

Δίκτυα Υπολογιστών



*Το επίπεδο δικτύου
(network layer)*

Κ. Βασιλάκης

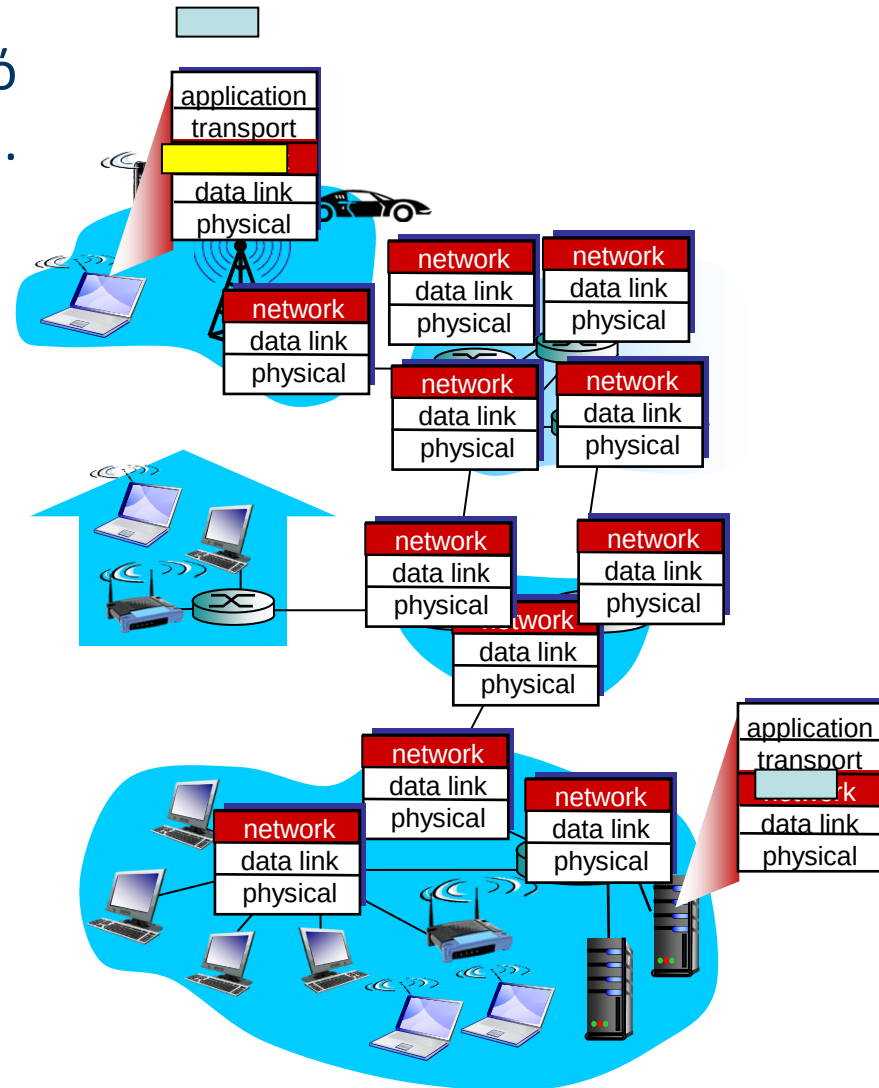
Περίγραμμα – ενότητες που εξετάζονται

- Μοντέλα υπηρεσιών του επιπέδου δικτύου
- Προώθηση έναντι δρομολόγησης (forwarding vs routing)
- IP: Πρωτόκολλο Διαδικτύου
- Μορφή δεδομενογράματος (datagram)
- Διευθυνσιοδότηση (addressing) IPv4
- Το πρωτόκολλο DHCP
- Μετάφραση Διευθύνσεων Δικτύου (NAT)



Επίπεδο Δικτύου

- Μεταφορά τμήματος (segment) από τον host αποστολέα στον host δέκτη.
- Στην πλευρά αποστολής τα τμήματα ενθυλακώνονται σε datagrams (δεδομενογράμματα).
- Στην πλευρά του δέκτη, παραδίδονται τα τμήματα στο επίπεδο μεταφοράς.
- Πρωτόκολλα επιπέδου δικτύου έχουμε σε κάθε υπολογιστή (host) και στους δρομολογητές.
- Κάθε δρομολογητής εξετάζει πεδία της κεφαλίδας όλων των IP datagrams που περνούν από αυτόν.
- Πρωτόκολλο στο Διαδίκτυο: το IP (Internet Protocol) v4 & v6



Δύο λειτουργίες κλειδιά του επιπέδου δικτύου

- **Πρώθηση (forwarding):**
Μετακίνηση πακέτων από μια εισερχόμενη ζεύξη του δρομολογητή στην κατάλληλη εξερχόμενη ζεύξη. Διεργασία τοπική στον δρομολογητή.
 - Χρησιμοποιούνται πίνακες πρώθησης (forwarding tables).
- **Δρομολόγηση (routing):**
Καθορισμός της διαδρομής που ακολουθούν τα πακέτα καθώς ρέουν από τον host προέλευσης στον host προορισμού. Διεργασία στο σύνολο του Διαδικτύου.
 - Χρησιμοποιούνται αλγόριθμοι δρομολόγησης (routing algorithms).

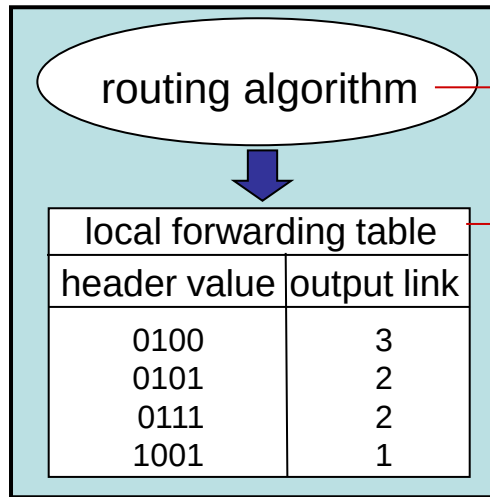
Αναλογία

- **Δρομολόγηση:**
Η διαδικασία σχεδιασμού ενός ταξιδιού από την προέλευση στον προορισμό.
- **Πρώθηση:**
Η διαδικασία επιλογής μιας εξόδου σε μια διασταύρωση (διάσχιση)

Κάθε δρομολογητής έχει ένα πίνακα πρώθησης



Αλληλεπίδραση μεταξύ δρομολόγησης και προώθησης

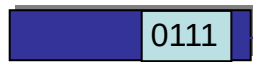


Ο αλγόριθμος δρομολόγησης προσδιορίζει την από άκρο-σε-άκρο διαδρομή.

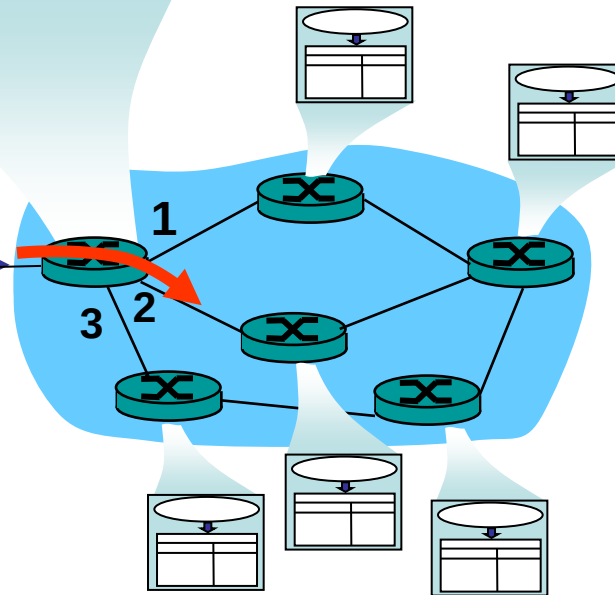
Ο πίνακας προώθησης προσδιορίζει τη τοπική προώθηση στον δρομολογητή.

Οι τιμές στους πίνακες προώθησης καθορίζονται σύμφωνα με τους αλγόριθμους δρομολόγησης.

Τιμή στη κεφαλίδα του αφικνούμενου πακέτου



Ο δρομολογητής αφού εξετάσει την κεφαλίδα (συγκεκριμένο πεδίο) του πακέτου προωθεί το πακέτο στη κατάλληλη ζεύξη.



Ένας αλγόριθμος δρομολόγησης:

- μπορεί να εκτελείται σε ένα μόνο σημείο ή
- μπορεί να είναι κατανεμημένος σε δρομολογητές,
- δέχεται μηνύματα του πρωτοκόλλου δρομολόγησης και παραμετροποιεί τους πίνακες στους δρομολογητές.



Μεταγωγείς πακέτων

- Ένας μεταγωγέας πακέτου (packet switch) μεταφέρει ένα πακέτο από τη διεπαφή ζεύξης εισόδου σε διεπαφή ζεύξης εξόδου (προώθηση).
- Μεταγωγείς επιπέδου ζεύξης
 - Η προώθηση γίνεται εξετάζοντας ένα πλαίσιο (frame) του επιπέδου ζεύξης (2nd layer switches / link-layer switches)
 - Χρησιμοποιούνται κυρίως στα τοπικά δίκτυα.
- Μεταγωγείς επιπέδου δικτύου
 - Η προώθηση γίνεται εξετάζοντας ένα datagram του επιπέδου δικτύου (3rd layer switches).
 - Ο όρος 3rd layer switch χρησιμοποιείται εναλλακτικά με τον όρο router (δρομολογητής).
 - Μπορούν και υλοποιούν πρωτόκολλα επιπέδου ζεύξης.
 - Χρησιμοποιούνται κυρίως στα δίκτυα κορμού.



Υπηρεσία σύνδεσης

- Πρόκειται για την 3η λειτουργία (εκτός της προώθησης και της δρομολόγησης) του επιπέδου δικτύου που είναι αρκετά σημαντική για ορισμένες δικτυακές αρχιτεκτονικές όπως:
 - ATM, Frame Relay, MPLS, X.25
- Πριν ξεκινήσει η ροή των datagrams, οι δύο τερματικοί υπολογιστές και οι δρομολογητές που μεσολαβούν αποκαθιστούν εικονική σύνδεση.
 - συμμετέχουν οι δρομολογητές
- Φυσικά και εδώ απαιτείται εγκαθίδρυση σύνδεσης πρώτα.
- Υπηρεσία σύνδεσης επιπέδου δικτύου vs μεταφοράς.
 - Δικτύου: σύνδεση μεταξύ δύο υπολογιστών, που όμως στην περίπτωση των εικονικών κυκλωμάτων (Virtual Circuits -VCs) μπορεί να συμμετέχουν και οι δρομολογητές που μεσολαβούν.
 - Μεταφοράς: σύνδεση μεταξύ δύο διεργασιών.



Μοντέλα υπηρεσιών δικτύου

- Πιθανές υπηρεσίες του επιπέδου δικτύου για ξεχωριστά datagrams:
 - Εγγυημένη παράδοση (το πακέτο θα φτάσει στο προορισμό του).
 - Εγγυημένη παράδοση με οριοθετημένη καθυστέρηση (πχ παράδοση από άκρο-σε-άκρο σε χρόνο μικρότερο από 40 msec).
- Πιθανές υπηρεσίες του επιπέδου δικτύου για ροή datagrams:
 - Παράδοση των datagrams με τη σωστή σειρά.
 - Εγγυημένο ελάχιστο εύρος ζώνης στη ροή (συγκεκριμένος ρυθμός μετάδοσης από την προέλευση στο προορισμό).
 - Εγγυημένη μέγιστη διακύμανση χρονισμού (jitter). Το χρονικό διάστημα μεταξύ δύο πακέτων στη αποστολή είναι το ίδιο και στη λήψη (ή αλλάζει μέχρι κάποιο όριο).
 - Υπηρεσίες ασφάλειας (κρυπτογράφηση).
 - Υπηρεσίες ακεραιότητας δεδομένων και επαλήθευσης προέλευσης.
- Στη πραγματικότητα: μόνο υπηρεσία βέλτιστης προσπάθειας.



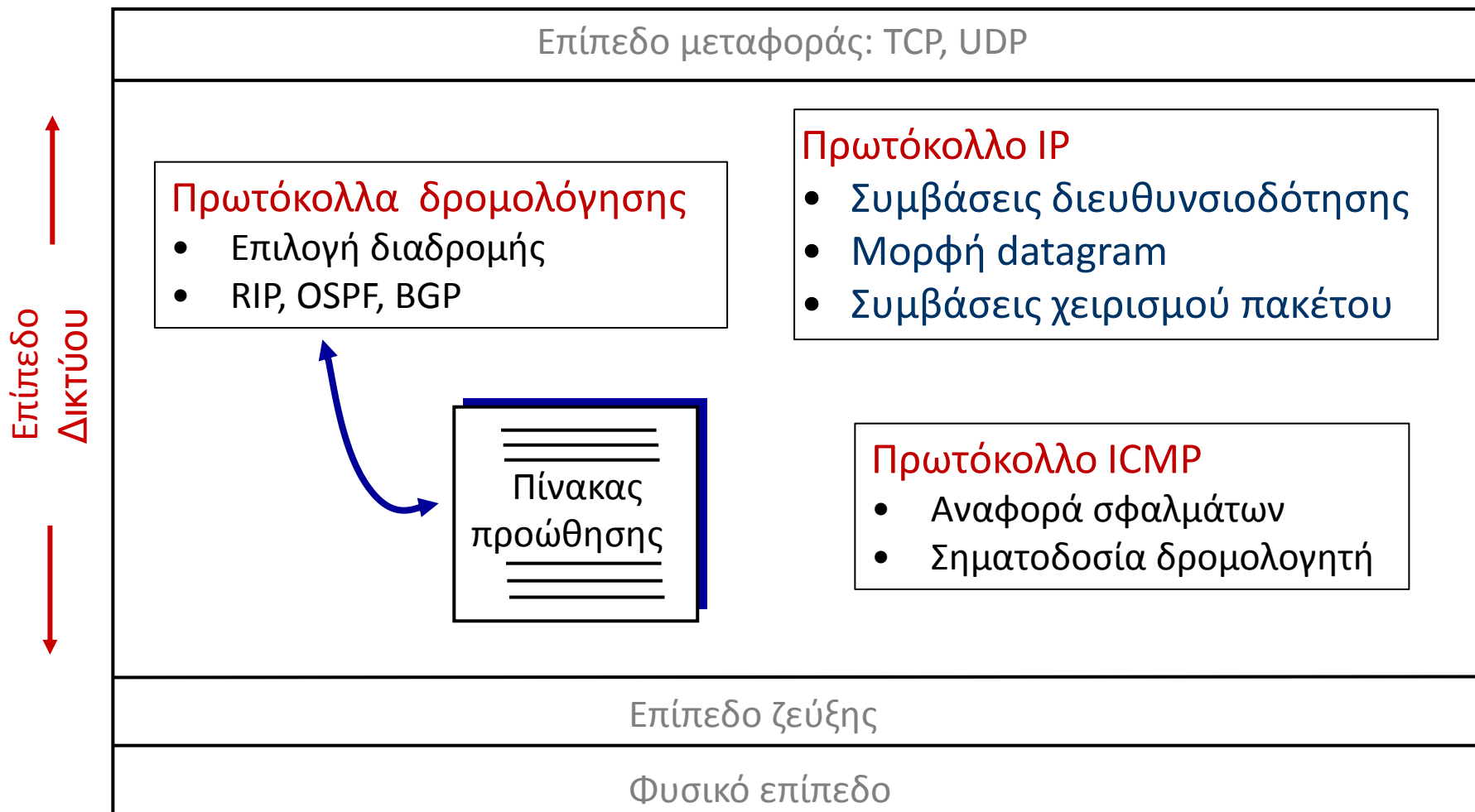
Τι προσφέρεται στο επίπεδο δικτύου

- Στη πραγματικότητα από το πρωτόκολλο του Διαδικτύου (IP protocol) προσφέρεται μόνο μια υπηρεσία **βέλτιστης προσπάθειας** και τίποτα άλλο.
- Χωρίς εγγύηση:
 - Διατήρησης του χρονισμού
 - Άφιξης των πακέτων στη σωστή σειρά
 - Για παράδοση όλων των πακέτων
- Στο επίπεδο δικτύου υπάρχουν όμως άλλες αρχιτεκτονικές που προσφέρουν κάτι παραπάνω:
 - Το ATM σταθερού ρυθμού bit και το
 - ATM διαθέσιμου ρυθμού bit.
- Αυτές χρησιμοποιούν συνδέσεις εικονικού κυκλώματος και προσφέρουν κάτι παραπάνω από την βέλτιστη προσπάθεια του IP πρωτοκόλλου.

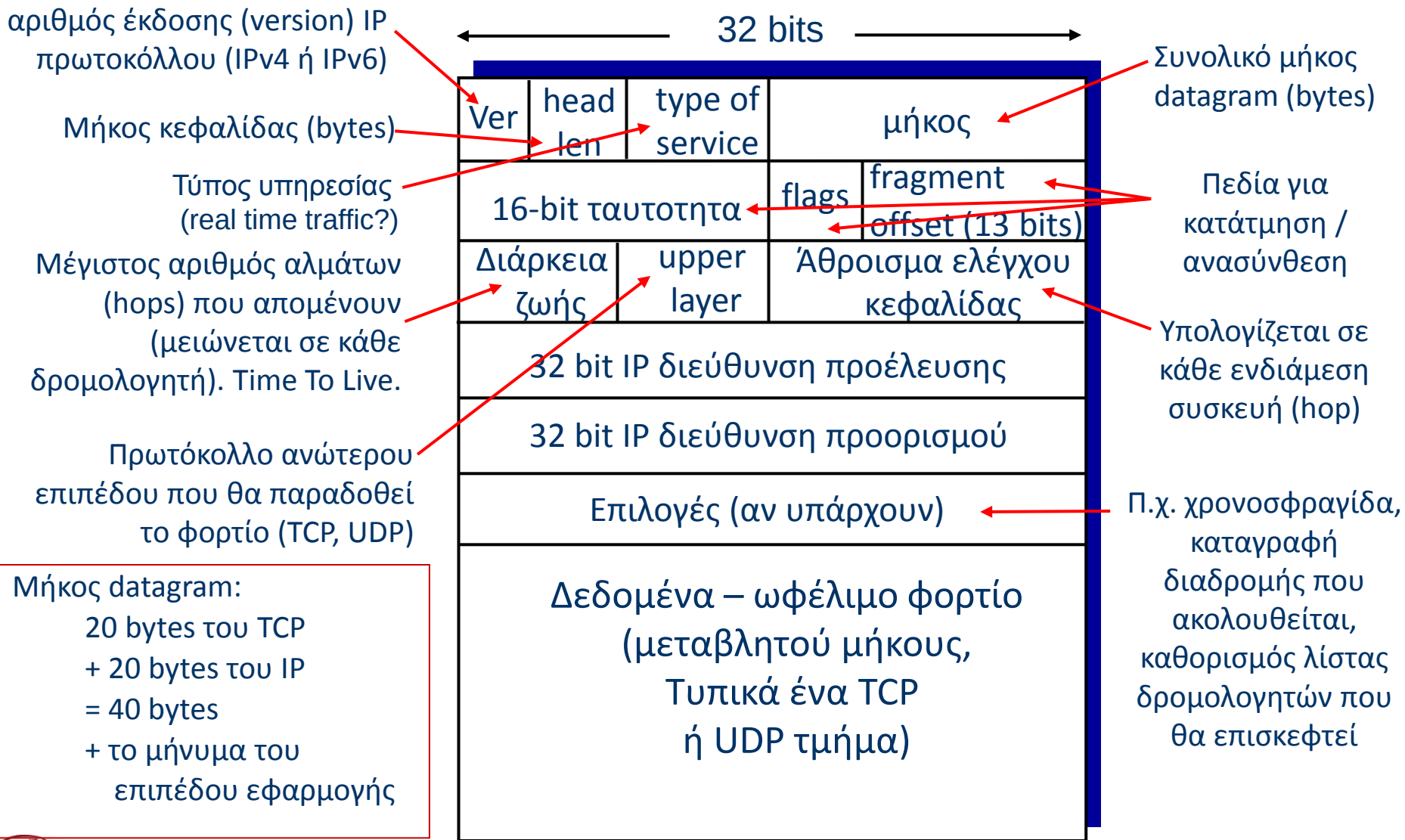


Το επίπεδο δικτύου στο Διαδίκτυο

- Τα συστατικά που το απαρτίζουν

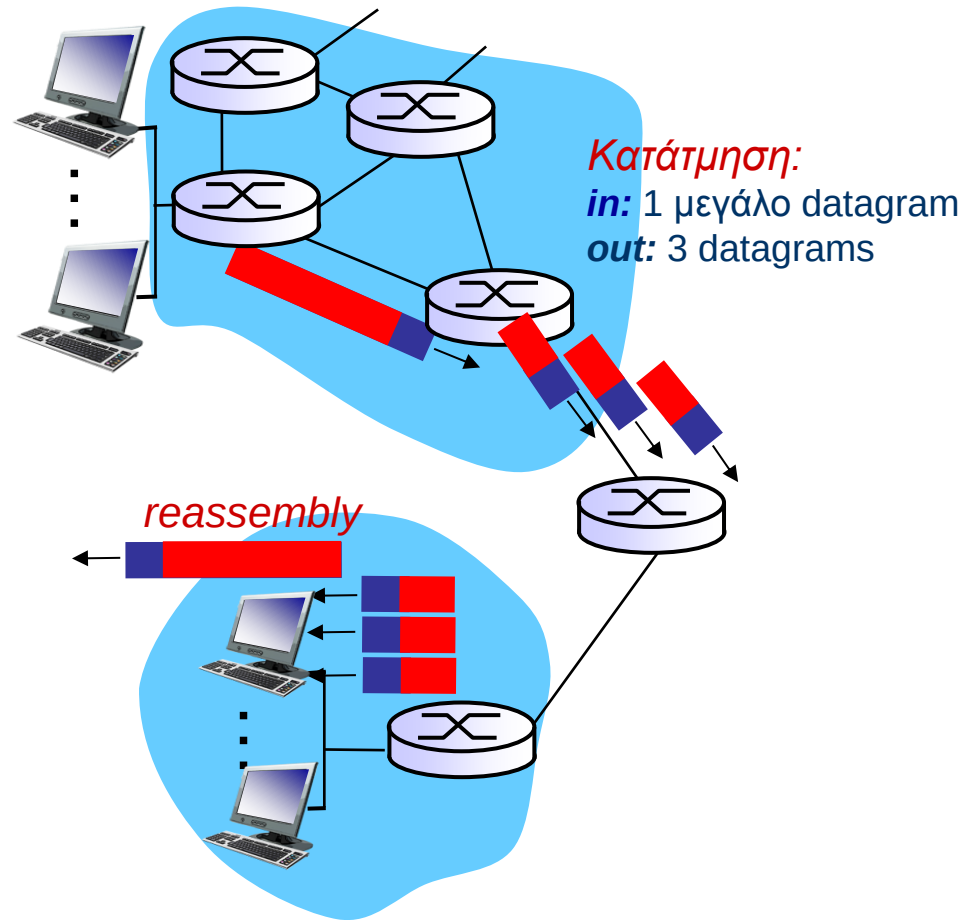


Μορφή datagram (δεδομενογράμματος) –IPv4



Κατάτμηση και ανασύνθεση του datagram

- Οι ζεύξεις του δικτύου ενδέχεται να έχουν κάποια μέγιστη μονάδα μεταφοράς (MTU -maximum transmission unit), δηλ. ένα μέγιστο δυνατό πακέτο επιπέδου ζεύξης.
 - Για διαφορετικούς τύπους ζεύξης, έχουμε διαφορετικές MTUs.
- Ένα μεγάλο IP datagram τεμαχίζεται στο δίκτυο (fragmentation):
 - ένα datagram γίνεται πολλαπλά datagrams,
 - “ανασυντίθενται” (reassembly) **μόνο** στον τελικό προορισμό,
 - τα bits της κεφαλίδας IP χρησιμοποιούνται για την ταυτοποίηση, διάταξη των σχετικών τεμαχίων.



Παράδειγμα κατάτμησης

έστω ότι έχουμε:

- ένα datagram 4000 byte
- και ότι
- MTU = 1500 bytes

	length	ID	frag	offset	
	=4000	=x	=0	=0	

Ένα μεγάλο datagram γίνεται πολλαπλά μικρότερα datagrams

1480 bytes στο
πεδίο δεδομένων

Μετατόπιση (offset)
= $1480/8$

	length	ID	flag	offset	
	=1500	=x	=1	=0	

	length	ID	flag	offset	
	=1500	=x	=1	=185	

	length	ID	flag	offset	
	=1040	=x	=0	=370	



Διευθυνσιοδότηση IP: εισαγωγή

- Μια διεύθυνση IP αποτελείται από 4 Bytes (32 bits, δηλαδή δυνητικά έχουμε 2^{32} IP διευθύνσεις).
- Τυπικά εκφράζονται με δεκαδικό συμβολισμό με τελείες (dotted-decimal notation)

- Αυτά τα τέσσερα Bytes χωρίζονται με τελείες και εκφράζονται στο δεκαδικό σύστημα (από 0 έως $2^8 - 1$):

147.95.40.60

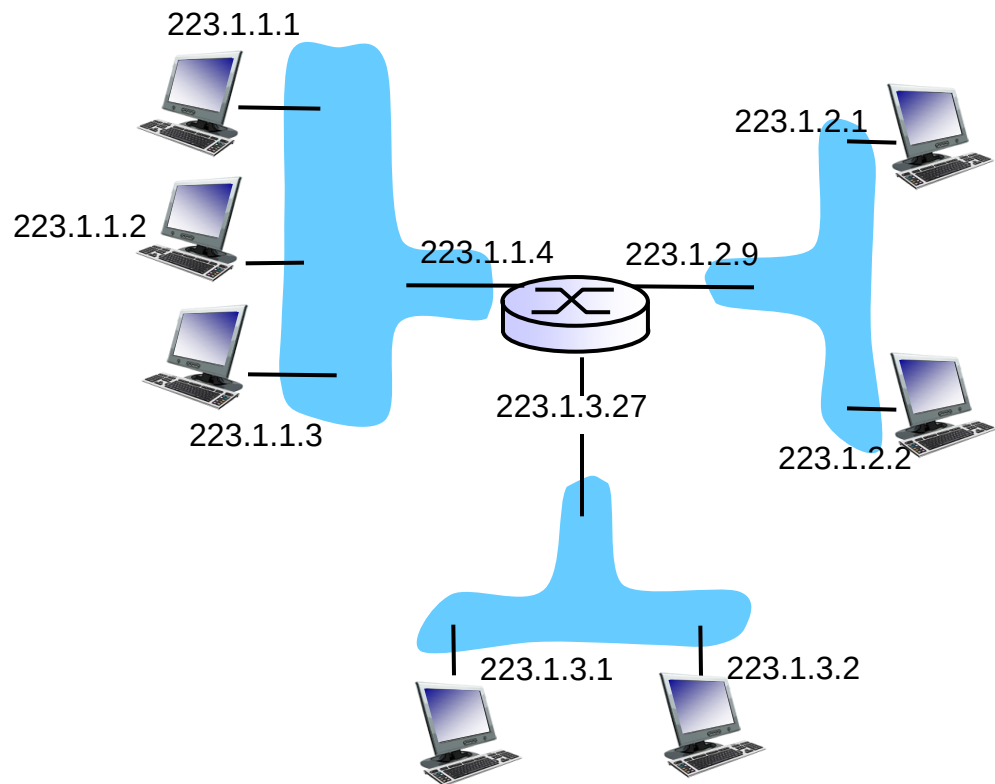
(10010011.01011111. 00101000.00111100)

- Η μορφή των IP διευθύνσεων είναι ιεραρχική (προχωρώντας από αριστερά προς τα δεξιά παίρνουμε όλο και πιο συγκεκριμένες πληροφορίες για τη θέση του υπολογιστή στο διαδίκτυο)
- Αυτές οι διευθύνσεις μπορεί να είναι είτε στατικές (μόνιμες) είτε δυναμικές (αποδίδονται από υπηρεσίες δυναμικά).



Αποδίδονται σε διεπαφές και όχι σε υπολογιστές

- Διεύθυνση IP (IP address): 32-bit ταυτότητα της διεπαφής (interface) του υπολογιστή / δρομολογητή.
- Διεπαφή ή διασύνδεση: το όριο μεταξύ υπολογιστή / δρομολογητή και της φυσικής ζεύξης.
- Μια διεύθυνση IP σχετίζεται με μια διεπαφή και όχι με υπολογιστή ή δρομολογητή.

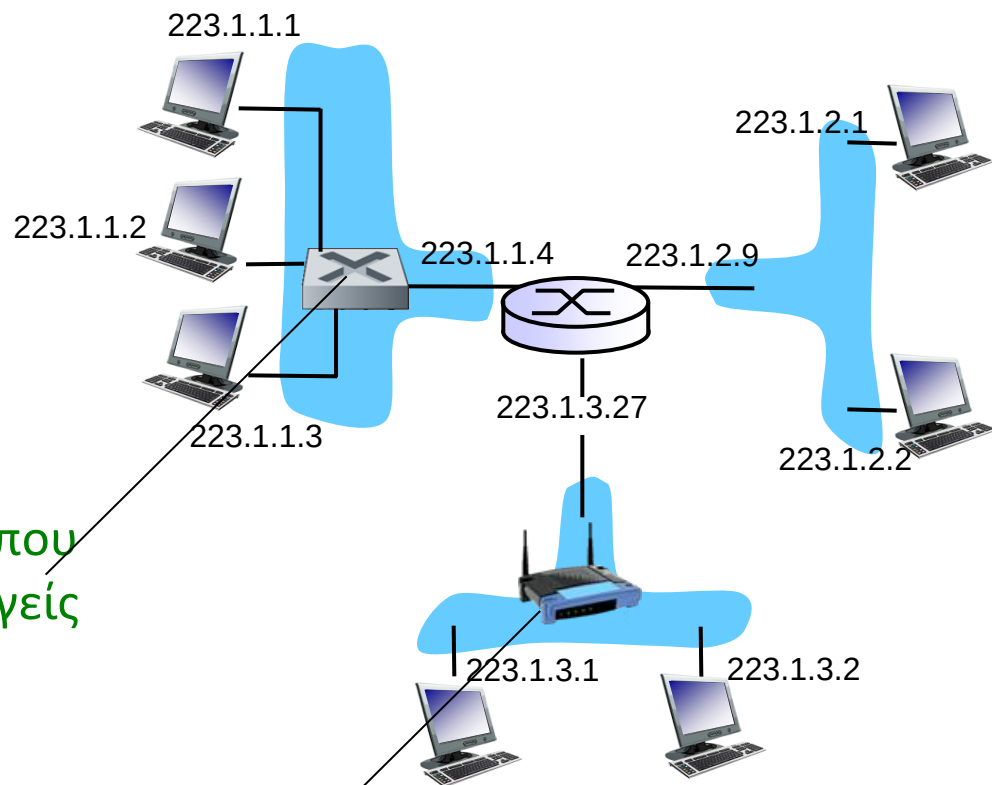


$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_1 \underbrace{00000001}_1 \underbrace{00000001}_1$$



Πως συνδέονται οι διεπαφές

- Οι δρομολογητές τυπικά έχουν πολλές διεπαφές.
- Ένας υπολογιστής τυπικά έχει μια διεπαφή.



Ενσύρματες Ethernet διεπαφές που συνδέονται με Ethernet μεταγωγείς

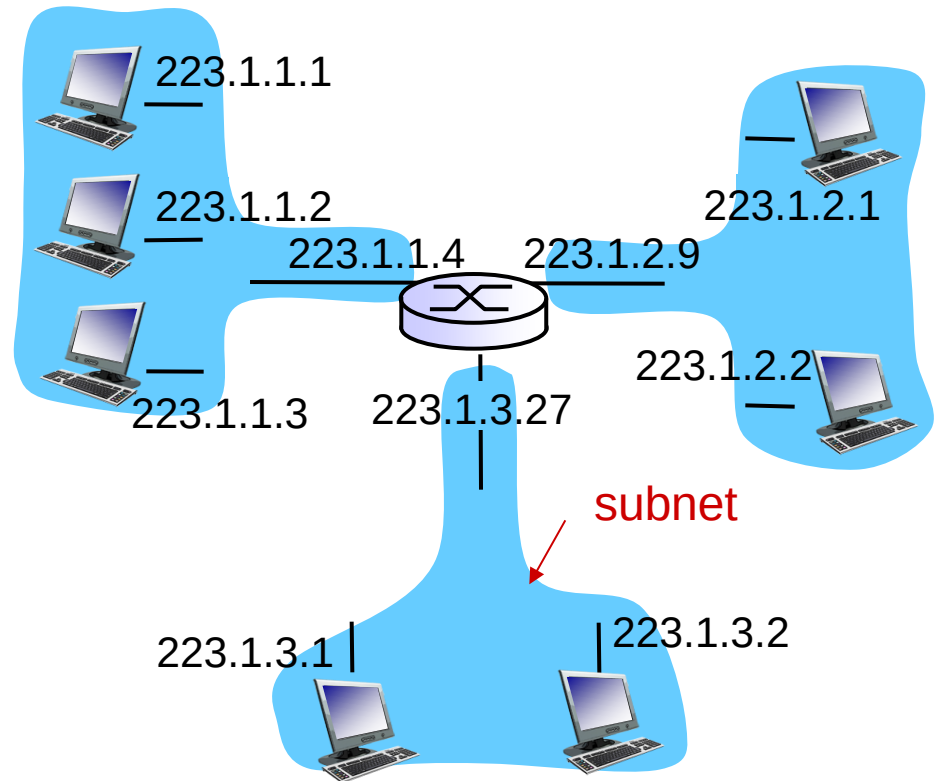
Ασύρματες WiFi διεπαφές που συνδέονται με WiFi συσκευές ασύρματης πρόσβασης

- Κάθε διεπαφή στο διαδίκτυο έχει μια **παγκόσμια μοναδική IP διεύθυνση**.



Υποδίκτυα (subnets)

- Διεύθυνση IP, 2 τμήματα:
 - Τμήμα υποδικτύου (subnet part) – υψηλής τάξης bits.
 - Τμήμα υπολογιστή (host part) - χαμηλής τάξης bits.
- Τι είναι ένα υποδίκτυο;
 - Διεπαφές συσκευών με ίδιο τμήμα υποδικτύου στις IP διευθύνσεις τους.
 - Έχουν φυσική πρόσβαση το ένα στο άλλο, χωρίς μεσολάβηση δρομολογητή

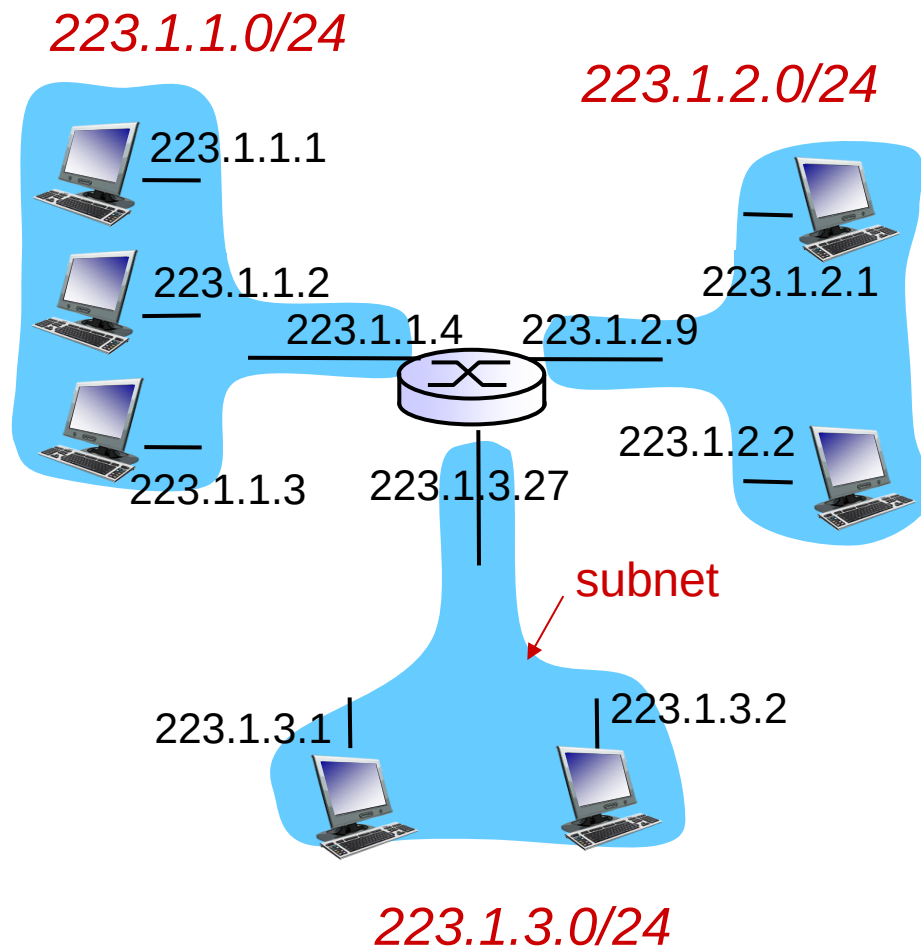


Δίκτυο που απαρτίζεται από 3 υποδίκτυα:
223.1.1.x, 223.1.2.x και 223.1.3.x



Συνταγή για τον προσδιορισμό των υποδικτύων

- Για τον καθορισμό των υποδικτύων, αποσυνδέστε κάθε διεπαφή από τον υπολογιστή ή το δρομολογητή, δημιουργώντας νησίδες απομονωμένων δικτύων.
- Κάθε απομονωμένο δίκτυο καλείται υποδίκτυο (subnet).



subnet mask: /24

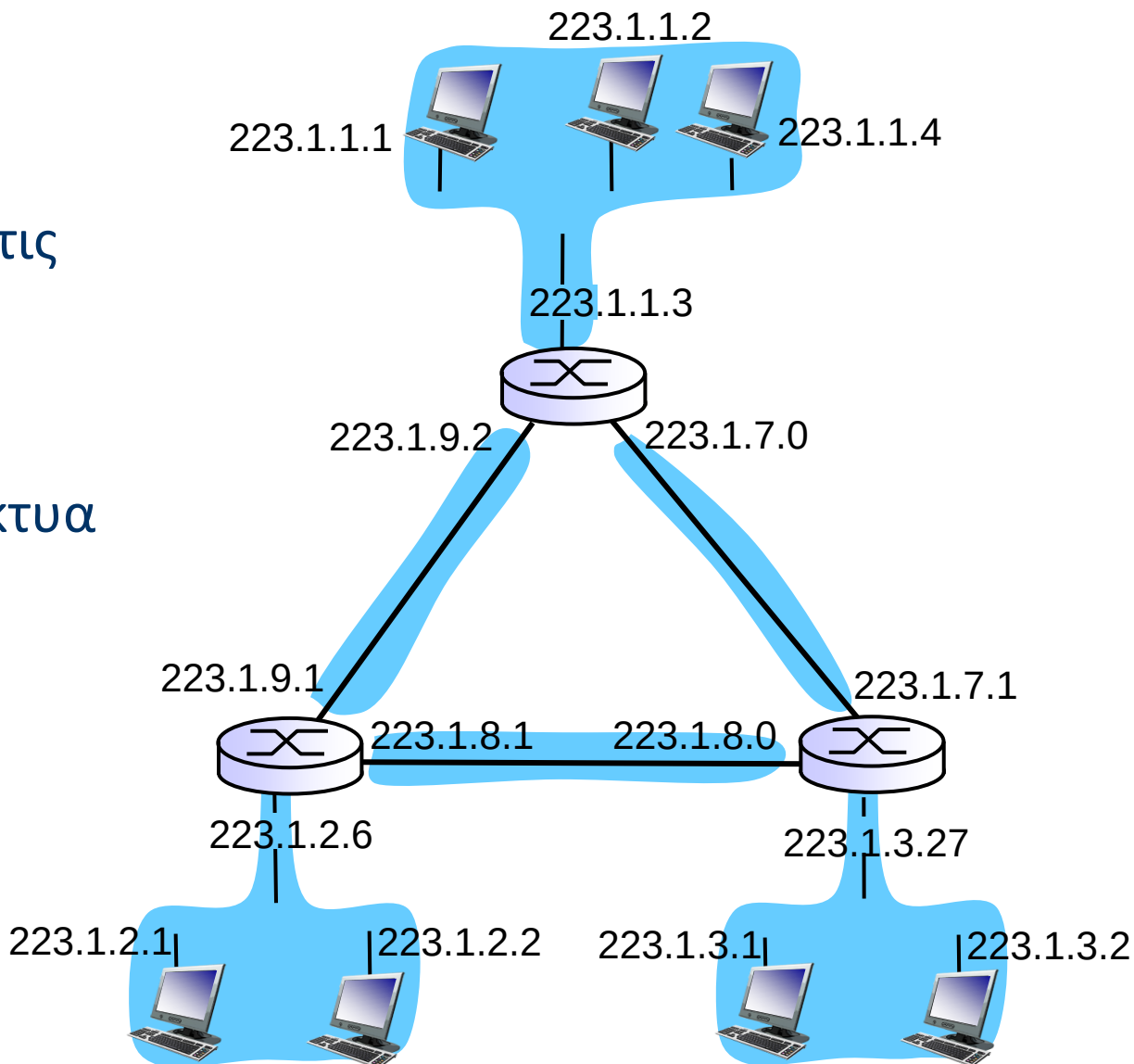
(μάσκα υποδικτύου)



Πόσα υποδίκτυα έχουμε;

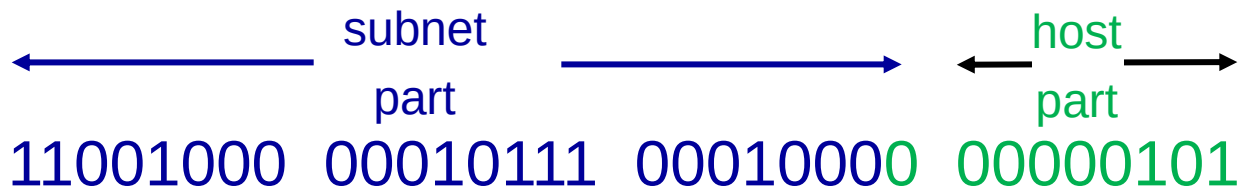
Απομονώνουμε τις
διεπαφές

Έχουμε 6 υποδίκτυα



Διευθυνσιοδότηση IP: CIDR

- **CIDR**: Classless InterDomain Routing (Αταξική Διατομεακή Δρομολόγηση).
- Το τμήμα (υπο-)δικτύου (subnet part) της διεύθυνσης έχει οποιοδήποτε μήκος.
- Η δομή της διεύθυνσης είναι: **a.b.c.d/x**,
όπου **x** είναι ο αριθμός των bits στο τμήμα (υπο-)δικτύου της διεύθυνσης (πρόθεμα)
- Οι δρομολογητές εξετάζουν μόνο το πρόθεμα του προορισμού όταν προωθούν ένα δεδομενογράφημα.



200.23.16.5/23



Διευθυνσιοδότηση με κλάσεις (classfull addressing)

- Ήσχυε πριν την υιοθέτηση του CIDR
- Το τμήμα του (υπο)δικτύου μιας IP διεύθυνσης περιοριζόταν σε μήκος 8, 16, 24 bit.
 - Δίκτυα κλάσης A (υποδίκτυο με διεύθυνση 8 bits)
 - Δίκτυα κλάσης B (υποδίκτυο με διεύθυνση 16 bits)
 - Δίκτυα κλάσης C (υποδίκτυο με διεύθυνση 8 bits)
- Αυτή η ταξινόμηση αποδείχτηκε προβληματική:
 - Τα δίκτυα κλάση C δεν επαρκούσαν για τις ανάγκες ενός οργανισμού.
 - Από την άλλη τα δίκτυα κλάσης B υπο-χρησιμοποιούσαν τις διευθύνσεις που διέθεταν.



Πως παίρνει κάποιος IP διευθύνσεις ;

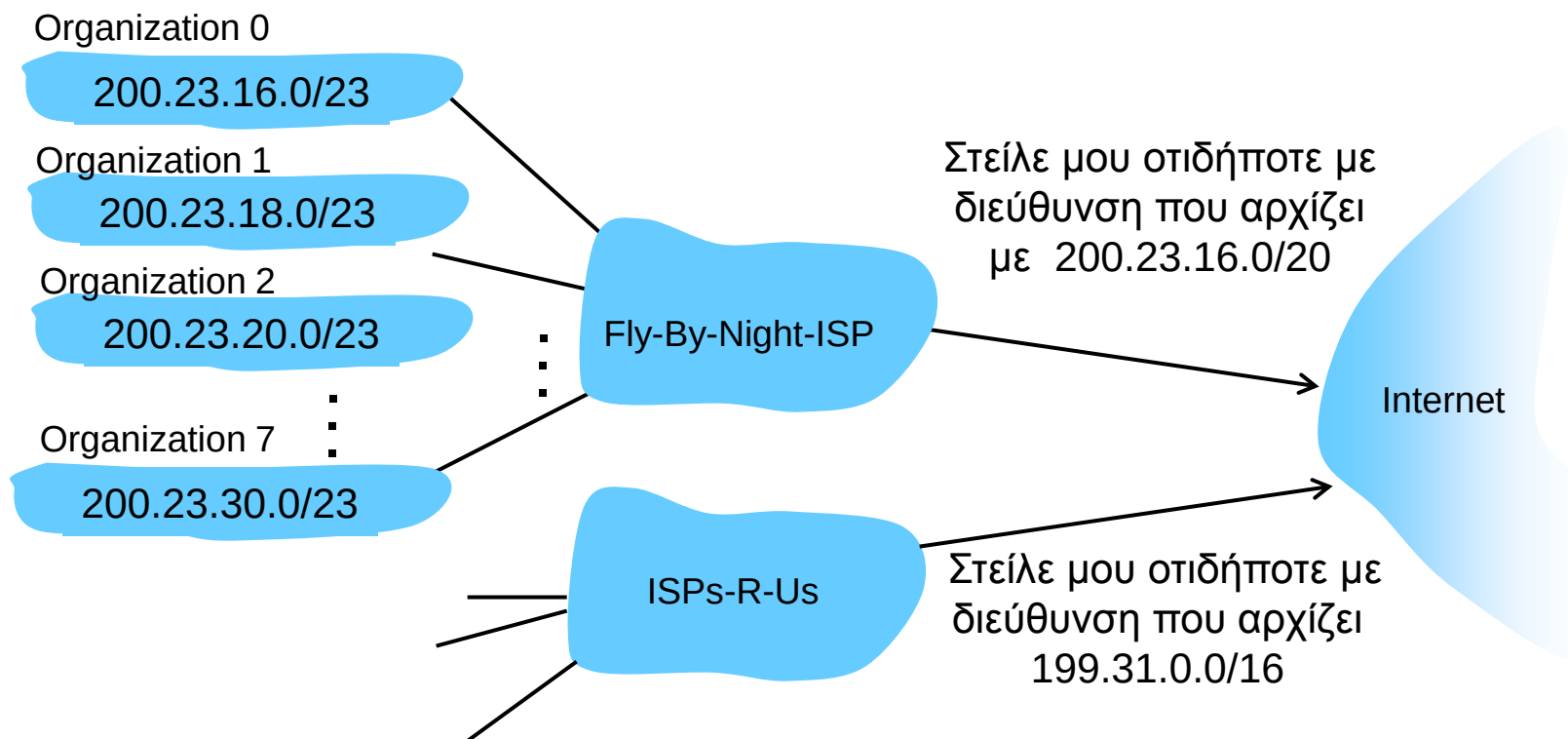
- Για να πάρει κάποιος οργανισμός μια ή περισσότερες IP διευθύνσεις θα πρέπει να απευθυνθεί στον ISP του.
- ICANN: Internet Corporation for Assigned Names and Numbers <http://www.icann.org/>
 - Κατανέμει διευθύνσεις στους ISPs.
 - Διαχειρίζεται DNS εξυπηρετητές ρίζας (root).
 - Αποδίδει ονόματα τομέων (domain names), διευθετεί διαφορές.

ISP's block	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/20
Organization 0	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/23
Organization 1	<u>11001000</u>	<u>00010111</u>	<u>00010010</u>	00000000	200.23.18.0/23
Organization 2	<u>11001000</u>	<u>00010111</u>	<u>00010100</u>	00000000	200.23.20.0/23
...					
Organization 7	<u>11001000</u>	<u>00010111</u>	<u>00011110</u>	00000000	200.23.30.0/23



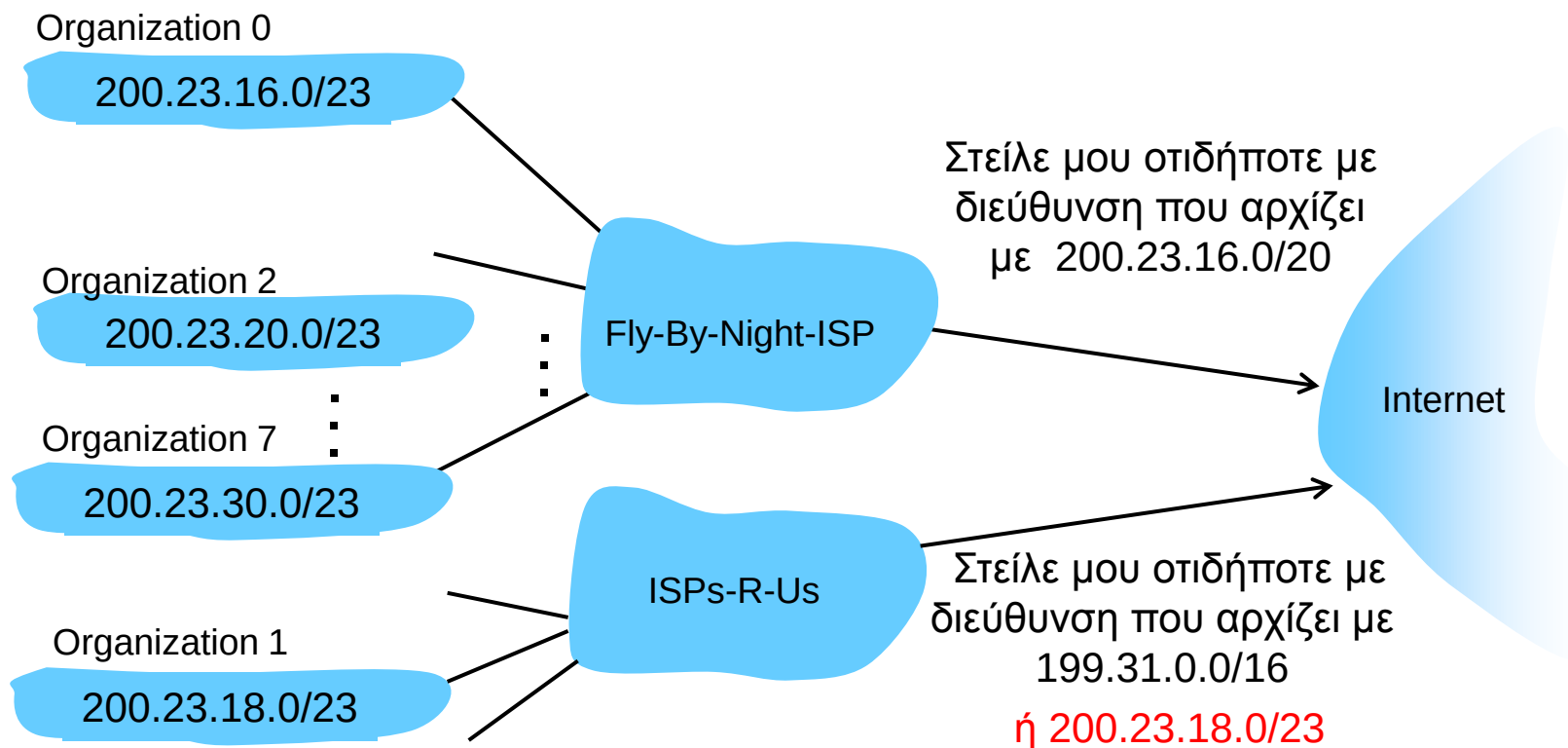
Ιεραρχική διευθυνσιοδότηση: συνάθροιση διαδρομών

- Hierarchical addressing: route aggregation
- Η ιεραρχική διευθυνσιοδότηση επιτρέπει την αποδοτική δημοσιοποίηση (advertisement) της πληροφορίας δρομολόγησης:



Επιλογή των πιο συγκεκριμένων διαδρομών

- Τι θα συμβεί αν ο Organization 1 πάει στον ISPs R-Us; (καταργείται η ιεραρχία)
- Ο ISPs R-Us θα πρέπει να δημοσιοποιεί και την 200.23.18.0/23.
- Και οι δύο ISPs δημοσιοποιούν τις διευθύνσεις του Organization 1.
- Όμως ο ISPs-R-Us έχει μια **πιο** συγκεκριμένη διαδρομή προς τον Organization 1.



Πώς παίρνει ένας υπολογιστής διεύθυνση IP;

- Προσδιορίζεται στο λειτουργικό σύστημα από το διαχειριστή του συστήματος.
 - Στα Windows:
Επιλογή: control-panel->network->configuration->tcp/ip->properties και καταχώρηση
 - Στα συστήματα UNIX:
Στο αρχείο /etc/rc.config
με καταχώρηση εγγραφής στο αρχείο.
- DHCP: Dynamic Host Configuration Protocol (δυναμική απόδοση διεύθυνσης από ένα εξυπηρετητή)
 - Η απόδοση γίνεται αυτόματα (“plug-and-play”).
- Οι IP διευθύνσεις των διεπαφών των δρομολογητών συνήθως αποδίδονται χειρονακτικά από τους διαχειριστές.

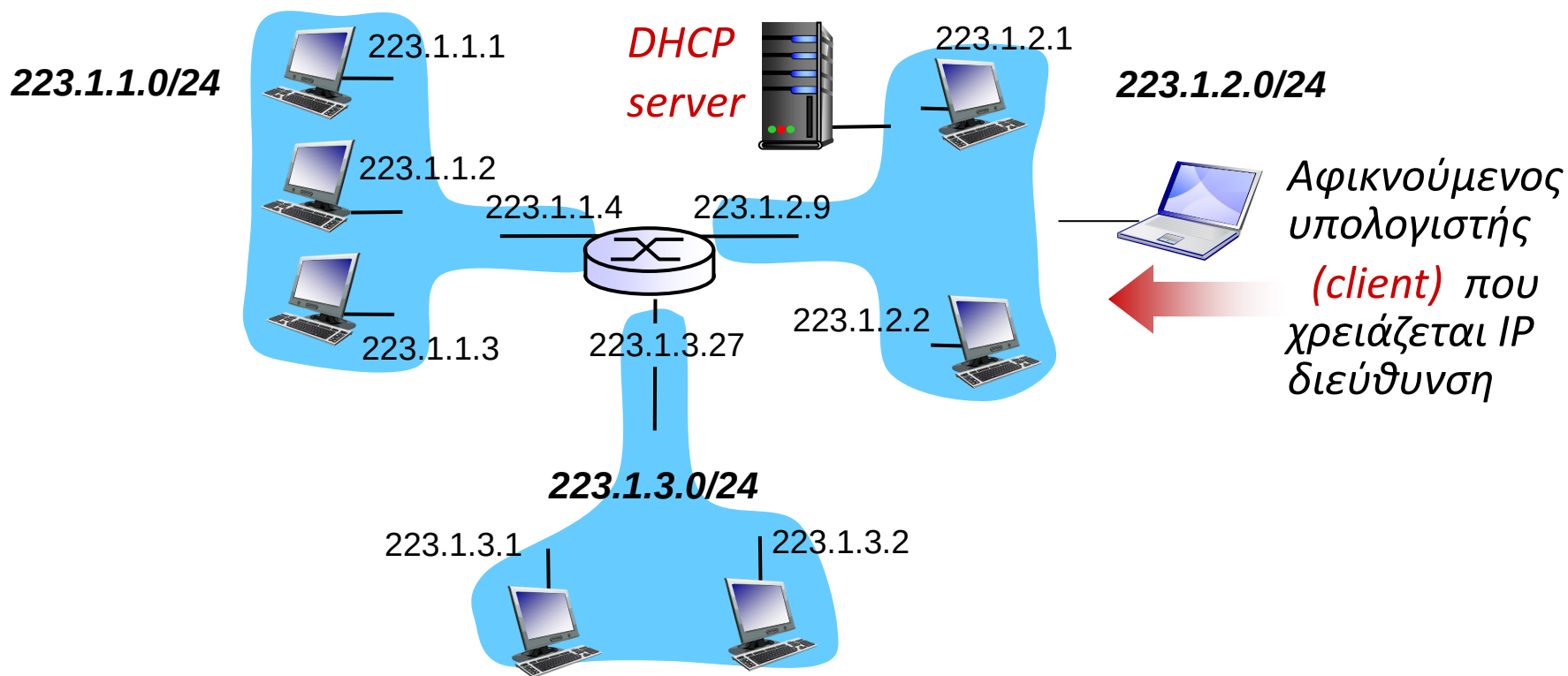


Το πρωτόκολλο DHCP

- Επιτρέπει στους υπολογιστές ν' αποκτούν (δεσμεύουν) δυναμικά διευθύνσεις IP όταν συνδέονται στο δίκτυο.
- Οι διευθύνσεις αποδίδονται αυτόματα από ένα DHCP εξυπηρετητή του δικτύου.
- Μπορεί να γίνεται ανανέωση της δέσμευσης της διεύθυνσης που χρησιμοποιείται.
- Επιτρέπεται η επαναχρησιμοποίηση των διευθύνσεων (η διεύθυνση δεσμεύεται μόνο όσο είναι συνδεδεμένος και «ενεργός» ο υπολογιστής –προσωρινή διεύθυνση).
- Υποστήριξη για κινητούς χρήστες που θέλουν να συνδεθούν στο δίκτυο.
- Επίσης, μέσω του DHCP προσφέρονται πρόσθετες πληροφορίες όπως η μάσκα του υποδικτύου και οι διευθύνσεις του εξυπηρετητή DNS και του τοπικού δρομολογητή.



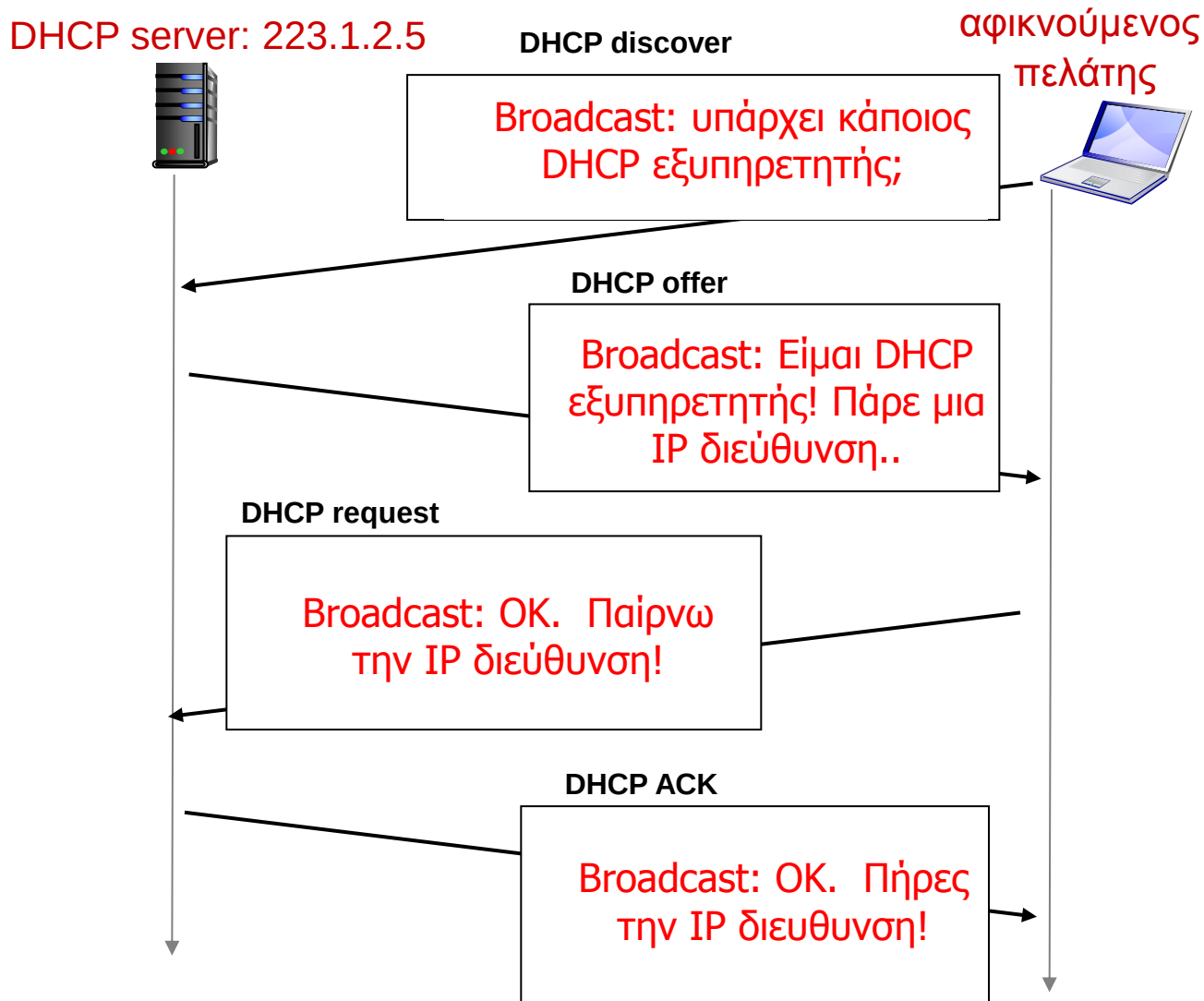
DHCP: επισκόπηση



- Ο υπολογιστής εκπέμπει (broadcasts) “DHCP discover” msg
- Ο εξυπηρετητής DHCP αποκρίνεται με “DHCP offer” msg
- Ο υπολογιστής ζητά διεύθυνση IP: “DHCP request” msg
- Ο εξυπηρετητής DHCP στέλνει τη διεύθυνση: “DHCP ack” msg

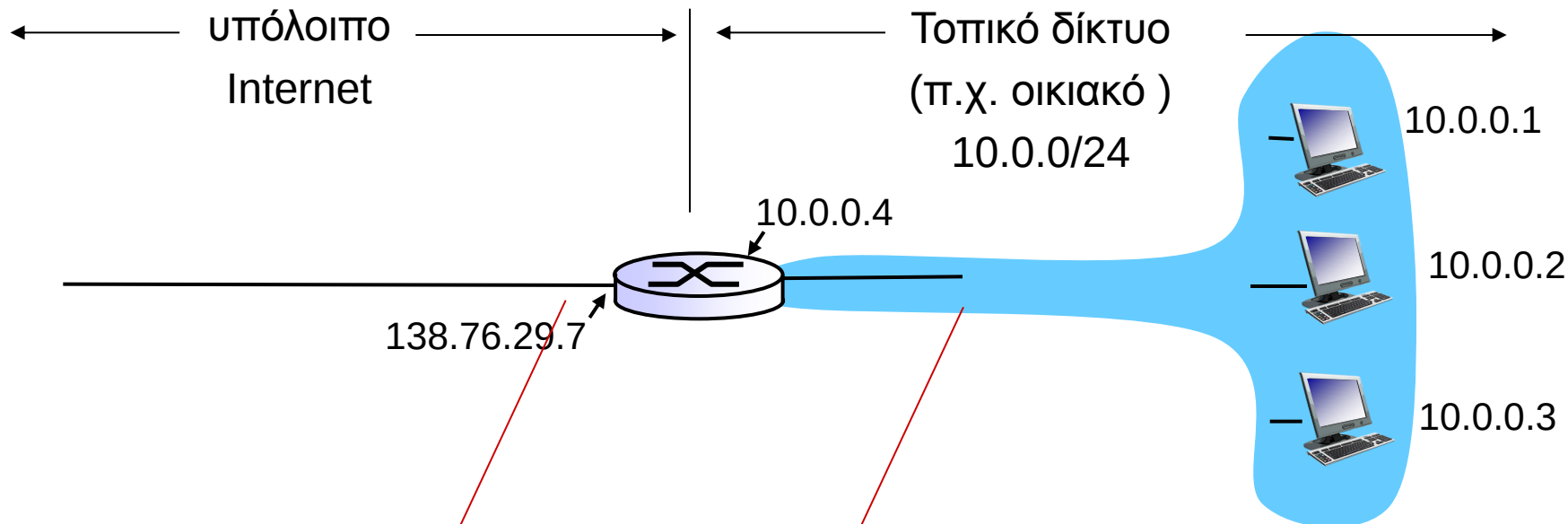


Σενάριο πελάτη-εξυπηρετητή DHCP



Μετάφραση Διευθύνσεων Δικτύου (NAT)

■ NAT: Network Address Translation



Όλα τα *datagrams* που φεύγουν από το τοπικό δίκτυο έχουν την ίδια διεύθυνση IP προέλευσης NAT: 138.76.29.7 και διαφορετικούς αριθμούς θύρας προέλευσης.

Τα *datagrams* με προέλευση ή προορισμό σε αυτό το δίκτυο έχουν διεύθυνση 10.0.0/24 ως προέλευση, προορισμό (όπως συνήθως.)



NAT: κίνητρο και χαρακτηριστικά

- Κίνητρο: το τοπικό δίκτυο χρησιμοποιεί μόνο μία διεύθυνση IP όσον αφορά τον εξωτερικό κόσμο.
- Δεν απαιτείται σύνολο διευθύνσεων από τον ISP: μόνο μία διεύθυνση IP για όλες τις συσκευές.
- Μπορούν να αλλαχτούν οι διευθύνσεις των συσκευών στο τοπικό δίκτυο χωρίς να ειδοποιηθεί ο έξω κόσμος.
- Μπορεί να αλλαχτεί ο ISP χωρίς να αλλάξουν οι διευθύνσεις στο τοπικό δίκτυο.
- Μια συσκευή εντός του τοπικού δικτύου δεν είναι ορατή από τον έξω κόσμο ως σαφώς διευθυνσιοδοτημένη (ένα συν στην ασφάλεια).

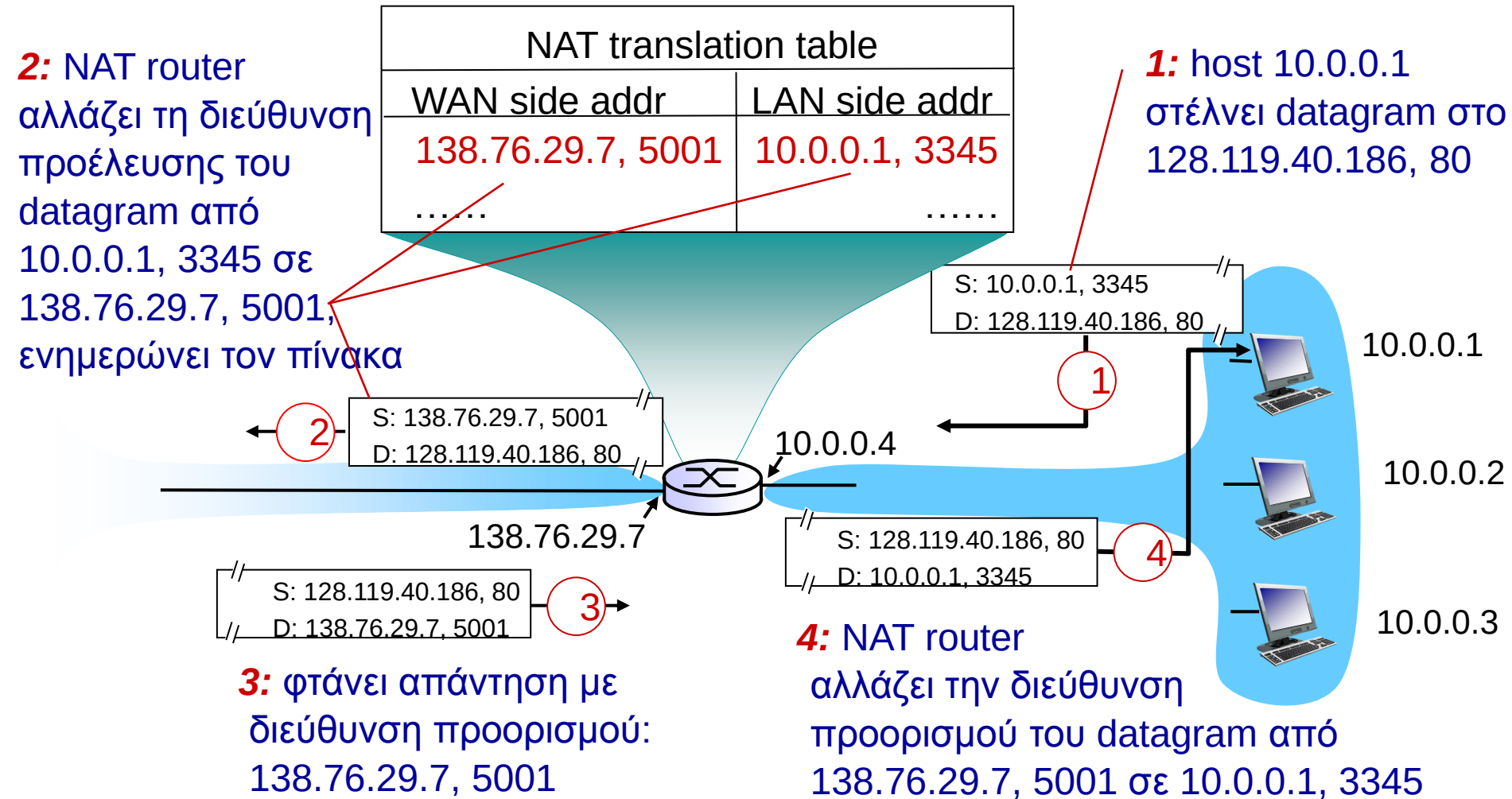


NAT: υλοποίηση (λειτουργίες δρομολογητή)

- Εξερχόμενα datagrams: αντικατάσταση [διεύθυνση IP προέλευσης, # θύρας] κάθε εξερχόμενου datagram με το [διεύθυνση IP NAT, νέος # θύρας]
... οι απομακρυσμένοι πελάτες/εξυπηρέτες θα απαντήσουν χρησιμοποιώντας (διεύθυνση IP NAT, νέος # θύρας) ως διεύθυνση προορισμού
- Αποθήκευση (στον πίνακα μετάφρασης NAT -translation table) κάθε ζεύγους μετάφρασης από [διεύθυνση IP προέλευσης, # θύρας] σε [διεύθυνση IP NAT, νέος # θύρας]
- Εισερχόμενα datagrams: αντικατάσταση [διεύθυνση IP NAT, νέος # θύρας] στα πεδία προορισμού κάθε εισερχόμενου datagram με το αντίστοιχο [διεύθυνση IP προέλευσης, # θύρας] που είναι αποθηκευμένο στον πίνακα NAT.



NAT: Παράδειγμα λειτουργίας



NAT: παρατηρήσεις

- Πεδίο 16-bit αριθμού θύρας:
 - 60.000 ταυτόχρονες συνδέσεις με μια μόνο διεύθυνση στην πλευρά του LAN!
- Το NAT είναι αμφιλεγόμενο:
 - Οι αριθμοί θυρών πρέπει να χρησιμοποιούνται για διευθυνσιοδότηση διεργασιών μόνο και όχι υπολογιστών.
 - Οι δρομολογητές θα πρέπει να επεξεργάζονται πακέτα μόνο μέχρι το επίπεδο 3.
 - Παραβιάζει την αρχή από-άκρο-σε-άκρο (end-to-end argument):
 - η δυνατότητα NAT πρέπει να ληφθεί υπόψη από τους σχεδιαστές εφαρμογών, πχ, εφαρμογές P2P.
 - Η έλλειψη διευθύνσεων θα πρέπει να επιλυθεί με το IPv6 (και όχι με το NAT).

