

ΔΙΚΤΥΑ Η/Υ ΙΙ – ΘΕΜΑΤΑ 2013

ΘΕΜΑ Α.

A1. Να χαρακτηρίσετε τις προτάσεις που ακολουθούν, γράφοντας στο τετράδιό σας, δίπλα στο γράμμα που αντιστοιχεί σε κάθε πρόταση τη λέξη Σωστό, αν η πρόταση είναι σωστή ή τη λέξη Λάθος, αν η πρόταση είναι λανθασμένη.

α. Ένα από τα μειονεκτήματα που χαρακτηρίζει το δημόσιο τηλεφωνικό δίκτυο μεταγωγής (PSTN) είναι η μεταβλητή ποιότητα και αξιοπιστία.

β. Το πρωτόκολλο RARP μετατρέπει τις IP διευθύνσεις στις αντίστοιχες φυσικές διευθύνσεις.

γ. Η ακεραιότητα (Integrity) αφορά στην απόδειξη ταυτότητας του χρήστη για παροχή πρόσβασης στα αγαθά του συστήματος.

δ. Το πρωτόκολλο TCP είναι υπεύθυνο για την εγκατάσταση αξιόπιστων ταυτόχρονων δι-κατευθυντήριων συνδέσεων.

Μονάδες 12

α. ΣΩΣΤΟ, β. ΛΑΘΟΣ, γ. ΛΑΘΟΣ, δ. ΣΩΣΤΟ

A2. Να μεταφέρετε στο τετράδιό σας το γράμμα της σωστής απάντησης. Το μήκος της IP διεύθυνσης στην τεχνολογία TCP/IP είναι:

α. 48 bits β. 48 bytes γ. 32 bits δ. 32 bytes

Μονάδες 5

Σωστή Απάντηση: (γ)

A3. Να γράψετε στο τετράδιό σας τους αριθμούς 1, 2, 3, 4 από τη στήλη Α και δίπλα ένα από τα γράμματα α, β, γ, δ, ε της στήλης Β που δίνει τη σωστή αντιστοίχιση.

Μονάδες 8

ΣΤΗΛΗ Α	ΣΤΗΛΗ Β
1. DNS	α. Δεν τεμαχίζει τα δεδομένα σε πολλαπλά τμήματα
2. Ασυμμετρική κρυπτογράφηση	β. TCP port 23
3. Telnet	γ. Μηχανισμός απεικόνισης των διευθύνσεων σε ονόματα και το αντίστροφο
4. UDP	δ. Πρωτόκολλο Μεταφοράς Αρχείων (FTP)
	ε. Βασίζεται στη χρήση δύο κλειδιών

1-γ, 2-ε, 3-β, 4-α

ΘΕΜΑ Β.

B1. Να περιγράψετε και να αναλύσετε τη διεπαφή βασικού ρυθμού (Basic Rate Interface - BRI) του ISDN. (Δεν χρειάζεται σχήμα)

Μονάδες 10

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

B2. Να περιγράψετε τα τρία (3) κριτήρια, με βάση τα οποία οι αλγόριθμοι δρομολόγησης λαμβάνουν τις αποφάσεις τους.

Μονάδες 10

- 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 συμμετέχουν με διαφορετική βαρύτητα οι ακόλουθοι παράγοντες: μέση καθυστέρηση, μέσο μήκος ουράς, χρήση εύρους ζώνης.

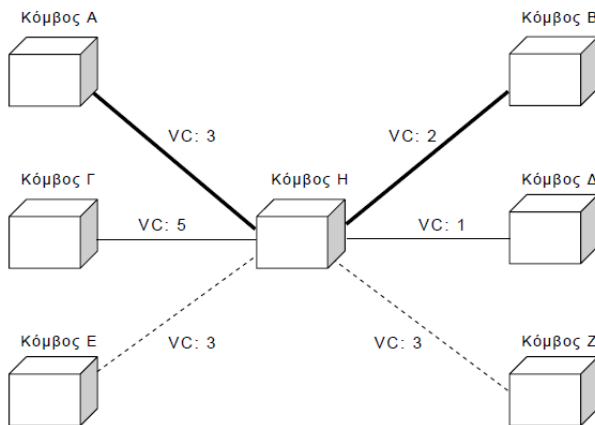
B3. Να αναφέρετε ονομαστικά τις πέντε (5) περιοχές διαχείρισης δικτύου που έχει ορίσει ο Διεθνής Οργανισμός Προτυποποίησης ISO για το μοντέλο διαχείρισης δικτύων, OSI.

Μονάδες 5

Διαχείριση παραμέτρων (configuration management), η διαχείριση επίδοσης (performance management), διαχείριση σφαλμάτων (fault management), η διαχείριση του κόστους των υπηρεσιών (accounting management) και διαχείριση ασφάλειας (security management).

ΘΕΜΑ Γ.

Γ1. Ένα δίκτυο περιλαμβάνει τους κόμβους Α,Β,Γ,Δ,Ε,Ζ,Η όπως φαίνεται στο παρακάτω σχήμα. Ο κόμβος Η συνδέεται με τους υπόλοιπους κόμβους με τρία (3) νοητά κυκλώματα (Virtual Circuits - VC). Το πρώτο νοητό κύκλωμα συμβολίζεται στο σχήμα με τη λεπτή συνεχόμενη γραμμή (—), το δεύτερο με την έντονη συνεχόμενη γραμμή (——) και το τρίτο με τη διακεκομμένη γραμμή (-----). Να μεταφέρετε στο τετράδιό σας και να συμπληρώσετε τον παρακάτω πίνακα νοητών κυκλωμάτων του κόμβου Η.



Κόμβος Εισόδου	VC Εισόδου	Κόμβος Εξόδου	VC Εξόδου
Γ			
Α			
Ε			

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

Πίνακας νοητών κυκλωμάτων κόμβου Η

Μονάδες 9

Γ2. Να μεταφέρετε στο τετράδιό σας τον παρακάτω πίνακα και να τον συμπληρώσετε με τις κλάσεις IP διευθύνσεων.

IP Διεύθυνση	11010000.01011001.10100111.11110000
Μάσκα υποδικτύου	11111111.11111111.11111111.00000000

α) Να βρείτε τη διεύθυνση υποδικτύου.

Μονάδες 16

11010000.01011001.10100111.00000000

ΘΕΜΑ Δ.

Δ1. Ένα IP αυτοδύναμο πακέτο μεταδίδεται μέσω ενός φυσικού δικτύου, που υποστηρίζει πακέτα συνολικού μήκους 620 bytes. Το πακέτο διασπάται σε πέντε (5) κομμάτια (fragments) και ένα από τα κομμάτια αυτά έχει στην επικεφαλίδα του τις εξής τιμές:

MF = 0, Μήκος Επικεφαλίδας = 5

Να απαντήσετε στα παρακάτω ερωτήματα:

α. Τι δηλώνει για το συγκεκριμένο κομμάτι η τιμή MF = 0;

Μονάδες 3

Ότι είναι το τελευταίο από τα κομμάτια στα οποία διασπάστηκε το πακέτο.

β. Από πόσα bytes αποτελείται η επικεφαλίδα του παραπάνω κομματιού; Να δικαιολογήσετε την απάντησή σας.

Μονάδες 4

20 byte. Είναι 5 λέξεις των 32 bit, δηλ. 160 bit, 160 bit / 8 = 20 byte.

γ. Ποιος είναι ο Δείκτης Εντοπισμού Τμήματος του πρώτου και του δεύτερου κομματιού; Να δικαιολογήσετε την απάντησή σας.

Μονάδες 4

600 / 8 = 75. Άρα οι Δείκτες Εντοπισμού Τμήματος των κομματιών είναι: 0, 75, 150, 225, 300. Του 2^{ου} κομματιού είναι το 75.

Δ2. Δύο χρήστες Α και Β επικοινωνούν μέσω ενός δικτύου υπολογιστών. Έστω ότι ο χρήστης Α θέλει να στείλει ένα κείμενο, στο οποίο να συμπεριλαμβάνεται η ψηφιακή του υπογραφή, στο χρήστη Β. Οι χρήστες Α και Β έχουν συμφωνήσει στη χρήση του αλγορίθμου κατατεμαχισμού MD5, έχουν δημιουργήσει ζευγάρια δημόσιου/ιδιωτικού κλειδιού και έχουν ανταλλάξει τα δημόσια κλειδιά τους.

α. Να περιγράψετε τις ενέργειες του χρήστη Α, προκειμένου να στείλει το μήνυμα με την ψηφιακή υπογραφή του στο χρήστη Β.

Θα πρέπει ο Α ναβάλει 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 Α για το συγκεκριμένο έγγραφο και τίθεται στο τέλος του αρχικού εγγράφου. Στη συνέχεια, ο Α θα αποστείλει το αρχικό μήνυμα μαζί με τη ψηφιακή υπογραφή στον Β.

β. Να περιγράψετε τις ενέργειες του χρήστη B, προκειμένου να είναι σίγουρος για την ταυτότητα του χρήστη A.
Μονάδες 14

Ο B θα πάρει το κρυπτογραφημένο μέρος και θα το αποκρυπτογραφήσει με το δημόσιο κλειδί του A. Το αποτέλεσμα της αποκρυπτογράφησης είναι το *message digest* του εγγράφου. Στη συνέχεια, ο B 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 B μπορεί να είναι σίγουρος, ότι το μήνυμα έχει σταλεί από τον A αφού μπόρεσε να κάνει αποκρυπτογράφηση με το δημόσιο κλειδί του A και ότι το έγγραφο δεν έχει υποστεί αλλαγές από τρίτους κατά την αποστολή, αφού τα δύο *message digest* είναι τα ίδια.