

# Routing and Remote Access Service / Virtual Private Network (RRAS/VPN)

## ΕΙΣΑΓΩΓΗ

**α.** Στη σημερινή εποχή όπου όλες οι επιχειρήσεις και οι οργανισμοί χρησιμοποιούν δίκτυα Η/Υ, σχεδόν όλοι οι υπάλληλοί τους είναι χρήστες της Λογικής Περιοχής (domain) του δικτύου της επιχείρησης/οργανισμού. Οι χρήστες αυτοί έχουν πρόσβαση στους κοινόχρηστους πόρους αυτών των δικτύων. Αυτό όμως ισχύει για τους χρήστες που εργάζονται μέσα στο κτήριο της έδρας της επιχείρησης/οργανισμού. Τι γίνεται όμως με τους υπαλλήλους που εργάζονται μακριά από την έδρα της επιχείρησης/οργανισμού, όπως είναι οι πωλητές ή οι τεχνικοί; Τι γίνεται με τους υπαλλήλους που εργάζονται από το σπίτι (teleworking);

**β.** Αρκετές επιχειρήσεις και οργανισμοί έχουν την έδρα τους, και το κεντρικό κτήριο των γραφείων τους, μέσα στον πολεοδομικό ιστό μιας πόλης. Ομως τις εγκαταστάσεις παραγωγής τους και τις αποθήκες τους τις έχουν σε Βιομηχανικές Περιοχές εκτός των πόλεων. Πως μπορούν τα δίκτυα Η/Υ των κεντρικών γραφείων, της εγκατάστασης παραγωγής και της αποθήκης να ανήκουν στην ίδια Λογική Περιοχή (domain) του δικτύου της επιχείρησης/οργανισμού;

**γ.** Δύο επιχειρήσεις/οργανισμοί που έχουν δίκτυα Η/Υ με διαφορετικές Λογικές Περιοχές (domains) θέλουν για συγκεκριμένους λόγους να διασυνδέσουν τα δίκτυά τους. Πως θα γίνει αυτό;

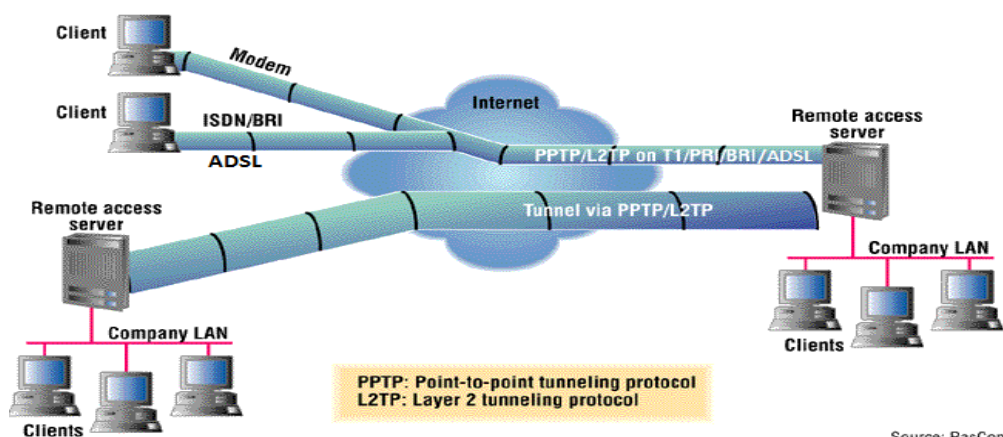
Στην **α.** περίπτωση χρειαζόμαστε μια υπηρεσία τύπου: Remote Access.

Η **β.** περίπτωση είναι ένα intranet και χρειάζεται μια υπηρεσία τύπου Routing.

Η **γ.** περίπτωση είναι ένα extranet και χρειάζεται μια υπηρεσία τύπου Routing.

Για να υλοποιηθούν τα παραπάνω χρειάζεται το internet και η δημιουργία Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks) με τη χρήση “σηράγγων (tunnels)” μέσα από αυτό. Θεωρώντας ότι το λειτουργικό σύστημα των προαναφερθέντων δικτύων είναι τα Windows, θα πρέπει οι servers αυτών των δικτύων να υποστηρίζουν την υπηρεσία Routing and Remote Access.

Στο παρακάτω Σχήμα 1 φαίνεται παραστατικά ένα Εικονικό Ιδιωτικό Δίκτυο. Ως clients ορίζονται οι απομεμακρυσμένοι χρήστες. Τα “tunnels” δημιουργούνται με τη χρήση των PPTP και L2TP ( πρωτόκολλα του 2ου επιπέδου κατά OSI αρχιτεκτονικής και του Link layer του 1ου επιπέδου κατά TCP/IP αρχιτεκτονικής).



Σχήμα 1. Virtual Private Network.

Στο παρελθόν οι φυσικές γραμμές επικοινωνίας για να υλοποιηθούν τα VPN των intranet και extranet ήταν οι μισθωμένες εξωκείμενες γραμμές (leased lines) ενώ οι αντίστοιχες γραμμές για τους απομακρυσμένους χρήστες ήταν συνήθως οι απλές τηλεφωνικές γραμμές με τη χρήση modems. Με την εξέλιξη της τεχνολογίας οι φυσικές γραμμές επικοινωνίας και για τις δύο χρήσεις έγιναν ISDN (PRI και BRI). Τώρα πλέον αυτές οι γραμμές επικοινωνίας είναι τύπου ADSL. Ακόμη και τώρα σε περίπτωση VPN για intranet όπου διακινείται μεγάλος όγκος δεδομένων χρησιμοποιούνται οι μισθωμένες εξωκείμενες γραμμές. (Τυπικώς όταν χρησιμοποιούνται οι μισθωμένες εξωκείμενες γραμμές δεν χρειάζεται η υλοποίηση VPN. Στη πράξη όμως εφαρμόζεται για την ασφάλεια των διακινούμενων πληροφοριών, καθώς αυτές οι γραμμές διέρχονται από μέρη που δεν ελέγχει η κάθε επιχείρηση ή οργανισμός.)

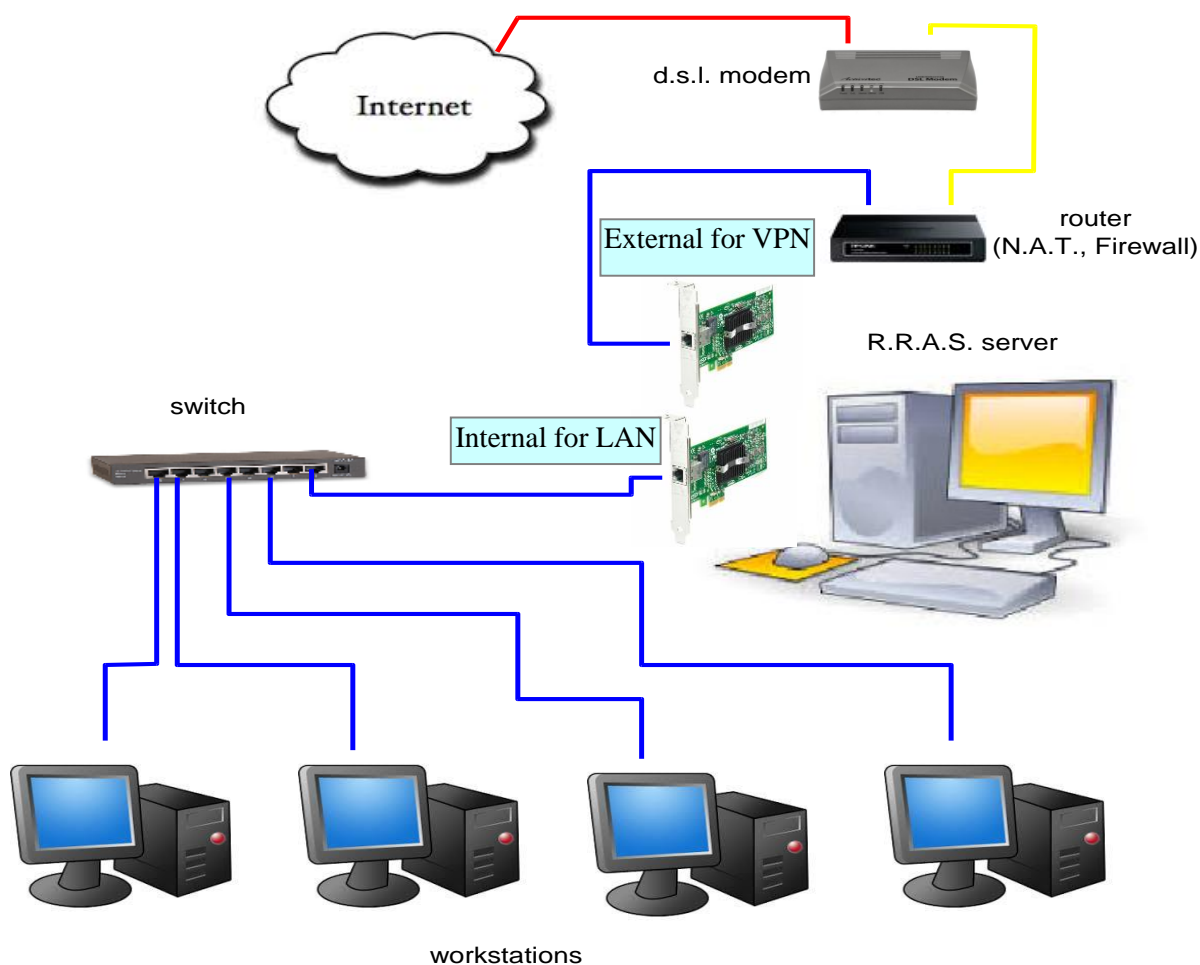
## ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΕΡΓΑΣΤΗΡΙΑΚΟΥ ΔΙΚΤΥΟΥ VPN

### A. Εγκατάσταση ρόλου RRAS σε server του δικτύου

Η εγκατάσταση του ρόλου RRAS θα γίνει σε server με λειτουργικό σύστημα Windows 2008.

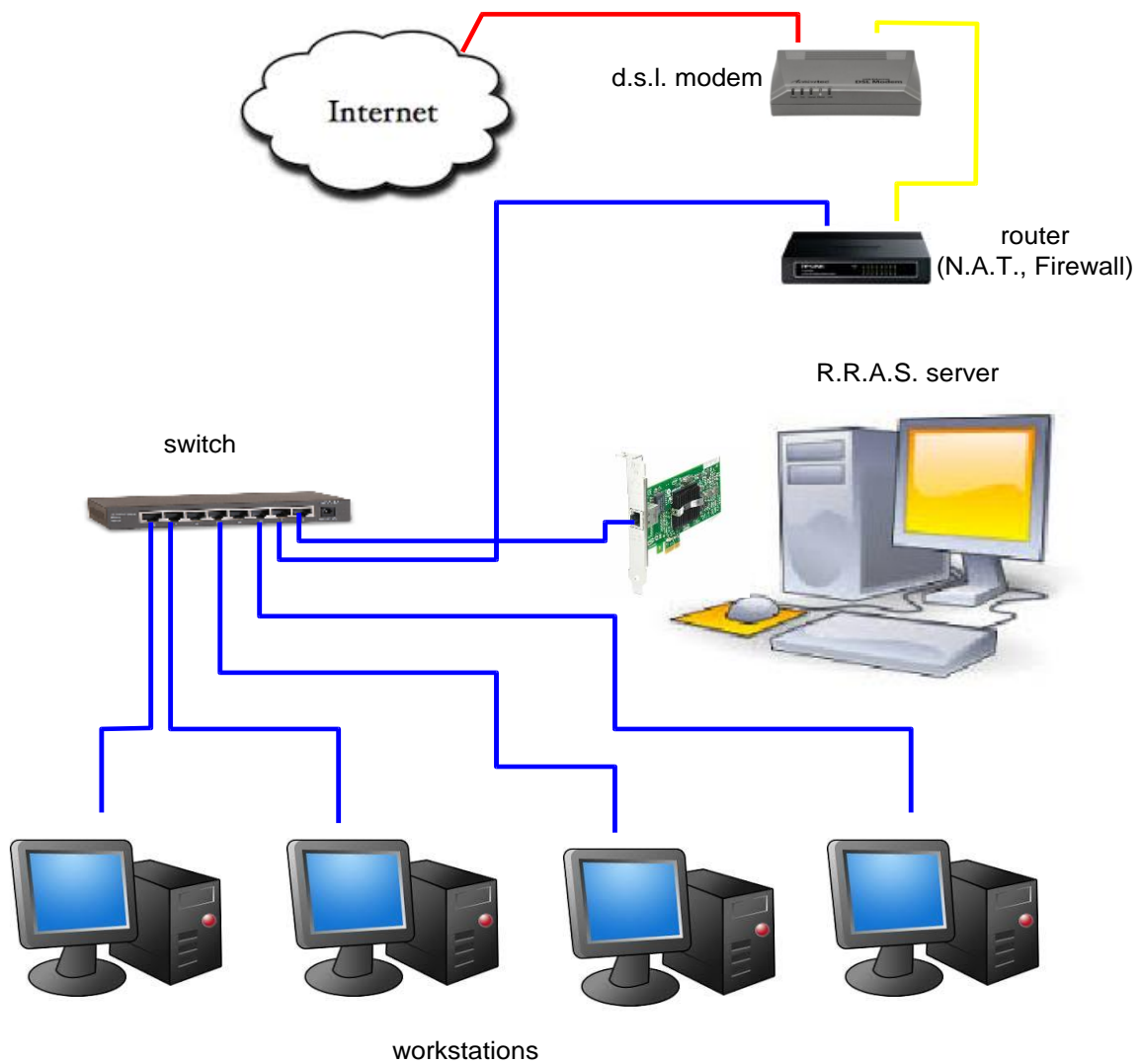
Η Microsoft προτείνει να μην εγκαθίστανται ο ρόλος RRAS σε server που είναι Domain Controller. Όμως καθώς εμείς δεν έχουμε τη δυνατότητα να διαθέσουμε και άλλο server θα χρησιμοποιήσουμε αυτόν που είναι DC.

Επίσης ο ρόλος RRAS πρέπει να παρέχεται από server που διαθέτει δύο κάρτες δικτύου (Network Interface Card). Η μία NIC συνδέεται στον router (WAN πλευρά) και η άλλη NIC στο switch (LAN πλευρά) (Σχήμα 2).



Σχήμα 2. VPN με δύο NIC

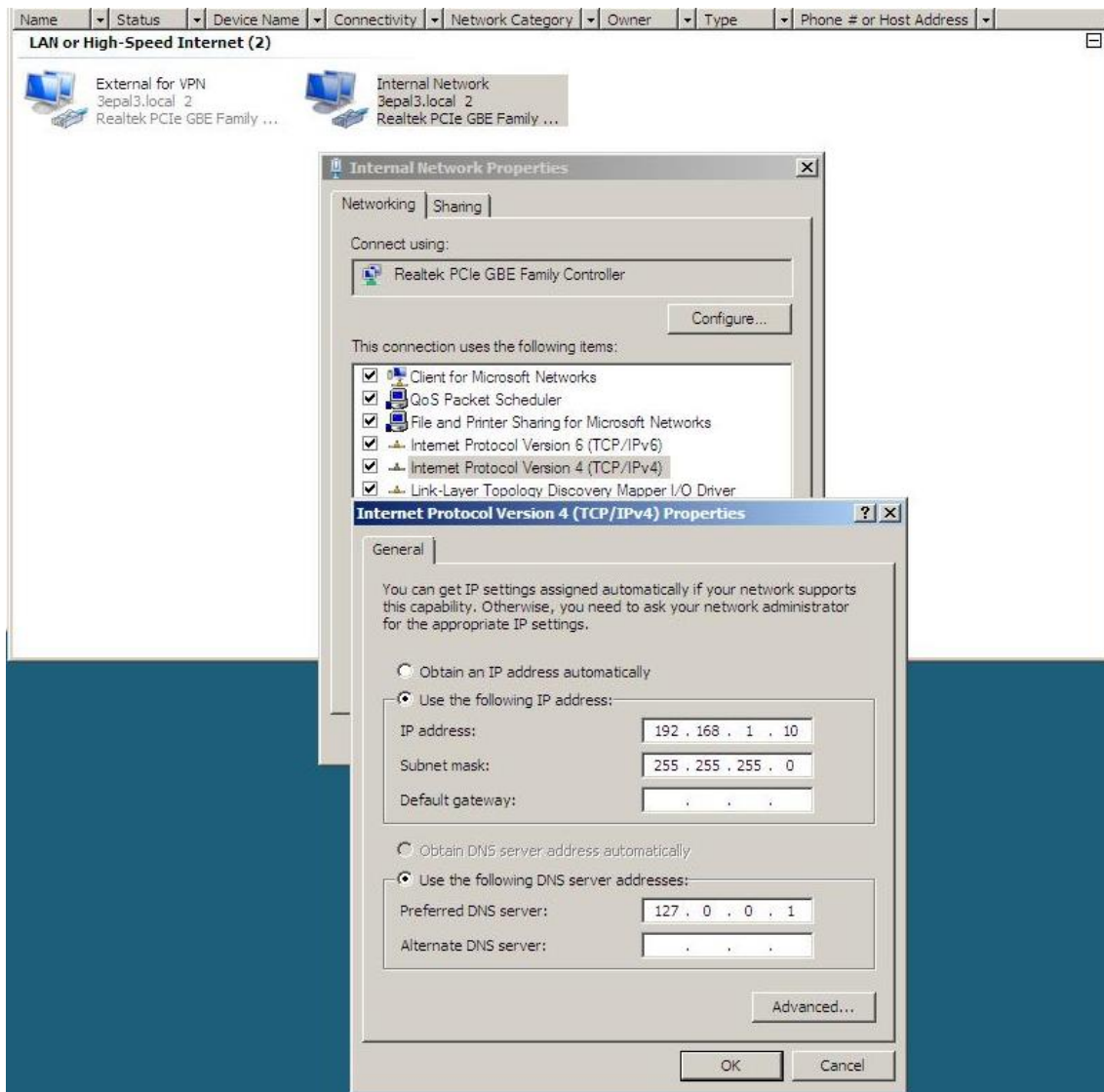
Ο ρόλος RRAS είναι δυνατόν να εγκατασταθεί και σε server που έχει μόνο μια NIC (Σχήμα 3) αν και δεν συνιστάται.



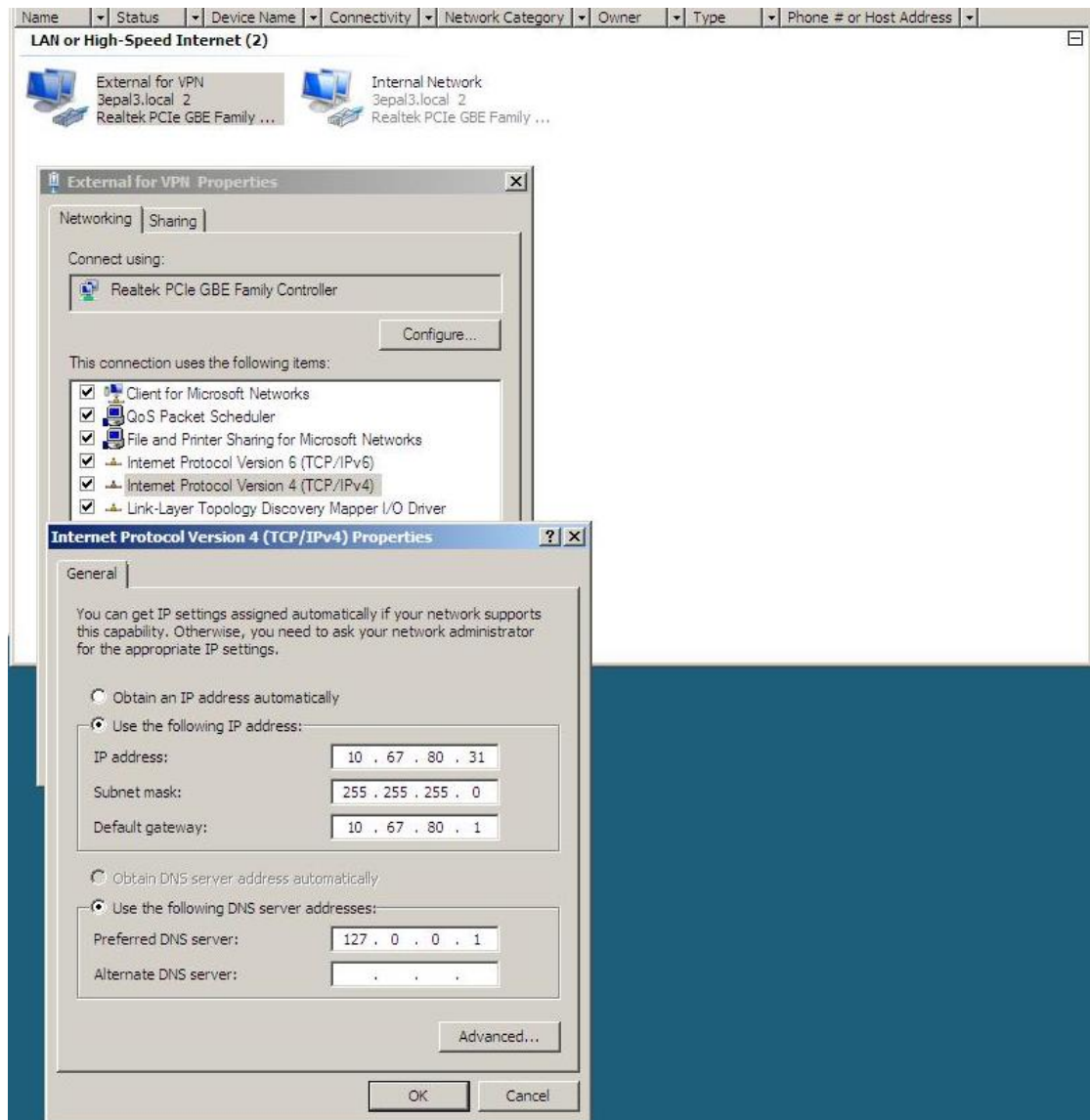
**Σχήμα 3. VPN με μία NIC**

Υλοποιούμε την συνδεσμολογία του Σχήματος 2. Και οι δύο NIC διαθέτουν στατικές IP διευθύνσεις. Στην “Internal for LAN” αποδίδουμε την: 192.168.1.10 και στην “External for VPN” αποδίδουμε την 10.67.80.31 (βλέπε Εικόνες 1 & 2). Στην “Internal for LAN” επιβάλλεται από την Microsoft να μην ορίζεται Default Gateway. Η IP διεύθυνση 127.0.0.1 του πεδίου: Preferred DNS Server είναι η loopback διεύθυνση, δηλώνοντας την διεύθυνση αυτού του ίδιου του Η/Υ δηλαδή την:192.168.1.10 ή 10.67.80.31 αντίστοιχα.

Η “Internal for LAN” NIC έπρεπε να είναι εγκατεστημένη πριν την εγκατάσταση του Active Directory σ’ αυτόν τον Server.

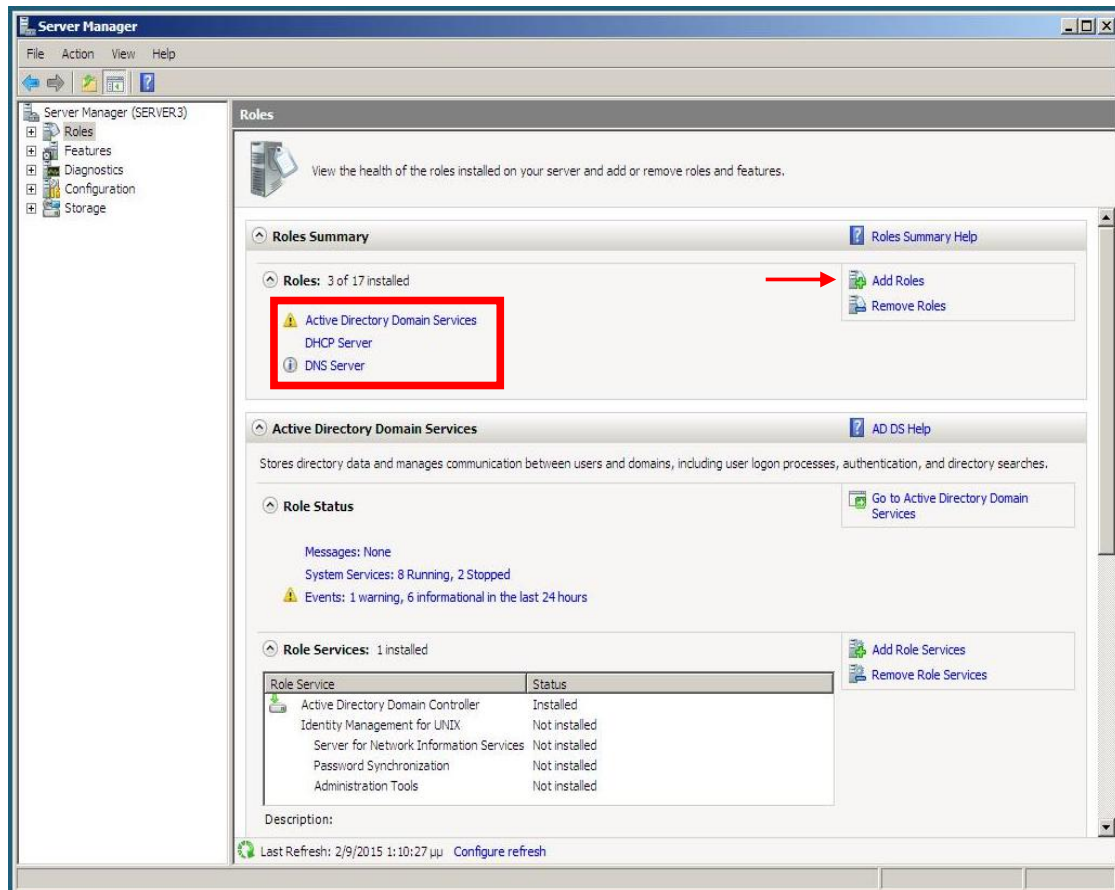


**Εικόνα 1. Δικτυακές Παράμετροι της “Internal for LAN” NIC.**



**Εικόνα 2. Δικτυακές Παράμετροι της “External for VPN” NIC.**

1. Επιλέγουμε: **Start** → **Server Manager** και στο παράθυρο που ανοίγει επιλέγουμε: **Roles**.



**Εικόνα 3. Εγκατεστημένοι ρόλοι στον Server.**

Στην Εικόνα 3 παρατηρούμε ότι έχουν εγκατασταθεί οι ρόλοι:

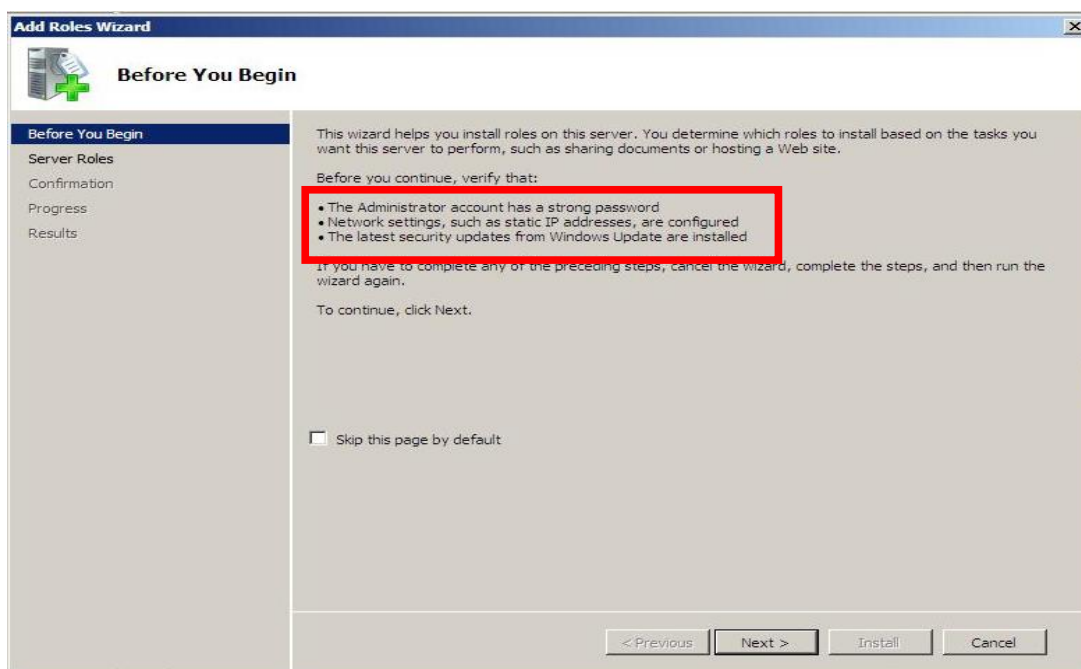
Active Directory Domain Services

DHCP Server

DNS Server

οι οποίοι είναι οι απολύτως απαραίτητοι για τη δημιουργία μιας Λογικής Περιοχής Δικτύου (Domain).

2. Επιλέγουμε: **Add Roles** (κόκκινο βέλος στην Εικόνα 3) και εμφανίζεται το παράθυρο της Εικόνας 4.



**Εικόνα 4. Προαπαιτούμενα εγκατάστασης ρόλου στον Server.**

Σ' αυτό το παράθυρο φαίνονται τα προαπαιτούμενα για την εγκατάσταση ενός ρόλου στον Server που είναι:

Ισχυρό Συνθηματικό για τον λογαριασμό του Administrator.

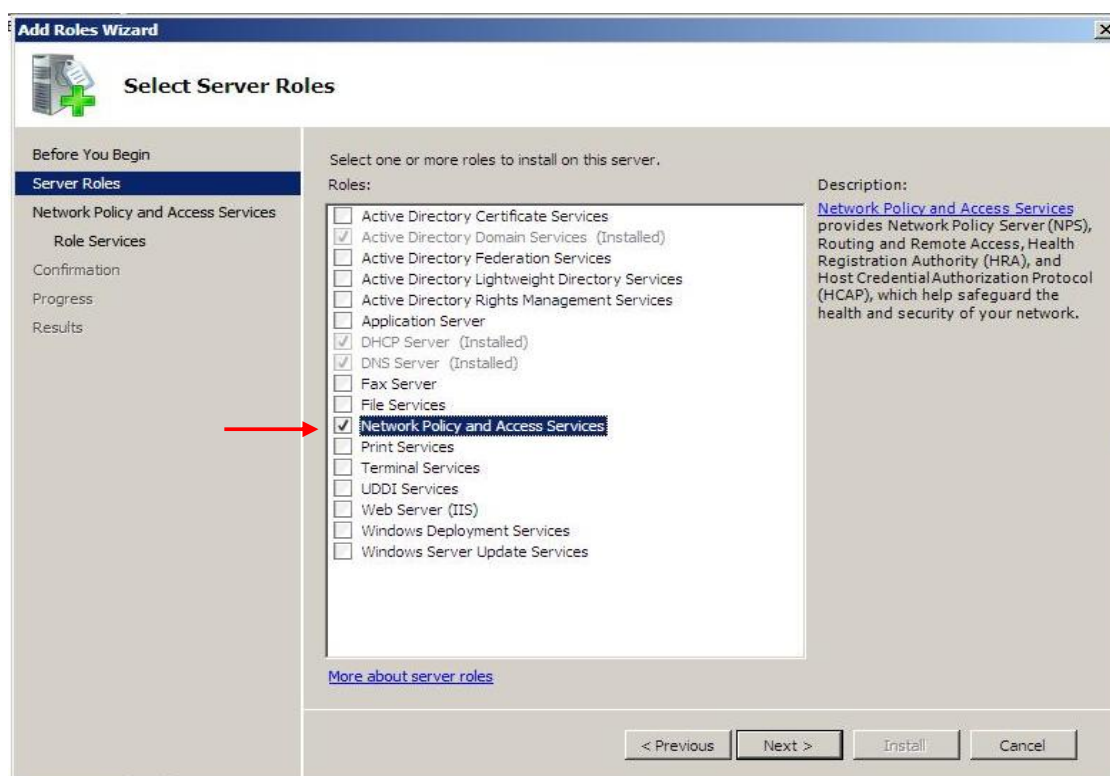
Να έχουν ορισθεί σωστά οι δικτυακές παράμετροι των NIC.

Να έχουν εγκατασταθεί οι ενημερώσεις των Windows που αφορούν την ασφάλεια.

Πριν προχωρήσουμε στο επόμενο βήμα θα πρέπει να είμαστε σίγουροι ότι έχει εγκατασταθεί και η δεύτερη NIC, ότι λειτουργεί σωστά και ότι έχουν ορισθεί σωστά οι δικτυακές παράμετροι. Εάν κάτι από τα προηγούμενα δεν ισχύει επιλέγουμε: **Cancel** και κάνουμε τις απαραίτητες ενέργειες ώστε να ισχύουν τα προαπαιτούμενα.

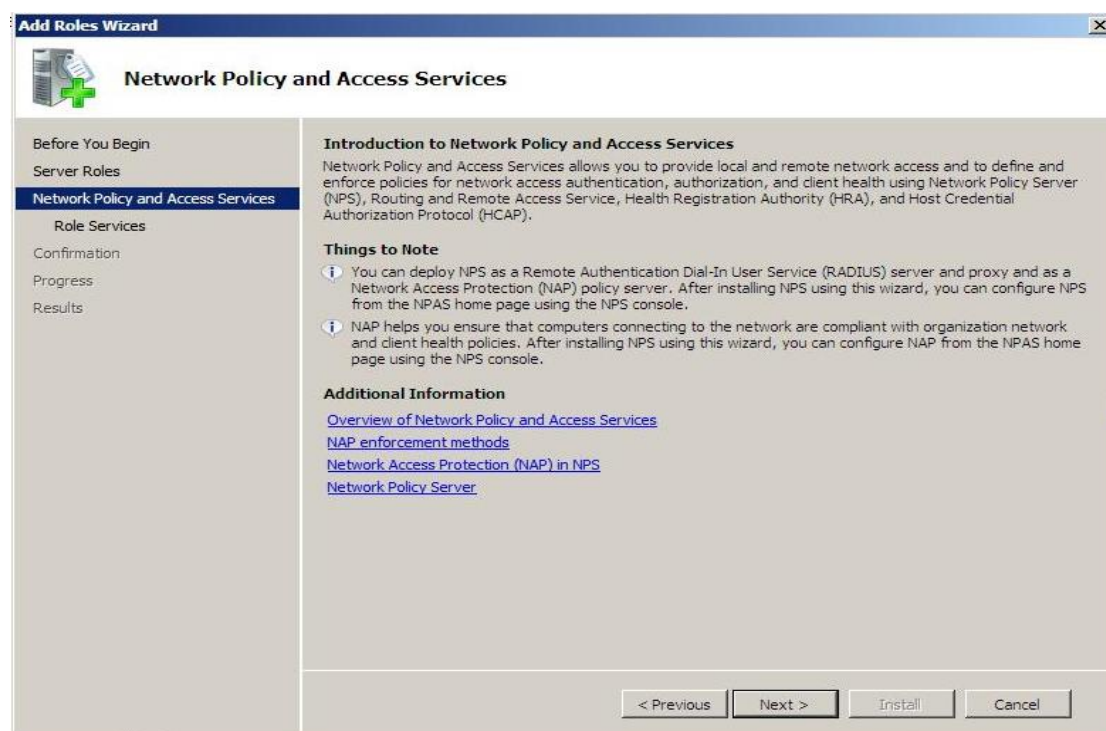
Αφού όλα είναι εντάξει επιλέγουμε: **Next**.

3. Επιλέγουμε να εγκαταστήσουμε τον ρόλο: **Network Policy and Access Services** (Εικόνα 5) και κατόπιν επιλέγουμε: **Next**.



Εικόνα 5. Επιλογή ρόλου: **Network Policy and Access Services**.

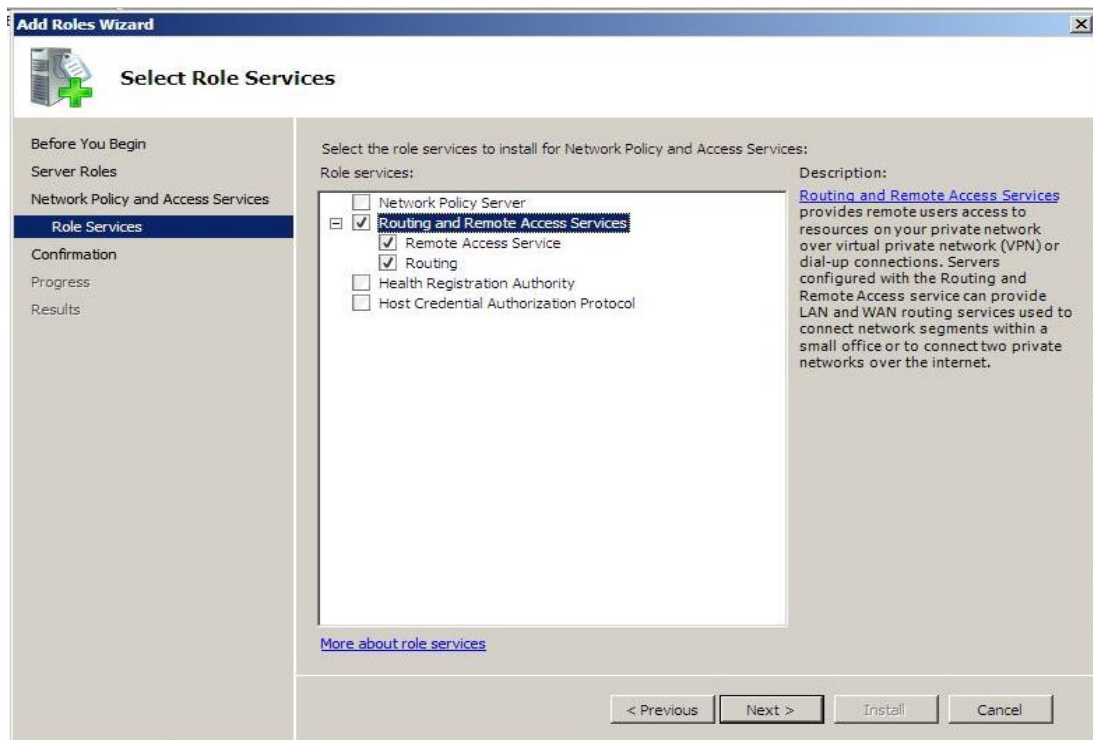
4. Σε αυτό το παράθυρο ενημερωνόμαστε περιληπτικά σχετικά με τις Network Policy and Access Services. Επιλέγουμε: **Next**.



Εικόνα 6. Εισαγωγή, Δυνατότητες και περαιτέρω Πληροφόρηση για τις **Network Policy and Access Services**.

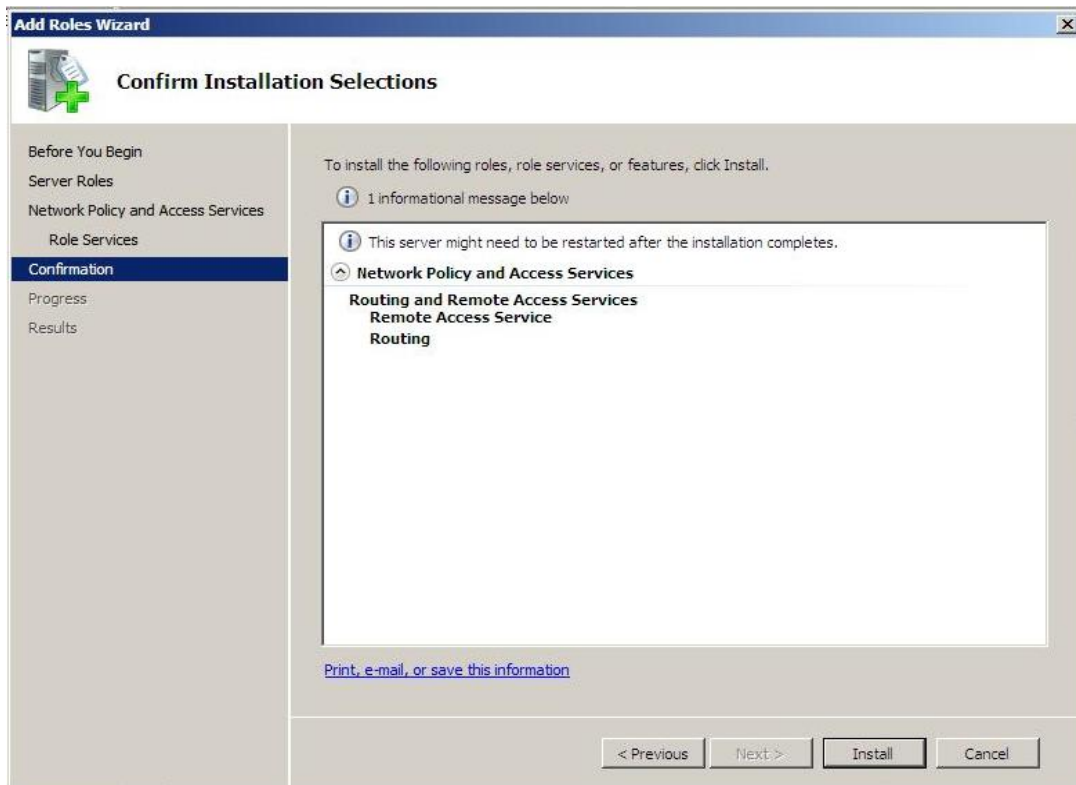


5. Σε αυτό το παράθυρο επιλέγουμε και τις δύο υπηρεσίες (Remote Access και Routing). Εάν θέλαμε να εξυπηρετήσουμε μόνο την απομακρυσμένη σύνδεση χρηστών θα μπορούσαμε να ενεργοποιήσουμε μόνο την **Remote Access Service**. Όμως συνηθίζουμε να ενεργοποιούμε και την **Routing** καθώς είναι πιθανό να μας εξυπηρετήσει μελλοντικά σε πιο σύνθετες καταστάσεις όπως διασύνδεση απομακρυσμένων μεταξύ τους LAN της ίδιας εταιρείας. Κατόπιν επιλέγουμε: **Next**.

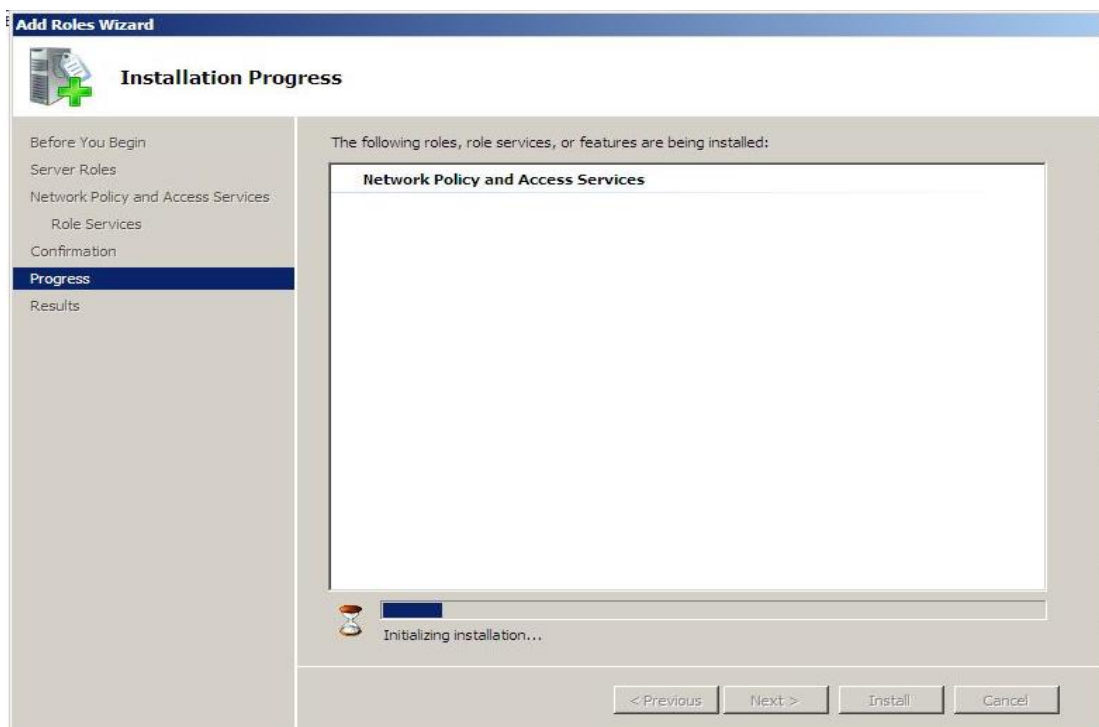


Εικόνα 7. Ενεργοποίηση υπηρεσιών Routing and Remote Access.

6. Σε αυτό το παράθυρο επιβεβαιώνουμε την πρόθεση μας για την εγκατάσταση των υπηρεσιών Routing and Remote Access επιλέγοντας: **Install**.



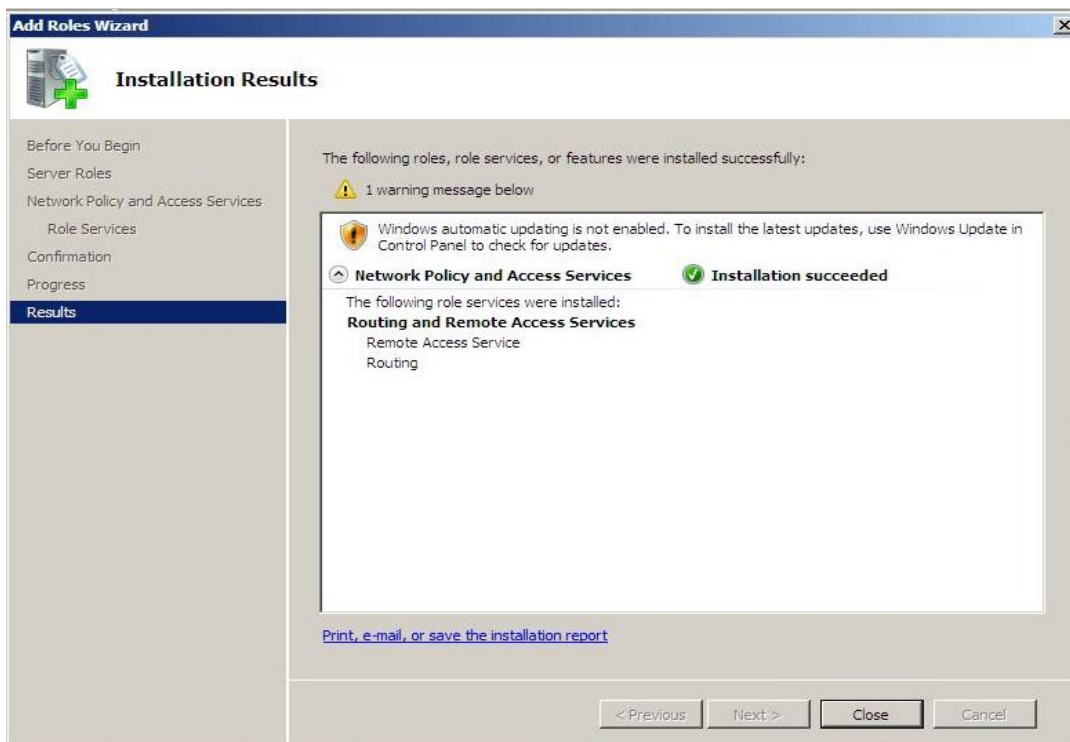
Εικόνα 8. Επιβεβαίωση εγκατάστασης υπηρεσιών Routing and Remote Access.



Εικόνα 9. Εξέλιξη εγκατάστασης υπηρεσιών Routing and Remote Access.

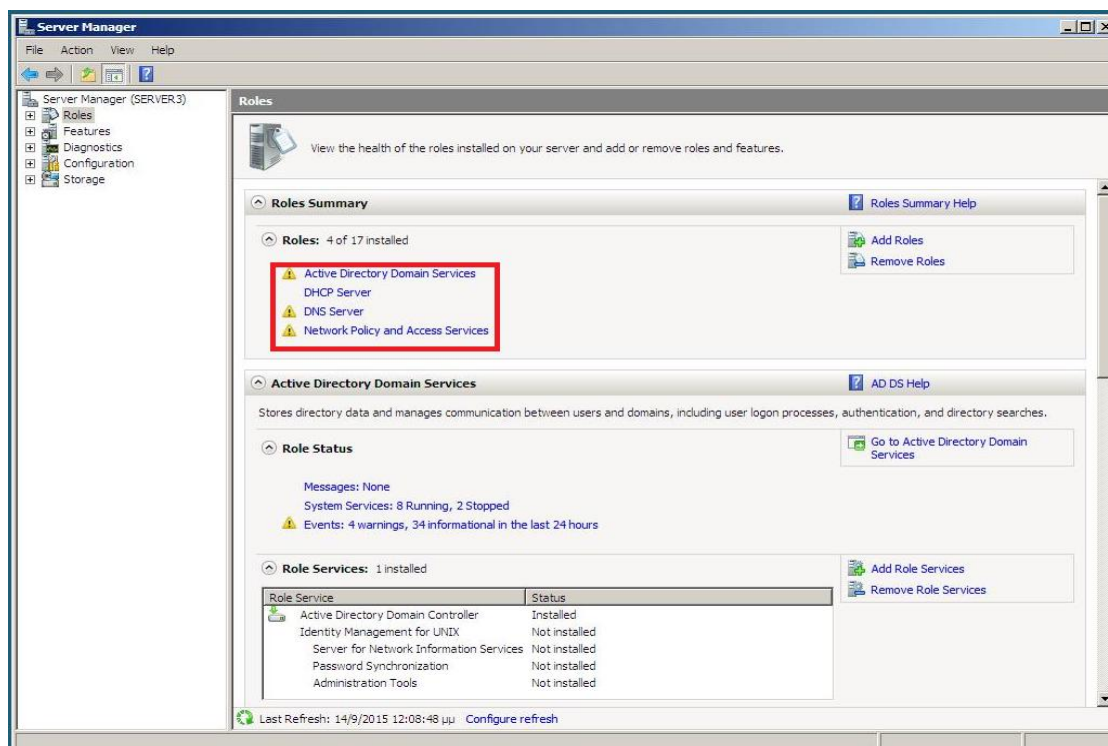
7. Στο παράθυρο αυτό διαπιστώνουμε ότι η εγκατάσταση των υπηρεσιών Routing and Remote

Access ήταν επιτυχής. Επιλέγουμε: **Close**.



**Εικόνα 10. Αποτέλεσμα εγκατάστασης υπηρεσιών Routing and Remote Access.**

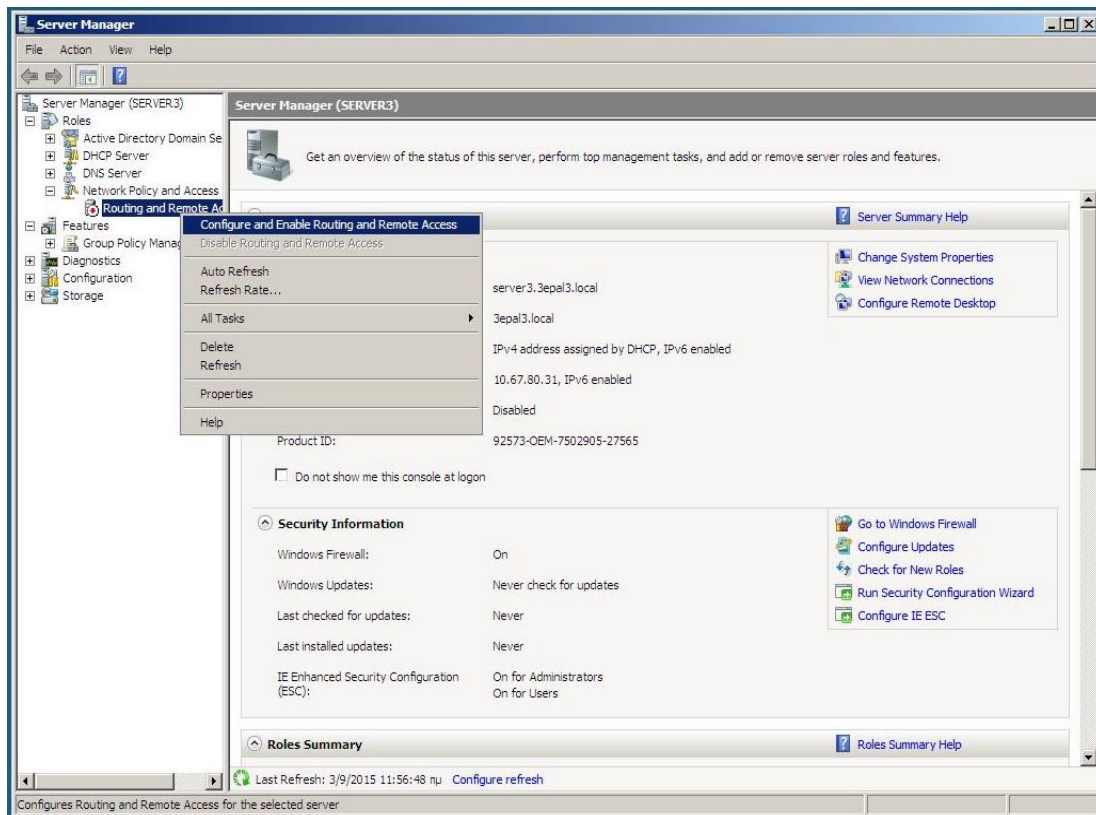
8. Στο παράθυρο του Server Manager φαίνονται οι εγκατεστημένοι ρόλοι του Server.



**Εικόνα 11. Εγκατεστημένοι ρόλοι του Server.**

**Β. Παραμετροποίηση RRAS για την παροχή της υπηρεσίας VPN.**

1. Επιλέγουμε **Start** → **Administrative Tools** → **Server Manager**, επεκτείνουμε το **Roles** container, επεκτείνουμε το **Network Policy and Access Services** container, κάνουμε δεξί click στο **Routing and Remote Access** και επιλέγουμε: **Configure and Enable Routing and Remote Access** (Εικόνα 12). Στο παράθυρο του Wizard που εμφανίζεται επιλέγουμε: **Next**.



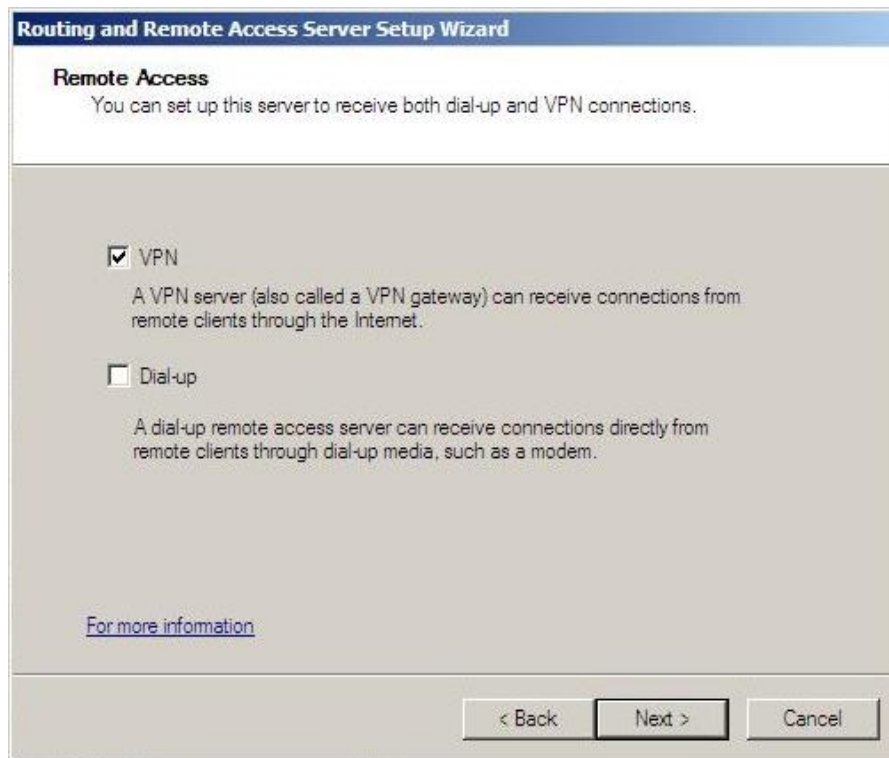
**Εικόνα 12. Ενεργοποίηση του RRAS.**

2. Στο επόμενο παράθυρο επιλέγουμε: **Remote access (dial-up or VPN)** και μετά: **Next**.



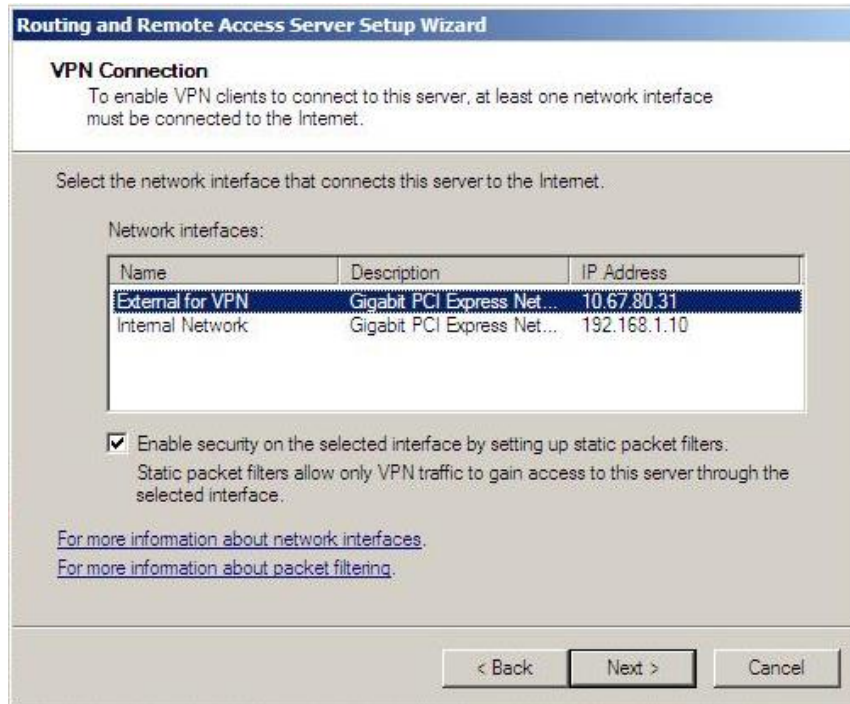
**Εικόνα 13. Επιλογή είδους απομακρυσμένης υπηρεσίας.**

3. Στο επόμενο παράθυρο επιλέγουμε τη συγκεκριμένη υπηρεσία: **VPN** και μετά: **Next**.



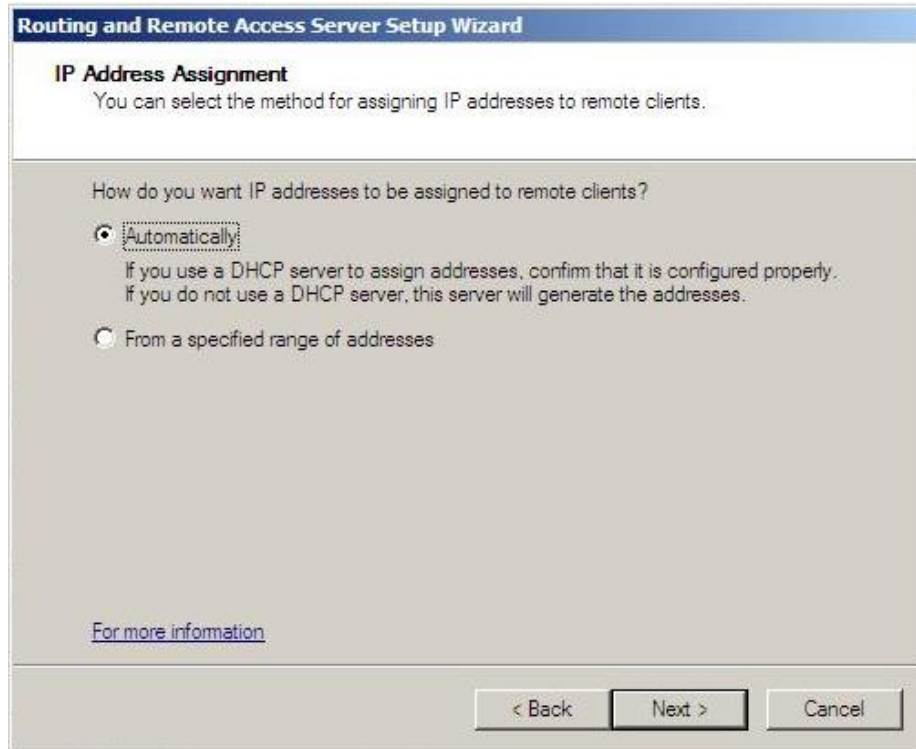
**Εικόνα 14. Επιλογή υπηρεσίας VPN.**

4. Στο επόμενο παράθυρο επιλέγουμε από ποια NIC θα συνδέονται οι VPN πελάτες (δλδ. Οι απομεμακρυσμένοι χρήστες) στον RRAS. Εξ ορισμού είναι ενεργοποιημένα τα Στατικά Φίλτρα Πακέτων δεδομένων για μέγιστη ασφάλεια. Αυτά με πολύ “στατικό” τρόπο επιτρέπουν την κυκλοφορία των VPN πακέτων δεδομένων και κανενός άλλου αποκλείοντας έτσι την πρόσβαση στις υπηρεσίες Διαδικτύου των Η/Υ του LAN. Για τα δεδομένα της άσκησης αφήνουμε την προεπιλογή της ενεργοποίησης των Στατικών Φίλτρων Πακέτων, επιλέγουμε τη NIC που μας ενδιαφέρει και επιλέγουμε: **Next**.



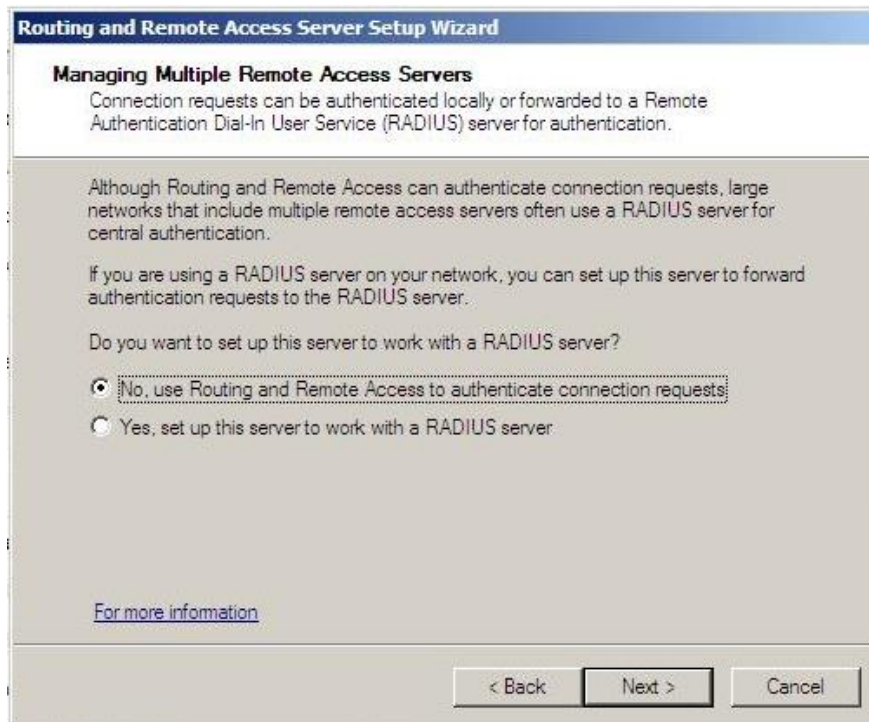
**Εικόνα 15. Επιλογή NIC σύνδεσης VPN πελατών στον RRAS.**

5. Στο επόμενο παράθυρο επιλέγουμε τον τρόπο εκχώρησης των IP διευθύνσεων στους VPN χρήστες. Κατά την προεπιλεγμένη περίπτωση (**Automatically**) ο DHCP Server του LAN παρέχει αυτές τις διευθύνσεις. Εάν δεν υπάρχει DHCP Server ή εάν δεν θέλουμε να γίνεται η εκχώρηση αυτών των διευθύνσεων από τον DHCP Server επιλέγουμε: **From a specified range of addresses** και θα πρέπει σε επόμενο στάδιο να καθορίσουμε αυτή τη περιοχή διευθύνσεων. Στη περίπτωση που επιλέξουμε: **From a specified range of addresses** και υπάρχει και DHCP Server θα πρέπει να ληφθεί πρόνοια για να μην εκχωρούνται ίδιες IP διευθύνσεις. Για τα δεδομένα της άσκησης αφήνουμε την προεπιλογή και επιλέγουμε: **Next**.



**Εικόνα 16. Επιλογή του τρόπου εκχώρησης των IP διευθύνσεων στους VPN χρήστες.**

6. Στο επόμενο παράθυρο επιλέγουμε τον τρόπο πιστοποίησης της αυθεντικότητας των VPN χρηστών. Η προεπιλογή πραγματοποιεί, κατ' ουσία, αυτή την πιστοποίηση μέσω του Ενεργού Καταλόγου (Active Directory) που είναι και η επαρκής για μικρά και απλά δίκτυα. Για πιο μεγάλα και σύνθετα δίκτυα είναι επιβεβλημένη η χρήση των RADIUS servers. Για τα δεδομένα της άσκησης αφήνουμε την προεπιλογή και επιλέγουμε: **Next**.



Εικόνα 17. Επιλογή του τρόπου αυθεντικοποίησης των VPN χρηστών.

7. Στο επόμενο παράθυρο παρουσιάζονται περιληπτικά οι επιλογές που έχουμε κάνει μέχρι τώρα. Επιλέγουμε: **Finish**.



Εικόνα 18. Περίληψη των επιλογών που έχουμε κάνει.

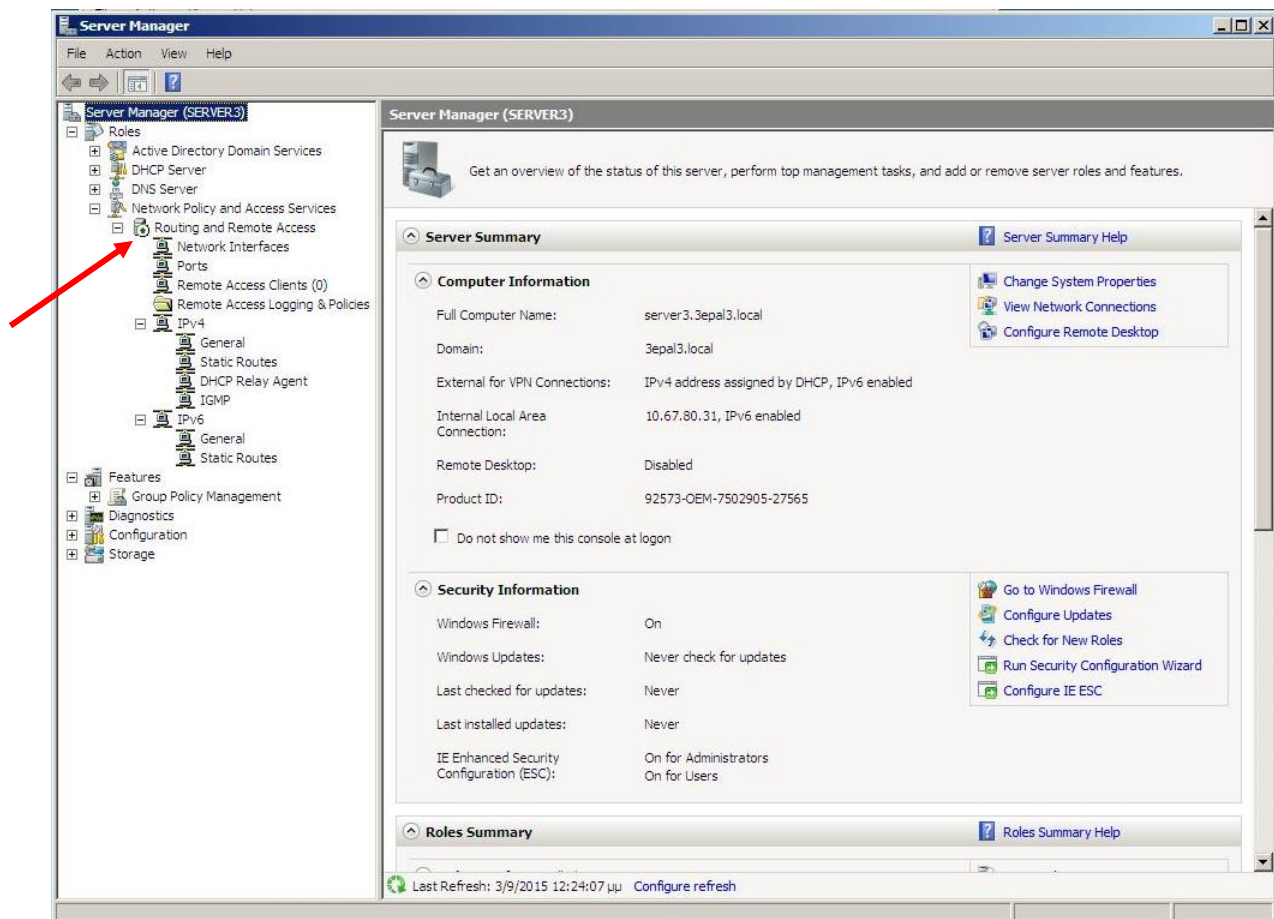


8. Το επόμενο προειδοποιητικό παράθυρο μας επισημαίνει ότι εφ' όσον θέλουμε να αναμεταδίδουμε τα αιτήματα παροχής υπηρεσίας DHCP από τους απομακρυσμένους VPN χρήστες, θα πρέπει καθορίσουμε καταλλήλως τις ιδιότητες του DHCP Relay Agent. Επιλέγουμε: **OK**.



**Εικόνα 19. Υπενθύμιση καθορισμού ιδιοτήτων DHCP Relay Agent.**

9. Στο επόμενο παράθυρο παρατηρούμε ότι η υπηρεσία Routing and Remote Access είναι ενεργή.

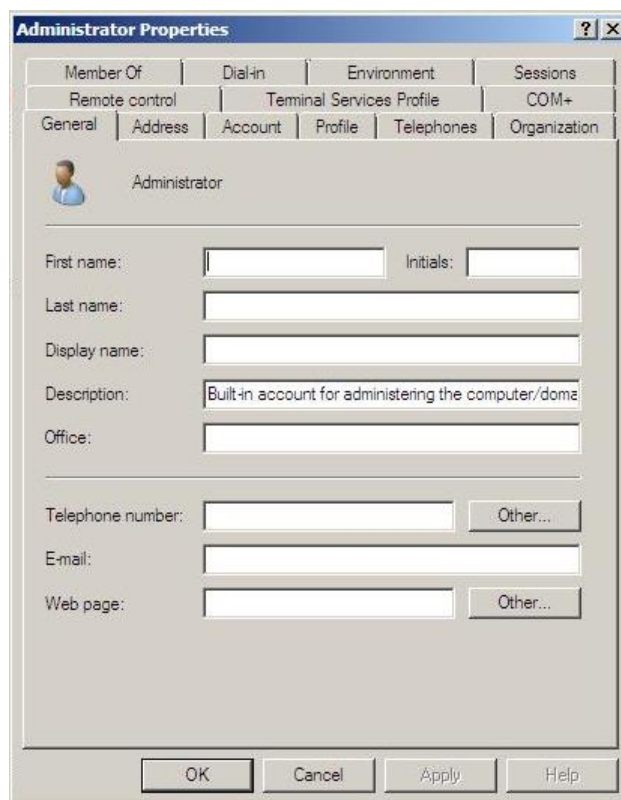


**Εικόνα 20. Ενεργοποιημένη υπηρεσία Routing and Remote Access.**

## Γ. Εγγραφή χρηστών στην υπηρεσία VPN.

1. Η διαδικασία δημιουργίας χρηστών που θα χρησιμοποιούν την υπηρεσία VPN είναι η ίδια με αυτή της δημιουργίας των χρηστών μιας Λογικής Περιοχής Δικτύου που έχουμε δει σε προηγούμενη άσκηση. Μπορούμε επίσης σε υπάρχοντα χρήστη να δώσουμε τη δυνατότητα της απομακρυσμένης πρόσβασης π.χ. στον Administrator.

Ανοίγουμε τις ιδιότητες του χρήστη Administrator και επιλέγουμε την ετικέτα (tab) **Dial-in**. Η ετικέτα αυτή δεν υπάρχει αν δεν είναι ενεργή η υπηρεσία Routing and Remote Access (βλέπε την Εικόνα 20).



The image shows a Windows dialog box titled "Administrator Properties". The "General" tab is selected. The dialog contains the following fields and controls:

- Member Of: [ ]
- Dial-in: [ ]
- Environment: [ ]
- Sessions: [ ]
- Remote control: [ ]
- Terminal Services Profile: [ ]
- COM+: [ ]
- General: [x]
- Address: [ ]
- Account: [ ]
- Profile: [ ]
- Telephones: [ ]
- Organization: [ ]

Fields for user information:

- First name: [ ] Initials: [ ]
- Last name: [ ]
- Display name: [ ]
- Description: Built-in account for administering the computer/doma...
- Office: [ ]
- Telephone number: [ ] Other...
- E-mail: [ ]
- Web page: [ ] Other...

Buttons at the bottom: OK, Cancel, Apply, Help.

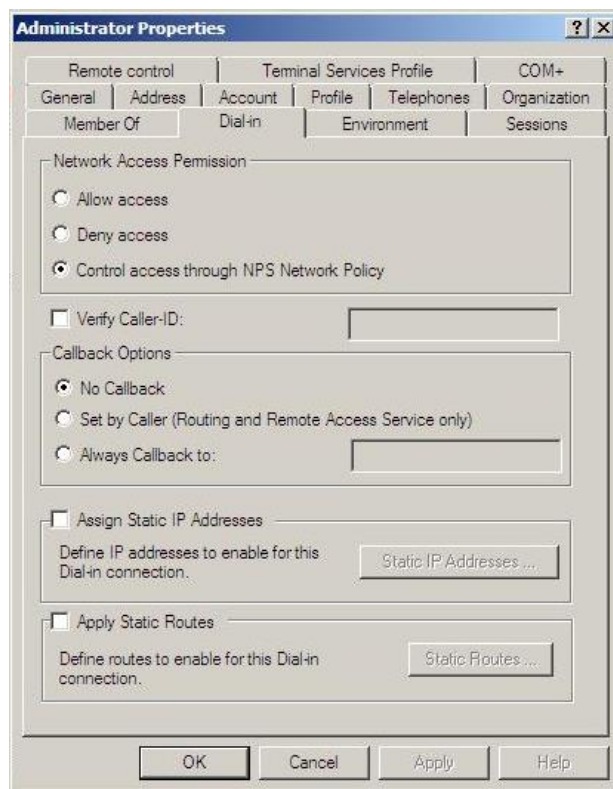
Εικόνα 21. Ιδιότητες Administrator.

2. Στο παράθυρο της ετικέτας Dial-in που ανοίγει (Εικόνα 22) φαίνονται τέσσερα διακριτά τμήματα.

Το δεύτερο τμήμα που περιλαμβάνει το Verify Caller-ID και τα Callback Options αφορά την σύνδεση του χρήστη μέσω ISDN ή PSTN με χρήση modem που δεν μας ενδιαφέρει σ' αυτή την περίπτωση.

Το τρίτο τμήμα αφορά την εκχώρηση στατικής IP διεύθυνσης στη δικτυακή σύνδεση αυτού του χρήστη που δεν μας ενδιαφέρει σ' αυτή την περίπτωση.

Το τέταρτο τμήμα που αφορά τη δημιουργία στατικών δικτυακών οδεύσεων μέσα από το υπόλοιπο δίκτυό μας για τη δικτυακή σύνδεση αυτού του χρήστη που δεν μας ενδιαφέρει σ' αυτή την περίπτωση.



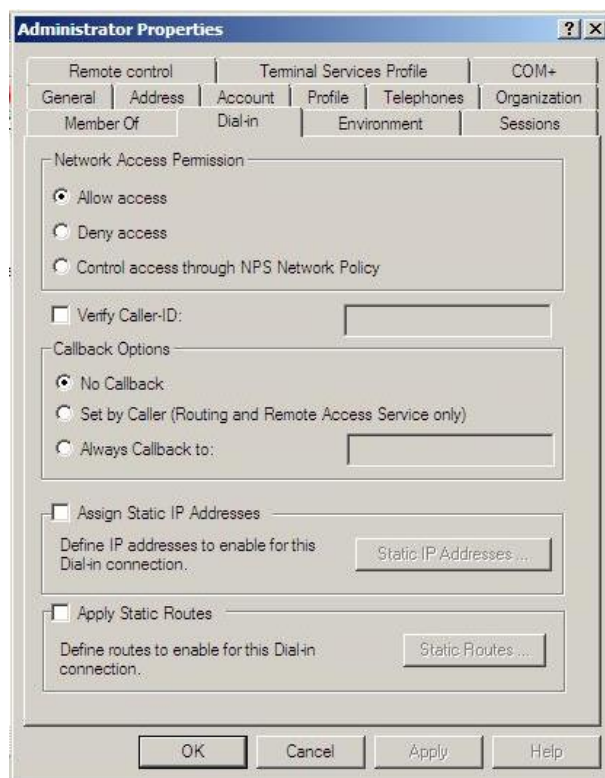
**Εικόνα 22. Ετικέτα Dial-in.**

Και το πρώτο τμήμα Network Access Permission που αφορά τον τρόπο αδειοδότησης πρόσβασης στο δίκτυό μας για τον συγκεκριμένο χρήστη.

Η προεπιλογή δείχνει ότι δικτυακή πολιτική πρόσβασης καθορίζεται από τον Network Policy Server (NPS). Επειδή δεν θέλουμε να μπλέξουμε με τη δικτυακή πολιτική του NPS

και επειδή δεν θέλουμε να εμποδίσουμε την δικτυακή πρόσβαση (Deny access)

επιλέγουμε: **Allow access**. (Εικόνα 23)

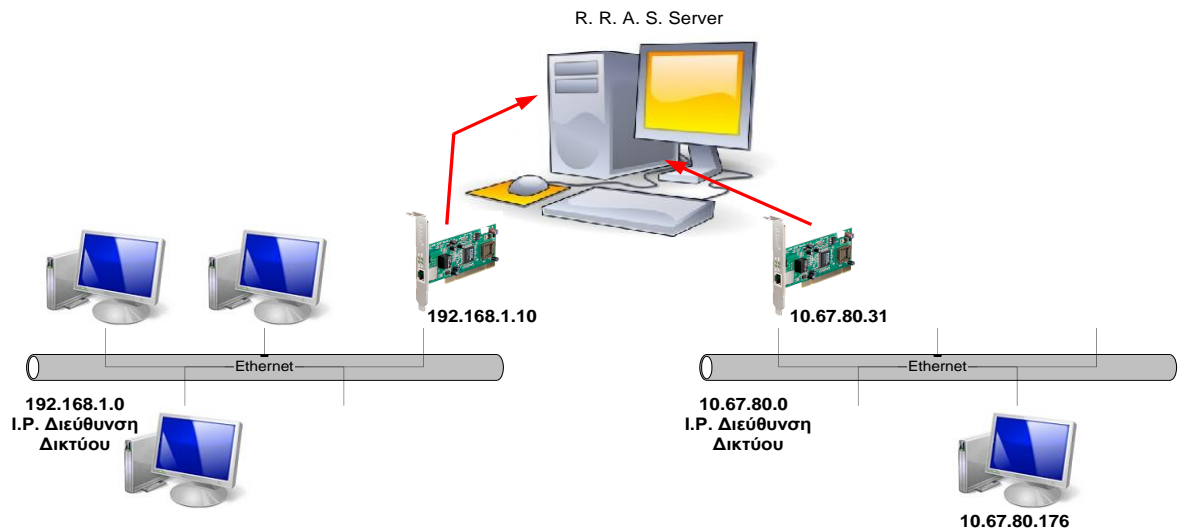


**Εικόνα 23. Επίτρεψη πρόσβασης του χρήστη από VPN σύνδεση.**

Τέλος επιλέγουμε: **OK** για να κλείσει το παράθυρο ιδιοτήτων του Administrator.

## Δ. Δημιουργία VPN σύνδεσης σε απομακρυσμένο Η/Υ (XP) και δοκιμές λειτουργίας.

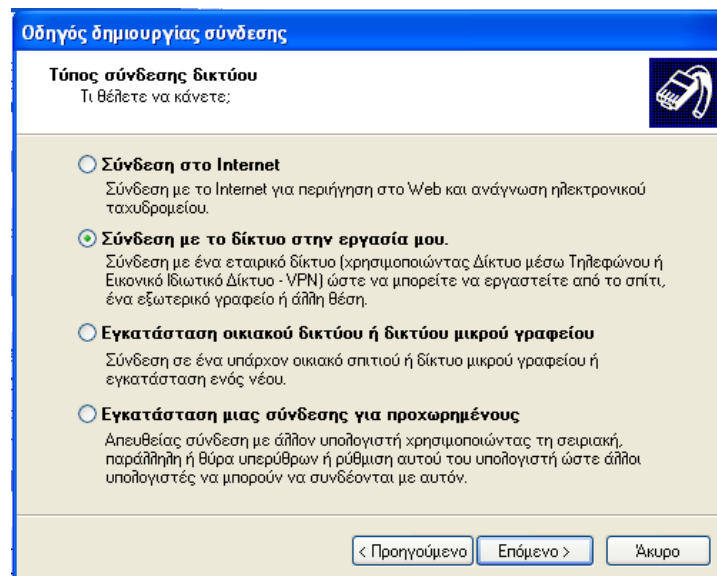
Το δίκτυό μας τώρα έχει τη μορφή που φαίνεται στην Εικόνα 24.



Εικόνα 24. Τα δίκτυα που διασύνδεει ο R.R.A.S. Server.

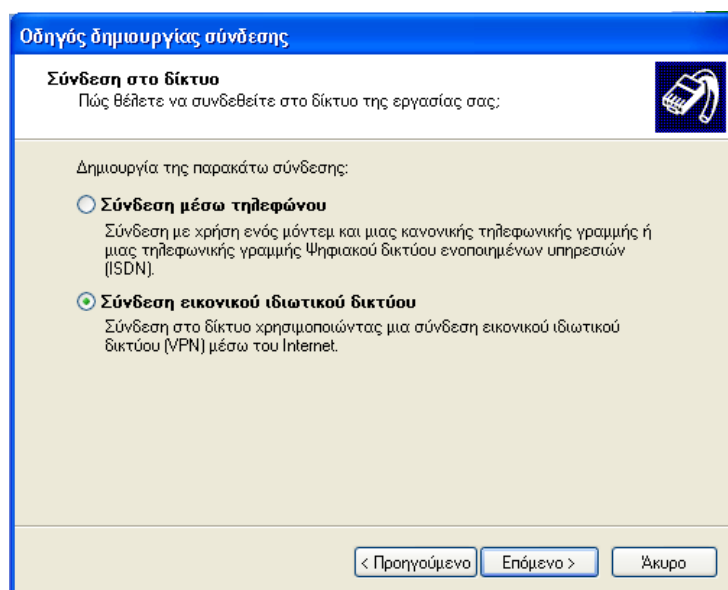
Δοκιμαστικά θα δημιουργήσουμε μια VPN σύνδεση σε ένα Η/Υ του δικτύου 10.67.80.0 για να επιτύχουμε VPN επικοινωνία με το δίκτυο 192.1698.1.0.

1. Ευρισκόμενοι στην επιφάνεια εργασίας των windows XP του Η/Υ με IP διεύθυνση 10.67.80.176 επιλέγουμε: **έναρξη** → **Πίνακας Ελέγχου** → **Συνδέσεις Δικτύου**. Στο παράθυρο που ανοίγει επιλέγουμε: **Δημιουργία νέας σύνδεσης**. Ανοίγει το παράθυρο του Οδηγού δημιουργίας σύνδεσης. Επιλέγουμε: **Επόμενο**.
2. Στο παράθυρο που ανοίγει επιλέγουμε: **Σύνδεση με το δίκτυο στην εργασία μου και Επόμενο** (Εικόνα 25).



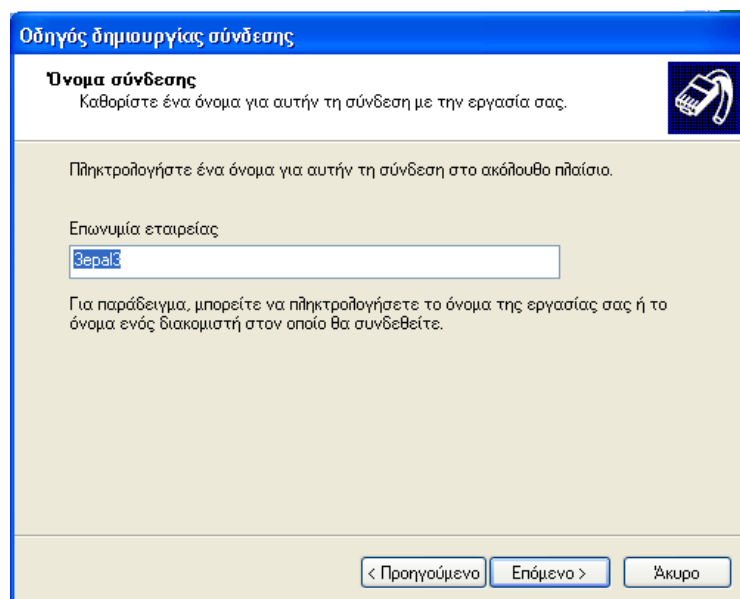
Εικόνα 25. Σύνδεση με το δίκτυο στην εργασία μου.

3. Στο παράθυρο που ανοίγει επιλέγουμε: **Σύνδεση εικονικού ιδιωτικού δικτύου** και **Επόμενο** (Εικόνα 26).



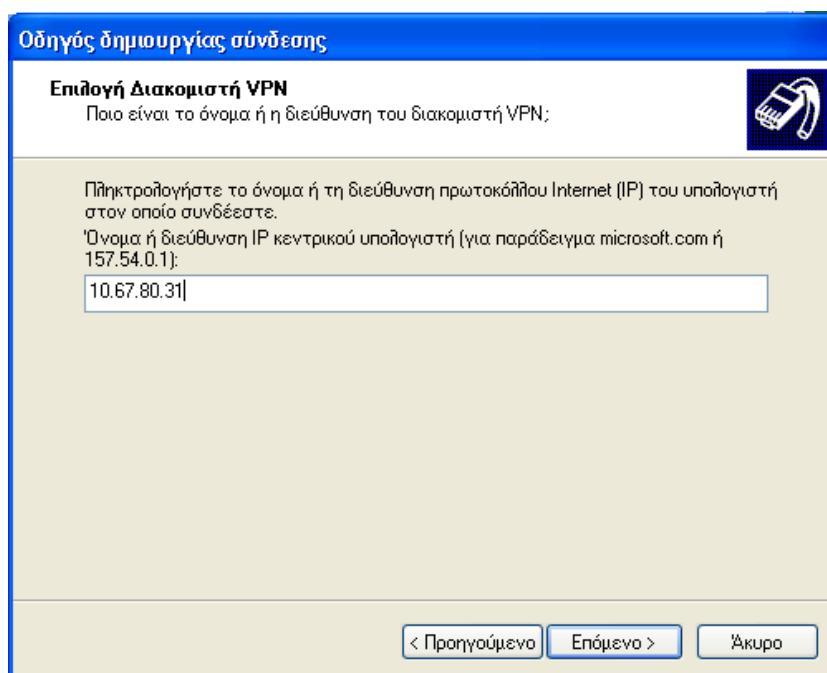
**Εικόνα 26. Σύνδεση εικονικού ιδιωτικού δικτύου.**

4. Στο παράθυρο που ανοίγει εισάγουμε ένα όνομα για τη σύνδεση μας π.χ. το όνομα του domain του δικτύου της εταιρείας και επιλέγουμε **Επόμενο** (Εικόνα 27).



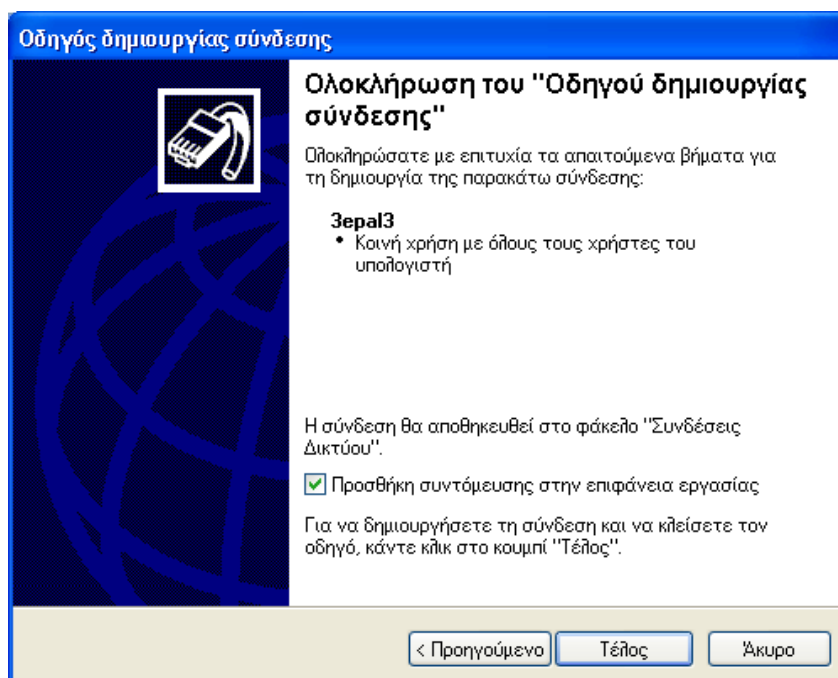
**Εικόνα 27. Όνομα της VPN σύνδεσης.**

5. Στο παράθυρο που ανοίγει εισάγουμε την IP Διεύθυνσης του R.R.A.S. Server και επιλέγουμε **Επόμενο** (Εικόνα 28).



Εικόνα 28. IP διεύθυνση του R.R.A.S. Server.

6. Τέλος στο παράθυρο που ανοίγει επιλέγουμε την **Προσθήκη** συντόμευσης στην **επιφάνεια εργασίας** και επιλέγουμε: **Τέλος** (Εικόνα 29).



Εικόνα 29.

7. Πριν προχωρήσουμε στη προσπάθεια της VPN σύνδεσης ας δούμε πως φαίνονται οι Network Connections του R.R.A.S. Server και του Σταθμού Εργασίας με τη χρήση της εντολής ipconfig/all στο Command Prompt (Εικόνες 30 και 31). Συγκρίνουμε τις σημειούμενες με κίτρινα βέλη IP διευθύνσεις με τις αντίστοιχες της Εικόνας 24.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SERVER3>ipconfig/all

Windows IP Configuration

Host Name . . . . . : server3
Primary Dns Suffix . . . . . : 3epal3.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : 3epal3.local

Ethernet adapter External for VPN :

Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 10-FE-ED-04-15-A7
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c805:1478:1de5:8fb2%12(Preferred)
IPv4 Address. . . . . : 10.67.80.31(Preferred) ←
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.67.80.1
DHCPv6 IAID . . . . . : 269549293
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-10-1F-FB-74-D4-35-92-C9-06

DNS Servers . . . . . : ::1
NetBIOS over Tcpip. . . . . : Disabled

Ethernet adapter Internal Network:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 74-D4-35-92-C9-06
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::749a:a09e:da73:4bda%10(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred) ←
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 225760309
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-10-1F-FB-74-D4-35-92-C9-06

DNS Servers . . . . . : ::1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 8:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : isatap.{FE5B81C4-87EC-4F7E-A794-3E62DCaC7
843}
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

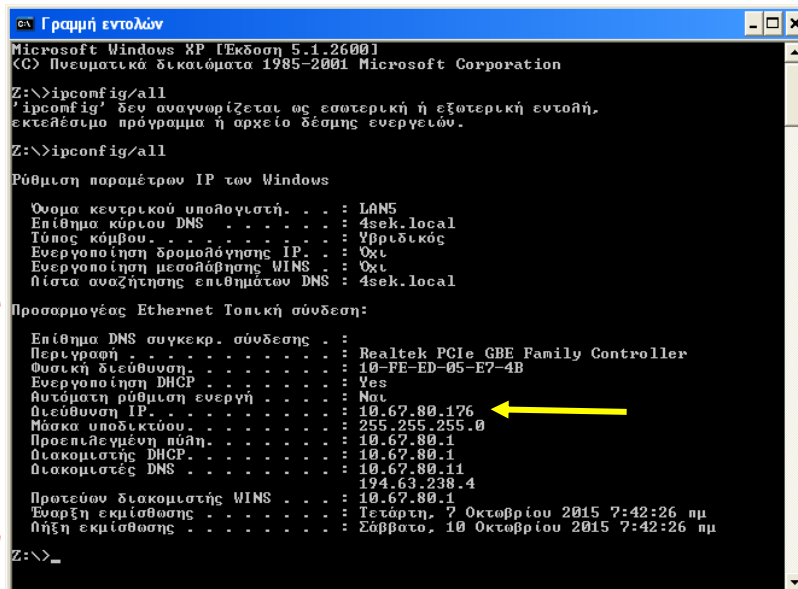
Tunnel adapter Local Area Connection* 9:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : isatap.{003EB5D1-04D4-4965-A33B-31A6CAF89
A85}
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator.SERVER3>
```

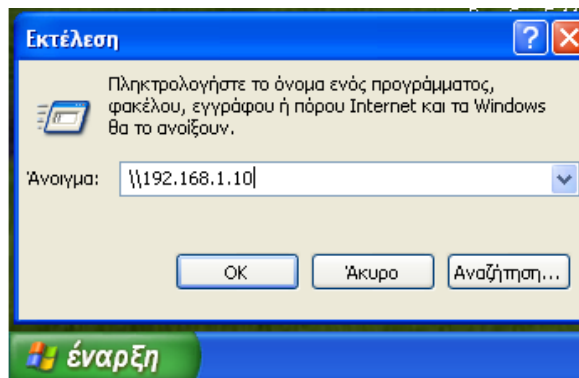
Εικόνα 30. Οι Network Connections του R.R.A.S. Server.





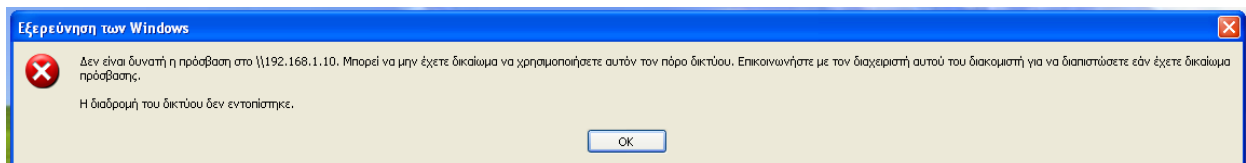
Εικόνα 31. Η Network Connection του Σταθμού Εργασίας.

8. Δοκιμαστικά από το Σταθμό Εργασίας προσπαθήσουμε να συνδεθούμε στον Server που εξυπηρετεί το δίκτυο 192.168.1.0. Επιλέγουμε: **έναρξη** → **Εκτέλεση**, εισάγουμε την IP διεύθυνση του Server και επιλέγουμε: **OK** (Εικόνα 32).



Εικόνα 32. Προσπάθεια σύνδεσης με 192.168.1.10.

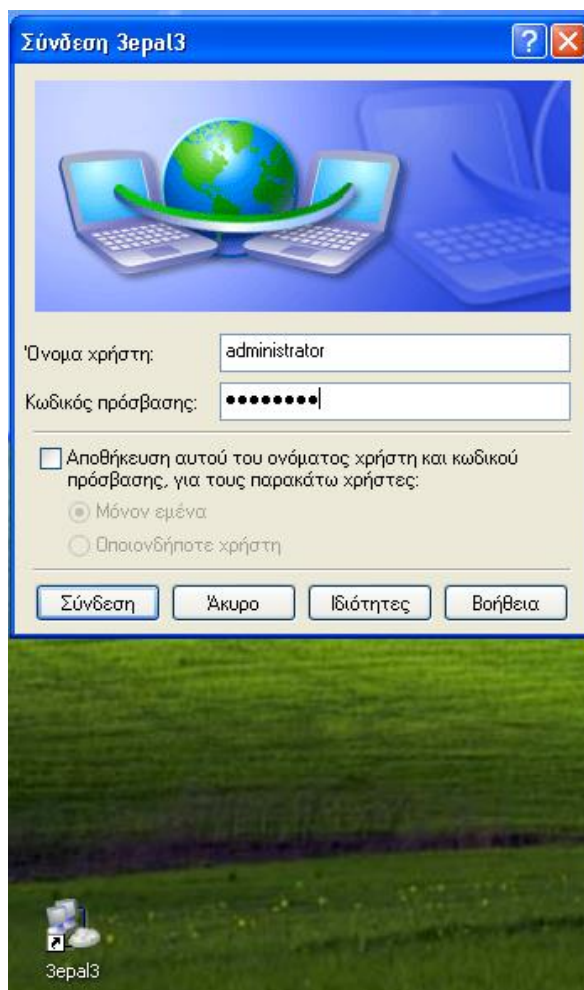
Όμως καθώς ο Σταθμός Εργασίας και η NIC του Server στον οποίο θέλουμε να συνδεθούμε βρίσκονται όχι μόνο σε διαφορετικά network segments αλλά και σε διαφορετικά φυσικά δίκτυα εμφανίζεται το μήνυμα της Εικόνας 33.



Εικόνα 33. Δεν είναι δυνατή η σύνδεση με 192.168.1.10.

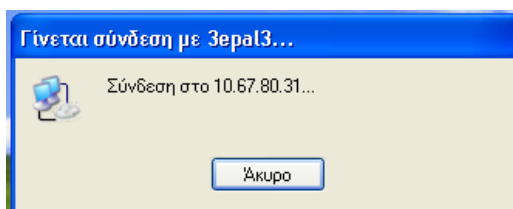
Επιλέγουμε: **OK**.

9. Για να μπορέσουμε να συνδεθούμε, λοιπόν, με το διαφορετικό αυτό network segment θα πρέπει πρώτα να πραγματοποιήσουμε τη VPN σύνδεση.  
Στον Σταθμό Εργασίας κάνουμε double click στο εικονίδιο της συντόμευσης της VPN σύνδεσης 3epal3 και στο παράθυρο που ανοίγει, εισάγουμε Ονομα χρήστη και Κωδικό πρόσβασης στα αντίστοιχα πεδία και επιλέγουμε: **Σύνδεση** (Εικόνα 34).



**Εικόνα 34. Εκκίνηση της VPN σύνδεσης.**

Στο παράθυρο που ανοίγει και δείχνει την εξέλιξη της σύνδεσης (Εικόνα 35) φαίνονται διάφορα ενδιαφέροντα μηνύματα που αποτελούν αντικείμενο διερεύνησης συνθετότερων ασκήσεων για τα δίκτυα VPN.



**Εικόνα 34. Εξέλιξη της VPN σύνδεσης.**

10. Αφού ο Σταθμός Εργασίας συνδέθηκε επιτυχώς, μέσω της VPN σύνδεσης, με τον R.R.A.S. Server ελέγχουμε πάλι τα network connections όπως κάναμε στο βήμα 7. Για τον R.R.A.S. Server βλέπετε την Εικόνα 35 και για τον Σταθμό Εργασίας βλέπετε την Εικόνα 36.

```
Administrator: Command Prompt
C:\Users\Administrator.SERUER3>ipconfig/all

Windows IP Configuration

Host Name . . . . . : server3
Primary Dns Suffix . . . . . : 3epal3.local
Mode Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : 3epal3.local

Ethernet adapter External for VPN :

Connection-specific DNS Suffix . . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 10-FE-ED-04-15-A7
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c805:1478:1de5:8fb2%12(Preferred)
IPv4 Address. . . . . : 10.67.80.31(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.67.80.1
DHCPv6 Iaid . . . . . : 267549273
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-10-1F-FB-74-D4-35-92-C9-06

DNS Servers . . . . . : ::1
127.0.0.1
NetBIOS over Tcpip. . . . . : Disabled

Ethernet adapter Internal Network:

Connection-specific DNS Suffix . . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 74-D4-35-92-C9-06
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::749a:a09e:da73:4bdax10(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 Iaid . . . . . : 225760309
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-10-1F-FB-74-D4-35-92-C9-06

DNS Servers . . . . . : ::1
127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled

PPP adapter RAS (Dial In) Interface:

Connection-specific DNS Suffix . . :
Description . . . . . : RAS (Dial In) Interface
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.1.137(Preferred)
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . :
NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter Local Area Connection* 8:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : isatap.<FE5B81C4-87EC-4F7E-A794-3E62DCAC7843>
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Local Area Connection* 9:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : isatap.<003EB5D1-04D4-4965-A33B-31A6CAF89085>
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Microsoft ISATAP Adapter #3
```

Εικόνα 35. Οι Network Connections του R.R.A.S. Server με VPN σύνδεση.

Παρατηρούμε ότι έχουν δημιουργηθεί οι δικτυακές συνδέσεις με χαρακτηριστικό PPP (Point to Point Protocol) (πρωτόκολλο VPN σύνδεσης) (πράσινες αγκύλες). Αυτές οι δικτυακές συνδέσεις συμπεριφέρονται σαν κάρτες δικτύου αφού έχουν πάρει και IP διευθύνσεις (πράσινα βέλη). Προσέξτε ότι αυτές οι IP διευθύνσεις ανήκουν στο δίκτυο 192.168.1.0. Βλέπετε και το παραστατικό σχήμα της Εικόνας 37. Δηλαδή ο Σταθμός Εργασίας έχει ενσωματωθεί το δίκτυο 192.168.1.0 μέσω του δημιουργημένου tunnel.

```

ca Γραμμή εντολών

Z:\>ipconfig/all

Ρύθμιση παραμέτρων IP του Windows

Όνομα κεντρικού υπολογιστή. . . : LAN5
Επίθημα κύριου DNS . . . . . : 4sek.local
Τύπος κόμβου. . . . . : Υβριδικός
Ενεργοποίηση δρομολόγησης IP. . : Όχι
Ενεργοποίηση μεσοδόμησης WINS . : Όχι
Πίστα αναζήτησης επιθημάτων DNS : 4sek.local
3epal3.local

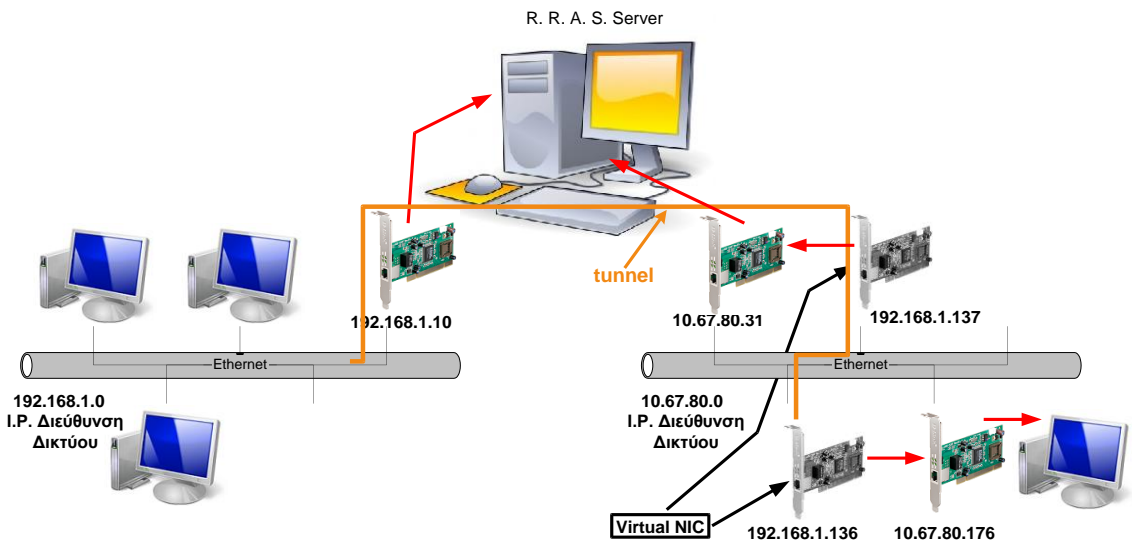
Προσαρμογές Ethernet Τοπική σύνδεση:
Επίθημα DNS συγκεκρ. σύνδεσης . :
Περιγραφή . . . . . : Realtek PCIe GBE Family Controller
Φυσική διεύθυνση. . . . . : 10-FE-ED-05-E7-4B
Ενεργοποίηση DHCP . . . . . : Yes
Αυτόματη ρύθμιση ενεργή . . . . : No
Διεύθυνση IP. . . . . : 10.67.80.176 ←
Μάσκα υποδικτύου. . . . . : 255.255.255.0
Προεπιλεγμένη πύλη. . . . . : 10.67.80.1
Διακομιστής DHCP . . . . . : 10.67.80.1
Διακομιστές DNS . . . . . : 10.67.80.11
194.63.238.4
Πρωτεύουσα διακομιστής WINS . . : 10.67.80.1
Έναρξη εκμίσθωσης . . . . . : Τετάρτη, 7 Οκτωβρίου 2015 7:42:26 πμ
Λήξη εκμίσθωσης . . . . . : Σάββατο, 10 Οκτωβρίου 2015 7:42:26 πμ

Προσαρμογές PPP 3epal3:
Επίθημα DNS συγκεκρ. σύνδεσης . : 3epal3.local
Περιγραφή . . . . . : MAN (PPP/SLIP) Interface
Φυσική διεύθυνση. . . . . : 00-53-45-00-00-00
Ενεργοποίηση DHCP . . . . . : No
Διεύθυνση IP. . . . . : 192.168.1.136 ←
Μάσκα υποδικτύου. . . . . : 255.255.255.255
Προεπιλεγμένη πύλη. . . . . : 192.168.1.136
Διακομιστές DNS . . . . . : 192.168.1.10
192.168.1.10

Z:\>_

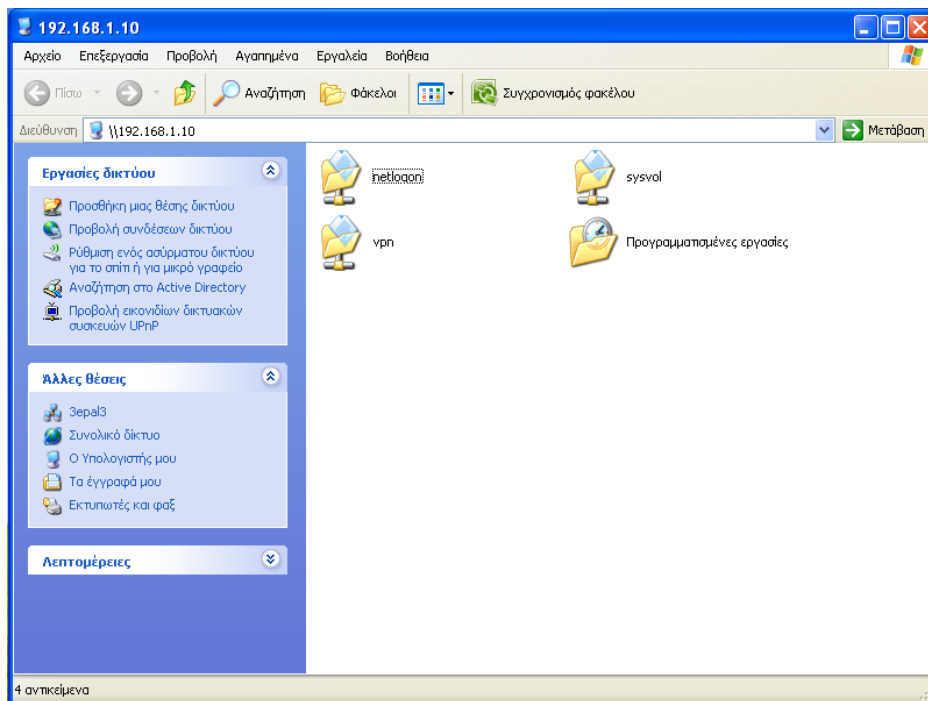
```

Εικόνα 36. Οι Network Connections του Σταθμού Εργασίας με VPN σύνδεση.



Εικόνα 37. Τα δίκτυα που διασύνδεει ο R.R.A.S. Server μετά την επιτυχή VPN σύνδεση.

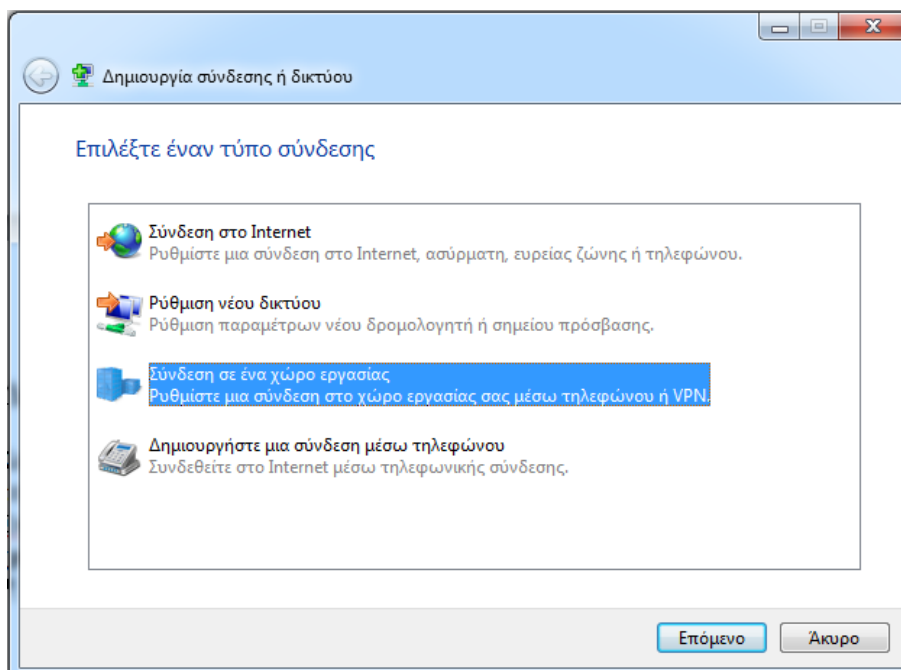
11. Αφού πλέον ο Σταθμός Εργασίας είναι μέρος του δικτύου 192.168.1.0, μπορούμε με τη διαδικασία του βήματος 8. (Εικόνα 32) να συνδεθούμε στον Server που εξυπηρετεί αυτό το δίκτυο. Το αποτέλεσμα φαίνεται στην Εικόνα 38 όπου εμφανίζονται οι κοινόχρηστοι φάκελοι αυτού του Server.



**Εικόνα 38. Ο Σταθμός Εργασίας συνδέθηκε στον Server.**

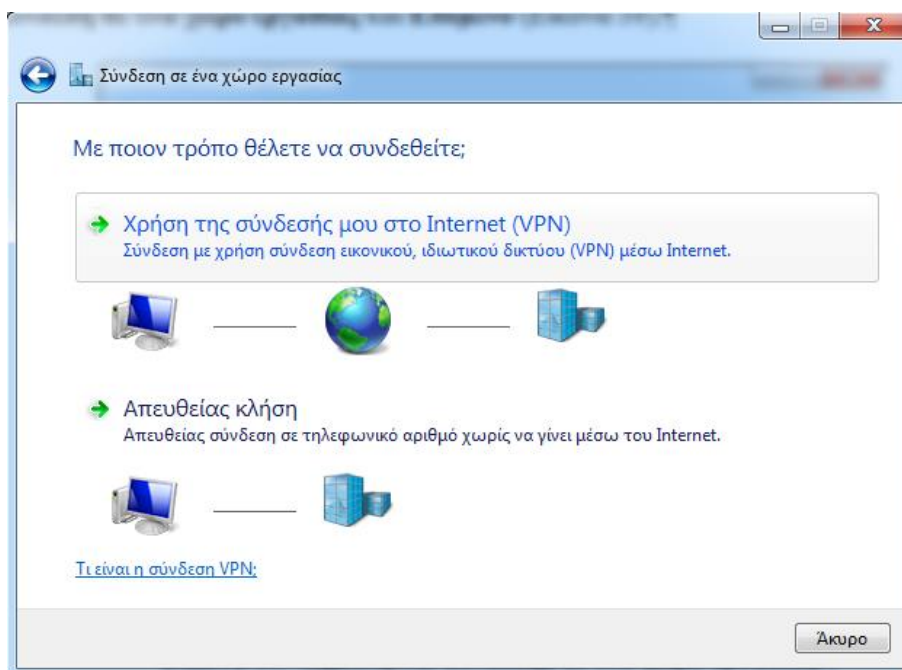
## Ε. Δημιουργία VPN σύνδεσης σε απομακρυσμένο Η/Υ (win7)

1. Κατ' αντιστοιχία προς την προηγούμενη ενότητα Δ και το βήμα 1 αυτής ευρισκόμενοι στην επιφάνεια εργασίας των windows 7 του Η/Υ με IP διεύθυνση 10.67.80.176 επιλέγουμε: **Εναρξη** → **Πίνακας Ελέγχου** → **Δίκτυο και Internet** → **Κέντρο δικτύου και κοινής χρήσης** → **Ρύθμιση νέας σύνδεσης ή δικτύου**. Στο παράθυρο που ανοίγει επιλέγουμε: **Σύνδεση σε ένα χώρο εργασίας** και **Επόμενο** (Εικόνα 39).



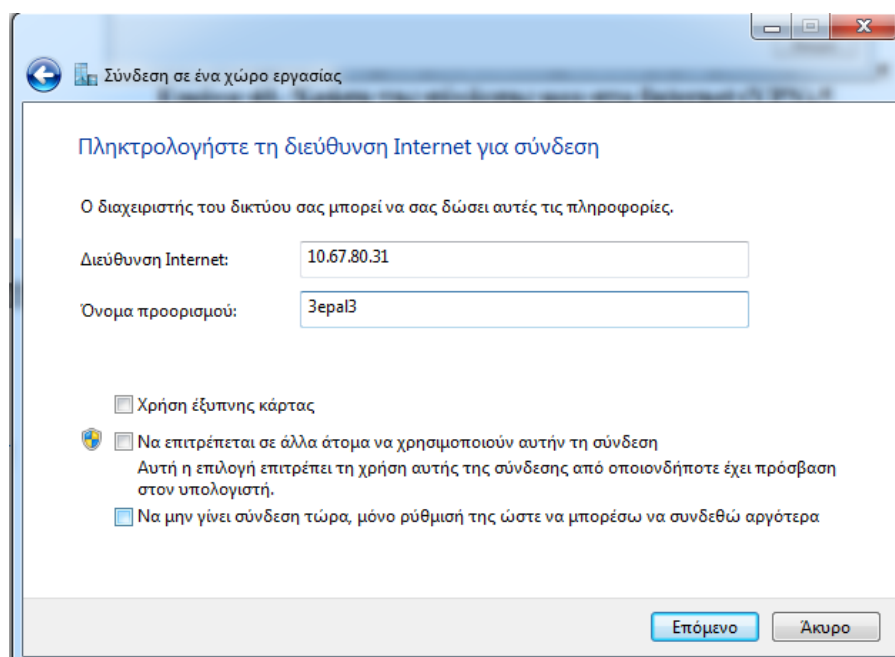
Εικόνα 39. Δημιουργία σύνδεσης σε ένα χώρο εργασίας.

2. Στο επόμενο παράθυρο επιλέγουμε: **Χρήση της σύνδεσής μου στο Internet (VPN)** (Εικόνα 40).



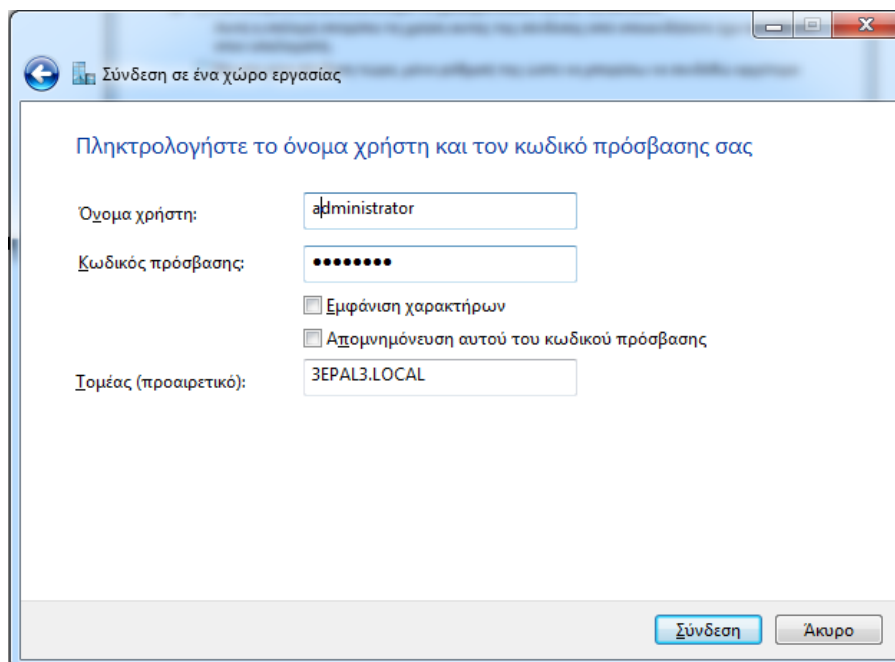
Εικόνα 40. Χρήση της σύνδεσής μου στο Internet (VPN).

3. Στο παράθυρο που ανοίγει εισάγουμε την IP Διεύθυνσης του R.R.A.S. Server, δίνουμε ένα σχετικό όνομα προορισμού στην σύνδεση και επιλέγουμε **Επόμενο** (Εικόνα 41).



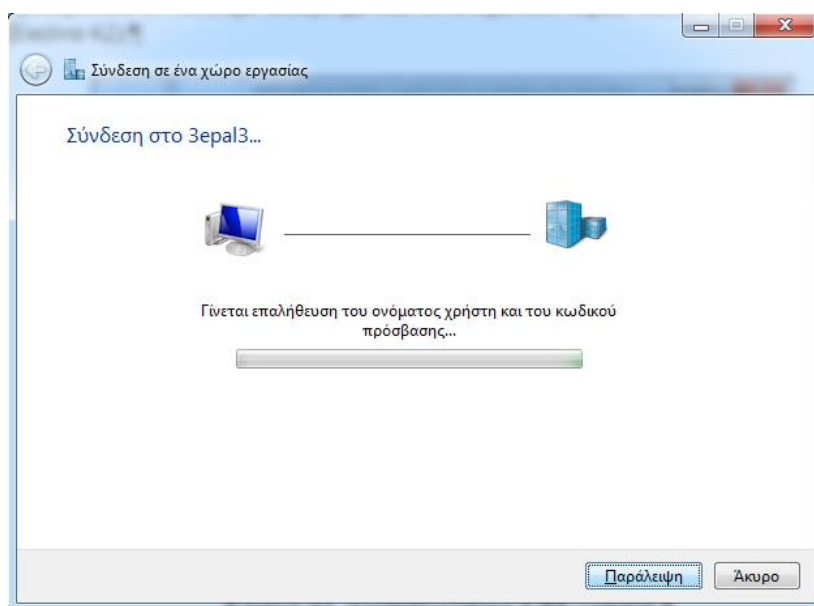
Εικόνα 41. IP διεύθυνση του R.R.A.S. Server και όνομα προορισμού.

4. Εισάγουμε το όνομα και τον κωδικό πρόσβασης του χρήστη στα αντίστοιχα πεδία. Προαιρετικά αν θέλουμε εισάγουμε και το όνομα του τομέα. Τέλος επιλέγουμε: **Σύνδεση** (Εικόνα 42).



Εικόνα 42. Διαπιστευτήρια VPN χρήστη.

5. Στο επόμενο παράθυρο βλέπουμε την εξέλιξη της διαδικασίας της VPN σύνδεσης (Εικόνα 43).



Εικόνα 43. Εξέλιξη της διαδικασίας της VPN σύνδεσης.

## ΣΤ. Σύνδεση μέσω Διαδικτύου.

Μέχρι τώρα οι συνδέσεις που δημιουργήσαμε στις ενότητες **Δ.** και **Ε.** και οι δοκιμές που κάναμε στην ενότητα **Δ.** αφορούσαν εργαστηριακές δοκιμές μέσα στα πλαίσια των σχετικών ασκήσεων για δίκτυα Η/Υ.

Θα μπορούσαν να αποτελούν και πραγματικές υλοποιήσεις VPN συνδέσεων εάν αφορούσαν τη διασύνδεση δύο εταιρειών μέσα στο ίδιο κτήριο, ή τη διασύνδεση δύο τμημάτων της ίδιας εταιρείας τα οποία για κάποιο λόγο θέλουν να διατηρήσουν τη σχετική αυτονομία των δικτύων των Η/Υ τους.

Η συνηθέστερη περίπτωση όμως που συμβαίνει στην πραγματικότητα είναι αυτές οι VPN συνδέσεις να πραγματοποιούνται μέσω Διαδικτύου. Σε αυτή την περίπτωση όμως ο VPN χρήστης δεν θα «δει» πρώτα τον R.R.A.S. Server αλλά τον dslmodem/router που διασύνδεει την εταιρεία με το Διαδίκτυο. Σε αυτή τη περίπτωση στο βήμα **5.** της ενότητας **Δ.** και στο βήμα **3.** της ενότητας **Ε.** θα πρέπει να εισαχθεί η στατική και βέβαια δημόσια IP διεύθυνση που μάλλον θα έχει η εταιρεία.

Στην περίπτωση που η εταιρεία δεν έχει δημόσια στατική IP διεύθυνση και θέλει να κάνει χρήση των VPN συνδέσεων τότε θα πρέπει να κάνει χρήση υπηρεσιών δυναμικού DNS που παρέχουν κάποιες εταιρίες, μάλλον, έναντι αμοιβής. Στη περίπτωση αυτή στα προαναφερθέντα βήματα εισάγουμε τα ονόματα που δηλώσαμε στις εταιρείες παροχής υπηρεσιών δυναμικού DNS. (Περισσότερες πληροφορίες για τη χρήση του δυναμικού DNS μπορείτε να βρείτε στην ενότητα **δ** της άσκησης: **Άλλες δικτυακές εφαρμογές** στο site του 4<sup>ου</sup> Ε. Κ. Γ' ΑΘΗΝΑΣ.



Ανεξάρτητα όμως από το είδος της IP διεύθυνσης του dslmodem/router θα πρέπει να επιτρέψουμε και την όδευση των κατάλληλων δικτυακών ports που αφορούν τις VPN συνδέσεις. Ανάλογα με τον dslmodem/router αυτή η δήλωση των οδεύσεων αναφέρεται ως port forwarding ή Virtual Server. Στην εικόνα 44 (κόκκινη αγκύλη) φαίνεται το port forwarding για διάφορα πρωτόκολλα της VPN επικοινωνίας.

The screenshot shows the OTE H108NS router configuration interface. The 'Advanced Setup' tab is active, and the 'Virtual Server' section is expanded. Below the configuration fields, the 'Virtual Server Listing' table is displayed. A red bracket highlights rules 2 through 6, which are related to VPN protocols.

Rule	Application	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	IPCAMERA	ALL	8000	8000	10.67.80.100	8000	8000		
1	DVR	ALL	8011	8011	10.67.80.101	8011	8011		
2	PPTP	ALL	1723	1723	10.67.80.31	1723	1723		
3	L2TP_1	UDP	500	500	10.67.80.31	500	500		
4	L2TP_2	UDP	4500	4500	10.67.80.31	4500	4500		
5	L2TP_3	ALL	1701	1701	10.67.80.31	1701	1701		
6	SSTP	TCP	443	443	10.67.80.31	443	443		
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A		
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A		
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A		

**Εικόνα 44. Port forwarding για πρωτόκολλα VPN επικοινωνίας.**

Πάντως το θέμα της επίτρησης των VPN συνδέσεων είναι λίγο πιο σύνθετο καθώς εμπλέκονται και Πάροχοι Υπηρεσιών Διαδικτύου (ISPs).

Π.χ. από γειτονική σχολική μονάδα καταφέραμε να δημιουργήσουμε VPN σύνδεση με τον δίκτυο 192.168.1.10 δηλώνοντας τη δημόσια στατική IP διεύθυνση του dslmodem/router του 4<sup>ου</sup> Ε.Κ. Γ' ΑΘΗΝΑΣ στα προαναφερθέντα βήματα σύνδεσης.

Όμως αυτό δεν κατέσται δυνατόν από Η/Υ που ως ISP έχει την WIND. Και οι δύο πάροχοι (ΠΣΔ και WIND) όταν ερωτήθηκαν ισχυρίστηκαν ότι δεν παρεμποδίζουν την VPN επικοινωνία.