

ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - NETWORK MANAGEMENT

Εικονικά Ιδιωτικά Δίκτυα & Πρωτόκολλα Tunneling
Virtual Private Networks (VPNs), Tunneling Protocols

Διαμόρφωση Virtual Private Networks (VPNs) & Tunneling
Virtual eXtended LANs (VXLANs), IPsec & GRE

B. Μάγκλαρης
maglaris@netmode.ntua.gr
www.netmode.ntua.gr

Νέα Κτίρια ΣΗΜΜΥ - Αίθουσα 013

27/10/2025

ΔΡΟΜΟΛΟΓΗΣΗ ΕΠΙΠΕΔΟΥ 2

ΣΕ ΔΙΚΤΥΑ ΠΑΡΟΧΩΝ (επανάληψη)

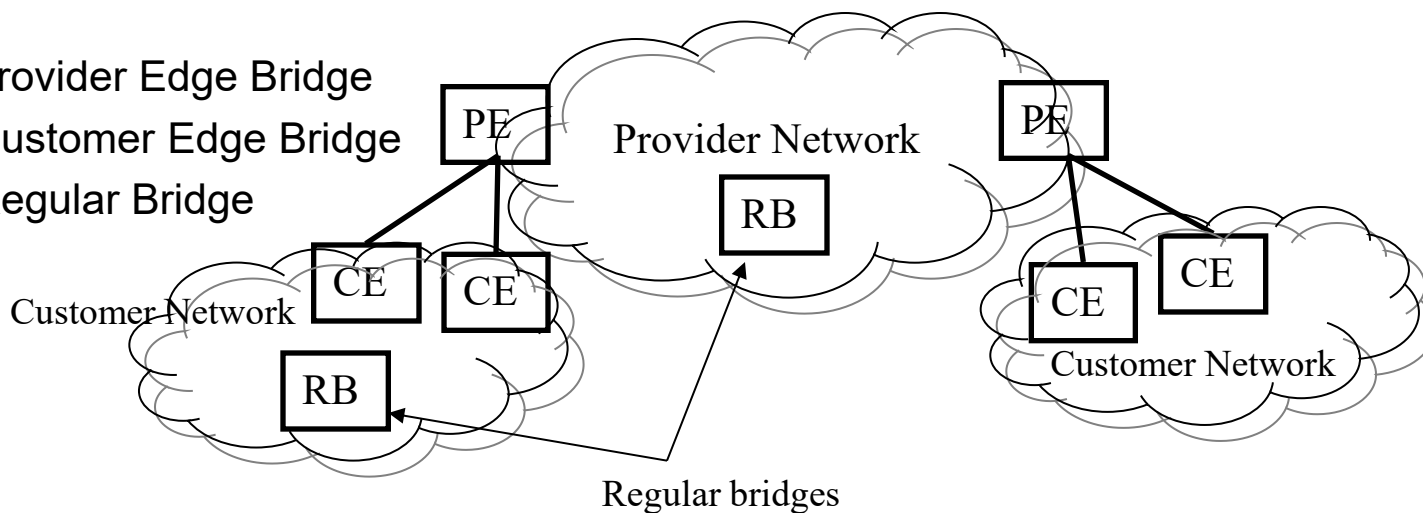
Provider Backbone Bridges – PBB

(mac-in-mac, IEEE 802.1ah)



CE: Customer Edge Bridge

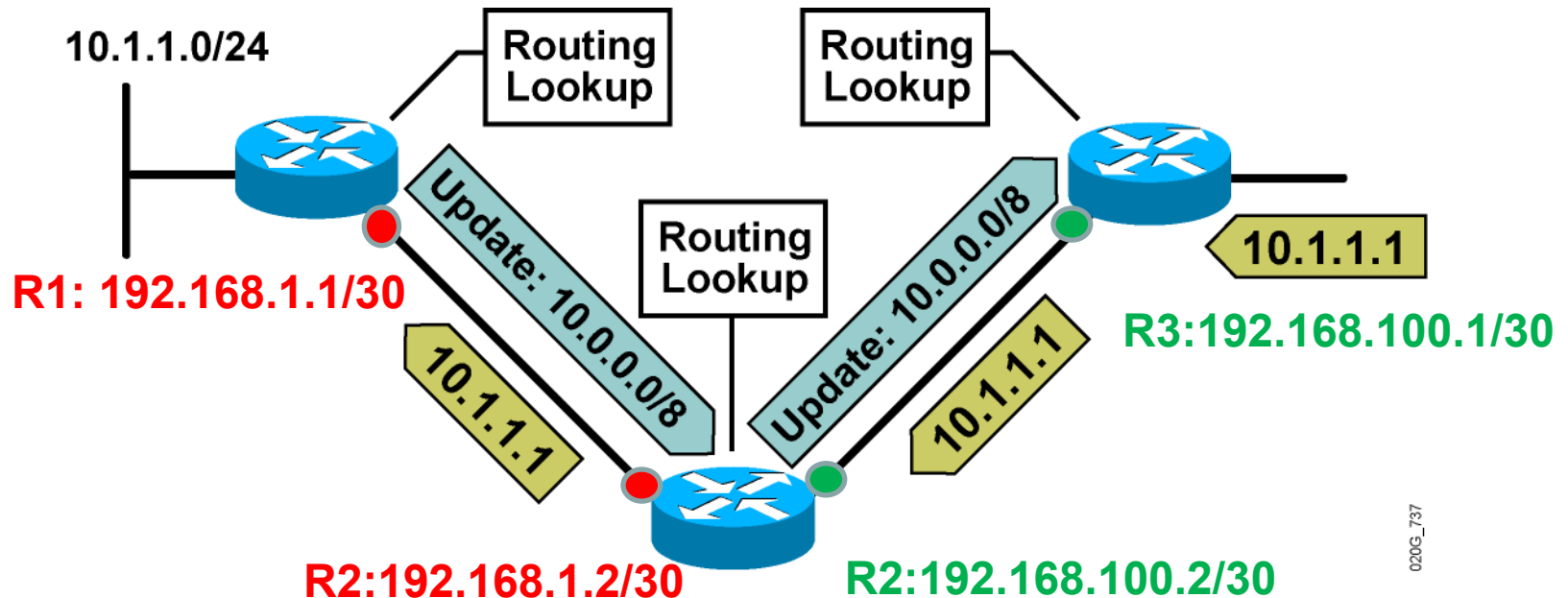
RB: Regular Bridge



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 (επανάληψη)



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

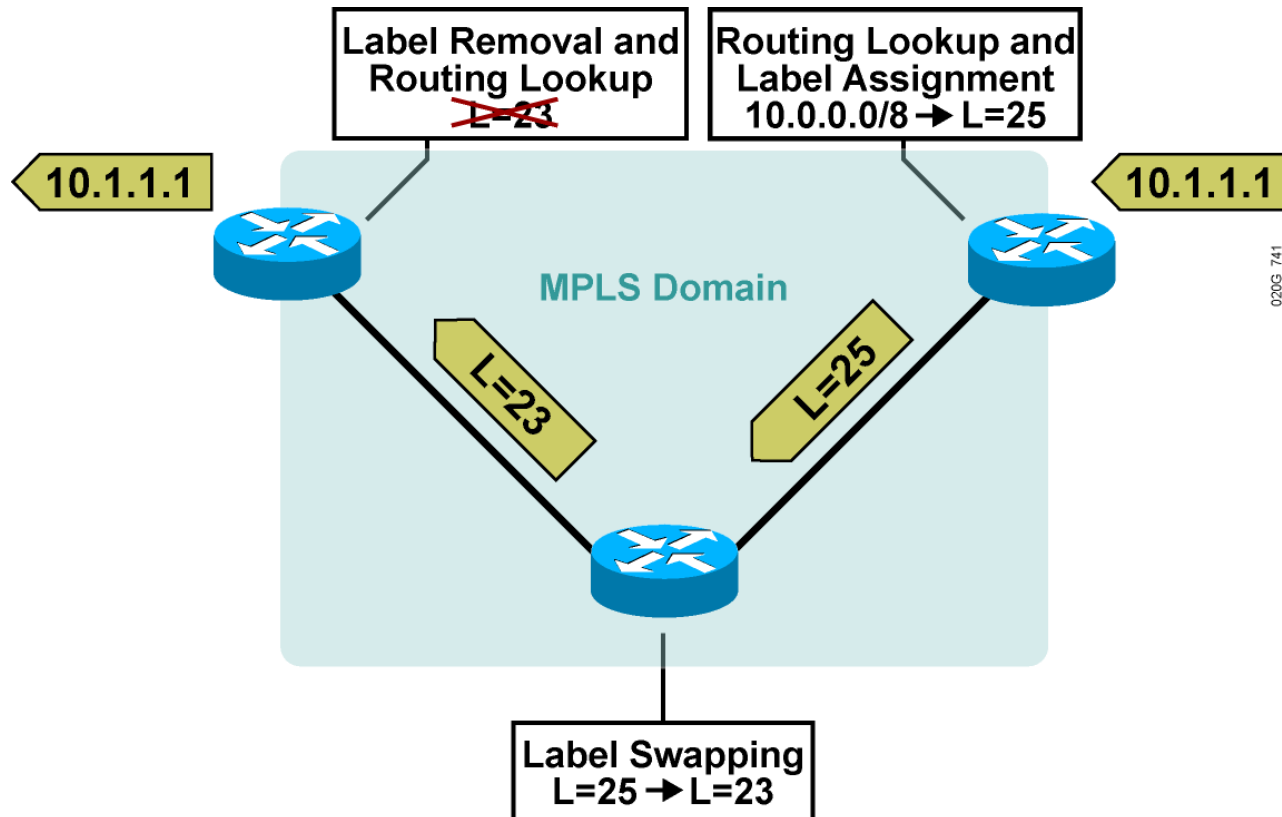
ΠΙΝΑΚΑΣ ΔΡΟΜΟΛΟΓΗΣΗΣ Router 2 (R2)

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:

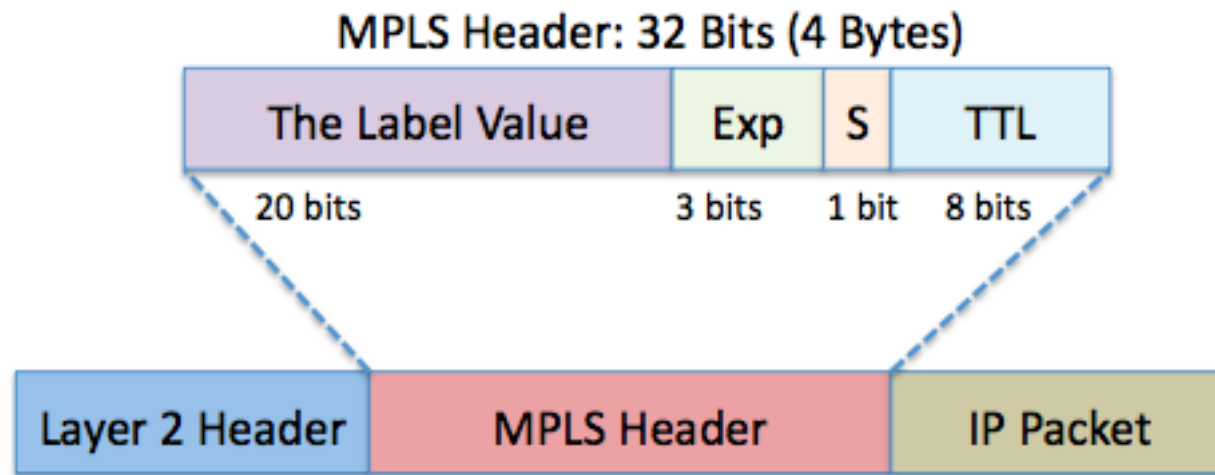
MPLS (Multi-Protocol Label Switching) (επανάληψη)



MPLS core routers : Label Switch Router – LSR
Αντικαθιστούν (swap) Labels
Πρωθούν 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 (επανάληψη)



Label : 20 bits (~ 1 million flows, 0 to 15 reserved for special use) assigned to **source & destination IP (flows)**, **traffic engineering option**

Exp : Experimental Use

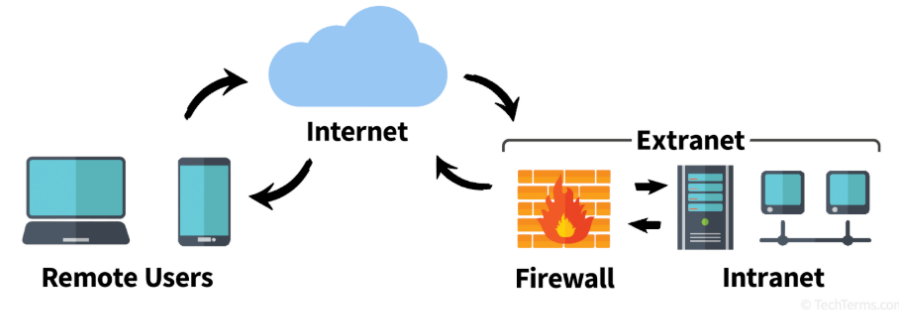
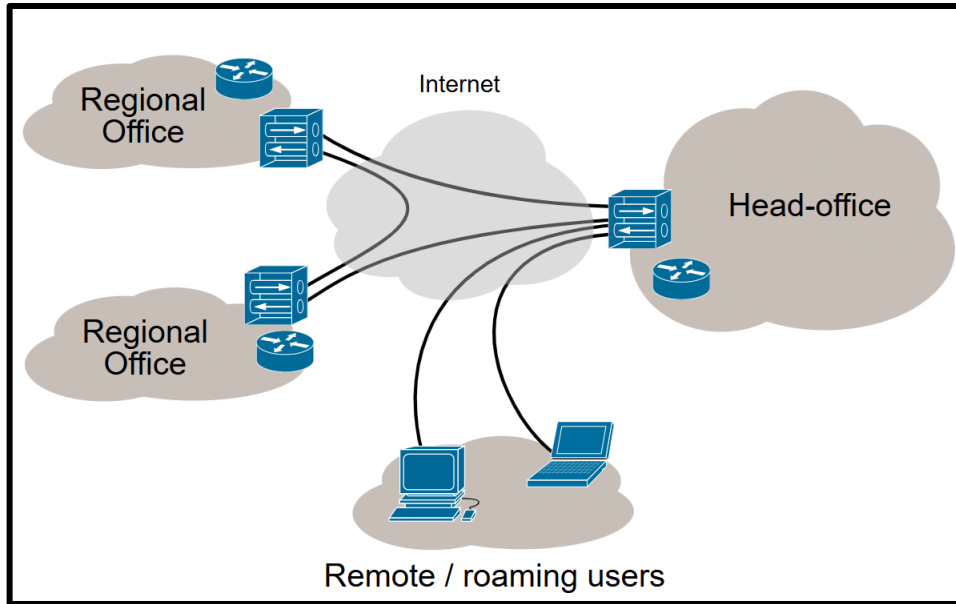
S : Bottom of Stack (set to 1 for the last entry in the label)

TTL : Time To Live

ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ

Virtual Private Networks - VPNs

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



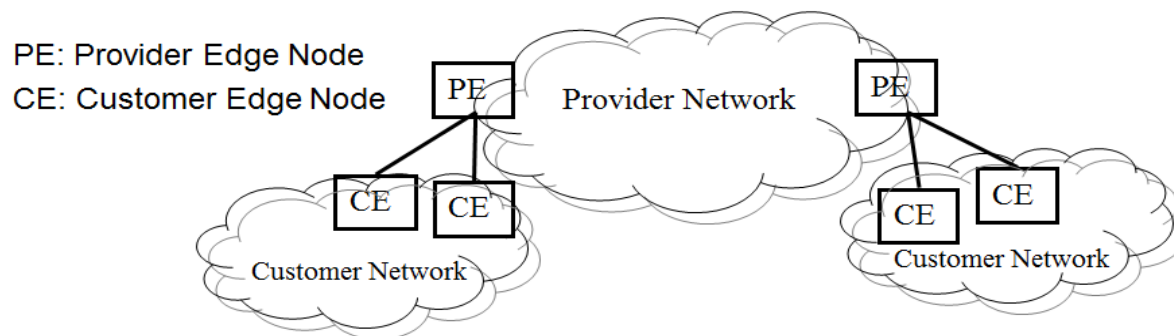
Extranets provide access to an intranet to remote users, protected by firewalls and other protection methods

<https://techterms.com/definition/extranet>

Με τα **VPNs** χρήστες κοινών κατακευκμένων 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) **IP/MPLS** ενός **ISP** ή **Enterprise Local Area Networks - LANs & Data Centers** σε εξουσιοδοτημένους χρήστες 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:
 - ο Επέκταση πεδίου διευθύνσεων **VLAN tags** ή **IP** σε απομακρυσμένες νησίδες ενός VPN
 - ο Δρομολόγηση με περιορισμούς ασφαλείας και διαμοιρασμού φορτίου – **traffic engineering**
 - ο Ασφαλής μετάδοση και σηματοδότηση όπως σε αυστηρά ελεγχόμενο τοπικό δίκτυο (LAN)

ΔΙΑΜΟΡΦΩΣΗ VPNs & Tunneling Protocols (1/2)



Layer 2 VPN (L2VPN): Επέκταση L2/VLAN over Provider WAN π.χ.

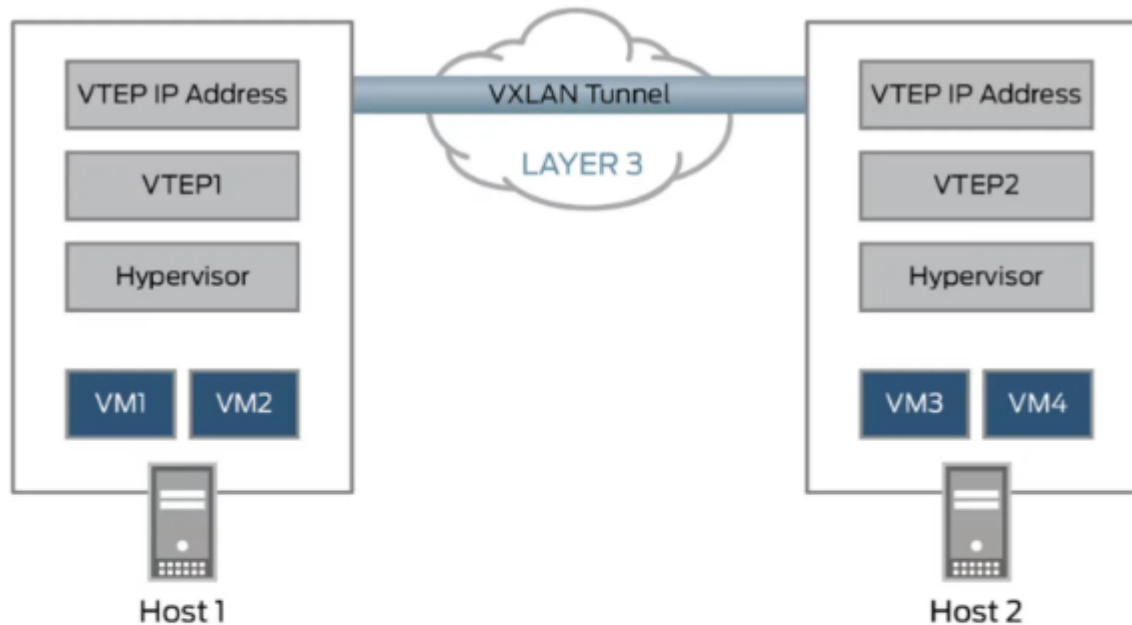
- Point-to-point **L2TP** (Layer 2 Tunneling Protocol) πάνω από IP/MPLS Provider Network
- Point-to-point Επεκτάσεις **PW** (Pseudo-Wire) πάνω από IP/MPLS Provider Network
- Multipoint **VPLS** (Virtual Private LAN Service) πάνω από MPLS Provider Network
- Επέκταση **Mac-in-Mac** (IEEE 802.1ah) πάνω 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) 7

ΕΙΔΗ VPNs & Tunneling Protocols (2/2)

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



In the figure above, when VTEP1 receives an Ethernet frame from Virtual Machine 1 (VM1) addressed to Virtual Machine 3 (VM3), it uses the VNI and the destination MAC to look up in its forwarding table for the VTEP to send the packet to. VTEP1 adds a VXLAN header that contains the VNI to the Ethernet frame, encapsulates the frame in a Layer 3 UDP packet, and routes the packet to VTEP2 over the Layer 3 network. VTEP2 decapsulates the original Ethernet frame and forwards it to VM3. VM1 and VM3 are completely unaware of the VXLAN tunnel and the Layer 3 network between them.

- ❖ Επέκταση από VLAN σε **VXLAN** (Virtual eXtensible LAN) για **Layer 2** υπερκείμενη (**overlay**) διασύνδεση τοπικών υποδικτύων (**subnets**) **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)
 - **VXLAN ID: 24bits/VTEP**
- ❖ Τα Layer 2 subnets ταυτοποιούνται από κωδικό **VNI** (VXLAN Network Identifier)
- ❖ Η σηματοδότηση πραγματοποιείται μέσω επέκτασης του πρωτοκόλλου **BGP** για **MAC/IP address announcements** μεταξύ διασυνδεόμενων (με IP UDP tunnels) υποδικτύων **Layer 2/3** και κατανομημένων **Data Centers**

IPsec

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

IPsec: Ανεξάρτητο Εφαρμογών
ενώ

TLS: για συνδέσεις Web

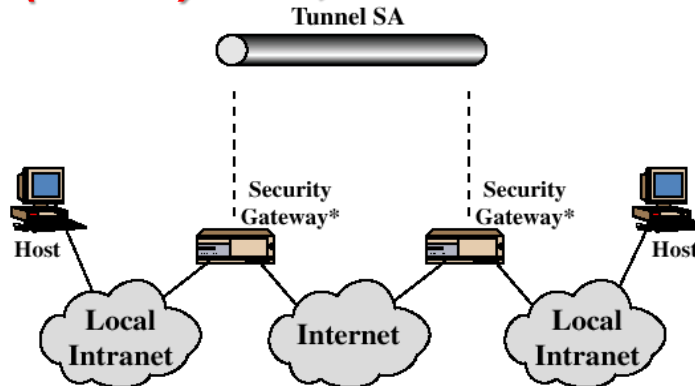
SSH: για Remote Login

Transport Mode

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

Tunnel Mode

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

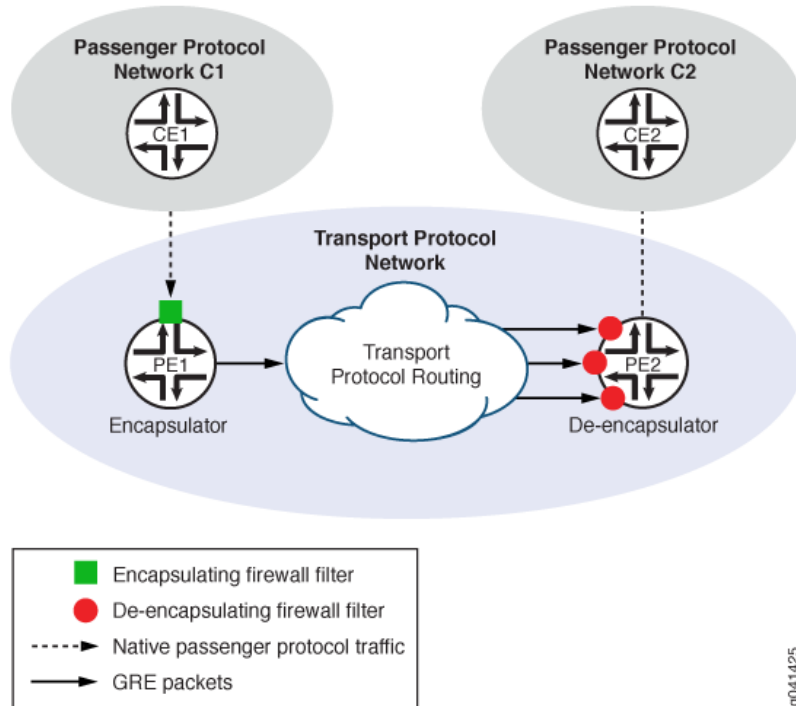


IP header (real dest)	IPsec header	TCP/UDP header + data	
IP header (gateway)	IPsec header	IP header (real dest)	TCP/UDP header + data

- **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

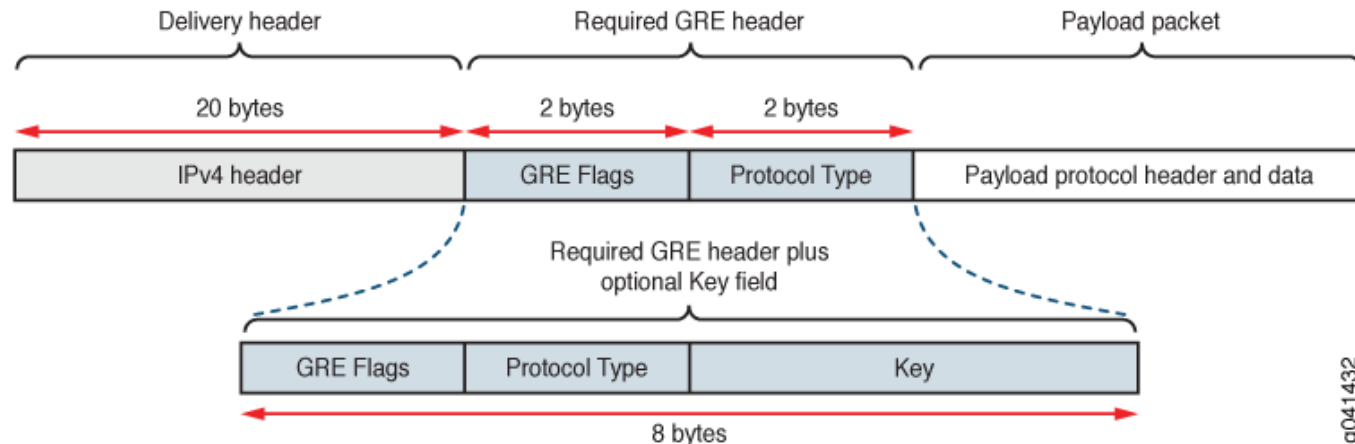
Generic Routing Encapsulation (GRE)

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



ΔΙΑΔΙΑΚΑΣΙΑ ΕΝΘΥΛΑΚΩΣΗΣ - GRE Tunneling

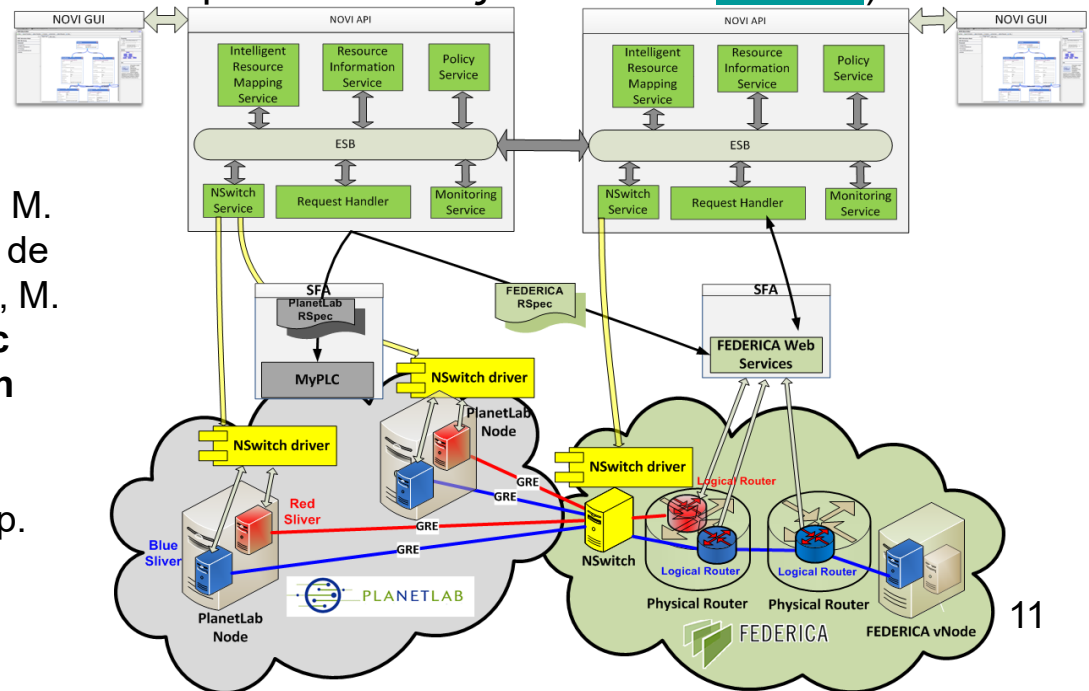
- Το payload packet πρέπει να μεταφερθεί από Customer (εφαρμογή) **C1** σε απομακρυσμένο Customer **C2** όπως σε απευθείας μονοκατευθυντική σύνδεση μεταξύ τοπικών κόμβων ζεύξης **CE1** (Customer Edge 1) και **CE2** (Customer Edge 2)
- Το Encapsulation filter στον διαδικτυακό κόμβο εισόδου **PE1** (Provider 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 διασυνδεδεμένα 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