EVPN-VxLAN στηρίζουν τα νέα ευέλικτα και cloud-ready δίκτυα σε Campus/Branch και Data Centers

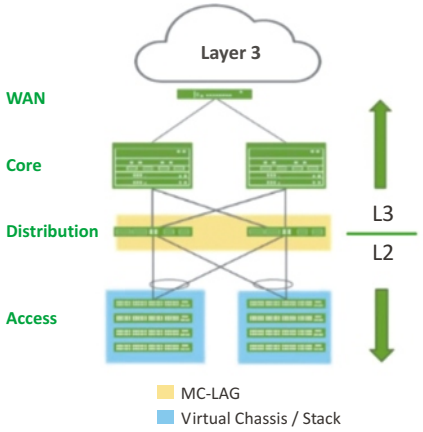
εισαγωγή, οφέλη και παραδείγματα χρήσης

*Άρθρο του **Σταύρου Καραγκιούλογλου**, Dipl.-Ing*
Managing Partner United-Telecom AE-
Partner Juniper Networks
e-mail: s.kara@united-telecom.gr

Τα δίκτυα υπολογιστών σήμερα

Το όραμα των μηχανικών δικτύων υπολογιστών είναι να εξελιχθεί και να απλοποιηθεί η δικτύωση σε όλο το γεωγραφικό εύρος των επιχειρήσεων σε τέτοιο βαθμό, που να καλύπτει με ολικό και ενιαίο τρόπο όλη τη διαδρομή από τον χρήστη μέχρι το cloud, περνώντας στη διαδρομή από τη συσκευή του χρήστη (ενσύρματα και ασύρματα), το SD-WAN, το Data Center και τις εφαρμογές cloud, συνοδευόμενη πάντα από την απαραίτητη ασφάλεια και επωφελούμενη από τις νέες ευκολίες που προσφέρει το AI (Τεχνητή Νοημοσύνη).

Η εικόνα 1 δείχνει τα κύρια ζητήματα που στέκονται εμπόδιο στα σημερινά campus δίκτυα για να εξελιχθούν και να εκπληρώσουν το παραπάνω όραμα. Στα σημερινά δίκτυα έχουμε στο επίπεδο πρόσβασης (δηλ. access layer) κυρίως συσκευές Layer-2, ενώ το διαδίκτυο και η ραχοκοκαλιά ενός δικτύου campus είναι Layer-3. Σε αυτό το περιβάλλον, η τεχνολογία που χρησιμοποιείται συνήθως είναι το ιδιωτικό πρωτόκολλο MC-LAG (Multi Chassis Link Aggregation Groups) όπου οι κατασκευαστές εφαρμόζουν ο καθένας την δική του προδιαγραφή. Επίσης πολλές φορές εφαρμόζεται τεχνολογία STP (Spanning Tree Protocol) που πλέον θεωρείται αρκετά προβληματική από πολλές απόψεις. Δικτυακός εξοπλισμός και υλοποιήσεις με MC-LAG και STP κατά κανόνα δεν είναι σύγχρονος, καθώς αυτά σε καμμία περίπτωση δεν έχουν σχεδιαστεί για νέες εφαρμογές όπως το Mobility, τις πολλαπλές και συγκλίνουσες πολύλειτουργικές συσκευές του κάθε χρήστη, συσκευές και εφαρμογές IoT που πολλές φορές απαιτούν μικροτμηματοποίηση (Micro-Segmentation) του δικτύου πέρα από τα VLANs και PVLANs (private VLAN). Τελευταίο, αλλά όχι λιγότερο σημαντικό πρόβλημα είναι ο διαρκώς αυξανόμενος αριθμός ACL (Access Control List) στις συσκευές δικτύων, όπου κατά κανόνα δεν υπάρχει επιμέλεια αφαίρεσης αχρηστευμένων



1) Συσκευές χρηστών επιπέδου Layer-2 συνδέονται στο δίκτυο Network (Layer 3)

2) Μη τυποποιημένες τεχνολογίες για αποφυγή βρόγχων STP

3) Δύσκαμπτα και δύσκολα μεγεθυνόμενα δίκτυα

4) Δεν έχουν σχεδιαστεί για Mobility και IoT

5) Ανεξέλεγκτη αύξηση των ACLs σε όλες τις συσκευές

Εικόνα 1. Αδυναμίες δικτύων Campus σήμερα

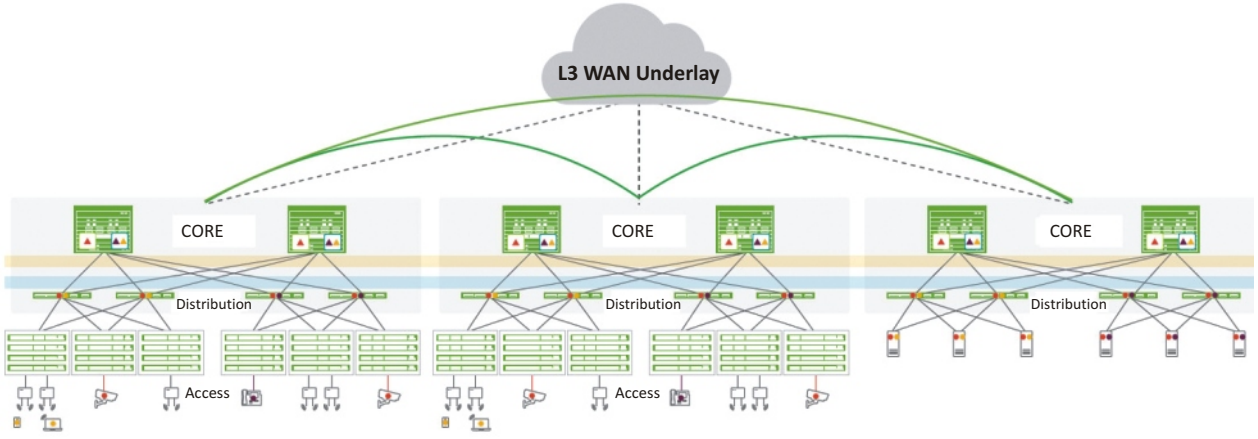
εντολών και έτσι οι εντολές ACL πληθαίνουν συν το χρόνο ανεξέλεγκτα με αποτέλεσμα να δημιουργείται ένα άχρηστο φορτίο και πηγή κινδύνων.

Ενδεικτικό παράδειγμα για την ανεπάρκεια των VLANs/PVLANs είναι πχ δίκτυο VLAN με κάμερες οι οποίες επικοινωνούν με τον διακομιστή καμερών. Η πρόνοια του VLAN δεν είναι σε θέση να εξασφαλίσει στο επίπεδο αυτό ότι οι κάμερες δεν θα επικοινωνούν μεταξύ τους, εξ αιτίας αυτού ενδέχεται να εισχωρήσει ξένη συσκευή πλαστογράφησης που θα μπορεί να αντλεί όλη την κίνηση. Γίνεται σαφές έτσι ότι με την πρόοδο του IoT η μικροτμηματοποίηση, και μάλιστα με κοινές προδιαγραφές μεταξύ των κατασκευαστών έχει γίνει πλέον πολύ σημαντική.

Σε αυτή την ίδια συζήτηση εντάσσεται και η ανάγκη να απεξαρτοποιηθούν πλέον τα Layer-2 και Layer-3 δίκτυα από τις συσκευές hardware στις οποίες "κατοικούν" σήμερα (Network Virtualization). Με την απεξάρτηση αυτή θα δινόταν η δυνατότητα δικτύωσης των δικτύων μέσω κανονικών γραμμών internet δίχως την ανάγκη (συνήθως ακριβών ακόμη) πρωτοκόλλων όπως πχ το MPLS. Η εικόνα 2 δείχνει μία τέτοια εξέλιξη όπου κανόνες και λογικές που σήμερα είναι εγκλωβισμένες σε επίπεδο LAN θα μπορούσαν να επεκταθούν και να βρουν εφαρμογή σε επίπεδο WAN μίας επιχείρησης. Έτσι επιτυγχάνεται μεγάλη απλούστευση και δίνεται σημαντικότατη ευκολία στην αρχική παραμετροποίηση (rollout) ως επίσης και στην μετέπειτα φάση, δηλ. την υποστήριξη και λειτουργία του δικτύου.

Τεχνολογική εξέλιξη δικτύων - Πρωτόκολλα βάσης

Ως απάντηση στα εμπόδια που αναφέρθηκαν εξελίχθηκε και εφαρμόζεται πλέον η τεχνολογία



Εικόνα 2. Παν-γεωγραφικό LAN/VLAN μεταξύ DataCenter, Campus και Branch

Ethenet-VPN με Virtual eXtended LAN (EVPN-VxLAN), η οποία λύνει τα προβλήματα και τις δυσκολίες που περιγράφονται πιο πάνω. Επιπλέον, η τεχνολογία EVPN-VxLAN έχει ιδιαίτερη αξία, αφού υπακούει σε ανοικτές προδιαγραφές και δεν είναι πλέον κάποιο κλειστό πρωτόκολλο συγκεκριμένου κατασκευαστή δίνοντας έτσι δυνατότητα βελτιστοποίησης κόστους μέσω ανταγωνισμού μεταξύ προμηθευτών.

Το EVPN-VxLAN απαντάει στα παραπάνω θέματα:

Στο EVPN-VxLAN όλες οι συσκευές στο Campus μπορούν να αντιμετωπίζονται ως Layer-2 που συνδέονται στο Layer-3. Αυτό μπορεί να ισχύσει μέχρι και για τις δικτυακές συσκευές στο επίπεδο πρόσβασης ανάλογα με την υλοποίηση.

Στο επίπεδο διανομής (distribution layer) με το EVPN-VxLAN μπορεί να ξεπεραστεί και ο περιορισμός των δύο συσκευών βάσει του MC-LAG. Επίσης δεν χρειάζεται πλέον το πρωτόκολλο STP.

Το EVPN-VxLAN παρέχει σημαντικές ευκολίες για την βέλτιστη διαχείριση της κίνησης στην κάθετη κατεύθυνση εντός του LAN και από προς το WAN (north-south traffic) ως επίσης και στην διαχείριση της οριζόντιας κίνησης εντός LAN και μεταξύ των σημείων παρουσίας μέσω του WAN (east-west traffic) επεκτείνοντας τις λειτουργίες VLAN με ενιαίο τρόπο σε όλο το LAN και WAN δίκτυο (VxLAN).

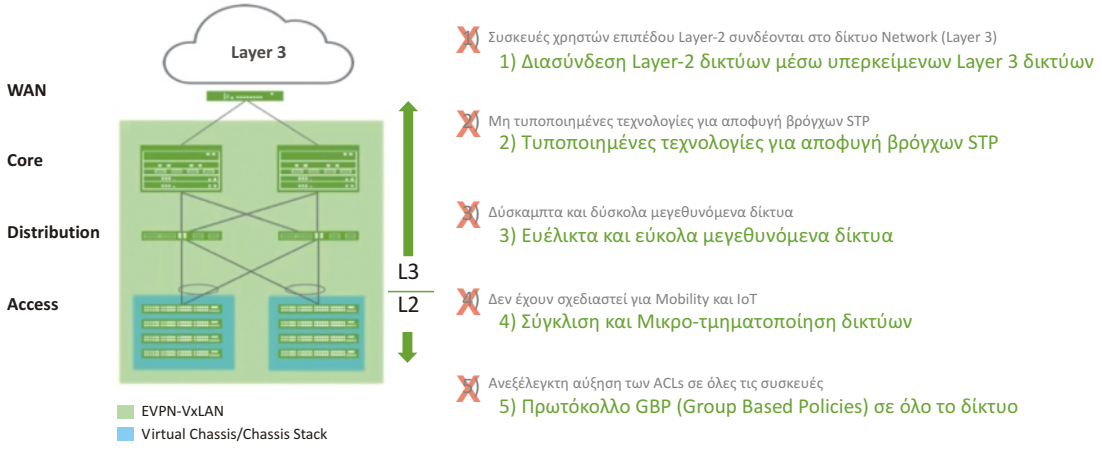
Επίσης, το EVPN υποστηρίζει και ενισχύει την μικροτμηματοποίηση και την γρήγορη σύγκλιση παρέχοντας νέα εργαλεία όπως την λειτουργία GBP (Group Based Policies). Με το GBP μπορεί να γίνει εύκολη δημιουργία και διαχείριση της μικροτμηματοποίησης των δικτύων και εφαρμογή πολιτικών εντός αυτών - ακόμη και για μικροτμήματα που επεκτείνονται σε πολλά σημεία μέσω του WAN.

Αναφορικά με το παράδειγμα των καμερών όπου δεν είναι επιθυμητό να επικοινωνούν μεταξύ τους, τον κανόνα αυτό μπορεί πλέον να τον επιβάλλει το GBP, και μάλιστα σε επίπεδο WAN εφαρμόζοντας τις πολιτικές μέσα σε όλη την έκταση του EVPN-VxLAN σε όλα τα σημεία παρουσίας.

Επίσης, το EVPN επιτρέπει να συνοψισθούν και να εφαρμοσθούν οι επιλεχθείσες πολιτικές σε ολόκληρο το δίκτυο μιας και τις μεταδίδει σε όλες τις συσκευές του δικτύου. Έτσι δεν χρειάζεται πλέον ενασχόληση με τα προβλήματα του ACL.

Το EVPN, εφαρμόζοντας καθολική συνδεσιμότητα επιπέδων Layer-2 και Layer-3 εντός του WAN δίνει την δυνατότητα να διαχωρισθεί η φροντίδα και η ευθύνη του εξοπλισμού δικτύου από την φροντίδα και ευθύνη των εφαρμογών που λειτουργούν επάνω στο δίκτυο.

Έχοντας λοιπόν διαχωρίσει τις λειτουργίες εντός του δικτύου, το τεχνικό τμήμα υποδομών επικεντρώνεται στην υποδομή "μεταφοράς",



Εικόνα 3. Η τεχνολογία EVPN-VxLAN δίνει λύσεις

United Telecom

Your Secure Network Integrator

United Telecom Υπηρεσίες:

- Managed Service Provider (MSP)
- Secure Wired & Wireless Networks – SD-WAN/LAN
- Remote Access Authentication & Teleworking/WFH
- CISSP Risk Assessment, Forensics & Security Policy
- Telecom Optimized Solutions

UNITED TELECOM A.E.

Περικλέους 29 Γέρακας, 15344 Αθήνα – Τηλ. 210.6085599

www.united-telecom.gr – info@united-telecom.gr

που αποτελείται πλέον μόνο από τις συσκευές και τις γραμμές του δικτύου. Οι υπηρεσίες τοποθετούνται επάνω στην υποδομή αυτή που εξασφαλίζει την καθολική συνδεσιμότητα.

Ακόμη και σε περιπτώσεις όπου το ίδιο τεχνικό IT τμήμα είναι υπεύθυνο και για την υποδομή και για τις εφαρμογές, συνεχίζουν να ισχύουν όλα τα παραπάνω πλεονεκτήματα από την εφαρμογή τεχνολογίας EVPN στην διασύνδεση μεταξύ δύο ή περισσότερων DCs (Data Center interconnect) και στην τμηματοποιημένη πρόσβαση σε περιβάλλοντα Campus/Branch.

Εν κατακλείδι, η αναβάθμιση των υποδομών και η τυποποίηση των υπηρεσιών που παρέχει το νέο δίκτυο μπορεί να μειώσει δραστικά τον φόρτο διαχειριστικών εργασιών στο τμήμα IT και έτσι θα μπορεί να εξοικονομηθεί χρόνος, ενέργεια και κόστος.

Η νέα δομή βάσει EVPN-VxLAN εξασφαλίζει επίσης τα κάτωθι πλεονεκτήματα που συνδέονται άρρηκτα με υψηλή διαθεσιμότητα, ασφάλεια και ευελιξία λειτουργιών και εφαρμογών (δικτυακών και τοπικών):

- Προβλεψιμότητα: Οι εργασίες παραμετροποίησης εξοπλισμών απλοποιούνται και ο χρόνος ανάπτυξης μειώνεται αντίστοιχα. Έτσι, ο χρόνος των υλοποιήσεων για συνδεσιμότητα γίνεται πιο προβλέψιμος.
- Ανταλλαξιμότητα μεταξύ εξοπλισμών λόγω εκατέρωθεν συμβατότητας. Μεταξύ άλλων, αυτό δίνει δυνατότητα για οικονομίες κλίμακας.
- Στεγανοποίηση: Λόγω των ιδεατών δικτύων και συνδέσεων που έχουν υλοποιηθεί με το EVPN-VxLAN, ενδεχόμενα προβλήματα σε κάποιο από τα δίκτυα δεν επηρεάζει καθόλου τα υπόλοιπα. Αυτό βελτιώνει το επίπεδο ασφάλειας και διαθεσιμότητας των εφαρμογών που λειτουργούν επάνω στην υποδομή.
- Υποστήριξη: Η εκτενής τυποποίηση υποδομών και λειτουργιών που πετυχαίνει η υποδομή βάσει EVPN-VxLAN εξασφαλίζει δυνατότητα αντίστοιχης τυποποίησης σχεδόν όλων των λειτουργιών για την τεχνική υποστήριξη πετυχαίνοντας βελτιστοποίηση κόστους αλλά και αύξηση της διαθεσιμότητας του δικτύου και των εφαρμογών.
- Ευκολόχρηστο: Η τυποποίηση των λειτουργιών εξασφαλίζει σημαντική ευκολία και στην χρήση και στην αυτό-εξυπηρέτηση (self-service) των διαθέσιμων λειτουργιών στο δίκτυο. Αυτό βοηθάει στην μείωση ρίσκου και χρόνου υλοποίησης στην ανάπτυξη και υποστήριξη των εφαρμογών. Σε περιβάλλοντα υψηλού ανταγωνισμού με μηδαμινούς χρόνους ανταπόκρισης η δυνατότητα αυτή είναι πολύ μεγάλης αξίας (Continuous Integration/ Continuous Delivery).

Παρουσίαση της τεχνολογίας VxLAN και χαρακτηριστικά

Η τεχνολογία VxLAN είναι μία Layer-2 τεχνολογία που συνδυάζεται με το Layer-3 πρωτόκολλο Ethernet VPN (EVPN).

Με το VxLAN μπορεί να τμηματοποιηθεί το δίκτυο (όπως άλλωστε γίνεται και με τα VLANs) πλην όμως το VxLAN εξασφαλίζει πρόσθετες δυνατότητες που δεν υπάρχουν στα VLANs.

Τα σημαντικότερα οφέλη από την χρήση VxLAN είναι:

- Τα δίκτυα μπορούν να διαχειριστούν πολλά περισσότερα VLANs. Βάσει της προδιαγραφής IEEE 802.1Q που ορίζει την ταυτότητα των παραδοσιακών VLANs στα 12 bit, αυτά περιορίζονται στα 4094 ανά δίκτυο. Το πρωτόκολλο VxLAN ξεπερνάει τον περιορισμό αυτό χρησιμοποιώντας μία μεγαλύτερη λογική διεύθυνση (logical network identifier) που επιτρέπει περισσότερα VLANs (θεωρητικά μέχρι 16 εκατομμύρια VxLAN) και ως συνέπεια αυτού παρέχει μεγαλύτερη ευελιξία στην στεγανοποίηση (isolation) μεταξύ των λογικών δικτύων (logical networks) εντός μεγάλων δικτύων όπως πχ τα δίκτυα που επεκτείνονται σε πολλαπλά Data Centers, δίκτυα με μικτή ή αποκλειστική χρήση

cloud, δίκτυα με πολλαπλά VM (Virtual Machines), κλπ.

- Δυνατότητα επικοινωνίας μεταξύ VMs που φιλοξενούνται σε servers που βρίσκονται σε διαφορετικούς Layer-2 τομείς δρομολογώντας κίνηση μέσω tunnel που στήνεται επάνω σε ένα Layer-3 δίκτυο. Έτσι ξεπερνούνται τα όρια ενός περιορισμένου Layer-2 δικτύου και δίνεται η δυνατότητα ευέλικτης και δυναμικής χρήσης πόρων που βρίσκονται εντός του οικίου ή εντός ενός απομακρυσμένου Data Center.
- Το VxLAN δίνει την δυνατότητα να αναπτύσσονται μικρότερα και περισσότερα Layer-2 δίκτυα και να διασυνδέονται μεταξύ τους επάνω από ένα Layer-3 δίκτυο. Αυτό σημαίνει πρακτικά ότι μπορεί να αποφευχθεί η χρήση του πρωτοκόλλου STP (Spanning Tree Protocol) και να αξιοποιηθούν αντί αυτού πιο συμπαγή και ολοκληρωμένα πρωτόκολλα δρομολογήσεων επάνω στο Layer-3 δίκτυο. Αποφεύγοντας το STP είναι πλέον διαθέσιμες όλες οι θύρες και όλο το εύρος του δικτύου μεταφοράς.
- Επιπλέον, το VxLAN, σε συνδυασμό με πρωτόκολλο δρομολόγησης για την διασύνδεση Layer-2 δικτύων μεταξύ τους, δίνει την δυνατότητα να εξισορροπηθεί η κίνηση μεταξύ πολλαπλών γραμμών (traffic load balance) και κατά συνέπεια να αξιοποιηθούν καλύτερα οι υπάρχοντες πόροι.

Με δεδομένο ότι σήμερα την εποχή των διασυνδεδεμένων εφαρμογών, η κίνηση εντός Data Center ή μεταξύ των Data Centers (east-west traffic) αυξάνεται δραματικά, η βελτίωση και η ευκολία που προσφέρει το VxLAN για την αύξηση της απόδοσης των υποδομών στην κίνηση αυτής της κατηγορίας γίνεται όλο και πιο σημαντική.

Προδιαγραφές του VxLAN

Το VxLAN προδιαγράφεται από τα κάτωθι RFC και Internet draft:

- RFC 7348, Virtual eXtensible Local Area Network (VxLAN): A Framework for Overlaying Virtualized Layer-2 Networks over Layer-3 Networks
- Internet draft draft-ietf-nvo3-VxLAN-gpe, Generic Protocol Extension for VxLAN.

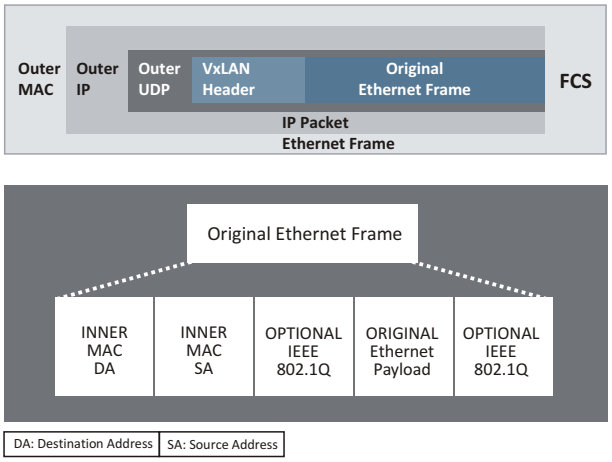
Το VxLAN περιγράφεται συχνά ως μία υπερκείμενη (overlay) τεχνολογία η οποία επιτρέπει να "τεντωθεί" ένα Layer-2 δίκτυο και να απλωθεί σε πολλά γεωγραφικά σημεία μέσω ενός Layer-3 δικτύου. Αυτό γίνεται δυνατό μέσω εγκιβωτισμού (tunneling) ακολουθιών Ethernet (frames) μέσα σε ένα Layer-3 UDP πακέτο, το οποίο περιλαμβάνει και τις διευθύνσεις IP.

Οι συσκευές δικτύου που είναι σε θέση να χειριστούν κίνηση VxLAN ονομάζονται VTPEs (Virtual Tunnel Endpoints). Αυτές μπορεί να είναι switches ή routers δικτύων ή ακόμη και servers.

Τα VTEPs εγκιβωτίζουν και αποκιβωτίζουν την κίνηση VxLAN όταν αυτή εισέρχεται και εξέρχεται προς και από το VxLAN tunnel.

Για τον εγκιβωτισμό μίας ακολουθίας Ethernet frame, τα VTEPs προσθέτουν τα κάτωθι πεδία:

- Outer media access control (MAC) destination address (MAC address του tunnel endpoint VTEP)
- Outer MAC source address (MAC address του tunnel source VTEP)
- Outer IP destination address (IP address του tunnel endpoint VTEP)



Εικόνα 4. VxLAN Packet Format

- Outer IP source address (IP address του tunnel source VTEP)
- Outer UDP header
- Μία επικεφαλίδα VxLAN που αποτελείται από 24-bit που ονομάζεται VNI (VxLAN Network Identifier) και ταυτοποιεί μοναδικά το κάθε VxLAN. Το VNI είναι όμοιο με το VLAN ID, αλλά επειδή έχει 24 bit, δίνει δυνατότητα για ορισμό πολύ περισσότερων VxLANs από ότι τα VLANs.

Τερματικές συσκευές (Endpoints) που βρίσκονται μέσα στο ίδιο ιδεατό δίκτυο VxLAN μπορούν να επικοινωνούν μεταξύ τους απ' ευθείας, ενώ τερματικές συσκευές σε διαφορετικά VxLANs χρειάζονται μία διάταξη router για την δια-VxLAN (inter-VNI) δρομολόγηση.

Το VxLAN προσθέτει 50 έως 54 bytes στην επικεφαλίδα των ακολουθιών Ethernet. Για τον λόγο αυτό θα πρέπει να προσαρμόζεται το MTU (Maximum Transmission Unit) των φυσικών θυρών του υποκείμενου δικτύου που μετέχει στην μεταφορά των συνδέσεων VxLAN.

Μέθοδοι εφαρμογής του VxLAN

Σήμερα είναι διαδεδομένοι οι εξής τρόποι εφαρμογής του πρωτοκόλλου VxLAN στα δίκτυα:

- EVPN-VxLAN - Στην περίπτωση αυτή στις συσκευές δικτύωσης εφαρμόζεται το πρωτόκολλο Ethernet VPN (EVPN) το οποίο λειτουργεί ως ελεγκτής (control plane) στο δίκτυο και δίνει την δυνατότητα να τοποθετηθούν διακομιστές (physical servers και VMs) παντού στο δίκτυο και να μπορούν αυτοί να επικοινωνούν με το υπερκείμενο Layer-2 δίκτυο. Στο δίκτυο αυτό το VxLAN δημιουργεί την λεωφόρο των data (data plane).
- OVSDB-VxLAN - Σε περιβάλλοντα όπου υπάρχουν ελεγκτές SDN (Software Defined Network controllers) όπως πχ VMware NSX, Juniper Networks Contrail, κ.α. χρησιμοποιείται το πρωτόκολλο διαχείρισης OVSDB (Open vSwitch Database) για την επικοινωνία και συνεννόηση μεταξύ των ελεγκτών και για να γίνεται η δρομολόγηση των ακολουθιών VxLAN μεταξύ των VTEPs που έχουν την ικανότητα αυτή και γνωρίζουν την OVSDB.
- Χειροκίνητο VxLAN - Στην περίπτωση αυτή ο εξοπλισμός δικτύου λειτουργεί μόνο ως διακομιστικό μέσο μεταφοράς (transit device) προς άλλες συσκευές που λειτουργούν ως VTEP. Στο περιβάλλον αυτό δεν χρησιμοποιούνται ελεγκτές SDN (Software Defined Network controllers).

Παρουσίαση πρωτοκόλλου EVPN

Το EVPN σημαίνει "Ethernet VPN", ή "Virtual Private Networking στο Ethernet". Αποτελείται από ανοικτές προδιαγραφές που περιγράφουν πως μία ή περισσότερες συσκευές δικτύωσης όπως switches, routers, gateways κλπ μπορούν να υποστηρίξουν έναν μεγάλο αριθμό VPNs (Virtual Private Networks) ως υπερκείμενες οντότητες επάνω στο υποκείμενο δίκτυο που απαρτίζεται από τον εξοπλισμό που διασυνδέει τις γραμμές μεταξύ των συσκευών δικτύωσης.

Με την τεχνολογία Ethernet VPN (EVPN) μπορεί να διασυνδεθεί ένας αριθμός γεωγραφικά σκόρπιων δικτύων δημιουργώντας ιδεατές Layer-2 γέφυρες (multipoint virtual bridges) μεταξύ των. Με το VxLAN "απλώνεται" η Layer-2 συνδεσιμότητα σε όλα τα σημεία μίας επιχείρησης μέσω ενός Layer-3 δικτύου όπως IP ή IP/MPLS, και με αυτό τον τρόπο διασφαλίζεται ότι η τμηματοποίηση (όπως συνέβαινε και στα VLANs) έχει απλωθεί και είναι πλέον ενιαία σε όλο το LAN και WAN δίκτυο, δίχως ποσοτικούς και γεωγραφικούς περιορισμούς και ότι η υποδομή αυτή είναι ενιαία διαχειρίσιμη.

Το VxLAN, όντας μόνο ένα πρωτόκολλο για τον εγκιβωτισμό των frames και την δημιουργία των tunnels δεν αλλάζει την συμπεριφορά του πρωτοκόλλου Ethernet για την εκμάθηση της διαθεσιμότητας των συσκευών στο δίκτυο δια μέσω του παραδοσιακού πλημμυρισμού του data plane με τις πληροφορίες αυτές, διαδικασία η οποία όμως δεν είναι και τόσο αποδοτική.

Το EVPN, που είναι το πρωτόκολλο που ελέγχει το VxLAN διορθώνει την συμπεριφορά αυτή εφαρμόζοντας το πρωτόκολλο MP-BGP (Multiprotocol BGP) για την διανομή των Layer-2 MAC διευθύνσεων και των Layer-3 IP διευθύνσεων στο control plane. Εκεί οι MAC διευθύνσεις ερμηνεύονται ως δρομολόγια. Επίσης, τα VTEPs έχουν την δυνατότητα να ανταλλάσσουν μεταξύ τους τις πληροφορίες διαθεσιμότητας για τις τερματικές συσκευές που εμπεριέχουν / εκπροσωπούν.

Η ταυτόχρονη διαθεσιμότητα των διευθύνσεων MAC και IP κατά την λήψη αποφάσεων για την δρομολόγηση των πακέτων δίνει στο EVPN την δυνατότητα - σε συνδυασμό με το VxLAN - να βελτιστοποιεί τις λειτουργίες routing και switching.

Περαιτέρω πλεονεκτήματα του EVPN μεταξύ άλλων είναι:

- Διαχειρίζεται την συνδεσιμότητα στο Layer-2 εφαρμόζοντας εγκιβωτισμό VxLAN άροντας ποσοτικούς και λειτουργικούς περιορισμούς που υπήρχαν δίχως αυτό
- Απαλλάσσει από τις αδυναμίες του πρωτοκόλλου STP (Spanning Tree Protocol STP) εφαρμόζοντας πιο ισχυρά πρωτόκολλα δρομολογήσεων για την διαδικτύωση
- Η λειτουργία EVPN με VxLAN δεν απαιτεί την υποχρεωτική ύπαρξη κάποιου ελεγκτή SDN (Software Defined Network controller) στο δίκτυο
- Κάθε VPN μπορεί να έχει χαρακτηριστικά Layer-2 ή και Layer-3 και να λειτουργεί τελείως ανεξάρτητα από τα άλλα VPNs με τα οποία συγκατοικεί μέσα στον ίδιο εξοπλισμό
- Τα EVPNs μπορούν να λειτουργήσουν τόσο επάνω σε δίκτυα MPLS (παροχικά και ιδιωτικά) όσο και επάνω σε κανονικά IP δίκτυα δίχως να υπάρχει MPLS. Έτσι τα EVPNs μπορούν να λειτουργήσουν τόσο εντός ενός Data Center ή σε περιβάλλον Campus/Branch όσο και σε περιβάλλον WAN για την διαδικτύωση όλων αυτών μεταξύ τους.

Γιατί έχει το EVPN τόσο μεγάλη σημασία;

- **Δεν χρειάζεται πλέον δίκτυο MPLS (ούτε MPLS license)**

Η διαδικτύωση των Data Centers μεταξύ τους για συνδεσιμότητα multipoint to multipoint Layer-3 και Layer-2 απαιτούσε παραδοσιακά την χρήση δικτύων βάσει MPLS που επέφερε αντίστοιχη οικονομική επιβάρυνση. Το EVPN λύνει το πρόβλημα αυτό εφαρμόζοντας το VxLAN.

Με το EVPN - VxLAN δημιουργούνται απομονωμένα, κατανεμημένα και προστατευμένα Layer-2 και Layer-3 δίκτυα και δίνεται συνδεσιμότητα μέσω αυτών εφαρμόζοντας απλές, δοκιμασμένες, ανθεκτικές και επεκτάσιμες αρχιτεκτονικές δικτύωσης όπως fabric, leaf-and-spine, κλπ.

Σε οικονομικό επίπεδο η αφαίρεση της απαίτησης για MPLS δίνει σημαντική οικονομική ωφέλεια και σε επίπεδο δια βίου λειτουργικών δαπανών OPEX αλλά και σε επίπεδο CAPEX λόγω οικονομικότερων εναλλακτικών για εξοπλισμό και licenses.

- **Μειωμένη πολυπλοκότητα λόγω ενιαίου πρωτοκόλλου**

Το EVPN υποστηρίζει όλους τους τύπους VPN σε Layer-2 (Ethernet) και σε Layer-3 (IPv4 και IPv6) και μάλιστα για μεγάλο πλήθος σημείων, δικτύων και εξοπλισμών. Έτσι, είναι μία ιδανική λύση για τις επιχειρησιακές ανάγκες, οι οποίες μπορούν να καλύπτουν όλο το εύρος όπως πχ διασύνδεση πλατφορμών εφαρμογών, διασύνδεση μεταξύ Data Centers, (δια)δικτύωση των Campus/Branch, κλπ.

Όλες οι παραπάνω ανάγκες ικανοποιούνται πλέον μόνο με ένα σετ πρωτοκόλλων και έτσι μειώνεται δραστικά η πολυπλοκότητα της υποδομής δικτύων με αντίστοιχα οφέλη από μειωμένη ανάγκη εκπαιδεύσεων, PoC's, τυποποίηση διαδικασιών εγκατάστασης & συντήρησης αυξάνοντας αντίστοιχα και την διαθεσιμότητα του δικτύου και τον βαθμό ανταπόκρισης σε απαιτήσεις προσαρμογών.

- **Καλύτερη αξιοποίηση πόρων**

Το πρωτόκολλο EVPN περιλαμβάνει πρόνοιες

για αποτελεσματική μεταχείριση κίνησης Broadcast, Unknown Unicast and Multicast (BUM traffic) και μπορεί επίσης να συμπιέσει το πρωτόκολλο ARP (Address Resolution Protocol). Έτσι αξιοποιείται καλύτερα η χωρητικότητα του δικτύου ενώ ταυτόχρονα μειώνεται και ο άχρηστος "θόρυβος δικτύου" που κατά τα άλλα λειτουργεί επιβαρυντικά στην απόδοση, αποπροσανατολίζει στις διαγνωστικές εργασίες και τελικά μειώνει την διαθεσιμότητα των υπηρεσιών.

Επιπλέον, το EVPN μπορεί να αξιοποιήσει πολλαπλές ισάξιες διαδρομές μεταξύ δύο σημείων (multiple available equal paths), συνήθη πρακτική σε αρχιτεκτονικές διαδικτύωσης μεταξύ σύγχρονων Data Centers. Αυτό σημαίνει ότι στα σύγχρονα πλέγματα δικτύων (network fabrics) δεν χρειάζεται να υπάρχουν λογικές, πρωτόκολλα και διατάξεις παρεμπόδισης σχηματισμού βρόγχων, που αχρήστευαν μέχρι τώρα μέρος της εγκατεστημένης χωρητικότητας των γραμμών δικτύου.

- **Προωθημένο Multi-Homing για βελτίωση της διαθεσιμότητας υπηρεσιών**

Σε πολλές περιπτώσεις υπάρχει η ανάγκη συσκευές όπως servers, non-EVPN switches, routers και άλλες διατάξεις να συνδεθούν στο δίκτυο μέσω περισσότερων της μίας γραμμής. Αυτό μπορεί να συμβαίνει για λόγους όπως η ανάγκη για επαύξηση χωρητικότητας, ανάγκη για εφεδρικές συνδέσεις ή και τα δύο.

Ο σχεδιασμός του EVPN εμπεριέχει βελτιώσεις που δίνουν ευελιξία στις συνδέσεις πολλαπλών γραμμών, μεταξύ αυτών και για αυξημένη ταχύτητα αποκατάστασης συνδέσεων. Το EVPN δίνει επίσης δυνατότητα προώθησης κίνησης και εφεδρείας με χρήση πολλαπλών γραμμών (multipath forwarding and redundancy) μέσω του μοντέλου All-active Multi-Homing, γεγονός που απαλλάσσει από τα πρωτόκολλα Multi-chassis LAG (MC-LAG). Αξιοποιώντας όλα αυτά, οι τερματικές συσκευές μπορούν να συνδεθούν ταυτόχρονα σε δύο ή περισσότερες γραμμές και να λάβουν/δώσουν κίνηση αξιοποιώντας όλες τις γραμμές που αλληλοκαλύπτονται μεταξύ τους με αποτέλεσμα να επιτυγχάνεται μία καλύτερη εκμετάλλευση των πόρων του δικτύου.

Εξελιγμένα Campus / Branch με τεχνολογία EVPN-VxLAN

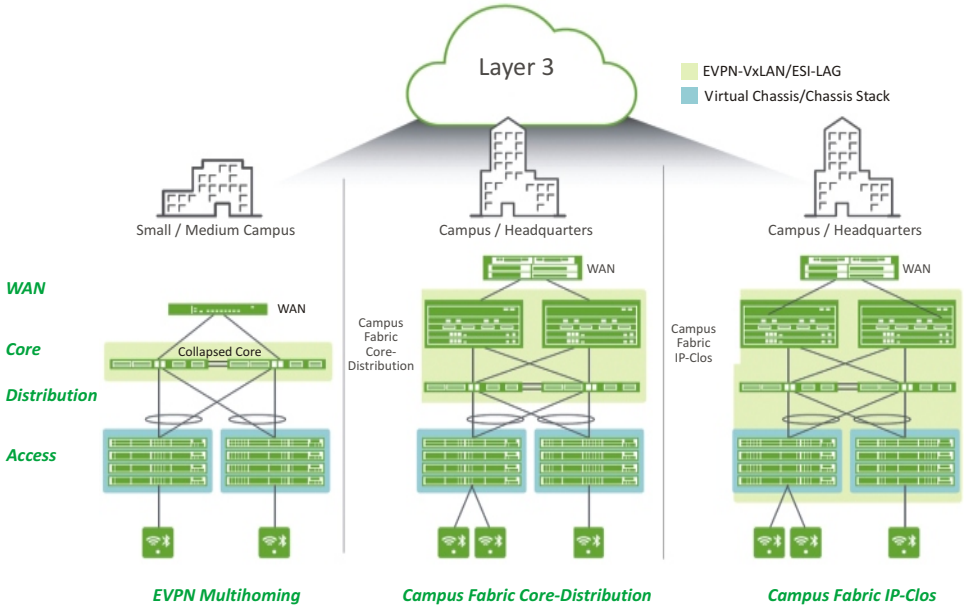
Ως πρώτο πεδίο εφαρμογής του EVPN-VxLAN θα εξετασθεί η περιοχή των Campus & Branch.

Οι εφαρμογές που εγκαθιστούν και λειτουργούν οι επιχειρήσεις σε όλα τους τα σημεία παρουσίας ως επίσης και στο cloud είναι πολλές και διαφορετικές και συνήθως χρειάζεται να επικοινωνούν μεταξύ τους. Οι εφαρμογές αυτές χρησιμοποιούν πλήθος προγραμμάτων και πληροφοριών που μπορεί να μην βρίσκονται όλα στο ίδιο σημείο. Παραδείγματα τέτοιων εφαρμογών είναι εφαρμογές κατηγορίας SaaS (πχ. Office-365, box, κλπ), unified communications (UC), video, IoT που συνήθως χρειάζονται συνδέσεις Layer-2 ως επίσης και άλλες εφαρμογές που πολλές φορές είναι υπερευαίσθητες σε καθυστέρηση σήματος (latency).

Παραδοσιακά αυτή η ανάγκη καλύπτεται εκτείνοντας τα VLANs από σημείο σε σημείο και εφαρμόζοντας την διαδικασία εκμάθησης των συνδεόμενων μέσω πλημμυρισμού στο data plane, διαδικασία σπάταλη, ανεπαρκή και δύσχρηστη σε όλο τον κύκλο ζωής του δικτύου (παραμετροποίηση, επεκτάσεις, τροποποιήσεις).

Επιπλέον, η ασφάλεια η οποία δεν είναι πλέον απλά μία υπόθεση που αφορά μόνο στην όποια περίμετρο, αποτελεί το νέο ζητούμενο. Το σύγχρονο σκεπτικό απαιτεί η ασφάλεια να είναι ενσωματωμένη εξ αρχής στις αρχιτεκτονικές των δικτύων - όχι μόνο μέσα στο campus ή στο branch - αλλά να ισχύει με ενιαίο τρόπο σε όλο το δίκτυο, περιλαμβανομένου και του Data Center, και μάλιστα να μπορεί να εξειδικεύεται ανά τομέα.

Στο περιβάλλον Campus/Branch το EVPN-VxLAN διαχωρίζει τις υπερκείμενες διατάξεις από τις υποκείμενες υποδομές εφαρμόζοντας



Εικόνα 5. Αρχιτεκτονικές EVPN-VxLAN σε Campus / Branch

τα πρωτόκολλα VxLAN και EVPN. Ο διαχωρισμός αυτός δίνει την δυνατότητα να αναπτυχθούν εντός του ίδιου δικτύου και επάνω στις ίδιες υποκείμενες υποδομές (εξοπλισμοί) διαφορετικά και ανεξάρτητα μεταξύ τους λογικά Layer-2 VPN και Layer-3 VPN δίκτυα.

Οι αρχιτεκτονικές που εφαρμόζονται συνήθως στα δίκτυα Campus / Branch εμφανίζονται στην εικόνα 5 και είναι οι εξής:

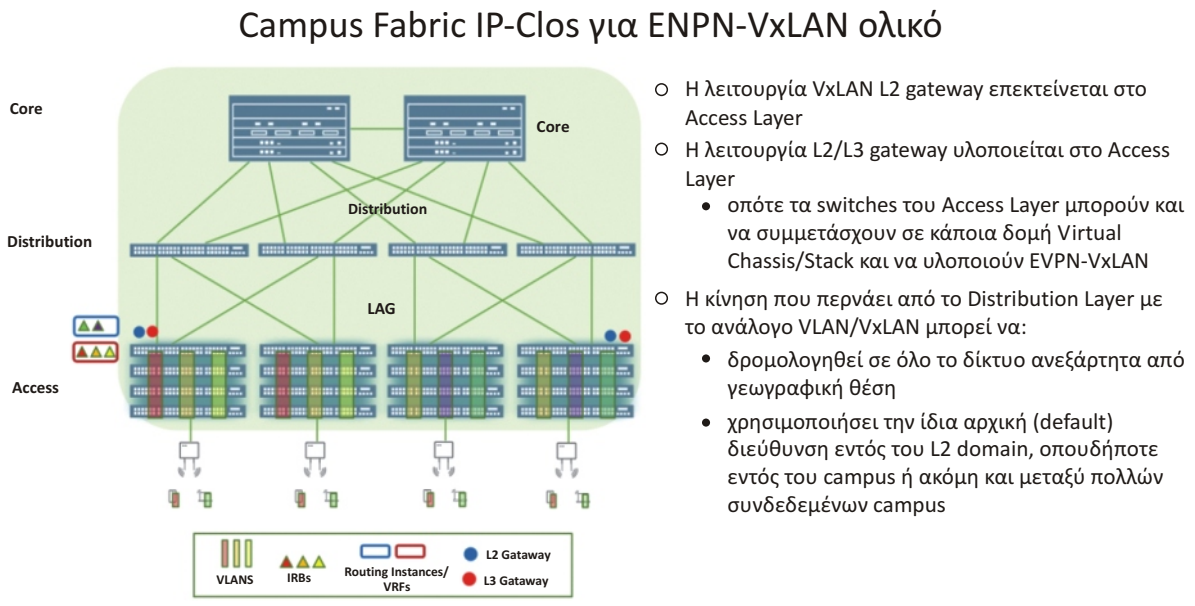
Α. EVPN Multihoming. Βρίσκει εφαρμογή σε μικρά ή μεσαία δίκτυα campus και γι'αυτό ονομάζεται συχνά ως EVPN Collapsed Core. Σε αυτό το σενάριο υπάρχουν μερικά αυτόνομα switches στο επίπεδο Access, που μπορεί να αποτελούν και κάποιο virtual chassis/stack και πιο πάνω βρίσκεται το Collapsed Core. Αυτός ο σχεδιασμός μπορεί εφαρμοστεί σε ένα σχετικά μικρό δίκτυο που καλύπτει λίγα κτίρια ή λίγους ορόφους μέχρι ένα άνω όριο τους λίγους χιλιάδες χρήστες.

Β. Campus Fabric Core-Distribution. Εφαρμόζεται σε δίκτυα με μεγάλο πλήθος χρηστών μέχρι 5.000-10.000 χρήστες όπως πχ σε πανεπιστημιουπόλεις ή σε επιχειρηματικά campuses με πολλά κτίρια. Εδώ το δίκτυο αποτελείται από τρία επίπεδα. Σε αυτό το σενάριο το EVPN-VxLAN εκτελείται μεταξύ των Core και Distribution επιπέδων. Το επίπεδο πρόσβασης (Access) μπορεί να αποτελείται από αυτόνομα switches ή μπορεί να λειτουργεί ως virtual chassis/stack.

Γ. Campus Fabric IP-CLOS[1]**.** Σε αυτή την αρχιτεκτονική επεκτείνεται το EVPN-VxLAN σε όλα τα switches, δηλ. και στο επίπεδο πρόσβασης. Σε αυτό το σενάριο τα VLANs, τα IRBs (Integrated Routing and Bridging ή αλλιώς vlan interface), καθώς και οι λειτουργίες Layer-2 και Layer-3 gateways, επεκτείνονται σε όλα τα switches του επιπέδου πρόσβασης. Αυτή η δομή εισαγάγει επίσης και μια πολύ σημαντική λειτουργικότητα, την μικρο-τμηματοποίηση με τη βοήθεια της τεχνολογίας GBP (Group Based Policies), στην οποία έγινε αναφορά πιο πάνω.

Έτσι, η αρχιτεκτονική IP Clos fabric επεκτείνει το EVPN μέχρι το επίπεδο πρόσβασης πετυχαίνοντας end-to-end EVPN-VxLAN. Σε αυτή την περίπτωση τα IRBs, η λειτουργία αντιστοίχισης VLAN με VxLAN (Layer-2 Gate-way) ως επίσης και οι λειτουργίες δρομολόγησης (Layer-3

1. Η Αρχιτεκτονική Clos/Clos Network εφευρέθηκε το 1938 από τον Edson Erwin και το 1952 ο Charles Clos το προσάρμοσε για την επικοινωνία μεταξύ των τηλεφωνικών κέντρων. Ο Charles Clos δημοσίευσε την μελέτη "A Study of Non-blocking Switching Networks" στο Bell System Technical Journal το έτος 1953.



Εικόνα 6. Δίκτυο Campus fabric IP-Clos για EVPN-VxLAN από άκρο σε άκρο

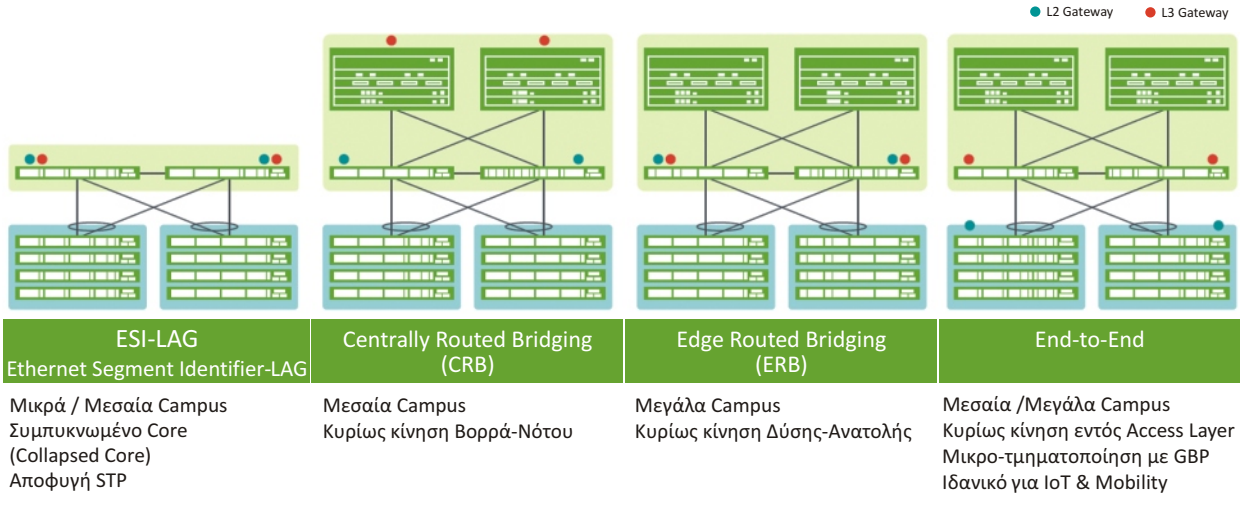
Gateway) υλοποιούνται όλα στα switches του επιπέδου πρόσβασης εικόνα 6.

Οι τρεις αρχιτεκτονικές EVPN-VxLAN που παρουσιάστηκαν πιο πάνω μπορούν να εφαρμοστούν με τους κάτωθι τέσσερεις τρόπους που απεικονίζονται συνοπτικά στην εικόνα 7 και είναι κατάλληλες να βοηθήσουν στην επίτευξη των πλεονεκτημάτων από την εφαρμογή αυτών των νέων πρωτοκόλλων:

1. EVPN Multihoming για τα μικρότερα campus. Τα πλεονεκτήματά του είναι ότι εξαλείφει το πρωτόκολλο STP (spanning tree) και ανοίγει την προοπτική για αναβάθμιση των πρωτοκόλλων Virtual Chassis/Stack και MC-LAG με το νέο ESI-LAG (Ethernet Segment Identifier - Link Aggregation Groups).

2. Centrally Routed Bridging (CRB), είναι κατάλληλο για περιβάλλοντα με πιο πολύ κάθετη κίνηση κατηγορίας Βορρά-Νότου στο δίκτυο. Σε αυτό το σενάριο η λειτουργία Layer-3 routing (για την δρομολόγηση από και προς το WAN) όπως και τα IRBs βρίσκονται στο Core επίπεδο και ταυτόχρονα το EVPN εκτείνεται μεταξύ των επιπέδων Core και Distribution.

3. Edge Routed Bridging (ERB), που είναι πολύ συνηθισμένο σε μεγάλα campuses με 5.000 - 10.000 χρήστες με πολλά κτίρια και πολλή κίνηση εντός του campus. Στις περιπτώσεις αυ-



Εικόνα 7. Αρχιτεκτονικές Fabrics με EVPN-VxLAN

τές υπερτερεί η κίνηση μεταξύ των κτιρίων και των τμημάτων, δηλαδή η οριζόντια κίνηση κατηγορίας Δύση προς Ανατολή. Για αυτόν τον λόγο η λειτουργία δρομολόγησης (L3 routing gateway) τοποθετείται και διεκπεραιώνεται στο Distribution Layer.

4. **To Campus Fabric IP-Clos** όπου επεκτείνεται η λειτουργία Layer-3 μέχρι τα switches στο επίπεδο Access.

Εφαρμόζοντας έναν από τους παραπάνω τρόπους για την υλοποίηση των EVPN-VxLAN fabric και αναπτύσσοντας ένα Layer-2 VPN ή ένα Layer-3 VPN που επίσης περιλαμβάνεται στο πρωτόκολλο EVPN, τα πλεονεκτήματα της τεχνολογίας αυτής μπορούν να εξαπλωθούν στα Campus και Branch, στα Data Centers ακόμη και στις υποδομές cloud.

Το EVPN - ως control plane πρωτόκολλο - προσφέρει σε περιβάλλον Campus/Branch τα κάτωθι ειδικότερα χαρακτηριστικά:

- **Μεγαλύτερη αποτελεσματικότητα με:**
  - Μείωση πλημμυρισμού από το πρωτόκολλο ARP (Address Resolution Protocol) μέσω ζεύξης MAC-με-IP στο control plane
  - Υποστήριξη κίνησης multipath μέσω πολλαπλών switches στο core επίπεδο (VxLAN entropy)
  - Υποστήριξη κίνησης multipath προς switches του επιπέδου πρόσβασης (access) σε διάταξη active/active με διπλές γραμμές (dual-homed) προς το επίπεδο διανομής (distribution).
- **Αποτελεσματική σύγκλιση και επαναφορά με:**
  - Ταχεία επανασύνδεση όταν υπάρξει δυσλειτουργία σε μία από τις διπλές γραμμές κάποιου dual-homed switch στο επίπεδο πρόσβασης (λειτουργία aliasing)
  - Υποστήριξη ταχείας επανασύνδεσης για τερματικά εν κινήσει.
- **Μεγέθυνση:**
  - Απροβλημάτιστη επέκταση και μεγέθυνση υποδομών και στα τρία επίπεδα του δικτύου core, distribution/aggregation και access.
- **Ευελιξία:**
  - Εύκολη ανάπτυξη & προσαρμογές δικτύου με Layer-3 VPN και Layer-2 VPNs
  - Εργαλεία εφαρμογής και ελέγχου πολιτικών σε βάθος και λεπτομέρεια.
- **Τεχνολογική ουδετερότητα:**
  - Δεν περιλαμβάνει και δεν υλοποιεί ιδιωτικές προδιαγραφές, ανοίγοντας έτσι τον δρόμο σε ευελιξία επιλογής εξοπλισμού και κατασκευαστών.

DataCenter Interconnect (DCI) με EVPN-VxLAN

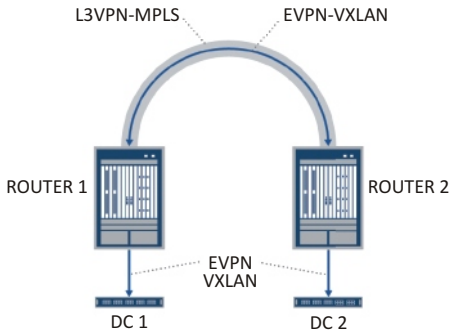
Στη συνέχεια θα εξετασθεί η εφαρμογή του πρωτοκόλλου EVPN-VxLAN σε ένα περιβάλλον ζεύξης Data Centers μεταξύ τους (DCI:Data Center Interconnect).

Αυτό το πεδίο εφαρμογής εξυπηρετεί την ανάγκη να απλωθεί η επικοινωνία στο Layer-2 επίπεδο σε πολλά Data Centers με ενιαίο τρόπο έτσι ώστε να βελτιωθεί η απόδοση των εφαρμογών προς τους χρήστες ως επίσης και τις ανάγκες σύνδεσης με εφεδρικά Data Centers για αποκατάσταση από καταστροφές (disaster recovery).

Αν και είναι διαθέσιμες διάφορες τεχνολογίες για την διασύνδεση των Data Centers μεταξύ τους, η τεχνολογία EVPN έχει πλεονεκτήματα ειδικά έναντι του συνήθως χρησιμοποιούμενου MPLS όπως πχ εφεδρεία active/active, ταχεία επανασύνδεση σε περίπτωση δυσλειτουργιών (aliasing), αποφυγή πλημμύρας διευθύνσεων MAC. Για την υλοποίηση λειτουργίας DCI, το VxLAN συνδυάζεται με το EVPN.

Ανάλογα με την υπόλοιπη υποδομή και τις γραμμές σύνδεσης, υπάρχουν 3 εναλλακτικά σχέδια για την υλοποίηση DCI με χρήση του πρωτοκόλλου EVPN-VxLAN:

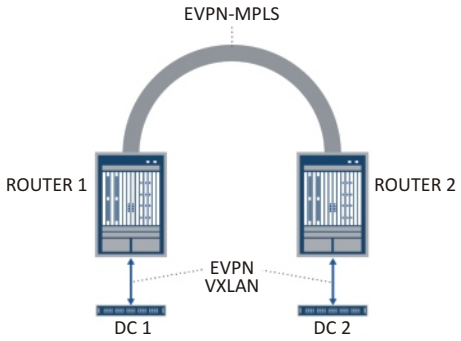
- Η περίπτωση που τα Data Centers είναι ήδη συνδεδεμένα μεταξύ τους με γραμμή Layer-3 MPLS που τερματίζει στις δύο πλευρές σε



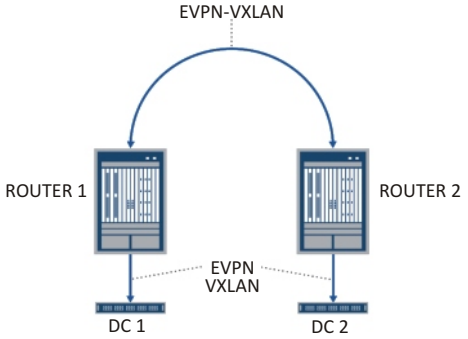
Εικόνα 8. DCI Λύση-1: Layer-3 VPN-MPLS

Router, τότε το VxLAN tunnel μεταξύ του DC1 και του DC2 ξεκινάει και τερματίζει στα αντίστοιχα switches στις δύο πλευρές. Αυτή η εναλλακτική δεν επηρεάζει το WAN καθόλου (εικόνα 8).

- Η περίπτωση που βασίζεται στην υπόθεση ότι μεταξύ των Data Centers έχει ήδη αναπτυχθεί ένα WAN που τερματίζεται σε Router ή άλλο κατάλληλο Layer-3 εξοπλισμό που εφαρμόζουν μεταξύ τους πρωτόκολλο EVPN-MPLS. Αυτή η λύση χρησιμοποιεί το EVPN ως control plane και το MPLS ως data plane και απαιτεί να γίνουν αλλαγές στο WAN. Επίσης, πρέπει να γίνει επέμβαση στην αρχιτεκτονική του LAN έτσι ώστε το EVPN να υποστηρίζεται ενδογενώς. Σε αυτήν την περίπτωση θα χρειαστεί να γίνουν προσαρμογές μεταξύ των routers και των switches στα DC1 και DC2 έτσι ώστε να λειτουργήσει το tunnel EVPN-VxLAN (εικόνα 9).
- Τα σημεία ενδιαφέροντος μπορούν να ζευχθούν μεταξύ τους επίσης μόνο με κανονικές γραμμές Internet. Η υλοποίηση αυτή δεν



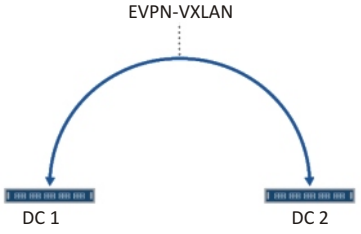
Εικόνα 9. DCI Λύση-2: EVPN-MPLS



Εικόνα 10. DCI Λύση-3: EVPN-VxLAN μέσα από το Internet

απαιτεί ούτε κάποιο WAN ούτε και MPLS. Η υλοποίηση χρησιμοποιεί το Internet ή ένα IP tunnel, όπου το VxLAN ταξιδεύει επάνω στο IP και το πρωτόκολλο EVPN εφαρμόζεται καθολικά (εικόνα 10).

- Αν δεν υπάρχει router στα σημεία, τότε τα Data Centers μπορούν απλά να συνδεθούν απ' ευθείας μεταξύ τους, και το EVPN θα χρησιμοποιηθεί καθολικά σε όλο το δίκτυο. Ούτε αυτή η υλοποίηση απαιτεί κάποιο WAN ή MPLS, αλλά η σύνδεση μεταξύ των σημείων θα πρέπει να γίνει με κάποιο αδόμητο μέσο, πχ με dark fiber (εικόνα 11).



Εικόνα 11. DCI Option: Layer-3 VPN-MPLS Direct Connection

Από πού μπορεί να γίνει η αρχή;

Ανάλογα με την επιχειρησιακή ετοιμότητα και τις ανάγκες των έργων, μπορεί να εισαχθεί μια λύση δικτύωσης που βασίζεται σε τεχνολογία EVPN με διάφορους τρόπους, αρχίζοντας από ένα ζευγάρι συσκευών έως και ένα πλήρες leaf & spine datacenter switching fabric.

Στην κατηγορία μικρότερων υλοποιήσεων υπάρχει η επιλογή να τοποθετηθούν 2 έως 4 συσκευές με δυνατότητα EVPN που διασυνδέ-

ονται μεταξύ τους για να σχηματίσουν μια τοπολογία δακτυλίου. Στην περίπτωση αυτή η «νησίδα» EVPN που δημιουργείται μπορεί να λειτουργήσει ως “core" που θα παρέχει συνδεσιμότητα Layer-2 ή/και Layer-3 μεταξύ των θυρών του.

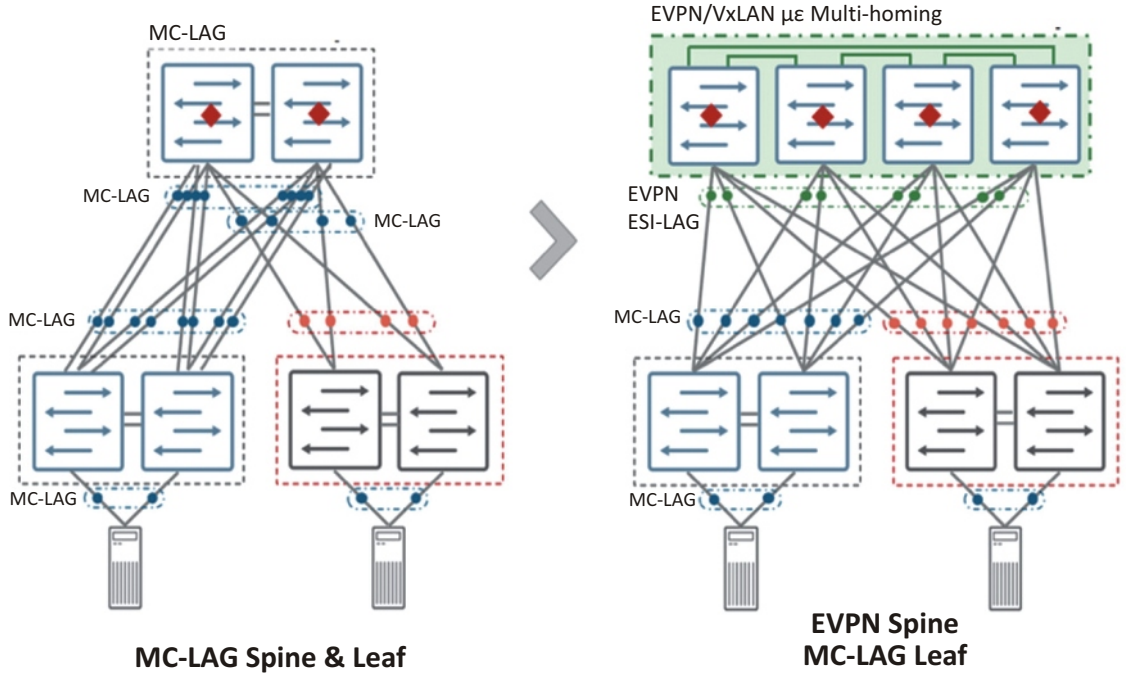
Στα πλαίσια μία διαδικασίας μετάβασης, αυτό το νέο "core" θα κατασκευαζόταν δίπλα σε ένα υπάρχον two-tier fabric στο Data Center, που είτε απαιτεί διευρυμένη χωρητικότητα είτε μεγαλύτερη ευελιξία είτε και τα δύο. Στη συνέχεια, οι παλιοί συνδεόμενοι κόμβοι (leafs) μετεγκαθίστανται από την παλιά τοπολογία δικτύου στο EVPN, όπως φαίνεται στην εικόνα 12.

Αυτή η προσέγγιση επιτρέπει τη σταδιακή εισαγωγή της τεχνολογίας EVPN σε μια υπάρχουσα υποδομή, δίνοντας την ευκαιρία να δημιουργηθούν σταδιακά οι απαραίτητες δεξιότητες και εμπειρία.

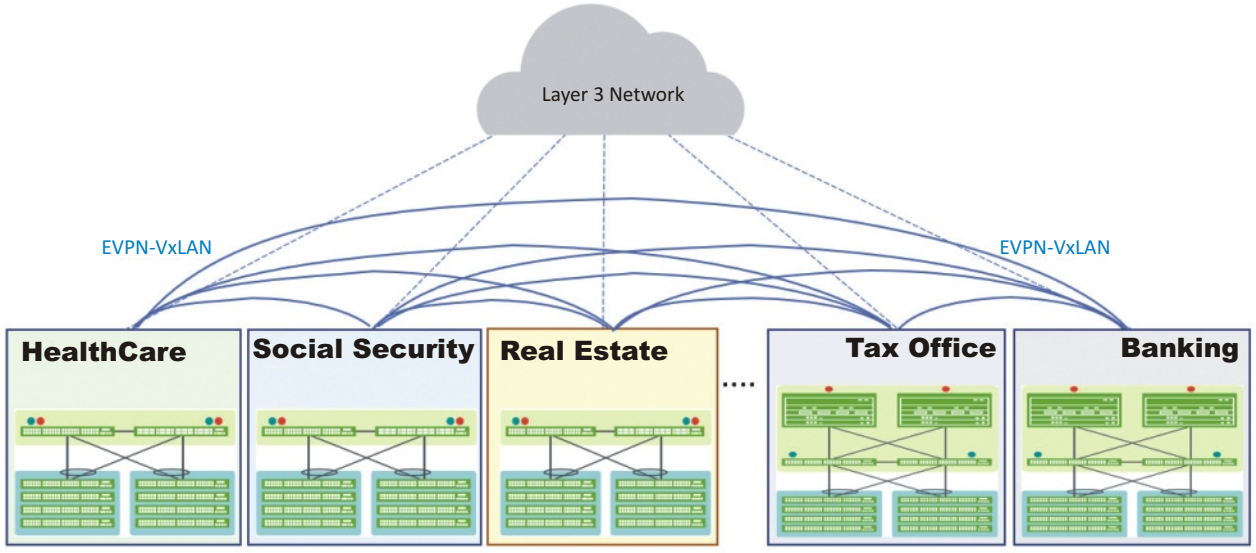
Συμπέρασμα

Η εξέλιξη των δυνατοτήτων της IT υποδομής μίας οργάνωσης για την υποστήριξη τέτοιων ευέλικτων δικτύων και λειτουργιών δεν πραγματοποιείται εν μία νυκτί. Σημαντικό μέρος της μετεξέλιξης είναι η προσαρμογή των υποδομών στις νέες τεχνολογίες και η εφαρμογή λύσεων Virtualization και στο δίκτυο, το οποίο βασίζεται το EVPN με όλα τα πλεονεκτήματα που μπορεί να δώσουν.

Το Ethernet VPN είναι μια τυποποιημένη λύση υψηλών προδιαγραφών που επιτρέπει την κατασκευή νέων fabrics που δεν βασίζονται σε ιδιωτικά (proprieatary) πρωτόκολλα. Έτσι, πρακτικά καθίσταται δυνατή η ανάπτυξη δικτύων υψηλών προδιαγραφών με εξοπλισμό από διαφορετικούς κατασκευαστές, επιτρέποντας στις επιχειρήσεις να εξελίσσονται χωρίς να εγκλωβίζονται στους υπάρχοντες προμηθευτές δικτυακών συσκευών. Μία τέτοια υλοποίηση θα πρέπει να προσφέρει έναν αποτελεσματικό και επεκτάσιμο τρόπο για την κατασκευή και τη διασύνδεση όλων των σημείων παρουσίας της επιχείρησης, των Data Centers ακόμη και των cloud υποδομών που χρησιμοποιεί, βοηθώντας έτσι να αξιοποιηθούν πλήρως οι δυνατότητες της τεχνολογίας EVPN-VxLAN, παρέχοντας βελτιστοποιημένη, απρόσκοπτη και τεχνολογικά αδέσμευτη καθολική συνδεσιμότητα Layer-2 ή και Layer-3.



Εικόνα 12. Μετάβαση από MC-LAG σε EVPN (collapsed core)



Εικόνα 13. Διασυνδεδεμένα Data Centers με ενδογενή Διαλειτουργικότητα με EVPN-VxLAN

Περίπτωση εφαρμογής EVPN-VxLAN: Διαλειτουργικότητα

Το EVPN-VxLAN διευκολύνει την ευέλικτη επικοινωνία - σε οριζόντιο επίπεδο - μεταξύ εφαρμογών που στεγάζονται σε διαφορετικά Data Centers, που κατά τα άλλα δεν επικοινωνούν εύκολα με γρήγορο, οικονομικό και ασφαλή τρόπο.

Στην εικόνα 13 απεικονίζεται η εφαρμογή EVPN-VxLAN σε μία υποθετική περίπτωση όπου διάφοροι φορείς όπως πχ ταμεία υγείας, συνταξιοδοτικοί φορείς, κτηματολόγια, κλπ θέλουν να γίνουν πιο φιλικοί προς τους χρήστες, μη απαιτώντας πλέον την φυσική παρουσία των συναλλασσομένων αλλά ανοίγοντας τα συστήματά τους στους χρήστες μέσω εύκολης πρόσβασης από το internet. Το κύριο εμπόδιο εδώ είναι η ασφαλής πιστοποίηση της ταυτότητας των συναλλασσομένων με αυτοματοποιημένο τρόπο. Το κενό αυτό μπορεί να καλυφθεί από άλλους έμπιστους φορείς που ήδη έχουν στα Data Centers τους ικανά συστήματα πιστοποίησης ταυτότητας (όπως πχ το σύστημα της εφορίας) ή ακόμη συστήματα ισχυρής πιστοποίησης (όπως πχ τα Data Centers των τραπεζικών ιδρυμάτων). Η εφαρμογή EVPN-VxLAN έρχεται να προσφέρει εδώ αμεσότητα, ταχύτητα και ασφάλεια στην απευθείας επικοινωνία μεταξύ των Data Centers λήπτη και δότη πληροφοριών ταυτοποίησης, μειώνοντας αφενός το φορτίο bandwidth και αφετέρου αποφεύγοντας πρόσθετες διατάξεις, που κατά τα άλλα θα απαιτούνταν (όπως πχ πρόσθετοι routers/switches/security & VPN gateways για MPLS/IPSec/SSL/TLS κλπ) και άρα εξοικονομώντας όχι μόνο κόστος κατασκευής, λειτουργίας και επικοινωνίας αλλά κερδίζοντας και χρόνο ανάπτυξης και ευελιξία απόκτησης λόγω τυποποιημένων προδιαγραφών των συστημάτων. Έτσι, και όσο εκσυγχρονίζονται τα συστήματα που επικοινωνούν, θα μπορούσαν να εξοικονομηθούν «Κέντρα Διαλειτουργικότητας[2]» που κατασκευάζονται ιστορικά με αποκλειστικό ρόλο την διασύνδεση παλιών δομών.

Εν κατακλείδι

- Το EVPN αν και ξεκίνησε ως τεχνικά ουδέτερη λύση για ορισμένες περιπτώσεις, έχει

2. https://www.gsis.gr/dimosia-dioikisi/ked

πλέον αναπτυχθεί από αρκετούς κατασκευαστές με ανοιχτές προδιαγραφές για την αντιμετώπιση σύνθετων απαιτήσεων, προσφέροντας πιο αποτελεσματικούς τρόπους από ότι οι παραδοσιακές τεχνολογίες.

- Το EVPN για DCI (Data Center Interconnect) προσφέρει τη δυνατότητα εξάπλωσης σε πολλαπλά domains, προσφέροντας ταυτόχρονα δυνατότητα επιβολής πολιτικών, ορισμού των συνόρων της εφαρμογής των πολιτικών ασφάλειας και δυνατότητα μείωσης των tunnels, καταργώντας περιορισμούς στην μεγέθυνση του δικτύου.
- Το EVPN αντικαθιστά πολλές τεχνολογίες με μία - προσφέρει multicast χρησιμοποιώντας το ίδιο control plane με το unicast, εξασφαλίζοντας έτσι σημαντική απλοποίηση.
- Το EVPN διαχωρίζει τις υπερκείμενες διατάξεις από τις υποκείμενες υποδομές (VxLAN, IP, MPLS ιδιωτικό ή παροχικό) του δικτύου και καθιστά έτσι τη δικτύωση απρόσκοπτη και ενιαία ανεξάρτητα από την τεχνολογία που χρησιμοποιείται στο underlay.
- Στην περίπτωση που απαιτείται επέκταση του δικτύου, το EVPN βοηθάει απαλλάσσοντάς από συνήθη ζητήματα στο Layer-2, π.χ. απενεργοποιώντας τα traffic broadcasts και αφαιρώντας προβληματικούς δακτυλίους.
- Το EVPN έχει ελεγχθεί για διαλειτουργικότητα με περισσότερους από 10 μεγάλους κατασκευαστές που μπορούν και συνεργάζονται απροβλημάτιστα σε ένα ενιαίο δίκτυο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. *https://tools.ietf.org/html/rfc7209#section-4*
2. *https://www.juniper.net/documentation/en_US/release-independent/solutions/information-products/pathway-pages/lb-evpn-vxlan-tn.pdf*
3. *https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/guide-c07-734107.pdf*
4. *https://www.juniper.net/documentation/us/en/software/junos/evpn-vxlan/topics/concept/evpn-bgp-multihoming-overview.html*
5. *https://www.arubanetworks.com/evpn-vxlan/*
6. *https://www.juniper.net/us/en/products-services/what-is/evpn-vxlan/*

Λίγα λόγια για τον αρθρογράφο

Ο κ. **Σταύρος Καραγκιούλογλου** κατάγεται από την Κωνσταντινούπολη και αποφοίτησε από το Γερμανο-Αυστριακό Κολλέγιο St.Georg. Στη συνέχεια σπούδασε Διπλ. Ηλεκτρολόγος-Μηχανολόγος Μηχανικός με ειδικότητα στα δίκτυα τηλεπικοινωνιών στο Technical University RWTH AACHEN Γερμανίας, όπου πήρε και το μεταπτυχιακό του με εργασία την εφαρμογή real-time τηλεματικής στον έλεγχο οδικής κυκλοφορίας. Είναι παντρεμένος και πατέρας δύο παιδιών. Στην τηλεπικοινωνιακή αγορά έχει εμπειρία 30 χρόνια, εκ των οποίων τα περισσότερα στη SIEMENS - στους τομείς εφαρμογής, πωλήσεων και marketing τηλεπικοινωνιακών προϊόντων και υπηρεσιών, όπου κατείχε καίριες θέσεις, μεταξύ αυτών και τη θέση του Διευθυντή Πωλήσεων Τηλεπικοινωνιακών Συστημάτων, Προϊόντων και Εφαρμογών. Το 2003 ίδρυσε και μετέχει ενεργά ως Διευθύνων Σύμβουλος στην διοίκηση της UNITED TELECOM AE, μία εταιρία που δραστηριοποιείται εντατικά στην παροχή και την ασφάλεια των κινητών, ασύρματων και σταθερών επιχειρησιακών δικτύων υπολογιστών, τηλεφωνίας και πολυμέσων δημόσιας και ιδιωτικής χρήσης καθώς και στην ασφάλεια των ηλεκτρονικών συναλλαγών, των δεδομένων και του Cloud.