Πανεπιστημιο Δυτικης Μακεδονιας

Τμημα Μηχανικων Πληροφορικης και Τηλεπικοινωνιων

Εργαστήριο Δικτύων και Προηγμένων Υπηρεσιών

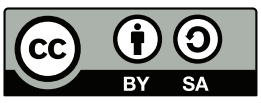
Εργαστήριο 2β: Διευθέτηση μεταγωγέα

Επιμέλεια:

Χρήστος Δαλαμάγκας

Επιβλέπουσα:

Δρ. Μαλαματή Λούτα



Κοζάνη, Ιανουάριος 2019

Περιγραφή

Λέξεις κλειδιά: Βασική παραμετροποίηση μεταγωγέων, ο πίνακας MAC, στατικές/δυναμικές διευθύνσεις MAC, ασφάλεια θυρών.

Προαπαιτούμενες γνώσεις: Εργαστηριακό φυλλάδιο 1α (Εισαγωγή στο Cisco IOS), Βασική ορολογία δικτύων υπολογιστών, ειδικότερα όσον αφορά το επίπεδο ζεύξης δεδομένων.

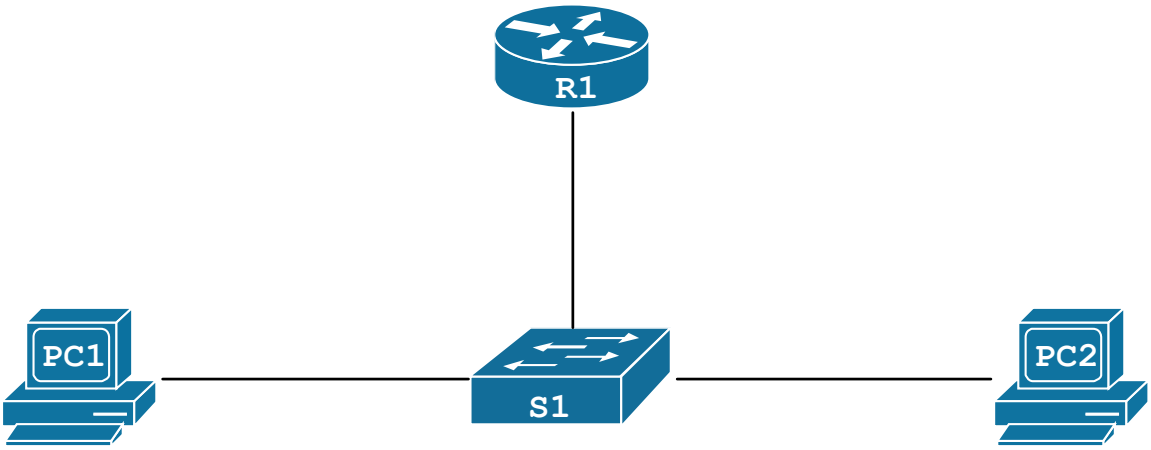
Περιεχόμενα

Κατάλογος σχημάτων

Κατάλογος πινάκων

Εισαγωγή

Αντικείμενο του παρόντος εργαστηριακού φυλλαδίου αποτελεί η επισκόπηση της λειτουργίας των μεταγωγέων, καθώς και η επισκόπηση βασικών εντολών χειρισμού τους. Στο πλαίσιο της εργαστηριακής άσκησης θα υλοποιήσετε την τοπολογία που φαίνεται στο σχήμα 1, η οποία αποτελείται από έναν μεταγωγέα, δυο υπολογιστές και έναν δρομολογητή. Η εργαστηριακή άσκηση αποτελείται από ένα σενάριο, το οποίο δίνει έμφαση στις κολλώδεις διευθύνσεις MAC.



Σχήμα 1: *Βασικό σχέδιο της δικτυακής τοπολογίας*

Για την υλοποίηση της τοπολογίας θα χρειαστείτε τις εξής συσκευές:

- x1 δρομολογητή Cisco 2921
- x2 μεταγωγείς Cisco Catalyst
- x2 υπολογιστές

1 Θεωρητικό υπόβαθρο

Ο μεταγωγέας (switch) είναι μια συσκευή που λειτουργεί κατά βάση στο δεύτερο στρώμα του OSI (στρώμα ζεύξης δεδομένων - data link layer) και χρησιμεύει για την προώθηση πλαισίων στο εύρος ενός δικτύου. Ουσιαστικός ρόλος ενός μεταγωγέα είναι να επιτρέπει την πολλαπλή πρόσβαση συσκευών στο ίδιο φυσικό μέσο μετάδοσης. Για παράδειγμα, στο σχήμα 1 η χρήση του μεταγωγέα επιτρέπει και στους δυο υπολογιστές να έχουν πρόσβαση στο ίδιο φυσικό μέσο, δηλαδή τη ζεύξη με τη διεπαφή του R1.

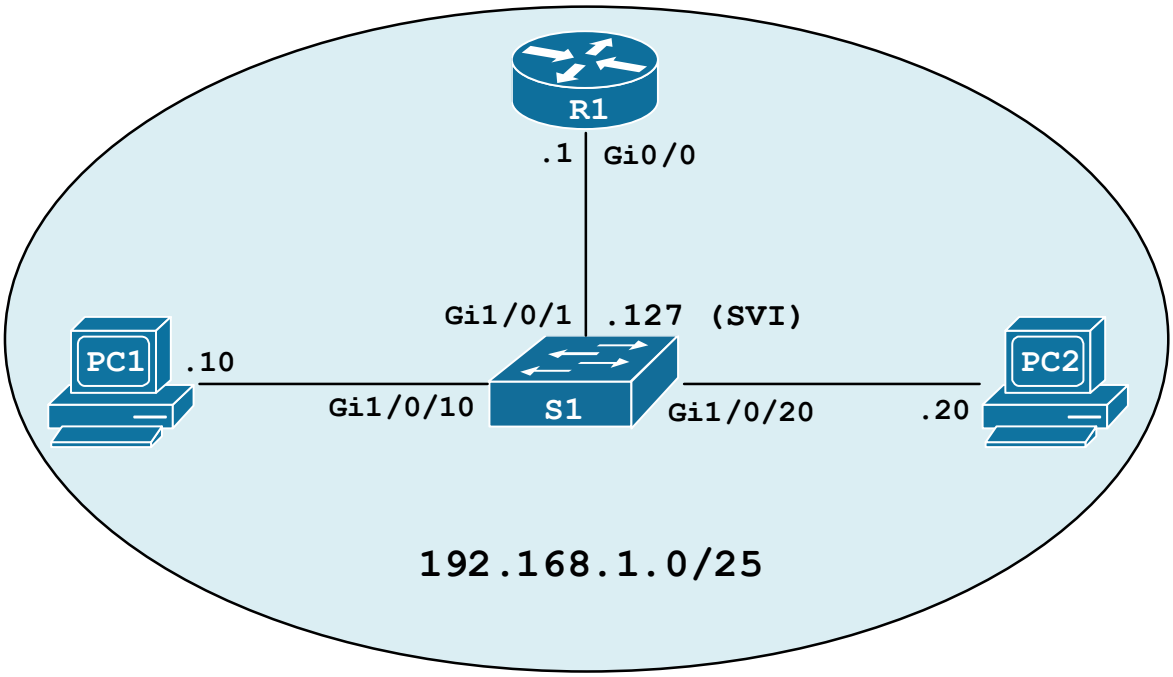
Στα παρακάτω σημεία συνοψίζονται οι βασικές ιδιότητες των μεταγωγέων που τους διαχωρίζει από τους δρομολογητές:

- Σε αντίθεση με τον δρομολογητή, ο οποίος προωθεί πακέτα μεταξύ διαφορετικών δικτύων, οι μεταγωγείς προωθούν πλαίσια μόνο μέσα στο εύρος του φυσικού δικτύου στο οποίο ανήκουν (τομέας ευρυεκπομπής - broadcast domain).
- Ο δρομολογητής επικοινωνεί με διαφορετικά δίκτυα με χρήση διεπαφών (interfaces), ενώ ο μεταγωγέας επικοινωνεί με το δίκτυο χρησιμοποιώντας θύρες (ports). Ουσιασικά, οι θύρες των μεταγωγέων είναι γεφυρωμένες διεπαφές (bridged interfaces), δηλαδή έχουν κατασκευαστεί ώστε να ανήκουν στον ίδιο τομέα ευρυεκπομπής.
- Οι δρομολογητές λαμβάνουν αποφάσεις προώθησης πακέτων εξετάζοντας τον πίνακα δρομολόγησης. Αντίθετα, οι μεταγωγείς λαμβάνουν απόφαση για το που θα προωθήσουν ένα πλαίσιο, εξετάζοντας τον πίνακα MAC.
- Οι δρομολογητές είναι ΚΑΙ μεταγωγείς, με τη διαφορά ότι κάθε διεπαφή ενός δρομολογητή βρίσκεται σε διαφορετικό φυσικό μέσο (τομέα ευρυεκπομπής) από τις υπόλοιπες. Συνεπώς, ο δρομολογητής επικοινωνεί σε επίπεδο μεταγωγής μόνο με τη συσκευή με την οποία συνδέεται απευθείας.
- Οι περισσότεροι μεταγωγείς ενεργοποιούνται αυτόματα, όταν συνδεθούν στην τροφοδοσία ρεύματος. Αντίθετα, οι δρομολογητές διαθέτουν διακόπτη τροφοδοσίας.
- Σε αντίθεση με τις διεπαφές του δρομολογητή, οι θύρες των μεταγωγέων δεν χρειάζονται καμία ρύθμιση για να καταστούν λειτουργικές. Σε περίπτωση που συνδεθεί σε μια θύρα καλώδιο βύσματος RJ-45, και το έτερο άκρο δίνει ήδη τάση, τότε η θύρα ενεργοποιείται αυτόματα και είναι έτοιμη να προωθήσει πλαίσια.

2 Υλοποίηση τοπολογίας

2.1 Αναλυτική σχεδίαση τοπολογίας

Όπως και στο προηγούμενο μέρος του εργαστηριακού φυλλαδίου, πριν την υλοποίηση της τοπολογίας θα πρέπει πρώτα να καθοριστεί η αναλυτική τοπολογία του δικτύου, δηλαδή να προσδιοριστούν τα δίκτυα (ή το δίκτυο) που συνθέτουν την τοπολογία, οι διευθύνσεις IP και οι διεπαφές που θα χρησιμοποιηθούν. Η αναλυτική σχεδίαση της τοπολογίας φαίνεται στο σχήμα 2 και το αντίστοιχο σχήμα διευθυνσιοδότησης στον πίνακα 1.



Σχήμα 2: *Το σχέδιο της αναλυτικής τοπολογίας προς υλοποίηση.*

Συσκευή	Διεπαφή	Διεύθυνση IP	Μάσκα υποδικτύου	Προεπιλεγμένη πύλη
R1	`G0/0`	`192.168.1.1`	`255.255.255.128`	-
S1	SVI	`192.168.1.127`	`255.255.255.128`	`192.168.1.1`
PC1	NIC	`192.168.1.10`	`255.255.255.128`	`192.168.1.1`
PC2	NIC	`192.168.1.20`	`255.255.255.128`	`192.168.1.1`

Πίνακας 1: *Σχήμα διευθυνσιοδότησης της τοπολογίας*

2.2 Καλωδίωση δικτύου

Ως αρχικό βήμα, συνδέστε με καλώδια UTP τις συσκευές μεταξύ τους, όπως φαίνεται στο σχήμα της τοπολογίας. Αν δεν είναι δυνατό να χρησιμοποιήστε τις διεπαφές που φαίνονται στο σχήμα τοπολογίας, τότε αποφασίστε εσείς για τις διεπαφές που θα χρησιμοποιήσετε.

2.3 Παραμετροποίηση μεταγωγέα

Συνδεθείτε με κονσόλα στις συσκευές Cisco, σύμφωνα με τις οδηγίες του φυλλαδίου «Εισαγωγή στο Cisco IOS», και βεβαιωθείτε ότι αυτές λειτουργούν με τις εργοστασιακές τους ρυθμίσεις. Αν εντοπίσετε παλαιότερες ρυθμίσεις, επαναφέρετε τις συσκευές στις εργοστασιακές τους ρυθμίσεις πριν προχωρήσετε.

Παρόλο που οι μεταγωγείς προωθούν πλαίσια χωρίς καμία πρόσθετη παρέμβαση, συνήθης πρακτική αποτελεί η ανάθεση διεύθυνσης IP στους μεταγωγείς, και συγκεκριμένα στην εικονική διεπαφή (Switch Virtual Interface - SVI) του προεπιλεγμένου τους VLAN, για διαχειριστικούς λόγους, όπως αυτός της απομακρυσμένης διαχείρισης μέσω SSH. Η SVI είναι μια εικονική διεπαφή, δηλαδή δεν αντιστοιχεί σε φυσική διεπαφή ή θύρα, η οποία αντιστοιχίζεται με κάποιο VLAN. Από προεπιλογή, όλες οι θύρες ενός μεταγωγέα ανήκουν στο VLAN 1.

Με τις εντολές που ακολουθούν, αναθέστε στην SVI του `vlan 1` του μεταγωγέα S1 τις κατάλληλες ρυθμίσεις IP, σύμφωνα με τον πίνακα 1:

```
S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.3 255.255.255.128
S1(config-if)#no shutdown
S1(config-if)#
```

Αν ο μεταγωγέας πρόκειται να διαχειριστεί από απομακρυσμένο δίκτυο που δεν ανήκει σε αυτό του μεταγωγέα, τότε πρέπει να ρυθμιστεί προεπιλεγμένη πύλη. Αν και για τη δεδομένη τοπολογία ο ορισμός προεπιλεγμένης πύλης δεν έχει κάποια σημασία, αφού το δίκτυο δεν επικοινωνεί με άλλα δίκτυα, ο ορισμός του R1 ως προεπιλεγμένη πύλη δικτύου του S1 μπορεί να γίνει με τις εξής εντολές:

```
S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway 192.168.1.1
S1(config)#
```

2.4 Διευθυνσιοδότηση δρομολογητή/υπολογιστών

Δώστε τις κατάλληλες εντολές στον δρομολογητή R1 για τη σωστή παραμετροποίηση της διεπαφής **`G0/0`**, σύμφωνα με το σχήμα διευθυνσιοδότησης. Κατόπιν, εφαρμόστε τις κατάλληλες ρυθμίσεις IP στους υπολογιστές.

2.5 Δοκιμές συνδεσιμότητας

Επιβεβαιώστε την ορθότητα των ρυθμίσεων, δοκιμάζοντας τη συνδεσιμότητα των PC1, PC2 και SVI του S1 με την εντολή **`ping`**. Αν οι εντολές εκτελεστούν με επιτυχία, τότε έχετε υλοποιήσει σωστά το δίκτυο και μπορείτε να προχωρήσετε στα επόμενα βήματα παραμετροποίησης των μεταγωγέων.

Εμπλέκεται ο δρομολογητής στην επικοινωνία των PC1 και PC2; Αν όχι, γιατί;

3 Ρυθμίσεις θυρών μεταγωγέα και σφάλματα

Βασική παραμετροποίηση που δέχονται οι θύρες των μεταγωγέων, καθώς και πηγή σφαλμάτων, αποτελεί η **καταστάση αμφιδρομικότητας** (duplex mode), η οποία έχει να κάνει με το αν στο ίδιο καλώδιο μπορούν να μεταδώσουν ταυτόχρονα και τα δυο άκρα (full-duplex) ή εναλλάξ (half-duplex). Μια θύρα μπορεί να λειτουργήσει σε μια από τις τρεις παρακάτω καταστάσεις:

`auto`: Ο μεταγωγέας διαπραγματεύεται αυτόματα με το άλλο άκρο της σύνδεσης την κατάσταση λειτουργίας της θύρας (autonegotiation).

`full`: Πλήρως αμφίδρομη κατάσταση λειτουργίας (full-duplex).

`half`: Ημιαμφίδρομη κατάσταση λειτουργίας (half-duplex), προεπιλογή για τις παλιές διεπαφές 10BASE-T.

Λάθος ρύθμιση μπορεί να οδηγήσει σε **αναντιστοιχία αμφίδρομης κατάστασης** (duplex mismatch). Αυτό προκαλείται όταν δυο θύρες έχουν οριστεί σε διαφορετικές καταστάσεις, συνήθως λόγω αποτυχίας της αυτόματης διαπραγμάτευσης ή χειροκίνητου ορισμού των διεπαφών σε διαφορετικές καταστάσεις. Για να αποφύγετε την αναντιστοιχία, πρέπει να επιβεβαιώνετε την κατάσταση των διεπαφών σε πλήρως αμφίδρομη.

Η κατάσταση μιας θύρας γίνεται εμφανής με την εντολή `show`. Για παράδειγμα, μπορείτε να διαπιστώσετε την κατάσταση της διεπαφής `GigabitEthernet1/0/1` με την εντολή:

```
S1>show interface Gi1/0/1
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.c962.4219 (bia 0001.c962.4219)
 BW 1000000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  ...
```

Όπως και στους δρομολογητές, για να παραμετροποιήσετε μια διεπαφή/θύρα, πρέπει να εισέλθετε σε κατάσταση ρύθμισης διεπαφής (interface configuration mode). Αυτό γίνεται με την εντολή `interface`, ακολουθούμενη από το όνομα της διεπαφής:

```
S1>enable
S1#configure terminal
S1(config)#interface Gi1/0/1
S1(config-if)#
```

Αν θέλετε να εφαρμόσετε τις ίδιες ρυθμίσεις σε περισσότερες διεπαφές, μπορείτε να επιλέξετε το επιθυμητό εύρος διευθύνσεων με τη λέξη-κλειδί `range`. Για παράδειγμα:

```
S1(config)#interface range GigabitEthernet 1/0/1 - 24
S1(config-if-range)#
```

Για να αλλάξετε την αμφιδρομικότητα μιας διεπαφής πρέπει να εισέλθετε πρώτα σε κατάσταση ρύθμισης διεπαφής και κατόπιν να δώσετε την εντολή `duplex`:

```
S1(config-if)#duplex {auto | full | half}
```

Για μια θύρα είναι δυνατός ο χειροκίνητος ορισμός της ταχύτητας μετάδοσης. Στις περισσότερες περιπτώσεις είναι προεπιλεγμένη η αυτόματη διαπραγμάτευση της ταχύτητας, αν και υπάρχουν σπάνιες περιπτώσεις στις οποίες πρέπει να οριστεί χειροκίνητα η ταχύτητα μετάδοσης. Λανθασμένη ρύθμιση μπορεί να οδηγήσει σε αδυναμία επικοινωνίας των δυο άκρων, αφού διαφορετική ταχύτητα συνεπάγεται διαφορετική διαμόρφωση του σήματος στο φυσικό στρώμα του OSI. Ο ορισμός της ταχύτητας γίνεται από την κατάσταση ρύθμισης διεπαφής, με χρήση της εντολής `speed`:

```
S1(config-if)#speed {auto | 10 | 100 | 1000}
```

Τέλος, μια πρόσθετη πηγή σφαλμάτων αποτελεί και ο τύπος καλωδίου UTP που χρησιμοποιείται σε μια σύνδεση, δηλαδή αν είναι crossover ή straight-through. Για συσκευές που λειτουργούν σε διαφορετικά στρώματα του TCP/IP (μεταγωγέας και δρομολογητής, υπολογιστής και μεταγωγέας) απαιτείται καλώδιο straight-through, ενώ για συσκευές που λειτουργούν στο ίδιο στρώμα (υπολογιστής με δρομολογητή, δρομολογητής με δρομο-

λογητή, μεταγωγέας με μεταγωγέα) χρειάζεται καλώδιο crossover.[1] Ο περιορισμός αυτός αντιμετωπίζεται στις νεώτερες συσκευές με τη λειτουργία **Auto-MDIX**, η οποία προσαρμόζει αυτόματα μια θύρα, ανάλογα με τον τύπο του καλωδίου που απαιτείται. Η εντολή για την ενεργοποίηση της λειτουργίας είναι η `mdix auto`. Επισημαίνεται ότι αν ενεργοποιηθεί η Auto-MDIX, θα πρέπει η θύρα να λειτουργεί σε αυτόματη διαπραγμάτευση.

```
S1(config)#interface Gi1/0/1
S1(config-if)#duplex auto
S1(config-if)#speed auto
S1(config-if)#mdix auto
S1(config-if)#end
S1(config)#
```

4 Ο πίνακας MAC

Κάθε μεταγωγέας, καθώς και οποιαδήποτε συσκευή με δυνατότητες μεταγωγής πλαισίων, όπως ο δρομολογητής, διατηρεί έναν πίνακα MAC, ο οποίος χρησιμοποιείται για τη λήψη αποφάσεων μεταγωγής, δηλαδή σε ποια θύρα πρέπει να προωθηθεί ένα πλαίσιο, με βάση τη διεύθυνση MAC προορισμού. Λόγο του ρόλου του, ο πίνακας αποθηκεύεται σε μια μνήμη τύπου CAM (Content-Addressable Memory).

Με την εντολή `show mac address-table` μπορείτε να δείτε το περιεχόμενο του πίνακα MAC για έναν μεταγωγέα ή δρομολογητή. [2]:

```
S1>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0050.0f06.b201    DYNAMIC     Gi1/0/1

S1>
```

Οι μεταγωγείς ανανεώνουν τους πίνακες MAC δυναμικά, εξετάζοντας για κάθε εισερχόμενο πλαίσιο τα εξής:

- τη διεύθυνση MAC πηγής (source mac address).

[1] Ο λόγος για τον οποίον οι προαναφερθείσες συνδέσεις απαιτούν crossover ή straight-through δεν είναι ότι λειτουργούν σε διαφορετικά ή ίδια στρώματα του TCP/IP. Ωστόσο, η παρατήρηση αυτή είναι χρήσιμη για τη μνημόνευση του απαιτούμενου τύπου καλωδίου ανά περίπτωση.

[2] Αν δεν βλέπετε κάποια συσκευή από αυτές της τοπολογίας στον πίνακα MAC, δοκιμάστε να προκαλέσετε δικτυακή κίνηση με το `ping`.

- την εισερχόμενη θύρα (ingress port).

Είναι εφικτό να προστεθούν και στατικές καταχωρήσεις στον συγκεκριμένο πίνακα από τον διαχειριστή ενός δικτύου με την εντολή `mac address-table static`. Για παράδειγμα, με την ακόλουθη εντολή μπορείτε να ορίσετε πως πλαίσια με διεύθυνση προορισμού `901B.0E13.AC0A` πρέπει να προωθούνται προς τη θύρα `Gi1/0/1`, η οποία ανήκει στο VLAN 1:

```
S1(config)#mac address-table static 901B.0E13.AC0A vlan 1 int Gi1/0/1
```

Για να διαγράψετε τη στατική ανάθεση διεύθυνσης MAC, απλά αναιρέστε την αντίστοιχη εντολή στατικής ανάθεσης με το `no`, δίνοντας την εξής εντολή:

```
S1(config)#no mac address-table static 901B.0E13.AC0A vlan 1 int Gi1/0/1
```

5 Ασφάλεια θυρών

Η λειτουργία ασφάλειας θυρών μπορεί να περιορίσει το πλήθος των διευθύνσεων MAC που μπορεί να συνδεθεί σε μια θύρα, ποιες διευθύνσεις MAC μπορούν να χρησιμοποιήσουν συγκεκριμένες θύρες του μεταγωγέα, καθώς και τι συνέπειες μπορεί να επιφέρει η παραβίαση ενός τέτοιου κανόνα. Στον πίνακα 2 παρατίθενται οι προεπιλεγμένες ρυθμίσεις ασφαλείας για κάθε θύρα, όσον αφορά τους μεταγωγείς Cisco.

Χαρακτηριστικό	**Προεπιλεγμένη ρύθμιση**
Ασφάλεια θυρών	Απενεργοποιημένη
Μέγιστος αριθμός ασφαλών διευθύνσεων	1
Κατάσταση παράβασης (Violation mode)	Απενεργοποίηση θύρας (Shutdown)
Λήξη (Aging)	Απενεργοποιημένη
Τύπος λήξης (Aging type)	Απόλυτος (Absolute)
Στατική λήξη (Static aging)	Απενεργοποιημένη
Κολλώδης διεύθυνση (Sticky address)	Απενεργοποιημένη

Πίνακας 2: *Οι προεπιλογές της λειτουργίας ασφάλειας θυρών.*

Όταν η ασφάλεια θυρών είναι απενεργοποιημένη για μια θύρα, τότε οποιαδήποτε συσκευή μπορεί να χρησιμοποιήσει αυτή τη θύρα. Αν ενεργοποιηθεί η ασφάλεια θυρών για μια θύρα, τότε μόνο συγκεκριμένες διευθύνσεις MAC μπορούν να στείλουν πλαίσια μέσω αυτής. Τα είδη ασφαλών διευθύνσεων MAC συνοψίζονται στα εξής:

- **Ασφαλείς στατικές MAC**: Είναι συγκεκριμένες διευθύνσεις που μπορούν να χρησιμοποιήσουν μια θύρα, οι οποίες ορίζονται χειροκίνητα από τον διαχειριστή. Οι διευθύνσεις που ορίζονται με αυτόν τον τρόπο αποθηκεύονται στον πίνακα MAC και στις τρέχουσες ρυθμίσεις (running configuration). Αν ο δια-

χειριστής αποθηκεύσει τις τρέχουσες ρυθμίσεις (`copy run start`), τότε οι διευθύνσεις αυτές ανακτώνται έπειτα από επανεκκίνηση της συσκευής.

- **Ασφαλείς δυναμικές MAC**: Είναι οι διευθύνσεις που μαθαίνονται δυναμικά για μια θύρα και αποθηκεύονται μόνο στον πίνακα MAC. Οι διευθύνσεις αυτές δεν αποθηκεύονται στις τρέχουσες ρυθμίσεις της συσκευής.
- **Ασφαλείς κολλώδεις (sticky) MAC**: Πρόκειται για τις διευθύνσεις που μαθαίνονται δυναμικά ή ορίζονται χειροκίνητα, οι οποίες αποθηκεύονται και στον πίνακα MAC και στις τρέχουσες ρυθμίσεις. Αν ο διαχειριστής αποθηκεύσει τις τρέχουσες ρυθμίσεις (`copy run start`), τότε οι διευθύνσεις αυτές ανακτώνται έπειτα από επανεκκίνηση της συσκευής.

5.1 Βασικές ρυθμίσεις ασφαλούς λειτουργίας θυρών

Για να προβάλλετε τις τρέχουσες ρυθμίσεις ασφαλείας θυρών για μια ή όλες τις θύρες μπορείτε να δώσετε την εξής εντολή:

```
S1>show port-security [int Gi1/0/1]
```

Αν δεν εμφανιστεί κάτι, αυτό σημαίνει πως η ασφάλεια θυρών είναι απενεργοποιημένη για την θύρα ή τις θύρες. Για να ενεργοποιήσετε την ασφάλεια θυρών μπορείτε να δώσετε εντολές του πίνακα 3, αφού έχετε εισέλθει στην κατάσταση ρυθμίσεων διεπαφής (ή του εύρους διευθύνσεων) που επιθυμείτε να ρυθμίσετε:

Εντολή	Περιγραφή
`S1(config)#interface Gi1/0/1`	Είσοδος σε κατάταση ρύθμισης διεπαφής
`S1(config-if)#switchport mode access`	Προαιρετικό. Η εντολή ορίζει ρητά τη θύρα σε κατάσταση πρόσβασης, ώστε να αποτραπεί το ενδεχόμενο μετατροπής της σε κατάσταση trunk από το πρωτόκολλο DTP. Οι θύρες trunk δεν δέχονται ρυθμίσεις ασφαλείας.
`S1(config-if)#switchport port-security`	Ενεργοποίηση της ασφάλειας θυρών με τις προεπιλεγμένες ρυθμίσεις.

Πίνακας 3: *Εντολές για την ενεργοποίηση ασφάλειας θυρών σε μια διεπαφή*

Έχοντας εκτελέσει τις παραπάνω εντολές και προβάλλοντας ξανά τις ρυθμίσεις ασφαλείας θυρών, μπορείτε να πληροφορηθείτε για το μέγιστο πλήθος επιτρεπόμενων MAC διευθύνσεων που μπορεί να συνδεθεί στη συγκεκριμένη θύρα (`MacSecureAddr`), το πλήθος των διευθύνσεων MAC που αντιστοιχεί σε μια θύρα (`CurrentAddr`), το πλήθος των παραβάσεων του μέτρου ασφαλείας που έχει καταγραφεί (`SecurityViolation`), καθώς και την ενέργεια που εφαρμόζεται σε περίπτωση παραβίασης (`Security Action`). Αυτές είναι οι προεπιλεγμένες ρυθμίσεις που παρατίθενται στον πίνακα 2.

```
S1#show port-security
```

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
---------------------------------------------------------------------
     Gi1/0/1        1           0                 0          Shutdown
---------------------------------------------------------------------
S1#
```

Μπορείτε να δώσετε την παρακάτω εντολή για να αυξήσετε το μέγιστο πλήθος επιτρεπόμενων ασφαλών διευθύνσεων MAC (`MacSecureAddr`) σε 2:

```
S1(config-if)#switchport port-security maximum 2
```

Με την παραπάνω εντολή, ο μεταγωγέας θεωρεί ασφαλείς και εξυπηρετεί μόνο τις πρώτες δυο διευθύνσεις MAC που θα μάθει δυναμικά. Αν έλθει στη συγκεκριμένη θύρα ένα πλαίσιο με MAC πηγής μια τρίτη διεύθυνση MAC, τότε θα γίνει ο,τι περιγράφεται στη στήλη `Secrity Action` της εντολής `show port-security`.

Για να απενεργοποιήσετε την ασφάλεια θύρας και να διαγράψετε όλες τις σχετικές ρυθμίσεις για τη συγκεκριμένη θύρα, αρκεί να δώσετε την εντολή:

```
S1(config-if)#no switchport port-security
```

5.2 Στατική ρύθμιση

Η στατική ρύθμιση ασφαλείας σε μια διεπαφή χρησιμεύει ώστε να οριστούν συγκεκριμένες διευθύνσεις MAC που μπορούν να συνδεθούν σε μια θύρα. Η προσθήκη μιας διεύθυνσης ως στατική γίνεται με την ακόλουθη εντολή:

```
S1(config-if)#switchport port-security mac-address XXXX.XXXX.XXXX
```

5.3 Κολλώδης διεύθυνση (Sticky)

Οι κολλώδεις διευθύνσεις είναι μια συχνά χρησιμοποιούμενη πρακτική, κατά την οποία οι διευθύνσεις που μαθαίνονται δυναμικά, «κολλάνε» στις τρέχουσες ρυθμίσεις της συσκευής και μπορούν να αποθηκευτούν μόνιμα όταν ο διαχειριστής αποθηκεύσει τις τρέχουσες ρυθμίσεις. Σε περιβάλλον εργασίας, όπου συνδέονται δεκάδες απλοί υπολογιστές ή εξυπηρετητές σε έναν μεταγωγέα, υπάρχει η επιθυμία για κάθε θύρα να αποτρέπεται το ενδεχόμενο κάποιος να παρεμβάλλει μια δεύτερη συσκευή ή να αφαιρέσει μια ήδη υπάρχουσα συσκευή για να χρησιμοποιήσει τη δική του. Δεδομένου ότι είναι μη πρακτική η στατική ρύθμιση ασφαλείας για κάθε μια θύρα και, παράλληλα, υπάρχει η επιθυμία οι ασφαλείς διευθύνσεις να παραμένουν μόνιμα, ακόμα και σε περίπτωση επανεκκίνησης, η λύση της κολλώδους ρύθμισης είναι η καταλληλότερη.

Μπορείτε να ενεργοποιήσετε την εν λόγω ρύθμιση για μια ασφαλή θύρα με την εντολή:

```
S1(config-if)#switchport port-security mac-address sticky
```

Τη ρύθμιση sticky μπορείτε να την εφαρμόσετε αντίστοιχα και για εύρος διευθύνσεων στις οποίες έχει ρυθμιστεί η ασφάλεια θυρών:

```
S1(config-if)#interface range GigabitEthernet 1/0/1 - 24
S1(config-if-range)#switchport port-security mac-address sticky
```

5.4 Λήξη και Κατάσταση παραβίασης

Οι καταστάσεις παραβίασης (violation modes), δηλαδή τι ενέργεια θα ληφθεί σε περίπτωση που παραβιαστεί μια ρύθμιση ασφαλείας, διακρίνονται στις εξής:

- **Protect**: Τα πλαίσια που παραβιάζουν τους κανόνες ασφαλείας απορρίπτονται, χωρίς να παραχθεί κάποιο μήνυμα ή ειδοποίηση προς τον διαχειριστή.
- **Restrict**: Τα πλαίσια που παραβιάζουν τους κανόνες ασφαλείας απορρίπτονται και κατόπιν παράγεται κατάλληλο μήνυμα syslog που αποστέλλεται στον διαχειριστή, μέσω του τερματικού ή προς ειδικό εξυπηρετητή Syslog.
- **Shutdown**: Όταν εντοπιστεί πλαίσιο που παραβαίνει τις ρυθμίσεις ασφαλείας, τότε το πλαίσιο απορρίπτεται, η διεπαφή κλείνει διαχειριστικά και στέλνεται ειδοποίηση SNMP. Αυτή είναι η προεπιλεγμένη κατάσταση παραβίασης για κάθε ασφαλή θύρα. Για να ενεργοποιηθεί η εν λόγω διεπαφή (έστω `Gi1/0/1`) πρέπει να δοθούν διαδοχικά οι εξής εντολές:

  ```
  S1(config)#int Gi1/0/1
  S1(config-if)#shutdown
  S1(config-if)#no shutdown
  ```

Ο ορισμός συγκεκριμένης κατάστασης παραβίασης για μια ασφαλή θύρα μπορεί να γίνει με την εξής εντολή:

```
S1(config-if)#switchport port-security violation {protect | restrict |
shutdown}
```

Τέλος, με την λειτουργία λήξης (aging) μπορείτε να ορίσετε το χρονικό διάστημα σε λεπτά, για το οποίο μια θύρα θα είναι ασφαλής. Η εντολή ακολουθεί την παρακάτω γενική μορφή:

```
S1(config-if)#switchport port-security { aging [ static | time aging_time
| type ( absolute | inactivity ) ] }
```

Τα ορίσματα της εντολής `aging` είναι τα εξής:

static : Ορίζεται ότι το aging αφορά και τις στατικές διευθύνσεις MAC.

time : Ορίζει την χρονική διάρκεια που θα ισχύει ο κανόνας ασφαλείας σε Ν λεπτά.

type : Ο τύπος `absolute` ορίζει ότι το διάστημα Ν λεπτών έχει ως εκκίνηση την στιγμή που τίθεται σε ισχύ ο κανόνας. Ο τύπος `inactivity` ορίζει ότι το διάστημα Ν λεπτών αφορά τον χρόνο για τον οποίο δεν παρατηρείται δικτυακή δραστηριότητα (κίνηση πακέτων) στην διεπαφή.

6 Σενάριο: Κολλώδεις διευθύνσεις MAC

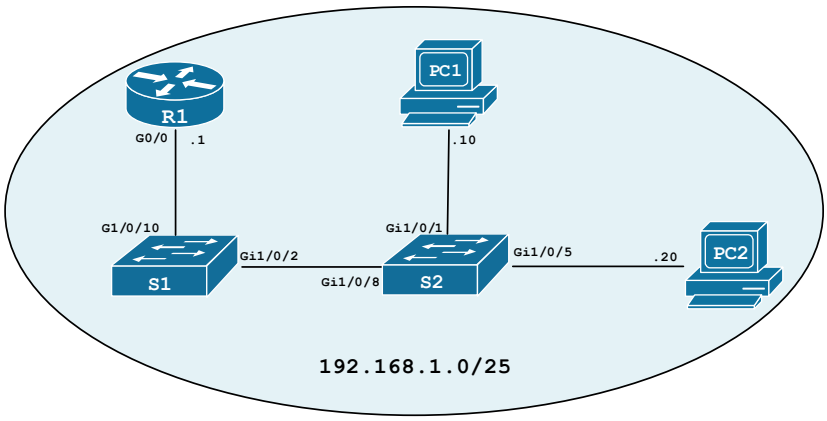
Πριν ξεκινήσετε, διαγράψτε τυχόν ρυθμίσεις που εφαρμόσατε εκτελώντας τα παραδείγματα που παρουσιάστηκαν στις προηγούμενες ενότητες του φυλλαδίου.

Στο πλαίσιο του σεναρίου, αναφερόμενοι στην αρχική τοπολογία που υλοποιήσατε (σχήμα 2), σας ζητείται να εφαρμόσετε τις εξής ρυθμίσεις στον μεταγωγέα S1:

- Ενεργοποιήστε την ασφάλεια θυρών σε όλες τις θύρες με κατάλληλη χρήση της εντολής `interface range`.
- Ενεργοποιήστε την κατάσταση sticky για όλες τις θύρες.
- Βεβαιωθείτε ότι μόνο μια διεύθυνση MAC μπορεί να χρησιμοποιήσει την κάθε θύρα.
- Ενεργοποιήστε την κατάλληλη κατάσταση παραβίασης, ώστε να περιορίζεται η πρόσβαση στις διευθύνσεις MAC που παραβιάζουν τον κανόνα, με παραγωγή σχετικής ειδοποίησης syslog.

Διατηρώντας την αρχική τοπολογία που υλοποιήσατε στην αρχή της εργαστηριακής άσκησης και αφού ολοκληρώσετε τα παραπάνω ζητούμενα, στείλτε πακέτα ICMP μεταξύ των δικτυακών συσκευών, ώστε να ανανεωθούν οι πίνακες MAC και να καταγραφούν από τον μεταγωγέα S1 οι ασφαλείς διευθύνσεις MAC για κάθε θύρα.

Δοκιμάστε να παραβιάσετε τους κανόνες που ορίσατε. Συγκεκριμένα, παρεμβάλλετε έναν δεύτερο μεταγωγέα μεταξύ του S1 και του PC2, συνδέοντας σε αυτόν τον PC1. Με αυτή την τροποποίηση, η τοπολογία πρέπει να έχει τη μορφή που απεικονίζεται στο σχήμα 3.



Σχήμα 3: *Η νέα μορφή της τοπολογίας.*

Έχοντας εφαρμόσει την κατάλληλη συνδεσμολογία που παραβιάζει τους κανόνες ασφαλείας, στείλτε πακέτα ICMP από τους υπολογιστές προς τον δρομολογητή. Πρέπει να επιτρέπεται στον PC2 να στέλνει πλαίσια προς τον R1, ενώ στον PC2 όχι. Παρατηρώντας το τερματικό κονσόλας του S1 καταγράψτε τα σχετικά μηνύματα syslog.