ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - NETWORK MANAGEMENT

Εσωτερική Δρομολόγηση L2, L2.5, L3 σε Φορείς (Carrier) του Internet & Πρωτόκολλα Tunneling - Carrier Extensions of Internet Routing, Tunneling Protocols

Αρχιτεκτονικές Carrier σε Layer 2, Provider Backbone Bridges (PBB)

Layer 2.5 Multi-Protocol Label Switching (MPLS) σε Δίκτυα Carrier

Εικονικά Ιδιωτικά Δίκτυα - Virtual Private Networks (VPNs): Πρωτόκολλα Tunneling, Virtual eXtended LANs (VXLANs), IPsec & GRE

Β. Μάγκλαρης

maglaris@netmode.ntua.gr

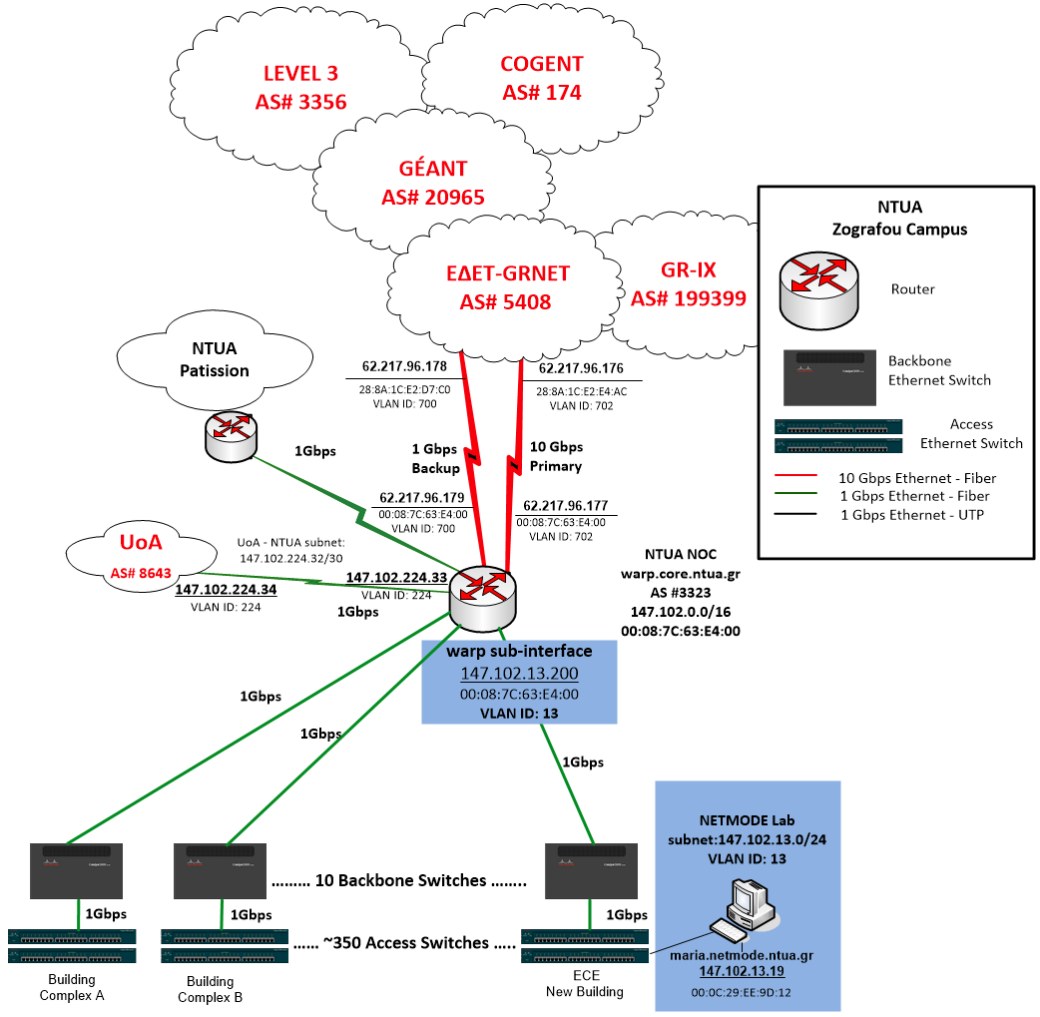
www.netmode.ntua.gr

Νέα Κτίρια ΣΗΜΜΥ - Αίθουσα 013

20/11/2023

ΠΑΡΑΔΕΙΓΜΑ ΕΣΩΤΕΡΙΚΗΣ ΔΡΟΜΟΛΟΓΗΣΗΣ: ΤΟ ΔΙΚΤΥΟ ΤΟΥ Ε.Μ.Π. *(επανάληψη)*

ntua.gr (147.102.0.0/16, ASN 3323)



ΠΡΟΣΟΧΗ

Οι πίνακες δρομολόγησης στο Internet για λόγους ομοιομορφίας είναι της μορφής:

- ***Prefix Δικτύου/Υποδικτύου Τελικού Προορισμού* :: *Interface Εξόδου προς Επόμενο Κόμβο***

ΠΑΡΑΔΕΙΓΜΑ:

Ο δρομολογητής του Ε.Μ.Π. ***147.102.224.33*** βρίσκει τον δρομολογητή του ΕΚΠΑ ***147.102.224.34*** σαν μέλος του υποδικτύου:

- **147.102.224.32/30** (*παροχή διευθύνσεων από Ε.Μ.Π.*)

Η γραμμή Ε.Μ.Π. – ΕΚΠΑ (όπως όλες οι γραμμές σε Δίκτυα Internet) ορίζεται σαν υποδίκτυο (prefix) με 4 τουλάχιστον διευθύνσεις IP:

- Υποδίκτυο: **147.102.224.32**
- Άκρο Ε.Μ.Π.: **147.102.224.33**
- Άκρο ΕΚΠΑ: **147.102.224.34**
- Broadcast: **147.102.224.35**

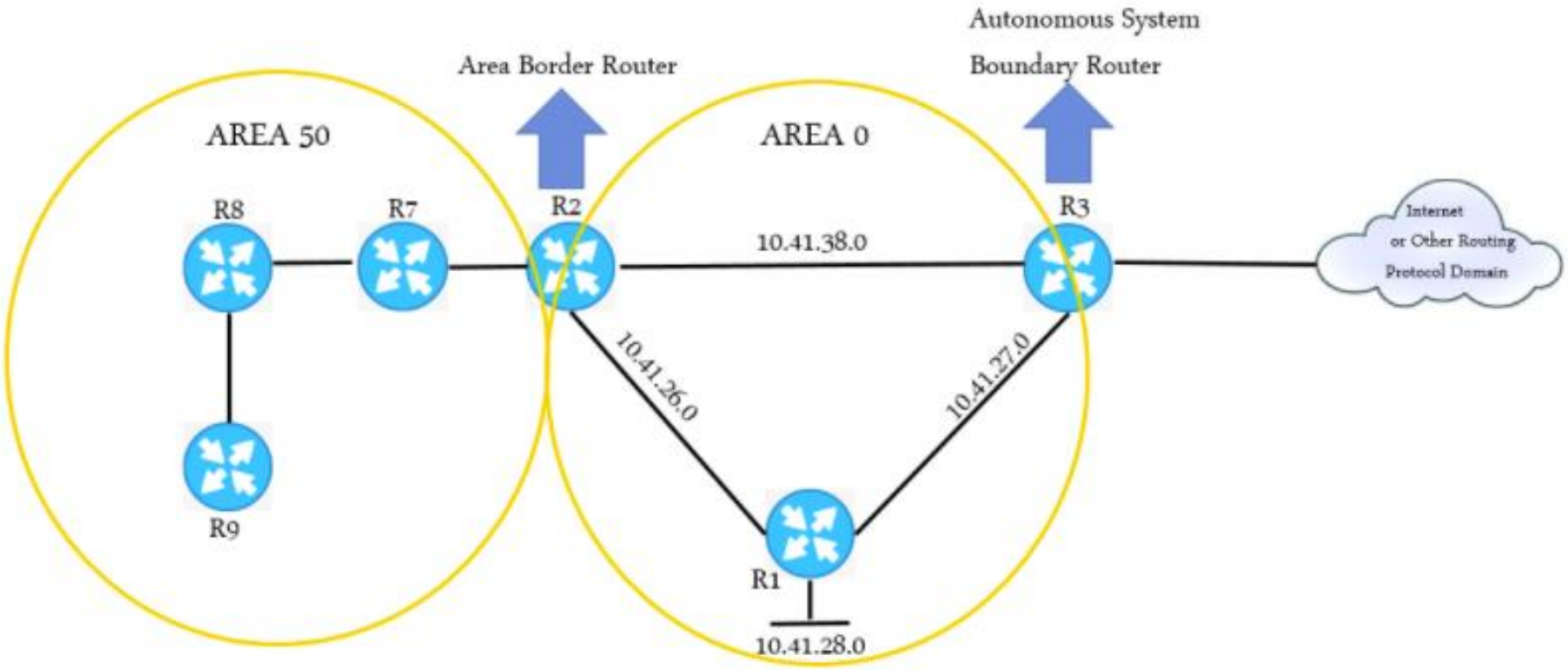
ΑΝΤΙ-ΠΑΡΑΔΕΙΓΜΑ:

Ο δρομολογητής του Ε.Μ.Π. ***62.217.96.177*** βρίσκει τον δρομολογητή του GRNET ***62.217.96.176*** σαν μέλος του υποδικτύου:

- **62.217.96.176/31** (*παροχή διευθύνσεων από GRNET*)

OSPF AREAS *(επανάληψη)*

https://networkel.com/ospf-protocol-ospf-basics-overview/



ABR: Area Border Router
ASBR: Autonomous System Boundary Router
LSA: Link State Advertisement
AREA 0: Backbone Area
AREA 50: Stub Area 50

ΔΡΟΜΟΛΟΓΗΣΗ ΕΠΙΠΕΔΟΥ 2 - MAC/LINK LAYER *(επανάληψη)*

ETHERNET & ΕΙΚΟΝΙΚΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ VLAN (IEEE 802.1Q)

IP ROUTER
warp.core.ntua.gr

00:08:7c:63:e4:00

DG (Default Gateway): 147.102.13.200

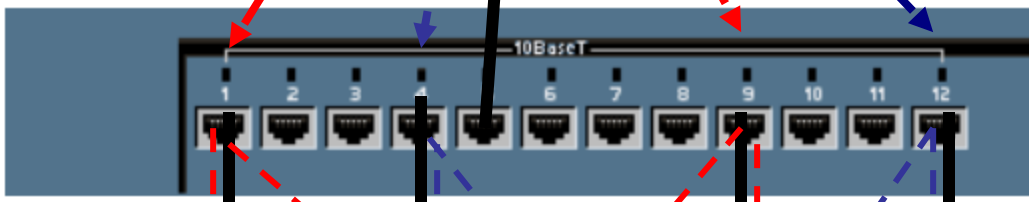
DG:147.102.3.200

VLAN "Red" (VID 00d)
Switch Ports 1 & 9
Subnet 147.102.13.0/24
Default Gateway 147.102.13.200

VLAN "Blue" (VID 003)
Switch Ports 4 & 12
IP Subnet 147.102.3.0/24
Default Gateway 147.102.3.200

ETHERNET SWITCH

Trunk Switch Port 5



ΦΥΣΙΚΗ ΣΥΝΔΕΣΗ:

ΛΟΓΙΚΗ ΔΙΑΣΥΝΔΕΣΗ:

DNS
ARP

matrix.netmode.ntua.gr
147.102.13.60
00:13:a9:34:dd:aa

DG: 147.102.13.200
00:08:7c:63:e4:00

147.102.3.1
00:13:72:f6:5f:83

DG: 147.102.3.200
00:08:7c:63:e4:00

147.102.13.38
00:50:da:51:95:10

DG: 147.102.13.200
00:08:7c:63:e4:00

147.102.3.90
00:16:17:72:72:76

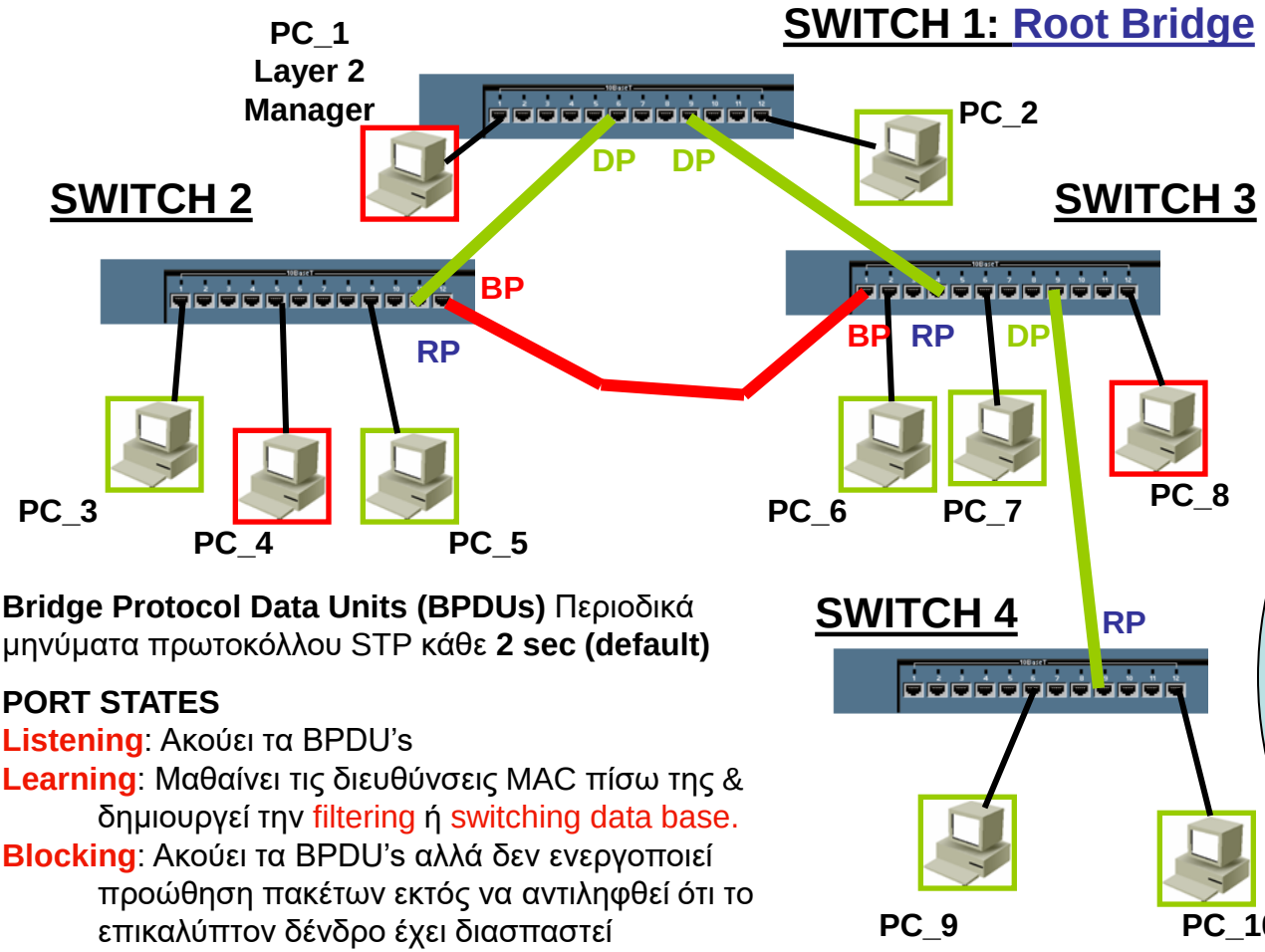
DG: 10.2.0.200
00:08:7c:63:e4:00

802.1Q Framing Add-On's
TPID: Tag Protocol ID
PCP: Priority Code Point
CFI: Canonical Format Identifier
VID: VLAN ID (< 4096)

MAC Address ETHERNET II	TPID	PCP	CFI	VID	IP, TCP/UDP, Data
	16 bits	3 bits	1 bit	12 bits	

ΠΡΩΤΟΚΟΛΛΟ ΔΙΑΜΟΡΦΩΣΗΣ ΔΕΝΔΡΙΚΗΣ ΤΟΠΟΛΟΓΙΑΣ ΜΕΤΑΓΩΓΕΩΝ ETHERNET (2/2) *(επανάληψη)*

Spanning Tree Protocol - STP, IEEE 802.1D



RP: Root Port
DP: Designated Port
BP: Blocked Port

Ενεργή σύνδεση
Ανενεργή σύνδεση

Γνωστό στο Switch 4

Άγνωστο στο Switch 4
Aging: **300 sec (default)**

Forwarding Data Base per Switch Port

Forward to **RP** **(port 9)** MAC frames to known destinations, e.g. PC_6, PC_7, PC_2, PC_3, PC_5 (**RP**: port from which it last heard them prior to aging)

Forward only to **PC_10** (port 12) MAC frames addressed to it & broadcasts

Broadcast unknown destination MAC frames (promiscuous mode)

Bridge Protocol Data Units (BPDUs) Περιοδικά μηνύματα πρωτοκόλλου STP κάθε **2 sec (default)**

PORT STATES

Listening: Ακούει τα BPDU's

Learning: Μαθαίνει τις διευθύνσεις MAC πίσω της & δημιουργεί την filtering ή switching data base.

Blocking: Ακούει τα BPDU's αλλά δεν ενεργοποιεί προώθηση πακέτων εκτός να αντιληφθεί ότι το επικαλύπτον δένδρο έχει διασπαστεί

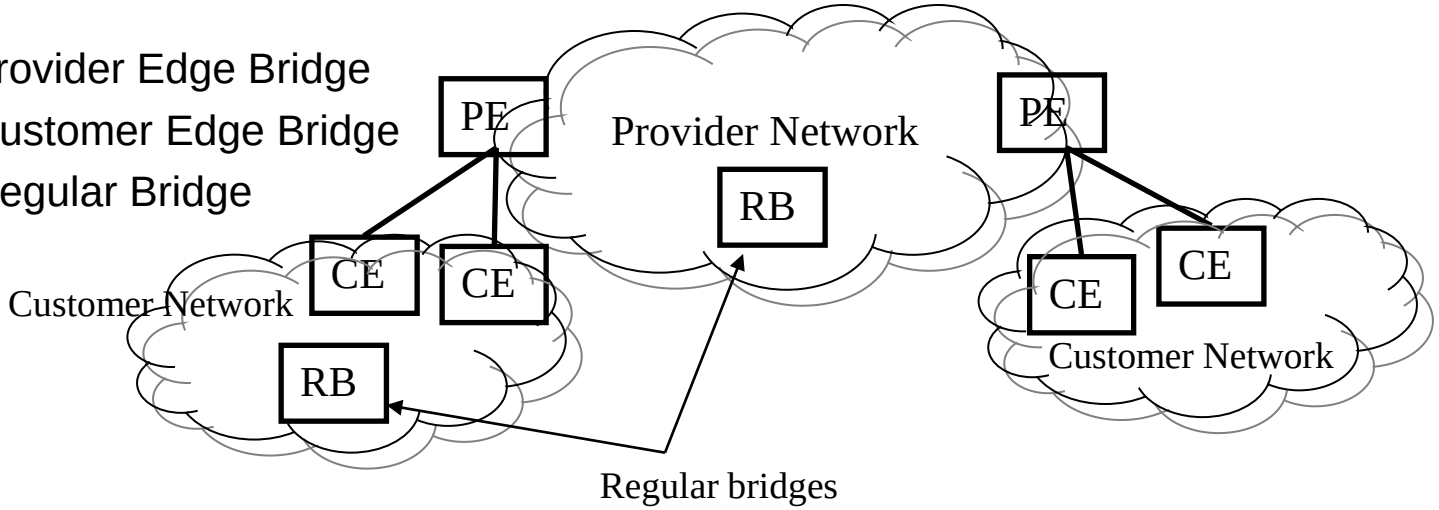
Forwarding: Ακούει τα BPDU's και προωθεί κανονικά τα πακέτα

Disabled: Μη ενεργή

ΔΡΟΜΟΛΟΓΗΣΗ ΕΠΙΠΕΔΟΥ 2 ΣΕ ΔΙΚΤΥΑ ΠΑΡΟΧΩΝ

Provider Backbone Bridges – PBB (mac-in-mac, IEEE 802.1ah)

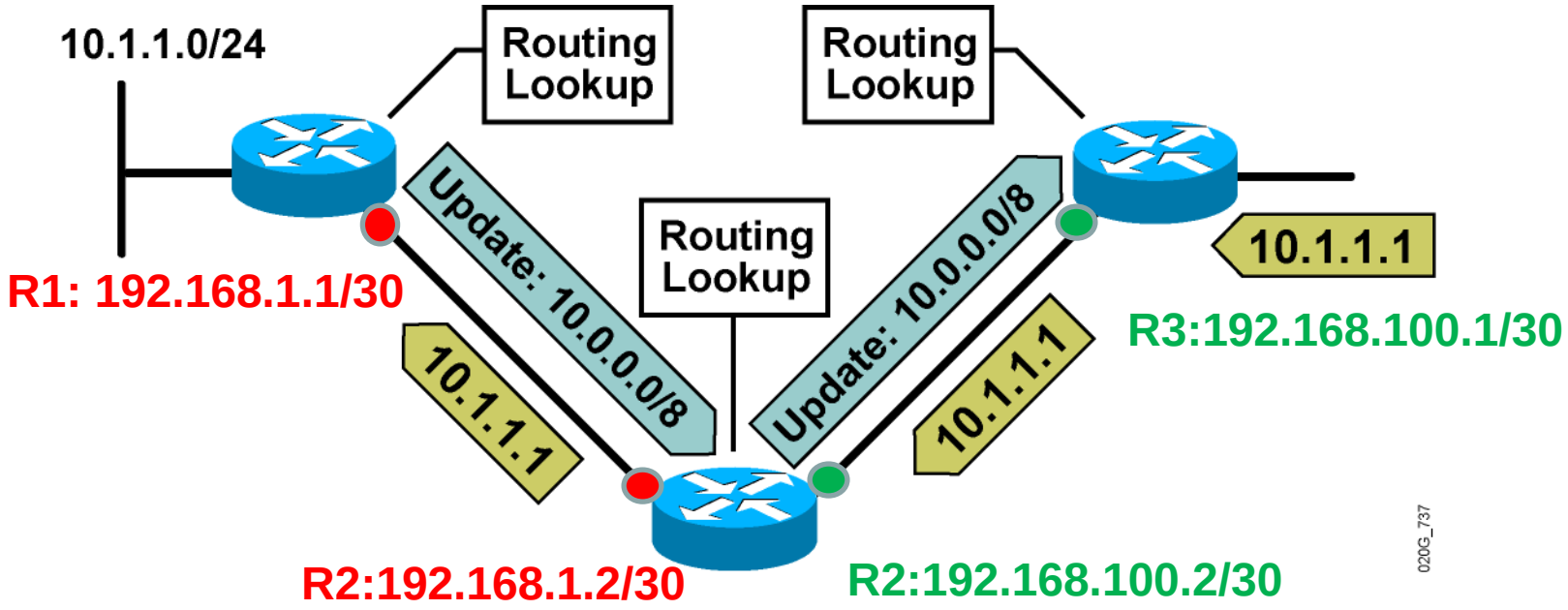
PE: Provider Edge Bridge
CE: Customer Edge Bridge
RB: Regular Bridge



IEEE 802.1ah (2008): Επέκταση Ethernet **LAN**'s (***IEEE 802.3z: 1 GigE, IEEE 802.3ae: 10 GigE***) σε Μητροπολιτικά Δίκτυα **MAN** & Δίκτυα Κορμού Ευρείας Περιοχής **WAN** (***1-10-40-100 GigE***)

- Τυποποίηση πρωτοκόλλων **VPLS**, **mac-in-mac** και **QinQ** tunnels για επέκταση VLAN's μεταξύ τοπικών δικτύων LAN's μέσω Layer 2 VPNs
- Προς συρρίκνωση τοπολογίας επιπέδου 3 → collapsed backbone με μηχανισμούς μεταφοράς επιπέδου 2: **10-100 Gig *point-to-point* Ethernet transport**

ΠΑΡΑΔΟΣΙΑΚΗ ΔΡΟΜΟΛΟΓΗΣΗ ΕΠΙΠΕΔΟΥ 3



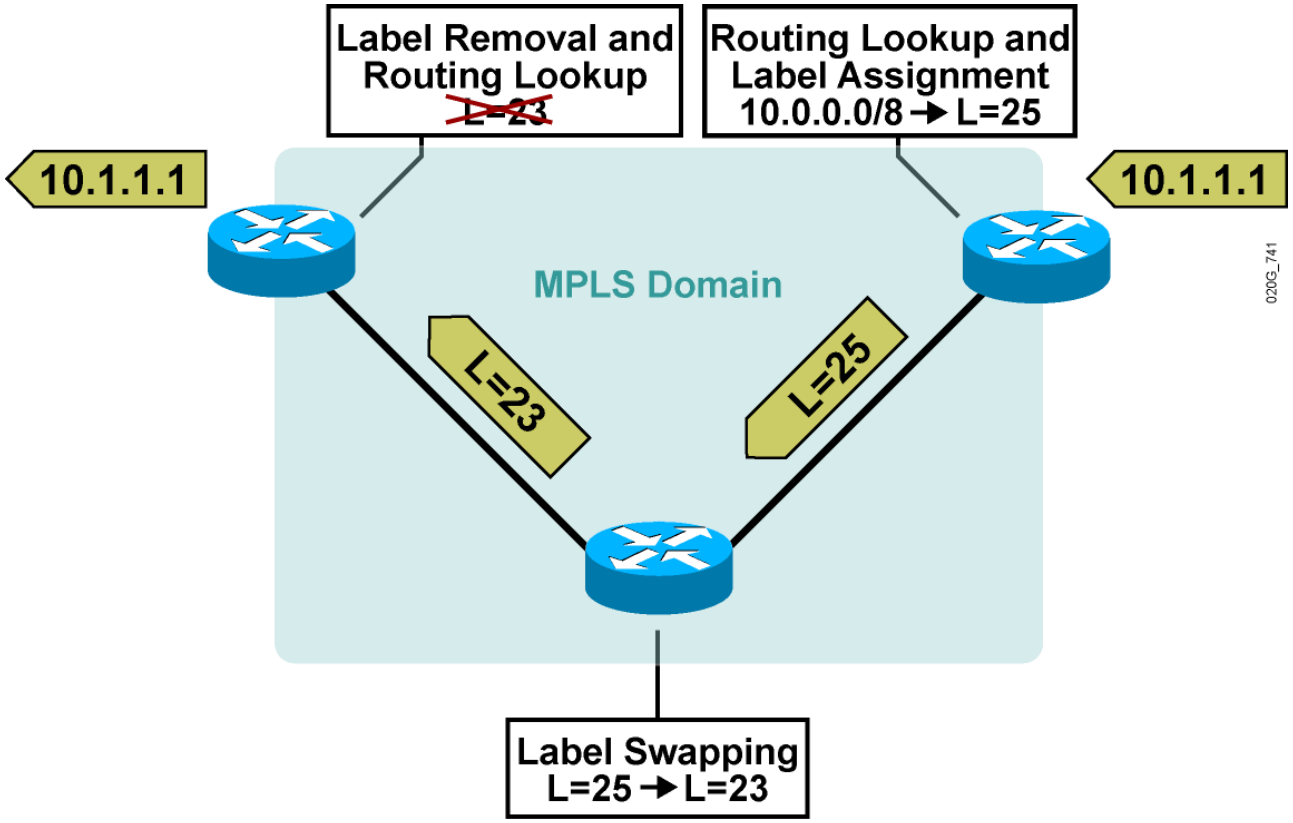
Σε κάθε κόμβο κάθε πακέτο δρομολογείται στο interface του επόμενου κόμβου IP με βάση το longest prefix match της διεύθυνσης IP τελικού προορισμού στον πίνακα δρομολόγησης

ΠΙΝΑΚΑΣ ΔΡΟΜΟΛΟΓΗΣΗΣ Router 2 (R2)

Destination Network	Next-Hop
10.1.1.0/24	192.168.1.1
10.0.0.0/8	192.168.1.1

Longest-prefix match (24bits)

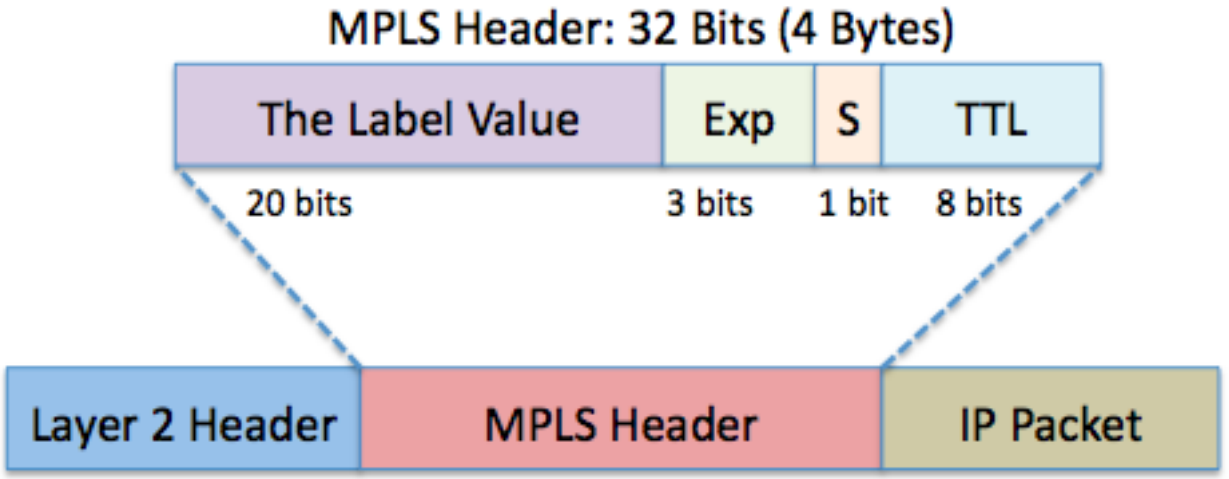
ΔΡΟΜΟΛΟΓΗΣΗ ΕΠΙΠΕΔΟΥ 2.5:
MPLS (Multi-Protocol Label Switching)



MPLS core routers : Label Switch Router – LSR
Αντικαθιστούν (swap) Labels
Προωθούν τα πακέτα με βάση πίνακες δρομολόγησης ανά Label

MPLS edge routers: Edge LSR, Label Edge Router – LER
Εισάγουν/διαγράφουν επικεφαλίδες MPLS
Δρομολογούν με βάση πίνακες δρομολόγησης IP και Labels

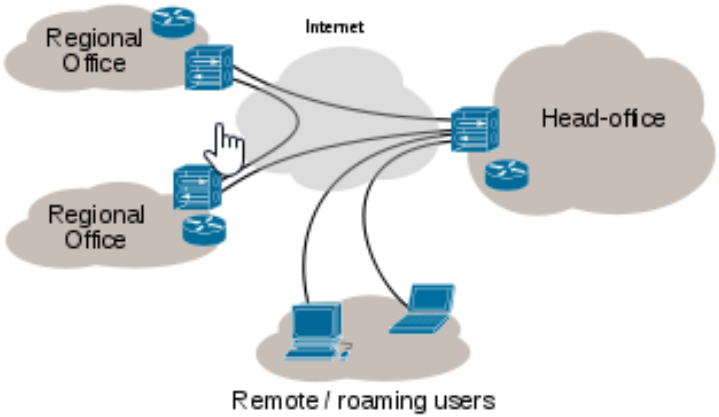
MPLS HEADER



- **Label :** Label value (0 to 15 are reserved for special use) assigned to **source & destination IP (flows) (traffic engineering option)**
- **Exp :** Experimental Use
- **S :** Bottom of Stack (set to 1 for the last entry in the label)
- **TTL :** Time To Live

ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ

Virtual Private Networks - VPNs

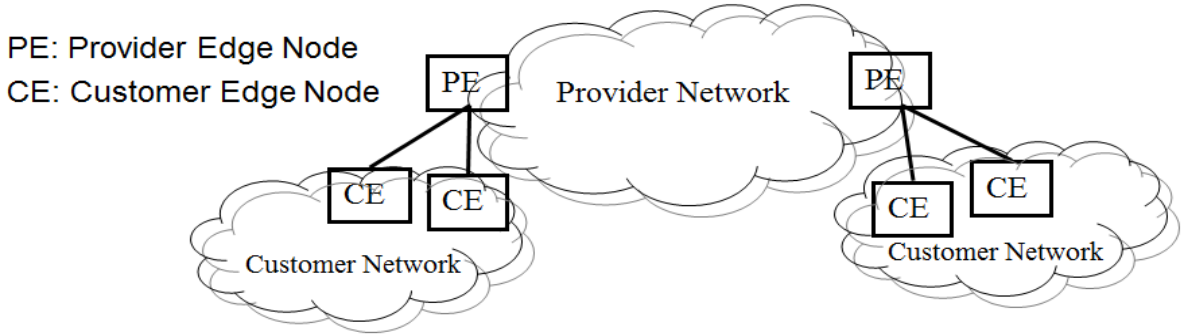


https://en.wikipedia.org/wiki/Virtual_private_network

Με τα **VPNs** χρήστες κοινών κατανεμημένων πόρων δημιουργούν **ιδιωτικές** υποδομές **Overlay Networks** ή εταιρικά δίκτυα **Intranet/Extranet** πάνω από **δημόσια** δίκτυα όπως το **Internet** ή δίκτυο μακράς αποστάσεως (Wide Area Network – WAN) ενός ISP αρχιτεκτονικής **IP/MPLS** ή **Enterprise Local Area Networks - LANs** & **Data Centers** με πολλαπλές αυτόνομες κοινότητες χρηστών, διασφαλίζοντας:

- Απομόνωση από άλλες κοινότητες π.χ. μέσω ενθυλάκωσης πακέτων του VPN (μαζί με τους ιδιωτικούς headers) σε πακέτα συμβατά με πρωτόκολλα Δημοσίου Δικτύου (**tunneling**)
- Διαχείριση δικτυακών πόρων & υπηρεσιών ανά VPN:
  - Επέκταση πεδίου διευθύνσεων **VLAN tags** ή **IP** σε απομακρυσμένες νησίδες ενός VPN
  - Δρομολόγηση με περιορισμούς ασφαλείας και διαμοιρασμού φορτίου – **traffic engineering**
  - Ασφαλής μετάδοση και σηματοδοσία όπως σε αυστηρά ελεγχόμενο τοπικό δίκτυο (LAN)

ΕΙΔΗ VPNs & Tunneling Protocols (1/2)

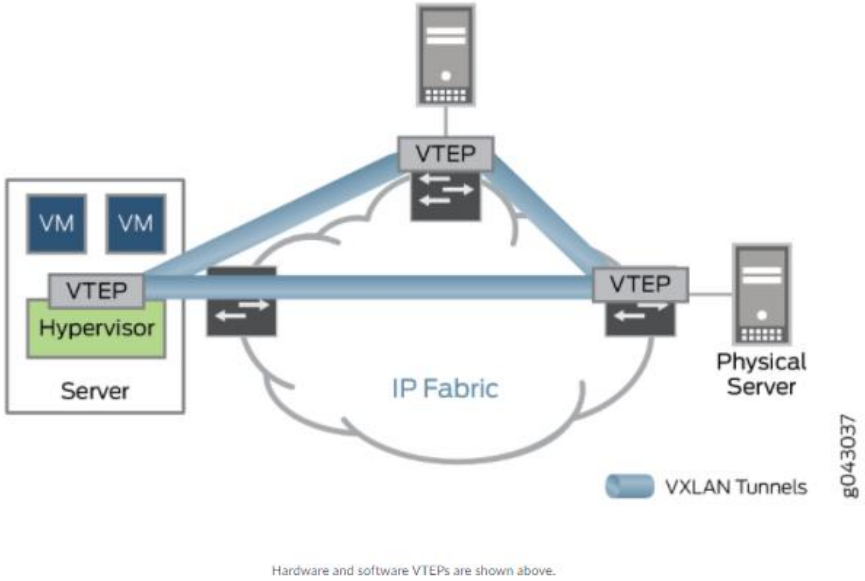


- Layer 2 VPN (**L2VPN**): Επέκταση L2/VLAN over Provider WAN π.χ.
  - Point-to-point **L2TP** (Layer 2 Tunneling Protocol) πάνω από IP/MPLS Provider Network
  - Point-to-point Επεκτάσεις **PW** (Pseudo-Wire) πάνω από IP/MPLS Provider Network
  - Multipoint **VPLS** (Virtual Private LAN Service) πάνω από MPLS Provider Network
  - Επέκταση **Mac-in-Mac** (IEEE 802.1ah) πάνω από L2 Provider Bridge Network

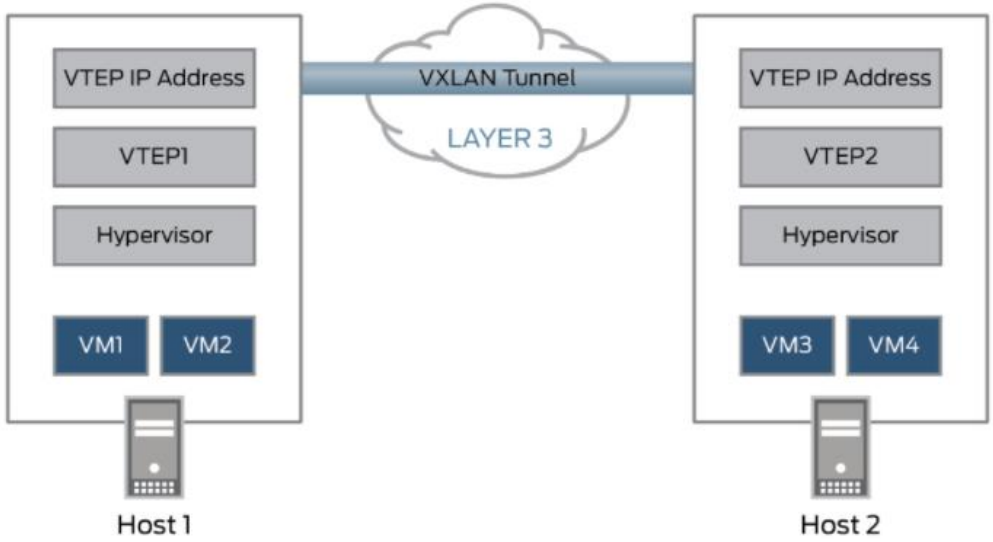
- Layer 3 VPN (**L3VPN**): Λογικές Νησίδες IP σε υποδομές Intranet/Extranet
  - IP ή MPLS tunnels μεταξύ εικονικών δρομολογητών (Virtual Routing & Forwarding, **VRF**) ορισμένων στους PE Nodes (Routers) ανά VPN
  - Διαδικασία Ασφαλούς Επικοινωνίας **IPsec Tunnels** μεταξύ PE's BGP/IP Provider Network(s)
  - Generic Routing Encapsulation **GRE Tunnels** μεταξύ PE's BGP/IP Provider Network(s)
  - Διαδικασία Ασφαλούς Επικοινωνίας **OpenVPN Tunnels** μεταξύ τερματικών συσκευών χρηστών client - server, hosted σε διαφορετικά διαχειριστικά περιβάλλοντα μέσω SSL/TLS (προτιμάται η χρήση πρωτοκόλλων UDP και η προ-εγκατάσταση certificates στον client)

ΕΙΔΗ VPNs & Tunneling Protocols (2/2)

ETHERNET VPN (EVPN) - Virtual eXtensible LAN (VXLAN): Layer 2 Overlays over IP Substrates



Hardware and software VTEPs are shown above.



Επέκταση από VLAN σε **VXLAN** – Virtual eXtensible LAN για **Layer 2** υπερκείμενη (**overlay**) διασύνδεση τοπικών υποδικτύων **Ethernet** και **Data Centers** σε λογικά (virtual) LANs πάνω από **IP/UDP** υποκείμενα (**substrate**) tunnels μεταξύ **VTEPs** (VXLAN Tunnel Endpoints)

- VLAN ID: 12 bits (< 4096 VLANs)
- **VXLAN ID: 24bits/VTEP**

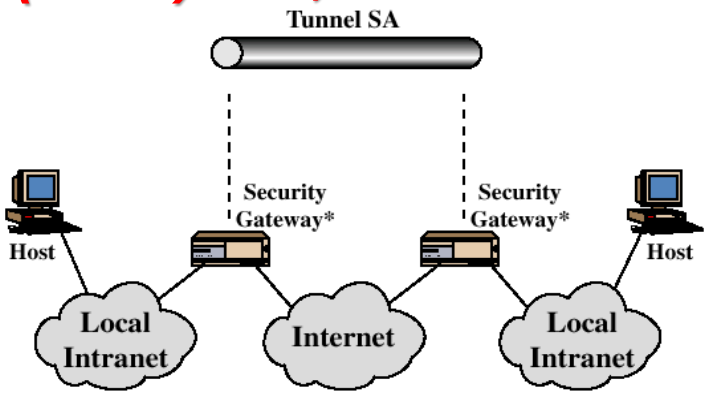
Σηματοδοσία μέσω επέκτασης του πρωτοκόλλου **BGP** για **MAC/IP address announcements** μεταξύ διασυνδεόμενων με IP tunnels υποδικτύων **Layer 2/3** και κατανεμημένων **Data Centers**

https://www.juniper.net/us/en/research-topics/what-is-vxlan.html

IPsec

ECE 454/CS 594, *Jinyuan (Stella) Sun*, Univ. of Tennessee, Fall 2011

IPsec: Ανεξάρτητο Εφαρμογών
ενώ
TLS: για Web
SSH: για Remote Login



Transport Mode

Ασφάλεια Περιεχομένου σε υποσύνολα της σύνδεσης e2e (*encryption του payload*)

IP header (real dest)	IPsec header	TCP/UDP header + data

Tunnel Mode

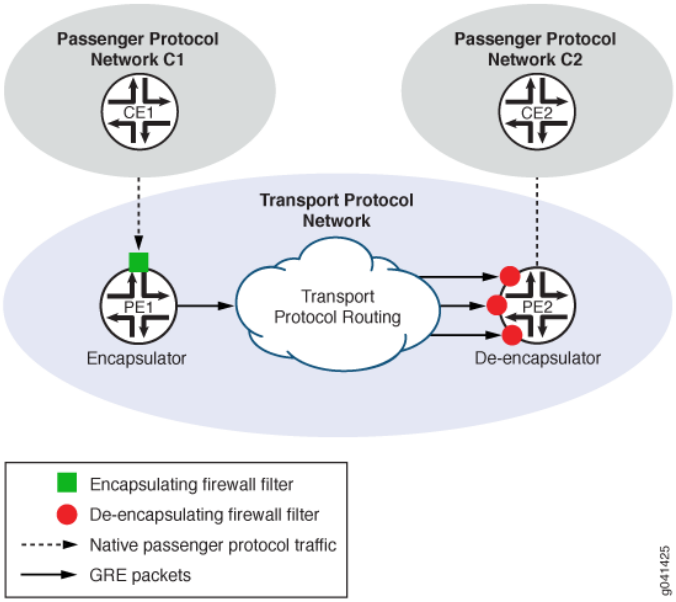
Ασφάλεια Πακέτου σε tunnel μεταξύ Security Gateways (*encryption αρχικού πακέτου*)

IP header (gateway)	IPsec header	IP header (real dest)	TCP/UDP header + data

- **SA**: Security Associations (one way)
  - SPI: Security Parameter Index (Cryptographic algorithms, keys, lifetimes, sequence numbers, mode - transport or tunnel)
  - Εναλλακτικές SA, αποθηκευμένες σε IPsec nodes, ενεργοποιούνται με επιλογή του πακέτου
- **AH**: Authentication Header
  - Επιβεβαίωση ταυτότητας αποστολέα (Sender Authentication) & μη παραποίησης μηνύματος (Message Integrity)
- **ESP**: Encapsulating Security Payload
  - Εμπιστευτικότητα (Confidentiality)
- **IKE**: Internet Key Exchange
  - Handshaking protocol για συμφωνία SA

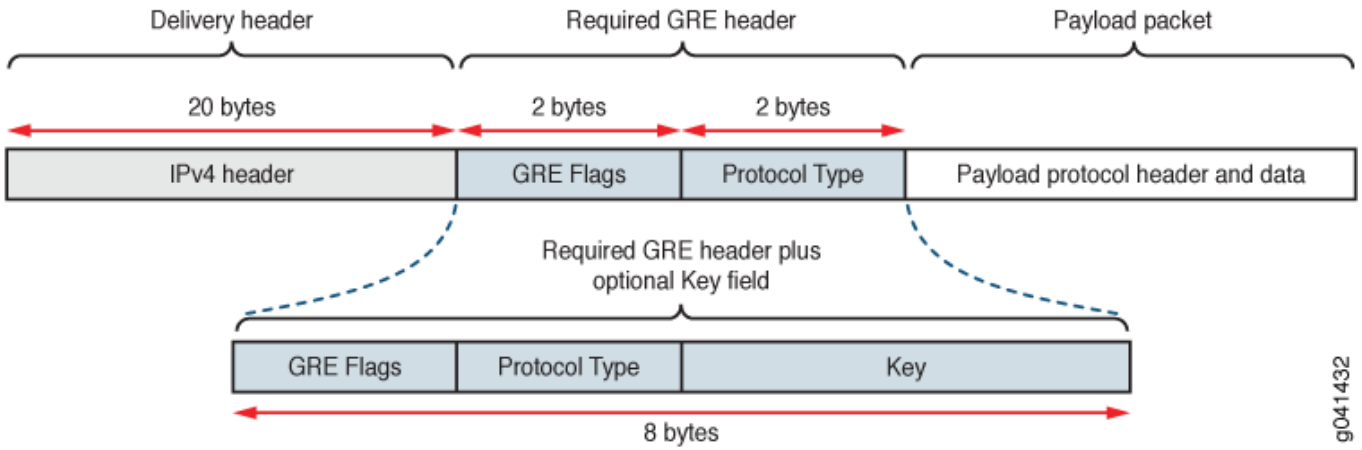
Generic Routing Encapsulation (GRE)

http://www.juniper.net/documentation/en_US/junos13.2/topics/concept/firewall-filter-tunneling-ipv4-gre-components.html



ΔΙΑΔΙΑΚΑΣΙΑ ΕΝΘΥΛΑΚΩΣΗΣ - GRE Tunneling

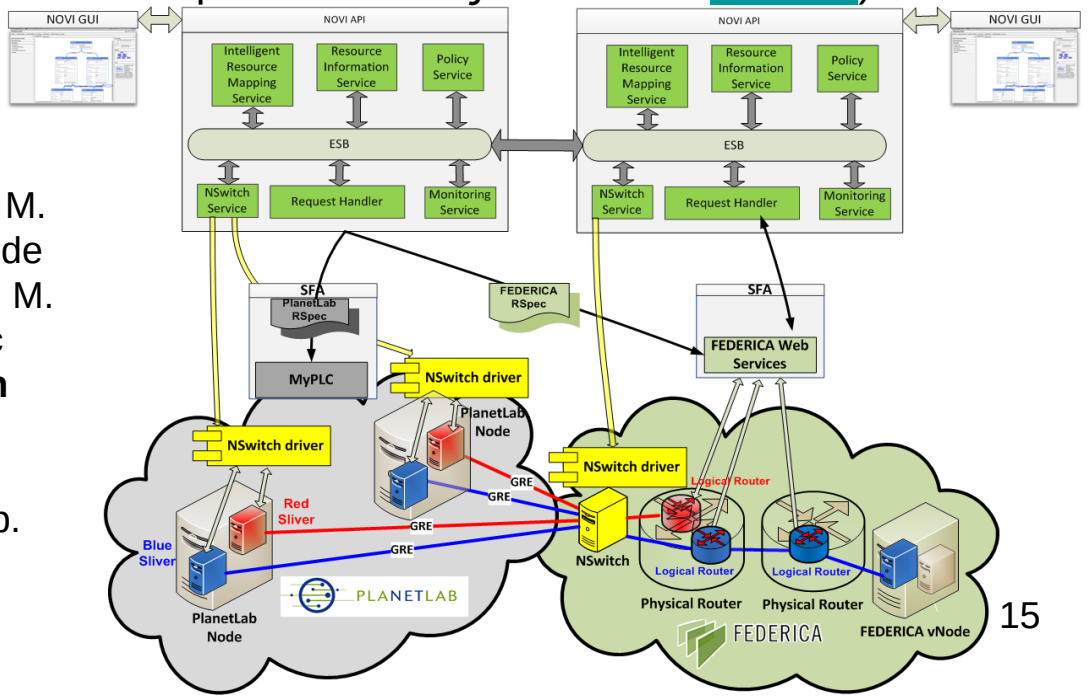
- Το payload packet πρέπει να μεταφερθεί από Customer (εφαρμογή) **C1** σε απομακρυσμένο Customer **C2** όπως σε απευθείας μονοκατευθυντική σύνδεση μεταξύ τοπικών κόμβων ζεύξης **CE1** (Customer Edge 1) και **CE2** (Customer Edge 2)
- Το Encapsulation filter στον διαδικτυακό κόμβο εισόδου **PE1** (Provider Edge 1) εισάγει GRE header με μοναδικό κλειδί για πακέτα **C1 → C2** (δεν ισχύει για C2 → C1)
- Το αποτέλεσμα ενθυλακώνεται με IPv4 header και προωθείται σαν IP datagram από τον Encapsulator **PE1** στον De-encapsulator **PE2** μέσω TCP/IP WAN (Internet)
- Το De-encapsulation filter στον διαδικτυακό κόμβο εξόδου **PE2** (Provider Edge 2) ανακτά το payload packet και το προωθεί στον **C2**



VPNs ΣΕ ΟΜΟΣΠΟΝΔΙΑ ΔΙΑΧΕΙΡΙΣΤΙΚΩΝ ΠΕΡΙΟΧΩΝ

Κοινοτικό Έργο NOVI (Networking innovations Over Virtualized Infrastructures)

- Συνύπαρξη σε διασυνδεόμενα δίκτυα πολλαπλών VPNs μέσω απομονωμένων εικονικών υποδομών με ασφαλή πρόσβαση τελικών χρηστών
- Οι εξουσιοδοτημένοι χρήστες δημιουργούν εικονικές φέτες - **slices** από «αφιερωμένα» στοιχεία - **slivers**: Virtual Machines (VMs), Virtual (Logical) Routers, Ethernet switches…
- Μη κρυπτογραφημένες συνδέσεις WAN: **GRE over IP tunnels** στο Internet & **layer 2 VLANs**
- Πειραματική υλοποίηση: Δημιουργία & λειτουργία απομονωμένων virtual slices με VM's στις εικονικές πειραματικές υποδομές ***PlanetLab*** (πάνω από το Internet) και ***FEDERICA*** (με Ethernet/VLANs των Ευρωπαϊκών ΑΕΙ & Ερευνητικών Κέντρων, των Εθνικών Ερευνητικών - Ακαδημαϊκών Δικτύων **NRENs** και του Πανευρωπαϊκού τους Διαδικτύου **GÉANT**)



Κύρια Αναφορά:

V. Maglaris, C. Papagianni, G. Androulidakis, M. Grammatikou, P. Grosso, J. van der Ham, C. de Laat, B. Pietrzak, B. Belter, J. Steger, S. Laki, M. Campanella & S. Sallent, **"Toward a Holistic Federated Future Internet Experimentation Environment: The Experience of NOVI Research & Experimentation"**, *IEEE Communications Magazine*, Vol. 53, No. 7, pp. 136-147, July 2015