

Ασφάλεια Δικτύων

Εργασία στο Packet Tracer

Δημήτρης Δεδούσης

28/4/2015

Περιεχόμενα

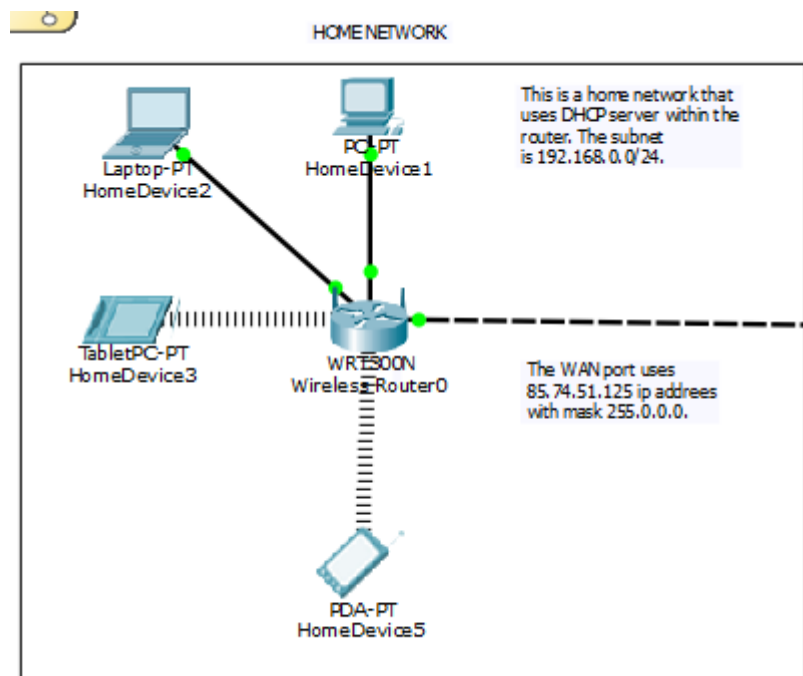
| | |
|---|---|
| Εισαγωγή..... | 2 |
| 1. Τοπολογία δικτύου | 2 |
| 2. Δρομολόγηση..... | 4 |
| 3. Network Address Translation (NAT)..... | 5 |
| 4. Port Security | 6 |
| 5. Υπηρεσίες..... | 8 |
| 6. Access Lists | 8 |

Εισαγωγή

Για την υλοποίηση της εργασίας αυτής χρησιμοποιήθηκε το πρόγραμμα Packet Tracer της Cisco, έκδοση 6.1.0.0120. Σκοπός της εργασίας ήταν η εξοικείωση του φοιτητή στον προγραμματισμό δικτυακών συσκευών όπως Router και Switches καθώς επίσης και η εξάσκηση στην δημιουργία τοπολογιών, χρήση δικτυακών πρωτοκόλλων, πρόβλεψη αναγκών ασφάλειας και υλοποίηση υπηρεσιών δικτύου.

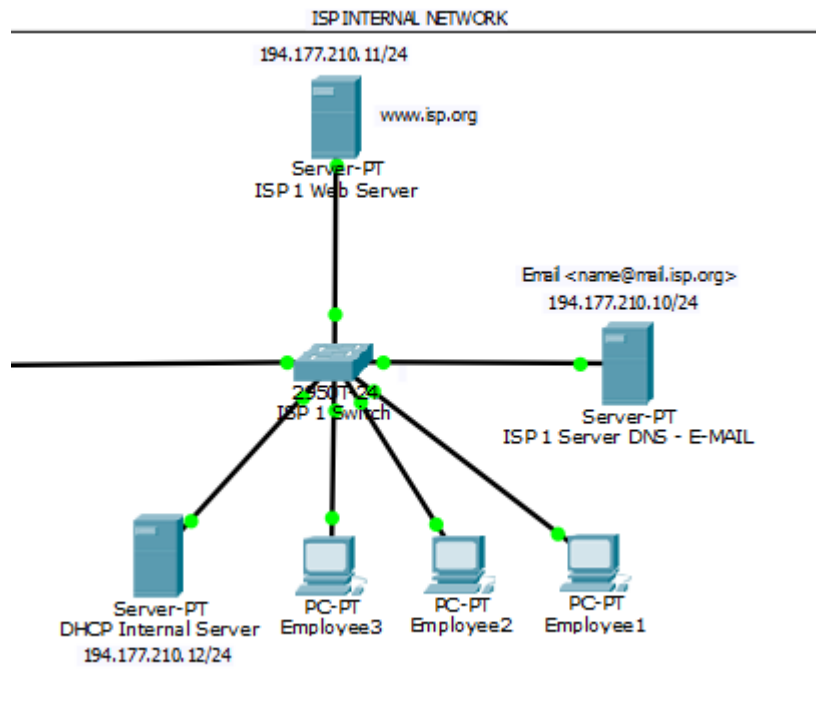
1. Τοπολογία δικτύου

Το δίκτυο το οποίο σχεδιάστηκε χωρίζεται σε τέσσερις διαφορετικές περιοχές με τέτοιο τρόπο ώστε να υπάρχει επικοινωνία μεταξύ των περιοχών αυτών. Οι περιοχές αυτές είναι, ένα οικιακό δίκτυο (Home Network), ένας πάροχος υπηρεσιών (Internet Service Provider - ISP) και δύο εταιρικά δίκτυα. Η κάθε μία από αυτές τις περιοχές έχει διαφορετική τοπολογία. Στην Εικόνα 1.1. απεικονίζεται η τοπολογία του οικιακού δικτύου



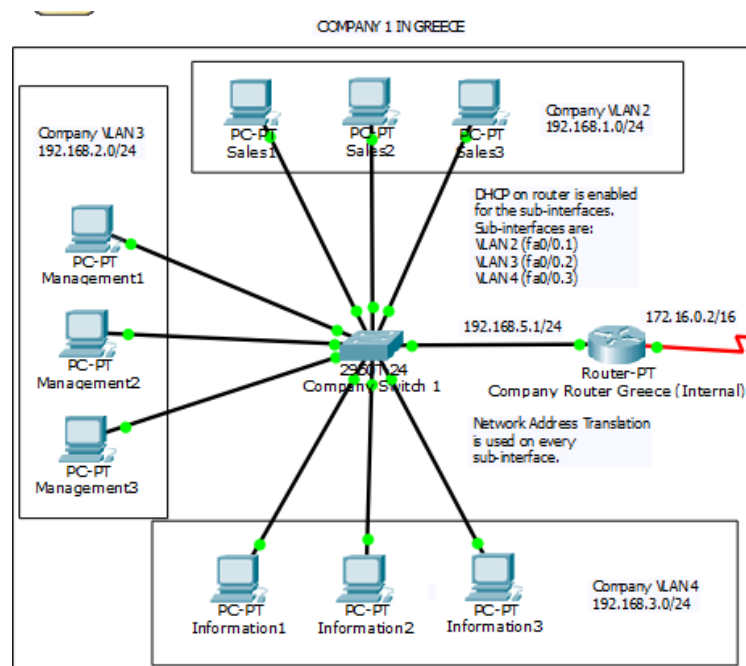
Εικόνα 1.1. Οικιακό δίκτυο.

Όπως βλέπουμε στην παραπάνω εικόνα, το οικιακό δίκτυο είναι αρκετά απλό και αποτελείται από δύο ενσύρματες συσκευές (HomeDevice1 και HomeDevice2), καθώς επίσης και από δύο ασύρματες συσκευές (HomeDevice3 και HomeDevice5). Το router που χρησιμοποιείται είναι ένα ασύρματο LinkSys wrt300 router το οποίο έχει τρεις βασικές λειτουργίες. Η πρώτη είναι η μετάφραση εσωτερικών ιδιωτικών διευθύνσεων σε μια δημόσια διεύθυνση (Network Address Translation – NAT), η δεύτερη είναι η απόδοση ιδιωτικών διευθύνσεων στις συσκευές που βρίσκονται στο εσωτερικό δίκτυο (Dynamic Host Configuration Protocol - DHCP) και τέλος η δρομολόγηση των πακέτων από το εσωτερικό δίκτυο στο εξωτερικό δίκτυο. Στην Εικόνα 1.2. απεικονίζεται το εσωτερικό δίκτυο του παρόχου υπηρεσιών.

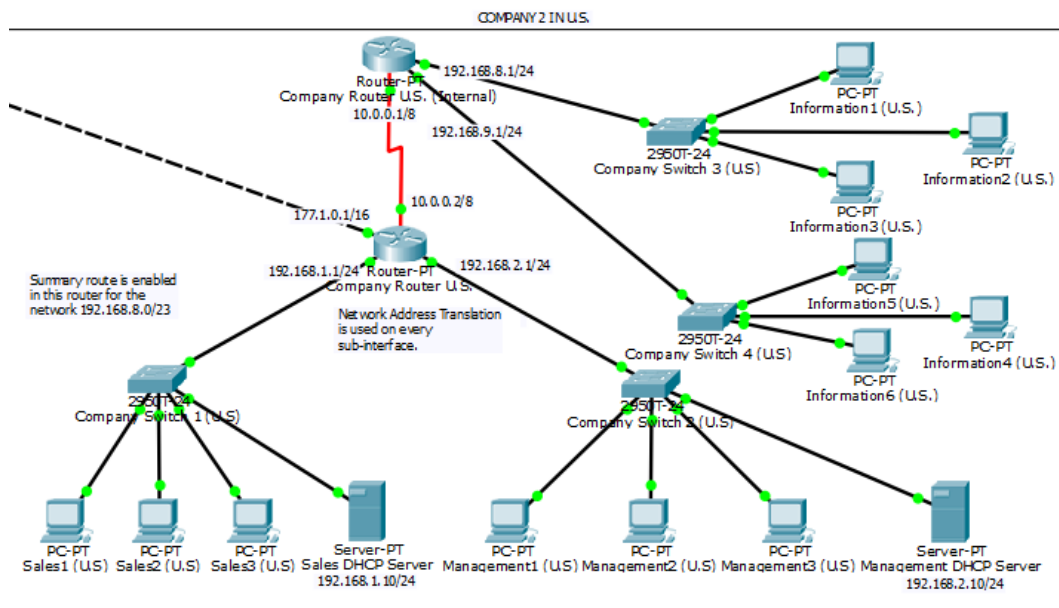


Εικόνα 1.2. Πάροχος υπηρεσιών (ISP).

Η τοπολογία του παρόχου υπηρεσιών αποτελείται από κάποιους υπολογιστές εργαζομένων καθώς επίσης και έναν DHCP server για την απόδοση διευθύνσεων στους υπολογιστές αυτούς. Αντίθετα υπάρχουν ακόμα δύο μηχανήματα τα οποία είναι προσβάσιμα από το κοινό και προσφέρουν τις ακόλουθες υπηρεσίες Web Server, DNS server και E-mail server. Στις Εικόνες 1.3. και 1.4. αναπαρίστανται οι τοπολογίες των δύο εταιριών.



Εικόνα 1.3. Τοπολογία της εταιρίας που βρίσκεται στην Ελλάδα.



Εικόνα 1.4. Τοπολογία της εταιρίας που βρίσκεται στην Αμερική.

Οι δύο παραπάνω τοπολογίες μπορεί να φαίνονται διαφορετικές αλλά οι βασικές αρχές που τις διέπουν είναι οι ίδιες. Οι δρομολογητές οι οποίοι προσφέρουν την επικοινωνία του εσωτερικού δικτύου με το δημόσιο δίκτυο υλοποιούν μετάφραση διευθύνσεων έτσι ώστε οι εσωτερικές συσκευές να μην μπορούν να είναι προσβάσιμες από τον έξω κόσμο. Η εταιρία στην Ελλάδα έχει χωρισμένα τα τμήματα της σε ξεχωριστά VLAN's και στο router έχουν γίνει ρυθμίσεις ώστε να μπορούν να δρομολογηθούν αυτά τα VLAN's στον έξω κόσμο. Το router επίσης προσφέρει την δυνατότητα διευθυνσιοδότησης ώστε ο κάθε υπολογιστής να μην έχει στατική διεύθυνση δικτύου. Αντίθετα στην τοπολογία της εταιρίας που βρίσκεται στην Αμερική υπάρχουν DHCP servers ώστε να γίνει η διευθυνσιοδότηση των υπολογιστών καθώς επίσης έχει γίνει ένας διαχωρισμός κάποιων από των τμημάτων με την χρήση περισσότερων του ενός δρομολογητή.

2. Δρομολόγηση

Για να υπάρξει επικοινωνία μεταξύ των παραπάνω περιοχών έχουν χρησιμοποιηθεί ενδιάμεσοι δρομολογητές στους οποίους έχει γίνει δυναμική δρομολόγηση με την χρήση του πρωτοκόλλου RIP (Routing Information Protocol). Όλες οι περιοχές μπορούν να επικοινωνήσουν μεταξύ τους, με κάποιους περιορισμούς φυσικά λόγω του ότι το NAT είναι ενεργοποιημένο σε όλα τα routers που βρίσκονται σε κάθε περιοχή. Στην Εικόνα 2.1. βλέπουμε κάποια παραδείγματα στα οποία έγινε ένα αίτημα τύπου ICMP (Internet Control Message Protocol) από κάποιους κόμβους προς κάποιους άλλους κόμβους.

| | | | | | |
|---|------------|-------------------|------------------|------|---|
| ● | Successful | Sales3 (U.S) | ISP 1 Web Server | ICMP | ● |
| ● | Successful | Management1 (U.S) | ISP 1 Web Server | ICMP | ● |
| ● | Failed | Management1 (U.S) | Sales1 | ICMP | ● |

Εικόνα 2.1. Αιτήματα ICMP.

Αυτό το οποίο μπορούμε να παρατηρήσουμε από την παραπάνω εικόνα είναι πως από την περιοχή που βρίσκονται οι υπολογιστές της εταιρίας που βρίσκεται στην Αμερική, υπάρχει επικοινωνία με τον ISP. Το ίδιο συμβαίνει και με τους υπολογιστές που βρίσκονται στην εταιρία στην Ελλάδα. Το αίτημα όμως χάνεται όταν προσπαθούν να επικοινωνήσουν δύο υπολογιστές όπου ο κάθε ένας βρίσκεται σε διαφορετική εταιρία. Αυτό το αναλύουμε στην ενότητα 3. Ας δούμε πάλι την περιοχή της εικόνας 1.4. Αυτό το οποίο παρατηρούμε είναι πως μέσα σε αυτή την περιοχή δεν υπάρχει μόνο ένας δρομολογητής (όπως στις υπόλοιπες περιοχές) αλλά δύο. Οι δρομολογητές αυτοί έχουν χρησιμοποιηθεί για να ενώσουν διαφορετικά τμήματα της εταιρίας μεταξύ τους. Όπως είναι λογικό η δρομολόγηση σε αυτή την περίπτωση δεν χρειάζεται να είναι δυναμική. Αντίθετα έχει χρησιμοποιηθεί στατική δρομολόγηση για την επικοινωνία των τμημάτων. Η δρομολόγηση που έλαβε χώρα φαίνεται στην εικόνα 2.2.

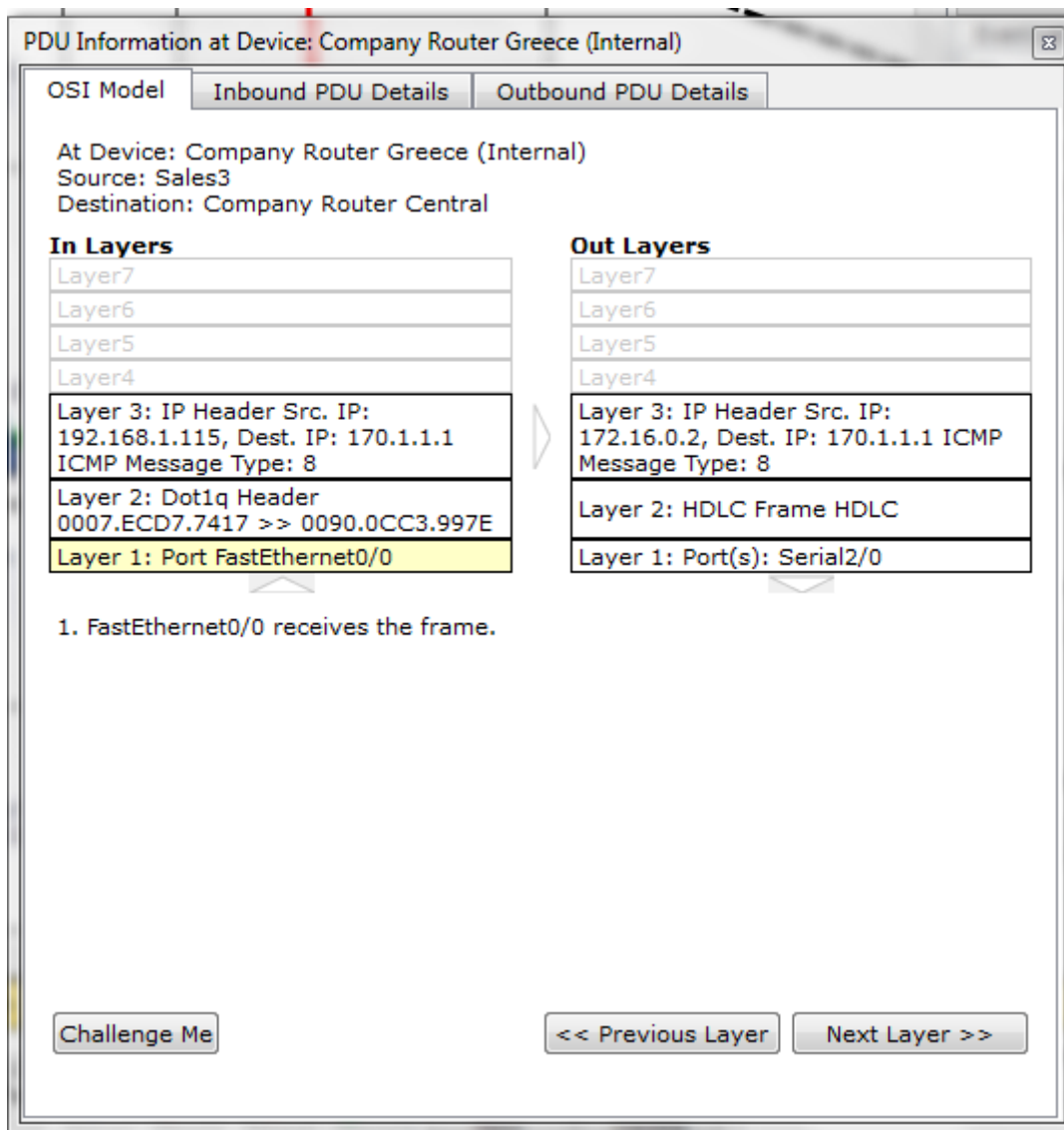
| Network Address |
|-----------------------------|
| 192.168.8.0/23 via 10.0.0.1 |

Εικόνα 2.2. Summary route στο Company Router U.S.

Αυτό που θα μπορούσε κάποιος να παρατηρήσει είναι πως, εφόσον έχουμε δύο υποδίκτυα πως γίνεται στην στατική δρομολόγηση να έχουμε μόνο ένα entry; Αυτό το οποίο έχει γίνει είναι να δημιουργηθεί ένα μόνο entry το οποίο για κάθε πακέτο το οποίο είναι να δρομολογηθεί ελέγχει το prefix της διεύθυνσης προορισμού. Με βάση λοιπόν αυτό, το longest prefix που ταιριάζει στην συγκεκριμένη δρομολόγηση, δρομολογείται και στο σωστό υποδίκτυο.

3. Network Address Translation (NAT)

Όπως είδαμε στην προηγούμενη ενότητα, υπάρχει επικοινωνία μεταξύ των περιοχών αλλά με κάποιους περιορισμούς. Στην εικόνα 2.1. είδαμε πως η άμεση επικοινωνία μεταξύ ενός υπολογιστή από την εταιρία στην Αμερική με έναν υπολογιστή στην εταιρία στην Ελλάδα, δεν είναι εφικτή. Αυτό συμβαίνει γιατί στους δρομολογητές είναι ενεργοποιημένο το NAT. Στην εικόνα 3.1. μπορούμε να δούμε τη σημαίνει αυτό.



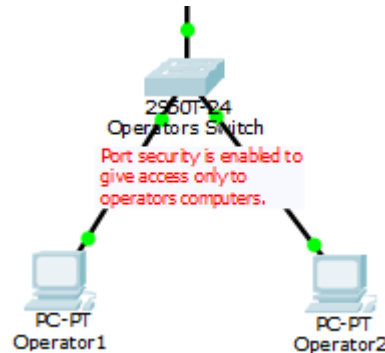
Εικόνα 3.1. Μετάφραση εσωτερικής διεύθυνσης IP σε δημόσια διεύθυνση.

Η παραπάνω εικόνα είναι στιγμιότυπο ενός πακέτου το οποίο προέρχεται από το εσωτερικό δίκτυο της εταιρίας στην Ελλάδα και έχει ως προορισμό έναν ενδιάμεσο κόμβο. Αυτό το οποίο παρατηρούμε είναι πως κατά την άφιξη του πακέτου στον δρομολογητή η διεύθυνση πηγής είναι η εσωτερική διεύθυνση του υπολογιστή που έκανε το αίτημα. Στην έξοδο όμως από τον δρομολογητή βλέπουμε πως η διεύθυνση πηγής αλλάζει και πλέον ως διεύθυνση πηγής ορίζεται η διεύθυνση της διεπαφής εξόδου του δρομολογητή. Με αυτό τον τρόπο καταφέρνουμε να κρατήσουμε την τοπολογία του εσωτερικού δικτύου κρυφή από τον έξω κόσμο καθώς επίσης και να αντιστοιχίσουμε περισσότερες διευθύνσεις IP με μόνο μία δημόσια διεύθυνση.

4. Port Security

Στην τοπολογία που έχει σχεδιαστεί, υπάρχουν δύο υπολογιστές που λειτουργούν ως operators για το router «Company Router Central». Στο συγκεκριμένο δρομολογητή έχουν πρόσβαση μέσω telnet. Η ασφάλεια που έλαβε χώρα βρίσκεται στο Switch που είναι

συνδεδεμένοι οι operators. Συγκεκριμένα στις διεπαφές που είναι συνδεδεμένοι, δεν επιτρέπεται να συνδεθεί καμία άλλη συσκευή εκτός από τις συγκεκριμένες. Στην εικόνα 4.1. βλέπουμε την συνδεσμολογία των συσκευών με το Switch.



Εικόνα 4.1. Το δίκτυο των operators.

Αυτό το οποίο έχει γίνει στις διεπαφές αυτές είναι να ενεργοποιηθεί το port security. Σκοπός του port security είναι να αντιστοιχίσει συγκεκριμένη MAC διεύθυνση με την συγκεκριμένη διεπαφή πάνω στο Switch. Σε περίπτωση που συνδεθεί άλλη συσκευή τότε η διεπαφή αυτή κλείνει και δεν δίνει πρόσβαση στο δίκτυο. Στην εικόνα 4.1. μπορούμε να δούμε της ρυθμίσεις αυτές.

```

Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
      Fa0/1          1          1          0      Shutdown
      Fa0/2          1          1          0      Shutdown
-----

Switch#show po
Switch#show port-security in
Switch#show port-security interface fa
Switch#show port-security interface fastEthernet 0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 00D0.BA5B.ED14:1
Security Violation Count : 0

Switch#show port-security interface fastEthernet 0/2
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 00E0.A327.E382:1
Security Violation Count : 0

```







Εικόνα 4.2. Ενεργοποιημένο port security για τις διεπαφές Fast Ethernet 0/1 και 0/2.

5. Υπηρεσίες

Στην τοπολογία που δημιουργήθηκε έχουν ενεργοποιηθεί κάποιες υπηρεσίες η οποίες είναι προσβάσιμες από όλες τις περιοχές μέσα στην τοπολογία. Οι υπηρεσίες αυτές είναι Web, DNS και E-mail. Μεταξύ των περιοχών μπορούν να σταλούν e-mails καθώς επίσης υπάρχει προσβασιμότητα στον web server και τέλος όλες οι περιοχές χρησιμοποιούν τον ίδιο DNS server.

6. Access Lists

Οι access list που χρησιμοποιήθηκαν στην συγκεκριμένη τοπολογία έχουν δημιουργηθεί με σκοπό την ενεργοποίηση του NAT στους δρομολογητές. Ως ασφάλεια, χρησιμοποιήθηκαν access lists μόνο στο switch του ISP ώστε να περιοριστεί η επικοινωνία του DHCP server μόνο με τους υπολογιστές που βρίσκονται στο τοπικό δίκτυο και να μην επεκταθεί έξω από αυτό. Στην εικόνα 6.1. μπορούμε να δούμε την λειτουργία αυτή.

| Fire | Last Status | Source | Destination | Type | Color |
|---|-------------|--------|---------------------------|------|---|
|  | Successful | Sales3 | ISP 1 Web Server | ICMP |  |
|  | Successful | Sales3 | ISP 1 Server DNS - E-MAIL | ICMP |  |
|  | Failed | Sales3 | DHCP Internal Server | ICMP |  |

Εικόνα 6.1. Παρεμπόδιση επικοινωνίας από το εξωτερικό δίκτυο με τον DHCP server.

Αυτό το οποίο μπορούμε να δούμε από την παραπάνω εικόνα είναι πως ο υπολογιστής που βρίσκεται στην εταιρία στην Ελλάδα έχει επικοινωνία με τον web server καθώς επίσης και με τον DNS server που βρίσκονται στον ISP, αλλά εμποδίζεται η επικοινωνία του με τον DHCP server του ISP. Για την επίτευξη αυτή χρησιμοποιήθηκε μια extended access list στον δρομολογητή του ISP η οποία εμποδίζει την κίνηση από οποιοδήποτε δίκτυο προς τον συγκεκριμένο server.