



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ**  
**ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ**

**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ  
& ΠΛΗΡΟΦΟΡΙΚΗΣ**

*Διπλωματική Εργασία*  
**«CARRIER GRADE ETHERNET»**

**ΚΑΤΕΡΙΝΑ – ΘΕΩΝΗ Σ. ΣΠΥΡΟΠΟΥΛΟΥ**

**A.M. 3746**

***ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ:***

**Χρήστος Μπούρας**

***ΕΠΙΒΛΕΠΩΝ:***

**Κώστας Στάμος**

**ΠΑΤΡΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2012**



---

Η εργασία αυτή ολοκληρώθηκε, συνυπολογίζοντας την προσωπική προσπάθεια και την σημαντική συμβολή ενός συνόλου ανθρώπων τους οποίους θα ήθελα να ευχαριστήσω.

Κατ' αρχάς, θα ήθελα να ευχαριστήσω θερμά τον κ. Χρήστο Μπούρα, καθηγητή του τμήματος Μηχανικών Η/Υ και Πληροφορικής του Πανεπιστημίου Πατρών, για τη δυνατότητα που μου παρείχε να ασχοληθώ με το συγκεκριμένο πολύ ενδιαφέρον θέμα, αλλά και τη διαρκή επίβλεψή του για την διεκπεραίωση της παρούσας εργασίας.

Ιδιαίτερες ευχαριστίες αξίζουν στο Δρ. Κώστα Στάμο, όχι μόνο για την πολύτιμη βοήθειά του, η οποία υπήρξε καταλυτική για την εκπόνηση αυτής της διπλωματικής εργασίας, αλλά και για την συμπαράστασή του καθ' όλη τη διάρκεια της συνεργασίας μας.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου για την ψυχική και υλική συμπαράστασή της όλα αυτά τα χρόνια σπουδών που πέρασαν και αυτά που θα έρθουν, και όλους τους φίλους που με στήριξαν, από κοντά κι από μακριά.

Κατερίνα – Θεώνη Σπυροπούλου

Πάτρα, Σεπτέμβριος 2012



# ΠΕΡΙΕΧΟΜΕΝΑ

<b>ΠΕΡΙΛΗΨΗ.....</b>	<b>7</b>
<b>ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ .....</b>	<b>9</b>
<b>ΚΕΦΑΛΑΙΟ 2: CARRIER GRADE ETHERNET.....</b>	<b>13</b>
<b>2.1 ΤΙ ΕΙΝΑΙ ΤΟ CARRIER GRADE ETHERNET.....</b>	<b>13</b>
<b>2.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ CARRIER ETHERNET .....</b>	<b>14</b>
<b>2.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ CARRIER ETHERNET .....</b>	<b>18</b>
2.3.1 <i>Τυποποιημένες Υπηρεσίες</i> .....	18
2.3.2 <i>Κλιμακωσιμότητα</i> .....	25
2.3.3 <i>Αξιοπιστία</i> .....	27
2.3.4 <i>Ποιότητα Υπηρεσιών</i> .....	28
2.3.5 <i>Διαχείριση Υπηρεσιών</i> .....	29
<b>2.4 ΧΡΗΣΕΙΣ ΤΟΥ CARRIER ETHERNET.....</b>	<b>31</b>
<b>ΚΕΦΑΛΑΙΟ 3: ΠΡΩΤΟΚΟΛΛΑ .....</b>	<b>35</b>
<b>3.1 PROVIDER BRIGDES (Q-in-Q).....</b>	<b>35</b>
3.1.1 <i>Αρχές λειτουργίας του Q-in-Q</i> .....	35
3.1.2 <i>Πλεονεκτήματα χρήσης του Q-in-Q</i> .....	38
3.1.3 <i>Υλοποιήσεις Q-in-Q διαφόρων προμηθευτών</i> .....	38
<b>3.2 PROVIDER BACKBONE BRIGDES (MAC-in-MAC) .....</b>	<b>39</b>
3.2.1 <i>Αρχές λειτουργίας του MAC-in-MAC</i> .....	39
<b>3.3 PROVIDER BACKBONE BRIGDE TRAFFIC ENGINEERING (PBB-TE) .....</b>	<b>44</b>
3.3.1 <i>Αρχές λειτουργίας του PBB-TE</i> .....	45
3.3.2 <i>Πλεονεκτήματα χρήσης του PBB-TE</i> .....	48
3.3.3 <i>PBB-TE vs MPLS</i> .....	49
<b>3.4 OPERATION ADMINISTRATION AND MAINTENANCE (OAM).....</b>	<b>52</b>
3.4.1 <i>Αρχές λειτουργίας του OAM</i> .....	54
<b>3.5 LINK LAYER DISCOVERY PROTOCOL (LLDP).....</b>	<b>56</b>
3.5.1 <i>Αρχές λειτουργίας του LLDP</i> .....	57
3.5.2 <i>Ιδιότητα πρωτόκολλα ανακάλυψης τοπολογίας δικτύου</i> .....	59
3.5.3 <i>Πλεονεκτήματα χρήσης του LLDP</i> .....	60
<b>ΚΕΦΑΛΑΙΟ 4: ΥΛΟΠΟΙΗΣΗ ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΔΙΚΤΥΟ .....</b>	<b>63</b>

---

<b>4.1 AutoBAHN</b> .....	63
<b>4.1.1 Αρχιτεκτονική του AutoBAHN</b> .....	65
<b>4.2 AUTOBAHN CARRIER GRADE ETHERNET TECHNOLOGY PROXY (CGE TP)</b> .....	69
<b>4.2.1 Υποστηριζόμενες τεχνολογίες</b> .....	69
<b>4.2.2 Υποδομή Carrier Ethernet</b> .....	71
<b>4.2.3 Ανακάλυψη τοπολογίας</b> .....	73
<b>4.2.4 Αρχιτεκτονική του CGE TP</b> .....	73
<b>4.2.5 Ρυθμίσεις μεταγωγέων (Switch Configuration)</b> .....	77
<b>4.2.6 Ρυθμίσεις CGE Technology Proxy (TP Configuration)</b> .....	78
<b>4.2.7 Καθορισμός εύρους ζώνης</b> .....	86
<b>4.2.8 Αποτελέσματα πειραματικού ελέγχου</b> .....	90
<b>ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ</b> .....	93
<b>ΑΚΡΩΝΥΜΑ</b> .....	99
<b>ΑΝΤΙΣΤΟΙΧΙΣΗ ΑΓΓΛΙΚΗΣ-ΕΛΛΗΝΙΚΗΣ ΟΡΟΛΟΓΙΑΣ</b> .....	103
<b>ΒΙΒΛΙΟΓΡΑΦΙΑ</b> .....	105

---

## ΠΕΡΙΛΗΨΗ

---

Το Ethernet είναι μια ευρύτατα διαδεδομένη τεχνολογία που δίνει υψηλό εύρος ζώνης, σε σχετικά χαμηλό κόστος, και εύκολη εγκατάσταση. Για τους λόγους αυτούς χρησιμοποιείται σε δίκτυα ευρείας περιοχής (Wide Area Networks, WANs), ακόμα και σε δίκτυα κορμού. Το Carrier Grade Ethernet (ή Carrier Ethernet) διακρίνεται από το απλό LAN Ethernet, καθώς έχει κάποιες επιπλέον ιδιότητες, όπως της κλιμακωσιμότητας, της αξιοπιστίας και της ποιότητας υπηρεσίας.

Στην παρούσα διπλωματική εργασία παρουσιάζονται, στο Κεφάλαιο 2, αναλυτικά η δομή, η λειτουργία, τα χαρακτηριστικά και οι υπηρεσίες που προσφέρει το Carrier Grade Ethernet. Στο Κεφάλαιο 3 γίνεται μια εκτεταμένη αναφορά στα πρωτόκολλα που ορίζει το IEEE για υποστήριξη του Carrier Ethernet σε δίκτυα κορμού, στις αρχές λειτουργίας τους και στα οφέλη που προκύπτουν από τη χρήση τους. Το Κεφάλαιο 4 αφορά τη μελέτη της παραπάνω τεχνολογίας και των βασικών της χαρακτηριστικών σε πραγματικό δίκτυο, η οποία περιλαμβάνει την προσπάθεια ανάπτυξης προγραμματιστικών εφαρμογών για την αυτοματοποιημένη διαχείριση κυκλωμάτων σε Carrier Ethernet δίκτυα. Τέλος, στο Κεφάλαιο 5 παρουσιάζονται γενικά τα πλεονεκτήματα υλοποίησης του Carrier Ethernet έναντι παραδοσιακών τεχνολογιών δικτύωσης, καθώς και συμπεράσματα που εξήχθησαν από την προαναφερθείσα πειραματική εφαρμογή.





---

## ΚΕΦΑΛΑΙΟ 1: *ΕΙΣΑΓΩΓΗ*

---

Όσοι κινούνται στο χώρο της πληροφορικής θα έχουν παρατηρήσει ότι κάποιες τεχνολογίες προσαρμόζονται στις συνεχείς αλλαγές των συνθηκών, ενώ άλλες, λιγότερο ευέλικτες, απλά «πεθαίνουν» ή χρησιμοποιούνται σε δευτερεύουσας σημασίας εφαρμογές. Το κανάλι οπτικών ινών, για παράδειγμα, δε θα μπορούσε να είναι το κύριο μέσο μεταφοράς και αποθήκευσης δεδομένων, αν δεν εξελισσόταν διαρκώς όσον αφορά την ταχύτητα και τις επιπλέον υπηρεσίες που προσφέρει. Τα κυκλώματα μεταγωγής, που συναντώνται σε όλα τα κέντρα δεδομένων παγκοσμίως, μοιάζουν ελάχιστα με τις πρώιμες υλοποιήσεις βρόχων διαιτησίας της «παιδικής ηλικίας» της τεχνολογίας.

Έχοντας εξίσου μακρά ιστορία, το Ethernet έχει παρόμοια προσαρμοστεί, με την πάροδο του χρόνου, σε νέες απαιτήσεις. Τις τελευταίες δεκαετίες εξελίχθηκε από ένα σύστημα μετάδοσης βασισμένο στον ανταγωνισμό ραδιοφωνικού καναλιού (connection-based radio channel transmission system) με ταχύτητα μερικών Kbps, στο πιο δημοφιλές πρότυπο τοπικών δικτύων (Local Area Networks, LANs) παγκοσμίως, ικανό να μεταδώσει 1 Gbps πάνω από αθωράκιστο τηλεφωνικό καλώδιο συνεστραμμένου ζεύγους.

Το Ethernet αναπτύχθηκε ως ένα ανοικτό δίκτυο δίκαιης πρόσβασης και πανταχού συνδεσιμότητας, για τη διασύνδεση υπολογιστών σε μια ενιαία οργάνωση. Οι προτεραιότητές του ήταν χαμηλό κόστος, ευκολία σύνδεσης και αποσύνδεσης στο και από το δίκτυο, δίκαιη κατανομή του μέγιστου εύρους ζώνης μεταξύ όλων των χρηστών και αυτόματη ανακάλυψη των πόρων του δικτύου. Η απλότητα των πρωτοκόλλων του, η στενή σχέση του με το TCP/IP μοντέλο αναφοράς, η προσαρμοστικότητά του στις νέες, βασισμένες στο πρωτόκολλο IP, τεχνολογίες και η τυποποίηση των υπηρεσιών του Ethernet, που καθιστά δυνατή την ανάπτυξή του από διάφορους προμηθευτές, αυξάνουν διαρκώς τη δημοτικότητά του στην επιχειρησιακή αγορά. Αυτή η δημοτικότητα έχει προκαλέσει σημαντική πρόοδο και έχει μειώσει το κόστος των βασικών τεχνολογικών τομέων σε πολύ χαμηλά επίπεδα, γεγονός που έκανε το Ethernet να επικρατήσει, ακόμα κι αν δεν υπερέρχει τεχνικά ή σε ταχύτητα.

Στο χώρο των «carrier» υπηρεσιών, δηλαδή των υπηρεσιών μεταφοράς πληροφοριών που εξυπηρετούν ένα ευρύ φάσμα πελατών μέσω μιας κοινής πλατφόρμας, οι πάροχοι μητροπολιτικών (Metropolitan Area Networks, MANs) και ευρείας περιοχής (WAN) δικτύων αντιμετωπίζουν τρεις βασικές ανάγκες:

- Να παρέχουν στους πελάτες τους υπηρεσίες Ethernet
- Να χρησιμοποιούν τη χωρητικότητα και τα οικονομικά πλεονεκτήματα των τεχνολογιών Ethernet στα δίκτυά τους
- Να αντικαταστήσουν τις μη-Ethernet τεχνολογίες με αντίστοιχες ανταγωνιστικές Ethernet, που έχουν επαρκή χωρητικότητα για αποθήκευση, δημιουργία αντιγράφων ασφαλείας και βίντεο υψηλής ευκρίνειας και εγγυώνται τα απαραίτητα χαρακτηριστικά (ασφάλεια μεταφοράς, χαμηλό latency) για την υποστήριξη αυτών των υπηρεσιών

Οι ιδιωτικές carrier υπηρεσίες πρέπει επίσης να προσφέρουν υψηλή ασφάλεια από υποκλοπές ή διαρροή πληροφορίας μεταξύ των πελατών, να αποτρέπουν οι βλάβες του δικτύου ή της υπηρεσίας ενός πελάτη να επηρεάζουν άλλους, να ελέγχουν την πρόσβαση των πελατών στις υπηρεσίες, ώστε ο καθένας να διαθέτει ό,τι έχει πληρώσει και τίποτα παραπάνω, να πιστοποιούν **ποιότητα υπηρεσιών (Quality of Service, QoS)** και να παρέχουν **εγγυημένο επίπεδο υπηρεσιών (Service Level Agreement, SLA)**.

Στα παραδοσιακά carrier δίκτυα, η προσφερόμενη υπηρεσία ήταν πολύ στενά συνδεδεμένη με την αντίστοιχη υποδομή. Η τεχνολογία IP/MPLS έχει αναπτυχθεί από πολλούς φορείς, ως μια προσπάθεια δημιουργίας ενός ενιαίου επιπέδου, αλλά η εμπειρία έχει δείξει ότι σε μεγάλα μεγέθη υπάρχουν προβλήματα διαχείρισης και κλιμακωσιμότητας που εμποδίζουν αυτή την ανάπτυξη. Αντίθετα, το Ethernet φαίνεται να προσφέρει μια παγκόσμια βάση, πάνω στην οποία μπορεί να οικοδομηθεί μια υποδομή μεταφορών, καθώς προσφέρει όλο και περισσότερες τυποποιημένες υπηρεσίες, πάνω στις οποίες αναπτύσσονται νέες τεχνολογίες.

Συνεπώς, το Ethernet γίνεται πολυπλοκότερο, για να μεταμορφώσει αυτό που κάποτε ήταν μια ασυνδεδεσμένη τεχνολογία μεταφοράς, σε μια πιο ντετερμινιστική συνδεοστραφή, το επονομαζόμενο Carrier Grade Ethernet. Η μετάλλαξη του

Ethernet από μία πιο «πρόχειρη» σε μια πιο εύρωστη, κλιμακώσιμη και αξιόπιστη τεχνολογία μεταφοράς δεδομένων, επιτυγχάνεται μέσω μιας σειράς προτύπων που επεκτείνουν της δυνατότητές της. Τα περισσότερα από τα πρότυπα του Ethernet εμπίπτουν στο **IEEE (Institute of Electrical and Electronic Engineers)**, αν και επιπλέον πρότυπα μπορούν να καλύψουν ειδικές απαιτήσεις πέρα από τις αρμοδιότητες του IEEE. Το **IETF (Internet Engineering Task Force)**, για παράδειγμα, αφορά βασισμένα στην τεχνολογία IP πρωτόκολλα διαχείρισης και πρωτοκόλλα που αφορούν επίπεδα υψηλότερα του **επιπέδου 2 του μοντέλου OSI (επίπεδο συνδέσμου μετάδοσης δεδομένων – Datalink Layer – Layer 2)**. Επίσης, η διαμόρφωση του Carrier Grade Ethernet εξαρτάται από την **ITU (International Telecommunications Union)** και το **MEF (Metro Ethernet Forum)**<sup>1</sup>.

Οι υπηρεσίες Carrier Ethernet είναι ιδιωτικές και συνδέουν προκαθορισμένους σταθμούς. Για το λόγο αυτό, πρέπει να είναι πλήρως διαφανείς και να αποτρέπουν την αλληλεπίδραση μεταξύ διακομιστών (servers) και πελατών (clients). Η σημαντικότερη καινοτομία του Carrier Ethernet είναι η απλότητα της υλοποίησης και η μείωση του κόστους, σε σύγκριση με τις συμβατικές WAN υπηρεσίες. Το Carrier Ethernet υποστηρίζεται σε πλήθος WAN μηχανισμών μεταφοράς δεδομένων, όπως οι DWDM, MPLS και SONET. Ο χειρισμός της μεταφοράς δεδομένων, τον οποίο προσφέρει, είναι επίσης «κλειδί» για τη μέτρηση της απόδοσης και τη γρήγορη διάγνωση προβλημάτων της υπηρεσίας.

---

<sup>1</sup> Το Metro Ethernet Forum (MEF) ιδρύθηκε το 2001 και είναι μία μη-κερδοσκοπική διεθνής κοινοπραξία, αφιερωμένη στην παγκόσμια υιοθέτηση των δικτύων και υπηρεσιών Carrier Ethernet. Το φόρουμ αποτελείται από κορυφαίους παρόχους υπηρεσιών, μεγάλους, επιβεβλημένους carriers τοπικών ανταλλαγών, προμηθευτές δικτυακού εξοπλισμού και άλλες εταιρίες δικτύωσης, που έχουν κοινό συμφέρον στο Metro Ethernet. Το Φεβρουάριο του 2010 το MEF απαρτιθόσε 160 μέλη. Το MEF ασχολείται τόσο με τεχνικά στοιχεία όσο και με στοιχεία μάρκετινγκ, για την προώθηση της χρήσης του Metro Ethernet. Αυτό είναι ένας βασικός παράγοντας διαφοροποίησης από άλλους οργανισμούς, όπως το IETF και το IEEE. Το φόρουμ κάνει συστάσεις σε υφιστάμενα όργανα και δημιουργεί προδιαγραφές που δεν αναπτύσσονται από άλλους οργανισμούς, ή δεν εμπίπτουν στο πεδίο εφαρμογής τους. Ιστορικά, πριν από το MEF ιδρύθηκε, επίσης το 2001, το Ethernet in the First Mile Alliance (EFMA), άλλη μια μη-κερδοσκοπική διεθνής κοινοπραξία, με σκοπό την προώθηση των προϊόντων και των τεχνολογιών Ethernet in the First Mile (EFM) και την καθιέρωση των EFM ως βασικών τεχνολογιών δικτύωσης, για ένα δίκτυο πρόσβασης. Το 2005, με την ολοκλήρωση του προτύπου 802.3ah από το IEEE, το EFMA έγινε μέλος του Metro Ethernet Forum.



---

## ΚΕΦΑΛΑΙΟ 2: *CARRIER GRADE ETHERNET*

---

### 2.1 ΤΙ ΕΙΝΑΙ ΤΟ ΤΟ CARRIER GRADE ETHERNET

---

Το Carrier Grade Ethernet, ή **Carrier Ethernet**, είναι η δυνατότητα χρησιμοποίησης του Ethernet σε διαφορετικές τεχνολογίες μεταφοράς δεδομένων, που ξεπερνά τα όρια των πανεπιστημιακών, εταιρικών ή μητροπολιτικών δικτύων και μπορεί να επεκταθεί σε παγκόσμιο επίπεδο. Υπό την έννοια αυτή, ορίζεται το **Metro Ethernet Network (MEN)**, ως ένα δίκτυο Ethernet που ξεπερνά την κλασσική έννοια του MAN και επεκτείνεται σε παγκόσμια δίκτυα και δίκτυα πρόσβασης.

Το Carrier Ethernet είναι μια «τυποποιημένη υπηρεσία», υπό την έννοια ότι οι υπηρεσίες που προσφέρει υλοποιούνται όχι μόνο στα παραδοσιακά Ethernet δίκτυα, αλλά και σε άλλες τεχνολογίες δικτύων. Παραδείγματα αυτής της υλοποίησης είναι:

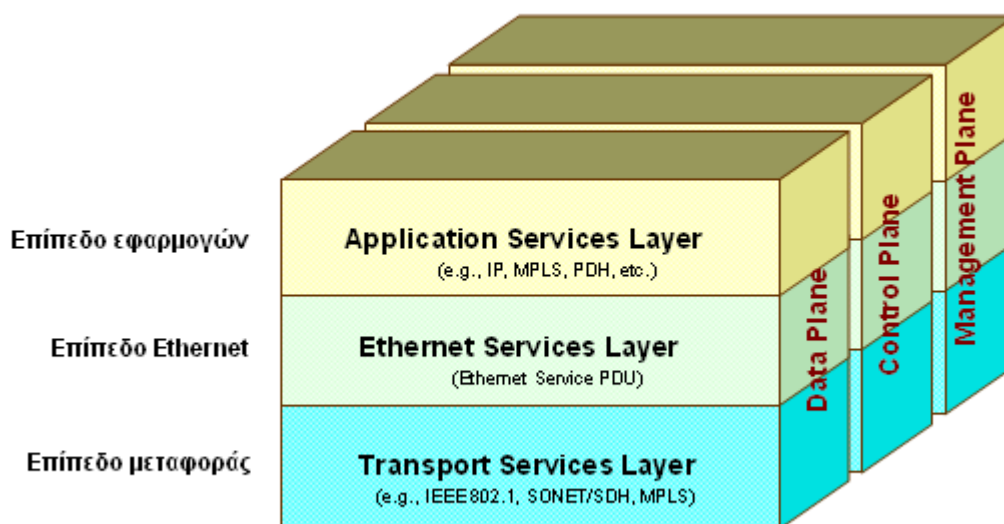
- Ethernet over SONET
- Εικονικά ιδιωτικά δίκτυα (Virtual Private Networks, VPNs) που χρησιμοποιούν μηχανισμό MPLS στο Layer 2
- IEEE 802.1ad Provider Bridges ( Q-in-Q, stacked VLANs)

Για λόγους ακρίβειας, υπάρχει διαχωρισμός μεταξύ των εννοιών των υπηρεσιών Carrier Ethernet και των Carrier Ethernet δικτύων μεταφοράς. Οι υπηρεσίες Carrier Ethernet είναι οι υπηρεσίες που πωλεί ένας πάροχος υπηρεσιών στους πελάτες του, ώστε οι τελευταίοι να μπορούν να διασυνδεθούν σε μια Ethernet υποδομή. Τα Carrier Ethernet δίκτυα μεταφοράς είναι η χρήση της υποδομής Ethernet για τη διασύνδεση των συστημάτων του παρόχου, π.χ. διασύνδεση DSL Πολυπλεκτών Πρόσβασης (DSL Access Multiplexers, DSLAMs) με διακομιστές Ευρυζωνικής Δρομολόγησης και Πρόσβασης (Broadband Routing and Access Server, BRAS) για την υποστήριξη ευρυζωνικών υπηρεσιών πρόσβασης.

Στην πραγματικότητα, μία από τις κύριες ομάδες χρηστών των υπηρεσιών Carrier Ethernet είναι πάροχοι υπηρεσιών, οι οποίοι χρησιμοποιούν αυτές τις υπηρεσίες για να καλύψουν τα κενά των δικών τους δικτύων μεταφορών. Αντίστοιχα, τα Carrier Ethernet δίκτυα μεταφοράς είναι συχνά, αλλά όχι πάντα, η τεχνολογία που χρησιμοποιείται για την παροχή υπηρεσιών Carrier Ethernet.

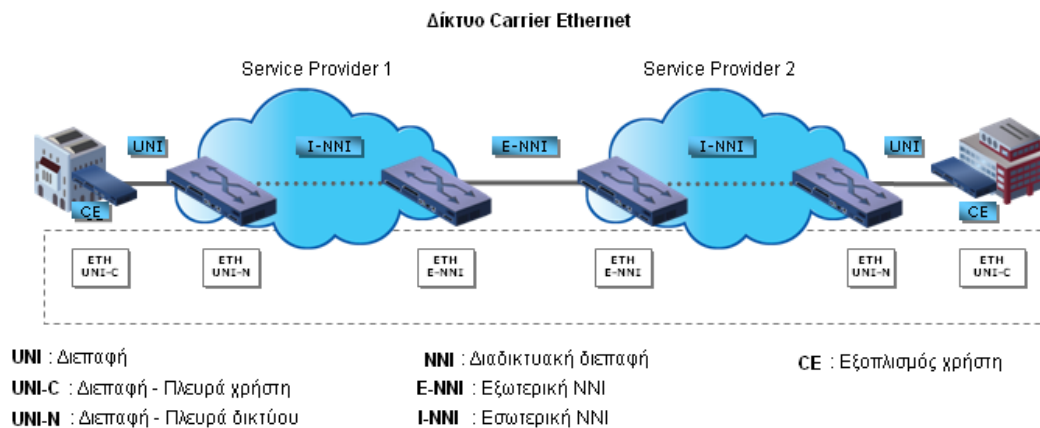
## 2.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ CARRIER ETHERNET

Μέσα σε ένα δίκτυο Carrier Ethernet, τα δεδομένα μεταφέρονται μεταξύ των δικτυακών διεπαφών των χρηστών (**User Network Interfaces, UNIs**), δηλαδή των οριακών σημείων μεταξύ του δικτύου Ethernet του παρόχου και του ιδιωτικού δικτύου του πελάτη, σε μια πολυεπίπεδη αρχιτεκτονική, η οποία φαίνεται στο σχήμα που ακολουθεί. Κάθε UNI είναι μια φυσική διεπαφή Ethernet, που λειτουργεί σε ταχύτητες 10Mbps, 100Mbps, 1Gbps ή 10Gbps.



**Εικόνα 1:** Αρχιτεκτονική του Carrier Ethernet (Carrier Ethernet Services Overview, MEF, 2008)

Όταν υπάρχει κίνηση στο επίπεδο Ethernet, το ίδιο συμβαίνει και στο επίπεδο μεταφοράς. Αυτό επιτρέπει στην Carrier Ethernet κίνηση να είναι αόρατη στα επιμέρους δίκτυα που διασχίζει.



**Εικόνα 2:** Επίπεδο Ethernet (Carrier Ethernet Services Overview, MEF, 2008)

Το επίπεδο μεταφοράς λειτουργεί αφαιρετικά μεταξύ των κόμβων μεταγωγής των υψηλότερων στρωμάτων και της φυσικής δικτυακής υποδομής. Επιτρέπει την «οπτικοποίηση» της τοπολογίας των συνδέσμων μεταξύ των δρομολογητών και καθιστά δυνατή την πλέον αποτελεσματική χρήση των πόρων του συστήματος και των κόμβων μεταγωγής (π.χ. διοχετεύοντας τη διαμετακομιστική κίνηση σε χαμηλότερα επίπεδα). Επίσης, αποτρέπει την αποτυχία των συνδέσμων, καθώς χρησιμοποιεί εργαλεία για την γρήγορη απομόνωση των βλαβών, κατά μήκος περίπλοκων εικονικών συνδέσεων μεταξύ δρομολογητών, οι οποίες συχνά ανήκουν σε διαφορετικά δίκτυα και διανύουν μεγάλες αποστάσεις.

Ο τύπος διεπαφής **Network to Network Interface (NNI)** είναι μια φυσική διεπαφή Ethernet που οριοθετεί τις υπηρεσίες μεταξύ των δικτύων δύο φορέων παροχής υπηρεσιών. Κάθε πάροχος είναι υπεύθυνος για την αντίστοιχη πλευρά της υπηρεσίας του, μέχρι το σημείο διασύνδεσης NNI. Το MEF ορίζει δύο κατηγορίες παρόχων που διασυνδέονται στη NNI. Ο ένας ονομάζεται «διαχειριστής» (operator) και ο άλλος «πάροχος υπηρεσιών» (Service Provider, SP). Σύμφωνα με τους ορισμούς αυτούς, ο πάροχος υπηρεσιών πωλεί Ethernet υπηρεσίες προς τους τελικούς

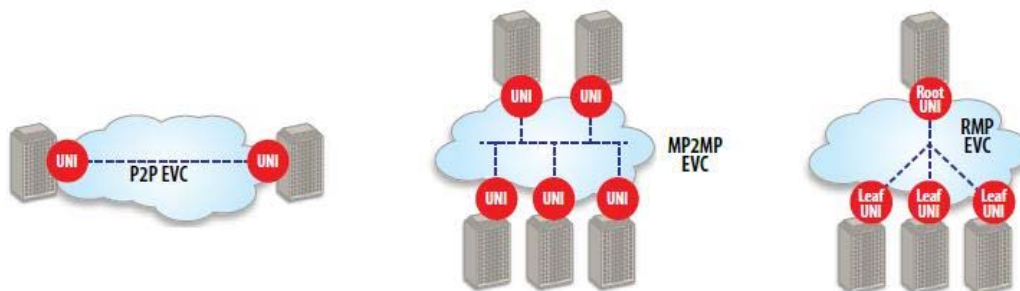
αγοραστές, οι οποίοι συνδέονται στο δίκτυο μέσω Ethernet UNI. Ο διαχειριστής πωλεί υπηρεσίες Ethernet στον πάροχο υπηρεσιών και τα δίκτυά τους είναι διασυνδεδεμένα μέσω Ethernet NNI. Ένας διαχειριστής χρησιμοποιείται όταν ο πάροχος υπηρεσιών δεν μπορεί να «φτάσει» τις εγκαταστάσεις των τελικών χρηστών, οι οποίες ονομάζονται «εκτός δικτύου».

Το MEF έχει ορίσει δύο τύπους **εικονικών Ethernet συνδέσεων**, την **EVC (Ethernet Virtual Connection)** και την **OVC (Operator Virtual Connection)**. Οι εικονικές αυτές συνδέσεις απεικονίζουν περισσότερο τη λογική κι όχι την πλήρη φυσική συνδεσιμότητα μεταξύ των UNIs ή NNIs.

Μια EVC συνδέει δύο ή περισσότερες UNIs, αποτρέποντας τη μεταφορά δεδομένων από σταθμούς που δεν ανήκουν στην ίδια EVC, ενώ μπορεί επίσης να συνδυαστεί με άλλου τύπου συνδέσεις ή να πολυπλεχθεί στην ίδια UNI. Υπάρχουν τρεις τύποι EVC:

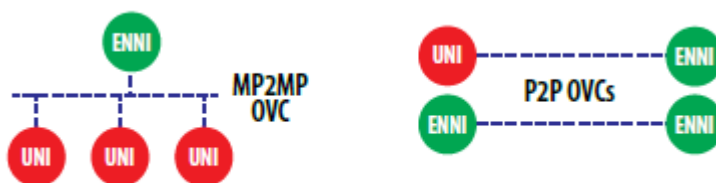
- **Από σημείο σε σημείο (Point-to-point, P2P):** παρέχει συνδεσιμότητα με άλλες παρόμοιες point-to-point MAN/WAN τεχνολογίες (T1/E1 ή Frame Relay). Διασυνδέει αποκλειστικά δύο UNIs.
- **Από πολλά σημεία σε πολλά σημεία (Multipoint-to-multipoint, MP2MP):** είναι παρόμοια με τη χρήση του Ethernet σε ένα LAN, καθώς όλα τα πλαίσια Ethernet που σχετίζονται με την EVC είναι ορατά και προσβάσιμα από όλα τα μέλη της. Χρησιμοποιείται για τη διασύνδεση απομακρυσμένων περιοχών.
- **Από ένα σημείο σε πολλά σημεία (Point-to-multipoint, Rooted Multipoint, RMP):** ειδική περίπτωση multipoint-to-multipoint EVC, όπου μια UNI ορίζεται ως ρίζα και οι υπόλοιπες προσδιορίζονται ως φύλλα. Η ρίζα συνδέεται πλήρως με όλα τα φύλλα, ενώ τα φύλλα συνδέονται μόνο με τη ρίζα. Χρησιμοποιείται σε εφαρμογές πολλαπλής εκπομπής, όπως π.χ. η μετάδοση βίντεο, όπου η ρίζα μεταδίδει τα κανάλια σε όλα τα φύλλα, ενώ τα φύλλα αποστέλλουν στη ρίζα αιτήσεις για αλλαγή καναλιού. Μια άλλη εφαρμογή είναι η «συγκέντρωση πρόσβασης στο διαδίκτυο», όπου η ρίζα συνδέεται απευθείας στο Internet, ενώ τα φύλλα συνδέονται στο Internet μέσω της σύνδεσης της ρίζας.





**Εικόνα 3:** Τύποι EVCs (Carrier Ethernet Essentials, Fujitsu Network Communications Inc., 2010)

Μια OVC συνδέει μια UNI με μια NNI ή δύο NNIs μεταξύ τους. Δύο ή περισσότερες OVCs μπορούν να ενωθούν για να δημιουργήσουν μια EVC, η οποία διασχίζει πολλαπλά δίκτυα παροχής υπηρεσιών. Το MEF έχει ορίσει επί του παρόντος δύο τύπους OVCs, point-to-point και multipoint-to-multipoint. Οι P2P OVCs είναι πιο δημοφιλείς, λόγω της απλότητας της υλοποίησής τους, σε σχέση με τις MP2MP.



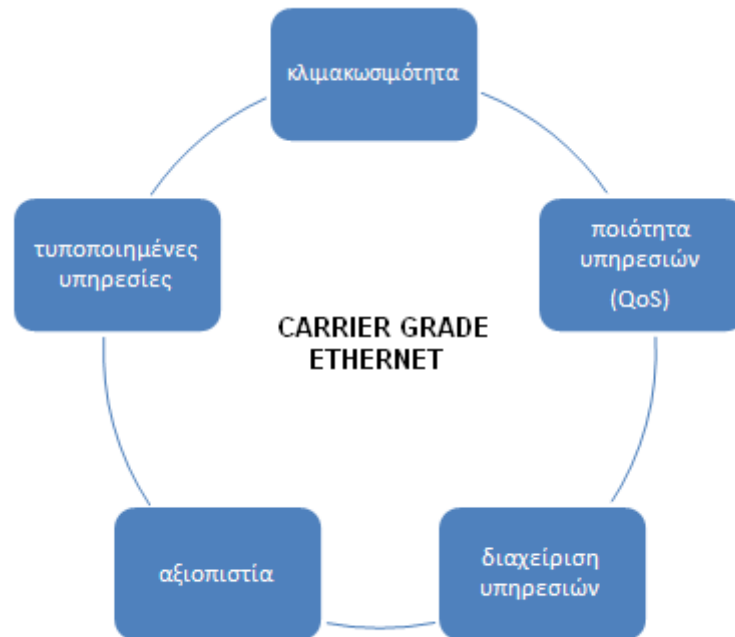
**Εικόνα 4:** Τύποι OVCs (Carrier Ethernet Essentials, Fujitsu Network Communications Inc., 2010)

---

## 2.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ CARRIER ETHERNET

---

Το Carrier Ethernet διακρίνεται από πέντε κύρια χαρακτηριστικά, όπως φαίνεται στο παρακάτω διάγραμμα:



**Εικόνα 4:** Χαρακτηριστικά του Carrier Ethernet

---

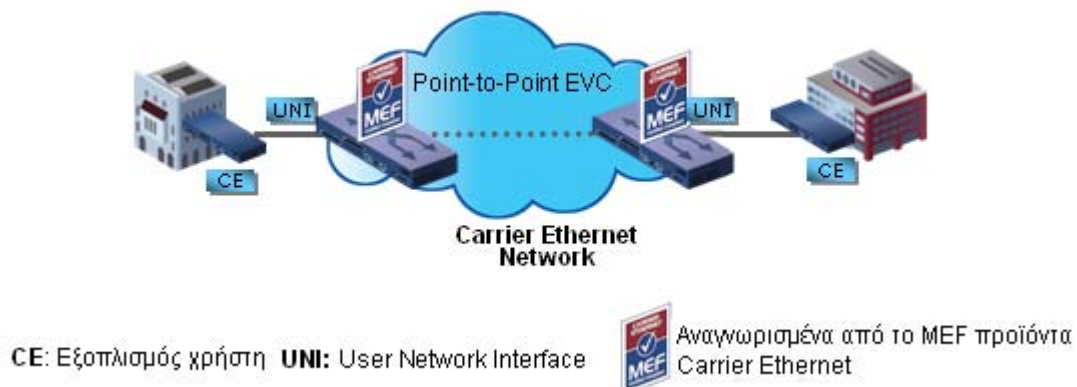
### 2.3.1 ΤΥΠΟΠΟΙΗΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ

---

Το Metro Ethernet Forum (MEF) έχει ως τώρα διακρίνει τρεις τύπους τυποποιημένων υπηρεσιών που βασίζονται στον EVC τύπο σύνδεσης, τις **E-LINE**, **E-LAN** και **E-Tree**. Στις αρχές του 2010, ξεκίνησε τον καθορισμό ενός νέου τύπου υπηρεσίας που ονομάζεται **E-Access** και βασίζεται στον OVC τύπο σύνδεσης.

## E-LINE

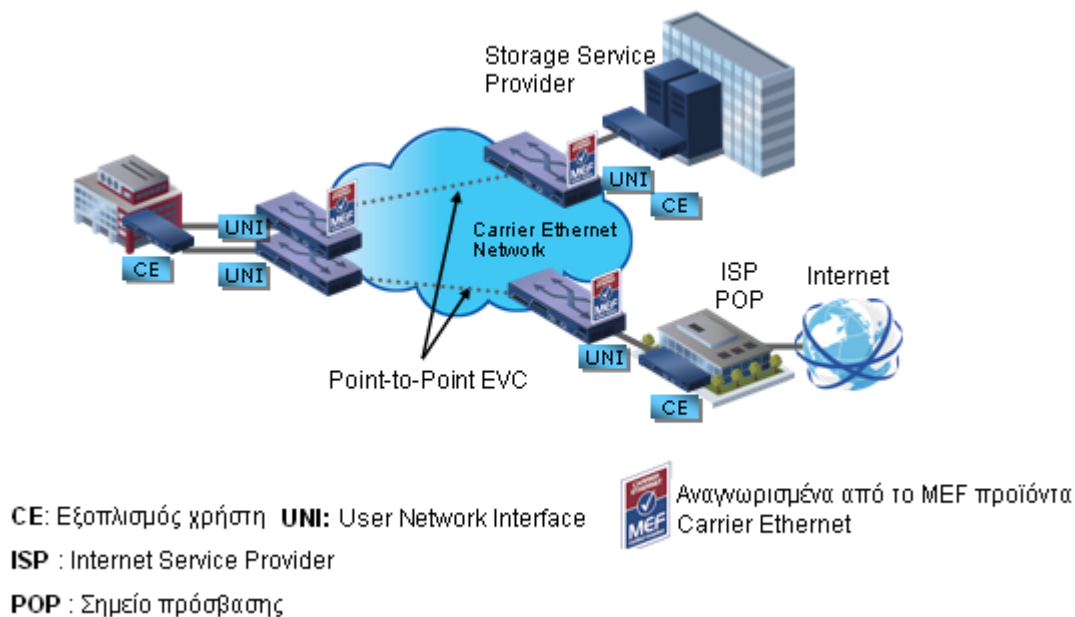
Η υπηρεσία E-LINE είναι μια point-to-point EVC μεταξύ δύο UNIs σ'ένα δίκτυο Ethernet.



**Εικόνα 5:** Υπηρεσία E-LINE (Carrier Ethernet Services Overview, MEF, 2008)

Η υπηρεσία E-LINE χρησιμοποιείται για την πρόσβαση στο Internet, όπως και με τις ακόλουθες μορφές:

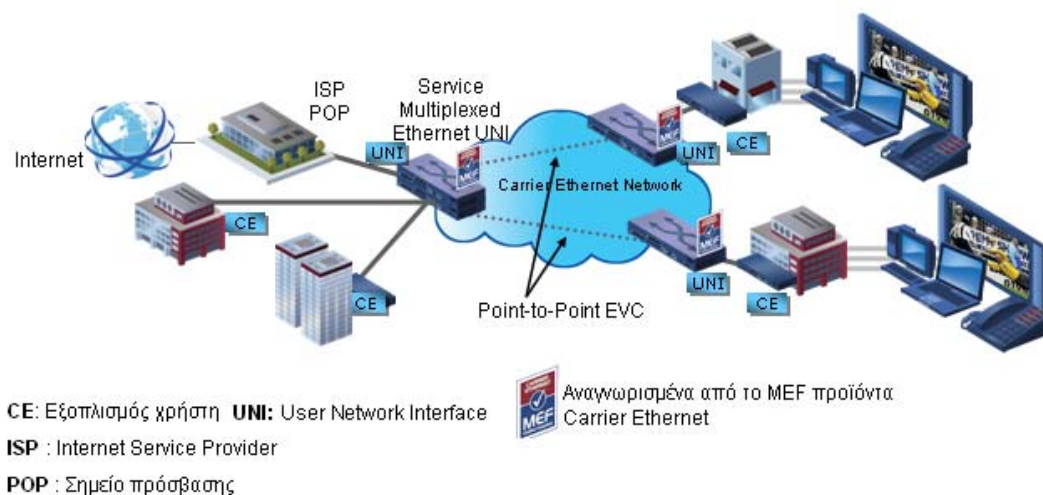
- Ως ιδιωτική γραμμή Ethernet (**Ethernet Private Line, EPL**): Point-to-point σύνδεση μεταξύ δύο UNIs, η οποία προσφέρει υψηλού βαθμού διαφάνεια στην ανταλλαγή δεδομένων μεταξύ των χρηστών. Για το σκοπό αυτό χρησιμοποιείται μια αφιερωμένη γραμμή, συνεπώς απαιτείται ο ελάχιστος δυνατός συντονισμός μεταξύ του παρόχου και του πελάτη. Η υπηρεσία EPL είναι ο ιδανικός τρόπος αντικατάστασης μιας μισθωμένης γραμμής. Πρόκειται, επίσης, για τον πιο δημοφιλή τύπο υπηρεσίας Ethernet, λόγω της απλότητας της υλοποίησής της.



**Εικόνα 6:** Υπηρεσία Ethernet Private Line (Carrier Ethernet Services Overview, MEF, 2008)

- Ως εικονική ιδιωτική γραμμή Ethernet (**Ethernet Virtual Private Line, EVPL**): Παρέχει επιπλέον τη δυνατότητα πολυπλεξίας, με άλλα λόγια τη δυνατότητα ύπαρξης περισσότερων της μίας EVC στην ίδια διεπαφή, όπου η αποστολή των πλαισίων δεδομένων διαμοιράζεται μεταξύ τους. Παρέχονται, επίσης, πολλά επίπεδα **Class of Service (CoS)**<sup>2</sup> στην ίδια διεπαφή, για τα πλαίσια δεδομένων διαφορετικών πελατών. Η υπηρεσία EVPL είναι ο ιδανικός τρόπος αντικατάστασης μιας υπάρχουσας point-to-point Frame Relay σύνδεσης ή ενός σταθερού εικονικού δικτύου ATM (Permanent Virtual Circuit, PVC).

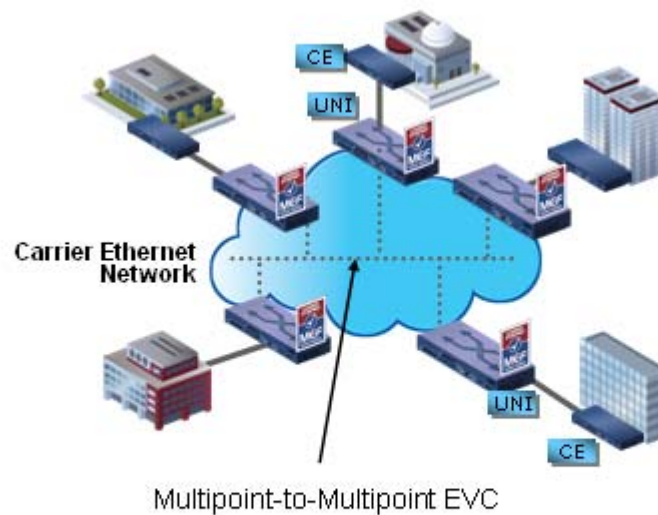
<sup>2</sup> **Class of Service:** πεδίο 3-bit στην επικεφαλίδα των Ethernet πλαισίων που έχουν υποστεί VLAN tagging (βλ. κεφάλαιο 3, Provider Bridges). Καθορίζει μια τιμή προτεραιότητας μεταξύ 0 και 7, η οποία χρησιμοποιείται από μεθόδους παροχής ποιότητας υπηρεσιών (Quality of Service) για τη διαφοροποίηση και τη διαμόρφωση της διαδικτυακής κίνησης.



**Εικόνα 7:** Υπηρεσία Ethernet Virtual Private Line (Carrier Ethernet Services Overview, MEF, 2008)

### **E-LAN**

Η υπηρεσία E-LAN είναι μια multipoint-to-multipoint EVC, η οποία προσφέρει πολλαπλή συνδεσιμότητα μεταξύ πολλών UNIs σε ένα δίκτυο Carrier Ethernet, αφιερωμένων ή πολυπλεγμένων. Παρέχει υψηλού βαθμού διαφάνεια και είναι το θεμέλιο για τις υπηρεσίες IPTV, τα δίκτυα πολλαπλής εκπομπής κ.ά.



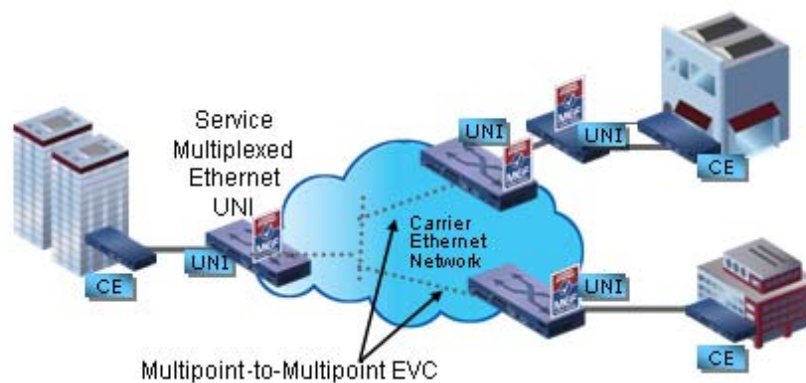
CE: Εξοπλισμός χρήστη UNI: User Network Interface



Αναγνωρισμένα από το MEF προϊόντα Carrier Ethernet

**Εικόνα 8:** Υπηρεσία E-LAN (Carrier Ethernet Services Overview, MEF, 2008)

Όπως και στην περίπτωση της υπηρεσίας E-LINE, υπάρχουν δύο μορφές της υπηρεσίας E-LAN, οι **EP-LAN (Ethernet Private LAN)** και **EVP-LAN (Ethernet Virtual Private LAN)**.



CE: Εξοπλισμός χρήστη UNI: User Network Interface

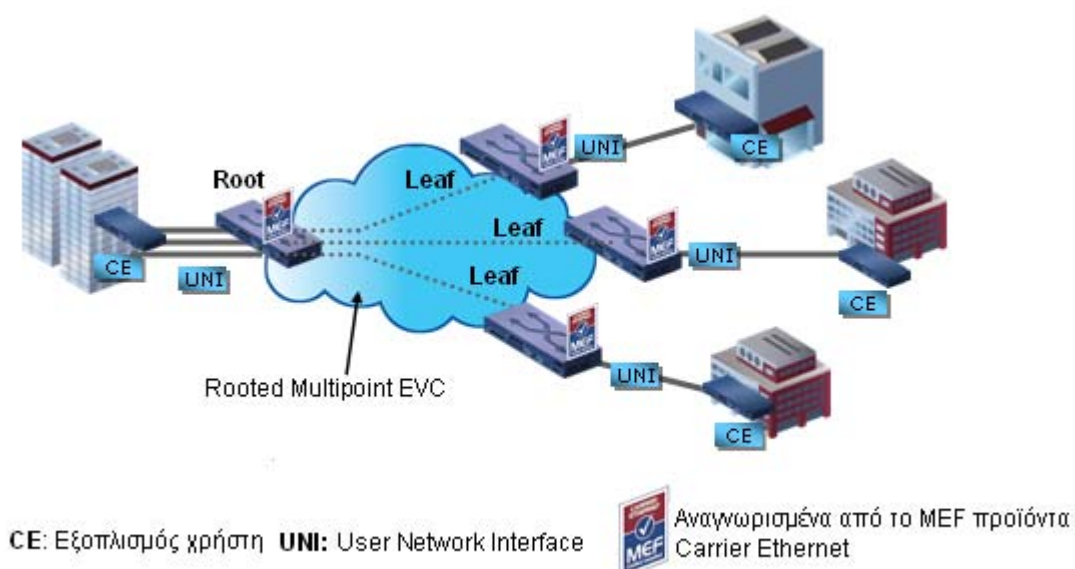


Αναγνωρισμένα από το MEF προϊόντα Carrier Ethernet

**Εικόνα 9:** Υπηρεσία Ethernet Virtual Private LAN (Carrier Ethernet Services Overview, MEF, 2008)

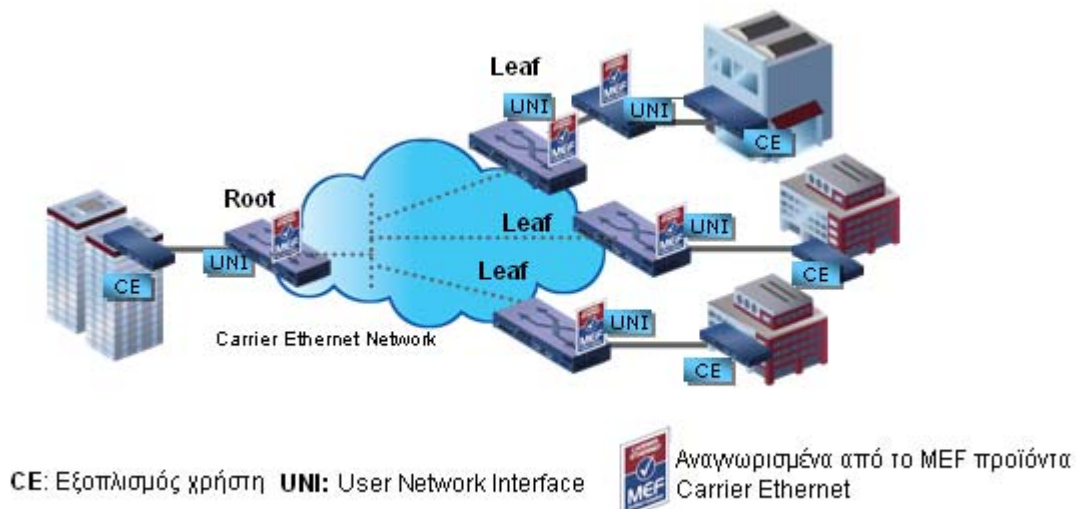
## E-Tree

Η υπηρεσία E-Tree είναι μια point-to-multipoint EVC, που συνδέει μία ή περισσότερες ρίζες και ένα σύνολο φύλλων, αλλά αποτρέπει την επικοινωνία μεταξύ των φύλλων. Απευθύνεται, συνεπώς, σε περιπτώσεις φιλοξενίας πολλών χρηστών, όπου η κίνηση του καθενός πρέπει να διατηρείται αόρατη στους υπολοίπους. Χρησιμοποιείται σε εφαρμογές που απαιτούν ανάλογη τοπολογία, όπως η πρόσβαση στο internet, η «κατ'απαίτηση» αναπαραγωγή βίντεο (video on demand) και εφαρμογές δικαιόχρησης (franchising).



**Εικόνα 10:** Υπηρεσία E-Tree (Carrier Ethernet Services Overview, MEF, 2008)

Όπως και στην περίπτωση των υπηρεσιών E-LINE και E-LAN, υπάρχουν δύο μορφές της υπηρεσίας E-Tree, οι **EP-Tree (Ethernet Private Tree)** και **EVP-Tree (Ethernet Virtual Private Tree)**.



**Εικόνα 11:** Υπηρεσία Ethernet Virtual Private Tree (Carrier Ethernet Services Overview, MEF, 2008)

### E-Access

Η υπηρεσία E-Access είναι μία point-to-point OVC μεταξύ μιας UNI και μιας NNI. Το MEF βρίσκεται σε στάδιο ανάπτυξης ορισμών της υπηρεσίας με βάση το VLAN ή τη θύρα (VLAN-based και port-based<sup>3</sup> αντίστοιχα). Οι υπηρεσίες E-Access πωλούνται από τους «χονδρικούς» παρόχους πρόσβασης Ethernet στους «λιανικούς» παρόχους, οι οποίοι με τη σειρά τους πωλούν EVC υπηρεσίες στους συνδρομητές τους.

Υπάρχουν δύο μορφές της υπηρεσίας E-Access, οι **Access EPL** και **Access EVPL**. Η υπηρεσία Access EPL είναι παρόμοια με την EPL, υποστηρίζοντας μια σύνδεση OVC, διαθέτει όμως και δυνατότητα πολυπλεξίας NNIs. Είναι port-based, πράγμα που την καθιστά την απλούστερη μορφή OVC υπηρεσίας και εξαλείφει την

<sup>3</sup> Μια **port-based** υπηρεσία δεν κάνει διάκριση μεταξύ των πλαισίων Ethernet που δεν διαθέτουν κάποιο ιδιαίτερο γνώρισμα (tag, προτεραιότητα) και τα προωθεί όλα. Μια **VLAN-based** υπηρεσία προβαίνει σε διάκριση μεταξύ των διαφορετικών τύπων πλαισίων Ethernet, επιτρέποντας σε πολλαπλές υπηρεσίες να πολυπλεχθούν στην ίδια UNI. Μια port-based υπηρεσία είναι απλούστερη στην υλοποίηση, αλλά λιγότερο ευέλικτη.



ανάγκη αντιστοίχισης VLAN-ID και συντονισμού μεταξύ του χονδρικού και του λιανικού παρόχου πρόσβασης Ethernet.

Η υπηρεσία Access EVPL, παρόμοια με την EVPL, υποστηρίζει την ύπαρξη πολλών OVCs σε μία UNI και την πολυπλεξία NNIs. Είναι VLAN-based, οπότε απαιτείται η αντιστοίχιση VLAN-ID και ο συντονισμός μεταξύ του χονδρικού και του λιανικού παρόχου πρόσβασης Ethernet. Ωστόσο, η Access EVPL παρέχει πρόσθετη ευελιξία και είναι πιο αποδοτική, από πλευράς κόστους, από την Access EPL, όταν απαιτείται η παροχή πολλαπλών υπηρεσιών. Αυτό συμβαίνει επειδή η Access EPL θα απαιτούσε μια ξεχωριστή UNI για κάθε υπηρεσία, με αποτέλεσμα την αύξηση του κόστους εξοπλισμού.

---

### **2.3.2 ΚΛΙΜΑΚΩΣΙΜΟΤΗΤΑ**

---

Ένας από τους πιο επιτακτικούς λόγους για τη χρήση Ethernet είναι η κλιμακωσιμότητα που προσφέρει, όσον αφορά το εύρος ζώνης. Πολλές τεχνολογίες χρησιμοποιούνται για την παροχή υπηρεσιών σε μητροπολιτικά ή ευρείας περιοχής δίκτυα. Οι τεχνολογίες TDM **επιπέδου 1 του OSI (φυσικό επίπεδο – Physical layer – Layer 1)**, που χρησιμοποιούνται για την παροχή ιδιωτικών υπηρεσιών, περιλαμβάνουν χάλκινα κυκλώματα τύπου T1/T3 και βασισμένα στο SONET οπτικά κυκλώματα. Οι τεχνολογίες Layer 2, που χρησιμοποιούνται για την παροχή υπηρεσιών δεδομένων πάνω από τις TDM Layer 1, περιλαμβάνουν το Frame Relay, το ATM (Asynchronous Transfer Mode) και το PPP (Point to Point Protocol). Σε όλες αυτές οι τεχνολογίες, η κλιμακωσιμότητα του εύρους ζώνης είναι άκαμπτη, καθώς το εύρος ζώνης υπαγορεύεται από την εκάστοτε τεχνολογία.

Τη στιγμή που πολλές επιχειρήσεις παρουσιάζουν ρυθμούς ανάπτυξης της τάξης του 20 με 30% κάθε χρόνο, η κλιμακωσιμότητα του Ethernet αντιμετωπίζεται ως ζωτικό στοιχείο για την κάλυψη αυτών των αναπτυξιακών απαιτήσεων. Όταν ένας πάροχος υπηρεσιών ή μια επιχείρηση χρειάζεται να αυξήσει το εύρος ζώνης, πρέπει είτε να συνδέσει πολλά κυκλώματα μαζί ή να αναβαθμίσει το δίκτυο και τον εξοπλισμό που διαθέτει, ώστε να υποστηρίξουν μια νέα τεχνολογία. Αυτό οδηγεί σε μη-γραμμικό εύρος ζώνης, που μπορεί να μην ανταποκρίνεται στις ανάγκες των

χρηστών ή, κυρίως, να μην είναι οικονομικά εφικτό. Η συγκόλληση κυκλωμάτων οδηγεί σε επιπλέον θύρες στο δικτυακό εξοπλισμού, αυξάνοντας το κόστος και τη λειτουργική πολυπλοκότητα, δεδομένου ότι κάθε κύκλωμα διαχειρίζεται ξεχωριστά και η υπηρεσία δεδομένων εξαρτάται από τα συνδεδεμένα κυκλώματα. Τέλος, νέα εργαλεία λειτουργίας, συντήρησης και διαχείρισης απαιτούνται, καθώς οι τεχνολογίες αλλάζουν για να υποστηρίξουν μεγαλύτερο εύρος ζώνης.

Το Carrier Ethernet ξεπερνά αυτούς τους περιορισμούς παρέχοντας ευέλικτη κλιμάκωση του εύρους ζώνης. Μόλις υλοποιείται μια υπηρεσία Ethernet, το επιθυμητό εύρος ζώνης απλά «προστίθεται» σε κάθε θύρα, ανάλογα με την ταχύτητά της, με τη διαδικασία της **απομακρυσμένης πρόβλεψης – remote provisioning** (οι επιθυμητές ρυθμίσεις γίνονται αυτοματοποιημένα σε όλους τους εξοπλισμούς, χωρίς να χρειάζεται η ξεχωριστή διαχείριση του καθενός). Αυτό επιτρέπει στον πάροχο υπηρεσιών να πωλήσει, ή στις επιχειρήσεις να αξιοποιήσουν, το εύρος ζώνης που χρειάζονται πραγματικά οι χρήστες, αντί να τους αναγκάζει να αγοράζουν ένα συγκεκριμένο εύρος ζώνης που υπαγορεύεται από την εκάστοτε τεχνολογία. Με το Carrier Ethernet, οι συνδρομητές μπορούν πλέον να χρησιμοποιούν την πλέον γνωστή τεχνολογία Ethernet για τα LAN, MAN και WAN τους. Αυτό μειώνει το κόστος του εξοπλισμού σύνδεσης με την υπηρεσία και απλουστεύει τις ενέργειες κατάρτισης.

Το Ethernet παρέχει ήδη ένα μεγάλο εύρος ταχυτήτων διεπαφών, από 10 Mbps μέχρι 100 Gbps. Ενδιάμεσες ταχύτητες μεταξύ των τυπικών φυσικών τιμών του Ethernet μπορούν να επιτευχθούν με την τεχνική συνάθροισης συνδέσεων (Link Aggregation). Από τη άλλη μεριά, το Ethernet επιτρέπει στις χάλκινες γραμμές μετάδοσης φωνής να επιτύχουν ταχύτητα 2 Mbps ή και πολλαπλάσιά της, χρησιμοποιώντας την τεχνική της συγκόλλησης (bonding). Καμία άλλη τεχνολογία δεν προσφέρει ούτε στο ελάχιστο τόσο ευρύ φάσμα επιλογών εύρους ζώνης (οι υπηρεσίες Frame Relay, για παράδειγμα, συνήθως προσφέρουν στο μέγιστο ταχύτητες 45 Mbps).

Ένα ελκυστικό χαρακτηριστικό του Carrier Ethernet είναι η δυνατότητα που έχει ο χρήστης να αναβαθμίσει εύκολα το εύρος ζώνης μιας υπάρχουσας Ethernet υπηρεσίας, χωρίς να απαιτείται, στις περισσότερες περιπτώσεις, να επέμβει ο πάροχος της υπηρεσίας. Αυτό οφείλεται στο γεγονός ότι μπορούμε να έχουμε μια μοναδική φυσική διεπαφή, που να μπορεί να επεκταθεί στα 10/100/1000/10000 Mbps, έτσι

ώστε οι αλλαγές στο εύρος ζώνης, ανάλογα με το προφίλ του κάθε χρήστη της υπηρεσίας, να πραγματοποιούνται εύκολα διαμέσου του ελέγχου λογισμικού στο Κέντρο Λειτουργίας Δικτύου (Network Operations Center, NOC). Αυτή η δυνατότητα επιτρέπει την υλοποίηση πολλών ενδιαφερουσών εφαρμογών, όπως η απαίτηση συγκεκριμένου εύρους ζώνης (Bandwidth on Demand, BoD). Επιπλέον, το γεγονός ότι δεν είναι απαραίτητο να σταλεί ένας τεχνικός υπηρεσίας στις εγκαταστάσεις του τελικού χρήστη, συντελεί στην εξοικονόμηση κόστους.

Η επεκτασιμότητα υπερβαίνει τη διαθεσιμότητα γρηγορότερων διεπαφών. Το γεγονός ότι χρησιμοποιείται από εκατομμύρια ανθρώπους μια δικτυακή υπηρεσία ιδανική για τη συντριπτική πλειοψηφία των επιχειρησιακών, πληροφοριακών, τηλεπικοινωνιακών και ψυχαγωγικών εφαρμογών, είναι απόδειξη της ευελιξίας του Carrier Ethernet. Αυτό σημαίνει ότι, ανεξάρτητα από τον τύπο της εφαρμογής, το Carrier Ethernet παρέχει την απαραίτητη ποιότητα που απαιτούν αυτές οι εφαρμογές για να εκτελεστούν απρόσκοπτα σε μια συνήθη υποδομή.

Μια ακόμα διάσταση της επεκτασιμότητας είναι η γεωγραφική εμβέλεια. Το Carrier Ethernet χρησιμοποιείται σε μητροπολιτικά, εθνικά και παγκόσμια δίκτυα. Το MEF ασχολείται και με την τυποποίηση της διασύνδεσης Ethernet δικτύων που χρησιμοποιούνται από διάφορους παρόχους υπηρεσιών, για να επεκτείνουν την πρόσβαση σε τέτοιου είδους υπηρεσίες και να προσφέρουν στους τελικούς χρήστες μια συνεπή υπηρεσία από άκρη σε άκρη.

---

### **2.3.3 ΑΞΙΟΠΙΣΤΙΑ**

---

Το παραδοσιακό Ethernet αντιμετωπιζόταν συχνά ως ο καλύτερος δυνατός μηχανισμός διασύνδεσης. Όμως, το Carrier Ethernet προσφέρει τη δυνατότητα της γρήγορης ανίχνευσης και αποκατάστασης αποτυχιών κόμβου, συνδέσμου ή υπηρεσίας και με τον τρόπο αυτό παρέχει μια υπηρεσία υψηλής διαθεσιμότητας στον τελικό χρήστη. Ανάκαμψη από αποτυχίες, όταν αυτές συμβαίνουν, έχουμε σε λιγότερο από 50 msec. Η ικανότητα αυτή καλύπτει τις πιο δύσκολες απαιτήσεις ποιότητας και διαθεσιμότητας για τη διεκπεραίωση των πιο κρίσιμων εταιρικών

εφαρμογών, υψηλής ποιότητας υπηρεσίες φωνής και βίντεο και στην πιο γενική περίπτωση, κάθε εφαρμογή που απαιτεί προηγμένο επίπεδο υπηρεσιών.

---

#### **2.3.4 ΠΟΙΟΤΗΤΑ ΥΠΗΡΕΣΙΩΝ**

---

Όπως αναφέρθηκε προηγουμένως, το Carrier Ethernet παρέχει μεγάλο φάσμα διακριτών τιμών εύρους ζώνης και επιλογές QoS. Έτσι, μπορεί να προσφερθεί προηγμένο επίπεδο υπηρεσιών, προκειμένου να επιτευχθούν οι απαιτούμενες επιδόσεις όσον αφορά μια συγκεκριμένη εφαρμογή. Το Carrier Ethernet επιτρέπει τη διασφάλιση αυτού του επιπέδου χρησιμοποιώντας εγγυήσεις QoS, με άλλα λόγια καθορίζοντας κάποια χαρακτηριστικά που σχετίζονται με την υπηρεσία και είναι τα ακόλουθα:

- **Committed Information Rate (CIR):** ρυθμός ροής πληροφορίας στη διεπαφή χρήστη
- **Απώλεια πλαισίων (Frame Loss):** αναλογία των ανεπίδοτων πλαισίων προς τα συνολικά πλαίσια του πελάτη που δέχεται το δίκτυο
- **Latency:** καθυστέρηση ενός από άκρη σε άκρη (end-to-end) δικτύου μεταξύ δύο διεπαφών πελατών
- **Διακύμανση Καθυστέρησης Πακέτων (Packet Delay Variation, PDV):** γνωστή ως **jitter**, η μεταβλητότητα της καθυστέρησης των πακέτων σ'ένα δίκτυο

Παραδείγματος χάριν, η φωνή απαιτεί συνήθως χαμηλή καθυστέρηση, ενώ πολλές οικονομικές εφαρμογές που διανέμουν πληροφορία χρονικά ευαίσθητη, απαιτούν εγγυήσεις μικρής απώλειας πλαισίων.

---

### 2.3.5 ΔΙΑΧΕΙΡΙΣΗ ΥΠΗΡΕΣΙΩΝ

---

Το πέμπτο κρίσιμο χαρακτηριστικό του Carrier Ethernet είναι η δυνατότητα ελέγχου, διάγνωσης και κεντρικής διαχείρισης του δικτύου, χρησιμοποιώντας τυποποιημένα εργαλεία, ανεξαρτήτως προμηθευτή. Για να πραγματοποιούν εξελιγμένη διαχείριση της υπηρεσίας, τα εργαλεία αυτά πρέπει να:

- Παρέχουν γρήγορες υπηρεσίες.
- Διαγιγνώσκουν προβλήματα σύνδεσης που αναφέρει ο πελάτης.
- Διαγιγνώσκουν σφάλματα στο δίκτυο, όχι μόνο στα σημεία τερματισμού αλλά και στα ενδιάμεσα.
- Αξιολογούν τα χαρακτηριστικά των προσφερόμενων υπηρεσιών.

Για την διεκπεραίωση αυτών των εργασιών, πολλά εργαλεία έχουν ήδη τυποποιηθεί ή βρίσκονται στη διαδικασία της τυποποίησης. Παραδείγματα τέτοιων εργαλείων είναι:

- Το πρότυπο **IEEE 802.3ah, Operation Administration and Maintenance (OAM)** παρέχει εργαλεία για τον έλεγχο των συνδέσμων, την ένδειξη απομακρυσμένης, κ.ά.
- Το πρότυπο **IEEE 802.1ag Connectivity Fault Management (CFM)** παρέχει εργαλεία για υπηρεσίες επιπέδου OAM και για την ανίχνευση, απομόνωση και αναφορά σφαλμάτων σύνδεσης στο δίκτυο του παρόχου.
- Το πρότυπο **ITU Y.1731** αφορά τη διαχείριση της συνδεσιμότητας και παρέχει επίσης εργαλεία για τη μέτρηση των παραμέτρων απόδοσης της υπηρεσίας, όπως το ποσοστό απώλειας πλαισίων, η καθυστέρηση πλαισίων και η διακύμανση καθυστέρησης πλαισίων.
- Το πρότυπο **MEF 15** καθορίζει τις απαιτήσεις για τη διαχείριση των στοιχείων του δικτύου από εξωτερικό σύστημα διαχείρισης.

Οι πάροχοι μπορούν να χρησιμοποιήσουν αυτά τα εξελιγμένα εργαλεία για να διαχειριστούν τις υπηρεσίες ενός δικτύου Carrier Ethernet. Για κάθε τύπο υπηρεσίας

ορίζονται κάποια χαρακτηριστικά, τα οποία επιτρέπουν στον πάροχο να την προσαρμόσει στις προσδοκίες του τελικού χρήστη και να παρέχει αποτελεσματικό επίπεδο υπηρεσιών. Παραδείγματα τέτοιων χαρακτηριστικών είναι:

- Φυσική ταχύτητα της διεπαφής χρήστη.
- Προφίλ εύρους ζώνης σε κάθε διεπαφή χρήστη που ρυθμίζει παραμέτρους όπως οι Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR) και Excess Burst Size (EBS).
- Προφίλ εύρους ζώνης για κάθε αναγνωριστικό Class of Service (CoS).
- Έλεγχος επεξεργασίας στο Layer 2 (π.χ. επιλογή απόρριψης ή προώθησης πλαισίων πρωτοκόλλων Layer 2, όπως BPDU ή GARP).

Η προσέγγιση των τυποποιημένων προσφερόμενων υπηρεσιών δεν απαιτεί αλλαγές στο LAN εξοπλισμό ή δίκτυο του τελικού χρήστη. Καθορίζοντας δυνατότητα επιλογής διακριτών τιμών για το εύρος ζώνης και την ποιότητα υπηρεσιών, οι πάροχοι έχουν την ελευθερία να διαμορφώσουν μια υπηρεσία που μπορεί να προσαρμοστεί στις ανάγκες του χρήστη. Η χρήση προηγμένων χαρακτηριστικών QoS καθιστά το Carrier Ethernet ιδανικό για την υλοποίηση multiplay υπηρεσιών (φωνή, βίντεο και δεδομένα) σε μια συγκλίνουσα υποδομή. Στο πλαίσιο αυτό, η δουλειά του MEF σχετικά με το Carrier Ethernet συμπληρώνει τη δουλειά άλλων αναγνωρισμένων προτύπων όπως το DSLForum TR-101, το οποίο ορίζει τα, βασισμένα στο Ethernet, αθροιστικά δίκτυα ψηφιακής συνδρομητικής γραμμής (Digital Subscriber Line, DSL).

## 2.4 ΧΡΗΣΕΙΣ ΤΟΥ CARRIER ETHERNET

Στην εικόνα και στους πίνακες που ακολουθούν παρουσιάζονται οι αλληλεξαρτήσεις μεταξύ των διαφορετικών ρόλων του Carrier Ethernet στο δίκτυο.

Εφαρμογή	Site-to-Site L2 VPN	Private Line	IP VPN	Wholesale Access	Internet Access	Video	Cloud Service	3G/4G MBH
Τύπος Υπηρεσίας Ethernet	E-Line, E-LAN, E-Tree, E-Access							
Τεχνολογία Μεταφοράς	Ethernet over Fiber	Ethernet over SDH/SONET	Ethernet over PDH	Ethernet over MPLS	Ethernet over OTN/WDM	Ethernet over Dry Copper	Ethernet over μWave	

**Εικόνα 12:** Χρήσεις του Carrier Ethernet (Carrier Ethernet Essentials, Fujitsu Network Communications Inc., 2010)

Εφαρμογή	Περιγραφή
<b>Site-to-site Layer 2 VPNs (εικονικά ιδιωτικά δίκτυα Layer 2 συνδεδεμένων ιστοσελίδων)</b>	Υψηλό εύρος ζώνης και ευέλικτη αντικατάσταση των αντίστοιχων Frame Relay Layer 2 VPNs
<b>EPL (Ethernet Private Line)</b>	Παρόμοια χαρακτηριστικά με ιδιωτική γραμμή Layer 1, αλλά υλοποίηση μέσω διεπαφών Ethernet
<b>Wholesale Ethernet access (χονδρική πρόσβαση στο Ethernet)</b>	First/Last mile <sup>4</sup> υπηρεσίες Ethernet, επιτρέπουν στους παρόχους υπηρεσιών να εξυπηρετήσουν ιδιωτικές εγκαταστάσεις του πελάτη
<b>3G/4G cell site mobile backhaul</b>	Διασύνδεση κινητών σταθμών βάσης 3G/4G με τους ελεγκτές βάσης, στο κέντρο μεταγωγής
<b>Ethernet access to IP services (Ethernet πρόσβαση σε IP υπηρεσίες)</b>	Αφιερωμένη πρόσβαση στο Internet, πρόσβαση σε IP VPNs και cloud υπηρεσίες, IP video μέσω DSLAM, GePON ή CMTS συλλέκτη

**Πίνακας 1:** Ethernet και εφαρμογές

<sup>4</sup> Το τελευταίο σκέλος της παροχής σύνδεσης από έναν πάροχο επικοινωνιών σε έναν πελάτη ονομάζεται «First mile» από την οπτική γωνία του πελάτη και «Last mile» από την οπτική γωνία του παρόχου.



<b>Ethernet συνδυασμένο με τεχνολογία μεταφοράς Layer 1</b>	<b>Περιγραφή</b>
<b>Ethernet over Fiber</b>	Ethernet στο IEEE 802.3 Layer 1
<b>Ethernet over SONET/SDH</b>	Ethernet εμφωλευμένο στο ITU-T G.8040 GFP, συνδυασμένο με SONET / SDH Virtual Concatenation (είδος πολυπλεξίας)
<b>Ethernet over PDH</b>	Ethernet εμφωλευμένο στο ITU-T G.8041 GFP, με χρήση ξεχωριστών ή συγκολλημένων T1, E1, E3 ή T3 κυκλωμάτων
<b>Ethernet over MPLS</b>	Ethernet με επικεφαλίδα MPLS χρησιμοποιούμενο με οποιαδήποτε τεχνολογία μεταφοράς Layer 1
<b>Ethernet over OTN</b>	Ethernet εμφωλευμένο στο ITU-T G.709 Digital Wrapper (είδος πολυπλεξίας)
<b>Ethernet over WDM</b>	Ethernet σε διάφορα μήκη κύματος
<b>Ethernet over dry copper pairs (χάλκινα καλώδια συνεστραμμένου ζεύγους)</b>	Ethernet εμφωλευμένο στο ITU-T G.SHDSL
<b>Ethernet over μWave</b>	Ethernet στο φάσμα μικροκυματικών συχνοτήτων

**Πίνακας 2:** Ethernet και τεχνολογίες μεταφοράς Layer 1



---

## ΚΕΦΑΛΑΙΟ 3: ΠΡΩΤΟΚΟΛΛΑ

---

### 3.1 PROVIDER BRIGDES (Q-IN-Q)

---

Στην ενότητα αυτή θα αναφερθούμε στο πρότυπο **IEEE 802.1ad**, γνωστό επίσης ως **Provider Bridges**, **stacked VLANs**, **802.1Q tunnel** ή **Q-in-Q**. Το πρωτόκολλο αυτό αποτελεί τροποποίηση του προτύπου IEEE 802.1Q, που αναφέρεται στην υποστήριξη απομονωμένων VLANs σε ένα δίκτυο Ethernet. Το Q-in-Q είχε ως σκοπό να αυξήσει τον αριθμό αυτών των VLANs, μια ουσιαστική ικανότητα για την υλοποίηση τοπολογιών Metro Ethernet. Για το λόγο αυτό, τα **Provider Bridges Networks (PBNs)** καλούνται και **Virtual Metro Area Networks, vMANs**. Η ιδέα είναι να παρέχεται στους πελάτες η δυνατότητα να λειτουργούν τα δικά τους VLANs μέσα σε ένα κοινό Ethernet δίκτυο. Με τον τρόπο αυτό, ο πάροχος υπηρεσιών ρυθμίζει μόνο ένα VLAN για τον πελάτη και ο πελάτης μπορεί, στη συνέχεια, να αντιμετωπίσει αυτό το VLAN σαν δίκτυο κορμού.

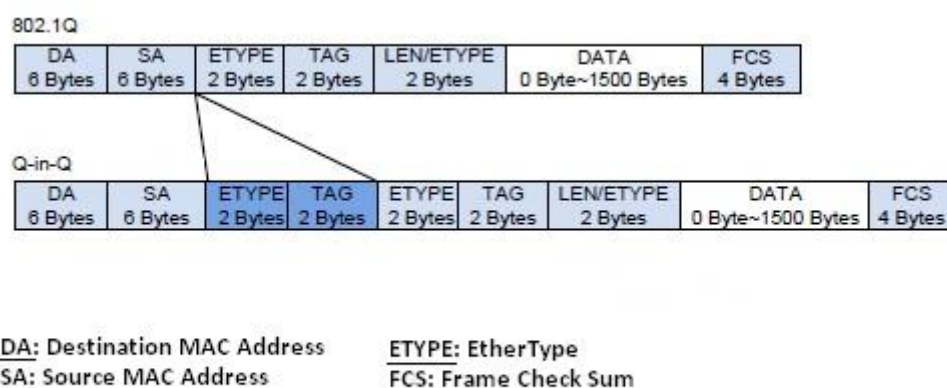
---

#### 3.1.1 ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ Q-IN-Q

---

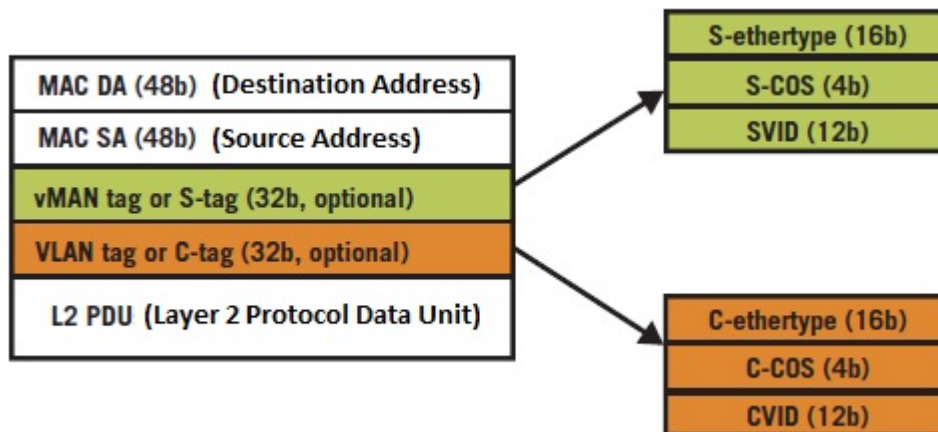
Αρχικά, πρέπει να διασαφηνίσουμε την έννοια του **VLAN tagging**, η οποία αποτελεί συστατικό στοιχείο του προτύπου 802.1Q. Πρόκειται για μια μέθοδο εντοπισμού των πακέτων που διέρχονται από συνδέσεις κορμού. Όταν ένα πλαίσιο Ethernet διασχίζει ένα σύνδεσμο κορμού, μια ειδική VLAN ετικέτα (**tag**) προστίθεται στο πλαίσιο, το οποίο πλέον αναφέρεται ως **tagged**, για να το ξεχωρίζει από τα υπόλοιπα πλαίσια που ανήκουν σε διαφορετικά VLANs. Στη συνέχεια το πλαίσιο αποστέλεται πάνω από το σύνδεσμο κορμού. Τα πλαίσια μέσα σε ένα συγκεκριμένο VLAN είναι **untagged**. Αντίστοιχα, όταν αναφερόμαστε σε κάποια θύρα ως **tagged**, εννοούμε ότι η θύρα αυτή δέχεται πλαίσια μόνο από ένα συγκεκριμένο VLAN. Αν η θύρα δέχεται πλαίσια από διαφορετικά VLANs, τότε είναι **untagged**. Οι θύρες που ανήκουν σε δίκτυο κορμού είναι **tagged**.

Η αρχική προδιαγραφή του 802.1Q επιτρέπει μόνο σε μία ετικέτα VLAN να εισάγεται στο πλαίσιο Ethernet, η οποία έχει μέγεθος 12 bits, επομένως υποστηρίζονται μόνο 4096 VLANs. Αντιθέτως, το Q-in-Q επιτρέπει σε πολλές ετικέτες VLAN να τοποθετούνται στο ίδιο πλαίσιο, γεγονός που αυξάνει εκθετικά τον αριθμό των υποστηριζόμενων VLANs. Η νέα ετικέτα προστίθεται πριν την ήδη υπάρχουσα, στη δομή του Ethernet πλαισίου και οι δύο μαζί αναφέρονται πλέον ως εξωτερική και εσωτερική αντίστοιχα.



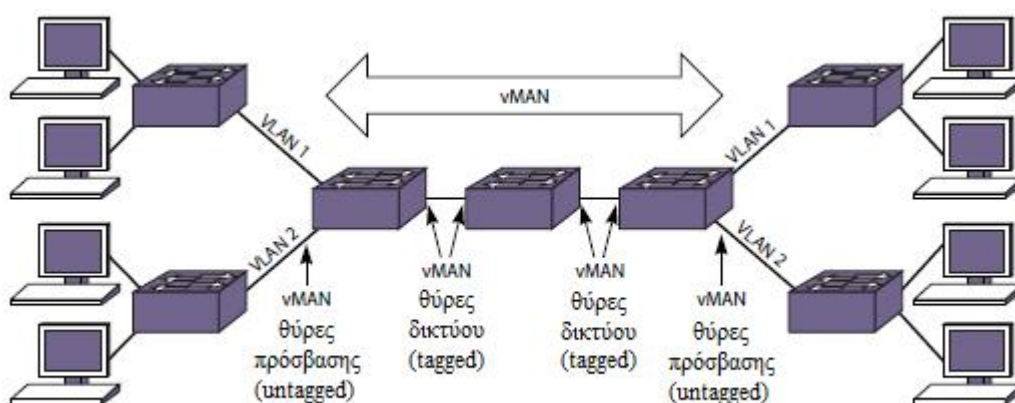
**Εικόνα 13:** Πλαίσια 802.1Q και 802.1ad (Q-in-Q)

Καθώς το Metro Ethernet εξελίσσεται, οι διαφορετικές ετικέτες μπορεί να υποδεικνύουν διαφορετικά πράγματα. Η εσωτερική ετικέτα αναφέρεται ως Customer-tag, ή αλλιώς **C-tag** και υποδεικνύει το VLAN του πελάτη, ενώ η εξωτερική ως Service-tag ή **S-tag** και χρησιμοποιείται για τη δρομολόγηση του πλαισίου μέσα στο vMAN. Κάθε ετικέτα περιλαμβάνει ένα πεδίο EtherType, bits προτεραιότητας Class of Service (CoS) και το αναγνωριστικό (ID) του VLAN/vMAN στο οποίο ανήκει το πλαίσιο.



**Εικόνα 14:** Ετικέτες Q-in-Q (ExtremeXOS 12.5.3 Concepts Guide)

Το vMAN χρησιμοποιεί Provider Bridges για να δημιουργήσει ένα δίκτυο, στο Layer 2, που υποστηρίζει vMAN κίνηση. Τα σημεία εισόδου στο vMAN είναι οι θύρες πρόσβασης των μεταγωγέων του, οι οποίες λειτουργούν ως Provider Bridges. Ο μεταγωγέας εισόδου δέχεται όλα τα tagged (C-tag) και untagged VLAN πλαίσια στις vMAN θύρες πρόσβασης και τους προσθέτει μια S-tag. Στη συνέχεια τα πλαίσια δρομολογούνται μέσα στο vMAN. Ο μεταγωγέας εξόδου δέχεται μόνο τα πλαίσια με τη σωστή S-tag, τους την αφαιρεί και τελικά, τα πλαίσια που εξάγονται από το vMAN είναι ακριβώς ίδια με αυτά που εισήχθησαν, δεδομένου ότι δεν υπήρξαν περαιτέρω ρυθμίσεις χειρισμού τους.



**Εικόνα 15:** vMAN (ExtremeXOS 12.5.3 Concepts Guide)

---

### **3.1.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ Q-IN-Q**

---

Η προσθήκη μιας δεύτερης ετικέτας στα Ethernet πλαίσια επιτρέπει λειτουργίες που δεν θα ήταν διαθέσιμες αν το πεδίο VLAN ID απλά επεκτεινόταν από 12 bit, για παράδειγμα, σε 24 ή περισσότερα. Έχοντας πολλαπλές ετικέτες, οι μεταγωγείς μπορούν πιο εύκολα να τροποποιήσουν τα πλαίσια, προσθέτοντας, αφαιρώντας ή τροποποιώντας μία ή πολλές ετικέτες.

Ο διαχωρισμός στη διαχείριση των VLAN και vMAN μειώνει την εξάρτηση της διαχείρισής τους και επιτρέπει την πραγματοποίηση ανεξάρτητων αλλαγών στο καθένα.

Τέλος, τα πλαίσια Q-in-Q είναι ένας εύκολος τρόπος κατασκευής Layer 2 tunnels ή εφαρμογής πολιτικών QoS.

---

### **3.1.3 ΥΛΟΠΟΙΗΣΕΙΣ Q-IN-Q ΔΙΑΦΟΡΩΝ ΠΡΟΜΗΘΕΥΤΩΝ**

---

Η **Extreme Networks** πραγματοποιεί Q-in-Q ενθυλάκωση με βάση τη θύρα πρόσβασης στο vMAN στην οποία καταφθάνουν πλαίσια, τα οποία μπορεί μεν να ανήκουν σε διαφορετικά VLANs και ως εκ τούτου να έχουν διαφορετικά VLAN tags (C-tags), αλλά αποκτούν την ίδια vMAN tag (S-tag). Το ίδιο συμβαίνει με τους μεταγωγείς των περισσότερων προμηθευτών δικτυακού εξοπλισμού, όπως Cisco, Juniper Networks, κ.ά.

Στους μεταγωγείς της **Huawei Networks** προσφέρεται επιπλέον η επιλογή του επονομαζόμενου «επιλεκτικού Q-in-Q». Σύμφωνα με αυτή, η συσκευή εκτελεί ταξινόμηση των δεδομένων που εισέρχονται σε μια θύρα και στη συνέχεια, αποφασίζει αν θα χρησιμοποιήσει μια εξωτερική ετικέτα για κάθε είδος κυκλοφορίας και ποια θα είναι αυτή η ετικέτα. Η ταξινόμηση των πλαισίων γίνεται σύμφωνα με:

- **VLAN ID:** Για παράδειγμα, το VLAN ID για πλοήγηση στο Internet κυμαίνεται από 101 έως 200, για την υπηρεσία IPTV από 201 έως 300, ενώ

---

για τους VIP πελάτες από 301 έως 400. Μετά την παραλαβή των δεδομένων, η κίνηση της πλοήγησης στο Internet λαμβάνει την τιμή 100 ως εξωτερική ετικέτα, της IPTV 300 και των VIP πελατών 500.

- **VLAN ID και προτεραιότητα:** Όταν ένας χρήστης χρησιμοποιεί το ίδιο VLAN ID για διάφορες υπηρεσίες, η κίνησή του μπορεί να ταξινομηθεί κατά προτεραιότητα η οποία επισημαίνεται με διαφορετικές εξωτερικές ετικέτες.
- **Διεύθυνση IP προορισμού:** Κατά την πλοήγηση στο Internet και τις υπηρεσίες φωνής, διαφορετικοί χρήστες έχουν διαφορετικές διευθύνσεις IP. Τα δεδομένα μπορούν να ταξινομηθούν μέσω μιας λίστας ελέγχου πρόσβασης (Access Control List, ACL) και στη συνέχεια να επισημανθούν με διαφορετικές εξωτερικές ετικέτες.
- **EtherType:** Για PPPoE πρόσβαση στο Internet και IPOE IPTV υπηρεσίες.

## **3.2 PROVIDER BACKBONE BRIGDES (MAC-IN-MAC)**

---

Το πρωτόκολλο **Provider Backbone Bridges (PBB)**, ή αλλιώς **MAC-in-MAC**, αρχικά δημιουργημένο από τη Nortel ως PBT (Provider Backbone Transport) και κατόπιν τυποποιημένο από τον IEEE ως **802.1ah**, είναι ένα σύνολο αρχιτεκτονικών για τη δρομολόγηση μέσα σε ένα **Provider Backbone Bridges Network (PBBN)**. Το PBBN είναι ένα δίκτυο που επιτρέπει την κίνηση vMAN (802.1ad πλαίσια) και VLAN (802.1Q πλαίσια) πάνω από ένα δίκτυο κορμού, όπως το Internet. Το πρότυπο 802.1ah αποτελεί εξέλιξη του 802.1ad (Q-in-Q).

---

### **3.2.1 ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ MAC-IN-MAC**

---

Το πρότυπο Q-in-Q, που αναλύσαμε στην προηγούμενη ενότητα, δεν προσφέρει πραγματικό διαχωρισμό μεταξύ των πελατών και των παρόχων. Είναι απλά ένας τρόπος να ξεπεραστούν οι περιορισμοί που αφορούν το μέγιστο αριθμό

των υποστηριζόμενων VLANs. Μπορεί, ωστόσο, να βοηθήσει στο διαχωρισμό των τομέων ελέγχου μεταξύ πελατών και παρόχων, όταν εμπλουτίζεται με άλλα χαρακτηριστικά, όπως ο έλεγχος των πρωτοκόλλων «σηράγγωσης» (tunneling protocols<sup>5</sup>) ή η δημιουργία γεννητικού δέντρου (spanning tree<sup>6</sup>) ανά VLAN. Υπάρχει ακόμα, όμως, το πρόβλημα του περιορισμένου ελέγχου των MAC διευθύνσεων, καθώς στο Q-in-Q η προώθηση των πλαισίων εξακολουθεί να βασίζεται στις MAC διευθύνσεις προορισμού των πελατών.

Για το λόγο αυτό, χρειάζεται περαιτέρω βελτίωση των μηχανισμών, την οποία προσφέρει το MAC-in-MAC καθιερώνοντας πλήρη διαχωρισμό μεταξύ τελικών χρηστών και παρόχων υπηρεσιών. Το PBBN επιτρέπει σε μια υπηρεσία παροχής Internet (Internet Service Provider, ISP) να δημιουργήσει ένα δίκτυο κορμού πάνω από το Internet, το οποίο υποστηρίζει κυκλοφορία Layer 2 από παρόχους υπηρεσιών (Service Providers, SPs). Κάθε SP αγοράζει ένα vMAN από τον ISP και πωλεί VLAN πρόσβαση σε πελάτες. Ο ISP ρυθμίζει το PBBN, κάθε SP ρυθμίζει το vMAN του και κάθε τελικός χρήστης το VLAN του. Τα PBBN, vMANs και VLANs είναι όλα απομονωμένα μεταξύ τους. Αντίστοιχα, όλοι οι μέτοχοι (ISP, SPs και τελικοί χρήστες) μπορούν να εγκαθιστούν τα δίκτυα και τις υπηρεσίες τους απαιτώντας ελάχιστη υποστήριξη ο ένας από τον άλλο και να πραγματοποιούν αλλαγές στις ρυθμίσεις τους ανεξάρτητα ο ένας από τον άλλο.

Υπάρχουν τρεις όροι που χρησιμοποιούνται κατά τη ρύθμιση ενός PBBN, οι **SVLAN (Service VLAN)**, **CVLAN (Customer VLAN)** και **BVLAN (Backbone VLAN)**. Καθώς το PBBN είναι μια εικονική «σήραγγα» (tunnel), τα SVLAN και CVLAN ορίζονται στα άκρα της, συγκεκριμένα στις θύρες πρόσβασης των οριακών μεταγωγέων, και καθορίζουν το είδος της κίνησης που μπαίνει και βγαίνει από αυτή (vMAN και VLAN κίνηση αντίστοιχα). Το BVLAN περιλαμβάνει τις θύρες που

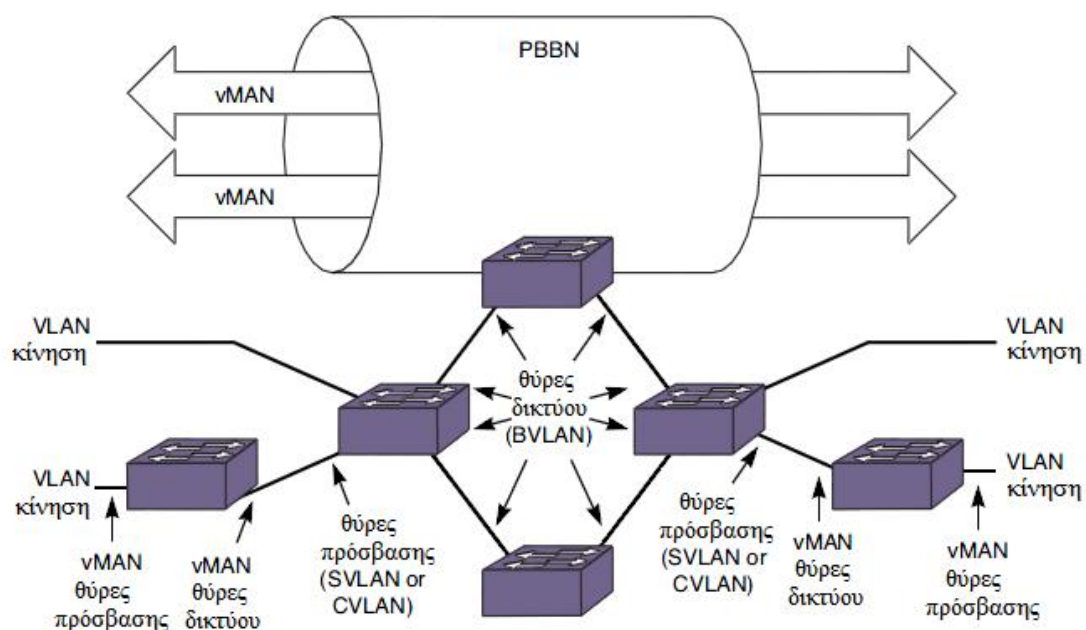
---

<sup>5</sup> Τα δίκτυα υπολογιστών χρησιμοποιούν ένα **πρωτόκολλο tunneling** όταν ένα πρωτόκολλο δικτύου εμπεριέχει ένα διαφορετικό πρωτόκολλο, μέσω του οποίου μεταφέρεται ωφέλιμο φορτίο πάνω από ένα μη συμβατό δίκτυο, ή παρέχεται ένα ασφαλές μονοπάτι μέσα από ένα μη αξιόπιστο δίκτυο.

<sup>6</sup> Στο παραδοσιακό LAN Ethernet χρησιμοποιείται το **Spanning Tree Protocol (STP)**, το οποίο δημιουργεί αυτόματα ένα «δέντρο» δρομολόγησης, αποτελούμενο από τους κόμβους του δικτύου. Κύριος στόχος του είναι η αποφυγή δημιουργίας βρόχων δρομολόγησης. Επίσης, εξασφαλίζει την ύπαρξη εναλλακτικών διαδρομών σε περίπτωση αποτυχίας.



συνδέουν τα άκρα της σήραγγας, δηλαδή τις θύρες δικτύου. Πρέπει να τονιστεί ότι οι τρεις αυτοί όροι είναι εικονικές οντότητες και όχι πραγματικοί Layer 2 domains. Χρησιμοποιούνται, απλά, για τον καθορισμό του ρόλου των θυρών του PBBN. Κάθε SVLAN και CVLAN συσχετίζονται με κάποιο BVLAN, προκειμένου να εγκαθιδρυθεί η σύνδεση μεταξύ των θυρών πρόσβασης του PBBN και των θυρών δικτύου του BVLAN. Η διαδικασία συσχετισμού ποικίλει ανάλογα με την τεχνολογία των μεταγωγέων.



**Εικόνα 16:** Provider Backbone Bridge Network (ExtremeXOS 12.5.3 Concepts Guide)

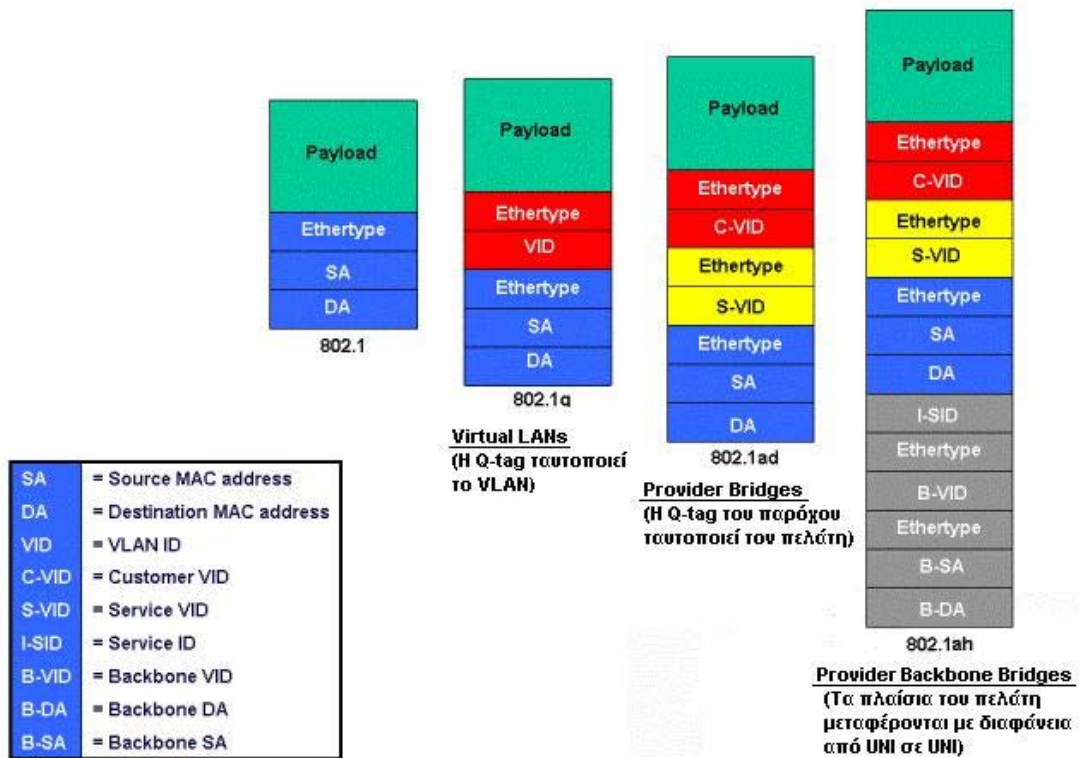
Όπως φαίνεται στην παραπάνω εικόνα, τα σημεία εισόδου στο PBBN είναι οι θύρες πρόσβασης των οριακών μεταγωγέων, οι οποίοι λειτουργούν ως οριακές γέφυρες κορμού (**Backbone Edge Bridges, BEBs**). Αυτές οι θύρες είναι σχεδιασμένες να λαμβάνουν και να μεταδίδουν vMAN και CVLAN κίνηση. Οι μεταγωγείς στους οποίους δεν έχουν ρυθμιστεί θύρες πρόσβασης, αλλά περιλαμβάνουν μόνο θύρες δικτύου, ονομάζονται κεντρικές γέφυρες κορμού (**Backbone Core Bridges, BCBs**) και διασυνδέουν τις BEBs του PBBN.

---

Το 802.1ah ορίζει μια νέα Ethernet επικεφαλίδα, η οποία μπορεί να πάρει πολλές μορφές. Οι αλλαγές σε σχέση με το Q-in-Q είναι οι παρακάτω προσθήκες:

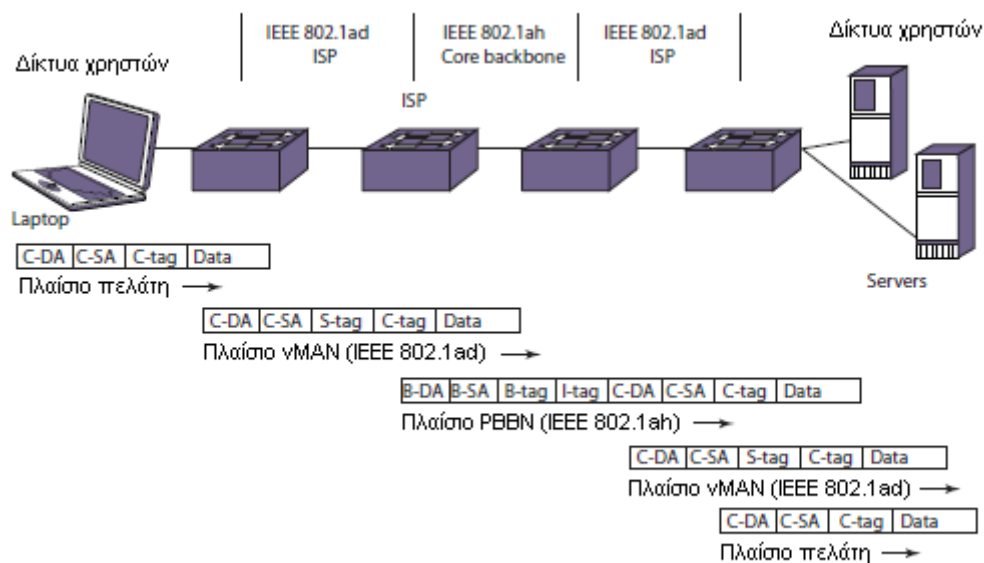
- **B-DA** (Backbone Destination MAC Address) και **B-SA** (Backbone Source MAC Address), για τη δρομολόγηση των πλαισίων μέσα στο PBBN.
- **B-VID** (Backbone VLAN ID) ή **B-tag**, για την ταυτοποίηση του BVLAN. Περιέχει πεδίο προτεραιότητας 3 bits, για Qos.
- **I-SID** (Service Instance VLAN ID) ή **I-tag**, για την ταυτοποίηση του παρόχου υπηρεσιών μέσα στο PBBN. Με άλλα λόγια, το BVLAN είναι το tunnel μέσα στο οποίο το σύστημα χρησιμοποιεί την I-tag για να ταυτοποιήσει τον πάροχο υπηρεσιών, αντιστοιχίζοντάς τη σε κάποια S-tag. Η επιπρόσθετη πληροφορία που προσφέρει η I-tag επιτρέπει την υποστήριξη πολύ περισσότερων vMANs, σε σχέση με τον αντίστοιχο αριθμό που προσφέρει η πληροφορία μόνο της S-tag. Διπλότυπα SVLANs επιτρέπονται, μόνο αν λαμβάνονται σε διαφορετικές θύρες πρόσβασης, καθώς αυτό οδηγεί σε διαφορετική I-tag για κάθε vMAN.

Συνολικά, μπορούμε να παρατηρήσουμε την εξέλιξη του Ethernet και της μορφής των πλαισίων του στην παρακάτω εικόνα.



Εικόνα 17: Εξέλιξη των πλαισίων Ethernet

Τα vMAN και VLAN πλαίσια ενσωματώνονται στο PBBN κατά τον ακόλουθο τρόπο:



Εικόνα 18: Ενσωμάτωση πλαισίων στο PBBN (ExtremeXOS 12.5.3 Concepts Guide)

Κατά την προώθηση του πλαισίου από μεταγωγέα σε μεταγωγέα, προστίθεται σε αυτό και μια νέα ετικέτα, ξεκινώντας από τους μεταγωγείς που μετασχηματίζουν τη VLAN κίνηση σε vMAN προσθέτοντας την S-tag και φτάνοντας στους μεταγωγείς του PBBN, οι οποίοι προσθέτουν τη B-tag. Κατά την έξοδο του πλαισίου από το PBBN ακολουθείται η αντίστροφη διαδικασία, δηλαδή αφαιρούνται οι επιπρόσθετες ετικέτες, έτσι ώστε το πλαίσιο να παραδίδεται στον προορισμό του έχοντας ανακτήσει την αρχική του μορφή.

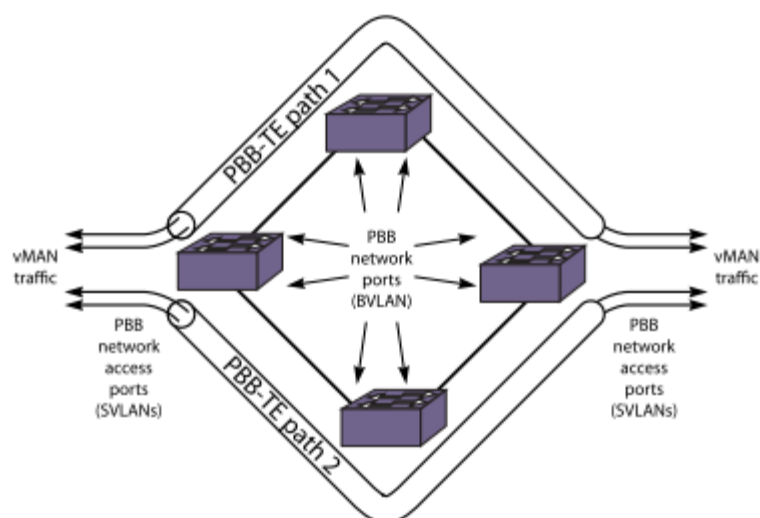
### 3.3 PROVIDER BACKBONE BRIDGE TRAFFIC ENGINEERING (PBB-TE)

Στην ενότητα αυτή θα αναφερθούμε στο πρωτόκολλο **802.1Qay, Provider Backbone Bridge Traffic Engineering (PBB-TE)**, το τελευταίο από μια σειρά προτύπων του IEEE, τα οποία αναπτύχθηκαν για να προσαρμόσουν την τεχνολογία Ethernet στα carrier δίκτυα. Το PBB-TE δημιουργήθηκε ως πιθανή αντικατάσταση των τεχνολογιών δικτύωσης που βασίζονται στα κυκλώματα μεταγωγής, όπως το SONET / SDH, και βασίστηκε σε παλαιότερο έργο, τα πρότυπα 802.1ad Provider Bridges, 802.1ah Provider Backbone Bridges και 802.1ag Connectivity Fault Management. Επίσης, πιο πρόσφατα πρότυπα, όπως τα 802.3ah «Ethernet in the First Mile» (EFM) και ITU-T Y.1731 «OAM Functions and Mechanisms», συνέβαλαν σημαντικά στη διαμόρφωση των δυνατοτήτων του Carrier Ethernet. Το PBB-TE μπορεί επίσης να παρέχει προστασία μονοπατιού παρόμοια με την υπηρεσία προστασίας UPSR (Unidirectional Path Switched Ring) στα SDH/SONET δίκτυα.

Πρέπει, τέλος, να σημειωθεί ότι το κυριότερο μέρος του πειράματος που διεξάχθηκε στα πλαίσια αυτής της διπλωματικής, στηρίχθηκε στη λειτουργικότητα του PBB-TE.

### 3.3.1 ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ PBB-TE

Το PBB-TE χρησιμοποιεί συνδεδεμοστρεφή τεχνολογία μεταφοράς πακέτων, επιτρέποντας τον ορισμό συγκεκριμένων μονοπατιών σε ένα δίκτυο Ethernet, τα οποία συμπεριφέρονται σαν αφιερωμένες γραμμές. Η λειτουργία του PBB-TE βασίζεται στις πολυεπίπεδες VLAN ετικέτες και στην ενθυλάκωση MAC-in-MAC, που ορίζεται στο πρότυπο IEEE 802.1ah, καθώς σε κάθε εισερχόμενο πακέτο στο δίκτυο ενσωματώνεται μια επιπρόσθετη Ethernet επικεφαλίδα, η οποία χρησιμοποιείται για τη δρομολόγησή του μέσα στο PBBN και αφαιρείται κατά την έξοδο του πακέτου από αυτό.



Εικόνα 19: PBB-TE (ExtremeXOS 12.5.3 Concepts Guide)

Κάθε PBB-TE διαδρομή είναι ένα στατικό μονοπάτι μέσω ενός PBBN. Αν ένα vMAN συσχετίζεται με ένα PBB-TE μονοπάτι, τα πλαίσιά του ακολουθούν πάντα την ίδια διαδρομή προς τον προορισμό τους. Αυτή είναι και η ειδοποιός διαφορά με το PBB, όπου σε ανάλογη περίπτωση, τα πλαίσια του vMAN δρομολογούνται βάσει της ρύθμισης κάθε μεταγωγέα του PBBN. Μεταξύ δύο ίδιων οριακών σημείων του δικτύου είναι δυνατό να ορίζονται πολλά διαφορετικά μονοπάτια, πράγμα που συμβάλλει στην προστασία του δικτύου, διότι σε περίπτωση

που ένα μονοπάτι αποτύχει, η κίνηση μεταφέρεται σε ένα άλλο μονοπάτι, για να αποκατασταθεί η σύνδεση. Σε αντίθεση με τους μηχανισμούς αυτορύθμισης και αυτοϊασης του Ethernet, οι οποίοι υποστηρίζονται από τα πρωτόκολλα MSTP (Multiple Spanning Tree Protocol), STP (Spanning Tree Protocol) και SPB (Shortest Path Bridging), το PBB-TE βασίζεται σε ένα εξωτερικό σύστημα πρόβλεψης, το οποίο περιλαμβάνει έλεγχο εισόδου και λειτουργίες δέσμευσης εύρους ζώνης, προκειμένου να καθοριστεί ένας συγκεκριμένος πίνακας δρομολόγησης.

Μια κίνηση που συσχετίζεται με ένα μονοπάτι PBB-TE, ταυτοποιείται από ένα **I-SID** (Service Instance VLAN ID). Κάθε PBB-TE μονοπάτι ταυτοποιείται από μια τριάδα: **B-SA** (Backbone Source MAC Address), **B-DA** (Backbone Destination MAC Address) και **B-VID** (Backbone VLAN ID). Τα δύο πρώτα αναγνωριστικά αφορούν τις MAC διευθύνσεις των άκρων του μονοπατιού, ενώ το τελευταίο χρησιμοποιείται για να ξεχωρίσουμε διαφορετικά μονοπάτια μεταξύ δύο ίδιων άκρων. Οι γέφυρες στα όρια του μονοπατιού αντιστοιχίζουν τα πλαίσια σε και από μια I-SID, ενώ παράλληλα είναι επιφορτισμένες με την εκτέλεση των λειτουργιών ενσωμάτωσης και αποκοπής των ετικετών. Οι ενδιάμεσες γέφυρες λειτουργούν ως κόμβοι μεταφοράς.

Κάθε γέφυρα περιέχει μια **Βάση Δεδομένων Προώθησης (Forwarding Data Base, FDB)**. Κάθε εγγραφή της FDB συνίσταται από τη MAC διεύθυνση της συσκευής, ένα αναγνωριστικό της θύρας στην οποία παραλήφθηκε το πλαίσιο, το VLAN στο οποίο ανήκει, την παλαιότητα της εγγραφής και κάποιες άλλες πληροφορίες. Τα πλαίσια με MAC διευθύνσεις προορισμού που δεν υπάρχουν στην FDB στέλνονται προς όλα τα μέλη του VLAN.

Οι εγγραφές της FDB διακρίνονται σε στατικές και δυναμικές. Οι **δυναμικές εγγραφές** δημιουργούνται ύστερα από εξέταση των πακέτων, προκειμένου να προσδιοριστεί η MAC διεύθυνση, η θύρα και το VLAN από όπου προέρχονται. Ο μεταγωγέας, στη συνέχεια, δημιουργεί ή ενημερώνει μια εγγραφή για τη συγκεκριμένη MAC διεύθυνση. Αρχικά, όλες οι καταχωρήσεις στην FDB είναι δυναμικές, με εξαίρεση ορισμένες που δημιουργούνται από το μεταγωγέα κατά την εκκίνηση. Εγγραφές που δεν έχουν χρησιμοποιηθεί για κάποιο χρονικό διάστημα (π.χ. λόγω αφαίρεσης από το δίκτυο της συσκευής με την οποία σχετίζονται) διαγράφονται από την FDB. Αυτό εμποδίζει την βάση από το να γίνει πλήρης από παρωχημένες καταχωρήσεις.

Οι **στατικές εγγραφές** δεν «γερνούν» και δεν ενημερώνονται μέσω της διαδικασίας ανακάλυψης MAC διευθύνσεων (MAC learning). Αντιθέτως, θεωρούνται μόνιμες, επειδή διατηρούνται στη βάση δεδομένων όταν ο μεταγωγέας αρχικοποιείται ή ενεργοποιείται/απενεργοποιείται. Μια στατική εγγραφή διατηρείται ακριβώς όπως δημιουργήθηκε. Καταστάσεις που οδηγούν στην ενημέρωση δυναμικών εγγραφών, όπως αλλαγές στις ρυθμίσεις του VLAN ή των θυρών, δεν επηρεάζουν στατικές εγγραφές.

Ο καθορισμός των PBB-TE μονοπατιών και η δρομολόγηση των πακέτων γίνεται δημιουργώντας στατικές εγγραφές στην FDB. Για να εξασφαλίσουμε ότι δε θα υπάρξουν βρόχοι δρομολόγησης και θα ακολουθηθεί η επιλεγμένη από το διαχειριστή του δικτύου διαδρομή, οι εξής ενέργειες είναι απαραίτητες:

- Απενεργοποίηση της ανακάλυψης MAC διευθύνσεων σε όλες τις θύρες των μεταγωγέων κατά μήκος της διαδρομής, έτσι ώστε ο μεταγωγέας να μη μπορεί να μάθει και να επιλέξει άλλες διαδρομές
- Απενεργοποίηση του αλγόριθμου «πλημμύρας» (flooding<sup>7</sup>), έτσι ώστε όλη η κίνηση να περιορίζεται στο επιλεγμένο μονοπάτι
- Οποιαδήποτε εισερχόμενα broadcast ή multicast πλαίσια, είτε απορρίπτονται είτε ενσωματώνονται στο μονοπάτι ως unicast, ενώ όλα τα πακέτα με προορισμό μια άγνωστη MAC διεύθυνση απορρίπτονται.

Η χειροκίνητη πρόβλεψη των μονοπατιών είναι μέχρι στιγμής ο κανόνας. Στο μέλλον, όμως, αναμένεται ότι θα προστεθεί στο PBB-TE ένα επίπεδο ελέγχου GMPLS (Generalized Multi-Protocol Label Switching), ώστε να υποστηρίξει το NOC με αυτοματοποιημένα εργαλεία ελέγχου, όπως ανακάλυψη τοπολογίας, σηματοδότηση και αναγνώριση πορείας.

---

<sup>7</sup> Το **flooding** είναι ένας απλός αλγόριθμος δρομολόγησης στον οποίο κάθε εισερχόμενο πακέτο στέλνεται μέσω κάθε σύνδεσμου του δικτύου.

---

### 3.3.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ PBB-TE

---

Σε σύγκριση με το PBB και τους προκατόχους του, το PBB-TE διαθέτει περισσότερο προβλέψιμη συμπεριφορά, η οποία ελέγχεται ευκολότερα από το χειριστή του δικτύου, διότι δίνει τον απόλυτο έλεγχο πάνω στο μονοπάτι του PBBN. Το αντίτιμο είναι η απαίτηση να ρυθμίζεται εκ των προτέρων κάθε γέφυρα, κατά μήκος του μονοπατιού δρομολόγησης. Το PBB-TE επεκτείνει τη λειτουργικότητα του PBB, προσθέτοντας συνδεοστρεφή λειτουργία, με τη χρήση point-to-point συνδέσεων, η οποία προσφέρει ανθεκτικότητα και ρυθμιζόμενα επίπεδα απόδοσης. Γνωρίζοντας τις ακριβείς διαδρομές στις οποίες «συμμετέχει» κάθε σύνδεσμος, θύρα ή δικτυακή συσκευή, καθώς και τη χωρητικότητά τους, είναι δυνατό να ρυθμίσουμε το φόρτο εργασίας σε κάθε σημείο του δικτύου και κατ'αυτό τον τρόπο να εγγυηθούμε επίπεδα απόδοσης (QoS) υπό τις χειρότερες συνθήκες. Κάτι τέτοιο δεν είναι εφικτό σε ασυνδεσμικά δίκτυα μεταγωγής πακέτων, όπως το IP και το MAC-learning Ethernet.

Ελαχιστοποιώντας τις πολλαπλές μεταδόσεις και το flooding και χρησιμοποιώντας στη θέση τους μόνο συγκεκριμένες, διαμορφωμένες από το διαχειριστή του δικτύου, απαλλαγμένες από βρόχους διαδρομές προώθησης, εξαλείφεται η ανάγκη χρήσης του STP. Συνεπώς, ένα PBB-TE μονοπάτι παρέχει μεγαλύτερο εύρος ζώνης, επειδή η επιβάρυνση του δικτύου και του επεξεργαστή, που προκαλείται εξαιτίας του flooding και άλλων διαδικασιών του επιπέδου μεταφοράς, είναι μικρότερη. Επίσης, η απόρριψη των πακέτων με άγνωστες MAC διευθύνσεις προορισμού καθιστά τη σύνδεση πολύ πιο σταθερή και ασφαλή σε WAN περιβάλλον.

Το PBB-TE χρησιμοποιεί απλούς, αλλά υψηλής απόδοσης, μεταγωγείς Ethernet στον πυρήνα του, οι οποίοι, αν και πολύ πιο προχωρημένοι από τον μέσο LAN μεταγωγέα, επωφελούνται από το ίδιο θεμελιώδες μοντέλο χαμηλού κόστους. Αυτό τους καθιστά ανταγωνιστικότερους από τον παραδοσιακό SONET/SDH σταυρό ή τους IP/MPLS δρομολογητές με παρόμοια απόδοση.

Άλλα πλεονεκτήματα του PBB-TE είναι η δυνατότητα Ethernet tunneling με πλήρη διαλειτουργικότητα με το MPLS και η ανεξαρτησία επιπέδων υπηρεσιών και



---

μεταφοράς (στο εσωτερικό του tunnel μπορούμε να έχουμε υπηρεσίες Ethernet, IP, MPLS pseudo-wires, ή VPLS).

Οι carrier υπηρεσίες μεταναστεύουν γρήγορα από το Frame Relay, το ATM και τις μισθωμένες γραμμές TDM προς τις ισοδύναμες Ethernet υπηρεσίες. Αν και η ικανότητα του PBB-TE να υποστηρίζει εγγενώς αυτές τις υπηρεσίες είναι ένα σημαντικό πλεονέκτημα, δεν είναι αυτός ο κύριος λόγος για τον οποίο επιλέγεται ως Carrier Ethernet δίκτυο μεταφοράς. Στην πραγματικότητα, η συνταγή της επιτυχίας του στο χώρο των επιχειρήσεων είναι η ίδια με αυτή του Ethernet: χαμηλό κόστος κατασκευαστικών στοιχείων και δυνατότητα ευέλικτης, βασισμένης σε βιομηχανικά πρότυπα, υποστήριξης ενός ευρέως φάσματος υπηρεσιών.

Αν και ακόμα «στα σπάργανα», αεροπορικές εταιρείες σε Ευρώπη και ΗΠΑ έχουν εκδηλώσει ενδιαφέρον να περιλαμβάνουν τα μελλοντικά σχέδιά τους PBB-TE λειτουργικότητα. Αν η υιοθέτηση αποδειχθεί τόσο ισχυρή όσο το αρχικό ενδιαφέρον, πολλοί αναλυτές πιστεύουν ότι το PBB-TE θα γίνει ένα τεχνολογικό πρότυπο για πολλές από τις μεγαλύτερες υποδομές αερομεταφορών στον κόσμο.

---

### ***3.3.3 PBB-TE VS MPLS***

---

Το πρωτόκολλο **MPLS (Multi Protocol Label Switching)** παρέχει ένα μηχανισμό για τη δρομολόγηση των πακέτων και τη διασφάλιση της ποιότητας των υπηρεσιών (QoS) σε δίκτυα κορμού. Αναπτύχθηκε στα τέλη της δεκαετίας του 1990 για να προσφέρει ταχύτερη προώθηση των πακέτων στους IP δρομολογητές (RFC 3031). Από τότε, οι δυνατότητές του έχουν επεκταθεί μαζικά. Για παράδειγμα, υποστηρίζει τη δημιουργία εικονικών ιδιωτικών δικτύων (VPNs), τη διαμόρφωση της δικτυακής κίνησης, τη διασύνδεση δικτύων και την αυξημένη ανθεκτικότητα. Για τους λόγους αυτούς είναι πλέον de facto πρότυπο για πολλά δίκτυα μεταφοράς και παροχής υπηρεσιών και τα σενάρια εξέλιξής του αυξάνονται.

Υπήρξε μια παρανόηση ότι ο MPLS είναι απαραίτητος για την υλοποίηση ενός Carrier Ethernet δικτύου. Αυτό οφείλεται, εν μέρει, στο γεγονός ότι αρχικά οι πάροχοι υπηρεσιών χρησιμοποιούσαν μεταγωγείς Ethernet στις πρώτες Carrier

Ethernet εφαρμογές τους. Οι υπηρεσίες που προσφέρονταν κατ'αυτό τον τρόπο παρείχαν μεγαλύτερο εύρος ζώνης και πιο ευέλικτες επιλογές συνδεσιμότητας από τις υπόλοιπες τεχνολογίες. Παρ'όλα αυτά, η απόδοσή τους δεν ήταν καλύτερη αναλογικά, επομένως δεν ανταποκρίνονταν στις απαιτήσεις των πελατών και έδωσαν ένα «κακό όνομα» στο Carrier Ethernet. Συνεπώς, ο MPLS χρησιμοποιήθηκε για τη βελτίωση αυτών των πρώιμων δικτύων Carrier Ethernet, φέρνοντας μια σειρά από χρήσιμες δυνατότητες, όπως η γρήγορη αναδρομολόγηση, η οποία μειώνει σημαντικά την ανάγκη προστασίας τμημάτων του δικτύου και τους χρόνους αποκατάστασης, και το VPLS (Virtual Private LAN Service), που αυξάνει την κλιμακωσιμότητα που απαιτείται σε μητροπολιτικά δίκτυα με μεγάλο αριθμό συνδρομητών.

Σήμερα, οι Carrier Ethernet τεχνολογίες και τα πρότυπά τους μπορούν πλέον να προσφέρουν την απόδοση και την κλιμακωσιμότητα που κάποτε ήταν διαθέσιμες μόνο μέσω της χρήσης του MPLS. Τα πρωτόκολλα PBB και PBB-TE, αν και πολύ νεότερα από τον MPLS, παρουσιάζονται ως μια φθηνότερη και λιγότερο πολύπλοκη εναλλακτική λύση για την υλοποίηση μητροπολιτικών δικτύων και δικτύων πρόσβασης. Εν τω μεταξύ, άλλες εναλλακτικές λύσεις, όπως ο T-MPLS (Transport Multi Protocol Label Switching), έχουν επίσης προκύψει.

Η επιλογή της υλοποίησης Carrier Ethernet δικτύου βασισμένο στο Ethernet ή στο MPLS εξαρτάται από τις εκάστοτε συνθήκες. Παραδείγματος χάριν, αν η δικτυακή κίνηση είναι κατά βάση κίνηση Ethernet, η Ethernet προσέγγιση είναι προφανώς προτιμότερη και απαιτεί μικρότερο λειτουργικό κόστος. Αντιθέτως, όταν έχουμε συνδυασμό δικτύων που υλοποιούν διαφορετικές τεχνολογίες μεταφοράς, προτιμάται η προσέγγιση με MPLS, δεδομένης της ικανότητάς του να υποστηρίζει πολλούς τύπους κίνησης. Η ικανότητα αυτή είναι γνώρισμα και τεχνολογιών με βάση το Ethernet αλλά χωρίς να επιτυγχάνουν τα υψηλά επίπεδα απόδοσης του MPLS, που διαθέτει περισσότερη εμπειρία στο θέμα αυτό λόγω της μακράς ιστορίας του.

Η καινοτομία της Nortel, όσον αφορά το PBT και τη μετεξέλιξή του σε PBB-TE, οδήγησε μια ταχέως αναπτυσσόμενη ομάδα ομοϊδεατών της προμηθευτών (Extreme Networks, Fujitsu Network Communications, Hammerhead Systems, Meriton Networks και Soapstone Networks) να ακολουθήσουν το παράδειγμά της, εγκαινιάζοντας το δικό τους PBT εξοπλισμό και προκαλώντας ανάφλεξη του ενδιαφέροντος σε όλο το βιομηχανικό κλάδο. Το PBT έχει ήδη υιοθετηθεί και από

---

ορισμένες ανεξάρτητες εταιρίες, όπως η Dakota Carrier Network και η Frontier Communications.

Αξίζει να σημειωθεί ότι σε αρκετές περιπτώσεις παρατηρείται περισσότερο ενδιαφέρον για τον «πρόγονο» του PBB-TE, το PBB, παρά για το ίδιο. Η Alcatel-Lucent, καθιερωμένος προμηθευτής MPLS εξοπλισμού για MANs, έμεινε αρχικά προσηλωμένη στις θέσεις τις και απέφυγε την υλοποίηση PBB-TE. Αργότερα, όμως, προσέθεσε PBB λειτουργικότητα στους 7450 ESS μεταγωγείς της, συνδυάζοντάς τη με υπηρεσίες VPLS και MPLS. Η Foundry Networks, επίσης, προσέθεσε το PBB στον εξοπλισμό της, με τρόπο λιγότερο εξαρτημένο από το MPLS, σε σχέση με την υλοποίηση της Alcatel. Η Verizon ξεκίνησε εργαστηριακά πειράματα στο μεταγωγέα Metro Ethernet Routing Switch 8600 της Nortel, για να εξακριβώσει αν οι PBB δυνατότητες θα μπορούσαν να επεκτείνουν και να διαφοροποιήσουν τις Carrier Ethernet υπηρεσίες, διατηρώντας ωστόσο επιφυλάξεις για την αποτελεσματικότητα του PBB-TE.

Σε γενικές γραμμές μπορούμε να πούμε ότι σήμερα το PBB-TE δεν είναι συντριπτικά δημοφιλές έναντι του παραδοσιακά χρησιμοποιούμενου MPLS, αλλά κερδίζει γρήγορα έδαφος. Στον πίνακα που ακολουθεί παρουσιάζεται η υποστήριξη PBB-TE ή MPLS διαφόρων προμηθευτών.

Vendor	MPLS Layer 2 Transport	MPLS Layer 3 Transport	PBB-TE	T-MPLS
Atrica	Yes	No	No	No, but offers a similar proprietary implementation
Alcatel-Lucent	Yes	Yes	No	Yes
Ciena	Yes	Yes	Yes	No
Cisco Systems	Yes	Yes	Investigating	No
ECI Telecom	Yes	No	No	Yes
Ericsson (Redback)	Yes	Yes	No	Yes
Extreme Networks	Yes	No	Yes	No
Foundry Networks	Yes	Yes	No	No
Juniper Networks	Yes	Yes	No	No
Nokia Siemens Networks	Yes	Yes	Yes	Not believed to support
Nortel Networks	Yes (over Ethernet PSN)	Yes (in ATM/FR MSS)	Yes	No
Tellabs	Yes	Yes	Yes	Yes
Telco Systems	Yes	Yes	Soon	No
World Wide Packets	Yes (in demarcation devices)	Yes (in demarcation devices)	Yes	No

**Πίνακας 3:** Υλοποιήσεις MPLS/PBB-TE διαφόρων προμηθευτών (Light Reading Insider, 2007)

### 3.4 OPERATION ADMINISTRATION AND MAINTENANCE (OAM)

Σε αυτή την ενότητα θα ασχοληθούμε με τη **λειτουργία, διαχείριση και συντήρηση (Operation Administration and Maintenance, OAM)** ενός Ethernet δικτύου, δηλαδή τις διαδικασίες που επιτελούνται για την ανίχνευση βλαβών του δικτύου, τη μέτρηση της απόδοσης και τη διανομή πληροφοριών που σχετίζονται με

τα σφάλματα. Μέχρι πρόσφατα το Ethernet δεν είχε OAM λειτουργίες, όπως το SONET/SDH ή το ATM, και ως εκ τούτου δεν χαρακτηριζόταν ως «carrier class». Τώρα έχει αποκτήσει δύο τύπους OAM, που έχουν αναπτυχθεί αφενός από το ITU και το IEEE, και αφετέρου από το EFM (Ethernet in the First Mile). Ο πρώτος τύπος διαθέτει ένα πλήρως εξοπλισμένο μηχανισμό OAM που λειτουργεί κατά μήκος ολόκληρου του δικτύου και περιλαμβάνει όλα τα παραδοσιακά στοιχεία OAM όπως ειδοποίηση σήματος συναγερμού (Alarm Indication Signal, AIS), ειδοποίηση απομακρυσμένου ελαττώματος (Remote Defect Indication, RDI) και μέτρηση της απόδοσης. Ο δεύτερος τύπος, γνωστός ως 802.3ah ή OAM Layer 2, περιορίζεται στη συνεχή παρακολούθηση ενός συνδέσμου και απευθύνεται σε εφαρμογές πρόσβασης. Καθώς ο πρώτος τύπος προστατεύει το επίπεδο υπηρεσιών και ο δεύτερος το φυσικό επίπεδο, οι δύο μπορούν να λειτουργήσουν συμπληρωματικά. Ωστόσο, δεν είναι σαφές γιατί υπάρχει ανάγκη για δύο διαφορετικά πρότυπα.

Το πρωτόκολλο που αναπτύχθηκε από το IEEE είναι το **802.1ag**, γνωστό και ως **Διαχείριση Συνδεσιμότητας και Σφαλμάτων (Connectivity Fault Management, CFM)**. Τα μητροπολιτικά και εθνικά δίκτυα περιλαμβάνουν πολλούς ανεξάρτητους παρόχους υπηρεσιών, καθένας με περιορισμένη πρόσβαση στον εξοπλισμό διαχείρισης του άλλου. Αυτό το πρότυπο παρέχει δυνατότητες για την ανίχνευση, τον έλεγχο και την απομόνωση των αποτυχιών σύνδεσης των δικτύων αυτών. Το 802.1ag είναι σε μεγάλο βαθμό ταυτόσημο με το πρωτόκολλο ITU-Y.1731.

Το OAM διασφαλίζει την τήρηση των εγγυήσεων QoS, την ανίχνευση ανωμαλιών πριν επεκταθούν και την απομόνωση ή παράκαμψη των ελαττωμάτων του δικτύου. Η λειτουργία των δικτύων χωρίς OAM απαιτεί πολύ περισσότερους πόρους για τη συνεχή χειρωνακτική παρέμβαση για την ανίχνευση λαθών, καθώς τα MANs και WANs εκτείνονται σε αποστάσεις εκατοντάδων ή χιλιάδων μιλίων, επομένως η αποκατάστασή τους δεν είναι απλά μια σύντομη βόλτα ενός τεχνικού στο χώρο καλωδίωσης ή δικτύωσης, όπως θα συνέβαινε με ένα LAN στα πλαίσια ενός κτιρίου. Έχει, επομένως, ιδιαίτερη σημασία η δυνατότητα εξ'αποστάσεως διάγνωσης των προβλημάτων του δικτύου.

---

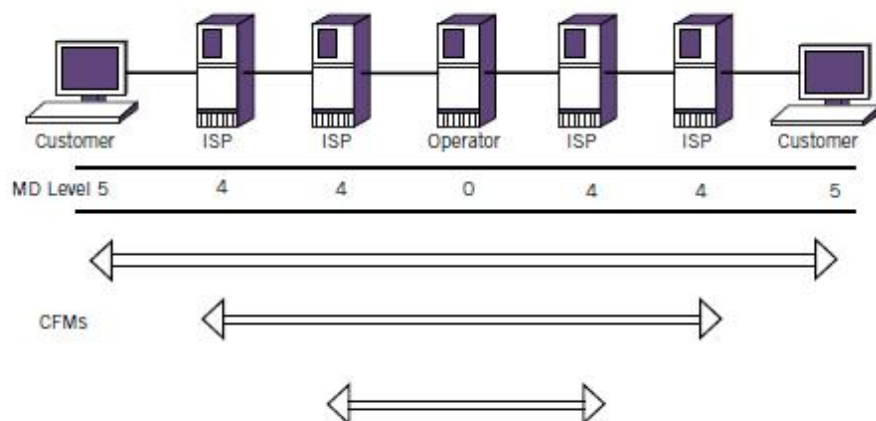
### 3.4.1 ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ ΟΑΜ

---

Κάθε στρώμα ενός πολυεπίπεδου δικτύου χρειάζεται το δικό του ΟΑΜ. Η ύπαρξη σφαλμάτων σε κάποιο στρώμα του δικτύου είναι συνήθως αντίκτυπο σφαλμάτων σε υψηλότερα στρώματα (όπως τα σφάλματα ενός διακομιστή που προκαλούν απώλεια πληροφοριών στους πελάτες) και δεν συσχετίζεται κατ'ανάγκη με σφάλματα των κατώτερων στρωμάτων.

Σε γενικές γραμμές, το πρότυπο 802.1ag καθορίζει τομείς συντήρησης, τα αντικείμενα που απαιτούνται για τη δημιουργία και τη διαχείριση τους, τη σχέση μεταξύ τους και τις υπηρεσίες που προσφέρουν και περιγράφει τα πρωτόκολλα και τις διαδικασίες που χρησιμοποιούνται για τη διάγνωση και τη διαχείριση βλαβών συνδεσιμότητας σε ένα τομέα συντήρησης. Επίσης, παρέχει τα μέσα για μελλοντική επέκταση αυτών των δυνατοτήτων.

Οι **τομείς συντήρησης (Maintenance Domains, MDs)** είναι χώροι διαχείρισης, μέσα σε ένα δίκτυο, οι οποίοι συνήθως ανήκουν και λειτουργούνται από μια ενιαία οντότητα. Κάθε MD χαρακτηρίζεται από όνομα και επίπεδο. Μεταξύ των διαφόρων MDs υπάρχει μια ιεραρχική σχέση, με βάση το επίπεδό τους. Όσο μεγαλύτερο είναι το εύρος κάθε MD, τόσο υψηλότερη είναι η τιμή του επιπέδου. Συνήθως, ο MD πελατών (customer) έχει το μεγαλύτερο εύρος, ακολουθεί ο MD των παρόχων (ISP) και τελευταίος έρχεται ο MD των διαχειριστών του δικτύου (operator). Μπορούν να υπάρχουν έως και 8 MDs σε ένα δίκτυο Ethernet, με τιμή επιπέδου 0-7.



**Εικόνα 20:** Maintenance Domains CFM (ExtremeXOS 12.5.3 Concepts Guide)

Μέσα σε κάθε MD υπάρχουν **σημεία συντήρησης (Maintenance Points, MPs)**, τα οποία διακρίνονται σε **οριακά (Maintenance End Points, MEPs)** και **ενδιάμεσα (Maintenance Intermediate Points, MIPs)**.

Ο έλεγχος της συνδεσιμότητας μέσα σε έναν MD γίνεται στο Layer 2, μέσω της ανταλλαγής μηνυμάτων που ονομάζονται **Μηνύματα Ελέγχου Συνδεσιμότητας (Connectivity Check Messages)**. Τα MEPs στέλνουν και λαμβάνουν CFM πλαίσια μέσω της λειτουργίας αναμετάδοσης, απορρίπτοντας εκείνα που προέρχονται από MDs ίδιου ή χαμηλότερου επιπέδου. Τα MIPs είναι παθητικά σημεία, ανταποκρίνονται μόνο όταν ενεργοποιούνται από CFM traceroute και loopback μηνύματα.

Το IEEE 802.1ag αποτελείται από τρία πρωτόκολλα, που συνεργάζονται για να βοηθήσουν τους διαχειριστές δικτύων Ethernet να διορθώσουν τα σφάλματα και είναι τα εξής:

- **Πρωτόκολλο ελέγχου συνέχειας (Continuity Check Protocol):** Παρέχει ένα μέσο για τον εντοπισμό προβλημάτων σύνδεσης. Τα αντίστοιχα Μηνύματα Ελέγχου Συνέχειας (Continuity Check Messages) είναι multicast, μίας κατεύθυνσης, δεν απαιτούν απάντηση και περιορίζονται στα όρια ενός MD.

Κάθε MEP μεταδίδει περιοδικά ένα τέτοιο μήνυμα προς τα υπόλοιπα MEPs του MD.

- **Εντοπισμός συνδέσμων ή διαδρομής (Link Trace ή MAC Trace Route):** Κάθε MEP μεταδίδει multicast μηνύματα για να παρακολουθήσει τη διαδρομή (hop-by-hop) προς ένα άλλο MEP. Τα MEPs που λαμβάνουν αυτά τα μηνύματα απαντούν στον αποστολέα και αναμεταδίδουν το μήνυμα. Είναι παρόμοιο στη σύλληψη με το UDP Trace Route.
- **Loopback (MAC ping):** Πρόκειται για unicast πλαίσια που εκπέμπουν τα MEPs, τα οποία αποστέλλονται πίσω στην πηγή χωρίς επεξεργασία ή τροποποίηση. Είναι παρόμοια στη σύλληψη με το πρωτόκολλο ICMP (Internet Control Message Protocol). Στέλνοντας loopback μηνύματα σε διαδοχικά MIPs, μπορούμε να καθορίσουμε τη θέση της βλάβης. Στέλνοντας μεγάλο όγκο loopback μηνυμάτων, μπορούμε να ελέγξουμε το εύρος ζώνης, την αξιοπιστία ή το jitter μιας υπηρεσίας. Σε αντίθεση με τα μηνύματα ελέγχου συνέχειας, τα loopback μηνύματα ξεκινούν και σταματούν κατά βούληση του διαχειριστή του δικτύου.

### **3.5 LINK LAYER DISCOVERY PROTOCOL (LLDP)**

---

Το **Link Layer Discovery Protocol (LLDP)** είναι ένα πρωτόκολλο που λειτουργεί στο Layer 2. Καθορίζεται από το πρότυπο **802.1ab** του IEEE και παρέχει μια τυποποιημένη μέθοδο για την ανακάλυψη φυσικών συσκευών του δικτύου και των ικανοτήτων τους, χρησιμοποιώντας Ethernet συνδεσιμότητα, μέσα σε ένα δεδομένο τομέα διαχείρισης του δικτύου. Το πρωτόκολλο αναφέρεται επίσημα από το IEEE ως «Ανακάλυψη συνδεσιμότητας σταθμών και ελέγχου μέσων πρόσβασης» (Station and Media Access Control Connectivity Discovery).



---

### 3.5.1 ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ LLDP

---

Οι δικτυακές συσκευές που υλοποιούν το LLDP είναι επαναλήπτες, γέφυρες, σημεία πρόσβασης, δρομολογητές και ασύρματοι σταθμοί. Το LLDP επιτρέπει στις συσκευές αυτές να κάνουν τα εξής:

- Διαφήμιση πληροφοριών και δυνατοτήτων της συσκευής σε άλλες συσκευές του τομέα διαχείρισης
- Λήψη και αποθήκευση πληροφοριών που λαμβάνονται από άλλες συσκευές του τομέα διαχείρισης
- Ανακάλυψη πληροφοριών που αφορούν συσκευές διαφορετικών κατασκευαστών, συμβατές με LLDP
- Ρύθμιση θυρών σε μεταγωγείς απομακρυσμένων συσκευών
- Παροχή πληροφοριών που μπορούν να χρησιμοποιηθούν για τον έλεγχο ταυτότητας και τη διαχείρισή της
- Παροχή πληροφοριών συσκευών σε συστήματα διαχείρισης δικτύων συμβατά με το πρωτόκολλο SNMP (Simple Network Management Protocol), όπως το Ridgeline, τα οποία παρουσιάζουν τις πληροφορίες αυτές σε αναφορές απογραφής και χάρτες τοπολογίας

Η LLDP πληροφορία αποστέλλεται από τις συσκευές, μέσω των διασυνδέσεών τους και σε σταθερό χρονικό διάστημα, με τη μορφή ενός πλαισίου Ethernet. Κάθε πλαίσιο περιέχει μία LLDP Μονάδα Δεδομένων (LLDP Data Unit, LLDPDU), η οποία είναι μια ακολουθία από δομές τύπου *type-length-value* (TLV). Οι υποχρεωτικές TLVs, αυτές δηλαδή που περιλαμβάνονται πάντα στην LLDPDU, είναι:

- **Chassis ID:** MAC διεύθυνση του συστήματος, χαρακτηρίζει μοναδικά τη συσκευή
- **Port ID:** θύρα από την οποία αποστέλλονται οι TLVs
- **Time-to-live (TTL):** υποδεικνύει το χρόνο διατήρησης της εγγραφής στην LLDP βάση δεδομένων, με προεπιλεγμένη τιμή 2 λεπτά. Όταν απενεργοποιείται είτε μια θύρα είτε η λειτουργία LLDP σε μια θύρα, η τιμή

του TTL γίνεται 0, το οποίο σημαίνει ότι η εγγραφή που αφορά αυτή τη θύρα πρέπει να διαγραφεί από τη βάση δεδομένων της συσκευής.

- **Τέλος της LLDPDU:** οριοθετεί το τέλος των δεδομένων σε κάθε πακέτο LLDP

Εκτός από τις υποχρεωτικές TLVs υπάρχουν και άλλες προαιρετικές, όπως το όνομα, η περιγραφή και οι δυνατότητες του συστήματος, το μέγιστο υποστηριζόμενο μέγεθος πλαισίου, στοιχεία του VLAN στο οποίο ανήκει η συσκευή (όνομα, θύρες) κ.ά. Το πλήθος και το είδος των προαιρετικών TLVs ποικίλουν ανάλογα με τον κατασκευαστή.

Η πληροφορία που συγκεντρώνεται με τη χρήση του LLDP αποθηκεύεται στη Βάση Δεδομένων Πληροφοριών Διαχείρισης (**Management Information Base, MIB**). Κάθε δικτυακή συσκευή διαθέτει τη δική της MIB.

Το **Media Discovery Endpoint (MED)** αποτελεί βελτίωση του LLDP και παρέχει επιπλέον τις ακόλουθες υπηρεσίες:

- Αυτόματη ανακάλυψη των πολιτικών LAN, όπως VLAN, ρυθμίσεις προτεραιότητας και διαφοροποιημένες υπηρεσίες (Diffserv).
- Ανακάλυψη θέσης συσκευής για τη δημιουργία βάσεων δεδομένων θέσης και ενισχυμένες υπηρεσίες έκτακτης ανάγκης, στην περίπτωση του Voice over IP (VoIP).
- Εκτεταμένη και αυτοματοποιημένη διαχείριση ενέργειας (Power over Ethernet, PoE).
- Διαχείριση αποθεμάτων, επιτρέποντας στους διαχειριστές του δικτύου να παρακολουθούν τις συσκευές του δικτύου τους και να καθορίζουν τα χαρακτηριστικά τους (κατασκευαστής, εκδόσεις λογισμικού και υλικού, σειριακό αριθμό).

Το LLDP-MED εγκρίθηκε επίσημα και δημοσιεύτηκε από το ANSI/TIA-1057 Telecommunications Industry Association (TIA) τον Απρίλιο του 2006.

---

### 3.5.2 ΙΔΙΟΚΤΗΤΑ ΠΡΩΤΟΚΟΛΛΑ ΑΝΑΚΑΛΥΨΗΣ ΤΟΠΟΛΟΓΙΑΣ ΔΙΚΤΥΟΥ

---

Το ιδιόκτητο πρωτόκολλο ανακάλυψης τοπολογίας δικτύου της εταιρείας Nortel, το οποίο έχει προσφάτως υιοθετηθεί και από τις Avaya και Ciena, είναι το **Nortel Discovery Protocol (NDP)**. Οι σχετικές πληροφορίες παρουσιάζονται γραφικά με το λογισμικό Avaya Enterprise Switch Manager. Το NDP έχει τις ρίζες του στο SynOptics Network Management Protocol (SONMP), που αναπτύχθηκε από τις εταιρείες SynOptics και Wellfleet, οι οποίες συγχωνεύτηκαν το 1994. Το SONMP επανατυποποιήθηκε ως Bay Network Management Protocol (BNMP ή BDP). Τέσσερα χρόνια αργότερα, το 1998, η Bay Networks εξαγοράστηκε από τη Nortel και το SONMP μετονομάστηκε σε NDP. Ενδεχόμενη είναι μια μελλοντική αλλαγή σε Avaya Discovery Protocol (ADP).

Η Cisco διαθέτει το **Cisco Discovery Protocol (CDP)** για την ανταλλαγή πληροφοριών μεταξύ του συνδεδεμένου εξοπλισμού της, όπως η έκδοση του λειτουργικού συστήματος ή η διεύθυνση IP. Το CDP μπορεί επίσης να χρησιμοποιηθεί για τη δρομολόγηση On-Demand, που είναι μια μέθοδος κατά την οποία οι πληροφορίες δρομολόγησης συμπεριλαμβάνονται στα CDP πακέτα, έτσι ώστε να μην χρησιμοποιούνται πρωτόκολλα δυναμικής δρομολόγησης στα απλά δίκτυα. Επειδή το CDP λειτουργεί σε Ethernet, ATM και Frame Relay συνδέσεις, είναι ανεξάρτητο από το πρωτόκολλο δικτύου που χρησιμοποιείται (π.χ. TCP/IP, Internetwork Packet Exchange, AppleTalk, κλπ.).

Οι συσκευές Cisco στέλνουν CDP πακέτα στη multicast διεύθυνση προορισμού 01-00-0c-cc-cc-cc, προς κάθε συνδεδεμένη διεπαφή. Αυτά τα multicast πακέτα μπορούν να ληφθούν από μεταγωγείς Cisco αλλά και άλλες συσκευές που υποστηρίζουν το CDP. Κάθε συσκευή που υποστηρίζει το CDP αποθηκεύει τις πληροφορίες που έλαβε από άλλες συσκευές σε έναν πίνακα, ο οποίος προβάλλεται με την εντολή *show cdp neighbors*. Αυτός ο πίνακας είναι επίσης προσβάσιμος μέσω SNMP. Οι πληροφορίες του πίνακα ανανεώνονται κάθε φορά που λαμβάνεται ένα CDP πακέτο. Η παράμετρος **holdtime** καθορίζει τη διάρκεια ζωής μιας καταχώρησης του πίνακα, αναλογικά με την παράμετρο TTL.

Τα CDP πλαίσια έχουν τη μορφή type-length-value (TLV) και οι πληροφορίες που περιέχουν ποικίλλουν ανάλογα με τον τύπο της συσκευής και την έκδοση του λειτουργικού συστήματος. Περιλαμβάνουν συνήθως την έκδοση του λειτουργικού συστήματος, το όνομα, τον τύπο και το μοντέλο της συσκευής, όλες τις διευθύνσεις από όλα τα πρωτόκολλα που ισχύουν στη θύρα όπου αποστέλλεται το CDP πλαίσιο, το αναγνωριστικό της θύρας από την οποία στάλθηκε το CDP πλαίσιο κ.ά.

Η Extreme Networks υποστηρίζει το LLDP αλλά και το δικό της **Extreme Discovery Protocol (EDP)**, ενώ η Enterasys Networks διαθέτει το **Cabletron Discovery Protocol**.

---

### **3.5.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ LLDP**

---

Ένα πράγμα βέβαιο, όσον αφορά το επίπεδο πρόσβασης ενός δικτύου, είναι το γεγονός ότι ο αριθμός και η πολυπλοκότητα των συσκευών που υπάρχουν σε αυτό το επίπεδο θα συνεχίσουν να παρουσιάζουν ταχεία ανάπτυξη. Αυτή η εκθετική αύξηση του αριθμού των συσκευών που απαιτούν συνδεσιμότητα LAN οφείλεται σε μεγάλο βαθμό στη διάδοση νέων εφαρμογών, όπως η IP τηλεφωνία και η ασύρματη πρόσβαση. Ο ανοικτός χαρακτήρας του LLDP αποτελεί θεμέλιο για την από κοινού ανάπτυξη νέων επιπρόσθετων λειτουργιών για την ανακάλυψη συσκευών, πράγμα το οποίο θα βοηθήσει την υλοποίηση νέων εφαρμογών και υπηρεσιών Ethernet στο μέλλον.

Τα πλεονεκτήματα που προκύπτουν από τη χρήση του LLDP είναι:

- **Χαμηλότερο κόστος λειτουργίας**, λόγω αύξησης της αυτοματοποίησης. Η διαχείριση και η συντήρηση του δικτύου απλουστεύονται, ως αποτέλεσμα της ενοποίησης των εργαλείων διαχείρισης και της αυτοματοποίησης των διαδικασιών διάγνωσης και ελέγχου συνέπειας. Επίσης, η αυτοματοποιημένη ανακάλυψη των συσκευών πρόσβασης μειώνει τα γενικά έξοδα εγκατάστασης του νέου εξοπλισμού. Το LLDP, απλοποιώντας τη διαχείριση και την

---

ανάπτυξη του δικτύου, ελαχιστοποιεί τον αριθμό και την πολυπλοκότητα των διαδικασιών και μειώνει τον αριθμό των απασχολούμενων προσώπων.

- **Βελτιωμένες επιλογές και ευελιξία στο σχεδιασμό του δικτύου.** Το LLDP, ως ανοικτό πρότυπο, συμβάλλει στη δημιουργία μιας ανοιχτής αγοράς και στη δυνατότητα επιλογής του πελάτη, ώστε μια επιχείρηση να μπορεί να επιλέξει τον καλύτερο προμηθευτή για μια συγκεκριμένη εφαρμογή του δικτύου. Επίσης, βοηθά στην εξάλειψη των εμποδίων που υφίστανται κατά την προσπάθεια δημιουργίας μιας βέλτιστης λύσης, με τη συνεργασία πολλών κατασκευαστών. Με τον τρόπο αυτό μπορεί να υλοποιηθεί ένα πιο προηγμένο δίκτυο και να μειωθεί το κεφάλαιο δαπανών που οφείλονται στην ανταγωνιστική προσφορά και την αυξημένη διαπραγματευτική δύναμη. Γενικά, τα ανοικτά πρότυπα λειτουργούν προς όφελος του τελικού χρήστη, διότι είναι το αποτέλεσμα της συνεργασίας των πωλητών για την ανάπτυξη της τεχνολογίας. Αυτός ο συντονισμός προκαλεί, ταυτόχρονα, πρόοδο στους κύκλους ανάπτυξης νέων τεχνολογιών και αύξηση των ανταγωνιστικών τιμών.



---

## ΚΕΦΑΛΑΙΟ 4: ΥΛΟΠΟΙΗΣΗ ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΔΙΚΤΥΟ

---

### 4.1 ΑΥΤΟΒΑΗΝ

---

Το **ΓÉANT** είναι το πανευρωπαϊκό δίκτυο δεδομένων, αφιερωμένο στην έρευνα και την εκπαιδευτική κοινότητα. Μαζί με τα εθνικά ερευνητικά δίκτυα στην Ευρώπη, το ΓÉANT συνδέει 40 εκατομμύρια χρήστες σε περισσότερα από 8.000 ιδρύματα σε 40 χώρες.

Το ευρωπαϊκό έργο GN3 είναι ένα ερευνητικό πρόγραμμα που χρηματοδοτείται από την Ευρωπαϊκή Ένωση και τα Εθνικά Ερευνητικά και Εκπαιδευτικά Δίκτυα της Ευρώπης (National Research and Educational Networks, NRENs). Αποτελεί συνέχεια προηγούμενου έργου, του GN2, και στοχεύει στην ανάπτυξη και την υποστήριξη της επόμενης γενιάς του πανευρωπαϊκού δικτύου έρευνας και εκπαίδευσης, το οποίο συνδέει πανεπιστήμια, ιδρύματα και άλλους ερευνητικούς και εκπαιδευτικούς οργανισμούς σε όλη την Ευρώπη και τους διασυνδέει με το υπόλοιπο του Διαδικτύου χρησιμοποιώντας συνδέσεις κορμού υψηλής ταχύτητας.

Η υπηρεσία **Bandwidth on Demand (BoD)**, όπως ορίζεται στα πλαίσια του έργου GN2, στοχεύει στην παροχή μιας, εγγυημένης χωρητικότητας, συνδεδεσμοστρεφούς υπηρεσίας μεταξύ δύο άκρων. Όταν τα άκρα βρίσκονται σε διαφορετικούς τομείς δικτύου (domains), η επικοινωνία μεταξύ τους είναι εκείνο το μέρος του συστήματος που βασίζεται σε λιγότερο γνωστά, δοκιμασμένα ή ισχύοντα πρότυπα και ως εκ τούτου αποτέλεσε τον κύριο άξονα δραστηριοτήτων του **JRA3<sup>8</sup>** (**Joint Research Activity 3**). Κάθε τομέας δικτύου μπορεί να επιλέξει τις δικές του

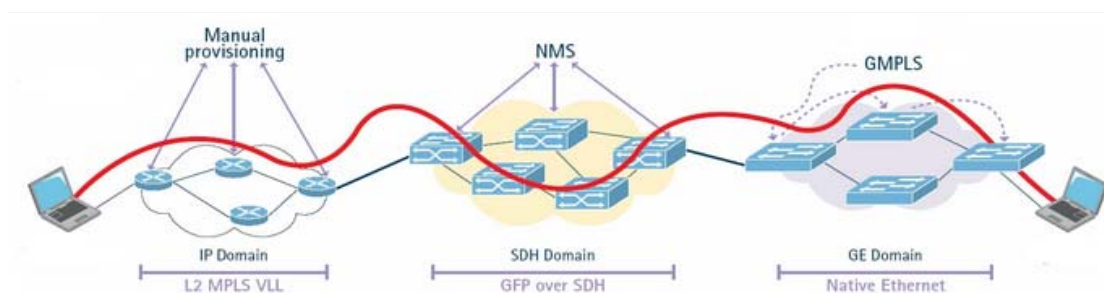
---

<sup>8</sup> Ομάδα έρευνας του ΓÉANT για την επέκταση των εφαρμογών και εργαλείων των χρηστών σε πολλούς τομείς, με σκοπό την απρόσκοπτη πρόσβαση σε υπηρεσίες και τη δημιουργία υποδομών που υποστηρίζουν τη συνεργασία μεταξύ διαφόρων κοινοτήτων.

πολιτικές και τεχνολογίες για την παροχή της BoD υπηρεσίας εντός των συνόρων του. Το μοντέλο αυτό επιτρέπει επίσης την κλιμάκωση σε μεγάλο αριθμό τομέων δικτύου και επιβάλλει χαλαρούς ή καθόλου περιορισμούς συγχρονισμού κατά την εφαρμογή του.

Παραδοσιακά, η παροχή αποκλειστικής χωρητικότητας δικτύου είναι μια σχετικά αργή διαδικασία, ιδίως για τις συνδέσεις υψηλής ταχύτητας. Η ανάπτυξη των δικτυακών τεχνολογιών μεταφοράς και η διαδεδομένη χρήση οπτικών ινών για μετάδοση δεδομένων επιτρέπουν τη δημιουργία νέων σεναρίων χρήσης του δικτύου, στα οποία η παραπάνω διαδικασία επιταχύνεται. Ταυτόχρονα εμφανίζονται ειδικές απαιτήσεις από την κοινότητα του GRID, καθώς και από ερευνητικές ομάδες στην Αστρονομία, στους Υπερυπολογιστές και στη Φυσική Υψηλής Ενέργειας, για την πρόσβαση σε ειδικές συνδέσεις υψηλής ταχύτητας σε ελάχιστο ή ακόμα και σε πραγματικό χρόνο.

Στα πλαίσια, λοιπόν, του GN3 αναπτύχθηκε μια υπηρεσία BoD, η οποία υποστηρίζεται από το εργαλείο AutoBAHN. **AutoBAHN** σημαίνει αυτόματη δέσμευση εύρους ζώνης σε ετερογενή δίκτυα (**Automated Bandwidth Allocation across Heterogenous Networks**). Πρόκειται για ένα σύστημα BoD, το οποίο δεσμεύει πόρους, βρίσκει μονοπάτια, ανακαλύπτει τοπολογίες, ελέγχει την κίνηση και γενικά εκτελεί διάφορες απαραίτητες λειτουργίες σε ετερογενή περιβάλλοντα που περιλαμβάνουν πολλούς τομείς. Στο τελικό στάδιο της επεξεργασίας, πρέπει να υλοποιηθεί ένα κύκλωμα και να αποσταλούν οι κατάλληλες εντολές ρύθμισης των συσκευών του δικτύου. Το έργο αναπτύχθηκε πιλοτικά από το GN2 και συνεχίστηκε από το GN3, που αποσκοπεί στην παροχή του απαιτούμενου εύρους ζώνης στα δίκτυα της GEANT κοινότητας.



**Εικόνα 21:** AutoBAHN (GÉANT Forge – AutoBAHN)



---

### 4.1.1 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ AUTOBAHN

---

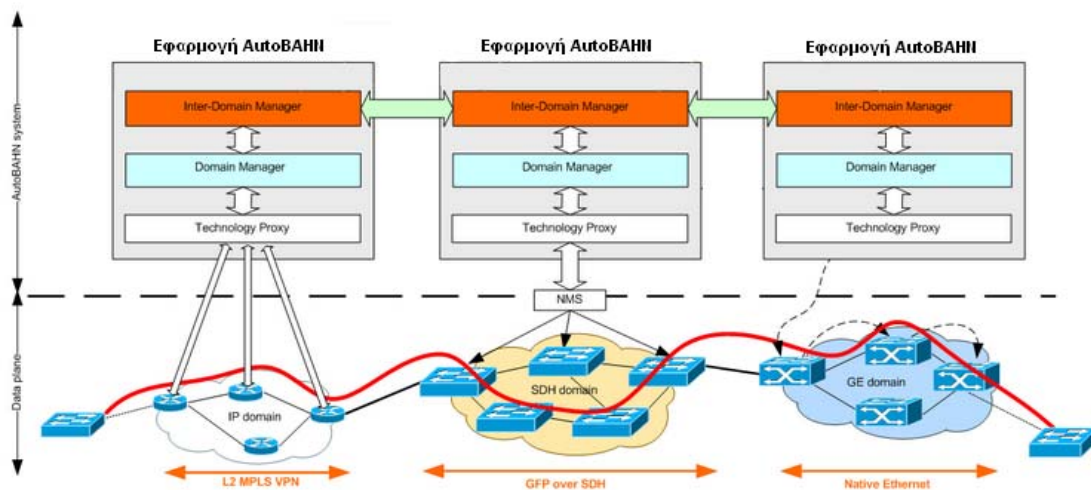
Μια απλή AutoBAHN εφαρμογή που υλοποιείται σε ένα τομέα δικτύου αποτελείται από τρία κύρια στοιχεία:

- **Διατομεακός διαχειριστής (Inter Domain Manager, IDM):** αναλαμβάνει την επικοινωνία με άλλους τομείς δικτύου και είναι υπεύθυνος για την αποδοχή, έγκριση και υλοποίηση της BoD αίτησης.
- **Διαχειριστής τομέα δικτύου (Domain Manager, DM):** ενεργεί ως πελάτης (client), αποστέλλοντας αιτήσεις τις οποίες οι εξωτερικές εφαρμογές, από την πλευρά του διακομιστή, λαμβάνουν και επεξεργάζονται. Σε γενικές γραμμές, οι αιτήσεις αυτές περιορίζονται στη δημιουργία ή τη διαγραφή των φυσικών κυκλωμάτων του δικτύου.
- **Τεχνολογικός μεσολαβητής (Technology Proxy, TP):** μεταφράζει τις αιτήσεις του DM στις κατάλληλες εντολές που πρέπει να αποσταλούν (συνήθως μέσω SSH) σε μια συσκευή δικτύου ή ένα **Σύστημα Διαχείρισης Δικτύου (Network Management System, NMS)**. Η αρχιτεκτονική του BoD προβλέπει διάφορους TPs, καθένας ανεξάρτητος από τους άλλους, οι οποίοι μπορεί να συνδέονται μεταξύ τους όταν χρειάζεται. Αυτή η λύση είναι προτιμότερη από το να υπήρχε μόνο ένας TP, τμηματοποιημένος ανά τεχνολογία, καθώς η τελευταία είναι λιγότερο επεκτάσιμη και δεν επιτρέπει φυσική αποσύνδεση ενός TP από τους άλλους.

Το AutoBAHN καθορίζει μια διεπαφή SOAP<sup>9</sup> μεταξύ DM και TP, την οποία κάθε τομέας δικτύου έχει τη δυνατότητα να προσαρμόσει σε συγκεκριμένες ανάγκες του.

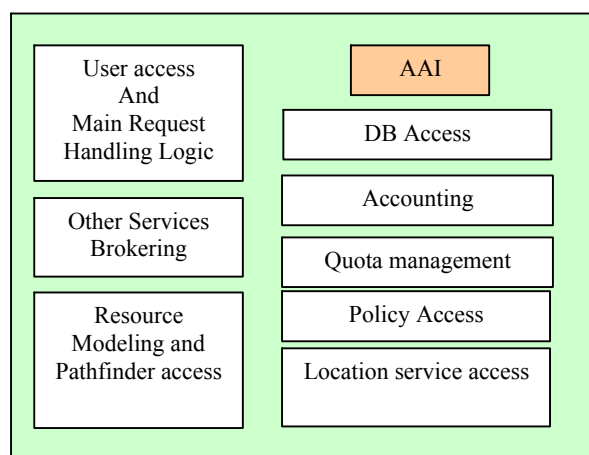
---

<sup>9</sup> **SOAP (Simple Object Access Protocol):** ένα απλό, βασισμένο στην XML, πρωτόκολλο που επιτρέπει στις εφαρμογές να ανταλλάσσουν πληροφορίες μέσω HTTP, ή την πρόσβαση σε μια υπηρεσία Web.



**Εικόνα 22:** Αρχιτεκτονική του AutoBAHN (GÉANT Forge – AutoBAHN)

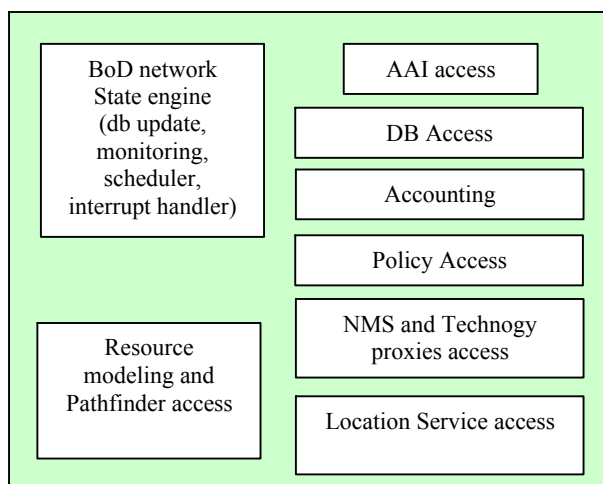
Στη συνέχεια παρουσιάζονται αναλυτικά οι δομικές μονάδες των IDM, DM και TP και ακολουθεί περαιτέρω επεξήγηση των μονάδων-κλειδιά τους.



**Εικόνα 23:** Inter Domain Manager (GÉANT2 Bandwidth on Demand Framework and General Architecture)

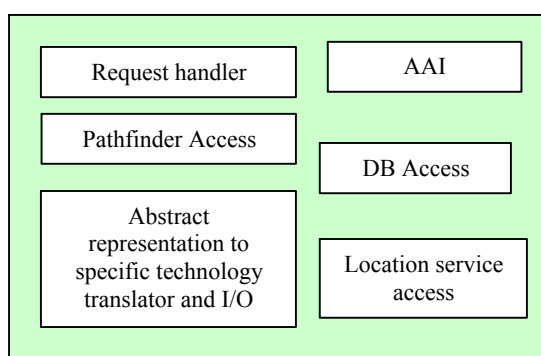
- **AAI (Authentication and Authorization Interface):** Πιστοποίηση και έγκριση των εισερχόμενων BoD αιτήσεων.

- **Quota Management:** Κατανομή των διαθέσιμων πόρων του συστήματος μεταξύ των εξουσιοδοτημένων χρηστών. Παρέχει πληροφορίες στη μονάδα Accounting και στον DM, το τελευταίο σε περίπτωση που δεν υπάρχουν αρκετοί πόροι για τον αιτούντα χρήστη, επομένως η αίτησή του απορρίπτεται.
- **Accounting:** Δραστηριότητες λογιστικής και παρακολούθησης των επιδόσεων του συστήματος (π.χ. αριθμός των αιτήσεων που εξυπηρετήθηκαν επιτυχώς ή απορρίφθηκαν, μέσος όρος χρήσης των πόρων του συστήματος, κ.ά.) και υποβολή των αντίστοιχων αναφορών.
- **Resource Modeling and Pathfinder Access:** Κατά την παραλαβή της σχετικής αίτησης, ο IDM εκτελεί μια σειρά ελέγχων τοπολογίας και λαμβάνει αποφάσεις δρομολόγησης. Αρχικά πρέπει να ανακαλύψει αν το σημείο εκκίνησης της αίτησης βρίσκεται εντός του domain του και να υπολογίσει μια διαδρομή μέσα σε αυτόν, διαφορετικά θα υπολογίσει μια διαδρομή έως τα σύνορά του. Για την εκτέλεση των ενεργειών αυτών, η μονάδα Pathfinder θα κληθεί να παράσχει έναν κατάλογο των πιθανών διαδρομών. Η μοντελοποίηση πόρων (resource modelling) είναι απαραίτητη κατά την αξιολόγηση των εναλλακτικών λύσεων χρήσης των πόρων του συστήματος. Στην περίπτωση που η επιλογή διαδρομής γίνεται από άλλον IDM, η μονάδα pathfinder μπορεί να μεταβάλει τη διαδρομή για μετέπειτα χρήση.
- **Communication with other services:** Περιλαμβάνει όλες τις διεπαφές για την επικοινωνία με άλλες υπηρεσίες υψηλού επιπέδου.
- **User Access and Request-handling Logic:** Μπορεί να δεχθεί ορισμό νέων τύπων διεπαφών.



**Εικόνα 24:** Domain Manager (GÉANT2 Bandwidth on Demand Framework and General Architecture)

- **BoD Network State Engine:** Διατήρηση ενημερωμένων πληροφοριών κατάστασης της BoD υπηρεσίας, χειρισμός βλαβών, προγραμματισμός περιοδικών εργασιών, έναρξη και λήξη δέσμευσης πόρων, παρακολούθηση και λογιστικές δραστηριότητες. Αυτή η μονάδα ενεργεί επίσης ως η κύρια θύρα εισόδου/εξόδου και εκτελεί τον προγραμματισμό και την αναμονή των αιτήσεων.
- **NMS and Technology Proxies Access:** Αλληλεπίδραση μεταξύ του DM και των οντοτήτων του δικτύου μέσω των TPs, ως ένα στρώμα προσαρμογής των πολλών διαφορετικών τεχνολογιών κάθε τομέα δικτύου και των υπαρχόντων NMS.



**Εικόνα 25:** Technology Proxy (GÉANT2 Bandwidth on Demand Framework and General Architecture)

- **Abstract Representation to Specific Technology Translator and I/O:** Μετάφραση από την αφηρημένη αναπαράσταση του δικτύου, η οποία χρησιμοποιείται από όλες τις BoD μονάδες, σε μία συγκεκριμένη τεχνολογία, σε επίπεδο εντολών. Η τεχνολογία αυτή κυμαίνεται από ένα πολύπλοκο σύστημα έως Ethernet μεταγωγείς Layer 2. Κάθε TP υλοποιεί μία μόνο τεχνολογία. Πρέπει να ληφθεί υπόψη η πιθανότητα ότι η μετάφραση δεν γίνεται απαραίτητα σε απόλυτη αντιστοιχία, καθώς ορισμένα χαρακτηριστικά μπορεί να απουσιάζουν ή να έχουν διαφορετική σημασία.

---

## 4.2 AUTOBAHN CARRIER GRADE ETHERNET TECHNOLOGY PROXY (CGE TP)

---

Στην ενότητα αυτή περιγράφονται τα βήματα που πραγματοποιήθηκαν για το σχεδιασμό και την εφαρμογή ενός πρωτότυπου Technology Proxy, ικανού να συνδυάζει την τεχνολογία Carrier Grade Ethernet με το AutoBAHN, με βάση τις εφαρμογές των σχετικών προτύπων και τεχνολογιών της Extreme Networks.

---

### 4.2.1 ΥΠΟΣΤΗΡΙΖΟΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

---

Οι βασικές τεχνολογίες που ορίζονται από το IEEE και παρέχουν ουσιαστική υποστήριξη για την ανάπτυξη ενός Ethernet δικτύου κορμού είναι τα ακόλουθα πρωτόκολλα, η ανάλυση των οποίων έγινε σε προηγούμενες ενότητες:

- **Link Layer Discovery Protocol – IEEE802.1AB**

Το πρωτόκολλο LLDP έχει μικρή επίδραση στο AutoBAHN, καθώς ο κύριος σκοπός του είναι να ανακαλύψει τα στοιχεία και την τοπολογία ενός δικτύου Ethernet. Η ανακαλυφθείσα τοπολογία θα πρέπει στη συνέχεια να διατηρηθεί, να διαχειριστεί και να αντληθεί από το AutoBAHN.

- **Provider Bridges / Q-in-Q – IEEE802.1ad**
- **Provider Backbone Bridging (PBB) / MAC-in-MAC - IEEE802.1ah**
- **Provider Backbone Bridge Traffic Engineering (PBB-TE) – IEEE802.1Qay**

Είναι ίσως το πιο σχετικό με το μοντέλο υπηρεσίας του AutoBAHN, δεδομένου ότι επιτρέπει τη ρητή επιλογή μονοπατιών, τα οποία έχουν κατασκευαστεί με γνώμονα την κυκλοφορία πληροφορίας, μέσα σε PBB δίκτυα. Η λειτουργικότητα του 802.1Qay προσφέρει ρητώς δρομολογημένα, με εγγυημένο εύρος ζώνης μονοπάτια μέσα σε ένα PBB πυρήνα, οπότε ο αντίστοιχος TP του AutoBAHN θα πρέπει να αναπτυχθεί αναλόγως.

- **Ethernet Operations, Administration and Maintenance (OAM) – IEEE802.1ag (ITU Y.1731)**

Το 802.1ag παρέχει λειτουργίες συντήρησης και διαχείρισης του δικτύου. Αυτές δεν σχετίζονται άμεσα με τη δυναμική δέσμευση κυκλωμάτων και τη λειτουργία πρόβλεψης, που απαιτούνται από το AutoBAHN. Ωστόσο, είναι απαραίτητες για τον έλεγχο της απόδοσης και την αντιμετώπιση των προβλημάτων των προβλεπόμενων κυκλωμάτων, επομένως αξιοποιούνται ανάλογα με την πλέον προηγμένη έκδοση του AutoBAHN CGE TP.

Εφόσον το AutoBAHN ασχολείται με point-to-point συνδέσεις, το ενδιαφέρον επικεντρώνεται στην υποστήριξη των E-Line (EPL και EVPL) υπηρεσιών. Το επίπεδο υλοποίησης του AutoBAHN CGE TP εξαρτάται από τις βασικές εφαρμογές των παραπάνω προτύπων. Η PBB/PBB-TE λειτουργικότητα, τουλάχιστον στα αρχικά στάδιά του, υποστηρίζεται κατά κύριο λόγο στο επίπεδο διαχείρισης. Συνεπώς, η προδιαγραφές του TP εξαρτώνται σε μεγάλο βαθμό από ατομικές εφαρμογές και όχι από ένα τυποποιημένο επίπεδο ελέγχου.

---

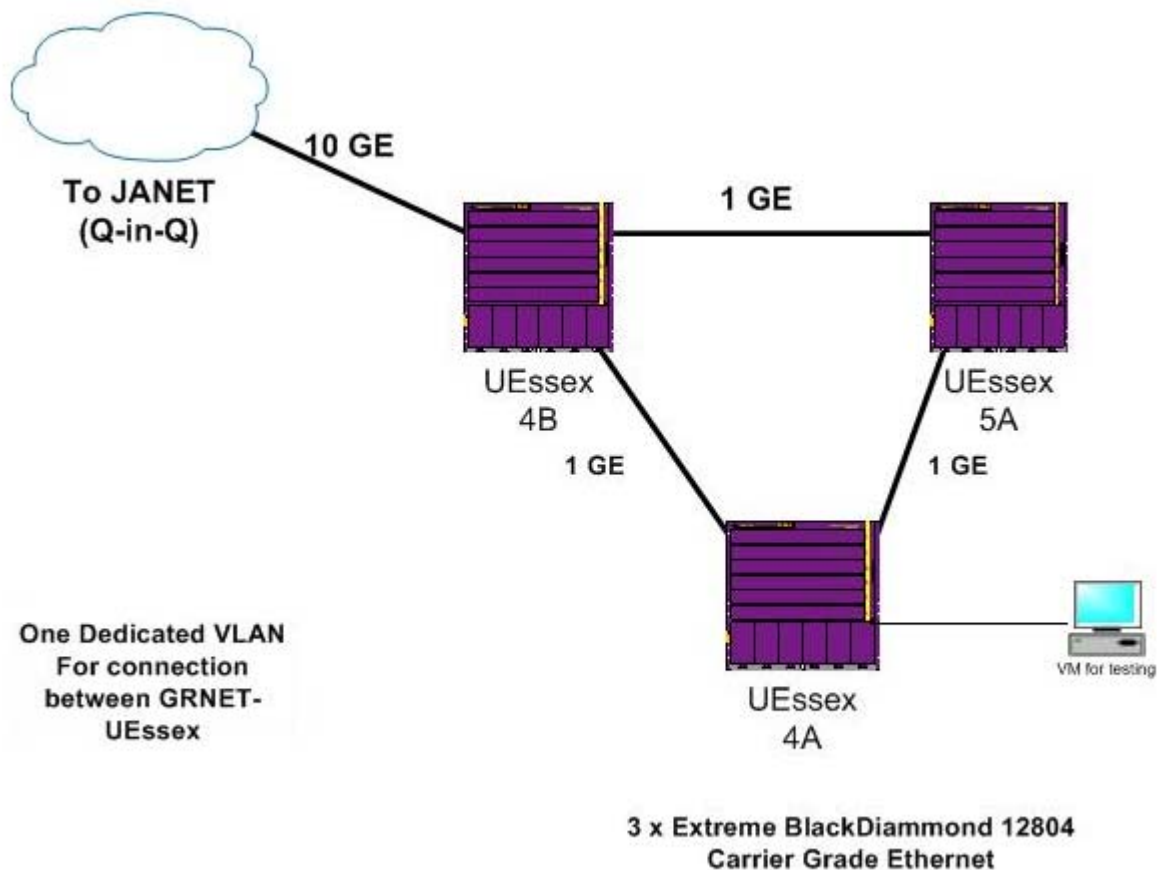
### **4.2.2 ΥΠΟΔΟΜΗ CARRIER ETHERNET**

---

Για τους σκοπούς του πειράματος και του ελέγχου εφαρμογής της τεχνολογίας CGE, χρησιμοποιήθηκε μια πλατφόρμα δοκιμών που παρέχεται από το Πανεπιστήμιο του Essex της Αγγλίας. Η πλατφόρμα αποτελείται κατά βάση από μεταγωγείς BlackDiamond, της σειράς 12800, της Extreme Networks. Ο εξοπλισμός αυτός χρησιμοποιείται ταυτόχρονα από διάφορες ερευνητικές ομάδες και η πρόσβαση σε αυτόν χορηγήθηκε από το Πανεπιστήμιο του Essex, προκειμένου να εξετάσει και να αξιολογήσει τη δυνατότητα υλοποίησης ενός TP για αυτή την υποδομή. Ο TP επικοινωνεί με το λογισμικό του AutoBAHN και δεσμεύει πόρους για την BoD υπηρεσία.

Η πλατφόρμα αποτελείται από τα ακόλουθα στοιχεία:

- Τρεις Carrier Grade Ethernet μεταγωγείς Extreme BlackDiamond 12804, με υποστήριξη OAM, PBB-TE και σύνδεσης με το δίκτυο JANET. Η δημιουργία των PBB-TE μονοπατιών πρόκειται να χρησιμοποιηθεί για τη μεταφορά της δυναμικά τροφοδοτούμενης VLAN κίνησης σε σαφώς καθορισμένες διαδρομές.
- TACACS και OpenVPN διακομιστές για την πρόσβαση στο δίκτυο και την έγκριση των πόρων
- Εικονικές μηχανές ως πηγές/προορισμούς κίνησης πληροφορίας



**Εικόνα 26:** UESsex-GRNet testbed

Οι τρεις μεταγωγείς έχουν τις ακόλουθες MAC διευθύνσεις:

**Μεταγωγέας 4A:** 00:04:96:1E:FD:60

**Μεταγωγέας 4B:** 00:04:96:3B:23:10

**Μεταγωγέας 5A:** 00:04:96:3B:09:60

ενώ η **εικονική μηχανή** έχει τη MAC διεύθυνση: 08:00:27:53:5e:5b

Οι μεταγωγείς BlackDiamond 12800 της Extreme Networks επιτρέπουν σε ένα δίκτυο Ethernet να παρέχει τόσο οικιακές, όσο και επιχειρηματικές υπηρεσίες. Είναι σχεδιασμένοι για χρήση στον πυρήνα του δικτύου. Στα χαρακτηριστικά τους περιλαμβάνονται γρήγορα εναλλασσόμενες μονάδες εισόδου/εξόδου, μονάδες διαχείρισης που παρέχουν ενεργό πλέγμα μεταγωγής και υποσύστημα ελέγχου της



CPU, αυτόματη διαπραγμάτευση για ημιαμφίδρομη ή πλήρως αμφίδρομη λειτουργία σε θύρες ταχυτήτων 10/100/1000 Mbps και καταμερισμός φόρτου σε πολλές θύρες.

Κάθε μεταγωγέας διαθέτει μια διεπαφή γραμμής εντολών που χρησιμοποιείται από τον CGE TP για να ρυθμίζει ανεξάρτητα κάθε μεταγωγέα στο δίκτυο. Αυτό σημαίνει ότι ο TP πρέπει να έχει γνώση του υποκείμενου δικτύου και να παίρνει περίπλοκες αποφάσεις. Η πρόσβαση στη γραμμή εντολών γίνεται μέσω Telnet.

---

### **4.2.3 ΑΝΑΚΑΛΥΨΗ ΤΟΠΟΛΟΓΙΑΣ**

---

Εφόσον ήδη γνωρίζουμε τις MAC διευθύνσεις της εικονικής μας μηχανής και των μεταγωγέων της πλατφόρμας δοκιμών, θα χρησιμοποιήσουμε το πρωτόκολλο LLDP για να ανακαλύψουμε τη MAC διεύθυνση του πρώτου κόμβου που συνδέεται με τον μεταγωγέα UEssex\_4B, ο οποίος ανήκει στο δίκτυο Janet, για το λόγο ότι κάθε κόμβος που έχει ενεργοποιημένο τη λειτουργία LLDP στις θύρες του, μπορεί να αποθηκεύσει πληροφορίες σχετικά με έως και τέσσερις γειτονικούς του κόμβους. Ως εκ τούτου, θα τρέξουμε στον UEssex\_4B τις ακόλουθες εντολές:

```
enable lldp ports *  
show lldp neighbors detailed
```

και με την εντολή «show» παίρνουμε πληροφορία για τη MAC διεύθυνση (Chassis ID) των γειτονικών κόμβων.

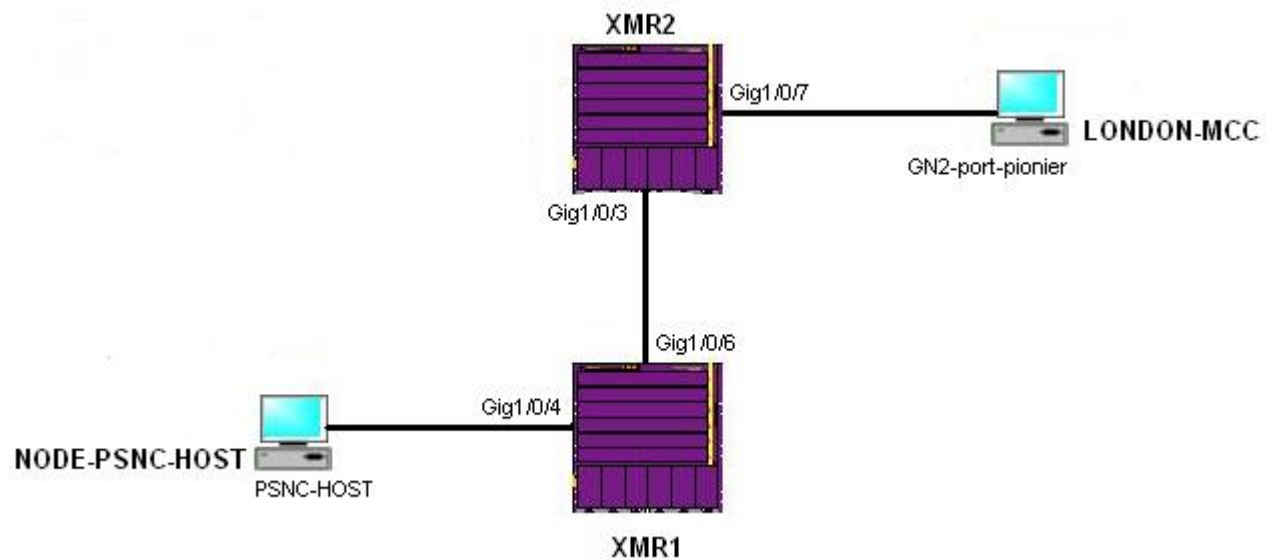
---

### **4.2.4 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ CGE TP**

---

Όπως αναφέρθηκε, ο καθορισμός ενός CGE TP βασίζεται στο επίπεδο διαχείρισης και όχι σε ένα τυποποιημένο επίπεδο ελέγχου. Ο DM υποβάλλει αιτήσεις για δέσμευση ή απελευθέρωση πόρων και ο TP στέλνει απαντήσεις χρησιμοποιώντας την καθορισμένη διασύνδεση SOAP. Η αίτηση δέσμευσης, εκ μέρους του DM, είναι

υπεύθυνη για την οριοθέτηση της επιθυμητής διαδρομής, αφήνοντας στον TP μόνο τη ρύθμιση των σχετικών μεταγωγέων. Ακολουθεί ένα παράδειγμα αίτησης δέσμευσης (**reservation request**) του DM προς τον TP για την εξής τοπολογία:



Εικόνα 27: Παράδειγμα τοπολογίας

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:addReservation xmlns:ns2="http://tool.jra3.geant2.net/">
      <resID>res1</resID>
      <links>
        <startInterface>
          <node>
            <name>XMR2</name>
            <ipAddress>172.10.1.59</ipAddress>
          </node>
          <name>Gig1/0/7</name>
          <bandwidth>1000000000</bandwidth>
        </startInterface>
        <endInterface>
          <node>
            <name>LONDON-MCC</name>
            <ipAddress>LONDON-MCC</ipAddress>
          </node>
          <name>GN2-port-pionier</name>
          <bandwidth>1000000000</bandwidth>
        </endInterface>
      </links>
      <domainId>https://poznan.autobahn.psn.pl:8443/autobahn/interdomain</domainId>
      <clientPort>>false</clientPort>
    </ns2:addReservation>
  </soap:Body>
</soap:Envelope>
```

```

        </endInterface>
        <protection>>false</protection>
        <propDelay>0.0</propDelay>
</links>
<links>
    <startInterface>
        <node>
            <name>XMR1</name>
            <ipAddress>172.10.1.58</ipAddress>
        </node>
        <name>Gig1/0/6</name>
        <bandwidth>1000000000</bandwidth>
        <clientPort>>false</clientPort>
    </startInterface>
</endInterface>
    <node>
        <name>XMR2</name>
        <ipAddress>172.10.1.59</ipAddress>
    </node>
    <name>Gig1/0/3</name>
    <bandwidth>1000000000</bandwidth>
    <clientPort>>false</clientPort>
</endInterface>
<protection>>false</protection>
<propDelay>0.0</propDelay>
</links>
<links>
    <startInterface>
        <node>
            <name>XMR1</name>
            <ipAddress>172.10.1.58</ipAddress>
        </node>
        <name> Gig1/0/4</name>
        <bandwidth>1000000000</bandwidth>
        <domainId>https://poznan.autobahn.psn.pl:8443/autobahn/interdomain/</d
omainId>
        <clientPort>>false</clientPort>
    </startInterface>
</endInterface>
    <node>
        <name>NODE-PSNC-HOST</name>
        <ipAddress>NODE-PSNC-
HOST</ipAddress>
    </node>
    <name>PSNC-HOST</name>
    <bandwidth>1000000000</bandwidth>
    <domainId>https://client.psn.pl/</domainId>
    <clientPort>>true</clientPort>
</endInterface>
<protection>>false</protection>
<propDelay>0.0</propDelay>
</links>
<params>
    <capacity>1000000000</capacity>
    <maxDelay>0</maxDelay>
    <bidirectional>>false</bidirectional>
    <startTime>2010-03-
05T15:41:31.015+01:00</startTime>
    <endTime>2010-03-05T15:41:56.015+01:00</endTime>
    <pathConstraints>
        <rangeNames>VLANS</rangeNames>
        <rangeConstraints>
            <ranges>
                <min>150</min>

```

```

<max>150</max>
</ranges>
</rangeConstraints>
</pathConstraints>
</params>
</ns2:addReservation>
</soap:Body>
</soap:Envelope>

```

Η παραπάνω αίτηση ζητά από τον TP να δημιουργήσει ένα κύκλωμα μέσα στον τομέα δικτύου «<https://poznan.autobahn.psn.pl:8443/autobahn/interdomain>» με τα ακόλουθα χαρακτηριστικά:

- **Διαδρομή για τη δημιουργία του κυκλώματος:** GN2-port-pionier (LONDON-MCC) - Gig1/0/7 (XMR2), Gig1/0/3 (XMR2) - Gig1/0/6 (XMR1), Gig1/0/4 (XMR1) - PSNC-HOST (NODE-PSNC-HOST). Μόνο ένα μέρος της διαδρομής είναι υπό τον έλεγχο του προαναφερθέντος τομέα δικτύου, καθώς τα GN2-port-pionier και NODE-PSNC-HOST είναι εξωτερικές θύρες, επομένως τους έχουν εκχωρηθεί άλλα αναγνωριστικά. Ως εκ τούτου, το πραγματικό κύκλωμα μέσα στον τομέα δικτύου θα δημιουργηθεί μεταξύ των διεπαφών Gig1/0/7 (XMR2) και Gig1/0/4 (XMR1).
- **Χωρητικότητα:** 1Gbps
- **Καθυστέρηση:** 0
- **Αμφίδρομη λειτουργία:** Όχι
- **VLAN ID για τη ρύθμιση του κυκλώματος:** 150

Κάθε αίτηση χαρακτηρίζεται από ένα μοναδικό **αναγνωριστικό (resID)**, το οποίο της ανατίθεται από τον IDM του αρχικού τομέα δικτύου. Κατά τη δημιουργία του κυκλώματος, ο TP είναι υποχρεωμένος να χρησιμοποιήσει τους ακριβείς **συνδέσμους (links)** και να ικανοποιήσει τις **παραμέτρους (params)** ποιότητας, χρονικής περιόδου και συγκεκριμένης τεχνολογίας μεταφοράς που ορίζονται στην αίτηση.

Αντίστοιχα, ο DM στέλνει μια αίτηση αποδέσμευσης πόρων του δικτύου, για την αφαίρεση ενός προηγουμένως δημιουργημένου κυκλώματος.

---

#### 4.2.5 ΡΥΘΜΙΣΕΙΣ ΜΕΤΑΓΩΓΕΩΝ (SWITCH CONFIGURATION)

---

Για τις ανάγκες του πειράματος και εφόσον η πλατφόρμα δοκιμών αποτελείται από τρεις μόνο μεταγωγείς, θεωρήσαμε ότι υποστηρίζονται μόνο 2 διαφορετικά μονοπάτια μέσα στο PBB tunnel, καθένα από τα οποία αποτελεί και ένα διαφορετικό BVLAN. Το πρώτο (b1) περιλαμβάνει μόνο τους οριακούς μεταγωγείς UEssex\_4A και UEssex\_4B, ενώ το δεύτερο (b2) περιλαμβάνει επιπλέον τον κεντρικό μεταγωγέα UEssex\_5A. Οι οριακοί μεταγωγείς δέχονται VLAN κίνηση από τις εικονικές μηχανές και τη μετασχηματίζουν σε SVLAN (VMAN), ενώ ο κεντρικός μεταγωγέας λειτουργεί ως μεταγωγέας κορμού του PBBN.

Οι ρυθμίσεις των Extreme BlackDiamond μεταγωγέων έγιναν στατικά σε κάθε μεταγωγέα της πλατφόρμας δοκιμών. Οι σχετικές εντολές ρύθμισης περιλαμβάνουν τη δημιουργία και ρύθμιση των BVLANs και SVLANs, απενεργοποιώντας τις λειτουργίες learning και flooding στα BVLANs και SVLANs που ορίζονται, καθώς και τη δημιουργία των εγγραφών της FDB και των MAC συνδέσεων (MAC bindings).

##### Μεταγωγέας UEssex\_4A:

```
create bvlan b1
create bvlan b2

configure bvlan b1 tag 100
configure bvlan b2 tag 200
configure bvlan b1 add port *4A_4B* tagged
configure bvlan b2 add port *4A_5A* tagged

disable learning bvlan b1
disable learning bvlan b2
disable flooding bvlan b1
disable flooding bvlan b2

create fdbentry 00:04:96:3B:23:10 vlan b1 *port_4A_4B*
create fdbentry 00:04:96:3B:23:10 vlan b2 *port_4A_5A*
```

### Μεταγωγέας UEssex\_4B:

```
create bvlan b1
create bvlan b2

configure bvlan b1 tag 100
configure bvlan b2 tag 200
configure bvlan b1 add port *4B_4A* tagged
configure bvlan b2 add port *4B_5A* tagged

disable learning bvlan b1
disable learning bvlan b2
disable flooding bvlan b1
disable flooding bvlan b2

create fdbentry 00:04:96:1E:FD:60 vlan b1 *port_4B_4A*
create fdbentry 00:04:96:1E:FD:60 vlan b2 *port_4B_5A*
```

### Μεταγωγέας UEssex\_5A:

```
create bvlan b2

configure bvlan b2 tag 200
configure bvlan b2 add port *5A_4B*,*5A_4A* tagged

disable learning bvlan b2
disable flooding bvlan b2

create fdbentry 00:04:96:1E:FD:60 vlan b2 *port_5A_4A*
create fdbentry 00:04:96:3B:23:10 vlan b2 *port_5A_4B*
```

---

#### ***4.2.6 ΠΥΘΜΙΣΕΙΣ CGE TECHNOLOGY PROXY (TP CONFIGURATION)***

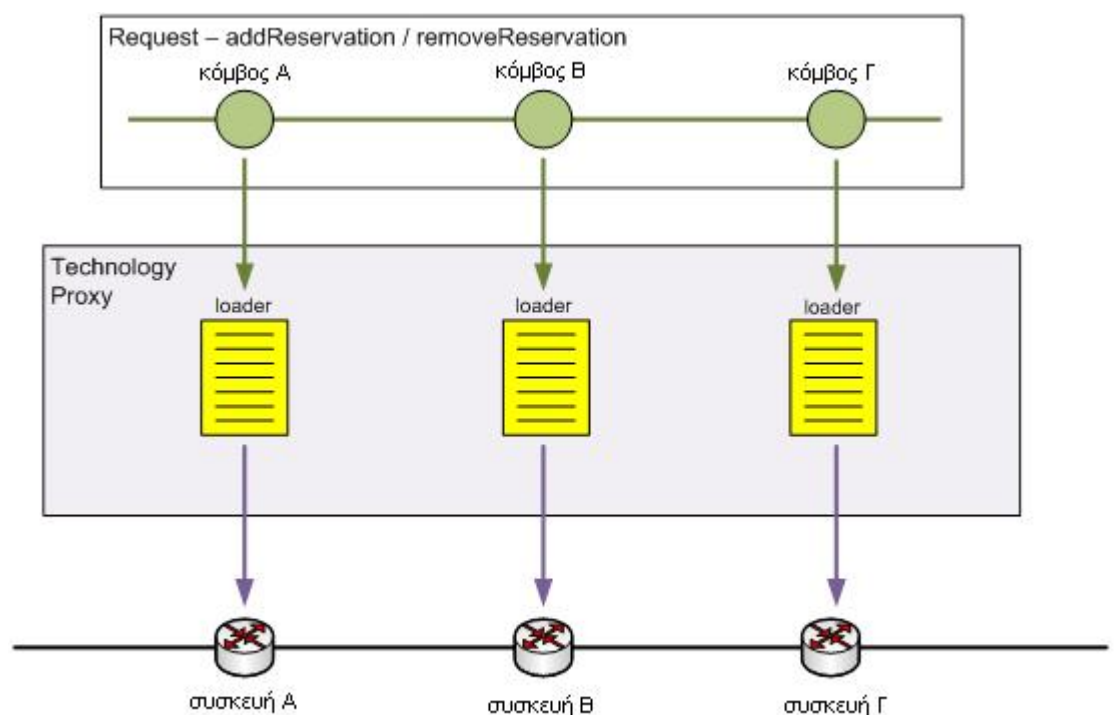
---

Το κύριο αρχείο ρυθμίσεων configuration.xml περιγράφει διάφορες πτυχές των μηχανισμών του TP. Χωρίζεται σε τέσσερα τμήματα:

- **Credentials:** περιέχει το σύνολο των διαπιστευτηρίων που χρησιμοποιούνται για τον έλεγχο ταυτότητας κατά την επικοινωνία με τις συσκευές. Για τον CGE TP, εφόσον υπάρχει σύνδεση Telnet, χρησιμοποιείται η πιο απλή μορφή, η οποία περιέχει μόνο τις παραμέτρους id, username και password.

- **Protocols:** ο TP προσφέρει τη δυνατότητα προσαρμογής των πρωτοκόλλων που χρησιμοποιούνται για τις συνδέσεις. Κάθε πρωτόκολλο μπορεί να διαμορφωθεί όσες φορές χρειάζεται και στη συνέχεια να ανατεθεί στην κατάλληλη σύνδεση. Επίσης, κάθε πρωτόκολλο πρέπει να δηλωθεί τουλάχιστον μία φορά στο configuration αρχείο. Στην περίπτωση μας χρησιμοποιείται το πρωτόκολλο Telnet με τις εξής παραμέτρους: **type** (μοναδικό αναγνωριστικό), **defaultPort** (θύρα συνδέσεων), **loginPrompt** (προτροπή εισαγωγής username), **passwordPrompt** (προτροπή εισαγωγής password), **prompt** και **superPrompt**.
- **Devices:** ορίζει μια σειρά συσκευών τις οποίες χειρίζεται ο TP και οι οποίες αποτελούν τις μοναδικές που μπορούμε να ρυθμίσουμε. Χρησιμοποιούνται οι παράμετροι **address** (IP διεύθυνση της συσκευής), **loopback** (loopback IP διεύθυνση) και **connections** (σύνολο των διαθέσιμων συνδέσεων για τη συγκεκριμένη συσκευή). Κάθε σύνδεση απαιτεί αναφορές στα διαπιστευτήρια και τους ορισμούς των πρωτοκόλλων. Προς το παρόν, επιτρέπεται μόνο μία σύνδεση ανά συσκευή και υποστηρίζονται μόνο δύο τύποι συνδέσεων, telnet και ssh.
- **Loaders:** είναι υπεύθυνοι για την εφαρμογή των ρυθμίσεων σε συγκεκριμένες συσκευές. Όποτε ο TP προτίθεται να εφαρμόσει οποιαδήποτε ρύθμιση σχετικά με μια συσκευή, ψάχνει για τον κατάλληλο loader, σύμφωνα με τις πληροφορίες που παρέχονται στην αίτηση δέσμευσης. Οι loaders εξειδικεύονται ανάλογα με τον προμηθευτή, το μοντέλο ή το λειτουργικό σύστημα. Προς το παρόν, μόνο οι εξειδικεύσεις προμηθευτή και μοντέλου υποστηρίζονται στο AutoBAHN. Ωστόσο, συνήθως μόνο ένας loader χρειάζεται σε κάθε τομέα δικτύου, επομένως δεν είναι απαραίτητο να παρέχονται όλα τα παραπάνω χαρακτηριστικά. Σε κάθε loader χρησιμοποιείται μια παράμετρος **protocol**, που αναφέρεται στο είδος του χρησιμοποιούμενου πρωτοκόλλου. Η διαδικασία φόρτωσης έχει ως εξής:
  1. Για κάθε κόμβο στο καθορισμένο μονοπάτι, ο TP ψάχνει για τον κατάλληλο loader. Ένας loader μπορεί να επαναχρησιμοποιηθεί για διαφορετικούς κόμβους/συσκευές, αλλά όταν εκτελείται επηρεάζει μόνο έναν κόμβο/συσκευή.

2. Όταν ο loader ξεκινά τη διαδικασία επεξεργασίας, καλεί την κατάλληλη *μέθοδο*. Οι μέθοδοι ορίζουν ρυθμίσεις προσθήκης (add) ή αφαίρεσης (remove) για τη δημιουργία ή την καταστροφή ενός μονοπατιού για μια συγκεκριμένη συσκευή και χαρακτηρίζονται από ένα μοναδικό αναγνωριστικό (id). Κάθε μέθοδος περιέχει διαφορετικά σεντ εντολών, για την επίτευξη του επιθυμητού αποτελέσματος. Απλές εντολές μπορούν να ομαδοποιηθούν σε μεγαλύτερα μπλοκ. Οι απλές εντολές ή τα μπλοκ εντολών αντιμετωπίζονται ως xml στοιχεία, με τις αντίστοιχες ιδιότητες και υποστοιχεία, και η εκτέλεσή τους είναι σειριακή.
3. Η καλούμενη μέθοδος πυροδοτεί μια σειρά από δραστηριότητες, όπως η εκκίνηση σύνδεσης με μια συσκευή, η εκτέλεση εντολών, ο έλεγχος αποτελεσμάτων κλπ.



**Εικόνα 28:** Loaders

Στο σημείο αυτό θα παραθέσουμε το αρχείο configuration.xml για τον Autobahn CGE TP που υλοποιήθηκε. Προηγούνται τα διαπιστευτήρια (username, password), ακολουθεί η δήλωση των δικτυακών συσκευών της πλατφόρμας δοκιμών



(μεταγωγείς UEssex\_4A, UEssex\_4B, UEssex\_5A) και δηλώνεται το Telnet ως χρησιμοποιούμενο πρωτόκολλο. Τέλος, στο τμήμα των loaders δηλώνονται δύο μέθοδοι, add και remove.

Η μέθοδος add ελέγχει αρχικά (με το script) αν τα VLANs εισόδου και εξόδου είναι τα ίδια, καθώς δεν υποστηρίζεται VLAN translation (αντιστοίχιση εξερχόμενης VLAN κίνησης στην εισερχόμενη). Σε περίπτωση που είναι διαφορετικά, προκαλείται εξαίρεση (system exception). Έπειτα, ελέγχεται αν βρισκόμαστε σε οριακό μεταγωγέα, εισόδου ή εξόδου, στο PBBN (UEssex\_4A ή UEssex\_4B), οπότε και πρέπει να δημιουργήσουμε SVLAN (vMAN) κίνηση, ενσωματώνοντας την κατάλληλη ετικέτα (tag) και προσθέτοντας στο SVLAN που ορίζεται τις θύρες που δηλώνονται στην αίτηση δέσμευσης. Στη συνέχεια, ο TP πρέπει να αποφασίσει ποιό μονοπάτι του PBBN θα επιλέξει για τη προώθηση της κίνησης και να αντιστοιχίσει το SVLAN στο αντίστοιχο BVLAN. Η απόφαση λαμβάνεται με βάση τον αριθμό των κόμβων της αίτησης δέσμευσης. Αν αυτός είναι 3, σημαίνει ότι στη διαδρομή περιλαμβάνεται, εκτός των οριακών, και ο κεντρικός μεταγωγέας UEssex\_5A, στον οποίο έχουμε ορίσει το BVLAN b2. Σε κάθε άλλη περίπτωση, το SVLAN συνδέεται στο BVLAN b1.

```
<?xml version="1.0" encoding="utf-8" ?>
<tool xmlns:sh="http://tool.autobahn.geant.net/configuration/shell">
  <credentials>
    <grnet id="grnet">
      <username>grnet</username>
      <password>grnet</password>
    </grnet>
  </credentials>
  <protocols>
    <telnet type="telnet" defaultPort="23">
      <loginPrompt>UserName:</loginPrompt>
      <passwordPrompt>PassWord:</passwordPrompt>
      <prompt>></prompt>
      <superPrompt>#</superPrompt>
    </telnet>
  </protocols>
  <devices>
    <!-->UEssex_4A<!-->
    <device address="192.168.8.251">
      <loopback>10.0.43.1</loopback>
      <connections>
        <telnet credentials="grnet" protocol="telnet" />
      </connections>
    </device>
    <!-->UEssex_4B<!-->
    <device address="192.168.8.252">
      <loopback>10.0.44.1</loopback>
      <connections>
```

```

        <telnet credentials="grnet" protocol="telnet"/>
    </connections>
</device>
<!--UESsex_5A<!-->
<device address="192.168.8.253">
    <loopback>10.0.42.1</loopback>
    <connections>
        <telnet credentials="grnet" protocol="telnet" />
    </connections>
</device>
</devices>
<loaders>
    <sh:loader protocols="telnet">
        <sh:method id="add">
            <textParser/>
            <action>
                <script>
#if($constraintsIn.getConstraintForName('VLANS').value!=$constraintsOut.getC
onstraintForName('VLANS').value)
$this.failure('system')
#end
                </script>
            </action>
            <shell>
                <if condition="$nodeType=='ingress' || $nodeType=='egress'">
                    <shell>
                        <command id="create_svlan">
                            <execute>create svlans$parser.limit($resId,32)</execute>
                        </command>
                        <command id="tag_svlan">
                            <execute>configure svlans$parser.limit($resId, 32) tag
$constraintsIn.getConstraintForName('VLANS').value</execute>
                        </command>
                        <command id="add_svlan_ports">
                            <execute>configure svlans$parser.limit($resId, 32) add port
$ifceIn.name, $ifceOut.name tagged</execute>
                        </command>
                    </shell>
                </if>
                <switch param="$nodesCount">
                    <case value="3">
                        <shell>
                            <command id="bind_bvlan_b2">
                                <execute>configure bvlan b2 add
svlans$parser.limit($resId,32)</execute>
                            </command>
                        </shell>
                    </case>
                    <default>
                        <shell>
                            <command id="bind_bvlan_b1">
                                <execute>configure bvlan b1 add
svlans$parser.limit($resId,32)</execute>
                            </command>
                        </shell>
                    </default>
                </switch>
                <command id="disable_learning">
                    <execute>disable learning svlans$parser.limit($resId,
32)</execute>
                </command>
                <command id="disable_flooding">
                    <execute>disable flooding svlans$parser.limit($resId,
32)</execute>
                </command>
                <if condition="$nodeType=='ingress' || $nodeType=='egress'">
                    <shell>
                        <if condition="$node.ipAddress == '192.168.8.251'">

```

```

        <shell>
            <command id="fdb_4A">
                <execute>create fdbentry 08:00:27:53:5e:5b
vlangs$parser.limit($resId,32) $ifceIn.name, $ifceOut.name</execute>
            </command>
            <switch param="$nodesCount">
                <case value="3">
                    <shell>
                        <command id="mac_binding_4A_b2">
                            <execute>create mac-binding bvlan b2
00:04:96:3B:23:10 svlangs$parser.limit($resId, 32) *MAC_janet*</execute>
                        </command>
                    </shell>
                </case>
                <default>
                    <shell>
                        <command id="mac_binding_4A_b1">
                            <execute>create mac-binding bvlan b2
00:04:96:3B:23:10 svlangs$parser.limit($resId, 32) *MAC_janet*</execute>
                        </command>
                    </shell>
                </default>
            </switch>
        </shell>
    </if>
    <if condition="$node.ipAddress == '192.168.8.252'">
        <shell>
            <command id="fdb_entries_4B">
                <execute>create fdbentry *MAC_janet*
vlangs$parser.limit($resId,32) $ifceIn.name, $ifceOut.name</execute>
            </command>
            <switch param="$nodesCount">
                <case value="3">
                    <shell>
                        <command id="mac_binding_4B_b2">
                            <execute>create mac-binding bvlan b2
00:04:96:1E:FD:60 svlangs$parser.limit($resId, 32)
08:00:27:53:5e:5b</execute>
                        </command>
                    </shell>
                </case>
                <default>
                    <shell>
                        <command id="mac_binding_4B_b1">
                            <execute>create mac-binding bvlan b1
00:04:96:1E:FD:60 svlangs$parser.limit($resId, 32)
08:00:27:53:5e:5b</execute>
                        </command>
                    </shell>
                </default>
            </switch>
        </shell>
    </if>
</shell>
</if>
</sh:method>
<sh:method id="remove">
    <textParser/>
    <if condition="$nodeType=='ingress' || $nodeType=='egress'">
        <shell>
            <command id="delete_svlan">
                <execute>delete svlangs$parser.limit($resId, 32)</execute>
            </command>
            <command id="delete_svlan_ports">
                <execute>configure svlangs$parser.limit($resId, 32) delete ports
all</execute>
            </command>
        </shell>
    </if>
</sh:method>

```

```

<command id="delete_mac_bindings">
  <execute>
    delete mac-binding bvlan b2
    delete mac-binding bvlan b1
  </execute>
</command>
<command id="delete_fdb_entries">
  <execute>
    delete fdbentry 08:00:27:53:5e:5b vlans$parser.limit($resId,32)
    delete fdbentry *MAC_janet* vlans$parser.limit($resId,32)
  </execute>
</command>
</shell>
</if>
</sh:method>
</sh:loader>
</loaders>
</tool>

```

Ακολουθεί πίνακας επεξήγησης των αντικειμένων που χρησιμοποιούνται στο configuration.xml

<i>Όνομα αντικειμένου</i>	<i>Προέλευση</i>	<i>Περιγραφή</i>
<b>resId</b>	reservation request	Reservation ID
<b>ifceIn ifceOut</b>	reservation request	Διεπαφές εισόδου-εξόδου με παραμέτρους: <ul style="list-style-type: none"> <li>• name</li> <li>• bandwidth (bps)</li> <li>• status (up/down)</li> <li>• mtu (bytes)</li> <li>• domain ID</li> <li>• description</li> <li>• clientPort (boolean)</li> </ul>
<b>constraintsIn constraintsOut</b>	reservation request	Περιορισμοί για τους συνδέσμους εισόδου/εξόδου στον κόμβο. Η πρόσβαση στους περιορισμούς γίνεται με την εντολή \$constraintsDIR.getConstraintForName('NAME') .value όπου:

		<ul style="list-style-type: none"> <li>• <b>DIR:</b> In/Out</li> <li>• <b>NAME:</b> VLAN / MTU / TIME_SLOTS / SUPPORTS_VLAN_TRANSLATION</li> </ul>
<b>node</b>	reservation request	<p>Τρέχων κόμβος με παραμέτρους:</p> <ul style="list-style-type: none"> <li>• ipAddress</li> <li>• name</li> <li>• description</li> <li>• status</li> <li>• vendor</li> <li>• model</li> <li>• osName (όνομα λειτουργικού συστήματος)</li> <li>• osVersion (έκδοση λειτουργικού συστήματος)</li> </ul>
<b>nodeType</b>	TP	<p>Είδος κόμβου:</p> <ul style="list-style-type: none"> <li>• ingress (πρώτος κόμβος μονοπατιού)</li> <li>• egress (τελευταίος κόμβος μονοπατιού)</li> <li>• internal (ενδιάμεσος κόμβος μονοπατιού)</li> <li>• local (το μονοπάτι περιλαμβάνει μόνο ένα κόμβο)</li> </ul>
<b>nodesCount</b>	TP	Συνολικός αριθμός κόμβων προς επεξεργασία
<b>this</b>	TP	Πρόσβαση στο ίδιο το στοιχείο και τις δικές του ιδιότητες/μεθόδους που υλοποιούνται με την αναφορά <i>\$this</i> .

Τέλος, για λόγους επεξεργασίας των αλφαριθμητικών στοιχείων του αρχείου configuration χρησιμοποιείται ένας συντακτικός αναλυτής (text parser), ο οποίος καλείται με την εντολή *\$parser*.

---

#### 4.2.7 ΚΑΘΟΡΙΣΜΟΣ ΕΥΡΟΥΣ ΖΩΝΗΣ

---

Το Carrier Ethernet παρέχει τη δυνατότητα καθορισμού συγκεκριμένου εύρους ζώνης για ένα δίκτυο. Για το σκοπό αυτό, οι μεταγωγείς Carrier Ethernet διαθέτουν μια λειτουργία **προφίλ εύρους ζώνης (bandwidth profiles)**. Ένα προφίλ εύρους ζώνης καθορίζει την κίνηση των πλαισίων Ethernet σε μια εξωτερική διεπαφή, UNI ή NNI. Τα προφίλ εισόδου εφαρμόζονται σε πλαίσια που εισέρχονται στη διεπαφή και συνδέονται με μια EVC ή OVC, ενώ τα προφίλ εξόδου εφαρμόζονται στα πλαίσια που εξέρχονται από τη διεπαφή. Τα οφέλη από την ύπαρξη προφίλ εύρους ζώνης είναι αφενός η δυνατότητα του συνδρομητή να αγοράζει μόνο το ποσό εύρους ζώνης που απαιτείται, αφετέρου η δυνατότητα του παρόχου να περιορίζει το ποσό του εύρους ζώνης που εισέρχεται στο δίκτυό του, σύμφωνα με τους όρους του SLA. Τα προφίλ εύρους ζώνης παρέχουν επίσης τη δυνατότητα υποστήριξης πολλαπλών EVCs (ή OVCs) στην ίδια UNI, διαιρώντας το εύρος ζώνης της διεπαφής μεταξύ των EVCs (ή OVCs). Ακόμα και στην ίδια EVC όμως, το εύρος ζώνης μπορεί να διαιρεθεί ανάλογα με CoS χαρακτηριστικά.

Κάθε προφίλ εύρους ζώνης προσδιορίζεται από τα εξής χαρακτηριστικά:

- **Committed Information Rate (CIR):** Καθορίζει το εύρος ζώνης του δικτύου, σύμφωνα με τις εγγυήσεις του SLA. Οι μετρήσεις της απόδοσης, σχετικά με την καθυστέρηση ή την απώλεια πλαισίων, γίνονται σύμφωνα με το CIR. Κίνηση με εύρος ζώνης που δεν συμμορφώνεται με το CIR εξαιρείται από τις μετρήσεις της απόδοσης και απορρίπτεται από το δίκτυο.
- **Excess Information Rate (EIR):** Καθορίζει το ποσό της υπέρβασης του εύρους ζώνης, που επιτρέπεται στο δίκτυο. Το EIR αυξάνει τη συνολική διαμετακομιστική ικανότητα της κυκλοφορίας, αλλά χωρίς να παρέχει εγγυήσεις, όπως συμβαίνει με το CIR. Κίνηση με εύρος ζώνης άνω του EIR θεωρείται «υπερβολική» και ως εκ τούτου δεν δρομολογείται.
- **Committed Burst Size (CBS) και Excess Burst Size (EBS):** Καθορίζουν το μέγιστο αριθμό bytes που μπορεί να εγχέεται στο δίκτυο, σύμφωνα πάντα με το CIR και το EIR αντίστοιχα. Για παράδειγμα, εάν το CBS είναι 50 KB, τότε μόνο πλαίσια Ethernet των 50 KB μπορούν να διοχετεύονται και να γίνονται αποδεκτά από το δίκτυο, αν επιπλέον συμφωνούν με το CIR. Αν μεταδίδονται

περισσότερα από 50 KB, το ποσό που υπερβαίνει τα 50 KB είτε θα απορρίπτεται,  $EIR=0$ , είτε θα αναγνωρίζεται ως υπερβολική κίνηση, αν  $EIR \neq 0$ . Αν η υπερβολική κυκλοφορία ξεπερνά το EBS, τότε απορρίπτεται.

- **Color Mode (CM):** Τα πλαίσια Ethernet που εισέρχονται σε μια UNI δηλώνονται πράσινα αν συμφωνούν με το CIR/CBS, κίτρινα αν δε συμφωνούν με το CIR/CBS αλλά συμφωνούν με το EIR/EBS, ή κόκκινα αν δε συμφωνούν ούτε με το CIR/CBS ούτε με το EIR/EBS. Τα κόκκινα πλαίσια πάντα απορρίπτονται, τα κίτρινα απορρίπτονται όταν υπάρχει συμφόρηση στο δίκτυο και τα πράσινα δεν πρέπει να απορρίπτονται ποτέ. Το CM καθορίζει εάν ο πάροχος υπηρεσιών πρέπει να λάβει υπ'όψιν του την προηγούμενη χρωματική σήμανση των πλαισίων Ethernet, η οποία είτε έχει γίνει από τον εξοπλισμό του συνδρομητή ή χρησιμοποιούνταν προηγουμένως στο LAN του. Αν το CM είναι απενεργοποιημένο, οι προηγούμενοι χρωματισμοί αγνοούνται, διαφορετικά συνυπολογίζονται σε μεταγενέστερες αποφάσεις δρομολόγησης. Στις περισσότερες Ethernet υπηρεσίες το CM είναι απενεργοποιημένο, καθώς οι συνδρομητές σπάνια, αν όχι ποτέ, εφαρμόζουν συστήματα διαχείρισης κυκλοφορίας στο LAN τους, ώστε να υπάρχει οποιαδήποτε χρωματική σήμανση των πλαισίων Ethernet τους.

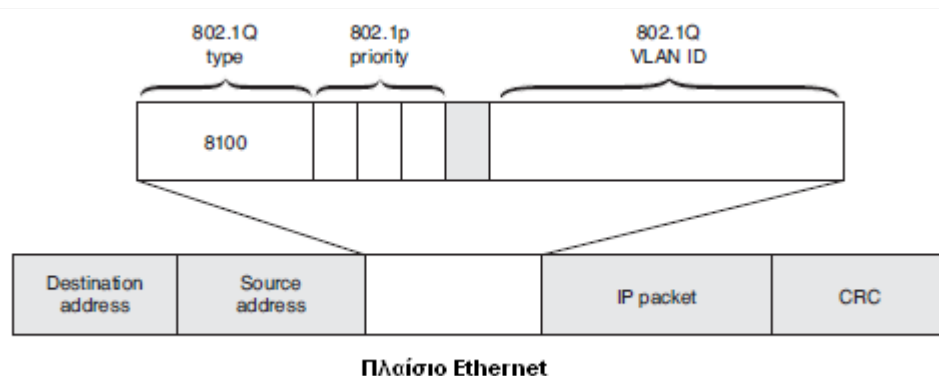
Στους μεταγωγείς της Extreme Networks, ο καθορισμός του εύρους ζώνης γίνεται στα πλαίσια των λειτουργιών QoS. Σύμφωνα με αυτές, υπάρχουν δύο προσφερόμενοι τύποι:

- **Single Rate-QoS:** καθορίζει μια ενιαία τιμή εύρους ζώνης για την κυκλοφορία που υπόκειται σε QoS. Είναι η πιο βασική μορφή περιορισμού της ταχύτητας μετάδοσης δεδομένων και είναι κατάλληλη για εφαρμογές συνεχούς ροής, όπως βίντεο. Η κίνηση που ικανοποιεί την τιμή αυτή θεωρείται *in-profile* (μαρκάρεται πράσινη) και προωθείται, διαφορετικά θεωρείται *out-of-profile* (μαρκάρεται κόκκινη) και είτε απορρίπτεται, είτε προωθείται όταν υπάρχει διαθέσιμο περισευούμενο εύρος ζώνης. Ανάλογα με το μοντέλο του μεταγωγέα, καθορίζεται κάποιο **Peak Rate (PR)** ή **CIR/PBS (Peak Burst Size)** για τη διάκριση της in/out-of-profile κίνησης.
- **Dual Rate-QoS:** καθορίζει δύο τιμές εύρους ζώνης για την κυκλοφορία που υπόκειται σε QoS. Η χαμηλότερη μεταξύ των δύο είναι το PR, το οποίο

θεσπίζει ένα άνω όριο εύρους ζώνης. Η Dual Rate-QoS χρησιμοποιείται ευρέως σε δίκτυα Frame Relay και ATM μισθωμένες γραμμές. Η κίνηση κάτω του PR θεωρείται in-profile, μαρκάρεται πράσινη και η προωθείται. Η κίνηση άνω του CIR ή κάτω του PIR (Peak Information Rate) θεωρείται out-of-profile και μαρκάρεται κίτρινη. Κίνηση άνω του PIR είναι επίσης out-of-profile και μαρκάρεται κόκκινη. Όταν εισερχόμενη κίνηση έχει ήδη μαρκαριστεί κίτρινη και θεωρείται out-of-profile, μαρκάρεται κόκκινη. Διαφορετικά μοντέλα μεταγωγέων χειρίζονται διαφορετικά την κίνηση που μαρκάρεται κίτρινη ή κόκκινη.

Τα στοιχεία που χρησιμοποιούνται για τον καθορισμό του εύρους ζώνης είναι τα ακόλουθα:

- **Μετρητές (Meters)**
- **Προφίλ QoS εισόδου (Ingress QoS Profiles):** χρησιμοποιούν την τιμή 802.1p (3 bit στην επικεφαλίδα των πλαισίων Ethernet) για τη διάκριση της προτεραιότητας της κυκλοφορίας. Ανάλογα με την τιμή αυτή, διακρίνονται μέχρι και 8 προφίλ.



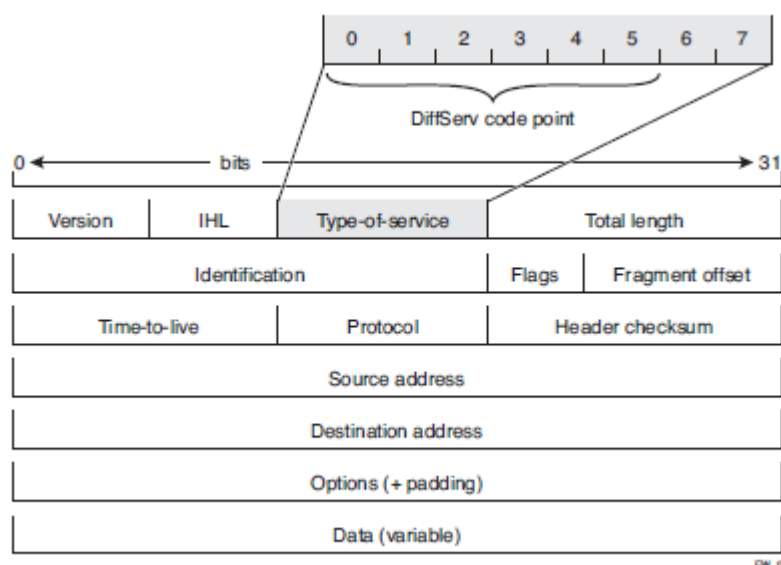
**Εικόνα 29:** 802.1p bit προτεραιότητας (ExtremeXOS 12.5.3 Concepts Guide)



Ingress 802.1p Priority Value	Ingress QoS Profile	Default Queue Service Priority Value
0	IQP1	1 (Low)
1	IQP2	2 (LowHi)
2	IQP3	3 (Normal)
3	IQP4	4 (NormalHi)
4	IQP5	5 (Medium)
5	IQP61	6 (MediumHi)
6	IQP7	7 (High)
7	IQP8	8 (HighHi)

**Πίνακας 4:** Ingress QoS Profiles (ExtremeXOS 12.5.3 Concepts Guide)

- **Προφίλ QoS εξόδου (Egress QoS Profiles):** διακρίνουν την προτεραιότητα της κυκλοφορίας ανάλογα με την τιμή 802.1p, το DiffServ Code Point (DSCP), τη θύρα ή το VLAN στο οποίο ανήκει η θύρα στην οποία εξέρχεται η κυκλοφορία.



**Εικόνα 30:** DiffServ Code Point (ExtremeXOS 12.5.3 Concepts Guide)

Traffic Group Code Point	Egress QoS Profile
0-7	QP1
8-15	QP2
16-23	QP3
24-31	QP4
32-39	QP5
40-47	QP6
48-55	QP7
56-63	QP8

**Πίνακας 5:** Egress QoS Profiles (ExtremeXOS 12.5.3 Concepts Guide)

- **Ουρές κυκλοφορίας εισόδου/εξόδου (Ingress/Egress traffic queues):** διακρίνουν την προτεραιότητα της κυκλοφορίας χρησιμοποιώντας ACLs, οι οποίες συνδέονται με κάθε ουρά κυκλοφορίας, ή την τιμή 802.1p.
- **Θύρα εξόδου (Egress Port)**

---

#### ***4.2.8 ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΕΙΡΑΜΑΤΙΚΟΥ ΕΛΕΓΧΟΥ***

---

Στους μεταγωγείς BlackDiamond 12804, που χρησιμοποιήθηκαν στο πείραμα, υποστηρίζονται μόνο τα προφίλ QoS εξόδου με χρήση της τιμής 802.1p. Επειδή, όμως, στο PBBN που δημιουργήσαμε δε μπορούμε να «εξάγουμε» την πληροφορία 802.1p από τα πλαίσια Ethernet, δεν καταστάθηκε δυνατός ο καθορισμός ενός συγκεκριμένου εύρους ζώνης. Η μόνη πληροφορία που διαθέτουμε είναι η ετικέτα VLAN, η οποία θα μπορούσε να χρησιμοποιηθεί αν υλοποιούσαμε το σύστημα με μεταγωγείς που υποστηρίζουν τον καθορισμό του εύρους ζώνης με βάση το VLAN προέλευσης.

Κατ'ανάλογο τρόπο, εφόσον δεν καταστάθηκε δυνατός ο διαχωρισμός της κίνησης, δεν υλοποιήθηκε κάποιου είδους καταμερισμός φόρτου του δικτύου, γι'αυτό και η επιλογή του μονοπατιού δρομολόγησης μέσα στο PBBN καθορίζεται αποκλειστικά από την αίτηση δέσμευσης του DM.

Είναι, τέλος, θέμα χρόνου να μας παραχωρηθεί εξουσιοδότηση από το Πανεπιστήμιο του Essex, όπου βρίσκεται η πλατφόρμα δοκιμών που χρησιμοποιήθηκε για την ανάπτυξη του CGE TP, για την εκτέλεση πειραμάτων, προκειμένου να επιβεβαιωθεί η ορθότητα της υλοποίησής μας.



---

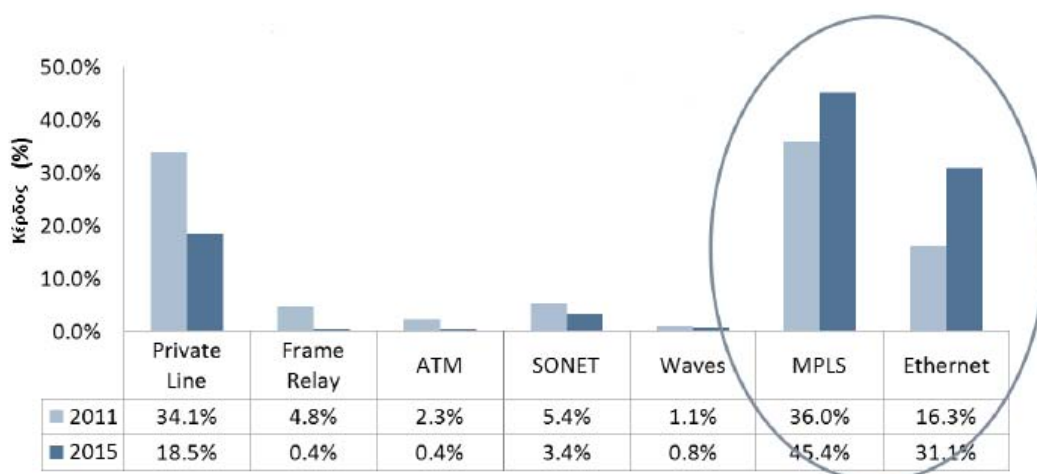
## ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ

---

Το Ethernet, εξαιτίας της μακράς ιστορίας του, έχει πλέον ωριμάσει και είναι ευρέως υλοποιούμενο, κρατώντας ήδη τα ηνία στη LAN δικτύωση, ενώ συνεχίζεται η εξέλιξη και βελτίωσή του. Όντας ευέλικτο, έχει αντέξει το πέρασμα του χρόνου και τον ανταγωνισμό των υπόλοιπων τεχνολογιών δικτύωσης. Προσφέρει μεγάλες ταχύτητες, υψηλή ανθεκτικότητα και μια πληθώρα άλλων χρήσιμων υπηρεσιών με εγγυημένη ποιότητα. Από άποψη κόστους, είναι σημαντικά οικονομικότερο από άλλες WAN τεχνολογίες, καθώς δεν απαιτεί την εκπαίδευση του προσωπικού σε νέα δεδομένα, ενώ σημαντικά μικρότερο είναι το κόστος λειτουργίας και αναβάθμισης του εξοπλισμού του.

Σε αυτό το πλαίσιο, το Carrier Ethernet αποτελεί μια πολύ σημαντική εξέλιξη του Ethernet, με ό,τι αυτό συνεπάγεται. Οι πάροχοι δικτυακών υπηρεσιών, αλλά και οι τελικοί χρήστες, «βλέπουν» στο Carrier Ethernet μια πολύ καλή λύση για τη σύγκλιση διαφορετικών δικτύων, με μειωμένες κεφαλαιουχικές δαπάνες και κόστος λειτουργίας, προσφορά ευέλικτων υπηρεσιών και υψηλού ρυθμού μετάδοσης δεδομένων, εξειδικευμένες λύσεις και πανταχού πρόσβαση. Επίσης, η τυποποίησή του εγγυάται ότι τα προϊόντα του θα περάσουν από ελέγχους πιστοποίησης ποιότητας.

Αυτό που μένει να αναρωτηθούν οι πάροχοι δικτυακών υπηρεσιών είναι το εξής: Αξίζει να συνδυαστούν οι υπάρχουσες τεχνολογίες μεταφοράς μιας επιχείρησης με τεχνολογίες Ethernet, σε μια κοινή υποδομή; Με άλλα λόγια, αν οι υπάρχουσες τεχνολογίες TDM/ATM έχουν περιοριστεί σε μικρή έως καμία ανάπτυξη, αξίζει τον κόπο και τα έξοδα να συνδυαστούν, στο ίδιο δίκτυο, με τις υψηλής ανάπτυξης Ethernet και IP υπηρεσίες; Το υπάρχον δίκτυο ενδέχεται να έχει ήδη αποσβεστεί και να λειτουργεί στη βέλτιστη αποδοτικότητα, οπότε η καλύτερη προσέγγιση θα ήταν να παραμείνει στη θέση του μέχρι η λειτουργικότητά του να μειωθεί σημαντικά ή να αντικατασταθεί πλήρως από το Ethernet. Κατά την εκτίμηση των επιλογών για την εφαρμογή Carrier Ethernet είναι απαραίτητο να εξεταστεί το σύνολο των ικανοτήτων του οργανισμού και τα εργαλεία OAM που διαθέτει για την ανάπτυξη και την υποστήριξη της συγκεκριμένης τεχνολογίας.



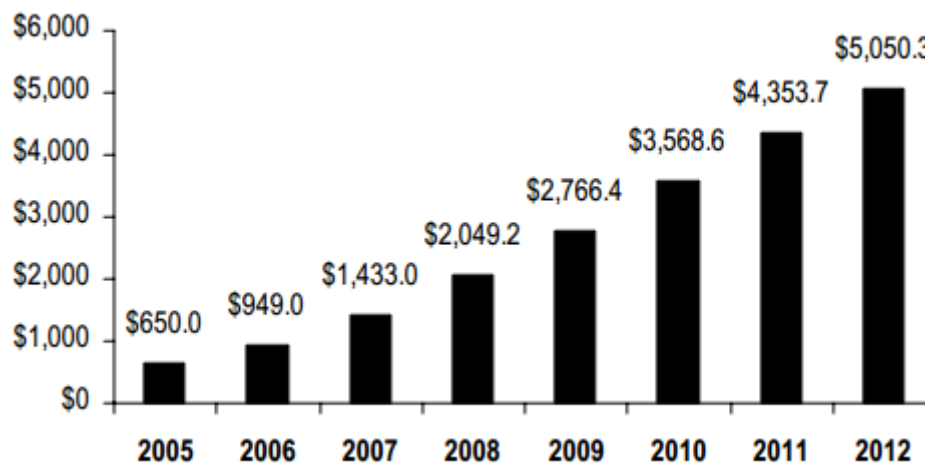
**Εικόνα 31:** Εξέλιξη των εσόδων της αγοράς τεχνολογιών μεταφοράς δεδομένων (Frost & Sullivan, BCS 5-7: U.S. Data Transport Services Market Update, 2011)

Υπάρχει επίσης ο περιορισμός της μη άμεσης μεταφοράς των υπηρεσιών αυτών από τοπικό επίπεδο σε ευρεία περιοχή, καθώς μπορεί να υπερβούν τις προβλέψεις συνολικής διαθεσιμότητας και αυτό να οδηγήσει σε απαράδεκτη ποιότητα. Οι υπηρεσίες που προσπαθούν να επεκταθούν πολύ γρήγορα χάνουν χρήματα, ενώ εκείνες που καθυστερούν πάρα πολύ χάνουν πελάτες. Συνεπώς, οι πάροχοι υπηρεσιών Carrier Ethernet πρέπει να τις επεκτείνουν με σύνεση και να δίνουν μεγάλη προσοχή στην ποιότητα υπηρεσιών (QoS).

Παρ' όλα αυτά, η γρήγορη πρόοδος της εργασίας των φορέων Carrier Ethernet και τα πλεονεκτήματα που απολαμβάνουν οι πρώτοι ανάδοχοι των υπηρεσιών του, έχουν ενδυναμώσει τις θετικές προοπτικές των αναλυτών που παρακολουθούν την αγορά του Carrier Ethernet.

Στην πραγματικότητα, ολόκληρη η αγορά τηλεπικοινωνιακού εξοπλισμού εκτιμάται ότι υπερέβει τα 110 δις. δολάρια μέσα στο 2011. Αυτή περιλαμβάνει οπτικά δίκτυα, υποδομές βίντεο, δρομολόγησης και μεταγωγής, καθώς και First Mile πρόσβαση. Το Carrier Ethernet, υποστηρίζοντας αυτές τις υποδομές και υπηρεσίες, επωφελείται από αυτή την ανάπτυξη. Το 2006 η παγκόσμια αγορά Carrier Ethernet

εξοπλισμού έφθασε τα 6,1 δις. δολάρια, ενώ μέχρι το τέλος του 2011 η αγορά αυτή αυξήθηκε πάνω 17 δις. δολάρια. Η παρακάτω εικόνα δείχνει την αύξηση των κερδών από τη χρήση υπηρεσιών Carrier Ethernet (σε εκατ. δολλάρια) στις ΗΠΑ.



**Εικόνα 32:** Συνολικά κέρδη Ethernet στις ΗΠΑ (The Insight Research Corporation, Public Ethernet Services 2007-2012)

Ο πίνακας δείχνει το ξέσπασμα των παγκοσμίων εσόδων από τις Carrier Ethernet υπηρεσίες ανά περιοχή, για το διάστημα 2006 - 2011.

	2006	2011	Ετήσιο Ποσοστό Αύξησης (%)
<b>Βόρεια Αμερική</b>	1,723	6,039	28
<b>Λατινική Αμερική</b>	0,016	0,058	29
<b>Ευρώπη, Μέση Ανατολή, Αφρική</b>	1,646	4,525	22
<b>Ασία</b>	2,779	6,928	20
<b>Σύνολο</b>	6,164	17,550	23

**Πίνακας 6:** Παγκόσμια έσοδα Carrier Ethernet υπηρεσιών για το 2006-2011 ανά περιοχή (IDC, 2008)

Αυτή η ενοποιημένη προσέγγιση στο κόστος του Carrier Ethernet επεκτείνει ουσιαστικά τα οφέλη του Ethernet, βοηθώντας τόσο τους παρόχους όσο και τους τελικούς χρήστες των υπηρεσιών Carrier Ethernet να επιτύχουν σημαντική εξοικονόμηση κόστους. Απαράμιλλες οικονομίες κλίμακας προκύπτουν από επιχειρησιακά, οικιακά και ασύρματα δίκτυα που μοιράζονται την ίδια υποδομή. Στον πίνακα που ακολουθεί παρουσιάζεται η εξέλιξη των ποσοστών χρήσης των υπηρεσιών Carrier Ethernet στις προαναφερθείσες υποδομές, στο διάστημα 2006 – 2012.

	2006	2007	2008	2009	2010	2011	2012
<b>Οικιακές Υποδομές</b>	28	33	38	39	40	40	40
<b>Επιχειρησιακές Υποδομές</b>	68	63	56	51	45	42	42
<b>Ασύρματες Τηλεπικοινωνίες</b>	4	4	6	10	15	18	18

**Πίνακας 7:** Εξέλιξη χρήσης Carrier Ethernet υπηρεσιών % (IDC, 2008)

Σχετικά με το πείραμα που διεξήχθη στα πλαίσια της παρούσας διπλωματικής εργασίας, στόχος μας ήταν η ανάπτυξη μιας Bandwidth on Demand υπηρεσίας με χρήση εξοπλισμού Carrier Ethernet. Η σημασία της BoD υπηρεσίας, η οποία αναπτύσσεται μέχρι στιγμής σε ευρωπαϊκό-ακαδημαϊκό επίπεδο, είναι κομβική, καθώς δίνει τη δυνατότητα διεθνούς διασύνδεσης και αποτελεσματικής συλλειτουργίας ετερόκλητων δικτύων. Συνδυάζοντας τη σημασία αυτή με την ραγδαία ανάπτυξη και τα οφέλη του Carrier Ethernet, θα μπορούσαμε να εξελίξουμε και να επεκτείνουμε την υπηρεσία BoD πέρα από τα ευρωπαϊκά-εκπαιδευτικά όρια.

Η πλατφόρμα δοκιμών του Πανεπιστημίου του Essex που χρησιμοποιήθηκε μας παρείχε ένα δίκτυο Carrier Ethernet που περιλάμβανε 3 μεταγωγείς, στο οποίο επιτύχαμε να δημιουργήσουμε ένα PBBN tunnel. Με τον τρόπο αυτό, ο TP που αναπτύχθηκε μπορούσε να επιλέγει το μονοπάτι που ακολουθεί η δικτυακή κίνηση,



---

σύμφωνα με την αντίστοιχη αίτηση δέσμευσης κυκλώματος από τον χρήστη. Λόγω, όμως, των περιορισμένων χαρακτηριστικών που διέθετε ο δικτυακός μας εξοπλισμός (μεταγωγείς Extreme BlackDiamond 12804), δεν καταφέραμε να διαχωρίσουμε τη δικτυακή κίνηση διαφορετικών χρηστών μέσα στο PBBN. Αποτέλεσμα αυτού ήταν να μην καταστεί δυνατός ο καθορισμός, από τον χρήστη, συγκεκριμένου εύρους ζώνης, καθώς και ο καταμερισμός φόρτου δικτυακής κίνησης μεταξύ διαφορετικών μονοπατιών, για να αποφευχθεί η συμφόρηση.

Η ανάπτυξη του παρόντος Carrier Ethernet Technology Proxy αποτελεί πρωτότυπο. Στο μέλλον προσδοκούμε να επιτύχουμε την τυποποίηση και την επέκταση της υλοποίησής μας σε μεγαλύτερα δίκτυα, τουτ'έστιν σε δίκτυα που περιλαμβάνουν σημαντικό αριθμό κόμβων και καλύπτουν μεγάλες γεωγραφικές περιοχές σε διεθνές επίπεδο. Επίσης, ευελπιστούμε να καταφέρουμε να επιλύσουμε τα θέματα παροχής συγκεκριμένου εύρους ζώνης και τον καταμερισμού φόρτου δικτυακής κίνησης μέσα στο PBBN, που αναφέρθηκαν προηγουμένως, χρησιμοποιώντας ενδεχομένως διαφορετικό δικτυακό εξοπλισμό με τα επιθυμητά χαρακτηριστικά.



---

**AKRONYMA**

---

**A**

---

<b>ACL</b>	Access Control List
<b>ATM</b>	Asynchronous Transfer Mode

---

**B**

---

<b>BCB</b>	Backbone Core Bridge
<b>B-DA</b>	Backbone Destination MAC Address
<b>BEB</b>	Backbone Edge Bridge
<b>BoD</b>	Bandwidth on Demand
<b>B-SA</b>	Backbone Source MAC Address
<b>B-VID (B-tag)</b>	Backbone VLAN ID
<b>BVLAN</b>	Backbone Virtual LAN

---

**C**

---

<b>CBS</b>	Committed Burst Size
<b>CCM</b>	Connectivity Check Message
<b>CFM</b>	Connectivity Fault Management
<b>CGE</b>	Carrier Grade Ethernet
<b>CIR</b>	Committed Information Rate
<b>CM</b>	Color Mode
<b>CoS</b>	Class of Service
<b>C-tag</b>	Customer tag
<b>CVLAN</b>	Customer Virtual LAN

---

---

**D**

---

<b>DM</b>	Domain Manager
-----------	----------------

---

**E**

---

<b>EBS</b>	Excess Burst Size
<b>EIR</b>	Excess Information Rate
<b>EPL</b>	Ethernet Private Line
<b>EVC</b>	Ethernet Virtual Connection
<b>EVPL</b>	Ethernet Virtual Private Line

---

**F**

---

<b>FDB</b>	Forwarding Data Base
------------	----------------------

---

**I**

---

<b>IDM</b>	Inter Domain Manager
<b>I-SID (I-tag)</b>	Service Instance VLAN ID
<b>ISP</b>	Internet Service Provider

---

**L**

---

<b>LAN</b>	Local Area Network
<b>LLDP</b>	Link Layer Discovery Protocol

---

---

**M**

---

<b>MAN</b>	Metropolitan Area Network
<b>MD</b>	Maintenance Domain
<b>MEP</b>	Maintenance End Point
<b>MIP</b>	Maintenance Intermediate Point
<b>MPLS</b>	Multi Protocol Label Switching

---

**N**

---

<b>NMS</b>	Network Management System
<b>NNI</b>	Network to Network Interface
<b>NOC</b>	Network Operations Center

---

**O**

---

<b>OAM</b>	Operation Administration and Maintenance
<b>OVC</b>	Operator Virtual Connection

---

**P**

---

<b>PBBN</b>	Provider Backbone Bridges Network
<b>PBB-TE</b>	Provider Backbone Bridges – Traffic Engineering
<b>PBN</b>	Provider Bridges Network
<b>PBS</b>	Peak Burst Size
<b>PIR</b>	Peak Information Rate
<b>PR</b>	Peak Rate

---

---

**Q**

---

<b>QoS</b>	Quality of Service
------------	--------------------

---

**S**

---

<b>SLA</b>	Service Level Agreement
------------	-------------------------

<b>SP</b>	Service Provider
-----------	------------------

<b>S-tag</b>	Service tag
--------------	-------------

<b>STP</b>	Spanning Tree Protocol
------------	------------------------

<b>SVLAN</b>	Service Virtual LAN
--------------	---------------------

---

**T**

---

<b>TDM</b>	Time Division Multiplexing
------------	----------------------------

<b>TLV</b>	Type – Length - Value
------------	-----------------------

<b>TP</b>	Technology Proxy
-----------	------------------

---

**U**

---

<b>UNI</b>	User Network Interface
------------	------------------------

---

**V**

---

<b>VLAN</b>	Virtual Local Area Network
-------------	----------------------------

<b>vMAN</b>	virtual Metro Area Network
-------------	----------------------------

<b>VPN</b>	Virtual Private Network
------------	-------------------------

---

**W**

---

<b>WAN</b>	Wide Area Network
------------	-------------------

---

---

**ΑΝΤΙΣΤΟΙΧΙΣΗ ΑΓΓΛΙΚΗΣ-ΕΛΛΗΝΙΚΗΣ ΟΡΟΛΟΓΙΑΣ**

---

<b>Bandwidth</b>	Εύρος ζώνης
<b>Bridge</b>	Γέφυρα
<b>Carrier</b>	Υπηρεσία μεταφοράς πληροφοριών
<b>Client</b>	Πελάτης
<b>Configuration</b>	Ρύθμιση
<b>Domain</b>	Τομέας δικτύου
<b>Frame</b>	Πλαίσιο
<b>Header</b>	Επικεφαλίδα
<b>Link</b>	Σύνδεσμος
<b>Node</b>	Κόμβος
<b>Packet</b>	Πακέτο
<b>Port</b>	Θύρα
<b>Router</b>	Δρομολογητής
<b>Service provider (SP)</b>	Πάροχος υπηρεσιών
<b>Server</b>	Διακομιστής
<b>Switch</b>	Μεταγωγέας
<b>Tag</b>	Ετικέτα





---

## ***ΒΙΒΛΙΟΓΡΑΦΙΑ***

---

- [1] Carrier Grade Ethernet (Brocade Inc., 2009)
- [2] Can PBB-TE bridge the gap to next-generation Carrier Ethernet? (ADVA Optical Networking Inc., 2008)
- [3] Carrier Ethernet Essentials (Fujitsu Network Communications Inc., 2010)
- [4] Carrier Ethernet Services Overview (MEF, 2008)
- [5] Technical White Paper for Q-in-Q (Huawei Technologies Co. Ltd, 2007)
- [6] Link Layer Discovery Protocol (LLDP): A New Standard for Discovering and Managing Converged Network Devices (Extreme Networks, 2006)
- [7] AutoBAHN and perfSONAR Integration: Circuit Monitoring (GÉANT, 2011)
- [8] Extreme Networks PBT Strategy (Martin van Schooten, Sr. Director, Worldwide Field Marketing, 2007)
- [9] Generalized Multiprotocol Label Switching (GMPLS) control of Ethernet PBB-TE (IETF, 2009)
- [10] Ethernet OAM (Yaakov Jonathan Stein, RAD Data Communications)
- [11] Technology Proxy Framework for AutoBAHN (Michal Giertych, Jacek Lukasik, 2012)
- [12] ExtremeXOS 12.3.5 Concepts Guide Rev03 (Extreme Networks)
- [13] ExtremeXOS 12.3.5 Command Reference Rev03 (Extreme Networks)
- [14] Ethernet as a Carrier Grade Technology: Developments and Innovations (Lampros Raptis, Kostas Vaxevanakis, 2008)
- [15] Public Ethernet Services 2007-2012 (The Insight Research Corporation, 2007)
- [16] GÉANT Forge – AutoBAHN  
(<https://forge.geant.net/forge/display/autobahn/Home>)
- [17] GÉANT2 Bandwidth on Demand Framework and General Architecture

[18] MPLS vs. PBT: The Empire Strikes Back (Light Reading Insider, vol.7, no.9, September 2007)

[19] Wikipedia ([www.wikipedia.org](http://www.wikipedia.org))

[20] Ericsson Delivers on Carrier Ethernet Solution (Ericsson Inc., 2009)

[21] White Paper: Carrier Ethernet (J. Kloots, V. Olifer, GÉANT 2010)

[22] LLDP-MED and Cisco Discovery Protocol (Cisco Systems Inc., 2006)