ΕΑΠ/ΠΛΗ22/ΑΘΗ.4
ΟΣΣ-4 Δίκτυα Η/Υ
Συμπληρωματικές Διαφάνειες

Νίκος Δημητρίου

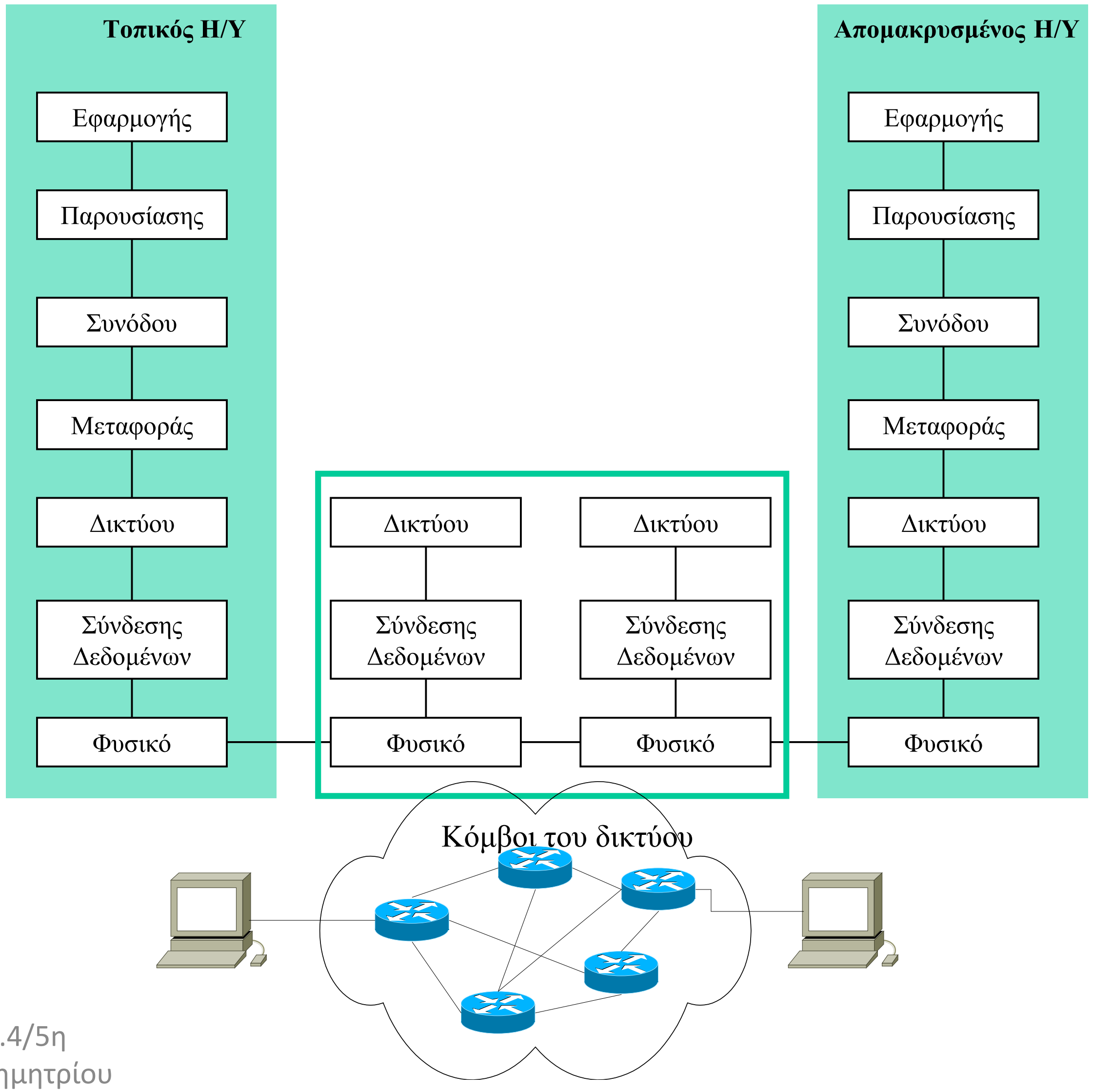
Σημείωση

- Στην παρουσίαση αυτή παρατίθενται παραπομπές σε συγκεκριμένες διαφάνειες της παρουσίασης *PLH22_OSS5_2016.pdf* που βρίσκεται στο **study.eap.gr** στο φάκελο *Ομαδικές Συμβουλευτικές Συναντήσεις (ΟΣΣ)/ΟΣΣ5*

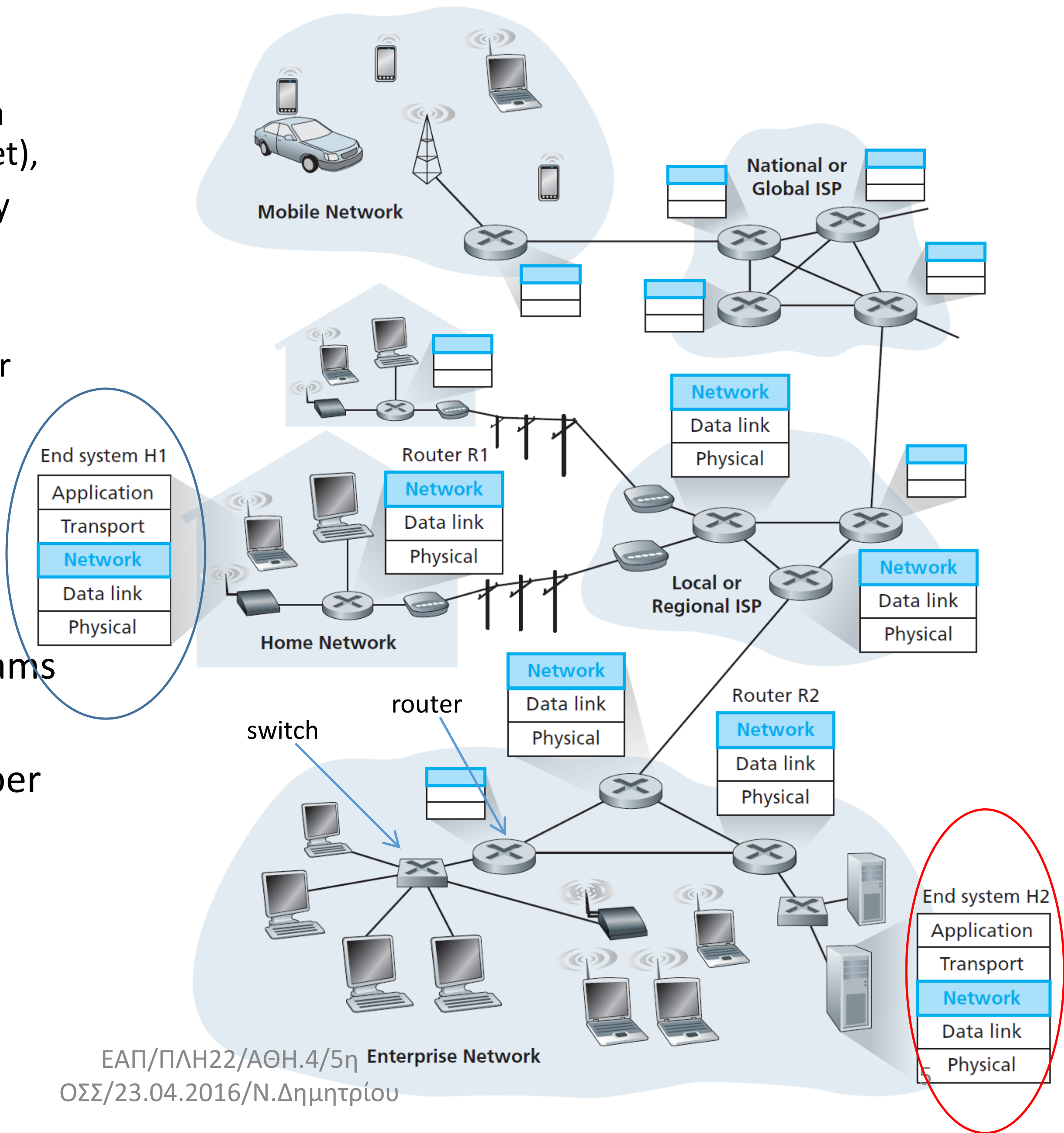
- Θέματα: OSI - TCP/IP layers, MAC protocols, TDMA, FDMA, Aloha/Slotted Aloha, Aloha Throughput, CSMA, CSMA/CD
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_2016.pdf*:

7,8,20,25,26,33,34,35,41,42,43,44,46,47

Το Μοντέλο Αναφοράς ISO/OSI



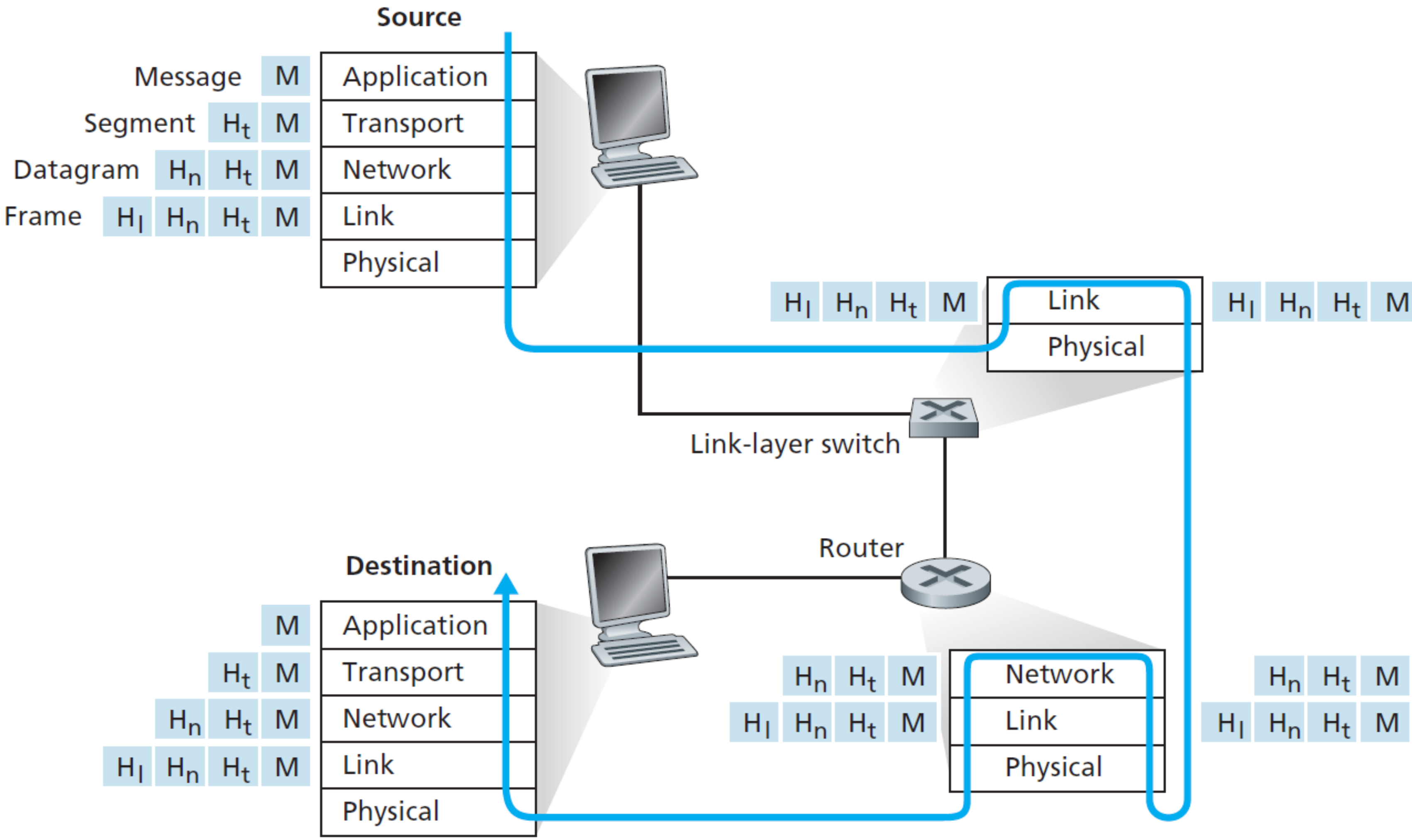
- Network with hosts, H1, H2, +several routers
- NET layer in H1
    - takes segments from transport layer , encapsulates each into a datagram (network-layer packet),
    - sends the datagrams to nearby router, R1.
- At H2, the NET layer
    - receives datagrams from router R2,
    - extracts transport-layer segments,
    - delivers the segments the transport layer at H2.
- Role of routers : forward datagrams from input links to output links.
- truncated protocol stack, no upper layers above the network layer
- routers mostly do not run application /transport-layer protocols



Επίπεδα / Στρώματα OSI

	5	Εφαρμογής	
segments	4	Μεταφοράς	end-end ([illegible])
datagrams	3	Δικτύου	routing devices (routers)
frames	2	Ζεύξης	switching devices. (switches, bridges)
	1	φυσικό	repeaters, hubs

Encapsulation- Ενθυλάκωση



repeaters, : Λήψη μεταδιδόμενων bits (ηλεκτρικό σήμα),

Ενίσχυση /αναγέννηση σήματος , αποστολή στην έξοδο
προώθηση

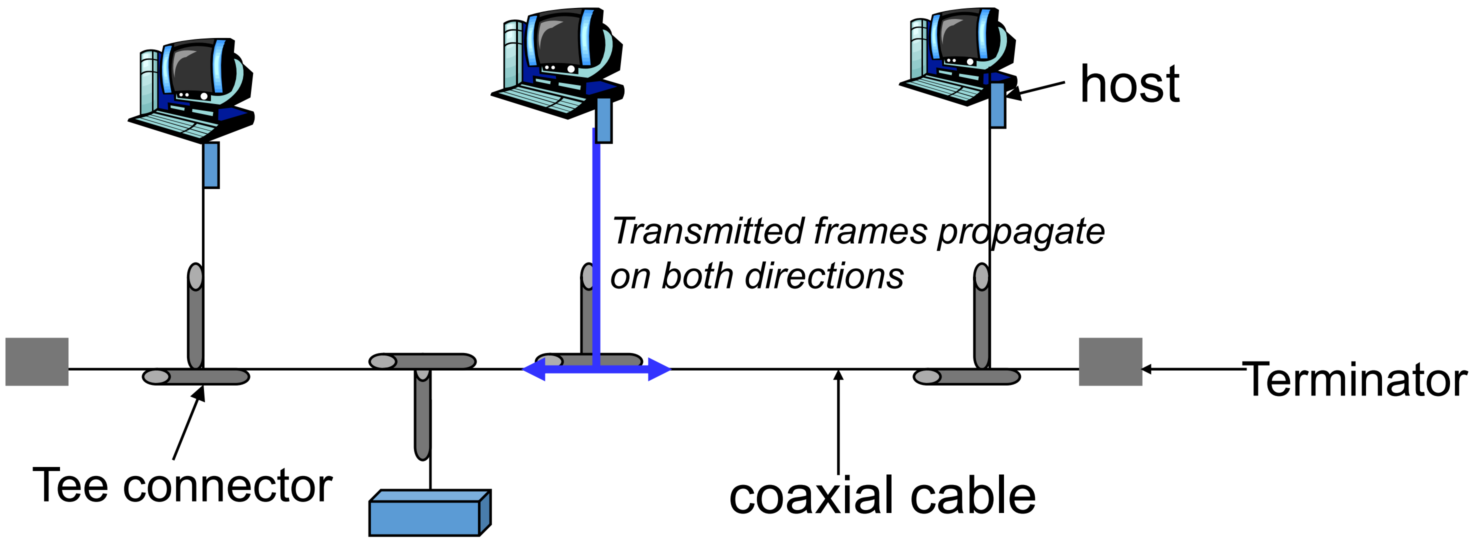
χρήση: επέκταση ενός διαύλου.

hubs : multiport repeaters. Κάθε εισερχόμενο frame

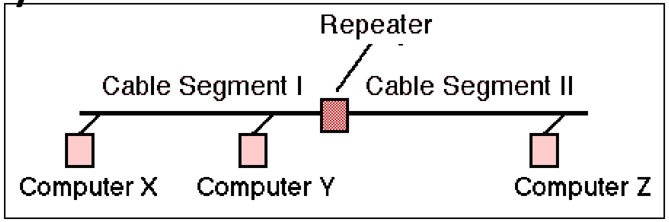
αναμεταδίδεται σε όλες τις υπόλοιπες θύρες του hub

χρήση: διασύνδεση πολλαπλών σταθμών σε τοπολογία αστέρα

Ethernet Bus connection



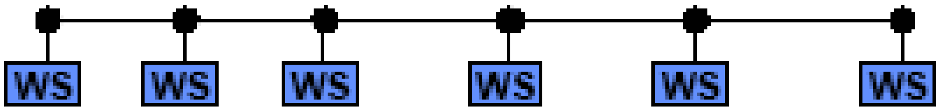
- When a frame enters a Tee connector
  - a frame copy is forwarded towards each of 2 directions of the connector
  - As frames propagate towards the terminator they ‘leave’ a copy on each host adapter they ‘traverse’
- To cover long distances, repeaters/relays are used

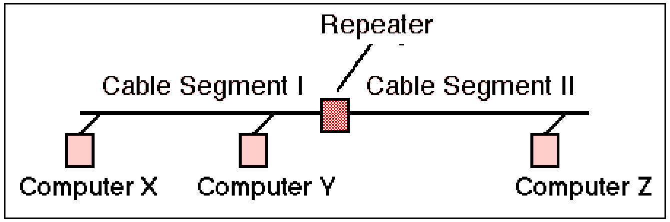


Ethernet Topologies

"Traditional " Ethernet

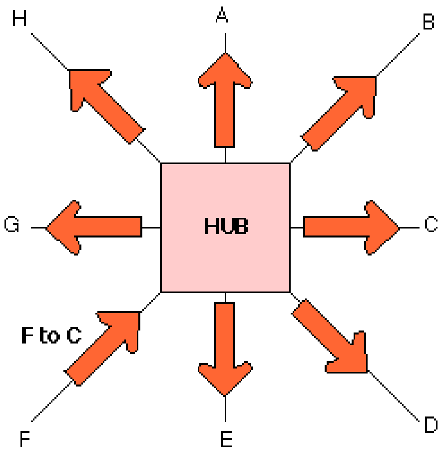
Interconnection over a long cable (a bus) using CSMA/CD.



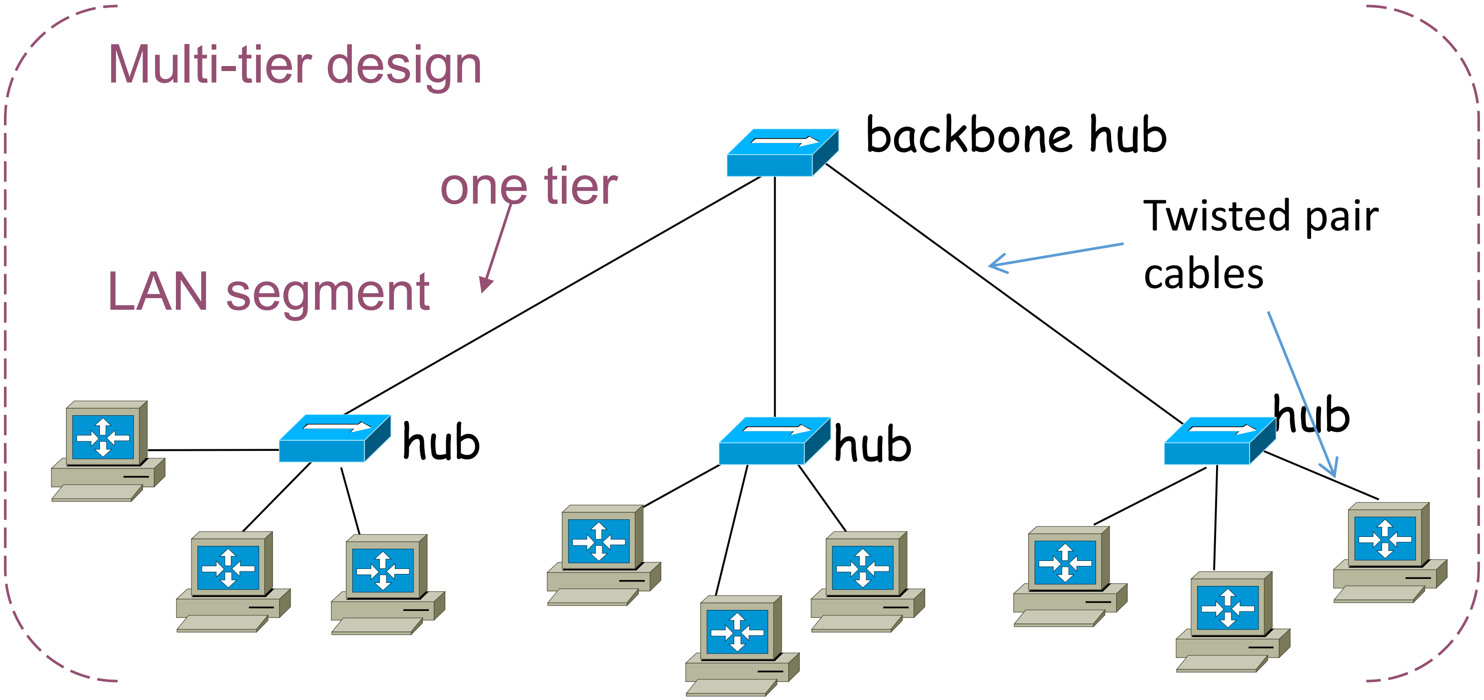


"Hub" Ethernet

Hosts interconnected via a hub that works as a repeater for all transmitted packets
using CSMA/CD.
(More flexible design)



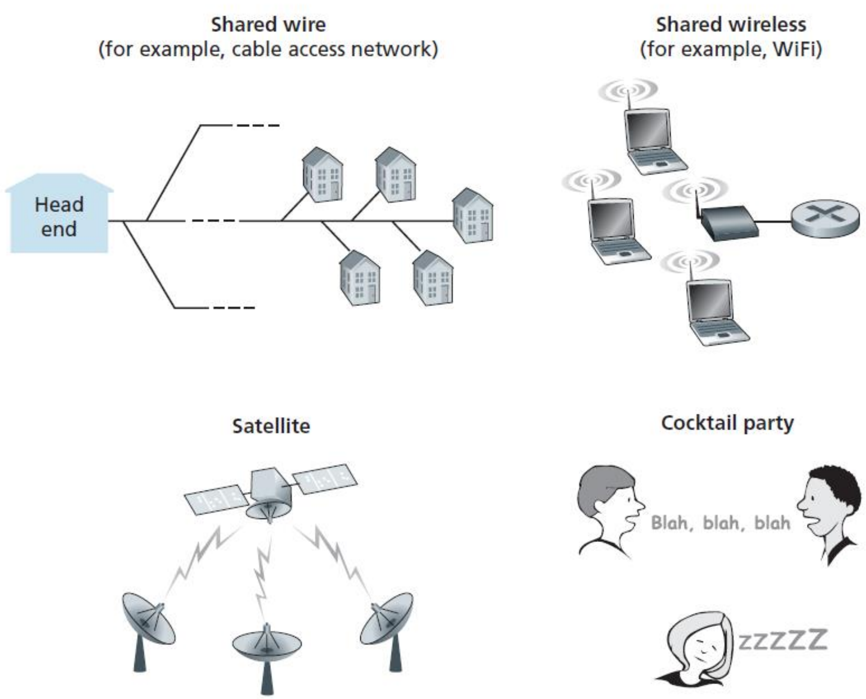
Ethernet hub connection



- Using hubs enables a more scalable topology interconnecting hosts at larger distances
- Limited by collision domains that increase as hosts/tiers increase

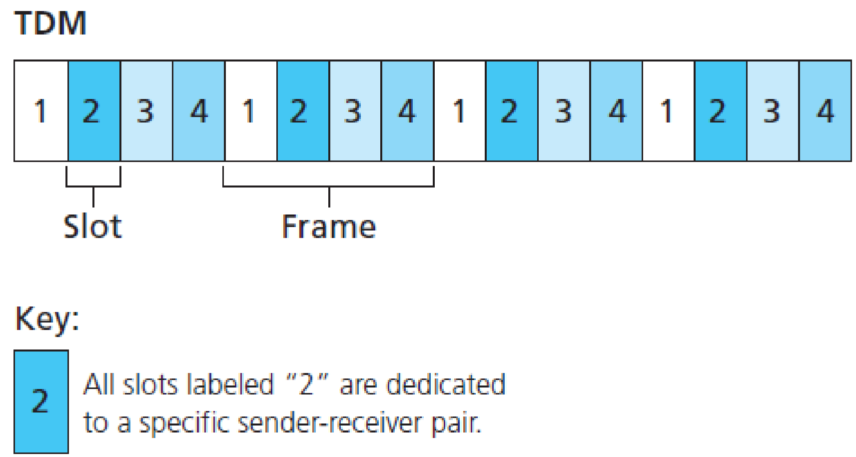
Multiple Access Links and Protocols

- Problem: multiple sending and receiving nodes to a shared broadcast channel
- At any time only one node can use the channel

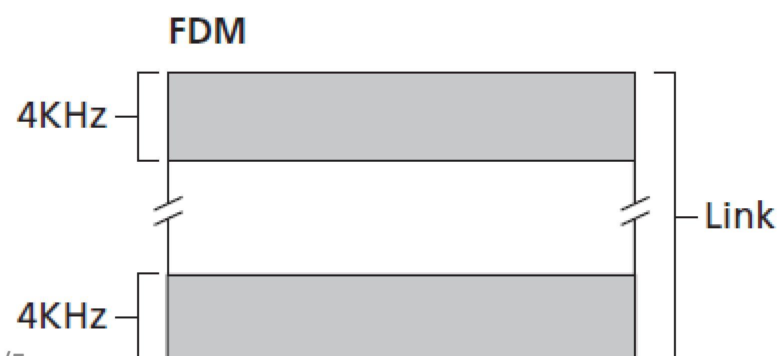


Channel Partitioning Protocols

- TDM
  - Each user allocated a timeslot in a frame



- FDM
  - Each user is assigned a frequency channel



Random Access Protocols

- A transmitting node always transmits at the full rate of the channel, R bps.
- When there is a collision, each node involved in the collision repeatedly retransmits its frame until its frame gets through without a collision.
- When a node experiences a collision, it doesn’t necessarily retransmit the frame right away.
  - Waits a random delay before retransmitting the frame.
- Each node involved in a collision chooses independent random delays.

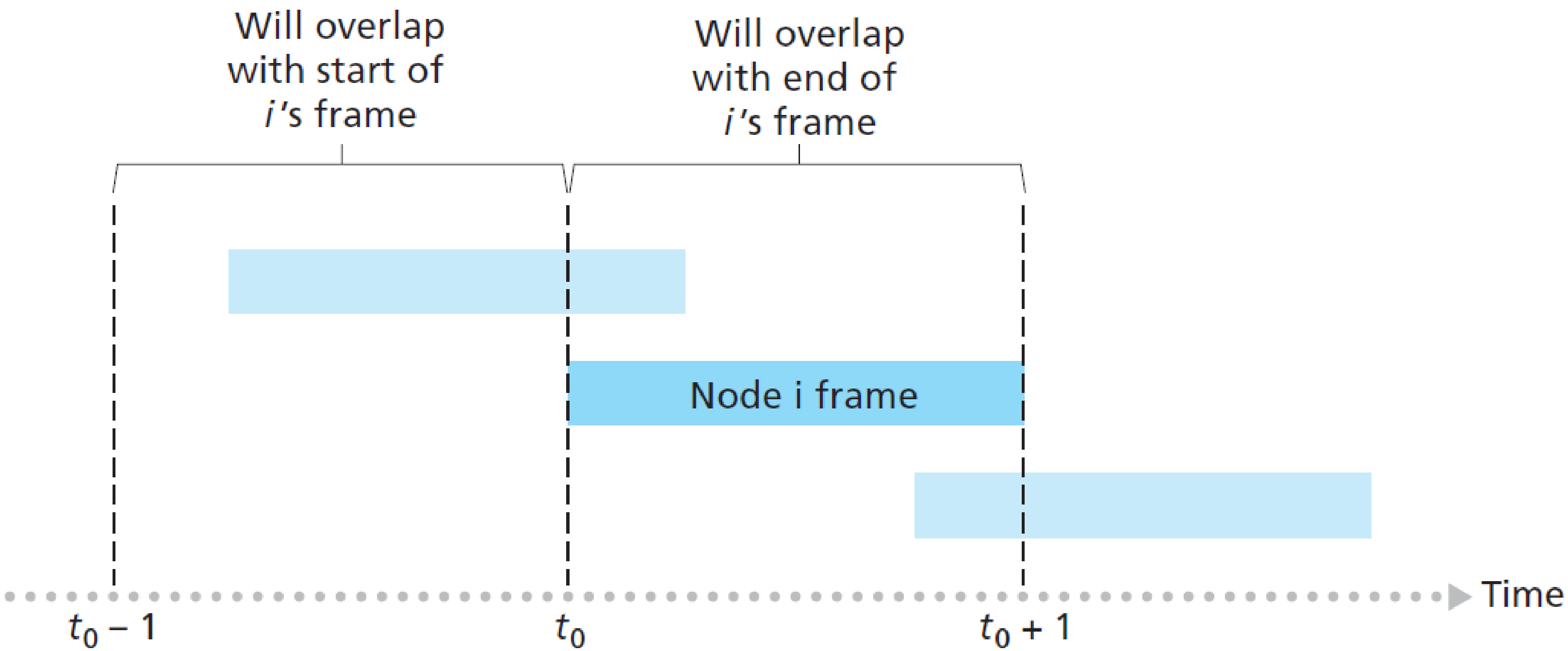
Basic assumptions

- All frames consist of exactly *L bits.*
- Time is divided into slots of size *L/R seconds (that is, a slot equals the time to* transmit one frame).

Aloha motivation

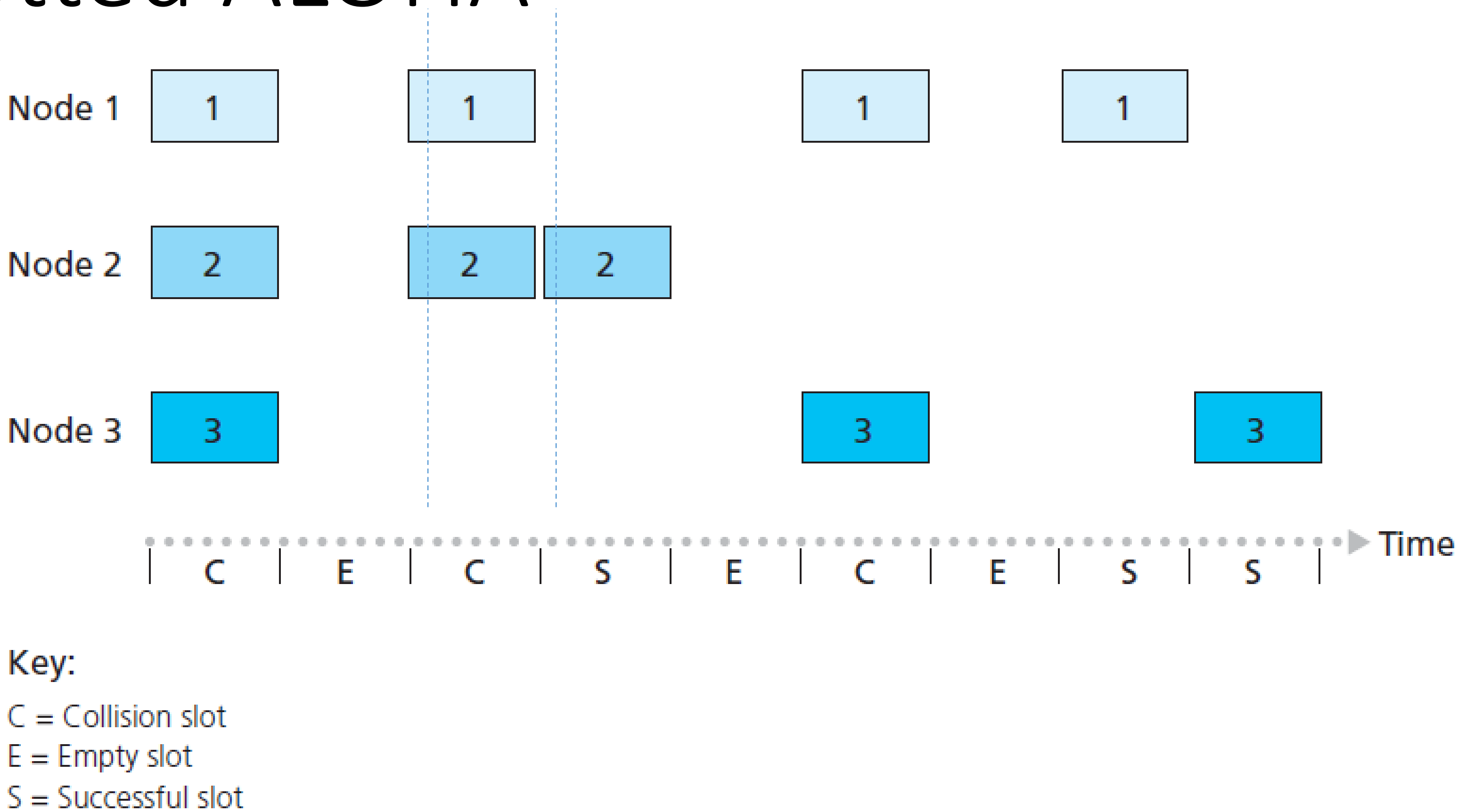
- Designed in Univ.Hawaii in the early 1970s (by N.Abramson,).
- Conditions: no working telephone system infrastructure
- Problem: how to connect users on remote islands to the main computer in Honolulu.
  - Laying underwater cables under the Pacific Ocean not an option…
- Solution: employ used short-range radios, with each user terminal sharing the same upstream frequency to send frames to the central computer.
- Basic idea: let users transmit whenever they have data to be sent OVER THE SAME UPLINK FREQUENCY CHANNEL.
- In case of muliple uplink transmissions - > collisions, colliding frames will be damaged.
- Senders need some way to find out if this is the case.
- In the ALOHA system, after each station has sent its frame to the central computer, this computer **rebroadcasts** the frame to all of the stations using the **separate downlink frequency channel** .
- A sending station can thus listen for the broadcast from the hub to see if its frame has gotten through.
- If frame destroyed, sender just waits a random amount of time and sends it again.
- Systems in which multiple users share a common channel in a way that can lead to conflicts are known as **contention systems.**

pure ALOHA



- Suppose this frame begins transmission at time t_0.
- To avoid collisions, no other nodes can begin their transmission in the interval of time $[t_0 – 1, t_0]$ AND $[t_0, t_0+1]$
- That means that all other nodes should be silent for 2 intervals

slotted ALOHA



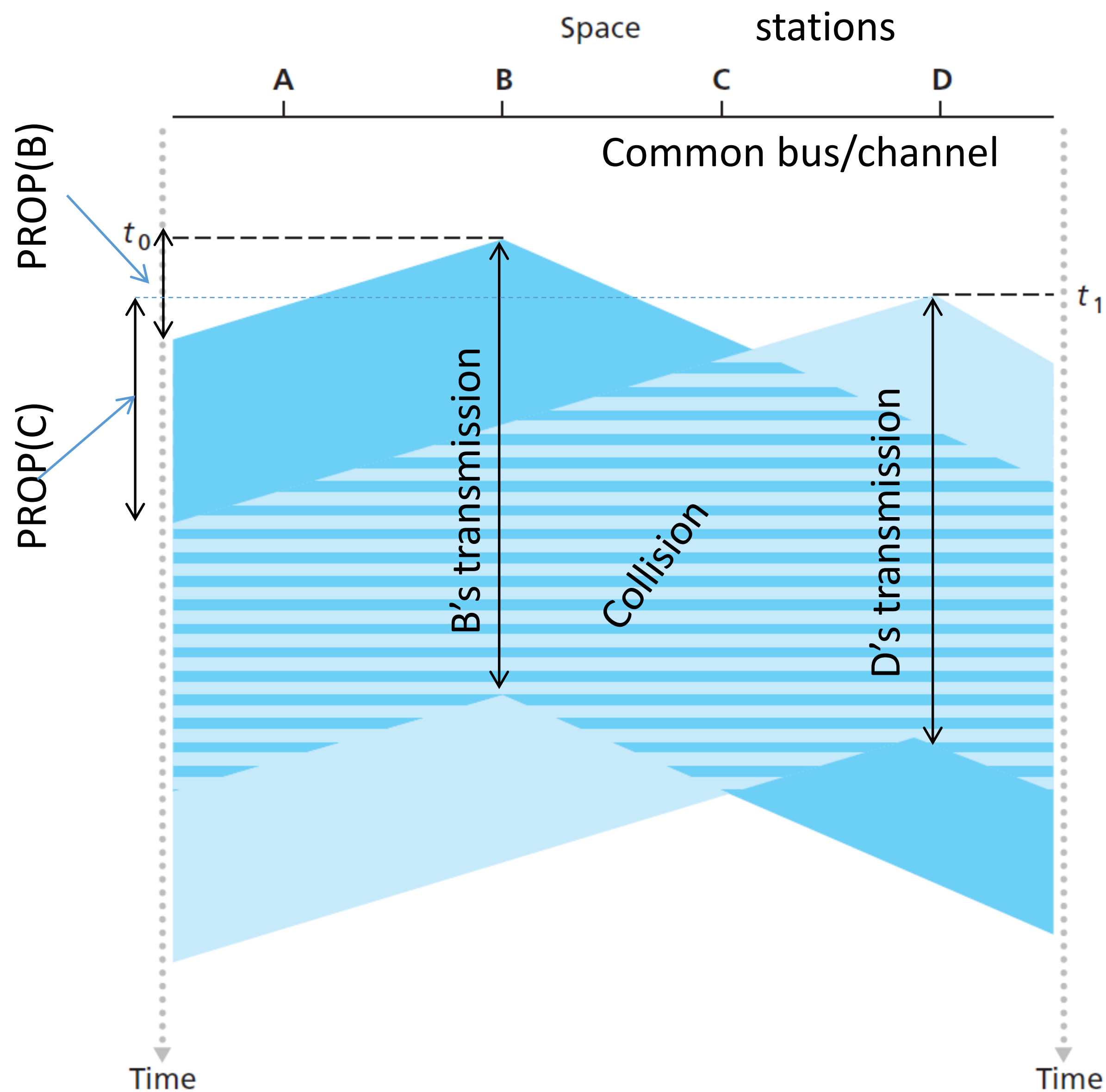
- To avoid collisions, no other nodes can begin their transmission in ONE timeslot duration
- That means that all other nodes should be silent for 1 timeslot (not 2 as shown in pure aloha)

Carrier Sense Multiple Access

- In both slotted and pure ALOHA, a node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel.
- A node neither
  - pays attention to whether another node happens to be transmitting when it begins to transmit,
  - nor stops transmitting if another node begins to interfere with its transmission.
- CSMA addresses the first issue
- CSMA/CD addresses the second issue

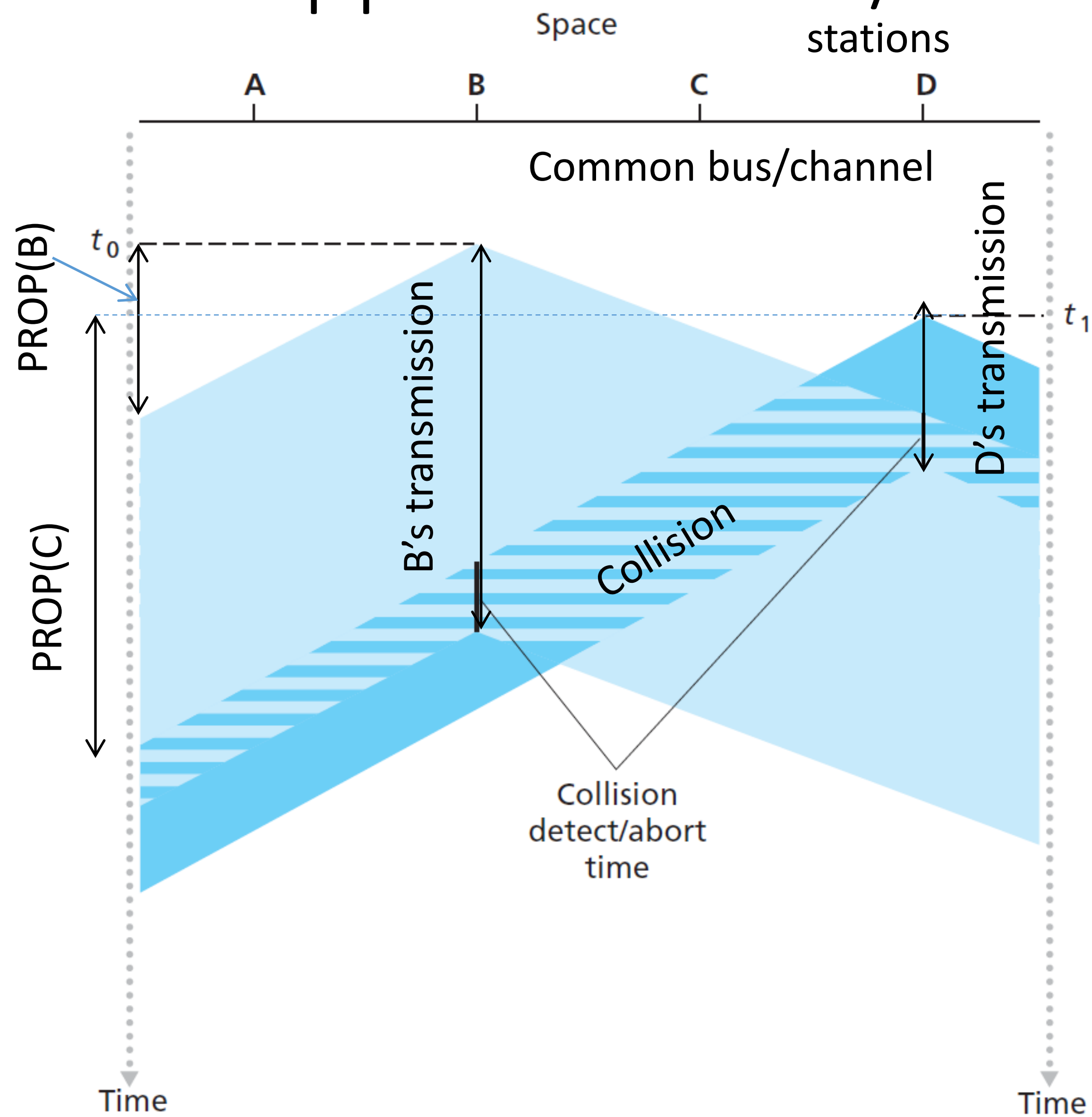
How do collisions happen in CSMA?

- No Collision detection assumed here
- A nonzero amount of time is needed the transmitted bits to propagate (albeit at near the speed of light) along the broadcast medium

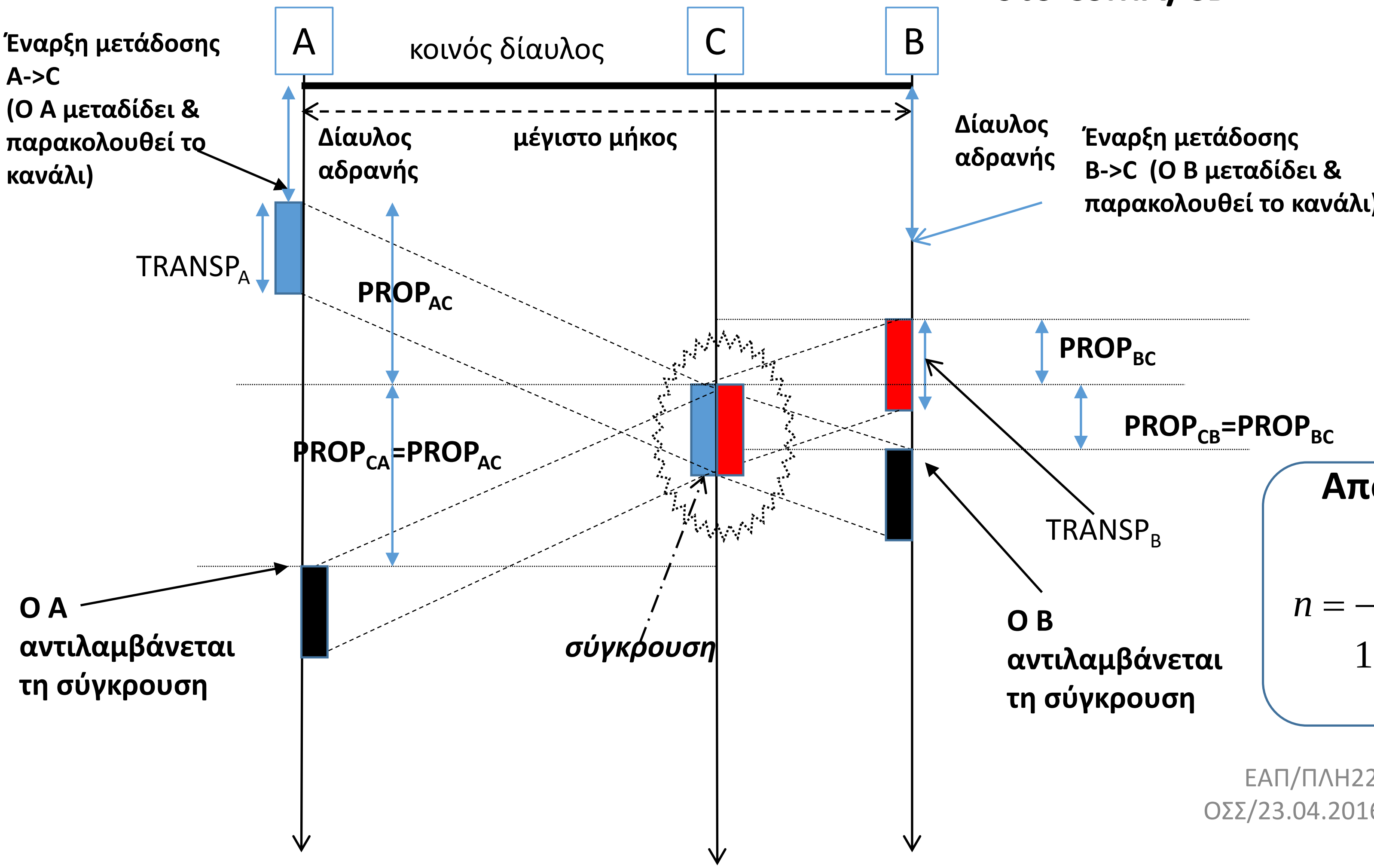


How do collisions happen in CSMA/CD?

- Collision detection assumed here
- the two nodes each abort their transmission a short time after detecting a collision.
- adding collision detection helps protocol performance by not transmitting a useless, damaged frames



Συνθήκη ανίχνευσης συγκρούσεων στο CSMA/CD



Αποδοτικότητα CSMA/CD

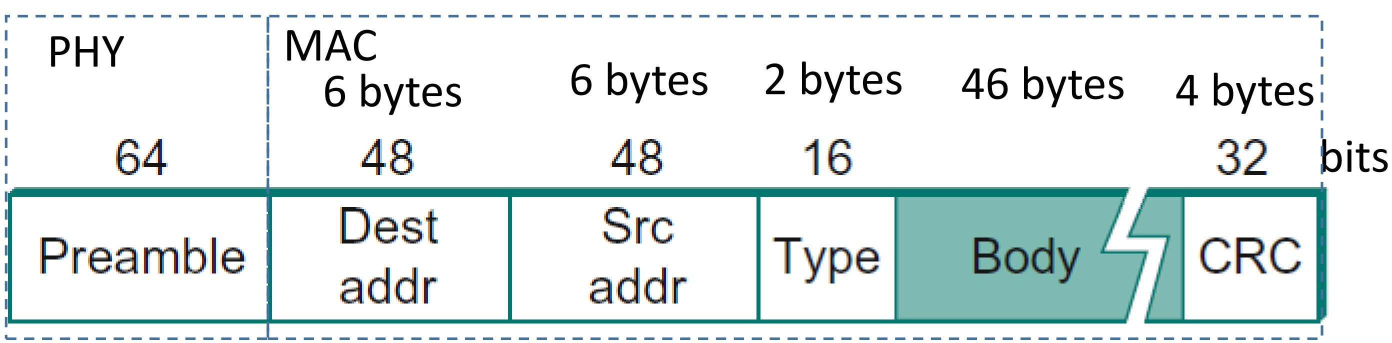
$$n = \frac{1}{1 + 5\dfrac{PROP}{TRANSP}}$$

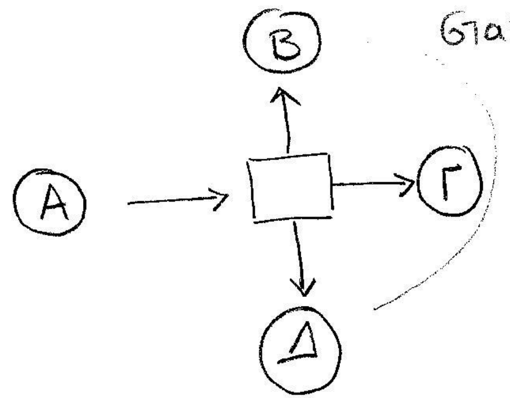
Για να μπορέσει ο αποστολέας να αντιληφθεί τη σύγκρουση (ενώ μεταδίδει το πλαίσιο) θα πρέπει TRANSP ≥ 2 PROP

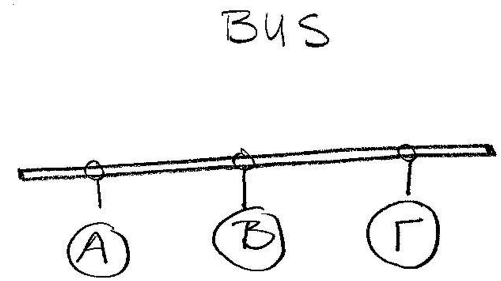
Χειρότερη περίπτωση: Ο C ταυτίζεται με το B (είναι στη μέγιστη δυνατή απόσταση από τον A)
$TRANSP \geq 2PROP_{MAX}$ (μέγιστος χρόνος διάδοσης ενός bit end-end)

Ethernet Frame Structure

- Layer 1
  - 64-bit preamble: receiver synchronization, sequence of alternating 0s and 1s. Source and destination hosts identified with a 48-bit address.
- Layer 2
  - Each frame contains up to 1500 bytes of data.
    - Minimally, a frame must contain at least 46 bytes of data,
    - frame must be long enough to detect a collision
  - each frame includes a 32-bit CRC.
  - 14-byte header / two 6-byte addresses and a 2-byte type field.







όλα τα πακέτα λαμβάνονται από όλους τους σταθμούς

Αποφυγή συγκρούσεων: CSMA/CD

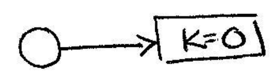
→ Μετάδοση όταν το κοινό μέσο δεν χρησιμοποιείται από άλλον

→ Αν μεταδόσουν ταυτόχρονα περισσότεροι του ενός → backoff μηχανισμός

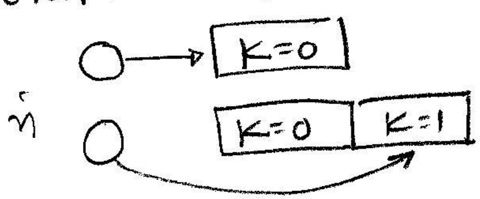
Αν έχουν συμβεί i- συγκρούσεις: επιλογή αποστολής σε χρόνο $\kappa \cdot T$

$$K = 0, 1, \ldots, 2^{i} - 1$$

0 συγκρούσεις: $K=0$: άμεση αποστολή



1 σύγκρουση: $K = 0$ ή 1 : είτε άμεση αποστολή είτε μετά χρόνο $1 \cdot T$

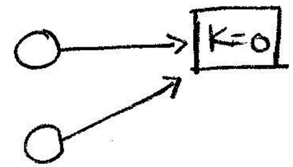


κ.ο.κ

2.

Αν $K=0$ και 2 σταθμοί στείλουν ταυτόχρονα

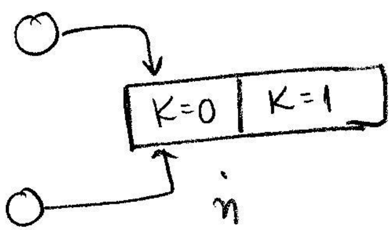
$$P(\text{collision}) = 1$$



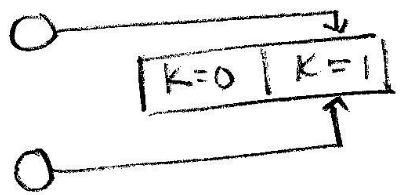
Αν $K=0$ ή T και 2 σταθμοί στείλουν

$P(\text{collision}) = P(\text{και οι δύο στο } K=0) + P(\text{και οι 2 στο } K=1)$

$$= \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$$



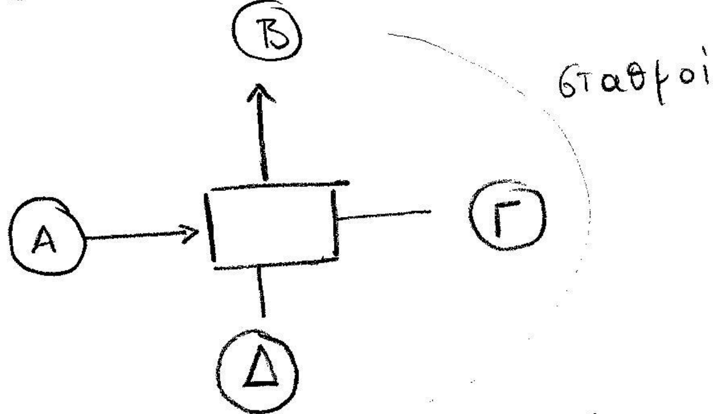
ή



- Θέματα: LAN topologies, Bus/relay/hub/switch/bridge
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_2016.pdf* :

57,58,73,79,85,86,87,90,91

SWITCH/BRIDGE



Τα πακέτα προωθούνται στην αντίστοιχη θύρα με βάση την αντιστοίχιση MAC address / θύρας (σε πίνακα)

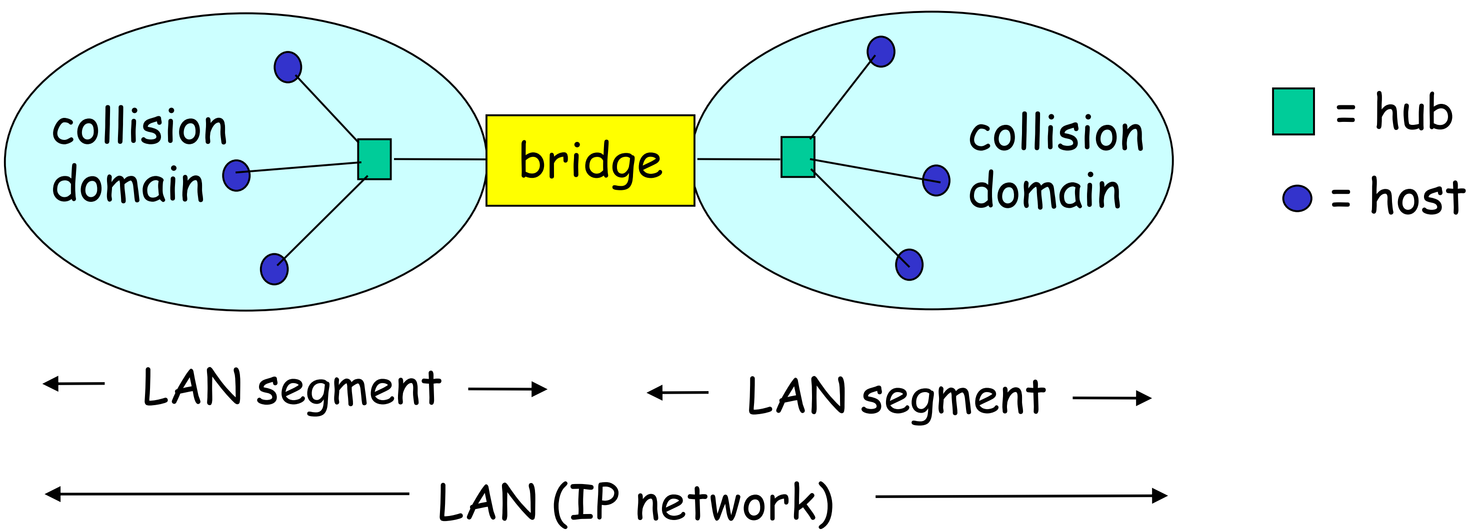
Ο πίνακας δημιουργείται με βάση την κίνηση των πακέτων (διαδικασία μάθησης)

Οι εγγραφές του πίνακα μπορεί να έχουν χρόνο ισχύος (Time To Live)

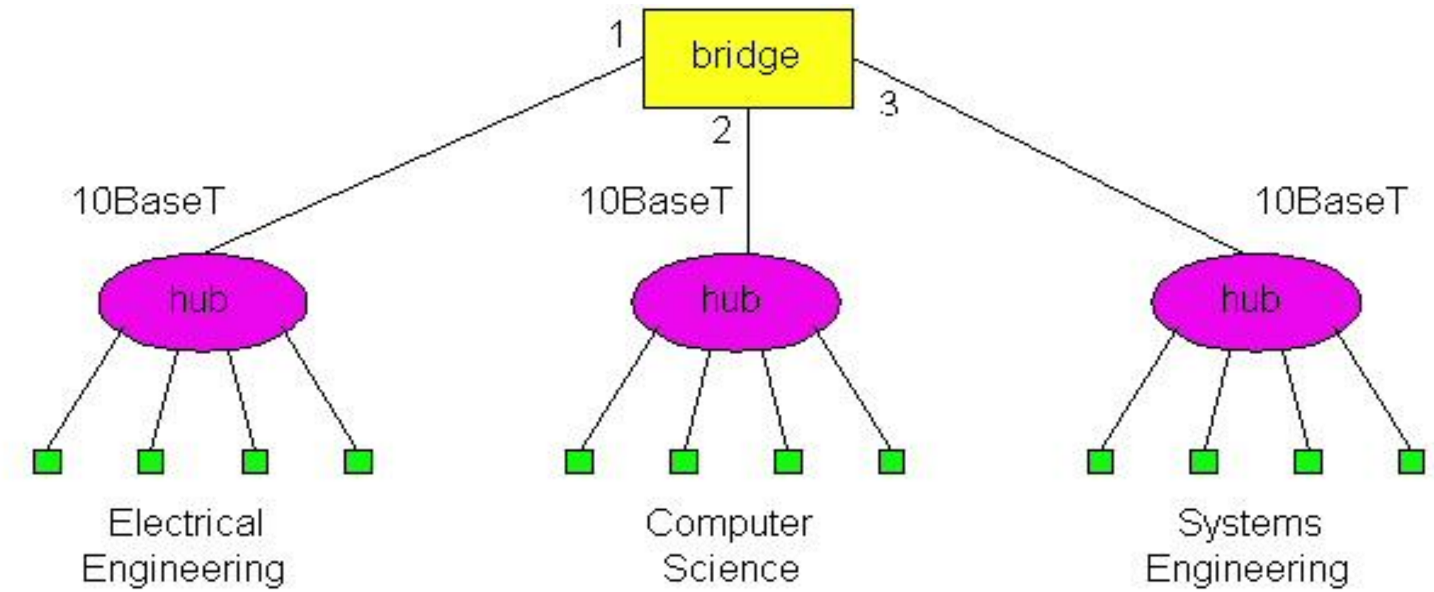
Αποφυγή συγκρούσεων

Bridges: traffic isolation

- Bridge installation breaks LAN into LAN segments
- bridges filter packets:
  - same-LAN-segment frames not usually forwarded onto other LAN segments
  - segments become separate collision domains



Forwarding

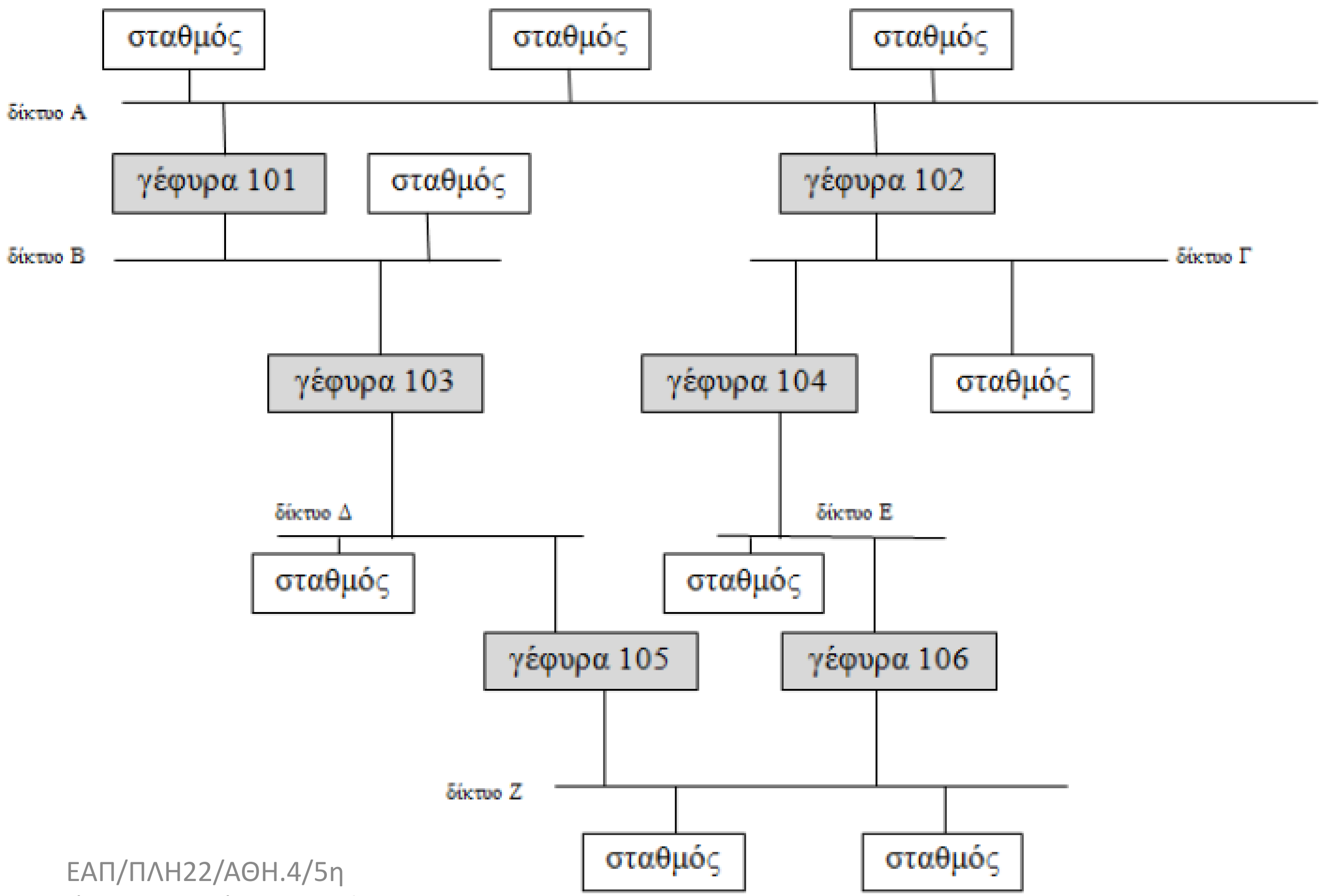


How do determine to which LAN segment to forward frame?

- Looks like a routing problem...

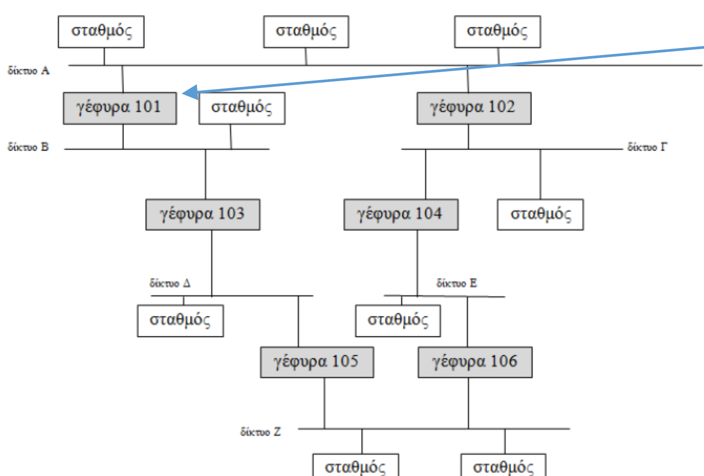
ΓΕ5/1415/Θ3

Δώστε την κεντρική μήτρα δρομολόγησης και τους πίνακες δρομολόγησης των γεφυρών 103 και 104 του παραπάνω σχήματος. Σε περίπτωση διαδρομών με το ίδιο κόστος αλμάτων, προτιμήστε την διαδρομή της νέας (ταχύτερης και με λιγότερη κίνηση) γέφυρας 105.



Κεντρική μήτρα δρομολόγησης:

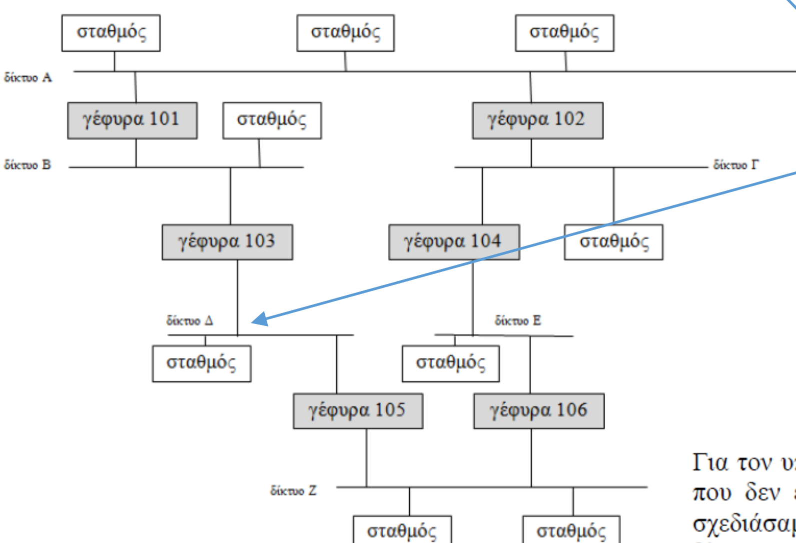
		δίκτυο πομπού					
		Α	Β	Γ	Δ	Ε	Ζ
δίκτυο δέκτη	Α	-	101	102	103	104	105
	Β	101	-	102	103	106	105
	Γ	102	101	-	105	104	106
	Δ	101	103	104	-	106	105
	Ε	102	103	104	105	-	106
	Ζ	101	103	104	105	106	-



next hop

Πίνακας γέφυρας 103				Πίνακας γέφυρας 104			
από δίκτυο Β		από δίκτυο Δ		από δίκτυο Γ		από δίκτυο Ε	
δέκτης	επόμενο	Δέκτης	επόμενο	δέκτης	επόμενο	δέκτης	επόμενο
Α	-	Α	Β	Α	-	Α	Γ
Γ	-	Β	Β	Β	-	Β	-
Δ	Δ	Γ	-	Δ	Ε	Γ	Γ
Ε	Δ	Ε	-	Ε	Ε	Δ	-
Ζ	Δ	Ζ	-	Ζ	Ε	Ζ	-

next hop



Για τον υπολογισμό των πινάκων δρομολόγησης κάθε γέφυρας σημειώνουμε με '-' κάθε συνδυασμό δικτύων που δεν επικοινωνούν μέσω της συγκεκριμένης γέφυρας. Για παράδειγμα από την κεντρική μήτρα που σχεδιάσαμε ελέγχουμε από το δίκτυο Β ποιο άλλο δίκτυο επικοινωνεί μέσω της γέφυρας 103 (ενώνει τα δίκτυα Β και Δ).. Εάν δεν επικοινωνεί σημειώνουμε "-". Εάν επικοινωνεί σημειώνουμε Δ ως το επόμενο δίκτυο. Για παράδειγμα το Β-Ζ επικοινωνεί μέσω της γέφυρας 103, οπότε σημειώνομε Δ.

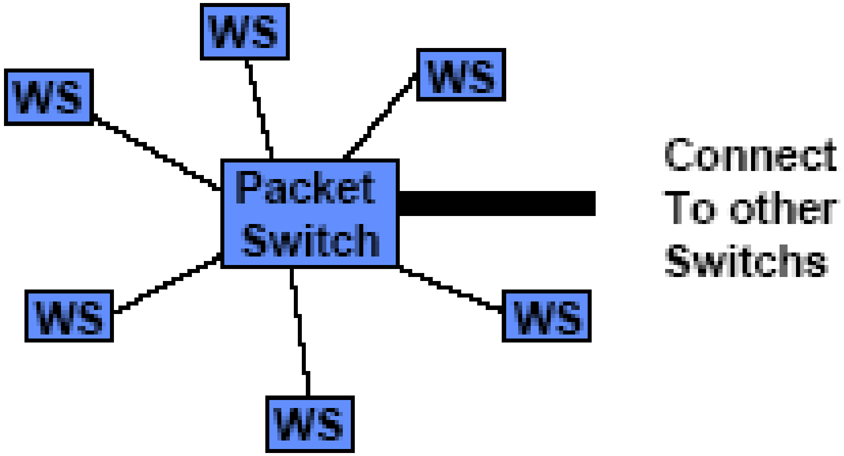
Switched Ethernet

•Star Connection

•No CSMA CD (No packet collisions

•Hosts send whenever they have available frames

•Store-and-Forward Switches



ΘΕΜΑ 1 **ΓΕ4/1314**

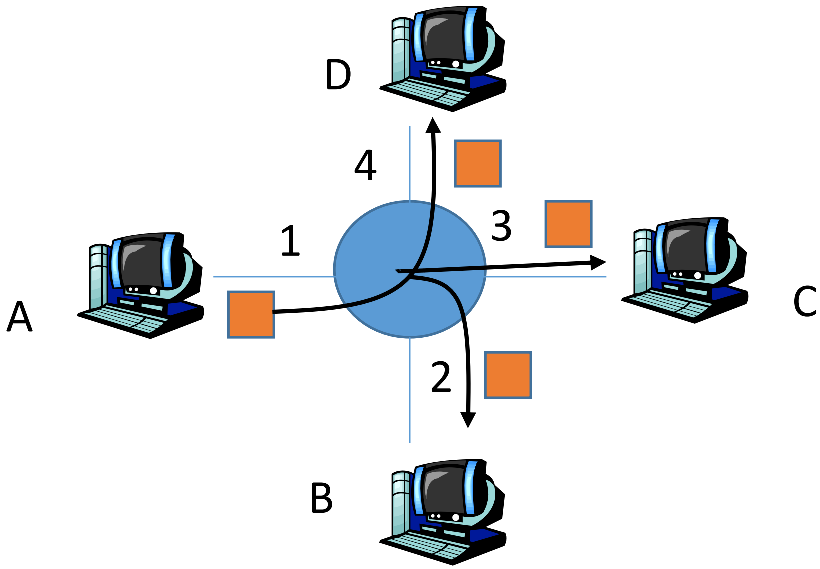
Στόχος της άσκησης *είναι η εξοικείωση με τις τεχνολογίες Ethernet και TCP/IP*

Μεθοδολογία Άσκησης: *Θα πρέπει να μελετήσετε τις λυμένες ενδεικτικές ασκήσεις σχετικά με Hub, Bridge, Switching και IP Forwarding, ARP*

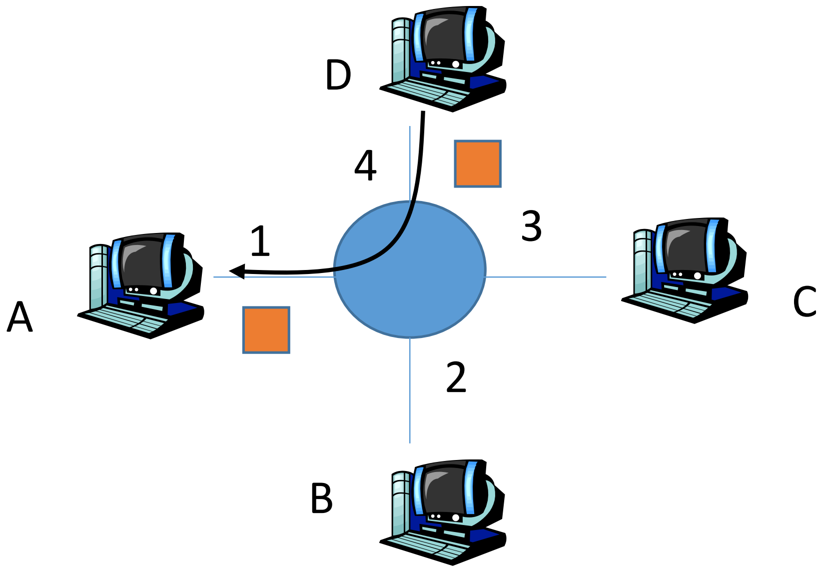
1. Να θεωρήσετε ένα Ethernet LAN switch στο οποίο είναι συνδεδεμένοι τέσσερις hosts: A, B, C, D. Οι κόμβοι χρησιμοποιούν την τοπολογία star για τη διασύνδεση των hosts A, B, C, D. O Host A είναι συνδεδεμένος στο interface 1 του μεταγωγέα, ο host B στο interface 2, ο host C στο interface 3 και ο host D στο interface 4. Να θεωρήσετε ότι ο πίνακας μεταγωγής του μεταγωγέα είναι άδειος. Για κάθε ένα από τα παρακάτω γεγονότα να δείξετε πως ανανεώνεται ο πίνακας αυτός και να αναφέρεται τα interfaces όπου τα πλαίσια μεταδίδονται.

- Ο A στέλνει ένα frame στο D
- Ο D στέλνει ένα frame στον A

Μεθοδολογία: Θα πρέπει να μελετήσετε τα Θέματα 2, 4 απ τις λυμένες ασκήσεις στην ενότητα Hub, Bridge, Switching



1. Μετάδοση A-D
2. O A αποστέλλει ένα πακέτο με τη MAC address του D
3. O πίνακας του switch είναι άδειος οπότε το πακέτο αποστέλλεται σε όλες τις θύρες Πλην της εισόδου (2,3,4)
4. Οι B,C απορρίπτουν το πακέτο.
5. Το switch ενημερώνει τον πίνακά του (A,1)



1. Μετάδοση D-A
2. O D αποστέλλει ένα πακέτο με τη MAC address του A
3. O πίνακας του switch table έχει την εγγραφή (A,1) οπότε το πακέτο αποστέλλεται MONO στη θύρα 1 και το σταθμό A.
4. To switch ενημερώνει τον πίνακά του (D,4)

ΘΕΜΑ 1

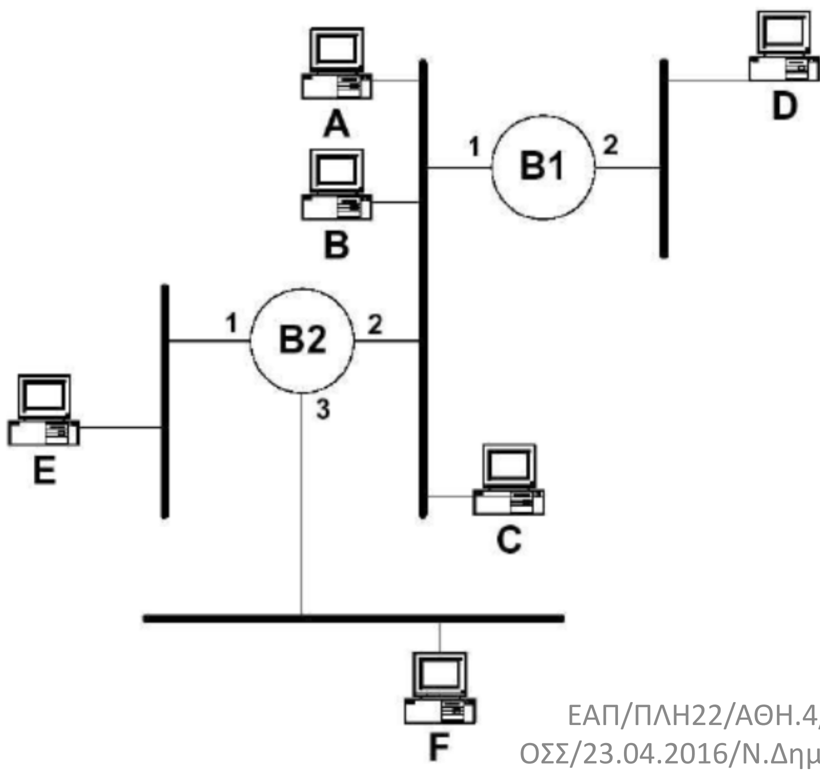
ΓΕ4/1314

Στόχος της άσκησης *είναι η εξοικείωση με τις τεχνολογίες Ethernet και TCP/IP*

Μεθοδολογία Άσκησης: *Θα πρέπει να μελετήσετε τις λυμένες ενδεικτικές ασκήσεις σχετικά με Hub, Bridge, Switching και IP Forwarding, ARP*

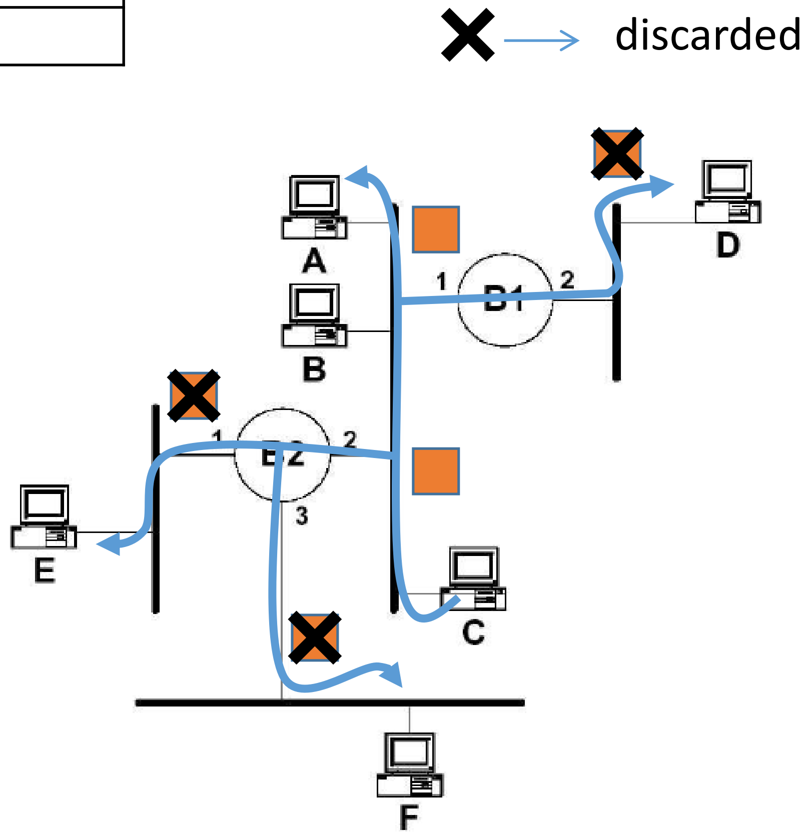
3. Να θεωρήσετε το δίκτυο του παρακάτω σχήματος. Αν θεωρήσετε ότι δεν υπάρχουν εγγραφές, να αναφέρετε πως θα τροποποιηθούν οι εγγραφές στις γέφυρες B1, B2, όταν γίνουν οι παρακάτω μεταδόσεις

- C στέλνει στον A
- F στέλνει στον E
- E στέλνει στον F



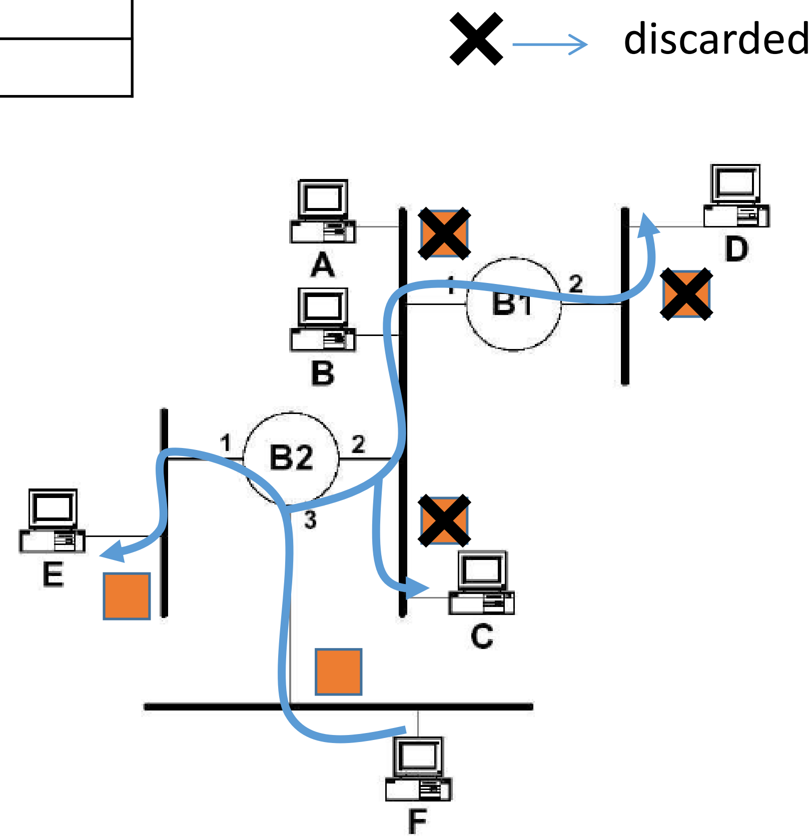
Μετάδοση C - A

Bridge B1		Bridge B2	
C	1	C	2



Μετάδοση F - E

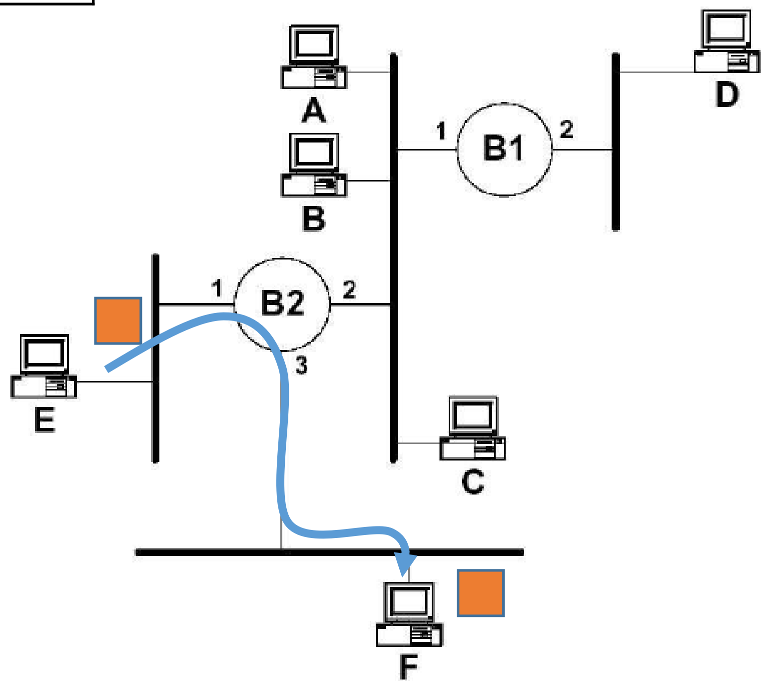
Bridge B1		Bridge B2	
C	1	C	2
F	1	F	3



Μετάδοση Ε - F

Bridge B1		Bridge B2	
C	1	C	2
F	1	F	3
		E	1

Ο πίνακας της Β2 έχει μια εγγραφή για το
Σταθμό F . Το πακέτο αποστέλλεται
Μόνο στη θύρα 3 της Β2 και καταλήγει
Στον παραλήπτη σταθμό F.
Η Β2 προσθέτει και την εγγραφή (Ε,1)

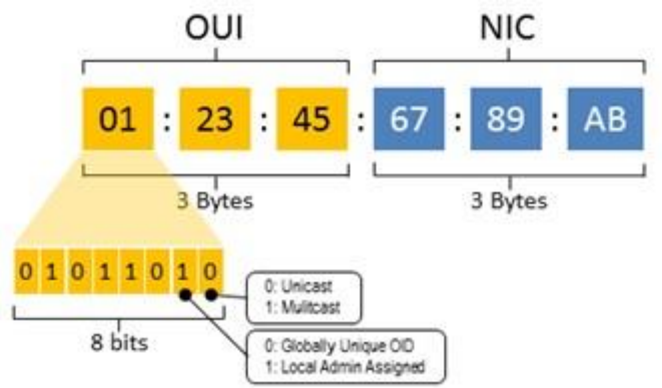


- Θέματα: MAC/IP Addressing, Subnets, Subnet Mask, Network/host addresses
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_2016.pdf* :

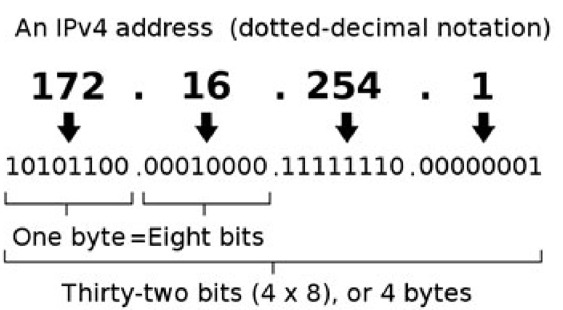
135,147,148

addresses...

- Each device interface has 2 address types:
  - MAC address (a.k.a. LAN/link layer/physical address)
    - Analogy: a person's ID/passport number
      - Flat address, to be used everywhere



  - IP address
    - Analogy: a person's contact telephone number
      - Hierarchical address, depends on the subnet to which the device connects



MAC address

- For most LANs (Ethernet and WiFi) MAC address is 6 bytes long, giving 2^{48} possible addresses.
- 6-byte addresses typically expressed in hexadecimal notation
  - each byte of the address expressed as a pair of hexadecimal numbers.
- no two adapters have the same address

Uniqueness of MAC addresses

- IEEE manages the MAC address space.
- When a company wants to manufacture adapters, purchases a ‘chunk’ of the address space consisting of 2^{24} addresses for a nominal fee.
- IEEE allocates the chunk of 2^{24} addresses by fixing the first 24 bits of a MAC address and letting the company create unique combinations of the last 24 bits for each adapter.

IPv4 Addressing

- Each IP address is 32 bits long (equivalently, 4 bytes), there are thus a total of 2^{32} possible IP addresses.
- By approximating 2^{10} by 10^3 ~ about 4 billion possible IP addresses
- These addresses are typically written in dotted-decimal notation
  - each byte of the address is written in its decimal form and is separated by a period (dot) from other bytes in the address.
- E.g. the IP address 193.32.216.9.
  - 193 is the decimal equivalent of the first 8 bits of the address
  - 32 is the decimal equivalent of the second 8 bits of the address etc.
  - The address 193.32.216.9 in binary notation is

11000001 00100000 11011000 00001001

IP Addressing

π.χ. 192.168.20.16

↓ ↓ ↓ ↓

0→255 0→255 0→255 0→255

↓

8 bits	8 bits	8 bits	8 bits

Network	Host

Το δίκτυο όπου ανήκει ο host βρίσκεται με τη βοήθεια του subnet mask ('1' bits από αριστερά προς τα δεξιά)

π.χ. 255.255.255.0

$$\underbrace{11111111.11111111.11111111}_{\text{IP Address}/24}.00000000$$

ΘΕΜΑ 4	**ΓΕ4/1314**

Στόχος της άσκησης *είναι η εξοικείωση με τις έννοιες των υποδικτύων*
Μεθοδολογία Άσκησης: *Θα πρέπει να μελετήσετε τις λυμένες ενδεικτικές ασκήσεις σχετικές με IP Forwarding, Addressing, ARP*

Ένας υπολογιστής έχει τις εξής παραμέτρους στο πρωτόκολλο IP:
Διεύθυνση IP : 202.60.215.150
Μάσκα υποδικτύου : 255.255.240.0

1. Ποιο είναι το μέγιστο πλήθος υπολογιστών που περιλαμβάνει η network address του δικτύου στο οποίο ανήκει;
2. Ποια είναι η πρώτη διεύθυνση host number του δικτύου στο οποίο ανήκει και ποια η τελευταία διεύθυνση host number του δικτύου ή διεύθυνση για αποστολή broadcasting μηνυμάτων;
3. Ποιός είναι ο αυξων αριθμός υπολογιστή (host number) στο δεκαδικό σύστημα;

(α) Η μάσκα υποδικτύου : 255.255.240.0σε δυαδική μορφή είναι:

255.255.224.0 → 1111111.1111111.11110000.00000000

άρα τα τελευταία 12 δυαδικά ψηφία χρησιμοποιούνται για τον αριθμό του υπολογιστή (host number ή subnet number και host number) ορίζοντας 2^{12}=4.096 συνδυασμούς. Το μέγιστο πλήθος υπολογιστών είναι 4.096-2=4.094 αφού οι διευθύνσεις με αριθμό υπολογιστή 0 αναφέρεται στο δίκτυο «this network» και 4.095χρησιμοποιείται για broadcasting μυνημάτων και δεν μπορούν να χρησιμοποιηθούν για IP υπολογιστή.

(β) Η πρώτη διεύθυνση host number του δικτύου προκύπτει αν θέσουμε τα bits του αριθμού υπολογιστή όλα 0 (λογικό AND ανάμεσα στην IP και στην μάσκα).

IP :	202.60.215.150 →	11001010.00111100.11010111.10010110
	AND	
Μάσκα υποδικτύου		11111111.11111111.11110000.00000000
πρώτη διεύθυνση host number		11001010.00111100.1101 $\boxed{\text{0000.00000000}}$

Άρα η ζητούμενη διεύθυνση υποδικτύου είναι: 202.60.208.0

Η τελευταία διεύθυνση host number του δικτύου προκύπτει αν θέσουμε τα bits του αριθμού υπολογιστή όλα 1, (λογικό OR ανάμεσα στην IP και στην ανάστροφη μάσκα) δηλαδή

IP :	202.60.215.150 →	11001010.00111100.11010111.10010110
	OR	
Ανάστροφη μάσκα υποδ.		00000000.00000000.00001111.11111111
διεύθυνση broadcast		11001010.00111100.1101 $\boxed{\text{1111.11111111}}$

Άρα η ζητούμενη τελευταία διεύθυνση host number του δικτύου είναι: 202.60.223.255

Σημείωση: Η 1^{η} διεύθυνση που μπορεί να δοθεί σε υπολογιστή είναι η 202.60.208.1 και η τελευταία είναι η 202.60.223.254

(γ) Ο ο αυξων αριθμός υπολογιστή (host number) προκύπτει αν στην IP διεύθυνση θέσουμε τα bits του δικτύου και του υποδικτύου ίσα με 0 (λογικό AND ανάμεσα στην IP και στην ανάστροφη μάσκα), δηλαδή

IP :	202.60.215.150 →	11001010.00111100.11010111.10010110
	AND	
Ανάστροφη μάσκα υποδ.		00000000.00000000.00001111.11111111
Αριθμός υπολογιστή		00000000.00000000.00000111.10010110

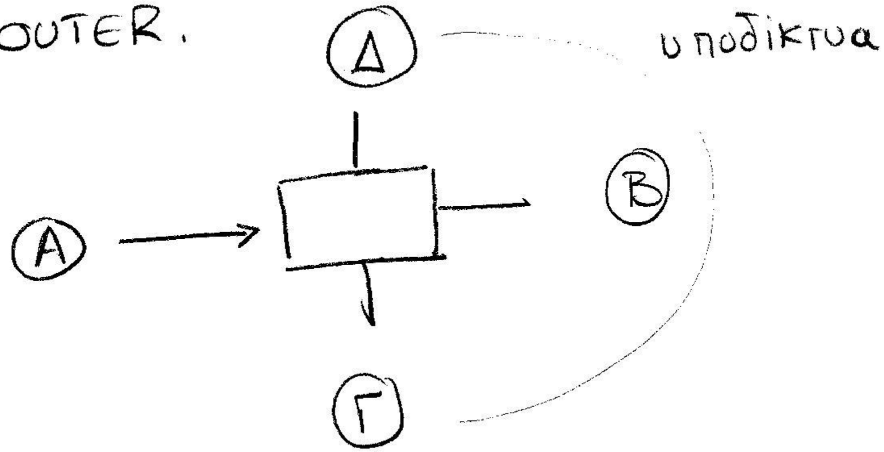
Άρα ο αριθμός υπολογιστή είναι ο 11110010110 =1942

- Θέματα: routers, packet routing/forwarding
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_2016.pdf* :

115,121,124

4

ROUTER.



προώθηση πακέτων με βάση την αντιστοίχιση
(Subnet) IP Address – θύρας σε πίνακα δρομολόγησης

Ο πίνακας δεν έχει self learning

Γίνεται επεξεργασία της διεύθυνσης προορισμού του εισερχόμενου πακέτου με τη subnet mask

IP Address
SUBNET_MASK AND
____
DESTINATION SUBNET ⟶ router port

IP Address
AND
MASK

SUBNET

IP Address
AND
Inverted MASK

PC Number

Subnet → | Network part | host part |

00...0 ← subnet

$\left.\begin{array}{l} 00\ldots01 \\ \vdots \\ 11\ldots10 \end{array}\right\}$ hosts (PCs, Gateway)

11...11 ← broadcast address

IP address
OR
Inverted Mask

---

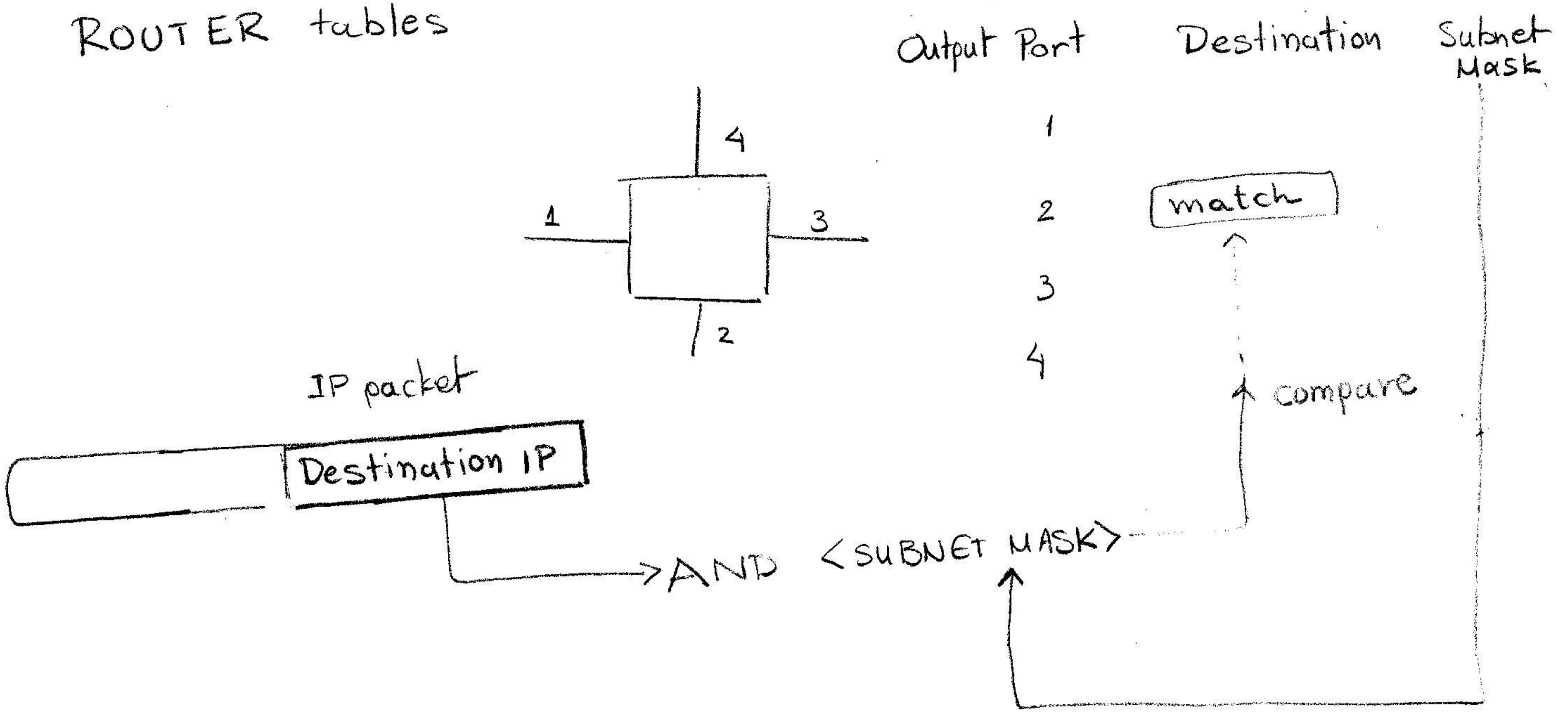
broadcast address

| x | . | y | . | z | . | w |

x AND 255 = x

x OR 0 = x

ROUTER tables



1. Να θεωρήσετε ένα δρομολογητή ο οποίος έχει τον καταχωρημένες τις παρακάτω εγγραφές

Subnet Number	Next Hop
128.96.39.0/25	Interface 0
128.96.39.128/25	Interface 1
128.97.0.9/16	R2
193.96.39.0/25	R3

Να βρείτε το next hop, αν θεωρήσετε ότι ο router λαμβάνει IP πακέτο για κάθε μια από τις περιπτώσεις (Να δικαιολογήσετε την απάντηση σας)
a) 128.96.39.132
β) 193.96.39.34

Θα πρέπει να γίνει η λογική πράξη AND μεταξύ της IP διεύθυνσης και της Subnet Mask. Αν η IP διεύθυνση ταιριάζει με κάποιο από τα records (με βάση το ".longest prefix matching"), το αντίστοιχο interface θα επιλεγεί.

α) 128. 96. 39. 132=> 128. 96. 39. 10000100
255. 255. 255. 128=> 255. 255.255. 10000000 (Μάσκα /25)
----
128. 96. 39. 128=> υπάρχει στην δεύτερη γραμμή
Το επόμενο hop θα είναι προς το Interface 1

Subnet Number	Next Hop
128.96.39.0/25	Interface 0
128.96.39.128/25	Interface 1
128.97.0.9/16	R2
193.96.39.0/25	R3

β) Κάνουμε τη λογική πράξη AND της 193.96.39.34 με την Μάσκα /25

193. 96. 39. 34=> 193. 96. 39. 00100100

255. 255. 255. 128=> 255. 255.255. 10000000

----

193. 96. 39. 0=> υπάρχει στην τέταρτη γραμμή

Το επόμενο hop θα είναι προς το R3

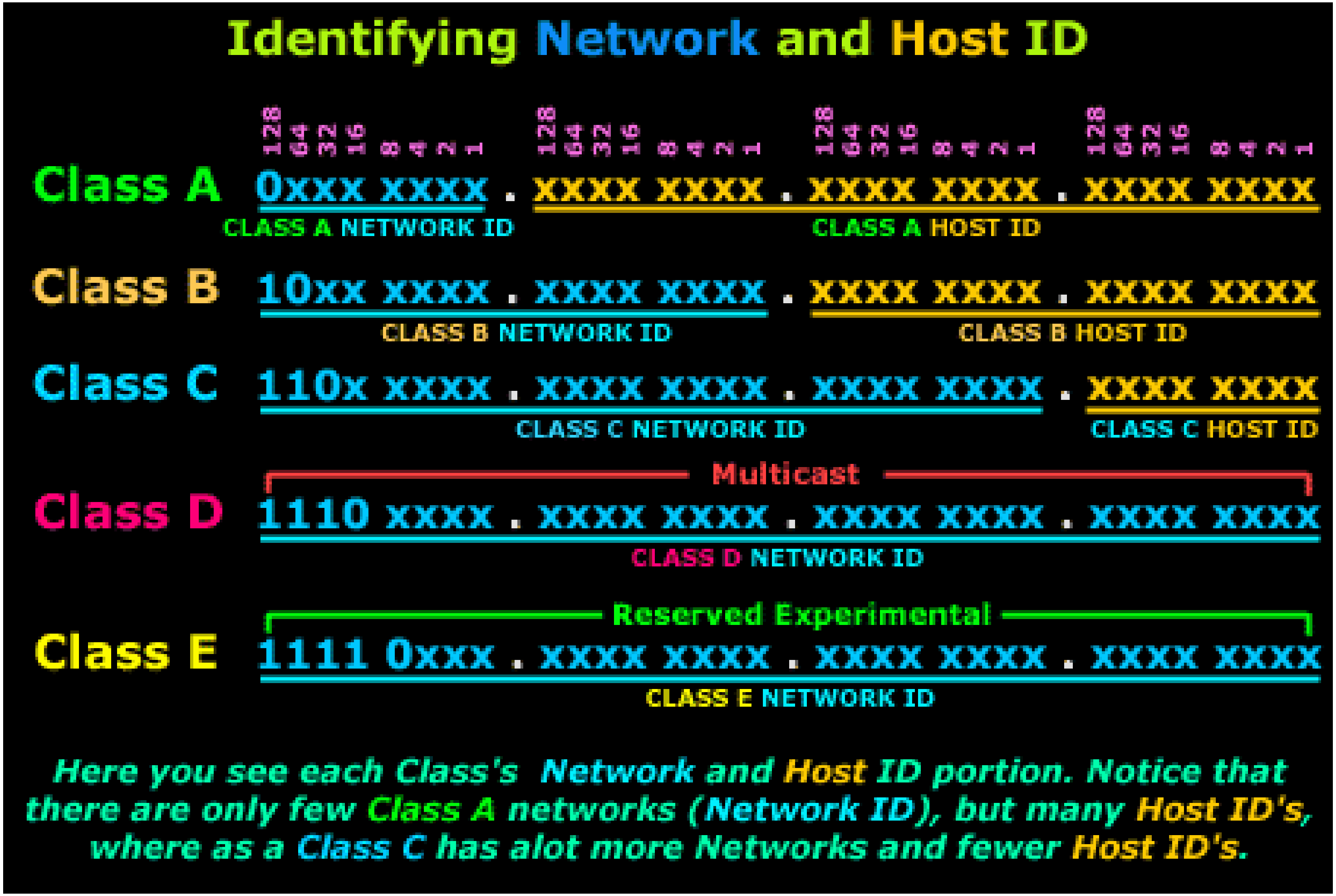
Παράδειγμα longest prefix match: Όταν ταιριάζουν με το υποδίκτυο προορισμού περισσότερες της μιας καταχωρίσεις σε έναν πίνακα δρομολόγησης

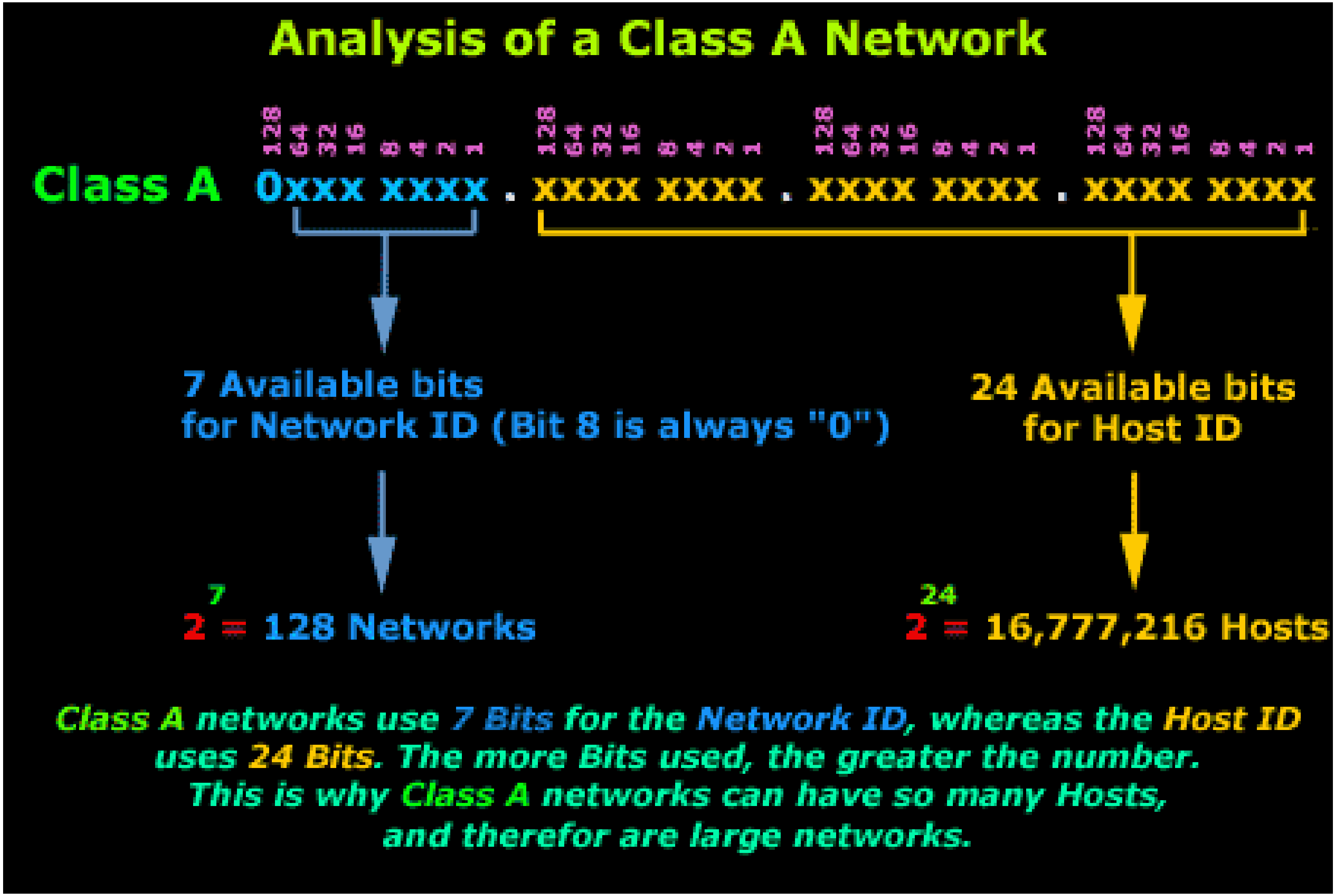
For example, consider this IPv4 forwarding table (CIDR notation is used):

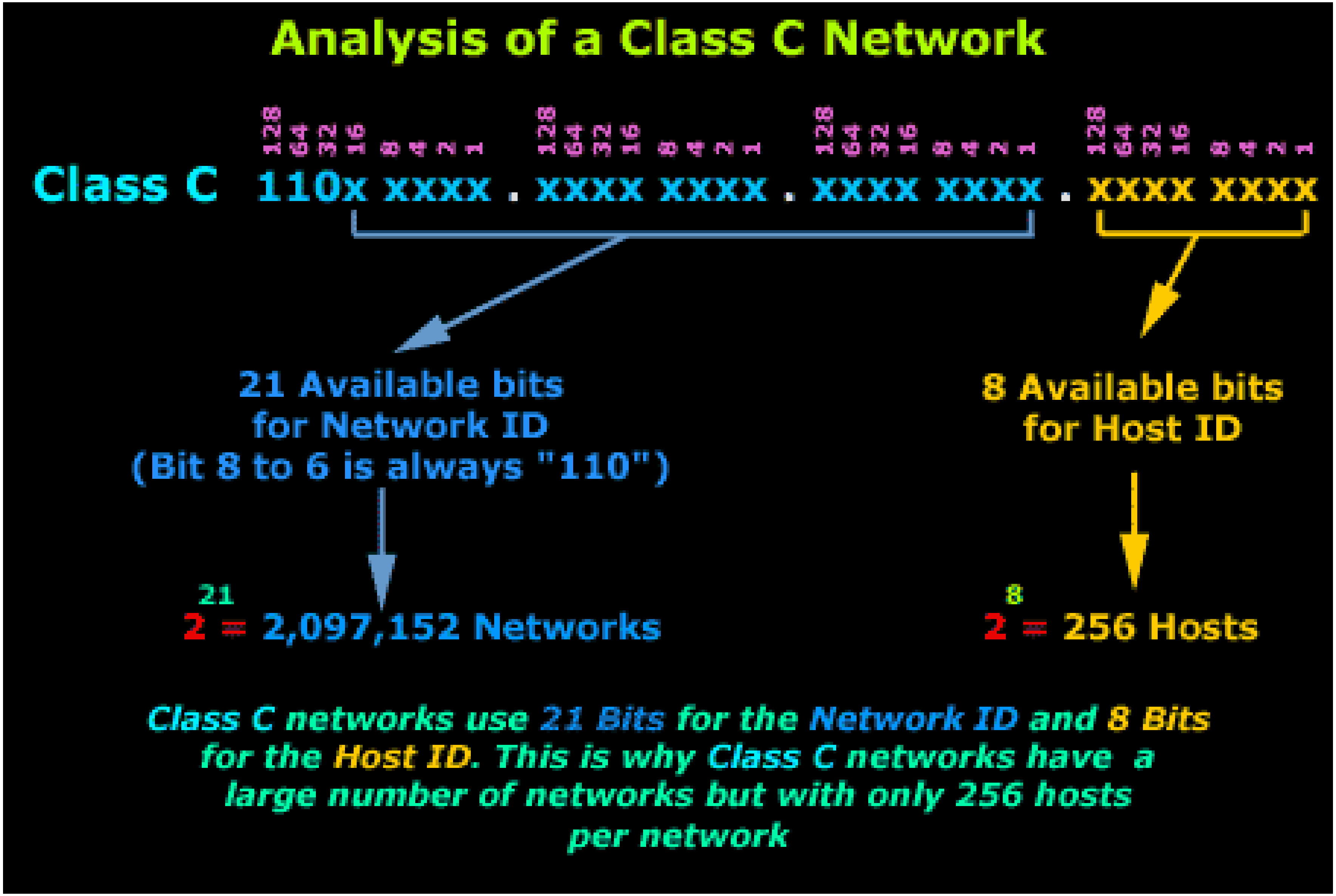
```
192.168.20.16/28
192.168.0.0/16
```

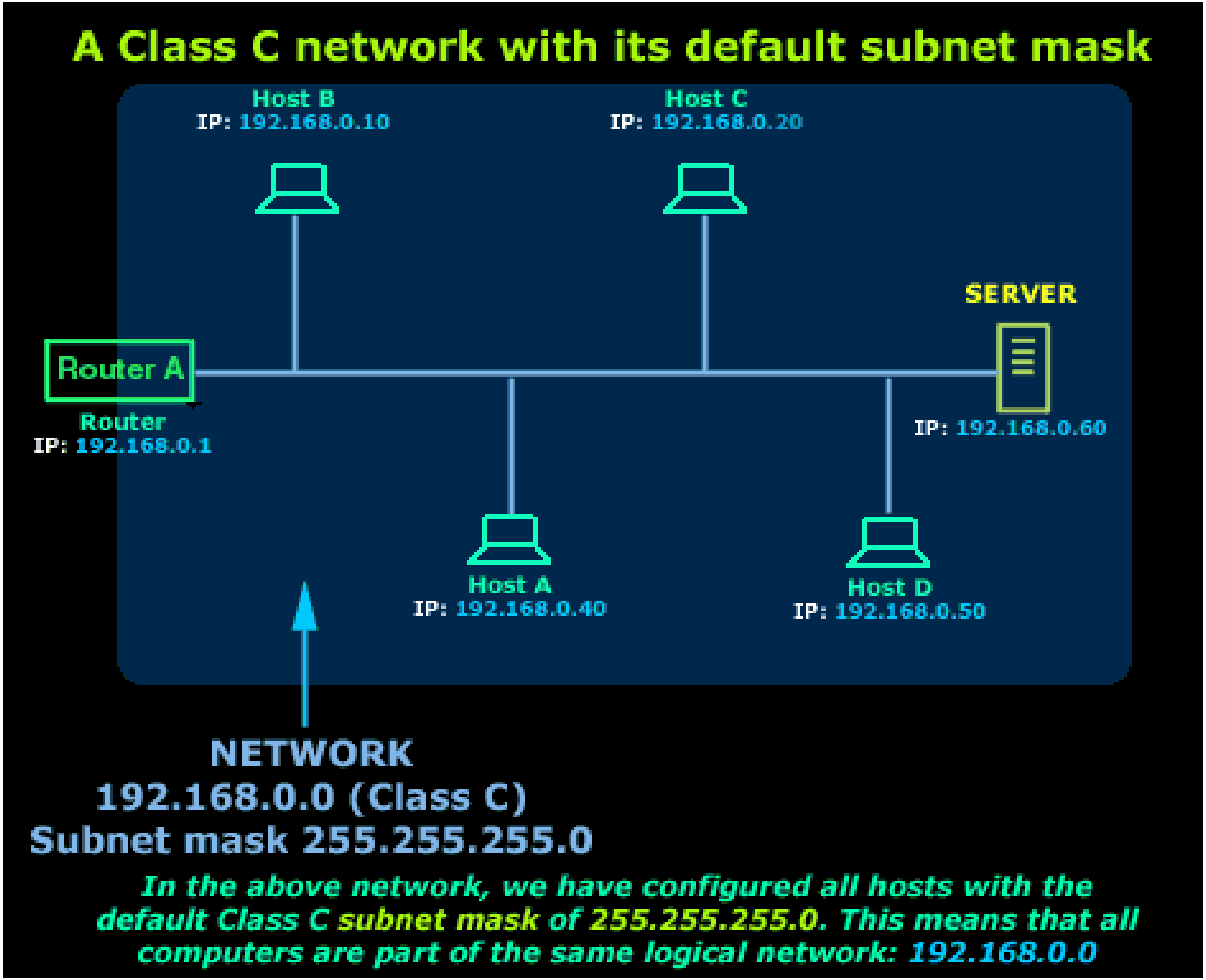
When the address `192.168.20.19` needs to be looked up, both entries in the forwarding table "match". That is, both entries contain the looked up address. In this case, the longest prefix of the candidate routes is `192.168.20.16/28`, since its subnet mask (/28) is longer than the other entry's mask (/16), making the route more specific.

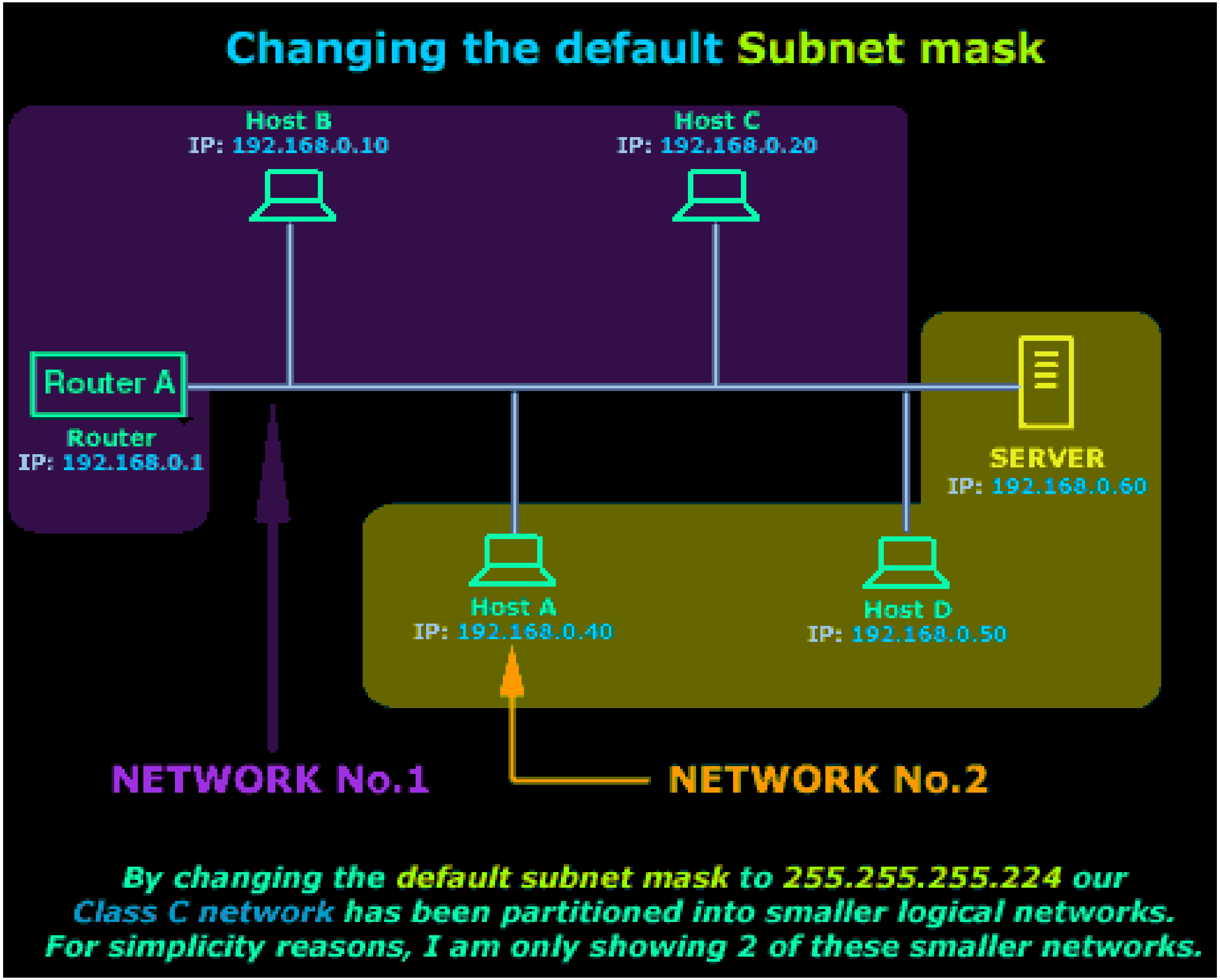
Forwarding tables often contain a default route, which has the shortest possible prefix match, to fall back on in case matches with all other entries fail.

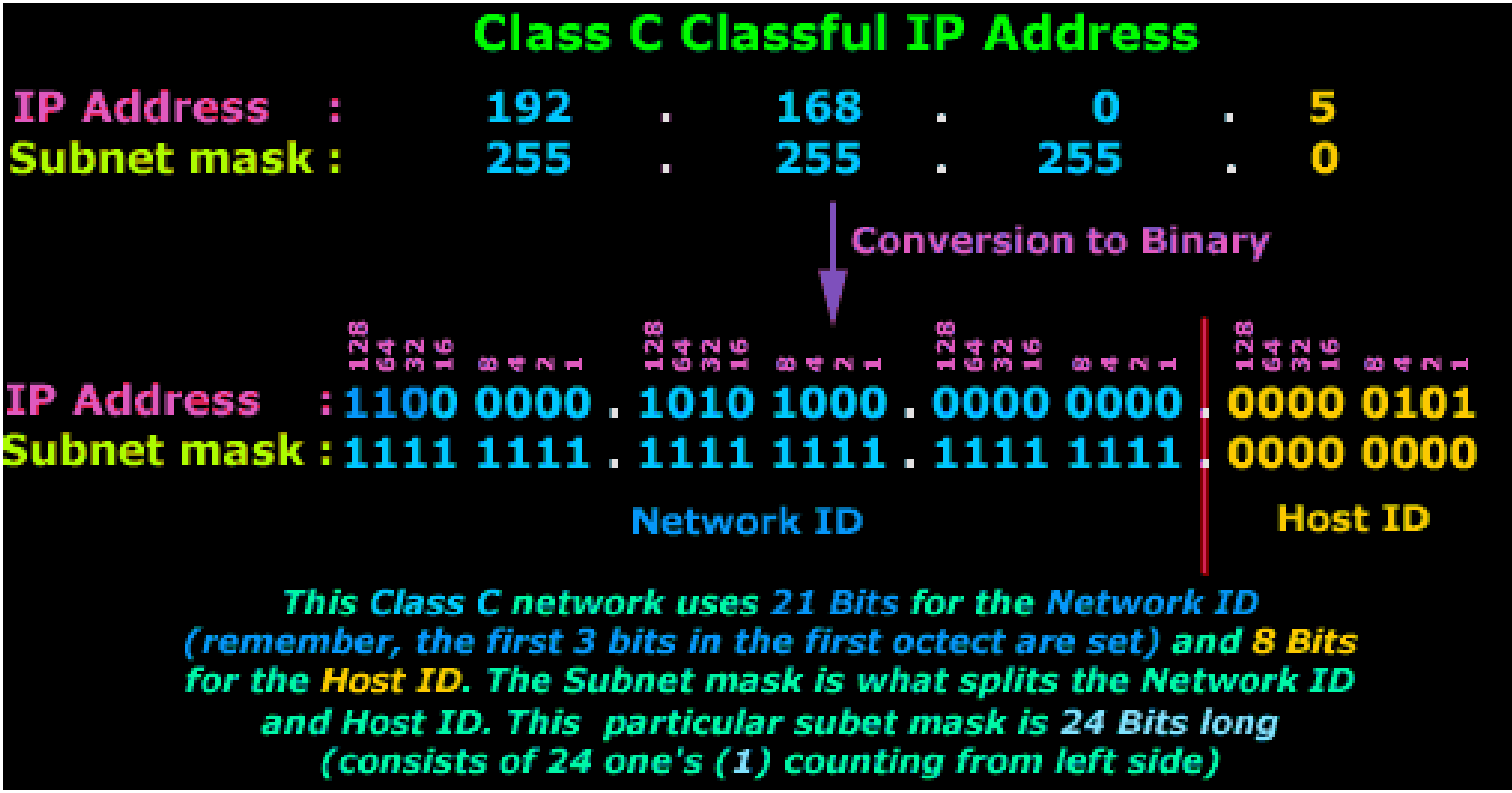

Identifying Network and Host ID
128 64 32 16 8 4 2 1
Class A 0xxx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS A NETWORK ID
CLASS A HOST ID
Class B 10xx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS B NETWORK ID
CLASS B HOST ID
Class C 110x xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS C NETWORK ID
CLASS C HOST ID
Multicast
Class D 1110 xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS D NETWORK ID
Reserved Experimental
Class E 1111 0xxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS E NETWORK ID
Here you see each Class's Network and Host ID portion. Notice that there are only few Class A networks (Network ID), but many Host ID's, where as a Class C has alot more Networks and fewer Host ID's.


Analysis of a Class A Network
128 64 32 16 8 4 2 1
Class A 0xxx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
7 Available bits
for Network ID (Bit 8 is always "0")
24 Available bits
for Host ID
2^7 = 128 Networks
2^24 = 16,777,216 Hosts
Class A networks use 7 Bits for the Network ID, whereas the Host ID uses 24 Bits. The more Bits used, the greater the number.
This is why Class A networks can have so many Hosts, and therefor are large networks.


Analysis of a Class C Network
128 64 32 16 8 4 2 1
Class C 110x xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
21 Available bits
for Network ID
(Bit 8 to 6 is always "110")
8 Available bits
for Host ID
2^21 = 2,097,152 Networks
2^8 = 256 Hosts
Class C networks use 21 Bits for the Network ID and 8 Bits for the Host ID. This is why Class C networks have a large number of networks but with only 256 hosts per network


A Class C network with its default subnet mask
Host B
IP: 192.168.0.10
Host C
IP: 192.168.0.20
SERVER
Router A
Router
IP: 192.168.0.1
IP: 192.168.0.60
Host A
IP: 192.168.0.40
Host D
IP: 192.168.0.50
NETWORK
192.168.0.0 (Class C)
Subnet mask 255.255.255.0
In the above network, we have configured all hosts with the default Class C subnet mask of 255.255.255.0. This means that all computers are part of the same logical network: 192.168.0.0


Changing the default Subnet mask
Host B
IP: 192.168.0.10
Host C
IP: 192.168.0.20
Router A
Router
IP: 192.168.0.1
SERVER
IP: 192.168.0.60
Host A
IP: 192.168.0.40
Host D
IP: 192.168.0.50
NETWORK No.1
NETWORK No.2
By changing the default subnet mask to 255.255.255.224 our
Class C network has been partitioned into smaller logical networks.
For simplicity reasons, I am only showing 2 of these smaller networks.


Class C Classful IP Address
IP Address : 192 . 168 . 0 . 5
Subnet mask : 255 . 255 . 255 . 0
Conversion to Binary
128 64 32 16 8 4 2 1
IP Address : 1100 0000 . 1010 1000 . 0000 0000 . 0000 0101
Subnet mask : 1111 1111 . 1111 1111 . 1111 1111 . 0000 0000
Network ID
Host ID
This Class C network uses 21 Bits for the Network ID
(remember, the first 3 bits in the first octect are set) and 8 Bits
for the Host ID. The Subnet mask is what splits the Network ID
and Host ID. This particular subet mask is 24 Bits long
(consists of 24 one's (1) counting from left side)

The Analysis Of Our Example - Part 2

128 64 32 16 8 4 2 1

IP Address : 1100 0000 . 1010 1000 . 0000 0000 . 000 0 1010
Subnet mask : 1111 1111 . 1111 1111 . 1111 1111 . 111 0 0000

This part of the IP Address and Subnet mask we take as is. In Decimal this part gives us:
192 . 168 . 0 .
255 . 255 . 255 .

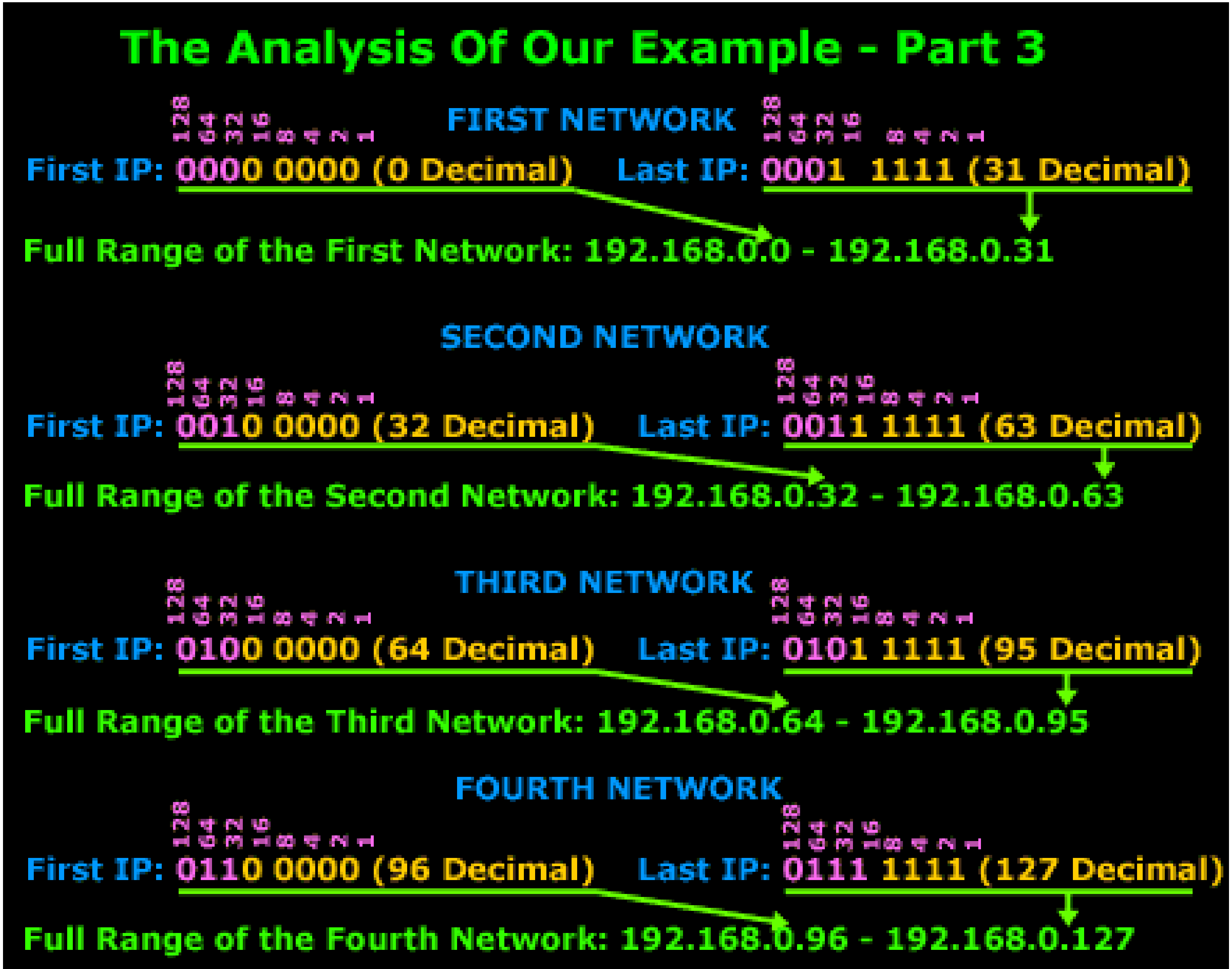
This is the section we focus. From here we will get all the info we are after ! Since I've colour coded the 3 subnet Bits, we won't need the subnet mask anymore to help us determine which bits are borrowed.

128 64 32 16 8 4 2 1

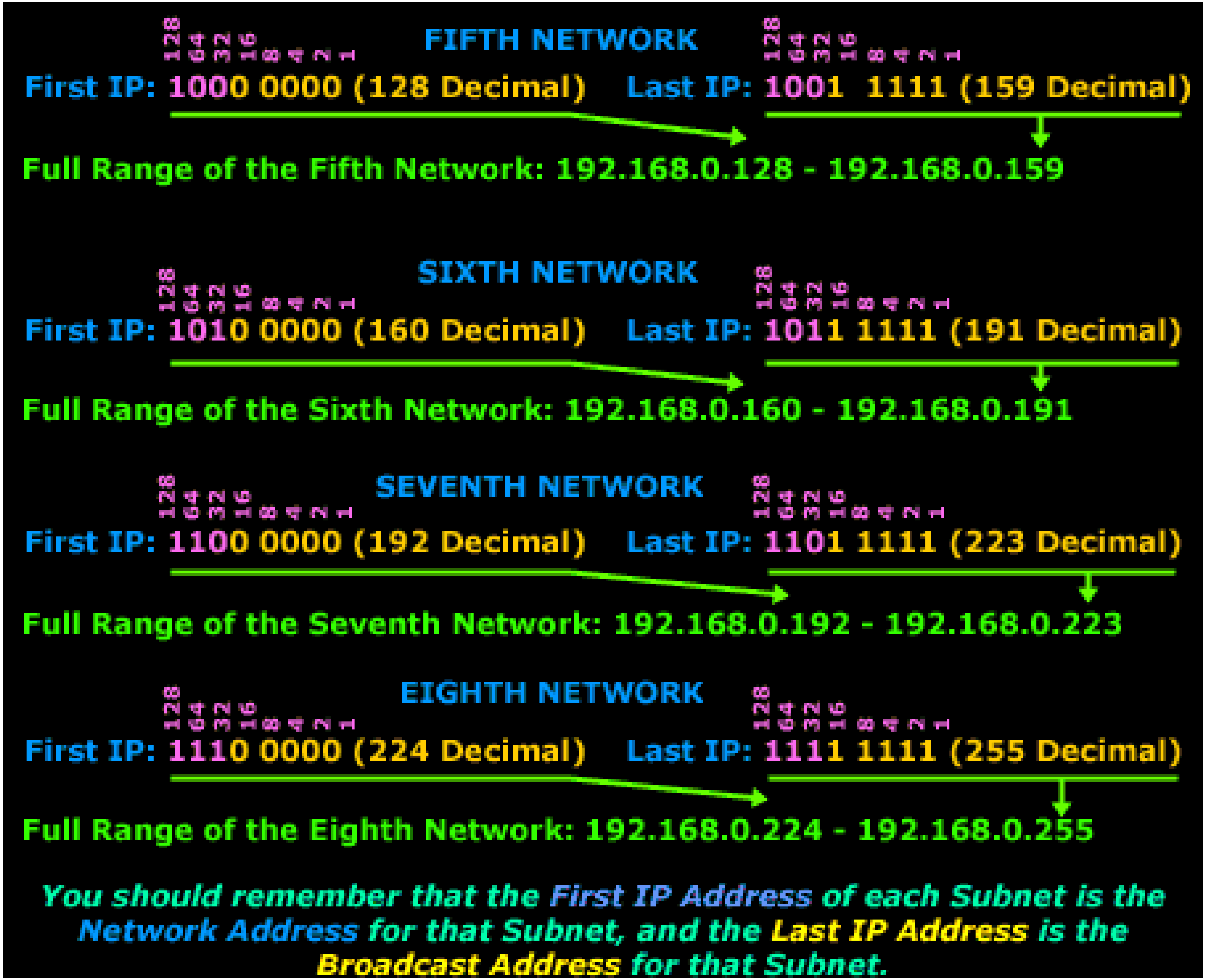
000 0 1010

Determining the Subnets	Determining the Hosts per Subnet
First: 000 (0 Decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)
Second: 001 (32 Decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)
Third: 010 (64 Decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)
Fourth: 011 (96 Decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)
Fifth: 100 (128 Decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)
Sixth: 101 (160 Decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)
Seventh: 110 (192 decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)
Eighth: 111 (224 Decimal)	0 0001 (1 Decimal) to 1 1110 (30 Decimal)

NOTE: 0 0000 (First IP in each subnet) is reserved as the Network Address for the Subnet .
1 1111 (Last IP in each subnet) is reserved as the Broadcast Address for that Subnet



The Analysis Of Our Example - Part 3
FIRST NETWORK
128 64 32 16 8 4 2 1
First IP: 0000 0000 (0 Decimal)
128 64 32 16 8 4 2 1
Last IP: 0001 1111 (31 Decimal)
Full Range of the First Network: 192.168.0.0 - 192.168.0.31
SECOND NETWORK
128 64 32 16 8 4 2 1
First IP: 0010 0000 (32 Decimal)
128 64 32 16 8 4 2 1
Last IP: 0011 1111 (63 Decimal)
Full Range of the Second Network: 192.168.0.32 - 192.168.0.63
THIRD NETWORK
128 64 32 16 8 4 2 1
First IP: 0100 0000 (64 Decimal)
128 64 32 16 8 4 2 1
Last IP: 0101 1111 (95 Decimal)
Full Range of the Third Network: 192.168.0.64 - 192.168.0.95
FOURTH NETWORK
128 64 32 16 8 4 2 1
First IP: 0110 0000 (96 Decimal)
128 64 32 16 8 4 2 1
Last IP: 0111 1111 (127 Decimal)
Full Range of the Fourth Network: 192.168.0.96 - 192.168.0.127


FIFTH NETWORK
128 64 32 16 8 4 2 1
First IP: 1000 0000 (128 Decimal)
128 64 32 16 8 4 2 1
Last IP: 1001 1111 (159 Decimal)
Full Range of the Fifth Network: 192.168.0.128 - 192.168.0.159
SIXTH NETWORK
128 64 32 16 8 4 2 1
First IP: 1010 0000 (160 Decimal)
128 64 32 16 8 4 2 1
Last IP: 1011 1111 (191 Decimal)
Full Range of the Sixth Network: 192.168.0.160 - 192.168.0.191
SEVENTH NETWORK
128 64 32 16 8 4 2 1
First IP: 1100 0000 (192 Decimal)
128 64 32 16 8 4 2 1
Last IP: 1101 1111 (223 Decimal)
Full Range of the Seventh Network: 192.168.0.192 - 192.168.0.223
EIGHTH NETWORK
128 64 32 16 8 4 2 1
First IP: 1110 0000 (224 Decimal)
128 64 32 16 8 4 2 1
Last IP: 1111 1111 (255 Decimal)
Full Range of the Eighth Network: 192.168.0.224 - 192.168.0.255
You should remember that the First IP Address of each Subnet is the Network Address for that Subnet, and the Last IP Address is the Broadcast Address for that Subnet.

Ένας υπολογιστής έχει τις εξής παραμέτρους στο πρωτόκολλο IP:

Διεύθυνση IP	92.213.193.53
Μάσκα υποδικτύου	255.255.252.0
Προεπιλεγμένη πύλη	92.213.193.35

α) Ποιο είναι το μέγιστο πλήθος υπολογιστών που περιλαμβάνει το υποδίκτυο στο οποίο ανήκει ο παραπάνω υπολογιστής; ***(5 μονάδες)***

β) Ποια είναι η πρώτη διεύθυνση του υποδικτύου (ή διεύθυνση υποδικτύου) και ποια η τελευταία διεύθυνση του υποδικτύου (ή διεύθυνση ευρείας εκπομπής - broadcast); ***(5 μονάδες)***

γ) Δύο πακέτα τα οποία αποστέλλονται από τον παραπάνω σταθμό με διευθύνσεις προορισμού 92.213.196.171 και 92.213.194.171 θα παραδοθούν εντός ή εκτός του υποδικτύου στο οποίο ανήκει ο αποστολέας; Αιτιολογείστε την απάντησή σας. ***(5+5=10 μονάδες)***

α) Η μάσκα υποδικτύου : 255.255.252.0 σε δυαδική μορφή είναι:

`255.255.252.0 → 11111111.11111111.11111100.00000000`

άρα τα τελευταία 10 δυαδικά ψηφία χρησιμοποιούνται για τον αριθμό του υπολογιστή ορίζοντας 2^{10}=1.024 συνδυασμούς. Το μέγιστο πλήθος υπολογιστών είναι 1.024-2=1.022 αφού οι διευθύνσεις με αριθμό υπολογιστή 0 (διεύθυνση υποδικτύου) και 1.023 (διεύθυνση broadcast) δεν μπορούν να χρησιμοποιηθούν για IP υπολογιστή.

β) Η πρώτη διεύθυνση του υποδικτύου (ή διεύθυνση υποδικτύου) προκύπτει αν θέσουμε τα bits του αριθμού υπολογιστή όλα 0 (λογικό AND ανάμεσα στην IP και στην μάσκα).

IP : 92.213.193.53 → 01011100.11010101.11000001.00110101

Μάσκα υποδικτύου → 11111111.11111111.11111100.00000000

AND

Διεύθυνση υποδικτύου→ 01011100.11010101.11000000.00000000→ **(92.213.192.0)**

Άρα η ζητούμενη τελευταία διεύθυνση του υποδικτύου (ή διεύθυνση broadcast) είναι: **92.213.195.255**

01011100.11010101.11000011.11111111

γ) Για να βρει ο υπολογιστής αν μια IP διεύθυνση προορισμού ανήκει στο ίδιο υποδίκτυο ή όχι, θα πρέπει να διαπιστώσει αν τα bits της δικής του IP διεύθυνσης που αντιστοιχούν στη μάσκα του υποδικτύου στο οποίο ανήκει ο υπολογιστής, ταυτίζονται με τα αντίστοιχα bits της IP διεύθυνσης προορισμού. Δηλαδή.

IP (προορ) :	92.213.196.171	→	01011100.11010101.11000**1**00.10101011
IP (υπολ):	92.213.193.53	→	01011100.11010101.11000**0**01.00110101
	255.255.252.0	→	11111111.11111111.11111100.00000000

Είναι φανερό ότι οι δύο IP διευθύνσεις διαφέρουν σε κάποιο από τα πρώτα 22 bits (που είναι 1) της μάσκας, και συγκεκριμένα στο ενδέκατο από δεξιά bit. Άρα η διεύθυνση προορισμού δεν βρίσκεται το ίδιο υποδίκτυο. Το IP πακέτο πρέπει να σταλεί στον δρομολογητή (προεπιλεγμένη πύλη) που συνδέει τον υπολογιστή με το διαδίκτυο, άρα η διεύθυνση του επόμενου άλματος είναι η 92.213.193.35.

Ομοίως και για την IP διεύθυνση προορισμού 92.213.194.171

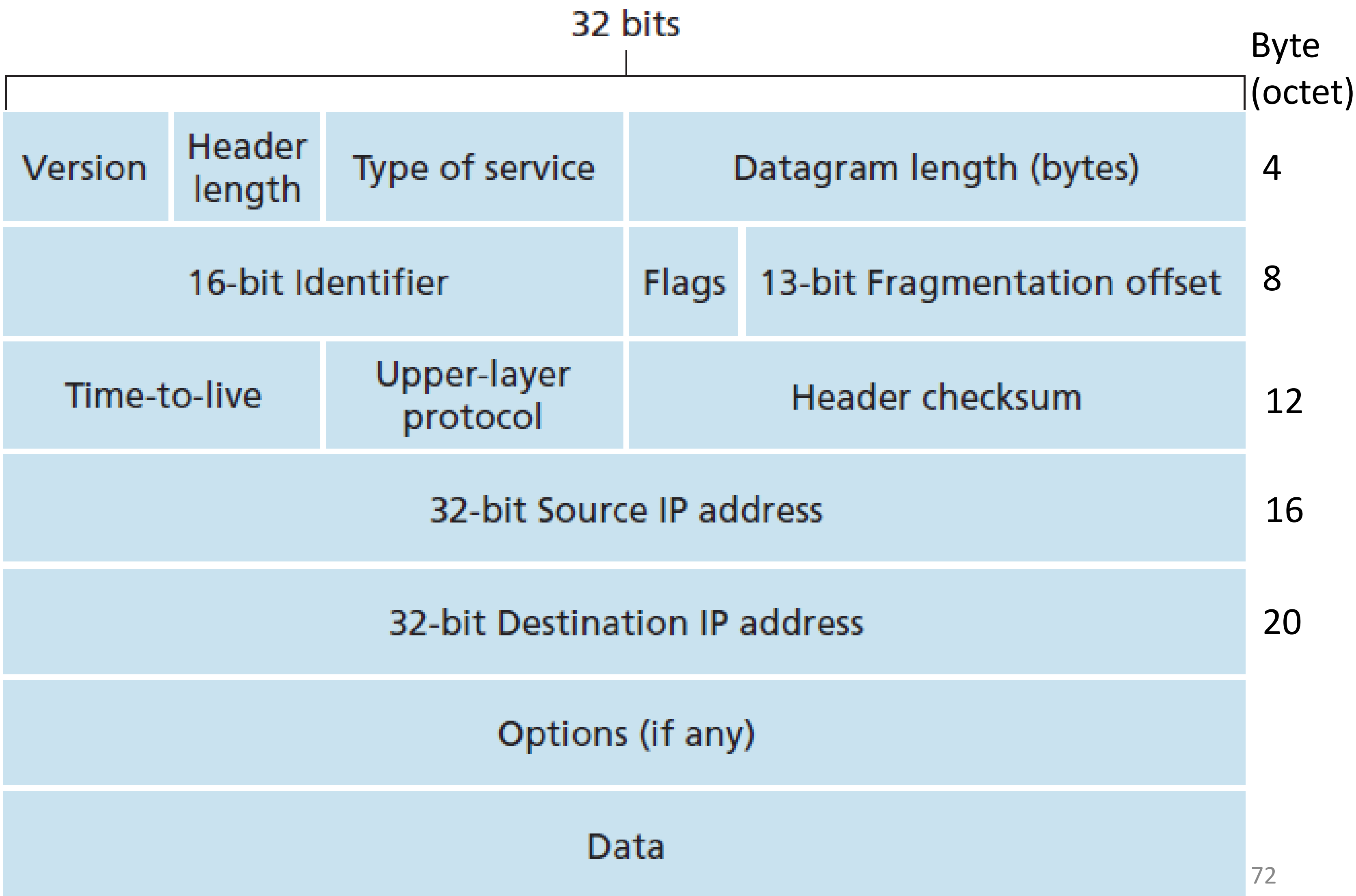
IP (προορ) :	92.213.194.171	→	01011100.11010101.11000**0**10.10101011
IP (υπολ):	92.213.193.53	→	01011100.11010101.11000**0**01.00110101
	255.255.252.0	→	11111111.11111111.11111100.00000000

Είναι φανερό ότι οι δύο IP διευθύνσεις δεν διαφέρουν σε κάποιο από τα πρώτα 22 bits (που είναι 1) της μάσκας. Άρα η διεύθυνση προορισμού βρίσκεται το ίδιο υποδίκτυο το 92.213.192.0. Το IP πακέτο θα σταλεί μέσω MAC απευθείας στον υπολογιστή με IP διεύθυνση αυτή του προορισμού δηλαδή 92.213.194.171.

- Θέματα: IP Datagram, MTU, Fragmentation
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_2016.pdf* :

117-119, 128,129

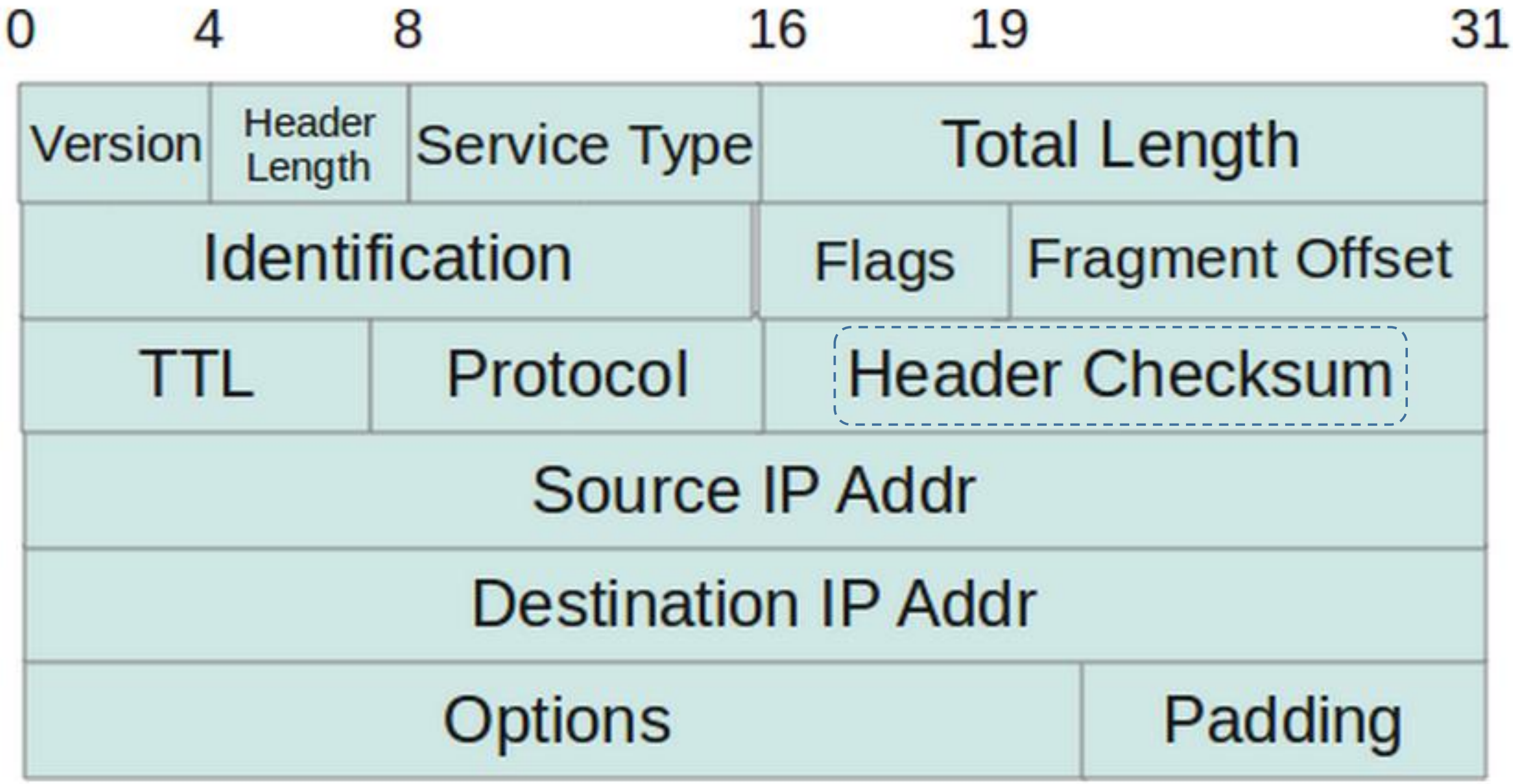
IPv4 Datagram format



IP header Checksum

- Check sum: Χρησιμοποιείται για την ανίχνευση λαθών στην επικεφαλίδα του IP datagram
  - (χρησιμοποιείται και σε άλλους τύπους πακέτων/πλαισίων σε άλλα OSI επίπεδα)
- Αποστολέας: Υπολογίζει το checksum και το προσθέτει στο σχετικό πεδίο της επικεφαλίδας.
- Παραλήπτης:
  - Υπολογίζει εκ νέου το checksum και το συγκρίνει με την τιμή που υπάρχει στο σχετικό πεδίο
  - (Ισοδύναμα) Αθροίζει όλα τα πεδία της επικεφαλίδας (και το checksum field) και ελέγχει αν το αποτέλεσμα είναι 0.

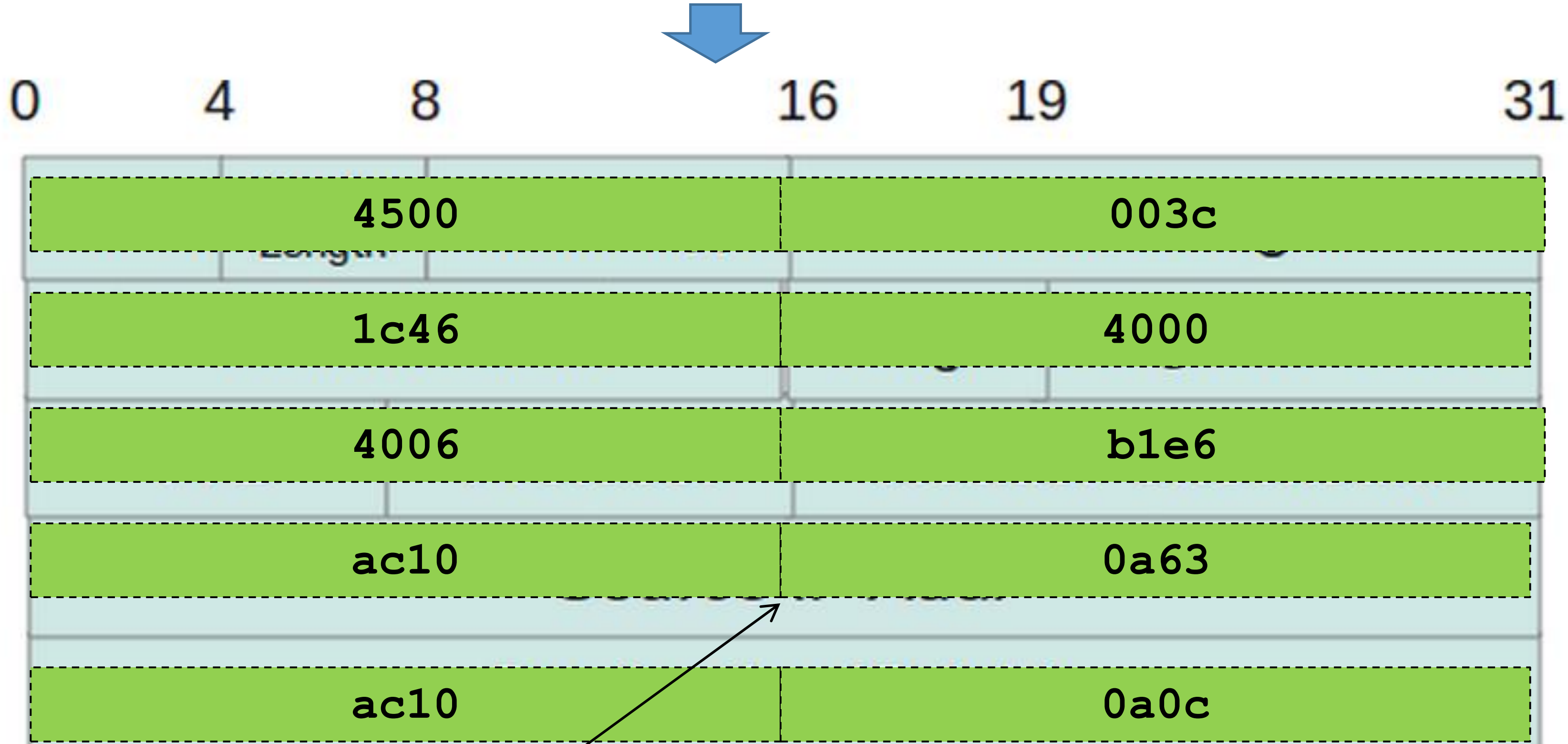
Checksum of IP header



- Το IP header checksum λαμβάνει υπόψη μόνο τα Bytes της επικεφαλίδας. Το τμήμα δεδομένων (που ουσιαστικά περιλαμβάνει ένα TCP ή UDP segment έχει ξεχωριστό – ανεξάρτητο- μηχανισμό υπολογισμού checksum (στο επίπεδο μεταφοράς)

Παράδειγμα: Έστω η ληφθείσα IP header

4500 003c 1c46 4000 4006 b1e6 ac10 0a63 ac10 0a0c



Κάθε δεκαεξαδικό ψηφίο αντιστοιχεί σε ένα 4-μπιτο δυαδικό αριθμό
π.χ. source IP address a c.1 0.0 a.6 3=
1010 1100.0001 0000.0000 1010.0110 0011=172.16.10.99

Ανάλυση IP header (για το παράδειγμα)

- Η προηγούμενη επικεφαλίδα (hexadecimal)

`4500 003c 1c46 4000 4006 b1e6 ac10 0a63 ac10 0a0c`

- ’**45**’:
  - ’4’ -> IP version, ’5’ ->header length. Μέγεθος header 5×4=20 bytes.
- ’**00**’ : type of service / normal operation.
- ’**003c**’ : Συνολικό μήκος IP datagram.
  - Στην περίπτωση του παραδείγματος είναι 60 bytes

    ($\mathbf{0\ 0\ 3\ c} = \mathbf{0} \times 16^4 + \mathbf{0} \times 16^3 + \mathbf{3} \times 16^1 + \mathbf{c} \times 16^0 = 48+12=60$)
- ’**1c46**’ : identification field.
- ’**4000**’ αντιστοιχεί σε 2 bytes (16 bits) για τη διαδικασία fragmentation.
  - 3 bits για flags και 13 bits για fragment offset.
- ’**4006**’:
  - ’40’ -> TTL field, ’06’ -> protocol field of the IP header (06->TCP).
- **‘b1e6’ : checksum υπολογισμένο από τον αποστολέα**
- ‘**ac100a63**’ : IP address αποστολέα
- **’ac100a0c’** : IP address παραλήπτη.

IP header checksum -παράδειγμα

Βήμα 1ο

- Δημιουργία γραμμών που αποτελούνται από 4 16δικά ψηφία (‘μισή’ γραμμή του IP header-2 δυαδικά bytes)
- Μετατροπή hex -> binary (κάθε 16δικό ψηφίο μετατρέπεται στον αντίστοιχο 4-μπιτο δυαδικό)

```
4500 -> 0100010100000000
003c -> 0000000000111100
1c46 -> 0001110001000110
4000 -> 0100000000000000
4006 -> 0100000000000110
0000 -> 0000000000000000
ac10 -> 1010110000010000
0a63 -> 0000101001100011
ac10 -> 1010110000010000
0a0c -> 0000101000001100
```

Το checksum πεδίο τίθεται ίσο με 0

Βήμα 2ο

Άθροιση όλων των γραμμών
με κρατούμενα

```
            1
 1 1 1 1 1               1 1 1 1 1
 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0
 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0
 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0
 0 0 0 0 1 0 1 0 0 1 1 0 0 0 1 1
 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0
 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0
---------------------------------
1 1 0 1 0 0 1 1 1 0 0 0 0 1 0 1 1 1
```

Τελικά κρατούμενα

Ενδιάμεσο αποτέλεσμα

ΕΑΠ/ΠΛΗ22/ΑΘΗ.4/5η
ΟΣΣ/23.04.2016/Ν.Δημητρίου

Βήμα 3ο

Άθροιση των τελικών κρατουμένων στο αποτέλεσμα

Ενδιάμεσο αποτέλεσμα προηγούμενης διαφάνειας

Τελικά Κρατούμενα προηγούμενης διαφάνειας

~~1~~

1 ~~1~~ ~~1~~ ~~1~~

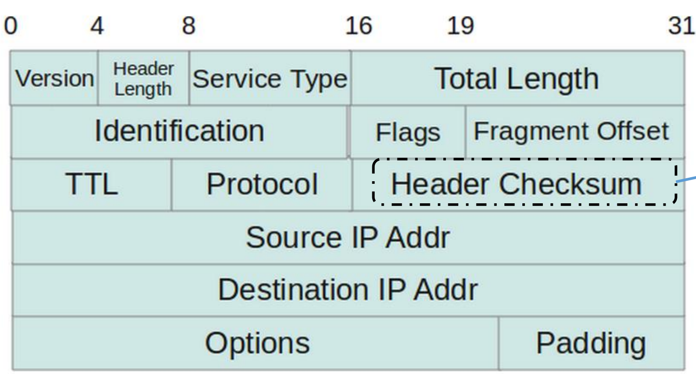
0 1 0 0 1 1 1 0 0 0 0 1 0 ~~1~~ ~~1~~ 1

0 1 0 0 1 1 1 0 0 0 0 1 1 0 0 1 **Τελικό αποτέλεσμα**

Συμπλήρωμα ως προς 1 του τελικού αποτελέσματος

1 0 1 1 0 0 0 1 1 1 1 0 0 1 1 0 **checksum**

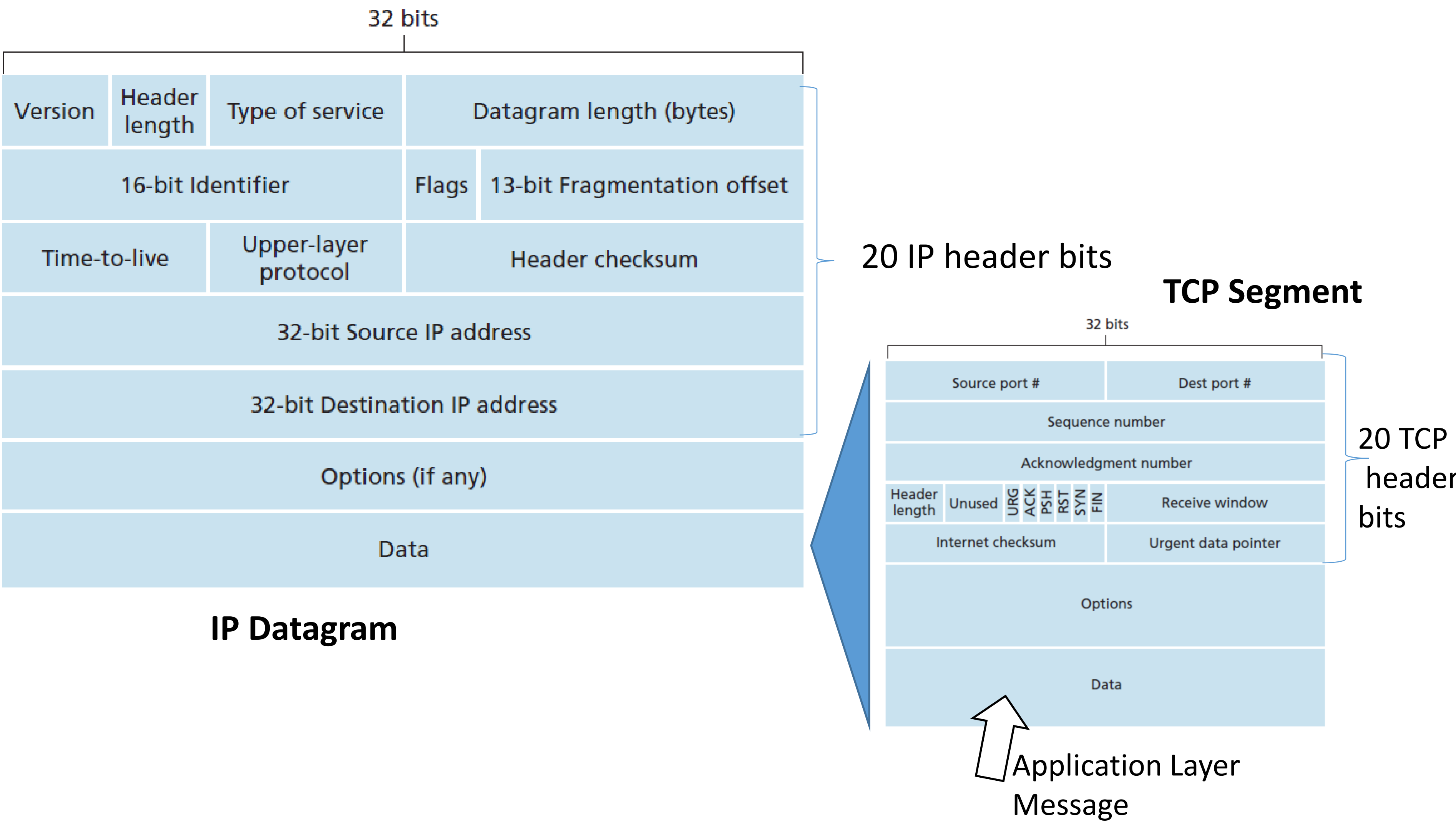
b 1 e 6 **Μετατροπή σε δεκαεξαδικό**



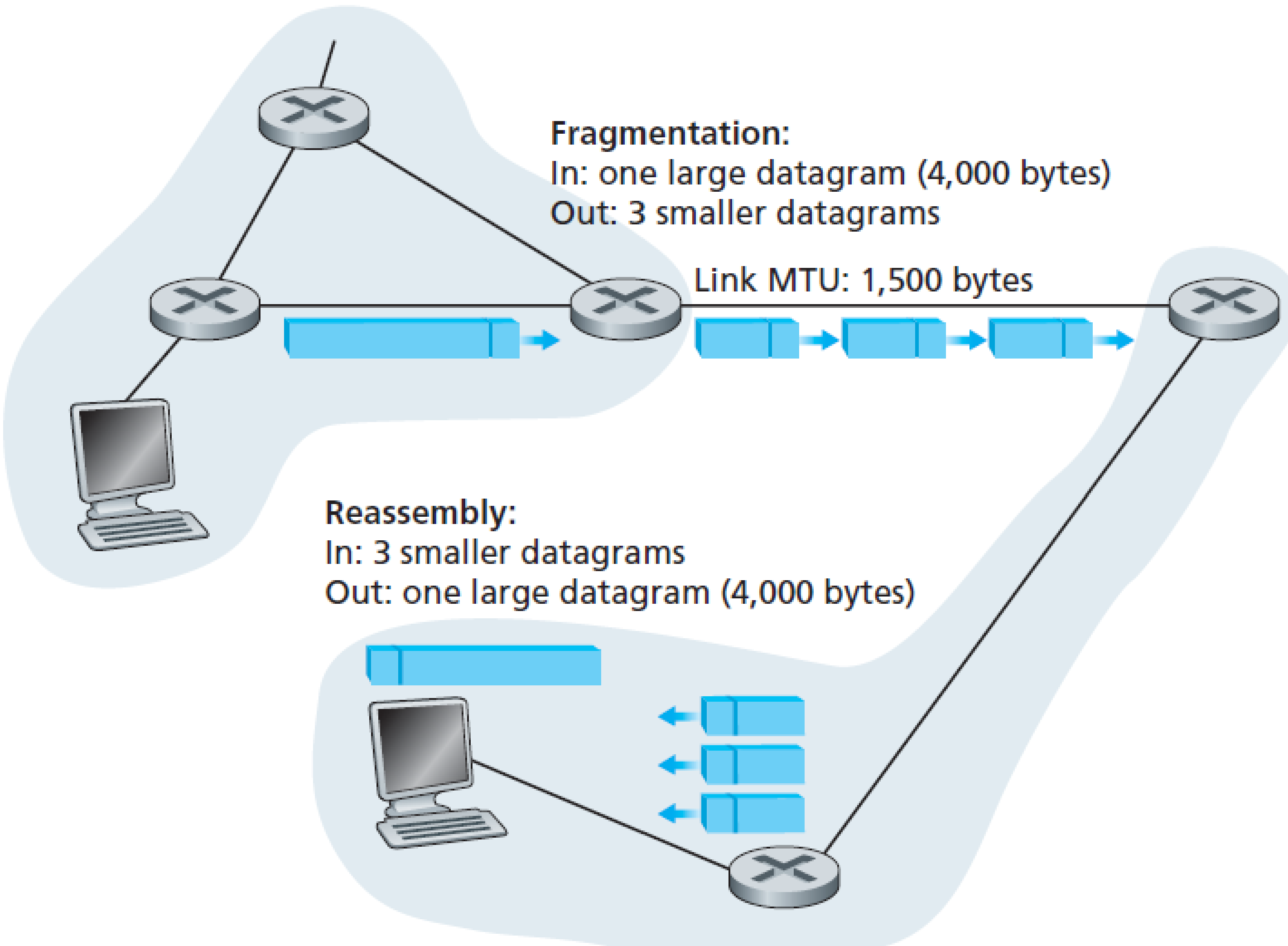
b1e6

Σύγκριση με το checksum που είχε προσθέσει ο αποστολέας στο σχετικό πεδίο.
Είναι ίσα, άρα στο header δεν ανιχνεύεται σφάλμα

Encapsulation of TCP Segment in IP Datagram



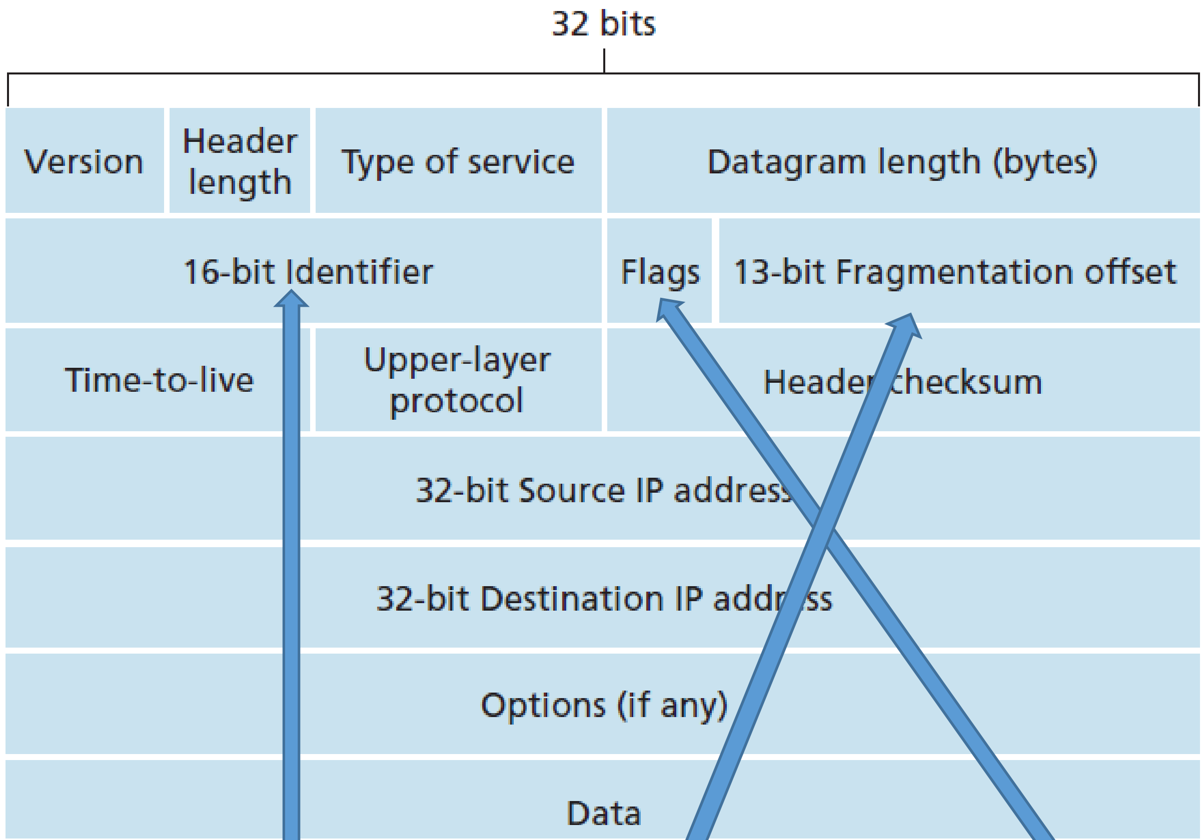
IP Fragmentation



Fragmentation Example

- A datagram of 4,000 bytes (20 bytes of IP header plus 3,980 bytes of IP payload) arrives at a router and must be forwarded to a link with an MTU of 1,500 bytes.
- The 3,980 data bytes in the original datagram must be allocated to three separate fragments
- Suppose that the original datagram is stamped with an identification number of 777.
- The amount of original payload data in all but the last fragment is a multiple of 8 bytes, and the offset value is specified in units of 8-byte chunks.

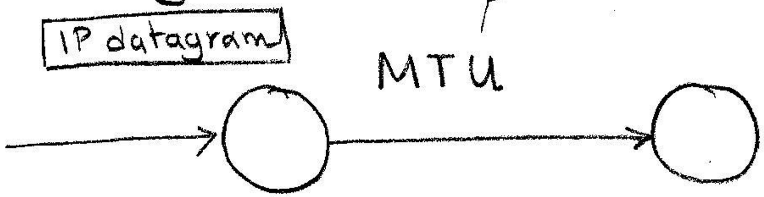
Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that $185 \cdot 8 = 1{,}480$)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that $370 \cdot 8 = 2{,}960$)	flag = 0 (meaning this is the last fragment)



Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

IP fragmentation

Maximum Transmission Unit



Data bytes = Datagram-Size - header

If Data Butes > MTU - header

Fragmentation

1st fragment $\underbrace{\overbrace{\left\lfloor \frac{MTU-(IP\_header)}{8} \right\rfloor}^{\text{offset}} \times 8}_{\text{1st fragment data}} + IP\_header$

Remaining bytes = (Data-Bytes) - (1st fragment data).

If Remaining-data > MTU - header

Repeat

else last fragment $\boxed{\text{Remaining-data + header}}$

Datagram 4000 bytes (3980 data + 20 bytes header)

MTU = 1500 bytes

4000 > MTU

Fragmentation

1st Fragment $\left\lfloor \frac{1500-20}{8} \right\rfloor \times 8 + 20 = \overbrace{185 \times 8}^{1480} + 20 = 1500$

offset : 0

Remaining bytes: 3980 − 1480 = 2500 > MTU − 20

2nd Fragment 1480 + 20 = 1500 bytes offset: 185

Remaining bytes 2500 − 1480 = 1020 < $\underbrace{\text{MTU} - 20}_{1480}$ offset $2 \times 185 = 370$

3rd Fragment 1020 + 20 = 1040 bytes

- Θέματα: ARP description, ARP examples
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_2016.pdf* :

155,156,157,159,160

Address Resolution Protocol (ARP)

- Both types of addresses:
  - network-layer addresses (for example, Internet IP addresses)
  - link-layer addresses (that is, MAC addresses), there is a need to translate
- ARP resolves an IP address to a MAC address
- it
- Analogous to DNS, which resolves host names to IP addresses.
- However DNS resolves host names for hosts anywhere in the Internet, whereas ARP resolves IP addresses only for hosts and router interfaces on the same subnet.

How it works

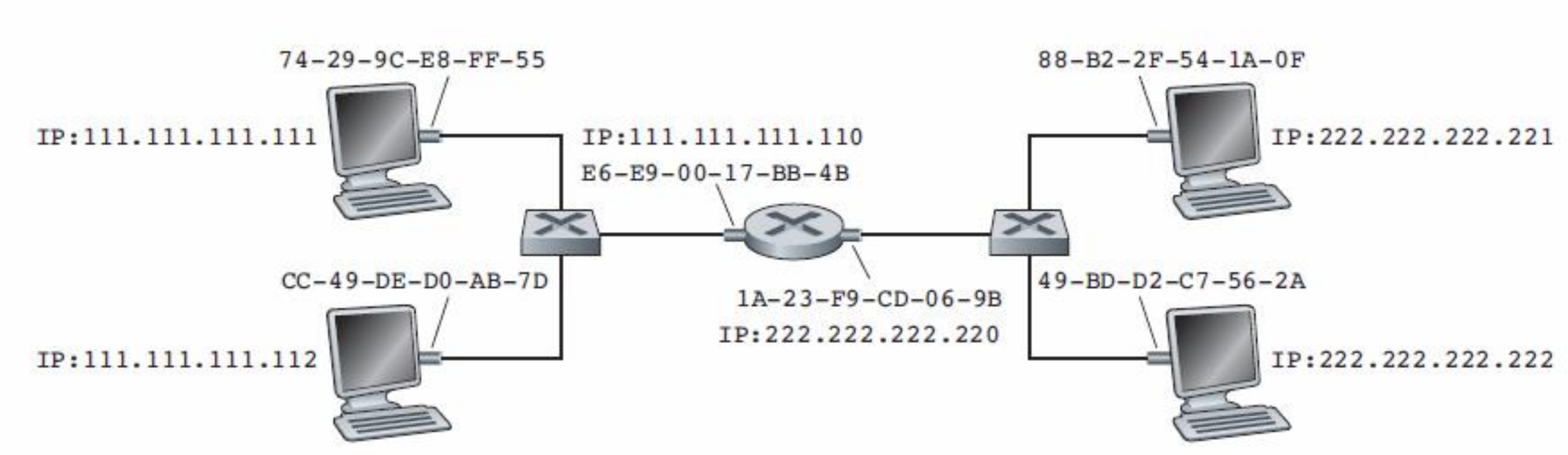
- Each host and router has an **ARP table in its memory:**
  - **contains mappings of IP** addresses to MAC addresses.
  - also contains a time-to-live (TTL) value, which indicates when each mapping will be deleted from the table.
  - typical expiration time for an entry: 20 minutes

IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

ARP protocol operation

- Suppose host wants to send a datagram that is IP addressed to another host or router **on that** subnet.
- The sending host needs to obtain the MAC address of the destination given the IP address.
- If the sender's ARP table has an entry for the destination node, OK.
- If the ARP table doesn't currently have an entry for the destination the sender uses the ARP protocol to resolve the address:
  1. The sender constructs a special **ARP query packet**.
     - This packet includes sender IP and MAC addresses, IP address of the destination node and a broadcast MAC address FF-FF-FF-FF-FF-FF.
  2. All nodes in the subnet receive the ARP query packet and check their ARP tables.
  3. If a match is found, an ARP reply packet with the requested MAC address is sent back to the sender to update its own ARP table

ARP protocol operation (II)



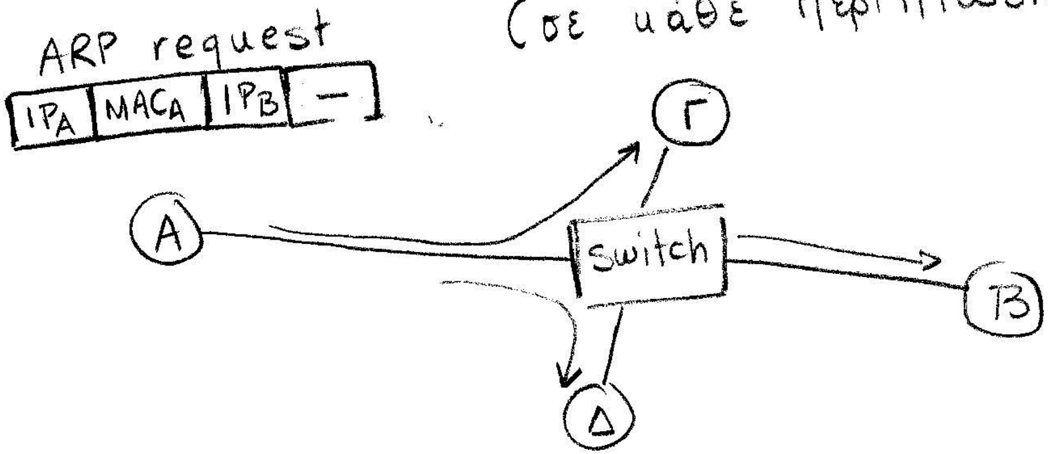
host 111.111.111.111 wants to send an IP datagram to a host 222.222.222.222.

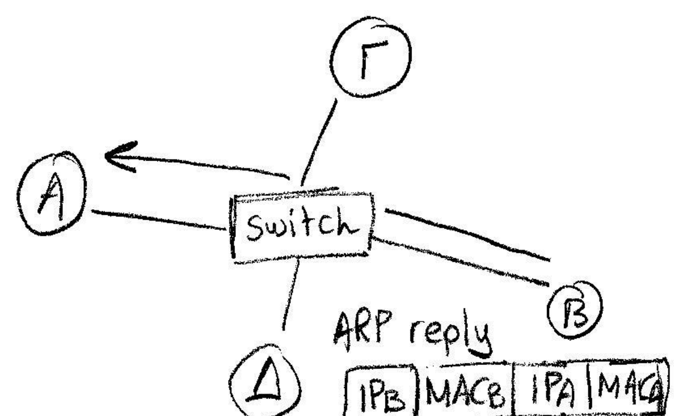
- What MAC address should the adapter use?
- If it uses directly 49-BD-D2-C7-56-2A,
  - none of the adapters on Subnet 1 would pass the IP datagram up to its network layer, (the frame's destination MAC address would not match the MAC address of any adapter on Subnet 1).
- Solution: the appropriate MAC address for the frame is the address of the adapter for router interface 111.111.111.110, namely, E6-E9-00-17-BB-4B (obtained via ARP).

ARP protocol. (IP address resolution)

Προκειμένου να λάβει ο παραλήπτης ένα πακέτο χρειάζεται ο αποστολέας να γνωρίζει

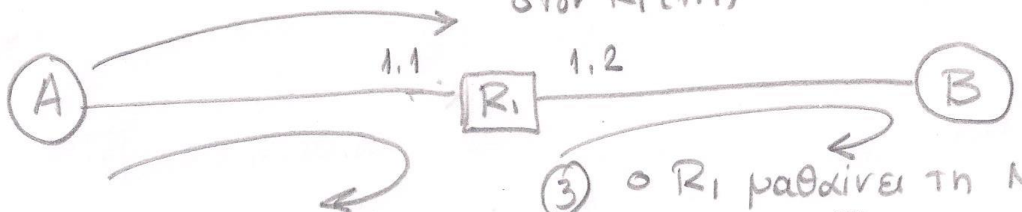
- τη MAC address του παραλήπτη (αν είναι στο ίδιο υποδίκτυο)
- την IP address του παραλήπτη (σε κάθε περίπτωση)





ARP protocol
(router)

② ο A στέλνει το πακέτο data
στον R_1 (1.1)



③ ο R_1 μαθαίνει τη MAC address
του B

① ο A μαθαίνει
την MAC address
του R_1 (1.1)

ο R_1 (1.2) στέλνει το πακέτο
data στον B
④

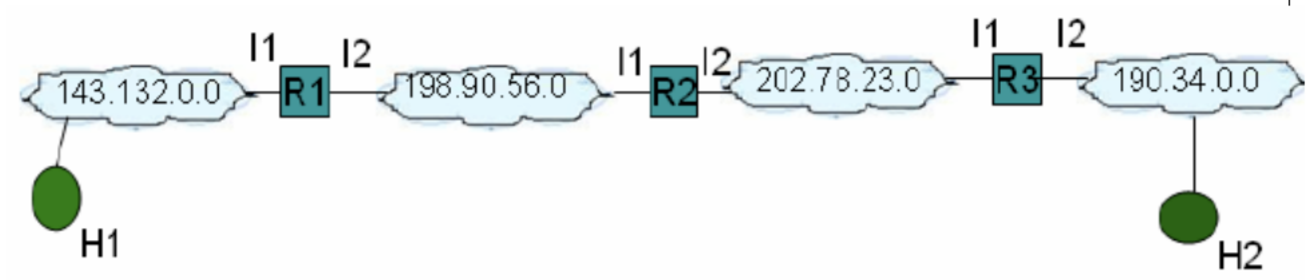
ΘΕΜΑ 1

ΓΕ4/1314

Στόχος της άσκησης *είναι η εξοικείωση με τις τεχνολογίες Ethernet και TCP/IP*

Μεθοδολογία Άσκησης: *Θα πρέπει να μελετήσετε τις λυμένες ενδεικτικές ασκήσεις σχετικά με Hub, Bridge, Switching και IP Forwarding, ARP*

2. Δίνεται το δίκτυο του παρακάτω σχήματος

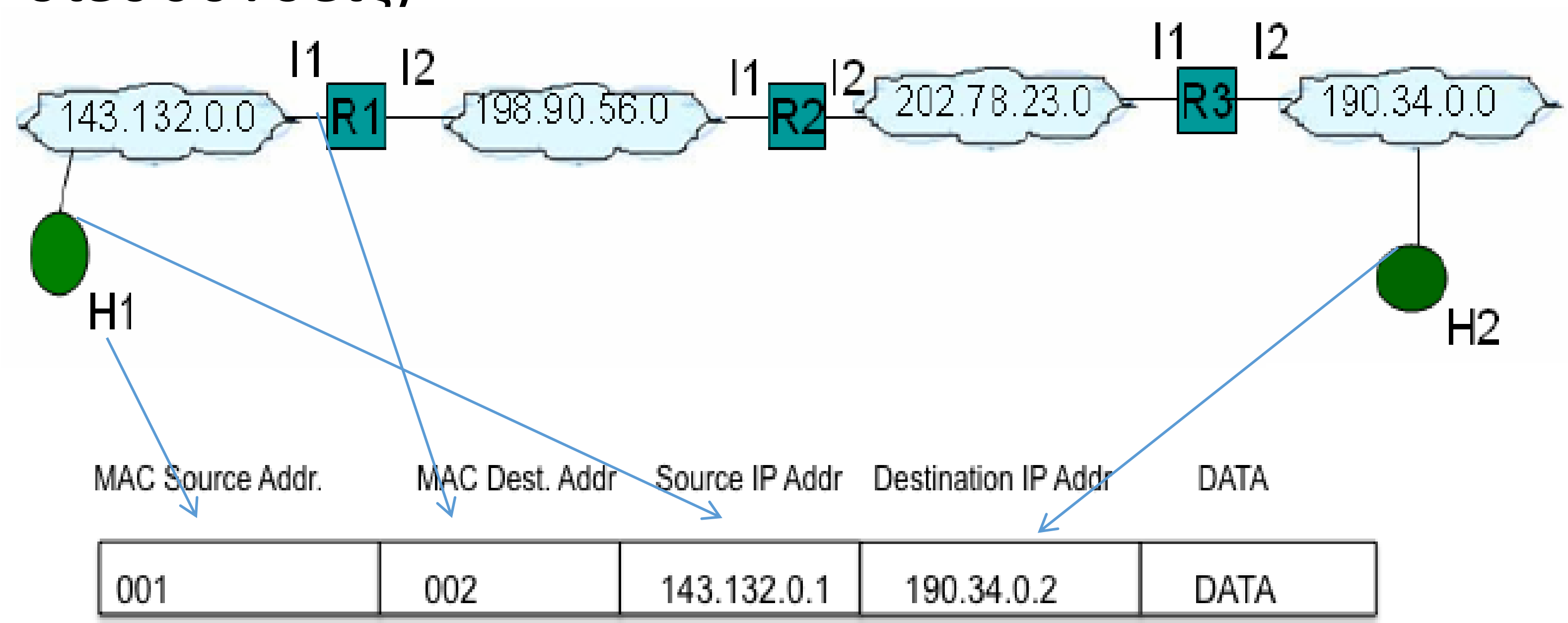


Να θεωρήσετε τις παρακάτω εγγραφές στο κάθε ένα δρομολογητή.

Host/Router	IP Διεύθυνση	MAC Διεύθυνση
H1	143.132.0.1	001
Interface 1 of R1	143.132.90.2	002
Interface 2 of R1	198.90.56.1	00002
Interface 1 of R2	198.90.56.2	00004
Interface 2 of R2	202.78.23.1	03
Interface 1 of R3	202.78.23.2	05
Interface 2 of R3	190.34.0.1	0004
H2	190.34.0.2	0005

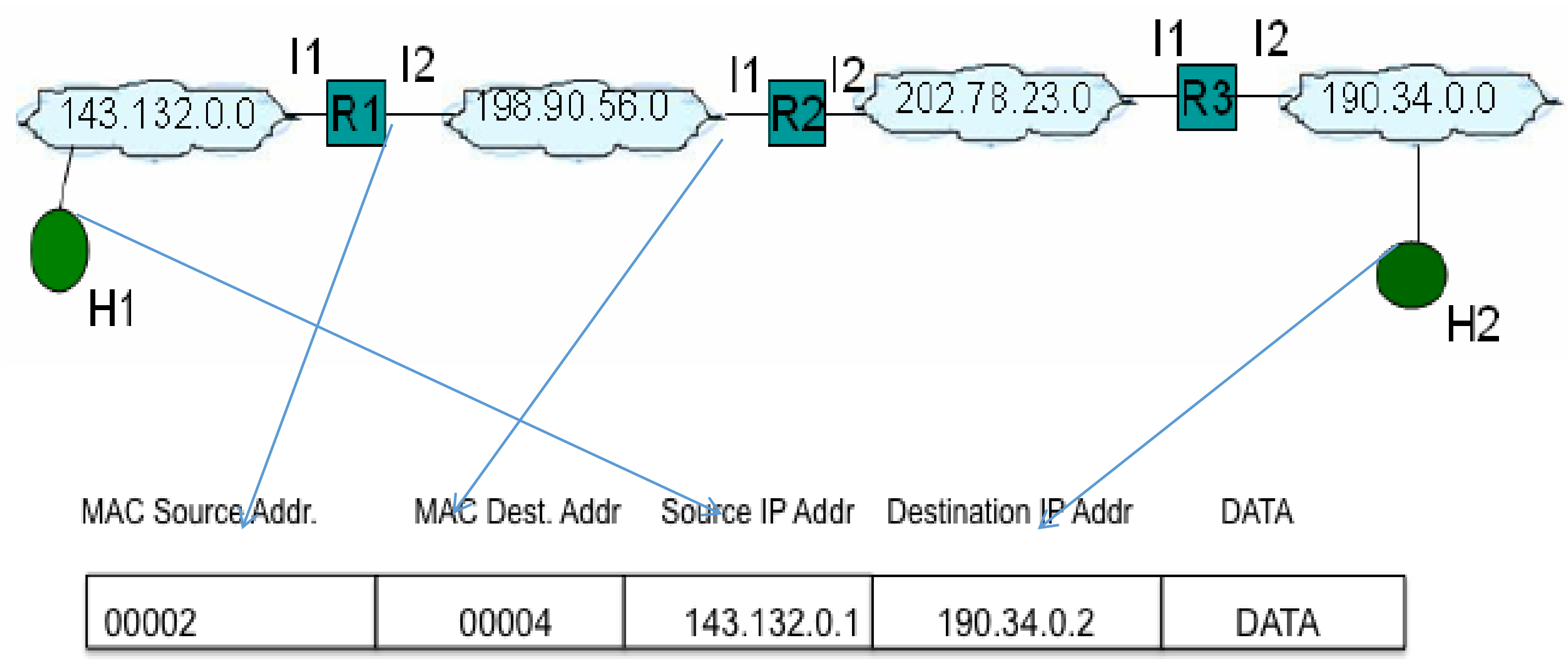
Να δείξετε τα πεδία που μεταβάλλονται καθώς ένα πακέτο μεταδίδεται από το H1 προς το H2 μέσω των R1, R2, R3.

- Μετάδοση H1 - R1 (αλλάζουν μόνο οι MAC διευθύνσεις)



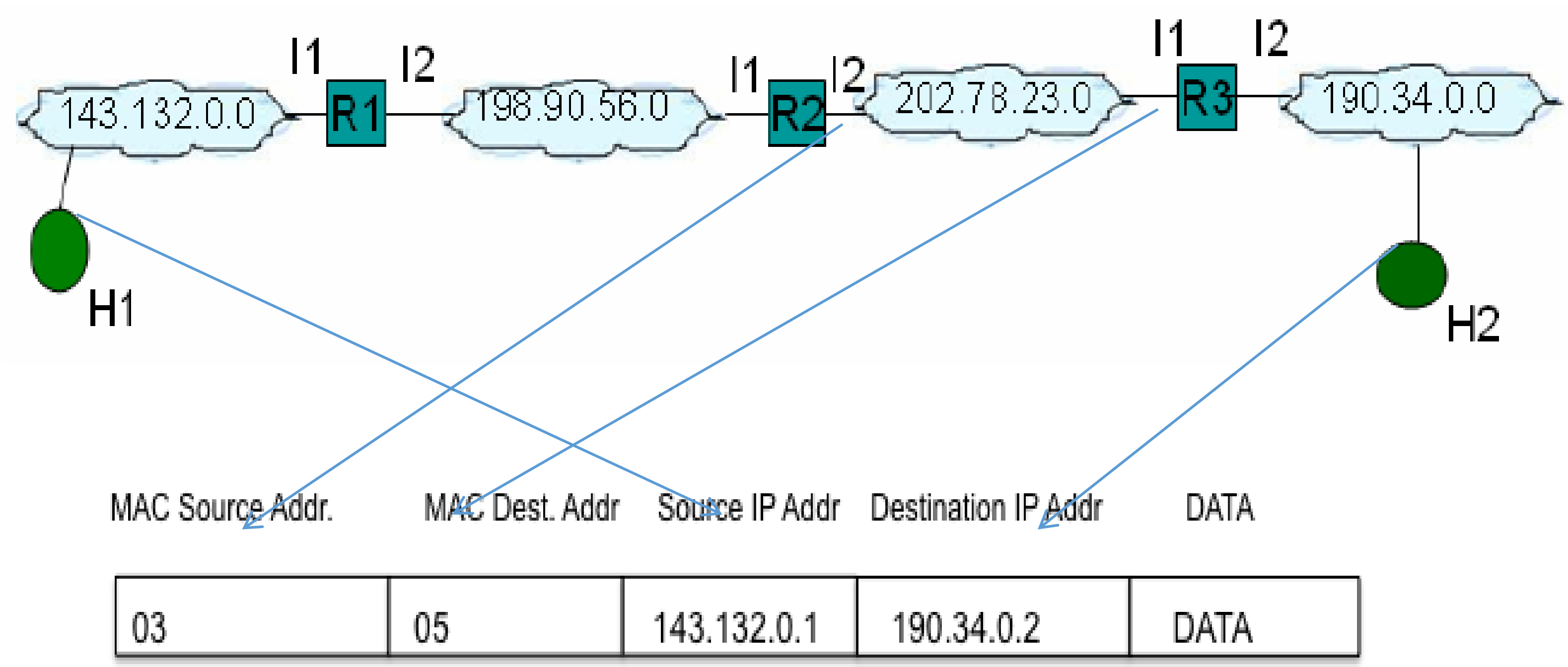
Host/Router	IP address	MAC address
H1	143.132.0.1	001
Interface 1 of R1	143.132.90.2	002
Interface 2 of R1	198.90.56.1	00002
Interface 1 of R2	198.90.56.2	00004
Interface 2 of R2	202.78.23.1	03
Interface 1 of R3	202.78.23.2	05
Interface 2 of R3	190.34.0.1	0004
H2	190.34.0.2	0005

- Μετάδοση R1 - R2



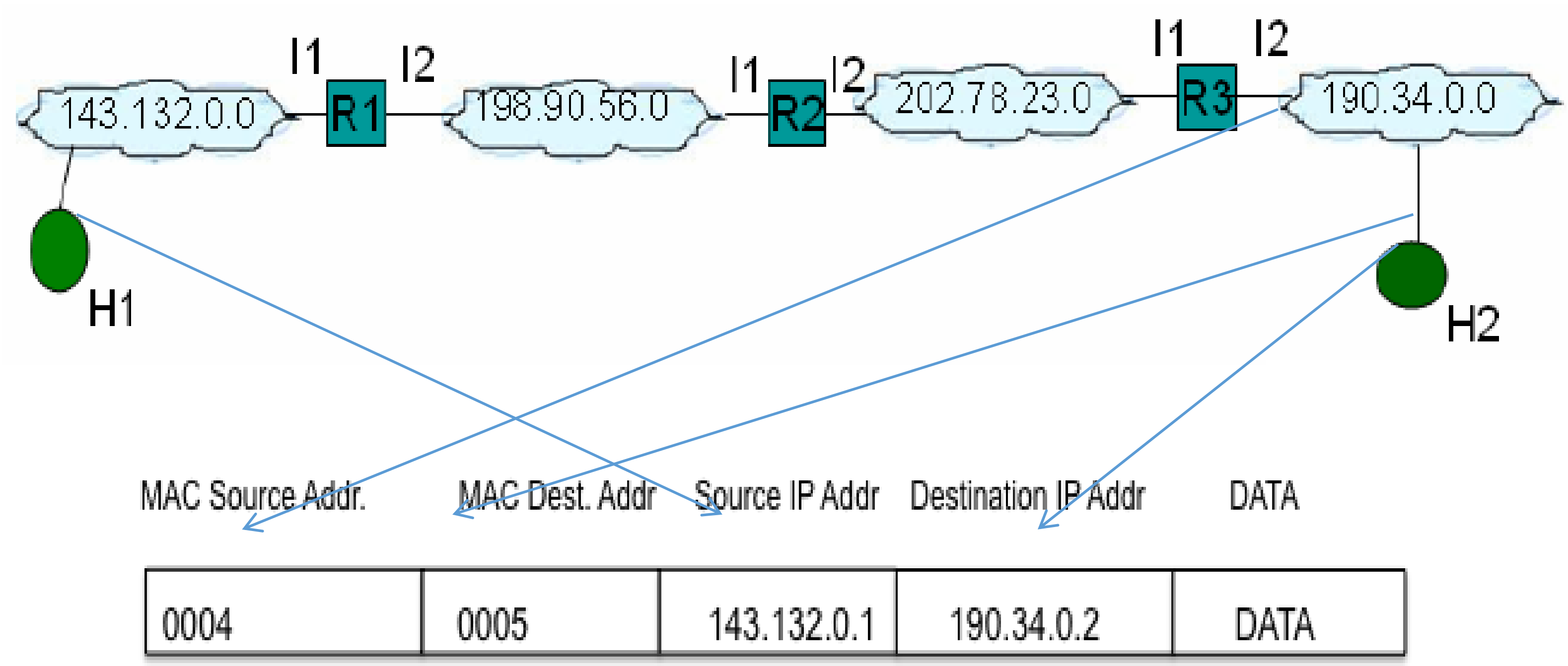
Host/Router	IP address	MAC address
H1	143.132.0.1	001
Interface 1 of R1	143.132.90.2	002
Interface 2 of R1	198.90.56.1	00002
Interface 1 of R2	198.90.56.2	00004
Interface 2 of R2	202.78.23.1	03
Interface 1 of R3	202.78.23.2	05
Interface 2 of R3	190.34.0.1	0004
H2	190.34.0.2	0005

- Μετάδοση R2 - R3



Host/Router	IP address	MAC address
H1	143.132.0.1	001
Interface 1 of R1	143.132.90.2	002
Interface 2 of R1	198.90.56.1	00002
Interface 1 of R2	198.90.56.2	00004
Interface 2 of R2	202.78.23.1	03
Interface 1 of R3	202.78.23.2	05
Interface 2 of R3	190.34.0.1	0004
H2	190.34.0.2	0005

- Μετάδοση R3 - H2



Host/Router	IP address	MAC address
H1	143.132.0.1	001
Interface 1 of R1	143.132.90.2	002
Interface 2 of R1	198.90.56.1	00002
Interface 1 of R2	198.90.56.2	00004
Interface 2 of R2	202.78.23.1	03
Interface 1 of R3	202.78.23.2	05
Interface 2 of R3	190.34.0.1	0004
H2	190.34.0.2	0005

Συνδυαστική Άσκηση

ΘΕΜΑ 2

ΓΕ5/ 2015-16

Στόχος της άσκησης *είναι η εξοικείωση με τις έννοιες δικτύωσης και διευθυνσιοδότησης.*

Σχετικές ασκήσεις: *ΓΕ4/1314/Θ1, ΓΕ4/1314/Θ3, ΓΕ4/1314/Θ4.*

Α. Απαντήστε με Σωστό/Λάθος στις παρακάτω ερωτήσεις αιτιολογώντας την απάντησή σας:

1. Όταν ένας επαναλήπτης έχει δεδομένα προς μετάδοση, περιμένει μέχρι το κανάλι να είναι κενό.
2. Όταν μια γέφυρα στέλνει ένα πακέτο προς τον τελικό του προορισμό, πρέπει να βάλει στο πακέτο σαν MAC διεύθυνση προορισμού την MAC διεύθυνση του επόμενου κόμβου.
3. Υποθέστε ότι ο Η/Υ Α στέλνει IP πακέτο στον Η/Υ Β μέσω της γέφυρας Ζ, και ότι και οι τρεις συσκευές βρίσκονται στο ίδιο απλά γεφυρωμένο δίκτυο. Η MAC διεύθυνση προορισμού στο πακέτο που στέλνεται από τον Α θα είναι η MAC διεύθυνση προορισμού του Ζ.
4. Σε ένα δίκτυο με γέφυρες και τοπικά δίκτυα, όπου υπάρχουν εναλλακτικές διαδρομές, δεν μπορούμε να εγγυηθούμε ότι τα πακέτα θα προωθούνται σε σειρά.
5. Οι γέφυρες δεν χρησιμοποιούν την IP διεύθυνση για να αποφασίσουν πού θα στείλουν ένα πακέτο.
6. Αν ο Η/Υ Α στο ΕΑΠ θέλει να στείλει ένα IP πακέτο σε Η/Υ Β στο Πανεπιστήμιο Αιγαίου και ο ARP πίνακας είναι άδειος, τότε ο Α στέλνει ARP request για να προσδιορίσει την IP διεύθυνση του συνοριακού δρομολογητή.
7. Όταν ένα δρομολογητής που συνδέει δύο Ethernet τομείς προωθεί ένα IP πακέτο από τον ένα τομέα στον άλλο, δεν αλλάζει την IP διεύθυνση προορισμού.
8. Σε ιδιωτικό δίκτυο με πολλούς δρομολογητές, η σειρά στην προώθηση πακέτων είναι εγγυημένη με την χρήση του πεδίου TTL.
9. Όταν ένας δρομολογητής μεταξύ δύο τοπικών δικτύων προωθεί ένα πακέτο από το ένα τοπικό δίκτυο στο άλλο, δεν μεταβάλλει την MAC διεύθυνση προορισμού.
10. Είναι δυνατόν πακέτα να οδηγηθούν να κυκλοφορούν αέναα στο δίκτυο αν υπάρχουν σφάλματα σε πίνακες προώθησης δρομολογητών.

Όταν ένας επαναλήπτης έχει δεδομένα προς μετάδοση, περιμένει μέχρι το κανάλι να είναι κενό.
Απάντηση: Λάθος. Ο επαναλήπτης απλά επαναλαμβάνει τα δεδομένα, ακόμα και αν προκαλέσει σύγκρουση.

Όταν μια γέφυρα στέλνει ένα πακέτο προς τον τελικό του προορισμό, πρέπει να βάλει στο πακέτο σαν MAC διεύθυνση προορισμού την MAC διεύθυνση του επόμενου κόμβου.
Απάντηση: Λάθος. Η γέφυρα δεν αλλάζει τις MAC διευθύνσεις.

Υποθέστε ότι ο Η/Υ Α στέλνει IP πακέτο στον Η/Υ Β μέσω της γέφυρας Ζ, και ότι και οι τρεις συσκευές βρίσκονται στο ίδιο απλά γεφυρωμένο δίκτυο. Η MAC διεύθυνση προορισμού στο πακέτο που στέλνεται από τον Α θα είναι η MAC διεύθυνση προορισμού του Ζ.
Απάντηση: Λάθος. Οι γέφυρες είναι διάφανες συσκευές στο Ethernet.

Σε ένα δίκτυο με γέφυρες και τοπικά δίκτυα, όπου υπάρχουν εναλλακτικές διαδρομές, δεν μπορούμε να εγγυηθούμε ότι τα πακέτα θα προωθούνται σε σειρά.
Απάντηση: Λάθος. Η άφιξη σε σειρά είναι εγγυημένη καθότι υλοποιείται ο αλγόριθμος του δένδρου επικάλυψης, οπότε η τοπολογία καταλήγει σε ένα δένδρο.

Οι γέφυρες δεν χρησιμοποιούν την IP διεύθυνση για να αποφασίσουν πού θα στείλουν ένα πακέτο.
Απάντηση: Σωστό. Οι γέφυρες δεν κοιτάνε πληροφορία από το επίπεδο 3.

Αν ο Η/Υ Α στο ΕΑΠ θέλει να στείλει ένα IP πακέτο σε Η/Υ Β στο Πανεπιστήμιο Αιγαίου και ο ARP πίνακας είναι άδειος, τότε ο Α στέλνει ARP request για να προσδιορίσει την IP διεύθυνση του συνοριακού δρομολογητή.
Απάντηση: Λάθος. Το μήνυμα ARP request χρησιμοποιείται για να προσδιοριστεί η MAC διεύθυνση του συνοριακού δρομολογητή.

Όταν ένα δρομολογητής που συνδέει δύο Ethernet τομείς προωθεί ένα IP πακέτο από τον ένα τομέα στον άλλο, δεν αλλάζει την IP διεύθυνση προορισμού.
Απάντηση: Σωστό.

Σε ιδιωτικό δίκτυο με πολλούς δρομολογητές, η σειρά στην προώθηση πακέτων είναι εγγυημένη με την χρήση του πεδίου TTL.
Απάντηση: Λάθος. Το IP δεν εγγυάται ότι πακέτα προωθούνται σε σειρά.

Όταν ένας δρομολογητής μεταξύ δύο τοπικών δικτύων προωθεί ένα πακέτο από το ένα τοπικό δίκτυο στο άλλο, δεν μεταβάλλει την MAC διεύθυνση προορισμού.
Απάντηση: Λάθος.

Είναι δυνατόν πακέτα να οδηγηθούν να κυκλοφορούν αέναα στο δίκτυο αν υπάρχουν σφάλματα σε πίνακες προώθησης δρομολογητών.

Απάντηση: Λάθος. Τα πακέτα απορρίπτονται όταν το πεδίο TTL γίνει 1.