

**Απαντήσεις πανελληνίων θεμάτων Δικτύων
(Μάθημα ειδικότητας ΕΠΑΛ – ομάδα Β)**

ΘΕΜΑ Α

A1.

α. Σ

β. Λ

γ. Λ

δ. Σ

A2 - γ.

A3.

1 - γ

2 - ε

3 - β

4 - α

ΘΕΜΑ Β

B1.

Η διεπαφή βασικού ρυθμού BRI παρέχει δύο κανάλια φορείς (2 κανάλια - B) κι ένα κανάλι σηματοδότησης (1 κανάλι - D). Κάθε κανάλι -B έχει ρυθμό μετάδοσης 64kbrs και χρησιμοποιεί για τη μεταφορά ψηφιοποιημένης φωνής και δεδομένων. Το κανάλι - D έχει ρυθμό μετάδοσης 16 kbrs και χρησιμοποιείται για την εγκαθίδρυση και διαχείριση της σύνδεσης. Οι τηλεπικοινωνιακοί φορείς δίνουν τη δυνατότητα στους χρήστες - πελάτες τους να χρησιμοποιούν το ένα ή και τα δύο κανάλια - B, πράγμα που σημαίνει, ότι η σύνδεση βασικού ρυθμού μπορεί να παρέχει ρυθμό μετάδοσης μέχρι 144 kbrs (2B + D).

B2.

Τα κριτήρια, με βάση τα οποία οι αλγόριθμοι δρομολόγησης λαμβάνουν τις αποφάσεις τους, είναι τα ακόλουθα:

- Συντομότερη διαδρομή, η οποία καθορίζεται με βάση:
 - ✓ Είτε τον αριθμό τμημάτων (γραμμών), που την αποτελούν
 - ✓ Είτε την μέση καθυστέρηση (ουράς και μετάδοσης), που εισάγει
 - ✓ Είτε τη χρησιμοποίηση του εύρους ζώνης
- Αριθμός πακέτων, που περιμένουν προς μετάδοση στην ουρά εξόδου
- Κόστος γραμμής. Το κόστος γραμμής είναι συνάρτηση, στην οποία έχουν συμμετέχουν με διαφορετική βαρύτητα οι ακόλουθοι παράγοντες:
 - ✓ Μέση καθυστέρηση
 - ✓ Μέσο μήκος
 - ✓ Χρήση εύρους ζώνης

B3.

1. Διαχείριση παραμέτρων του δικτύου (configuration management)
2. Διαχείριση επίδοσης του δικτύου (Performance management)
3. Διαχείριση σφαλμάτων (Fault management)
4. Διαχείριση του κόστους των υπηρεσιών (Accounting management)
5. Διαχείριση ασφάλειας (Security management)

ΘΕΜΑ Γ

Γ1.

Κόμβος Εισόδου	VC Εισόδου	Κόμβος Εξόδου	VC Εξόδου
Γ	5	Δ	1
Α	3	Β	2
Ε	3	Ζ	3

Γ2.

Η διεύθυνση υποδικτύου είναι:

11010000.01011001.10100111.00000000

Η διεύθυνση προέκυψε από το αποτέλεσμα της πράξης **AND** η οποία πραγματοποιήθηκε **μεταξύ** της IP διεύθυνσης και της μάσκας υποδικτύου.

ΘΕΜΑ Δ

Δ1.

α.

Το συγκεκριμένο κομμάτι δηλώνει ότι είναι το τελευταίο κομμάτι του πακέτου αφού το DF=0.

Ενώ τα υπόλοιπα (εκτός από το τελευταίο) τμήματα έχουν DF=1.

β.

Αποτελείται από 20 bytes **διότι** γνωρίζουμε ότι τα 20 bytes αντιστοιχούν σε 5 λέξεις των 32 bits.

γ.

Γνωρίζουμε επίσης ότι το πεδίο δείκτης εντοπισμού τμήματος για το πρώτο κομμάτι παίρνει πάντα την τιμή 0, για το δεύτερο υπολογίζεται ως εξής:

$600\text{bytes}/8=75$, δηλαδή διαιρούμε τα καθαρά δεδομένα με το 8.

Συνεπώς ο δείκτης εντοπισμού τμήματος για το πρώτο κομμάτι είναι 0 και για το δεύτερο 75.

Δ2.

α.

Εφόσον οι χρήστες που θέλουν να επικοινωνήσουν έχουν συμφωνήσει στη χρήση του αλγόριθμου (αλγόριθμο θα χρησιμοποιήσουν, στην προκειμένη περίπτωση τον MD5) και επίσης έχουν δημιουργήσει τα αντίστοιχα κλειδιά σύμφωνα με την εκφώνηση, η διαδικασία έχει ως εξής:

Θα πρέπει ο A να βάλει ως είσοδο στον αλγόριθμο κατατεμαχισμού το έγγραφο και να παράγει το message digest. Στη συνέχεια θα πρέπει να κρυπτογραφήσει το message digest με το ιδιωτικό του κλειδί. Το αποτέλεσμα της κρυπτογράφησης του message digest είναι η ψηφιακή υπογραφή του A για το συγκεκριμένο έγγραφο και τίθεται στο τέλος του αρχικού εγγράφου. Στη συνέχεια, ο A θα αποστείλει το αρχικό μήνυμα μαζί με τη ψηφιακή υπογραφή στον B.

β.

Με τη σειρά του ο Β θα πάρει το κρυπτογραφημένο μέρος και θα το αποκρυπτογραφήσει με το δημόσιο κλειδί του Α.

Το αποτέλεσμα της αποκρυπτογράφησης είναι το message digest του εγγράφου.

Στη συνέχεια, ο Β θα πάρει το αρχικό έγγραφο και θα το περάσει από τον αλγόριθμο κατατεμαχισμού και θα παράγει message digest, το οποίο θα συγκρίνει, εάν είναι το ίδιο με το message digest που προέκυψε από την αποκρυπτογράφηση. Εάν τα δύο message digest είναι ίδια, ο Β μπορεί να είναι σίγουρος, ότι το μήνυμα έχει σταλεί από τον Α αφού μπόρεσε να κάνει αποκρυπτογράφηση με το δημόσιο κλειδί του Α και ότι το έγγραφο δεν έχει υποστεί αλλαγές από τρίτους κατά την αποστολή, αφού τα δύο message digest είναι τα ίδια.

ΑΚΑΔΗΜΑΪΚΟ
ΦΡΟΝΤΙΣΤΗΡΙΟ
ΑΘΗΝΑ