**ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ**
**ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ**
**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε**

# ΜΕΛΕΤΗ ΤΟΥ SPANNING TREE PROTOCOL ΜΕ ΧΡΗΣΗ ΤΟΥ GNS3

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ του**

ΠΑΝΤΑΖΗ ΑΘΑΝΑΣΙΟΥ (2695)

Επιβλέπων: Αναστάσιος Χ. Πολίτης, καθηγητής εφαρμογών

**ΣΕΡΡΕΣ, ΜΑΪΟΣ 2017**

**Υπεύθυνη Δήλωση** : *Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής του Τ.Ε.Ι. Κεντρικής Μακεδονίας.*

# ΠΕΡΙΛΗΨΗ

Σκοπός αυτής της πτυχιακής εργασίας είναι η μελέτη του πρωτοκόλλου Spanning Tree Protocol που ανήκει στο πρότυπο 802.1D και υλοποιείται στις συσκευές διασύνδεσης ενός τοπικού δικτύου τεχνολογίας Ethernet, τα switches.

Αρχικά, στο πρώτο κεφαλαίο γίνεται μια ιστορική αναδρομή της τεχνολογίας για τη δημιουργία των αρχικών τοπικών δικτύων τεχνολογίας Ethernet και της κατασκευής των πρώτων συσκευών διασύνδεσης δικτύου. Έπειτα, στο δεύτερο κεφαλαίο θα αναφερθούμε στα switches, αναλύοντας τη χρησιμότητα και το τρόπο λειτουργία τους. Στη συνέχεια, στο τρίτο κεφάλαιο αναλύεται η λειτουργία του βασικού πρωτοκόλλου Spanning Tree Protocol καθώς και των διάφορων εκδοχών του πρωτοκόλλου. Τέλος, στο τέταρτο κεφάλαιο, θα δείξουμε στη πράξη μέσω της εφαρμογής GNS3 πως εφαρμόζεται το Spanning Tree Protocol στα switches εκτελώντας διάφορες προσομοιώσεις.

# Περιεχόμενα

# ΚΕΦΑΛΑΙΟ 1

## 1. ΕΙΣΑΓΩΓΗ

Το πρώτο τοπικό δίκτυο τεχνολογίας Ethernet (Ethernet Local Area Network) αναπτύχθηκε από την εταιρία Xerox PARC γύρω στο 1973-1975. Στα μέσα της δεκαετίας του 1980 η οργάνωση IEEE τυποποίησε το Ethernet LAN ως το πρότυπο 802.3. Τα Ethernet LANs λειτουργούν καλύτερα με μικρό αριθμό μηχανών που στέλνουν μεγάλο όγκο πληροφοριών σε μεγάλο χρονικό διάστημα. Η τεχνολογία Ethernet που είναι και η πιο συνηθισμένη δουλεύει στα 10 Mbs. Καθώς όμως η τεχνολογία εξελίχθηκε ραγδαία με τη δημιουργία του Διαδικτύου (Internet), την ανάπτυξη των πρώτων προσωπικών υπολογιστών (PCs) και την χρήση τους στα τοπικά δίκτυα άρχισαν να εμφανίζονται προβλήματα στη λειτουργία των τοπικών δικτύων που ήταν αρκετά εμφανείς. Οι χρήστες αυξήθηκαν υπερβολικά καθώς και η ανάγκη για την αποστολή δεδομένων σε μικρότερα χρονικά διαστήματα. Αυτό είχε σαν αποτέλεσμα η διαδικασία της λειτουργίας της τεχνολογίας Ethernet να επιβραδύνει την αποτελεσματικότητα του και οι χρήστες να βιώνουν μικρούς χρόνους απόκρισης. Για την αντιμετώπιση αυτού του προβλήματος έπρεπε τα τοπικά δίκτυα να χωριστούν σε τμήματα.

Η πρώτη δικτυακή συσκευή για τον διαχωρισμό των τοπικών δικτύων σε τμήματα ήταν, και είναι ακόμη και σήμερα η γέφυρα (bridge). Οι πρώτες γέφυρες κατασκευάστηκαν στις αρχές του 1980, είχαν δύο θύρες, και μπορούσαν να συνδέσουν δύο τοπικά δίκτυα μαζί μέσω ομοαξονικού καλωδίου. Λόγω των λίγων θυρών που είχαν οι γέφυρες, τα τμήματα στα οποία χωριζόταν ένα δίκτυο ήταν ελάχιστα, σε αντίθεση με τα πεδία σύγκρουσης (collision domain) που δημιουργόντουσαν λόγω της αυξημένης κίνησης δεδομένων και των πολλών χρηστών ενός δικτύου. Για τον λόγο αυτό, μετά από λίγα χρόνια αναπτύχθηκαν οι μεταγωγείς (switches).

Τα switches κατασκευάστηκαν στα τέλη της δεκαετίας του 1980 και είναι ουσιαστικά μια συσκευή που περιέχει πολλαπλές γέφυρες. Στο επόμενο

κεφάλαιο θα εξηγήσουμε τη λειτουργία του switch, καθώς μέχρι και σήμερα, είναι μια συσκευή που χρησιμοποιείται και αποτελεί το μεγαλύτερο μέρος ενός τοπικού δικτύου αφού οι χρηστές χρησιμοποιούν και συνδέουν πολλαπλές συσκευές σε θέσεις εργασίας σε κάποιο δίκτυο ή στο διαδίκτυο μέσω αυτού.

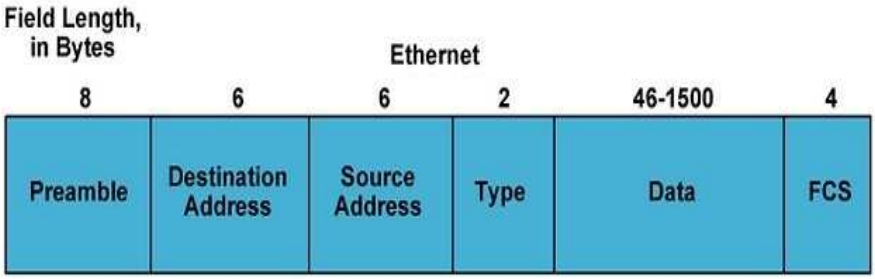
# ΚΕΦΑΛΑΙΟ 2

## 2. LAYER 2 SWITCHES

## 2.1 ΠΛΑΙΣΙΑ

Τα LAN εξασφαλίζουν τη μετακίνηση δεδομένων μεταξύ των υπολογιστών και των συσκευών που συμμετέχουν στο LAN, ώστε να μπορούν να επικοινωνούν. Για να γίνει αυτό, το λογισμικό των δικτύων οργανώνει τα δεδομένα σε πλαίσια που λέγονται Ethernet Frames. Τα πλαίσια που ταξιδεύουν μέσα σε ένα δίκτυο περιέχουν ακολουθίες πληροφοριών των οποίων η μορφή είναι τυποποιημένη.[1]

Η μορφή για ένα τέτοιου είδους πλαισίου Ethernet, περιλαμβάνει μια διεύθυνση προορισμού στην αρχή που περιέχει τη διεύθυνση της συσκευής στην οποία αποστέλλεται το πλαίσιο. Ακολουθεί μια διεύθυνση αποστολέα που περιέχει τη διεύθυνση της συσκευής που στέλνει το πλαίσιο. Οι διευθύνσεις ακολουθούνται από διάφορα άλλα πεδία, συμπεριλαμβανομένου το πεδίο δεδομένων που μεταφέρει τα δεδομένα που αποστέλλονται μεταξύ των υπολογιστών, όπως φαίνεται στην εικόνα που ακολουθεί.[1]




***Εικόνα 2.1:*** *Βασική δομή ενός Ethernet Frame*.[32]

Τα πλαίσια καθορίζονται από το δεύτερο επίπεδο του μοντέλου αναφοράς OSI, το επίπεδο σύνδεσης δεδομένων. Το μοντέλο αναφοράς OSI αναπτύχθηκε για να οργανώνει τα είδη των πληροφοριών που αποστέλλονται

μεταξύ των υπολογιστών. Χρησιμοποιείται για να καθορίσει τον τρόπο με τον οποίο θα αποστέλλονται οι πληροφορίες και να δομήσει την ανάπτυξη των προτύπων για τη μεταφορά των δεδομένων. Από τότε που τα Ethernet switches λειτουργούν βάση των πλαισίων ενός τοπικού δικτύου στο επίπεδο σύνδεσης δεδομένων, θα ακούσετε να αναφέρονται σε αυτά με διάφορες ορολογίες όπως συσκευές διασύνδεσης ή συσκευές δευτέρου επιπέδου ή μεταγωγείς δευτέρου επιπέδου.[1]

Ένα switch δέχεται τυπικά τρία είδη πλαισίων, χωρίς κάποιο συγκεκριμένο προορισμό. Τα πλαίσια αυτά με τη σειράς τους μεταδίδονται προς όλες τις θύρες ενός switch εκτός της θύρας από την οποία έφτασε στο switch. Τέτοιου είδους πλαίσια είναι τα broadcast frames, τα multicast frames και τα unknown unicast frames.[3]

Τα πλαίσια μετάδοσης (broadcast frames) και τα πολλαπλής διανομής πλαίσια (multicast frames) έχουν ένα κοινό χαρακτηριστικό. Κανένα από τα δύο είδη δεν έχει κάποιο συγκεκριμένη διεύθυνση υλικού προορισμού. Η διεύθυνση του αποστολέα είναι επίσης η διεύθυνση υλικού της συσκευής που στέλνει το πλαίσιο. Στη περίπτωση των broadcast frames, η διεύθυνση προορισμού που εμφανίζεται στην κεφαλίδα ενός πακέτου είναι όλα της μορφής 1, που υποδεικνύει πως η μετάδοση πηγαίνει σε όλους τους κόμβους του δικτύου. Στη περίπτωση ενός multicast frame, το πλαίσιο καθορίζει ένα δίκτυο, αλλάζοντας όλα τα bits διεύθυνσης του δέκτη σε 1. Για παράδειγμα, ένα broadcast frame και ένα multicast frame σε δυαδική μορφή φαίνονται στο παρακάτω πίνακα .[3]

***Πίνακας 2.1:*** *Παράδειγμα Broadcast and Multicast destination addresses.*[3]

| Frame Type | Binary Value | Broadcast Address |
|---|---|---|
| Broadcast | 11111111.11111111.11111111.11111111 | 255.255.255.255 |
| Multicast | 00001010.00000001.11111111.11111111 | 10.1.255.255 |

Ένα άγνωστο μοναδικής διανομής πλαίσιο (unknown unicast) είναι παρόμοιο με ένα broadcast frame. Αυτό του είδους πλαισίου αποστέλλεται όταν η διεύθυνση προορισμού είναι άγνωστη από το switch. Σε αυτή τη περίπτωση, το switch προωθεί το πλαίσιο ακολουθώντας την ίδια διαδικασία με το broadcast frame. Το πλαίσιο αποστέλλεται σε όλες τις θύρες εκτός της θύρας που έλαβε το πλαίσιο.[3]

Όταν ένα switch λαμβάνει ένα από αυτά τα πλαίσια με άγνωστες διευθύνσεις προορισμού τότε τα αποστέλλει προς όλες τις θύρες εκτός της θύρας που έλαβε το πλαίσιο. Η διαδικασία αυτή είναι γνωστή με τον όρο πλημμύρα.[1]

Ωστόσο συμβαίνει μόνο σε όλες τις θύρες ενός switch που δεν είναι συνδεδεμένα με εικονικά δίκτυα (Virtual LANs) και σε επιλεγμένες θύρες του switch που είναι συνδεδεμένες με τέτοιου είδους δίκτυα.[1]

Επιπλέον για τα vlans, έχουν αναπτυχθεί τεχνικές που ελέγχουν τις υπερβολικές μεταδόσεις. Τέτοιες τεχνικές είναι το spoofing. Με αυτή τη τεχνική κάποια switches που δεν παίρνουν πλήρης λειτουργικότητα δρομολόγησης, παρεμβαίνουν σε κάποια πρωτόκολλα όπως NetWare's SAP and RIP. Η τεχνική αυτή είναι ιδιαίτερα πολύτιμη για τις γραμμές χαμηλής ταχύτητας, που μπορούν εύκολα να υπερφορτωθούν από διαφημιστικές διανομές, ενημερώσεις διαδρομών του δικτύου ή από την διαθεσιμότητα του διακομιστή.[1]

Κάποια switches επιτρέπουν στο διαχειριστή του δικτύου να επιλέξει ένα μέγιστο επίπεδο διανομής και να απορρίψει τις διανομές που υπερβαίνουν το όριο αυτό. Αν το επίπεδο επιλεχτεί προσεχτικά, το επίπεδο αυτό δεν θα ξεπερνιέται ποτέ παρά μόνο σε περίπτωση που συμβεί broadcast storm.[1]

## 2.2 ΔΙΑΦΟΡΕΣ ΜΕΤΑΞΥ BRIDGES ΚΑΙ SWITCHES

Όπως έχουμε αναφέρει τα switches είναι συσκευές παρόμοιες με τις γέφυρες παρόλο που έχουν κάποιες σημαντικές λεπτές τεχνολογικές διαφορές μεταξύ τους.[4][6]

Πρώτον, οι γέφυρες ήταν σχεδιασμένες να λειτουργούν με βάση το λογισμικό ώστε να σχεδιάζουν και να διατηρούν το δικό τους πίνακα φυσικών διευθύνσεων ενώ τα switches σχεδιάστηκαν να λειτουργούν βάση του υλικού αφού χρησιμοποιούν συγκεκριμένη εφαρμογή ολοκληρωμένων κυκλωμάτων για να χτίσουν και να διατηρήσουν τον πίνακα φυσικών διευθύνσεων τους.[4][5] Διαφορετικά οι γέφυρες και τα switch είναι ταυτόσημα στη λειτουργία τους.[6] Ένα switch επίσης μπορεί να θεωρηθεί ως μια γέφυρα με πολλαπλές θύρες και μπορεί να έχει πολλές περιπτώσεις του Spanning Tree Protocol, ενώ η γέφυρα μπορεί να έχει μόνο μία.[4]

Παρ' όλα αυτά, και τα switches και οι γέφυρες προωθούν πλαίσια του επιπέδου 2, μαθαίνουν τις φυσικές διευθύνσεις εξετάζοντας τη διεύθυνση της πηγής του κάθε πλαισίου που καταφθάνουν σε αυτά και τέλος παίρνουν αποφάσεις προώθησης των πλαισίων με βάση τη διευθυνσιοδότηση του επιπέδου 2.[4]

## 2.3 ΛΕΙΤΟΥΡΓΙΕΣ ΤΩΝ LAYER 2 SWITCHES

Τα switches για να μπορούν να προωθούν τα πλαίσια από τη μία θύρα στην άλλη, αλλά και σε άλλες συσκευές, εκτελούν τρεις διαφορετικές λειτουργίες του επιπέδου 2 που είναι αρκετά σημαντικές: τη λειτουργία Address Learning, Forward/Filter Decisions, και τη λειτουργία Loop Avoidance.[7]

Ας δούμε συνοπτικά τις λειτουργίες αυτές μία προς μία.

- Address Learning (εκμάθηση διευθύνσεων): Τα switches επιπέδου 2 αποθηκεύουν και διατηρούν τις φυσικές διευθύνσεις (Media Access Control Addresses)[11] των υλικών πηγών του κάθε πλαισίου που λαμβάνονται σε μια διασύνδεση και εισάγουν τις πληροφορίες αυτές σε μια βάση δεδομένων φυσικών διευθύνσεων που λέγεται πίνακας forward/filter.[6]
- Forward/Filter Decisions (αποφάσεις προώθηση/φιλτραρίσματος): Όταν ένα πλαίσιο λαμβάνεται σε μία διασύνδεση, το switch κοιτάζει τη διεύθυνση υλικού προορισμού και έπειτα διαλέγει από το πίνακα forward/filter τη κατάλληλη διεπαφή εξόδου για να αποστείλει το πλαίσιο. Με αυτό τον τρόπο, το πλαίσιο προωθείται μόνο από τη σωστή θύρα προορισμού.[8]
- Loop Avoidance (αποφυγή βρόχου): Αν δημιουργήσουμε πολλαπλές συνδέσεις μεταξύ των switches σε ένα δίκτυο για λόγους εφεδρείας τότε υπάρχει το ενδεχόμενα να προκληθούν δικτυακοί βρόχοι. Το Spanning Tree Protocol χρησιμοποιείται για να εμποδίσει τη δημιουργία βρόχων στο δίκτυο επιτρέποντας την ύπαρξη εφεδρικών διαδρομών μεταξύ των switches.[7]

### 2.3.1 ADDRESS LEARNING

Ένα Ethernet switch ελέγχει τη μεταφορά των πλαισίων μεταξύ των θυρών του, που συνδέονται με τα καλώδια Ethernet χρησιμοποιώντας του κανόνες μετάδοσης της κίνησης που περιγράφονται στο πρότυπο 802.1D. Η μετάδοση της κίνησης βασίζεται στην εκμάθηση των φυσικών διευθύνσεων. Τα switches αποφασίζουν τη προώθηση κίνησης βάση των 48-bit φυσικών διευθύνσεων που χρησιμοποιούνται στις προδιαγραφές ενός Ethernet LAN.[2]

Ένα switch που βρίσκεται σε ένα δίκτυο, έρχεται πρώτη φορά σε λειτουργία, ο πίνακας MAC forward/filter είναι κενός.

Όταν μια συσκευή του δικτύου μεταδίδει πλαίσια και μια διεπαφή τα λάβει, το switch τότε τοποθετεί τη διεύθυνση υλικού πηγής που έστειλε το πλαίσιο, στο πίνακα MAC forward/filter[7], που του επιτρέπει να θυμάται που βρίσκεται η διεπαφή της συσκευής που έστειλε το πλαίσιο.[8] Το switch αναγκάζεται να πλημμυρίσει το δίκτυο, στέλνοντας το πλαίσιο από όλες τις θύρες εκτός από τη θύρα που παρέλαβε το συγκεκριμένο πλαίσιο διότι δεν γνωρίζει τη διεύθυνση προορισμού του πλαισίου.[6]

Αν μια συσκευή απαντήσει σε αυτό το πλαίσιο στέλνοντας ένα άλλο πλαίσιο ως απάντηση, το switch τότε θα πάρει τη φυσική διεύθυνση του αποστολέα και θα τη βάλει στο πίνακα του, συσχετίζοντας τη διεύθυνση αυτή με την διεπαφή που δέχτηκε το πλαίσιο. Έχοντας πλέον το switch και τις δύο σχετικές διευθύνσεις στη βάση δεδομένων του, οι δύο αυτές συσκευές μπορούν να συνδεθούν από σημείο-σε σημείο. Το switch δεν θα χρειαστεί να ξαναπλημμυρίσει το δίκτυο με το πλαίσιο όπως τη πρώτη φορά διότι τα πλαίσια πλέον μπορούν και προωθούνται μόνο μεταξύ αυτών των δύο συσκευών μέσω του switch.[8]

Αν κάποια συσκευή δεν επικοινωνήσει για ένα χρονικό διάστημα με το switch, τότε το switch διαγράφει τις εγγραφές της συγκεκριμένης συσκευής από τη βάση δεδομένων του για να τη διατηρήσει όσο πιο ενημερωμένη μπορεί.[6]

Για το λόγο αυτό, τα επιπέδου 2 switches είναι πολύ ανώτερα των hubs. Σε δίκτυα που είναι συνδεδεμένα μέσω hubs, όλα τα πλαίσια προωθούνται από όλες τις θύρες τους κάθε φόρα, ότι και αν συμβεί.[7]

## 2.3.2 FORWARD/FILTER DECISIONS

Αφού τελικά το switch έχει γεμίσει το πίνακα με τις φυσικές διευθύνσεις, έχει όλες τις απαραίτητες πληροφορίες που χρειάζεται για να ξεκινήσει το φιλτράρισμα και τη προώθηση των πλαισίων επιλεκτικά στο δίκτυο. Καθώς το switch μαθαίνει τις φυσικές διευθύνσεις, ταυτόχρονα ελέγχει κάθε πλαίσιο για να πάρει μια απόφαση προώθησης πακέτου βάση της διεύθυνσης προορισμού που έχει το πλαίσιο.[2]

Επίσης, κάθε θύρα του switch μπορεί να κρατάει πλαίσια στην μνήμη της πριν τα μεταδόσει από το καλώδιο Ethernet που είναι συνδεδεμένο σε αυτή. Για παράδειγμα, αν μια θύρα είναι ήδη απασχολημένη προωθώντας κάποιο πλαίσιο, και φτάσει ένα δεύτερο πλαίσιο για μετάδοση, τότε το πλαίσιο κρατείται για ένα μικρό χρονικό διάστημα, ώστε να ολοκληρώσει τη μετάδοση του προηγούμενου πλαισίου. Για να μεταδώσει το πλαίσιο, το switch τοποθετεί το πλαίσιο στην ουρά μεταγωγής πακέτου.[2]

Όταν ένα πλαίσιο φτάσει σε μια διεπαφή του switch, το switch ελέγχει αν η διεύθυνση προορισμού του υλικού βρίσκεται στο πίνακα forward/filter MAC database. Αν είναι γνωστή και βρίσκεται στον πίνακα η διεύθυνση, τότε το πλαίσιο αποστέλλεται μόνο από την κατάλληλη εγγεγραμμένη διεπαφή εξόδου.[6] Κατά τη διάρκεια της διαδικασίας αυτής, το switch που μεταδίδει το πλαίσιο από τη μια θύρα στην άλλη, δεν πραγματοποιεί καμία αλλαγή σε κανένα πεδίο του πλαισίου.[2] Το switch δεν θα μεταδόσει το πλαίσιο από οποιαδήποτε διεπαφή, εξαιρώντας την διεπαφή προορισμού.[6] Να σημειωθεί πως ένα switch δεν θα προωθήσει κάποιο πλαίσιο που έχει προορισμό έναν σταθμό και βρίσκεται στη βάση δεδομένων προώθησης της θύρας εκτός αν η θύρα είναι συνδεδεμένη με το προορισμό στόχο. Δηλαδή η κίνηση που προορίζεται για μια συσκευή σε μια συγκεκριμένη θύρα, θα σταλεί μόνο σε εκείνη τη θύρα, και καμία άλλη θύρα δεν θα δει τη κίνηση που προορίζεται για την εν λόγω συσκευή. Αυτή η λογική μεταγωγής κρατάει τη κίνηση απομονωμένη μόνο για τα καλώδια Ethernet ή τα τμήματα που απαιτούνται για να λάβουν το πλαίσιο από τον αποστολέα και να μεταδώσουν το πλαίσιο στη συσκευή προορισμού.[2]

Αυτό εμποδίζει τη ροή μη απαραίτητης κίνησης σε άλλα τμήματα του δικτύου, το οποίο είναι τεράστιο πλεονέκτημα για ένα switch. Αυτό έρχεται σε αντίθεση με τα πρώτα συστήματα Ethernet, όπου η κίνηση από οποιονδήποτε σταθμό γινόταν γνωστή σε όλους τους σταθμούς του δικτύου, είτε χρειαζόταν τις πληροφορίες είτε

όχι. Το φιλτράρισμα της κίνησης των switches μειώνει το κυκλοφοριακό φόρτο που μεταφέρεται από το σύνολο των καλωδίων Ethernet που είναι συνδεδεμένα στο switch, καθιστώντας έτσι πιο αποτελεσματική χρήση του εύρους ζώνης του δικτύου.[2] Αυτή η διαδικασία ονομάζεται φιλτράρισμα πλαισίου (frame filtering).[6]

Αν όμως η διεύθυνση προορισμού του υλικού δεν είναι γνωστή και δεν είναι εγγεγραμμένη στο πίνακα forward/filter MAC database τότε το πλαίσιο αποστέλλεται από όλες τις ενεργές διεπαφές εκτός της διεπαφής που έφτασε το πλαίσιο. Έπειτα αν κάποια άλλη συσκευή απαντήσει σε αυτό το διαμοιραζόμενο πλαίσιο, τότε το switch θα ενημερώσει τη βάση δεδομένων του με τη διεύθυνση της συσκευής ώστε να έχει τη σωστή διασύνδεση.[8]

### 2.3.3 LOOP AVOIDANCE

Οι εφεδρικές συνδέσεις μεταξύ των switches είναι μια πολύ καλή ιδέα διότι βοηθούν στην αποτροπή πλήρης αποτυχιών του δικτύου σε περίπτωση που μια ενεργή σύνδεση σταματήσει να λειτουργεί.[8]

Παρ' όλο όμως που οι συνδέσεις αυτές μπορεί να είναι υπερβολικά χρήσιμες, μπορούν να δημιουργήσουν περισσότερα προβλήματα από όσα μπορούν να λύσουν. Κάποια από αυτά τα προβλήματα αναλύονται στη συνέχεια.[6]

Σε ένα δίκτυο μπορεί να προκύψει μεγάλη συσσώρευση από την κίνηση πλαισίων broadcast και multicast που προωθούν τα switches ασταμάτητα.[6][12] Αυτό συμβαίνει όταν διαφορετικοί κόμβοι στέλνουν δεδομένα πάνω σε μία σύνδεση, και οι άλλες συσκευές που δέχονται τα δεδομένα αυτά, τα αναμεταδίδουν πίσω στο σύνδεσμο του δικτύου ως απάντηση, προκαλώντας έτσι το συνολικό δίκτυο να υπερφορτωθεί από τη μεγάλη κίνηση δεδομένων και να οδηγήσει στην αποτυχία της επικοινωνίας του δικτύου.[13] Αυτή η διαδικασία ονομάζεται broadcast storm ή network storm και μπορεί να οφείλεται είτε στη κακιά τεχνολογία που αποτελεί το δίκτυο, είτε σε switches που έχουν χαμηλής ταχύτητας θύρες είτε σε ακατάλληλες διαμορφώσεις του δικτύου.[13]

Επιπλέον, μια συσκευή μπορεί να δεχτεί πολλαπλά αντίγραφα ενός ίδιου πλαισίου διότι μπορεί να έχει φτάσει στη συσκευή από διάφορα τμήματα του δικτύου ταυτόχρονα επιβαρύνοντας έτσι το δίκτυο. Αυτό οδηγεί σε ένα άλλου είδους πρόβλημα.[8]

Ο πίνακας των φυσικών διευθύνσεων ενός switch θα μπορούσε να μπερδευτεί σχετικά με τη τοποθεσία της συσκευής που στέλνει ένα πλαίσιο, αφού το switch δέχεται το ίδιο πλαίσιο από διαφορετικές διεπαφές. Ακόμη χειρότερα το μπερδεμένο switch θα είναι συνεχώς απασχολημένο προσπαθώντας να ενημερώνει το πίνακα διευθύνσεων, με τη διεύθυνση πηγής που θα αποτυχαίνει να προωθεί το πλαίσιο. Αυτό ονομάζεται thrashing MAC table.[6]

Τέλος, ένα από τα χειρότερα γεγονότα που μπορούν να συμβούν είναι όταν πολλαπλοί βρόχοι αναπαράγονται μέσω του δικτύου. Βρόχοι μπορούν να δημιουργηθούν μέσα σε άλλους βρόχους, και αν είναι να συμβεί ταυτόχρονα και broadcast storm το δίκτυο δεν θα είναι σε θέση να εκτελέσει τη μεταγωγή πλαισίων.[8]

Αυτά τα προβλήματα λοιπόν, αποτελούν καταστροφή για ένα δίκτυο και είναι καταστάσεις που επιβάλλεται να αποφεύγονται ή να διορθώνονται με κάποιο τρόπο. Ένας τέτοιος τρόπος είναι η χρήση του πρωτοκόλλου Spanning Tree για το οποίο θα μιλήσουμε και θα αναλύσουμε περαιτέρω στο επόμενο κεφάλαιο.[8]

## 2.4 CSMA/CD ΠΡΩΤΟΚΟΛΛΟ

Τα Ethernet δίκτυα χρησιμοποιούν το πρωτόκολλο Carrier Sense Multiple Access with Collision Detection (CSMA/CD), το οποίο βοηθάει τις συσκευές να μοιράζονται το εύρος ζώνης ισοδύναμα ενώ παράλληλα αποτρέπουν δύο συσκευές από το να μεταδίδουν ταυτόχρονα στο ίδιο μέσο του δικτύου. Στην ουσία το CSMA/CD δημιουργήθηκε για να αντιμετωπιστεί το πρόβλημα των συγκρούσεων όταν οι κόμβοι μεταδίδουν ταυτόχρονα πακέτα την ίδια στιγμή. Η διαχείριση των συγκρούσεων είναι πολύ κρίσιμη για τη σωστή λειτουργία ενός δικτύου. Όταν ένας κόμβος μεταδίδει πακέτα σε δίκτυο που χρησιμοποιεί το πρωτόκολλο CSMA/CD, όλοι οι υπόλοιποι κόμβοι του δικτύου λαμβάνουν και εξετάζουν τη μετάδοση. Μόνο τα switches και τα routers μπορούν να αποτρέψουν αποτελεσματικά μια μετάδοση από το να πολλαπλασιαστεί σε όλο το δίκτυο.[7][5]

Όταν ένας χρήστης θέλει να μεταδώσει πληροφορίες στο δίκτυο, πρώτα ελέγχει στο μέσο διάδοσης για τη παρουσία ψηφιακού σήματος. Αν δεν υπάρχει κάποιο σήμα και κανένας άλλος χρήστης δεν μεταδίδει πληροφορίες, τότε ο αρχικός χρήστης μπορεί να συνεχίσει τη μετάδοση. Ωστόσο, ο χρήστης που μεταδίδει

πληροφορίες παρακολουθεί συνέχεια το καλώδιο για να είναι σίγουρος πως κανένας άλλος χρήστης δεν έχει αρχίσει να μεταδίδει πληροφορίες παράλληλα.[7]

Αν ο χρήστης εντοπίσει κάποιο άλλο σήμα στο καλώδιο στέλνει ένα διαδοχικό σήμα κίνησης ώστε να προκαλέσει όλους τους χρήστες του δικτύου να σταματήσουν τη παράλληλη μετάδοση πληροφοριών. Οι κόμβοι τότε θα ανταποκριθούν σε αυτό το σήμα κίνησης αναμένοντας για ένα μικρό χρονικό διάστημα πριν ξεκινήσουν την μετάδοση πάλι. Η διαδικασία αυτή είναι γνωστή και ως backoff algorithm. Ο αλγόριθμος αυτός καθορίζει πότε οι σταθμοί που αντιμετωπίζουν συγκρούσεις επιτρέπεται να ξεκινήσουν τη μετάδοση.[7] Ο χρήστης θα πρέπει να εντοπίζει τη σύγκρουση πριν τελειώσει τη μετάδοση ενώ πλαισίου διαφορετικά το πρωτόκολλο δεν μπορεί να λειτουργήσει αξιόπιστα. Αυτό επιτυγχάνεται χρησιμοποιώντας ένα σταθερό χρονικό περιθώριο (slot time), τον απαιτούμενο χρόνο δηλαδή που χρειάζεται για να σταλεί από τον χρήστη σε κάποιον προορισμό και πίσω, και μετριέται σε bits. Ο χρήστης επιπλέον θα πρέπει να συνεχίσει τη μετάδοση ενός πλαισίου για τον ελάχιστο χρόνο του χρονικού περιθωρίου. Σε ένα κατάλληλα διαμορφωμένο δίκτυο, μια σύγκρουση θα πρέπει πάντα να συμβαίνει μέσα σε αυτό το χρονικό περιθώριο καθώς έχει περάσει αρκετή ώρα για να φτάσει το πλαίσιο ως την άλλη άκρη του δικτύου και προς τα πίσω, γνωρίζοντας οι υπόλοιπες συσκευές του δικτύου τη συγκεκριμένη μετάδοση. Το χρονικό αυτό περιθώριο περιορίζει σημαντικά το φυσικό μέγεθος του δικτύου αφού αν ένα τμήμα του δικτύου είναι πολύ μεγάλο, κάποιος χρήστης πιθανόν να μην μπορέσει να ανιχνεύσει τη σύγκρουση μέσα στο χρονικό περιθώριο. Η σύγκρουση που συμβαίνει μετά πέρας του χρονικού περιθωρίου αναφέρεται ως καθυστερημένη σύγκρουση (late collision).[5]

Αν οι συγκρούσεις εξακολουθούν να συμβαίνουν μετά από δεκαπέντε προσπάθειες μεταξύ αυτών των κόμβων τότε θα σταματήσουν εντελώς τη μετάδοση.[7]

Όταν συμβεί κάποια σύγκρουση σε ένα δίκτυο Ethernet αρχικά ένα σήμα κίνησης στέλνεται και ενημερώνει όλες τις συσκευές πως έχει συμβεί σύγκρουση. Στη συνέχεια η σύγκρουση εφαρμόζει τυχαία τον αλγόριθμο backoff και κάθε συσκευή στο δίκτυο σταματάει τη μετάδοση για ένα σύντομο χρονικό διάστημα εώς ότου ο αλγόριθμος backoff τελειώσει. Όλοι οι χρήστες έχουν την ίδια προτεραιότητα να μεταδώσουν αφού τελειώσουν τα χρονικά όρια του αλγόριθμου backoff.[7][5]

Γι' αυτό το λόγο τα δίκτυα που χρησιμοποιούν το πρωτόκολλο CSMA/CD έχουν καθυστερήσεις, χαμηλό ρυθμό μετάδοσης και μεγάλη κυκλοφοριακή συμφόρηση.[7]

## 2.5 HALF-DUPLEX ΚΑΙ FULL-DUPLEX ΕΠΙΚΟΙΝΩΝΙΑ

Η τεχνολογία Ethernet αναπτύχθηκε για να μπορεί να υποστηρίζει περιβάλλοντα που χρησιμοποιούν κοινόχρηστα μέσα. Έτσι επιτρέπεται στους χρήστες να χρησιμοποιούν το ίδιο φυσικό μέσο του δικτύου. Υπάρχουν δύο μέθοδοι επικοινωνίας σε ένα κοινόχρηστο φυσικό μέσο. Η ημι-αμφίδρομη επικοινωνία (Half-Duplex Communication) που επιτρέπει στους χρήστες να μεταδίδουν ή να λαμβάνουν πληροφορίες, αλλά όχι ταυτόχρονα και η πλήρης αμφίδρομη επικοινωνία (Full-Duplex Communication) επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν πληροφορίες ταυτόχρονα.[5]

Η επικοινωνία με τη μέθοδο Half-Duplex ορίζεται στις αρχικές προδιαγραφές του Ethernet στο πρότυπο IEEE 802.3. Το πρωτόκολλο CSMA/CD χρησιμοποιεί τη μέθοδο half-duplex για να μπορεί να αποτρέπει τις συγκρούσεις και να επιτρέπει την επαναμετάδοση αν συμβεί κάποια σύγκρουση. Αν είναι συνδεμένο ένα hub με ένα switch, πρέπει να λειτουργήσει με τη ημι-αμφίδρομη μέθοδο διότι οι τερματικοί σταθμοί θα πρέπει να μπορούν να εντοπίζουν την ύπαρξη των συγκρούσεων. Το πρόβλημα είναι ότι μόνο η ημι-αμφίδρομη μέθοδος μπορεί να λειτουργήσει και αν δυο χρήστες προσπαθήσουν να επικοινωνήσουν ταυτόχρονα θα προκύψει σύγκρουση.[7]

Αντιθέτως η μέθοδος της πλήρης αμφίδρομης επικοινωνίας χρησιμοποιεί δύο ζευγάρια καλωδίων την ίδια στιγμή και χρησιμοποιεί συνδέσεις από σημείο σε σημείο μεταξύ της συσκευής που μεταδίδει και της συσκευής που λαμβάνει τα δεδομένα.[7] Η μέθοδος πλήρης αμφίδρομης επικοινωνίας καθορίζεται στο πρότυπο 802.3x και δεν χρησιμοποιεί το πρωτόκολλο CSMA/CD ούτε slot times.[5] Ως εκ τούτου έχουμε ταχύτερη μετάδοση, καλύτερη αποτελεσματικότητα και υποστήριξη μεγαλύτερων αποστάσεων σε σχέση με την ημι-αμφίδρομη μεταφορά.[5][7] Επίσης, υποστηρίζει ταυτόχρονη επικοινωνία παρέχοντας ξεχωριστές διαδρομές για τις μεταδιδόμενες και τις λαμβανόμενες πληροφορίες, με αποτέλεσμα την εξάλειψη των συγκρούσεων.[5]

Πλήρη αμφίδρομη επικοινωνία μπορούμε να έχουμε σε έξι διαφορετικές περιπτώσεις:

1. Σε απευθείας συνδέσεις μεταξύ χρήστη και switch.
2. Σε απευθείας συνδέσεις μεταξύ δύο switches.
3. Σε απευθείας συνδέσεις μεταξύ δύο χρηστών.
4. Σε απευθείας συνδέσεις μεταξύ switch και router.
5. Σε απευθείας συνδέσεις μεταξύ δύο router.
6. Σε απευθείας συνδέσεις μεταξύ router και χρήστη.[7]

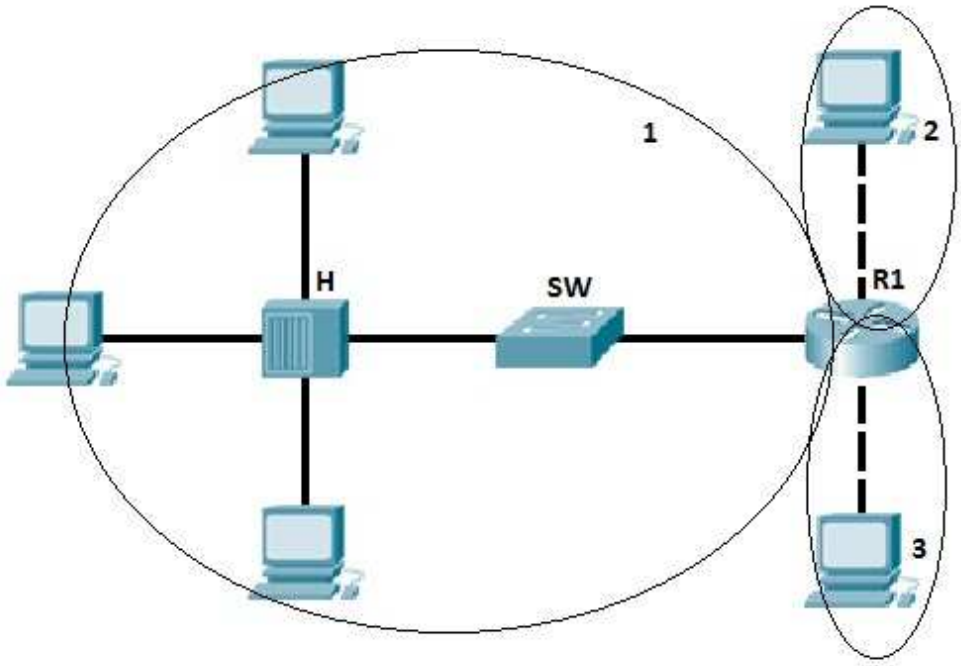
# 2.6 ΜΕΘΟΔΟΙ ΠΡΟΩΘΗΣΗΣ ΠΛΑΙΣΙΟΥ

Τα switches υποστηρίζουν τρεις διαφορετικές μεθόδους για να προωθούν τα πλαίσια. Κάθε μία μέθοδος από αυτές αντιγράφει ολόκληρο ή μέρος του πλαισίου στη μνήμη του, παρέχοντας έτσι διαφορετικά επίπεδα καθυστέρησης και αξιοπιστίας. Μικρότερη καθυστέρηση σημαίνει ταχύτερη προώθηση του πλαισίου.[5]

1. Η μέθοδος Store and Forward αντιγράφει ολόκληρο το πλαίσιο στη μνήμη του και εκτελεί τον έλεγχο Cycle Redundancy Check (CRC) για να εξασφαλίσει απόλυτα την ακεραιότητα του πλαισίου. Ωστόσο, αυτό επίπεδο ελέγχου, για τυχόν σφάλματα στο πλαίσιο, προκαλεί τη μεγαλύτερη καθυστέρηση από τις υπόλοιπες μεθόδους.[5]
2. Η μέθοδος Cut Through (Real Time) αντιγράφει ένα μέρος της κεφαλίδας του πλαισίου για να καθορίσει τη διεύθυνση προορισμού. Αυτό το κομμάτι είναι τα πρώτα 6 bytes μετά την εισαγωγή. Η μέθοδος αυτή επιτρέπει τα πλαίσια να μεταφέρονται με τη ταχύτητα του καλωδίου και έχει το μικρότερο επίπεδο καθυστέρησης και από τις τρεις μεθόδους. Επιπλέον δεν συμβαίνει έλεγχος για σφάλματα στο πλαίσιο με αυτή τη μέθοδο.[5]
3. Η μέθοδος Fragment Free (Modified Cut Through) αντιγράφει μόνο τα 64 πρώτα bytes του πλαισίου για έλεγχο σφαλμάτων. Οι περισσότερες συγκρούσεις και αλλοιώσεις συμβαίνουν σε αυτό το τμήμα του πλαισίου. Η μέθοδος αυτή είναι συνδυασμός των μεθόδων CRC και Cut Through για την καλύτερη αξιοπιστία και ταχύτητα.[5]

# 2.7 BROADCAST AND COLLISION DOMAINS

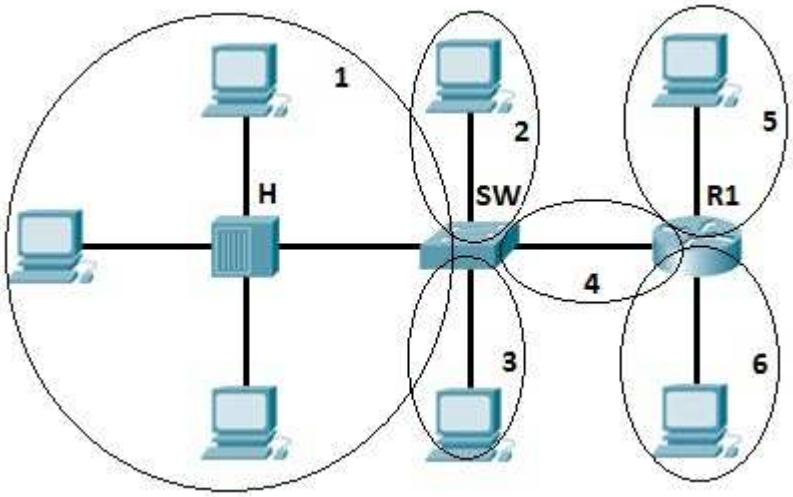
Τομέας εκπομπής (broadcast domain) είναι το τμήμα στο οποίο προωθείται μία εκπομπή. Ένας τέτοιος τομέας περιέχει όλες τις συσκευές οι οποίες μπορούν να επικοινωνήσουν μεταξύ τους με βάση το data link layer χρησιμοποιώντας τη εκπομπή. Όλες οι θύρες ενός hub ή ενός switch ανήκουν στον ίδιο τομέα μετάδοσης εξ' ορισμού. Οι θύρες ενός router ανήκουν σε διαφορετικό τομέα μετάδοσης και τα router δεν προωθούν τις εκπομπές από το ένα τμήμα εκπομπής στο άλλο.[14] Στην εικόνα που ακολουθεί μπορούμε να δούμε πως ακριβώς σχηματίζονται οι τομείς εκπομπής.




***Εικόνα 2.2 :*** *Broadcast Domain.[14]*

Τομέας σύγκρουσης (collision domain) είναι το τμήμα στο οποίο μπορούν να συμβούν συγκρούσεις πακέτων/πλαισίων. Οι συγκρούσεις συμβαίνουν όταν δύο συσκευές στέλνουν πακέτα την ίδια στιγμή στο κοινόχρηστό τμήμα του δικτύου. Τα πακέτα συγκρούονται μεταξύ τους και οι συσκευές πρέπει εκ νέου να τα ξαναστείλουν, πράγμα που μειώνει την απόδοση της λειτουργίας του δικτύου. Συγκρούσεις έχουμε συχνά σε περιβάλλοντα που υπάρχουν συνδέσεις μέσω hubs, διότι κάθε θύρα του hub βρίσκεται στο ίδιο τομέα σύγκρουσης. Αντιθέτως, κάθε θύρα ενός switch ή ενός router αποτελεί ξεχωριστό τομέα σύγκρουσης.[14]

Στην εικόνα που ακολουθεί μπορούμε να δούμε πως ακριβώς σχηματίζονται οι τομείς σύγκρουσης.




***Εικόνα 2.3:*** *Collision Domain.*[14]

# 2.8 ΕΙΚΟΝΙΚΑ ΔΙΚΤΥΑ-VLANs

Ένα τοπικό δίκτυο που αποτελείται μόνο από switches επιπέδου 2 αναφέρεται και ως flat network topology. Ένα τέτοιο δίκτυο αποτελεί ένα ενιαίο τομέα μετάδοσης, έτσι ώστε κάθε συνδεδεμένη συσκευή να παρακολουθεί την οποιαδήποτε αποστολή πακέτου που μεταδίδεται.[4]

Εξ' αιτίας της φύσης του επιπέδου 2, τα flat networks δεν μπορούν να έχουν επιπλέον διαδρομές για να εξισορροπήσουν το φορτίο ή να έχουν ανοχή σε σφάλματα. Για να συμβεί κάτι τέτοιο θα πρέπει να εισάγουμε στο δίκτυο λειτουργίες δρομολόγησης του επιπέδου 3. Η τεχνολογία των switches μας δίνει τη δυνατότητα να ξεπεράσουμε αυτό το πρόβλημα των περιορισμών των flat networks. Τα δίκτυα μεταγωγής μπορούν να υποδιαιρεθούν σε vlans.[4]

Ένα εικονικό τοπικό δίκτυο (Virtual Local Area Network-VLAN) είναι μια ομάδα που αποτελείται από σταθμούς εργασίας, διακομιστές και δικτυακές συσκευές και φαίνονται αν ανήκουν στο ίδιο τοπικό δίκτυο ανεξαρτήτως της γεωγραφική τους κατανομής. Ένα τέτοιο δίκτυο επιτρέπει σε ένα δίκτυο από υπολογιστές και χρήστες να επικοινωνούν σε ένα τεχνητό περιβάλλον σαν να συνυπάρχουν σε ένα τοπικό δίκτυο και μοιράζονται ένα ενιαίο τομέα σύγκρουσης και ένα ενιαίο τομέα μετάδοσης. Τα vlans εφαρμόζονται για να επιτύχουμε την επεκτασιμότητα του

τοπικού μας δικτύου, την ασφάλεια του και την εύκολη διαχείριση του δικτύου που μπορούν χωρίς πρόβλημα να προσαρμοστούν στις αλλαγές και στις απαιτήσεις του δικτύου γρήγορα, καθώς και στην μετεγκατάσταση των σταθμών εργασίας και των διακομιστών.[4][15]

Τα switches επιπέδου 2 που έχουν διαμορφωθεί με τη χαρτογράφηση των vlans και παρέχουν τη λογική σύνδεση μεταξύ των χρηστών ενός vlan, επιτρέπουν τη λειτουργία και την εφαρμογή των vlans.[4][15]

### 2.8.1 VLAN MEMBERSHIP

Όταν ένα VLAN παρέχεται σε switch που συνδέεται απευθείας με κάποιον χρήστη, ο χρήστης θα πρέπει να έχει κάποια μέσα για να μπορέσει να συμμετέχει στο VLAN. Τα switches της σειράς Catalyst της εταιρίας Cisco χρησιμοποιούν δύο μεθόδους συμμετοχής: static vlans και dynamic vlans.[4]

Το static VLAN προσφέρει τη συμμετοχή του χρήστη βάση της θύρας, όταν οι θύρες του switch έχουν ανατεθεί σε συγκεκριμένα vlans. Οι χρήστες γίνονται μέλη ενός vlan, βάση της θύρας του switch στην οποία είναι συνδεδεμένοι. Δεν απαιτείται κάποιο πρωτόκολλο συμμετοχής για τις συσκευές. Αυτόματα θεωρούν πως έχουν συνδεθεί σε κάποιο vlan όταν συνδέονται σε μια θύρα. Κανονικά οι συσκευές δεν γνωρίζουν καν την ύπαρξη των vlans. Η θύρα του switch και το vlan του φαίνεται και χρησιμοποιείται απλά όπως κάθε άλλο κομμάτι του δικτύου, μαζί με άλλους χρήστες που χρησιμοποιούν το ίδιο καλώδιο.[4] Οι θύρες των switches ανατίθενται σε vlans χειροκίνητα από τον διαχειριστή του δικτύου. Οι θύρες ενός switch μπορούν να ανατεθούν και να ομαδοποιηθούν σε πολλά vlans. Ακόμα και αν συνδέονται αρκετές συσκευές στο ίδιο switch, η κίνηση δεν θα περάσει από τις συσκευές αυτές αν είναι συνδεδεμένες σε θύρες που ανήκουν σε διαφορετικά vlans. Για να συμβεί αυτό, είτε μια συσκευή επιπέδου 3 θα μπορούσε να χρησιμοποιηθεί για τη δρομολόγηση πακέτων ή μια εξωτερική συσκευή επιπέδου 2 θα μπορούσε να χρησιμοποιηθεί μεταξύ δύο vlans για τη σύνδεση τους.[4] Η στατική θύρα συμμετοχής χρήστη σε vlan γίνεται βάση του υλικού, με εφαρμογή ειδικών ολοκληρωμένων κυκλωμάτων (Application Specific Integrated Circuits-ASICs) στο switch. Η χρήση αυτού του είδους συμμετοχής προσφέρει καλή απόδοση του vlan διότι η χαρτογράφηση όλων

των θυρών γίνεται σε επίπεδο υλικού χωρίς να απαιτούνται περίπλοκες αναζητήσεις σε κάποιο πίνακα.[4]

Τα dynamic vlans χρησιμοποιούνται για παροχή των χρηστών με βάση τη φυσική διεύθυνση της συσκευής του.[4] Όταν μια συσκευή συνδέεται με μια θύρα του switch, το switch πρέπει να κάνει αναζήτηση σε μια βάση δεδομένων για να εξακριβώσει τη συμμετοχή του χρήστη στο vlan.[4] Στα δυναμικά VLANs, αντίθετα με τα static vlans, δεν απαιτούν από το διαχειριστή να διαμορφώσει τις θύρες των switches, αλλά να διαμορφώσει ένα κεντρικό εξυπηρετητή που λέγεται Vlan Member Policy Server (VMPS).[16] Το VMPS χρησιμοποιείται για να χειριστεί τις παραμέτρους των θυρών των switches που συμμετέχουν σε vlan. Το VMPS περιέχει μια βάση δεδομένων από όλες τις φυσικές διευθύνσεις των υπολογιστών καθώς και σε ποιο vlan ανήκουν αυτές οι φυσικές διευθύνσεις.[16] Τις πληροφορίες αυτές πρέπει να τις εκχωρεί ο διαχειριστής κάθε φορά που συνδέεται μια καινούργια συσκευή.[4] Για το λόγο αυτό μπορούμε να υποθέσουμε πως έχουμε χαρτογράφηση του vlan μέσω των φυσικών διευθύνσεων των υπολογιστών (Vλαν-to-Mac Address).[16] Τα dynamic vlans αναπτύχθηκαν με στόχο να παρέχουν ευελιξία και περιπλοκότητα κάτι που τα static vlans δεν παρείχαν. Λόγω της περιπλοκότητας τους, των απαιτήσεων και την συνεχή επίβλεψη από το διαχειριστή του δικτύου, τα συναντάμε πολύ σπάνια και προτείνονται από τους διαχειριστές και τους τεχνικού δικτύων η χρήση των static vlans.[16]

### 2.8.2 VLAN TRUNKS

Όπως έχουμε ήδη αναφέρει οι συνδεδεμένες συσκευές των τελικών χρηστών ενός δικτύου δεν έχουν επίγνωση της ύπαρξης των vlans και της δομής τους, και φαίνονται πως είναι συνδεδεμένες σε ένα κανονικό τμήμα του δικτύου. Επίσης για να έχουμε επικοινωνία μεταξύ διαφορετικών vlans απαιτείται η χρήση ενός router ή μιας εξωτερικής γέφυρας.

Μία σύνδεση trunk ή μια θύρα του switch που είναι διαμορφωμένη ως trunk port, μπορεί να μεταφέρει πακέτα όχι από ένα, αλλά από όλα τα vlans που υπάρχουν στο δίκτυο χρησιμοποιώντας μία μόνο σύνδεση. Τέτοιες συνδέσεις είναι πιο ωφέλιμες μεταξύ switches ή σε συνδέσεις μεταξύ switches και routers. [4][17]

Καθώς ο αριθμός των vlans αυξάνεται σε ένα δίκτυο, αυξάνεται και ο αριθμός των συνδέσεων μεταξύ τους. Είναι εφικτό να συνδεθούν δύο switches μεταξύ τους με ξεχωριστές συνδέσεις για το κάθε vlan. Αλλά είναι πιο αποτελεσματική η χρήση των συνδέσεων trunking αφού μπορεί να αντικαταστήσει πολλές ατομικές συνδέσεις των vlans.[4]

### 2.8.3 VLAN FRAME TAGGING

Με τη χρήση των συνδέσεων trunk έχουμε μεταφορά δεδομένων από διάφορα VLANs τα οποία ένα switch θα πρέπει να λάβει και αναμεταδώσει γνωρίζοντας το προορισμό τους. Για να επιτευχθεί αυτό η διαδικασία frame identification ή tagging, εκχωρεί ένα μοναδικό αναγνωριστικό σε κάθε πλαίσιο που μεταφέρεται μέσω της σύνδεσης trunk. Αυτό το αναγνωριστικό μπορεί να είναι είτε κάποιος αριθμός ή κάποιο χρώμα, αν έχει σχεδιαστεί σε διάγραμμα του δικτύου με κάποιο συγκεκριμένο χρώμα.

Το vlan frame identification αναπτύχθηκε για τα δίκτυα μεταγωγής. Καθώς πλαίσια μεταφέρονται μέσω της trunk σύνδεσης, το αναγνωριστικό τοποθετείται στη κεφαλίδα του πλαισίου. Καθώς τα switches δέχονται και αναμεταδίδουν τα πλαίσια αυτά, το αναγνωριστικό τους εξετάζεται για να καθοριστεί σε ποιο vlan ανήκουν.

Αν τα πλαίσια πρέπει να μεταφέρονται μεταξύ συνδέσεων trunk το αναγνωριστικό vlan παραμένει στην επικεφαλίδα του πλαισίου. Διαφορετικά αν έχουν ως προορισμό κάποιον τελικό χρήστη τα switches αφαιρούν το αναγνωριστικό αυτό πριν μεταδοθεί το πλαίσιο στο χρήστη. Ως εκ τούτου, τα ίχνη των συνεταιρίζεσθαι vlans παραμένουν κρυφά στον τελικό χρήστη.

Η ταυτοποίηση του vlan αναγνωριστικού μπορεί να διεξαχθεί με διαφορετικές μεθόδους, που κάθε μια από αυτές χρησιμοποιεί διαφορετικό μηχανισμό αναγνωριστικού πλαισίου και μερικά είναι κατάλληλα για συγκεκριμένες δικτυακές συσκευές.

### 2.8.4 INTER-SWITCH LINK PROTOCOL

Το Inter-Switch Link Protocol (ISL) πρωτόκολλο έχει δημιουργηθεί από την εταιρία Cisco με σκοπό τη διατήρηση του vlan αναγνωριστικού του πλαισίου της

πηγής μέσω των συνδέσεων trunk. Το ISL εφαρμόζει την ταυτοποίηση πλαισίου στο επίπεδο 2 εμπεριέχοντας κάθε πλαίσιο μεταξύ της επικεφαλίδας και της ουράς. Οποιοδήποτε Cisco switch ή router που είναι διαμορφωμένο για το ISL μπορεί να διαχειριστεί και να καταλάβει τις πληροφορίες του ISL vlan.[4][19]

Όταν ένα πλαίσιο προορίζεται από μία trunk σύνδεση για κάποιο router ή switch, το ISL προσθέτει μια επικεφαλίδα μεγέθους 26-byte και μια ουρά μεγέθους 4-byte στο πλαίσιο. Η πηγή vlan αναγνωρίζεται από το αναγνωριστικό vlan (VLAN ID) που έχει μέγεθος 10-bit και βρίσκεται στην επικεφαλίδα. Η ουρά περιέχει έναν έλεγχο CRC για να εγγυηθεί την ακεραιότητα του νέου περιλαμβανομένου πλαισίου. Επειδή το ISL προσθέτει στην αρχή και στο τέλος του πλαισίου πληροφορίες, μερικές φορές αναφέρεται και ως double tagging.[4][19]

### 2.8.5 VLAN TRUNKING PROTOCOL

Η διαμόρφωση ενός μικρού vlan δικτύου και των συνδέσεων vlan trunk είναι εύκολο να διαχειριστεί. Αντιθέτως όμως, η διαχείριση των vlan και των vlan trunking ports σε τεράστια δίκτυα με interconnected switches είναι αρκετά δύσκολο.[18]

Η Cisco ανέπτυξε το πρωτόκολλο Vlan Trunking Protocol (VTP), το οποίο είναι αρκετά χρήσιμο στη δημιουργία, διαχείριση και τη συντήρηση ενός μεγάλου τοπικού δικτύου που περιέχει πολλά interconnected switches. Με το VTP επίσης μπορούμε να διαχειριστούμε την πρόσθεση, την αφαίρεση και την μετονομασία ενός vlan από ένα κεντρικό σημείο χωρίς καμία χειροκίνητη παρέμβαση. Έτσι, το VTP μειώνει τη διαχείριση του δικτύου σε ένα δίκτυο μεταγωγής.[18]

### 2.8.6 VTP DOMAIN

Το VTP είναι οργανωμένο σε τομείς διαχείρισης ή περιοχές με κοινές απαιτήσεις του vlan. Ένα switch μπορεί να ανήκει μόνο σε ένα τομέα VTP και μπορεί να διαμοιράζεται πληροφορίες με άλλα switches που ανήκουν στον ίδιο τομέα. Παρόμοια με τα vlans, τα switches που ανήκουν σε διαφορετικούς τομείς δεν μπορούν να μοιραστούν πληροφορίες του VTP.[4]

Τα switches σε ένα VTP τομέα, διαφημίζουν μερικά διαφορετικά χαρακτηριστικά σε γειτονικά switches που ανήκουν σε κοινό τομέα. Τέτοια διαφημιστικά περιέχουν πληροφορίες σχετικά με το VTP τομέα διαχείρισης, την ενημέρωση αριθμού του VTP, καθώς και γνωστά VLANs και συγκεκριμένες παραμέτρους του vlan. Όταν ένα vlan προστίθεται σε ένα switch μέσα σε ένα τομέα διαχείρισης, τα υπόλοιπα switches ενημερώνονται για το καινούργιο vlan μέσω των VTP διαφημίσεων. Με αυτό τον τρόπο, όλα τα switches στο τομέα μπορούν να λαμβάνουν κίνηση στις trunk θύρες τους χρησιμοποιώντας το νέο vlan.[4]

### 2.8.7 VTP MODES

Κάθε switch θα πρέπει να διαμορφωθεί και να λειτουργεί σε μία από τις τρεις καταστάσεις για να συμμετάσχει σε κάποιο VTP τομέα διαχείρισης. Η κατάσταση VTP θα καθορίσει πως το switch θα επεξεργάζεται και θα διαφημίζει τις πληροφορίες του VTP. Οι καταστάσεις στις οποίες μπορούν να διαμορφωθούν τα switches είναι οι ακόλουθες:[4]

- **Server Mode** (Κατάσταση Εξυπηρετητή): Σε αυτή τη κατάσταση οι VTP εξυπηρετητές έχουν τον πλήρη έλεγχο στη δημιουργία ενός vlan και την τροποποίηση του για τους τομείς τούς. Όλες οι VTP πληροφορίες διαφημίζονται σε άλλα switches στο τομέα, ενώ όλες οι λαμβανόμενες VTP πληροφορίες συγχρονίζονται μεταξύ των switches. Εξ' ορισμού ένα switch βρίσκεται σε κατάσταση εξυπηρετητή. Κάθε VTP τομέας πρέπει να έχει τουλάχιστον ένα switch σε κατάσταση εξυπηρετητή για να είναι εφικτή η δημιουργία και η τροποποίηση ενός vlan και να μπορούν οι πληροφορίες του vlan να διαφημίζονται.[4]
- **Client Mode** (Κατάσταση Πελάτη): Οι VTP πελάτες δεν επιτρέπουν στον διαχειριστή να δημιουργήσει ή να επεξεργαστεί ένα vlan. Αντιθέτως, ακούν τις VTP διαφημίσεις των άλλων switches και τροποποιούν τη διαμόρφωση του VLAN κατάλληλα. Στη πραγματικότητα είναι μία παθητική κατάσταση ακρόασης. Οι λαμβανόμενες VTP πληροφορίες προωθούνται από τις συνδέσεις trunk προς τα υπόλοιπα switches του τομέα.[4]

- **Transparent Mode** (Ανοιχτή Κατάσταση): Τα switches που βρίσκονται σε αυτή τη κατάσταση δεν συμμετέχουν σε κάποιο VTP. Επιπλέον, δεν διαφημίζουν τις δικές τους διαμορφώσεις των vlans και δεν συγχρονίζουν τις λαμβανόμενες διαφημίσεις με τη βάση δεδομένων των vlans στα οποία ανήκουν.[4]

# 2.9 LAYER 3 SWITCHING

Μέχρι στιγμής έχουμε αναφερθεί στα switches που λειτουργούν στο δεύτερο επίπεδο του μοντέλου αναφοράς OSI, το επίπεδο σύνδεσης δεδομένων. Ωστόσο, υπάρχουν switches που λειτουργούν με βάση το τρίτο επίπεδο, το επίπεδο δικτύου.

Στο επίπεδο αυτό, ως γνωστόν, λειτουργούν οι συσκευές router. Υπάρχουν όμως και τα επιπέδου 3 switches που έχουν όλες τις δυνατότητες των switches επιπέδου 2 και επιπλέον μπορούν να εκτελέσουν λειτουργίες ενός router και να μεταφέρουν δεδομένα μεταξύ των LANs και WANs με την ταχύτητα του καλωδίου.[20] Κάποιες από τις τεχνολογίες που εφαρμόζουν αυτού του τύπου τα switches συμπεριλαμβάνουν πρωτόκολλα δρομολόγησης πύλης δικτύου όπως το RIP (Routing Information Protocol) και το OSPF (Open Shortest Path First).[20][21] Τα επιπέδου 3 switches δρομολογούν τα δεδομένα μεταξύ των διαφορετικών τμημάτων του δικτύου περιορίζοντας τον αριθμό των πρωτοκόλλων δρομολόγησης, και χρησιμοποιούν περισσότερο την τεχνολογία των ASIC κυκλωμάτων παρά των RISC κυκλωμάτων ή το λογισμικό.[20]

## 2.9.1 ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ LAYER 3 SWITCHES

Τα επιπέδου 3 switches είναι κατασκευασμένα για τη μεταγωγή πλαισίων και πακέτων και αυτό τα κάνει να διαφέρουν από τα επιπέδου 2 switches. Τα επιπέδου 2 switches παρ' όλο που μπορούν να χωρίσουν σε τμήματα τους τομείς μετάδοσης, αλλά δεν μπορούν να δρομολογήσουν τα δεδομένα σε διαφορετικά δίκτυα. Όταν χρειάζεται να δρομολογηθεί ένα πακέτο δεδομένων τότε αξιοποιούνται τα πρωτοκόλλα δρομολόγησης του επιπέδου 3.[20]

Μία από τις μεθόδους δρομολόγησης που χρησιμοποιούν τα επιπέδου 3 switches όταν λαμβάνουν κάποιο πακέτο δεδομένων είναι πως στέλνουν το πρώτο πακέτο που λαμβάνουν σε κάποιο router ή σε route server ώστε να αποφασιστεί αν τα επόμενα πακέτα δεδομένων στη σειρά θα είναι καλύτερο να δρομολογηθούν ή να γίνει μεταγωγή αυτών. Αν αποφασιστεί να δρομολογηθούν τότε η μετάδοση των πακέτων γίνεται μέσω του δρομολογητή. Αν αποφασιστεί πως η μεταγωγή είναι ταχύτερη μέθοδος τότε τα πακέτα θα προωθηθούν δια μέσου του switch επιπέδου 3.[20]

Αυτό επιτυγχάνεται διαμέσου των ακολούθων βημάτων:

1. Τα πακέτα δεδομένων στέλνονται προς το switch, μέσω διάφορων μέσων, χρησιμοποιώντας τα πρωτοκόλλα του επιπέδου 1.
2. Το switch ελέγχει τη φυσική διεύθυνση επιπέδου 2 της συσκευής προορισμού για να δει αν η συσκευή είναι μέλος του τοπικού δικτύου.
3. Αν η συσκευή ανήκει στο τοπικό δίκτυο, τότε το switch προωθεί τα δεδομένα χρησιμοποιώντας τα πρωτοκόλλα του επιπέδου 2 και τις τεχνικές μεταγωγής πακέτων.
4. Αν η συσκευή προορισμού δεν ανήκει στο τοπικό δίκτυο, πρέπει να προωθηθεί βάση των πρωτοκόλλων του επιπέδου 3, όπως το IP ή το IPX.
5. Στη συνέχεια το switch επιπέδου 3 στέλνει το πρώτο πακέτο δεδομένων από την ακολουθία των πακέτων σε ένα router το οποίο θα εκτελέσει τις λειτουργίες δρομολόγησης RIP ή OSPF.
6. Η διεύθυνση IP επιπέδου 3 και η φυσική διεύθυνση επιπέδου 2 της συσκευής προορισμού αποφασίζονται και γίνεται γνωστή η καλύτερη διαδρομή.
7. Αφού τα πρωτόκολλα του επιπέδου 3 έχουν εφαρμοστεί, το πακέτο IP εμπεριέχεται στο πλαίσιο.
8. Ο τελικός σταθμός αποφασίζει αν είναι ταχύτερος τρόπος να συνεχιστεί η μετάδοση των πακέτων μέσω της δρομολόγησης χρησιμοποιώντας τα πρωτόκολλα επιπέδου 3 ή να γίνει η μεταγωγή των δεδομένων μέσω των πρωτοκόλλων του επιπέδου 2.
9. Αν αποφασιστεί πως η δρομολόγηση είναι ταχύτερη, τότε τα εναπομείναντα πλαίσια δρομολογούνται.

10. Αν αποφασιστεί πως η μεταγωγή είναι ταχύτερη, τότε τα πλαίσια αποστέλλονται πίσω στο switch, το οποίο πλέον γνωρίζει από το router πώς να στείλει τα δεδομένα στο προορισμό του ξεχωριστού δικτύου και ποια διαδρομή είναι καλύτερη.
11. Τα εναπομείναντα πλαίσια μπορούν να σταλούν μέσω της μεταγωγής με τη ταχύτητα του καλωδίου χρησιμοποιώντας τα πρωτόκολλα επιπέδου 2.[20]

Τα επιπέδου 3 switches έχουν δύο μεθόδους μεταγωγής δεδομένων. Η πρώτη μέθοδος είναι η Packet-by-Packet Layer 3 (PPL3). Τα switches ψάχνουν κάθε πακέτο για να προσδιορίσουν τη λογική διεύθυνση προορισμού επιπέδου 3 (όπως είναι η διεύθυνση IP προορισμού). Τα PPL3 switches λειτουργούν ουσιαστικά ως υψηλής ταχύτητας router που έχουν κατασκευασμένη τη λειτουργία δρομολόγησης στο υλικό τους και όχι στο λογισμικό τους. Όπως και τα routers, εκτός από τη προώθηση πακέτων προς το προορισμό, έτσι και τα PPL3 switches εκτελούν και άλλες λειτουργίες που ένα router εκτελεί όπως να χρησιμοποιεί τον έλεγχο των πακέτων για βεβαιώσει την ακεραιότητα του πακέτου, να ενημερώνει τις πληροφορίες του χρόνου ζωής του πακέτου (Time to Live – TTL) μετά από κάθε άλμα, και να επεξεργάζεται την επιπλέον πληροφορία στην επικεφαλίδα του πακέτου. Τα PPL3 switches επικοινωνούν μεταξύ τους χρησιμοποιώντας τα πρωτοκόλλα RIP και OSFP με σκοπό να μάθουν την ολική τοπολογία του δικτύου.[22]

Η άλλη μέθοδος που χρησιμοποιείται για την δρομολόγηση πακέτων είναι η Cut-Through ή Flow Control.[20] Τα switches που χρησιμοποιούν αυτή τη μέθοδο ελέγχουν μόνο το πρώτο πακέτο, από μια σειρά πακέτων που δέχονται, ώστε να καθορίσουν τη λογική διεύθυνση προορισμού επιπέδου 3, και στη συνέχεια προωθούν τα υπόλοιπα πακέτα χρησιμοποιώντας τη φυσική διεύθυνση του επιπέδου 2. Έτσι μπορούμε να πετύχουμε υψηλότερα ποσοστά διεκπεραίωσης δεδομένων.[22]

Τέλος, τα switches επιπέδου 3 αποτελούν συνήθως τη ραχοκοκαλιά των τοπικών δικτύων. Τα routers συνδέουν κυρίως τα τοπικά δίκτυα με μεγαλύτερα δίκτυα ευρείας περιοχής ή για τη σύνδεση μεταξύ των vlans.[6]

# 2.10 MULTILAYER SWITCHES

Ένα πολυεπίπεδο switch (multilayer switch-MLS) είναι μια δικτυακή συσκευή που έχει τη δυνατότητα να λειτουργεί στα υψηλότερα επίπεδα του μοντέλου αναφοράς OSI, σε αντίθεση με τα παραδοσιακά switches που λειτουργούν στο δεύτερο επίπεδο. Ένα άλλο όνομα για τα MLS επίσης είναι το NetFlow-Based Switching.[24] Ένα MLS εκτελεί τις λειτουργίες ενός switch καθώς και ενός router με πολύ γρήγορες ταχύτητες. Το MLS εξετάζει αναλυτικότερα τις πληροφορίες που λαμβάνει ή αποστέλλει (σε πακέτα ή σε επίπεδο τομέα). Το MLS χρησιμοποιεί τα κυκλώματα ASIC για να εκτελέσει τη δρομολόγηση των πακέτων σε αντίθεση με τα παραδοσιακά routers που εδρεύουν σε μικροεπεξεργαστές και χρησιμοποιούν εφαρμογές που εκτελούνται σε αυτό, για να εκτελέσουν τις λειτουργίες δρομολόγησης τους.[23]

Για να αναλύσουμε τη λειτουργεία των MLS πρέπει πρώτα να κατανοήσουμε, πώς το δίκτυο στέλνει τη κίνηση μεταξύ δύο σημείων. Χρησιμοποιώντας άλλα πρωτόκολλα συμπεριλαμβανομένων των πρωτοκόλλων του επιπέδου 2 και του του επιπέδου 4, η δικτυακή κίνηση δημιουργείτε από πολλές διατερματικές συζητήσεις που είναι γνωστές και με τον όρο ροή (flows). Το MLS αναγνωρίζει τη δικτυακή ροή από τη πηγή προς το δέκτη χρησιμοποιώντας τις πληροφορίες του δικτύου και του επιπέδου 4 στην επικεφαλίδας του πακέτου και έπειτα προωθεί τα πακέτα. Αυτή η ακολουθία των πακέτων από μία κατεύθυνση μεταξύ μία συγκεκριμένης πηγής και δέκτη και χρησιμοποιεί το ίδιο πρωτόκολλο και τις πληροφορίες του επιπέδου 4 της επικεφαλίδας.[4]

## 2.10.1 ΙΕΡΑΡΧΙΑ ΡΟΗΣ ΚΙΝΗΣΗΣ

Το MLS αναγνωρίζει τη μοναδική ροή μεταξύ των υπολογιστών αναγνωρίζοντας την εφαρμογή του χρήστη και ταξινομώντας τη κίνηση δεδομένων με το κατάλληλο επίπεδο προτεραιότητας. Οι ροές μπορεί να είναι κίνηση μοναδικής διανομής ή πολλαπλής διανομής.[4]

Το MLS αναγνωρίζει τις μεμονωμένες ροές δικτυακής κίνησης ώστε να παρέχει προβλεπόμενες υπηρεσίες του δικτύου. Αυτό το πετυχαίνει παρέχοντας ένα ειδικό εύρος ζώνης για τις εφαρμογές που το έχουν ανάγκη περισσότερο.[4]

## 2.10.2 ΣΤΟΙΧΕΙΑ ΕΝΟΣ MULTILAYER SWITCH

Το MLS περιέχει τρία στοιχεία τα οποία χρησιμοποιεί για να μπορέσει να αποφασίσει τη διαδρομή προορισμού που θα ακολουθήσει η αρχική ροή των πακέτων. Τα στοιχεία αυτά είναι:

1. MLS switching Engine (MLS-SE): Το switch που υποστηρίζει τη λειτουργία MLS.[4][24]
2. MLS Router Processor (MLS-RP): Είναι ο εσωτερικός επεξεργαστής μέσα στο switch ή το εξωτερικό router που υποστηρίζει τη λειτουργία MLS.[4][24]
3. Multilayer Switch Protocol (MLSP): Είναι το πρωτόκολλο που λειτουργεί μεταξύ του MLS-SE και MLS-RP για την ενεργοποίηση της λειτουργίας MLS.[4][24]

## 2.10.3 ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ MULTILAYER SWITCHES

Όταν η διαδικασία ροής ξεκινήσει, το MLS-SE ξεκινάει και στέλνει πολλαπλής διανομής μηνύματα hello κάθε δεκαπέντε δευτερόλεπτα σε όλα τα switches του δικτύου που λαμβάνουν MLS-RP μηνύματα. Τα μηνύματα ενημερώνουν τα switches πως το MLS-RP μπορεί να παρέχει πληροφορίες δρομολόγησης στα MLS switches επιτρέποντας τα να αποθηκεύουν προσωρινά τις διαδρομές που έχουν μάθει.[4]

Το πρωτόκολλο MLSP χρησιμοποιεί το πρωτόκολλο Cisco Group Management Protocol (CGMP) πολλαπλής διανομής διεύθυνσης έτσι ώστε κάθε MLS-SE που ενεργοποιείται για το CGMP να δεχτεί τα HELLO μηνύματα. Για να ξεχωρίζουν τα μηνύματα CGMP και τα μηνύματα MLS, το MLS-RP χρησιμοποιεί ένα ειδικό τύπου πρωτόκολλο, μέσα στο δικό του μήνυμα HELLO.[4]

Το MLSP HELLO μήνυμα, που αλλιώς λέγεται και διαφήμιση του MLS-RP, περιέχει τις παρακάτω πληροφορίες:

- Τις φυσικές διευθύνσεις των διεπαφών των routers που συμμετέχουν στη διαδικασία MLS.[4]
- Τις πληροφορίες των routers για τα γνωστά VLANs.[4]
- Τις λίστες πρόσβασης του MLS-RP.[4]

- Και τη κάθε γνωστή ή ενημερωμένη πληροφορία δρομολόγησης. [4]

Το switch που συμμετέχει στη διαδικασία MLS έχει ένα στοιχείο του MLS-SE. Το στοιχείο αυτό, επεξεργάζεται το HELLO μήνυμα και καταγράφει τις φυσικές διευθύνσεις των διεπαφών των MLS-RP στο πίνακα της προσωρινής μνήμης του. Αν υπάρχει στο δίκτυο πολλά MLS-RP τότε το MLS-SE εκχωρεί ένα αναγνωριστικό μεγέθους 1-byte που λέγεται XTAG. Το XTAG είναι ένας αριθμός που διακρίνει τη δικτυακή ροή κάθε MLS-RP.[4]

Όταν ένας υπολογιστής ενός VLAN στο δίκτυο αρχίσει μια δικτυακή ροή που προορίζεται για έναν άλλο υπολογιστή που ανήκει σε διαφορετικό VLAN, το MLS switch που θα λάβει το πρώτο πακέτο της ροής εξάγει τις πληροφορίες του επιπέδου 3. Οι πληροφορίες αυτές περιέχουν τη διεύθυνση προορισμού και της πηγής, και τον αριθμό θυρών του πρωτοκόλλου. Έπειτα, το MLS-SE προωθεί το πακέτο αυτό στο MLS-RP για την ανάλυση της διαδρομής. Το MLSP χρησιμοποιείται για να ενημερώσει το MLS-SE, για την διαδρομή του δέκτη, επικοινωνώντας με τη ροή. Λόγω του ότι είναι το πρώτο πακέτο της ροής, δεν υπάρχει καμία εγγραφή στη προσωρινή μνήμη. Στην MLS προσωρινή μνήμη δημιουργείται μια μερική MLS εγγραφή.[4]

Όταν το MLS-RP λάβει το πακέτο, κοιτάει το πίνακα δρομολόγησης του για να καθορίσει το προορισμό του πακέτου και εφαρμόζει τυχόν ισχύουσες πολιτικές, όπως μια λίστα πρόσβασης από εισερχόμενων ή εξερχόμενων. Το MLS-RP θα ξαναγράψει τη επικεφαλίδα του πακέτου, προσθέτωντας τη φυσική διεύθυνση του δέκτη και χρησιμοποιώντας ως διεύθυνση πηγής, τη δική του φυσική διεύθυνση. Έπειτα θα ξαναστείλει πίσω στο MLS-SE το πακέτο. Σε αυτό το σημείο, το MLS router έχει μετατρέψει τη διεύθυνση ενός πακέτου, VLAN ή τη λογική διεύθυνση επιπέδου 3, σε μια φυσική διεύθυνση επιπέδου 2. Το MLS-SE μπορεί να χρησιμοποιήσει τη διεύθυνση αυτή για να πάρει την απόφαση προώθησης και να στείλει το πακέτο από τη σωστή θύρα που συνδέεται με το δέκτη, βάση των εγγραφών που έχει το switch στο πίνακα της προσωρινής του μνήμης. Επίσης, το MLS-SE καθορίζει πως η φυσική διεύθυνση του MLS router είναι η διεύθυνση πηγής στο πακέτο και πως η ροή πληροφοριών του πακέτου ταιριάζει με την υποψήφια εγγραφή που έχει αποθηκευμένη στη προσωρινή MLS μνήμη του.[4]

Τώρα που έχει προστεθεί στη προσωρινή μνήμη του MLS η εγγραφή για τη ροή, οποιοδήποτε άλλο πακέτο αναγνωριστεί πως ανήκει σε αυτή τη ροή, θα το

διαχειριστεί το MLS-SE και η μεταγώγιση θα γίνει βάση των εγγραφών της προσωρινής μνήμης του. Το MLS-SE ξαναγράφει τις επικεφαλίδες, επιδιορθώνει το άθροισμα των ελέγχων και προωθεί τα πακέτα χωρίς αυτά να χρειάζεται να περάσουν από το router. Το MLS-SE ξαναγράφει τα πακέτα έτσι ώστε να φαίνεται πως έχουν ήδη προωθηθεί από το router.[4]

Όταν η επικοινωνία μεταξύ δύο κόμβων τελειώσει ή διακοπεί για τον οποιοδήποτε λόγο, η προσωρινή μνήμη του MLS διαγράφεται. Πρέπει η διαδικασία να ξαναρχίσει από την αρχή, για να λάβει μέρος μια νέα συνομιλία μεταξύ δύο κόμβων.[4]

### 2.10.4 ACCESS LIST FLOW MASKS

Οι μάσκες ροής (flow masks) χρησιμοποιούνται από το MLS-SE για να καθοριστεί πως οι ροές συγκρίνονται με τις εγγραφές της προσωρινής μνήμης MLS. Ποιος τύπος μάσκας ροής θα χρησιμοποιηθεί καθορίζεται από τρεις τύπους λιστών πρόσβασης που διαμορφώνονται από τα MLS-RP που συμμετέχουν στη διαδικασία MLS. Το MLS-SE ενημερώνεται για αυτή τη πληροφορία διαμέσου των MLSP μηνυμάτων από το κάθε MLS-RP ξεχωριστά για το ποιο MLS-SE θα χρησιμοποιήσει τη δρομολόγηση επιπέδου 3. Οι τρεις τύποι των λιστών πρόσβασης είναι οι εξής:[4]

- Destination-IP
- Source-Destination-IP
- IP-Flow

**Destination-IP Flow Mask:** Κάθε φορά χρησιμοποιείται μόνο μια μάσκα ροής και καθορίζεται από το βαθμό αυστηρότητας που έχει η λίστα πρόσβασης. Η μάσκα ροής με το μικρότερο βαθμό αυστηρότητας είναι η μάσκα ροής Destination-IP. Χρησιμοποιείται όταν οι λίστες πρόσβασης δεν έχουν διαμορφωθεί σε κανένα από τα MLS-RP που συμμετέχουν στη διαδικασία MLS. Στη περίπτωση αυτή, το MLS-SE θα διατηρεί μόνο μια εγγραφή MLS για κάθε IP διεύθυνση προορισμού. Οποιαδήποτε ροή που έχει προορισμό τη δεδομένη IP διεύθυνση προορισμού θα χρησιμοποιήσει τη καταχωρημένη εγγραφή MLS.[4]

**Source-Destination-IP Flow Mask:** Αυτή η μάσκα χρησιμοποιείται όταν οποιοδήποτε MLS-RP στο δίκτυο χρησιμοποιεί μια συνηθισμένη λίστα πρόσβασης. Η συγκεκριμένη μάσκα ροής χρησιμοποιείται για όλες τις ροές. Το MLS-SE διατηρεί μόνο μια MLS εγγραφή για κάθε ζευγάρι IP διεύθυνσης προορισμού και πηγής. Οποιαδήποτε ροή μεταξύ δεδομένης πηγής και προορισμού χρησιμοποιούν την εγγραφή MLS, ανεξαρτήτως του πρωτόκολλο IP που χρησιμοποιεί η διεπαφή.[4]

**IP-Flow Flow Mask:** Η IP-Flow μάσκα ροής έχει τον υψηλότερο βαθμό αυστηρότητας. Η μάσκα ροής τύπου IP-Flow χρησιμοποιείται όταν στα MLS-RP του δικτύου έχουν διαμορφωθεί εκτεταμένες λίστες πρόσβασης. Αυτή η λίστα πρόσβασης πως η IP-Flow μάσκα ροής θα χρησιμοποιηθεί για όλες τις ροές. Το MLS-SE δημιουργεί μια ξεχωριστή MLS προσωρινή μνήμη με εγγραφές για όλες τις ροές IP. Οι εγγραφές IP-Flow περιέχουν της πληροφορίες της IP διεύθυνσης της πηγής, του προορισμού, το είδος του πρωτοκόλλου, και τα πρωτόκολλα των διεπαφών.[4]

# ΚΕΦΑΛΑΙΟ 3

## 3. SPANNING TREE PROTOCOL

## 3.1 ΕΙΣΑΓΩΓΗ

Το Spanning Tree Protocol (STP) είναι ένα πρωτόκολλο διαχείρισης σύνδεσης, που ανήκει στο δεύτερο επίπεδο του μοντέλου αναφοράς OSI, το επίπεδο σύνδεσης δεδομένων και λειτουργεί στις συσκευές διασύνδεσης, τα switches.[9][27] Το πρωτόκολλο βασίζεται σε αλγόριθμο, τον οποίο ανέπτυξε η Radia Perlman ενώ εργαζόταν για την εταιρία Digital Equipment Corporation (DEC) το 1990. Τότε η τεχνολογία των switches δεν υπήρχε αλλά χρησιμοποιούσαν τη τεχνολογία των γεφυρών (Bridges) που ουσιαστικά εξυπηρετούν τον ίδιο σκοπό με τα switches, αφού τα switches αποτελούν ένα σύνολο από bridges. Για το λόγο αυτό οι ορολογίες που μπορεί να χρησιμοποιούνται και να αναφερθούν στη συνέχεια μπορεί να περιέχουν κάποιες από τις ορολογίες των γεφυρών.[4][27]

Η βασική λειτουργία του πρωτοκόλλου είναι να εξασφαλίζει την εξάλειψη των βρόχων σε ένα τοπικό δίκτυο μεταγωγής όταν τα switches συνδέονται μεταξύ τους μέσω πολλαπλών διαδρομών, και δημιουργούν παραπάνω από μια διαδρομές για έναν προορισμό, με στόχο να επιτρέπει μόνο μία ενεργή διαδρομή, την καλύτερη, μεταξύ δύο σταθμών. Τις επιπλέον διαδρομές τις μπλοκάρει προσωρινά και τις κρατάει ως εφεδρικές σε περίπτωση που η ενεργή διαδρομή σταματήσει να λειτουργεί ή υπάρξει κάποιο πρόβλημα σε αυτήν. Τότε την αντικαταστεί με κάποια από τις εφεδρικές.[27]

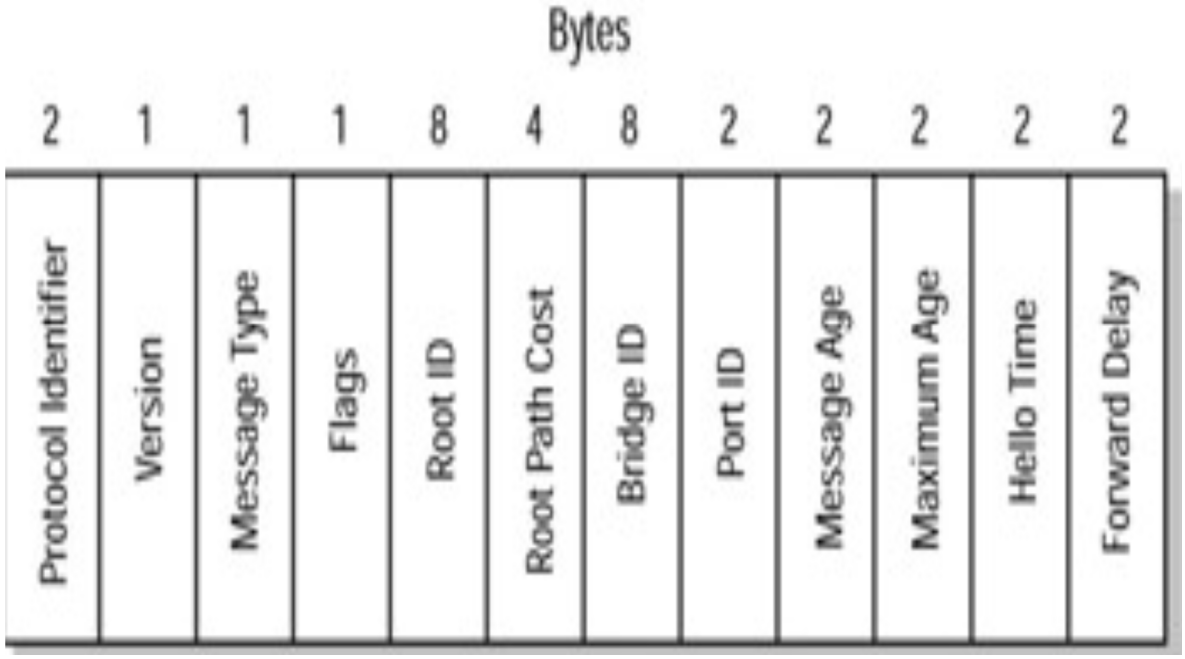
# 3.2. ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ STP

## 3.2.1 BPDU

Η σωστή λειτουργία του STP βασίζεται στην επικοινωνία μεταξύ των switches, με στόχο να γίνουν γνωστοί οι φυσικοί βρόχοι του δικτύου και να αφαιρεθούν θέτοντας συγκεκριμένες περιττές θύρες σε κατάσταση μπλοκαρίσματός ή αναμονής. [9] Η επικοινωνία αυτή γίνεται μέσω της ανταλλαγής κάποιων μηνυμάτων που περιέχουν δεδομένα. [4] Τα μηνύματα ανταλλάσσονται με τη μορφή πλαισίων των Bridge Protocol Data Units (BPDUs). Τα μηνύματα αυτά περνούν μεταξύ των switches με σκοπό να βοηθήσουν το STP να υπολογίσει και να μάθει τη τοπολογία του δικτύου. [4] Τα switches στέλνουν ένα πλαίσιο BPDU χρησιμοποιώντας τη μοναδική φυσική διεύθυνση (MAC address) της ίδιας της θύρας ως τη διεύθυνση της πηγής. Το switch που στέλνει το πλαίσιο από τη θύρα δεν γνωρίζει για τα υπόλοιπα switches γύρω από αυτό. [4] Τα μηνύματα BPDU προωθούνται από όλα τα switches, μεταξύ αυτών, προς όλες τις θύρες των switches με αποτέλεσμα οι πληροφορίες να εξαπλώνονται σε όλα τα switches του δικτύου. Επομένως, ένα μήνυμα BPDU έχει μια διεύθυνση προορισμού, τη γνωστή διεύθυνση πολλαπλής διανομής του STP 01-80-c2-00-00-00 ώστε να φτάσει σε όλα τα switches που βρίσκονται σε κατάσταση ακρόασης.[5] Τα μηνύματα αυτά αποστέλλονται τυπικά ανά 1 ως 4 δευτερόλεπτα.[3] Από προεπιλογή, τα μηνύματα BPDU αποστέλλονται κάθε 2 δευτερόλεπτα σε κάθε θύρα για να εξασφαλίσουν ένα σταθερό δίκτυο χωρίς τυχαίους βρόχους δεδομένων. [3] Αυτά τα μηνύματα ελέγχου περιέχουν πληροφορίες σχετικά με το switch που έστειλε το μήνυμα και θα χρησιμοποιηθούν από τον παραλήπτη switch για να πάρει αποφάσεις του πρωτόκολλου αν αυτό είναι απαραίτητο.[9]

Υπάρχουν τρεις τύποι μηνυμάτων BPDUs : το configuration BPDU (CBPDU) που χρησιμοποιείται για τον υπολογισμό σχεδίασης της τοπολογίας δέντρου του STP, και το Topology Change Notification (TCN) BPDU που χρησιμοποιείται για να αναφέρει αλλαγές που έχουν συμβεί στη τοπολογία του δικτύου και το Topology Notification Acknowledgement (TCA).[26]

Παρακάτω βλέπουμε τα πεδία ενός configuration BPDU μηνύματος καθώς και το μέγεθος του κάθε πεδίου.




***Εικόνα 3.1:*** *Πεδία του μηνύματος Configuration BPDU[4]*

- **Protocol Identifier** (2 bytes): Περιέχει τη τιμή 0000 για το πρότυπο IEEE 802.1d.[3]
- **Version Identifier** (1 byte): Περιέχει τη τιμή 0.[3]
- **Message Type** (1 byte): Περιέχει το τύπου του μηνύματος του BPDU, Configuration ή TCN BPDU.[3]
- **Flags** (1 byte): Περιέχει 8 bit. Από τα 8 αυτά bit μόνο τα δύο χρησιμοποιούνται. Το 1$^{ο}$ bit που περιέχει τη πληροφορία για το αν υπάρχει αλλαγή στη τοπολογία ( Topology Change bit: TC) και το 8$^{ο}$ bit που περιέχει τη πληροφορία βεβαίωσης (Topology Change Acknowledgement: TCA) για το αν έχει υπάρξει αλλαγή στο τοπολογία.[3]

  1:Topology Change Flag
  2:unused 0
  3:unused 0
  4:unused 0
  5:unused 0
  6:unused 0
  7:unused 0
  8:Topology Change Ack

- **Root ID** (8 bytes): Περιέχει το μοναδικό αναγνωριστικό του switch, που ο αποστολέας πιστεύει πως είναι το switch ρίζα (root switch) καταγράφοντας τον αριθμό προτεραιότητας (2 bytes) ακολουθούμενο από τη φυσική διεύθυνση (MAC Address) (6 bytes).[3]
- **Root Path Cost** (4 bytes): Περιέχει τη πληροφορία του κόστους της διαδρομής από τη θύρα μετάδοσης προς το root switch.[3]
- **Bridge ID ή Switch ID** (8 bytes): Περιέχει το μοναδικό αναγνωριστικό του switch που μεταδίδει το μήνυμα.[3]
- **Port ID** (2 bytes): Περιέχει το αναγνωριστικό της θύρας του switch μέσω του οποίου μεταδόθηκε το μήνυμα.[3]
- **Message Age** (2 bytes): Περιέχει το συνολικό χρόνο που έκανε το μήνυμα BPDU να μεταδοθεί από το root switch προς το επόμενο switch. Το root switch στέλνει το BPDU μήνυμα με μια τιμή 0 και κάθε επόμενο switch που δέχεται το μήνυμα προσθέτει 1 σε αυτή τη τιμή.[3][31]
- **Maximum Age ή Max Age** (2 bytes): Περιέχει τη τιμή του χρονικού ορίου που θέτει το root switch και χρησιμοποιείται για να περιοριστεί το χρονικό διάστημα για το οποίο θεωρείται έγκυρο το τελευταίο μήνυμα και μετά διαγράφεται. Η προεπιλεγμένη τιμή είναι 20 δευτερόλεπτα.[3]
- **Hello Time** (2 bytes): Περιέχει τη χρονική στιγμή για το πόσο συχνά στέλνονται τα μηνύματα από το root switch. Η προεπιλεγμένη τιμή είναι 2 δευτερόλεπτα.[3]
- **Forward Delay** (2 bytes): Περιέχει το χρονικό όριο για το οποίο τα switches θα πρέπει να περιμένουν πριν μεταβούν σε μια νέα κατάσταση αφού έχει προηγηθεί κάποια αλλαγή στη τοπολογία του δικτύου. Η προεπιλεγμένη τιμή είναι 15 δευτερόλεπτα.[3]

### 3.2.2 ΕΚΛΟΓΗ ΤΟΥ SWITCH ROOT

Σε ένα δίκτυο για να συμφωνούν όλα τα switches σε μια τοπολογία χωρίς βρόχους, πρέπει να υπάρχει ένα κοινό σημείο αναφοράς που θα το χρησιμοποιούν για καθοδήγηση. Το σημείο αναφοράς αυτό ονομάζεται Root Switch ή Root Bridge. [4]

Το root switch επιλέγεται μέσω μιας διαδικασίας εκλογής μεταξύ όλων των συνδεδεμένων switches στο δίκτυο. Κάθε switch έχει μια μοναδική ταυτότητα, το αναγνωριστικό του switch, το Switch ID, που χρησιμοποιούν για να ξεχωρίζει το καθένα τον εαυτό του από τα υπόλοιπα. Το αναγνωριστικό αποτελείται από τιμή των 8 byte και περιέχει δύο πεδία.[4] Την προτεραιότητα γέφυρας ή την προτεραιότητα μεταγωγέα (Bridge Priority ή Switch Priority) (2 bytes). Είναι η προτεραιότητα ή το βάρος ενός switch σε σχέση με τα άλλα switches. Το πεδίο προτεραιότητας έχει ένα εύρος τιμής από το 0 – 65,535. Η προεπιλεγμένη τιμή για όλες τις συσκευές που εκτελούν το πρότυπο IEEE STP version είναι 32,768. Η τιμή αυτή μπορεί να αλλαχτεί από τον χρήστη.[4] Και τη φυσική διεύθυνση (MAC Address) (6 bytes). Η διεύθυνση αυτή, είναι μία μοναδική ταυτότητα που αποδίδεται στα switches για την επικοινωνία. Αυτή η διεύθυνση μπορεί να προκύψει είτε από τον ίδιο τον κατασκευαστή της συσκευής είτε από ένα πλήθος 1024 διευθύνσεων που έχουν ανατεθεί σε κάθε κατασκευαστή, εξαρτώντας το μοντέλο του switch. Σε κάθε περίπτωση, η διεύθυνση αυτή είναι μόνιμη, μοναδική και δεν μπορεί να αλλαχτεί από τον χρήστη.[4]

Όταν ένα switch έρθει σε λειτουργία για πρώτη φορά δεν έχει πλήρη εικόνα για το ποιες άλλες συσκευές υπάρχουν γύρω του και έτσι θεωρεί τον εαυτό του ως root switch. Αυτό όπως είναι λογικό αλλάζει καθώς και άλλα switches μπαίνουν σε λειτουργία και μπαίνουν στην διαδικασία της εκλογής στέλνοντας τα δικά τους μηνύματα BPDU. Παρόλα αυτά, μόνο τα μηνύματα που έχουν πληροφορίες για το πραγματικό root switch εξακολουθούν να προωθούνται μέσω των switches. Τα υπόλοιπα μηνύματα θεωρούνται τελικά κατώτερα σε σχέση με αυτά που έχουν τις πληροφορίες του πραγματικού root switch με αποτέλεσμα να μην προωθούνται πλέον και ως εκ τούτου να χάνονται από το δίκτυο. [4]

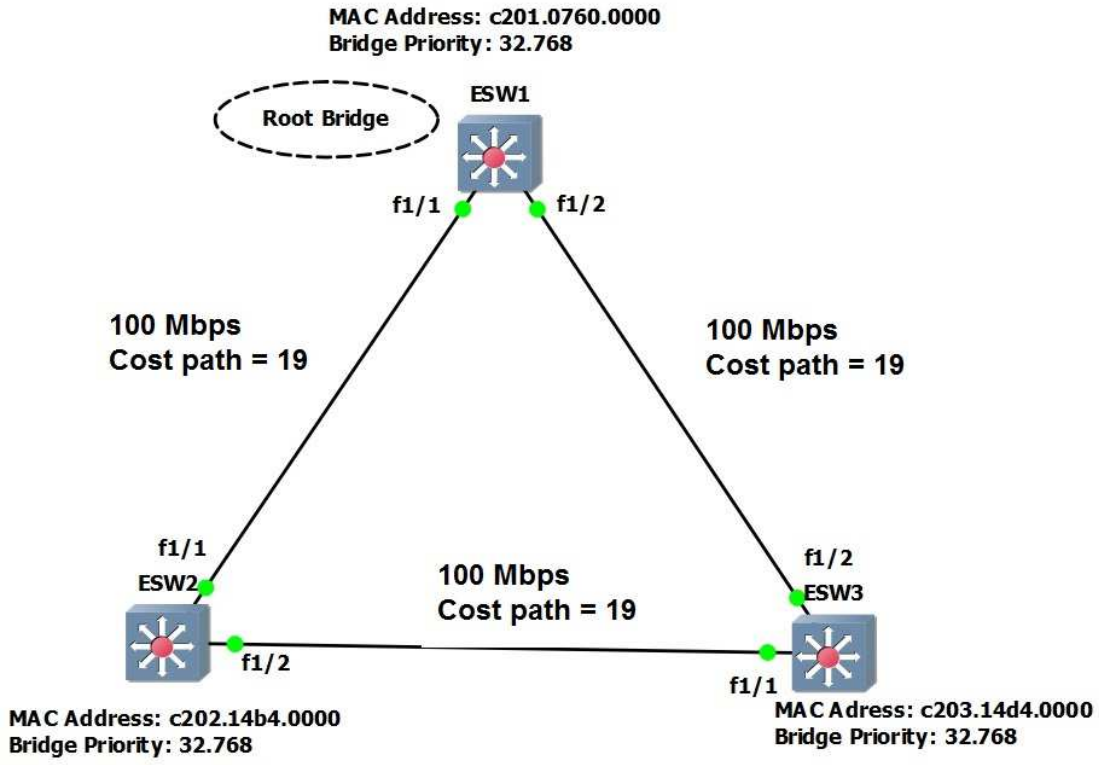
Η λειτουργία της εκλογής του Root Bridge ή του Root Switch έχει ως εξής: Κάθε switch ξεκινάει τη λειτουργία του στέλνοντας μηνύματα BPDUs που περιέχουν το αναγνωριστικό γέφυρας ρίζας (Root Bridge ID) ίδιο με το δικό του αναγνωριστικό γέφυρας (Bridge ID) και το αναγνωριστικό αποστολέα γέφυρας (Sender Bridge ID)

που είναι ίδιο με το αναγνωριστικό γέφυρας (Bridge ID) του. Το αναγνωριστικό αποστολέα γέφυρας ενημερώνει τα υπόλοιπα switches για το ποιος είναι ο αποστολέας του BPDU μηνύματος.

Τα λαμβανόμενα μηνύματα BPDU αναλύονται για να ανακοινωθεί το καλύτερο root switch. Καλύτερο switch root είναι το switch που έχει τη χαμηλότερη τιμή του root bridge ID. Όπως αναφέραμε το root bridge ID περιέχει δύο πεδία. Αν δύο switches έχουν ίδια προτεραιότητα γέφυρας τότε καλύτερο είναι το switch με τη μικρότερη φυσική διεύθυνση.[4] Επομένως, όταν ένα switch λάβει ένα μήνυμα BPDU στο οποίο αναφέρεται καλύτερο root bridge ID, τότε το switch αντικαθιστά το δικό του root bridge ID με αυτό του μηνύματος BPDU που έλαβε. Επίσης απαιτείται να ορίσει το νέο root bridge ID στο μήνυμα BPDU που θα προωθήσει διατηρώντας το δικό του αναγνωριστικό αποστολέα γέφυρας.[4]

Όταν όλα τα switches στείλουν μεταξύ τους μηνύματα BPDU η εκλογή θα συγκλίνει και όλα τα switches θα συμφωνούν στην ιδέα πως κάποιο από αυτά είναι η γέφυρα ρίζα. Είναι προφανές πως αν ένα switch μπει σε λειτουργία με χαμηλότερη τιμή προτεραιότητας ή ίσης τιμής προτεραιότητας και χαμηλότερης τιμής της φυσικής διεύθυνσης θα στέλνει μηνύματα BPDU υποστηρίζοντας πως αυτό είναι η νέα γέφυρα ρίζα. Λόγω του ότι όντως καινούργια switches έχουν μικρότερη τιμή αναγνωριστικού γέφυρας, όλα τα switches θα το θεωρούν και θα το καταγράψουν ως τη νέα γέφυρα ρίζα. Η εκλογή γέφυρας ρίζας είναι μια συνεχόμενη διαδικασία η οποία προκαλείται σε αλλαγές της τιμής του αναγνωριστικού γέφυρας ρίζας στα μηνύματα BPDU κάθε δύο δευτερόλεπτα.[4]

Ένα παράδειγμα εκλογής του root switch μπορούμε να δούμε στην εικόνα που ακολουθεί:[4]




***Εικόνα 3.2:*** *Παράδειγμα εκλογής του root switch.*

Σε αυτό το δίκτυο έχουμε τρία switches τα οποία έχουν την ίδια τιμή προτεραιότητας γέφυρας 32,768. Διασυνδέονται μεταξύ τους με συνδέσεις FastEthernet και έχουν τη προεπιλεγμένη τιμή κόστους διαδρομής 19. Τα τρία switches προσπαθούν να εκλέξουν τον εαυτό τους ως γέφυρα ρίζα αλλά έχουν ίδια τιμή προτεραιότητα γέφυρας. Συνεπώς η εκλογή γίνεται με κριτήριο τη χαμηλότερη φυσική διεύθυνση μεταξύ αυτών, και προφανώς τη μικρότερη φυσική διεύθυνση κατέχει το switch ESW1.[4]

## 3.2.3 ΕΠΙΛΟΓΗ ΤΩΝ ROOT PORTS

Αφού ολοκληρωθεί η εκλογή του switch root ως σημείο αναφοράς για όλο το δίκτυο, πρέπει κάθε ένα από τα υπόλοιπα switch να κατανοήσει ποια είναι η σχέση του με το σημείο αναφοράς δηλαδή το root switch. Για να επιτευχθεί κάτι τέτοιο επιλέγεται μία από τις θύρες κάθε switch ως θύρα ρίζας (Root Port). Η root port έχει κατεύθυνση πάντα προς το τρέχον switch root, και η θύρα που θα επιλεχτεί είναι αυτή που θα έχει το μικρότερο cost path προς το root switch. Το STP χρησιμοποιεί τον όρο

«κόστος» για να καθορίσει αρκετά πράγματα. Η επιλογή μιας root port συνεπάγεται την αξιολόγηση του κόστους διαδρομής της ρίζας (Root Path Cost). Το root path cost του κάθε switch προσδιορίζεται με τον εξής τρόπο: [4]

Πρώτον το root switch στέλνει ένα μήνυμα BPDU με ένα root path cost ίσο με το 0 διότι οι θύρες που στέλνουν το μήνυμα είναι οι θύρες του root switch. Στη συνέχεια όταν το επόμενο κοντινό switch παραλάβει αυτό το μήνυμα προσθέτει το path cost της ίδιας της θύρας που έφτασε το μήνυμα. Έπειτα προωθεί το μήνυμα BPDU με το νέο αθροιστικό κόστος ως το root path cost. Τέλος το root path cost αυξάνεται από την είσοδο του cost path της θύρας καθώς λαμβάνονται τα μηνύματα BPDU σε κάθε επόμενο switch. [4] Μετά την προσαύξηση του root path cost, τα switches καταγράφουν τις τιμές αυτές στη μνήμη. Όταν ένα BPDU μήνυμα λαμβάνεται από μια άλλη θύρα και το νέο root path cost είναι μικρότερο από την προηγούμενη τιμή που είχε αποθηκεύσει η θύρα, αυτή η χαμηλότερη τιμή γίνεται το νέο path cost του switch. Επιπρόσθετα το χαμηλότερο κόστος της τιμής ενημερώνει το switch πως η διαδρομή προς το root switch είναι καλύτερη χρησιμοποιώντας αυτή θύρα σε σχέση με τις άλλες θύρες. Ως εκ τούτου η νέα root port είναι η θύρα που έχει τη μικρότερη τιμή του root path cost.[4]

Ένα switch μπορεί να έχει ενεργή μόνο μία θύρα ρίζας. Το root path cost προς το root switch υπολογίζεται από το άθροισμα των path cost που έχουν εκχωρηθεί εξ ορισμού σε κάθε θύρα για το ελάχιστο path cost. Οι εκχωρήσεις γίνονται συνήθως ως συνάρτηση του εύρους ζώνης των συνδέσεων. Όσο πιο μεγάλο είναι το εύρος ζώνης τόσο πιο μικρό είναι το path cost.[4] Το μικρότερο path cost προτιμάται διότι είναι το καλύτερο.[5]

| Bandwidth | Path Cost |
|---|---|
| 4 Mbps | 250 |
| 10 Mbps | 100 |
| 16 Mbps | 62 |
| 45 Mbps | 39 |
| 100 Mbps | 19 |
| 155 Mbps | 14 |
| 200 Mbps | 12 |
| 622 Mbps | 6 |

| | |
|---|---|
| 1 Gbps | 4 |
| 2 Gbps | 3 |
| 10 Gbps | 2 |

***Πίνακας 3.1****: Αντιστοιχία εύρους ζώνης με κόστος διαδρομής.*

## 3.2.4 ΕΠΙΛΟΓΗ ΤΩΝ DESIGNATED PORTS

Μετά την επιλογή των root ports, το STP κάνει έναν επιπλέον υπολογισμό και αναγνωρίζει μία καθορισμένη θύρα (Designated Port) σε κάθε switch του δικτύου με παρόμοιο τρόπο όπως και τις θύρες ρίζας.[5]

Τα switches επιλέγουν τη designated port σε σχέση με το συνολικό path cost προς τη root port. Αν υπάρχει ισοπαλία μεταξύ δύο switches ή παραπάνω, τότε γίνεται έλεγχος για το Bridge ID και επιλέγουν με βάση το κριτήριο αυτό τη designated port. Το ίδιο ισχύει και για την επιλογή της root port.[5]

Η θύρα αυτή χρησιμοποιείται για την προώθηση κίνησης από και προς τα switches στο δίκτυο. Επιπλέον, είναι η θύρα που συνδέει το switch στο φυσικό σημείο σύνδεσης του ορισμένου switch. Κάθε switch έχει μόνο μία designated port. [9] Οι υπόλοιπες θύρες που δεν έχουν οριστεί ως root port ή designated port θεωρούνται ως εναλλακτικές (Alternative Ports ή Non Designated Ports), μπαίνουν σε κατάσταση μπλοκαρίσματος (blocking) και δεν προωθείται κίνηση μέσω αυτών των θυρών.[5]

## 3.2.5 PORT STATES

Στα τοπικά δίκτυα μεταγωγών επειδή η τοπολογία των switches μπορεί να αλλάξει σε διαφορετικές χρονικές στιγμές και σε διαφορετικά σημεία του δικτύου με αποτέλεσμα τα switches να προσαρμόζονται σε αυτές τις αλλαγές. Η προσαρμογή γίνεται με τη μετάβαση σε διαφορετικές καταστάσεις των θυρών των switches. Οι θύρες μπορούν να μεταβούν σε πέντε διαφορετικές καταστάσεις:[4]

- **Blocking:** Όλες οι θύρες των switches όταν ενεργοποιούνται για πρώτη φορά είναι εξ ορισμού σε κατάσταση μπλοκαρίσματος. Οι θύρες σε αυτή τη κατάσταση δεν μπορούν να προωθήσουν κίνηση ούτε να προσθέσουν τις

φυσικές διευθύνσεις από άλλες συσκευές στο πίνακα των φυσικών διευθύνσεων. Μπορούν να ακούν μόνο τα BPDUs μηνύματα από τα γειτονικά switches για να μαθαίνουν αλλαγές που γίνονται στο δίκτυο. Σκοπός αυτής της κατάστασης είναι να αποτρέψει τη δημιουργία βρόχων.[4]

- **Listening:** Μία θύρα μεταβαίνει σε αυτή τη κατάσταση όταν το switch πιστεύει ότι η θύρα αυτή μπορεί να επιλεχτεί ως root port ή designated port. Με άλλα λόγια προετοιμάζεται η θύρα στη προώθηση δεδομένων. Σε αυτή τη κατάσταση δεν μπορεί ούτε να λάβει ούτε να στείλει δεδομένα. Επιτρέπεται όμως να δέχεται και να στέλνει BPDUs μηνύματα για να πάρει μέρος στη διαδικασία της δημιουργίας της τοπολογίας του STP. Τότε η θύρα μπορεί να χαρακτηριστεί ως root port ή designated port αφού το switch ενημερώνει τα υπόλοιπα switches στέλνοντας BPDUs μηνύματα. Αν η θύρα δεν χαρακτηριστεί ως root port ή designated port τότε επιστρέφει στη κατάσταση blocking.[4]
- **Learning:** Αν η θύρα χαρακτηριστεί ως root port ή designated port, μετά από μια χρονική περίοδο που λέγεται forward delay, στη κατάσταση listening, επιτρέπεται να μεταβεί στη κατάσταση learning. Η θύρα εξακολουθεί να στέλνει και να δέχεται BPDUs μηνύματα όπως και πριν. Σε αυτή τη κατάσταση επιπλέον μπορεί να μαθαίνει και να προσθέτει στο πίνακα του τις φυσικές διευθύνσεις άλλων συσκευών. Forward delay είναι ο χρόνος που χρειάζεται για τη μετάβαση από τη κατάσταση learning στη κατάσταση listening, η οποία εξ ορισμού είναι δεκαπέντε δευτερόλεπτα.[4]
- **Forwarding:** Μετά από άλλη μια χρονική περίοδο forward delay στη κατάσταση learning επιτρέπεται στη θύρα να μεταβεί στη κατάσταση forwarding. Σε αυτή τη κατάσταση η θύρα μπορεί να στέλνει και να δέχεται πακέτα δεδομένων, να συλλέγει τις φυσικές διευθύνσεις και να τις προσθέτει στο πίνακα του, να στέλνει και να δέχεται BPDUs μηνύματα. Η θύρα πλέον σε πλήρη λειτουργικότητα. [4]
- **Disabled:** Οι θύρες μεταβαίνουν σε αυτή τη κατάσταση όταν απενεργοποιούνται από τον διαχειριστή του δικτύου ή από το ίδιο το σύστημα εξαιτίας κάποιου ελαττώματος. Η κατάσταση αυτή είναι ιδιαίτερη και δεν αποτελεί μέρος της φυσιολογικής εξέλιξης του STP για μια θύρα. [4]

### 3.2.6 TOPOLOGY CHANGE NOTIFICATION

Σε ένα τοπικό δίκτυο μεταγωγής, αν συμβούν αλλαγές στη τοπολογία τότε πρέπει να ληφθούν υπόψη οι αλλαγές στη διαδικασία εκμάθησης των φυσικών διευθύνσεων. Με την οποιαδήποτε αλλαγή ή τροποποίηση του δικτύου μπορεί να επιφέρει αλλαγές στις διαδρομές που ακολουθούν οι μεταδόσεις των δεδομένων διαμέσου των θυρών των switches. Για το λόγο αυτό είναι αναγκαίος ένας μηχανισμός με σκοπό την ενημέρωση της νέας επικοινωνίας μεταξύ των θυρών και των φυσικών διευθύνσεων που απαιτείται. Αυτός ο μηχανισμός ονομάζεται Topology Change. Στόχος του είναι να ενημερώνει όλα τα switches για τις αλλαγές που έχουν συμβεί στη τοπολογία του δικτύου και τα αναγκάζει να διαγράψουν όλες τις φυσικές διευθύνσεις των συσκευών που είχαν αποθηκεύσει. [9]

Η ενημέρωση για την οποιαδήποτε αλλαγή στη τοπολογία ενός ενεργού δικτύου γίνεται με την μετάδοση των TCN BPDUs μηνυμάτων από τα switches μέσω των root ports προς το root switch. Σε αυτό το περιεχόμενο του μηνύματος δεν περιέχονται πεδία πληροφοριών γιατί είναι προειδοποιητικό μήνυμα για το root switch. Ωστόσο, διαφέρει από το configuration BPDU μήνυμα και δεν εμπεριέχεται σε κάποιο από τα πεδία του διότι τα Configuration BPDUs μηνύματα προέρχονται από τα non-designated switches και δεν παραμένουν στη μνήμη των switches αλλά διαγράφονται. Γι' αυτό το λόγο χρησιμοποιούνται για τη διαδικασία αυτή τα TCN BPDUs μηνύματα. [9]

Υπάρχουν δύο περιπτώσεις στις οποίες συμβαίνει ανίχνευση αλλαγή της τοπολογίας ενός δικτύου. Όταν ένα switch αλλάξει τη κατάσταση μιας θύρας σε κατάσταση forwarding και είναι ταυτόχρονα και designated ή όταν το switch αλλάξει τη κατάσταση μιας θύρα σε κατάσταση blocking. Δηλαδή όταν μια θύρα γίνεται ενεργή ή παύει να λειτουργεί. Τότε το switch στέλνει μέσω του root port ένα TCN BPDU μήνυμα έτσι ώστε να το λάβει το root switch και να ενημερωθεί για την αλλαγή που προέκυψε. [5][9]

Έτσι λοιπόν, κάθε switch όταν ανιχνεύει μία αλλαγή ή δέχεται ένα τέτοιο μήνυμα, αρχίζει και στέλνει το ίδιο μήνυμα κάθε δύο δευτερόλεπτα που είναι ο χρόνος hello time μέχρι να παραλάβει επιβεβαίωση από κάποιο γειτονικό switch που βρίσκεται από πάνω του. Όταν τα γειτονικά switches λάβουν το TCN BPDU μήνυμα τότε θα το διαδώσουν προς το root switch. Αφού λάβει το μήνυμα το root switch, τότε θα στείλει πίσω ένα μήνυμα επιβεβαίωσης μέσω των designated ports. Άλλωστε, τα

TCN BPDUs μηνύματα αποστέλλονται προς το root switch. Επιπλέον, προσθέτει το topology change flag στο configuration BPDU μήνυμα που διαδίδει έτσι ώστε όλα τα υπόλοιπα switches να ενημερωθούν για την αλλαγή που έγινε και πως τις φυσικές διευθύνσεις που έχουν μάθει οι θύρες τους πλέον μπορεί να είναι λανθασμένες. Με αυτό τον τρόπο, το topology change flag, αναγκάζει τα switches να μειώσουν το μέγιστο χρόνο εκμάθησης του πίνακα διευθύνσεων από τη προεπιλεγμένη τιμή (300 δευτερόλεπτα) στη τιμή του χρόνου του forward delay. Με αυτό τον τρόπο τα switches αναγκάζονται να διαγράψουν συντομότερα από το κανονικό χρονικό όριο τις φυσικές διευθύνσεις που έχουν μάθει, διευκολύνοντας την αλλοίωση του πίνακα διευθύνσεων που θα μπορούσε να συμβεί με την αλλαγή της τοπολογίας του δικτύου. Ωστόσο, οι φυσικές διευθύνσεις των συσκευών που επικοινωνούν ενεργά κατά τη διάρκεια αυτής της ενέργειας, θα παραμείνουν στο πίνακα των switches. Η ενέργεια αυτή διαρκεί 15+20=35 δευτερόλεπτα (forward delay + max age).[5][9]

### 3.2.7 CONVERGENCE TIME

Το κομμάτι αυτό συγκεκριμένα υπολογίζει ποια ακριβώς είναι η χρονική στιγμή την οποία όλα τα switches έχουν φτάσει στη τελική τους διαμόρφωση στη τοπολογία του STP, και συνεπώς την ολοκλήρωση της λειτουργίας του πρωτοκόλλου.[9]

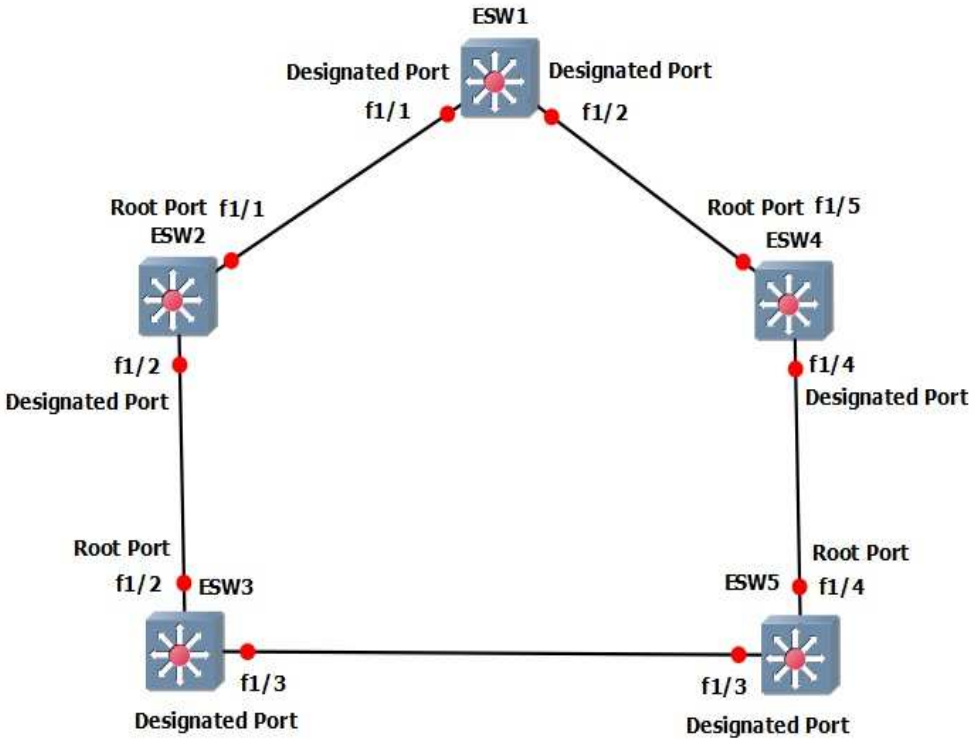
Υπάρχουν αρκετές και διαφορετικές περιπτώσεις στις οποίες το STP εκτελεί μια επαναδιαμόρφωση των switches, που μπορεί να είναι είτε μερική είτε ολική. Η πιο απλή περίπτωση είναι όταν ξεκινούμε τη λειτουργία ενός δικτύου και τα switches θα ενεργοποιηθούν για πρώτη φορά και θα πρέπει να συμφωνήσουν σε μια νέα τοπολογία και βάση δεδομένων. Με απλά λόγια είναι το χρονικό διάστημα που απαιτείται για τις θύρες των switches όταν έρχονται για πρώτη φορά σε λειτουργία να μεταβούν από τη κατάσταση blocking σε κατάσταση forwarding και να ξεκινήσει η προώθηση των δεδομένων. Ο συνολικός χρόνος σύγκλισης των θυρών από τη μετάβαση της κατάσταση τους από listening σε learning και forwarding είναι συνολικά 30 δευτερόλεπτα (15+15 ή 2* forward delay). Αυτό συμβαίνει διότι οι θύρες δεν βρίσκονταν σε κατάσταση blocking με αποτέλεσμα να εξοικονομούν 20 δευτερόλεπτα που είναι ο χρόνος max age. Αν οι θύρες βρίσκονται στη κατάσταση blocking τότε ο χρόνο μετάβασης σε κατάσταση forwarding είναι 50 δευτερόλεπτα

(15+15 ή 2* forwarding delay + 20 (max age)) που είναι και ο προεπιλεγμένος χρόνος των switches.[25] Ο χρόνος αυτός γίνεται να αλλαχτεί από τον διαχειριστή του δικτύου αλλά δεν συνιστάται. Αυτή η χρονική σύγκλιση ονομάζεται Initial Convergence.[9]

Μια άλλη περίπτωση είναι όταν έχουμε επαναδιαμόρφωση της τοπολογίας του δέντρου του STP όταν μια ενεργή σύνδεση παθαίνει κάποια βλάβη και καταρρέει.[9] Αυτού του είδους η επαναδιαμόρφωση της τοπολογίας μπορεί να είναι μερική γιατί αν έχει καταρρεύσει μια σύνδεση θα πρέπει να αντικατασταθεί από κάποια άλλη. Τέτοιου είδος σύγκλισης ονομάζεται Convergence After a Failure.[9]

Ακόμη και μια διακοπή σύνδεσης στο δίκτυο έχει διαφορετικές επιπτώσεις και επιδράσεις στο χρόνο επανασύγκλισης του STP ανάλογα σε ποιο σημείο της τοπολογίας έχει συμβεί η βλάβη. Ωστόσο, δεν είναι θέμα της φυσικής τοποθεσίας, αλλά θέμα αντίληψης των switches. Το STP αναφέρεται σε δύο ειδών βλάβες. Την άμεση βλάβη (Direct Failure) και την έμμεση βλάβη (Indirect Failure).[5]

Για να καταλάβουμε τι ακριβώς είναι το direct failure και τι το indirect failure, και από ποια προοπτική βλέπει τη κάθε βλάβη ένα switch ας δούμε το παρακάτω δίκτυο και θα εξηγήσουμε πως αντιλαμβάνεται το STP τις βλάβες.[5]




***Εικόνα 3.3:*** *Δίκτυο παραδείγματος.*

Αν για παράδειγμα το root port του switch ESW2 έχει κάποια βλάβη το ίδιο το switch θα θεωρήσει τη βλάβη αυτή ως direct failure. Το switch θα εντοπίσει άμεσα πως η φυσική του θύρα δεν λειτουργεί και το STP θα ενεργήσει αναλόγως για να επιλύσει το πρόβλημα. Την ίδια βλάβη αντίστοιχα το switch ESW3 θα την αντιμετωπίσει ως indirect failure. Αυτό θα συμβεί, γιατί η θύρα που έχει το πρόβλημα ανήκει στο switch ESW2 και όχι στο switch ESW3. Το switch ESW3 θα χάσει το δρόμο του προς root switch που είναι το switch ESW1 και θα πρέπει να ενημερωθεί μέσω των BPDUs μηνυμάτων από τα γειτονικά switch για την αλλαγή που έχει συμβεί στη τοπολογία αφού δεν μπορεί πλέον να προωθήσει πληροφορίες μέσω του ESW2.[5]

Επομένως καταλαβαίνουμε πως όταν μία θύρα ενός switch έχει κάποια βλάβη και δεν λειτουργεί, το ίδιο το switch την θεωρεί ως direct failure ενώ αντίθετα τα γειτονικά switch την αντιμετωπίζουν ως indirect failure.Και στις δύο περιπτώσεις, κατά τη διάρκεια της σύγκλισης δεν έχουμε προώθηση της κίνησης δεδομένων μέσω των switches.[5]

## 3.3 RAPID SPANNING TREE PROTOCOL

Μέχρι τώρα έχουμε αναφερθεί στο αρχικό STP. Το STP για εκείνη την εποχή που χρησιμοποιήθηκε δούλεψε σωστά. Με το πέρασμα των χρόνων και την εξέλιξη της τεχνολογίας, συνεπώς και την εξέλιξη των δικτύων και των τηλεπικοινωνιών, η ανάγκη για αναβάθμιση των διάφορων πρωτοκόλλων ήταν απαραίτητη μιας και οι απαιτήσεις της τεχνολογίας των τοπικών δικτύων αυξάνονταν παράλληλα.[29] Έτσι και το STP δέχτηκε κάποιες βελτιώσεις. Μία από τις βελτιώσεις που δέχτηκε στη πάροδο του χρόνου ήταν η εισαγωγή του Rapid Spanning Tree Protocol (RSTP) που εισήχθη ως το πρότυπο IEEE 802.1w.[29] Αρχικά η IEEE δημοσίευσε τη τροποποίηση του πρότυπου 802.1w το 2001. Έπειτα, το 2004 η επιτροπή του IEEE ενημερώνει το πρότυπο 802.1d και στη συνέχεια παίρνει τις λεπτομέρειες του τροποποιημένου προτύπου 802.1w και τις προσθέτουν στο πρότυπο 802.1d-2004. [9][10][6][27]

### 3.3.1 ΣΥΓΚΡΙΣΗ RSTP ΜΕ STP ΚΑΙ ΕΠΙΠΛΕΟΝ ΧΑΡΑΚΤΗΡΙΣΤΗΚΑ

Εάν συγκρίνουμε τα δύο πρωτόκολλα STP και RSTP θα δούμε ότι έχουν πάρα πολλές ομοιότητες και ουσιαστικά το RSTP λειτουργεί όπως και το αυθεντικό STP.[29]

- Εκλέγει το root switch χρησιμοποιώντας τις ίδιες παραμέτρους και τις ίδιες προϋποθέσεις.[29]
- Επιλέγει το root port σε κάθε switch με τους ίδιους κανόνες.[29]
- Επιλέγει τις designated ports σε κάθε τομέα του τοπικού δικτύου με τους ίδιους κανόνες.
- Τοποθετεί τις θύρες των switches στις διάφορες καταστάσεις, από forwarding ή blocking.[29]

Παρ' όλο που τα δυο πρωτόκολλα φαίνεται να δουλεύουν ακριβώς με τον ίδιο τρόπο, έχουν μια σημαντική διαφορά, που είναι και ο κύριος λόγος που δημιουργήθηκε το RSTP. Η διαφορά αυτή είναι ο χρόνος σύγκλισης. Το STP για να συγκλίνει χρειάζεται 30-50 δευτερόλεπτα ανάλογα με το είδος της βλάβης στο δίκτυο, με τις προεπιλεγμένες ρυθμίσεις όταν πρέπει να ακολουθούνται όλοι οι χρόνοι αναμονής. Χρόνος αρκετά μεγάλος και σημαντικός που είναι απαράδεκτος για την εποχή μας. Το RSTP έρχεται να βελτιώσει αυτή τη σύγκλιση, όταν υπάρξουν αλλαγές στη τοπολογία του δικτύου, μέσα σε λίγα δευτερόλεπτα (ή σε αργές συνθήκες, σε περίπου 10 δευτερόλεπτα).[29]

Το RSTP αλλάζει και προσθέτει στο STP τρόπους με τους οποίους αποφεύγει να περιμένει τους χρόνους του STP, με αποτέλεσμα τις γρήγορες μεταβολές των καταστάσεων των θυρών των switches από forward σε blocking και το αντίστροφο. Πιο συγκεκριμένα, το RSTP ορίζει περισσότερες περιπτώσεις στις οποίες ένα switch μπορεί να αποφύγει την αναμονή των χρονομέτρων ως την λήξη τους, όπως είναι οι ακόλουθες.[29]

- Προσθέτει έναν νέο μηχανισμό στο να αντικαταστεί το root port, χωρίς να περιμένει να φτάσει σε κατάσταση forwarding (σε ορισμένες περιπτώσεις).[29]
- Προσθέτει έναν νέο μηχανισμό στο να αντικαταστεί το designated port, χωρίς να περιμένει να φτάσει σε κατάσταση forwarding (σε ορισμένες περιπτώσεις).[29]

- Μειώνει τους χρόνους αναμονής σε περίπτωση που το RSTP πρέπει να περιμένει.[29]

Με το RSTP, κάθε switch ξεχωριστά, αναπαράγει RSTP Configuration BPDUs μηνύματα κάθε δύο δευτερόλεπτα (hello time). Αντιθέτως, στο STP κάθε switch αναμεταδίδει ένα hello μήνυμα το οποίο αναπαράγεται από το root switch. Το τοπικά παραγόμενο BPDU μήνυμα εξυπηρετεί το ρόλο του "διασώστη" που επαληθεύει τη συνδεσιμότητα μεταξύ των γειτονικών switches. Για παράδειγμα, όταν ένα switch σταματήσει να δέχεται hellos από ένα άλλο γειτονικό συνδεδεμένο switch, τότε μπορεί να υποθέσει με σιγουριά πως έχει χαθεί η συνδεσιμότητα σε αυτή τη θύρα χωρίς να περιμένει να λήξουν τα χρονόμετρα του πρωτοκόλλου. Απώλεια συνδεσιμότητας θεωρείται όταν τρία συνεχόμενα hellos μηνύματα έχουν χαθεί. Ένα switch μπορεί να επιταχύνει περαιτέρω τη διαδικασία ανακατεύθυνσης παρακολουθώντας τις διασυνδέσεις του ώστε να ανιχνεύσει θύρες και συνδέσεις που δεν λειτουργούν χωρίς να χρειάζεται να περιμένει για τα χαμένα RSTP Hellos.[25]

### 3.3.2 RSTP PORT ROLES

Ο καλύτερος τρόπος για να καταλάβουμε πως λειτουργούν οι μηχανισμοί που αναφέραμε προηγουμένως, είναι να εξηγήσουμε πως η εναλλακτική θύρα (alternate port) και η εφεδρική θύρα (backup port) δουλεύουν. Είναι δύο νέοι ρόλοι που το RSTP προσθέτει επιπλέον στο αρχικό STP.[25][9][25][29]

### 3.3.3 ΛΕΙΤΟΥΡΓΙΑ ΕΝΑΛΛΑΚΤΙΚΗΣ ΘΥΡΑΣ

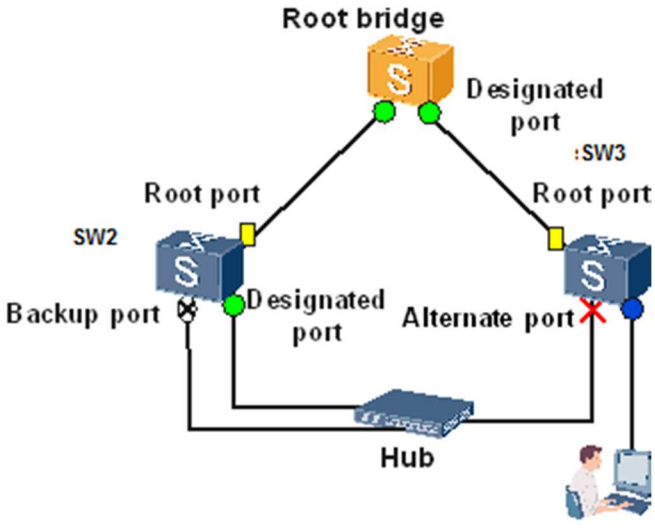
Όπως με το STP, τα switches καθόριζαν μία από τις θύρες τους ως root port έτσι και το RSTP ακολουθεί την ίδια συνθήκη με τους ίδιους ακριβώς κανόνες για να επιλέξει το root port. Έπειτα όμως το RSTP προχωράει κάνοντας ένα ακόμη βήμα, επιλέγοντας μία ή παραπάνω θύρες ως εναλλακτικές πιθανές root ports. Για να οριστεί μία θύρα ως εναλλακτική θα πρέπει και το root port και το alternate port να δέχονται hellos μηνύματα που θα αναγνωρίζουν το ίδιο root switch. Μία alternate port ουσιαστικά δουλεύει ως τη δεύτερη καλύτερη επιλογή για το root port. Η alternate port μπορεί να αναλαμβάνει τον ρόλο του root port, συχνά πολύ γρήγορα, χωρίς να απαιτείται αναμονή σε άλλες ενδιάμεσες καταστάσεις του RSTP.[29]

Για παράδειγμα, όταν ένα root port καταρρεύσει, ή όταν σταματήσει να δέχεται hellos, τότε το switch αλλάζει το ρόλο του root port σε disable port και την κατάσταση του από forwarding σε discarding. Στη συνέχεια, χωρίς να περιμένει άλλα χρονόμετρα, το switch αλλάζει το ρόλο του alternate port σε root port και τη κατάστασή του σε forwarding. Επίσης σημαντικό είναι να σημειωθεί πως το νέο root port δεν χρειάζεται επίσης να ξοδέψει χρόνο σε άλλες καταστάσεις όπως τη learning, αλλά αντιθέτως μπαίνει απευθείας σε κατάσταση forwarding.[29]

### 3.3.4 ΛΕΙΤΟΥΡΓΙΑ ΕΦΕΔΡΙΚΗΣ ΘΥΡΑΣ

Παρόμοια με το RSTP alternate port έτσι και το RSTP backup port, δίνει τη δυνατότητα στο RSTP να αντικαταστήσει γρήγορα την designated port ενός switch με μία εφεδρική θύρα. Η ανάγκη για χρήση του backup port συμβαίνει πολύ σπάνια στις μέρες μας , και ο λόγος είναι πως η σχεδίαση θα πρέπει να περιέχει hubs, τα οποία επιτρέπουν τη πιθανότητα ένα switch να συνδέει περισσότερες από μια θύρα στην ίδια περιοχή σύγκρουσης.[29]

Στην εικόνα 3.4 μπορούμε να δούμε ένα τέτοιο παράδειγμα.[33]




***Εικόνα 3.4:*** *Δίκτυο παραδείγματος της λειτουργίας εφεδρικής θύρας.*

Τα switches SW2 και SW3 συνδέονται και τα δύο στο ίδιο hub. Το SW2 τυχαίνει να κερδίσει την εκλογή ως το designated port. Η άλλη θύρα του SW2 που συνδέεται στο ίδιο πεδίο σύγκρουσης λειτουργεί ως backup port. Με την εφεδρική

αυτή θύρα, αν καταρρεύσει η designated port τότε το switch SW2 μπορεί να ξεκινήσει να χρησιμοποιεί την εφεδρική θύρα με πολύ γρήγορη σύγκλιση. Με αυτό τον τρόπο θα μπορέσει να κάνει τη μετάβαση του backup port σε designated port χωρίς καμία καθυστέρηση στη μετακίνηση της κατάστασης από discarding σε forwarding.[29]

### 3.3.5 RSTP PORT STATES

Και το RSTP και το STP χρησιμοποιούν port states αλλά με κάποιες διαφορές. Το RSTP παρέχει μια σαφή διαφοροποίηση μεταξύ της κατάστασης μιας θύρας (π.χ forwarding or blocking) και το ρόλο τον οποίο παίζει στη λειτουργία του STP (π.χ root port, ή designated port). Με το RSTP υπάρχουν μόνο τρεις καταστάσεις στις οποίες μπορεί να βρεθεί μια θύρα.[29]

- **Discarding:** Σε αυτήν τη κατάσταση η θύρα δέχεται πακέτα δεδομένων, αλλά δεν τα προωθεί. Δεν μαθαίνει τις φυσικές διευθύνσεις και ακούει για τα BPDUs μηνύματα. Σε αυτή τη κατάσταση έχουν ενσωματωθεί οι τρεις καταστάσεις του STP, blocking, listening και disabled.[29]
- **Learning:** Σε αυτή τη κατάσταση η θύρα δέχεται και μεταδίδει BPDUs μηνύματα και μαθαίνει φυσικές διευθύνσεις, αλλά δεν μπορεί να προωθήσει πακέτα δεδομένων.[29]
- **Forwarding:** Σε αυτή τη κατάσταση η θύρα δέχεται και στέλνει πακέτα δεδομένων, δέχεται και μεταδίδει BPDUs μηνύματα, μαθαίνει φυσικές διευθύνσεις και βρίσκεται σε πλήρη λειτουργικότητα.[29]

Το RSTP επίσης αλλάζει κάποιες διαδικασίες και περιεχόμενα των μηνυμάτων σε σχέση με αυτά του STP, για να επιτύχει πιο γρήγορη σύγκλιση. Για παράδειγμα, το STP περιμένει για ένα χρονικό διάστημα (forward delay) στις καταστάσεις learning και listening. Το RSTP για να κάνει τη σύγκλιση ταχύτερα αποφεύγει να χρησιμοποιεί αυτούς τους χρόνους. Αυτό συμβαίνει διότι τα switches που υποστηρίζουν το RSTP χρησιμοποιούν μηνύματα για να επικοινωνήσουν μεταξύ τους όταν υπάρχει αλλαγή στη τοπολογία του δικτύου. Αυτά τα μηνύματα κατευθύνουν τα switches να ξεφορτωθούν τις φυσικές διευθύνσεις που έχουν αποθηκεύσει στο πίνακα τους με τέτοιο τρόπο ώστε να αφαιρέσει όλες τις πιθανές εγγραφές που μπορεί να προκαλέσουν βρόχους, χωρίς να περιμένει κάποιο χρονικό

διάστημα. Ως αποτέλεσμα, το RSTP δημιουργεί περισσότερα σενάρια στα οποία μία πρώην απορριπτόμενη θύρα να μπορεί να μεταβάλει τη κατάσταση της σε κατάσταση forward αμέσως, χωρίς να περιμένει και χωρίς να χρειαστεί να περάσει από τη κατάσταση learning.[29]

### 3.3.6 RSTP PORT LINK TYPES

Μία ακόμη έννοια που περιέχει το RSTP σχετίζεται με κάποιους όρους που χρησιμοποιεί το πρωτόκολλο για να αναφερθεί σε διάφορα είδη θυρών και συνδέσεις, που συνδέουν τις θύρες αυτές.[29]

Τα switches σε ένα τοπικό δίκτυο μπορεί να συνδέονται με άλλα switches, με τερματικούς σταθμούς όπως υπολογιστές ή servers ή ακόμη και με hubs. Το RSTP θεωρεί τις συνδέσεις αυτές ως συνδέσεις από σημείο σε σημείο (point-to-point links) και τις θύρες που είναι συνδεδεμένες ως θύρες από σημείο σε σημείο (point-to-point ports) διότι οι συνδέσεις αυτές διασυνδέουν ακριβώς δύο συσκευές (points). Το RSTP επιπλέον ταξινομεί τις θύρες από σημείο σε σημείο σε δύο κατηγορίες. Οι θύρες από σημείο σε σημείο που διασυνδέουν δύο switches και δεν είναι ακριανά σημεία του δικτύου ονομάζονται απλά θύρες από σημείο σε σημείο. Αν όμως οι θύρες συνδέουν μόνο μία συσκευή (PC ή Server) στην άκρη του δικτύου, τότε οι θύρες ονομάζονται point-to-point edge ports ή πιο απλά edge ports.[29]

Αν μια θύρα λαμβάνει μηνύματα BPDUs τότε δεν μπορεί να είναι edge port. Οι edge ports μπορούν να μεταβούν σε κατάσταση forward αμέσως χωρίς να προκαλέσουν αλλαγή στη τοπολογία του δικτύου διότι η αλλαγή δεν επηρεάζει τα άλλα switches.[25] Η άμεση μετάβαση σε κατάσταση forward των θυρών των switches με το RSTP είναι πιθανή κάτω από ορισμένες συνθήκες:

- Η θύρα είναι Alternate Port (το τμήμα του τοπικού δικτύου στο οποίο είναι συνδεδεμένο μπορεί να είναι είτε από σημείο σε σημείο ή διαμοιραζόμενο).[25]
- Η θύρα είναι Designated Port και είναι συνδεδεμένη με κάποιο τμήμα του δικτύου από σημείο σε σημείο (και μπορεί να συνδεθεί το πολύ ακόμη ένα switch σε αυτό το τμήμα).[25]
- Η θύρα είναι Edge Port.[25]

Τέλος, το RSTP καθορίζει με τον όρο διαμοιραζόμενο (shared) για να περιγράψει τις θύρες που συνδέονται σε κάποιο hub. Ο όρος αυτός προήλθε από το γεγονός πως τα hubs δημιουργούν κοινής χρήσης δίκτυο Ethernet. Επίσης τα hubs εξαναγκάζουν το switch που είναι διασυνδεδεμένο πάνω του να χρησιμοποιεί ημι-αμφίδρομη λογική. Το RSTP θεωρεί πως όλες οι ημι-αμφίδρομες θύρες που μπορεί να συνδέονται σε hub, τις μεταχειρίζεται ως κοινόχρηστες θύρες (shared ports). Το RSTP συγκλίνει πιο αργά σε τέτοιου είδους θύρες σε σχέση με τις point-to-point ports.[29]

Στα σημερινά δίκτυα μεταγωγής, οι περισσότερες διασυνδέσεις λειτουργούν σε πλήρη διπλή κατεύθυνση και αντιμετωπίζονται από το RSTP ως συνδέσεις point-to-point.[25]

### 3.3.7 TOPOLOGY CHANGE PROCESS

Το RSTP μπορεί και χειρίζεται τις μεταβολές στην τοπολογία του δικτύου πολύ πιο αποτελεσματικά σε σχέση με το STP, το οποίο παράγει ειδοποιήσεις για τις αλλαγές που έχουν προκύψει στο τοπολογία σε δύο περιπτώσεις. Όταν μια θύρα μεταβεί στην κατάσταση forwarding ή όταν μια θύρα μεταβεί στην κατάσταση blocking ή down.[5]

Στο RSTP, αλλαγή της τοπολογίας συμβαίνει μόνο όταν μία θύρα που δεν είναι edge port μεταβεί στη κατάσταση forward. Επίσης, κάθε switch μπορεί να εντοπίσει αλλαγή στη τοπολογία, να δημιουργήσει και να προωθήσει TC BPDUs μηνύματα για να ενημερώσει τα γειτονικά switches για τις αλλαγές και να επιτευχθεί σύγκλιση πιο γρήγορα. Ωστόσο, μία χαλάρωση στη συνδεσιμότητα δεν θεωρείται ως αλλαγή τοπολογίας στο RSTP.[5]

Στη περίπτωση που ένα γειτονικό switch λάβει ένα TC BPDU μήνυμα, διαγράφει τη μνήμη των φυσικών διευθύνσεων σε όλες του τις θύρες εκτός της θύρας που δέχτηκε το TC BPDU μήνυμα και αποστέλλει το δικό του μήνυμα TC BPDU στο root port και σε όλες τις designated ports με αποτέλεσμα η ειδοποίηση για την αλλαγή της τοπολογία να εξαπλωθεί πολύ γρήγορα σε όλο το δίκτυο χωρίς να βασιστεί στο root switch. Επιπλέον, σε μια τέτοια περίπτωση, το RSTP επιτρέπει σε όλες τις θύρες που είναι alternate ports ή backup ports να μπουν σε κατάσταση forward.[25]

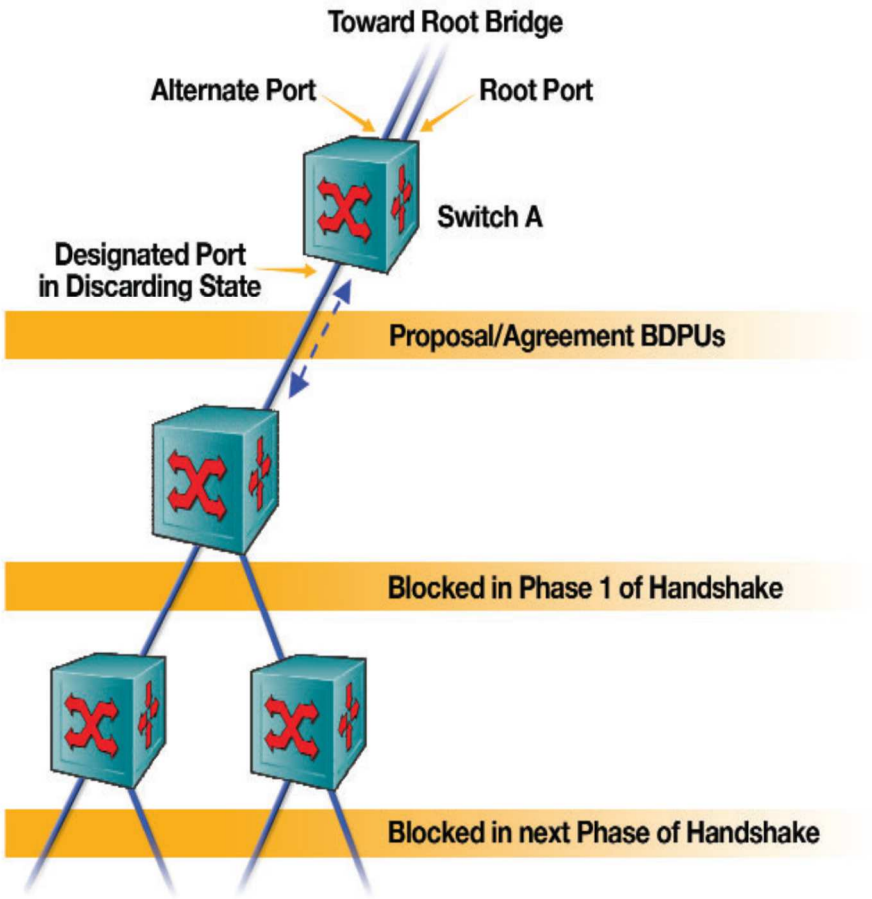
Η αντιμετώπιση των switches σε μια τέτοια ειδοποίηση είναι άμεση καθώς χρειάζονται μόλις μερικά hello times ώστε να διαγράψουν όλες τις διευθύνσεις που έχουν αποθηκεύσει στη μνήμη τους σε όλο το δίκτυο.[25]

### 3.3.8 RSTP CONVEGRENCE

Η σύγκλιση στο RSTP επιτυγχάνεται αμέσως και χωρίς χρονικούς περιορισμούς. Οι θύρες των switches μπορούν να μεταβαίνουν σε κατάσταση discarding χωρίς να υπάρχει το ρίσκο για δημιουργία βρόχων στο δίκτυο. Αφ' ετέρου, όμως η μεταβολή της κατάστασης των θυρών σε κατάσταση forwarding είναι πιο ριψοκίνδυνες διότι θα πρέπει να συμφωνούν με τις καταστάσεις των θυρών των γειτονικών switches.[25]

Το RSTP όπως έχουμε μπορεί να μεταβάλει μια alternate port σε κατάσταση forwarding αμέσως μόλις εντοπίσει βλάβη σε μια root port γιατί η μόνη αλλαγή που θα προκύψει στο δίκτυο και είναι αναγκαία, είναι διαγραφή των διευθύνσεων στο προς τα πάνω γειτονικό switch στο διάγραμμα του δέντρου.[25]

Για τη μεταβολή της κατάστασης όμως μιας designated port σε κατάσταση forwarding, η συμφωνία μεταξύ των ρόλων που θα έχουν οι θύρες ενός switch επιτυγχάνεται μέσω μιας ρητής "χειραψίας" μεταξύ των γειτονικών switches. Αυτή η διαδικασία της χειραψίας περιέχει τρία βήματα.




***Εικόνα 3.5:*** *Παράδειγμα της διαδικασίας handshake.*

Παρατηρούμε στην εικόνα 3.5, αρχικά ότι το switch A στέλνει μία αίτηση προς το από κάτω του, γειτονικό switch με τη μορφή ενός BPDU μηνύματος. Όταν το switch δεχτεί το μήνυμα τότε θα ελέγξει αν οι υπόλοιπες θύρες του συμφωνούν και είναι σε συντονισμό με τις θύρες του αποστολέα switch A. Οι θύρες είναι συντονισμένες όταν βρίσκονται σε κατάσταση discarding ή είναι edge ports. Αυτό σημαίνει πως το switch που δέχτηκε την αίτηση θα πρέπει να μεταβάλλει τη κατάσταση, των designated ports που είναι ήδη σε κατάσταση forward, σε κατάσταση discarding ή blocking. Αφού γίνει αυτό, θα στείλει ένα μήνυμα BPDU συμφωνίας πίσω στο switch A, και η αντίστοιχη θύρα θα μπει σε κατάσταση forward. Στη συνέχεια, το ενδιάμεσο switch θα ξεκινήσει τη διαδικασία χειραψίας με τα γειτονικά προς τα κάτω switches προκειμένου να επιχειρήσει να μεταβάλει τις designated ports από τη κατάσταση blocking σε κατάσταση forward. Η διαδικασία αυτή επαναλαμβάνεται σταδιακά και τμηματικά προς τα κάτω σύμφωνα με το διάγραμμα δέντρου εώς ότου φτάσει στο τέλος. Σε κάθε βήμα, η διαδικασία βεβαιώνει πως δεν προκύπτουν προσωρινοί βρόχοι καθώς οι θύρες σταδιακά μεταβαίνουν σε κατάσταση

forward. Όταν η διαδικασία φτάσει στο τέλος του δέντρου, τότε έχουμε πλήρης σύγκλιση χωρίς να περιμένουμε για τη λήξη των χρονομέτρων του πρωτοκόλλου όπως συμβαίνει στο STP.[25]

Τέλος το RSTP είναι συμβατό με το STP. Ωστόσο, αν ένα γειτονικό switch δεν ανταποκριθεί στη διαδικασία χειραψίας του RSTP, τότε η θύρα επανέρχεται πίσω στη μετάβαση καταστάσεων μέσω τις διαδικασίας του STP. Αν συμβεί κάτι τέτοιο, τότε η συγκεκριμένη θύρα χάνει όλα τα οφέλη του RSTP.[25]

## 3.3.9 ΤΡΟΠΟΙ ΕΠΙΤΑΧΥΝΣΗΣ ΧΡΟΝΟΥ ΣΥΓΚΛΙΣΗΣ

Σε αρκετά περιβάλλοντα, και σε ορισμένα τοπικά δίκτυα, τα 30 δευτερόλεπτα που απαιτούνται για τη σύγκλιση του STP είναι μη αποδεκτά και αποτελούν πρόβλημα για τη σωστή και γρήγορη λειτουργία του δικτύου. Η εταιρία CISCO για να βελτιώσει αυτή τη λειτουργία της σύγκλισης ανέπτυξε και πρόσθεσε στο STP μια σειρά από τρείς διαφορετικές λειτουργίες στα switches. Τη λειτουργία του PortFast, UplinkFast και BackboneFast.[5]

### *3.3.9.1 PORTFAST*

Εξ' ορισμού όλες οι θύρες ενός switch συμμετέχουν στη τοπολογία του STP. Αυτό περιλαμβάνει και οποιαδήποτε θύρα του switch συνδέει έναν εξυπηρετητή, όπως ένα σταθμό εργασίας. Η θύρα του εξυπηρετητή θα μεταδίδει πληροφορίες μέσω των καταστάσεων του STP. Ωστόσο, ο εξυπηρετητής δεν θα έχει συνδεσιμότητα με το δίκτυο για 30 δευτερόλεπτα όταν λειτουργήσει για πρώτη φορά.[5]

Αυτό δεν είναι ιδανικό όμως για τρεις λόγους. Πρώτον, οι χρήστες θα ενοχλούνται από τη αναμονή για τη σύνδεση τους στο δίκτυο. Δεύτερον, ένας εξυπηρετητής συχνά κάνει αίτηση για μία IP διεύθυνση δια μέσου του DHCP (Dynamic Host Configuration Protocol) κατά τη διάρκεια της εκκίνησης του. Αν μία θύρα του switch δεν μεταβεί γρήγορα στη κατάσταση forward αρκετά γρήγορα, η αίτηση του DHCP μπορεί να αποτύχει. Και τρίτον, οι συσκευές που ξεκινούν τη λειτουργία τους από το δίκτυο μπορεί επίσης να αποτύχουν στο να λειτουργήσουν σωστά ή και καθόλου. [5][6]

Η λειτουργία του PortFast, επιτρέπει στη θύρα του switch να προσπεράσει τη τυπική διαδικασία του STP για τη μεταβολή των καταστάσεων των θυρών. Η θύρα μεταβαίνει έτσι αμέσως από τη κατάσταση blocking σε forwarding χωρίς να περάσει από τις καταστάσεις listening και learning, εξαλείφοντας το χρονικό διάστημα της καθυστέρησης των 30 δευτερολέπτων. [29]

Παρ' όλα αυτά, στις θύρες που μπορούμε με σιγουριά και ασφάλεια να ενεργοποιήσουμε τη λειτουργία του PortFast είναι στις θύρες τις οποίες γνωρίζουμε πως δεν είναι συνδεδεμένες με κάποιο άλλο swtich, hub ή συσκευές που παίρνουν μέρος στο STP. Αλλιώς, υπάρχει μεγάλη πιθανότητα να δημιουργηθούν βρόχοι, και οι θύρες που βρίσκονται σε κατάσταση learning και listening θα αγνοήσουν αυτό το πρόβλημα. Είναι πιο συνετό να χρησιμοποιείται η λειτουργία αυτή για συνδέσεις μεταξύ τερματικών συσκευών. Αν ενεργοποιήσουμε τη λειτουργία σε θύρες που συνδέονται με τέτοιες συσκευές, με την εκκίνηση των συσκευών, θα μεταβούν σε κατάσταση forwarding και θα ξεκινήσουν τη προώθηση κίνησης αμέσως μόλις η κάρτα δικτύου της συσκευής είναι ενεργή. Διαφορετικά, χωρίς το PortFast, κάθε θύρα θα πρέπει να περιμένει την επιβεβαίωση του switch πως η συγκεκριμένη θύρα είναι designated port και μετά να περιμένει καθώς η διεπαφή βρίσκεται προσωρινά στις καταστάσεις learning και listening πριν μεταβεί στη κατάσταση forwarding. [29]

Η λειτουργία του PortFast είναι γνωστό χαρακτηριστικό για τις edge ports. Στη πραγματικότητα το RSTP ενσωματώνει αυτή την έννοια όπως έχουμε αναφέρει, αφού, από το σχεδιασμό του το πρωτόκολλο συγκλίνει γρήγορα στις θύρες που είναι point-to-point edge ports, προσπερνώντας γρήγορα τη κατάσταση learning, που συνάπτει με την ιδέα της εταιρίας CISCO που αρχικά είχε εισαχθεί με το PortFast. Στη πράξη, τα switches της εταιρίας CISCO ενεργοποιούν τις RSTP point-to-point edge ports με την ενεργοποίηση της λειτουργίας του PortFast. [29]

Η ενεργοποίηση της λειτουργίας αυτής σε κάποια θύρα δεν απενεργοποιεί το STP στη θύρα, αλλά επιταχύνει το χρόνο σύγκλισης του STP. Αν σε μια θύρα που έχει ενεργοποιηθεί η λειτουργία PortFast, λάβει ένα BPDU μήνυμα τότε θα μεταβεί στην αρχική κατάσταση της κανονικής λειτουργίας του STP.

Επίσης, το PortFast προσφέρει άλλο ένα πλεονέκτημα στο STP. Να θυμήσουμε πως όταν η θύρα ενός switch μεταβάλλει τη κατάστασης σε κάποια άλλη τότε το switch δημιουργεί και αποστέλλει ένα TCN BPDU. [5] Αυτό συμβαίνει ακόμη και αν η θύρα είναι συνδεδεμένη με κάποιον εξυπηρετητή. Βάζοντας σε λειτουργία για πρώτη φορά τον εξυπηρετητή θα προκαλέσει τη προώθηση

μηνυμάτων TCN BPDU προς το Root Switch, το οποίο θα απαντήσει με τη σειρά του με ένα Configuration BPDU μήνυμα. Αυτό θα συμβεί ακόμη και αν δεν υπάρχει κάποια τεχνική αλλαγή στη τοπολογία του δικτύου ούτε κάποια διακοπή λειτουργίας. Ωστόσο όμως όλα τα switches θα μειώσουν το CAM (Content Addressable Memory) χρονικό όριο στα 15 δευτερόλεπτα, διαγράφοντας τις φυσικές διευθύνσεις πολύ γρήγορα από το πίνακα τους. Αυτό θα αυξήσει την υπερχείλιση των πακέτων και θα μειώσει την αποδοτικότητα του δικτύου.[5]

Η λειτουργία του PortFast εξαλείφει την μη αναγκαία μετάδοση BPDU μηνυμάτων και την υπερχείλιση των πακέτων στο δίκτυο. Με την ενεργοποίηση της λειτουργίας σε κάποια θύρα δεν δημιουργούνται και δεν αποστέλλονται TCN BPDU μηνύματα.[5]

### *3.3.9.2 UPLINKFAST*

Η λειτουργία UplinkFast βοηθάει επίσης στην ταχύτερη σύγκλιση του STP σε περίπτωση όμως κάποιας αποτυχίας σε κάποια γραμμή σύνδεσης. Όπως και με τη λειτουργία του PortFast έτσι και με τη λειτουργία του UplinkFast θα πρέπει να είμαστε σίγουροι σε ποια ή ποιες θύρες των switches θα την ενεργοποιήσουμε. Το UplinkFast έχει σχεδιαστεί στο να λειτουργεί σε δίκτυα τα οποία περιέχουν switches που συνδέονται μεταξύ τους με δύο οι περισσότερες συνδέσεις και συνδέονται με κάποιον σταθμό εργασίας. Έχουν δηλαδή τουλάχιστον μία alternate port ή backup port. Γι' αυτό το λόγο συνιστάται να χρησιμοποιείται σε switches που έχουν θύρες σε κατάσταση blocking.[3]

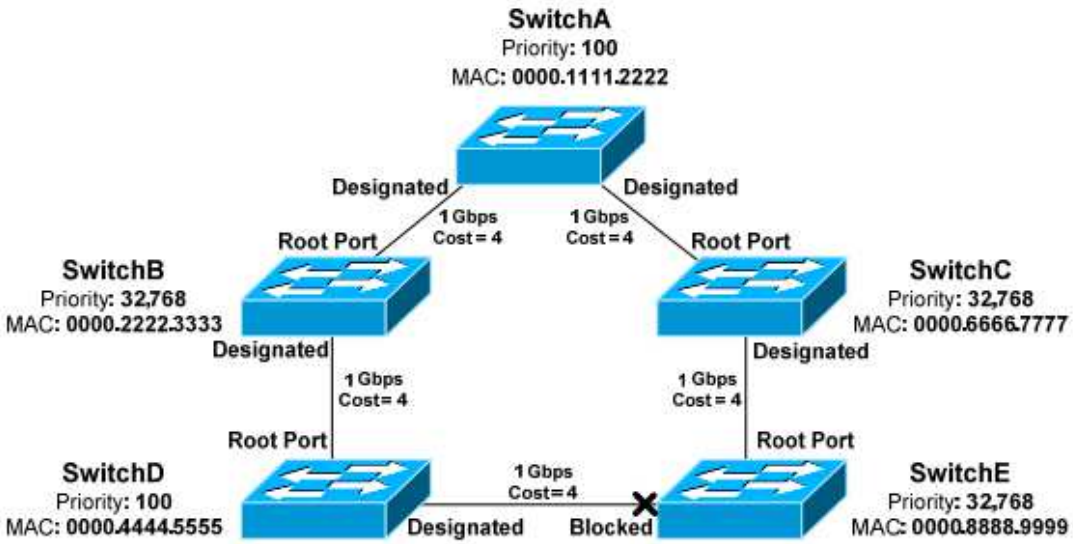
Το UplinkFast έχει την ιδιότητα να κρατάει σε κατάσταση αναμονής τις θύρες που βρίσκονται σε κατάσταση blocking ώστε αν η root port υποστεί βλάβη τότε να μπορεί η θύρα που είναι σε κατάσταση blocking να μεταβεί αμέσως στη κατάσταση forwarding ως εναλλακτική λύση. Επιπρόσθετα, το UplinkFast βελτιώνει το χρόνο σύγκλισης σε περίπτωση direct failure στη τοπολογία του STP. Αν υπάρχουν πολλαπλές θύρες σε κατάσταση blocking, θα μεταβεί σε κατάσταση forwarding η θύρα με το μικρότερο root path cost.[5]

Το UplinkFast είναι απενεργοποιημένο εξ' ορισμού. Μπορεί να το ενεργοποιήσει ο διαχειριστής του δικτύου αλλά μόνο αν γνωρίζει σίγουρα την τοπολογία των switches που συνδέονται με παραπάνω από μια συνδέσεις. Με την

ενεργοποίηση της λειτουργία του UplinkFast σε κάποιο switch αυξάνεται το switch priority σε 49,152. Η λειτουργία του UplinkFast δεν υποστηρίζεται από το Root Switch. [5]

### *3.3.9.3 BACKBONEFAST*

Η λειτουργία του BackboneFast σε αντίθεση με τη λειτουργία του UplinkFast, βοηθάει στη ταχύτερη σύγκλιση της τοπολογίας του STP σε περίπτωση indirect failure. Για να γίνει κατανοητή η λειτουργία του BackboneFast θα εξηγήσουμε στην εικόνα που ακολουθεί πως ενεργούν τα switches στα οποία έχει ενεργοποιηθεί η εξής λειτουργία.[3][5]




***Εικόνα 3.6:*** *Παράδειγμα λειτουργίας του BackboneFast.*

Ας υποθέσουμε ότι η σύνδεση μεταξύ των switchA και switchB καταρρέει. Τότε το switchD θα αναγκαστεί να υπολογίσει εκ νέου μία διαδρομή προς το switchA, που στη περίπτωση μας είναι το root switch, διαμέσου του switchD. Ωστόσο, το switchD θα πρέπει να περιμένει να λήξει το χρονικό όριο Max Age για να διαγράψει τις πληροφορίες των μηνυμάτων BPDUs που δέχεται από το ανώτερο switchB. Εξ' ορισμού αυτός ο χρόνος είναι 20 δευτερόλεπτα. Αφού περάσει ο χρόνος αυτός, τότε το switchD θα αρχίσει να στέλνει μηνύματα BPDUs προς το switchE υποστηρίζοντας πως αυτό είναι το root switch. Στη συνέχεια το switchE δέχεται ταυτόχρονα από το switchD και το switchC ξεχωριστά μηνύματα BPDUs και παίρνει

πληροφορίες για δύο root switches. Για να εξακριβώσει το switchE ποιο είναι το πραγματικό root switch αρχίζει να στέλνει μηνύματα του τύπου Root Link Queries (RLQs) προς το root switch. Τότε το switchA θα στείλει ως απάντηση ένα RLQ Reply. Αν το switchE λάβει από το root port του αυτό το μήνυμα τότε θα ξέρει πως αυτό το switch που γνώριζε από πριν ως root switch εξακολουθεί να είναι να το πραγματικό root switch και διαδρομή που ακολουθεί είναι σταθερή. Αν το λάβει από κάποια άλλη θύρα τότε το switch καταλαβαίνει πως η σύνδεση με τη διαδρομή προς το root switch έχει καταρρεύσει. Το χρονικό όριο Max Age λήγει απευθείας ώστε να επιτρέψει την εκλογή μιας καινούργιας root port. Έστω λοιπόν, πως το switchE δέχεται από το root port του το RLQ Reply, τότε θα μεταβάλει τη κατάσταση της θύρας που βρίσκεται σε κατάσταση blocked σε κατάσταση forwarding, έτσι ώστε να προωθήσει μηνύματα BPDUs προς το switchD και να το ενημερώσει για το ποιο είναι το πραγματικό root switch. [3][5]

Η λειτουργία λοιπόν του BackboneFast, αν είναι ενεργοποιημένη στα switches, επιτρέπει τη παράκαμψη του χρονικού ορίου Max Age μειώνοντας ουσιαστικά το χρόνο σύγκλισης από τα 50 δευτερόλεπτα στα 30 σε περίπτωση που συμβεί indirect failure. [8]

Η συγκεκριμένη λειτουργία θα πρέπει να ενεργοποιηθεί από τον διαχειριστή του δικτύου, σε όλα τα switches έτσι ώστε να λειτουργήσει σωστά.[5]

## 3.4 Per Vlan STP AND Per Vlan STP+

Με την εξέλιξη της τεχνολογίας και την εισαγωγή των Virtual LANs (VLANs) στα δίκτυα μεταγωγής, τα οποία χρησιμοποιούνται πλέον, για περαιτέρω υποδιαίρεση των μεταδιδόμενων ή ανεπαρκών τομέων, με σκοπό την απομόνωση της μεταδιδόμενης κίνησης βάση την ομάδα χρηστών ή τύπο εφαρμογής και να υποστηρίξει την εξισορρόπηση του φορτίου σε όλες τις περιττές συνδέσεις.

Το πρότυπο 802.1D (STP) σε συνδυασμό με το πρότυπο 802.1Q (vlans) θέτουν αυστηρούς περιορισμούς στη ποικιλομορφία των vlans που μπορεί να διαμορφωθεί. Πιο συγκεκριμένα, το STP υποθέτει πως θα πρέπει να υπάρχει μία μοναδική λογική τοπολογία στο δίκτυο μεταγωγής. Αυτό σημαίνει πως η χρήση του STP σε ένα δίκτυο όπου vlans επεκτείνονται σε πολλά switches χρησιμοποιώντας το

πρωτόκολλο πολλαπλών γραμμών (trunking protocol) όπως το 802.1Q προϋποθέτει πως όλα τα vlans μοιράζονται την ίδια τοπολογία. Με τον τρόπο αυτό μειώνεται ο βαθμός απομόνωσης της κίνησης δεδομένων που μπορούν να παρέχουν, και σπαταλούν εύρος ζώνης κατά τη διάρκεια της μετάδοσης και υπερχείλισης των πακέτων δεδομένων. Επιπλέον, η μοναδική τοπολογία εξαναγκάζει κάθε εφεδρική διαδρομή να είναι σε κατάσταση blocking για όλη τη διάρκεια της κίνησης δεδομένων, σπατάλη της χωρητικότητας του εύρους ζώνης που μπορεί να αποφευχθεί, αν πολλαπλές λογικές τοπολογίες μπορούν να συνυπάρχουν σε κάποιο δίκτυο μεταγωγής.[25]

Η έλλειψη για την επίγνωση των vlans οδήγησε στην ανάπτυξη ενός άλλου συνόλου κατοχυρωμένων βελτιώσεων, από τον οργανισμό IEEE και την εταιρία CISCO, για την επίγνωση των vlans στο STP, όπως το Per-Vlan Spanning Tree (PVST) και το PVST+ .[25]

### 3.4.1 PVST

Με το PVST μας επιτρέπεται να έχουμε στο δίκτυο μας αρκετές περιπτώσεις του STP που να εκτελούνται. Με την εκτέλεση διαφορετικής περίπτωσης του STP σε μια βάση ανά vlan, μπορούμε να τρέξουμε μερικά vlans σε θύρες που είναι σε κατάσταση blocking από κάποια άλλη περίπτωση του STP που τρέχει σε κάποιο άλλο vlan. Σε μια τέτοια περίπτωση, μπορούμε να ορίσουμε τη προτεραιότητα της κάθε θύρας σε κάθε βάση του vlan, επιτρέποντας μας να χρησιμοποιήσουμε τις εφεδρικές διαδρομές του δικτύου να τρέχουν ίδιο ποσό της κίνησης δεδομένων σε κάθε σύνδεση. Τα vlans ξεχωριστά καθορίζουν από ποιες συνδέσεις θα προωθήσουν κίνηση και ποιες θα μπλοκάρουν.[3][4]

Όπως με τον καθορισμό προτεραιότητας των θυρών, η θύρα με τη μικρότερη τιμή προτεραιότητας για κάθε vlan είναι αυτή που θα προωθεί τα πλαίσια. Αν δύο ή παραπάνω θύρες έχουν την ίδια τιμή προτεραιότητας για ένα συγκεκριμένο vlan, τότε η θύρα με τη χαμηλότερη τιμή θύρας θα προωθήσει τα πλαίσια για το vlan.[3]

Το PVST είναι μια ανεπτυγμένη λύση της εταιρίας CISCO για τα προβλήματα κλιμάκωσης και σταθερότητας που σχετίζονται με το STP σε μεγάλης κλίμακας δίκτυα που εκτείνονται στη τοπολογία μορφής δέντρου. Το PVST δημιουργεί μια ξεχωριστή περίπτωση του STP σε κάθε vlan στο τμήμα του switch. Αυτή η

εγκατάσταση δίνει σε κάθε vlan μία μοναδική τοπολογία του STP που περιέχει το δικό του κόστος θύρας, κόστος διαδρομής, προτεραιότητα και root switch.[3]

Χρησιμοποιώντας ξεχωριστές περιπτώσεις του PVST σε κάθε vlan, μειώνουμε το χρόνο σύγκλισης για τον υπολογισμό εκ νέου του STP και αυξάνουμε την αξιοπιστία του δικτύου. Με την εκτέλεση του PVST, το γενικό μέγεθος της τοπολογίας του STP μειώνεται σε σημαντικό βαθμό. Επιπλέον, βελτιώνει την κλιμάκωση και μειώνει το χρόνο σύγκλισης με αποτέλεσμα να παρέχει ταχύτερα την επαναφορά του δικτύου σε περίπτωση κατάρρευσης του δικτύου. Επιτρέπει επίσης, τον έλεγχο των διαδρομών που προωθούν κίνηση σε κάθε βάση υποδικτύου.[3]

Το PVST ωστόσο, δημιουργεί μειονεκτήματα στη τοπολογία του STP. Χρησιμοποιεί περισσότερη επεξεργαστική ισχύ και καταναλώνει περισσότερο εύρος ζώνης για να μπορεί να υποστηρίξει τη διατήρηση της τοπολογίας του STP και τα μηνύματα BPDUs για κάθε vlan διότι επιτρέπεται για κάθε vlan να έχουμε ένα root switch. Αυτό δίνει τη δυνατότητα στο STP να αξιοποιήσει με τον καλύτερο τρόπο την κίνηση δεδομένων για κάθε vlan επιτρέποντας να ρυθμίσουμε το root switch στο κέντρο του κάθε vlan.[3]

Με το PVST σημαίνει πως 1.000 vlans θα εκτελούν 1.000 διαφορετικές περιπτώσεις του STP. Λόγω της φύσης του, το PVST χρειάζεται τη χρήση συνδέσεων Cisco Inter-Switch Link (ISL) και κανάλια ενθυλάκωσης μεταξύ των switches. Σε δίκτυα που συνυπάρχουν το STP και το PVSTP, μπορεί να συμβούν προβλήματα διαλειτουργικότητας. Κάθε ένα από αυτά απαιτεί και διαφορετική μέθοδο ενθυλάκωσης έτσι ώστε τα μηνύματα BPDUs να μην ανταλάσονται ποτέ μετάξύ των τύπων του STP. Οι συνδέσεις ISL χρησιμοποιούν μια τοπολογία STP για κάθε vlan, χρησιμοποιώντας το PVST πάνω στα κανάλια του ISL. Επίσης το PVST λειτουργεί εξ' ορισμού στα switches της εταιρίας CISCO, το οποίο σημαίνει την επιλογή της καλύτερης δυνατής διαδρομής, συνεχίζοντας ο χρόνος σύγκλισης να είναι αργός.[3][25]

### 3.4.2 PVST+

Όσο αφορά τη τεχνολογία του PVST+ , η εταιρία CISCO, δεν έχει τεκμηριώσει πολύ ορθά τη λειτουργία της. Το πρότυπο 802.1Q μπορεί να χρησιμοποιήσει το PVST+ για να χαρτογραφήσει πολλαπλές τοπολογίες του STP στη

τοπολογία του αυθεντικού προτύπου 802.1Q που υποστηρίζουν τα switches. Ο τύπος σύγκλισης ταιριάζει αρκετά με το τύπο σύγκλισης του STP, που έχει μόνο μία περίπτωση του STP ανεξαρτήτως του αριθμό των vlan που υπάρχουν στο δίκτυο. Η διαφορά είναι πως με το PVST+, η σύγκλιση συμβαίνει σε κάθε βάση των vlan, με κάθε vlan να τρέχει τη δικιά του περίπτωση του STP, το οποίο μας δείχνει πως τώρα έχουμε μια αποτελεσματική εκλογή του root switch για κάθε vlan.[7]

Για να επιτραπεί στο PVST+ η λειτουργία, υπάρχει ένα πεδίο μέσα στα μηνύματα BPDUs που δέχεται το εκτεταμένο ID συστήματος (Extended System ID) ώστε το PVST+ να μπορεί να έχει ένα διαμορφωμένο root switch για κάθε περίπτωση του STP.[7]

Το PVST+ υποστηρίζει αποτελεσματικά τρεις ομάδες του STP που μπορούν να λειτουργούν σε ένα κοινό δίκτυο. Switches που υποστηρίζουν το PVST, PVST+ και το CST/MST πάνω στο πρότυπο IEEE 802.1Q μπορούν να επικοινωνούν και να δουλεύουν άρτια.[4]

Για να συμβεί αυτό, το PVST+ λειτουργεί ως μεταφραστής μεταξύ των switches που υποστηρίζουν το STP και των switches που υποστηρίζουν PVST. Το PVST+ μπορεί να επικοινωνήσει απευθείας με το με PVST μέσω των ISL καναλιών. Για να επικοινωνήσει με το STP όμως, το PVST+ ανταλλάζει μηνύματα BPDUs με το STP στο vlan 1. BPDUs από άλλα vlans εξαπλώνονται διαμέσου των STP τμημάτων του δικτύου από σήραγγες. Το PVST+ στέλνει αυτά τα BPDUs χρησιμοποιώντας μια μοναδική διεύθυνση πολλαπλής διανομής έτσι ώστε τα CST switches να προωθήσουν τα μηνύματα αυτά προς τα κατώτερα γειτονικά switches. Τελικά, τα tunneled BPDUs μηνύματα θα καταλήξουν σε άλλα PVST+ switches που θα τα καταλάβουν.[4]

## 3.5 MULTIPLE SPANNING TREE

Το Multiple Spanning Tree Protocol (MSTP) θεωρείται ως εξέλιξη του STP και του RSTP. Αρχικά τυποποιήθηκε ως πρότυπο IEEE 802.1s και αργότερα ενσωματώθηκε στο πρότυπο 802.1Q – 2005. Είναι εμπνευσμένο από την ονομασία που έδωσε η εταιρία CISCO, Multiple Instances Spanning Tree Protocol (MISTP).[10] Το MSTP αναπτύχθηκε έτσι ώστε να ξεπεραστούν τα προβλήματα που υπήρχαν σχετικά με την έλλειψη γνώσεων των vlans γύρω από STP και τις ανεπάρκειες του PVST. Δεδομένου πως ο αριθμός των διαφορετικών λογικών

τοπολογιών είναι πολύ μικρότερος σε σχέση με τον αριθμό των vlans, συγκριτικά, χρειάζονται λίγες μόνο περιπτώσεις RSTP. Για παράδειγμα, ένα τυπικό δίκτυο μπορεί να έχει ανάγκη από δύο περιπτώσεις του RST, όπου κάθε περίπτωση μπορεί να υποστηρίξει 2.048 vlans. Το MSTP επομένως απεικονίζει μια σημαντική βελτίωση των επεκτάσεων του STP που υποστηρίζουν ξεχωριστές περιπτώσεις του STP για κάθε vlan, και πιο συγκεκριμένα όταν το δίκτυο περιλαμβάνει πάρα πολλά vlans.[25]

### 3.5.1 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ MSTP

Για να μπορέσουν τα δίκτυα μεταγωγής επιπέδου 2 να υποστηρίξουν ένα εύρος ποικιλόμορφων vlans, το MSTP εισάγει την έννοια των περιοχών MST. Η περιοχή MST είναι μια ομάδα από switches που βρίσκονται κάτω από μια κοινή διαχείριση διαμοιρασμού ίδιων χαρακτηριστικών του vlan, όπως το όνομα διαμόρφωσης (32-byte), τον διαμορφωμένο αριθμό ενημέρωσης (16-byte), και ένα πίνακα διαμόρφωσης που περιέχει ως και 4.096 vlans, και τη σχέση τους με τις MST περιπτώσεις του RSTP. Επιπρόσθετα, το MST ορίζει ένα Internal Spanning Tree (IST), το οποίο είναι άλλη μία περίπτωση του RSTP που εκτείνεται σε όλα τα switches στη συγκεκριμένη περιοχή. Το IST είναι υπεύθυνο για την διατήρηση της τοπολογίας ολόκληρης της περιοχής και όλων των MSTIs. Κάθε MSTI χτίζει την δικιά του RSTP βάση τοπολογίας, εμπεριέχοντας και την εκλογή δικό του root switch. Ένα vlan μπορεί να αναθετηθεί σε μια περίπτωση. Το MSTP συνδέει όλες τις συσκευές και τοπικά δίκτυα με ένα Common Internal Spanning Tree (CIST) που υποστηρίζει αυτόματο σχηματισμό της κάθε MST περιοχής, και αναθέτει πακέτα σε διαφορετικά vlans να ακολουθήσουν διαφορετικές διαδρομές που βασίζονται σε διαφορετικά MSTs.[25]

Για τα περισσότερα συστήματα της εταιρίας CISCO, μία περιοχή μπορεί να περιέχει το μέγιστο 16 MSTIs (0-15). Εξ' ορισμού, όλα τα VLANs ανήκουν στη περίπτωση 0. Επίσης, και το IST σχεδιάζεται πάντα στη περίπτωση 0.[34]

Τα όρια τον περιοχών του MST καθορίζονται από της θύρες ορίων (Boundary Ports) που συνδέουν τις περιοχές μεταξύ τους. Οι θύρες ορίων γίνονται γνωστές μέσω ανταλλαγής μηνυμάτων BPDUs. Τα MST BPDUs περιέχουν το όνομα διαμόρφωσης, τον διαμορφωμένο αριθμό ενημέρωσης, και ένα πίνακα που περιλαμβάνει συνοπτικά τις πληροφορίες του συσχετισμένου vlan. Όταν δύο switches μεταξύ τους

διαφωνήσουν για κάποια από τις παραμέτρους διαμόρφωσης, τότε οι θύρες μεταξύ τους αναγνωρίζονται ως θύρες ορίων. Επίσης, αν δύο switches είναι διαμορφωμένα με διαφορετικές MST παραμέτρους τότε ανήκουν και σε διαφορετικές MST περιοχές. [25]

Οι περιοχές MST, συνδέονται μεταξύ τους μέσω του STP. Η περίπτωση του IST είναι απλά μία περίπτωση του RSTP που επεκτείνει το STP μέσα σε μια MST περιοχή. Κατά συνέπεια, η περίπτωση IST σε κάθε περιοχή δέχεται και στέλνει μηνύματα BPDUs προς το STP, και μπορεί να ενθυλακώσει πληροφορίες του MSTI μέσα στα μηνύματα BPDUs ως μία καταγραφή MST (MST record). Το IST αντιπροσωπεύει ολόκληρη τη MST περιοχή ως ένα μοναδικό εικονικό switch που παίρνει μέρος στο STP. Τα μηνύματα BPDUs των MST περιπτώσεων δεν προωθούνται από τις θύρες ορίων, αλλά μόνο τα STP BPDUs μηνύματα. [25]

Το MST είναι συμβατό με όλες τις εφαρμογές του STP. Αν μία MST περιοχή δεν είναι κατανοητή από switches που δεν υποστηρίζουν το MSTP, τότε θα αντιμετωπιστεί ολόκληρη η περιοχή ως μεμονωμένο STP switch ή ως RSTP switch. Αυτό συμβαίνει, διότι τα MST switches ακούν για τα μηνύματα STP BPDUs στις θύρες τους. Αν λάβουν μηνύματα τέτοιας μορφής, τότε οι θύρες χρησιμοποιούν συμπεριφορά του STP για να εξασφαλίσουν τη συμβατότητα.[25]

# 3.6 EXTENDED SYSTEM ID

Καθώς το STP εξελίχθηκε ώστε να είναι συμβατό και με τα VLANs, ένα μοναδικό Bridge ID έγινε υποχρεωτικό και για κάθε vlan. Αρχικά, αυτό επιτεύχθηκε εκχωρώντας μία μοναδική φυσική διεύθυνση του switch στο bridge ID κάθε vlan. Αυτή η προσέγγιση όμως υπέφερε αρκετά προβλήματα κλιμάκωσης, καθώς απαιτούσε πως ένα switch θα υποστηρίζει τουλάχιστον 1024 μοναδικές φυσικές διευθύνσεις συστήματος, μία για κάθε vlan.[5]

Το MSTP μετατρέπει το bridge ID ώστε να περιέχει ένα extended system ID, το οποίο αναγνωρίζει των αριθμό των vlans στις περιπτώσεις του STP. Το bridge ID παρέμεινε στα 64 bits, αλλά τώρα αποτελείται από 3 στοιχεία. Το bridge priority (4 bits), το system or vlan ID (12 bits) που μπορούμε να δούμε τη περιέχει λεπτομερώς μέσω μια εντολής εξόδου του STP, και τη MAC Address (48 bits). [5]

Παίρνοντας 12 bits από το bridge priority, το εύρος των προτεραιοτήτων αλλάζει. Το πραγματικό priority έχει εύρος από 0 – 65,535, με προεπιλεγμένη τιμή 32,768. Με τα extended system IDs, το νέο priority εύρος είναι από 0–61,440 και πρέπει να είναι κομμάτια πολλαπλάσια του 4,096, ενώ στο STP είχαμε ένα κομμάτι μόνο. Η προεπιλεγμένη τιμή παραμένει ίδια.[5]

Τέλος τα extended system IDs είναι ενεργοποιημένα από προεπιλογή και δεν μπορούν να απενεργοποιηθούν αν το switch δεν υποστηρίζει το σύστημα για 1024 φυσικές διευθύνσεις. Για τα switches που υποστηρίζουν το σύστημα αυτό το extended system ID μπορεί να ενεργοποιηθεί και χειροκίνητα. Τα extended system ID μπορεί να αυξήσει τον αριθμό των υποστηριζόμενων vlans για κάποια τοπολογία του STP από 1005 σε 4094.[5]

# 3.7 ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ STP

Το STP είναι ευάλωτο σε επιθέσεις για δύο λόγους. Πρώτον, διότι το STP δημιουργεί τη τοπολογία του βάση των μηνυμάτων BPDUs που ανταλλάζουν τα switches μεταξύ τους και δεύτερον το root switch καθορίζεται από τη χαμηλότερη του bridge ID. Ένα switch με χαμηλή τιμή προτεραιότητας μπορεί να είναι κακόβουλο ή κατά λάθος εγκατεστημένο σε ένα δίκτυο, και να εκλεγεί ως root switch. Αυτό έχει ως αποτέλεσμα το STP να συγκλίνει από την αρχή συχνά κάτι που οδηγεί σε ασταθής και μη βέλτιστη τοπολογία.[5]

Η εταιρία CISCO ενσωμάτωσε τρεις τρόπους αντιμετώπισης πιθανών επιθέσεων για την προστασία της τοπολογίας του STP. Το root guard, το BPDU guard και το BPDU filtering. Και οι τρεις μηχανισμοί μπορούν ρυθμιστούν σε κάθε θύρα των switches ξεχωριστά και είναι εξ’ ορισμού απενεργοποιημένοι. Ο διαχειριστής του δικτύου μπορεί να τους ενεργοποιήσει για την ορθή λειτουργία κατά των επιθέσεων.[5]

### 3.7.1 Root Guard

Το root guard προστατεύει το αυθεντικό root switch από την αντικατάσταση του με κάποιο κακόβουλο. Όταν ένα switch, στου οποίου τις θύρες έχει ενεργοποιηθεί η λειτουργία root guard, δεχτεί από ανώτερα μηνύματα από ένα κακόβουλο switch, τότε η λειτουργία της θύρα μπαίνει σε μια κατάσταση root-inconsistent state, με αποτέλεσμα να ενεργοποιείται η θέση του αυθεντικού root switch. Αφού μεταβεί στη κατάσταση root-inconsistent state που είναι παρόμοια με την κατάσταση listening, παύουν να μεταφέρονται δεδομένα μέσω της θύρας αυτής. Ωστόσο, αφού τελειώσει η ροή των μηνυμάτων BPDUs του κακόβουλου switch, η κατάσταση της θύρα θα επανέλθει στην αρχική της forwarding κατάσταση. Με άλλα λόγια η λειτουργία root guard στα Cisco switches εμποδίζουν την αλλαγή μιας designated port σε root port. Η λειτουργία αυτή μπορεί να ενεργοποιηθεί σε θύρες των switches που συνδέονται με άλλα switches και δεν προορίζονται να γίνουν ποτέ root switch. [30]

### 3.7.2 BPDU Guard

Η λειτουργία του BPDU Guard συνιστάται να ενεργοποιείται σε θύρες στις οποίες έχει ενεργοποιηθεί και η λειτουργία του portfast και σε switches που συνδέονται απευθείας με υπολογιστές. Αν μια θύρα ενός switch που έχει ενεργοποιημένες αυτές τις δύο λειτουργίες δεχτεί ένα μήνυμα BPDU, η κατάσταση της θύρα θα μεταβεί σε μια κατάσταση error disable state ή errdisable state ανεξαρτήτως αν το μήνυμα προέρχεται από κάποιο ανώτερο ή κατώτερο switch. Αυτό βοηθάει στην εμπόδιση του ενδεχομένου του διαχειριστή του δικτύου να συνδέσει κατά λάθος μια οποιαδήποτε θύρα ενός switch ή hub με κάποια θύρα ενός άλλου switch που έχει ενεργοποιημένη τη λειτουργία portfast. Έτσι προστατεύονται τα switches αλλά και το δίκτυο ολόκληρο. Η λειτουργία του BPDU μπορεί να ενεργοποιηθεί σε διαφορετικές θύρες ξεχωριστά ή και σε όλες τις θύρες μαζί που έχουν ενεργοποιημένη τη λειτουργία portfast. Μια θύρα μπορεί χειροκίνητα να επανακτηθεί από μια errdisable κατάσταση εκτελώντας τις εντολές shutdown και no shutdown.[5][29]

### 3.7.3 BPDU Filtering

Η λειτουργία του BPDU filtering επίσης χρησιμοποιείται σε συνδυασμό με τη λειτουργία portfast. Από τη στιγμή που μια θύρα με ενεργοποιημένη τη λειτουργία portfast εξακολουθεί να δέχεται μηνύματα BPDUs εξ' ορισμού, μπορούμε να χρησιμοποιήσουμε το BPDU filtering ώστε να σταματήσουμε οριστικά την μετάδοση ή την αποδοχή αυτών των μηνυμάτων από τη συγκεκριμένη θύρα. Αν λοιπόν έχουμε ενεργοποιήσει τη λειτουργία BPDU filtering σε όλο το δίκτυο τότε η θύρα που θα δεχτεί το μήνυμα BPDU, θα απενεργοποιηθεί αμέσως η λειτουργία του portfast στη θύρα και θα μεταβεί κανονικά σε κάποια κατάσταση μέσω των καταστάσεων του STP. Αν έχει ενεργοποιηθεί η λειτουργία BPDU filtering σε ξεχωριστές θύρες, μεμονωμένα τότε το εισερχόμενο BPDU μήνυμα απλά αγνοείται.[5]

Πρέπει να δοθεί ιδιαίτερη προσοχή όταν ενεργοποιούμε χειροκίνητα την λειτουργία BPDU filtering σε κάποια θύρα διότι η θύρα θα αγνοήσει το εισερχόμενο BPDU μήνυμα με αποτέλεσμα το STP να απενεργοποιηθεί στη θύρα. Η θύρα δεν θα βρίσκεται ούτε σε errdisable κατάσταση ούτε θα προχωρήσει μέσω της διαδικασίας του STP. Επομένως θα είναι ευπαθής σε βρόχους.[5]

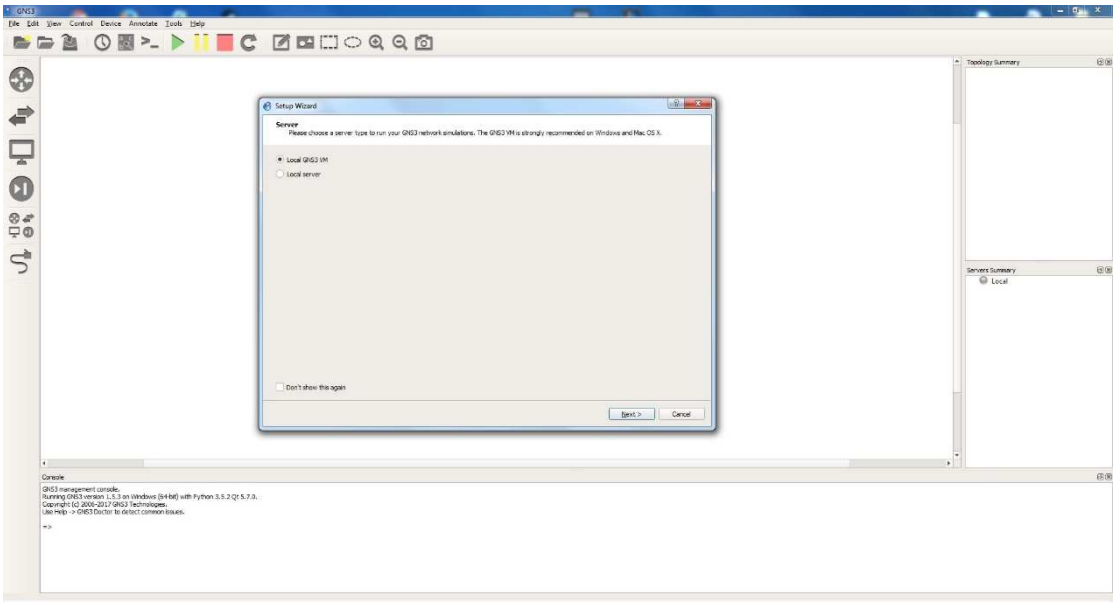
# ΚΕΦΑΛΑΙΟ 4

## 4.1 ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο θα ασχοληθούμε με προσομοιώσεις διαφορετικών περιπτώσεων διασύνδεσης μεταξύ των switches αναλύοντας πως εφαρμόζεται το STP σε ένα δίκτυο, πως αντιμετωπίζει το STP διάφορες αλλαγές που προκύπτουν στο δίκτυο, και τι πληροφορίες μας δίνει το STP για τα switches και το τοπικό δίκτυο μας. Για το σκοπό αυτό θα χρησιμοποιήσουμε το πρόγραμμα GNS3, για εκπαιδευτικούς σκοπούς, το οποίο είναι ένα πρόγραμμα προσομοιώσεων πολύπλοκων δικτύων που συνδυάζει εικονικές και πραγματικές συσκευές. Το GNS3 χρησιμοποιεί ένα πρόγραμμα εξομοιωτή που έχει γραφτεί για να εξομοιώνει τις δικτυακές συσκευές της εταιρίας Cisco. Στη δική μας περίπτωση θα χρησιμοποιήσουμε το EtherSwitch Router C3725 το οποίο περιέχει μέσα του και τις λειτουργίες ενός switch.

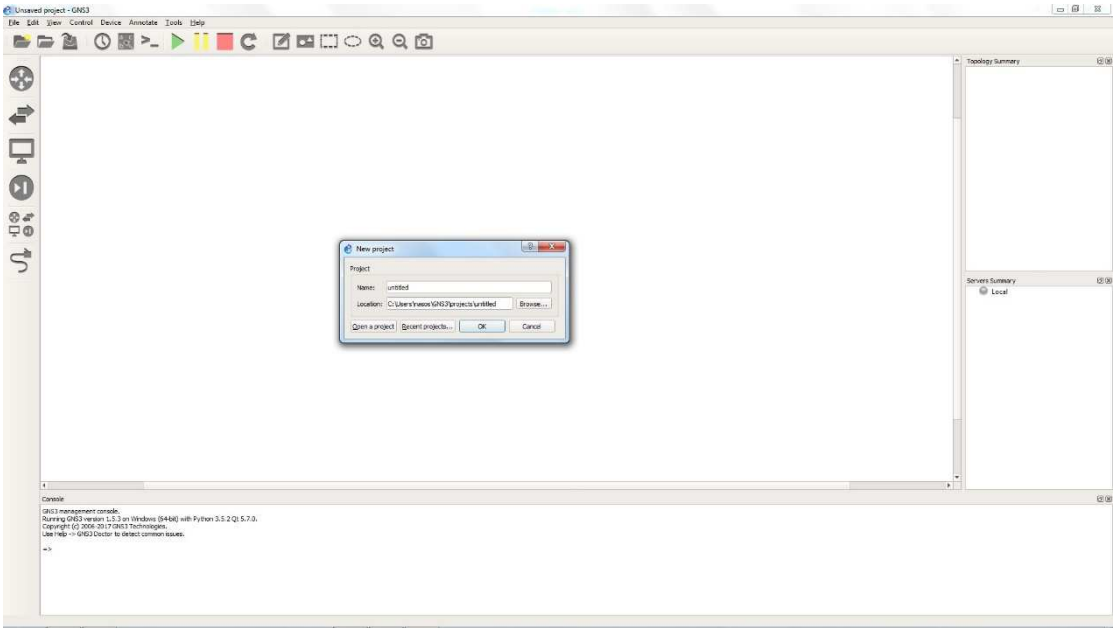
# 4.2 ΕΙΣΑΓΩΓΗ ΣΤΟ GNS3

Αφού εγκαταστήσουμε την εφαρμογή GNS3, κατά την εκτέλεση της θα μας ανοίξει το παρακάτω παράθυρο.




***Εικόνα 4.2.1:*** *Το περιβάλλον εργασίας του GNS3.*

Επιλέγουμε την επιλογή Cancel και στην συνέχεια μας εμφανίζει ένα άλλο παράθυρο για το αν θέλουμε να ανοίξουμε κάποιο υπάρχων project. Επιλέγουμε επίσης Cancel και συνεχίζουμε.

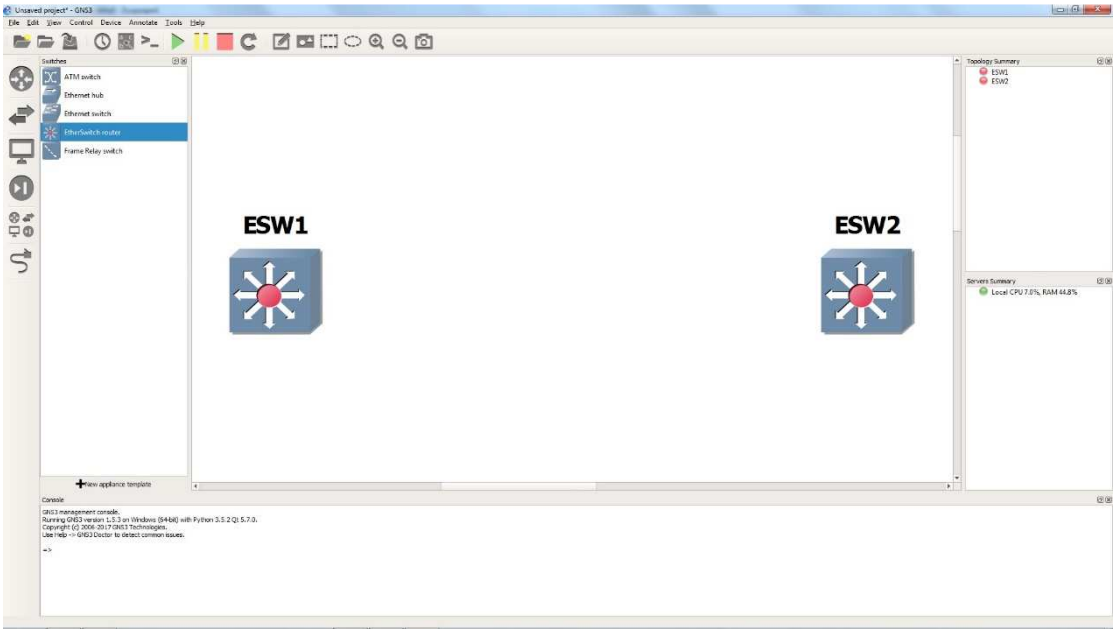


***Εικόνα 4.2.2:*** *Το περιβάλλον εργασίας του GNS3.*

Έχουμε μεταφερθεί πλέον στο κενό χώρο εργασίας του GNS3 και μπορούμε να προσθέσουμε τα στοιχεία που χρειαζόμαστε για να ετοιμάσουμε τη προσομοίωση που επιθυμούμε. Στα αριστερά μας υπάρχει ένα menu με έξι κατηγορίες.

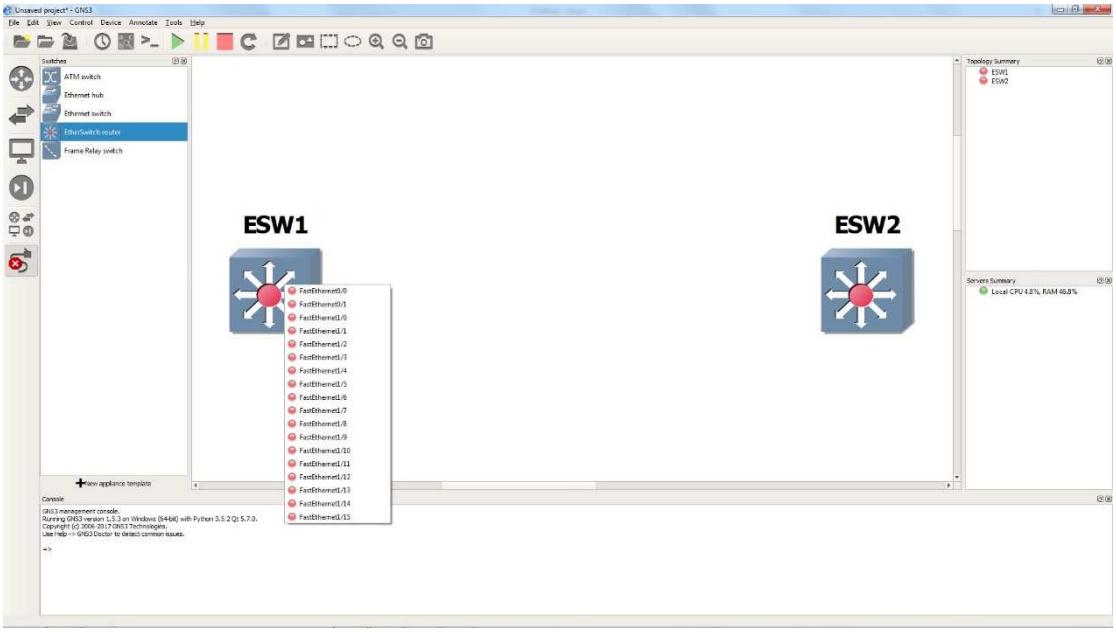
***Εικόνα 4.2.3****: Αντικείμενα προς χρήση σε κατηγορίες.*

Από τις κατηγορίες αυτές θα διαλέξουμε τη δεύτερη  που περιέχει τα δείγματα των switches. Από αυτή τη κατηγορία θα επιλέξουμε το EtherSwitch Router  και θα το τοποθετήσουμε στο περιβάλλον μας σύροντας το δύο φορές στο κενό χώρο εργασίας, διότι θα χρειαστούμε δύο switch σε αυτή τη περίπτωση.




***Εικόνα 4.2.4:*** *Αντικείμενα του παραδείγματος που θα χρησιμοποιηθούν.*

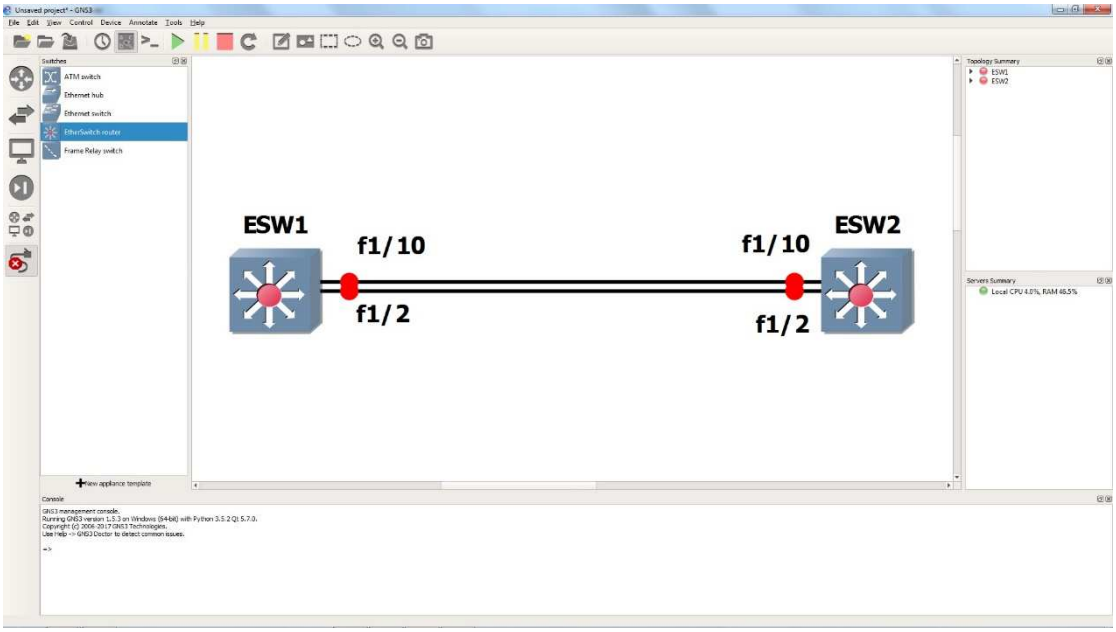
Αφού τοποθετήσαμε τα switches θα τα συνδέσουμε κάνοντας μια φορά κλικ στην έκτη επιλογή  από το menu στα αριστερά μας. Στη συνέχεια κάνοντας αριστερό κλικ και διαλέγοντας ένα από τα δύο switches θα μας εμφανιστεί μία λίστα από τις διεπαφές του switch ώστε να διαλέξουμε τις διεπαφές που θέλουμε να συνδέσουμε μεταξύ των switches.




***Εικόνα 4.2.5:*** *Οι διεπαφές ενός EtherSwitch Router C3725.*

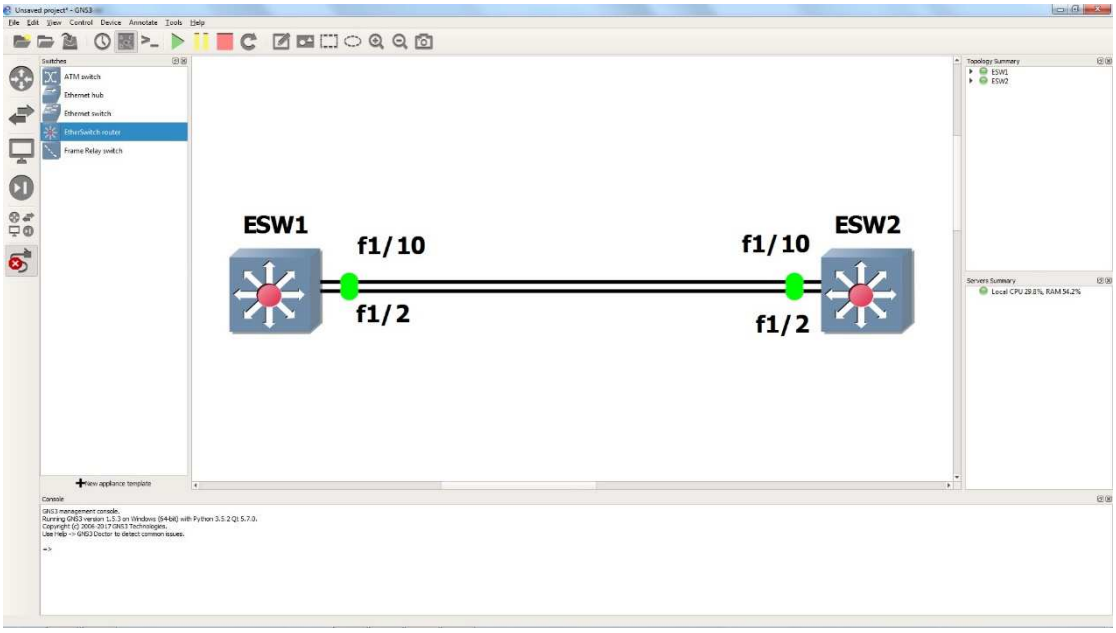
Οι διεπαφές έχουν μια αρίθμηση ώστε να ξεχωρίζουν σε περίπτωση πολλαπλών συνδέσεων. Για να εμφανίζεται η ονομασία και η αρίθμηση των διεπαφών σε κάθε σύνδεση στο χώρο εργασίας μπορείτε να επιλέξετε το κουμπί  που βρίσκεται κάτω από το κεντρικό μενού του προγράμματος.

Στη περιπτώση μας, τυχαία επιλέγουμε τη σύνδεση της διεπαφής f 1/2 του ESW1 με την διεπαφή f 1/2 του ESW2 και τη σύνδεση της διεπαφής f 1/10 του switch ESW1 με την διεπαφή f 1/10 του switch ESW2.




***Εικόνα 4.2.6:*** *Το δίκτυο του παραδείγματος.*

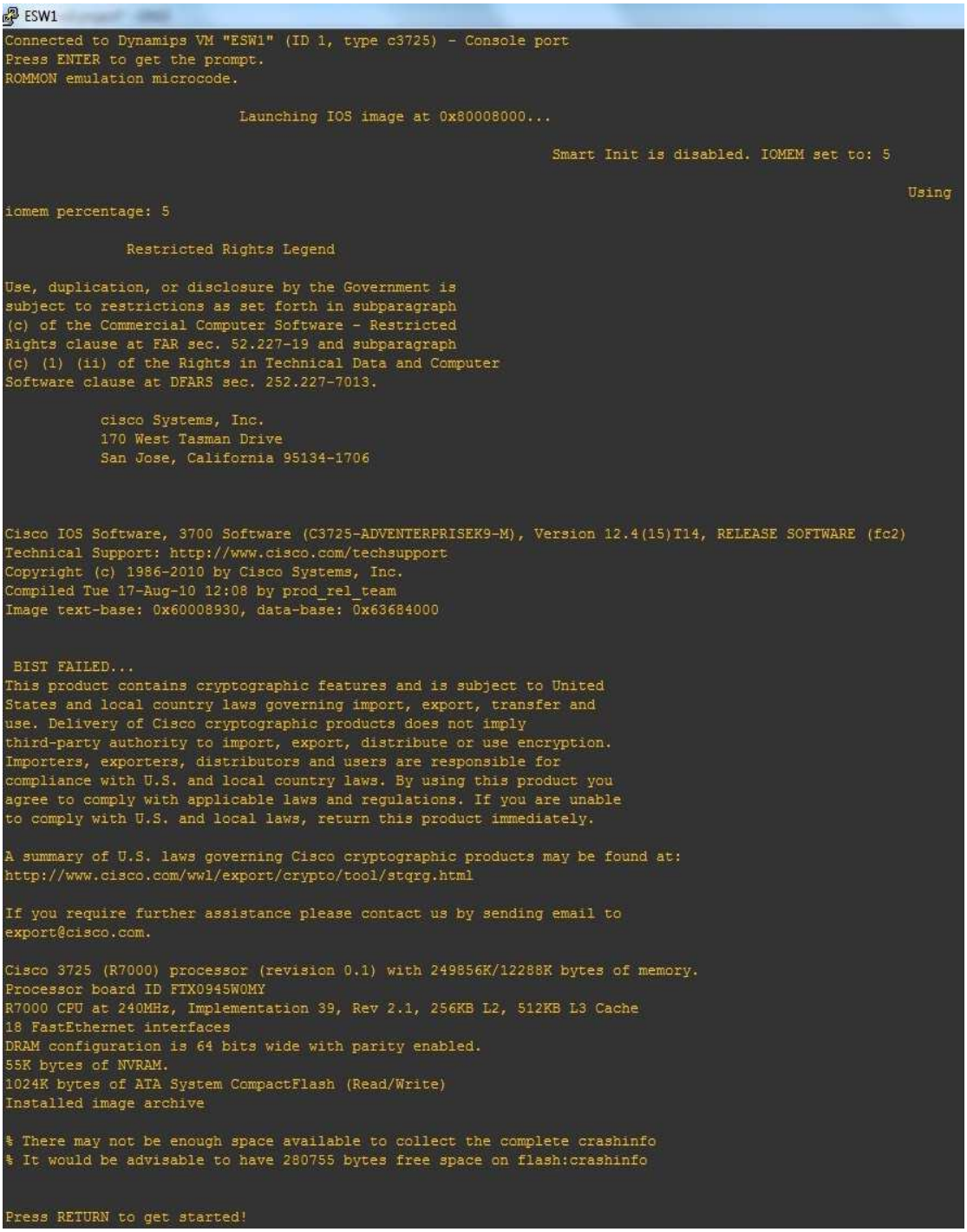
Παρατηρούμε πως μετά την σύνδεση των διεπαφών μεταξύ των δύο switches εμφανίζονται 4 κόκκινες κουκίδες δίπλα σε κάθε switch. Αυτό σημαίνει πως οι διεπαφές είναι εκτός λειτουργίας. Για να ενεργοποιήσουμε τις διεπαφές αρκεί να επιλέξουμε το κουμπί  που βρίσκεται επίσης κάτω από το μενού του προγράμματος. Αμέσως μόλις κάνουμε κλικ στο κουμπί μπορούμε να δούμε πως οι κουκίδες από κόκκινες έγιναν πράσινες που σημαίνει πως έχουν ενεργοποιηθεί.




***Εικόνα 4.2.7:*** *Ενεργοποίηση του δικτύου του παραδείγματος.*

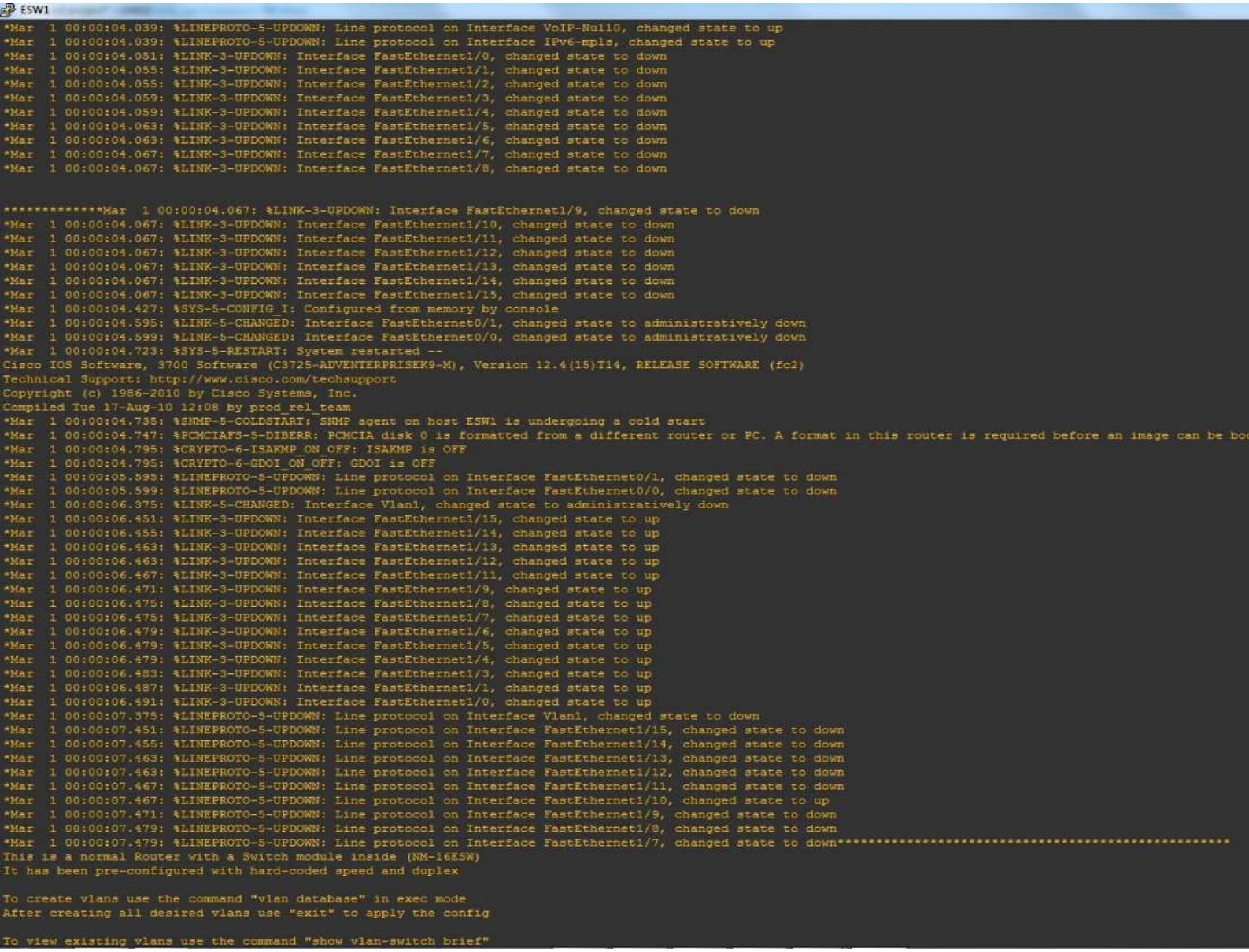
Για να τις απενεργοποιήσουμε ξανά, αν θέλουμε, μπορούμε να επιλέξουμε το κουμπί  .

Έχοντας συνδέσει τα switches κατάλληλα και έχουμε ενεργοποιήσει τις διεπαφές τους, μπορούμε πλέον, με διπλό κλικ σε ένα από τα δύο switches να μεταφερθούμε στο λειτουργικό τους σύστημα το οποίο ονομάζεται IOS. Όπως φαίνεται στις εικόνες 4.2.8 και 4.2.9 έχουμε μεταφερθεί στο λειτουργικό σύστημα του ESW1.




***Εικόνα 4.2.8:*** *Λειτουργικό Σύστημα του ESW1 του παραδείγματος.*

Στην εικόνα 4.2.8 φαίνονται τα νομικά δικαιώματα της εταιρίας Cisco, η έκδοση του λογισμικού που χρησιμοποιεί το EtherSwitch Router C3725 καθώς και τα τεχνικά χαρακτηριστικά του.




***Εικόνα 4.2.9:*** *Λειτουργικό Σύστημα του ESW1 του παραδείγματος.*

Στην εικόνα 4.2.9 φαίνονται οι καταστάσεις των διεπαφών του ESW1, αν είναι ενεργές ή όχι. Στην αρχή ενεργοποιούνται όλες οι διεπαφές και έπειτα απενεργοποιεί όσες δεν είναι συνδεδεμένές με άλλες διεπαφές και δεν χρησιμοποιούνται.

Παρόμοια στοιχεία θα εμφανιστούν στην περίπτωση που κάνουμε διπλό κλικ και ανοίξουμε το λειτουργικό σύστημα του ESW2.

# 4.3 ΠΡΟΣΟΜΟΙΩΣΗ 1

Στη πρώτη προσομοίωση που θα εκτελέσουμε, θα χρησιμοποιήσουμε το δίκτυο από το προηγούμενο παράδειγμα, που αποτελείται από δύο EtherSwitch Routers C3725, για να δείξουμε τα βασικά χαρακτηριστικά του STP ενός απλού δικτύου. Ωστόσο λόγω της έκδοσης λογισμικού του συγκεκριμένου μοντέλου χρησιμοποιεί αυτόματα και την έκδοση του STP, το PVST+ .

Έχοντας δει τα βασικά στοιχεία που μας είναι απαραίτητα στην εφαρμογή του GNS3, είμαστε πλέον σε θέση να επεξεργαστούμε τις ρυθμίσεις του ESW1 καθώς και να δούμε συγκεκριμένα στοιχεία του ή στοιχεία του δικτύου πληκτρολογώντας στην γραμμή prompt τις κατάλληλες εντολές.

Στη συγκεκριμένη περίπτωση, μας ενδιαφέρει να δούμε τις πληροφορίες του STP και τα στοιχεία των switches που συμμετέχουν στο STP.

Για να εμφανίσουμε λοιπόν, τα χαρακτηριστικά του STP για το ESW1 αρκεί να πληκτρολογήσουμε στη γραμμή prompt την εντολή «show spanning-tree brief» όπως φαίνεται στην εικόνα 4.3.1.

```
ESW1#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     c201.0d94.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c201.0d94.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- --------
FastEthernet1/2      128.43   128    19 FWD     0 32768 c201.0d94.0000 128.43
FastEthernet1/10     128.51   128    19 FWD     0 32768 c201.0d94.0000 128.51

ESW1#
```

***Εικόνα 4.3.1:*** *Εκτέλεση της εντολής show spanning-tree brief και τα αποτελέσματα για το ESW1.*

Τα αποτελέσματα που παίρνουμε από την εκτέλεση της εντολής μας αναφέρουν αναλυτικά τη κατάσταση του ESW1. Αρχικά, βλέπουμε πως το STP είναι ενεργοποιημένο εξ' ορισμού. Επίσης βλέπουμε πως ανήκει σε ένα Vlan με αριθμό ID

το 1. Αυτό οφείλεται στην έκδοση του λογισμικού του EtherSwitch που υποστηρίζει την έκδοση του STP, το PVST+. Στη συνέχεια φαίνονται αναλυτικά τα περιεχόμενα των πεδίων Root ID και Bridge ID.

Το Root ID είναι το Bridge ID του Root Switch. Περιέχει τη τιμή προτεραιότητας (Priority = 32,768) που είναι η προεπιλεγμένη τιμή για όλα τα cisco switches. Χρησιμοποιείται για την εκλογή του switch root και ακολουθείται από τη φυσική διεύθυνση του ESW1 (Mac Address : c201.0d94.0000). Έπειτα μας ενημερώνει πως το ESW1 είναι η ρίζα του STP.

Τέλος, μας εμφανίζει τρία χρονόμετρα, το Hello Time, το Max Age και το Forward Delay. Το Hello time είναι ίσο με δύο δευτερόλεπτα, που είναι η προεπιλεγμένη τιμή, και αναφέρεται στη συχνότητα αποστολής μηνυμάτων του switch root προς τα άλλα switches. Το Max Age είναι το χρονικό όριο που θέτει το root switch και έτσι ώστε να περιορίσει το χρονικό διάστημα για το οποίο θεωρείται έγκυρο το τελευταίο μήνυμα που έχει δεχτεί και μετά διαγράφεται. Η προεπιλεγμένη τιμή είναι 20 δευτερόλεπτα. Το Forward Delay, που είναι το χρονικό όριο για το οποίο τα switches θα πρέπει να περιμένουν πριν μεταβούν σε μια νέα κατάσταση αφού έχει προηγηθεί κάποια αλλαγή στη τοπολογία του δικτύου. Η προεπιλεγμένη τιμή είναι 15 δευτερόλεπτα.

Τα πεδία του Bridge ID όπως μπορούμε να παρατηρήσουμε είναι ακριβώς ίδια με τα πεδία του Root ID και αυτό οφείλεται στο ότι το ESW1 είναι το root switch. Τέλος το Aging Time είναι ο χρόνος που διαρκεί για να μάθει το switch τις φυσικές διευθύνσεις των τερματικών σταθμών ενός δικτύου. Αυτός ο χρόνος ισούται με 300 δευτερόλεπτα και είναι ο προεπιλεγμένος χρόνος.

Στη συνέχεια φαίνονται οι πληροφορίες για τις διεπαφές του ESW1. Το ESW1 όπως είχαμε δει στην εικόνα 4.2.6 συνδέεται με το ESW2 με δύο συνδέσεις. Το ίδιο, μας δείχνει και η εικόνα 3.10. Το ESW1 συνδέεται με το ESW2 μέσω των διεπαφών FastEthernet 1/2 και FastEthernet 1/10. Η διεπαφή FastErthernet 1/2 έχει ως αναγνωριστικό ταυτότητας τη τιμή 43, τιμή προτεραιότητας τη τιμή 128 που είναι η προεπιλεγμένη τιμή και κόστος διαδρομής ίσο με 19 αφού το εύρος ζώνης των διεπαφών είναι 100Mbps. Βρίσκεται σε κατάσταση forwarding που σημαίνει πως μπορεί να λαμβάνει και να μεταδίδει μηνύματα. Το designated cost είναι 0 αφού το ESW1 είναι το root switch και το κόστος διαδρομής επομένως προς τις designated ports του είναι 0. Τέλος ακολουθεί το αναγνωριστικό Bridge ID που όπως είπαμε

περιλαμβάνει τη τιμή προτεραιότητας ακολουθούμενη από τη φυσική διεύθυνση του ESW1.

Η διεπαφή FastErthernet 1/10 έχει ως αναγνωριστικό ταυτότητας τη τιμή 51, τιμή προτεραιότητας τη τιμή 128 που είναι η προεπιλεγμένη τιμή και κόστος διαδρομής ίσο με 19 αφού το εύρος ζώνης των διεπαφών είναι 100Mbps. Βρίσκεται σε κατάσταση forwarding που σημαίνει πως μπορεί να λαμβάνει και να μεταδίδει μηνύματα. Το designated cost είναι επίσης 0 αφού το ESW1 είναι το root switch και το κόστος διαδρομής επομένως προς τις designated ports του είναι 0. Τέλος ακολουθεί το αναγνωριστικό Bridge ID που περιλαμβάνει τη τιμή προτεραιότητας ακολουθούμενη από τη φυσική διεύθυνση του ESW1. Αυτά επομένως είναι τα στοιχεία για το ESW1.

Για να δούμε τα στοιχεία του ESW2 αρκεί να κάνουμε διπλό κλικ πάνω στο ESW2 ώστε να μετακινηθούμε στο λειτουργικό σύστημα του και να πληκτρολογήσουμε ξανά στη γραμμή prompt την εντολή «show spanning-tree brief» όπως φαίνεται στην εικόνα 4.3.2.

```
ESW2#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     c201.0d94.0000
              Cost        19
              Port        43 (FastEthernet1/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c202.1450.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/2      128.43   128    19 FWD     0 32768 c201.0d94.0000 128.43
FastEthernet1/10     128.51   128    19 BLK     0 32768 c201.0d94.0000 128.51

ESW2#
```

***Εικόνα 4.3.2:*** *Εκτέλεση της εντολής show spanning-tree brief και τα αποτελέσματα για το ESW2.*

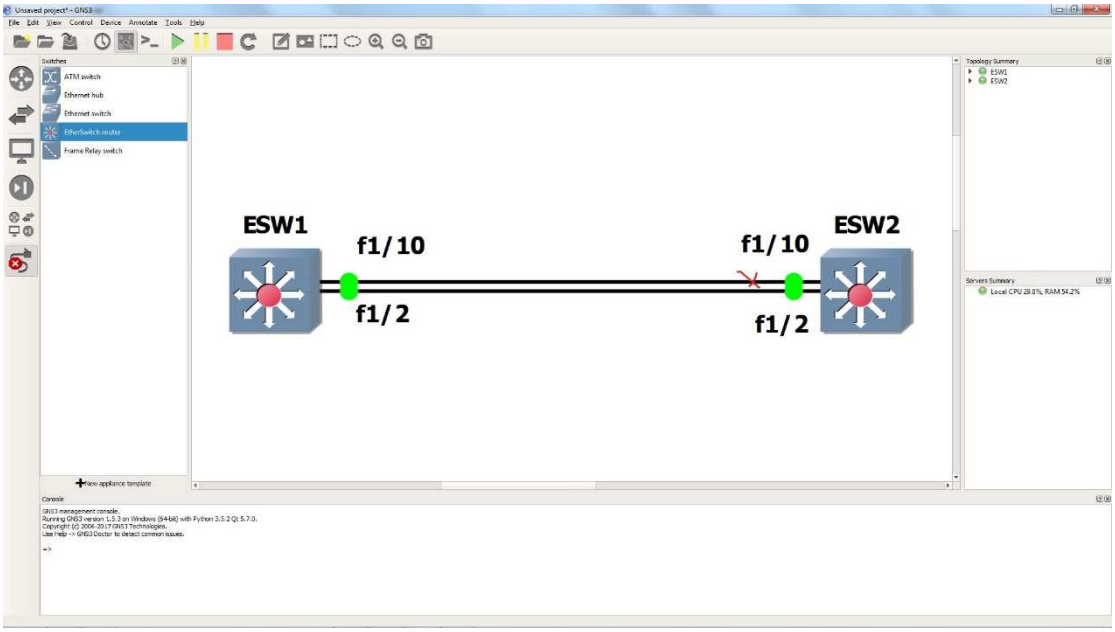
Παρατηρούμε πως οι πληροφορίες που παίρνουμε για το ESW2 είναι παρόμοιες με τις πληροφορίες του ESW1. Αρχικά, βλέπουμε πως και στο ESW2 είναι ενεργοποιημένο το STP εξ' ορισμού. Στο πεδίο Root ID έχουμε τις ίδιες τιμές για τη

προτεραιότητα και για τη φυσική διεύθυνση του Root Switch. Επιπλέον, τώρα μας εμφανίζει το κόστος διαδρομής προς το Root Switch που είναι 19 λόγο του εύρους ζώνης των διεπαφών. Επίσης, μας δείχνει με ποια θύρα του ESW1 είναι συνδεδεμένο το ESW2 και τον αριθμό της διεπαφής. Παρ' όμοια με το ESW1 έχουμε τους χρόνους Hello Time, Max Age και Forward Delay που είναι κοινοί για όλα τα switches και προεπιλεγμένοι.

Το πεδίο Bridge ID περιλαμβάνει τη προεπιλεγμένη τιμή προτεραιότητας του ESW2 που είναι ίδια με αυτή του ESW1 καθώς και τη φυσική του διεύθυνση. Παρατηρούμε πως η φυσική διεύθυνση του ESW2 είναι μεγαλύτερη σε σύγκριση με τη φυσική διεύθυνση του ESW1 και για αυτό το λόγο εκλέχτηκε το ESW1 ως Root Switch. Οι χρόνοι Hello Time, Max Age και Forward Delay είναι κοινοί με το ESW1.

Έπειτα βλέπουμε τις ονομασίες των διεπαφών και τις πληροφορίες τους. Για την διεπαφή FastEthernet 1/2 του ESW2 παρατηρούμε πως ισχύουν οι ίδιες τιμές και χαρακτηριστικά όπως και στο ESW1. Για την διεπαφή FastEthernet 1/10 του ESW2 επίσης όλα τα χαρακτηριστικά και οι τιμές είναι ίδιες με αυτά του ESW1 εκτός από τη κατάσταση στην οποία βρίσκεται η διεπαφή. Η θύρα βρίσκεται σε κατάσταση blocking. Δηλαδή, δεν μπορεί να δεχτεί δεδομένα από το ESW1, ούτε να μεταδώσει προς το ESW1. Επίσης δεν μπορεί να προσθέσει τις φυσικές διευθύνσεις από τερματικούς σταθμούς στο πίνακα διευθύνσεων του ESW2.

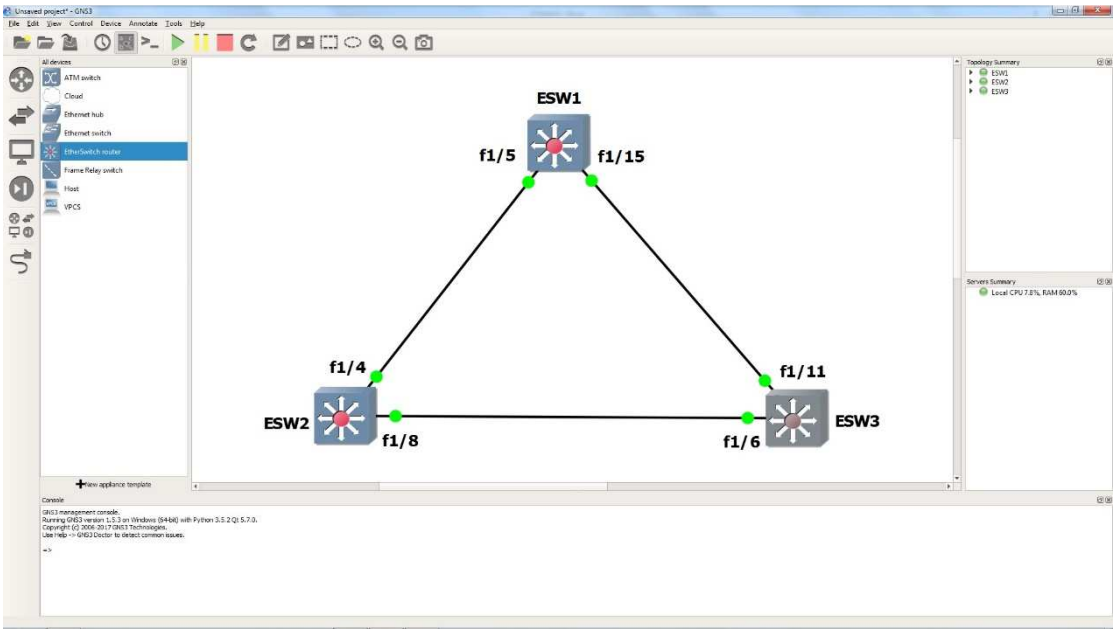
Συμπεραίνουμε λοιπόν, πως παρόλο που έχουμε συνδέσει δύο switches μεταξύ τους, με δύο διασυνδέσεις, το STP εφαρμόζεται από μόνο του, και μπλοκάρει τη μία εκ των δύο συνδέσεων μεταξύ τους όπως φαίνεται στην εικόνα 4.3.3, διότι την θεωρεί ως επιπλέον σύνδεση και την κρατάει ως εφεδρική σε περίπτωση που αυτή η ενεργή σύνδεση μεταξύ των switch υποστεί κάποια βλάβη.




***Εικόνα 4.3.3:*** *Κατάσταση διεπαφής f1/10 του ESW2.*

# 4.4 ΠΡΟΣΟΜΟΙΩΣΗ 2

Στη δεύτερη προσομοίωση θα χρησιμοποιήσουμε τρία EtherSwitch Router C3725, θα τα συνδέσουμε μεταξύ τους και θα δείξουμε πως μπορούμε να αλλάξουμε τις τιμές προτεραιότητας σε κάθε switch, και πώς αυτές οι αλλαγές επηρεάζουν την εκλογή του root switch στο STP.




***Εικόνα 4.4.1:*** *Κύκλωμα δεύτερης προσομοίωσης.*

Όπως βλέπουμε στην εικόνα 4.4.1, έχουμε προσθέσει στο χώρο εργασίας του GNS3 τρία EtherSwitch Routers τύπου C3725, το ESW1, το ESW2 και το ESW3 που είναι συνδεδεμένα σε μορφή τριγώνου. Το ESW1 συνδέεται με το ESW2 μέσω της διεπαφής f1/5 και με το ESW3 μέσω της διεπαφής f1/15. Το ESW2 συνδέεται με το ESW1 μέσω της διεπαφής f1/4 και με το ESW3 μέσω της διεπαφής f1/8. Το ESW3 συνδέεται με το ESW1 μέσω της διεπαφής f1/11 και με το ESW2 μέσω της διεπεφής f1/6. Παρατηρούμε πως όλες οι διεπαφές είναι ενεργές οπότε μπορούμε να συνεχίσουμε στην εκτέλεση της προσομοίωσης.

Μεταβαίνοντας στο λειτουργικό σύστημα σε κάθε switch, θα εκτελέσουμε την εντολή «show spanning-tree brief» για να δούμε ποιό είναι το root switch, αν συμφωνούν τα υπόλοιπα switches με την εκλογή του root switch και στη συνέχεια θα συγκρατήσουμε τις τιμές των προτεραιοτήτων τους καθώς και τις φυσικές διευθύνσεις τους ώστε να δούμε με ποιο κριτήριο εκλέχτηκε το root switch και έπειτα

θα επεξεργαστούμε τις τιμές αυτές, έτσι ώστε εσκεμμένα να αναγκάσουμε τα switches να προχωρήσουν σε μια νέα εκλογή του root switch.

Τα στοιχεία του ESW1 φαίνονται στην εικόνα 4.4.2

```
ESW1#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     c203.1144.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c203.1144.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/5      128.46   128    19 FWD     0 32768 c203.1144.0000 128.46
FastEthernet1/15     128.56   128    19 FWD     0 32768 c203.1144.0000 128.56

ESW1#
```

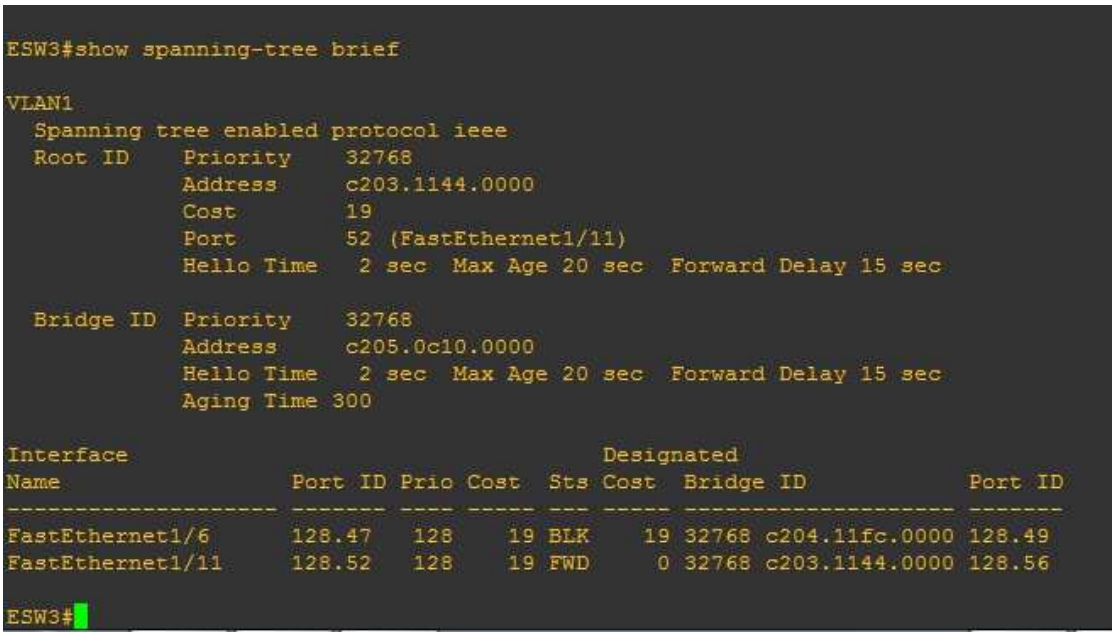
***Εικόνα 4.4.2:*** *Αποτελέσματα εντολής για το ESW1.*

Τα στοιχεία του ESW2 φαίνονται στην εικόνα 4.4.3.

```
ESW2#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     c203.1144.0000
              Cost        19
              Port        45 (FastEthernet1/4)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c204.11fc.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/4      128.45   128    19 FWD     0 32768 c203.1144.0000 128.46
FastEthernet1/8      128.49   128    19 FWD    19 32768 c204.11fc.0000 128.49

ESW2#
```

***Εικόνα 4.4.3:*** *Αποτελέσματα εντολής για το ESW2.*

Τα στοιχεία του ESW3 φαίνονται στην εικόνα 4.4.4.




***Εικόνα 4.4.4:*** *Αποτελέσματα εντολής για το ESW3.*

Από τα αποτελέσματα στις εικόνες παρατηρούμε πως το ESW1 είναι το root switch. Εκλέχτηκε σύμφωνα με το μέγεθος της φυσικής του διεύθυνσης λόγω του ότι και τα τρία switches έχουν την ίδια τιμή προτεραιότητας. Έχει τη μικρότερη φυσική διεύθυνση και συμφωνούν τα υπόλοιπα switches ως προς την εκλογή του root switch.

***Πίνακας 4.4.1:*** *Συγκεντρωτικά στοιχεία των βασικών χαρακτηριστικών των switches.*

| SWITCH | MAC ADDRESS | PRIORITY |
|---|---|---|
| ESW1 | c203.1144.0000 | 32768 |
| ESW2 | c203.11fc.0000 | 32768 |
| ESW3 | c205.0c10.0000 | 32768 |

Έχοντας συγκεντρώσει τα στοιχεία που αφορούν στην εκλογή του root switch, μπορούμε να επηρεάσουμε την εκλογή και να αναγκάσουμε ένα από τα τρία switches της επιλογής μας, να γίνει το root switch, αφού αλλάξουμε τη τιμή της προτεραιότητας πρώτα. Για να το επιτύχουμε αυτό χρειάζεται να μπούμε αρχικά στο λογισμικό του ESW2 ή του ESW3 και στη συνέχεια να μπούμε σε κατάσταση διαμόρφωσης της συσκευής. Έστω πως επιλέγουμε να κάνουμε το ESW3 root switch, και να αλλάξουμε τη τιμή προτεραιότητας του. Αφού μπούμε στο λογισμικό του, γράφοντας στη γραμμή prompt την εντολή «configure terminal» μπαίνουμε αμέσως στην κατάσταση διαμόρφωσης της συσκευής. Με το που εισέλθουμε σε αυτή

τη κατάσταση μας ενημερώνει το λογισμικό πως οι εντολές που θα χρησιμοποιηθούν θα πρέπει να γράφονται και να εκτελούνται ανά γραμμή, και για την έξοδο της κατάστασης αυτής θα πρέπει να πληκτρολογήσουμε την εντολή «exit» ή πατώντας τα πλήκτρα Ctrl+Z όπως θα δείτε στην εικόνα που ακολουθεί.

```
ESW3#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

***Εικόνα 4.4.5:*** *Εκτέλεση εντολής config terminal και αποτελέσματα.*

Στη συνέχεια για να δούμε το εύρος ζώνης της προτεραιότητας σε περίπτωση που δεν το θυμόμαστε ή δεν το γνωρίζουμε μπορούμε να χρησιμοποιήσουμε την εντολή «spanning-tree vlan 1 priority ?». Με τη χρήση του «?» θα μας εμφανίσει το εύρος ζώνης των τιμών που μπορούμε να δώσουμε στην τιμή της προτεραιότητας. Εάν δεν θέλουμε να εμφανίσουμε το εύρος ζώνης των τιμών αλλά θέλουμε απευθείας να εκχωρήσουμε μια τιμή μπορούμε να το κάνουμε με τη χρήση κάποιας τιμής, που να ανήκει στο εύρος ζώνης των τιμών που μπορεί να δεχτεί, στη θέση του «?».

```
ESW3(config)#spanning-tree vlan 1 priority ?
  <0-65535>  bridge priority

ESW3(config)#spanning-tree vlan 1 priority 10000
ESW3(config)#exit
ESW3#
*Mar  1 01:20:13.371: %SYS-5-CONFIG_I: Configured from console by console
ESW3#
```

***Εικόνα 4.4.6:*** *Εμφάνιση εύρους ζώνης τιμών προτεραιότητας, εκχώρηση τιμής προτεραιότητας και έξοδος από τη κατάσταση διαμόρφωσης συσκευής.*

Από την εικόνα 4.4.6 διαπιστώνουμε πως το εύρος ζώνης των τιμών είναι από το 0-65535 όπως είχαμε αναφέρει στο κεφαλαίο 2. Πλέον του έχουμε δώσει τη τιμή προτεραιότητας 10000, και επιστρέφοντας στην κατάσταση που μπορούμε να εκτελέσουμε και να δούμε κάποιες ρυθμίσεις βλέπουμε πως έχει γίνει η αλλαγή σωστά. Αν είχαμε δώσει κάποια τιμή εκτός του εύρους ζώνης των επιτρεπόμενων τιμών θα εμφανιζόταν στην οθόνης μας το εξής αποτέλεσμα της εικόνας 4.4.7 πως δεν είναι έγκυρη η τιμή. και θα έπρεπε να ξαναγράψουμε την εντολή με κάποια τιμή εντός του εύρους ζώνης. Επίσης θα εκτελέσουμε ακόμη μια φορά την εντολή « show spanning-tree brief» για να ελέγξουμε αν όντως έγινε η αλλαγή στη τιμή

προτεραιότητας του ESW3 και αν όντως καταφέραμε να επηρεάσουμε την εκλογή του root switch.

```
ESW3#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ESW3(config)#spanning-tree vlan 1 priority 99999
                                            ^
% Invalid input detected at '^' marker.

ESW3(config)#
```

***Εικόνα 4.4.7:*** *Αποτέλεσμα εκχώρησης μη έγκυρης τιμής προτεραιότητας.*

```
ESW3#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    10000
              Address     c205.0c10.0000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    10000
              Address     c205.0c10.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- --------
FastEthernet1/6      128.47   128    19 FWD     0 10000 c205.0c10.0000 128.47
FastEthernet1/11     128.52   128    19 FWD     0 10000 c205.0c10.0000 128.52

ESW3#
```

***Εικόνα 4.4.8:*** *Εμφάνιση στοιχείων του ESW3.*

Από την εικόνα 4.4.8, πράγματι βλέπουμε πως έχει εκχωρηθεί η τιμή 10000 στη τιμή προτεραιότητας, και έχουμε καταφέρει να επηρεάσουμε την εκλογή του root switch και να αναγκάσουμε το STP να εκλέξει ένα switch της επιλογής μας ως root switch και στο οποίο συμφωνούν και τα άλλα δύο switches βλέποντας τις επόμενες εικόνες.

```
ESW1#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    10000
              Address     c205.0c10.0000
              Cost        19
              Port        56 (FastEthernet1/15)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c203.1144.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/5      128.46   128    19 FWD    19 32768 c203.1144.0000 128.46
FastEthernet1/15     128.56   128    19 FWD     0 10000 c205.0c10.0000 128.52

ESW1#
```

***Εικόνα 4.4.9:*** *Εμφάνιση στοιχείων του ESW1.*

```
ESW2#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    10000
              Address     c205.0c10.0000
              Cost        19
              Port        49 (FastEthernet1/8)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c204.11fc.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/4      128.45   128    19 BLK    19 32768 c203.1144.0000 128.46
FastEthernet1/8      128.49   128    19 FWD     0 10000 c205.0c10.0000 128.47

ESW2#
```

***Εικόνα 4.4.10:*** *Εμφάνιση στοιχείων του ESW2.*

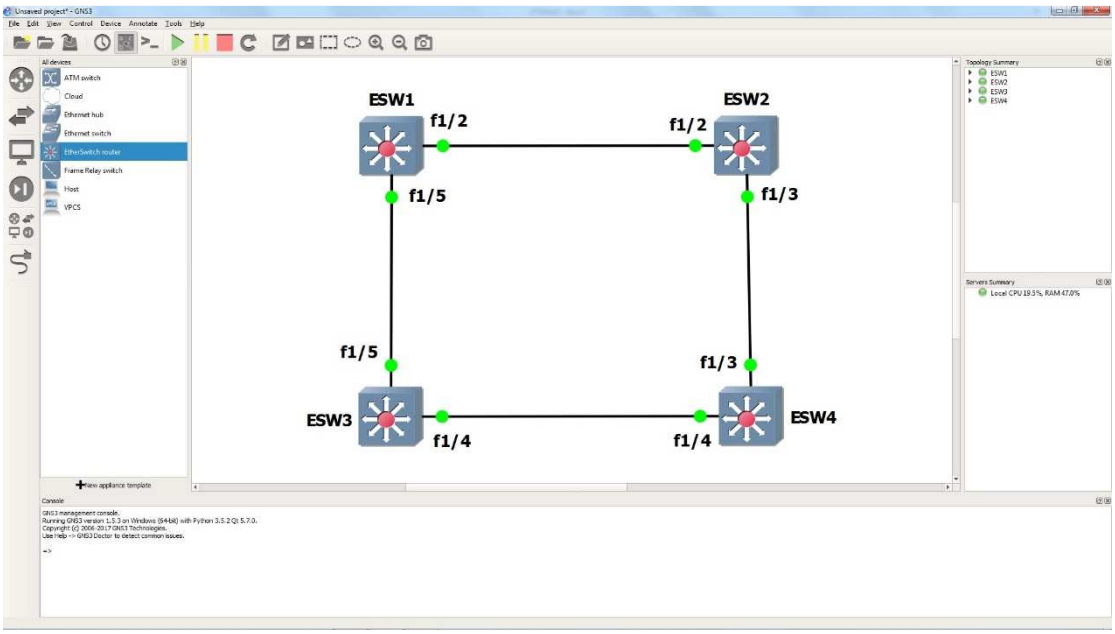
Τέλος, με την παρέμβαση μας στην εκλογή ενός νέου root switch, το STP αναγκάστηκε από μόνο του να αλλάξει και την κατάσταση της θύρας, της οποίας τη σύνδεση θεωρούσε ως επιπλέον σύνδεση με βάση το προηγούμενο εκλεγόμενο root switch. Αν παρατηρήσουμε τις εικόνες 4.4.2 και 4.4.4 θα δούμε πως όσο ήταν root switch το ESW1, το STP θεωρούσε ως επιπλέον σύνδεση, τη σύνδεση μεταξύ του ESW3 και του ESW2 οπότε και μετέβαλε τη κατάσταση της διεπαφής f1/6 σε κατάσταση blocking. Μετά την εκλογή όμως του ESW3 ως root switch που φαίνεται

στην εικόνα 4.4.8, η σύνδεση αυτή ενεργοποιήθηκε και μεταβλήθηκε η κατάσταση της διεπαφής f1/6 σε κατάσταση forwarding. Έτσι το STP αποφάσισε πως πλέον η περιττή σύνδεση βρίσκεται μεταξύ των switches ESW1 και ESW2 και μεταβάλλει τη κατάσταση της διεπαφής f1/4 του ESW2 σε κατάσταση blocking όπως μπορούμε να δούμε στην εικόνα 4.4.10.

# 4.5 ΠΡΟΣΟΜΟΙΩΣΗ 3

Στη τρίτη προσομοίωση θα δείξουμε με ποιον τρόπο καθορίζεται η εκλογή των ρόλων των θυρών από τα switches που συμμετέχουν στο STP και πως μπορούμε να το δούμε στην εφαρμογή GNS3.

Το δίκτυο μας, σε αυτή τη περίπτωση, αποτελείται από τέσσερα switches, το ESW1, το ESW2 το ESW3 και το ESW4.




***Εικόνα 4.5.1:*** *Δίκτυο προσομοίωσης 3.*

Στη συνέχεια, θα μεταβούμε στο λειτουργικό σύστημα του κάθε switch και θα εκτελέσουμε στη γραμμή prompt την εντολή «show spanning-tree». Η εντολή θα μας εμφανίσει ως αποτέλεσμα, αναλυτικά τις πληροφορίες για το συγκεκριμένο switch που έχει εκτελεστεί η εντολή καθώς και τις πληροφορίες για τις θύρες των διεπαφών του switch. Τα στοιχεία φαίνονται αναλυτικά στις παρακάτω εικόνες.

```
ESW1#show spanning-tree

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c201.04e0.0000
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:01:56 ago
          from FastEthernet1/2
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 43 (FastEthernet1/2) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 128.43.
    Designated root has priority 32768, address c201.04e0.0000
    Designated bridge has priority 32768, address c201.04e0.0000
    Designated port id is 128.43, designated path cost 0
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    BPDU: sent 73, received 1

 Port 46 (FastEthernet1/5) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 128.46.
    Designated root has priority 32768, address c201.04e0.0000
    Designated bridge has priority 32768, address c201.04e0.0000
    Designated port id is 128.46, designated path cost 0
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    BPDU: sent 73, received 1
```

***Εικόνα 4.5.2:*** *Πληροφορίες διεπαφών του ESW1.*

```
ESW2#show spanning-tree

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c202.0a14.0000
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address c201.04e0.0000
  Root port is 43 (FastEthernet1/2), cost of root path is 19
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:02:07 ago
          from FastEthernet1/2
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 43 (FastEthernet1/2) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 128.43.
    Designated root has priority 32768, address c201.04e0.0000
    Designated bridge has priority 32768, address c201.04e0.0000
    Designated port id is 128.43, designated path cost 0
    Timers: message age 2, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    BPDU: sent 1, received 79

 Port 44 (FastEthernet1/3) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 128.44.
    Designated root has priority 32768, address c201.04e0.0000
    Designated bridge has priority 32768, address c202.0a14.0000
    Designated port id is 128.44, designated path cost 19
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    BPDU: sent 80, received 0
```

***Εικόνα 4.5.3:*** *Πληροφορίες διεπαφών του ESW2.*

```
ESW3#show spanning-tree

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c203.1540.0000
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address c201.04e0.0000
  Root port is 46 (FastEthernet1/5), cost of root path is 19
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:02:16 ago
          from FastEthernet1/4
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 45 (FastEthernet1/4) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.45.
   Designated root has priority 32768, address c201.04e0.0000
   Designated bridge has priority 32768, address c203.1540.0000
   Designated port id is 128.45, designated path cost 19
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 85, received 1

 Port 46 (FastEthernet1/5) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.46.
   Designated root has priority 32768, address c201.04e0.0000
   Designated bridge has priority 32768, address c201.04e0.0000
   Designated port id is 128.46, designated path cost 0
   Timers: message age 1, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 1, received 85
```

***Εικόνα 4.5.4:*** *Πληροφορίες διεπαφών του ESW3.*

```
ESW4#show spanning-tree

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c204.0c74.0000
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address c201.04e0.0000
  Root port is 44 (FastEthernet1/3), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 00:02:55 ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 44 (FastEthernet1/3) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 128.44.
    Designated root has priority 32768, address c201.04e0.0000
    Designated bridge has priority 32768, address c202.0a14.0000
    Designated port id is 128.44, designated path cost 19
    Timers: message age 3, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    BPDU: sent 0, received 88

 Port 45 (FastEthernet1/4) of VLAN1 is blocking
    Port path cost 19, Port priority 128, Port Identifier 128.45.
    Designated root has priority 32768, address c201.04e0.0000
    Designated bridge has priority 32768, address c203.1540.0000
    Designated port id is 128.45, designated path cost 19
    Timers: message age 2, forward delay 0, hold 0
    Number of transitions to forwarding state: 0
    BPDU: sent 1, received 90
```

***Εικόνα 4.5.5:*** *Πληροφορίες διεπαφών του ESW4.*

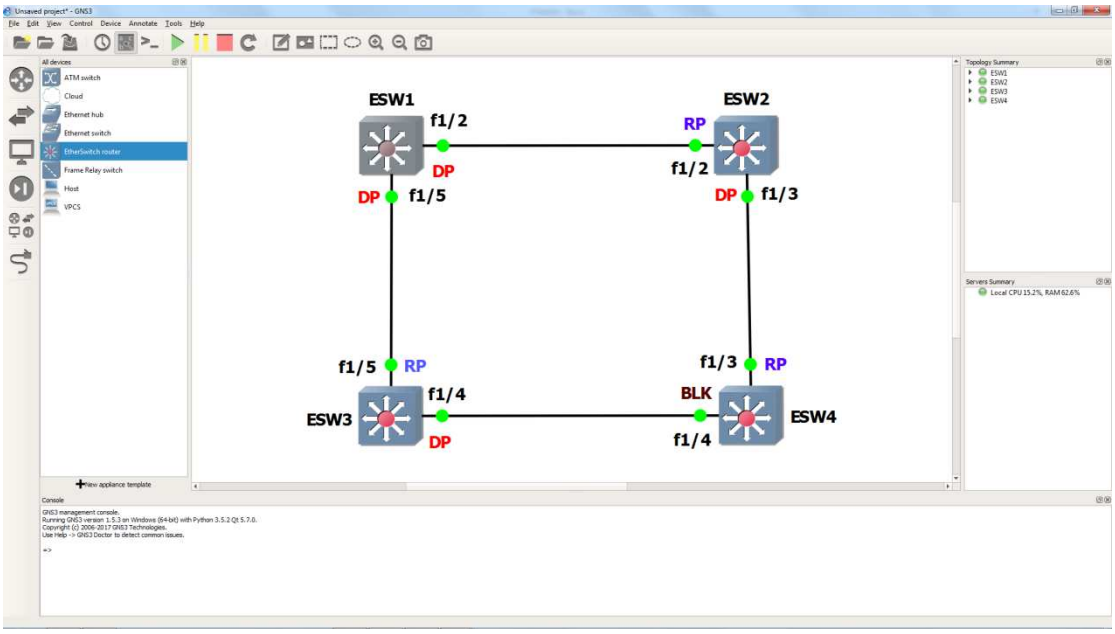
Στην εικόνα 4.5.2 παίρνουμε ως αποτέλεσμα τις εξής πληροφορίες για το switch ESW1. Τη τιμή της προτεραιότητας του, τη φυσική του διεύθυνση, τις προκαθορισμένες τιμές των χρονομέτρων hello time, max age και forward delay. Έπειτα εμφανίζει τις αλλαγές που έχουν συμβεί στη τοπολογία του δικτύου (στη περίπτωση μας έχουν συμβεί 35 αλλαγές) και πόσες ειδοποιήσεις έχει δεχτεί για τις αλλαγές που έχουν συμβεί.

Τέλος, εμφανίζονται αναλυτικά οι πληροφορίες για τη θύρα της διεπαφής f1/3 του ESW1 οι οποίες είναι κατάσταση στην οποία βρίσκεται η διεπαφή, το κόστος διαδρομής προς το root switch, η τιμή προτεραιότητας της θύρας, το ID της θύρας, το κόστος διαδρομής προς τη designated port του root switch, τον αριθμό των μεταβολών των καταστάσεων που έγιναν ώστε να φτάσει η θύρα στη κατάσταση forwarding και τέλος τον αριθμό των απεσταλμένων και λαμβανομένων BPDU

μηνυμάτων της θύρας. Παρόμοια είναι και τα στοιχεία της θύρας της διεπαφής f1/4 του ESW1.

Στο κεφαλαίο 2, αναφέραμε πως οι θύρες ενός root switch χαρακτηρίζονται όλες ως designated ports διότι όλες οι θύρες προωθούν δεδομένα προς τα άλλα switches. Πράγμα που δεν εμφανίζεται στης πληροφορίες που παίρνουμε. Μας ενημερώνει ωστόσο, πως το συγκεκριμένο switch είναι το root switch οπότε εννοείται πως οι θύρες του χαρακτηρίζονται ως designated. Επίσης παρόμοιες είναι οι πληροφορίες που παίρνουμε στις εικόνες 4.5.3, 4.5.4, και 4.5.5 για τα switches ESW2 ESW3 και ESW4 αντίστοιχα. Η μόνη διαφορά που μπορούμε να διακρίνουμε παρατηρώντας τα στοιχεία που παίρνουμε για τα υπόλοιπα switches είναι η ενημέρωση για το ποια θύρα χαρακτηρίζεται ως root port και σε ποια διεπαφή ανήκει. Για το ESW2, στην εικόνα 4.5.3, μας ενημερώνει πως η θύρα 43 της διεπαφής f1/2 είναι η root port και το κόστος διαδρομής είναι 19. Αντίστοιχα η πληροφορία αυτή φαίνεται στην εικόνα 4.5.4 για το switch ESW3 και στην εικόνα 4.5.5 για το switch ESW4.

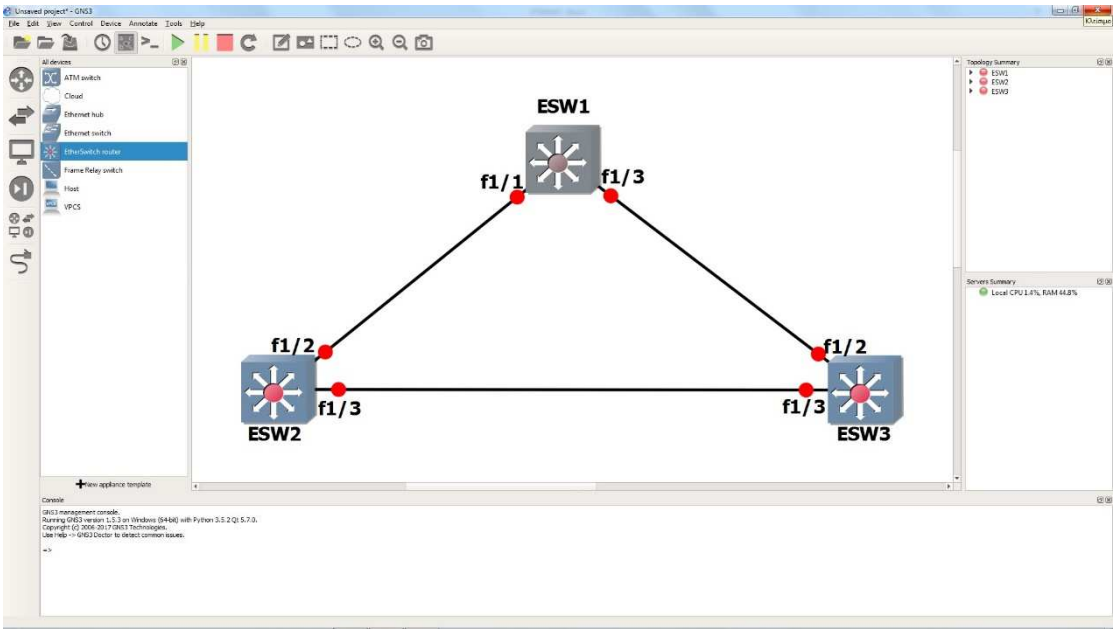
Γνωρίζοντας αυτές τις πληροφορίες, μπορούμε να τις εισάγουμε στο δίκτυο μας για να φαίνεται πιο παραστατικό.




***Εικόνα 4.5.6:*** *Δίκτυο προσομοίωσης 3 συμπεριλαμβανομένων των ρόλων των θυρών.*

# 4.6 ΠΡΟΣΟΜΟΙΩΣΗ 4

Σε αυτή τη περίπτωση θα δείξουμε πως μεταβάλλονται οι καταστάσεις των θυρών ενός switch, όταν ενεργοποιείται για πρώτη φορά το switch και οι διεπαφές του. Επίσης θα δείξουμε τον χρόνο που απαιτείται για τη μεταβολή από τη μία κατάσταση στην άλλη και αν αυτός χρόνος είναι σύμφωνος με τη θεωρία του STP καθώς και το πώς επηρεάζεται το STP από αυτές τις μεταβολές. Για το σκοπό αυτό, το δίκτυο που θα σχεδιάσουμε θα αποτελείται από τρία switches συνδεδεμένα σύμφωνα με την εικόνα 4.6.1.




***Εικόνα 4.6.1:*** *Δίκτυο προσομοίωσης 4.*

Αφού ενεργοποιήσουμε τα switches και τις διεπάφες του δικτύου μας, στη συνεχεία θα μεταβούμε στο λειτουργικό σύστημα του κάθε switch. Με την μετάβαση μας στο λειτουργικό σύστημα χρειάζεται να περάσει ένα διάστημα λίγων δευτερολέπτων ώστε να μπορούμε να γράψουμε κάποια εντολή στη γραμμή prompt. Σε αυτό το διάστημα οι διεπαφές των switches έχουν ήδη καταλήξει στη τελική τους κατάσταση και δεν μπορούμε να δούμε τη διαδικασία που πραγματοποιήθηκε για να φτάσουν σε αυτή τη κατάσταση.

Για αυτό το λόγο θα εκτελέσουμε τη εντολή «debug spanning-tree events» σε κάθε switch. Με την εντολή αυτή, ενεργοποιούμε την ιδιότητα του εντοπισμού

οποιασδήποτε αλλαγής προκύψει σε κάποιο από τα switches και θα εμφανιστεί στο λειτουργικό σύστημα σε κάθε ένα από αυτά.

```
ESW3#debug spanning-tree events
Spanning Tree event debugging is on
ESW3#
```

***Εικόνα 4.6.2:*** *Εκτέλεση εντολής «debug spanning-tree events» για το ESW3.*

Παρόμοια εκτελούμε την ίδια εντολή για το ESW1 και το ESW2.

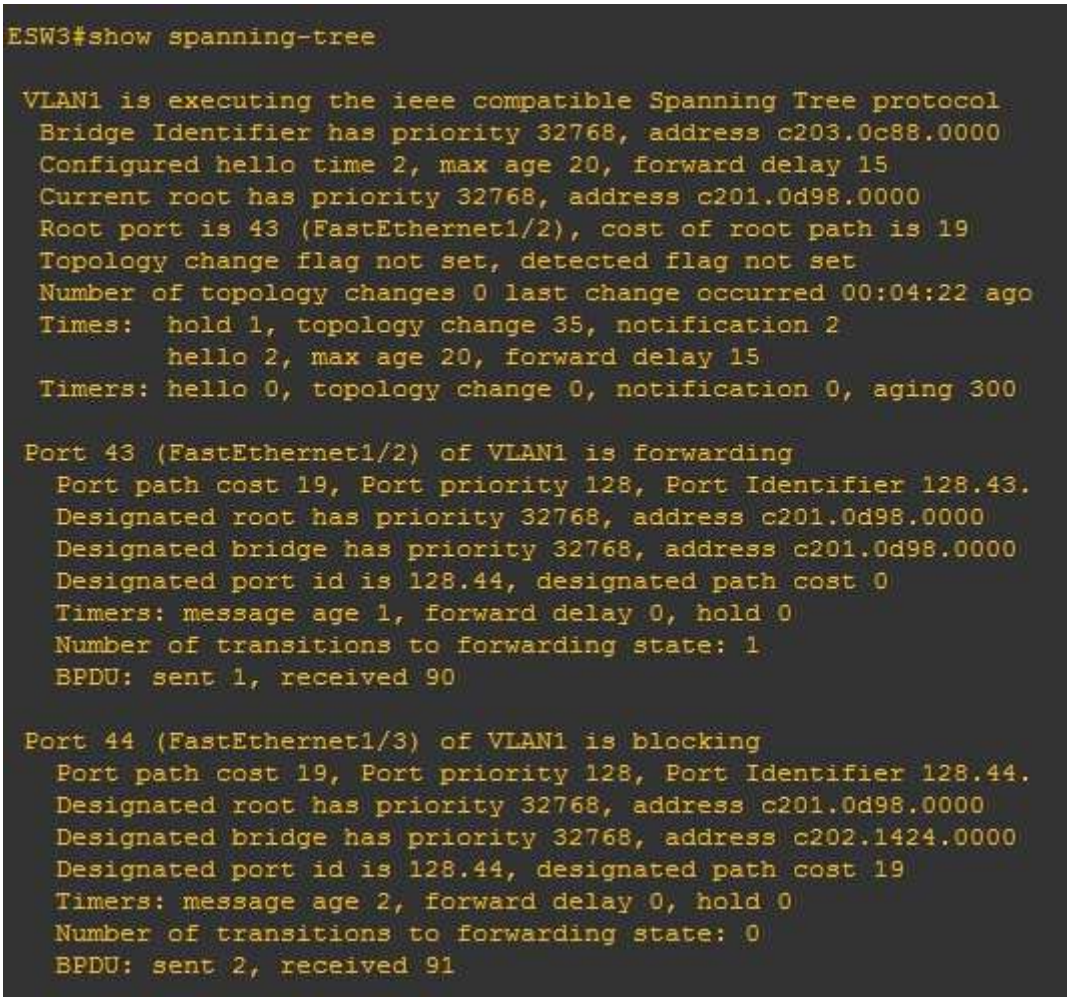
Στη συνέχεια θα χρειαστεί να απενεργοποιήσουμε και να ενεργοποιήσουμε εκ νέου μία από τις διεπαφές, αφού όπως αναφέραμε βρίσκονται είδη στη τελική τους κατάσταση, για να δούμε αναλυτικά τις μεταβολές των καταστάσεων τους.

Εσκεμμένα θα δείξουμε τη διαδικασία για το switch ESW3. Θα εξηγήσουμε το λόγο στη συνέχεια. Η ίδια διαδικασία μπορεί να χρησιμοποιηθεί και στα υπόλοιπα switches. Οι καταστάσεις των διεπαφών του switch ESW3 αρχικά φαίνονται στην εικόνα 4.6.3.

```
ESW3#show spanning-tree brief

VLAN1
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     c201.0d98.0000
              Cost        19
              Port        43 (FastEthernet1/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c203.0c88.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                   Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/2      128.43   128    19 FWD     0 32768 c201.0d98.0000 128.44
FastEthernet1/3      128.44   128    19 BLK    19 32768 c202.1424.0000 128.44
```

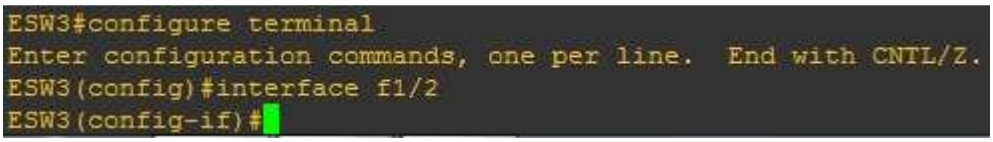
***Εικόνα 4.6.3:*** *Εμφάνιση πληροφοριών του ESW3.*

Βλέπουμε πως η διεπαφή f1/2 βρίσκεται σε κατάσταση forwarding και η διεπαφή f1/3 βρίσκεται σε κατάσταση blocking. Στην εικόνα 4.6.4 διαπιστώνουμε πως η διεπαφή f1/2 αποτελεί τη root port του switch ESW3.



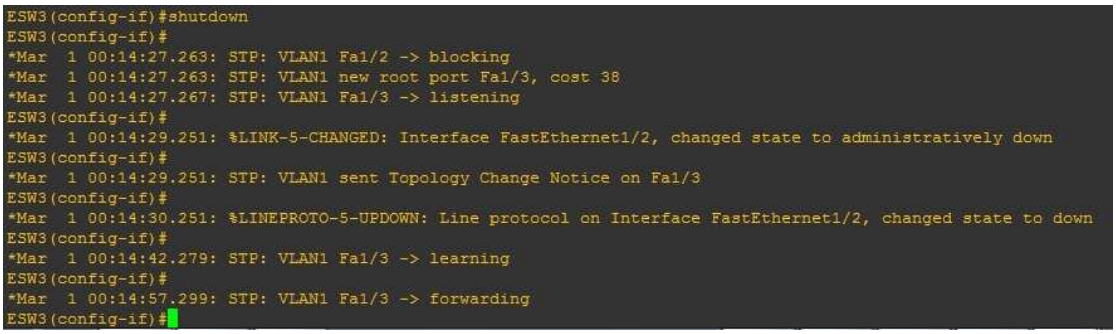

***Εικόνα 4.6.4:*** *Εμφάνιση πληροφοριών διεπαφών του ESW3.*

Για να ενεργοποιήσουμε ή να απενεργοποιήσουμε μία διεπαφή ενός switch, θα πρέπει να μεταβούμε στη κατάσταση διαμόρφωσης του συγκεκριμένου switch και έπειτα στη κατάσταση διαμόρφωσης της διεπαφής, την οποία θέλουμε να επεξεργαστούμε. Για επιτύχουμε κάτι τέτοιο, στη περίπτωση μας για το switch ESW3, πρέπει να εκτελέσουμε την εντολή «configure terminal» που θα μας επιτρέψει να μπούμε στη κατάσταση διαμόρφωσης του switch και στη συνέχει να εκτελέσουμε την εντολή «interface (τύπο διεπαφής) (αριθμό διεπαφής» για να μεταβούμε στη κατάσταση διαμόρφωσης της διεπαφής.




***Εικόνα 4.6.5:*** *Μετάβαση στη κατάσταση διαμόρφωσης του ESW3 και μετάβαση στη κατάσταση διαμόρφωσης διεπαφής f1/2.*

Όπως φαίνεται στην εικόνα 4.6.5, έχουμε μεταφερθεί από τη κατάσταση περιορισμένης πρόσβασης, στη κατάσταση διαμόρφωσης του switch, και έπειτα της διεπαφής. Είμαστε σε θέση πλέον να επεξεργαστούμε τη διεπαφή μας. Στη περίπτωση μας θα επανεκκινήσουμε την διεπαφή f1/2 πρώτα και στη συνέχεια την διεπαφή f1/3. Για την απενεργοποίηση μιας διεπαφής χρειάζεται να πληκτρολογήσουμε την εντολή «shutdown» και για την ενεργοποίηση την εντολή «no shutdown». Απενεργοποιώντας την διεπαφή f1/2, μας ενημερώνει το σύστημα πως η διεπαφή απενεργοποιήθηκε από το χρήστη όπως δηλώνει η γραμμή «%LINK-5-CHANGED: Interface FastEthernet1/2, changed state to administratively down». Παράλληλα αποστέλλεται μία ειδοποίηση από το switch για αλλαγή στη τοπολογία στην διεπαφή f1/3 και το STP μεταβάλει αμέσως τη κατάσταση της διεπαφής f1/2 από forwarding σε blocking. Παρατηρούμε όμως, από τα αποτελέσματα που μας εμφανίζει, από την προηγούμενη εντολή debug που εκτελέσαμε, πως παράλληλα ενεργοποιεί τη διεπαφή f1/3 που βρισκόταν σε κατάσταση blocking και ορίζει ως νέο root port τη θύρα της διεπαφής με κόστος διαδρομής 38. Και αφού ενεργοποιείται η μπλοκαρισμένη θύρα ξεκινάει να μεταβάλλεται από όλες τις καταστάσεις μέχρι να φτάσει στη κατάσταση forwarding και να είναι πλήρως λειτουργική.

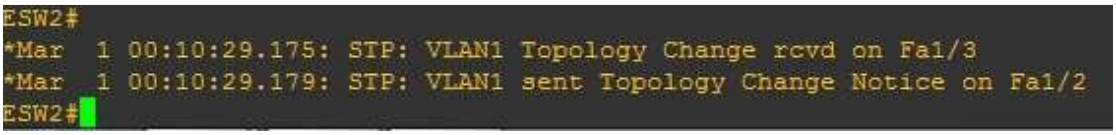



***Εικόνα 4.6.6:*** *Απενεργοποίηση της διεπαφής f1/2 και μεταβολή καταστάσεων της διεπαφής f1/3 του ESW3.*

Παρατηρώντας την εικόνα 4.6.6 μπορούμε να δούμε και το χρόνο που απαιτείται για την αλλαγή της μίας κατάστασης στην άλλη. Η διεπαφή f1/3 μεταβαίνει σε κατάσταση listening την χρονική στιγμή 00:14:27. Μετά από 15 δευτερόλεπτα (Forward Delay), τη χρονική στιγμή 00:14:42 μεταβαίνει στη κατάσταση learning και στη συνέχεια μετά από 15 δευτερόλεπτα ξανά (Forward Delay), τη χρονική στιγμή 00:14:57 μεταβαίνει στη κατάσταση forwarding. Επομένως ο χρόνος μεταβολής μιας θύρας από τη κατάσταση blocking σε forwarding

απαιτεί 30 δευτερόλεπτα. Επίσης, απενεργοποιώντας την διεπαφή f1/2 του ESW3, αμέσως ενημερώθηκαν τα switches ESW1 και ESW2 για αυτήν την αλλαγή στη τοπολογία όπως φαίνεται στις παρακάτω εικόνες 4.6.7 και 4.6.8 αντίστοιχα.


***Εικόνα 4.6.7:*** *Ενημέρωση του ESW1 της αλλαγής της τοπολογίας.*

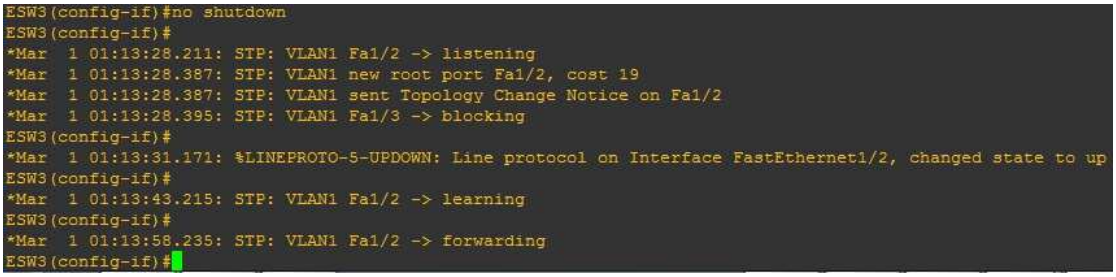



***Εικόνα 4.6.8:*** *Ενημέρωση του ESW2 της αλλαγής της τοπολογίας.*

Το switch ESW1 ενημερώθηκε για την αλλαγή τοπολογίας από την διεπαφή του fa1/1 και το switch ESW2 ενημερώθηκε για την αλλαγή τοπολογίας από την διεπαφή του fa1/3 και ενημέρωσε τη διεπαφή του fa1/2 στέλνοντας επίσης μια ενημέρωση της αλλαγής τοπολογίας.

Για αυτό το σκοπό δείξαμε εσκεμμένα την επεξεργασία των διεπαφών του switch ESW3. Για να δείξουμε, πως το STP σε περίπτωση βλάβης ή απενεργοποίησης μιας ενεργής διεπαφής ενός switch, ενεργοποιεί και χρησιμοποιεί την εφεδρική σύνδεση που βρίσκεται σε κατάσταση blocking.

Αν ενεργοποιήσουμε ξανά την διεπαφή f1/2, τότε το STP θα ορίσει την θύρα της διεπαφής ξανά ως root port διότι έχει μικρότερο κόστος διαδρομής προς το root switch από τη διεπαφή f1/3, θα μπλοκάρει την διεπαφή f1/3 και η διεπαφή f1/2 θα ξεκινήσει τη μετάβαση της από τη κατάσταση listening, αφού δεν βρισκόταν σε κατάσταση blocking αλλά ήταν απενεργοποιημένη, στη κατάσταση learning σε χρονικό διάστημα 15 δευτερολέπτων και στα επόμενα 15 δευτερόλεπτα θα μεταβεί στη κατάσταση forwarding. Η διαδικασία αυτή φαίνεται στην εικόνα 4.6.9.




***Εικόνα 4.6.9:*** *Ενεργοποίηση διεπαφής f1/2 του ESW3 και μεταβολή των καταστάσεών της.*

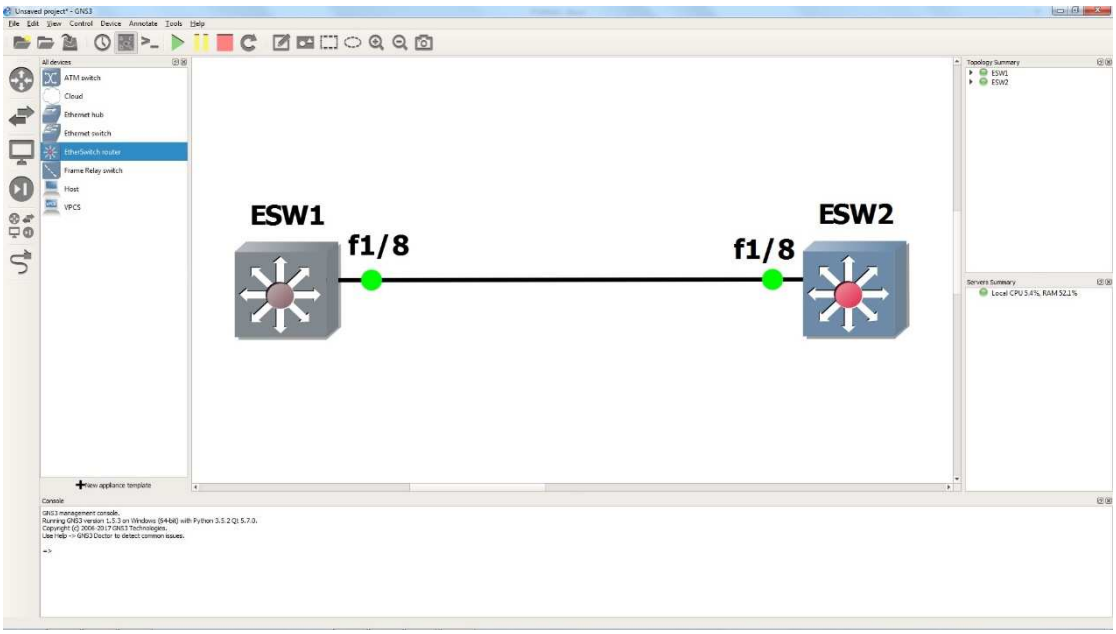
Στη περίπτωση απενεργοποίησης και ενεργοποίησης της διεπαφής f1/3 του ESW3 δεν θα προκύψει κάποια αλλαγή στο δίκτυο μας διότι η διεπαφή είναι μπλοκαρισμένη από το STP, με αποτέλεσμα να μην επηρεάζει τη λειτουργικότητα του δικτύου, και να μην γνωρίζουν για την ύπαρξη της τα switches ESW1 και ESW2 με αποτέλεσμα να μην ενημερωθούν για κάποια αλλαγή.

# 4.7 ΠΡΟΣΟΜΟΙΩΣΗ 5

Στη τελευταία μας προσομοίωση θα δείξουμε πώς μπορούμε να δείξουμε τα μηνύματα BPDU, και το περιεχόμενό τους, που μεταφέρονται μεταξύ των switches, σε ένα δίκτυο, και συμμετέχουν στο STP. Αυτό μπορούμε να το επιτύχουμε με δύο τρόπους. Ο πρώτος τρόπος είναι να χρησιμοποιήσουμε κάποιες εντολές στο πρόγραμμα GNS3 και να εμφανίσουμε στην οθόνη μας τα μηνύματα και δεύτερον με τη χρήση του προγράμματος Wireshark, το οποίο είναι μια εφαρμογή που χρησιμοποιείται για την ανάλυση και την παρακολούθηση ενός δικτύου, σε συνεργασία με το GNS3.

Πρώτα, θα σχεδιάσουμε το δίκτυο μας, το οποίο θα αποτελείται από δύο EtherSwitches συνδεδεμένα με 1 διεπαφή μεταξύ τους, και στην συνέχεια θα δείξουμε τον εντοπισμό τον μηνυμάτων BPDU που αποστέλλονται μεταξύ τους χρησιμοποιώντας και τους δύο τρόπους που αναφέραμε. Στη συνέχεια θα προσθέσουμε ένα τρίτο switch και θα κάνουμε διάφορες επεξεργασίες στο δίκτυο μας για να εντοπίσουμε αλλαγές μεταξύ των μηνυμάτων BPDU που ανταλάσσονται.

Με τη χρήση του προγράμματος GNS3, αφού σχεδιάσουμε το αρχικό δίκτυο της εικόνας 4.7.1, θα μεταβούμε στο λειτουργικό σύστημα των switches.




***Εικόνα 4.7.1:*** *Δίκτυο προσομοίωσης 5.*

Για να εμφανίσουμε τα μηνύματα BPDU που αποστέλλονται από το ESW1 με προορισμό το ESW2, αρκεί να εκτελέσουμε την εντολή «debug spanning-tree bpdu» στο λειτουργικό σύστημα του ESW2. Με την εκτέλεση της, θα αρχίσει η εμφάνιση της συνεχόμενης ροής των μεταδιδόμενων BPDU μηνυμάτων εώς ότου χρησιμοποιήσουμε την εντολή «undebug spanning-tree bpdu».

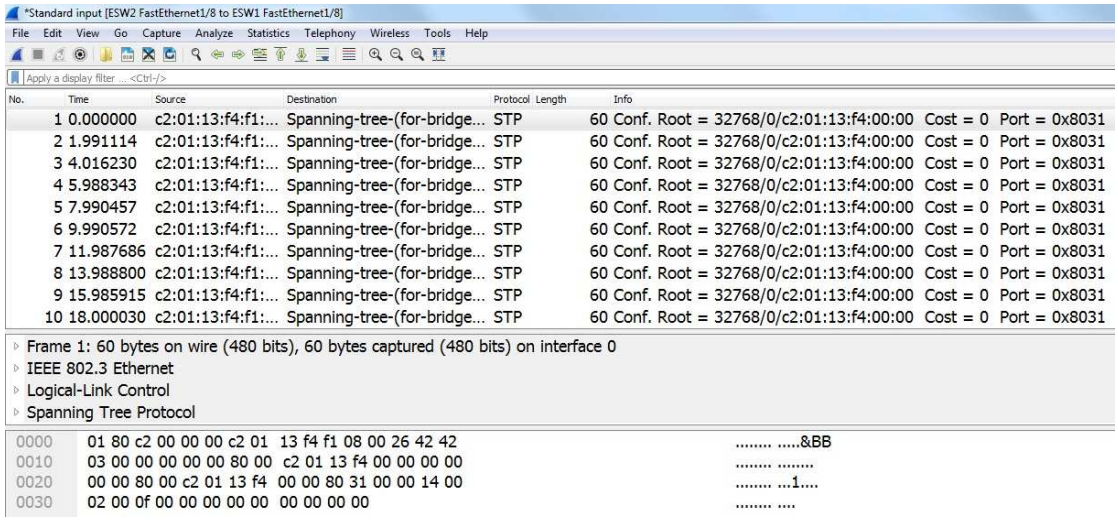
```
ESW2#debug spanning-tree bpdu
Spanning Tree BPDU debugging is on
ESW2#
*Mar  1 00:02:17.383: STP: VLAN1: config protocol = ieee, packet from FastEthernet1/8  , linktype IEEE_SPANNING , enctype 2, encsize 17
*Mar  1 00:02:17.383: STP: enc 01 80 C2 00 00 00 C2 01 13 F4 F1 08 00 26 42 42 03
*Mar  1 00:02:17.391: STP: Data     0000000000800OC20113F400000000000008000C20113F4000080310000140002000F00
*Mar  1 00:02:17.403: STP: VLAN1 Fa1/8:0000 00 00 00 8000C20113F40000 00000000 8000C20113F40000 8031 0000 1400 0200 0F00
ESW2#debug spanning-tree bpdu
*Mar  1 00:02:21.247: STP: VLAN1: config protocol = ieee, packet from FastEthernet1/8  , linktype IEEE_SPANNING , enctype 2, encsize 17
*Mar  1 00:02:21.247: STP: enc 01 80 C2 00 00 00 C2 01 13 F4 F1 08 00 26 42 42 03
*Mar  1 00:02:21.255: STP: Data     0000000000800OC20113F400000000000008000C20113F4000080310000140002000F00
*Mar  1 00:02:21.267: STP: VLAN1 Fa1/8:0000 00 00 00 8000C20113F40000 00000000 8000C20113F40000 8031 0000 1400 0200 0F00
ESW2#undebug spanning-tree bpdu
*Mar  1 00:02:25.203: STP: VLAN1: config protocol = ieee, packet from FastEthernet1/8  , linktype IEEE_SPANNING , enctype 2, encsize 17
*Mar  1 00:02:25.203: STP: enc 01 80 C2 00 00 00 C2 01 13 F4 F1 08 00 26 42 42 03
*Mar  1 00:02:25.211: STP: Data     0000000000800OC20113F400000000000008000C20113F4000080310000140002000F00
*Mar  1 00:02:25.223: STP: VLAN1 Fa1/8:0000 00 00 00 8000C20113F40000 00000000 8000C20113F40000 8031 0000 1400 0200 0F00
ESW2#undebug spanning-tree bpdu
Spanning Tree BPDU debugging is off
ESW2#
```

***Εικόνα 4.7.2:*** *Εμφάνιση μεταδιδόμενων μηνυμάτων BPDU από το ESW1 προς το ESW2.*

Στην εικόνα 4.7.2 έχουμε εμφανίσει την μετάδοση τριών μηνυμάτων BPDU από το ESW1 προς το ESW2. Από το BPDU μήνυμα παίρνουμε τις πληροφορίες για το είδος του πρωτοκόλλου που χρησιμοποιείται (config protocol = ieee), την διεπαφή η οποία δέχτηκε το μήνυμα (packet from FastEthernet1/8), το τύπο σύνδεσης των μηνυμάτων (linktype IEEE_SPANNING), τον τύπο της ενθυλάκωσης του μηνύματος (enctype 2) και το μέγεθος της ενθυλάκωσης του μηνύματος (encsize 17). Στη συνέχεια μας εμφανίζει ολόκληρο το περιεχόμενο του μηνύματος ενθυλάκωσης με την μορφή bits, έπειτα το περιεχόμενο του συνολικού πλαισίου με την μορφή bits και τέλος τη μορφή με την οποία εισήχθησαν οι πληροφορίες στην διεπαφή f1/8 του ESW2. Με αυτό τον τρόπο μπορούμε να παρακολουθούμε την ροή των μηνυμάτων BPDU που αποστέλλονται από το root switch προς τα άλλα switches.

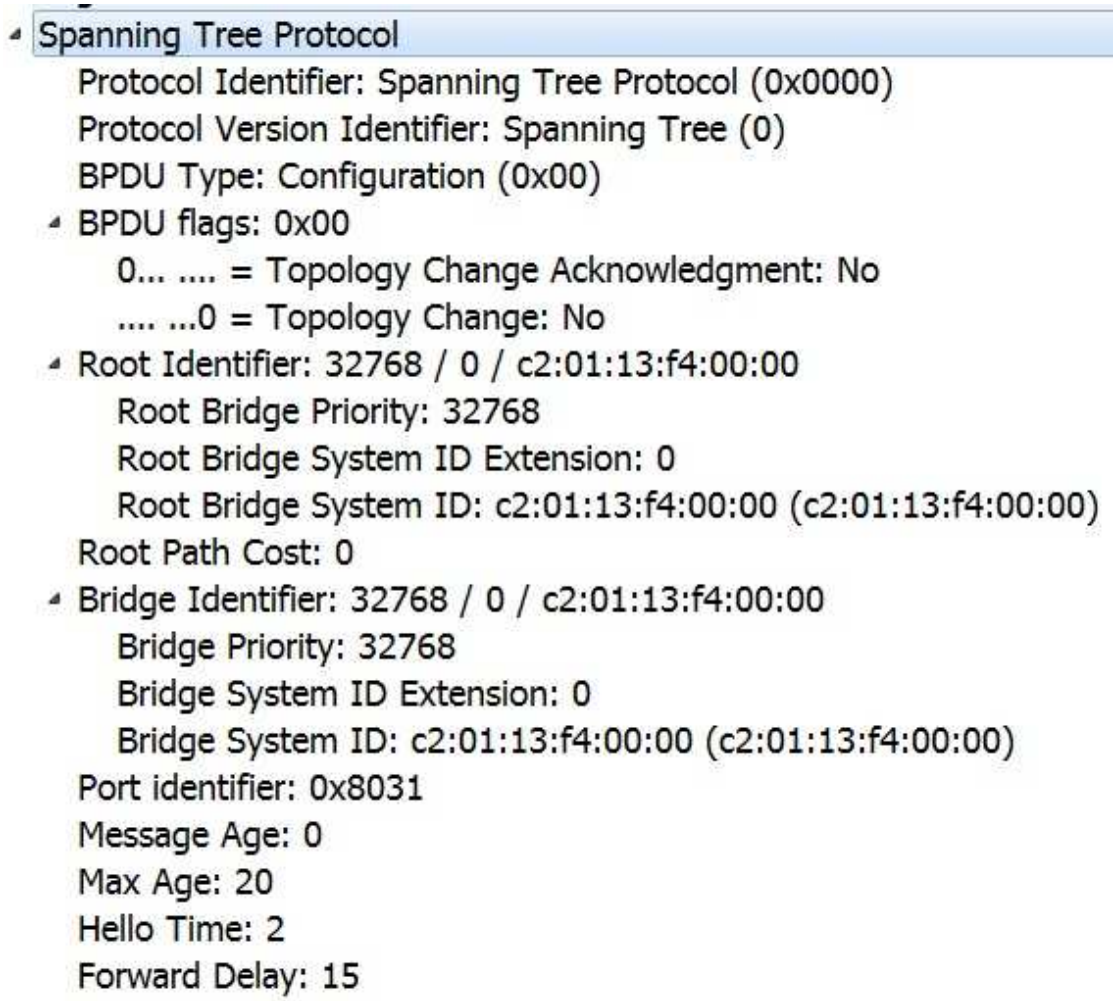
Για να εμφανίσουμε τα πακέτα τώρα, με το πρόγραμμα Wireshark χρειάζεται να μεταφερθούμε στο χώρο εργασίας του GNS3, να κάνουμε δεξί κλικ στη διεπαφή

που συνδέει τα δυο switches και να πατήσουμε την επιλογή «start capture». Αυτόματα, θα ανοίξει η εφαρμογή Wireshark και θα ξεκινήσει αμέσως να μας εμφανίζει τα μηνύματα BPDU που αποστέλλονται προς το ESW2, δίνοντας μας την δυνατότητα να αναλύσουμε περεταίρω ένα από τα μηνύματα BPDU.



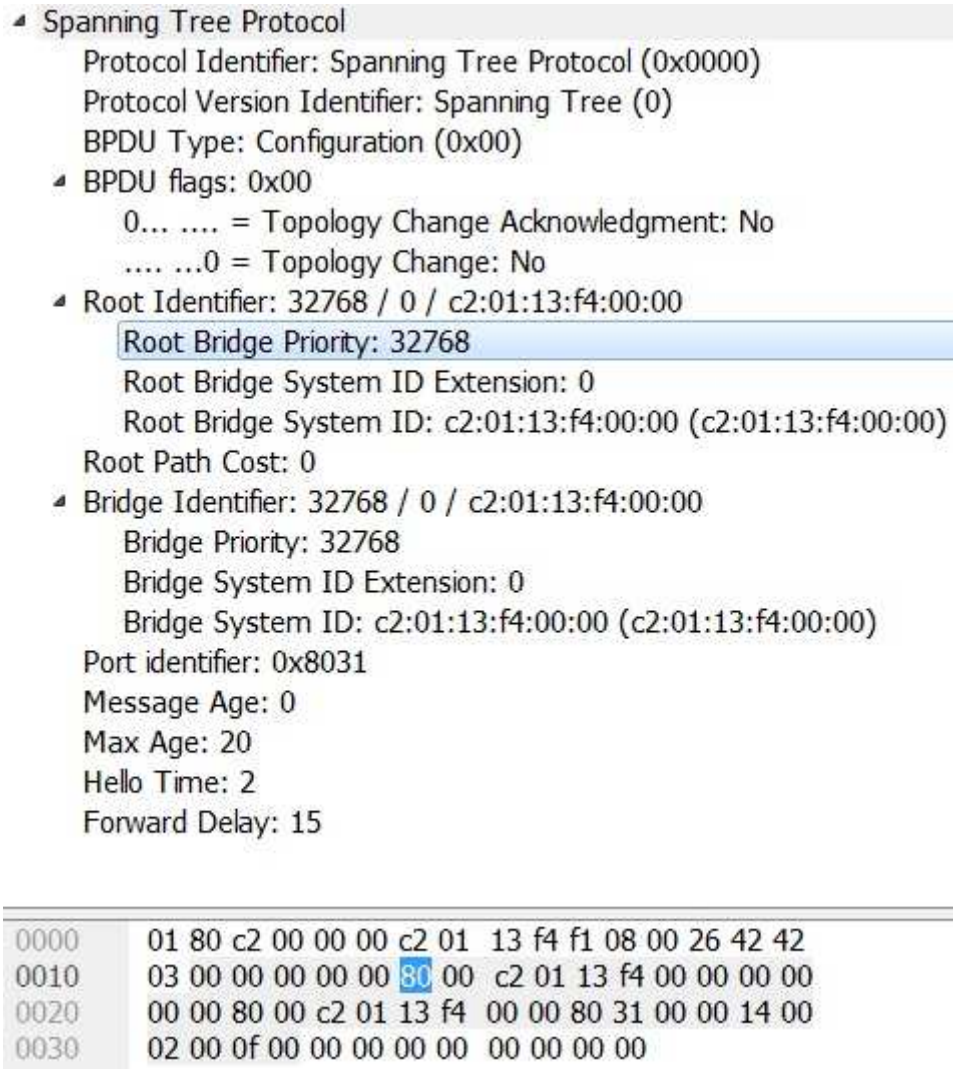

***Εικόνα 4.7.3:*** *Εμφάνιση μεταδιδόμενων μηνυμάτων BPDU από το ESW1 προς το ESW2 μέσω του Wireshark.*

Όπως μπορούμε να δούμε στην εικόνα 4.7.3, έχουμε εντοπίσει τα δέκα πρώτα μηνύματα BPDU που έχουν αποσταλεί προς το ESW2 από το ESW1. Διαλέγοντας ένα από τα μηνύματα αυτά μπορούμε να δούμε αναλυτικότερα τα περιεχόμενα του και σε ποια bits αντιστοιχούν κάνοντας κλικ στο βελάκι της επιλογής Spanning Tree Protocol. Αφού το επιλέξουμε θα εμφανιστούν τα τμήματα που αποτελούν ένα τέτοιο μήνυμα σύμφωνα με την εικόνα 4.7.4.




***Εικόνα 4.7.4:*** *Περιεχόμενα ενός BPDU μηνύματος.*

Επιλέγοντας ένα από αυτά τα πεδία θα μας μπορούμε να δούμε από πόσα bits αποτελείται και την αντίστοιχη θέση τους μέσα σε ένα πλαίσιο όπως για παράδειγμα μπορούμε να δούμε στην εικόνα 4.7.5




***Εικόνα 4.7.5:*** *Αντιστοιχία πεδίου Root Bridge Priority σε μορφή byte.*

Αν παρατηρήσουμε τις εικόνες 4.7.3 και 4.7.4 μπορούμε να συγκρίνουμε τις πληροφορίες που έχουμε λάβει και να ελέγξουμε αν λειτουργεί σωστά το STP. Βάση αυτών των πληροφοριών μπορούμε να βγάλουμε τα εξής συμπεράσματα.

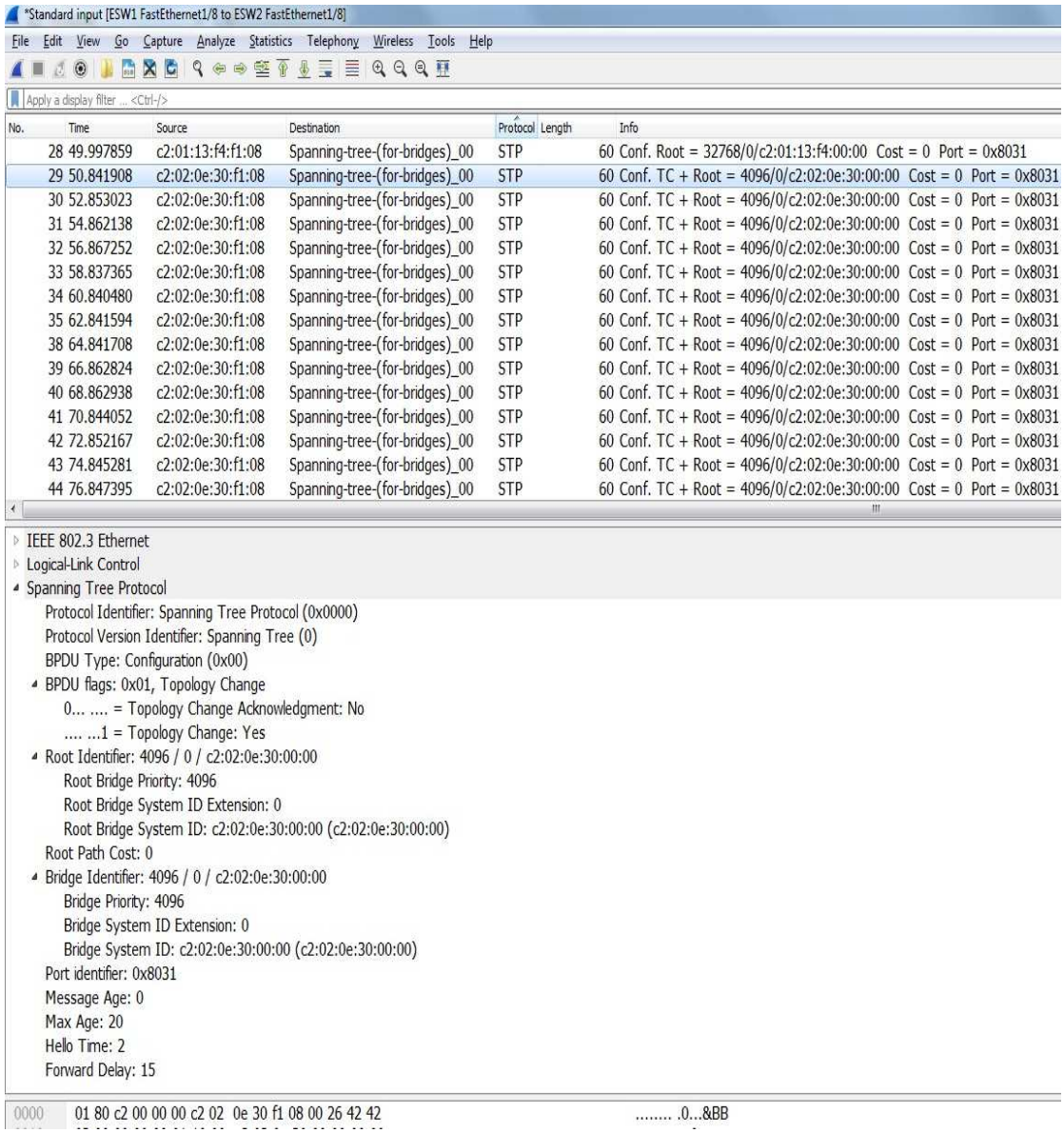
Αρχικά διαπιστώνουμε πως ο χρόνος μετάδοσης των μηνυμάτων είναι ανά δύο δευτερόλεπτα που αντιστοιχεί στο χρόνο Hello Time. Επίσης, όλα τα μηνύματα έχουν την ίδια διεύθυνση πηγής (c2:01:13:f4:00:00) και την ίδια διεύθυνση προορισμού (01:80:c2:00:00:00). Επιπρόσθετα, η τιμή της προτεραιότητας του root switch είναι 32768 και η τιμή της αλλαγής τοπολογίας παραμένει 0. Αυτό σημαίνει πως το δίκτυο μας είναι σταθερό χωρίς καμία αλλαγή.

Τι θα συμβεί όμως αν αλλάξουμε κάποια από αυτές τις τιμές? Παρατηρήσαμε προηγουμένως πως τα μηνύματα μεταδίδονται από το root switch προς τα υπόλοιπα switch. Οπότε εσκεμμένα, καθώς δεχόμαστε τα μηνύματα από το root switch ESW1,

θα επεξεργαστούμε τη τιμή προτεραιότητας του ESW2 επιβάλλοντας το να γίνει το νέο root switch για να δούμε τι θα συμβεί με την αποστολή των μηνυμάτων BPDU.

```
ESW2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ESW2(config)#spanning-tree vlan 1 priority 4096
ESW2(config)#
```

***Εικόνα 4.7.6:*** *Αλλαγή τιμής προτεραιότητας του ESW2.*




***Εικόνα 4.7.7:*** *Εμφάνιση μηνυμάτων μετά την αλλαγή της τιμής προτεραιότητας του ESW2.*

Αφού αλλάξαμε τη τιμή προτεραιότητας του ESW2, από 32768 σε 4096, και το εξαναγκάσαμε να γίνει το νέο root switch, παρατηρώντας την εικόνα 4.7.7 βλέπουμε πως τα απεσταλμένα μηνύματα αρχικά ως και το 28$^{ο}$ μήνυμα είχαν την ίδια διεύθυνση πηγής. Από το 29$^{ο}$ που πραγματοποιήσαμε την αλλαγή στο ESW2, αμέσως οι πληροφορίες των μηνυμάτων άλλαξαν. Πλέον τα μηνύματα έχουν νέα διεύθυνση πηγής, τη διεύθυνση του ESW2, και ως τιμή προτεραιότητας, τη τιμή 4096, που εμείς ορίσαμε. Επίσης μπορούμε να δούμε πως έχει αλλάξει και το bit του πεδίου αλλαγής τοπολογίας σε 1 ώστε να δηλώνει πως έχει συμβεί αλλαγή στη τοπολογία του δικτύου μας. Οι υπόλοιπες τιμές και πληροφορίες έχουν μείνει ίδιες αφού δεν τις μεταβάλλαμε καθόλου.

Παρατηρούμε, λοιπόν, πως ενώ τα μηνύματα αποστέλλονται κανονικά από το root switch σε σωστά χρονικά διαστήματα, με την οποιαδήποτε αλλαγή στο τοπολογία του δικτύου μας έχουμε άμεση και έγκυρη πληροφόρηση χωρίς καμία καθυστέρηση και δυσλειτουργία στο δίκτυο μας.

# ΣΥΜΠΕΡΑΣΜΑΤΑ

Με βάση την ανάλυση των προσομοιώσεων που εκτελέσαμε στο 4$^{ο}$ κεφάλαιο, συμπεραίνουμε πως το Spanning Tree Protocol αποτελεί ένα θεμελιώδης μέρος ενός δικτύου Ethernet. Είναι ένα βασικό εργαλείο που μας βοηθάει να εξασφαλίσουμε τη σταθερότητα ενός δικτύου, που αποτελείται από πολλά switches, να βελτιώσουμε την απόδοση του, αποτρέποντας την δημιουργία πλημμύρας του δικτύου με πακέτα, αφού καταστέλλονται οι επιπλέον διαδρομές μεταξύ των switches, καθώς και να εντοπίζουμε τεχνικά προβλήματα εντός του δικτύου.

Επιπλέον, λόγω της πολυπλοκότητας των σημερινών δικτύων, το Spanning Tree Protocol βοηθάει στη γρήγορη προσαρμογή των αλλαγών που συμβαίνουν στη τοπολογία ενός δικτύου. Αυτό οφείλεται στα switches και πως ο διαχειριστής ενός δικτύου θα πρέπει να κατανοεί τα βασικά χαρακτηριστικά τους. Έτσι θα μπορέσει να διατηρήσει το root switch σε κεντρική θέση ώστε να εξασφαλίσει τη δημιουργία περιττών συνδέσεων μεταξύ των switches.

Τέλος, στο Spanning Tree Protocol σημαντικό ρόλο παίζει ο χρόνος που απαιτείται για τη σύγκλιση των switches καθώς εξαρτάται απόλυτα από τα χρονόμετρα του πρωτοκόλλου, κάτι το οποίο στις προσομοιώσεις φαίνεται πως τηρεί απόλυτα για την ορθή λειτουργία των switches αλλά και του δικτύου.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]Switching Book 2 by Xylan.

[2]Ethernet Switches by Charles E. Spurgeon and Joann Zimmerman
Copyright c 2013 Charles Spurgeon and Joann Zimmerman. All rights reserved.

[3]Cisco Switching Black Book: A Practical In-Depth Guide to Configuring, Operating and Managing Cisco LAN Switches by Sean Odom and Hanson Nottingham Paperback Edition 2000

[4]Cisco CCNP Switching Exam Certification Guide by Tim Boyles and David Hucaby
Copyright © 2001 Cisco Systems, Inc.
Published by: Cisco Press

[5]Cisco CCNP Switching Study Guide v2.01 © 2014
By Aaron Balchunas

[6]CCNA Routing and Switching Study Guide Exams 100-101, 200-101, and 200-120 by Lammle Todd
Copyright c 2013 by John Wiley & Sons, Inc., Indianapolis, Indiana
Published by: John Wiley & Sons Inc 2013

[7]CCNA Routing and Switching Review Guide Exams 100-101, 200-101 and 200-120 by Lammle Todd
Copyright c 2014 by John Wiley & Sons, Inc., Indianapolis, Indiana
Published by: John Wiley & Sons Inc 2014

[8]CCNA Cisco Certified Network Associate Study Exam 6th Version by Lammle Todd. Copyright c 2007 by Wiley Publishing, Inc., Indianapolis, Indiana

[9]Characterization of the Spanning Tree Protocol by Eduard Bonada 09/2007

[10]Evaluation and Comparison of Spanning Tree Protocol and Rapid Spanning Tree Protocol on Cisco switches via OPNET. ENSC 427: COMMUNICATION NETWORKS FINAL PROJECT
By Joseph Lu, Sen Jiang, Tao Xiong

[11]https://en.wikipedia.org/wiki/MAC_address

[12]https://en.wikipedia.org/wiki/Broadcast_radiation

[13]https://www.techopedia.com/definition/6270/broadcast-storm

[14]http://study-ccna.com/collision-broadcast-domain/

[15]https://www.techopedia.com/definition/4804/virtual-local-area-network-vlan

[16]http://www.firewall.cx/networking-topics/vlan-networks/designing-vlans/217-dynamic-vlans.html

[17]http://www.firewall.cx/networking-topics/vlan-networks/218-vlan-access-trunk-links.html

[18]http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-vlan-trunking-protocol-vtp.php

[19]http://etutorials.org/Networking/lan+switching/Chapter+8.+Virtual+LANs+VLANs/VLAN+Operation/

[20]https://cdn.preterhuman.net/texts/computing/internet_information/08_805A_2-3_SG.pdf

[21]Δίκτυα Υπολογιστών , ANDREW S. TANENBAUM , Εκδόσεις Κλειδάριθμος (ΤΕΤΑΡΤΗ ΑΜΕΡΙΚΑΝΙΚΗ ΕΚΔΟΣΗ)

[22]http://www.thenetworkencyclopedia.com/entry/layer-3-switch/

[23]https://www.techopedia.com/definition/8465/multilayer-switch

[24]http://www.ciscopress.com/articles/article.asp?p=700137

[25]http://www.force10networks.com/whitepapers/pdf/F10_wp19_v1%201.pdf

[26]http://www.divaportal.org/smash/get/diva2:214185/FULLTEXT01.pdf

[27]https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

[28]https://broadcaststormblog.wordpress.com/2016/01/31/spanning-tree-protocol-from-a-future-ccna-perspective/

[29]CCNA Routing and Switching ICDN2 200-105 Official Cert Guide
Published by: Cisco Press

[30]http://www.omnisecu.com/ccna-security/what-is-root-guard-and-how-to-configure-root-guard-in-cisco-switches.php

[31]http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/19120-122.html

[32]http://www.learncisco.net/courses/icnd-1/building-a-network/ethernet-protocol.html

[33]http://forum.huawei.com/thread-34771-1-1.html

[34]http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html

# ΠΑΡΑΡΤΗΜΑΤΑ

# ΠΑΡΑΡΤΗΜΑ ΠΙΝΑΚΩΝ



# ΠΑΡΑΡΤΗΜΑ ΕΙΚΟΝΩΝ