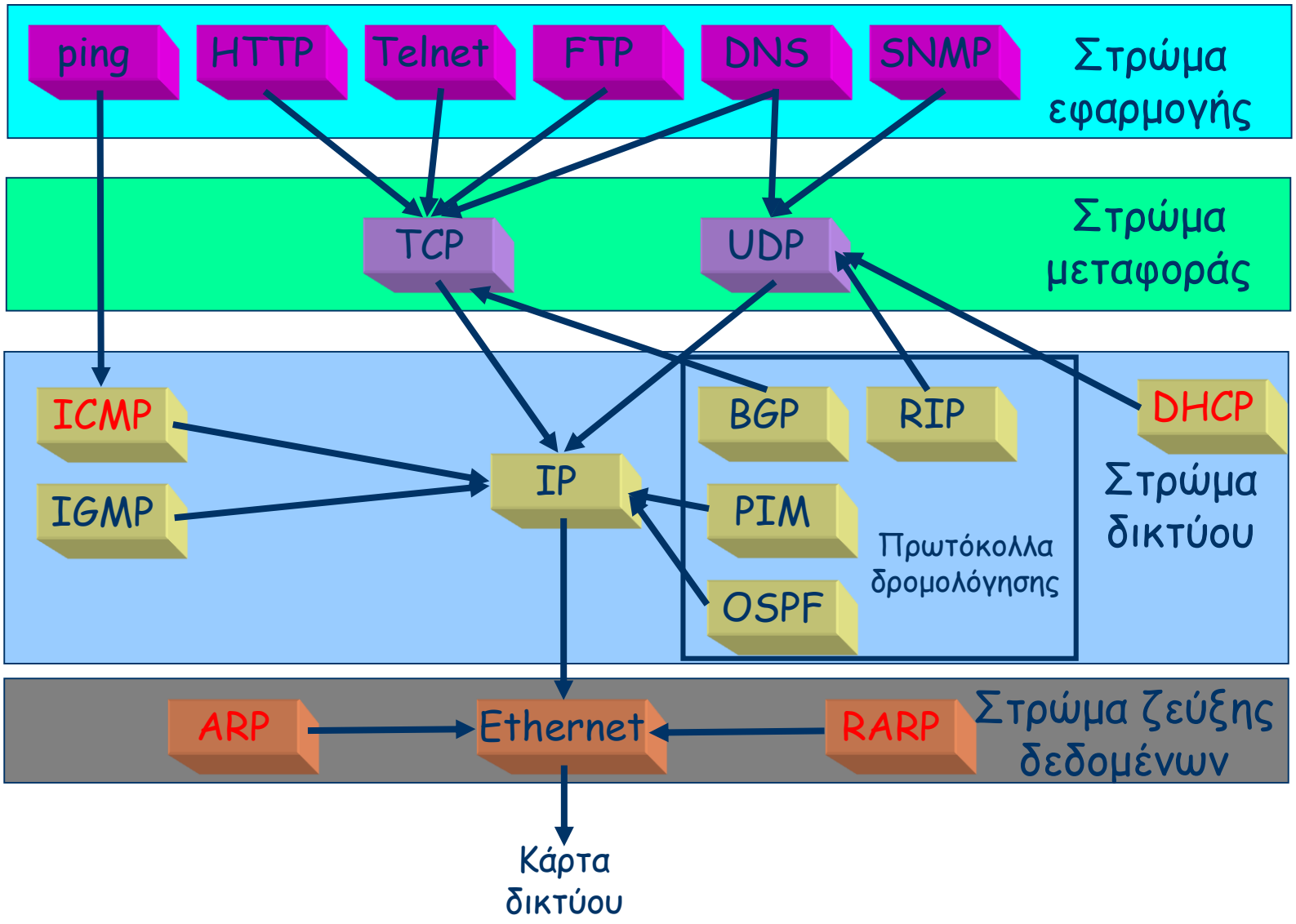
ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Βοηθητικά
Πρωτόκολλα
Ελέγχου IP

Πρωτόκολλα στρώματος δικτύου στο Internet

- Στο Internet, το IP χρησιμοποιείται για τη μεταφορά δεδομένων. Όμως για την εύρυθμη λειτουργία του IP χρησιμοποιείται μια πλειάδα άλλων πρωτοκόλλων, όπως:
- Πρωτόκολλα ελέγχου στο στρώμα δικτύου
  - ICMP, IGMP, BOOTP, DHCP
- Πρωτόκολλα δρομολόγησης
  - RIP, OSPF, PIM, BGP
- Πρωτόκολλα για την επίλυση διευθύνσεων
  - ARP, RARP (λογικά τοποθετούνται στο στρώμα ζεύξης δεδομένων)
  - NAT (εξάντληση διευθύνσεων IPv4)
- Πρωτόκολλα για την υποβοήθηση της κινητικότητας χρηστών
  - Mobile IP, Cellular IP

Αντιστοιχία στρωμάτων OSI και πρωτοκόλλων σουίτας TCP/IP



Αναζήτηση διευθύνσεων IP

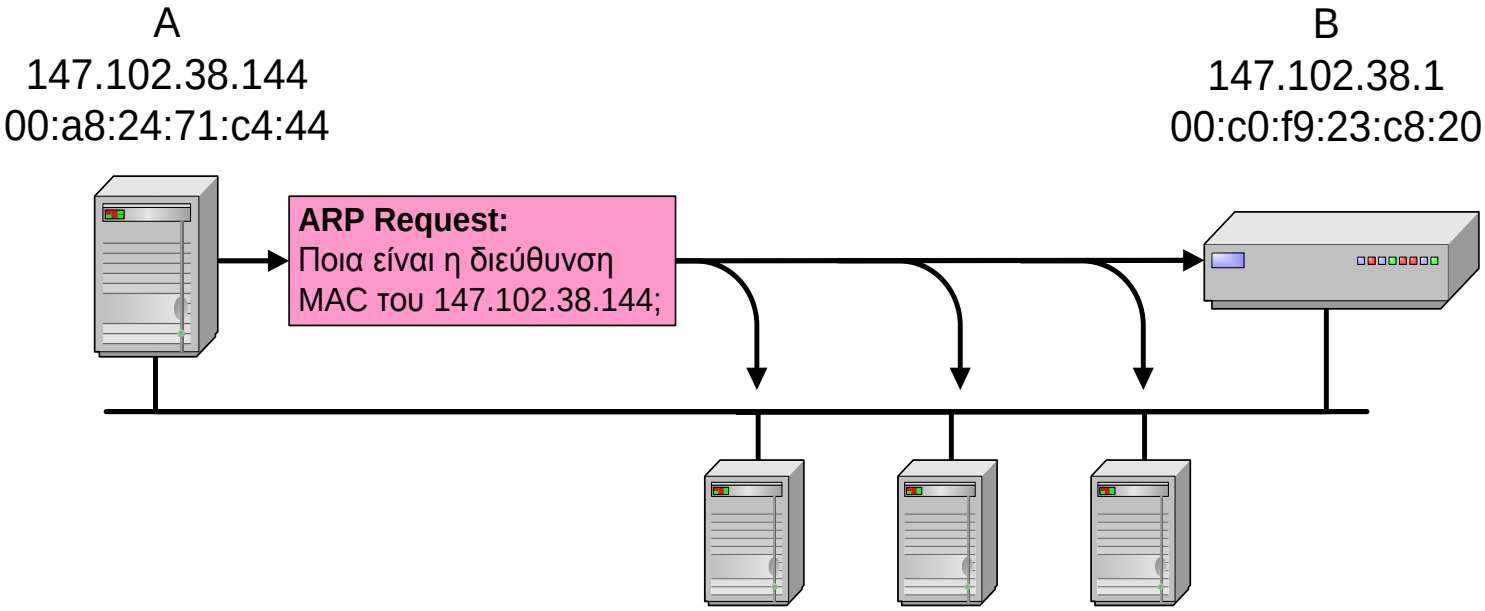
Πρωτόκολλα
ARP/RARP

Πρωτόκολλο ARP

- Δεδομένης της διεύθυνσης IP, να βρεθεί η διεύθυνση MAC
- Μια λύση είναι να υπάρχει κάπου στο σύστημα ένα αρχείο διάρθρωσης που να αντιστοιχεί τις διευθύνσεις IP σε Ethernet
  - 197.15.3.1 $\Rightarrow$ 0A:4B:00:00:07:08
- Καλύτερη λύση το πρωτόκολλο επίλυσης διευθύνσεων ARP (Address Resolution Protocol)

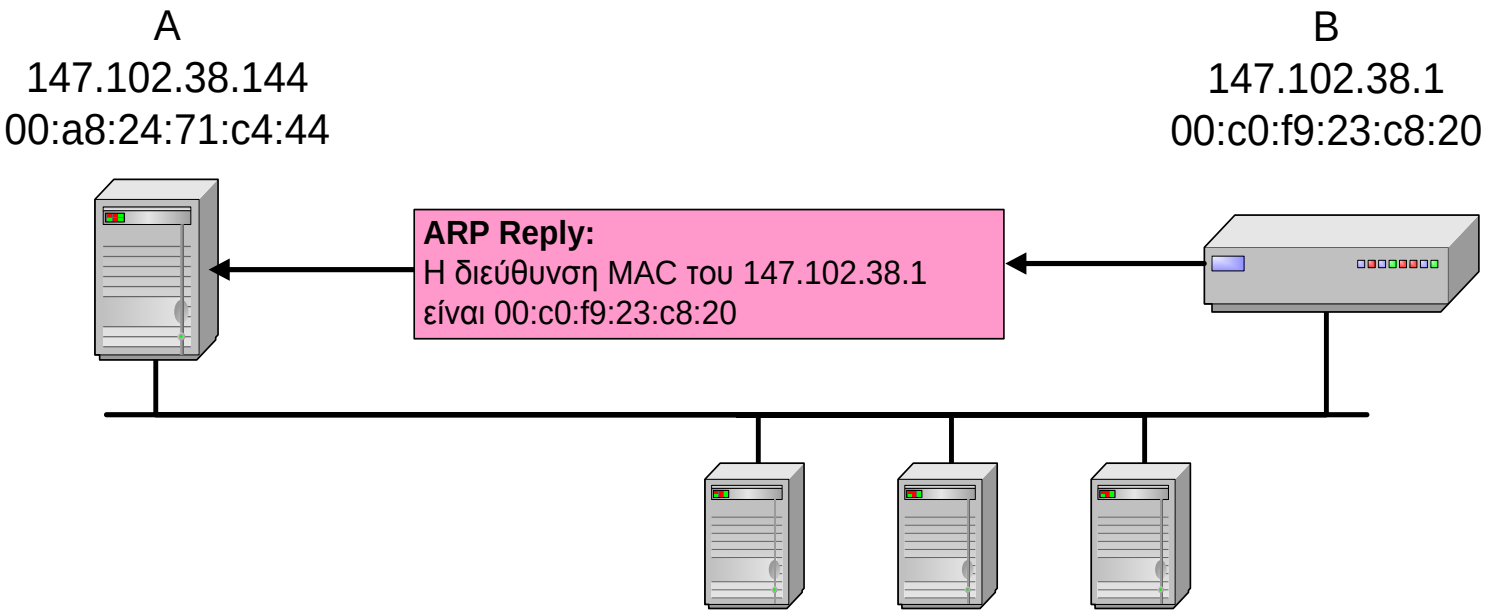
Λειτουργία

- Ο Α γνωρίζει τη διεύθυνση IP του Β και θέλει να μάθει τη φυσική διεύθυνση (MAC) του Β
- Ο Α εκπέμπει (broadcast) μια αίτηση ARP που περιέχει τη διεύθυνση IP του Β
  - όλες οι μηχανές στο LAN λαμβάνουν την αίτηση ARP

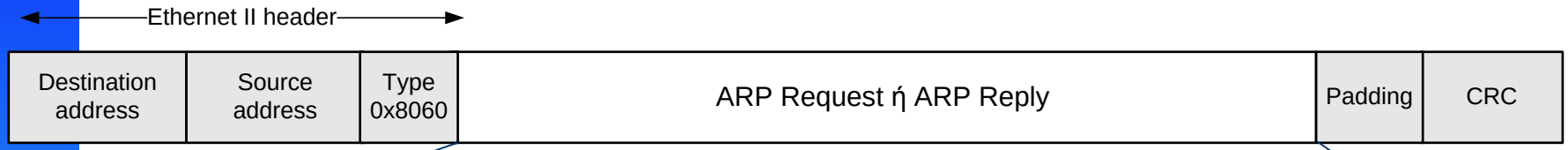


Λειτουργία (συν)

- Ο Β λαμβάνει το πακέτο ARP και απαντά (unicast) με τη φυσική του διεύθυνση (MAC)
  - ενημερώνει τον πίνακα ARP του με τις διευθύνσεις της πηγής (σύντομα θα κληθεί να απαντήσει)



Μορφή πακέτου ARP



Hardware type (2 byte)		Protocol type (2 byte)
Hardware address length (1 byte)	Protocol address length (1 byte)	Operation code (2 byte)
Sender Hardware Address (SHA)*		
Sender Protocol Address (SPA)*		
Target Hardware Address (THA)*		
Target Protocol Address (TPA)*		

* Το μήκος καθορίζεται από τα αντίστοιχα πεδία μήκους της επικεφαλίδας

Λειτουργία (συν)

- *ARP Request από τον Α:*

  SHA: 00:a8:24:71:c4:44
  SPA: 147.102.38.144
  THA: 00:00:00:00:00:00 (η τιμή αγνοείται στα ARP request)
  TPA: 147.102.38.1

- *ARP Reply από τον Β:*

  SHA: 00:c0:f9:23:c8:20
  SPA: 147.102.38.1
  THA: 00:a8:24:71:c4:44
  TPA: 147.102.38.144

- *Ο Α αποθηκεύει το ζεύγος (SHA, SPA) σε προσωρινή μνήμη (cache) μέχρις ότου παλιώσει η πληροφορία*

Προσωρινή μνήμη ARP (ARP cache)

- κάθε κόμβος IP (Host, Router) έχει ένα πίνακα (ARP cache ή Neighbor cache)
- περιέχει τις τρέχουσες εγγραφές, ζεύγη διευθύνσεων IP/MAC κόμβων στο ίδιο LAN
  - δεν γίνεται ARP request/reply για κάθε πακέτο IP
- η εγγραφή διαγράφεται εάν δεν ενημερωθεί προτού εκπνεύσει ο χρόνος (TTL)
  - 2 min μέχρι το πολύ 20 min

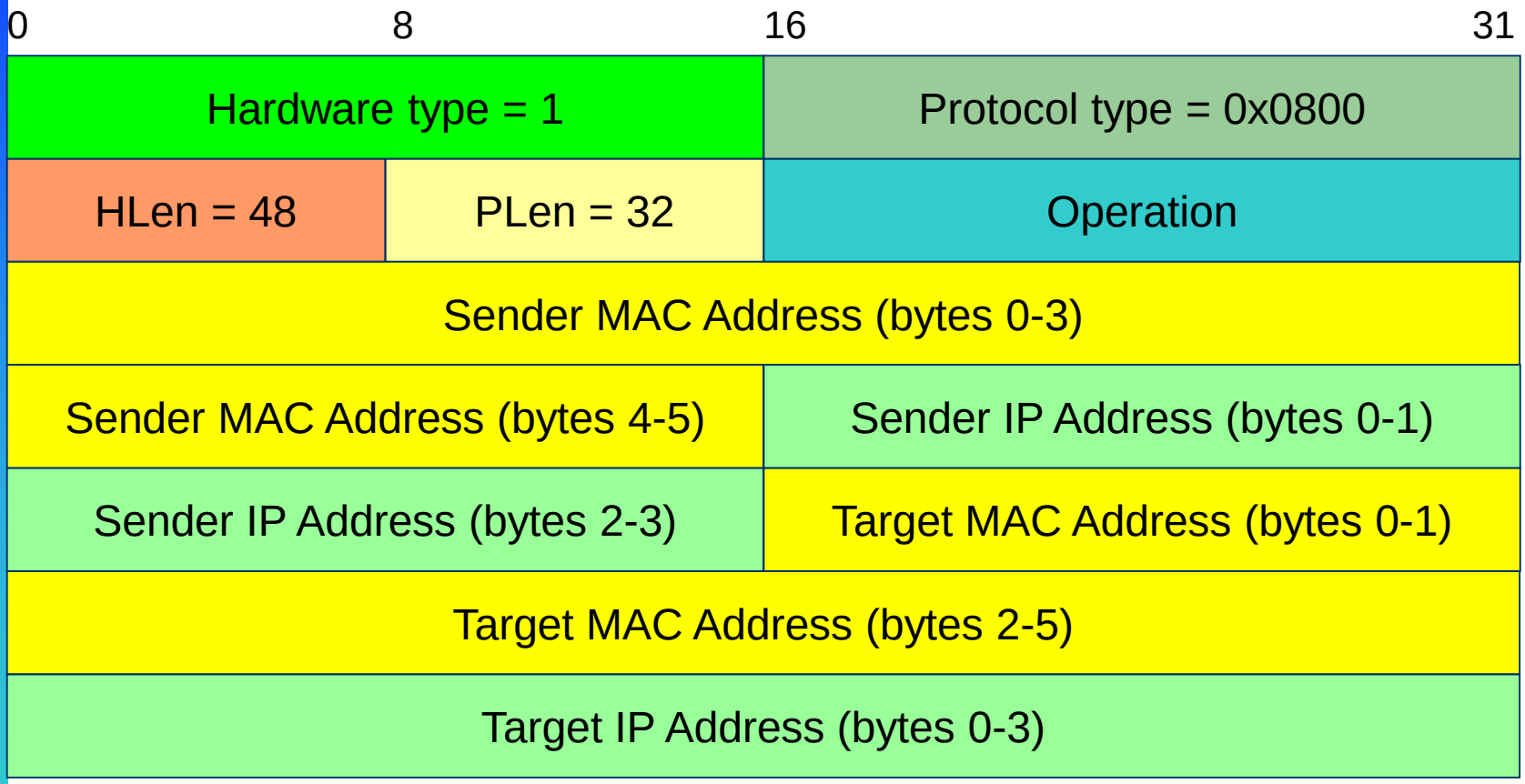
Προσωρινή μνήμη (συν)

- για κάθε μήνυμα ARP (Request ή Reply) που λαμβάνει ένας κόμβος
  - ενημερώνει την SHA
    - εάν ήδη έχει εγγραφή για την SPA στην προσωρινή μνήμη
  - προσθέτει την εγγραφή (SPA,SHA) στην προσωρινή μνήμη
    - εάν η TPA του μηνύματος ταυτίζεται με την IP διεύθυνσή του
  - απαντά με ARP Reply, εάν έλαβε ARP Request
    - ανταλλάσσοντας τα πεδία διευθύνσεων sender/target και θέτοντας τις δικές του διευθύνσεις SPA, SHA

Πακέτο ARP

- Το ARP δεν ειδικεύεται σε Ethernet & IP μόνο
  - Hardware Type: τύπος φυσικής διεύθυνσης (π.χ., Ethernet)
  - Protocol Type: τύπος πρωτοκόλλου ανωτέρου στρώματος (π.χ., IP)
  - Hardware address length: μήκος φυσικής διεύθυνσης
  - Protocol address length: μήκος διεύθυνσης πρωτοκόλλου
  - Operation: αίτηση ARP (1) ή απάντηση ARP (2)
  - Sender/Target Physical/Protocol address: οι αντίστοιχες φυσικές/πρωτοκόλλου διευθύνσεις πηγής/προορισμού

Πακέτο ARP για IP και Ethernet



Ενθυλάκωση ARP σε Ethernet

Destination Address (bytes 0-3)	0
Destination Address (bytes 4-5)	Source Address (bytes 0-1)
Source Address (bytes 2-5)	
Protocol type = 0x0806	ARP (28 bytes)
ARP (28 bytes)	
ARP (28 bytes)	
ARP (28 bytes)	
ARP (28 bytes)	
ARP (28 bytes)	
ARP (28 bytes)	
ARP (28 bytes)	Padding (18 bytes)
Padding(18 bytes)	
Padding(18 bytes)	
Padding(18 bytes)	
Padding(18 bytes)	
CRC (4 bytes)	

Δύο ερωτήσεις για το ARP

- Τι συμβαίνει όταν το ARP Request απευθύνεται σε υπολογιστή που δεν υπάρχει;
  - αποστέλλονται πολλά ARP Request με αυξανόμενα διαστήματα μεταξύ διαδοχικών αιτήσεων
  - τελικά το ARP εγκαταλείπει
- Σε κάποια συστήματα (όπως Linux) ο host στέλνει περιοδικά ARP Request για όλες τις διευθύνσεις στον πίνακα ARP
  - διατηρεί τον πίνακα, αλλά αυξάνει και την κίνηση

Δύο ερωτήσεις για το ARP

- Τι συμβαίνει εάν ο υπολογιστής στείλει ARP request για τη δικιά του διεύθυνση IP (απρόκλητο ARP);
  - Οι άλλες μηχανές το χειρίζονται σαν να ήταν κανονικό ARP request

Απρόκλητο ARP (Gratuitous ARP)

- Αποστολή μηνύματος ARP από host για τη δικιά του διεύθυνση IP
  - ARP Request με TPA=SPA και THA=0, εναλλακτικά
  - ARP Reply με TPA=SPA και THA=SHA
- Δεν αναμένει απάντηση, ενημερώνει τους πίνακες των άλλων με τη δική του διεύθυνση MAC
- Χρήσιμο κατά την εκκίνηση για να ανιχνευθεί εάν μια διεύθυνση IP έχει αποδοθεί σε άλλη μηχανή

Απρόκλητο ARP (Gratuitous ARP)

- Εάν ο στόχος (TPA) ενός Gratuitous ARP υπάρχει
  - μπορεί να απαντήσει και αυτός Gratuitous ARP
  - για να υπερασπισθεί την IP διεύθυνσή του και
  - να μη μολυνθούν οι πίνακες ARP
- Εάν αμφότεροι οι κόμβοι επιμένουν δημιουργείται αδιέξοδο
  - Οι TCP συνδέσεις τους θα διακόπτονται συνεχώς
- Ανάγκη για μηχανισμό εντοπισμού διπλών διευθύνσεων (Duplicate address detection)
  - ARP Probe

ARP with Duplicated IP Addresses

- Scenario 1: **NodeA_IP_addr=NodeB_IP_addr**
  - Host/Server: IP_addr=Y1 MAC_addr=X1
  - Node A: IP_addr=Y2 MAC_addr=X2
  - Node B: IP_addr=Y2 MAC_addr=X3
  - If Node A connects to Host then Host's ARP cache contains: Y2<-->X2
  - If Node B connects to Host then Host's ARP cache is updated to: Y2<-->X3
  - Eventually traffic from Host destined to Node A goes to Node B that discards it and the traffic is lost

ARP with Duplicated IP Addresses

- Scenario 2: **Host_IP_addr=NodeB_IP_addr**
  - Host: IP_addr=Y1 MAC_addr=X1
  - Node A: IP_addr=Y2 MAC_addr=X2
  - Node B: IP_addr=Y1 MAC_addr=X3
  - If Node A tries to connect to Host then both Host and Node B may reply to Node A's ARP request. Depending on timing and implementation Node A keeps in its ARP cache either the MAC address of Host or Node B.
    - If Host's MAC then everything is ok.
    - If Node B's MAC then there is problem
    - If Node B is off then everything looks ok.
  - The problem may go up and down.

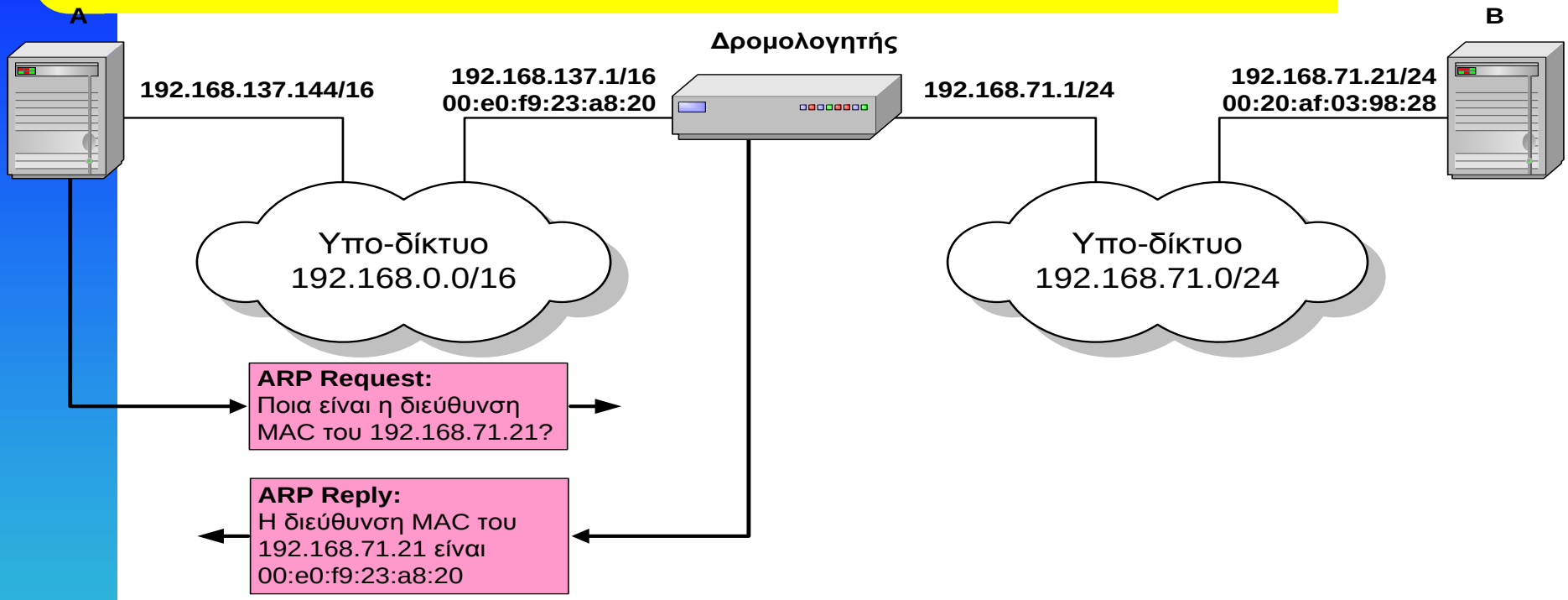
Διερευνητικό ARP (ARP Probe)

- Το ARP Probe διερευνά κατά πόσο μια διεύθυνση IP ήδη χρησιμοποιείται από άλλο host στο LAN
  - χωρίς να μολύνει τους πίνακες ARP!
- Αποστολή ARP Request με διεύθυνση αποστολέα (SPA) την 0.0.0.0
  - SHA: διεύθυνση MAC του αποστολέα
  - SPA: 0.0.0.0
  - THA: 00:00:00:00:00:00
  - TPA: αναζητούμενη διεύθυνση IP

Πληρεξούσιο ARP (Proxy ARP)

- Ένας δρομολογητής μπορεί να λειτουργεί ως πληρεξούσιος (proxy) για πολλές διευθύνσεις IP, απαντώντας εκ μέρους τους
- Απαντά σε ARP Request που φτάνει σε ένα υποδίκτυό του, αλλά απευθύνεται σε υπολογιστή που βρίσκεται σε άλλο υποδίκτυό του, δίνοντας τη δική του διεύθυνση MAC
  - Τυπική χρήση εξυπηρετητή απομακρυσμένης πρόσβασης (RAS - Remote Access Server)

Πληρεξούσιο ARP



- Γιατί ο A στέλνει ARP και δεν προωθεί το πακέτο IP;
  - Για τον A, ο B βρίσκεται στο ίδιο υποδίκτυο με αυτόν, άρα είναι άμεσα προσβάσιμος (χωρίς χρήση δρομολογητή)

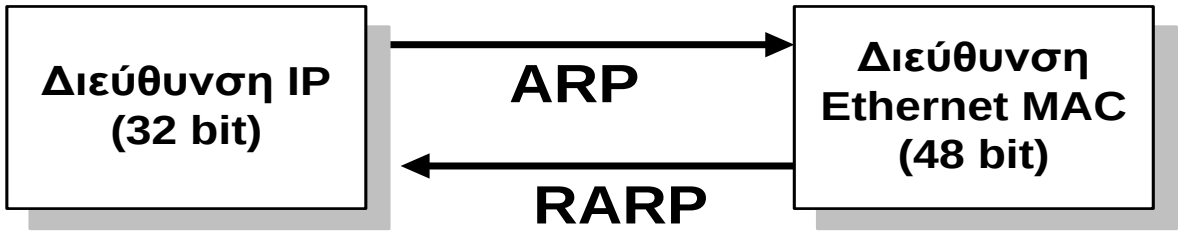
Τρωτά σημεία

- Δεν υπάρχει μηχανισμός πιστοποίησης αυθεντικότητας των αιτήσεων και αποκρίσεων ARP
  - Οι αιτήσεις και απαντήσεις ARP μπορεί να παραποιηθούν
- Το ARP δεν διαθέτει μνήμη κατάστασης
  - ARP Reply μπορεί να σταλούν χωρίς αντίστοιχο ARP Request
- Σύμφωνα με την προδιαγραφή του πρωτόκολλου ARP:
  - Όταν ληφθεί πακέτο ARP (Request ή Reply) ο κόμβος **πρέπει** να ενημερώσει τον τοπικό πίνακα ARP με τη διεύθυνση MAC αποστολέα, εάν έχει εγγραφή για τη διεύθυνση IP του αποστολέα
- Συνήθης εκμετάλλευση αυτών των τρωτών σημείων:
  - Αποστέλλεται παραποιημένο ARP Request ή Reply ώστε να ενημερωθεί ο πίνακας ενός απομακρυσμένου μηχανήματος με μια κίβδηλη εγγραφή (ARP Poisoning)
  - Έτσι η κίνηση IP δρομολογείται προς άλλους host

Πρωτόκολλο RARP

- Ποια είναι η διεύθυνση IP για δοθείσα διεύθυνση Ethernet;
  - π.χ., κατά την εκκίνηση ενός σταθμού εργασίας χωρίς δίσκο (π.χ., X-terminals)
- Πρωτόκολλο αντίστροφης επίλυσης διευθύνσεων, RARP
- Το RARP χρησιμοποιεί εκπομπή στο τοπικό δίκτυο

Λειτουργία



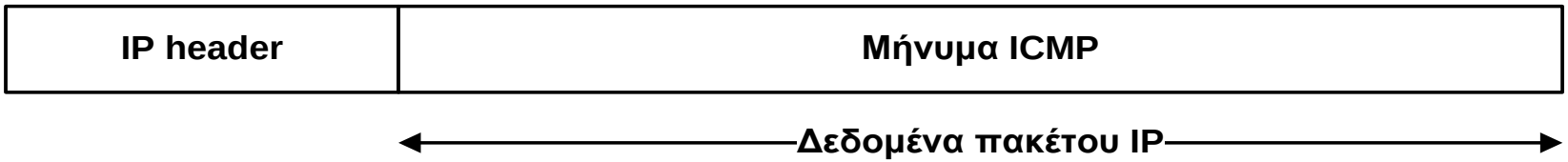
- Λειτουργεί όπως το ARP
- Το πακέτο RARP είναι ίδιο με το ARP
  - Operation: αίτηση RARP (3) ή απάντηση RARP (4)
- Το RARP δεν χρησιμοποιείται πλέον
- Δίνει μόνο διευθύνσεις IP (όχι τον default δρομολογητή ούτε τη μάσκα του υποδικτύου)

Πρωτόκολλα ελέγχου

ICMP

ICMP

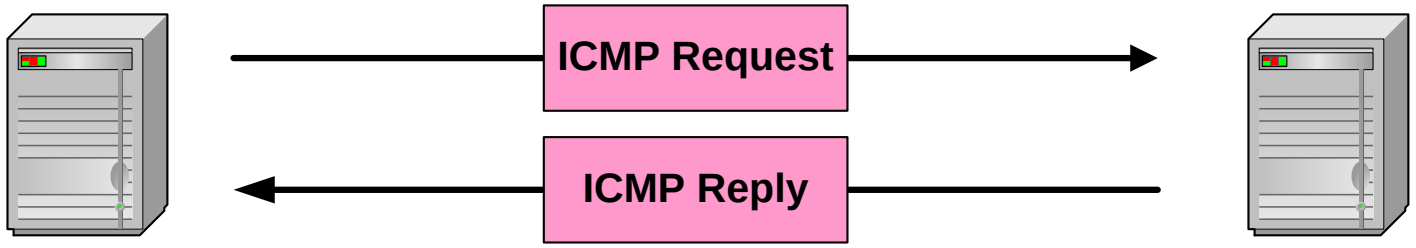
- Το IP δεν παρέχει άμεσους τρόπους που να δείχνουν τι έγινε με τα πακέτα IP
- Απαιτείται μηχανισμός για διαγνωστικούς σκοπούς και αναφορά λαθών
- Το ICMP είναι ένα βοηθητικό (helper) πρωτόκολλο που παρέχει στο IP τη δυνατότητα
  - αναφοράς λαθών (errors)
  - απλών ερωτημάτων (queries)
- Τα μηνύματα ICMP ενθυλακώνονται σε πακέτα IP!
  - Η τιμή στο πεδίο protocol είναι 0x01



Internet Control Message Protocol

- Το ICMP αποτελεί λογικό μέρος του IP, αλλά στην πραγματικότητα ενθυλακώνεται σε πακέτα IP (protocol=1)
- Το ICMP μήνυμα στέλνεται πίσω προς την πηγή του πακέτου που δημιούργησε το πρόβλημα
  - Αναξιόπιστο
- Τα μηνύματα ICMP συνήθως παράγονται και επεξεργάζονται από το λογισμικό IP (λειτουργικό σύστημα) και όχι από τις εφαρμογές χρήστη
- Ορίζεται στο RFC 792

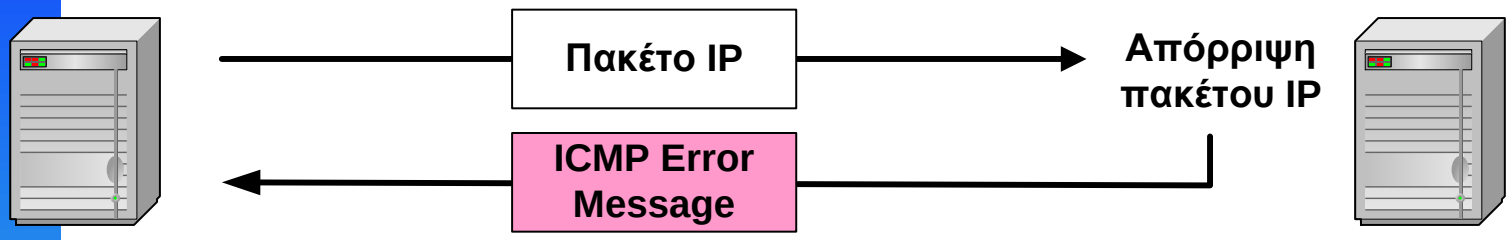
ICMP μηνύματα ερωτήσεων



ICMP query:

- Request αποστέλλεται από υπολογιστή προς δρομολογητή ή άλλο υπολογιστή
- Reply γυρνάει στον υπολογιστή που ερώτησε

ICMP μηνύματα λαθών



- Τα ICMP μηνύματα λαθών αναφέρουν καταστάσεις λάθους
- Συνήθως αποστέλλονται όταν απορρίπτεται κάποιο πακέτο
- Συνήθως περνάνε από το ICMP απ' ευθείας στην εφαρμογή

Περιορισμοί στην παραγωγή μηνυμάτων ICMP

- Τίθενται περιορισμοί για να αποφευχθούν πλημμύρες
- Δεν επιτρέπονται μηνύματα ICMP σε απάντηση:
  - Μηνυμάτων λάθους ICMP (ok για queries)
  - Πακέτων IP που δεν τηρούν τους κανόνες για την επικεφαλίδα
    - Αρκετό μήκος πλαισίου
    - σωστό IP checksum
  - IP πακέτων εκπομπής ή πολλαπλής διανομής
  - Άκυρης διεύθυνσης πηγής
  - Θραυσμάτων πλην του πρώτου

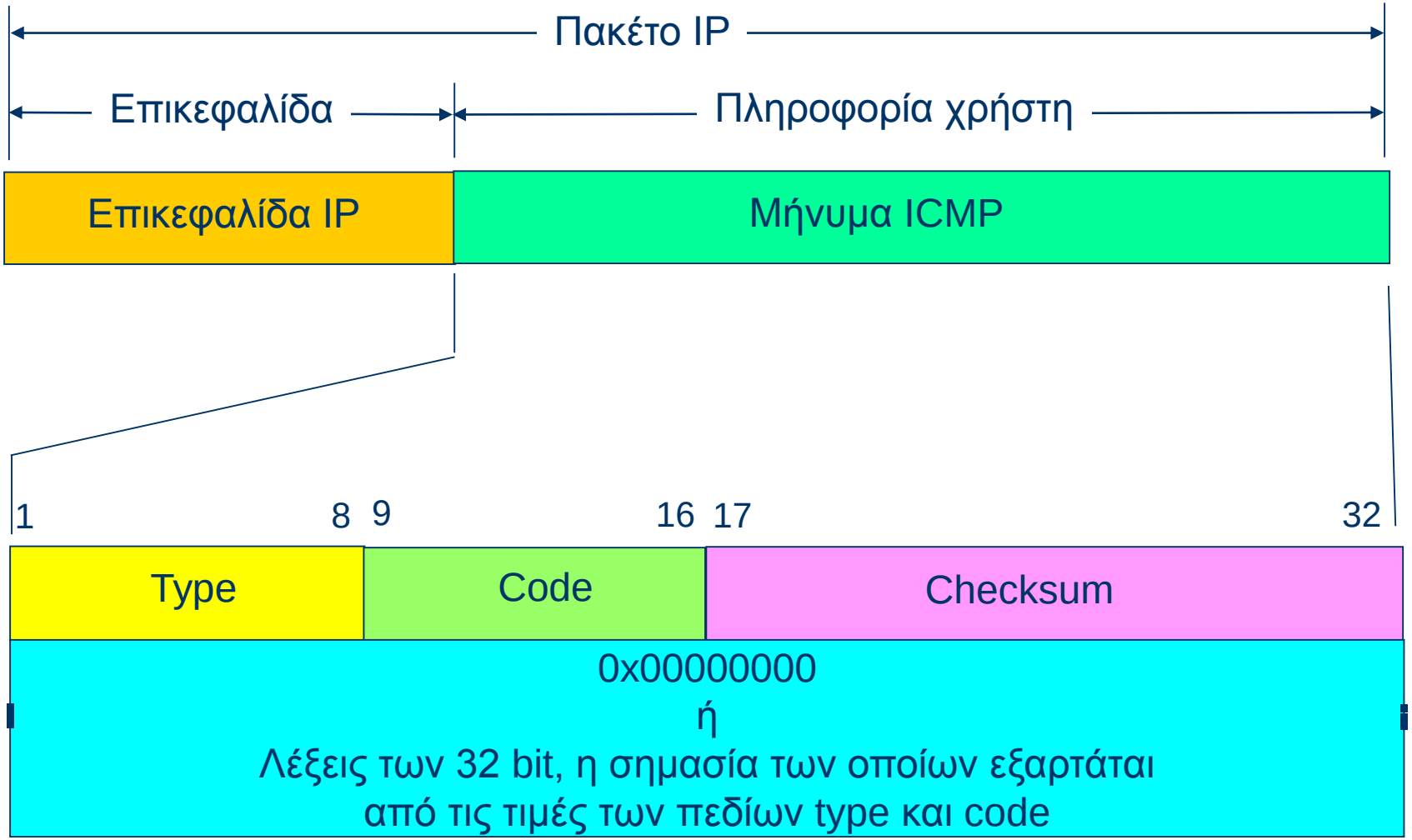
Τύποι μηνυμάτων ICMP

- Μορφή μηνύματος ICMP:
  type, code, checksum, δεδομένα

- Type: 15 τύποι μηνυμάτων
- Code: δείχνει ειδικού υπο-τύπους
- Checksum: καλύπτει όλο το μήνυμα ICMP
- Δεδομένα: ανάλογα με τις τιμές των πεδίων type και code
  - Εάν δεν υπάρχουν δεδομένα τότε 4 byte τίθενται στο 0

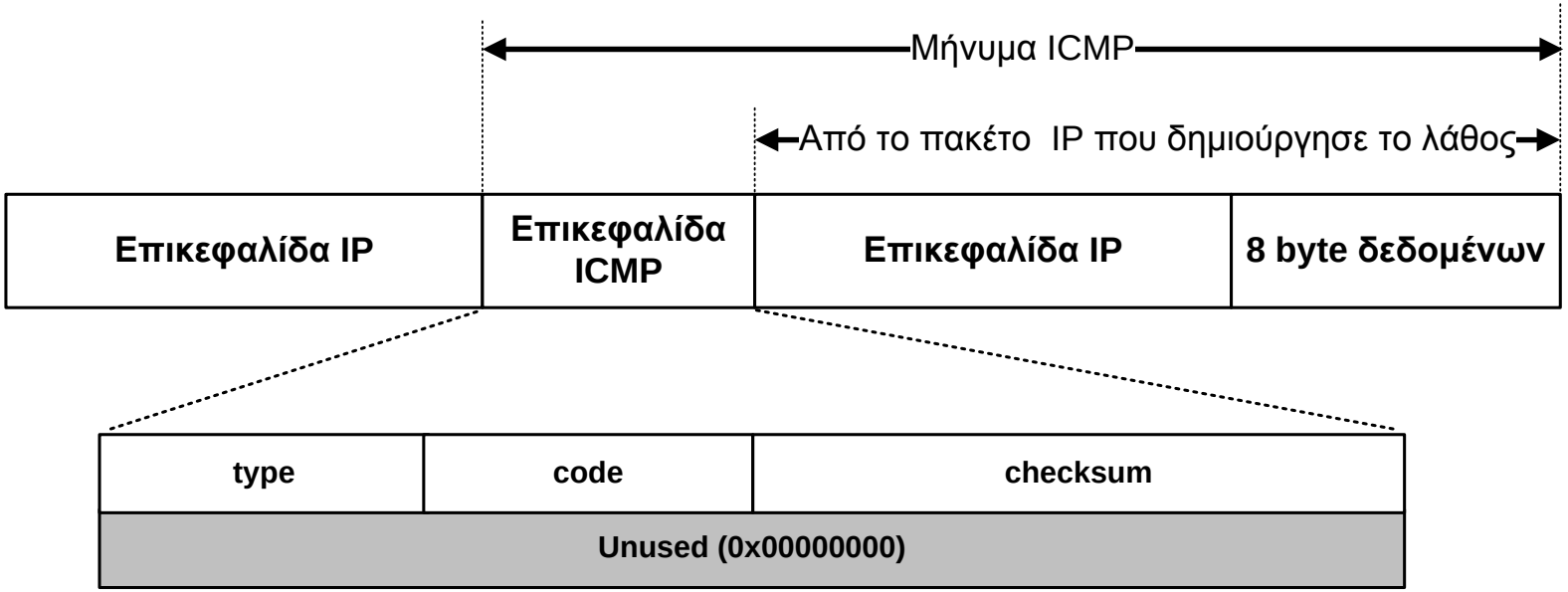
  → το μήνυμα ICMP έχει ελάχιστο μήκος 8 byte

Μορφή μηνύματος ICMP



ICMP μηνύματα λάθους

Μορφή μηνύματος λάθους ICMP



Μορφή μηνύματος λάθους ICMP

- Ιστορικά, τα μηνύματα λάθους ICMP επέστρεφαν την επικεφαλίδα IP του πακέτου που δημιούργησε το λάθος και τα πρώτα 8 byte δεδομένων
  - Δεν επαρκεί σήμερα για πιο πολύπλοκες περιστάσεις, όπως IP σε IP
- Οι νέοι κανόνες: θα περιλαμβάνει το περισσότερο δυνατό, χωρίς το μήκος του πακέτου ICMP > 576 byte (το επίσημο μήκος πακέτου στο Internet)

Συνήθη μηνύματα λάθους ICMP

Type	Code	περιγραφή
3	0-15	απρόσιτος προορισμός (destination unreachable)
4		σιγή πηγής (source quench)
5	0-3	παράκαμψη (redirect)
11	0,1	λήξη χρόνου (time exceeded)
12	0,1	πρόβλημα με παραμέτρους (parameter problem)

ICMP Destination Unreachable (Type=3)

Ειδοποίηση ότι το πακέτο IP δεν προωθήθηκε και απορρίφθηκε

Type=3	Code	Checksum
Unused=0		
(copy of packet)		

Το πεδίο Code περιέχει την εξήγηση

Code	περιγραφή
0	απρόσιτο δίκτυο προορισμού (ο δρομολογητής δεν έχει διαδρομή προς τα εκεί: δεν έχει εγγραφή στον πίνακα δρομολόγησης)

ICMP Destination Unreachable (Type=3)

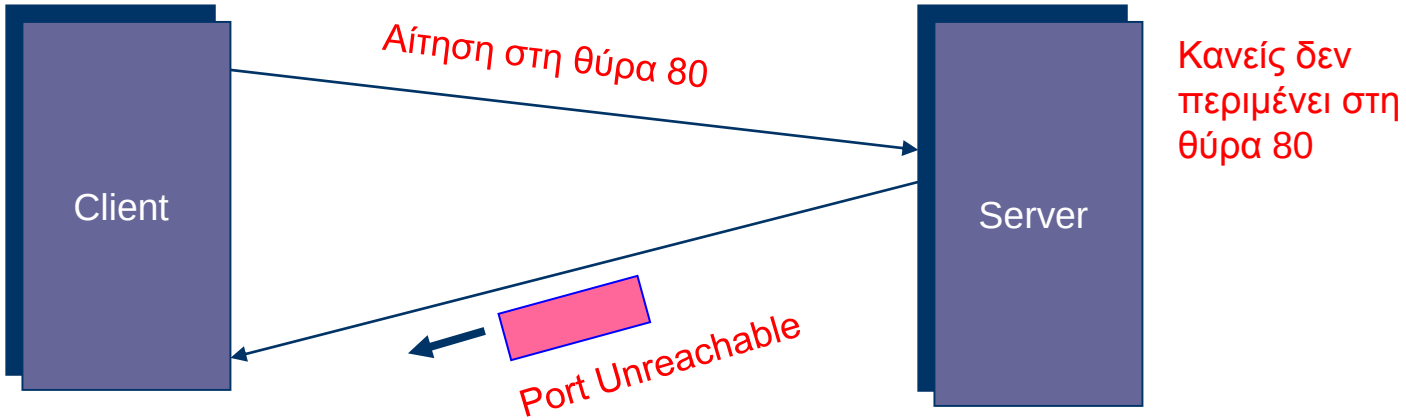
1 απρόσιτος host προορισμού
(ο τελευταίος δρομολογητής δεν μπορεί να φτάσει τον host: ο host έπρεπε να είναι άμεσα προσβάσιμος, αλλά δεν απαντά σε ARP)

2 απρόσιτο πρωτόκολλο προορισμού
(ο host δεν διαθέτει το πρωτόκολλο στρώματος 4: το πρωτόκολλο στο πεδίο Protocol της επικεφαλίδας IP δεν υποστηρίζεται από τον προορισμό)

3 απρόσιτη θύρα προορισμού
(το πρωτόκολλο μεταφοράς στον προορισμό δεν μπορεί να προωθήσει το πακέτο: η θύρα δεν έχει προσδεμένη διεργασία - Συνήθως UDP)

ICMP Destination Unreachable

- RFC 792: Εάν στον προορισμό το IP δεν μπορεί να παραδώσει το πακέτο επειδή το υποδεικνυόμενο πρωτόκολλο δεν είναι ενεργό, ο προορισμός μπορεί να στείλει στην πηγή το μήνυμα ICMP destination unreachable
- Παράδειγμα:



ICMP Destination Unreachable (Type=3)

Code	περιγραφή
4	απαιτείται θρυμματισμός, αλλά το DF bit = 1 [μπορεί να επιστρέφει μια τιμή MTU στην αχρησιμοποίητη 2η λέξη] Ο host μπορεί να αλλάξει το μέγεθος του πακέτου ώστε να αποφευχθεί ο θρυμματισμός χρησιμοποιώντας αυτή την τιμή της MTU ή άλλη συνήθη τιμή (path MTU discovery)
6	άγνωστο δίκτυο προορισμού
7	άγνωστος host προορισμού
11	απρόσιτο δίκτυο για τον τύπο υπηρεσίας
12	απρόσιτος host για τον τύπο υπηρεσίας

- Ορίζονται και άλλοι κωδικοί στο RFC 1122

ICMP Redirect (Type=5)

Πληροφορεί για την ύπαρξη εναλλακτικής διαδρομής και οδηγεί σε ενημέρωση του πίνακα δρομολόγησης

- Από δρομολογητή προς host: Οι δρομολογητές υποτίθεται ότι ξέρουν τις σωστές διαδρομές
- Δείχνει ότι χρησιμοποιείται λάθος δρομολογητής για το πρώτο βήμα
- Η παράκαμψη δείχνει τον σωστό δρομολογητή

Type=5	Code	Checksum
IP address of router		
(copy of packet)		

Το πεδίο Code περιέχει τον λόγο αλλαγής της διαδρομής

Code	περιγραφή
0	παράκαμψη για το δίκτυο (obsolete)
1	παράκαμψη για τον host
2	παράκαμψη για τον τύπο υπηρεσίας και δίκτυο
3	παράκαμψη για τον τύπο υπηρεσίας και host

ICMP Time Exceeded (Type=11)

Στέλνεται από τον δρομολογητή που απορρίπτει πακέτο επειδή το TTL μηδενίσθηκε ή όταν ο χρόνος εξέπνευσε περιμένοντας κάποιο θραύσμα

Type=11	Code	Checksum
Unused=0		
(copy of packet)		

Code	περιγραφή
0	εκπνοή μετρητή TTL (η traceroute χρησιμοποιεί επωφελώς αυτή την ένδειξη λάθους)
1	εκπνοή χρόνου συναρμολόγησης

ICMP Parameter Problem (Type=12)

- Γενικής χρήσης για λάθη που δεν καλύπτονται αλλιώς
- Αποστέλλεται όταν η επικεφαλίδα IP δεν είναι έγκυρη ή όταν λείπει μια προαιρετική επιλογή (option)

Type=12	Code	Checksum
Pointer	Unused=0	
(copy of packet)		

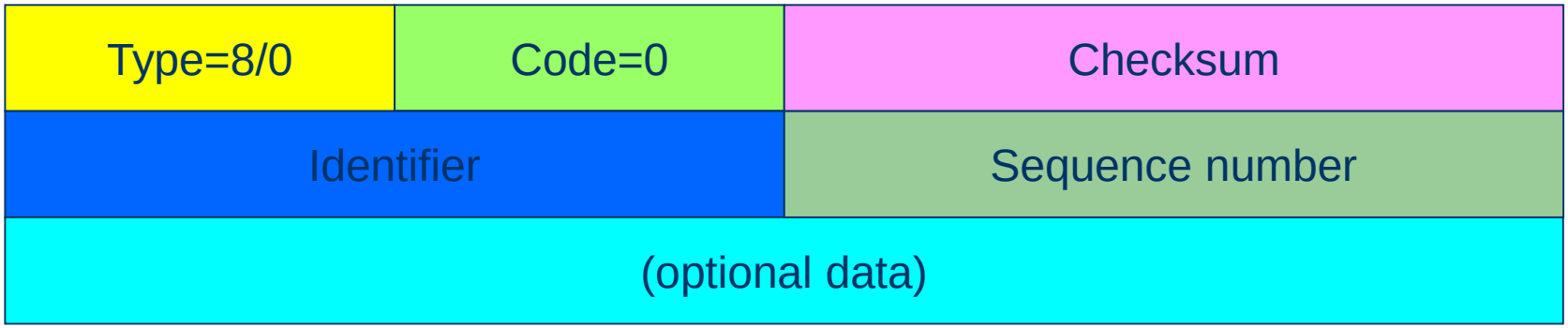
Code	περιγρφή
0	μη έγκυρη επικεφαλίδα (ο pointer δείχνει την απόσταση του byte όπου εμφανίζεται το λάθος σε σχέση με την αρχή της επικεφαλίδας IP)
1	λείπει υποχρεωτική επιλογή της επικεφαλίδας (ο pointer δεν χρησιμοποιείται)

ICMP μηνύματα ερώτησης

Συνήθη ICMP μηνυμάτα ερώτησης

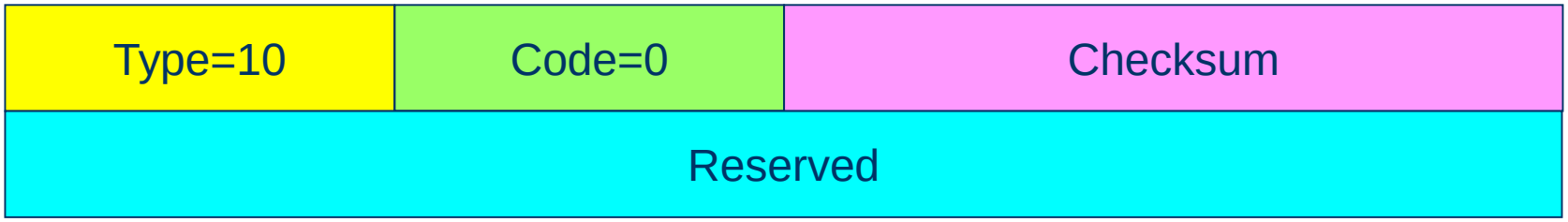
Type	περιγραφή
0	απάντηση ηχούς (echo reply - ping)
8	αίτηση ηχούς (Echo request - ping)
9	διαφήμιση δρομολογητή (router advertisement)
10	αναζήτηση δρομολογητή (router solicitation)
13	αίτηση χρονικής σφραγίδας (Time Stamp Request)
14	απάντηση χρονικής σφραγίδας (Time Stamp Reply)
15	αίτηση πληροφορίας (Information request) obsolete
16	απάντηση πληροφορίας (Information reply) obsolete
17	αίτηση μάσκας δικτύου (Address Mask Request)
18	απάντηση μάσκας δίκτυο (Address Mask Reply)

ICMP Echo request/reply (Type=8/0)



- Συνήθως χρησιμοποιείται ως σύντομος τρόπος εξακρίβωσης της ύπαρξης σύνδεσης ("πρόγραμμα ping").
- Επίσης μπορεί να δείξει απώλειες, αντίγραφα και αλλαγές σειράς (με χρήση του sequence number)
- Ο Identifier επιτρέπει το ταίριασμα των αιτήσεων με τις απαντήσεις
- Optional data είναι δεδομένα μεταβλητού μήκους που επιστρέφονται στον αποστολέα

ICMP Router Solicitation (Type=10)



- Συνήθως στέλνεται από host (κατά τη διάρκεια της εκκίνησης) για να βρει κοντινούς δρομολογητές
- Ο δρομολογητής που το λαμβάνει απαντά με Router Advertisement
- Μπορεί να περιέχει τη διεύθυνση αποστολής 0.0.0.0
- Εάν υποστηρίζεται πολλαπλή διανομή στέλνεται στο 224.0.0.2 [όλοι οι δρομολογητές]
- Αλλιώς, τοπική εκπομπή (όλα 1)

ICMP Router Advertisement (Type=9)

Type=12	Code=0	Checksum
Num addrs	Addr size	Lifetime
Router address 1		
Preference Level 1		
…		

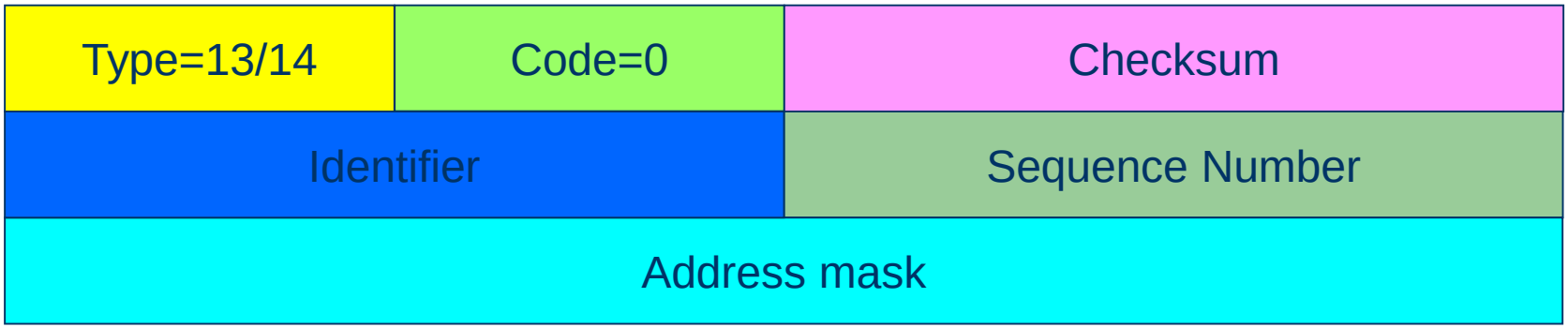
- Στέλνεται από δρομολογητές περιοδικά για να υποδειχθούν διαδρομές.
- Χρήσιμο για να βρεθεί ο default router όταν υπάρχουν τουλάχιστον δύο δρομολογητές [σήμερα το DHCP είναι πιο δημοφιλές]
- Στέλνεται στο 224.0.0.1 [όλα τα συστήματα] ή με τοπική εκπομπή
- Το Num addrs δίνει το πλήθος των μπλοκ διευθύνσεων που ακολουθούν
- Το Addr size δίνει το μέγεθος της διεύθυνσης (1 για IPv4)
- Το Lifetime είναι η διάρκεια σε sec που η πληροφορία είναι έγκυρη (συνήθως 30 min)
- Ο host διαλέγει τη διεύθυνση με το μεγαλύτερο preference level

ICMP Timestamp Request/Reply (Type=13/14)

Type=13/14	Code=0	Checksum
Identifier		Sequence Number
Originate timestamp		
Receive timestamp		
Transmit timestamp		

- Χρησιμοποιείται για συγχρονισμό των ρολογιών και εκτίμηση του χρόνου διαδρομής
- Χρόνοι σε msec από τα μεσάνυχτα UTC
- Originate timestamp: αμέσως πριν σταλεί από την πηγή
- Receive timestamp : μόλις το έλαβε ο παραλήπτης
- Transmit timestamp : αμέσως πριν σταλεί από τον παραλήπτη

ICMP Address Mask Request/Reply (Type=17/18)



- Χρησιμοποιείται για να βρεθεί η μάσκα του υποδικτύου με ICMP
- Ο host μπορεί να το στείλει κατά την εκκίνηση (σε γνωστό δρομολογητή ή εκπομπή με αποστολέα 0.0.0.0)
- Συνήθως σήμερα χρησιμοποιείται το DHCP

Πρωτόκολλα ελέγχου

ICMPv6

ICMPv6

- Το ICMPv6 είναι η υλοποίηση του ICMP για το IPv6
- Αποτελεί κεντρικό μέρος του πρωτοκόλλου IPv6
- Ενθυλακώνεται σε πακέτα IPv6 όπου η τιμή Next Header=58
- Ενσωματώνει λειτουργίες:
- Neighbor Discovery Protocol (NDP)
  - που αντικαθιστούν το πρωτόκολλο ARP
- Multicast Listener Discovery (MLD)
  - που αντικαθιστούν το πρωτόκολλο IGMP

ICMPv6

- Το ICMPv6 περιλαμβάνει μηνύματα λάθους και μηνύματα πληροφόρησης
- Διαθέτει μηχανισμούς για μελλοντικές επεκτάσεις
- Η μορφή της επικεφαλίδας ICMPv6 είναι ίδια με αυτή του ICMPv4

  type, code, checksum, δεδομένα

  όπου τα δεδομένα εξαρτώνται από το συγκεκριμένο μήνυμα ICMPv6
- Πολλά από τα μηνύματα είναι ίδια με το ICMPv4, παρότι οι τιμές των πεδίων type και code είναι διαφορετικές

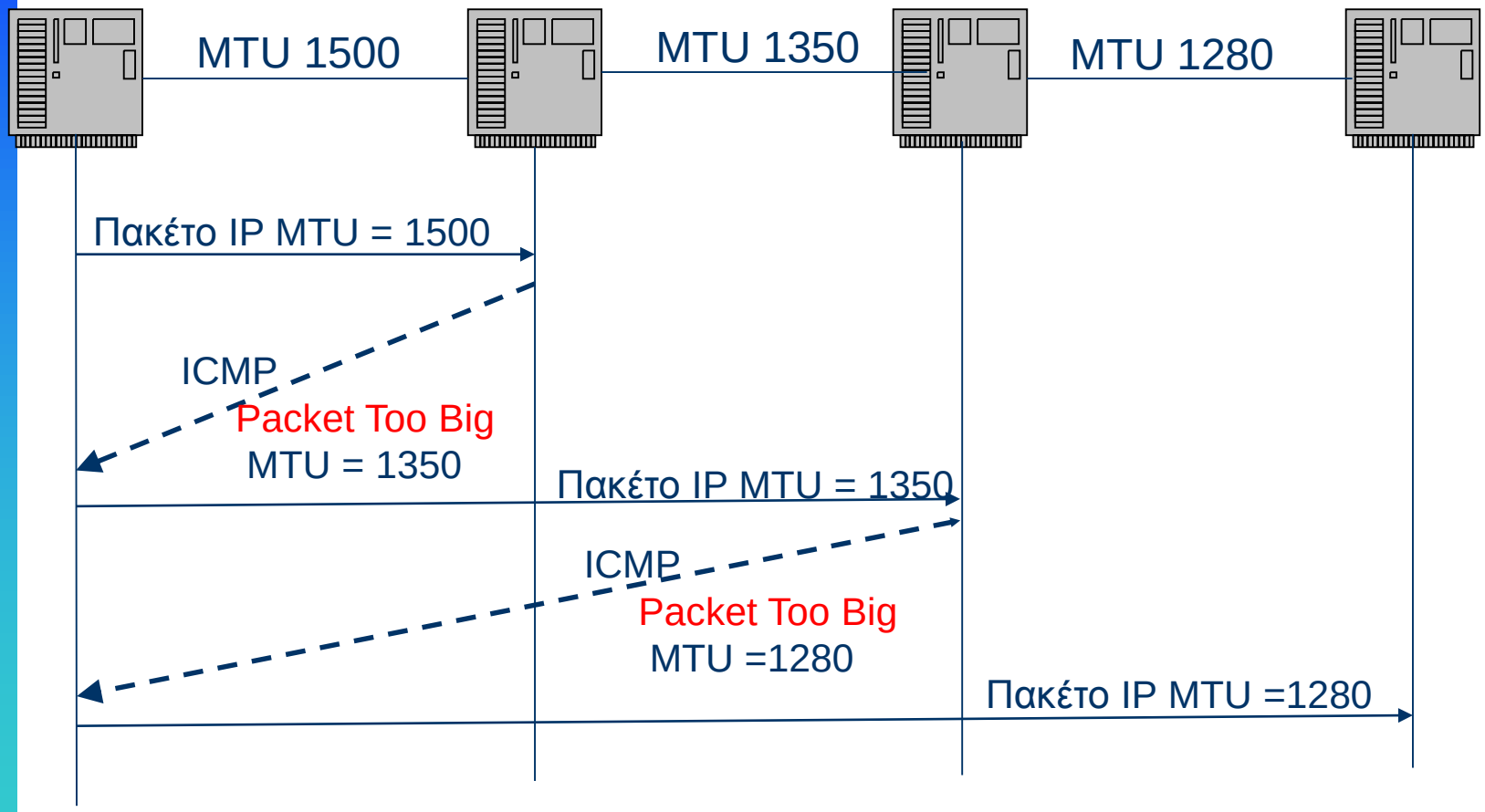
Μηνύματα λάθους ICMPv6

IPv6	IPv4
Destination Unreachable	Destination Unreachable
Time exceeded	Time exceeded
Packet too big	-

Ανακάλυψη MTU διαδρομής

- Στο IPv6 μόνο η πηγή μπορεί να θρυμματίσει πακέτα
  - Όχι οι δρομολογητές
- Η πηγή πρέπει να προσδιορίσει επομένως τη ζεύξη με την μικρότερη MTU κατά μήκος της διαδρομής
  - Η πηγή στέλνει πακέτα μεγέθους όσο επιτρέπει η MTU της ζεύξης της
  - Εάν ένα πακέτο είναι πολύ μεγάλο για να προωθηθεί, ο ενδιάμεσος δρομολογητής στέλνει στην πηγή το μήνυμα packet too big που περιλαμβάνει την τιμή της MTU της προβληματικής ζεύξης
  - Η πηγή μειώνει την MTU της διαδρομής στην υποδεικνυόμενη τιμή
  - Η διαδικασία μπορεί να επαναληφθεί όσες φορές χρειαστεί
  - Η πηγή δεν στέλνει με MTU μικρότερη από 1280

Ανακάλυψη ελάχιστης MTU



Μηνύματα πληροφόρησης ICMPv6

IPv6	IPv4
Echo Reply	Echo Reply
Echo Request	Echo Request
Neighbor Solicitation (NS)	ARP Request
Neighbor Advertisement (NA)	ARP Reply
Router Solicitation (RS)	Router Solicitation
Router Advertisement (RA)	Router Advertisement
Redirect	Redirect

Ανακάλυψη γειτόνων

- Τα μηνύματα RS, RA και Redirect έχουν παρόμοια χρήση με τα αντίστοιχα του ICMPv4
- Τα μηνύματα NS και NA χρησιμοποιούνται αντί του ARP
- Οι πληροφορίες που μεταφέρουν χρησιμεύουν επιπλέον και για
  - Αυτο-ρύθμιση (autoconfiguration) διευθύνσεων IPv6
  - Προσδιορισμό παραμέτρων (π.χ, MTU)
  - Προσδιορισμό μη προσβάσιμων κόμβων:
    Neighbor unreachability detection (NUD)
  - Προσδιορισμό χρησιμοποιούμενων διευθύνσεων:
    Duplicate address detection (DAD)

  σε μια διαδικασία γνωστή ως πρωτόκολλο ανακάλυψης γειτόνων NDP (Neighbor Discovery Protocol) που αποτελεί μέρος του ICMPv6

Δυναμική εκχώρηση διευθύνσεων IP

RARP, BOOTP, DHCP

Πώς παίρνει ένας host διεύθυνση IP;

- Η διεύθυνση που εκχωρείται από τον διαχειριστή καταγράφεται σε αρχείο ή παραμέτρους του λειτουργικού συστήματος
- Λαμβάνεται μέσω δυναμικής εκχώρησης

Δυναμική εκχώρηση διευθύνσεων IP

- Η δυναμική εκχώρηση διευθύνσεων IP είναι επιθυμητή για πολλούς λόγους:
  - Οι διευθύνσεις IP αποδίδονται όταν ζητηθούν
  - Αποφεύγεται η χειροκίνητη διάρθρωση του IP
  - Υποστηρίζεται η κινητικότητα των υπολογιστών (laptops, tablets, κλπ)
- Τρία πρωτόκολλα:
  - RARP (μέχρι 1985, δεν χρησιμοποιείται πια)
  - BOOTP (1985-1993)
  - DHCP (από 1993)
- Σήμερα χρησιμοποιείται ευρέως το DHCP

Εκκίνηση (Bootstrapping)

- Ο υπολογιστής εκκινεί με ένα απλό πρόγραμμα (boot program)
- Το πρόγραμμα boot φορτώνει το λειτουργικό σύστημα
  - Σε μηχανές χωρίς δίσκο (diskless), ο υπολογιστής χρειάζεται τη διεύθυνση IP του εξυπηρετητή όπου βρίσκεται η εικόνα του λειτουργικού συστήματος
- Χρειάζεται τη δικιά του διεύθυνση IP
- Γνωρίζει μόνο τη δικιά του φυσική διεύθυνση

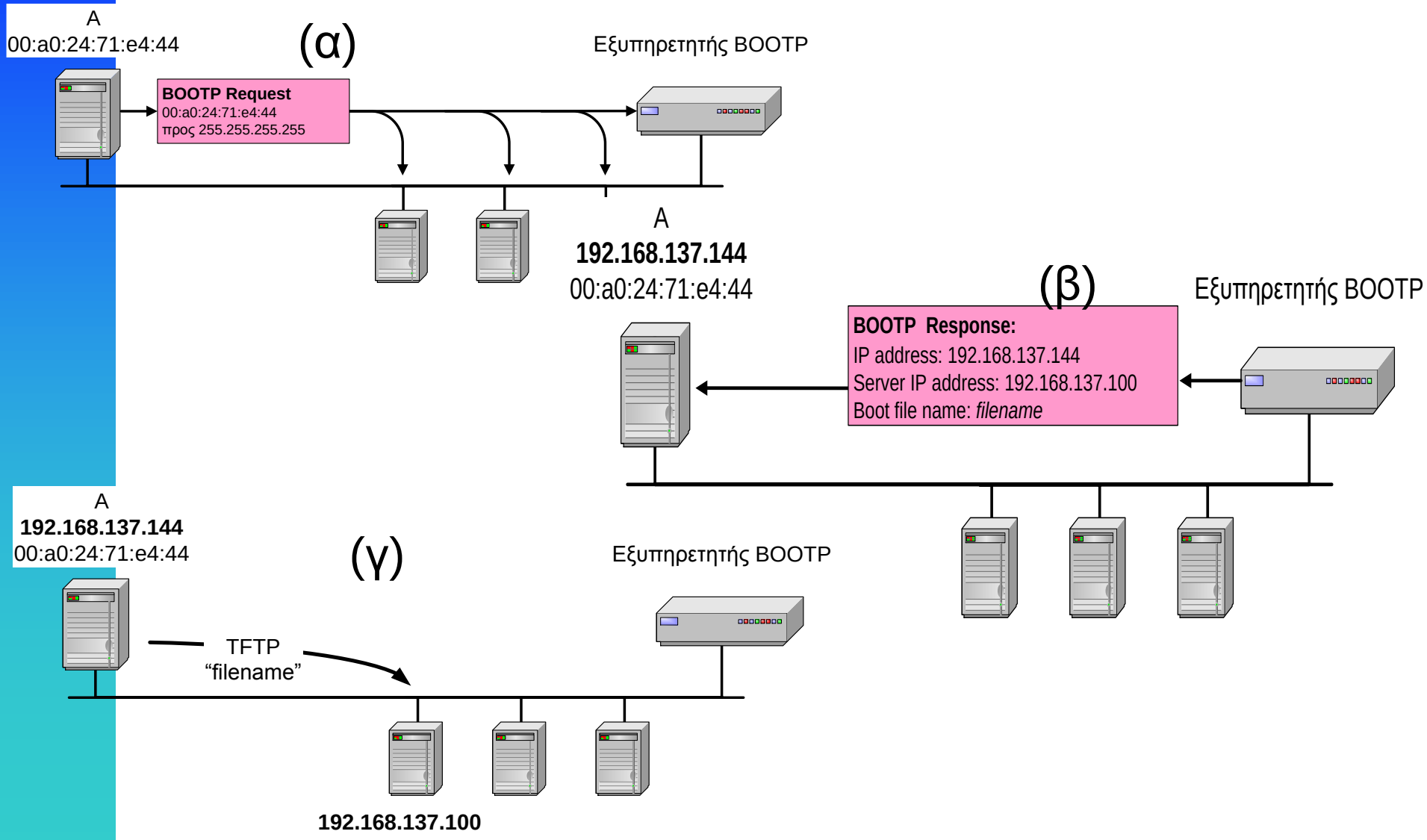
Μια λύση

- Reverse ARP: Ποια είναι η διεύθυνση IP για τη φυσική διεύθυνση xx:xx:xx:xx:xx:xx;
- ICMP: Ποια είναι η μάσκα του υποδικτύου;
- ICMP: Ποιος είναι ο default δρομολογητής;
- Πρόβλημα: Που είναι το αρχείο για τη διεύθυνση IP nnn.nnn.nnn.nnn;

BOOTP (Bootstrap Protocol)

- Το πρωτόκολλο εκκίνησης (bootstrap) BOOTP χρησιμοποιεί μηνύματα UDP
- Ο υπολογιστής μπορεί να προσδιορίσει τις παραμέτρους IP κατά την εκκίνηση
- Διαχωρισμός της διάρθρωσης (configuration) από το φόρτωμα (download) αρχείων
- Τρεις υπηρεσίες:
  - Εκχώρηση διεύθυνσης IP
  - Εύρεση της διεύθυνσης IP του εξυπηρετητή BOOTP
  - Προσδιορισμός ονόματος του αρχείου που θα φορτώσει και εκτελέσει ο πελάτης (boot file name)

Λειτουργία BOOTP



BOOTP

- Η απάντηση στην αίτηση BOOTP δεν εκχωρεί μόνο τη διεύθυνση IP, προσδιορίζει επίσης τον Default Router και τη μάσκα υποδικτύου
- Χρησιμοποιεί δεδομενογράμματα UDP
  - UDP Port 67 (server)
  - UDP Port και 68 (host)
  - με διευθύνσεις εκπομπής (255.255.255.255)
    - Αυτές οι διευθύνσεις δεν προωθούνται

BOOTP

- Η boot image λαμβάνεται με το πρόγραμμα TFTP (Trivial File Transfer Protocol)
- Η αντιστοίχιση διευθύνσεων IP είναι στατική!
- Πρόβλημα: Γιατί να χάνεται μια διεύθυνση που δεν χρησιμοποιείται;

Dynamic Host Configuration Protocol

- Επιτρέπει σε κάποιο host, όταν εκκινεί, να αποκτήσει δυναμικά από εξυπηρετητή του δικτύου την IP διεύθυνσή του, τη μάσκα υποδικτύου, τον default gateway, τον εξυπηρετητή DNS, κ.α.,
  - Μέσω του DHCP οι host μπορούν να μοιράζονται μια ομάδα διευθύνσεων IP
  - Οι διευθύνσεις μπορούν να ξαναχρησιμοποιηθούν, αφού δίδονται στον host όταν εισέρχεται στο δίκτυο και διατηρούνται μόνο όσο είναι συνδεδεμένος
  - Μπορεί να υποστηριχθεί κινητικότητα των host

Πρωτόκολλο DHCP

- Επέκταση του BOOTP (πολλές ομοιότητες)
  - Σχεδιάσθηκε το 1993
  - Χρησιμοποιεί τις ίδιες πόρτες με το BOOTP
  - Επεκτάσεις:
    - Υποστηρίζει προσωρινές εκχωρήσεις ("δάνεια") διευθύνσεων IP
    - Ο πελάτης DHCP μπορεί να λάβει όλες τις σχετικές με το IP παραμέτρους
  - Το DHCP είναι ο προτιμώμενος μηχανισμός
  - Το DHCP υποστηρίζει και πελάτες BOOTP

Πρωτόκολλο DHCP

- Οι εξυπηρετητές DHCP διαθέτουν ομάδες διευθύνσεων IP
- Το DHCP επιτρέπει τον δανεισμό διευθύνσεων IP για κάποιες χρονικές περιόδους
- Όταν το δάνειο λήξει, ο εξυπηρετητής μπορεί να την ξαναδανίσει
  - Τα δάνεια ανανεώνονται όταν παρέλθει το 50% της χρονικής τους διάρκειας

Λειτουργία DHCP

Συνοπτική λειτουργία DHCP:

- ο host εκπέμπει το μήνυμα DHCP discover
- ο εξυπηρετητής DHCP απαντά με DHCP offer
- ο host ζητά διεύθυνση IP με το DHCP request
- ο εξυπηρετητής DHCP στέλνει διεύθυνση με DHCP ack

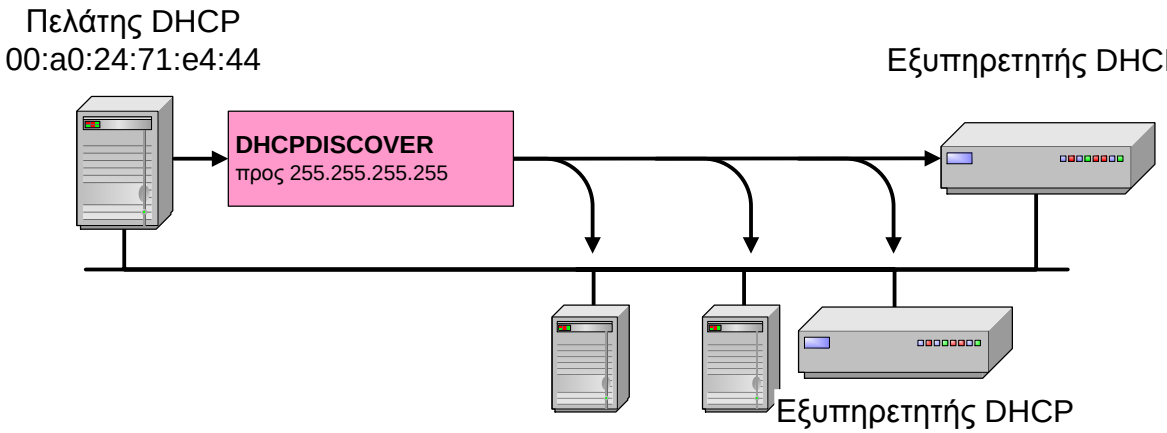
Λειτουργία DHCP (συν)

- Μόλις ο host εκκινήσει εκπέμπει ένα μήνυμα *discover*
- Οι εξυπηρετητές DHCP απαντούν με το μήνυμα *offer* που ορίζει διευθύνσεις IP
- Ο host επιλέγει μία και εκπέμπει την αίτηση *request* προς τον εξυπηρετητή
- Όλοι οι άλλοι εξυπηρετητές αποχωρούν και ο επιλεχθείς εξυπηρετητής στέλνει *ack*

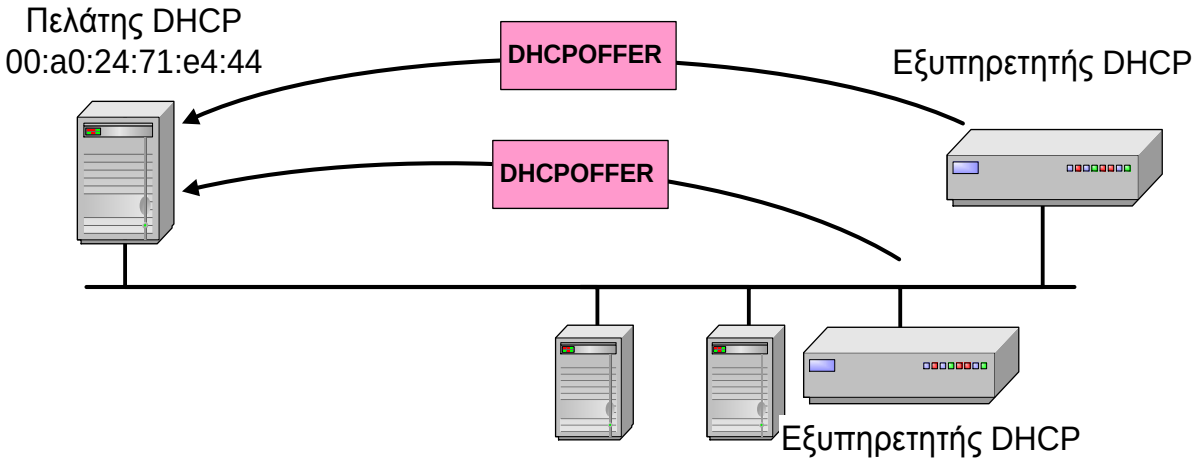
Λειτουργία DHCP (συν)

- Η διεύθυνση IP παραχωρείται με δάνειο για συγκεκριμένο χρονικό διάστημα
  - Ο host αρχίζει να την χρησιμοποιεί μόλις λάβει το *ack*
- Ο host πρέπει να ανανεώσει το δάνειο με μήνυμα *request* προτού λήξει ο χρόνος
  - στέλνεται μόλις περάσει το 50% του χρόνου
- Όταν ο host τελειώσει στέλνει ένα *release*
- Ο εξυπηρετητής επαναχρησιμοποιεί διευθύνσεις IP
  - όταν το δάνειο λήξει
  - λάβει *release*

Λειτουργία DHCP (λεπτομέρειες)

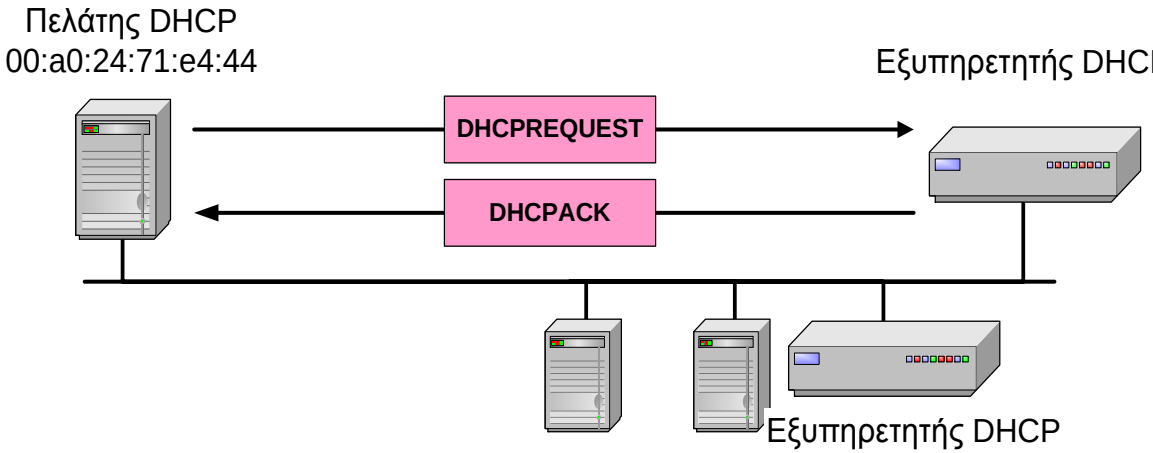


Ανακάλυψη

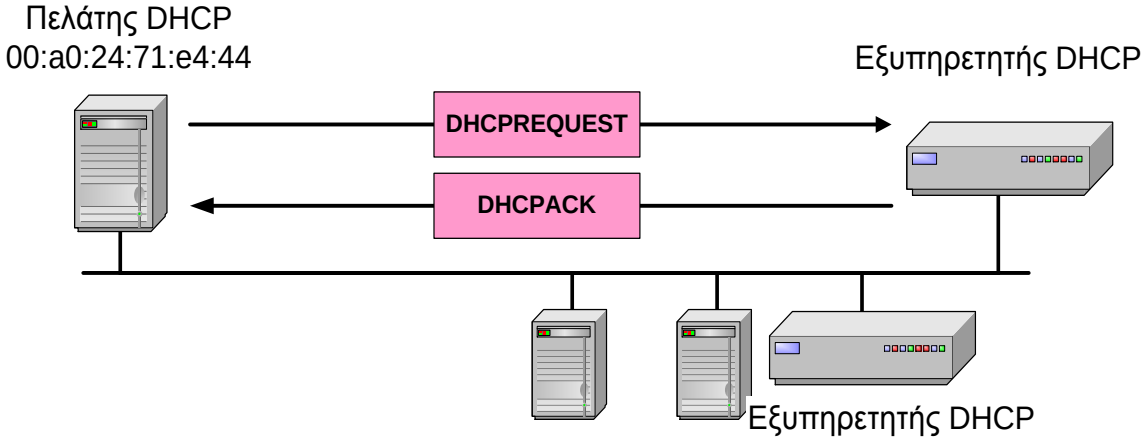


Προσφορές

Λειτουργία DHCP (λεπτομέρειες)

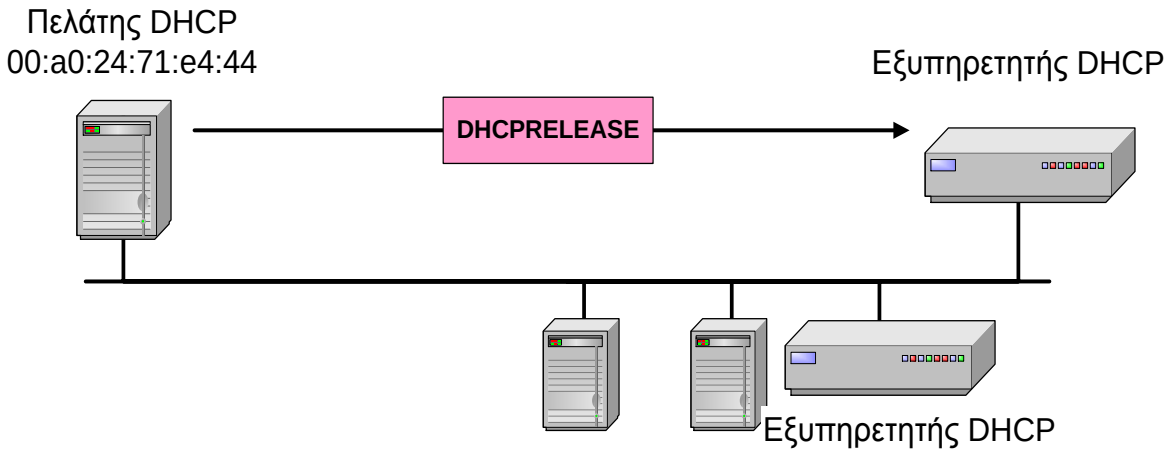


Αίτηση για “δάνειο”



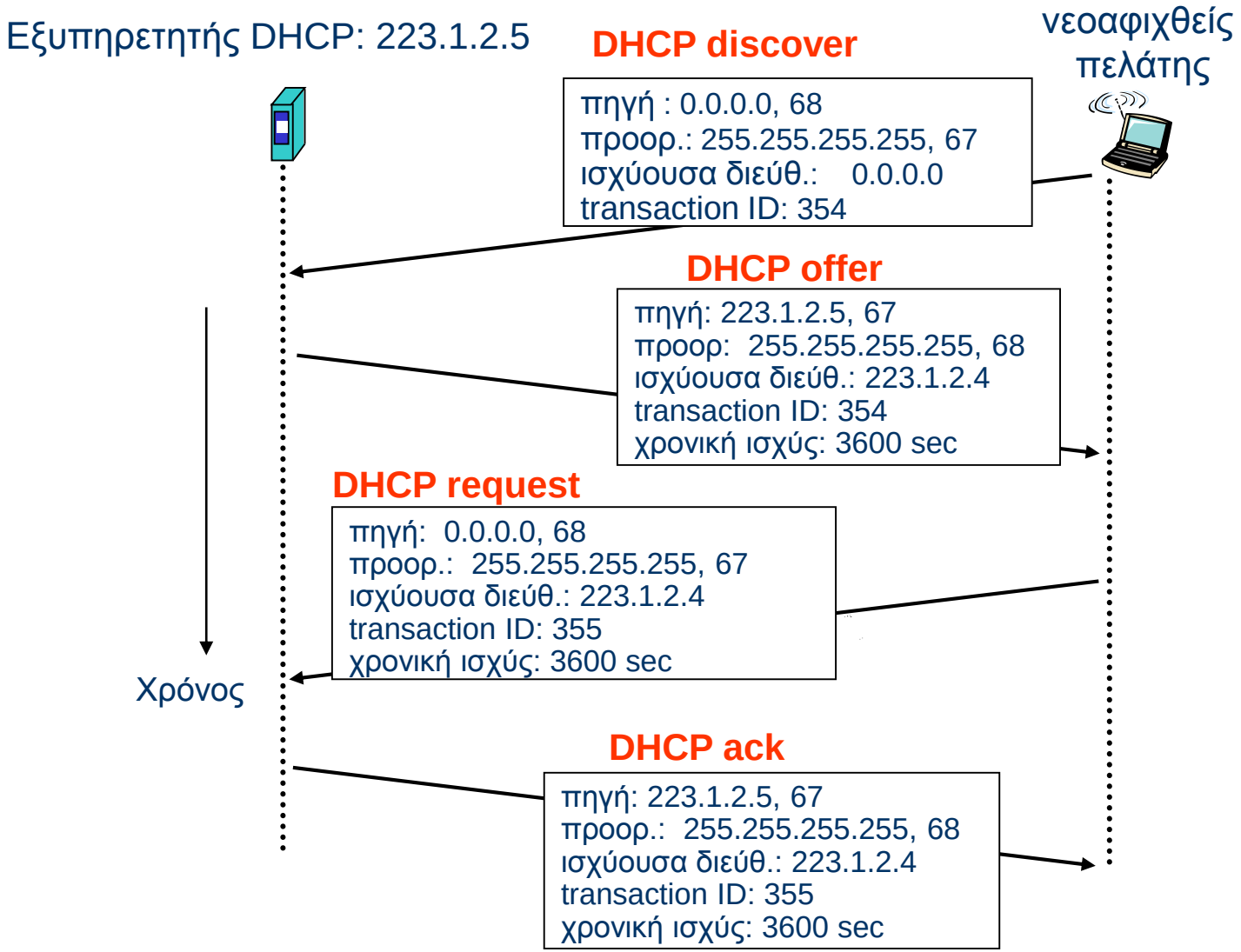
Ανανέωση “δανείου”

Λειτουργία DHCP (λεπτομέρειες)



Λήξη “δάνειου”

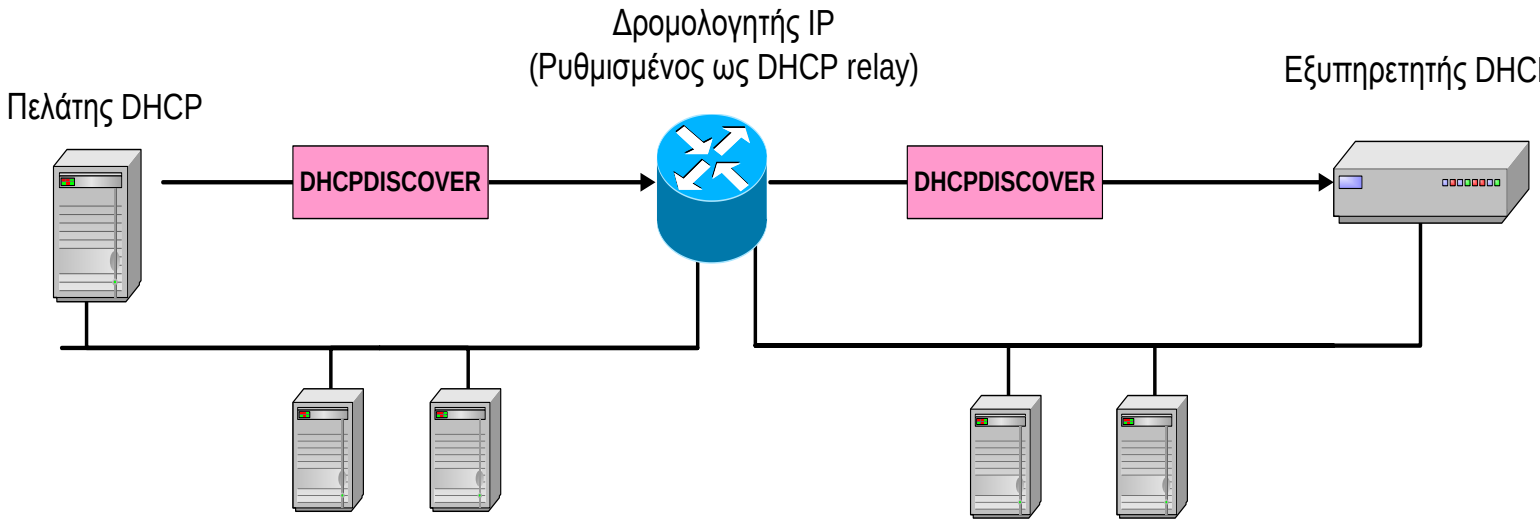
Παράδειγμα χρήσης DHCP



Εκπομπή ή όχι

- Η όλη διαδικασία μπορεί να γίνει με χρήση εκπομπής
- Συχνά χρησιμοποιείται μονοεκπομπή (unicast)
  - Όταν ο πελάτης DHCP γνωρίζει τη διεύθυνση του εξυπηρετητή DHCP
  - Ο πελάτης μπορεί να ζητήσει απάντηση unicast από τον εξυπηρετητή εάν θέσει στο μηδέν την broadcast flag (ο εξυπηρετητής μπορεί να το αγνοήσει)
  - Ο εξυπηρετητής μπορεί να στείλει unicast στον πελάτη που δεν έχει ακόμη αποκτήσει διεύθυνση IP προσθέτοντας εγγραφή ARP με τη διεύθυνση MAC του πελάτη και την επιλεχθείσα διεύθυνση IP

Αναμετάδοση DHCP (DHCP Relay)



- Πελάτης και εξυπηρετητής DHCP δεν βρίσκονται στο ίδιο υποδίκτυο IP (π.χ. δίκτυο με πολλά VLAN)
- Η διεύθυνση 255.255.255.255 δεν προωθείται
- Ο δρομολογητής δρα ως αναμεταδότης μηνυμάτων DHCP
  - στέλνει αίτηση με unicast στον εξυπηρετητή με τη διεύθυνσή του
  - ο εξυπηρετητής DHCP απαντά ανάλογα με τη διεύθυνση IP του δρομολογητή

Μήνυμα BOOTP/DHCP

OpCode	Hardware Type	Hardware address length	Hop Count
Seconds		Αχρησιμοποίητο (BOOTP) Σημαίες (DHCP)	
Transaction ID			
Διεύθυνση IP πελάτη			
Η IP διεύθυνσή σας			
Διεύθυνση IP εξυπηρετητή			
Διεύθυνση IP πύλης			
Διεύθυνση υλικού πελάτη (16 byte)			
Όνομα εξυπηρετητή (64 byte)			
Όνομα boot file (128 byte)			
Επιλογές			

Υπάρχουν περισσότερες από 100 επιλογές

BOOTP/DHCP

- OpCode: 1 (Request), 2 (Reply)
  - Ο τύπος μηνύματος DHCP περιλαμβάνεται στις επιλογές
- Hardware Type: 1 (Ethernet)
- Hardware address length: 6 (Ethernet)
- Hop count: τίθεται στο 0 από τον πελάτη
- Transaction ID: ακέραιος αριθμός (για να προσδιορισθεί η απάντηση στην αίτηση)
- Seconds: αριθμός δευτερολέπτων από την εκκίνηση (boot) του πελάτη
- Client IP address, your IP address, server IP address, Gateway IP address, client hardware address, server host name, boot file name: ο πελάτης συμπληρώνει ό,τι ξέρει και αφήνει τα άλλα κενά

Τύποι μηνυμάτων DHCP

- Ο τύπος μηνύματος στέλνεται ως επιλογή

Τιμή	Τύπος μηνύματος
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM

Άλλες επιλογές

- Άλλες πληροφορίες που στέλνει το DHCP ως επιλογές:

  Subnet Mask, Name Server, Hostname, Domain Name, Forward On/Off, Default IP TTL, Broadcast Address, Static Route, Ethernet Encapsulation, X Window Manager, X Window Font, DHCP Msg Type, DHCP Renewal Time, DHCP Rebinding, Time SMTP-Server, SMTP-Server, Client FQDN, Printer Name, …