

ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Υλοποίηση Δικτυακών Υποδομών και Υπηρεσιών

Διδάσκων: Απόστολος Γκάμας (Λέκτορας –ΠΔ 407/80)

3^η Εργαστηριακή Άσκηση

Σκοπός

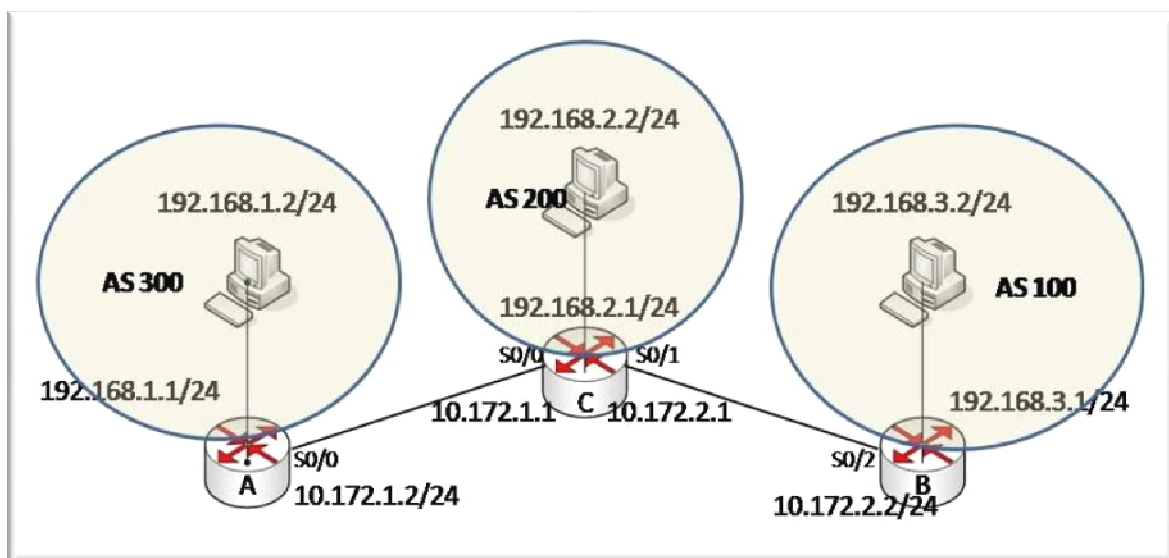
Σκοπός αυτής της άσκησης είναι η εξοικείωση με τις access-lists στους δρομολογητές CISCO. Οι φοιτητές θα χρησιμοποιήσουν πραγματικούς δρομολογητές CISCO στους οποίους θα πρέπει να δώσουν τις κατάλληλες εντολές.

Ημερομηνίες

Το εργαστήριο θα πραγματοποιηθεί την **Παρασκευή 11/04/2008**, ενώ προπαρασκευαστική διάλεξη θα δοθεί την **Παρασκευή 04/04/2008**. Οι αναφορές του εργαστηρίου θα πρέπει να αποσταλούν μέσω e-class στον διδάσκοντα μέχρι την **Πέμπτη 10/04/2008**.

Περιγραφή - Ζητούμενα

1. Ζητείται να υλοποιηθεί η παρακάτω τοπολογία (στους δρομολογητές είναι ήδη configure to Fast Ethernet interface).



2. Ο υπολογιστής με ip 192.168.1.2 τρέχει υπηρεσία FTP.
Ο υπολογιστής με ip 192.168.2.2 τρέχει υπηρεσία HTTP.
3. Ζητείται να ενεργοποιήσετε σε κάθε δρομολογητή το πρωτόκολλο BGP (Εργαστήριο 2).
4. Ζητείται να καθοριστούν access-lists στον δρομολογητή C έτσι ώστε:
 - 4.1. Το δίκτυο 192.168.3.0 να μπορεί να βλέπει σελίδες που παρέχει ο HTTP server ενώ το δίκτυο 192.168.1.0 όχι.
 - 4.2. Επίσης ζητείται το δίκτυο 192.168.3.0 να μπορεί να κάνει ping το δίκτυο 192.168.2.0 ενώ όχι το δίκτυο 192.168.1.0. [Υποστηρικτικό υλικό]
5. Ζητείται να καθορισθούν access-lists στον δρομολογητή A έτσι ώστε:
 - 5.1. Το δίκτυο 192.168.3.0 να μπορεί μπει με telnet σε αυτόν ενώ να απαγορεύεται η πρόσβαση στο δίκτυο 192.168.2.0.
 - 5.2. Να απαγορεύεται η πρόσβαση στην υπηρεσία FTP από το δίκτυο 192.168.2.0 ενώ να επιτρέπεται από το δίκτυο 192.168.3.0.
6. Ζητείται να καθορισθούν access-lists στον δρομολογητή B έτσι ώστε:
 - 6.1. Να επιτρέπεται το traceroute από το δίκτυο 192.168.2.0 ενώ να απαγορεύεται από το δίκτυο 192.168.1.0.
 - 6.2. Να επιτρέπεται μόνο το δίκτυο 192.168.3.0 να αρχικοποιήσει ένα TCP session ενώ να απαγορεύεται η αρχικοποίηση και η εγκατάσταση TCP sessions από τα άλλα δίκτυα.
7. Εφαρμόστε filtering based on AS path. Στόχος είναι (δηλαδή από τον δρομολογητή C) ώστε να εφαρμοστεί σχετική πολιτική του AS200. Μετά την εφαρμογή των εντολών παρατηρήστε τα routing tables των δρομολογητών και αποφανθείτε για την σωστή λειτουργία του path filtering.
8. Στα παραπάνω ζητήματα ο φοιτητής πρέπει να έχει την ικανότητα να αποφασίσει τι είδος access list θα χρησιμοποιήσει και γιατί.
9. Αφού έχετε θέσει τις access lists ελέγχατε εάν πραγματικά ακολουθούν τα ζητούμενα.

Παραδοτέα της αναφοράς εργαστηρίου

Θα πρέπει οι φοιτητές να παραδώσουν αναφορά εργαστηρίου η οποία να περιλαμβάνει τις εντολές που έδωσαν για να πραγματοποιήσουν κάθε ένα από τα παραπάνω βήματα, τις απαντήσεις στα ερωτήματα τα οποία ερωτώνται σε κάθε βήμα καθώς επίσης και ένα αντίγραφο (copy – paste) από το configuration του δρομολογητή.

Υποστηρικτικό Υλικό

Στο web site του μαθήματος στο κατάλογο «Εγγραφα/Εργαστήριο» υπάρχει το αρχείο «Lab3_support.zip» το οποίο παρέχει υποστηρικτικό υλικό για το εργαστήριο.

Επίσης στο web site του μαθήματος στο κατάλογο «Έγγραφα/Εργαστήριο» υπάρχει το αρχείο «Lab_general_support.zip» το οποίο περιέχει γενικότερο υποστηρικτικό υλικό για το εργαστήριο για αυτό καθώς και για άλλα εργαστήρια.

Βασικές εντολές οι οποίες θα χρησιμοποιηθούν

1. Δημιουργία Standard access-list.
 - a. Μπαίνουμε σε configure mode με την εντολή
[Router#] configure terminal.
 - b. Από εκεί θέτουμε την access list
[Router(config)#] **access-list** *access-list-number* {permit|deny}
{host/source source-wildcard|any}
 - c. Έπειτα μπαίνουμε στο interface που θέλουμε να εφαρμόσουμε την access list με την εντολή
[Router(config)#] interface [interface name and number]
 - d. Εφαρμόζουμε την access list με την εντολή
[Router(config-if)#] **ip access-group** *access-list-number* {in|out}

2. Δημιουργία Extended access-list
 - a. Μπαίνουμε σε configure mode με την εντολή
[Router#] configure terminal.
 - b. Από εκεί θέτουμε την access list
 1. IP
access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {deny | permit} *protocol* *source* *source-wildcard* *destination* *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*]
 2. ICMP
access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {deny | permit} **icmp** *source* *source-wildcard* *destination* *destination-wildcard* [*icmp-type* | [*icmp-type* *icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*]
 3. TCP
access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {deny | permit} **tcp** *source* *source-wildcard* [*operator* [*port*]] *destination* *destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*]
 4. UDP
access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {deny | permit} **udp** *source* *source-wildcard* [*operator* [*port*]] *destination* *destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*]
 - c. Έπειτα μπαίνουμε στο interface που θέλουμε να εφαρμόσουμε την access list με την εντολή
[Router(config)#] interface [interface name and number]
 - d. Εφαρμόζουμε την access list με την εντολή
[Router(config-if)#] **ip access-group** *access-list-number* {in|out}

3. Για να περιορίσουμε τις πληροφορίες τις οποίες μαθαίνει ή διαφημίζει ένας δρομολογητής μπορούμε να κάνουμε φιλτράρισμα των BGP routing updates από ή προς συγκεκριμένους γείτονες. Για τον σκοπό αυτό μπορεί να δημιουργηθεί μια access-list η οποία να θέτει κάποιους περιορισμούς:

	Command	Purpose
Step 1	Router# ip as-path access-list access-list-number (permit deny) <i>as-regexp</i>	Defines a BGP-related access list.
Step 2	Router# router bgp as-number	Enters router configuration mode.
Step 3	Router(config-router)# neighbor { <i>ip-address</i> <i>peer-group-name</i> } filter-list access-list-number (in out)	Establishes a BGP filter.

Μετά την εφαρμογή των εντολών αυτών για να ενεργοποιηθούν οι ρυθμίσεις πρέπει να γίνει reset το bgp με την εντολή
[Router#] clear ip bgp *

Σημείωση: Τα regular expressions (as-regexp) δίνονται στο υποστηρικτικό υλικό.