**Network Design**

**Network planning**

Η επιλογή έγινε υπέρ του ιεραρχικού μοντέλου δικτύου, ένα προσεγμένο πλαίσιο σχεδίασης που εφαρμόζεται στα δίκτυα για την οργάνωση και διαχείριση της υποδομής τους εντός μιας εταιρείας. Αυτό το μοντέλο διαμορφώνει το δίκτυο σε διακριτά επίπεδα, όπως το επίπεδο πρόσβασης, το επίπεδο διανομής και το επίπεδο πυρήνα, τα οποία καθένα εκτελεί συγκεκριμένες λειτουργίες και φέρει συγκεκριμένες ευθύνες. Αυτή η προσέγγιση βοηθά στη βελτιστοποίηση της απόδοσης και της ασφάλειας του δικτύου, καθώς και στην αποτελεσματική διαχείρισή του. Επιπλέον, παρέχει επεκτασιμότητα και ευελιξία, γεγονός που το καθιστά δημοφιλές σε διάφορα επιχειρηματικά περιβάλλοντα.

**Network drawing**

Παρουσιάζεται το σχεδιάγραμμα του δικτύου που υλοποιήθηκε. (Δημιουργήθηκε με το εργαλείο draw.io)

A diagram of a computer network

Description automatically generated

Για την εσωτερική διευθυνσιοδότηση χρησιμοποιήθηκε το δίκτυο κλάσης Β 172.16.0.0 (0.0.255.255), καθώς για την επικοινωνία εκτός εταιρείας χρησιμοποιήθηκε το δίκτυο 77.140.99.90/29 (255.255.255.248). Ο κεντρικός CentralRouter αποτελεί τον πυρήνα του δικτύου. Αναλαμβάνει τη δρομολόγηση της κίνησης μεταξύ των διαφορετικών VLANS και επιτρέπει την επικοινωνία μεταξύ τους και προς το εξωτερικό δίκτυο internet. Το κεντρικό CentralSwitch συνδέει όλα τα μηχανήματα του δικτύου σε ένα κεντρικό σημείο. Έχει τον ρόλο VTP SERVER καθώς είναι υπεύθυνο για την δημιουργία και διαχείριση όλων των VLANS. Κάθε VLAN αντιπροσωπεύει μια διαφορετική ομάδα – τμήμα στο δίκτυο. Κάθε VLAN έχει το δικό του Switch, που συνδέεται με τον κεντρικό CentralSwitch. Ο κεντρικός CentralRouter μπορεί να ρυθμίσει την επικοινωνία μεταξύ των διαφορετικών VLANS.

**Floor plans**

Χρησιμοποιήθηκαν τα έτοιμα σχέδια τα οποία μας χορηγήθηκαν όπως παρουσιάζονται παρακάτω:

1. **Εταιρικό Κτήριο**

A blueprint of a computer

Description automatically generated

1. **Κτήριο Γραφείων**

A blueprint of a building

Description automatically generated

**IP Addressing Scheme**

Για το υπολογισμό των διευθύνσεων χρησιμοποιήθηκε η μέθοδος που ακολουθεί, σύμφωνα με τις οδηγίες τις εργασίας:

Τμ. Διοικητικής Υποστήριξης & Υποδοχής: 8

Hosts = 8 + 10% = 9, άρα 172.16.10.1/28, Συνολικοί χρήστες: 14

Τμ. Διαχείρισης Εφοδιαστικής Αλυσίδας: 20

Hosts = 20 + 10% =22, άρα 172.16.20.1/27, Συνολικοί χρήστες: 30

Τμ. Υγείας & Ασφάλειας: 12

Hosts = 12 + 10% =13, άρα 172.16.30.1/28, Συνολικοί χρήστες: 14

Τμ. Έρευνας & Ανάπτυξης: 18

Hosts = 18 + 10% =20, άρα 172.16.40.1/27, Συνολικοί χρήστες: 30

Τμ. Υποστήριξης Πληροφορικής & Δικτύων: 16

Hosts = 16 + 10% =18, άρα 172.16.50.1/27, Συνολικοί χρήστες: 30

Τμ. Οικονομικών: 12

Hosts = 12 + 10% =13, άρα 172.16.60.1/28, Συνολικοί χρήστες: 14

Τμ. Ανθρωπίνου Δυναμικού: 14

Hosts = 14 + 10% =15, άρα 172.16.70.1/27, Συνολικοί χρήστες: 30

Τμ. Εξυπηρέτησης Πελατών: 80

Hosts = 80 + 10% =88, άρα 172.16.80.1/25, Συνολικοί χρήστες: 126

Τμ. Πωλήσεων: 60

Hosts = 60 + 10% =66, άρα 172.16.90.1/25, Συνολικοί χρήστες: 126

Υποδίκτυο Servers: 5

Hosts = 5 + 10% =6, άρα 172.16.100.1/29, Συνολικοί χρήστες: 6

Ομάδα Διοίκησης: 10

Hosts = 10 + 10% =11, άρα 172.16.101.1/28, Συνολικοί χρήστες: 14

Υποδίκτυο Printers: 21

Hosts = 21 + 10% =23, άρα 172.16.102.1/27, Συνολικοί χρήστες: 30

Υποδίκτυο FileServers: 10

Hosts = 10 + 10% =11, άρα 172.16.103.1/28, Συνολικοί χρήστες: 14

**Switched Design**

**Πίνακας VLANS**

|  |  |  |  |
| --- | --- | --- | --- |
| ΤΜΗΜΑ | VLAN | NETWORK ID | SUBNET MASK |
| ADMIN & RECEPTION | 10 | 172.16.10.1/28 | 255.255.255.240 |
| SUPPLY CHAIN | 20 | 176.16.20.1/27 | 255.255.255.224 |
| HEALTH & SAFETY | 30 | 172.16.30.1/28 | 255.255.255.240 |
| RESEARCH & DEVELOPMENT | 40 | 172.16.40.1/27 | 255.255.255.224 |
| IT & NETWORKS | 50 | 172.16.50.1/27 | 255.255.255.224 |
| FINANCE | 60 | 172.16.60.1/28 | 255.255.255.240 |
| HUMAN RESOURCES | 70 | 172.16.70.1/27 | 255.255.255.224 |
| CUSTOMER SERVICE | 80 | 172.16.80.1/25 | 255.255.255.128 |
| SALES | 90 | 172.16.90.1/25 | 255.255.255.128 |
| SERVERS | 100 | 172.16.100.1/29 | 255.255.255.248 |
| MANAGERS | 101 | 172.16.101.1/28 | 255.255.255.240 |
| PRINTERS | 102 | 172.16.102.1/27 | 255.255.255.224 |
| FILE SERVERS | 103 | 172.16.103.1/28 | 255.255.255.240 |

**VTP – Trunking**

Για τη δημιουργία των VLANS είναι υπεύθυνο το κεντρικό CentralSwitch, καθώς αποτελεί τον VTP SERVER του δικτύου. Η παρουσία του VTP (VLAN Trunking Protocol) server είναι σημαντική γιατί βοηθάει στη διαχείριση των VLAN σε ένα δίκτυο με πολλαπλά switches. Λειτουργεί ως κεντρικό σημείο ελέγχου για τη διαμόρφωση και τον συγχρονισμό των VLAN σε όλα τα συμμετέχοντα switches. Χρησιμοποιήθηκαν οι εντολές vtp\_mode\_server/vtp domain\_Network/ vtp\_**password 4545**.

**Layer 2 Security**

Για το layer 2 security χρησιμοποιήθηκαν οι παρακάτω εντολές:

Για την δημιουργία κωδικού κατά την είσοδο στο enable του switch:

*-enable* ***secret 4545***

Για την δημιουργία κωδικού κατά την είσοδο στην κονσόλα του switch:

*-line console 0*

*-****password 4545***

*-login*

*-end*

Ενεργοποιεί τη λειτουργία ασφαλείας της θύρας (port security) στο switch port. Η λειτουργία ασφαλείας της θύρας βοηθάει στην προστασία του δικτύου από ανεπιθύμητες συσκευές που προσπαθούν να συνδεθούν:

*-switchport port-security*

Ορίζει το μέγιστο αριθμό από διευθύνσεις MAC που επιτρέπονται να συνδεθούν στη θύρα. Σε αυτή την περίπτωση, μόνο μία διεύθυνση MAC επιτρέπεται στη θύρα:

*-switchport port-security maximum 1*

Ορίζει την ενέργεια που θα ακολουθήσει η θύρα εάν παραβιάσει τις πολιτικές ασφαλείας που έχουν οριστεί. Σε αυτή την περίπτωση, η θύρα θα κλείσει (shutdown):

*-switchport port-security violation shutdown*

Επιτρέπει στο switch να αποθηκεύει αυτόματα τις διευθύνσεις MAC των συσκευών που συνδέονται στη θύρα. Αυτό γίνεται δυναμικά (sticky):

*-switchport port-security mac-address sticky*

Ενεργοποιεί τη λειτουργία BPDU Guard στη θύρα. Η BPDU Guard προστατεύει το δίκτυο από προβλήματα δικτύου που προκαλούνται από κακόβουλες ή λανθασμένες BPDU (Bridge Protocol Data Units):

*-spanning-tree bpduguard enable*

Αυτή η εντολή ενεργοποιεί τη λειτουργία PortFast στη θύρα:

*-spanning-tree portfast*

Τέλος, σε όλα τα switches έχουν κλείσει όλες οι θύρες οι οποίες δεν χρησιμοποιούνται για επιπλέον προστασία.

**Routing Network**

**Static Routing**

Η εφαρμογή στατικής δρομολόγησης με την εντολή ip route 0.0.0.0 0.0.0.0 77.140.99.94 στον κεντρικό CentralRouter της εταιρείας ορίζει μία γενική πύλη εξόδου (gateway of last resort) για όλη την επικοινωνία με το internet. Αυτό σημαίνει ότι οποιαδήποτε κίνηση δεν μπορεί να προωθηθεί μέσω των υφιστάμενων καταχωρημένων διαδρομών, θα προωθηθεί μέσω του καθορισμένου γενικού πυλώνα εξόδου. Ενώ η δυναμική δρομολόγηση μπορεί να είναι πιο ευέλικτη σε ορισμένες περιπτώσεις, η διαχείριση του στατικού δρομολογητή είναι συνήθως πιο απλή και δεν απαιτεί συνεχείς ενημερώσεις όπως η δυναμική δρομολόγηση.

**DHCP**

Δημιουργήθηκε DHCP Server με ΙΡ 172.16.100.2, o οποίος με την εντολή ip helper-address 172.16.100.2 σε κάθε sub-interface που κρίθηκε αναγκαίο, δίνει αυτόματα IPs στα αντίστοιχα μηχανήματα. Παρακάτω παρουσιάζεται ο πίνακας με τα pools για τα vlans που παίρνουν IPs από τον DHCP Server.A screenshot of a computer

Description automatically generated

Στον πίνακα μπορούμε να δούμε ότι η default gateway για όλα τα subnets είναι η Virtual IP 172.16.110.3 που δημιουργήθηκε για την υλοποίηση του HSRP.

**HSRP**

Υλοποιήθηκε το πρωτόκολλο HSRP με δύο routers (CentralRouter και CentralRouterBackup) για την εξασφάλιση υψηλής διαθεσιμότητας στην πρόσβαση του δικτύου. Ο πρώτος από τους δύο δρομολογητές CentralRouter έχει οριστεί ως ενεργός (active), ενώ ο δεύτερος CentralRouterBackup είναι σε κατάσταση αναμονής (standby). Σε περίπτωση που ο ενεργός δρομολογητής αποτύχει ή χάσει τη συνδεσιμότητα, ο δρομολογητής σε κατάσταση αναμονής αναλαμβάνει αυτόματα το ρόλο του ενεργού, εξασφαλίζοντας τη συνεχή λειτουργία του δικτύου χωρίς διακοπή της υπηρεσίας. Χρησιμοποιήθηκε η Virtual IP 172.16.110.3 που αναφέρθηκε παραπάνω.

**ACL**

Δημιουργήθηκαν οι παρακάτω extended access lists για να έρθουν εις πέρας όλες οι απαιτήσεις τις εργασίας:

ACL Managers

ACL Admin&Reception

ACL SupplyChain

ACL Health&Safety

ACL Research&Development

ACL IT&Networks

ACL Finance

ACL HumanResources

ACL CustomerService

ACL Sales

ACL Servers

ACL Printers

ACL FileServers

ACL NAT-ACL

**NAT / PAT (ISP connectivity)**

Υλοποιήθηκε PAT, το οποίο επιτρέπει σε πολλές συσκευές να χρησιμοποιούν μία μόνο διεύθυνση IP προς τον έξω κόσμο, εξοικονομώντας διευθύνσεις IPv4 και προστατεύοντας έτσι το εσωτερικό δίκτυο από ανεπιθύμητες εισβολές και επιθέσεις. Οι εντολή που χρησιμοποιήθηκε είναι η ip\_nat\_inside\_source\_list\_NAT-ACL\_interface\_gigabitEthernet 0/1\_overload. Επίσης για να έχει οποιοσδήποτε πρόσβαση εκτός δικτύου στον email server χρησιμοποιήθηκε η εντολή ip\_nat\_inside\_source\_static\_172.16.100.6 77.140.99.95.

**Test Plan & Output**

Όλα τα παρακάτω tests είναι επιτυχημένα.

**1o Test:** Managing Director : Απεριόριστη πρόσβαση σε πόρους και δεδομένα. H IP 172.16.101.11 μπορεί να κάνει ping σε όλο το δίκτυο.

**2o Test:** Managers : Απεριόριστη πρόσβαση σε πόρους και δεδομένα εντός τμήματός τους. Π.χ. ο Sales Manager – IP 172.16.101.10 μπορεί να κάνει ping στο δικό του τμήμα ΙΡ 172.16.90.2 – 4, δεν μπορεί να κάνει ping σε κανένα άλλο τμήμα.

**3o Test:** Ο Managing Director έχει πλήρη πρόσβαση στο ERP. Μπορεί να κάνει ping στην ΙΡ 172.16.100.3 .

**4o Test:** Όλοι οι Managers έχουν πλήρη πρόσβαση στο ERP. Μπορούν όλοι να κάνουν ping στην ΙΡ 172.16.100.3 .

**5o Test:** Οι χρήστες των τμημάτων Finance και Admin&Reception έχουν πρόσβαση στον ERP Server. Μπορούν όλοι να κάνουν ping στην ΙΡ 172.16.100.3 .

**6o Test:** Οι χρήστες του τμήματος IT&Networks έχουν πρόσβαση στον ERP Server. Μπορούν όλοι να κάνουν ping στην ΙΡ 172.16.100.3 .

**7o Test:** Κανένας άλλος χρήστης δεν έχει πρόσβαση στον ERP Server. Δεν μπορούν να κάνουν ping στην ΙΡ 172.16.100.3 .

**8o Test:** Ο Managing Director έχει πλήρη πρόσβαση στο CRM. Μπορεί να κάνει ping στην ΙΡ 172.16.100.4 .

**9o Test:** Όλοι οι Managers έχουν πλήρη πρόσβαση στο CRM. Μπορούν όλοι να κάνουν ping στην ΙΡ 172.16.100.4 .

**10o Test:** Οι χρήστες των τμήματος Sales έχουν πρόσβαση στον ERP Server. Μπορούν όλοι να κάνουν ping στην ΙΡ 172.16.100.4 .

**11o Test:** Οι χρήστες του τμήματος IT&Networks έχουν πρόσβαση στον CRM Server. Μπορούν όλοι να κάνουν ping στην ΙΡ 172.16.100.4 .

**12o Test:** Κανένας άλλος χρήστης δεν έχει πρόσβαση στον CRP Server. Δεν μπορούν να κάνουν ping στην ΙΡ 172.16.100.4 .

**13o Test:** Οι χρήστες από ένα τμήμα έχουν πρόσβαση στον εκτυπωτή δωματίου και στο εκτυπωτή κτιρίου. Π.χ. στον εκτυπωτή με ΙΡ 172.16.102.13 έχουν μόνο πρόσβαση οι χρήστες του τμήματος SupplyChain.

**14o Test:** Κάθε τμήμα έχει πρόσβαση σε έναν File Server. Π.χ. οι χρήστες του τμήματος Health&Safety έχουν μόνο πρόσβαση στον File Server με ΙΡ 172.16.103.4 .

**15o Test:** Οι χρήστες του τμήματος CustomerService έχουν πρόσβαση στον File Server του τμήματος Finance. Μπορούν να κάνουν ping στην ΙΡ 172.16.103.7 .

**16o Test:** Οι χρήστες του τμήματος Finance δεν έχουν πρόσβαση στο File Server του τμήματος CustomerService.Δεν μπορούν να κάνουν ping στην ΙΡ 172.16.103.9 .

**17o Test:** Υπάρχει Antivirus Server με ΙΡ 172.16.100.5 ο οποίος μπορεί ping σε όλους τους χρήστες του δικτύου.

**18o Test:** HSRP - Κλείνοντας τον CentralRouter με shut στην πόρτα gig0/0 ενεργοποιείται αυτόματα ο CentralRouterBackup και το δίκτυο είναι πλήρως λειτουργικό.

**19o Test:** DHCP – Σε όσους υπολογιστές έχει ενεργοποιηθεί, αλλάζοντας από DHCP σε Static και το αντίστροφο, παίρνουν αμέσως IPs.

**20o Test:** NAT/PAT – Όταν γίνεται ping στο internet IP 192.168.1.2, με show ip nat statistics έχουμε πάντα Hit.

\*Όπου έχει οριστεί κωδικός, είναι ο 4545.