



### 3ο Εργαστήριο

#### Στόχος Α

Μελέτη των πρωτοκόλλων του επιπέδου μεταφοράς (transport), L4 της στοίβας πρωτοκόλλων Διαδικτύου (TCP/IP).

#### Περίληψη Θεωρίας

##### L5 - Επίπεδο Εφαρμογής

Μία διεργασία, που υλοποιεί κάποιο πρωτόκολλο επιπέδου εφαρμογής (L5), έχει δεδομένα προς αποστολή με αποδέκτη μια άλλη διεργασία που υλοποιεί το ίδιο πρωτόκολλο επιπέδου εφαρμογής. Οι δύο διεργασίες σχετίζονται ως προς την μεταξύ τους επικοινωνία με το μοντέλο πελάτη-εξυπηρετητή (client-server), μια κατακεντρωμένη αρχιτεκτονική εφαρμογών κατά την οποία ο server προσφέρει υπηρεσίες που εξυπηρετούν τον client.

Η μονάδα πληροφορίας (PDU) στο επίπεδο εφαρμογής είναι τα δεδομένα (data) που ανταλλάσσονται μεταξύ client και server. Ένα PDU οποιουδήποτε πρωτοκόλλου του επιπέδου, περιέχει μια κεφαλίδα (header) με πληροφορίες οργανωμένες σε πεδία, που χρησιμοποιούνται για τον έλεγχο του διαλόγου μεταξύ των διεργασιών. Για παράδειγμα:

- Σε ένα αίτημα HTTP (HTTP request) προς μια διεργασία web server το πεδίο κεφαλίδας `User-Agent` γνωστοποιεί τον τύπο της διεργασίας client, δηλαδή ποιον web browser χρησιμοποιεί ο χρήστης που ζητάει την ιστοσελίδα. Αυτό μπορεί στην συνέχεια να χρησιμοποιηθεί στον server για να στείλει διαφορετική απόκριση (HTTP response) στον client.
- Στην κεφαλίδα του HTTP response στο πεδίο `Server` υπάρχει το είδος του web server.

Γενικά οι κεφαλίδες υποδεικνύουν αν το μήνυμα είναι μία ερώτηση, απάντηση ή και δεδομένα τα οποία ανταλλάξουν οι δύο διεργασίες. Οποιοδήποτε πρωτόκολλο επιπέδου εφαρμογής ορίζει ρητά το/τα πρωτόκολλο(-α) που πρέπει να χρησιμοποιηθούν στο επίπεδο μεταφοράς.

##### L4 - Επίπεδο Μεταφοράς

Τα πρωτόκολλα επιπέδου μεταφοράς (L4) εξυπηρετούν την μεταφορά δεδομένων που ζητείται από τα πρωτόκολλα επιπέδου εφαρμογής (L5), πλαισιώνοντας τα δεύτερα με πρόσθετη πληροφορία. Οι υπηρεσίες του L4 είναι υλοποιημένες και τρέχουν ως τμήμα του λειτουργικού συστήματος (OS). Με αυτές τα δεδομένα μεταφέρονται από μια διεργασία OS του τοπικού υπολογιστή, προς μια διεργασία OS του απομακρυσμένου υπολογιστή.

Ενώ στο παρακάτω επίπεδο δικτύου - L3 γίνεται προσπάθεια για μεταφορά πακέτων (packets) μεταξύ δύο συστημάτων, στο επίπεδο L4 γίνεται μεταφορά τμημάτων (segments) μεταξύ διεργασιών των δύο συστημάτων. Αυτή η επέκταση λέγεται **πολύπλεξη (multiplexing)** και **αποπολύπλεξη επιπέδου μεταφοράς (transport-layer demultiplexing)**. Για την αναγνώριση των διεργασιών που ανταλλάσσουν segments στο επίπεδο μεταφορά υπάρχουν τα sockets. Σύμφωνα με το αρχικό πρότυπο RFC 147 υπάρχει ένας 32bit αριθμός αναγνώρισης, αλλά θεωρούνται επίσης στην βιβλιογραφία ως συνδυασμός IP/Port.

Το επίπεδο δικτύου δεν εγγυάται την μεταφορά των πακέτων με την σωστή σειρά, ούτε και την ακεραιότητα των πληροφοριών που μεταφέρονται. Υλοποιεί δηλαδή μια **υπηρεσία καλύτερης προσπάθειας (best-effort delivery service)**. Αυτά υλοποιούνται στο επίπεδο μεταφοράς με τα πρωτόκολλα TCP και UDP.

#### Επίπεδο Μεταφοράς (L4)

	TCP	UDP
Παράδοση από διεργασία σε διεργασία.	NAI	NAI
Έλεγχος ασφαλείας.	NAI	NAI
Εγγύηση για την σωστή παραλαβή των δεδομένων (L5) του επιπέδου εφαρμογής.	NAI	OXI
Εγγύηση για την σωστή σειρά λήψης των τμημάτων (L3).	NAI	OXI
Έλεγχος συμφόρησης.	NAI	OXI

#### Επίπεδο Δικτύου (L3)

	IP
Παράδοση από σύστημα σε σύστημα.	NAI
Έλεγχος ασφαλείας.	Προαιρετικός
Εγγύηση για την σωστή παραλαβή των τμημάτων (L4) του επιπέδου μεταφοράς.	OXI
Εγγύηση για την σωστή σειρά λήψης των πακέτων (L3).	OXI
Έλεγχος συμφόρησης.	OXI

### A1) Wireshark - TCP διαδικασία

Στα Windows βρείτε και εκκινήστε το Wireshark από το εικονίδιο του. Το αντίστοιχο στο λειτουργικό σύστημα Linux είναι το “wireshark network analyzer for studin”. Αρχικά εμφανίζει μια λίστα με τις διεπαφές δικτύου (network interfaces) που έχει ο υπολογιστής σας. Παρατηρήστε ότι υπάρχει κίνηση δεδομένων σε κάποιες από αυτές. Σε Windows επιλέξτε την “Local Area Connection” που αντιστοιχεί στην ενσύρματη κάρτα δικτύου και στο Linux το “Any”.

- Με την επιλογή του interface το Wireshark αρχίζει απευθείας να καταγράφει δεδομένα που διέρχονται από το φυσικό μέσο του δικτύου σας.
- Ανοίξτε ένα web browser, καθαρίστε το προηγούμενο ιστορικό περιήγησης (Mozilla/Chrome: Shift+Ctrl+Del) και μεταβείτε στην διεύθυνση του δοκιμαστικού server που σας δόθηκε για αυτό το εργαστήριο.
- Μόλις ολοκληρωθεί το κατέβασμα της σελίδας, επιλέξτε το κουμπί του τερματισμού καταγραφής στο Wireshark.
- Επιλέξτε το κατάλληλο φίλτρο ώστε να εμφανίζονται πληροφορίες οποιουδήποτε πρωτοκόλλου αλλά μόνο μεταξύ του υπολογιστή σας και του δοκιμαστικού server, σε οποιαδήποτε κατεύθυνση. Θυμηθείτε πως χρησιμοποιούμε στο φίλτρο τα ορίσματα ip.src και ip.dst.

## Ερωτήσεις Wireshark - TCP διαδικασία

**E3.1** Εντοπίστε το πρώτο αίτημα HTTP και μελετήστε τα πεδία της κεφαλίδας (Info: GET / HTTP/1.1). Εντοπίστε την αμέσως επόμενη απόκριση HTTP από τον server και μελετήστε την κεφαλίδα.

**E3.2** Παρατηρήστε ότι πριν αρχίσει ο διάλογος του πρωτοκόλλου εφαρμογής HTTP υπάρχει διάλογος του πρωτοκόλλου μεταφοράς TCP. Μελετήστε τα πεδία της κεφαλίδας του TCP για όλα τα segment που ανταλλάχθηκαν πριν αρχίσει ο HTTP διάλογος.

**E3.3** Τι πληροφορία περιέχει το πεδίο Sequence Number στην κεφαλίδα των TCP segments;

**E3.4** Πόσα segment αντάλλαξαν οι δύο μεριές πριν αρχίσουν να αποστέλλουν δεδομένα επιπέδου εφαρμογής (του πρωτοκόλλου HTTP στην περίπτωση μας);

**E3.5** Τι πληροφορία μας δίνει το πεδίο Timestamps στην κεφαλίδα του TCP segment που αντιστοιχεί στην πρώτη απόκριση HTTP;

**E3.6** Με ποιον τρόπο τερματίζεται η επικοινωνία, που εδώ ονομάζεται TCP σύνδεση (connection);

**E3.7** Πόσα segment αντάλλαξαν οι δύο μεριές πριν συμφωνήσουν στον τερματισμό της TCP σύνδεσης;

**E3.8** Στην κεφαλίδα υπάρχει το πεδίο Flags. Ποιο flag είναι set (αναμμένο bit) στην περίπτωση τερματισμού μιας TCP σύνδεσης; Παρατηρήστε τα flags στο άνω panel του Wireshark.

**E3.9** Ποια port χρησιμοποιήθηκαν από την μεριά του client και ποιά από τη μεριά του server;

**E3.10** Όπως ήδη γνωρίζετε από προηγούμενο εργαστήριο ο server ακούει για αιτήματα στην θύρα 80 (listen port 80). Πόσα sockets χρησιμοποιήθηκαν από τον client και ποιοι οι αντίστοιχοι αριθμοί των θυρών τους;

## A2) Wireshark - UDP διαδικασία

- Στην γραμμή εντολών Windows καθαρίστε την dns cache με **ipconfig /flushdns**
- Ανοίξτε την καταγραφή στο Wireshark για την παρακάτω δικτυακή επικοινωνία:
- Εκτελέστε την εντολή **dig www.iana.org A**
- Σταματήστε την καταγραφή στο Wireshark.
- Για το πρωτόκολλο DNS βρείτε σε ποιον server έστειλε το ερώτημα ο υπολογιστής σας.
- Επιλέξτε το κατάλληλο φίλτρο ώστε να εμφανίζονται πληροφορίες οποιουδήποτε πρωτοκόλλου αλλά μόνο μεταξύ του υπολογιστή σας και του DNS server, προς οποιαδήποτε κατεύθυνση. Θυμηθείτε πως χρησιμοποιούμε στο φίλτρο τα ορίσματα **ip.src** και **ip.dst**.

## Ερωτήσεις Wireshark - UDP διαδικασία

**E3.11** Μελετήστε τα πεδία της κεφαλίδας του πρώτου UDP segment του DNS διαλόγου.

**E3.12** Ποιες διαφορές μεταξύ TCP και UDP εντοπίζετε άμεσα μέσα από τις κεφαλίδες των δύο πρωτοκόλλων του επιπέδου μεταφοράς;

**E3.13** Γιατί κατά την γνώμη σας το DNS (L5) χρησιμοποιεί UDP (L4) και όχι TCP (L4);

## Στόχος Β

Μελέτη των πρωτοκόλλων του επιπέδου δικτύου (network), L3 της στοίβας πρωτοκόλλων Διαδικτύου. Κατανόηση της μηχανικής των διευθύνσεων του πρωτοκόλλου IP version 4.

### L3 - Επίπεδο Δικτύου

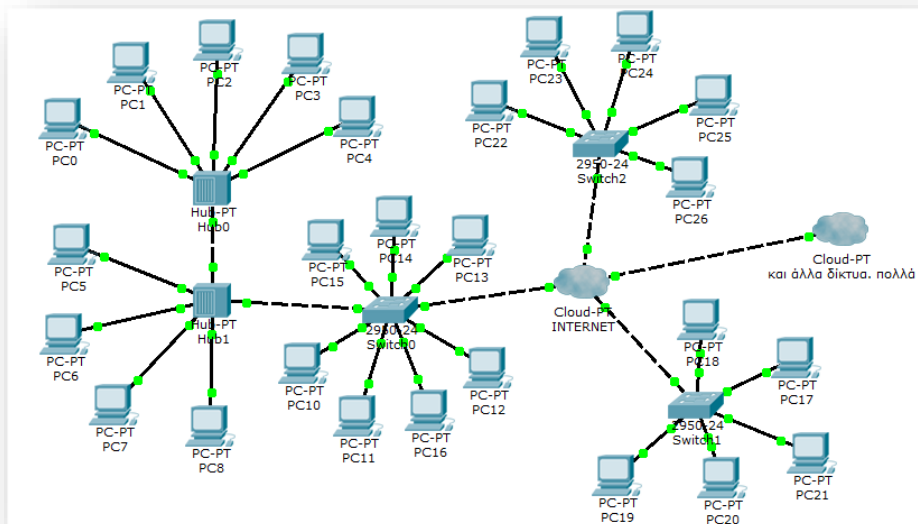
Στο πρωτόκολλο επιπέδου δικτύου (L3) εισέρχεται για πρώτη φορά η έννοια της διευθυνσιοδότησης των δύο μερών της επικοινωνίας, ώστε να μπορεί να γίνει η μεταφορά του segment από την πηγή στον προορισμό. Οι διευθύνσεις αυτές λέγονται Internet Protocol Addresses και σήμερα χρησιμοποιούνται κυρίως οι IP v4 που έχουν μήκος 32bit και γράφονται ως τέσσερις αριθμοί 8bit χωρισμένοι με τελείες (dotted-decimal), π.χ. 192.168.1.1. Από τους διαθέσιμους  $2^{32} - 1$  αριθμούς κάποιοι είναι δεσμευμένοι από τον οργανισμό IANA (Αναζητήστε Online: IANA IPv4 Special-Purpose Address Registry), οι οποίοι χρησιμοποιούνται κυρίως σε τοπικά δίκτυα (local area networks). Σήμερα αρχίζει σταδιακά η μετάβαση σε IP v6 με μήκος 128bit που γράφονται ως οκτώ δεκαεξαδικοί αριθμοί των 16bit. Για παράδειγμα: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Συνήθως σε κάθε συσκευή (σταθερό υπολογιστή, φορητή συσκευή, συσκευή IoT) ανατίθεται μια μοναδική διεύθυνση IP στο Διαδίκτυο. Σε οικιακούς χρήστες η διεύθυνση IP μπορεί να αλλάζει σε τακτά χρονικά διαστήματα, και αυτή λέγεται dynamic IP. Μπορείτε να παρατηρήσετε τις διαφορετικές IP που ανατίθενται στο οικιακό δίκτυο σας σε ένα διάστημα κάποιων ημερών, μέσω της σελίδας <https://whatismyipaddress.com/>. Επίσης υπάρχει η περίπτωση που σε έναν εξυπηρετητή ανατίθενται πολλαπλές σταθερές (static) διευθύνσεις IP.

Τα πρωτόκολλα επιπέδου δικτύου (L3) εξυπηρετούν την αναγνώριση πηγής και προορισμού που απαιτείται από τα πρωτόκολλα επιπέδου μεταφοράς (L4), πλαισιώνοντας τα δεύτερα με πρόσθετη πληροφορία. Στην περίπτωση TCP / IP απλά προστίθεται στο segment μια κεφαλίδα, δημιουργώντας την PDU του L3 που ονομάζεται πακέτο (packet).

### B1) Διευθύνσεις IP

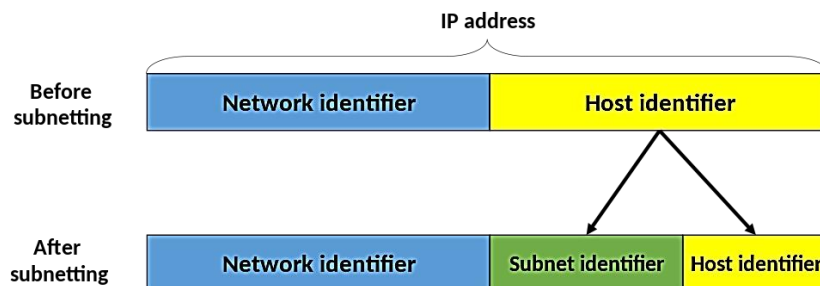
Η εικόνα 1 παρουσιάζει ένα δημόσιο δίκτυο (public network). Οι υπολογιστές συνδέονται μεταξύ τους με συσκευές του L1 ή L2 επιπέδου. Οι συσκευές αυτές επίσης συνδέονται μεταξύ τους. Στο σύννεφο υποθέστε ότι υπάρχουν όλα τα υπόλοιπα δίκτυα τα οποία είναι προσβάσιμα μέσω του Διαδικτύου. Σημειώστε ότι υπάρχουν και δίκτυα που δεν είναι συνδεδεμένα στο διαδίκτυο, για παράδειγμα ένα τοπικό δίκτυο (LAN) για τα κρίσιμα συστήματα ενός αεροσκάφους.



Εικόνα 1: Δημόσιο δίκτυο του CNLab3.pkt

Οι δρομολογητές (routers) που μεταφέρουν τα πακέτα μεταξύ δικτύων δεν γνωρίζουν την ακριβή διεύθυνση του συστήματος αλλά μόνο το δίκτυο στο οποίο ανήκουν. Έχουν ένα εσωτερικό **πίνακα δρομολόγησης (routing table)** που καταγράφει τις διαδρομές προς τα δίκτυα προορισμού που προωθούν ένα πακέτο. Όταν φτάσει στο δίκτυο προορισμού θα παραδοθεί στον παραλήπτη.

Το πρωτόκολλο IP δίνει την δυνατότητα στους διαχειριστές δικτύων να ορίσουν μικρότερα υποδίκτυα. Για αυτόν τον λόγο έχουμε μια μάσκα υποδικτύου (subnet mask) που χωρίζει την διεύθυνση IP σε δύο μέρη, το **πρόθεμα δικτύου (network prefix ή network identifier)** και το **αναγνωριστικό συστήματος (host identifier)**, δηλαδή το **σύστημα** με το **δίκτυο** στο οποίο ανήκει. Έτσι το πρωτόκολλο καθορίζει αν ο host είναι στο ίδιο υποδίκτυο ή σε κάποιο απομακρυσμένο.



**Εικόνα 2: Διαχωρισμός διεύθυνσης IP**

Μετά την εφαρμογή της μάσκας με την δυαδική πράξη  $\{IP\ Address\} \text{ AND } \{Subnet\ Mask\}$  παίρνουμε το network prefix που θα χρησιμοποιήσει ο δρομολογητής. Με την αντιστροφή της μάσκας και κατόπιν OR, δηλαδή  $(\text{NOT } \{Subnet\ Mask\}) \text{ OR } \{IP\ Address\}$  παίρνουμε την **broadcast address** μια διεύθυνση που χρησιμοποιείται για αποστολή προς όλα τα συνδεδεμένα συστήματα που δέχονται πακέτα IP. Για παράδειγμα :

**IP** : 192.168.1.10 (Class C)  
**Subnet Mask** : 255.255.255.0  
 Subnet Mask (Bin) : 1111 1111 • 1111 1111 • 1111 1111 • 0000 0000  
 Subnet Mask (Bits) : /24 (Το πλήθος των bits από αριστερά προς τα δεξιά)  
 Subnets : 1  
**Network** : 192.168.1 **Host:** 10  $\in \{1, \dots, 254\}$   
**Broadcast Address** : 192.168.1.255

Επειδή υπάρχουν 24 bits αναμμένα στην μάσκα μπορούμε να αναπαραστήσουμε το υποδίκτυο με την σημειογραφία CIDR **{network identifier}/{mask bits}** δηλαδή 192.168.1.0/24. Στο παραπάνω παράδειγμα το τέταρτο τμήμα της IP διεύθυνσης ενός συστήματος (τα τελευταία 8 bits) δεν μπορεί να είναι 0 ή 255. Το 0 χρησιμοποιείται ως αναγνωριστικό για το δίκτυο και το 255 είναι το αναγνωριστικό για όλα συνδεδεμένα συστήματα που δέχονται πακέτα IP, δηλαδή ένα **wildcard** που σημαίνει «όλα τα συστήματα». Έτσι με την παραπάνω ρύθμιση έχουμε κρατήσει θέσεις για τους hosts 1-254 σε 1 υποδίκτυο. Αλλάζοντας την μάσκα αλλάζει το πλήθος των υποδικτύων και των συστημάτων σε αυτά:

**IP** : 192.168.1.10 (Class C)  
**Subnet Mask** : 255.255.255.128  
 Subnet Mask (Bin) : 1111 1111 • 1111 1111 • 1111 1111 • 1 000 0000  
 Subnet Mask (Bits) : /25  
 Subnets : 2 (Με 1 bit έχουμε δύο subnets)  
**Network (Subnet 1)** : 192.168.1.0/25 **Host:** 10  $\in \{1, \dots, 126\}$   
**Subnet 2** : 192.168.1.128/25 {129,...,254}  
**Broadcast Addresses** : **Subnet 1:** 192.168.1.127 **Subnet 2:** 192.168.1.255



Παρατηρούμε ότι πλέον έχουμε ένα bit επιπλέον αναμμένο που αποτελεί το subnet identifier στην περίπτωση της κλάσης C, στην οποία ανήκει η διεύθυνση IP. Με αυτήν την μάσκα έχουμε ορίσει  $2^1$  υποδίκτυα το κάθε ένα με πλήθος διαφορετικών host  $2^7 - 2$ . και το 127 λειτουργεί ως wildcard. Η κλάση C υποστηρίζει από 24 ως 30 bits της διεύθυνσης IP ως network prefix.

Class A			Class B			Class C		
Bits	Mask	Hosts/SubNet	Bits	Mask	Hosts/SubNet	Bits	Mask	Hosts/SubNet
/8	255.0.0.0	16,777,214	/16	255.255.0.0	65,534	/24	255.255.255.0	254
/9	255.128.0.0	8,388,606	/17	255.255.128.0	32,766	/25	255.255.255.128	126
/10	255.192.0.0	4,194,302	/18	255.255.192.0	16,382	/26	255.255.255.192	62
/11	255.224.0.0	2,097,150	/19	255.255.224.0	8,19	/27	255.255.255.224	30
/12	255.240.0.0	1,048,574	/20	255.255.240.0	4,094	/28	255.255.255.240	14
/13	255.248.0.0	524,286	/21	255.255.248.0	2,046	/29	255.255.255.248	6
/14	255.252.0.0	262,142	/22	255.255.252.0	1,022	/30	255.255.255.252	2
/15	255.254.0.0	131,07	/23	255.255.254.0	510			

## Βέλτιστη ανάθεση διευθύνσεων IP με subnetting

### Παράδειγμα 1 - Απλούστερη Λύση

Έστω ότι πρέπει να μοιράσουμε τις διευθύνσεις που μπορεί να υπάρξουν στο 192.168.1.0/24 σε τρία υποδίκτυα που έχουν το κάθε ένα από 23, 50 και 5 hosts.

- Οργανώνουμε μια λίστα με τις ανάγκες βάσει του μεγέθους (size) και βρίσκουμε την subnet mask της κατάλληλης χωρητικότητας. Θα ξεκινήσουμε από τα μεγαλύτερα και μετά θα διαχωρίζουμε κατάλληλα τον υπόλοιπο χώρο διευθύνσεων για να χωρέσουν τα μικρότερα.

n	Size	Bits	Capacity $C_i$
1	50	/26	62
2	23	/27	30
3	5	/29	6

- Ξεκινάμε να βρούμε το subnet  $n = 1$  για το μεγαλύτερο μέγεθος  $s_1 = 50$ . Με χρήση της μάσκας /26 χωρίζουμε στα εξής subnets:

	Network Address	Usable Host Range	Broadcast Address:
1	192.168.1.0	192.168.1.1 - 192.168.1.62	192.168.1.63
2, 3	192.168.1.64	192.168.1.65 - 192.168.1.126	192.168.1.127
	192.168.1.128	192.168.1.129 - 192.168.1.190	192.168.1.191
	192.168.1.192	192.168.1.193 - 192.168.1.254	192.168.1.255

- Θα χρησιμοποιήσουμε το πρώτο και δεύτερο υποδίκτυο (προσέξτε τα χρώματα των subnet bits).

- 1100 0000.1010 1000.0000 0001.00 000000 → 192.168.1.0
  - 1100 0000.1010 1000.0000 0001.01 000000 → 192.168.1.64

- Αναθέτουμε το εύρος διευθύνσεων για το  $n = 1$

n	Size	Bits	Capacity	SubNet	Usable IP Range
1	50	/26	62	192.168.1.0/26	192.168.1.1 - 192.168.1.62
2	23	/27	30		
3	5	/29	6		

- Προχωράμε στην θέση  $n = 2$  και χρησιμοποιούμε μάσκα /27 για το δεύτερο υποδίκτυο 192.168.1.64. Έτσι ο διαχωρισμός γίνεται

Subnet address	Netmask	Range of addresses	Useable IPs	Hosts	Divide	Join
192.168.1.0/26	255.255.255.192	192.168.1.0 - 192.168.1.63	192.168.1.1 - 192.168.1.62	62	Divide	/26
192.168.1.64/27	255.255.255.224	192.168.1.64 - 192.168.1.95	192.168.1.65 - 192.168.1.94	30	Divide	/27
192.168.1.96/27	255.255.255.224	192.168.1.96 - 192.168.1.127	192.168.1.97 - 192.168.1.126	30	Divide	/27

- 1100 0000.1010 1000.0000 0001.0100 0000 → 192.168.1.64
  - 1100 0000.1010 1000.0000 0001.0110 0000 → 192.168.1.96

- Αναθέτουμε το εύρος διευθύνσεων για το  $n = 2$

n	Size	Bits	Capacity	SubNet	Usable IP Range
1	50	/26	62	<b>192.168.1.0/26</b>	192.168.1.1 - 192.168.1.62
2	23	/27	30	<b>192.168.1.64/27</b>	192.168.1.65 - 192.168.1.94
3	5	/29	6		

- Για την θέση  $n = 3$  μπορούμε να χρησιμοποιήσουμε το υποδίκτυο 192.168.1.96

n	Size	Bits	Capacity	SubNet	Usable IP Range
1	50	/26	62	<b>192.168.1.0/26</b>	192.168.1.1 - 192.168.1.62
2	23	/27	30	<b>192.168.1.64/27</b>	192.168.1.65 - 192.168.1.94
3	5	/29	6	<b>192.168.1.96/29</b>	192.168.1.97 - 192.168.1.102

το οποίο διχοτομείται περαιτέρω με την μάσκα /28 και κατόπιν με την /29.

Subnet address	Netmask	Range of addresses	Useable IPs	Hosts	Divide	Join
192.168.1.0/26	255.255.255.192	192.168.1.0 - 192.168.1.63	192.168.1.1 - 192.168.1.62	62	Divide	/26 /27 /29 /28 /25
192.168.1.64/27	255.255.255.224	192.168.1.64 - 192.168.1.95	192.168.1.65 - 192.168.1.94	30	Divide	
192.168.1.96/29	255.255.255.248	192.168.1.96 - 192.168.1.103	192.168.1.97 - 192.168.1.102	6	Divide	
192.168.1.104/29	255.255.255.248	192.168.1.104 - 192.168.1.111	192.168.1.105 - 192.168.1.110	6	Divide	
192.168.1.112/28	255.255.255.240	192.168.1.112 - 192.168.1.127	192.168.1.113 - 192.168.1.126	14	Divide	

Όπως είναι προφανές περισσεύουν τα υποδίκτυα 192.168.1.104/29 και 192.168.1.112/28 που χωρούν 6 και 14 hosts το κάθε ένα.

### Παράδειγμα 1 - Εναλλακτική Λύση

Έστω ότι πρέπει να μοιράσουμε τις διευθύνσεις που μπορεί να υπάρχουν στο 192.168.1.0/24 σε τρία υποδίκτυα που έχουν το κάθε ένα από 23, 50 και 5 hosts.

- Οργανώνουμε μια λίστα με τις ανάγκες βάσει του μεγέθους (size) και βρίσκουμε την subnet mask της κατάλληλης χωρητικότητας. Θα ξεκινήσουμε από τα μεγαλύτερα και μετά θα αναθέτουμε κατάλληλα τον κενό χώρο διευθύνσεων που προκύπτει στα μικρότερα.

n	Size	Bits	Capacity
1	50	/26	$c_i$ 62
2	23	/27	30
3	5	/29	6

- Ξεκινάμε να βρούμε το subnet  $n = 1$  για το μεγαλύτερο μέγεθος  $s_1 = 50$ . Πριν το εύρος διευθύνσεων που θα αναθέσουμε σε αυτό, πρέπει να αφήσουμε χωρητικότητα  $c_r$  τα υπόλοιπα subnets  $\{n + 1, \dots, k\}$  από τα συνολικά  $k = 3$ , ώστε να υπάρχει χώρος και για τα δικά τους εύρη διευθύνσεων. Δηλαδή για το άθροισμα  $r = \sum_{i=n+1}^k c_i$  πρέπει να ισχύει  $c_r \geq r$ . Εδώ τα subnets 2,3 αθροίζουν σε  $r = 36$  και αρκεί χωρητικότητα  $c_r = 62$  που μπορεί να επιτευχθεί με χρήση της μάσκας /26. Αυτή δημιουργεί τα εξής subnets.

Network Address	Usable Host Range	Broadcast Address:
192.168.1.0	192.168.1.1 - 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 - 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.254	192.168.1.255

- Θα χρησιμοποιήσουμε τα δύο πρώτα subnets (προσέξτε τα χρώματα των subnet bits).
  - 1100 0000.1010 1000.0000 0001.00 000000 → 192.168.1.0
  - 1100 0000.1010 1000.0000 0001.01 000000 → 192.168.1.64
- Το πρώτο subnet το δεσμεύουμε για τα 2,3 και αναθέτουμε το δεύτερο στο 1:

n	Size	Bits	Capacity	SubNet	Usable IP Range
1	50	/26	62	<b>192.168.1.64/26</b>	192.168.1.65 - 192.168.1.126
2	23	/27	30		
3	5	/29	6		

- Προχωράμε στην θέση  $n = 2$  και με τον ίδιο τρόπο έχουμε  $r = 5$ ,  $c_r = 6$  και χρησιμοποιούμε μάσκα  $/27$ . Με αυτήν την μάσκα έχουμε τα εξής subnets, αποκλείοντας αυτά που έχουμε ήδη αναθέσει:

Network Address	Usable Host Range	Broadcast Address:
192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
<del>192.168.1.64</del>	<del>192.168.1.65 - 192.168.1.94</del>	<del>192.168.1.95</del>
<del>192.168.1.96</del>	<del>192.168.1.97 - 192.168.1.126</del>	<del>192.168.1.127</del>
192.168.1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

- Θα χρησιμοποιήσουμε τα δύο πρώτα subnets. Εδώ διαφοροποιείται το τρίτο subnet bit και παραμένουν τα δύο πρώτα σταθερά **00**. Αυτό γίνεται επειδή αν τα δύο πρώτα ήταν **01** θα υπήρχε διένεξη IP με το δίκτυο 1 (δείτε τα ίδια χρώματα και παραπάνω).
  - 1100 0000.1010 1000.0000 0001.**0000** 0000 → 192.168.1.**0**
  - 1100 0000.1010 1000.0000 0001.**0010** 0000 → 192.168.1.**32**
- Το πρώτο subnet το δεσμεύουμε για το 3 και αναθέτουμε το δεύτερο στο 2:

n	Size	Bits	Capacity	SubNet	Usable IP Range
1	50	/26	62	<b>192.168.1.64/26</b>	192.168.1.65 - 192.168.1.126
2	23	/27	30	<b>192.168.1.32/27</b>	192.168.1.33 - 192.168.1.62
3	5	/29	6		

- Το δεσμευμένο subnet που περισσεύει αντιστοιχεί στο τελευταίο δίκτυο 3:

n	Size	Bits	Capacity	SubNet	Usable IP Range
1	50	/26	62	<b>192.168.1.64/26</b>	192.168.1.65 - 192.168.1.126
2	23	/27	30	<b>192.168.1.32/27</b>	192.168.1.33 - 192.168.1.62
3	5	/29	6	<b>192.168.1.0/29</b>	192.168.1.1 - 192.168.1.6

- Έτσι χρησιμοποιούμε διευθύνσεις IP μέχρι την 192.168.1.126 και μένουν αχρησιμοποίητες  $(62 - 50) + (30 - 23) + (30 - 6) = 43$  μέσα στα τρία δίκτυα. Παράλληλα δεν δεσμεύουμε όλο το εύρος των 254 πιθανών διευθύνσεων IP που υπάρχουν στο 192.168.1.0/24.
- Στην περίπτωση που μέσα στους hosts υπολογίζεται και ο δρομολογητής, συνήθως αναθέτουμε το πρώτο IP του εύρους σε αυτόν. Αν είχαμε τρεις routers στο παράδειγμα μας τότε οι IP διευθύνσεις τους θα ήταν:

n	Router IP Address
1	192.168.1.65
2	192.168.1.33
3	192.168.1.1

- Το μέγεθος (size) θεωρείται και ως το πλήθος από διαφορετικά **interfaces (ifs)**. Ένα σύστημα μπορεί να έχει παραπάνω από δύο interfaces, ενώ για κάθε interface ανατίθεται διαφορετική διεύθυνση IP

Μπορούμε να οπτικοποιήσουμε το παραπάνω παράδειγμα, βλέποντας τον κενό χώρο διευθύνσεων IP που προκύπτει. Σε αυτόν μπορούμε να χωρέσουμε επιπλέον ένα subnet με χωρητικότητα 14 υπολογιστών δηλαδή με subnet mask  $/28$ .



network	IP space allocation	subnet (bits)			host (bits)	hosts	chunk
		/26	/27	/28			
192.168.1.0	5	0 0	0	0	0000	2^4 - 2	16
192.168.1.32	23	0 0	1		0 0000	2^5 - 2	32
192.168.1.64	50	0 1			00 0000	2^6 - 2	64

Η εναλλακτική κατάτμηση σε υποδίκτυα εμφανίζεται και παρακάτω:

Όπως είναι προφανές περισσεύουν τα υποδίκτυα 192.168.1.8/29 και 192.168.1.16/28 που χωρούν 6 και 14 hosts το κάθε ένα.

**E3.14** Για ποιο λόγο νομίζετε ότι είναι απαραίτητος ο διαχωρισμός των 32bit μιας IP διεύθυνσης σε δύο μέρη και κατόπιν σε τρία μέρη; Ελέγξτε την υπόθεση που κάνατε με αυτά που αναφέρει το <https://www.networkcomputing.com/data-centers/5-subnetting-benefits>

- <http://www.subnet-calculator.com/>
- <https://www.calculator.net/ip-subnet-calculator.html>
- <https://www.tunnelsup.com/subnet-calculator/>

**E3.16** Έχουμε 13 υπολογιστές στο τοπικό δίκτυο 192.168.1.0. Γράψτε την κατάλληλη μάσκα υποδικτύου σε μορφή: **{network identifier}/{mask bits}** ώστε αφενός να τους χωράει στο ίδιο υποδίκτυο, αφετέρου να υπάρχουν οι λιγότερες μη χρησιμοποιημένες θέσεις host.

**E3.18** Σε ποια κλάση ανήκει το subnet 255.192.0.0/10

**E3.19** Για IP - Subnet Mask: 195.251.123.0 - 255.255.240.0 (κλάση B) προσπαθήστε να κάνετε τις πράξεις για να βρείτε το network prefix και το την broadcast address με το χέρι. Κατόπιν επιβεβαιώστε την ορθότητα με τα online εργαλεία. Ποιο είναι το πλήθος των υποδικτύων, των διαθέσιμων διευθύνσεων ανά υποδίκτυο, ο πρώτος και ο τελευταίος διαθέσιμος αριθμός host;

**E3.20** Κάντε το ίδιο για τις παρακάτω διευθύνσεις.

- 10.0.10.0 - 255.128.0.0 (κλάση A)
- 176.10.5.4 - 255.255.255.252 (κλάση C)
- 194.20.0.32 - 255.255.255.224 (κλάση C)

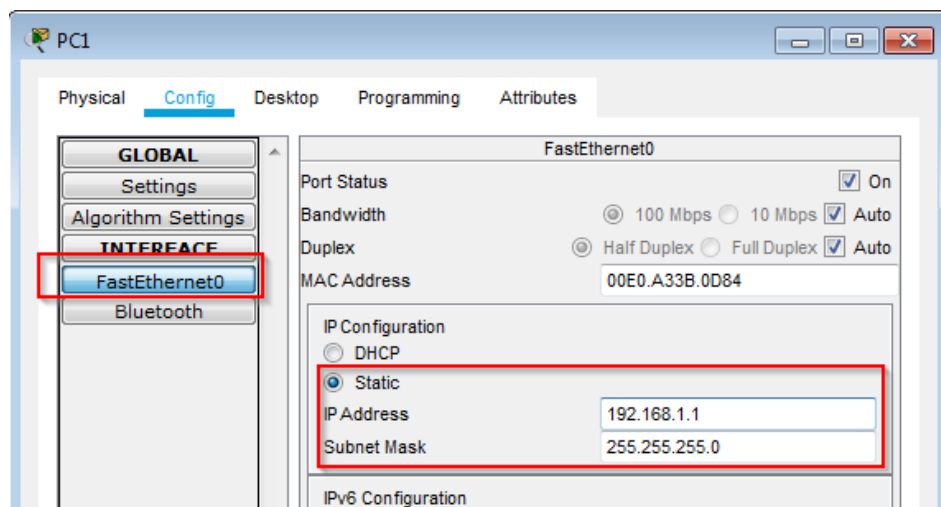
**E3.21** Στο παράδειγμα βέλτιστης ανάθεσης διευθύνσεων IP ποιο είναι το broadcast address για να στείλουμε ένα πακέτο στην περίπτωση της ομάδας με τους 50 hosts;

## B2) Διευθυνσιοδότηση IPv4

Θα χρησιμοποιήσουμε το κυρίαρχο πρωτόκολλο για το επίπεδο δικτύου σήμερα το IPv4, σε ένα δίκτυο που θα προσομοιώσουμε στο **Cisco Packet Tracer**. Ομαδοποιήστε με όποιον τρόπο επιθυμείτε τα PC που συνδέονται στο έτοιμο δίκτυο που περιέχεται στο **CNLab3.pkt** το οποίο εμφανίζεται στην εικόνα 1. Σημειώνεται ότι τα hubs είναι συσκευές μεταγωγής πακέτων που πλέον έχουν αντικατασταθεί από τα switches. Για περισσότερα διαβάστε το:

<https://medium.com/@fiberstoreorenda/do-you-know-the-difference-between-hub-switch-router-b74c2e8a8143>

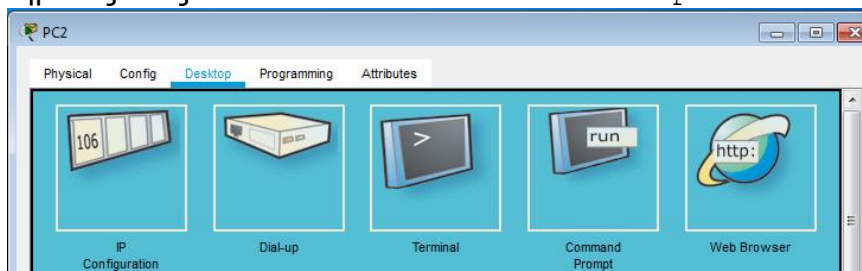
Οργανώστε τις ομάδες σε υποδίκτυα και αναθέστε τις αντίστοιχες στατικές διευθύνσεις IP v4 της μορφής 192.168.x.x για τις μάσκες υποδικτύου που θα δημιουργήσετε. Θυμηθείτε ότι στις συσκευές επιπέδων ζεύξης (L2) και φυσικού (L1) δεν λειτουργεί το πρωτόκολλο IP. Κάνουμε κλικ πάνω σε ένα από τα PC, π.χ. PC1 και εμφανίζεται το παράθυρο με τις δυνατότητες ρύθμισης και δοκιμών.



Εικόνα 3: Ρύθμιση IP στο Cisco Packet Tracer

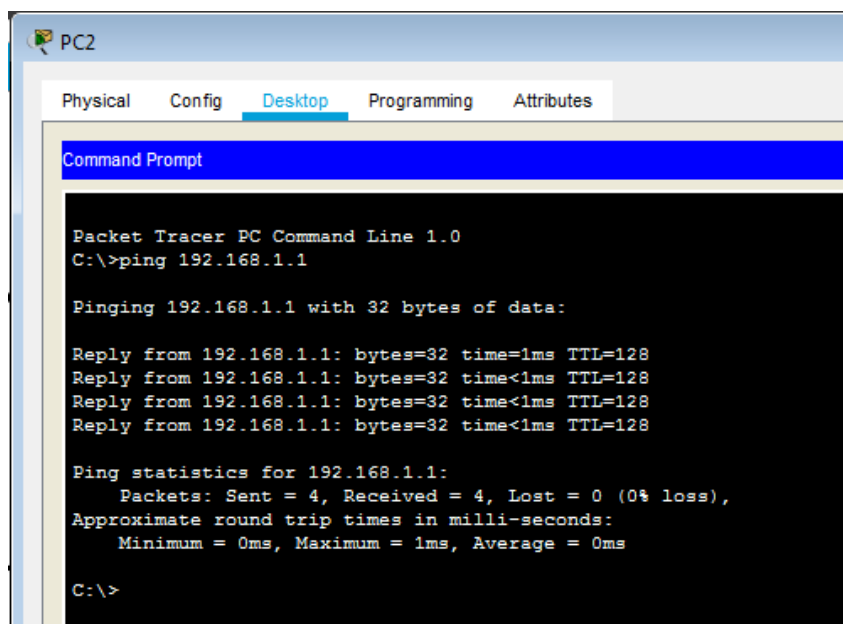
## Διαδικασία Ελέγχου Προσβασιμότητας με Ping

Στο Cisco Packet Tracer υπάρχει η δυνατότητα προσομοίωσης της γραμμής εντολών του λειτουργικού συστήματος ενός PC στο εικονίδιο Command Prompt.



Εικόνα 4: Προσομοίωση ΛΣ

Μπορείτε να εκτελέσετε την εντολή **ping {IP Address}** η οποία θα στείλει πακέτα του πρωτοκόλλου δικτύου ICMP στην **{IP Address}**. Με αυτόν τον τρόπο δοκιμάζει αν είναι εφικτή η επικοινωνία μέσω IP πρωτοκόλλου μεταξύ του τοπικού και του απομακρυσμένου συστήματος. Παράλληλα εμφανίζει στοιχεία σχετικά με τον χρόνο που χρειάστηκε για να φτάσουν τα πακέτα αλλά και την απώλεια πακέτων (packet loss).



Εικόνα 5: Ping στο Cisco Packet Tracer

## Ερωτήσεις - Εργασίες

**E3.22** Τεκμηριώστε τις επιλογές σας ως προς την διευθυνσιοδότηση. Για ποιον λόγο επιλέξατε τις συγκεκριμένες subnet mask.

**E3.22** Επιλέξτε έναν υπολογιστή και με την εντολή **ping** προσπαθήστε να επικοινωνήσετε μέσω του πρωτοκόλλου IP με υπολογιστές του ίδιου IP δικτύου αλλά και με υπολογιστές από όλα τα υπόλοιπα IP δίκτυα. Τι παρατηρείτε;

**E3.23** Αν τυχόν υπάρχει πρόβλημα στην επικοινωνία και εμφανίζονται μηνύματα Request timed out σε ποιο επίπεδο εντοπίζεται;

**E3.24** Αν αλλάξετε μια IP Address εκτός του εύρους των έγκυρων host του subnet, βάσει του subnet mask που επιλέξατε, υπάρχει επικοινωνία με τους υπόλοιπους host; Σε ποιο επίπεδο δικτύου εντοπίζεται το πρόβλημα;