ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

Cisco Systems

CCNA Αυτοδιδασκαλία:
Διασύνδεση Συσκευών Δικτύου Cisco (ICND)

Δεύτερη Αμερικανική έκδοση

Εγκεκριμένο από τη Cisco για αυτοδιδασκαλία στα βασικά προγράμματα εκπαίδευσης CCNA® 640-801 και ICND 640-811

ΚΛΕΙΔΑΡΙΘΜΟΣ

ciscopress.com

Επιμελητής πρωτοτύπου:
Steve McQuerry, CCIE® No. 6108

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 6

Βασική διαχείριση και μετάφραση κυκλοφορίας IP με λίστες πρόσβασης

Σε αυτό το κεφάλαιο καλύπτονται οι τυπικές και επεκτεταμένες (extended) λίστες πρόσβασης IP ως μέσο ταξινόμησης της κυκλοφορίας δικτύου. Όταν ολοκληρώσετε αυτό το κεφάλαιο, θα πρέπει να είστε σε θέση να περιγράφετε τις λειτουργίες και τις διαδικασίες με τις οποίες οι λίστες πρόσβασης καθορίζουν την κυκλοφορία, και τον τρόπο με τον οποίο οι λειτουργίες αυτές μπορούν να υλοποιηθούν σε τεχνολογίες όπως ο έλεγχος πρόσβασης (ασφάλεια), η κρυπτογράφηση, η δρομολόγηση που βασίζεται σε πολιτικές, η ποιότητα εξυπηρέτησης (Quality of Service — QoS), και η Μετάφραση Διευθύνσεων Δικτύου/Μετάφραση Διευθύνσεων Θυρών (Network Address Translation/Port Address Translation — NAT/PAT). Θα μάθετε επίσης πώς να διευθετείτε μια τυπική και μια επεκτεταμένη λίστα πρόσβασης, καθώς και να περιορίζετε την πρόσβαση μέσω Telnet προς και από το δρομολογητή χρησιμοποιώντας μια τυπική λίστα πρόσβασης. Τέλος, θα μάθετε πώς να ελέγχετε τη διευθέτηση σε λίστες πρόσβασης.

Κατανόηση των λιστών πρόσβασης

Τα δίκτυα σχεδιάζονται για να μεταφέρουν την κυκλοφορία των χρηστών από μια θέση σε μια άλλη, σαν τους δρόμους που εξυπηρετούν την οδική κυκλοφορία από μια τοποθεσία σε μια άλλη. Οι δρομολογητές αποτελούν τα σημεία σύνδεσης της κυκλοφορίας στα δίκτυα δεδομένων. Ο έλεγχος της ροής της κυκλοφορίας τόσο στους δρόμους όσο και στα δίκτυα είναι μερικές φορές απαραίτητος. Αυτό μπορεί να γίνει με πολλούς τρόπους σε έναν αυτοκινητόδρομο, αλλά σε ένα δίκτυο χρειάζεστε κάποιο τρόπο για την αναγνώριση και το φιλτράρισμα της κυκλοφορίας προς και από πολλά διαφορετικά δίκτυα δεδομένων. Για το σκοπό αυτόν, στους δρομολογητές χρησιμοποιούνται οι λίστες ελέγχου πρόσβασης (access control lists —

ACL) που αναγνωρίζουν την κυκλοφορία και κατόπιν τη φιλτράρουν, την κρυπτογραφούν, την ταξινομούν, ή τη μεταφράζουν ώστε να διαχειρίζονται και να ελέγχουν καλύτερα τις λειτουργίες του δικτύου.

Τα πρώτα δίκτυα με δρομολόγηση συνέδεαν ένα μέτριο αριθμό LAN και υπολογιστών υπηρεσίας. Καθώς αυξήθηκαν οι συνδέσεις δρομολογητών στα παραδοσιακά και τα εξωτερικά δίκτυα, και με την αυξανόμενη χρήση του Διαδικτύου, παρουσιάστηκαν νέες προκλήσεις για τον έλεγχο της πρόσβασης, όπως φαίνεται από το παράδειγμα δικτύου που παρουσιάζεται στο Σχήμα 6-1.

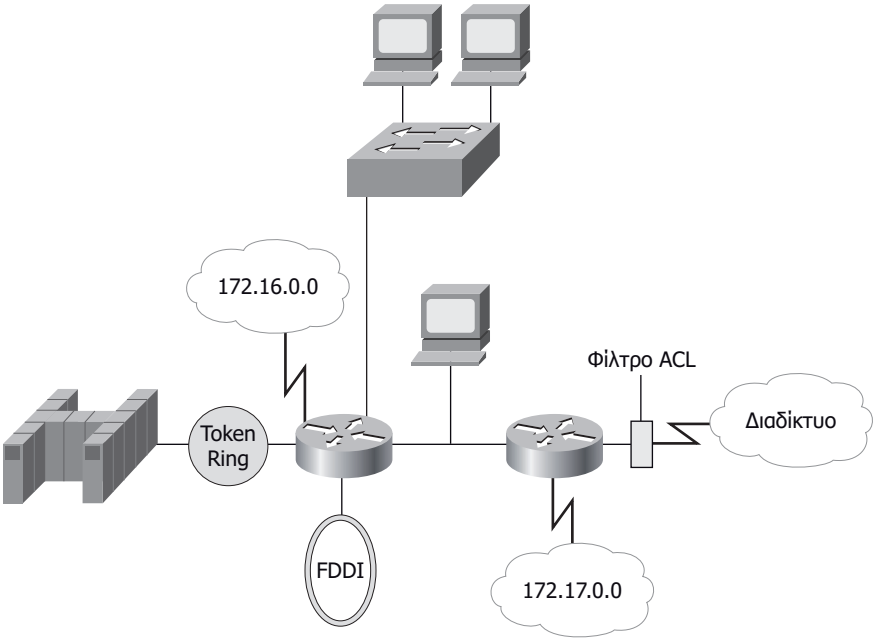
Με την αύξηση των διαφόρων τύπων συνδέσεων στα δίκτυα, οι διαχειριστές πρέπει να αποφασίζουν πώς θα απαγορεύουν τις ανεπιθύμητες συνδέσεις επιτρέποντας ταυτόχρονα την πρόσβαση όπου χρειάζεται. Αν και εργαλεία όπως οι κωδικοί πρόσβασης (passwords), οι συσκευές επανάκλησης (callback equipment), και οι φυσικές συσκευές ασφαλείας είναι χρήσιμα, συνήθως δεν παρέχουν τον ευέλικτο και συγκεκριμένο έλεγχο που προτιμούν οι περισσότεροι διαχειριστές.

Οι λίστες πρόσβασης αποτελούν ένα άλλο ισχυρό εργαλείο για τον έλεγχο των δικτύων. Επίσης, παρέχουν ευελιξία επιτρέποντας το φιλτράρισμα της ροής πακέτων προς ή από τις διασυνδέσεις των δρομολογητών. Αυτού του είδους ο έλεγχος μπορεί να βοηθήσει στον περιορισμό της κυκλοφορίας στο δίκτυο και της χρήσης του δικτύου από ορισμένους χρήστες ή συσκευές.

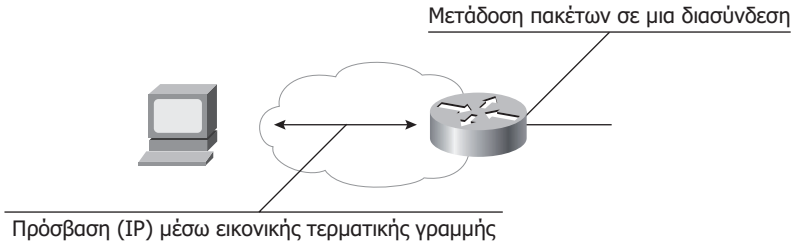
Η πιο συνηθισμένη χρήση μιας λίστας πρόσβασης είναι ως φίλτρου πακέτων (packet filter). Χωρίς φίλτρα πακέτων, όλα τα πακέτα θα μπορούσαν να μεταδίδονται σε όλα τα μέρη ενός διαδικτύου.

Το φιλτράρισμα πακέτων βοηθά στον έλεγχο της μετακίνησης των πακέτων μέσα στο δίκτυο, περιορίζοντας την κυκλοφορία του δικτύου και τη χρήση του δικτύου από ορισμένους χρήστες ή συσκευές. Για την άδεια ή την άρνηση μεταφοράς πακέτων σε καθορισμένες διασυνδέσεις δρομολογητών, η Cisco παρέχει λίστες πρόσβασης. Μια *λίστα πρόσβασης IP* (IP access list) είναι ένας ακολουθιακός κατάλογος με συνθήκες άδειας (permit) και άρνησης (deny) πρόσβασης που εφαρμόζονται σε διευθύνσεις IP ή σε πρωτόκολλα IP ανώτερων επιπέδων. Οι λίστες πρόσβασης προσδιορίζουν την κυκλοφορία που θα φιλτραριστεί κατά τη διέλευσή της μέσω του δρομολογητή, αλλά δεν φιλτράρουν την κυκλοφορία που προέρχεται από το δρομολογητή. Επειδή ένας δρομολογητής δεν μπορεί να "μπλοκάρει" ένα πακέτο που προέρχεται από έναν άλλο δρομολογητή, δεν έχετε τη δυνατότητα να εμποδίσετε την πρόσβαση μέσω Telnet από το δρομολογητή. Όπως φαίνεται στο Σχήμα 6-2, τα πακέτα μπορεί να ταξιδεύουν μέσω μιας διασύνδεσης, ή να προσπελάζουν μια θύρα vty ώστε να παρέχουν συνδετικότητα Telnet στον ίδιο το δρομολογητή. Οι λίστες πρόσβασης επιτρέπουν τον έλεγχο αυτής της κυκλοφορίας.

Σχήμα 6-1 *Ο λόγος για τον οποίο χρησιμοποιούνται λίστες πρόσβασης*

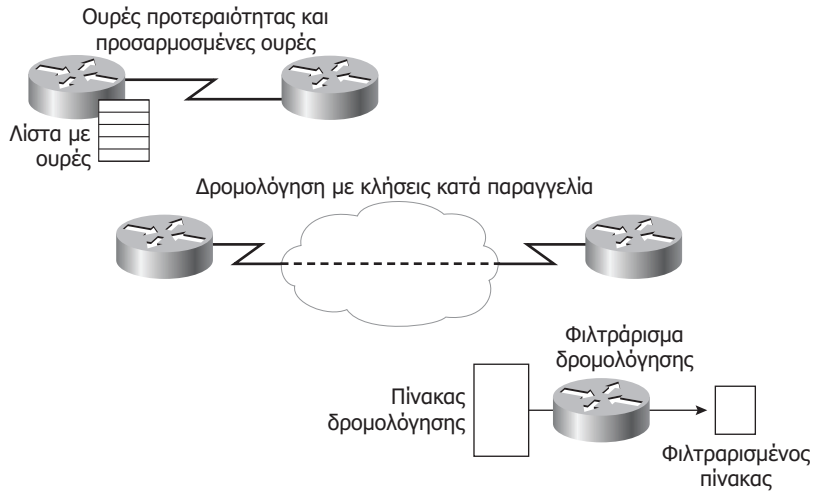


Σχήμα 6-2 *Λίστα πρόσβασης ως φίλτρο πακέτων*



Αν και οι λίστες πρόσβασης σχετίζονται συνήθως με φίλτρα πακέτων, έχουν πολλές άλλες χρήσεις όπως φαίνεται στο Σχήμα 6-3. Χρησιμοποιώντας λίστες πρόσβασης IP, μπορείτε να εξειδικεύσετε ακόμη περισσότερο τον έλεγχο κατά το διαχωρισμό της κυκλοφορίας σε ουρές προτεραιότητας (priority queues) και προσαρμοσμένες ουρές (custom queues). Μια λίστα πρόσβασης μπορεί επίσης να χρησιμοποιηθεί για τον προσδιορισμό συγκεκριμένων πακέτων που χρησιμεύουν για την ενεργοποίηση των κλήσεων, σε δρομολόγηση με κλήση βάσει ζήτησης (dial-on-demand routing — DDR). Οι λίστες πρόσβασης αποτελούν επίσης ένα θεμελιώδες συστατικό των χαρτών δρομολογίων (route maps), οι οποίες φιλτράρουν και, σε μερικές περιπτώσεις, τροποποιούν τις πληροφορίες που περιλαμβάνονται σε μια ενημέρωση πρωτοκόλλου δρομολόγησης.

Σχήμα 6-3 *Άλλες χρήσεις των λιστών πρόσβασης*



Στο Κεφάλαιο 9, "Ολοκλήρωση κλήσης BRI ISDN", εξηγείται η δρομολόγηση DDR με περισσότερες λεπτομέρειες.

Λειτουργίες και διαδικασίες λιστών πρόσβασης

Οι λίστες πρόσβασης είναι προαιρετικοί μηχανισμοί του λογισμικού IOS της Cisco που μπορούν να ρυθμιστούν για να φιλτράρουν ή να ελέγχουν πακέτα ώστε να μπορεί να προσδιοριστεί αν θα επιτραπεί η προώθησή τους στον προορισμό τους ή αν θα απορριφθούν. Στην ενότητα αυτή περιγράφουμε τι είναι οι λίστες πρόσβασης και πώς λειτουργούν.

Υπάρχουν δύο γενικοί τύποι λιστών πρόσβασης:

- **Τυπικές λίστες πρόσβασης** (standard access lists) — Οι τυπικές λίστες πρόσβασης IP ελέγχουν τη διεύθυνση προέλευσης των πακέτων που μπορούν να δρομολογηθούν. Το αποτέλεσμα του ελέγχου καθορίζει αν θα επιτραπεί ή όχι η έξοδος των πακέτων για ολόκληρη την γκάμα πρωτοκόλλων, με βάση τη διεύθυνση προέλευσης IP του δικτύου, του υποδικτύου, ή του υπολογιστή υπηρεσίας.
- **Επεκτεταμένες λίστες πρόσβασης** (extended access lists) — Οι επεκτεταμένες λίστες πρόσβασης IP ελέγχουν και για διευθύνσεις προέλευσης και για διευθύνσεις προορισμού πακέτων. Μπορούν επίσης να πραγματοποιούν έλεγχο για συγκεκριμένα πρωτόκολλα, αριθμούς θυρών, και άλλες παραμέτρους, κάτι που δίνει στους διαχειριστές περισσότερη ευελιξία στην περιγραφή των αναφερόμενων πακέτων.

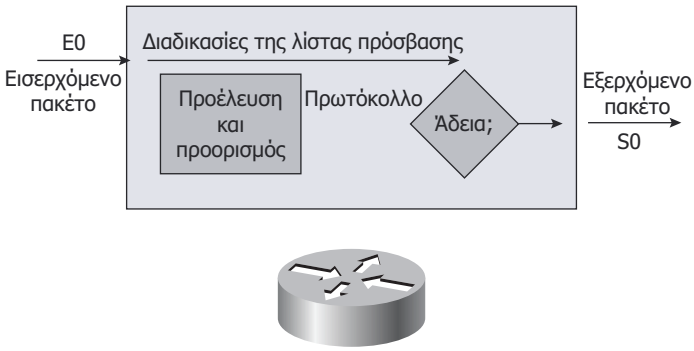
Οι λίστες πρόσβασης μπορούν να χρησιμοποιηθούν ως εξής:

- **Λίστες πρόσβασης εισόδου** (inbound access lists) — Τα εισερχόμενα πακέτα υποβάλλονται σε επεξεργασία πριν δρομολογηθούν σε μια διασύνδεση εξόδου. Μια λίστα πρόσβασης εισόδου είναι αποδοτικότερη από μια λίστα πρόσβασης εξόδου επειδή δεν προκαλεί επιβάρυνση λόγω αναζητήσεων στον πίνακα δρομολόγησης στην περίπτωση που το πακέτο πρόκειται να απορριφθεί από τους ελέγχους φιλτραρίσματος. Αν οι έλεγχοι επιτρέψουν την προώθηση του πακέτου, αυτό υποβάλλεται σε επεξεργασία για δρομολόγηση.
- **Λίστες πρόσβασης εξόδου** (outbound access lists) — Τα εισερχόμενα πακέτα δρομολογούνται στη διασύνδεση εξόδου και υποβάλλονται σε επεξεργασία μέσω της λίστας πρόσβασης εξόδου πριν από τη μετάδοσή τους.

Λειτουργίες λίστας πρόσβασης

Στο Σχήμα 6-4 παρουσιάζεται μια σχηματική αναπαράσταση της λειτουργίας μιας λίστας πρόσβασης για ένα πακέτο που μεταφέρεται μέσω ενός δρομολογητή. Αυτή η διαδικασία είναι η ίδια και για ένα εισερχόμενο πακέτο, με εξαίρεση τον έλεγχο που γίνεται στον πίνακα δρομολόγησης. Μπορείτε να παρομοιάσετε τη λίστα με έναν τροχονόμο που δεν αφήνει κάποια συγκεκριμένη κυκλοφορία να εισέλθει σε συγκεκριμένες περιφέρειες του δικτύου.

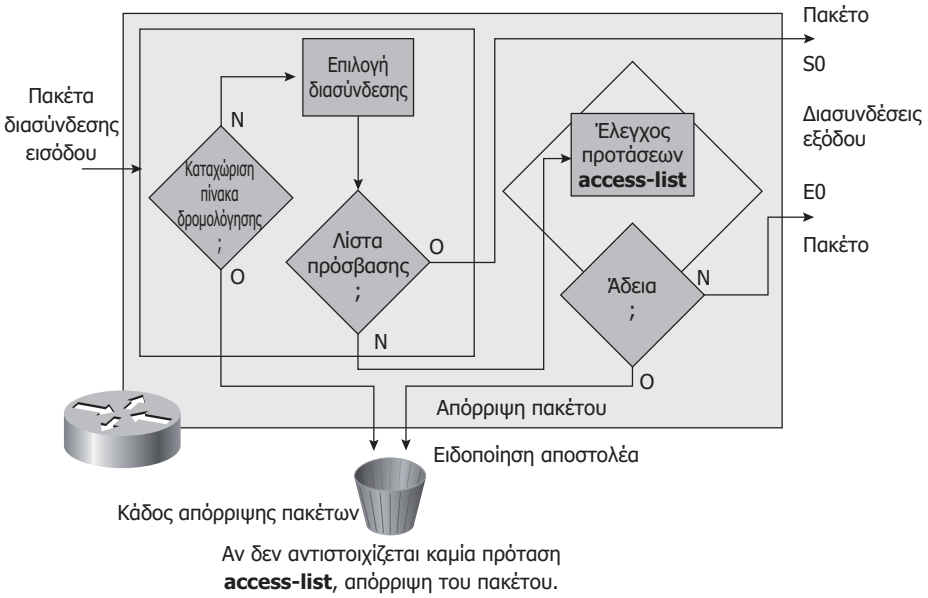
Σχήμα 6-4 *Περιγραφή φίλτρου λίστα πρόσβασης*



Οι λίστες πρόσβασης εκφράζουν το σύνολο των κανόνων που επιτρέπουν περαιτέρω έλεγχο σε πακέτα τα οποία εισέρχονται σε διασυνδέσεις εισόδου, αναμεταδίδονται μέσω του δρομολογητή, ή εξέρχονται από τις διασυνδέσεις εξόδου του δρομολογητή. Οι λίστες πρόσβασης ***δεν*** επιδρούν με κανέναν τρόπο σε πακέτα που προέρχονται από τον ίδιο το δρομολογητή, όπως οι ενημερώσεις δρομολόγησης ή οι εξερχόμενες συνδιαλέξεις Telnet. Αντίθετα, οι λίστες πρόσβασης είναι προτάσεις (εντολές) που καθορίζουν συνθήκες σχετικά με το πώς θα χειριστεί ο δρομολογητής τη ροή κυκλοφορίας μέσω συγκεκριμένων διασυνδέσεων. Οι λίστες πρόσβασης παρέχουν επιπλέον έλεγχο για την επεξεργασία των συγκεκριμένων πακέτων.

Το Σχήμα 6-5 επεκτείνει το παράδειγμα μιας λίστας πρόσβασης εξόδου.

Σχήμα 6-5 *Λειτουργία λίστας πρόσβασης εξόδου*



Η αρχή της διαδικασίας είναι η ίδια, ανεξάρτητα από το αν χρησιμοποιούνται λίστες πρόσβασης εξόδου. Καθώς ένα πακέτο εισέρχεται σε μια διασύνδεση, ο δρομολογητής ελέγχει τον πίνακα δρομολόγησης για να διαπιστώσει αν το πακέτο μπορεί να δρομολογηθεί. Αν δεν υπάρχει κανένα δρομολόγιο προς τη διεύθυνση προορισμού, το πακέτο απορρίπτεται.

Έπειτα, ο δρομολογητής ελέγχει αν η διασύνδεση προορισμού περιλαμβάνεται σε κάποια λίστα πρόσβασης. Αν δεν περιλαμβάνεται, το πακέτο μπορεί να σταλεί στην περιοχή προσωρινής αποθήκευσης εξόδου (output buffer). Για παράδειγμα:

- Αν το εξερχόμενο πακέτο προορίζεται για τη σειριακή διασύνδεση 0 (Serial 0 — S0) η οποία δεν περιλαμβάνεται σε μια λίστα πρόσβασης εξόδου, το πακέτο στέλνεται απευθείας στη διασύνδεση S0.
- Αν το εξερχόμενο πακέτο προορίζεται για τη διασύνδεση Ethernet 0 (E0) η οποία υπάρχει σε μια λίστα πρόσβασης εξόδου, πριν το πακέτο σταλεί στη διασύνδεση E0 ελέγχεται από ένα συνδυασμό προτάσεων (εντολών) της λίστας πρόσβασης που σχετίζονται με αυτή τη διασύνδεση. Με βάση τους ελέγχους αυτούς, το πακέτο μπορεί να επιτραπεί ή να απορριφθεί.

Για τις λίστες εξόδου, η λέξη *επιτρέπω* (permit) σημαίνει αποστολή στην περιοχή προσωρινής αποθήκευσης εξόδου (output buffer), και η λέξη *απορρίπτω* (deny) σημαίνει απόρριψη του πακέτου. Για τις λίστες εισόδου, αντίστοιχα, η λέξη *επιτρέπω* σημαίνει συνέχιση της επεξερ-

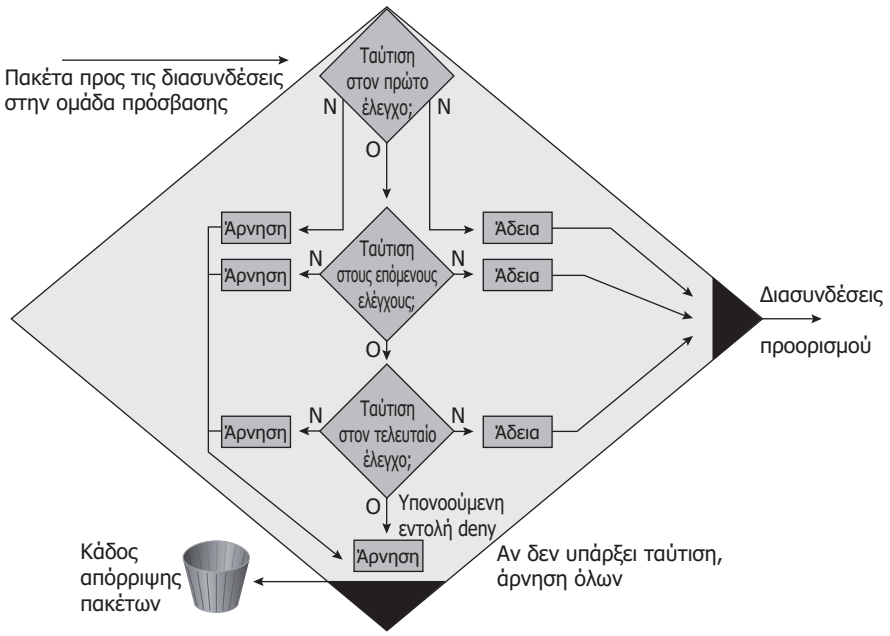
γασίας του πακέτου μετά τη λήψη του σε μια διασύνδεση εισόδου, και η λέξη *απορρίπτω* σημαίνει απόρριψη του πακέτου. Όταν ένα πακέτο IP απορρίπτεται, το ICMP επιστρέφει ένα ειδικό πακέτο για να ενημερώσει τον αποστολέα ότι ο προορισμός είναι μη προσπελάσιμος.

Έλεγχος συνθηκών λιστών πρόσβασης

Οι προτάσεις μιας λίστας πρόσβασης λειτουργούν σε διαδοχική, λογική σειρά. Αξιολογούν πακέτα από επάνω προς τα κάτω, μία πρόταση τη φορά. Αν υπάρχει αντιστοιχία μεταξύ μιας κεφαλίδας πακέτου και μιας πρότασης της λίστας πρόσβασης, οι υπόλοιπες προτάσεις της λίστας παραλείπονται, και το πακέτο επιτρέπεται ή απορρίπτεται όπως καθορίζεται στην αντιστοιχισμένη πρόταση. Αν μια κεφαλίδα πακέτου δεν ταιριάζει με μια πρόταση λίστας πρόσβασης, συγκρίνεται με την επόμενη πρόταση της λίστας. Αυτή η διαδικασία ταύτισης συνεχίζεται μέχρι το τέλος της λίστας, οπότε το πακέτο απορρίπτεται από μια έμμεση εντολή άρνησης (implicit deny).

Στο Σχήμα 6-6 παρουσιάζεται η ροή ελέγχου των πακέτων μιας λίστας πρόσβασης· σε αυτό το παράδειγμα, χρησιμοποιούνται οι επιλογές **permit** ή **deny**, και όλοι οι επακόλουθοι έλεγχοι τερματίζονται για το συγκεκριμένο πακέτο. Μια συνθήκη που απορρίπτει ένα πακέτο σε μια προηγούμενη πρόταση δεν μπορεί να υποσκελιστεί από μια επόμενη πρόταση. Η συνέπεια αυτής της συμπεριφοράς είναι ότι η σειρά των προτάσεων μέσα σε οποιαδήποτε δεδομένη λίστα πρόσβασης είναι σημαντική.

Σχήμα 6-6 *Έλεγχοι συνθηκών λίστας πρόσβασης*



Μια τελική υπονοούμενη πρόταση (implied statement) καλύπτει όλα τα πακέτα για τα οποία οι συνθήκες δεν προέκυψαν αληθείς. Αυτή η τελική συνθήκη ελέγχου αντιστοιχίζει όλα τα άλλα πακέτα και καταλήγει σε μια συνθήκη απόρριψης (deny), απορρίπτοντας έτσι το πακέτο. Αντί να εξέλθουν από μια διασύνδεση, όλα τα πακέτα που δεν έχουν ταυτιστεί από προηγούμενες προτάσεις της λίστας πρόσβασης απορρίπτονται. Αυτή η τελική πρόταση αναφέρεται συχνά ως *υπονοούμενη deny any* στο τέλος κάθε λίστας πρόσβασης. Παρόλο που αυτή η πρόταση δεν εμφανίζεται στη διευθέτηση του δρομολογητή, είναι πάντα ενεργός. Λόγω της υπονοούμενης πρότασης deny any, μια λίστα πρόσβασης πρέπει να περιέχει τουλάχιστον μία πρόταση **permit**· διαφορετικά, η λίστα πρόσβασης θα μπλοκάρει όλη την κυκλοφορία.

Οδηγίες για την υλοποίηση λιστών πρόσβασης

Μια λίστα πρόσβασης μπορεί να υλοποιηθεί σε πολλές διασυνδέσεις· όμως, μπορεί να υπάρχει μόνο μία λίστα πρόσβασης ανά πρωτόκολλο, ανά κατεύθυνση, και ανά διασύνδεση.

Οι παρακάτω γενικές αρχές θα σας βοηθήσουν να εξασφαλίσετε ότι οι λίστες πρόσβασης που δημιουργείτε θα έχουν τα αποτελέσματα που θέλετε:

- Χρησιμοποιήστε αριθμούς λιστών πρόσβασης μόνον από το εύρος που ορίζει η Cisco για το πρωτόκολλο και τον τύπο της λίστας που δημιουργείτε. (Δείτε τον Πίνακα 6-1 στην επόμενη ενότητα, "Τα βασικά των εντολών λιστών πρόσβασης".)
- Επιτρέπεται μόνο μία λίστα πρόσβασης ανά πρωτόκολλο, ανά κατεύθυνση, και ανά διασύνδεση. Σε κάθε διασύνδεση επιτρέπονται πολλές λίστες πρόσβασης, αλλά κάθε μία πρέπει να ορίζεται για διαφορετικό πρωτόκολλο.
- Η επεξεργασία πρέπει να γίνεται από επάνω προς τα κάτω:
  - Οργανώστε τη λίστα πρόσβασης ώστε οι πιο συγκεκριμένες αναφορές σε ένα δίκτυο ή υποδίκτυο να εμφανίζονται πριν από τις γενικότερες αναφορές. Τοποθετήστε τις συνθήκες που εμφανίζονται συχνότερα πριν από αυτές που εμφανίζονται λιγότερα συχνά.
  - Επακόλουθες προσθήκες γίνονται πάντα στο τέλος της λίστας πρόσβασης, αλλά πριν από την υπονοούμενη deny.
  - Δεν μπορείτε να προσθέτετε ή να αφαιρείτε επιλεκτικά προτάσεις κατά τη χρήση αριθμημένων λιστών πρόσβασης, αλλά μπορείτε να το κάνετε κατά τη χρήση επωνύμων λιστών πρόσβασης IP (μια δυνατότητα του Cisco IOS Έκδοση 11.2).

ΣΥΜΒΟΥΛΗ Επειδή η πραγματοποίηση αλλαγών σε ενεργούς λίστες πρόσβασης σε ένα δρομολογητή ή μεταγωγέα είναι δύσκολη, συνηθίζεται η αντιγραφή του κειμένου της λίστας πρόσβασης σε ένα αρχείο κειμένου και η επεξεργασία του με ένα διορθωτή κειμένου. Κατά την επεξεργασία, η λίστα πρόσβασης μπορεί να αφαιρεθεί εντελώς και τα περιεχόμενα του αρχείου να επικολληθούν ξανά στο αρχείο διευθέτησης της συσκευής.

- Υπονοούμενη πρόταση deny all:
  - Εκτός αν ολοκληρώσετε τη λίστα πρόσβασής σας με μια ρητή (explicit) πρόταση permit any, η λίστα εξ ορισμού θα απορρίπτει όλη την κυκλοφορία που δεν ταιριάζει με κάποια από τις συνθήκες της.
  - Κάθε λίστα πρόσβασης πρέπει να έχει τουλάχιστον μία πρόταση **permit**· διαφορετικά, θα απορρίπτεται όλη η κυκλοφορία.
- Ολοκληρώστε τη λίστα πρόσβασης πριν την εφαρμόσετε σε μια διασύνδεση. Μια διασύνδεση στην οποία έχει εφαρμοστεί μια ανύπαρκτη ή μη ορισμένη λίστα πρόσβασης επιτρέπει όλη την κυκλοφορία.
- Οι λίστες πρόσβασης φιλτράρουν μόνο την κυκλοφορία που περνάει μέσα από το δρομολογητή. Δεν φιλτράρουν την κυκλοφορία που προέρχεται από το δρομολογητή.

Τα βασικά των εντολών λιστών πρόσβασης

Στην πράξη, οι εντολές που χρησιμοποιούνται για τη διευθέτηση των λιστών πρόσβασης μπορεί να είναι μεγάλες σειρές αλφαριθμητικών. Επίσης, η καταχώριση ή η ερμηνεία των λιστών πρόσβασης μπορεί να είναι πολύπλοκη. Ωστόσο, μπορείτε να κατανοήσετε καλύτερα τις γενικές εντολές διευθέτησης των λιστών πρόσβασης χωρίζοντάς τες σε δύο γενικά στοιχεία:

- Η λίστα πρόσβασης περιέχει καθολικές προτάσεις που χρησιμοποιούνται στον προσδιορισμό πακέτων. Αυτές οι λίστες δημιουργούνται με την καθολική εντολή **access-list**.
- Η εντολή διευθέτησης διασύνδεσης **ip access-group** ενεργοποιεί μια λίστα πρόσβασης IP σε μια διασύνδεση.

Η επόμενη σύνταξη παρουσιάζει τη γενική μορφή της εντολής **access-list**, η οποία περιέχει καθολικές προτάσεις:

```
Router(config)# access-list αριθμός λίστας πρόσβασης {permit • deny} {συνθήκες ελέγχου}
```

Αυτή η καθολική εντολή προσδιορίζει τη λίστα πρόσβασης με έναν αριθμό λίστας πρόσβασης. Αυτός ο αριθμός δείχνει τον τύπο της λίστας πρόσβασης που θα δημιουργηθεί. Στο λογισμικό Cisco IOS Release 11.2 και σε πιο πρόσφατες εκδόσεις, οι λίστες πρόσβασης IP μπορούν επίσης να χρησιμοποιούν ένα όνομα λίστας πρόσβασης αντί για αριθμό. Οι επώνυμες (named) λίστες πρόσβασης IP καλύπτονται στη συνέχεια αυτού του κεφαλαίου.

Ο όρος **permit** ή **deny** στην καθολική πρόταση **access-list** δείχνει τον τρόπο που το λογισμικό IOS θα χειριστεί τα πακέτα τα οποία ικανοποιούν τις συνθήκες ελέγχου. Η επιλογή **permit** σημαίνει ότι στο πακέτο θα επιτραπεί να περάσει μέσα από τις διασυνδέσεις στις οποίες εφαρμόζεται η λίστα. Η επιλογή **deny** σημαίνει ότι ο δρομολογητής θα απορρίψει το πακέτο.

Οι τελευταίες παράμετροι της πρότασης **access-list** καθορίζουν τις συνθήκες ελέγχου που χρησιμοποιούνται. Ο έλεγχος μπορεί να είναι τόσο απλός όσο ο προσδιορισμός μίας μόνο διεύθυνσης προέλευσης. Όμως η λίστα πρόσβασης μπορεί να επεκταθεί ώστε να συμπεριλάβει αρκετές συνθήκες ελέγχου, όπως θα δείτε στην ενότητα για τις επεκτεταμένες λίστες πρόσβασης. Θα χρησιμοποιήσετε περισσότερες από μία καθολικές προτάσεις **access-list** με τον ίδιο αριθμό ή όνομα λίστας πρόσβασης για να συγκεντρώσετε αρκετές συνθήκες ελέγχου σε μια λογική ακολουθία ή λίστα ελέγχων.

Στην παρακάτω σύνταξη παρουσιάζεται η γενική μορφή της εντολής {*πρωτόκολλο*} **access-group**, με την οποία εφαρμόζεται μια λίστα πρόσβασης σε μια διασύνδεση:

```
Router(config-if)#{πρωτόκολλο} access-group αριθμός λίστας πρόσβασης {in • out}
```

Για παράδειγμα, η εφαρμογή της εντολής διευθέτησης διασύνδεσης **ip access-group** ενεργοποιεί μια λίστα πρόσβασης IP σε μια διασύνδεση.

ΠΡΟΣΟΧΗ Αν εφαρμόζετε μια λίστα πρόσβασης με την εντολή **ip access-group** σε μια διασύνδεση πριν δημιουργήστε κάποιες γραμμές στη λίστα πρόσβασης, το αποτέλεσμα θα είναι η χορήγηση άδειας σε οποιαδήποτε κυκλοφορία (permit any). Η λίστα είναι ενεργός· επομένως, αν προσθέσετε μόνο μία γραμμή άδειας (permit) και πατήσετε **Enter**, η κατάστασή της μεταβάλλεται από άδεια για οποιαδήποτε κυκλοφορία (permit any) σε άρνηση της περισσότερης κυκλοφορίας (deny most) λόγω της υπονοούμενης εντολής deny στο τέλος. Για το λόγο αυτόν, δημιουργήστε τη λίστα πρόσβασής σας πριν την εφαρμόσετε σε μια διασύνδεση.

Οι λίστες πρόσβασης μπορούν να ελέγχουν τα περισσότερα πρωτόκολλα σε ένα δρομολογητή τής Cisco. Στον Πίνακα 6-1 παρουσιάζονται τα πρωτόκολλα και τα εύρη αριθμών για τις λίστες πρόσβασης τύπου IP.

Πίνακας 6-1 *Αριθμοί λίστας πρόσβασης*

Λίστα πρόσβασης IP	Εύρος αριθμών/αναγνωριστικό
Τυπική	1 έως 99, 1300 έως 1999
Επεκτεταμένη	100 έως 199, 2000 έως 2699
Επώνυμη	Όνομα

Ως πρώτο όρισμα της καθολικής πρότασης **access-list**, ο διαχειριστής καταχωρίζει έναν αριθμό από το εύρος αριθμών του πρωτοκόλλου. Έτσι, ο δρομολογητής προσδιορίζει ποιο λογισμικό θα χρησιμοποιήσει για τις λίστες πρόσβασης με βάση αυτή την αριθμημένη καταχώριση. Στη συνέχεια τοποθετούνται οι συνθήκες ελέγχου ως ορίσματα. Αυτά τα ορίσματα καθο-

ρίζουν ελέγχους σύμφωνα με τους κανόνες της συγκεκριμένης γκάμας πρωτοκόλλων. Οι συνθήκες ελέγχου των λιστών πρόσβασης διαφέρουν ανάλογα με το πρωτόκολλο.

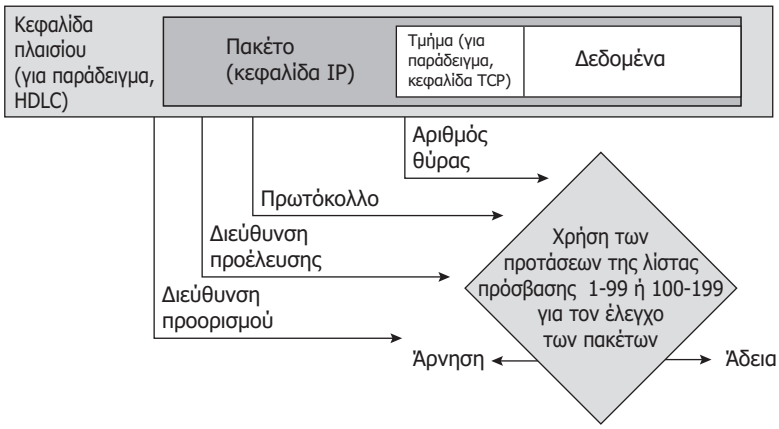
Για κάθε πρωτόκολλο υπάρχει δυνατότητα χρήσης πολλών λιστών πρόσβασης. Απλώς, για κάθε νέα λίστα πρόσβασης πρέπει να διαλέγετε ένα διαφορετικό αριθμό από το εύρος αριθμών του πρωτοκόλλου. Ο διαχειριστής μπορεί να καθορίσει μόνο μία λίστα πρόσβασης ανά πρωτόκολλο, ανά κατεύθυνση, και ανά διασύνδεση.

Όταν καθορίζετε έναν αριθμό λίστας πρόσβασης από 1 έως 99 ή από 1300 έως 1999, δίνετε οδηγία στο δρομολογητή να δέχεται τυπικές προτάσεις IP **access-list**. Παρόμοια, όταν καθορίζετε έναν αριθμό λίστας πρόσβασης από 100 έως 199 ή από 2000 έως 2699, δίνετε οδηγία στο δρομολογητή να δέχεται εκτεταμένες προτάσεις IP **access-list**.

Λίστες πρόσβασης TCP/IP

Μια λίστα πρόσβασης που εφαρμόζεται σε μια διασύνδεση αναγκάζει το δρομολογητή να κοιτάξει στην κεφαλίδα Επιπέδου 3 (IP) και, πιθανόν, στην κεφαλίδα Επιπέδου 4 (TCP/UDP) ενός πακέτου κυκλοφορίας δικτύου για να δει αν ταιριάζουν οι συνθήκες ελέγχου. Οι τυπικές λίστες πρόσβασης IP ελέγχουν μόνο τη διεύθυνση προέλευσης στην κεφαλίδα (Επιπέδου 3) του πακέτου, ενώ οι επεκτεταμένες λίστες πρόσβασης IP μπορούν να ελέγχουν πολλές επιλογές, μεταξύ των οποίων και επιλογές κεφαλίδας (Επιπέδου 4) που αφορούν το τμήμα (segment), όπως αριθμοί θυρών. Στο Σχήμα 6-7 φαίνεται η κατάτμηση ενός συνηθισμένου πακέτου IP για τον έλεγχο της λίστας πρόσβασης.

Σχήμα 6-7 *Έλεγχος πακέτων TCP/IP*



Για το φιλτράρισμα πακέτων TCP/IP, οι λίστες πρόσβασης IP του IOS ελέγχουν το πακέτο και τις κεφαλίδες ανώτερων επιπέδων για τα εξής:

- Διευθύνσεις προέλευσης IP που χρησιμοποιούν τυπικές λίστες πρόσβασης. Οι τυπικές λίστες πρόσβασης χαρακτηρίζονται με έναν αριθμό στο εύρος 1 έως 99 και 1300 έως 1399.
- Διεύθυνση προορισμού και προέλευσης IP, συγκεκριμένα πρωτόκολλα, και αριθμούς θυρών TCP ή UDP που χρησιμοποιούν επεκτεταμένες λίστες πρόσβασης. Οι επεκτεταμένες λίστες πρόσβασης χαρακτηρίζονται με έναν αριθμό στο εύρος 100 έως 199 και 2000 έως 2699.

Για όλες αυτές τις λίστες πρόσβασης IP, μόλις γίνει ο έλεγχος ταύτισης ενός πακέτου με την πρόταση **access-list**, μπορεί να επιτραπεί ή να απαγορευθεί στο πακέτο η χρήση της διασύνδεσης για την οποία έχει οριστεί μια πρόταση **access-group**.

Ίσως χρειαστεί έλεγχος συνθηκών για μια ομάδα ή ένα εύρος διευθύνσεων IP, ή μόνο για μια διεύθυνση IP. Για το λόγο αυτόν, χρειάζεστε μια μέθοδο ώστε να προσδιορίζετε ποια bit μιας συγκεκριμένης διεύθυνσης IP πρέπει να ελέγχονται για ταύτιση.

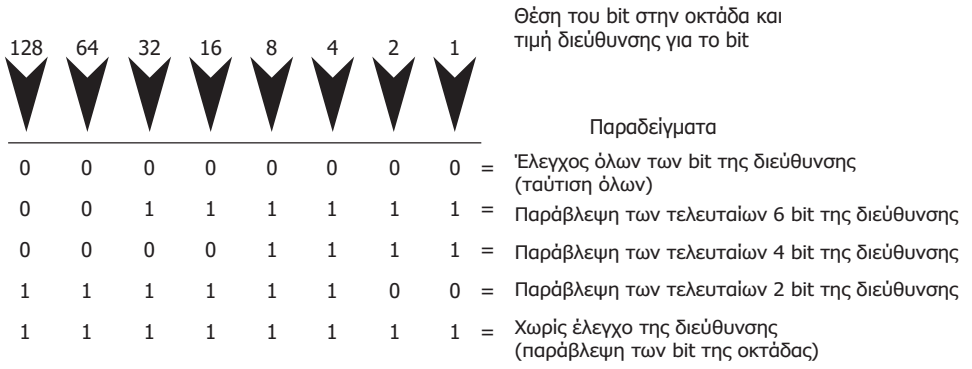
Η ταύτιση διευθύνσεων (address matching) πραγματοποιείται με τη χρήση μασκών (χαρακτήρων) μπαλαντέρ (wildcard masks) σε διευθύνσεις μιας λίστας πρόσβασης για τον προσδιορισμό των bit μιας διεύθυνσης IP που απαιτούν ρητή ταύτιση, και των bit που μπορούν να αγνοηθούν.

Οι μάσκες μπαλαντέρ για bit διευθύνσεων IP χρησιμοποιούν τους αριθμούς 1 και 0 για την υπόδειξη του τρόπου χειρισμού των αντίστοιχων bit:

- Ένα bit μάσκας μπαλαντέρ με τιμή 0 ερμηνεύεται ως "Έλεγξε την αντίστοιχη τιμή bit".
- Ένα bit μάσκας μπαλαντέρ με τιμή 1 ερμηνεύεται ως "Μην ελέγξεις (αγνόησε) την αντίστοιχη τιμή bit".

Ορίζοντας προσεκτικά μάσκες μπαλαντέρ, ένας διαχειριστής μπορεί να επιλέξει μία μόνο διεύθυνση ή πολλές διευθύνσεις IP για ελέγχους χορήγησης ή άρνησης πρόσβασης. Στο Σχήμα 6-8 φαίνεται πώς γίνεται η ταύτιση bit με μια μάσκα μπαλαντέρ.

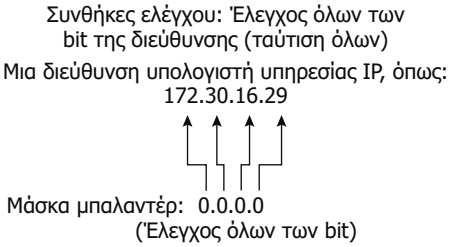
Σχήμα 6-8 *Bit μπαλαντέρ*



Οι μάσκες μπαλαντέρ για λίστες πρόσβασης λειτουργούν διαφορετικά από τις μάσκες υποδικτύων IP. Ένα 0 σε μια θέση bit της μάσκας λίστας πρόσβασης σημαίνει ότι πρέπει να ελεγχθεί το αντίστοιχο bit της διεύθυνσης· το 1 σε μια θέση bit της μάσκας σημαίνει ότι το αντίστοιχο bit της διεύθυνσης δεν έχει "ενδιαφέρον" και μπορεί να παραλειφθεί.

Είδατε λοιπόν πώς τα bit 0 και 1 σε μια μάσκα μπαλαντέρ λίστας πρόσβασης κάνουν τη λίστα πρόσβασης είτε να ελέγχει είτε να αγνοεί το αντίστοιχο bit της διεύθυνσης IP. Στο Σχήμα 6-9, βλέπετε ένα παράδειγμα αυτής της διαδικασίας ταύτισης με μάσκες μπαλαντέρ.

Σχήμα 6-9 *Ταύτιση συγκεκριμένου υπολογιστή υπηρεσίας IP*



Ας δούμε το παράδειγμα ενός διαχειριστή δικτύου που θέλει να καθορίσει ότι μια συγκεκριμένη διεύθυνση υπολογιστή υπηρεσίας IP θα απορρίπτεται κατά τον έλεγχο μιας λίστας πρόσβασης. Για να δηλώσει μια διεύθυνση υπολογιστή υπηρεσίας IP, ο διαχειριστής καταχωρίζει την πλήρη διεύθυνση — για παράδειγμα, 172.30.16.29. Κατόπιν, για να δείξει ότι η λίστα πρόσβασης πρέπει να ελέγχει όλα τα bit στη διεύθυνση, τα αντίστοιχα bit της μάσκας μπαλαντέρ γι' αυτή τη διεύθυνση πρέπει να είναι όλα 0 — δηλαδή, 0.0.0.0.

Η χρήση δεκαδικών αναπαραστάσεων bit σε δυαδικές μάσκες μπαλαντέρ μπορεί να είναι κουραστική. Για τις πιο συνηθισμένες χρήσεις των μασκών μπαλαντέρ, μπορείτε να χρησιμοποιείτε συντομογραφίες. Με αυτές τις συντομογραφίες μειώνεται το πλήθος των αριθμών που πρέπει να καταχωρίζουν οι διαχειριστές κατά τη διευθέτηση των συνθηκών ελέγχου διευθύνσεων. Για παράδειγμα, όταν θέλετε να ταυτίσετε μια συγκεκριμένη διεύθυνση υπολογιστή υπηρεσίας, μπορείτε να χρησιμοποιήσετε μια συντομογραφία αντί για ένα μακροσκελές αλφαριθμητικό μάσκας μπαλαντέρ.

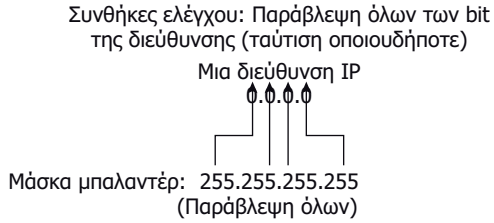
Ο διαχειριστής μπορεί να χρησιμοποιήσει τη συντομογραφία **host** πριν από τη διεύθυνση IP για να δηλώσει την ίδια συνθήκη ελέγχου στο λογισμικό λιστών πρόσβασης IOS τής Cisco. Έτσι, για παράδειγμα, αντί να πληκτρολογήσει **172.30.16.29 0.0.0.0**, μπορεί να χρησιμοποιήσει το αλφαριθμητικό **host 172.30.16.29**.

ΣΗΜΕΙΩΣΗ Για τις τυπικές λίστες πρόσβασης, αν δεν χρησιμοποιήσετε μια λέξη-κλειδί ή δεν ορίσετε μάσκα μπαλαντέρ, η συσκευή θα υποθέσει ότι η μάσκα μπαλαντέρ είναι 0.0.0.0 ή host.

Μια δεύτερη συνήθης συνθήκη με την οποία το λογισμικό IOS τής Cisco επιτρέπει έναν όρο συντομογραφίας στη μάσκα μπαλαντέρ της λίστας πρόσβασης είναι όταν ο διαχειριστής θέλει να ελέγξει για ταύτιση με μια οποιαδήποτε διεύθυνση IP. Αυτή συνήθως τοποθετείται ως τελευταία πρόταση σε μια λίστα πρόσβασης, αμέσως πριν από την υπονοούμενη εντολή **deny any**, αφού η λίστα θα έχει ήδη απαγορεύσει ή επιτρέψει όλη την υπόλοιπη κυκλοφορία την οποία ο διαχειριστής είχε σκοπό να προσδιορίσει με τη λίστα ελέγχου πρόσβασης (ACL).

Ας δούμε το παράδειγμα ενός διαχειριστή δικτύου που θέλει να καθορίσει ότι θα επιτρέπεται οποιαδήποτε διεύθυνση προορισμού κατά τον έλεγχο μιας λίστας πρόσβασης. Για να δηλώσει μια οποιαδήποτε διεύθυνση IP, ο διαχειριστής πρέπει να πληκτρολογήσει **0.0.0.0**. Κατόπιν, για να δείξει ότι η λίστα πρόσβασης πρέπει να αγνοεί (δηλαδή, να επιτρέπει χωρίς να ελέγχει) οποιαδήποτε τιμή, τα αντίστοιχα bit της μάσκας μπαλαντέρ γι' αυτή τη διεύθυνση πρέπει να είναι όλα 1 (255.255.255.255), όπως φαίνεται στο Σχήμα 6-10.

Σχήμα 6-10 *Ταύτιση με οποιαδήποτε διεύθυνση IP*



Ο διαχειριστής μπορεί να χρησιμοποιήσει τη συντομογραφία **any** για να δηλώσει την ίδια συνθήκη ελέγχου στο λογισμικό λιστών πρόσβασης IOS. Αντί να πληκτρολογήσει **0.0.0.0 255.255.255.255**, μπορεί να χρησιμοποιήσει τη λέξη-κλειδί **any**.

Υποθέστε ότι ένας διαχειριστής θέλει να ελέγξει ένα εύρος υποδικτύων IP τα οποία θα επιτρέπονται ή θα απαγορεύονται. Για μια δεδομένη διεύθυνση IP Κλάσης B (οι δύο πρώτες οκτάδες είναι ο αριθμός δικτύου) με 8 bit υποδικτύου (η τρίτη οκτάδα είναι για υποδίκτυα), ο διαχειριστής ίσως πρέπει να χρησιμοποιήσει τα bit της μάσκας μπαλαντέρ IP για να ελέγξει για ταύτιση τα υποδίκτυα στο εύρος 172.30.16.0 /24 έως 172.30.31.0 /24.

Το Σχήμα 6-11 δείχνει τη μάσκα μπαλαντέρ που θα χρησιμοποιούσαμε για το σκοπό αυτόν.

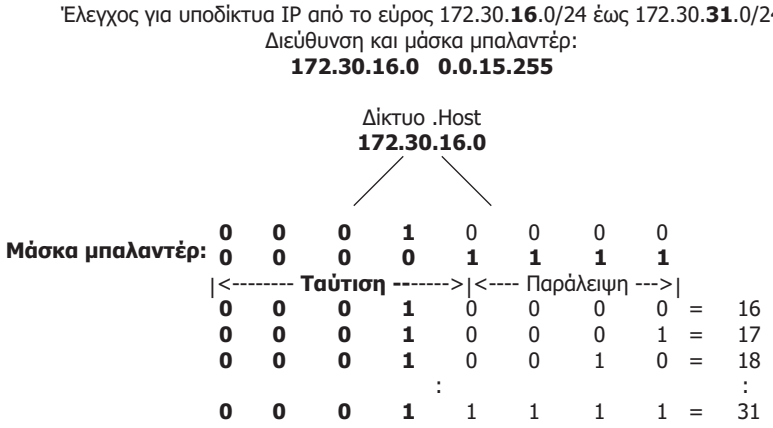
Πρώτα, η μάσκα μπαλαντέρ ελέγχει τις δύο πρώτες οκτάδες (172.30) χρησιμοποιώντας τα αντίστοιχα bit 0 της μάσκας.

Επειδή δεν σας ενδιαφέρει κάποιος μεμονωμένος υπολογιστής υπηρεσίας, πρέπει να ρυθμίσετε τη μάσκα μπαλαντέρ ώστε να αγνοεί όλα τα bit στην τελική οκτάδα. Ορίζοντας όλα τα bit στην τελική οκτάδα ίσα με 1, αγνοείτε το τμήμα της διεύθυνσης που αφορά τον υπολογιστή υπηρεσίας. Όλα τα 1 σε μια οκτάδα είναι ίσα με τη δεκαδική τιμή 255.

Στην τρίτη οκτάδα, όπου εμφανίζεται η διεύθυνση υποδικτύου, η μάσκα μπαλαντέρ ελέγχει αν το bit για το δυαδικό 16 είναι "ενεργοποιημένο" και αν όλα τα bit υψηλότερης τάξης είναι

"απενεργοποιημένα", χρησιμοποιώντας bit 0 στη μάσκα μπαλαντέρ. Όσο αφορά τα τελευταία (χαμηλότερα) 4 bit αυτής της οκτάδας, η μάσκα μπαλαντέρ δείχνει ότι μπορούν να αγνοηθούν. Σε αυτές τις θέσεις, η τιμή της διεύθυνσης μπορεί να είναι δυαδικό 0 ή δυαδικό 1, αλλά η σύμβαση είναι να δίνεται η τιμή 0 στη διεύθυνση στην οποία εφαρμόζεται η μάσκα με μια μάσκα μπαλαντέρ "παράλειψης". Κατά συνέπεια, η μάσκα μπαλαντέρ βρίσκει ταύτιση με τα υποδίκτυα 16, 17, 18, κ.λπ., μέχρι το υποδίκτυο 31, και δε βρίσκει ταύτιση με άλλα υποδίκτυα.

Σχήμα 6-11 *"Μπλοκάρισμα" ενός εύρους υποδικτύων*



Στο Σχήμα 6-11, η διεύθυνση 172.30.16.0 με τη μάσκα μπαλαντέρ 0.0.15.255 ταυτίζεται με τα υποδίκτυα 172.30.16.0 /24 έως 172.30.31.0 /24.

ΣΗΜΕΙΩΣΗ Αν και η μάσκα μπαλαντέρ ονομάζεται μερικές φορές *ανεστραμμένη μάσκα υποδικτύου* (inverted subnet mask), το όνομα αυτό δεν ανταποκρίνεται πάντα στην πραγματικότητα. Η μάσκα υποδικτύου στο Σχήμα 6-11 είναι 255.255.255.0, και η ανεστραμμένη μάσκα θα ήταν 0.0.0.255. Επειδή επιλέξαμε να ελέγξουμε για ταύτιση με μερικές μόνον από τις διευθύνσεις τού εύρους των υποδικτύων, η μάσκα μπαλαντέρ ήταν 0.0.15.255. Σημειώστε επίσης ότι μπορείτε να επιλέξετε έλεγχο για ταύτιση μόνο με την τελευταία οκτάδα και να αγνοήσετε τις πρώτες τρεις οκτάδες, χρησιμοποιώντας τη μάσκα μπαλαντέρ 255.255.255.0.

Ερωτηματολόγιο Ενότητας 1

1 Σωστό ή λάθος: Οι λίστες πρόσβασης χρησιμοποιούνται μόνο για λόγους ασφαλείας, ώστε να απαγορεύουν την κυκλοφορία μέσω μιας συσκευής.

Cisco Systems

CCNA Αυτοδιδασκαλία:
Διασύνδεση Συσκευών Δικτύου Cisco (ICND)
Δεύτερη Αμερικανική έκδοση

ΑΥΤΟΔΙΔΑΣΚΑΛΙΑ

- Προετοιμαστείτε για τις εξετάσεις 640-811 του CCNA ICND ή τις εξετάσεις 640-801 του CCNA με αυτόν τον εγκεκριμένο από τη Cisco οδηγό αυτοδιδασκαλίας
- Διευθετήστε λειτουργίες των μεταγωγέων Catalyst της Cisco, όπως η προωθήση (forwarding) και το Spanning Tree Protocol (STP)
- Κατανοήστε τη θεωρία και τη λειτουργία των εικονικών LAN (VLAN), όπως η σήμανση πλαισίων με ετικέτες (frame tagging) και η χρήση του VLAN Trunking Protocol
- Μάθετε πώς οι δρομολογητές ανταλλάσσουν και διατηρούν πληροφορίες δρομολόγησης χρησιμοποιώντας πρωτόκολλα δρομολόγησης όπως τα RIP, IGRP, EIGRP, και OSPF
- Χρησιμοποιήστε μάσκες υποδικτύου μεταβλητού μήκους (VLSM) για να διαχειριζόστε τη διευθυνσιοδότηση IP
- Εφαρμόστε λίστες πρόσβασης για να διαχειριζόστε την κυκλοφορία στους δρομολογητές Cisco
- Κατανοήστε τις παραμέτρους λειτουργίας και διευθέτησης της Μετάφρασης Διευθύνσεων Δικτύου (Network Address Translation - NAT)
- Συνδέστε απομακρυσμένες τοποθεσίες χρησιμοποιώντας μισθωμένες γραμμές με πρωτόκολλα, όπως τα Point-to-Point Protocol (PPP) και High-Level Data Link Control (HDLC)
- Επιτρέψτε την πρόσβαση σε απομακρυσμένες τοποθεσίες μέσω υπηρεσιών Frame Relay
- Διευθετήστε ένα κύκλωμα κλήσεων κατ' απαίτηση (dial-on-demand) προς μια απομακρυσμένη τοποθεσία χρησιμοποιώντας κυκλώματα ISDN

Αυτός ο τόμος ανήκει στη σειρά αυτοδιδασκαλίας για εξετάσεις πιστοποίησης (Certification Self-Study Series) που διατίθεται από τη Cisco Press. Τα βιβλία αυτής της σειράς παρέχουν εγκεκριμένες εκπαιδευτικές λύσεις για να βοηθήσουν τους επαγγελματίες της δικτύωσης να κατανοήσουν την υλοποίηση διαφόρων τεχνολογιών και να προετοιμαστούν για τις εξετάσεις Cisco Career Certifications.

Το βιβλίο *CCNA Αυτοδιδασκαλία: Διασύνδεση Συσκευών Δικτύου Cisco (ICND), Δεύτερη Αμερικανική Έκδοση*, είναι ένας οδηγός εκμάθησης εγκεκριμένος από τη Cisco για τα βασικά προγράμματα εκπαίδευσης CCNA. Αυτό το βιβλίο σάς παρέχει τις γνώσεις που χρειάζεστε για να προσδιορίζετε και να προτείνετε τις καλύτερες λύσεις Cisco για μικρομεσαίες επιχειρήσεις. Σας μαθαίνει πώς να εκτελείτε όλες τις βασικές εργασίες για τη δημιουργία διαδικτύων με πολλούς δρομολογητές και πολλές ομάδες χρηστών, τα οποία χρησιμοποιούν διασυνδέσεις LAN και WAN για τα πρωτόκολλα δρομολόγησης (routing protocols) και τα δρομολογημένα πρωτόκολλα (routed protocols) που χρησιμοποιούνται συχνότερα.

Αυτός ο κατανοητός οδηγός παρουσιάζει αναλυτικές πληροφορίες και εύληπτες οδηγίες σχετικά με τον τρόπο χρήσης των μεταγωγέων Catalyst της Cisco και των δρομολογητών Cisco σε συνδεδεμένα LAN και WAN. Αφού μελετήσετε το βιβλίο, θα αποκτήσετε τις δεξιότητες που απαιτούνται για την επιλογή, τη σύνδεση, τη διευθέτηση, και την αντιμετώπιση προβλημάτων συσκευών δικτύωσης Cisco. Το Μέρος Ι παρουσιάζει βασικές έννοιες δικτύωσης και τον τρόπο εγκατάστασης και διευθέτησης μεταγωγέων Catalyst της Cisco και VLAN. Στο Μέρος ΙΙ περιγράφεται η λειτουργία και η διευθέτηση των δρομολογητών μέσα σε ένα διαδίκτυο. Το Μέρος ΙΙΙ επεκτείνεται πέρα από τα γεωγραφικά περιορισμένα δίκτυα και περιγράφει τη σύνδεση συσκευών σε πολύ απομακρυσμένες περιοχές. Κάθε κεφάλαιο τελειώνει με εκτενείς ερωτήσεις επανάληψης για να ελέγχετε τις γνώσεις σας, ενώ οι μελέτες περιπτώσεων σας βοηθούν να κατανοήσετε την πραγματική εφαρμογή των εννοιών. Τα παρατήρησα περιλαμβάνουν χρήσιμες αναφορές για διαχειριστές σχετικά με την ανάκτηση κωδικών πρόσβασης και χαμένων ειδώλων μεταγωγέων (switch images). Είτε προετοιμάζεστε για την πιστοποίηση CCNA είτε απλώς θέλετε να κατανοήσετε καλύτερα τις υπηρεσίες LAN, WAN, και πρόσβασης μέσω τηλεφώνου για μικρά δίκτυα, θα επωφεληθείτε σημαντικά από τις πληροφορίες αυτού του βιβλίου.

Το βιβλίο *CCNA Αυτοδιδασκαλία: Διασύνδεση Συσκευών Δικτύου Cisco (ICND), Δεύτερη Αμερικανική Έκδοση*, αποτελεί μέρος μιας προτεινόμενης εκπαιδευτικής σειράς από τη Cisco Systems, η οποία περιλαμβάνει θεωρητική και πρακτική εκπαίδευση από εξουσιοδοτημένους συνεργάτες της Cisco και προϊόντα αυτοδιδασκαλίας από τη Cisco Press. Για να μάθετε περισσότερα σχετικά με εκπαιδευτικά προγράμματα, την ηλεκτρονική εκμάθηση (e-learning), και την παράδοση πρακτικών μαθημάτων από εξουσιοδοτημένους συνεργάτες της Cisco σε ολόκληρο τον κόσμο, παρακαλούμε επισκεφθείτε τη διεύθυνση www.cisco.com/go/authorizedtraining.

Ο **Steve McQuerry**, CCIE No. 6108, είναι εκπαιδευτής, τεχνικός συγγραφέας, και σύμβουλος διαδικτύωσης με περισσότερα από 10 έτη πείρα στο χώρο της δικτύωσης. Είναι πιστοποιημένος εκπαιδευτής της Cisco Systems και διδάσκει θέματα δρομολόγησης και μεταγωγής σε επαγγελματίες της διαδικτύωσης σε ολόκληρο τον κόσμο. Ο Steve είναι επίσης σύμβουλος στην Intrellix, LLC (www.intrellix.com), μιας συμβουλευτικής εταιρείας διαδικτύωσης που παρέχει υπηρεσίες μετά την πώληση (post sales).

CCNA

ΚΛΕΙΔΑΡΙΘΜΟΣ
Σολωμού 57, 10432, ΑΘΗΝΑ, Τηλ. 210-5237635

Επισκεφθείτε μας στο Internet:
http://www.klidarithmos.gr

ISBN 960-209-914-3