ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

Προγραμματισμός Δικτυακών Συσκευών

με τη χρήση του GNS3

Δρ. Αναστάσιος Χ. Πολίτης

Καθηγητής Εφαρμογών

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.

Δεκέμβριος 2016

Α΄ Έκδοση

Front page sketch by *John Ferrigan (www.johnferrigan.com)*

ΠΕΡΙΕΧΟΜΕΝΑ

1. Στόχοι

Αυτός ο εργαστηριακός οδηγός έχει δυο στόχους: την εξοικείωση των φοιτητών με το πρόγραμμα προσομοίωσης δικτύων GNS3 και την εκμάθηση των βασικών διαδικασιών προγραμματισμού δικτυακών συσκευών της εταιρίας Cisco.

Το πρόγραμμα GNS3 είναι ένας προσομοιωτής δικτύων ο οποίος παρέχεται ελεύθερα και αποτελεί σημαντικό εργαλείο για εκπαιδευτικούς σκοπούς. Χρησιμοποιείται ευρύτατα σε εργαστηριακά μαθήματα δικτύων υπολογιστών αλλά και στην προετοιμασία υποψηφίων για τις εξαιρετικά δημοφιλείς εξετάσεις πιστοποίησης CCENT / CCNA / CCNP / CCIE της εταιρίας Cisco.

Η εταιρία Cisco αποτελεί έναν από τους μεγαλύτερους κατασκευαστές δικτυακών συσκευών στον κόσμο και η πιστοποιημένη ικανότητα ρύθμισης των συσκευών αυτών αποτελεί σημαντικό επαγγελματικό εφόδιο για τους μηχανικούς δικτύων.

Το παρόν εγχειρίδιο δεν έχει γραφεί με στόχο την εξαντλητική ανάλυση των θεμάτων που παρουσιάζονται, ωστόσο, παρέχονται όλες οι απαραίτητες οδηγίες για την πλήρη ρύθμιση των δικτυακών συσκευών που εξετάζονται. Αφήνεται στην διάθεση του φοιτητή η βαθύτερη εξάσκηση του στα θέματα που αναλύονται στο εγχειρίδιο.

Φιλοδοξώντας να υπάρξουν νεότερες εκδόσεις του παρόντος εγχειριδίου με ακόμα περισσότερες και διαβαθμισμένου δείκτη δυσκολίας ασκήσεις πράξης στο μέλλον, επιζητείται κάθε καλοπροαίρετη πρόταση (ειδικά από τους φοιτητές του Τμήματος μας). Τέλος, είναι αυτονόητο ότι κάθε επισήμανση/παρατήρηση/εύρεση λαθών, είναι ευπρόσδεκτες από τους συγγραφείς.

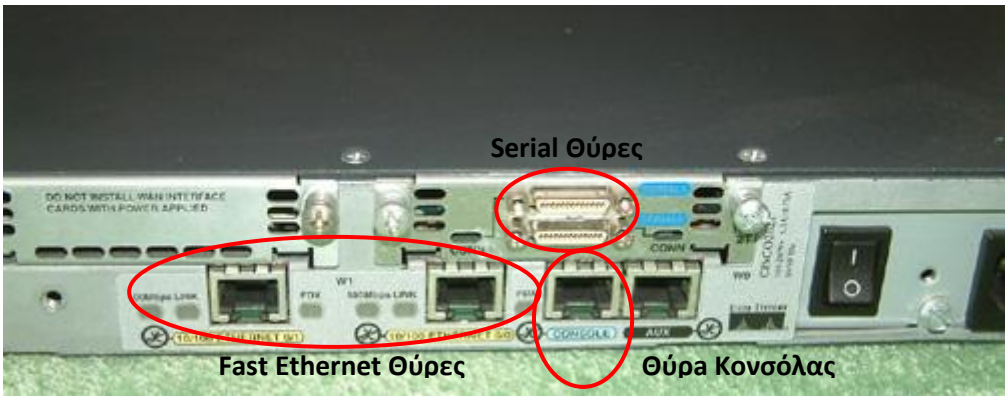
Αναστάσιος Χ. Πολίτης

Καθηγητής Εφαρμογών

2. Φυσική επισκόπηση συσκευών δρομολόγησης

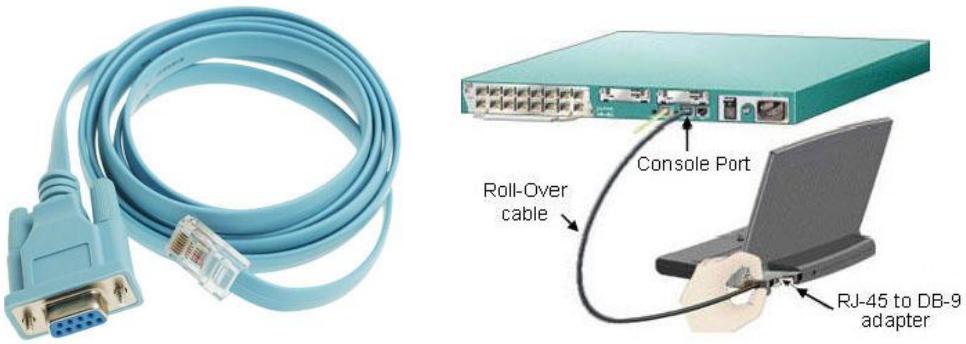
Ένας δρομολογητής είναι μια συσκευή η οποία εκτελεί την διαδικασία της IP δρομολόγησης. Πρόκειται για μια συσκευή τρίτου επιπέδου (Layer-3) η οποία είναι εξοπλισμένη με φυσικές διεπαφές διαφόρων τύπων. Ο στόχος της είναι να διασυνδέει δίκτυα (ή υποδίκτυα) μεταξύ τους.

Στην Εικόνα 1 φαίνεται η οπίσθια όψη ενός δρομολογητή 2621 της εταιρίας Cisco. Παρατηρείστε ότι διαθέτει διακόπτη ενεργοποίησης και μια σειρά από θύρες. Οι δικτυακές θύρες που διαθέτει ο συγκεκριμένος δρομολογητής είναι τύπου Fast Ethernet και οι Serial (Σειριακές). Επίσης, διαθέτει μια θύρα σύνδεσης εξωτερικού τερματικού. Η θύρα αυτή είναι η Θύρα Κονσόλας (Console) και σε αυτή συνδέεται ο διαχειριστής της συσκευής για να την ρυθμίσει τοπικά. Η θύρα Auxiliary μπορεί να χρησιμοποιηθεί για απομακρυσμένη σύνδεση μέσω modem (τηλεφωνική κλήση) στην συσκευή. Φυσικά, υπάρχει η δυνατότητα ρύθμισης των συσκευών μέσω telnet ή ssh αλλά αφού πρώτα γίνουν μια σειρά από βασικές ρυθμίσεις τοπικά (ή μέσω modem).



Εικόνα 1. Οπίσθια όψη ενός πραγματικού δρομολογητή 2621.

Ο διαχειριστής χρησιμοποιεί ένα ειδικό καλώδιο που ονομάζεται rollover cable το οποίο συνδέει τον δρομολογητή με το τερματικό του, όπως φαίνεται στην Εικόνα 2.



Εικόνα 2. Rollover cable και διασύνδεση τερματικού με δικτυακή συσκευή.

Στην Εικόνα 3 φαίνεται ένας δρομολογητής Cisco c1700 που διαθέτει το Εργαστήριο Δικτύων του Τμήματος Μηχανικών Πληροφορικής του οποίου το λογισμικό πρόκειται να χρησιμοποιηθεί στις εργαστηριακές ασκήσεις.

Εικόνα 3. Συσκευή δρομολόγησης Cisco c1700.

Παρατηρείστε ότι ο συγκεκριμένος δρομολογητής διαθέτει μια θύρα 10/100 Fast Ethernet και δυο θύρες WIC (WAN Interface Cards) Σειριακές (Serial). Επίσης, διαθέτει την θύρα Console και AUX για την ρύθμιση της συσκευής.

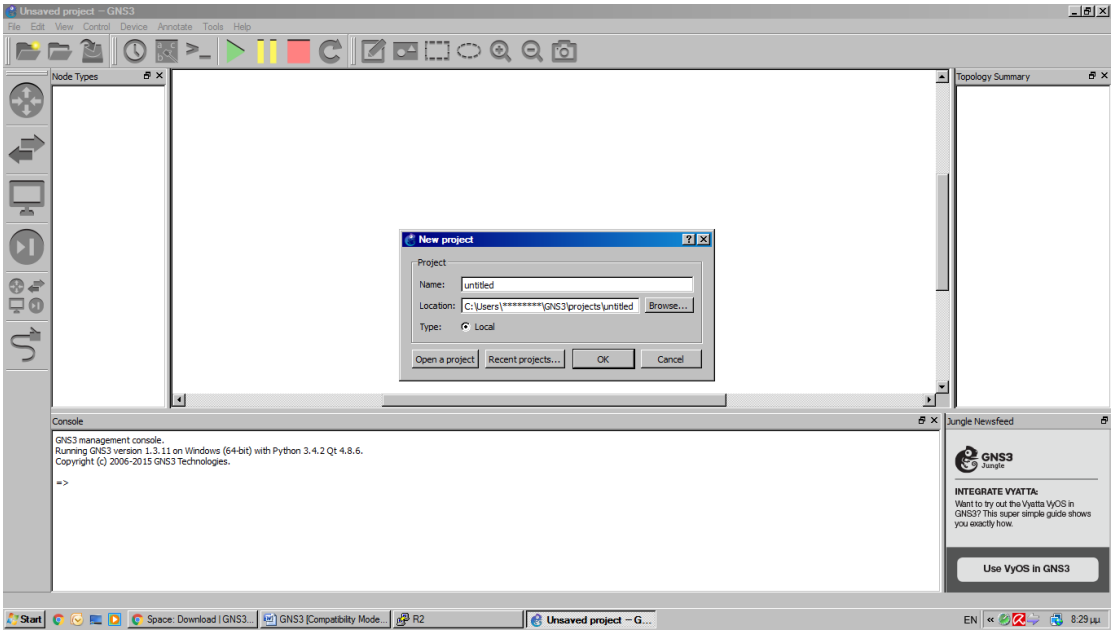
Αναλυτική περιγραφή για την φυσική διασύνδεση ενός τερματικού σταθμού στην συσκευή δρομολόγησης και πρόσβαση στο λειτουργικό της σύστημα βρίσκεται στο Παράρτημα Α.

3. Απόκτηση και εγκατάσταση του προγράμματος GNS3

Το πρόγραμμα GNS3 παρέχεται ελεύθερα από την ιστοσελίδα *http://www.gns3.com/*. Επισκεφθείτε την σελίδα και αναζητείστε το πρόγραμμα. Διατίθεται για όλα τα λειτουργικά συστήματα (Windows/Linux/MAC). Επιλέξτε το λειτουργικό σύστημα του υπολογιστή σας και ξεκινήστε την διαδικασία απόκτησης του προγράμματος. Θα σας ζητηθεί να δημιουργήσετε έναν λογαριασμό συμπληρώνοντας μια φόρμα με τα στοιχεία σας, και κατόπιν το πρόγραμμα διατίθεται προς απόκτηση. Την περίοδο συγγραφής του παρόντος εγχειριδίου, η τρέχουσα έκδοση του προγράμματος είναι η 1.3.11.

3.1 Βασικές ρυθμίσεις του προγράμματος

Αφού εγκαταστήσετε το πρόγραμμα και το ανοίξετε θα δείτε το περιβάλλον εργασίας που φαίνεται στην Εικόνα 4.

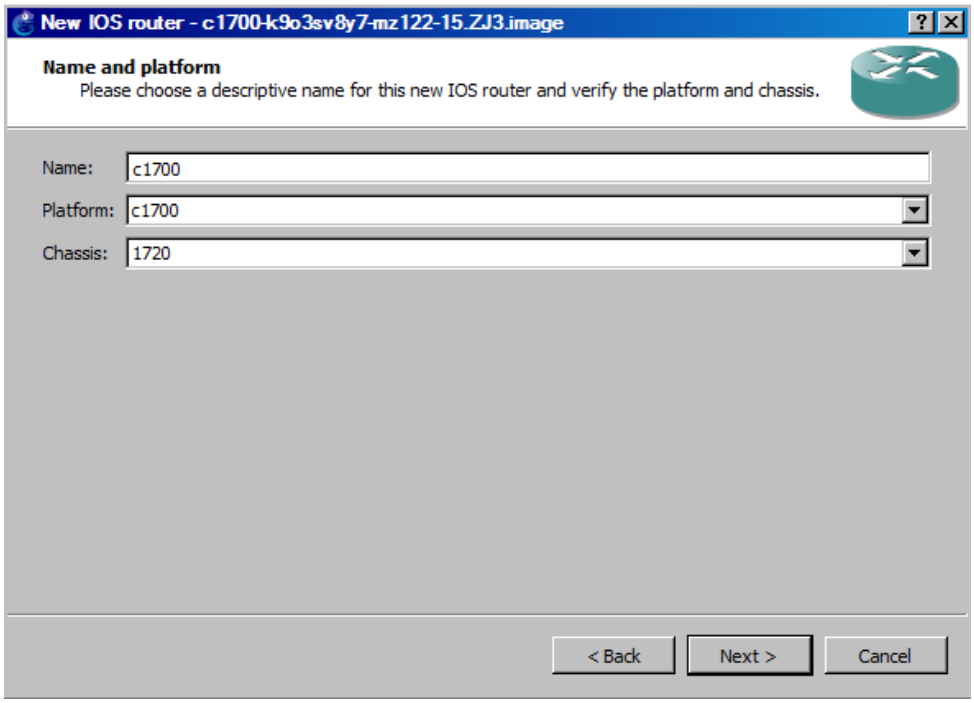


Εικόνα 4. *Το περιβάλλον εργασίας του GNS3.*

Το παράθυρο διαλόγου σας προτρέπει να δημιουργήσετε ένα νέο project με την ονομασία που επιθυμείτε. Σε αυτή τη φάση επιλέξτε ***Cancel***.

Το GNS3, ενώ έχει την δυνατότητα να προσομοιώνει συσκευές δρομολόγησης της εταιρίας Cisco, δεν περιλαμβάνει καμία από αυτές στις βιβλιοθήκες αντικειμένων του. Δίνει όμως την δυνατότητα να τις προσθέσει ο χρήστης, με την προϋπόθεση ότι διαθέτει ένα αντίγραφο (image) του λειτουργικού συστήματος που λειτουργεί σε αυτές. Το Εργαστήριο Δικτύων του Τμήματος Μηχανικών Πληροφορικής ΤΕ του ΤΕΙ Κεντρικής Μακεδονίας διαθέτει πραγματικές συσκευές δρομολόγησης της εταιρίας Cisco και μπορεί να σας παρέχει ένα αντίγραφο του λειτουργικού συστήματος αυτών των συσκευών για να το συμπεριλάβετε στο GNS3 για εκπαιδευτικούς σκοπούς.

Αποκτήστε το αντίγραφο του λειτουργικού συστήματος καθοδηγούμενοι από τον διδάσκοντα και εφαρμόστε το στον GNS3 επιλέγοντας από το μενού **Edit → Preferences → IOS Routers → New** επιλέξτε **Browse** και εντοπίστε το σημείο στον δίσκο που έχετε αποθηκεύσει το image. Επιλέξτε **Next** και αφήστε τις ονομασίες όπως φαίνονται στην Εικόνα 5.



Εικόνα 5. *Το παράθυρο με την ονομασία της συσκευής.*

Επιλέξτε **Next** και διατηρείστε την προεπιλογή για την διαθέσιμη μνήμη.

Επιλέξτε **Next** και θα εμφανιστεί ένα παράθυρο που θα αναφέρει τις διεπαφές που θα έχει η συσκευή στο slot 0.

Επιλέξτε **Next** και θα εμφανιστεί το παράθυρο με τις διεπαφές WAN (WAN Interface Cards – WIC). Στο wic 0 επιλέξτε WIC-2T (είναι ένα module με 2 σειριακές διεπαφές). Στο wic 1 επιλέξτε WIC-1ENET (ένα module με 1 απλή Ethernet διεπαφή).

Επιλέξτε **Next** και στο νέο παράθυρο πατήστε το κουμπί Idle-PC finder. Μετά από λίγο θα εμφανιστεί ένα μήνυμα με έναν δεκαεξαδικό αριθμό. Δεχθείτε το και πατήστε **Finish**. Εάν για οποιονδήποτε λόγο δεν σας εμφανίσει κάποιον δεκαεξαδικό αριθμό δοκιμάστε να εισάγετε χειροκίνητα τον 0x811c8000.

Σημείωση: *ο δεκαεξαδικός αριθμός που σας δίνεται δεν σας εγγυάται την σωστή λειτουργία. Απλά έχει λειτουργήσει σε ένα πλήθος υπολογιστικών συστημάτων Windows XP και παρατίθεται προς διευκόλυνση.*

Ένας καλός δικτυακός τόπος για το τι είναι τι Idle-PC και πως μπορεί να βρεθεί η τιμή του είναι ο παρακάτω:

http://www.smartpctricks.com/2014/05/calculate-idle-pc-value-in-gns3.html

Εάν όλα έχουν γίνει σωστά θα πρέπει να έχετε στη διάθεση σας έναν Cisco Router της σειράς c1700 σαν και αυτόν που φαίνεται στην Εικόνα 3.

Ένα τελευταίο βήμα που πρέπει να κάνετε πριν την χρήση του προγράμματος είναι να εντοπίστε το αρχείο *ios_base_startup_config.txt* το οποίο διαθέτει τις αρχικές βασικές ρυθμίσεις για το λειτουργικό σύστημα των δρομολογητών. Ανοίξτε το αρχείο με έναν editor (π.χ. στα Windows μπορείτε να χρησιμοποιήσετε το WordPad) και εντοπίστε την γραμμή `privilege level 15` και αφαιρέστε την όσες φορές υπάρχει. Κατόπιν αποθηκεύστε το αρχείο με την ίδια ονομασία και στο ίδιο σημείο του δίσκου.

Σημείωση: *Για τα Windows XP το αρχείο αυτό βρίσκεται στην διαδρομή C:\Documents and Settings**Το_Δικό_Σας_Όνομα**\Application Data\GNS3\base_configs η οποία είναι κρυφή (hidden) και θα πρέπει να κάνετε τις κατάλληλες ρυθμίσεις για να μπορέσετε να το εντοπίσετε. Για τα Windows 8: C:\Users**Το_Δικό_Σας_Όνομα**\AppData\Roaming\GNS3\base_configs*

3.2 Πρώτη γνωριμία με το πρόγραμμα

Ανοίξτε το GNS3, ονομάστε το project σας ***Basic_Conf***, επιλέξτε τον φάκελο στο τοπικό σας σύστημα που επιθυμείτε να το αποθηκεύσετε και πατήστε OK. Τώρα έχετε μεταφερθεί στον κενό χώρο εργασίας του GNS3. Τα διαθέσιμα προς χρήση αντικείμενα βρίσκονται στα αριστερά χωρισμένα σε κατηγορίες:

- οι *δρομολογητές (Routers)* επιλέγοντας το κουμπί  .
- οι *μεταγωγείς (Switches)* επιλέγοντας το κουμπί  .
- οι *τερματικοί κόμβοι (End devices)*επιλέγοντας το κουμπί  .
- *όλες οι διαθέσιμες συσκευές (All devices)* επιλέγοντας το κουμπί  .

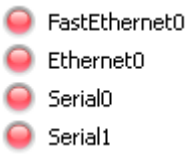
Επιλέξτε το κουμπί  και τοποθετείστε ένα αντικείμενο ***c1700 router***, ένα αντικείμενο ***ethernet switch*** και ένα αντικείμενο ***VPCS (Virtual PC Simulator)*** κάνοντας «drag and drop». Θα πρέπει να έχετε τις συσκευές που φαίνονται στην Εικόνα 6.

Εικόνα 6. Τα αντικείμενα του παραδείγματος **Basic_Conf**.

Το επόμενο βήμα θα είναι να συνδέσουμε τα αντικείμενα με φυσικές ζεύξεις. Επιθυμούμε να συνδέσουμε τον R1 με το SW1 και το SW1 με τον PC1. Για να κάνετε τις συνδέσεις επιλέξτε από την αριστερή μπάρα στον χώρο εργασίας το κουμπί  και κάντε μια φορά κλίκ στον έναν κόμβο και μια φορά κλίκ στον άλλο κόμβο που θέλετε να κάνετε την σύνδεση. Κάνοντας κλικ στον c1700 router θα πρέπει να δείτε ένα αναδυόμενο παράθυρο με κάποιες επιλογές οι οποίες φαίνονται στην Εικόνα 7. Πρόκειται για τις διαθέσιμες φυσικές διεπαφές του δρομολογητή:

- Μια *Fast Ethernet* διεπαφή.
- Μια *Ethernet* διεπαφή.
- Δύο *Serial* διεπαφές.

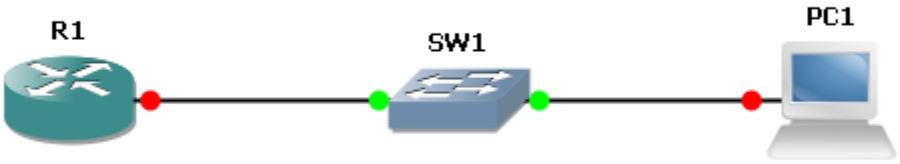
Οι διεπαφές αυτές έχουν μια αρίθμηση η οποία τις κάνει να ξεχωρίζουν στην περίπτωση που υπάρχουν πολλαπλές ίδιου τύπου (π.χ. *Serial0* και *Serial1)*.



Εικόνα 7. Οι διαθέσιμες διεπαφές του c1700.

Επιλέξτε την ***FastEthernet0*** στον c1700 και έπειτα κάντε κλικ στο SW1. Θα δείτε επίσης ένα αναδυόμενο παράθυρο με 8 διαθέσιμες διεπαφές. Πρόκειται για ένα switch με 8 θύρες (ports). Επιλέξτε την πρώτη θύρα του switch. Κατόπιν συνδέστε την δεύτερη διεπαφή του SW1 με τον PC1 (στον PC1 θα δείτε ότι έχετε μια επιλογή μόνο: *Ethernet0*).

Θα πρέπει να έχετε στην οθόνη σας το δίκτυο που φαίνεται στην Εικόνα 8.



Εικόνα 8. Το δίκτυο του παραδείγματος **Basic_Conf**.

Παρατηρείστε τις κόκκινες και πράσινες κουκίδες δίπλα από κάθε αντικείμενο. Η κόκκινη κουκίδα δηλώνει ότι το interface είναι απενεργοποιημένο και η πράσινη ότι είναι ενεργοποιημένο (τα interface των switch είναι πάντοτε ενεργοποιημένα στο GNS3 ως προεπιλογή).

Για να ενεργοποιήσετε τα interfaces όλων των κόμβων πατήστε το κουμπί  από τα διαθέσιμα κουμπιά που βρίσκονται κάτω από το μενού του προγράμματος. Για να τα

απενεργοποιήσετε πατήστε . Ενεργοποιήστε όλα τα interface των κόμβων του παραδείγματος σε αυτή τη φάση και αμέσως μετά κάντε διπλό κλικ στον R1.

Σημείωση: *Για να εμφανίσετε τις ονομασίες των διεπαφών στο GNS3 πατήστε το κουμπί . Δίπλα από κάθε διεπαφή που είναι συνδεδεμένη με καλώδιο θα σας εμφανίσει την ονομασία της.*

Κάνοντας διπλό κλικ στον R1 μεταφέρεστε στο λειτουργικό του σύστημα το οποίο ονομάζεται IOS και αντικρύζετε αυτό που θα βλέπατε σε έναν πραγματικό δρομολογητή c1700 εάν είχατε κάνει την φυσική συνδεσμολογία στην θύρα console με ένα rollover cable.

Κλείστε το παράθυρο που ανοίξατε κάνοντας διπλό κλικ στον R1 και κάντε διπλό κλικ στον PC1. Ο PC1 είναι ένα αντικείμενο VPCS το οποίο προσομοιώνει ένα πραγματικό προσωπικό υπολογιστή (PC). Ωστόσο, διαθέτει την δικιά του συλλογή εντολών με ορισμένες από τις οποίες θα πρέπει να εξοικειωθείτε. Το παράθυρο γραμμής εντολών που ανοίξατε στον PC1 μοιάζει (αλλά διαφέρει σε πολλά σημεία) με αυτό του MS-DOS παραθύρου που διαθέτει το λειτουργικό σύστημα των MS-Windows.

Πληκτρολογήστε στο prompt **?** και θα σας εμφανιστούν οι διαθέσιμες εντολές ρυθμίσεων που μπορούν να γίνουν στον κόμβο (Εικόνα 9).

```
PC1> ?

?                       Print help
! COMMAND [ARG ...]     Invoke an OS COMMAND with optional ARG(s)
arp                       Shortcut for: show arp. Show arp table
clear ARG               Clear IPv4/IPv6, arp/neighbor cache, command history
dhcp [OPTION]           Shortcut for: ip dhcp. Get IPv4 address via DHCP
disconnect              Exit the telnet session (daemon mode)
echo TEXT               Display TEXT in output. See also  set echo ?
help                    Print help
history                 Shortcut for: show history. List the command history
ip ARG ... [OPTION]     Configure the current VPC's IP settings. See ip ?
load [FILENAME]         Load the configuration/script from the file FILENAME
ping HOST [OPTION ...]  Ping HOST with ICMP (default) or TCP/UDP. See ping ?
quit                    Quit program
relay ARG ...           Configure packet relay between UDP ports. See relay ?
rlogin [ip] port        Telnet to port on host at ip (relative to host PC)
save [FILENAME]         Save the configuration to the file FILENAME
set ARG ...             Set VPC name and other options. Try set ?
show [ARG ...]          Print the information of VPCs (default). See show ?
sleep [seconds] [TEXT]  Print TEXT and pause running script for seconds
trace HOST [OPTION ...] Print the path packets take to network HOST
version                 Shortcut for: show version

To get command syntax help, please enter '?' as an argument of the command.

PC1>
```

Εικόνα 9. Κονσόλα του κόμβου PC1.

Μερικές από τις εντολές με τις οποίες θα πρέπει να εξοικειωθείτε γιατί θα χρησιμοποιηθούν στις μετέπειτα ασκήσεις είναι:

- `ip`
- `dhcp`
- `ping`
- `trace`
- `save`

- `load`
- `show`

Κάποιες από τις εντολές μπορεί να σας είναι ήδη γνωστές (π.χ. η ping) από άλλα εργαστηριακά μαθήματα δικτύων και κάποιες θα αναλυθούν στη συνέχεια. Μπορείτε να δείτε την βοηθητική περιγραφή των εντολών αυτών γράφοντας στην κονσόλα την επιθυμητή εντολή ακολουθούμενη από το σύμβολο **?.** Για παράδειγμα μπορούμε να εμφανίσουμε την βοηθητική περιγραφή της εντολής **`ip`**:

```
PC1> ip ?
ip ARG ... [OPTION]
  Configure the current VPC's IP settings
    ARG ...:
    address [mask] [gateway]
    address [gateway] [mask]
                    Set the VPC's ip, default gateway ip and network mask
                    Default IPv4 mask is /24, IPv6 is /64. Example:
                    ip 10.1.1.70/26 10.1.1.65 set the VPC's ip to 10.1.1.70,
                    the gateway to 10.1.1.65, the netmask to 255.255.255.192.
                    In tap mode, the ip of the tapx is the maximum host ID
                    of the subnet. In the example above the tapx ip would be
                    10.1.1.126
                    mask may be written as /26, 26 or 255.255.255.192
    auto            Attempt to obtain IPv6 address, mask and gateway using SLAAC
    dhcp [OPTION]   Attempt to obtain IPv4 address, mask, gateway, DNS via DHCP
          -d          Show DHCP packet decode
          -r          Renew DHCP lease
          -x          Release DHCP lease
    dns ip          Set DNS server ip, delete if ip is '0'
    domain NAME     Set local domain name to NAME
```

Διαβάζοντας την πρώτη γραμμή της παραπάνω εξόδου μπορούμε να αντιληφθούμε ότι πρόκειται για την εντολή ρύθμισης των IP παραμέτρων του κόμβου (IP διεύθυνση, μάσκα υποδικτύωσης, προεπιλεγμένη πύλη κλπ). Πρόκειται δηλαδή για μια πολύ σημαντική εντολή την οποία θα χρησιμοποιήσουμε ευρύτατα στις ασκήσεις που ακολουθούν.

Επιθυμούμε να ρυθμίσουμε τον PC1 με τις εξής IP παραμέτρους:

- IP Address: 185.100.100.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 185.100.100.1

Δώστε την παρακάτω εντολή στην κονσόλα του PC1:

```
PC1> ip 185.100.100.2 255.255.255.0 185.100.100.1
Checking for duplicate address...
PC1 : 185.100.100.2 255.255.255.0 gateway 185.100.100.1
```

Θα πρέπει να σημειώσουμε ότι η IP διεύθυνση της προεπιλεγμένης πύλης (Default Gateway) θα ανήκει στο interface **f0** του R1 αλλά αυτό δεν έχει ρυθμιστεί ακόμα και θα γίνει στην επόμενη παράγραφο.

Σε αυτή τη φάση θα πρέπει να αναφερθούμε και στις εντολές `save` και `load`: στις εργαστηριακές ασκήσεις που θα κάνουμε στη συνέχεια, αφού κάνουμε κάποιες ρυθμίσεις στους κόμβους VPCS θα πρέπει να αποθηκεύσουμε τις ρυθμίσεις αυτές γιατί εάν κλείσουμε το GNS3 ή απενεργοποιήσουμε την συσκευή (και μετά την ενεργοποιήσουμε) οι ρυθμίσεις χάνονται και θα πρέπει να ξαναγίνουν εκ νέου.

Για την αποθήκευση των ρυθμίσεων που έχουμε κάνει δίνουμε την εντολή: `save <filename>` στην κονσόλα του VPCS. Συνηθίζουμε να χρησιμοποιούμε την ονομασία του κόμβου για το filename για να είναι εύκολή η ανάκτηση των ρυθμίσεων. Έτσι δίνουμε:

```
PC1> save pc1
Saving startup configuration to pc1.vpc
.  done
```

και οι τρέχουσες ρυθμίσεις του κόμβου PC1 αποθηκεύονται στο αρχείο με την ονομασία `pc1.vpc`.

Όταν ανοίξουμε ένα project και θέλουμε να ανακτήσουμε τις ρυθμίσεις που είχαμε αποθηκεύσει για κάποιον VPCS μπορούμε να δώσουμε:

```
PC1> load pc1

Executing the file "pc1"
```

Ένα καλό tutorial για τις δυνατότητες των VPCS και οι ρυθμίσεις που υποστηρίζονται σε αυτούς βρίσκεται στην [1].

4. Βασικές ρυθμίσεις ενός δρομολογητή

Ένας δρομολογητής συνοδεύεται από ένα λειτουργικό σύστημα το οποίο είναι υπεύθυνο να υλοποιεί, μεταξύ άλλων, τα επικοινωνιακά πρωτόκολλα και να παρέχει ασφάλεια στην πρόσβαση στο λογισμικό της συσκευής. Το λογισμικό το οποίο συνοδεύει τους δρομολογητές της εταιρίας Cisco ονομάζεται *Cisco Internetwork Operating System (IOS)*, όπως αναφέρθηκε σε προηγούμενη παράγραφο. Το IOS διεθέτει ένα μεγάλο πλήθος εντολών (ανάλογα με την έκδοση του) το οποίο περιλαμβάνεται στο image το οποίο ενεργοποιήσατε στο GNS3.

4.1 User και Privileged Mode

Το IOS έχει δύο βασικές καταστάσεις λειτουργίας: *user mode* και *privileged mode*. Η κατάσταση στην οποία βρισκόμαστε υποδηλώνεται από το σήμα του prompt. Το σήμα "**>**" υποδηλώνει την **user mode** και το σήμα "**#**" υποδηλώνει την **privileged mode**. Στην πρώτη κατάσταση είμαστε σε θέση να επισκοπήσουμε ορισμένες από τις ρυθμίσεις που έχουν γίνει στην συσκευή, ενώ στην δεύτερη κατάσταση μπορούμε να εκτελέσουμε όλες τις ρυθμίσεις.

Σημείωση: *εάν δεν έχετε κάνει την τελευταία ρύθμιση που αναφέρεται στην παράγραφο 3.1 κατά την σύνδεση σας στην συσκευή δρομολόγησης θα μεταφέρεστε απευθείας στην κατάσταση διαχείρισης.*

Αφού μεταφερθείτε στο λογισμικό του δρομολογητή R1 (κάνοντας διπλό κλίκ επάνω του) μπορείτε να μεταφερθείτε από την κατάσταση user στην κατάσταση privileged και πάλι πίσω δίνοντας:

```
R1 con0 is now available

Press RETURN to get started.

R1>enable

R1#disable

R1>
```

Για έξοδο από οποιαδήποτε κατάσταση δίνουμε:

```
R1>logout

R1 Con0 is now available

Press RETURN to get started!
```

Όταν βρισκόμαστε στην privileged mode μπορούμε να μεταβούμε σε **κατάσταση ρυθμίσεων** όπως παρακάτω:

```
R1>enable

R1#config terminal

Enter configuration commands, one per line.  End with CNTL/Z

R1(config)#exit
```

Σημείωση: *Το IOS μας δίνει την δυνατότητα να γράφουμε μέρος των εντολών ή να τις συμπληρώνουμε. Για παράδειγμα εάν αντί για* `enable` *στην κατάσταση* user *γράψετε* `en` *το IOS θα την αναγνωρίσει και θα σας μεταφέρει στην κατάσταση* privileged. *Εάν γράψετε* `en` *και πατήσετε το πλήκτρο* tab *στο πληκτρολόγιο το IOS θα συμπληρώσει την εντολή (δεδομένου ότι δεν υπάρχει άλλη εντολή που ξεκινά με τα ίδια γράμματα). Επίσης, αν γράψετε* `en?` *το IOS θα σας εμφανίσει όλες τις εντολές που ξεκινάνε με τα γράμματα* `en`.

4.2 Πληροφορίες για την συσκευή

Σε μια πρώτη γνωριμία με την συσκευή και το IOS που την συνοδεύει θα ήταν καλό να συλλέξουμε πληροφορίες για τις δυνατότητες και τα χαρακτηριστικά της ίδια της συσκευής. Δώστε την παρακάτω εντολή στον R1 του παραδείγματος **Basic_Conf**:

```
R1#show version

Cisco IOS Software, C1700 Software (C1700-ADVIPSERVICESK9-M), Version
12.4(15)T11, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2009 by Cisco Systems, Inc.

Compiled Thu 29-Oct-09 08:57 by prod_rel_team

ROM: ROMMON Emulation Microcode

ROM: C1700 Software (C1700-ADVIPSERVICESK9-M), Version 12.4(15)T11, RELEASE
SOFTWARE (fc2)

R1 uptime is 18 minutes

System returned to ROM by unknown reload cause - suspect
boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19

System image file is "tftp://255.255.255.255/unknown"

This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not implythird-party authority to
import, export, distribute or use encryption. Importers, exporters,
distributors and users are responsible for compliance with U.S. and local
country laws. By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
```

```
export@cisco.com.

Cisco 1720 (MPC860T) processor (revision 0x202) with 139264K/8192K bytes of
memory.

Processor board ID FTX0945W0MY (4279256517), with hardware revision 0000

MPC860T processor: part number 0, mask 0

1 Ethernet interface

1 FastEthernet interface

2 Serial(sync/async) interfaces

128K bytes of NVRAM.

4096K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Από την παραπάνω έξοδο μπορούμε να συλλέξουμε αρκετές πληροφορίες για την συγκεκριμένη συσκευή, όπως: ο αριθμός των φυσικών διεπαφών που έχει, η έκδοση του IOS που έχει εγκατεστημένη, ο χρόνος λειτουργίας της, το μέγεθος της μνήμης της (ROM και RAM) κ.α.

Σημείωση: *Η εντολή `show` είναι μια πολύ χρήσιμη εντολή την οποία θα την χρησιμοποιήσουμε αρκετές φορές. Η έξοδος της εντολής ποικίλλει ανάλογα με το τι την ακολουθεί: στο προηγούμενο παράδειγμα η λέξη `version` ορίζει ότι η έξοδος της εντολής `show` θα περιλαμβάνει την έκδοση του IOS της συσκευής και των βασικών της χαρακτηριστικών. Όπως θα δούμε στη συνέχεια η ίδια εντολή χρησιμοποιείται για να μας δείξει λεπτομέρειες των διεπαφών, τις λεπτομέρειες του πίνακα δρομολόγησης κλπ.*

4.3 Ρυθμίσεις ασφαλείας

Για την ασφάλεια των Cisco δρομολογητών υπάρχουν πέντε passwords:

- Console.
- Auxiliary.
- Telnet (VTY-Virtual TeletYpe).
- Enable password.
- Secret password.

4.3.1 Console Password

Το Console password χρησιμοποιείται για να προστατεύσει την φυσική πρόσβαση στην κονσόλα της συσκευής. Να μην μπορεί κανείς, δηλαδή, να συνδεθεί με ένα rollover cable και να έχει πρόσβαση στο IOS χωρίς την προστασία ενός

συνθηματικού (εκτός από τον διαχειριστή προφανώς). Για να το ενεργοποιήσετε δώστε τις παρακάτω εντολές:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z

R1(config)#line console 0

R1(config-line)#password console

R1(config-line)#login
```

Στο παράδειγμα θέσαμε το συνθηματικό να είναι η λέξη «console». Μπορείτε να ελέγξετε την ορθή ενεργοποίηση του συνθηματικού αφήνοντας τις καταστάσεις ρυθμίσεων γράφοντας διαδοχικές εντολές `exit`, όπως παρακάτω:

```
R1(config-line)#exit

R1(config)#exit

R1#exit
```

Στη συνέχεια πατήστε enter και θα δείτε ότι θα σας ζητηθεί να εισάγετε ένα συνθηματικό.

Σημείωση: *Όταν θα γράφετε το συνθηματικό τα γράμματα που θα πληκτρολογείτε δεν θα φαίνονται στην οθόνη για λόγους ασφαλείας αλλά θα λαμβάνονται υπόψιν από το IOS.*

4.3.2 Auxiliary Password

Το Auxiliary password είναι ένα συνθηματικό που προστατεύει την απομακρυσμένη πρόσβαση μέσω modem στην συσκευή δρομολόγησης χρησιμοποιώντας την θύρα AUX. Η διαδικασία ενεργοποίησης του Auxiliary password είναι πανομοιότυπη με αυτή του Console password:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z

R1(config)#line aux 0

R1(config-line)#password auxiliary

R1(config-line)#login
```

4.3.3 Telnet Password

Το Telnet password προστατεύει την απομακρυσμένη πρόσβαση στην συσκευή με τη χρήση της εφαρμογής telnet. Η ενεργοποίηση του γίνεται όπως παρακάτω:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z

R1(config)#line vty 0 15

R1(config-line)#password telnet

R1(config-line)#login
```

Η συγκεκριμένη συσκευή δύναται να διαχειριστεί 16 ταυτόχρονες συνδέσεις telnet (0-15). Για όλες αυτές τις συνδέσεις ορίσαμε ότι θα πρέπει να δοθεί το συνθηματικό «telnet».

4.3.4 Enable Password

Πρόκειται για το συνθηματικό που προστατεύει την μετακίνηση από την κατάσταση user στην κατάσταση privileged. Επειδή για να μεταφερθούμε στην κατάσταση privileged από την κατάσταση user δίνουμε την εντολή `enable` γι' αυτό και το password αυτό ονομάζεται enable password:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#enable password abcd
```

Εδώ το συνθηματικό που ορίσαμε είναι η ακολουθία γραμμάτων «abcd». Το μειονέκτημα του συνθηματικού αυτού είναι ότι το συνθηματικό δεν είναι κρυπτογραφημένο.

4.3.5 Enable Secret

Ο σκοπός του enable secret password είναι ίδιος με αυτόν του enable password: να προστατεύσει την μεταπήδηση από την κατάσταση user στην κατάσταση privileged. Η διαφορά είναι ότι το συνθηματικό είναι αυτή τη φορά κρυπτογραφημένο:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#enable secret crypto
```

4.4 Ρύθμιση των δικτυακών διεπαφών

Η ρύθμιση των φυσικών διεπαφών ενός δρομολογητή αποτελεί μια από τις πιο σημαντικές ρυθμίσεις που πρέπει να εκτελέσει ένας διαχειριστής. Επιπλέον, οι δικτυακές ρυθμίσεις πρέπει να είναι απόλυτα ακριβείς προκειμένου να καταστήσουν εφικτή την επικοινωνία μεταξύ συσκευών.

Μια πρώτη πληροφόρηση για τον τύπο και το πλήθος των διεπαφών που διαθέτει η συσκευή που επιθυμούμε να ρυθμίσουμε μας έδωσε η εντολή `show version` που είδαμε στην παράγραφο 3.2. Μια πιο εξειδικευμένη εντολή είναι η `show int` της οποίας η έξοδος εμφανίζει τις παρακάτω πληροφορίες:

```
R1#show int
Ethernet0 is administratively down, line protocol is down
Hardware is PQUICC Ethernet, address is d001.1b88.1000 (bia d001.1b88.1000)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10BaseT
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
--More--
```

Με την εντολή αυτή εμφανίζονται περισσότερες λεπτομέριες για τις διεπαφές της συσκευής. Με μια πρώτη ματιά μπορούμε να δούμε ότι η συγκεκριμένη διεπαφή είναι ανενεργή (administratively down), η MAC διεύθυνση της είναι d001.1b88.1000, το MTU της είναι 1500 bytes, η «ταχύτητα» της είναι 10 Mbps κ.α. Πατώντας enter μεταφέρεστε γραμμή-γραμμή και πατώντας space μεταφέρεστε ανά σελίδα. Η έξοδος της συγκεκριμένης εντολής είναι αρκετά μεγάλη (περιλαμβάνει όλες τις διαθέσιμες διεπαφές της συσκευής) γι' αυτό και δεν την παραθέτουμε ολόκληρη. Μπορούμε να εμφανίσουμε τα χαρακτηριστικά μόνο μιας συγκεκριμένης διεπαφής, π.χ. της s0, δίνοντας `show int s0`.

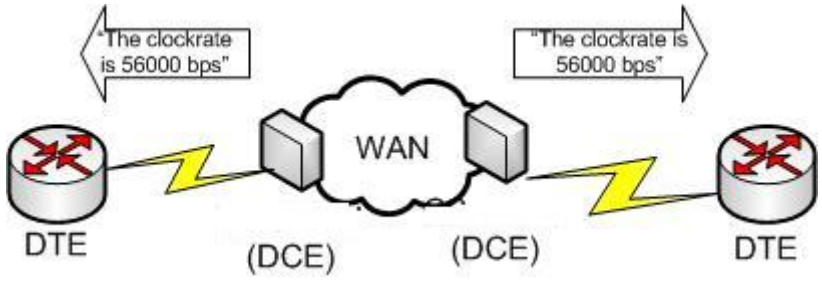
4.4.1 Στατική απόδοση IP παραμέτρων

Εάν επιυθυμούμε να δώσουμε μια συγκεκριμένη IP διεύθυνση σε μια διεπαφή του δρομολογητή πρέπει σε πρώτη φάση να γνωρίζουμε την ονομασία της διεπαφής. Κατόπιν δίνουμε τις παρακάτω εντολές. Εμείς επιθυμούμε να ρυθμίσουμε την διεπαφή **f0** οποία είναι συνδεδεμένη με το SW1:

```
R1(config)#int f0

R1(config-if)#ip address 185.100.100.1 255.255.255.0

R1(config-if)#description link to SW1

R1(config-if)#no shut

*Mar 1 00:30:53.019: %LINK-3-UPDOWN: Interface FastEthernet0, changed state
to up

*Mar 1 00:30:54.019: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0, changed state to up
```

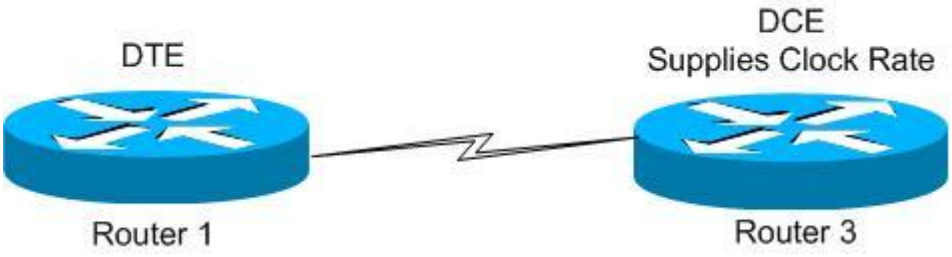
Αρχικά δηλώνουμε το interface που επιθυμούμε να ρυθμίσουμε, κατόπιν ορίζουμε την IP διεύθυνση και την subnet mask και τέλος ενεργοποιούμε την διεπαφή. Ας σημειωθεί εδώ ότι αυτή είναι η αλληλουχία των εντολών για όλα τα interfaces τύπου Ethernet. Η εντολή description είναι προαιρετική και δίνει μια περιγραφεί στην διεπαφή η οποία θα φαίνεται στην έξοδο της εντολής `show int`.

Πολλοί δρομολογητές διαθέτουν σειρικά interfaces (όπως ο 1720 που χρησιμοποιούμε) τα οποία συνήθως χρησιμοποιούνται για την διασύνδεση τους με ειδικές διατάξεις που τοποθετεί ο *Πάροχος Υπηρεσιών Διαδικτύου (Internet Service Provider)* στις εγκαταστάσεις του πελάτη και ονομάζονται *Data Circuit-terminating Equipment (DCE)*. Η διάταξη αυτή παρέχει πρόσβαση στο δίκτυο του παροχέα (WAN) και ορίζει την ταχύτητα της σύνδεσης η οποία ονομάζεται *ρυθμός ρολογιού (clock rate)*. Ο ρυθμός αυτός παρέχει επίσης συχρονισμό μεταξύ των συσκευών και μετριέται σε *bits per second*. Ο δρομολογητής του πελάτη ονομάζεται *Data Terminal Equipment (DTE)*. Οι δρομολογητές, γενικά, είναι DTE διατάξεις όπως και οι προσωπικοί υπολογιστές (PC). Η διασύνδεση των DCE και DTE συσκευών φαίνεται στην Εικόνα 10.



Εικόνα 10. Διασύνδεση DTE και DCE διατάξεων.

Προκειμένου να προσομοιώσουμε WAN ζεύξεις μεταξύ δρομολογητών στο εργαλείο προσομοίωσης μπορούμε να συνδέσουμε δύο δρομολογητές απευθείας με μια *Σημειακή (Point-to-Point)* σειριακή ζεύξη όπως φαίνεται στην Εικόνα 11. Η σύνδεση αυτή χρησιμοποιεί σημειακά πρωτόκολλα όπως το PPP, το SLIP ή το HDLC και ο ένας από τους δύο δρομολογητές αναλαμβάνει τον ρόλο του DCE ενώ ο άλλος αυτόν του DTE.



Εικόνα 11. Σημειακή σειριακή σύνδεση δύο δρομολογητών.

Ο δρομολογητής που θα αναλάβει τον ρόλο του DCE θα πρέπει να ρυθμιστεί για να παρέχει το clock rate της ζεύξης. Ενώ στην πραγματικότητα θα πρέπει να κάνουμε συγκεκριμένες ρυθμίσεις για τις σειριακές ζεύξεις, στο GNS3 οι ρυθμίσεις αυτές μπορούν να παραληφθούν. Απλά ρυθμίζουμε την IP διεύθυνση / μάσκα της διεπαφής και την ενεργοποιούμε.

4.4.2 Απόδοση IP παραμέτρων μέσω DHCP

Για την αυτόματη απόδοση IP παραμέτρων στους κόμβους ενός LAN μπορεί να χρησιμοποιηθεί το *DHCP πρωτόκολλο (Dynamic Host Configuration Protocol)* [2]. Το πρωτόκολλο αυτό χρησιμοποιείται ευρύτατα σε δίκτυα επιχειρήσεων, δίκτυα πανεπιστημιακών ιδρυμάτων αλλά και σε οικιακά δίκτυα για την δυναμική απόδοση IP παραμέτρων σε κόμβους.

Η υπηρεσία DHCP μπορεί να παρέχεται από έναν DHCP server στο δίκτυο ή ακόμα από έναν δρομολογητή που λειτουργεί στα όρια ενός LAN ο οποίος μπορεί να ρυθμιστεί ως DHCP server έτσι ώστε οι κόμβοι του LAN να αποκτούν τις IP παραμέτρους τους από τον δρομολογητή.

Η αλληλουχία των πακέτων που ανταλλάσσονται μεταξύ DHCP client (κόμβος-host) και DHCP server (δρομολογητής ή εξυπηρετητής) φαίνονται στην Εικόνα 12. Οι

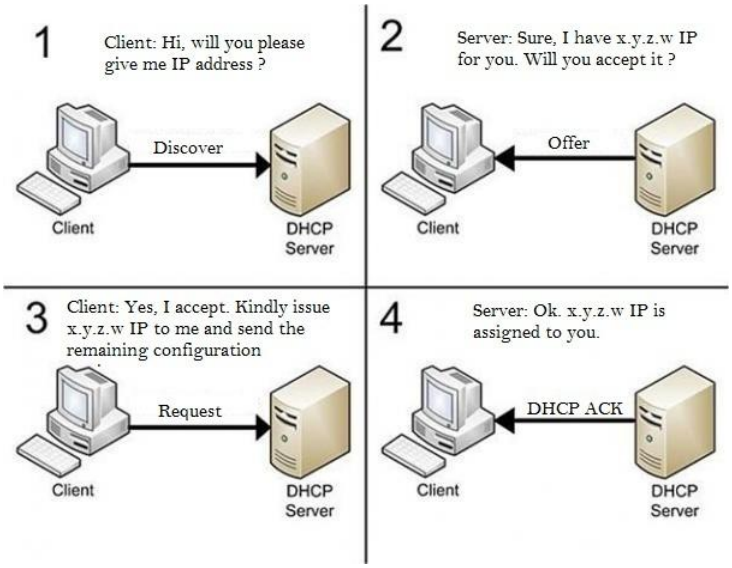
αλληλουχία αυτή καλείται πολλές φορές με τα αρχικά των λέξεων που περιγράφουν κάθε πακέτο που ανταλλάσσεται: *Discover-Offer-Request-Acknowledgment (DORA).*

- **Discover:** είναι το πρώτο πακέτο της DORA ακολουθίας που μεταδίδεται από τον DHCP client για να ανακαλύψει έναν διαθέσιμο DHCP server. Δεδομένου ότι ο client δεν διαθέτει ακόμα IP διεύθυνση τοποθετεί ως IP διεύθυνση αποστολέα την 0.0.0.0. Μπορεί να αναγνωριστεί όμως στο τοπικό δίκτυο από την MAC διεύθυνση του. Μη γνωρίζωντας ποιος είναι ο DHCP server στο δίκτυο, τοποθετεί ως IP διεύθυνση προορισμού την 255.255.255.255 (IP broadcast) και την ff:ff:ff:ff:ff:ff (MAC broadcast) ως MAC διεύθυνση παραλήπτη.

- **Offer:** μεταδίδεται από τον DHCP server ως προσφορά προς τον client δηλώνοντας τις IP παραμέτρους.

- **Request:** μεταδίδεται από τον DHCP client προς τον server ως αίτημα για την δέσμευση της IP διεύθυνσης που περιλαμβανόταν στο Offer μήνυμα.

- **Acknowledgment:** μεταδίδεται από τον DHCP server προς τον client ως απόκριση στο αίτημα του client και ανάθεση των IP παραμέτρων (IP address, Subnet Mask, Default router, DNS server).



Εικόνα 12. Η αλληλουχία των πακέτων που ανταλλάσσονται με το DHCP.

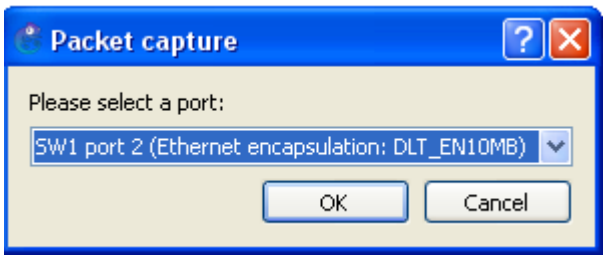
Για τη ρύθμιση του δρομολογητή R1 ως DHCP server ακολουθείστε την παρακάτω διαδικασία:

```
R1(config)#ip dhcp pool Mypool

R1(dhcp-config)#network 185.100.100.0 255.255.255.0

R1(dhcp-config)#default-router 185.100.100.1
```

```
R1(dhcp-config)#lease 0 6 0

R1(dhcp-config)#exit

R1(config)#ip dhcp excluded-address 185.100.100.1
```

Αρχικά ορίζουμε μια ονομασία για την τράπεζα διαθέσιμων IP διευθύνσεων. Στο παράδειγμα την ονομάσαμε «Mypool». Κατόπιν ορίζουμε την IP διεύθυνση δικτύου που θα χρησιμοποιηθεί μαζί με την μάσκα. Ορίζεται η IP της προκαθορισμένης πύλης (default router) και η διάρκεια ανάθεσης των δικτυακών παραμέτρων (0 ημέρες, 6 ώρες, 0 λεπτά). Τέλος, εξαιρείται από την τράπεζα των διαθέσιμων IP διευθύνσεων η διεύθυνση που έχει αποδοθεί στην προκαθορισμένη πύλη.

Μπορούμε να δούμε την αλληλουχία DORA επιλέγοντας την ζεύξη που συνδέει τον PC1 με το switch και εκτελώντας **δεξί κλίκ→start capture**. Θα σας εμφανίσει το παράθυρο που φαίνεται στην Εικόνα 13 και αναφέρεται στην επιλογή θύρας.



Εικόνα 13. Επιλογή θύρας για την εκκίνηση καταγραφής πακέτων.

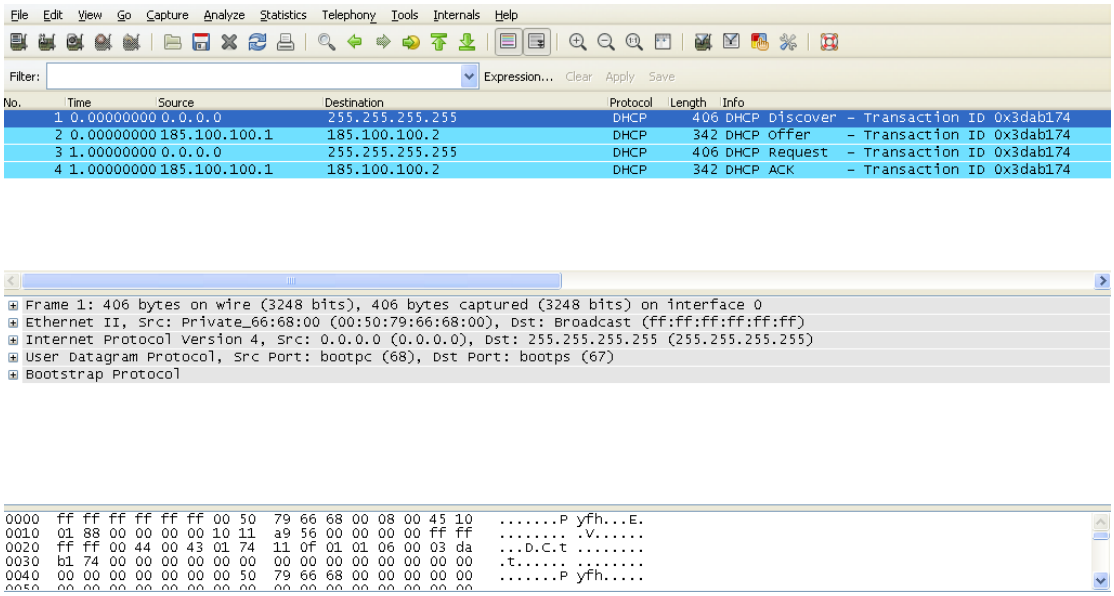
Επιλέξτε την προεπιλογή η οποία αναφέρει ότι θα εκκινήσει η καταγραφή πακέτων στην θύρα port 2 του switch και πατήστε OK. Κατόπιν, θα ανοίξει ο αναλυτής πρωτοκόλλων Wireshark. Φυσικά θα πρέπει να ρυθμίσουμε τον κόμβο-host (PC1) να λαμβάνει αυτόματα (και όχι στατικά) τις IP παραμέτρους. Αυτό μπορεί να γίνει στους VPCS του GNS3 ως εξής:

```
PC1> dhcp
DDORA IP 185.100.100.2/24 GW 185.100.100.1
PC1> show
NAME       IP/MASK              GATEWAY                MAC
PC1     185.100.100.2/24        185.100.100.1       00:50:79:66:68:00
```

Δίνοντας την εντολή `dhcp` στον PC1 τον προκαλούμε να εκκινήσει την διαδικασία DORA αναζητώντας τον DHCP server. Βλέπουμε ότι οι ρυθμίσεις έγιναν αυτόματα στον PC1.

Σημείωση: *Η MAC διεύθυνση του PC1 που θα τοποθετήσετε μπορεί να διαφέρει από αυτήν που φαίνεται στο παραπάνω παράδειγμα.*

Το εργαλείο Wireshark θα εμφανίσει την ανταλλαγή μηνυμάτων της διαδικασίας DORA, όπως φαίνεται στην Εικόνα 14.



Εικόνα 14. Η καταγραφή της διαδικασίας DHCP με το Wireshark.

Από την παραπάνω καταγραφή μπόρούμε να παρατηρήσουμε ότι το DHCP πρωτόκολλο ουσιαστικά χρησιμοποιεί το (παλαιότερο) *Bootstrap Protocol (BOOTP)* [3], [4] το οποίο έχει ενισχυθεί με τους νεότερους μηχανισμούς του DHCP. Επίσης, παρατηρείστε ότι το πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιείται από το DHCP είναι το *User Datagram Protocol (UDP)* και οι UDP θύρες (UDP ports) που έχουν ανατεθεί για αυτή διαδικασία είναι η 68 για τον DHCP client και η 67 για τον DHCP server.

Από την καταγραφή φαίνεται ότι το πακέτο DHCP Discover αποστέλλεται από τον client με IP διεύθυνση αποστολέα την *0.0.0.0*. Επιλέγεται αυτή η IP διεύθυνση διότι ο client δεν έχει ακόμα κάποια IP διεύθυνση. Ως IP διεύθυνση προορισμού είναι η *255.255.255.255* η οποία είναι μια broadcast διεύθυνση και η οποία δηλώνει ότι το συγκεκριμένο πακέτο έχει προορισμό όλους του κόμβους του δικτύου. Αναλύοντας τον *Ethernet header* παρατηρούμε ότι ως MAC διεύθυνση αποστολέα έχει τοποθετηθεί η MAC διεύθυνση του client (η οποία είναι η *00:50:79:66:68:00* για το παράδειγμα του βιβλίου) και ως MAC διεύθυνση προορισμού η *ff:ff:ff:ff:ff:ff* η οποία επίσης είναι μια broadcast διεύθυνση.

Στη συνέχεια, ελέγχοντας τον *Bootstrap header* εντοπίστε ένα πεδίο με ονομασία *Bootp flags*. Το πεδίο αυτό δηλώνει στον παραλήπτη του πακέτου εάν επιθυμεί η απάντηση να είναι unicast ή broadcast. Στη συγκεκριμένη περίπτωση δείτε ότι δηλώνεται η επιλογή unicast. Αυτό θα έχει ως αποτέλεσμα ο DHCP server να αποστείλει το πακέτο DHCP Offer με unicast διευθύνσεις προορισμού (IP και MAC). Πράγματι, εάν ελέγξουμε τις διευθύνσεις IP και MAC του DHCP Offer θα δούμε ότι οι διευθύνσεις είναι unicast.

4.5 Αποθήκευση ρυθμίσεων στην μνήμη του δρομολογητή

Η δικτυακές συσκευές της Cisco (είτε δρομολογητές είτε switches) έχουν ένα σύνολο προεγκατεστημένων ρυθμίσεων οι οποίες είναι αποθηκευμένες σε μια Non-Volatile RAM (NVRAM). Οι τρέχουσες ρυθμίσεις που γίνονται από τον διαχειριστή αποθηκεύονται στην RAM της συσκευής η οποία εάν επανεκκινηθεί διατηρεί τις ρυθμίσεις της NVRAM και διαγράφει αυτές της RAM. Οι ρυθμίσεις στην NVRAM ονομάζονται *startup configuration* ενώ οι τρέχουσες *running configuration*. Για την αποθήκευση των τρεχουσών ρυθμίσεων στην NVRAM δίνουμε:

```
R1#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]
```

Εάν επιθυμούμε την διαγραφή των ρυθμίσεων που είναι αποθηκευμένες στην NVRAM της συσκευής τότε γράφουμε:

```
R1#erase start

Erasing the nvram filesystem will remove all configuration files!

Continue? [confirm]

[OK]

Erase of nvram: complete
```

5. Δρομολόγηση σε IP δίκτυα

Οι δρομολογητές είναι συσκευές οι οποίες έχουν ως στόχο την διασύνδεση διαφορετικών δικτύων. Επομένως, δεν τους απασχολεί η φυσική θέση ενός σταθμού (host) αλλά το δίκτυο στο οποίο ανήκει και ο «συντομότερος» δρόμος (ο δρόμος με το μικρότερο κόστος) προς αυτό. Όταν ένας δρομολογητής λαμβάνει ένα πακέτο με κάποιον προορισμό (την IP διεύθυνση ενός host), ο δρομολογητής εξάγει την IP διεύθυνση του δικτύου και επιχειρεί να βρεί ποιος είναι ο επόμενος γειτονικός δρομολογητής στην συντομότερη διαδρομή προς αυτό. Για να το επιτύχει αυτό συμβουλεύεται τον *Πίνακα Δρομολόγησης (Routing Table).* Ο πίνακας δρομολόγησης είναι το σημαντικότερο χαρακτηριστικό ενός δρομολογητή και περιέχει κυρίως δύο πληροφορίες:

- **IP διεύθυνση δικτύου προορισμού (Destination network IP address)**
- **IP διεύθυνση επόμενου (γειτονικού) κόμβου (IP next-hop)**

Εάν ο δρομολογητής που λαμβάνει το εισερχόμενο πακέτο είναι άμεσα συνδεδεμένος (directly connected) στο δίκτυο προορισμού τότε, προφανώς, δεν υπάρχει κάποια καταχώρηση για την IP next-hop. Ο δρομολογητής απλά εναποθέτει το πακέτο στην διεπαφή του η οποία ανήκει στο δίκτυο προορισμού και αυτό καταλήγει στον τελικό προορισμό (host) μέσω της κεντρικής δικτυακής συσκευής (π.χ. switch ή hub).

Το κάθε ζεύγος ***<Dest net IP,IP next-hop>*** συνοδεύεται και από έναν αριθμό από το 0 έως το 255 ο οποίος καλείται *Administrative Distance (AD).* Πρόκειται για ένα μέτρο της βαρύτητας που έχει κάθε καταχώρηση μέσα στον πίνακα δρομολογησης. Όσο μικρότερη η τιμή του AD τόσο μεγαλύτερη βαρύτητα έχει η καταχώρηση. Για παράδειγμα αν ο πίνακας δρομολόγησης έχει δύο καταχωρήσεις προς το ίδιο δίκτυο προορισμού αλλά η πρώτη έχει AD=150 και η δεύτερη έχει AD=151, τότε κάθε πακέτο που φθάνει στον δρομολογητή με κατεύθυνση αυτό το δίκτυο θα δρομολογείται μέσω του *next-hop* που ορίζεται στην πρώτη καταχώρηση. Εάν για κάποιο λόγο η ζεύξη του δρομολογητή με το next-hop που ορίζεται στην πρώτη καταχώρηση είναι πλέον μη λειτουργική, τότε επιλέγεται η δεύτερη καταχώρηση (αυτή με AD=151). Το AD φυσικά λαμβάνεται υπ' όψιν μόνο όταν υπάρχουν δυο καταχωρήσεις για το ίδιο δίκτυο προορισμού μέσω διαφορετικών next-hop.

Επιπρόσθετα, κάθε καταχώρηση συνοδεύεται από μια ακόμα παράμετρο που ονομάζεται *metric*. Το metric είναι ένα μέτρο του «κόστους» που πρέπει να καταβληθεί για να σταλεί το πακέτο στο συγκεκριμένο next-hop. Για παράδειγμα, το κόστος αυτό μπορεί δηλώνει τον αριθμό των αλμάτων (hop count) που παρεμβάλλονται ανάμεσα στον δρομολογητή και το δίκτυο προορισμού. Το metric έχει νόημα στην δυναμική δρομολόγηση και θα αναφερθούμε εκτενέστερα παρακάτω.

Συνοπτικά, ο πίνακας δρομολόγησης ενός δρομολογητή περιέχει καταχωρήσεις οι οποίες περιλαμβάνουν, κατά κύριο λόγο, τις ακόλουθες παραμέτρους:

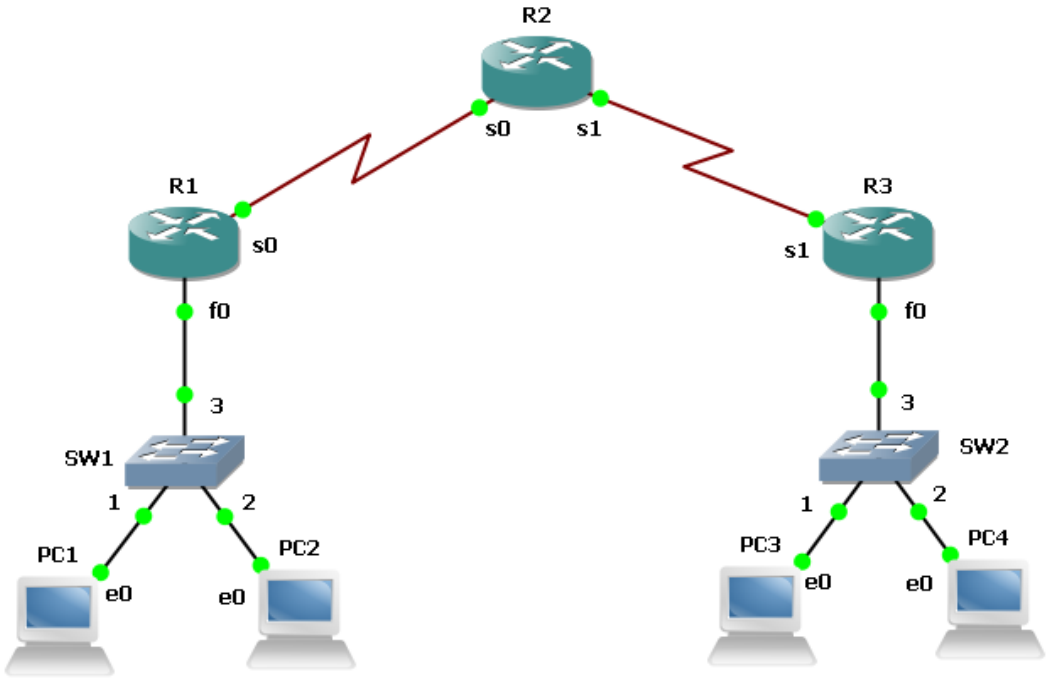
`<Dest_net_IP,IP_next_hop,AD,metric>`

Οι καταχωρήσεις αυτές στον πίνακα δρομολόγησης μπορούν να γίνουν είτε χειροκίνητα από τον διαχειριστή είτε αυτόματα με τη χρήση πρωτοκόλλων δρομολόγησης. Στην πρώτη περίπτωση μιλάμε για *Στατική Δρομολόγηση (static routing)* ενώ στην δεύτερη για *Δυναμική Δρομολόγηση (dynamic routing).* Στα σύγχρονα μεγάλα δίκτυα χρησιμοποιείται συνήθως ένας συνδυασμός δυναμικής και στατικής δρομολόγησης.

6. Ένα πλήρες δίκτυο

Σε αυτή τη παράγραφο θα εφαρμόσουμε όλες τις προηγούμενες ρυθμίσεις σε ένα υποτιθέμενο εταιρικό δίκτυο στο εργαλείο προσομοίωσης GNS3.

Ανοίξτε το GNS3 και ονομάστε το project σας ως *Corp_Net*. Κατασκευάστε το δίκτυο που φαίνεται στην Εικόνα 15 χρησιμοποιώντας τα αντικείμενα του Πίνακα 1.



Εικόνα 15. Το δίκτυο *Corp_Net*.

Ποσότητα	Αντικείμενο	Ονομασία στην Εικόνα
4	VPCS	PC1, PC2, PC3, PC4
3	c1700	R1, R2, R3
2	Ethernet Switch	SW1, SW2

Πίνακας 1. Τα αντικείμενα του δικτύου *Corp_Net*.

6.1 IP διευθυνσιοδότηση

Σε πρώτη φάση θα πρέπει να ετοιμάσουμε το σχέδιο διευθυνσιοδότησης των κόμβων του δικτύου. Ας θεωρήσουμε ότι ο διαχειριστής του δικτύου έχει την IP διεύθυνση 195.251.44.0/24 στην διάθεση του. Με την διάταξη που φαίνεται στην Εικόνα 15 το δίκτυο διαθέτει τέσσερα υποδίκτυα και επομένως πρέπει να εφαρμόσουμε τις αρχές της υποδικτύωσης. Προκειμένου να ορίσουμε τέσσερα υποδίκτυα στο συγκεκριμένο δίκτυο θα πρέπει να χρησιμοποιήσουμε την *Μάσκα Υποδικτύωσης (Subnet Mask)*

255.255.255.192 (/26). Με τον τρόπο αυτό μπορούμε να ορίσουμε τα υποδίκτυα με τις παρακάτω ταυτότητες:

- 195.251.44.0
- 195.251.44.64
- 195.251.44.128
- 195.251.44.192

Αυτά οργανώνονται όπως φαίνεται στον Πίνακα 2.

Κόμβοι στο υποδίκτυο	**Ταυτότητα Υποδικτύου/Μάσκα**
PC1, PC2, R1	195.251.44.0/26
R1, R2	195.251.44.64/26
R2, R3	195.251.44.128/26
PC3, PC4, R3	195.251.44.192/26

Πίνακας 2. Τα υποδίκτυα και οι ταυτότητες τους για το δίκτυο *Corp_Net*.

Οι IP διευθύνσεις που επιθυμούμε να αποδώσουμε στα interfaces των κόμβων συνοψίζονται στον Πίνακα 3.

Παρατηρείστε ότι επιθυμούμε να αποδώσουμε IP διευθύνσεις μέσω DHCP στους κόμβους PC1 και PC2. Επομένως, θα πρέπει να ορίσουμε τον R1 και ως DHCP server. Στη συνέχεια δίνεται το σύνολο των εντολών που πρέπει να δώσουμε για τον κάθε κόμβο ξεχωριστά. Ας σημειωθεί ότι για λόγους απλότητας δεν θα κάνουμε ρυθμίσεις ασφαλείας στους κόμβους (δεν θα οριστούν passwords στους δρομολογητές).

Κόμβος (Διεπαφή)	**Διεύθυνση / Μάσκα**
R1 (f0)	195.251.44.1/26
PC1 (e0)	DHCP
PC2 (e0)	DHCP
R1 (s0)	195.251.44.65/26
R2 (s0)	195.251.44.66/26
R2 (s1)	195.251.44.129/26
R3 (s1)	195.251.44.130/26
R3 (f0)	195.251.44.193/26

PC3 (e0)	195.251.44.194/26
PC4 (e0)	195.251.44.195/26

Πίνακας 3. IP διευθυνσιοδότηση για του κόμβους του δικτύου *Corp_Net*.

6.1.1 Κόμβος R1

```
R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0
R1(config-if)#ip address 195.251.44.1 255.255.255.192
R1(config-if)#no shut
R1(config-if)#int s0
R1(config-if)#ip address 195.251.44.65 255.255.255.192
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip dhcp pool MyPool
R1(dhcp-config)#network 195.251.44.0 255.255.255.192
R1(dhcp-config)#default-router 195.251.44.1
R1(dhcp-config)#lease 1 0 0
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 195.251.44.1
R1(config)#exit
R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

6.1.2 Κόμβος PC1

```
PC1> dhcp
DDORA IP 195.251.44.2/26 GW 195.251.44.1
```

6.1.3 Κόμβος PC2

```
PC2> dhcp

DDORA IP 195.251.44.3/26 GW 195.251.44.1
```

6.1.4 Κόμβος R2

```
R2>enable

R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#int s0

R2(config-if)#ip address 195.251.44.66 255.255.255.192

R2(config-if)#no shut

R2(config-if)#int s1

R2(config-if)#ip address 195.251.44.129 255.255.255.192

R2(config-if)#no shut

R2(config-if)#end

R2#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]
```

6.1.5 Κόμβος R3

```
R3>enable

R3#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int s1

R3(config-if)#ip address 195.251.44.130 255.255.255.192

R3(config-if)#no shut

R3(config-if)#int f0

R3(config-if)#ip address 195.251.44.193 255.255.255.192

R3(config-if)#no shut

R3(config-if)#end
```

```
R3#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]
```

6.1.6 Κόμβος PC3

```
PC3> ip 195.251.44.194 255.255.255.192 195.251.44.193

Checking for duplicate address...

PC3 : 195.251.44.194 255.255.255.192 gateway 195.251.44.193

PC3> save pc3

Saving startup configuration to pc3.vpc

.  done
```

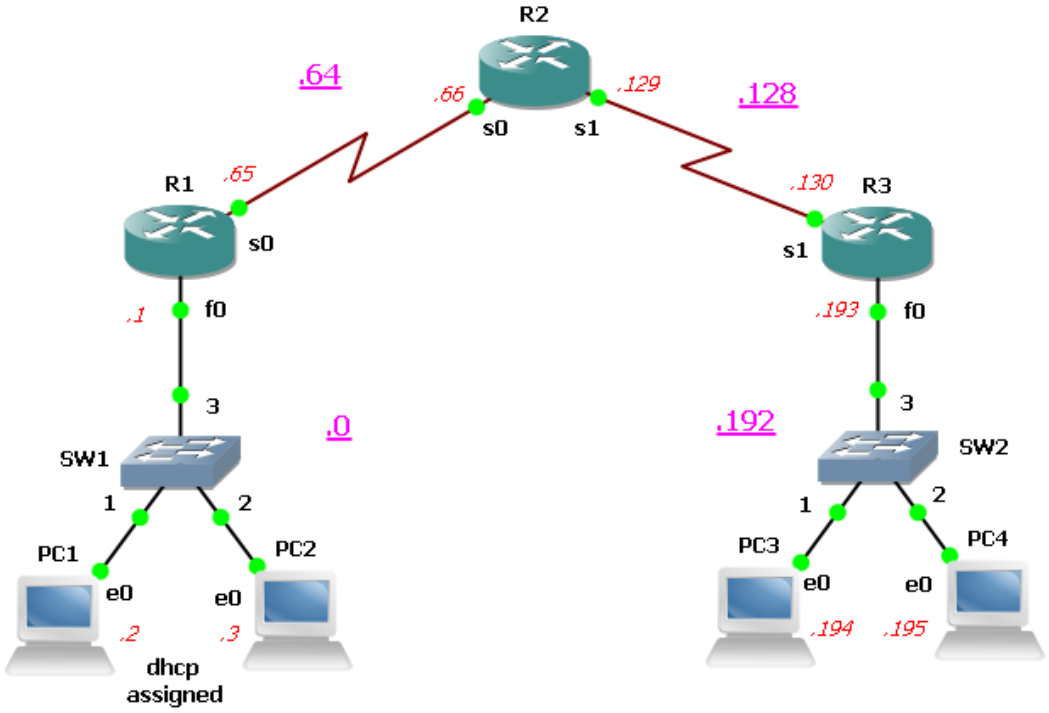
6.1.7 Κόμβος PC4

```
PC4> ip 195.251.44.195 255.255.255.192 195.251.44.193

Checking for duplicate address...

PC4 : 195.251.44.195 255.255.255.192 gateway 195.251.44.193

PC4> save pc4

Saving startup configuration to pc4.vpc

.  done
```

6.2 Στατική δρομολόγηση

Έπειτα από την IP διευθυνσιοδότηση για να μπορέσει το δίκτυο μας να είναι πλήρως λειτουργικό, θα πρέπει να ορίσουμε και τις κατάλληλες δρομολογήσεις. Σε αυτή τη παράγραφο θα τις ορίσουμε με στατικό τρόπο.

Στην Εικόνα 16 εμφανίζεται το εταιρικό δίκτυο με τις IP διευθύνσεις που έχουν αποδοθεί στα υποδίκτυα του.



Εικόνα 16. Το δίκτυο *Corp_Net* με ολοκληρωμένη την IP διευθυνσιοδότηση.

Στόχος της στατικής δρομολόγησης είναι να "χτιστεί" ο πίνακας δρομολόγησης του κάθε δρομολογητή στο δίκτυο. Αυτός ο πίνακας θα περιλαμβάνει ήδη τα υποδίκτυα στα οποία είναι άμεσα συνδεδεμένος ο κάθε δρομολογητής. Προφανώς, δεν θα περιλαμβάνει αυτά στα οποία δεν είναι άμεσα συνδεδεμένος και επομένως θα πρέπει να τοποθετηθούν χειρονακτικά. Για να το επιτύχουμε αυτό εξετάζουμε έναν δρομολογητή κάθε φορά και κάνουμε την εξής ερώτηση:

«ποια είναι τα υποδίκτυα στα οποία δεν είναι άμεσα συνδεδεμένος (directly connected) ο δρομολογητής υπό εξέταση;».

Το σύνολο των υποδικτύων που αποτελούν απάντηση στην παραπάνω ερώτηση πρέπει να τοποθετηθούν στον πίνακα δρομολόγησης.

Ξεκινώντας από τον δρομολογητή R1, συνδεθείτε στην κονσόλα του και εκτελέστε την παρακάτω εντολή για να εμφανίσετε τον πίνακα δρομολόγησης του:

```
R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static
route

       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set


     195.251.44.0/26 is subnetted, 2 subnets

C       195.251.44.0 is directly connected, FastEthernet0

C       195.251.44.64 is directly connected, Serial0
```

Η έξοδος της παραπάνω εντολής περιλαμβάνει κάποιους επεξηγηματικούς κώδικες και στη συνέχεια εμφανίζει τον πίνακα δρομολόγησης. Ο πίνακας δρομολόγησης (που φαίνεται χρωματισμένος στην παραπάνω έξοδο) του R1 εμφανίζει δυο καταχωρήσεις: μια για κάθε υποδίκτυο στο οποίο είναι άμεσα συνδεδεμένος (directly connected) ο R1.

Παρατηρώντας την Εικόνα 16 καταλήγουμε ότι ο R1 δεν είναι άμεσα συνδεδεμένος στα υποδίκτυα 195.251.44.128 και 195.251.44.192. Γι' αυτά τα υποδίκτυα θα πρέπει να υπάρξει μια καταχώρηση στον πίνακα δρομολόγησης. Αυτό γίνεται δίνοντας τις παρακάτω εντολές:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip route 195.251.44.128 255.255.255.192 195.251.44.66

R1(config)#ip route 195.251.44.192 255.255.255.192 195.251.44.66

R1(config)#exit

R1#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]
```

Η γενική μορφή της εντολής για την τοποθέτησης μιας στατικής καταχώρησης είναι επομένως:

ip route [dest network] [subnet mask] [next-hop address] [AD]

Ο ορισμός του AD είναι προεραιτικός. Εάν δεν οριστεί στην εντολή που θα δώσουμε τότε χρησιμοποιείται η προκαθορισμένη τιμή για την στατική δρομολόγηση. Η τιμή

του AD για την στατική δρομολόγηση καθώς και για άλλες καταχωρήσεις φαίνονται στον Πίνακα 4.

Είδος Δρομολόγησης από το οποίο προήλθε η καταχώρηση	**Προκαθορισμένη τιμή AD (Default AD)**
Συνδεδεμένη διεπαφή (connected interface)	*0*
Στατική δρομολόγηση	*1*
OSPF	*110*
RIP	*120*

Πίνακας 4. Προκαθορισμένες τιμές AD.

Παρατηρούμε ότι αν, για παράδειγμα, έχουμε σε λειτουργία το πρωτόκολλο RIP και τοποθετηθεί μια καταχώρηση στον πίνακα δρομολόγησης προς ένα δίκτυο από αυτό το πρωτόκολλο, αυτή η καταχώρηση θα υπερκεραστεί από μια εκ των υστέρων στατική καταχώρηση που μπορεί να κάνει ο διαχειριστής.

Επιστρέφοντας στο προηγούμενο παράδειγμα, ορίσαμε ως next-hop address (επόμενο άλμα) τον R2 και πιο συγκεκριμένα την IP διεύθυνση του interface `s0` του R2.

Εμφανίστε τώρα τον πίνακα δρομολόγησης του R1:

```
R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static
route

       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set


     195.251.44.0/26 is subnetted, 4 subnets

C       195.251.44.0 is directly connected, FastEthernet0

C       195.251.44.64 is directly connected, Serial0

S       195.251.44.128 [1/0] via 195.251.44.66
```

```
S       195.251.44.192 [1/0] via 195.251.44.66
```

Εμφανίζονται δύο στατικές δρομολογήσεις που υποδηλώνονται από το γράμμα «S» μπροστά από την καταχώρηση για τα δίκτυα 195.251.44.128 και 195.251.44.192, με AD=1 και metric=0, και τα οποία είναι προσβάσιμα μέσω της 195.251.44.66.

Σημείωση: *Αν επιθυμούμε να αφαιρέσουμε μια στατική καταχώρηση από τον πίνακα δρομολόγησης δίνουμε ακριβώς την ίδια εντολή που δώσαμε για την τοποθέτηση της βάζοντας, όμως, στην αρχή την λέξη* `no`*. Για παράδειγμα η εντολή:*

```
R1(config)#no ip route 195.251.44.128 255.255.255.192 195.251.44.66
```

αφαιρεί την καταχώρηση:

```
S       195.251.44.128 [1/0] via 195.251.44.66
```

από τον πίνακα δρομολόγησης του δρομολογητή R1.

Κάντε τις παρακάτω ρυθμίσεις στον R2 και επιβεβαιώστε τις καταχωρήσεις στον πίνακα δρομολόγησης του:

```
R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config)#ip route 195.251.44.0 255.255.255.192 195.251.44.65

R2(config)#ip route 195.251.44.192 255.255.255.192 195.251.44.130

R2(config)#exit

R2#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

R2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static
route
```

```
       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set


     195.251.44.0/26 is subnetted, 4 subnets
S       195.251.44.0 [1/0] via 195.251.44.65
C       195.251.44.64 is directly connected, Serial0
C       195.251.44.128 is directly connected, Serial1
S       195.251.44.192 [1/0] via 195.251.44.130
```

Τέλος, κάντε τις παρακάτω ρυθμίσεις στον R3:

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 195.251.44.0 255.255.255.192 195.251.44.129
R3(config)#ip route 195.251.44.64 255.255.255.192 195.251.44.129
R3(config)#exit
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set
```

```
     195.251.44.0/26 is subnetted, 4 subnets

S       195.251.44.0 [1/0] via 195.251.44.129

S       195.251.44.64 [1/0] via 195.251.44.129

C       195.251.44.128 is directly connected, Serial1

C       195.251.44.192 is directly connected, FastEthernet0
```

6.3 Επαλήθευση της λειτουργίας του δικτύου

Για να μπορέσουμε να επαληθεύσουμε την διασυνδεσιμότητα όλων των κόμβων του δικτύου μπορούμε να χρησιμοποιήσουμε τις εντολές `ping` και `traceroute`. Αυτές μπορούν να εκτελεστούν σε οποιονδήποτε κόμβο (router ή PC) με προορισμό οποιονδήποτε άλλον. Για παράδειγμα εκτελέστε την εντολή `ping` στον PC1 με προορισμό τον PC4:

```
PC1> ping 195.251.44.195

195.251.44.195 icmp_seq=1 timeout

84 bytes from 195.251.44.195 icmp_seq=2 ttl=61 time=78.125 ms

84 bytes from 195.251.44.195 icmp_seq=3 ttl=61 time=62.500 ms

84 bytes from 195.251.44.195 icmp_seq=4 ttl=61 time=62.500 ms

84 bytes from 195.251.44.195 icmp_seq=5 ttl=61 time=62.500 ms
```

Παρατηρείστε την επιτυχή εκτέλεση της εντολής που μαρτυρά την διασυνδεσιμότητα των κόμβων και την ορθή λειτουργία των δρομολογήσεων.

Εκτελέστε και την εντολή `traceroute` στον ίδιο κόμβο με τον ίδιο προορισμό:

```
PC1> trace 195.251.44.195

trace to 195.251.44.195, 8 hops max, press Ctrl+C to stop

 1   195.251.44.1   31.250 ms  0.000 ms  31.250 ms

 2   195.251.44.66   31.250 ms  62.500 ms  31.250 ms

 3   195.251.44.130   93.750 ms  62.500 ms  93.750 ms

 4   *195.251.44.195   62.500 ms (ICMP type:3, code:3, Destination port
unreachable)
```

Παρατηρείστε ότι στην έξοδο της εντολής `trace` (η οποία είναι ουσιαστικά η `traceroute`) εμφανίζεται η διαδρομή προς τον προορισμό: ο R1 (195.251.44.1), ο R2 (195.251.44.66) και ο R3 (195.251.44.130). Η τελευταία κατάχώρηση είναι ο τελικός προορισμός.

Οι ίδιες εντολές μπορούν να εκτελεστούν και στους δρομολογητές. Για παράδειγμα εκτελέστε την εντολή ping στον δρομολογητή R1 με προορισμό τον PC3:

```
R1#ping 195.251.44.194

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 195.251.44.194, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 28/40/72 ms
```

Εκτελέστε επίσης την εντολή traceroute στον R1 με τον ίδιο προορισμό:

```
R1#traceroute 195.251.44.194

Type escape sequence to abort.

Tracing the route to 195.251.44.194

  1 195.251.44.66 16 msec 0 msec 28 msec

  2 195.251.44.130 32 msec 32 msec 28 msec

  3 195.251.44.194 36 msec 52 msec 24 msec
```

6.4 Προκαθορισμένες διαδρομές

Παρατηρείστε ότι οι δρομολογητές R1 και R3 του δικτύου έχουν στατικές δρομολογήσεις οι οποίες όλες προωθούν τα πακέτα προς τον R2 (είτε στο `s0` είτε στο `s1`). Εάν είχαμε ένα μεγαλύτερο δίκτυο τότε θα έπρεπε να έχουμε περισσότερες στατικές καταχωρήσεις στον πίνακα δρομολόγησης που θα προωθούσαν τα πακέτα στο ίδιο interface του ίδιου δρομολογητή. Αυτό μπορεί να αποφευχθεί με τη χρήση των *προκαθορισμένων διαδρομών (default routes).* Για να δούμε την λειτουργία των default routes θα πρέπει, κατ' αρχάς, να αφαιρέσουμε τις στατικές δρομολογήσεις στον R1:

```
R1(config)#no ip route 195.251.44.192 255.255.255.192 195.251.44.66

R1(config)#no ip route 195.251.44.128 255.255.255.192 195.251.44.66

R1(config)#exit

R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static
route

       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set


     195.251.44.0/26 is subnetted, 2 subnets

C       195.251.44.0 is directly connected, FastEthernet0

C       195.251.44.64 is directly connected, Serial0
```

Δείτε ότι πλέον δεν υπάρχουν οι στατικές καταχωρήσεις στον πίνακα δρομολόγησης του R1.

Κατόπιν δώστε τις παρακάτω εντολές για να εφαρμόσουμε default routes στον δρομολογητή:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#ip route 0.0.0.0 0.0.0.0 195.251.44.66

R1(config)#ip classless

R1(config)#exit

R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static
route

       o - ODR, P - periodic downloaded static route


Gateway of last resort is 195.251.44.66 to network 0.0.0.0


     195.251.44.0/26 is subnetted, 2 subnets

C       195.251.44.0 is directly connected, FastEthernet0
```

```
C       195.251.44.64 is directly connected, Serial0

S*   0.0.0.0/0 [1/0] via 195.251.44.66
```

Η πρώτη εντολή δηλώνει ότι οποιοδήποτε πακέτο με οποιοδήποτε προορισμό θα πρέπει να προωθηθεί προς την διεύθυνση 195.251.44.66 που είναι το `s0` του R2 (εκτός φυσικά από τα πακέτα που έχουν προορισμό κάποιο από τα δίκτυα που είναι άμεσα συνδεδεμένος ο R1). Η δεύτερη εντολή αγνοεί την subnet mask. Έτσι, εάν έρθει ένα πακέτο αυτό άμεσα θα προωθηθεί προς τον R2. Η προκαθορισμένη διαδρομή υποδηλώνεται στον πίνακα δρομολόγησης ως «S*».

Αντίστοιχες ρυθμίσεις θα πρέπει να εκτελέσουμε και στον R3:

```
R3#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#no ip route 195.251.44.64 255.255.255.192 195.251.44.129

R3(config)#no ip route 195.251.44.0 255.255.255.192 195.251.44.129

R3(config)#ip route 0.0.0.0 0.0.0.0 195.251.44.129

R3(config)#ip classless

R3(config)#exit

R3#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static
route

       o - ODR, P - periodic downloaded static route


Gateway of last resort is 195.251.44.129 to network 0.0.0.0


     195.251.44.0/26 is subnetted, 2 subnets

C       195.251.44.128 is directly connected, Serial1

C       195.251.44.192 is directly connected, FastEthernet0

S*   0.0.0.0/0 [1/0] via 195.251.44.129
```

Για να επαληθεύσουμε την ορθή λειτουργία του δικτύου εκτελέστε την εντολή `ping` στον PC2 με προορισμό τον PC3:

```
PC2> ping 195.251.44.194

84 bytes from 195.251.44.194 icmp_seq=1 ttl=61 time=93.750 ms

84 bytes from 195.251.44.194 icmp_seq=2 ttl=61 time=62.500 ms

84 bytes from 195.251.44.194 icmp_seq=3 ttl=61 time=62.500 ms

84 bytes from 195.251.44.194 icmp_seq=4 ttl=61 time=62.500 ms

84 bytes from 195.251.44.194 icmp_seq=5 ttl=61 time=62.500 ms
```

Οι προκαθορισμένες διαδρομές είναι πολύ χρήσιμες προκειμένου να μειωθεί ο αριθμός των καταχωρήσεων στον πίνακα δρομολόγησης και άρα το μέγεθος του.

6.5 Δυναμική δρομολόγηση

Το σημαντικότερο μειονέκτημα της στατικής δρομολόγησης είναι η αδυναμία αυτόματης επικαιροποίησης των πινάκων δρομολόγησης στις περιπτώσεις που αλλάζει η συνδεσμολογία του δικτύου. Η ενημέρωση των πινάκων δρομολόγησης όλων των δρομολογητών θα πρέπει να γίνει με χειροκίνητο τρόπο. Για παράδειγμα, εάν προστεθεί ένα ακόμα υποδίκτυο στην δικτυακή τοπολογία τότε θα πρέπει να τοποθετηθεί μια νέα καταχώρηση στους δρομολογητές που δεν είναι άμεσα συνδεδεμένοι σε αυτό, αν θέλουμε να έχουμε ένα πλήρως λειτουργικό δίκτυο. Με την στατική δρομολόγηση η διαδικασία αυτή θα χρειαστεί χρόνο και κόπο.

Με την δυναμική δρομολόγηση η κατασκευή των πινάκων δρομολόγησης των δρομολογητών μπορεί να γίνει αυτόματα και χωρίς την εμπλοκή του διαχειριστή. Η συμπλήρωση των πινάκων δρομολόγης με τις καταχωρήσεις προς όλα τα δίκτυα γίνεται έπειτα από την επικοινωνία των συσκευών δρομολόγησης οι οποίες ενημερώνουν τις γειτονικές τους για τα δίκτυα στα οποία είναι άμεσα συνδεδεμένες.

Υπάρχουν πολλά πρωτόκολλα δρομολόγησης που είναι διαθέσιμα προς χρήση σήμερα. Αυτά χωρίζονται στα *Εσωτερικά Πρωτόκολλα Δρομολόγησης (Interior Gateway Protocols – IGP)* και τα *Εξωτερικά Πρωτόκολλα Δρομολόγησης (Exterior Gateway Protocols – EGP).* Τα IGP χρησιμοποιούνται για την κατασκευή των πινάκων δρομολόγησης εντός των *Αυτόνομων Συστημάτων (Autonomous Systems – AS).* Ένα AS είναι ένα διαδίκτυο το οποίο διαχειρίζεται ένας οργανισμός (π.χ. το εσωτερικό δίκτυο μιας εταιρίας ή ενός Πανεπιστημίου ή ενός ISP). Τα EGP χρησιμοποιούνται για την επικοινωνία μεταξύ των αυτόνομων συστημάτων. Εμείς θα ασχοληθούμε μόνο με τα IGP. Ενδεικτικά αναφέρουμε τα γνωστότερα IGP: το *Routing Information Protocol (RIP)* και το *Open Shortest Path First (OSPF).*

Το RIP είναι το παλαιότερο πρωτόκολλο δρομολόγησης και ανήκει στην κατηγορία των distance-vector πρωτοκόλλων. Το OSPF είναι ένα από τα δημοφιλέστερα πρωτόκολλα δρομολόγησης και ανήκει στην κατηγορία των link-state πρωτοκόλλων.

Τα distance-vector πρωτόκολλα επιτρέπουν στους δρομολογητές να επικοινωνούν με τους γειτονικούς τους και να τους ενημερώνουν για τα δίκτυα στα οποία είναι άμεσα συνδεδεμένοι. Με τον τρόπο αυτό ο κάθε δρομολογητής ενημερώνει τον πίνακα δρομολόγησης του με νέες καταχωρήσεις δικτύων που μπορούν να προσεγγιστούν μέσω των γειτονικών του. Η επικοινωνία μεταξύ γειτονικών δρομολογητών γίνεται περιοδικά ώστε να εξασφαλιστεί η ενημέρωση των πινάκων δρομολόγησης σε περίπτωση αλλαγής της δικτυακής τοπολογίας.

Τα link-state πρωτόκολλα δίνουν την δυνατότητα σε κάθε δρομολογητή να «χτίσει» έναν χάρτη του δικτύου. Ο κάθε δρομολογητής αποστέλλει προς όλους τους υπόλοιπους δρομολογητές ότι πληροφορία έχει διαθέσιμη: ζεύξεις, IP διευθύνσεις, γειτονικούς δρομολογητές, εύρος ζώνης ζεύξεων κλπ. Έτσι όλοι οι δρομολογητές διαθέτουν τις ίδιες πληροφορίες για το δίκτυο όπως όλοι οι υπόλοιποι.

Η ενημέρωση όλων των δρομολογητών στα link-state πρωτόκολλα γίνεται με μια τεχνική που λέγεται *flooding* και σύμφωνα με αυτήν ο κάθε δρομολογητής «πλυμμυρίζει» (floods) το δίκτυο με τις πληροφορίες για τις διασυνδέσεις του. Οι πληροφορίες αυτές ονομάζονται *Link State Advertisement (LSA)*. Ένας δρομολογητής που έχει συγκεντρώσει τα LSA από όλους τους υπολοίπους δρομολογητές τα οργανώνει σε μια βάση δεδομένων η οποία ονομάζεται *Link State Database (LSDB)*. Αυτή η βάση δεδομένων είναι στην ουσία μια χαρτογράφηση του δικτύου. Εφαρμόζοντας αλγορίθμους, όπως ο αλγόριθμος Dijkstra, ο δρομολογητής μπορεί να υπολογίσει την συντομότερη διαδρομή. Για να μπορέσει να πλυμμηρίσει το LSA του κάποιος δρομολογητής θα πρέπει να έχει αναπτύξει σχέσεις με τους γειτονικούς του η οποίοι θα αναμεταδίδουν τα LSA του. Η ανάπτυξη σχέσεων μεταξύ των γειτονικών δρομολογητών επιτυγχάνεται με την περιοδική αποστολή ειδικών μηνυμάτων που ονομάζονται *OSPF Hello*.

6.5.1 Κριτήριο δρομολόγησης

Το κριτήριο με βάση το οποίο γίνεται η επιλογή της διαδρομής προς τον προορισμό (όταν υπάρχουν πολλές εναλλακτικές) ονομάζεται *Κριτήριο Δρομολόγησης (Routing Metric)*. Τα ποιό γνωστά κριτήρια δρομολόγησης είναι ο αριθμός των δρομολογητών και το συνολικό bandwidth της διαδρομής. Το πρώτο κριτήριο χρησιμοποιείται από το πρωτόκολλο δρομολόγησης RIP ενώ το δεύτερο από το OSPF.

Στην περίπτωση του RIP το routing metric ονομάζεται *Αριθμός Αλμάτων (Hop Count)* και επιλέγεται η διαδρομή με τον μικρότερο αριθμό αλμάτων (δηλαδή τον μικρότερο αριθμό δρομολογητών μεταξύ αποστολέα και παραλήπτη).

Όσον αφορά στο OSPF, η Cisco έχει τον δικό της τρόπο υπολογισμού του metric μιας διαδρομής. Εφόσον επιλέγεται η διαδρομή με το μικρότερο κόστος (metric) θα πρέπει το κόστος αυτό να είναι αντιστρόφως ανάλογο με το διαθέσιμο bandwidth μιας ζεύξης. Σύμφωνα με την Cisco, το metric μιας ζεύξης δίνεται από τον παρακάτω τύπο:

$$metric = \left\lfloor \frac{10^8}{BW} \right\rfloor$$

Για παράδειγμα, μια 100 Mbps ζεύξη θα έχει metric 1, μια 10 Mbps ζεύξη θα έχει metric 10 ενώ μια 1.544 Mbps (T1) ζεύξη θα έχει metric 64. Το συνολικό κόστος μιας διαδρομής θα υπολογίζεται από το άθροισμα των επιμέρους κοστών των ζεύξεων που την απαρτίζουν:

$$\left\lfloor \frac{10^8}{BW_1} \right\rfloor + \left\lfloor \frac{10^8}{BW_2} \right\rfloor + \left\lfloor \frac{10^8}{BW_3} \right\rfloor + ... + \left\lfloor \frac{10^8}{BW_n} \right\rfloor$$

Όπου *n*, το σύνολο των ζεύξεων που παρεμβάλλονται μεταξύ του συνοριακού δρομολογητή (gateway) του αποστολέα και του κόμβου προορισμού.

6.5.2 Εφαρμογή του RIP πρωτοκόλλου

Σε αυτή τη παράγραφο θα ενεργοποιήσουμε το RIP πρωτόκολλο στο δίκτυο *Corp_Net*. Προκειμένου να εντοπίσουμε τα πακέτα που αποστέλλονται μεταξύ των δρομολογητών θα πρέπει να εκκινήσουμε τον αναλυτή πρωτοκόλλων wireshark σε μια ζεύξη. Εκκινήστε την καταγραφή στην σειριακή ζεύξη που συνδέει των R1 και R2 της Εικόνας 16.

Πριν όμως ενεργοποιήσουμε το RIP θα πρέπει να αφαιρέσουμε τις στατικές δρομολογήσεις που είχαμε τοποθετήσει προηγουμένως στους δρομολογητές. Παρακάτω φαίνονται τα βήματα για τον κάθε δρομολογητή της Εικόνας 16.

Για τον R1 δίνουμε τις παρακάτω εντολές:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#no ip route 0.0.0.0 0.0.0.0 195.251.44.66

R1(config)#router rip

R1(config-router)#network 195.251.44.0
```

Αρχικά αφαιρούμε την προκαθορισμένη διαδρομή που είχαμε καταχωρήσει και κατόπιν ενεργοποιούμε το RIP πρωτόκολλο με τις δύο τελευταίες εντολές. Η τελευταία εντολή προσδιορίζει το δίκτυο στο οποίο θα λειτουργεί το RIP.

Για τον R2 δίνουμε τις παρακάτω εντολές:

```
R2#config t

R2(config)#no ip route 195.251.44.0 255.255.255.192 195.251.44.65
```

```
R2(config)#no ip route 195.251.44.192 255.255.255.192 195.251.44.130
R2(config)#router rip
R2(config-router)#network 195.251.44.0
```

Για τον R3 δίνουμε τις παρακάτω εντολές:

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#no ip route 0.0.0.0 0.0.0.0 195.251.44.129
R3(config)#router rip
R3(config-router)#network 195.251.44.0
```

Κατόπιν μπορούμε να εμφανίσουμε τους πίνακες δρομολόγησης όλων των δρομολογητών:

Για τον R1:

```
R1(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     195.251.44.0/26 is subnetted, 4 subnets
C       195.251.44.0 is directly connected, FastEthernet0
C       195.251.44.64 is directly connected, Serial0
R       195.251.44.128 [120/1] via 195.251.44.66, 00:00:21, Serial0
R       195.251.44.192 [120/2] via 195.251.44.66, 00:00:21, Serial0
```

Παρατηρούμε την αυτόματη ενημέρωση του πίνακα με δυο καταχωρήσεις με την χρήση του RIP (το «R» μπροστά από την καταχώρηση υποδηλώνει την χρήση του

πρωτοκόλλου): μια για το υποδίκτυο 195.251.44.128 με metric 1 μέσω του 195.251.44.66 (R2) και μια για το δίκτυο 195.251.44.128 με metric 2 μέσω του 195.251.44.66 (R2). Το κόστος προσέγγισης για το πρώτο δίκτυο είναι ένα hop (ένας δρομολογητής) ενώ για το δεύτερο δύο hop (δύο δρομολογητές).

Σημείωση: *Παρατηρήστε ότι για να εμφανιστεί ο πίνακας δρομολόγησης δόθηκε η εντολή* **do show ip route** *η οποία εκτελέστηκε από την κατάσταση ρυθμίσεων (config). Γενικά από την κατάσταση ρυθμίσεων μπορούμε να εκτελέσουμε τις εντολές* **show** *με τη χρήση του λεκτικού* **do** *πριν την εντολή. Με τον τρόπο αυτό δεν χρειάζεται να εξέλθουμε της κατάστασης config για να εκτελέσουμε την εντολή show.*

Για τον R2:

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     195.251.44.0/26 is subnetted, 4 subnets
R       195.251.44.0 [120/1] via 195.251.44.65, 00:00:17, Serial0
C       195.251.44.64 is directly connected, Serial0
C       195.251.44.128 is directly connected, Serial1
R       195.251.44.192 [120/1] via 195.251.44.130, 00:00:03, Serial1
```

Για τον R3:

```
R3(config)#do show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static
route

       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set


     195.251.44.0/26 is subnetted, 4 subnets

R       195.251.44.0 [120/2] via 195.251.44.129, 00:00:00, Serial1

R       195.251.44.64 [120/1] via 195.251.44.129, 00:00:00, Serial1

C       195.251.44.128 is directly connected, Serial1

C       195.251.44.192 is directly connected, FastEthernet0
```

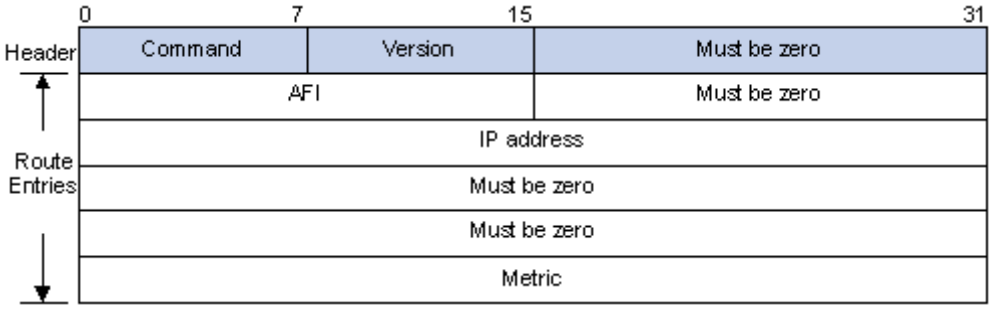
Κατά τη διάρκεια που κάναμε τις ρυθμίσεις στους δρομολογητές, ο αναλυτής πρωτοκόλλων κατέγραφε τα RIP πακέτα που μεταδιδόταν μεταξύ των δρομολογητών. Εφόσον θέσαμε σε καταγραφή την σειριακή ζεύξη μεταξύ του R1 και R2, θα πρέπει να διαθέτουμε πλέον στον αναλυτή πρωτοκόλλων την αλληλουχία των πακέτων RIP ανταλλάχθηκαν μεταξύ αυτών των δύο δρομολογητών. Για να τα κατανοήσουμε πρέπει να θυμηθούμε την δομή της επικεφαλίδας και των δεδομένων του RIP πρωτοκόλλου που φαίνεται στην Εικόνα 17.

Η επικεφαλίδα είναι απλοϊκή και περιλαμβάνει τρία πεδία:

- *Command:* προσδιορίζει εάν είναι RIP request ή RIP response. Τα πακέτα RIP που περιλαμβάνουν πληροφορίες του πινακα δρομολόγησης ενός δρομολογητή είναι τύπου RIP response.

- *Version:* προσδιορίζει την έκδοση του RIP. Έχει την τιμή 1 για το RIPv1 και την τιμή 2 για το RIPv2.

- *Must be zero:* το πεδίο αυτό δεν λαμβάνεται υπόψη και πρέπει να περιλαμβάνει μόνο μηδενικά.



Εικόνα 17. Επικεφαλίδα και δεδομένα του RIP.

Μετά την επικεφαλίδα ακολουθούν τα δεδομένα τα οποία στην περίπτωση που πρόκειται για RIP response θα περιλαμβάνουν τα δίκτυα που είναι άμεσα συνδεδεμένος ο δρομολογητής που στέλνει αυτό το πακέτο ενημέρωσης:

- *Address Family Identifier (AFI):* προσδιορίζει τον τύπο των IP διευθύνσεων που ακολουθούν. Έχει την τιμή 2 για το IP.
- *Must be zero:* το πεδίο αυτό δεν λαμβάνεται υπόψη και πρέπει να περιλαμβάνει μόνο μηδενικά.
- *IP address:* η διεύθυνση του δικτύου για το οποίο μεταδίδεται το πακέτο.
- *Must be zero:* το πεδίο αυτό δεν λαμβάνεται υπόψη και πρέπει να περιλαμβάνει μόνο μηδενικά.
- *Must be zero:* το πεδίο αυτό δεν λαμβάνεται υπόψη και πρέπει να περιλαμβάνει μόνο μηδενικά.
- *Metric:* το κόστος προσέγγισης αυτού του δικτύου. Πρόκειται για τον αριθμό των αλμάτων (δρομολογητών) που πρόκειται να προσπελαστούν πριν φθάσει ένα πακέτο στο δίκτυο.

Τα πεδία που αναλύθηκαν προηγουμένως αποτελούν μια *Καταχώρηση Διαδρομής (Route Entry)* στο RIP response. Ένα RIP response μπορεί να περιλαμβάνει μέχρι και 25 τέτοιες καταχωρήσεις.

Στον αναλυτή πρωτοκόλλων wireshark εμφανίζονται διαδοχικά τα RIP response πακέτα με αποστολείς είτε τον R1 (195.251.44.65) είτε τον R2 (195.251.44.66). Όλα έχουν προορισμό την διεύθυνση 255.255.255.255 που υποδηλώνει ότι το RIP είναι ένα broadcast πρωτόκολλο. Κάτι άλλο που μπορούμε να παρατηρήσουμε είναι ότι το RIP χρησιμοποιεί το UDP πρωτόκολλο στο επίπεδο μεταφοράς και την θύρα 520 για την επικοινωνία των δρομολογητών.

Για να επαληθεύσουμε την ορθή λειτουργία του δικτύου εκτελέστε την εντολή `ping` στον PC1 με προορισμό τον PC3:

```
PC1> ping 195.251.44.194

195.251.44.194 icmp_seq=1 timeout

84 bytes from 195.251.44.194 icmp_seq=2 ttl=61 time=46.875 ms

84 bytes from 195.251.44.194 icmp_seq=3 ttl=61 time=31.250 ms

84 bytes from 195.251.44.194 icmp_seq=4 ttl=61 time=31.250 ms

84 bytes from 195.251.44.194 icmp_seq=5 ttl=61 time=15.625 ms
```

6.5.3 Εφαρμογή του OSPF πρωτοκόλλου

Για να μπορέσει να ενεργοποιηθεί πλήρως το OPSF πρωτόκολλο σε έναν δρομολογητή θα πρέπει να ακολουθήσουμε δυο ρυθμιστικά βήματα:

1. Δήλωση στον δρομολογητή ότι θα χρησιμοποιήσει το OSPF πρωτόκολλο.
2. Δήλωση των διεπαφών (interfaces) του δρομολογητή που θα χρησιμοποιήσουν το OSPF πρωτόκολλο.

Για παράδειγμα, σε έναν δρομολογητή, έστω R, το πρώτο βήμα ολοκληρώνεται με την ακόλουθη εντολή:

```
R(config)#router ospf 1
```

Με την εντολή `router ospf` δηλώνουμε την ενεργοποίηση του OSPF στον δρομολογητή. Η παράμετρος **"1"** είναι μια τιμή που αναθέτουμε στην διεργασία που θα εκτελεί το OSPF πρωτόκολλο. Μπορούμε να έχουμε πολλαπλές OSPF διεργασίες σε κάποιον δρομολογητή και οι οποίες θα πρέπει να ξεχωρίζουν. Στα δίκτυα που θα μας απασχολήσουν θα έχουμε μια μόνο διεργασία. Ωστόσο, θα πρέπει να δωθεί κάποια τιμή σε αυτήν. Μπορείτε να δώσετε όποια τιμή θέλετε και η οποία δεν είναι απαραίτητο να είναι η ίδια στους διαφορετικούς δρομολογητές που θα εκτελούν το OSPF. Στο παραπάνω παράδειγμα δώσαμε την τιμή 1. Συνολικά μπορείτε να ορίσετε 65535 διεργασίες που εκτελούν ένα πρωτόκολλο δρομολόγησης η κάθε μια.

Για να υλοποιηθεί το δεύτερο βήμα θα πρέπει να δηλώσουμε σε ποια interfaces επιθυμούμε να εκτελείται η διεργασία OSPF. Έστω, ότι ο δρομολογητής R έχει δυο interfaces με IP διευθύνσεις 195.251.44.1/24 και 195.251.45.1/24 που ανήκουν στα υποδίκτυα 195.251.44.0/24 και 195.251.45.0/24, αντίστοιχα. Θα μπορούσαμε να δώσουμε τις εντολές:

```
R(config-router)#network 195.251.44.1 0.0.0.0 area 1

R(config-router)#network 195.251.45.1 0.0.0.0 area 1
```

Ας ξεκινήσουμε από το τέλος της κάθε εντολής. Το "area 1" δηλώνει την περιοχή στην οποία θα είναι ενεργοποιημένο το πρωτόκολλο και η τιμή που θα δώσουμε πρέπει να είναι η ίδια σε όλους τους δρομολογητές (και τα interfaces τους) που έχουμε σχεδιάσει να ανήκουν στην ίδια περιοχή. Για παράδειγμα, στην περίπτωση

του μικρού μας δικτύου οι δρομολογητές βρίσκονται στην ίδια περιοχή στην οποία εμείς αναθέσαμε την τιμή 1. Ως γνωστόν το OSPF είναι ιεραρχικό πρωτόκολλο και η ευρύτερη περιοχή στην οποία θα λειτουργεί μπορεί να διασπαστεί σε μικρότερες περιοχές με στόχο την μείωση του φόρτου που παράγεται από διαδικασία flooding των LSA.

Το κομμάτι της εντολής **«0.0.0.0»** ονομάζεται *Wildcard* και μοιάζει με IP διεύθυνση αλλά στην ουσία δηλώνει στον δρομολογητή ποια bytes από την IP διεύθυνση που δηλώθηκε πριν το wildcard πρέπει να ταιριάζουν ακριβώς και ποια είναι αδιάφορα. Το **«0»** δηλώνει *απόλυτο ταίριασμα* ενώ το **«255»** δηλώνει *αδιάφορο*. Επομένως, όσον αφορά στις δυο παραπάνω εντολές δηλώνουμε ότι το OSPF θα πρέπει να ενεργοποιηθεί στα interfaces 195.251.44.1 και 195.251.45.1 ακριβώς και τα οποία θα ανήκουν στην περιοχή 1.

Η παρακάτω αλληλουχία εντολών θα οδηγήσει στο ίδιο αποτέλεσμα:

```
Router(config-router)#network 195.251.44.0 0.0.0.255 area 1

Router(config-router)#network 195.251.45.0 0.0.0.255 area 1
```

Εδώ δηλώνουμε ότι οποιοδήποτε interface του δρομολογητή με IP διεύθυνση που ξεκινά από 195.251.44 (αδιάφορο το τέταρτο byte) θα πρέπει να ενεργοποιήσει το OSPF και να ανήκει στην περιοχή 5.

Στο ίδιο αποτέλεσμα θα οδηγηθούμε, όμως, και με την παρακάτω εντολή:

```
Router(config-router)#network 195.251.0.0 0.0.255.255 area 1
```

Με την τελευταία προσέγγιση εκτελούμε μια εντολή αντί για δύο. Σε κάθε περίπτωση χρησιμοποιούμε αυτή που μας βολεύει.

Πριν όμως ενεργοποιήσουμε το OSPF θα πρέπει να αφαιρέσουμε τις δρομολογήσεις που είχαμε τοποθετήσει προηγουμένως στους δρομολογητές με το RIP. Παρακάτω φαίνονται τα βήματα για τον κάθε δρομολογητή της Εικόνας 16.

Για τον R1 δίνουμε τις παρακάτω εντολές:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#no router rip

R1(config)#router ospf 1

R1(config-router)# network 195.251.44.0 0.0.0.255 area 1

R1(config-router)# end

R1#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     195.251.44.0/26 is subnetted, 4 subnets
C       195.251.44.0 is directly connected, FastEthernet0
C       195.251.44.64 is directly connected, Serial0
O       195.251.44.128 [110/128] via 195.251.44.66, 00:03:27, Serial0
O       195.251.44.192 [110/129] via 195.251.44.66, 00:01:07, Serial0
```

Για τον R2 δίνουμε τις παρακάτω εντολές:

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no router rip
R2(config)#router ospf 2
R2(config-router)#network 195.251.44.0 0.0.0.255 area 1
R2(config-router)#end
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set


     195.251.44.0/26 is subnetted, 4 subnets
O       195.251.44.0 [110/65] via 195.251.44.65, 00:04:44, Serial0
C       195.251.44.64 is directly connected, Serial0
C       195.251.44.128 is directly connected, Serial1
O       195.251.44.192 [110/65] via 195.251.44.130, 00:02:23, Serial1
```

Για τον R3 δίνουμε τις παρακάτω εντολές:

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#no router rip
R3(config)#router ospf 3
R3(config-router)#network 195.251.44.0 0.0.0.255 area 1
R3(config-router)#end
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set


     195.251.44.0/26 is subnetted, 4 subnets
O       195.251.44.0 [110/129] via 195.251.44.129, 00:02:59, Serial1
O       195.251.44.64 [110/128] via 195.251.44.129, 00:02:59, Serial1
C       195.251.44.128 is directly connected, Serial1
```

```
C       195.251.44.192 is directly connected, FastEthernet0
```

Σε κάθε δρομολογητή έπειτα από την ρύθμιση του OSPF, εμφανίζουμε και το routing table στο οποίο φαίνονται οι καταχωρήσεις για τα δίκτυα προορισμού (με κίτρινο χρώμα).

Για να επαληθεύσουμε την ορθή λειτουργία του δικτύου εκτελέστε την εντολή `ping` στον PC2 με προορισμό τον PC4:

```
PC2> ping 195.251.44.195

195.251.44.195 icmp_seq=1 timeout

84 bytes from 195.251.44.195 icmp_seq=2 ttl=61 time=0.000 ms

84 bytes from 195.251.44.195 icmp_seq=3 ttl=61 time=46.875 ms

84 bytes from 195.251.44.195 icmp_seq=4 ttl=61 time=78.125 ms

84 bytes from 195.251.44.195 icmp_seq=5 ttl=61 time=62.500 ms
```

6.5.4 Classful και Classless

Οι λέξεις Classful και Classless χρησιμοποιούνται σε τρείς διαφορετικές θεματικές ενότητες και σε κάθε μια έχουν και διαφορετικό νόημα. Γι' αυτό πολλές φορές αποτελούν και σημείο σύγχησης. Έτσι, λοιπόν, μπορούμε να έχουμε:

- **Classful και Classless Διευθυνσιοδότηση (Addressing)**
- **Classful και Classless Πρωτόκολλα Δρομολόγησης (Routing Protocols)**
- **Classful και Classless Δρομολόγηση (Routing)**

Από τα μαθήματα δικτύων που έχετε διδαχθεί μέχρι τώρα θα πρέπει να είστε εξοικειομένοι με τις έννοιες της **Classful και Classless Διευθυνσιοδότησης.** Συνοπτικά, μπορούμε να πούμε ότι η Classlful Διευθυνσιοδότηση αναφέρεται στο γεγονός ότι το πρόθεμα (prefix) μιας IP διεύθυνσης χωρίζεται σε δύο μέρη: στο μέρος του δικτύου (network) και στο μέρος του υποδικτύου (subnet). Το μέγεθος τους μέρους του δικτύου προσδιορίζεται από την κλάση της IP διεύθυνσης ενώ το μέγεθος του μέρους του υποδικτύου προσδιορίζεται από την μάσκα υποδικτύωσης. Στην Classless Διευθυνσιοδότηση η κλάση της IP διεύθυνσης δεν παίζει κάποιο ρόλο. Επομένως, αντιμετωπίζουμε το πρόθεμα ως ένα ενιαίο κομμάτι χωρίς να διαχωρίζεται σε μέρη δικτύου και υποδικτύου.

Τα **Classful και Classless Πρωτόκολλα Δρομολόγησης** διαχωρίζονται από το εάν στις ενημερώσεις (routing updates) που αποστέλλονται με τη χρήση του πρωτοκόλλου οι IP διευθύνσεις δικτύου συνοδεύονται και από τις μάσκες υποδικτύωσης. Έτσι, ένα Classful πρωτόκολλο δρομολόγησης δεν συμπεριλαμβάνει την μάσκα υποδικτύωσης στις ενημερώσεις του, ενώ ένα Classless πρωτόκολλο τις συμπεριλαμβάνει. Το RIP (version 1) είναι ένα χαρακτηριστικό παράδειγμα ενός Classful Πρωτοκόλλου Δρομολόγησης, ενώ, το OSPF είναι ένα παράδειγμα ενός Classless Πρωτοκόλλου Δρομολόγησης.

Επομένως, δημιουργείται το εξής ερωτηματικό: *ποια μάσκα υποδικτύωσης θα εφαρμόσει ένας δρομολογητής στις IP διευθύνσεις δικτύου που θα λάβει από τις ενημερώσεις του πρωτοκόλλου δρομολόγησης;* Ένας δρομολογητής που έχει εγκατεστημένο ένα Classful Πρωτόκολλο Δρομολόγησης (όπως το RIPv1) θα αντιδράσει στη λήψη μιας ενημέρωσης με έναν από τους παρακάτω δυο τρόπους:

- Εάν ο δρομολογητής έχει μια άμεσα συνδεδεμένη διεπαφή (directly connected interface) η οποία ανήκει στο ίδιο **ευρύτερο** δίκτυο με αυτό που θα λάβει από την ενημέρωση, τότε θα εφαρμόσει στην IP διεύθυνση δικτύου που θα λάβει την ίδια μάσκα υποδικτύωσης με αυτήν που διαθέτει για την άμεσα συνδεδεμένη διεπαφή του.

- Εάν ο δρομολογητής δεν έχει διεπαφές που να ανήκουν στο ίδιο **ευρύτερο** δίκτυο με αυτό της ενημέρωσης που θα λάβει, τότε θα εφαρμόσει την προκαθορισμένη (default) μάσκα υποδικτύωσης της κλάσης στην οποία ανήκει η IP διεύθυνση δικτύου που περιλαμβάνεται στην ενημέρωση.

Με την λέξη **ευρύερο** δίκτυο εννοούμε το classful δίκτυο. Ας δώσουμε μερικά παραδείγματα:

A. η IP διεύθυνση 10.3.1.0 και η 10.5.5.0 ανήκουν στο ίδιο **ευρύτερο** δίκτυο (10.0.0.0).

B. Η IP διεύθυνση 10.1.4.5 και η 11.1.34.4 δεν ανήκουν στο ίδιο **ευρύτερο** δίκτυο.

C. Η IP διεύθυνση 192.168.1.1 και η 192.168.1.254 ανήκουν στο ίδιο **ευρύτερο** δίκτυο (192.168.1.0).

D. Η IP διεύθυνση 192.168.1.5 και η 192.167.2.5 δεν ανήκουν στο ίδιο **ευρύτερο** δίκτυο.

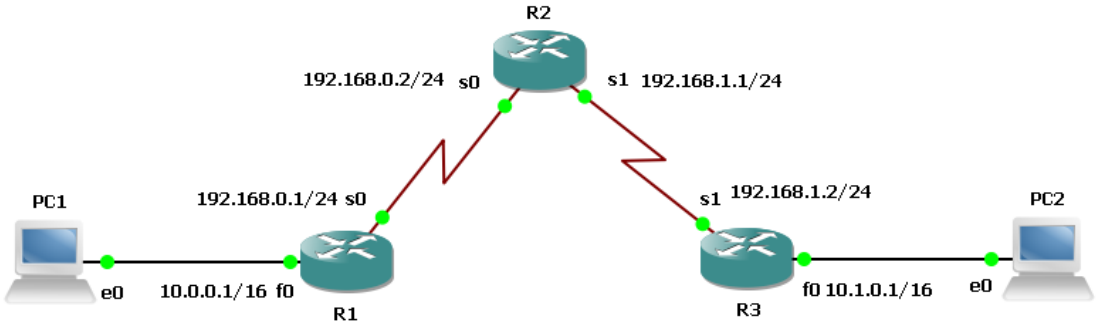
Στην Εικόνα 18 φαίνεται ένα παράδειγμα στο οποίο υποθέτουμε ότι το πρωτόκολλο δρομολόγησης είναι Classful (όπως το RIP). Σε κάποια φάση της λειτουργίας του δικτύου ο R2 στέλνει μια ενημέρωση δρομολόγησης στον R1 η οποία περιέχει την IP διεύθυνση του δικτύου 10.2.0.0. Ωστόσο, η ενημέρωση αυτή δεν συνοδεύεται και από

την μασκα υποδικτύωσης (η οποία στο παράδειγμα είναι η 255.255.0.0). Ο R1 πρέπει να επιλέξει μάσκα υποδικτύωσης η οποία θα εφαρμοστεί στο δίκτυο 10.2.0.0.

Εικόνα 18. Classful Δρομολόγηση.

Σύμφωνα με αυτά που αναφέρθηκαν προτύτερα, εάν ο R1 διαθέτει ένα interface το οποίο ανήκει στο ίδιο ευρύτερο δίκτυο με αυτό της ενημέρωσης που έλαβε (σε αυτή την περίπτωση θα είναι το 10.0.0.0) τότε θα εφαρμόσει την μάσκα υποδικτύωσης αυτού του interface. Για παράδειγμα, εάν εάν το interface e0 του R1 είχε την IP διεύθυνση 10.4.0.1/16 τότε ο R1 θα εφαρμόσει την μάσκα /16 στο δίκτυο 10.2.0.0 για το οποίο ενημερώθηκε από το πρωτόκολλο δρομολόγηση (σε αυτή την περίπτωση τυγχάνει να είναι η ίδια με αυτή που έχει το εν λόγω υποδίκτυο). Στην περίπτωση, όμως, που δεν έχει κανένα interface που να ανήκει στο ευρύτερο δίκτυο 10.0.0.0, τότε θα εφαρμοστεί η προκαθορισμένη μάσκα υποδικτύωσης της κλάσης στην οποία ανήκει η IP διεύθυνση δικτύου της ενημέρωσης. Δηλαδή, η /8 (255.0.0.0). Αυτό μπορεί να προκαλέσει προβλήματα στη διαδικασία της δρομολόγησης όπως θα αναλυθεί στο επόμενο παράδειγμα.

Υλοποιείστε, το δίκτυο που φαίνεται στην Εικόνα 19 ονομάζοντας το project ***Classful_Routing***.



Εικόνα 19. Το δίκτυο *RIP_OSPF* με ολοκληρωμένη την IP διευθυνσιοδότηση.

Δώστε τις παρακάτω εντολές στον δρομολογητή R1:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int f0

R1(config-if)#ip address 10.0.0.1 255.255.0.0

R1(config-if)#no shut
```

```
R1(config-if)#int s0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#router rip
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.0.0
```

Δώστε τις παρακάτω εντολές στον δρομολογητή R2:

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0
R2(config-if)#ip address 192.168.0.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#router rip
R2(config-router)#network 192.168.0.0
R2(config-router)#network 192.168.1.0
```

Δώστε τις παρακάτω εντολές στον δρομολογητή R3:

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int f0
R3(config-if)#ip address 10.1.0.1 255.255.0.0
R3(config-if)#no shut
R3(config-if)#int s1
R3(config-if)#ip address 192.168.1.2 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
```

```
R3(config)#router rip

R3(config-router)#network 10.1.0.0

R3(config-router)#network 192.168.1.0
```

Ρυθμίσαμε όλα τα interface των δρομολογητών με τις κατάλληλες IP διευθύνσεις και ενεργοποιήσαμε το RIP πρωτόκολλο σε κάθε δρομολογητή. Στη συνέχεια ας εμφανίσουμε τους πίνακες δρομολόγησης στους δρομολογητές:

Στον R1:

```
R1#show ip route

     10.0.0.0/16 is subnetted, 1 subnets

C       10.0.0.0 is directly connected, FastEthernet0

C    192.168.0.0/24 is directly connected, Serial0

R    192.168.1.0/24 [120/1] via 192.168.0.2, 00:00:09, Serial0
```

Παρατηρούμε την προσθήκη μιας διαδρομής προς το υποδίκτυο 192.168.1.0/24 μέσω της 192.168.0.2 αλλά απουσιάζει το δίκτυο 10.1.0.0/16!

Στον R3 θα δούμε κάτι ανάλογο:

```
R3#show ip route

     10.0.0.0/16 is subnetted, 1 subnets

C       10.1.0.0 is directly connected, FastEthernet0

R    192.168.0.0/24 [120/1] via 192.168.1.1, 00:00:24, Serial1

C    192.168.1.0/24 is directly connected, Serial1
```

Στον R3 υπάρχει μια καταχώρηση για το υποδίκτυο 192.168.0.0/24 αλλά όχι για το 10.0.0.0/16!

Η αποκάλυψη του προβλήματος θα προκύψει από την εμφάνιση του πίνακα δρομολόγησης στον R2:

```
R2#show ip route

R    10.0.0.0/8 [120/1] via 192.168.1.2, 00:00:07, Serial1

                [120/1] via 192.168.0.1, 00:00:15, Serial0
```

```
C    192.168.0.0/24 is directly connected, Serial0

C    192.168.1.0/24 is directly connected, Serial1
```

Πράγματι! Παρατηρείστε ότι υπάρχει μια περίεργη καταχώρηση για το υποδίκτυο 10.0.0.0/8 μέσω δύο (!) διαφορετικών διαδρομών οι οποίες, μάλιστα, έχουν το ίδιο administrative distance (120) και το ίδιο metric (1).

Ο λόγος αυτής της ιδιόμορφης καταχώρησης στον πίνακα δρομολόγησης του R2 είναι ότι κατά την λήψη των ενημερώσεων για τα υποδίκτυα 10.0.0.0/16 και 10.1.0.0/16 από τους R1 και R2, αντίστοιχα, ο R2 δεν γνωρίζει ποια μάσκα υποδικτύωσης να εφαρμόσει σε αυτά τα υποδίκτυα και αποφασίζει να εφαρμόσει την default για την κλάση των υποδικτύων αυτών, δηλαδή την 255.0.0.0 (/8). Έτσι, η επικοινωνία μεταξύ των PC1 και PC2 καθίσταται αδύνατη. Πράγματι εάν προσπαθήσετε να κάνετε ping από τον PC1 στον PC2 δεν θα λάβετε καμία απόκριση.

Το παράδειγμα αυτό αναδυκνύει την αδυναμία των classful πρωτοκόλλων δρομολόγησης (όπως το RIPv1) να εφαρμόσουν σωστές καταχωρήσεις δρομολόγησης εξαιτίας της μη αποστολής των μασκών υποδικτύωσης στις ενημερώσεις τους.

Η λύση στο πρόβλημα για το δίκτυο του παραδείγματος είναι η εφαρμογή ενός classless πρωτοκόλλου δρομολόγησης, όπως το OSPF.

Εφαρμόστε το OSPF στον R1 ως εξής:

```
R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#no router rip

R1(config)#router ospf 1

R1(config-router)#network 10.0.0.1 0.0.0.0 area 1

R1(config-router)#network 192.168.0.1 0.0.0.0 area 1
```

Στον R2 δώστε τις παρακάτω εντολές:

```
R2(config)#no router rip

R2(config)#router ospf 1

R2(config-router)#network 192.168.0.0 0.0.255.255 area 1
```

Τέλος, στον R3:

```
R3#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#no router rip

R3(config)#router ospf 1

R3(config-router)#network 10.1.0.1 0.0.0.0 area 1

R3(config-router)#network 192.168.1.2 0.0.0.0 area 1
```

Τώρα μπορούμε να ελέγξουμε τους πίνακες δρομολόγησης των δρομολογητών. Για τον R1:

```
R1#show ip route

C       10.0.0.0 is directly connected, FastEthernet0

O       10.1.0.0 [110/129] via 192.168.0.2, 00:01:12, Serial0

C    192.168.0.0/24 is directly connected, Serial0

O    192.168.1.0/24 [110/128] via 192.168.0.2, 00:03:56, Serial0
```

Βλέπουμε ότι, σε αντίθεση με την περίπτωση του RIP, στον πίνακα δρομολόγησης του R1 υπάρχουν καταχωρήσεις και για τα δυο υποδίκτυα 10.1.0.0/16 και 192.168.1.0/16.

Στον R3:

```
R3#show ip route

     10.0.0.0/16 is subnetted, 2 subnets

O       10.0.0.0 [110/129] via 192.168.1.1, 00:07:15, Serial1

C       10.1.0.0 is directly connected, FastEthernet0

O    192.168.0.0/24 [110/128] via 192.168.1.1, 00:07:15, Serial1

C    192.168.1.0/24 is directly connected, Serial1
```

Ανάλογα και στον R3 η καταχώρηση που έλειπε για το δίκτυο 10.0.0.0/16, τώρα βρίσκεται στον πίνακα δρομολόγησης.

Τέλος, στον R2:

```
R2#show ip route

     10.0.0.0/16 is subnetted, 2 subnets

O       10.0.0.0 [110/65] via 192.168.0.1, 00:11:23, Serial0

O       10.1.0.0 [110/65] via 192.168.1.2, 00:08:48, Serial1
```

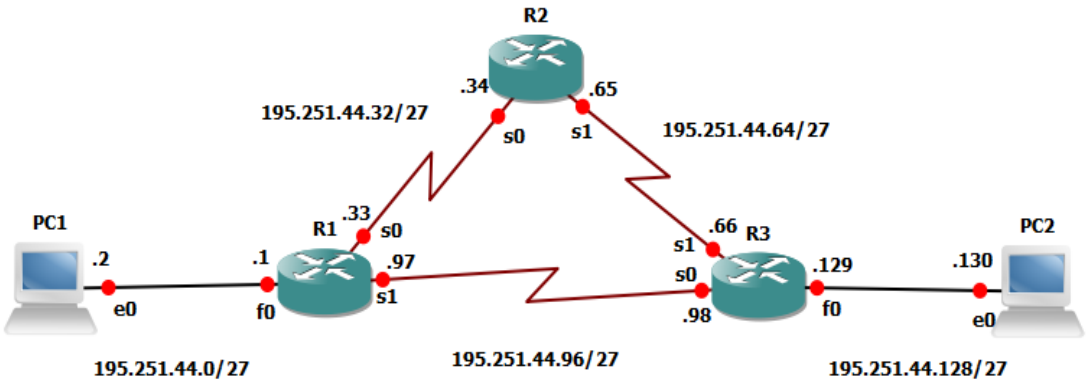
```
C    192.168.0.0/24 is directly connected, Serial0

C    192.168.1.0/24 is directly connected, Serial1
```

Φαίνεται ξεκάθαρα η ύπαρξη των υποδικτύων 10.0.0.0/16 και 10.1.0.0/16 ως διακριτές καταχωρήσεις. Εάν ελέγξουμε την επικοινωνία των PC1 και PC2 με την εντολή ping, θα πρέπει να είμαστε σε θέση να λάβουμε επιτυχώς αποκρίσεις.

6.5.5 Σύγκριση του OSPF και του RIP με βάση το κριτήριο δρομολόγησης

Σε αυτή τη παράγραφο θα επιχειρήσουμε μια σύγκριση των δυο πρωτοκόλλων δρομολόγησης που περιγράφηκαν προηγουμένως με βάση το κριτήριο δρομολόγησης που χρησιμοποιεί το κάθε ένα. Για τον σκοπό αυτό κατασκευάστε στο GNS3 το δίκτυο που φαίνεται στην Εικόνα 20 και ονομάστε το project *RIP_OSPF*.

Αρχικά ας ρυθμίσουμε τους δρομολογητές με τις απαραίτητες IP διευθύνσεις και ας ενεργοποιήσουμε το πρωτόκολλο RIP σε αυτούς.



Εικόνα 20. Το δίκτυο *RIP_OSPF* με ολοκληρωμένη την IP διευθυνσιοδότηση.

Για τον δρομολογητή R1 εκτελέστε τις παρακάτω εντολές:

```
R1>

R1>en

R1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#int f0

R1(config-if)#ip address 195.251.44.1 255.255.255.224

R1(config-if)#no shut

R1(config-if)#int s0

R1(config-if)#ip address 195.251.44.33 255.255.255.224
```

```
R1(config-if)#no shut

R1(config-if)#int s1

R1(config-if)#ip address 195.251.44.97 255.255.255.224

R1(config-if)#bandwidth 64

R1(config-if)#no shut

R1(config-if)#router rip

R1(config-router)#network 195.251.44.0
```

Παρατηρείστε ότι ορίσαμε το bandwidth της ζεύξης στην οποία είναι συνδεδεμένο το s1 να είναι 64 Kbit/s. Να σημειώσουμε εδώ ότι η προκαθορισμένη τιμή bandwidth των σειριακών ζεύξεων είναι 1.544 Mbit/s. Η εντολή που δόθηκε για να ορίσει το bandwidth δεν αλλάζει την πραγματική χωρητικότητα της ζεύξης ωστόσο το IOS της συσκευής λαμβάνει υπόψιν του αυτή τη ρύθμιση για την κατασκευή των πινάκων δρομολόγησης.

Για τον δρομολογητή R2 εκτελέστε τις παρακάτω εντολές:

```
R2>en

R2#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R2(config-if)#int s0

R2(config-if)#ip address 195.251.44.34 255.255.255.224

R2(config-if)#no shut

R2(config-if)#int s1

R2(config-if)#ip address 195.251.44.66 255.255.255.224

R2(config-if)#no shut

R2(config-if)#router rip

R2(config-router)#network 195.251.44.0
```

Για τον δρομολογητή R3 εκτελέστε τις παρακάτω εντολές:

```
R3>en

R3#config t

Enter configuration commands, one per line.  End with CNTL/Z.

R3(config)#int f0
```

```
R3(config-if)#ip address 195.251.44.129 255.255.255.224

R3(config-if)#no shut

R3(config)#int s0

R3(config-if)#ip address 195.251.44.98 255.255.255.224

R3(config-if)#bandwidth 64

R3(config-if)#no shut

R3(config-if)#int s1

R3(config-if)#ip address 195.251.44.66 255.255.255.224

R3(config-if)#no shut

R3(config-if)#router rip

R3(config-router)#network 195.251.44.0
```

Παρατηρείστε ότι ορίσαμε το bandwidth της ζεύξης στην οποία είναι συνδεδεμένο το s0 να είναι 64 Kbit/s.

Τώρα ρυθμίστε τον PC1:

```
PC1> ip 195.251.44.2 255.255.255.224 195.251.44.1

Checking for duplicate address...

PC1 : 195.251.44.2 255.255.255.224 gateway 195.251.44.1
```

Τώρα ρυθμίστε τον PC2:

```
PC2> ip 195.251.44.130 255.255.255.224 195.251.44.129

Checking for duplicate address...

PC1 : 195.251.44.130 255.255.255.224 gateway 195.251.44.129
```

Για να επαληθεύσετε την λειτουργία του δικτύου εκτελέστε την εντολή `ping` στον PC2 με προορισμό τον PC1:

```
PC2> ping 195.251.44.2

195.251.44.2 icmp_seq=1 timeout

84 bytes from 195.251.44.2 icmp_seq=2 ttl=62 time=46.875 ms

84 bytes from 195.251.44.2 icmp_seq=3 ttl=62 time=46.875 ms

84 bytes from 195.251.44.2 icmp_seq=4 ttl=62 time=31.250 ms

84 bytes from 195.251.44.2 icmp_seq=5 ttl=62 time=31.250 ms
```

Βλέπουμε ότι οι ρυθμίσεις έγιναν σωστά καθώς ο PC2 επικοινωνεί με τον PC1. Αυτό μπορείτε να το επαληθεύσετε και κοιτάζοντας τα routing tables των δρομολογητών στα οποία θα πρέπει να φαίνονται οι καταχωρήσεις με το RIP πρωτόκολλο.

Εξετάζοντας την Εικόνα 17 βλέπουμε ότι υπάρχουν δυο εναλλακτικές διαδρομές από τον PC2 στον PC1: η μία μέσω των δρομολογητών R3 και R1 και η άλλη μέσω των δρομολογητών R3, R2 και R1. Δεδομένου ότι το κριτήριο δρομολογησης του RIP είναι ο ελάχιστος αριθμός δρομολογητών η διαδρομή που θα ακολουθηθεί είναι προφανώς η πρώτη. Αυτό μπορεί να εξακριβωθεί εκτελώντας την εντολή `trace` στον PC2 με προορισμό τον PC1:

```
PC2> trace 195.251.44.2

trace to 195.251.44.2, 8 hops max, press Ctrl+C to stop

 1    195.251.44.129   0.000 ms  0.000 ms  31.250 ms

 2    195.251.44.97    31.250 ms  62.500 ms  31.250 ms

 3    *195.251.44.2    31.250 ms (ICMP type:3, code:3, Destination port
unreachable)
```

Με το πρωτόκολλο OSPF η διαδρομή μπορεί να αλλάξει, σύμφωνα με το bandwidth τις κάθε ζεύξης. Το κόστος κάθε διασύνδεσης είναι αντιστρόφως ανάλογο με το εύρος ζώνης της, επομένως, ένα υψηλότερο εύρος ζώνης σημαίνει χαμηλότερο κόστος.

Ας ενεργοποιήσουμε το OSPF και ας εξετάσουμε την διαδρομή που ακολουθούν τα πακέτα αυτή τη φορά.

Για τον δρομολογητή R1 εκτελέστε τις παρακάτω εντολές:

```
R1(config)#no router rip

R1(config)#router ospf 1

R1(config-router)#network 195.251.44.0 0.0.0.255 area 1
```

Για τον δρομολογητή R2 εκτελέστε τις παρακάτω εντολές:

```
R2(config)#no router rip

R2(config)#router ospf 2

R2(config-router)#network 195.251.44.0 0.0.0.255 area 1
```

Για τον δρομολογητή R3 εκτελέστε τις παρακάτω εντολές:

```
R3(config)#no router rip

R3(config)#router ospf 3

R3(config-router)#network 195.251.44.0 0.0.0.255 area 1
```

Για να επαληθεύσετε την λειτουργία του δικτύου εκτελέστε την εντολή `ping` στον PC2 με προορισμό τον PC1:

```
PC2> ping 195.251.44.2

84 bytes from 195.251.44.2 icmp_seq=1 ttl=61 time=78.125 ms

84 bytes from 195.251.44.2 icmp_seq=2 ttl=61 time=78.125 ms

84 bytes from 195.251.44.2 icmp_seq=3 ttl=61 time=78.125 ms

84 bytes from 195.251.44.2 icmp_seq=4 ttl=61 time=62.500 ms

84 bytes from 195.251.44.2 icmp_seq=5 ttl=61 time=78.125 ms
```

Τώρα εκτελέστε την εντολή `trace` στον PC2 με προορισμό τον PC1:

```
PC2> trace 195.251.44.2

trace to 195.251.44.2, 8 hops max, press Ctrl+C to stop

 1    195.251.44.129   15.625 ms  0.000 ms  0.000 ms

 2    195.251.44.65    62.500 ms  31.250 ms  31.250 ms

 3    195.251.44.33    62.500 ms  62.500 ms  62.500 ms

 4    *195.251.44.2    62.500 ms (ICMP type:3, code:3, Destination port
unreachable)
```

Παρατηρείστε ότι με το OSPF η διαδρομή που επιλέχθηκε για τον προορισμό (PC1) είναι αυτή μέσω των δρομολογητών R3, R2 και R1 διότι αυτή διαθέτει το μεγαλύτερο bandwidth.

7. Access Control Lists

Μια λίστα πρόσβασης (Access Control List – ACL) είναι ουσιαστικά ένα φίλτρο πακέτων (packet filter) με στόχο τον έλεγχο των πακέτων που επιτρέπεται να έχουν πρόσβαση σε πόρους όπως servers. Μια ACL είναι ουσιαστικά μια λίστα από συνθήκες οι οποίες κατηγοριοποιούν πακέτα. Η ρύθμιση τους μοιάζει πολύ με τον προγραμματισμό διαδοχικών if-then συνθηκών: εάν μια συνθήκη ικανοποιηθεί, τότε λαμβάνει χώρας μια συγκεκριμένη ενέργεια. Εάν δεν ικανοποιηθεί η συνθήκη τότε δεν εκτελείται καμία ενέργεια. Απλά προχωράμε στον επόμενο έλεγχο συνθήκης.

Συνολικά υπάρχουν τρία είδη ACL αλλά εμάς θα μας απασχολήσουν οι δυο παρακάτω κατηγορίες:

- *Standard ACL:* Αυτές οι ACL περιλαμβάνουν μόνο την IP διεύθυνση πηγής ως έλεγχο συνθήκης. Δεν λαμβάνουν υπόψιν στοιχεία όπως είναι το πρωτόκολλο επιπέδου μεταφοράς (TCP-UDP) ή τις θύρες (ports).

- *Extended ACL:* Αυτές οι ACL μπορούν να χρησιμοποιήσουν ως συνθήκη πεδία των πρωτοκόλλων επιπέδου-3 και 4 (τύπος πρωτοκόλλου, θύρα, IP διεύθυνση κλπ)

Η κάθε κατηγορία ACL χωρίζεται σε δύο άλλες υποκατηγορίες ανάλογα με το αν εφαρμόζονται σε εισερχόμενη κίνηση ή εξερχόμενη κίνηση σε έναν δρομολογητή:

- *ACL εισερχομένης κίνησης (inbound ACL)*: σε αυτή τη περίπτωση η ACL εφαρμόζεται στα πακέτα πριν ακόμα αυτά δρομολογηθούν προς την διεπαφή εξόδου.

- *ACL εξερχομένης κίνησης (outbound ACL)*: σε αυτή τη περίπτωση η ACL εφαρμόζεται στα πακέτα που έχουν δρομολογηθεί στην εξερχόμενη διεπαφή του δρομολογητή

Για τις ανάγκες αυτού του εργαστηριακού οδηγού θα επικεντρωθούμε στις Standard και Extended ACL. Πριν προχωρήσουμε με τις εφαρμογές των ACL θα πρέπει να αναφέρουμε ότι υπάρχει μια σειρά από γενικές σχεδιαστικές οδηγίες-συμβουλές τις οποίες μπορεί κανείς να εφαρμόσει όταν υλοποιεί ACLs:

1. Μια μόνο ACL μπορεί να εφαρμοστεί ανά διεπαφή ανά πρωτόκολλο ανά κατεύθυνση. Αυτό σημαίνει ότι όταν εφαρμόζουμε μια IP ACL, μπορούμε να έχουμε μόνο μια ACL εισερχομένης κίνησης και μια μόνο ACL εξερχομένης κίνησης ανά διεπαφή.

2. Όταν συντάσσουμε τις ACL, τότε οι έλεγχοι των συνθηκών που είναι πιο συγκεκριμένες πρέπει να γίνονται πρώτες.

3. Κάθε νέα προσθήκη στην ACL τοποθετείται στο τέλος της λίστας.

4. Δεν μπορούμε να αφαιρέσουμε μια μόνο καταχώρηση από την λίστα. Πρέπει να αφαιρέσουμε όλη την ACL.

5. Εάν ένα πακέτο δεν κατηγοριοποιηθεί από τους ελέγχους των συνθηκών τότε αυτό απορρίπτεται (είναι η προκαθορισμένη επιλογή).

6. Πρώτα δημιουργούμε τις ACL και κατόπιν τις εφαρμόζουμε σε διεπαφή.

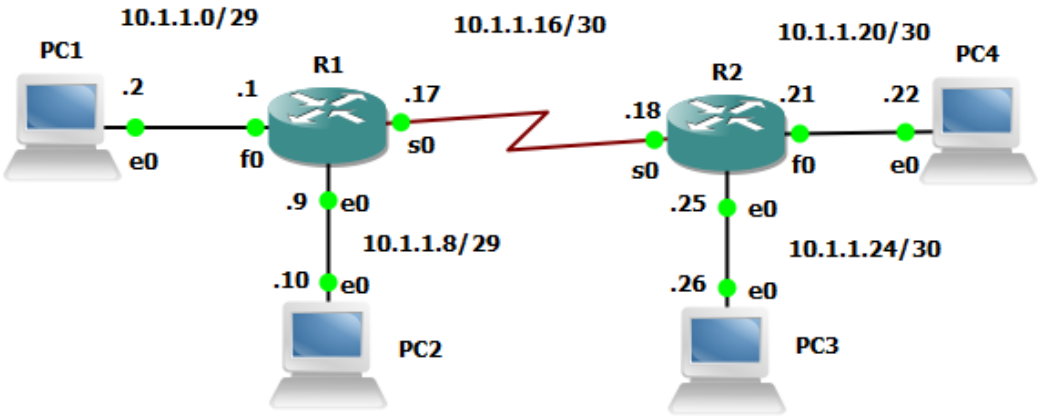
7. Οι ACL φιλτράρουν κίνηση που διέρχεται του δρομολογητή. Δεν φιλτράρουν κίνηση η οποία προέρχεται ή προορίζεται για τον δρομολογητή.

8. Τοποθετούμε την standard ACL κοντύτερα στον προορισμό που θέλουμε να προστατεύσουμε, όσο αυτό είναι εφικτό. Ο λόγος είναι ότι φιλτράρουμε κίνηση με συνθήκη τις IP διευθύνσεις αποστολέα και μια τοποθέτηση κοντά στον αποστολέα θα έχει επίπτωση σε όλους τους πιθανούς προορισμούς.

Τοποθετούμε μια extended ACL κοντύτερα στην πηγή κίνησης που θέλουμε να φιλτράρουμε, όσο αυτό είναι εφικτό. Επειδή με αυτού του είδους τις ACL μπορούμε να φιλτράρουμε κίνηση με βάση πολλά πεδία επικεφαλίδων, αν βάζαμε τις extended ACL κοντύτερα στον προορισμό που θέλουμε να προστατεύσουμε τότε θα επιτρέπαμε στην κίνηση η οποία τελικά θα φιλτραριστεί να διανύσει μεγάλο μέρος του δικτύου χωρίς λόγο (αφού αυτή τελικά θα απορριφθεί από την ACL). Πράγμα που θα σπαταλούσε πολύτιμους δικτυακούς πόρους.

7.1 Standard ACL

Ξεκινώντας από τις Standard ACL, θα τις εφαρμόσουμε στην δικτυακή τοπολογία που εικονίζεται στην Εικόνα 21. Ονομάστε το project <**Το ΑΕΜ σας**>**_std_ACL.** Υλοποιείστε το δίκτυο όπως φαίνεται στην εικόνα με τις IP διευθύνσεις που φαίνονται. Ενεργοποιείστε το OSPF πρωτόκολλο στους δρομολογητές.



Εικόνα 21. Το δίκτυο για την υλοποίηση των standard ACL.

Έστω ότι επιθυμούμε να προστατεύσουμε τον PC4 από πιθανή πρόσβαση προερχόμενη από τον PC1. Ωστόσο, όλοι οι υπόλοιποι κόμβοι θα πρέπει να μπορούν

να έχουν πρόσβαση στον PC4, όπως επίσης και ο PC1 θα πρέπει να έχει πρόσβαση σε όλους τους υπόλοιπους κόμβους εκτός του PC4.

Σύμφωνα με αυτές τις προδιαγραφές και βασιζόμενοι στην σχεδιαστική οδηγία-συμβουλή 8 που αναφέραμε μόλις πριν το σημείο στο οποίο θα πρέπει να εφαρμόσουμε την ACL είναι ο δρομολογητής R2. Επειδή στον R2 είναι συνδεδεμένος και ο PC3 προς τον οποίο δεν επιθυμούμε να κόψουμε την πρόσβαση από τον PC1 φαίνεται λογικό η ACL να τοποθετηθεί στο `f0` interface του R2 ως outbound ACL (ACL εξερχομένης κίνησης).

Συνδεόμαστε με την κονσόλα του R2 και δίνουμε τις εξής εντολές:

```
R2(config)#access-list ?

  <1-99>            IP standard access list

  <100-199>         IP extended access list

  <1100-1199>       Extended 48-bit MAC address access list

  <1300-1999>       IP standard access list (expanded range)

  <200-299>         Protocol type-code access list

  <2000-2699>       IP extended access list (expanded range)

  <700-799>         48-bit MAC address access list

  dynamic-extended  Extend the dynamic ACL absolute timer

  rate-limit        Simple rate-limit specific access list
```

Παρατηρούμε ότι υπάρχει μια γκάμα από ACL. Εμείς επιθυμούμε τις standard ACL. Θα πρέπει να επιλέξουμε έναν αριθμό ο οποίος θα προσδιορίζει μοναδικά την ACL:

```
R2(config)#access-list 1 ?

  deny    Specify packets to reject

  permit  Specify packets to forward

  remark  Access list entry comment
```

Εδώ επιλέγουμε αν θέλουμε να επιτρέπεται η διέλευση πακέτων με συγκεκριμένες IP διευθύνσεις ή όχι.

```
R2(config)#access-list 1 deny ?

  Hostname or A.B.C.D  Address to match

  any                  Any source host

  host                 A single host address
```

Τώρα θα πρέπει να ορίσουμε τις IP διευθύνσεις (εάν πρόκειται για σύνολο) ή την IP διεύθυνση που θέλουμε να αρνηθούμε διέλευση.

```
R2(config)#access-list 1 deny 10.1.1.2
```

Τώρα δημιουργήσαμε μια standard ACL η οποία διαθέτει μέχρι στιγμής έναν έλεγχο συνθήκης ο οποίος ελέγχει τα πακέτα που διέρχονται του δρομολογητή και εάν αυτά έχουν ως IP διεύθυνση αποστολέα την 10.1.1.2, τότε αυτά απορρίπτονται. Τι συμβαίνει όμως στα υπόλοιπα πακέτα που διέρχονται από τον δρομολογητή και δεν ικανοποιούν την συνθήκη αυτή; Και αυτά απορρίπτονται! Είναι αποτέλεσμα της οδηγίας-συμβουλής 5. Σκεφθείτε ότι στο τέλος της κάθε λίστας υπάρχει μια εντολή του τύπου **`access-list 1 deny any`**. Επομένως, θα πρέπει να δώσουμε μια ακόμα εντολή πριν ολοκληρώσουμε την ACL:

```
R2(config)#access-list 1 permit any
```

Αυτό σημαίνει ότι οποιοδήποτε πακέτο δεν ικανοποιεί την πρώτη συνθήκη θα επιτραπεί να περάσει. Αυτό είναι άλλωστε αυτό που ζητάμε: οι υπόλοιποι κόμβοι να έχουν κανονικά πρόσβαση στον PC4. Παρατηρείστε ότι η αλληλουχία των εντολών-συνθηκών που ορίσαμε στον δρομολογητή ακολουθούν την οδηγία-συμβουλή 2.

Πριν ολοκληρώσουμε θα πρέπει να εφαρμόσουμε την ACL 1 στην διεπαφή `f0` του R2:

```
R2(config)#int f0
```

```
R2(config-if)#ip access-group 1 out
```

Εδώ εφαρμόζουμε την ACL 1 στο interface `f0` και ορίζουμε ότι θα είναι μια ACL εξερχομένης κίνησης του `f0`.

Ελέγξτε τις ρυθμίσεις που κάνατε εκτελώντας ping από τον PC1 στον PC3 και PC4:

```
PC1> ping 10.1.1.26 -l 32

60 bytes from 10.1.1.26 icmp_seq=1 ttl=62 time=15.625 ms

60 bytes from 10.1.1.26 icmp_seq=2 ttl=62 time=15.625 ms

60 bytes from 10.1.1.26 icmp_seq=3 ttl=62 time=15.625 ms

60 bytes from 10.1.1.26 icmp_seq=4 ttl=62 time=0.000 ms

60 bytes from 10.1.1.26 icmp_seq=5 ttl=62 time=15.625 ms


PC1> ping 10.1.1.22 -l 32

*10.1.1.18 icmp_seq=1 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)
```

```
*10.1.1.18 icmp_seq=2 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)

*10.1.1.18 icmp_seq=3 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)

*10.1.1.18 icmp_seq=4 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)

*10.1.1.18 icmp_seq=5 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)
```

Παρατηρείστε ότι η εντολή είναι επιτυχής για τον PC3 ενώ στην περίπτωση του PC4 ο δρομολογητής R2 (10.1.1.18) στον οποίο έχει εφαρμοστεί το φίλτρο απαντά με ICMP μήνυμα `type:3, code:13, Communication administratively prohibited` όπως ορίζεται από το *RFC 1812-Requirements for IP Version 4 Routers* (σελ. 80-82).

Εάν επιθυμούμε να αποκόψουμε την πρόσβαση από ένα σύνολο IP διευθύνσεων (π.χ. από τους υπολογιστές ενός υποδικτύου) τότε στις εντολές της ACL θα πρέπει να χρησιμοποιήσουμε wildcards.

Συνεχίζοντας το προηγούμενο παράδειγμα υποθέστε ότι για κάποιον λόγο πρέπει να αποκοπεί η πρόσβαση στον PC3 από όλους τους υπολογιστές (hosts) του υποδικτύου 10.1.1.8/29. Στο σχήμα φαίνεται ότι υπάρχει μόνο ένας υπολογιστής σε αυτό το υποδίκτυο αλλά θα μπορούσαν να υπάρχουν και άλλοι 4 (με τη χρήση ενός switch/hub φυσικά).

Για να αποκόψουμε την κίνηση που έχει προορισμό τον PC3 και προέρχεται από το υποδίκτυο 10.1.1.8/29 θα πρέπει να φτιάξουμε μια νέα standard ACL:

```
R2(config)#access-list 2 deny 10.1.1.8 0.0.0.7

R2(config)#access-list 2 permit any

R2(config)#int e0

R2(config-if)#ip access-group 2 out
```

Το wildcard στην πρώτη εντολή δηλώνει όλες τις IP διευθύνσεις που ανήκουν στο υποδίκτυο 10.1.1.8/29 και προκύπτει από αν αφαιρέσουμε από το 255 το 248 που είναι η τιμή του τέταρτου byte της subnet mask. Εάν τοποθετούσαμε 255 αντί για 7 στο wildcard τότε όλες οι IP διευθύνσεις που θα ξεκινούσαν από 10.1.1 θα κοβόταν.

Για επιβεβαίωση κάντε ping από τον PC2 προς τους PC4 και PC3:

```
PC2> ping 10.1.1.22

10.1.1.22 icmp_seq=1 timeout

10.1.1.22 icmp_seq=2 timeout

84 bytes from 10.1.1.22 icmp_seq=3 ttl=62 time=0.000 ms
```

```
84 bytes from 10.1.1.22 icmp_seq=4 ttl=62 time=15.625 ms

84 bytes from 10.1.1.22 icmp_seq=5 ttl=62 time=15.625 ms
```

Πρόσβαση στον PC4 εξακολουθεί να υπάρχει.

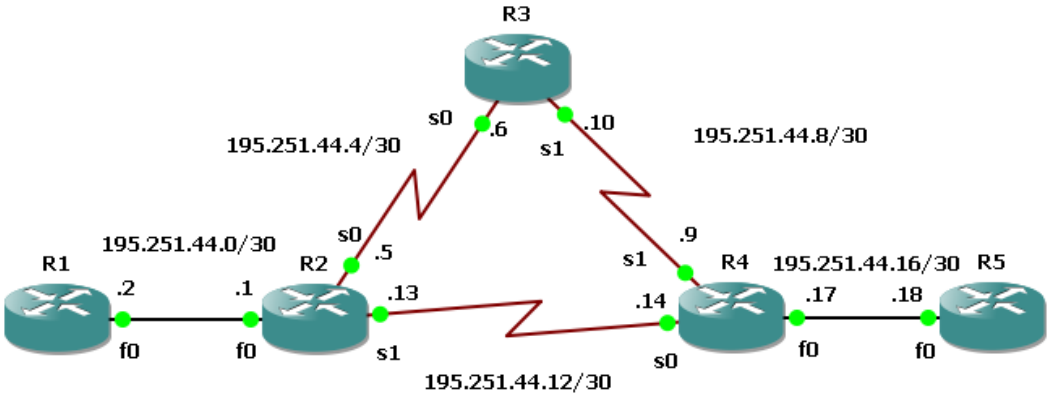
```
PC2> ping 10.1.1.26

*10.1.1.18 icmp_seq=1 ttl=254 time=0.000 ms (ICMP type:3, code:13,
Communication administratively prohibited)

*10.1.1.18 icmp_seq=2 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)

*10.1.1.18 icmp_seq=3 ttl=254 time=0.000 ms (ICMP type:3, code:13,
Communication administratively prohibited)

*10.1.1.18 icmp_seq=4 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)

*10.1.1.18 icmp_seq=5 ttl=254 time=15.625 ms (ICMP type:3, code:13,
Communication administratively prohibited)
```

Η πρόσβαση στον PC3 είναι απαγορευμένη.

7.2 Extended ACL

Ευκολα μπορεί να παρατηρήσει κανείς ότι με τις standard ACL το μοναδικό κριτήριο για την σύνταξη συνθηκών είναι η IP διεύθυνση αποστολέα. Εάν για παράδειγμα επιθυμούσαμε να επιτρέψουμε την πρόσβαση ενός κόμβου στην υπηρεσία HTTP ενός server αλλά να του απαγορέψουμε την πρόσβαση μέσω telnet, αυτό δεν θα ήταν εφικτό με τις standard ACL.

Για να δούμε τον τρόπο με τον οποίο εφαρμόζονται οι extended ACL, ετοιμάστε στον GNS3 την τοπολογία της Εικόνας 22 με τις IP διευθύνσεις που φαίνονται σε αυτή. Ονομάστε το project <**Το ΑΕΜ σας**>**_ext_ACL** και ενεργοποιήστε το OSPF ως πρωτόκολλο δρομολόγησης σε όλους τους δρομολογητές. Ειδικά στον R5 ενεργοποιήστε την πρόσβαση μέσω telnet και ορίστε το password: **cisco**. Επίσης στον R5, ορίστε το secret password: **abcd**.



Εικόνα 22. Το δίκτυο για την υλοποίηση των extended ACL.

Επιθυμούμε να απαγορεύσουμε την πρόσβαση μέσω telnet από τον R1 προς τον R2 αλλά όχι άλλων υπηρεσιών. Σύμφωνα με την οδηγία 9 θα πρέπει να τοποθετήσουμε την ACL όσο γίνεται κοντύτερα στην πηγή της κίνησης που θέλουμε να απαγορεύσουμε. Εφόσον υπάρχει η δυνατότητα θα πρέπει να την τοποθετήσουμε στον R2 δηλαδή.

Πριν ακόμα ορίσουμε την ACL δοκιμάστε την ping από τον R1 προς τον R5:

```
R1#ping 195.251.44.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.251.44.18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/56/92 ms
```

Θα πρέπει να έχετε απιτυχή σύνδεση. Δοκιμάστε ακόμα την σύνδεση από τον R1 προς τον R5 με την χρήση telnet:

```
R1#telnet 195.251.44.18
Trying 195.251.44.18 ... Open
User Access Verification
Password:
R5>exit
```

Και τώρα θα πρέπει να μπορείτε να συνδεθείτε επιτυχώς στην κονσόλα του δρομνολογητή R5.

Για να μπορέσουμε να εφαρμόσουμε την πολιτική ασφαλείας που αναφέραμε προηγουμένως θα πρέπει να συνδεθείτε στην κονσόλα του R2 και να δώσετε τις παρακάτω εντολές:

```
R2(config)#$access-list 101 deny tcp host 195.251.44.2 host 195.251.44.18 eq 23

R2(config)#access-list 101 permit ip any any

R2(config)#int f0

R2(config-if)#ip access-group 101 in
```

Στην πρώτη εντολή δημιουργούμε την extended ACL με χαρακτηριστικό αριθμό 101. Επίσης, ορίζουμε ότι θα πρέπει να απορριφθούν τα πακέτα που χρησιμοποιούν το TCP πρωτόκολλο (το telnet χρησιμοποιεί το TCP), έχουν ως αποστολέα τον 195.251.44.2 (R1), έχουν ως προορισμό τον 195.251.44.18 (R5) και έχουν ως θύρα προορισμού (destination port) την θύρα 23. Το «**eq**» σημαίνει equal. Χρησιμοποιείστε το "?" για να δείτε όλες τις επιλογές.

Στην δεύτερη εντολή γινόμαστε λίγο πιο γενικοί δηλώνοντας ότι επιτρέπεται οποιαδήποτε IP κίνηση από οποιονδήποτε αποστολέα προς οποιονδήποτε παραλήπτη. Χωρίς αυτή την εντολή όλη η κίνηση του R1 προς οποιονδήποτε άλλο κόμβο θα απορριπτέται καθώς στο τέλος κάθε λίστας υπονοείται η ύπαρξη μιας εντολής `deny any any` (οδηγία 5).

Οι δύο τελευταίες εντολές εφαρμόζουν την λίστα στο `f0` του R1 και ορίζουν την λίστα ως λίστα εισερχομένης κίνησης.

Μπορείτε να πειραματιστείτε με τις extended ACL υλοποιώντας μια ACL για την απαγόρευση της telnet πρόσβασης του R3 προς τον R5. Σκεφθείτε εδώ ότι υπάρχει περίπτωση το πρωτόκολλο δρομολόγησης να αλλάξει την διαδρομή προς τον προορισμό. Που θα τοποθετούσατε την λίστα;

Μπορείτε να χρησιμοποιήσετε τις εντολές `show access-list` και `show ip access-lists` για να δείτε τον αριθμό και το είδος των λιστών πρόσβασης που έχουν εφαρμοστεί στον δρομολογητή.

8. Network Address Translation

Η μέθοδος Network Address Translation (NAT) είναι ο λόγος για τον οποίο δεν έχουν εξαντληθεί οι IPv4 διευθύνσεις σήμερα. Η τεχνική αυτή επιτρέπει την αντιστοίχιση ιδιωτικών (private) IP διευθύνσεων (10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.16.31.255, 192.168.0.0 – 192.168.255.255) σε μία ή περισσότερες δημόσιες (public).

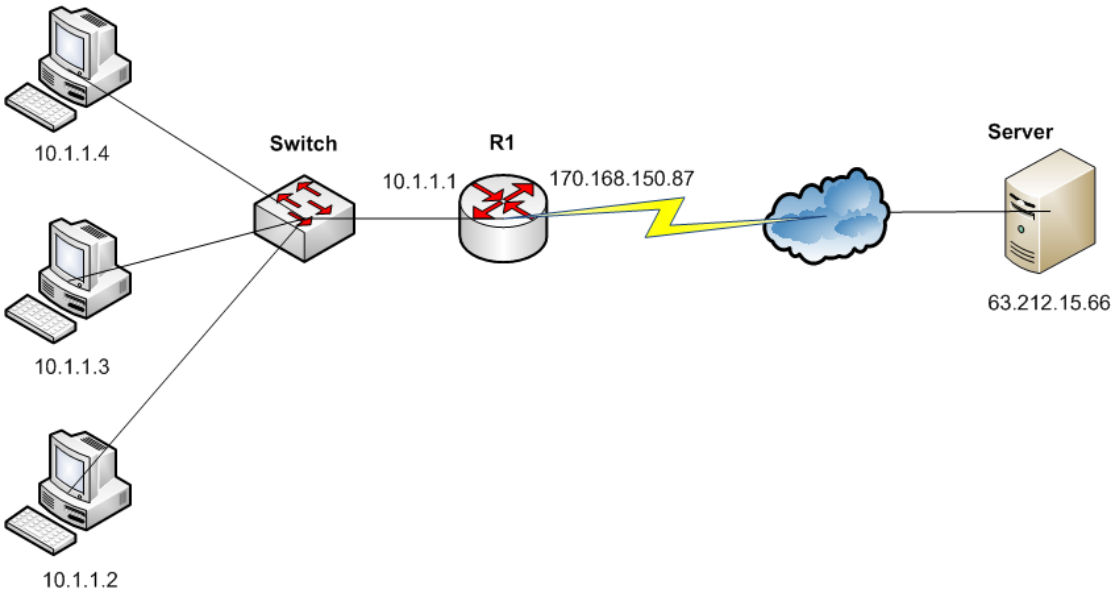
Με τον τρόπο αυτό μπορούμε να έχουμε ένα τοπικό δίκτυο στους κόμβους του οποίου έχουν ανατεθεί ιδιωτικές διευθύνσεις και όταν αυτοί επιθυμούν να επικοινωνήσουν με κόμβους στο δημόσιο διαδίκτυο να χρησιμοποιούν μια ή περισσότερες δημόσιες διευθύνσεις που έχουν ανατεθεί στον δρομολογητή-πύλη από τον ISP.

Υπάρχουν τρείς μέθοδοι NAT:

- Στατικό NAT
- Δυναμικό NAT
- Υπερφορτωμένο (overload) NAT

Η γνωστότερη τεχνική NAT είναι η τρίτη και είναι γνωστή και ως Network Address Translation / Port Address Translation (NAT/PAT) ή NAT overload.

Σύμφωνα με αυτή τη τεχνική πολλές ιδιωτικές IP διευθύνσεις μπορούν να αντιστοιχηθούν σε μια δημόσια. Αυτό μπορεί να γίνει με την βοήθεια των ports που χρησιμοποιούνται από το πρωτόκολλο επιπέδου μεταφοράς (TCP/UDP). Για παράδειγμα ελέγξτε την Εικόνα 23. Εμφανίζεται ένα τυπικό οικιακό δίκτυο που διαθέτουν οι περισσότεροι οικιακοί χρήστες.



Εικόνα 223. Τυπικό οικιακό δίκτυο.

Protocol	Inside Local IP:Port	Inside Global IP: Port	Outside Global IP: Port
TCP	10.1.1.4:1723	170.168.150.87:1723	63.212.15.66:80
TCP	10.1.1.3:1888	170.168.150.87:1888	63.212.15.66:80

Πίνακας 5. Πίνακας NAT/PAT του R1 για το δίκτυο της Εικόνας 8.

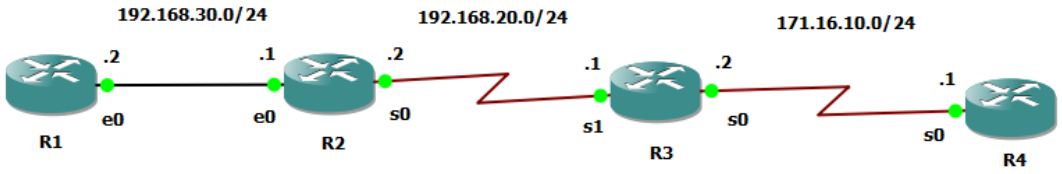
Στον Πίνακα 5 εμφανίζεται ο πίνακας NAT/PAT που διατηρεί ο R1 για τις συνδέσεις των κόμβων του οικιακού δικτύου με τον Server. Οι συνδέσεις TCP ξεχωρίζουν από τον συνδυασμό των ιδιωτικών IP διευθύνσεων και των port που χρησιμοποιεί ο κάθε κόμβος. Στο NAT χρησιμοποιείται μια ειδική ορολογία για τις IP διευθύνσεις:

Inside Local: *Η εσωτερική ιδιωτική IP διεύθυνση*

Inside Global: *Η δημόσια IP διεύθυνση*

Outside Global: *Η IP διεύθυνση του κόμβου προορισμού*

Ετοιμάστε το δίκτυο δρομολογητών της Εικόνας 24 στο GNS3 και ονομάστε το project <**Το ΑΕΜ σας**>**_NAT_PAT**. Βάλτε τις κατάλληλες IP διευθύνσεις που φαίνονται στην εικόνα. Επίσης, ενεργοποιείστε το OSPF πρωτόκολλο σε όλους τους δρομολογητές. Ενεργοποιείστε το password για την κατάσταση executive με συνθηματικό την λέξη **cisco** και την απομακρυσμένη πρόσβαση (vty) στον R4 με password **abcd**.



Εικόνα 24. Το δίκτυο για NAT/PAT.

Από την εικόνα μπορείτε να αντιληφθείτε ότι η τεχνική NAT/PAT θα εφαρμοστεί στον R3. Μεταφερθείτε στην κονσόλα του R3 και δώστε τις παρακάτω εντολές:

```
R3(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

Η εντολή αυτή υλοποιεί μια λίστα ιδιωτικών IP διευθύνσεων που θα επιτρέπεται να μεταφραστούν στον R3 με τη χρήση του NAT/PAT. Πρόκειται για μια λίστα πρόσβασης για τις οποίες θα μιλήσουμε στην επόμενη πράγραφο.

```
R3(config)#ip nat inside source list 1 interface s0 overload
```

Εδώ ενεργοποιείται η τεχνική NAT/PAT με υπερφόρτωση του s0 του R3.

```
R3(config)#int s1
```

```
R3(config-if)#ip nat inside
```

Εδώ δηλώνεται ότι το interface s1 είναι εσωτερικό (inside).

```
R3(config-if)#int s0
```

```
R3(config-if)#ip nat outside
```

Εδώ δηλώνεται ότι το interface s0 είναι εξωτερικό (outside).

Μεταφερθείτε στην κονσόλα του R1 και συνδεθείτε μέσω telnet στον R4. Αμέσως μετά συνδεθείτε μέσω telnet στον R4 από τον R2.

Δείτε στον R3 τις μεταφράσεις ιδιωτικών σε δημόσιες διευθύνσεις με την παρακάτω εντολή:

```
R3#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 171.16.10.2:39258  192.168.20.2:39258 171.16.10.1:23     171.16.10.1:23
tcp 171.16.10.2:36881  192.168.30.2:36881 171.16.10.1:23     171.16.10.1:23
```

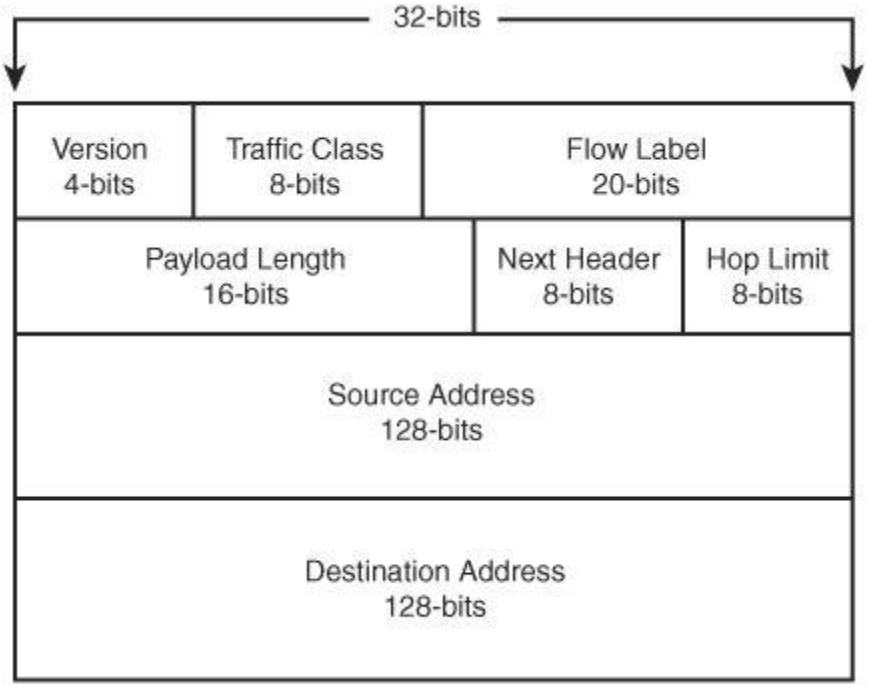
Φαίνεται ότι έχουν γίνει δύο μεταφράσεις των εσωτερικών διευθύνσεων/θυρών 192.168.20.2:39258 (R2) και 192.168.30.2:36881 (R1) στην δημόσια διεύθυνση/θύρα 171.16.10.2:39258 και 171.16.10.2:36881, αντίστοιχα. Προορισμός είναι η διεύθυνση 171.16.10.1:23 με ζητούμενη υπηρεσία το telnet (port:23).

Μπορείτε να ενεργοποιήσετε το wireshark στην ζεύξη μεταξύ R3 και R4 για να δείτε την μεταφορά των πακέτων και τις IP διευθύνσεις και θύρες.

9. IPv6

Η έκτη έκδοση του πρωτοκόλλου IP (γνωστή και ως IPv6) αντικαθιστά την τέταρτη έκδοση του ίδου πρωτοκόλλου (IPv4). Ο κυριότερος λόγος για την αντικατάσταση αυτή προήλθε από το γεγονός της εξάντλησης των IPv4 διευθύνσεων. Στο IPv4 οι διαθέσιμες διευθύνσεις είναι μερικά δισεκατομμύρια και η εξάντληση τους ήταν απλά θέμα χρόνου. Το 2011 ο υπεύθυνος οργανισμός για την διαχείρηση τους αποδέσμευσε το τελευταίο block IP διευθύνσεων κλάσης Α. Βέβαια, η πρόγνωση του προβλήματος έγινε πολύ παλαιότερα, στην δεκαετία του 1980.

Το IPv6 αυξάνει τον αριθμό των διαθέσιμων IP διευθύνσεων αλλάζοντας πλήρως την μορφή της IP επικεφαλίδας όπως φαίνεται στην Εικόνα 25.



Εικόνα 25. Η μορφή της επικεφαλίδας IPv6.

Παρατηρούμε, λοιπόν, ότι το διαθέσιμο μέγεθος του πεδίου για τις διευθύνσεις αποστολέα και παραλήπτη έχει αυξηθεί στα 128 bits, έναντι 32 bits που ήταν στο IPv4. Με αυτή την αλλαγή ευελπιστεί η κοινότητα του Internet να λυθεί το πρόβλημα για πολλές δεκαετίες ακόμα.

Ωστόσο, με την αλλαγή αυτή έχουν γίνει κάποιες τροποποιήσεις (έστω και λίγες) στους κανόνες διευθυνσιοδότησης. Αυτό έχει επίπτωση και στη λειτουργία πολλών πρωτοκόλλων που βασίζονται στο IP. Για παράδειγμα, το πρωτόκολλο ARP έχει μετονομαστεί σε NDP (Neighbor Discovery Protocol) και λειτουργεί με του κανόνες που ορίζει το IPv6. Το ίδιο ισχύει και για το πρωτόκολλο DHCPv6 το οποίο είναι η ανανεωμένη έκδοση του DHCP για το IPv4. Επίσης, τα πρωτόκολλα δρομολόγησης προσαρμόστηκαν στην νέα έκδοση του IPv6 και μετονομάστηκαν σε RIPng (RIP next generation) και OSPFv3.

9.1 IPv6 διευθυνσιοδότηση

Ο τρόπος αναπαράστασης των IPv6 διευθύνσεων χρησιμοποιεί την δεκαεξαδική μορφή των διευθύνσεων, σε αντίθεση με την αναπαράσταση των IPv4 διευθύνσεων που αναγράφονται στην δεκαδική τους μορφή. Πιο συγκεκριμένα, η αναπαράσταση χρησιμοποιεί οκτώ ομάδες των τεσσάρων δεκαεξαδικών ψηφίων, με κάθε ομάδα να διαχωρίζεται από την επόμενη με τον χαρακτήρα «**:**» (άνω-κάτω τελεία). Για παράδειγμα:

2340:1111:0000:3333:0000:0000:1234:5678

Η παραπάνω αναπαράσταση χωρίζεται σε οκτώ ομάδες των 16 bits. Κάθε ομάδα τεσσάρων δεκαεξαδικών ψηφίων αντιστοιχεί σε 16 bits δίνοντας μας συνολικά μια διεύθυνση των 128 bits.

Όπως είναι αναμενόμενο θα αναρωτηθεί κανείς μήπως υπάρχει κάποιος ευκολότερος τρόπος αναπαράστασης των IPv6 διευθύνσεων. Πράγματι, υπάρχει. Η παραπάνω διεύθυνση, για παράδειγμα, θα μπορούσε να συντμηθεί όπως παρακάτω:

2340:1111:0:3333::1234:5678

Αυτό που εφαρμόστηκε είναι η περικοπή των μηδενικών που υπάρχουν στην αρχική αναπαράσταση. Πιο συγκεκριμένα, η πρώτη ομάδα τεσσάρων μηδενικών (η αριστερή) αντικαταστάθηκε με ένα μηδενικό, ενώ οι επόμενες δυο ομάδες τεσσάρων μηδενικών εξαλήφθηκαν πλήρως και αντικαταστάθηκαν με «**::**».

Οι κανόνες για την σύντμηση της αναπαράστασης των IPv6 διευθύνσεων συνοψίζονται παρακάτω:

1. Μέσα σε κάθε ομάδα τεσσάρων δεκαεξαδικών ψηφίων, αφαιρέστε τα μηδενικά που βρίσκονται αριστερότερα (εάν υπάρχουν). Προσοχή, πρέπει να αφεθεί το δεξιότερο ψηφίο στην ομάδα, εάν δεν ισχύει ο δεύτερος κανόνας.

2. Εάν υπάρχουν δύο ή περισσότερες διαδοχικές ομάδες μηδενικών, τότε αυτές μπορούν να αντικατασταθούν με το σύμβολο «**::**». Το σύμβολο αυτό σημαίνει *«δύο ή περισσότερες ομάδες τεσσάρων δεκαεξαδικών συμβόλων τα οποία είναι 0»*. Ωστόσο, μπορούμε να χρησιμοποιήσουμε μόνο μια φορά το σύμβολο αυτό σε μια αναπαράσταση IPv6 διεύθυνσης. Ο λόγος είναι ότι εάν χρησιμοποιηθεί περισσότερες φορές, θα υπάρχει σύγχηση για την ακριβή αναπαράσταση της IPv6 διεύθυνσης.

Έτσι, σαν δεύτερο παράδειγμα η παρακάτω διεύθυνση:

FE00:0000:0000:0001:0000:0000:0000:0056

μπορεί να απλοποιηθεί στην:

FE00:0:0:1::56

Δυστυχώς, η παρακάτω διεύθυνση δεν μπορεί να απλοποιηθεί καθόλου και πρέπει να γραφεί ολόκληρη:

FE00:1111:2222:3333:AAAA:BBBB:1234:4567

Για την αντίστροφη διαδικασία, δηλαδή την γραφή της πλήρης μορφής μιας IPv6 διεύθυνσης από την συντμημένη της μορφή, ακολουθούμε τους παρακάτω δυο κανόνες:

1. Σε κάθε ομάδα δεκαεξαδικών ψηφίων, προσθέτουμε αριστερά όσα μηδενικά χρειάζονται μέχρι η ομάδα να έχει τέσσερα δεκαεξαδικά ψηφία.

2. Εάν υπάρχει το σύμβολο «**::**», μετράμε τις ομάδες δεκαεξαδικών ψηφίων που υπάρχουν. Σε σύνολο πρέπει να είναι μικροτερο του 8. Αντικαθιστούμε το σύμβολο «**::**» με πολλαπλές ομάδες τεσσάρων διαδοχικών 0, τόσες ώστε συνολικά να υπάρχουν 8 ομάδες δεκαεξαδικών ψηφίων.

Ως πρακτική άσκηση μπορείτε να συμπληρώσετε τον παρακάτω Πίνακα 6:

Πλήρης IPv6 διεύθυνση	**Συντμημένη IPv6 διεύθυνση**
2340:0000:0010:0100:1000:ABCD:0101:1010	
	30A0:ABCD:EF12:3456:ABC:B0B0:9999:9009
210F:0000:0000:0000:DEAD:0000:0000:0707	
	3210::
FE80:000F:00E0:0D00:FACE:BAFF:FE00:0000	
	34BA:B:B::20

Πίνακας 6. Παραδείγματα πλήρους και συντμημένης IPv6 διεύθυνσης.

Το IPv6 χρησιμοποιεί την έννοια της μάσκας, όπως οι μάσκες υποδικτύωση στο IPv4, την οποία όμως την ονομάζει *prefix length*. Η αναπαράσταση του prefix length συμβολίζεται με ανάλογο τρόπο όπως στο IPv4: με τη χρήση της πλαγιοκαθέτου (/) ακολουθούμενη από έναν δεκαδικό αριθμό. Ο αριθμός αυτός προσδιορίζει πόσα bits της IPv6 διεύθυνσης είναι δεσμευμένα για την ταυτότητα δικτύου και υποδικτύου. Ας πάρουμε για παράδειγμα, την παρακάτω διεύθυνση:

FE00:1111:2222:3333:AAAA:BBBB:1234:4567/64

Το prefix length είναι 64 bits, δηλαδή 8 bytes και επομένως η ταυτότητα δικτύου (η οποία στην ορολογία του IPv6 ονομάζεται prefix) θα είναι η παρακάτω:

FE00:1111:2222:3333:0000:0000:0000:0000/64

Η παραπάνω διεύθυνση δικτύου μπορεί να αναπαρασταθεί και συντμημένη:

FE00:1111:2222:3333::/64

9.1.1 Τύποι IPv6 διευθύνσεων

Θα πρέπει να είστε αρκετά εξοικειωμένοι με τους διαφορετικούς τύπους των IPV4 διευθύνσεων: unicast, broadcast, multicast, private και public. Το IPv6 ορίζει ανάλογους τύπους διευθύνσεων. Η ονομασία τους και η σημασία τους αναλύεται στη συνέχεια:

- Unicast: Τα πακέτα που προορίζονται για unicast διευθύνσεις καταφθάνουν σε μια μόνο διεπαφή (interface) ενός κόμβου.

- Global Unicast: Αυτές οι διευθύνσεις είναι όμοιες με τις δημόσιες (public) IPv4 διευθύνσεις. Οι διευθύνσεις αυτές ξεκινούν με πρώτο δεκαεξαδικό ψηφίο το 2.

- Link-local: Αυτές οι διευθύνσεις είναι όμοιες με τις ιδιωτικές (private) IPv4 διευθύνσεις. Κάθε interface με ενεργοποιημένο το IPv6 έχει πάντα μια Link-local διεύθυνση συσχετισμένη, παρόλο που μπορεί να του έχει αποδοθεί μια Global Unicast διεύθυνση. Οι Link-local διευθύνσεις δεν χρησιμοποιούνται σε ροές πακέτων που περιλαμβάνουν δεδομένα εφαρμογών. Η χρήση τους περιορίζεται σε ορισμένα χρήσιμα πρωτόκολλα. Τα πρωτόκολλα που απαιτούν την μετάδοση πακέτων μέσα σε ένα υποδίκτυο χρησιμοποιούν τις Link-local διευθύνσεις αντί τις Global unicast. Οι δρομολογητές δεν προωθούν πακέτα με Link-local διευθύνσεις σε άλλα υποδίκτυα. Οι διευθύνσεις αυτές ξεκινούν με τα δεκαεξαδικά ψηφία FE. Σχεδόν πάντα, οι Link-local διευθύνσεις έχουν τα πρώτα 16 δεκαεξαδικά ψηφία να είναι FE80:0000:0000:0000.

- Multicast: Αυτές οι διευθύνσεις χρησιμοποιούνται για την μετάδοση πακέτων σε περισσότερα του ενός interfaces. Είναι ιδιαίτερα εύκολο να εντοπίσουμε μια multicast IPv6 διεύθυνση διότι ξεκινά πάντα με τα δεκαεξαδικά ψηφία FF.

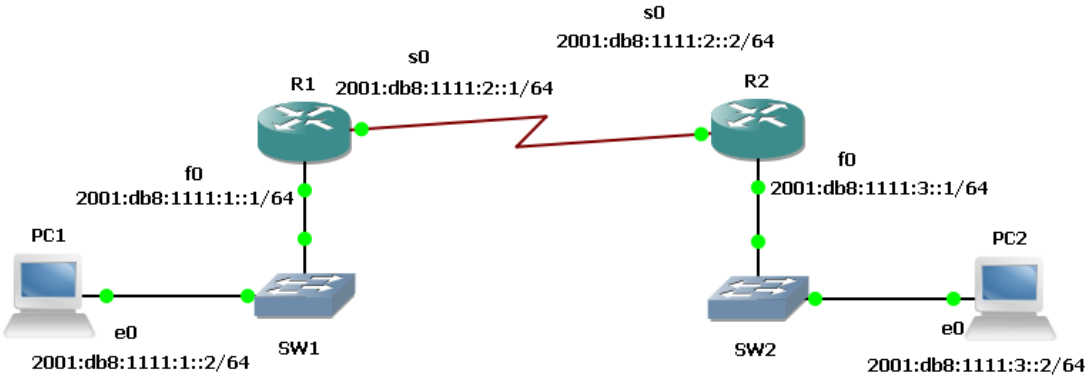
Ο Πίνακας 7 συνοψίζει τους σημαντικότερους τύπους IPv6 διευθύνσεων και την σημασία τους.

Τύπος IPv6 διεύθυνσης	Σημασία
2000::/3	Το εύρος των Global Unicast διευθύνσεων
FE80::/10	Το εύρος των Link Local διευθύνσεων
FF00::/8	Το εύρος των multicast διευθύνσεων

Πίνακας 7. Τύποι IPv6 διευθύνσεων.

9.2 Απόδοση IPv6 διευθύνσεων σε δρομολογητές και σταθμούς

Δημιουργείστε το το δίκτυο που φαίνεται στην Εικόνα 26 και ονομάστε το project σας *IPv6*. Στην εικόνα φαίνονται και οι IPv6 διευθύνσεις που πρέπει να αποδωθούν στις διεπαφές των κόμβων. Το πλάνο διευθυνσιοδότησης προέκυψε υποθέτοντας ότι έχουμε στη διάθεση μας την IPv6 διεύθυνση 2001:db8:1111::/48 την οποία υποδικτυώσαμε.



Εικόνα 26. Η μορφή της επικεφαλίδας IPv6.

Η διαδικασία της υποδικτύωσης στο IPv6 είναι ακριβώς η ίδια όπως και στο IPv4 μόνο που είναι απλούστερη. Αυτό προκύπτει από το μεγάλο πλήθος των διευθύνσεων που έχουμε διαθέσιμο. Έτσι, αναφερόμενοι και πάλι στο παραπάνω δίκτυο, το σύνολο των υποδικτύων που διαθέτουμε είναι 3. Επομένως, θα πρέπει να αυξήσουμε το prefix ώστε να περιλαμβάνει και το subnet ID. Στο παράδειγμα μας θα μπορούσαμε να χρησιμοποιήσουμε 2 bits για να μας δώσουν τις ταυτότητες των υποδικτύων. Να κάνουμε, δηλαδή, το prefix /50. Αυτό θα μας έδινε 4 υποδίκτυα με 2^{78}-2 host διευθύνσεις. Το νούμερο είναι εξαιρετικά μεγάλο. Εάν κάναμε το prefix /64, δεσμεύαμε δηλαδή μια ολόκληρη τετράδα δεκαεξαδικών ψηφίων (16 bits) θα μας έδινε 65536 υποδίκτυα με 2^{64}-2 διαθέσιμες διευθύνσεις host. Αυτό θα έκανε την διαδικασία της υποδικτύωσης ευκολότερη διατηρώντας ένα πολύ μεγάλο πλήθος διευθύνσεων για τους host. Στο παράδειγμα μας ακολουθήσαμε την δεύτερη προσέγγιση και τα υποδίκτυα είναι: 2001:db8:1111:1::/64, 2001:db8:1111:2::/64 και 2001:db8:1111:3::/64.

Για να αποδώσουμε τις IPv6 διευθύνσεις που φαίνονται στην εικόνα στον δρομολογητή R1 ακολουθούμε την παρακάτω διαδικασία:

```
R1#config t

R1(config)#ipv6 unicast-routing

R1(config)#int f0

R1(config-if)#ipv6 address 2001:db8:1111:1::1/64

R1(config-if)#no shut

R1(config-if)#int s0

R1(config-if)#ipv6 address 2001:db8:1111:2::1/64

R1(config-if)#no shut
```

Η εντολή `ipv6 unicast-routing` είναι απαραίτητη προκειμένου να ενεργοποιηθεί η διαδικασία της IPv6 δρομολογησης στον δρομολογητή (η IPv4 δρομολόγηση είναι ενεργοποιημένη στους Cisco δρομολογητές αλλά η IPv6 δρομολόγηση δεν είναι). Από εκεί και πέρα η διαδικασία είναι απλή: δηλώνουμε το interface και αναθέτουμε την διεύθυνση.

Προκειμένου να δούμε τις IPv6 ρυθμίσεις ενός interface δίνουμε την παρακάτω εντολή:

```
R1#show ipv6 int f0

FastEthernet0 is up, line protocol is up

  IPv6 is enabled, link-local address is FE80::D201:AFF:FE1C:0

  No Virtual link-local address(es):

  Global unicast address(es):

    2001:DB8:1111:1::1, subnet is 2001:DB8:1111:1::/64

  Joined group address(es):

    FF02::1

    FF02::2

    FF02::1:FF00:1

    FF02::1:FF1C:0

  MTU is 1500 bytes

  ICMP error messages limited to one every 100 milliseconds

  ICMP redirects are enabled

  ICMP unreachables are sent

  ND DAD is enabled, number of DAD attempts: 1
```

```
  ND reachable time is 30000 milliseconds

  ND advertised reachable time is 0 milliseconds

  ND advertised retransmit interval is 0 milliseconds

  ND router advertisements are sent every 200 seconds

  ND router advertisements live for 1800 seconds

  ND advertised default router preference is Medium

  Hosts use stateless autoconfig for addresses.
```

Στην έξοδο της εντολής φαίνονται οι link-local και global unicast διευθύνσεις του interface. Επίσης, εμφανίζονται και οι multicast ομάδες (groups) στις οποίες ανήκει το συγκεκριμένο interface.

Μπορούμε να αποδώσουμε μια IPv6 διεύθυνση και στον PC1 δίνοντας την παρακάτω εντολή:

```
PC1> ip 2001:db8:1111:1::2/64

PC1 : 2001:db8:1111:1::2/64
```

Κατόπιν μπορούμε να δούμε τις ρυθμίσεις του PC1:

```
PC1> show

NAME   IP/MASK      GATEWAY        MAC            LPORT  RHOST:PORT

PC1    0.0.0.0/0    0.0.0.0   00:50:79:66:68:01  10000  127.0.0.1:10001

       fe80::250:79ff:fe66:6801/64

       2001:db8:1111:1::2/64
```

Παρατηρούμε ότι έχει αποδωθεί η IPv6 Link-local και Global Unicast διεύθυνση. Τέλος, μπορούμε να ελέγξουμε την διασυνδεσιμότητα του PC1 κάνοντας ping με προορισμό το `f0` του R1:

```
PC1> ping 2001:db8:1111:1::1

2001:db8:1111:1::1 icmp6_seq=1 ttl=64 time=0.000 ms

2001:db8:1111:1::1 icmp6_seq=2 ttl=64 time=0.000 ms

2001:db8:1111:1::1 icmp6_seq=3 ttl=64 time=0.000 ms

2001:db8:1111:1::1 icmp6_seq=4 ttl=64 time=31.250 ms

2001:db8:1111:1::1 icmp6_seq=5 ttl=64 time=0.000 ms
```

Μπορούμε να καταγράψουμε με τον αναλυτή πρωτοκόλλων την επικοινωνία αυτή του PC1 και του R1 (Εικόνα 27). Το πρώτο πράγμα που μπορούμε να παρατηρήσουμε είναι ότι στην στήλη *Protocol* του αναλυτή το πρωτόκολλο που

χρησιμοποιείται είναι το ICMPv6. Επίσης, μπορούμε να δούμε την λειτουργία του NDP πρωτοκόλλου η οποία προηγείται της επικοινωνίας του PC1 και R1 με την ping. Βλέπουμε ότι ο PC1 μεταδίδει ένα πακέτο ανακάλυψης, το οποίο ονομάζεται *Neighbor Solicitation* (το αντίστοιχο του ARP request στο IPv4), το οποίο μεταδίδεται στην multicast διευθυνση ff02::1:ff00:1 της οποίας μέλος είναι το `f0` του R1 (δείτε τα αποτελέσματα της εντολής `show ipv6 int f0` στον R1). Έπειτα, ο R1 αποκρίνεται με ένα πακέτο το οποίο καλείται *Neighbor Advertisment* και περιλαμβάνει την MAC διεύθυνση του `f0` του R1. Αμέσως μετά ξεκινά η ping επικοινωνία μεταξύ PC1 και R1.

Επεκτείνοντας τα περιεχόμενα των πρωτοκόλλων μπορείτε να δείτε τα πεδία των επικεφαλίδων του IPv6 και του ICMPv6. Επιλέξτε ένα ICMPv6 echo request και δείτε ότι περιλαμβάνει 56 Bytes δεδομένων. Τα δεδομένα αυτά φαίνονται στην δεκαεξαδική αναπαράσταση του πακέτου (Εικόνα 28). Παρατηρούμε ότι προκειμένουν να συμπληρωθούν τα 56 Bytes δεδομένων της εντολής ping, έχουν τοποθετηθεί οι αριθμοί 0,1,2,3,4,5,…. μεταφρασμένοι στην δεκαεξαδική τους μορφή.

Δοκιμάστε να κάνετε ping στην Link-local διεύθυνση που έχει συσχετιστεί με το `f0` του R1 (FE80::D201:AFF:FE1C:0). Θα πρέπει να δείτε ότι η επικοινωνία είναι επιτυχής [12].

Συνεχίζουμε, αναθέτοντας και τις διευθύνσεις στους υπόλοιπους κόμβους που φαίνονται στην Εικόνα 23. Πιο συγκεκριμένα στον R2 εκτελούμε τις παρακάτω ρυθμίσεις:

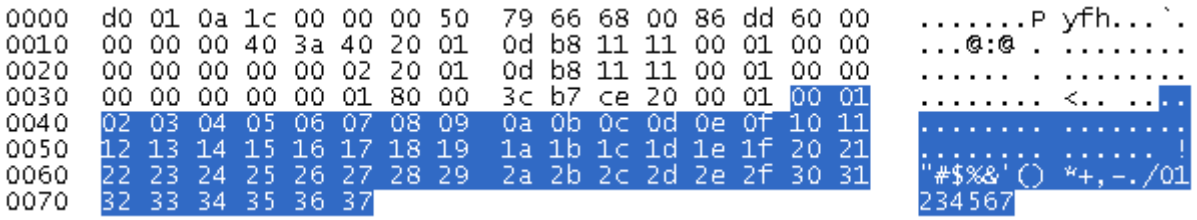
```
R2#config t
R2(config)#ipv6 unicast-routing
R2(config)#int s0
R2(config-if)#ipv6 address 2001:db8:1111:2::2/64
R2(config-if)#no shut
R2(config-if)#int f0
R2(config-if)#ipv6 address 2001:db8:1111:3::1/64
R2(config-if)#no shut
```

Πριν κάνετε τις ρυθμίσεις και στον PC2 μεταφερθείτε στο prompt και εκτελέστε την ακόλουθη εντολή:

```
PC2> show
NAME   IP/MASK          GATEWAY       MAC                 LPORT   RHOST:PORT
PC2    0.0.0.0/0        0.0.0.0       00:50:79:66:68:00   10000   127.0.0.1:10003
       fe80::250:79ff:fe66:6800/64
```

1	0.00000000	2001:db8:1111:1::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001:db8:1111:1::1 from 00:50:79:66:68:00
2	0.01562500	2001:db8:1111:1::1	2001:db8:1111:1::2	ICMPv6	86	Neighbor Advertisement 2001:db8:1111:1::1 (rtr, sol, ovr) is at d0:01:0a:1c:00:00
3	1.00000000	2001:db8:1111:1::2	2001:db8:1111:1::1	ICMPv6	118	Echo (ping) request id=0xce20, seq=1
4	1.00000000	2001:db8:1111:1::1	2001:db8:1111:1::2	ICMPv6	118	Echo (ping) reply id=0xce20, seq=1
5	1.00000000	2001:db8:1111:1::2	2001:db8:1111:1::1	ICMPv6	118	Echo (ping) request id=0xce20, seq=2
6	1.03125000	2001:db8:1111:1::1	2001:db8:1111:1::2	ICMPv6	118	Echo (ping) reply id=0xce20, seq=2
7	1.04687500	2001:db8:1111:1::2	2001:db8:1111:1::1	ICMPv6	118	Echo (ping) request id=0xce20, seq=3
8	1.04687500	2001:db8:1111:1::1	2001:db8:1111:1::2	ICMPv6	118	Echo (ping) reply id=0xce20, seq=3
9	1.04687500	2001:db8:1111:1::2	2001:db8:1111:1::1	ICMPv6	118	Echo (ping) request id=0xce20, seq=4
10	1.07812500	2001:db8:1111:1::1	2001:db8:1111:1::2	ICMPv6	118	Echo (ping) reply id=0xce20, seq=4
11	1.09375000	2001:db8:1111:1::2	2001:db8:1111:1::1	ICMPv6	118	Echo (ping) request id=0xce20, seq=5
12	1.12500000	2001:db8:1111:1::1	2001:db8:1111:1::2	ICMPv6	118	Echo (ping) reply id=0xce20, seq=5

Εικόνα 27. Καταγραφή της επικοινωνίας του PC1.



Εικόνα 28. Δεκαεξαδική μορφή των δεδομένων ενός ICMPv6 echo request.

Παρατηρείστε ότι ήδη έχει ρυθμισμένη μια Link-local διεύθυνση χωρίς εμείς να έχουμε κάνει καμία IPv6 ρύθμιση ακόμα. Αμέσως μετά κάντε ping στο `f0` του R2.

```
PC2> ping 2001:db8:1111:3::1

2001:db8:1111:3::1 icmp6_seq=1 ttl=64 time=0.000 ms

2001:db8:1111:3::1 icmp6_seq=2 ttl=64 time=15.625 ms

2001:db8:1111:3::1 icmp6_seq=3 ttl=64 time=15.625 ms

2001:db8:1111:3::1 icmp6_seq=4 ttl=64 time=15.625 ms

2001:db8:1111:3::1 icmp6_seq=5 ttl=64 time=15.625 ms
```

Αφού δείτε ότι η επικοινωνία ήταν επιτυχής, εμφανίστε και πάλι τις IP ρυθμίσεις του PC2:

```
PC2> show

NAME   IP/MASK          GATEWAY       MAC                 LPORT   RHOST:PORT

PC2    0.0.0.0/0        0.0.0.0       00:50:79:66:68:00   10000   127.0.0.1:10003

       fe80::250:79ff:fe66:6800/64

       2001:db8:1111:3:250:79ff:fe66:6800/64 eui-64
```

Παρατηρούμε ότι αυτομάτως τοποθετήθηκε μια Global unicast διεύθυνση στον PC2 χωρίς εμείς να έχουμε κάνει κάποια ρύθμιση. Η μέθοδος με την οποία ανατέθηκε αυτή η μοναδική διεύθυνση ονομάζεται *Extended Unique Identifier (EUI-64)* και θα αναλυθεί παρακάτω.

9.2.1 Extended Unique Identifier (EUI-64)

Στο IPv6 μπορούμε με δυο τρόπους να αναθέσουμε μοναδικές διευθύνσεις σε μια διεπαφή (είτε είναι host είτε είναι router). Ο πρώτος είναι αυτός που εξετάσαμε στην προηγούμενη παράγραφο με τον οποίο τοποθετήσαμε χειρονακτικά μια μοναδική Global-unicast διεύθυνση χρησιμοποιώντας την εντολή **`ipv6 address`**. Ο δεύτερος τρόπος είναι ημι-αυτοματοποιημένος και χρησιμοποιείται όταν έχουμε prefix /64 (που είναι και η συνηθέστερη περίπτωση) γι' αυτό και η ονομασία του είναι EUI-64.

Με την μέθοδο δημιουργίας μοναδικών διευθύνσεων EUI-64, τα πρώτα 64 bits της διεύθυνσης παραμένουν αναλλοίωτα, ενώ τα υπόλοιπα 64 προκύπτουν από την MAC διεύθυνση της διεπαφής. Επειδή οι MAC διευθύνσεις είναι μοναδικές ανά διεπαφή, έτσι και η προκύπτουσα IPv6 διεύθυνση θα είναι μοναδική. Ωστόσο, ως γνωστόν, η MAC διεύθυνση έχει 48 bits και επομένως θα πρέπει να συμπληρωθούν με άλλα 16

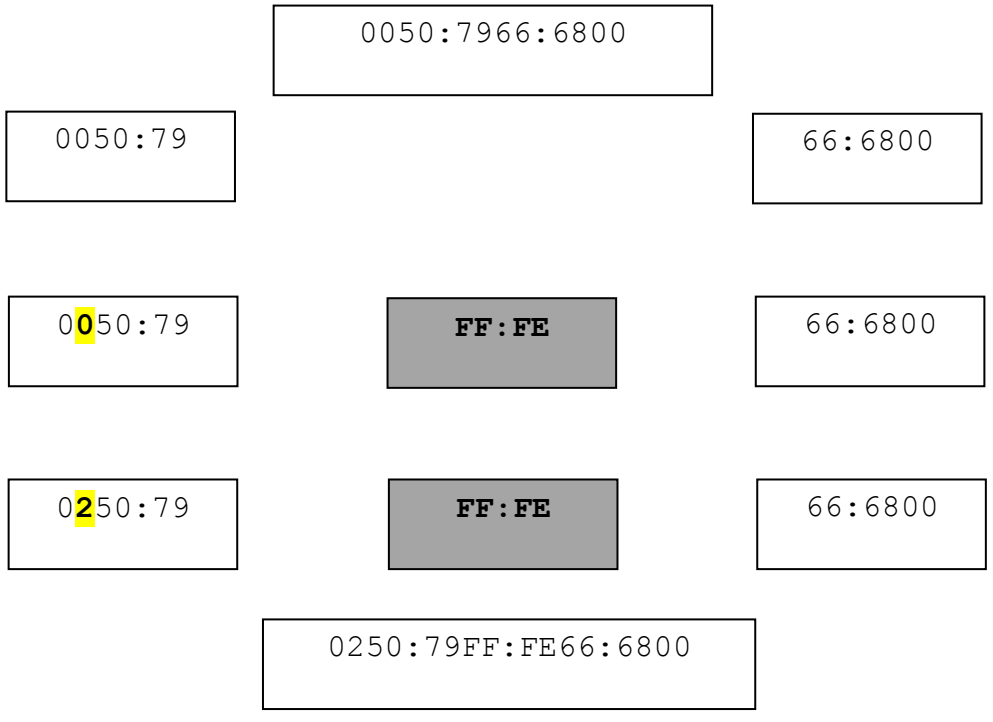
προκειμένου να έχουμε συνολικό μέγεθος 64. Ας δούμε την όλη διαδικασία με το παράδειγμα του PC2 της προηγούμενης παραγράφου.

Η διεπαφή `e0` του PC2 έχει MAC διεύθυνση `00:50:79:66:68:00` η οποία θα χρησιμοποιηθεί για να συμπληρώσει το prefix `2001:db8:1111:3::/64`. Για να γίνει αυτό ακολουθούμε τους ακόλουθους κανόνες:

- Χωρίζουμε την MAC διεύθυνση σε δυο ίσα μέρη (3 byte το κάθε ένα).
- Τοποθετούμε ανάμεσα τους τα δεκαεξαδικά ψηφία FFFE.
- Αναστρέφουμε το 7^{ο} bit (αν είναι 0 το κάνουμε 1 και το αντίστροφο) του πρώτου byte της MAC διεύθυνσης.

Η διαδικασία φαίνεται σχηματικά στην Εικόνα 29.

Σημείωση: *Οι MAC διευθύνσεις των κόμβων στο δικό σας project ενδέχεται να διαφέρουν από αυτές του παραδείγματος.*



Εικόνα 29. Η διαδικασία EUI-64.

Μπορείτε να παρατηρείσετε ότι οι link-local διευθύνσεις των R1 και R2 έχουν αποδωθεί αυτόματα με τη χρήση του EUI-64. Για παράδειγμα ας εξετάσουμε το interface f0 του R2:

```
R2(config)#do sh ipv6 int f0

FastEthernet0 is up, line protocol is up

  IPv6 is enabled, link-local address is FE80::D202:FFF:FE60:0

  No Virtual link-local address(es):

  Global unicast address(es):

    2001:DB8:1111:3::1, subnet is 2001:DB8:1111:3::/64

  Joined group address(es):

    FF02::1

    FF02::2

    FF02::1:FF00:1

    FF02::1:FF60:0

  MTU is 1500 bytes

  ICMP error messages limited to one every 100 milliseconds

  ICMP redirects are enabled

  ICMP unreachables are sent

  ND DAD is enabled, number of DAD attempts: 1

  ND reachable time is 30000 milliseconds

  ND advertised reachable time is 0 milliseconds

  ND advertised retransmit interval is 0 milliseconds

  ND router advertisements are sent every 200 seconds

  ND router advertisements live for 1800 seconds

  ND advertised default router preference is Medium

  Hosts use stateless autoconfig for addresses.
```

Παρατηρώντας την link-local διεύθυνση του f0 του R2 μπορούμε να εντοπίσουμε την ακολουθία FFFE (η οποία χρησιμοποιείται στην τεχνική EUI-64) και να εξάγουμε την MAC διεύθυνση του f0. Απλά εξετάζουμε τα τρία bytes αριστερά της ακολουθίας (D2020F) και τα τρία bytes δεξιά της (600000). Στο 7^{o} bit του πρώτου byte (το D2 δηλαδή) εκτελούμε αναστροφή και η MAC διεύθυνση της διεπαφής μπορεί να προβλεφθεί ότι θα είναι: D002:0F60:0000. Πράγματι, εκτελώντας την παρακάτω εντολή στον R2 βλέπουμε:

```
R2#show int f0

FastEthernet0 is up, line protocol is up
```

```
  Hardware is PQUICC_FEC, address is d002.0f60.0000 (bia d002.0f60.0000)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
…….
```

Η μέθοδος EUI-64 μπορεί να εφαρμοστεί και στις Global-unicast διευθύνσεις των δρομολογητών προσθέτοντας στο τέλος της εντολής **ipv6 address** το χαρακτηριστικό **eui-64**.

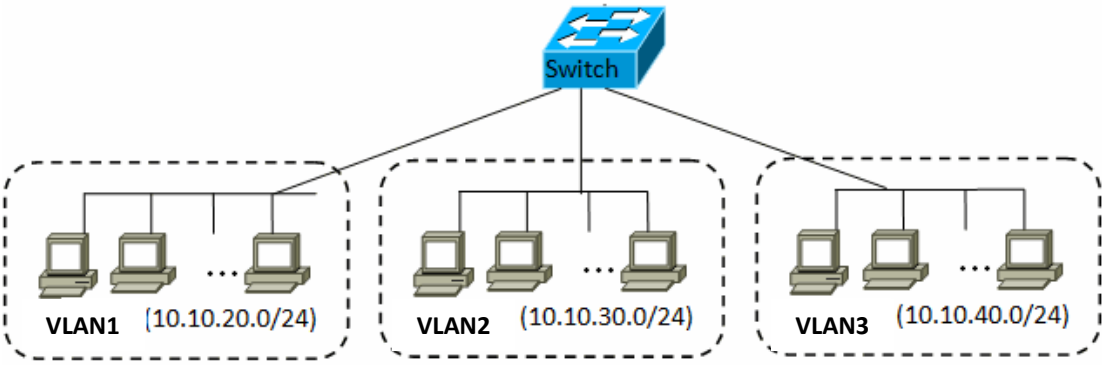
Επιστρέφοντας στον PC2, αν δώσουμε μια IPv6 διεύθυνση με τον χειρονακτικό τρόπο, τότε η νέα καταχώρηση θα υπερκαλύψει αυτήν που αποδόθηκε αυτόματα με την μέθοδο EUI-64:

```
PC2> show
NAME   IP/MASK         GATEWAY          MAC              LPORT  RHOST:PORT
PC2    0.0.0.0/0       0.0.0.0       00:50:79:66:68:01  10009  127.0.0.1:10008
       fe80::250:79ff:fe66:6800/64
       2001:db8:1111:3:2050:79ff:fe66:6801/64 eui-64
PC2> ip 2001:db8:1111:3::2/64
PC1 : 2001:db8:1111:3::2/64
PC2> show
NAME   IP/MASK          GATEWAY         MAC                LPORT  RHOST:PORT
PC2    0.0.0.0/0        0.0.0.0      00:50:79:66:68:01  10009  127.0.0.1:10008
       fe80::250:79ff:fe66:6800/64
       2001:db8:1111:3::2/64
```

10. Εικονικά Τοπικά Δίκτυα (Virtual LANs)

Ως γνωστόν, ένα τοπικό δίκτυο με switch ή hub αποτελεί μια *περιοχή ευρυεκπομπής (broadcast domain)* και η διάσπαση του σε περισσότερες απαιτεί την χρήση μιας συσκευής δρομολόγησης. Τα *εικονικά τοπικά δίκτυα (Virtual LANs – VLANs)* αποτελούν έναν τρόπο για να διασπάσουμε ένα τοπικό δίκτυο (LAN) σε πολλές *περιοχές ευρυεκπμπής* χωρίς την χρήση δρομολογητή. Επίσης, αποτελούν έναν τρόπο να έχουμε κόμβους που βρίσκονται σε απομακρυσμένη φυσική τοποθεσία ο ένας από τον άλλον, στο ίδιο τοπικό δίκτυο (LAN).

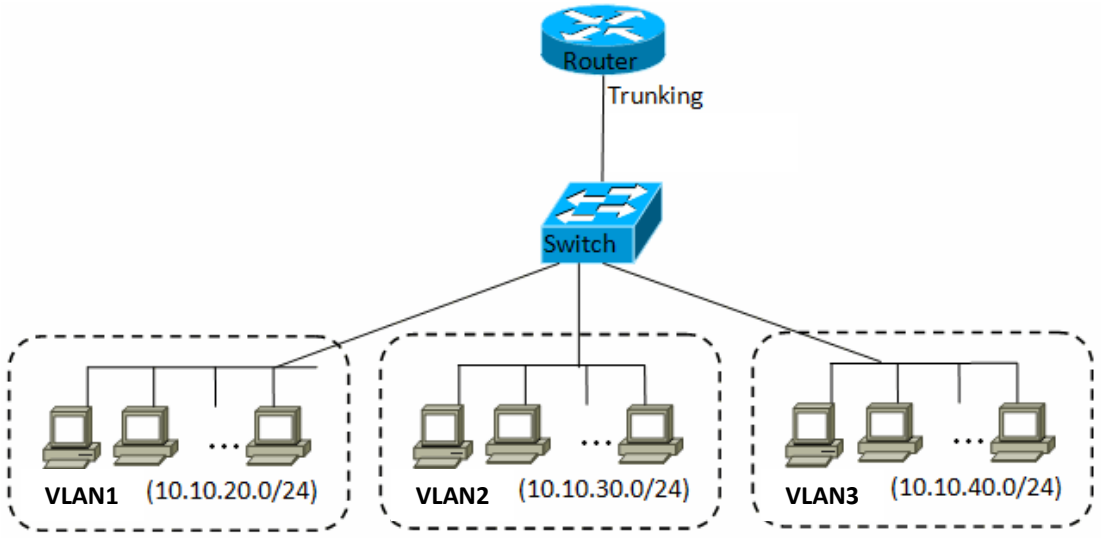
Ας φανταστούμε ένα LAN με ένα πλήθος κόμβων συνδεδεμένους στην κεντρική δικτυακή συσκευή η οποία είναι ένα switch. Μπορούμε να ομαδοποιήσουμε τους κόμβους του δικτύου σε μικρότερες ομάδες οι οποίες θα αποτελούν η κάθε μια ένα VLAN (Εικόνα 30). Οι κόμβοι που θα ανήκουν στο ίδιο VLAN θα πρέπει να ανήκουν και στο ίδιο υποδίκτυο. Στην Εικόνα 30 φαίνεται ότι όλοι οι κόμβοι που ανήκουν στο **VLAN 1** ανήκουν στο υποδίκτυο 10.10.20.0/24. Οι κόμβοι που ανήκουν στο **VLAN 2** ανήκουν στο υποδίκτυο 10.10.30.0/24 και οι κόμβοι του **VLAN 3** στο υποδίκτυο 10.10.40.0/24.



Εικόνα 30. Ομαδοποίηση των κόμβων ενός δικτύου σε VLANs.

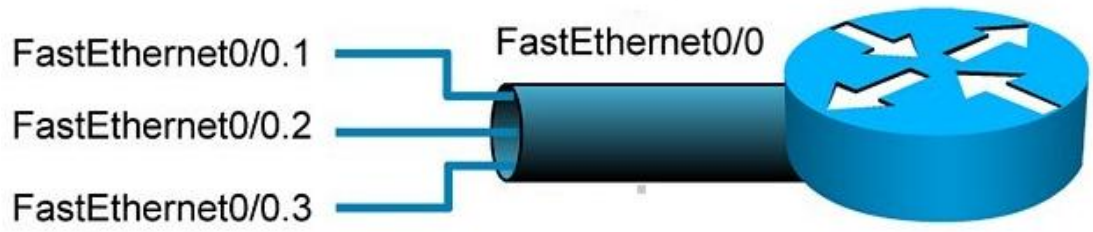
Με τη χρήση των VLAN υποδικτυώσαμε ένα τοπικό δίκτυο χωρίς τη χρήση δρομολογητών. Για να γίνει αυτό οι προϋποθέσεις είναι η ρύθμιση των θυρών (ports) στο switch και η ανάλογη διευθυνσιοδότηση των κόμβων.

Με μια τέτοια ρύθμιση οι κόμβοι που ανήκουν στο ένα VLAN δεν μπορούν να επικοινωνήσουν με τους κόμβους σε ένα άλλο VLAN διότι το switch δεν προωθεί τα πακέτα του ενός υποδικτύου σε άλλο υποδίκτυο. Εάν επιθυμούμε την επικοινωνία μεταξύ των VLANs είναι απαραίτητη η χρήση δρομολογητή. Στην Εικόνα 31 φαίνεται αυτή η διάταξη. Ο δρομολογητής λογικά θα πρέπει να έχει τουλάχιστον τρία interface, ένα για το κάθε VLAN. Αυτό φυσικά είναι αδύνατον να γίνει καθώς τα LAN αυτά είναι εικονικά και για αυτό βλέπουμε την σύνδεση του δρομολογητή με ένα μόνο interface.



Εικόνα 31. Επικοινωνία VLANs μέσω δρομολογητή.

Με εικονικό τρόπο «διασπάμε» το interface αυτό του δρομολογητή σε τρια sub-interfaces, ένα για το κάθε VLAN. Αυτό φαίνεται στην Εικόνα 32. Το interface FastEthernet 0/0 «σπάει» σε τρία (FastEthernet0/0.1, FastEthernet0/0.2, FastEthernet0/0.3) όπου το κάθε ένα θα πρέπει να ανήκει σε διαφορετικό VLAN.



Εικόνα 32. Sub-interfaces σε έναν δρομολογητή.

Στον Πίνακα 6 φαίνεται η διευθυνσιοδότηση των sub-interfaces του δρομολογητή.

Sub-interface	VLAN Number	IP address
FastEthernet0/0.1	1	10.10.20.1/24
FastEthernet0/0.2	2	10.10.30.1/24
FastEthernet0/0.3	3	10.10.40.1/24

Πίνακας 6. Διευθυνσιοδότηση των Sub-interfaces του δρομολογητή της Εικόνας 23.

Η σύνδεση του δρομολογητή με το switch (αυτή που έχει διασπαστεί δηλαδή) ονομάζεται trunk (κορμός) και χρησιμοποιεί ένα πρωτόκολλο για την τοποθέτηση «ετικετών» (VLAN tagging) στα πακέτα που προέρχονται από ένα VLAN και έχουν προορισμό ένα άλλο VLAN. Στην πράξη τοποθετείται μια νέα επικεφαλίδα η οποία

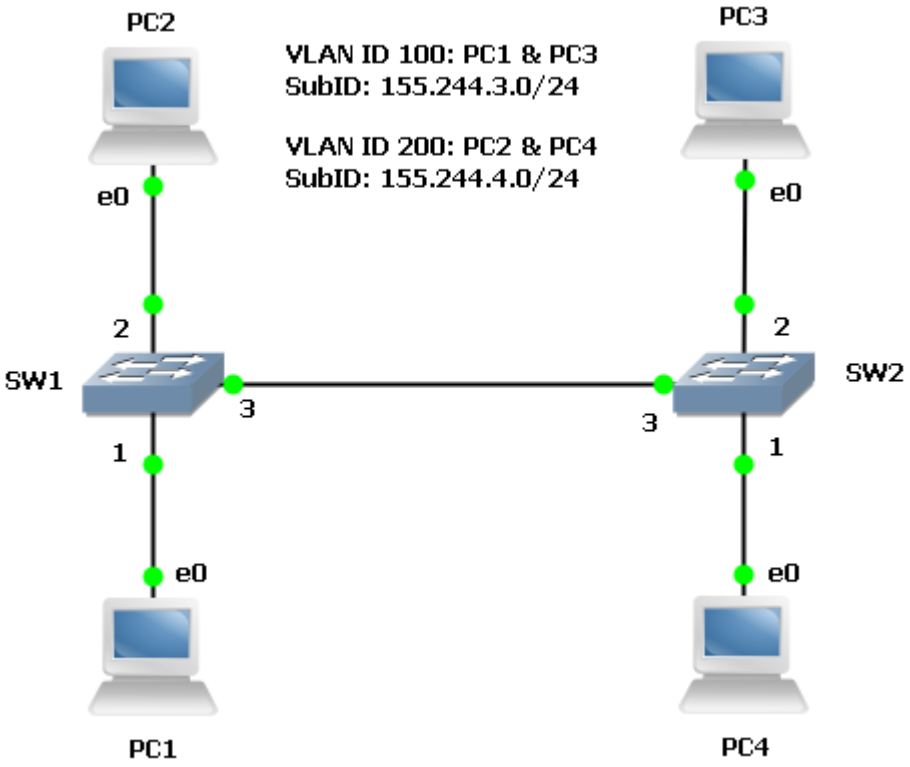
προσδιορίζει το VLAN από το οποίο προέρχεται το πακέτο (VLAN ID), έτσι ώστε το switch να γνωρίζει σε ποιο VLAN ανήκει το κάθε πακέτο. Το πρωτόκολλο που χρησιμοποιείται συνήθως είναι το IEEE 802.1Q και η τοπολογία ονομάζεται router-on-a-stick.

9.1 Δημιουργία VLANs

Δημιουργείστε ένα νέο project στον GNS3 με την ονομασία *VLAN* και κατόπιν κατασκευάστε το δίκτυο της Εικόνας 33.

Οι κόμβοι PC1 και PC3 ανήκουν στο ίδιο VLAN με VLAN ID: 100, παρόλο που μπορεί να βρίσκονται σε απομακρυσμένα σημεία (π.χ. σε διαφορετικά κτίρια). Η IP διεύθυνση του υποδικτύου που ανήκουν και οι δύο είναι η 155.244.3.0/24. Οι κόμβοι PC2 και PC4 ανήκουν στο ίδιο VLAN με VLAN ID: 200 με IP διεύθυνση του υποδικτύου την 155.244.4.0/24.

Συνοπτικά οι IP διευθυνσιοδότηση των συσκευών που πρέπει να ρυθμιστεί φαίνεται στον Πίνακα 7.



Εικόνα 33. Η τοπολογία του project *VLAN*.

VLAN	Member	Subnet	IP address
100	PC1	155.244.3.0/24	155.244.3.1/24
	PC3		155.244.3.2/24
200	PC2	155.244.4.0/24	155.244.4.1/24
	PC4		155.244.4.2/24

Πίνακας 7. Διευθυνσιοδότηση των συσκευών για το project *VLAN*.

Στον PC1 δώστε τις εξής εντολές:

```
PC1> ip 155.244.3.1 255.255.255.0

Checking for duplicate address...

PC1 : 155.244.3.1 255.255.255.0

PC1> save pc1

Saving startup configuration to pc2.vpc

.  done
```

Στον PC3 δώστε τις εξής εντολές:

```
PC3> ip 155.244.3.2 255.255.255.0

Checking for duplicate address...

PC3 : 155.244.3.2 255.255.255.0

PC3> save pc3

Saving startup configuration to pc2.vpc

.  done
```

Στον PC2 δώστε τις εξής εντολές:

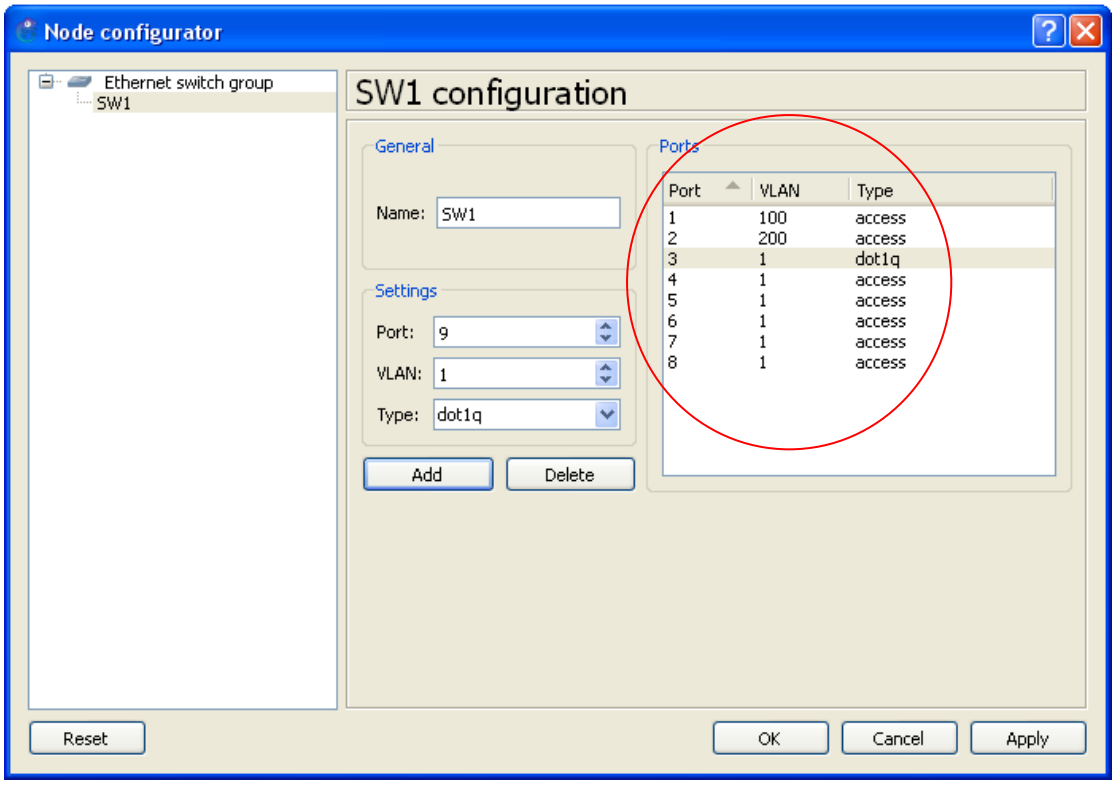
```
PC2> ip 155.244.4.1 255.255.255.0

Checking for duplicate address...

PC2 : 155.244.4.1 255.255.255.0

PC2> save pc2

Saving startup configuration to pc2.vpc

.  done
```

Στον PC4 δώστε τις εξής εντολές:

```
PC4> ip 155.244.4.2 255.255.255.0

Checking for duplicate address...

PC4 : 155.244.4.2 255.255.255.0


PC4> save pc4

Saving startup configuration to pc4.vpc

.  done
```

Παρατηρείστε ότι στις παραπάνω εντολές δεν συμπεριλάβαμε διεύθυνση gateway.

Η σύνδεση μεταξύ των δύο switch είναι μια trunk σύνδεση και πρέπει να γίνουν οι κατάλληλες ρυθμίσεις στα δύο switch. Κάντε δεξί κλίκ επάνω στο SW1 και επιλέξτε configure. Κατόπιν κάντε τις ρυθμίσεις που φαίνονται στην Εικόνα 34.



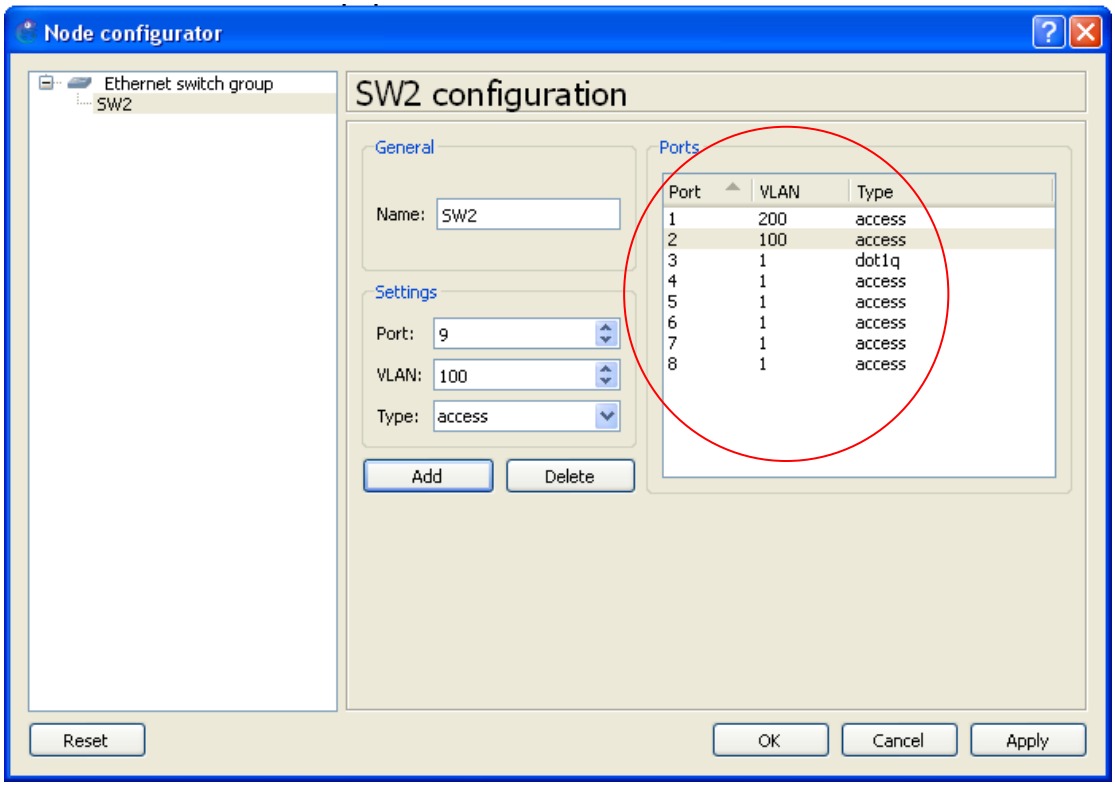
Εικόνα 34. Ρυθμίσεις στο SW1.

Εδώ ορίσαμε ότι το port 1 (σύνδεση στον PC1) του SW1 θα είναι ένα access port (όχι trunk) και θα ανήκει στο VLAN με VLAN ID 100. Το port 2 (σύνδεση στον PC2) του SW1 θα είναι ένα access port (όχι trunk) και θα ανήκει στο VLAN με VLAN ID 200. Το port 3 (σύνδεση στο SW2) του SW1 θα είναι ένα trunk port και θα χρησιμοποιεί το IEEE 802.1Q πρωτόκολλο.

Ανάλογες ρυθμίσεις πρέπει να γίνουν και στο SW2, όπως φαίνεται στην Εικόνα 35.

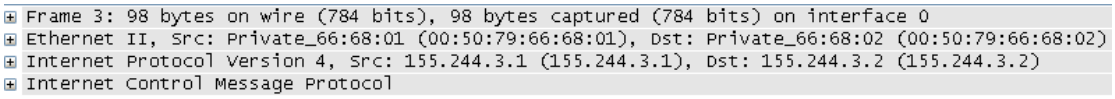
Ξεκινήστε την καταγραφή της ζεύξης μεταξύ των SW1 και SW2 και της ζεύξης μεταξύ PC1 και SW1 με το Wireshark. Θα πρέπει να έχετε ανοικτά δύο παράθυρα του Wireshark. και στην συνέχεια εκτελέστε την εντολή ping στον PC1 με προορισμό τον PC3:

```
PC1> ping 155.244.3.2

84 bytes from 155.244.3.2 icmp_seq=1 ttl=64 time=0.000 ms

84 bytes from 155.244.3.2 icmp_seq=2 ttl=64 time=0.000 ms

84 bytes from 155.244.3.2 icmp_seq=3 ttl=64 time=0.000 ms

84 bytes from 155.244.3.2 icmp_seq=4 ttl=64 time=0.000 ms

84 bytes from 155.244.3.2 icmp_seq=5 ttl=64 time=0.000 ms
```



Εικόνα 35. Ρυθμίσεις στο SW2.

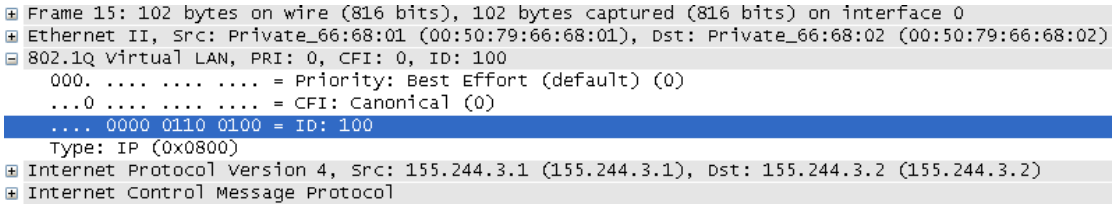
Στο Wireshark θα πρέπει να έχετε καταγράψει όλη την αλληλουχία των ICMP echo request και reply. Μεταφερθείτε στο παράθυρο του Wireshark που κατέγραψε τα πακέτα που μεταφέρθηκαν στην ζεύξη μεταξύ του PC1 και SW1 και αναλύστε το πρώτο ICMP echo request (Εικόνα 36).



Εικόνα 28. Καταγραφή ICMP echo request στη ζεύξη PC1-SW1.

Παρατηρείστε ότι το πακέτο αποτελείται από τις αναμενόμενες επικεφαλίδες (Ethernet, ICMP και IP).

Τώρα μεταφερθείτε στο παράθυρο του Wireshark που κατέγραψε την ίδια επικοινωνία αλλά στην ζεύξη μεταξύ SW1 και SW2 (Εικόνα 29).



Εικόνα 36. Καταγραφή ICMP echo request στη ζεύξη SW1-SW2.

Παρατηρείστε ότι πλέον το ίδιο ICMP echo request διαθέτει ακόμα μια επικεφαλίδα (802.1Q). Αναλύοντας την μπορούμε να δούμε ότι στα περιοχόμενα της περιλαμβάνεται το VLAN ID 100 το οποίο προσδιορίζει ότι το ICMP echo request στάλθηκε από κόμβο που ανήκει στο VLAN 100 (PC1). Αυτή η πληροφορία βοηθά το SW2 να γνωρίζει από ποιο VLAN στάλθηκε το πακέτο και σε ποιο VLAN μπορεί να μεταφερθεί.

Πριν ολοκληρώσουμε προσπαθήστε να κάνετε ping στον PC1 με προορισμό τον PC4. Θα δείτε ότι αυτό δεν είναι δυνατόν καθώς οι δύο κόμβοι βρίσκονται σε διαφορετικά VLANs. Για να μπορέσουμε να έχουμε επικοινωνία μεταξύ κόμβων σε διαφορετικά VLAN θα πρέπει να εφαρμόσουμε την τοπολογία Router-on-a-stick.

11. Εργαστηριακές Ασκήσεις

Σε αυτή τη παράγραφο δίνονται μερικές εργαστηριακές ασκήσεις για την εξάσκηση των φοιτητών στη χρήση του GNS3 και σε κάποια από τα θέματα που αναλύθηκαν προτύτερα στο βιβλίο.

11.1 Εργαστηριακή Άσκηση 1

Η παρούσα άσκηση αφορά στην απόδοση IP διευθύνσεων σε συσκευές και στην στατική δρομολόγηση.

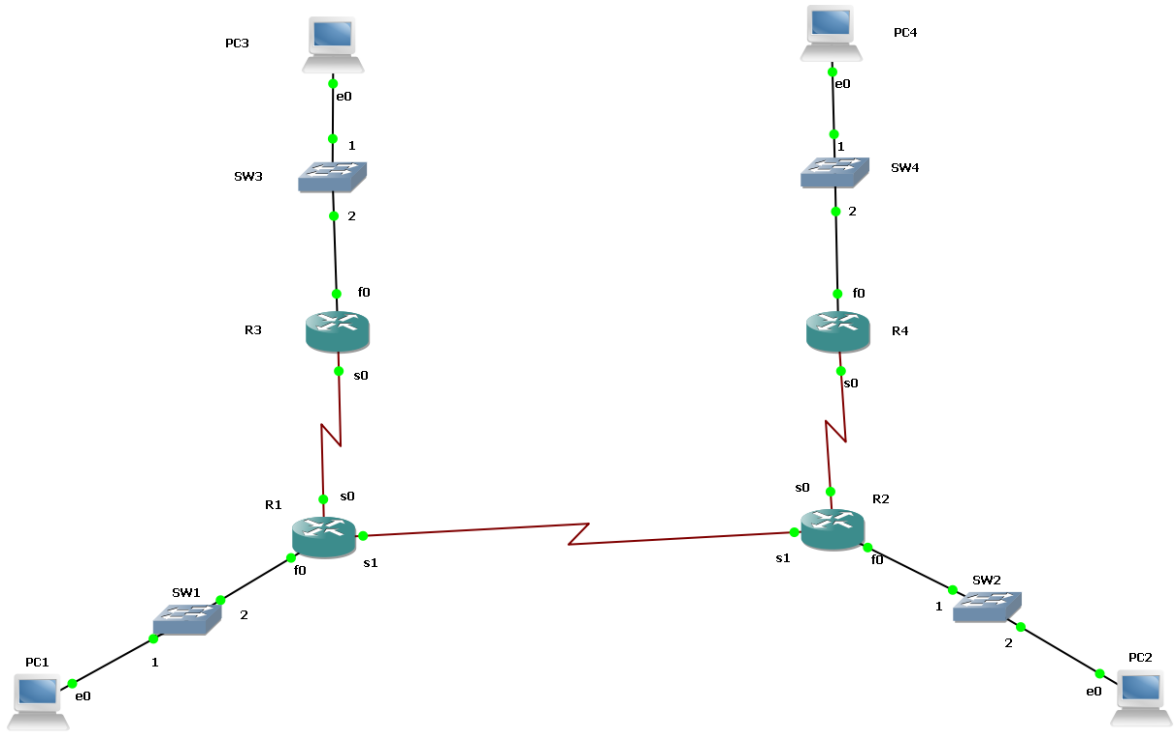
Α) Να δημιουργηθεί το δίκτυο που φαίνεται στην Εικόνα 37 στο GNS3.

Β) Έχετε στην διάθεση σας την διεύθυνση 97.0.0.0/8. Να αποδώσετε με στατικό τρόπο IP διευθύνσεις στις διεπαφές των συσκευών (χωρίς τη χρήση DHCP). Λάβετε υπόψιν ότι επιθυμούμε να δεσμεύσουμε τον μικρότερο δυνατό αριθμό bits από τα διαθέσιμα hostID bits για την απόδοση ταυτότητας στα υποδίκτυα (subnetID). Να κάνετε όλες τις ρυθμίσεις στους κόμβους (PCs και δρομολογητές) για την απόδοση των σωστών IP διευθύνσεων.

Γ) Ρυθμίστε τον δρομολογητή R2 να αποδίδει IP παραμέτρους στον PC2 με τη χρήση του DHCP.

Δ) Να κάνετε τις κατάλληλες στατικές δρομολογήσεις στους δρομολογητές έτσι ώστε το δίκτυο να είναι πλήρως λειτουργικό (όλοι οι κόμβοι να μπορούν να επικοινωνήσουν με τους υπόλοιπους).

Ε) Να αντικατασταθούν (όπου είναι αυτό εφικτό) οι στατικές καταχωρήσεις με προκαθορισμένες διαδρομές (default routes) και το δίκτυο να παραμείνει πλήρως λειτουργικό.



Εικόνα 37. Το δίκτυο για την εργαστηριακή άσκηση 11.1.

11.2 Εργαστηριακή Άσκηση 2

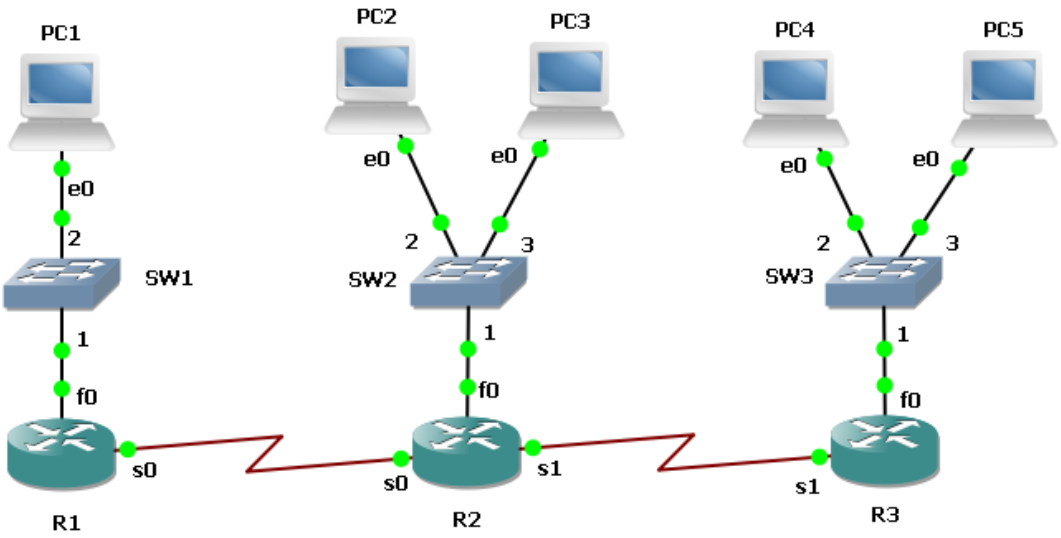
Η παρούσα άσκηση αφορά στην απόδοση IP διευθύνσεων σε συσκευές και στην εφαρμογή πρωτοκόλλων δυναμικής δρομολόγησης.

Α) Να δημιουργηθεί το δίκτυο που φαίνεται στην Εικόνα 38 στο GNS3.

Β) Έχετε στην διάθεση σας την διεύθυνση 175.59.0.0/16. Να αποδώσετε με στατικό τρόπο IP διευθύνσεις στις διεπαφές των συσκευών (χωρίς τη χρήση DHCP). Λάβετε υπόψιν ότι επιθυμούμε να δεσμεύσουμε τον μεγαλύτερο δυνατό αριθμό bits από τα διαθέσιμα hostID bits για την απόδοση ταυτότητας στα υποδίκτυα (subnetID).

Γ) Να εφαρμοστεί το πρωτόκολλο RIP ως πρωτόκολλο δρομολόγησης στις συσκευές δρομολόγησης.

Δ) Να εφαρμοστεί το πρωτόκολλο OSPF ως πρωτόκολλο δρομολόγησης στις συσκευές δρομολόγησης.



Εικόνα 38. Το δίκτυο για την εργαστηριακή άσκηση 11.2.

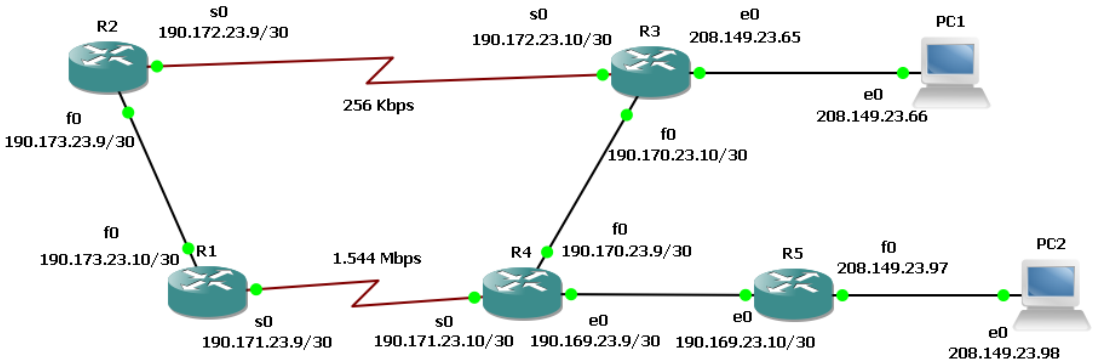
11.3 Εργαστηριακή Άσκηση 3

Η παρούσα άσκηση αφορά στη σύγκριση των πρωτοκόλλων δρομολόγησης RIP και OSPF.

Α) Να δημιουργηθεί το δίκτυο που φαίνεται στην Εικόνα 39 στο GNS3 και να δοθούν οι IP διευθύνσεις που φαίνονται στις διεπαφές.

Β) Να εφαρμόσετε το RIP πρωτόκολλο στις συσκευές δρομολόγησης και να καταγράψετε τους πίνακες δρομολόγησης όλων των δρομολογητών. Να ερμηνευτούν τα αποτελέσματα.

Γ) Να εφαρμόσετε το OSPF πρωτόκολλο στις συσκευές δρομολόγησης και να καταγράψετε τους πίνακες δρομολόγησης όλων των δρομολογητών. Να ερμηνευτούν τα αποτελέσματα.



Εικόνα 39. Το δίκτυο για την εργαστηριακή άσκηση 11.3.

12. Βιβλιογραφία

[1] *http://rednectar.net/2014/08/17/vpcs-tutorial-updated/*

[2] RFC 2132, "DHCP Options and BOOTP Vendor Extensions", IETF, 1997.

[3] RFC 951, "Bootstrap Protocol (BOOTP)", IETF, 1985.

[4] RFC 1542, "Clarifications and Extensions for the Bootstrap Protocol", IETF, 1993.

[5] *CCNA Routing and Switching 200-120 Official Cert Guide Library*, Wendell Odom.

[6] *CCNA Routing and Switching 200-120 Exam Cram*, Michael Valentine and Keith Barker

[7]*http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html*

[8]*http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/27082-ip-static-routes.html*

[9]*http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro-cfg.html*

[10]*http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html*

[11]*http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html*

[12] *http://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-lla.html*

Παράρτημα Α

Σύνδεση τερματικού στη θύρα console δικτυακών συσκευών

Η ρύθμιση των συσκευών δρομολόγησης ή μεταγωγής της εταιρίας Cisco προϋποθέτει την φυσική διασύνδεση ενός τερματικού σταθμού στη διαθέσιμη θύρα με την ένδειξη console η οποία μπορεί να βρεθεί είτε στην πρόσθια είτε στην οπίσθια όψη της συσκευής. Το καλώδιο που απαιτείται λέγεται rollover cable και διαθέτη στη μία άκρη του έναν συνδετήρα τύπου RJ-45 ενώ στην άλλη έναν συνδετήρα σειριακής σύνδεσης (DB-9 θηλυκό). Το καλώδιο παρέχεται στη συσκευασία της συσκευής και το χρώμα του είναι γαλάζιο για να ξεχωρίζει από τα υπόλοιπα δικτυακά καλώδια (Εικόνα Α.1).

Εικόνα Α.1. Rollover cable.

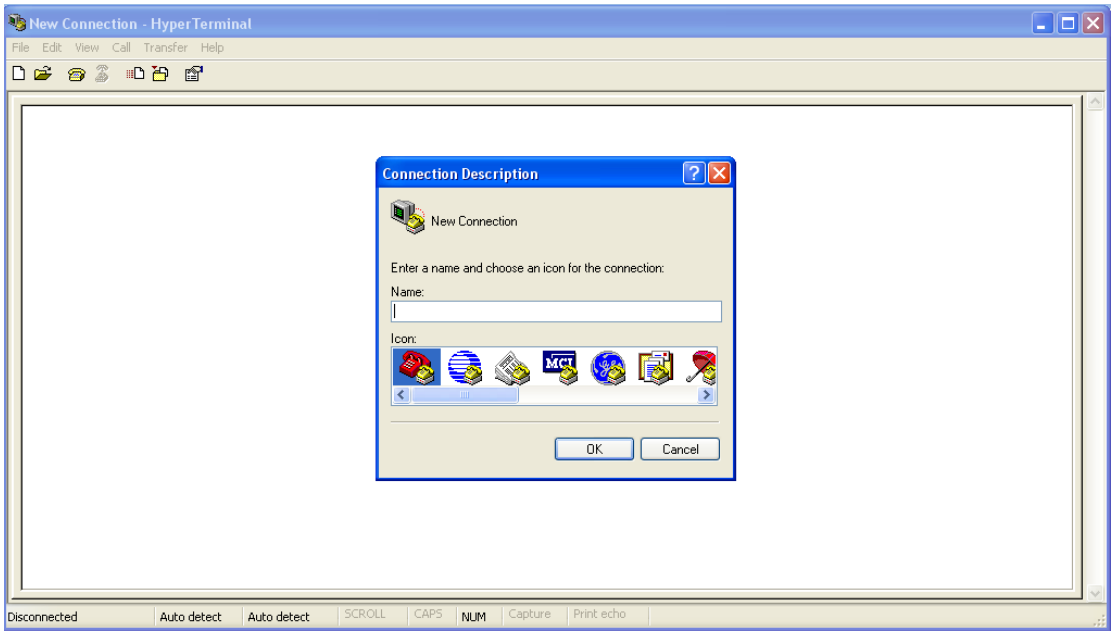
Η άκρη του καλωδίου με τον RJ-45 συνδετήρα θα πρέπει να τοποθετηθεί στην θύρα console της δικτυακής συσκευής και η άκρη με τον σειριακό συνδετήρα στον τερματικό σταθμό (PC).

Αφού κάνετε τις απαραίτητες φυσικές συνδέσεις του καλωδίου θα πρέπει να χρησιμοποιήσετε ένα λογισμικό επικοινωνίας για την πρόσβαση στο λειτουργικό σύστημα της δικτυακής συσκευής. Ένα από τα γνωστότερα λογισμικά είναι το Hyperterminal του λειτουργικού συστήματος Windows το οποίο όμως έπαψε να υποστηρίζεται στις σύγχρονες εκδόσεις του λειτουργικού. Ένα εναλλακτικό πρόγραμμα είναι το PuTTY το οποίο παρέχεται δωρεάν (είναι open source) και αποτελεί μια εφαρμογή πελάτη (client) για χρήση με τα πρωτόκολλα Telnet, rlogin και SSH. Ωστόσο μπορεί να χρησιμοποιηθεί και ως εξομοιωτής τερματικού (terminal emulator) σε σειριακές συνδέσεις.

Παρακάτω περιγράφονται οι τρόποι ρύθμισης του Hyperterminal (Windows) και PuTTY.

A. *Hyperterminal*

Ανοίξτε το Hyperterminal επιλέγοντας *Start* → *All Programs* → *Accessories* → *Communications* → *HyperTerminal*. Στην οθόνη σας θα αντικρύσετε αυτό που φαίνεται στην Εικόνα Α.2.



Εικόνα Α.2. Το Hyperterminal των Windows.

Δώστε μια ονομασία και επιλέξτε ένα εικονίδιο της αρεσκείας σας στο παράθυρο *Connection Description* και πατήστε OK. Θα εμφανιστεί ένα νέο παράθυρο με την ονομασία που μόλις δώσατε. Στην επιλογή *Connect using:* επιλέξτε τη θύρα COM στην οποία έχετε συνδέσει το console cable στον υπολογιστή σας και πατήστε OK. Στο αμέσως επόμενο παράθυρο κάντε τις εξής ρυθμίσεις:

- Baud: 9600
- Data bits: 8
- Parity: No
- Stop bits: 1
- Flow control: None

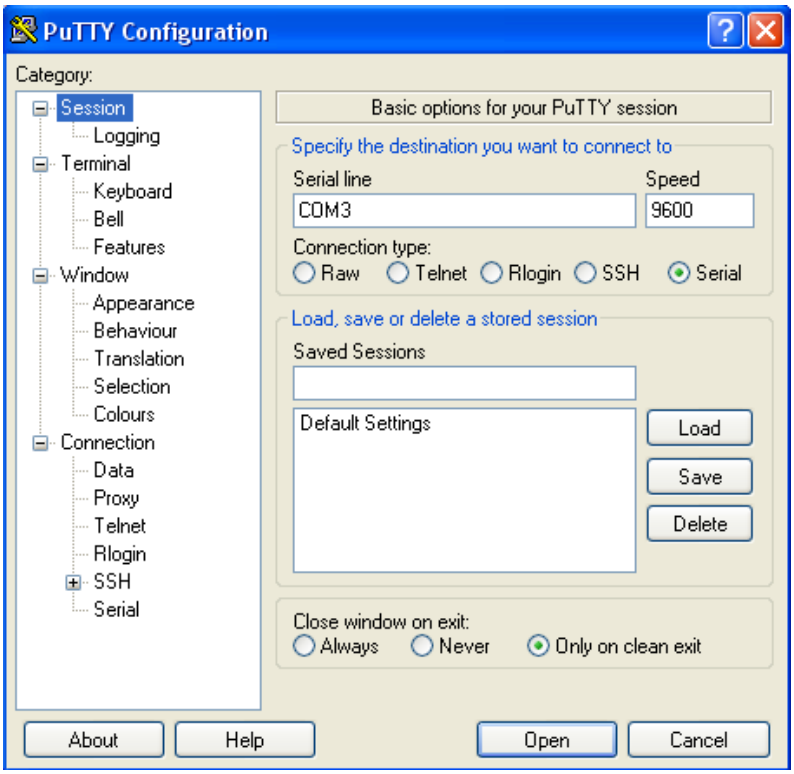
Κατόπιν πατήστε OK. Θα πρέπει να έχετε μεταφερθεί στο λειτουργικό σύστημα της συσκευής δρομολόγησης.

B. *PuTTY*

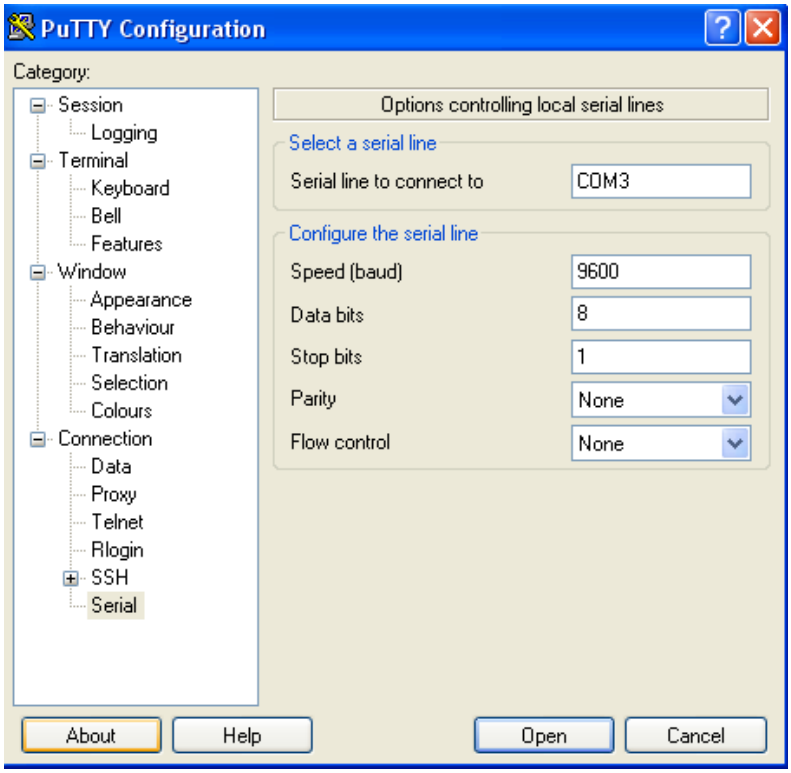
Αποκτήστε το PuTTY και εγκαταστήστε το στον υπολογιστή σας. Όταν θα το εκτελέσετε θα πρέπει να δείτε ένα παράθυρο σαν αυτό που φαίνεται στην Εικόνα Α.3. Στο πεδίο *Host Name (or IP address)* γράψτε την θύρα COM στην οποία είναι συνδεδεμένο το console cable στον υπολογιστή σας (π.χ. COM3). Μετά τσεκάρετε την επιλογή *Serial* που βρίσκεται στο *Connection Type*.

Κατόπιν από τις επιλογές που φαίνονται αριστερά επιλέξτε *Serial* και εκεί κάντε τις ίδιες ρυθμίσεις που κάναμε και στο Hyperterminal (Επιλέξτε θύρα COM και ρυθμίστε Baud, Data

bits, Parity, Stop bits και Flow control) (Εικόνα Α.4). Τέλος, πατήστε *Open*. Θα πρέπει να έχετε συνδεθεί στο λειτουργικό σύστημα της συσκευής.



Εικόνα Α.3. Ρύθμιση του PuTTY.



Εικόνα Α.4. Ρύθμιση του PuTTY.

Παράρτημα Β

Ανάκτηση συνθηματικού συσκευής δρομολόγησης

Φανταστείτε την περίπτωση που ένας διαχειριστής λησμόνησε (!) το συνθηματικό που είχε ρυθμίσει παλαιότερα σε μια συσκευή δρομολόγησης. Ευτυχώς υπάρχει τρόπος ανάκτησης του και ρύθμισης του εκ νέου. Η μόνη απαίτηση είναι η φυσική πρόσβαση στην συσκευή. Αυτό σημαίνει ότι η διαδικασία ανάκτησης δεν μπορεί να γίνει απομακρυσμένα (π.χ. μέσω telnet). Μπορείτε να ακολουθήσετε τα παρακάτω βήματα για την ανάκτηση του συνθηματικού και των ρυθμίσεων:

Βήμα 1: Έχοντας την συσκευή σε λειτουργία συνδεθείτε στην θύρα console του δρομολογητή με το *rollover cable*.

Βήμα 2: Συνδεθείτε με τη χρήση ενός λογισμικού επικοινωνίας (π.χ. *hyperterminal*) στην συσκευή. Οι ρυθμίσεις που θα πρέπει να γίνουν είναι:

Βήμα 3: Εκτελέστε επανεκκίνηση στην συσκευή (κλείνοντας και ανοίγοντας τον διακόπτη παροχής).

Βήμα 4: Στο πληκτρολόγιο πιέστε το πλήκτρο *Break* (συνήθως βρίσκεται μαζί με το *Pause* και μπορείτε να το επιλέξετε με πατημένο το πλήκτρο *Ctrl*) όσες φορές χρειάζεται προκειμένου να διακοπεί η διαδικασία φόρτωσης ρυθμίσεων.

Βήμα 5: Στο prompt (το οποίο θα πρέπει να δείχνει `rommon 1>`) πληκτρολογήστε την εντολή `confreg 0x2142`. Η ρύθμιση αυτή λέει στην συσκευή να παρακάμψει την NVRAM (δηλαδή να μην φορτωθεί το αρχείο `startup configuration`).

Βήμα 6: Πληκτρολογήστε `reset` για την επανεκκίνηση της συσκευής και επιλέξτε no στην ερώτηση `Would you like to enter the initial configuration dialog? [yes/no]:`

Βήμα 7: Τώρα πλέον θα δείτε ότι βρίσκεστε μέσα στο IOS και μπορείτε να μεταφερθείτε στην κατάσταση διαχείρισης με την εντολή `enable` και να ρυθμίσετε εκ νέου το password ή ακόμα και να διαγράψετε το αρχείο `startup configuration` για να κάνετε νέες ρυθμίσεις.

Βήμα 8: Αφού κάνετε τις ρυθμίσεις που σας βολεύουν εκτελέστε την εντολή `config-register 0x2102` στην κατάσταση ρυθμίσεων `config`. Αυτό θα επαναφέρει την συσκευή ώστε να μην παρακάμπτει πλέον την NVRAM και το νέο αρχείο `startup configuration` που μόλις φτιάξατε.

Βήμα 9: Εκτελέστε την εντολή reload έξω από την κατάσταση ρυθμίσεων config για να επανεκκινήσετε την συσκευή και να λάβουν χώρα οι νέες ρυθμίσεις.