



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

ΑΝΟΙΚΤΑ ακαδημαϊκά
μαθήματα ΠΠ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

Ενότητα #6: MPLS Τεχνολογία

Καθηγητής Χρήστος Ι. Μπούρας

Τμήμα Μηχανικών Η/Υ & Πληροφορικής, Πανεπιστήμιο
Πατρών

email: bouras@cti.gr, site: <http://ru6.cti.gr/ru6/bouras>

Σκοποί ενότητας

- Εξοικείωση με την τεχνολογία MPLS



Περιεχόμενα ενότητας

- Τεχνολογία
- Πλεονεκτήματα
- Αρχές λειτουργίας
- Traffic Engineering
- Εξελιγμένα χαρακτηριστικά
- Virtual Private Networks
- GMPLS



MPLS Τεχνολογία

MPLS Τεχνολογία

- Αρχικά προτάθηκε σαν ένα μέσο για τη βελτίωση της ταχύτητας προώθησης και της απόδοσης των IP δρομολογητών
- Ενοποιεί τη λειτουργικότητα των επιπέδων IP και σύνδεσης δεδομένων
- Ανήκει μόνο στους δρομολογητές
- Προσφέρει Λειτουργικότητα, Κλιμάκωση, Εξέλιξη, Ολοκλήρωση



MPLS Πλεονεκτήματα (1/2)

- Υποστήριξη πολλών πρωτοκόλλων
- Ανεξαρτησία επιπέδου διασύνδεσης δεδομένων
- Αυξημένη απόδοση
- Ρητή δρομολόγηση
- Traffic engineering
- Διαχωρισμός των λειτουργιών ελέγχου και προώθησης



MPLS Πλεονεκτήματα (2/2)

- Έλεγχος κυκλοφορίας
- Συνάθροιση ροών
- Επεκτασιμότητα της δρομολόγησης του επιπέδου δικτύου
- Υποστήριξη πολλαπλών τύπων κυκλοφορίας
- Υποστήριξη QoS

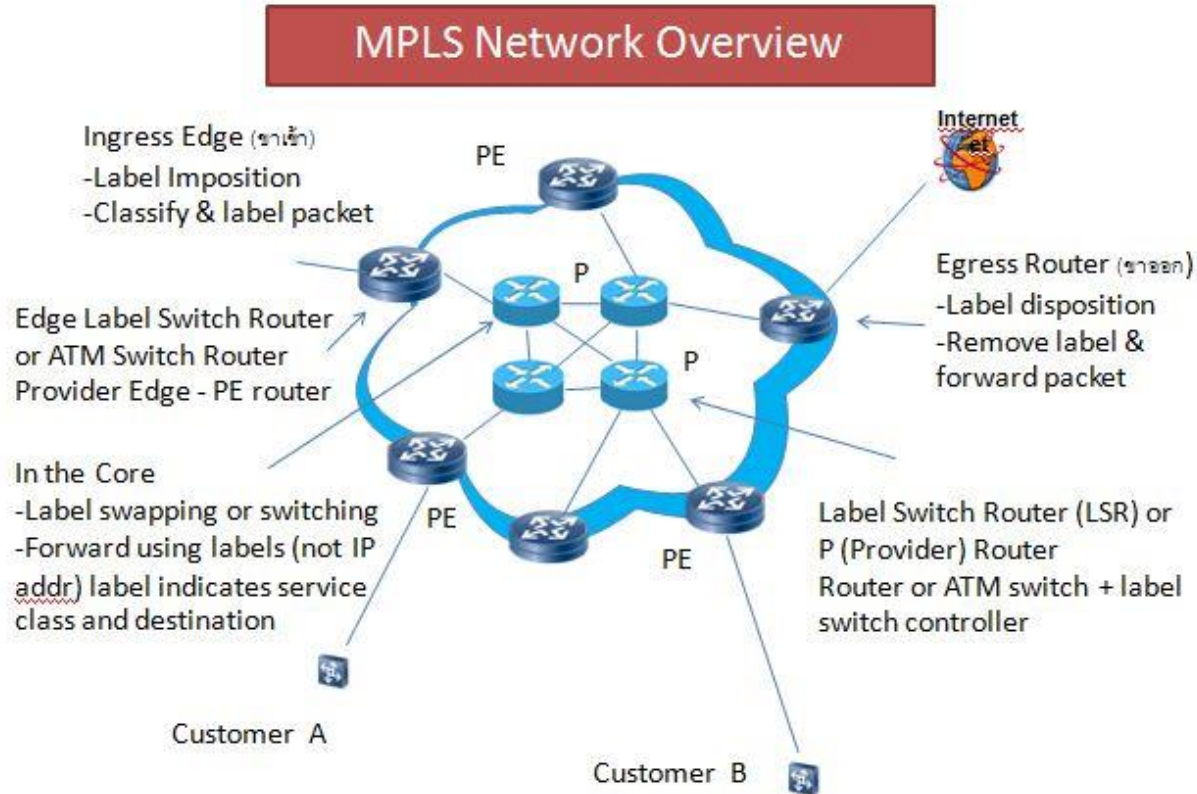


Αρχές

- Το MPLS χρησιμοποιεί προώθηση που βασίζεται σε ετικέτες
- Στο σημείο εισόδου, τα εισερχόμενα πακέτα επεξεργάζονται και εφαρμόζονται σε αυτά ετικέτες
- Το δίκτυο κορμού εφαρμόζει τις κατάλληλες υπηρεσίες και προωθεί τα πακέτα βάση της ετικέτας
- Η αναλυτική επεξεργασία, η κατηγοριοποίηση και το 'φιλτράρισμα' γίνονται μόνο μια φορά, στο σημείο εισόδου
- Στο σημείο εξόδου, οι ετικέτες αφαιρούνται και τα πακέτα προωθούνται στον τελικό προορισμό τους



Διάγραμμα MPLS δικτύου



Διάγραμμα MPLS δικτύου

(πηγή:

https://commons.wikimedia.org/wiki/File:MPLS_Network_Overview.JPG)



Ορολογία (1/2)

- Label Switch Router, (LSR):
 - Πραγματοποιεί τη μεταγωγή των πακέτων
- Label edge router, (LER):
 - Πραγματοποιεί την αρχική επεξεργασία και κατηγοριοποίηση του πακέτου, και εφαρμόζει την πρώτη ετικέτα
- Forwarding Equivalence Class, FEC :
 - Ένα σύνολο IP πακέτων που προωθούνται με τον ίδιο τρόπο
- MPLS Label:
 - Μία label (ετικέτα) είναι μια μικρή, σταθερού μήκους επικεφαλίδα που χρησιμοποιείται για την προώθηση των πακέτων
- Label Switched Path, LSP:
 - Το μονοπάτι που καθορίζεται από όλες τις ετικέτες



Ορολογία (2/2)

- Ingress/Egress LER:
 - Ο LER που αρχίζει/τερματίζει ένα LSP
- Label Switched Hop:
 - Το hop μεταξύ δύο MPLS κόμβων
- Label Distribution Protocol:
 - Αναθέτει ετικέτες με στόχο την εγκατάσταση των LSPs
- Label Information Base – LIB
 - Η βάση των πληροφοριών σχετικά με τις ετικέτες



Αρχές λειτουργίας (1/2)

- Η επιλογή του δρομολογητή μπορεί να θεωρηθεί σαν τη σύνθεση δύο λειτουργιών
 - Η πρώτη λειτουργία χωρίζει τα πακέτα σε ένα σύνολο από FECs
 - Η δεύτερη λειτουργία αντιστοιχεί σε κάθε FEC έναν επόμενο δρομολογητή
- Όλα τα πακέτα που ανήκουν στην ίδια FEC και ταξιδεύουν από ένα συγκεκριμένο κόμβο θα ακολουθήσουν το ίδιο μονοπάτι
- Η FEC κωδικοποιείται στην MPLS ετικέτα. Όταν ένα πακέτο προωθείται στον επόμενο δρομολογητή, η ετικέτα αποστέλλεται μαζί με αυτό
- Στη διαδρομή του πακέτου δεν πραγματοποιείται περαιτέρω ανάλυση της επικεφαλίδας του



Αρχές λειτουργίας (2/2)

- Η ετικέτα χρησιμοποιείται σαν ένας δείκτης σε ένα πίνακα που καθορίζει το επόμενο βήμα και μια νέα ετικέτα
- Η παλιά ετικέτα αντικαθίσταται από την καινούρια, και το πακέτο προωθείται στο επόμενο βήμα
- Έτσι, όλη η προώθηση οδηγείται από τις ετικέτες
- Ορισμένοι δρομολογητές αναλύουν την επικεφαλίδα του επιπέδου δικτύου του πακέτου και για να καθορίσουν την προτεραιότητά του ή την κλάση υπηρεσίας
- Το MPLS επιτρέπει (αλλά δεν απαιτεί) η προτεραιότητα και η κλάση υπηρεσίας να εξάγονται πλήρως ή μερικώς από την ετικέτα



Ετικέτες και αντιστοίχιση ετικετών

- Κάθε πακέτο αντιστοιχίζεται σε μια FEC και του ανατίθεται ετικέτα με βάση κάποιο γεγονός ή πολιτική (μοντέλο δεδομένων ή ελέγχου)
- Η απόφαση της ανάθεσης ετικέτας μπορεί να βασίζεται σε κριτήρια προώθησης όπως:
 - Unicast δρομολόγηση με βάση τον περιορισμό
 - Έλεγχος κυκλοφορίας
 - Multicast
 - QoS



MPLS ετικέτες

MPLS Label Structure



EXP=Class of Service(CoS) 3 bits
S=Bottom of stack
TTL=Time to live

Δομή MPLS ετικέτας

(πηγή:

https://commons.wikimedia.org/wiki/File:MPLS_Label_Structure.JPG)



Μεταγωγή Ετικέτας (1/2)

- Η Μεταγωγή Ετικέτας (Label Switching) είναι ένας εξελιγμένος τρόπος προώθησης πακέτων που αντικαθιστά την προώθηση που βασίζεται στην αντιστοίχιση των διευθύνσεων
- Παρουσιάζει ένα πλήθος πλεονεκτημάτων σχετικά με τη συνηθισμένη δρομολόγηση:
 - Η MPLS προώθηση μπορεί να γίνει και από switches που δεν μπορούν να αναλύσουν τις επικεφαλίδες δικτυακού επιπέδου
 - Ο δρομολογητής εισόδου καθώς αποφασίζει την ανάθεση, μπορεί να χρησιμοποιήσει οποιαδήποτε πληροφορία που διαθέτει σχετικά με το πακέτο



Μεταγωγή Ετικέτας (2/2)

- Ένα πακέτο που εισέρχεται στο δίκτυο μέσω ενός συγκεκριμένου δρομολογητή μπορεί να λάβει διαφορετική ετικέτα από αυτή που θα έπαιρνε αν έμπαινε στο δίκτυο από κάποιο διαφορετικό δρομολογητή
- Οι διαδικασίες που καθορίζουν τον τρόπο που ένα πακέτο ανατίθεται σε μια FEC μπορεί να γίνονται όλο και πιο πολύπλοκες χωρίς να επηρεάζουν τους δρομολογητές
- Οι αποφάσεις δρομολόγησης παραδοσιακά βασίζονται στη διεύθυνση, ενώ στο MPLS μπορεί να βασίζονται σε οποιοδήποτε πλήθος παραμέτρων, όπως ποιότητα υπηρεσίας, συμμετοχή σε VPN, κ.ά.
- Η διαδρομή του πακέτου επιλέγεται σαφώς πριν ή ακριβώς τη στιγμή που το πακέτο εισέρχεται στο δίκτυο

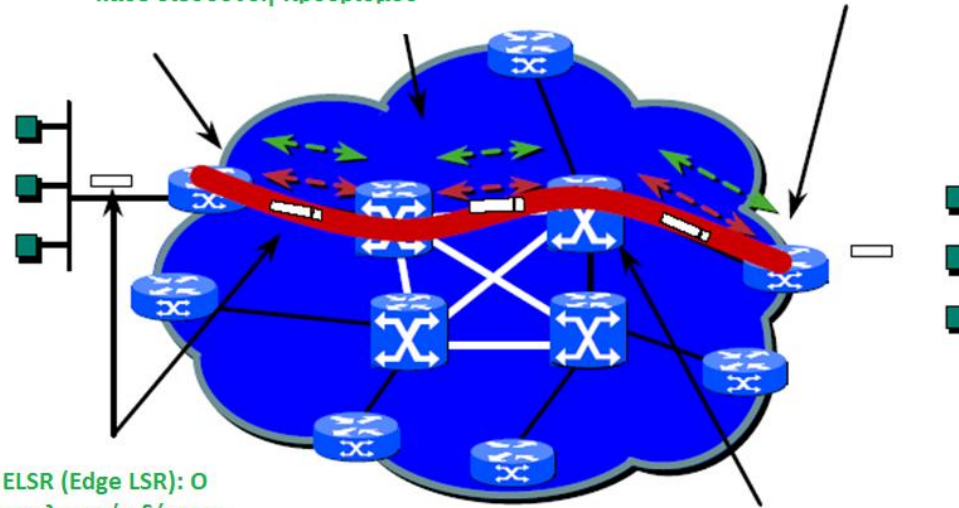


MPLS switching

1α. Το πρωτόκολλο δρομολόγησης (OSPF, IGRP,...) υπολογίζει το μικρότερο μονοπάτι προς τον προορισμό μέσα από το δίκτυο

1β. Το LDP (Label Distribution Protocol) δένει μια ετικέτα σε κάθε διεύθυνση προορισμού

4. Ο τελευταίος MPLS switch διαγράφει την ετικέτα



2. ELSR (Edge LSR): Ο δρομολογητής δέχεται πακέτα, τρέχει συνηθισμένες L3 υπηρεσίες και στη συνέχεια προσθέτει ετικέτες

3. LSR: μεταγάγει πακέτα βάσει της ετικέτας

MPLS switching

Στοιχείο Προώθησης Μεταγωγής Ετικέτας

- Το MPLS παρέχει τις ακόλουθες επιλογές προώθησης
 - Δρομολόγηση Βήμα-προς-Βήμα:
 - Κάθε LSR επιλέγει ανεξάρτητα το επόμενο βήμα για μια δεδομένη κλάση ισοδύναμης προώθησης (FEC)
 - Ρητή δρομολόγηση:
 - Ο LSR εισόδου ορίζει τη λίστα των κόμβων δια των οποίων διέρχεται το μονοπάτι ρητής δρομολόγησης
 - Κατά μήκος του μονοπατιού, δεσμεύονται οι πόροι έτσι ώστε να εξασφαλιστεί η ποιότητα της υπηρεσίας



Στοιχείο Ελέγχου Μεταγωγής Ετικέτας

- Είναι υπεύθυνο για
 - τη διανομή των πληροφοριών δρομολόγησης μεταξύ των LSRs
 - την εκτέλεση των διαδικασιών που χρησιμοποιούνται για να μετατρέψουν τις πληροφορίες σε πίνακα προώθησης
- Περιλαμβάνει όλα τα συμβατικά πρωτόκολλα δρομολόγησης (π.χ. OSPF, BGP) που παρέχουν στους LSRs την αντιστοίχιση μεταξύ της FEC και των διευθύνσεων των επόμενων βημάτων
- Επιπλέον, ο LSR πρέπει να:
 - Δημιουργεί τις αντιστοιχίσεις μεταξύ ετικετών και FECs
 - Διανέμει τις αντιστοιχίες αυτές στους άλλους LSRs
 - Κατασκευάζει το δικό του πίνακα προώθησης



Διανομή Πληροφορίας Ετικετών

- Μια καταχώρηση του πίνακα προώθησης έχει πληροφορίες για:
 - Το εξερχόμενο interface
 - Μία καινούργια ετικέτα
 - Λοιπές πληροφορίες (π.χ. εξερχόμενη πολιτική αναμονής)
- Οι καταχωρήσεις πραγματοποιούνται ως εξής:
 - Το επόμενο βήμα παρέχεται από τα πρωτόκολλα δρομολόγησης
 - Η εισερχόμενη και η εξερχόμενη ετικέτα παρέχονται από μια τοπική και απομακρυσμένη αντιστοίχιση ανάμεσα σε μια FEC και στην ετικέτα
- Πολλά πρωτόκολλα έχουν επεκταθεί / δημιουργηθεί με σκοπό να υποστηρίζουν ανταλλαγή ετικετών (BGP, RSVP, LDP)



Edge LSR

- Διαδραματίζει έναν από τους σημαντικότερους ρόλους
 - Κατηγοριοποιεί την κυκλοφορία και τοποθετεί / αφαιρεί τις ετικέτες
 - Καθορίζει αν η κυκλοφορία είναι μια ροή μεγάλης διάρκειας
 - Υλοποιεί πολιτικές διαχείρισης και ελέγχους πρόσβασης
 - Συναθροίζει την κυκλοφορία σε μεγαλύτερες ροές
- Δυνατότητες νέας γενιάς edge LSR:
 - Wire speed δυνατότητες κατηγοριοποίησης των IP ροών
 - Εκτεταμένες VPN δυνατότητες



Tunnels

- Το MPLS μπορεί να ελέγχει ολόκληρο το μονοπάτι ενός πακέτου χωρίς να καθορίζει ρητώς τους ενδιάμεσους δρομολογητές
- Από τη στιγμή που έχει πραγματοποιηθεί ανταλλαγή των ετικετών μεταξύ των LSRs που υποστηρίζουν ένα LSP, οι ενδιάμεσοι LSRs που ανήκουν στο LSP δε χρειάζεται να εξετάζουν το περιεχόμενο των πακέτων δεδομένων που περνούν από το LSP
- Για αυτό το λόγο, τα LSPs συχνά θεωρείται ότι σχηματίζουν tunnels κατά μήκος ολόκληρου ή ενός τμήματος του MPLS δικτύου κορμού



Tunnels και Labels stacks

- Ένα tunnel μεταφέρει αδιαφανή δεδομένα μεταξύ του LSR εισόδου του tunnel και του LSR εξόδου του tunnel
- Αυτό σημαίνει ότι ολόκληρο το ωφέλιμο φορτίο, συμπεριλαμβανομένων των IP επικεφαλίδων, μπορεί να αποκρύπτεται με ασφάλεια χωρίς να επιβαρύνει την ικανότητα του δικτύου να προωθεί δεδομένα
- Επιπλέον το tunneling επιτρέπει τη διανομή ετικετών για πολλαπλά FECs και εγκατάσταση πολλαπλών LSPs
- Η ανάθεση πολλαπλών ετικετών καλείται Label Stacking και επιτρέπει καλύτερη κατηγοριοποίηση της κυκλοφορίας μεταξύ των κόμβων εισόδου και εξόδου



Label Information Base – LIB

- LIB είναι η βάση των πληροφοριών σχετικά με τις ετικέτες
- Κάθε LSR κατασκευάζει έναν πίνακα για να καθορίσει πώς θα πρέπει να προωθηθεί κάποιο πακέτο
 - Αποθηκεύει όλες τις ετικέτες που έχουν διαφημιστεί από άλλους LSRs στο MPLS δίκτυο
- LFIB (cache)
 - Χρησιμοποιείται από τη διεργασία προώθησης πακέτων
 - Είναι ανάλογο του IP forwarding table
 - Περιέχει incoming και outgoing label, FEC, next hop
- LFIB = συνδυασμός LIB και IP routing table

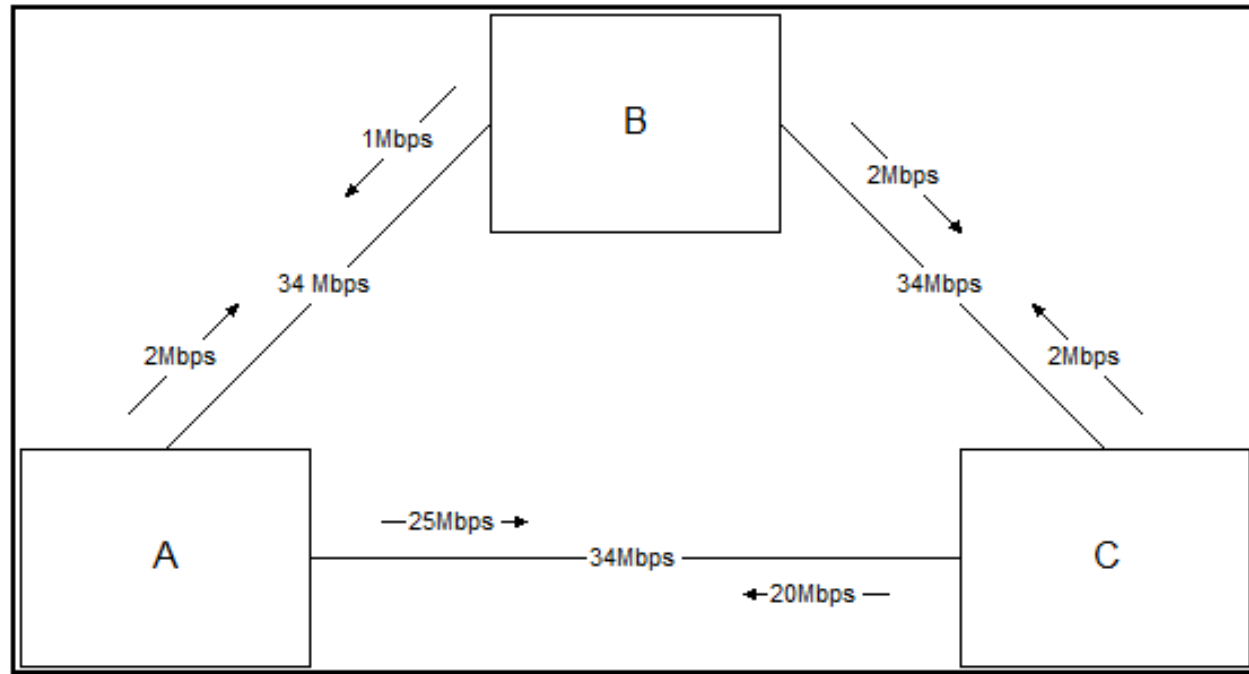


Traffic Engineering

- Στα περισσότερα δίκτυα η κίνηση είναι ανομοιόμορφη
- Traffic engineering είναι η διαδικασία καταμερισμού της κίνησης μέσα στο δίκτυο, ώστε να ικανοποιηθούν οι απαιτήσεις των εφαρμογών
- Στόχο έχει να δρομολογηθεί η κίνηση πάνω από τις κατάλληλες συνδέσεις με τέτοιο τρόπο ώστε να αποφευχθεί η συμφόρηση και να μην υπάρχει άμεση ανάγκη για εφαρμογή άλλων σχημάτων QoS
- Ουσιαστικά βελτιστοποιεί την απόδοση μέσω της αντιστοίχισης των ροών κυκλοφορίας στην τοπολογία του δικτύου



Δίκτυο με ανομοιόμορφη κίνηση



Δίκτυο με ανομοιόμορφη κίνηση πάνω στα links

MPLS – Traffic Engineering (1/2)

- Η αντιστοίχιση των ροών κυκλοφορίας επιτυγχάνει την εξισορρόπηση του φορτίου στους συνδέσμους, δρομολογητές και switches
- Η διαδικασία αποτελείται από το σχεδιασμό του δικτύου (επιλογή των μονοπατιών) και τη βελτιστοποίηση
- Δύο κατηγορίες δρομολόγησης της κυκλοφορίας:
 - ρητή δρομολόγηση: το μονοπάτι έχει προεπιλεγεί και μπορεί να γίνει και δέσμευση πόρων
 - έμμεση δρομολόγηση: επιλέγεται μονοπάτι που ικανοποιεί τις απαιτήσεις προώθησης των ροών και δεσμεύονται οι πόροι



MPLS – Traffic Engineering (2/2)

- Προϋπόθεση: πρέπει στη διαδικασία της επιλογής του μονοπατιού:
 - να γνωρίζει η πηγή τα πλήρη χαρακτηριστικά του δικτύου
 - να γίνεται διανομή των στοιχείων του δικτύου και
 - να υπάρχει δυνατότητα δέσμευσης των πόρων
- Οι πιο γνωστοί και διαδεδομένοι μηχανισμοί σηματοδότησης για την διανομή των ετικετών είναι:
 - CR-LDP
 - RSVP-TE



Traffic Engineering - Πλεονεκτήματα

- Δρομολόγηση των κυρίων μονοπατιών
- Παροχή ακριβούς ελέγχου
- Αποδοτικότερη χρησιμοποίηση του εύρους ζώνης
- Ελαχιστοποίηση της απώλειας πακέτων, των παρατεταμένων περιόδων συμφόρησης και μεγιστοποίηση του throughput
- Παροχή περισσότερων επιλογών, χαμηλότερου κόστους και καλύτερης υπηρεσίας στους πελάτες



Resource Reservation Protocol (RSVP)

- Το RSVP είναι ένα πρωτόκολλο επιπέδου μεταφοράς για την δημιουργία μονοπατιών και δέσμευση πόρων
- Επιτρέπει σε τεχνολογίες που δεν παρέχουν εγγενώς QoS, να μπορούν να ζητούν συγκεκριμένους πόρους από το δίκτυο και να τους χρησιμοποιούν κατά τη διάρκεια μίας σύνδεσης
- Πρέπει όλοι οι κόμβοι που παρεμβάλλονται από το ένα άκρο μέχρι το άλλο να υποστηρίζουν το πρωτόκολλο



RSVP με Traffic Engineering Extensions (1/2)

- Η RSVP σηματοδοσία λαμβάνει χώρα μεταξύ δρομολογητών (traffic trunk), ενώ το επεκταμένο RSVP εφαρμόζεται σε μια συλλογή ροών που μοιράζονται ένα κοινό μονοπάτι και ένα κοινό σύνολο δικτυακών πόρων
 - Επιτυγχάνεται διανομή των MPLS ετικετών
 - Μειώνεται το πλήθος των μηνυμάτων ανανέωσης και οι σχετικές απαιτήσεις για επεξεργασία
 - Το μονοπάτι δεν περιορίζεται από την τυπική δρομολόγηση που βασίζεται στον προορισμό



RSVP με Traffic Engineering Extensions (2/2)

- Το RSVP δέχτηκε ειδικότερες επεκτάσεις για την υποστήριξη LSP Tunnels:
 - Downstream-on-demand διανομή ετικέτας
 - Αρχικοποίηση ρητών LSPs
 - Κατανομή των δικτυακών πόρων στα ρητά LSPs
 - Επαναδρομολόγηση των εγκατεστημένων LSP tunnels
 - Ανίχνευση της πραγματικής διαδρομής που ακολουθεί ένα LSP tunnel
 - Εισαγωγή της έννοιας των abstract κόμβων



Constraint Routing- Label Distribution Protocol (CR-LDP) (1/2)

- Είναι μια μέθοδος για εγκατάσταση των LSPs από-σημείο-σε-σημείο
- Επιτρέπει τον ορισμό ρητών διαδρομών, που ουσιαστικά λαμβάνεται η ακολουθία των κόμβων ως είσοδος από αυτό, χρησιμοποιώντας αυστηρά και abstract hops
- Ένας abstract κόμβος είναι ένα σύνολο κόμβων που η εσωτερική τοπολογία είναι αδιαφανής στον κόμβο εισόδου των LSPs
- Ένας abstract κόμβος θεωρείται απλός αν περιέχει μόνο ένα φυσικό κόμβο
- Παρέχει απλοποίηση του δικτύου, αξιοπιστία, κλιμάκωση, διαλειτουργικότητα



Constraint Routing- Label Distribution Protocol (CR-LDP) (2/2)

- Το CR-LDP ουσιαστικά είναι ένα σύνολο επεκτάσεων στο LDP. Οι επεκτάσεις είναι πλήρως καθορισμένες και αφορούν τα ακόλουθα θέματα:
 - Παράμετροι QoS και κυκλοφορίας
 - Επανα-βελτιστοποίηση μονοπατιού
 - Γνωστοποίηση αποτυχίας εγκατάστασης LSP
 - Ανάκαμψη από αποτυχία κάποιου μονοπατιού
 - Ανίχνευση βρόχων
 - Multi-protocol υποστήριξη



Advanced MPLS features

- Υποστήριξη multicast λειτουργίας στο MPLS
 - Multicast δένδρο
- Υποστήριξη IPv6 over MPLS
 - Για την υποστήριξη IPv6 σε περιπτώσεις όπου δεν υποστηρίζεται από όλο το δίκτυο (6PE)



Λειτουργία Multicast

- Αρχικά το MPLS δε σχεδιάστηκε να υποστηρίζει multicast
- Έχει προταθεί η εισερχόμενη ετικέτα να αντιστοιχίζεται σε ένα σύνολο από εξερχόμενες ετικέτες
- Αυτό μπορεί να κατασκευαστεί μέσω ενός multicast δένδρου
- Η εισερχόμενη ετικέτα αντιστοιχίζεται στο multicast δένδρο και χρησιμοποιείται ένα σύνολο από θύρες εξόδου για να μεταδοθεί το πακέτο
- Το HSMP (hub & spoke multipoint) LSP επιτρέπει την κυκλοφορία από τη ρίζα στα φύλλα του δέντρου μέσω point-to-multipoint (P2MP) LSP και από τα φύλλα στη ρίζα κατά μήκος της αντίστροφης διαδρομής



6PE λειτουργία

- Μέθοδος για την παροχή IPv6 υπηρεσιών σε δίκτυα που δεν υποστηρίζεται
- Στηρίζεται στην ιδέα της ενεργοποίησης του IPv6 πρωτοκόλλου μόνο στους Provider Edge (PE) δρομολογητές (6PEs δρομολογητές)
- Με τον τρόπο αυτό οι 6PEs δρομολογητές γίνονται διπλής στοίβας (Dual Stacked) και χρησιμοποιούν το IPv6 για να επικοινωνήσουν με τους ακραίους δρομολογητές ενώ η διασύνδεση τους με το υπόλοιπο MPLS δίκτυο γίνεται μόνο με την IPv4 στοίβα
- Το υπόλοιπο δίκτυο (MPLS Core) δεν "γνωρίζει" τίποτα σχετικά με το IPv6



MPLS - Εφαρμογές

- Το MPLS μπορεί να χρησιμοποιηθεί ώστε να παρέχει:
 - ποιότητα υπηρεσίας (QoS)
 - δυνατότητα εφαρμογής traffic engineering
 - πιο εύκολη και αποδοτική μεταφορά IP κυκλοφορίας πάνω από ATM υποδομή
 - μια αποδοτική λύση στο πρόβλημα της ασφάλειας των προσωπικών δεδομένων καθώς και υποστήριξη της χρήσης μη μοναδικών, ιδιωτικών IP διευθύνσεων στο εσωτερικό ενός VPN
 - ιδεατά κυκλώματα ή tunnels κατά μήκος ενός IP δικτύου



Virtual Private Networks

- Τα κλασικά ιδιωτικά δίκτυα βασίζονται σε μισθωμένες γραμμές με σημαντικό κόστος και δύσκολη και απαιτητική διαχείριση
- Τα ιδεατά ιδιωτικά δίκτυα (Virtual Private Networks - VPN) είναι ένας τύπος ιδιωτικών δικτύων που χρησιμοποιούν δημόσιες διασυνδέσεις, όπως το Internet, αντί για αφιερωμένες γραμμές (leased lines)
 - Έγιναν δημοφιλή καθώς οι εργαζόμενοι άρχισαν να εργάζονται από απομακρυσμένες τοποθεσίες
- Λύνουν τα προβλήματα κόστους αφού χρησιμοποιείται η δημόσια υποδομή και παράλληλα προσφέρουν την ασφάλεια και την αξιοπιστία των μισθωμένων γραμμών



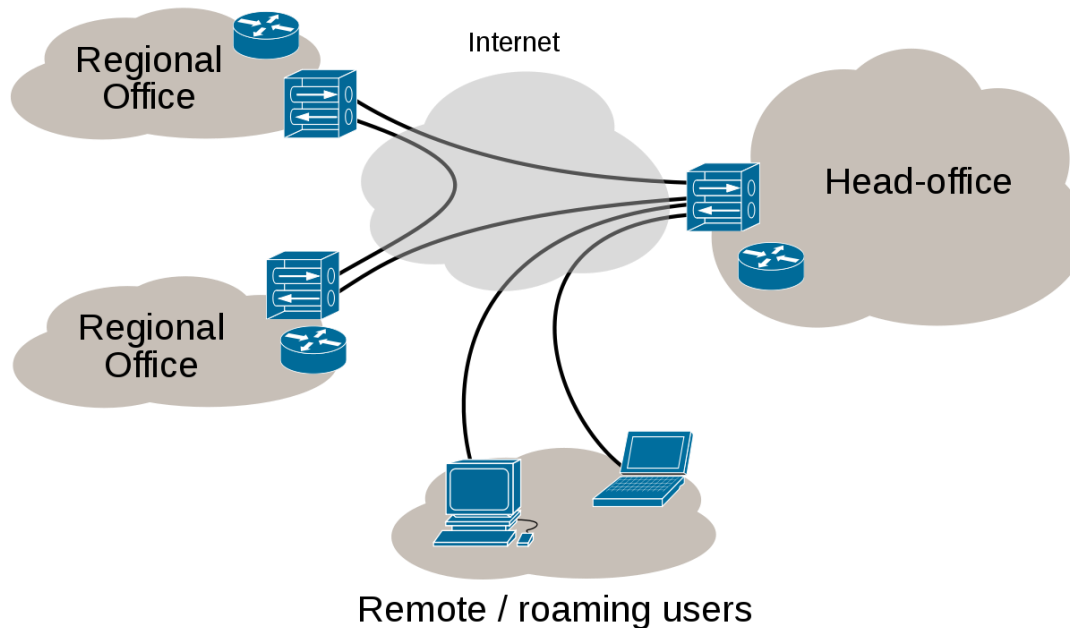
Είδη VPNs

- Βασισμένα σε IP tunnels
 - Η προς μετάδοση πληροφορία διαμορφώνεται σε IP πακέτα
 - Έχουν χαμηλό κόστος και χαρακτηρίζονται από ευκολία στις συνδέσεις εκτός δικτύου
 - Μειονέκτημα: απαιτούνται επιπλέον τεχνικές κρυπτογράφησης
- Βασισμένα σε ISDN, Frame relay ή ATM
 - χρησιμοποιούν τις υπηρεσίες των δημόσιων δικτύων μεταγωγής και επιπλέον ISDN B κανάλια, ή SVCs ή PVCs για να διαχωρίζουν την κυκλοφορία
 - Μπορούν να χρησιμοποιηθούν για οποιονδήποτε τύπο επικοινωνίας
 - Μειονέκτημα: οι ISDN, Frame Relay και ATM υπηρεσίες είναι ακριβές και λιγότερο διαδεδομένες από τις IP-based υπηρεσίες



Virtual Private Networks

Internet VPN



Virtual Private Networks

(πηγή:

https://en.wikipedia.org/wiki/Virtual_private_network#/media/File:Virtual_Private_Network_overview.svg)



Κατηγοριοποίηση βάση διασύνδεσης

- Intranet
 - Διασύνδεση ανάμεσα στις τοποθεσίες μιας εταιρίας όπου επιτρέπεται το ιδιωτικό δίκτυο να επεκτείνεται πάνω σε ένα δημόσιο δίκτυο με ασφάλεια
- Απομακρυσμένη πρόσβαση
 - Απομακρυσμένοι χρήστες μπορούν και συνδέονται με τη χρήση ενός tunnel κρυπτογράφησης δεδομένων
 - Το tunnel δημιουργείται από το χρήστη με το κατάλληλο λογισμικό ή από το κεντρικό δίκτυο της εταιρίας
- Διασύνδεση μεταξύ διαφορετικών εταιριών
 - Παρόμοιο με το intranet με τη διαφορά ότι η πρόσβαση επιτρέπεται και σε άτομα άλλης εταιρίας



MPLS VPNs

- Η MPLS τεχνολογία παρέχει τη δυνατότητα δημιουργίας ιδεατών ιδιωτικών δικτύων (MPLS VPNs)
- Τα ιδιωτικά αυτά δίκτυα μπορούν να υλοποιηθούν:
 - σε επίπεδο 3 (L3 MPLS VPN) ή
 - σε επίπεδο 2 (L2 MPLS VPN)



Δρομολογητές

- Τα MPLS VPNs καθορίζουν τρεις ρόλους για τους δρομολογητές:
 - CE (customer edge): συνδέονται με τις τοποθεσίες του πελάτη και συνήθως τους διαχειρίζεται αυτός
 - PE (provider edge): χρησιμεύουν σαν τα σημεία εισόδου και εξόδου για το VPN και τους διαχειρίζεται ο πάροχος. Διαμοιράζονται τις πληροφορίες δρομολόγησης και ενημερώνουν τους πίνακες δρομολόγησης
 - P (provider): απαρτίζουν το δίκτυο κορμού του παρόχου και ασχολούνται με την προώθηση της VPN κυκλοφορίας που έχει τοποθετηθεί σε MPLS πλαίσια από τους CE και PE δρομολογητές. Τους διαχειρίζεται ο πάροχος



Απαιτήσεις Ασφάλειας

- Ορισμένες απαιτήσεις-κλειδιά που θα πρέπει να ικανοποιούνται είναι οι ακόλουθες:
 - Είναι απαραίτητο να υπάρχει διαχωρισμός διευθυνσιοδότησης και δρομολόγησης
 - Η εσωτερική δομή του δικτύου κορμού πρέπει να παραμένει κρυφή
 - Όπως το Frame Relay ή το ATM δίκτυο κορμού είναι κρυμμένο, έτσι θα πρέπει να είναι και ένα MPLS VPN δίκτυο κορμού
 - Το δίκτυο πρέπει να μπορεί να αντιστέκεται σε επιθέσεις που οφείλονται είτε στην άρνηση υπηρεσίας (Denial of Service – DoS) ή σε οποιαδήποτε εισβολή



Λειτουργία L3 MPLS VPN (1/2)

- Ο πάροχος αναθέτει σε κάθε VPN ένα μοναδικό αναγνωριστή που καλείται αναγνωριστής διαδρομής (Route Distinguisher – RD) και είναι διαφορετικός για κάθε Intranet και Extranet εντός του δικτύου
- Οι πίνακες προώθησης περιέχουν μοναδικές διευθύνσεις για κάθε τελικό σημείο στο δίκτυο, οι οποίες καλούνται VPN-IP διευθύνσεις
- Κάθε VPN συσχετίζεται με ένα ή περισσότερα VPN στιγμιότυπα δρομολόγησης/προώθησης (VRFs) που καθορίζουν τη VPN συμμετοχή της τοποθεσίας ενός πελάτη που συνδέεται σε έναν PE δρομολογητή



Λειτουργία L3 MPLS VPN (2/2)

- Ένα VRF αποτελείται από έναν πίνακα IP δρομολόγησης, έναν πίνακα προώθησης, ένα σύνολο από interfaces που χρησιμοποιούν τον πίνακα προώθησης και από ένα σύνολο κανόνων και παραμέτρων δικτυακών πρωτοκόλλων
- Οι πίνακες αποτρέπουν την προώθηση των πληροφοριών έξω από το VPN και την προώθηση πακέτων που βρίσκονται έξω από ένα VPN προς ένα δρομολογητή εντός του VPN
- Βάση των πληροφοριών στους πίνακες IP δρομολόγησης και προώθησης, τα πακέτα προωθούνται στον προορισμό τους χρησιμοποιώντας MPLS
- Γίνεται χρήση των LSPs για προώθηση δεδομένων ανάμεσα στους ακραίους δρομολογητές που καθορίζουν τα όρια σε ένα VPN

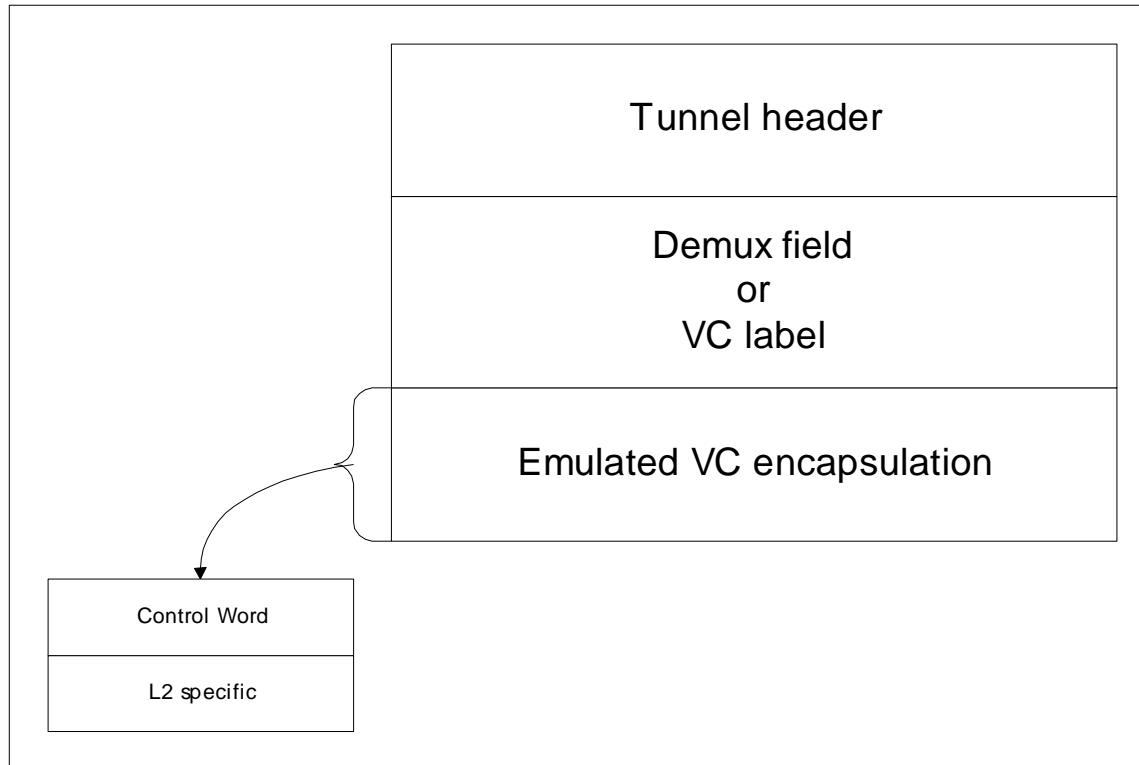


L2 MPLS VPNs

- Μετάδοση πλαισίων του επιπέδου 2 (layer 2 frames) πάνω από MPLS
- Η υλοποίηση γίνεται στο επίπεδο 2 (data link) σαν να μην υπάρχει μετάδοση των πλαισίων πάνω από MPLS, αλλά σαν να υπήρχαν κανονικές συνδέσεις του επιπέδου 2
 - επιτρέπει τη διατήρηση και διαχείριση μίας κοινής υποδομής από τους παρόχους
- Βασίζεται στη δυνατότητα ενθυλάκωσης και μεταφοράς των PDUs, για διάφορα πρωτόκολλα του επιπέδου 2, πάνω από ένα MPLS δίκτυο



Ενθυλάκωση πλαισίων του επιπέδου 2



Ενθυλάκωση πλαισίων του επιπέδου 2

Πλεονεκτήματα

- Έμφυτη δυνατότητα κλιμάκωσης
- Διαχωρισμός διαχειριστικών αρμοδιοτήτων
- Μυστικότητα πληροφοριών δρομολόγησης
- Ευκολία ρύθμισης
- Ανεξαρτησία από το πρωτόκολλο του επιπέδου 3
- Μειωμένο overhead
- Ομοιογένεια στις διαφορετικές L2 τεχνολογίες
- Πραγματική end-to-end connectivity



Μειονεκτήματα

- Απαίτηση για κοινή τεχνολογία επιπέδου 2 σε κάθε VPN
- Πολυπλοκότητα δρομολόγησης για τους πελάτες
- Τα σχετικά προϊόντα δεν είναι ακόμα ώριμα
- Τα standards βρίσκονται σε εξέλιξη



Υποστήριξη από κατασκευαστές

- Επιπέδου 3 VPNs
 - Υποστηρίζονται ευρέως
- Επιπέδου 2 VPNs
 - Juniper
 - MPLS/CCC (MPLS Circuit Cross-Connect)
 - MPLS/TCC
 - Kompella drafts
 - Cisco
 - AToM
 - Ethernet over MPLS (EoMPLS)
 - Martini drafts



CCC τεχνολογία

- Τα κυκλώματα CCC εμπίπτουν σε δύο κατηγορίες οι οποίες περιλαμβάνουν DLCIs, VCs, VLAN IDs, PPP και διεπαφές Cisco HDLC, και LSPs
- Παρέχουν 3 τύπους cross-connect:
 - Layer 2 switching
 - MPLS tunneling
 - LSP stitching
- Για το Layer 2 switching και το MPLS tunneling, το cross-connect είναι αμφίδρομο. Για το LSP stitching, το cross - connect είναι μονής κατεύθυνσης



AToM τεχνολογία

- Η μετάδοση με τη χρήση του AToM ακολουθεί τα ακόλουθα βήματα:
 - Ένα εισερχόμενο πακέτο στην κάρτα της γραμμής εισόδου του PE δρομολογητή δέχεται επεξεργασία αφαιρώντας την Layer 2 επικεφαλίδα
 - Μια λέξη ελέγχου και η ετικέτα εικονικού κυκλώματος τοποθετούνται στην κορυφή του πακέτου
 - Επιλέγεται το Interface εξόδου
 - Ένα tunnel label προωθείται για φυσιολογική MPLS δρομολόγηση στο δίκτυο κορμού
- Η εξέλιξη της τεχνικής AToM περιλαμβάνει την υποστήριξη L2 MPLS VPNs μεταξύ Interfaces που χρησιμοποιούν διαφορετικές τεχνολογίες και τη διασύνδεση πολλαπλών κυκλωμάτων



GMPLS

- Το Generalized Multi-Protocol Label Switching (GMPLS) είναι μια σουίτα πρωτοκόλλου που επεκτείνει το MPLS
- Στόχος της δημιουργίας του GMPLS είναι η διαχείριση περαιτέρω διασυνδέσεων και τεχνολογιών μεταγωγής, όπως πολυπλεξία διαίρεσης χρόνου, μεταγωγή μήκους κύματος και μεταγωγή οπτικής ίνας



Generalized labels

- Το GMPLS βασίζεται στις generalized labels
- Αυτές είναι ετικέτες που μπορεί να αντιπροσωπεύουν είτε
 - μια οπτική ίνα σε μια δέσμη ινών,
 - μια ζώνη συχνοτήτων μέσα στην ίνα,
 - ένα μήκος κύματος μέσα σε μια ζώνη συχνοτήτων (ή ίνα), ή
 - ένα σύνολο χρονοθυρίδων μέσα σε ένα μήκος κύματος



Σύντομη ανασκόπηση

- Τεχνολογία
- Πλεονεκτήματα
- Αρχές λειτουργίας
- Traffic Engineering
- Εξελιγμένα χαρακτηριστικά
- Virtual Private Networks
- GMPLS



Βιβλιογραφία

- Σημειώσεις μαθήματος (Κεφάλαιο 6)
- Βιβλία:
 - Next-Generation Internet Architectures and Protocols, B. Ramamurthy, G. N. Rouskas, K. Sivalingam
 - Virtual Private Networks: Technologies and Solutions, R. Yuan, W. T. Strayer
- Links:
 - <http://ru6.cti.gr/ru6/bouras/undergraduate-courses/diktua-dhmosias-xrhshs-kai-diasundesh-diktuwn?language=el> (Δικτυακός τόπος μαθήματος)
 - <http://mirror.unpad.ac.id/orari/library/library-ref-eng/ref-eng-3/network/mpls/200001.pdf> (White Paper on MPLS)
 - <http://tools.ietf.org/html/rfc4364RFC> (RFC on BGP/MPLS IP VPNs)



Ερωτήσεις



Τέλος Ενότητας



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στο πλαίσιο του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αθηνών**» έχει χρηματοδοτήσει μόνο την αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.



Σημειώματα

Σημείωμα Ιστορικού Εκδόσεων Έργου

Το παρόν έργο αποτελεί την έκδοση **2.0**.



Σημείωμα Αναφοράς

Copyright Πανεπιστήμιο Πατρών, Χρήστος Μπούρας 2014. «Δίκτυα δημόσιας χρήσης και διασύνδεση δικτύων. MPLS Τεχνολογία». Έκδοση: 2.0. Πάτρα 2017. Διαθέσιμο από τη δικτυακή διεύθυνση:
<https://eclass.upatras.gr/courses/CEID1064/>



Σημείωμα Αδειοδότησης

Το παρόν υλικό διατίθεται με τους όρους της άδειας χρήσης Creative Commons Αναφορά, Μη Εμπορική Χρήση Παρόμοια Διανομή 4.0 [1] ή μεταγενέστερη, Διεθνής Έκδοση. Εξαιρούνται τα αυτοτελή έργα τρίτων π.χ. φωτογραφίες, διαγράμματα κ.λ.π., τα οποία εμπεριέχονται σε αυτό και τα οποία αναφέρονται μαζί με τους όρους χρήσης τους στο «Σημείωμα Χρήσης Έργων Τρίτων».



[1] <http://creativecommons.org/licenses/by-nc-sa/4.0/>

Ως **Μη Εμπορική** ορίζεται η χρήση:

- που δεν περιλαμβάνει άμεσο ή έμμεσο οικονομικό όφελος από την χρήση του έργου, για το διανομέα του έργου και αδειοδόχο
- που δεν περιλαμβάνει οικονομική συναλλαγή ως προϋπόθεση για τη χρήση ή πρόσβαση στο έργο
- που δεν προσπορίζει στο διανομέα του έργου και αδειοδόχο έμμεσο οικονομικό όφελος (π.χ. διαφημίσεις) από την προβολή του έργου σε διαδικτυακό τόπο

Ο δικαιούχος μπορεί να παρέχει στον αδειοδόχο ξεχωριστή άδεια να χρησιμοποιεί το έργο για εμπορική χρήση, εφόσον αυτό του ζητηθεί.