# Εργαστήριο Δικτύων - Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

**1η Εργασία για το μάθημα Εργαστήριο Δικτύων**
**Υποχρεωτική υποβολή για την συμμετοχή στην εξέταση.**

## Α. Μέρος – Το πρωτόκολλο DNS

Στην παρούσα εργασία θα μελετηθεί το DNS σύστημα χρησιμοποιώντας τις εντολές nslookup και ifconfig/ipconfig (Linux/Windows) αντίστοιχα. Για να εξοικειωθείτε με τις εντολές εκτελέστε τις παρακάτω και αναφέρατε τα αποτελέσματα:

1. nslookup www.ceid.upatras.gr
2. ifconfig (Linux)
3. ipconfig \all (windows)
4. ipconfig /displaydns
5. ipconfig /flushdns

Εκκινήστε το Wireshark. Καταγράψτε και δείξτε τα πακέτα DNS που στέλνονται από τον υπολογιστή σας εκτελώντας πριν την καταγραφή πρώτα τα παρακάτω :

- ipconfig για να σβήσετε το DNS cache.
- Εκκαθάριση του cache του browser
- δήλωση “ip.addr == your_IP_address” στο φίλτρο του Wireshark

Εκκινήστε την καταγραφή στο Wireshark και πραγματοποιείστε τα παρακάτω:

- επισκεφτείτε την σελίδα http://www.ietf.org
- σταματήσει την καταγραφή στο Wireshark.

**Απαντήστε στα παρακάτω ερωτήματα και δώστε screenshots από τα πακέτα.**

1. Βρείτε και αναφέρατε τα DNS μηνύματα που ανταλλάχθηκαν.
2. Αναλύστε ολόκληρο το πακέτο, εξηγείται κάθε πεδίο του μηνύματος καθώς και το είδος του πρωτοκόλλου (TCP/UDP) που χρησιμοποιήθηκε.
3. Ποια είναι η θύρα προορισμού για το μήνυμα ερώτησης DNS;
4. Ποια είναι η θύρα προέλευσης του μηνύματος απόκρισης DNS;
5. Σε ποια διεύθυνση IP εμφανίζεται το μήνυμα ερώτησης DNS; Χρησιμοποιήστε το ipconfig για να καθορίσετε την Διεύθυνση IP του τοπικού σας διακομιστή DNS. Αυτές οι δύο διευθύνσεις IP είναι ίδιες;
6. Εξετάστε το μήνυμα ερώτησης DNS. Τι “τύπος" ερωτήματος DNS είναι; Περιέχει το ερώτημα οποιεσδήποτε "απαντήσεις"?
7. Εξετάστε το μήνυμα απόκρισης DNS. Πόσες "απαντήσεις" παρέχονται; Τι περιέχει η κάθε απάντηση?
8. Εξετάστε το επόμενο πακέτο TCP SYN που στέλνει ο υπολογιστής σας. Η διεύθυνση IP του πακέτου SYN αντιστοιχεί σε οποιαδήποτε από τις διευθύνσεις IP που παρέχονται στο το μήνυμα απάντησης DNS;

Εκκινήστε ξανά την καταγραφή στο Wireshark. Εκτελέστε την εντολή **nslookup www.ceid.upatras.gr.** Σταματήστε την καταγραφή στο Wireshark. Εφόσον βρείτε παραπάνω από ένα DNS queries αγνοήστε τα και δείτε μόνο το τελευταίο (3ο).

**Απαντήστε στα παρακάτω ερωτήματα και δώστε screenshots από τα πακέτα:**

9. Ποια είναι η θύρα προορισμού για το μήνυμα ερώτησης DNS; Ποια είναι η θύρα προέλευσης του μηνύματος απόκρισης DNS; Δώστε screenshot.από το πακέτο.
10. Σε ποια διεύθυνση IP εμφανίζεται το μήνυμα ερώτησης DNS; Είναι αυτή η διεύθυνση IP του προεπιλεγμένου τοπικού διακομιστή DNS;
11. Εξετάστε το μήνυμα ερώτησης DNS. Τι "Τύπος" ερωτήματος DNS είναι; Περιέχει οποιεσδήποτε "απαντήσεις";
12. Εξετάστε το μήνυμα απόκρισης DNS. Πόσες "απαντήσεις" παρέχονται; Τι περιέχει η κάθε απάντηση?

**Απαντήστε στα παρακάτω γενικά ερωτήματα για τον τρόπο λειτουργίας του DNS**

13. Ποιες οι διαφορές μεταξύ των Recursive resolvers, root nameservers, TLD nameservers, and authoritative nameservers.
14. Ποια τα πεδία του header ενος DNS πακέτου? Εξηγείστε το καθένα.
15. Αναλύστε κάθε πεδίο του παρακάτω DNS πακέτου. Τι είδους DNS πακέτο είναι? Για ποιο domain ζητάει την IP?

```
48 F8 B3 26 DF 49 BA BA BA BA BA BA 08 00 45 00 00 38 66 BD 00 00 80 11
02 0C C0 A8 01 34 08 08 08 08 D5 39 00 35 00 24 44 8F 00 03 01 00 00 01 00 00
00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 01 00 01
```

**16.** Ομοίως αναλύστε κάθε πεδίο του παρακάτω DNS πακέτου: Τι είδους DNS πακέτο είναι?

BA BA BA BA BA BA 48 F8 B3 26 DF 49 08 00 45 08 00 E8 B2 EF 00 00 37 11
FE 21 08 08 08 08 C0 A8 01 34 00 35 D5 39 00 D4 28 A2 00 03 81 80 00 01 00 0B
00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 01 00 01 C0 0C 00 01 00 01
00 00 00 04 00 04 4A 7D EC 23 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC
25 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 27 C0 0C 00 01 00 01 00 00 00
04 00 04 4A 7D EC 20 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 28 C0 0C
00 01 00 01 00 00 00 04 00 04 4A 7D EC 21 C0 0C 00 01 00 01 00 00 00 04 00 04
4A 7D EC 29 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 22 C0 0C 00 01 00
01 00 00 00 04 00 04 4A 7D EC 24 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D
EC 2E C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 26

**Περαιτέρω μελέτη (προαιρετική):**

Σε λειτουργικό Linux εγκαταστήστε κάποιο εκ των BIND9 ή Dnsmasq. Τα λογισμικά είναι ανοικτού κώδικα και υλοποιούν DNS server. Ορίστε τους servers ως authoritative και εγκαταστήστε μηχανισμό καταγραφής (logging).
Εκκινήστε ποικίλες εφαρμογές στον υπολογιστή σας (skype, browser, κλπ) και παρατηρείστε το πλήθος των queries που γίνονται.
**Ερώτηση:** Καταγράφετε η IP διεύθυνση, ο χρόνος και τα προσωπικά στοιχεία του υπολογιστή σας? Δώστε ένα δείγμα του log αρχείου.

**Υπόδειξη Λειτουργίας Wireshark**. Για την λειτουργία του Wireshark και την καταγραφή πακέτων, θα χρησιμοποιήσετε τη λειτουργία Capture με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Για να κάνετε μια καταγραφή με φίλτρο, από το μενού Capture->Interfaces... πιέστε το κουμπί Options. Στο παράθυρο που θα εμφανισθεί επιλέξτε την κάρτα δικτύου του υπολογιστή σας στην οποία θέλετε να κάνετε την καταγραφή. Με διπλό κλικ στο όνομα της κάρτας θα εμφανισθεί το μενού για το φίλτρο σύλληψης.

Στο πεδίο δίπλα από το κουμπί “Capture Filter” πληκτρολογήστε μια λογική έκφραση σύμφωνη με τη σύνταξη των φίλτρων καταγραφής. Πιέζοντας το Start θα αρχίσει η καταγραφή. Όπως αναφέρθηκε και σε προηγούμενη εργαστηριακή άσκηση, υπάρχουν έτοιμοι κανόνες χρωματισμού από την εγκατάσταση του Wireshark, τους οποίους μπορείτε να κρατήσετε ή να αλλάξετε από τη θέση View→Coloring rules.... Τα πλαίσια που καταγράφονται θα εμφανιστούν έγχρωμα στο παράθυρο με τη λίστα καταγεγραμμένων πακέτων του Wireshark. Κάθε γραμμή αντιστοιχεί σε ένα πλαίσιο που συλλαμβάνεται. Μπορείτε να επιλέξτε ένα οποιοδήποτε από τα πλαίσια που καταγράφηκαν κάνοντας κλικ στην αντίστοιχη γραμμή του παραθύρου.

Τα βασικά πεδία της επικεφαλίδας κάθε πρωτοκόλλου, που περιέχεται στο πλαίσιο που επιλέξατε, εμφανίζονται με γραφικό τρόπο στο παράθυρο με τις λεπτομέρειες επικεφαλίδας στο μεσαίο τμήμα της οθόνης. Στο παράθυρο με τα περιεχόμενα (κάτω τμήμα της οθόνης) εμφανίζονται τα δεδομένα του επιλεγμένου πλαισίου σε δεκαεξαδική και ASCII μορφή. Μπορείτε να δείτε όλο το περιεχόμενο μιας επικεφαλίδας με διπλό κλικ ή κάνοντας κλικ επάνω της και πιέζοντας το πλήκτρο ‘+’ ή με κλικ στο σύμβολο στα αριστερά της. Όταν κάνετε κλικ πάνω σε κάποια επικεφαλίδα ή σε κάποιο πεδίο μιας επικεφαλίδας (στο παράθυρο με τις λεπτομέρειες επικεφαλίδας), τότε εμφανίζεται με αντιστροφή χρώματος (highlighted) το αντίστοιχο κομμάτι του πλαισίου στο παράθυρο με τα περιεχόμενα του πλαισίου. Τέλος, το μέγεθος και των τριών παραθύρων (καταγεγραμμένα πλαίσια, λεπτομέρειες επικεφαλίδας, περιεχόμενα πλαισίου) μπορεί να μεταβληθεί επιλέγοντας και σύροντας τις οριζόντιες μπάρες που τα διαχωρίζουν.

## Β μέρος - Το πρωτόκολλο IP

**1) Ανάλυση πλαισίου.** Δίνεται το παρακάτω frame δεδομένων.

00 A0 92 48 72 45 00 00 0C 05 C3 58 08 00 4 5 00 00 29 DB FB 40 00 FE 06 7D CB 81 6E 1E 1A 81 6E 02 11 02
03 00 50 6A 86 7B 57 B6 B6 B0 20 50 10 24 00 17 c4 00 00 02 54 41 4D 49 4C D7 87 6C A4

Κάντε πλήρη ανάλυση όλων των hex πεδίων και επιπλέον απαντήστε στα παρακάτω ερωτήματα:

1. Ποια η IP διεύθυνση προορισμού και αποστολής?
2. Ποιο το μήκος του IP μέρους?
3. Είναι το frame μέρους ενός μεγαλύτερου πακέτου?
4. Ποια η TCP θύρα αποστολέα και δέκτη.
5. Ποια η τιμή του header checksum? Υπολογίστε εάν η τιμή στο frame είναι η σωστή.

Δείξτε αναλυτικά πως εντοπίσατε τα πεδία.

**2) Πείραμα IP με χρήση Wireshark,**

**a) Χρόνος ζωής (TTL) των πακέτων IP**

Η διαδρομή που ακολουθεί ένα πακέτο IP μπορεί να ανιχνευθεί με την εντολή tracert σε Windows περιβάλλον (ή traceroute σε Linux). Η tracert στέλνει μηνύματα ICMP τύπου Echo Request με μεταβαλλόμενες τιμές του πεδίου Time-To-Live (TTL), του πακέτου IP, προς τον προορισμό. Κάθε δρομολογητής κατά μήκος της διαδρομής προς τον προορισμό μειώνει το TTL κατά 1, προτού προωθήσει το πακέτο. Όταν το TTL μηδενισθεί, ο δρομολογητής οφείλει να στείλει μήνυμα ICMP τύπου Time Exceeded στην πηγή. Η διαδρομή βρίσκεται εξετάζοντας τα μηνύματα Time Exceeded που προκαλούνται από διαδοχικά μηνύματα ηχούς με συνεχώς αυξανόμενες τιμές του TTL και καταγράφοντας την εκάστοτε διεύθυνση IP της πηγής που παράγει το μήνυμα ICMP τύπου Time Exceeded.

Ανοίξτε το Wireskark και δημιουργήστε ένα φίλτρο σύλληψης, ώστε να καταγράφονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας και απαντήστε στις παρακάτω ερωτήσεις.

1. Καταγράψτε τα διερχόμενα πλαίσια όταν εκτελείτε την εντολή tracert -d 83.212.8.210. Ποια είναι η σημασία της παραμέτρου -d που χρησιμοποιήσατε κατά την κλήση της tracert;
2. Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας.

Εφαρμόστε τώρα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

3. Ποια σύνταξη του φίλτρου απεικόνισης χρησιμοποιήσατε?

Επιλέξτε ένα μήνυμα ICMP τύπου Echo Request και στο αντίστοιχο παράθυρο παρατηρείστε τις λεπτομέρειες της επικεφαλίδας που σχετίζονται με το πρωτόκολλο IP καθώς και τα σχετικά με αυτές περιεχόμενα του πακέτου IP. Απαντήστε στις παρακάτω ερωτήσεις.

4. Ποια είναι η διεύθυνση IP του υπολογιστή σας; Σε ποιο πεδίο της επικεφαλίδας IP εμφανίζεται αυτή;
5. Καταγράψτε την τιμή του πεδίου Protocol της επικεφαλίδας IP του μηνύματος ICMP Echo request.
6. Πόσα byte έχει η επικεφαλίδα IP;
7. Πόσα byte μεταφέρει το πακέτο IP στο πεδίο δεδομένων;
8. Εξηγείστε πώς προσδιορίζεται το παραπάνω μήκος του πεδίου δεδομένων από τα στοιχεία που περιέχει η επικεφαλίδα.

Στη συνέχεια ταξινομείστε κατά φθίνουσα σειρά τα πακέτα IP σύμφωνα με τη διεύθυνση IP της πηγής τους (Source) κάνοντας κλικ στην αντίστοιχη επικεφαλίδα του παράθυρου με τη λίστα καταγεγραμμένων πακέτων. Εάν το μικρό βέλος δείχνει προς τα πάνω (αύξουσα σειρά), κάντε πάλι κλικ στην επικεφαλίδα ώστε να δείχνει προς το κάτω (φθίνουσα σειρά). Στη λίστα καταγεγραμμένων πακέτων θα πρέπει να εμφανίζονται τώρα με τη σειρά όλα τα μηνύματα ICMP που έστειλε ο υπολογιστής σας. Επιλέξτε το πρώτο μήνυμα ICMP τύπου Echo Request που έστειλε ο υπολογιστής σας. Με κλικ στο σύμβολο στα αριστερά της επικεφαλίδας Internet Protocol (στο παράθυρο με τις λεπτομέρειες επικεφαλίδας του επιλεγμένου πακέτου) αναπτύξετε τα περιεχόμενά της. Χρησιμοποιώντας το πλήκτρο ↓ (κάτω βέλος) μετακινηθείτε από το πρώτο στο τελευταίο μήνυμα της σειράς μηνυμάτων ICMP που έστειλε ο υπολογιστής σας.

9. Ποια πεδία της επικεφαλίδας IP αλλάζουν πάντα από το ένα πακέτο στο επόμενο (της σειράς μηνυμάτων ICMP που έστειλε ο υπολογιστής σας);
10. Ποια πεδία της επικεφαλίδας IP παραμένουν αμετάβλητα;
11. Ποια πεδία της επικεφαλίδας IP πρέπει να παραμείνουν αμετάβλητα και γιατί;
12. Ποια πεδία της επικεφαλίδας IP πρέπει να αλλάξουν και γιατί;

Στη συνέχεια με τα μηνύματα ταξινομημένα όπως πριν, βρείτε τη σειρά μηνυμάτων ICMP τύπου Time Exceeded που στέλνονται από τον κοντινότερο προς τον υπολογιστή σας δρομολογητή. Απαντήστε στις παρακάτω ερωτήσεις:

13. Ποια είναι η διεύθυνση IP του κοντινότερου προς τον υπολογιστή σας δρομολογητή;
14. Ποια είναι η τιμή του πεδίου TTL της επικεφαλίδας IP του πρώτου πακέτου της σειράς;
15. Παραμένουν οι τιμές του πεδίου αυτού σταθερές για όλα τα πακέτα της σειράς; Γιατί;

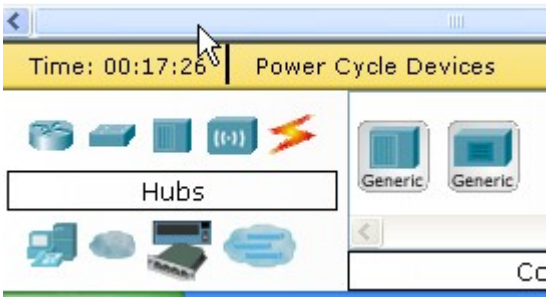
# Εργαστήριο Δικτύων - Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

## Γ μέρος - Cisco Packet Tracer -Υλοποίηση Hub

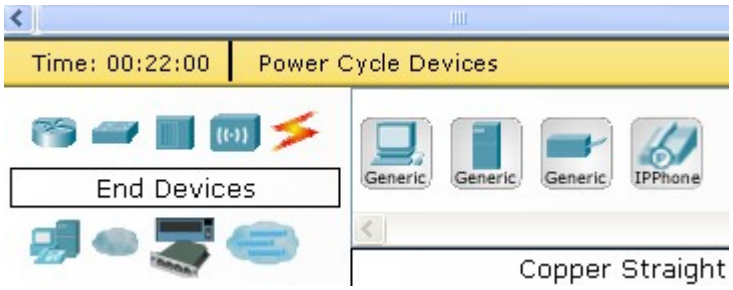
Για την εργασία αυτή, θα χρησιμοποιηθεί ο προσσομοιωτής Cisco Packet Tracer, τον οποίο μπορείτε να κατεβάστε από την ιστοσελίδα της CISCO (https://www.netacad.com/) ή και από εδώ

Τρέξτε την εφαρμογή Cisco Packet Tracer.

1. Επιλέξτε ένα Hub (Generic) όπως φαίνεται στην παρακάτω εικόνα και τοποθετήστε το στην επιφάνεια εργασίας του εξομοιωτή

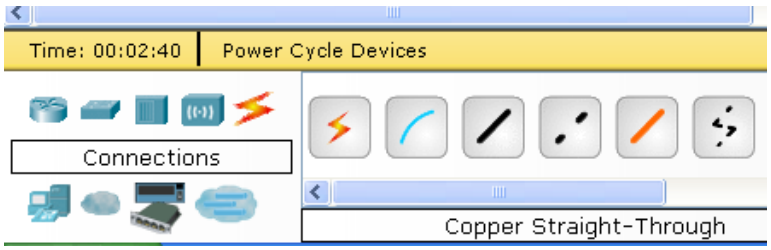



2. Τώρα επιλέξτε και τοποθετήστε τέσσερα Host (PCs) από την κατηγορία End Devices (Τερματικές συσκευές) όπως φαίνεται στην παρακάτω εικόνα.

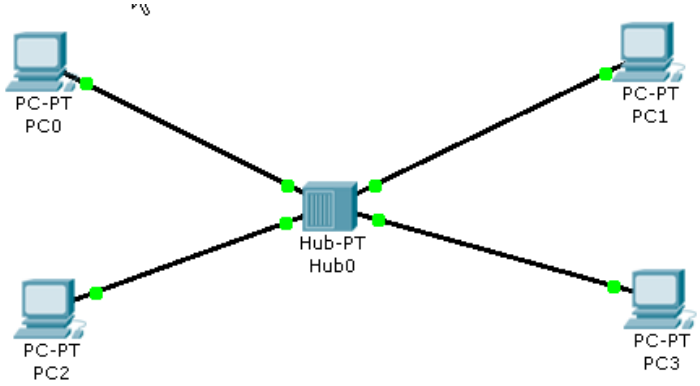



3. Η επιφάνεια του εξομοιωτή δικτύου θα είναι όπως στην παρακάτω εικόνα.

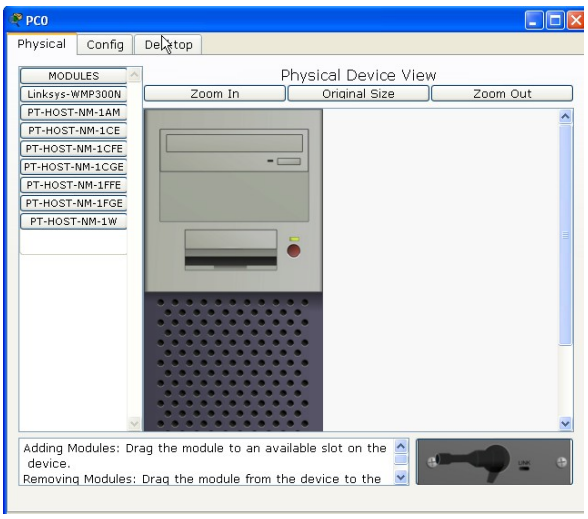

4. Επιλέξτε την κατηγορία Connections και διαλέξτε τύπο καλωδίου (Τι τύπου κα λώδιο θα επιλέξουμε για μια σύνδεση PC to Hub)?



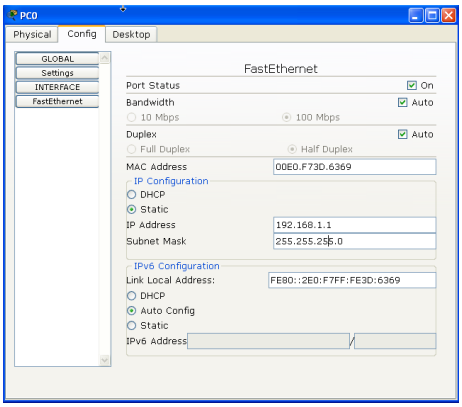

**5.** 5. Με αριστερό κλικ σε κάθε PC, σας εμφανίζονται τα διαθέσιμα interfaces (RS232 – FastEthernet). Επιλέξτε το FastEthernet και με το νήμα φέρτε το επάνω στο Hub και πιέζοντας το αριστερό κλικ συνδέστε το με ένα από τα διαθέσιμα FastEthernet Interfaces. Όταν ολοκληρώσετε με όλα τα PCs το δίκτυό σας θα μοιά ζει με την παρακάτω εικόνα




**6.** Στη συνέχεια για να μπορούν να επικοινωνούν τα PCs (Hosts) θα πρέπει να τους δώσετε IP διευθύνσεις. Κάνουμε αριστερό κλικ επάνω σε ένα PC. Και εμφανίζεται το παράθυρο διαχείρισης όπως φαίνεται στην παρακάτω εικόνα.



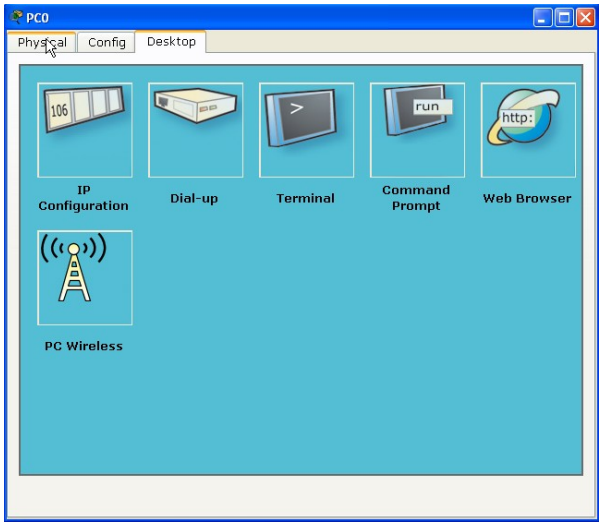

**7.** Επιλέγουμε Config και στο εμφανιζόμενο παράθυρο Fastethenet. Τώρα στο πεδίο IP address και Subnet Mask τοποθετούμε την IP διεύθυνση δικτύου που θέλουμε να έχει αυτό το PC και τη μάσκα υποδικτύου όπως φαίνεται στην παρακάτω εικόνα.



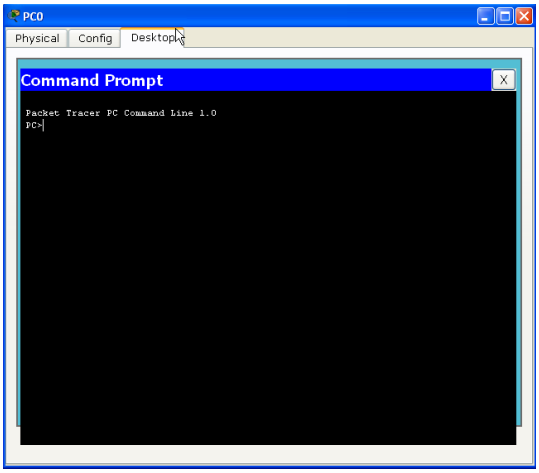

**8.** Για όλα τα PCs του δικτύου μας ομοίως τοποθετούμε τις IP διευθύνσεις σύμφωνα με τον παρακάτω πίνακα.

| Όνομα Host | IP Διεύθυνση | Μάσκα Υποδικτύου |
|---|---|---|
| PC0 | 192.168.1.1 | 255.255.255.0 |
| PC1 | 192.168.1.2 | 255.255.255.0 |
| PC2 | 192.168.1.3 | 255.255.255.0 |
| PC3 | 192.168.1.4 | 255.255.255.0 |

**9.** Κάνουμε αριστερό κλικ επάνω στο PC0 και επιλέγουμε Desktop->Command Prompt όπως φαίνεται στο παρακάτω παράθυρο.




**10.** Από την επιλογή αυτή εμφανίζεται το παρακάτω παράθυρο το οποίο μας δίνει την βασική κονσόλα εντολών από το λειτουργικό σύστημα του PC0 (MS-DOS) όπως φαίνεται στο παρακάτω παράθυρο.




**11.** Δίνουμε από το PC0 την εντολή Ping στις παρακάτω διευθύνσεις. Απαντήστε στις παρακάτω ερωτήσεις:

**I.** (192.168.1.1) Σε ποιόν απευθύνεται αυτό το ping;
- Στο PC1
- Στο PC2
- Στο τοπικό Interface του PC0

**II.** (192.168.1.2) Έχουμε απάντηση;
- NAI
- OXI

**III.** (192.168.1.2) Έχουμε απάντηση;
1. NAI
2. OXI

Δικαιολογήστε τις απαντήσεις σας.

**Τι πρέπει να παραδώσετε:**
1. Τις απαντήσεις στις ερωτήσεις
2. Το λυμένο pka αρχείο.

## Δ) μέρος - Packet Tracer - Configure SSH

Ανοίξτε το αρχείο Packet Tracer - Configure SSH.pka και υλοποιήστε τα παρακάτω βήματα.
Κατάλογο με εντολές για μεταγωγείς CISCO μπορείτε να βρείτε εδώ.

**Μέρος 1: Ασφαλείς κωδικοί πρόσβασης**
- Χρησιμοποιώντας τη γραμμή εντολών στο PC1, κάντε Telnet στο S1. Ο κωδικός για τον χρήστη EXEC είναι cisco.
- Αποθηκεύστε την τρέχουσα διαμόρφωση, έτσι ώστε τυχόν σφάλματα που μπορεί να κάνετε μπορούν να αντιστραφούν με την εναλλαγή της ισχύος για το S1.
- Εμφανίστε την τρέχουσα διαμόρφωση και σημειώστε ότι οι κωδικοί πρόσβασης είναι σε απλό κείμενο. Εισαγάγετε την εντολή που κρυπτογραφεί τους κωδικούς πρόσβασης απλού κειμένου:
  `S1(config)# service password-encryption`
- Βεβαιωθείτε ότι οι κωδικοί πρόσβασης είναι κρυπτογραφημένοι.

**Μέρος 2: Κρυπτογράφηση επικοινωνιών**
- Ορίστε το όνομα τομέα IP και δημιουργήστε ασφαλή κλειδιά. Γενικά δεν είναι ασφαλές να χρησιμοποιείτε το Telnet, επειδή τα δεδομένα μεταφέρονται σε απλό κείμενο. Επομένως, χρησιμοποιήστε το SSH όταν είναι διαθέσιμο.

- Διαμορφώστε το όνομα τομέα ως netacad.pka.
- Απαιτούνται κλειδιά ασφαλείας για την κρυπτογράφηση των δεδομένων. Δημιουργήστε τα κλειδιά RSA χρησιμοποιώντας ένα μήκος 1024.
- Δημιουργήστε έναν χρήστη SSH και επαναρυθμίστε τις γραμμές VTY για πρόσβαση μόνο SSH.
  Ως username και password χρησιμοποιείστε το username που έχετε στο eclass.
- Δημιουργήστε έναν χρήστη διαχειριστή με “Cisco” ως μυστικό κωδικό πρόσβασης.
- Ρυθμίστε τις γραμμές VTY για να ελέγξετε την τοπική βάση δεδομένων ονόματος χρήστη για τα διαπιστευτήρια σύνδεσης και για να επιτρέψετε μόνο SSH για απομακρυσμένη πρόσβαση. Καταργήστε τον υπάρχοντα κωδικό πρόσβασης γραμμής vty.

**Μέρος 3: Επαλήθευση της εφαρμογής SSH**

- Πραγματοποιήστε έξοδο από την περίοδο λειτουργίας Telnet και προσπαθήστε να συνδεθείτε ξανά χρησιμοποιώντας το Telnet. Η προσπάθεια πρέπει να αποτύχει.
- Προσπαθήστε να συνδεθείτε χρησιμοποιώντας SSH. Πληκτρολογήστε ssh και πατήστε Enter χωρίς παραμέτρους για να αποκαλύψετε τις οδηγίες χρήσης εντολών. Συμβουλή: Η επιλογή -l είναι το γράμμα "L", όχι ο αριθμός 1.
- Μετά την επιτυχή σύνδεση, εισαγάγετε την προνομιακή λειτουργία EXEC και αποθηκεύστε τη διαμόρφωση. Αν δεν μπόρεσετε να έχετε επιτυχή πρόσβαση στο S1, κάντε εναλλαγή της τροφοδοσίας και έναρξη πάλι όπως στο Μέρος 1.

**Τι πρέπει να παραδώσετε:**

3. Την ακριβή λίστα των εντολών που εκτελέσατε
4. Το λυμένο pka αρχείο.