

**Ανοικτά Ακαδημαϊκά Μαθήματα**

**Τεχνολογικό Εκπαιδευτικό Ίδρυμα Αθήνας**

Δίκτυα Η/Υ ΙΙ (E)

**Εργαστηριακή άσκηση 8: Υπηρεσία ΝΑΤ**

Παραμετροποίηση της υπηρεσίας NAT – Network Address Translation, σε δρομολογητή του διαδικτύου μας

Ιφιγένεια Φουντά

Τμήμα Μηχανικών Πληροφορικής Τ.Ε.

|  |  |
| --- | --- |
| Το περιεχόμενο του μαθήματος διατίθεται με άδεια Creative Commons εκτός και αν αναφέρεται διαφορετικά | Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους. |

|  |  |
| --- | --- |
| **Εργαστηριακή άσκηση** | **Υπηρεσία ΝΑΤ**Παραμετροποίηση της υπηρεσίας NAT – Network Address Translation, σε δρομολογητή του διαδικτύουΖητείται να υλοποιηθεί και να διαμορφωθεί κατάλληλα το εικονιζόμενο διαδίκτυο ώστε τα PCs του διαδικτύου να μπορούν να αξιοποιούν όλες τις παρεχόμενες υπηρεσίες του διαδικτύου. O δρομολογητής router1 παρέχει στα PCs των LAN0 & LAN1 τις υπηρεσίες DHCP & ΝΑΤ.Για την υλοποίηση του διαδικτύου θα ληφθούν υπόψιν όλα τα στοιχεία που ορίζονται στο σχήμα καθώς και αυτά που περιγράφονται στο σενάριο της εργαστηριακής άσκησης. |
| **Στόχοι άσκησης** | 1. η εξοικείωση με τη διαμόρφωση δύο βασικών τύπων (Ν-1 & 1-1) της υπηρεσίας **Μετάφρασης Δικτυακών Διευθύνσεων** – **ΝΑΤ** σε δρομολογητή που χρησιμοποιείται ως πύλη (gateway) προς το διαδίκτυο και
2. η κατανόηση της υπηρεσίας ως σημαντικού εργαλείου για:
* την εξοικονόμηση πραγματικών (global) IP διευθύνσεων μέσω της χρήσης ιδιωτικών (private) διευθύνσεων (Ν-1)
* την παροχή επιπέδου ασφάλειας σε υπολογιστές με ιδιωτικές IP διευθύνσεις, που προσπελαύνουν το διαδίκτυο (Ν-1).
* την απόδοση πραγματικής IP διεύθυνσης σε εξυπηρετητή που βρίσκεται σε τοπικό δίκτυο με ιδιωτικές IP διευθύνσεις (1-1).
 |



**Σενάριο εργαστηριακής άσκησης:**

1. Το διαδίκτυο θα υλοποιηθεί με τη βοήθεια του Packet tracer
2. Στο Interface του δρομολογητή router0 με το Lan0 αποδίδουμε στατικά την IP 192.168.10.1/24, ενώ στο Interface του δρομολογητή router0 με το Lan1 αποδίδουμε στατικά την IP 10.10.10.1/24
3. Στον εξυπηρετητή server0 αποδίδουμε στατικά την IP 192.168.10.2/24, domain name **server0,** ψευδώνυμο **inside\_web,** ενώ ενεργοποιούμε τις υπηρεσίες Web & DNS.
4. Στον εξυπηρετητή server2 αποδίδουμε στατικά την IP 195.130.10.2/24, domain name **server2,** ψευδώνυμο **outside\_web,** ενώ ενεργοποιούμε τις υπηρεσίες Web & DNS.
5. Το δίκτυο διασύνδεσης μεταξύ των δύο δρομολογητών router1 & router2 έχει IP 195.1.2.0 /29
6. Στον δρομολογητή router0 θα διαμορφώσουμε:

α. την υπηρεσία Δυναμικής Διευθυνσιοδότησης **DHCP** για να παρέχει στοιχεία διευθέτησης στα PCs των Lan0 & Lan1.

β. την υπηρεσία Μετάφρασης Δικτυακών Διευθύνσεων τύπου «πολλά προς ένα» - **ΝΑΤ Ν-1,** για να μπορούν τα PCs των Lan0 & Lan1 να βγαίνουν στο Internet με μία πραγματική (global) IP διεύθυνση.

γ. την υπηρεσία Μετάφρασης Δικτυακών Διευθύνσεων τύπου «ένα προς ένα» - **ΝΑΤ 1-1,** για να μπορεί ο **serve0** να φαίνεται από τον έξω κόσμο (outside) μετην πραγματική (global) IP διεύθυνση 195.1.2.3.

1. Θα πρέπει να διαμορφώσουμε κατάλληλα το διαδίκτυο σύμφωνα με τα παραπάνω δεδομένα ώστε:
	1. Να υπάρχει επικοινωνία μεταξύ των δικτυακών συσκευών του διαδικτύου
	2. Οι χρήστες των PCs να έχουν πρόσβαση στο Internet και να μπορούν να αξιοποιούν όλες τις παρεχόμενες υπηρεσίες του διαδικτύου.

**Υλοποίηση εργασίας**

**Για την υλοποίηση της άσκησης προτείνεται ο παρακάτω βηματισμός:**

1. **Υλοποίηση του διαδικτύου (L3)**

Υλοποιούμε το διαδίκτυο και αποδίδουμε τις IP στατικές διευθύνσεις, σύμφωνα με το σενάριο της άσκησης.

1. **Υλοποίηση της δικτυακής Υπηρεσίας DHCP**

**Βήμα 1o – Υλοποίηση DHCP υπηρεσίας στον δρομολογητή**

Παραμετροποιούμε τον δρομολογητή router1 ώστε να παρέχει την υπηρεσία της δυναμικής διευθυνσιοδότησης στα PCs των τοπικών δικτύων Lan0 & Lan1. Ο δρομολογητής θα ρυθμιστεί για απόδοση: IP διευθύνσεων & μάσκας υποδικτύου, προεπιλεγμένου δρομολογητή (default gateway), DNS διακομιστή**. Οι dhcp δεξαμενές θα ονομαστούν αντίστοιχα poolLan0 & poolLan1.**

**Βήμα 2o – ενεργοποίηση του DHCP client στα** PCs των τοπικών δικτύων Lan0 & Lan1

**Βήμα 3ο – έλεγχος της ορθής λειτουργίας της υπηρεσίας DHCP**

Ελέγχουμε τον πίνακα **DHCP** με την εντολή **show ip dhcp binding**, καθώς και τα δικτυακά στοιχεία των PCs ( **ipconfig /all)**.

1. **Υλοποίηση στατικής δρομολόγησης**

Εφαρμόζουμε στατική δρομολόγηση με στόχο την επικοινωνία μεταξύ όλων των συσκευών του διαδικτύου.

1. **Υλοποίηση & έλεγχος της υπηρεσίας ΝΑΤ «Ν-1» στον δρομολογητή**

Στον δρομολογητή Router1, ρυθμίζουμε την υπηρεσία ΝΑΤ «Ν-1», ως εξής:

**Βήμα 1ο – Δημιουργούμε τη λίστα των ΙΡ διευθύνσεων που θέλουμε να «μεταφραστούν» σε κάθε τοπικό δίκτυο με την εντολή**:

**access-list <αριθμός λίστας> permit ip <ip δικτύου> <wildcard bits δικτύου> any**

Η παραπάνω εντολή είναι τύπου **λίστας ελέγχου πρόσβασης** (A**ccess Control List**), η οποία γενικά χρησιμοποιείται κυρίως για ασφάλεια υπηρεσιών και δικτύου, ελέγχει την πρόσβαση από/προς συγκεκριμένα μηχανήματα, δίκτυα, υπηρεσίες.

Στην παράμετρο **<αριθμός λίστας>” μπορούμε να βάλουμε οποιοδήποτε αριθμό από 100-199** ( πρόκειται για extended ACL), ενώ μετά την IP **του private subnet** που πρόκειται να μεταφράσουμε ακολουθούν αντί της subnet mask, τα “wildcard bits”. Τα wildcard bits ουσιαστικά είναι το συμπλήρωμα ως προς 255 της μάσκας υποδικτύου και χρησιμοποιούνται από τη cisco για την ευκολότερη και συντομότερη επίτευξη μαθηματικών υπολογισμών από τους δρομολογητές. Έτσι για παράδειγμα αντί της μάσκας 255.255.255.0 θέτουμε τα wildcard bits **0.0.0.255 και αντί της μάσκας 255.255.255.240 τα** wildcard bits **0.0.0.15**

* **access-list 100 permit ip 192.168.1.0 0.0.0.255 any (Lan0)**
* **access-list 101 permit ip 10.10.10.0 0.0.0.255 any (Lan1)**

**Βήμα 2ο – Για τις λίστες που δημιουργήσαμε, ορίζουμε την ΙΡ διεύθυνση πάνω από την οποία θα γίνει η «μετάφραση»:**

 **ip nat inside source list <αριθμός λίστας> interface <όνομα WAN interface>  ~~ή “global ip του WAN interface“~~**

* **ip nat inside source list 100 interface s2/0** **(Lan0)**

ή  ~~ip nat inside source list 100 195.1.2.1~~

* **ip nat inside source list 101 interface s2/0** **(Lan1)**

ή  ~~ip nat inside source list 101 195.1.2.1~~

**Βήμα 3ο –** Στα interfaces που εμπλέκονται στην υπηρεσία ΝΑΤ, από interface global configuration mode, εφαρμόζουμε την εντολή **ip nat**, με την παράμετρο **inside** εάν πρόκειται για εσωτερικό interface και **outside** εάν πρόκειται για εξωτερικό interface.

* **Router0(config)#interface Fa0/0**

**Router0 (config-if)#ip nat inside**

* **Router0(config)#interface Fa1/0**

**Router0 (config-if)#ip nat inside**

* **Router0 (config)#interface S2/0**

**Router0 (config-if)#ip nat outside**

Οι εντολές των τριών παραπάνω βημάτων επιτρέπουν στις δικτυακές συσκευές των LAN0 & LAN1 να στέλνουν ip πακέτα προς **οποιονδήποτε** προορισμό (λεκτικό any) στο Internet, με μεταφρασμένες τις **source ip private διευθύνσεις** τους στην **source ip global διεύθυνση** του interface s2/0.

*!!!! Επομένως, τ****α δίκτυα LAN0 & LAN1 (που βρίσκονται inside) δεν είναι πλέον ορατά από το Internet. Έχουν κρυφτεί πίσω από την global IP διεύθυνση του εξωτερικού interface s2/0.***

* ***Οι υπολογιστές των LAN0 & LAN1 δεν κινδυνεύουν από κακόβουλους εξωτερικούς χρήστες, διότι δεν μπορούν να τους εντοπίσουν ως μοναδικές διαδικτυακές οντότητες***
* ***η στατική δρομολόγηση στον router2, για τα δίκτυα LAN0 & LAN1 είναι ΠΕΡΙΤΤΗ.***

**Βήμα 4ο – Έλεγχος λειτουργίας υπηρεσίας NAT Ν-1**

Για να μπορέσουμε να ελέγξουμε τη λειτουργία της υπηρεσίας ΝΑΤ Ν-1, πρέπει να δημιουργήσουμε δικτυακή κίνηση από μέσα ( inside) προς τα έξω (outside). Για παράδειγμα από το PC0 εκτελούμε **ping 195.130.10.1**.

Στη συνέχεια, εκτελούμε την εντολή **show ip nat translations,** η οποία μας εμφανίζει τη λίστα με τις τρέχουσες «ΙΡ μεταφράσεις», για την κίνηση δεδομένων που πραγματοποιείται τη δεδομένη χρονική στιγμή.

1. **Υλοποίηση & έλεγχος της υπηρεσίας ΝΑΤ 1-1 στον δρομολογητή**

Στον δρομολογητή router0 ρυθμίζουμε την υπηρεσία ΝΑΤ 1-1, ως εξής:

**Βήμα 1ο –** Ορίζουμε την global ΙΡ διεύθυνση πάνω από την οποία θα γίνει η «μετάφραση» της private Ip διεύθυνσης τουserver0 του Lan0:

* ip nat inside source static 192.168.10.2 195.1.2.3

**Βήμα 2ο –** Στα εμπλεκόμενα interfaces, από interface configuration mode, εφαρμόζουμε την εντολή **ip nat**, με την παράμετρο **inside** εάν πρόκειται για το εσωτερικό interface και **outside** εάν πρόκειται για εξωτερικό interface.

* Router1(config)#interface Fa0/1

Router1 (config-if)#ip nat inside

* Router1 (config)#interface S0/0

Router1 (config-if)#ip nat outside

**Βήμα 3ο – Έλεγχος λειτουργίας της υπηρεσίας NAT Ν-1**

Εκτελούμε εκ νέου την εντολή **show ip nat translations**

1. **Διαμόρφωση της υπηρεσίας WEB στους εξυπηρετητές:**

Στον Packet tracer συνήθως η υπηρεσία WEB είναι ενεργοποιημένη σε κάθε εξυπηρετητή (πρωτόκολλα HTTP & HTTPS on), ενώ υπάρχει HTML sample αρχείο.

1. **Διαμόρφωση της υπηρεσίας DNS στους εξυπηρετητές**

Με τη βοήθεια του Packet tracer ενεργοποιούμε την υπηρεσία DNS στους Server0 & Server2 και προσθέτουμε στη βάση κάθε ενός αντίστοιχα τις απαραίτητες εγγραφές ώστε να υποστηριχτούν οι απαιτήσεις του σεναρίου μας.

1. **Έλεγχος της λειτουργικότητας του δικτύου & των υπηρεσιών**

Ελέγχουμε τη λειτουργικότητα του δικτύου και των υπηρεσιών εκτελώντας κατ’ελάχιστον τις παρακάτω διαδικασίες δοκιμών (test):

1. **από το PC0:** Ping server0, Ping server21 (μέσω command line), πρόσβαση στα html έγγραφα των Web servers (μέσω web browser)
2. **από τον server2:** ping server0(μέσω command line), πρόσβαση στην ιστοσελίδα του server0 (μέσω web browser)
3. **Ζητείται να απαντήσουμε στα παρακάτω ερωτήματα:**
4. Όταν γίνεται αποστολή ενός πακέτου από το PC0 στο PC2 αξιοποιείται η υπηρεσία ΝΑΤ; Ναι ή όχι; Εξηγήστε
5. Αναφέρατε τις εγγραφές που καταχωρήσατε σε κάθε έναν DNS server (server0 & server1) και εξηγήστε τη χρήση κάθε μιας
6. Αναφέρατε τουλάχιστον δύο τρόπους πρόσβασης από τον server2 στην ιστοσελίδα του server0
7. Μπορούμε από τον server2 να προσπελάσουμε το PC0; Αν ναι με ποιο τρόπο, αν όχι εξηγήστε το λόγο.
8. Ποια πληροφορία μας δίνει η εντολή **show ip nat translations**; Κατά τη διάρκεια ποιάς διαδικασίας πληθυσμώνεται ο αντίστοιχοςς πίνακας και από ποια οντότητα; Αντιγράψτε το περιεχόμενο του πίνακα ΝΑΤ και εξηγήστε ποιες δοκιμασίες δημιούργησαν το συγκεκριμένο περιεχόμενο.
9. Ποια πληροφορίαμας δίνει ηεντολή **show ip dhcp binding** Αντιγράψτε το περιεχόμενο του πίνακα και σχολιάστε τις εγγραφές
10. Σχολιάστε το περιεχόμενο του πίνακα ΝΑΤ:

**Router1#sh ip nat translations**

**Pro Inside global Inside local Outside local Outside global**

**icmp 195.1.2.1:1 10.10.10.2:1 195.130.10.2:1 195.130.10.2:1**

**icmp 195.1.2.1:2 10.10.10.2:2 195.130.10.2:2 195.130.10.2:2**

**icmp 195.1.2.1:3 10.10.10.2:3 195.130.10.2:3 195.130.10.2:3**

**icmp 195.1.2.1:4 10.10.10.2:4 195.130.10.2:4 195.130.10.2:4**

**--- 195.1.2.3 192.168.10.2 --- ---**

**Χρήσιμες εντολές για την υλοποίηση των υπηρεσιών DHCP & NAT**

**Υπηρεσία DHCP**

**Router(config)#** ip dhcp pool <όνομα pool>

**Router(config - dhcp)#** network <ΙΡ υποδικτύου> <μάσκα υποδικτύου>

**Router(config - dhcp)#** dns-server <ΙΡ διακομιστή DNS>

**Router(config - dhcp)#** default-router <ΙΡ δρομολογητή πύλης>

**~~Router(config - dhcp)# domain-name <όνομα>~~**

**~~Router(config - dhcp)# lease <μέρες> <ώρες> <λεπτά>~~**

**Router(config)# ip dhcp excluded-address <αρχική IP διεύθυνση> <τελική IP διεύθυνση>**

**Υπηρεσία NAT Ν-1**

**Router(config)#** access-list <αριθμός ACL> permit ip <υποδίκτυο> <wild card> any

**Router(config)#** ip nat inside source list <αριθμός ACL> interface <όνομα WAN interface> overload

**Router(config-if)#** ip nat inside

**Router(config-if)#** ip nat outside

**Υπηρεσία NAT 1-1**

**Router(config)#** ip nat inside source static <IP inside local> <IP inside global>

|  |
| --- |
| **Ανοικτά Ακαδημαϊκά Μαθήματα****Τεχνολογικό Εκπαιδευτικό Ίδρυμα Αθήνας** |
| **Τέλος Ενότητας** |
| **Χρηματοδότηση*** Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
* Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Αθήνας**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
* Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

 |

**Σημειώματα**

**Σημείωμα Αναφοράς**

Copyright ΤΕΙ Αθήνας, Ιφιγένεια Φουντά, 2014. Ιφιγένεια Φουντά. «Δίκτυα Η/Υ ΙΙ (E). Εργαστηριακή άσκηση 8: Υπηρεσία ΝΑΤ». Έκδοση: 1.0. Αθήνα 2014. Διαθέσιμο από τη δικτυακή διεύθυνση: [ocp.teiath.gr](https://ocp.teiath.gr/).

**Σημείωμα Αδειοδότησης**

Το παρόν υλικό διατίθεται με τους όρους της άδειας χρήσης Creative Commons Αναφορά, Μη Εμπορική Χρήση Παρόμοια Διανομή 4.0 [1] ή μεταγενέστερη, Διεθνής Έκδοση. Εξαιρούνται τα αυτοτελή έργα τρίτων π.χ. φωτογραφίες, διαγράμματα κ.λ.π., τα οποία εμπεριέχονται σε αυτό. Οι όροι χρήσης των έργων τρίτων επεξηγούνται στη διαφάνεια «Επεξήγηση όρων χρήσης έργων τρίτων».

Τα έργα για τα οποία έχει ζητηθεί άδεια αναφέρονται στο «Σημείωμα Χρήσης Έργων Τρίτων».



[1] http://creativecommons.org/licenses/by-nc-sa/4.0/

Ως **Μη Εμπορική** ορίζεται η χρήση:

* που δεν περιλαμβάνει άμεσο ή έμμεσο οικονομικό όφελος από την χρήση του έργου, για το διανομέα του έργου και αδειοδόχο
* που δεν περιλαμβάνει οικονομική συναλλαγή ως προϋπόθεση για τη χρήση ή πρόσβαση στο έργο
* που δεν προσπορίζει στο διανομέα του έργου και αδειοδόχο έμμεσο οικονομικό όφελος (π.χ. διαφημίσεις) από την προβολή του έργου σε διαδικτυακό τόπο

Ο δικαιούχος μπορεί να παρέχει στον αδειοδόχο ξεχωριστή άδεια να χρησιμοποιεί το έργο για εμπορική χρήση, εφόσον αυτό του ζητηθεί.

**Επεξήγηση όρων χρήσης έργων τρίτων**

|  |  |
| --- | --- |
| © | Δεν επιτρέπεται η επαναχρησιμοποίηση του έργου, παρά μόνο εάν ζητηθεί εκ νέου άδεια από το δημιουργό. |
| διαθέσιμο με άδεια CC-BY | Επιτρέπεται η επαναχρησιμοποίηση του έργου και η δημιουργία παραγώγων αυτού με απλή αναφορά του δημιουργού. |
| διαθέσιμο με άδεια CC-BY-SA | Επιτρέπεται η επαναχρησιμοποίηση του έργου με αναφορά του δημιουργού, και διάθεση του έργου ή του παράγωγου αυτού με την ίδια άδεια. |
| διαθέσιμο με άδεια CC-BY-ND | Επιτρέπεται η επαναχρησιμοποίηση του έργου με αναφορά του δημιουργού. Δεν επιτρέπεται η δημιουργία παραγώγων του έργου. |
| διαθέσιμο με άδεια CC-BY-NC | Επιτρέπεται η επαναχρησιμοποίηση του έργου με αναφορά του δημιουργού. Δεν επιτρέπεται η εμπορική χρήση του έργου. |
| διαθέσιμο με άδεια CC-BY-NC-SA | Επιτρέπεται η επαναχρησιμοποίηση του έργου με αναφορά του δημιουργού και διάθεση του έργου ή του παράγωγου αυτού με την ίδια άδεια. Δεν επιτρέπεται η εμπορική χρήση του έργου. |
| διαθέσιμο με άδεια CC-BY-NC-ND | Επιτρέπεται η επαναχρησιμοποίηση του έργου με αναφορά του δημιουργού. Δεν επιτρέπεται η εμπορική χρήση του έργου και η δημιουργία παραγώγων του. |
| διαθέσιμο με άδεια CC0 Public Domain | Επιτρέπεται η επαναχρησιμοποίηση του έργου, η δημιουργία παραγώγων αυτού και η εμπορική του χρήση, χωρίς αναφορά του δημιουργού. |
| διαθέσιμο ως κοινό κτήμα | Επιτρέπεται η επαναχρησιμοποίηση του έργου, η δημιουργία παραγώγων αυτού και η εμπορική του χρήση, χωρίς αναφορά του δημιουργού. |
| χωρίς σήμανση | Συνήθως δεν επιτρέπεται η επαναχρησιμοποίηση του έργου. |

**Διατήρηση Σημειωμάτων**

* Οποιαδήποτε αναπαραγωγή ή διασκευή του υλικού θα πρέπει να συμπεριλαμβάνει:
* Το Σημείωμα Αναφοράς
* Το Σημείωμα Αδειοδότησης
* Τη δήλωση Διατήρησης Σημειωμάτων
* Το Σημείωμα Χρήσης Έργων Τρίτων (εφόσον υπάρχει) μαζί με τους συνοδευόμενους υπερσυνδέσμους.