ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΛΗΡΟΦΟΡΙΑΚΑ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Τεχνικές Μεταγωγής και Δρομολόγησης Εμπορικών Προϊόντων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Dusica Mirkovic (3252021030)

Επιβλέπων : κύριος καθηγητής Κορμέντζας Γεώργιος

Μέλη εξεταστικής επιτροπής:

Σάμος, Ιανουάριος

Πρόλογος και ευχαριστίες

της

DusicaMirkovic

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Πίνακας εικόνων και πηγές τους

Εικόνα15 Λειτουργία πολυστρωματικού διακόπτη.	*https://www.ciscopress.com/articles/article.asp?p=2348265&seqNum=2*
Εικόνα 16 Κατανεμημένη προώθηση υλικού.	*https://www.ciscopress.com/articles/article.asp?p=2348265&seqNum=2*
Εικόνα 17 Δρομολογητής.	*Burdova (2024)*
Εικόνα18 Δρομολόγηση δικτύου.	*Cloudflare (2024)*
Εικόνα19 RIPv1	https://digi.ninja/blog/rip_v1.php 1
Εικόνα20 OSPF	*https://selmanhaxhijaha.wordpress.com/20 1*
Εικόνα21 EIGRP	*htps://skminhaj.wordpress.com/2018/02/1 1*
Εικόνα22 Μετρήσεις επιδόσεων δρομολογητή.	*CommunicationsInc. (2024)*
Εικόνα23 VLAN	*https://www.zframez.com/articles/switchi 1*
Εικόνα24 VXLAN	*https://ipcisco.com/lesson/virtual-exten 1*
Εικόνα 25 Παράδειγμα επίθεσης ARP με τον κακόβουλο χρήστη ως άνθρωπο στο ενδιάμεσο.	*Mehdizadeha, et. al., (2017).*

Περίληψη

Οι τεχνολογίες μεταγωγής και δρομολόγησης της Cisco αποτελούν το θεμέλιο της σύγχρονης δικτύωσης, επιτρέποντας την αποτελεσματική ροή δεδομένων εντός και μεταξύ των δικτύων. Η μεταγωγή, η οποία επικεντρώνεται κυρίως σε τοπικά δίκτυα (LAN), συνδέει πολλαπλές συσκευές, όπως υπολογιστές, εκτυπωτές και διακομιστές, για τον την εσωτερική επικοινωνία. Οι μεταγωγείς της Cisco προσφέρουν προηγμένα χαρακτηριστικά, όπως εικονικά τοπικά δίκτυα (VLAN), πρωτόκολλο Spanning Tree Protocol (STP) και δυνατότητες επιπέδου 3, εξασφαλίζοντας απρόσκοπτη μεταφορά δεδομένων, ενισχυμένη ασφάλεια και βελτιστοποιημένη απόδοση δικτύου. Αυτές οι τεχνολογίες μειώνουν τις συγκρούσεις δεδομένων, διαχειρίζονται τη συμφόρηση του δικτύου και παρέχουν δρομολόγηση μεταξύ των VLAN για καλύτερες οργανωτικές ροές εργασίας.

Από την άλλη πλευρά, η δρομολόγηση απευθύνεται στη μεταφορά δεδομένων μεταξύ δικτύων, γεγονός ζωτικής σημασίας για τα δίκτυα ευρείας περιοχής (WAN). Οι δρομολογητές της Cisco αξιοποιούν ισχυρά πρωτόκολλα δρομολόγησης, όπως τα RIP, OSPF, EIGRP και BGP, για τον προσδιορισμό των βέλτιστων διαδρομών για την παράδοση δεδομένων σε πολύπλοκα και γεωγραφικά διασκορπισμένα δίκτυα. Προηγμένα χαρακτηριστικά, όπως λίστες ελέγχου πρόσβασης (ACL), εικονικά ιδιωτικά δίκτυα (VPN) και πρωτόκολλα πλεονασμού, εξασφαλίζουν ασφαλή, αξιόπιστη και υψηλής απόδοσης συνδεσιμότητα.

Με μια ολοκληρωμένη επιλογή μεταγωγέων και δρομολογητών, από απλές μη διαχειριζόμενες συσκευές για μικρές εγκαταστάσεις έως αρθρωτά συστήματα για δίκτυα επιχειρηματικού επιπέδου, η Cisco προσαρμόζεται στις ποικίλες ανάγκες δικτύωσης. Η ενσωμάτωση από τη Cisco της δικτύωσης που καθορίζεται από λογισμικό (SDN), των λύσεων διαχείρισης που βασίζονται στο cloud, και της υποστήριξης αναδυόμενων τεχνολογιών, όπως το IoT και το VXLAN, ενισχύει την επεκτασιμότητα και τη μελλοντική προστασία.

Λέξεις κλειδιά

Cisco Switching, Cisco Routing, τοπικό δίκτυο (LAN), Εικονικό τοπικό δίκτυο (VLAN).

Abstract

Cisco switching and routing technologies are the foundation of modern networking, enabling efficient data flow within and between networks. Switching, which focuses primarily on local area networks (LANs), connects multiple devices, such as computers, printers, and servers, to streamline internal communications. Cisco switches offer advanced features such as virtual local area networks (VLANs), Spanning Tree Protocol (STP) and Layer 3 capabilities, ensuring seamless data transfer, enhanced security and optimized network performance. These technologies reduce data conflicts, manage network congestion and provide routing between VLANs for better organizational workflows.

On the other hand, routing addresses data transfer between networks, which is vital for wide area networks (WANs). Cisco routers leverage powerful routing protocols, such as RIP, OSPF, EIGRP and BGP, to determine the best routes for data delivery across complex and geographically dispersed networks. Advanced features such as access control lists (ACLs), virtual private networks (VPNs) and redundancy protocols ensure secure, reliable and high-performance connectivity.

With a comprehensive selection of switches and routers, from simple unmanaged devices for small deployments to modular systems for enterprise-class networks, Cisco accommodates a variety of networking needs. Cisco's integration of software-defined networking (SDN), cloud-based management solutions, and support for emerging technologies such as IoT and VXLAN enhances scalability and future-proofing.

Keywords

Cisco Switching, Cisco Routing, Local Area Network (LAN), Virtual Local Area Network (VLAN).

Εισαγωγή

Η Cisco Systems είναι μια αμερικανική εταιρεία, γνωστή για τις τεχνολογίες δικτύωσης υπολογιστών. Αν και η Cisco απευθυνόταν κυρίως σε πελάτες B2B, αναδείχθηκε σε έναν από τους κορυφαίους οργανισμούς στις Ηνωμένες Πολιτείες καθ' όλη τη δεύτερη δεκαετία του 21ου αιώνα. Η Cisco ιδρύθηκε το 1984 και έχει την έδρα της στο Σαν Χοσέ της Καλιφόρνια (Javaid, 2010).

Ο Leonard Bosack και η Sandra Lerner, ένα παντρεμένο ζευγάρι που αργότερα χώρισε, ήταν οι συνιδρυτές της Cisco Systems. Οι δρόμοι τους διασταυρώθηκαν αρχικά κατά τη διάρκεια των σπουδών τους στο Πανεπιστήμιο του Στάνφορντ. Μετά την ολοκλήρωση των σπουδών τους το 1981, προσλήφθηκαν από τη σχολή για να επιβλέπουν τις εγκαταστάσεις υπολογιστών δύο διαφορετικών τμημάτων. Ο Bosack ανακάλυψε μια μέθοδο για τη σύνδεση των επιμέρους δικτύων υπολογιστών τους χρησιμοποιώντας τεχνολογία που είχε αναπτυχθεί από άλλο προσωπικό του Στάνφορντ κατά τη δεκαετία του 1970. Ο ίδιος και ο Lerner συνειδητοποίησαν ότι η τεχνολογία δρομολογητών, συχνά γνωστή ως, μπορεί να είναι ιδιαίτερα επικερδής όταν εφαρμόζεται σε μεγάλη κλίμακα πέρα από το ίδρυμα. Τον Δεκέμβριο του 1984, τα δύο άτομα ίδρυσαν τη CiscoSystems (αρχικά γράφτηκε ως "ciscoSystems"), αντλώντας το όνομα της εταιρείας από την πόλη του Σαν Φρανσίσκο. Το Στάνφορντ παραχώρησε τελικά άδεια χρήσης στη Cisco για το αποκλειστικό λογισμικό της (Javaid, 2010).

Η Cisco πραγματοποίησε την πρώτη της πώληση το 1985, προσφέροντας μια συσκευή διασύνδεσης δικτύου για τους υπολογιστές της Digital Equipment Corporation. Το αρχικό σημαντικό επίτευγμα της εταιρείας ήταν η ανάπτυξη ενός δρομολογητή που μπορούσε να υποστηρίξει πολλά πρωτόκολλα δικτύου, η οποία πραγματοποιήθηκε το επόμενο έτος. Αναζητώντας κεφάλαια για την επέκταση της επιχείρησης, οι ιδρυτές προσέγγισαν τη Sequoia Capital, μια εταιρεία επιχειρηματικών κεφαλαίων. Η Sequoia ανέλαβε τον επιχειρησιακό έλεγχο της εταιρείας στα τέλη του 1987 και διόρισε τον John Morgridge ως πρόεδρο και διευθύνοντα σύμβουλο το 1988. Ο ίδιος επέδειξε επιδεξιότητα στις διοικητικές του ικανότητες, αν και η σχέση του με τους ιδρυτές ήταν τεταμένη. Το 1990, λίγο μετά την αρχική δημόσια προσφορά της Cisco, ο Lerner απομακρύνθηκε από την εταιρεία και ο Bosack παραιτήθηκε αργότερα (Entezami&Politis, 2013).

Η Cisco Systems σημείωσε σημαντική ανάπτυξη στις αρχές της δεκαετίας του 1990. Το 1993, η επιχείρηση λάνσαρε το βελτιωμένο μοντέλο δρομολογητή 7000 και ταυτόχρονα

ξεκίνησε τη διαδικασία εξαγοράς άλλων επιχειρήσεων. Η εξαγορά της Crescendo Communications από τη Cisco επέτρεψε στην εταιρεία να εισέλθει με αυτοπεποίθηση στην αγορά συσκευών μεταγωγής δικτύου (Wazir Zada Khanetal, 2012). Το 1994, η εταιρεία μετέφερε τα κεντρικά της γραφεία από το Menlo Park της Καλιφόρνια στο SanJose. Την επόμενη χρονιά, ο John T. Chambers ανέλαβε τη θέση του διευθύνοντος συμβούλου, αντικαθιστώντας τον Morgridge. Ο Chambers επέμεινε στην εφαρμογή της προσέγγισης της επέκτασης μέσω της εξαγοράς άλλων εταιρειών. Το 1998, η Cisco εξαγόρασε τη Selsius Systems, μια επιχείρηση που ειδικευόταν στην τηλεφωνία μέσω του Διαδικτύου, γεγονός που συνέβαλε σημαντικά στην εδραίωση της Cisco σε ηγετική θέση στην τεχνολογία VoIP. Το 2006, η Cisco λάνσαρε το Tele Presence, ένα προηγμένο είδος τηλεδιάσκεψης που έχει σχεδιαστεί για να διευκολύνει την απρόσκοπτη αλληλεπίδραση μεταξύ ατόμων που βρίσκονται σε διαφορετικές γεωγραφικές περιοχές, αναπαράγοντας την εμπειρία της φυσικής παρουσίας στον ίδιο χώρο. Η επάρκεια της Cisco στη δικτύωση την έχει καταστήσει εξέχοντα προμηθευτή προϊόντων Internet of Things, όρος που συχνά αποδίδεται ότι επινοήθηκε στη Cisco. Ο Chambers αποσύρθηκε το 2015 λόγω της μετατόπισης της εστίασης της εταιρείας από το υλικό στο λογισμικό, όπως καταγράφεται από τους Entezami&Politis (2013).

Η Cisco Systems είναι ένας εξέχων παίκτης στον τομέα της δικτύωσης, γνωστός για τις υπερσύγχρονες λύσεις υλικού και λογισμικού που επιτρέπουν την ομαλή επικοινωνία μεταξύ συσκευών, συστημάτων και δικτύων. Οι μεταγωγείς και οι δρομολογητές της Cisco αποτελούν το θεμέλιο των υπηρεσιών της, συνεργαζόμενοι για τη ρύθμιση της κυκλοφορίας, τον έλεγχο της κίνησης δεδομένων και την εξασφάλιση της αποτελεσματικής και ασφαλούς λειτουργίας των δικτύων. Η μεταγωγή είναι η πράξη της δρομολόγησης πακέτων δεδομένων εντός ενός τοπικού δικτύου (LAN). Οι μεταγωγείς της Cisco διευκολύνουν τη μεταξύ τους επικοινωνία μεταξύ συσκευών εντός ενός ενιαίου δικτύου, όπως υπολογιστές, εκτυπωτές και διακομιστές. Οι μεταγωγείς της Cisco χειρίζονται αποτελεσματικά τις συγκρούσεις δεδομένων, ελαχιστοποιούν τη συμφόρηση του δικτύου και βελτιώνουν την ασφάλεια με τη χρήση VLANs (εικονικά τοπικά δίκτυα) και σύνθετων πρωτοκόλλων, όπως το πρωτόκολλο Spanning Tree Protocol (STP). Δρομολόγηση είναι η διαδικασία καθοδήγησης των δεδομένων σε διάφορα δίκτυα, όπως αυτά που υπάρχουν στα δίκτυα ευρείας περιοχής (WAN) (Macfarlane, 2007).

Οι δρομολογητές της Cisco αξιολογούν τα πακέτα δεδομένων, διαπιστώνουν τον προορισμό τους και επιλέγουν τη βέλτιστη διαδρομή μέσω του δικτύου. Αυτή η τεχνική είναι ζωτικής σημασίας για τη διευκόλυνση της επικοινωνίας μεταξύ διαφορετικών τμημάτων του

δικτύου και τη διασφάλιση της άμεσης και αξιόπιστης παράδοσης των δεδομένων στον προορισμό τους. Οι μεταγωγείς και οι δρομολογητές της Cisco λειτουργούν από κοινού για τη δημιουργία ενός ενοποιημένου και ολοκληρωμένου περιβάλλοντος δικτύου, ικανού να υποστηρίξει ένα ευρύ φάσμα εφαρμογών, από τη βασική ανταλλαγή δεδομένων έως τα περίπλοκα εταιρικά συστήματα. Παίζουν καθοριστικό ρόλο στη δημιουργία τοπολογιών δικτύου, στη βελτίωση της απόδοσης μέσω της ποιότητας υπηρεσιών (QoS) και στην εξασφάλιση υψηλής διαθεσιμότητας με τη χρήση πρωτοκόλλων όπως το HSRP (Hot Stand by Router Protocol) και το VRRP (Virtual Router Redundancy Protocol) (Carthern. Et. al., 2021).

Βασικές αρχές δικτύωσης

Ένα δίκτυο αποτελείται από δύο ή περισσότερους υπολογιστές που έχουν συνδεθεί, ώστε να μπορούν να επικοινωνούν μεταξύ τους και να μοιράζονται πόρους και αρχεία.

Μέρη ενός δικτύου

Ένα δίκτυο αποτελείται από πέντε βασικά στοιχεία: πελάτες, διακομιστές, κανάλια, συσκευές διασύνδεσης και λειτουργικά συστήματα (Dye, McDonald&Rufi, 2007).

Εξυπηρετητές

Οι εξυπηρετητές, γνωστοί και ως κεντρικοί υπολογιστές, είναι ανθεκτικές μηχανές που έχουν σχεδιαστεί για την αποθήκευση δεδομένων και εφαρμογών, επιτρέποντας στους χρήστες του δικτύου να έχουν πρόσβαση σε κοινόχρηστους πόρους.

Πελάτες

Οι πελάτες είναι οι υπολογιστές που λειτουργούν οι χρήστες του δικτύου για να συνδεθούν σε αυτούς τους διακομιστές και να χρησιμοποιήσουν πόρους όπως σκληρούς δίσκους και εκτυπωτές. Σήμερα, είναι σύνηθες για τους ιδιώτες να χρησιμοποιούν προσωπικούς υπολογιστές για τις ιδιωτικές, μη δικτυακές δραστηριότητές τους. Για παράδειγμα, στα εργαστήρια Tisch, οι προσωπικοί υπολογιστές λειτουργούν ως πελάτες, ενώ τα μηχανήματα που αποθηκεύουν δεδομένα του δίσκου ή και ιστοσελίδες λειτουργούν ως διακομιστές.

Κανάλια

Τα κανάλια, ή κυκλώματα δικτύου, είναι διαδρομές που διευκολύνουν τη μετάδοση δεδομένων μεταξύ διαφόρων δικτυακών υπολογιστών (πελατών και διακομιστών). Οι συσκευές διασύνδεσης είναι εξαρτήματα υλικού που επιτρέπουν συνδέσεις μεταξύ πελατών, διακομιστών και μερικές φορές άλλων δικτύων, επιτρέποντας την επικοινωνία μέσω του καναλιού. Παραδείγματα αποτελούν τα μόντεμ και οι κάρτες διασύνδεσης δικτύου. Το λειτουργικό σύστημα είναι λογισμικό που διαχειρίζεται και ελέγχει τις λειτουργίες του

δικτύου, παίζοντας έναν ρόλο παρόμοιο με αυτόν του λειτουργικού συστήματος σε ένα αυτόνομο μηχάνημα (Dye, McDonald&Rufi, 2007).

Κατανόηση των καναλιών δικτύου

Τα δικτυακά κανάλια ποικίλλουν ευρέως ως προς τους τύπους, τις ταχύτητες και τις δυνατότητες, με τέσσερις βασικές διαστάσεις να είναι ιδιαίτερα σημαντικές για την κατανόηση της λειτουργίας τους, όπως συζητήθηκε από τους Snyder και EngLee-Partridge το 2013.

1. Μέσο μετάδοσης
2. Ρυθμός μετάδοσης ή εύρος ζώνης
3. Κατευθυντικότητα
4. Τύπος σήματος

1. **Μέσο μετάδοσης:** Αυτό αναφέρεται στα φυσικά μέσα μέσω των οποίων τα σήματα ταξιδεύουν στο κανάλι δικτύου. Τα κανάλια δικτύου χρησιμοποιούν είτε ενσύρματα είτε ασύρματα μέσα.

- **Ενσύρματα μέσα ενημέρωσης**: Αυτή η κατηγορία περιλαμβάνει φυσική μετάδοση μέσω καλωδίων. Υπάρχουν τρεις βασικοί τύποι ενσύρματων μέσων:

- σύρμα συνεστραμμένου ζεύγους,
- ομοαξονικό καλώδιο
- και καλώδιο οπτικών ινών.

Τα συνεστραμμένα ζεύγη και τα ομοαξονικά καλώδια εξακολουθούν να χρησιμοποιούνται συνήθως, αν και υπάρχει μια αυξανόμενη στροφή προς τα καλώδια οπτικών ινών λόγω της υψηλότερης ταχύτητας και αποδοτικότητάς τους.

Τα καλώδια συνεστραμμένου ζεύγους αποτελούνται από ζεύγη χάλκινων καλωδίων συνεστραμμένα μεταξύ τους και χρησιμοποιούνται συνήθως σε τηλεφωνικές γραμμές και καλώδια Ethernet.

Τα ομοαξονικά καλώδια, με έναν μόνο χάλκινο αγωγό στον πυρήνα τους, χρησιμοποιούνται για υπηρεσίες καλωδιακής τηλεόρασης και διαδικτύου.

Τα καλώδια οπτικών ινών, από την άλλη πλευρά, χρησιμοποιούν σήματα φωτός για τη μετάδοση δεδομένων και προτιμώνται όλο και περισσότερο για την ικανότητά τους να μεταφέρουν μεγάλες ποσότητες δεδομένων σε πολύ υψηλές ταχύτητες σε μεγάλες αποστάσεις.

- **Ασύρματα μέσα:** Τα ασύρματα κανάλια μεταδίδουν πληροφορίες μέσω του αέρα και όχι μέσω φυσικών καλωδίων. Παραδείγματα περιλαμβάνουν το ραδιόφωνο, τα κυψελοειδή δίκτυα, τις συνδέσεις μικροκυμάτων και τις δορυφορικές επικοινωνίες. Η ασύρματη μετάδοση χρησιμοποιείται ευρέως σε τεχνολογίες όπως η τηλεοπτική μετάδοση, το ραδιόφωνο FM και οι ασύρματες υπηρεσίες διαδικτύου, αν και οι υποκείμενες τεχνολογίες μπορεί να διαφέρουν ελαφρώς ανάλογα με την εφαρμογή. Τα ασύρματα κανάλια προσφέρουν ευελιξία και ευκολία, ιδίως σε περιβάλλοντα όπου η τοποθέτηση καλωδίων είναι ανέφικτη ή αδύνατη.

2. **Ρυθμός μετάδοσης ή εύρος ζώνης:** Αναφέρεται στην ταχύτητα με την οποία τα δεδομένα μπορούν να μεταδοθούν μέσω ενός καναλιού δικτύου, συνήθως μετριέται σε bits ανά δευτερόλεπτο (bps). Το εύρος ζώνης είναι ένας κρίσιμος παράγοντας που καθορίζει πόσο γρήγορα μπορούν να σταλούν και να ληφθούν δεδομένα, επηρεάζοντας τη συνολική απόδοση του δικτύου. Ένας υψηλότερος ρυθμός μετάδοσης επιτρέπει την ταχύτερη μεταφορά δεδομένων, κάτι που είναι ιδιαίτερα σημαντικό σε δίκτυα υψηλής κυκλοφορίας όπου ανταλλάσσονται μεγάλες ποσότητες δεδομένων. Ο όρος "εύρος ζώνης" χρησιμοποιείται συχνά εναλλακτικά με τον όρο "ρυθμός μετάδοσης" για να περιγράψει αυτή την ταχύτητα.

3. **Κατευθυντικότητα:** Η κατεύθυνση με την οποία μπορούν να μεταδοθούν πληροφορίες μέσω ενός καναλιού είναι μια άλλη κρίσιμη διάσταση, η οποία καθορίζεται από το αν το κανάλι λειτουργεί σε λειτουργία simplex, half-duplex ή full-duplex.

-**Απλό:** Οι πληροφορίες ρέουν μόνο προς μία κατεύθυνση. Ένα παράδειγμα συστήματος simplex είναι ένα πληκτρολόγιο προς έναν υπολογιστή, όπου τα δεδομένα αποστέλλονται μόνο από το πληκτρολόγιο προς τον υπολογιστή.

- **Half-duplex:** Τα δεδομένα μπορούν να μεταδίδονται και προς τις δύο κατευθύνσεις, αλλά όχι ταυτόχρονα. Ένα γουόκι-τόκι λειτουργεί σε λειτουργία half-duplex, όπου το ένα μέρος πρέπει να περιμένει να τελειώσει την ομιλία του άλλου πριν απαντήσει.

- **Full-duplex:** Όπως παρατηρείται στις τηλεφωνικές συνομιλίες, όπου και τα δύο μέρη μπορούν να μιλούν και να ακούν ταυτόχρονα.

4. **Τύπος σήματος:** Τα κανάλια δικτύου μπορούν να μεταφέρουν είτε αναλογικά είτε ψηφιακά σήματα.

-**Αναλογικά σήματα**: Πρόκειται για συνεχή σήματα που μπορούν να λάβουν ένα ευρύ φάσμα τιμών. Ιστορικά, πολλά κανάλια επικοινωνίας, όπως οι τηλεφωνικές γραμμές και το ραδιόφωνο, σχεδιάστηκαν για να μεταφέρουν αναλογικά σήματα.

-**Ψηφιακά σήματα:** Αυτά είναι διακριτά και δυαδικά, καθιστώντας τα πιο φυσικά για τα δίκτυα υπολογιστών, όπου οι πληροφορίες αναπαρίστανται σε δυαδική μορφή. Τα ψηφιακά σήματα έχουν αντικαταστήσει σε μεγάλο βαθμό τα αναλογικά στα περισσότερα σύγχρονα συστήματα επικοινωνίας λόγω της συμβατότητάς τους με την ψηφιακή τεχνολογία υπολογιστών.

Κατηγοριοποίηση δικτύων επίσης με βάση τη γεωγραφική τους εμβέλεια

Τα δίκτυα κατηγοριοποιούνται επίσης με βάση τη γεωγραφική τους εμβέλεια, μια θεμελιώδη αλλά ευρεία μέθοδο ταξινόμησης. Σύμφωνα με τους Krichene και Boudriga (2008), υπάρχουν τέσσερις πρωταρχικοί τύποι δικτύων:

- **Τοπικά δίκτυα (LAN):** Τα δίκτυα αυτά περιορίζονται σε μια μικρή γεωγραφική περιοχή, συνήθως σε ένα μόνο κτίριο ή σε ένα σύμπλεγμα κοντινών κτιρίων. Τα τοπικά δίκτυα συνδέουν τους πελάτες και τους διακομιστές μέσω ενός κοινού καναλιού επικοινωνίας, επιτρέποντας τη λειτουργία του δικτύου σε κοντινή απόσταση.

- **Δίκτυα κορμού:** Αυτά είναι κανάλια υψηλής χωρητικότητας που συνδέουν πολλαπλά τοπικά δίκτυα μεταξύ τους, σχηματίζοντας τον πυρήνα μεγαλύτερων δικτύων. Παρέχουν την απαραίτητη υποδομή για την υποστήριξη εκτεταμένης κυκλοφορίας δεδομένων μεταξύ διασυνδεδεμένων LAN.

- **Μητροπολιτικά δίκτυα (MAN):** καλύπτουν μεγαλύτερη περιοχή από τα LAN, όπως μια πανεπιστημιούπολη ή ένα πανεπιστήμιο. Παρέχουν δικτυακή συνδεσιμότητα σε μια μητροπολιτική περιοχή, γεφυρώνοντας πολλαπλά τοπικά δίκτυα εντός μιας πόλης ή μιας περιοχής.

- **Δίκτυα ευρείας περιοχής (WAN):** Τα WAN εκτείνονται σε τεράστιες γεωγραφικές περιοχές, όπως χώρες ή ηπείρους. Συνδέουν πολλαπλά LAN και MAN, διευκολύνοντας την επικοινωνία σε μεγάλες αποστάσεις και υποστηρίζοντας τις ανάγκες παγκόσμιας δικτύωσης.

Πρωτόκολλα δικτύωσης

Τα περισσότερα δίκτυα λειτουργούν μεταδίδοντας πληροφορίες με τη μορφή πακέτων, όπου τα αρχικά δεδομένα χωρίζονται σε μικρότερες μονάδες και αποστέλλονται διαδοχικά. Αυτά τα πακέτα επανασυναρμολογούνται στη συνέχεια στον προορισμό για την ανακατασκευή των αρχικών δεδομένων. Κάθε πακέτο αποτελείται από δυαδικά ψηφία. Ωστόσο, όταν τα πακέτα διανύουν μεγάλες αποστάσεις σε πολλαπλά δίκτυα, ενδέχεται να αντιμετωπίσουν προβλήματα όπως σφάλματα μετάδοσης, όπου τα δεδομένα αλλοιώνονται κατά τη διαδικασία. Για να εξασφαλιστεί η ακριβής, αποτελεσματική και αξιόπιστη μετάδοση δεδομένων, τα δίκτυα υπολογιστών βασίζονται σε πρωτόκολλα δικτύωσης - σύνολα κανόνων που έχουν σχεδιαστεί για τη διαχείριση αυτών των διαδικασιών. Αυτά τα πρωτόκολλα είναι κυρίως υπεύθυνα για λειτουργίες τόσο στο επίπεδο δικτύου όσο και στο επίπεδο σύνδεσης δεδομένων, με κάθε επίπεδο να διέπεται από συγκεκριμένους κανόνες (Salman&Jain, 2016).

Τα πρωτόκολλα επιπέδου δικτύου, γνωστά και ως πρωτόκολλα επιπέδου 3, διεκπεραιώνουν τρεις βασικές εργασίες σε ένα δίκτυο (Bonaventure, 2024):

- **Συσκευασία πακέτων:** Διάσπαση των πληροφοριών σε πακέτα και επανασυναρμολόγησή τους στο άκρο λήψης.

- **Διεύθυνση:** Προσδιορισμός του υπολογιστή προορισμού και του δικτύου για τα πακέτα.

- **Δρομολόγηση:** Καθορισμός της βέλτιστης διαδρομής για να φτάσουν τα πακέτα στον προορισμό τους.

Το **TCP/IP** είναι το πιο συχνά χρησιμοποιούμενο πρωτόκολλο επιπέδου δικτύου σήμερα, αν και το IPX/SPX χρησιμοποιήθηκε επίσης ευρέως στο παρελθόν.

πρωτόκολλα επιπέδου 2

Τα πρωτόκολλα επιπέδου σύνδεσης δεδομένων, ή πρωτόκολλα επιπέδου 2, διαχειρίζονται τις ακόλουθες εργασίες (Bonaventure, 2024):

- **Οριοθέτηση:** Προσδιορισμός της αρχής και του τέλους ενός πακέτου.

- **Έλεγχος σφαλμάτων:** Ανίχνευση και διόρθωση σφαλμάτων μετάδοσης.

- **Πρόσβαση στο κανάλι:** Διαχείριση του πότε ένας συγκεκριμένος πελάτης ή διακομιστής μπορεί να έχει πρόσβαση στο κανάλι επικοινωνίας.

Υπάρχουν διάφορα πρωτόκολλα επιπέδου σύνδεσης δεδομένων, με το Ethernet να είναι το πιο διαδεδομένο σε οργανισμούς και ιδρύματα. Το Ethernet ήταν το πρώτο ευρέως υιοθετημένο πρωτόκολλο δικτύου και η ιστορία του είναι σημαντική. Η έρευνα για την προέλευσή του, συμπεριλαμβανομένων λεπτομερειών σχετικά με τον εφευρέτη του, τον τόπο όπου αναπτύχθηκε και το έτος δημιουργίας του, θα παρείχε πολύτιμες πληροφορίες.

Ένα άλλο ευρέως χρησιμοποιούμενο πρωτόκολλο είναι το σύστημα tokenring της IBM. Κατά τη σύνδεση σε δίκτυα από το σπίτι, συνήθως μέσω τηλεφωνικών γραμμών, συναντώνται συχνά τα πρωτόκολλα σύνδεσης δεδομένων SLIP (Serial Line Internet Protocol) ή PPP (Point-to-Point Protocol). Αυτά τα πρωτόκολλα διασφαλίζουν ότι ακόμη και σε μεγάλες αποστάσεις και δυνητικά αναξιόπιστες συνδέσεις, τα δεδομένα μεταδίδονται με ακρίβεια και αποτελεσματικότητα (Bonaventure, 2024).

Τοπολογίες δικτύων

Η τοπολογία του δικτύου αναφέρεται στη φυσική διάταξη του τρόπου με τον οποίο συνδέονται οι πελάτες και οι διακομιστές, δημιουργώντας το πλαίσιο για τις αλληλεπιδράσεις τους.

Οι τρεις κύριες τοπολογίες δικτύου είναι

- ο αστέρας,
- ο δίαυλος
- και ο δακτύλιος.

Η τοπολογία σχετίζεται στενά με την πρόσβαση στο κανάλι, όπως σημειώνεται στα πρωτόκολλα επιπέδου 2, επειδή ο τρόπος με τον οποίο οι υπολογιστές συνδέονται σε ένα

κανάλι επηρεάζει την ικανότητά τους να έχουν πρόσβαση σε αυτό. Κατά συνέπεια, κάθε πρωτόκολλο επιπέδου 2 απαιτεί μια συγκεκριμένη τοπολογία για την πρόσβαση στο κανάλι (Haddadietal., 2008).

- **Η τοπολογία διαύλου** είναι η πιο διαδεδομένη διαμόρφωση LAN, όπου όλοι οι πελάτες, οι διακομιστές και οι κοινόχρηστοι πόροι συνδέονται σε ένα ενιαίο κανάλι, γνωστό ως δίαυλος, το οποίο εκτείνεται σε ολόκληρο το δίκτυο. Αυτή η τοπολογία χρησιμοποιείται σε όλα τα δίκτυα Ethernet.

- **Η τοπολογία δακτυλίου** χαρακτηρίζεται από ένα σχεδιασμό δικτύου όπου όλοι οι υπολογιστές σε ένα τοπικό δίκτυο συνδέονται σε ένα κλειστό κύκλωμα, με κάθε υπολογιστή να συνδέεται άμεσα με τον άμεσο γείτονά του. Τα δίκτυα που χρησιμοποιούν το πρωτόκολλο tokenring χρησιμοποιούν αυτή την τοπολογία.

- **Η τοπολογία αστέρα** περιλαμβάνει μια ρύθμιση όπου κάθε πελάτης συνδέεται απευθείας σε έναν κεντρικό διακομιστή μέσω ενός αποκλειστικού καναλιού. Ενώ αυτή η διαμόρφωση ήταν κοινή κατά την εποχή των κεντρικών υπολογιστών και χρησιμοποιείται ακόμη σε ορισμένα δίκτυα ευρείας περιοχής, δεν απαντάται συνήθως σε τοπικά δίκτυα (Haddadietal., 2008).

Μόντεμ και κάρτες Ethernet

Οι συσκευές διασύνδεσης δικτύου είναι ζωτικής σημασίας σε κάθε τοπικό δίκτυο (LAN), καθώς επιτρέπουν τις συνδέσεις μεταξύ πελατών και διακομιστών. Η κάρτα διασύνδεσης δικτύου (NIC), κοινώς γνωστή ως κάρτα Ethernet, είναι η πιο ευρέως χρησιμοποιούμενη συσκευή σε επιχειρηματικά και ακαδημαϊκά τοπικά δίκτυα. Αυτό οφείλεται στο γεγονός ότι τα περισσότερα από αυτά τα δίκτυα βασίζονται στο Ethernet, με το τοπικό δίκτυο να αναφέρεται συχνά απλώς ως Ethernet. Για τους οικιακούς χρήστες, το μόντεμ είναι η κύρια συσκευή διασύνδεσης δικτύου που χρησιμοποιείται για τη σύνδεση με τον πάροχο υπηρεσιών Διαδικτύου ή τα διαδικτυακά τους δίκτυα.

Η κύρια λειτουργία ενός μόντεμ είναι η μετατροπή ψηφιακών δεδομένων από υπολογιστές σε αναλογικά σήματα για τη μετάδοση μέσω τηλεφωνικών γραμμών και αντίστροφα (Kessler, 2015). Οι παραδοσιακές ταχύτητες μόντεμ κυμαίνονται σήμερα από

14,4 Kbps έως 53,3 Kbps. Ωστόσο, λόγω περιορισμών, δεν είναι εφικτή η λήψη δεδομένων μέσω μιας αναλογικής τηλεφωνικής γραμμής με ταχύτητες που υπερβαίνουν τα 53,3 Kbps ή η αποστολή δεδομένων με ταχύτητες υψηλότερες από 33,6 Kbps(Kessler, 2015).

- Τα καλωδιακά μόντεμ είναι συσκευές που χρησιμοποιούνται με οικιακά τηλεοπτικά καλώδια για την παροχή ευρυζωνικής πρόσβασης στο διαδίκτυο. Μόλις ο πάροχος καλωδιακής τηλεόρασης αναβαθμίσει το δίκτυο και εγκαταστήσει ένα καλωδιακό μόντεμ στο σπίτι του χρήστη, μπορεί να χρησιμοποιηθεί μια τυπική κάρτα Ethernet για την επίτευξη πρόσβασης στο διαδίκτυο υψηλής ταχύτητας. Τα καλωδιακά μόντεμ μπορούν να προσφέρουν εύρος ζώνης έως και 10 Mbps, αλλά σε περιοχές με πολλούς χρήστες, το εύρος ζώνης μπορεί να μειωθεί σημαντικά όταν πολλά άτομα συνδέονται ταυτόχρονα στο διαδίκτυο.

- Το DSL (Digital Subscriber Lines) είναι η εναλλακτική λύση του κλάδου των τηλεπικοινωνιών στα καλωδιακά μόντεμ. Η τεχνολογία DSL συνδέει ένα μόντεμ DSL σε μια τυπική αναλογική τηλεφωνική γραμμή, δημιουργώντας ένα ψηφιακό κανάλι υψηλής ταχύτητας, προσβάσιμο μέσω μιας κάρτας Ethernet. Το DSL είναι διαθέσιμο μόνο σε περιοχές όπου οι πάροχοι τηλεφωνίας έχουν αναβαθμίσει τα δίκτυά τους. Το μέγιστο εύρος ζώνης που μπορεί να επιτύχει μια κατοικία εξαρτάται σε μεγάλο βαθμό από την απόστασή της από το πλησιέστερο τηλεφωνικό κεντρικό γραφείο. Επί του παρόντος, το DSL προσφέρει ταχύτητες λήψης έως και 7 Mbps, με σταθερή απόδοση ακόμη και όταν πολλοί χρήστες βρίσκονται κοντά (Majumdar, 2018).

Σύγκλιση και οικιακή ευρυζωνικότητα

Όπως αναφέρθηκε, διάφοροι τύποι μέσων όπως κείμενο, εικόνες, μουσική και βίντεο μπορούν να μετατραπούν σε ψηφιακά δεδομένα. Αυτό επιτρέπει στους οικιακούς χρήστες να χρησιμοποιούν θεωρητικά ένα ενιαίο ψηφιακό κανάλι επικοινωνίας για πρόσβαση στο διαδίκτυο, τηλεφωνικές κλήσεις και τηλεοπτικές εκπομπές. Η σύγκλιση των μέσων αναφέρεται στη συγχώνευση των επικοινωνιών δεδομένων, φωνής και βίντεο σε ένα ενιαίο κανάλι (Paul, 2011).

Ωστόσο, υπάρχουν τρεις κύριες προκλήσεις που αντιμετωπίζει μια εταιρεία όταν προσπαθεί να δημιουργήσει ένα ενιαίο και ολοκληρωμένο κανάλι για την άμεση παροχή υπηρεσιών στα σπίτια των ανθρώπων (Majumdar, 2018):

- απαίτηση για υψηλό εύρος ζώνης
- πρόβλημα του τελευταίου μιλίου
- παλαιά αναλογικά δίκτυα

-Η απαίτηση για υψηλό εύρος ζώνης προκύπτει λόγω της μετατροπής της φωνής και του βίντεο σε ψηφιακά δεδομένα, η οποία απαιτεί σημαντικό αριθμό bits για την αναπαράσταση κάθε δευτερολέπτου του ήχου ή του βίντεο. Επομένως, εάν κάποιος σκοπεύει να χρησιμοποιήσει ένα μοναχικό ψηφιακό κανάλι, είναι απαραίτητο το κανάλι αυτό να διαθέτει σημαντικά μεγάλο εύρος ζώνης.

-Το πρόβλημα του τελευταίου μιλίου αναφέρεται στο σημαντικό κόστος που συνδέεται με τη δημιουργία νέων καναλιών για να φτάσει σε κάθε νοικοκυριό, καθιστώντας το οικονομικά επαχθές για κάθε μεμονωμένη επιχείρηση. Το κόστος των ίδιων των καλωδίων είναι σχετικά ασήμαντο. Η κύρια πρόκληση έγκειται στην επίπονη διαδικασία εσκαφής στην άκρη του δρόμου, στην εγκατάσταση των καλωδίων για τη σύνδεση κάθε νοικοκυριού, στην απόκτηση των απαραίτητων αδειών (όπως το δικαίωμα διέλευσης) και στο να πειστούν οι κάτοικοι να επιτρέψουν την πρόσβαση στα σπίτια τους για την εγκατάσταση των καλωδίων. Το ζήτημα του "τελευταίου μιλίου" αναφέρεται στο σημαντικό κόστος που συνεπάγεται η γρήγορη εγκατάσταση νέων ψηφιακών καλωδίων στις κατοικίες των ανθρώπων.

-Τα παλαιά αναλογικά δίκτυα αναφέρονται στα σημερινά κανάλια που παρέχουν υπηρεσίες στα νοικοκυριά, όπως οι γραμμές καλωδιακής τηλεόρασης και τα τηλεφωνικά καλώδια. Τα δίκτυα αυτά έχουν κατασκευαστεί για να διαχειρίζονται αναλογικά σήματα, και αυτό ισχύει τόσο για το δίκτυο μετάδοσης καλωδιακής τηλεόρασης όσο και για το τοπικό τηλεφωνικό δίκτυο. Επιπλέον, το δίκτυο καλωδιακής τηλεόρασης αναπτύχθηκε αρχικά για μονόδρομη επικοινωνία, όταν το ίδιο περιεχόμενο μεταδίδεται σε διαφορετικά νοικοκυριά. Είναι σαφές ότι αυτός ο τύπος δικτύου δεν είναι κατάλληλος για πρόσβαση στο Διαδίκτυο ή για τηλεφωνικές κλήσεις, καθώς απαιτούν αμφίδρομη επικοινωνία, όπου τόσο ο αποστολέας όσο και ο παραλήπτης ανταλλάσσουν ξεχωριστές πληροφορίες.

Για να αντιμετωπίσουν την πρόκληση του περιορισμένου εύρους ζώνης, οι πάροχοι

τηλεπικοινωνιών και καλωδιακής τηλεόρασης αναβαθμίζουν τις υποδομές τους με τη μετάβαση από την αναλογική στην ψηφιακή τεχνολογία, η οποία περιλαμβάνει την αντικατάσταση παλαιότερων γραμμών και εξοπλισμού με σύγχρονες. Παρά το συνεχιζόμενο ζήτημα των περιορισμών του εύρους ζώνης, έχουν εμφανιστεί δύο προηγμένες ψηφιακές τεχνολογίες επικοινωνίας υψηλού εύρους ζώνης, οι οποίες γίνονται όλο και πιο δημοφιλείς για οικιακή πρόσβαση: τα καλωδιακά μόντεμ και το DSL (ψηφιακή συνδρομητική γραμμή). Συλλογικά, οι υπηρεσίες αυτές είναι γνωστές ως οικιακή ευρυζωνικότητα (Paul, 2011).

Χαρακτηριστικά δικτύωσης της Cisco

Ίδρυση της εταιρίας

Η Cisco Systems, Inc. αποτελεί έναν αμερικανικό πολυεθνικό όμιλο επιχειρήσεων ψηφιακής τεχνολογίας επικοινωνιών με έδρα το Σαν Χοσέ της Καλιφόρνιας. Ιδρύθηκε τον Δεκέμβριο του 1984 από τους Leonard Bosack και Sandy Lerner, δύο επιστήμονες πληροφορικής του Πανεπιστημίου του Στάνφορντ, οι οποίοι είχαν συμβάλει καθοριστικά στη σύνδεση υπολογιστών στο Στάνφορντ. Πρωτοστάτησαν στην ιδέα ενός τοπικού δικτύου (LAN) που χρησιμοποιείται για τη σύνδεση απομακρυσμένων υπολογιστών μέσω ενός συστήματος δρομολογητών πολλαπλών πρωτοκόλλων. Η εταιρεία εισήχθη στο χρηματιστήριο το 1990 και μέχρι το τέλος της του 2000 ξεπέρασε την Microsoft κι’έγινε ,η πιο πολύτιμη εταιρεία στον κόσμο (Lucas, 2009).

Εικόνα 1 λογότυπο της cisco

Ποιος ήταν ο στόχος της :

Στόχος της εταιρίας ήταν να αναπτύσσει και κατασκευάζει υλικό δικτύωσης, λογισμικό, τηλεπικοινωνιακό εξοπλισμό και άλλες υπηρεσίες και προϊόντα υψηλής τεχνολογίας.: όπως τη δικτύωση (συμπεριλαμβανομένων των Ethernet, οπτικών, ασύρματων και κινητικότητας), την ασφάλεια, τη συνεργασία (συμπεριλαμβανομένων φωνής, βίντεο και δεδομένων), το κέντρο δεδομένων και το Διαδίκτυο των πραγμάτων

Που απευθύνεται :

Απευθύνεται σε συγκεκριμένες τεχνολογικές αγορές, όπως το Διαδίκτυο των πραγμάτων (IoT), η ασφάλεια τομέων, η τηλεδιάσκεψη και η διαχείριση ενέργειας, με προϊόντα όπως τα Webex, OpenDNS, Jabber, Duo Security, Silicon One και Jasper (Cisco Networking Academy, 2014). Τα προϊόντα και οι υπηρεσίες της επικεντρώνονται σε τρία τμήματα της αγοράς τις μεγάλες επιχειρήσεις, τους παρόχους υπηρεσιών και τις μεσαίες και μικρές επιχειρήσεις. Τις τελευταίες τρεις δεκαετίες ,οι υπηρεσίες της την έχουν κάνει πολύ δημοφιλή στην περιοχή της Ασίας και είναι ο κυρίαρχος προμηθευτής στην αγορά της Αυστραλίας

Βασικές έννοιες του εξοπλισμού δικτύωσης

Υλικό δικτύωσης μεταγωγείς ,δρομολογητές

Στον πυρήνα κάθε δικτύου, είτε είναι μια μικρή οικιακή εγκατάσταση είτε ένα τεράστιο εταιρικό σύστημα, υπάρχουν δύο κρίσιμοι τύποι συσκευών: οι μεταγωγείς και οι δρομολογητές. Αυτές οι συσκευές είναι οι συνδετικοί κρίκοι της δικτύωσης, επιτρέποντας την επικοινωνία μεταξύ υπολογιστών, διακομιστών και διαδικτύου

Κατηγορίες των μεταγωγέων

Το χαρτοφυλάκιο της Cisco περιλαμβάνει μια ευρεία γκάμα μεταγωγέων, από μη διαχειριζόμενους μεταγωγείς κατάλληλους για μικρές επιχειρήσεις έως εξαιρετικά σύνθετους διαχειριζόμενους σχεδιασμένους για μεγάλες επιχειρήσεις και κέντρα δεδομένων. Η

κατανόηση των συγκεκριμένων χαρακτηριστικών και των προβλεπόμενων περιπτώσεων χρήσης κάθε τύπου μεταγωγέα είναι ζωτικής σημασίας για το σχεδιασμό ενός αποτελεσματικού, επεκτάσιμου και ασφαλούς δικτύου.

Μη διαχειριζόμενοι μεταγωγείς

Επισκόπηση: Οι μη διαχειριζόμενοι μεταγωγείς της Cisco είναι το πιο απλό είδος μεταγωγέων, προσφέροντας βασική συνδεσιμότητα χωρίς την ανάγκη διαμόρφωσης. Αποτελούν συσκευές plug-and-play, οι οποίες είναι ιδανικές για μικρά γραφεία, οικιακά γραφεία ή οποιοδήποτε περιβάλλον όπου απαιτείται βασική συνδεσιμότητα δικτύου χωρίς την ανάγκη προηγμένων λειτουργιών.

Περιπτώσεις χρήσης: Σύνδεση μικρού αριθμού συσκευών σε ένα τοπικό δίκτυο, όπου η απλότητα και το χαμηλό κόστος έχουν προτεραιότητα έναντι της προσαρμογής.

Διαχειριζόμενοι μεταγωγείς

Επισκόπηση: Οι διαχειριζόμενοι μεταγωγείς προσφέρουν υψηλότερο επίπεδο ελέγχου του δικτύου. Επιτρέπουν τη διαμόρφωση, τη διαχείριση και την παρακολούθηση του δικτύου, επιτρέποντας τη βελτιστοποίηση της απόδοσης και της ασφάλειας του δικτύου. Η Cisco.

Περιπτώσεις χρήσης:

- **Υποστήριξη VLAN**: Εξασφαλίζει τη δημιουργία εικονικών LAN για την τμηματοποίηση της κυκλοφορίας του δικτύου και τη βελτίωση της ασφάλειας και της απόδοσης.
- **Ποιότητα υπηρεσίας (QoS)**: Ιεραρχεί την κυκλοφορία για να διασφαλίσει ότι οι κρίσιμες εφαρμογές λαμβάνουν το εύρος ζώνης που χρειάζονται.
- **Προηγμένα χαρακτηριστικά ασφαλείας**: Περιλαμβάνει λίστες ελέγχου πρόσβασης (ACL), ασφάλεια θυρών και άλλα για την προστασία του δικτύου από μη εξουσιοδοτημένη πρόσβαση.

  Μπορούν να χρησιμοποιηθούν για επιχειρήσεις όλων των μεγεθών που χρειάζονται προσαρμοσμένες ρυθμίσεις δικτύου, ενισχυμένη ασφάλεια και δυνατότητα χειρισμού πολύπλοκων αρχιτεκτονικών δικτύου (Cisco Networking Academy, 2014).

Έξυπνοι μεταγωγείς

Επισκόπηση: Οι έξυπνοι μεταγωγείς, γνωστοί και ως ελαφρώς διαχειριζόμενοι μεταγωγείς, προσφέρουν μια μέση λύση μεταξύ των μη διαχειριζόμενων και των διαχειριζόμενων μεταγωγέων. Παρέχουν κάποιο επίπεδο διαχείρισης χωρίς την πολυπλοκότητα και το κόστος των πλήρως διαχειριζόμενων μεταγωγέων.

Χαρακτηριστικά: Συνήθως περιέχουν ορισμένες λειτουργίες VLAN και QoS, βασικές λειτουργίες ασφαλείας και εύχρηστες διεπαφές διαχείρισης.

Περιπτώσεις χρήσης: Κατάλληλες για μικρές και μεσαίες επιχειρήσεις (MME) που χρειάζονται περισσότερο έλεγχο στο δίκτυό τους από ό,τι προσφέρουν οι μη διαχειριζόμενοι μεταγωγείς, αλλά δεν απαιτούν όλα τα προηγμένα χαρακτηριστικά των διαχειριζόμενων μεταγωγέων (Cisco Networking Academy, 2014).

Ο 3850-X χρησιμοποιείται επίσης στο επίπεδο πυρήνα μικρών επιχειρήσεων χωρίς επίπεδο διανομής και χρησιμοποιείται συχνά σε μεγάλα εταιρικά δίκτυα στο επίπεδο πρόσβασης για να παρέχει πλεονασμό και πλήρεις δυνατότητες επιπέδου 3 (KvitoslavaObelovskaetal., 2023).

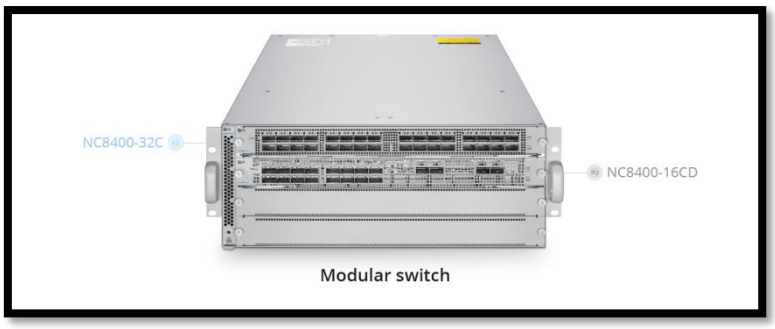
Στο επίπεδο διανομής της επιχείρησης, χρησιμοποιούνται τόσο σταθερά όσο και αρθρωτά μεταγωγείς, ανάλογα με τις ειδικές απαιτήσεις του δικτύου πανεπιστημιούπολης.

Διακόπτες με δυνατότητα στοίβαξης

Επισκόπηση: Οι στοιβαζόμενοι μεταγωγείς έχουν σχεδιαστεί για να ομαδοποιούνται ή να «στοιβάζονται» φυσικά και λογικά. Αυτό τους επιτρέπει να λειτουργούν ως ενιαία οντότητα, απλοποιώντας τη διαχείριση και την επεκτασιμότητα(η πρόσθεση μεταγωγέων στην στοίβα ώστε να επεκταθεί η χωρητικότητα του δικτύου).

Περιπτώσεις χρήσης: Ιδανικές για αναπτυσσόμενες επιχειρήσεις που προβλέπουν ότι πρέπει να επεκτείνουν την υποδομή του δικτύου τους καθώς αναπτύσσονται (Cisco Networking Academy, 2014).

αρθρωτοί μεταγωγείς [Modular Switches]



Εικόνα 2 Modular switch

Επισκόπηση: Τα modular switches προσφέρουν το υψηλότερο επίπεδο ευελιξίας και επεκτασιμότητας. Αποτελούνται από ένα πλαίσιο στο οποίο μπορούν να εισαχθούν διαφορετικές μονάδες, παρέχοντας διάφορους τύπους επιλογών συνδεσιμότητας και υπηρεσιών δικτύου. Έχουν υψηλή επεκτασιμότητα και ευελιξία καθώς και υψηλές αποδόσεις σχεδιασμένοι για την υποστήριξη των πιο απαιτητικών δικτύων. Οι αρθρωτοί μεταγωγείς, όπως οι σειρές CiscoCatalyst 6500 και 6800, χρησιμοποιούνται συνήθως στο επίπεδο πυρήνα των επιχειρηματικών δικτύων. Ο Catalyst 6800, ειδικότερα, διαθέτει αρθρωτή σχεδίαση που επιτρέπει την ξεχωριστή εγκατάσταση μεμονωμένων στοιχείων, όπως η μονάδα επεξεργασίας δρομολόγησης/επιτήρησης, οι μονάδες Ethernet, μέσα στο πλαίσιο. Αυτή η αρθρωτή προσέγγιση προσφέρει ευελιξία και τη δυνατότητα προσαρμογής του μεταγωγέα για υψηλή διαθεσιμότητα ανάλογα με τις ανάγκες.

Περιπτώσεις χρήσης: Κατάλληλες για μεγάλες επιχειρήσεις και κέντρα δεδομένων όπου οι απαιτήσεις δικτύου είναι υψηλές και μπορούν να αλλάξουν γρήγορα, απαιτώντας μια προσαρμόσιμη λύση δικτύωσης.

Μεταγωγείς Cisco αναλυτικά

Οικογένεια διακοπτών Cisco Catalyst 6500

Εικόνα 3 Οικογένεια διακοπτών Cisco Catalyst 6500

Η οικογένεια μεταγωγέων Cisco Catalyst 6500 είναι οι πιο δημοφιλείς μεταγωγείς που παρήγαγε ποτέ η Cisco. Βρίσκονται σε μεγάλη ποικιλία εγκαταστάσεων, όχι μόνο σε πανεπιστημιουπόλεις, κέντρα δεδομένων και δίκτυα κορμού, αλλά και σε ανάπτυξη υπηρεσιών, WAN, υποκαταστημάτων κ.ο.κ. τόσο σε δίκτυα επιχειρήσεων όσο και σε δίκτυα παρόχων υπηρεσιών.

Για τους σκοπούς του CCNPSWITCH, οι μεταγωγείς της οικογένειας Cisco Catalyst 6500 συνοψίζονται ως εξής (Froom, 2010):

- Κλιμακούμενο αρθρωτό μεταγωγέα έως και 13 υποδοχές

- Υποστηρίζει διασυνδέσεις Ethernet έως και 1610 Gigabit ανά υποδοχή σε μοντέλο υπερσυνδρομής

- Εύρος ζώνης έως και 80 Gbps ανά υποδοχή σε υλικό τρέχουσας γενιάς

- Υποστηρίζει CiscoIOS με πληθώρα χαρακτηριστικών μεταγωγής επιπέδου 2 και επιπέδου 3

- Υποστηρίζει προαιρετικά έως και χαρακτηριστικά επιπέδου 7 με εξειδικευμένες μονάδες

- Ενσωματωμένα πλεονάζοντα και υψηλής διαθεσιμότητας τροφοδοτικά, ανεμιστήρες και μηχανικοί επόπτη

- Υποστηρίζει Layer 3 Non-Stop Forwarding (NSF), με την οποία οι ομότιμοι δρομολόγησης διατηρούνται κατά τη διάρκεια μιας εναλλαγής του επόπτη.

- Η δυνατότητα επιστροφής προς τα πίσω και η προστασία των επενδύσεων έχουν οδηγήσει σε μακρύ κύκλο ζωής

Οικογένεια μεταγωγέων Cisco Catalyst 4500

Εικόνα 4 Οικογένεια μεταγωγέων Cisco Catalyst 4500

Η οικογένεια μεταγωγέων Cisco Catalyst 4500 είναι ένας εξαιρετικά δημοφιλής αρθρωτός μεταγωγέας που συναντάται σε πολλά πανεπιστημιακά δίκτυα στο επίπεδο διανομής ή σε κατεστραμμένα δίκτυα πυρήνα μικρών και μεσαίων δικτύων. Οι σχεδιασμοί κολλημένου πυρήνα συνδυάζουν τα στρώματα πυρήνα και διανομής σε μια ενιαία περιοχή. Το Catalyst 4500 είναι ένα βήμα κάτω από το Catalyst 6500, αλλά υποστηρίζει ένα ευρύ φάσμα χαρακτηριστικών Layer 2 και Layer 3.

Συνοπτικά, οι μεταγωγείς της οικογένειας Catalyst 4500 της Cisco συνοψίζονται ως εξής (Mcquerryetal., 2009):

- Κλιμακούμενος μεταγωγέας μονάδων με έως και 10 υποδοχές

- Υποστηρίζει πολλαπλές διασυνδέσεις 10 Gigabit Ethernet ανά υποδοχή

- Υποστηρίζει CiscoIOS

- Υποστηρίζει τόσο μεταγωγή επιπέδου 2 όσο και μεταγωγή επιπέδου 3

- Υποστηρίζει προαιρετικά ενσωματωμένα εφεδρικά και υψηλής διαθεσιμότητας τροφοδοτικά και μηχανές supervisor

Οικογένεια μεταγωγέων Cisco Catalyst 4948G, 3750 και 3560

Εικόνα5 Οικογένεια μεταγωγέων Cisco Catalyst 4948G, 3750 και 3560

Οι μεταγωγείς της οικογένειας Cisco Catalyst 4948G, 3750 και 3560 είναι δημοφιλείς μεταγωγείς που χρησιμοποιούνται σε πανεπιστημιακά δίκτυα για σενάρια σταθερών θυρών, τις περισσότερες φορές στο επίπεδο πρόσβασης. Αυτοί οι μεταγωγείς συνοψίζονται ως εξής (Mcquerryetal., 2009):

- Διατίθενται σε διάφορες διαμορφώσεις σταθερών θυρών με έως και 48 θύρες στρώματος πρόσβασης 1 Gbps και 4 διασυνδέσεις 10-Gigabit Ethernet για ανερχόμενες συνδέσεις στο στρώμα διανομής

- Υποστηρίζει CiscoIOS

- Υποστηρίζει μεταγωγή τόσο επιπέδου 2 όσο και επιπέδου 3

- Δεν έχει σχεδιαστεί με πλεονάζον υλικό

Οικογένεια μεταγωγέων Cisco Catalyst 2000

Εικόνα 6 Οικογένεια μεταγωγέων Cisco Catalyst *2000*

Η οικογένεια μεταγωγέων Cisco Catalyst 2000 είναι μεταγωγείς μόνο επιπέδου 2, οι οποίοι είναι ικανοί για λίγες λειτουργίες επιπέδου 3 εκτός από τη δρομολόγηση επιπέδου 3. Αυτές οι λειτουργίες βρίσκονται συχνά στο επίπεδο πρόσβασης σε πανεπιστημιακά δίκτυα. Αυτοί οι μεταγωγείς συνοψίζονται ως εξής (Mcquerryetal., 2009):

- Διατίθενται σε διάφορες διαμορφώσεις σταθερών θυρών με έως και 48 θύρες στρώματος πρόσβασης 1 Gbps και πολλαπλές ανερχόμενες συνδέσεις Ethernet 10 Gigabit

- Υποστηρίζει το CiscoIOS

- Υποστηρίζει μόνο μεταγωγή επιπέδου 2

- Δεν έχει σχεδιαστεί με πλεονάζον υλικό

Οικογένεια μεταγωγέων Nexus 7000

Εικόνα7 Οικογένεια μεταγωγέων Nexus 7000

Η οικογένεια μεταγωγέων Nexus 7000 είναι οι κορυφαίοι μεταγωγείς κέντρων δεδομένων της Cisco. Το προϊόν κυκλοφόρησε το 2008 και, ως εκ τούτου, το λογισμικό Nexus 7000 δεν υποστηρίζει ακόμη όλα τα χαρακτηριστικά του CiscoIOS. Παρ' όλα αυτά, το Nexus 7000 συνοψίζεται ως εξής (Mcquerryetal., 2009):

- Αρθρωτός μεταγωγέας με έως και 18 υποδοχές

- Υποστηρίζει έως και 230 Gbps ανά υποδοχή Υποστηρίζει NexusOS (NX-OS)

- Το πλαίσιο των 10 υποδοχών βασίζεται στη ροή αέρα από εμπρός προς τα πίσω

- Υποστηρίζει εφεδρικές μηχανές supervisor, ανεμιστήρες και τροφοδοτικά

Οικογένεια μεταγωγέων Nexus 5000 και 2000

Εικόνα8 Οικογένεια μεταγωγέων Nexus 5000 και 2000

https://www.cisco.com/c/en/us/support/sw 4

Η οικογένεια μεταγωγέων Nexus 5000 και 2000 είναι μεταγωγείς χαμηλής καθυστέρησης που έχουν σχεδιαστεί για εγκατάσταση στο επίπεδο πρόσβασης του κέντρου δεδομένων. Αυτά τα μεταγωγείς είναι σήμερα μεταγωγείς μόνο επιπέδου 2, αλλά υποστηρίζουν μεταγωγή cut-through για χαμηλή καθυστέρηση. Οι μεταγωγείς Nexus 5000 έχουν σχεδιαστεί για εφαρμογές 10-GigabitEthernet και υποστηρίζουν επίσης Fibre Channel over Ethernet (FCOE) (Mcquerryetal., 2009).

Δρομολογητές:

Τύποι δρομολογητών Cisco

Δρομολογητές: Οι δρομολογητές είναι οι φύλακες πύλης μεταξύ του τοπικού σας δικτύου και του ευρύτερου διαδικτύου (ή μεταξύ πολλαπλών τοπικών δικτύων σε μεγαλύτερα δίκτυα). Λειτουργούν στο επίπεδο δικτύου (επίπεδο 3) του μοντέλου OSI. Οι δρομολογητές αναλύουν τον προορισμό των εισερχόμενων πακέτων δεδομένων από το διαδίκτυο και καθορίζουν την καλύτερη διαδρομή για να φτάσουν στον τελικό προορισμό τους, είτε εντός του τοπικού δικτύου είτε σε άλλο δίκτυο. Είναι απαραίτητοι για την καθοδήγηση της κυκλοφορίας, την παροχή ασφάλειας μέσω πολιτικών τείχους προστασίας και τη δυνατότητα σε πολλές συσκευές να μοιράζονται μια ενιαία σύνδεση στο διαδίκτυο.

Δρομολογητές οικιακού και μικρού γραφείου

Επισκόπηση: Η Cisco προσφέρει δρομολογητές σχεδιασμένους για περιβάλλοντα μικρών γραφείων/οικιακών γραφείων (SOHO), με έμφαση στην απλότητα, την προσιτή τιμή και τα βασικά χαρακτηριστικά ασφαλείας. Αυτοί οι δρομολογητές εγκαθίστανται και διαχειρίζονται εύκολα, παρέχοντας αξιόπιστη πρόσβαση στο διαδίκτυο για μικρό αριθμό χρηστών και συσκευών.

Πλεονεκτήματα

- **Συνδεσιμότητα Wi-Fi**: Υποστήριξη των πιο πρόσφατων προτύπων Wi-Fi για την παροχή γρήγορης και αξιόπιστης ασύρματης πρόσβασης.
- **Ασφάλεια**: Περιέχει δυνατότητες τείχους προστασίας, υποστήριξη VPN και πρόσβαση σε δίκτυο επισκεπτών για την προστασία ευαίσθητων πληροφοριών.

Δρομολογητές για μικρές και μεσαίες επιχειρήσεις

Επισκόπηση: Προσφέρουν βελτιωμένη απόδοση, ασφάλεια και επεκτασιμότητα σε σύγκριση με τους δρομολογητές SOHO.

Πλεονεκτήματα

- **Προηγμένη ασφάλεια**: όπως πρόληψη εισβολής, κρυπτογράφηση και ασφαλείς επιλογές VPN για απομακρυσμένη πρόσβαση.

- **Ποιότητα υπηρεσίας (QoS)**: Ιεράρχηση των σημαντικών εφαρμογών για τη διασφάλιση της βέλτιστης απόδοσης.

Περιπτώσεις χρήσης: Κατάλληλες για μικρομεσαίες επιχειρήσεις που απαιτούν αξιόπιστη συνδεσιμότητα ,με μεγαλύτερο αριθμό χρηστών, υπηρεσίες VoIP και ασφαλή απομακρυσμένη πρόσβαση για τους υπαλλήλους (Tetz, 2011).

επιχειρησιακοί δρομολογητές

Επισκόπηση: Οι επιχειρησιακοί δρομολογητές της Cisco αποτελούν συσκευές υψηλών επιδόσεων που έχουν σχεδιαστεί για να ανταποκρίνονται στις απαιτήσεις μεγάλων δικτύων.

Διαθέτουν μέγιστη ευελιξία, επεκτασιμότητα και ασφάλεια, υποστηρίζοντας ένα ευρύ φάσμα διεπαφών και εκτεταμένων πρωτοκόλλων δικτύου.

Πλεονεκτήματα:

- **Υψηλή επεκτασιμότητα**: Η Αρθρωτή τους σχεδίαση επιτρέπει την εύκολη επέκτασιμότητα.
- **Στιβαρή ασφάλεια και επιδόσεις**: Διαθέτει προηγμένα χαρακτηριστικά ασφαλείας, έχει υψηλή απόδοση και υποστηρίζει πολλαπλές διασυνδέσεις υψηλής ταχύτητας.

Περιπτώσεις χρήσης: Ιδανικό για μεγάλες εταιρείες και ιδρύματα με σύνθετες ανάγκες δικτύωσης, που απαιτούν υψηλή διαθεσιμότητα, μεγαλύτερη ασφάλεια και δυνατότητα διαχείρισης σημαντικής διακίνησης δεδομένων .

Δρομολογητές παρόχων υπηρεσιών

Επισκόπηση: Είναι σχεδιασμένοι για παρόχους υπηρεσιών διαδικτύου και μεγάλους παρόχους τηλεπικοινωνιών, Είναι σχεδιασμένοι ώστε να υποστηρίζουν τη ραχοκοκαλιά του διαδικτύου.

Χαρακτηριστικά:

- **Διαχείριση δεδομένων υψηλής χωρητικότητας**: Έχουν κατασκευαστεί για τη διαχείριση τεράστιων ποσοτήτων κυκλοφορίας δεδομένων σε δίκτυα ευρείας περιοχής (WAN).
- **Προηγμένα χαρακτηριστικά δρομολόγησης**: Υποστήριξη σύνθετων πρωτοκόλλων δρομολόγησης και υπηρεσιών δικτύου που είναι απαραίτητες για παρόχους υπηρεσιών διαδικτύου και δίκτυα δεδομένων μεγάλης κλίμακας.

Περιπτώσεις χρήσης: (Tetz, 2011).

Η ολοκληρωμένη γκάμα δρομολογητών της Cisco έχει σχεδιαστεί για να ανταποκρίνεται στις ανάγκες συνδεσιμότητας, επιδόσεων και ασφάλειας κάθε μεγέθους δικτύου, από απλές οικιακές ρυθμίσεις έως τις πολύπλοκες απαιτήσεις μεγάλων επιχειρήσεων και παρόχων υπηρεσιών. Κάθε κατηγορία δρομολογητών της Cisco προσφέρει συγκεκριμένα χαρακτηριστικά προσαρμοσμένα στο περιβάλλον-στόχο της, διασφαλίζοντας ότι οι

επιχειρήσεις και οι ιδιώτες μπορούν να βρουν μια λύση δρομολόγησης που ταιριάζει απόλυτα στις ανάγκες τους.

Διακόπτες: Αυτές οι συσκευές είναι αναπόσπαστο στοιχείο για τη δημιουργία ενός δικτύου. Συνδέουν πολλαπλές συσκευές, όπως υπολογιστές, σημεία ασύρματης πρόσβασης, εκτυπωτές και διακομιστές, σε ένα ενιαίο τοπικό δίκτυο (LAN). Οι μεταγωγείς δραστηριοποιούνται στο επίπεδο ζεύξης δεδομένων (επίπεδο 2) του μοντέλου OSI, αλλά μπορούν επίσης να εκτελούν λειτουργίες δρομολόγησης στο επίπεδο 3, καθιστώντας τους ευέλικτα στοιχεία στο σχεδιασμό δικτύων. Η κύρια λειτουργία τους είναι να παραλαμβάνουν τα εισερχόμενα πακέτα δεδομένων και να τα κατευθύνουν στον προορισμό τους εντός του τοπικού δικτύου.

Μη διαχειριζόμενοι διακόπτες:

Πρόκειται για συσκευές plug-and-play χωρίς την ανάγκη διαμόρφωσης. Κατάλληλες για μικρά δίκτυα όπου απαιτείται βασική συνδεσιμότητα.

Ασύρματη δικτύωση

Η Cisco ανέπτυξε δύο εργαλεία που μπορούν να εξασφαλίσουν ασφαλή και κλιμακούμενη ασύρματη συνδεσιμότητα σε διάφορα περιβάλλοντα, από μικρά γραφεία έως μεγάλες επιχειρήσεις και υπαίθριους χώρους

Αυτά τα εργαλεία είναι:

Το Cisco Aironet και Catalyst Access Points που παρέχει ισχυρή ασύρματη κάλυψη, συνδεσιμότητα υψηλής πυκνότητας και προηγμένα χαρακτηριστικά ασφαλείας για την υποστήριξη ενός κινητού εργατικού δυναμικού και συσκευών IoT

και το:

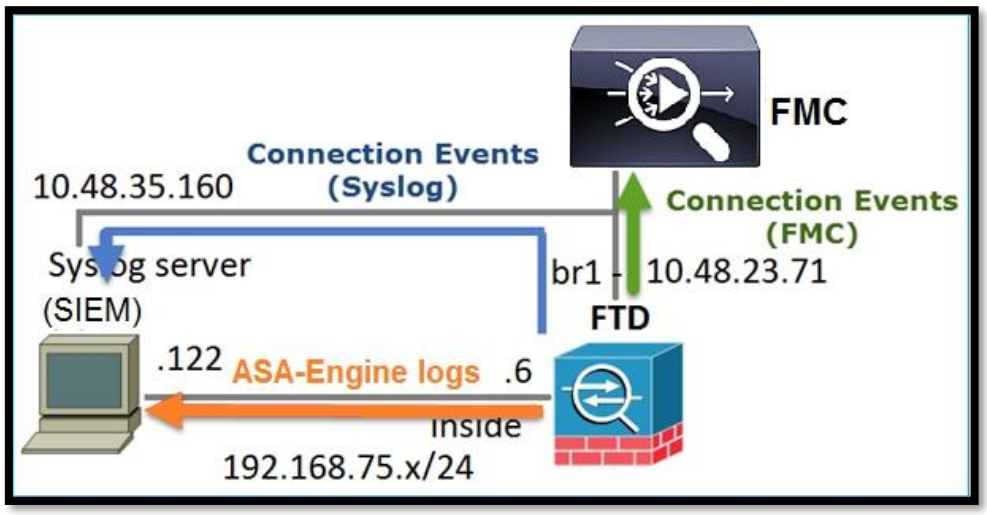
- **Cisco Meraki Cloud-Managed Wireless** που είναι μια πλήρως διαχειριζόμενη από το cloud ασύρματη λύση που απλοποιεί την ανάπτυξη, τη διαχείριση και την αντιμετώπιση προβλημάτων ασύρματων δικτύων μέσω ενός κεντρικού πίνακα ελέγχου.

Περιπτώσεις χρήσης: Ιδανικές για επιχειρήσεις που επιθυμούν να υλοποιήσουν ή να αναβαθμίσουν την υποδομή Wi-Fi τους με επεκτάσιμα, ασφαλή και εύκολα διαχειρίσιμα ασύρματα δίκτυα.

- **ασφάλεια δικτύου**

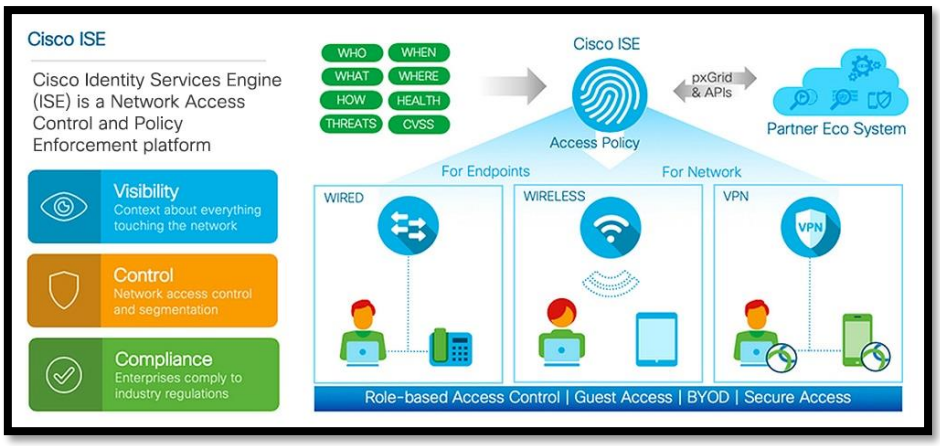
Και σε αυτόν τον τομέα η εταιρία κατάφερε να υλοποιήσει δύο εργαλεία ,που προσφέρουν τείχος προστασίας αλλά και διαχείριση των πολιτικών ασφαλείας .Τα εργαλεία αυτά είναι :

- **το Cisco Firepower Threat Defense** που δημιουργεί τείχος προστασίας επόμενης γενιάς (NGFW) έλεγχο εφαρμογών και προηγμένη προστασία από κακόβουλο λογισμικό



Εικονα9 Cisco Firepower Threat Defense

- **Cisco Identity Services Engine (ISE)**: που προσφέρει διαχείριση πολιτικών ασφαλείας και έλεγχο της πρόσβασης σε πόρους του δικτύου, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες και συσκευές μπορούν να έχουν πρόσβαση σε ευαίσθητες επιχειρηματικές πληροφορίες.



Εικόνα 10 ***Cisco Identity Services Engine (ISE)***

Περιπτώσεις χρήσης: Απαραίτητες για οργανισμούς όλων των μεγεθών που απαιτούν ισχυρά μέτρα ασφαλείας για την προστασία από τις εξελισσόμενες απειλές κυβερνοασφαλείας.

Συνεργασία και ενοποιημένες επικοινωνίες

Η Cisco διαθέτει μια σειρά εργαλείων συνεργασίας και λύσεων ενοποιημένων επικοινωνιών για τη διευκόλυνση της επικοινωνίας και συνεργασίας μεταξύ των ομάδων, ανεξάρτητα από την τοποθεσία τους (Cisco Networking Academy, 2014).

εργαλεία:

- **Cisco Webex**: εργαλείο για τηλεδιασκέψεις, διαδικτυακές συσκέψεις, κοινή χρήση οθόνης και διαδικτυακά σεμινάρια, που υποστηρίζει την απομακρυσμένη εργασία και την ψηφιακή συνεργασία.
- **Cisco Unified Communications Manager (UCM)**: Προσφέρει δυνατότητες φωνής, βίντεο, ανταλλαγής μηνυμάτων, κινητικότητας και διαδικτυακών διασκέψεων για τη διευκόλυνση της αποτελεσματικότερης επικοινωνίας και συνεργασίας.
- **Περιπτώσεις χρήσης**: Κατάλληλες για επιχειρήσεις που επιθυμούν να ενισχύσουν τη συνεργασία ομάδων, να βελτιώσουν την παραγωγικότητα και να υποστηρίξουν απομακρυσμένα ή υβριδικά περιβάλλοντα εργασίας αλλά και για περιπτώσεις εκτακτης ανάγκης όπως την εποχή του COVID όπου τα εκπαιδευτικά ιδρύματα λειτουργούσαν εξ' αποστάσεως μέσω του εργαλείου **Cisco Webex**.

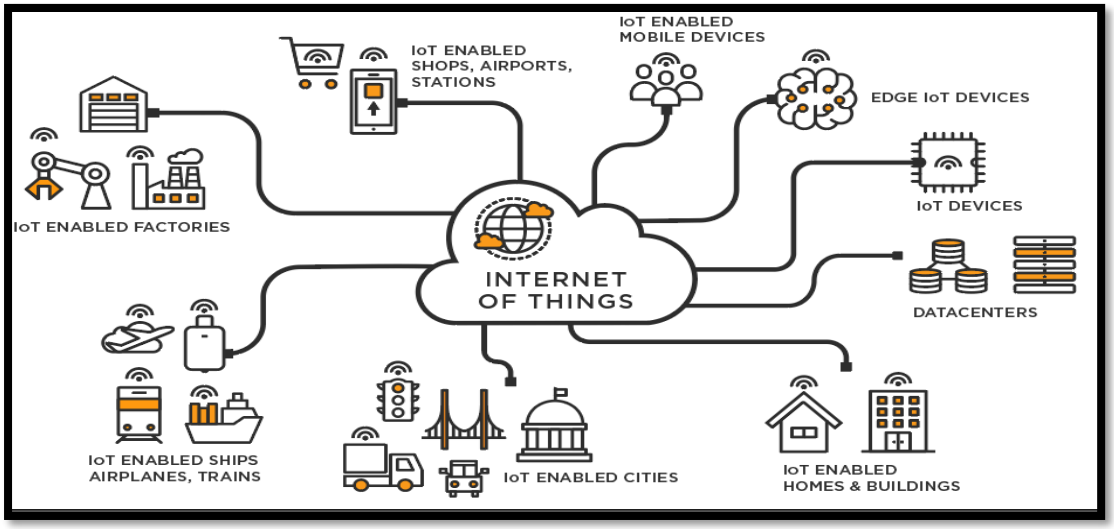
Κέντρο δεδομένων και λύσεις Cloud Data center **και Cloud**

Οι λύσεις data center και cloud της Cisco έχουν σχεδιαστεί για να καλύπτουν τις απαιτήσεις κλιμάκωσης, απόδοσης και λειτουργικής αποδοτικότητας των σύγχρονων κέντρων δεδομένων (Cisco Networking Academy, 2014).Και σε αυτήν την περίπτωση υπάρχουν δύο εργαλεία αρκετά χρήσιμα.

- **Το Cisco UCS (Unified Computing System)**: Είναι ικανό να ενσωματώσει τον υπολογισμό, τη δικτύωση, την πρόσβαση στην αποθήκευση και την εικονικοποίηση σε ένα ενιαίο συνεκτικό σύστημα που διευκολύνει τη διαχείριση του κέντρου δεδομένων και αυξάνει τη λειτουργική αποδοτικότητα.
- **Και το Cisco Hyper Flex** που παρέχει μια λύση υπερσυγκεντρωμένης υποδομής που συνδυάζει τον υπολογισμό, την αποθήκευση και τη δικτύωση σε μια απλοποιημένη, εύχρηστη πλατφόρμα για την ανάπτυξη, τη διαχείριση και την κλιμάκωση εφαρμογών.

Περιπτώσεις χρήσης: Ιδανικές για οργανισμούς που επιθυμούν να εκσυγχρονίσουν τα κέντρα δεδομένων τους, να υιοθετήσουν το cloud computing και να επιταχύνουν τις πρωτοβουλίες ψηφιακού μετασχηματισμού.

Internet of Things (IoT)



Εικόνα11 ***Internet of Things***

https://www.vshgroup.com.my/what-is-iot- 2

Οι λύσεις IoT της Cisco επιτρέπουν ασφαλή και κλιμακούμενη συνδεσιμότητα για συσκευές IoT, υποστηρίζοντας κλάδους όπως η μεταποίηση, και οι μεταφορές

Χαρακτηριστικά:

- **Βιομηχανικά Ethernet Switches**: Σχεδιασμένα για να αντέχουν σε σκληρά βιομηχανικά περιβάλλοντα, παρέχοντας αξιόπιστη συνδεσιμότητα για βιομηχανικές συσκευές.
- **Ασφάλεια IoT**: Ολοκληρωμένες λύσεις ασφαλείας για την προστασία των συσκευών και των δεδομένων IoT από απειλές.

Περιπτώσεις χρήσης: Ιδανικές για βιομηχανίες και οργανισμούς που επιθυμούν να αξιοποιήσουν την τεχνολογία IoT για τη βελτίωση της λειτουργικής αποδοτικότητας, τη βελτίωση της εμπειρίας των πελατών και την προώθηση της καινοτομίας.

Αξιολόγηση των απαιτήσεων δικτύου

Το πρώτο βήμα για την επιλογή εξοπλισμού Cisco είναι η διεξοδική αξιολόγηση των απαιτήσεων του δικτύου όπως:

Το μέγεθος του δικτύου: Δηλαδή ο καθορισμός του αριθμού των χρηστών, των τύπων των συσκευών που συνδέονται στο δίκτυο και του όγκου της κίνησης δεδομένων.

Οι επιχειρηματικές ανάγκες και στόχοι: Δηλαδή η εξέταση του τρόπου με τον οποίο το δίκτυο υποστηρίζει τους επιχειρηματικούς στόχους, όπως η δυνατότητα απομακρυσμένης εργασίας, η υποστήριξη εφαρμογών που βασίζονται στο cloud ή η διευκόλυνση ασφαλών συναλλαγών.

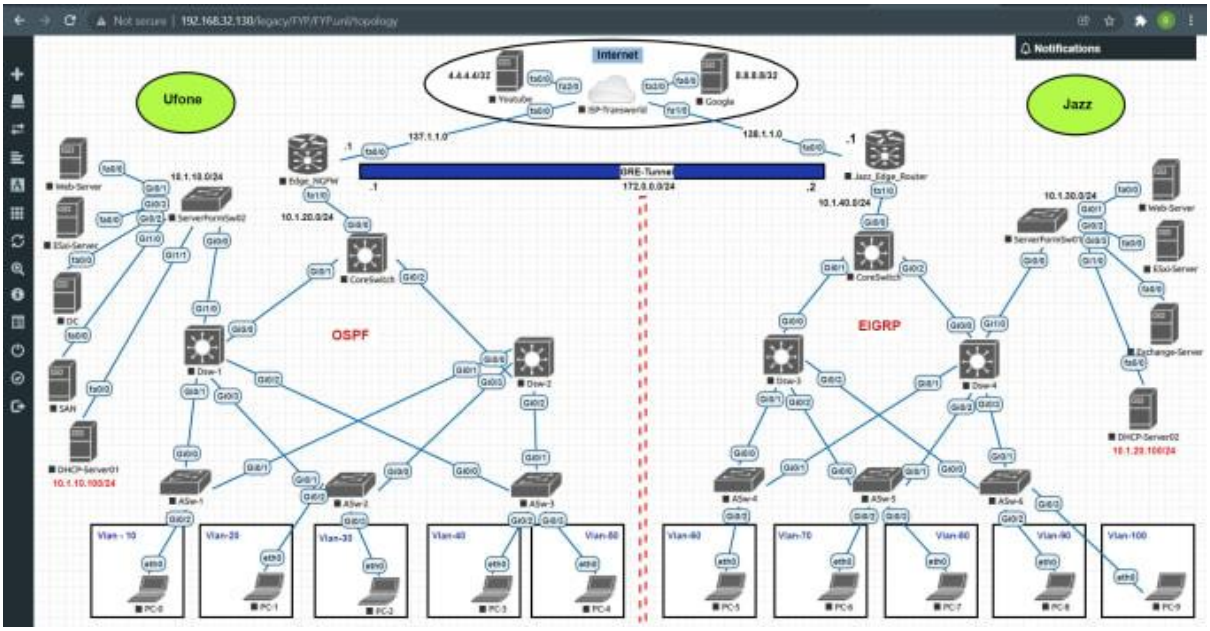
- **Οι τρέχουσες προκλήσεις δικτύου**: Δηλαδή ο εντοπισμός προβλημάτων όπως η συμφόρηση, τα τρωτά σημεία ασφαλείας ή οι περιοχές με έλλειψη πλεονασμού.
- Η Cisco παρέχει λεπτομερείς προδιαγραφές για τη συγκρότηση του δικτύου ,όπως :

- **Τις μετρήσεις επιδόσεων**:
- **Την επεκτασιμότητα**: Εξέταση του πόσο εύκολα μπορεί να αναβαθμιστεί ή να επεκταθεί ο εξοπλισμός

- **Τα εργαλεία διαμόρφωσης και διαχείρισης**: δηλαδή η αναζήτηση εξοπλισμού που προσφέρει διαισθητικές διεπαφές διαχείρισης, όπως το DNA Center της Cisco ή το ταμπλό της Meraki, οι οποίες μπορούν να απλοποιήσουν τις λειτουργίες του δικτύου.

- **Η υποστήριξη και ενημερώσεις**: δηλαδή η εξέταση του επιπέδου υποστήριξης που συμπεριλαμβανομένης της πρόσβασης σε τακτικές ενημερώσεις λογισμικού, διορθώσεις και εξυπηρέτηση πελατών, ώστε να διατηρείται η ομαλή λειτουργία του δικτύου.

Cisco Packet Tracer



Εικόνα12 Cisco Packet Tracer

Το Cisco Packet Tracer είναι ένα ισχυρό εργαλείο προσομοίωσης που χρησιμοποιείται για το σχεδιασμό, τη διαμόρφωση και την αντιμετώπιση προβλημάτων δικτύων. Δίνει στους χρήστες τη δυνατότητα να σχεδιάζουν εικονικές τοπολογίες δικτύων και στη συνέχεια να τις εκτελούν σαν να επρόκειτο για πραγματικά δίκτυα υπολογιστών. από τον μήνα Αύγουστο του 2017

Χαρακτηριστικά και λειτουργία

- Είναι cross-platform, δηλαδή μπορεί να λειτουργήσει σε πολλές πλατφόρμες. Όσον αφορά την προσθήκη και την αφαίρεση συσκευών δικτύου, το γραφικό περιβάλλον χρήστη (GUI) προσφέρει στον χρήστη κάθε δυνατή άνεση από την αρχή έως το τέλος.

- Εκτός από την προσομοίωση δικτύων διαφόρων μεγεθών, το Packet Tracer είναι επίσης σε θέση να προσομοιώνει δίκτυα που μπορούν να επικοινωνούν μεταξύ τους σε πραγματικό χρόνο.
- Είναι επίσης δυνατή η διαμόρφωση διακομιστών έτσι ώστε να μπορούν να υποστηρίζουν μια μεγάλη ποικιλία υπηρεσιών, όπως FTP, HTTP, DNS, DHCP και τείχος προστασίας
- Το σύστημα έχει τη δυνατότητα να επιλέγει ή να αποφασίζει αυτόματα το είδος της καλωδίωσης που πρέπει να χρησιμοποιηθεί μεταξύ των συσκευών.
- Μέσω της χρήσης του Internet Operating System (IOS) της Cisco, είναι δυνατή η προσομοίωση μιας διεπαφής γραμμής εντολών (CLI), (με περιορισμένο σύνολο εντολών), προκειμένου να διαμορφωθούν οι δρομολογητές και οι μεταγωγείς.
- Η δοκιμή πραγματοποιείται σε πραγματικό χρόνο, με την ανταλλαγή πακέτων δεδομένων μεταξύ των διαφόρων τμημάτων του δικτύου
- Όταν προκύψει κάποιο πρόβλημα στο δίκτυο, ο Packet Tracer μας δίνει τη δυνατότητα να παρακολουθούμε βήμα προς βήμα την κίνηση των πακέτων στην περιοχή όπου εμφανίστηκε η βλάβη. Έτσι ,είμαστε σε θέση να διερευνήσουμε τη δομή και τη διαδρομή των πακέτων με σχεδόν κάθε πιθανή λεπτομέρεια που έχουμε στη διάθεσή μας.

- Παρέχει δύο *χώρους εργασίας:*

Το *Λογικό Χώρο Εργασίας* (Logical Workspace) Εδώ γίνεται η παραμετροποίηση του

το *Φυσικό Χώρο Εργασίας* (Physical Workspace) όπου τα μέρη του δικτύου τοποθετούνται στις πραγματικές τους θέσεις Υπάρχει μια κάτοψη του χώρου όπου σε ειδικό δωμάτιο βρίσκονται οι σημαντικές δικτυακές συσκευές (εξυπηρετητές, δρομολογητές, κλπ) και στους υπόλοιπους χώρους οι θέσεις εργασίας τα PCs, οι εκτυπωτές, κλπ.

Παρέχει δύο *καταστάσεις λειτουργίας* (CiscoPacketTracer, 2013):

Αυτήν του πραγματικού χρόνου (Real Time Mode) στην οποία το δίκτυο κάνει προσομοίωση σε πραγματικές συνθήκες όσον αφορά όγκο πληροφοριών, χρόνο μετάδοσης, κλπ.

Και αυτήν της προσομοίωσης (Simulation Mode) όπου παρατηρούμε βήμα-βήμα τη λειτουργία του δικτύου για να εντοπίσουμε σφάλματα, αλλά και να αναλύσουμε την όλη διαδικασία σε κάθε λεπτομέρειά της.

- Το *εικονικό υλικό* (hardware) περιλαμβάνει

Δικτυακές συσκευές (μεταγωγείς, δρομολογητές, κλπ) που αποτελούνται από δομοστοιχεία και μπορούν να τροποποιηθούν (modular devices) σε γραφικό περιβάλλον (GUI).

Καλωδίωση κάθε είδους, Ethernet , ομοαξονικά, τηλεφωνικά , οπτικές ίνες, κλπ.

Λειτουργία *πολλών χρηστών* (multiuser) που μπορούν να εργάζονται σε τμήματα του ίδιου εικονικού δικτύου.

- Για την εξοικείωση του χρήστη συνοδεύεται με εμπεριστατωμένη Βοήθεια (Help) και εκπαιδευτικό υλικό (tutorial) (Cisco Packet Tracer, 2013).

Πλεονεκτήματα

- Ένα από τα σημαντικά πλεονεκτήματα της χρήσης του Cisco Packet Tracer είναι η φιλική προς το χρήστη διεπαφή του.
- Παρέχει επίσης μια οικονομικά αποδοτική λύση για τον πειραματισμό δικτύων χωρίς την ανάγκη φυσικού δικτυακού εξοπλισμού.

Μειονεκτήματα

- Το κύριο μειονέκτημα της χρήσης του Cisco Packet Tracer είναι η περιορισμένη υποστήριξή του για προηγμένα πρωτόκολλα δικτύωσης. Δεν υποστηρίζει ορισμένα βασικά πρωτόκολλα, όπως το BGP και το OSPF, καθιστώντας το λιγότερο κατάλληλο για προηγμένες πρακτικές δικτύωσης.
- Ένα άλλο μειονέκτημα είναι ότι δεν αποτελεί προσομοίωση πραγματικού κόσμου και, ως εκ τούτου, ενδέχεται να μην αναπαριστά με ακρίβεια τη συμπεριφορά του δικτύου σε σενάρια πραγματικού χρόνου (Cisco Packet Tracer, 2013)

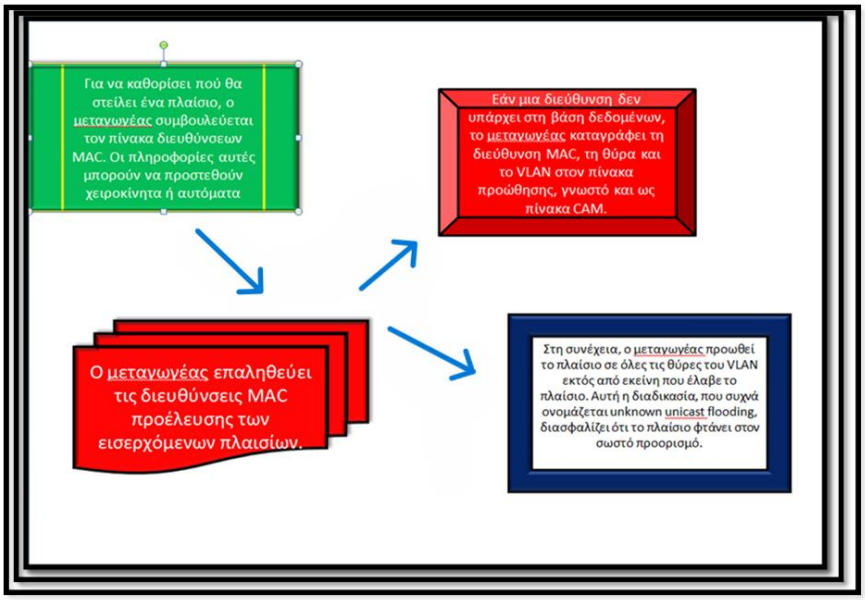
Λειτουργία μεταγωγέα

Ένας μεταγωγέας Ethernet λειτουργεί στο επίπεδο σύνδεσης δεδομένων του μοντέλου OSI, χρησιμοποιώντας τις διευθύνσεις MAC προορισμού στο πλαίσιο για να καθορίσει τον τρόπο προώθησης των πλαισίων. Στη βασική δικτύωση, κάθε σύνδεση μεταξύ δύο θυρών σε έναν μεταγωγέα αποτελεί το δικό της πεδίο σύγκρουσης, δηλαδή κάθε θύρα του μεταγωγέα και η συνδεδεμένη με αυτήν συσκευή έχουν ένα ξεχωριστό πεδίο σύγκρουσης. Εφόσον δεν υπάρχει συμφόρηση του μέσου, όλοι οι κεντρικοί υπολογιστές μπορούν να λειτουργούν σε λειτουργία πλήρους διπλής όψης, επιτρέποντας την ταυτόχρονη μετάδοση και λήψη δεδομένων. Η έννοια του half-duplex είναι πλέον ξεπερασμένη και ισχύει μόνο για τους κόμβους και τους παλαιότερους μεταγωγείς 10/100-Mbps, καθώς οι σύγχρονες συνδέσεις 1 Gbps είναι προεπιλεγμένες σε fullduplex (Liu, 2009).

Μεταγωγή cut-through

Στη λειτουργία αποθήκευσης και προώθησης, ένας μεταγωγέας ελέγχει το πλαίσιο για σφάλματα και αναμεταδίδει μόνο εκείνα με έγκυρο κυκλικό έλεγχο πλεονασμού (CRC). Ορισμένοι μεταγωγείς, όπως τα μοντέλα Nexus, χρησιμοποιούν μια μέθοδο που ονομάζεται cut-through switching, όπου προωθούν πλαίσια με βάση αποκλειστικά τις πληροφορίες επιπέδου 2 χωρίς να εκτελούν έλεγχο CRC. Αυτό μειώνει την καθυστέρηση μετάδοσης εξαλείφοντας την ανάγκη αποθήκευσης ολόκληρου του πλαισίου πριν από την προώθησή του σε άλλη θύρα. Η μεταγωγή cut-through πλεονεκτεί για εφαρμογές χαμηλής καθυστέρησης, όπως η αλγοριθμική διαπραγμάτευση σε κέντρα δεδομένων. Ωστόσο, αφήνει το χειρισμό σφαλμάτων στην κάρτα διασύνδεσης δικτύου (NIC) της τελικής συσκευής ή σε ένα πρωτόκολλο ανώτερου επιπέδου. Οι περισσότεροι μεταγωγείς Catalyst χρησιμοποιούν τη μέθοδο αποθήκευσης και προώθησης, εξασφαλίζοντας μεγαλύτερη αξιοπιστία με την επαλήθευση της ακεραιότητας των πλαισίων πριν από τη μετάδοση (Liu, 2009).

Προώθηση διευθύνσεων MAC



Εικόνα 13 προώθηση διευθύνσεων MAC 2

Για να καθορίσει πού θα στείλει ένα πλαίσιο, ο μεταγωγέας συμβουλεύεται τον πίνακα διευθύνσεων MAC. Οι πληροφορίες αυτές μπορούν να προστεθούν χειροκίνητα ή αυτόματα.

Ο μεταγωγέας επαληθεύει τις διευθύνσεις MAC προέλευσης των εισερχόμενων πλαισίων. Εάν μια διεύθυνση δεν υπάρχει στη βάση δεδομένων, το μεταγωγέας καταγράφει τη διεύθυνση MAC, τη θύρα και το VLAN στον πίνακα προώθησης, γνωστό και ως πίνακα CAM.

Στη συνέχεια, ο μεταγωγέας προωθεί το πλαίσιο σε όλες τις θύρες του VLAN εκτός από εκείνη που έλαβε το πλαίσιο. Αυτή η διαδικασία, που συχνά ονομάζεται unknown unicast flooding, διασφαλίζει ότι το πλαίσιο φτάνει στον σωστό προορισμό.

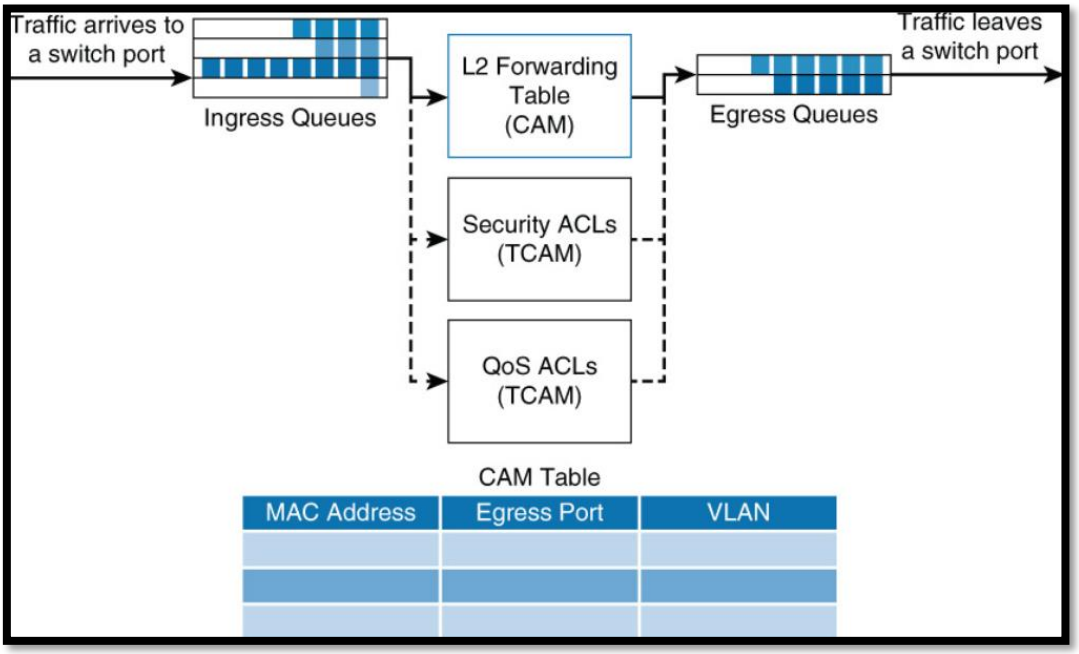
Η κίνηση εκπομπής και πολλαπλής διανομής, που έχει σχεδιαστεί για να λαμβάνεται από πολλές συσκευές, αντιμετωπίζεται με παρόμοιο αυτοματοποιημένο τρόπο (Froom&Frahim, 2015).

Λειτουργία μεταγωγέα επιπέδου 2

Όταν ένας μεταγωγέας λαμβάνει ένα πλαίσιο, το τοποθετεί αμέσως σε μια ουρά εισόδου. Μια θύρα μπορεί να έχει πολλαπλές ουρές εισόδου, οι οποίες συνήθως χρησιμοποιούνται για τη διαχείριση πλαισίων με διάφορους τρόπους, όπως η εφαρμογή

μέτρων ποιότητας υπηρεσίας (QoS). Από μια απλουστευμένη άποψη, όταν ο μεταγωγέας επιλέγει ένα πλαίσιο από μια ουρά για να το μεταδώσει σε διάφορους προορισμούς, οι μεταγωγείς πρέπει να εξετάσουν πολλά (Kvitoslava Obelovskaetal., 2023):

- Πού πρέπει να προωθηθεί το πλαίσιο;
- Αν υπάρχουν περιορισμοί που εμποδίζουν την προώθηση του πλαισίου;
- Αν υπάρχει κάποια ιεράρχηση ή σήμανση που πρέπει να εφαρμοστεί στο πλαίσιο;



Εικόνα 14 Λειτουργία μεταγωγέα επιπέδου 2

https://www.ciscopress.com/articles/article.asp?p=2348265&seqNum=2

Μια μελέτη των Kvitoslava Obelovska και συν. το 2023 εξετάζει τρία βασικά ερωτήματα και απαντά στο πού πρέπει να προωθηθεί το πλαίσιο:

- Ο πίνακας προώθησης επιπέδου 2, που συχνά αναφέρεται ως πίνακας MAC, παρακολουθεί τους προορισμούς των πλαισίων καταγράφοντας τις διευθύνσεις MAC και τις αντίστοιχες θύρες προορισμού.
- Οι μεταγωγείς χρησιμοποιούν αυτόν τον πίνακα για να προσδιορίζουν τη διεύθυνση MAC προορισμού των εισερχόμενων πλαισίων και να κατευθύνουν τα πλαίσια στις κατάλληλες θύρες.

- Εάν η διεύθυνση MAC δεν βρεθεί στον πίνακα, το πλαίσιο μεταδίδεται σε όλες τις θύρες εντός του ίδιου VLAN.

Στο αν υπάρχουν περιορισμοί που εμποδίζουν την προώθηση του πλαισίου:

- Οι Λίστες Ελέγχου Πρόσβασης (ACL) δεν αφορούν αποκλειστικά τους δρομολογητές- οι μεταγωγείς μπορούν επίσης να επιβάλλουν ACL χρησιμοποιώντας διευθύνσεις MAC και IP. Γενικά, μόνο οι προηγμένοι μεταγωγείς είναι σε θέση να χρησιμοποιούν ACLs που ενσωματώνουν και τους δύο τύπους διευθύνσεων. Αντίθετα, οι μεταγωγείς επιπέδου 2 περιορίζονται σε ACLs που βασίζονται αποκλειστικά σε διευθύνσεις MAC.

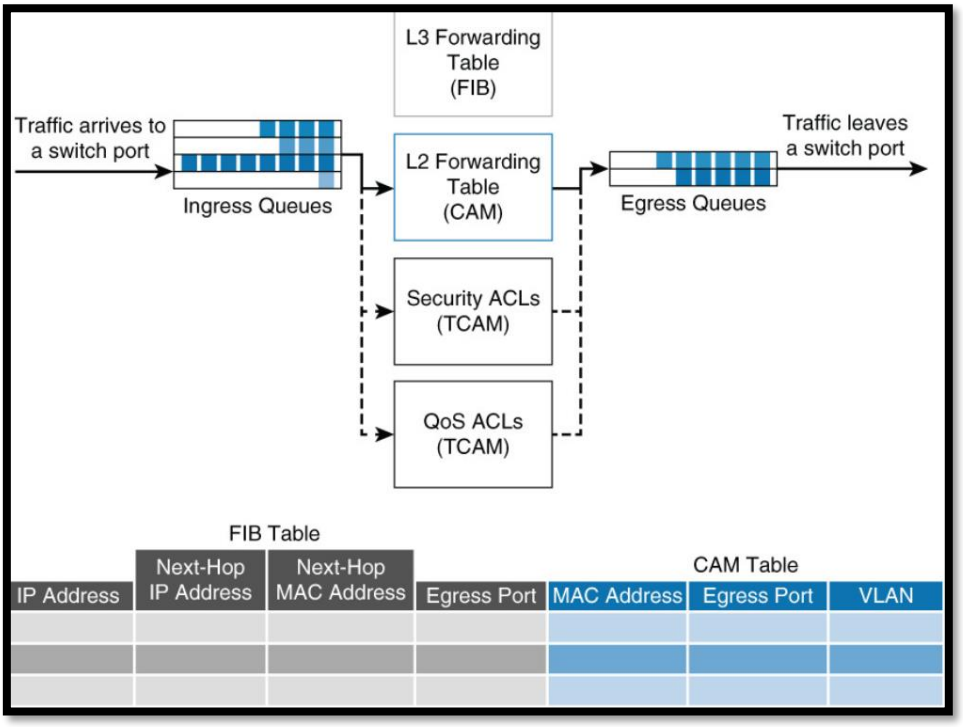
Στο αν υπάρχει κάποια ιεράρχηση ή σήμανση που πρέπει να εφαρμοστεί στο πλαίσιο:

Τα πλαίσια μπορούν να ταξινομηθούν σύμφωνα με κριτήρια ποιότητας υπηρεσίας (QoS), επιτρέποντας την ιεράρχηση, τον προσδιορισμό ή τους περιορισμούς ταχύτητας. Οι μεταγωγείς χρησιμοποιούν εξειδικευμένο υλικό για τη διαχείριση του πίνακα MAC, των δεδομένων ACL και των πληροφοριών QoS. Η Content Addressable Memory (CAM) αποθηκεύει τον πίνακα MAC λόγω της ικανότητάς της να παρέχει γρήγορη πρόσβαση με δυαδικά αποτελέσματα (0 ή 1), καθιστώντας την ιδανική για πίνακες προώθησης επιπέδου 2. Η τριμερής μνήμη με διεύθυνση περιεχομένου (TCAM) χειρίζεται τους πίνακες ACL και QoS, προσφέροντας τρία πιθανά αποτελέσματα (0, 1 ή μια απροσδιόριστη τιμή). Η TCAM είναι επωφελής για εργασίες όπως η δρομολόγηση IP, όπου υποστηρίζει αναζητήσεις για τις μεγαλύτερες αντιστοιχίες προθέματος. Η χρήση της TCAM διασφαλίζει ότι οι εφαρμογές ACL δεν μειώνουν την απόδοση του μεταγωγέα, καθώς υποστηρίζει αποτελεσματικά τις διεργασίες ανώτερου επιπέδου (KvitoslavaObelovskaetal., 2023).

Λειτουργία μεταγωγέα επιπέδου 3 (πολλαπλών επιπέδων)

Οι πολυεπίπεδοι μεταγωγείς είναι ικανοί τόσο για μεταγωγή επιπέδου 2 όσο και για προώθηση πλαισίων με βάση πληροφορίες επιπέδου 3 και επιπέδου 4. Ενσωματώνουν τις λειτουργίες ενός μεταγωγέα και ενός δρομολογητή και διαθέτουν επίσης κρυφή μνήμη ροής. Ενώ εκτελούν παρόμοιες λειτουργίες με τους μεταγωγείς επιπέδου 2, οι πολυεπίπεδοι μεταγωγείς διαθέτουν ένα πρόσθετο σύστημα παράλληλης αναζήτησης για τη δρομολόγηση

πακέτων. Αυτές οι πληροφορίες δρομολόγησης αποθηκεύονται σε έναν πίνακα Forwarding Information Base (FIB), ο οποίος περιλαμβάνει δεδομένα σχετικά με τις θύρες εξόδου, τα VLAN και την επανεγγραφή MAC. Οι παράλληλες αναζητήσεις για ACLs και QoS στους πολυεπίπεδους μεταγωγείς λειτουργούν όπως αυτές στους μεταγωγείς επιπέδου 2, αλλά προσφέρουν βελτιωμένες δυνατότητες για ACLs επιπέδου 3 και ιεράρχηση QoS(Carthernetal., 2021).



Εικόνα15 Λειτουργία πολυστρωματικού διακόπτη.

Για παράδειγμα, ένας μεταγωγέας επιπέδου 2 έχει περιορισμένη ικανότητα να επιβάλλει περιορισμό ρυθμού στα πλαίσια με βάση απλώς τις διευθύνσεις MAC της πηγής ή του προορισμού. Από την άλλη πλευρά, ένας πολυεπίπεδος μεταγωγέας επιτρέπει συνήθως τον περιορισμό των ρυθμών των πλαισίων λαμβάνοντας υπόψη τις διευθύνσεις IP/MAC. Δυστυχώς, πολλοί τύποι μεταγωγέων της Cisco έχουν διαφορετικές δυνατότητες και μόνο ορισμένοι μεταγωγείς επιπέδου 2 μπορούν να χειριστούν ACLs επιπέδου 3 και αναζητήσεις QoS.

Στο πλαίσιο του CCNP Switch, οι μεταγωγείς επιπέδου 2 προσφέρουν βοήθεια για τις λίστες ελέγχου πρόσβασης (ACL) και την ποιότητα υπηρεσίας (QoS) που βασίζονται σε διευθύνσεις ελέγχου πρόσβασης μέσων (MAC). Αντίθετα, οι μεταγωγείς επιπέδου 3

παρέχουν βοήθεια για Λίστες Ελέγχου Πρόσβασης (ACL) και Ποιότητα Υπηρεσίας (QoS) που βασίζονται σε διευθύνσεις Πρωτοκόλλου Διαδικτύου (IP) ή MAC(Froom&Frahim, 2015).

Κατανεμημένη προώθηση υλικού

Οι δικτυακές συσκευές λειτουργούν με τουλάχιστον τρία επίπεδα (Carthernetal., 2021) που είναι :

- το Επίπεδο διαχείρισης

- το Επίπεδο ελέγχου

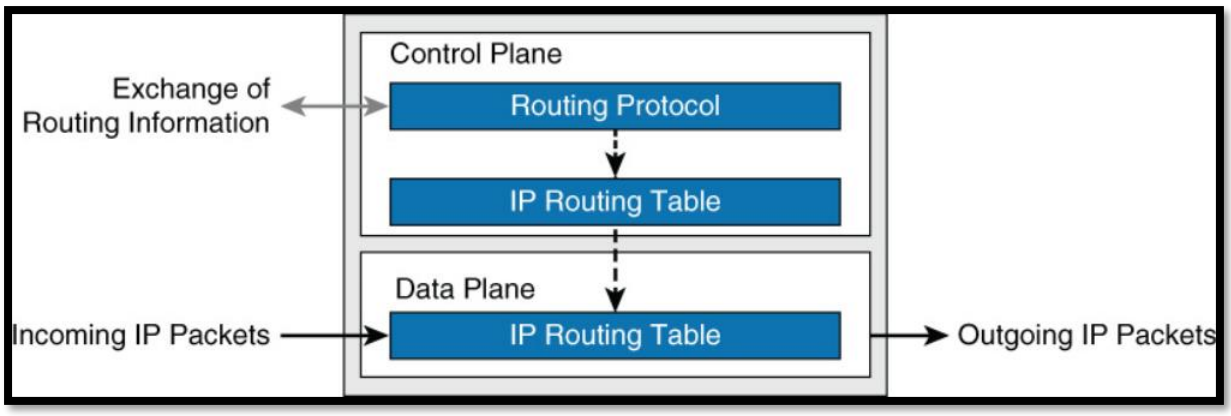
- και το Επίπεδο προώθησης

Το επίπεδο διαχείρισης χειρίζεται εργασίες διαχείρισης δικτύου, όπως πρόσβαση SSH και διαμόρφωση SNMP, και μπορεί να λειτουργεί μέσω θύρας εκτός ζώνης (OOB).

Το επίπεδο ελέγχου διαχειρίζεται τα πρωτόκολλα και λαμβάνει αποφάσεις δρομολόγησης.

Το επίπεδο προώθησης είναι υπεύθυνο για τη φυσική δρομολόγηση ή μεταγωγή της πλειονότητας των πακέτων.

Για να αποδίδουν αποτελεσματικά οι πολυεπίπεδοι μεταγωγείς, πρέπει να παρέχουν υψηλές επιδόσεις σε μέγιστους ρυθμούς δεδομένων σε πολυάριθμες θύρες. Για να το επιτύχουν αυτό, οι πολυεπίπεδοι μεταγωγείς χρησιμοποιούν ξεχωριστά επίπεδα ελέγχου και προώθησης. Το επίπεδο ελέγχου κατευθύνει το επίπεδο προώθησης σχετικά με τον τρόπο δρομολόγησης των πακέτων. Επιπλέον, οι πολυεπίπεδοι μεταγωγείς μπορεί να διαθέτουν πολλαπλά επίπεδα προώθησης. Για παράδειγμα, το Catalyst 6800 χρησιμοποιεί επίπεδα προώθησης σε κάθε μονάδα γραμμής και ένα κεντρικό επίπεδο ελέγχου στη μονάδα εποπτείας (Chilukuri, 2017). Στο Catalyst 6800, κάθε μονάδα γραμμής διαθέτει μια μικροκωδικοποιημένη CPU που διαχειρίζεται την προώθηση πακέτων και ένα πρωτόκολλο επικοινωνίας επιπέδου ελέγχου διευκολύνει την αλληλεπίδραση μεταξύ του επιπέδου ελέγχου του supervisor και των μονάδων γραμμής (Chilukuri, 2017).



Εικόνα 16 Κατανεμημένη προώθηση υλικού.

Το πρωτόκολλο επιπέδου ελέγχου, το οποίο λειτουργεί μεταξύ του επιπέδου ελέγχου και του επιπέδου προώθησης, έχει διάφορους βασικούς ρόλους (Chilukuri, 2017)όπως :

- τη διαχείριση εσωτερικών κυκλωμάτων δεδομένων και ελέγχου που σχετίζονται με τη δρομολόγηση και τον έλεγχο πακέτων.

- την εξαγωγή πρόσθετων πληροφοριών δρομολόγησης και προώθησης πακέτων από τα πρωτόκολλα και τα δεδομένα διαμόρφωσης των επιπέδων 2 και 3 και, στη συνέχεια, αποστολή αυτών των πληροφοριών στη μονάδα διασύνδεσης για τη διαχείριση της ροής δεδομένων.

- τη συλλογή πληροφοριών διαδρομής δεδομένων και στατιστικών στοιχείων κίνησης από τη μονάδα διασύνδεσης και προώθησή τους στον επεξεργαστή διαδρομής.

- την επεξεργασία συγκεκριμένων πακέτων δεδομένων από μονάδες διασύνδεσης Ethernet προς τον επεξεργαστή δρομολόγησης, συμπεριλαμβανομένων των αιτήσεων DHCP, των πακέτων εκπομπής και των πακέτων πρωτοκόλλου δρομολόγησης.

Επισκόπηση του πρωτοκόλλου Spanning Tree (STP)

Το πρωτόκολλο Spanning Tree Protocol (STP) (IEEE 802.1D) χρησιμοποιείται κυρίως για την αποφυγή βρόχων επιπέδου 2 και καταιγίδων εκπομπής, ενώ παράλληλα παρέχει πλεονασμό δικτύου. Σχεδιάστηκε σε μια εποχή όπου η αποκατάσταση από διακοπές που διαρκούσαν ένα λεπτό ή περισσότερο ήταν αποδεκτή. Ωστόσο, καθώς η τεχνολογία έχει

εξελιχθεί και οι κρίσιμες εφαρμογές εξαρτώνται όλο και περισσότερο από αξιόπιστες συνδέσεις, υπήρξε στροφή προς ταχύτερες μεθόδους αποκατάστασης (CiscoMeraki, 2020).

Το πρωτόκολλο Rapid Spanning Tree Protocol (RSTP) (802.1w) είναι μια βελτιωμένη έκδοση του STP (802.1D), προσφέροντας αρκετά πλεονεκτήματα. Το RSTP εισάγει πρόσθετες καταστάσεις και ρόλους θυρών και βελτιώνει σημαντικά τους χρόνους σύγκλισης.

Η υιοθέτηση του RSTP αντί του STP παρέχει στους διαχειριστές δικτύων σημαντικά οφέλη για τη διατήρηση ενός ανθεκτικού δικτύου

Πώς λειτουργεί η διαδικασία εκλογής STP

Πριν από την εκτέλεση του αλγορίθμου του δέντρου σάρωσης, οι μεταγωγείς στο ίδιο δίκτυο πρέπει πρώτα να ενεργοποιήσουν το πρωτόκολλο δέντρου σάρωσης (STP) για να εκλέξουν μια "γέφυρα ρίζας".

Η γέφυρα ρίζας, αφού επιλεγεί, στέλνει μονάδες δεδομένων πρωτοκόλλου γέφυρας (BPDU) διαμόρφωσης και άλλες σχετικές πληροφορίες στους άμεσα συνδεδεμένους μεταγωγείς της.

Οι μεταγωγείς αυτοί προωθούν στη συνέχεια τις BPDUs στους γειτονικούς τους μεταγωγείς.

Το αναγνωριστικό γέφυρας (BID) κάθε μεταγωγέα καθορίζεται συνδυάζοντας μια προεπιλεγμένη τιμή προτεραιότητας 32768 με τη διεύθυνση MAC του μεταγωγέα. Ο μεταγωγέας με το χαμηλότερο αναγνωριστικό γέφυρας θα οριστεί ως γέφυρα ρίζας (CiscoMeraki, 2020).

Κατάσταση θύρας STP

Το πρωτόκολλο Spanning Tree Protocol (STP) ορίζει πέντε καταστάσεις θύρας μεταγωγής (Cisco Meraki, 2020):

- Απενεργοποιημένη: Θύρα που έχει απενεργοποιηθεί χειροκίνητα.

- Αποκλεισμός: Όταν μια συσκευή συνδέεται, η θύρα εισέρχεται αρχικά στην κατάσταση φραγής.
- Ακούγοντας: Ο διακόπτης ακούει και στέλνει Μονάδες Δεδομένων Πρωτοκόλλου Γέφυρας (BPDUs).
- Μάθηση: Ο διακόπτης σταματά να στέλνει τα δικά του BPDUs μόλις λάβει ένα ανώτερο BPDU και αρχίζει να αναμεταδίδει τα ανώτερα BPDUs.
- Προώθηση: Η θύρα προωθεί ενεργά την κυκλοφορία.

Το STP ορίζει επίσης τρεις ρόλους θύρας:

- Ρίζα: Θύρες σε μεταγωγείς χωρίς ρίζα με το χαμηλότερο κόστος διαδρομής προς τη γέφυρα ρίζας, που χρησιμοποιούνται για την προώθηση δεδομένων προς τη γέφυρα ρίζας.
- Καθορισμένο: Θύρες σε μεταγωγείς ρίζας και καθορισμένους μεταγωγείς, με όλες τις θύρες στη γέφυρα ρίζας να είναι καθορισμένες.
- Αποκλεισμένη: Όλες οι άλλες θύρες βρίσκονται σε κατάσταση αποκλεισμού, εκτός από τις θύρες πρόσβασης σε σταθμούς εργασίας ή υπολογιστές, οι οποίες παραμένουν ανεπηρέαστες.

Διαδικασία εκλογών STP

Όταν οι μεταγωγείς ενεργοποιούνται αρχικά, στέλνουν μονάδες δεδομένων πρωτοκόλλου γέφυρας (BPDUs) διαμόρφωσης που περιέχουν τα αναγνωριστικά γέφυρας (BIDs), και κάθε μεταγωγέας θεωρεί ότι είναι η γέφυρα ρίζας.

Όταν ένας μεταγωγέας λαμβάνει ένα BPDU με χαμηλότερο BID, παύει να παράγει τα δικά του BPDU διαμόρφωσης και αντ' αυτού προωθεί τα ανώτερα BPDU σε γειτονικούς μεταγωγείς.

Αφού ανακοινωθεί η γέφυρα ρίζας, ξεκινά μια δευτερεύουσα διαδικασία εκλογής για τον προσδιορισμό της "θύρας ρίζας", η οποία είναι η θύρα που είναι υπεύθυνη για την κατεύθυνση των πλαισίων προς τη γέφυρα ρίζας.

Ακολουθεί η διαδικασία:

- Μια θύρα μεταγωγέα λαμβάνει ανώτερες BPDU και αναγνωρίζει τον μεταγωγέα που τις αποστέλλει ως γέφυρα ρίζας.

- Η θύρα με το χαμηλότερο κόστος διαδρομής προς τη γέφυρα ρίζας επιλέγεται ως θύρα ρίζας.
- Εάν πολλές θύρες έχουν το ίδιο κόστος διαδρομής, επιλέγεται η θύρα με το χαμηλότερο BID αποστολέα.
- Εάν το BID του αποστολέα είναι πανομοιότυπο (συχνά το ίδιο switch), η θύρα με τον χαμηλότερο φυσικό αριθμό θύρας στο switch αποστολής επιλέγεται ως θύρα ρίζας, χρησιμεύοντας ως τελική ισοπαλία (CiscoMeraki, 2020).

Μέθοδοι μεταγωγής της Cisco

Οι δρομολογητές CiscoIOS χρησιμοποιούν τρεις κύριες μεθόδους προώθησης πακέτων:

- μεταγωγή διεργασιών,
- ταχεία μεταγωγή
- και Cisco Express Forwarding (CEF).

Η μεταγωγή διεργασιών είναι η λιγότερο αποδοτική μέθοδος, καθώς απαιτεί από την CPU του δρομολογητή να χειρίζεται τόσο τη δρομολόγηση όσο και την επανεγγραφή πακέτων μέσω λογισμικού. Αυτή η μέθοδος πάσχει από περιορισμούς απόδοσης λόγω της εξάρτησής της από το λογισμικό και των περιορισμένων πόρων πυρήνα, γεγονός που την καθιστά ακατάλληλη για κλιμακούμενες εφαρμογές.

Η ταχεία μεταγωγή προσφέρει βελτιωμένη απόδοση, καθώς κατευθύνει και τροποποιεί το πρώτο πακέτο σε μια ακολουθία χρησιμοποιώντας λογισμικό, ενώ τα επόμενα πακέτα υποβάλλονται σε επεξεργασία από το υλικό.

Η μεταγωγή βάσει τοπολογίας, γνωστή και ως Cisco Express Forwarding (CEF), είναι ένα βασικό χαρακτηριστικό των μεταγωγέων Cisco Catalyst που βελτιώνει την απόδοση μεταγωγής επιπέδου 3. Αυτή η μέθοδος προτιμάται έναντι της προσωρινής αποθήκευσης διαδρομών λόγω της ανώτερης απόδοσης και της επεκτασιμότητάς της.

Το CEF χρησιμοποιεί τον πίνακα δρομολόγησης για τη δημιουργία μιας κρυφής μνήμης δρομολόγησης ή Βάσης Πληροφοριών Προώθησης (FIB), χωρίς να περιμένει τις ροές κυκλοφορίας για να ξεκινήσει η διαδικασία κρυφής μνήμης. Αυτή η προσέγγιση διασφαλίζει ότι τα πακέτα προωθούνται αποτελεσματικά με βάση τη FIB, ανεξάρτητα από τον όγκο της κίνησης. Μόλις μια διεύθυνση προορισμού έχει μια διαδρομή στον πίνακα δρομολόγησης, η FIB διασφαλίζει ότι όλα τα πακέτα για αυτή τη ροή αντιμετωπίζονται

αποτελεσματικά. Το CEF υποστηρίζει επίσης πολλαπλές ταυτόχρονες διαδρομές, βελτιώνοντας την κατανομή του φόρτου εργασίας στο επίπεδο IP. Οι σύγχρονοι μεταγωγείς Catalyst, όπως οι Catalyst 4500 και 6800, είναι εξοπλισμένοι με CEF, το οποίο περιλαμβάνει επίσης λειτουργίες εξισορρόπησης φορτίου.

Η εξισορρόπηση φορτίου στο CEF επιτυγχάνεται με την κατανομή της κυκλοφορίας σε διάφορα κανάλια χρησιμοποιώντας συνδυασμούς διευθύνσεων IP πηγής, διευθύνσεων IP προορισμού και αριθμών θυρών TCP/UDP (Chilukuri, 2017). Αυτός ο μηχανισμός βοηθά στην αποτελεσματική αξιοποίηση των πόρων και διασφαλίζει ότι τα πακέτα μεταξύ ενός συγκεκριμένου ζεύγους πηγής και προορισμού ακολουθούν την ίδια διαδρομή, γεγονός που είναι επωφελές για εφαρμογές που απαιτούν τάξη πακέτων, ιδίως σε παλαιά συστήματα (Muhammet Emin Kamiloğlu, 2015).

Ωστόσο, η εξισορρόπηση φορτίου που βασίζεται αποκλειστικά στις διευθύνσεις IP πηγής και προορισμού έχει περιορισμούς. Ενδέχεται να μην αξιοποιεί πλήρως όλες τις διαθέσιμες συνδέσεις, ιδίως σε σενάρια όπου επιλέγεται μια μόνιμη ενιαία διαδρομή για ένα πολύ χρησιμοποιούμενο ζεύγος πηγής-προορισμού, όπως ένα τείχος προστασίας και ένας διακομιστής ιστού. Αυτός ο περιορισμός μειώνει το πλεονέκτημα της ύπαρξης πολλαπλών διαθέσιμων διαδρομών για το ίδιο ζεύγος κεντρικών υπολογιστών (Chilukuri, 2017).

Η αποτελεσματικότητα οποιασδήποτε στρατηγικής εξισορρόπησης φορτίου εξαρτάται από την κατανομή της κυκλοφορίας. Με μεγαλύτερο αριθμό ζευγών IP πηγής-προορισμού, η κατανομή του φορτίου βελτιώνεται. Η ομοιόμορφη κατανομή της κίνησης μεταξύ των ζευγών υποδοχής μετριάζει τα προβλήματα πόλωσης, αλλά αν λίγα ζεύγη υποδοχής παράγουν σημαντική κίνηση δικτύου, η πόλωση μπορεί να γίνει σημαντικό πρόβλημα (Chilukuri, 2017).

Οι νεοεγκατεστημένοι μεταγωγείς Catalyst συνήθως προεπιλέγουν εξισορρόπηση φορτίου με βάση τις διευθύνσεις IP πηγής και προορισμού, καθώς και τους αριθμούς θυρών TCP/UDP. Αυτή η διαμόρφωση συμβάλλει στη μείωση της πιθανότητας πόλωσης με την ενσωμάτωση πρόσθετων παραμέτρων στο σχήμα εξισορρόπησης φορτίου. Οι μεταγωγείς CiscoCatalyst προσφέρουν διάφορες τεχνικές και λειτουργίες εξισορρόπησης φορτίου που μπορούν να προσαρμοστούν σε συγκεκριμένα μοντέλα υλικού και εκδόσεις λογισμικού. Για περαιτέρω προσαρμογή και βελτιστοποίηση, συνιστάται η συμβουλευτική στο Cisco.com για λεπτομέρειες διαμόρφωσης (Froom&Frahim, 2015).

Η μεταγωγή διεργασίας χρησιμοποιείται μόνο όταν είναι απολύτως απαραίτητο, καθώς επηρεάζει σημαντικά την απόδοση.

Στη μεταγωγή Cisco Catalyst, η "γρήγορη μεταγωγή" **περιλαμβάνει προσωρινή αποθήκευση διαδρομών**, ενώ η "μεταγωγή βάσει τοπολογίας" ή η χρήση CEF με κατανεμημένη προώθηση υλικού χρησιμοποιείται για αποδοτική λειτουργία (Froom&Frahim, 2015).

Προσωρινή αποθήκευση διαδρομής

Η προσωρινή αποθήκευση διαδρομών στους μεταγωγείς Cisco Catalyst λειτουργεί παρόμοια με τη γρήγορη μεταγωγή. Για να λειτουργήσει η προσωρινή αποθήκευση διαδρομής, η διεύθυνση MAC προορισμού ενός εισερχόμενου πλαισίου πρέπει να αντιστοιχεί σε μια διασύνδεση μεταγωγέα με δυνατότητες επιπέδου 3.

Το πρώτο πακέτο σε μια ροή δεδομένων επεξεργάζεται από τον επεξεργαστή δρομολόγησης με τη χρήση λογισμικού, επειδή δεν υπάρχει υπάρχουσα καταχώρηση προσωρινής αποθήκευσης για αυτή τη νέα ροή.

Μόλις ο επεξεργαστής δρομολόγησης λάβει μια απόφαση προώθησης, αυτή καταγράφεται σε έναν πίνακα προσωρινής αποθήκευσης, γνωστό ως πίνακας προώθησης υλικού.

Τα επόμενα πακέτα της ίδιας ροής δρομολογούνται στη συνέχεια μέσω υλικού χρησιμοποιώντας ειδικά κυκλώματα διασύνδεσης που ονομάζονται ASIC.

Ο μεταγωγέας ενημερώνει τον πίνακα προώθησης υλικού όταν εντοπίζει νέες ροές κυκλοφορίας, ενώ οι καταχωρήσεις σε αυτόν τον πίνακα λήγουν αυτόματα εάν δεν χρησιμοποιηθούν μέσα σε ένα καθορισμένο χρονικό διάστημα (Froom&Frahim, 2015).

Η προσωρινή αποθήκευση διαδρομής διασφαλίζει ότι τουλάχιστον ένα πακέτο σε κάθε ροή επεξεργάζεται με τη χρήση λογισμικού και είναι επίσης γνωστή ως μεταγωγή Net Flow LAN, μεταγωγή βάσει ροής ή βάσει ζήτησης και μεταγωγή μία φορά, μεταγωγή πολλές φορές (Froom&Frahim, 2015).

Μεταγωγή με βάση την τοπολογία

Η μεταγωγή βάσει τοπολογίας, γνωστή και ως Cisco Express Forwarding (CEF), είναι ένα βασικό χαρακτηριστικό των μεταγωγέων Cisco Catalyst που βελτιώνει την απόδοση μεταγωγής επιπέδου 3. Αυτή η μέθοδος προτιμάται έναντι της προσωρινής αποθήκευσης διαδρομών λόγω της ανώτερης απόδοσης και της επεκτασιμότητάς της.

Hardware Forward

Η μεταγωγή πακέτων επιπέδου 3 σε μεταγωγείς Catalyst μπορεί να πραγματοποιηθεί σε δύο διαφορετικές ρυθμίσεις:

- κεντρική συγκεντρωτική
- ή κατανεμημένη.

Η συγκεντρωτική μεταγωγή πραγματοποιείται σε μια μονάδα επόπτη, ενώ η κατανεμημένη μεταγωγή λαμβάνει χώρα σε μεμονωμένες μονάδες γραμμής.

Η συγκεντρωτική μεταγωγή προσφέρει πλεονεκτήματα όπως χαμηλότερο κόστος υλικού και απλούστερη διαχείριση. Αντίθετα, η κατανεμημένη μεταγωγή είναι καταλληλότερη για την επέκταση και τη διαχείριση κεντρικών δικτύων μεγάλων επιχειρήσεων.

Συνήθως, οι μικρότεροι μεταγωγείς χρησιμοποιούν συγκεντρωτική μεταγωγή. Ορισμένοι από αυτούς τους μικρότερους μεταγωγείς μπορεί να ενσωματώνουν μια σχεδίαση switch-on-chip (SOC), όπου όλες οι λειτουργίες του μεταγωγέα διεκπεραιώνονται από ένα ενιαίο, χαμηλού κόστους ASIC. Αυτός ο σχεδιασμός έχει γίνει κοινός στην αγορά για μεταγωγείς φιλικούς προς τον προϋπολογισμό με περιορισμένες δυνατότητες. Ορισμένα μοντέλα Catalyst και Nexus της Cisco με σταθερό αριθμό θυρών χρησιμοποιούν συχνά αυτή την προσέγγιση.

Οι προηγμένοι αρθρωτοί μεταγωγείς, όπως το Nexus 9000, μπορούν να ενσωματώσουν την τεχνολογία SOC, η οποία συνδυάζει παραδοσιακές και κατανεμημένες μεθόδους μεταγωγής. Σε αυτούς τους μεταγωγείς, κάθε μονάδα γραμμής μπορεί να διαθέτει

το δικό της SOC, επιτρέποντάς τους να αξιοποιήσουν αποτελεσματικά τις αρχές της κατανεμημένης μεταγωγής, διατηρώντας παράλληλα αποδοτικές επιδόσεις (Froom&Frahim, 2015).

Έννοιες δρομολόγησης

Η δρομολόγηση δικτύου περιλαμβάνει την επιλογή της καλύτερης διαδρομής για την κίνηση των δεδομένων μέσω ενός ή περισσότερων δικτύων. Η έννοια αυτή είναι εφαρμόσιμη σε διάφορους τύπους δικτύων, συμπεριλαμβανομένων των τηλεφωνικών συστημάτων και των δικτύων δημόσιας συγκοινωνίας.

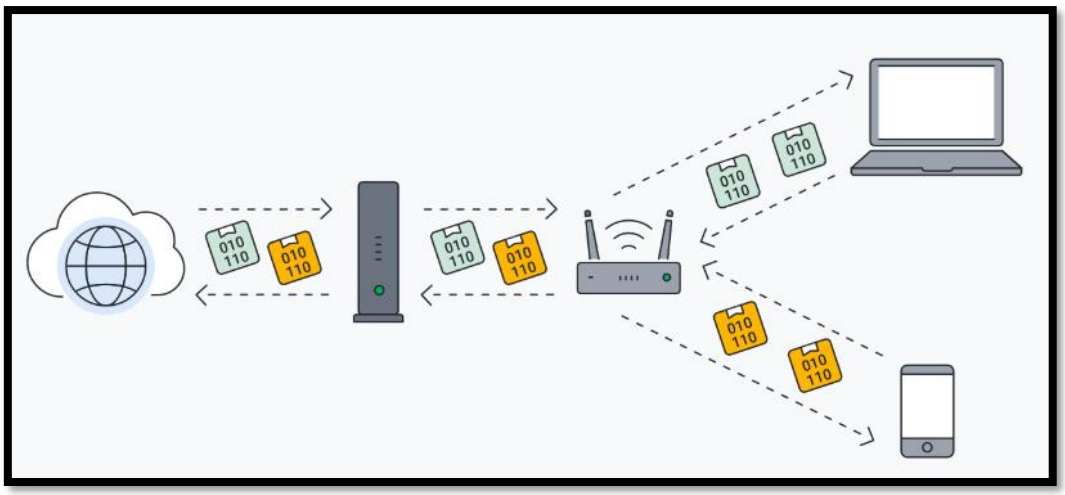
Στα δίκτυα μεταγωγής πακέτων, όπως το Διαδίκτυο, η δρομολόγηση περιλαμβάνει τον καθορισμό των διαδρομών για τα πακέτα του πρωτοκόλλου Διαδικτύου (IP) που θα ταξιδέψουν από την πηγή τους στον προορισμό τους. Οι εξειδικευμένες συσκευές που είναι γνωστές ως δρομολογητές είναι υπεύθυνες για τη λήψη αυτών των αποφάσεων δρομολόγησης (Anagnostopoulos&Zaslavsky, 2014).

Οι δρομολογητές χρησιμοποιούν εσωτερικούς πίνακες δρομολόγησης για να βρίσκουν τις πιο αποδοτικές διαδρομές για τη δρομολόγηση των πακέτων. Ένας πίνακας δρομολόγησης περιέχει λεπτομερείς πληροφορίες σχετικά με τις διαδρομές που πρέπει να ακολουθήσουν τα πακέτα για να φτάσουν στον προορισμό τους, τις οποίες διαχειρίζεται ο δρομολογητής (Poss&Raack, 2012).

Όταν ένας δρομολογητής λαμβάνει ένα πακέτο, εξετάζει την επικεφαλίδα του πακέτου για να προσδιορίσει τον προορισμό του,

Στη συνέχεια, ο δρομολογητής συμβουλεύεται τον πίνακα δρομολόγησής του για να καθορίσει την καλύτερη διαδρομή για το πακέτο.

Αυτή η διαδικασία λαμβάνει χώρα εκατομμύρια φορές ανά δευτερόλεπτο, καθώς οι δρομολογητές διαχειρίζονται τεράστιες ποσότητες κίνησης πακέτων.



Εικόνα 17 Δρομολογητής.

\

Τα πακέτα μπορεί να ανακατευθυνθούν πολλές φορές από διαφορετικούς δρομολογητές κατά τη διαδρομή τους.

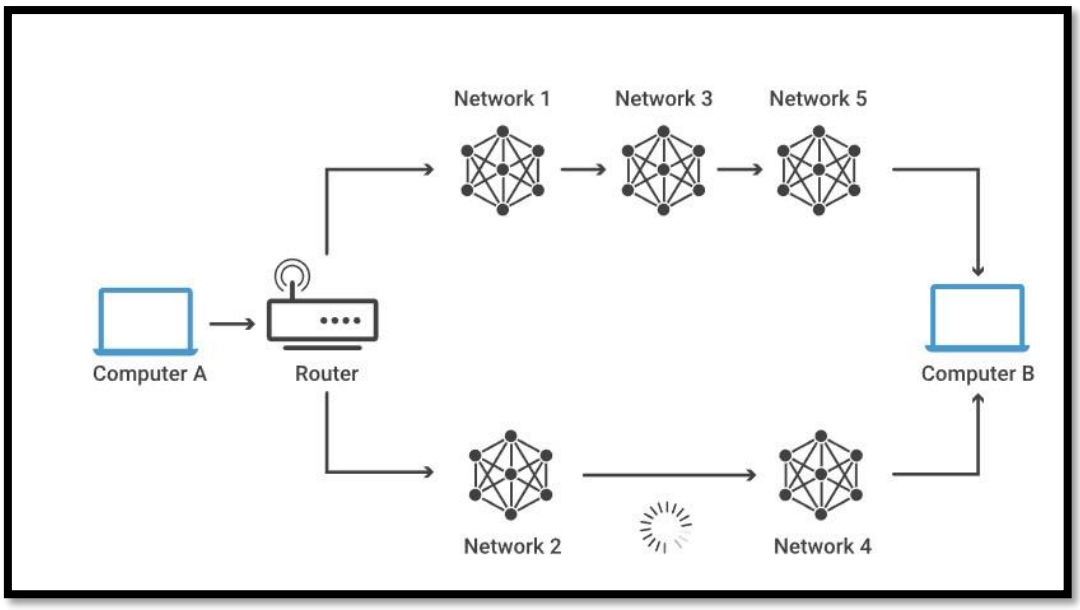
Οι πίνακες δρομολόγησης είναι δύο τύπων:

- στατικοί
- και δυναμικοί.

Οι στατικοί πίνακες δρομολόγησης είναι σταθεροί και απαιτούν χειροκίνητη διαμόρφωση από το διαχειριστή του δικτύου. Αυτοί οι πίνακες καθορίζουν προκαθορισμένες διαδρομές για τα πακέτα δεδομένων, οι οποίες παραμένουν αμετάβλητες, εκτός αν προσαρμοστούν χειροκίνητα από τον διαχειριστή (Poss&Raack, 2012).

Αντίθετα, οι δυναμικοί πίνακες δρομολόγησης ενημερώνονται αυτόματα. Οι δυναμικοί πίνακες χρησιμοποιούν διάφορα πρωτόκολλα δρομολόγησης για να αξιολογήσουν και να επιλέξουν τις πιο αποδοτικές διαδρομές με βάση την καθυστέρηση των πακέτων,

Τα μικρότερα δίκτυα χρησιμοποιούν συχνά στατική δρομολόγηση λόγω των χαμηλότερων υπολογιστικών απαιτήσεων σε σύγκριση με τη δυναμική δρομολόγηση. Ωστόσο, για μεσαία και μεγάλα δίκτυα, η δυναμική δρομολόγηση είναι συνήθως πιο αποτελεσματική, επειδή προσαρμόζεται στις μεταβαλλόμενες συνθήκες του δικτύου και βελτιστοποιεί αποτελεσματικότερα τα μονοπάτια δρομολόγησης (Anagnostopoulos&Zaslavsky, 2014).



Εικόνα18 Δρομολόγηση δικτύου. Πηγή: Cloudflare (2024)

Κύρια πρωτόκολλα δρομολόγησης

Στη δικτύωση, ένα πρωτόκολλο ορίζει τους κανόνες για τη δόμηση των δεδομένων, ώστε οι διασυνδεδεμένες συσκευές να μπορούν να τα κατανοήσουν.

Ένα πρωτόκολλο δρομολόγησης είναι ένα σύνολο κανόνων που χρησιμοποιούνται για τον καθορισμό ή την ανακοίνωση διαδρομών δικτύου. Αυτά τα πρωτόκολλα επιτρέπουν στους δρομολογητές να ανταλλάσσουν πληροφορίες για τον προσδιορισμό των αποδοτικότερων διαδρομών μεταξύ των κόμβων ενός δικτύου. Οι δρομολογητές χρησιμοποιούν αυτά τα πρωτόκολλα για να κατευθύνουν τα πακέτα δεδομένων από τον ένα δρομολογητή στον άλλο μέσω των δικτύων μέχρι να φτάσουν στον προορισμό τους.

Τα πρωτόκολλα δρομολόγησης επιτρέπουν στο δίκτυο να προσαρμόζεται δυναμικά στις αλλαγές, διασφαλίζοντας ότι οι αποφάσεις δρομολόγησης δεν είναι άκαμπτες αλλά μπορούν να προσαρμόζονται ανάλογα με τις ανάγκες. Το Διαδίκτυο βασίζεται στα πρωτόκολλα δρομολόγησης για τη διατήρηση της ανοχής σε σφάλματα και της υψηλής διαθεσιμότητας, με την προσαρμογή στις μεταβαλλόμενες συνθήκες του δικτύου (Akkaya&Younis, 2005).

Τα δυναμικά πρωτόκολλα δρομολόγησης χρησιμοποιούνται για τη διευκόλυνση της ανταλλαγής πληροφοριών δρομολόγησης μεταξύ δρομολογητών.

Οι κύριοι στόχοι τους είναι :

- να βρίσκουν και να εντοπίζουν απομακρυσμένα δίκτυα,
- να διατηρούν τις πληροφορίες δρομολόγησης ενημερωμένες,
- να καθορίζουν την πιο αποτελεσματική διαδρομή προς τα δίκτυα προορισμού
- και να βρίσκουν εναλλακτικές διαδρομές εάν η τρέχουσα διαδρομή καθίσταται μη διαθέσιμη.

Στοιχεία των δυναμικών πρωτοκόλλων δρομολόγησης:

- Αλγόριθμος: Μια πεπερασμένη ακολουθία βημάτων που χρησιμοποιούνται για την επίλυση ενός προβλήματος. Τα πρωτόκολλα δρομολόγησης χρησιμοποιούν αλγόριθμους για την επεξεργασία πληροφοριών δρομολόγησης και την εύρεση της βέλτιστης διαδρομής.

-Μηνύματα πρωτοκόλλου δρομολόγησης: Μηνύματα που βοηθούν τους δρομολογητές να ανακαλύπτουν γείτονες, να ανταλλάσσουν πληροφορίες δρομολόγησης και να εκτελούν άλλες εργασίες όπως η ενημέρωση των δεδομένων του δικτύου.

- Δομές δεδομένων: που χρησιμοποιούνται από τα πρωτόκολλα δρομολόγησης για τη διαχείριση πληροφοριών δρομολόγησης (GarcíaVillalbaetal., 2009).

Λειτουργική διαδικασία:

1. Οι δρομολογητές στέλνουν και λαμβάνουν μηνύματα δρομολόγησης μέσω των διεπαφών τους.

2. Οι δρομολογητές ανταλλάσσουν μηνύματα δρομολόγησης και δεδομένα με άλλους δρομολογητές που χρησιμοποιούν το ίδιο πρωτόκολλο.

3. Μοιράζονται πληροφορίες δρομολόγησης για να μαθαίνουν για απομακρυσμένα δίκτυα.

4. Όταν ανιχνεύονται αλλαγές τοπολογίας, οι δρομολογητές μπορούν να μεταδίδουν τις πληροφορίες αυτές σε άλλους δρομολογητές.

. Τα διάφορα πρωτόκολλα δρομολόγησης έχουν διαφορετικούς ρυθμούς σύγκλισης και ταξινομούνται σε κατηγορίες όπως classful ή classless, distance vector ή link-state και Interior Gateway Protocol (IGP) ή Exterior Gateway Protocol (EGP) (García Villalbaetal., 2009).

Μερικά από τα πρωτόκολα

Πρωτόκολλα διανύσματος απόστασης:

Τα πρωτόκολλα διανύσματος απόστασης χρησιμοποιούν δρομολογητές για να αναμεταδίδουν πληροφορίες κατά μήκος της διαδρομής προς τον προορισμό. Η άποψη κάθε δρομολογητή για το δίκτυο περιορίζεται στην απόσταση ή τη μετρική για την επίτευξη ενός απομακρυσμένου δικτύου και τη διεπαφή που χρησιμοποιείται. Αυτά τα πρωτόκολλα δεν παρέχουν πλήρη εικόνα της τοπολογίας του δικτύου. Παραδείγματα περιλαμβάνουν το πρωτόκολλο πληροφοριών δρομολόγησης (RIP).

Πρωτόκολλα κατάστασης σύνδεσης

Τα πρωτόκολλα κατάστασης συνδέσεων επιτρέπουν στους δρομολογητές να δημιουργούν έναν λεπτομερή χάρτη τοπολογίας δικτύου συλλέγοντας πληροφορίες από όλους τους δρομολογητές του δικτύου. Αυτή η ολοκληρωμένη εικόνα επιτρέπει τον ακριβέστερο προσδιορισμό της διαδρομής σε σύγκριση με τα πρωτόκολλα διανύσματος απόστασης (Boukercheetal., 2011).

Πρωτόκολλα εσωτερικής πύλης (IGP):

Αυτά τα πρωτόκολλα χειρίζονται τη δρομολόγηση εντός ενός AS, γνωστή και ως δρομολόγηση εντός του AS. Χρησιμοποιούνται στα εσωτερικά δίκτυα επιχειρήσεων, οργανισμών και παρόχων υπηρεσιών. Παραδείγματα περιλαμβάνουν τα **RIP**, IGRP, **EIGRP**, **OSPF** και **IS-IS**

RIP

- **<u>Πρωτόκολλο πληροφοριών δρομολόγησης (RIP):</u>**

Το RIP υπολογίζει τις καλύτερες διαδρομές με βάση τον "αριθμό αλμάτων", ο οποίος μετρά τον αριθμό των δρομολογητών από τους οποίους πρέπει να περάσει ένα πακέτο.

Είναι ένα από τα πιο ανθεκτικά πρωτόκολλα δρομολόγησης. Το RIP αποτελείται από τέσσερα βασικά στοιχεία:

- διαδικασία ενημέρωσης δρομολόγησης,
- μετρικές δρομολόγησης RIP,
- σταθερότητα δρομολόγησης
- και χρονομετρητές δρομολόγησης.

Οι συσκευές που υποστηρίζουν το RIP στέλνουν μηνύματα ενημέρωσης δρομολόγησης σε τακτά χρονικά διαστήματα ακόμα και όταν αλλάζει η τοπολογία του δικτύου. Αυτά τα πακέτα RIP περιέχουν πληροφορίες σχετικά με τα δίκτυα που μπορούν να προσεγγίσουν οι συσκευές, καθώς και τον αριθμό των δρομολογητών ή πυλών που πρέπει να περάσει ένα πακέτο για να φτάσει στη διεύθυνση προορισμού. Το RIP τηρεί τα ακόλουθα χαρακτηριστικά διανύσματος απόστασης (Manzooretal., 2020):

- αποστέλλει περιοδικές ενημερώσεις δρομολόγησης (κάθε 30 δευτερόλεπτα)
- αποστέλλει τον πλήρη πίνακα δρομολόγησης σε κάθε περιοδική ενημέρωση
- χρησιμοποιεί μια μορφή απόστασης ως μετρική (στην προκειμένη περίπτωση, τον αριθμό των αλμάτων)
- χρησιμοποιεί τον αλγόριθμο Bellman-Ford Distance Vector για να καθορίσει το καλύτερο «μονοπάτι» προς έναν συγκεκριμένο προορισμό.

Το πρωτόκολλο πληροφοριών δρομολόγησης χρησιμοποιεί τους ακόλουθους χρονιστές ως μέρος της λειτουργίας του (Manzooretal., 2020):

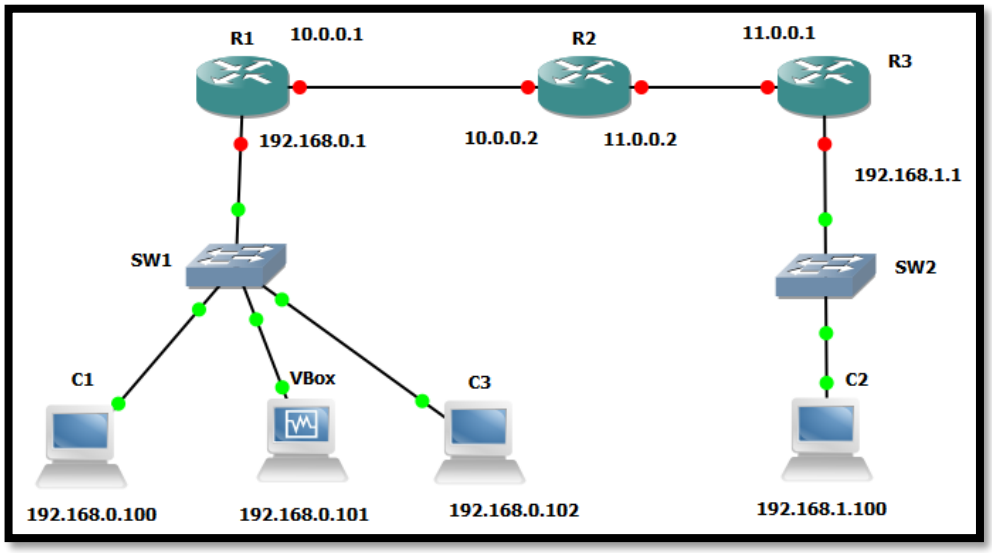
- Χρονοδιακόπτης ενημέρωσης
- Χρονοδιακόπτης μη έγκυρης ενημέρωσης
- Χρονοδιακόπτης έκπλυσης
- Χρονοδιακόπτης αναμονής

RIPv1

Ένα πρωτόκολλο κλάσης, μεταδίδει ενημερώσεις κάθε 30 δευτερόλεπτα, περίοδος αναμονής 180 δευτερόλεπτα. Ο αριθμός των μεταπηδήσεων είναι μετρική (μέγιστο 15). Το RIP υποστηρίζει έως και έξι μονοπάτια ίσου κόστους προς έναν προορισμό, όπου και τα έξι μονοπάτια μπορούν να τοποθετηθούν στον πίνακα δρομολόγησης και ο δρομολογητής μπορεί να κάνει load-balance μεταξύ τους. Η προεπιλογή είναι στην

πραγματικότητα τέσσερα μονοπάτια, αλλά αυτό μπορεί να αυξηθεί μέχρι το μέγιστο των έξι. Υπενθυμίζεται ότι ένα μονοπάτι ίσου κόστους είναι εκείνο όπου η τιμή του αριθμού των μεταπηδήσεων είναι η ίδια. Το RIP δεν θα εξισορροπήσει το φορτίο σε μονοπάτια άνισου κόστους (Manzooretal., 2020).

Από τη δεκαετία του 1990, το Πρωτόκολλο Πληροφοριών Δρομολόγησης έκδοση 2, μερικές φορές γνωστό ως RIPv2, είχε ευρεία υιοθέτηση, ωστόσο δεν είναι πλέον λειτουργικό. Ο μέγιστος αριθμός των 15 αλμάτων που μπορεί να υποστηρίξει και ο χρόνος που χρειάζεται για τον επανυπολογισμό των διαδρομών συμβάλλουν και τα δύο στα προβλήματα κλιμάκωσής του, γεγονός που το καθιστά λιγότερο κατάλληλο για χρήση σε σύγχρονα δίκτυα. Συνήθως μπορεί να βρεθεί σε δίκτυα που έχουν ξεπεραστεί ή σε δρομολογητές καταναλωτικής ποιότητας που είναι φθηνοί (Manzooretal., 2020).



Εικόνα20 RIPv1

OSPF: Open Shortest Path First (OSPF)

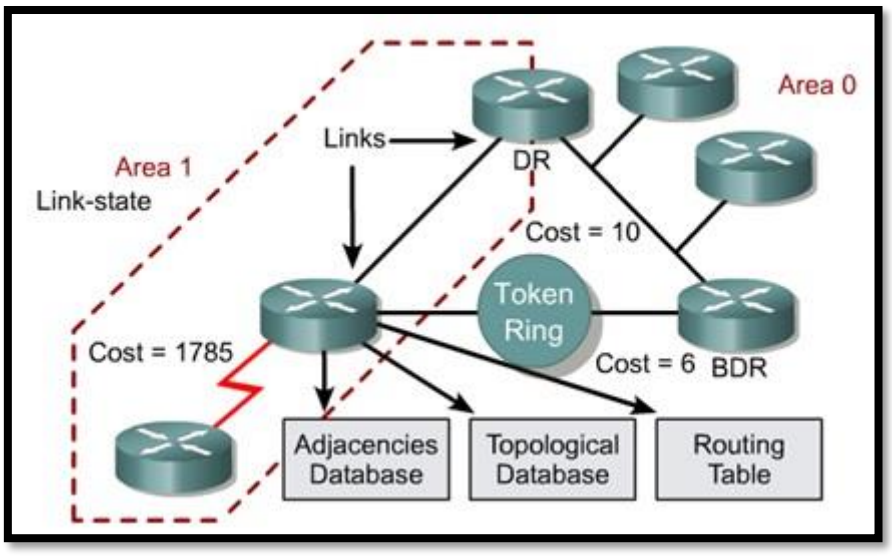
Το OSPF βοηθά τους δρομολογητές να καθορίζουν δυναμικά τις πιο αποδοτικές διαδρομές για την παράδοση πακέτων

Είναι δυνατόν να ρυθμιστεί με πιο περίπλοκο τρόπο- ωστόσο, όταν γίνει κατανοητό, η διαχείρισή του γίνεται μάλλον απλή. Το Open Shortest Path First (OSPF) χρησιμοποιείται συχνά σε δίκτυα που δεν εξαρτώνται αποκλειστικά από τη Cisco ή που είναι μεγαλύτερης κλίμακας (Manzooretal., 2020).

Το OSPF υλοποιεί έναν μηχανισμό για την ασφαλή μετάδοση των μηνυμάτων.

Για τον υπολογισμό της συντομότερης διαδρομής χρησιμοποιείται ο αλγόριθμος Dijkstra. Ο αλγόριθμος σχεδιάζει γραφήματα που έχουν εκχωρήσει σε κάθε τμήμα μεταξύ δύο ενδιάμεσων σημείων ένα ορισμένο κόστος, το οποίο προκύπτει ως αποτέλεσμα ενός τύπου. Η γειτνίαση στην περίπτωση του OSPF πραγματοποιείται με μηνύματα τύπου Hello που αποστέλλονται κάθε 10 δευτερόλεπτα και δημιουργείται μόνο με τους γείτονες και όχι με τους άλλους δρομολογητές. Για το μοντέλο αυτό, κάθε δρομολογητής θα έχει ένα αναγνωριστικό. Ο αριθμός των δικτύων καθορίζει τον αριθμό των LSA που εμφανίζονται στον πίνακα δρομολόγησης κάθε δρομολογητή. Το πλεονέκτημα αυτού του γεγονότος είναι ότι ανά πάσα στιγμή θα βρεθεί μια εναλλακτική διαδρομή σε περίπτωση αποτυχίας μιας σύνδεσης, αλλά αυτό έρχεται με πολλούς πρόσθετους πόρους που απαιτούνται.

Ένα άλλο πλεονέκτημα του OSPF είναι ότι μπορεί επίσης να χωρίσει μια τοπολογία σε περισσότερες περιοχές. Αυτό λειτουργεί μεταξύ των περιοχών ως πρωτόκολλο δρομολόγησης διανύσματος απόστασης και εντός των περιοχών (areas) ως πρωτόκολλο κατάστασης συνδέσεων. Αυτό συμβαίνει επειδή μεταξύ των περιοχών δεν έχει ολόκληρο όραμα, και εντός των περιοχών, αυτό γνωρίζει ολόκληρη την τοπολογία. Το πρωτόκολλο OSPF επικοινωνεί μέσω μηνυμάτων πολλαπλής διανομής με χρήση των IP 224.0.0.5 και 224.0.0.0.6 (Dumitracheetal., 2017).



Εικόνα20 OSPF

EIGRP Enhanced Interior Gateway Routing Protocol (EIGRP)

Το EIGRP είναι ένα υβριδικό πρωτόκολλο διανύσματος απόστασης που είναι πιο προηγμένο από το RIPv2. Προσφέρει καλύτερη επεκτασιμότητα και ταχύτερη σύγκλιση από το RIPv2.

Λόγω της ταχύτητάς του και της ευκολίας με την οποία μπορεί να διαχειριστεί, χρησιμοποιείται όλο και περισσότερο για ακαδημαϊκά δίκτυα.

Αποτελεί ένα πρωτόκολλο εσωτερικής πύλης κατάλληλο για πολλές διαφορετικές τοπολογίες και μέσα. Σε ένα καλά σχεδιασμένο δίκτυο, το EIGRP κλιμακώνεται καλά και παρέχει εξαιρετικά γρήγορους χρόνους σύγκλισης με ελάχιστη κίνηση δικτύου. Ορισμένα από τα πλεονεκτήματα του EIGRP είναι τα εξής (Savage, et. al., 2013):

- Πολύ χαμηλή χρήση των πόρων του δικτύου κατά την κανονική λειτουργία- σε ένα σταθερό δίκτυο μεταδίδονται μόνο πακέτα hello
- Όταν συμβαίνει μια αλλαγή, διαδίδονται μόνο οι αλλαγές στον πίνακα δρομολόγησης και όχι ολόκληρος ο πίνακας δρομολόγησης- αυτό μειώνει το φορτίο που θέτει το ίδιο το πρωτόκολλο δρομολόγησης στο δίκτυο
- Ταχείς χρόνοι σύγκλισης για αλλαγές στην τοπολογία του δικτύου (σε ορισμένες περιπτώσεις η σύγκλιση μπορεί να είναι σχεδόν στιγμιαία).

Βασίζεται στον αλγόριθμο διάχυτης ενημέρωσης (DUAL) για τον υπολογισμό της συντομότερης διαδρομής προς έναν προορισμό εντός ενός δικτύου.

Ο αλγόριθμος διάχυτης ενημέρωσης (DUAL) είναι ο αλγόριθμος που χρησιμοποιείται για την επίτευξη της ελευθερίας βρόχων σε κάθε στιγμή καθ' όλη τη διάρκεια του υπολογισμού μιας διαδρομής. Αυτό επιτρέπει σε όλους τους δρομολογητές που εμπλέκονται σε μια αλλαγή τοπολογίας να συγχρονίζονται ταυτόχρονα. Οι δρομολογητές που δεν επηρεάζονται από τις αλλαγές τοπολογίας δεν συμμετέχουν στον επανϋπολογισμό. Ο χρόνος σύγκλισης με το DUAL συναγωνίζεται αυτόν οποιουδήποτε άλλου υπάρχοντος πρωτοκόλλου δρομολόγησης (Chenetal., 2016).

1) Το EIGRP αποτελείται από τέσσερα βασικά στοιχεία:

- Ανακάλυψη/ανάκτηση γειτόνων Πρωτόκολλο αξιόπιστης μεταφοράς
- DUAL Μηχανή πεπερασμένων καταστάσεων
- Εξαρτώμενες από το πρωτόκολλο ενότητες

2) Το EIGRP χρησιμοποιεί πέντε τύπους πακέτων:

- Hello /επιβεβαίωση
- Ενημερώσεις

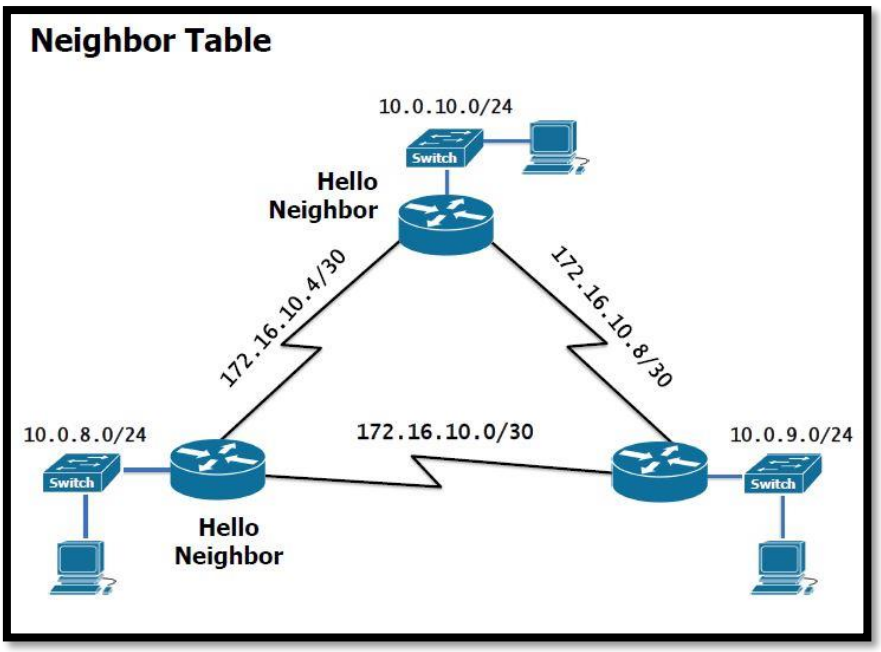
- Ερωτήσεις
- Απαντήσεις
- Αιτήματα

Το EIGRP, αντί να υπολογίζει σε πλήρεις περιοδικές ενημερώσεις για την επανασύγκλιση, δημιουργεί έναν πίνακα τοπολογίας από κάθε διαφήμιση του γείτονά του (αντί να απορρίπτει τα δεδομένα) και συγκλίνει είτε αναζητώντας μια πιθανή διαδρομή χωρίς βρόχους στον πίνακα τοπολογίας είτε, αν δεν γνωρίζει άλλη διαδρομή, ρωτώντας τους γείτονές του. Είναι προφανές ότι το EIGRP πρέπει να παρέχει (Savage, et. al., 2013):

- Ένα σύστημα όπου στέλνει μόνο τις ενημερώσεις που χρειάζεται σε μια δεδομένη στιγμή- αυτό επιτυγχάνεται μέσω της ανακάλυψης και της συντήρησης των γειτόνων
- Έναν τρόπο προσδιορισμού των μονοπατιών που έχει μάθει ένας δρομολογητής χωρίς βρόχους
- Μια διαδικασία για την εκκαθάριση των κακών διαδρομών από τους πίνακες τοπολογίας όλων των δρομολογητών του δικτύου
- Μια διαδικασία για την αναζήτηση γειτόνων για την εύρεση διαδρομών προς χαμένους προορισμούς

Εμπορική εφαρμογή του EIGRP (Lammle, 2000):

- Είναι λιγότερο πολύπλοκο στην υλοποίηση και προσφέρει επίσης αποδοτικούς υπολογισμούς διαδρομών σε σύγκριση με το OSPF, π.χ. το EIGRP χρησιμοποιεί το εύρος ζώνης, την καθυστέρηση, την αξιοπιστία και το φορτίο κατά τον υπολογισμό των βέλτιστων διαδρομών, ενώ το OSPF λαμβάνει υπόψη μόνο το εύρος ζώνης κατά τον υπολογισμό των βέλτιστων διαδρομών.
- Λαμβάνοντας υπόψη τα παραπάνω σημεία, το EIGRP θα είναι πιο βιώσιμο εμπορικά υπό την προϋπόθεση ότι πρόκειται για μια πλήρη endtoend υλοποίηση της Cisco- μπορεί επίσης να αναδιανέμει πληροφορίες δρομολόγησης με άλλα πρωτόκολλα δρομολόγησης με αναδιανομή δρομολογητών.



Εικονα21 EIGRP

- Ενδιάμεσο σύστημα προς ενδιάμεσο σύστημα (IS-IS): χρησιμοποιείται για τη δρομολόγηση εντός ενός AS.

Αυτόνομο σύστημα

Ένα Αυτόνομο Σύστημα (AS) αναφέρεται σε μια συλλογή δρομολογητών που διαχειρίζεται μια ενιαία οντότητα, όπως μια εταιρεία ή ένας οργανισμός. Αυτό το σύστημα, γνωστό και ως τομέας δρομολόγησης, συχνά περιλαμβάνει τόσο το εσωτερικό δίκτυο μιας εταιρείας όσο και εκείνο ενός παρόχου υπηρεσιών Διαδικτύου (ISP). Το Διαδίκτυο βασίζεται στην έννοια των Αυτόνομων Συστημάτων, γεγονός που καθιστά αναγκαία την ύπαρξη δύο βασικών τύπων πρωτοκόλλων δρομολόγησης (Ali, Tabassum&Mathew, 2016):

Πρωτόκολλα εξωτερικής πύλης (EGP):

Αυτά τα πρωτόκολλα διαχειρίζονται τη δρομολόγηση μεταξύ διαφορετικών αυτόνομων συστημάτων, γνωστή ως δρομολόγηση μεταξύ των AS. Επιτρέπουν τη συνδεσιμότητα μεταξύ παροχών υπηρεσιών και μεγάλων επιχειρήσεων. Το πρωτόκολλο πύλης συνόρων (BGP) είναι το κύριο και επί του παρόντος το μόνο λειτουργικό EGP που χρησιμοποιείται για το σκοπό αυτό. Λόγω της κυριαρχίας του BGP, ο όρος EGP χρησιμοποιείται σπάνια- οι μηχανικοί συνήθως αναφέρονται απευθείας στο BGP.

Πρωτόκολλο πύλης συνόρων (BGP)

Μεταξύ των διαφόρων πρωτοκόλλων δρομολόγησης που χρησιμοποιούνται για την επικοινωνία μεταξύ δικτύων, το BGP ξεχωρίζει ως το πιο βασικό. Το BGP είναι ένα πρωτόκολλο εξωτερικής πύλης που χρησιμοποιείται για τη μετάδοση πληροφοριών δρομολόγησης σε διάφορα δίκτυα. Αυτό έρχεται σε αντίθεση με τα πρωτόκολλα εσωτερικής πύλης, όπως το EIGRP και το OSPF, τα οποία χρησιμοποιούνται για τη βελτιστοποίηση της δρομολόγησης εντός ενός δικτύου.

Το BGP χρησιμοποιείται για τη δήλωση της κυριότητας των διευθύνσεων IP και τη δημιουργία συνδέσεων μεταξύ διαφορετικών δικτύων. Λειτουργεί εντός μεγάλων δικτύων που ονομάζονται αυτόνομα συστήματα και ανταλλάσσει δυναμικά πληροφορίες δρομολόγησης για την εύρεση της καλύτερης διαδρομής για τα πακέτα.

Για τη διασύνδεση με τους παρόχους υπηρεσιών διαδικτύου (ISP), το πρωτόκολλο πύλης εκπομπής (BGP) χρησιμοποιείται στην άκρη του δικτύου. Το BGP είναι το θεμελιώδες πρωτόκολλο δρομολόγησης για το Διαδίκτυο(Manzooretal., 2020).

Ο αλγόριθμος καλύτερης διαδρομής στο BGP λειτουργεί με βάση τα χαρακτηριστικά της διαδρομής. Κάθε χαρακτηριστικό διαδρομής συνδέεται με μια συγκεκριμένη τιμή. Μόνο ένα χαρακτηριστικό διαδρομής θα λαμβάνεται υπόψη κάθε φορά. Ο αλγόριθμος χαρακτηριστικών διαδρομής λειτουργεί ως εξής (Manzoor et al., 2020):

- Προτιμά τη διαδρομή με το υψηλότερο ΒΑΡΟΣ. Πρόκειται για παράμετρο ιδιοκτησίας της Cisco, η οποία είναι τοπική στους δρομολογητές στους οποίους αποδίδεται το WEIGHT.

- Προτιμά τη διαδρομή με την υψηλότερη LOCAL_PREFERENCE. Έχει οριστεί 100 από προεπιλογή, ωστόσο προσαρμόζεται.

- Προτιμά τη διαδρομή που είναι τοπικά ORIGINATED. Οι τοπικές διαδρομές προτιμώνται εξ ορισμού.

- Προτιμά τη διαδρομή με το συντομότερο AS_PATH.

- Προτίμηση του eBGP έναντι του iBGP.

- Προτιμά τη διαδρομή με το χαμηλότερο MED εάν υπάρχει το ίδιο AS_PATH.

- Επιλέγει τη διαδρομή με την παλαιότερη διαδρομή.

- Προτιμά τη διαδρομή με το μικρότερο ID δρομολογητή.

Για να διασφαλιστεί η εξισορρόπηση φορτίου σε πολλαπλά path_attributes, το BGP παρέχεται με την εισαγωγή maximum-paths ακολουθούμενη από number-of-paths στο δρομολογητή κατά τη διαμόρφωση του BGP. Το BGP μπορεί να διαχειριστεί το πολύ έξι path_attributes (Manzooretal., 2020).

Πρωτόκολλα δικτύου

Τα πρωτόκολλα δικτύου είναι τυποποιημένα σύνολα κανόνων που διέπουν τη μετάδοση δεδομένων μεταξύ συσκευών σε ένα δίκτυο. Εξασφαλίζουν ότι οι συσκευές, ανεξάρτητα από τις εσωτερικές τους λειτουργίες, μπορούν να επικοινωνούν αποτελεσματικά. Τα πρωτόκολλα δικτύου είναι απαραίτητα για την παγκόσμια επικοινωνία στα ψηφιακά συστήματα (GarcíaVillalbaetal., 2009). Η σουίτα πρωτοκόλλων του Διαδικτύου είναι μια σουίτα ανοικτού συστήματος που διευκολύνει την επικοινωνία μεταξύ διασυνδεδεμένων δικτύων και είναι συμβατή τόσο με LAN όσο και με WAN. Τα δύο πιο γνωστά πρωτόκολλα του Διαδικτύου είναι το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP) και το Πρωτόκολλο Διαδικτύου (IP). Αυτά τα πρωτόκολλα, μαζί με πρωτόκολλα χαμηλότερου επιπέδου και τυποποιημένες εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο, η εξομοίωση τερματικών και η μεταφορά αρχείων, αποτελούν τη ραχοκοκαλιά της επικοινωνίας στο Διαδίκτυο (Bhattacharyyaetal., 2010).

Μετρικές πρωτοκόλλου δρομολόγησης

Μερικές φορές, ένα σύστημα δρομολόγησης συναντά πολλαπλές διαδρομές προς τον ίδιο προορισμό. Για να διασφαλιστεί ότι επιλέγεται η βέλτιστη διαδρομή, το πρωτόκολλο δρομολόγησης πρέπει να αναλύει και να συγκρίνει αυτές τις εναλλακτικές λύσεις. Αυτή η διαδικασία περιλαμβάνει τη χρήση μετρικών δρομολόγησης, οι οποίες είναι αριθμητικές τιμές που αποδίδονται σε διαφορετικές διαδρομές από το πρωτόκολλο δρομολόγησης. Οι μετρικές μπορεί να περιλαμβάνουν παράγοντες όπως ο αριθμός των αλμάτων, το εύρος

ζώνης, η καθυστέρηση, η αξιοπιστία και το φορτίο. Χαμηλότερες τιμές μετρικών συνήθως υποδεικνύουν καλύτερες διαδρομές.

Οι βασικές μετρικές που χρησιμοποιούνται από τα πρωτόκολλα δρομολόγησης περιλαμβάνουν:

-Αξιοπιστία: Συχνά αποδίδονται αριθμητικές τιμές από τον διαχειριστή του συστήματος. Οι βαθμολογίες αξιοπιστίας λαμβάνουν υπόψη παράγοντες όπως η συχνότητα των διακοπών και η ευκολία επισκευής των συνδέσεων δικτύου. Τα δίκτυα με υψηλότερες βαθμολογίες αξιοπιστίας προτιμώνται έναντι εκείνων με συχνές διακοπές.

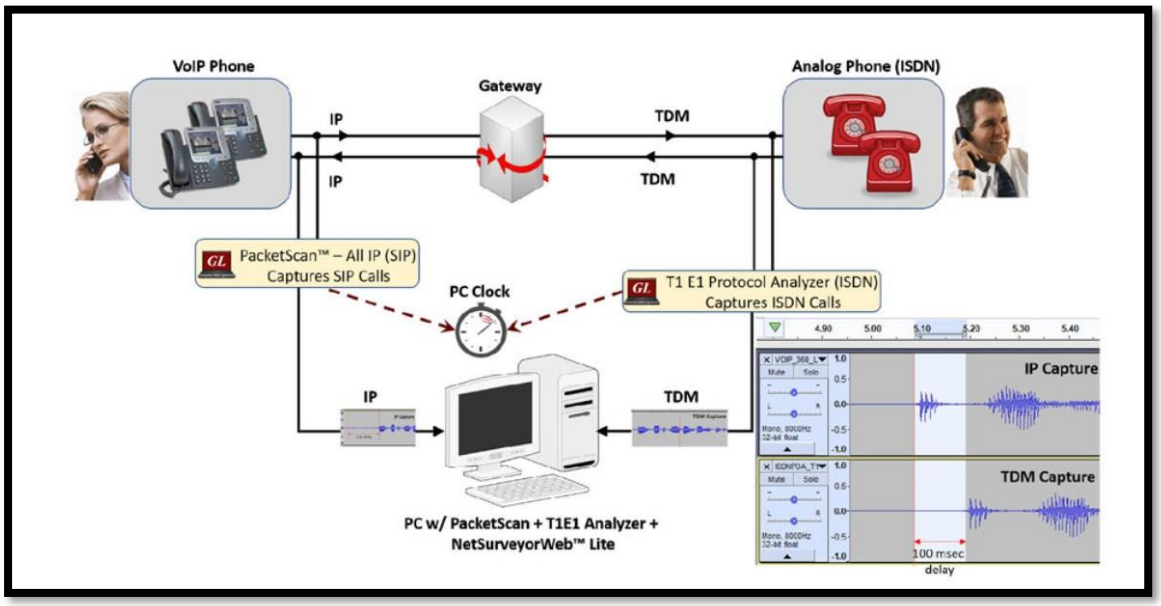
- Καθυστέρηση: Αυτό αντιπροσωπεύει το χρόνο που χρειάζεται ένας δρομολογητής για να επεξεργαστεί, να βάλει στην ουρά και να μεταδώσει ένα datagram σε μια διασύνδεση. Τα πρωτόκολλα χρησιμοποιούν μετρικές καθυστέρησης για την αξιολόγηση της συνολικής καθυστέρησης σε όλες τις συνδέσεις μιας διαδρομής. Η διαδρομή με τη χαμηλότερη τιμή καθυστέρησης θεωρείται η πιο αποδοτική.

- Αριθμός λυκίσκου: Αυτή η μετρική παρακολουθεί τον αριθμό των ενδιάμεσων συσκευών, όπως δρομολογητές, από τις οποίες πρέπει να περάσει ένα πακέτο για να φτάσει στον προορισμό του. Εάν ένα πρωτόκολλο δίνει προτεραιότητα στον αριθμό των αλμάτων, η διαδρομή με τα λιγότερα άλματα θεωρείται η βέλτιστη διαδρομή.

-Φορτίο: Αυτό μετρά το επίπεδο χρήσης ενός πόρου δικτύου, όπως ένας δρομολογητής ή μια σύνδεση. Ο φόρτος μπορεί να αξιολογηθεί με την παρακολούθηση της χρήσης της CPU και των ρυθμών επεξεργασίας πακέτων. Καθώς αυξάνεται η κυκλοφορία, η τιμή του φορτίου αυξάνεται ανάλογα. Το πρωτόκολλο δρομολόγησης λαμβάνει υπόψη το φορτίο για την αποφυγή υπερφορτωμένων συνδέσμων.

- Εύρος ζώνης: Το εύρος ζώνης δηλώνει τη χωρητικότητα μιας σύνδεσης, μετρούμενη σε bit ανά δευτερόλεπτο. Οι συνδέσεις υψηλότερου εύρους ζώνης, όπως οι συνδέσεις gigabit, προτιμώνται έναντι των επιλογών χαμηλότερης χωρητικότητας, όπως οι συνδέσεις 56 kb. Το πρωτόκολλο δρομολόγησης αξιολογεί το εύρος ζώνης κάθε σύνδεσης και ευνοεί διαδρομές με μεγαλύτερο εύρος ζώνης για καλύτερη απόδοση.

Αυτές οι μετρικές βοηθούν τα πρωτόκολλα δρομολόγησης να προσδιορίσουν την πιο αποδοτική διαδρομή λαμβάνοντας υπόψη διάφορους παράγοντες που επηρεάζουν την απόδοση της διαδρομής.



Εικόνα22 Μετρήσεις επιδόσεων δρομολογητή.

Αλγόριθμοι δρομολόγησης

Είναι η διαδικασία με την οποία οι πληροφορίες αφήνουν το σημείο προέλευσής τους και κατευθύνονται μέσω του δικτύου στον τελικό προορισμό τους αναφέρεται ως δρομολόγηση

Σύμφωνα με τους Alotaibi και Mukherjee (2012), κάθε αλγόριθμος καθορίζει την ιδανική διαδρομή λαμβάνοντας υπόψη τη συντομότερη διαδρομή, τον αριθμό των πακέτων και το κόστος κάθε γραμμής. Αυτοί οι παράγοντες καθορίζονται από το εύρος ζώνης, τον ρυθμό μετάδοσης και τον χρόνο που απαιτείται για τη δρομολόγησή τους στο δίκτυο.

. Ωστόσο, υπάρχει μια ποικιλία διαφορετικών διαδρομών που μπορούν να ακολουθηθούν προκειμένου η πληροφορία να φτάσει στον προορισμό της. Η επιλογή της καλύτερης διαδρομής αποτελεί βασικό μέρος της δρομολόγησης, πράγμα που σημαίνει ότι η διαδρομή που θα πρέπει να διανύσει η πληροφορία θα πρέπει να είναι η πιο αποδοτική. Η απόφαση επιλέγεται από το δίκτυο με βάση τις πληροφορίες που είναι αποθηκευμένες στους κόμβους αντίστοιχα. Η σύνταξη των πινάκων δρομολόγησης για κάθε κόμβο είναι ένα απαραίτητο βήμα στη διαδικασία δρομολόγησης. Οι πίνακες αυτοί παράγονται με τη χρήση περίπλοκων κατανεμημένων αλγορίθμων.

Σύμφωνα με τους Alotaibi και Mukherjee (2012), ο πίνακας δρομολόγησης που κατασκευάζεται στην άμεση δρομολόγηση περιλαμβάνει τα δεδομένα για το πρωτόκολλο

δικτύου, τη θύρα εξόδου και τη διεύθυνση προορισμού. Κατά τη διαδικασία της έμμεσης δρομολόγησης, τα πακέτα δεδομένων που προέρχονται από διάφορα δίκτυα αποστέλλονται από την πηγή και στη συνέχεια δρομολογούνται μέσω των σχετικών δρομολογητών προκειμένου να φτάσουν στον τελικό προορισμό τους. Σύμφωνα με τους Medhi και Ramasamy (2017), ο πίνακας δρομολόγησης που σχηματίζεται με την έμμεση δρομολόγηση μπορεί να δημιουργηθεί με δύο διαφορετικούς τρόπους: είτε μπορεί να είναι στατικός, ο οποίος δημιουργείται από τον διαχειριστή του δικτύου, είτε μπορεί να είναι δυναμικός, ο οποίος δημιουργείται με τη χρήση των πρωτοκόλλων που έχουν καθιερωθεί από τον διαχειριστή του δικτύου.

Σύμφωνα με τους Medhi και Ramasamy (2017), οι αλγόριθμοι διαθέτουν ορισμένα χαρακτηριστικά, τα οποία είναι τα εξής:

1) Απλότητα: ο αλγόριθμος θα πρέπει να έχει ως στόχο να είναι όσο το δυνατόν πιο απλός και κατανοητός και η λειτουργία του θα πρέπει να ρυθμίζεται από κανόνες που είναι σαφείς και απλοί.

2) Ορθότητα: ο αλγόριθμος θα πρέπει να είναι σε θέση να λειτουργεί χωρίς προβλήματα, και σε περίπτωση που αντιμετωπίσει κάποια δυσκολία, θα πρέπει να είναι δυνατή η εξεύρεση λύσης για το ίδιο πρόβλημα.

3) Ευστάθεια: ο αλγόριθμος θα πρέπει να είναι σε θέση να αντιμετωπίσει τυχόν αλλαγές που λαμβάνουν χώρα στο δίκτυο και να δίνει απαντήσεις σε τυχόν προβλήματα που προκύπτουν. Για να το θέσουμε αλλιώς, πρέπει να είναι σε θέση να αντιμετωπίσει κάθε είδους μηχανική δυσλειτουργία ή δυσλειτουργία λογισμικού.

4) Δικαιοσύνη: τα πακέτα που έχουν δρομολογηθεί θα πρέπει να αντιμετωπίζονται δίκαια, ανεξάρτητα από το αν προέρχονται από ξεχωριστή σύνδεση ή όχι.

5)Βελτιστοποίηση: ο αλγόριθμος είναι σε θέση να καθορίσει την καλύτερη διαδρομή λαμβάνοντας υπόψη όλες τις διαφορετικές μεταβλητές που σχετίζονται με το δίκτυο.

Σύμφωνα με τους Ratnasamy και συν. (2002), οι αλγόριθμοι δρομολόγησης μπορούν να ταξινομηθούν στις αντίστοιχες ομάδες τους ως εξής:

1) Αλγόριθμοι συγκέντρωσης: δεν είναι αξιόπιστοι, καθώς θα σταματήσουν να λειτουργούν εάν ένας κεντρικός κόμβος υποστεί βλάβη. Το ίδιο ισχύει και στην περίπτωση

που ο κεντρικός κόμβος υποστεί βλάβη. Ο κεντρικός κόμβος είναι αυτός που είναι υπεύθυνος για τον καθορισμό της δρομολόγησης κάθε πληροφορίας. Είναι εξοπλισμένος με μια ισχυρή CPU την οποία μπορεί να χρησιμοποιήσει για τη σάρωση των πινάκων δρομολόγησης και έχει επίσης τη δυνατότητα αποθήκευσης δεδομένων.

2) Κατανεμημένοι αλγόριθμοι: Αυτοί οι αλγόριθμοι είναι αξιόπιστοι, αλλά χρειάζονται πολύ χρόνο για να δημιουργήσουν μια σταθερή κατάσταση όταν ένας κόμβος προσχωρεί ή όταν υπάρχει δυσλειτουργία. Δεν υπάρχει κεντρικός κόμβος, αλλά οι δύο κόμβοι που συνδέονται μεταξύ τους και μοιράζονται πληροφορίες σχετικά με το δίκτυο είναι αυτοί που λαμβάνουν τις αποφάσεις σχετικά με τη δρομολόγηση της κυκλοφορίας.

3) Αλγόριθμοι μονής διαδρομής ή πολλαπλών διαδρομών: Οι αλγόριθμοι μονής διαδρομής μεταφέρουν τα δεδομένα τους μέσω των ίδιων διαδρομών και θα αλλάξουν μόνο όταν ο κόμβος ή μια σύνδεση σταματήσει να λειτουργεί σωστά. Είναι επίσης γνωστοί ως αλγόριθμοι πολλαπλών διαδρομών. Επιπλέον, δεν επηρεάζονται από την κυκλοφορία στο δίκτυο. Οι αλγόριθμοι πολλαπλών διαδρομών, από την άλλη πλευρά, εκμεταλλεύονται πολλές διαδρομές για να φτάσουν στον ίδιο στόχο, γεγονός που οδηγεί σε βελτιωμένη απόδοση και αυξημένη αξιοπιστία.

4) Προσαρμοσμένοι αλγόριθμοι δρομολόγησης: Ο αλγόριθμος έχει τη δυνατότητα να προσαρμόζει τη διαδρομή με βάση το φορτίο που ασκείται σε κάθε γραμμή αντίστοιχα.

Σημασία των πρωτοκόλλων δρομολόγησης

Τα πρωτόκολλα δρομολόγησης είναι ζωτικής σημασίας για τον εντοπισμό και τη διατήρηση πληροφοριών σχετικά με απομακρυσμένα δίκτυα και τη διασφάλιση της αξιοπιστίας αυτών των πληροφοριών.

Τα δίκτυα δεδομένων εξυπηρετούν ποικίλους σκοπούς, από εκπαιδευτικούς και ψυχαγωγικούς μέχρι επαγγελματικές δραστηριότητες, και μπορεί να κυμαίνονται από μικρές, περιφερειακές ρυθμίσεις μέχρι εκτεταμένα παγκόσμια δίκτυα. Για μια μεγάλη εταιρεία, η σύνδεση εκατοντάδων έως χιλιάδων υπολογιστών απαιτεί συχνά πολλαπλούς δρομολογητές και μεταγωγείς. Τα πρωτόκολλα δρομολόγησης παίζουν καθοριστικό ρόλο σε αυτή τη ρύθμιση, επιτρέποντας στους δρομολογητές να μοιράζονται δυναμικά και να ενσωματώνουν πληροφορίες σχετικά με εξωτερικά δίκτυα στους πίνακες δρομολόγησης. Χρησιμοποιώντας τα δεδομένα σε αυτούς τους πίνακες, οι δρομολογητές μπορούν να κατευθύνουν τα πακέτα κατά μήκος των αποδοτικότερων διαδρομών προς τους προορισμούς τους. Οι δρομολογητές

μπορούν να καθορίσουν διαδρομές προς απομακρυσμένα δίκτυα τόσο μέσω στατικών όσο και μέσω δυναμικών μεθόδων, με τα πρωτόκολλα δρομολόγησης να διασφαλίζουν τις βέλτιστες διαδρομές (Chitkara&Ahmad, 2014).

Η διαχείριση στατικών διαδρομών σε πολύπλοκα δίκτυα με πολλά υποδίκτυα απαιτεί σημαντική διοικητική προσπάθεια και λειτουργικούς πόρους, ιδίως όταν πρόκειται για αλλαγές στο δίκτυο, όπως η μειωμένη μετάδοση δεδομένων ή η προσθήκη νέων περιοχών διευθύνσεων IP. Τα δυναμικά πρωτόκολλα δρομολόγησης ανακουφίζουν αυτό το βάρος με την αυτοματοποίηση της διαμόρφωσης και της συντήρησης, ενισχύοντας έτσι την επεκτασιμότητα του δικτύου (Elhadj, Chaari&Kamoun, 2012). Ένα σημαντικό πλεονέκτημα της δυναμικής δρομολόγησης είναι ότι οι δρομολογητές μπορούν να ανταλλάσσουν συνεχώς πληροφορίες σχετικά με τις αλλαγές στο δίκτυο, επιτρέποντάς τους να ανιχνεύουν και να προσαρμόζονται σε νέα δίκτυα και εναλλακτικές διαδρομές σε περίπτωση αποτυχίας σύνδεσης. Αυτό μειώνει την ανάγκη για χειροκίνητη παρέμβαση σε σύγκριση με τη στατική δρομολόγηση.

Ωστόσο, η δυναμική δρομολόγηση απαιτεί από τους δρομολογητές να χρησιμοποιούν ορισμένους από τους πόρους τους, όπως χρόνο CPU και εύρος ζώνης δικτύου, για τις λειτουργίες του πρωτοκόλλου. Παρά τα πλεονεκτήματα της δυναμικής δρομολόγησης, η στατική δρομολόγηση εξακολουθεί να έχει τη θέση της και να προσφέρει πλεονεκτήματα σε ορισμένες περιπτώσεις. Τόσο η στατική όσο και η δυναμική δρομολόγηση μπορούν να χρησιμοποιηθούν αποτελεσματικά ανάλογα με την πολυπλοκότητα και τις ανάγκες του δικτύου (Chitkara&Ahmad, 2014).

Εφαρμογή ασφάλειας σε δρομολογητές Cisco

Φυσική ασφάλεια

Μόλις ένα άτομο αποκτήσει φυσική πρόσβαση σε ένα κομμάτι εξοπλισμού δικτύωσης, δεν υπάρχει καμία μέθοδος για να αποτρέψει αυτό το άτομο από το να κάνει αλλαγές στο σύστημα. Το ζήτημα αυτό δεν αφορά μόνο τις συσκευές δικτύου, αλλά ισχύει

και για τους υπολογιστές και κάθε άλλη συσκευή που είναι είτε ηλεκτρικής είτε μηχανικής φύσης. Υπάρχουν πράγματα που μπορούν να γίνουν για να γίνει αυτό πιο δύσκολο, αλλά ένας επιτιθέμενος που έχει γνώσεις και πρόσβαση δεν θα νικηθεί ποτέ εντελώς- μπορεί μόνο να επιβραδυνθεί. Ο περιορισμός της πρόσβασης θεωρείται συνήθως μια από τις πιο αποτελεσματικές βελτιώσεις των χαρακτηριστικών ασφαλείας ενός δικτύου υπολογιστών. Οι δρομολογητές και άλλα στοιχεία της δικτυακής υποδομής είναι ιδιαίτερα σημαντικά λόγω του γεγονότος ότι χρησιμοποιούνται συχνά με σκοπό την προστασία ορισμένων τμημάτων του δικτύου και μπορούν επίσης να χρησιμοποιηθούν με σκοπό την εξαπόλυση επιθέσεων σε άλλα τμήματα του δικτύου.

Γι αυτό προτείνεται:

ο δικτυακός εξοπλισμός, ιδίως οι δρομολογητές και οι μεταγωγείς, να βρίσκονται σε χώρο με περιορισμένη πρόσβαση ανά πάσα στιγμή.

Ανά πάσα στιγμή, επτά ημέρες την εβδομάδα και εικοσιτέσσερις ώρες την ημέρα, η περιοχή αυτή θα πρέπει να βρίσκεται υπό κάποια παρακολούθηση. Η χρησιμοποίηση φρουρών, προσωπικού από το σύστημα ή η ηλεκτρονική παρακολούθηση είναι όλες βιώσιμες επιλογές για την επίτευξη αυτού του στόχου.

Οι πολιτικές και οι διαδικασίες για τη φυσική ασφάλεια δεν πρέπει, στην πραγματικότητα, να δυσχεραίνουν υπερβολικά την είσοδο σε περιορισμένες περιοχές για τους εξουσιοδοτημένους εργαζόμενους- διαφορετικά, τα άτομα αυτά μπορεί να ανακαλύψουν τρόπους για να παρακάμψουν τις προφυλάξεις φυσικής ασφάλειας.

Εάν η απομακρυσμένη διαχείριση χρησιμοποιείται για τη διαμόρφωση και τον έλεγχο των δρομολογητών, τότε είναι σημαντικό να σκεφτείτε ασφαλείς τρόπους για την προστασία των μηχανημάτων που χρησιμοποιούνται για την απομακρυσμένη διαχείριση καθώς και των δικτύων που χρησιμοποιούνται από αυτές τις συσκευές για τη σύνδεση με τον δρομολογητή. Είναι δυνατό να περιορίσετε την απομακρυσμένη διαχειριστική πρόσβαση σε τοποθεσίες που διαθέτουν ένα ικανοποιητικό επίπεδο φυσικής προστασίας, χρησιμοποιώντας λίστες πρόσβασης.

Η κρυπτογράφηση θα πρέπει να χρησιμοποιείται όπου είναι εφικτό, προκειμένου να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα της σύνδεσης που χρησιμοποιείται για την απομακρυσμένη διαχείριση. Σκεφτείτε τη διαδικασία ανάκτησης ενός κωδικού πρόσβασης για έναν δρομολογητή της Cisco ως παράδειγμα ενός από τους λόγους για τους

οποίους η φυσική ασφάλεια είναι απαραίτητη για τη συνολική ασφάλεια των δρομολογητών. Ακολουθώντας αυτή τη διαδικασία, ένα άτομο που έχει φυσική πρόσβαση σε έναν δρομολογητή Cisco μπορεί να αποκτήσει πλήρη προνομιακή πρόσβαση στον δρομολογητή χωρίς να χρειάζεται να χρησιμοποιήσει κωδικό πρόσβασης.

Υπάρχουν κάποιες διαφοροποιήσεις στις ιδιαιτερότητες της λειτουργίας ανάλογα με το μοντέλο του δρομολογητή, αλλά περιλαμβάνει πάντα τις ακόλουθες θεμελιώδεις φάσεις. Ακολουθώντας τα βήματα που περιγράφονται παρακάτω, τα οποία προέρχονται από το άρθρο «Password Recovery Process» (Waheed&Ali, 2018), ένας διαχειριστής (ή ένας επιτιθέμενος) μπορεί εύκολα να συνδέσει ένα τερματικό ή έναν υπολογιστή στη θύρα κονσόλας και στη συνέχεια να προχωρήσει στη λειτουργία.

Η διαδικασία μετατροπής της φυσικής πρόσβασης σε πλήρη προνομιακή διαχειριστική πρόσβαση επιτυγχάνεται μέσα σε λίγα λεπτά και μπορεί να πραγματοποιηθεί από οποιονδήποτε έχει προηγούμενη εμπειρία ή εκπαίδευση στη χρήση δρομολογητών Cisco.

Η χρήση καρτών μνήμης flash είναι ένας δεύτερος λόγος για τον οποίο είναι απαραίτητος ο έλεγχος της φυσικής πρόσβασης στο δρομολογητή. Οι υποδοχές PC-Card και οι υποδοχές CompactFlash είναι διαθέσιμες σε πολλά μοντέλα δρομολογητών της Cisco. Αυτές οι υποδοχές είναι ικανές να φιλοξενήσουν πρόσθετη μνήμη flash. Σύμφωνα με τον Paquet (2012), οι δρομολογητές που είναι εξοπλισμένοι με αυτούς τους τύπους υποδοχών θα δίνουν προτεραιότητα στη μνήμη που είναι εγκατεστημένη σε μια υποδοχή έναντι της μνήμης που είναι τοποθετημένη στο πλαίσιο. Είναι δυνατό για έναν αντίπαλο που έχει φυσική πρόσβαση σε έναν δρομολογητή στο δίκτυό σας να εγκαταστήσει μια κάρτα μνήμης flash ή να αντικαταστήσει μια παλαιότερη που υπάρχει ήδη εκεί. Η μνήμη flash θα μπορούσε στη συνέχεια να χρησιμοποιηθεί για την εκκίνηση του δρομολογητή, με αποτέλεσμα ο δρομολογητής να εκτελεί την προτιμώμενη από τον χρήστη έκδοση του λειτουργικού συστήματος και των ρυθμίσεων. Η ανίχνευση αυτής της μορφής επίθεσης μπορεί να είναι εξαιρετικά δύσκολη, αν πραγματοποιηθεί με προσοχή και δεξιότητα. Μια ισχυρή φυσική άμυνα είναι ο πιο αποτελεσματικός τρόπος προστασίας από αυτήν. Το φυσικό περιβάλλον λειτουργίας είναι ένα ζήτημα στο μέτωπο της επιχειρησιακής ασφάλειας που συνδέεται στενά με την πτυχή της φυσικής ασφάλειας.

Εάν ένας δρομολογητής δεν βρίσκεται σε χώρο φιλικό προς το περιβάλλον, μπορεί να λειτουργήσει με τρόπους που δεν είναι αναμενόμενοι, γεγονός που θα έχει ως αποτέλεσμα τη

μείωση του επιπέδου ασφαλείας του. Η ασφάλεια του εργατικού δυναμικού είναι επίσης ένα ζήτημα που απασχολεί εδώ. Προκειμένου να αποφευχθούν οι ηλεκτροστατικές και μαγνητικές παρεμβολές, ο χώρος στον οποίο εγκαθίστανται οι δρομολογητές θα πρέπει να είναι απαλλαγμένος και από τα δύο. Επιπλέον, τα επίπεδα θερμοκρασίας και υγρασίας στο περιβάλλον θα πρέπει να είναι αυστηρά διαχειρίσιμα. Συνιστάται να συνδέονται όλοι οι δρομολογητές με ένα UPS (Uninterruptible Power Supply), αν είναι δυνατόν. Αυτό οφείλεται στο γεγονός ότι μια σύντομη διακοπή ρεύματος μπορεί να προκαλέσει ορισμένες θέσεις του δικτυακού εξοπλισμού που δεν μπορούν να προσδιοριστούν.

Στους δρομολογητές Cisco, οι θύρες κονσόλας (con) και βοηθητικές θύρες (aux) χρησιμοποιούνται για τη δημιουργία σειριακών συνδέσεων με τον κεντρικό δρομολογητή. Η συντριπτική πλειονότητα των δρομολογητών Cisco είναι εξοπλισμένοι τόσο με θύρα κονσόλας όσο και με βοηθητική θύρα- ωστόσο, ορισμένες από τις πιο συμπαγείς εκδόσεις διαθέτουν μόνο θύρα κονσόλας. Το γεγονός ότι η θύρα κονσόλας είναι η μόνη που μπορεί να κάνει χρήση του μηχανισμού ανάκτησης κωδικού πρόσβασης είναι η θεμελιώδης διάκριση μεταξύ των δύο τρόπων επικοινωνίας. Σε μεγάλο βαθμό, η βοηθητική θύρα δεν αξιοποιείται. Προκειμένου να απλοποιηθεί η απομακρυσμένη διαχείριση μέσω dial-up, ορισμένοι διαχειριστές συνδέουν ένα μόντεμ στη βοηθητική θύρα εντός του συστήματος. Η πρακτική να επιτρέπεται η άμεση πρόσβαση μέσω κλήσης σε οποιοδήποτε βασικό στοιχείο της υποδομής του δικτύου είναι γεμάτη με πιθανούς κινδύνους και θα έπρεπε να εφαρμόζεται μόνο σε περιπτώσεις όπου η έγκαιρη πρόσβαση μέσω άλλων μέσων είναι δύσκολο να επιτευχθεί. Στις περισσότερες περιπτώσεις, η βοηθητική θύρα πρέπει να απενεργοποιείται.

Το υπόλοιπο τμήμα αυτής της ενότητας θα σας καθοδηγήσει στις εργασίες ρύθμισης που πρέπει να κάνετε προκειμένου να ασφαλίσετε τους δρομολογητές σας. Πριν συνδέσετε έναν νέο δρομολογητή σε οποιοδήποτε δίκτυο που θα μπορούσε ενδεχομένως να είναι εχθρικό, είναι απαραίτητο να εφαρμόσετε αυτές τις προφυλάξεις(Antoine, et. al., 2005).

Εργασίες ρύθμισης προκειμένου να ασφαλιστούν οι δρομολογητές

Διαμόρφωση και εντολές δρομολογητή (IOS)

Μετά τη σύνδεση σε έναν δρομολογητή και την αρχική σύνδεση, το σύστημα βρίσκεται σε κατάσταση λειτουργίας χρήστη, γνωστή και ως κατάσταση EXEC. Η λειτουργία EXEC παρέχει περιορισμένη πρόσβαση στο σύνολο εντολών του δρομολογητή. Η πρόσβαση σε

όλες τις εντολές του δρομολογητή, συμπεριλαμβανομένης της δυνατότητας αλλαγής των ρυθμίσεων, προορίζεται για την προνομιακή κατάσταση λειτουργίας EXEC.

Η πληκτρολόγηση της εντολής enable σε μια προτροπή λειτουργίας EXEC θα δώσει πρόσβαση στην προνομιακή λειτουργία EXEC.

Η κατάσταση λειτουργίας Privileged EXEC αποκαλείται μερικές φορές «κατάσταση ενεργοποίησης».

Υπάρχουν διάφοροι τρόποι διαμόρφωσης σε έναν δρομολογητή Cisco. Για να εισέλθετε στην κατάσταση παγκόσμιας διαμόρφωσης (config) πληκτρολογήστε την εντολή configureterminal , συνήθως συντομογραφία «configt». Στην κατάσταση globalconfigurationmode μπορεί να αλλάξει μια μεγάλη ποικιλία από γενικές λειτουργίες και ρυθμίσεις του δρομολογητή:

- banners, συστήματα ελέγχου ταυτότητας, λίστες πρόσβασης, καταγραφή, πρωτόκολλα δρομολόγησης και πολλά άλλα. Υπάρχουν επιμέρους λειτουργίες που χρησιμοποιούνται για τη διαμόρφωση συγκεκριμένων ρυθμίσεων για διασυνδέσεις, γραμμές, πρωτόκολλα δρομολόγησης κ.λπ. Ο παρακάτω κατάλογος περιγράφει ορισμένους από τους υπο-ρυθμούς - interface (config-if) χρησιμοποιείται για τη διαμόρφωση πτυχών μιας συγκεκριμένης διασύνδεσης, όπως FastEthernet0, Ethernet 0/1 ή Vlan2 (Antoine, et. al., 2005).

- line (config-line) χρησιμοποιείται για τη ρύθμιση της θύρας κονσόλας, της βοηθητικής θύρας και των γραμμών εικονικού τερματικού. - access-list (λίστα πρόσβασης): Υπάρχουν δύο τύποι λιστών πρόσβασης με όνομα IP, οι εκτεταμένες (config-ext-n) και οι τυπικές (config-std-n), οι οποίες μπορούν να χρησιμοποιηθούν αντί των αριθμημένων λιστών. Η λειτουργία access-list χρησιμοποιείται για τη δημιουργία ονομαστικών λιστών πρόσβασης.

- route (config-route) στο οποίο μπορούν να οριστούν και να τροποποιηθούν συγκεκριμένες παράμετροι για ένα επιλεγμένο πρωτόκολλο δρομολόγησης. Εκτός από τις τυπικές λειτουργίες ελέγχου ταυτότητας, εξουσιοδότησης και καταγραφής δρομολογητών, το CiscoIOS 11.1 και μεταγενέστερες εκδόσεις προσφέρουν ένα ολοκληρωμένο μοντέλο ελέγχου ταυτότητας, εξουσιοδότησης και λογιστικής (AAA), το λεγόμενο «νέο μοντέλο».

Κυκλοφορία δικτύου δρομολογητή και Loopback

Η κύρια λειτουργία ενός δρομολογητή είναι να διευκολύνει τη μεταφορά δεδομένων μεταξύ δικτύων- ωστόσο, οι δρομολογητές συμμετέχουν επίσης στην παραγωγή της δικτυακής κίνησης. Μια ποικιλία πρωτοκόλλων διαχείρισης, συμπεριλαμβανομένων των πρωτοκόλλων δρομολόγησης, SNMP, NTP και TFTP, χρησιμοποιούνται από δρομολογητές και άλλες συσκευές δικτύου προκειμένου να επικοινωνούν μεταξύ τους. Μια διεύθυνση πηγής απαιτείται για την εγκαθίδρυση μιας σύνδεσης δικτύου όταν αυτή ξεκινά από το δρομολογητή. Στις περισσότερες περιπτώσεις, ένας δρομολογητής επιλέγει μια διεύθυνση πηγής από τις διευθύνσεις που είναι συνδεδεμένες με μια από τις διεπαφές δικτύου του. Αυτό μπορεί να είναι ενοχλητικό με διάφορους τρόπους, ο σημαντικότερος από τους οποίους είναι ότι η διεύθυνση πηγής για ορισμένες υπηρεσίες μπορεί να αλλάξει. Οι δρομολογητές CiscoIOS έχουν τη δυνατότητα να ορίζουν εσωτερικές εικονικές διεπαφές, οι οποίες αναφέρονται ως διεπαφές loopback (Paquet, 2012). Η δυνατότητα αυτή είναι επιπλέον της δυνατότητας ορισμού φυσικών διεπαφών. Κατά την εγκατάσταση δρομολογητών Cisco, θεωρείται βέλτιστη πρακτική ο ορισμός μιας διεπαφής loopback και ο ορισμός της ως διεπαφής πηγής για την πλειονότητα της κυκλοφορίας που παράγεται από τον ίδιο τον δρομολογητή. Λόγω του γεγονότος ότι η διεύθυνση της διεπαφής loopback διατηρείται σταθερά, η εφαρμογή αυτής της τεχνικής έχει ως αποτέλεσμα μια σειρά από πλεονεκτήματα για τη συνολική σταθερότητα και τη διαχείριση της ασφάλειας ενός δικτύου. Η ασφάλεια άλλων συσκευών στο δίκτυο μπορεί να ρυθμιστεί πιο αυστηρά όταν ένας δρομολογητής έχει ρυθμιστεί να χρησιμοποιεί τη διεπαφή loopback για υπηρεσίες. Αυτό καθιστά εφικτή τη διαμόρφωση της ασφάλειας του δρομολογητή. Κάθε φορά που μια υπηρεσία ρυθμίζεται ώστε να χρησιμοποιεί τη διεπαφή loopback ως πηγή, αναφερόμαστε σε αυτή την υπηρεσία ως δεσμευμένη σε αυτή τη διεπαφή. Επιπλέον, υποδηλώνει ότι τα πακέτα IP που παράγονται από το δρομολογητή θα έχουν ως διεύθυνση πηγής τη διεύθυνση της διεπαφής loopback. Είναι επίσης σημαντικό να σημειωθεί ότι η διεύθυνση της διεπαφής loopback δεν περιλαμβάνεται σε οποιουσδήποτε χάρτες δικτύου που βασίζονται σε διαδρομές. Γενικά θεωρείται καλή πρακτική να αποκρύπτετε τα διοικητικά στοιχεία του δικτύου σας όποτε είναι δυνατόν (Antoine, et. al., 2005).

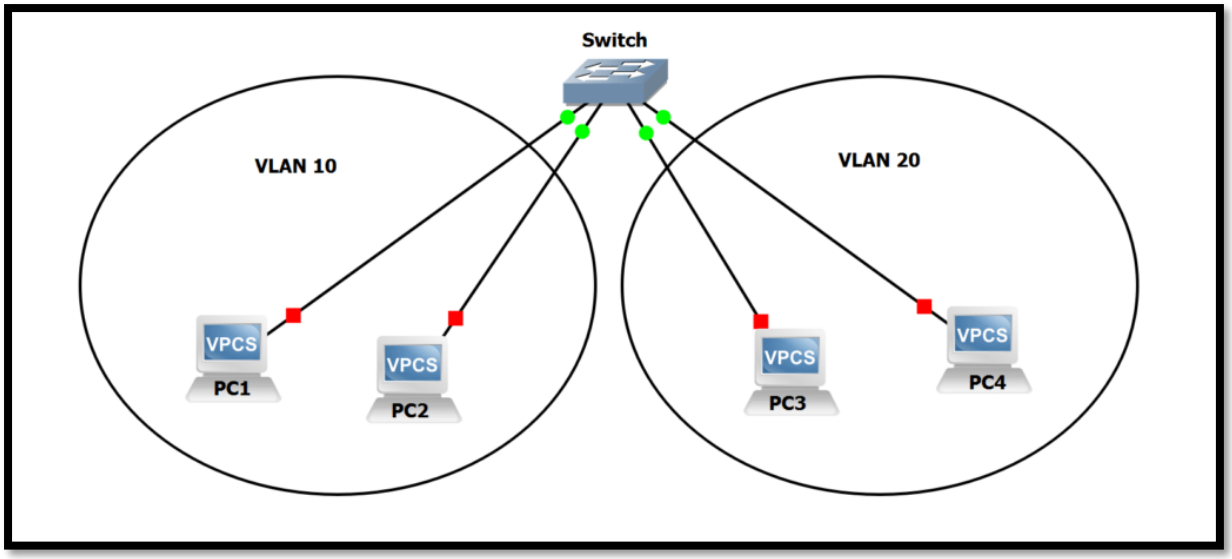
Virtual Local Area Network (VLAN)

Διαμόρφωση VLAN

Τι είναι

Ένα VLAN ή Virtual Local Area Network (Εικονικό τοπικό δίκτυο) είναι ένα λογικό δίκτυο που δημιουργείται με την ομαδοποίηση συσκευών με βάση τις συνδέσεις τους και όχι τη φυσική τους θέση.

Ένας διαχειριστής δικτύου έχει τη δυνατότητα να χωρίσει ένα τοπικό δίκτυο σε πολλαπλά ανεξάρτητα δίκτυα μέσω της χρήσης εικονικών τοπικών δικτύων (VLAN). Τα εικονικά τοπικά δίκτυα (VLANs) εφαρμόζονται συχνά τόσο σε μεγάλα όσο και σε μικρά δίκτυα. Σε μεγάλα δίκτυα, τα εικονικά τοπικά δίκτυα (VLANs) χρησιμοποιούνται περιστασιακά για να συνδυάσουν λογικά τοπικά δίκτυα (LANs) που είναι φυσικά διαχωρισμένα μεταξύ τους. Δηλαδή τα VLAN επιτρέπουν την κατάνομή ενός ενιαίου φυσικού δικτύου σε πολλαπλά λογικά δίκτυα, καθένα από τα οποία λειτουργεί ως ανεξάρτητος τομέας εκπομπής.



Εικόνα23 VLAN

https://www.zframez.com/articles/switchi 2

Πλεονεκτήματα

Απόδοση

Αυτός ο διαχωρισμός **μειώνει τις επιπτώσεις της υπερβολικής κίνησης μετάδοσης**, βελτιώνοντας τη συνολική απόδοση του δικτύου. Επιπλέον,

Ασφάλεια

τα VLAN **ενισχύουν την ασφάλεια του δικτύου** με την απομόνωση της δικτυακής κίνησης, η οποία συμβάλλει στην προστασία των ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση.

Οι διαχειριστές του δικτύου μπορούν να έχουν τον έλεγχο κάθε θύρας. Ένας κακόβουλος χρήστης δεν μπορεί πλέον απλά να συνδέσει τη συσκευή του σε οποιαδήποτε θύρα μεταγωγής και να παρακολουθεί ή να κλέβει την κυκλοφορία του δικτύου χρησιμοποιώντας ένα λογισμικό sniffer χωρίς να ανιχνεύεται. Η θύρα και οι πόροι που επιτρέπονται να χρησιμοποιεί μπορούν να ελέγχονται από τον διαχειριστή του δικτύου. Η ευαίσθητη κυκλοφορία που προέρχεται από ένα τμήμα της επιχείρησης στο εσωτερικό της μπορεί να περιοριστεί με VLANs.

Εξοικονόμηση κόστους

Επειδή απαιτείται μόνο ένας φυσικός μεταγωγέας, αυτό έχει ως αποτέλεσμα την εξοικονόμηση κόστους. Επιπλέον, έχει τη δυνατότητα να διευκολύνει τη διαδικασία υλοποίησης και σχεδιασμού ενός δικτύου, επειδή μπορεί να διαμορφωθεί χρησιμοποιώντας λογισμικό και όχι υλικό.

Εξοικονόμηση κόστους

Το κόστος δημιουργίας ενός δικτύου ή επέκτασης ενός δικτύου μπορεί να μειωθεί με την εξάλειψη της ανάγκης για πρόσθετο ακριβό εξοπλισμό δικτύου, όπως μακρύτερα καλώδια ή επιπλέον δρομολογητές.

Εικονική ομάδα εργασίας:

Ένα άλλο πλεονέκτημα του VLAN είναι η δημιουργία εικονικών ομάδων εργασίας. Για παράδειγμα, συνάδελφοι από διαφορετικά τμήματα που εργάζονται σε ένα μέρος ενός μεγάλου έργου ή ενδεχομένως στο ίδιο έργο μπορούν να στέλνουν μηνύματα ο ένας στον άλλο χωρίς να χρειάζεται να βρίσκονται στο ίδιο τμήμα. Αυτό μπορεί να βοηθήσει στη μείωση της κυκλοφορίας στο δίκτυο.

Εύκολη αντιμετώπιση προβλημάτων

Οι διαχειριστές του δικτύου είναι σε θέση να παρατηρούν ευκολότερα τις δραστηριότητες των VLANs. Ως εκ τούτου, τα προβλήματα του δικτύου μπορούν εύκολα να εντοπιστούν και να διορθωθούν.

καλύτερη χρήση του εύρους ζώνης

Τα VLANs θα παρέχουν τη δυνατότητα καλύτερης χρήσης του εύρους ζώνης και των πόρων και, επομένως, το δίκτυο μπορεί να λειτουργήσει πιο αποτελεσματικά.

Οι διαχειριστές δικτύων είναι σε θέση να ομαδοποιούν τους κεντρικούς υπολογιστές χρησιμοποιώντας εικονικά τοπικά δίκτυα (VLAN), ακόμη και αν οι κεντρικοί υπολογιστές δεν βρίσκονται στον ίδιο μεταγωγέα δικτύου.

Υλοποίηση

Τα VLAN υλοποιούνται συνήθως με τη χρήση μεταγωγέων δικτύου εξοπλισμένων με δυνατότητες επισήμανσης VLAN. Η επισήμανση VLAN περιλαμβάνει την προσθήκη μιας επικεφαλίδας στα πλαίσια Ethernet που υποδεικνύει τη συσχέτισή τους με VLAN.

Όταν ένας μεταγωγέας λαμβάνει ένα πλαίσιο, εξετάζει την ετικέτα VLAN και προωθεί το πλαίσιο μόνο σε συσκευές που ανήκουν στο ίδιο VLAN με τον αποστολέα. Αυτή η διαδικασία ετικετοποίησης ελαχιστοποιεί την περιττή κίνηση μετάδοσης και βελτιώνει την αποδοτικότητα του δικτύου.

Η δημιουργία ενός λειτουργικού δικτύου VLAN περιλαμβάνει διάφορα βασικά βήματα. Πρώτον, οι διαχειριστές του δικτύου πρέπει να καθορίσουν ποιες συσκευές θα αντιστοιχιστούν σε κάθε VLAN. Αυτό μπορεί να διαχειριστεί με την ανάθεση των VLAN σε συγκεκριμένες θύρες μεταγωγής (Somasundaram&Chandran, 2018).

Για να εκχωρήσουν μια θύρα σε ένα VLAN, οι διαχειριστές ρυθμίζουν τις παραμέτρους της θύρας του μεταγωγέα ώστε να ανήκει στο καθορισμένο VLAN, χρησιμοποιώντας είτε μια διεπαφή γραμμής εντολών είτε το γραφικό περιβάλλον χρήστη του μεταγωγέα. Η θύρα του μεταγωγέα θα πρέπει να οριστεί ως θύρα πρόσβασης για το καθορισμένο VLAN για να διασφαλιστεί η βέλτιστη απόδοση. Επιπλέον, το VLAN πρέπει να δημιουργηθεί στο μεταγωγέα, εάν δεν υπάρχει ήδη πριν από την εκχώρηση θύρας (Somasundaram&Chandran, 2018).

Μετά τη δημιουργία VLAN και την εκχώρηση θύρας, πρέπει να ρυθμιστεί η ετικέτα VLAN. Αυτή η επισήμανση περιλαμβάνει την προσθήκη μιας επικεφαλίδας στα πακέτα Ethernet, η οποία βοηθά στο διαχωρισμό της κυκλοφορίας από διαφορετικά VLAN και επιτρέπει την επικοινωνία μεταξύ των VLAN. Δύο βασικές μέθοδοι επισήμανσης VLAN είναι το IEEE

802.1Q και το πρωτόκολλο ISL (Inter-SwitchLink). Το IEEE 802.1Q, το πιο ευρέως χρησιμοποιούμενο πρότυπο, προσθέτει μια ετικέτα 4 byte στο πλαίσιο Ethernet για πληροφορίες VLAN και είναι συμβατό με τους περισσότερους μεταγωγείς δικτύου. Το ISL, ένα παλαιότερο πρωτόκολλο, είναι ειδικό για τους μεταγωγείς της Cisco (Somasundaram&Chandran, 2018).

Για να ενεργοποιηθεί η επισήμανση VLAN με IEEE 802.1Q, η θύρα του μεταγωγέα θα πρέπει να οριστεί ως θύρα κορμού. Οι θύρες κορμού μεταδίδουν δεδομένα για πολλαπλά VLAN, με την ετικέτα VLAN να χρησιμοποιείται για τη διαφοροποίηση μεταξύ της κυκλοφορίας από διαφορετικά VLAN. Έτσι, η διαμόρφωση VLAN περιλαμβάνει την ανάθεση θυρών σε VLAN, τη δημιουργία VLAN και τη διαμόρφωση της ετικέτας VLAN. Η σωστή εφαρμογή VLAN βοηθά τους διαχειριστές δικτύων να δημιουργήσουν ασφαλή, αποδοτικά και προσαρμόσιμα δίκτυα προσαρμοσμένα στις ανάγκες του οργανισμού (PankajGhimire, 2023).

Δρομολόγηση

Η δρομολόγηση μεταξύ των VLAN είναι απαραίτητη για τη διασφάλιση της απρόσκοπτης επικοινωνίας μεταξύ των VLAN εντός ενός δικτύου (Pankaj Ghimire, 2023).

Η δρομολόγηση μεταξύ των VLAN (δρομολόγηση μεταξύ VLAN) βασίζεται στην προώθηση της δικτυακής κυκλοφορίας από ένα VLAN σε ένα άλλο VLAN με τη χρήση ενός δρομολογητή. Επιτρέπει στις συσκευές που είναι συνδεδεμένες στα διαφορετικά VLAN να επικοινωνούν μεταξύ τους με τη χρήση ενός δρομολογητή. Οι κόμβοι σε ένα VLAN παραμένουν στο δικό τους πεδίο εκπομπής και θα μπορούν να επικοινωνούν ελεύθερα. Τα VLAN μπορούν να κάνουν διαμερισμό του δικτύου και διαχωρισμό της κίνησης στο επίπεδο δύο, στο επίπεδο σύνδεσης δεδομένων. Επομένως, εάν οι κεντρικοί υπολογιστές ή οποιαδήποτε άλλη συσκευή με διεύθυνση IP θέλει να επικοινωνήσει μεταξύ των VLANs, απαιτείται μια συσκευή επιπέδου 3 για την παροχή υπηρεσιών δρομολόγησης. Η χρήση εικονικής τεχνολογίας και πρωτοκόλλων για την κατάτμηση ενός δικτύου μπορεί να είναι χρήσιμη για τον έλεγχο της κυκλοφορίας μετάδοσης και την εφαρμογή ορίων ασφαλείας. Ωστόσο, το να μην επιτρέπεται απολύτως ΚΑΜΙΑ πρόσβαση μεταξύ των VLAN δεν είναι ποτέ πολύ επωφελές. Για την επίλυση αυτού του προβλήματος, προτείνεται η εφαρμογή δρομολόγησης μεταξύ των VLAN. Σε επίπεδο CCNA, υπάρχουν δύο τρόποι με τους οποίους μπορούμε να το πραγματοποιήσουμε αυτό και συγκεκριμένα (Mehdizadeh, et. al. 2017):

α) Σύνδεση μιας μοναδικής θύρας δρομολογητή σε κάθε VLAN

β) Δημιουργία ενός δρομολογητή σε ένα στικ.

Χρήση

Σύμφωνα με τους Garimellaetal. (2007), τα εικονικά τοπικά δίκτυα (VLANs) χρησιμοποιούνται ευρέως στα δίκτυα επιχειρήσεων. Χρησιμοποιούνται συχνά για να απευθύνονται σε ομάδες χρηστών ως ενιαία μονάδα, προκειμένου να απλοποιείται η διαχείριση, παρά το γεγονός ότι οι χρήστες αυτοί βρίσκονται σε διαφορετικές φυσικά τοποθεσίες.

Δυσκολίες

Παρά την ευρεία χρήση τους, η διαμόρφωση των εικονικών τοπικών δικτύων (VLAN) εξακολουθεί να είναι μια επίπονη και περίπλοκη διαδικασία. Ορισμένοι παράγοντες συμβάλλουν στην πολυπλοκότητα της διαμόρφωσης εικονικών τοπικών δικτύων (VLAN). Στους παράγοντες αυτούς περιλαμβάνονται η κλίμακα και η πολυπλοκότητα των σημερινών εταιρικών δικτύων, τα οποία μπορεί να προσεγγίζουν ακόμη και τα δίκτυα μεταφορέων. Στην περίπτωση μιας απλής ρύθμισης, όπως η προσθήκη ενός νέου κεντρικού υπολογιστή σε ένα εικονικό τοπικό δίκτυο (VLAN), μπορεί να χρειαστεί να προσαρμοστεί η διαμόρφωση πολλών μεταγωγέων μέσα στο δίκτυο, η οποία αναφέρεται ως η διαδικασία ρύθμισης των συνδέσεων «κορμού» (Sungetal., 2008).

Από την άλλη πλευρά, υπάρχει έλλειψη εργαλείων που μπορούν να αυτοματοποιήσουν, να οπτικοποιήσουν ή να επικυρώσουν τη διαμόρφωση των εικονικών τοπικών δικτύων (VLAN). Στην πραγματικότητα, σχεδόν όλα τα καθήκοντα που σχετίζονται με τη διαμόρφωση των VLAN εκτελούνται προς το παρόν με εντελώς χειροκίνητο και adhoc τρόπο (Whalen, 2001).

Λόγω της ad-hoc φύσης αυτής της προσέγγισης του σχεδιασμού VLAN, υπάρχει μεγάλος αριθμός πιθανών αιτιών προβλημάτων που μπορεί να προκύψουν. Λάθη αυτής της φύσης μπορούν εύκολα να οδηγήσουν σε σημαντικά προβλήματα συνδεσιμότητας, τρωτά σημεία ασφαλείας και αναποτελεσματικότητα στο δίκτυο. Ενδεικτικά, οι πλεονάζοντες σύνδεσμοι κορμού που έχουν κατασκευαστεί με πλεονασμό έχουν τη δυνατότητα να επεκτείνουν λανθασμένα την κυκλοφορία ενός εικονικού τοπικού δικτύου (VLAN) σε ένα τμήμα του δικτύου που δεν προορίζεται να διασχίσει. Είναι πιθανό αυτό να καταστήσει το δίκτυο πιο ευάλωτο σε επιθέσεις μέσω ARP poisoning και ARP stormanipulation.

Επιπλέον, οι φορείς εκμετάλλευσης δυσκολεύονται πολύ να παρακολουθούν τα δίκτυά τους και να αντιμετωπίζουν προβλήματα, επειδή δεν υπάρχουν αρκετά εργαλεία για την οπτικοποίηση και την επικύρωση. Ως αποτέλεσμα, υπάρχει άμεση απαίτηση για την ανάπτυξη τεχνολογιών που μπορούν να παρέχουν βοήθεια στους διαχειριστές δικτύων στη διαμόρφωση εικονικών τοπικών δικτύων (Kumar, 2005).

κατηγορίες VLAN

Υπάρχουν δύο **κατηγορίες** VLAN (Pal, 2013):

- Στατικά VLANs

Τα στατικά VLANs διαμορφώνονται από τον διαχειριστή του δικτύου, κυρίως για λόγους ασφαλείας . Δεδομένου ότι ένα ανατίθεται χειροκίνητα σε ένα VLAN θα είναι πάντα finxed και διατηρείται. Αυτός ο τύπος mebership είναι βέβαια εύκολος στην εγκατάσταση και τη διαμόρφωση, αλλά απαιτείται η χειροκίνητη ενημέρωση εάν υπάρχουν αλλαγές στον κεντρικό υπολογιστή. Τα στατικά VLANs δεν είναι εφικτό να εφαρμοστούν για ένα μεγάλο δίκτυο που απαιτεί συχνές ενημερώσεις. Σε αυτή την περίπτωση προτείνεται μια δυναμική λύση.

- Δυναμικά VLANs

Τα VLAN μπορούν να εκχωρηθούν αυτόματα με τη χρήση λογισμικού, με βάση τη διεύθυνση υλικού (MAC), τα πρωτόκολλα και τις εφαρμογές. Για παράδειγμα, υποθέστε ότι μια διεύθυνση MAC έχει καταχωρηθεί σε κεντρικό λογισμικό VLAN. Εάν είναι συνδεδεμένη σε μια μη εκχωρημένη θύρα μεταγωγής, η βάση δεδομένων διαχείρισης του VLAN μπορεί να αναζητήσει τη διεύθυνση υλικού και να εκχωρήσει και να διαμορφώσει τη θύρα μεταγωγής στο σωστό VLAN. Η δυσκολία αυτής της μεθόδου έγκειται στη ρύθμιση της βάσης δεδομένων σε αρχικό επίπεδο (Pal, 2013).

Τύποι VLAN

Στα σύγχρονα δίκτυα, υπάρχουν διάφοροι τύποι VLAN. Ορισμένα από αυτά μπορούν να εξηγηθούν και να ταξινομηθούν με βάση τις κατηγορίες κυκλοφορίας τους. Άλλοι τύποι

VLAN θα μπορούσαν να οριστούν με βάση τη συγκεκριμένη λειτουργία που εξυπηρετούν (Pal, 2013):

VLAN δεδομένων

Ένα VLAN δεδομένων θα μπορούσε να χρησιμεύσει και να διαμορφωθεί για να αντέξει την κυκλοφορία που παράγεται από έναν χρήστη. Δεν θα περιελάμβανε ένα VLAN που μεταφέρει κίνηση φωνής ή διαχείρισης. Αποτελεί κοινή πρακτική η διάκριση της κίνησης φωνής και της κίνησης διαχείρισης από την κίνηση δεδομένων. Μερικές φορές αναφέρεται ως VLAN χρήστη. Αυτά τα VLAN αναπτύσσονται για να διαχωρίζουν το δίκτυο σε ομάδες χρηστών ή ομάδες συσκευών.

Προεπιλεγμένο VLAN

Όταν φορτώνεται η προεπιλεγμένη διαμόρφωση κατά την αρχική εκκίνηση, όλες οι θύρες ενός μεταγωγέα γίνονται μέρος του προεπιλεγμένου VLAN. Αυτές οι θύρες του μεταγωγέα που είναι τώρα μέρος του προεπιλεγμένου VLAN, στην πραγματικότητα είναι μέρος του ίδιου τομέα εκπομπής. Αυτό σημαίνει ότι κάθε συσκευή που είναι συνδεδεμένη σε οποιαδήποτε θύρα του μεταγωγέα επιτρέπεται να επικοινωνεί με άλλες συσκευές σε άλλες θύρες του μεταγωγέα. Το VLAN 1 θεωρείται ως προεπιλεγμένο VLAN για τους μεταγωγείς της Cisco.

Native VLAN

Ένα εγγενές VLAN ορίζεται σε μια θύρα κορμού 802.1Q η οποία θεωρείται ως οι συνδέσεις μεταξύ μεταγωγέων για την παροχή της μετάδοσης κίνησης που σχετίζεται με περισσότερα από ένα VLAN. Υποστηρίζει την κυκλοφορία που προέρχεται από πολλά VLAN, καθώς και την κυκλοφορία που δεν προέρχεται από κάποιο VLAN, η οποία θεωρείται ως κυκλοφορία με ετικέτα και χωρίς ετικέτα, αντίστοιχα. Η θύρα κορμού (802.1Q) τοποθετεί την κίνηση χωρίς ετικέτες στο προεπιλεγμένο VLAN 1, το οποίο είναι γνωστό ως εγγενές VLAN. Τα εγγενή VLAN καθορίζονται για να διατηρηθεί η συμβατότητα προς τα πίσω με την κυκλοφορία χωρίς ετικέτα που είναι κοινή σε παλαιά σενάρια LAN. Αποτελεί βέλτιστη πρακτική να ρυθμίζετε το native VLAN ως ένα αχρησιμοποίητο VLAN, διαφορετικό από το VLAN 1 και τα άλλα VLAN. Μπορεί να χαρακτηριστεί ως σταθερό VLAN για να εξυπηρετεί το ρόλο του εγγενούς VLAN για όλες τις θύρες κορμού στον τομέα μεταγωγής.

VLAN διαχείρισης

Κάθε VLAN που έχει ρυθμιστεί για πρόσβαση στις δυνατότητες διαχείρισης ενός μεταγωγέα θεωρείται ως VLAN διαχείρισης, το οποίο από προεπιλογή είναι το VLAN 1.

Με την εκχώρηση μιας διεύθυνσης IP και μιας μάσκας υποδικτύου στην εικονική διεπαφή μεταγωγής (SVI), το VLAN διαχείρισης μπορεί να δημιουργηθεί και να διαχειριστεί μέσω HTTP, Telnet, SSH ή SNMP.

Δεν είναι καλή πρακτική να επιλέγετε το VLAN 1 ως VLAN διαχείρισης (το οποίο είναι από προεπιλογή) επειδή η out-of-the-box διαμόρφωση ενός μεταγωγέα Cisco. Στο παρελθόν, το VLAN διαχείρισης για ένα switch της σειράς 2960 ήταν το μόνο ενεργό SVI. Στις εκδόσεις 15.x του CiscoIOS για τα μεταγωγείς Catalyst 2960, θα είναι δυνατή η ύπαρξη περισσότερων του ενός ενεργών SVI. Ωστόσο, η ύπαρξη περισσότερων του ενός VLAN διαχείρισης που θεωρητικά μπορεί να έχει ένα switch, θα δώσει την ευκαιρία σε επιτιθέμενους στο δίκτυο. Υπάρχει κίνδυνος εάν το εγγενές VLAN είναι το ίδιο με το VLAN διαχείρισης. Επομένως, το εγγενές VLAN θα πρέπει να είναι διακριτό από οποιοδήποτε άλλο VLAN, εάν χρησιμοποιείται.

VLAN φωνής

Για την υποστήριξη του VoiceoverIP (VoIP), απαιτείται ένα διαφορετικό VLAN το οποίο μπορεί να ονομαστεί voiceVLAN. Η κυκλοφορία VoIP χρειάζεται τα ακόλουθα (Pal, 2013):

- Εξασφαλισμένο εύρος ζώνης για την παροχή αποδεκτής ποιότητας φωνής

- Προτεραιότητα μετάδοσης έναντι άλλων τύπων δικτυακής κίνησης

- Δυνατότητα δρομολόγησης γύρω από περιοχές με συμφόρηση στο δίκτυο

- Μικρότερη καθυστέρηση (μικρότερη από 150ms) σε όλο το δίκτυο

Αυτές οι απαιτήσεις πρέπει να επιτευχθούν για την υποστήριξη του VoIP.

Προσδιορισμός VLANs

Μόνο ένα εικονικό τοπικό δίκτυο (VLAN) ή όλα τα VLAN θα μπορούσαν να αντιστοιχιστούν με μια θύρα σε έναν μεταγωγέα. Θα μπορούσε κανείς να ρυθμίσει χειροκίνητα μια θύρα ώστε να λειτουργεί είτε ως θύρα πρόσβασης είτε ως θύρα κορμού. Για

τους σκοπούς της ρύθμισης της λειτουργίας της θύρας του μεταγωγέα, θα πρέπει να επιτρέπεται η λειτουργία του πρωτοκόλλου δυναμικής διακλάδωσης (DTP) ανά θύρα. Για να επιτευχθεί αυτό, είναι δυνατή η διαπραγμάτευση με τη θύρα που βρίσκεται στο αντίθετο άκρο της σύνδεσης (Mehdizadehetal. 2017).

Εντός του δικτύου μεταγωγής, υπάρχουν δύο διακριτά είδη συνδέσεων, τα οποία είναι τα εξής:

i) Θύρες εισόδου: Η κυκλοφορία ενός ενιαίου εικονικού τοπικού δικτύου (VLAN) μεταφέρεται συνήθως από μία μόνο θύρα πρόσβασης. Σε αυτό το σενάριο χρησιμοποιούνται εγγενείς μορφές τόσο για την αποστολή όσο και για τη λήψη της κίνησης και δεν εμπλέκεται καμία επισήμανση VLAN. Οτιδήποτε φτάνει σε μια θύρα πρόσβασης θεωρείται αυτόματα μέλος του εικονικού τοπικού δικτύου (VLAN) που έχει εκχωρηθεί στη θύρα. Κάθε συσκευή που είναι συνδεδεμένη σε μια σύνδεση πρόσβασης δεν γνωρίζει τη συμμετοχή της σε ένα εικονικό τοπικό δίκτυο (VLAN). Αντίθετα, η συσκευή απλώς θεωρεί ότι αποτελεί μέρος του ίδιου τομέα εκπομπής και δεν αναγνωρίζει την αρχιτεκτονική του φυσικού δικτύου. Μόνο αν η δρομολόγηση έχει ρυθμιστεί, οι συσκευές σύνδεσης πρόσβασης θα μπορούν να στέλνουν και να λαμβάνουν δεδομένα από και προς συσκευές που δεν αποτελούν μέρος του εικονικού τοπικού δικτύου (VLAN) τους. Μπορεί μόνο να καταστήσει μια θύρα μεταγωγής είτε θύρα πρόσβασης είτε θύρα κορμού- δεν μπορεί να την καταστήσει και τα δύο αυτά πράγματα ταυτόχρονα. Θα πρέπει να τεθεί υπόψη σας ότι η θύρα πρόσβασης μπορεί να συνδεθεί μόνο σε ένα και μόνο εικονικό τοπικό δίκτυο (Mehdizadehetal. 2017).

ii) Θύρες κορμού: Οι θύρες κορμού, από την άλλη πλευρά, αξιοποιούνται με σκοπό την ταυτόχρονη μεταφορά πολυάριθμων VLAN. Μια ζεύξη κορμού είναι μια ζεύξη σημείου προς σημείο που μετράει 100 ή 1000 Mbps και χρησιμοποιείται για την ταυτόχρονη μεταφορά της κίνησης πολλών εικονικών τοπικών δικτύων (VLAN). Μπορεί να χρησιμοποιηθεί μεταξύ δύο μεταγωγέων, μεταξύ ενός μεταγωγέα και ενός δρομολογητή ή ακόμη και μεταξύ ενός μεταγωγέα και ενός διακομιστή. Πρόκειται για μια εξαιρετική λειτουργικότητα, επειδή οι θύρες μπορούν να ρυθμιστούν ώστε ένας διακομιστής να βρίσκεται ταυτόχρονα σε δύο διαφορετικούς τομείς εκπομπής. Ως αποτέλεσμα, οι χρήστες δεν θα πρέπει να διασχίσουν μια συσκευή επιπέδου δικτύου (επίπεδο 3) προκειμένου να συνδεθούν και να αποκτήσουν πρόσβαση στο διακομιστή. Η δυνατότητα των συνδέσεων κορμού να μεταφέρουν διαφορετικές ποσότητες δεδομένων VLAN μέσω της σύνδεσης είναι ένα άλλο πλεονέκτημα της χρήσης συνδέσεων κορμού (Mehdizadeh, et. al. 2017).

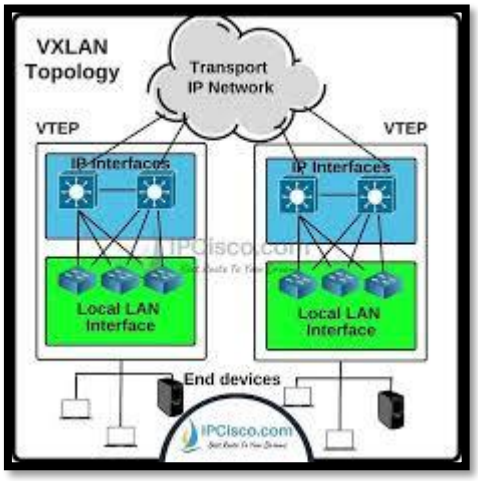
Μέθοδος αναγνώρισης VLAN

Η αναγνώριση VLAN είναι το σημείο όπου οι μεταγωγείς μπορούν να παρακολουθούν όλα τα πλαίσια καθώς ταξιδεύουν μέσω ενός δικτύου μεταγωγής. Καθορίζει τον τρόπο με τον οποίο οι μεταγωγείς μπορούν να αναγνωρίζουν ποια πλαίσια ανήκουν σε ποια VLAN, όταν υπάρχουν περισσότερες από μία μέθοδο διακλάδωσης (Pal, 2013):

i) Σύνδεσμος μεταξύ των μεταγωγέων (ISL): Το Inter-SwitchLink (ISL) είναι μια μέθοδος που επισημαίνει τα δεδομένα VLAN σε ένα πλαίσιο Ethernet. Αυτή η επισήμανση δεδομένων επιτρέπει την πολυπλεξία των VLANs σε ένα trunk μέσω μιας εξωτερικής μεθόδου ενθυλάκωσης (ISL). Στην πραγματικότητα, επιτρέπει στο μεταγωγέα να αναγνωρίζει τη συμμετοχή VLAN ενός πλαισίου μέσω της ζεύξης κορμού. Με την εφαρμογή της ISL, μπορεί να γίνει διασύνδεση πολλαπλών μεταγωγέων και να διατηρηθούν οι πληροφορίες VLAN καθώς η κυκλοφορία ταξιδεύει ; μεταξύ των μεταγωγέων σε συνδέσεις κορμού. Το ISL λειτουργεί στο επίπεδο δύο ενθυλακώνοντας ένα πλαίσιο δεδομένων με μια νέα επικεφαλίδα και έλεγχο κυκλικού πλεονασμού (CRC). Χρησιμοποιείται μόνο για συνδέσεις Fast Ethernet και Gigabit Ethernet. Η δρομολόγηση ISL είναι ευέλικτη και μπορεί να χρησιμοποιηθεί σε μια θύρα μεταγωγής, σε μια διεπαφή δρομολογητή και σε κάρτες διεπαφής διακομιστή για τη διακλάδωση ενός διακομιστή.

ii) IEEE 802.1Q: είναι μια τυποποιημένη μέθοδος που δημιουργήθηκε από την IEEE για την επισήμανση πλαισίων, το IEEE 802.1Q εισάγει ένα πεδίο στο πλαίσιο για την αναγνώριση του VLAN. Εάν είναι απαραίτητο να γίνει trunking μεταξύ ενός συνδέσμου μεταγωγής της Cisco και ενός μεταγωγέα διαφορετικής μάρκας, πρέπει να χρησιμοποιηθεί το 802.1Q για να λειτουργήσει το trunk. Ο βασικός σκοπός των μεθόδων ISL και 802.1Qframe-tagging είναι η παροχή επικοινωνίας VLAN μεταξύ των μεταγωγέων. Επίσης, θα πρέπει να σημειωθεί ότι οποιαδήποτε επισημείωση πλαισίου ISL ή 802.1Q αφαιρείται εάν ένα πλαίσιο προωθηθεί από μια ζεύξη πρόσβασης- η επισημείωση χρησιμοποιείται μόνο σε ζεύξεις κορμού.

Εικονικό διευρυμένο τοπικό δίκτυο (VXLAN)



Εικόνα24 VXLAN

Εντός των ορίων του επιπέδου 2 ή των τομέων εκπομπής, τα εικονικά τοπικά δίκτυα (VLAN) προσφέρουν λογική κατάτμηση. Παρ' όλα αυτά, η χρήση των εικονικών τοπικών δικτύων (VLANs) έχει γίνει περιοριστικός παράγοντας για τα τμήματα τεχνολογίας πληροφοριών και τους παρόχους cloud καθώς κατασκευάζουν μεγάλα κέντρα δεδομένων πολλαπλών μισθωτών. Αυτό οφείλεται στο γεγονός ότι η αξιοποίηση των διαθέσιμων συνδέσεων δικτύου είναι αναποτελεσματική όταν χρησιμοποιούνται VLANs, υπάρχουν αυστηρές απαιτήσεις σχετικά με την τοποθέτηση των συσκευών εντός του δικτύου του κέντρου δεδομένων και η επεκτασιμότητα περιορίζεται σε 4094 VLANs κατ' ανώτατο όριο. Το πρότυπο VXLAN, το οποίο εισήχθη στην Ομάδα Εργασίας Τεχνολογίας Διαδικτύου (IETF) από τη Cisco, σε συνεργασία με άλλους διακεκριμένους προμηθευτές, ως λύση στα προβλήματα που παρουσιάζει η παραδοσιακή τεχνολογία VLAN στα δίκτυα κέντρων δεδομένων. Το πρότυπο VXLAN επιτρέπει την τοποθέτηση των φόρτων εργασίας με ελαστικό τρόπο και παρέχει βελτιωμένη επεκτασιμότητα της τμηματοποίησης επιπέδου 2, τα οποία είναι απαραίτητα για την ικανοποίηση των αυξανόμενων απαιτήσεων των εφαρμογών σήμερα (Mehdizadeh, et. al. 2017).

Πλεονεκτήματα VXLAN

Το VXLAN προτείνεται για να παρέχει τις ίδιες υπηρεσίες δικτύου Ethernet επιπέδου δύο που παρέχει σήμερα το VLAN, αλλά με μεγαλύτερη ευελιξία και επεκτασιμότητα. Το

VXLAN προσφέρει τα ακόλουθα πλεονεκτήματα σε σύγκριση με το VLAN (Kapadia, et. al., 2017):

1. Η ευέλικτη τοποθέτηση τμημάτων σε όλο το κέντρο δεδομένων δίνει έναν τρόπο επέκτασης των τμημάτων επιπέδου δύο πάνω στην υποκείμενη υποδομή κοινόχρηστου δικτύου. Ως εκ τούτου, ο φόρτος εργασίας των μισθωτών μπορεί να τοποθετηθεί μεταξύ φυσικών τμημάτων στο κέντρο δεδομένων.

2. Υψηλότερη επεκτασιμότητα για την αντιμετώπιση περισσότερων τμημάτων επιπέδου δύο σε σύγκριση με τα VLANs, η οποία έχει ως αποτέλεσμα τον περιορισμό της επεκτασιμότητας μόνο σε 4094 VLANs. Το VXLAN χρησιμοποιεί ένα αναγνωριστικό τμήματος 24 bit, γνωστό ως αναγνωριστικό δικτύου VXLAN (VNID). Αυτό επιτρέπει τη συνύπαρξη έως και 16 εκατομμυρίων τμημάτων VXLAN στον ίδιο τομέα διαχείρισης.

3. Καλύτερη αξιοποίηση των διαδρομών δικτύου που είναι διαθέσιμες στην υποκείμενη υποδομή, όπου το VLAN χρησιμοποιεί το πρωτόκολλο Spanning Tree για την πρόληψη βρόχων. Θα πρέπει να σημειωθεί ότι χρησιμοποιεί τις μισές από τις συνδέσεις δικτύου σε ένα δίκτυο αποκλείοντας τις περιττές διαδρομές. Τα πακέτα VXLAN μεταφέρονται μέσω του υποκείμενου δικτύου με βάση την επικεφαλίδα επιπέδου 3 και μπορούν να εκμεταλλευτούν πλήρως τη δρομολόγηση επιπέδου 3, τη δρομολόγηση πολλαπλών διαδρομών ίσου κόστους (ECMP) και τα πρωτόκολλα συγκέντρωσης συνδέσεων για να μπορούν να χρησιμοποιούν όλα τα διαθέσιμα μονοπάτια.

Ασφάλεια

Καλύψαμε μια ευρεία ποικιλία θεμάτων που σχετίζονται με την ασφάλεια του δικτύου και προσφέραμε επίσης μια περιεκτική εξήγηση του προβλήματος που σχετίζεται με την ασφάλεια του δικτύου. Ένα καλό δίκτυο θα πρέπει να μπορεί να λειτουργεί χωρίς προβλήματα με άλλα δίκτυα, να είναι διαφανές για τους χρήστες, να προσφέρει απομακρυσμένη πρόσβαση και να διατηρεί την απόδοσή του στο υψηλότερο επίπεδο. Τα ασφαλή δίκτυα, από την άλλη πλευρά, προστατεύουν τις ευαίσθητες πληροφορίες, παρέχουν αξιοπιστία και εγγυώνται την ακεραιότητα των δεδομένων. Οι Mehdizadeh και συν. (2017) διαπίστωσαν ότι οι δύο διαστάσεις έρχονται συχνά σε αντίθεση μεταξύ τους.

Καθώς η τεχνολογική πρόοδος συνεχίζει να επιταχύνεται, αυξάνεται αντίστοιχα και η προϋπόθεση για την ασφάλεια των δικτύων. Αυτό οφείλεται στο γεγονός ότι παράλληλα με την πρόοδο της τεχνολογίας αυξάνεται και η διαθεσιμότητα μιας μεγάλης ποικιλίας εργαλείων παραβίασης. Αυτές οι τεχνικές hacking χρησιμοποιούνται σε μια ποικιλία δικτύων, όπως το δίκτυο ευρείας περιοχής (WAN) και το τοπικό δίκτυο (LAN), μεταξύ άλλων. Ωστόσο, παρά το γεγονός ότι τα εικονικά τοπικά δίκτυα (VLAN) είναι απαραίτητα για τη διατήρηση της ευέλικτης δικτύωσης, παρουσιάζουν επίσης ανησυχίες για την ασφάλεια των επιχειρήσεων, επειδή αποθηκεύουν ζωτικές πληροφορίες που διακινούνται χρησιμοποιώντας τα VLAN. Οι ανησυχίες για την ασφάλεια του δικτύου στο εικονικό τοπικό δίκτυο (VLAN) είναι εξαιρετικά σημαντικές και θα έπρεπε να λαμβάνονται υπόψη, να συζητούνται και να εξετάζονται (Heron, 2014).

Περιπτώσεις επιθέσεων που πλαστογραφούν το πρωτόκολλο επίλυσης διευθύνσεων (ARP)

Η μέθοδος με την οποία ένας αντίπαλος μεταδίδει (πλαστογραφημένα) πακέτα του πρωτοκόλλου επίλυσης διευθύνσεων (ARP) σε ένα τοπικό δίκτυο αναφέρεται ως πλαστογράφηση ARP, δηλητηρίαση της προσωρινής μνήμης ARP ή δρομολόγηση με δηλητήριο ARP.

Ο πρωταρχικός στόχος του επιτιθέμενου είναι να συνδέσει τη διεύθυνση MAC του κόμβου-στόχου με τη διεύθυνση IP ενός άλλου κόμβου, όπως η προεπιλεγμένη πύλη. Σύμφωνα με τους Bruschi και συν. (2003), ένας επιτιθέμενος έχει τη δυνατότητα να εξαναγκάσει οποιαδήποτε επικοινωνία που προορίζεται για μια συγκεκριμένη διεύθυνση IP να παραδοθεί αντί αυτής στον επιτιθέμενο.

Ο επιτιθέμενος θα στέλνει πλαστά πακέτα στον διακομιστή, καθένα από τα οποία θα έχει μια διεύθυνση IP που θα μοιάζει πολύ με την αρχική διεύθυνση IP.

Στη συνέχεια, ο επιτιθέμενος θα ισχυριστεί ότι είναι ο πραγματικός κεντρικός υπολογιστής.

Ο διακομιστής αρχίζει να μεταδίδει τα δεδομένα στον επιτιθέμενο αντί του αρχικού κεντρικού υπολογιστή όταν λάβει το πακέτο και διαπιστώσει ότι η διεύθυνση MAC του επιτιθέμενου είναι ο προοριζόμενος προορισμός των πακέτων.

Αυτό συμβαίνει επειδή ο επιτιθέμενος χρησιμοποιεί μια διεύθυνση IP που είναι παρόμοια με αυτή που χρησιμοποιεί ο αρχικός κεντρικός υπολογιστής. Είναι δυνατόν ο

επιτιθέμενος να αποκτήσει δεδομένα που προορίζονταν για τον νόμιμο παραλήπτη. Είναι δυνατό για έναν επιτιθέμενο να υποκλέψει πλαίσια δεδομένων σε ένα δίκτυο, να αλλάξει την κυκλοφορία ή να σταματήσει όλη την κυκλοφορία μέσω της χρήσης του ARPspoofing, σύμφωνα με τους Zargar και συν. (2013).

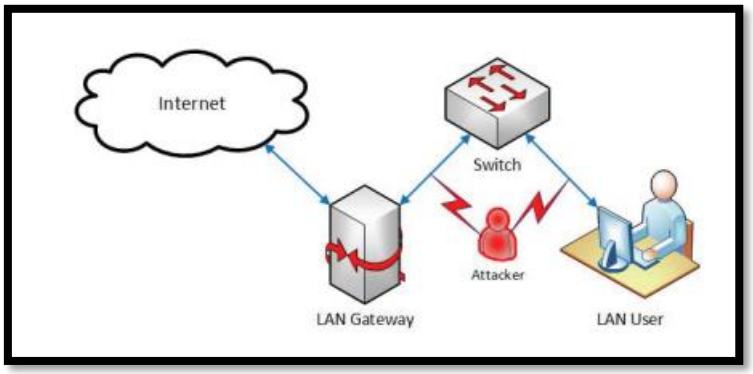
Μεταπήδηση σε τοπικό δίκτυο

Το VLAN hopping είναι ένας τύπος εκμετάλλευσης ασφάλειας υπολογιστών που επιτρέπει σε έναν εισβολέα να επιτεθεί σε δικτυακούς πόρους που βρίσκονται σε ένα εικονικό τοπικό δίκτυο (VLAN).

Σε όλα αυτά τα διαφορετικά είδη επιθέσεων, η θεμελιώδης ιδέα είναι ότι ένας κεντρικός υπολογιστής επίθεσης σε ένα εικονικό τοπικό δίκτυο (VLAN) προσπαθεί να αποκτήσει πρόσβαση στην κυκλοφορία σε άλλα VLAN που δεν πρέπει να είναι προσβάσιμα. Το VLANhopping είναι μια τεχνική επίθεσης κατά την οποία ο επιτιθέμενος στέλνει πακέτα με ετικέτα που περιέχουν το αναγνωριστικό VLAN του VLAN στο οποίο στοχεύει.

Στη συνέχεια, το αναγνωριστικό VLAN θα επικυρωθεί και το πακέτο θα σταλεί στο VLAN που προοριζόταν για αυτό.

Όπως φαίνεται στην εικόνα 4, ο επιτιθέμενος εξαπολύει επίθεση στο εικονικό τοπικό δίκτυο (VLAN) μέσω του trunk του δικτύου. Το αναγνωριστικό VLAN του VLAN που αποτελεί στόχο θα σταλεί στο πακέτο που μεταδίδεται από τον επιτιθέμενο (Mehdizadehetal., 2017).



Εικόνα 25 Παράδειγμα επίθεσης ARP με τον κακόβουλο χρήστη ως άνθρωπο στο ενδιάμεσο.

MAC Flooding

MAC flooding είναι μια μέθοδος που εφαρμόζεται για να παραβιάσει την ασφάλεια των μεταγωγέων δικτύου. Σκοπός του επιτιθέμενου είναι να καταναλώσει την περιορισμένη μνήμη που έχει οριστεί στο μεταγωγέα για την αποθήκευση του πίνακα διευθύνσεων MAC

Σε αυτή την επίθεση, ο επιτιθέμενος στέλνει πολλές διαφορετικές ψεύτικες διευθύνσεις MAC πηγής..

Στη συνέχεια, η κυκλοφορία κατακλύζεται και γίνεται προσβάσιμη, καθώς ο μεταγωγέας δεν μπορεί πλέον να διατηρήσει τη συγκεκριμένη διεύθυνση προορισμού στη μνήμη.

Εφόσον η κίνηση είναι πλημμυρισμένη, ο εισβολέας μπορεί στη συνέχεια να δει απλά την κίνηση που δημιουργείται και να βρει τις πληροφορίες (Mehdizadehetal., 2017).

Βελτιώσεις VXLAN

Για την αντιμετώπιση μεγαλύτερου αριθμού τμημάτων επιπέδου 2, το VXLAN διαθέτει μεγαλύτερη επεκτασιμότητα. Όταν πρόκειται για τη διευθυνσιοδότηση τμημάτων επιπέδου 2, τα εικονικά τοπικά δίκτυα (VLAN) χρησιμοποιούν ένα αναγνωριστικό VLAN 12 bit. Αυτό έχει ως αποτέλεσμα το όριο κλιμάκωσης να είναι μόνο 4094 VLANs. Εντός του ίδιου διοικητικού τομέα, είναι δυνατόν να συνυπάρχουν έως και 16 εκατομμύρια τμήματα VXLAN (Mehdizadehetal., 2017). Αυτό καθίσταται δυνατό με τη χρήση ενός αναγνωριστικού τμήματος που έχει μήκος 24 bit και αναφέρεται ως αναγνωριστικό δικτύου VXLAN (VNID).

Προκειμένου να παρέχεται ένας μηχανισμός επέκτασης των τμημάτων επιπέδου 2 στο δίκτυο του κέντρου δεδομένων, κάνει χρήση της ενθυλάκωσης MACAddress-in-UserDatagramProtocol (MAC-in-UDP). Το VXLAN είναι ένα σύστημα που επιτρέπει τη λειτουργία ενός περιβάλλοντος που είναι ευέλικτο και μεγάλης κλίμακας, ενώ παράλληλα χρησιμοποιεί μια κοινή φυσική υποδομή.

Το IP σε συνδυασμό με το UDP είναι το πρωτόκολλο μεταφοράς που χρησιμοποιείται στο φυσικό δίκτυο του κέντρου δεδομένων. Το πρωτόκολλο VXLAN προσφέρει μια τεχνική ενθυλάκωσης MAC-in-UDP. Αυτό το σχήμα ενθυλάκωσης περιλαμβάνει την προσθήκη μιας επικεφαλίδας VXLAN στο πρώτο πλαίσιο επιπέδου 2, το

οποίο στη συνέχεια εισάγεται σε ένα πακέτο UDP-IP. Αυτή η ενθυλάκωση MAC-in-UDP επιτρέπει στο VXLAN να δημιουργήσει μια σήραγγα μεταξύ του δικτύου επιπέδου 2 και του δικτύου τρίτου επιπέδου.

Μια επικεφαλίδα VXLAN 8 byte είναι κάτι που εισάγεται από το VXLAN. Αυτή η επικεφαλίδα αποτελείται από ένα VNID 24 bit και μερικά δεσμευμένα bit. Μέσα στο ωφέλιμο φορτίο UDP, η επικεφαλίδα VXLAN περιλαμβάνεται μαζί με το πλαίσιο Ethernet που μεταδόθηκε αρχικά.

Η ταυτοποίηση των τμημάτων επιπέδου 2 και η διατήρηση της απομόνωσης επιπέδου 2 μεταξύ των τμημάτων επιτυγχάνονται και τα δύο με τη βοήθεια του VNID των 24 bit. Το VXLAN μπορεί να υποστηρίξει 16 εκατομμύρια τμήματα LAN όταν χρησιμοποιούνται και τα 24 bit του VNID. Η αντιστοίχιση των τελικών συσκευών των μισθωτών σε τμήματα VXLAN και η απόδοση της ενθυλάκωσης και της απο-ενθυλάκωσης VXLAN επιτυγχάνονται και τα δύο μέσω της χρήσης των συσκευών VXLANTunnelEndPoint (VTEP), όπως αναφέρουν οι Mehdizadeh και συν. (2013).

Για κάθε λειτουργία VTEP είναι διαθέσιμες δύο διεπαφές: Η μία είναι μια διεπαφή IP στο δίκτυο IP μεταφοράς, ενώ η άλλη είναι μια διεπαφή μεταγωγέα στο τοπικό τμήμα LAN που υποστηρίζει τη σύνδεση τοπικού τελικού σημείου μέσω γεφύρωσης. Και οι δύο αυτές διεπαφές βρίσκονται στο ίδιο τμήμα. Στο δίκτυο IP μεταφοράς που αναφέρεται ως VLAN υποδομής, η συσκευή VTEP αναγνωρίζεται από μια μοναδική διεύθυνση IP που εκχωρείται στη συγκεκριμένη διασύνδεση IP. Αυτή η διεύθυνση IP χρησιμοποιείται από τη συσκευή VTEP για την ενθυλάκωση πλαισίων Ethernet. Στη συνέχεια, τα ενθυλακωμένα πακέτα μεταδίδονται στο δίκτυο μεταφοράς μέσω της εφαρμογής της διεπαφής IP.

Μια συσκευή VTEP είναι επίσης σε θέση να μαθαίνει απομακρυσμένες αντιστοιχίσεις διευθύνσεων MAC προς VTEP μέσω της διεπαφής IP, εκτός από την ανακάλυψη των απομακρυσμένων VTEP που σχετίζονται με τα τμήματα VXLAN της. Με τον ίδιο τρόπο που το υποκείμενο δίκτυο IP μεταξύ των VTEP είναι ανεξάρτητο από την επικάλυψη VXLAN, τα τμήματα VXLAN δεν εξαρτώνται από την τοπολογία του υποκείμενου δικτύου.

Η εξωτερική επικεφαλίδα διεύθυνσης IP, η οποία έχει το αρχικό VTEP ως διεύθυνση IP πηγής και το τελικό VTEP ως διεύθυνση IP προορισμού, χρησιμοποιείται για τον προσδιορισμό της δρομολόγησης των ενθυλακωμένων πακέτων (Mehdizadehetal., 2013).

Συμπέρασμα

Όταν πρόκειται για την κατασκευή σύγχρονων δικτυακών υποδομών που δίνουν προτεραιότητα στην αποδοτικότητα, την επεκτασιμότητα και την ασφάλεια, οι τεχνολογίες μεταγωγής και δρομολόγησης που προσφέρει η Cisco είναι απαραίτητες.

Όταν πρόκειται για τοπικά δίκτυα (LAN), η μεταγωγή είναι υπεύθυνη για τη διαχείριση της ροής δεδομένων εντός του ίδιου του δικτύου. Αυτό επιτρέπει την απρόσκοπτη επικοινωνία μεταξύ των συσκευών που είναι συνδεδεμένες στο δίκτυο, όπως υπολογιστές, εκτυπωτές, διακομιστές και άλλα περιφερειακά. Μέσω της χρήσης εξελιγμένων μεθόδων μεταγωγής, η Cisco εγγυάται την αποδοτικότερη αξιοποίηση των πόρων του δικτύου, ενώ ταυτόχρονα διατηρεί την ακρίβεια και την ταχύτητα της μετάδοσης δεδομένων.

Η δυνατότητα τμηματοποίησης ενός δικτύου, η οποία βελτιώνει τόσο την ασφάλεια όσο και τις επιδόσεις με το διαχωρισμό σημαντικών ροών δεδομένων, καθίσταται δυνατή χάρη σε χαρακτηριστικά όπως τα εικονικά τοπικά δίκτυα (VLAN).

Το πρωτόκολλο SpanningTreeProtocol (STP) διατηρεί μια τοπολογία χωρίς βρόχους, η οποία είναι απαραίτητη για τη διατήρηση της σταθερότητας του δικτύου.

Οι μεταγωγείς επιπέδου 3 συνδυάζουν τις δυνατότητες μεταγωγής και δρομολόγησης για να βελτιώσουν τη λειτουργική αποδοτικότητα και να επιτρέψουν την επικοινωνία σε εικονικά τοπικά δίκτυα (VLAN).

Η δρομολόγηση, από την άλλη πλευρά, αφορά την επικοινωνία μεταξύ δικτύων. Πρωταρχικός στόχος της είναι να εγγυηθεί ότι τα δεδομένα μεταφέρονται σε διάφορα δίκτυα, συμπεριλαμβανομένων των δικτύων ευρείας περιοχής (WAN), με αποτελεσματικό τρόπο.

Τα πρωτόκολλα RIP, OSPF, EIGRP και BGP είναι μερικά από τα προηγμένα πρωτόκολλα δρομολόγησης που χρησιμοποιούν οι δρομολογητές της Cisco για να εξασφαλίζουν την αξιόπιστη παράδοση δεδομένων, να βελτιστοποιούν τις διαδρομές δεδομένων και να συνδέουν απομακρυσμένες τοποθεσίες.. Αυτά τα πρωτόκολλα καθιστούν δυνατή την εύρεση από τους δρομολογητές των πιο αποδοτικών διαδρομών για τη μεταφορά δεδομένων, μειώνοντας έτσι το ποσό της καθυστέρησης και αποφεύγοντας τα σημεία συμφόρησης.

Οι λίστες ελέγχου πρόσβασης (ACL), τα εικονικά ιδιωτικά δίκτυα (VPN) και οι ασφαλείς διεπαφές loopback είναι μερικά από τα ισχυρά χαρακτηριστικά ασφαλείας που προσφέρουν οι δρομολογητές της Cisco. Αυτά τα χαρακτηριστικά διασφαλίζουν ότι η ροή των δεδομένων είναι τόσο ασφαλής όσο και υπό έλεγχο.

Το χαρτοφυλάκιο προϊόντων της Cisco δείχνει την ικανότητα της εταιρείας να προσαρμόζεται σε μια μεγάλη ποικιλία απαιτήσεων δικτύωσης. Η Cisco προσφέρει ολοκληρωμένες λύσεις που προσαρμόζονται στις εκάστοτε επιχειρησιακές απαιτήσεις. Οι λύσεις αυτές κυμαίνονται από μη διαχειριζόμενους μεταγωγείς που έχουν σχεδιαστεί για βασική συνδεσιμότητα μικρής κλίμακας έως αρθρωτούς μεταγωγείς και δρομολογητές που έχουν αναπτυχθεί για μεγάλα επιχειρησιακά συστήματα. Δίνει μεγάλη έμφαση στην ποιότητα υπηρεσίας (QoS), η οποία εγγυάται ότι οι βασικές εφαρμογές, όπως οι υπηρεσίες cloud ή οι τηλεδιασκέψεις, λαμβάνουν το απαιτούμενο εύρος ζώνης. Επιπλέον, τα πρωτόκολλα πλεονασμού, όπως το HSRP (Hot Stand by Router Protocol) και το VRRP (Virtual Router Redundancy Protocol), προσφέρουν υψηλή διαθεσιμότητα και ανοχή σε σφάλματα.

Οι καινοτόμες δυνατότητες της εταιρείας περιλαμβάνουν την ενσωμάτωση της δικτύωσης που καθορίζεται από λογισμικό (SDN) και των δυνατοτήτων cloud, όπως αποδεικνύεται από προϊόντα όπως το Cisco DNA και το Meraki. Όσον αφορά τη διαχείριση του δικτύου, οι λύσεις αυτές διευκολύνουν τη διαδικασία παρέχοντας κεντρικό έλεγχο, δεδομένα σε πραγματικό χρόνο και συστήματα αυτόματης αντιμετώπισης προβλημάτων.

Η Cisco παρέχει βοήθεια στις επιχειρήσεις για την πλοήγηση στην πολυπλοκότητα του ψηφιακού μετασχηματισμού γεφυρώνοντας το χάσμα μεταξύ του παραδοσιακού υλικού και των καινοτόμων λύσεων λογισμικού.

Οι τεχνολογίες μεταγωγής και δρομολόγησης που αναπτύσσει η Cisco χρησιμεύουν ως η θεμελιώδης δομή υποστήριξης για τα οικοσυστήματα δικτύων. Παρέχουν στις επιχειρήσεις τη δυνατότητα να κλιμακώσουν τις δραστηριότητές τους, να βελτιώσουν τις επιδόσεις τους και να προστατευτούν από επιθέσεις στον κυβερνοχώρο. Είτε πρόκειται για μια μικρή επιχείρηση που θέλει να βελτιώσει τις εσωτερικές της ροές εργασίας είτε για μια παγκόσμια επιχείρηση που χρειάζεται ισχυρά, διασυνδεδεμένα δίκτυα, η Cisco συνεχίζει να θέτει τα πρότυπα στην αρχιτεκτονική δικτύων παρέχοντας λύσεις αξιόπιστες, καινοτόμες και έτοιμες για το μέλλον. Με αυτές τις δεξιότητες, η Cisco είναι σε θέση να γίνει ένας ανεκτίμητος συνεργάτης για τις επιχειρήσεις που προσπαθούν να ευημερήσουν σε έναν κόσμο που δίνει προτεραιότητα στην ψηφιακή τεχνολογία.

Βιβλιογραφία

Akkaya, K., &Younis, M. (2005). Μια έρευνα για τα πρωτόκολλα δρομολόγησης για ασύρματα δίκτυα αισθητήρων. *Ad Hoc Networks*, *3*(3), 325-349. https://doi.org/10.1016/j.adhoc.2003.09.010.

Ali, A. B., Tabassum, M., & Mathew, K. (2016, Μάρτιος). Συγκριτική μελέτη των πρωτοκόλλων δρομολόγησης IGP και EGP, αξιολόγηση επιδόσεων μαζί με την εξισορρόπηση φορτίου και τον πλεονασμό σε διαφορετικά AS. In Proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 2, pp. 487-967).

Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless Ad-Hoc and mesh networks. *Computer Networks*, *56*(2), 940–965. https://doi.org/10.1016/j.comnet.2011.10.011

Anagnostopoulos, T., & Zaslavsky, A. (2014). Αποτελεσματική συλλογή απορριμμάτων με ημι-στατική και δυναμική δρομολόγηση συντομότερης διαδρομής. *Springer EBooks*, 95-105. https://doi.org/10.1007/978-3-319-10353-2_9

Antoine, V., Bongiorni, R., Borza, A., Bosmajian, P., Duesterhaus, D., Dransfield, M., ... & Ziring, N. (2005). Router Security Configuration Guide. System and Network Attack Center, National Security Agency.

Behera, T. M., Samal, U. C., & Mohapatra, S. K. (2018). Πρωτόκολλα δρομολόγησης. *Studies in Computational Intelligence*, 79-99. https://doi.org/10.1007/978-3-662-57277-1_4

Bergamasco, D., & Pan, R. (2005, Σεπτέμβριος). Ειδοποίηση συμφόρησης προς τα πίσω έκδοση 2.0. Στη συνάντηση του IEEE 802.1.

Bhattacharyya, D., Kim, T., &Pal, S. (2010). Συγκριτική μελέτη των ασύρματων δικτύων αισθητήρων και των πρωτοκόλλων δρομολόγησης τους. *Sensors*, *10*(12), 10506-10523. https://doi.org/10.3390/s101210506

Blahut, R. E. (2003). Αλγεβρικοί κώδικες για μετάδοση δεδομένων. CambridgeUniversityPress.

Bonaventure, O. (2024). Δίκτυα υπολογιστών: Αρχές, πρωτόκολλα και πρακτική. *Hust.edu.vn*. https://doi.org/OER000002122.

Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., &Turgut, D. (2011). Πρωτόκολλα δρομολόγησης σε adhoc δίκτυα: Μια έρευνα. Δίκτυα υπολογιστών, 55(13), 3032-3080.

Britannica Money. (n.d.). Www.britannica.com. https://www.britannica.com/money/business-organization/Limited-liability

Bruschi, D., Ornaghi, A., & Rosti, E. (2003, December 1). *S-ARP: a secure address resolution protocol*. IEEE Xplore. https://doi.org/10.1109/CSAC.2003.1254311

Burdova, C. (2024). *What Is a Router and How Does It Work?* What Is a Router and How Does It Work? https://www.avg.com/en/signal/what-is-a-router

Carthern, C., Wilson, W., & Rivera, N. (2021). *Δίκτυα Cisco*. Apress. https://doi.org/10.1007/978-1-4842-6672-4

Carthern, C., Wilson, W., Rivera, N., & Bedwell, R. (2021). Δίκτυα Cisco: NX-OS και ASA. Apress.

Chatman, J., O'Reilly, C., & Chang, V. (2005). Cisco Systems: Developing a Human Capital Strategy. *California Management Review*, *47*(2), 137–167. https://doi.org/10.2307/41166299

Chatzimisios, P., Boucouvalas, A., & Vitsas, V. (2005). Ασύρματα τοπικά δίκτυα IEEE 802.11: Ανάλυση επιδόσεων και τελειοποίηση πρωτοκόλλων: Ανάλυση επιδόσεων και τελειοποίηση πρωτοκόλλων. *EURASIP Journal on Wireless Communications and Networking*, *2005*(1). https://doi.org/10.1155/wcn.2005.67.

Chen, R. (Ronxin), Ravichandar, R., & Proctor, D. (2016). Managing the transition to the new agile business and product development model: Lessons from Cisco Systems. *Business Horizons*, *59*(6), 635–644. https://doi.org/10.1016/j.bushor.2016.06.005

Chilukuri, M. P. D. (2017). Προφίλ ισχύος των μεταγωγέων δικτύου. Στο www.diva-portal.org. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1077099

Chitkara, M., & Ahmad, M. W. (2014). Ανασκόπηση του manet: χαρακτηριστικά, προκλήσεις, επιταγές και πρωτόκολλα δρομολόγησης. International journal of computer science and mobile computing, 3(2), 432-437.

Cisco Meraki. (2020, 5 Οκτωβρίου). *Επισκόπηση του πρωτοκόλλου Spanning Tree Protocol (STP)*. Cisco Meraki. https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_(STP)_Overview

Cisco Networking Academy, & Cisco Networking Academy Program. (2014). *Routing and Switching Essentials Companion Guide*. Pearson Education.

Cisco Packet Tracer, (2013). Tracer. URL: http://www. cisco. com/web/learning/netacad/coursecatalog/PacketTracer. html.

Cisco Press. (2014). *Types of Routing Protocols > Cisco Networking Academy's Introduction to Routing Dynamically*. Www.ciscopress.com. https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7

Cisco Systems, Incorporated, C. O. R. P. O. R. A. T. E. (1999). Cisco IOS 12.0 Configuration Fundamentals. Cisco Press.

Cloudflare. (2024). What Is routing? | IP Routing | Cloudflare. *Cloudflare*. https://www.cloudflare.com/learning/network-layer/what-is-routing/

Communications Inc. (2024). *Gateway/Router Performance Measurements*. Gl.com. https://www.gl.com/gateway-router-performance-measurements.html

Deal, R. (2004). Cisco router firewall security. Cisco Press.

Dumitrache, C. G., Predusca, G., Circiumarescu, L. D., Angelescu, N., & Puchianu, D. C. (2017, October 1). *Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer*. IEEE Xplore. https://doi.org/10.1109/ISEEE.2017.8170694

Dye, M., McDonald, R., & Rufi, A. (2007). Βασικές αρχές δικτύου, συνοδευτικός οδηγός εξερεύνησης CCNA. Ciscopress.

Elhadj, H. B., Chaari, L., &Kamoun, L. (2012). Μια έρευνα πρωτοκόλλων δρομολόγησης σε ασύρματα δίκτυα περιοχής σώματος για εφαρμογές υγειονομικής περίθαλψης. International Journal of E-Health and Medical Communications (IJEHMC), 3(2), 1-18.

Entezami, F., & Politis, C. (2013). Μετρικές πρωτοκόλλου δρομολόγησης για ασύρματα δίκτυα πλέγματος - Kingston University Research Repository. *Kingston.ac.uk.* https://eprints.kingston.ac.uk/id/eprint/25608/1/Routing%20Protocol%20Metrics%20for%20Wireless%20Mesh%20Networks.pdf

Feeney, L. M., Cetin, B., & Hollos, D. (2004). Αναμετάδοση πολλαπλών συχνοτήτων για βελτίωση της απόδοσης σε IEEE 802.11 WLANs. Proc. universitat Paderborn.

Froom, R. (2010). *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide*.

Froom, R., & Frahim, E. (2015). *Τύποι μεταγωγέων Cisco > Οδηγός εκμάθησης του Ιδρύματος Implementing Cisco IP Switched Networks (SWITCH): Network Design*

Fundamentals | Cisco Press. Www.ciscopress.com. https://www.ciscopress.com/articles/article.asp?p=2348265&seqNum=2.

García Villalba, L., Sandoval Orozco, A., Triviño Cabrera, A., & Barenco Abbas, C. (2009). Πρωτόκολλα δρομολόγησης σε ασύρματα δίκτυα αισθητήρων. *Sensors*, *9*(11), 8399-8421. https://doi.org/10.3390/s91108399.

Garimella, P., Sung, Y.-W. E., Zhang, N., & Rao, S. (2007). Characterizing VLAN usage in an operational network. *Proceedings of the 2007 SIGCOMM Workshop on Internet Network Management - INM '07*. https://doi.org/10.1145/1321753.1321772

H. Altunbasak, & Owen, H. (2007). *An architectural framework for data link layer security with security inter-layering*. https://doi.org/10.1109/secon.2007.342975

Haddadi, H., Rio, M., Iannaccone, G., Moore, A., & Mortier, R. (2008). Τοπολογίες δικτύων: εξαγωγή συμπερασμάτων, μοντελοποίηση και δημιουργία. *IEEECommunicationsSurveysTutorials*, *10*(2), 48-69. https://doi.org/10.1109/COMST.2008.4564479

Hasan, Md. Kamrul., & Ahammed, S. (2015). Σχεδιασμός και υλοποίηση εταιρικού δικτύου με χρήση πρωτοκόλλου δρομολόγησης μεταξύ των Vlan. *133.167.5*. http://dspace.ewubd.edu/handle/2525/1840

Heron, S. (2014). Ten top threats to VLAN security.

IEEE, R. (2010). IEEE Standard for Information Technology-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. IEEE Std 802.11 p-2010 (Amendment to IEEE Std 802.11-2007 as Amended by IEEE Std 802.11 k-2008, IEEE Std 802.11 r-2008, IEEE Std 802.11 y-2008, IEEE Std 802.11 n-2009, and IEEE Std 802.11 w-2009), 1-51.

Javaid, N. (2010). *Ανάλυση και σχεδιασμός μετρικών ποιότητας σύνδεσης για πρωτόκολλα δρομολόγησης σε ασύρματα δίκτυα.* https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=017aaa194527ac3c257b89db1e5161b18bc34be6

Kapadia, S., Subagio, P. H., Yang, Y., Shah, N., Jain, V., & Agrawal, A. (2017). U.S. Patent No. 9,565,105. Washington, DC: U.S. Patent and Trademark Office.

Kessler, G. C. (2015). Τοπολογίες, πρωτόκολλα και σχεδιασμός τοπικών δικτύων. *Computer Security Handbook*, 6.1-6.31. https://doi.org/10.1002/9781118851678.ch6.

Kraemer, K. L., & Dedrick, J. (2002). Strategic use of the Internet and e-commerce: Cisco Systems. *The Journal of Strategic Information Systems*, *11*(1), 5–29. https://doi.org/10.1016/s0963-8687(01)00056-7

Kumar, S. (2005). Impact of Distributed Denial of Service (DDoS) Attack Due to ARP Storm. *Networking - ICN 2005*, 997–1002. https://doi.org/10.1007/978-3-540-31957-3_113

Kvitoslava Obelovska, I. Kozák, & Yaromyr Snaichuk. (2023). Ανάλυση και σύγκριση των διαδικασιών δρομολόγησης και μεταγωγής σε δίκτυα περιοχής πανεπιστημιουπόλεων με χρήση του CiscoPacketTracer. *Lecture Notes on Data Engineering and Communications Technologies*, 100-110. https://doi.org/10.1007/978-3-031-24475-9_9.

Lammle, T. (2000). CCNA Cisco certified network associate study guide. Sybex.

Liu, D. (2009). Εγκληματολογία δρομολογητών και μεταγωγέων Cisco: Διερεύνηση και ανάλυση κακόβουλης δραστηριότητας δικτύου. Syngress.

Lucas, M. W. (2009). Cisco Routers for the Desperate: Router Management, the Easy Way. NoStarchPress.

Macfarlane, J. (2007). Βασικά στοιχεία δρομολόγησης δικτύου: Κατανόηση της δρομολόγησης IP σε συστήματα Cisco. JohnWiley&Sons.

Majumdar, A. K. (2018). Οπτικές ασύρματες επικοινωνίες για ευρυζωνική παγκόσμια συνδεσιμότητα στο διαδίκτυο: βασικές αρχές και πιθανές εφαρμογές. Elsevier.

Malik, S. (2003). Network security principles and practices.

Manzoor, A., Hussain, M., & Mehrban, S. (2020). Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols. *Computer Standards & Interfaces*, *68*, 103391. https://doi.org/10.1016/j.csi.2019.103391

Manzoor, A., Hussain, M., & Mehrban, S. (2020). Ανάλυση επιδόσεων και βελτιστοποίηση διαδρομής: EIGRP, OSPF&BGP: Ανακατανομή μεταξύ των πρωτοκόλλων δρομολόγησης. *Computer Standards & Interfaces*, *68*, 103391. https://doi.org/10.1016/j.csi.2019.103391

Mcquerry, S., Jansen, D., & Hucaby, D. (2009). *Cisco LAN Switching configuration Handbook : a concise reference for implementing the most frequently used features of the Cisco Catalyst family of switches*. Cisco Press.

Medhi, D., & Ramasamy, K. (2017). Network routing: algorithms, protocols, and architectures. Morgan kaufmann.

Mehdizadeh, A., Abdullah, R. S. A. R., Hashim, F., Ali, B. M., Othman, M., & Khatun, S. (2013). Reliable Key Management and Data Delivery Method in Multicast Over Wireless IPv6 Networks. *Wireless Personal Communications*, *73*(3), 967–991. https://doi.org/10.1007/s11277-013-1226-5

Mehdizadeh, A., Raja Abdullah, R. S. A., & Hashim, F. (2012). Secure group communication scheme in wireless IPv6 networks: An experimental test-bed. *2012 International*

Symposium on Communications and Information Technologies (ISCIT), 724–729. https://doi.org/10.1109/iscit.2012.6380997

Mehdizadeha, A., Suinggia, K., Mohammadpoorb, M., & Haruna, H. (2017, December). Virtual Local Area Network (VLAN): Segmentation and Security. In The Third International Conference on Computing Technology and Information Management (ICCTIM2017) (Vol. 78, p. 89).

MuhammetEminKamiloğlu. (2015). Αξιολόγηση της απόδοσης του δικτύου Cisco με τη χρήση του PacketTracer. *International Journal of Electronics Mechanical and Mechatronics Engineering*, *5*(1), 905-911. https://dergipark.org.tr/en/pub/ijemme/issue/26179/275746

Neila Krichene, & Noureddine Boudriga. (2008). Δίκτυα πλέγματος σε ασύρματα PANs, LANs, MANs και WANs. *Auerbach Publications EBooks*, 45-109. https://doi.org/10.1201/b13595-2

Nguyen, V. G., & Kim, Y. H. (2016). SDN-based enterprise and campus networks: a case of VLAN management. Journal of Information Processing Systems, 12(3), 511-524.

Pal, G. (2013). Virtual local area network (VLAN). Faculty of Electronics & Communication Engineering Department.

Pankaj Ghimire. (2023, 10 Μαΐου). *VLAN AND INTER VLAN ROUTING - Pankaj Ghimire - Medium*. Medium; Medium. https://medium.com/@karan.ghimire3107/vlan-and-inter-vlan-routing-66a65078acc4

Paquet, C. (2012). Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide. CiscoPress.

Paul, S. (2011). Διανομή ψηφιακού βίντεο σε ευρυζωνικά, τηλεοπτικά, κινητά και συγκλινόμενα δίκτυα: Τάσεις, προκλήσεις και λύσεις. John Wiley & Sons.

Poss, M., & Raack, C. (2012). Affine recourse for the robust network design problem: Between static and dynamic routing. *Networks*, *61*(2), 180-198. https://doi.org/10.1002/net.21482

QiangNi. (2005). Ανάλυση επιδόσεων και βελτιώσεις για ασύρματα δίκτυα IEEE 802.11e. *IEEENetwork*, *19*(4), 21-27. https://doi.org/10.1109/mnet.2005.1470679.

Rao, P. M., & Raju, G. S. N. (2014). International Journal of Advanced Research in Computer Science and Software Engineering. International Journal, 4(5).

Ratnasamy, S., Stoica, I., & Shenker, S. (2002). Routing Algorithms for DHTs: Some Open Questions. *Lecture Notes in Computer Science*, 45–52. https://doi.org/10.1007/3-540-45748-8_4

Salman, T., & Jain, R. (2016). ΠΡΩΤΌΚΟΛΛΑ ΚΑΙ ΠΡΌΤΥΠΑ ΔΙΚΤΥΩΣΗΣ ΓΙΑ ΤΟ ΔΙΑΔΊΚΤΥΟ ΤΩΝ ΠΡΑΓΜΆΤΩΝ. *Internet of Things and Data Analytics Handbook*, 215-238. https://doi.org/10.1002/9781119173601.ch13.

Savage, D., Slice, D., Ng, J., Moore, S., & White, R. (2013). Enhanced interior gateway routing protocol. Internet Engineering Task Force.

Schneier, B. (2008). The Psychology of Security. *Progress in Cryptology – AFRICACRYPT 2008*, 50–79. https://doi.org/10.1007/978-3-540-68164-9_5

Snyder, J., & Eng Lee-Partridge, J. (2013). Κατανόηση των επιλογών καναλιών επικοινωνίας στην ομαδική ανταλλαγή γνώσεων. *Corporate Communications: An International Journal*, *18*(4), 417-431. https://doi.org/10.1108/ccij-03-2012-0026.

Somasundaram, S., & Chandran, M. (2018). A Simulation based study on Network Architecture Using Inter-VLAN Routing and Secure Campus Area Network (CAN). network, 10, 19.

Sung, Y.-W. E., Rao, S. G., Xie, G. G., & Maltz, D. A. (2008). Towards systematic design of enterprise networks. *Proceedings of the 2008 ACM CoNEXT Conference on - CONEXT '08*. https://doi.org/10.1145/1544012.1544034

Tetz, E. (2011). *Cisco networking all-in-one for dummies*. John Wiley & Sons.

Tsimonis, G., & Dimitriadis, S. (2014). Brand Strategies in Social Media. *Marketing Intelligence & Planning*, *32*(3), 328–344. https://doi.org/10.1108/MIP-04-2013-0056

Ul Haq, S. E., & Parveen, S. (2017). IMPLEMENTATION OF NETWORK ARCHITECTURE, ITS SECURITY AND PERFORMANCE ANALYSIS OF VLAN. International Journal of Advanced Research in Computer Science, 8(7).

Van Heddeghem, W., Lambert, S., Lannoo, B., Colle, D., Pickavet, M., & Demeester, P. (2014). Trends in worldwide ICT electricity consumption from 2007 to 2012. *Computer Communications*, *50*, 64–76. https://doi.org/10.1016/j.comcom.2014.02.008

Waheed, F., & Ali, M. (2018, July 1). *Hardening CISCO Devices Based on Cryptography and Security Protocols - Part One: Background Theory*. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3523710

Wazir Zada Khan, Saad, N. M., & Aalsalem, M. Y. (2012). *Μια επισκόπηση των μετρικών αξιολόγησης για πρωτόκολλα δρομολόγησης σε ασύρματα δίκτυα αισθητήρων.* https://doi.org/10.1109/icias.2012.6306083

Whalen, S. (2001). *An Introduction to ARP Spoofing*. http://www.gbppr.net/2600/arp_spoofing_intro.pdf

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*, *15*(4), 2046–2069. https://doi.org/10.1109/surv.2013.031413.00127