

ΕΑΠ/ΠΛΗ22/ΑΘΗ.2
ΟΣΣ-5 Δίκτυα Η/Υ
Συμπληρωματικές Διαφάνειες

Νίκος Δημητρίου

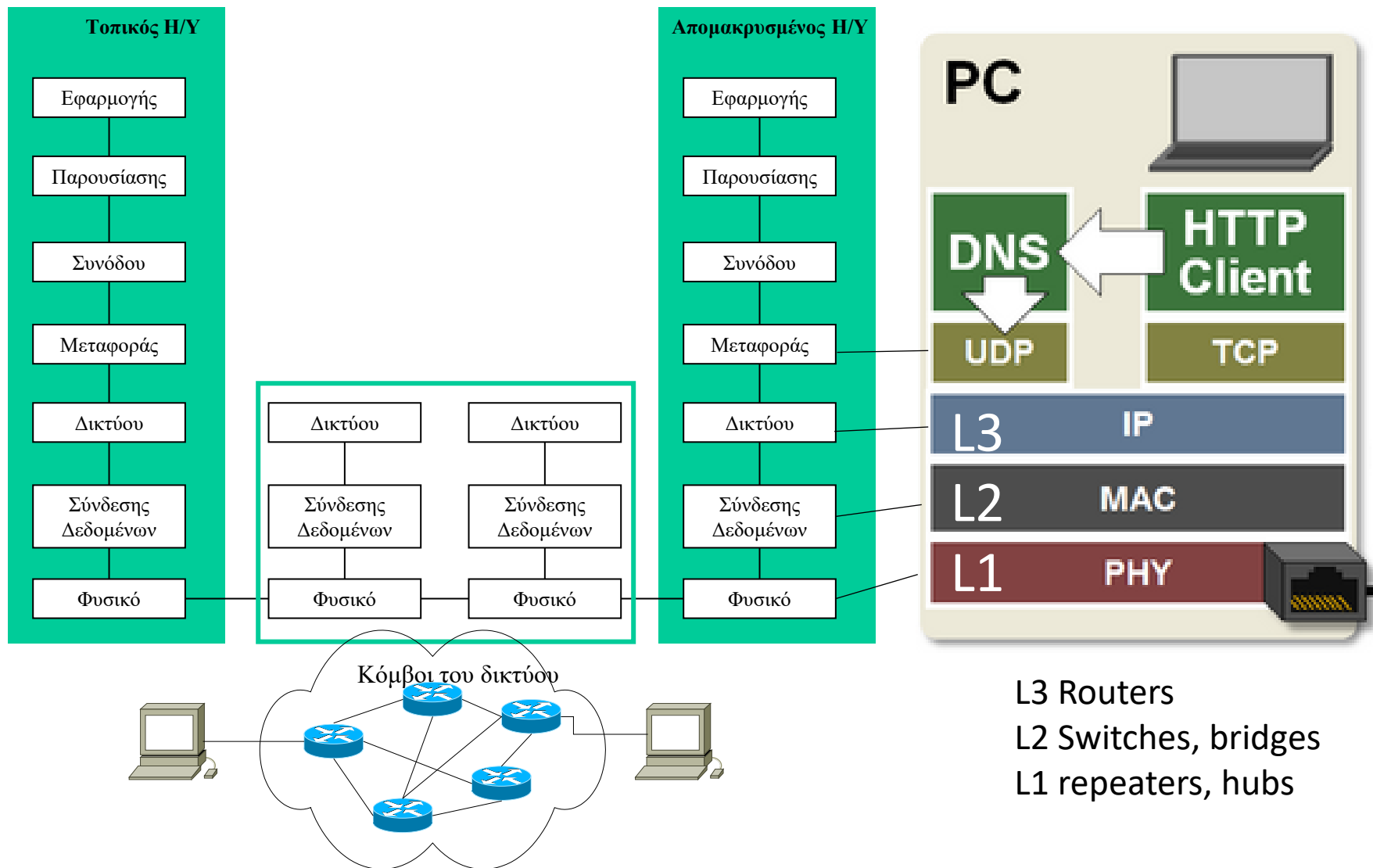
Σημείωση

- Στην παρουσίαση αυτή παρατίθενται παραπομπές σε συγκεκριμένες διαφάνειες της παρουσίασης *PLH22_OSS5_slides_2017-18.ppt* που βρίσκεται στο **study.eap.gr** στο φάκελο *Βοηθητικό Υλικό ΟΣΣ/ΟΣΣ5*

- Θέματα: OSI - TCP/IP layers, encapsulation
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_slides_2017-18.ppt*:

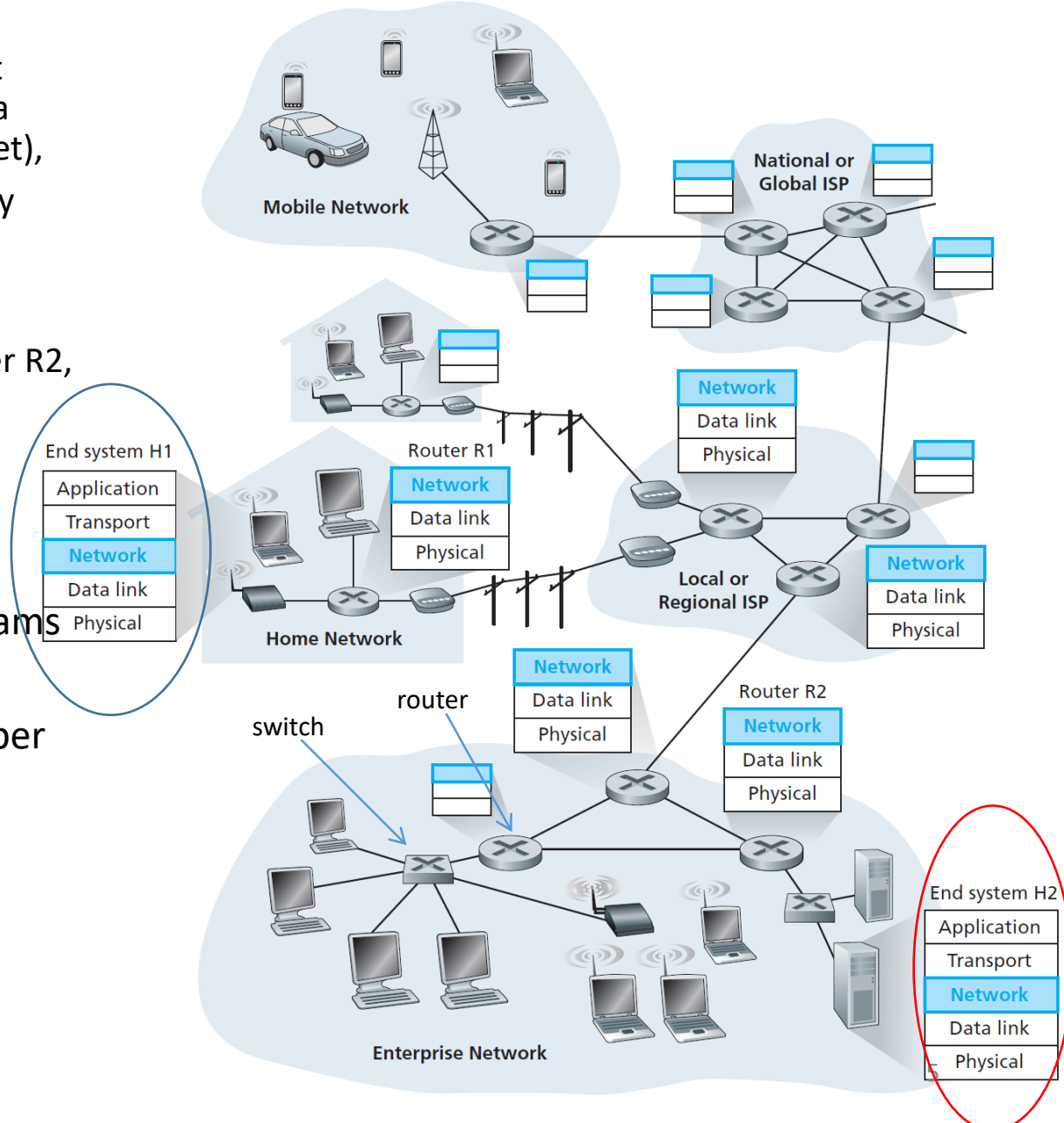
3,4

Το Μοντέλο Αναφοράς ISO/OSI

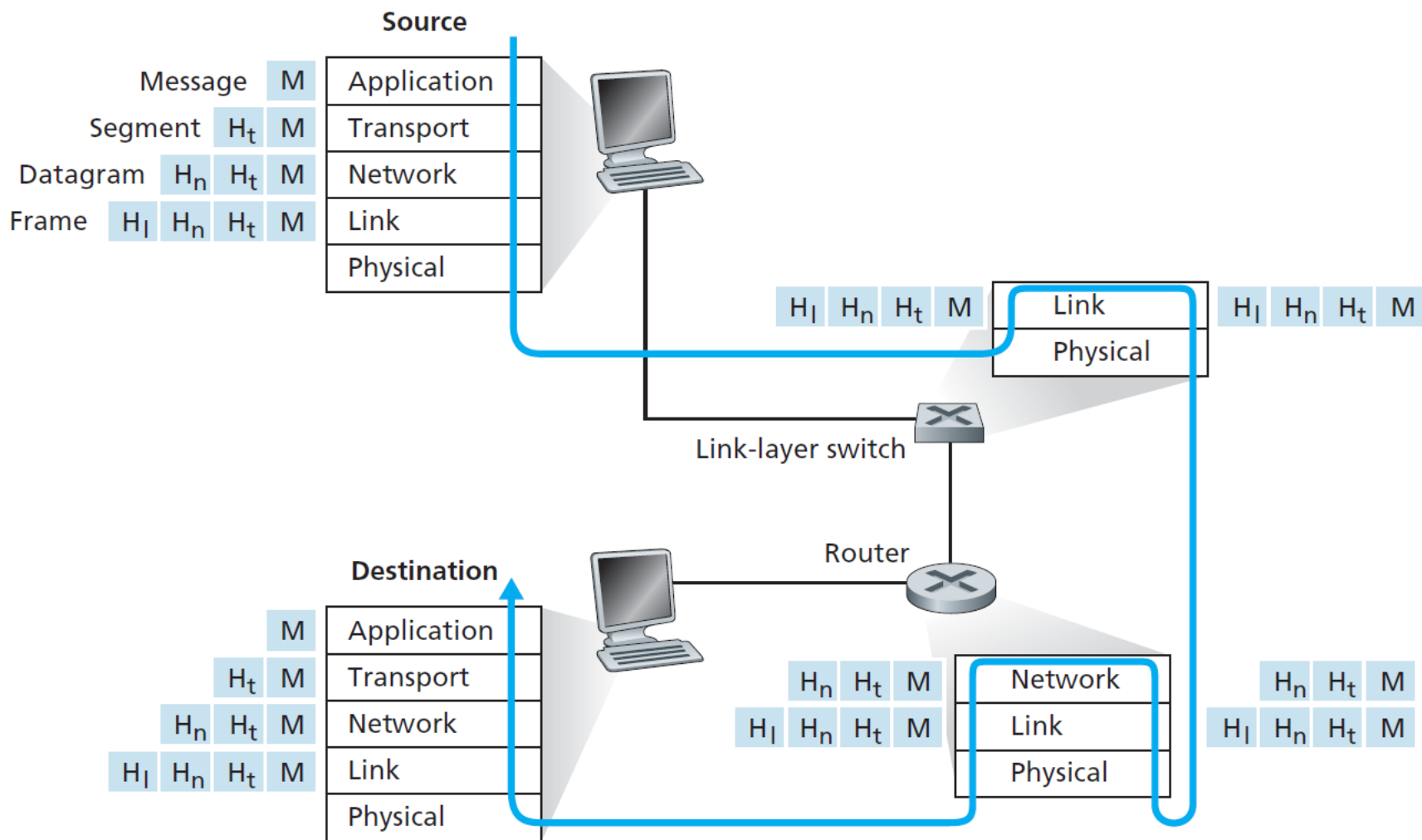


L3 Routers
L2 Switches, bridges
L1 repeaters, hubs

- 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



Encapsulation- Ενθυλάκωση



- Θέματα: LAN topologies,
Bus/relay/hub/switch/bridge
- Δείτε τις παρακάτω διαφάνειες του
PLH22_OSS5_slides_2017-18.ppt :
5-37

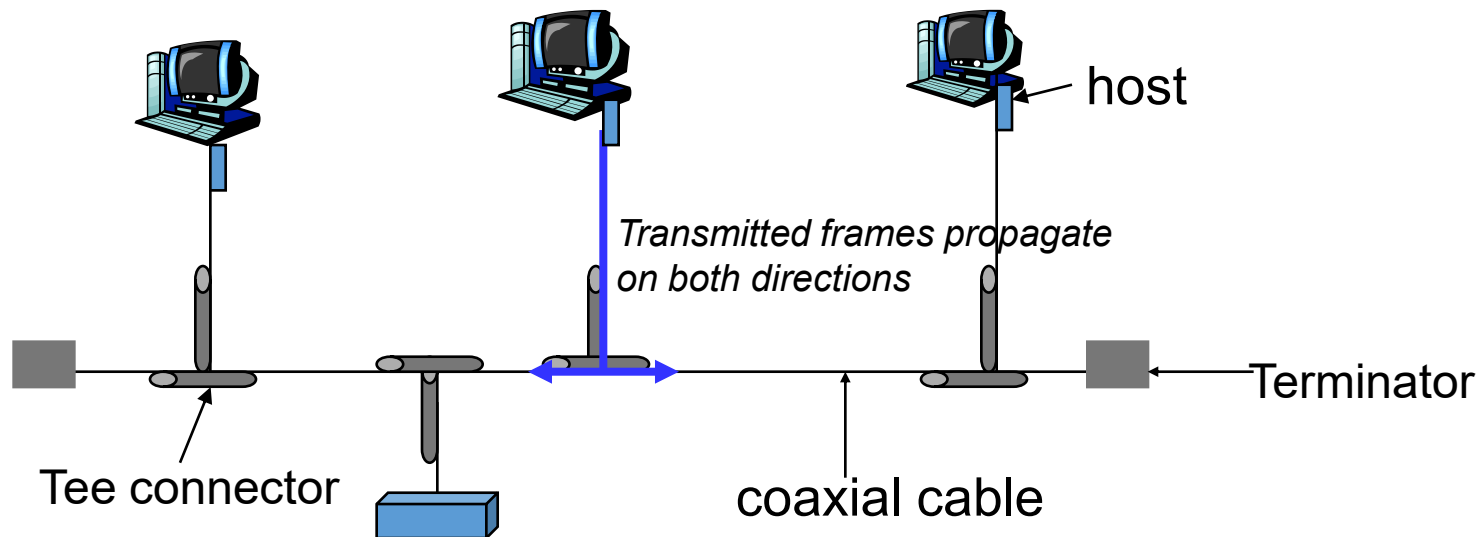
repeaters, hubs : Λήψη μεταδιδόμενων bits (ηλεκτρικό σήμα),

Επίσχυση / αναγέννηση σήματος, αποστολή στην έξοδο
χρήση: επέκταση ενός διαύλου. ^{πρωίηση}

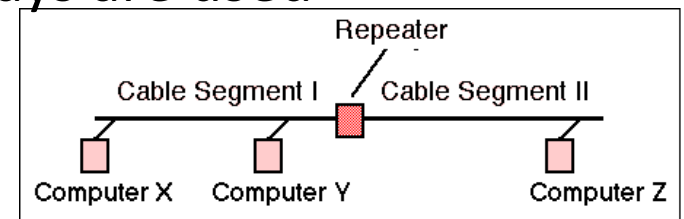
hubs : multi port repeaters. Κάθε εισερχόμενο frame

αναμεταδίδεται σε όλες τις υπόλοιπες θύρες του hub
χρήση: διασύνδεση πολλαπλών σταθμών σε
τοπολογία αστέρα

Ethernet Bus connection



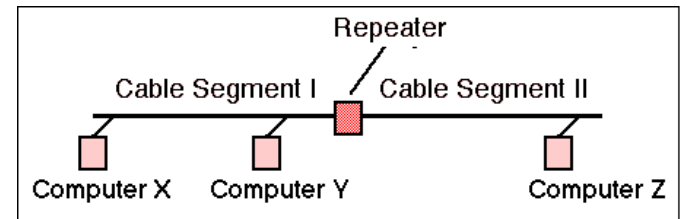
- When a frame enters a Tee connector
 - a frame copy is forwarded towards each of 2 directions of the connector
 - As frames propagate towards the terminator they 'leave' a copy on each host adapter they 'traverse'
- To cover long distances, repeaters/relays are used



Ethernet Topologies

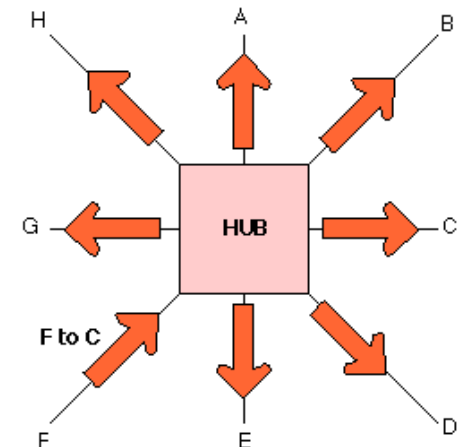
“Traditional” Ethernet

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

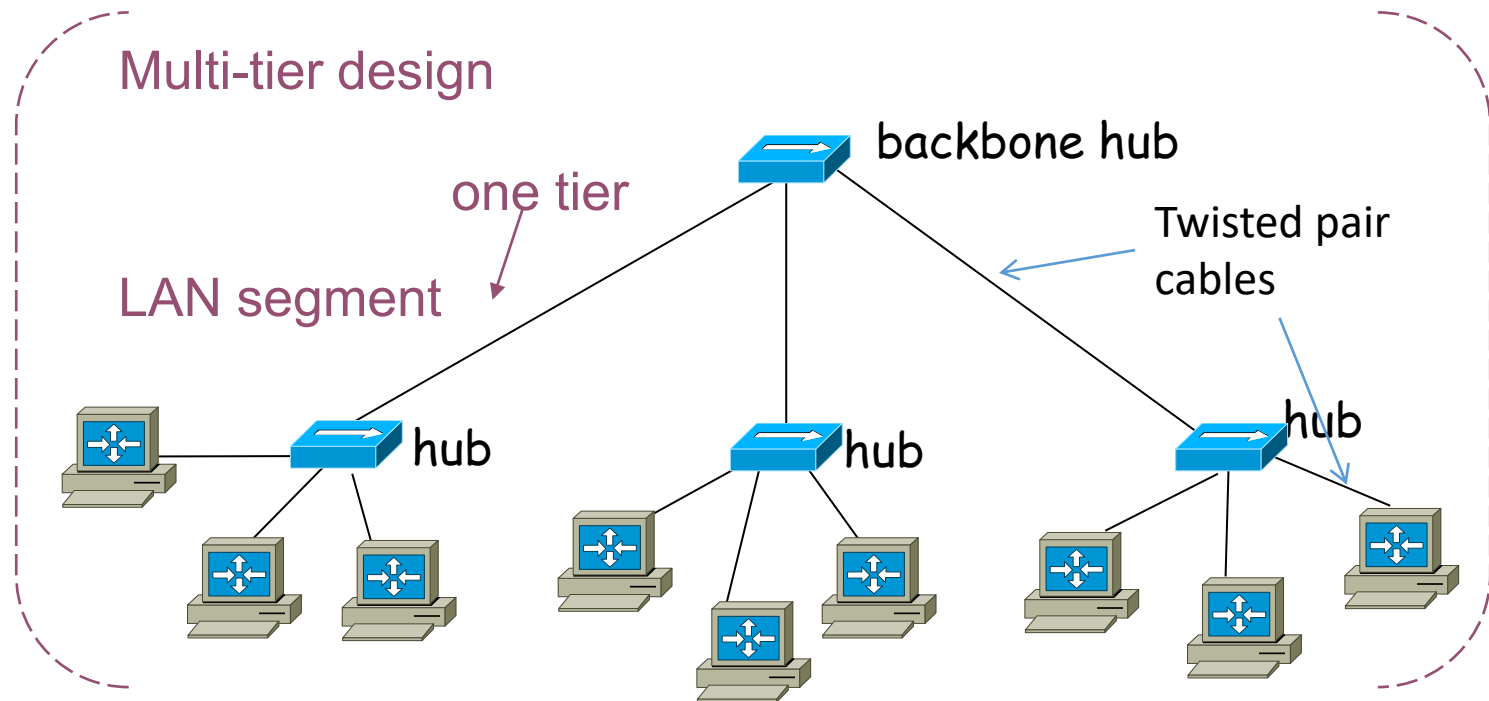


“Hub” Ethernet

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

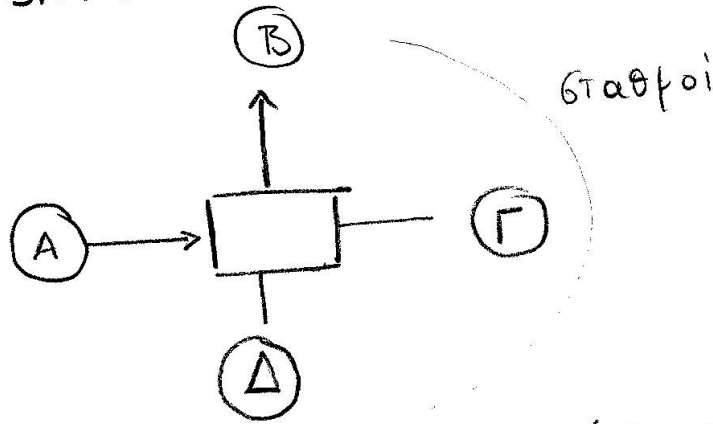


Ethernet hub connection



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

SWITCH/BRIDGE



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

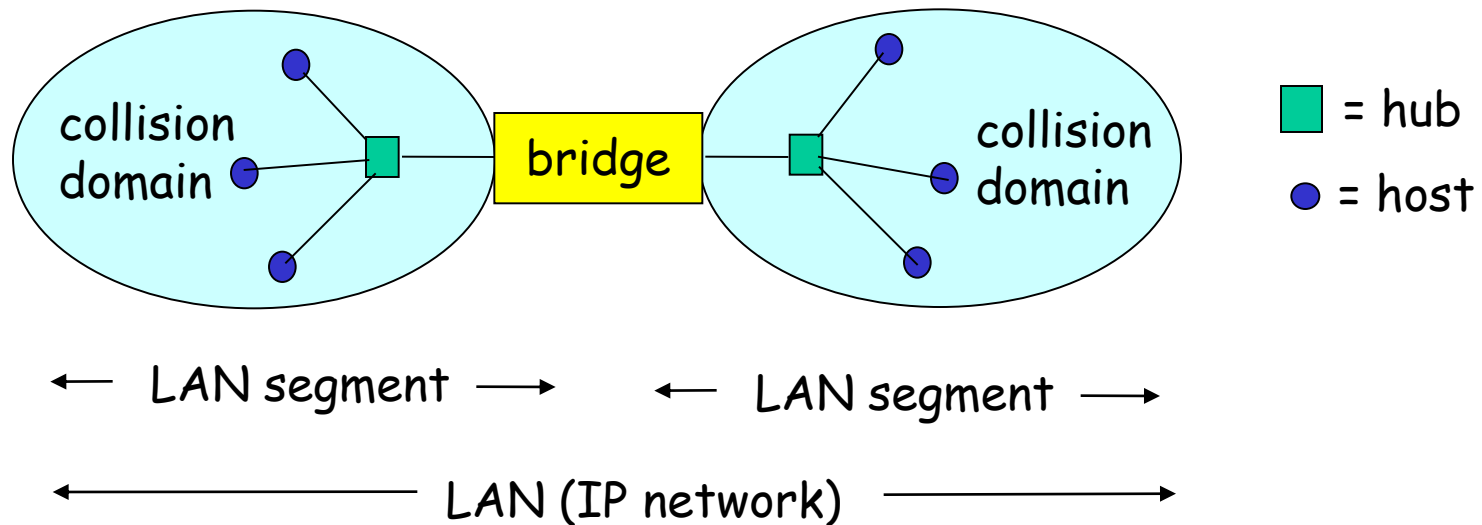
Ο πίνακας δημιουργείται με βάση την κίνηση των πακέτων (διαδικασία μάθησης)

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

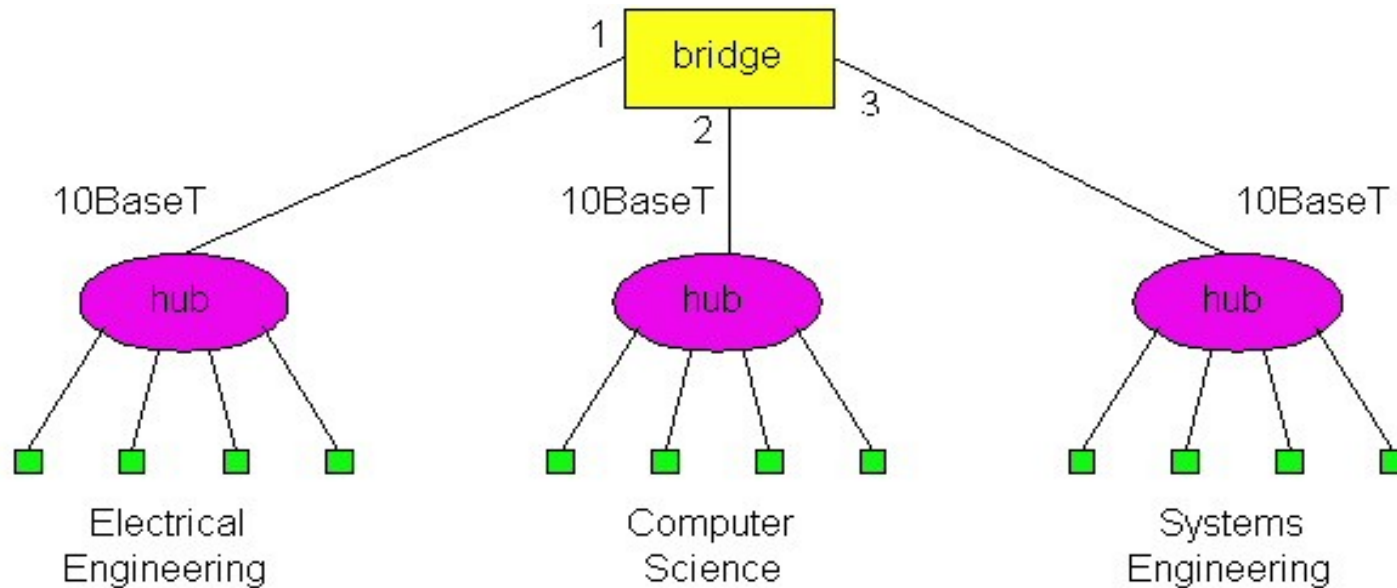
Αποφυγή συγκρούσεων

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

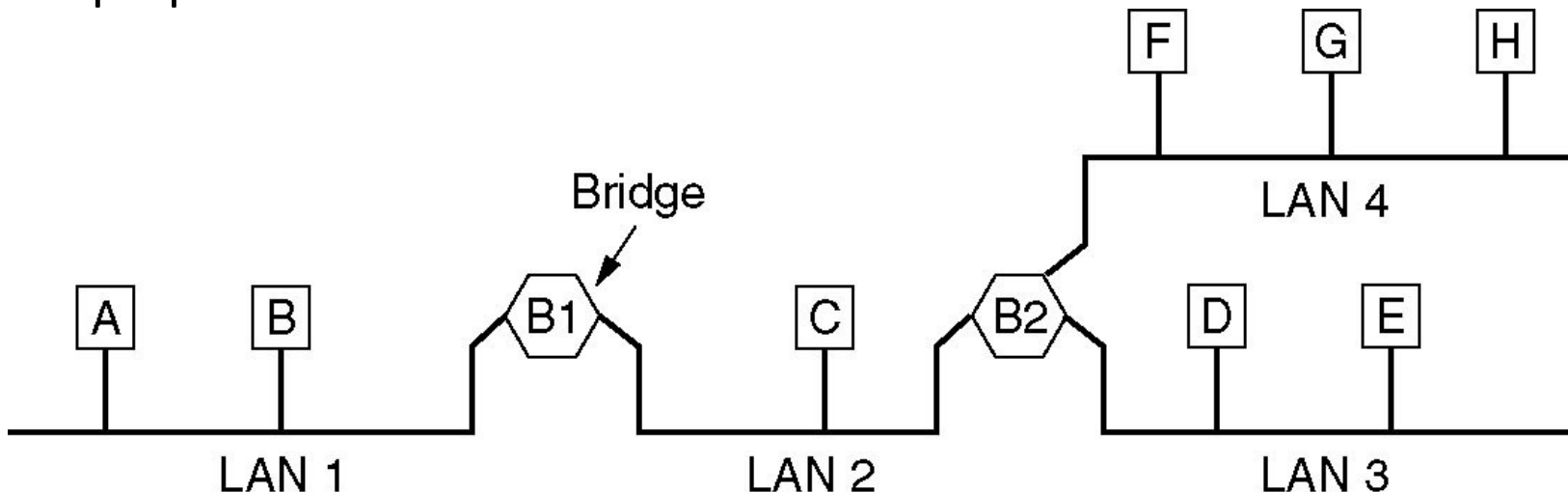


How do determine to which LAN segment to forward frame?

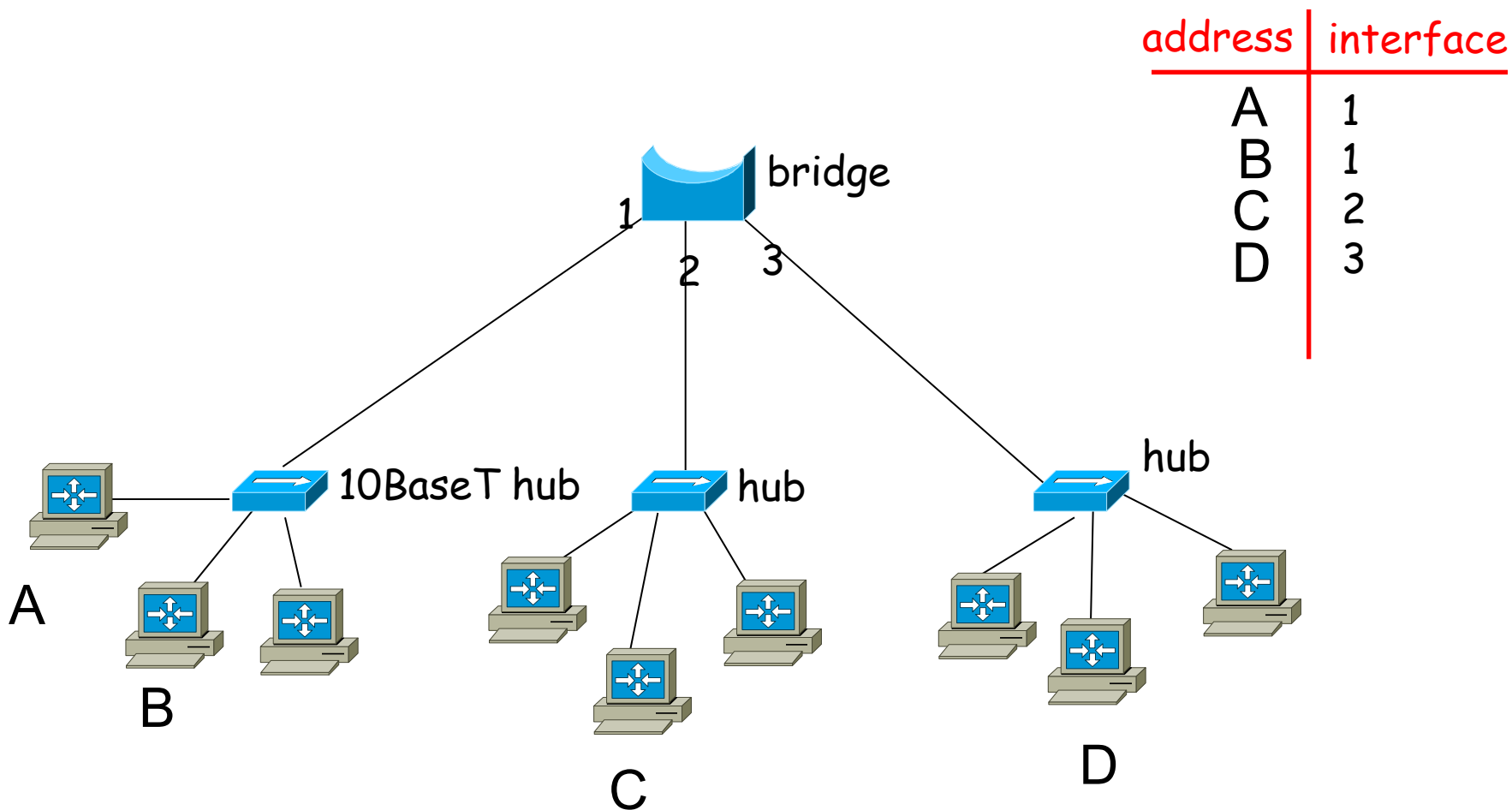
- Looks like a routing problem...

Λειτουργία Γέφυρας

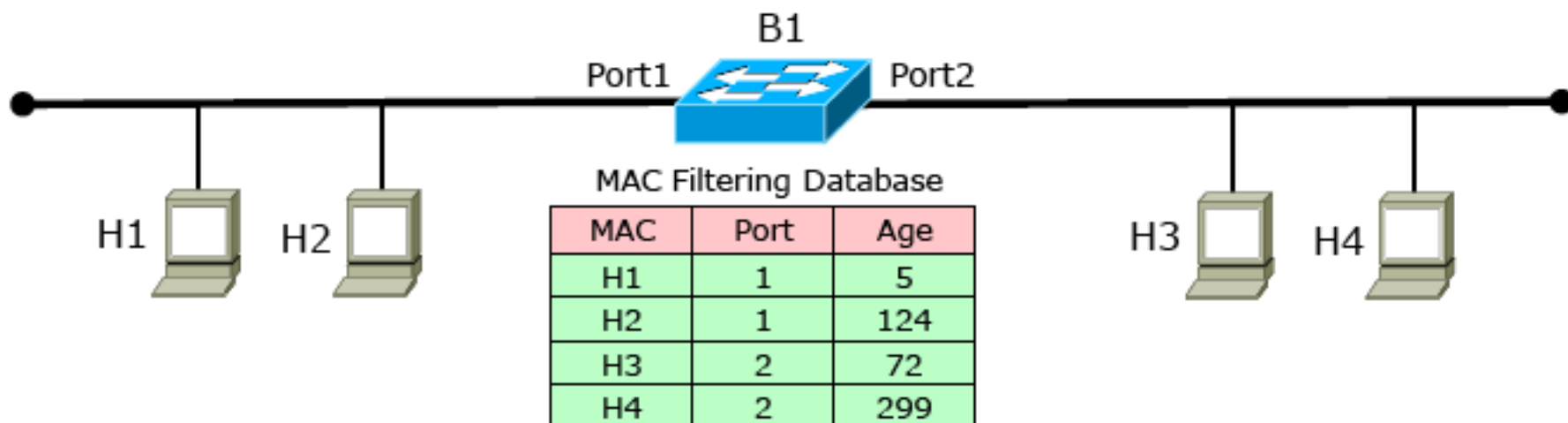
- Διαβάζει την διεύθυνση MAC παραλήπτη από τα πλαίσια που φθάνουν από κάθε δίκτυο. Προωθεί τα πλαίσια στο δίκτυο στο οποίο βρίσκεται ο παραλήπτης
- Εάν δεν ξέρει που βρίσκεται ο παραλήπτης, τότε προωθεί το πλαίσιο σε όλα τα δίκτυα εκτός από το δίκτυο από όπου προήλθε.



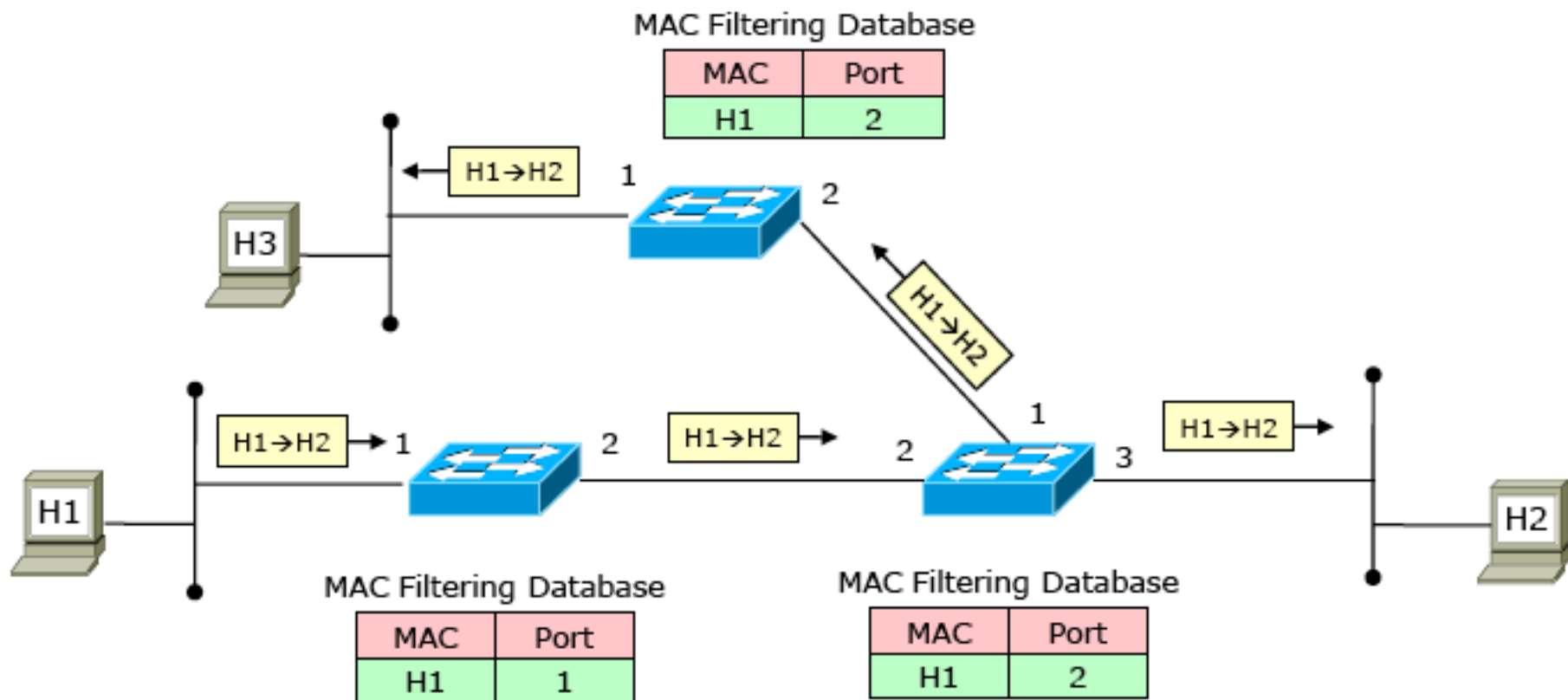
Παράδειγμα Bridge (1)



Παράδειγμα Bridge (2)

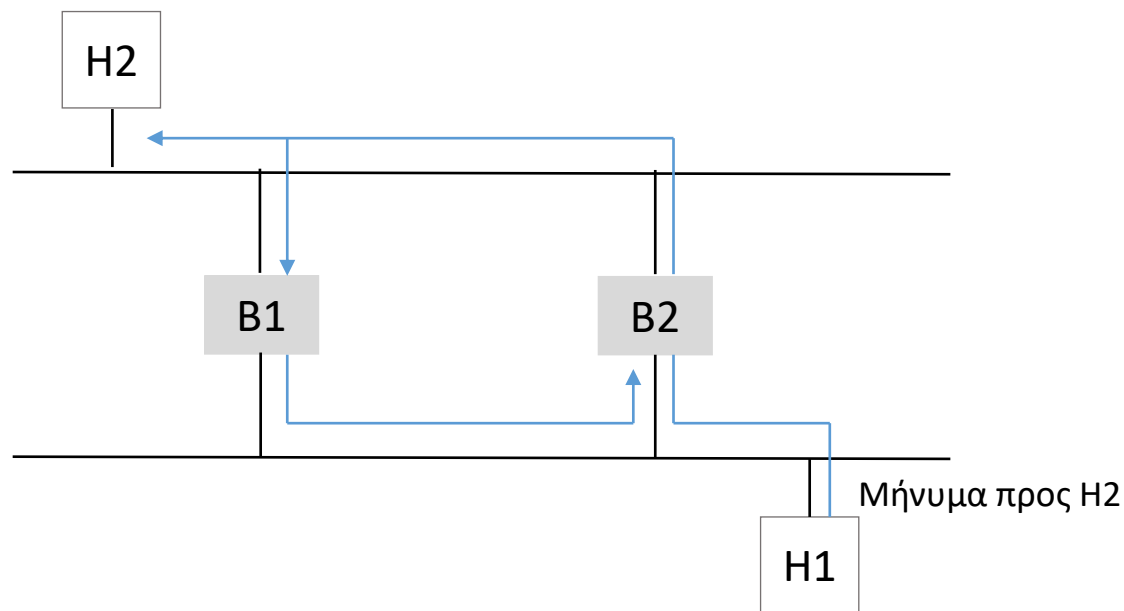


Παράδειγμα Bridge (3)



Εμφάνιση βρόχων

- Για μεγαλύτερη αξιοπιστία, πολλές φορές υπάρχουν εναλλακτικές διαδρομές από τον αποστολέα στον παραλήπτη
- Οι πολλαπλές διαδρομές δημιουργούν **βρόχους** (loops) μέσω των οποίων οι γέφυρες μπορεί να προωθούν ένα πλαίσιο συνέχεια



Δέντρο επικάλυψης γεφυρών

- Για τη λύση του προβλήματος εμφάνισης βρόχων, οι Γέφυρες «δημιουργούν» ένα Δέντρο Επικάλυψης (Spanning Tree-SP) «απενεργοποιώντας» κάποιες από τις διεπαφές/θύρες
- Το δέντρο επικάλυψης είναι ένα υποδίκτυο του αρχικού δικτύου το οποίο προσφέρει συνδεσιμότητα σε όλους τους κόμβους χωρίς την εμφάνιση βρόχων
- Ο αλγόριθμος δημιουργίας του δέντρου επικάλυψης υλοποιείται στο πρωτόκολλο IEEE802.1d

Βασικές έννοιες αλγορίθμου (1)

- Γέφυρα-ρίζα (Root Bridge) που έχει όλες τις θύρες ενεργές
 - Είναι η γέφυρα με το μικρότερο αναγνωριστικό (ID)
 - Το ID αντιστοιχεί στην MAC διεύθυνση όμως αυτό μπορεί να το αλλάξει ο διαχειριστής του δικτύου
- Κόστος μονοπατιού μέχρι τη ρίζα (Root Path Cost) είναι το κόστος σύνδεσης μια γέφυρας με τη ρίζα.
Το κόστος κάθε συνδέσμου:
 - παίρνει την τιμή 1 ή
 - υπολογίζεται ως $1000 / \text{Mbps}$ όπου Mbps είναι η ταχύτητα του συνδέσμου στο οποίο είναι συνδεδεμένη μια θύρα (σε Mbps)

Βασικές έννοιες αλγορίθμου (2)

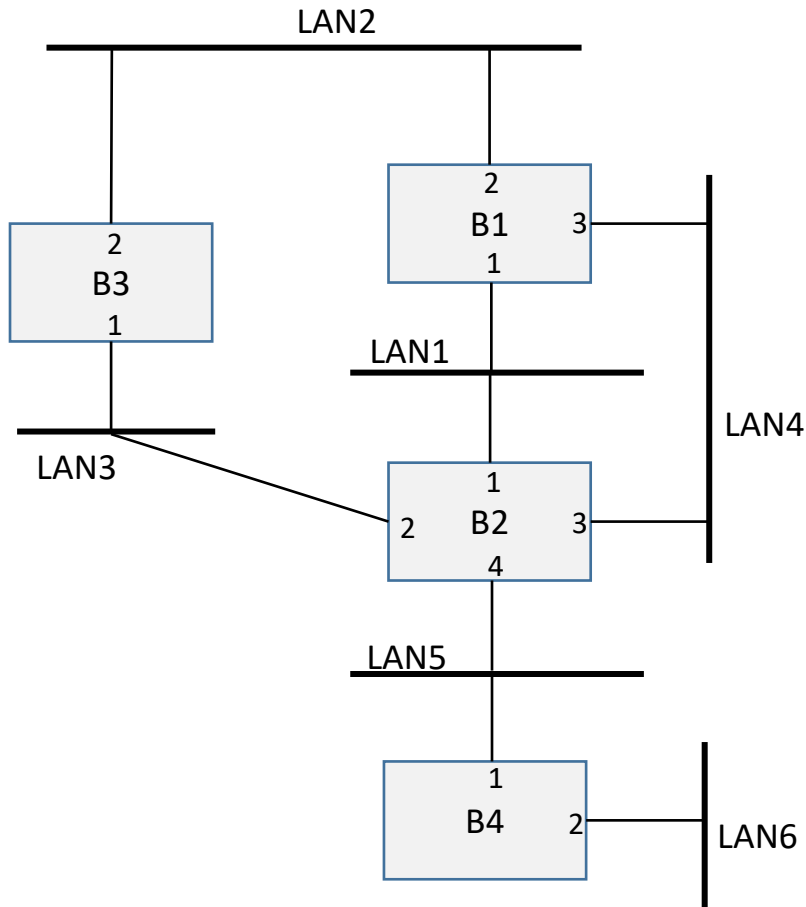
- Για το σχηματισμό του SP κάποιες γέφυρες θα είναι ενεργές και κάποιες ανενεργές (standby)
- Στις ενεργές γέφυρες, κάποιες θύρες θα είναι ενεργές και κάποιες ανενεργές (blocked)
- Η γέφυρα-ρίζα είναι η «κυρίαρχη» γέφυρα
- Στις υπόλοιπες ενεργές γέφυρες (designated bridge) μια θύρα (root port) καθορίζεται για επικοινωνία με τη γέφυρα-ρίζα και οι υπόλοιπες ενεργές θύρες (designated ports) διασυνδέουν τα τοπικά δίκτυα (LANs)

Αλγόριθμος Δέντρου Επικάλυψης με Γέφυρες

1. Επιλέγεται η ρίζα (γέφυρα με το μικρότερο αναγνωριστικό)
2. Σε κάθε γέφυρα επιλέγεται ένα root port ώστε το μονοπάτι μέχρι τη ρίζα να έχει το μικρότερο κόστος
3. Για κάθε δίκτυο επιλέγεται μία γέφυρα για τη διασύνδεση με τη ρίζα

Κατά την εκτέλεση του αλγορίθμου, όταν προκύπτουν μονοπάτια ίσου κόστους, προτιμάται η γέφυρα με το μικρότερο αναγνωριστικό

Παράδειγμα Δέντρου Επικάλυψης (1)

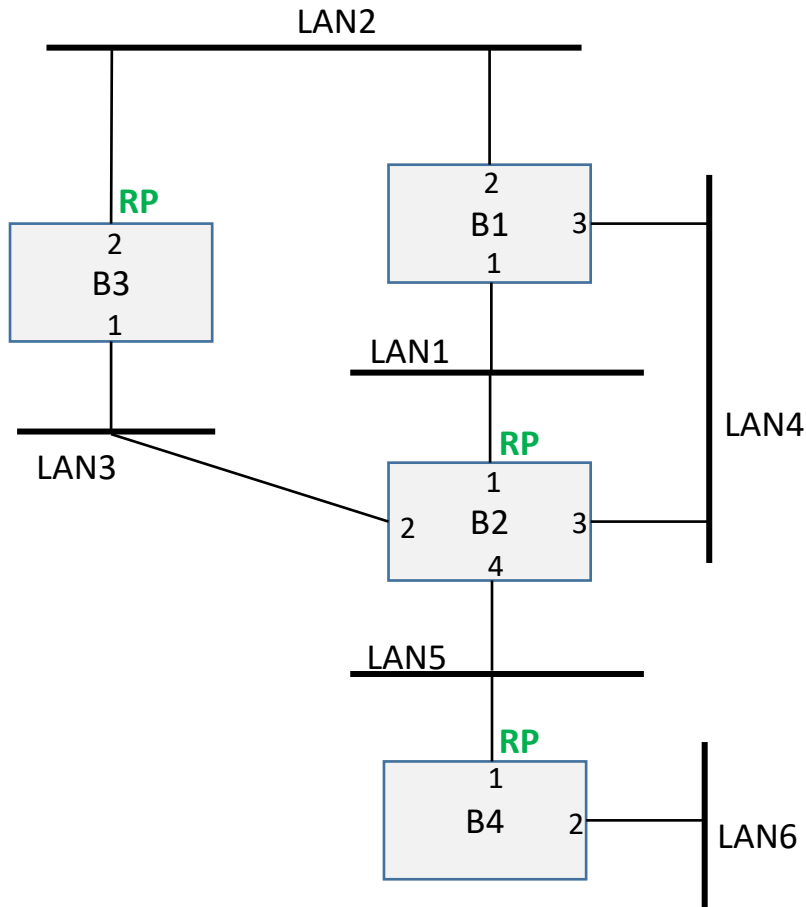


1. Ορίζουμε ως ρίζα την B1
2. Επιλέγουμε τα Root Ports

Γέφυρα	Μονοπάτι	Κόστος	Root Port
B2	B2.1→B1.1	1	B2.1
B3	B3.2→B1.2	1	B3.2
B4	B4.1→B2.4→ B2.1→B1.1	2	B4.1

* Στο παράδειγμα αυτό θεωρούμε κόστος συνδέσεων = 1

Παράδειγμα Δέντρου Επικάλυψης (2)

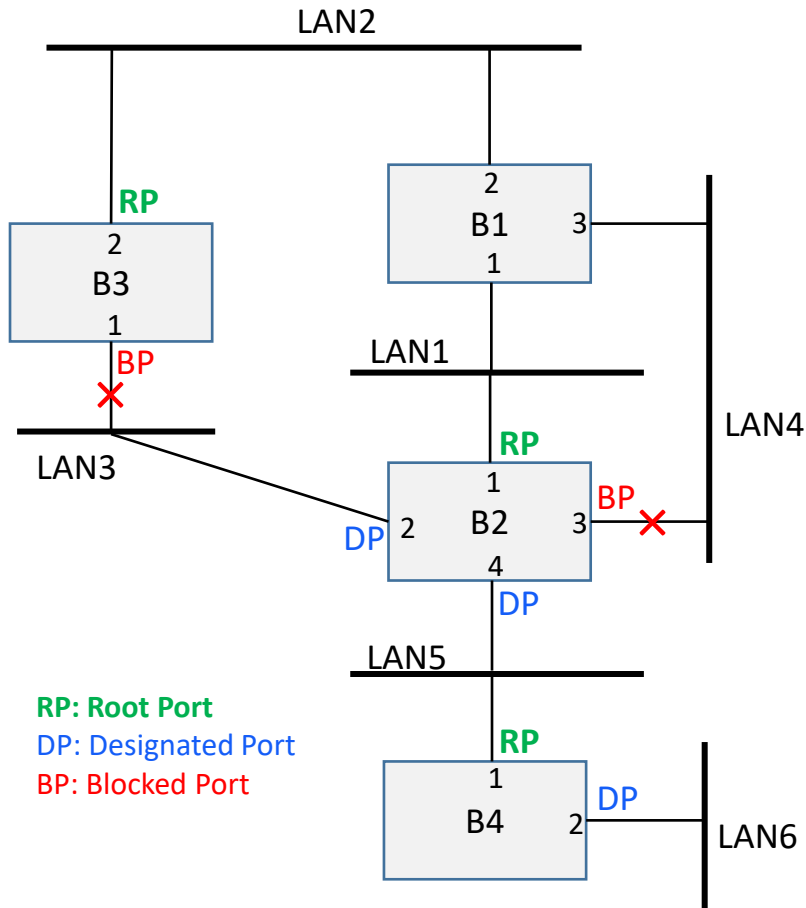


3. Για κάθε LAN επιλέγω μια γέφυρα

Δίκτυο	Designated bridge/port
LAN1	B1.1
LAN2	B1.2
LAN3	B2.2
LAN4	B1.3
LAN5	B2.4
LAN6	B4.2

επιλογή B2 λόγω μικρότερου ID

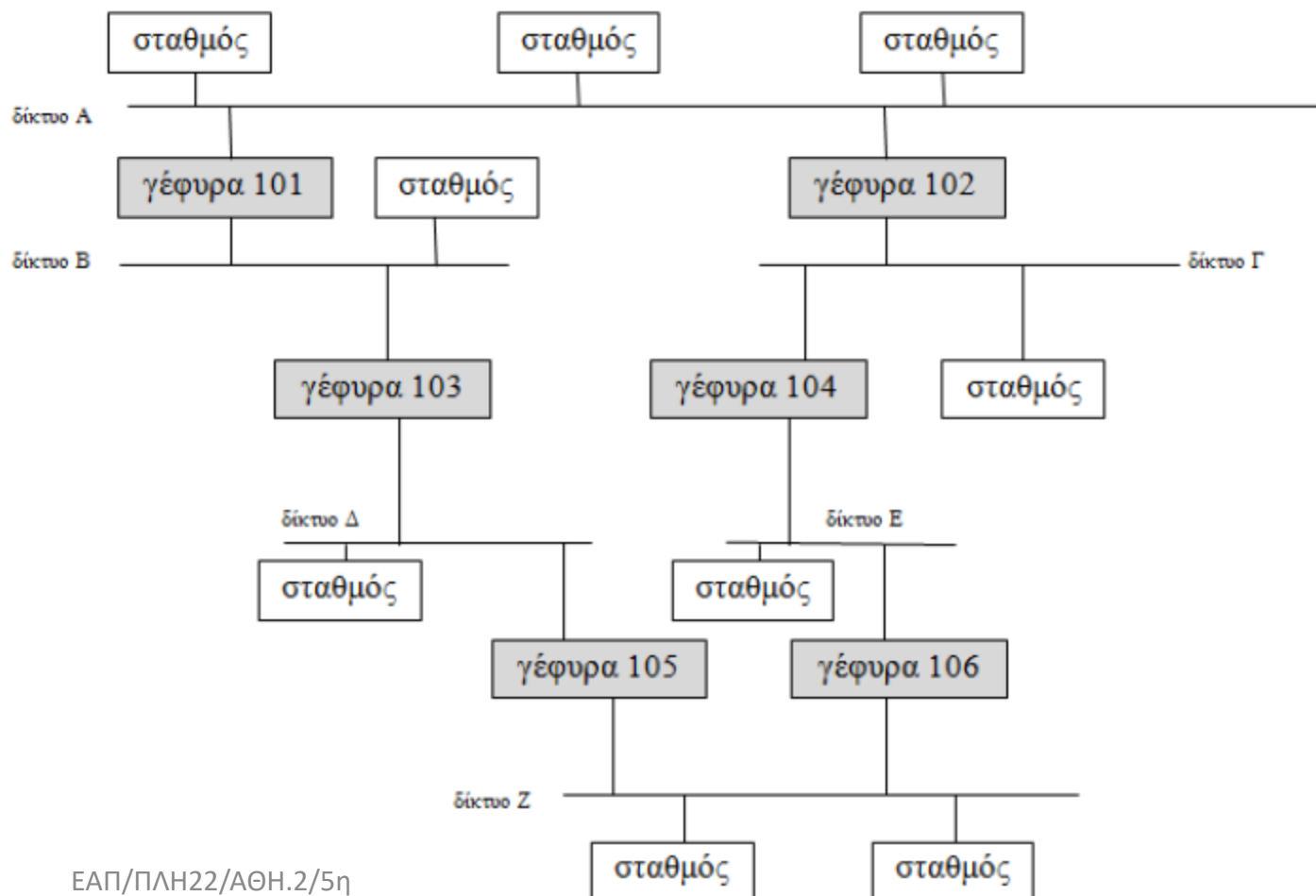
Δημιουργία Δέντρου Επικάλυψης



Γέφυρα	RP	DP	BP
B2	B2.1	B2.2, B2.4	B2.3
B3	B3.2	—	B3.1
B4	B4.1	B4.2	—

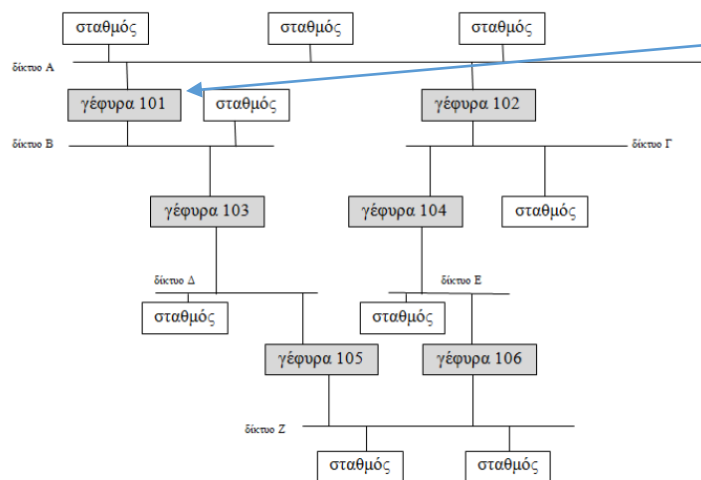
ΓΕ5/1415/Θ3

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.



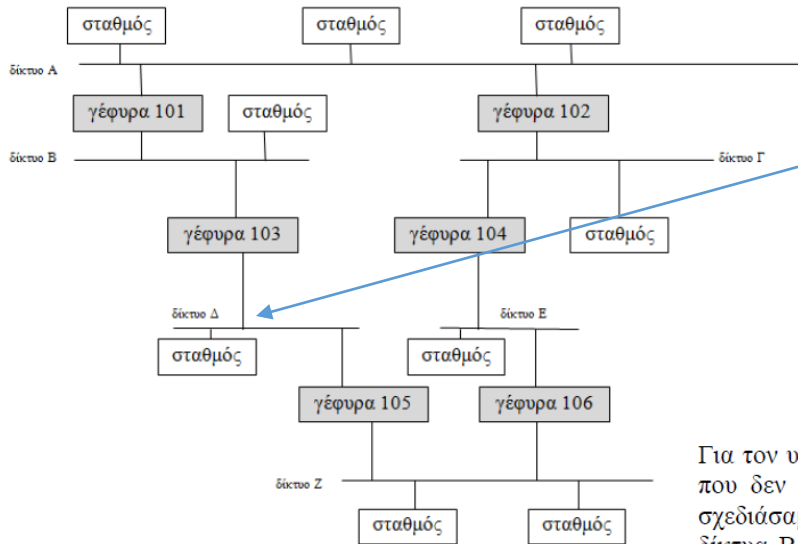
Κεντρική μήτρα δρομολόγησης:

		δίκτυο πομπού					
		A	B	Γ	Δ	E	Z
δίκτυο δέκτη	A	-	101	102	103	104	105
	B	101	-	102	103	106	105
	Γ	102	101	-	105	104	106
	Δ	101	103	104	-	106	105
	E	102	103	104	105	-	106
	Z	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
A	-	A	B	A	-	A	Γ
Γ	-	B	B	B	-	B	-
Δ	Δ	Γ	-	Δ	Ε	Γ	Γ
Ε	Δ	Ε	-	Ε	Ε	Δ	-
Z	Δ	Z	-	Z	Ε	Z	-



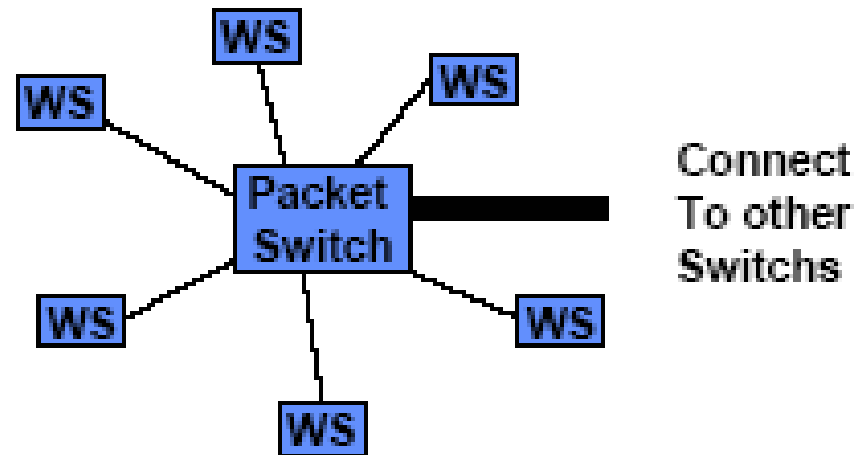
next hop

ΕΑΠ/ΠΛΗ22/ΑΘΗ.2/5η
 ΟΣΣ/28.04.2018/Ν.Δημητρίου

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-Z 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

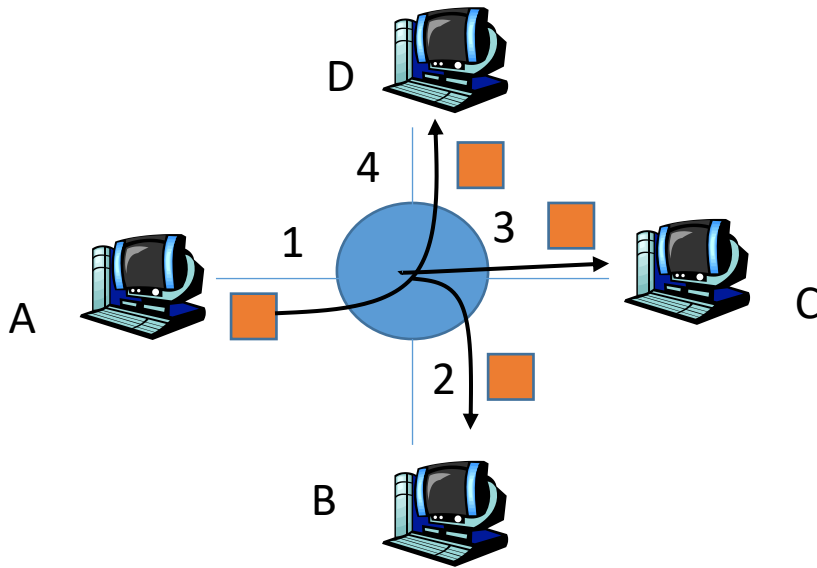
Στόχος της άσκησης είναι η εξοικείωση με τις τεχνολογίες Ethernet και TCP/IP

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

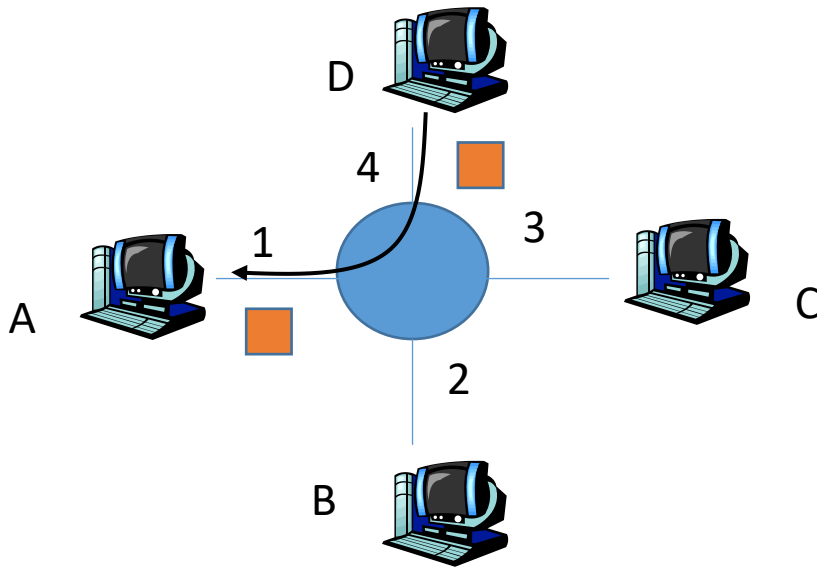
1. Να θεωρήσετε ένα Ethernet LAN switch στο οποίο είναι συνδεδεμένοι τέσσερις hosts: A, B, C, D. Οι κόμβοι χρησιμοποιούν την τοπολογία star για τη διασύνδεση των hosts A, B, C, D. Ο Host A είναι συνδεδεμένος στο interface 1 του μεταγωγέα, ο host B στο interface 2, ο host C στο interface 3 και ο host 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. Ο A αποστέλλει ένα πακέτο με τη MAC address του D
3. Ο 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. Ο D αποστέλλει ένα πακέτο με τη MAC address του A
3. Ο πίνακας του switch table έχει την εγγραφή (A,1) οπότε το πακέτο αποστέλλεται ΜΟΝΟ στη θύρα 1 και το σταθμό A.
4. Το switch ενημερώνει τον πίνακά του (D,4)

ΘΕΜΑ 1

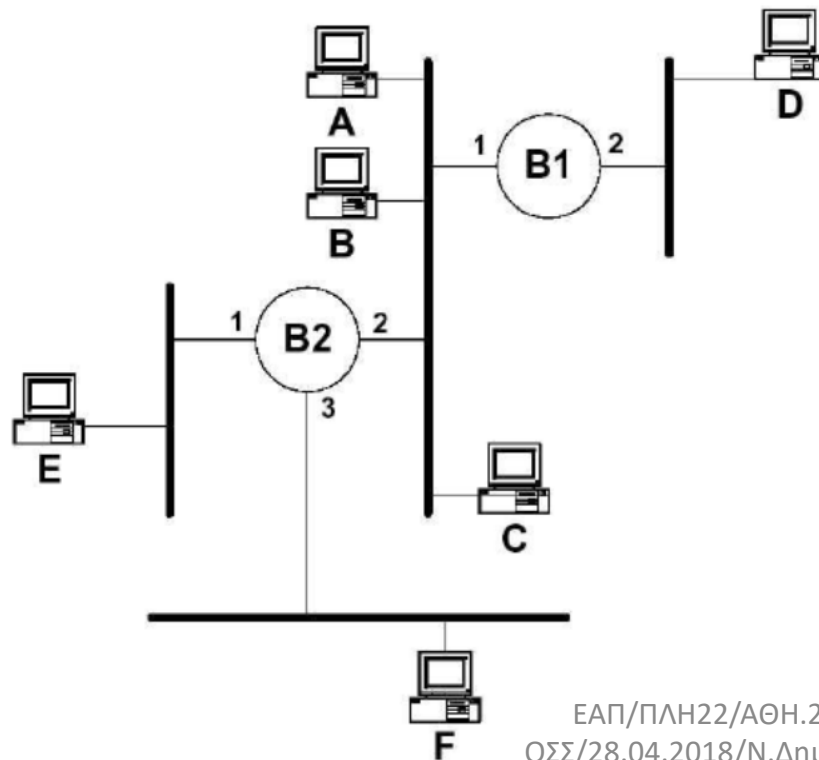
ΓΕ4/1314

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

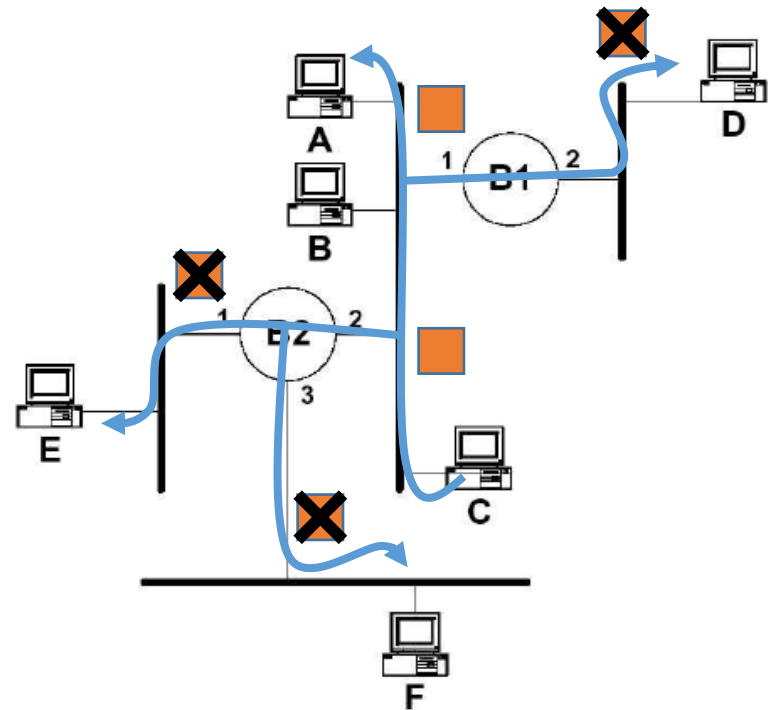
- C στέλνει στον A
- F στέλνει στον E
- E στέλνει στον F



Μετάδοση C - A

Bridge B1		Bridge B2	
C	1	C	2

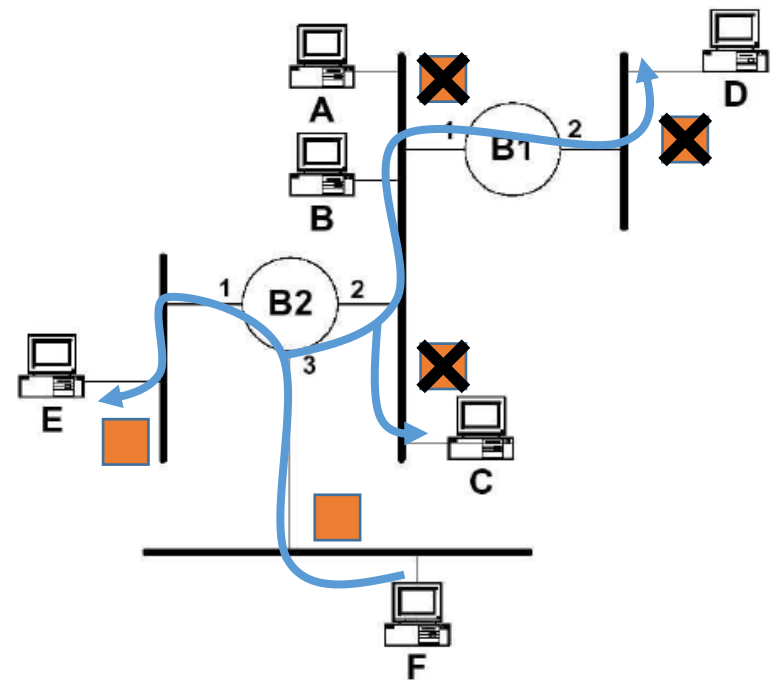
✗ → discarded



Μετάδοση F - E

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

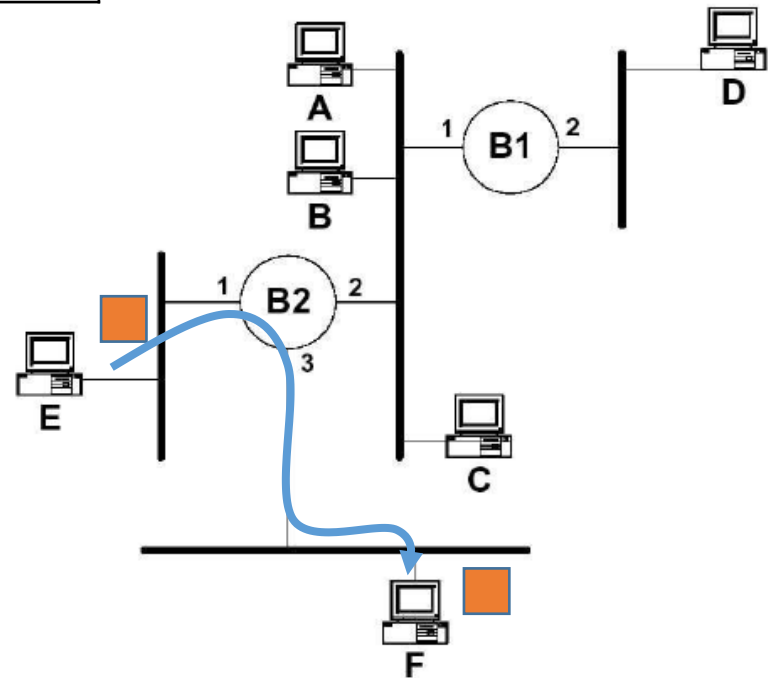
✗ → discarded



Μετάδοση E - F

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

Ο πίνακας της B2 έχει μια εγγραφή για το Σταθμό F . Το πακέτο αποστέλλεται Μόνο στη θύρα 3 της B2 και καταλήγει Στον παραλήπτη σταθμό F . Η B2 προσθέτει και την εγγραφή (E,1)

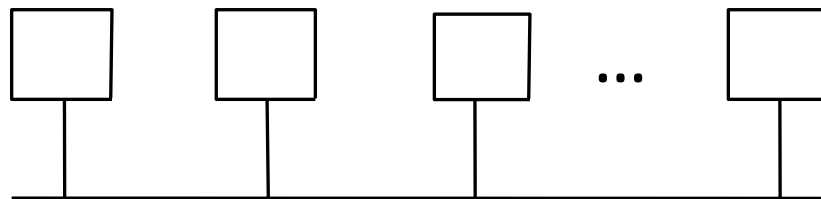


- Θέματα: MAC protocols, TDMA, FDMA, Aloha/Slotted Aloha, Aloha Throughput, CSMA, CSMA/CD, CSMA/CA
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_slides_2017-18.ppt*:

38-77

Συστήματα Πολλαπλής Πρόσβασης

- Συστήματα πολλαπλής πρόσβασης (multiple access)
- Οι κόμβοι συνδέονται σε κοινό κανάλι επικοινωνίας
- Συγκρούσεις συμβαίνουν όταν δύο ή περισσότεροι σταθμοί αποφασίσουν να στείλουν πακέτα ταυτόχρονα
- Έλεγχος πρόσβασης (access control): περιορίζει τη μείωση της απόδοσης λόγω συγκρούσεων και κενών περιόδων

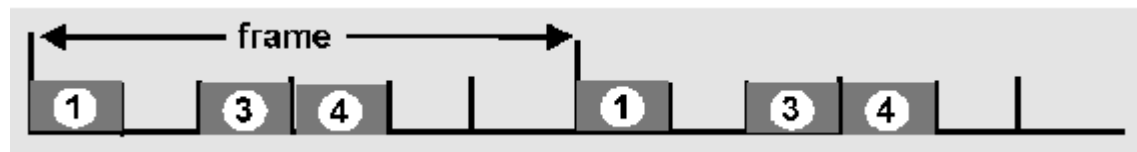


Έλεγχος Πολλαπλής Πρόσβασης

- TDM, FDM: χρησιμοποιούνται ευρέως σε ασύρματα συστήματα
- Ethernet: βασίζεται στο Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
 - περίμενε μέχρι το κανάλι να είναι κενό, τότε στείλε πακέτο
 - σταμάτησε τη μετάδοση αν συμβεί σύγκρουση
 - περίμενε τυχαίο χρόνο μετά την σύγκρουση
- ALOHA: λιγότερο “ευγενικό” από το Ethernet
 - μετέδωσε όταν ένα πακέτο είναι έτοιμο
 - περίμενε τυχαίο χρόνο μετά την σύγκρουση

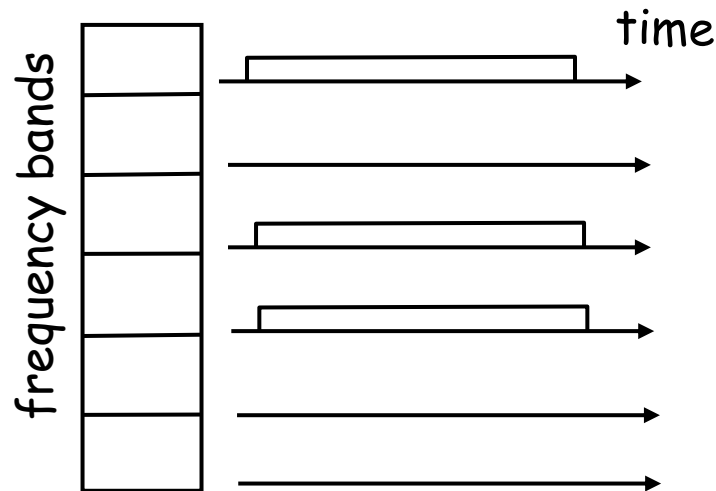
Πρωτόκολλα TDMA

- Πρόσβαση στο κανάλι σε «γύρους»
- Κάθε σταθμός δεσμεύει μία σχισμή σταθερού μήκους (μήκος = χρόνος μετάδοσης πακέτου) σε κάθε γύρο
- Οι μη χρησιμοποιούμενες σχισμές παραμένουν ανενεργές
- παράδειγμα: 6-σταθμών LAN, 1,3,4 έχουν πακέτα, ανενεργές οι σχισμές 2,5,6



Πρωτόκολλα FDMA

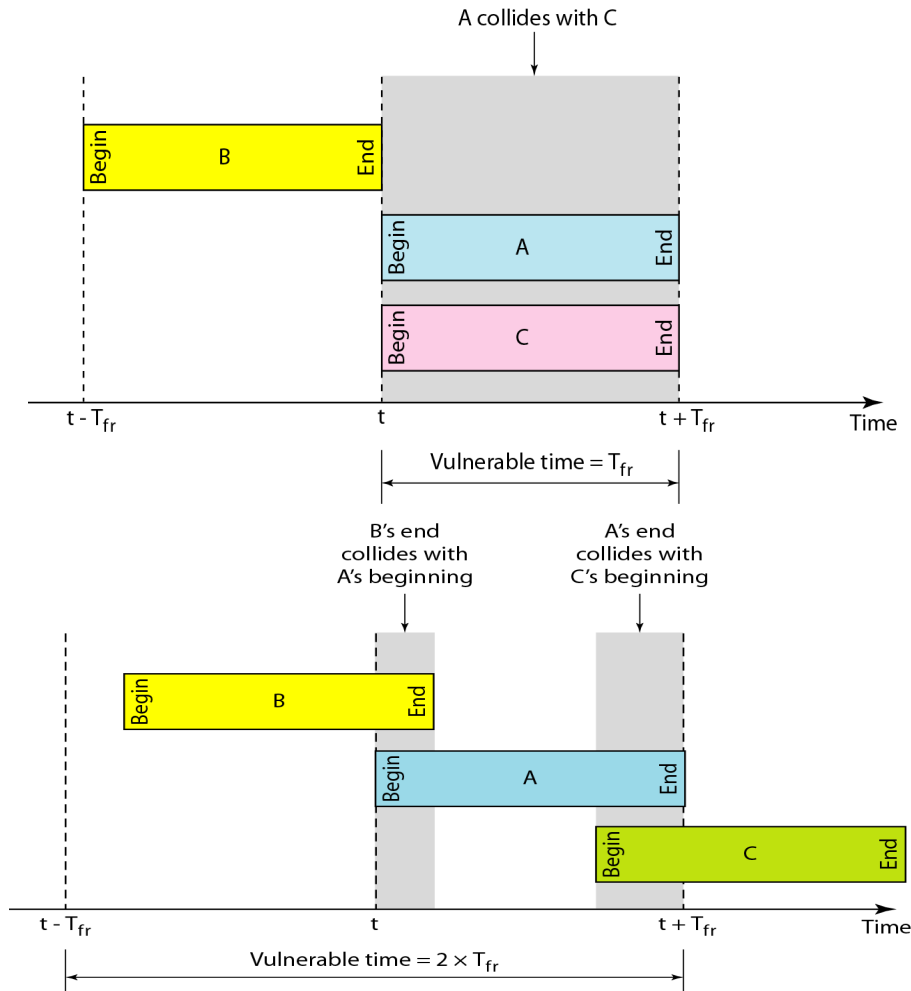
- το φάσμα του καναλιού χωρίζεται σε ζώνες συχνοτήτων
- σε κάθε σταθμό δίνεται συγκεκριμένη ζώνη συχνότητας
- στις ζώνες συχνοτήτων που δεν χρησιμοποιούνται, το αντίστοιχο φάσμα μένει ανενεργό
- παράδειγμα: 6-σταθμοί LAN, 1,3,4 έχουν πακέτα, οι ζώνες συχνοτήτων 2,5,6 είναι ανενεργές



Πρωτόκολλα Τυχαίας Προσπέλασης

- Όταν ένας κόμβος έχει πακέτο να στείλει
 - Μεταδίδει στον πλήρη ρυθμό του καναλιού
 - Δεν υπάρχει συγχρονισμός μεταξύ των κόμβων
- Δύο οι περισσότεροι κόμβοι μεταδίδουν \Rightarrow «σύγκρουση»
- το MAC πρωτόκολλο τυχαίας πρόσβασης καθορίζει:
 - Πως να ανιχνευθούν οι συγκρούσεις
 - Πως να ανακάμψει από τις συγκρούσεις (π.χ., μέσω καθυστερημένης αναμετάδοσης)
- Παραδείγματα από MAC πρωτόκολλα τυχαίας πρόσβασης:
 - slotted ALOHA
 - ALOHA
 - CSMA/CD, CSMA/CA

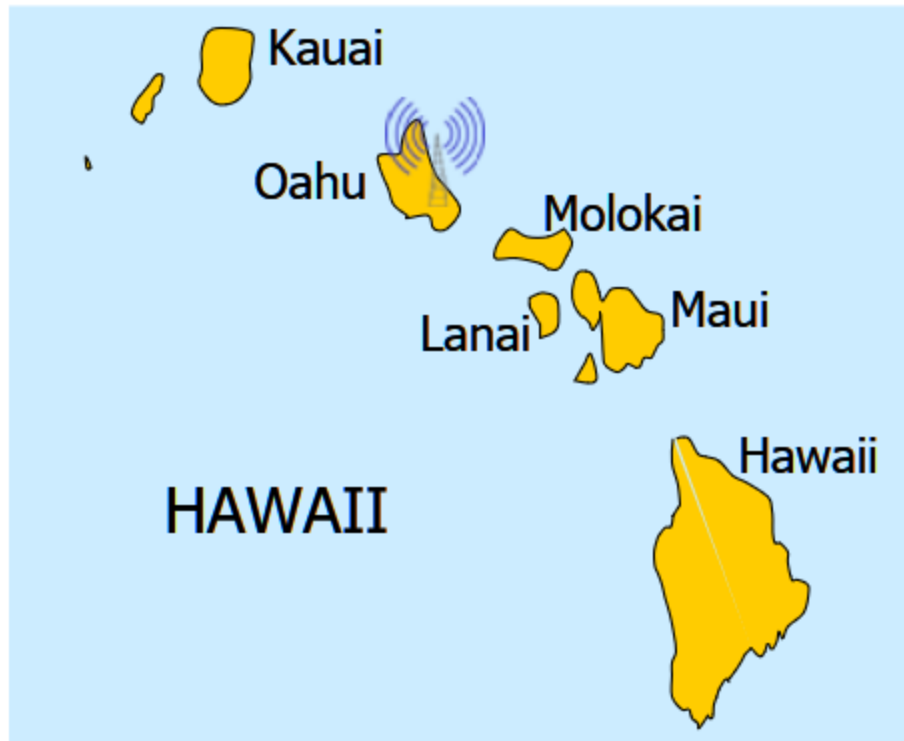
Επικίνδυνοι Περίοδοι για slotted και unslotted ALOHA



Πρωτόκολλα Τυχαίας Προσπέλασης

- Όταν ένας κόμβος έχει πακέτο να στείλει
 - Μεταδίδει στον πλήρη ρυθμό του καναλιού
 - Δεν υπάρχει συγχρονισμός μεταξύ των κόμβων
- Δύο οι περισσότεροι κόμβοι μεταδίδουν \Rightarrow «σύγκρουση»
- το MAC πρωτόκολλο τυχαίας πρόσβασης καθορίζει:
 - Πως να ανιχνευθούν οι συγκρούσεις
 - Πως να ανακάμψει από τις συγκρούσεις (π.χ., μέσω καθυστερημένης αναμετάδοσης)
- Παραδείγματα από MAC πρωτόκολλα τυχαίας πρόσβασης:
 - slotted ALOHA
 - ALOHA
 - CSMA/CD, CSMA/CA

Aloha motivation



The Aloha protocol was implemented in '70 also in a satellite network, named ALOHAnet.

N. Abramson, "The ALOHA System-Another Alternative for Computer Communications", *Fall Joint Computer Conference*, 1970.

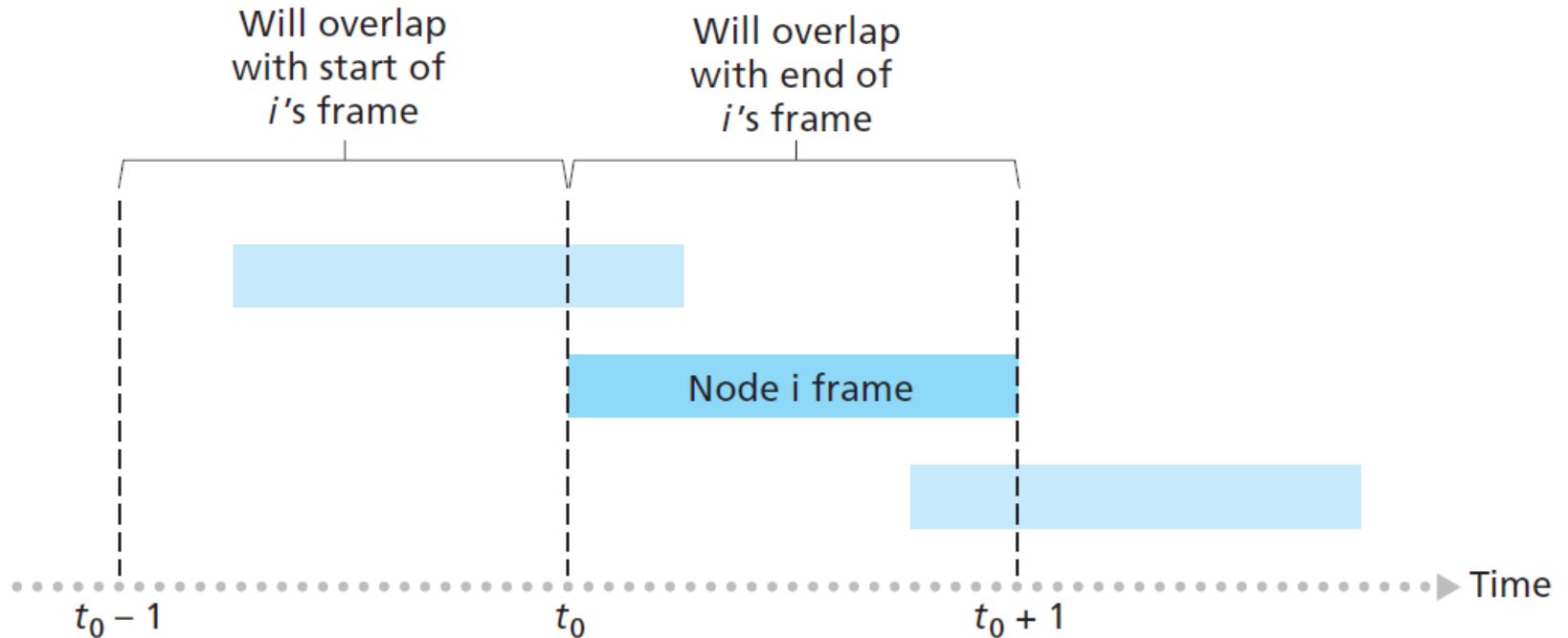
The Aloha protocol was proposed at the beginning of '70 by Professor Norman Abramson who needed to connect terminals dispersed among different islands and a central host (= controller) at the Hawaii University in Honolulu (Oahu island).

The main idea is **allowing terminals to transmit to the central controller as soon as they need to do so.**

- Collisions
- Mechanism to reveal collisions (The Aloha protocol is reliable: ACK and timer based on the round trip propagation delay or use of a broadcast channel)
- Retransmission attempts after a collision are rescheduled using a random **backoff** time

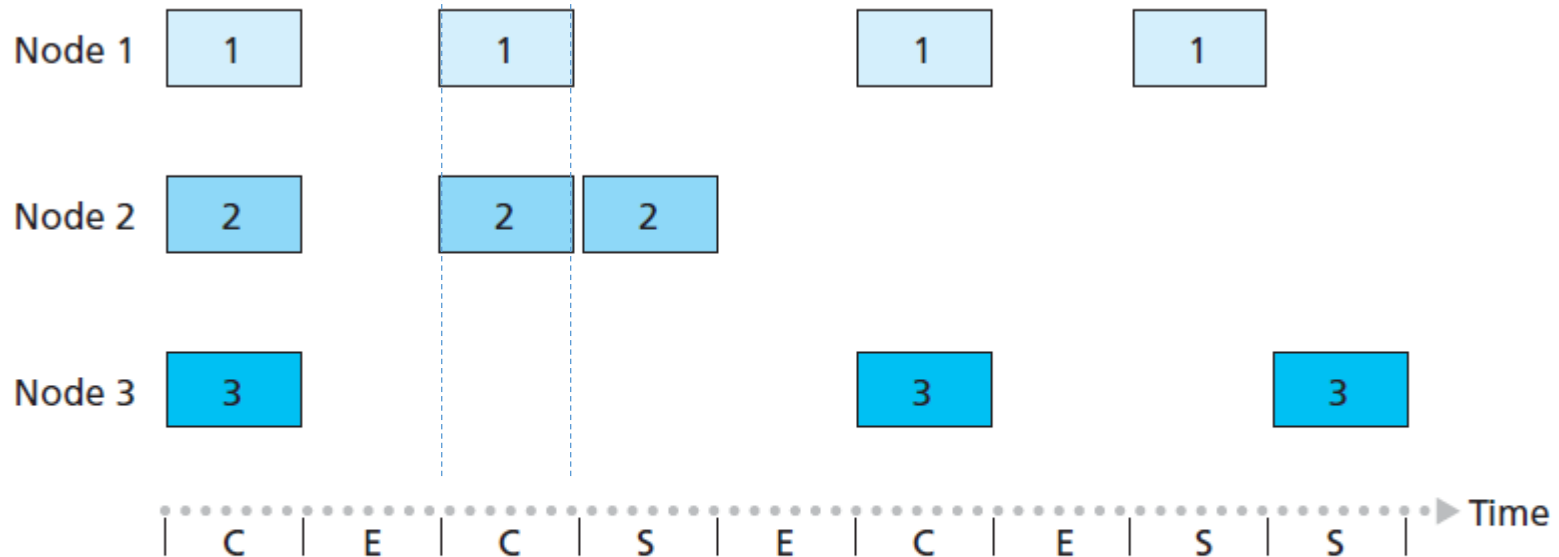
Note: Aloha is not an acronym, but the classical Hawaiian welcome expression.

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



Key:

C = Collision slot

E = Empty slot

S = Successful slot

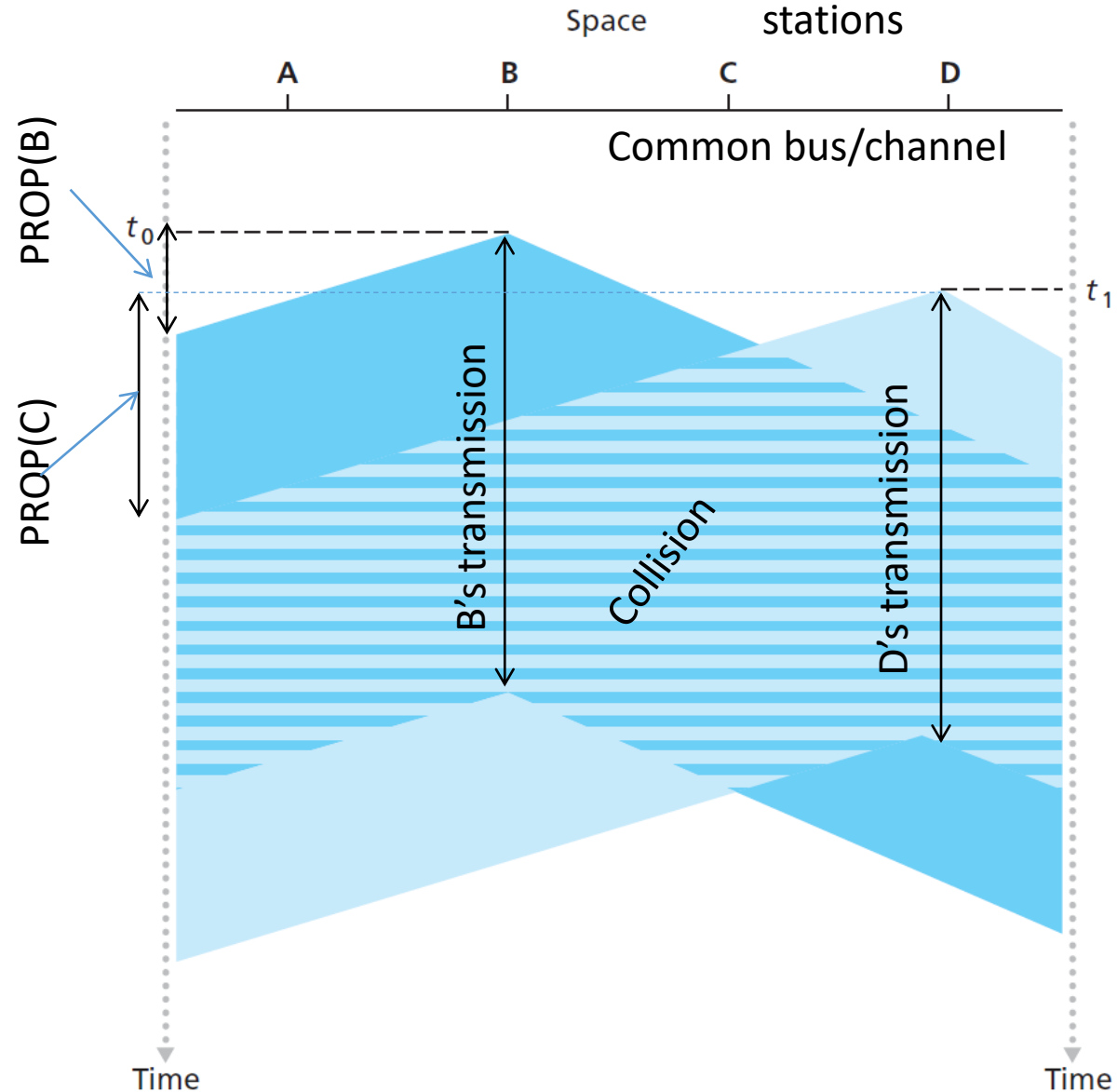
- To avoid collisions, no other nodes can begin their transmission in ONE timeslot duration
- That means that all other nodes should be silent for 1 timeslot (not 2 as shown in pure aloha)

Carrier Sense

- “Αισθανόμενος” τον φορέα (Carrier sensing) (“άκου πριν μιλήσεις”)
 - Ένας κόμβος “ακούει” το κανάλι πριν στείλει
 - Εάν υπάρχει μετάδοση στο κανάλι:
 - ένας κόμβος περιμένει για ένα τυχαίο χρονικό διάστημα (“backs off”) και μετά αισθάνεται ξανά το κανάλι
 - Εάν ένα κανάλι αισθανθεί να μην έχει κίνηση, τότε ξεκινάει η μετάδοση του πλαισίου
- Εντοπισμός σύγκρουσης (Collision detection) (“Εάν κάποιος άλλος αρχίζει να μιλάει την ίδια ώρα, σταμάτα να μιλάς”)
 - Ένας κόμβος που μεταδίδει ακούει το κανάλι καθώς μεταδίδει
 - Εάν εντοπίσει ότι κάποιος άλλος κόμβος μεταδίδει ένα πλαίσιο που προκαλεί παρεμβολές:
 - σταματάει να μεταδίδει και χρησιμοποιεί κάποιο πρωτόκολλο για να προσδιορίσει πότε θα προσπαθήσει ξανά να μεταδώσει

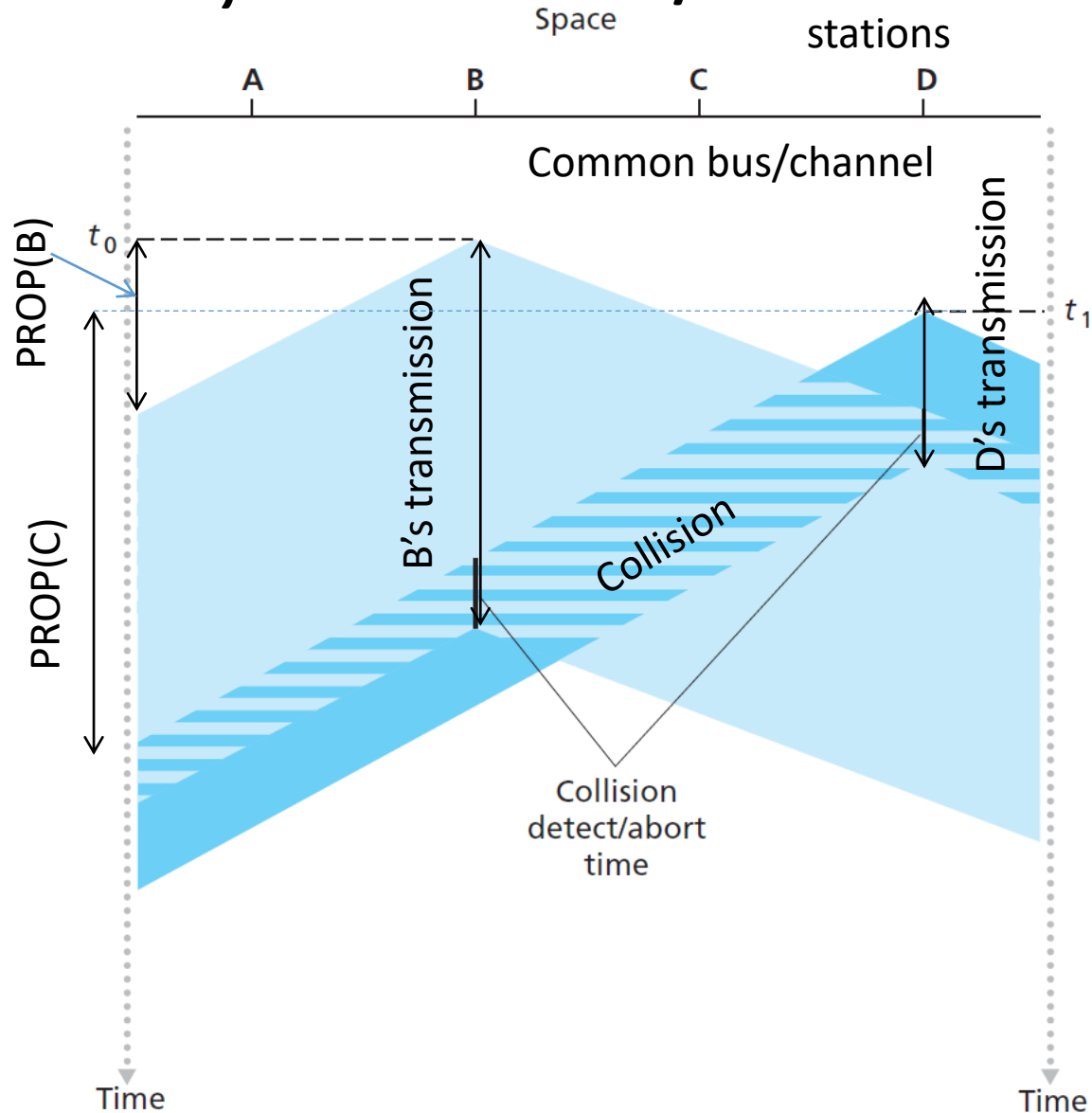
Συγκρούσεις στο CSMA

- 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

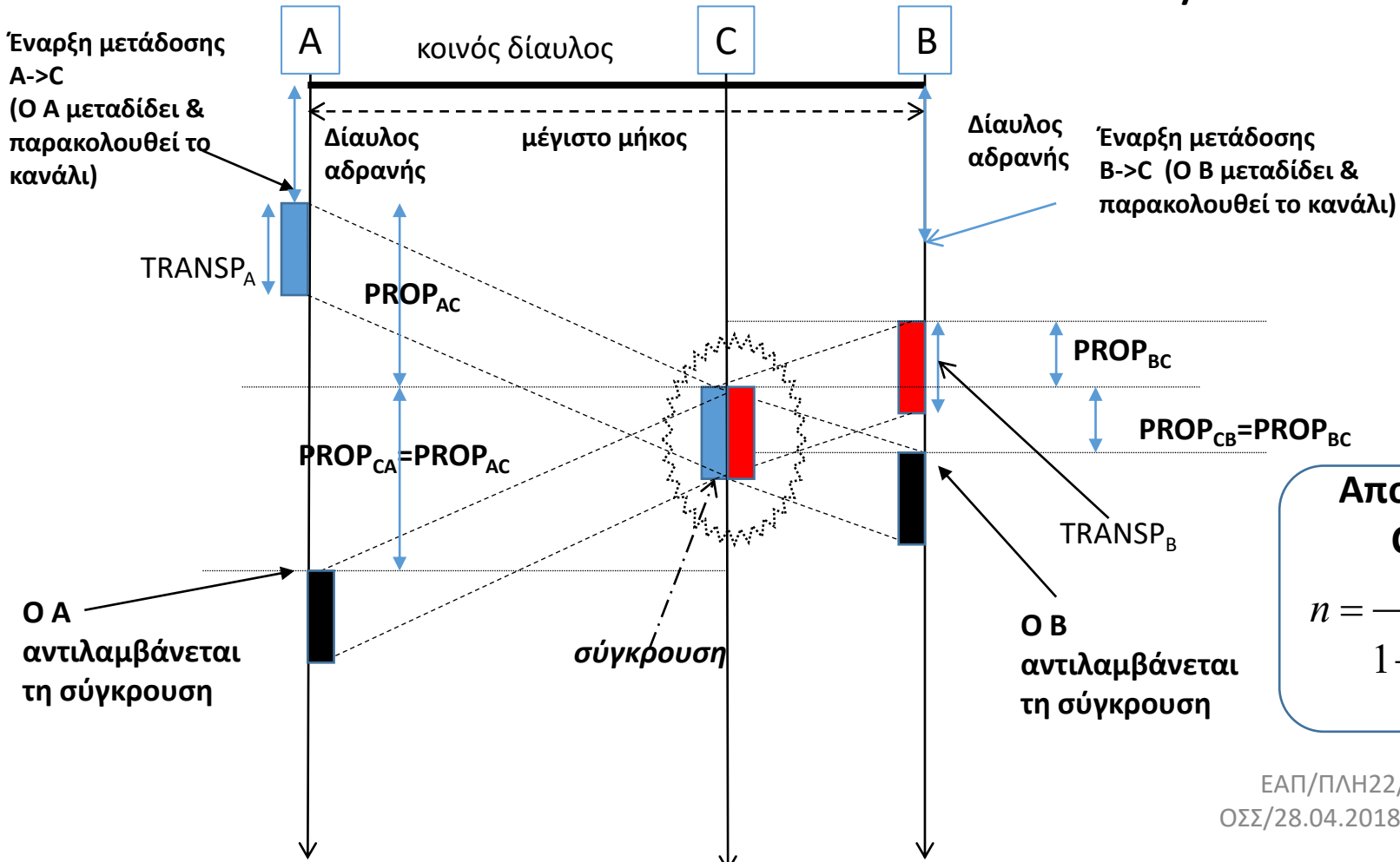


Συγκρούσεις στο CSMA/CD

- 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

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

ΕΑΠ/ΠΛΗ22/ΑΘΗ.2/5η
 ΟΣΣ/28.04.2018/Ν.Δημητρίου

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

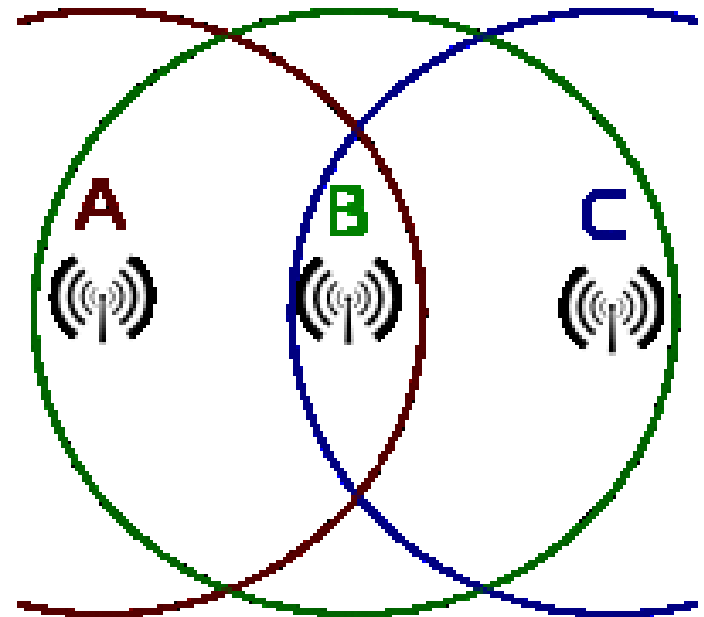
Χειρότερη περίπτωση: Ο C ταυτίζεται με το B (είναι στη μέγιστη δυνατή απόσταση από τον A)
 $TRANSP \geq 2PROP_{MAX}$ (μέγιστος χρόνος διάδοσης ενός bit end-end)

Εξέλιξη CSMA/CD για ασύρματα μέσα: CSMA/CA

- 2 επιπλέον σημαντικά προβλήματα
 - Hidden node problem
 - Exposed node problem

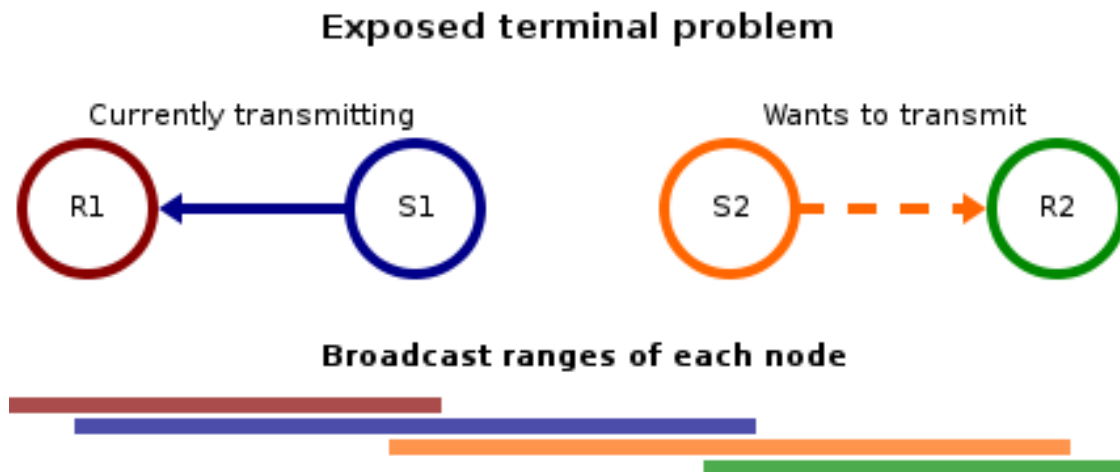
Hidden node problem

- Κατάσταση
 - Ο A ακούει τον B
 - Ο C ακούει τον B
 - Ο A είναι κρυμμένος από τον C και το ανάποδο
- Πρόβλημα:
 - Πως θα συγχρονιστούν A και C να μην μεταδώσουν ο ένας πάνω στον άλλο ?



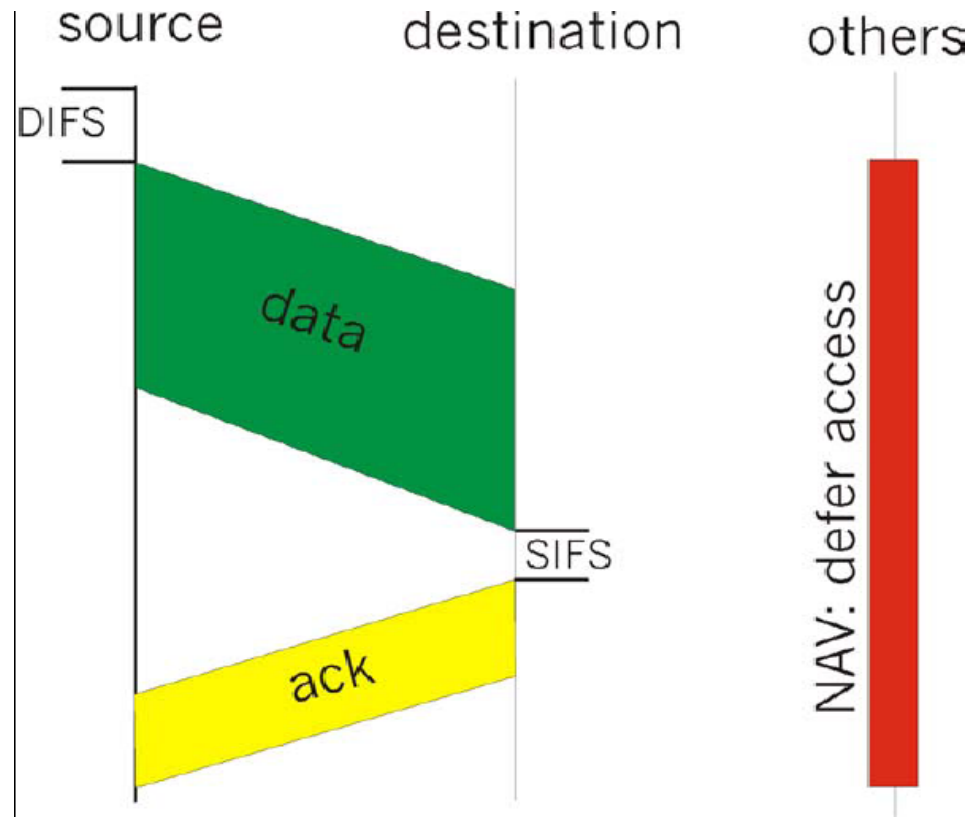
Exposed node problem

- Κατάσταση
 - Λόγω της $S1 \rightarrow R1$ μετάδοσης ο $S2$ αντιλαμβάνεται busy μέσο και δεν μεταδίδει στον $R2$ ενώ μπορεί
- Πρόβλημα:
 - Πως ο $S2$ μπορεί να καταλάβει ότι μπορεί να μεταδώσει προς $R2$ χωρίς σύγκρουση



IEEE 802.11 MAC: CSMA/CA

- 802.11 CSMA: εκπομπή
 - Εάν ο δίαυλος είναι αδρανής για DIFS sec. Τότε στέλνεται ένα πλαίσιο (δεν ανιχνεύεται σύγκρουση)
 - Εάν ο δίαυλος είναι κατειλημμένος τότε γίνεται δυαδική οπισθοχώρηση
- 802.11 CSMA λήψη:
 - Εάν το πλαίσιο ληφθεί σωστά αποστέλλεται ACK μετά από SIFS sec



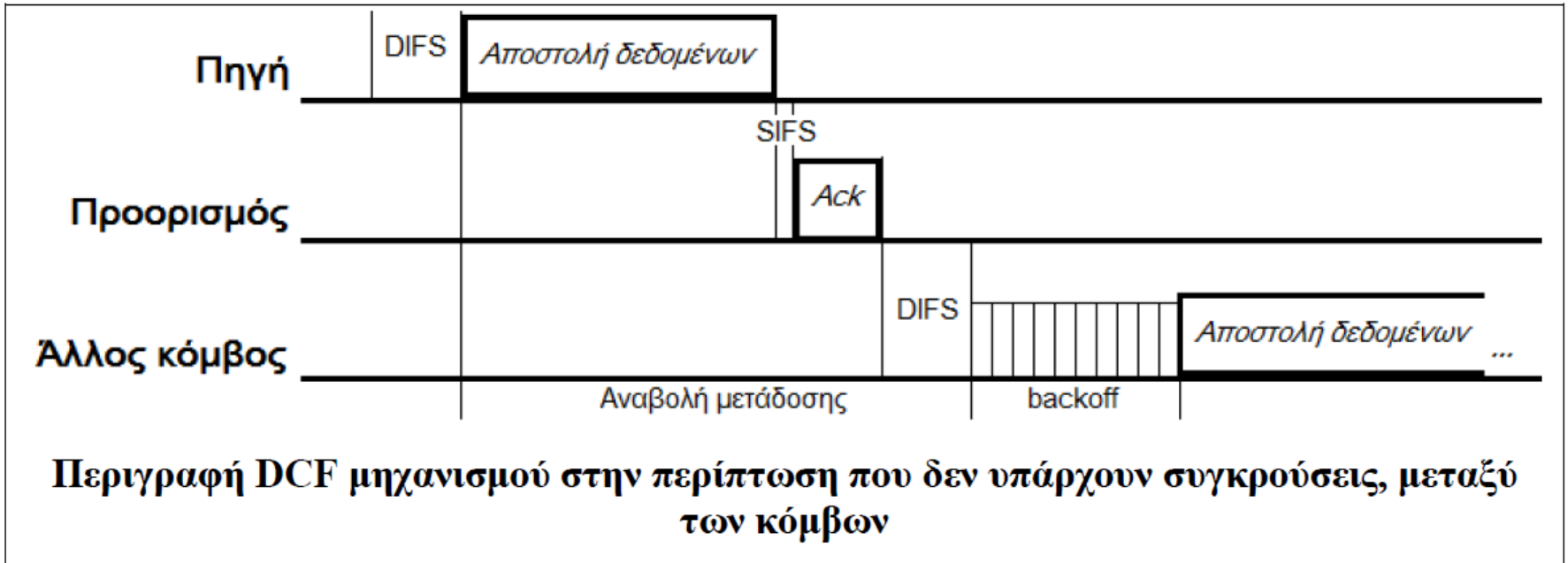
ΘΕΜΑ 1

ΓΕ5/1415

Στόχος της άσκησης είναι η εξοικείωση με την διαδικασία *backoff* και γενικότερα με την λειτουργία των ασύρματων δικτύων.

Σχετικές ασκήσεις: Δεν υπάρχουν.

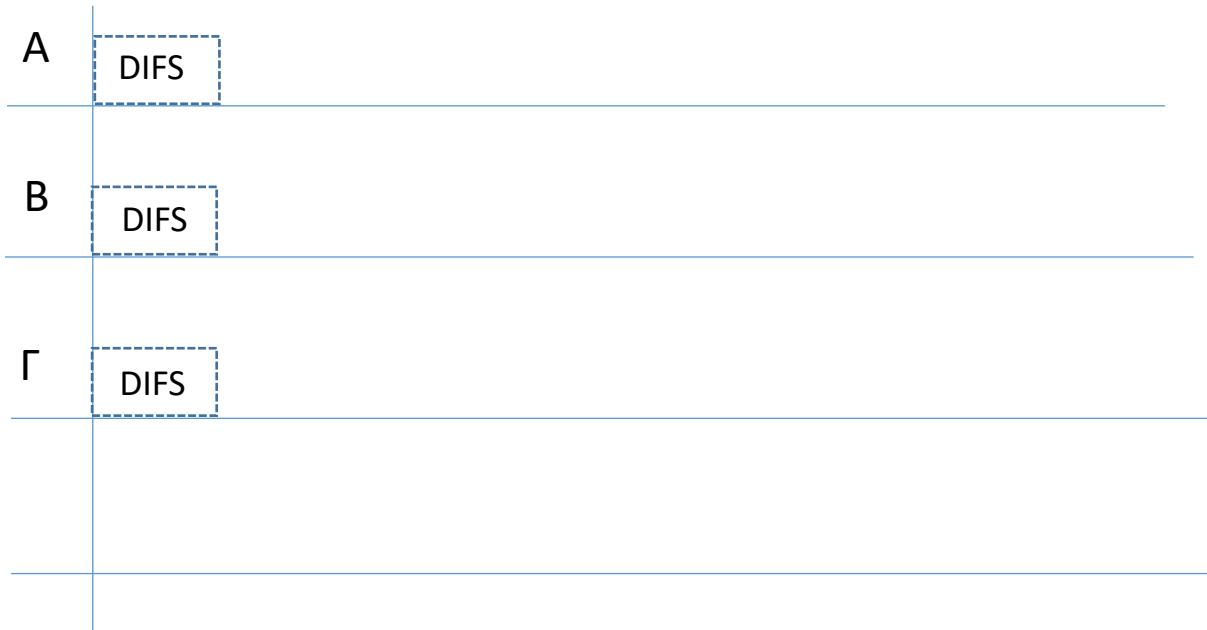
Σε ένα δίκτυο 802.11 DCF, 3 τερματικά (Α, Β, Γ) προσπαθούν να μεταδώσουν από ένα πακέτο. Όταν το κανάλι γίνει διαθέσιμο, με τη διαδικασία *backoff*, το τερματικό Α διαλέγει παράθυρο (CW) 3, το τερματικό Β διαλέγει παράθυρο (CW) 15, και το τερματικό Γ διαλέγει παράθυρο (CW) 10. Να υπολογίσετε τις χρονικές στιγμές που θα ολοκληρωθεί η μετάδοση των τριών πακέτων των τερματικών, και τις χρονικές στιγμές που θα ολοκληρωθεί η λήψη των αντίστοιχων επαληθεύσεων. Δίδονται: $\text{Slottime} = 9\mu\text{s}$, $\text{SIFS} = 16\mu\text{s}$, $\text{DIFS} = 34\mu\text{s}$. Η μετάδοση του κάθε πακέτου, μαζί με τις επικεφαλίδες και το preamble καταλαμβάνει $1300\mu\text{s}$ στο κανάλι, ενώ αντίστοιχα οι επαληθεύσεις, μαζί με τα headers και το preamble καταλαμβάνουν από $200\mu\text{s}$. Δεν χρησιμοποιείται ο μηχανισμός RTS/CTS. Θεωρείστε επίσης ότι σε περίπτωση σύγκρουσης οι σταθμοί αρχικά περιμένουν για χρονικό διάστημα ίσο με DIFS πριν ξεκινήσουν τη διαδικασία οπισθοχώρησης. Επίσης θεωρείστε ότι όταν ο μετρητής ενός σταθμού μηδενιστεί ο σταθμός ξεκινά τη μετάδοση αμέσως.



Τα τερματικά Α, Β και Γ περιμένουν για χρόνο DIFS= $34\mu\text{s}$ και στη συνέχεια προσπαθούν να μεταδώσουν ταυτόχρονα με αποτέλεσμα να υπάρξει σύγκρουση.

Στη συνέχεια κάθε τερματικό περιμένει μέχρι να ανιχνεύσει ελεύθερο το κανάλι για χρόνο DIFS. Έτσι ύστερα από DIFS= $34\mu\text{s}$:

- Ο Α διαλέγει το παράθυρο 3
- Ο Β διαλέγει το παράθυρο 15
- Ο Γ διαλέγει το παράθυρο 10

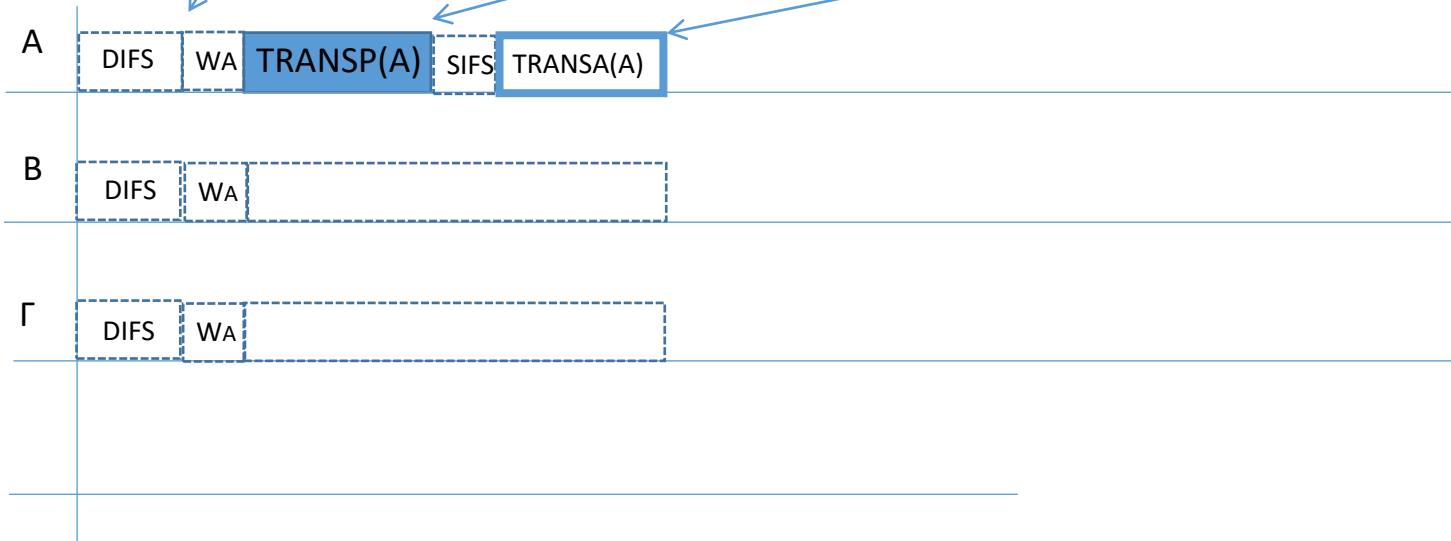


Οι μετρητές των A, B και Γ αρχίζουν να μετρούν αντίστροφα. Σημειώνουμε ότι η τιμή του κάθε μετρητή μειώνεται κατά ένα κάθε φορά που περνάει ένα slot, δηλαδή κάθε 9μs.

Υστερα από $3 \cdot 9\mu s = 27\mu s$ ο μετρητής του A μηδενίζεται και ο A ξεκινάει τη μετάδοση. Σε αυτό το σημείο σταματάνε οι μετρητές των B και Γ, έχοντας τις τιμές $15 - 3 = 12$ και $10 - 3 = 7$, αντίστοιχα.

Η μετάδοση του πακέτου από τον A διαρκεί **1300μs**, κάτι το οποίο συνεπάγεται ότι η χρονική στιγμή ολοκλήρωσης της συγκεκριμένης μετάδοσης είναι η $34 + 34 + 27 + 1300 = \underline{1395\mu s}$.

Στη συνέχεια ο παραλήπτης περιμένει για χρόνο SIFS=**16μs** και ακολούθως στέλνει πίσω στον A την επαλήθευση. Η αποστολή της επαλήθευσης διαρκεί **200μs**. Έτσι, η χρονική στιγμή κατά την οποία θα ολοκληρωθεί η λήψη της επαλήθευσης είναι η $1395 + 16 + 200 = \underline{1611\mu s}$.

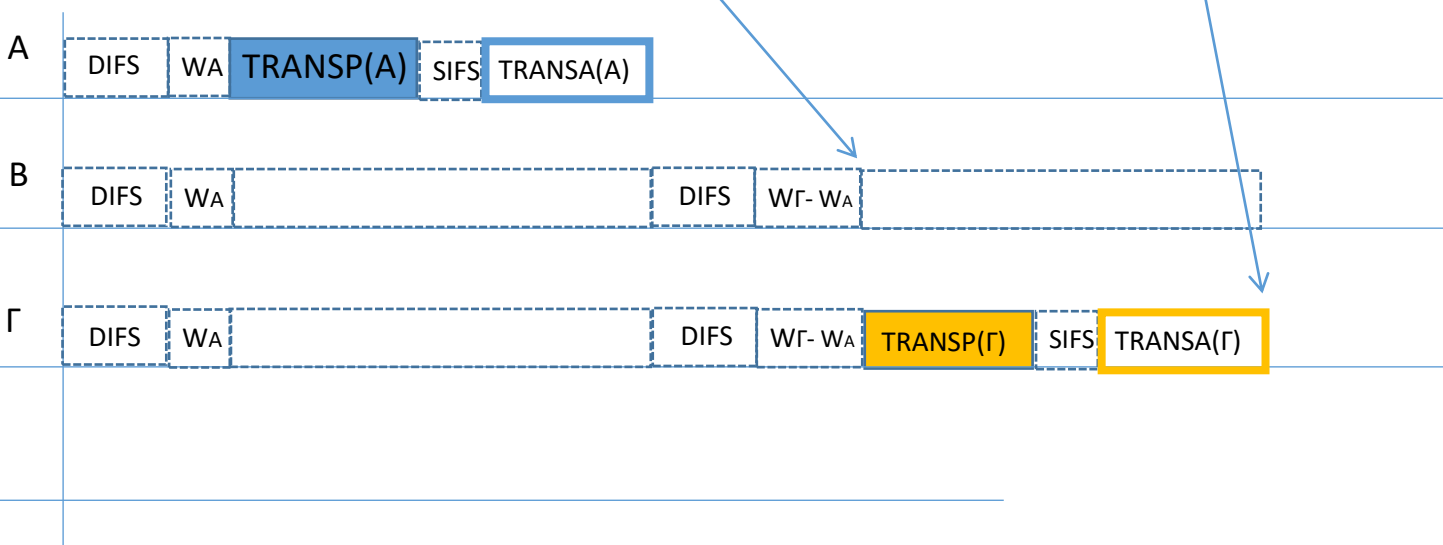


Στη συνέχεια οι Β και Γ συνεχίζουν την αντίστροφη μέτρηση (βρίσκονται σε διαδικασία backoff, για αυτό απλά ενεργοποιείται ξανά η αντίστροφη μέτρηση) αφού πρώτα περιμένουν για χρόνο DIFS.

Ύστερα από $7 \cdot 9\mu\text{s} = 63\mu\text{s}$ ο μετρητής του Γ μηδενίζεται και ο Γ ξεκινάει τη μετάδοση. Σε αυτό το σημείο σταματάει ο μετρητής του Β, έχοντας την τιμή $12 - 7 = 5$.

Η μετάδοση του πακέτου από τον Γ διαρκεί **1300μs**, κάτι το οποίο συνεπάγεται ότι η χρονική στιγμή ολοκλήρωσης της συγκεκριμένης μετάδοσης είναι η $1611 + 34 + 63 + 1300 = 3008\mu\text{s}$.

Στη συνέχεια ο παραλήπτης περιμένει για χρόνο SIFS = **16μs** και ακολούθως στέλνει πίσω στον Γ την επαλήθευση. Η αποστολή της επαλήθευσης διαρκεί **200μs**. Έτσι, η χρονική στιγμή κατά την οποία θα ολοκληρωθεί η λήψη της επαλήθευσης είναι η $3008 + 16 + 200 = 3224\mu\text{s}$.

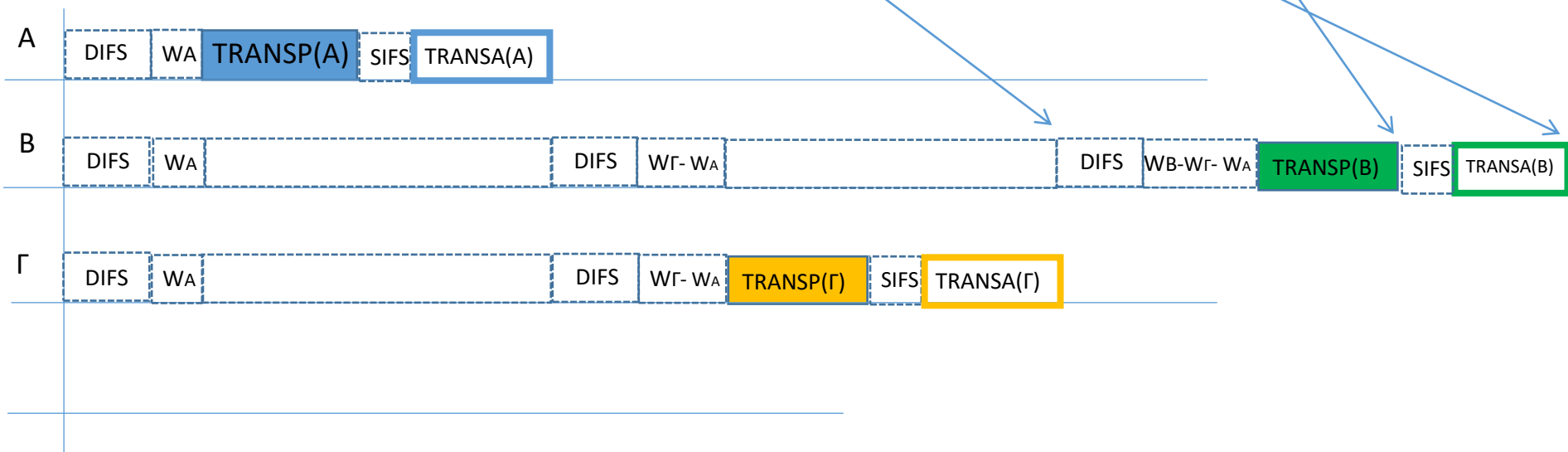


Στη συνέχεια οι B συνεχίζει την αντίστροφη μέτρηση μετά από χρόνο DIFS.

Ύστερα από $5 \cdot 9\mu\text{s} = 45\mu\text{s}$ ο μετρητής του B μηδενίζεται και ο B ξεκινάει τη μετάδοση.

Η μετάδοση του πακέτου από τον B διαρκεί **1300μs**, κάτι το οποίο συνεπάγεται ότι η χρονική στιγμή ολοκλήρωσης της συγκεκριμένης μετάδοσης είναι η $3224+34+45+1300 = \underline{4603\mu\text{s}}$.

Στη συνέχεια ο παραλήπτης περιμένει για χρόνο SIFS=**16μs** και ακολούθως στέλνει πίσω στον Γ την επαλήθευση. Η αποστολή της επαλήθευσης διαρκεί **200μs**. Έτσι, η χρονική στιγμή κατά την οποία θα ολοκληρωθεί η λήψη της επαλήθευσης είναι η $4603+16+200 = \underline{4819\mu\text{s}}$.

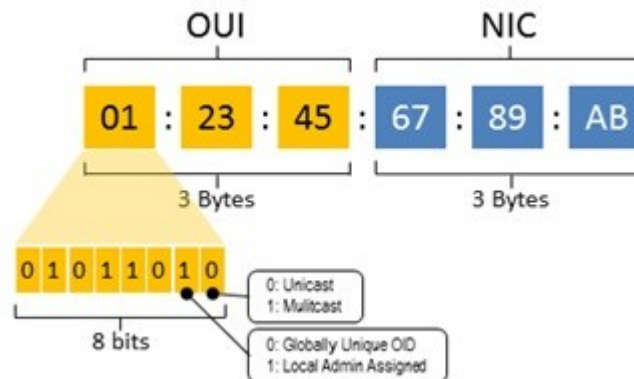


- Θέματα: IP Addressing, Subnets, Subnet Mask, Network/host addresses, Routing
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_slides_2017-18.ppt* :

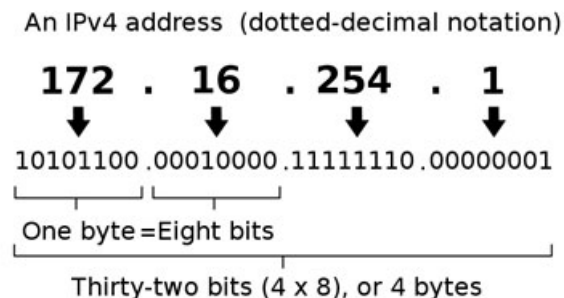
78-107

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



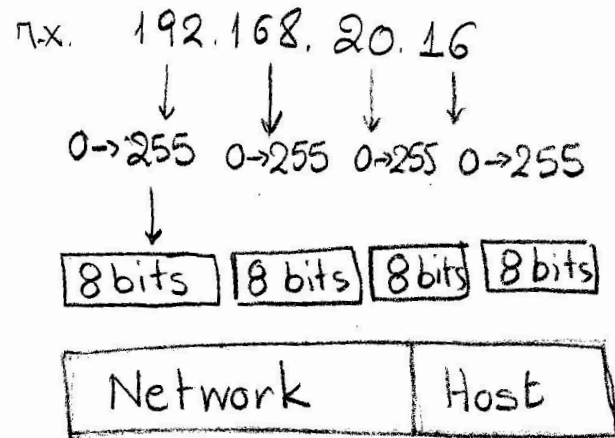
IP Διευθύνσεις (1)

- Κάθε IP διεύθυνση αποτελείται από το παρακάτω ζευγάρι αριθμών
 - IP address=<network number><host number>
 - Το network number (αριθμός δικτύου) είναι μοναδική IP διεύθυνση η οποία διαχειρίζεται από τον οργανισμό Internet Network Information Center
 - Το host number (αριθμός κόμβου) καθορίζει κάποιο host σε ένα Δίκτυο
- Οι IP διευθύνσεις έχουν μήκος 32 bit
 - Διαχωρίζεται σε 4 groups των 8 bits
 - Κάθε οκτάδα αναπαριστάται σαν αριθμός στο δεκαδικό σύστημα (κλίμακα 0...255). Διαχωρισμός της κάθε οκτάδας με στίγμα
 - π.χ. 128.2.7.10

IP Διευθύνσεις (2)

- Ο αριθμός κόμβου που έχει όλα bits ίσα με '1' δεσμεύεται ως η *διεύθυνση εκπομπής (broadcast address)* του δικτύου (π.χ. 128.2.255.255)
- Ο αριθμός κόμβου που έχει όλα bits ίσα με '0' αντιστοιχεί στη *διεύθυνση δικτύου* (προσδιορίζει όλο το δίκτυο π.χ. 197.54.40.0)
- Οι δύο παραπάνω αριθμοί κόμβου ΔΕΝ μπορούν να δοθούν σε κόμβο του δικτύου
 - άρα εάν n bits για αριθμό κόμβων, μπορούν να εξυπηρετηθούν $2^n - 2$ κόμβοι
- Υπάρχουν πέντε κατηγορίες IP διευθύνσεων οι οποίες ονομάζονται *κλάσεις* (classes)

IP Addressing



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

11111111.11111111.11111111.00000000

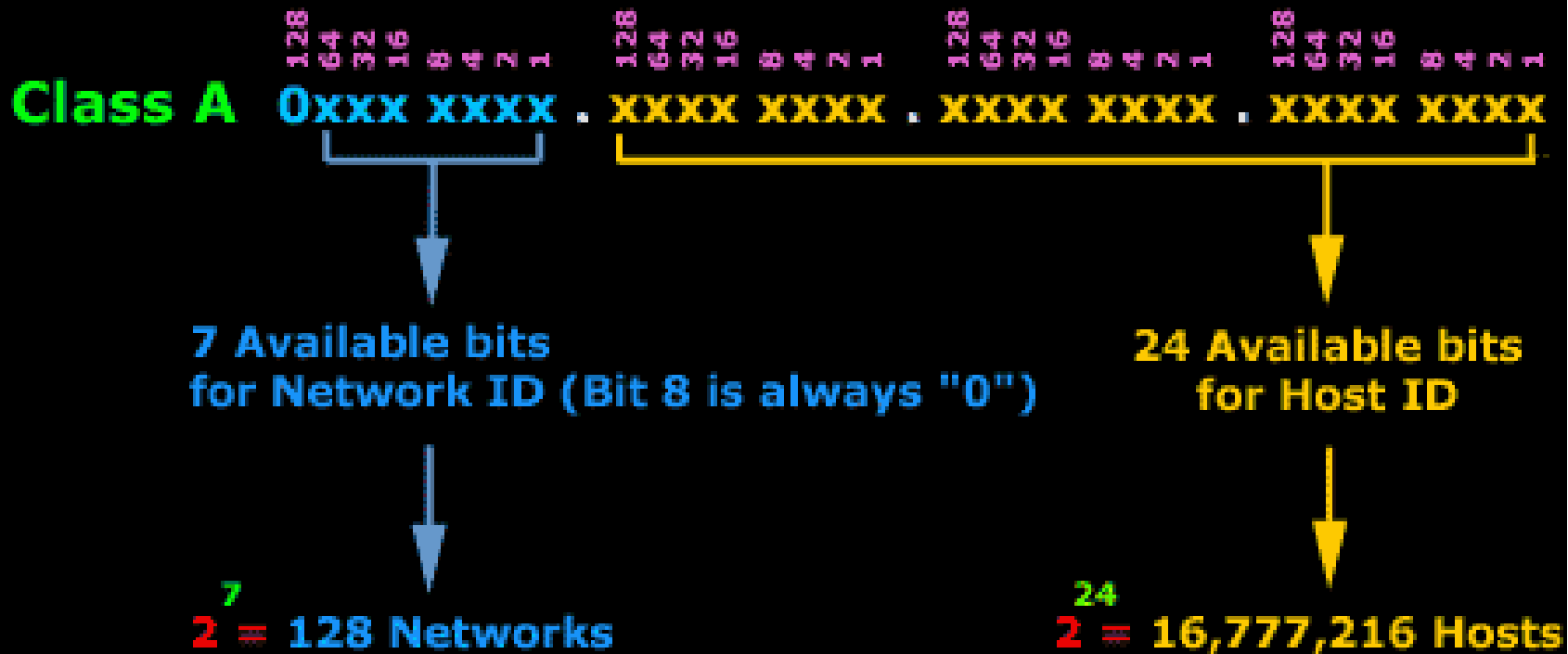
IP Address /24

Identifying Network and Host ID

	128 128 128 128	16 16 16 16	0 0 0 0	1 1 1 1		128 128 128 128	16 16 16 16	0 0 0 0	1 1 1 1		128 128 128 128	16 16 16 16	0 0 0 0	1 1 1 1
Class A	<u>0xxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>
	CLASS A NETWORK ID					CLASS A HOST ID								
Class B	<u>10xx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>
	CLASS B NETWORK ID					CLASS B HOST ID								
Class C	<u>110x</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>
	CLASS C NETWORK ID					CLASS C HOST ID								
Class D	Multicast													
	<u>1110</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>
	CLASS D NETWORK ID													
Class E	Reserved Experimental													
	<u>1111</u>	<u>0xxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>	.	<u>xxxx</u>	<u>xxxx</u>
	CLASS E NETWORK ID													

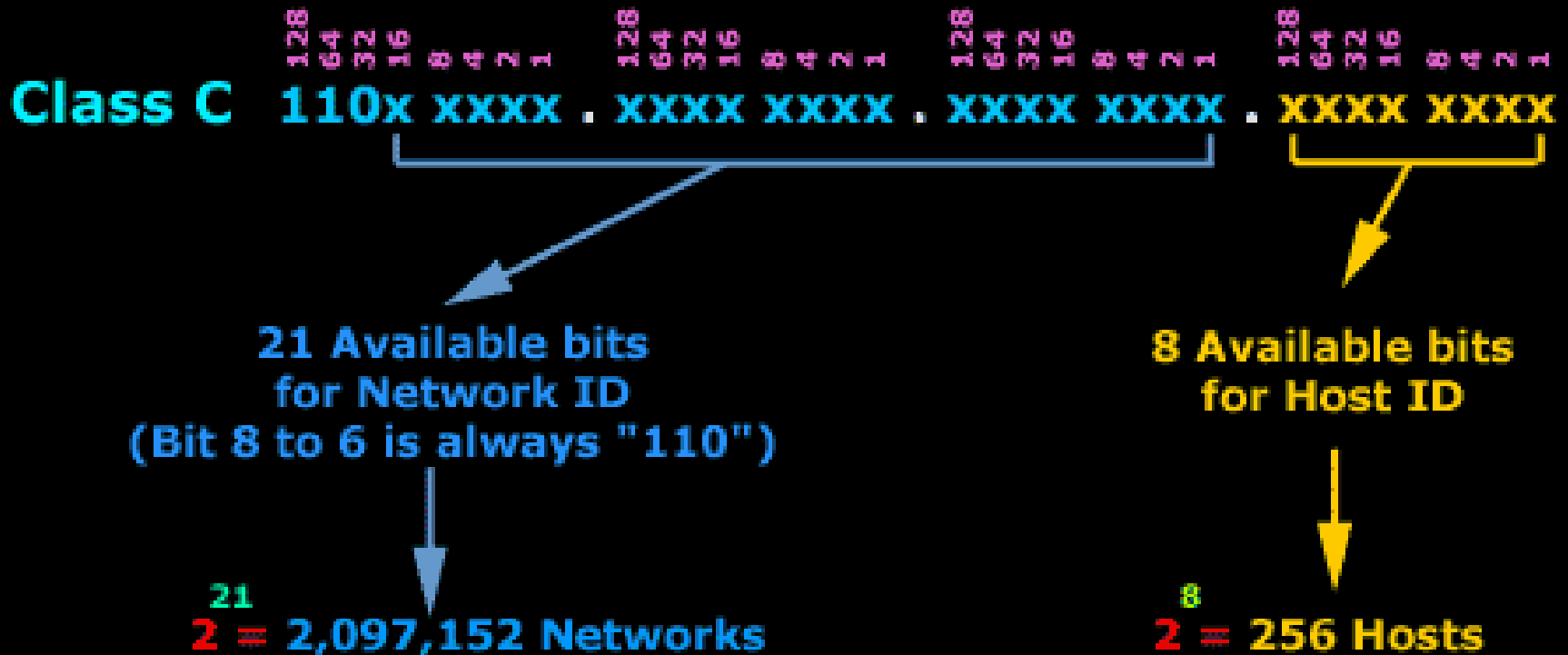
Here you see each Class's Network and Host ID portion. Notice that there are only few Class A networks (Network ID), but many Host ID's, where as a Class C has a lot more Networks and fewer Host ID's.

Analysis of a Class A Network



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



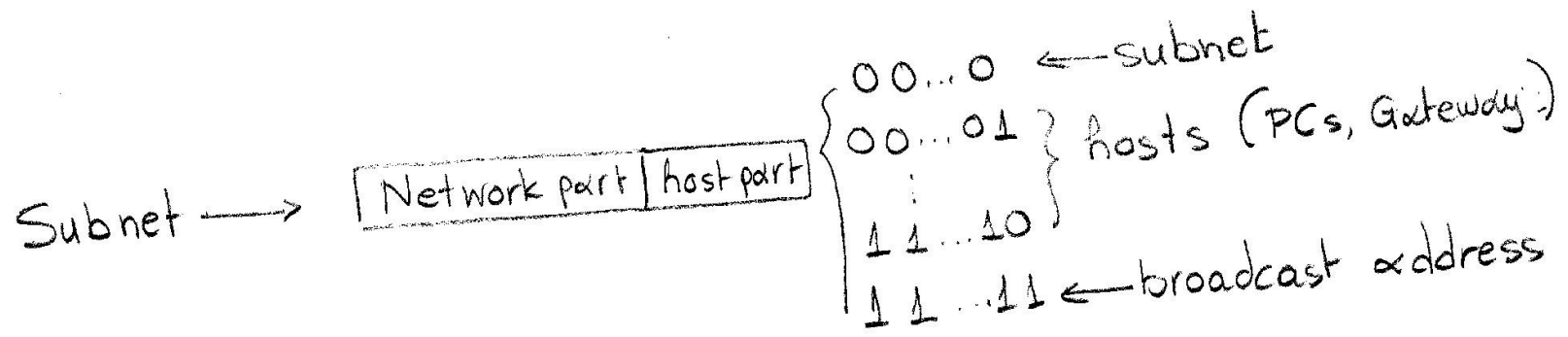
Class C networks use 21 Bits for the Network ID and 8 Bits for the Host ID. This is why Class C networks have a large number of networks but with only 256 hosts per network

IP Address
AND
 MASK

 SUBNET

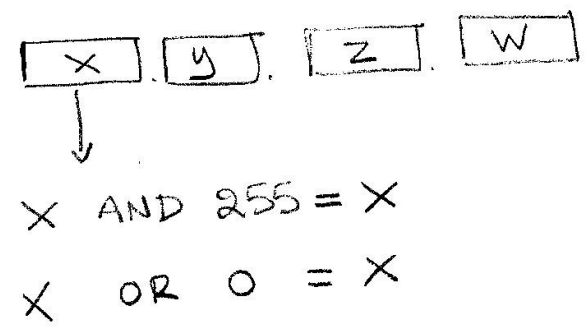
IP Address
AND
 Inverted MASK

 PC Number



IP address
OR
 Inverted Mask

 broadcast address



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 : 255.255.240.0 σε δυαδική μορφή είναι:

255.255.224.0 → 11111111.11111111.11110000.00000000

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 4.095 χρησιμοποιείται για broadcasting μνημάτων 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 11001010.00111100.11010000.00000000

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 11001010.00111100.11011111.11111111

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 άξων 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

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	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	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 octet are set) and 8 Bits for the Host ID. The Subnet mask is what splits the Network ID and Host ID. This particular subnet mask is 24 Bits long (consists of 24 one's (1) counting from left side)

The Analysis Of Our Example - Part 2

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.

Determining the Subnets

First: 000 (0 Decimal)
 Second: 001 (32 Decimal)
 Third: 010 (64 Decimal)
 Fourth: 011 (96 Decimal)
 Fifth: 100 (128 Decimal)
 Sixth: 101 (160 Decimal)
 Seventh: 110 (192 decimal)
 Eighth: 111 (224 Decimal)

Determining the Hosts per Subnet

0 0001 (1 Decimal) to 1 1110 (30 Decimal)
 0 0001 (1 Decimal) to 1 1110 (30 Decimal)
 0 0001 (1 Decimal) to 1 1110 (30 Decimal)
 0 0001 (1 Decimal) to 1 1110 (30 Decimal)
 0 0001 (1 Decimal) to 1 1110 (30 Decimal)
 0 0001 (1 Decimal) to 1 1110 (30 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

128
128 128 128 128
128 128 128 128
128 128 128 128
128 128 128 128

FIRST NETWORK

First IP: 0000 0000 (0 Decimal) Last IP: 0001 1111 (31 Decimal)

Full Range of the First Network: 192.168.0.0 - 192.168.0.31

128
128 128 128 128
128 128 128 128
128 128 128 128
128 128 128 128

SECOND NETWORK

First IP: 0010 0000 (32 Decimal) Last IP: 0011 1111 (63 Decimal)

Full Range of the Second Network: 192.168.0.32 - 192.168.0.63

128
128 128 128 128
128 128 128 128
128 128 128 128
128 128 128 128

THIRD NETWORK

First IP: 0100 0000 (64 Decimal) Last IP: 0101 1111 (95 Decimal)

Full Range of the Third Network: 192.168.0.64 - 192.168.0.95

128
128 128 128 128
128 128 128 128
128 128 128 128
128 128 128 128

FOURTH NETWORK

First IP: 0110 0000 (96 Decimal) Last IP: 0111 1111 (127 Decimal)

Full Range of the Fourth Network: 192.168.0.96 - 192.168.0.127

128
04
32
16
8
4
2
1

FIFTH NETWORK

128
04
32
16
8
4
2
1

First IP: 1000 0000 (128 Decimal) Last IP: 1001 1111 (159 Decimal)

Full Range of the Fifth Network: 192.168.0.128 - 192.168.0.159

128
04
32
16
8
4
2
1

SIXTH NETWORK

128
04
32
16
8
4
2
1

First IP: 1010 0000 (160 Decimal) Last IP: 1011 1111 (191 Decimal)

Full Range of the Sixth Network: 192.168.0.160 - 192.168.0.191

128
04
32
16
8
4
2
1

SEVENTH NETWORK

128
04
32
16
8
4
2
1

First IP: 1100 0000 (192 Decimal) Last IP: 1101 1111 (223 Decimal)

Full Range of the Seventh Network: 192.168.0.192 - 192.168.0.223

128
04
32
16
8
4
2
1

EIGHTH NETWORK

128
04
32
16
8
4
2
1

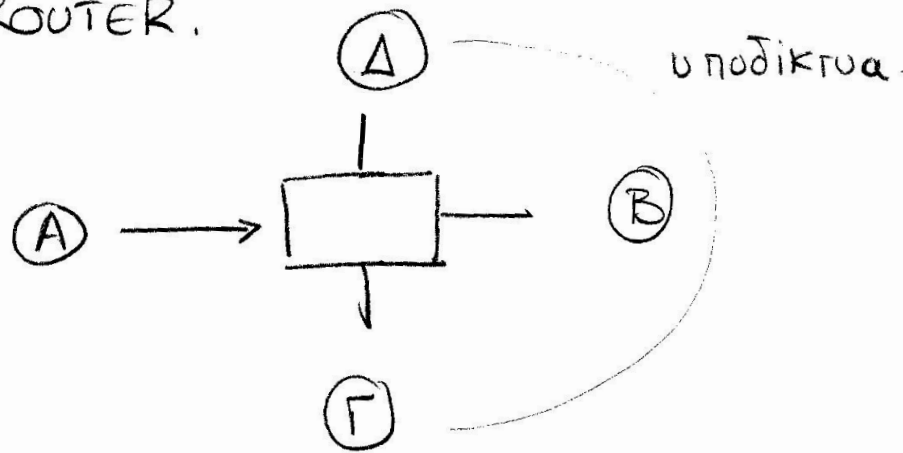
First IP: 1110 0000 (224 Decimal) Last IP: 1111 1111 (255 Decimal)

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.

- Θέματα: routers, packet routing/forwarding
- Δείτε τις παρακάτω διαφάνειες του *PLH22_OSS5_slides_2017-18.ppt* :
115,121,124

ROUTER.

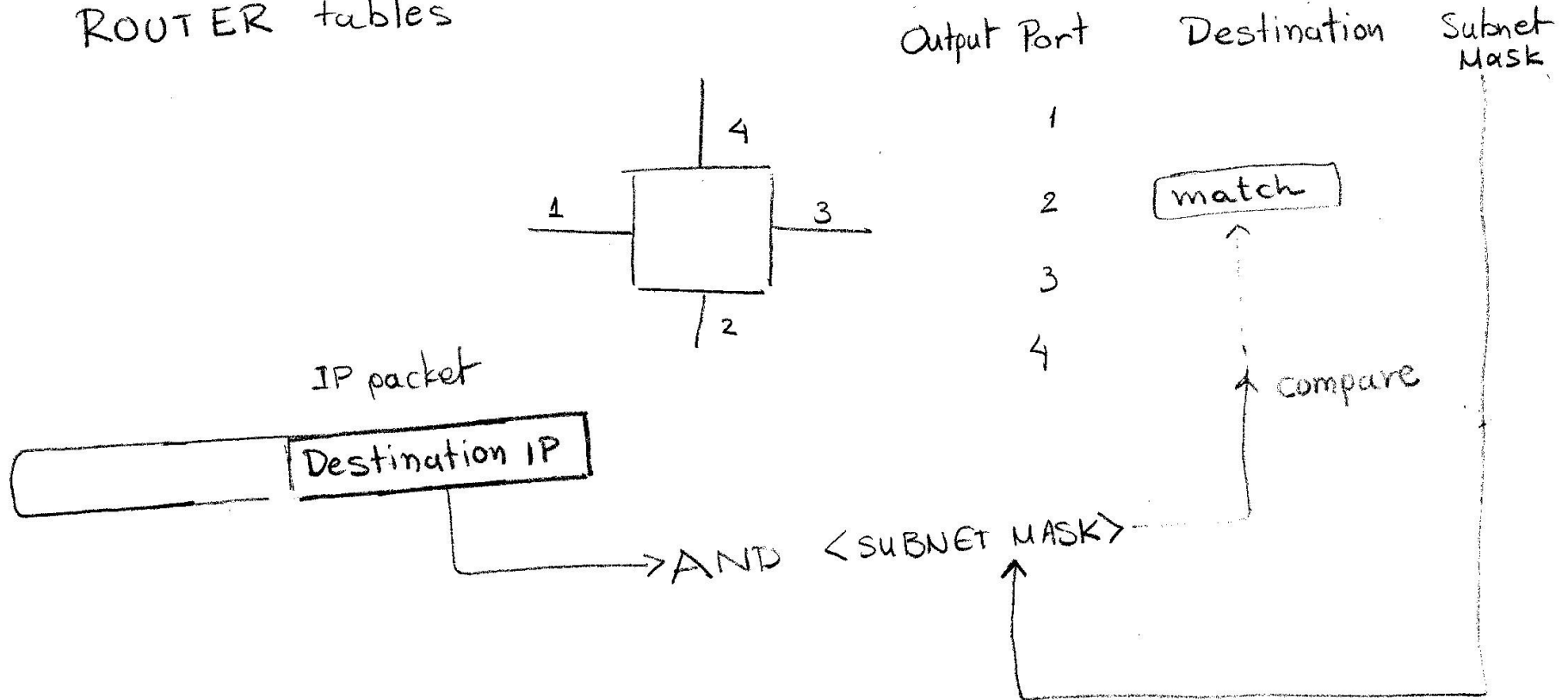


Πρωτόκολλο πακέτων με βάση την αντιστοίχιση
(Subnet) IP Address - Θύρας σε πίνακα διαδρομολόγησης
Ο πίνακας δεν έχει self learning

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

$$\frac{\text{IP Address} \quad \text{SUBNET_MASK}}{\text{DESTINATION SUBNET}} \text{ (AND)} \longrightarrow \text{router port}$$

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 απάντησή σας)

α) 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.

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 → 01011100.11010101.11000100.10101011
IP (υπολ): 92.213.193.53 → 01011100.11010101.11000001.00110101
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 → 01011100.11010101.11000010.10101011
IP (υπολ): 92.213.193.53 → 01011100.11010101.11000001.00110101
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.

2017B

ΘΕΜΑ 6

Για τις ακόλουθες IPv4 διευθύνσεις:

- i) 192.168.1.64/29
- ii) 192.168.37.190/25
- iii) 172.17.16.255/23
- iv) 10.0.8.1/22

Να αναφέρετε και να αιτιολογήσετε εν συντομία τι είδους διευθύνσεις είναι αυτές, επιλέγοντας από τις ακόλουθες: α) network, β) broadcast, γ) host.

- **Network** είναι όταν το host number είναι 00...0
- **Directed Broadcast** είναι όταν το host number είναι 11...1
- **Host** είναι όταν το host number είναι διάφορο του 00...0 και 11...1

Επομένως για τις παραπάνω διευθύνσεις ισχύουν:

- i) Η διεύθυνση 192.168.1.64/29 σε δυαδική μορφή είναι:

11000000 . 10101000 . 00000001 . 01000000

Τα 3 πρώτα bit είναι **110** άρα ανήκει στην κλάση C. Η μάσκα υποδικτύου είναι 29, δηλαδή τα 32-29=3 τελευταία bit είναι το host number, τα οποία είναι 000. **Αυτό σημαίνει ότι είναι η διεύθυνση είναι network.**

- ii) Η διεύθυνση 192.168.37.190/25 σε δυαδική μορφή είναι:

11000000 . 10101000 . 00100101 . 10111110

Η μάσκα υποδικτύου είναι 25, δηλαδή τα 32-25=7 τελευταία bit είναι το host number, τα οποία είναι 111110. **Αυτό σημαίνει ότι είναι η διεύθυνση ανήκει σε host.**

- iii) Η διεύθυνση 172.17.16.255/23 σε δυαδική μορφή είναι:

10101100 . 00010001 . 00010000 . 11111111

Η μάσκα υποδικτύου είναι 25, δηλαδή τα 32-23=9 τελευταία bit είναι το host number, τα οποία είναι **01111111**. **Αυτό σημαίνει ότι είναι η διεύθυνση ανήκει σε host.**

- iv) Η διεύθυνση 10.0.8.1/22 σε δυαδική μορφή είναι:

00001010 . 00000000 . 00001000 . 00000001

Η μάσκα υποδικτύου είναι 22, δηλαδή τα 32-22=10 τελευταία bit είναι το host number, τα οποία είναι **000000001**. **Αυτό σημαίνει ότι είναι η διεύθυνση ανήκει σε host.**

- Δίνεται η διεύθυνση δικτύου 90.0.0.0/16 (όπου 16 ο συνολικός αριθμός των bits που χρησιμοποιούνται για το δίκτυο), ζητούνται:
 - η Κλάση Διεύθυνσης, η Default Subnet Mask,
 - η Custom Subnet Mask, ο συνολικός Αριθμός subnets, ο συνολικός Αριθμός των διαθέσιμων Διευθύνσεων ανά subnet, ο αριθμός των χρησιμοποιήσιμων host Διευθύνσεων ανά subnet και ο αριθμός των bits που έχουν δανειστεί για τη δημιουργία των subnets.
- Ποιο είναι το range των διευθύνσεων του 7ου subnet? Ποιος είναι ο αριθμός υποδικτύου για το 8ο subnet; Ποια είναι η broadcast διεύθυνση για το 10ο subnet?, Ποιες είναι οι χρησιμοποιήσιμες host διευθύνσεις του 2ου subnet;

- Καθώς οι περιοχές των διευθύνσεων από 001.0.0.0 ως 127.255.255.255 ανήκει στην κλάση A, η διεύθυνση δικτύου 90.0.0.0 ανήκει στην κλάση A.
- ή επειδή η κλάση μιας IP διεύθυνσης καθορίζεται από τα πρώτα 4 bits
- 90 -> 01011010 άρα η διεύθυνση IP ανήκει είναι κλάσης A αφού το πρώτο bit είναι 0 και το δεύτερο 1.
- Η default subnet mask είναι 255.0.0.0
- Δεδομένου ότι το network τμήμα της ip διεύθυνσης προκύπτει από το λογικό AND μεταξύ ip και custom μάσκας και καθώς τα bits που είναι διαθέσιμα για το network τμήμα είναι 16 (8+8, δηλαδή όσοι οι άσοι της custom μάσκας) συμπεραίνουμε ότι τα bits που είναι διαθέσιμα για τους host στο δίκτυο αυτό είναι 16 (=32-16), όσα δηλαδή και τα δεξιότερα μηδενικά στην μάσκα υποδικτύου. Αν μετά τις πρώτη οκτάδα που χρησιμοποιείται από τα 90. ο αριθμός των bits που απομένει να χρησιμοποιηθούν από το δίκτυο είναι 8, συνεπώς ο συνολικός αριθμός των subnets είναι $2^8=256$ και ο αριθμός των bits που δανείστηκε είναι 8.
- Συνεπώς η custom mask είναι η 255.255.0.0.
- Τα υπόλοιπα 16 bits χρησιμοποιούνται από τους hosts όποτε ο συνολικός αριθμός των hosts είναι $2^{16}= 65536$
- Για λόγους πληρότητας το μέγιστο πλήθος υπολογιστών που μπορούμε να έχουμε με 16 bits είναι:
- $2^{16} - 2 = 65534$
- Οι δύο διευθύνσεις που δεν συμπεριλαμβάνονται είναι αυτές που έχουν στο host τμήμα όλα μηδενικά (αντιστοιχούν στο δίκτυο) και όλα 1 (αντιστοιχούν στην broadcast address).

- Το range των διευθύνσεων του 7ου υποδικτύου είναι
- 90.6.0.0 – 90.6.255.255
- Ο αριθμός υποδικτύου για το 8ο υποδίκτυο είναι
- 90.7.0.0
- Η broadcast διεύθυνση για το 10ο subnet είναι
- 90.9.255.255
- Οι χρησιμοποιούμενες host διευθύνσεις του 2ου Υποδικτύου;
- 90.1.0.1 – 90.1.255.254