

Πολυτεχνική Σχολή
Τμήμα Μηχανικών Η/Υ & Πληροφορικής

Διπλωματική Εργασία

Υλοποίηση Ανοικτού Λογισμικού Δρομολογητή με Χρήση της Σουίτας Πρωτοκόλλων FRR (Free Range Routing)

Χρήστος Βασιλειάδης
Α.Μ. 5263

Επιβλέπων
Κυριάκος Βλάχος
Καθηγητής

Πάτρα, 2022

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Κυριάκο Βλάχο που μου έδωσε την ευκαιρία να ασχοληθώ σε βάθος με τα πρωτόκολλα δρομολόγησης OSPF και BGP της σουίτας FRR και να διευρύνω τις γνώσεις στον τομέα των τηλεπικοινωνιακών δικτύων, κάτι που θεωρώ πολύ χρήσιμο για την μετέπειτα ενασχόλησή μου με αυτό τον τομέα.

Περίληψη

Στην παρούσα διπλωματική εργασία μελετώνται και αναλύονται τα πρωτόκολλα δρομολόγησης OSPF (Open Shortest Path First) και BGP (Border Gateway Protocol) της σουίτας ανοιχτού λογισμικού FRR (Free Range Routing).

Αρχικά παρουσιάζονται οι βασικές αρχές που διέπουν τη δρομολόγηση δεδομένων, τα κύρια χαρακτηριστικά των ανωτέρω πρωτοκόλλων, καθώς και ο τρόπος λειτουργίας τους.

Το OSPF είναι ένα ευέλικτο IGP (Interior Gateway Protocol) πρωτόκολλο που χρησιμοποιείται ευρέως στη δρομολόγηση εντός των Αυτόνομων Συστημάτων (AS - Autonomous Systems) και προσφέρει πολλές δυνατότητες στον διαχειριστή, αλλά ταυτόχρονα απαιτεί σωστό σχεδιασμό δικτύου για την αποδοτική λειτουργία του.

Το BGP είναι ένα EGP (Exterior Gateway Protocol) πρωτόκολλο δρομολόγησης το οποίο είναι σχετικά πολύπλοκο στη διαχείρισή του, αλλά παρόλα αυτά προσφέρει πολλές δυνατότητες διευθέτησης για την πραγματοποίηση οποιασδήποτε πολιτικής δρομολόγησης της κίνησης των πακέτων διαμέσου των διάφορων ανά τον κόσμο AS.

Στη συνέχεια υλοποιούνται δύο μελέτες περιπτώσεων των πρωτοκόλλων OSPF και BGP αντίστοιχα της σουίτας FRR οι οποίες περιλαμβάνουν την εγκατάσταση και διευθέτησή τους σε τρεις συσκευές Raspberry Pi 4 οι οποίες μέσω του νέφους (cloud) διασυνδέονται με όλους τους άλλους δρομολογητές της σουίτας FRR που έχουν εγκατασταθεί και λειτουργούν με τη χρήση του προσομοιωτή GNS3.

Στην παρούσα μελέτη περίπτωσης έχει χρησιμοποιηθεί ένα υβριδικό περιβάλλον μεταξύ τριών πραγματικών συσκευών και του προσομοιωτή GNS3 για λόγους οικονομίας και ευελιξίας. Αναλυτικότερα, στο κομμάτι της προσομοίωσης υλοποιείται μια εκτεταμένη τοπολογία η οποία περιλαμβάνει την εγκατάσταση και διευθέτηση δέκα δρομολογητών με στόχο την ανάδειξη της συνολικής εικόνας λειτουργίας και δυνατοτήτων των ανωτέρω πρωτοκόλλων.

Λέξεις Κλειδιά: FRR, OSPF, BGP, AS, GNS3, Raspberry Pi 4

Abstract

In this dissertation, the OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) routing protocols of the FRR (Free Range Routing) suite are studied and analyzed.

First, the basic principles of data routing, the main features, as well as the operation of the above protocols are presented.

OSPF is a flexible IGP (Interior Gateway Protocol) that is widely used in routing within AS (Autonomous Systems) and offers many capabilities to the administrator, but at the same time requires proper network design for its efficient operation.

BGP is an EGP (Exterior Gateway Protocol) routing protocol that is relatively complex to manage, yet offers many configuration options to implement any packet routing policy across the various ASs around the world.

Next, two case studies of the OSPF and BGP protocols of the FRR suite are implemented, which include their installation and configuration on three Raspberry Pi 4 devices which, through the cloud, connect to all the other routers of the FRR suite that have been installed and operate using the GNS3 simulator.

In the present case study, a hybrid configuration environment has been used between three real devices and the GNS3 simulator for reasons of economy and flexibility. More specifically, in the part of the simulation, an extensive topology is implemented, which includes the installation and configuration of ten routers in order to highlight the overall picture of operation and capabilities of the above protocols.

Keywords: FRR, OSPF, BGP, AS, GNS3, Raspberry Pi 4

Πίνακας Περιεχομένων

1 11

Πρόλογος - Εισαγωγή 11

1.1 Εισαγωγή στη Δρομολόγηση 12

1.2 Λειτουργίες Δρομολογητών 12

1.3 Είδη Δρομολόγησης 13

1.4 Κατηγορίες Πρωτοκόλλων Δρομολόγησης 14

2 17

Σουίτα FRR (Free Range Routing) 17

2.1 Εισαγωγή στη Σουίτα FRR 17

2.2 Αρχιτεκτονική Σουίτας FRR 18

2.3 Εγκατάσταση και Διευθέτηση Σουίτας FRR 19

3 23

Πρωτόκολλο OSPF 23

3.1 Τύποι OSPF Δρομολογητών 24

3.2 Κατηγορίες OSPF Δρομολόγησης 25

3.3 Τύποι OSPF Πακέτων 26

3.4 Καταστάσεις OSPF Γειτνίασης 28

3.5 OSPF LSAs (Link State Advirtisements) 28

3.5.1 Router LSAs (type 1) 29
3.5.2 Network LSAs (type 2) 29
3.5.3 Network Summary LSAs (type 3) 30
3.5.4 AS Summary LSAs (type 4) 30
3.5.5 AS External LSAs (type 5) 30
3.5.6 Multicast LSAs (type 6) 31
3.5.7 NSSA LSAs (type 7) 31
3.5.8 BGP LSAs (type 8) 31
3.5.9 Opaque LSAs (type 9, 10, 11) 32
3.5.10 LSA header 32

3.6 OSPF Περιοχές 33

3.6.1 Backbone Area 33
3.6.2 Standard Area 33
3.6.3 Transit Area 34
3.6.4 Stub Area 35
3.6.5 Totally Stubby Area 35
3.6.6 Not-So-Stubby Area (NSSA) 36
3.6.7 Totally Not-So-Stubby Area 37
3.6.8 Διαφορές Stubby Areas και Not-So-Stubby Areas 37

3.7 Ασφάλεια OSPF 38
3.7.1 Πιστοποίηση Clear-text 38
3.7.2 Πιστοποίηση MD5 39
3.8 OSPFv3 40
4 41
Πρωτόκολλο BGP 41
4.1 Λειτουργία BGP Πρωτοκόλλου 42
4.2 Τύποι BGP Πακέτων 44
4.3 BGP Χαρακτηριστικά 45
4.4 Κριτήρια Επιλογής BGP Διαδρομής 46
4.5 Διευθέτηση BGP Πρωτοκόλλου 47
4.5.1 External Border Gateway Protocol (eBGP) vs. Internal Border Gateway Protocol (iBGP) 47
4.5.2 eBGP Multihop Load Balancing 48
4.5.3 BGP Origin Attribute 49
4.5.4 BGP Network Command vs. Redistribution 50
4.5.5 BGP Route Maps 51
4.5.6 BGP Synchronization vs. Non-Synchronization 52
4.5.7 BGP Weight Attribute 53
4.5.8 BGP Local Preference Attribute 54
4.5.9 BGP Route Filtering 55
4.5.10 BGP Path Filtering 55
4.5.11 BGP Community Filtering 56
4.5.12 BGP Classless InterDomain Routing (CIDR) and Aggregate Addresses 58
5 59
Προσομοιωτής GNS3 59
5.1 Αρχιτεκτονική GNS3 60
5.2 Εγκατάσταση και Διαμόρφωση Προσομοιωτή GNS3 60
6 65
Μελέτη Περιπτώσεων Δρομολόγησης με Χρήση της Σουίτας FRR 65
6.1 Μελέτη Περίπτωσης Πρωτοκόλλου Δρομολόγησης OSPF Σουίτας FRR 65
6.1.1 Διευθέτηση Δρομολογητή R1 66
6.1.2 Διευθέτηση Δρομολογητή R2 68
6.1.3 Διευθέτηση Δρομολογητή R3 69
6.1.4 Διευθέτηση Δρομολογητή R4 70
6.1.5 Διευθέτηση Δρομολογητή R5 72
6.1.6 Διευθέτηση Δρομολογητή R6 75
6.1.7 Διευθέτηση Δρομολογητή R7 76
6.1.8 Διευθέτηση Δρομολογητή R8 78
6.1.9 Διευθέτηση Δρομολογητή R9 80
6.1.10 Διευθέτηση Δρομολογητή R10 81
6.1.11 Εγκατάσταση Raspberry Pi OS Lite (64-bit) 82
6.1.12 Εγκατάσταση Σουίτας FRR σε Συσκευή Raspberry Pi 83
6.1.13 Εγκατάσταση ενός Bridged Wireless Access Point σε Συσκευή Raspberry Pi 84
6.1.14 Διευθέτηση Κανόνων Πρόσβασης στο Διαδίκτυο σε Συσκευή Raspberry Pi 85
6.1.15 Διευθέτηση Δρομολογητή RSB1 (Raspberry Pi 4) 86

6.1.16 Διευθέτηση Δρομολογητή RSB2 (Raspberry Pi 4)....88
6.1.17 Διευθέτηση Δρομολογητή RSB3 (Raspberry Pi 4)....89

6.2 Μελέτη Περίπτωσης Πρωτοκόλλου Δρομολόγησης BGP Σουίτας FRR....91
6.2.1 Διευθέτηση Δρομολογητή R1....91
6.2.2 Διευθέτηση Δρομολογητή R2....94
6.2.3 Διευθέτηση Δρομολογητή R3....96
6.2.4 Διευθέτηση Δρομολογητή R4....97
6.2.5 Διευθέτηση Δρομολογητή R5....99
6.2.6 Διευθέτηση Δρομολογητή R6....101
6.2.7 Διευθέτηση Δρομολογητή R7....102
6.2.8 Διευθέτηση Δρομολογητή R8....104
6.2.9 Διευθέτηση Δρομολογητή R9....105
6.2.10 Διευθέτηση Δρομολογητή R10....106
6.2.11 Διευθέτηση Δρομολογητή RSB1 (Raspberry Pi 4)....108
6.2.12 Διευθέτηση Δρομολογητή RSB2 (Raspberry Pi 4)....110
6.2.13 Διευθέτηση Δρομολογητή RSB3 (Raspberry Pi 4)....111

7....113

Επίλογος - Συμπεράσματα....113

Βιβλιογραφία-Αναφορές....115

Λίστα Εικόνων

Εικόνα 1: Κατηγορίες Πρωτοκόλλων Δρομολόγησης 11
Εικόνα 2: Αλληλεπίδραση Δρομολόγησης και Προώθησης 13
Εικόνα 3: Αρχιτεκτονική FRR 18
Εικόνα 4: Αρχιτεκτονική Quagga 19
Εικόνα 5: Τύποι OSPF Δρομολογητών 24
Εικόνα 6: Κατηγορίες OSPF Δρομολόγησης 25
Εικόνα 7: DR και BDR 26
Εικόνα 8: Ανταλλαγή OSPF πακέτων 26
Εικόνα 9: OSPF header 27
Εικόνα 10: Router LSA 29
Εικόνα 11: Network LSA (DR Generated) 29
Εικόνα 12: Network Summary LSA (ABR Summary Route) 30
Εικόνα 13: AS Summary LSA (ASBR Location) 30
Εικόνα 14: AS External LSA (ASBR Summary Route) 31
Εικόνα 15: NSSA LSA 31
Εικόνα 16: LSA header 32
Εικόνα 17:Backbone Area 33
Εικόνα 18: Standard Area 34
Εικόνα 19: Transit Area 34
Εικόνα 20: Stub Area 35
Εικόνα 21: Totally Stuby Area 35
Εικόνα 22: NSSA 36
Εικόνα 23: Totally NSSA 37
Εικόνα 24: Stubby Areas and NSSAs 38
Εικόνα 25: Single-homed AS 42
Εικόνα 26: Multi-homed AS 43
Εικόνα 27: BGP Header 44
Εικόνα 28: eBGP & iBGP 47
Εικόνα 29: eBGP Multihop 48
Εικόνα 30: Origin Attribute 49
Εικόνα 31: BGP Network vs. Redistribute 50
Εικόνα 32: Bgp Route Maps 51
Εικόνα 33: BGP Syncronization 52
Εικόνα 34: BGP Non-Syncronization 52
Εικόνα 35: BGPWeight 53
Εικόνα 36: BGP Local Preference 54
Εικόνα 37: BGP Route Filtering 55
Εικόνα 38: BGP Path Filtering 55
Εικόνα 39: BGP Community 56
Εικόνα 40: BGP CIDR 58
Εικόνα 41: Μελέτη Περίπτωσης Πρωτοκόλλου OSPF 66
Εικόνα 42: Μελέτη Περίπτωσης Πρωτοκόλλου BGP 91

Συντομογραφίες

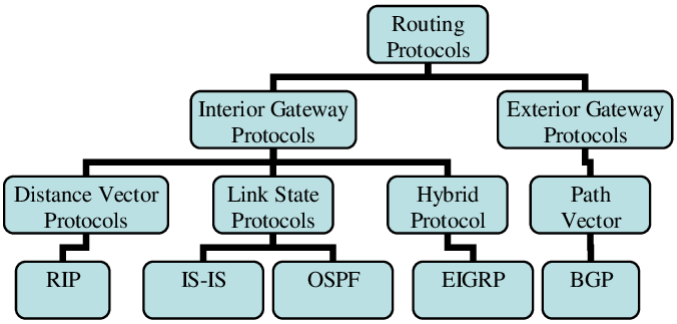
ABR: Area Boarder Router
AS: Autonomous System
ASBR: Autonomous System Boundary Router
BDR: Backup Designated Router
BGP: Border Gateway Protocol
DBD: Data Base Descriptor
DDP: Database Description Packet
DHCP: Dynamic Host Configuration Protocol
DNS: Domain Name System
DR: Designated Router
EBGP: External Border Gateway Protocol
EGP: Exterior Gateway Protocol
FIB: Forwarding Information Base
FRR: Free Range Routing
GPL: General Public License
GNS3: Graphical Network Simulator
GUI: Graphical User Interface
IBGP: Internal Border Gateway Protocol
IGP: Interior Gateway Protocol
IP: Internet Protocol
ISP: Internet Service Provider
LS: Link State
LSA: Link State Advertisement
LSR: Link State Request
LSU: Link State Update
NBMA: Non-Broadcast Multiple Access
NSSA: Not-So-Stubby Area
OSPF: Open Shortest Path First
RIB: Routing Information Base
RIP: Routing Information Protocol
LSAck: Link State Acknowledgement
SPT: Shortest Path Tree
VLSM: Variable Length Subnet Mask
VM: Virtual Machine
VoIP: Voice over IP

1

Πρόλογος - Εισαγωγή

Αναμφίβολα το διαδίκτυο (internet) αποτελεί πλέον ένα αναπόσπαστο κομμάτι της κοινωνίας, υπηρεσίες όπως το ηλεκτρονικό ταχυδρομείο, οι φωνητικές κλήσεις (Voice over IP VoIP) και η μεταφορά αρχείων πάσης φύσεως μεταξύ των χρηστών του το καθιστούν ένα πολύ σημαντικό εργαλείο στην ζωή του σύγχρονου ανθρώπου.

Η λειτουργία των παραπάνω υπηρεσιών βασίζεται στα πακέτα δεδομένων και επιτυγχάνεται με την ορθή παράδοσή τους στους εκάστοτε παραλήπτες. Για τον σκοπό αυτό χρησιμοποιούνται τα πρωτόκολλα δρομολόγησης, τα οποία αναλαμβάνουν την παράδοση των πακέτων δεδομένων στους χρήστες μέσω του διαδικτύου.



Εικόνα 1: Κατηγορίες Πρωτοκόλλων Δρομολόγησης

Υπάρχουν αρκετά πρωτοκόλλα δρομολόγησης που μπορούν να χρησιμοποιηθούν για τη μεταγωγή πακέτων στο διαδίκτυο. Η ανάλυσή μας θα επικεντρωθεί στα δυο πιο σημαντικά:

α) Το πρωτόκολλο OSPF (Open Shortest Path First), το οποίο αποτελεί ένα πρωτόκολλο εσωτερικής πύλης (Interior Gateway Protocol IGP) που χρησιμοποιεί τον αλγόριθμο Dijkstra για τον υπολογισμό των συντομότερων μονοπατιών δρομολόγησης. Το πρωτόκολλο αυτό υιοθετώντας τη μέθοδο της κατάστασης ζεύξης (Link State) αξιολογεί/κοστολογεί κάθε γειτονική ζεύξη λαμβάνοντας υπόψιν διάφορες παραμέτρους, όπως το εύρος ζώνης και το φορτίο μιας διασύνδεσης, ξεπερνώντας με αυτόν τον τρόπο την απόδοση των Distance Vector πρωτοκόλλων, όπως π.χ. του RIP (Routing Information Protocol), τα

οποία για την επιλογή των βέλτιστων διαδρομών βασίζονται αποκλειστικά και μόνο στο μήκος των αντίστοιχων μονοπατιών (hop count).

β) Το επόμενο πρωτόκολλο που θα μελετήσουμε είναι το BGP (Border Gateway Protocol) το οποίο είναι ένα πρωτόκολλο εξωτερικής πύλης (Exterior Gateway Protocol EGP). Τα πρωτόκολλα εξωτερικής πύλης είναι τα πρωτόκολλα που χρησιμοποιούν οι συνοριακοί δρομολογητές ενός αυτόνομου συστήματος (Autonomous System AS) για να ανταλλάσσουν πληροφορίες δρομολόγησης με τους δρομολογητές ενός άλλου αυτόνομου συστήματος. Το BGP είναι ένα path vector protocol που με την χρήση του αλγόριθμου του Bellman Ford υπολογίζει τα συντομότερα μονοπάτια δρομολόγησης.

1.1 Εισαγωγή στη Δρομολόγηση

Δρομολόγηση ονομάζεται η διαδικασία με την οποία επιτυγχάνεται η εκμάθηση των διαδρομών (routes) μεταξύ των συνδεδεμένων δικτύων, καθώς και η επιλογή των βέλτιστων διαδρομών για προορισμούς που προσεγγίζονται από πολλαπλά μονοπάτια με σκοπό η αποστολή των πακέτων/δεδομένων να γίνεται πιο αποδοτική.

Την παραπάνω διαδικασία καλούνται να φέρουν εις πέρας ηλεκτρονικές συσκευές τις οποίες αποκαλούμε δρομολογητές (routers). Ένας δρομολογητής όταν παραλάβει ένα πακέτο για κάποιο προορισμό θα πρέπει να υπολογίσει τη βέλτιστη διαδρομή και να το προωθήσει στον επόμενο δρομολογητή. Η διαδικασία αυτή επαναλαμβάνεται έως ότου το πακέτο φτάσει στον τελευταίο δρομολογητή της διαδρομής, ο οποίος αναλαμβάνει να το προωθήσει στον τερματικό σταθμό του παραλήπτη. Για την αποτελεσματική δρομολόγηση κάθε δρομολογητής δημιουργεί και διατηρεί στη μνήμη του πίνακες που περιέχουν όλες τις διαθέσιμες διαδρομές προς τους προορισμούς που μπορεί να φτάσει ένα πακέτο και με τη σειρά του τις χρησιμοποιεί για να αποφασίσει ποια θα είναι η βέλτιστη διαδρομή που πρέπει να ακολουθήσει κάθε πακέτο που αναλαμβάνει να δρομολογήσει. Οι διαδρομές αυτές αποτελούνται από IP διευθύνσεις του διαδικτύου, αλλά και από την διεύθυνση του επόμενου κόμβου (next hop) μέσω του οποίου ο δρομολογητής θα πρέπει να προωθήσει ένα πακέτο. Οι δρομολογητές επικοινωνούν μεταξύ τους σύμφωνα με το σύνολο των κανόνων που ορίζονται από τα πρωτόκολλα που τρέχουν και ανταλλάσσουν πληροφορίες σχετικά με την τοπολογία του δικτύου και με παραμέτρους που τους επιτρέπουν τον υπολογισμό βέλτιστων διαδρομών μεταξύ τους.

Για την κατανόηση του τρόπου λειτουργίας των πρωτοκόλλων βασική προϋπόθεση αποτελεί η ανάλυση των βασικών λειτουργειών των δρομολογητών, τα διαφορετικά είδη δρομολόγησης, καθώς και οι τρόποι με τους οποίους συνδέονται μεταξύ τους τα διάφορα δίκτυα που σχηματίζουν το διαδίκτυο.

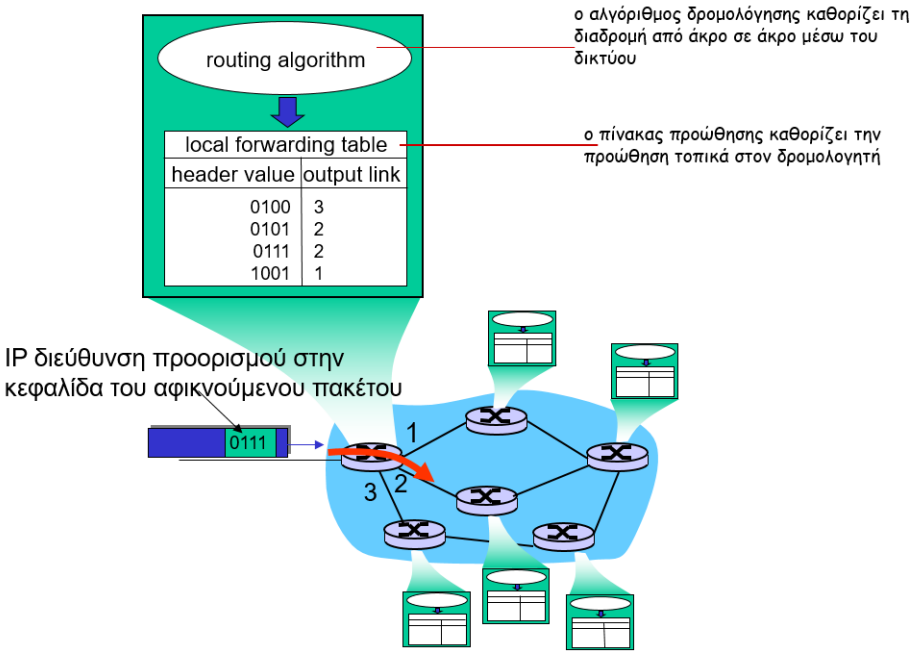
1.2 Λειτουργίες Δρομολογητών

Δυο είναι οι βασικότερες λειτουργίες ενός δρομολογητή: η προώθηση πακέτων και η δρομολόγησή τους.

Προώθηση: Η διαδικασία κατά την οποία ένας δρομολογητής όταν λαμβάνει ένα πακέτο από μια διεπαφή εισόδου (input interface), αναζητά στον πίνακα δρομολόγησής του την κατάλληλη διεπαφή εξόδου (output interface) ανάλογα με την διεύθυνση προορισμού που φέρει το πακέτο (ταίριασμα), το οποίο στη συνέχεια ενθυλακώνεται (encapsulated) και παραδίδεται στο επίπεδο 2 (layer 2) προκειμένου να προωθηθεί. Δηλαδή, προώθηση είναι η ενέργεια που πραγματοποιείται σε έναν δρομολογητή για τη

μετάδοση ενός πακέτου (datagram) από μια διεπαφή εισόδου προς την κατάλληλη διεπαφή εξόδου, έτσι ώστε το πακέτο να συνεχίσει τη δρομολόγησή ακολουθώντας τη βέλτιστη διαδρομή.

Δρομολόγηση: Ένας δρομολογητής θεωρείται συσκευή επιπέδου 3 (layer 3), επειδή η αρχική απόφαση προώθησης ενός πακέτου βασίζεται στις πληροφορίες του IP πρωτοκόλλου. Η διαδικασία εκμάθησης της βέλτιστης διαδρομής ενός πακέτου είναι γνωστή ως δρομολόγηση (routing). Δρομολόγηση δηλαδή είναι ο καθορισμός της διαδρομής που ακολουθούν τα πακέτα από την προέλευση έως τον προορισμό τους και η αποθήκευση και ενημέρωση των διαδρομών αυτών στους πίνακες δρομολόγησης.



Εικόνα 2: Αλληλεπίδραση Δρομολόγησης και Προώθησης

Με απλά λόγια αν παρομοιάσουμε την διαδρομή που ακολουθεί το πακέτο από την προέλευση μέχρι τον προορισμό του με ένα ταξίδι, η διαδικασία σχεδιασμού ταξιδιού από την προέλευση στον προορισμό ονομάζεται δρομολόγηση, ενώ η διαδικασία περάσματος από μία διασταύρωση που συναντάμε στο ταξίδι μας προώθηση [1].

1.3 Είδη Δρομολόγησης

Στατική Δρομολόγηση: Η στατική δρομολόγηση συνήθως χρησιμοποιείται σε μικρού μεγέθους δίκτυα των οποίων οι τοπολογίες είναι απλές και επιτρέπουν την χειροκίνητη ενημέρωσή τους. Αυτό σημαίνει ότι οι διαδρομές που θα ακολουθήσουν τα πακέτα καθορίζονται εξαρχής και όταν οι δρομολογητές μπουν σε λειτουργία είναι ήδη φορτωμένες σε αυτούς. Στα δίκτυα αυτά, οι διαδρομές είναι προκαθορισμένες και δεν δημιουργούνται δυναμικά. Το βασικό μειονέκτημα της στατικής δρομολόγησης είναι ότι αν για οποιοδήποτε λόγο συμβεί κάποια αλλαγή στην τοπολογία ή στο σχεδιασμό του δικτύου οι στατικές δρομολογήσεις που γίνανε χειροκίνητα θα πρέπει να επανασχεδιαστούν, διότι οι δρομολογητές δεν μπορούν να επαναπροσδιορίσουν δυναμικά τις νέες διαδρομές. Η στατική δρομολόγηση είναι πρακτικά αδύνατη και μη συμφέρουσα σε δίκτυα μεσαίου και μεγάλου μεγέθους λόγω του όγκου των διάδρομων που θα πρέπει να οριστούν χειροκίνητα.

Δυναμική Δρομολόγηση: Η δυναμική δρομολόγηση επιτυγχάνεται με αλγορίθμους δρομολόγησης οι οποίοι αναγνωρίζουν τυχών αλλαγές στο δίκτυο και προσαρμόζονται δυναμικά σε αυτές. Οι αλγόριθμοι

αυτοί ενημερώνουν τους πίνακες δρομολόγησης όταν ανιχνεύσουν αλλαγές στο δίκτυο και επιλέγουν τα βέλτιστα μονοπάτια κάνοντας χρήση τεχνικών οι οποίες αναλύουν τα νέα δεδομένα και τις αλλαγές στο δίκτυο και βάσει αυτών επιλέγουν τις νέες βέλτιστες διαδρομές προς κάθε προορισμό.

Η τεράστια και αδιάκοπη επέκταση των δικτύων έφερε στο παρασκήνιο την ανάγκη του διαχωρισμού τους σε μικρότερα τμήματα. Σκοπός του διαμερισμού αυτού είναι η διαχείριση της κίνησης από τα πρωτόκολλα δρομολόγησης με τρόπο πιο αποδοτικό. Έτσι λοιπόν, το διαδίκτυο χωρίζεται σε τμήματα τα οποία αποκαλούμε Αυτόνομα Συστήματα ή αλλιώς Autonomous Systems (AS).

Το σημερινό διαδίκτυο αποτελείται από τεράστιο αριθμό δρομολογητών. Η αποθήκευση πληροφοριών δρομολόγησης σε κάθε έναν από αυτούς, θα απαιτούσε τεράστιες ποσότητες μνήμης. Ο φόρτος που απαιτείται για εκπομπή ενημερώσεων κατάστασης συνδέσμων ανάμεσα σε όλους τους δρομολογητές μέσα στο διαδίκτυο δε θα άφηνε καθόλου ελεύθερο εύρος ζώνης για αποστολή πακέτων δεδομένων. Τα σημερινά πρωτόκολλα δρομολόγησης δεν μπορούν να διαχειριστούν ολόκληρο το διαδίκτυο σαν να είναι ένα και μόνο αχανές δίκτυο, οπότε δημιουργήθηκε η ανάγκη για τη διαίρεση των μεγάλων δικτύων σε μικρότερα τμήματα. Έτσι, κυριάρχησε το μοντέλο της ιεραρχικής δρομολόγησης.

Στο πρώτο επίπεδο οι δρομολογητές χωρίζονται ανά περιοχές σε AS κάτω από κοινή ομάδα διαχείρισης και μοιράζονται την ίδια μέθοδο δρομολόγησης. Παραδείγματα AS αποτελούν τα δίκτυα ISP (Internet Service Provider), τα πανεπιστημιακά δίκτυα τα δίκτυα πολυεθνικών εταιριών κτλ. Όλο το διαδίκτυο αποτελείται από διασυνδεδεμένα AS.

Όλοι οι δρομολογητές εντός ενός AS τρέχουν συνήθως το ίδιο πρωτόκολλο για την δρομολόγηση των πακέτων το οποίο ονομάζεται πρωτόκολλο εσωτερικής πύλης (Interior Gateway Protocol). Κάθε εσωτερικός δρομολογητής (interior router) γνωρίζει την θέση των άλλων δρομολογητών. Επίσης γνωρίζει με ποιο τρόπο θα δρομολογήσει τα πακέτα εντός του AS, αλλά δεν γνωρίζει την τοπολογία των άλλων AS. Καθένα AS μπορεί να τρέχει τον δικό του αλγόριθμο δρομολόγησης.

Ορισμένα από τα πλεονεκτήματα της ιεραρχικής δρομολόγησης είναι τα εξής:

- Τα πρωτόκολλα δρομολόγησης που υπάρχουν δεν δύναται να διαχειριστούν την κίνηση ολοκλήρου του διαδικτύου. Έτσι χωρίζονται σε AS για να γίνεται εφικτή η δρομολόγηση.
- Η ιεραρχική δρομολόγηση επιτρέπει στο κάθε AS να ακολουθεί τους δικούς του κανόνες δρομολόγησης ανάλογα με τις ανάγκες.
- Κάνει ευκολότερο τον υπολογισμό των διαδρομών, πιο γρήγορη την προσαρμογή σε τυχόν αλλαγές και προσφέρει μεγαλύτερη αυτονομία στα AS.
- Η ιεράρχηση μέσα στο ίδιο AS σε περιοχές έχει επίσης αντίστοιχα πλεονεκτήματα όπως η ευκολία στη διαχείριση, η ευελιξία και η αυτονομία.

1.4 Κατηγορίες Πρωτοκόλλων Δρομολόγησης

Όπως αναφέρθηκε παραπάνω μπορούμε να διακρίνουμε τα πρωτόκολλα σε πρωτόκολλα εσωτερικής πύλης δικτύου (IGP), τα οποία αναλαμβάνουν τη δρομολόγηση εσωτερικά ενός AS και σε πρωτόκολλα εξωτερικής πύλης (EGP). Μοναδικό πρωτόκολλο εξωτερικής πύλης σήμερα είναι το BGP (Border Gateway Protocol) το οποίο επιτρέπει τη μεταφορά πακέτων μεταξύ δυο AS χωρίς να γνωρίζει την ακριβή τοπολογία του καθενός.

Επιπλέον ανάλογα με τη μέθοδο δρομολόγησης που χρησιμοποιούν χωρίζονται σε πρωτόκολλα δρομολόγησης με διανύσματα απόστασης (distance vector routing protocols) και σε πρωτόκολλα δρομολόγησης με κατάσταση συνδέσμων (link state protocols).

Τέλος, ανάλογα με τον τρόπο που διαχειρίζονται τις IP διευθύνσεις τα πρωτόκολλα χωρίζονται σε classfull και classless. Τα classfull πρωτόκολλα αναγνωρίζουν μόνο την προκαθορισμένη μάσκα δικτύου για κάθε κλάση δικτύου A, B και C. Συνεπώς δεν υποστηρίζουν VLSM (Variable Length Subnet Mask). Αντίθετα, τα classless πρωτόκολλα δρομολόγησης υποστηρίζουν VLSM και έτσι έχουν επικρατήσει σήμερα.

2

Σουίτα FRR (Free Range Routing)

2.1 Εισαγωγή στη Σουίτα FRR

Η υλοποίηση εφαρμογών/σεναρίων IP δρομολόγησης συνήθως περιλαμβάνει την αγορά ακριβού εξοπλισμού από συγκεκριμένες εταιρείες. Αυτός όμως ο τρόπος προσέγγισης παρουσιάζει διάφορους περιορισμούς όπως το κόστος υλικού, λογισμικού κλειστού κώδικα, καθώς και το κόστος εκπαίδευσης που απαιτείται για τη λειτουργία και τη διαμόρφωση τέτοιων συσκευών. Οι ερευνητές και γενικότερα οι επαγγελματίες του χώρου της δικτύωσης συχνά περιορίζονται από τις δυνατότητες τέτοιων προϊόντων δρομολόγησης. Επιπλέον, η δρομολόγηση αυτών των προϊόντων όταν συνδυάζεται με τα υπάρχοντα πακέτα λογισμικού ανοιχτού κώδικα συνήθως διέπεται από πρόσθετους περιορισμούς όπως ο αριθμός των ξεχωριστών συσκευών που μπορούν να υποστηριχθούν.

Σε περίπτωση που κάποιοι μηχανικοί δικτύων θα ενδιαφερόντουσαν να συλλέξουν διάφορες πληροφορίες σχετικά με τη συμπεριφορά αυτών των συσκευών δρομολόγησης, να τις επεξεργαστούν και να τις καταστήσουν διαθέσιμες στην κοινότητα θα απαιτούνταν πρόσθετες δυνατότητες αποθήκευσης και δέσμης ενεργειών (scripting capabilities). Τέτοιοι όμως πόροι δεν είναι διαθέσιμοι στις υπάρχουσες συσκευές δρομολόγησης. Κάποιοι άλλοι ερευνητές θα μπορούσαν π.χ. να ενδιαφερθούν για την ανάπτυξη νέων πρωτοκόλλων δρομολόγησης επεκτείνοντας κάποια από τα ήδη υπάρχοντα πρωτόκολλα, χωρίς να χρειαστεί να προβούν σε μια πλήρη υλοποίηση αυτών ξεκινώντας από την αρχή, δηλαδή από μηδενική βάση.

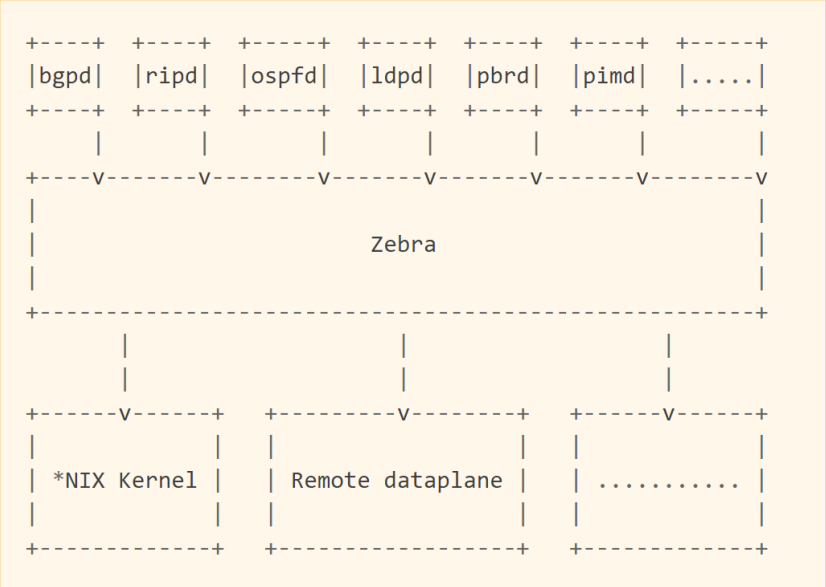
Η σουίτα FRR είναι ένα πακέτο λογισμικού Unix/Linux που υλοποιεί και υποστηρίζει τη δρομολόγηση δικτύων και βασίζεται πάνω σε γνωστά πρωτόκολλα δρομολόγησης, όπως το Routing Information Protocol (RIP), το Open Shortest Path First (OSPF) και το Border Gateway Protocol (BGP). Η εν λόγω σουίτα περιλαμβάνει επίσης μια διαδικασία διαχείρισης των πληροφοριών δρομολόγησης που λειτουργεί ως ενδιάμεση μεταξύ των διαφόρων πρωτοκόλλων δρομολόγησης και των ενεργών διαδρομών που έχουν εγκατασταθεί στον πυρήνα ενός δρομολογητή. Για το σκοπό αυτό έχει αναπτυχθεί μια βιβλιοθήκη (library) που παρέχει υποστήριξη στη διαμόρφωση (configuration) ενός δρομολογητή, καθώς και μια διαδραστική διεπαφή γραμμής εντολών (command-line interface). Τα πρωτόκολλα δρομολόγησης που υποστηρίζονται από τη σουίτα FRR, μπορούν να επεκταθούν επιτρέποντας την ανάπτυξη νέων σεναρίων πειραματισμού, καταγραφής ή προσαρμοσμένης επεξεργασίας. Επιπλέον, οι βιβλιοθήκες και ο δαίμονας πυρήνα (kernel daemon) παρέχουν ένα πλαίσιο για τη διευκόλυνση της ανάπτυξης νέων δαιμόνων για την

υλοποίηση νέων πρωτοκόλλων δρομολόγησης. Τέλος, με το συνδυασμό άλλων πακέτων λογισμικού μπορεί να επιτευχθεί ένα ευρύ φάσμα λειτουργιών που μπορεί να ενσωματωθεί σε μια ενιαία συσκευή παρέχοντας έτσι τη δυνατότητα καινοτόμων λύσεων σε προβλήματα δικτύωσης.

Το FRR διανέμεται υπό τη Γενική Δημόσια Άδεια (General Public License v2.0 ή GPLv2). Η κοινότητα των χειριστών (operators), πωλητών (vendors), μη κερδοσκοπικών οργανισμών και ερευνητών συμβάλουν στην προβολή της σουίτας FRR ώστε αυτή να καταστεί πιο δημοφιλής και προβαίνουν σε ευρύτερες δοκιμές προτεινόμενων τροποποιήσεων των υπαρχόντων πρωτοκόλλων δρομολόγησης ή ακόμη και την ανάπτυξη νέων πρωτοκόλλων δρομολόγησης.

2.2 Αρχιτεκτονική Σουίτας FRR

Η σουίτα frr ακολουθεί έναν διαφορετικό τρόπο προσέγγισης σε σύγκριση με το παραδοσιακό λογισμικό των συσκευών δρομολόγησης το οποίο αποτελείται από ένα ενιαίο πρόγραμμα διεργασίας που παρέχει όλες τις λειτουργίες των πρωτοκόλλων δρομολόγησης. Η πλατφόρμα frr αποτελείται από μια σουίτα δαιμόνων που συνεργάζονται μεταξύ τους με σκοπό να δημιουργήσουν έναν πίνακα δρομολόγησης. Κάθε πρωτόκολλο δρομολόγησης υλοποιείται από ξεχωριστό δαίμονα (π.χ. το πρωτόκολλο BGP υλοποιείται από το δαίμονα bgpd). Οι δαίμονες των πρωτοκόλλων δρομολόγησης ανταλλάσσουν πληροφορίες μέσω ενός άλλου δαίμονα που ονομάζεται zebra, ο οποίος είναι υπεύθυνος για τη συμπερίληψη των αποφάσεων δρομολόγησης και τη διαχείριση του επιπέδου δεδομένων.

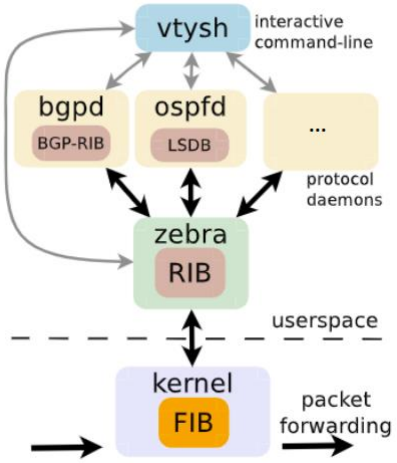


Εικόνα 3: Αρχιτεκτονική FRR

Δεδομένου ότι όλα τα πρωτόκολλα εκτελούνται ανεξάρτητα, αυτή η αρχιτεκτονική παρέχει υψηλή ανθεκτικότητα, που σημαίνει ότι ένα σφάλμα ή μια ολοσχερής αποτυχία σε έναν δαίμονα πρωτοκόλλου γενικά δεν θα επηρεάσει τα άλλα πρωτόκολλα. Η ανωτέρω αρχιτεκτονική είναι επίσης ευέλικτη και επεκτάσιμη, καθώς η αρθρωτότητά της (modularity) καθιστά εύκολη την ανάπτυξη νέων πρωτοκόλλων και την προσάρτησή τους στη σουίτα frr [2]. Επιπλέον, κάθε δαίμονας υλοποιεί ένα σύστημα πρόσθετων (plugin system) που επιτρέπει τη φόρτωση νέων λειτουργιών κατά το χρόνο εκτέλεσής του.

Στο διάγραμμα που ακολουθεί παρουσιάζεται η αρχιτεκτονική της σουίτας quagga πάνω στην οποία στηρίχτηκε και αναπτύχθηκε η σουίτα frr. Η εν λόγω αρχιτεκτονική αποτελείται από ένα σύνολο διεργασιών που επικοινωνούν μεταξύ τους μέσω του πρωτοκόλλου Inter Procces Communication (IPC),

το οποίο στην ουσία αποτελεί έναν μηχανισμό που παρέχεται από το λειτουργικό σύστημα για τη διαχείριση κοινών δεδομένων μεταξύ διαφορετικών διεργασιών. Τα πρωτόκολλα δρομολόγησης όπως τα BGP, OSPF κλπ. υλοποιούνται από τις αντίστοιχες διεργασίες που είναι οι δαίμονες bgpd, ospfd κλπ. Ένας άλλος δαίμονας, που ονομάζεται zebra, δρα ως ενδιάμεσος μεταξύ του επιπέδου προώθησης του πυρήνα και των διεργασιών των πρωτοκόλλων δρομολόγησης. Επιπλέον, ένα διαδραστικό εργαλείο γραμμής εντολών που ονομάζεται vtysh επιτρέπει την παρακολούθηση και τη διαμόρφωση αυτών των διεργασιών. Το εργαλείο γραμμής εντολών vtysh επικοινωνεί με τις διεργασίες μέσω ενός απλού πρωτοκόλλου μετάδοσης συμβολοσειρών, όπου οι συμβολοσειρές είναι ουσιαστικά πανομοιότυπες με τις εντολές που εισάγονται.



Εικόνα 4: Αρχιτεκτονική Quagga

Ο δαίμονας zebra αποτελεί αναπόσπαστο μέρος της αρχιτεκτονικής. Ο βασικός ρόλος του δαίμονα zebra είναι να διατηρεί ένα αντίγραφο ασφαλείας της κατάστασης προώθησης πακέτων, όπως οι διεπαφές δικτύου (network interfaces), καθώς και του πίνακα με τις τρέχουσες ενεργές διαδρομές (active routes). Οι τρέχουσες ενεργές διαδρομές αναφέρονται επίσης και ως Βάση Πληροφοριών Προώθησης (Forwarding Information Base FIB) [3]. Επιπλέον, η διεργασία zebra συλλέγει πληροφορίες δρομολόγησης από τις διεργασίες των πρωτοκόλλων δρομολόγησης και τις αποθηκεύει στη δική της Βάση Πληροφοριών Δρομολόγησης (Routing Information Base RIB) [3] μαζί με τις στατικές διαδρομές που έχουν διευθετηθεί. Στη συνέχεια, η διαδικασία zebra είναι υπεύθυνη για την επιλογή της βέλτιστης διαδρομής από όλες τις διαθέσιμες για έναν προορισμό διαδρομές και την ενημέρωση του Forwarding Information Base (FIB) [4]. Οι πληροφορίες που αφορούν τις τρέχουσες βέλτιστες διαδρομές μπορούν να διανεμηθούν και στους δαίμονες των πρωτοκόλλων. Τέλος, η διαδικασία zebra ενημερώνει τους δαίμονες δρομολόγησης, εάν συμβεί οποιαδήποτε αλλαγή στην κατάσταση της διεπαφής δικτύου (network interface state).

2.3 Εγκατάσταση και Διευθέτηση Σουίτας FRR

Για να εγκαταστήσουμε την σουίτα frr εκτελούμε τις ακόλουθες εντολές:

```
$ sudo apt update
$ sudo apt upgrade
$ sudo apt install frr
```

Μετά την εγκατάσταση της πλατφόρμας frr θα διαπιστώσουμε ότι αυτή δεν ξεκινά αυτόματα (by default) τη λειτουργία της. Οπότε, πριν κάποιος προσπαθήσει να τρέξει την σουίτα frr θα πρέπει πρώτα να είναι σίγουρος ότι έχουν ενεργοποιηθεί όλοι οι απαραίτητοι δαίμονες που σκοπεύει να χρησιμοποιήσει (π.χ. ospfd και bgpd). Ο μοναδικός δαίμονας που ενεργοποιείται αυτόματα μετά την εγκατάσταση της σουίτας frr είναι ο δαίμονας zebra. Συνεπώς, όσοι από τους δαίμονες των πρωτοκόλλων δρομολόγησης σας είναι απαραίτητοι για την υλοποίηση του σχεδίου δρομολόγησης που έχετε εκπονήσει θα πρέπει να ενεργοποιηθούν από εσάς. Αυτό επιτυγχάνεται με την επεξεργασία (edit) του αρχείου /etc/frr/daemons, θέτοντας την τιμή yes στους δαίμονες που επιθυμείτε να ενεργοποιήσετε.

```
...
bgpd=yes
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
fabricd=no
pimd=no
ldpd=no
nhrpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
vrrpd=no
...
```

Στη συνέχεια αφού έχουμε ενεργοποιήσει τους απαραίτητους δαίμονες ξεκινούμε την υπηρεσία frr ως εξής:

```
$ sudo systemctl enable frr
$ sudo systemctl start frr
```

Με την πρώτη εντολή "systemctl enable frr" ενεργοποιούμε την υπηρεσία frr, ώστε αυτή να εκτελείται αυτόματα κάθε φορά που η συσκευή ξεκινά τη λειτουργίας της, ενώ με τη δεύτερη εντολή "systemctl start frr" ξεκινούμε την υπηρεσία frr μιας και η συσκευή έχει ήδη ξεκινήσει τη λειτουργία της, ώστε να αποφύγουμε την επανεκκίνησή της (reboot). Προφανώς, την επόμενη φορά που θα ξεκινήσει τη λειτουργία της η συσκευή δεν απαιτείται η εκτέλεση των ανωτέρω εντολών. Δεδομένου ότι η λειτουργία των δαιμόνων των πρωτοκόλλων δρομολόγησης (π.χ. bgpd, ospfd, ospf6d, ripd) εξαρτώνται από τη λειτουργία του δαίμονα zebra όταν ξεκινάει η υπηρεσία frr εάν ο δαίμονας zebra για κάποιο λόγο δεν τρέχει, πρώτα ξεκινάει τη λειτουργία του δαίμονα zebra και κατόπιν η λειτουργία των δαιμόνων των πρωτοκόλλων δρομολόγησης που έχουν ενεργοποιηθεί. Ο έλεγχος αυτός επιτυγχάνεται με την εντολή "systemd". Γενικότερα, όταν μια υπηρεσία επανεκκινείται όλες οι εξαρτώμενες με αυτήν υπηρεσίες επανεκκινούνται και αυτές. Συνεπώς, όταν εκτελούμε την εντολή "systemctl restart frr" επανεκκινούνται όλοι οι δαίμονες των πρωτοκόλλων δρομολόγησης που έχουν ενεργοποιηθεί.

Ο προτεινόμενος τρόπος λειτουργίας (by default) της σουίτας frr είναι να αποθηκεύει στο ενιαίο αρχείο διευθέτησης (integrated configuration) με όνομα frr.conf όλες τις διευθετήσεις των δαιμόνων των πρωτοκόλλων δρομολόγησης μαζί με αυτήν του δαίμονα zebra. Αν παρόλα αυτά κάποιος επιθυμεί να απενεργοποιήσει την ανωτέρω λειτουργία πρέπει πρώτα να συνδεθεί στη γραμμή εντολών της σουίτας frr εκτελώντας την εντολή "sudo vtysh" (το περιβάλλον της γραμμής εντολών της εν λόγω πλατφόρμας είναι παρόμοιο με εκείνο της Cisco και πολλές από τις εντολές είναι πανομοιότυπες με αυτές του Cisco IOS) και στη συνέχεια να απενεργοποιήσει αυτήν την υπηρεσία ως εξής:

```
$ sudo vtysh
# configure terminal
  (config)# no service integrated-vtysh-config
```

Σε αυτή την περίπτωση αποθηκεύονται οι διευθετήσεις (configurations) του κάθε δαίμονα σε ξεχωριστά αρχεία.

```
# write memory
Building Configuration...
Configuration saved to /etc/frr/zebra.conf
Configuration saved to /etc/frr/bgpd.conf
Configuration saved to /etc/frr/ospfd.conf
[OK]
#
```

Εδώ αξίζει να αναφέρουμε ότι για να ξεκινήσει τη λειτουργία του ένας συγκεκριμένος δαίμονας εκτός του ότι θα πρέπει να έχει ενεργοποιηθεί θα πρέπει να υφίσταται και το αντίστοιχο αρχείο διευθέτησης έστω και αν αυτό είναι άδειο.

Αν πάλι κάποιος επιθυμεί να ενεργοποιήσει ξανά αυτή την υπηρεσία με σκοπό την αποθήκευση των διευθετήσεων (configurations) όλων των δαιμόνων σε ένα ενιαίο αρχείο διευθέτησης (integrated configuration) απλά εκτελεί την ακόλουθη εντολή από τη γραμμή εντολών της σουίτας frr.

```
$ sudo vtysh
# configure terminal
  (config)# service integrated-vtysh-config
```

Σε αυτή την περίπτωση οι διευθετήσεις (configurations) όλων των δαιμόνων αποθηκεύονται σε ένα ενιαίο αρχείο.

```
# write memory
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
#
```

Τέλος, εάν κάποιος επιθυμεί να επαναφέρει την προτεινόμενη διευθέτηση (restore default configuration) θα πρέπει πρώτα να διαγράψει το αρχείο frr.conf και στη συνέχεια να επανεκκινήσει την υπηρεσία frr. Καλό βέβαια θα ήταν πριν κάποιος διαγράψει το αρχείο frr.conf να κρατήσει ένα αντίγραφο (backup) αυτού του αρχείου. Τα βήματα που πρέπει να ακολουθήσει σε αυτήν την περίπτωση είναι τα εξής:

- Επιβεβαίωση ότι η υπηρεσία service integrated-vtysh-config είναι ενεργοποιημένη. Σε περίπτωση όμως που αυτή η υπηρεσία είναι απενεργοποιημένη την ενεργοποιούμε από τη γραμμή εντολών της σουίτας frr με τον τρόπο που έχουμε δείξει προηγουμένως.
- Διαγραφή του αρχείου /etc/frr/frr.conf (προαιρετικά κρατάμε αντίγραφο).
- Επανεκκίνηση της σουίτας frr.

```
$ net show configuration | grep integrated
service integrated-vtysh-config
$ sudo rm /etc/frr/frr.conf
$ sudo systemctl restart frr
```

3

Πρωτόκολλο OSPF

Το OSPF (Open Shortest Path First) είναι ένα ιεραρχικό link-state πρωτόκολλο το οποίο χρησιμοποιείται για τη δρομολόγηση μέσα στα όρια ενός Αυτόνομου Συστήματος (AS).

Τα link state πρωτόκολλα υποχρεώνουν τους δρομολογητές να ενημερώνονται σχετικά με την κατάσταση των διεπαφών (interfaces), είτε μέρους, είτε του συνόλου των δρομολογητών του AS που ανήκουν και να ενημερώνουν τους άλλους δρομολογητές για την δική τους κατάσταση.

Με αυτόν τον τρόπο κάθε δρομολογητής του AS μαθαίνει πώς συνδέονται οι υπόλοιποι δρομολογητές μεταξύ τους, και στη συνέχεια συνθέτοντας τις επιμέρους αυτές πληροφορίες αποκτά ολοκληρωμένη γνώση της τοπολογίας του δικτύου και έτσι είναι σε θέση να δρομολογεί τα εισερχόμενα πακέτα προς τους προορισμούς μέσω των κατάλληλων διαδρομών.

Σε αντίθεση με παλαιότερα distance-vector πρωτόκολλα, όπως το RIP, όπου η δρομολόγηση γίνεται λαμβάνοντας υπόψιν μόνο το πόσους ενδιάμεσους σταθμούς πρέπει να ταξιδέψει ένα πακέτο μέχρι να φτάσει στον προορισμό του, το OSPF πρωτόκολλο αναπτύχθηκε με τη λογική ότι η συντομότερη διαδρομή θα πρέπει να υπολογίζεται όχι μόνο με βάση τον αριθμό των ενδιάμεσων σταθμών, αλλά λαμβάνοντας υπόψιν και άλλες παραμέτρους όπως το εύρος ζώνης (bandwidth) των ζεύξεων, την καθυστέρηση μετάδοσης (delay) των πακέτων, καθώς επίσης και τον φόρτο (load) κάθε ενδιάμεσου σταθμού.

Ο κάθε κόμβος αφού ανακαλύψει όλους τους γειτονικούς του κόμβους υπολογίζει για καθένα τους το κόστος μετάβασης ή αλλιώς το metric της σύνδεσης. Το metric των επιμέρους συνδέσεων μέχρι να φτάσουμε στον προορισμό μας δίνει το τελικό κόστος δρομολόγησης και επιλέγεται από το πρωτόκολλο η διαδρομή η οποία έχει το μικρότερο τελικό (αθροιστικό) κόστος. Η παραπάνω πληροφορία αποθηκεύεται σε Link State Advertisement (LSA) πακέτα τα οποία αποστέλλονται σε όλους τους κόμβους με πλημμύρα (flooding) έως ότου γίνει γνωστή σε όλους η πλήρης τοπολογία του δικτύου.

Για τον υπολογισμό του Δέντρου Ελάχιστης Διαδρομής SPT (Shortest Path Tree) εφαρμόζεται ο αλγόριθμος του Dijkstra, επίσης γνωστός και ως αλγόριθμος του συντομότερου μονοπατιού.

Για την επίτευξη της μέγιστης δυνατής ευελιξίας, το OSPF πρωτόκολλο δίνει τη δυνατότητα στους διαχειριστές να περιγράφουν μια εικονική τοπολογία δικτύου. Για παράδειγμα, ένας διαχειριστής μπορεί να διευθετήσει έναν εικονικό σύνδεσμο μεταξύ δύο δρομολογητών στο γράφημα της δρομολόγησης,

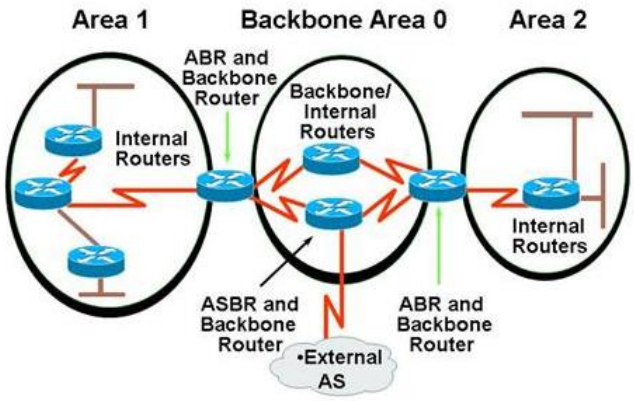
ακόμα και αν η φυσική σύνδεση μεταξύ των δύο δρομολογητών απαιτεί επικοινωνία μέσω ενός μεταβατικού δικτύου.

Το OSPF πρωτόκολλο δίνει τη δυνατότητα στους δρομολογητές να ανταλλάσσουν πληροφορίες δρομολόγησης που προέρχονται από άλλες (εξωτερικές) τοποθεσίες. Κατά βάση, ένας ή περισσότεροι δρομολογητές που είναι συνδεδεμένοι με άλλες τοποθεσίες λαμβάνουν πληροφορίες για αυτές τις τοποθεσίες και τις συμπεριλαμβάνουν στα μηνύματα ενημέρωσης που ίδιοι αποστέλλουν. Η μορφή του μηνύματος είναι διαφορετική όταν μεταφέρει πληροφορίες που προέρχονται από εξωτερικές πηγές και όταν μεταφέρει πληροφορίες που προέρχονται από εσωτερικούς δρομολογητές, με αποτέλεσμα να μην υπάρχει καμία ασάφεια όσον αφορά την προέλευση ή την αξιοπιστία των δρομολογήσεων.

3.1 Τύποι OSPF Δρομολογητών

Το OSPF [7] είναι ιεραρχικό πρωτόκολλο και χωρίζει το δίκτυο σε περιοχές (area 0, area 1, area 2 κλπ.), όπου η κάθε μια από αυτές αναγνωρίζεται από ένα μοναδικό id. Η area 0 αποτελεί την κύρια περιοχή του δικτύου στην οποία πρέπει να έχουν πρόσβαση όλες οι υπόλοιπες περιοχές. Κάθε δρομολογητής είναι σχεδιασμένος έτσι ώστε να γνωρίζει όλους τους άλλους δρομολογητές που ανήκουν στην περιοχή του. Πέραν όμως της ανταλλαγής μηνυμάτων και πληροφοριών μέσα σε μία συγκεκριμένη περιοχή το OSPF πρωτόκολλο επιτρέπει την επικοινωνία και μεταξύ γειτονικών περιοχών. Έτσι, ένας συνοριακός δρομολογητής που συνδέει δύο διαφορετικές περιοχές μπορεί να συνοψίζει τις πληροφορίες δρομολόγησης κάθε περιοχής και να τις ανακοινώνει στους άλλους δρομολογητές.

Οι OSPF δρομολογητές ανάλογα με το έργο που καλούνται να υλοποιήσουν και το ρόλο που επιτελούν μέσα στο Αυτόνομο Σύστημα (AS) που ανήκουν χωρίζονται στις παρακάτω κατηγορίες:



Εικόνα 5: Τύποι OSPF Δρομολογητών

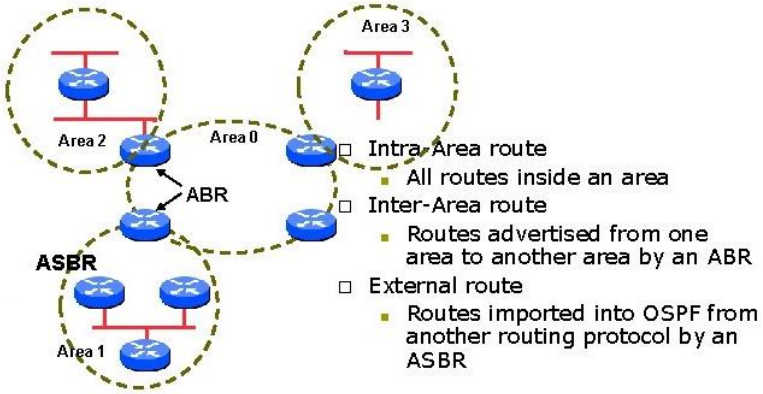
Internal Routers: Είναι οι δρομολογητές των οποίων όλες οι διεπαφές (interfaces) είναι συνδεμένες εντός μιας συγκεκριμένης περιοχής (area).

Backbone Routers: Είναι οι δρομολογητές οι οποίοι έχουν τουλάχιστον μία από τις διεπαφές τους συνδεδεμένη με την Backbone Area (area 0) και ως εκ τούτου υλοποιούν τη δρομολόγηση του δικτύου κορμού.

Area Boarder Routers (ABRs): Είναι οι δρομολογητές που ανήκουν σε δύο ή και περισσότερες περιοχές μια εκ των οποίον είναι η area 0. Οι δρομολογητές αυτοί αναλαμβάνουν να συνοψίσουν τις διαδρομές των δικτύων των περιοχών στις οποίες ανήκουν και να τις ανακοινώσουν στους άλλους ABRs (Area Boarder Routers).

Autonomous System Boundary Routers (ASBRs): Είναι οι δρομολογητές που έχουν τουλάχιστον μια διεπαφή τους συνδεδεμένη με ένα άλλο Αυτόνομο Σύστημα (AS) και μέσω αυτών των δρομολογητών επικοινωνούν τα διάφορα Αυτόνομα Συστήματα μεταξύ τους. Ένας ASBR μπορεί να εισάγει και να εξάγει πληροφορίες δρομολόγησης από άλλα Αυτόνομα Συστήματα (ASs) τα οποία δεν χρησιμοποιούν απαραίτητα το OSPF πρωτόκολλο. Αυτό επιτυγχάνεται γιατί ο ASBR μεταφράζει τις πληροφορίες δρομολόγησης σε μορφή που να μπορεί να επεξεργαστεί από τους εσωτερικούς δρομολογητές του Αυτόνομου Συστήματος (AS).

3.2 Κατηγορίες OSPF Δρομολόγησης



Εικόνα 6: Κατηγορίες OSPF Δρομολόγησης

Intra-area: Αυτός ο τύπος δρομολόγησης εκτελείται μεταξύ των εσωτερικών δρομολογητών μιας συγκεκριμένης περιοχής.

Inter-area: Αυτός ο τύπος δρομολόγησης εκτελείται μεταξύ δρομολογητών που ανήκουν σε διαφορετικές περιοχές. Προφανώς, η ανταλλαγή δεδομένων μεταξύ διαφορετικών περιοχών πραγματοποιείται πάντα μέσω του δικτύου κορμού (area 0).

External route: Αφορά διαδρομές που προέρχονται από άλλα Αυτόνομα Συστήματα (ASs) .

Υπάρχουν δύο τύποι external routes οι οποίοι διαφέρουν στον τρόπο υπολογισμού του κόστος τους (metric). Αρχικά, τα external routes όταν εισάγονται (redistributed) στο OSPF αποκτούν metric συμβατό με τα metrics του OSPF πρωτοκόλλου .

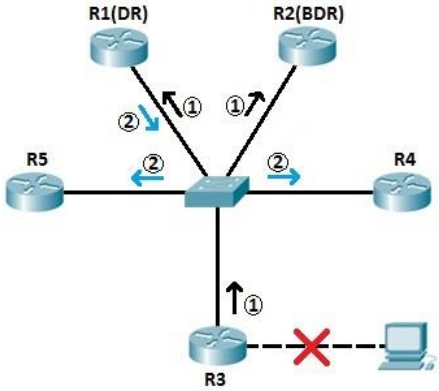
- **E1 external routes (type 1):** Αυτές οι διαδρομές όταν εισέλθουν στο OSPF πρωτόκολλο το κόστος τους συνεχίζει να αυξάνεται κανονικά προσθέτοντας τα επιμέρους κόστη των εσωτερικών διαδρομών. Οι ανωτέρω διαδρομές έχουν την ένδειξη E1 στους routing tables των OSPF δρομολογητών.

- **E2 external routes (type 2):** Αυτές τις διαδρομές όταν εισέλθουν στο OSPF και αποκτήσουν κάποιο κόστος αυτό δε μεταβάλλεται καθόλου. Οι ανωτέρω διαδρομές έχουν την ένδειξη E2 στους routing tables των OSPF δρομολογητών.

3.3 Τύποι OSPF Πακέτων

Το OSPF πρωτόκολλο υποχρεώνει τους δρομολογητές να αποστέλλουν πακέτα ώστε να εντοπίζουν τους γείτονές τους, εγκαθιδρύοντας έτσι γειτονικές σχέσεις (adjacencies). Το OSPF πρωτόκολλο υποστηρίζει τα παρακάτω είδη πακέτων:

Hello Packets (type 1): Στέλνονται ανά τακτά χρονικά διαστήματα για την αναζήτηση γειτόνων και χρησιμοποιούνται από τους δρομολογητές για να διατηρούν ενημερωμένη την κατάσταση γειτνίασή τους με τους άλλους OSPF δρομολογητές.

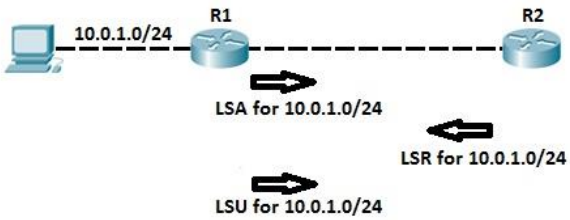


Εικόνα 7: DR και BDR

Ο Designated Router (DR) και ο Backup Designated Router (BDR) είναι δρομολογητές οι οποίοι εκλέγονται από το δίκτυο με σκοπό να μειώνουν την κίνηση του δικτύου. Ο DR είναι υπεύθυνος να λαμβάνει την πληροφορία δρομολόγησης από όλους τους δρομολογητές σε μια συγκεκριμένη περιοχή (area) και να την διανέμει ο ίδιος μέσω πολυεκπομπής (multicast) στους υπόλοιπους. Σε περίπτωση που ο DR βγει εκτός λειτουργίας το ρόλο αυτόν αναλαμβάνει ο BDR. Με αυτό τον τρόπο δεν χρειάζεται να ενημερώνουν όλοι οι δρομολογητές ο ένας τον άλλο συνεχώς, και μπορούν να παίρνουν τις ενημερώσεις τους από μια πηγή. Ο DR και ο BDR δημιουργούν γειτονικές σχέσεις (adjacencies) με όλους τους δρομολογητές μιας συγκεκριμένης περιοχής (area) για να μπορούν έτσι να ανταλλάξουν πληροφορίες δρομολόγησης. Ως DR εκλέγεται ο δρομολογητής με τη μεγαλύτερη προτεραιότητα (router priority) και σε περίπτωση που έχουν όλοι το ίδιο router priority επιλέγεται αυτός με το μεγαλύτερο router ID.

Database Description Packet (DDP) (type 2): Χρησιμοποιούνται μετά τη γειτνίαση των δρομολογητών και παρέχουν πληροφορίες για το περιεχόμενο της topology database, δηλαδή για πληροφορίες για το περιεχόμενο των διαδρομών που γνωρίζει ο δρομολογητής αποστολέας. Στη συνέχεια αυτές οι πληροφορίες λαμβάνονται και ελέγχονται από τους δρομολογητές λήψης έτσι ώστε να εξασφαλιστεί η διατήρηση της ίδιας τοπολογίας στους δρομολογητές μιας περιοχής.

Link State Request (LSR) (type 3): Χρησιμοποιούνται για την αίτηση των πιο ενημερωμένων Link State Advertisements (LSAs) από άλλους δρομολογητές. Σε περίπτωση που κάποιος δρομολογητής ανακαλύψει ότι η δική του topology database δεν έχει τις τελευταίες πιο ενημερωμένες διαδρομές στέλνει ένα LSR πακέτο ζητώντας να του σταλούν τα LSAs που του λείπουν.

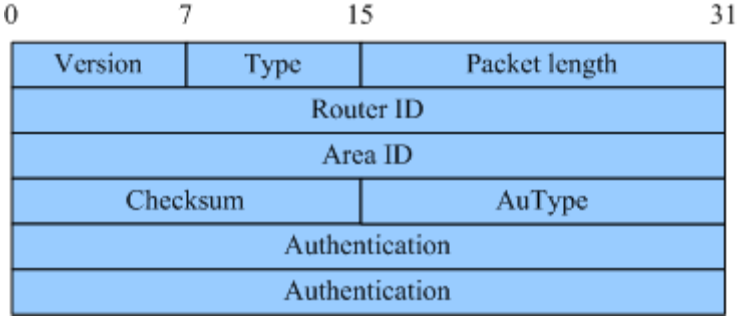


Εικόνα 8: Ανταλλαγή OSPF πακέτων

Link State Update (LSU) (type 4): Τα πακέτα LSU αποστέλλονται ως απάντηση στο αίτημα του LSR πακέτου και χρησιμοποιούνται για την γνωστοποίηση καινούργιων πληροφοριών και περιλαμβάνουν τα ζητούμενα LSAs.

Link State Acknowledgement (LSAck) (type 5): Πρόκειται για επιβεβαιώσεις (acknowledgements) ότι η παραλαβή των παραπάνω LSUs ήταν επιτυχής. Δηλαδή, όταν ένας δρομολογητής παραλαμβάνει ένα πακέτο LSU αποστέλλει ένα πακέτο LSAck για να επικυρώσει ότι πράγματι τα πακέτο αυτό ελήφθη επιτυχώς.

Τα ανωτέρω OSPF πακέτα ενθυλακώνονται (encapsulated) κατευθείαν μέσα στο IP πακέτο. Τα πεδία της επικεφαλίδας ενός OSPF πακέτου είναι τα εξής:



Εικόνα 9: OSPF header

- **Version number** (8 bits): δηλώνει την έκδοση του OSPF, Version 2 για IPv4 και Version 3 για IPv6
- **Type** (8 bits): υποδεικνύει τον τύπο του OSPF πακέτου ακολουθεί (1=Hello, 2=DBD, 3=LSR, 4=LSU, 5=LSack).
- **Packet Length** (16 bits): δηλώνει το μέγεθος του OSPF πακέτου μαζί με την επικεφαλίδα σε bytes.
- **Router ID** (32 bits): δηλώνει τον αριθμό του δρομολογητή (προσδιορίζοντάς τον μοναδικά) που δημιούργησε το OSPF πακέτο.
- **Area ID** (32 bits): δηλώνει τον αριθμό της OSPF περιοχή (προσδιορίζοντάς την μοναδικά) από την οποία προήλθε το OSPF πακέτο.
- **Checksum** (16 bits): χρησιμοποιείται για τον εντοπισμό ενδεχόμενων σφαλμάτων που προέκυψαν κατά την εκπομπή του OSPF πακέτου. Αν ο παραλήπτης διαπιστώσει αλλοιώσεις στη μετάδοσή του τότε το πακέτο απορρίπτεται.
- **Authentication Type** (16 bits): περιγράφει την μέθοδο της επιβεβαίωσης των πακέτων (0=δεν υπάρχει επιβεβαίωση, 1=απλή επιβεβαίωση, 2=MD5 επιβεβαίωση).
- **Authentication** (64 bits): περιέχει πληροφορίες που επιβεβαιώνουν την αξιοπιστία του πακέτου.

3.4 Καταστάσεις OSPF Γειτνίασης

Το OSPF [7] πρωτόκολλο δημιουργεί γειτονικές σχέσεις (adjacencies) μεταξύ επιλεγμένων δρομολογητών, οι εμπλεκόμενοι αυτοί δρομολογητές ονομάζονται adjacents και είναι οι μόνοι δρομολογητές που μπορούν να ανταλλάξουν μεταξύ τους πληροφορίες δρομολόγησης μέσα σε μία συγκεκριμένη περιοχή. Η διαδικασία γειτνίασης (adjacency) ολοκληρώνεται με την ανταλλαγή μιας σειράς OSPF πακέτων μεταξύ των δυο εμπλεκόμενων δρομολογητών και αφού περάσει πρώτα από τα ακόλουθα 8 στάδια (neighbor states):

Down: Είναι η πρώτη κατάσταση που βρίσκεται ένας γειτονικός δρομολογητής και σημαίνει ότι δεν έχει ανταλλαχθεί ακόμα καμία πληροφορία (hello packets) με το συγκεκριμένο δρομολογητή.

Attempt: Αφορά μόνο τα Non-Broadcast Multiple Access (NBMA) δίκτυα, πχ ATM, και σημαίνει ότι αν δεν έχει ληφθεί μέσα σε ένα συγκεκριμένο χρονικό περιθώριο κάποια πληροφορία από κάποιο γείτονα, οπότε θα πρέπει να γίνει προσπάθεια επικοινωνίας με αυτόν με αποστολή unicast hello πακέτων.

Init: Στην κατάσταση αυτή ο δρομολογητής έχει λάβει ένα hello packet από κάποιον γείτονα, αλλά παρόλα αυτά, δε μπορεί να υπάρξει επικοινωνία, γιατί αυτή ακόμα δεν έχει επιβεβαιωθεί.

2-Way: Η κατάσταση αυτή μας δείχνει ότι η επικοινωνία μεταξύ δύο γειτονικών δρομολογητών έχει εγκατασταθεί και προς τις δύο κατευθύνσεις (bi-directional). Σε περίπτωση όμως που οι δρομολογητές ανήκουν σε broadcast ή NBMA δίκτυα μεταφέρονται στην κατάσταση FULL, ώστε να γίνει η εκλογή Designated Router (DR) ή/και Backup Designated Router (BDR).

Exstart: Οι δρομολογητές DR και BDR εφαρμόζουν μια σχέση master-slave (κυρίου-σκλάβου) ώστε να πραγματοποιηθεί η ανταλλαγή των LSA της βάσης δεδομένων δρομολόγησης. Ο δρομολογητής με το μεγαλύτερο router id εκλέγεται ως master και στη συνέχεια οι δρομολογητές μεταπηδούν στην κατάσταση Exchange στην οποία ξεκινάει η ανταλλαγή πληροφορίας δρομολόγησης. Ο master ξεκινά πρώτος την ανταλλαγή, στέλνοντας στον slave αίτηση για πληροφορία δρομολόγησης.

Exchange: Σε αυτό το στάδιο οι OSPF δρομολογητές ανταλλάσσουν database descriptor (DBD) πακέτα με την link-state πληροφορία για να ενημερώσουν ο ένας τον άλλον. Περιγράφουν την link-state database ο ένας στον άλλο και συγκρίνουν την εισερχόμενη link-state database πληροφορία με αυτή που ήδη έχουν στην δική τους link-state database και αν διαπιστώσουν ότι τους λείπουν κάποιας εγγραφές, κάνουν αίτηση για να σταλεί από τον άλλο δρομολογητή πλήρης ενημέρωση.

Loading: Σε αυτό το στάδιο μπορεί να ζητηθεί από κάποιο δρομολογητή μια πιο ολοκληρωμένη πληροφόρηση με LSRs εάν αυτός λάβει ένα outdated (απαρχαιωμένο) LSA. Όταν ένας δρομολογητής λάβει ένα LSR θα απαντήσει με ένα μήνυμα LSU. Στη συνέχεια, το LSU είναι απαραίτητο να επικυρωθεί με την αποστολή ενός acknowledgement (LSAck).

Full: Αφού ολοκληρωθεί η κατάσταση Loading οι εμπλεκόμενοι δρομολογητές είναι πλέον fully adjacent και έχουν την ίδια topology database. Η κατάσταση full είναι η κατάσταση που τελικά πρέπει να βρίσκεται ένας OSPF δρομολογητής, με μοναδική εξαίρεση την κατάσταση 2-way σε ένα broadcast δίκτυο.

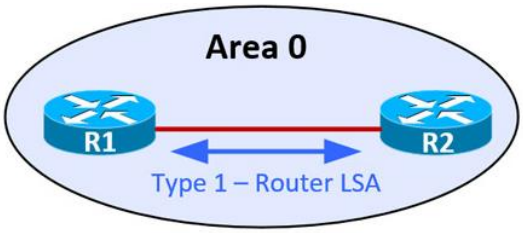
3.5 OSPF LSAs (Link State Advirtisements)

Το Link State Advertisement (LSA) αποτελεί ένα βασικό μέσο επικοινωνίας του πρωτοκόλλου OSPF για το Internet Protocol (IP) και περιέχει Link State (LS) πληροφορίες, καθώς και πληροφορίες δρομολόγησης που είναι κοινές στους OSPF δρομολογητές. Τα OSPF πακέτα διανέμουν τα LSAs με

σκοπό την ενημέρωση και τον συγχρονισμό των topology databases. Το OSPF πρωτόκολλο επιτρέπει στους δρομολογητές να δημιουργούν τους εξής 11 τύπους LSAs [5] που περιγράφονται παρακάτω :

3.5.1 Router LSAs (type 1)

Τα LSAs τύπου 1 δημιουργούνται από κάθε εσωτερικό δρομολογητή μιας περιοχής και διανέμονται με πλημμύρα (flooding) μόνο μέσα στα όρια της συγκεκριμένης περιοχής.

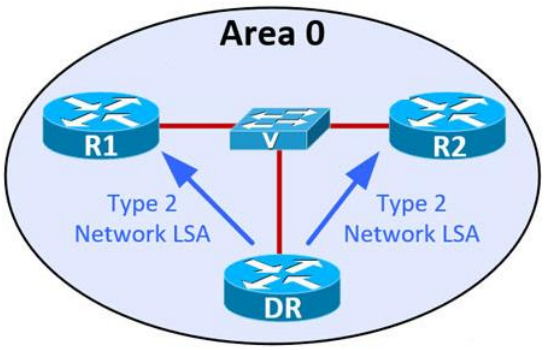


Εικόνα 10: Router LSA

Το LSA (τύπου 1) είναι ο πιο βασικός τύπος και δημιουργείται όταν συνδέεται ένας νέος δρομολογητής στο δίκτυο. Αυτός ο νέος δρομολογητής χρησιμοποιεί ένα LSA τύπου 1 για να ενημερώσει το δίκτυο ότι αποτελεί πλέον μέρος της αρχιτεκτονικής του. Για όλους τους τύπους LSA, υπάρχουν επικεφαλίδες LSA 20 byte. Ένα από τα πεδία της επικεφαλίδας LSA είναι το αναγνωριστικό κατάστασης σύνδεσης (link-state ID). Το ID LSA τύπου 1 είναι ίσο με το αναγνωριστικό του δρομολογητή .

3.5.2 Network LSAs (type 2)

Τα LSAs τύπου 2 δημιουργούνται από τους Designated Routers (DRs) και περιέχουν πληροφορίες για τους εσωτερικούς δρομολογητές της περιοχής που είναι συνδεδεμένοι σε αυτούς. Διανέμονται μόνο μέσα στα όρια της περιοχής που ανήκουν και περιγράφουν μόνο το συγκεκριμένο τμήμα δικτύου.

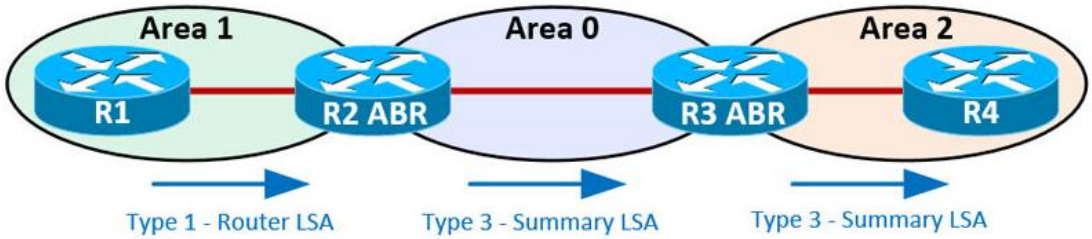


Εικόνα 11: Network LSA (DR Generated)

Οι DRs χρησιμοποιούνται για να ελαχιστοποιηθεί ο αριθμός των γειτνιάσεων και χρησιμεύουν ως κεντρικό σημείο για την ανταλλαγή πληροφοριών δρομολόγησης. Δημιουργούν Network LSAs τύπου 2 και ανακοινώνουν ποιοι δρομολογητές συνδέονται στο broadcast δίκτυο. Το αναγνωριστικό κατάστασης σύνδεσης ενός LSA τύπου 2 είναι η διεύθυνση διεπαφής IP του DR. Ο LSA τύπου 2 περιλαμβάνει τόσο τους δρομολογητές που συνδέονται στο broadcast δίκτυο όσο και το prefix του δικτύου μαζί με τη μάσκα του.

3.5.3 Network Summary LSAs (type 3)

Τα LSAs τύπου 3 δημιουργούνται από τους ABRs και διανέμονται με πλημμύρα (flooding) προς στους υπόλοιπους ABRs μέσω του δικτύου κορμού.

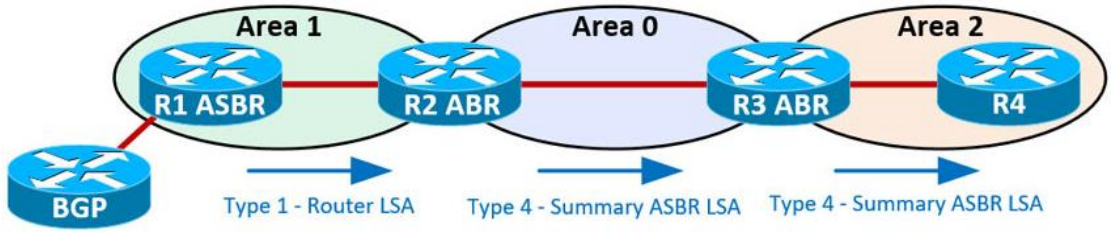


Εικόνα 12: Network Summary LSA (ABR Summary Route)

Ένας ABR λαμβάνει τις πληροφορίες δρομολόγησης από τις περιοχές στις οποίες διασυνδέεται και τις συνοψίζει πριν τις στείλει στις υπόλοιπες περιοχές. Η συνάθροιση των δικτύων μιας περιοχής δεν είναι προεπιλεγμένη διαδικασία, δηλαδή δε πραγματοποιείται αυτόματα από το OSPF πρωτόκολλο, αλλά από τον διαχειριστή του δικτύου. Το link-state ID της επικεφαλίδας LSA τύπου 3 ισούται με την IP διεύθυνση του δικτύου προορισμού.

3.5.4 AS Summary LSAs (type 4)

Τα LSAs τύπου 4 δημιουργούνται από τους ABRs των διάφορων περιοχών και περιγράφουν τις διαδρομές προς τους ASBRs, με σκοπό να γνωστοποιήσουν τον τρόπο εξόδου από το δικό τους Αυτόνομο Σύστημα (AS).

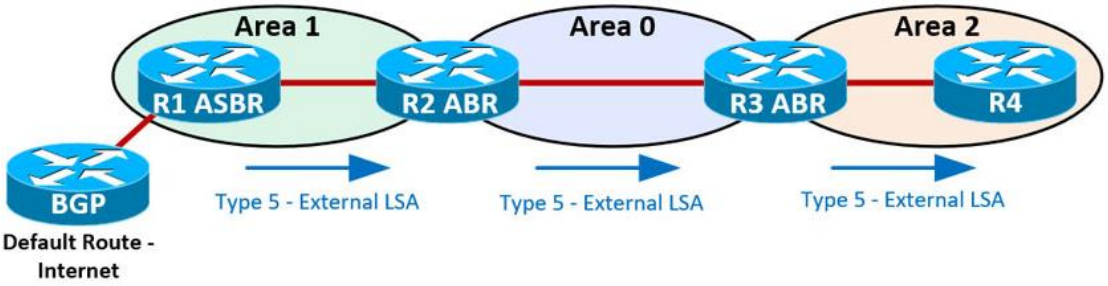


Εικόνα 13: AS Summary LSA (ASBR Location)

Το αναγνωριστικό κατάστασης σύνδεσης ενός LSA τύπου 4 ισούται με το router ID του ASBR.

3.5.5 AS External LSAs (type 5)

Τα LSAs τύπου 5 δημιουργούνται από τους ASBRs του Αυτόνομου Συστήματος (AS) και περιγράφουν τις εξωτερικές διαδρομές προς άλλα AS.



Εικόνα 14: AS External LSA (ASBR Summary Route)

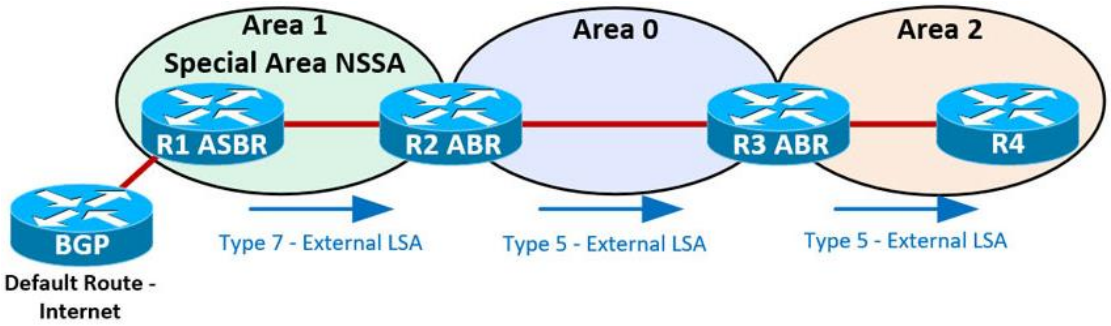
Τα LSAs τύπου 5 περιλαμβάνουν διαδρομές οι οποίες προέρχονται από εξωτερικά AS και διαδίδονται σε όλες τις περιοχές του δικτύου, εκτός από κάποιες ειδικές περιοχές που θα αναλύσουμε στην επόμενη ενότητα. Το αναγνωριστικό κατάστασης σύνδεσης ενός LSA τύπου 5 είναι ίσο με την διεύθυνση του εξωτερικού δικτύου.

3.5.6 Multicast LSAs (type 6)

Τα LSAs τύπου 6 χρησιμοποιούνται για multicast εφαρμογές.

3.5.7 NSSA LSAs (type 7)

Τα LSAs τύπου 7 είναι ειδικού σκοπού LSAs, δημιουργούνται από τους NSSA ASBRs και διανέμονται μέσα στις Not-So-Stubby Areas για να περιγράφουν διαδρομές από εξωτερικά δίκτυα.



Εικόνα 15: NSSA LSA

Θα πρέπει εδώ να σημειώσουμε ότι για να μπορέσουν να μεταδοθούν οι πληροφορίες δρομολόγησης που μεταφέρουν τα LSAs τύπου 7 και σε άλλες περιοχές θα πρέπει πρώτα να μετατραπούν σε AS External LSAs τύπου 5.

3.5.8 BGP LSAs (type 8)

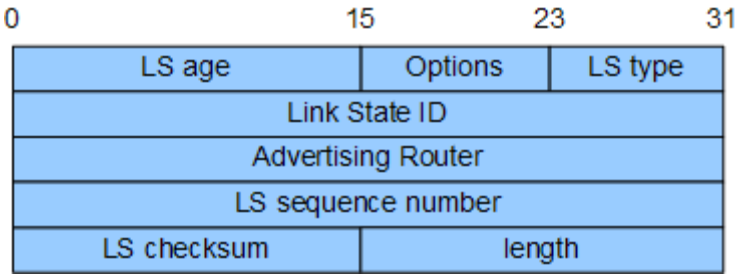
Τα LSAs τύπου 8 δημιουργήθηκαν αρχικά για τη μετάδοση των attributes των BGP διαδρομών μέσα από transit OSPFv2 AS. Σήμερα χρησιμοποιούνται από τη νεότερη έκδοση του πρωτοκόλλου OSPFv3 μόνο τοπικά σε κάθε link, χωρίς να ανακοινώνονται έξω από αυτό και περιέχουν πληροφορίες για τους άμεσα συνδεδεμένους δρομολογητές, καθώς επίσης και τα IPv6 δίκτυα που σχετίζονται με αυτό.

3.5.9 Opaque LSAs (type 9, 10, 11)

Τα LSAs τύπου 9, 10 και 11 είναι δεσμευμένα για μελλοντική χρήση για ειδικές εφαρμογές

3.5.10 LSA header

Τα ανωτέρω LSAs ενθυλακώνονται μέσα στο OSPF πακέτο. Τα πεδία της επικεφαλίδας (header) ενός LSA πακέτου είναι τα εξής:



Εικόνα 16: LSA header

- **LSA age** (16 bits): περιέχει την ηλικία ενός LSA πακέτου με αρχική τιμή τα 0 δευτερόλεπτα και τελική τα 1800 δευτερόλεπτα (30 λεπτά). Όταν η ηλικία ενός LSA φτάσει τα 1800 δευτερόλεπτα (30 λεπτά) τότε ο δρομολογητής που το δημιούργησε το διανέμει ξανά αρχικοποιώντας όμως την ηλικία του στα 0 δευτερόλεπτα και αυξάνοντας την τιμή του πεδίου sequence number της επικεφαλίδας του. Αν για κάποιο λόγο η παραπάνω διαδικασία αποτύχει να λάβει χώρα τότε η ηλικία του LSA πακέτου θα συνεχίσει να αυξάνεται μέχρι να φτάσει τη μέγιστη επιτρεπτή τιμή MaxAge=3.600 δευτερόλεπτα (60 λεπτά). Όταν ένα LSA πακέτο σε ένα δρομολογητή φτάσει τη MaxAge ηλικία τότε αυτό διαγράφεται από την topology database, ενώ ταυτόχρονα διανέμεται και στους υπόλοιπους δρομολογητές για να τους ειδοποιήσει ότι πρέπει και αυτοί να το διαγράψουν.

- **Options** (8 bits): η τιμή του αναφέρεται σε κάποιες ιδιαίτερες απαιτήσεις που μπορεί έχει η διανομή ενός LSA πακέτου (E: Type 5 LSAs are flooded, MC: IP multicast packets are forwarded, N/P: Type 7 LSAs are processed, DC: On-demand links are processed).

- **LSA type** (8 bits): περιέχει τον τύπο του LSA πακέτου (type 1, type 2 κτλ).

- **Link State ID** (32 bits): προσδιορίζει μοναδικά το LSA πακέτο ενός δρομολογητή.

- **Advertising router** (32 bits): περιέχει το Router id του δρομολογητή που δημιούργησε το LSA πακέτο.

- **LSA sequence number** (32 bits): είναι ένας αριθμός ακολουθίας με βάση τον οποίο οι γείτονες (neighbors) μπορούν να αναγνωρίζουν τη νεότερη (τελευταία) έκδοση ενός LSA πακέτου.

- **LSA checksum** (16 bits): χρησιμοποιείται για να εντοπίζει τυχόν αλλοιώσεις των LSA πακέτων.

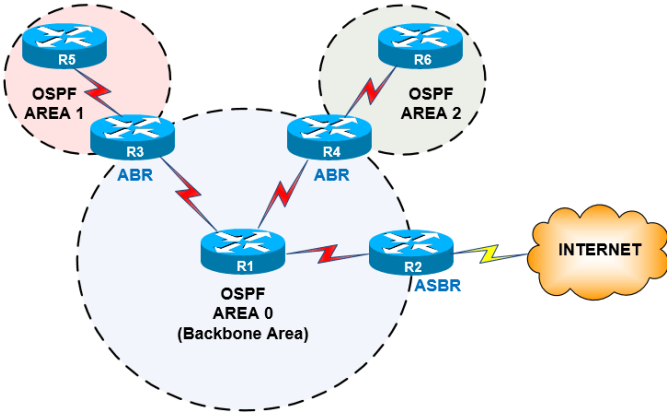
- **Length** (16 bits): περιέχει το μέγεθος (μήκος) του LSA πακέτου συμπεριλαμβανομένης της επικεφαλίδας του σε bytes. Το μέγιστο μήκος που μπορεί να λάβει το πακέτο ανέρχεται στα 65535 bytes, αλλά συνήθως δεν ξεπερνά τις μερικές εκατοντάδες bytes.

3.6 OSPF Περιοχές

Δεδομένου ότι το πρωτόκολλο OSPF είναι ιεραρχικό επιτρέπει σε έναν διαχειριστή να διαχωρίζει τους δρομολογητές και τα δίκτυα ενός Αυτόνομου Συστήματος (AS) σε πολλές περιοχές, δίνοντάς του έτσι τη δυνατότητα να μπορεί να χειρίζεται ευκολότερα μεγαλύτερο όγκο δρομολογητών σε σχέση με άλλα πρωτόκολλα Εσωτερικής Πύλης (IGP). Μια OSPF περιοχή ορίζει ένα σύνολο δρομολογητών που έχουν τα ίδια χαρακτηριστικά. Ας δούμε λοιπόν αναλυτικά όλους τους τύπους περιοχών του OSPF πρωτοκόλλου.

3.6.1 Backbone Area

Το δίκτυο κορμού (συνήθως area 0) αποτελεί την κύρια περιοχή του δικτύου ενός Αυτόνομου Συστήματος (AS) στην οποία πρέπει να έχουν πρόσβαση όλες οι υπόλοιπες περιοχές μέσω ενός Συνοριακού Δρομολογητή Περιοχής (ABR).



Εικόνα 17:Backbone Area

Συνεπώς, οι πληροφορίες δρομολόγησης μεταφέρονται από τη μια περιοχή στην άλλη μέσα από το δίκτυο κορμού (area 0).

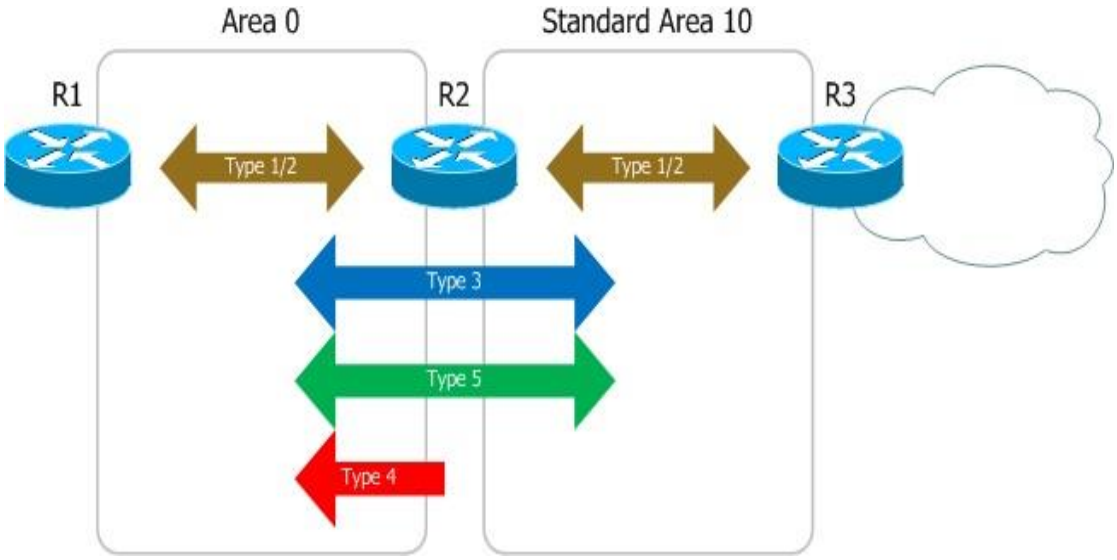
3.6.2 Standard Area

Είναι μια τυπική περιοχή στην οποία μεταφέρονται LSAs τύπου 1,2,3,4 και 5. Προφανώς, η backbone area θεωρείται και αυτή μία τυπική περιοχή.

Στο παράδειγμα που ακολουθεί, ο δρομολογητής R2 λειτουργεί ως ένας Συνοριακός Δρομολογητής Περιοχής (ABR) μεταξύ της τυπικής περιοχής (area 10) και του δικτύου κορμού (area 0), ενώ ο δρομολογητής R3 αναδιανέμει (redistribute) διαδρομές από έναν εξωτερικό domain και έτσι αποτελεί το Συνοριακό Δρομολογητή του Αυτόνομου Συστήματος (ASBR).

Τα LSA τύπου 1 και 2 αποστέλλονται μεταξύ δρομολογητών που ανήκουν στην ίδια περιοχή. Αυτό ισχύει για όλους τους τύπους περιοχών, καθώς αυτά τα LSA χρησιμοποιούνται για την κατασκευή του δέντρου με τη συντομότερη διαδρομή μιας περιοχής και, κατά συνέπεια, αφορούν μόνο μια μεμονωμένη περιοχή.

Τα LSA τύπου 3 και 5, τα οποία περιγράφουν εσωτερικές και εξωτερικές διαδρομές αντίστοιχα, κυκλοφορούν τόσο στο δίκτυο κορμού όσο και στις υπόλοιπες τυπικές περιοχές. Οι εξωτερικές διαδρομές δημιουργούνται από έναν ASBR, ενώ οι εσωτερικές διαδρομές μπορούν να δημιουργηθούν από οποιονδήποτε ABR.

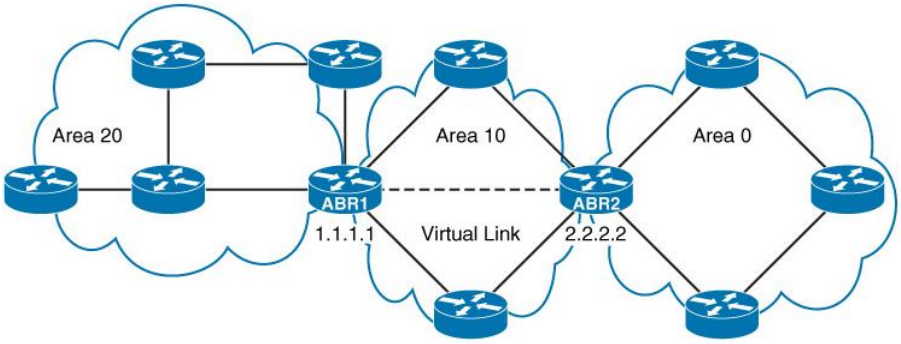


Εικόνα 18: Standard Area

Οι τυπικές περιοχές λειτουργούν έτσι ώστε να διασφαλίζουν τη βέλτιστη δρομολόγηση, καθώς όλοι οι δρομολογητές γνωρίζουν όλες τις διαδρομές. Ωστόσο, υπάρχουν συχνά περιπτώσεις όπου μια περιοχή έχει περιορισμένη πρόσβαση στο υπόλοιπο δίκτυο και η διατήρηση μιας πλήρους βάσης δεδομένων κατάστασης σύνδεσης δεν είναι απαραίτητη. Επιπλέον, μια περιοχή μπορεί να περιέχει δρομολογητές χαμηλού επιπέδου που δεν μπορούν να διατηρήσουν μια πλήρη βάση δεδομένων για ένα μεγάλο δίκτυο OSPF. Τέτοιες περιοχές μπορούν να διαμορφωθούν έτσι ώστε να εξαλείφουν ορισμένους τύπους LSA (θα τις δούμε αναλυτικότερα στη συνέχεια).

3.6.3 Transit Area

Αν για μια τυπική περιοχή δεν υπάρχει φυσική διασύνδεση με το δίκτυο κορμού (backbone area) τότε δημιουργείται μια εικονική διασύνδεση μεταξύ της τυπικής περιοχής και του δικτύου κορμού μέσω μιας άλλης περιοχής που ονομάζεται transit area.

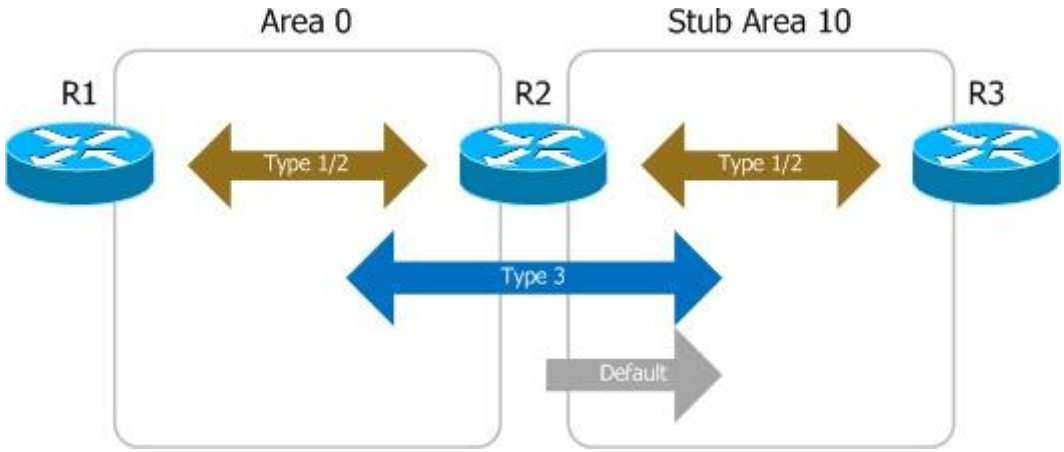


Εικόνα 19: Transit Area

Στο ανωτέρω διάγραμμα, η εικονική διασύνδεση (virtual link) πραγματοποιείται μεταξύ των δυο Συνοριακών Δρομολογητών Περιοχής ABR1 και ABR2 της transit area (area 10) και έτσι η επικοινωνία της τυπικής περιοχής (area 20) με το δίκτυο κορμού (area 0) περνάει μέσα από αυτή τη ζεύξη.

3.6.4 Stub Area

Μέσα σε αυτή την περιοχή διανέμονται μόνο LSA τύπου 1 και 2 και 3. Δηλαδή, οι stub areas μπλοκάρουν τα LSA τύπου 5, που μεταφέρουν πληροφορίες για διαδρομές προς εξωτερικά δίκτυα. Επιπλέον, δεδομένου ότι σε αυτές τις περιοχές δεν ανακοινώνονται εξωτερικές διαδρομές οι ABR δεν προωθούν ούτε LSA τύπου 4.

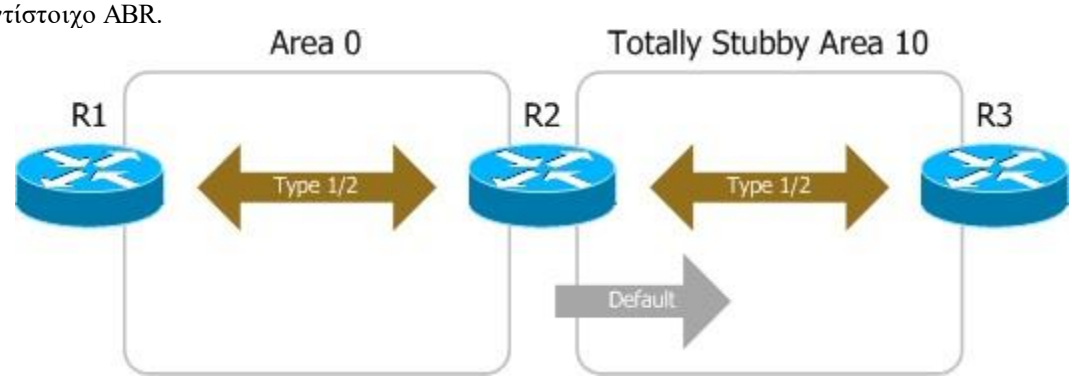


Εικόνα 20: Stub Area

Αφού οι εσωτερικοί δρομολογητές μιας stub area δεν χρειάζεται να γνωρίζουν πώς να φτάσουν σε εξωτερικά δίκτυα, δηλαδή σε δίκτυα που βρίσκονται εκτός του Αυτόνομου Συστήματος (AS), δεν απαιτείται από αυτούς να αποθηκεύουν τέτοιου είδους πληροφορίες στη μνήμη τους, διασφαλίζοντας με αυτό τον τρόπο τη διατήρηση μιας μικρής μόνο τοπολογίας δικτύου στη βάση δεδομένων τους. Η έξοδος των ανωτέρω δρομολογητών προς όλα τα εξωτερικά δίκτυα πραγματοποιείται πάντα μέσα από τον ABR της περιοχής τους. Για το σκοπό αυτό ο ABR διανέμει σε κάθε εσωτερικό δρομολογητή της περιοχής με την αποστολή LSAs τύπου 4 μια προκαθορισμένη διαδρομή (default route) ως έξοδο. Αυτό διασφαλίζει ότι οι όλοι δρομολογητές στην stab area θα μπορούν να δρομολογούν την κυκλοφορία σε εξωτερικούς προορισμούς, χωρίς να χρειάζεται να διατηρούν στη μνήμη τους πληροφορίες για όλες τις μεμονωμένες εξωτερικές διαδρομές. Αυτό επιτυγχάνεται με την ακόλουθη εντολή: Router(config-router)# area 10 stub.

3.6.5 Totally Stubby Area

Όπως οι εσωτερικοί δρομολογητές των stub areas, έτσι και οι δρομολογητές των totally stabby areas δεν λαμβάνουν LSA τύπου 4 ή 5 από τους ABR τους. Ωστόσο, οι δρομολογητές των totally stabby areas δεν λαμβάνουν επίσης LSA τύπου 3, οπότε όλη η δρομολόγηση έξω από την περιοχή τους βασίζεται αποκλειστικά και μόνο στην ενιαία προκαθορισμένη διαδρομή (default route) που εισάγεται από τον αντίστοιχο ABR.



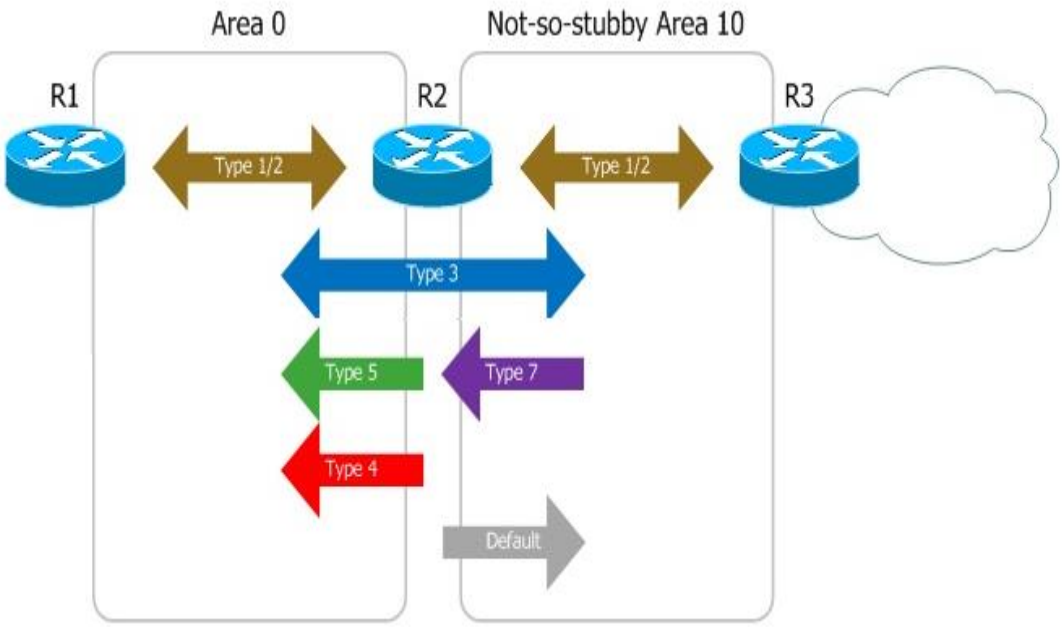
Εικόνα 21: Totally Stuby Area

Μια stab area επεκτείνεται σε μια totally stabby area με την προσθήκη της παραμέτρου no-summary ως εξής: Router(config-router)# area 10 stub no-summary.

Η χρήση των stabby areas και totally stabby areas είναι πράγματι βολική στη μείωση της χρήσης πόρων των δρομολογητών σε περιοχές του δικτύου που δεν απαιτούν πλήρη γνώση δρομολόγησης. Ωστόσο, κανένας από αυτούς τους δύο τύπους περιοχών δεν μπορεί να περιέχει ASBR, καθώς τα LSA τύπου 4 και 5 δεν επιτρέπονται εντός αυτών των περιοχών. Το πρόβλημα αυτό λύθηκε με τον καθορισμό των Not-So-Stubby Areas (NSSAs) που θα μελετήσουμε στη συνέχεια.

3.6.6 Not-So-Stubby Area (NSSA)

Είναι η περιοχή εκείνη όπου υλοποιεί την λειτουργικότητα μιας stub area, όπως αυτή αναλύθηκε προηγουμένως, περιλαμβάνοντας όμως και έναν ASBR που βρίσκεται εντός της περιοχής της, επιτρέποντας έτσι external διαδρομές. Οι external αυτές διαδρομές μπορούν να αποσταλούν και στις υπόλοιπες περιοχές, αλλά όμως απαγορεύεται η εισαγωγή external διαδρομών από άλλες περιοχές.



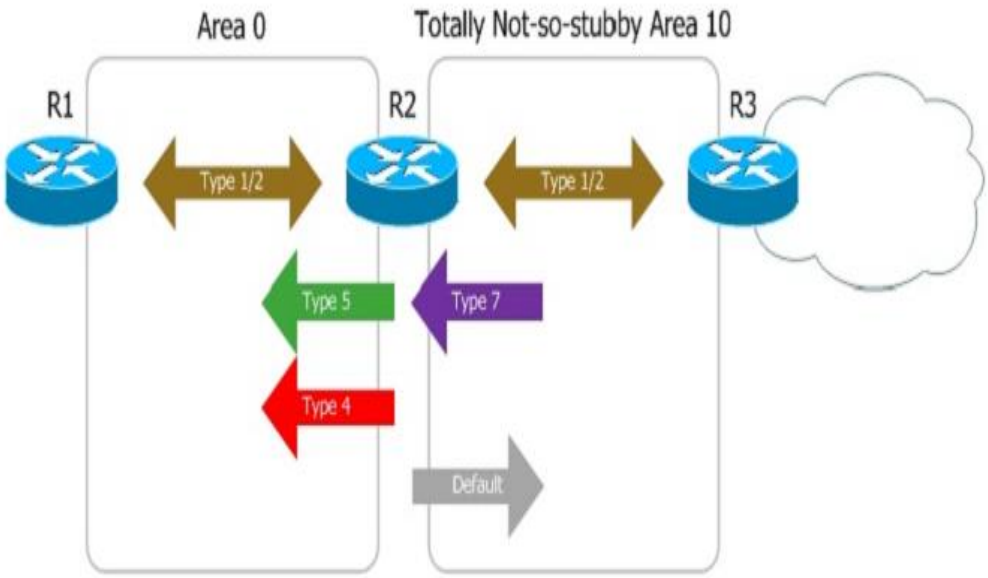
Εικόνα 22: NSSA

Ο ανωτέρω ASBR λαμβάνει LSAs τύπου 7 τα οποία στη συνέχεια μετατρέπονται σε LSAs τύπου 5 πριν αυτά αποσταλούν από τους ABRs προς τις υπόλοιπες περιοχές.

Η δήλωση μιας τέτοιας περιοχής επιτυγχάνεται με την ακόλουθη εντολή: Router(config-router)# area 10 nssa.

3.6.7 Totally Not-So-Stubby Area

Για να επεκταθεί μια περιοχή τύπου NSSA ώστε να λειτουργεί ως μια περιοχή τύπου totally NSSA, μπλοκάροντας έτσι και τα LSAs τύπου 3, ο ABR πρέπει να διαμορφωθεί με την επιπρόσθετη παράμετρο no-summary.



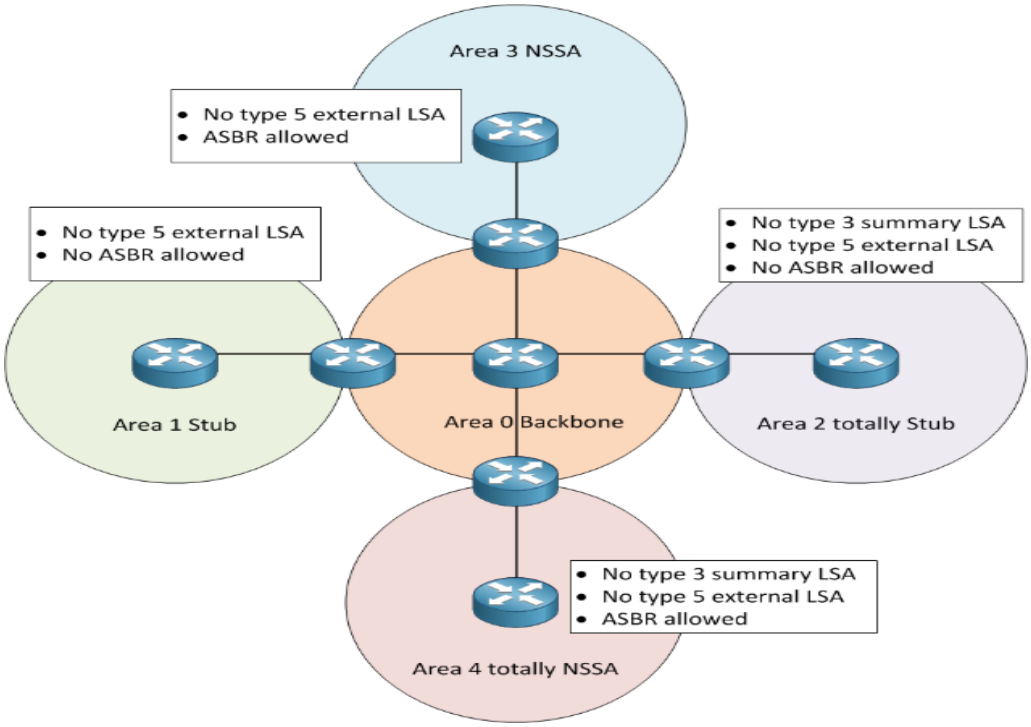
Εικόνα 23: Totally NSSA

Οπότε, η αντίστοιχη εντολή στο ανωτέρω παράδειγμα διαμορφώνεται ως εξής: Router(config-router)# area 10 nssa no-summary.

3.6.8 Διαφορές Stubby Areas και Not-So-Stubby Areas

Οι ανωτέρω τέσσερις τύποι ειδικών περιοχών εισάγουν προκαθορισμένες διαδρομές (default routes) σε μια περιοχή με σκοπό να αντικαταστήσουν τα αντίστοιχα summary LSAs τύπου 3 και τα external LSAs τύπου 5. Έτσι, το γεγονός αυτό συγκρατεί στον ελάχιστο δυνατό βαθμό την αποστολή LSAs σε αυτές τις περιοχές, οδηγώντας τους αντίστοιχους δρομολογητές των εν λόγω περιοχών σε λιγότερους υπολογισμούς SPF και κατ' επέκταση μικρότερους πίνακες δρομολόγησης.

Στο διάγραμμα που ακολουθεί συνοψίζονται σχηματικά οι διαφορές των τεσσάρων ειδικών περιοχών που αναλύθηκαν στις προηγούμενες παραγράφους.



Εικόνα 24: Stubby Areas and NSSAs

3.7 Ασφάλεια OSPF

Οι δρομολογητές που τρέχουν το πρωτόκολλο OSPF έχουν τη δυνατότητα να πιστοποιούν (authenticate) τα μηνύματα που ανταλλάσσουν μεταξύ τους, επιτρέποντας έτσι μόνο έμπιστους δρομολογητές να συμμετέχουν στην ανταλλαγή OSPF μηνυμάτων με σκοπό την αποφυγή κακόβουλων εισβολών.

Δεδομένου ότι γενικά τα πακέτα OSPF που ανταλλάσσονται μεταξύ των δρομολογητών δεν πιστοποιούνται μπορούν εύκολα να πλαστογραφηθούν. Για να λυθεί αυτό το πρόβλημα το πρωτόκολλο OSPF μας παρέχει τη δυνατότητα διαμόρφωσης δύο τύπων πιστοποίησης (authentication): τον απλό (σε μορφή clear text) και τον md5 (message digest) .

Είναι προφανές ότι ο έλεγχος ταυτότητας όταν πραγματοποιείται σε μορφή clear-text δεν είναι πολύ ασφαλής. Αντίθετα η πιστοποίηση md5 βασίζεται σε μυστικά κλειδιά που έχουν οριστεί σε όλους τους δρομολογητές και θεωρείται πιο ασφαλής και δεδομένου ότι χρησιμοποιούνται αριθμοί ακολουθίας μαζί με το md5 υπάρχει προστασία και από επαναλαμβανόμενες επιθέσεις (replay attacks).

3.7.1 Πιστοποίηση Clear-text

Έστω, ότι θέλουμε να διαμορφώσουμε clear-text authentication μεταξύ των δρομολογητών R1 και R2 που βρίσκονται στην area 0 και συνδέονται μεταξύ τους μέσω της διεπαφής eth0. Οι εντολές που πρέπει να δώσουμε είναι οι εξής:

```
R1(config)#int eth0
R1(config-if)#ospf authentication-key  SECRET-KEY
R1(config-if)#ospf authentication
```

```
R2(config)#int eth0
R2(config-if)#ospf authentication-key  SECRET-KEY
R2(config-if)#ospf authentication
```

Το κλειδί SECRET-KEY πρέπει να είναι κοινό και στους δύο δρομολογητές.

Εναλλακτικά, αν επιθυμούμε η πιστοποίηση να ισχύει για όλη την περιοχή (area 0) τότε την ενεργοποιούμε στο πρωτόκολλο OSPF και επομένως δε χρειάζεται να δίνουμε την αντίστοιχη εντολή ξεχωριστά σε κάθε interface που θέλουμε να ενεργοποιηθεί η πιστοποίηση. Αυτό συνήθως το χρησιμοποιούμε όταν κάποιος δρομολογητής έχει ενεργοποιημένο το πρωτόκολλο OSPF σε πολλές διεπαφές και θέλουμε να ενεργοποιήσουμε πιστοποίηση σε αυτές.

```
R1(config)#router ospf
R1(config-router)#area 0 authentication
```

```
R2(config)#router ospf
R2(config-router)#area 0 authentication
```

3.7.2 Πιστοποίηση MD5

Έστω, ότι θέλουμε να διαμορφώσουμε md5 authentication μεταξύ των δρομολογητών R1 και R2 που βρίσκονται στην area 0 και συνδέονται μεταξύ τους μέσω της διεπαφής eth0. Οι εντολές που πρέπει να δώσουμε είναι οι εξής:

```
R1(config)#int eth0
R1(config-if)#ospf message-digest-key 1 md5 SECRET-KEY
R1(config-if)#ospf authentication message-digest
```

```
R2(config)#int eth0
R2(config-if)#ospf message-digest-key 1 md5 SECRET-KEY
R2(config-if)#ospf authentication message-digest
```

Το κλειδί SECRET-KEY πρέπει να είναι κοινό και στους δύο δρομολογητές. Προφανώς, υπάρχει η δυνατότητα σε έναν δρομολογητή να χρησιμοποιηθούν διαφορετικά md5 κλειδιά όταν αυτός διαθέτει περισσότερες από μία διεπαφές στις οποίες έχει ενεργοποιηθεί το πρωτόκολλο OSPF.

Ομοίως, αν επιθυμούμε η πιστοποίηση να ισχύει για όλη την περιοχή (area 0) τότε την ενεργοποιούμε στο πρωτόκολλο OSPF και επομένως δε χρειάζεται να δίνουμε την αντίστοιχη εντολή ξεχωριστά σε κάθε interface που θέλουμε να ενεργοποιηθεί η πιστοποίηση.

```
R1(config)#router ospf
R1(config-router)#area 0 authentication message-digest
```

```
R2(config)#router ospf
R2(config-router)#area 0 authentication message-digest
```

3.8 OSPFv3

Η νεότερη έκδοση OSPF (OSPFv3) υποστηρίζει τη δρομολόγηση πακέτων IPv6 και περιγράφεται στο RFC2740. Γι το σκοπό αυτό το OSPFv3 ενσωματώνει όλες τις απαραίτητες αλλαγές για τη λειτουργία του σε ένα δίκτυο IPv6 [6]

Οι κυριότερε αλλαγές είναι οι εξής :

1. Τα LSA πακέτα περιέχουν και διευθύνσεις IPv6.

2. Το OSPFv3 απαιτεί να ρυθμιστεί πρώτα το Router Id και μετά να ξεκινήσει η δρομολόγηση.

3. Οι δρομολογητές DR και BDR είναι πλέον αναγνωρίσιμοι από τα Router Id τους αντί των IP διευθύνσεών τους.

4. Όλες οι πληροφορίες προθέματος IP έχουν καταργηθεί από το πακέτο ανίχνευσης Hello, καθιστώντας έτσι το OSPFv3 ένα ουσιαστικά ανεξάρτητο πρωτόκολλο.

5. Οι μηχανισμοί ασφαλείας που χρησιμοποιεί το πρωτόκολλο OSPFv3 για την προστασία των ενημερώσεων δρομολόγησης του παρέχονται από το πρωτόκολλο IPsec σε περιβάλλον IPv6.

4

Πρωτόκολλο BGP

Το πρωτόκολλο δρομολόγησης εξωτερικών πυλών BGP έχει σχεδιαστεί με σκοπό να προσφέρει ένα κατάλληλο περιβάλλον δρομολόγησης μεταξύ των Εταιρειών Παροχής Υπηρεσιών Διαδικτύου (Internet Service Providers), των Οργανισμών, των λοιπών Εταιρειών και γενικότερα των AS. Το BGP δημιουργήθηκε το 1994 με σκοπό να αντικαταστήσει το EGP το οποίο δεν μπορούσε πλέον να καλύψει τις συνεχείς απαιτήσεις της δρομολόγησης παγκοσμίως και αποτελεί πλέον το μοναδικό πρωτόκολλο δρομολόγησης εξωτερικών πυλών που χρησιμοποιείται σήμερα. Η τρέχουσα έκδοση του BGP πρωτοκόλλου είναι η version 4 και περιγράφεται στο RFC4271 [8] του 2006.

Ένα από τα βασικότερα χαρακτηριστικά του BGP είναι ότι δεν θέτει κανέναν περιορισμό στις αλληλοσυνδέσεις που μπορούν να υπάρξουν ανάμεσα στα διάφορα AS. Επιπλέον, το πρωτόκολλο BGP χρησιμοποιεί έναν αποδοτικό και ευέλικτο αλγόριθμο δρομολόγησης για τη διανομή, τον υπολογισμό και τη διαχείριση των διαθέσιμων διαδρομών (routes) μεταξύ των AS, επιτρέποντας έτσι σε έναν δρομολογητή να αναγνωρίσει πολλαπλά μονοπάτια, να εντοπίσει και να αποφύγει πιθανούς βρόχους δρομολόγησης και τέλος να επιλέξει με αποτελεσματικό τρόπο τη διαδρομή που θα ακολουθήσει μεταξύ των πολλαπλών μονοπατιών που ενδεχομένως διαθέτει.

Το BGP χρησιμοποιείται κυρίως για την εφαρμογή πολιτικών δρομολόγησης από τους ISPs (Internet Service Providers) και βασίζεται σε πολιτικές δρομολόγησης (policy based protocol) και όχι σε απλά metrics όπως τα IGPs (Internal Gateway Protocols). Με την ανάπτυξη κατάλληλων πολιτικών μπορούν π.χ. να τεθούν περιορισμοί στην κυκλοφορία των εισερχόμενων ή/και των εξερχόμενων πακέτων ανάλογα με τη διάθεση των ενδιαφερόμενων μερών να παρέχουν υπηρεσίες διακίνησης δεδομένων μεταξύ των AS.

Τα κυριότερα πλεονεκτήματα που κατέστησαν κυρίαρχο το BGP πρωτόκολλο μέχρι και σήμερα είναι τα εξής:

- Παρέχει υψηλή διαθεσιμότητα (availability) και πλεονασμό (redundancy), όπου αυτά απαιτούνται.
- Διαθέτει ταχύτατη προσαρμογή στην εύρεση εναλλακτικών διαδρομών σε περιπτώσεις ενδεχόμενων δικτυακών αποτυχιών.
- Υποστηρίζει ενεργές εναλλακτικές ή παράλληλες διαδρομές προς τα δίκτυα προορισμού.

- Διασφαλίζει ταχεία επίλυση σε ενδεχόμενες ανωμαλίες δρομολόγησης, όπως βρόχοι (routing loops).
- Προσαρμόζει την δικτυακή κυκλοφορία ανάλογα με το μέγεθος του δικτύου (scalability).
- Παρέχει ταχεία σύγκλιση σε μία αποδεκτή τοπολογία για κάθε σημείο του δικτύου έπειτα από μια αλλαγή δρομολόγησης.
- Διαθέτει χαρακτηριστικά ασφαλείας για την αποφυγή πιθανής λανθασμένης μετάδοσης.
- Είναι προσανατολισμένο σε δρομολόγηση που βασίζεται σε πολιτικές.
- Παρέχει τεχνικές μείωσης των αναγκών για διαθέσιμους πόρους των δρομολογητών, όπως μνήμη, επεξεργαστική ισχύς και εύρος ζώνης.

4.1 Λειτουργία BGP Πρωτοκόλλου

Το BPG αποτελεί ένα χαρακτηριστικό παράδειγμα path vector πρωτοκόλλου που χρησιμοποιείται για τη δρομολόγηση εξωτερικών πυλών και διαφέρει από τα πρωτόκολλα τύπου distance vector, όπως το RIP, και link state, όπως το OSPF, που χρησιμοποιούνται για τη δρομολόγηση εσωτερικών πυλών. Το BGP πρωτόκολλο διατηρεί πληροφορίες με τις πλήρεις διαδρομές των προορισμών οι οποίες ανανεώνονται δυναμικά και διαθέτει μηχανισμό που να ανιχνεύει και να απορρίπτει εκείνες τις διαδρομές που οδηγούν σε βρόχους. Κάθε νέα εγγραφή στον πίνακα δρομολόγησης περιέχει το δίκτυο προορισμού, τον επόμενο δρομολογητή (next hop) και το μονοπάτι (as path) που οδηγεί στον προορισμό.

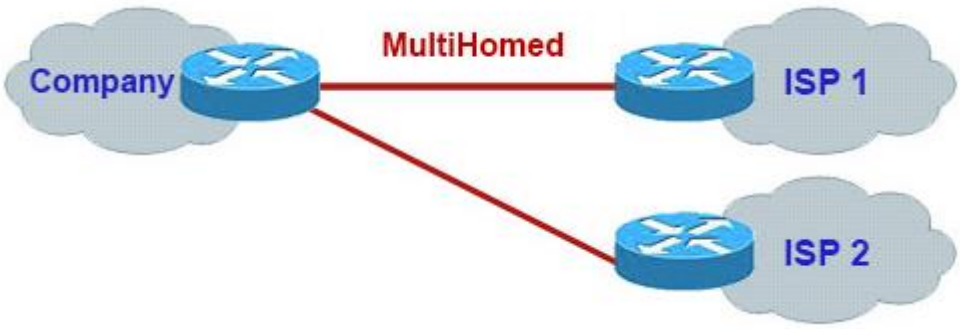
Το BGP, ως ένα path vector πρωτόκολλο, δεν λαμβάνει υπόψη μόνο το κόστος πρόσβασης προς έναν προορισμό, αλλά αναλύει και την αντίστοιχη διαδρομή του ώστε να ανιχνευτούν πιθανοί βρόχοι. Έτσι, κάθε φορά που ένας δρομολογητής λαμβάνει μια διαδρομή (route) μέσα στην οποία υπάρχει ένα μέρος του μονοπατιού που ήδη γνωρίζει, η ανακοίνωση αυτή δεν λαμβάνεται υπόψη, καθώς στην αντίθετη περίπτωση θα οδηγούσε σε βρόχο. Με αυτόν τον μηχανισμό το πρωτόκολλο εγγυάται μονοπάτια χωρίς βρόχους τα οποία στη συνέχεια μπορεί να τα ανακοινώσει σε γειτονικούς δρομολογητές. Θα πρέπει εδώ να σημειώσουμε ότι στον πίνακα δρομολόγησης του πρωτοκόλλου διατηρούνται μονοπάτια AS και όχι δρομολογητών. Έτσι, το πρωτόκολλο επιλέγει εκείνες τις διαδρομές που διασχίζουν τον ελάχιστο αριθμό αλμάτων AS (AS hops) και όχι δρομολογητών, μιας και το πρωτόκολλο δεν παρακολουθεί εξ ολοκλήρου την τοπολογία του διαδικτύου σε επίπεδο δρομολογητών παρά μόνο σε επίπεδο AS.

Υπάρχουν τρεις βασικοί τύποι AS στους οποίους μπορεί να εφαρμοστεί το πρωτόκολλο BGP.

- Τα single-homed, τα οποία διαθέτουν μόνο ένα σημείο εξόδου προς άλλα AS.
- Τα multi-homed, τα οποία διαθέτουν πολλαπλά σημεία εξόδου προς άλλα AS.
- Τα transit, τα οποία επιτρέπουν να διέρχεται κίνηση που έχει προέλευση και προορισμό έξω από τα τοπικά AS.



Εικόνα 25: Single-homed AS



Εικόνα 26: Multi-homed AS

Το BGP χρησιμοποιείται κυρίως από τους ISPs που στην ουσία συνθέτουν ολόκληρο το διαδίκτυο (internet) πάνω στους οποίους είναι συνδεδεμένα τα υπόλοιπα AS των χρηστών. Οι ISPs διαθέτουν συνήθως διαβιβαστικά (transit) AS, ενώ οι πελάτες, όπως ένα εταιρικό δίκτυο, διαθέτουν κυρίως μη διαβιβαστικά (non-transit) AS που σημαίνει ότι επιτρέπουν μόνο την κίνηση η οποία έχει παραχθεί ή έχει προορισμό τα ίδια AS. Φυσικά κάποιο AS αν το επιθυμεί μπορεί να επιτρέψει οποιαδήποτε κίνηση να περνά μέσα από αυτό ελεύθερα. Γενικότερα, οι ISPs αναπτύσσουν συμβάσεις σχηματίζοντας σχέσεις μεταξύ τους, επιτρέποντας με αυτόν τον τρόπο να πραγματοποιούνται διαβάσεις της κίνησης ανάμεσα στους πελάτες τους, παρέχοντας συντομεύσεις διαδρομών και συμβάλλοντας έτσι στην αποδοτικότερη δρομολόγηση στο διαδίκτυο.

Είναι προφανές ότι από μόνη της η διασύνδεση μεταξύ των AS δεν επαρκεί για να υποστηρίξει το διαδίκτυο, καθώς θα πρέπει να παρέχεται και η δυνατότητα δρομολόγησης από έναν εσωτερικό δρομολογητή ενός AS προς έναν δρομολογητή ενός άλλου AS. Τον ρόλο αυτό αναλαμβάνουν οι συνοριακοί δρομολογητές που βρίσκονται πάνω στις ζεύξεις που συνδέουν δύο AS και ονομάζονται ASBRs (Autonomous Systems Border Routers). Οι ASBRs ανακοινώνουν την προσβασιμότητα των δικτύων σε γειτονικά σε αυτούς AS. Καθώς, η κυκλοφορία των πακέτων διασχίζει το εσωτερικό ενός AS, τα πακέτα αυτά περνούν και από άλλους δρομολογητές πέραν των ASBRs οι οποίοι ονομάζονται transit δρομολογητές. Συνήθως τα περιφερειακά AS διαθέτουν έναν μόνο ASBR ως μοναδική πύλη εξόδου. Υπάρχουν όμως και AS που διαθέτουν πολλαπλούς ASBRs, όπου η επιλογή πύλης εξόδου για κάποιο δρομολογητή αποτελεί μια πιο σύνθετη διαδικασία.

Το BGP πρωτόκολλο χρησιμοποιεί το αξιόπιστο (connection-oriented) TCP πρωτόκολλο, εκχωρώντας τον έλεγχο για θέματα αξιόπιστης παράδοσης, αναμετάδοσης και ανίχνευσης λαθών των πακέτων στο πρωτόκολλο μεταφοράς ώστε να μπορεί το ίδιο το πρωτόκολλο να εστιάσει αποκλειστικά και μόνο σε θέματα δρομολόγησης. Η αρχικοποίηση ενός BGP δρομολογητή πραγματοποιείται με τη χρήση μιας τοπικής προσωρινής θύρας (>1024), στη συνέχεια ο δρομολογητής εγκαθιδρύει μια σχέση ομότιμου (peer) με έναν άλλο BGP δρομολογητή χρησιμοποιώντας την θύρα 179 (well-known BGP port).

Η πρώτη ενέργεια που λαμβάνει χώρα στους BGP δρομολογητές, αφού προηγουμένως έχουν πραγματοποιηθεί οι αντίστοιχες TCP συνδέσεις των δρομολογητών και είναι σε θέση να ανταλλάξουν μηνύματα μεταξύ τους, είναι η εγκαθίδρυση μιας BGP συνόδου (session), δηλ. μιας σύνδεσης από σημείο σε σημείο (point-to-point) ανάμεσα σε ομότιμους (peers) ή γειτονικούς (neighbors) δρομολογητές. Πιο συγκεκριμένα, ο δρομολογητής που αρχικοποιεί τη σύνοδο ονομάζεται ενεργός (active), ενώ αυτός που την αποδέχεται (passive). Όταν δύο δρομολογητές προσπαθούν ταυτόχρονα να συνδεθούν με έναν τρίτο δρομολογητή λαμβάνει χώρα σύγκρουση και αυτή επιλύεται συγκρίνοντας ο καθένας το ID του τοπικού δρομολογητή με το ID του συγκρουόμενου γείτονα και απορρίπτοντας ο μεν δρομολογητής που διαθέτει το μεγαλύτερο ID τη σύνοδο στην οποία είναι ενεργητικός, ο δε δρομολογητής που διαθέτει το μικρότερο ID τη σύνοδο στην οποία είναι παθητικός. Στην ουσία διατηρείται μόνο η σύνοδος που αρχικοποιήθηκε από τον δρομολογητή που διέθετε το μεγαλύτερο ID. Όταν μια σύνοδος ολοκληρωθεί δεν έχει καμία απολύτως σημασία ποιος δρομολογητής είναι ενεργητικός και ποιος παθητικός.

Οι BGP neighbors ανταλλάσσοντας μεταξύ τους ενημερώσεις μαθαίνουν πολλαπλές διαδρομές (routes) προς διάφορους προορισμούς, στη συνέχεια επιλέγουν τις βέλτιστες από αυτές διαδρομές τις οποίες τοποθετούν στον BGP routing table και τις αποστέλλουν στους γειτονικούς δρομολογητές (neighbors). Οι βέλτιστες διαδρομές επιλέγονται βάση των πολιτικών δρομολόγησης που εφαρμόζονται σε αυτές. Οι BGP δρομολογητές διατηρούν τρεις τύπους πινάκων ή βάσεων δεδομένων: τον neighbor table που περιέχει την λίστα όλων των γειτόνων, τον BGP database ή RIB (Routing Information Base) που περιέχει όλες τις γνωστές διαδρομές και τον BGP routing table που περιέχει μόνο τις βέλτιστες διαδρομές.

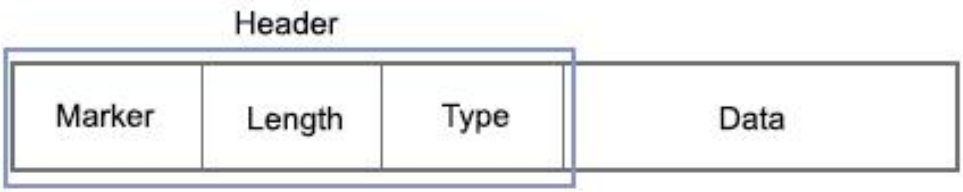
Όταν ένας BGP τίθεται σε λειτουργία αποστέλλει ολόκληρο τον routing table στους γειτονικούς δρομολογητές (neighbors), ώστε να τους ενημερώσει για τα δίκτυα που μπορούν να προσεγγίσουν μέσω αυτού, ενώ σε περίπτωση που συμβούν κάποιες αλλαγές τους αποστέλλει νέες ενημερώσεις. Όλες οι νέες διαδρομές αποθηκεύονται στην RIB η οποία συνήθως διατηρεί πολλαπλές διαδρομές προς κάθε προορισμό. Αντίθετα, ο routing table διατηρεί μόνο μια διαδρομή προς κάθε προορισμό, αυτή που προκύπτει μετά την εφαρμογή του μηχανισμού επιλογής βέλτιστης διαδρομής.

4.2 Τύποι BGP Πακέτων

Για τη λειτουργία του BGP πρωτοκόλλου χρησιμοποιούνται τα ακόλουθα ειδικού τύπου πακέτα:

- **Open:** για την εγκαθίδρυση σχέσεων.
- **Update**: για ενημερώσεις διαδρομών (routes) και ιδιοτήτων (attributes) τους.
- **Notification**: για ενημερώσεις σφαλμάτων στην επικοινωνία που οδηγούν σε επανεκκίνηση (reset) των σχέσεων.
- **Keep-alive**: για τη διατήρηση της γειτονικής σχέσης.

Η επικεφαλίδα (header) που χρησιμοποιείται από τα BGP πακέτα είναι η εξής:



Εικόνα 27: BGP Header

- **Marker:** είναι ένα πεδίο με μήκος 16-byte και χρησιμοποιείται για πιστοποίηση (authentication) του BGP.
- **Length:** είναι ένα πεδίο με μήκος 2-byte και περιέχει το συνολικό μήκος του μηνύματος σε byte.
- **Type:** είναι ένα πεδίο με μήκος 1-byte και περιέχει έναν ακέραιο αριθμό που δείχνει τον τύπο του μηνύματος (1= Open, 2=Update, 3=Notification, 4=Keep-Alive).

Η διαδικασία δημιουργίας γειτονικής σχέσης (adjacent) μεταξύ των δρομολογητών περιλαμβάνει τα ακόλουθα 6 στάδια:

1. **Idle:** φανερώνει ότι ο δρομολογητής μπορεί να έχει κάποιο πρόβλημα ή να βρίσκεται σε κατάσταση αναμονής για τη δημιουργία TCP συνόδου.

2. **Connect:** δείχνει ότι ο δρομολογητής βρίσκεται σε κατάσταση αναμονής για την ολοκλήρωση της TCP συνόδου.

3. **Active:** σημαίνει ότι η TCP σύνοδος έχει εγκαθιδρυθεί, αλλά δεν έχει ξεκινήσει ακόμη η διαδικασία δημιουργίας BGP συνόδου.

4. **Open sent:** σημαίνει ότι ολοκληρώθηκε η TCP σύνοδος, έχει ξεκινήσει η διαδικασία της BGP συνόδου, αλλά δεν έχει ληφθεί ακόμα πακέτο Open.

5. **Open confirmed:** σημαίνει ότι το πακέτο Open έχει αποσταλεί και ληφθεί και από τους δύο peers.

6. **Established:** φανερώνει ότι οι παράμετροι και στους δύο peers έχουν ελεγχτεί, η BGP σύνοδος έχει ολοκληρωθεί και μπορούν πλέον να ανταλλάξουν μεταξύ τους πακέτα update.

4.3 BGP Χαρακτηριστικά

Το BGP πρωτόκολλο για να επιλέξει τη βέλτιστη διαδρομή προς κάποιον προορισμό αναπτύσσει διάφορες πολιτικές δρομολόγησης με τη βοήθεια μιας σειράς από χαρακτηριστικά ή ιδιότητες (attributes) που μεταφέρουν τα BGP πακέτα. Έτσι, για μια διαδρομή (route) αποθηκεύονται εκτός από τις διευθύνσεις των προορισμών, ένα σύνολο από χαρακτηριστικά (attributes). Οπότε, με την κατάλληλη ρύθμιση των ακόλουθων χαρακτηριστικών επιτυγχάνεται η επιθυμητή πολιτική δρομολόγησης που θέτει ο κάθε ISP.

- Γνωστά Υποχρεωτικά Χαρακτηριστικά (well known mandatory attributes)
  - **Origin** (Προέλευση)
  - **AS_Path** (Μονοπάτι Αυτόνομων Συστημάτων)
  - **Next_Hop** (Επόμενος Βήμα)

- Γνωστά Διακριτικά Χαρακτηριστικά (well known discretionary attributes)
  - **Local_Preference** (Τοπική Προτίμηση)
  - **Atomic_Aggregate** (Συνάθροιση Διαδρομής)

- Προαιρετικά Μεταβατικά Χαρακτηριστικά (Optional transitive attributes)
  - **Aggregator** (Δρομολογητής που έκανε τη Συνάθροιση της Διαδρομής)
  - **Community** (Κοινότητα)

- Προαιρετικά μη Μεταβατικά Χαρακτηριστικά (Optional non-transitive attributes)
  - **Multi-Exit Discriminator-MED** (Διευκρινιστής πολλαπλής εξόδου)

Τα γνωστά υποχρεωτικά χαρακτηριστικά πρέπει να αναγνωρίζονται και να υλοποιούνται από όλους τους BGP δρομολογητές και να συμπεριλαμβάνονται οπωσδήποτε σε κάθε πακέτο ενημέρωσης του BGP

πρωτοκόλλου, ενώ τα γνωστά διακριτικά χαρακτηριστικά δεν είναι υποχρεωτικό να περιλαμβάνονται σε όλα τα πακέτα ενημερώσεων.

Τα προαιρετικά μεταβατικά attributes δεν είναι υποχρεωτικό να αναγνωρίζονται και να επεξεργάζονται από όλους τους BGP δρομολογητές, ενώ τα προαιρετικά μη μεταβατικά χαρακτηριστικά δεν αναμεταδίδονται σε άλλους ομότιμους (peers) αν δεν μπορούν να αναγνωριστούν.

Προφανώς, όσο περισσότερα χαρακτηριστικά (attributes) διαθέτει μια διαδρομή τόσο μεγαλύτερος είναι και ο έλεγχος στην προτίμηση ή την πολιτική δρομολόγησης της.

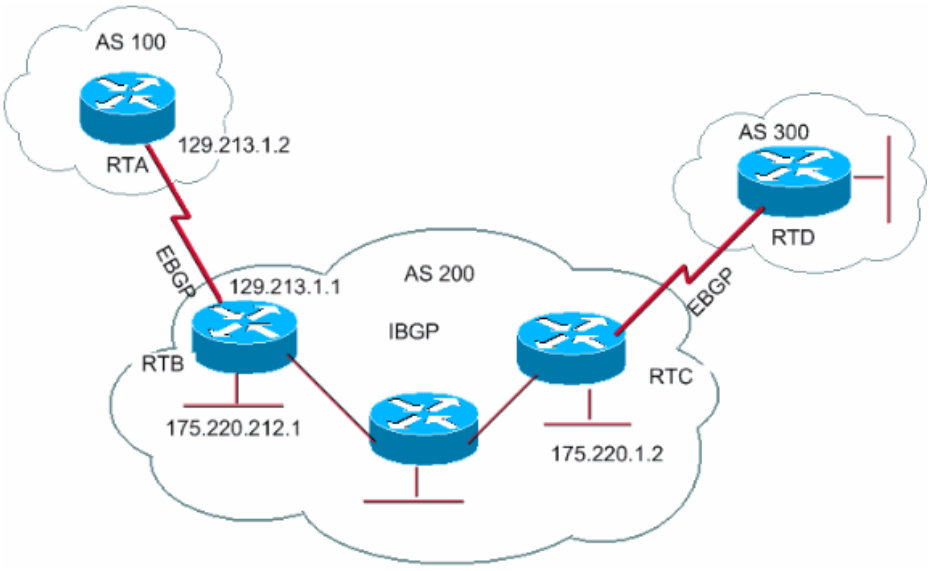
4.4 Κριτήρια Επιλογής BGP Διαδρομής

Το BGP πρωτόκολλο για να επιλέξει έναν προορισμό σε περίπτωση που διαθέτει πολλαπλά μονοπάτια προσέγγισής του εφαρμόζει με σειρά προτεραιότητας τα ακόλουθα κριτήρια, όπου κάθε κριτήριο μπορεί να χρησιμοποιηθεί ως καθοριστικό στην λήψη της απόφασης αν όλα τα προηγούμενα κριτήρια είναι ίδια:

- Αρχικά απορρίπτει όλες τις διαδρομές για τις οποίες δεν γνωρίζει το NEXT_HOP, αφού δεν ξέρει πώς να τις προσεγγίσει.
- Στη συνέχεια επιλέγει εκείνη τη διαδρομή στην οποία έχει αποδοθεί υψηλότερο weight στον τοπικό δρομολογητή.
- Το επόμενο κριτήριο αποτελεί η υψηλότερη τιμή του LOCAL_PREF.
- Κατόπιν επιλέγονται διαδρομές που δημιούργησε ο ίδιος ο δρομολογητής έναντι αυτών που έλαβε ως ενημέρωση από κάποιον άλλον BGP peer.
- Το επόμενο κριτήριο είναι το AS_PATH, όπου το μικρότερο AS_PATH κερδίζει.
- Αν πάλι όλα τα παραπάνω είναι ίδια επιλέγονται οι διαδρομές με τον προτιμότερο origin code (IGP>EGP>Incomplete).
- Στη συνέχεια επιλέγεται η διαδρομή με το μικρότερο MED.
- Αν όλα τα παραπάνω είναι πανομοιότυπα προτιμάται η εξωτερική eBGP διαδρομή έναντι της αντίστοιχης εσωτερικής iBGP.
- Αν πάλι όλα τα παραπάνω είναι ίδια προτιμάται ο κοντινότερος iBGP δρομολογητής.
- Τέλος, προτιμάται η πιο παλιά eBGP διαδρομή που θεωρείται πιο σταθερή (stable). Είναι προφανώς σπάνιο να λάβει ένας BGP δρομολογητής δύο πανομοιότυπες διαδρομές το ίδιο ακριβώς δευτερόλεπτο. Σε αυτήν την περίπτωση προτιμάται η διαδρομή που έχει το μικρότερο BGP router ID απλά και μόνο για να τερματίσει η διαδικασία επιλογής.

4.5 Διευθέτηση BGP Πρωτοκόλλου

4.5.1 External Border Gateway Protocol (eBGP) vs. Internal Border Gateway Protocol (iBGP)



Εικόνα 28: eBGP & iBGP

```
RTA#
  router bgp 100
    neighbor 129.213.1.1 remote-as 200

RTB#
  router bgp 200
    neighbor 129.213.1.2 remote-as 100
    neighbor 175.220.1.2 remote-as 200

RTC#
  router bgp 200
    neighbor 175.220.212.1 remote-as 200
```

Παρατηρούμε ότι ο δρομολογητής RTB έχει δύο peers (neighbors): τον 129.213.1.2 που βρίσκεται σε διαφορετικό AS100, οπότε πρόκειται για eBGP διασύνδεση και τον 175.220.1.2 που βρίσκεται στο ίδιο AS200, οπότε πρόκειται για iBGP διασύνδεση.

Με τον ίδιο τρόπο θα πρέπει να δηλωθεί και η eBGP διασύνδεση μεταξύ των δρομολογητών RTC και RTD που ανήκουν στα AS200 και AS300 αντίστοιχα.

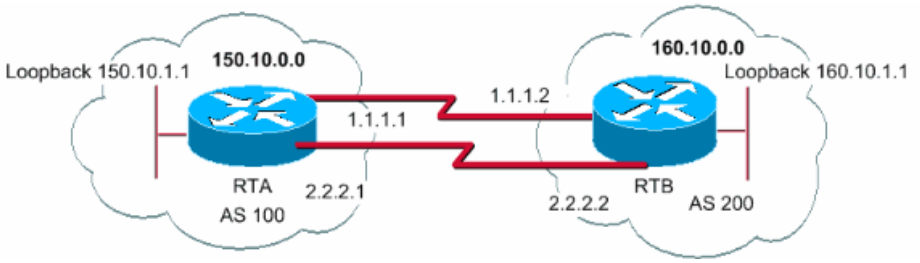
Το default Administrative Distance του eBGP είναι 20, ενώ του iBGP είναι 200.

Εξωτερικές διαδρομές (eBGP διαδρομές, δηλαδή διαδρομές εκτός AS) που λαμβάνονται από έναν eBGP peer μπορούν να ανακοινωθούν (advertised) τόσο σε άλλους eBGP peers όσο και σε άλλους iBGP peers, ενώ εσωτερικές διαδρομές (iBGP διαδρομές, δηλαδή διαδρομές εντός του ίδιου AS) που λαμβάνονται από έναν iBGP peer δεν μπορούν να ανακοινωθούν σε άλλον iBGP peer, αλλά μπορούν να ανακοινωθούν σε άλλους eBGP peers.

Στους eBGP peers το default TTL=1, ενώ στους iBGP peers το default TTL=255.

Όταν μια διαδρομή ανακοινώνεται σε έναν eBGP peer το Next Hop αλλάζει και παίρνει στην IP διεύθυνση του τοπικού δρομολογητή, ενώ όταν μια διαδρομή ανακοινώνεται σε έναν iBGP peer το Next Hop παραμένει το ίδιο.

4.5.2 eBGP Multihop Load Balancing



Εικόνα 29: eBGP Multihop

```
RTA#
  interface loopback 0
     ip address 150.10.1.1 255.255.255.0

  router bgp 100
    neighbor 160.10.1.1 remote-as 200
    neighbor 160.10.1.1 ebgp-multihop
    neighbor 160.10.1.1 update-source loopback 0
    network 150.10.0.0

  ip route  160.10.0.0   255.255.0.0   1.1.1.2
  ip route  160.10.0.0   255.255.0.0   2.2.2.2
```

```
RTB#
  interface loopback 0
    ip address 160.10.1.1 255.255.255.0

  router bgp 200
    neighbor 150.10.1.1 remote-as 100
    neighbor 150.10.1.1 ebgp-multihop
    neighbor 150.10.1.1 update-source loopback 0
    network 160.10.0.0

  ip route  150.10.0.0   255.255.0.0   1.1.1.1
  ip route  150.10.0.0   255.255.0.0   2.2.2.1
```

Δεδομένου ότι οι eBGP διαδρομές χρησιμοποιούν ως default TTL=1 όταν ένας BGP neighbor βρίσκεται σε απόσταση μεγαλύτερη του ενός σταθμού (hop) το TTL ενός BGP πακέτου θα μειωθεί στο 0 στον επόμενο σταθμό και έτσι το πακέτο θα απορριφθεί (discarded). Επομένως, όταν οι eBGP peers δεν είναι απευθείας συνδεδεμένοι μεταξύ τους (directly connected) θα πρέπει να δηλωθούν ως **ebgp-multihop**.

Στο ανωτέρω παράδειγμα για την eBGP διασύνδεση των δύο δρομολογητών έχει χρησιμοποιηθεί το loopback interface 0 και από τους δύο peers με σκοπό να δημιουργηθεί load balancing μεταξύ των δύο point-to-point συνδέσεών τους. Οπότε, αναγκαστικά σε αυτή την περίπτωση θα πρέπει να δηλωθούν οι neighbors και στους δύο δρομολογητές ως **ebgp-multihop** δεδομένου ότι η απόστασή τους γίνεται πλέον μεγαλύτερη του ενός σταθμού (hop). Επιπλέον, στην ανωτέρω περίπτωση που χρησιμοποιούμε ως neighbors loopback IP διευθύνσεις θα πρέπει οπωσδήποτε οι neighbors να δηλωθούν ως **update-source loopback 0**.

Τέλος, το load balancing επιτυγχάνεται χρησιμοποιώντας σε κάθε δρομολογητή δύο στατικές διαδρομές ίσου κόστους (metric).

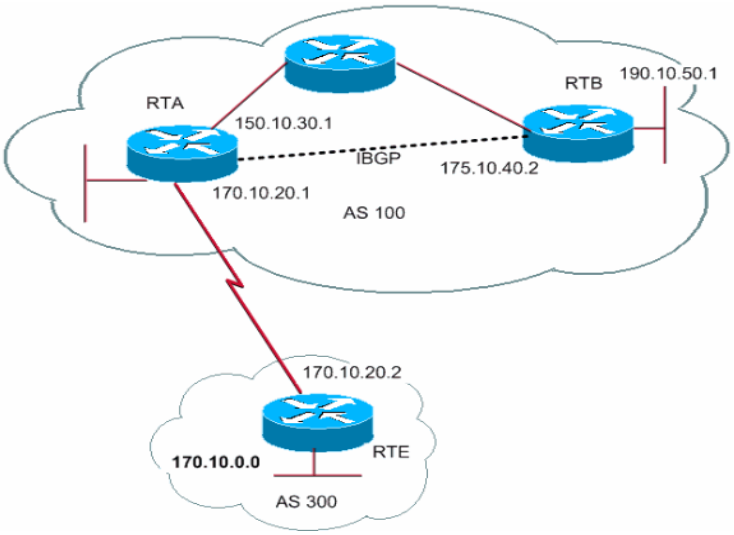
4.5.3 BGP Origin Attribute

IGP: Δημιουργούνται από το BGP πρωτόκολλο.

EGP: Δημιουργούνται από το EGP πρωτόκολλο.

Incomplete: Γίνονται redistributed από άλλα πρωτόκολλα δρομολόγησης ή στατικές διαδρομές.

Origin codes: i - IGP, e - EGP, ? – incomplete.



Εικόνα 30: Origin Attribute

```
RTA#
  router bgp 100
    neighbor 190.10.50.1 remote-as 100
    neighbor 170.10.20.2 remote-as 300
    network 150.10.0.0
    redistribute static

  ip route 190.10.0.0 255.255.0.0 null0

RTB#
  router bgp 100
    neighbor 150.10.30.1 remote-as 100
    network 190.10.50.0

RTE#
  router bgp 300
    neighbor 170.10.20.1 remote-as 100
    network 170.10.0.0
```

Ο RTA φτάνει στο δίκτυο 170.10.0.0 μέσω **300 i**.
Το "**300 i**" σημαίνει ότι το επόμενο AS path είναι το 300 και το origin είναι IGP.

Ο RTA φτάνει στο δίκτυο 190.10.50.0 μέσω **i**.
Το "**i**" σημαίνει ότι δίκτυο βρίσκεται στο ίδιο AS και το origin είναι IGP.

Ο RTE φτάνει στο δίκτυο 150.10.0.0 μέσω **100 i**.
Το "**100 i**" σημαίνει ότι το επόμενο AS path είναι το 100 και το origin είναι IGP.

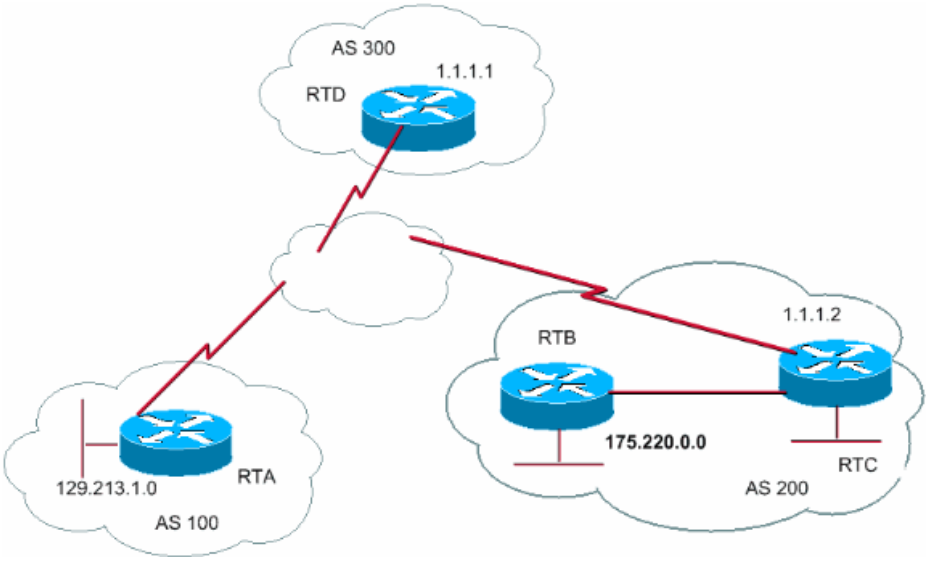
Ο RTE φτάνει στο δίκτυο 190.10.0.0 μέσω **100 ?**.
Το "**100 ?**" σημαίνει ότι το επόμενο AS path είναι το 100 και το origin είναι incomplete και προέρχεται από ένα static route.

Όταν ένα δίκτυο ανακοινώνεται (advertised) με την εντολή network από το BGP πρωτόκολλο τότε το origin attribute εμφανίζεται ως IGP (origin code i).

Δεδομένου ότι το EGP είναι ένα παλαιό πρωτόκολλο το οποίο πλέον δεν χρησιμοποιείται η τιμή (origin code e) είναι απλά ιστορική και δε θα τη δούμε πουθενά να εμφανίζεται.

Τέλος, η τιμή incomplete (origin code ?) σε ένα δίκτυο σημαίνει ότι αυτό έγινε redistributed στο BGP πρωτόκολλο και δεν δηλώθηκε με την εντολή network του BGP πρωτοκόλλου. Για αυτό και η τιμή (origin code ?) θεωρείται λιγότερο αξιόπιστη από την τιμή (origin code i).

4.5.4 BGP Network Command vs. Redistribution



Εικόνα 31: BGP Network vs. Redistribute

Παράδειγμα 1ο

```
RTC#
  router ospf 1
    area 0
    network 175.220.0.0
    redistribute bgp 200  metric 1  subnets

  router bgp 200
    neighbor 1.1.1.1 remote-as 300
    network 175.220.0.0 mask 255.255.0.0
```

Παράδειγμα 2ο

```
RTC#
  router ospf 1
    area 0
    network 175.220.0.0
    redistribute bgp 200  metric 1  subnets

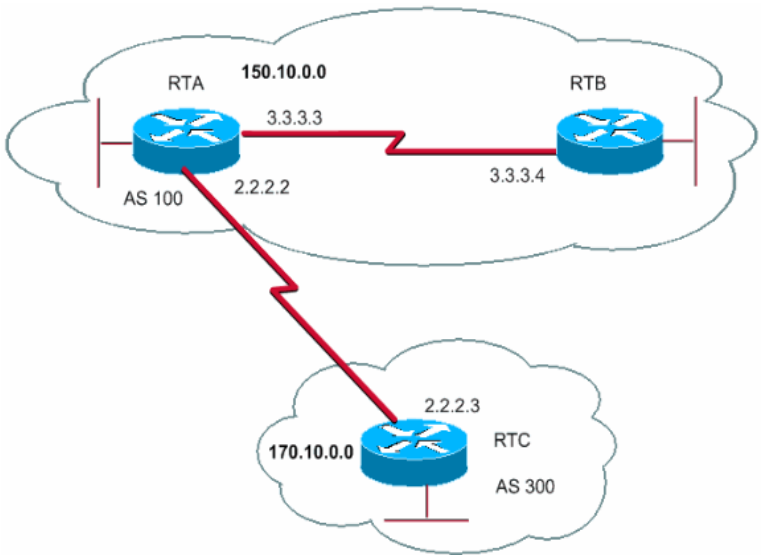
  router bgp 200
    neighbor 1.1.1.1 remote-as 300
    redistribute ospf 1 match internal
```

Όταν σε έναν δρομολογητή ανακοινώνονται δύο ίδιες διαδρομές με τη μοναδική διαφορά ότι η μία προήλθε μέσω της εντολής "network" του BGP πρωτοκόλλου και η άλλη μέσω "redistribute" από άλλο πρωτόκολλο θα προτιμηθεί η πρώτη διαδρομή η οποία θεωρείται πιο αξιόπιστη (BGP Best Path Selection: IGP>incomplete).

Γενικά, καλό είναι να αποφεύγεται η χρήση του "redistribute" διότι υπάρχει καλύτερος έλεγχος με τη χρήση του "network" .

Παρόλα αυτά όταν απαιτείται να ανακοινωθεί μεγάλος αριθμός από prefixes (δίκτυα) η χρήση του "redistribute" είναι βολική. Σε αυτή την περίπτωση όμως μπορεί να χρησιμοποιηθεί ένα route-map για να ελεγχούν τα prefixes που επιθυμούμε να εισαχθούν στο BGP πρωτόκολλο.

4.5.5 BGP Route Maps



Εικόνα 32: Bgp Route Maps

Παράδειγμα 1ο

```
RTA#
  router rip
    network 3.0.0.0
    network 2.0.0.0
    network 150.10.0.0
    passive-interface Serial0
    redistribute bgp 100 route-map SETMETRIC

  router bgp 100
    neighbor 2.2.2.3 remote-as 300
    network 150.10.0.0

  route-map SETMETRIC  permit 10
    match ip-address 1
    set metric 2

  route-map SETMETRIC permit 20
    set metric 5

  access-list 1  permit  170.10.0.0  0.0.255.255
```

Παράδειγμα 2ο

```
RTC#
  router bgp 300
    network 170.10.0.0
    neighbor 2.2.2.2 remote-as 100
    neighbor 2.2.2.2 route-map STOPUPDATES out

  route-map STOPUPDATES permit 10
    match ip address 1

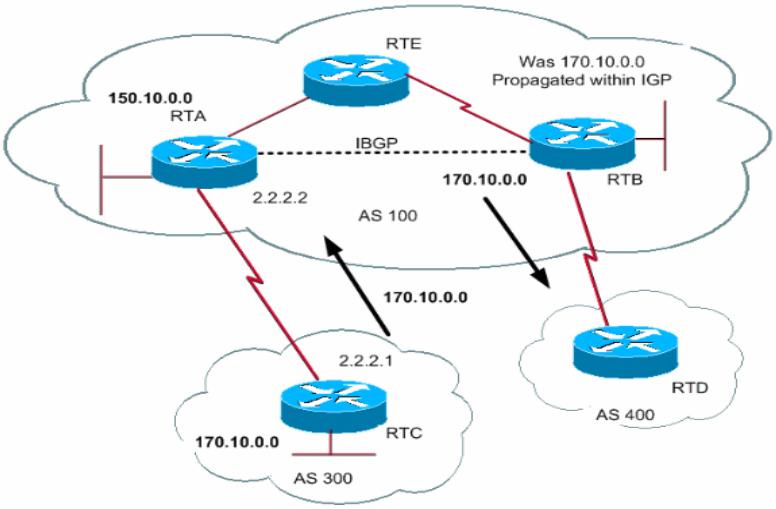
  access-list 1 deny  170.10.0.0  0.0.255.255
  access-list 1 permit  0.0.0.0  255.255.255.255
```

Στο πρώτο παράδειγμα με την εντολή «route-map» δημιουργήσαμε ένα φίλτρο με όνομα «SETMETRIC», το οποίο με τη χρήση του access-list 1 θέτει ως metric το 2 για το δίκτυο 170.10.0.0/16 και metric το 5 σε όλα τα υπόλοιπα δίκτυα. Με τη χρήση του ανωτέρω φίλτρου όταν τα δίκτυα που ανακοινώνονται στο eBGP πρωτόκολλο του δρομολογητή RTA γίνονται "redistribute" στο πρωτόκολλο RIP λαμβάνουν ως metric το 2 ή το 5.

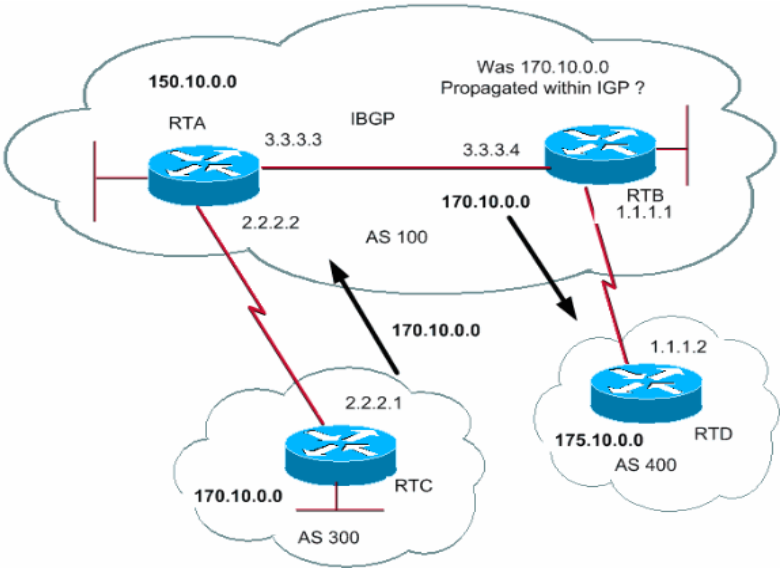
Εξαιτίας του γεγονότος ότι το πρωτόκολλο RIP χρησιμοποιεί ως κόστος διαδρομής (metric) το "hop-count" στο δίκτυο 170.10.0.0/16 που βρίσκεται στο γειτονικό AS300 έχει αποδοθεί ως metric το 2. Γενικά, τα πρωτόκολλα χρησιμοποιούν διαφορετικό αλγόριθμο για τον υπολογισμό του κόστους μιας διαδρομής, οπότε όταν πραγματοποιείται "redistribute" κάποιων διαδρομών από ένα πρωτόκολλο σε κάποιο άλλο θα πρέπει να ορίζεται νέο metric.

Στο δεύτερο παράδειγμα με την εντολή «route-map» δημιουργήσαμε ένα φίλτρο με όνομα «STOPUPDATES», το οποίο με τη χρήση του access-list 1 αποκλείει (deny) το δίκτυο 170.10.0.0/16. Έτσι με την εφαρμογή του εν λόγω φίλτρου στα εξερχόμενα πακέτα του eBGP πρωτοκόλλου του δρομολογητή RTC δεν ανακοινώνεται το δίκτυο 170.10.0.0/16 στον δρομολογητή RTA σε αντίθεση με όλα τα υπόλοιπα δίκτυα τα οποία ανακοινώνονται μιας και γίνονται permit από το access-list 1. Τέλος, όπως παρατηρούμε στα access-lists χρησιμοποιείται η reverse mask.

4.5.6 BGP Synchronization vs. Non-Synchronization



Εικόνα 33: BGP Syncronization



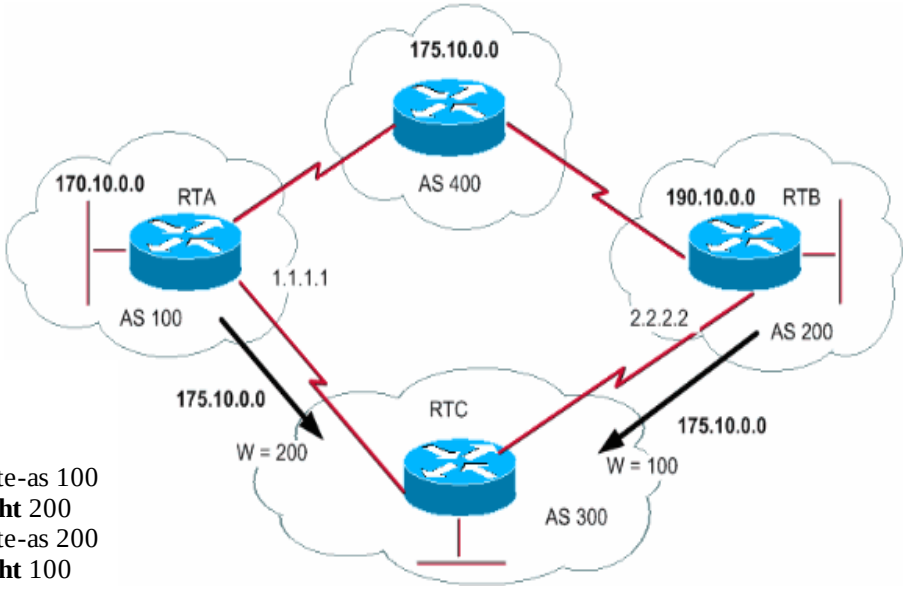
RTB#
router bgp 100
network 150.10.0.0
neighbor 1.1.1.2 remote-as 400
neighbor 3.3.3.3 remote-as 100
no synchronization

Εικόνα 34: BGP Non-Syncronization

Ο συγχρονισμός (synchronization) δηλώνει ότι, εάν ένα AS (εδώ το AS100) μεταφέρει κίνηση από ένα άλλο AS σε ένα τρίτο AS, το BGP δεν θα πρέπει να ανακοινώσει αυτές τις διαδρομές σε εξωτερικούς peers προτού όλοι οι δρομολογητές μέσα στο ίδιο AS μάθουν τις διαδρομές μέσω ενός IGP πρωτοκόλλου. Το BGP περιμένει μέχρι το IGP να διαδώσει αυτές τις διαδρομές εντός του AS και στη συνέχεια τις ανακοινώνει στους εξωτερικούς peers.

Σε ορισμένες περιπτώσεις, δεν χρειάζεστε συγχρονισμός. Εάν δεν περάσετε κίνηση από διαφορετικό AS μέσω του AS σας, μπορείτε να απενεργοποιήσετε το συγχρονισμό. Μπορείτε επίσης να απενεργοποιήσετε το συγχρονισμό εάν όλοι οι δρομολογητές στο AS σας εκτελούν BGP. Η απενεργοποίηση αυτής της δυνατότητας μπορεί να σας επιτρέψει να μεταφέρετε λιγότερες διαδρομές (routes) στο IGP σας και να επιτρέψει στο BGP να συγκλίνει πιο γρήγορα.

4.5.7 BGP Weight Attribute



Εικόνα 35: BGPWeight

Τρόπος Α

```
RTC#
  router bgp 300
    neighbor 1.1.1.1 remote-as 100
    neighbor 1.1.1.1 weight 200
    neighbor 2.2.2.2 remote-as 200
    neighbor 2.2.2.2 weight 100
```

Τρόπος Β

```
RTC#
  router bgp 300
    neighbor 1.1.1.1 remote-as 100
    neighbor 1.1.1.1 filter-list 1 weight 200
    neighbor 2.2.2.2 remote-as 200
    neighbor 2.2.2.2 filter-list 2 weight 100

  ip as-path access-list 1 permit ^100$
  ip as-path access-list 2 permit ^200$
```

Τρόπος Γ

```
RTC#
  router bgp 300
    neighbor 1.1.1.1 remote-as 100
    neighbor 1.1.1.1 route-map SETWEIGHT in
    neighbor 2.2.2.2 remote-as 200
    neighbor 2.2.2.2 route-map SETWEIGHT in

  ip as-path access-list 1 permit ^100$

  route-map SETWEIGHT permit 10
    match as-path 1
    set weight 200

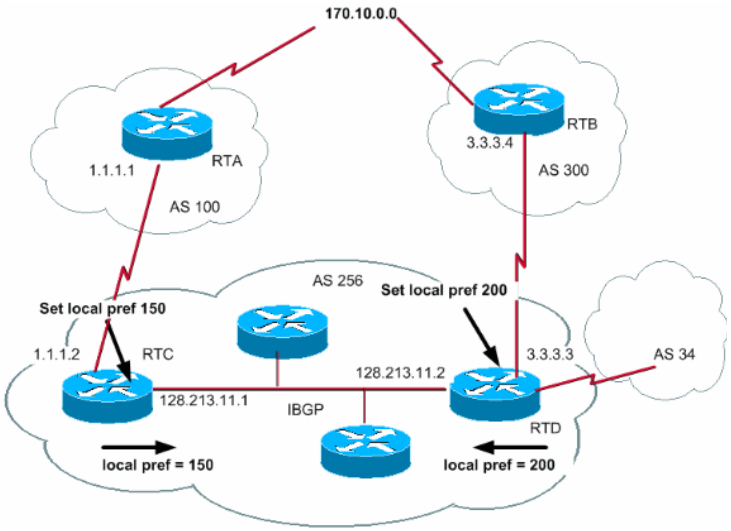
  route-map SETWEIGHT permit 20
    set weight 100
```

Το βαρος (weight) ισχύει μόνο τοπικά σε έναν δρομολογητή, δεν ανταλλάσσεται μεταξύ των BGP δρομολογητών και προτιμάται η διαδρομή με το μεγαλύτερο βάρος.

Στο ανωτέρω παράδειγμα (πολιτική δρομολόγησης) έχει τεθεί στο δρομολογητή RTC weight 200 για τη διασύνδεσή του με το δρομολογητή RTA και weight 100 για τη διασύνδεσή του με το δρομολογητή RTB. Συνεπώς, για το δρομολογητή RTC η διαδρομή μέσω του AS100 (RTA) προτιμάται έναντι της διαδρομής μέσω του AS200 (RTB). Οπότε, όταν ο δρομολογητής RTC μαθαίνει το δίκτυο 175.10.0/16 και από τους δύο neighbors θα προτιμήσει την πρώτη διαδρομή.

Στον πρώτο τρόπο υλοποίησης της ανωτέρω πολιτικής οι βαρύτητες των διαδρομών (weights) έχουν τεθεί απευθείας στις δηλώσεις των neighbors. Στο δεύτερο τρόπο υλοποίησης έχουν δημιουργηθεί δύο filter-lists με βάση το as-path μέσω των οποίων αποδίδονται οι βαρύτητες των διαδρομών (weights). Στον τρίτο τρόπο υλοποίησης έχουν δημιουργηθεί δύο route-maps στα εισερχόμενα πακέτα του δρομολογητή RTC όπου βάση του as-path αποδίδονται βαρύτητες (weights) στις διαδρομές. Στα access-lists το σύμβολο ^ δηλώνει την αρχή της συμβολοσειράς εισόδου, ενώ το σύμβολο $ δηλώνει τέλος της συμβολοσειράς εισόδου.

4.5.8 BGP Local Preference Attribute



Εικόνα 36: BGP Local Preference

```
RTC#
  router bgp 256
    neighbor 1.1.1.1 remote-as 100
    neighbor 128.213.11.2 remote-as 256
    bgp default local-preference 150

RTD#
  router bgp 256
    neighbor 3.3.3.4 remote-as 300
    neighbor 3.3.3.4 route-map SETLOCAL in
    neighbor 128.213.11.1 remote-as 256

  ip as-path access-list 1 permit ^300$

  route-map SETLOCAL permit 10
    match as-path 1
    set local-preference 200

  route-map SETLOCAL permit 20
    set local-preference 150
```

Το χαρακτηριστικό τοπικής προτίμησης (local preference attribute) υποδεικνύει ποια διαδρομή θα χρησιμοποιηθεί για έξοδο από το AS. Αποτελεί ένα γνωστό διακριτικό χαρακτηριστικό που χρησιμοποιείται μεταξύ ομοτίμων (peers) iBGP και δεν μεταβιβάζεται σε εξωτερικούς ομοτίμους BGP. Η προεπιλεγμένη τοπική προτίμηση (default local preference) είναι 100 και προτιμάται πάντοτε η υψηλότερη τιμή τοπικής προτίμησης.

Σε αντίθεση με το χαρακτηριστικό βάρους (weight attribute), το χαρακτηριστικό τοπικής προτίμησης (local preference attribute) διαδίδεται σε όλο το τοπικό AS. Εάν υπάρχουν πολλά σημεία εξόδου από το AS, το χαρακτηριστικό τοπικής προτίμησης χρησιμοποιείται για την επιλογή του σημείου εξόδου για μια συγκεκριμένη διαδρομή (route).

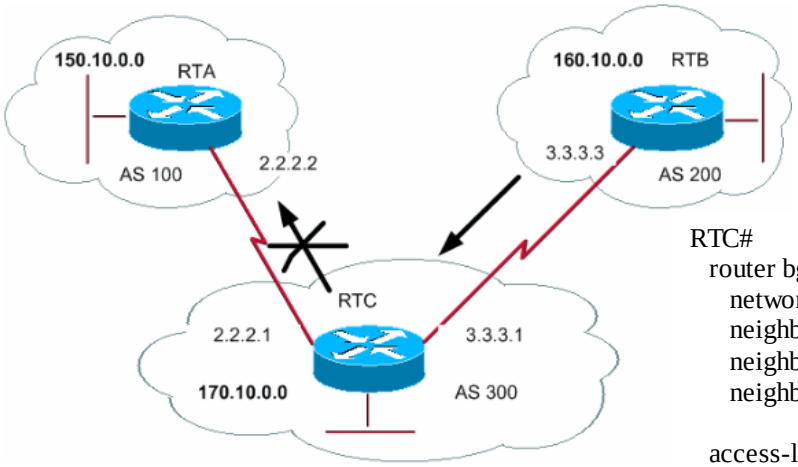
Όπως παρατηρούμε στο ανωτέρω παράδειγμα για το AS256 υπάρχουν δύο σήμεια εξόδου (δρομολογητές RTC και RTD). Το πρώτο σημείο εξόδου συνδέεται με το AS100, ενώ το δεύτερο σημείο εξόδου συνδέεται με τα AS300 και AS34.

Στο πρώτο σημείο εξόδου (δρομολογητής RTC) έχει δηλωθεί ως default local-preference το 150, ενώ στο δεύτερο σημείο εξόδου (δρομολογητής RTD) έχει εφαρμοστεί ένα route-map με όνομα SETLOCAL στα εισερχόμενα πακέτα που προέρχονται από το δρομολογητή RTB, βάση του οποίου στις διαδρομές που προέρχονται από το AS 300 προσδίδεται local preference 200 και στις υπόλοιπες local preference 150.

Συνεπώς, αν κάποιος που βρίσκεται εντός του AS256 θέλει να προσεγγίσει ένα οποιοδήποτε δίκτυο το οποίο ανήκει στο AS300 θα ακολουθήσει το δεύτερο σημείο εξόδου το οποίο έχει υψηλότερη τιμή στο local preference attribute.

Αντίθετα, αν κάποιος που βρίσκεται εντός του AS 256 θέλει να προσεγγίσει το δίκτυο 170.10.0.0/16 θα διαπιστώσει ότι υπάρχουν δύο σημεία εξόδου, αλλά η τιμή του local preference attribute είναι η ίδια (150) και για τα δύο σημεία εξόδου. Οπότε σε αυτή την περίπτωση θα ληφθούν υπόψην και άλλοι παράμετρες, όπως το as-path.

4.5.9 BGP Route Filtering



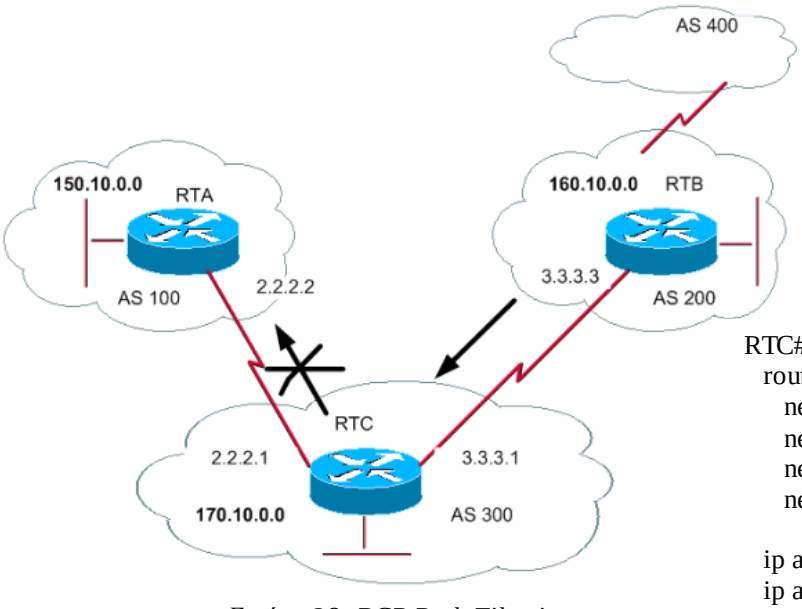
Εικόνα 37: BGP Route Filtering

```
RTC#
  router bgp 300
    network 170.10.0.0
    neighbor 3.3.3.3 remote-as 200
    neighbor 2.2.2.2 remote-as 100
    neighbor 2.2.2.2 distribute-list 1 out

  access-list 1 deny  160.10.0.0  0.0.255.255
  access-list 1 permit  0.0.0.0  255.255.255.255
```

Στο ανωτέρω παράδειγμα έχει δημιουργεί ένα φίλτρο στα εξερχόμενα πακέτα του δρομολογητή RTC προς το δρομολογητή RTA μέσω του οποίου απογορεύεται η ανακοίνωση του δικτύου 160.10.0.0/16 από το δρομολογητή RTC στο δρομολογητή RTA. Έτσι, οι δρομολογητές που βρίσκονται εντός του AS100 δεν θα γνωρίζουν την ύπαρξη του δικτύου 160.10.0.0/16.

4.5.10 BGP Path Filtering



Εικόνα 38: BGP Path Filtering

```
RTC#
  router bgp 300
    network 170.10.0.0
    neighbor 3.3.3.3 remote-as 200
    neighbor 2.2.2.2 remote-as 100
    neighbor 2.2.2.2 filter-list 1 out

  ip as-path access-list 1 deny ^200$
  ip as-path access-list 1 permit .*
```

Στο ανωτέρω παράδειγμα έχει δημιουργεί ένα φίλτρο στα εξερχόμενα πακέτα του δρομολογητή RTC προς το δρομολογητή RTA, όπου με βάση το as-path απογορεύεται η ανακοίνωση όσων δικτύων προέρχονται από το AS200, ενώ επιτρέπεται η ανακοίνωση όλων των υπολοίπων. Έτσι, οι δρομολογητές

που βρίσκονται εντός του AS100 δεν θα γνωρίζουν την ύπαρξη του δικτύου 160.10.0.0/16 που βρίσκεται εντός του AS200, ενώ αντίθετα θα γνωρίζουν όλα τα δίκτυα που βρίσκονται εντός του AS400.

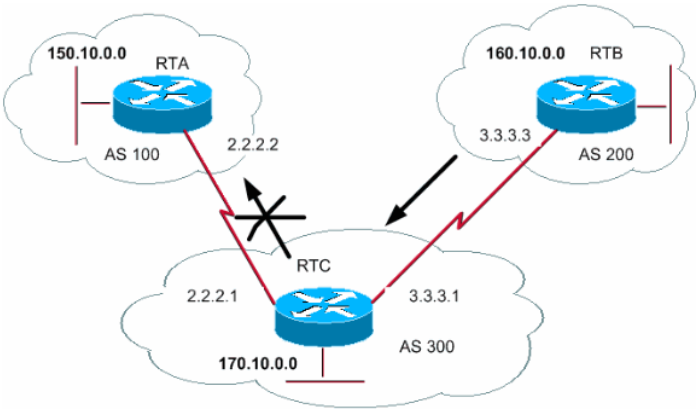
Στη συνέχεια επεξηγούμε όλους τους συμβολισμούς του as-path.

Ατομικός (atom)
. ένας απλός χαρακτήρας.
^ αρχή συμβολοσειράς εισόδου.
$ τέλος συμβολοσειράς εισόδου.
_ κόμμα (,), αριστερό άγκιστρο ({), δεξί άγκιστρο (}), αρχή συμβολοσειράς εισόδου, τέλος συμβολοσειράς εισόδου ή κενό.

Ομάδα
* 0 ή περισσότερες ακολουθίες atom.
+ 1 ή περισσότερες ακολουθίες atom.
? atom ή null συμβολοσειρά.

Έκφραση	Έννοια
.*	Οτιδήποτε
^$	Τοπικές διαδρομές (locally originated routes)
^100_	Μαθαίνονται από το AS100 (learned from AS100)
_100$	Προέρχονται από το AS100 (originated in AS100)
_100_	Περιλαμβάνουν το AS100 (any instance of AS100)
^[0-9]+$	Απευθείας Συνδεδεμένα ASes (directly connected ASes)

4.5.11 BGP Community Filtering



Εικόνα 39: BGP Community

<u>Σενάριο Α</u>

RTB#
router bgp 200
network 160.10.0.0
neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 **send-community**
neighbor 3.3.3.1 **route-map SETCOMMUNITY** out

route-map **SETCOMMUNITY**
match ip address 1
set community **no-export**

access-list 1 permit 0.0.0.0 255.255.255.255

Στο πρώτο σενάριο έχει δημιουργηθεί ένα route-map με όνομα SETCOMMUNITY το οποίο θέτει ως community το no-export σε όλες τις διαδρομές (routes) και εφαρμόζεται στα εξερχόμενα πακέτα του δρομολογητή RTB προς το δρομολογητή RTC. Με αυτόν τον τρόπο δεν ανακοινώνεται από το δρομολογητή RTC κανένα δίκτυο στο δρομολογητή RTA, διότι ο RTA είναι ένας εξωτερικός peer.

Σενάριο Β

```
RTB#
  router bgp 200
    network 160.10.0.0
    neighbor 3.3.3.1 remote-as 300
    neighbor 3.3.3.1 send-community
    neighbor 3.3.3.1 route-map SETCOMMUNITY out

  route-map SETCOMMUNITY
    match ip address 1
    set community 100 200 additive

  access-list 1 permit 0.0.0.0 255.255.255.255

RTC#
  router bgp 300
    neighbor 2.2.2.2 remote-as 100
    neighbor 3.3.3.3 remote-as 200
    neighbor 3.3.3.3 route-map CHECK-COMMUNITY in

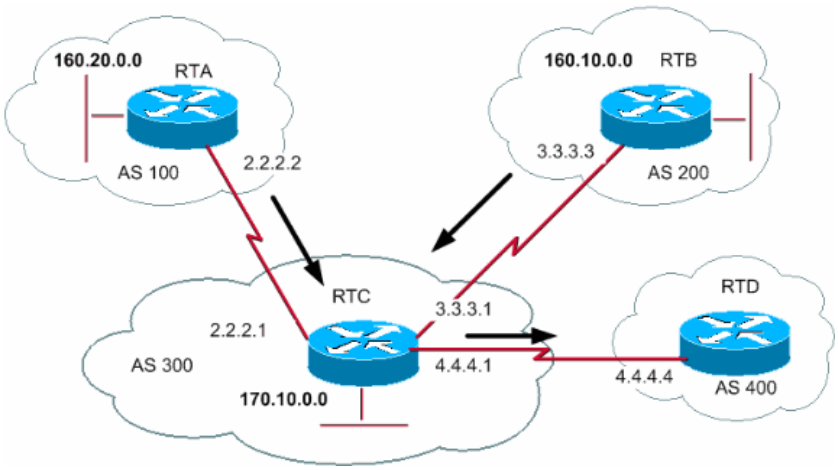
  route-map CHECK-COMMUNITY permit 10
    match community 1
    set weight 20
  route-map CHECK-COMMUNITY permit 20
    match community 2 exact
    set weight 10
  route-map CHECK-COMMUNITY permit 30
    match community 3
    set weight 5

  ip community-list 1 permit 100
  ip community-list 2 permit 200
  ip community-list 3 permit internet
```

Στο δεύτερο σενάριο έχει δημιουργηθεί ένα route-map με όνομα SETCOMMUNITY το οποίο προσθέτει στα ήδη υπάρχοντα communities τα 100 και 200 σε όλες τις διαδρομές (routes) και εφαρμόζεται στα εξερχόμενα πακέτα του δρομολογητή RTB προς το δρομολογητή RTC. Στη συνέχεια έχει δημιουργηθεί ένα route-map με όνομα CHECKCOMMUNITY το οποίο θέτει weight=20 σε όλες τις διαδρομές των οποίων ένα από τα communities είναι το 100, weight=10 στις διαδρομές που διαθέτουν ένα ακριβώς community το 200 και weight=5 σε όλες τις υπόλοιπες διαδρομές του διαδικτύου. Τέλος, το route-map με όνομα CHECKCOMMUNITY εφαρμόζεται στα εισερχόμενα πακέτα του δρομολγητή RTC που ανακοινώνονται από τον δρομολογητή RTB. Αυτό έχει ως αποτέλεσμα όλες οι διαδρομές που ανακοινώνονται από τον δρομολογητή RTB στον δρομολογητή RTC να λαμβάνουν weight=20 μιας και ένα από τα communities που διαθέτουν είναι το 100. Προφανώς, το route-map CHECKCOMMUNITY είναι γενικό και έχει σχεδιαστεί με σκοπό να εφαρμοστεί και σε άλλους peers του δρομολγητή RTC. Τελος, ακολουθεί πίνακας με ανάλυση των σημαντικότερων communities.

none	Δηλώνει ότι δεν υπάρχει community.
aa : nn	Δηλώνει τον αριθμό AS και τον αριθμό δικτύου σε ένα 4-byte new community format. Αυτή η τιμή απαρτίζεται από δύο αριθμούς των 2-byte ο καθένας χωρισμένοι με το σύμβολο :
additive	Προσθέτει ένα νέο community στα ήδη υπάρχοντα.
local-as	Τα δίκτυα ανακοινώνονται μόνο στους τοπικούς και όχι στους εξωτερικούς peers. Μπορεί όμως να εφαρμοστεί και σε επίπεδο sub-ASes.
no-advertise	Τα δίκτυα δεν ανακοινώνονται ούτε στους τοπικούς ούτε στους εξωτερικούς peers.
no-export	Τα δίκτυα ανακοινώνονται μόνο στους τοπικούς και όχι στους εξωτερικούς peers.

4.5.12 BGP Classless InterDomain Routing (CIDR) and Aggregate Addresses



Εικόνα 40: BGP CIDR

Τρόπος Α

RTC#
```
router bgp 300
  neighbor 3.3.3.3 remote-as 200
  neighbor 2.2.2.2 remote-as 100
  neighbor 4.4.4.4 remote-as 400
  aggregate 160.0.0.0 255.0.0.0 summary-only
```

Τρόπος Β

RTC#
```
router bgp 300
  neighbor 3.3.3.3 remote-as 200
  neighbor 2.2.2.2 remote-as 100
  neighbor 4.4.4.4 remote-as 400
  aggregate 160.0.0.0 255.0.0.0 summary-only
  aggregate 160.0.0.0 255.0.0.0 as-set
```

RTB#
```
router bgp 200
  network 160.10.0.0
  neighbor 3.3.3.1 remote-as 300
```

RTA#
```
router bgp 100
  network 160.20.0.0
  neighbor 2.2.2.1 remote-as 300
```

Στον πρώτο τρόπο υλοποίησης με την εντολή **aggregate 160.0.0.0 255.0.0.0 summary-only** ο δρομολογητής RTC στέλνει στον δρομολογητή RTD ενημερώσεις για το δίκτυο 160.0.0.0/8, χωρίς να παρέχεται η ένδειξη ότι το δίκτυο αυτό προέρχεται στην πραγματικότητα από δύο διαφορετικά ASes. Το γεγονός όμως αυτό μπορεί να δημιουργήσει βρόχους (loops) εάν ο δρομολογητής RTD διαθέτει μια εγγραφή προς το AS100 ή το AS200.

Στο δεύτερο τρόπο υλοποίησης με την προσθήκη της εντολής **aggregate 160.0.0.0 255.0.0.0 as-set** ο δρομολογητής RTC στέλνει στον δρομολογητή RTD ενημερώσεις για το δίκτυο 160.0.0.0/8, παρέχοντας όμως την ένδειξη ότι το δίκτυο αυτό προέρχεται στην πραγματικότητα από δύο διαφορετικά ASes (συγκεκριμένα ότι ανήκει στο set ASes{100,200}) με αποτέλεσμα την αποφυγή δημιουργίας βρόχων (loops).

5

Προσομοιωτής GNS3

Το GNS3 (Graphical Network Simulator 3) είναι ένα open-source λογισμικό που μας επιτρέπει τη δημιουργία, προσομοίωση και δοκιμή δικτύων όσο το δυνατόν πιο κοντά σε ένα πραγματικό test bed. Παρέχεται δωρεάν στους χρήστες και μπορεί να εγκατασταθεί σε λειτουργικά συστήματα Windows, Mac και Linux.



`

Το GNS3 δημιουργήθηκε από τον Jeremy Grossmann ο οποίος αρχικά συγκέντρωσε έναν αριθμό εφαρμογών όπως το Dynamips και τα εισήγαγε σε ένα φιλικό προς τον χρήστη περιβάλλον, κυρίως για να μπορεί να τρέχει Cisco IOS images, στην πορεία όμως το GNS3 αναβαθμίστηκε και σήμερα μπορεί να υποστηρίζει λογισμικό της Juniper, της Mikrotik, της ανοιχτής πλατφόρμας δρομολόγησης FRR και διάφορων άλλων δημοφιλών εταιρειών δικτύωσης.

Το GNS3 έχει τη δυνατότητα να χρησιμοποιεί διάφορα Virtual Machines, όπως το VMWare Workstation Pro και το VirtualBox σε εγκαταστάσεις που λειτουργούν πάνω σε σχετικά ελαφριά λειτουργικά συστήματα και χάρη σε αυτό μπορούμε να γεφυρώσουμε την κάρτα δικτύου του PC μας για να εκτελέσουμε σενάρια ακόμα πιο κοντά στην πραγματικότητα.

Οι εφαρμογές που έχουν ενσωματωθεί στο GNS3 όπως τα Dynamips, QEMU, VirtualBox, VPCS κ.α. παρέχουν ένα ολοκληρωμένο περιβάλλον σχεδίασης δικτύων. Το Dynamips χρησιμοποιείται για την εξομοίωση συσκευών, όπως δρομολογητές Cisco των σειρών 2600, 3600, 3700 και 7200. Τα QEMU και VirtualBox ως Virtual Machines βοηθούν στη δοκιμή και στον έλεγχο λειτουργίας πραγματικών λειτουργικών συστημάτων σε ένα δίκτυο, ενώ το VPCS αποτελεί μια απλή εικονική αναπαράσταση ενός υπολογιστή ικανή να εκτελέσει απλές λειτουργίες, όπως η χρήση της εντολής ping και DHCP.

Υπάρχουν πολλοί λόγοι για τους οποίους το GNS3 έχει γίνει δημοφιλές, όπως το να στήσουμε ευκολότερα ένα δίκτυο για λόγους εκπαίδευσης, δεδομένου ότι η αγορά ή η ενοικίαση δικτυακού εξοπλισμού αποτελεί σημαντική οικονομική επιβάρυνση αλλά και ρίσκο. Επιπλέον, το γραφικό περιβάλλον που παρέχεται από το GNS3 διευκολύνει τους διαχειριστές, τους τεχνικούς δικτύων και τους φοιτητές στη σχεδίαση και υλοποίηση δικτυακών σεναρίων χωρίς περιορισμούς. Η δημιουργία τέτοιων προσομοιωτών δικτύων με πλούσιο γραφικό περιβάλλον άλλαξαν κυριολεκτικά την τελευταία δεκαετία τον τρόπο μάθησης των δικτύων. Σήμερα η κοινότητα του GNS3 αποτελείται από πάνω από 800.000 μέλη [9] τα οποία μπορούν να εμπλουτίσουν και να δοκιμάσουν τις γνώσεις τους δημιουργώντας μια τεράστια κοινότητα φοιτητών και τεχνικών, η οποία βοηθά ενεργά στην εξέλιξη και την υποστήριξη του.

5.1 Αρχιτεκτονική GNS3

Το λογισμικό GNS3 αποτελείται από τα ακόλουθα δύο τμήματα [11]:

- Τμήμα Πελάτη: Πρόκειται για το λογισμικό GNS3-all-in-one (GUI) που παρέχει ένα γραφικό περιβάλλον χρήστη, όπου μπορούν να δημιουργηθούν διάφορες τοπολογίες δικτύων.
- Τμήμα Διακομιστή: Αποτελείται από την εικονική μηχανή GNS3 (VM)

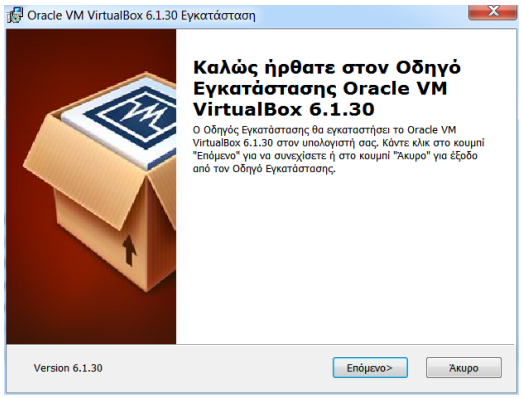
Όσον αφορά την επιλογή του διακομιστή υπάρχουν τρείς δυνατότητες:

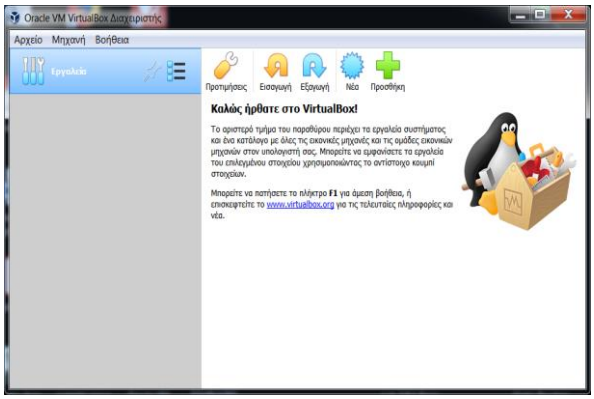
- Τοπικός διακομιστής GNS3: εκτελείται τοπικά στον ίδιο υπολογιστή που έγινε εγκατάσταση του λογισμικού GNS3 all-in-one.
- Τοπικό GNS3 VM: μπορεί να εκτελεστεί στον ίδιο Η/Υ χρησιμοποιώντας λογισμικό εικονικοποίησης όπως VMware Workstation ή VirtualBox. Αυτή είναι και η προτεινόμενη εγκατάσταση που θα χρησιμοποιηθεί και στη διπλωματική εργασία.
- Απομακρυσμένο GNS3 VM: εκτελεστεί από απόσταση σε ένα διακομιστή το οποίο χρησιμοποιεί το VMware ESXi ή στο Cloud.

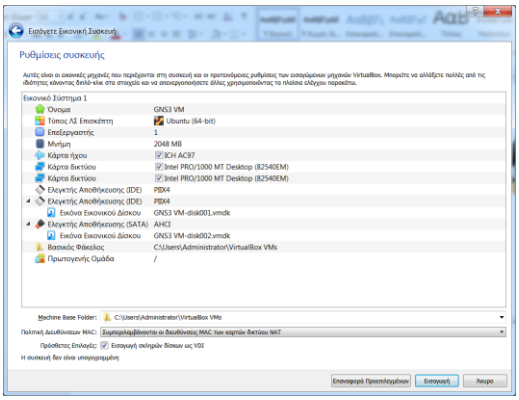
5.2 Εγκατάσταση και Διαμόρφωση Προσομοιωτή GNS3

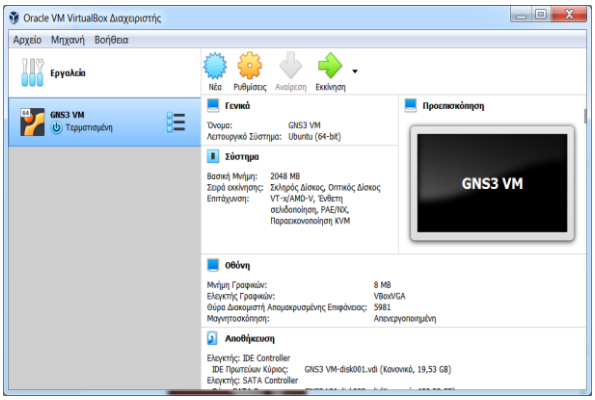
Από την επίσημη σελίδα του GNS3 [10] μπορούμε να κατεβάσουμε και να ανοίξουμε το αντίστοιχο εκτελέσιμο αρχείο για το λειτουργικό σύστημα που επιθυμούμε, το οποίο φυσικά μας παρέχεται χωρίς χρέωση, αφού πρώτα εγγραφούμε στο σύστημα. Οδηγίες εγκατάστασης μπορούμε να βρούμε τόσο στο σχετικό documentation του GNS3 [11] όσο και σε διάφορους συνδέσμους όπως https://www.youtube.com/watch?v=SqgDn0YezoI.

Καλό θα ήταν πριν ξεκινήσουμε την εγκατάσταση του GNS3 να έχουμε εγκαταστήσει έναν Virtual Machine Player π.χ. το Virtual Box [12] και στη συνέχεια να φορτώσουμε (επιλέγοντας εισαγωγή συσκευής) το αντίστοιχο GNS3 VM [13].





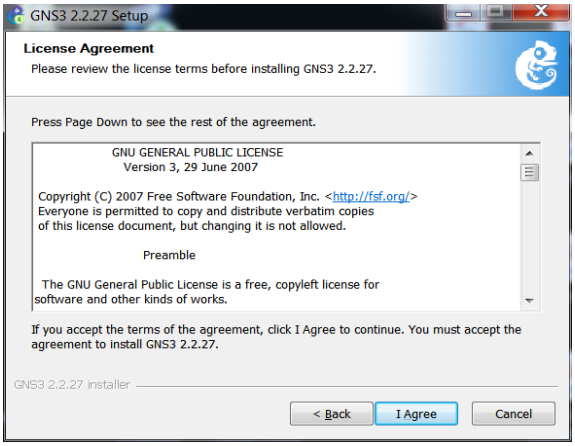


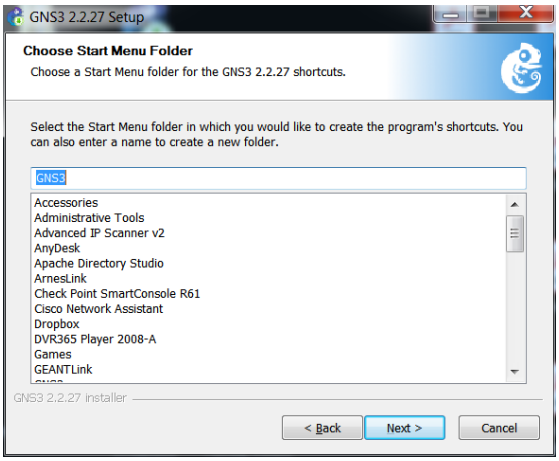


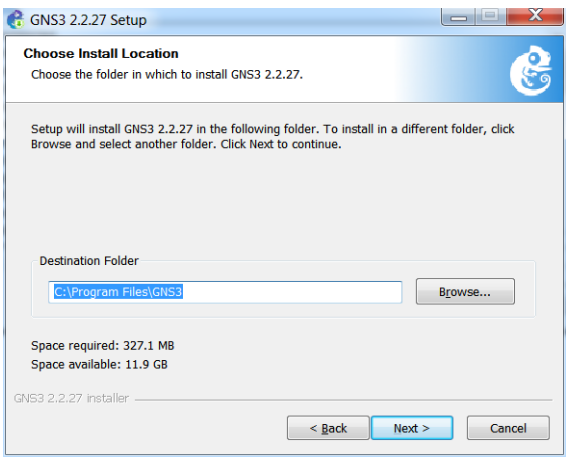
Κατά την εγκατάσταση του GNS3 σε περιβάλλον Windows στην επιλογή των Components μας παρέχονται οι εξής οδηγοί: Local Installation, Web Ui – GNS3VM (beta) ή Custom. Επιλέγουμε τοπική εγκατάσταση. Το GNS3 VM θα το φορτώσουμε στη συνέχεια, αφού πρώτα πραγματοποιηθεί η εγκατάσταση του GNS3 στον τοπικό μας Η/Υ.

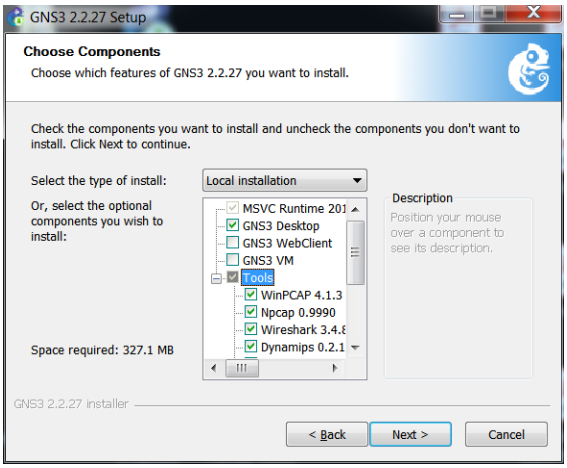
Επιπλέον, η εγκατάσταση μας δίνει την επιλογή αν επιθυμούμε το GNS3 να ξεκινά παράλληλα και άλλα προγράμματα όπως τα WinPcap, Wireshark και Solar-PuTTY. Ακολουθούν τα βήματα εγκατάστασης του GNS3 στον τοπικό μας Η/Υ.

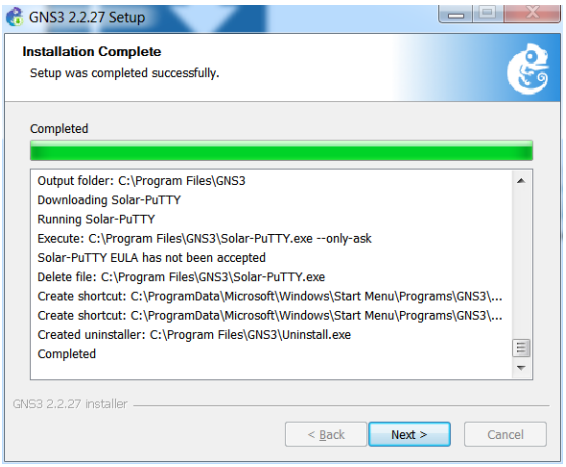


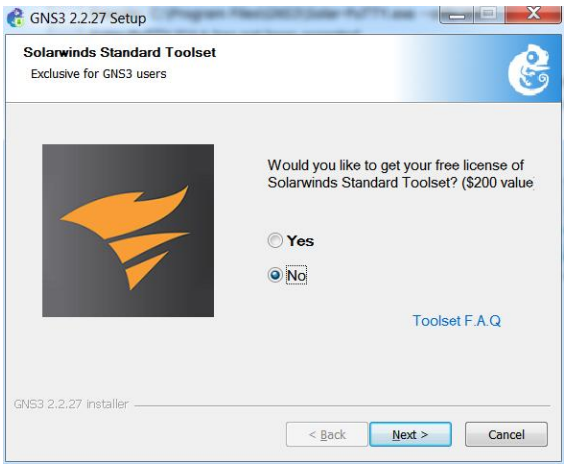






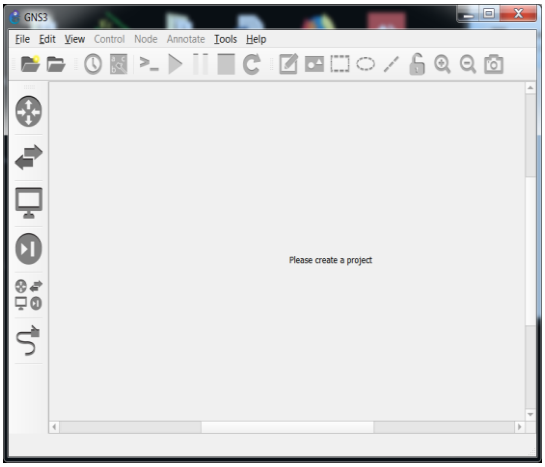


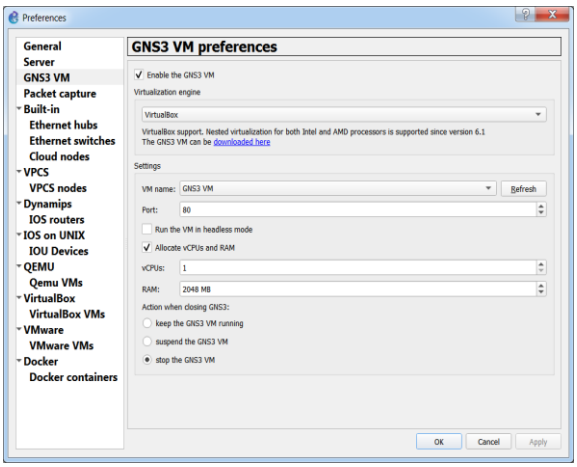




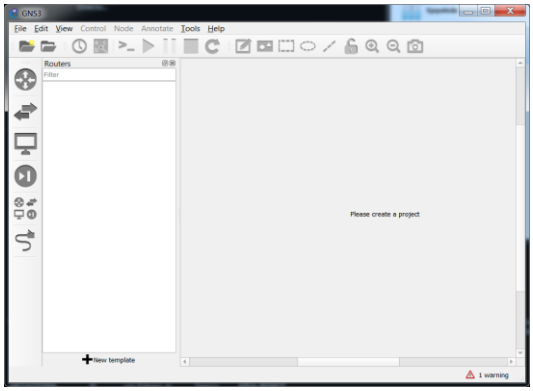


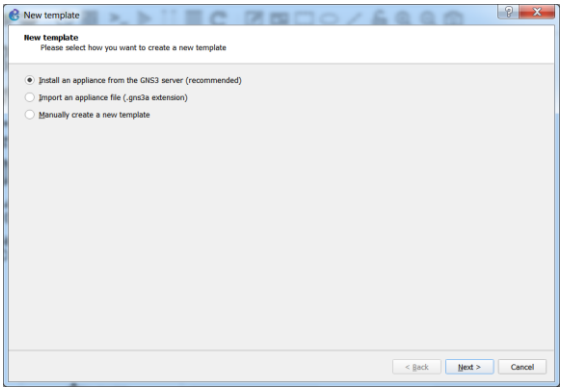
Όταν η εγκατάσταση ολοκληρωθεί μπορούμε να ανοίξουμε το GNS3. Στη συνέχεια από την επιλογή Edit -> Preferences ενεργοποιούμε το virtual machine που έχουμε επιλέξει και φορτώσει προηγουμένως.

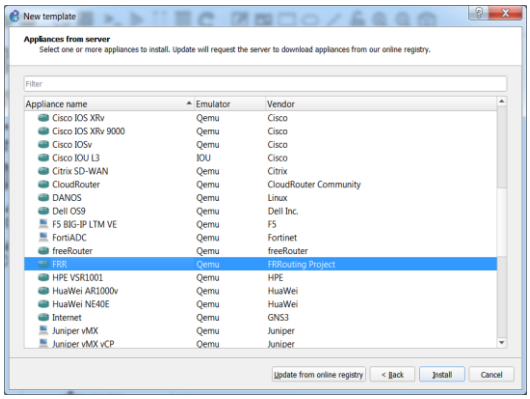


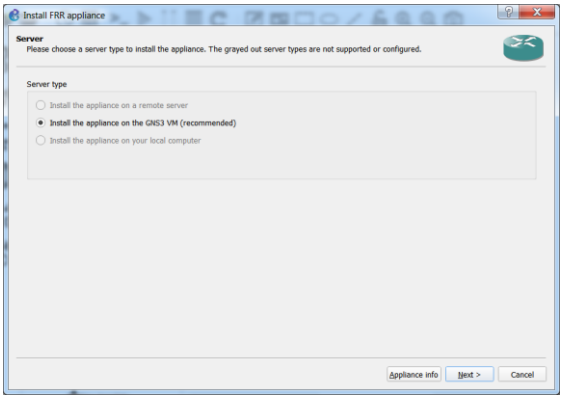


Τέλος, φορτώνουμε στο GNS3 VM ως appliance το δρομολογητή FRR ακολουθώντας τα παρακάτω βήματα.









6

Μελέτη Περιπτώσεων Δρομολόγησης με Χρήση της Σουίτας FRR

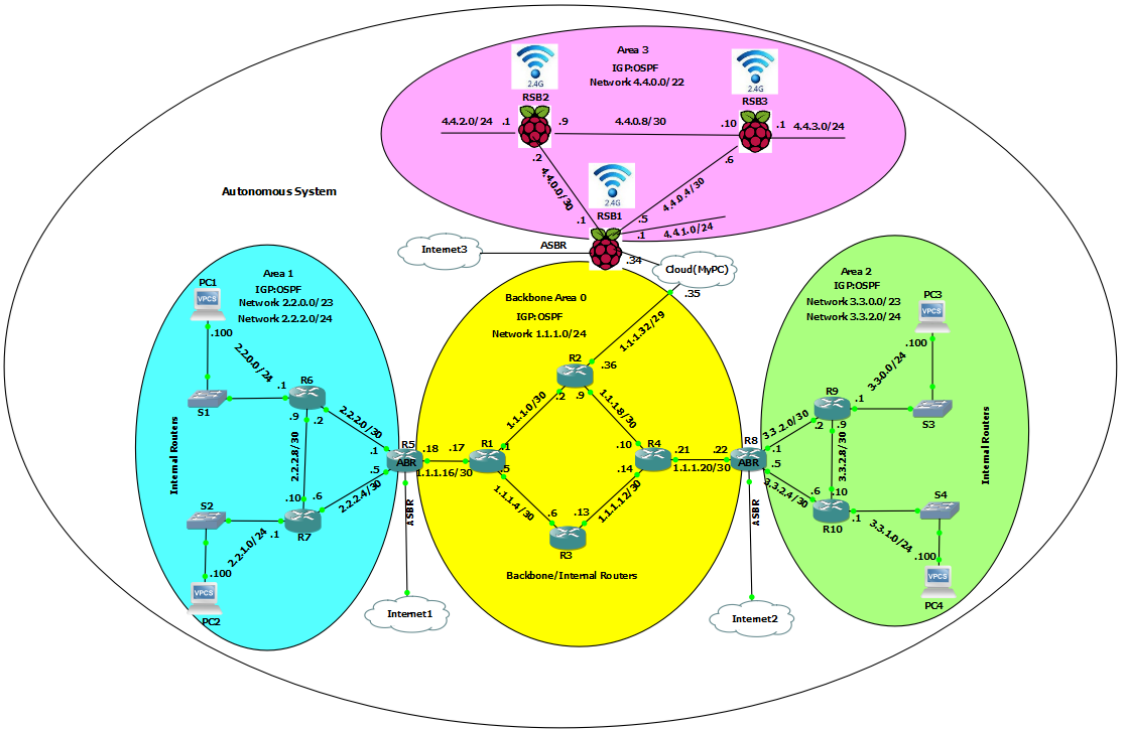
Η μελέτη περίπτωσεων δρομολόγησης της σουίτας FRR περιλαμβάνει την εγκατάσταση και τη διευθέτηση των πρωτοκόλλων OSPF και BGP τόσο σε μια συσκευή Raspberry Pi 4 όσο και στον προσομοιωτή GNS3.

Από τη σουίτα πρωτοκόλλων δρομολόγησης FRR επιλέξαμε να μελετήσουμε και να αναλύσουμε τη συμεριφορά του κυριότερου IGP πρωτοκόλλου - του OSPF - εντός των ορίων ενός Autonomous System (AS), καθώς και τη συμπεριφορά του μοναδικού EGP πρωτοκόλλου - του BGP - που χρησιμοποιείται για την πραγματοποίηση των πολιτικών δρομολόγησης της κίνησης των πακέτων διαμέσου των διάφορων ανά τον κόσμο AS.

6.1 Μελέτη Περίπτωσης Πρωτοκόλλου Δρομολόγησης OSPF Σουίτας FRR

Η μελέτη περίπτωσης του πρωτοκόλλου OSPF της σουίτας FRR περιλαμβάνει την εγκατάσταση και διευθέτηση του εν λόγω πρωτοκόλλου σε τρεις συσκευές Raspberry Pi 4 οι οποίες μέσω cloud διασυνδέονται με άλλους δέκα OSPF δρομολογητές της σουίτας FRR που έχουν εγκατασταθεί και λειτουργούν με τη χρήση του προσομοιωτή GNS3. Στην παρούσα μελέτη περίπτωσης έχει χρησιμοποιηθεί ένα υβριδικό περιβάλλον μεταξύ πραγματικών συσκευών δρομολόγησης και αντίστοιχων συσκευών που έχουν εγκατασταθεί στον προσομοιωτή GNS3 για λόγους οικονομίας και ευελιξίας. Αναλυτικότερα, μελετούμε τη συμπεριφορά του ιεραρχικού πρωτοκόλλου OSPF σε ένα σχήμα που απαρτίζεται από δεκατρείς δρομολογητές που ανήκουν σε τέσσερις διαφορετικές περιοχές.

Στη συνέχεια ακολουθούν οι διευθετήσεις (configurations) του πρωτοκόλλου OSPF και των δεκατριών δρομολογητών της μελέτης περίπτωσης, καθώς και η ανάλυση των αντίστοιχων πινάκων δρομολόγησης.



Εικόνα 41: Μελέτη Περίπτωσης Πρωτοκόλλου OSPF

6.1.1 Διευθέτηση Δρομολογητή R1

R1# show running-config
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R1
service integrated-vtysh-config
!
interface eth0
 description Point-to-Point Connection with R5
 ip address 1.1.1.17/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth1
 description Point-to-Point Connection with R2
 ip address 1.1.1.1/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth2
 description Point-to-Point Connection with R3
 ip address 1.1.1.5/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
router ospf
 network 1.1.1.0/30 area 0

```
 network 1.1.1.4/30 area 0
 network 1.1.1.16/30 area 0
 area 0 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής R1 ανήκει στο δίκτυο κορμού (backbone area 0). Μέσω των διεπαφών eth0, eth1 και eth2 συνδέεται με τους δρομολογητές R5, R2 και R3 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY1.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R1. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 0, και συγεκριμένα του δικτύου 1.1.1.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή R5 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R1 αποκτά πρόσβαση σε όλο το διαδίκτυο.

```
R1#  show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 1.1.1.18, eth0, 00:05:16
O   1.1.1.0/30 [110/100] is directly connected, eth1, 00:06:28
C>* 1.1.1.0/30 is directly connected, eth1, 00:06:32
O   1.1.1.4/30 [110/100] is directly connected, eth2, 00:06:28
C>* 1.1.1.4/30 is directly connected, eth2, 00:06:32
O>* 1.1.1.8/30 [110/200] via 1.1.1.2, eth1, 00:05:30
O>* 1.1.1.12/30 [110/200] via 1.1.1.6, eth2, 00:05:38
O   1.1.1.16/30 [110/100] is directly connected, eth0, 00:05:27
C>* 1.1.1.16/30 is directly connected, eth0, 00:06:32
O>* 1.1.1.20/30 [110/300] via 1.1.1.2, eth1, 00:05:14
  *                       via 1.1.1.6, eth2, 00:05:14
O>* 1.1.1.32/29 [110/200] via 1.1.1.2, eth1, 00:05:30
O>* 2.2.0.0/23 [110/300] via 1.1.1.18, eth0, 00:05:17
O>* 2.2.2.0/24 [110/300] via 1.1.1.18, eth0, 00:05:17
O>* 3.3.0.0/23 [110/500] via 1.1.1.2, eth1, 00:05:11
  *                       via 1.1.1.6, eth2, 00:05:11
O>* 3.3.2.0/24 [110/500] via 1.1.1.2, eth1, 00:05:11
  *                       via 1.1.1.6, eth2, 00:05:11
O>* 4.4.0.0/22 [110/400] via 1.1.1.2, eth1, 00:05:30
```

6.1.2 Διευθέτηση Δρομολογητή R2

R1# show running-config
Building configuration...

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R2
service integrated-vtysh-config
!
interface eth0
 description Connection with Raspberry RSB1
 ip address 1.1.1.36/29
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth1
 description Point-to-Point Connection with R1
 ip address 1.1.1.2/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth2
 description Point-to-Point Connection with R4
 ip address 1.1.1.9/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
router ospf
 network 1.1.1.0/30 area 0
 network 1.1.1.8/30 area 0
 network 1.1.1.32/29 area 0
 area 0 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής R2 ανήκει στο δίκτυο κορμού (backbone area 0). Μέσω των διεπαφών eth0, eth1 και eth2 συνδέεται με τους δρομολογητές RSB1, R1 και R4 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY1.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R2. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 0, και συγεκριμένα του δικτύου 1.1.1.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF των δρομολογητών RSB1 και R8 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R2 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R2# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
```

```
      > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 1.1.1.1, eth1, 00:00:10
  *                    via 1.1.1.10, eth2, 00:00:10
O    1.1.1.0/30 [110/100] is directly connected, eth1, 00:13:47
C>* 1.1.1.0/30 is directly connected, eth1, 00:13:53
O>* 1.1.1.4/30 [110/200] via 1.1.1.1, eth1, 00:12:57
O    1.1.1.8/30 [110/100] is directly connected, eth2, 00:13:47
C>* 1.1.1.8/30 is directly connected, eth2, 00:13:53
O>* 1.1.1.12/30 [110/200] via 1.1.1.10, eth2, 00:12:40
O>* 1.1.1.16/30 [110/200] via 1.1.1.1, eth1, 00:12:57
O>* 1.1.1.20/30 [110/200] via 1.1.1.10, eth2, 00:12:40
O    1.1.1.32/29 [110/100] is directly connected, eth0, 00:13:47
C>* 1.1.1.32/29 is directly connected, eth0, 00:13:53
O>* 2.2.0.0/23 [110/400] via 1.1.1.1, eth1, 00:12:43
O>* 2.2.2.0/24 [110/400] via 1.1.1.1, eth1, 00:12:43
O>* 3.3.0.0/23 [110/400] via 1.1.1.10, eth2, 00:12:36
O>* 3.3.2.0/24 [110/400] via 1.1.1.10, eth2, 00:12:36
O>* 4.4.0.0/22 [110/300] via 1.1.1.34, eth0, 00:00:04
```

6.1.3 Διευθέτηση Δρομολογητή R3

R3# show running-config
Building configuration...

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R3
service integrated-vtysh-config
!
interface eth1
 description Point-to-Point Connection with R4
 ip address 1.1.1.13/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth2
 description Point-to-Point Connection with R1
 ip address 1.1.1.6/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
router ospf
 network 1.1.1.4/30 area 0
 network 1.1.1.12/30 area 0
 area 0 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής R3 ανήκει στο δίκτυο κορμού (backbone area 0). Μέσω των διεπαφών eth1 και eth2 συνδέεται με τους δρομολογητές R4 και R1 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους

ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλεδί SECRETKEY1.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R3. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 0, και συγεκριμένα του δικτύου 1.1.1.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF των δρομολογητών R5 και R8 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R3 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R3# show ip route
```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 1.1.1.5, eth2, 00:14:33
  *                    via 1.1.1.14, eth1, 00:14:33
O>* 1.1.1.0/30 [110/200] via 1.1.1.5, eth2, 00:15:04
O   1.1.1.4/30 [110/100] is directly connected, eth2, 00:15:06
C>* 1.1.1.4/30 is directly connected, eth2, 00:15:53
O>* 1.1.1.8/30 [110/200] via 1.1.1.14, eth1, 00:14:44
O   1.1.1.12/30 [110/100] is directly connected, eth1, 00:15:47
C>* 1.1.1.12/30 is directly connected, eth1, 00:15:53
O>* 1.1.1.16/30 [110/200] via 1.1.1.5, eth2, 00:15:04
O>* 1.1.1.20/30 [110/200] via 1.1.1.14, eth1, 00:14:44
O>* 1.1.1.32/29 [110/300] via 1.1.1.5, eth2, 00:14:44
  *                       via 1.1.1.14, eth1, 00:14:44
O>* 2.2.0.0/23 [110/400] via 1.1.1.5, eth2, 00:14:40
O>* 2.2.2.0/24 [110/400] via 1.1.1.5, eth2, 00:14:40
O>* 3.3.0.0/23 [110/400] via 1.1.1.14, eth1, 00:14:34
O>* 3.3.2.0/24 [110/400] via 1.1.1.14, eth1, 00:14:34
O>* 4.4.0.0/22 [110/500] via 1.1.1.5, eth2, 00:00:44
  *                      via 1.1.1.14, eth1, 00:00:44
```

6.1.4 Διευθέτηση Δρομολογητή R4

frr# show running-config
```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R4
service integrated-vtysh-config
!
interface eth0
 description Point-to-Point Connection with R8
 ip address 1.1.1.21/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
```

```
interface eth1
 description Point-to-Point Connection with R3
 ip address 1.1.1.14/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth2
 description Point-to-Point Connection with R2
 ip address 1.1.1.10/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
router ospf
 network 1.1.1.8/30 area 0
 network 1.1.1.12/30 area 0
 network 1.1.1.20/30 area 0
 area 0 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής R4 ανήκει στο δίκτυο κορμού (backbone area 0). Μέσω των διεπαφών eth0, eth1 και eth2 συνδέεται με τους δρομολογητές R8, R3 και R2 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY1.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R4. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 0, και συγεκριμένα του δικτύου 1.1.1.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή R8 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R4 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R4# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 1.1.1.22, eth0, 00:19:36
O>* 1.1.1.0/30 [110/200] via 1.1.1.9, eth2, 00:19:47
O>* 1.1.1.4/30 [110/200] via 1.1.1.13, eth1, 00:19:47
O   1.1.1.8/30 [110/100] is directly connected, eth2, 00:19:47
C>* 1.1.1.8/30 is directly connected, eth2, 00:20:43
O   1.1.1.12/30 [110/100] is directly connected, eth1, 00:20:31
C>* 1.1.1.12/30 is directly connected, eth1, 00:20:43
O>* 1.1.1.16/30 [110/300] via 1.1.1.9, eth2, 00:19:47
  *                       via 1.1.1.13, eth1, 00:19:47
O   1.1.1.20/30 [110/100] is directly connected, eth0, 00:20:31
C>* 1.1.1.20/30 is directly connected, eth0, 00:20:43
O>* 1.1.1.32/29 [110/200] via 1.1.1.9, eth2, 00:19:47
O>* 2.2.0.0/23 [110/500] via 1.1.1.9, eth2, 00:19:43
  *                       via 1.1.1.13, eth1, 00:19:43
O>* 2.2.2.0/24 [110/500] via 1.1.1.9, eth2, 00:19:43
  *                       via 1.1.1.13, eth1, 00:19:43
```

```
O>* 3.3.0.0/23 [110/300] via 1.1.1.22, eth0, 00:19:37
O>* 3.3.2.0/24 [110/300] via 1.1.1.22, eth0, 00:19:37
O>* 4.4.0.0/22 [110/400] via 1.1.1.9, eth2, 00:05:47
```

6.1.5 Διευθέτηση Δρομολογητή R5

R5# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R5
service integrated-vtysh-config
!
ip route 0.0.0.0/0 192.168.40.2
!
interface eth0
 description Point-to-Point Connection with R1
 ip address 1.1.1.18/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth1
 description Point-to-Point Connection with R6
 ip address 2.2.2.1/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with R7
 ip address 2.2.2.5/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Internet
 ip address 192.168.40.201/24
!
router ospf
 ospf router-id 1.1.1.18
 passive-interface eth3
 network 1.1.1.16/30 area 0
 network 2.2.2.0/30 area 1
 network 2.2.2.4/30 area 1
 area 0 authentication message-digest
 area 0 range 1.1.1.0/24
 area 1 authentication message-digest
 area 1 range 2.2.0.0/23
 area 1 range 2.2.2.0/24
 default-information originate
!
line vty
!
end
```

Ο δρομολογητής R5 είναι ένας ABR που ενώνει το δίκτυο κορμού (backbone area 0) με την περιοχή area 1. Επιπλέον, ο δρομολογητής R5 είναι ένας ASBR, δηλαδή αποτελεί μια πύλη (gateway) για το autonomous system προς το διαδίκτυο. Μέσω των διεπαφών eth0, eth1, eth2 και eth3 συνδέεται με τους δρομολογητές R1, R6, R7 και το διαδίκτυο αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τον δρομολογητή R1 πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλεδί SECRETKEY1, ενώ με τους δρομολογητές R6, και R7 χρησιμοποιώντας το συμμετρικό κλεδί SECRETKEY2. Ο δρομολογητής R5 για να λειτουργήσει σωστά ως ABR συναθροίζει όλα τα δίκτυα των δύο περιοχών που ανήκει και ανακοινώνει στην κάθε περιοχή τα summary routes της άλλης περιοχής. Τέλος, στο πρωτόκολλο OSPF του δρομολογητή R5 έχει δωθεί η εντολή default-information originate με σκοπό να γνωστοποιηθεί το default route 0.0.0.0/0 σε όλους τους neighbors.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R5. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων των περιοχών που ανήκει, δηλ. των area 0 και area 1, και συγεκριμένα των δικτύων 1.1.1.0/24, 2.2.0.0/23 και 2.2.2.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 που το έχουμε δηλώσει τόσο με στατική δρομολόγηση όσο και μέσω του πρωτοκόλλου OSPF. Όπως, παρατηρούμε ως default route επιλέγεται η εγγραφή που έχει πραγματοποιηθεί μέσω της στατικής δήλωσης έναντι αυτής που ανακοινώθηκε από το πρωτόκολλο OSPF λόγω του χαμηλότερου administrative distance (1<110). Έτσι, ο δρομολγητής R5 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R5# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O    0.0.0.0/0 [110/10] via 1.1.1.17, eth0, 00:07:22
S>* 0.0.0.0/0 [1/0] via 192.168.40.2, eth3, 00:22:11
O>* 1.1.1.0/24 [110/0] unreachable (blackhole), 00:07:23
O>* 1.1.1.0/30 [110/200] via 1.1.1.17, eth0, 00:21:20
O>* 1.1.1.4/30 [110/200] via 1.1.1.17, eth0, 00:21:20
O>* 1.1.1.8/30 [110/300] via 1.1.1.17, eth0, 00:21:20
O>* 1.1.1.12/30 [110/300] via 1.1.1.17, eth0, 00:21:20
O    1.1.1.16/30 [110/100] is directly connected, eth0, 00:22:10
C>* 1.1.1.16/30 is directly connected, eth0, 00:22:27
O>* 1.1.1.20/30 [110/400] via 1.1.1.17, eth0, 00:21:20
O>* 1.1.1.32/29 [110/300] via 1.1.1.17, eth0, 00:21:20
O>* 2.2.0.0/23 [110/0] unreachable (blackhole), 00:07:23
O>* 2.2.0.0/24 [110/200] via 2.2.2.2, eth1, 00:21:19
O>* 2.2.1.0/24 [110/200] via 2.2.2.6, eth2, 00:21:27
O>* 2.2.2.0/24 [110/0] unreachable (blackhole), 00:07:23
O    2.2.2.0/30 [110/100] is directly connected, eth1, 00:22:10
C>* 2.2.2.0/30 is directly connected, eth1, 00:22:27
O    2.2.2.4/30 [110/100] is directly connected, eth2, 00:22:10
C>* 2.2.2.4/30 is directly connected, eth2, 00:22:27
O>* 2.2.2.8/30 [110/200] via 2.2.2.2, eth1, 00:21:19
  *                        via 2.2.2.6, eth2, 00:21:19
O>* 3.3.0.0/23 [110/600] via 1.1.1.17, eth0, 00:21:13
O>* 3.3.2.0/24 [110/600] via 1.1.1.17, eth0, 00:21:13
O>* 4.4.0.0/22 [110/500] via 1.1.1.17, eth0, 00:07:23
C>* 192.168.40.0/24 is directly connected, eth3, 00:22:26
```

Τέλος, εκτελώντας την εντολή **show ip ospf database** εμφανίζονται αναλυτικότερες πληροφορίες για τον πίνακα δρομολόγησης του πρωτοκόλλου OSPF του δρομολογητή R5. Οι πληροφορίες που αντλούμε ομαδοποιούνται ανα περιοχή (area) και αφορούν το αναγγωριστικό σύνδεσης (link ID), τον δρομολογητή ανακοίνωσης (advertised router), τον τύπο του LSA (Router-LSA, Network-LSA, Summary-LSA, External-LSA), την ηλικία (age), τον αριθμό ακολουθίας (sequence number) και το checksum των διαδρομών.

R5# show ip ospf database

OSPF Router with ID (1.1.1.18)

Router Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.13	1.1.1.13	1490	0x8000000f	0x8992	2
1.1.1.17	1.1.1.17	1543	0x80000012	0xe7a5	3
1.1.1.18	1.1.1.18	1512	0x8000000c	0x4e3f	1
1.1.1.21	1.1.1.21	1482	0x80000010	0x431a	3
1.1.1.22	1.1.1.22	1530	0x8000000c	0x6e0f	1
1.1.1.34	1.1.1.34	998	0x8000002b	0xa487	1
1.1.1.36	1.1.1.36	978	0x80000018	0xb47e	3

Net Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum
1.1.1.2	1.1.1.36	1468	0x80000008	0x19d5
1.1.1.5	1.1.1.17	1453	0x80000008	0x2aeb
1.1.1.9	1.1.1.36	1458	0x80000008	0xbe25
1.1.1.14	1.1.1.21	1492	0x80000008	0xff05
1.1.1.18	1.1.1.18	1472	0x80000008	0xe71b
1.1.1.22	1.1.1.22	1400	0x80000008	0x08ea
1.1.1.36	1.1.1.36	1008	0x8000000b	0x506c

Summary Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	CkSum	Route
2.2.0.0	1.1.1.18	1482	0x80000009	0x77fc	2.2.0.0/23
2.2.2.0	1.1.1.18	762	0x80000008	0x680a	2.2.2.0/24
3.3.0.0	1.1.1.22	1470	0x80000008	0x4827	3.3.0.0/23
3.3.2.0	1.1.1.22	1530	0x80000009	0x3536	3.3.2.0/24
4.4.0.0	1.1.1.34	38	0x80000009	0x1216	4.4.0.0/22

Router Link States (Area 0.0.0.1)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.18	1.1.1.18	1552	0x8000000f	0x1dfd	2
2.2.2.9	2.2.2.9	1480	0x80000010	0x7d2a	3
2.2.2.10	2.2.2.10	1498	0x8000000f	0x5f3d	3

Net Link States (Area 0.0.0.1)

Link ID	ADV Router	Age	Seq#	CkSum
2.2.2.2	2.2.2.9	1400	0x80000008	0x32e8
2.2.2.6	2.2.2.10	1558	0x80000008	0x1203
2.2.2.10	2.2.2.10	1478	0x80000008	0xa76f

Summary Link States (Area 0.0.0.1)

Link ID	ADV Router	Age	Seq#	CkSum	Route
1.1.1.0	1.1.1.18	1462	0x80000009	0x614a	1.1.1.0/24
3.3.0.0	1.1.1.18	1492	0x80000008	0x0ed3	3.3.0.0/23
3.3.2.0	1.1.1.18	1472	0x80000008	0xfce1	3.3.2.0/24
4.4.0.0	1.1.1.18	972	0x8000000b	0x31d7	4.4.0.0/22

ASBR-Summary Link States (Area 0.0.0.1)

Link ID	ADV Router	Age	Seq#	CkSum
1.1.1.22	1.1.1.18	1462	0x80000008	0x781d
1.1.1.34	1.1.1.18	1012	0x8000000b	0x0edc

AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
0.0.0.0	1.1.1.18	1652	0x80000008	0xb4f7	E2 0.0.0.0/0 [0x0]
0.0.0.0	1.1.1.22	1550	0x80000008	0x9c0c	E2 0.0.0.0/0 [0x0]
0.0.0.0	1.1.1.34	88	0x80000009	0x5249	E2 0.0.0.0/0 [0x0]

6.1.6 Διευθέτηση Δρομολογητή R6

R6# show running-config
Building configuration...

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R6
service integrated-vtysh-config
!
interface eth0
 description LAN
 ip address 2.2.0.1/24
!
interface eth1
 description Point-to-Point Connection with R5
 ip address 2.2.2.2/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Point-to-Point Connection with R7
 ip address 2.2.2.9/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface eth0
 network 2.2.0.0/24 area 1
 network 2.2.2.0/30 area 1
 network 2.2.2.8/30 area 1
 area 1 authentication message-digest
```

```
!
line vty
!
end
```

Ο δρομολογητής R6 ανήκει στην περιοχή area 1. Μέσω των διεπαφών eth0, eth1 και eth3 συνδέεται με το τοπικό δίκτυο LAN και τους δρομολογητές R5 και R7 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY2.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R6. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 1, και συγεκριμένα των δικτύων 2.2.0.0/23 και 2.2.2.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή R5 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R6 αποκτά πρόσβαση σε όλο το διαδίκτυο.

```
R6# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 2.2.2.1, eth1, 00:22:14
O>* 1.1.1.0/24 [110/500] via 2.2.2.1, eth1, 00:22:15
O   2.2.0.0/24 [110/100] is directly connected, eth0, 00:23:13
C>* 2.2.0.0/24 is directly connected, eth0, 00:23:19
O>* 2.2.1.0/24 [110/200] via 2.2.2.10, eth3, 00:22:29
O   2.2.2.0/30 [110/100] is directly connected, eth1, 00:23:12
C>* 2.2.2.0/30 is directly connected, eth1, 00:23:19
O>* 2.2.2.4/30 [110/200] via 2.2.2.1, eth1, 00:22:15
  *                      via 2.2.2.10, eth3, 00:22:15
O   2.2.2.8/30 [110/100] is directly connected, eth3, 00:23:12
C>* 2.2.2.8/30 is directly connected, eth3, 00:23:19
O>* 3.3.0.0/23 [110/700] via 2.2.2.1, eth1, 00:22:08
O>* 3.3.2.0/24 [110/700] via 2.2.2.1, eth1, 00:22:08
O>* 4.4.0.0/22 [110/600] via 2.2.2.1, eth1, 00:08:18
```

6.1.7 Διευθέτηση Δρομολογητή R7

```
R7# show running-config
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R7
service integrated-vtysh-config
!
interface eth0
```

```
 description LAN
 ip address 2.2.1.1/24
!
interface eth2
 description Point-to-Point Connection with R5
 ip address 2.2.2.6/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Point-to-Point Connection with R6
 ip address 2.2.2.10/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface eth0
 network 2.2.1.0/24 area 1
 network 2.2.2.4/30 area 1
 network 2.2.2.8/30 area 1
 area 1 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής R7 ανήκει στην περιοχή area 1. Μέσω των διεπαφών eth0, eth1 και eth3 συνδέεται με το τοπικό δίκτυο LAN και τους δρομολογητές R5 και R6 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY2.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή 7. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 1, και συγεκριμένα των δικτύων 2.2.0.0/23 και 2.2.2.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή R5 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R7 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R7# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 2.2.2.5, eth2, 00:22:57
O>* 1.1.1.0/24 [110/500] via 2.2.2.5, eth2, 00:22:51
O>* 2.2.0.0/24 [110/200] via 2.2.2.9, eth3, 00:22:58
O    2.2.1.0/24 [110/100] is directly connected, eth0, 00:23:45
C>* 2.2.1.0/24 is directly connected, eth0, 00:23:52
O>* 2.2.2.0/30 [110/200] via 2.2.2.5, eth2, 00:22:50
  *                       via 2.2.2.9, eth3, 00:22:50
O    2.2.2.4/30 [110/100] is directly connected, eth2, 00:23:45
C>* 2.2.2.4/30 is directly connected, eth2, 00:23:52
O    2.2.2.8/30 [110/100] is directly connected, eth3, 00:23:45
C>* 2.2.2.8/30 is directly connected, eth3, 00:23:52
O>* 3.3.0.0/23 [110/700] via 2.2.2.5, eth2, 00:22:43
```

```
O>* 3.3.2.0/24 [110/700] via 2.2.2.5, eth2, 00:22:43
O>* 4.4.0.0/22 [110/600] via 2.2.2.5, eth2, 00:08:54
```

6.1.8 Διευθέτηση Δρομολογητή R8

R8# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R8
service integrated-vtysh-config
!
ip route 0.0.0.0/0 192.168.40.2
!
interface eth0
 description Point-to-Point Connection with R4
 ip address 1.1.1.22/30
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
interface eth1
 description Point-to-Point Connection with R9
 ip address 3.3.2.1/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with R10
 ip address 3.3.2.5/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Internet
 ip address 192.168.40.202/24
!
router ospf
 ospf router-id 1.1.1.22
 passive-interface eth3
 network 1.1.1.20/30 area 0
 network 3.3.2.0/30 area 2
 network 3.3.2.4/30 area 2
 area 0 authentication message-digest
 area 0 range 1.1.1.0/24
 area 2 authentication message-digest
 area 2 range 3.3.0.0/23
 area 2 range 3.3.2.0/24
 default-information originate
!
line vty
!
end
```

Ο δρομολογητής R8 είναι ένας ABR που ενώνει το δίκτυο κορμού (backbone area 0) με την περιοχή area 2. Επιπλέον, ο δρομολογητής R8 είναι ένας ASBR, δηλαδή αποτελεί μια πύλη (gateway) για το autonomous system προς το διαδίκτυο. Μέσω των διεπαφών eth0, eth1, eth2 και eth3 συνδέεται με τους δρομολογητές R4, R9, R10 και το διαδίκτυο αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τον δρομολογητή R4 πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλεδί SECRETKEY1, ενώ με τους δρομολογητές R9, και R10 χρησιμοποιώντας το συμμετρικό κλεδί SECRETKEY2. Ο δρομολογητής R5 για να λειτουργήσει σωστά ως ABR συναθροίζει όλα τα δίκτυα των δύο περιοχών που ανήκει και ανακοινώνει στην κάθε περιοχή τα summary routes της άλλης περιοχής. Τέλος, στο πρωτόκολλο OSPF του δρομολογητή R8 έχει δωθεί η εντολή default-information originate με σκοπό να γνωστοποιηθεί το default route 0.0.0.0/0 σε όλους τους neighbors.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R8. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων των περιοχών που ανήκει, δηλ. των area 0 και area 2, και συγεκριμένα των δικτύων 1.1.1.0/24, 3.3.0.0/23 και 3.3.2.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 που το έχουμε δηλώσει τόσο με στατική δρομολόγηση όσο και μέσω του πρωτοκόλλου OSPF. Όπως, παρατηρούμε ως default route επιλέγεται η εγγραφή που έχει πραγματοποιηθεί μέσω της στατικής δήλωσης έναντι αυτής που ανακοινώθηκε από το πρωτόκολλο OSPF λόγω του χαμηλότερου administrative distance (1<110). Έτσι, ο δρομολγητής R8 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R8# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O   0.0.0.0/0 [110/10] via 1.1.1.21, eth0, 00:09:32
S>* 0.0.0.0/0 [1/0] via 192.168.40.2, eth3, 00:24:17
O>* 1.1.1.0/24 [110/0] unreachable (blackhole), 00:09:33
O>* 1.1.1.0/30 [110/300] via 1.1.1.21, eth0, 00:23:23
O>* 1.1.1.4/30 [110/300] via 1.1.1.21, eth0, 00:23:23
O>* 1.1.1.8/30 [110/200] via 1.1.1.21, eth0, 00:23:23
O>* 1.1.1.12/30 [110/200] via 1.1.1.21, eth0, 00:23:23
O>* 1.1.1.16/30 [110/400] via 1.1.1.21, eth0, 00:23:23
O   1.1.1.20/30 [110/100] is directly connected, eth0, 00:24:23
C>* 1.1.1.20/30 is directly connected, eth0, 00:24:31
O>* 1.1.1.32/29 [110/300] via 1.1.1.21, eth0, 00:23:23
O>* 2.2.0.0/23 [110/600] via 1.1.1.21, eth0, 00:23:23
O>* 2.2.2.0/24 [110/600] via 1.1.1.21, eth0, 00:23:23
O>* 3.3.0.0/23 [110/0] unreachable (blackhole), 00:09:33
O>* 3.3.0.0/24 [110/200] via 3.3.2.2, eth1, 00:23:38
O>* 3.3.1.0/24 [110/200] via 3.3.2.6, eth2, 00:23:37
O>* 3.3.2.0/24 [110/0] unreachable (blackhole), 00:09:33
O   3.3.2.0/30 [110/100] is directly connected, eth1, 00:24:23
C>* 3.3.2.0/30 is directly connected, eth1, 00:24:30
O   3.3.2.4/30 [110/100] is directly connected, eth2, 00:24:23
C>* 3.3.2.4/30 is directly connected, eth2, 00:24:30
O>* 3.3.2.8/30 [110/200] via 3.3.2.2, eth1, 00:23:37
  *                      via 3.3.2.6, eth2, 00:23:37
O>* 4.4.0.0/22 [110/500] via 1.1.1.21, eth0, 00:09:33
C>* 192.168.40.0/24 is directly connected, eth3, 00:24:30
```

6.1.9 Διευθέτηση Δρομολογητή R9

R9# show running-config
Building configuration...

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R9
service integrated-vtysh-config
!
interface eth0
 description LAN
 ip address 3.3.0.1/24
!
interface eth1
 description Point-to-Point Connection with R8
 ip address 3.3.2.2/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Point-to-Point Connection with R10
 ip address 3.3.2.9/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface eth0
 network 3.3.0.0/24 area 2
 network 3.3.2.0/30 area 2
 network 3.3.2.8/30 area 2
 area 2 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής R9 ανήκει στην περιοχή area 2. Μέσω των διεπαφών eth0, eth1 και eth3 συνδέεται με το τοπικό δίκτυο LAN και τους δρομολογητές R8 και R10 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY2.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R9. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 2, και συγεκριμένα των δικτύων 3.3.0.0/23 και 3.3.2.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή R8 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R9 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R9# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
```

```
      > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 3.3.2.1, eth1, 00:24:22
O>* 1.1.1.0/24 [110/500] via 3.3.2.1, eth1, 00:24:08
O>* 2.2.0.0/23 [110/700] via 3.3.2.1, eth1, 00:24:08
O>* 2.2.2.0/24 [110/700] via 3.3.2.1, eth1, 00:24:08
O    3.3.0.0/24 [110/100] is directly connected, eth0, 00:25:07
C>* 3.3.0.0/24 is directly connected, eth0, 00:25:15
O>* 3.3.1.0/24 [110/200] via 3.3.2.10, eth3, 00:24:22
O    3.3.2.0/30 [110/100] is directly connected, eth1, 00:25:07
C>* 3.3.2.0/30 is directly connected, eth1, 00:25:15
O>* 3.3.2.4/30 [110/200] via 3.3.2.1, eth1, 00:24:22
  *                        via 3.3.2.10, eth3, 00:24:22
O    3.3.2.8/30 [110/100] is directly connected, eth3, 00:25:07
C>* 3.3.2.8/30 is directly connected, eth3, 00:25:15
O>* 4.4.0.0/22 [110/600] via 3.3.2.1, eth1, 00:10:18
```

6.1.10 Διευθέτηση Δρομολογητή R10

R10# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname R10
service integrated-vtysh-config
!
interface eth0
 description LAN
 ip address 3.3.1.1/24
!
interface eth2
 description Point-to-Point Connection with R8
 ip address 3.3.2.6/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Point-to-Point Connection with R9
 ip address 3.3.2.10/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface eth0
 network 3.3.1.0/24 area 2
 network 3.3.2.4/30 area 2
 network 3.3.2.8/30 area 2
 area 2 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής R10 ανήκει στην περιοχή area 2. Μέσω των διεπαφών eth0, eth1 και eth3 συνδέεται με το τοπικό δίκτυο LAN και τους δρομολογητές R8 και R9 αντίστοιχα. Η ανταλλαγή των OSPF

μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY2.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R10. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 2, και συγεκριμένα των δικτύων 3.3.0.0/23 και 3.3.2.0/24. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή R8 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής R10 αποκτά πρόσβαση σε όλο το διαδίκτυο.

R10# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
F - PBR, f - OpenFabric,
> - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 3.3.2.5, eth2, 00:24:51
O>* 1.1.1.0/24 [110/500] via 3.3.2.5, eth2, 00:24:37
O>* 2.2.0.0/23 [110/700] via 3.3.2.5, eth2, 00:24:37
O>* 2.2.2.0/24 [110/700] via 3.3.2.5, eth2, 00:24:37
O>* 3.3.0.0/24 [110/200] via 3.3.2.9, eth3, 00:24:43
O 3.3.1.0/24 [110/100] is directly connected, eth0, 00:25:43
C>* 3.3.1.0/24 is directly connected, eth0, 00:25:48
O>* 3.3.2.0/30 [110/200] via 3.3.2.5, eth2, 00:24:43
* via 3.3.2.9, eth3, 00:24:43
O 3.3.2.4/30 [110/100] is directly connected, eth2, 00:25:43
C>* 3.3.2.4/30 is directly connected, eth2, 00:25:48
O 3.3.2.8/30 [110/100] is directly connected, eth3, 00:25:43
C>* 3.3.2.8/30 is directly connected, eth3, 00:25:48
O>* 4.4.0.0/22 [110/600] via 3.3.2.5, eth2, 00:10:47

6.1.11 Εγκατάσταση Raspberry Pi OS Lite (64-bit)

Κατά την εκκίνηση της συσκευής πατάμε το πλήκτρο Shift για να εισέλθουμε στο boot menu. Στη συνέχεια συνδεόμαστε στο ασύρματο δίκτυο και αφού επιλέξουμε ως λειτουργικό σύστημα το Raspberry Pi OS Lite (64-bit) προχωρούμε στην εγκατάστασή του. Αφού πραγματοποιηθεί η εγκατάσταση του ανωτέρω λειτουργικού συστήματος για να εισέλθουμε στην κονσόλα πληκτρολογούμε ως username το pi και password το raspberry.

Στη συνέχεια εκχωρούμε ως συνθηματικό του χρήστη root το raspberry ως εξής:
passwd root
…

Κατόπιν με την χρήση της εντολής su συνδεόμαστε στο κέλυφος του λειτουργικού συστήματος ως super user, ώστε να μη χρειάζεται να δίνουμε το πρόθεμα sudo κάθε φορά που πρέπει να εκτελέσουμε μια εντολή που απαιτεί δικαιώματα super user (έτσι όλες εντολές που ακολουθούν θα μπορούσαν να εκτελεστούν και χωρίς το πρόθεμα sudo).

Στη συνέχεια εκτελούμε ένα update για να φορτώσουμε όλες τις νεότερες εκδόσεις των πακέτων λογισμικού του ανωτέρω λειτουργικού συστήματος.
sudo apt update

sudo apt upgrade

Έπειτα εγκαθιστούμε και ενεργοποιούμε το πακέτο λογισμικού openssh-server για να μπορούμε να συνδεόμαστε απομακρυσμένα.
sudo apt install openssh-server
sudo systemctl enable ssh
sudo systemctl start ssh

Στη συνέχεια δημιουργούμε έναν κανόνα 76-netnames.rules, ώστε τα usb lan ports που έχουμε συνδέσει να λαμβάνουν ως ονόματα eth1, eth2, κοκ και κατόπιν επιβεβαιώνουμε τα ονόματα που τους έχουν αποδοθεί.
sudo nano /etc/udev/rules.d/76-netnames.rules
SUBSYSTEM=="net", ACTION=="add", NAME="eth%n"
sudo apt install lshw
sudo lshw –class network -short

Έπειτα απενεργοποιούμε τη δυνατότητα από όλα τα διαθέσιμα interfaces της συσκευής να λαμβάνουν δυναμικά IP διευθύνσεις από κάποιον dhcp server δεδομένου ότι θα εκχωρήσουμε στατικά IP διευθύνσεις, όπου αυτό είναι απαραίτητο, μέσω της σουίτας FRR. Εναλλακτικά θα μπορούσαμε να απενεργοποιήσουμε ή ακόμα και να απεγκαταστήσουμε τον δαίμονα dhcpcd.
sudo nano /etc/dhcpcd.conf
denyinterfaces wlan0 eth0 eth1 eth2 eth3 eth4

Στη συνέχεια διευθετούμε το loopback interface lo ως εξης:
sudo nano /etc/network/interfaces.d/interfaces.conf
auto lo
iface lo inet loopback
dns-nameservers 8.8.8.8 8.8.4.4

Τέλος, ενεργοποιούμε τη δυνατότητα δρομολόγησης δικτύων ως εξής:
sudo nano /etc/sysctl.d/routed.conf
 # Enable IPv4 routing
net.ipv4.ip_forward=1

6.1.12 Εγκατάσταση Σουίτας FRR σε Συσκευή Raspberry Pi

Αρχικά εγκαθιστούμε τη σουίτα λογισμικού frr ως εξής:
sudo apt install frr

Μετά την εγκατάσταση της πλατφόρμας frr θα πρέπει πρώτα να ενεργοποιηθούν όλοι οι απαραίτητοι δαίμονες που σκοπεύουμε να χρησιμοποιήσουμε (π.χ. ospfd και bgpd). Ο μοναδικός δαίμονας που ενεργοποιείται αυτόματα μετά την εγκατάσταση της σουίτας frr είναι ο δαίμονας zebra. Για το σκοπό αυτόν επεξεργαζόμαστε το αρχείο /etc/frr/daemons, θέτοντας την τιμή yes στους δαίμονες που επιθυμούμε να ενεργοποιήσουμε.
sudo nano /etc/frr/daemons
bgpd=yes
ospfd=yes

Στη συνέχεια αφού έχουμε ενεργοποιήσει τους απαραίτητους δαίμονες ξεκινούμε την υπηρεσία frr ως εξής:
sudo systemctl enable frr
sudo systemctl start frr

Με την πρώτη εντολή "systemctl enable frr" ενεργοποιούμε την υπηρεσία frr, ώστε αυτή να εκτελείται αυτόματα κάθε φορά που η συσκευή ξεκινά τη λειτουργίας της, ενώ με τη δεύτερη εντολή "systemctl start frr" ξεκινούμε την υπηρεσία frr μιας και η συσκευή έχει ήδη ξεκινήσει τη λειτουργία της.

Τέλος, για να συνδεθούμε στη γραμμή εντολών της σουίτας frr εκτελούμε την εντολή "sudo vtysh" (το περιβάλλον της γραμμής εντολών της εν λόγω πλατφόρμας είναι παρόμοιο με εκείνο της Cisco και πολλές από τις εντολές είναι πανομοιότυπες με αυτές του Cisco IOS).

6.1.13 Εγκατάσταση ενός Bridged Wireless Access Point σε Συσκευή Raspberry Pi

Αρχικά εγκαθιστούμε το απαραίτητο πακέτο λογισμικού hostapd ως εξής:
sudo apt install hostapd

Στη συνέχεια ενεργοποιούμε την υπηρεσία hostapd ώστε αυτή να ξεκινάει αυτόματα όταν η συσκευή κάνει επανεκκίνηση.
sudo systemctl unmask hostapd
sudo systemctl enable hostapd

Στο επόμενο βήμα δημιουργούμε ένα network bridge με όνομα br0 ως εξής:
sudo nano /etc/systemd/network/bridge-br0.netdev
[NetDev]
Name=br0
Kind=bridge

Στη συνέχεια προσθέτουμε ως πρώτο μέλος του network bridge br0 τη διεπαφή eth0 ως εξής:
sudo nano /etc/systemd/network/br0-member-eth0.network
[Match]
Name=eth0

[Network]
Bridge=br0
Να σημειώσουμε εδώ ότι δεν χρειάζεται να προσθέσουμε ως δεύτερο μέλος του bridge br0 τη διεπαφή wlan0, διότι αυτό πραγματοποιείται από το λογισμικό του access point, όπως θα δούμε στη συνέχεια.

Αφού έχουμε δημιουργήσει τα ανωτέρω δύο αρχεία στον κατάλογο /etc/systemd/network θα πρέπει στη συνέχεια να ενεργοποιήσουμε την υπηρεσία systemd-networkd ώστε η γέφυρα br0 να δημιουργείται και να λειτουργεί αυτόματα όταν η συσκευή κάνει επανεκκίνηση.
sudo systemctl enable systemd-networkd

Στη συνέχεια διευθετούμε το λογισμικό του access point, χρησιμοποιώντας ως κανάλι εκπομπής το 12 (channel=12) με όνομα δικτύου RSB1 (ssid=RSB1) και συνθηματικό 0123456789 (wpa_passphrase=0123456789). Προφανώς, στις εγκαταστάσεις των άλλων δύο raspberries δίνουμε διαφορετικά ssids και channels. Το συνθηματικό θα πρέπει να είναι μεταξύ 8 και 64 χαρακτήρων, χωρίς αυτό να περικλείεται σε αποστρόφους (quotes). Με την εντολή bridge=br0 προστίθεται ως δεύτερο μέλος του bridge br0 η διεπαφή wlan0. Σε περίπτωση που επιθυμούμε να χρησιμοποιήσουμε τη συχνότητα των 5 GHz αντί των 2.4 GHz αλλάζουμε το mode από hw_mode=g σε hw_mode=a.
sudo nano /etc/default/hostapd
DAEMON_CONF="/etc/hostapd/hostapd.conf"
sudo nano /etc/hostapd/hostapd.conf
country_code=GR
interface=wlan0
bridge=br0
driver=nl80211
ssid=RSB1
hw_mode=g
channel=12
macaddr_acl=0
auth_algs=1

```
wpa=2
wpa_passphrase=0123456789
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Στο τελευταίο βήμα εγκαθιστούμε και διευθετούμε το λογισμικό του isc-dhcp-server ως εξής:
Αρχικά εγκαθιστούμε το πακέτο λογισμικού isc-dhcp-server.

```
sudo apt install isc-dhcp-server
```

Στη συνέχεια δηλώνουμε τις διεπαφές τις οποίες θα εξυπηρετεί ο ανωτέρω dhcp server.

```
sudo nano /etc/defaults/isc-dhcp-server
    INTERFACESv4="br0"
```

Τέλος, δημιουργούμε ένα dhcp pool που θα εκχωρείται στους dhcp clients και θα περιλαμβάνει τις IP διευθύνσεις μεταξύ 4.4.1.100 έως 4.4.1.200 με πύλη (gateway) την IP διεύθυνση 4.4.1.1 της γέφυρας br0 και διακομιστές ονοματολογίας (dns severs) τους 8.8.8.8 και 8.8.4.4.

```
sudo nano /etc/dhcp/dhcpd.conf
    default-lease-time 600;
    max-lease-time 7200;
    ddns-update-style none;
    authoritative;
    subnet 4.4.1.0  netmask 255.255.255.0 {
        range 4.4.1.100 4.4.1.200;
        option subnet-mask 255.255.255.0;
        option broadcast-address 4.4.1.255;
        option routers 4.4.1.1;
        option domain-name-servers 8.8.8.8 8.8.4.4;
    }
```

Προφανώς, στις εγκαταστάσεις των άλλων δύο raspberries δίνουμε διαφορετικό dhcp pool και πύλη (gateway). Αναλυτικότερα, στην εγκατάσταση της ανωτέρω υπηρεσίας στα raspberries RSB2 και RSB3 αντικαθίσταται το δίκτυο 4.4.1.0/24 με τα δίκτυα 4.4.2.0/24 και 4.4.3.0/24 αντίστοιχα.

6.1.14 Διευθέτηση Κανόνων Πρόσβασης στο Διαδίκτυο σε Συσκευή Raspberry Pi

Δεδομένου ότι όλες οι IP διευθύνσεις που χρησιμοποιούμε σε όλες τις μελέτες περιπτώσεων είναι public δε θα απαιτούνταν να ενεργοποιήσουμε ip nat translation στον δρομολογητή RSB1 αρκεί βέβαια να διαθέταμε τα αντίστοιχα public static pools. Αφού, λοιπόν δε διαθέτουμε τα ανωτέρω public static pools για πειραματικούς σκοπούς ενεργοποιούμε στον δρομολογητή RSB1 ip nat translation για να έχουμε τη δυνατότητα πρόσβασης στο διαδίκτυο.

```
sudo iptables --table nat --append POSTROUTING --out-interface eth3 -j MASQUERADE
sudo iptables --append FORWARD --in-interface br0 -j ACCEPT
sudo iptables --append FORWARD --in-interface eth1 -j ACCEPT
sudo iptables --append FORWARD --in-interface eth2 -j ACCEPT
sudo iptables --append FORWARD --in-interface eth4 -j ACCEPT
sudo iptables-save >/etc/iptables/rules.v4
```

Στη συνέχεια ελέγχουμε αν πράγματι έχουν αποθηκευτεί οι ανωτέρω κανόνες.

```
more /etc/iptables/rules.v4
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -i br0 -j ACCEPT
```

-A FORWARD -i eth1 -j ACCEPT
-A FORWARD -i eth2 -j ACCEPT
-A FORWARD -i eth4 -j ACCEPT
COMMIT
****nat***
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o eth3 -j MASQUERADE
COMMIT

6.1.15 Διευθέτηση Δρομολογητή RSB1 (Raspberry Pi 4)

RSB1# show running-config
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname raspberrypi
log syslog informational
no ipv6 forwarding
hostname RSB1
service integrated-vtysh-config
!
ip route 0.0.0.0/0 192.168.2.1
!
interface br0
 description Connection with LAN (Bridge eth0 with wlan0)
 ip address 4.4.1.1/24
!
interface eth1
 description Point-to-Point Connection with RSB2
 ip address 4.4.0.1/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with RSB3
 ip address 4.4.0.5/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Connection with WAN
 ip address 192.168.2.100/24
!
interface eth4
 description Connection with GNS3
 ip address 1.1.1.34/29
 ip ospf message-digest-key 1 md5 SECRETKEY1
!
router ospf
 ospf router-id 1.1.1.34
 passive-interface br0
 passive-interface eth3

```
 network 1.1.1.32/29 area 0
 network 4.4.0.0/30 area 3
 network 4.4.0.4/30 area 3
 network 4.4.1.0/24 area 3
 area 0 authentication message-digest
 area 0 range 1.1.1.0/24
 area 3 authentication message-digest
 area 3 range 4.4.0.0/22
 default-information originate
!
line vty
!
end
```

Ο δρομολογητής RSB1 είναι ένας ABR που ενώνει το δίκτυο κορμού (backbone area 0) με την περιοχή area 3. Επιπλέον, ο δρομολογητής RSB1 είναι ένας ASBR, δηλαδή αποτελεί μια πύλη (gateway) για το autonomous system προς το διαδίκτυο. Αναλυτικότερα, ο δρομολογητής RSB1 συνδέεται με το τοπικό δίκτυο LAN (τόσο το ενσύρματο όσο και το ασύρματο), τους δρομολογητές RSB2 και RSB3, τον δρομολογητή R2 του προσομοιωτή GNS3 και το διαδίκτυο μέσω των διεπαφών br0, eth1, eth2, eth3 και eth4 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τον δρομολογητή R2 πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY1, ενώ η ανταλλαγή των OSPF μηνυμάτων με τους δρομολογητές RSB2 και RSB3 πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY2. Ο δρομολογητής RSB1 για να λειτουργήσει σωστά ως ABR συναθροίζει όλα τα δίκτυα των δύο περιοχών που ανήκει και ανακοινώνει στην κάθε περιοχή τα summary routes της άλλης περιοχής. Τέλος, στο πρωτόκολλο OSPF του δρομολογητή RSB1 έχει δωθεί η εντολή default-information originate με σκοπό να γνωστοποιηθεί το default route 0.0.0.0/0 σε όλους τους neighbors.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή RSB1. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων των περιοχών που ανήκει, δηλ. των area 0 και area 3, και συγεκριμένα των δικτύων 1.1.1.0/24 και 4.4.0.0/22. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνονται και δύο εγγραφές για το default route 0.0.0.0/0, αυτή που δηλώθηκε με στατική δρομολόγηση και αυτή που ανακακοινώθηκε από το πρωτοκόλλο OSPF. Όπως, παρατηρούμε ως default route επιλέγεται η εγγραφή που έχει ανακοινωθεί μέσω της στατικής δρομολόγησης έναντι αυτής που ανακοινώθηκε από το πρωτόκολλο OSPF λόγω του χαμηλότερου administrative distance (1<110). Έτσι, ο δρομολγητής RSB1 αποκτά πρόσβαση σε όλο το διαδίκτυο.

RSB1# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

O    0.0.0.0/0 [110/10] via 1.1.1.36, eth4, weight 1, 00:00:06
S>*  0.0.0.0/0 [1/0] via 192.168.2.1, eth3, weight 1, 00:26:47
O>*  1.1.1.0/24 [110/0] unreachable (blackhole), weight 1, 00:00:06
O>*  1.1.1.0/30 [110/110] via 1.1.1.36, eth4, weight 1, 00:00:24
O>*  1.1.1.4/30 [110/210] via 1.1.1.36, eth4, weight 1, 00:00:07
O>*  1.1.1.8/30 [110/110] via 1.1.1.36, eth4, weight 1, 00:00:24
O>*  1.1.1.12/30 [110/210] via 1.1.1.36, eth4, weight 1, 00:00:09
O>*  1.1.1.16/30 [110/210] via 1.1.1.36, eth4, weight 1, 00:00:07
O>*  1.1.1.20/30 [110/210] via 1.1.1.36, eth4, weight 1, 00:00:09
O    1.1.1.32/29 [110/10] is directly connected, eth4, weight 1, 00:26:50
C>*  1.1.1.32/29 is directly connected, eth4, 00:26:50
O>*  2.2.0.0/23 [110/410] via 1.1.1.36, eth4, weight 1, 00:00:06
```

```
O>* 2.2.2.0/24 [110/410] via 1.1.1.36, eth4, weight 1, 00:00:06
O>* 3.3.0.0/23 [110/410] via 1.1.1.36, eth4, weight 1, 00:00:07
O>* 3.3.2.0/24 [110/410] via 1.1.1.36, eth4, weight 1, 00:00:07
O>* 4.4.0.0/22 [110/0] unreachable (blackhole), weight 1, 00:00:06
O   4.4.0.0/30 [110/100] is directly connected, eth1, weight 1, 00:11:57
C>* 4.4.0.0/30 is directly connected, eth1, 00:12:45
O   4.4.0.4/30 [110/100] is directly connected, eth2, weight 1, 00:11:47
C>* 4.4.0.4/30 is directly connected, eth2, 00:12:29
O>* 4.4.0.8/30 [110/200] via 4.4.0.2, eth1, weight 1, 00:11:37
  *                       via 4.4.0.6, eth2, weight 1, 00:11:37
O   4.4.1.0/24 [110/1] is directly connected, br0, weight 1, 00:27:55
C>* 4.4.1.0/24 is directly connected, br0, 00:27:55
O>* 4.4.2.0/24 [110/101] via 4.4.0.2, eth1, weight 1, 00:11:50
O>* 4.4.3.0/24 [110/101] via 4.4.0.6, eth2, weight 1, 00:11:37
C>* 192.168.2.0/24 is directly connected, eth3, 00:26:47
```

6.1.16 Διευθέτηση Δρομολογητή RSB2 (Raspberry Pi 4)

RSB2# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname raspberrypi
log syslog informational
no ipv6 forwarding
hostname RSB2
service integrated-vtysh-config
!
interface br0
 description Connection with LAN (Bridge eth0 with wlan0)
 ip address 4.4.2.1/24
!
interface eth1
 description Point-to-Point Connection with RSB1
 ip address 4.4.0.2/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with RSB3
 ip address 4.4.0.9/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface br0
 network 4.4.0.0/30 area 3
 network 4.4.0.8/30 area 3
 network 4.4.2.0/24 area 3
 area 3 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής RSB2 ανήκει στην περιοχή area 3. Μέσω των διεπαφών br0, eth1 και eth2 συνδέεται με το τοπικό δίκτυο LAN (τόσο το ενσύρματο όσο και το ασύρματο) και τους δρομολογητές RSB1 και RSB3 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY2.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή RSB2. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 3, και συγεκριμένα των δικτύων 4.4.0.0/22. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή RSB1 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής RSB2 αποκτά πρόσβαση σε όλο το διαδίκτυο.

RSB2# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
F - PBR, f - OpenFabric,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup

O>* 0.0.0.0/0 [110/10] via 4.4.0.1, eth1, weight 1, 00:19:22
O>* 1.1.1.0/24 [110/310] via 4.4.0.1, eth1, weight 1, 00:07:38
O>* 2.2.0.0/23 [110/510] via 4.4.0.1, eth1, weight 1, 00:07:37
O>* 2.2.2.0/24 [110/510] via 4.4.0.1, eth1, weight 1, 00:07:37
O>* 3.3.0.0/23 [110/510] via 4.4.0.1, eth1, weight 1, 00:07:38
O>* 3.3.2.0/24 [110/510] via 4.4.0.1, eth1, weight 1, 00:07:30
O 4.4.0.0/30 [110/100] is directly connected, eth1, weight 1, 00:20:13
C>* 4.4.0.0/30 is directly connected, eth1, 00:20:14
O>* 4.4.0.4/30 [110/200] via 4.4.0.1, eth1, weight 1, 00:19:07
* via 4.4.0.10, eth2, weight 1, 00:19:07
O 4.4.0.8/30 [110/100] is directly connected, eth2, weight 1, 00:19:59
C>* 4.4.0.8/30 is directly connected, eth2, 00:20:00
O>* 4.4.1.0/24 [110/101] via 4.4.0.1, eth1, weight 1, 00:19:23
O 4.4.2.0/24 [110/1] is directly connected, br0, weight 1, 00:20:12
C>* 4.4.2.0/24 is directly connected, br0, 00:20:12
O>* 4.4.3.0/24 [110/101] via 4.4.0.10, eth2, weight 1, 00:19:07

6.1.17 Διευθέτηση Δρομολογητή RSB3 (Raspberry Pi 4)

RSB3# show running-config
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname raspberrypi
log syslog informational
no ipv6 forwarding
hostname RSB3
service integrated-vtysh-config
!
interface br0
description Connection with LAN (Bridge eth0 wlan0)
ip address 4.4.3.1/24

```
!
interface eth1
 description Point-to-Point Connection with RSB1
 ip address 4.4.0.6/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with RSB2
 ip address 4.4.0.10/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface br0
 network 4.4.0.4/30 area 3
 network 4.4.0.8/30 area 3
 network 4.4.3.0/24 area 3
 area 3 authentication message-digest
!
line vty
!
end
```

Ο δρομολογητής RSB3 ανήκει στην περιοχή area 3. Μέσω των διεπαφών br0, eth1 και eth2 συνδέεται με το τοπικό δίκτυο LAN (τόσο το ενσύρματο όσο και το ασύρματο) και τους δρομολογητές RSB1 και RSB2 αντίστοιχα. Η ανταλλαγή των OSPF μηνυμάτων με τους ανωτέρω δρομολογητές πραγματοποιείται με κρυπτογράφηση md5 χρησιμοποιώντας το συμμετρικό κλειδί SECRETKEY2.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή RSB3. Παρατηρούμε ότι εμφανίζονται αναλυτικά όλα τα υποδίκτυα των δικτύων της περιοχής που ανήκει, δηλ. της area 3, και συγεκριμένα των δικτύων 4.4.0.0/22. Αντίθετα για όλα τα δίκτυα των υπόλοιπων περιοχών εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινόνονται από τους αντίστοιχους ABRs. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή RSB1 έχει δωθεί η εντολή default-information originate. Έτσι, ο δρομολγητής RSB3 αποκτά πρόσβαση σε όλο το διαδίκτυο.

RSB3# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

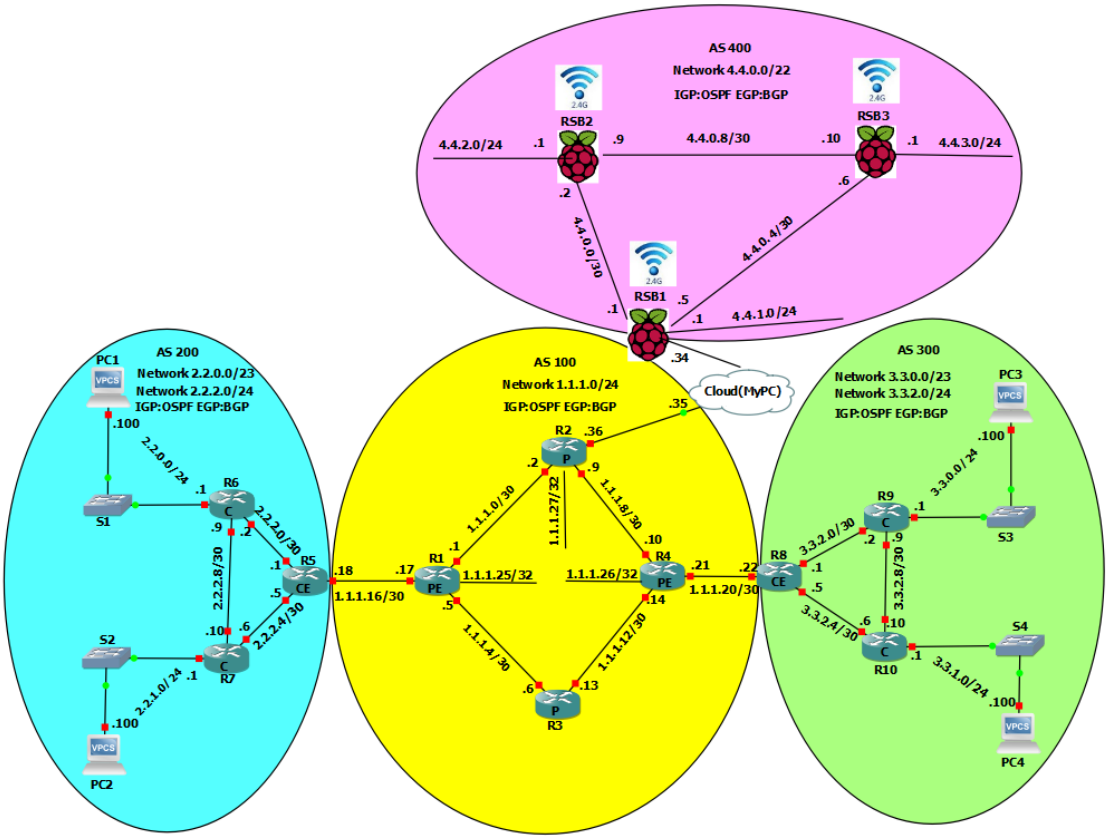
O>* 0.0.0.0/0 [110/10] via 4.4.0.5, eth1, weight 1, 00:19:47
O>* 1.1.1.0/24 [110/310] via 4.4.0.5, eth1, weight 1, 00:08:18
O>* 2.2.0.0/23 [110/510] via 4.4.0.5, eth1, weight 1, 00:08:17
O>* 2.2.2.0/24 [110/510] via 4.4.0.5, eth1, weight 1, 00:08:17
O>* 3.3.0.0/23 [110/510] via 4.4.0.5, eth1, weight 1, 00:08:18
O>* 3.3.2.0/24 [110/510] via 4.4.0.5, eth1, weight 1, 00:08:10
O>* 4.4.0.0/30 [110/200] via 4.4.0.5, eth1, weight 1, 00:19:48
  *                       via 4.4.0.9, eth2, weight 1, 00:19:48
O    4.4.0.4/30 [110/100] is directly connected, eth1, weight 1, 00:20:38
C>* 4.4.0.4/30 is directly connected, eth1, 00:20:39
O    4.4.0.8/30 [110/100] is directly connected, eth2, weight 1, 00:20:38
C> *4.4.0.8/30 is directly connected, eth2, 00:20:39
O>* 4.4.1.0/24 [110/101] via 4.4.0.5, eth1, weight 1, 00:19:48
O>* 4.4.2.0/24 [110/101] via 4.4.0.9, eth2, weight 1, 00:19:48
O    4.4.3.0/24 [110/1] is directly connected, br0, weight 1, 00:20:37
```

C>* 4.4.3.0/24 is directly connected, br0, 00:20:37

6.2 Μελέτη Περίπτωσης Πρωτοκόλλου Δρομολόγησης BGP Σουίτας FRR

Η μελέτη περίπτωσης του πρωτοκόλλου BGP της σουίτας FRR περιλαμβάνει την εγκατάσταση και διευθέτηση σε τρεις συσκευές Raspberry Pi 4 οι οποίες μέσω cloud διασυνδέονται με άλλους δέκα δρομολογητές της σουίτας FRR που έχουν εγκατασταθεί και λειτουργούν με τη χρήση του προσομοιωτή GNS3. Στην παρούσα μελέτη περίπτωσης έχει χρησιμοποιηθεί ένα υβριδικό περιβάλλον μεταξύ πραγματικών συσκευών δρομολόγησης και αντίστοιχων συσκευών που έχουν εγκατασταθεί στον προσομοιωτή GNS3 για λόγους οικονομίας και ευελιξίας.

Αναλυτικότερα, μελετούμε τη συμπεριφορά του πρωτοκόλλου BGP σε ένα σχήμα που απαρτίζεται από δεκατρείς δρομολογητές που ανήκουν σε τέσσερα διαφορετικά AS. Στη συνέχεια ακολουθούν οι διευθετήσεις (configurations) των πρωτοκόλλων OSPF και BGP και των δεκατριών δρομολογητών της μελέτης περίπτωσης, καθώς και η ανάλυση των αντίστοιχων πινάκων δρομολόγησης.



Εικόνα 42: Μελέτη Περίπτωσης Πρωτοκόλλου BGP

6.2.1 Διευθέτηση Δρομολογητή R1

R1# show running-config
Building configuration...

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R1
service integrated-vtysh-config
!
ip route 1.1.1.0/24 Null0 254
!
interface eth0
 description eBGP
 ip address 1.1.1.17/30
!
interface eth1
 description Point-to-Point Connection with R2
 ip address 1.1.1.1/30
!
interface eth2
 description Point-to-Point Connection with R3
 ip address 1.1.1.5/30
!
interface lo
 description iBGP
 ip address 1.1.1.25/32
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.18 remote-as 200
 neighbor 1.1.1.26 remote-as 100
 neighbor 1.1.1.26 update-source lo
 neighbor 1.1.1.27 remote-as 100
 neighbor 1.1.1.27 update-source lo
 !
 address-family ipv4 unicast
  network 1.1.1.0/24
  neighbor 1.1.1.18 soft-reconfiguration inbound
  neighbor 1.1.1.26 next-hop-self
  neighbor 1.1.1.26 soft-reconfiguration inbound
  neighbor 1.1.1.27 next-hop-self
  neighbor 1.1.1.27 soft-reconfiguration inbound
 exit-address-family
!
router ospf
 redistribute bgp route-map CHECKCOMMUNITY
 passive-interface eth0
 passive-interface lo
 network 1.1.1.0/30 area 0
 network 1.1.1.4/30 area 0
 network 1.1.1.16/30 area 0
 network 1.1.1.25/32 area 0
!
bgp community-list 1 permit 100:200
!
route-map CHECKCOMMUNITY permit 10
 match community 1
!
```

```
line vty
!
end
```

Ο δρομολογητής R1 βρίσκεται στο AS100 και χρησιμοποιεί ως IGP το OSPF και EGP το BGP. Ο ανωτέρω δρομολογητής έχει τρεις BGP peers (neighbors): τον 1.1.1.18 που βρίσκεται σε διαφορετικό AS (AS200), οπότε πρόκειται για eBGP διασύνδεση και τους 1.1.1.26 και 1.1.1.27 που βρίσκονται στο ίδιο AS (AS100), οπότε πρόκειται για iBGP διασυνδέσεις. Για τις iBGP διασυνδεσεις έχει χρησιμοποιηθεί το loop back interface lo από όλους τους peers με σκοπό να υπάρχει η δυνατότητα επιμερισμού του φορτίου κίνησης (load balancing). Όπως παρατηρούμε τα δίκτυα που ανακοινώνονται στο πρωτόκολλο BGP γνωστοποιούνται και στο πρωτόκολλο OSPF με σκοπό να ενημερωθούν για αυτά και οι υπόλοιποι δρομολογητές εντός του AS. Αυτό πραγματοποιείται με την εντολή redistribute η οποία μάλιστα χρησιμοποεί και το φίλτρο CHECKCOMMUNITY για να ανακοινώσει στο πρωτόκολλο OSPF μόνο τα δίκτυα που προέρχονται από το AS200 και όχι αυτά που προέρχονται από τα AS300 και AS400.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R1. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS100, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, ενώ αντίθετα για όλα τα δίκτυα των υπόλοιπων AS που έχουν ανακοινωθεί από το πρωτόκολλο BGP εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινώθηκαν από τους αντίστοιχους eBGP preers.

R1# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O    1.1.1.0/30 [110/100] is directly connected, eth1, 04:27:05
C>* 1.1.1.0/30 is directly connected, eth1, 04:27:23
O    1.1.1.4/30 [110/100] is directly connected, eth2, 04:27:05
C>* 1.1.1.4/30 is directly connected, eth2, 04:27:23
O>* 1.1.1.8/30 [110/200] via 1.1.1.2, eth1, 01:52:37
O>* 1.1.1.12/30 [110/200] via 1.1.1.6, eth2, 04:26:15
O    1.1.1.16/30 [110/100] is directly connected, eth0, 04:27:05
C>* 1.1.1.16/30 is directly connected, eth0, 04:27:23
O>* 1.1.1.20/30 [110/300] via 1.1.1.2, eth1, 01:52:36
  *                       via 1.1.1.6, eth2, 01:52:36
O    1.1.1.25/32 [110/0] is directly connected, lo, 04:27:05
C>* 1.1.1.25/32 is directly connected, lo, 04:27:23
O>* 1.1.1.26/32 [110/200] via 1.1.1.2, eth1, 01:52:36
  *                       via 1.1.1.6, eth2, 01:52:36
O>* 1.1.1.27/32 [110/100] via 1.1.1.2, eth1, 01:52:37
O>* 1.1.1.32/29 [110/200] via 1.1.1.2, eth1, 01:52:37
B>* 2.2.0.0/23 [20/0] via 1.1.1.18, eth0, 04:27:11
B>* 2.2.2.0/24 [20/0] via 1.1.1.18, eth0, 04:27:11
O>* 3.3.0.0/23 [110/20] via 1.1.1.2, eth1, 01:52:35
  *                     via 1.1.1.6, eth2, 01:52:35
B    3.3.0.0/23 [200/0] via 1.1.1.26 (recursive), 01:52:36
                        via 1.1.1.2, eth1, 01:52:36
                        via 1.1.1.6, eth2, 01:52:36
O>* 3.3.2.0/24 [110/20] via 1.1.1.2, eth1, 01:52:35
  *                     via 1.1.1.6, eth2, 01:52:35
B    3.3.2.0/24 [200/0] via 1.1.1.26 (recursive), 01:52:36
                        via 1.1.1.2, eth1, 01:52:36
                        via 1.1.1.6, eth2, 01:52:36
B   4.4.0.0/22 [200/0] via 1.1.1.27 (recursive), 01:02:15
```

```
                    via 1.1.1.2, eth1, 01:02:15
O>* 4.4.0.0/22 [110/20] via 1.1.1.2, eth1, 01:02:15
```

Τέλος, εκτελώντας την εντολή **show ip bgp** εμφανίζονται αναλυτικές πληροφορίες για όλες τις εξωτερικές διαδρομές του πίνακα δρομολόγησης που περιλαμβάνουν διάφορα χαρακτηριστικά του BGP πρωτοκόλλου όπως το next hop, το local preference, το weight, καθώς και το as-path.

R1# show ip bgp
BGP table version is 5, local router ID is 1.1.1.25, vrf id 0
Default local pref 100, local AS 100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* i1.1.1.0/24	1.1.1.27	0	100	0	i
* i	1.1.1.26	0	100	0	i
*>	0.0.0.0	0		32768	i
*> 2.2.0.0/23	1.1.1.18	0		0	200 i
*> 2.2.2.0/24	1.1.1.18	0		0	200 i
*>i3.3.0.0/23	1.1.1.26	0	100	0	300 i
*>i3.3.2.0/24	1.1.1.26	0	100	0	300 i
*>i4.4.0.0/22	1.1.1.27	0	100	0	400 i

6.2.2 Διευθέτηση Δρομολογητή R2

R2# show running-config
Building configuration...

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R2
service integrated-vtysh-config
!
ip route 1.1.1.0/24 Null0 254
!
interface eth0
 description eBGP
 ip address 1.1.1.36/29
!
interface eth1
 description Point-to-Point Connection with R1
 ip address 1.1.1.2/30
!
interface eth2
 description Point-to-Point Connection with R4
 ip address 1.1.1.9/30
!
interface lo
 description iBGP
 ip address 1.1.1.27/32
!
```

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.25 remote-as 100
 neighbor 1.1.1.25 update-source lo
 neighbor 1.1.1.26 remote-as 100
 neighbor 1.1.1.26 update-source lo
 neighbor 1.1.1.34 remote-as 400
 !
 address-family ipv4 unicast
  network 1.1.1.0/24
  neighbor 1.1.1.34 soft-reconfiguration inbound
  neighbor 1.1.1.25 next-hop-self
  neighbor 1.1.1.25 soft-reconfiguration inbound
  neighbor 1.1.1.26 next-hop-self
  neighbor 1.1.1.26 soft-reconfiguration inbound
 exit-address-family
!
router ospf
 redistribute bgp route-map CHECKCOMMUNITY
 passive-interface eth0
 passive-interface lo
 network 1.1.1.0/30 area 0
 network 1.1.1.8/30 area 0
 network 1.1.1.27/32 area 0
 network 1.1.1.32/29 area 0
!
bgp community-list 1 permit 100:400
!
route-map CHECKCOMMUNITY permit 10
 match community 1
!
line vty
!
end
```

Ο δρομολογητής R2 βρίσκεται στο AS100 και χρησιμοποιεί ως IGP το OSPF και EGP το BGP. Ο ανωτέρω δρομολογητής έχει τρεις BGP peers (neighbors): τον 1.1.1.34 που βρίσκεται σε διαφορετικό AS (AS400), οπότε πρόκειται για eBGP διασύνδεση και τους 1.1.1.25 και 1.1.1.26 που βρίσκονται στο ίδιο AS (AS100), οπότε πρόκειται για iBGP διασυνδέσεις. Για τις iBGP διασυνδεσεις έχει χρησιμοποιηθεί το loop back interface lo από όλους τους peers με σκοπό να υπάρχει η δυνατότητα επιμερισμού του φορτίου κίνησης (load balancing). Όπως παρατηρούμε τα δίκτυα που ανακοινώνονται στο πρωτόκολλο BGP γνωστοποιούνται και στο πρωτόκολλο OSPF με σκοπό να ενημερωθούν για αυτά και οι υπόλοιποι δρομολογητές εντός του AS. Αυτό πραγματοποιείται με την εντολή redistribute η οποία μάλιστα χρησιμοποεί και το φίλτρο CHECKCOMMUNITY για να ανακοινώσει στο πρωτόκολλο OSPF μόνο τα δίκτυα που προέρχονται από το AS400 και όχι αυτά που προέρχονται από τα AS200 και AS300.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R2. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS100, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, ενώ αντίθετα για όλα τα δίκτυα των υπόλοιπων AS που έχουν ανακοινωθεί από το πρωτόκολλο BGP εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινώθηκαν από τους αντίστοιχους eBGP preers.

R2# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
```

```
> - selected route, * - FIB route, q - queued route, r - rejected route

O   1.1.1.0/30 [110/100] is directly connected, eth1, 02:04:17
C>* 1.1.1.0/30 is directly connected, eth1, 02:04:21
O>* 1.1.1.4/30 [110/200] via 1.1.1.1, eth1, 02:04:13
O   1.1.1.8/30 [110/100] is directly connected, eth2, 02:04:19
C>* 1.1.1.8/30 is directly connected, eth2, 02:04:21
O>* 1.1.1.12/30 [110/200] via 1.1.1.10, eth2, 02:04:13
O>* 1.1.1.16/30 [110/200] via 1.1.1.1, eth1, 02:04:13
O>* 1.1.1.20/30 [110/200] via 1.1.1.10, eth2, 02:04:13
O>* 1.1.1.25/32 [110/100] via 1.1.1.1, eth1, 02:04:13
O>* 1.1.1.26/32 [110/100] via 1.1.1.10, eth2, 02:04:13
O   1.1.1.27/32 [110/0] is directly connected, lo, 02:04:19
C>* 1.1.1.27/32 is directly connected, lo, 02:04:21
O   1.1.1.32/29 [110/100] is directly connected, eth0, 02:04:19
C>* 1.1.1.32/29 is directly connected, eth0, 02:04:21
B   2.2.0.0/23 [200/0] via 1.1.1.25 (recursive), 02:03:59
                       via 1.1.1.1, eth1, 02:03:59
O>* 2.2.0.0/23 [110/20] via 1.1.1.1, eth1, 02:04:12
B   2.2.2.0/24 [200/0] via 1.1.1.25 (recursive), 02:03:59
                       via 1.1.1.1, eth1, 02:03:59
O>* 2.2.2.0/24 [110/20] via 1.1.1.1, eth1, 02:04:12
B   3.3.0.0/23 [200/0] via 1.1.1.26 (recursive), 02:04:10
                       via 1.1.1.10, eth2, 02:04:10
O>* 3.3.0.0/23 [110/20] via 1.1.1.10, eth2, 02:04:12
B   3.3.2.0/24 [200/0] via 1.1.1.26 (recursive), 02:04:10
                       via 1.1.1.10, eth2, 02:04:10
O>* 3.3.2.0/24 [110/20] via 1.1.1.10, eth2, 02:04:12
B>* 4.4.0.0/22 [20/0] via 1.1.1.34, eth0, 01:13:52
```

6.2.3 Διευθέτηση Δρομολογητή R3

R3# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R3
service integrated-vtysh-config
!
interface eth1
 description Point-to-Point Connection with R4
 ip address 1.1.1.13/30
!
interface eth2
 description Point-to-Point Connection with R1
 ip address 1.1.1.6/30
!
router ospf
 network 1.1.1.4/30 area 0
 network 1.1.1.12/30 area 0
!
line vty
```

```
!
end
```

Ομοίως ο δρομολογητής R3 βρίσκεται στο AS100 και χρησιμοποιεί ως IGP το OSPF πρωτόκολλο. Δεδομένου ότι δρομολογητής R3 δεν αποτελεί έναν ASBR για το AS100 δεν τρέχει σε αυτόν το πρωτόκολλο BGP.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R3. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS100, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, ενώ αντίθετα για όλα τα δίκτυα των υπόλοιπων AS που έχουν γίνει redistribute από το πρωτόκολλο BGP στο OSPF πρωτόκολλο εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινώθηκαν από τους αντίστοιχους eBGP preers.

R3# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


O>* 1.1.1.0/30 [110/200] via 1.1.1.5, eth2, 04:40:53
O   1.1.1.4/30 [110/100] is directly connected, eth2, 04:41:03
C>* 1.1.1.4/30 is directly connected, eth2, 04:42:02
O>* 1.1.1.8/30 [110/200] via 1.1.1.14, eth1, 04:40:54
O   1.1.1.12/30 [110/100] is directly connected, eth1, 04:41:48
C>* 1.1.1.12/30 is directly connected, eth1, 04:42:02
O>* 1.1.1.16/30 [110/200] via 1.1.1.5, eth2, 04:40:53
O>* 1.1.1.20/30 [110/200] via 1.1.1.14, eth1, 04:40:54
O>* 1.1.1.25/32 [110/100] via 1.1.1.5, eth2, 04:40:53
O>* 1.1.1.26/32 [110/100] via 1.1.1.14, eth1, 04:40:54
O>* 1.1.1.27/32 [110/200] via 1.1.1.5, eth2, 02:07:15
  *                       via 1.1.1.14, eth1, 02:07:15
O>* 1.1.1.32/29 [110/300] via 1.1.1.5, eth2, 02:07:15
  *                       via 1.1.1.14, eth1, 02:07:15
O>* 2.2.0.0/23 [110/20] via 1.1.1.5, eth2, 04:40:53
O>* 2.2.2.0/24 [110/20] via 1.1.1.5, eth2, 04:40:53
O>* 3.3.0.0/23 [110/20] via 1.1.1.14, eth1, 04:40:53
O>* 3.3.2.0/24 [110/20] via 1.1.1.14, eth1, 04:40:53
O>* 4.4.0.0/22 [110/20] via 1.1.1.5, eth2, 01:16:54
  *                     via 1.1.1.14, eth1, 01:16:54
```

6.2.4 Διευθέτηση Δρομολογητή R4

R4# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R4
service integrated-vtysh-config
```

```
!
ip route 1.1.1.0/24 Null0 254
!
interface eth0
 description eBGP
 ip address 1.1.1.21/30
!
interface eth1
 description Point-to-Point Connection with R3
 ip address 1.1.1.14/30
!
interface eth2
 description Point-to-Point Connection with R2
 ip address 1.1.1.10/30
!
interface lo
 description iBGP
 ip address 1.1.1.26/32
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.22 remote-as 300
 neighbor 1.1.1.25 remote-as 100
 neighbor 1.1.1.25 update-source lo
 neighbor 1.1.1.27 remote-as 100
 neighbor 1.1.1.27 update-source lo
 !
 address-family ipv4 unicast
  network 1.1.1.0/24
  neighbor 1.1.1.22 soft-reconfiguration inbound
  neighbor 1.1.1.25 next-hop-self
  neighbor 1.1.1.25 soft-reconfiguration inbound
  neighbor 1.1.1.27 next-hop-self
  neighbor 1.1.1.27 soft-reconfiguration inbound
 exit-address-family
!
router ospf
 redistribute bgp route-map CHECKCOMMUNITY
 passive-interface eth0
 passive-interface lo
 network 1.1.1.8/30 area 0
 network 1.1.1.12/30 area 0
 network 1.1.1.20/30 area 0
 network 1.1.1.26/32 area 0
!
bgp community-list 1 permit 100:300
!
route-map CHECKCOMMUNITY permit 10
 match community 1
!
line vty
!
end
```

Ο δρομολογητής R1 βρίσκεται στο AS100 και χρησιμοποιεί ως IGP το OSPF και EGP το BGP. Ο ανωτέρω δρομολογητής έχει τρεις BGP peers (neighbors): τον 1.1.1.22 που βρίσκεται σε διαφορετικό AS (AS300), οπότε πρόκειται για eBGP διασύνδεση και τους 1.1.1.25 και 1.1.1.27 που βρίσκονται στο ίδιο AS (AS100), οπότε πρόκειται για iBGP διασυνδέσεις. Για τις iBGP διασυνδεσεις έχει

χρησιμοποιηθεί το loop back interface lo από όλους τους peers με σκοπό να υπάρχει η δυνατότητα επιμερισμού του φορτίου κίνησης (load balancing). Όπως παρατηρούμε τα δίκτυα που ανακοινώνονται στο πρωτόκολλο BGP γνωστοποιούνται και στο πρωτόκολλο OSPF με σκοπό να ενημερωθούν για αυτά και οι υπόλοιποι δρομολογητές εντός του AS. Αυτό πραγματοποιείται με την εντολή redistribute η οποία μάλιστα χρησιμοποεί και το φίλτρο CHECKCOMMUNITY για να ανακοινώσει στο πρωτόκολλο OSPF μόνο τα δίκτυα που προέρχονται από το AS300 και όχι αυτά που προέρχονται από τα AS200 και AS400.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R1. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS100, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, ενώ αντίθετα για όλα τα δίκτυα των υπόλοιπων AS που έχουν ανακοινωθεί από το πρωτόκολλο BGP εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινώθηκαν από τους αντίστοιχους eBGP preers.

R4# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 1.1.1.0/30 [110/200] via 1.1.1.9, eth2, 02:12:31
O>* 1.1.1.4/30 [110/200] via 1.1.1.13, eth1, 04:46:05
O   1.1.1.8/30 [110/100] is directly connected, eth2, 04:46:55
C>* 1.1.1.8/30 is directly connected, eth2, 04:47:10
O   1.1.1.12/30 [110/100] is directly connected, eth1, 04:46:55
C>* 1.1.1.12/30 is directly connected, eth1, 04:47:10
O>* 1.1.1.16/30 [110/300] via 1.1.1.9, eth2, 02:12:31
  *                       via 1.1.1.13, eth1, 02:12:31
O   1.1.1.20/30 [110/100] is directly connected, eth0, 04:46:55
C>* 1.1.1.20/30 is directly connected, eth0, 04:47:10
O>* 1.1.1.25/32 [110/200] via 1.1.1.9, eth2, 02:12:31
  *                       via 1.1.1.13, eth1, 02:12:31
O   1.1.1.26/32 [110/0] is directly connected, lo, 04:46:55
C>* 1.1.1.26/32 is directly connected, lo, 04:47:10
O>* 1.1.1.27/32 [110/100] via 1.1.1.9, eth2, 02:12:31
O>* 1.1.1.32/29 [110/200] via 1.1.1.9, eth2, 02:12:31
O>* 2.2.0.0/23 [110/20] via 1.1.1.9, eth2, 02:12:30
  *                     via 1.1.1.13, eth1, 02:12:30
B   2.2.0.0/23 [200/0] via 1.1.1.25 (recursive), 02:12:31
                       via 1.1.1.9, eth2, 02:12:31
                       via 1.1.1.13, eth1, 02:12:31
O>* 2.2.2.0/24 [110/20] via 1.1.1.9, eth2, 02:12:30
  *                     via 1.1.1.13, eth1, 02:12:30
B   2.2.2.0/24 [200/0] via 1.1.1.25 (recursive), 02:12:31
                       via 1.1.1.9, eth2, 02:12:31
                       via 1.1.1.13, eth1, 02:12:31
B>* 3.3.0.0/23 [20/0] via 1.1.1.22, eth0, 04:47:01
B>* 3.3.2.0/24 [20/0] via 1.1.1.22, eth0, 04:47:01
B   4.4.0.0/22 [200/0] via 1.1.1.27 (recursive), 01:22:11
                       via 1.1.1.9, eth2, 01:22:11
O>* 4.4.0.0/22 [110/20] via 1.1.1.9, eth2, 01:22:11
```

6.2.5 Διευθέτηση Δρομολογητή R5

R5# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R5
service integrated-vtysh-config
!
ip route 2.2.0.0/23 Null0 254
ip route 2.2.2.0/24 Null0 254
!
interface eth0
 description Point-to-Point Connection with R1
 ip address 1.1.1.18/30
!
interface eth1
 description Point-to-Point Connection with R6
 ip address 2.2.2.1/30
!
interface eth2
 description Point-to-Point Connection with R7
 ip address 2.2.2.5/30
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 1.1.1.17 remote-as 100
 !
 address-family ipv4 unicast
  network 2.2.0.0/23
  network 2.2.2.0/24
  neighbor 1.1.1.17 soft-reconfiguration inbound
  neighbor 1.1.1.17 route-map SETCOMMUNITY out
 exit-address-family
!
router ospf
 passive-interface eth0
 network 2.2.2.0/30 area 0
 network 2.2.2.4/30 area 0
!
ip prefix-list PLIST seq 20 permit 2.2.0.0/23
ip prefix-list PLIST seq 25 permit 2.2.2.0/24
!
route-map SETCOMMUNITY permit 10
 match ip address prefix-list PLIST
 set community 100:200
!
line vty
!
end
```

Ο δρομολογητής R5 βρίσκεται στο AS200 και χρησιμοποιεί ως IGP το OSPF και EGP το BGP. Ο ανωτέρω δρομολογητής έχει έναν BGP peer (neighbor): τον 1.1.1.17 που βρίσκεται σε διαφορετικό AS (AS100), οπότε πρόκειται για eBGP διασύνδεση. Όπως παρατηρούμε στα δίκτυα που ανακοινώνονται από το πρωτόκολλο BGP προς τον eBGP peer 1.1.1.17 τοποθετείται με βάση το φίλτρο SETCOMMUNITY το community 100:200, έτσι ώστε όταν αυτά εισέλθουν στο AS100 να μπορούν να φιλτραριστούν με βάση αυτό το community και να ξεχωρίσουν από εκείνα που εισέρχονται από τα

AS300 και AS400 στα οποία έχει τοποθετηθεί το community 100:300 και 100:400 αντίστοιχα. Δεδομένου ότι το εν λόγω AS διαθέτει μόνο μία έξοδο προς τα άλλα AS αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1, R2 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο εν λόγω δρομολογητής ως last resort (default router) για τους υπόλοιπους δρομολογητές του AS200.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R5. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS200, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, ενώ αντίθετα για όλα τα δίκτυα των υπόλοιπων AS που έχουν ανακοινωθεί από το πρωτόκολλο BGP εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινώθηκαν από τον αντίστοιχο eBGP preer.

R5# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
F - PBR, f - OpenFabric,
> - selected route, * - FIB route, q - queued route, r - rejected route

B>* 1.1.1.0/24 [20/0] via 1.1.1.17, eth0, 04:52:30
C>* 1.1.1.16/30 is directly connected, eth0, 04:52:38
O>* 2.2.0.0/24 [110/200] via 2.2.2.2, eth1, 04:51:32
O>* 2.2.1.0/24 [110/200] via 2.2.2.6, eth2, 04:51:31
O 2.2.2.0/30 [110/100] is directly connected, eth1, 04:52:22
C>* 2.2.2.0/30 is directly connected, eth1, 04:52:38
O 2.2.2.4/30 [110/100] is directly connected, eth2, 04:52:22
C>* 2.2.2.4/30 is directly connected, eth2, 04:52:38
O>* 2.2.2.8/30 [110/200] via 2.2.2.2, eth1, 04:51:31
* via 2.2.2.6, eth2, 04:51:31
B>* 3.3.0.0/23 [20/0] via 1.1.1.17, eth0, 04:51:25
B>* 3.3.2.0/24 [20/0] via 1.1.1.17, eth0, 04:51:25
B>* 4.4.0.0/22 [20/0] via 1.1.1.17, eth0, 01:27:34

6.2.6 Διευθέτηση Δρομολογητή R6

R6# show running-config
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R6
service integrated-vtysh-config
!
ip route 0.0.0.0/0 2.2.2.1
!
interface eth0
description LAN
ip address 2.2.0.1/24
!
interface eth1
description Point-to-Point Connection with R5
ip address 2.2.2.2/30

```
!
interface eth3
 description Point-to-Point Connection with R7
 ip address 2.2.2.9/30
!
router ospf
 passive-interface eth0
 network 2.2.0.0/24 area 0
 network 2.2.2.0/30 area 0
 network 2.2.2.8/30 area 0
!
line vty
!
end
```

Όπως παρατηρούμε ο δρομολογητής R6 βρίσκεται στο AS200 και χρησιμοποιεί ως IGP το OSPF πρωτόκολλο. Δεδομένου ότι δρομολογητής R6 δεν αποτελεί έναν ASBR για το AS200 δεν τρέχει σε αυτόν το πρωτόκολλο BGP. Δεδομένου ότι το εν λόγω AS διαθέτει μόνο μία έξοδο προς τα άλλα AS αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο δρομολογητής R5 ως last resort (default router).

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R6. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS200, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, καθώς επίσης και το default route 0.0.0.0/0 προς τον δρομολογητή R5.

R6# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 0.0.0.0/0 [1/0] via 2.2.2.1, eth1, 04:54:00
O     2.2.0.0/24 [110/100] is directly connected, eth0, 04:54:08
C>* 2.2.0.0/24 is directly connected, eth0, 04:54:17
O>* 2.2.1.0/24 [110/200] via 2.2.2.10, eth3, 04:53:11
O     2.2.2.0/30 [110/100] is directly connected, eth1, 04:54:08
C>* 2.2.2.0/30 is directly connected, eth1, 04:54:17
O>* 2.2.2.4/30 [110/200] via 2.2.2.1, eth1, 04:53:11
  *                        via 2.2.2.10, eth3, 04:53:11
O     2.2.2.8/30 [110/100] is directly connected, eth3, 04:53:21
C>* 2.2.2.8/30 is directly connected, eth3, 04:54:16
```

6.2.7 Διευθέτηση Δρομολογητή R7

R7# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
```

```
hostname R7
service integrated-vtysh-config
!
ip route 0.0.0.0/0 2.2.2.5
!
interface eth0
 description LAN
 ip address 2.2.1.1/24
!
interface eth2
 description Point-to-Point Connection with R5
 ip address 2.2.2.6/30
!
interface eth3
 description Point-to-Point Connection with R6
 ip address 2.2.2.10/30
!
router ospf
 passive-interface eth0
 network 2.2.1.0/24 area 0
 network 2.2.2.4/30 area 0
 network 2.2.2.8/30 area 0
!
line vty
!
end
```

Ομοίως ο δρομολογητής R7 βρίσκεται στο AS200 και χρησιμοποιεί ως IGP το OSPF πρωτόκολλο. Δεδομένου ότι δρομολογητής R7 δεν αποτελεί έναν ASBR για το AS200 δεν τρέχει σε αυτόν το πρωτόκολλο BGP. Δεδομένου ότι το εν λόγω AS διαθέτει μόνο μία έξοδο προς τα άλλα AS αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο δρομολογητής R5 ως last resort (default router).

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R7. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS200, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, καθώς επίσης και το default route 0.0.0.0/0 προς τον δρομολογητή R5.

R7# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>*  0.0.0.0/0 [1/0] via 2.2.2.5, eth2, 04:55:12
O>* 2.2.0.0/24 [110/200] via 2.2.2.9, eth3, 04:54:30
O     2.2.1.0/24 [110/100] is directly connected, eth0, 04:55:15
C>* 2.2.1.0/24 is directly connected, eth0, 04:55:32
O>* 2.2.2.0/30 [110/200] via 2.2.2.5, eth2, 04:54:30
  *                          via 2.2.2.9, eth3, 04:54:30
O     2.2.2.4/30 [110/100] is directly connected, eth2, 04:55:15
C>* 2.2.2.4/30 is directly connected, eth2, 04:55:32
O     2.2.2.8/30 [110/100] is directly connected, eth3, 04:55:15
C>* 2.2.2.8/30 is directly connected, eth3, 04:55:32
```

6.2.8 Διευθέτηση Δρομολογητή R8

R8# show running-config
Building configuration...

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R8
service integrated-vtysh-config
!
ip route 3.3.0.0/23 Null0 254
ip route 3.3.2.0/24 Null0 254
!
interface eth0
 description Point-to-Point Connection with R4
 ip address 1.1.1.22/30
!
interface eth1
 description Point-to-Point Connection with R9
 ip address 3.3.2.1/30
!
interface eth2
 description Point-to-Point Connection with R10
 ip address 3.3.2.5/30
!
router bgp 300
 bgp log-neighbor-changes
 neighbor 1.1.1.21 remote-as 100
 !
 address-family ipv4 unicast
  network 3.3.0.0/23
  network 3.3.2.0/24
  neighbor 1.1.1.21 soft-reconfiguration inbound
  neighbor 1.1.1.21 route-map SETCOMMUNITY out
 exit-address-family
!
router ospf
 passive-interface eth0
 network 3.3.2.0/30 area 0
 network 3.3.2.4/30 area 0
!
ip prefix-list PLIST seq 10 permit 3.3.2.0/24
ip prefix-list PLIST seq 5 permit 3.3.0.0/23
!
route-map SETCOMMUNITY permit 10
 match ip address prefix-list PLIST
 set community 100:300
!
line vty
!
end
```

Ο δρομολογητής R8 βρίσκεται στο AS300 και χρησιμοποιεί ως IGP το OSPF και EGP το BGP. Ο ανωτέρω δρομολογητής έχει έναν BGP peer (neighbor): τον 1.1.1.21 που βρίσκεται σε διαφορετικό AS (AS100), οπότε πρόκειται για eBGP διασύνδεση. Όπως παρατηρούμε στα δίκτυα που ανακοινώνονται

από το πρωτόκολλο BGP προς τον eBGP peer 1.1.1.21 τοποθετείται με βάση το φίλτρο SETCOMMUNITY το community 100:300, έτσι ώστε όταν αυτά εισέλθουν στο AS100 να μπορούν να φιλτραριστούν με βάση αυτό το community και να ξεχωρίσουν από εκείνα που εισέρχονται από τα AS200 και AS400 στα οποία έχει τοποθετηθεί το community 100:200 και 100:400 αντίστοιχα. Δεδομένου ότι το εν λόγω AS διαθέτει μόνο μία έξοδο προς τα άλλα AS αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1, R2 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο εν λόγω δρομολογητής ως last resort (default router) για τους υπόλοιπους δρομολογητές του AS300.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R8. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS300, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, ενώ αντίθετα για όλα τα δίκτυα των υπόλοιπων AS που έχουν ανακοινωθεί από το πρωτόκολλο BGP εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινώθηκαν από τον αντίστοιχο eBGP preer.

```
R8# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

B>* 1.1.1.0/24 [20/0] via 1.1.1.21, eth0, 04:58:25
C>* 1.1.1.20/30 is directly connected, eth0, 04:58:33
B>* 2.2.0.0/23 [20/0] via 1.1.1.21, eth0, 04:57:27
B>* 2.2.2.0/24 [20/0] via 1.1.1.21, eth0, 04:57:27
O>* 3.3.0.0/24 [110/200] via 3.3.2.2, eth1, 04:57:29
O>* 3.3.1.0/24 [110/200] via 3.3.2.6, eth2, 04:57:37
O   3.3.2.0/30 [110/100] is directly connected, eth1, 04:57:36
C>* 3.3.2.0/30 is directly connected, eth1, 04:58:33
O   3.3.2.4/30 [110/100] is directly connected, eth2, 04:57:38
C>* 3.3.2.4/30 is directly connected, eth2, 04:58:32
O>* 3.3.2.8/30 [110/200] via 3.3.2.2, eth1, 04:57:29
  *                       via 3.3.2.6, eth2, 04:57:29
B>* 4.4.0.0/22 [20/0] via 1.1.1.21, eth0, 01:33:35
```

6.2.9 Διευθέτηση Δρομολογητή R9

```
R9# show running-config
Building configuration...

Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R9
service integrated-vtysh-config
!
ip route 0.0.0.0/0 3.3.2.1
!
interface eth0
 description LAN
 ip address 3.3.0.1/24
```

```
!
interface eth1
 description Point-to-Point Connection with R8
 ip address 3.3.2.2/30
!
interface eth3
 description Point-to-Point Connection with R10
 ip address 3.3.2.9/30
!
router ospf
 passive-interface eth0
 network 3.3.0.0/24 area 0
 network 3.3.2.0/30 area 0
 network 3.3.2.8/30 area 0
!
line vty
!
end
```

Όπως παρατηρούμε ο δρομολογητής R9 βρίσκεται στο AS300 και χρησιμοποιεί ως IGP το OSPF πρωτόκολλο. Δεδομένου ότι δρομολογητής R9 δεν αποτελεί έναν ASBR για το AS300 δεν τρέχει σε αυτόν το πρωτόκολλο BGP. Δεδομένου ότι το εν λόγω AS διαθέτει μόνο μία έξοδο προς τα άλλα AS αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1, R2 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο δρομολογητής R8 ως last resort (default router).

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R9. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS300, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, καθώς επίσης και το default route 0.0.0.0/0 προς τον δρομολογητή R8.

```
R9# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 0.0.0.0/0 [1/0] via 3.3.2.1, eth1, 04:59:44
O     3.3.0.0/24 [110/100] is directly connected, eth0, 04:59:47
C>* 3.3.0.0/24 is directly connected, eth0, 05:00:01
O>* 3.3.1.0/24 [110/200] via 3.3.2.10, eth3, 04:58:53
O     3.3.2.0/30 [110/100] is directly connected, eth1, 04:59:47
C>* 3.3.2.0/30 is directly connected, eth1, 05:00:01
O>* 3.3.2.4/30 [110/200] via 3.3.2.1, eth1, 04:58:53
  *                       via 3.3.2.10, eth3, 04:58:53
O     3.3.2.8/30 [110/100] is directly connected, eth3, 04:59:47
C>* 3.3.2.8/30 is directly connected, eth3, 05:00:01
```

6.2.10 Διευθέτηση Δρομολογητή R10

```
frr# show running-config
Building configuration...
```

```
Current configuration:
!
frr version 7.3.1
frr defaults traditional
hostname frr
hostname R10
service integrated-vtysh-config
!
ip route 0.0.0.0/0 3.3.2.5
!
interface eth0
 description LAN
 ip address 3.3.1.1/24
!
interface eth2
 description Point-to-Point Connection with R8
 ip address 3.3.2.6/30
!
interface eth3
 description Point-to-Point Connection with R9
 ip address 3.3.2.10/30
!
router ospf
 passive-interface eth0
 network 3.3.1.0/24 area 0
 network 3.3.2.4/30 area 0
 network 3.3.2.8/30 area 0
!
line vty
!
end
```

Ομοίως ο δρομολογητής R10 βρίσκεται στο AS300 και χρησιμοποιεί ως IGP το OSPF πρωτόκολλο. Δεδομένου ότι δρομολογητής R10 δεν αποτελεί έναν ASBR για το AS300 δεν τρέχει σε αυτόν το πρωτόκολλο BGP. Δεδομένου ότι το εν λόγω AS διαθέτει μόνο μία έξοδο προς τα άλλα AS αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1, R2 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο δρομολογητής R8 ως last resort (default router).

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή R10. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS300, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, καθώς επίσης και το default route 0.0.0.0/0 προς τον δρομολογητή R8.

```
R10#  show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>*  0.0.0.0/0 [1/0] via 3.3.2.5, eth2, 05:01:05
O>* 3.3.0.0/24 [110/200] via 3.3.2.9, eth3, 05:00:13
O     3.3.1.0/24 [110/100] is directly connected, eth0, 05:00:55
C>* 3.3.1.0/24 is directly connected, eth0, 05:01:10
O>* 3.3.2.0/30 [110/200] via 3.3.2.5, eth2, 05:00:05
  *                           via 3.3.2.9, eth3, 05:00:05
O     3.3.2.4/30 [110/100] is directly connected, eth2, 05:00:55
```

```
C>* 3.3.2.4/30 is directly connected, eth2, 05:01:10
O   3.3.2.8/30 [110/100] is directly connected, eth3, 05:00:55
C>* 3.3.2.8/30 is directly connected, eth3, 05:01:09
```

6.2.11 Διευθέτηση Δρομολογητή RSB1 (Raspberry Pi 4)

RSB1# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname raspberrypi
hostname RSB1
log syslog informational
no ipv6 forwarding
service integrated-vtysh-config
!
ip route 0.0.0.0/0 192.168.2.1
ip route 4.4.0.0/22 Null0 254
!
interface br0
 description Connection with LAN (Bridge eth0 with wlan0)
 ip address 4.4.1.1/24
!
interface eth1
 description Point-to-Point Connection with RSB2
 ip address 4.4.0.1/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with RSB3
 ip address 4.4.0.5/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth3
 description Connection with WAN
 ip address 192.168.2.100/24
!
interface eth4
 description Connection with GNS3
 ip address 1.1.1.34/29
!
router bgp 400
 bgp log-neighbor-changes
 neighbor 1.1.1.36 remote-as 100
 !
 address-family ipv4 unicast
  network 4.4.0.0/22
  neighbor 1.1.1.36 soft-reconfiguration inbound
  neighbor 1.1.1.36 route-map ALLOWALL in
  neighbor 1.1.1.36 route-map SETCOMMUNITY out
 exit-address-family
!
router ospf
```

```
 ospf router-id 1.1.1.34
 passive-interface br0
 passive-interface eth3
 passive-interface eth4
 network 4.4.0.0/30 area 3
 network 4.4.0.4/30 area 3
 network 4.4.1.0/24 area 3
 area 3 authentication message-digest
 default-information originate
!
ip prefix-list PLIST seq 5 permit 4.4.0.0/22
!
route-map SETCOMMUNITY permit 10
 match ip address prefix-list PLIST
 set community 100:400
!
route-map ALLOWALL permit 10
!
line vty
!
end
```

Ο δρομολογητής RSB1 βρίσκεται στο AS400 και χρησιμοποιεί ως IGP το OSPF και EGP το BGP. Ο ανωτέρω δρομολογητής έχει έναν BGP peer (neighbor): τον 1.1.1.36 που βρίσκεται σε διαφορετικό AS (AS100), οπότε πρόκειται για eBGP διασύνδεση. Όπως παρατηρούμε στα δίκτυα που ανακοινώνονται από το πρωτόκολλο BGP προς τον eBGP peer 1.1.1.36 τοποθετείται με βάση το φίλτρο SETCOMMUNITY το community 100:400, έτσι ώστε όταν αυτά εισέλθουν στο AS100 να μπορούν να φιλτραριστούν με βάση αυτό το community και να ξεχωρίσουν από εκείνα που εισέρχονται από τα AS200 και AS300 στα οποία έχει τοποθετηθεί το community 100:200 και 100:300 αντίστοιχα. Δεδομένου ότι το εν λόγω AS διαθέτει μόνο μία έξοδο προς τα άλλα AS αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1, R2 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο εν λόγω δρομολογητής ως last resort (default router) για τους υπόλοιπους δρομολογητές του AS400. Έτσι, στο πρωτόκολλο OSPF του δρομολογητή RSB1 έχει δωθεί η εντολή default-information originate με σκοπό να γνωστοποιηθεί το default route 0.0.0.0/0 σε όλους τους neighbors.

Στη συνέχεια εκτελώντας την εντολή **show ip route** εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή RSB1. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS400, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF, ενώ αντίθετα για όλα τα δίκτυα των υπόλοιπων AS που έχουν ανακοινωθεί από το πρωτόκολλο BGP εμφανίζονται μόνο οι αντίστοιχες συναθροίσεις (summary routes), όπως αυτές ανακοινώθηκαν από τον αντίστοιχο eBGP preer.

```
RSB1#  show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

S>* 0.0.0.0/0 [1/0] via 192.168.2.1, eth3, weight 1, 04:08:56
B>* 1.1.1.0/24 [20/0] via 1.1.1.36, eth4, weight 1, 02:05:01
C>* 1.1.1.32/29 is directly connected, eth4, 04:09:01
B>* 2.2.0.0/23 [20/0] via 1.1.1.36, eth4, weight 1, 02:05:01
B>* 2.2.2.0/24 [20/0] via 1.1.1.36, eth4, weight 1, 02:05:01
B>* 3.3.0.0/23 [20/0] via 1.1.1.36, eth4, weight 1, 02:05:01
B>* 3.3.2.0/24 [20/0] via 1.1.1.36, eth4, weight 1, 02:05:01
S>* 4.4.0.0/22 [1/0] unreachable (blackhole), weight 1, 01:53:13
```

```
O   4.4.0.0/30 [110/100] is directly connected, eth1, weight 1, 04:08:19
C>* 4.4.0.0/30 is directly connected, eth1, 04:09:01
O   4.4.0.4/30 [110/100] is directly connected, eth2, weight 1, 01:27:29
C>* 4.4.0.4/30 is directly connected, eth2, 01:27:29
O>* 4.4.0.8/30 [110/200] via 4.4.0.2, eth1, weight 1, 01:26:36
  *                      via 4.4.0.6, eth2, weight 1, 01:26:36
O   4.4.1.0/24 [110/1] is directly connected, br0, weight 1, 04:08:55
C>* 4.4.1.0/24 is directly connected, br0, 04:08:55
O>* 4.4.2.0/24 [110/101] via 4.4.0.2, eth1, weight 1, 04:08:13
O>* 4.4.3.0/24 [110/101] via 4.4.0.6, eth2, weight 1, 01:26:36
C>* 192.168.2.0/24 is directly connected, eth3, 04:09:01
```

6.2.12 Διευθέτηση Δρομολογητή RSB2 (Raspberry Pi 4)

RSB2# show running-config

```
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname raspberrypi
hostname RSB2
log syslog informational
no ipv6 forwarding
service integrated-vtysh-config
!
interface br0
 description Connection with LAN (Bridge eth0 with wlan0)
 ip address 4.4.2.1/24
!
interface eth1
 description Point-to-Point Connection with RSB1
 ip address 4.4.0.2/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with RSB3
 ip address 4.4.0.9/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface br0
 network 4.4.0.0/30 area 3
 network 4.4.0.8/30 area 3
 network 4.4.2.0/24 area 3
 area 3 authentication message-digest
!
line vty
!
end
```

Όπως παρατηρούμε ο δρομολογητής RSB2 βρίσκεται στο AS400 και χρησιμοποιεί ως IGP το OSPF πρωτόκολλο. Δεδομένου ότι δρομολογητής RSB2 δεν αποτελεί έναν ASBR για το AS400 δεν τρέχει σε αυτόν το πρωτόκολλο BGP. Επιπλέον, εξαιτίας του γεγονότος ότι το εν λόγω AS διαθέτει μόνο έναν ASBR αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF

πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1, R2 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο δρομολογητής RSB1 ως last resort (default router).

Στη συνέχεια εκτελώντας την εντολή show ip route εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή RSB2. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS400, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή RSB1 έχει δωθεί η εντολή default-information originate.

RSB2# show ip route
```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

O>* 0.0.0.0/0 [110/10] via 4.4.0.1, eth1, weight 1, 04:27:05
O     4.4.0.0/30 [110/100] is directly connected, eth1, weight 1, 04:27:54
C>* 4.4.0.0/30 is directly connected, eth1, 04:27:54
O>* 4.4.0.4/30 [110/200] via 4.4.0.1, eth1, weight 1, 01:45:27
  *                       via 4.4.0.10, eth2, weight 1, 01:45:27
O     4.4.0.8/30 [110/100] is directly connected, eth2, weight 1, 01:45:37
C>* 4.4.0.8/30 is directly connected, eth2, 01:46:20
O>* 4.4.1.0/24 [110/101] via 4.4.0.1, eth1, weight 1, 04:27:06
O     4.4.2.0/24 [110/1] is directly connected, br0, weight 1, 06:04:59
C>* 4.4.2.0/24 is directly connected, br0, 06:04:59
O>* 4.4.3.0/24 [110/101] via 4.4.0.10, eth2, weight 1, 01:45:27
```

6.2.13 Διευθέτηση Δρομολογητή RSB3 (Raspberry Pi 4)

RSB3# show running-config
```
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname raspberrypi
hostname RSB3
log syslog informational
no ipv6 forwarding
service integrated-vtysh-config
!
interface br0
 description Connection with LAN (Bridge eth0 wlan0)
 ip address 4.4.3.1/24
!
interface eth1
 description Point-to-Point Connection with RSB1
 ip address 4.4.0.6/30
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
interface eth2
 description Point-to-Point Connection with RSB2
 ip address 4.4.0.10/30
```

```
 ip ospf message-digest-key 2 md5 SECRETKEY2
!
router ospf
 passive-interface br0
 network 4.4.0.4/30 area 3
 network 4.4.0.8/30 area 3
 network 4.4.3.0/24 area 3
 area 3 authentication message-digest
!
line vty
!
end
```

Όπως παρατηρούμε ο δρομολογητής RSB3 βρίσκεται στο AS400 και χρησιμοποιεί ως IGP το OSPF πρωτόκολλο. Δεδομένου ότι δρομολογητής RSB3 δεν αποτελεί έναν ASBR για το AS400 δεν τρέχει σε αυτόν το πρωτόκολλο BGP. Επιπλέον, εξαιτίας του γεγονότος ότι το εν λόγω AS διαθέτει μόνο έναν ASBR αντί οι εξωτερικές διαδρομές που λαμβάνονται από το BGP να γνωστοποιούνται και στο OSPF πρωτόκολλο με την εντολή redistribute, όπως στην περίπτωση των δρομολογητών R1, R2 και R4 έχει επιλεχθεί να χρησιμοποιηθεί ο δρομολογητής RSB1 ως last resort (default router).

Στη συνέχεια εκτελώντας την εντολή show ip route εμφανίζεται ο πίνακας δρομολόγησης του δρομολογητή RSB3. Παρατηρούμε ότι στον πίνακα δρομολόγησης του ανωτέρω δρομολογητή εμφανίζονται αναλυτικά όλα τα υποδίκτυα του AS400, όπως αυτά έχουν ανακοινωθεί από το πρωτόκολλο OSPF. Τέλος, στον πίνακα δρομολόγησης συμπεριλαμβάνεται και το default route 0.0.0.0/0 παρόλο που δεν το έχουμε δηλώσει με στατική δρομολόγηση και αυτό διότι στο πρωτόκολλο OSPF του δρομολογητή RSB1 έχει δωθεί η εντολή default-information originate.

RSB3# show ip route

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

O>* 0.0.0.0/0 [110/10] via 4.4.0.5, eth1, weight 1, 01:48:10
O>* 4.4.0.0/30 [110/200] via 4.4.0.5, eth1, weight 1, 01:48:11
  *                       via 4.4.0.9, eth2, weight 1, 01:48:11
O   4.4.0.4/30 [110/100] is directly connected, eth1, weight 1, 01:48:58
C>* 4.4.0.4/30 is directly connected, eth1, 01:48:59
O   4.4.0.8/30 [110/100] is directly connected, eth2, weight 1, 01:48:58
C>* 4.4.0.8/30 is directly connected, eth2, 01:48:59
O>* 4.4.1.0/24 [110/101] via 4.4.0.5, eth1, weight 1, 01:48:11
O>* 4.4.2.0/24 [110/101] via 4.4.0.9, eth2, weight 1, 01:48:11
O   4.4.3.0/24 [110/1] is directly connected, br0, weight 1, 01:48:58
C>* 4.4.3.0/24 is directly connected, br0, 01:48:58
```

7

Επίλογος - Συμπεράσματα

Με την παρούσα διπλωματική εργασία παρουσιάζονται και αναλύονται τα βασικά χαρακτηριστικά και ιδιότητες των πρωτοκόλλων δρομολόγησης OSPF και BGP της σουίτας ανοιχτού λογισμικού FRR. Οι μελέτες περιπτώσεων αναπτύχθηκαν και εφαρμόστηκαν σε ένα υβριδικό περιβάλλον που περιλαμβάνει πραγματικές συσκευές (Raspberry Pi 4) που διασυνδέονται μέσω νέφους (cloud) με άλλους δρομολογητές FRR που λειτουργούν σε περιβάλλον προσομοίωσης GNS3 για λόγους οικονομίας και ευελιξίας. Με αυτόν τον τρόπο μπόρεσαν και αναπτύχθηκαν πιο πολύπλοκες μελέτες περιπτώσεων που αναλύουν τόσο την ιεραρχία του πρωτοκόλλου δρομολόγησης OSPF με τη χρήση τεσσάρων περιοχών (areas) όσο και τις δυνατότητες πολιτικών δρομολόγησης του πρωτοκόλλου BGP σε ένα σχήμα που περιλαμβάνει τέσσερα διαφορετικά Αυτόνομα Συστήματα (AS).

Η σουίτα FRR που χρησιμοποιήθηκε αποτελεί ένα πακέτο λογισμικού Unix/Linux που υλοποιεί και υποστηρίζει τη δρομολόγηση δικτύων ακολουθώντας έναν διαφορετικό τρόπο προσέγγισης σε σύγκριση με το παραδοσιακό λογισμικό των συσκευών δρομολόγησης το οποίο αποτελείται από ένα ενιαίο πρόγραμμα διεργασίας που παρέχει όλες τις λειτουργίες των πρωτοκόλλων δρομολόγησης, διασφαλίζοντας έτσι υψηλή ανθεκτικότητα (high resiliency), ευελιξία, επεκτασιμότητα και αρθρωτότητα (modularity).

Βιβλιογραφία-Αναφορές

[1]. James F. Kurose, Keith W. Ross, "Δικτύωση Υπολογιστών, Προσέγγιση από πάνω προς τα κάτω 6η Έκδοση".

[2]. "FRRouting User Guide", [Online]. Available: http://docs.frrouting.org/en/latest/

[3]. P. Jakma, D. Lamparter. "Introduction to the quagga routing suite," 2014, IEEE Network.

[4]. K. Ishiguro, "Gnu zebra", [Online]. Available: http://www.cesarkallas.net/arquivos/faculdade/redes_2/The_Internet_Manual/zebra-manual-Sept2002.pdf

[5]. Cisco Press, "OSPF Implementation", [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=2294214&seqNum=2

[6]. Richard John Whitfield, Shao Ying Zhu "A Comparison of OSPFv3 and EIGRPv6 in a Small IPv6 Enterprise Network", International Journal of Advanced Computer Science and Applications, Vol. 6, No. 1, 2015.

[7]. Cisco, "OSPF Design Guide", [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

[8]. RFC4271, "A Border Gateway Protocol 4 (BGP-4)", [Online]. Available: http://www.ietf.org/rfc/rfc4271.txt

[9]. "Getting Started with GNS3", [Online]. Available: https://docs.gns3.com/docs/

[10]. "GNS3 Download, gns3.com" [Online]. Available: https://www.gns3.com/software

[11]. "GNS3 Documentation, docs.gns3.com", [Online]. Available: https://docs.gns3.com/

[12]. "Download VirtualBox", [Online]. Available: https://www.virtualbox.org/wiki/Downloads

[13]. “Download GNS3 VM”, [Online]. Available: https://gns3.com/software/download-vm