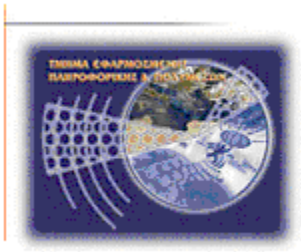
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Προσομοίωση Ασφαλών Δικτυακών Αρχιτεκτονικών με χρήση OPNET

Καραλής Γιάννης (ΑΜ: 1402)
E-mail: karalis.giannis@gmail.com

Ηράκλειο – 23/03/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Υπεύθυνη Δήλωση: *Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Α.Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους γονείς μου για την αμέριστη υποστήριξη κατά την διάρκεια εκπόνησης της εργασίας αυτής.

Θα ήθελα επίσης να ευχαριστήσω τον καθηγητή κ. Μανιφάβα Χαράλαμπο για την πολύτιμη καθοδήγηση και υποστήριξη του σε όλη τη διάρκεια εκπόνησης της εργασίας αυτής, αλλά και την δυνατότητα που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον επιστημονικό αντικείμενο. Ιδιαίτερα όμως θα ήθελα να τον ευχαριστήσω γιατί υπήρξε ο άνθρωπος που με παρότρυνε να συνεχίσω παρ' όλες τις δυσκολίες που αντιμετωπίσαμε, πιστεύοντας στις δυνάμεις και στις δυνατότητες μου.

Περιεχόμενα

Ευχαριστίες ii
Πίνακας εικόνων vii
Chapter 1 Εισαγωγή 1
1.1 Τι είναι το OPNET 1
1.2 Χρήση του OPNET 1
1.3 Εγκατάσταση του OPNET 2
1.4 Περιγραφή των Menus 7
1.4.1 File Menu 8
1.4.2 Edit Menu 9
1.4.3 View Menu 10
1.4.4 Scenarios Menu 11
1.4.5 Topology Menu 12
1.4.6 Protocols Menu 13
1.4.7 Simulation Menu 14
1.4.8 Results Menu 15
1.4.9 Windows Menu 16
1.4.10 Help Menu 17
1.5 Περιγραφή των Security Labs 18
1.5.1 ICMP Pings 18
1.5.2 Subnetting και OSI Model 18
1.5.3 Firewalls 18
1.5.4 RIP 18
1.5.5 OSPF 18
1.5.6 VPN 18
1.5.7 VLAN 18
1.5.8 Dual Homed Router/Host, Security Lab 9: Screened Host/Subnet. DMZ και Security Lab10: Collapsed DMZ 18
Chapter 2 ICMP Ping 18
2.1 Εισαγωγή 18
2.2 Περιγραφή Σεναρίου 18

2.3 Δημιουργία του Σεναρίου 18
2.4 Ρυθμίστε την προσομοίωση 28
2.5 Ανάλυση Αποτελεσμάτων 28
2.6 Ερωτήσεις 29
2.6.1 Ερώτηση 1η 29
2.7 Απαντήσεις 29
2.7.1 Απάντηση 1η 29
2.8 Συμπεράσματα 30
Chapter 3 Firewalls 31
3.1 Εισαγωγή 31
3.2 Network Firewalls (packet filtering) 31
3.3 Proxies (Application Gateways) 31
3.4 Περιγραφή Σεναρίου 32
3.4.1 Δημιουργία του Σεναρίου 32
3.4.2 Δημιουργία του Δεύτερου Σεναρίου 46
3.5 Ανάλυση Αποτελεσμάτων 46
3.6 Ερωτήσεις 48
3.6.1 Ερώτηση 1η 48
3.6.2 Ερώτηση 2η 48
3.6.3 Ερώτηση 3η 48
3.7 Απαντήσεις 49
3.7.1 Απάντηση 1η 49
3.7.2 Απάντηση 2η 50
3.7.3 Απάντηση 3η 51
Chapter 4 VPN 52
4.1 Εισαγωγή 52
4.2 Περιγραφή Σεναρίου 53
4.3 Δημιουργία του Σεναρίου 53
4.4 Δημιουργία του δεύτερου και τρίτου σεναρίου 61
4.5 Ερωτήσεις 62
4.5.1 Ερώτηση 1η 62

4.5.2 Ερώτηση 2η 62
4.5.3 Ερώτηση 3η 63
4.5.4 Ερώτηση 4η 63
4.5.5 Ερώτηση 5η 63
4.6 Απαντήσεις 63
4.6.1 Απάντηση 1η 63
4.6.2 Απάντηση 2η 66
4.6.3 Απάντηση 3η 68
4.6.4 Απάντηση 4η 68
4.6.5 Απάντηση 5η 69
Chapter 5 Firewall and VPN 70
5.1 Σκοπός 70
5.2 Επισκόπηση 70
5.3 Μέθοδος 71
5.3.1 Δημιουργία του νέου Project 71
5.3.2 Δημιουργία και Διαμόρφωση του Δικτύου 72
5.3.3 Διαμόρφωση των Κόμβων 74
5.3.4 Επιλογή των στατιστικών στοιχείων 77
5.4 Το Σενάριο Firewall 79
5.5 Το Σενάριο Firewall_VPN 81
5.5.1 Δημιουργία του Σεναρίου 81
5.5.2 Διαμόρφωση του VPN 83
5.5.3 Πραγματοποιώντας την Προσομοίωση 83
5.5.4 Ανάλυση Αποτελεσμάτων 84
5.6 Περαιτέρω Αναγνώσεις 87
5.7 Ερωτήσεις 87
5.7.1 Ερώτηση 1η 87
5.7.2 Ερώτηση 2η 87
5.7.3 Ερώτηση 3η 87
5.7.4 Ερώτηση 4η 87
Chapter 6 VLAN's 88

6.1 Εισαγωγή ... 88
6.2 Περιγραφή Σεναρίου ... 89
6.3 Δημιουργία του Σεναρίου ... 90
6.4 Δημιουργία του δεύτερου και τρίτου σεναρίου ... 93
6.5 Δημιουργία του δεύτερου σεναρίου ... 99
6.6 Ερωτήσεις ... 103
6.6.1 Ερώτηση 1η ... 103
6.6.2 Ερώτηση 2η ... 103
6.7 Απαντήσεις ... 105
6.7.1 Απάντηση 1η ... 105
6.7.2 Απάντηση 2η ... 105
Chapter 7 Screened Host / Subnet (DMZ) ... 108
7.1 Γενικά για το Screened Host ... 108
7.2 Γενικά για το Screened Subnet (DMZ) ... 108
7.3 Περιγραφή Σεναρίου ... 109
7.4 Δημιουργία του Σεναρίου ... 109
7.5 Ρυθμίστε την προσομοίωση ... 122
7.6 Δημιουργία του Δεύτερου Σεναρίου ... 123
7.7 Ερωτήσεις ... 126
7.7.1 Ερώτηση 1η ... 126
7.7.2 Ερώτηση 2η ... 126
7.7.3 Ερώτηση 3η ... 126
7.7.4 Ερώτηση 4η ... 126
7.8 Απαντήσεις ... 127
7.8.1 Απάντηση 1η ... 127
7.8.2 Απάντηση 2η ... 127
7.8.3 Απάντηση 3η ... 128
7.8.4 Απάντηση 4η ... 128
Chapter 8 Βιβλιογραφία/Αναφορές ... 130
8.1 Παράθεση χρήσιμων πληροφοριών ... 130

Πίνακας εικόνων

Εικόνα 1-1 Registry Form 1
Εικόνα 1-2 Confirmation E-mail 1
Εικόνα 1-3 Log in the Opnet Server 1
Εικόνα 1-4 Saving the executable file on the local disk 1
Εικόνα 1-5 Downloading the Load Files and Load Manuals 1
Εικόνα 1-6 Starting the Program using the start bar 1
Εικόνα 1-7 License Manager 1
Εικόνα 1-8 License Transaction (step 1) 1
Εικόνα 1-9 License Transaction (step 2) 1
Εικόνα 1-10 File Menu 1
Εικόνα 1-11 Edit Menu 1
Εικόνα 1-12 View Menu 1
Εικόνα 1-13 Scenarios Menu 1
Εικόνα 1-14 Topology Menu 1
Εικόνα 1-15 Protocols Menu 1
Εικόνα 1-16 Simulation Menu 1
Εικόνα 1-17 Results Menu 1
Εικόνα 1-18 Windows Menu 1
Εικόνα 1-19 Help Menu 1
Εικόνα 2-1 Create the Project 18
Εικόνα 2-2 Project And Scenario Name 18
Εικόνα 2-3 Topology of Our Network 18
Εικόνα 2-4 Network Scale 18
Εικόνα 2-5 Select The Ring Configuration 18
Εικόνα 2-6 Parameters of The Ring 18
Εικόνα 2-7 Select Model List 18
Εικόνα 2-8 Workstation of Our Network 18
Εικόνα 2-9 Attributes Of node_5 18
Εικόνα 2-10 Select the Wires 18
Εικόνα 2-11 Select the IP Attribute Config 18
Εικόνα 2-12 The Scenario is completed 18
Εικόνα 2-13 Ping Report 18
Εικόνα 2-14 Ping Report for the scenario WithFailure 18
Εικόνα 3-1 The scenario 18
Εικόνα 3-2 Components list 18
Εικόνα 3-3 Application Config Attributes 18
Εικόνα 3-4 Configuring the application traffic 18
Εικόνα 3-5 Configuring the application traffic 18

Εικόνα 3-6 Configuring Profile Config 18
Εικόνα 3-7 Configuring the Firewall 18
Εικόνα 3-8 MusicAndVideoServer supported Services 18
Εικόνα 3-9 Supported Services 18
Εικόνα 3-10 Assigning profiles to workstations at LAN 1 18
Εικόνα 3-11 Internet-Firewall link statistics 18
Εικόνα 3-12 Global statics 18
Εικόνα 3-13 Manage Scenarios 18
Εικόνα 3-14 Compare Results 18
Εικόνα 3-15 Average DB Query Response Time 18
Εικόνα 3-16 Average point-to-point throughput of the link 18
Εικόνα 3-17 Average utilization of the link 18
Εικόνα 4-1 Με την πηγή Tunnel στο FEP 1
Εικόνα 4-2 Με την πηγή Tunnel στο PPP Client 1
Εικόνα 4-3 The Map 1
Εικόνα 4-4 Components of the network 1
Εικόνα 4-5 The scenario 1
Εικόνα 4-6 Application Definitions: Default 1
Εικόνα 4-7 Application Definitions: Default 1
Εικόνα 4-8 Applications supported by Multiservice Server 1
Εικόνα 4-9 Servers Profiles 1
Εικόνα 4-10 Selecting the profiles for stations 2,5 and 10 1
Εικόνα 4-11 Setting up the Firewall 1
Εικόνα 4-12 Configuring the VPNs on the control IP VPN Config 1
Εικόνα 4-13 Successful database queries 1
Εικόνα 4-14 Simulation Log for VPNVoluntary 1
Εικόνα 4-15 Simulation Log for VPNCompulsory 1
Εικόνα 4-16 Simulation Log for NoVPN 1
Εικόνα 4-17 Ping traces at NoVPN 1
Εικόνα 4-18 Ping response times 1
Εικόνα 5-1 Create The Project 1
Εικόνα 5-2 Project And Scenario Name 1
Εικόνα 5-3 Topology Of Our Network 1
Εικόνα 5-4 Choose Border Map 1
Εικόνα 5-5 Object Palette 1
Εικόνα 5-6 Our Network 1
Εικόνα 5-7 Applications Attributes 1
Εικόνα 5-8 Profiles Attributes 1
Εικόνα 5-9 Server Attributes 1
Εικόνα 5-10 Sales A Attributes 1

Εικόνα 5-11 Choose Results 1
Εικόνα 5-12 Choose Results (Sales A) 1
Εικόνα 5-13 Choose Results (Sales B) 1
Εικόνα 5-14 Duplicate the old and 1
Εικόνα 5-15 Sales C Attributes 1
Εικόνα 5-16 Scenario VPN Firewall 1
Εικόνα 5-17 Scenario Firewall_VPN 1
Εικόνα 5-18 Our New Scenario 1
Εικόνα 5-19 VPN Attributes 1
Εικόνα 5-20 Manage Scenarios 1
Εικόνα 5-21 Compare Results 1
Εικόνα 5-22 Sales A Graphs 1
Εικόνα 5-23 Sales B Graphs 1
Εικόνα 5-24 Sales A Graphs 1
Εικόνα 5-25 Sales B Graphs 1
Εικόνα 6-1 Tagged Packet 1
Εικόνα 6-2 Distributing stations into groups 1
Εικόνα 6-3 Components of our network 1
Εικόνα 6-4 The scenario once completed 1
Εικόνα 6-5 Creating Pings 1
Εικόνα 6-6 Changing the Scheme of Switches 1
Εικόνα 6-7 Finding out the link interfaces 1
Εικόνα 6-8 Switches' Attributes 1
Εικόνα 6-9 Adding Supported VLANs in a switch 1
Εικόνα 6-10 VLANs supported by this Lab's switches 1
Εικόνα 6-11 Configuring the Lab's switches 1
Εικόνα 6-12 Changing any component to an ethernet_one_armed_router 1
Εικόνα 6-13 The new OneArmedRouter 1
Εικόνα 6-14 IP Addresses of all workstations 1
Εικόνα 6-15 Setting the OneArmedRouter subinterfaces 1
Εικόνα 6-16 Station IP Addresses 1
Εικόνα 6-17 VLAN Configuration 1
Εικόνα 6-18 Traffic Load Reduction because of VANs 1
Εικόνα 7-1 Screened Host 1
Εικόνα 7-2 Screened Subnet (DMZ) 1
Εικόνα 7-3 Components of our network 1
Εικόνα 7-4 The completed scenario 1
Εικόνα 7-5 Networks in the scenario 1
Εικόνα 7-6 Addresses for the network 1
Εικόνα 7-7 Configuring the Proxy subinterfaces 1

Εικόνα 7-8 HTTP Profile 1
Εικόνα 7-9 FTTP Profile 1
Εικόνα 7-10 HTTP Profile 1
Εικόνα 7-11 Services supported by servers 1
Εικόνα 7-12 Station's profiles 1
Εικόνα 7-13 Server Address of the servers 1
Εικόνα 7-14 Application Demands 1
Εικόνα 7-15 Static Routing Table of the Proxy 1
Εικόνα 7-16 Configuring the Proxy 1
Εικόνα 7-17 Static Routing Table at Internal Router 1
Εικόνα 7-18 Internal Router ACL 1
Εικόνα 7-19 VLAN Identifiers 1
Εικόνα 7-20 Configuring VLAN at Switch 2 1
Εικόνα 7-21 The scenario ScreenedSubnetWithDMZ 1
Εικόνα 7-22 New IP addresses 1
Εικόνα 7-23 ACL of Internal Router # 2 1
Εικόνα 7-24 Adding up new conditions to the ACL 1
Εικόνα 7-25 Ping 1
Εικόνα 7-26 It is not possible to avoid the Proxy 1
Εικόνα 7-27 The ACL helps to reduce the load on the Proxy 1
Εικόνα 7-28 Internal attacks can be avoided only with DMZ 1

Chapter 1 Εισαγωγή

1.1 Τι είναι το OPNET

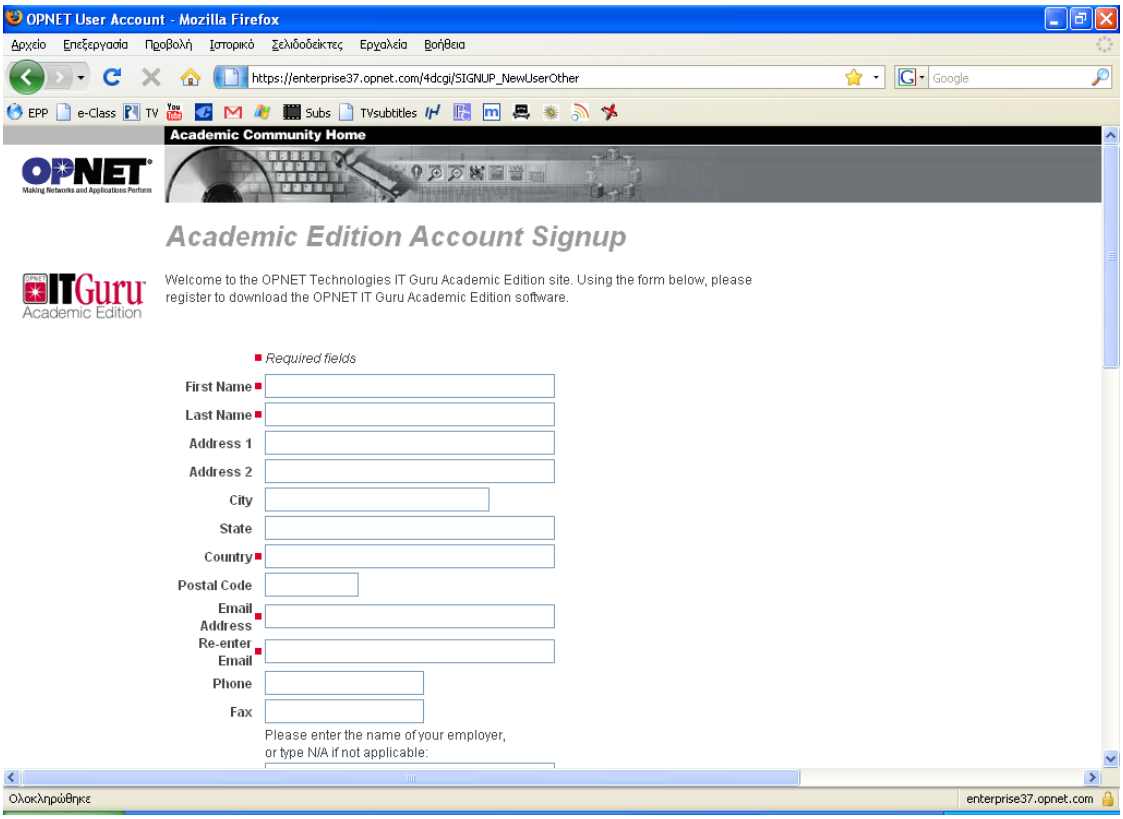
Το OPNET είναι μια ευρέως γνωστή εμπορική εφαρμογή, με κύρια χρήση της τη προσομοίωση δικτύων. Στη συγκεκριμένη πτυχιακή θα χρησιμοποιήσουμε την έκδοση IT GURU Academic Edition. Η συγκεκριμένη έκδοση του OPNET αποτελεί ένα εξειδικευμένο ακαδημαϊκό εργαλείο στο χώρο των επικοινωνιών, που προσφέρει τη δυνατότητα με τη βοήθεια ενός γραφικού περιβάλλοντος να μοντελοποιηθούν και να προσομοιωθούν διάφορα είδη δικτύων.
Το OPNET παρέχει δυνατότητες για δημιουργία πληρέστατων και μεγάλων δικτύων σχεδιασμένων μέχρι τη παραμικρή λεπτομέρεια, τα οποία μπορούμε να τα «στήσουμε» σχετικά εύκολα, να τα δοκιμάσουμε με χρήση πολλών σύγχρονων τεχνολογιών και να τα βελτιστοποιήσουμε γενικότερα.

1.2 Χρήση του OPNET

Αν και το OPNET σε διάφορες εκδόσεις του σαν ισχυρός προσομοιωτής δίνει τη δυνατότητα στο χρήστη να διαλέξει το είδος της δομής του δικτύου στο οποίο θα δουλέψει το πιο διαδεδομένο μοντέλο είναι αυτό των δικτύων το οποίο θα χρησιμοποιηθεί και στο εργαστήριο. Το μοντέλο κόμβων και το μοντέλο επεξεργασίας συμπληρώνουν τη βασική τριάδα των προαναφερθέντων ειδών αλλά επικεντρώνονται περισσότερο στη μοντελοποίηση εσωτερικών χαρακτηριστικών και λειτουργιών όπως δημιουργία δεδομένων, αποθήκευση κ.τ.λ. ή διαγράμματα πεπερασμένων καταστάσεων (finite state machines - FSMs) που ελέγχουν την εσωτερική λειτουργικότητα των αντικειμένων στο μοντέλο κόμβων. Σε κάθε περίπτωση θα πρέπει να γίνει κατανοητό ότι το OPNET λόγω της ευρείας γκάμας τεχνολογιών και δικτύων που ειδικεύεται παρέχει προηγμένες δυνατότητες στο χρήστη αλλά και θέτει ένα υψηλό επίπεδο «δυσκολίας» στο οποίο ο σπουδαστής αντεπεξέρχεται ευκολότερα εάν καταλάβει κάποιες βασικές λειτουργίες του που εξηγούνται παρακάτω και ακολουθεί κατά γράμμα τις υποδείξεις των ασκήσεων.
Επίσης να αναφέρω ότι από την εξουσιοδοτημένη σελίδα του OPNET μπορούμε να πάρουμε κάποιες σημαντικές πληροφορίες όσον αφορά τα security labs και διάφορες άλλες πληροφορίες που θέλουμε για το πρόγραμμα και των συστατικών, από το παρακάτω Link:
http://www.opnet.com/university_program/teaching_with_opnet/textbooks_and_materials/index.html

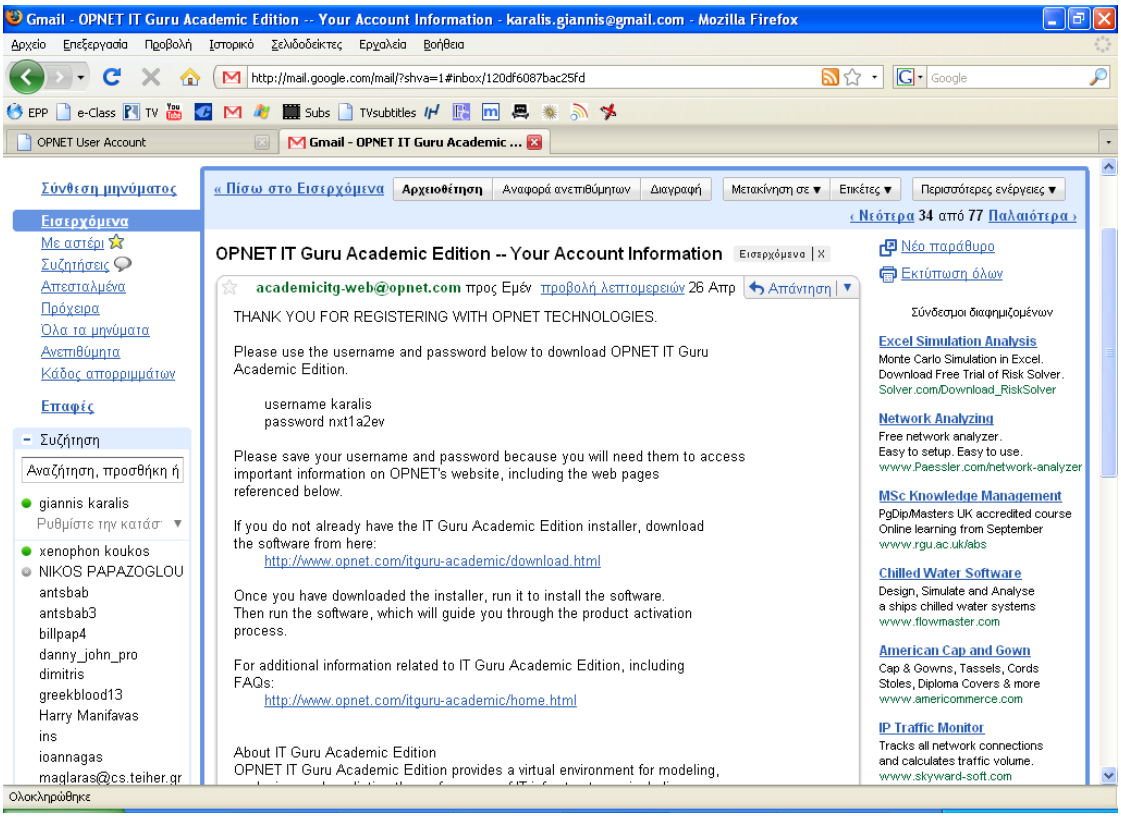
1.3 Εγκατάσταση του OPNET

Το πρώτο βήμα για να αποκτήσετε το OPNET είναι να μεταβείτε στην εξουσιοδοτημένη σελίδα: www.opnet.com και έπειτα να δημιουργήσετε ένα λογαριασμό εδώ: https://enterprise37.opnet.com/4dcgi/SIGNUP_NewUserOther, για να μπορέσετε να αποκτήσετε το πρόγραμμα.



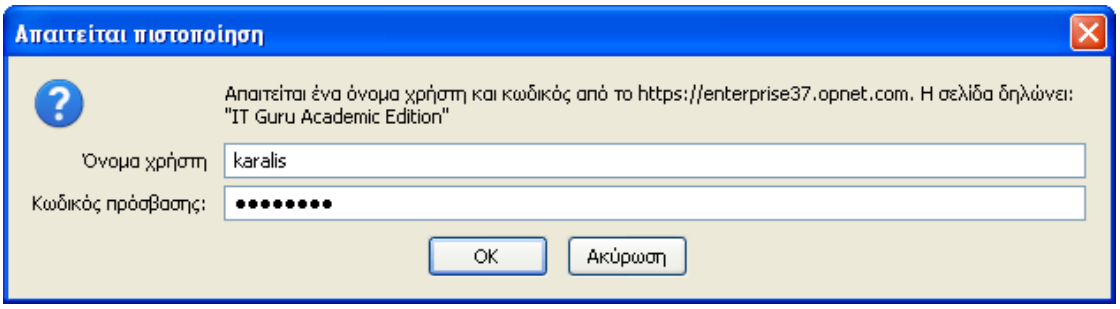
Εικόνα 1-1 Registry Form

Θυμηθείτε ότι μπορείτε να δημιουργήσετε μόνο έναν λογαριασμό για να αποκτήσετε πρόσβαση στο OPNET IT Guru Academic Edition. Παρ' όλα αυτά εάν θέλετε να εγκαταστήσετε το πρόγραμμα σε περισσότερους υπολογιστές θα πρέπει να χρησιμοποιήσετε διαφορετικά e-mail κάθε φορά για να κάνετε register και να αποκτήσετε τον κωδικό πρόσβασης.
Μετά από μερικά λεπτά θα λάβετε ένα e-mail που θα επιβεβαιώνει ότι ο λογαριασμός σας δημιουργήθηκε επιτυχώς καθώς επίσης και τον κωδικό πρόσβασης.



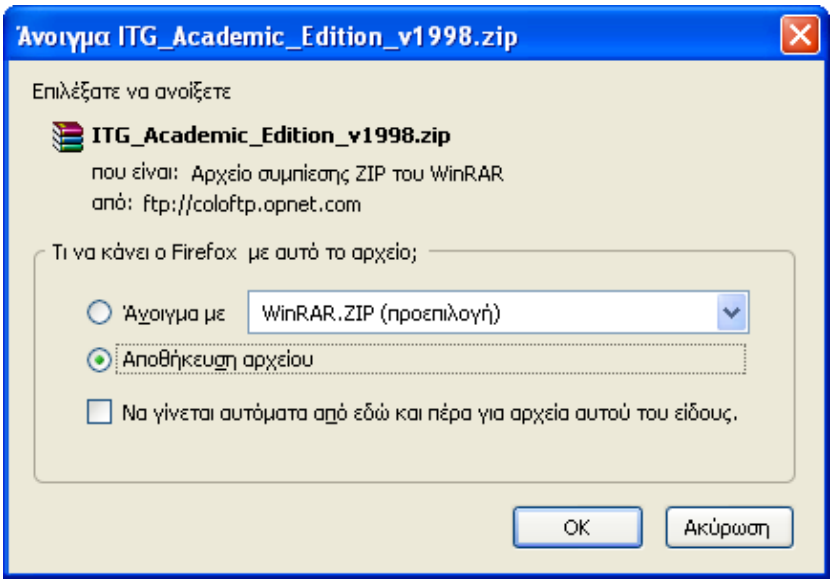
Εικόνα 1-2 Confirmation E-mail

Τώρα κάντε κλικ στο hyperlink: http://www.opnet.com/itguru-academic/download.html που εμφανίζεται στο main page του e-mail. Αυτό θα σας οδηγήσει σε ένα νέο web site όπου μπορείτε να κάνετε login, πληκτρολογώντας το όνομα χρήστη που δηλώσατε και τον κωδικό πρόσβασης που αποκτήσατε προηγουμένως:



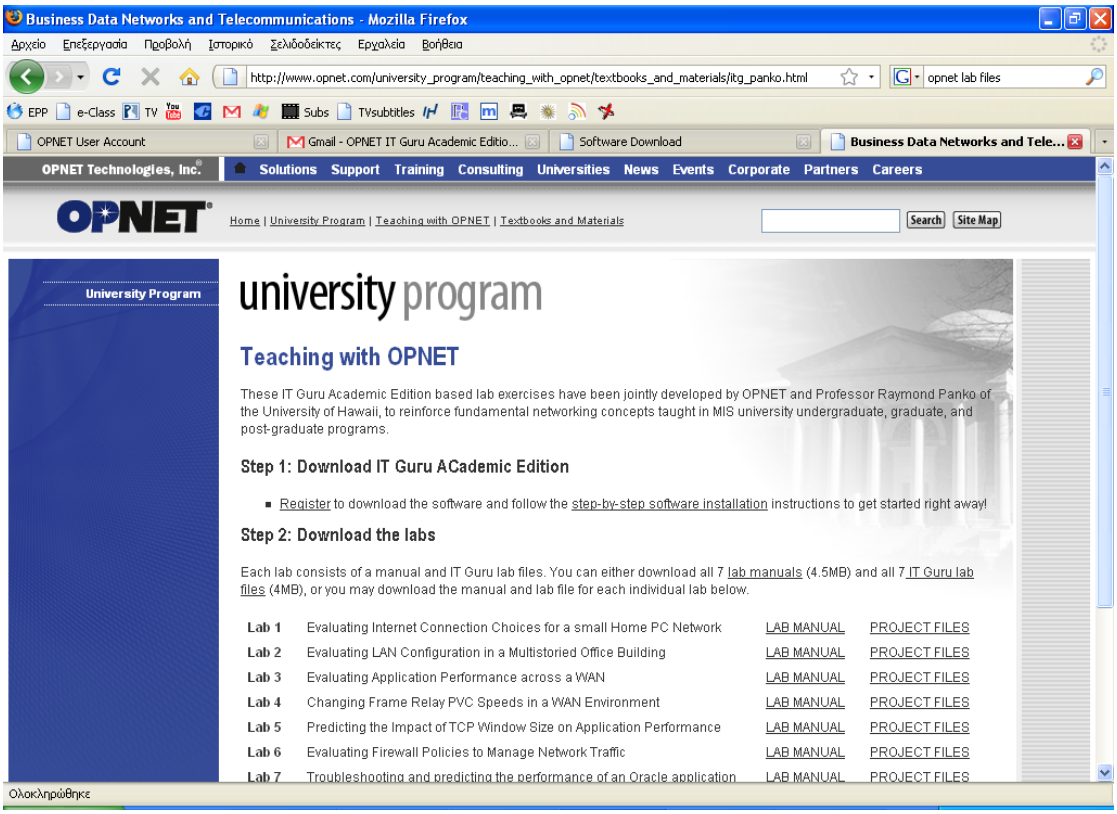
Εικόνα 1-3 Log in the Opnet Server

Μετά από αυτό μπορείτε να "κατεβάσετε" το πρόγραμμα, επιλέγοντας το λογισμικό που χρησιμοποιείτε στον υπολογιστή σας. Το πρόγραμμα είναι περίπου 47 MB και πρέπει να είστε σε Administrator Mode για να το κάνετε εγκατάσταση.



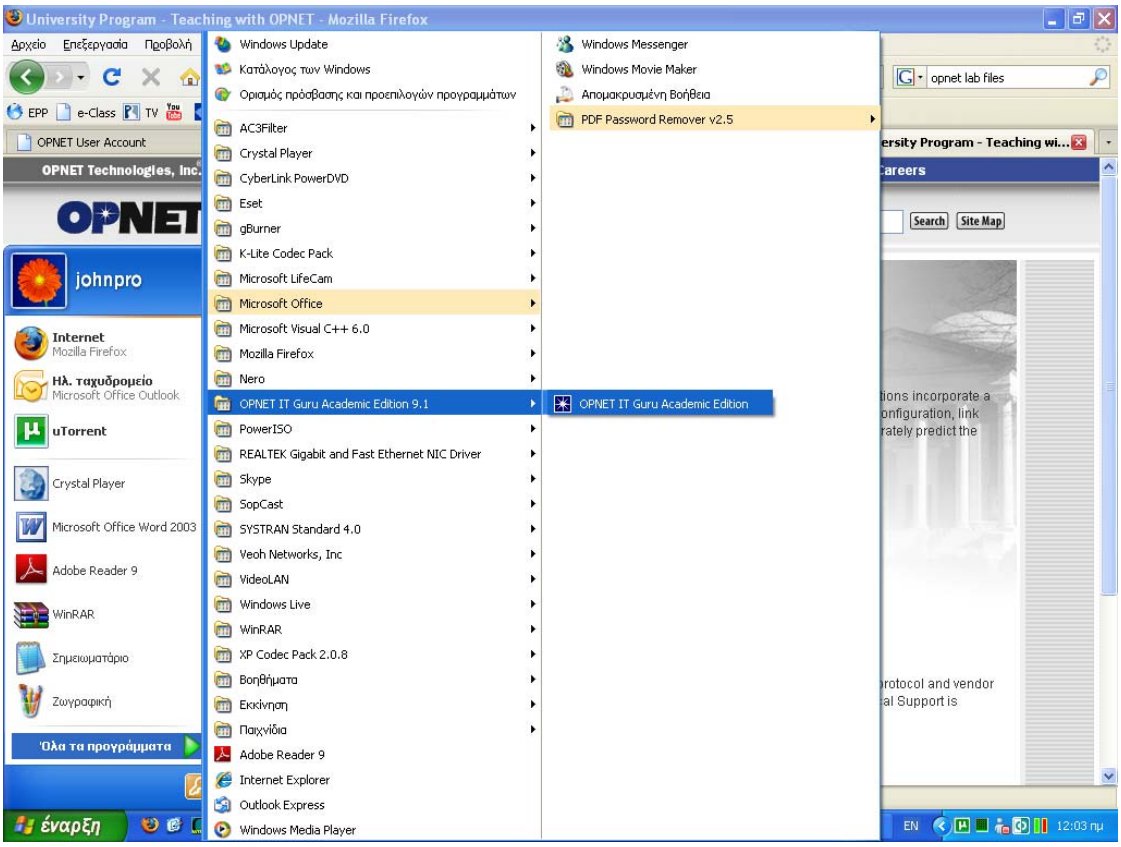
Εικόνα 1-4 Saving the executable file on the local disk

Το δεύτερο βήμα είναι να "κατεβάσετε" τα Lab Manuals και τα Lab Files κάνοντας κλικ στο παρακάτω link: http://www.opnet.com/university_program/teaching_with_opnet/textbooks_and_materials/itg_panko.html



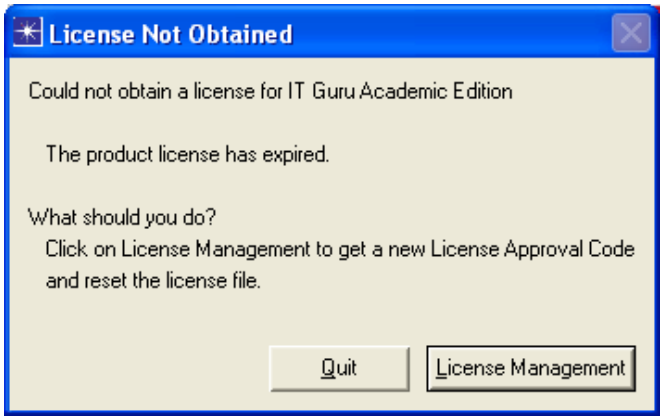
Εικόνα 1-5 Downloading the Load Files and Load Manuals

Μπορείτε επίσης να "κατεβάσετε" όλα Lab Manuals καθώς και όλα τα IT Guru Lab Files την ίδια στιγμή σε 2 διαφορετικά συμπιεσμένα αρχεία.
Μόλις ολοκληρωθεί το "κατέβασμα" του installer, μπορείτε να το εκτελέσετε και να ακολουθήσετε τα παρακάτω βήματα για να ξεκινήσετε την εγκατάσταση.



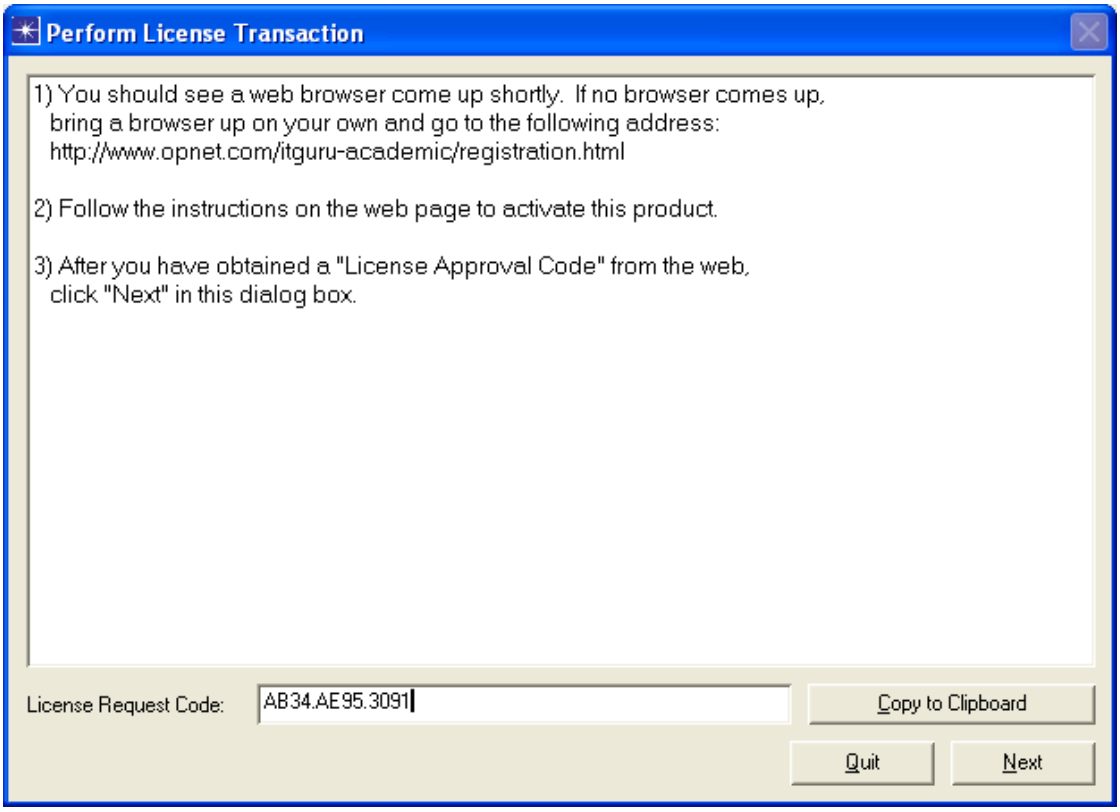
Εικόνα 1-6 Starting the Program using the start bar

Εκτελούμε το πρόγραμμα και μετά κάνουμε κλικ στο "License Manager".



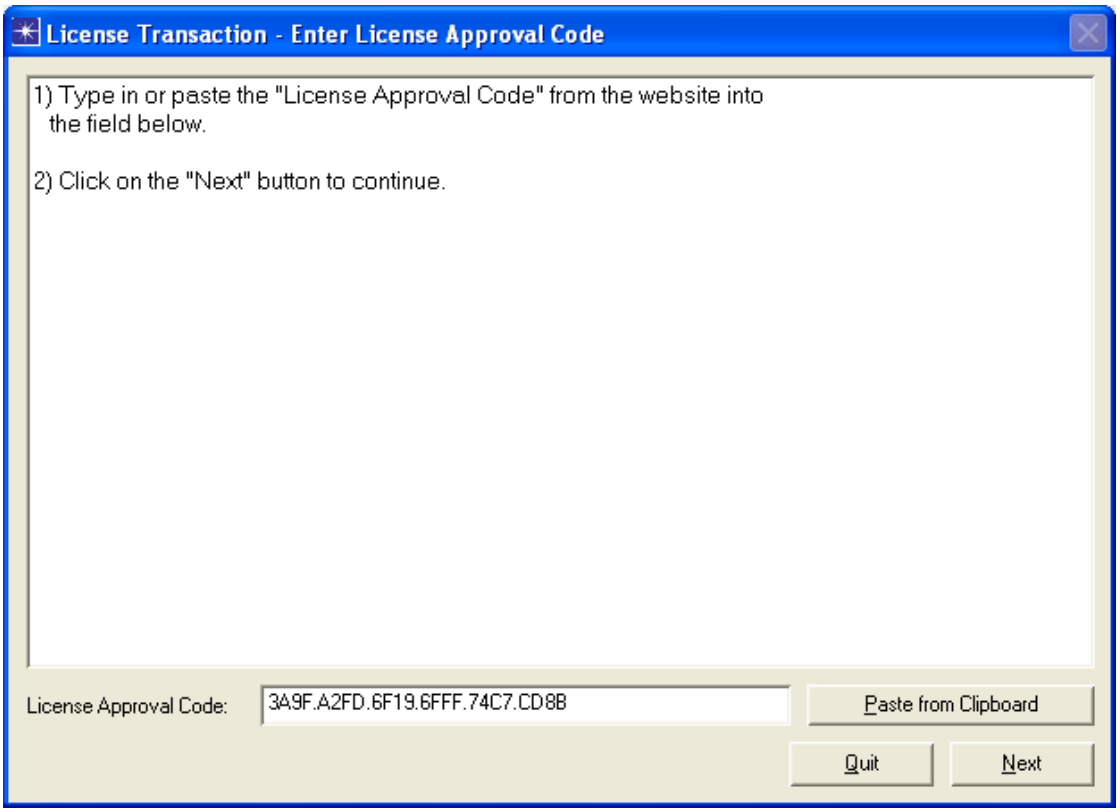
Εικόνα 1-7 License Manager

Μετά από αυτό το παράθυρο διαλόγου θα εμφανιστεί ένα νέο. Κάνουμε κλικ στο “Next” και κατόπιν εμφανίζεται ακόμα ένα παράθυρο διαλόγου όμοιο με το παρακάτω:



Εικόνα 1-8 License Transaction (step 1)

Τώρα εκτελούμε την εφαρμογή License Transaction προκειμένου να μας γνωστοποιήσει ως χρήστες Opnet. Πρέπει να σημειώσετε το License Request Code (ή να κάνετε κλικ στο “Copy to Clipboard” και στην συνέχεια να κάνετε κλικ στο “Next”). Είναι πολύ σημαντικό να έχετε ήδη το License Request Code προτού ζητήσετε το License Activation Code. Κάθε φορά που θα ανοίγετε το Opnet και δεν θα έχετε κάνει “activate” θα σας εμφανίζεται ένα νέο “License Request Code” παράθυρο διαλόγου.



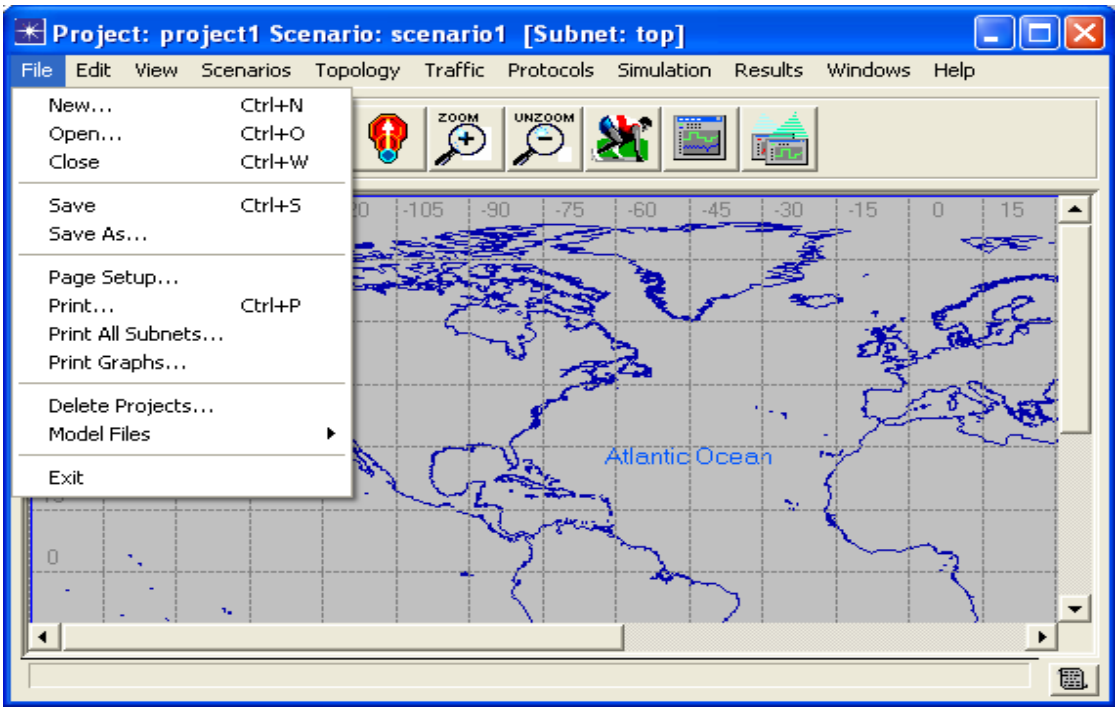
Εικόνα 1-9 License Transaction (step 2)

Τώρα μπορούμε να εκτελέσουμε το OPNET IT Guru Academic Edition 9.1!

1.4 Περιγραφή των Menus

Παρακάτω ακολουθεί μια συνοπτική περιγραφή των διαφόρων Menus του OPNET. Κάποιες από τις επιλογές των Menus που αναφέρονται είναι πασίγνωστες ή η χρήση τους συμπεραίνεται εύκολα, κάποιων άλλων όμως η επεξήγηση πιθανότατα θα φανεί χρήσιμη καθώς θα χρησιμοποιηθούν επανειλημμένα στις εργαστηριακές ασκήσεις.

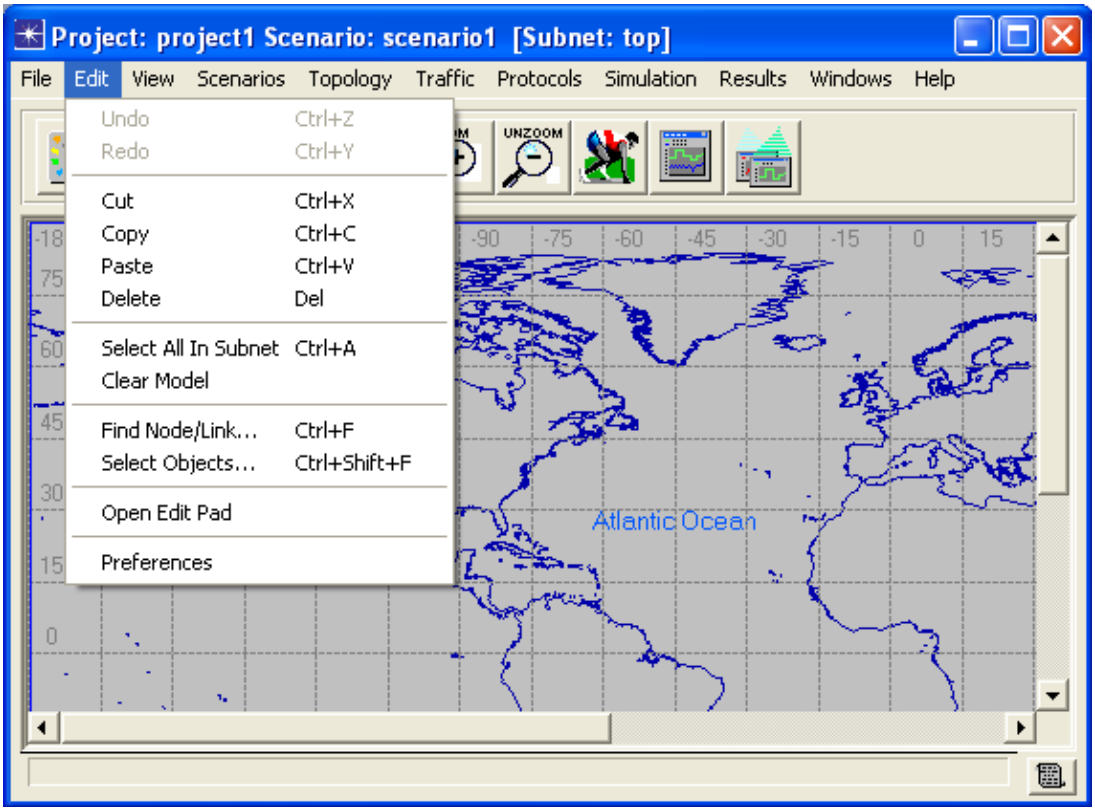
1.4.1 File Menu



Εικόνα 1-10 File Menu

New: Σβήνει τον προηγούμενο χώρο εργασίας και δημιουργεί ένα νέο για την δημιουργία του μοντέλου.
Open: Ανοίγει ένα υπάρχον μοντέλο.
Close: Κλείνει το τρέχον μοντέλο.
Save: Αποθηκεύει το υπάρχον μοντέλο.
Save as: Αποθηκεύει το υπάρχον μοντέλο με το όνομα που καθορίζει ο χρήστης
Page Setup: Ρυθμίσεις απεικόνισης του χώρου εργασίας για εκτύπωση/εμφάνιση ως .pdf κλπ.
Print: Εκτύπωση του δικτυακού μας μοντέλου.
Print All Subnets: Εκτύπωση όλων των υποδικτύων.
Print Graphs: Εκτύπωση των γραφικών.
Delete Projects: Διαγράφει όποιο έτοιμο project επιλεγεί.
Model Files: Διαγράφει/προσθέτει/ανανεώνει έτοιμα μοντέλα.
Exit: Έξοδος από το OPNET.

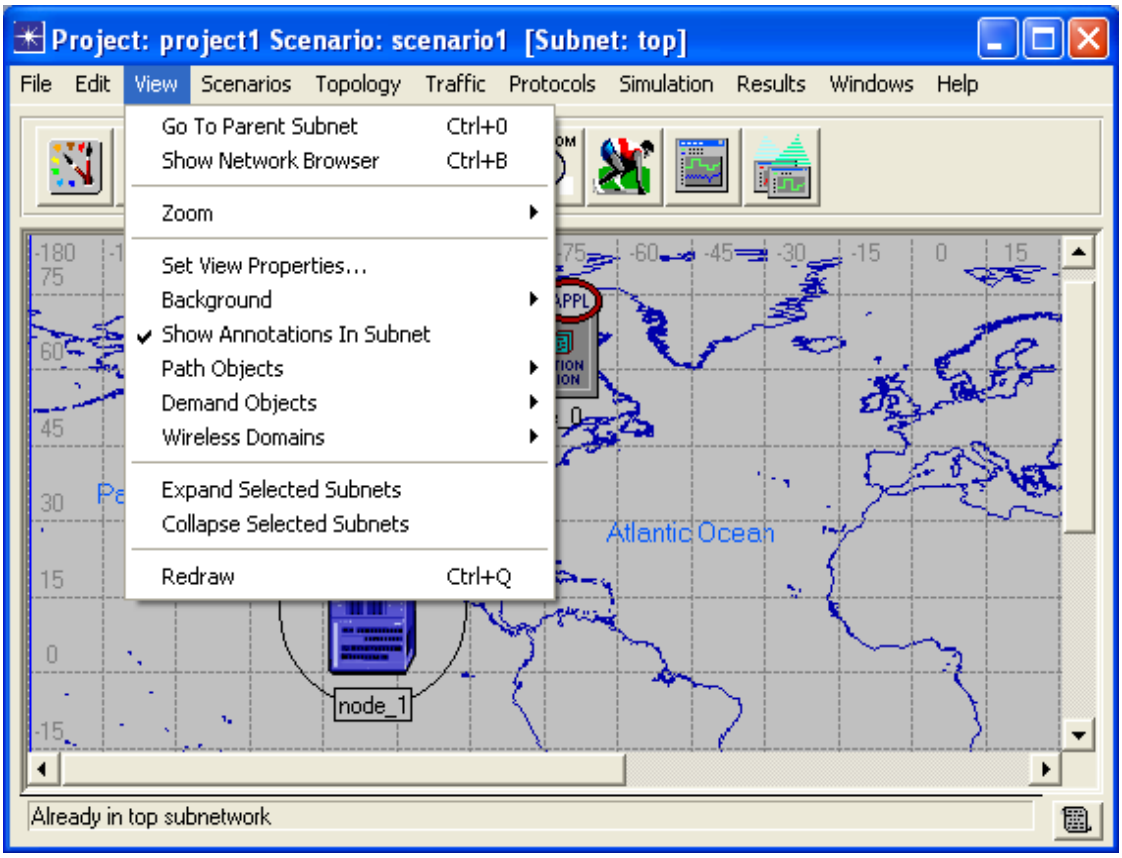
1.4.2 Edit Menu



Εικόνα 1-11 Edit Menu

Undo: Χρησιμεύει στη περίπτωση που θέλουμε να γυρίσουμε πίσω στη κατάσταση πριν τη τελευταία ενέργεια που κάναμε.
Redo: Όταν επιλεγεί μετά από Undo, το αναιρεί και μας γυρίζει στη προηγούμενη κατάσταση πριν το Undo.
Cut: Σβήνει το επιλεγμένο αντικείμενο και το τοποθετεί στο clipboard.
Copy: Αντιγράφει το επιλεγμένο αντικείμενο και το τοποθετεί στο clipboard.
Paste: Τοποθετεί το αντικείμενο που είναι στο clipboard στον χώρο εργασίας.
Delete: Διαγραφή του επιλεγμένου αντικειμένου.
Select All in Subnet: Μεταφέρει τα επιλεγμένα αντικείμενα σε ένα υποδίκτυο.
Clear Model: Διαγράφει όλα τα αντικείμενα του τρέχοντος δικτύου και «καθαρίζει» την οθόνη.
Find Node/Link: Εύρεση αντικειμένου.
Select Objects: Επιλέγει ανά κριτήρια συγκεκριμένα αντικείμενα του τρέχοντος δικτύου.
Open Edit Pad: Ανοίγει το Edit Pad του OPNET.
Preferences: Με την επιλογή αυτή μας δίνεται η δυνατότητα να αλλάξουμε διάφορες παραμέτρους συγκεκριμένων «στοιχείων».

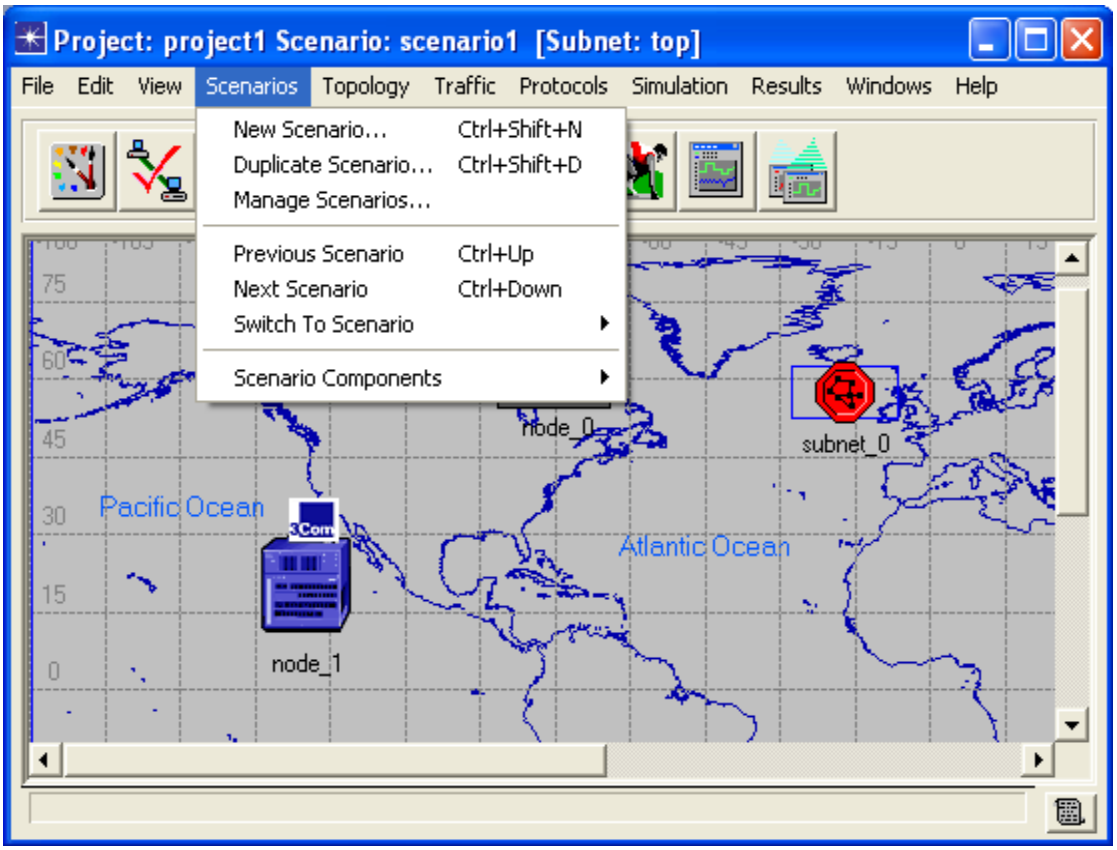
1.4.3 View Menu



Εικόνα 1-12 View Menu

Go To Parent Subnet: Εάν έχουμε υποδίκτυα, μας οδηγεί στο «κεντρικό».
Show Network Browser: Βλέπουμε όλα τα στοιχεία του γραφικού περιβάλλοντος σε μορφή Browser.
Zoom: Κεντράρει/Ζουμάρει με διάφορες επιλογές
Set View Properties: Ρυθμίσεις για την εμφάνιση του γραφικού περιβάλλοντος (αποστάσεις κλπ)
Background: Επιλογή χαρτών για το background
Show Annotations in Subnet: Αφορά την εμφάνιση συγκεκριμένων στοιχείων όταν έχουμε υποδίκτυο.
Path Objects: Εμφανίζει ή αποκρύπτει τα Path Objects στον Editor του OPNET.
Demand Objects: Αντίστοιχα με Path Objects.
Wireless Domains: Αντίστοιχα με Path/Demand Objects αλλά για ασύρματη επικοινωνία.
Expand Selected Subnets: Επεκτείνει τα επιλεγμένα υποδίκτυα
Collapse Selected Subnets: Ακριβώς το αντίθετο με το από πάνω.
Redraw: «Ανανέωση» της απεικόνισης του γραφικού περιβάλλοντος.

1.4.4 Scenarios Menu



Εικόνα 1-13 Scenarios Menu

Τα Scenarios είναι έτοιμα projects/δίκτυα, διάφορα «σενάρια» δηλαδή φτιαγμένα από τους τεχνικούς του προγράμματος προς βοήθεια και παρατήρηση των χρηστών του OPNET. Το OPNET διαθέτει μεγάλη ποικιλία τέτοιων σεναρίων που εξαντλούν σχεδόν κάθε δομή και τεχνολογία δικτύου. (ενσύρματο/ασύρματο, υποδίκτυο ή μη κ.τ.λ.) Επίσης και ο χρήστης έχει τη δυνατότητα να δημιουργήσει ένα δικό του σενάριο.

New Scenario: Δημιουργία νέου σεναρίου. Ο χρήστης μπορεί να το δημιουργήσει εξολοκλήρου μόνος του.

Duplicate Scenario: «Αντιγραφή» σεναρίου.

Manages Scenarios: Διαχείριση σεναρίων.

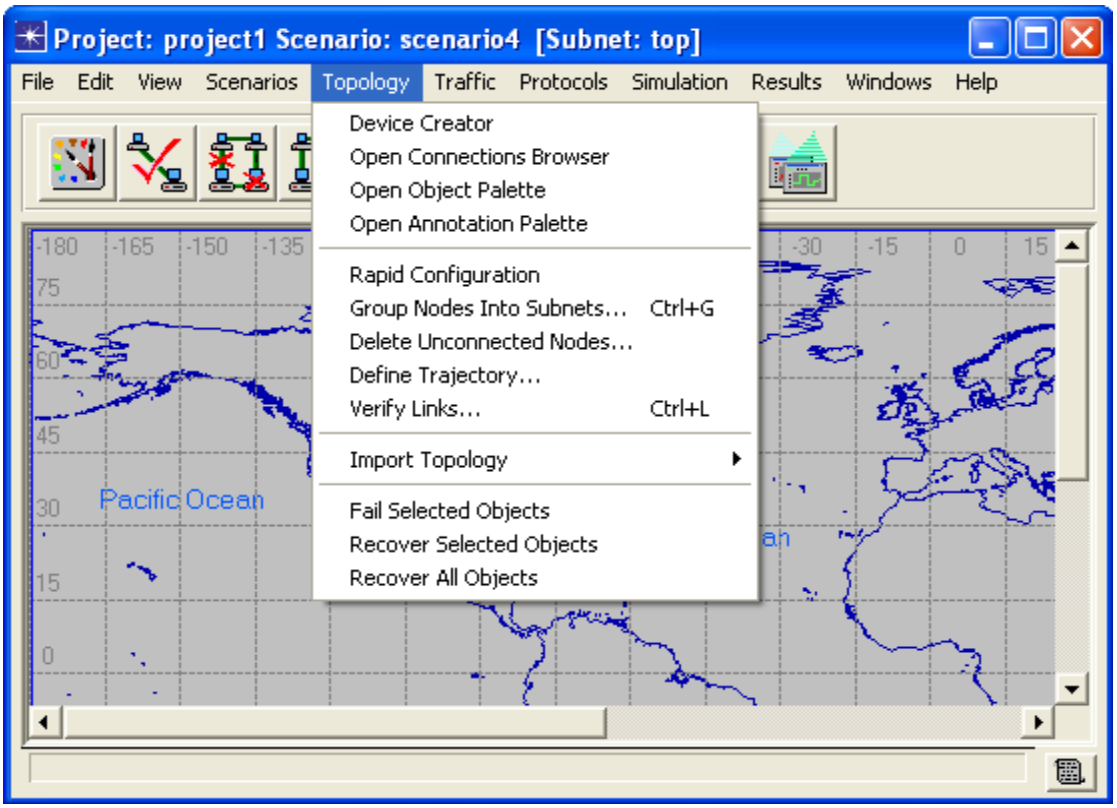
Previous Scenario: Μετάβαση στο προηγούμενο σενάριο.

Next Scenario: Μετάβαση στο επόμενο σενάριο.

Switch to Scenario: Επιλογή σεναρίου ενώ περισσότερα από ένα «τρέχουν»

Scenario Components: Εισαγωγή ή εξαγωγή στοιχείων από ένα σενάριο.

1.4.5 Topology Menu



Εικόνα 1-14 Topology Menu

Device Creator: Επιλογή και ρύθμιση διάφορων εφαρμογών (LAN Models/ Routers κ.τ.λ.)

Open Connections Browser: Ανοίγει νέος Browser μέσω του οποίου μπορούμε να διαχειριστούμε ανά είδος στοιχεία και συνδέσεις. (destination/source nodes κ.τ.λ.)

Open Object Palette: Ανοίγει τη παλέτα αντικειμένων του OPNET η οποία έχει περιγραφτεί παραπάνω.

Rapid Configuration: Επιλογή για διάφορες ρυθμίσεις μέσα στο δίκτυο.

Group Nodes Into Subnets: Ομαδοποίηση υπολογιστών/μηχανημάτων μέσα σε υποδίκτυο.

Delete Unconnected Nodes: Με την επιλογή διαγράφουμε όλους τους «υπολογιστές» που δεν είναι συνδεμένοι κάπου μέσα στο δίκτυο. Εάν το πρόγραμμα δεν βρει nodes που να μην είναι συνδεμένα εμφανίζει warning.

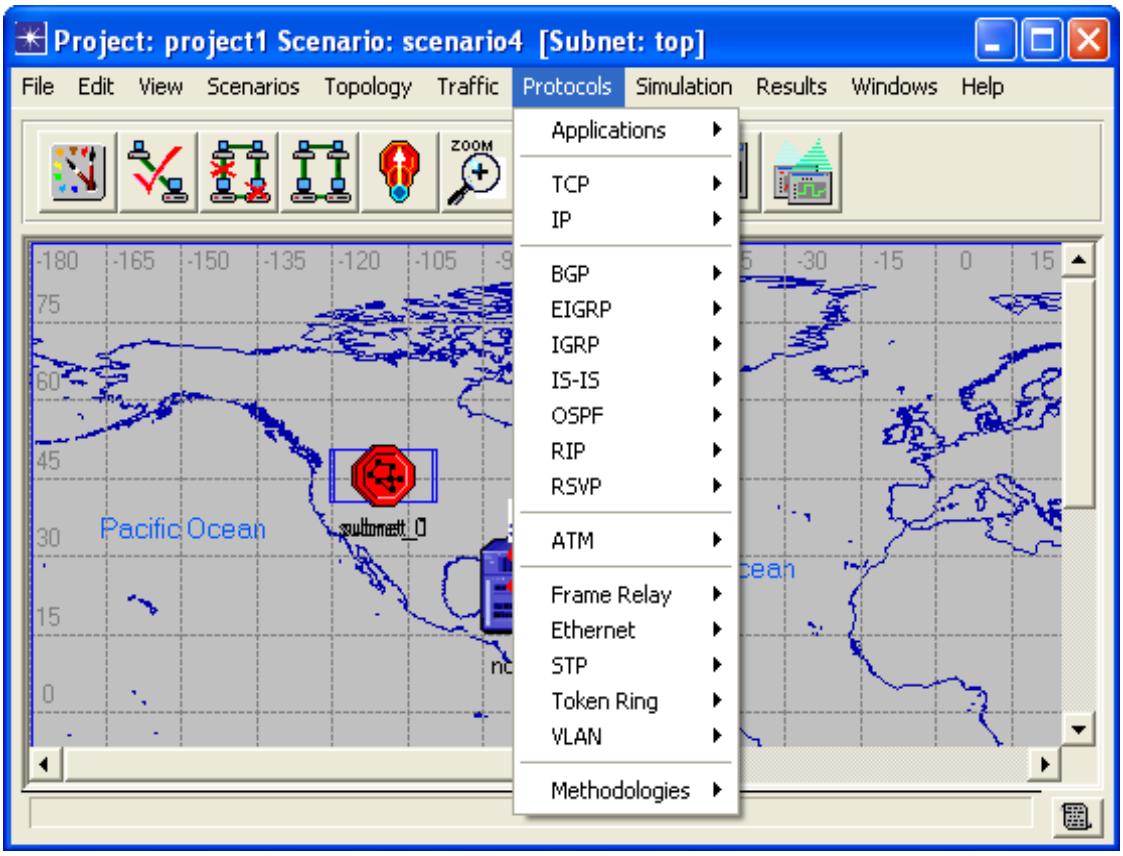
Verify Links: Επιλογή έλεγχο των διαφόρων συνδέσεων του δικτύου.

Fail Selected Objects: Με αυτή την επιλογή θέτουμε εκτός λειτουργίας τυχόν επιλεγμένο αντικείμενο.

Recover Selected Objects: Επαναφορά αντικειμένου που έχει τεθεί εκτός λειτουργίας.

Recover All Objects: Επαναφορά όλων των αντικειμένων που έχουν τεθεί εκτός λειτουργίας.

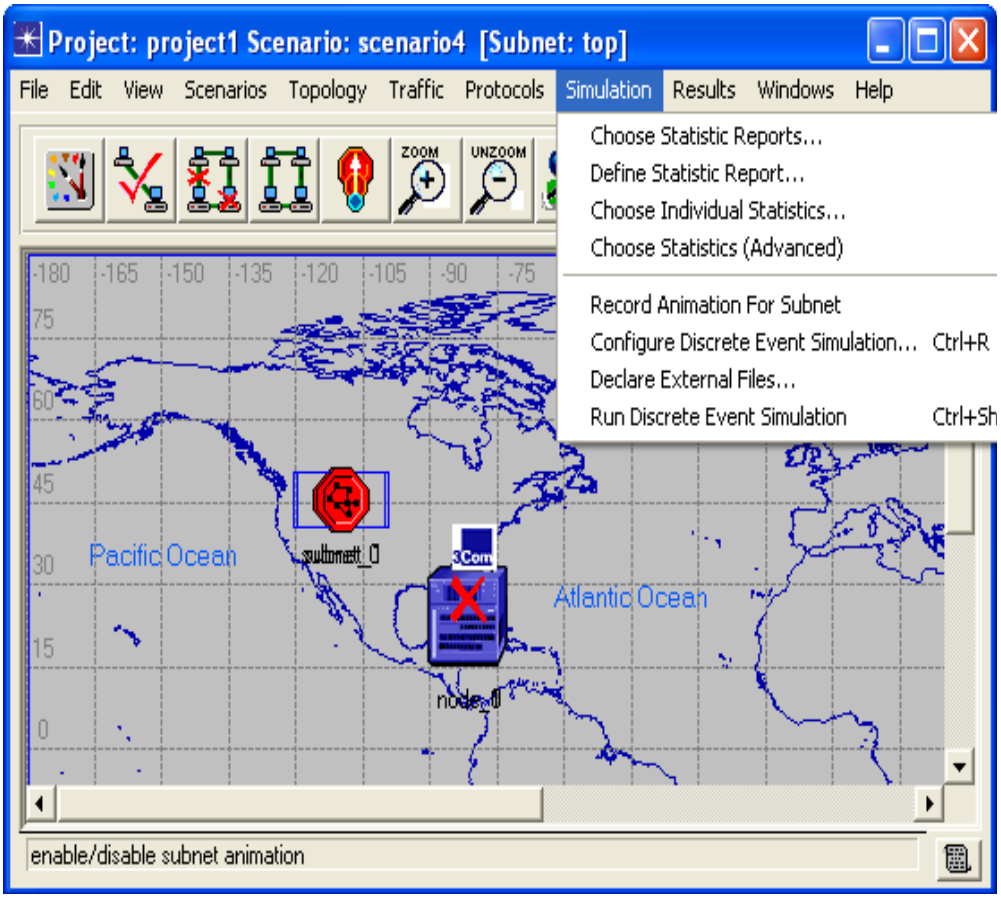
1.4.6 Protocols Menu



Εικόνα 1-15 Protocols Menu

Στο προηγούμενο μενού(Traffic) η μόνη επιλογή που έχουμε σαν χρήστες είναι η «Open Flows Browser» η οποία μέσω ενός Browser μας δίνει την επιλογή να πάρουμε λεπτομέρειες πάνω στη κίνηση του δικτύου ανά εφαρμογές/μέρη του δικτύου. Το επόμενο menu είναι αυτό των Protocols. Μέσα από αυτό το menu μπορούμε είτε να ανατρέξουμε σε βοήθεια για συγκεκριμένα πρωτόκολλα επικοινωνίας είτε να κάνουμε διάφορες ρυθμίσεις από τη στιγμή που θα χρησιμοποιηθούν μέσα στο δίκτυο. Οι εργαστηριακές ασκήσεις είναι σαφείς σχετικά με τα πρωτόκολλα που θα χρησιμοποιηθούν και οι ενέργειες που πρέπει να γίνουν σε κάθε μία από αυτές περιγράφονται αναλυτικά.

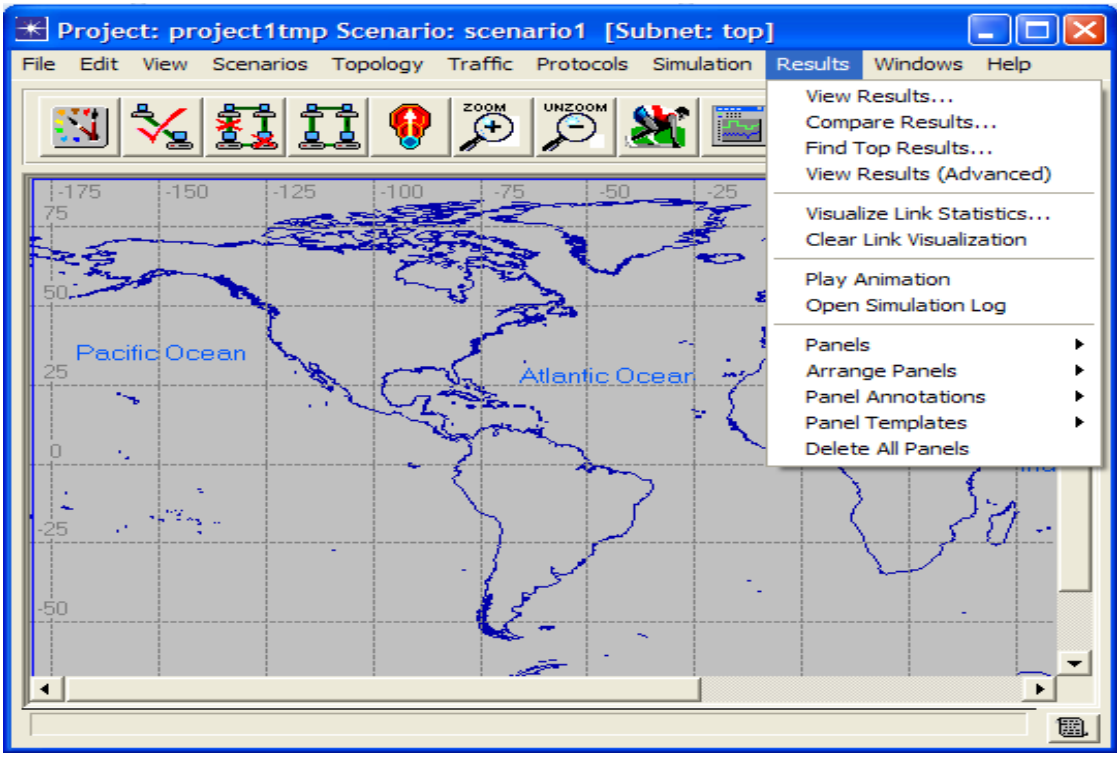
1.4.7 Simulation Menu



Εικόνα 1-16 Simulation Menu

Choose Statistic Reports: Επιλέγει την αναφορά που θα δημιουργηθεί για το δίκτυο που έχουμε δημιουργήσει.
Define Statistic Report: Ανοίγει ή δημιουργεί μια νέα αναφορά.
Choose Individual Statistics: Επιλέγουμε τι είδους στατιστικά θέλουμε να έχουμε στην αναφορά.
Choose Statistics (Advanced): Και πάλι επιλογή στατιστικών αυτή τη φορά πιο αναλυτικά με περισσότερες λεπτομέρειες.
Record Animation for Subnet: Καταγραφή της κίνησης των πακέτων για να μπορούμε μετά να δούμε την κίνηση με γραφικά.
Configure Discrete Event Simulation: (Βλέπε εικονίδιο 8 της toolbar)
Declare External Files: Προσδιορισμός εξωτερικών αρχείων αντικειμένων για χρήση τους στην εξομοίωση.
Run Discrete Event Simulation: Τρέξιμο της προσομοίωσης.

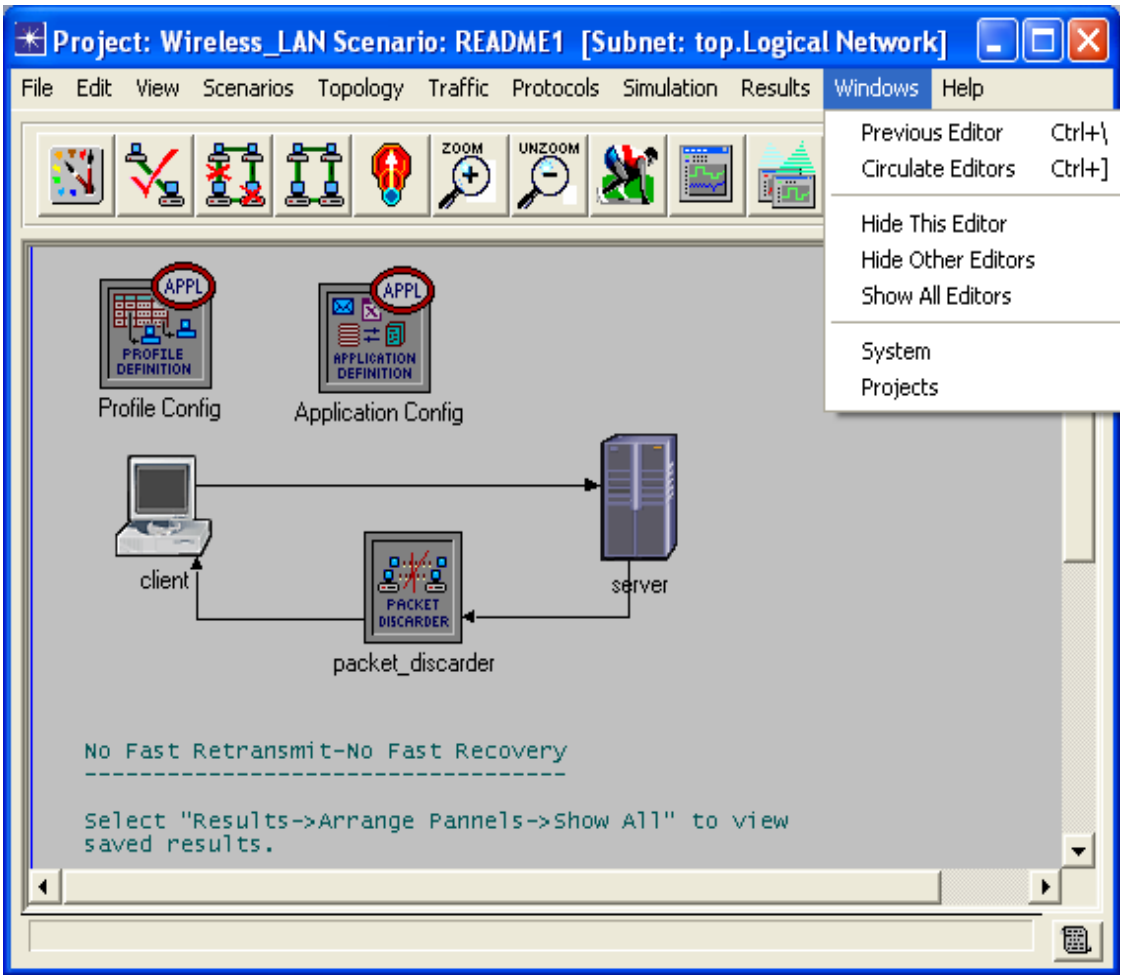
1.4.8 Results Menu



Εικόνα 1-17 Results Menu

View Results: Επιθεώρηση Αποτελεσμάτων.
Compare Results: Σύγκριση των αποτελεσμάτων διαφορετικών σεναρίων.
Find Top Results: Εμφάνιση μεγίστων/ ελαχίστων/ μέσων τιμών των αποτελεσμάτων ανά ομάδα αποτελεσμάτων. Με δυνατότητες φιλτραρίσματος εξαγωγής γραφήματος και αρχείου κειμένου.
View Results (Advanced): Ανάλυση των αποτελεσμάτων της εξομοίωσης
Visualize Link Statistics: Εμφάνιση των συνδέσμων (καλωδίων) με διαφορετικό χρώμα ή/και πάχος ανάλογα με τις τιμές των Utilization ή/και Throughput, αντίστοιχα.
Clear Link Visualization: Εκκαθάριση των οπτικών αλλαγών που έγιναν από την παραπάνω επιλογή.
Play Animation: Γραφική απεικόνιση της ροής των πακέτων που έχουν καταγραφή από την επιλογή Simulation Menu→ Record Animation for Subnet.
Open Simulation Log: Εμφάνιση όλων των μηνυμάτων που δημιουργήθηκαν από το πρόγραμμα κατά τη διάρκεια της εξομοίωσης.
Panels : Επιλογή των πάνελ που έχουν ανοιχτή.
Arrange Panels: Επιλογές για την διαρρύθμιση των πάνελ.
Panel Annotations: Μετατροπή των πάνελ σε σημειώσεις (attachments) και αντίστροφα.
Panel Templates: Δημιουργία φόρμας πάνελ από κάποιο υπάρχων.
Delete All Panels: Διαγραφή όλων των πάνελ.

1.4.9 Windows Menu



Εικόνα 1-18 Windows Menu

Previous Editor: Εμφάνιση άλλων ενεργών παραθύρων του OPNET σαν πρώτων (On top). Εάν μόνο ένα είναι ανοιχτό με την επιλογή αυτή ανοίγει η πρώτη/αρχική οθόνη του προγράμματος

Circulate Editors: Εναλλαγή ενεργών παραθύρων.

Hide This Editor: Απόκρυψη ενεργού παραθύρου.

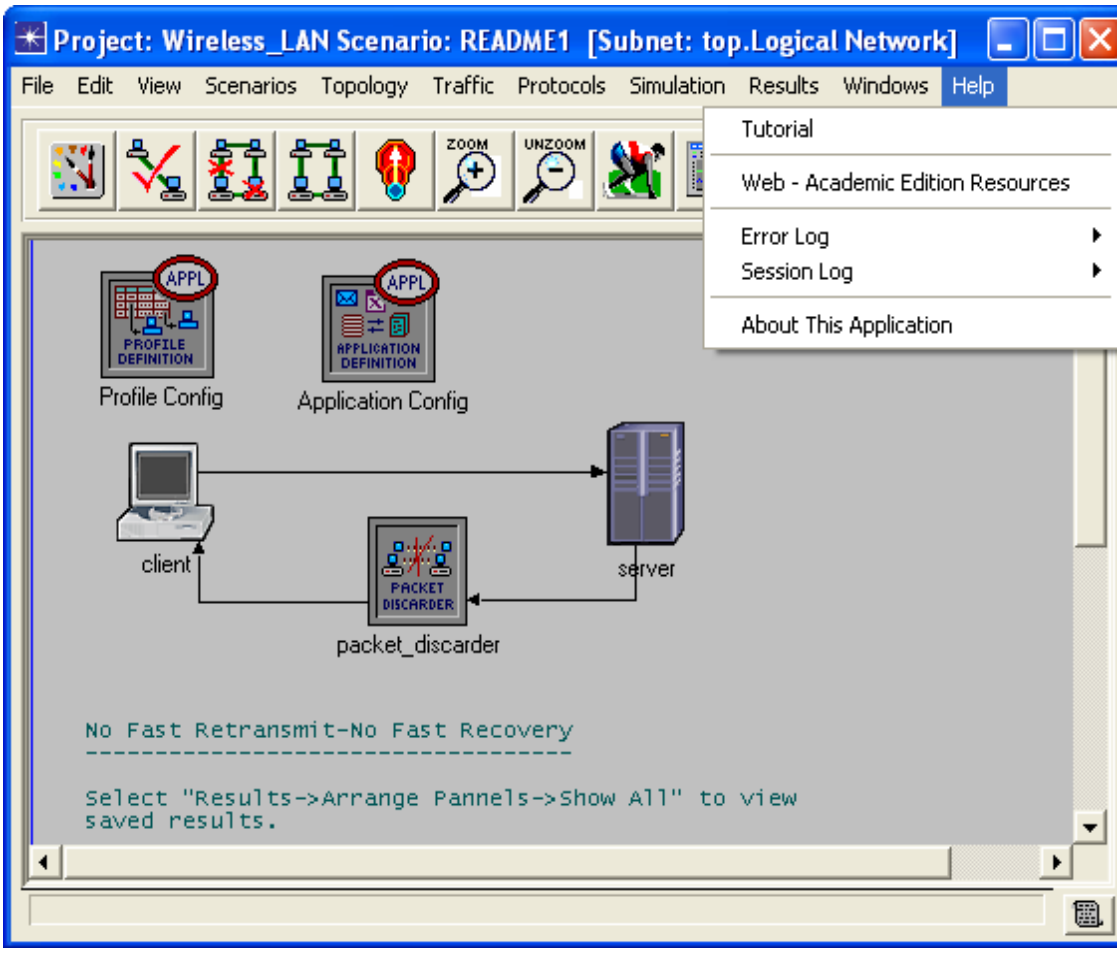
Hide Other Editors: Απόκρυψη άλλων ενεργών παραθύρων.

Show all Editors: Εμφάνιση όλων των παραθύρων OPNET

System: Με την επιλογή αυτή εμφανίζεται η αρχική οθόνη του OPNET.

Projects: Επιλέγουμε ποιο project θέλουμε να βλέπουμε στο περιβάλλον εργασίας εάν πάνω από ένα είναι ανοικτά.

1.4.10 Help Menu



Εικόνα 1-19 Help Menu

Tutorial: Με την επιλογή αυτή ανοίγουμε το tutorial του OPNET.
Web-Academic Edition Resources: Η επιλογή αυτή μας οδηγεί σε επίσημη ιστοσελίδα του OPNET.
Error Log: Εμφάνιση ή καθαρισμός του Error Log.
Session Log: Εμφάνιση ή καθαρισμός του Session Log.
About this Application: Εμφανίζονται πληροφορίες για την έκδοση του OPNET που χρησιμοποιείται.

1.5 Περιγραφή των Security Labs

1.5.1 ICMP Pings

Στο συγκεκριμένο σενάριο θα μελετήσουμε το Ping Trace και τις διαδρομές που ακολουθούν τα πακέτα σε μια επικείμενη αποτυχία κάποιον ζωτικών συνδέσεων.

1.5.2 Subnetting και OSI Model

Εδώ θα μελετήσουμε τα τρία επίπεδα του μοντέλου αναφοράς OSI, καθώς και το εργαλείο Packet Analyser για να παρατηρήσουμε τις TCP συνδέσεις.

1.5.3 Firewalls

Θα κάνουμε μια εισαγωγή στα Proxies και στα Firewalls. Έπειτα θα περιορίσουμε το παράνομο downloading με ένα Proxy, και θα μελετήσουμε την απόδοση της σύνδεσης μας.

1.5.4 RIP

Θα εξηγήσουμε το πρωτόκολλο RIP Routing, και πώς δημιουργούμε timed link αποτυχίες και ανανήψεις.

1.5.5 OSPF

Θα συγκρίνουμε το OSFP με το RIP πρωτόκολλο, και θα μελετήσουμε το Load Balancing.

1.5.6 VPN

Θα μελετήσουμε ασφαλής μη-τοπικές συνδέσεις. Επίσης ένας Hacker θα προσπαθήσει να αποκτήσει πρόσβαση στον server που προστατεύουμε χρησιμοποιώντας εικονικά ιδιωτικά δίκτυα (VPNs).

1.5.7 VLAN

Θα δημιουργήσουμε λογικές ομάδες χρηστών χρησιμοποιώντας Εικονικά LANs. Επίσης θα μελετήσουμε την διασύνδεση One-Armed-Router.

1.5.8 Dual Homed Router/Host, Security Lab 9: Screened Host/Subnet. DMZ και Security Lab10: Collapsed DMZ

Σε αυτά τα τρία σενάρια ασφαλείας θα εξηγήσουμε τους στατικούς πίνακες δρομολόγησης, επίσης θα μελετήσουμε τα ACLs, τα Proxies καθώς και την σύγκριση μεταξύ εσωτερικής και περιμετρικής ασφάλειας. Το σενάριο 10 είναι 100% πρακτικό, κάτι το οποίο θέλουμε να το δημιουργήσετε μόνοι σας, για να δούμε το επίπεδο σας.

Στην συγκεκριμένη πτυχιακή εργασία πραγματοποιήθηκαν τα εξής σενάρια ασφαλείας από τα παραπάνω:

1) ICMP Pings
2) Firewalls
3) VPN
4) Firewalls VPN
5) VLAN's
6) Screened Host / Subnet (DMZ)

Όσον αφορά τα υπόλοιπα σενάρια δηλαδή τα εξής:

1) Subnetting και OSI Model
2) RIP
3) OSFP
4) Dual Homed Router / Host
5) Collapsed DMZ

Η υλοποίηση τους δεν κατέστη δυνατή καθώς θα έπρεπε να επιλέξουμε μαζί με τον υπεύθυνο καθηγητή μου κ. Χ.Μανιφάβα μερικά από αυτά και όχι όλα, για ευνόητους λόγους.
Παρόλα αυτά η επιλογή των υλοποιημένων σεναρίων ήρθε μετά από πολύ σκέψη και πιστεύω ότι επιλέξαμε τα πιο καίρια (ας μου επιτραπεί η έκφραση σημαντικά), σενάρια και αυτά των οποίων οι τεχνολογίες έχουν μεγαλύτερη απήχηση σε πρακτικό επίπεδο στον τομέα των δικτύων (χωρίς να θέλω να υποβαθμίσω τις μη υλοποιημένες τεχνολογίες).

Chapter 2 ICMP Ping

2.1 Εισαγωγή

ICMP (Internet Control Message Protocol[1]) είναι ενσωματωμένο μέσα στο IP πρωτόκολλο, και χρησιμοποιείται για την ανίχνευση λαθών δικτύων και στον έλεγχο μηνυμάτων. Χρησιμοποιείται επίσης για να γνωστοποιήσει ότι ένα διάγραμμα δεδομένων δεν έφτασε στον προορισμό του, είτε επειδή ο ξενιστής προορισμού (destination host) δεν βρέθηκε (UNREACHABLE HOST) ή επειδή τα IP πακέτα ταξίδεψαν μέσα από πολλούς δρομολογητές (TTL EXCEEDED).

Αυτό το κεφάλαιο εξηγεί ακόμα μια εφαρμογή: ICMP ECHO REQUEST / ECHO REPLY[2] (aka Ping). Ένα ECHO REQUEST μήνυμα στέλνεται σε μια IP διεύθυνση για να ανακαλύψει εάν η επικοινωνία μεταξύ των peer λειτουργεί. Ο υπολογιστής προορισμού υποτίθεται ότι πρέπει να απαντήσει με ένα ECHO REPLY μήνυμα.

2.2 Περιγραφή Σεναρίου

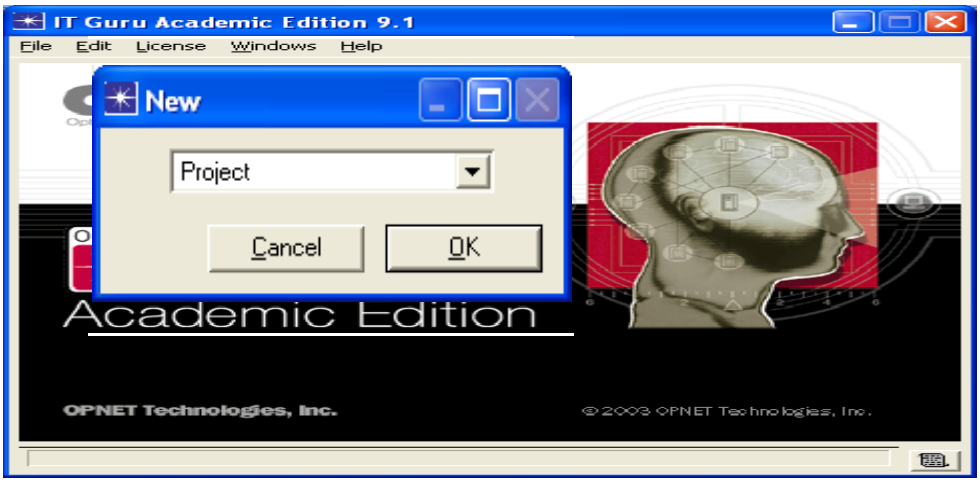
Ένα δίκτυο δημιουργείται με 5-routers-ring-backbone[3] και 2 τερματικούς σταθμούς (A και B) ακριβώς απέναντι. Ο σταθμός A θα στείλει ένα ECHO REQUEST στον σταθμό B, και ο B σταθμός θα απαντήσει με ένα ECHO REPLY. Θα εξετάσουμε εάν το REQUEST πακέτο πέρασε μέσα από τους 3 δρομολογητές μεταξύ των peers, και το REPLY πακέτο επέστρεψε χρησιμοποιώντας ακριβώς το ίδιο μονοπάτι (το πρωτόκολλο δρομολόγησης γι' αυτό το εργαστήριο είναι το RIP[4]). Σε ένα δεύτερο σενάριο, μία από αυτές τις συνδέσεις θα αποτύχει, και θα μελετήσουμε πως αυτό επηρεάζει το ping trace.

2.3 Δημιουργία του Σεναρίου

1. Ανοίγουμε ένα καινούργιο Project στο OPNET IT Guru Academic Edition (**File→ New Project**) χρησιμοποιώντας τις παρακάτω παραμέτρους (αφήστε σε default κατάσταση τις υπόλοιπες τιμές).

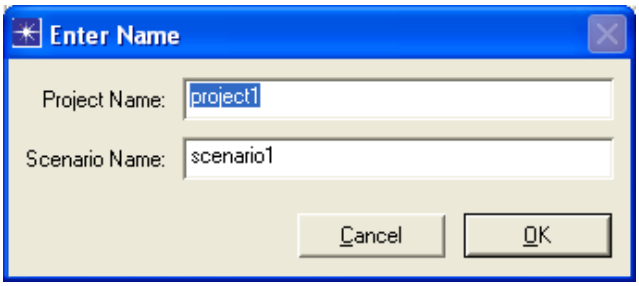
    - **Project Name: <your_name>_Ping**
    - **Scenario Name: NoFailure**
    - **Network Scale: Campus**

[1] http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
http://john.albin.net/essential-icmp
[2] http://www.tech-faq.com/icmp.shtml
[3] http://www-mice.cs.ucl.ac.uk/multimedia/misc/tcp_ip/8803.mm.www/0165.html
[4] http://en.wikipedia.org/wiki/Routing_Information_Protocol

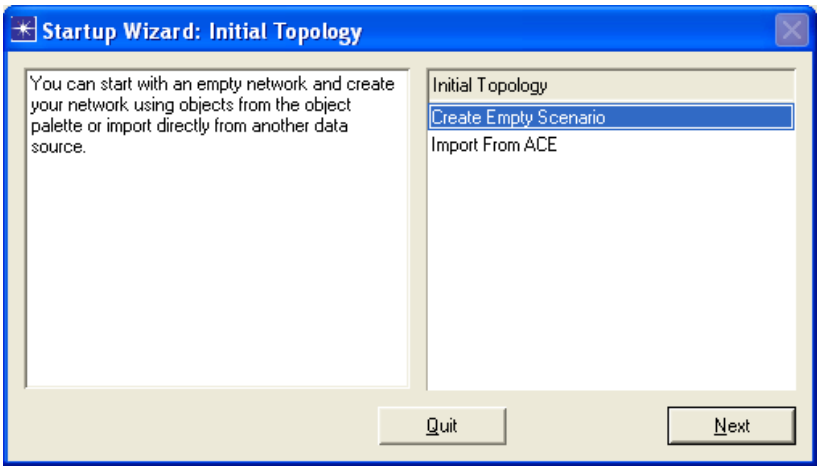


Εικόνα 2-1 Create the Project

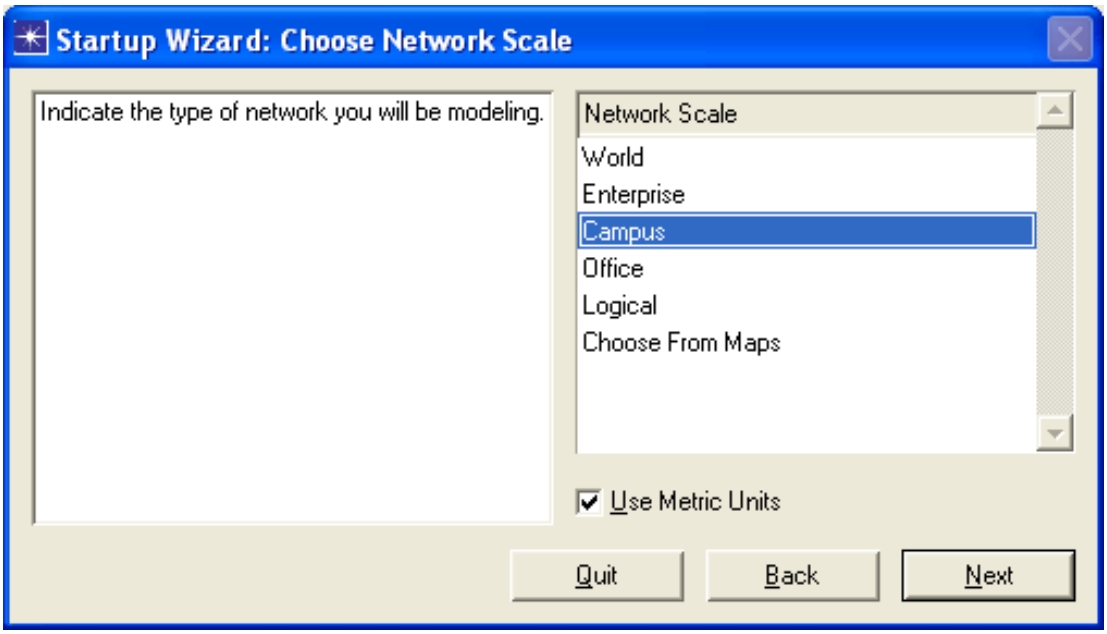
- **Project Name: <your_name>_Ping**
- **Scenario Name: NoFailure**
- **Network Scale: Campus**



Εικόνα 2-2 Project And Scenario Name



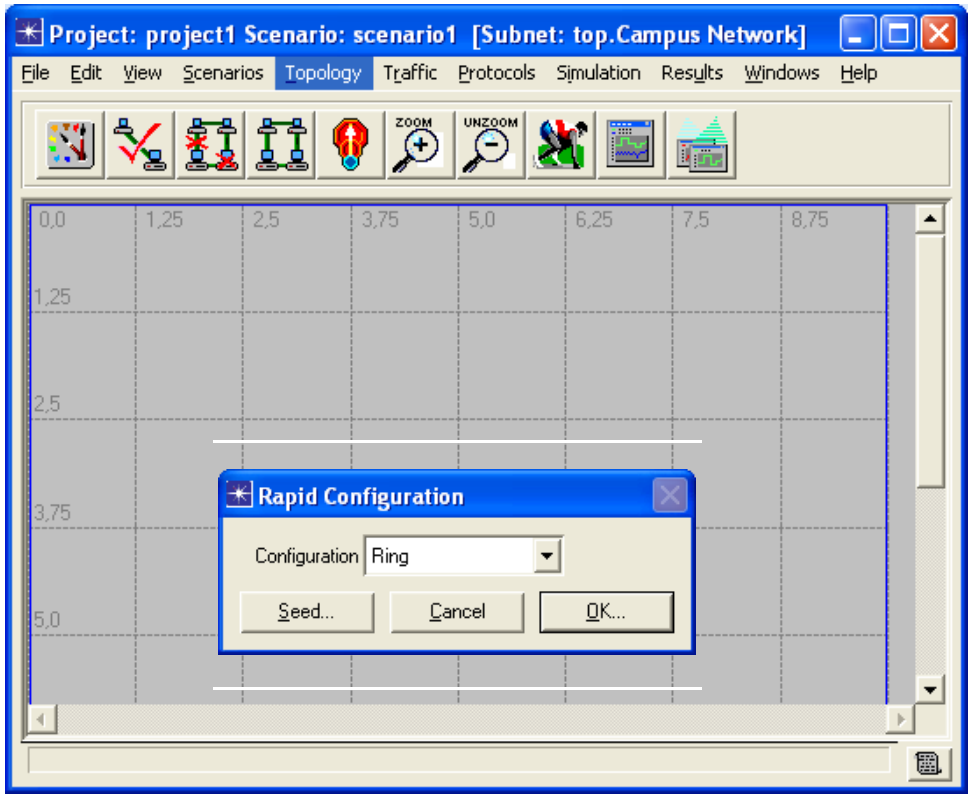
Εικόνα 2-3 Topology of Our Network



Εικόνα 2-4 Network Scale

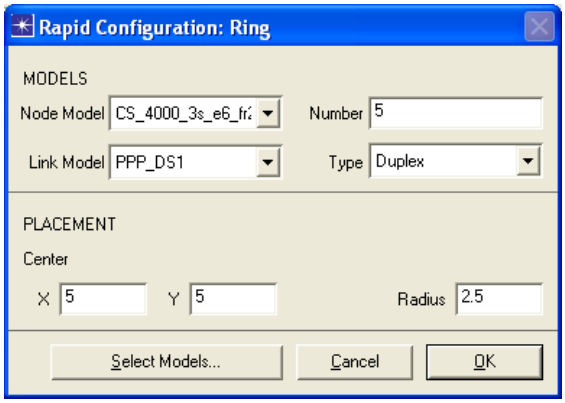
Πιέστε **Next** αρκετές φορές μέχρι να τελειώσει το Startup Wizard. Ο Project Editor θα προωθηθεί σε ένα κενό πλέγμα.

2. Για να δημιουργήσουμε το 5-router-ring: **Topology→ Rapid Configuration**,

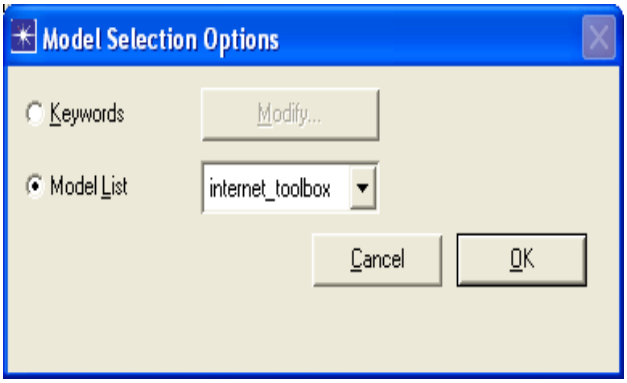


Εικόνα 2-5 Select The Ring Configuration

- Στο Popup παράθυρο, **Configuration: Ring**, και πατάμε **OK.**
- Κάνουμε κλικ στο **Select Models** και επιλέγουμε το **internet_toolbox** από το combo box, για να επιλέξουμε τη βιβλιοθήκη απ' όπου θέλουμε να πάρουμε τους δρομολογητές και τις συνδέσεις. Και τέλος πατάμε **OK**.



Εικόνα 2-6 Parameters of The Ring



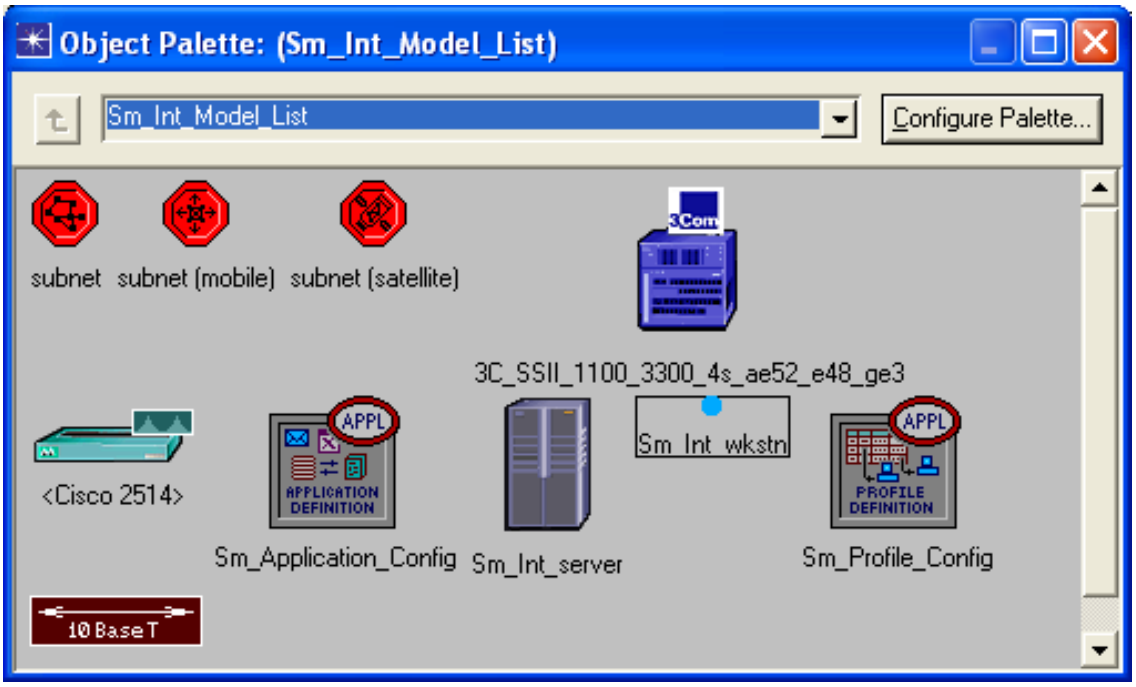
Εικόνα 2-7 Select Model List

- Στο **Node Model** combo box, επιλέγουμε τον εξής δρομολογητή: **CS_4000_3s_e6_fr2_sl2_tr2.**
- Επιλέγουμε την εξής σύνδεση για να συνδέσουμε τους δρομολογητές, **Link Model: PPP_DS1.**
- **Number: 5** δρομολογητές.
- Το κέντρο του δαχτυλιδιού είναι (X,Y)= (5,5).
- Το μήκος της ακτίνας είναι 2,5.
- Πατάμε **OK** για να δημιουργήσουμε το δίκτυο.

3. Εισάγουμε 2 **Sm_Int_wkstn** σταθμούς εργασίας και τους συνδέουμε με **10BaseT** καλώδια:

   Ανοίξτε το **Object Palette** κάνοντας κλικ σε αυτό το εικονίδιο  .

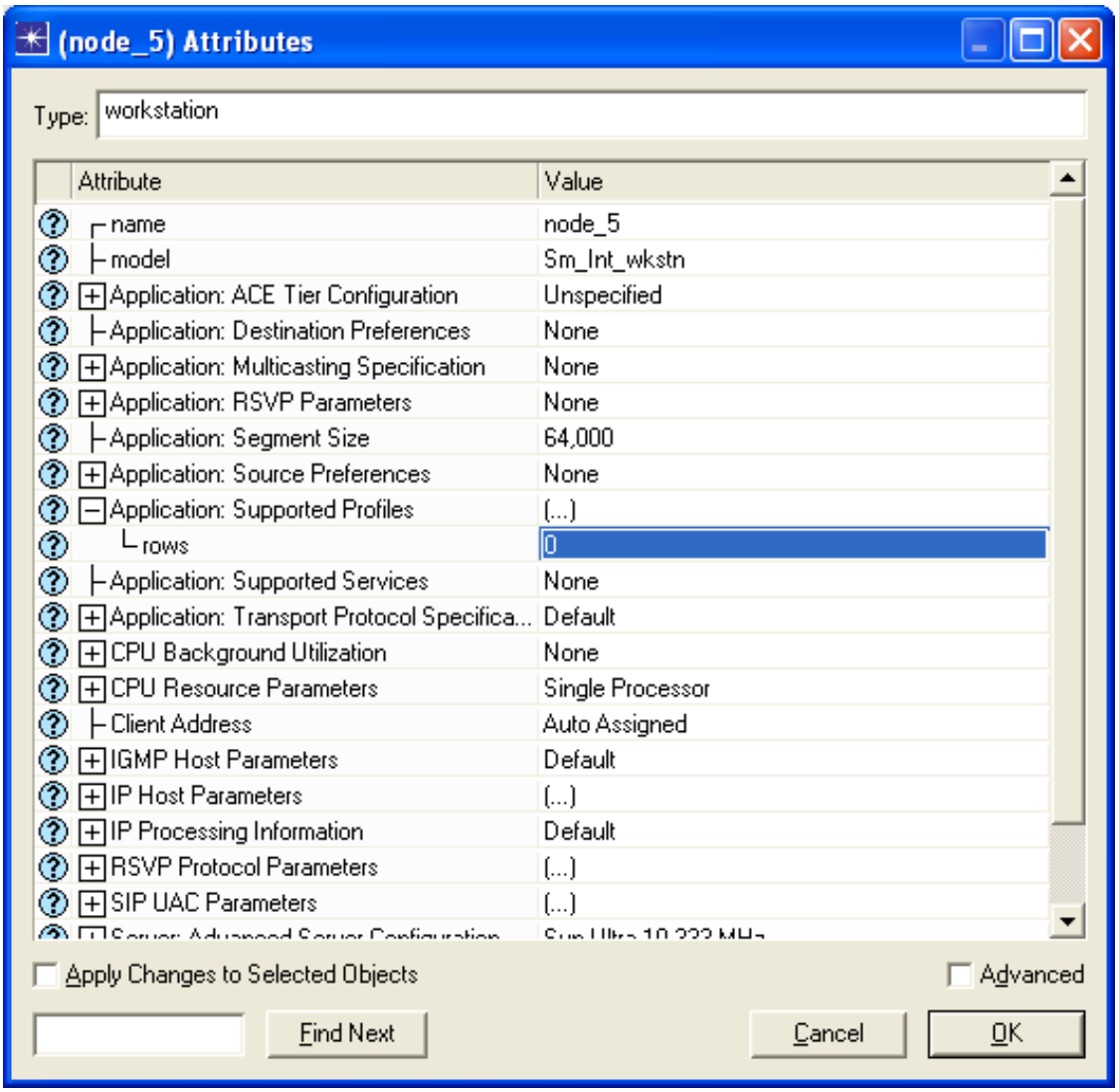
   - Σύρετε τους δύο **Sm_Int_wkstn** σταθμούς εργασίας, και τοποθετήστε τους στο πλέγμα.
     Αυτό μπορεί να βρεθεί από το combo box της παλέτας αντικειμένων.



Εικόνα 2-8 Workstation of Our Network

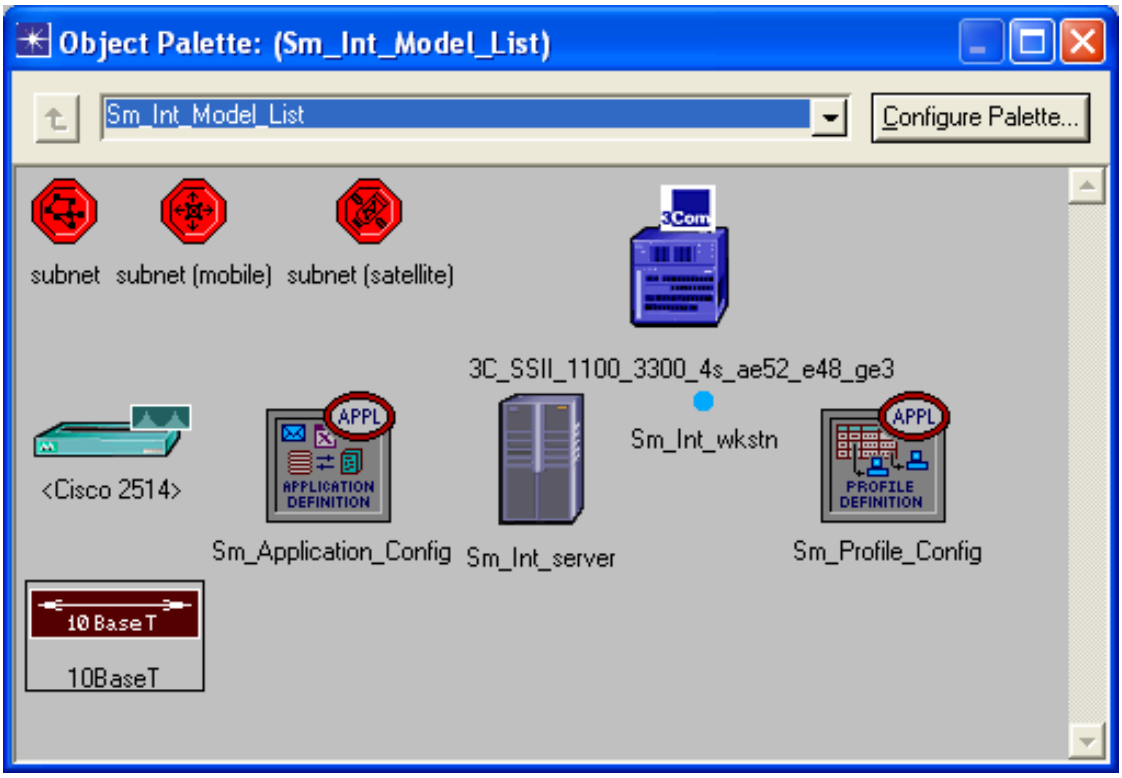
Αλλάξτε τις εξής ιδιότητες:

- Δεξί κλικ στον σταθμό και πατήστε **Edit Attributes**.
- Επιλέξτε **Application Supported Profiles→ rows: 0**. Πραγματοποιώντας αυτό, οι σταθμοί εργασίας δεν θα έχουν κάποιο καθορισμένο προφίλ (εξάλλου δεν χρειαζόμαστε κάποιο, επειδή η μοναδική κυκλοφορία που θέλουμε είναι το Ping).
- Επαναλάβετε αυτήν την διαδικασία και για τους δύο σταθμούς εργασίας.



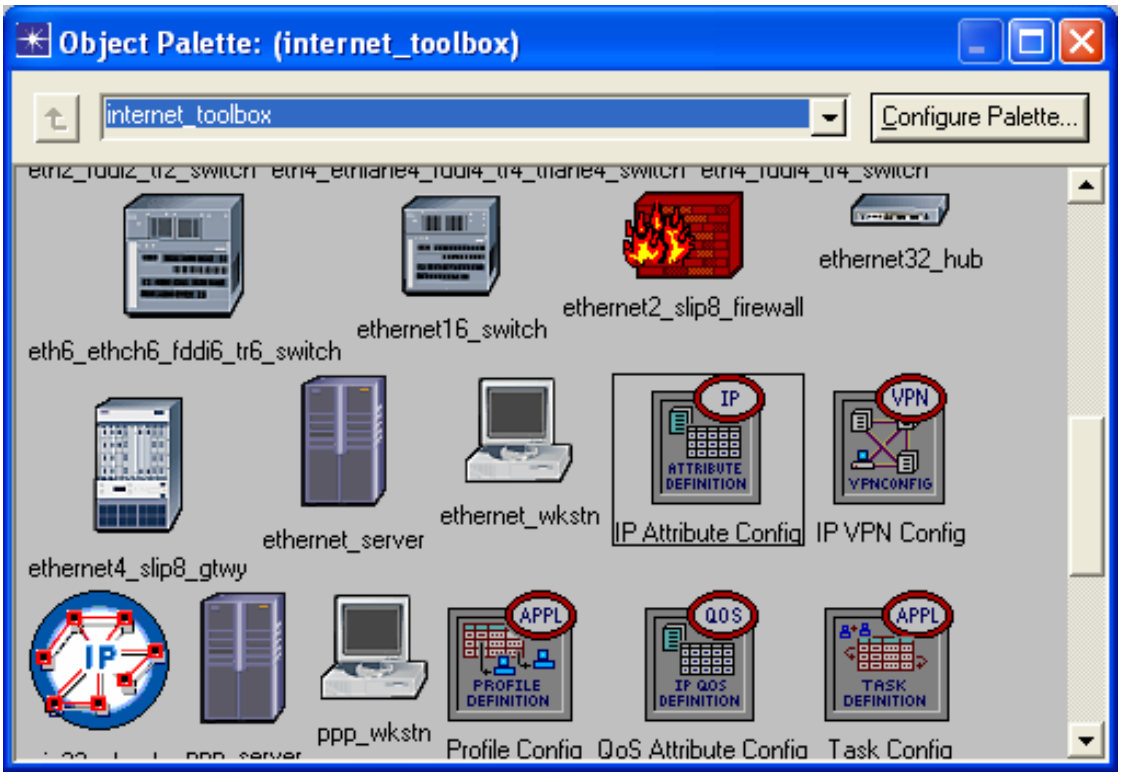
Εικόνα 2-9 Attributes Of node_5

- Συνδέστε τους δύο σταθμούς εργασίας στους δύο δρομολογητές που βρίσκονται απέναντι ο ένας από τον άλλον, χρησιμοποιώντας **10BaseT** καλώδια από την ίδια παλέτα.



Εικόνα 2-10 Select the Wires

- Τώρα το δίκτυο είναι έτοιμο, και ήρθε η ώρα να ρυθμίσουμε την ICMP κίνηση. Το πρώτο βήμα είναι να τοποθετήσουμε ένα **IP Attribute Config** control. Αυτό μπορεί να βρεθεί από την επιλογή **internet_toolbox** της παλέτας αντικειμένων.



Εικόνα 2-11 Select the IP Attribute Config

- Επεξεργαστείτε τις ιδιότητες ελέγχου **(δεξί κλικ→ Edit Attributes).** Οι παράμετροι που ρυθμίζουμε μπορούν να βρεθούν στο **IP Ping Parameters→ row 0 (Pattern: Default**):
  - **Interval (sec): 90**
  - **Count: 1000**
  - **Record Route: Enabled**
- Πατήστε **OK** για να εφαρμόσετε τις αλλαγές.

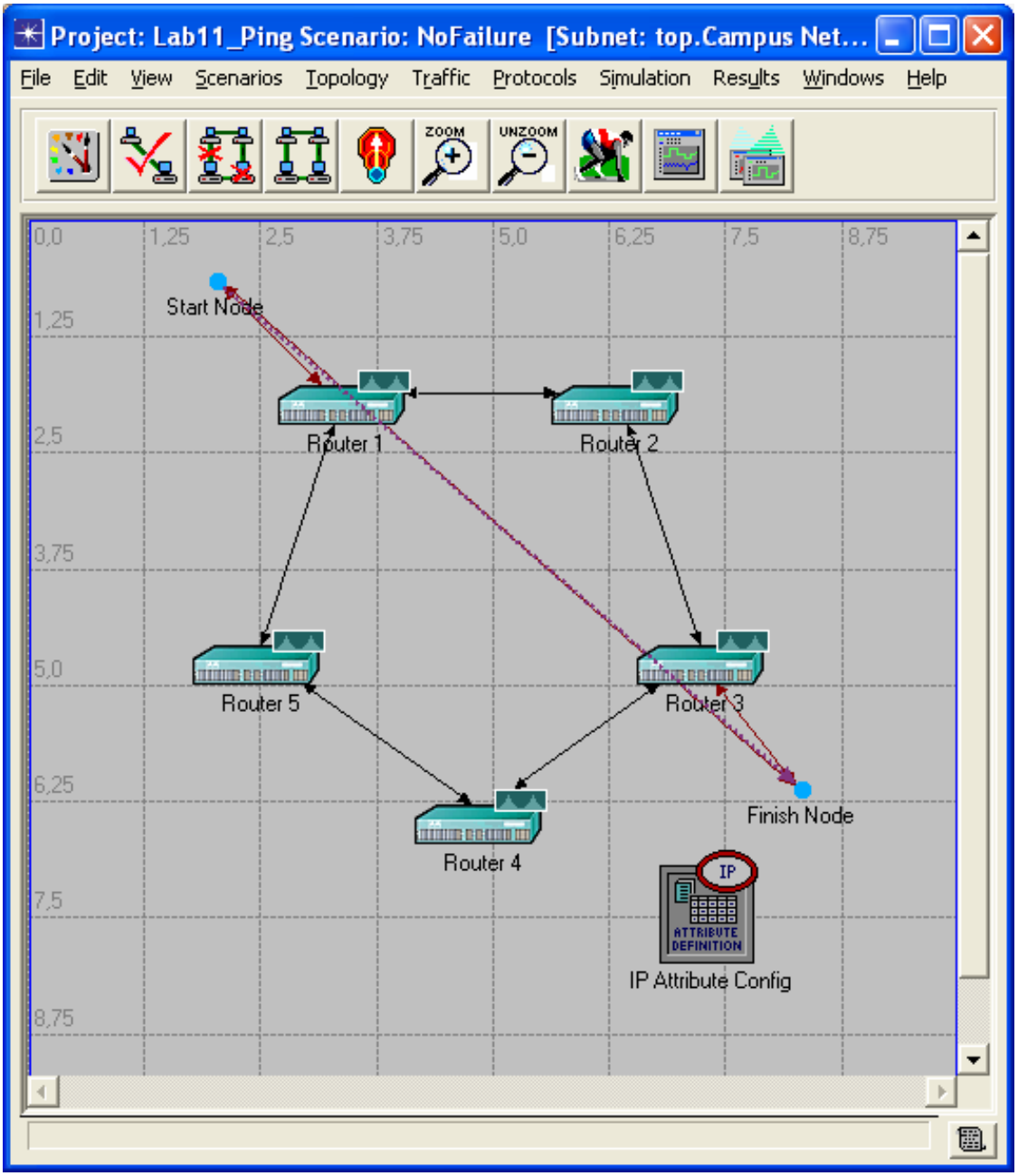
4. Χρησιμοποιώντας το **ip_ping_traffic** αντικείμενο από την **παλέτα αντικείμενου** (**internet_toolbox**), σύρετε μια ICMP Ping απαίτηση από το ένα host στο άλλο:

   - Επιλέξτε το **ip_ping_traffic** από την παλέτα αντικειμένων.
   - Κάντε κλικ στον ένα σταθμό εργασίας (εκκίνησης) και έπειτα στον άλλον (τερματισμού).
   - Όταν τελειώσετε, πατήστε δεξί κλικ και επιλέξτε το **Abord Demand Definition**.
   - Δεξί κλικ στην ελεύθερη γραμμή, μετά κλικ στο **Edit Attributes** και έπειτα ρυθμίστε τα εξής:
     - **Ping Pattern: Default**
     - **Start Time: constant(1000)**

Επιλέξτε το RIP πρωτόκολλο δρομολόγησης για το σενάριο:

- Στον Project Editor, **Protocols→ IP Routing→ Configure Routing Protocols…** Ελέγξτε ότι μόνο το RIP είναι επιλεγμένο, και στην συνέχεια πατήστε **OK.**
- **Protocols→ RIP→ Configure Start Time.** Επιλέξτε **Mean OutCome: 20** και πατήστε **OK**. Το πρωτόκολλο RIP θα αρχίσει να δημιουργεί τους πίνακες δρομολόγησης από αυτήν την στιγμή.

Αλλάξτε τα ονόματα των κόμβων όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 2-12 The Scenario is completed

2.4 Ρυθμίστε την προσομοίωση

1. Κάντε κλικ στο **configure/run simulation**  από τον Project Editor και θέστε τις παρακάτω τιμές:

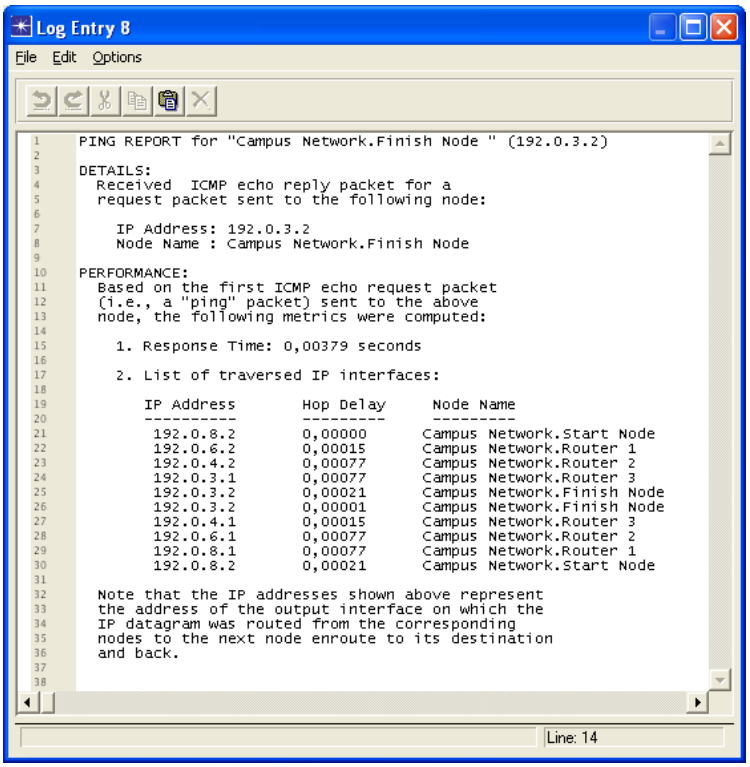
    - **Duration: 1 hour(s).**
    - Στο **Global Attribute** tab,

        - **RIP Sim Efficiency: Disabled.** Τα μηνύματα RIP θα στέλνονται όλη την ώρα κατά την διάρκεια της προσομοίωσης.
        - **RIP Stop Time: 10000**. Οι πίνακες δρομολόγησης θα ενημερώνονται κατά την διάρκεια της προσομοίωσης (η προσομοίωση θα τελειώσει πριν σταματήσει το RIP).
        - **IP Routing Table Export/Import: Export.** Θα εξάγουμε τους πίνακες δρομολόγησης σε ένα αρχείο στο τέλος.
2. Κάντε κλικ στο **Run**.

2.5 Ανάλυση Αποτελεσμάτων

Μόλις τελειώσει η προσομοίωση:

1. Κλείστε το παράθυρο της προσομοίωσης, κάνοντας κλικ στο **Close**.
2. Στον **Project Editor,** κάντε κλικ στο **Results→ Open Simulation Log.** Επανεξετάστε τα ECHO και ECHO REPLY μονοπάτια καθώς και τα πακέτα που έχουν περάσει μέσα από τους δρομολογητές. Όλες αυτές οι πληροφορίες είναι στο **PING REPORT**, όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 2-13 Ping Report

2.6 Ερωτήσεις

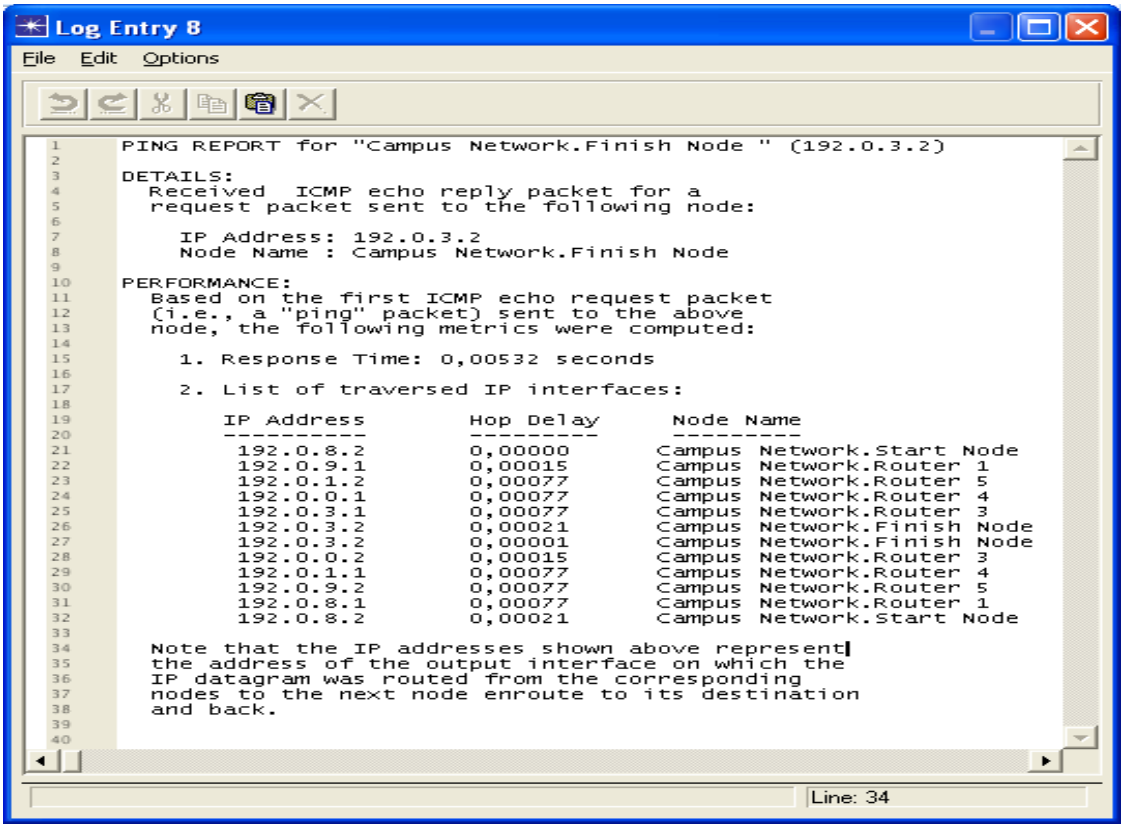
2.6.1Ερώτηση 1η

Αναπαράγετε το σενάριο **NoFailure** και ονομάστε το **WithFailure**. Επιλέξτε μια σύνδεση που το Ping χρησιμοποιούνταν στην τελευταία προσομοίωση (π.χ. **Router 1-Router 2**), και κάντε το να αποτύχει, επιλέγοντας το και κάνοντας κλικ στο **mark selected node or link as failed**  κουμπί. Αναλύστε το νέο Ping trace.

2.7 Απαντήσεις

2.7.1 Απάντηση 1η

Από τον Project Editor, επιλέξτε **Scenario→ Duplicate Scenario**. Το νέο σενάριο ονομάζεται **Scenario Name: WithFailure** και πατάμε **OK**. Επιλέγουμε να αποτύχει η σύνδεση μεταξύ **Router 1 – Router 2** και εκτελούμε την προσομοίωση. Το Ping trace ακολουθεί ένα καινούργιο μονοπάτι όπως φαίνεται από το **Ping Report**:



Εικόνα 2-14 Ping Report for the scenario WithFailure

2.8 Συμπεράσματα

Όπως παρατηρούμε και στις δύο περιπτώσεις το echo reply μήνυμα χρησιμοποιεί ακριβώς το ίδιο μονοπάτι με αυτό που χρησιμοποίησε το echo request για να φτάσει σε αυτό. Στην πρώτη περίπτωση ακολούθησε το μονοπάτι: Start Node→ Router 1→ Router 2→ Router 3→ Finish Node θα μπορούσε να χρησιμοποιήσει και το άλλο μονοπάτι το οποίο είναι το Start Node→ Router 1→Router 5→ Router 4→ Router 3→ Finish Node, αλλά σύμφωνα με τους αλγόριθμους δρομολόγησης χρησιμοποίησε το πρώτο. Στην δεύτερη περίπτωση επειδή είχαμε διακόψει την σύνδεση μεταξύ του Router 1 και Router 2, αναγκάστηκε να χρησιμοποιήσει το μοναδικό μονοπάτι που καθιστούσε δυνατή την επικοινωνία μεταξύ Start Node και Finish Node, και το οποίο είναι Start Node→ Router 1→ Router 5→ Router 4→ Router 3→ Finish Node. Το σημαντικό είναι ότι και στις 2 περιπτώσεις το ping trace δεν επηρεάστηκε από την αποτυχία μιας σύνδεσης ή όχι στο δίκτυο μας με αποτέλεσμα τα echo reply μηνύματα να ακολουθήσουν το ίδιο ακριβώς μονοπάτι που χρησιμοποίησαν τα echo request.

Chapter 3 Firewalls

3.1 Εισαγωγή

Το Firewall[5] είναι ένα σύστημα ελέγχου πρόσβασης στο δίκτυο που χωρίζει ένα δίκτυο που θεωρούμε ασφαλές από ένα άλλο δίκτυο που είναι δεν είναι. Παρόλο που μπορεί να ελέγχει την εισερχόμενη και την εξερχόμενη κυκλοφορία, η πιο κοινή χρήση των Firewall είναι να ελέγχουν μόνο την εισερχόμενη κυκλοφορία. Σημειώστε ότι τα Firewall δεν παρέχουν καμία προστασία από τις εσωτερικές επιθέσεις.

3.2 Network Firewalls (packet filtering)

Οι δρομολογητές (routers) μπορούν να ελέγξουν τα IP πακέτα που πηγαίνουν σε αυτούς αποδέχοντας τα ή απορρίπτοντας τα, σύμφωνα με τις πολιτικές που έχουν επιπτώσεις στις επικεφαλίδες πρωτοκόλλου (IP, ICMP, UDP, TCP,…). Μπορούμε να αναλύσουμε την πηγή/προορισμό τις διεύθυνσης (source/destination addresses), τα ports,τους τύπους των πρωτοκόλλων περιεχόμενο και μέγεθος των πακέτων, κλπ... Υπάρχουν δύο γενικές πολιτικές: α) μπορούμε να αποδεχθούμε όλα τα πακέτα εκτός από ένα περιορισμένο σύνολο περιπτώσεων, και β) να απορρίψουμε όλη την κίνηση, εκτός από ένα περιορισμένο σύνολο περιπτώσεων. Η περίπτωση β είναι δυσκολότερο να εφαρμοστεί, αλλά γενικά είναι πιο αποδεκτή.
Κάθε πακέτο που φθάνει στην συσκευή θα αναζητήσει τους κανόνες φιλτραρίσματος και θα σταματήσει στο πρώτο «match», και μετά από αυτό θα πάρει την απόφαση είτε της άρνησης είτε της αποδοχής της κυκλοφορίας. Μια προκαθορισμένη (default) πολιτική είναι πάντα σε κατάσταση λειτουργίας.

3.3 Proxies (Application Gateways)

Συμπεριφέρονται ως Application-level συσκευές αναμετάδοσης. Οι χρήστες δικτύων καθιερώνουν μια επικοινωνία με το πληρεξούσιο (proxy[6]), διαιρώντας κατά συνέπεια τη σύνδεση πηγή-προορισμού σε δύο ανεξάρτητες συνδέσεις (πηγή-firewall και firewall-προορισμός). Ο proxy server διαχειρίζεται τις αιτήσεις για σύνδεση (request connections).
Αυτή η τεχνολογία έχει μια πιο αργή απόδοση από το network firewalling[7] επειδή λειτουργεί στο ανώτατο στρώμα του OSI[8]. Είναι συνηθισμένο να χρησιμοποιούνται και τα δύο firewall συγχρόνως.

[5] http://en.wikipedia.org/wiki/Firewall
[6] http://proxy.org/
[7] http://www.more.net/technical/netserv/tcpip/firewalls/
[8] http://en.wikipedia.org/wiki/OSI_model

Τα Cache Proxies[9] είναι ένας δημοφιλής τρόπος να αυξηθεί η απόδοση, μέσω της αποθήκευσης των δεδομένων, η πύλη (gateway) διαβιβάζεται στο firewall, έτσι δεν είναι απαραίτητο να ψάξουμε στο Internet για τα ίδια δεδομένα την επόμενη φορά που ένας άλλος υπολογιστής τα ζητήσει.

3.4 Περιγραφή Σεναρίου

Το συγκεκριμένο κεφάλαιο έχει δύο τμήματα, καθένα με το δίκτυο του (Lan1 και Lan2), προσπαθώντας να έχει πρόσβαση σε έναν Database Server, όπου μια βάση δεδομένων με τις πληροφορίες των πελατών είναι αποθηκευμένη, καθώς και ένας E-mail και HTTP server. Συγχρόνως, μερικοί εργαζόμενοι της εταιρείας χρησιμοποιούν παράνομα πολυμέσα που μεταμορφώνουν (multimedia downloading), και έτσι επιβραδύνουν την απόδοση του Internet. Η επιχείρηση ζήτησε να τοποθετήσουμε ένα Firewall για να αποφύγουμε την παράνομη κυκλοφορία των πολυμέσων προκειμένου να μειωθεί ο μέσος χρόνος πρόσβασης στις βάσεις δεδομένων κατά 1 sec.

3.4.1Δημιουργία του Σεναρίου

1. Ανοίξτε το **OPNET IT Guru Academic Edition**→ και στην συνέχεια επιλέξτε **New Project** από το **File menu.** (χρησιμοποιήστε τις παρακάτω παραμέτρους και αφήστε τις υπόλοιπες σε default κατάσταση):

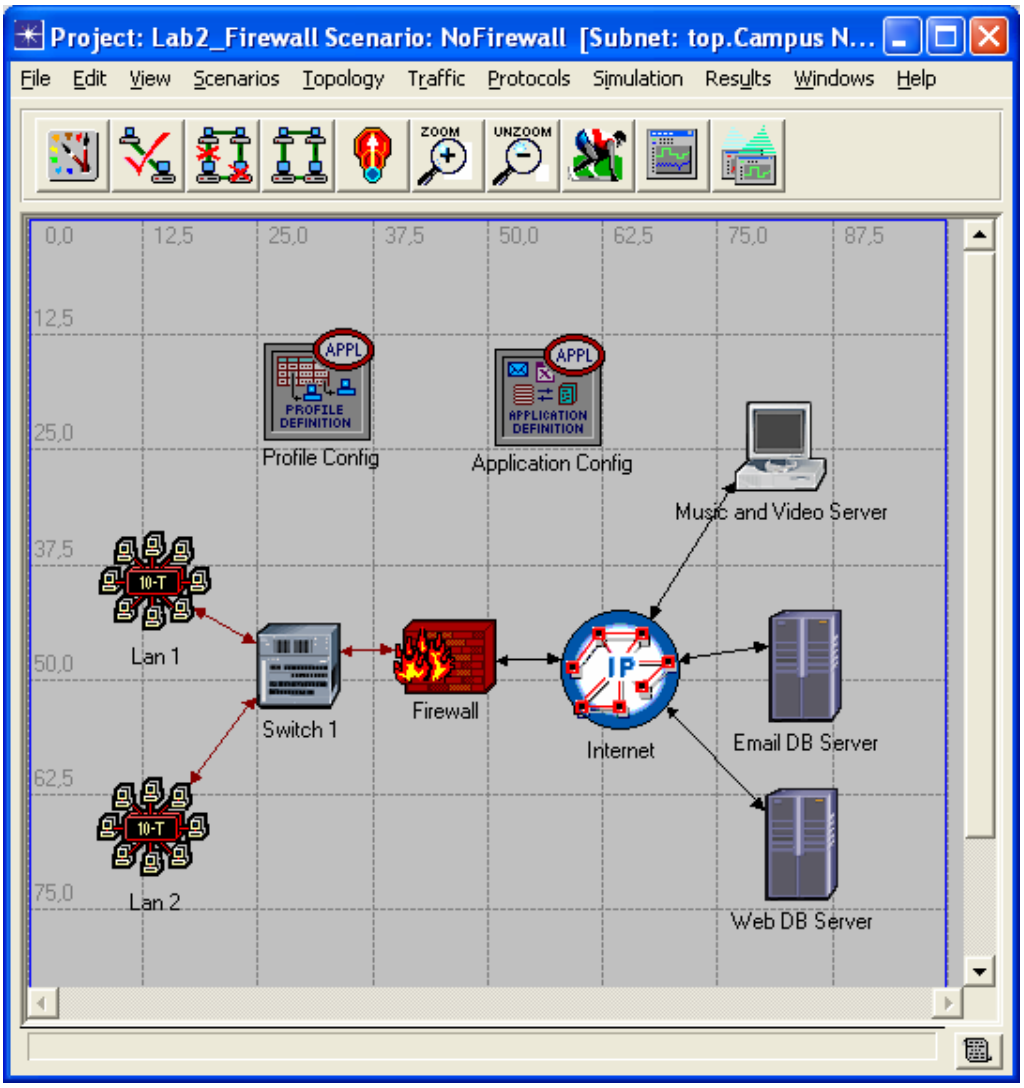
   - Project Name: <your name>_Firewall
   - Scenario Name: No Firewall
   - Network Scale: Campus
   - Size 100x100 meters

   Πατήστε **Next** έως ότου τελειώσει το Startup Wizard

2. Δημιουργία του Δικτύου :

   Δημιουργούμε το σενάριο της εικόνας 3.1. Τα συστατικά και η παλέτα που χρησιμοποιούνται μπορούν να βρεθούν στο **Object Palette** που συνοψίζονται στον πίνακα L3.2

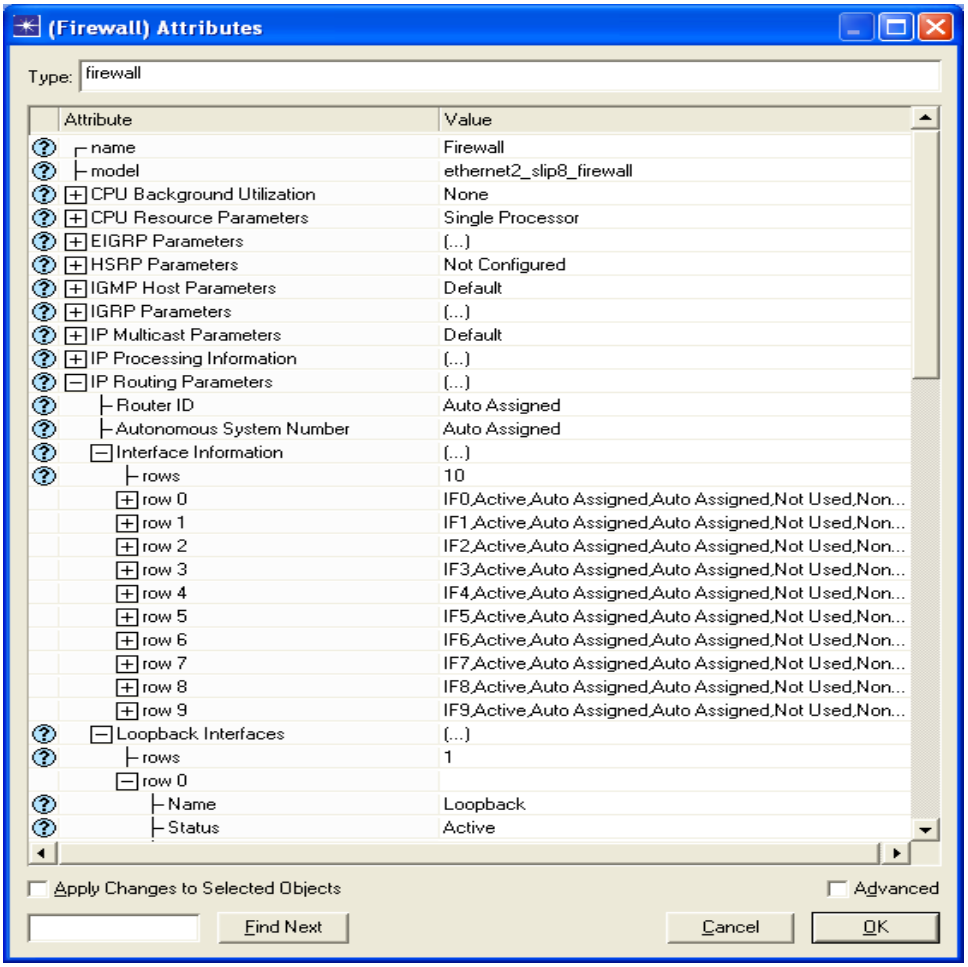
[9] http://www.web-caching.com/proxy-caches.html

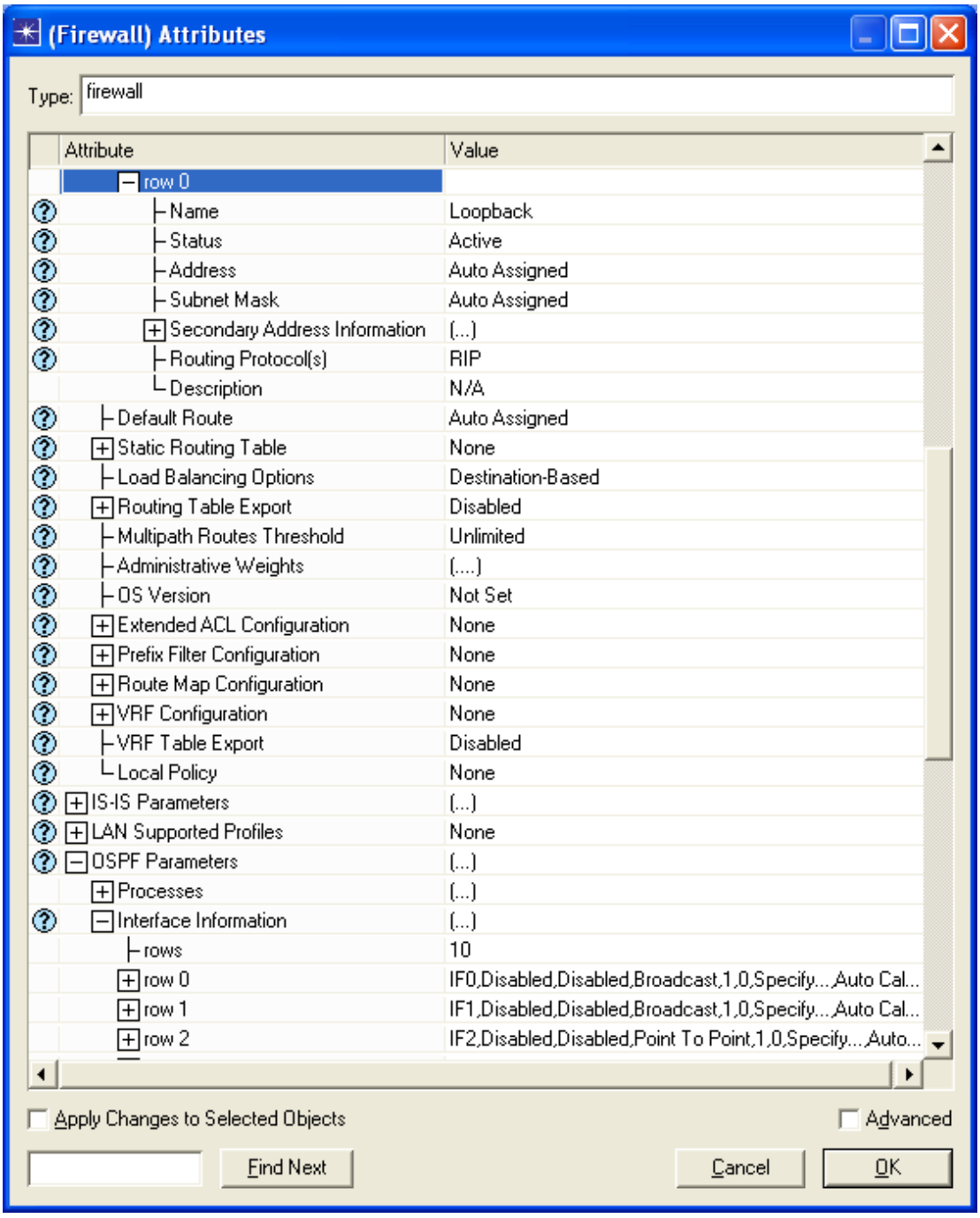


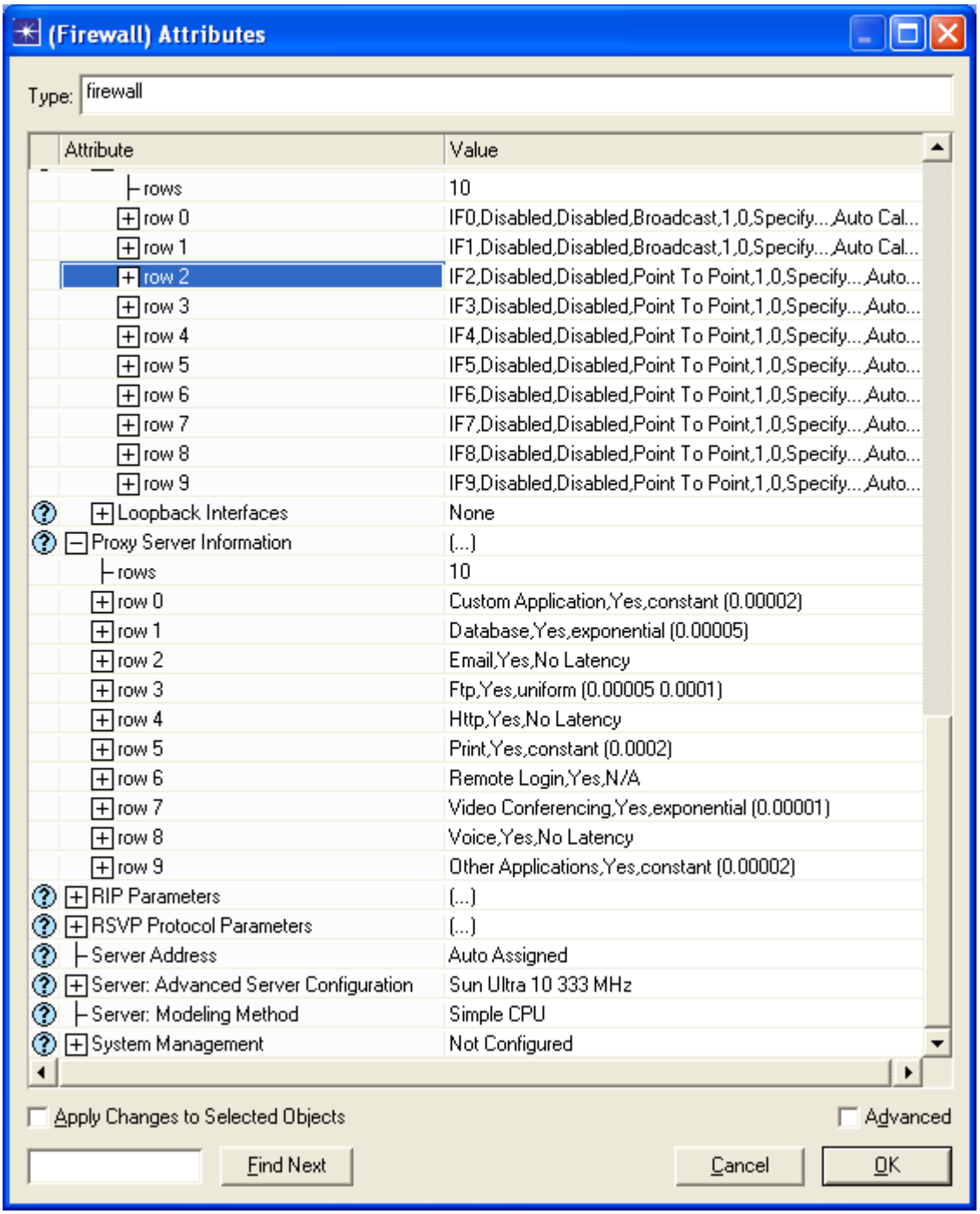
Εικόνα 3-1 The scenario

Qty	Component	Palette	Description
1	ethernet16_switch	internet_toolbox	Switches
2	10BaseT_LAN	internet_toolbox	LAN network models
1	ethernet2_slip8_firewall	internet_toolbox	Routers
1	ip32_cloud	internet_toolbox	Internet model
2	ppp_server	internet_toolbox	EmailAndWebServer DBServer
1	ppp_wkstn	internet_toolbox	MusicAndVideoServer
1	Application Config	internet_toolbox	
1	Profile Config	internet_toolbox	
3	10BaseT	internet_toolbox	Connects the Switch with the Firewalls and the two LANs
1	ppp_adv	links_advanced	Connects the Firewall to the Internet
3	T1	links	Connects the 3 servers to the Internet

Εικόνα 3-2 Components list




(Firewall) Attributes
Type: firewall
Attribute
Value
row 0
Name
Loopback
Status
Active
Address
Auto Assigned
Subnet Mask
Auto Assigned
Secondary Address Information
(...)
Routing Protocol(s)
RIP
Description
N/A
Default Route
Auto Assigned
Static Routing Table
None
Load Balancing Options
Destination-Based
Routing Table Export
Disabled
Multipath Routes Threshold
Unlimited
Administrative Weights
(....)
OS Version
Not Set
Extended ACL Configuration
None
Prefix Filter Configuration
None
Route Map Configuration
None
VRF Configuration
None
VRF Table Export
Disabled
Local Policy
None
IS-IS Parameters
(...)
LAN Supported Profiles
None
OSPF Parameters
(...)
Processes
(...)
Interface Information
(...)
rows
10
row 0
IF0,Disabled,Disabled,Broadcast,1,0,Specify...,Auto Cal...
row 1
IF1,Disabled,Disabled,Broadcast,1,0,Specify...,Auto Cal...
row 2
IF2,Disabled,Disabled,Point To Point,1,0,Specify...,Auto...
Apply Changes to Selected Objects
Advanced
Find Next
Cancel
OK



Εικόνα 3-3 Application Config Attributes

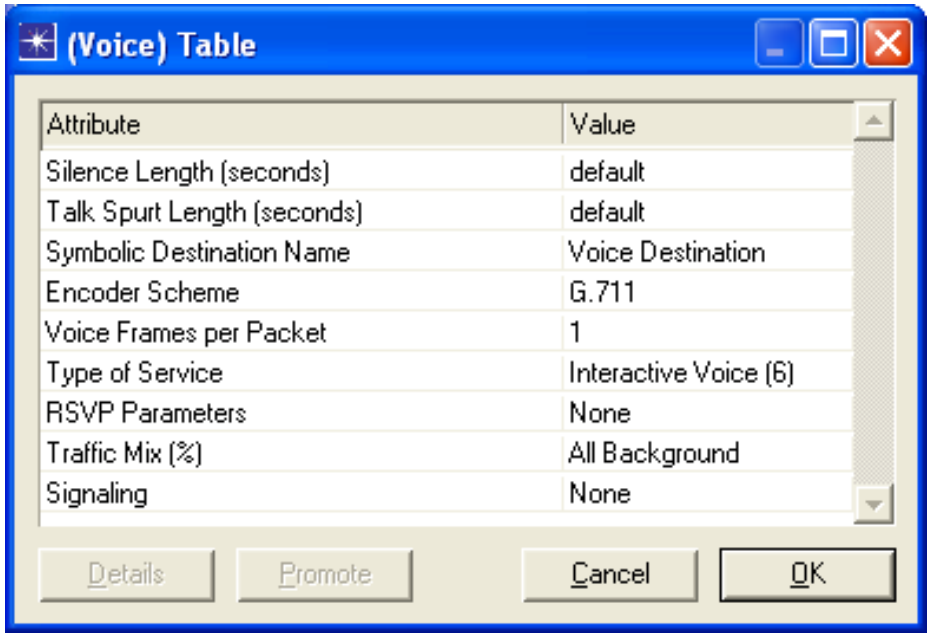
Δεξί Κλικ σε κάθε κόμβο, κλικ στο **Set Name** και γράψτε τα ονόματα όπως φαίνονται στην εικόνα.

3. Ρυθμίστε το **Application Config** control :

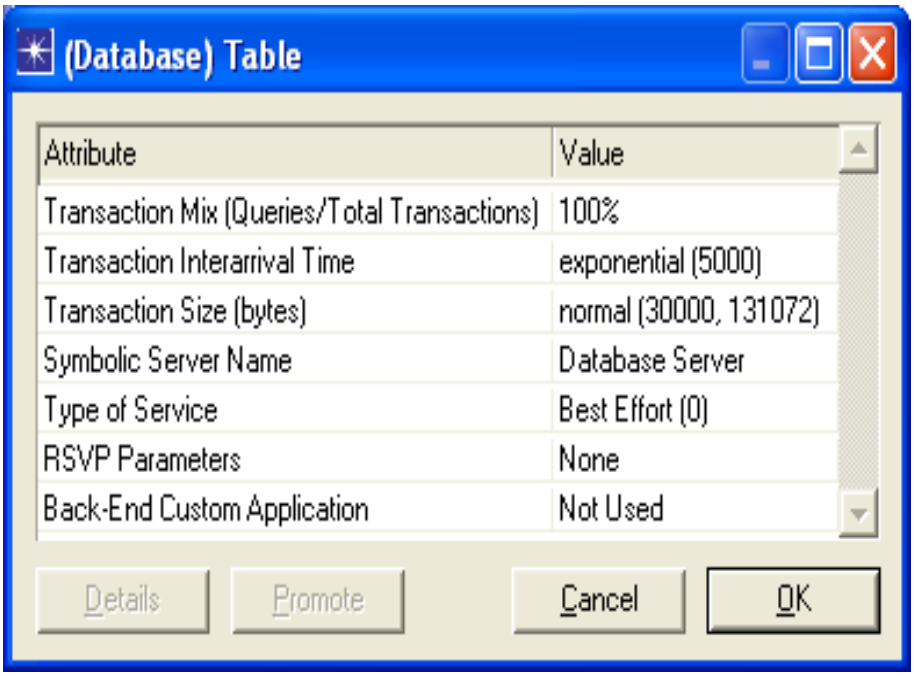
   Επιλέξτε το Application Config control, και πηγαίνετε στο **Edit Attributes**. Το μόνο που πρέπει να τροποποιήσουμε είναι το Application Definitions. Διαγράψτε όλες τις εφαρμογές που μπορεί να υπάρχουν (tip: set **rows**: 0), και δημιουργήστε 4 εφαρμογές όπως φαίνονται όπως φαίνεται στην εικόνα (set **rows**:4 και επεξεργαστείτε τις 4 εφαρμογές όπως φαίνεται στην εικόνα 3.3). Το πρώτο βήμα είναι να αλλαχτεί το όνομα: **Email**, **HTTP**, **DB** και **MusicAndVideo**. Αλλάξτε τα application load αργότερα:

   - HTTP: Permits HTTP (Light Browsing)
   - Email: Permits Email (Low Load)

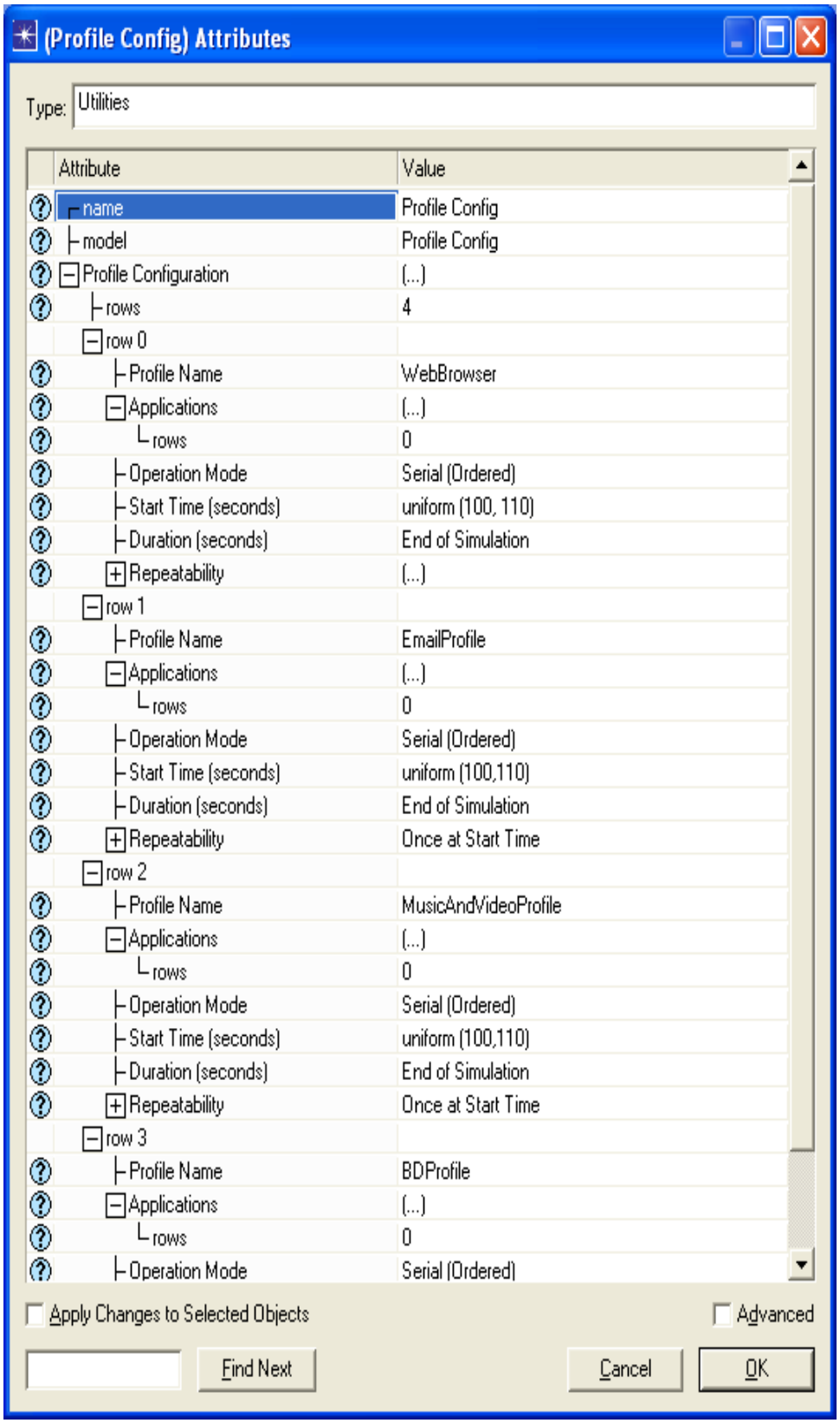
Αυτές οι δύο εφαρμογές μπορούν να διαμορφωθούν αυτόματα κάνοντας διπλό-κλικ στα αντίστοιχα πεδία. Για να διαμορφώσουμε το **MusicAndVideo** και το **DB**, κάνουμε διπλό-κλικ στα πεδία της εικόνας 3.3 που είναι μαρκαρισμένα με το εξής σύμβολο **(...) : DB→ Database, MusicAndVideo→ Voice**, και έπειτα θέστε τις τιμές όπως φαίνονται στην εικόνες 3.4 και 3.5



Εικόνα 3-4 Configuring the application traffic



Εικόνα 3-5 Configuring the application traffic



Εικόνα 3-6 Configuring Profile Config

Επιλέξτε το control **Profile Config** και χρησιμοποιήστε το **σωστό κουμπί** για να κάνετε click στο **Edit Attributes** και να δημιουργήσετε 4 προφίλ(profile):

- **WebBrowser**, για να αναγνωρίσετε την HTTP εφαρμογή
- **EmailProfile**, για να αναγνωρίσετε την email εφαρμογή
- **MusicAndVideoProfile**,γ ια να αναγνωρίσετε την MusicAndVideo εφαρμογή
- **DBProfile**, για να αναγνωρίσετε την DB εφαρμογή

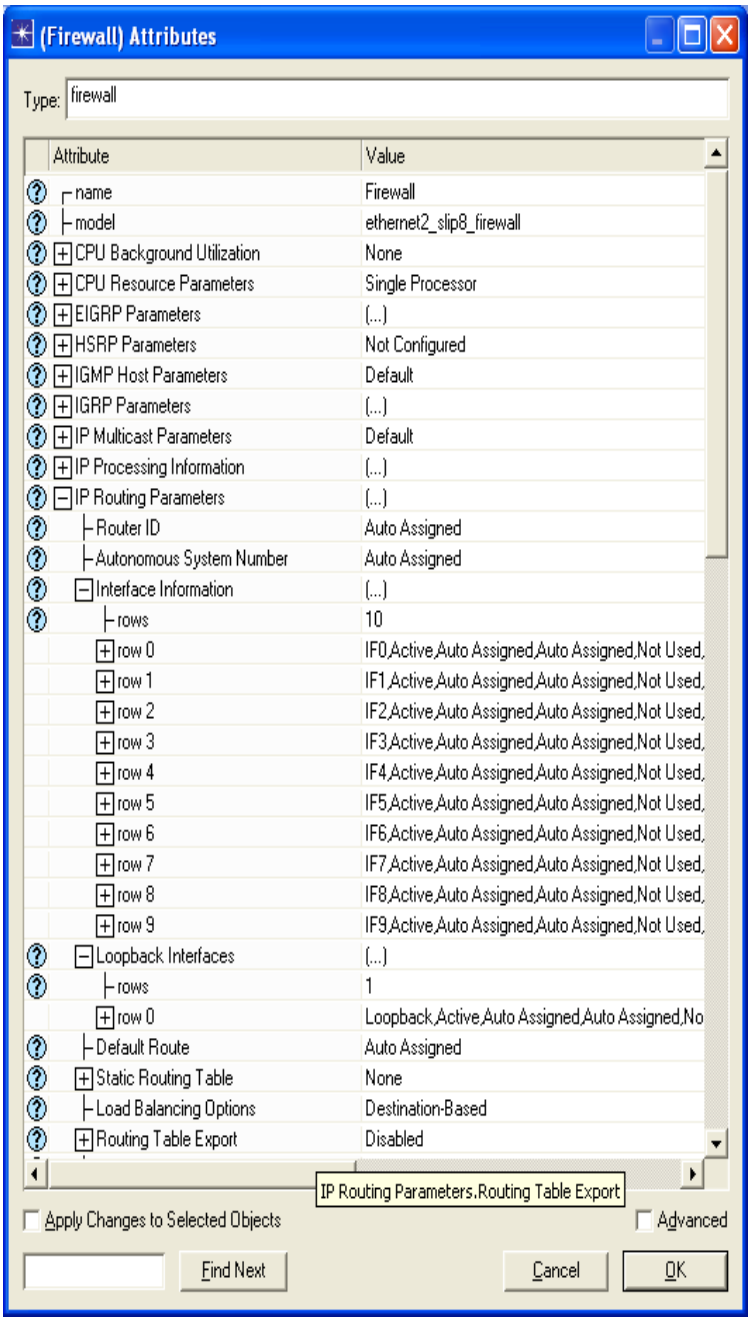
Πρέπει να κάνουμε τα ίδια βήματα όπως πριν: Θέτουμε 0 rows για να σβήσουμε όλα τα rows που μπορεί να έχουμε, και έπειτα θέτουμε 4 rows για να προγραμματίσουμε τις 4 εφαρμογές, επεκτείνουμε κάθε row και θέτουμε τις τιμές όπως φαίνονται στις εικόνες. Οι ιεραρχίες που δεν επεκτείνονται στις εικόνες χρησιμοποιούν τις προκαθορισμένες τιμές. Οι εφαρμογές μπορούν να επισυναφθούν στα σχεδιαγράμματα που προσθέτουν νέα rows στο πεδίο εφαρμογών, και που θέτουν το **όνομα πεδίων** σε κάθε **row 0** του κλάδου εφαρμογών. Μπορούμε επίσης να τροποποιήσουμε τον **χρόνο έναρξης** όλων των εφαρμογών και των σχεδιαγραμμάτων (διανομή λήψης πακέτων), τον **τρόπο λειτουργίας** και το **επαναληπτικό πρότυπο**.

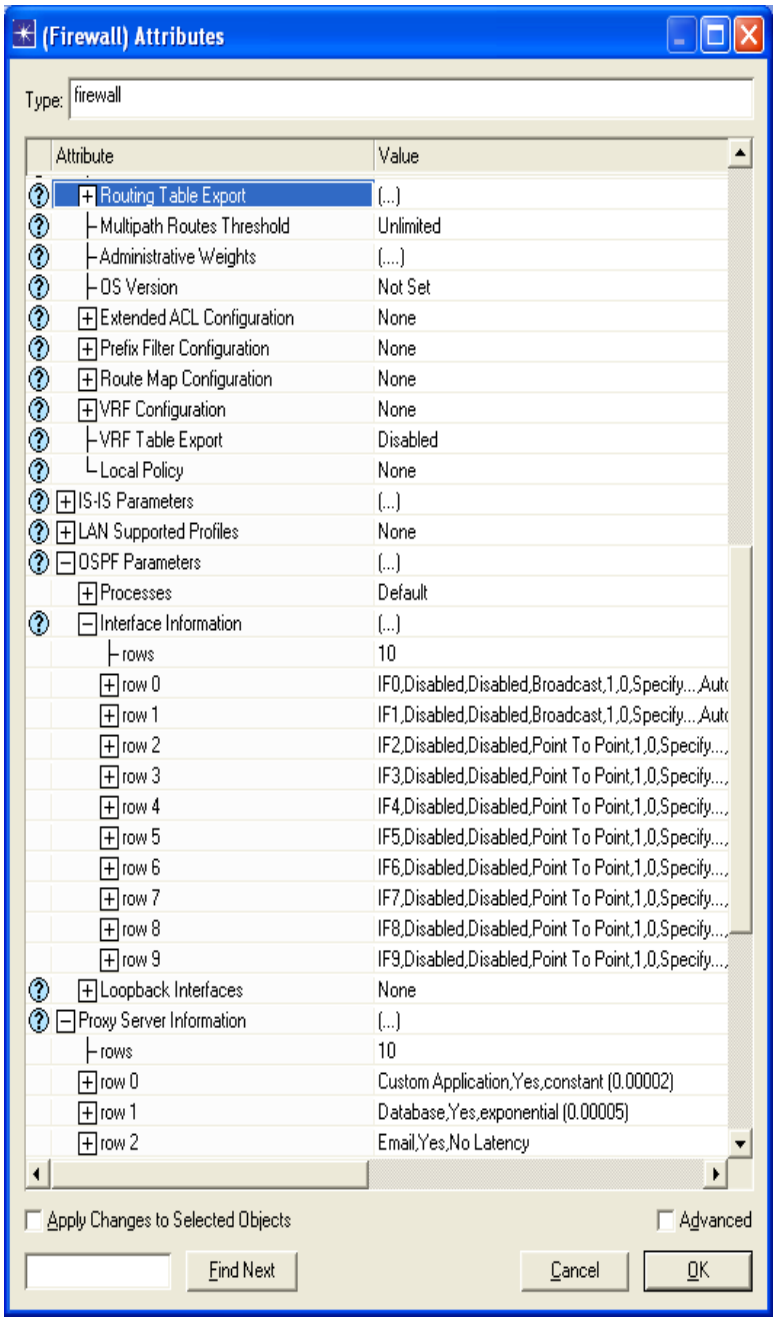
4. Ρυθμίστε το Firewall:

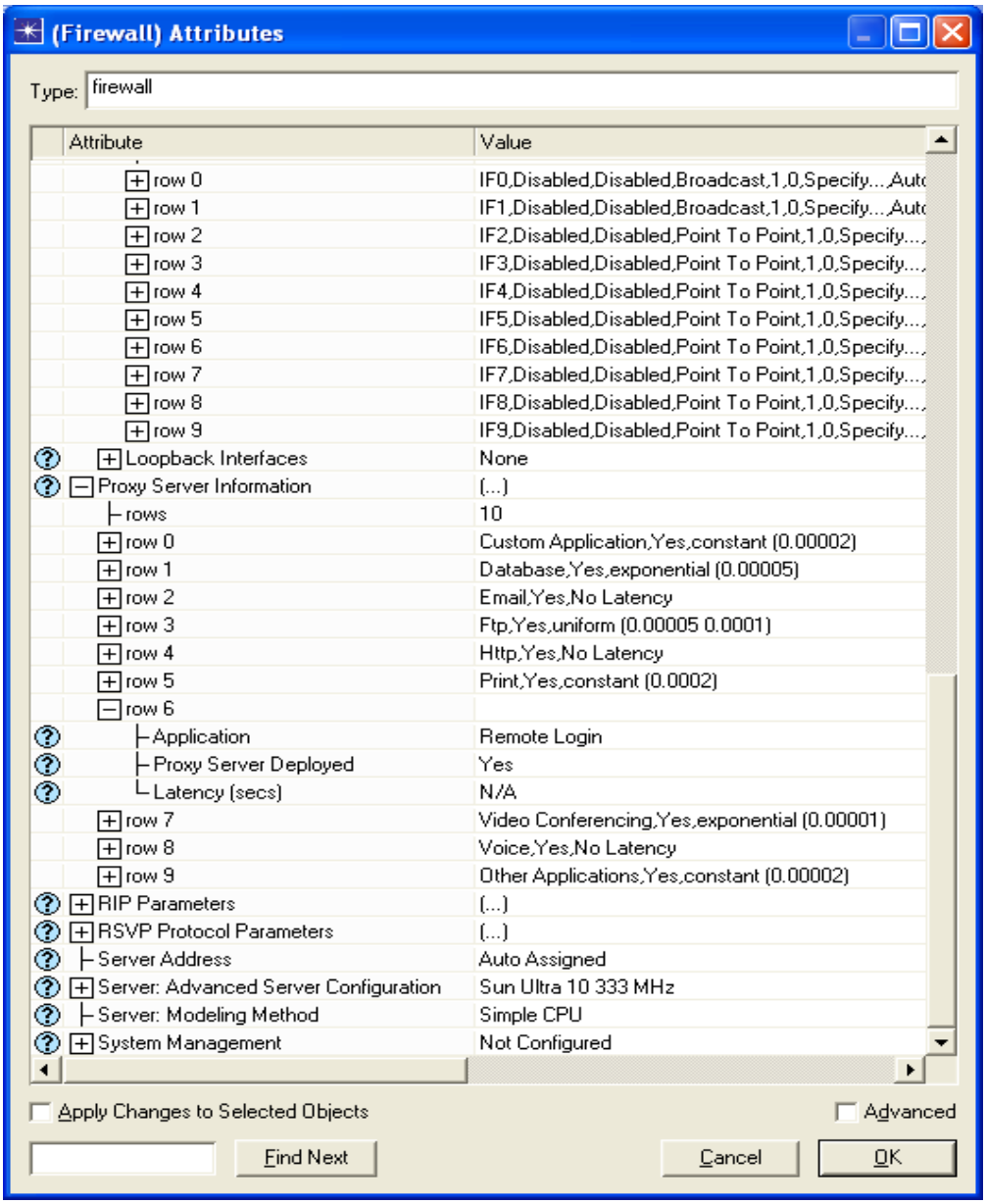
Αυτό το πρώτο σενάριο επιτρέπει την κυκλοφορία φωνής. Η εικόνα 3.7 εμφανίζει βασικές προαιρετικές δυνατότητες για να διαμορφώσετε τον δρομολογητή. Οι ιδιότητες που μεταβάλλονται είναι οι εξής:

- Η διεύθυνση και η μάσκα υποδικτύου: Autoaddressed σε όλα τα rows **IP Routing Parameters→ Interface Information** και **IP Routing Parameters→ Loopback Interfaces**.
- Πρέπει να ρυθμίσουμε το πρωτόκολλο δρομολόγησης OSPF: **OSPF Parameters→ Interface Information→ row 0** και **row 1** (τα μοναδικά interfaces των δρομολογητών)**→ Type: Broadcast**. Ρυθμίστε **Point-to-Point** στο υπόλοιπο(rows 2-9).

Proxy Server Information→ row 6(αντιστοιχεί σε **Application Remote Login,** απαραίτητο για πρόσβαση σε βάση δεδομένων)**→ Proxy Server Deployed: Yes,** αυτό εξασφαλίζει ότι η κυκλοφορία βάσεων δεδομένων έχει το δικαίωμα να περάσει.


(Firewall) Attributes
Type: firewall
Attribute
Value
name
Firewall
model
ethernet2_slip8_firewall
CPU Background Utilization
None
CPU Resource Parameters
Single Processor
EIGRP Parameters
(...)
HSRP Parameters
Not Configured
IGMP Host Parameters
Default
IGRP Parameters
(...)
IP Multicast Parameters
Default
IP Processing Information
(...)
IP Routing Parameters
(...)
Router ID
Auto Assigned
Autonomous System Number
Auto Assigned
Interface Information
(...)
rows
10
row 0
IF0,Active,Auto Assigned,Auto Assigned,Not Used,
row 1
IF1,Active,Auto Assigned,Auto Assigned,Not Used,
row 2
IF2,Active,Auto Assigned,Auto Assigned,Not Used,
row 3
IF3,Active,Auto Assigned,Auto Assigned,Not Used,
row 4
IF4,Active,Auto Assigned,Auto Assigned,Not Used,
row 5
IF5,Active,Auto Assigned,Auto Assigned,Not Used,
row 6
IF6,Active,Auto Assigned,Auto Assigned,Not Used,
row 7
IF7,Active,Auto Assigned,Auto Assigned,Not Used,
row 8
IF8,Active,Auto Assigned,Auto Assigned,Not Used,
row 9
IF9,Active,Auto Assigned,Auto Assigned,Not Used,
Loopback Interfaces
(...)
rows
1
row 0
Loopback,Active,Auto Assigned,Auto Assigned,No
Default Route
Auto Assigned
Static Routing Table
None
Load Balancing Options
Destination-Based
Routing Table Export
Disabled
IP Routing Parameters.Routing Table Export
Apply Changes to Selected Objects
Advanced
Find Next
Cancel
OK

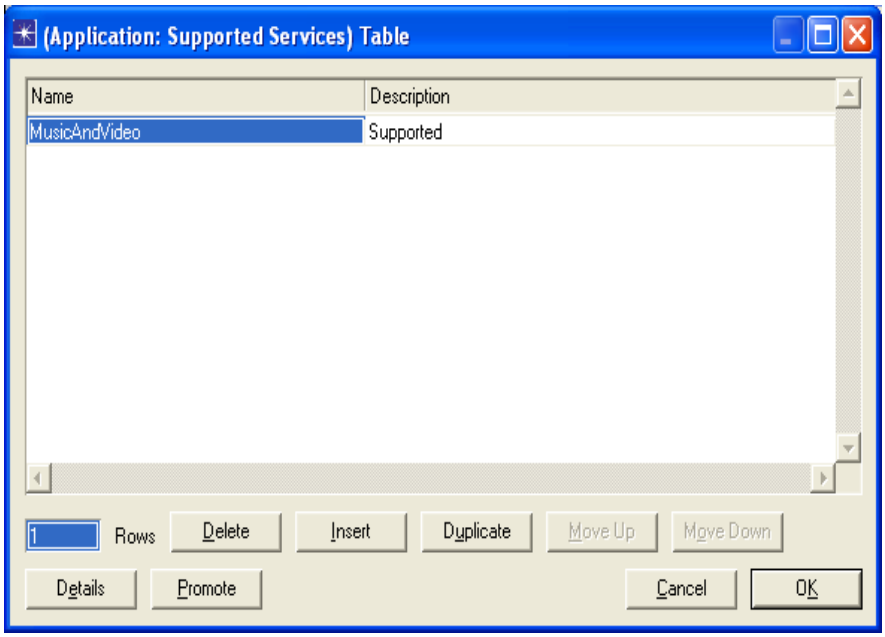

(Firewall) Attributes
Type: firewall
Attribute
Value
Routing Table Export
(...)
Multipath Routes Threshold
Unlimited
Administrative Weights
(....)
OS Version
Not Set
Extended ACL Configuration
None
Prefix Filter Configuration
None
Route Map Configuration
None
VRF Configuration
None
VRF Table Export
Disabled
Local Policy
None
IS-IS Parameters
(...)
LAN Supported Profiles
None
OSPF Parameters
(...)
Processes
Default
Interface Information
(...)
rows
10
row 0
IF0,Disabled,Disabled,Broadcast,1,0,Specify...,Auto
row 1
IF1,Disabled,Disabled,Broadcast,1,0,Specify...,Auto
row 2
IF2,Disabled,Disabled,Point To Point,1,0,Specify...,
row 3
IF3,Disabled,Disabled,Point To Point,1,0,Specify...,
row 4
IF4,Disabled,Disabled,Point To Point,1,0,Specify...,
row 5
IF5,Disabled,Disabled,Point To Point,1,0,Specify...,
row 6
IF6,Disabled,Disabled,Point To Point,1,0,Specify...,
row 7
IF7,Disabled,Disabled,Point To Point,1,0,Specify...,
row 8
IF8,Disabled,Disabled,Point To Point,1,0,Specify...,
row 9
IF9,Disabled,Disabled,Point To Point,1,0,Specify...,
Loopback Interfaces
None
Proxy Server Information
(...)
rows
10
row 0
Custom Application,Yes,constant (0.00002)
row 1
Database,Yes,exponential (0.00005)
row 2
Email,Yes,No Latency
Apply Changes to Selected Objects
Advanced
Find Next
Cancel
OK



Εικόνα 3-7 Configuring the Firewall

5. Ρυθμίζοντας το MusicAndVideoServer:

Δεξί κλικ στο MusicAndVideoServer και κάντε κλικ στο **Edit Attributes**.
Πρέπει να τροποποιήσουμε την εφαρμογή: **Supported Services**, ρυθμίζοντας τις παραμέτρους όπως φαίνεται στην παρακάτω εικόνα(πρέπει να ρυθμίσουμε τα rows: 1 για να αποδεχθούμε το MusicAndVideo). Αφήστε τις προαιρετικές επιλογές στις προκαθορισμένες τιμές.



Εικόνα 3-8 MusicAndVideoServer supported Services

6. Ρυθμίστε τον DBServer και τον WebAndEmailServer:

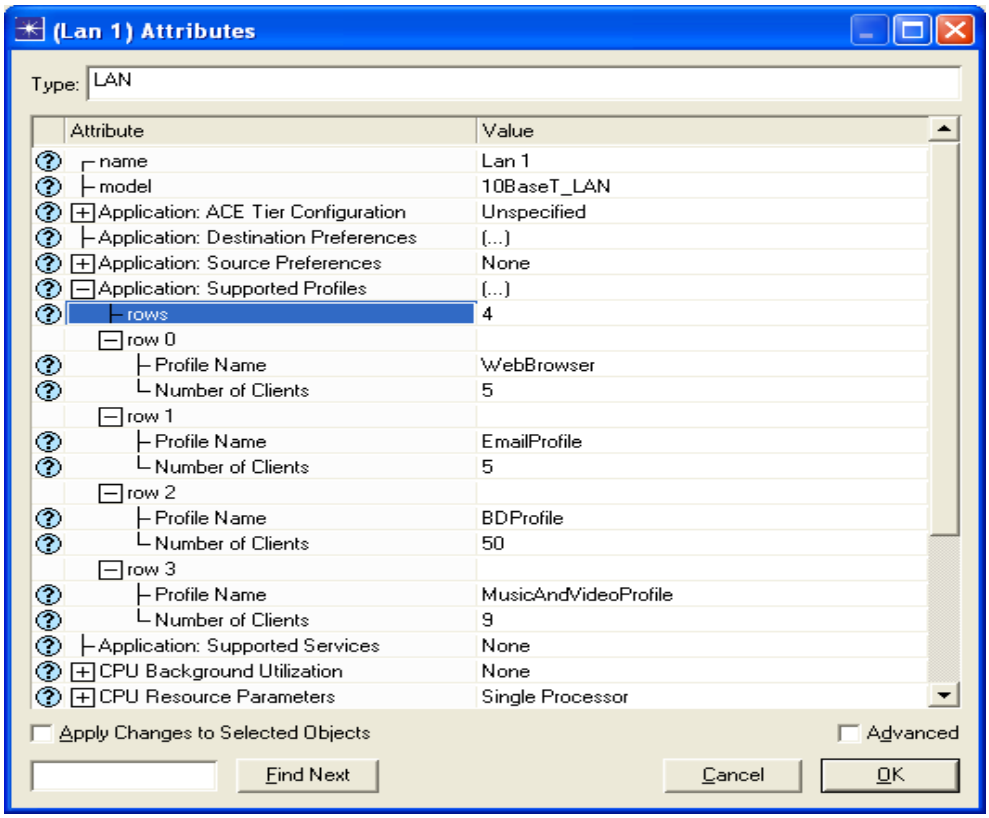
Ο κεντρικός υπολογιστής **Supported Services** πρέπει να ρυθμιστεί όπως φαίνεται στην παρακάτω εικόνα:

Server	**Supported Services**
DBServer	DB
WebAndEmailServer	HTTP Email

Εικόνα 3-9 Supported Services

7. Διαμορφώστε τα LANs:

Επιλέξτε το **LAN 1** κάνοντας κλικ σε αυτό, και μετά το σωστό **button→ Edit Attributes**. Χρησιμοποιήστε τις τιμές από την εικόνα 3.10 (μη επεκταμένοι κλάδοι χρησιμοποιούν τις προκαθορισμένες παραμέτρους). Αυτή η διαμόρφωση θα χρησιμοποιήσει 250 τερματικούς σταθμούς για το κάθε τοπικό LAN (**αριθμός τερματικών σταθμών**), 5 από αυτούς θα κάνουν web browsing, 5 θα χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο, 50 προσπαθούν να συνδεθούν στην βάση δεδομένων και οι 9 χρησιμοποιούν MusicAndVideoServers παράνομα(**Εφαρμογή: Supported Profiles**). Όταν τελειώσετε κάντε κλικ στο **OK**.



Εικόνα 3-10 Assigning profiles to workstations at LAN 1

Το τοπικό LAN 2 θα διαμορφωθεί με τις ίδιες τιμές. Χρησιμοποιήστε την αντιγραφή και επικόλληση για να αναπαράγετε το τοπικό LAN και για να αλλάξετε το όνομα κατόπιν.

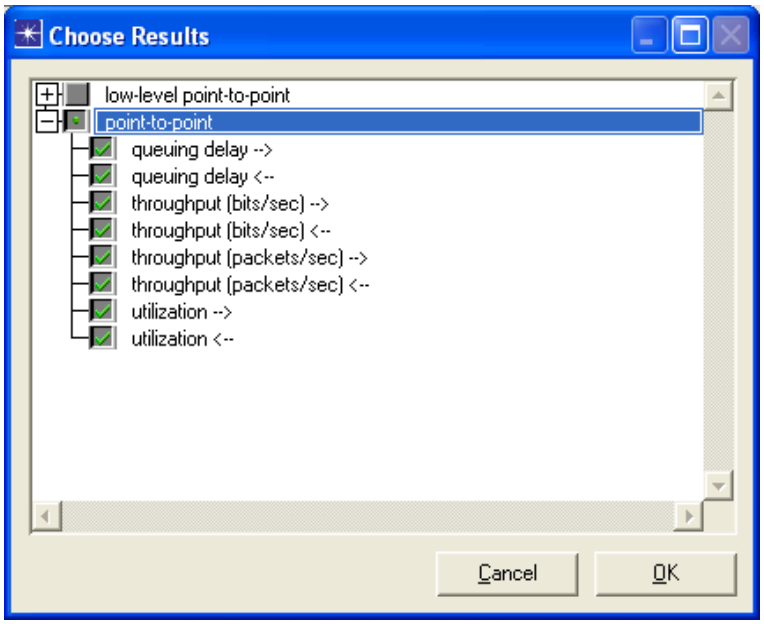
8. Διαμόρφωση σύνδεσης μεταξύ διαδικτύου και firewall :

Δεξί κλικ στην σύνδεση και μετά **Edit Attributes** και ρυθμίστε το εξής **Data Race: T1**.

9. Διαμόρφωση των στατιστικών προσομοίωσης:

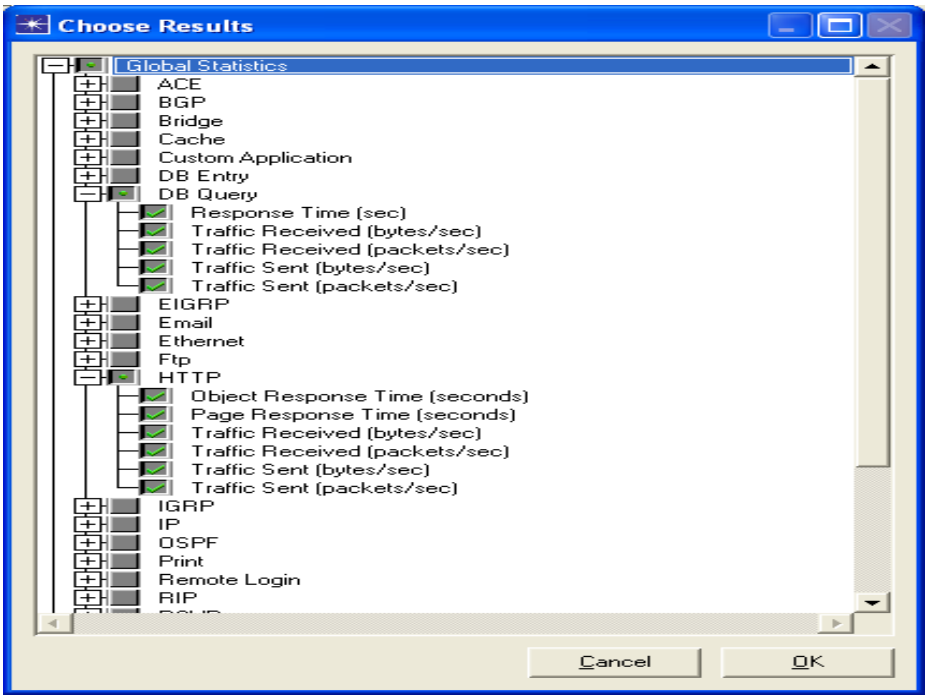
Οι παράμετροι στατιστικής απόδοσης και ο ρυθμός απόδοσης μπορούν να δώσουν ενδιαφέρουσες πληροφορίες όπως και το DB Query Delay:

Δεξί κλικ στην σύνδεση Internet-Firewall→ **Choose Individual Statistics** και μαρκάρετε τα checkbox όπως φαίνεται στην εικόνα 3.11. Κάντε κλικ στο **OK**.



Εικόνα 3-11 Internet-Firewall link statistics

- Προκειμένου να επιλεχθούν οι στατιστικές προσομοίωσης DB Query, κάνουμε **δεξί κλικ** οπουδήποτε στο πλέγμα εκτός από κάποιον κόμβο, και επιλέγουμε **Choose Individual Statistics** και τσεκάρουμε τα πεδία όπως φαίνεται στην εικόνα 3.12.Κάνουμε κλικ στο **OK**.



Εικόνα 3-12 Global statics

Για να ελέγξετε όλες τις στατιστικές των παιδιών ενός κόμβου-πατέρα, κάντε κλικ στον κόμβο-πατέρα και έπειτα όλα τα παιδιά των κόμβων θα είναι τσεκαρισμένα (marked).

10. Διαμόρφωση της προσομοίωσης:

Από τον επεξεργαστή προγράμματος, κάντε κλικ στο **configure/run simulation**  , και ρυθμίστε το εξής: **Duration: 1 hour(s).** Μην ξεκινήσετε την προσομοίωση ακόμα.

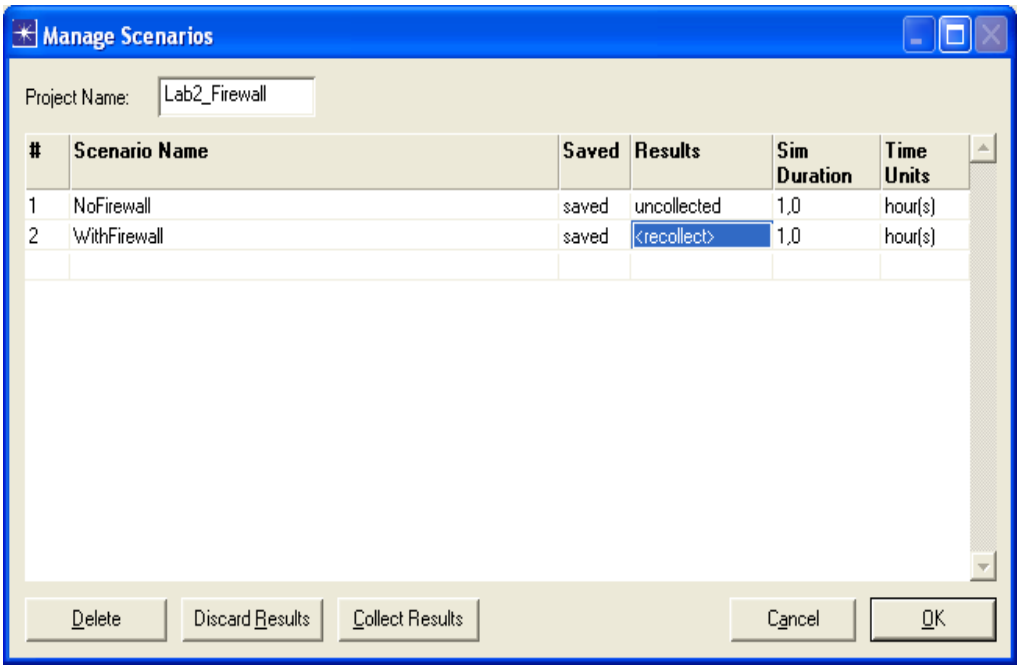
3.4.2 Δημιουργία του Δεύτερου Σεναρίου

Το δεύτερο σενάριο είναι ένα αντίγραφο του πρώτου, αλλά με μερικούς κανόνες δρομολογητών που αποφεύγουν τα ιδιαίτερα πακέτα από και προς τις υπηρεσίες μουσικής και δεδομένων. Αργότερα θα δούμε πώς αυτό μειώνει το ρυθμό απόδοσης της σύνδεσης του διαδικτύου και τον χρόνο σύνδεσης στην βάση δεδομένων αρκετά κάτω από 1 δευτερόλεπτο του ορίου.
Από τον **επεξεργαστή κειμένου**, **Scenarios→ Duplicate Scenario…**Μετονομάστε το νέο σενάριο σε**: WithFirewall**, και κάντε **δεξί κλικ** στο **Firewall** και μετά **Edit Attributes.** Αφήστε όλες τις τιμές όπως έχουν, εκτός από το εξής: **Proxy Server Information→ row 8(Application Voice** data**)**, χρησιμοποιώντας **Proxy Server Deployed: No.**

3.5 Ανάλυση Αποτελεσμάτων

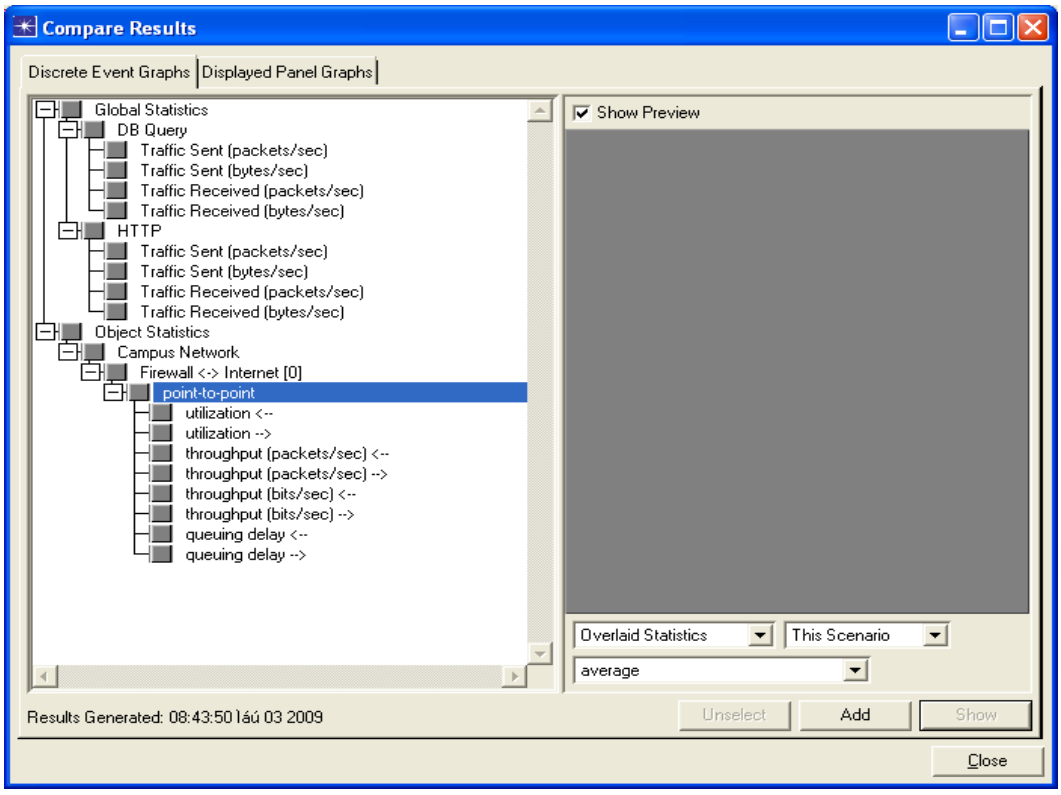
Τρέξτε όλες τις προσομοιώσεις, και ρίξτε μια ματιά στη γραφική παράσταση:

1. Στον **επεξεργαστή κειμένου, Scenarios→ Manage Scenarios…**και διαμορφώστε τις παραμέτρους προσομοίωσης όπως φαίνεται στην εικόνα, θέτοντας **<collect>** στο **Results** row και στα δύο σενάρια(χρησιμοποιήστε **<recollect>** εάν δεν είναι η πρώτη φορά που τρέχετε την προσομοίωση). Κάντε κλικ στο **OK**.



Εικόνα 3-13 Manage Scenarios

2. Συγκρίνετε τον **χρόνο απόκρισης του DB Query**, κάνοντας **δεξί κλικ** στο πλέγμα σε οποιοδήποτε σενάριο και **συγκρίνετε τα αποτελέσματα**. Τώρα μπορούμε να ξεφυλλίσουμε όλες τις γενικές στατιστικές που προγραμματίσαμε προηγουμένως στην αριστερή μεριά του δέντρου. Ελέγξτε ότι οι overlaid στατιστικές, όλα τα σενάρια και οι μέσες προαιρετικές δυνατότητες είναι επιλεγμένες.



Εικόνα 3-14 Compare Results

3.6 Ερωτήσεις

3.6.1 Ερώτηση 1η

Συγκρίνετε το χρόνο απόκρισης του DB Query(sec). Μπορείτε να δείτε μια σημαντική βελτίωση όταν εφαρμόζεται το Firewall στο proxy? Τηρούμε την ευαισθησία(threshold) 1 sec?

3.6.2 Ερώτηση 2η

Συγκρίνετε τον από σημείο σε σημείο ρυθμό απόδοσης(packets/sec) σε οποιαδήποτε κατεύθυνση της σύνδεσης διαδίκτυο-firewall. Πώς είναι το μη-παράνομο αποτελεσματικό εύρος ζώνης εφαρμογών που επηρεάζεται από το proxy?

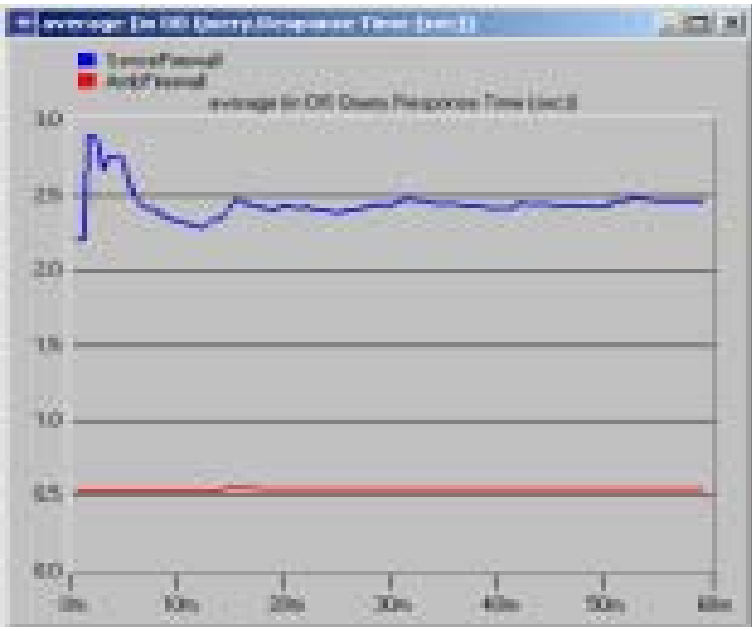
3.6.3 Ερώτηση 3η

Συγκρίνετε τη χρησιμοποίηση της ίδιας σύνδεσης. Ποιές αλλαγές εκτιμάτε?

3.7 Απαντήσεις

3.7.1 Απάντηση 1η

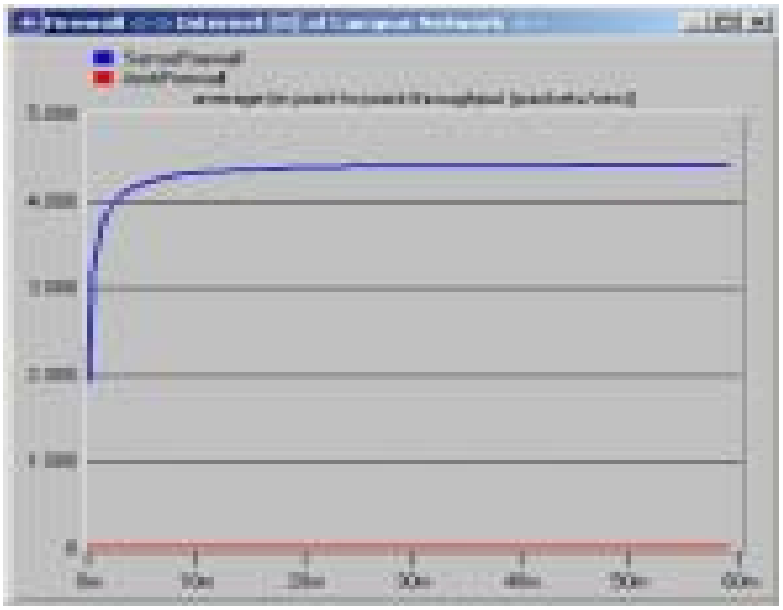
Ο χρόνος απόκρισης του DB Query ήταν ιλιγγιώδης υψηλός σε 2,5 δευτερόλεπτα, και μειώθηκε σε 0,5 δευτερόλεπτα όταν το proxy ήταν ανοικτό λόγω ενός αποτελεσματικού καθαρού κέρδους εύρους ζώνης, σημαντικά κάτω από 1 δευτερόλεπτο ευαισθησία (threshold).



Εικόνα 3-15 Average DB Query Response Time

3.7.2 Απάντηση 2η

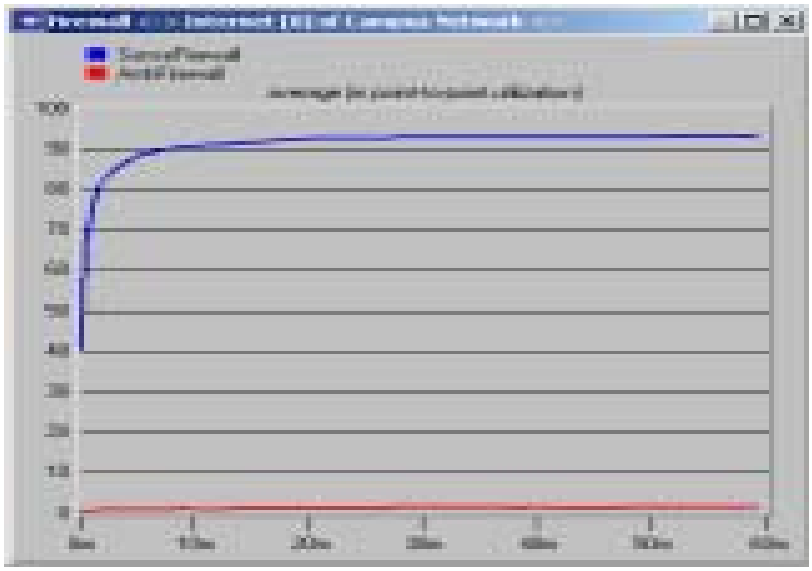
Είναι αξιοπρόσεκτη η μεγάλη ποσότητα πακέτων ανά δευτερόλεπτο που υπήρχε όταν η κυκλοφορία πολυμέσων επιτράπηκε(περίπου 4.500), και ο τρόπος που αυτή μειώθηκε σε μια ανεξήγητη τιμή όταν η κυκλοφορία αποτράπηκε. Το εύρος ζώνης ήταν απολύτως κορεσμένο.



Εικόνα 3-16 Average point-to-point throughput of the link

3.7.3 Απάντηση 3η

Το βασικό μέρος της κυκλοφορίας των δικτύων ήταν η κυκλοφορία της φωνής, αλλά αυτό που δεν ξέραμε ήταν ότι αυτό επιβάρυνε την απόδοση της σύνδεσης του διαδικτύου. Όταν το proxy είναι ανοικτό η χρησιμοποίηση φθάνει σχεδόν το 0%.



Εικόνα 3-17 Average utilization of the link

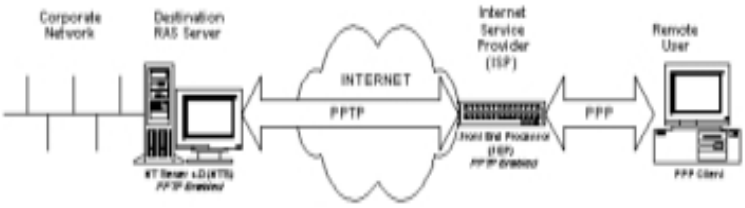
Chapter 4 VPN

4.1 Εισαγωγή

Το Point-to-Point Tunneling Protocol[10] (PPTP) είναι ένα σύνολο κανόνων επικοινωνίας που επιτρέπουν σε έναν οργανισμό να επεκτείνει το εταιρικό του δίκτυο χρησιμοποιώντας ιδιωτικά tunnels μέσω ενός δημόσιου δικτύου ως Διαδίκτυο. Κατά συνέπεια, οι χρήστες έχουν ίδια εντύπωση σαν να λειτουργούσαν σε ένα δικό τους WAN[11], και δεν χρειάζεται να μισθώσουν μια ιδιωτική γραμμή επικοινωνίας. Ωστόσο η ασφάλεια εξασφαλίζεται σε ένα μη-ασφαλές δίκτυο όπως το Διαδίκτυο. Αυτό το είδος σύνδεσης είναι ένα Ιδιωτικό Εικονικό Δίκτυο (Virtual Private Network ή VPN[12]).
Το PPTP είναι μια επέκταση του PPP πρωτοκόλλου (Point-to-Point Protocol).
Οι χρήστες μπορούν να χρησιμοποιήσουν έναν ISP Provider για να συνδεθούν με έναν κεντρικό υπολογιστή του οργανισμού, στο Διαδίκτυο.
Τα VPNs χρησιμοποιούν IP tunnels[13] (tunneling), point-to-point συνδέσεις μεταξύ οποιονδήποτε δύο σταθμών. Η εικονική σύνδεση δημιουργείται στο δρομολογητή εισόδου, όταν δίνεται η IP διεύθυνση προορισμού. Όταν ο δρομολογητής εισόδου θέλει να μεταδώσει ένα IP πακέτο χρησιμοποιώντας την εικονική σύνδεση, τοποθετεί το πακέτο σε ένα IP διάγραμμα δεδομένων. Οι διευθύνσεις πηγής και προορισμού του IP διαγράμματος δεδομένων είναι αυτές μεταξύ των δρομολογητών, που κάνουν την τοποθέτηση και την αφαίρεση.
Ένας PPP client χρήστης θα εγκαθιδρύσει μια κλήση με έναν ISP[14] (Internet Service Provider ή φορέα παροχής υπηρεσιών διαδικτύου),the Front End Processor (FEP[15]). Επίσης εξασφαλίζεται η ασφάλεια. Το FEP και ο PPP client θα συνεργαστούν σε ένα VPN tunnel με έναν απομακρυσμένο PPTP κεντρικό υπολογιστή (Remote Access Server, RAS[16]). Τα δύο peers είναι η πηγή Tunnel και ο προορισμός Tunnel. Ο προορισμός Tunnel είναι πάντα ένας απομακρυσμένος κεντρικός υπολογιστής PPTP.
Ένα VPN δίκτυο μπορεί να βρίσκεται σε 2 καταστάσεις :

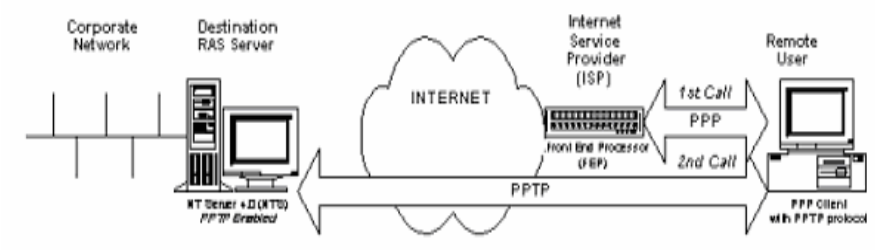
[10] http://en.wikipedia.org/wiki/PPTP
[11] http://en.wikipedia.org/wiki/Wide_Area_Network
[12] http://en.wikipedia.org/wiki/Virtual_private_network
[13] http://en.wikipedia.org/wiki/IP_tunnel
[14] http://en.wikipedia.org/wiki/Internet_service_provider
[15] http://en.wikipedia.org/wiki/Front_end_processor
[16] http://en.wikipedia.org/wiki/Remote_Access_Server

- **Με την πηγή Tunnel στο FEP**



Εικόνα 4-1 Με την πηγή Tunnel στο FEP

- **Με την πηγή Tunnel στο PPP Client**



Εικόνα 4-2 Με την πηγή Tunnel στο PPP Client

Οπωσδήποτε, τα tunneled δεδομένα έχουν τοποθετηθεί μέσα στο διάγραμμα δεδομένων στον προορισμό. Το παράδειγμα στην εικόνα δείχνει την επικοινωνία χρησιμοποιώντας το πρώτο σχέδιο. Μπορούμε να δούμε πως ο client στέλνει τα μηνύματα PPP στο FEP. Κατά την διάρκεια ολόκληρης της διαδικασίας ο client νομίζει ότι έχει μια PPP σύνδεση με τον κεντρικό υπολογιστή PPTP στην άλλη πλευρά.
Στο δεύτερο σχέδιο, η τοποθέτηση γίνεται στον PPTP Client .

4.2 Περιγραφή Σεναρίου

Μια εταιρεία με γραφεία χρησιμοποιεί VPNs δίκτυα σε μερικές ευρωπαϊκές χώρες για να επιτύχει την ασφάλεια επικοινωνίας κατά την διάρκεια επικοινωνίας με την κεντρική περιοχή, και για να χρησιμοποιήσει επίσης την υποδομή Διαδικτύου, προκειμένου να πετύχει χαμηλότερο κόστος. Αυτό το σχέδιο επικοινωνίας έχει το Tunnel Source στο FEP.

4.3 Δημιουργία του Σεναρίου

1. Ανοίξτε ένα καινούργιο Project στο OPNET IT Guru Academic Edition (**File→ New Project**) χρησιμοποιώντας τις παρακάτω παραμέτρους (αφήστε σε default κατάσταση τις υπόλοιπες τιμές).

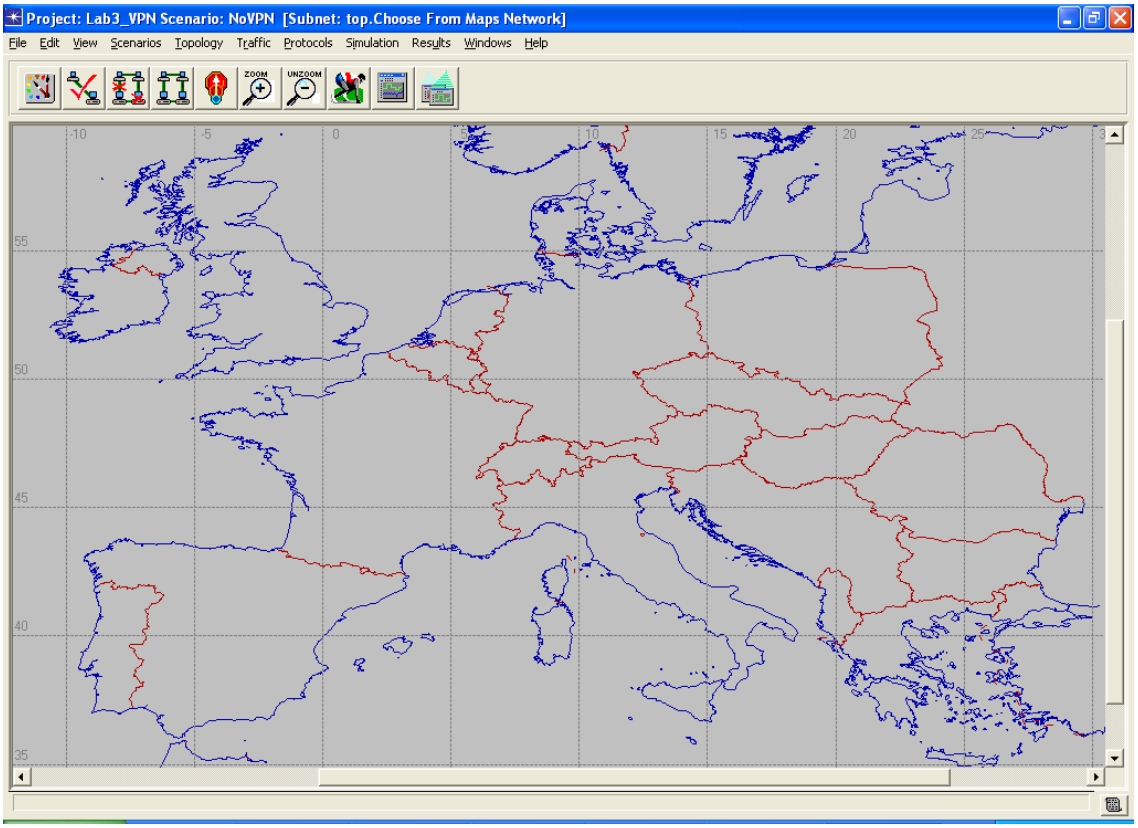
    - **Project Name: <your_name>_VPN**

- **ScenarioName: NoVPN**
- **Network Scale: Choose From Maps.** Επιλέξτε το χάρτη της **Ευρώπης.**

Πιέστε **Next** αρκετές φορές μέχρι να τελειώσει το Startup Wizard. Ο Project Editor θα προωθηθεί σε ένα κενό πλέγμα.

Μόλις εμφανιστεί ο **Project Editor,** μπορείτε να χρησιμοποιήσετε το **Zoom** + 

κουμπί για να μεγιστοποιήσετε το παράθυρο με το χάρτη, όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 4-3 The Map

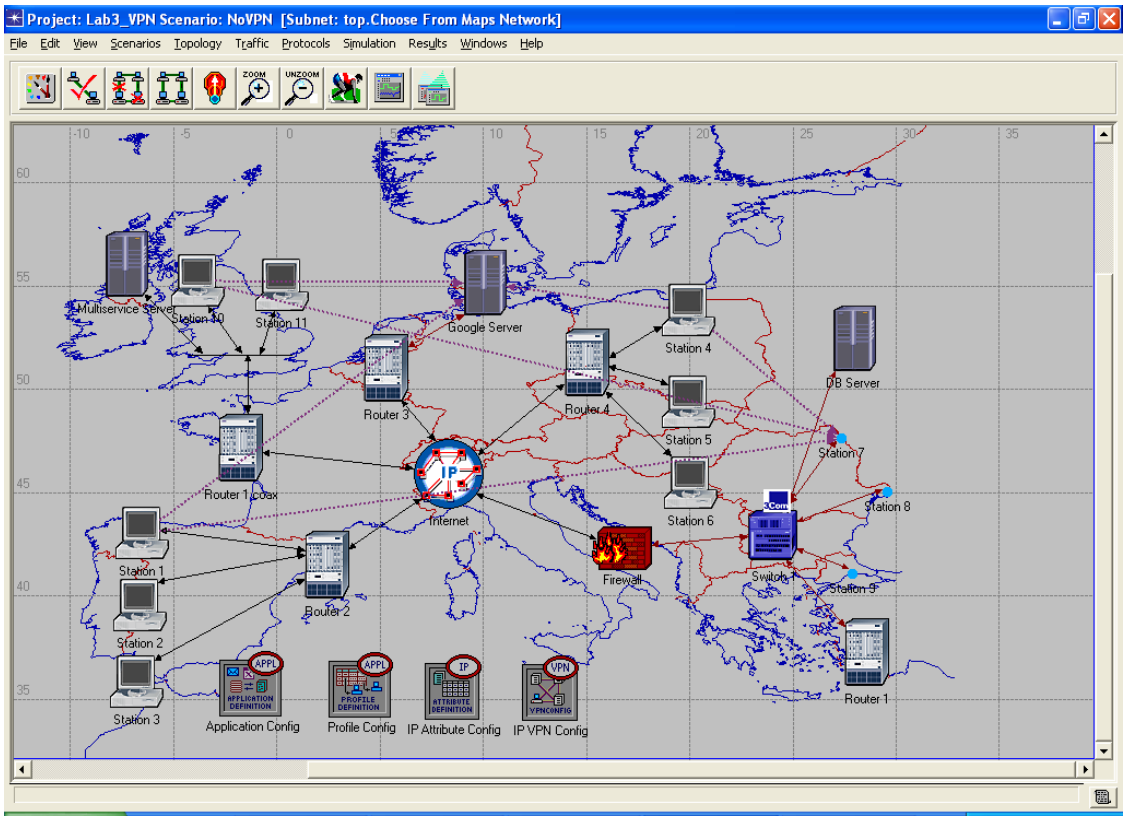
2. Καθορίζοντας τις συσκευές και τις ρυθμίσεις του σεναρίου:

   Τοποθετήστε τα components επάνω στο πλέγμα, όπως φαίνεται στον παρακάτω πίνακα:

Qty	Component	Palette	Label
4	ethernet4_slip8_gtwy	internet_toolbox	Router 2…4. Network Server
1	ethernet2_slip8_firewall	internet_toolbox	Firewall
1	ip32_cloud	internet_toolbox	Internet
1	Application Config	internet_toolbox	Application Config
1	Profile Config	internet_toolbox	Profile Config
1	IP Attribute Config	internet_toolbox	IP Attribute Config
2	ethernet_server	internet_toolbox	Google, DB Server
7	100BaseT	links	
11	PPP_DS1	links	
6	ppp_wkstn	internet_toolbox	Station 1..6
1	eth_coax	ethcoax	Coaxial Wire (buses)
2	ethcoax_wkstn	ethcoax	Station 10 και 11
1	ethcoax_server	ethcoax	Multiservice Server
4	eth_tap	ethcoax	
1	ethcoax_slip8_gtwy_adv	routers_advanced	Router 1 (coax)
3	Sm_Int_wkstn	Sm_Int_Model_List	Station 7..9
1	3C_SSII_1100_3300_4s_ae52_e48_ge3	3 Com	Switch 1
1	IP VPN Config	utilities	IP VPN Config

Εικόνα 4-4 Components of the network

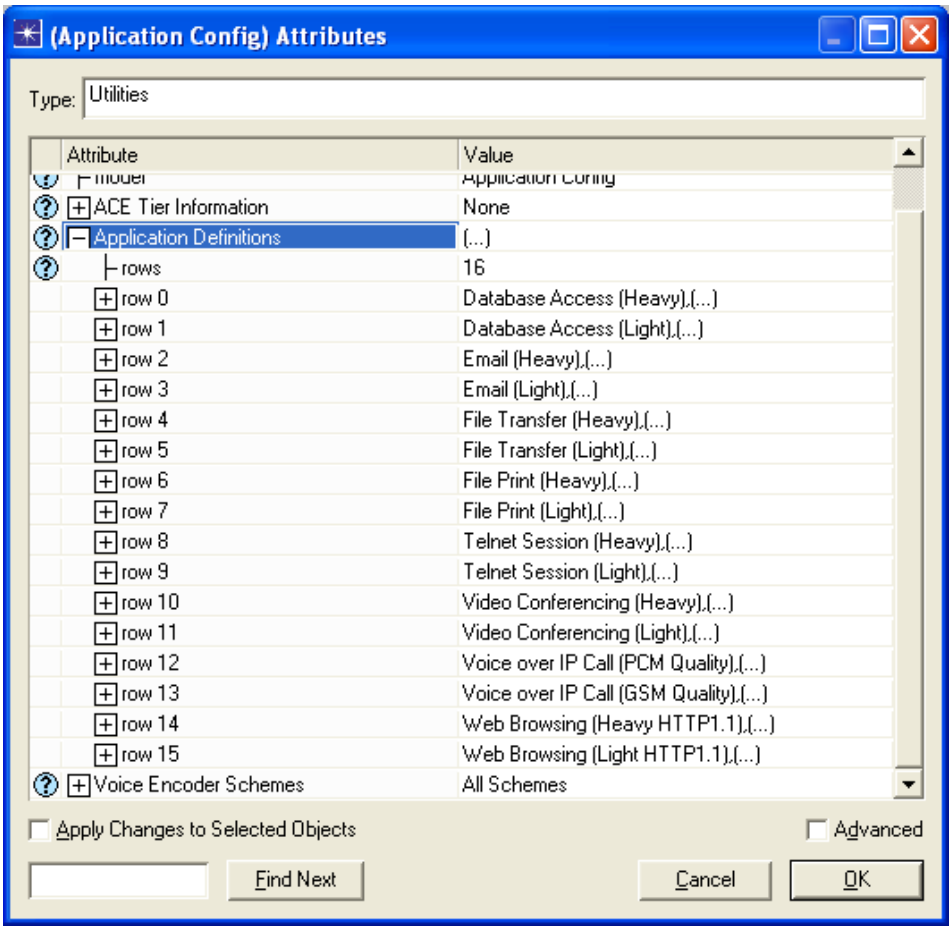
Η εικόνα **4.5** μας δείχνει το δίκτυο που δημιουργείται από τα components που μόλις αναφέραμε. Χρησιμοποιήστε τα ίδια ονόματα(**Δεξί κλικ→ Μετονομασία**), γιατί θα αναφερόμαστε στα components με τα ονόματα που μόλις δώσαμε από εδώ και στο εξής.



Εικόνα 4-5 The scenario

3. Καθορίστε τις εφαρμογές, τα profiles και τις απαιτήσεις κυκλοφορίας:

- Δεξί κλικ στο **Application Config control** και μετά κλικ στο **Edit Attributes**. Επιλέξτε **Application Definitions: Default**. Αυτό θα δημιουργήσει 8 νέες εφαρμογές χρησιμοποιώντας heavy και light modes. Κατόπιν κάντε κλικ στο **OK**.



Εικόνα 4-6 Application Definitions: Default

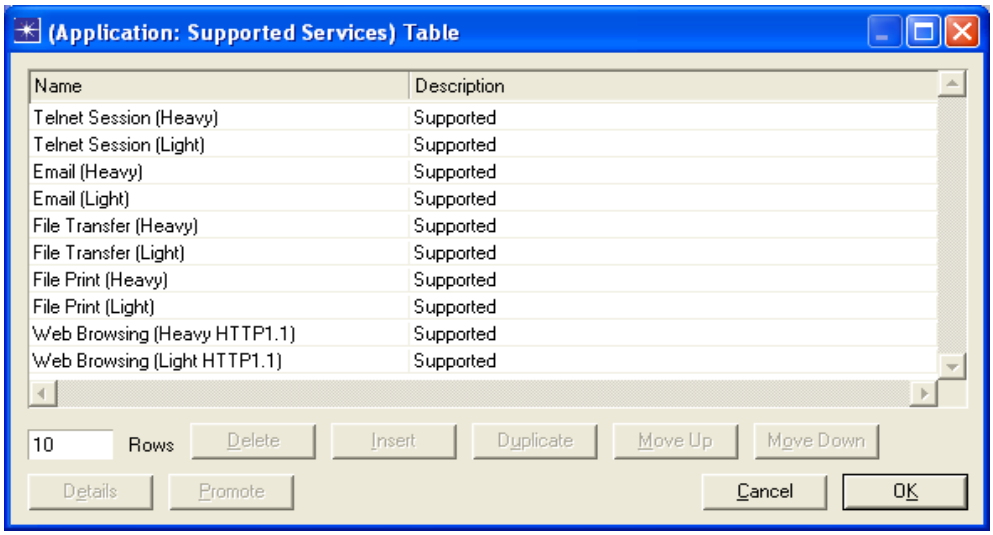
- Επεξεργασθείτε τα attributes του Profile Config, και επιλέξτε **Sample Profiles**, από το πεδίο **Profile Configuration**. Αυτό θα δημιουργήσει 5 σχεδιαγράμματα. Εμείς θέλουμε 6, οπότε κάνουμε το εξής: **Profile Configuration→ rows = 6.** Ανοίξτε το **row 6,** και κάνετε τις εξής αλλαγές: **Profile Name: DB Access Profile.** Ρυθμίστε την τιμή **Profile Configuration→ row 5→ Applications→ rows: 1,** και επιλέξτε την εφαρμογή **Database Access (Heavy)** στο πεδίο **Name** του νέου row. Κατόπιν κάντε κλικ στο **OK.**

- Δημιουργήστε 6 pings, όπως φαίνεται στον παρακάτω πίνακα:

Source Node	Destination Node
Station 4	Station 7
Station 1	Station 7
Station 10	Station 7
Station 4	Google
Station 1	Google
Station 10	Google

Εικόνα 4-7 Application Definitions: Default

- Για να δημιουργήσετε ένα Ping, ανοίξτε την παλέτα αντικειμένων και επιλέξτε το εργαλείο **ip_ping_traffic** από το **internet_toolbox**, και θέστε τους κόμβους πηγής και προορισμού του ping για κάθε έναν.
- Αναλύστε το ping trace: Επιλέξτε όλα τα ping demands, και επεξεργασθείτε τα **Attributes** χρησιμοποιώντας ως **Ping Pattern: Record Route.** Επιλέξτε το **Apply Changes to Selected Objects,** για να κάνει τις αλλαγές σε κάθε επιλεγμένο component, και κατόπιν πατήστε **OK**.
- Καθορίστε τις υπηρεσίες που υποστηρίζονται από τους κεντρικούς υπολογιστές: Δεξί κλικ στον **Multiservice Server** και μετά **Edit Attributes.** Κάντε κλικ στο **Application: Supported Services** και μετά επιλέξτε **Edit.** Στο νέο παράθυρο διαλόγου, όλες οι εφαρμογές εκτός από την βάση δεδομένων θα υποστηρίζονται χρησιμοποιώντας **Rows: 10** και εισάγοντας μια διαφορετική εφαρμογή για κάθε row. Πρέπει να τις αποδεχτούμε όλες εκτός από τις εξής: **Database Access (Heavy)** και **Database Access (Light).**



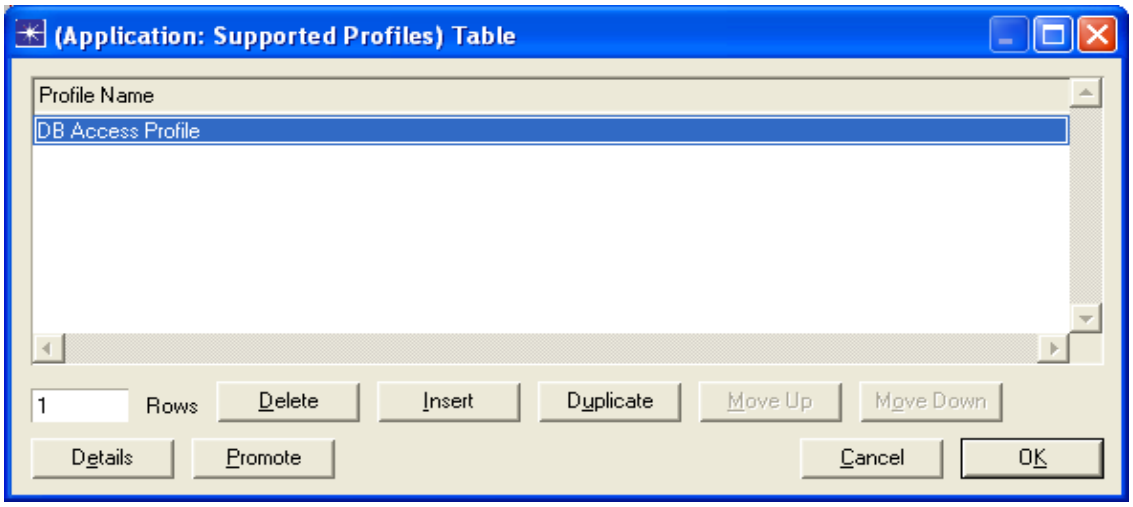
Εικόνα 4-8 Applications supported by Multiservice Server

- Κάντε την ίδια διαδικασία για τον **DB Server** αλλά τώρα θέλουμε να υποστηρίξουμε τις υπόλοιπες εφαρμογές: **Database Access (Heavy)** και **Database Access (Light).**
- Καθορίστε τα σχεδιαγράμματα των σταθμών. Αναθέστε τα ακόλουθα profiles στους κεντρικούς υπολογιστές:

Nodes	**Application: Supported Profiles**
Station 2, Station 5 και Station 10	DB Access Profile
Remaining stations	Engineer

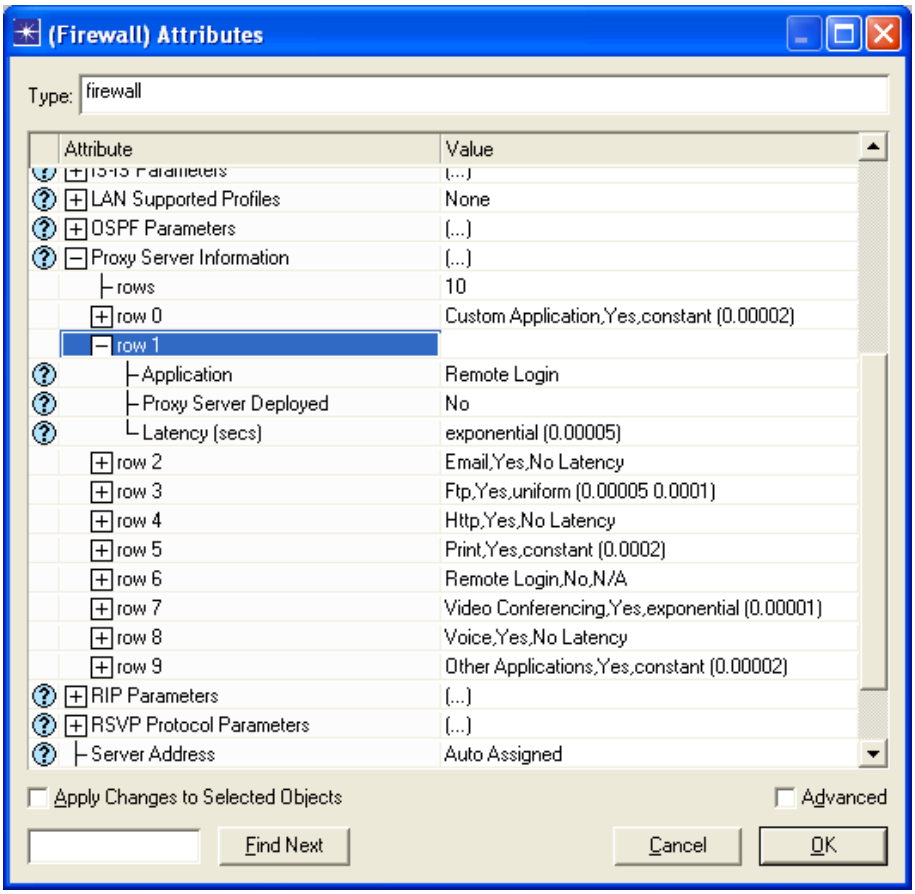
Εικόνα 4-9 Servers Profiles

Επιλέξτε όλους τους σταθμούς για να εφαρμοστούν οι αλλαγές σε ένα κοινό profile. **Δεξί κλικ** σε έναν από αυτούς, μετά κλικ στο **Edit Attributes** και μετά **διπλό κλικ** στο **Application: Supported Profiles.** Κατόπιν, προσθέστε τις εφαρμογές που θέλετε



Εικόνα 4-10 Selecting the profiles for stations 2,5 and 10

- Προγραμματίστε το Firewall του Proxy, να απορρίπτει την κίνηση της εφαρμογής βάσης δεδομένων. **Επεξεργασθείτε** τις **ιδιότητες** του Firewall, ανοίξτε το **Proxy Server Information→ row 1**(γι' αυτήν την εφαρμογή) και αλλάξτε το εξής: **Proxy Server Deployed: No.** Οι υπόλοιπες εφαρμογές μπορούν να αποδεχτούν από αυτή την συσκευή, έτσι στις υπόλοιπες θα συμπληρώσουμε το εξής: **Proxy Server Deployed:Yes**. Επίσης αλλάζουμε το Application σε **Remote Login**. Και κατόπιν πατήστε **OK.**



Εικόνα 4-11 Setting up the Firewall

4. Αναθέστε τις IP διευθύνσεις σε όλα τα Interfaces:

Από τον **Project Editor, Protocols→ IP→ Addressesing→ Auto-Assign IP Addresses.**

5. Αναθέστε τον default router στους **σταθμούς 7, 8, 9 και στον κεντρικό υπολογιστή DB:**

Επιλέξτε τους σταθμούς 7, 8, 9 και τον κεντρικό υπολογιστή DB. Επεξεργασθείτε τις ιδιότητες και αλλάξτε την παράμετρε **IP Hosts Parameters→ Default Route,** τοποθετώντας την IP διεύθυνση του Firewall-to-Switch 1 interface. Για να ανακαλύψετε αυτήν την IP διεύθυνση του interface, πρώτα κάντε κλικ στη σύνδεση Switch 1- Firewall και περιμένετε το κίτρινο μήνυμα να εμφανιστεί. Μόλις έχουμε αυτή την τιμή μπορούμε να ανακαλύψουμε την IP διεύθυνση, **επεξεργάζωντας** τις **ιδιότητες** του Firewall, και διαβάζοντας την τιμή για το **IP Routing Parameters→ Interfaces Information→ row i** (όπου i είναι το νούμερο του interface).

6. Διαμόρφωση της προσομοίωσης:

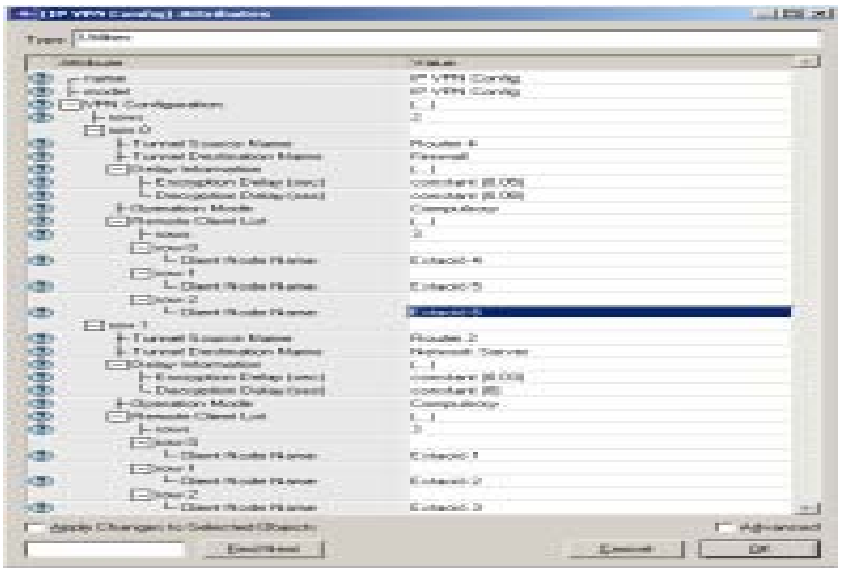
Από τον επεξεργαστή κειμένου, κάντε κλικ στο **configure/run simulation**  , και χρησιμοποιήστε ως διάρκεια προσομοίωσης **Duration: 10 minute(s).** Τέλος πατήστε **OK.** (μην ξεκινήσετε την προσομοίωση ακόμα).

4.4 Δημιουργία του δεύτερου και τρίτου σεναρίου

1. Δημιουργία του VPN σεναρίου χρησιμοποιώντας mode: Compulsory

Αναπαράγετε το σενάριο και καθορίστε δύο VPNs δημιουργώντας την σύνδεση **Router 4 – Firewall** και **Router 2 - Network Server.** Τα VPNs μπορούν να διαμορφωθούν χρησιμοποιώντας **mode: Compulsory**. Αυτό θα κάνει όλη την κίνηση που παράγεται από τους σταθμούς, να περάσει από το VPN Server Compulsory, ακόμα και αν αυτός δεν είναι το συντομότερο μονοπάτι. Τα δύο VPNs θα χρησιμοποιήσουν αλγόριθμους κρυπτογράφησης μεταξύ των δύο LANs, έτσι οι χρόνοι κρυπτογράφησης και αποκρυπτογράφησης θα είναι διαφορετικοί.

- Αναπαράγετε το σενάριο: από τον επεξεργαστή κειμένου, **Scenarios→ Duplicate Scenario…**
- Ονομάστε το νέο σενάριο **Scenario Name: WithVPNCompulsory**
- Επεξεργασθείτε τις ιδιότητες του IP VPN Config control. Δημιουργήστε δύο νέα rows μέσα στο VPN Configuration branch, ένα κάθε φορά για κάθε VPN με αυτές τις τιμές:



Εικόνα 4-12 Configuring the VPNs on the control IP VPN Config

Παρατηρήστε ότι έχουμε δημιουργήσει δύο VPNs: **Router 4 – Firewall** και **Router 2 – Network Server.** Έχουμε ρυθμίσει χρόνους κρυπτογράφησης και αποκρυπτογράφησης στους ανατεθειμένους σταθμούς client και στα δύο VPNs.Το Operation Mode για τις δύο περιπτώσεις έχει ρυθμιστεί σε Compulsory (default value).

1. Δημιουργία του σεναρίου with Virtual Private Networks (VPNs) χρησιμοποιώντας mode: Voluntary

   - Ξεκινώντας από το σενάριο **VPNCompulsoryb** μπορούμε να αναπαράγουμε το σενάριο από τον **Project Editor** κάνοντας τα εξής: **Scenarios-> Duplicate Scenario…**Ονομάζουμε το σενάριο **Scenario Name: VPNVoluntary.** Και μετά κάνουμε κλικ στο **OK.**
   - **Edit** στα **Attributes** του **IP VPN** control, και για κάθε ένα από τα δύο **rows** που καθορίζουν τα VPNs, αλλάζουμε το πεδίο του **Operation Mode** σε **Voluntary.**

2. Τρέξτε την προσομοίωση των τριών σεναρίων συγχρόνως:

Από τον **Project Editor, Scenarios→ Manage Scenarios…**Επιλέξτε **«collect»** ή **«recollect»** από την στήλη **Results** του κάθε σεναρίου και μετά πιέστε **OK.** Όταν οι τρείς προσομοιώσεις τελειώσουν, κάντε κλικ στο **Close.**

4.5 Ερωτήσεις

4.5.1Ερώτηση 1η

Ανοίξτε το Simulation Log των τριών σεναρίων, και χρησιμοποιώντας τα error messages προσπαθήστε να βρείτε σε ποιές περιπτώσεις έχουμε πρόσβαση στη βάση δεδομένων

Scenario	DB query start station		
	Station 2	Station 5	Station 10
NoVPN			
VPNCompulsory			
VPNVoluntary			

4.5.2Ερώτηση 2η

Συγκρίνετε τα traces όλων των ping για όλα τα σενάρια. Για τα pings που αρχίζουν στο Station 1 και τελειώνουν στο Google,είναι τα μονοπάτια ICMP Packets ίσα και για τα τρία σενάρια; Τι θα συνέβαινε αν η πηγή ήταν ο Station 4; Και τι εάν ήταν ο Station 10;

4.5.3 Ερώτηση 3η

Εκτός από την ασφάλεια ποιος από τους τρόπους είναι γρηγορότερος και γιατί;

4.5.4 Ερώτηση 4η

Εξηγήστε την επιρροή της παρουσίας του VPN στο ping delay. Σημειώστε το χρόνο απόκρισης για όλα τα pings.

4.5.5 Ερώτηση 5η

Γιατί το trace του Station 1 – Station 7 δεν δείχνει το πακέτο που έχει διασχίσει το router Firewall,πότε φυσικά είναι ο μόνος πιθανός τρόπος;

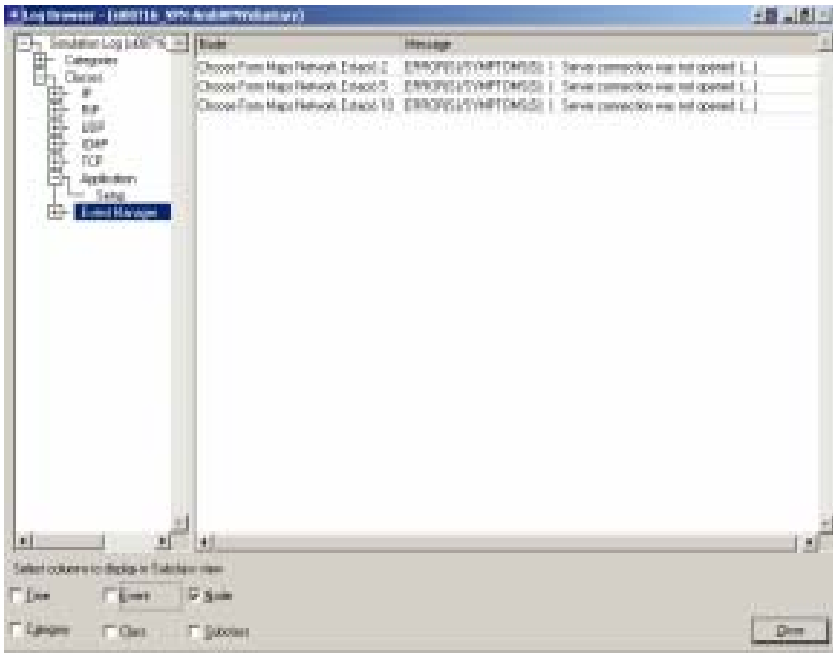
4.6 Απαντήσεις

4.6.1 Απάντηση 1η

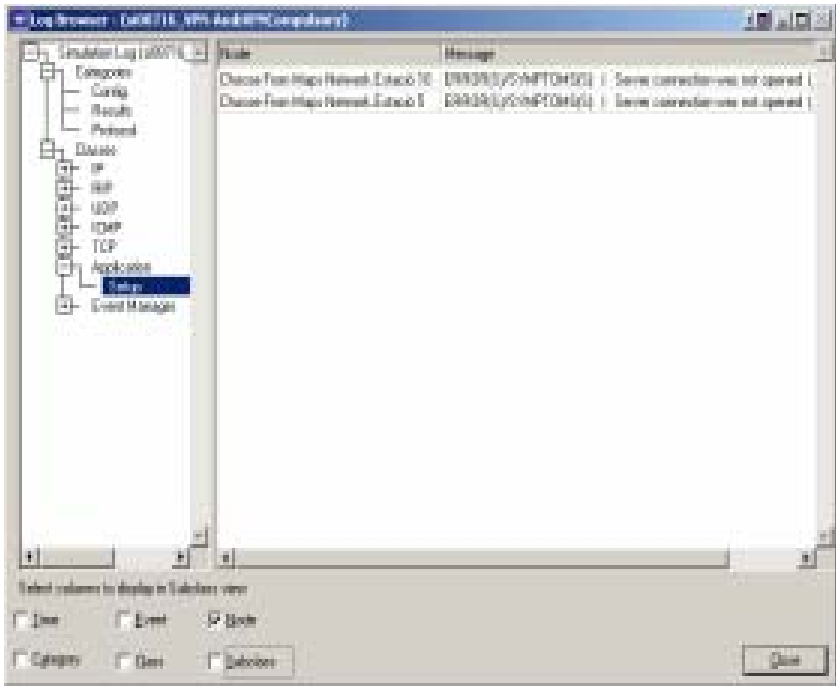
Όταν ανοίγουμε το Simulation Log και βλέπουμε τα error messages, μπορούμε να διακρίνουμε ότι η κυκλοφορία για μερικούς σταθμούς δεν έχει φθάσει στον προορισμό (Database service). Με τα error messages των τριών σεναρίων, μπορούμε να δημιουργήσουμε έναν πίνακα όπως τον παρακάτω

Scenario	**DB query start station**		
	Station 2	**Station 5**	**Station 10**
NoVPN			
VPNCompulsory	✓		
VPNVoluntary			

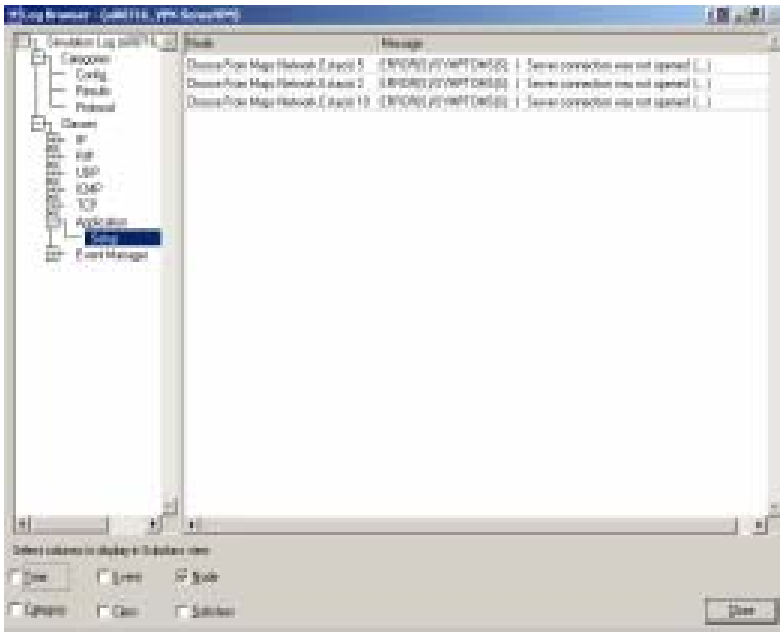
Εικόνα 4-13 Successful database queries



Εικόνα 4-14 Simulation Log for VPNVoluntary



Εικόνα 4-15 Simulation Log for VPNCompulsory



Εικόνα 4-16 Simulation Log for NoVPN

Είναι σαφές ότι όταν δεν έχουμε VPNs, όλη η κυκλοφορία περνάει μέσα από το Firewall χωρίς οποιαδήποτε ενθυλάκωση και έτσι το proxy δεν επιτρέπει στην κυκλοφορία να περάσει από την εφαρμογή βάσης δεδομένων. Αν υπάρχουν VPNs σε Operation Mode: Compulsory, η μόνη κυκλοφορία που μπορεί να περάσει είναι για τους tunnels destination μετά από το router,διαφορετικά το Firewall δεν θα της επέτρεπε να περάσει. Γι' αυτό το λόγο τα DB queries στο σενάριο με Tunnel Destination: Network Server (όπως για το Station 2). Είναι σαφής ότι η κυκλοφορία από το Station 10 πάντα θα απαγορεύεται (banned) από το Firewall. Ακόμα και η κυκλοφορία από το Station 5 με Tunnel Destination ρυθμισμένο στο Firewall δεν μπορεί να περάσει.
Όταν έχουμε Operation Mode: Voluntary, η κυκλοφορία δεν είναι encapsulated, ακριβώς όπως στα NoVPNs.

4.6.2 Απάντηση 2η

Τα Traces για τα 6 Pings, για τα τρία σενάρια είναι:

NoVPN

Source	Destination: Google			Destination: Station 7		
Station 1	192.0.1.2	0	Network.Station 1	192.0.1.2	0	Network.Station 1
	192.0.4.1	0.00366	Network.Router 2	192.0.4.1	0.00297	Network.Router 2
	192.0.6.1	0.00319	Network.Internet	192.0.8.2	0.00319	Network.Internet
	192.0.13.2	0.00307	Network.Router 3	192.0.12.2	0.00389	Network.Firewall
	192.0.13.1	0.00261	Network.Google	192.0.12.3	0.00591	Network.Station 7
	192.0.13.1	0.00001	Network.Google	192.0.12.3	0.00001	Network.Station 7
	192.0.6.2	0.0026	Network.Router 3	192.0.8.1	0.0059	Network.Firewall
	192.0.4.2	0.0026	Network.Internet	192.0.4.2	0.00343	Network.Internet
	192.0.1.1	0.00317	Network.Router 2	192.0.1.1	0.00317	Network.Router 2
	192.0.1.2	0.00298	Network.Station 1	192.0.1.2	0.00298	Network.Station 1
Station 4	192.0.9.1	0	Network.Station 4	192.0.9.1	0	Network.Station 4
	192.0.7.2	0.00306	Network.Router 4	192.0.7.2	0.00238	Network.Router 4
	192.0.6.1	0.00358	Network.Internet	192.0.8.2	0.00358	Network.Internet
	192.0.13.2	0.00258	Network.Router 3	192.0.12.2	0.00341	Network.Firewall
	192.0.13.1	0.00261	Network.Google	192.0.12.3	0.00591	Network.Station 7
	192.0.13.1	0.00001	Network.Google	192.0.12.3	0.00001	Network.Station 7
	192.0.6.2	0.0026	Network.Router 3	192.0.8.1	0.0059	Network.Firewall
	192.0.7.1	0.0026	Network.Internet	192.0.7.1	0.00343	Network.Internet
	192.0.9.2	0.00359	Network.Router 4	192.0.9.2	0.00356	Network.Router 4
	192.0.7.1	0.00259	Network.Station 4	192.0.9.1	0.00239	Network.Station 4
Station 10	192.0.14.1	0	Network.Station 10	192.0.14.1	0	Network.Station 10
	192.0.5.2 (coax)	0.00085	Network.Router 1	192.0.5.2 (coax)	0.00071	Network.Router 1
	192.0.6.1	0.00332	Network.Internet 3	192.0.8.2	0.00277	Network.Internet
	192.0.13.2	0.00258	Network.Router	192.0.12.2	0.00341	Network.Firewall
	192.0.13.1	0.00261	Network.Google	192.0.12.3	0.00591	Network.Station 7
	192.0.13.1	0.00001	Network.Google	192.0.12.3	0.00001	Network.Station 7
	192.0.6.2	0.0026	Network.Router 3	192.0.8.1	0.0059	Network.Firewall
	192.0.5.1 Network.Router	0.0026	Network.Internet	192.0.5.1	0.00343	Network.Internet
	192.0.14.3	0.00275	1(coax)	192.0.14.3 (coax)	0.00275	Network.Router 1
	192.0.14.1	0.00072	Network.Station 10	192.0.14.1	0.00072	Network.Station 10

Εικόνα 4-17 Ping traces at NoVPN

VPNCompulsory

Origen	Destination: Google	Destination: Station 7
Station 1	192.0.1.2 0 Network.Station 1 192.0.3.1 0, 00366 Network.Router 2 [label=0] [exp=0] 192.0.12.1 0,01587 Network.Network Server 192.0.8.1 0,00759 Network.Firewall 192.0.6.1 0,00343 Network.Internet 192.0.13.2 0,00258 Network.Router 3 192.0.13.1 0,00261 Network.Google 192.0.13.1 0,00001 Network.Google 192.0.6.2 0,0026 Network.Router 3 192.0.8.2 0,0026 Network.Internet 192.0.12.2 0,00341 Network.Firewall 192.0.12.1 0,00759 Network.Network Server [label=0] [exp=0] 192.0.1.1 0,01439 Network.Router 2 192.0.1.2 0,00298 Network.Station 1	192.0.1.2 0 Network.Station 1 192.0.3.1 0,00297 Network.Router 2 [label=0] [exp=0] 192.0.12.1 0,01498 Network.Network Server 192.0.12.4 0,00693 Network.Station 7 192.0.12.4 0,00001 Network.Station 7 192.0.12.1 0,00692 Network.Network Server [label=0] [exp=0] 192.0.1.1 0,01439 Network.Router 2 192.0.1.2 0,00298 Network.Station 1
Station 4		
Station 10		

VPNVoluntary

Origen	Destination: Google	Destination: Station 7
Station 1		
Station 4		
Station 10		

Όταν δεν υπάρχουν VPNs το μονοπάτι είναι πολύ δύσκολο να βρεθεί.
Όταν έχουμε VPNs σε Mode: Compulsory, τότε πρέπει πάντα να περάσουμε από το VPN ακόμα κι αν το μονοπάτι είναι μεγαλύτερο. Παραδείγματος χάριν, όταν ο Station 1 κάνει ping στο Google,αυτό περνά από το Network Server. Το VPN θα ληφθεί όταν το σημείο έναρξης είναι ένας VPN client,έτσι όταν ο Station 4 θα κάνει Pings ενάντια στο Google θα πάρει το άλλο VPN και θα περάσει από το Firewall. Από την άλλη μεριά όταν ο Station 10 θα κάνει pings ενάντια στο Google, δεν θα περάσει από κάποιο VPN επειδή δεν είναι client κάποιου VPN και έτσι το μονοπάτι είναι πολύ απλό για ακόμα μία φορά.
Όταν το Operation Mode είναι ρυθμισμένο σε Voluntary,τότε τα μονοπάτια που χρησιμοποιούνται είναι τα ίδια όπως όταν δεν έχουμε VPNs. Στην πραγματικότητα η κυκλοφορία δεν είναι encapsulated.

4.6.3 Απάντηση 3η

Εάν δεν ενδιαφερόμαστε για την ασφάλεια, το μονοπάτι με το λιγότερο αριθμό από hops δεν θα μπορέσει ποτέ να είναι VPNCompulsory, επειδή πρέπει να περάσει από το Tunnel Destination και έπειτα να πάρει έναν μακρύτερο μονοπάτι για να γυρίσει πίσω. Γι' αυτόν το λόγο, το μικρότερο και το γρηγορότερο μονοπάτι θα είναι πάντα χωρίς VPNs.

4.6.4 Απάντηση 4η

Όταν χρησιμοποιούμε VPNs, εμφανίζεται μια σύντομη καθυστέρηση, η οποία οφείλεται στις καθυστερήσεις κρυπτογράφησης και αποκρυπτογράφησης. Αυτό το πράγμα δεν θα είχε συμβεί ποτέ χωρίς VPNs.Όπως μπορούμε να δούμε ο χρόνος απόκρισης δεν επηρεάζεται από το VPN mode (Compulsory/Voluntary).

Source	Destination: Google	Destination: Station 7
Station 1	No VPN: 0,02390 seconds Compulsory: 0,06933 seconds Voluntary: 0,02390 seconds	No VPN: 0,03146 seconds Compulsory: 0,04919 seconds Voluntary: 0,03146 seconds
Station 4	Sense VPN: 0,02301 seconds Compulsory: 0,03798 seconds Voluntary: 0,02301 seconds	Sense VPN: 0,03057 seconds Compulsory: 0,03099 seconds Voluntary: 0,03057 seconds
Station 10	Sense VPN: 0,01807 seconds Compulsory: 0,01807 seconds Voluntary: 0,01807 seconds	Sense VPN: 0,02562 seconds Compulsory: 0,02562 seconds Voluntary: 0,02562 seconds

Εικόνα 4-18 Ping response times

4.6.5 Απάντηση 5η

Το ping packet δεν πηγαίνει από τους δρομολογητές όπως είναι, αλλά κρυπτογραφημένο. Το VPN δημιουργεί μια εικονική σύνδεση μεταξύ των δύο τελευταίων σημείων, δεδομένου ότι μια point-to-point σύνδεση έχει δημιουργηθεί χωρίς οποιεσδήποτε ενδιάμεσες συσκευές layer-3.

Chapter 5 Firewall and VPN

5.1 Σκοπός

Του συγκεκριμένου εργαστηρίου είναι να μελετηθεί ο ρόλος του Firewall και των ιδιωτικών εικονικών δικτύων (VPNs[17]), στην παροχή ασφάλειας σε δημόσια δίκτυα ευρείας χρήσης όπως το internet.

5.2 Επισκόπηση

Ένα βασικό χαρακτηριστικό των δικτύων υπολογιστών είναι το ότι αποτελούν έναν κοινόχρηστο πόρο και χρησιμοποιούνται από πολλές εφαρμογές και για πολλούς διαφορετικούς σκοπούς.
Μερικές φορές τα δεδομένα που μετακινούνται μεταξύ των εφαρμογών είναι αναγκαίο να είναι απόρρητα, και οι χρήστες των εφαρμογών επιδιώκουν να διαφυλαχτεί αυτό το απόρρητο των αρχείων τους.
Το Firewall είναι ένας ειδικά προγραμματισμένος δρομολογητής που βρίσκεται μεταξύ μιας συγκεκριμένης τοποθεσίας (site) και του υπόλοιπου δικτύου. Είναι ένας δρομολογητής με την έννοια του ότι συνδέεται με δύο ή περισσότερα φυσικά δίκτυα και προωθεί πακέτα από το ένα δίκτυο σε άλλο. Επίσης φιλτράρει τα πακέτα που διακινούνται.
Το Firewall επιτρέπει στον διαχειριστή συστήματος να εφαρμόσει μια πολιτική ασφαλείας σε κάποια συγκεκριμένη θέση. Τα Filter-based Firewalls[18] είναι τα πιο απλά και ευρέως διαδεδομένα φίλτρα. Διαμορφώνονται με ένα πίνακα διευθύνσεων ο οποίος προσδιορίζει ποιά πακέτα θα περάσουν και ποιά όχι.
Τα VPN είναι ένα παράδειγμα παροχής ελεγχόμενης συνδεσιμότητας σε ένα δημόσιο δίκτυο όπως το internet. Τα VPNs χρησιμοποιούν την έννοια IP-tunnel, μια εικονική point-to-point σύνδεση μεταξύ ενός ζεύγους κόμβων, οι οποίοι στην πραγματικότητα διαχωρίζονται από έναν αυθαίρετο αριθμό δικτύων. Η εικονική σύνδεση δημιουργείται μέσα στο δρομολογητή, στην είσοδο της σήραγγας (IP-tunnel), παρέχοντας της την IP διεύθυνση του δρομολογητή που βρίσκεται στο άλλο άκρο της.
Όποτε ο δρομολογητής που βρίσκεται στην είσοδο της σήραγγας θέλει να στείλει ένα πακέτο μέσω της εικονικής σύνδεσης, τοποθετεί το πακέτο μέσα σε ένα IP-διάγραμμα. Η διεύθυνση προορισμού στην επικεφαλίδα IP είναι η διεύθυνση του δρομολογητή που βρίσκεται στο τέλος της σήραγγας, ενώ η διεύθυνση προέλευσης είναι αυτή του δρομολογητή που στέλνει το πακέτο.

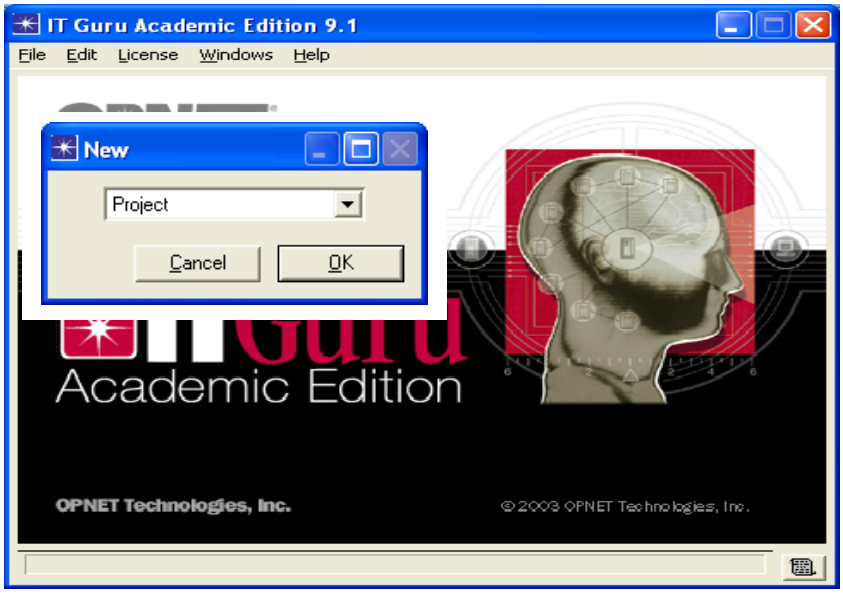
[17] http://en.wikipedia.org/wiki/Virtual_private_network
[18] http://www.obfuscation.org/ipf/ipf-howto.txt

Σε αυτό το σενάριο θα οργανώσετε ένα δίκτυο όπου οι κεντρικοί υπολογιστές θα είναι προσπελάσιμοι μέσω του διαδικτύου από πελάτες με διαφορετικά δικαιώματα. Θα μελετήσετε πώς τα Firewall και τα VPNs μπορούν να παρέχουν ασφάλεια στα δεδομένα του κεντρικού υπολογιστή (server), ενώ παράλληλα διατηρούν την πρόσβαση των πελατών με τα ανάλογα δικαιώματα.

5.3 Μέθοδος

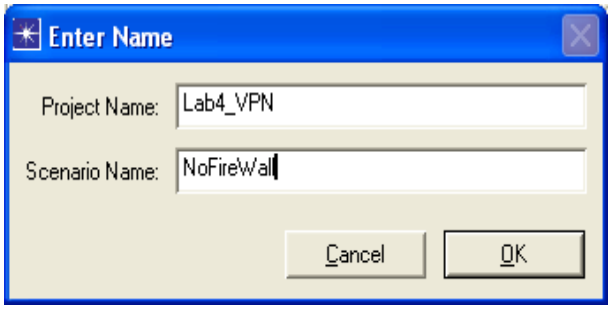
5.3.1 Δημιουργία του νέου Project

1. Ανοίξτε το **OPNET IT Guru Academic Edition**→ και στην συνέχεια επιλέξτε **New** από το **File menu**.



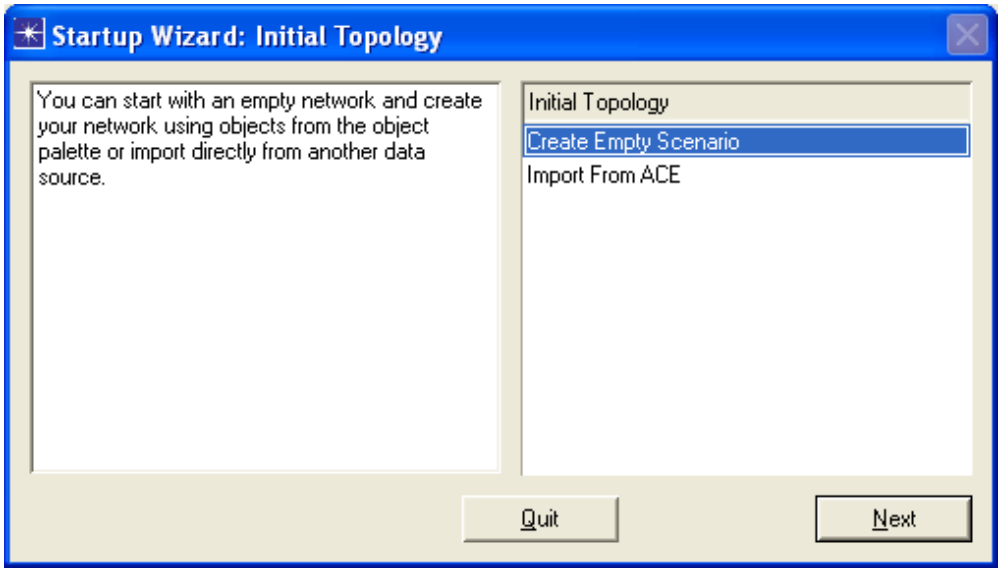
Εικόνα 5-1 Create The Project

2. Επιλέξτε **Project** και πατήστε **OK**→ ονομάστε το **Project <τα αρχικά σάς>_VPN**, και το scenario **NoFirewall**→ και μετά πατήστε **OK**.



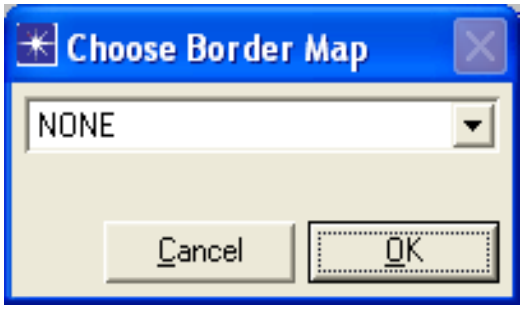
Εικόνα 5-2 Project And Scenario Name

3. Πατήστε **Quit** στο **Startup Wizard**.



Εικόνα 5-3 Topology Of Our Network

4. Για να μετακινήσετε το υπόβαθρο(background), επιλέξτε από το menu **View→ Background→ Set Border Map→** Επιλέξτε **NONE** από το drop-down menu→ και τέλος κάντε κλικ στο **OK.**

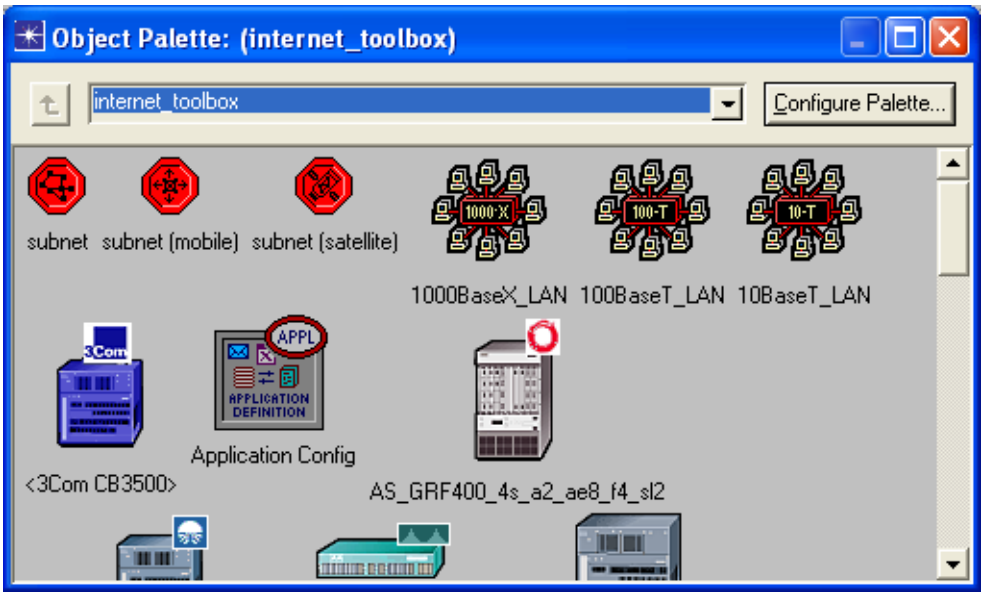


Εικόνα 5-4 Choose Border Map

5.3.2 Δημιουργία και Διαμόρφωση του Δικτύου

Ξεκινώντας το Δίκτυο

1. Ανοίξτε το ***Object Palette*** παράθυρο διαλόγου κάνοντας κλικ στο εικονίδιο  . Βεβαιωθείτε πως το **internet_toolbox** είναι επιλεγμένο από το pull-down menu του ***object palette***.

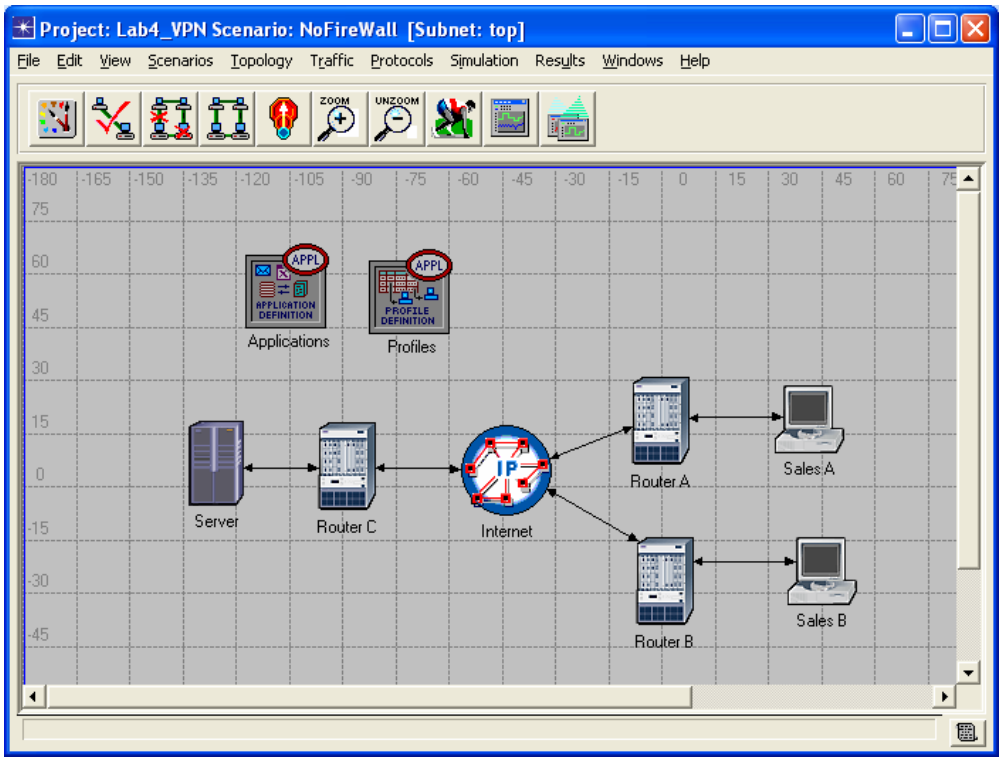


Εικόνα 5-5 Object Palette

2. Προσθέστε τα ακόλουθα αντικείμενα από την παλέτα, στην επιφάνεια εργασίας του project(κοιτάξτε την παρακάτω εικόνα όσον αφορά την τοποθέτηση): **Application Config**, ένα **ip32_cloud**, ένα **ppp_server**, 3 **ethernet4_slip8_gtwy** δρομολογητές και 2 **ppp_wkstn** hosts.

    a. Για να προσθέσετε ένα αντικείμενο από την παλέτα, επιλέγετε το αντικείμενο από την παλέτα→ Κουνάτε το ποντίκι στην επιφάνεια εργασίας μας (workspace), και κάνετε κλικ εκεί όπου θέλετε να τοποθετήσετε το αντικείμενο σας→ και τέλος κάντε δεξί κλικ για να τερματίσετε την επεξεργασία.

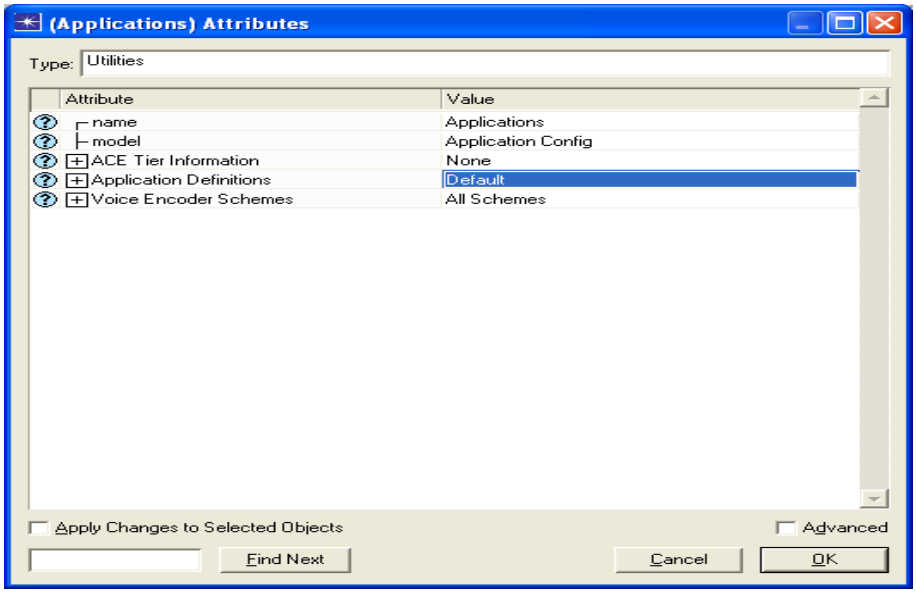
3. Μετονομάστε τα αντικείμενα που προσθέσατε προηγουμένως και στη συνέχεια συνδέστε τα χρησιμοποιώντας **PPP DS1** συνδέσεις, όπως φαίνεται και παρακάτω:



Εικόνα 5-6 Our Network

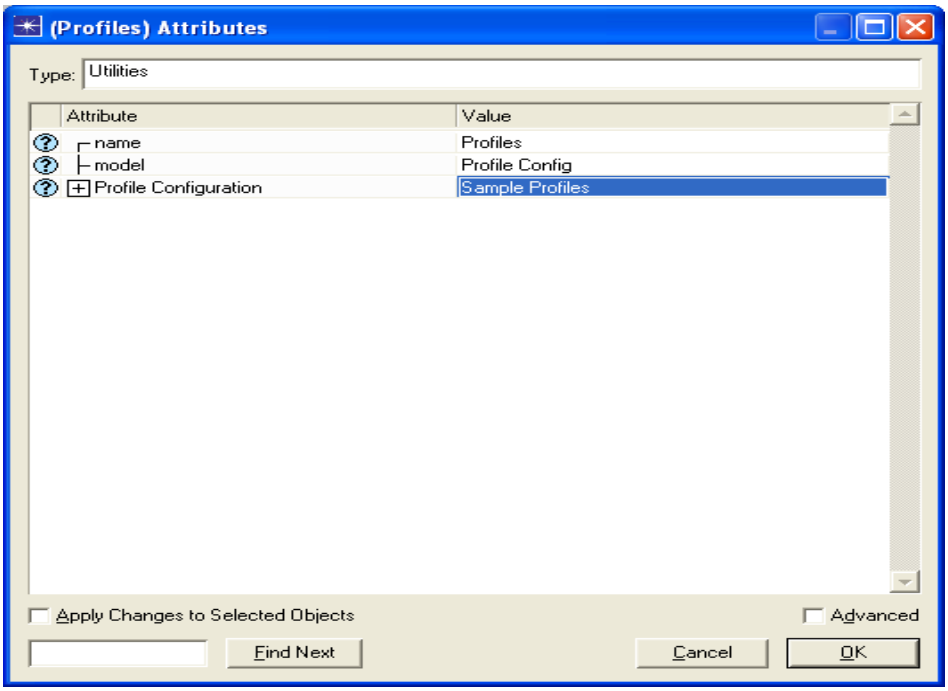
5.3.3 Διαμόρφωση των Κόμβων

1. Δεξί κλικ στο menu **Applications**→ μετά **Edit Attributes**→ επιλέξτε το **Default** στις ιδιότητες του **Application Definition**→ και τέλος πατήστε **OK**.



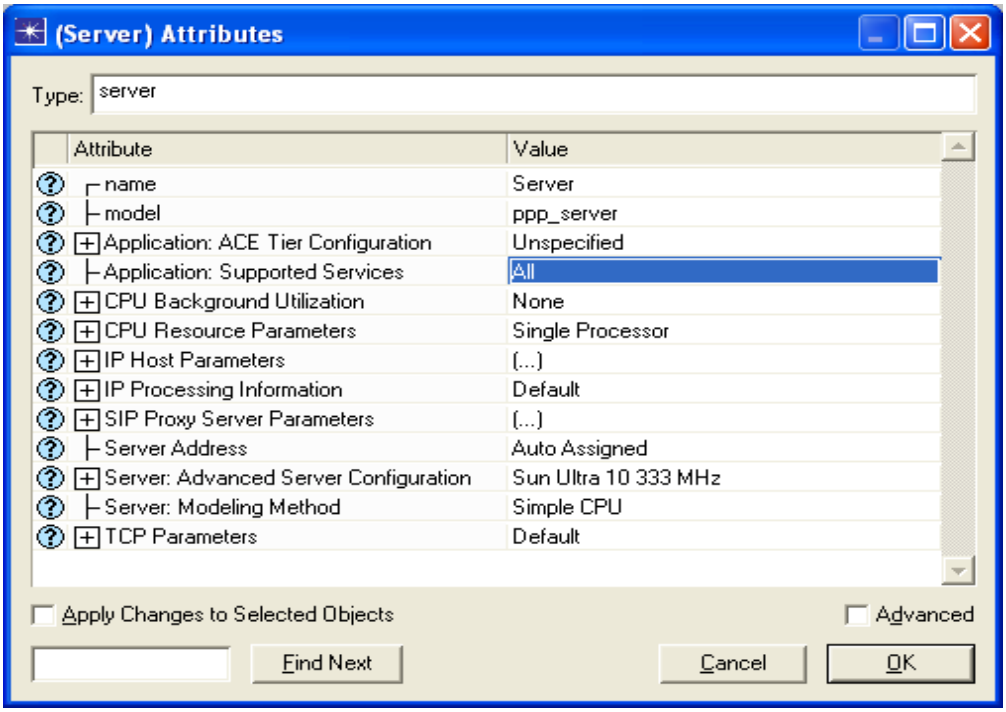
Εικόνα 5-7 Applications Attributes

2. Δεξί κλικ στο menu **Profile→** μετά **Edit Attributes→** επιλέξτε το **Sample Profiles** στις ιδιότητες του **Profile Configuration→** και τέλος πατήστε **OK**.



Εικόνα 5-8 Profiles Attributes

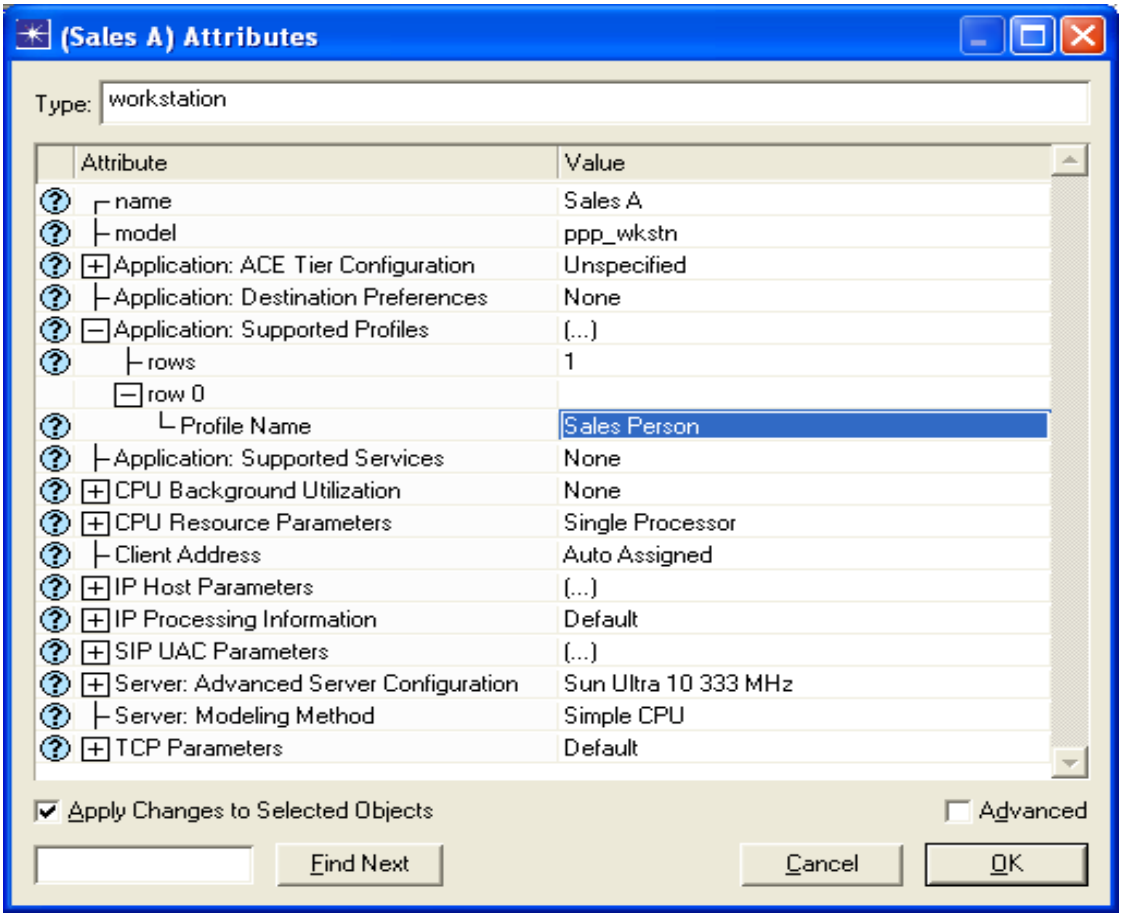
3. Δεξί κλικ στο menu **Server→** μετά **Edit Attributes→** επιλέξτε το **ALL** στις ιδιότητες του **Application: Supported Services→** και τέλος πατήστε **OK**.



Εικόνα 5-9 Server Attributes

4. Δεξί κλικ στον κόμβο **Sales A→ Select Similar Nodes** (βεβαιωθείτε ότι οι κόμβοι **Sales A** και **Sales B** είναι επιλεγμένοι).

   i. Δεξί κλικ στον κόμβο **Sales A→** μετά **Edit Attributes→** κάνετε κλικ το **Apply Changes to Selected Objects.**
   ii. Επεκτείνετε το **Application: Supported Profiles→** ρυθμίστε το **rows** στο 1→ Ανοίξτε το δέντρο του **row 0→ Profile Name** = **Sales Person** (ένα από τα **Sample Profiles** που διαμορφώσατε στο **Profile** του κόμβου).
   iii. Τέλος κάντε κλικ στο **OK**.

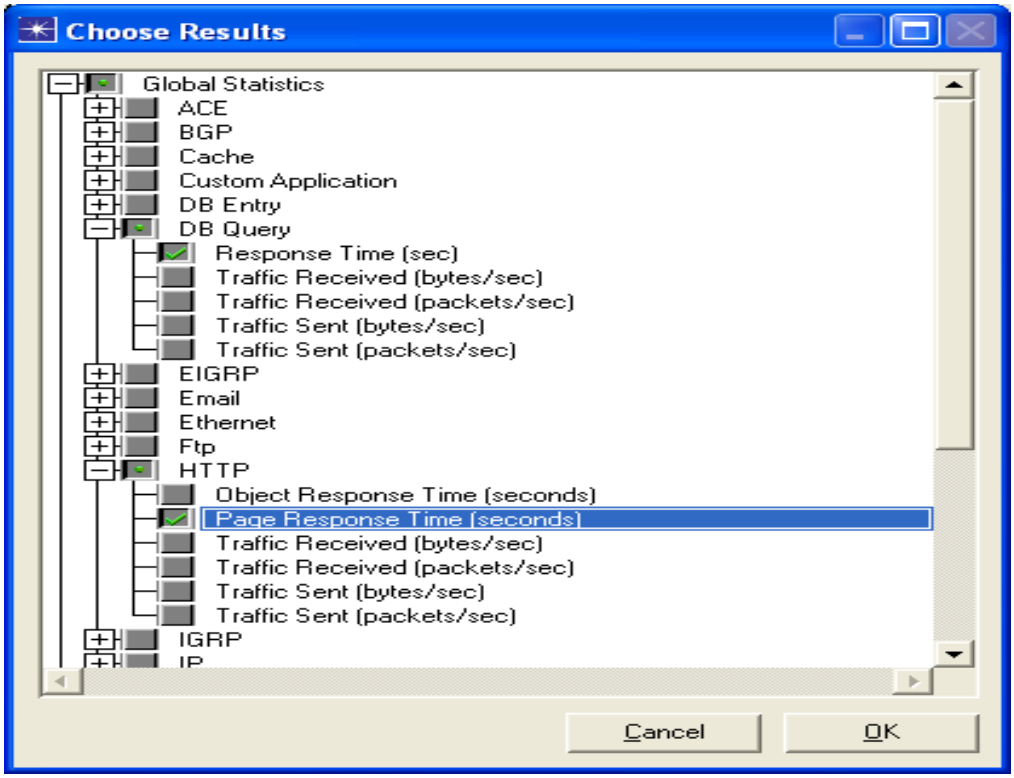


Εικόνα 5-10 Sales A Attributes

5. Αποθηκεύστε το Project σας.

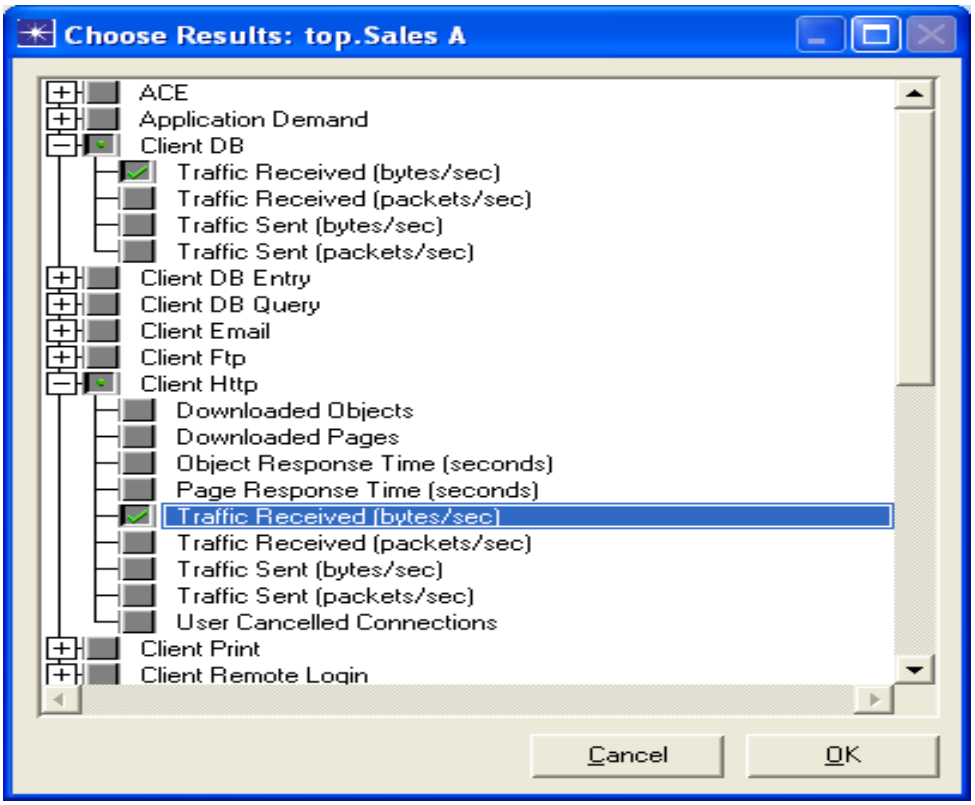
5.3.4 Επιλογή των στατιστικών στοιχείων

1. Δεξί κλικ οπουδήποτε στην επιφάνεια εργασίας του προγράμματος και επιλέξτε **Choose Individual Statistics** από το pop-up menu.
2. Στο παράθυρο διαλόγου *Choose Results*, επιλέξτε τα παρακάτω :
   i. **Global Statistics → DB Query → Response Time (sec).**
   ii. **Global Statistics → HTTP → Page Response Time (seconds).**



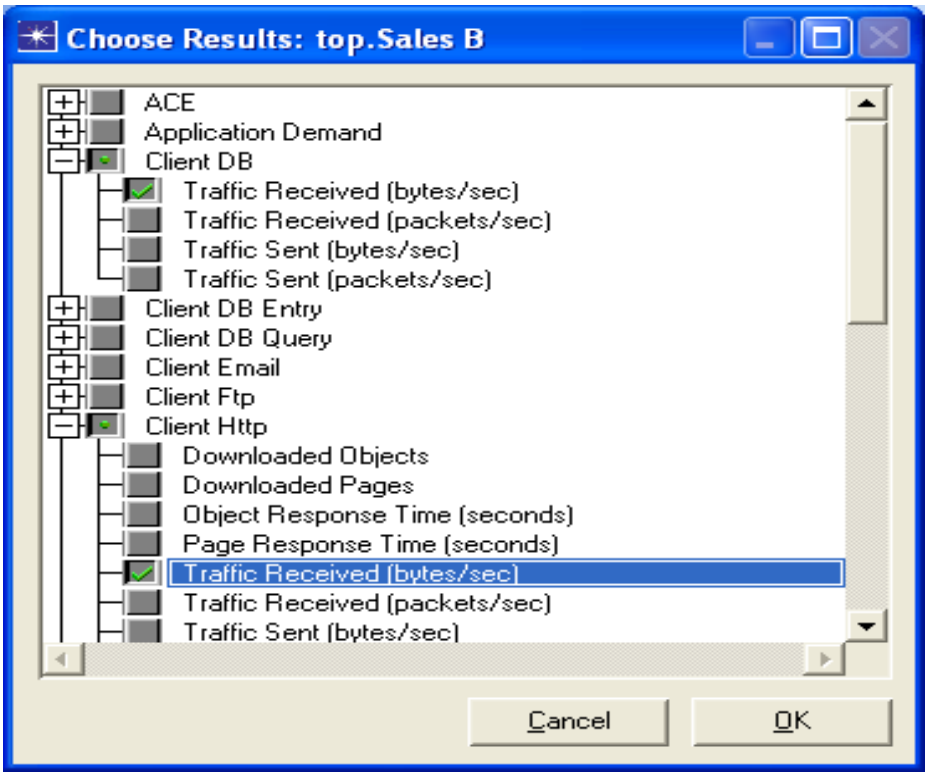
Εικόνα 5-11 Choose Results

3. Και τέλος πατήστε **OK**.
4. Δεξί κλικ στον κόμβο **Sales A** και μετά επιλέξτε **Choose Individual Statistics** από το pop-up menu.
5. Στο παράθυρο διαλόγου *Choose Results*, επιλέξτε τα παρακάτω:
   i. **Client DB → Traffic Received (bytes/sec).**
   ii. **Client Http → Traffic Received (bytes/sec).**



Εικόνα 5-12 Choose Results (Sales A)

6. Και τέλος πατήστε **OK**.
7. Δεξί κλικ στον κόμβο **Sales B** και μετά επιλέξτε **Choose Individual Statistics** από το pop-up menu.
8. Στο παράθυρο διαλόγου *Choose Results,* επιλέξτε τα παρακάτω :
   i. **Client DB → Traffic Received (bytes/sec).**
   ii. **Client Http → Traffic Received (bytes/sec).**



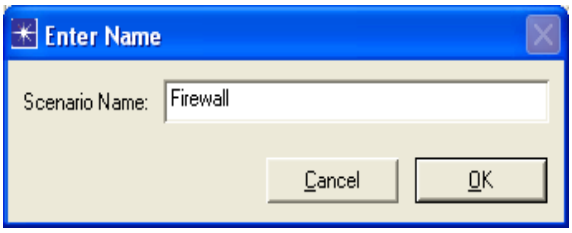
Εικόνα 5-13 Choose Results (Sales B)

9. Κάνετε κλικ στο **OK** και αποθηκεύστε το Project.

5.4 Το Σενάριο Firewall

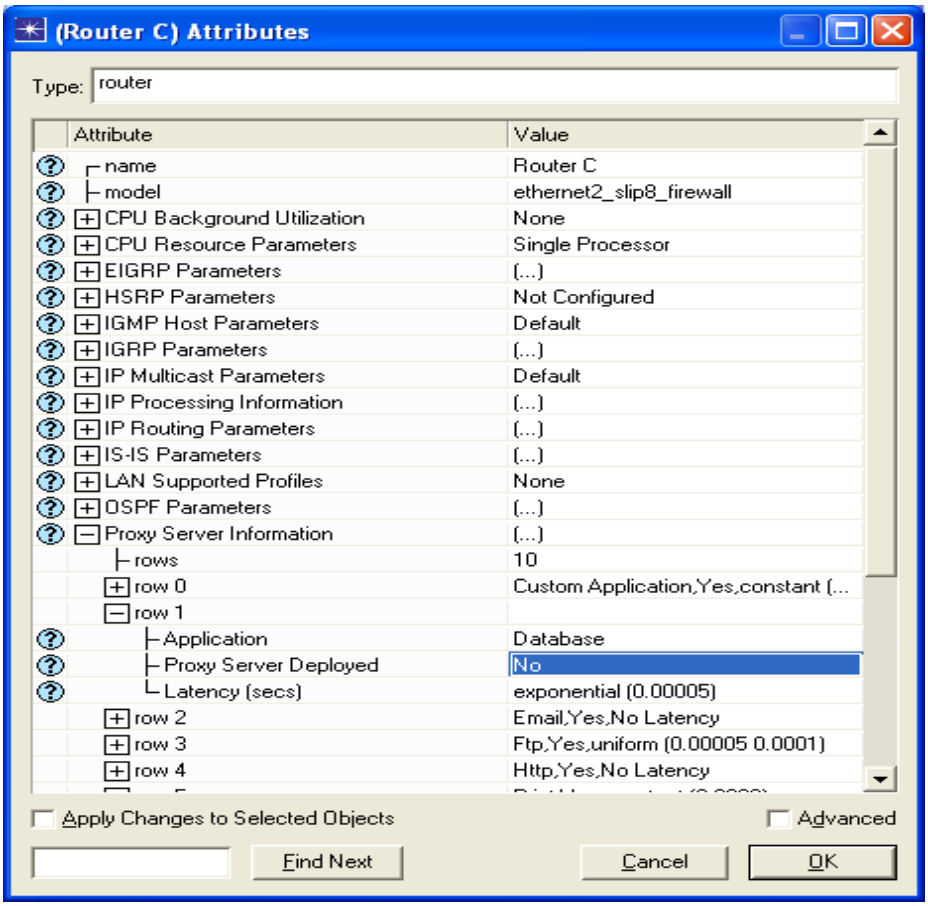
Στο δίκτυο που μόλις δημιουργήσατε, το Sales Person profile επιτρέπει και στα δύο sale sites να έχουν πρόσβαση σε εφαρμογές όπως η βάση δεδομένων (Database Access), το Email, και το Web Browsing από τον server (από το **profile** του κόμβου τσεκάρετε την επιλογή **Profile Configuration**). Θεωρείστε ότι πρέπει να προστατευτεί η βάση δεδομένων από εξωτερικές προσβάσεις, συμπεριλαμβανομένων και των **sales people**. Ένας τρόπος να γίνει αυτό είναι να αντικατασταθεί το Router C με ένα Firewall όπως φαίνεται παρακάτω:

1. Επιλέξτε **Duplicate Scenario** από το **Scenarios** menu, και ονομάστε το **Firewall**→ πατήστε **OK**.



Εικόνα 5-14 Duplicate the old and name Firewall the new Scenario

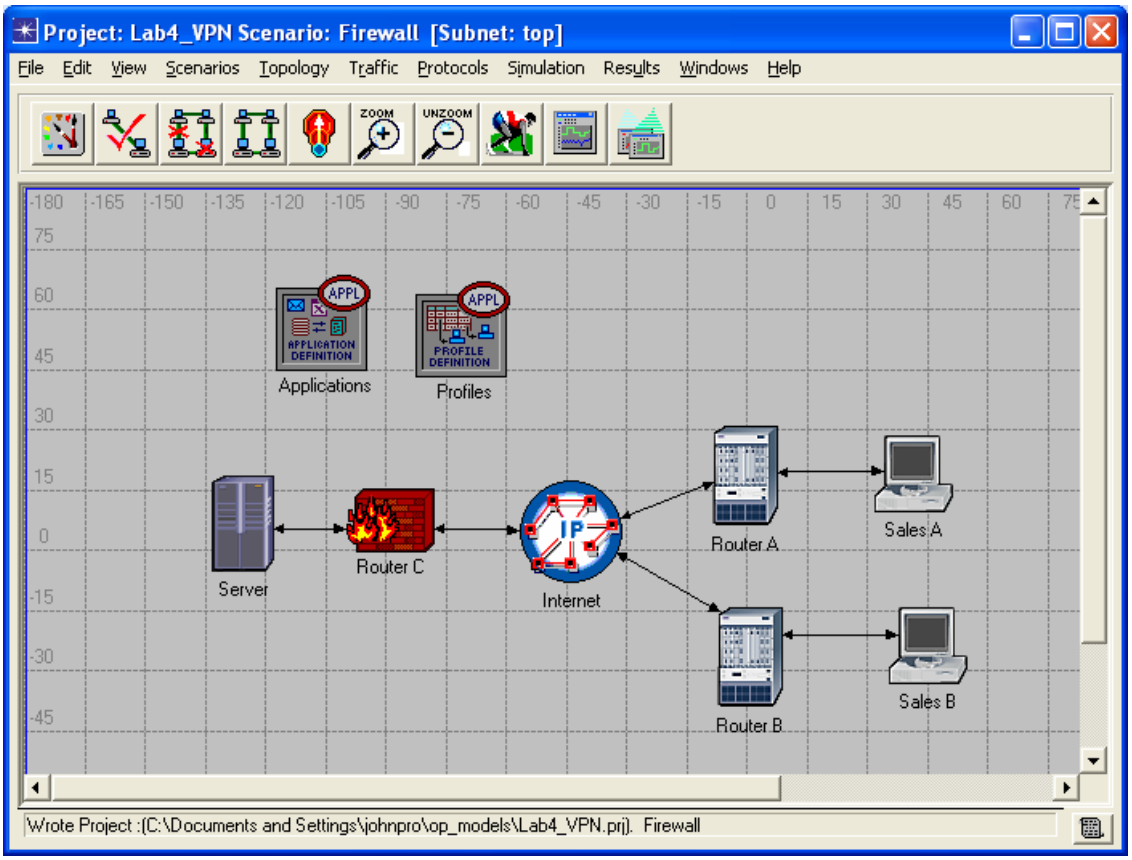
2. Στο νέο σενάριο κάντε δεξί κλικ στον **Router C→ Edit Attributes**.
3. Στην ιδιότητα **model** εκχωρήστε **ethernet2_slip8_firewall**.
4. Ανοίξτε το δέντρο επιλογών του **Proxy Server Information→** διπλό κλικ στο **row 1**, το οποίο αφορά την εφαρμογή της βάσης δεδομένων→ Επιλέξτε **No** στο πεδίο **Proxy Server Information** όπως φαίνεται παρακάτω:



Εικόνα 5-15 Sales C Attributes

5. Κάντε κλικ στο **OK** και αποθηκεύστε το Project.

Οι ρυθμίσεις του Firewall δεν επιτρέπουν κίνηση η οποία σχετίζεται με την βάση δεδομένων, φιλτράροντας πακέτα τα οποία σχετίζονται με αυτή. Με αυτόν τον τρόπο οι βάσεις δεδομένων του κεντρικού υπολογιστή προστατεύονται από τυχόν εξωτερική πρόσβαση. Το σενάριο του Firewall θα πρέπει να μοιάζει με την παρακάτω εικόνα.



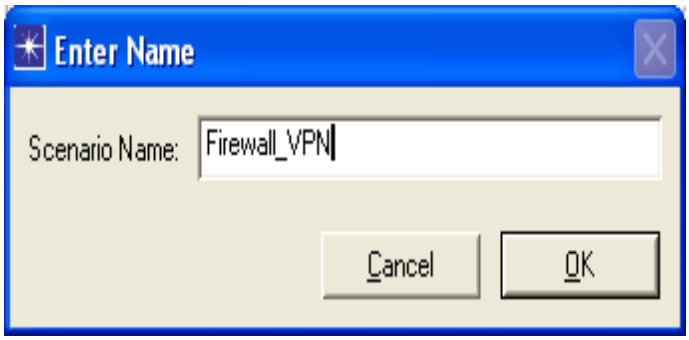
Εικόνα 5-16 Scenario VPN Firewall

5.5 Το Σενάριο Firewall_VPN

Στο σενάριο Firewall προστατεύατε την βάση δεδομένων του server από οποιαδήποτε εξωτερική πρόσβαση χρησιμοποιώντας ένα firewall router. Ας υποθέσουμε ότι θέλετε να αφήσετε τους ανθρώπους που βρίσκονται στον **Sales A** να έχουν πρόσβαση στην βάση δεδομένων του server. Εφόσον το firewall φιλτράρει όλη την κίνηση που σχετίζεται με την βάση δεδομένων, ανεξάρτητα από την πηγή της, πρέπει να εξετάσουμε την λύση VPN. Μπορεί να χρησιμοποιηθεί από τον **Sales A** μία εικονική σήραγγα μέσω της οποίας θα στέλνει τα αιτήματα που αφορούν τη βάση δεδομένων. Το firewall δεν θα μπλοκάρει την κίνηση που προέρχεται από τον **Sales A** επειδή τα IP πακέτα που βρίσκονται στην σήραγγα θα τοποθετηθούν μέσα σε ένα διάγραμμα IP.

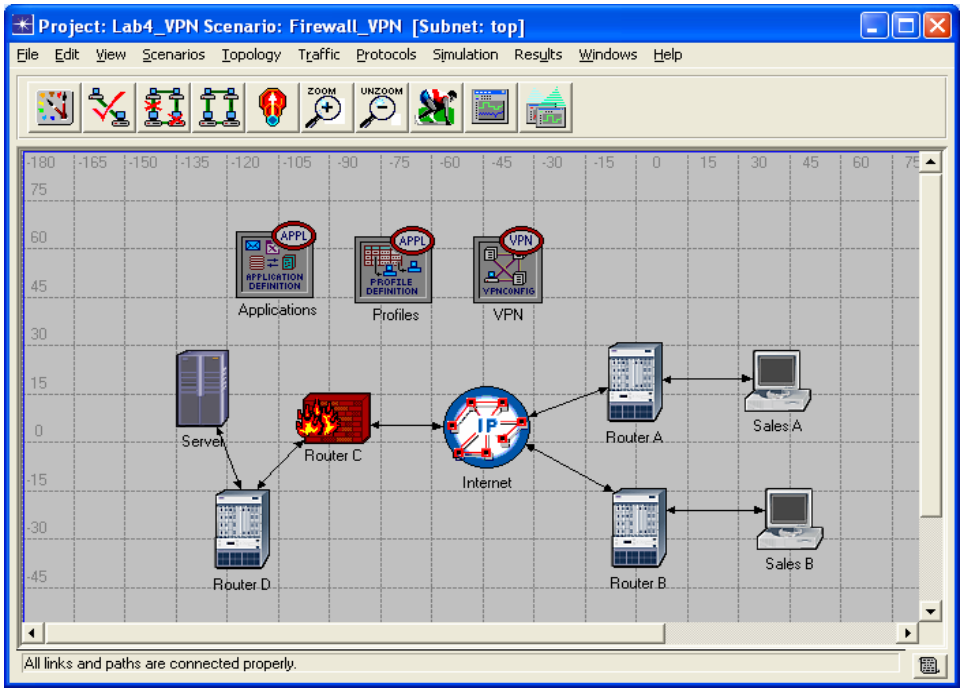
5.5.1 Δημιουργία του Σεναρίου

1. Ενώ είστε στο Firewall σενάριο, επιλέξτε **Duplicate Scenario** από το scenario menu και δώστε του το όνομα Firewall_VPN→ πατήστε **OK**.



Εικόνα 5-17 Scenario Firewall_VPN

2. Καταργείστε την σύνδεση ανάμεσα στον **Router C** και στον **Server**.
3. Ανοίξτε το *Object Palette* παράθυρο διαλόγου κάνοντας κλικ σε αυτό το εικονίδιο  . Βεβαιωθείτε πως το **internet_toolbox** είναι επιλεγμένο από το pull-down menu του *object palette.*
   i. Προσθέστε στην επιφάνεια εργασίας του Project ένα **etherner4_slip8_gtwy** και ένα **IP VPN Config**(δείτε το παρακάτω σχήμα)
   ii. Από το *Object Palette*, χρησιμοποιήστε δύο **PPP DS1** links,για να συνδέσετε το νέο router στο **Router C** (το Firewall) και στον **Server** όπως εμφανίζεται παρακάτω.
   iii. Κλείστε το *Object Palette.*
4. Μετονομάστε το **IP VPN Config** σε **VPN.**
5. Μετονομάστε το νέο router σε **Router D** όπως φαίνεται παρακάτω:



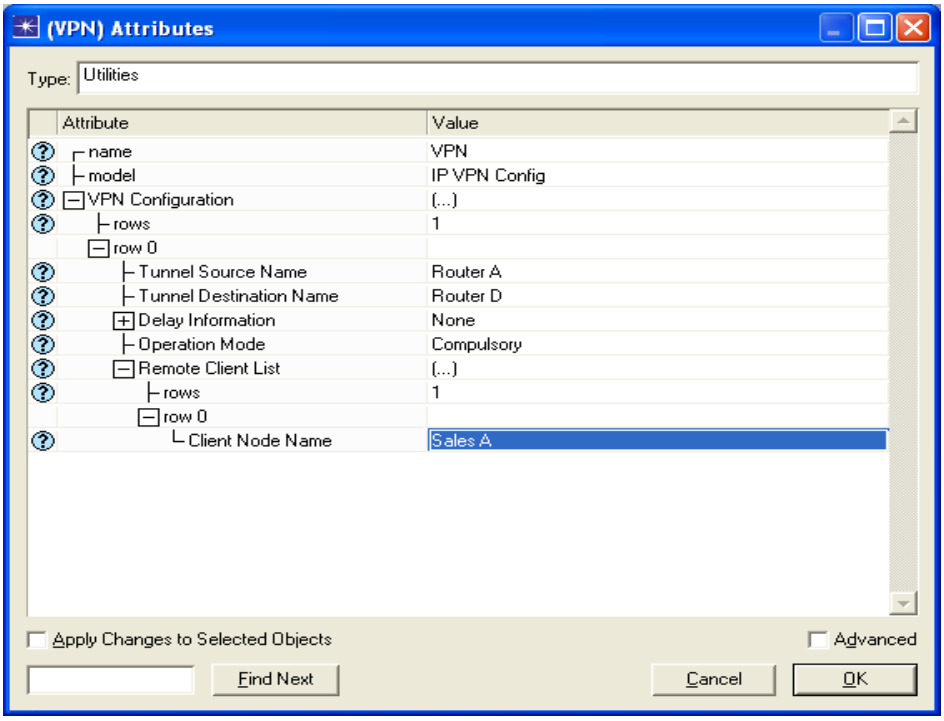
Εικόνα 5-18 Our New Scenario

5.5.2 Διαμόρφωση του VPN

1. Δεξί κλικ στον κόμβο **VPN→ Edit Attributes**.

   i. Ανοίξτε το δέντρο επιλογών του **VPN Configuration→** ρυθμίστε το **rows** στο 1→ Ανοίξτε το δέντρο επιλογών του **row 0→** Αλλάξτε το **Tunnel Source Name** και γράψτε **Router A→** Αλλάξτε το **Tunnel Destination Name** και γράφουμε **Router D.**

   ii. Ανοίξτε το δέντρο επιλογών του **Remote Client List→** ρυθμίστε το **rows** στο 1→ Ανοίξτε το δέντρο επιλογών του **row 0→** Αλλάξτε το **Client Node Name** και γράψτε **Sales A**.



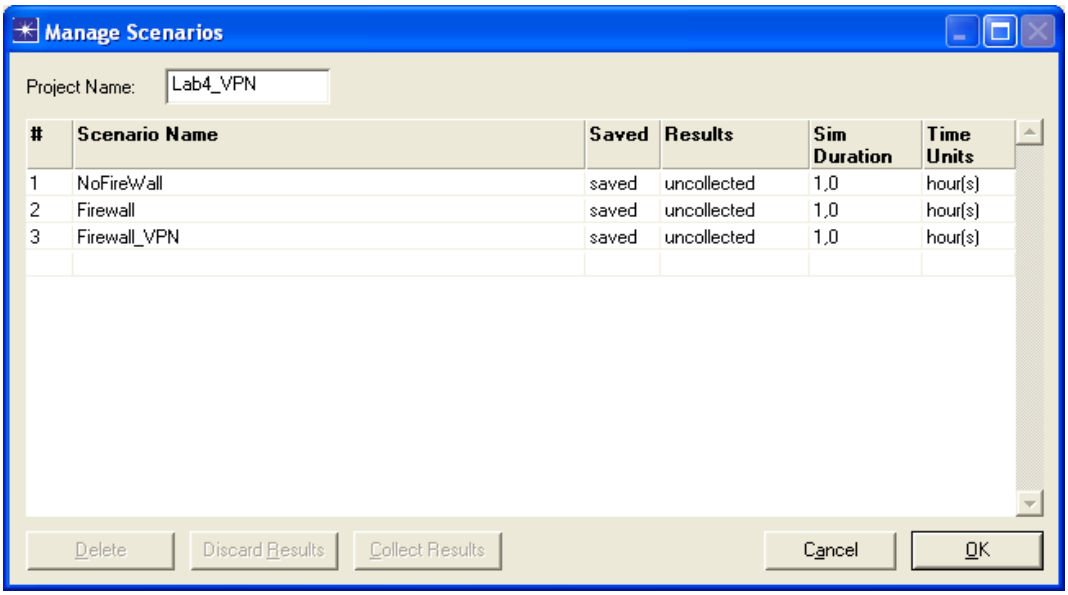
Εικόνα 5-19 VPN Attributes

   iii. Κάντε κλικ στο **OK** και αποθηκεύστε το Project μας.

5.5.3 Πραγματοποιώντας την Προσομοίωση

Για να πραγματοποιήσετε την προσομοίωση για τα τρία σενάρια ταυτόχρονα:

1. Πηγαίνετε στο **Scenarios** menu→ Επιλέξτε **Manage Scenarios**.
2. Αλλάξτε τις τιμές της στήλης **Results** σε «collect» για τα τρία σενάρια. Κρατήστε την default τιμή για το **Sim Duration** (1 hour). Συγκρίνετε με τον ακόλουθο αριθμό.



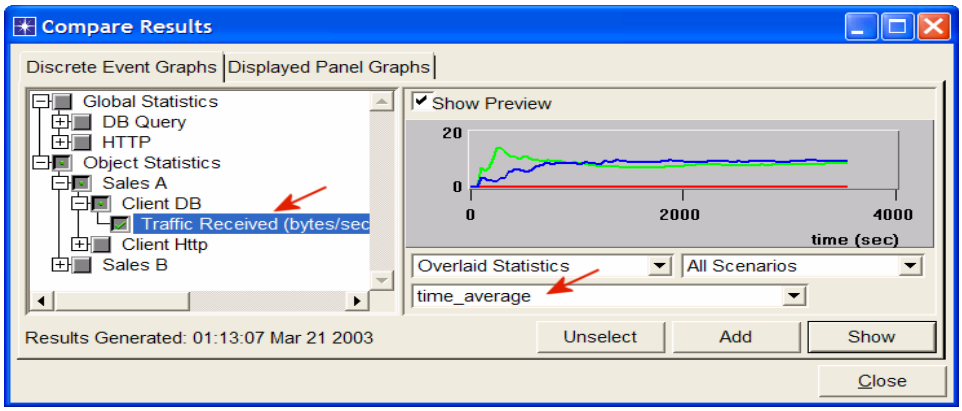
Εικόνα 5-20 Manage Scenarios

3. Κάντε κλικ στο **OK** για να τρέξετε τις τρεις προσομοιώσεις. Ανάλογα με την ταχύτητα του υπολογιστή σας, αυτό μπορεί να πάρει μερικά λεπτά μέχρι να ολοκληρωθεί.
4. Αφού ολοκληρωθούν οι τρείς προσομοιώσεις, μια για κάθε σενάριο, κάνετε κλικ στο **Close**→ και τέλος αποθηκεύστε το project.

5.5.4 Ανάλυση Αποτελεσμάτων

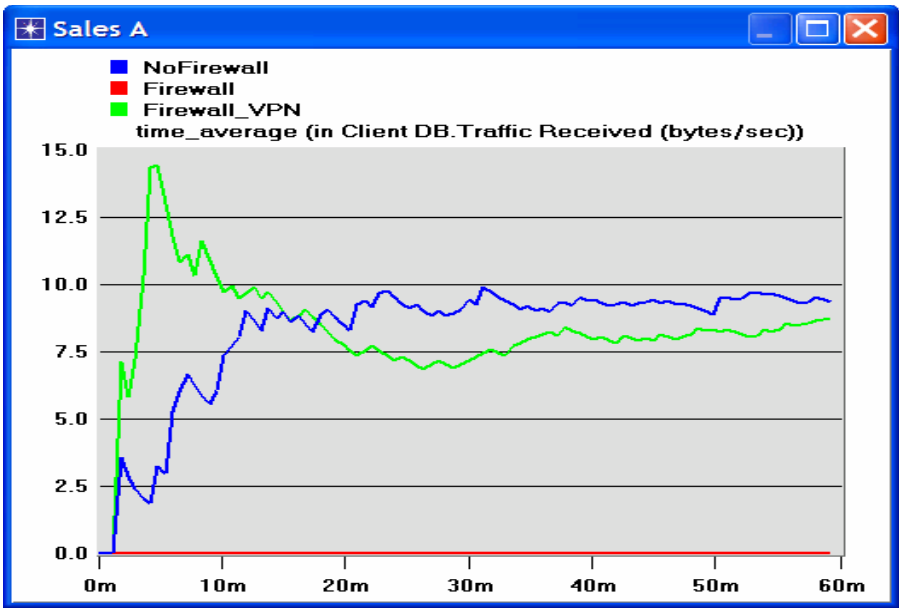
Εμφάνιση και ανάλυση αποτελεσμάτων:

1. Επιλέξτε **Compare Results** από το **Results** menu.
2. Ανοίξτε το δέντρο επιλογών του **Sales A**→ Ανοίξτε το δέντρο επιλογών του **Client DB**→ και επιλέξτε το **Traffic Received**.
3. Αλλάξτε το drop-down menu που υπάρχει στο κάτω δεξί μέρος του **Compare Results** από **As Is** σε **time_average**(βλέπε το παρακάτω σχήμα).



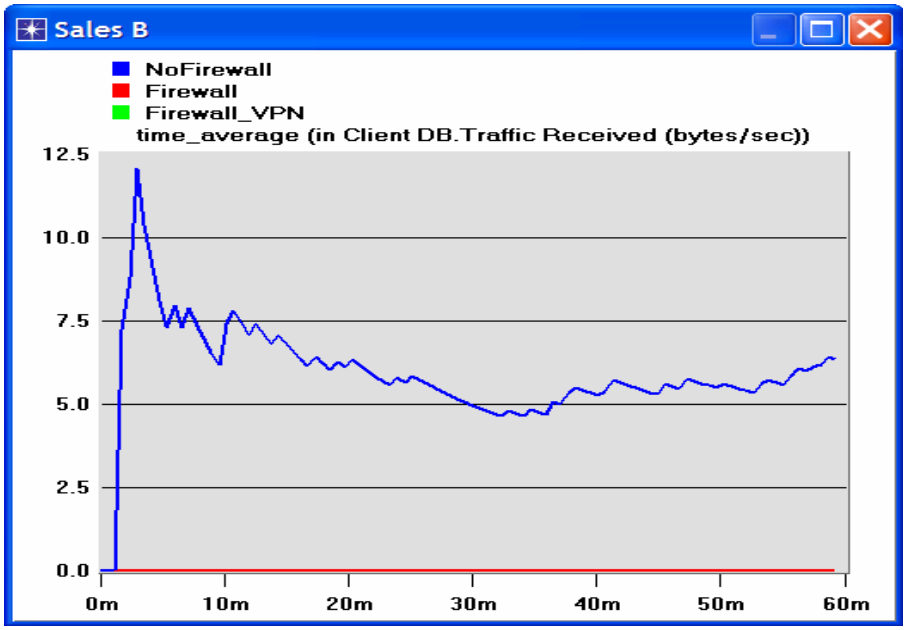
Εικόνα 5-21 Compare Results

4. Πατώντας **Show** το γράφημα των αποτελεσμάτων που θα εμφανιστεί πρέπει να μοιάζει με το παρακάτω



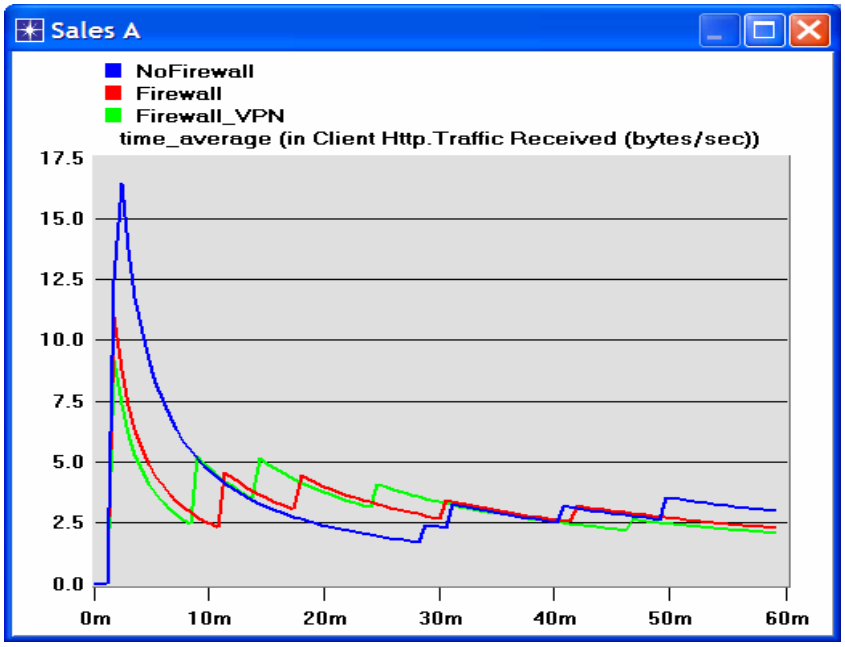
Εικόνα 5-22 Sales A Graphs

5. Δημιουργήστε ένα γράφημα παρόμοιο με το προηγούμενο, αλλά για τον **Sales B**:

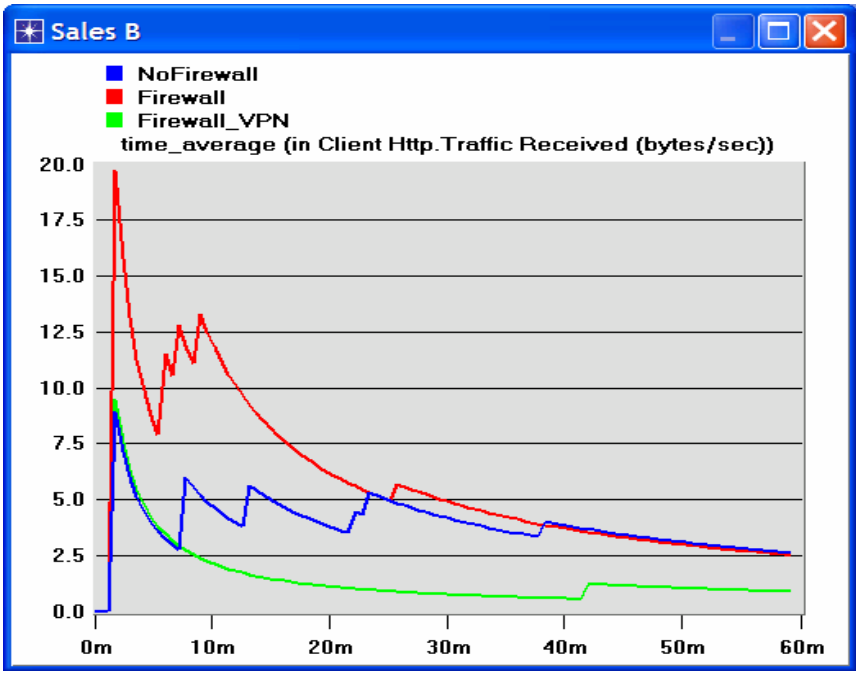


Εικόνα 5-23 Sales B Graphs

6. Δημιουργήστε δύο γραφήματα παρόμοια με τα προηγούμενα για να απεικονίσετε την κυκλοφορία που λαμβάνεται από το **Http Client** για τον **Sales A** και **Sales B**.



Εικόνα 5-24 Sales A Graphs



Εικόνα 5-25 Sales B Graphs

Σημείωση: Τα αποτελέσματα μπορούν να ποικίλουν ελαφρώς λόγω στη διαφορετική τοποθέτηση κόμβων.

5.6 Περαιτέρω Αναγνώσεις

- Ο αντίκτυπος της ικανότητας συνδέσεων Διαδικτύου στην απόδοση εφαρμογής: Από το **Protocols** menu, επιλέγουμε **Methodologies → Capacity Planning**.
- Εικονικά Ιδιωτικά Δίκτυα : IETF RFC number 2685 (www.ietf.org/rfc.html)

5.7 Ερωτήσεις

5.7.1 Ερώτηση 1η

Από τις γραφικές παραστάσεις που προκύπτουν, εξηγήστε την επίδραση του Firewall, και του διαμορφωμένου VPN στην κίνηση της βάσης δεδομένων που προέρχεται απο τους **Sales A** και **Sales B**.

5.7.2 Ερώτηση 2η

Συγκρίνετε τα γραφήματα που εμφανίζουν λαμβανόμενη κίνηση HTTP με εκείνα που εμφανίζουν λαμβανόμενη κίνηση βάσεων δεδομένων.

5.7.3Ερώτηση 3η

Δημιουργήστε και αναλύστε τα γραφήματα που εμφανίζουν την επίδραση του Firewall, καθώς επίσης το διαμορφωμένο VPN, στο χρόνο απόκρισης(καθυστέρηση) των σελίδων HTTP και των ερωτήσεων βάσεων δεδομένων.

5.7.4 Ερώτηση 4η

Στο **Firewall_VPN** σενάριο διαμορφώστε τον κόμβο **VPN** έτσι ώστε καμία κίνηση από τον **Sales A** να μην εμποδίζετε από το Firewall. Δημιουργήστε ένα αντίγραφο του σεναρίου **Firewall_VPN** και ονομάστε το νέο σενάριο **Q4_DB_Web**. Στο σενάριο **Q4_DB_Web** θέλουμε να διαμορφώσετε το δίκτυο έτσι ώστε :

a. Στην βάση δεδομένων του server έχουν πρόσβαση μόνο οι άνθρωποι του **Sales A** site.
b. Στις ιστοσελίδες του server έχουν πρόσβαση οι άνθρωποι του **Sales B** site.

Συμπεριλάβετε στην αναφορά σας το διάγραμμα του νέου διαμορφωμένου δικτύου συμπεριλαμβανομένων οποιωνδήποτε αλλαγών κάνατε στις ιδιότητες των παλιών η νέων κόμβων. Δημιουργήστε τα απαραίτητα γραφήματα για να δείξετε ότι το νέο δίκτυο πληροί τις παραπάνω προϋποθέσεις.

Chapter 6 VLAN's

6.1 Εισαγωγή

Τα VLANs[19] (Virtual Bridged Area Network, or Virtual Lans) καθορίζονται από το πρότυπο IEEE 802.1Q[20]. Χρησιμοποιούνται για να διαιρέσουν ένα δίκτυο σε διαφορετικά λογικά εικονικά LANs. Κάθε χρήστης ανήκει σε ένα εικονικό δίκτυο ανεξάρτητα από την θέση στην οποία βρίσκεται. Οι λογικές ομάδες χρηστών συγκεντρώνουν τα components των δικτύων που είναι εξαπλωμένα σε όλο το διαδίκτυο σε ένα common broadcast domain[21]. Η απόδοση αυξάνεται, και τα collision domains μειώνονται. Κάθε VLAN προσδιορίζεται από ένα VID[22] (VLAN ID),δηλαδή έναν ακέραιο από το 1 έως το 4094.
Τα VLAN μπορούν να εφαρμοστούν κυρίως μέσω bridges και switches (VLAN – aware).
Οι bridges και τα switches ports χωρίζονται σε δύο τύπους, αναλόγως της χρήσης τους μέσα στα VLANs:

- Access Ports: Είναι default ports. Ένα access port μπορεί να ανήκει μόνο σε ένα VLAN, και τα μηνύματα που θα περάσουν από το port θα είναι untagged. Συνδέουν τις VLAN – aware συσκευές με τις VLAN – unaware συσκευές.
- Trunk Ports: Μπορούν να διασύνδεουν VLANs. Με αυτό τον τρόπο, frames από πολλά switches μπορούν να ανταλλαχθούν, ανεξάρτητα από το VLAN στο οποίο ανήκουν. Τα frames που παίρνουν από αυτά τα ports είναι tagged.

Οι πληροφορίες για τα LAN που τους ανήκουν τα frames, είναι να μεταδίδονται μόνο όταν τα frames μεταδίδονται από το Trunk Port μέσω του Trunk link στον προορισμό που είναι το switch. Σε αυτή την περίπτωση, οι πληροφορίες για το LAN προορισμού είναι μέσα στο tag (header). Τα Frames που βγαίνουν από τα Access Ports δεν έχουν κάποιο tag, επειδή υπάρχει μόνο ένα VLAN για κάθε ένα Access Port. Τα tag που προσδιορίζουν τις ιδιότητες μέλους VLAN είναι εσωτερικά level 2 frames, μεταξύ του MAC header και του ωφέλιμου φορτίου.
Η επικοινωνία μεταξύ των switches σε ένα VLAN γίνεται χρησιμοποιώντας trunk links. Μπορούμε να συνδέσουμε τα VLANs μεταξύ τους χρησιμοποιώντας routers ή one – armed–routers.

[19] http://www.techtutorials.info/vlan.html
[20] http://en.wikipedia.org/wiki/IEEE_802.1Q
[21] http://en.wikipedia.org/wiki/Broadcast_domain
[22] http://www.oit.ucsb.edu/committees/cnc-beg/vlan_id.asp

Εικόνα 6-1 Tagged Packet

Τα VLANs είναι συμβατά με πολλά level – 2 – layers όπως Ethernet, FDDI, Token Ring και MAC.

6.2 Περιγραφή Σεναρίου

Σε αυτό το σενάριο πρόκειται να προσομοιώσουμε το δίκτυο EADC(European Aeronautic και Defence Company), το οποίο αποτελείται από 4 δίκτυα: 2 project groups (Eurofighter και AirbusA380), τα οποία πρέπει να μοιραστούν πληροφορίες για ένα νέο σχέδιο μηχανών; ένα γενικό σωματειακό δίκτυο πληροφοριών(WebAndMailServer), και ένα δίκτυο αποκαλούμενο TopSecret με τις εμπιστευτικές πληροφορίες που θέλουμε να προστατέψουμε από τους εισβολείς που θέλουν να αποκτήσουν πρόσβαση. Έχουμε ένα κατάσκοπο(the secretary), ο οποίος υποτίθεται ότι έχει πρόσβαση οπουδήποτε αλλού εκτός από τον WebAndMailServer.

Group	Server	Stations
Secretary	WebAndMailServer	Secretary
Eurofighter	Eurofighter DB	EurofighterEnginner, EurofighterTeamLeader
Airbus A380	Airbus A380 DB	AirbusA380Enginner, AirbusA380TeamLeader
Managers	TopSecret DB	President, CEO

Εικόνα 6-2 Distributing stations into groups

Στο πρώτο σενάριο, NoVLAN, δεν θα διαμορφώσουμε τις δυνατότητες των switch VLAN, και κατόπιν ο κατάσκοπος θα αποκτήσει πρόσβαση στην εμπιστευτική βάση δεδομένων. Στο δεύτερο σενάριο, SeperatedVLANs, τέσσερα ανεξάρτητα VLANs θα κάνουν οποιονδήποτε άλλον εκτός από τους χρήστες που έχουν πρόσβαση στον κεντρικό υπολογιστή TopSecret. Αυτό θα εξασφαλίσει την ασφάλεια, αλλά δεν θα επιτρέψει στον Eurofighter και στον AirbusA380 να επικοινωνήσουν μεταξύ τους, και έτσι οι απαιτήσεις σεναρίου δεν είναι εκπληρωμένες. Στο τρίτο σενάριο, VLANsCommunicatedWithOneArmedRouter θα επιτρέψουμε στα δύο groups να επικοινωνήσουν μεταξύ τους με την βοήθεια ενός μοναδικού router.

6.3 Δημιουργία του Σεναρίου

1. Ανοίξτε ένα καινούργιο Project στο OPNET IT Guru Academic Edition(**File→ New Project**) χρησιμοποιώντας τις παρακάτω παραμέτρους (αφήστε τις υπόλοιπες παραμέτρους σε default κατάσταση):
    - **Project Name: <your_name>_VLANs**
    - **Scenario Name: SenseVLAN**
    - **NetworkScale: Office**

Πιέστε **Next** κατά τη διάρκεια ολόκληρου του Startup Wizard μέχρι το τέλος.

Zoom + 

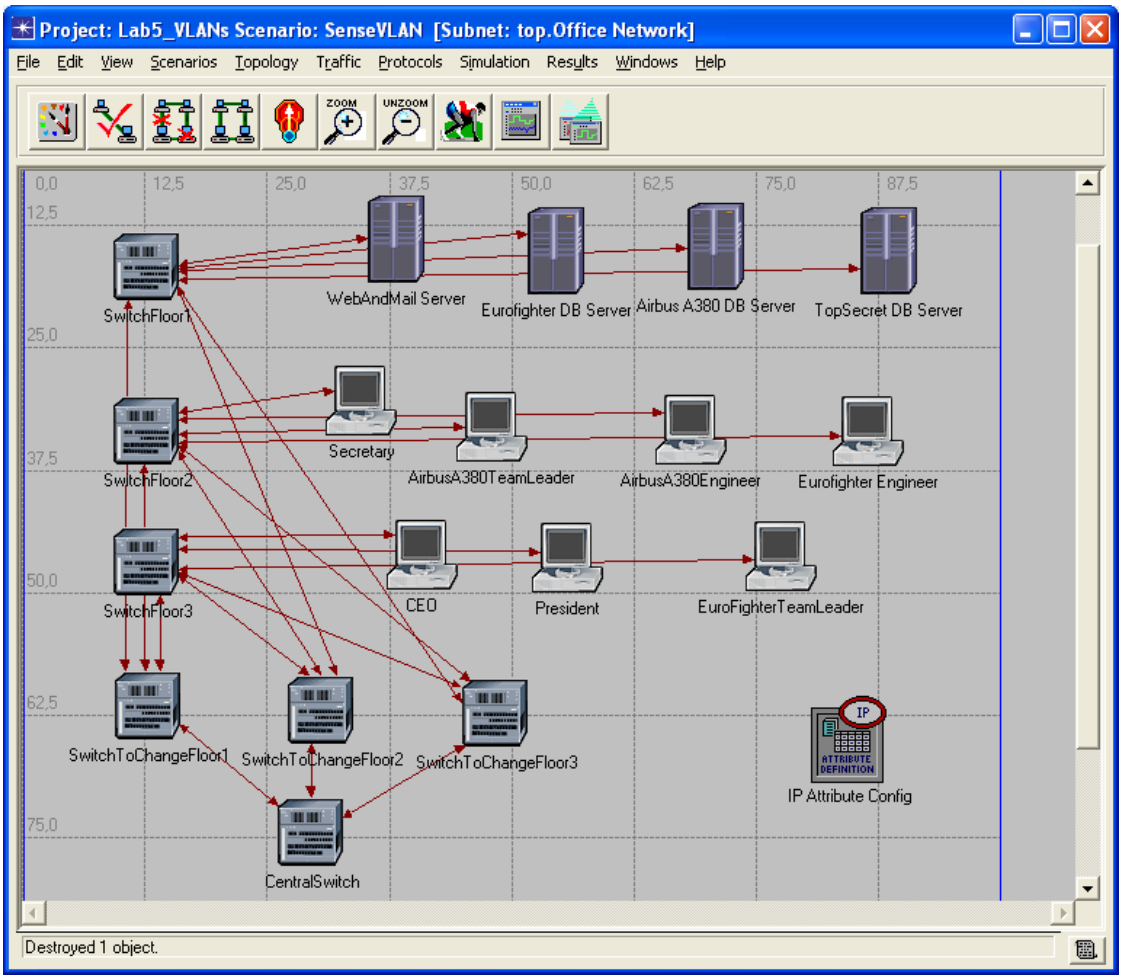
, πάνω από μια ζώνη στο σενάριο προκειμένου να εργασθείτε με όλο το πλέγμα όταν το παράθυρο μεγιστοποιηθεί.

2. Συμπληρώστε στο σενάριο τα παρακάτω χαρακτηριστικά:

Qty	Component	Palette
4	ethernet_server	internet toolbox
7	ethernet_wkstn	internet toolbox
7	ethernet16_switch	internet toolbox
1	IP Attribute Config	internet toolbox
	100BaseT	internet toolbox

Εικόνα 6-3 Components of our network

Η εικόνα 6.4 μας παρουσιάζει τα χαρακτηριστικά στο πλέγμα με το τελικό τους σχεδιάγραμμα. Είναι πολύ σημαντικό να διατηρηθούνε οι συγκεκριμένες ονομασίες(**δεξί κλικ→ Set Name**), γιατί θα αναφερόμαστε με τα ονόματα από εδώ και στο εξής.



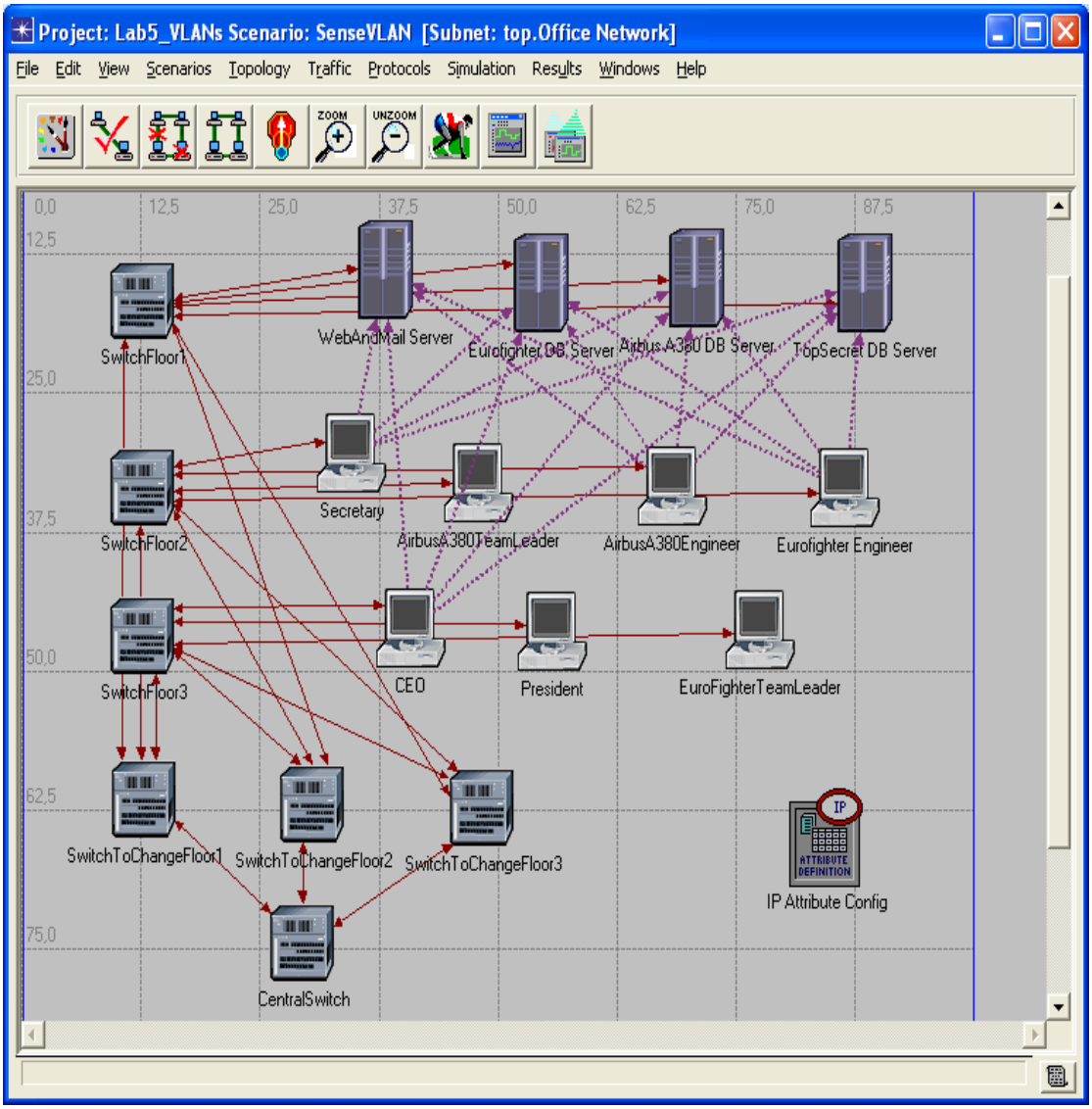
Εικόνα 6-4 The scenario once completed

Η δομή συνίσταται σε 4 ορόφους με κάθε σταθμό να έχει ένα switch και κεντρικό υπολογιστή στους ορόφους που ονομάζονται SwitchFloor1…3. Στον όροφο 0 έχουμε επίσης 3 switch που ονομάζονται SwitchToChangeFloor1…3 και ένα CentralSwitch. Το CentralSwitch με όλα τα switch που ονομάζονται SwitchToChangeFloors, και κάθε SwitchToChangeFloor είναι συνδεδεμένο με όλα τα SwitchFloor.
Στον όροφο #1, έχουμε τα εξής: CEO, President και τον EurofighterTeamLeader. Στον όροφο #2, έχουμε τα εξής: Secretary, AirbusA380TeamLeader, AirbusA380Engineer και τον Eurofighter Engineer. Στον όροφο #3, έχουμε όλους τους κεντρικούς υπολογιστές: WebAndMailServer, TopSecret DB, AirbusA380 DB και τον Eurofighter.
Επιπλέον έχουμε αλλάξει μερικά όχι και τόσο σημαντικά χαρακτηριστικά(αλλάξαμε το εικονίδιο Hacker και σύραμε τη δομή του κτηρίου).

3. Διαμόρφωση των Pings:

Κανένα σχεδιάγραμμα ή εφαρμογή δεν θα διαμορφωθεί σε αυτό το σενάριο, επειδή το μόνο που θέλουμε να μάθουμε είναι ποιοί σταθμοί έχουν πρόσβαση σε ποιούς

κεντρικούς υπολογιστές. Πρέπει μόνο να χρησιμοποιήσουμε τα ping tools. Θα εκτελέσουμε ένα ping από έναν τυχαίο σταθμό από κάθε ομάδα(Eurofighter, AirbusA380, Secretary και CEO) σε κάθε έναν από τους 4 κεντρικούς υπολογιστές. Συγχρόνως θα μελετήσουμε το trace, έτσι ώστε να επεξεργασθούμε τις ιδιότητες του ping, και να ρυθμίσουμε το εξής: **Ping Pattern: Record Route.** Τα pings δημιουργούνται με το συστατικό **ip_ping_traffic** από την παλέτα **internet_toolbox**. Αντί να δημιουργήσουμε τις απαιτήσεις κυκλοφορίας, και να επεξεργασθούμε τις ιδιότητες, μετά την αλλαγή του Ping Pattern, είναι ευκολότερο να δημιουργήσουμε μια απαίτηση κυκλοφορίας και να την κάνουμε αντιγραφή-επικόλληση τις υπόλοιπες φορές που θα μας χρειαστεί.



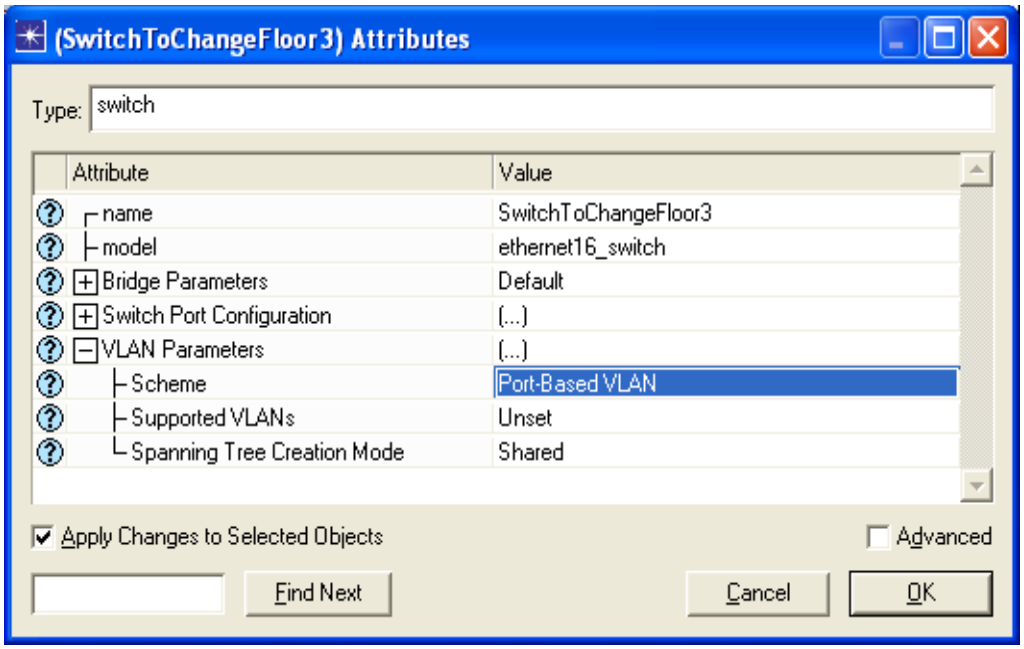
Εικόνα 6-5 Creating Pings

4. Διαμόρφωση της διάρκειας προσομοίωσης:

Στον project editor, κάνουμε κλικ στο **configure/run simulation**  , και ρυθμίζουμε το **Duration: 15 minute(s).** Κάνουμε κλικ στο **OK**.(μην ξεκινήσετε την προσομοίωση ακόμα)

6.4 Δημιουργία του δεύτερου και τρίτου σεναρίου

1. Από τον project editor, **Scenario→ Duplicate Scenario**… Ονομάστε το νέο σενάριο **SeperatedVLANs** και πιέστε **OK.**
2. Επιλέξτε όλα τα switches και αλλάξτε από τις ιδιότητες την εξής τιμή: **VLAN Parameters→ Scheme: Port-Based VLAN,** σε όλα από αυτά. Τώρα αυτά τα switches θα διαιρέσουν τις συνδεδεμένες συσκευές στα εικονικά δίκτυα. Θυμηθείτε να χρησιμοποιήσετε το εξής: **Apply Changes to Selected Objects.**



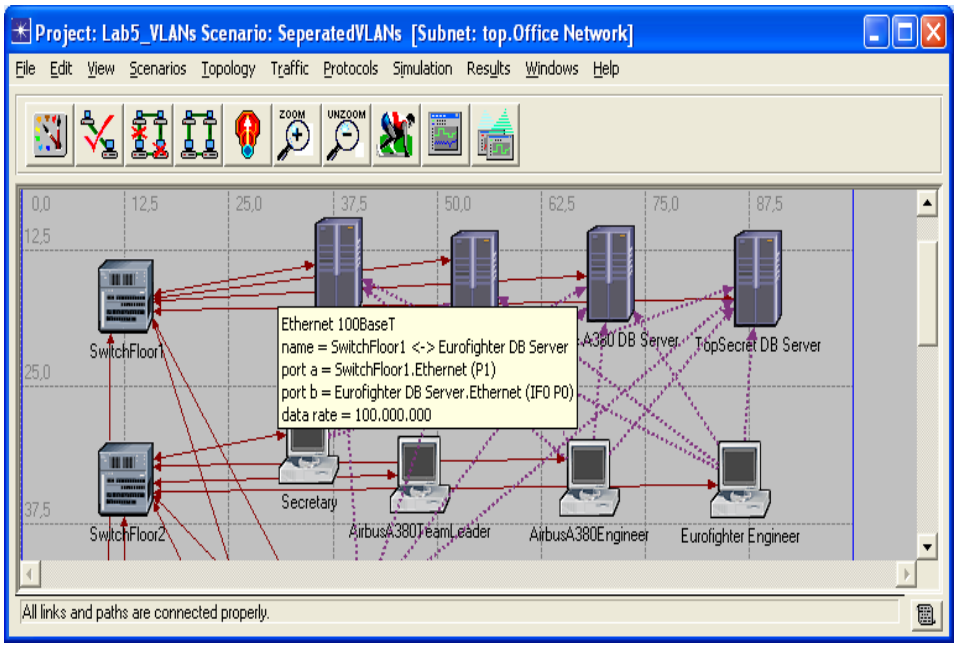
Εικόνα 6-6 Changing the Scheme of Switches

3. Καθορισμός των VLANs:

   - Καθορισμός των switches

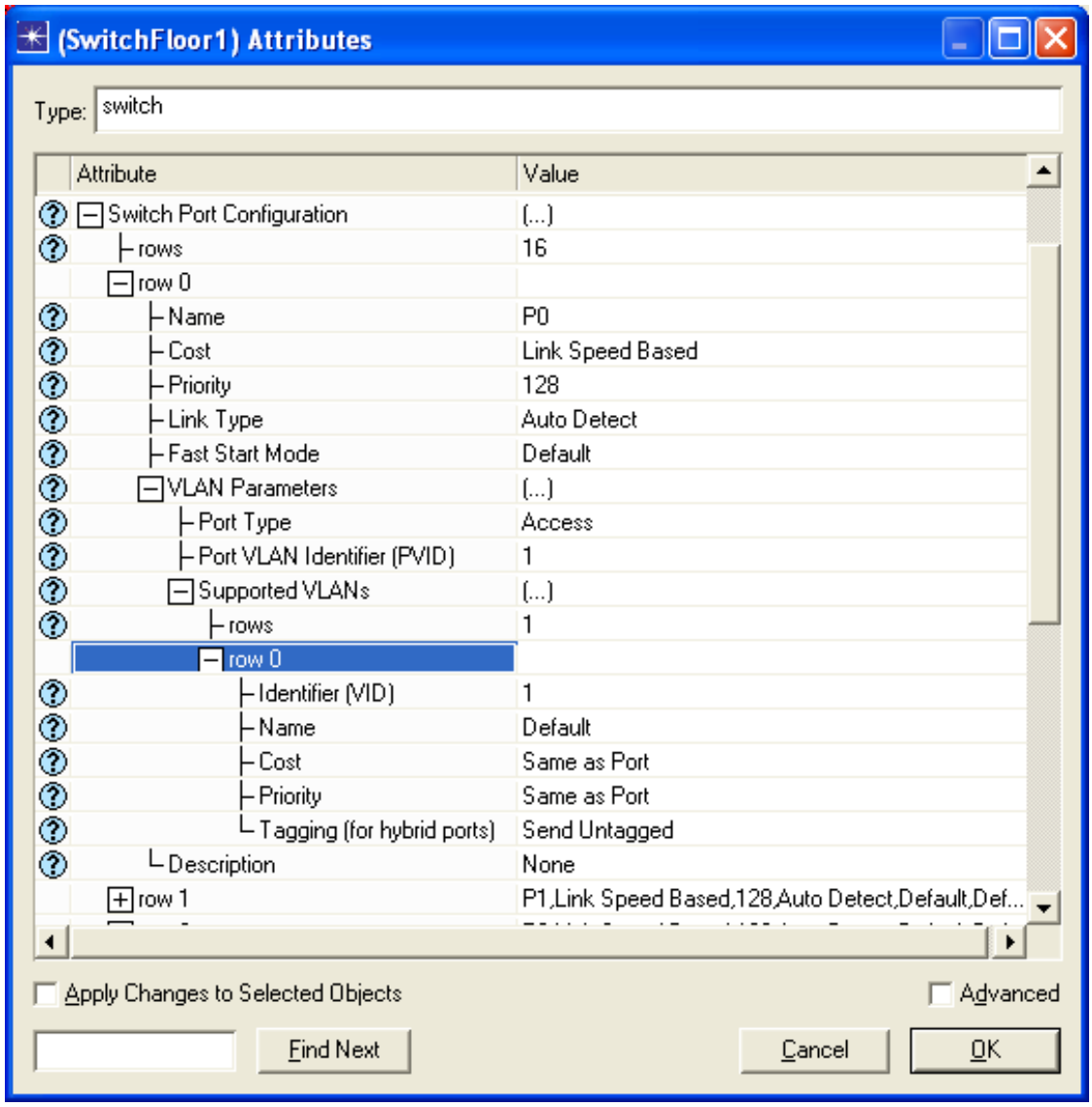
Κάθε σταθμός ή κεντρικός υπολογιστής ανήκει σε ένα VLAN. Κάθε switch είναι συνδεδεμένο στους σταθμούς με ένα διαφορετικό port. Μπορούμε να το δούμε επιλέγοντας την σύνδεση με τον δείκτη του ποντικιού και περιμένοντας λίγα

δευτερόλεπτα. Στην εικόνα 6.6 η σύνδεση είναι το SwitchFloor1 – EurofighterDB, και η port του switch είναι η P0. Σημειώστε όλες τις συνδέσεις και τα ονόματα των ports, γιατί θα σας χρειαστούν στην συνέχεια.



Εικόνα 6-7 Finding out the link interfaces

Το ταίριασμα port, αριθμός-σύνδεσης καθιερώνεται όταν η σύνδεση δημιουργείται, και μπορεί να είναι διαφορετικό ανάλογα με την σειρά δημιουργίας, έτσι είναι λάθος να τα γράψουμε μέσα σε αυτό το manual, αλλά μπορούμε να εργαστούμε με τις ιδιότητες των switch.



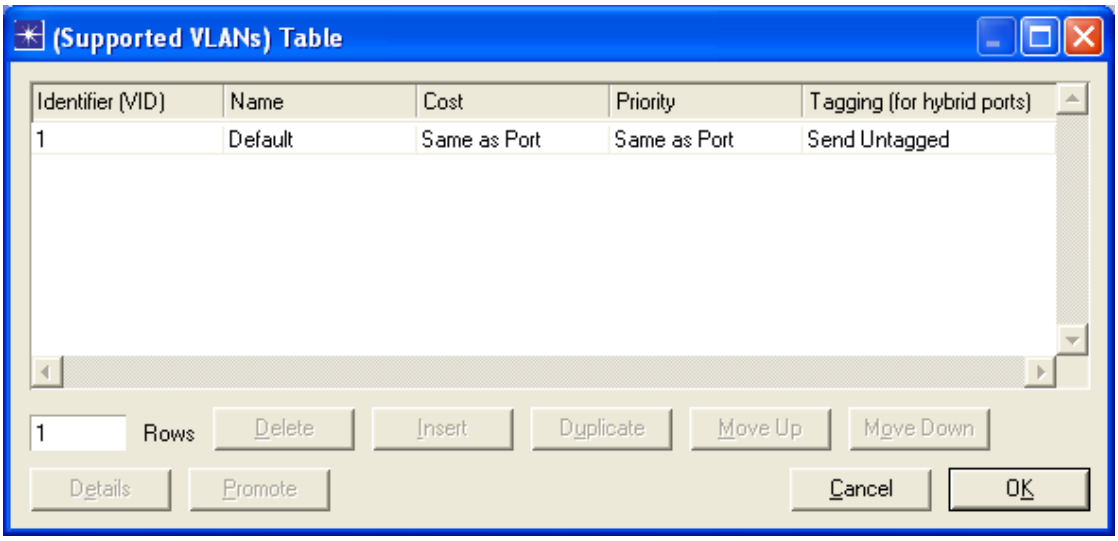
Εικόνα 6-8 Switches' Attributes

Εάν κάνουμε κλικ στο σημείο ερώτησης του κάθε πεδίου μπορούμε να δούμε μια λεπτομερή περιγραφή.

- **VLAN Parameters→ Supported VLANs**

Συγκεκριμένα VLANs που υποστηρίζονται απο αυτόν τον κόμβο παρέχουν τις απαραίτητες ιδιότητες για να διαμορφώσουμε αυτά τα υποστηριγμένα VLANs. Σε default κατάσταση ο κόμβος υποστηρίζει ένα απλό VLAN, το οποίο είναι "VLAN 1" (δηλαδή default VLAN)

Για να διαμορφώσουμε τα VLANs που υποστηρίζονται από ένα port μπορούμε να κάνουμε κλικ στο πεδίο, select **Edit…**και στο παράθυρο διαλόγου που θα εμφανιστεί προσθέτουμε μια σειρά για κάθε VLAN που υποστηρίζεται από τον κόμβο, ο οποίος προσδιορίζεται από το VID του. Οι υπόλοιπες παράμετροι θα μείνουν με τις default τιμές.



Εικόνα 6-9 Adding Supported VLANs in a switch

- **Switch Port configuration→ row *num_port*→ VLAN Parameters→ Port VLAN Identifier (PVID)**

Διευκρινίζει το προσδιοριστικό VLAN που θα οριστεί σε "all incoming" "untagged" πακέτα σε αυτό το port (εάν η συσκευή υποστηρίζει VLANs).
Για τα access ports, το PVID του port πρέπει να είναι το VID ενός από τα VLANs που διευκρινίζονται κάτω από τις παραμέτρους του κόμβου "VLAN Parameters→ Supported VLANs"

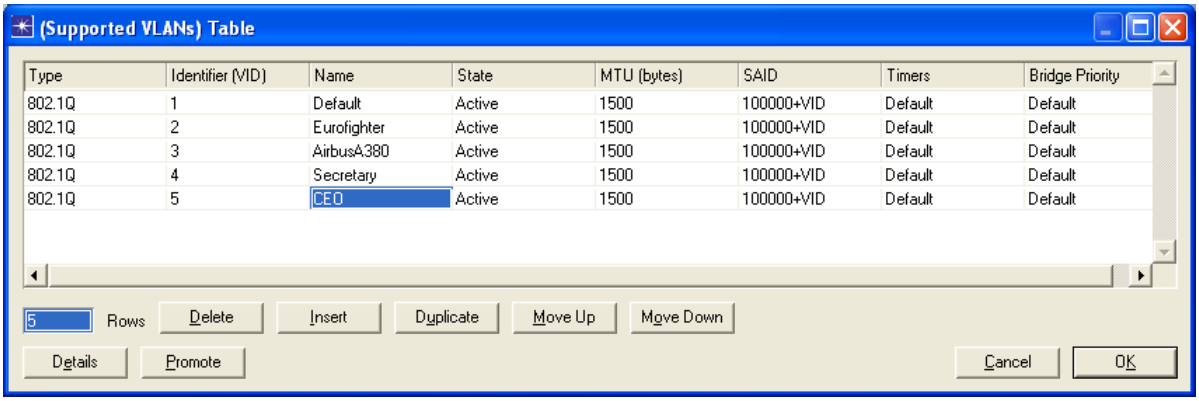
- **Switch Port configuration→row *num_port*→ VLAN Parameters→ Port Type**

Διευκρινίζει το port type. Ο τύπος του port καθορίζει πως θα προωθηθούν τα πακέτα. Τα Access port παίρνουν αποσπούν πληροφορίες από τα VLANs από τα πακέτα πριν αυτά προωθηθούν, ενώ τα tunk ports στέλνουν πάντα τα πακέτα VLAN-tagged, έτσι πάντα περιέχουν πληροφορίες για τα VLAN. Τα υβριδικά ports κάνουν κάτι ανάμεσα σε: στέλνουν τα πακέτα είτε VLAN-tagged είτε untagged κάτι που βασίζεται στην ταξινόμηση VLAN του πακέτου. Στις τυπικές διαμορφώσεις, τα access ports χρησιμοποιούνται για να συνδέσουν end-nodes και VLAN-unaware-nodes με το VLAN-aware-bridged-network, ενώ οι trunk ports χρησιμοποιούνται για να συνδέσουν το VLAN-aware bridges/switches του bridged-network το ένα με το άλλο. Με βάση την ίδια λογική, υβριδικοί ports χρησιμοποιούνται για να συνδεθούν με το VLAN μέσω του οποίου μερικά end nodes και μερικά VLAN-aware nodes είναι αποδεχτά. Ανεξάρτητα από αυτόν τον τύπο, οι ports μπορούν να υποστηρίξουν όσα VLANs θέλουν εφόσον αυτά τα VLANs υποστηρίζονται από τον περιβάλλοντα κόμβο. Από τις trunk ports αναμένουμε να υποστηρίξουν multiple VLANs, αλλά πρέπει να διαμορφωθούν με

- **Switch Port configuration→ row *num_port*→ VLAN Parameters→ Supported VLANs→ Identifier**

Προσδιοριστικό του VLAN που υποστηρίζεται σε αυτόν τον port. Αυτό το προσδιοριστικό VLAN πρέπει να καθοριστεί υπό τις παραμέτρους του κόμβου "VLAN Parameters→ Supported VLANs"

Αυτή η παράμετρος διαμορφώνεται για κάθε port (*num_port*).
Διαμορφώνουμε κάθε switch me **Supported VLANs: Default (VID 1), Eurofighter (2), AirbusA380 (3), Secretary (4) και Management (5).** Έκτοτε πρέπει να επιλέξουμε όλα τα switches, **right button→ Edit Attributes** και ρυθμίζουμε το Supported VLANs όπως φαίνεται στην παρακάτω εικόνα. Μην ξεχάσετε να τσεκάρετε το **Apply Changes to Selected Objects.**



Εικόνα 6-10 VLANs supported by this Lab's switches

Ο επόμενος πίνακας μας δίνει λεπτομέρειες για τη διαμόρφωση για το κάθε switch's port, και πως οι ιδιότητες πρέπει να ρυθμιστούν. Ο αριθμός των port γράφεται στην παρένθεση, επειδή είναι ο αριθμός port που είχαμε ήδη, αλλά μπορεί να είναι και διαφορετικός ανάλογα με την σειρά δημιουργίας.

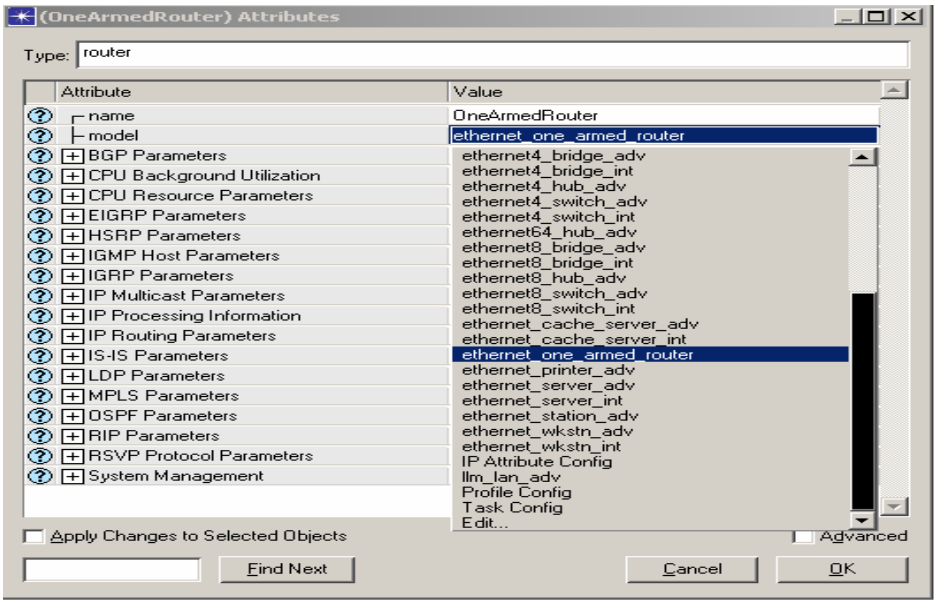
Switch	Port	Type	Supported VLANs	PVID
SwitchFloor3	Link EurofighterDB (P14)	Access	2 (Eurofighter)	2
	Link BDAirbusA380 (P13)	Access	3 (Airbus380)	3
	Link WebAndMailServer (P11)	Access	4 (Secretary)	4
	Link BDTopSecret (P12)	Access	5 (Management)	5
	Links with SwitchToChangeFloor1,2 και 3 (P0,P1,P10)	Trunk	2,3,4,5 (Eurofighter, Airbus380, Secretary, Management)	1
SwitchFloor2	Link Secretary (P11)	Access	4 (Secretary)	4
	Link AirbusA380TeamLeader (P12)	Access	3 (Airbus380)	3
	Link AirbusA380Engineer (P13)	Access	3 (Airbus380)	3
	Link EurofighterEngineer (P14)	Access	2 (Eurofighter)	2
	Links with SwitchToChangeFloor1,2 και 3 (P0,P1,P10)	Trunk	2,3,4,5 (Eurofighter, Airbus380, Secretary, Management)	1
SwitchFloor1	Link CEO (P11)	Access	5 (Management)	5
	Link President (P12)	Access	5 (Management)	5
	Link Eurofighter TeamLeader (P13)	Access	2 (Eurofighter)	2
	Links with SwitchToChangeFloor1,2 και 3 (P0,P1,P10)	Trunk	2,3,4,5 (Eurofighter, Airbus380, Secretary, Management)	1
SwitchToChangeFloor1, SwitchToChangeFloor2, SwitchToChangeFloor3, CentralSwitch	Links SwitchToChangeFloor to Central Switch (P0) Links CentralSwitch to SwitchToChangeFloor1,2 and 3 (P0,P1,P10) Link CentralSwitch-OneArmed-Router (P11) (Αυτή η σύνδεση θα δημιουργηθεί στο σενάριο VLANsCommunicatedWithOneArmedRouter)	Trunk	2,3,4,5 (Eurofighter, Airbus380, Secretary, Management)	1

Εικόνα 6-11 Configuring the Lab's switches

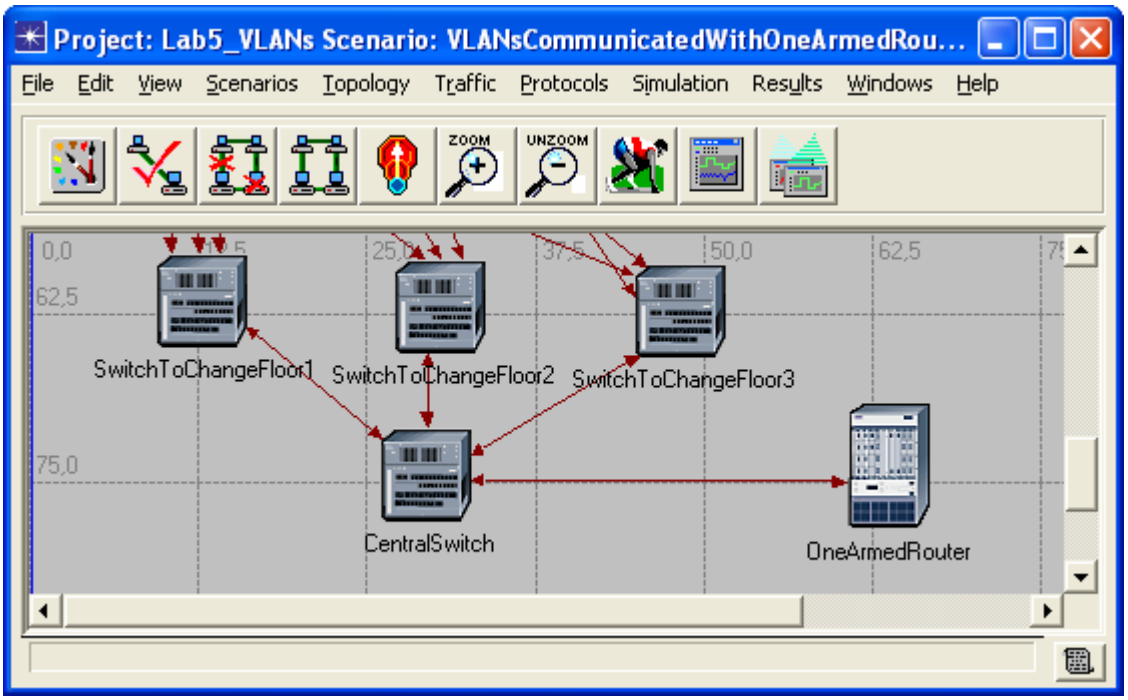
6.5 Δημιουργία του δεύτερου σεναρίου

Το πρώτο σενάριο χωρίζει τα VLANs φροντίζοντας την ασφάλεια της διαχείρισης VLAN, αλλά δημιουργεί 4 απομονωμένα δίκτυα που δεν μπορούν να επικοινωνήσουν μεταξύ τους. Θέλουμε τα δίκτυα Eurofighter και AirbusA380 να επικοινωνούν μεταξύ τους, έτσι σε αυτό το σενάριο θα χρησιμοποιήσουμε ένα δρομολογητή για να καταστήσουμε την επικοινωνία μεταξύ τους δυνατή.
Η επικοινωνία Inter-VLAN μπορεί να πραγματοποιηθεί χρησιμοποιώντας δρομολογητές, επειδή οι πληροφορίες που σχετίζονται με την ορθότητα VLAN δεν υπάρχουν όταν τα πακέτα ταξιδεύουν στο IP. Εάν ένας δρομολογητής είναι συνδεμένος σε μια συσκευή VLAN-aware με ένα Access Port με PVID 1(default VLAN) τότε τα πακέτα που φθάνουν σε αυτόν τον δρομολογητή θα ενσωματωθούν στο VLAN #1, έπειτα θα αναμεταδοθούν σε όλα τα ports δικτύων στον προορισμό τους, εφόσον αυτά τα ports ανήκουν στο VLAN #1.

1. Από τον **Project Editor, Scenarios→ Duplicate Scenario…** Το νέο σενάριο θα έχει **Scenario Name: VLANsCommunicatedWithOneArmedRouter.**
2. Επεκτείνετε στο σενάριο ένα **ethrenet_one_armed_router.** Αυτό το προϊόν μπορεί να μην είναι διαθέσιμο από την παλέτα αντικειμένων, εξαρτάται από ποιά έκδοση OPNET IT Guru έχετε, αλλά μπορείτε να το χρησιμοποιήσετε με την τοποθέτηση στο πλέγμα οποιασδήποτε συσκευής, και μετά αλλάξτε την τιμή του **model** από τα **Attributes**, και κατόπιν επιλέξτε το σωστό component από το list box (εικόνα L7.11). Συνδέστε το δρομολογητή στο Central Switch χρησιμοποιώντας 100BaseT καλώδια. Μετονομάστε το δρομολογητή, **Name: OneArmedRouter.** Τέλος κάντε κλικ στο OK.



Εικόνα 6-12 Changing any component to an ethernet_one_armed_router



Εικόνα 6-13 The new OneArmedRouter

3. Ρυθμίζουμε το δρομολογητή για να επιτρέψει την inter-VLAN επικοινωνία:

Η περιγραφή του εργαστηρίου μας λέει ότι τα μόνα δύο VLAN που πρέπει να επικοινωνήσουν μεταξύ τους είναι τα Eurofighter και AirbusA380. Αυτό μπορεί να γίνει με ένα one-armed-router, ο οποίος είναι ένας δρομολογητής με ένα ενιαίο φυσικό interface που υποστηρίζει πολλά subinterfaces. Κάθε ένα από αυτά τα subinterfaces είναι σημειωμένα στα VLANs που θέλουμε να επικοινωνήσουν μεταξύ τους. Παραδείγματος χάριν, σε αυτό το δίκτυο το φυσικό interface του δρομολογητή υποστηρίζει δύο subinterfaces που θα δρομολογούν τα Eurofighter και AirbusA380. Οι IP διευθύνσεις του subinterface, Οι κόμβοι που ανήκουν στο ίδιο VLAN, οι τερματικοί σταθμοί και οι κεντρικοί υπολογιστές που ανήκουν στο ίδιο VLAN είναι παράμετροι που μπορούν να διαμορφώσουν κάθε VLAN προκειμένου να αντιστοιχηθεί σε ένα IP δίκτυο:

- VLAN Eurofighter: 192.0.2.0/24
- VLAN AirbusA380: 192.0.3.0/24
- VLAN Secretary: 192.0.4.0/24
- VLAN Management: 192.0.5.0/24

Τα πακέτα που φθάνουν σε μια μία IP διεύθυνση του δρομολογητή θα ενσωματωθούν στο sub interface που ανήκουν, ανάλογα με το VLAN, έτσι τα πακέτα θα δρομολογηθούν στο επόμενο hop, μέσω ενός άλλου sub interface, το οποίο καθορίζει αν το VLAN είναι το κατάλληλο για το εξερχόμενο πακέτο.

Για να διαμορφώσουμε το sub interface του one-armed-router πρέπει να επεξεργασθούμε τις ιδιότητες **IP Routing Parameters→ Interface Information→ row 0→ Subinterface information→ row *num_subinterface.*** Σε αυτήν την ιδιότητα, μπορούμε να αντιστοιχίσουμε κάθε interface σε ένα VLAN αλλάζοντας την ιδιότητα **Layer 2 Mapping→ VLAN Identifier.** Κατά την διαμόρφωση ενός interface για να υποστηρίζει subinterfaces, είναι απαραίτητο να διαμορφώσουμε επίσης και τις παραμέτρους κάτω από την διακλάδωση **Interface Information→ Subinterface Information** του πρωτοκόλλου δρομολόγησης που χρησιμοποιείται σε αυτό το subinterface. Για το παράδειγμα μας, αυτό είναι το **RIP Parameters.**

- Αναθέτουμε τις IP διευθύνσεις σε όλους τους σταθμούς

Station	IP Address
EurofighterEngineer	192.0.2.2
EurofighterTeamLeader	192.0.2.3
EurofighterDB	192.0.2.4
AirbusA380Engineer	192.0.3.2
AirbusA380TeamLeader	192.0.3.3
AirbusA380DB	192.0.3.4
Secretary	192.0.4.2
WebAndMailServer	192.0.4.3
CEO	192.0.5.2
President	192.0.5.3
TopSecretDB	192.0.5.4

Εικόνα 6-14 IP Addresses of all workstations

Η μάσκα υποδικτύου είναι 255.255.255.0 για όλες τις συσκευές.
Αυτές οι παράμετροι πρέπει να ρυθμιστούν στις ιδιότητες των σταθμών απο εδώ: **IP Host Parameters→ Interface Information,** στα πεδία **Address** και **Subnet Mask.**

- Επεξεργαζόμαστε τις ιδιότητες του **OneArmedRouter.**

Επεκτείνετε την ιεραρχία **IP Routing Parameters→ Inetrface Information→ row.** Καθορισμένη διεύθυνση: No Address και αλλάξτε τις τιμές στο Subinterface Information→ rows σε 4, για κάθε ξεχωριστό Subinterface των VLANs. Κατόπιν επεκτείνετε τα rows και αλλάξτε μόνο τα ακόλουθα:

row	Name	Status	Address	Subnet Mask	VLAN ID
0	IF0.2	Same as Parent	192.0.2.1	255.255.255.0	2
1	IF0.3	Same as Parent	192.0.3.1	255.255.255.0	3
2	IF0.4	Shutdown	192.0.4.1	255.255.255.0	4
3	IF0.5	Shutdown	192.0.5.1	255.255.255.0	5

Εικόνα 6-15 Setting the OneArmedRouter subinterfaces

Το Status Field μας λέει ποιά VLANs πρέπει να διασυνδεθούν, έτσι μόνο το VLAN 2 και 3 πρέπει να είναι up, και όταν ρυθμίζουμε **Same as Parent** σημαίνει ότι έχει την ίδια κατάσταση με το interface, έτσι αυτό το subinterface θα είναι up επίσης.

- Θέτουμε τις παραμέτρους δρομολόγησης των subintefaces.

Στις ιδιότητες του OneArmedRouter, επεκτείνουμε τον κλάδο RIP, **Parameters→ Interface Information→ row 0→ Subinterface Information.** Είναι πιθανό ότι τα 4 rows των δύο subinterfaces που μόλις δημιουργήσαμε να μην είναι ορατά ακόμα, σε

αυτήν την περίπτωση κλείνουμε το παράθυρο διαλόγου πατώντας **OK** και το ανοίγουμε πάλι. Πρέπει να ελέγξουμε ότι όλα έχουν το **Name** πεδίο με τις τιμές που ρυθμίσαμε πριν.

- Επεξεργαζόμαστε τις παραμέτρους της port, της σύνδεσης **CentralSwitch** με το **OneArmedRouter.**

Στην περίπτωση μας ήταν P11. Πρέπει να ρυθμίσουμε τις εξής τιμές: **Switch Port Configuration→ row num_port→ VLAN Parameters→ Port VLAN Identifier (PVID): 1; Port Type: Trunk; Supported VLANs: 2 και 3**(πρέπει να δημιουργήσουμε δύο νέα rows και να ρυθμίσουμε αυτά τα VIDs).

4. Ξεκινάμε την προσομοίωση.

Από το **Project Editor→ Scenarios→ Manage Scenarios…** Μπορούμε είτε να επιλέξουμε **<collect>** είτε **<recollect>** από την στήλη **Results** για κάθε σενάριο, και κατόπιν να πατήσουμε **OK.** Όταν οι 3 προσομοιώσεις τελειώσουν κάνουμε κλικ στο **Close.**

6.6 Ερωτήσεις

6.6.1 Ερώτηση 1η

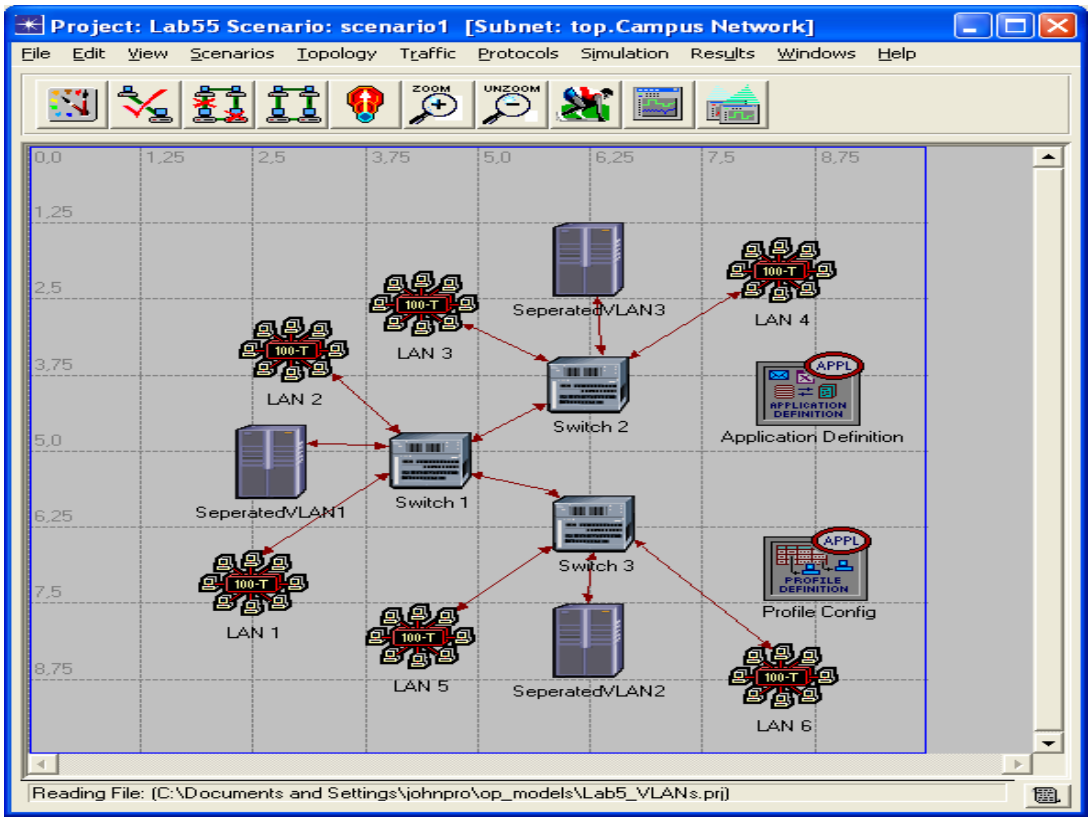
Συγκρίνετε τα επιτυχημένα και ανεπιτυχή pings. Σε ποια σενάρια έχουμε ασφαλή TopSecretDB ενάντια στις επιθέσεις Secretary? Σε ποιά σενάρια οι σταθμοί Eurofighter και AirbusA380 επικοινωνούν μεταξύ τους?

6.6.2 Ερώτηση 2η

Τα VLANs χρησιμοποιούνται επίσης για την μείωση της κίνησης δικτύων. Δημιουργήστε ένα σενάριο που περιλαμβάνει:

- 6 LANs 100BaseT_LAN
- 3 switches ethernet16_switch
- 1 control Application Config
- 1 control Profile Config
- 3 ethernet_server servers

Με αυτά τα χαρακτηριστικά δημιουργούμε το σενάριο της εικόνας L7.15 που ονομάζεται **VLANsTrafficReductionWithoutVLANs,** το οποίο χρησιμοποιεί 100BaseT καλώδια. Είναι σημαντικό να χρησιμοποιήσουμε τα ίδια ονόματα που χρησιμοποιούνται στην εικόνα καθώς θα αναφερόμαστε σε κάθε μονάδα χρησιμοποιώντας τα ονόματα της από εδώ και στο εξής.



Εικόνα 6-16 Station IP Addresses

Στο Application Config control μπορούμε να αλλάξουμε μόνο την τιμή του πεδίου Application Definitions στην default τιμή. Με αυτόν τον τρόπο θα δημιουργηθούν μερικές τυπικές εφαρμογές, τις οποίες μπορούμε να δούμε αργότερα από το Profile Config control.

Δημιουργήστε ένα μοναδικό σενάριο με όνομα **CommonProfile**, το οποίο θα δεχθεί τις εφαρμογές **Database Access (Heavy), File Transfer (Heavy), Email (Heavy),** οι οποίες θα είναι μέρος της **Default Application Definitions.**

Αλλάξτε τις ιδιότητες των 3 κεντρικών υπολογιστών έτσι ώστε να έχουν το πεδίο **Application: Supported Servises** σε **ALL.** Με αυτό τον τρόπο τώρα έχουμε όλες τις εφαρμογές με όλες τις υπηρεσίες καθορισμένες στο Applications control.

Τα 6 δίκτυα LANs μπορούν να δημιουργηθούν με τις παρακάτω τιμές:

- **Number of Workstations: 10**
- **Applications: Supported Profiles** εισάγουν ένα μοναδικό προφίλ που καθορίζεται στο **CommonProfile.** Θέλουμε όλοι οι τερματικοί σταθμοί του LAN να έχουν αυτό το προφίλ, έτσι μπορούμε να ρυθμίσουμε το **Entire Lan** στο πεδίο **Number of Clients.**

Ονομάστε τους 6 τερματικούς σταθμούς **LAN 1,…,LAN 6,** και τους κεντρικούς υπολογιστές **ServerVLAN 1,…,ServerVLAN3;** Ρυθμίστε την διάρκεια προσομοίωσης

σε **20 minutes;** Αναπαράγετε το σενάριο και ονομάστε το νέο **VLANsTrafficReductionWithVLANs.** Ρυθμίστε τα switches του σεναρίου έτσι ώστε να έχουν 3 VLANs που το κάθε ένα φέρει 2 VLANs, όπως φαίνεται στην εικόνα. Ονομάστε τα 3 νέα VLANs με τα εξής ονόματα **Red, Green,** και **Blue** με VIDs 2, 3 και 4. Τα VLANs φέρουν τους ακόλουθους υπολογιστές:

- VLAN Red: LAN 2, LAN 4 και Server VLAN 2.
- VLAN Green: LAN 1, LAN 5 και Server VLAN 3.
- VLAN Blue: LAN 3, LAN 6 και Server VLAN 4.

α) Ποιές τιμές χρησιμοποιήσατε για να ρυθμίσετε τα switches?
β) Συγκρίνετε την point-to-point απόδοση δικτύου (throughput bits/sec) για κάθε μία από τις δύο συνδέσεις των δύο σεναρίων. Πόσο (%) έχει μειωθεί η κίνηση του δικτύου? Και γιατί?

6.7 Απαντήσεις

6.7.1 Απάντηση 1η

Μπορούμε να δούμε τα pings που πέτυχαν, όπως φαίνεται κι από εδώ **Simulation Log→ Classes→ ICMP→ Performance.**

- **NoVLAN**: Όλα τα Pings είναι πετυχημένα, έτσι ο Secretary μπορεί να επιτεθεί στον TopSecretDB.
- **SeparatedVLAN**: Τα μόνα πετυχημένα pings είναι του Intra-VLAN, επειδή δεν υπάρχει καμία Inter-VLAN επικοινωνία. Έκτοτε ο Secretary μπορεί να επιτεθεί στον TopSecretDB

VLANsCommunicatedWithOneArmedRouter. Τα μόνα πετυχημένα pings είναι του Intra-VLAN και για τα Inter-VLANs μόνο αυτά μεταξύ του Eurofighter και του AirbusA380, έτσι ο Secretary δεν μπορεί να επιτεθεί στον TopSecretDB.

6.7.2 Απάντηση 2η

Τα σενάρια είναι στο project.

α)

Switch	Port	Port Type	Supported VLANs	PVID
Switch1 Supported VLANs: 1,2,3,4	Link Switch2 (P10)	Trunk	2,3,4	1
	Link Switch3 (P11)	Trunk	2,3,4	1
	Link LAN (P0)	Access	3	3
	Link LAN (P1)	Access	1	1
	Link LAN (P12)	Access	4	4
Switch2	Link Switch1 (P10)	Trunk	2,3,4	1
	Link LAN (P0)	Access	4	4
Supported VLANs: 1,2,3,4	Link LAN (P1)	Access	2	2
	Link LAN (P11)	Access	3	3
Switch3 Supported VLANs: 1,2,3,4	Link Switch1 (P10)	Trunk	2,3,4	1
	Link LAN (P0)	Access	3	3
	Link LAN (P1)	Access	4	4
	Link LAN (P11)	Access	2	2

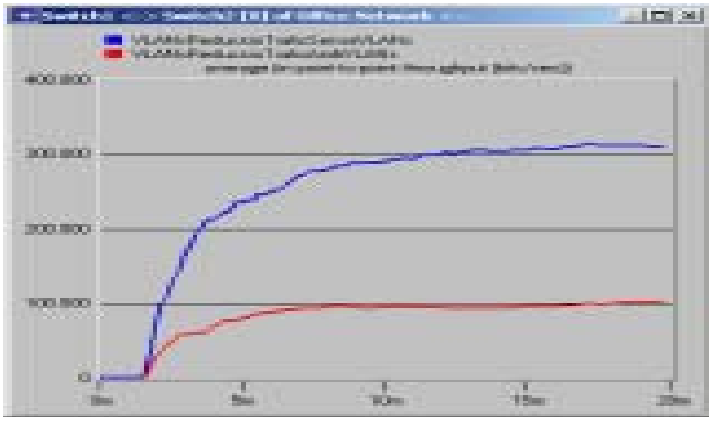
Εικόνα 6-17 VLAN Configuration

Όλα τα switches έχουν υποστηρίξει τα εξής VLANs: 1 (Default), 2 (Red), 3 (Green), 4 (Blue) και Scheme: Port-Based VLAN.

β)

Το φορτίο κυκλοφορίας χωρίς VLANs είναι 300,000 bits/sec και εάν δημιουργήσουμε 3 VLANs με τον ίδιο αριθμό τερματικών σταθμών και οι σταθμοί διανέμονται ομοιόμορφα μέσα στο δίκτυο, τότε το φορτίο κυκλοφορίας διαιρείται με 3 επειδή το τρίτο μέρος της "συναλλαγής" περιλαμβάνει κάποια εξαφάνιση (δεν υπάρχει καμία Inter-VLAN

επικοινωνία). Έκτοτε το φορτίο κυκλοφορίας μειώνεται στο τρίτο μέρος, περίπου κατά 100,000 bits/sec

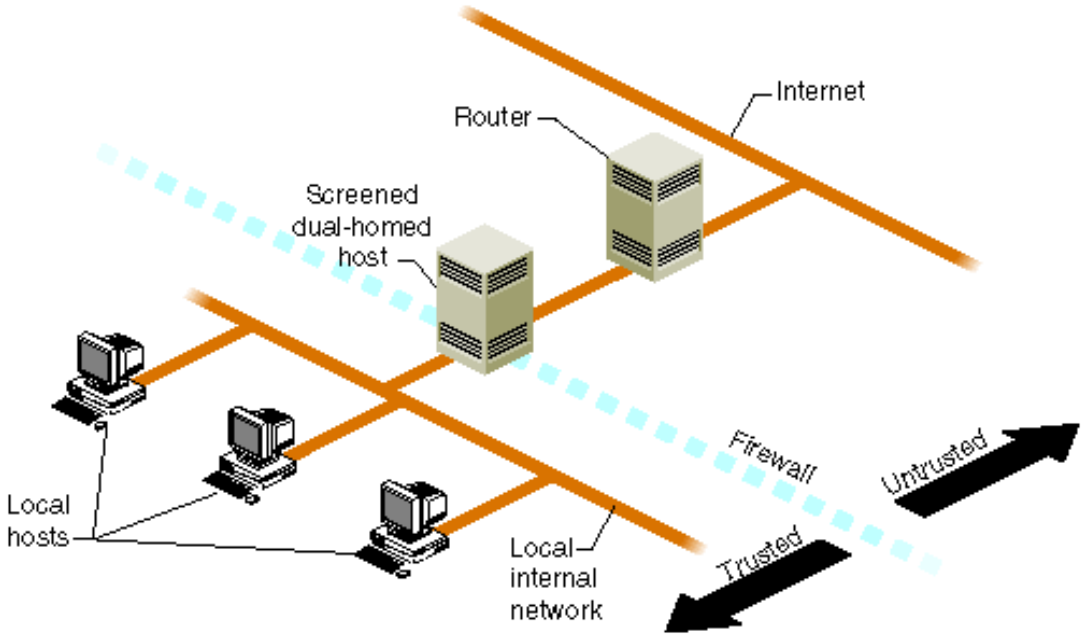


Εικόνα 6-18 Traffic Load Reduction because of VANs

Chapter 7 Screened Host / Subnet (DMZ)

7.1 Γενικά για το Screened Host[23]

- Φιλτράρισμα σε στρώμα-3 (πακέτα) και στρώμα-5 (εφαρμογή)
- Το φιλτράρισμα των πακέτων εκτελείται από τους δρομολογητές
- Ένα Firewall (aka bastion host) στο εσωτερικό δίκτυο λειτουργεί ως proxy και εγκαθιστά τις εξωτερικές και εσωτερικές συνδέσεις.
- Περιμετρική ασφάλεια (εσωτερικά/ εξωτερικά μηνύματα)
- Ο δρομολογητής χρησιμοποιείται για να περιορίσει την ποσότητα της κυκλοφορίας στον bastion host, που απορρίπτει ορισμένα πακέτα που καθορίζονται από την πολιτική ασφαλείας του δρομολογητή



Εικόνα 7-1 Screened Host

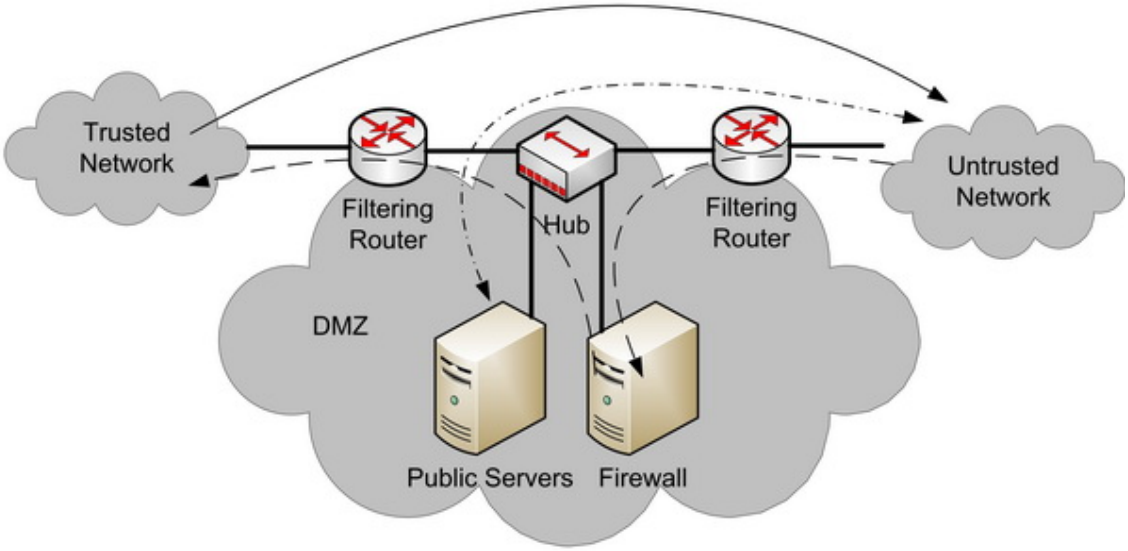
7.2 Γενικά για το Screened Subnet[24] (DMZ)

- Περιμετρική και εσωτερική ασφάλεια.
- Ο ίδιος δρομολογητής του Screened Host(εξωτερικό Firewall) προστατεύει τον κεντρικό υπολογιστή από τις εξωτερικές επιθέσεις.
- Ένας πρόσθετος δρομολογητής (εσωτερικό Firewall) προστατεύει τον κεντρικό υπολογιστή από τις εσωτερικές επιθέσεις.

[23] http://www.dmst.aueb.gr/dds/secimp/fv/sh.htm
[24] http://en.wikipedia.org/wiki/Screened-subnet_firewall

- Κατά συνέπεια έχουμε μια αποστρατικοποιημένη ζώνη (DMZ).Όλη η κυκλοφορία που έχει πρόσβαση σε αυτήν την περιοχή έχει διασχίσει έναν δρομολογητή (η εσωτερική καθώς επίσης και η εξωτερική κυκλοφορία δικτύων).

- Οι συνδέσεις που ελέγχονται από το proxy εξαρτώνται από το επίπεδο ασφαλείας που θέλουμε να πετύχουμε.



Εικόνα 7-2 Screened Subnet (DMZ)

7.3 Περιγραφή Σεναρίου

Πρώτα δημιουργούμε ένα σενάριο χρησιμοποιώντας το Screened Host, και έπειτα ένα δεύτερο σενάριο που αρχίζει από το πρώτο χρησιμοποιώντας Screened Subnet (DMZ). Θα δημιουργήσουμε ένα εσωτερικό δίκτυο με έναν κεντρικό υπολογιστή FTP, HTTP και DB, και ένα εσωτερικό δίκτυο με έναν κεντρικό υπολογιστή DB και FTP, και έναν κεντρικό υπολογιστή HTTP. Θέλουμε να προστατέψουμε τον DB και FTP κεντρικό υπολογιστή, από δύο είδη επιθέσεων: εσωτερικές και εξωτερικές. Επιπλέον θέλουμε να επιτρέψουμε την κυκλοφορία στον κεντρικό υπολογιστή HTTP.
Και τέλος θα κάνουμε μερικές ερωτήσεις για την περιμετρική ασφάλεια ενάντια στην εσωτερική ασφάλεια; τα πακέτα που απορρίπτονται από το proxy με/ή χωρίς ACLs, στον εσωτερικό δρομολογητή δικτύων, και θα μελετηθεί πώς το proxy διαχειρίζεται τις συνδέσεις στο εσωτερικό δίκτυο, με την μελέτη του ping trace.

7.4 Δημιουργία του Σεναρίου

1. Ανοίξτε ένα καινούργιο Project στο OPNET IT Guru Academic Edition (**File→ New Project**) με τις παρακάτω τιμές (αφήστε τις υπόλοιπες τιμές σε default κατάσταση).

- **Project Name: <your_name>_Screened.**
- **Scenario Name: ScreenedHost**
- **Network Scale: Office**

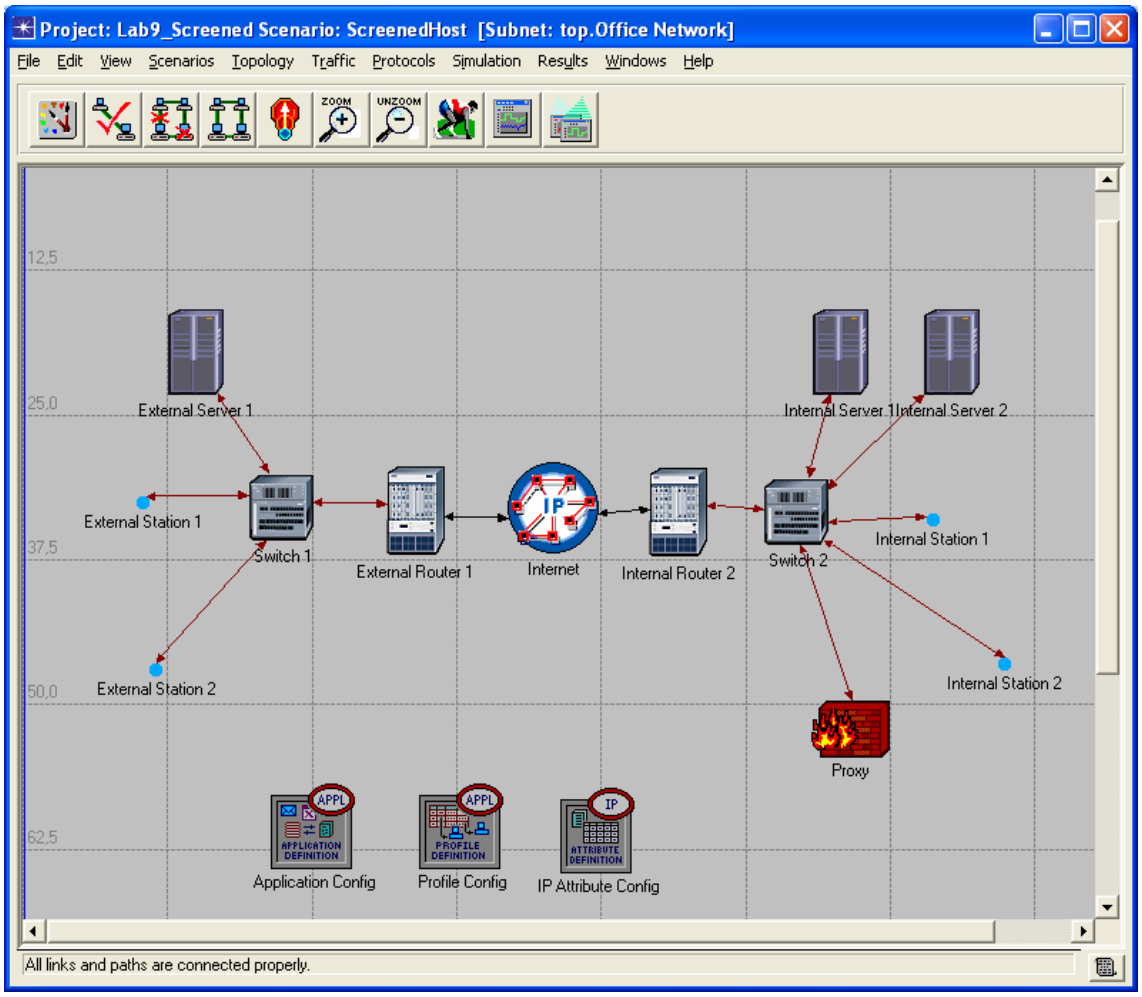
Ζουμ +  στο πλέγμα έτσι ώστε να μπορέσουμε να μεγιστοποιήσουμε το σενάριο αργότερα αν χρειαστούμε λίγο περισσότερο χώρο

2. Αναπτύξτε τα ακόλουθα συστατικά στο σενάριο:

Qty	Component	Palette	Description
1	ip_32_cloud	internet_toolbox	
1	Application Config	internet_toolbox	
1	Profile Config	internet_toolbox	
1	IP Attribute Config	internet_toolbox	
2	ethernet4_slip8_gtwy	internet_toolbox	
1	ethernet2_slip8_firewall	internet_toolbox	
2	ethernet16_switch	internet_toolbox	
4	Sm_Int_wkstn	Sm_Int_Model_Link	
3	Sm_Int_Server	Sm_Int_Model_Link	
	PPP_DS1	internet_toolbox	Links to Internet
	100BaseT	internet_toolbox	Remaining links

Εικόνα 7-3 Components of our network

3. Τοποθετήστε τα συστατικά στο σενάριο, όπως φαίνεται στην εικόνα 8.4. Μετονομάζουμε τους κόμβους όπως βλέπουμε στην εικόνα, επειδή θα αναφερόμαστε σε αυτούς με το όνομα τους από εδώ και στο εξής. Ο εσωτερικός σταθμός #1 μπορεί να αλλάξει το εικονίδιο του προαιρετικά, θα είναι hacker στο εσωτερικό δίκτυο. Ο εξωτερικός σταθμός #2 θα είναι hacker στο εξωτερικό δίκτυο επίσης.



Εικόνα 7-4 The completed scenario

4. Αναθέτουμε τις IP διευθύνσεις σε όλους τους σταθμούς, στα interfaces και στα subinterfaces:

Επεξεργαζόμαστε τις ιδιότητες για όλους τους σταθμούς, και τους κεντρικούς υπολογιστές, μπορούμε επίσης να αλλάξουμε τις IP διευθύνσεις και τη μάσκα διευθύνσεων, από εδώ: **IP Host Parameters→ Address** και **Subnet Mask**. Για τους δρομολογητές, **IP Routing Parameters→ Interface Information→ row i**, αυτό θα μας δώσει πρόσβαση στις ίδιες παραμέτρους για το interface IF i.

Θα δημιουργήσουμε 5 δίκτυα:

Interface	Address / Subnet Mask
Internal Network	213.180.1.0/24
External Network	194.179.95.0/24
Internet (to External Network)	190.50.50.0/24
Internet (to Internal Network)	190.40.40.0/24
Internal Router –Switch2-Proxy	190.30.30.0/24

Εικόνα 7-5 Networks in the scenario

Ορίζουμε τις διευθύνσεις όπως φαίνεται στην εικόνα 8.6. Χρησιμοποιούμε πάντα τη μάσκα υποδικτύου 255.255.255.0

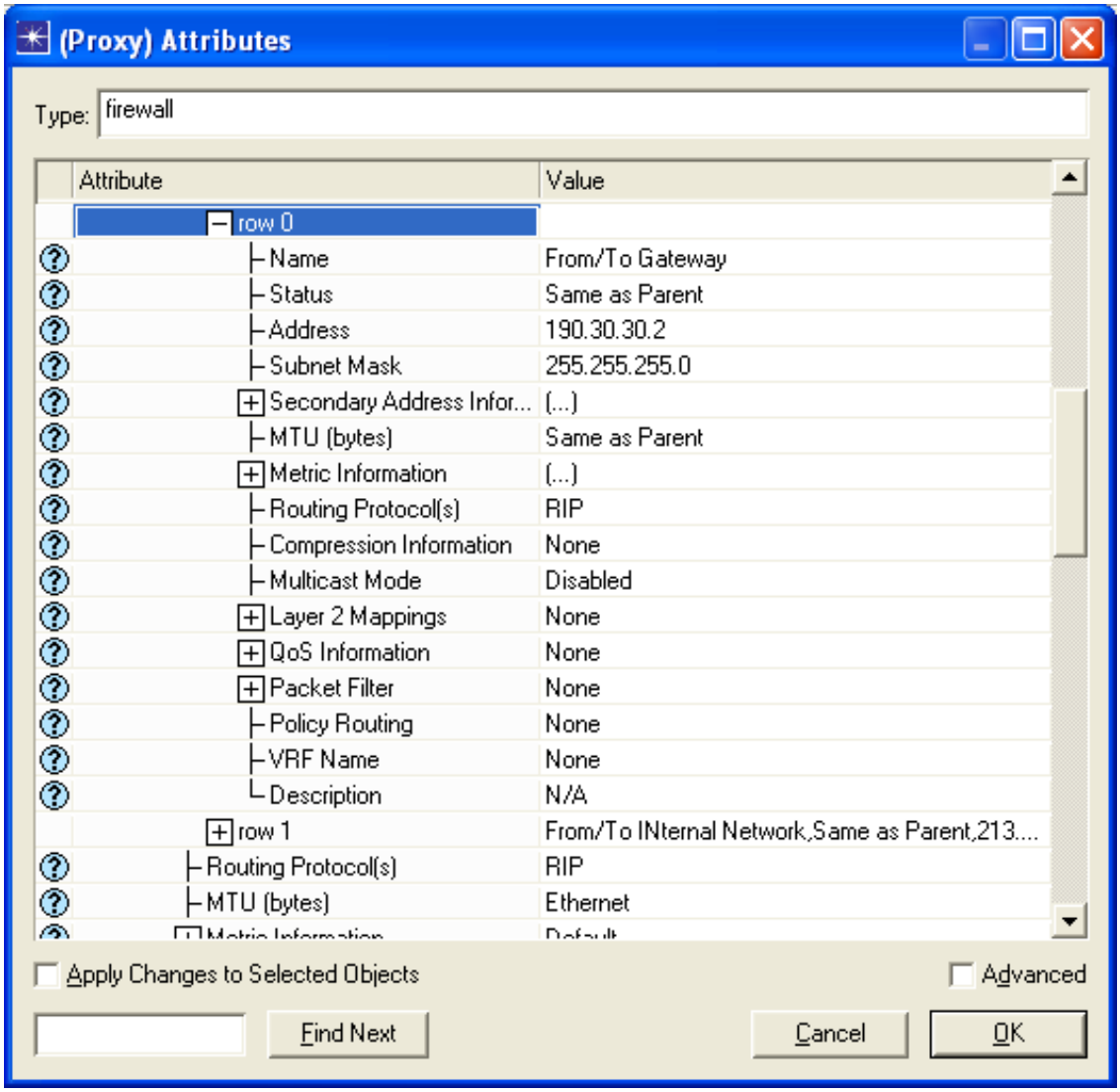
Interface	Address / Subnet Mask
External Station #1	194.179.95.4/24
External Station #2	194.179.95.3/24
External Server #1	194.179.95.2/24
External Router – interface to Switch 1 (IF0)	194.179.95.1/24
External Router – interface to Internet (IF10)	190.50.50.1/24
Internet – interface to External Router (IF0)	190.50.50.2/24
Internet – interface to Internal Router (IF10)	190.40.40.1/24
Internet Router – interface to internet (IF1)	190.40.40.2/24
Internet Router – interface to Switch 2 (IF0)	190.30.30.1/24
Internal Station #1	213.180.1.2/24
Internal Station #2	213.180.1.3/24
Internal Server #1	213.180.1.4/24
Internal Server #2	213.180.1.5/24
Proxy (IF0) – subinterface to internal Network (IF0.1)	213.180.1.6/24
Proxy (IF0) – subinterface to internal Router (IF0.2)	190.30.30.2/24

Εικόνα 7-6 Addresses for the network

Οι τιμές των ονομάτων interfaces εξαρτώνται από την σειρά με την οποία τα κατασκευάζει η συσκευή. Το proxy έχει δύο subinterfaces στο interface που συνδέεται με το διακομιστή (Switch) 2 (IF0). Μπορούμε να τον αλλάξουμε στις ιδιότητες του Proxy: **Interface Information→ row i** (i για το interface του switch 2, 0 για τη δικιά μας περίπτωση)→ **Subinterface Information→ rows: 2**. Αναπτύξτε και τους δύο κλάδους του subinterface και ρυθμίστε τις ακόλουθες παραμέτρους και στις δύο περιπτώσεις:

- **Name: From/To Gateway, Address: 190.30.30.2, Subnet Mask: 255.255.255.0. Layer 2 Mapping→ VLAN Identifier: 2** (έτσι έχουμε το ίδιο interface που ανήκει σε δύο δίκτυα ταυτόχρονα)
- **Name: From/To Internal Network, Address: 213.180.1.6, Subnet Mask: 255.255.255.0. Layer 2 Mapping→ VLAN Identifier: 3**

Δεν χρειάζεται να δώσουμε μια IP διεύθυνση ή μια μάσκα υποδικτύου στο ίδιο το interface, μπορούμε να ρυθμίσουμε το εξής: **Address: No IP Address** και **Subnet Mask: Auto Assigned**



Εικόνα 7-7 Configuring the Proxy subinterfaces

5. Αναθέτουμε μια προκαθορισμένη πύλη στους σταθμούς και στους κεντρικούς υπολογιστές:

Αναθέτουμε ως προκαθορισμένη πύλη όλων των σταθμών και των κεντρικών υπολογιστών του δικτύου την εξής: 213.180.1.0/24 που δείχνει το interface από/ και προς το εσωτερικό δίκτυο (213.180.1.6). Αυτή η παράμετρος ρυθμίζετε από εδώ: **IP Host**

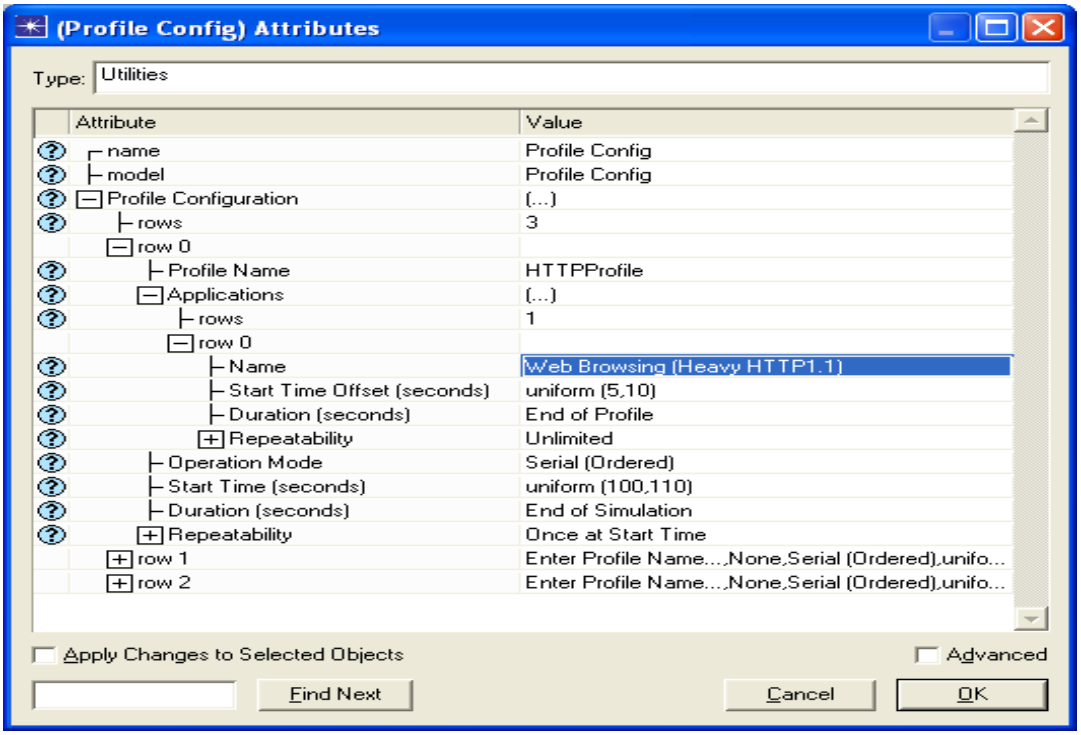
Parameters→ Interface Information→ Default Route. Πρέπει να επιλέξουμε **Internal Station #1, Internal Station #2, Internal Server #1, Internal Server #2** και να αλλάξουμε αυτήν την **ιδιότητα**. Ελέγχουμε το: **Apply Changes To Selected Objects** για να εφαρμόσετε τις αλλαγές ταυτόχρονα σε όλους τους κόμβους.

6. Διαμόρφωση του Application Config Control:
Edit Attributes και ρυθμίζουμε το εξής: **Application Definitions: Default.**

7. Διαμόρφωση του Profile Config Control:
Edit Attributes και δημιουργούμε 3 προφίλ. Χρησιμοποιήστε τις προκαθορισμένες τιμές για τα υπόλοιπα.

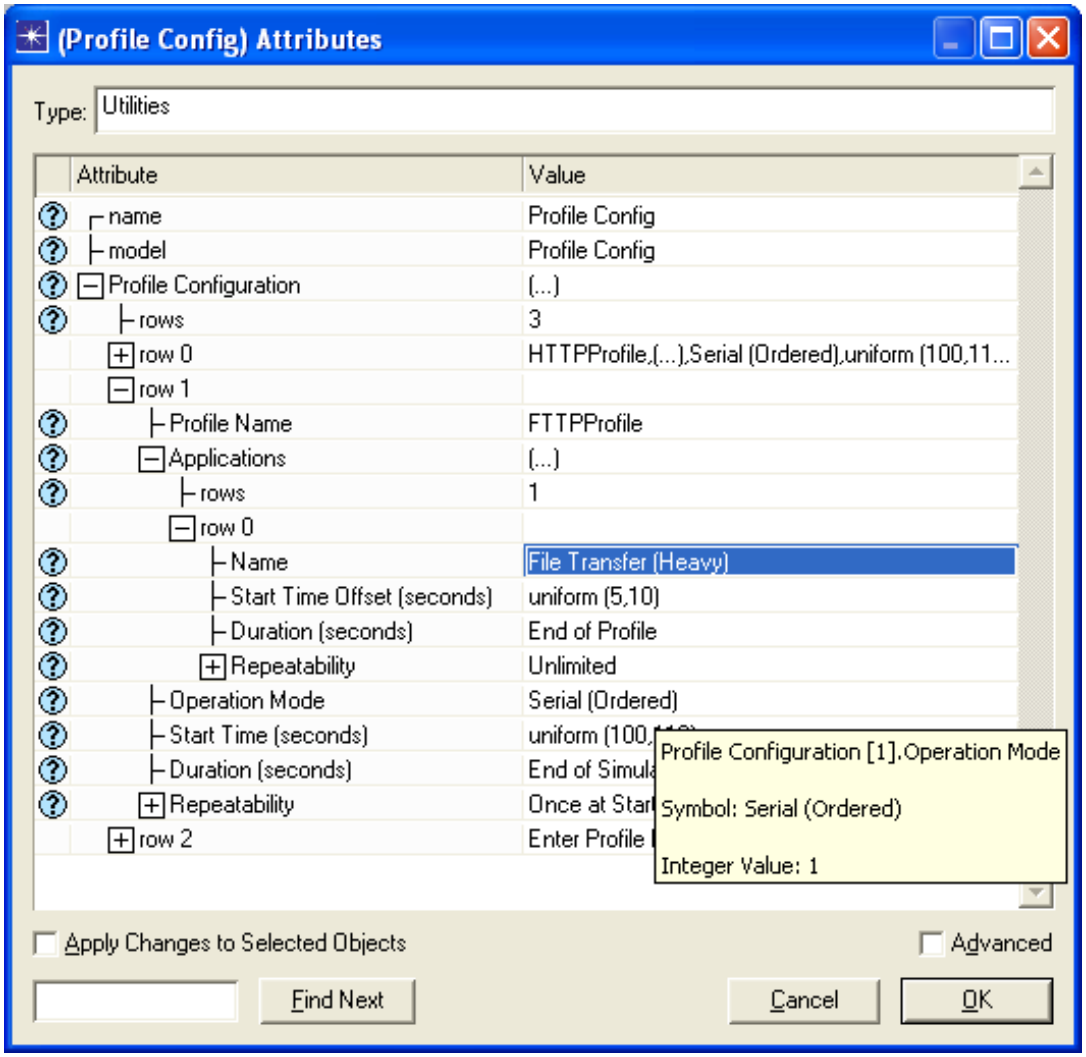
Τα προφίλ είναι:

- **HTTPProfile**, συμπεριλαμβανομένης της εφαρμογής **Web Browsing (Heavy HTTP 1.1)**



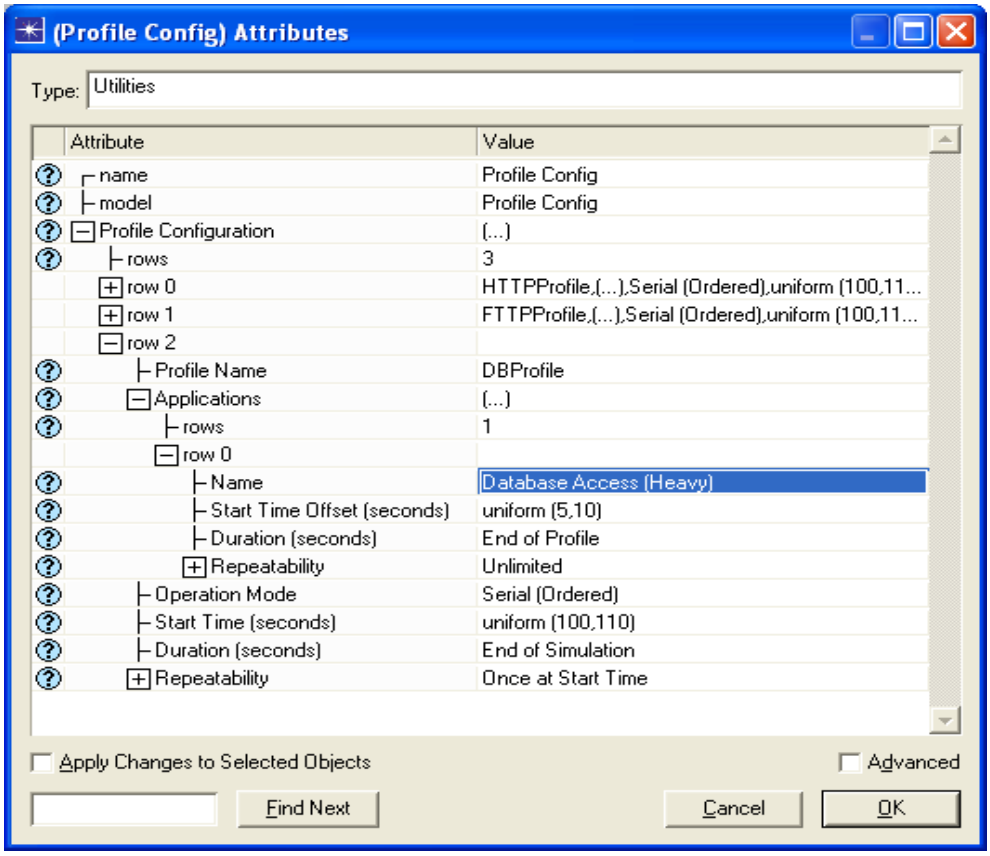
Εικόνα 7-8 HTTP Profile

- **FTPProfile**, συμπεριλαμβανομένης της εφαρμογής **File Tranfer (Heavy)**



Εικόνα 7-9 FTTP Profile

- **DBProfile**, συμπεριλαμβανομένης της εφαρμογής **Database Access (Heavy)**



Εικόνα 7-10 HTTP Profile

8. Κατανομή των εφαρμογών και των υπηρεσιών:
Κατανέμουμε τις υπηρεσίες που υποστηρίζονται από τους κεντρικούς υπολογιστές όπως φαίνεται στον πίνακα παρακάτω:

Server	Services
External Server #1	File Transfer (Heavy), Web Browsing (Heavy HTTP 1.1), Database Access (Heavy)
Internal Server #1	Database Access (Heavy), File Transfer (Heavy)
Internal Server #2	Web Browsing (Heavy HTTP 1.1)

Εικόνα 7-11 Services supported by servers

Πρέπει να αλλάξουμε το **Attribute Application: Supported Services** σε όλους τους κεντρικούς υπολογιστές.

9. Αναθέτουμε τα profile στους σταθμούς εργασίας:
Αναθέτουμε στους τερματικούς σταθμούς τα profile που μπορούν να υποστηρίξουν όπως φαίνεται στον παρακάτω πίνακα:

Station	Profiles
External Station # 1	HTTPProfile
External Station # 2	DBProfile, FTPProfile
Internal station # 1	FTPProfile, DBProfile
Internal station # 2	HTTPProfile, FTPProfile

Εικόνα 7-12 Station's profiles

Πρέπει να αλλάξουμε το **Attribute Application: Supported Services** σε όλους τους κεντρικούς υπολογιστές.

10. Αναθέτουμε τις διευθύνσεις, σε όλους τους κεντρικούς υπολογιστές:

Server	Server Address
External Server # 1	SExt1HTTPFTPDB
Internal Server # 1	SInt1FTPDB
Internal Server # 2	SInt2HTTP

Εικόνα 7-13 Server Address of the servers

11. Αναθέτουμε τις απαιτήσεις στις εφαρμογές:
Πρέπει να αλλάξουμε το Attribute Application: Destination Preferences

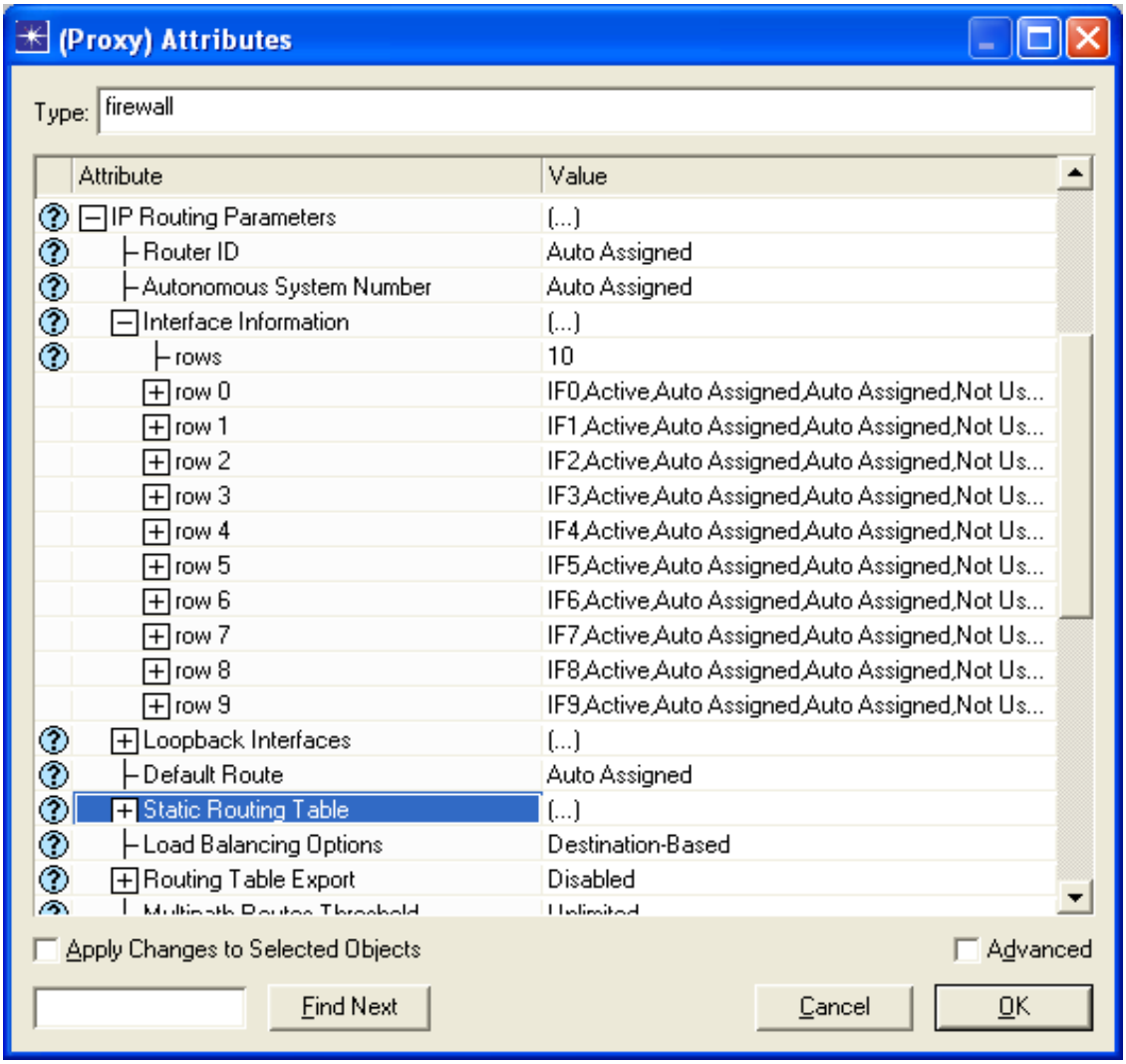
Station	Symbolic Name	Actual Name
External Station # 1	HTTP Server	SInt2HTTP
External Station # 2	Database Server	SInt1FTPDB
	FTP Server	SInt1FTPDB
Internal Station # 1	Database Server	SInt1FTPDB
	FTP Server	SInt1FTPDB
Internal Station # 2	HTTP Server	SExt1HTTPFTPDB
	FTP Server	SExt1HTTPFTPDB

Εικόνα 7-14 Application Demands

12. Επεξεργασία του στατικού πίνακα δρομολόγησης και φιλτράρισμα των κανόνων του proxy:
Θα κάνουμε επίσης:

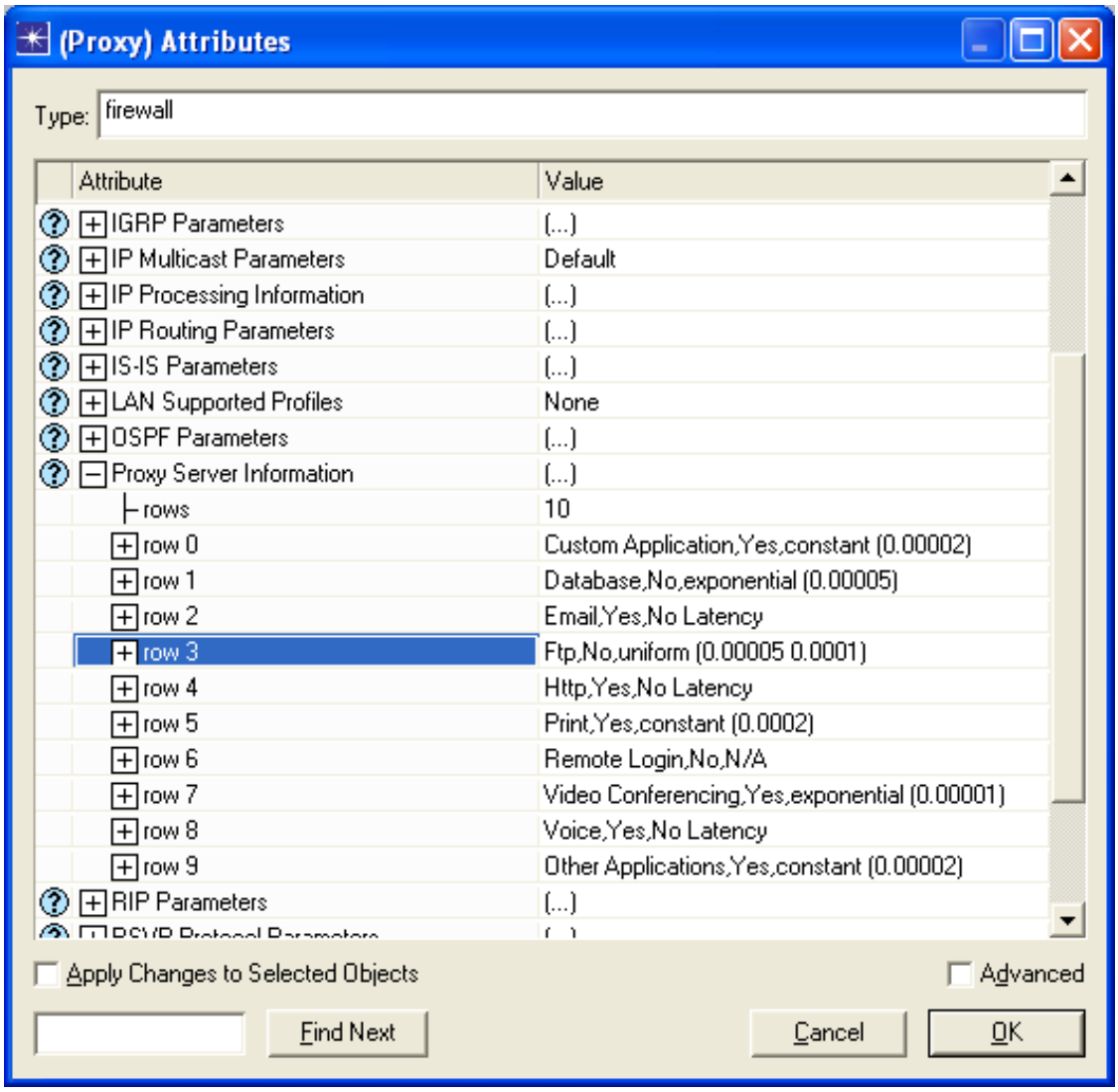
- Λάβετε τα IP πακέτα του εσωτερικού δικτύου που στέλνονται στο διαδίκτυο, και ξαναστείλε τα στην πύλη (εσωτερικός δρομολογητής) για να σταλούν στο διαδίκτυο.
- Λάβετε τα IP πακέτα που ο εσωτερικός δρομολογητής στέλνει από το διαδίκτυο και τα οποία στάλθηκαν στο εσωτερικό δίκτυο και ξαναστείλε τα στον τελικό σταθμό του εσωτερικού δικτύου.
- Και στις δύο περιπτώσεις, εκτελέστε ένα φιλτράρισμα proxy (στρώματος 5).

Τα δύο πρώτα σημεία θα επιτευχθούν με επεξεργασία του στατικού πίνακα δρομολόγησης, προσιτό μέσω του **IP Routing Parameters→ Static Routing Table**. Στον ακόλουθο πίνακα μπορούμε να δούμε τον πίνακα δρομολόγησης που διαμορφώνεται.



Εικόνα 7-15 Static Routing Table of the Proxy

Θα διαμορφώσουμε το proxy προκειμένου να μην επιτρέψουμε την κυκλοφορία από το FTP και την υπηρεσία βάσεων δεδομένων από τον εσωτερικό υπολογιστή. Πρέπει να τροποποιήσουμε την ιεραρχία του Proxy Server Information για να πάρουμε το εξής: **Proxy Server Deployed: No** στην βάση δεδομένων, και να επιτρέπει τα υπόλοιπα.



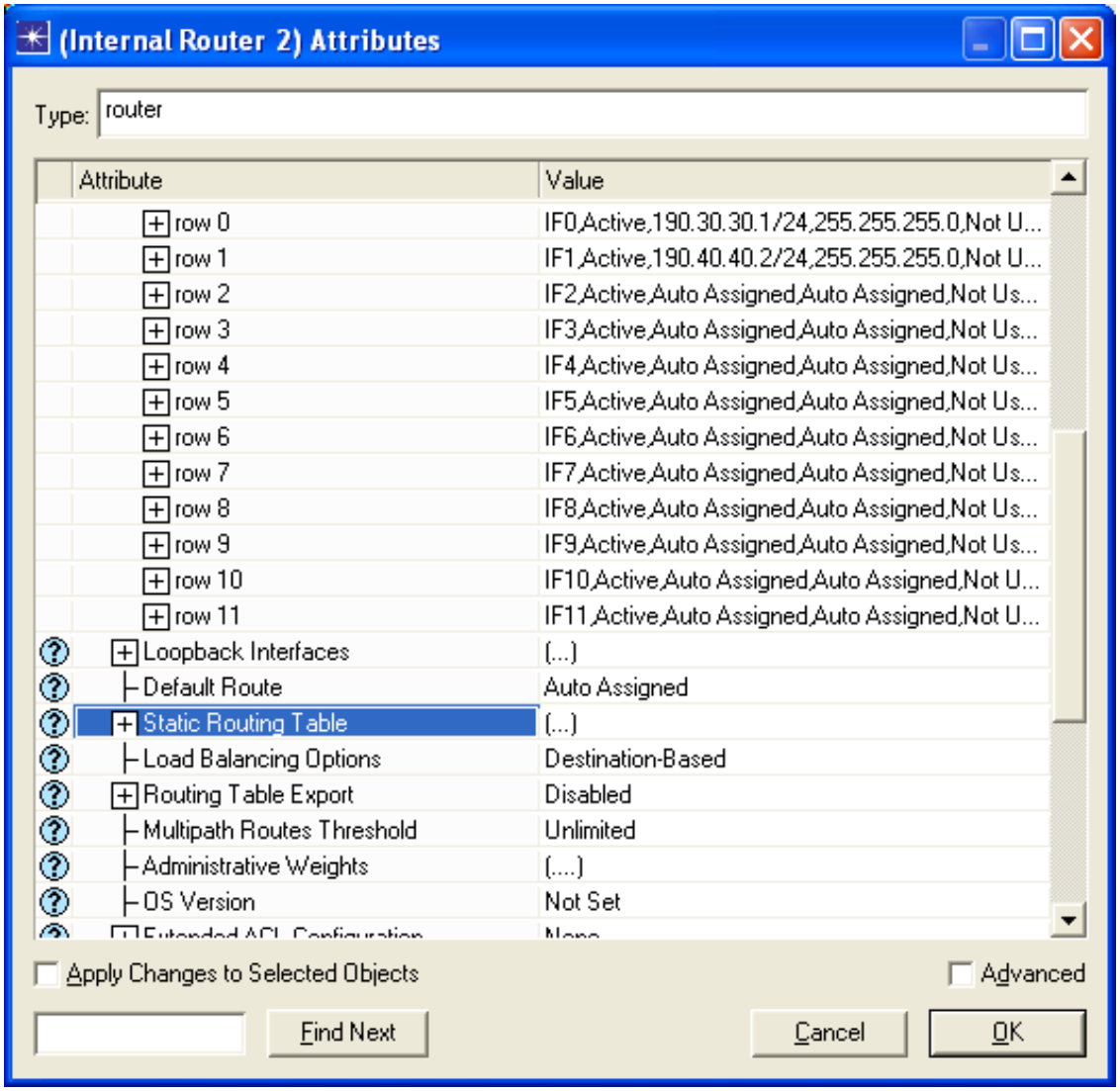
Εικόνα 7-16 Configuring the Proxy

13. Επεξεργασία του εσωτερικού πίνακα δρομολόγησης του εσωτερικού δρομολογητή: Θα κάνουμε επίσης:

- Λάβετε τα IP πακέτα από το Proxy (που προέρχονται από το εσωτερικό δίκτυο) και ξαναστείλε τα στο διαδίκτυο.
- Λάβετε τα πακέτα από το διαδίκτυο που έχουν προορισμό το εσωτερικό δίκτυο, και ξαναστείλε τα στο Proxy.

- Και στις δύο περιπτώσεις, εκτελέστε ένα φιλτράρισμα πακέτων στρώματος-3 με ACLs.
- Πακέτα που έχουν απορριφθεί, παραλαμβάνονται άμεσα από το εσωτερικό δίκτυο (είναι υποχρεωτικό να περάσουν και από τους 2 δρομολογητές για την εισερχόμενη και εξερχόμενη επικοινωνία).Αυτό μπορεί να γίνει με VLANs.

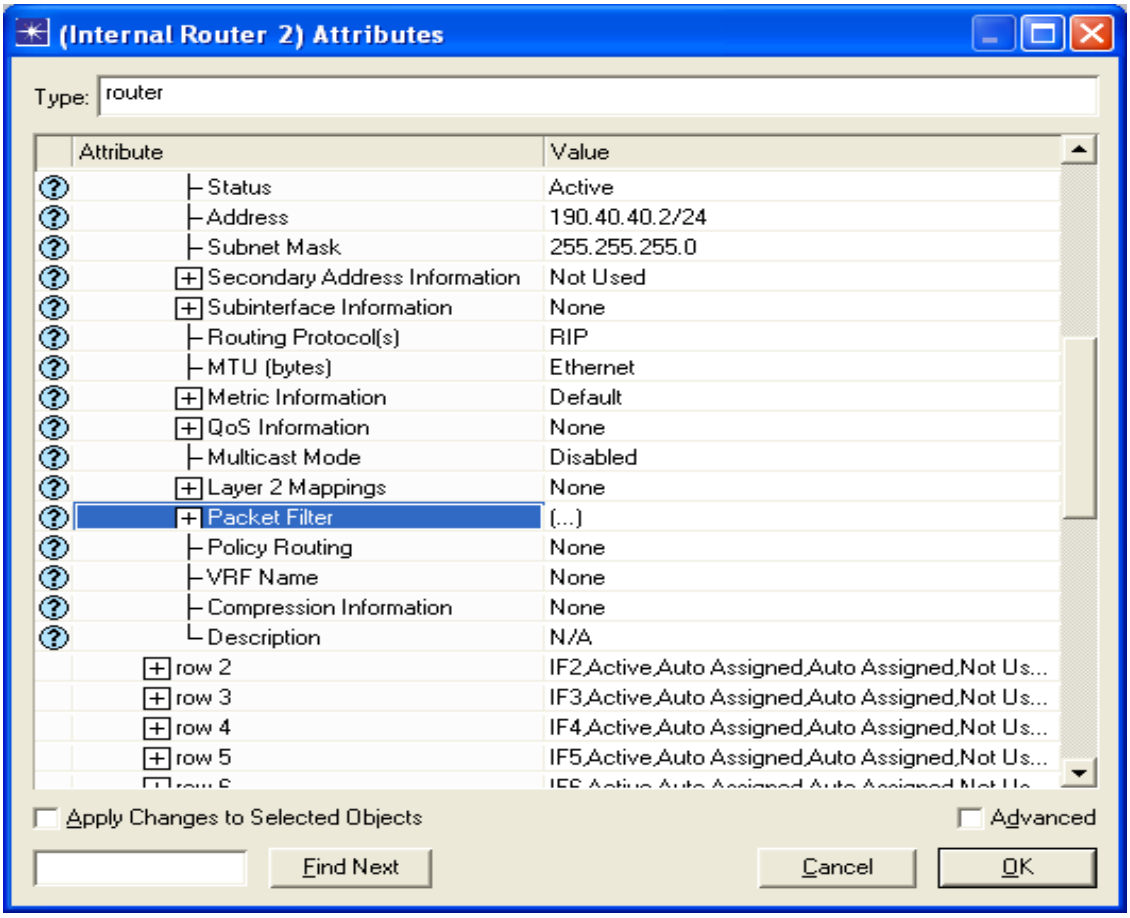
Στην εικόνα 8.17 μπορούμε να δούμε την διαμόρφωση του στατικού πίνακα δρομολόγησης, και στην εικόνα 8.18 την διαμόρφωση ACL.



Εικόνα 7-17 Static Routing Table at Internal Router

Πρέπει να αναθέσουμε τους πίνακες ACL στα interfaces: **IP Routing Parameters→ Interface Information→ row 1**(το μοναδικό με το interface στο Internet)**→ Packet**

Filter→ Send Filter: **Outgoing Traffic** και **Receive Filter**: Incoming **Traffic**. Για το εσωτερικό δίκτυο (IF0), αναστρέφουμε την σειρά.



Εικόνα 7-18 Internal Router ACL

14. Ρυθμίζοντας το VLAN στο εσωτερικό δίκτυο:

Για να δουλέψει το proxy με πολλά subinterfaces στο ίδιο interface, πρέπει το κάθε subinterface να ανήκει σε διαφορετικό δίκτυο, και αυτό μπορεί να γίνει με VLANs. Δημιουργούμε δύο απλά VLANs, το πρώτο VLAN με αναγνωριστικό επιβεβαίωσης: 2 (δίκτυο190.30.30.0/24) και το δεύτερο με αναγνωριστικό επιβεβαίωσης: 3 (δίκτυο 213.180.1.0/24).

Αντιστοιχούμε τα αναγνωριστικά επιβεβαίωσης του VLAN όπως φαίνεται στον παρακάτω πίνακα, με τα εσωτερικά interfaces του δικτύου. Θυμηθείτε ότι πρόσβαση σε αυτή την παράμετρο μπορείτε να έχετε ως εξής: **IP Host Parameters→ Interface Information→ Layer 2 Mapping→ VLAN Identifier** για τους σταθμούς; και **IP Routing Parameters→ Interface Information→ row i** (i για το interface)**→ Layer 2 Mapping→ VLAN Identifier** για τους δρομολογητές.

Interface	VLAN Identifier
Internal Router – interface to Switch 2 (If0)	3
Proxy – subinterface From/To gateway	3
Proxy – subinterface From/To Internal Network	2
Internal Station # 1	2
Internal Station # 2	2
Internal Server # 1	2
Internal Server # 2	2

Εικόνα 7-19 VLAN Identifiers

Αναθέτουμε επίσης αυτές τις παραμέτρους στο *Switch 2*, για να διαμορφώσουμε το VLAN. Οι τιμές των Ports είναι αυτές που είχαμε και εξαρτώνται από την σειρά δημιουργίας.

Port	Port Type	Port VLAN Id.	Supported VLANs
Interface to Internal Router (P0)	Access	2	2
Interface to Proxy (P13)	Trunk	1	1,2,3
Interface to Internal Station # 1 (P1)	Access	3	3
Interface to Internal Station # 2 (P10)	Access	3	3
Interface to Internal Server # 1 (P11)	Access	3	3
Interface to Internal Server # 2 (P12)	Access	3	3

Εικόνα 7-20 Configuring VLAN at Switch 2

Αυτές οι πληροφορίες μπορούν να βρεθούν εδώ: **Switch Port Configuration→ row i** (i για το interface)**→ VLAN Parameters.**
Πρέπει να διαμορφώσουμε εκτός από αυτές τις παραμέτρους και τα εξής: **VLAN Parameters→ Supported VLANs** για να υποστηρίξουν VLANs 1,2,3 (**Name: Default, Gateway** και **Internal Network** αντίστοιχα) και **VLAN Parameters→ Scheme: Port-Based VLANs.**

7.5 Ρυθμίστε την προσομοίωση

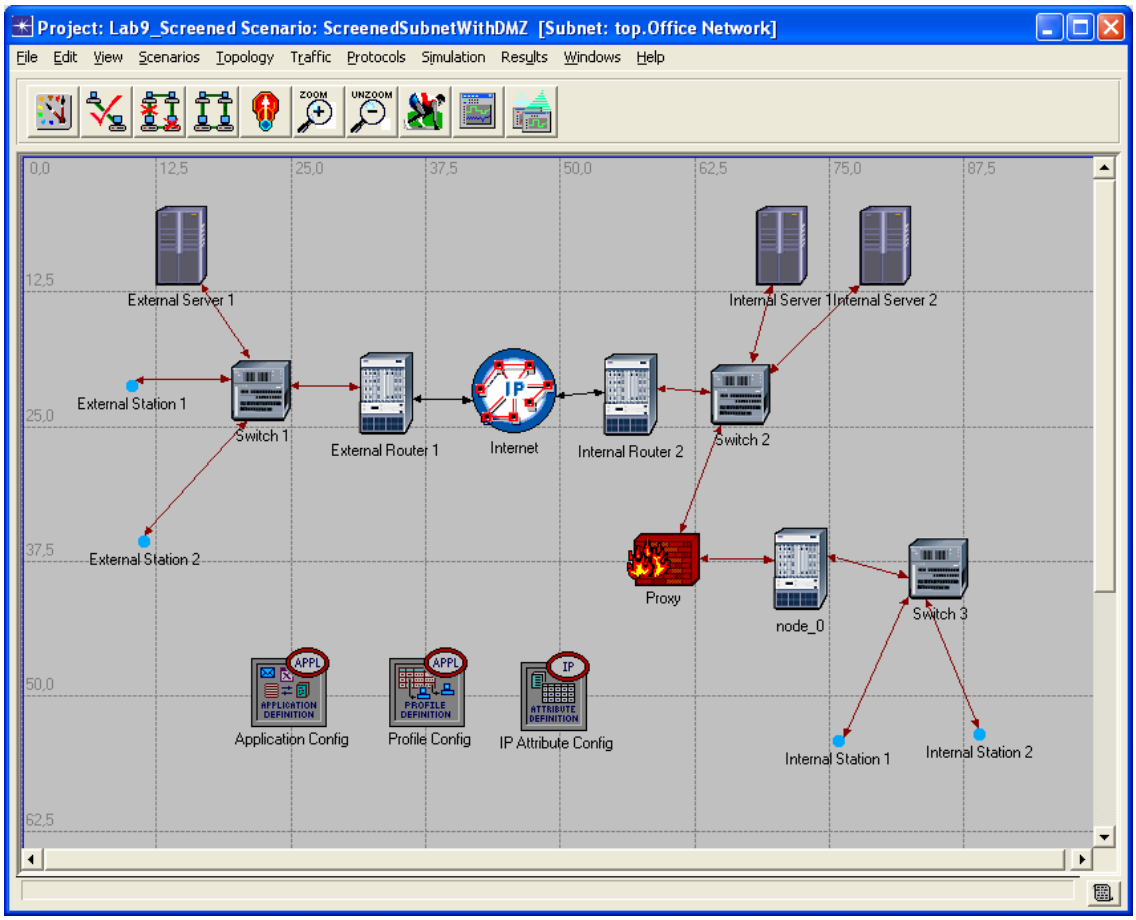
- Επιλέξτε τη στατική **IP Traffic Dropped (packets/sec)** στο **Proxy**. (**δεξί κλικ→ Choose Individual Statistics**).
- Με αυτόν τον τρόπο μπορούμε να δούμε το ποσό της κυκλοφορίας που απορρίπτεται από το Proxy.

Κάνουμε κλικ στο **Configure/Run simulation**  και ρυθμίζουμε την παράμετρο **Duration: 15 minute(s)**. Κάνουμε κλικ στο **OK** (Μην αρχίσετε την προσομοίωση ακόμα).

7.6 Δημιουργία του Δεύτερου Σεναρίου

1. Αναπαράγετε το σενάριο:

Από τον επεξεργαστή προγράμματος, και με το σενάριο ανοιχτό, **Scenarios→ Duplicate Scenario…** Ονομάστε το νέο σενάριο ως εξής: **Scenario Name: ScreenedSubnetWithDMZ.**
Το νέο σενάριο είναι ακριβώς ίδιο όπως αυτό που είχαμε ως τώρα, αλλά αυτή την φορά οι εσωτερικοί σταθμοί θα συνδεθούν στο *Switch 2* μέσω ενός δρομολογητή ethernet_4_slip8_gtwy (στην παλέτα internet_toolbox), ο οποίος θα τους συνδέσει με το proxy. Οι εσωτερικοί χρήστες θα είναι στο switched LAN με ethernet16_switch (στην παλέτα internet_toolbox). Τα νέα καλώδια που θα χρησιμοποιηθούν για την σύνδεση θα είναι 100BaseT (στην παλέτα συνδέσεων). Το σχεδιάγραμμα των κεντρικών υπολογιστών θα είναι ίδιο με αυτό που έχουμε (DMZ).



Εικόνα 7-21 The scenario ScreenedSubnetWithDMZ

2. Αναθέστε τις IP διευθύνσεις ξανά:

Δημιουργήστε το δίκτυο 213.190.1.0/25, ξεχωριστά από το 213.180.1.0 (μόνο οι κεντρικοί υπολογιστές θα είναι εδώ τώρα). Τώρα αυτό το δίκτυο ονομάζεται Demilitarized Zone (DMZ) επειδή είναι απομονωμένο από τις εσωτερικές και εξωτερικές επιθέσεις .Ένα άλλο δίκτυο δημιουργείται: 190.20.20.0.24, μεταξύ του εσωτερικού δρομολογητή #2 και του Proxy.
Οι νέες IP διευθύνσεις είναι:

Interface	IP Address
Internal Station #1	213.190.1.2
Internal Station #2	213.190.1.3
Internal Router #2 – interface to Switch 3 (IF0)	213.190.1.1
Internal Router #2 – interface to Proxy (IF1)	190.20.20.1
Proxy – interface to Internal Router #2 (IF1)	190.20.20.2

Εικόνα 7-22 New IP addresses

Για άλλη μια φορά τα intefaces στις παρενθέσεις είναι αυτά που είχαμε, αλλά μπορεί να είναι και διαφορετικά από τα δικά σας, ανάλογα με την σειρά δημιουργίας των συνδέσεων στο πλέγμα.

3. Αναθέστε ένα ACL στον εσωτερικό δρομολογητή #2:

Η πολιτική ασφαλείας του δικτύου μας παραμένει η ίδια: πρέπει να αποφύγουμε την πρόσβαση στον εσωτερικό κεντρικό υπολογιστή #1 (κεντρικός υπολογιστής FTP και DB). Θα δημιουργήσουμε ένα ACL στον κεντρικό υπολογιστή #1, χρησιμοποιώντας τις πληροφορίες της εικόνας 8.22, όπου:

- Ο κατάλογος IncomingTrafficAtDmz απορρίπτει όλη την κυκλοφορία που στέλνεται στον εσωτερικό κεντρικό υπολογιστή #1 (213.180.1.4) και επιτρέπει όλη την υπόλοιπη κυκλοφορία.
- Ο κατάλογος OutgomingTrafficFromDmz απορρίπτει την εξερχόμενη κυκλοφορία από τον εσωτερικό κεντρικό υπολογιστή #1, αλλά επιτρέπει την υπόλοιπη εξερχόμενη κυκλοφορία.

List Name	Action	Source	Destination
IncomingTrafficToDMZ	Deny	*	213.180.1.4/host
	Permit	*	213.180.1.0/24
	Permit	*	*
OutgoingTrafficFromDMZ	Deny	213.180.1.4/host	*
	Permit	*	*

Εικόνα 7-23 ACL of Internal Router # 2

4. Αναθέστε τα ACLs στα interfaces του εσωτερικού δρομολογητή # 2.

   - Interface to Proxy (IF1).**Send Filter: IncomingTrafficToDMZ, Receive Filter: OutgoingTrafficFromDMZ**

   - Inteface to Switch 3 (IF0). **Send Filter: OutgoingTrafficFromDMZ, Receive Filter: IngoingTrafficToDMZ**

5. Δημιουργία του πίνακα δρομολόγησης του εσωτερικού δρομολογητή # 2, και τροποποίηση των πινάκων δρομολόγησης του εσωτερικού δρομολογητή #1 και του Proxy.
   - Για τον εσωτερικό δρομολογητή # 2, **Destination: 190.20.20.0/24 Next Hop: 190.20.20.1; Destination: 213.190.1.0/24 Next Hop: 213.190.1.1** και **Default: 190.20.20.2**
   - Για το Proxy, προσθέτουμε ένα νέο entry: **Destination: 213.190.1.0/24 Next Hop: 190.20.20.1**
   - Για τον εσωτερικό δρομολογητή # 1, προσθέτουμε ένα νέο entry: **Destination: 213.190.1.0/24 Next Hop: 190.30.30.2**
   - Εκχώρηση της default διαδρομής του εσωτερικού σταθμού # 1, και του εσωτερικού σταθμού # 2 στο σημείο 213.190.1.1

6. Αναπρογραμματισμός του ACL του εσωτερικού δρομολογητή:

Πρέπει να τροποποιήσουμε ελαφρώς το ACL της εισερχόμενης και εξερχόμενης κυκλοφορίας για να επιτρέψουμε το πέρασμα της κυκλοφορίας από/προς τα νέα δίκτυα που μόλις δημιουργήσαμε, 213.190.1.0/24 (στο νέο εσωτερικό δίκτυο) και 190.20.20.0/24 (ο δρομολογητής μεταξύ του εσωτερικού δρομολογητή # 2 και του proxy). Στην εικόνα 8.24 μπορούμε να δούμε τα νέα ACLs που πρέπει να προγραμματίσουμε στον εσωτερικό δρομολογητή (οι υπόλοιπες παράμετροι αφήνονται σε default κατάσταση).

List Name	Action	Source	Destination
Incoming Traffic	Deny	*	213.180.1.4/host
	Permit	*	213.180.1.0/24
	Permit	*	213.190.1.0/24
	Permit	*	190.20.20.0/24
Outgoing Traffic	Permit	213.190.1.0/24	*
	Permit	190.20.20.0/24	*
	Permit	213.180.1.0/24	*
	Permit	190.30.30..0/24	*

Εικόνα 7-24 Adding up new conditions to the ACL

7. Εκτέλεση της προσομοίωσης:

Από τον επεξεργαστή κειμένου, **Scenarios→ Manage Scenarios.** Ελέγχουμε όλα τα σενάρια με **<collected>** στο **Results** πεδίο και πατάμε **OK.**

7.7 Ερωτήσεις

7.7.1 Ερώτηση 1η

Στο σενάριο ScreenedHost, δημιουργούμε ένα νέο ping από τον εξωτερικό σταθμό # 1 στον εσωτερικό κεντρικό υπολογιστή # 2 με Ping Pattern: Record Route. Παρατηρήστε το Ping trace στο Simulation Log. Τι παρατηρείτε;

7.7.2 Ερώτηση 2η

Αναπαράγετε το σενάριο ScreenedHost και ονομάστε το νέο σενάριο ScreenedHostQ2. Δημιουργήστε ένα νέο ping trace από τον εξωτερικό σταθμό # 1 στον εσωτερικό σταθμό # 1 (Record Route).
Στο νέο σενάριο, αλλάξτε την default διαδρομή του εσωτερικού σταθμού # 1στο σημείο190.30.30.1 (εσωτερικός δρομολογητής – interface to Switch 2). Τρέξτε την προσομοίωση και αναλύστε το frame των pings στο Q1. Είναι πιθανό να αποφύγει το Firewall με αυτόν τον τρόπο;

7.7.3 Ερώτηση 3η

Αναπαράγετε το σενάριο ScreenedHost και ονομάστε το νέο σενάριο ScreenedHostQ3. Θέστε εκτός λειτουργίας το ACLs που έχουμε προγραμματίσει στον εσωτερικό δρομολογητή (ο γρηγορότερος τρόπος είναι να θέσουμε rows: 0 στο πεδίο IP Routing Parameters→ Extended ACL Configuration). Τρέξτε την προσομοίωση και συγκρίνετε τα στατιστικά IP→ Traffic Dropped (packets/sec) στο Proxy στα σενάρια ScreenedHost και ScreenedHostQ3. Τι συμπεράσματα βγάζετε;

7.7.4 Ερώτηση 4η

Συμπληρώστε τον ακόλουθο πίνακα, παίρνοντας τις πληροφορίες από το Simulation Log των traffic demands στον εσωτερικό κεντρικό υπολογιστή # 1 (κυκλοφορία από το DB ή από το FTTP). Σημειώστε αν ο προορισμός επιτεύχθηκε ή όχι.

Scenario	Internal Station # 1	External Station # 2
ScreenedHost		
ScreenedSubnetAmdDMZ		

Τι μπορούμε να πούμε για την ασφάλεια και στις δύο περιπτώσεις; (θυμηθείτε ότι οποιοσδήποτε από τους δύο σταθμούς έχει το δικαίωμα να χρησιμοποιήσει τις υπηρεσίες του FTP και της βάσης δεδομένων στον εσωτερικό κεντρικό υπολογιστή # 1, και ο εσωτερικός σταθμός # 1 και ο εξωτερικός σταθμός # 2 είναι hacker).

7.8 Απαντήσεις

7.8.1 Απάντηση 1η

Το ενδιαφέρον σημείο είναι να παρατηρήσουμε ότι όλη η κυκλοφορία μεταξύ του εσωτερικού και εξωτερικού δικτύου πηγαίνει απαραίτητα προς το δρομολογητή και το Firewall

IP Address	Hop Delay	Node Name
194.179.95.4	0,00000	Office Network.External Station # 1
190.50.50.1	0,00005	Office Network.External Router
192.0.0.1	0,00070	Office Network.Internet
190.30.30.1	0,00068	Office Network.Internal Router
213.180.1.6	0,00005	Office Network.Proxy
213.180.1.5	0,00005	Office Network.Internal Server # 2
213.180.1.5	0,00001	Office Network.Internal Server # 2
190.30.30.2	0,00004	Office Network.Proxy
192.0.0.2	0,00005	Office Network.Internal Router
190.50.50.2	0,00070	Office Network.Internet
194.179.95.1	0,00068	Office Network.External Router
194.179.95.4	0,00005	Office Network.External Station # 1

Εικόνα 7-25 Ping

7.8.2 Απάντηση 2η

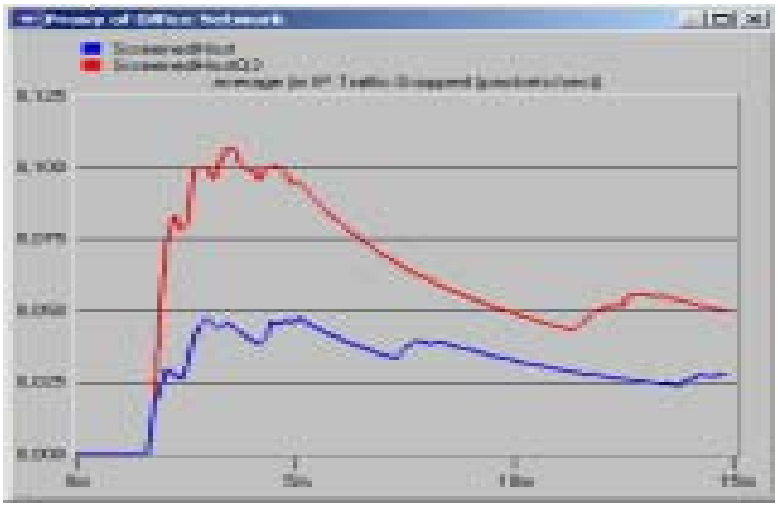
Είναι αδύνατο για έναν εσωτερικό σταθμό να αποφύγει το «bastion host changing the default gateway»

IP Address	Hop Delay	Node Name
194.179.95.4	0,00000	Office Network.Estasio
190.50.50.1	0,00006	Office Network.
192.0.0.1	0,00137	Office Network.
190.30.30.1	0,00068	Office Network.
213.180.1.6	0,00005	Office Network.
213.180.1.2	0,00005	Office Network.
213.180.1.2	0,00001	Office Network.
190.30.30.2	0,00004	Office Network.Proxy
192.0.0.2	0,00005	Office Network.Router Intern
190.50.50.2	0,00070	Office Network.Internet
194.179.95.1	0,00068	Office Network.Router Extern
194.179.95.4	0,00005	Office Network.

Εικόνα 7-26 It is not possible to avoid the Proxy

7.8.3 Απάντηση 3η

Παρατηρούμε ότι το φορτίο κυκλοφορίας που απορρίπτεται από το Proxy αυξάνεται εάν τα ACLs του δρομολογητή είναι εκτός λειτουργίας επειδή αυτή η κυκλοφορία απορριπτόταν από το δρομολογητή, π.χ., οι συνδέσεις στον εσωτερικό κεντρικό υπολογιστή # 1.



Εικόνα 7-27 The ACL helps to reduce the load on the Proxy

7.8.4 Απάντηση 4η

Το ενδιαφέρον πράγμα είναι να συγκριθεί η περιμετρική ασφάλεια που προσφέρεται από το Screened Host με την περιμετρική ασφάλεια και την εσωτερική ασφάλεια επίσης η οποία προσφέρεται από το DMZ.

Scenario	Internal Station # 1	External Station # 2
ScreenedHost	Yes	No
ScreenedSubnetAmdDMZ	No	No

Εικόνα 7-28 Internal attacks can be avoided only with DMZ

Chapter 8 Βιβλιογραφία/Αναφορές

8.1 Παράθεση χρήσιμων πληροφοριών

Σε αυτό το σημείο θα ήθελα να αναφέρω ότι για την πραγματοποίηση της συγκεκριμένης πτυχιακής εργασίας, έλαβα βοήθεια από μια ήδη ολοκληρωμένη πτυχιακή εργασία του Τμήματος μας από τους εξής συμφοιτητές μου: Γιατράκης Λυσίμαχος – Στέφανος, Πεπονάκης Γεώργιος.
Η πτυχιακή τους εργασία «Χρήση του Λογισμικού OPNET στην προσομοίωση δικτύων δεδομένων», ήταν η αφετηρία για να ξεκινήσω την δική μου πτυχιακή εργασία με τίτλο «Προσομοίωση Ασφαλών Δικτυακών Αρχιτεκτονικών με χρήση του OPNET», και μου έδωσε το ερέθισμα καθώς και τις απαραίτητες-αναγκαίες γνώσεις για να ξεπεράσω τις όποιες δυσκολίες αντιμετώπισα στα πρώτα στάδια και να φτάσω τελικά εις πέρας την πτυχιακή μου εργασία.