια τριπλέτα (ταυτότητας δρομολογητών, ταυτότητας δικτύων, κόστος).

Ο πιο σύντομος πρώτος (spf) αλγόριθμος πορειών οργανώνεται μία φορά για τις πληροφορίες συνδέσεων δρομολογητών για να καθιερώσει τις κοντύτερες πορείες σε κάθε δρομολογητή και έπειτα οι πληροφορίες δικτύων στελεχών χρησιμοποιούνται για να προσθέσουν αυτά τα δίκτυα στους δρομολογητές. Το σχήμα 4.10 παρουσιάζει ένα internetwork των δρομολογητών και των συνδέσεων μεταξύ τους, τα δίκτυα στελεχών δεν παρουσιάζονται για χάρη της απλότητας. Παρατηρήστε ότι διάφορες συνδέσεις έχουν διαφορετικό κόστος που συνδέεται μαζί τους σε κάθε τέλος. Ένα κόστος συνδέεται με την εξερχόμενη κατεύθυνση μιας διεπαφής. Παραδείγματος χάριν, η σύνδεση από RB σε RC έχει ένα κόστος 1, αλλά η ίδια σύνδεση έχει ένα κόστος 5 από RC σε RB κατεύθυνση.



Σχήμα 4.10
Το κόστος σύνδεσης υπολογίζεται για την εξερχόμενη κατεύθυνση από μια διεπαφή και δεν είναι αναγκαίο να είναι ίδιο σε όλες τις διεπαφές του internetwork.

Ο πίνακας 4.2 παρουσιάζει μια γενική link state βάση δεδομένων για το internetwork του σχήματος 4.10, ένα αντίγραφο του οποίου αποθηκεύεται σε κάθε δρομολογητή. Όπως διαβάζετε αυτή τη βάση δεδομένων, θα δείτε ότι περιγράφει εντελώς το internetwork. Τώρα είναι δυνατό να υπολογιστεί ένα δέντρο που περιγράφει την κοντύτερη πορεία σε κάθε δρομολογητή με το τρέξιμο του SPF αλγορίθμου.

Πίνακας 4.2
Η τοπολογιακή βάση δεδομένων για το internetwork του σχήματος 4.10

Router ID	Neighbor	Cost
RA	RB	2
RA	RD	4
RA	RE	4

RB	RA	2
RB	RC	1
RB	RE	10
RC	RB	5
RC	RF	2
RD	RA	4
RD	RE	3
RD	RG	5
RE	RA	5
RE	RB	2
RE	RD	3
RE	RF	2
RE	RG	1
RE	RH	8
RF	RC	2
RF	RE	2
RF	RH	4
RG	RD	5
RG	RE	1
RH	RE	8
RH	RF	6

Περιοχές

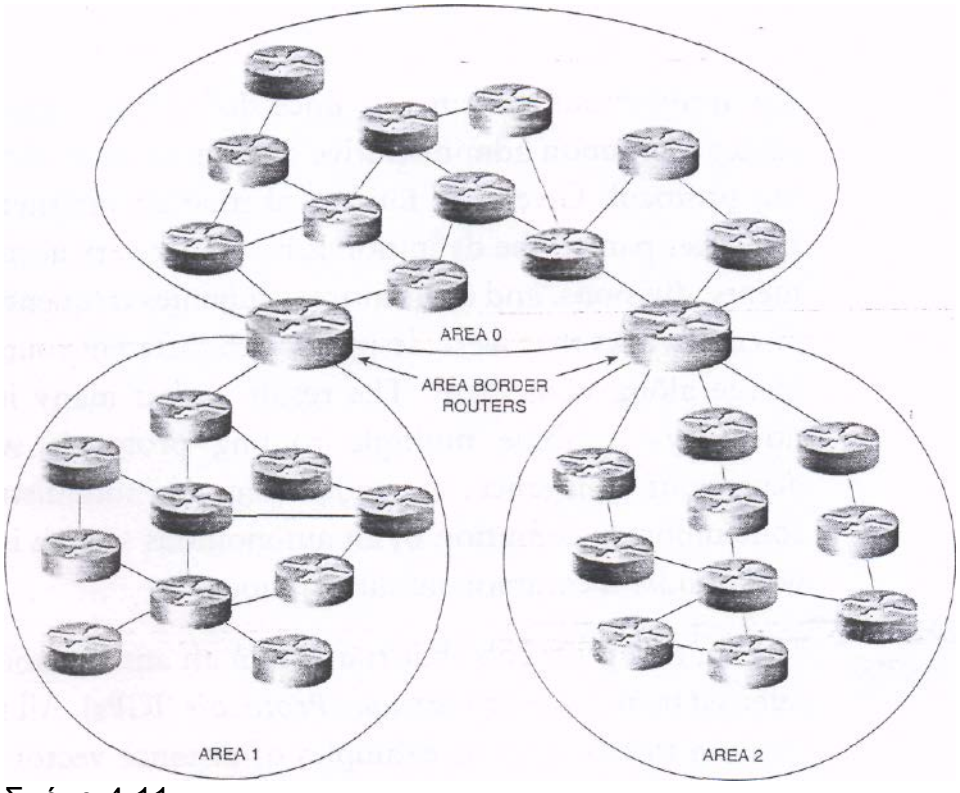
Μια *περιοχή* είναι ένα υποσύνολο των δρομολογητών που αποτελούν ένα Internetwork. Η διαίρεση ενός internetwork σε περιοχές είναι μια απάντηση σε τρεις ανησυχίες που εκφράζονται συνήθως για τα link state πρωτόκολλα:

- Οι απαραίτητες βάσεις δεδομένων απαιτούν περισσότερη μνήμη από ότι ένα διανυσματικό πρωτόκολλο απόστασης απαιτεί.
- Ο σύνθετος αλγόριθμος απαιτεί περισσότερο χρόνο ΚΜΕ από ότι ένα διανυσματικό πρωτόκολλο απόστασης απαιτεί.
- Η πλημμύρα των link state πακέτων έχει επιπτώσεις στο διαθέσιμο εύρος ζώνης, ιδιαίτερα στα ασταθή internetworks.

Τα σύγχρονα link state πρωτόκολλα και οι δρομολογητές που τους τρέχουν σχεδιάζονται για να μειώσουν αυτά τα αποτελέσματα, αλλά δεν μπορούν να τα αποβάλουν. Το τελευταίο τμήμα εξετάζει πως η link state βάση δεδομένων μπορεί να μοιάσει και πώς ένας SPF αλγόριθμος μπορεί να λειτουργήσει, για ένα μικρό οκτώ-δρομολογητών internetwork. Θυμηθείτε ότι τα δίκτυα στελεχών που θα ήταν συνδεμένα με εκείνους τους οκτώ δρομολογητές και θα διαμόρφωναν τα φύλλα του SPF δέντρου δεν λήφθηκαν υπόψη. Τώρα φανταστείτε έναν 8000-δρομολογητών internetwork, μπορείτε να καταλάβετε την ανησυχία για τον αντίκτυπο στη μνήμη, την ΚΜΕ και το εύρος ζώνης.

Αυτός ο αντίκτυπος μπορεί να μειωθεί πολύ με την χρήση των περιοχών, όπως στο σχήμα 4.11. Όταν ένα internetwork υποδιαιρείται σε περιοχές, οι δρομολογητές μέσα σε μια περιοχή χρειάζονται την πλημμύρα LSAs μόνο μέσα σε εκείνη την περιοχή και επομένως πρέπει να διατηρήσουν μια link state βάση δεδομένων μόνο για εκείνη την περιοχή. Η μικρότερη βάση δεδομένων σημαίνει λιγότερη απαραίτητη μνήμη σε κάθε δρομολογητή και λιγότερους κύκλους ΚΜΕ για να τρέξει τον SPF αλγόριθμο σε εκείνη την βάση δεδομένων. Εάν εμφανιστούν συχνές αλλαγές τοπολογίας, η προκύπτουσα πλημμύρα θα περιοριστεί στην περιοχή της αστάθειας.

Οι δρομολογητές που συνδέουν δύο περιοχές *(δρομολογητές συνόρων περιοχής,* στην ορολογία OSPF) ανήκουν και στις δύο περιοχές και πρέπει να διατηρήσουν χωριστές τοπολογικές βάσεις δεδομένων για κάθε μια. Ακριβώς όπως ένας οικοδεσπότης σε ένα δίκτυο που θέλει να στείλει ένα πακέτο σε ένα άλλο δίκτυο πρέπει να ξέρει πώς να βρει τον τοπικό δρομολογητή του, ένας δρομολογητής σε μια περιοχή που θέλει να στείλει ένα πακέτο σε μια άλλη περιοχή πρέπει να ξέρει πώς να βρει τον τοπικό δρομολογητή συνόρων της περιοχής του. Με άλλα λόγια, η σχέση δρομολογητών intra-area/inter-area είναι η ίδια με τη σχέση οικοδεσποτών/δρομολογητών αλλά σε πιο υψηλό ιεραρχικό επίπεδο.



Σχήμα 4.11
Η χρήση των περιοχών μειώνει την απαίτηση link state για πόρους του συστήματος.

Τα διανυσματικά πρωτόκολλα απόστασης, όπως RIP και IGRP, δεν χρησιμοποιούν τις περιοχές. Δεδομένου ότι αυτά τα πρωτόκολλα δεν έχουν καμία προσφυγή αλλά να θεωρήσουν ένα μεγάλο internetwork ως μια ενιαία οντότητα, πρέπει να υπολογίσετε μια διαδρομή σε κάθε δίκτυο, και πρέπει

να broadcast τον προκύπτοντα τεράστιο πίνακα διαδρομών κάθε 30 ή 90 δευτερόλεπτα, γίνεται σαφές ότι τα link state πρωτόκολλα που χρησιμοποιούν τις περιοχές μπορούν πραγματικά να σώσουν τους πόρους του συστήματος.

ΕΣΩΤΕΡΙΚΑ ΚΑΙ ΕΞΩΤΕΡΙΚΑ ΠΡΩΤΟΚΟΛΛΑ ΠΥΛΩΝ

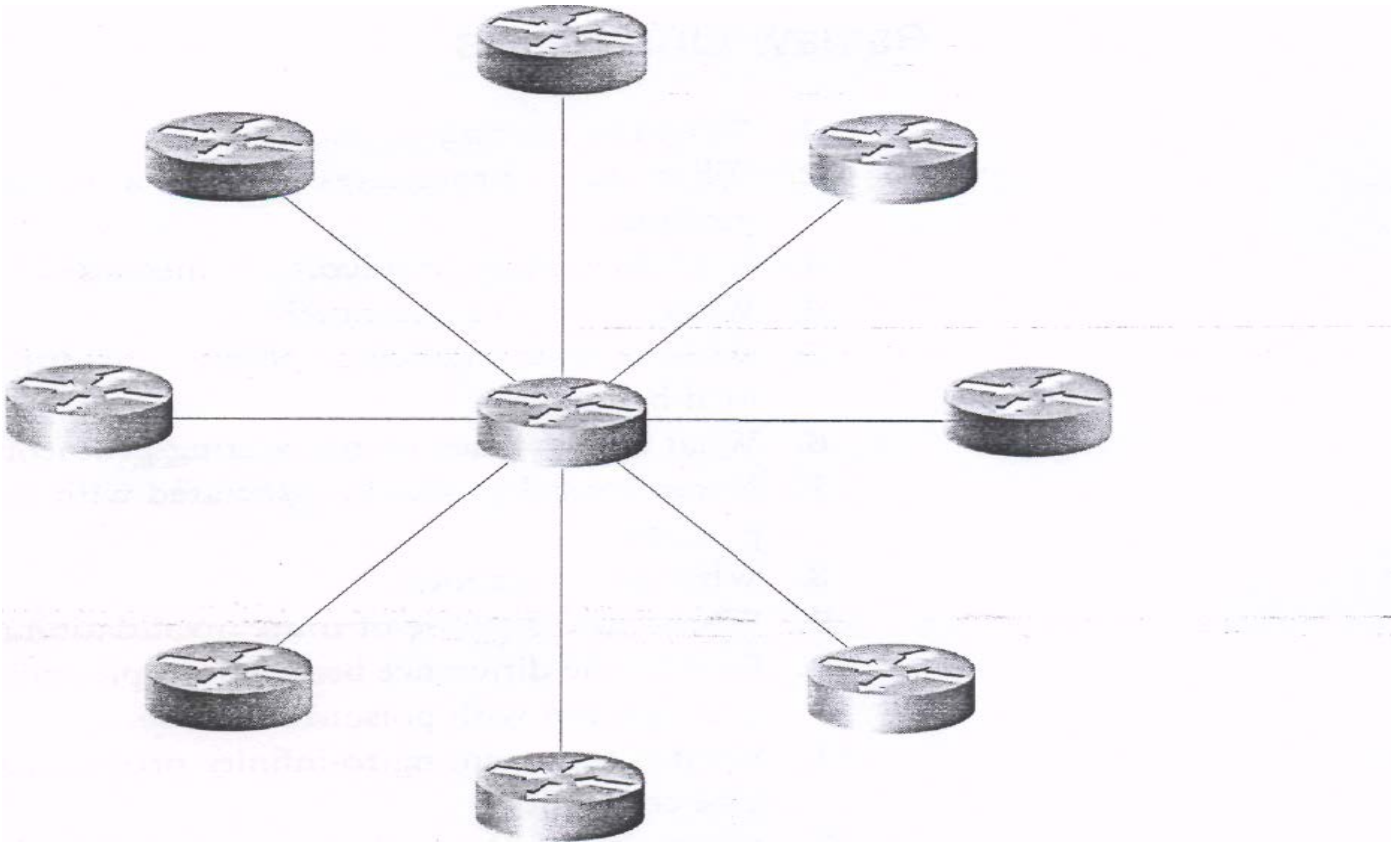
Οι περιοχές εισάγουν μια ιεραρχία στην αρχιτεκτονική internetwork. Ένα άλλο στρώμα προστίθεται σε αυτήν την ιεραρχική δομή με την ομαδοποίηση περιοχών σε μεγαλύτερες περιοχές. Αυτές οι υψηλότερου επιπέδου περιοχές καλούνται *αυτόνομα συστήματα* στον κόσμο IP και *περιοχές δρομολόγησης* στον κόσμος του ISO. Ένα αυτόνομο σύστημα ορίστηκε ως μια ομάδα δρομολογητών κάτω από μια κοινή διοικητική περιοχή που τρέχει ένα κοινό πρωτόκολλο δρομολόγησης. Λαμβάνοντας υπόψη τη ρευστότητα της σύγχρονης internetworking ζωής το τελευταίο μέρος του καθορισμού δεν είναι πλέον πολύ ακριβές. Τα τμήματα, οι κατηγορίες, ακόμη και ολόκληρες επιχειρήσεις συχνά συγχωνεύονται και τα internetworks που σχεδιάστηκαν με διαφορετικά πρωτόκολλα δρομολόγησης συγχωνεύτηκαν μαζί με αυτά. Τα πρωτόκολλα δρομολόγησης που τρέχουν μέσα σε ένα αυτόνομο σύστημα αναφέρονται ως *εσωτερικά πρωτόκολλα πυλών* (IGPs). Όλα τα πρωτόκολλα που δίνονται σε αυτό το κεφάλαιο ως παραδείγματα των διανυσματικών πρωτοκόλλων απόστασης ή link state πρωτοκόλλων είναι IGPs.

Τα πρωτόκολλα δρομολόγησης που καθοδηγούν μεταξύ των αυτόνομων συστημάτων ή των περιοχών δρομολόγησης αναφέρονται ως *εξωτερικά πρωτόκολλα πυλών* (EGPs). Εκτιμώντας ότι IGPs ανακαλύπτουν τις πορείες μεταξύ των δικτύων, EGPs ανακαλύπτουν τις πορείες μεταξύ των αυτόνομων συστημάτων. Παραδείγματα EGPs περιλαμβάνουν τα ακόλουθα:

- Πρωτόκολλο πυλών συνόρων (BGP) για IP
- Εξωτερικό πρωτόκολλο πυλών (EGP) για IP
- Το πρωτόκολλο δρομολόγησης του ISO Interdomain (IDRP).

ΣΤΑΤΙΚΗ Η ΔΥΝΑΜΙΚΗ ΔΡΟΜΟΛΟΓΗΣΗ;

Κατά την ανάγνωση όλων των λαμπρών λεπτομερειών των δυναμικών πρωτοκόλλων δρομολόγησης, είναι δύσκολο να μην έχεις την εντύπωση ότι η δυναμική δρομολόγηση είναι πάντα καλύτερη από τη στατική δρομολόγηση. Είναι σημαντικό να λάβει υπόψη ότι το αρχικό καθήκον ενός δυναμικού πρωτοκόλλου δρομολόγησης είναι να ανιχνεύσει αυτόματα και να προσαρμοστεί στις τοπολογικές αλλαγές στο internetwork.Η τιμή αυτής της "αυτοματοποίησης " καταβάλλεται στο εύρος ζώνης και ίσως στο διάστημα σειρών αναμονής, στη μνήμη, και στο χρόνο επεξεργασίας. Μια συχνή αντίρρηση στη στατική δρομολόγηση είναι ότι είναι δύσκολο να διαχειριστεί. Αυτή η κριτική μπορεί να ισχύει για το μέσο στις μεγάλες τοπολογίες με πολλές εναλλακτικές διαδρομές, αλλά δεν ισχύει βεβαίως για τα μικρά internetworks με λίγη ή καμία εναλλακτική διαδρομή. Το internetwork στο σχήμα 4.12 έχει μια hub-and-spoke τοπολογία δημοφιλή στα μικρότερα internetworks. Εάν μια ακτίνα σε οποιοδήποτε δρομολογητή σπάσει, υπάρχει καμία άλλη διαδρομή για ένα δυναμικό πρωτόκολλο δρομολόγησης να επιλέξει; Αυτό το internetwork είναι ο ιδανικός υποψήφιος για τη στατική δρομολόγηση. Διαμορφώστε μια στατική διαδρομή στον hub δρομολογητή γιατί κάθε spoke δρομολογητή και μια ενιαία διαδρομή προεπιλογής σε κάθε spoke δρομολογητή που δείχνει σε hub και το internetwork είναι έτοιμο να ξεκινήσει. Κατά το σχεδιασμό ενός internetwork, η απλούστερη λύση είναι σχεδόν πάντα η καλύτερη λύση. Είναι ορθή πρακτική να επιλεχτεί ένα δυναμικό πρωτόκολλο δρομολόγησης μόνο μετά από τον καθορισμό ότι η στατική δρομολόγηση δεν είναι μια πρακτική λύση για το σχέδιο.



Σχήμα 4.12
Αυτό το hub και spoke internetwork είναι το ιδανικό για στατική δρομολόγηση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. http://www.lab.epmhs.gr/gr/html/ptixiakes/ATM_IPv6_&_SecurityConsiderations/kefalaio2.htm

2. http://www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/teaching_m/tcpip/ipv6.htm

3. CCIE Professional Development: Routing TCP/IP, Volume I