Πανεπιστήμιο Πειραιώς -Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Πλεονεκτήματα του πρωτόκολλου διαδικτύου IPv6 στο Υπολογιστικό Νέφος “Advantages of IPv6 in Cloud Computing”
Ονοματεπώνυμο Φοιτητή	Τσιμπίδης Γεώργιος
Πατρώνυμο	Θεόδωρος
Αριθμός Μητρώου	ΜΠΣΠ/15091
Επιβλέπων	Καθηγητής Δουληγέρης Χρήστος
Ημερομηνία παράδοσης	20 Νοεμβρίου 2018

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης Καθηγητής	Δημήτριος Βέργαδος Αναπληρωτής Καθηγητής	Παναγιώτης Κοτζανικολάου Επίκουρος Καθηγητής

Περίληψη.

Σκοπός αυτής της μεταπτυχιακής διατριβής είναι να τονιστεί η αύξηση των χρηστών που έχουν πρόσβαση στο διαδίκτυο παγκοσμίως καθώς και η ανάγκη τους για ανταλλαγή κάθε είδους πληροφορίας όπου και αν βρίσκονται και από οποιαδήποτε υπολογιστική συσκευή διαθέτουν, είτε είναι ένας σταθερός υπολογιστής είτε μία "έξυπνη" κινητή συσκευή. Αυτό βεβαίως δεν θα ήταν εφικτό χωρίς την ανάπτυξη και τη συνεχή εξέλιξη του υπολογιστικού νέφους (Cloud Computing). Οι διαρκώς αυξανόμενες απαιτήσεις των χρηστών συντονίζονται με την ίδια τάση για εξέλιξη που πρέπει να έχουν και οι δομές – αρχιτεκτονικές των δικτύων που χρησιμοποιεί το υπολογιστικό νέφος. Στην παρούσα εργασία τονίζονται οι σημαντικότερες απαιτήσεις που καθιστούν αναγκαία την χρήση του νέου πρωτοκόλλου IPv6 και φανερώνουν την αδυναμία του IPv4 να ανταποκριθεί στα σύγχρονα δεδομένα την εποχής. Τέλος αφού έχει παρουσιαστεί η δομή και η λειτουργία των δύο αυτών πρωτοκόλλων καθώς και οι μηχανισμοί που τα συνοδεύουν, εξάγονται συμπεράσματα σχετικά με την ασφάλεια των δεδομένων και την κινητικότητα των χρηστών μέσα σε δίκτυα που χρησιμοποιούνται από το υπολογιστικό νέφος.

Abstract.

The purpose of this postgraduate thesis is to highlight the growing trend of users who have access to the internet world wide, as well as the need to exchange all sorts of information wherever they might be and from any computing device, whether it is a fixed computer or a "smart" mobile device. This would certainly not be feasible without the development and continuous advancements of cloud-computing. The ever increasing demands of users are co-ordinated with the same trend for development as the one seen in cloud-computing network architectures. This paper highlights the most important requirements that require the use of the new IPv6 protocol and reveal the inability of IPv4 to respond to modern day data. Finally, after the structure and the operation of these two protocols as well as the accompanying mechanisms have been presented, conclusions are drawn on data security and user mobility within networks used by cloud computing.

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

1. Εισαγωγή

2. Το νέο πρωτόκολλο διαδικτύου IPv6

3. Cloud service models και Virtualization

4. Πλεονεκτήματα του πρωτοκόλλου IPv6 στο Cloud computing

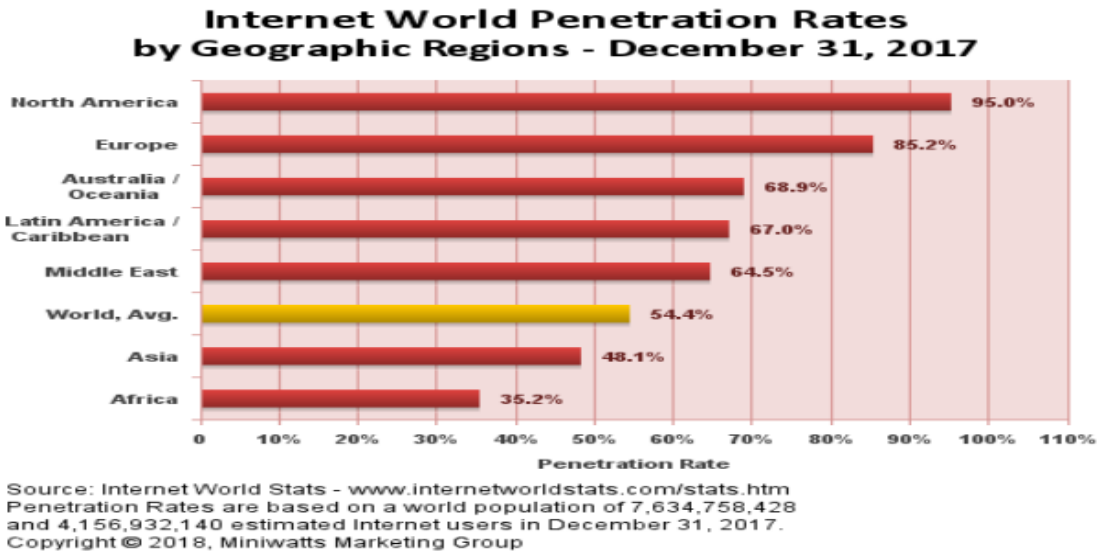
1. Εισαγωγή.

1.1 Η εξέλιξη του διαδικτύου.

Η ραγδαία και γεωμετρικά αυξανόμενη εξέλιξη της τεχνολογίας που συμβαίνει ειδικότερα τα τελευταία χρόνια στον χώρο των μικρό-ελεγκτών των υπολογιστικών συστημάτων, των κινητών συσκευών τηλεφωνίας (smartphones) της νέας τάσης για διαδίκτυο των πραγμάτων (Internet of things) και της δημιουργίας εφαρμογών που αναπτύσσονται καθημερινά ώστε να καλύψουμε τις όλοένα αυξανόμενες ανάγκες μας για ανταλλαγή πληροφοριών, φέρνουν σε πρωταγωνιστική θέση την έννοια του διαδικτύου [1] και φέρνουν στο προσκήνιο τις μεγάλες ανάγκες που υπάρχουν για την εξέλιξη των τεχνολογιών δικτύωσης, αποθήκευσης πληροφοριών και γρήγορης και με ασφάλεια διάδοσης δεδομένων.

1.1.1 Αύξηση απαιτήσεων από τους χρήστες.

Στο παρακάτω διάγραμμα βλέπουμε το ποσοστό πρόσβασης στο διαδίκτυο ανά γεωγραφική περιοχή όπως παρουσιάζεται στην ιστοσελίδα www.internetworldstats.com. Εδώ παρατηρείται ότι πρώτη με 95% είναι η Βόρεια Αμερική και ακολουθεί η Ευρώπη με 85.2%. Αξιοσημείωτο είναι το χαμηλότερο σε σύγκριση ποσοστό των υπόλοιπων γεωγραφικών περιοχών και των ευκαιριών για διασύνδεση που θα προκύψουν στο άμεσο μέλλον σε αυτές τις περιοχές.



Σχήμα 1: Χρήση του διαδικτύου σε παγκόσμιο επίπεδο με γεωγραφικό προσδιορισμό [5].

1.2 Η ανάπτυξη του υπολογιστικού νέφους.

Είναι πλέον δεδομένο ότι υπάρχει η ανάγκη για μια ολοένα αυξανόμενη μετάδοση κάθε είδους πληροφορίας από όπου και εάν βρισκόμαστε. Η ανάγκη ανταλλαγής πολλών δεδομένων μεταξύ των χρηστών όπως για παράδειγμα η αναπαραγωγή video, η επικοινωνία μέσω βίντεο κλήσεων η ανταλλαγή φωτογραφιών, η χρήση εφαρμογών κοινωνικής δικτύωσης από οποιαδήποτε συσκευή, είτε είναι ένας ηλεκτρονικός υπολογιστής είτε ένα έξυπνο κινητό τηλέφωνο, χωρίς να απασχολεί τον χρήστη εάν η συσκευή που χρησιμοποιεί διαθέτει την κατάλληλη υπολογιστική ισχύ ή τον κατάλληλο χώρο αποθήκευσης. Η ευελιξία αυτή που μας προσφέρεται τόσο άμεσα από την εξέλιξη της τεχνολογίας δεν θα ήταν εφικτή χωρίς την ραγδαία αύξηση του "cloud computing". [2]

Υπολογιστικό Νέφος ονομάζεται η κατ' αίτηση διαδικτυακή κεντρική διάθεση υπολογιστικών πόρων (όπως δίκτυο, εξυπηρετητές, εφαρμογές και υπηρεσίες) με υψηλή ευελιξία, ελάχιστη προσπάθεια από τον χρήστη και υψηλή αυτοματοποίηση. Στο Υπολογιστικό Νέφος η αποθήκευση, η επεξεργασία και η χρήση δεδομένων, λογισμικού και υπηρεσιών γίνεται διαδικτυακά, μέσω απομακρυσμένων υπολογιστών σε κεντρικά κέντρα δεδομένων.[3]

1.2.1 Πλεονεκτήματα του υπολογιστικού νέφους.

Οικονομία πόρων. Σε πολλές περιπτώσεις και ειδικότερα στις νεοφυείς επιχειρήσεις δεν είναι πια απαραίτητο μια εταιρεία, όπως π.χ μια νεοφυής επιχείρηση να δαπανήσει ένα μεγάλο ποσό σε εξοπλισμό εξυπηρετητών, αποθηκευτικό χώρο, δικτυακό εξοπλισμό και λογισμικό, το οποίο είναι σε πολλές περιπτώσεις δαπανηρό, όχι μόνο ως προς την απόκτησή του αλλά ως προς την συντήρησή του. Με τις διάφορες αμοιβές αδειών, αναβαθμίσεις και εκπαιδεύσεις που θα χρειαστούν, η εταιρεία μπορεί να έχει μια καλή πρώτη ευκαιρία με σχετικά μικρό κόστος για να μπορέσει τελικά να εισέλθει στην αγορά αφού πολύ εύκολα τέτοιες λύσεις IaaS, PaaS, και SaaS μπορεί να φιλοξενούνται σε έναν πάροχο υπολογιστικού νέφους. [7]

Ως παράδειγμα τέτοιων νεοφυών επιχειρήσεων, οι οποίες με μικρό αρχικό κόστος επένδυσης αλλά βέβαια με μεγάλες και καλές ιδέες μπόρεσαν να αναπτυχθούν και να πρωταγωνιστήσουν στην αγορά είναι, το Instagram, το Tumblr κ.α.

Προσβασιμότητα. Η πρόσβαση, σε κάθε είδους δεδομένα μπορεί να είναι εφικτή από οπουδήποτε στον κόσμο αρκεί η συσκευή μας να έχει σύνδεση στο διαδίκτυο. Για παράδειγμα, η εφαρμογή Google drive μας δίνει την δυνατότητα να έχουμε ανά πάσα στιγμή διαθέσιμα σημαντικά για την προσωπική μας ζωή δεδομένα και μάλιστα να μπορούμε εάν θέλουμε να τα μοιραστούμε με οποιονδήποτε χρήστη.[4]

Ένα ακόμα παράδειγμα της ευελιξίας που μας παρέχει το cloud computing είναι το λεγόμενο business at home κάτι που στις μέρες μας το επιλέγουν πολλές εταιρείες. Σύμφωνα με αυτό ο εργαζόμενος κάποιες μέρες του μήνα έχει την δυνατότητα να εργαστεί από το σπίτι του ή από οποιονδήποτε χώρο και αν βρίσκεται, αφού το γραφείο του δεν είναι τίποτε άλλο παρά ο ηλεκτρονικός του υπολογιστής, αρκεί βέβαια να υπάρχει πρόσβαση στο διαδίκτυο.

1.2.2 Μειονεκτήματα του cloud computing.

Ασφάλεια δεδομένων. Ενώ το να είναι τα δεδομένα μας αποθηκευμένα σε έναν πάροχο cloud μας παρέχει πολλά πλεονεκτήματα λόγω ευελιξίας και προσβασιμότητας όπως αναφέραμε παραπάνω, δεν παύει όμως να εγείρει ερωτήματα κυρίως σε θέματα ασφάλειας, δηλαδή το κατά πόσο είναι ασφαλή τα δεδομένα μας και δεν μπορούν να κλαπούν από αυτόν που τα φιλοξενεί ή από άλλους, ακόμα και το κατά πόσο αυτός που τα φιλοξενεί δεν μπορεί να τα εκμεταλλευτεί και να τα διαθέσει ως πληροφορίες σε τρίτους.[4]

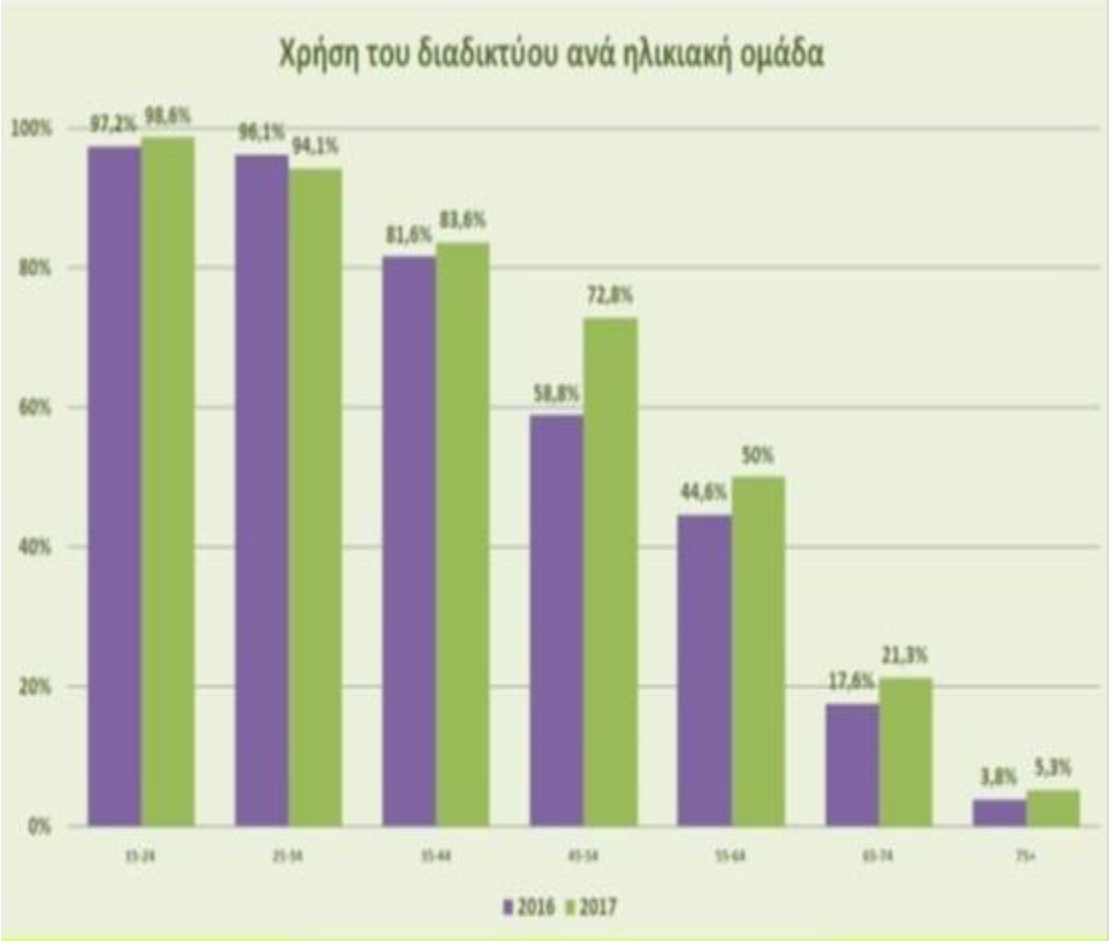
Ένα παράδειγμα κλοπής και διάδοσης δεδομένων από μια εφαρμογή cloud συνέβη τον Αύγουστο του 2014 από την πολύ γνωστή εφαρμογή icloud όπου περίπου 500 προσωπικές φωτογραφίες διασήμων κυρίως γυναικών διέρρευσαν σε ιστοσελίδες και μέσα κοινωνικής δικτύωσης. Εκεί κυβερνοεισβολείς εκμεταλλεύτηκαν τα [κενά] ασφαλείας που βρήκαν στο API του icloud και δοκίμαζαν συνεχώς κωδικούς πρόσβασης στους λογαριασμούς των θυμάτων τους, χωρίς η σελίδα να τους αποκλείει την σύνδεση.

Για τον λόγο αυτό χρησιμοποίησαν τεχνικές "ωμής βίας" και με αυτό τον τρόπο μπόρεσαν ανενόχλητοι να ανακαλύψουν τους κωδικούς πρόσβασης των χρηστών.

Πολυπλοκότητα τέτοιων δομών. Ίσως ένα ακόμα μειονέκτημα του cloud computing, ειδικότερα στην χώρα μας, έχει να κάνει με την δυσκολία ατόμων όχι και τόσο εξοικειωμένων με την τεχνολογία και την πληροφορική και κυρίως μεγαλύτερης

ηλικίας, που θα πρέπει για να έχουν πρόσβαση σε τέτοιες εφαρμογές οι οποίες όπως αναφέραμε προηγουμένως διευκολύνουν την καθημερινότητά μας και καθιστούν ολοένα και πιο αναγκαία την χρήση τους σε αυτή. Τα άτομα αυτά να για να μπορέσουν να εγκλιματιστούν σε τέτοιες δομές πρέπει να παρακολουθήσουν κάποιο σεμινάριο εκπαιδεύσεων.[1]

Στο παρακάτω διάγραμμα φαίνεται το ποσοστό χρήσης του διαδικτύου ανά ηλικιακή ομάδα στην Ελλάδα. Εδώ παρατηρούμε ότι σε ηλικίες 15-54 το ποσοστό χρήσης του διαδικτύου είναι αρκετά υψηλό αλλά σε ηλικίες χρηστών 55 ετών και άνω, τα ποσοστά αυτά μειώνονται εντυπωσιακά. Άρα, εδώ προκύπτει το ψηφιακό χάσμα για το οποίο μιλήσαμε παραπάνω.



Σχήμα 2: Χρήση του διαδικτύου μεταξύ ηλικιακών ομάδων στην Ελλάδα. [1]

1.3 Η ανάγκη για εφαρμογή του νέου πρωτοκόλλου IPv6.

Η ιλιγγιώδης εξέλιξη της τεχνολογίας, όπως αναφέραμε και παραπάνω, ειδικότερα στον τομέα τον δικτύων υπολογιστών, σε συνάρτηση με την ολοένα αυξανόμενη

εξέλιξη των δομών του cloud computing συνδυαστικά με τη νέα τάση που βλέπουμε να κυριαρχεί γύρω μας για την δικτύωση των πραγμάτων (internet of thinks), καθιστά κυρίαρχο το πρωτόκολλο επικοινωνίας στο οποίο είναι βασισμένη η λειτουργία του διαδικτύου, δηλαδή το πρωτόκολλο IPv4. Στο πρωτόκολλο αυτό, όμως, φανερώνεται μια αδυναμία να ανταποκριθεί στα σύγχρονα δεδομένα την εποχής, τόσο στις τωρινές οσο σίγουρα και στις μελλοντικές ανάγκες για τον ολοένα αυξανόμενο αριθμό των χρηστών και των δικτύων που αποτελούν σήμερα το σύνολο του διαδίκτυου.

Στην συνέχεια παρατίθενται οι σημαντικότερες απαιτήσεις που κατέστησαν επιτακτική την ανάγκη για το νέο πρωτόκολλο δικτύου, το IPv6.

Κινητικότητα (mobility). Λόγω της ραγδαίας εξάπλωσης των ασυρμάτων δικτύων οι δικτυακοί χρήστες οι όποιοι χρησιμοποιούν το πρωτόκολλο IPv4 δεν έχουν την δυνατότητα να διατηρήσουν την διεύθυνσή τους στην μετάβασή τους από ένα υπό δίκτυο σε άλλο.

Ποιότητα υπηρεσιών (QoS). Όπως αναφέραμε και παραπάνω, ο αριθμός των εφαρμογών που αναπτύσσονται για να καλύψουν τις διάφορες ανάγκες μας αυξάνεται συνεχώς, για τον λόγο αυτό η Ποιότητα υπηρεσιών είναι μια έννοια η οποία έχει πρωταγωνιστικό ρόλο στην χρήση των διαφόρων εφαρμογών. Για παράδειγμα, μια πολυμεσική και πραγματικού χρόνου εφαρμογή έχει διαφορετικές απαιτήσεις από μια άλλη που η ταχύτητα μετάδοσης δεδομένων δεν παίζει τόσο καθοριστικό ρόλο για τον χρήστη της.

Αν και στην επικεφαλίδα του πρωτόκολλο IPv4, υπάρχει το πεδίο DSCP (Differentiated Services) αυτό πρακτικά δεν εφαρμόζεται και ουσιαστικά η όλη διαδικασία ελέγχου της ποιότητας υπηρεσίας μεταφέρεται σε παραπάνω επίπεδο δηλαδή στον διαχωρισμό των UDP και TCP πακέτων με αποτέλεσμα μεγαλύτερη σπατάλη σε ισχύ στους δρομολογητές.

Εξάντληση των διευθύνσεων IPv4. Ο ολοένα αυξανόμενος αριθμός χρηστών και η μεγάλη επέκταση του διαδικτύου σε παγκόσμιο επίπεδο οδήγησαν στην εξάντληση των διευθύνσεων IPv4. Για τον λόγο αυτό παρουσιάστηκαν και υλοποιήθηκαν διάφορες λύσεις, αρχικά η αταξική δρομολόγηση η οποία έδωσε παραπάνω χρόνια στο IPv4 και αργότερα ήρθε ο πολύ γνωστός μηχανισμός NAT (Network Address

Traslation) παρέχοντας δίκτυα ιδιωτικών διευθύνσεων κάτω όμως από παγκόσμιες διευθύνσεις.

Μειονεκτήματα της παραπάνω υλοποίησης είναι η μείωση της απόδοσης καθώς και προβλήματα στην ασφάλεια της επικοινωνίας από άκρο σε άκρο.

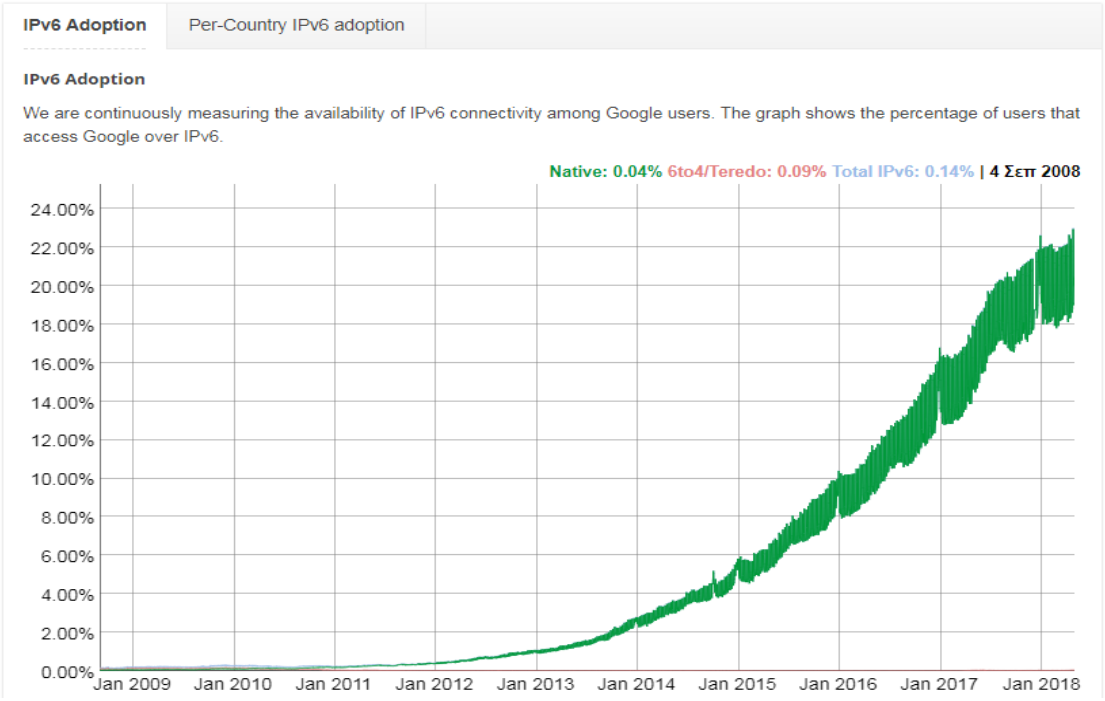
Ασφάλεια. Οι απαιτήσεις για ασφάλεια στο επίπεδο IP είναι μεγάλες. Εάν και σήμερα χρησιμοποιούμε τον μηχανισμό IPsec για εφαρμογές εταιριών και τραπεζών θα ήταν σίγουρα προτιμότερο ο μηχανισμός ασφαλείας να βρισκόταν στο επίπεδο IP ενσωματωμένο δηλαδή στην επικεφαλίδα.

Για όλους τους παραπάνω λόγους το 1994 η Internet Engineering Task Force (IETF) ξεκινώντας με την έκδοση RFC 1983 ανακοίνωσε το νέο πρωτόκολλο δικτύου, το IPv6, το οποίο σε πολύ γενικές γραμμές προσφέρει μια άλλη δυναμική στις δικτυακές επικοινωνίες καθώς εκμεταλλεύεται και υποστηρίζει τις δυνατότητες των νέων εφαρμογών.

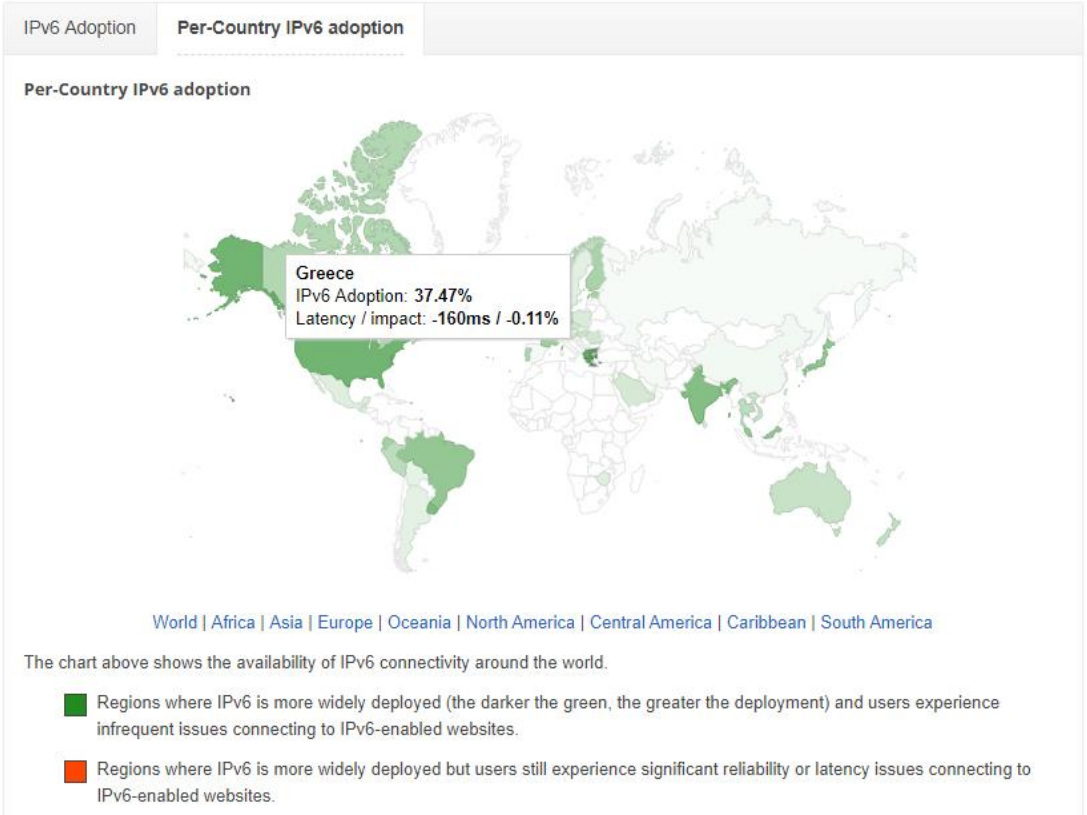
Η μετάβαση στο νέο πρωτόκολλο αποδείχτηκε κάθε άλλο παρά εύκολη, κάτι που συνεχίζει και στις μέρες μας, για τον λόγο αυτό, δημιουργήθηκαν μηχανισμοί σταδιακής μετάβασης όπως οι μηχανισμοί tunneling. Σε παρακάτω κεφάλαιο θα γίνει εκτενέστερη αναφορά στο παραπάνω πρωτόκολλο δικτύου, στην ανάγκη για μετάβαση στο IPv6 και στους μηχανισμούς μετάβασης ανάμεσα στα δύο πρωτόκολλα IPv4-IPv6. [4]

Στο παρακάτω διάγραμμα (Σχήμα 3) βλέπουμε το ποσοστό των χρηστών παγκοσμίως από το 2009, που χρησιμοποιούν το πρωτόκολλο IPv6 για την πρόσβασή τους στο διαδίκτυο, μέσω τις εταιρείας Google. Παρατηρείται η ραγδαία αύξηση ειδικότερα τα τελευταία 3 χρόνια από το 2015 δηλαδή μέχρι σήμερα όπου από το 6% έχουμε φτάσει στο 22%.

Στο επόμενο διάγραμμα (Σχήμα 4) βλέπουμε έναν ακόμα πίνακα που διατίθεται από την Google και στο οποίο βλέπουμε το ποσοστό χρήσης του πρωτοκόλλου IPv6 ανά χώρα. Παρατηρείται ότι η χώρα μας βρίσκεται στις πρώτες που υιοθέτησαν το νέο πρωτόκολλο με ποσοστό 37.47 %, πιο πάνω δηλαδή και από τις Ηνωμένες Πολιτείες Αμερικής με ποσοστό 34% και σε ίδιο ποσοστό με την επίσης χώρα της Ευρωπαϊκής ένωσης Γερμανία με ποσοστό 38%.



Σχήμα 3: Υιοθέτηση του πρωτοκόλλου IPv6 από το 2008 μέχρι σήμερα. [6]



Σχήμα 4: Υιοθέτηση του πρωτοκόλλου IPv6 από το 2008 μέχρι σήμερα ανά χώρα. [6]

2. Το νέο πρωτόκολλο διαδικτύου IPv6.

2.1 Η δομή και η λειτουργία του νέου πρωτόκολλου IPv6.

Σε αυτή την ενότητα θα αναλυθεί η μορφή που έχει ένα πακέτο πληροφορίας του πρωτόκολλου IPv6, η λειτουργία των διαφόρων στοιχείων της επικεφαλίδας και τέλος θα παρατεθούν τα πλεονεκτήματα που μας προσφέρει το νέο αυτό πρωτόκολλο.

Ένα πακέτο πληροφορίας του IPv6 χωρίζεται σε δύο μέρη: στην επικεφαλίδα και τα δεδομένα που μεταφέρει το πακέτο. Η επικεφαλίδα με την σειρά της αποτελείται από ένα σταθερό τμήμα, το οποίο μας δίνει την ελάχιστη λειτουργικότητα που είναι απαραίτητη για την μεταφορά δεδομένων και από τις προαιρετικές επεκτάσεις που μας παρέχουν ειδικές λειτουργίες.

Στο σχήμα 5 βλέπουμε το σταθερό τμήμα της επικεφαλίδας το οποίο και καταλαμβάνει τα πρώτα 320 bits του συνολικού πακέτου.

<table>
<tr><th>Octet</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td colspan="4">Version</td><td colspan="8">Traffic Class</td><td colspan="20">Flow Label</td></tr>
<tr><td>32</td><td colspan="16">Payload Length</td><td colspan="8">Next Header</td><td colspan="8">Hop Limit</td></tr>
<tr><td>64</td><td colspan="32" rowspan="4">Source Address</td></tr>
<tr><td>96</td></tr>
<tr><td>128</td></tr>
<tr><td>160</td></tr>
<tr><td>192</td><td colspan="32" rowspan="4">Destination Address</td></tr>
<tr><td>224</td></tr>
<tr><td>256</td></tr>
<tr><td>288</td></tr>
</table>

Σχήμα 5: Η επικεφαλίδα IPv6 - en.wikipedia.org/wiki/IPv6_packet

Στην συνέχεια θα αναλυθούν τα διάφορα πεδία της επικεφαλίδας καθώς και η λειτουργία τους ξεκινώντας από το τέλος. [8]

Destination address (128 bit): Σε αυτό το πεδίο φαίνεται η διεύθυνση του κόμβου προορισμού του πακέτου.

Source address (128 bit): Σε αυτό το πεδίο φαίνεται η διεύθυνση του αρχικού κόμβου του πακέτου.

Hop Limit (8 bits): Η λειτουργία αυτού του πεδίου είναι η αναγνώριση πακέτων που βρίσκονται ενδεχομένως σε ατέρμονα βρόχο. Κάθε φορά που το πακέτο μεταφέρεται από τον ένα κόμβο σε άλλον το πεδίο μειώνει τον απαριθμητή του κατά μία μονάδα και έτσι έχοντας ως όριο τις 255 προωθήσεις διασφαλίζεται η σωστή λειτουργία του δικτύου. Με αυτόν τον τρόπο διασφαλίζουμε ότι ένα πακέτο δεν θα κυκλοφορεί συνεχώς στο δίκτυο χωρίς ποτέ να βρει τον προορισμό του.

Next header (8 bits): Σε αυτό το πεδίο καθορίζεται ο τύπος της επικεφαλίδας που ακολουθείται στο παραπάνω επίπεδο. Δηλαδή σε αυτό το πεδίο αναγνωρίζεται το είδος της κεφαλίδας επέκτασης εάν βέβαια υπάρχει ή το είδος πακέτου που ακολουθεί σε παραπάνω επίπεδο εάν δηλαδή είναι TCP ή UDP.

Payload length (16 bits): Το πεδίο αυτό περιέχει το μέγεθος του πεδίου data octets/bits που ακολουθεί μετά την επικεφαλίδα.

Flow label (20 bits): Το πεδίο αυτό εισάγει την έννοια της ροής πακέτων, δηλαδή πακέτα από την ίδια προέλευση προς τον ίδιο προορισμό. Για παράδειγμα, μπορεί να είναι πακέτα για εφαρμογές video και γενικότερα για εφαρμογές στις οποίες θέλουμε η καθυστέρηση να μην είναι παρατηρήσιμη από τον χρήστη.

Αυτό επιτυγχάνεται διότι, στην μετάβαση των πακέτων από τους διάφορους δρομολογητές, αυτοί δεν χρειάζεται να "δουν" σε παραπάνω επίπεδο ώστε να καταλάβουν το είδος του πακέτου.

Με αυτόν τον τρόπο οι δρομολογητές δεν σπαταλούν υπολογιστική ισχύ με αποτέλεσμα να μην προσθέτουν επιπλέον χρόνο στην μεταφορά ενός πακέτου.

Traffic class (8 bits): Το πεδίο αυτό δουλεύει συμπληρωματικά με το προηγούμενο (Flow label) και αυτό διότι μπορεί και αναθέτει διαφορετικές προτεραιότητες ανά

πακέτο. ‘Ετσι οι δρομολογητές μπορούν να ξεχωρίζουν ποια πακέτα ανήκουν στην ίδια κλάση κίνησης και να ξεχωρίζουν αυτά με διαφορετικές προτεραιότητες.

Version (4 bit): Αυτό το πεδίο των 4 bits περιέχει τον αριθμό 6. Το πεδίο αυτό δηλώνει την έκδοση του IPv6. Το πεδίο αυτό έχει το ίδιο μέγεθος με το πεδίο της έκδοσης IPv4 που περιέχει τον αριθμό 4.

Παραπάνω παρουσιάστηκε η λειτουργία των διάφορων πεδίων της σταθερής επικεφαλίδας του πρωτοκόλλου IPv6, τώρα θα δούμε τις προαιρετικές επεκτάσεις του που μας παρέχουν ειδικές λειτουργιές και αναλύσουμε τις κυριότερες. [8]

Στο σχήμα 6 βλέπουμε επιγραμματικά τις προαιρετικές επεκτάσεις και την λειτουργία τους.

Extension Header	Type	Description
Hop-by-Hop Options	0	Options that need to be examined by all devices on the path.
Destination Options (before routing header)	60	Options that need to be examined only by the destination of the packet.
Routing	43	Methods to specify the route for a datagram (used with Mobile IPv6).
Fragment	44	Contains parameters for fragmentation of datagrams.
Authentication Header (AH)	51	Contains information used to verify the authenticity of most parts of the packet.
Encapsulating Security Payload (ESP)	50	Carries encrypted data for secure communication.
Destination Options (before upper-layer header)	60	Options that need to be examined only by the destination of the packet.
Mobility (currently without upper-layer header)	135	Parameters used with Mobile IPv6.
Host Identity Protocol	139	Used for Host Identity Protocol version 2 (HIPv2).[11]
Shim6 Protocol	140	Used for Shim6.[12]
Reserved	253	Used for experimentation and testing.[13][4]
Reserved	254	Used for experimentation and testing.[13][4]

Σχήμα 6: Επικεφαλίδες επεκτάσεων IPv6 - en.wikipedia.org/wiki/IPv6_packet.

Hop by Hop options: Είναι μια επικεφαλίδα που διαβάζεται από κάθε δρομολογητή, ακολουθεί την βασική επικεφαλίδα εάν στο πεδίο Next header που είδαμε παραπάνω είναι η hop by hop τότε η πληροφορία που φέρει υπολογίζεται σε κάθε κόμβο κατά τη διαδρομή διάδοσης του πακέτου.

Destination Options: Είναι μια επικεφαλίδα που μεταφέρει προαιρετικές πληροφορίες που υπολογίζονται μόνο από τους κόμβους προορισμού.

Routing Header: Είναι μια επικεφαλίδα που χρησιμοποιείται όταν μια πηγή επιθυμεί να περάσει το πακέτο από έναν η περισσότερους ενδιάμεσους κόμβους και αναγνωρίζεται από το πεδίο Next header.

Fragment: Είναι μια επικεφαλίδα που περιέχει το αναγνωριστικό του πακέτου, τον αριθμό του θραύσματος κατά την μεταφορά του σε έναν προορισμό. Ένα πακέτο δεν διασπάται κατά μήκος της διαδρομής, παρά μόνο από την αρχική πηγή.

Authentication Header: Είναι μια επικεφαλίδα που πιστοποιεί την αυθεντικότητα της ταυτότητας των διαφόρων πακέτων.

Encapsulation Security Payload: Είναι μια επικεφαλίδα που έχει ως στόχο να μεταφερθούν τα κρυπτογραφημένα δεδομένα με ασφάλεια κατά την διαδρομή του πακέτου προς τον παραλήπτη.

Mobility Header: Είναι μια επικεφαλίδα που χρησιμοποιείται από χρήστες κινητών συσκευών**.**

2.1.1 Πλεονεκτήματα του νέου πρωτοκόλλου.

Παραπάνω έγινε αναφορά στην δομή του IPv6 και στα πεδία των επικεφαλίδων, τώρα θα αναφερθούν επιγραμματικά τα πλεονεκτήματα που παρέχονται από το νέο αυτό πρωτόκολλο.

- Δίνεται οριστικά λύση στο πρόβλημα στον αριθμό διευθύνσεων IP. Το μέγεθος μιας διεύθυνσης IP στο νέο πρωτόκολλο αποτελείται από 128 bit τέσσερις φόρες μεγαλύτερο από αυτές του πρωτοκόλλου IPv4. Θεωρητικά μπορούμε να έχουμε 2^{128} μοναδικές διευθύνσεις IP, έτσι συμπεραίνεται ότι ο κάθε χρήστης στον κόσμο μπορεί να έχει την δική του μοναδική διεύθυνση IP για κάθε συσκευή που χρησιμοποιεί και για κάθε είδους νέα υπηρεσία που μπορεί να του προσφέρει ο παροχός του. Ακόμα η χρήση της τεχνικής NAT που χρησιμοποιείται στο πρωτόκολλο IPv4 πλέον δεν θεωρείται αναγκαία γιατί δεν χρειάζεται. [8]

- Έχουμε καλύτερη ποιότητα υπηρεσίας (QoS). Όπως τονίστηκε και παραπάνω, τα πεδία traffic class και flow label της σταθερής επικεφαλίδας μας δίνουν μια νέα δυνατότητα με την οποία έχουμε ένα πλεονέκτημα στην χρήση υπηρεσιών κυρίως πραγματικής ροής μεταδόσεων όπως και σε εφαρμογές audio και ροής βίντεο.

- Το νέο πρωτόκολλο είναι σχεδιασμένο με βάση την ασφαλή μετάδοση της πληροφορίας καθώς το πρωτόκολλο ασφαλείας IPsec είναι ενσωματωμένο μέσα στο νέο πρωτόκολλο. [9]

- Το IPv6 μας παρέχει πολύ βελτιωμένη κινητικότητα καθώς οι χρήστες έχουν την δυνατότητα να διατηρούν την σύνδεσή τους σε όλη την διαδρομή τους από το ένα δίκτυο στο άλλο. Ο χρήστης στο νέο πρωτόκολλο έχει τη δυνατότητα να διατηρεί τη διεύθυνση του τοπικού του δικτύου και παράλληλα να είναι ενημερωμένος για τις διευθύνσεις των δικτύων που εισέρχεται κάθε φορά. Στο νέο MIPv6 έχουμε την άμεση δρομολόγηση όπου η αρχική πύλη είναι συνεχώς ενημερωμένη για τις διευθύνσεις του χρήστη. [10]

2.2 Διαφορές του πρωτοκόλλου IPv4 σε σχέση με το IPv6.

Παρακάτω παρουσιάζονται οι βασικές διαφορές των δύο πρωτοκόλλων. [11]

Περιγραφή	**IPv4**	**IPv6**
Διευθύνσεις	Οι διευθύνσεις στο IPv4 είναι 32bits, αποτελούνται από το μέρος του δικτύου και το μέρος των host. Η μορφή μιας διεύθυνσης είναι για παράδειγμα ccc.ccc.ccc.ccc, όπου ccc από 0 έως 255.	Οι διευθύνσεις στο IPv6 είναι 128 bits, 64 bits για το network κομμάτι και 64bits για το host. Ο αριθμός των μοναδικών διευθύνσεων φτάνει τις 10^{28} σε αριθμό και έχουν την παρακάτω μορφή. cccc:cccc:cccc:cccc:cccc:cccc:cccc:cccc όπου c είναι ένας δεκαεξαδικός αριθμός και αποτελείται από 4bit.
Quality of service (QoS)	Δεν υπάρχει η δυνατότητα για QoS στην επικεφαλίδα	Το νέο πρωτόκολλο έχει στην επικεφαλίδα το πεδίο flow label που μας επιτρέπει την υποστηρίξει QoS.

	του πρωτοκόλλου IPv4	
Fragments	Στο IPv4 όταν ένα πακέτο είναι πολύ μεγάλο μπορεί να διασπαστεί σε μικρότερα από τον αποστολέα ή τον δρομολογητή είτε και από τον host.	Στο IPv6 το πακέτο μπορεί να διασπαστεί μονάχα από τον αποστολέα και η επανασυναρμολόγηση του γίνεται στον κόμβο με την βοήθεια της επικεφαλίδας επέκτασης κατακερματισμού.
DHCP	Στο IPv4 η λειτουργία DynamicHost Configuration είναι δυνατή μόνο σε τοπικά δίκτυα από τους δρομολογητές	Στο IPv6 η λειτουργία αυτή δεν υπάρχει μόνο σε τοπικό επίπεδο αλλά επεκτείνεται και στους μετέπειτα δρομολογητές κατά την πορεία ενός πακέτου.
IP header	Ο IP header στο IPv4 είναι μεταβλητού μήκους από 20-60 bytes.	Στο IPv6 έιναι σταθερού μήκους 40 bytes. Γενικότερα ο ip header είναι πιο απλός από αυτόν του IPv4.
MTU	Στο IPv4 έχουμε μέγιστο τα 576 που μπορούν να μεταφερθούν από ένα κανάλι μεταφοράς.	Στο IPv6 ως μέγιστο έχουμε τα 1280 bytes.
NAT	Το πρόβλημα στον αριθμό των μοναδικών διευθύνσεων στο πρωτόκολλο IPv4 λύνεται με την τεχνική NAT(Network address translation).	Στο IPv6 δεν έχουμε την ανάγκη τέτοιας τεχνικής λόγω του πολύ μεγάλου αριθμού διευθύνσεων που υποστηρίζει το νέο πρωτόκολλο.

2.3 Μηχανισμοί μετάβασης από το Ipv4 στο Ipv6.

Όπως αναφέρθηκε και παραπάνω, η μετάβαση από το πρωτόκολλο IPv4 στο νέο πρωτόκολλο διαδικτύου μόνο εύκολη δεν είναι εξαιτίας του πολύ μεγάλου μεγέθους του διαδικτύου το οποίο βέβαια ολοένα και μεγαλώνει. Πολλοί οργανισμοί και εταιρίες στηρίζουν καθαρά την λειτουργία τους σε εφαρμογές που κυρίαρχο ρόλο παίζει το διαδίκτυο, οπότε είναι φυσικό να μην έχουν την δυνατότητα από την μία μέρα στην άλλη να αναβαθμίσουν άμεσα τα συστήματά τους. Αυτό συμβαίνει βέβαια για να μην αναστείλουν τις διάφορες λειτουργίες τους αλλά επιπλέον διότι τα

συστήματα που έχουν επενδύσει μέχρι σήμερα μπορεί να μην είναι συμβατά με το νέο πρωτόκολλο. Αρα είναι σαφές ότι η μετάβαση είναι μια διαδικασία χρονοβόρα άλλα και με κόστος για τις επιχειρήσεις και τους οργανισμούς, επομένως, μία σταδιακή και όχι απότομη μετάβαση φαντάζει μια πιο πραγματική λύση στο πρόβλημα αυτό. [4]

Η όλη αυτή δυσκολία είχε βέβαια προβλεφθεί από την IETF στον σχεδιασμό του νέου πρωτοκόλλου IPv6 και για τον λόγο αυτό προτάθηκαν μηχανισμοί που έχουν ως κύριο στόχο να προσφέρουν τα εξής χαρακτηριστικά: [24]

- **Δυνατότητα σταδιακής μετάβασης**
- **Απλότητα διευθυνσιοδότησης**
- **Ελάχιστες απαιτήσεις αναβάθμισης**
- **Καμία προετοιμασία εγκατάστασης για την αναβάθμιση από IPv4 σε IPv6**

Για να επιτευχθούν τα παραπάνω χαρακτηριστικά ενσωματώθηκε στο νέο πρωτόκολλο το Simple Internet Transition (SIT), το οποίο αποτελείται από κανόνες και πρωτόκολλα για να διευκολύνει την μετάβαση ανάμεσα στα δυο αυτά πρωτόκολλα. [25]

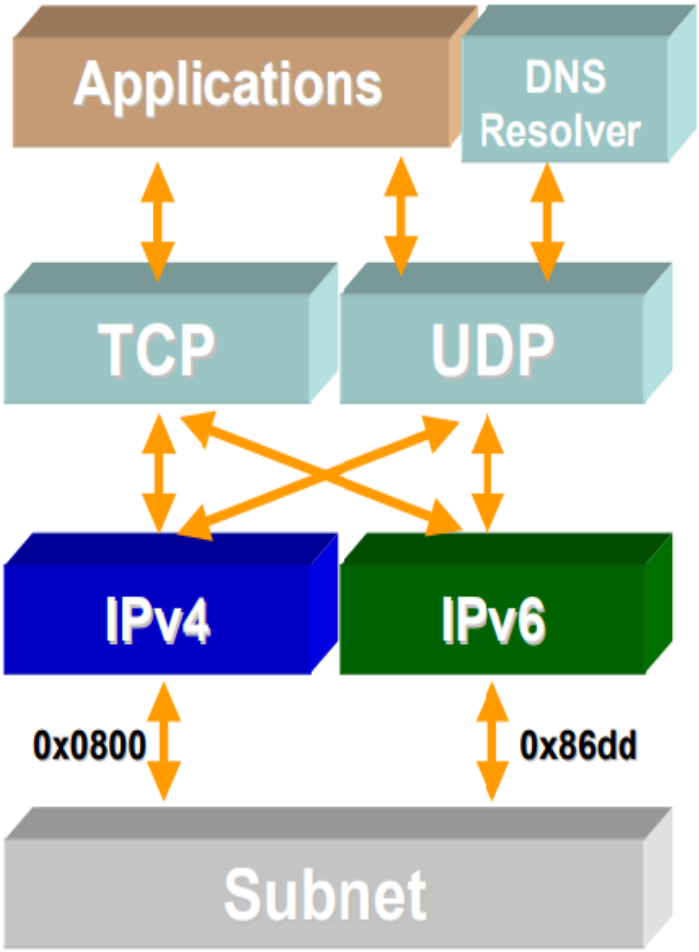
- Μία διεύθυνση IPv6 μπορεί να προκύψει από μία IPv4 διεύθυνση.
- Να μπορούν τα συστήματα να λειτουργούν με διπλή στοίβα πρωτοκόλλων, το κάθε μηχάνημα να έχει την δυνατότητα να επιλέγει ποία από τις δύο στοίβες θα χρησιμοποιήσει για την επικοινωνία.
- Να έχουμε έναν μηχανισμό για να ενθυλακώσουμε ένα πακέτο IPv6 μέσα σε πακέτα IPv4(tunneling).
- Να υπάρχει η δυνατότητα ένα πακέτο IPv6 να μετατραπεί σε IPv4 και βέβαια να ισχύει και το αντίστροφο.

Με βάση τα παραπάνω, προέκυψαν μηχανισμοί μετάβασης οι οποίοι κατηγοριοποιούνται ως εξής: μηχανισμοί διπλής στοίβας και μηχανισμοί tunneling στους οποίους και θα γίνει αναφορά επιγραμματικά παρακάτω. [12]

2.3.1 Μηχανισμοί διπλής στοίβας.

Ο μηχανισμός αυτός στηρίχτηκε στην ιδέα ότι οι διάφοροι κόμβοι ενός δικτύου μπορούν και υποστηρίζουν και τα δύο πρωτοκόλλα διαδικτύου ταυτόχρονα, έτσι για να μπορέσει να επιτευχθεί μια επικοινωνία ο κάθε κόμβος θα πρέπει να έχει την δυνατότητα να εφαρμόζει και τις δύο στοίβες των διαφορετικών αυτών πρωτοκόλλων. Η επιλογή για το ποια στοίβα θα χρησιμοποιηθεί γίνεται κατά κύριο λόγο με βάση το αποτελέσματα από την αναζήτηση DNS. Επιπλέον, είναι απαραίτητη η αναβάθμιση των διάφορων εφαρμογών και συστημάτων ώστε να έχουν την δυνατότητα να χρησιμοποιούν την στοίβα για το πρωτόκολλο IPv6.

Στο σχήμα 7 βλέπουμε σχηματικά την διαδικασία μετάβασης διπλής στοίβας.

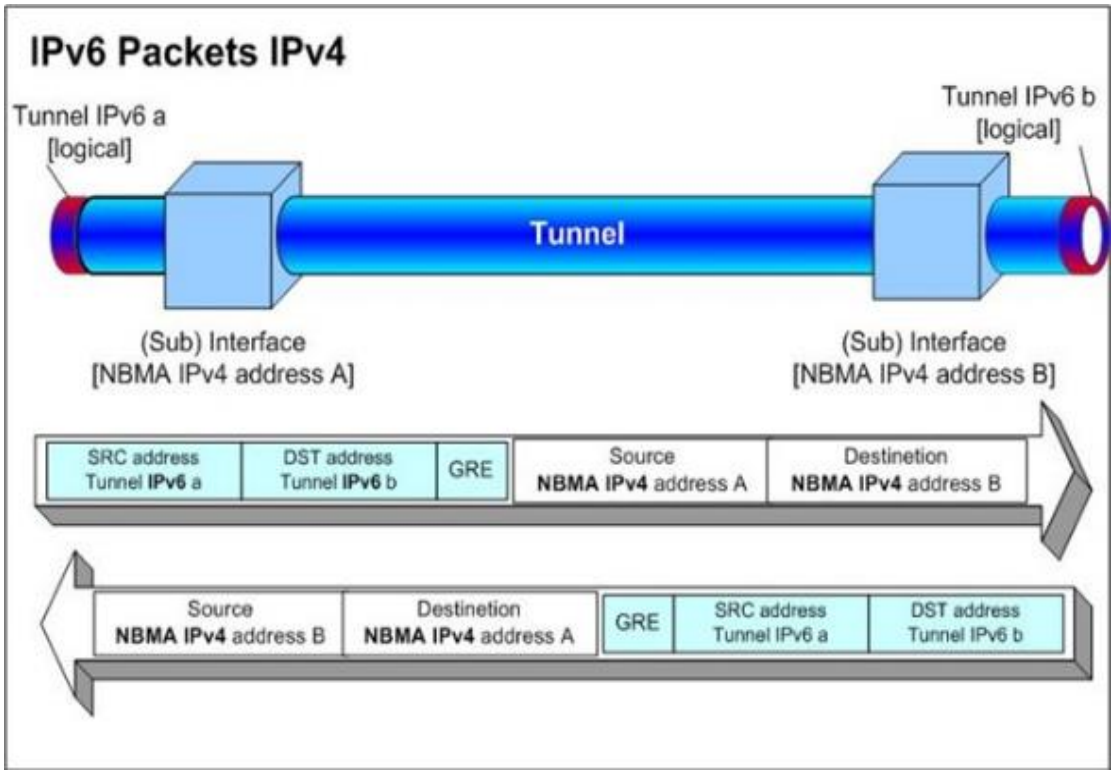


Σχήμα 7: Μηχανισμός Dual – Stack. [12]

2.3.2 Μηχανισμοί tunneling.

Στο μεταβατικό στάδιο κατά την διεύρυνση του πρωτοκόλλου IPv6 στο οποίο και βρισκόμαστε είναι χρήσιμο η υποδομή του πρωτοκόλλου IPv4 να παραμείνει λειτουργική ως έχει. Οι μηχανισμοί tunneling που θα αναφερθούν επιγραμματικά παρακάτω, έχουν ως στόχο αυτό ακριβώς δηλαδή το να χρησιμοποιηθεί η υπάρχουσα υποδομή για την μεταφορά πακέτων IPv6. Η τεχνική tunneling χρησιμοποιείται ευρέως σήμερα και στηρίζεται στην αρχή της ενθυλάκωσης ενός πρωτοκόλλου σε πακέτα άλλου πρωτοκόλλου, δηλαδή IPv6 hosts και routers έχουν την ικανότητα να μεταφέρουν IPv6 πακέτα τα οποία ενθυλακώνονται σε πακέτα IPv4 και μεταφέρονται πάνω από το υπάρχον δίκτυο. Με αυτό τον τρόπο καταφέρνουμε να ανταλλάσσονται πακέτα IPv6 ακόμα και από κόμβους, στους οποίους υποστηρίζεται μόνο το παλιό πρωτόκολλο δικτύου το IPv4. Ως προϋπόθεση υπάρχει ότι οι δύο κόμβοι στα άκρα του tunnel θα πρέπει να υποστηρίζουν την διπλή στοίβα ώστε να καταφέρουν να κάνουν την ενθυλάκωση και από ενθυλάκωση των πακέτων από IPv6 σε IPv4 και αντίστροφα. [13]

Στο παρακάτω σχήμα φαίνεται η διάδοση IPv6 πακέτων κάτω από το πρωτόκολλο IPv4 μεταξύ δύο κόμβων.



Σχήμα 8: Διάδοση IPv6 πακέτων κάτω από το IPv4 δίκτυο. [13]

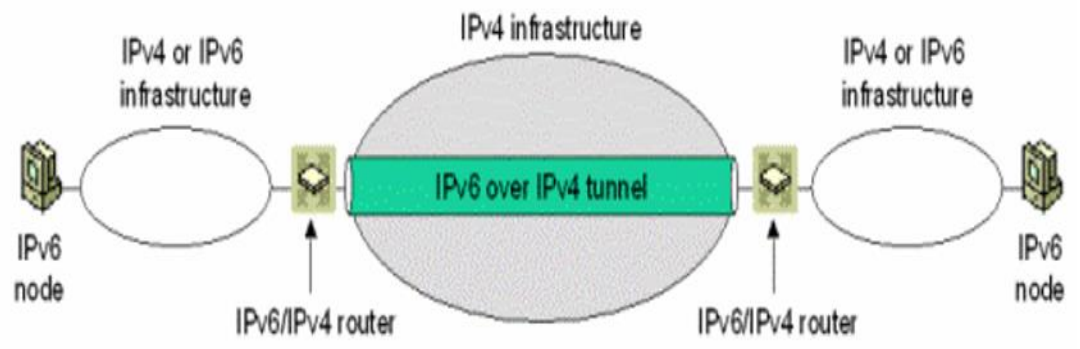
Παρακάτω θα αναφερθούν επιγραμματικά τα είδη μηχανισμών tunneling. Οι μηχανισμοί αυτοί κατηγοριοποιούνται με βάση τον τρόπο τον οποίο χρησιμοποιεί ο κόμβος εισόδου για να καθορίσει την διεύθυνση του κόμβου εξόδου και χωρίζονται σε μηχανισμούς που χρησιμοποιούν ρυθμισμένο tunneling (configured) και στατικό που χρησιμοποιούν αυτόματο tunneling (automatic).

Στον μηχανισμό configured tunneling η διεύθυνση IPv4 του άκρου εισόδου του tunnel εξαρτάται από τις πληροφορίες διαμόρφωσης που έχουν οριστεί από την αρχή στον κόμβο αυτόν στον οποίον γίνεται και η ενθυλάκωση των διαφόρων πακέτων. Για κάθε tunnel πρέπει να υπάρχει αποθηκευμένη η διεύθυνση του άλλου άκρου καθώς όταν έχουμε μεταφορά ενός πακέτου η διεύθυνση του άκρου εξόδου τίθεται ως η διεύθυνση προορισμού στην επικεφαλίδα IPv4 που ενθυλακώνεται στο πακέτο IPv6.

Παρακάτω θα δούμε τις περιπτώσεις επικοινωνίας μεταξύ δύο άκρων. [13]

- Router-to-Router

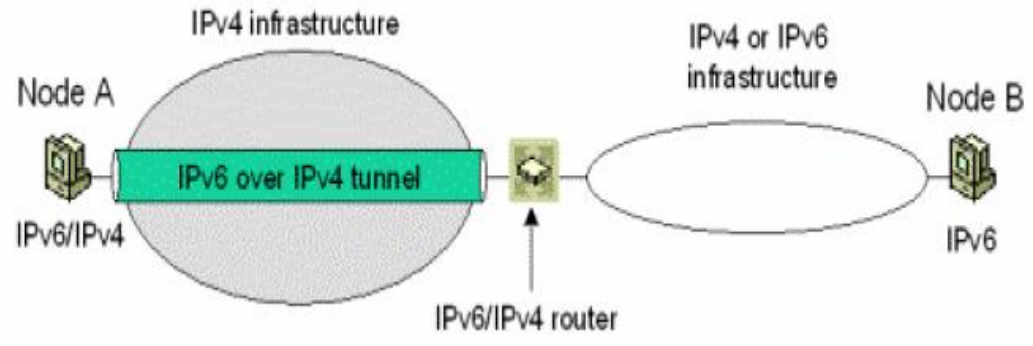
Στην περίπτωση αυτή οι δρομολογητές IPv6 / IPv4 που είναι διασυνδεδεμένοι με μία υποδομή IPv4 μπορούν να μεταδώσουν πακέτα IPv6 μεταξύ τους με την βοήθεια του tunnel που έχουν δημιουργήσει από άκρο σε άκρο.



Σχήμα 9: Επικοινωνία μεταξύ δύο άκρων (Router-to-Router)

- Host-to-Router

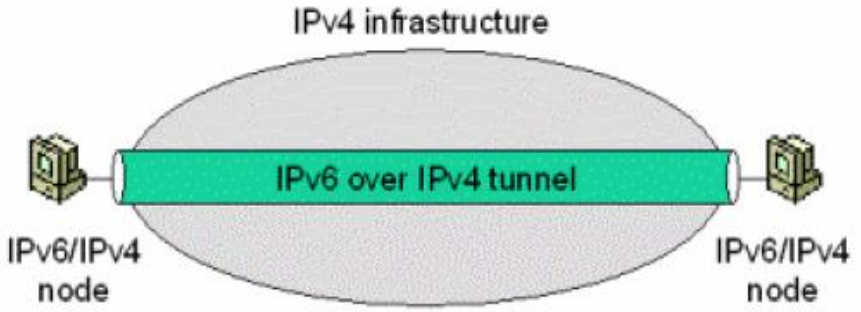
Στην περίπτωση αυτή οι hosts IPv6 / IPv4 μπορούν να μεταφέρουν πακέτα IPv6 σε ένα ενδιάμεσο δρομολογητή IPv6 / IPv4 ο οποίος είναι προσβάσιμος μέσω μίας IPv4 υποδομής.



Σχήμα 10: Επικοινωνία μεταξύ δύο άκρων (Host-to-Router)

- Host-to-Host

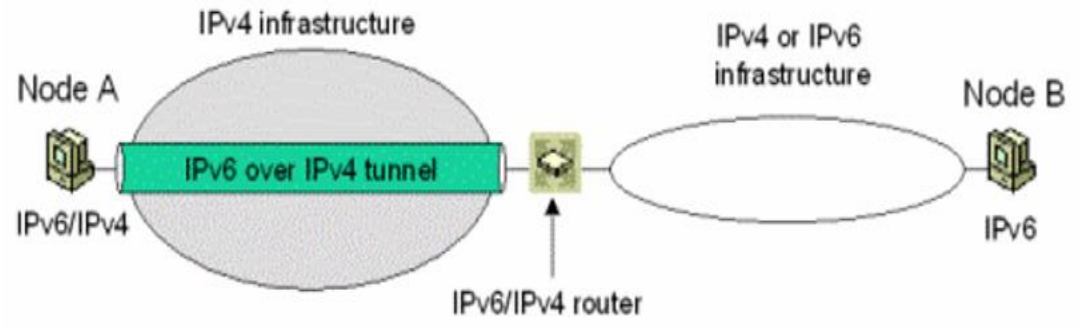
Στην περίπτωση αυτή οι hosts IPv6 / IPv4 που είναι διασυνδεδεμένοι πάνω από μια IPv4 υποδομή μπορούν να μεταδώσουν πακέτα IPv6 μεταξύ τους. Σε αυτή την περίπτωση, το tunnel εκτείνεται σε ολόκληρη τη διαδρομή από άκρο σε άκρο που περνάει το πακέτο.



Σχήμα 11: επικοινωνία μεταξύ δύο άκρων (Host-to-Host)

- Router-to-Host

Στην περίπτωση αυτή, οι δρομολογητές IPv6 / IPv4 μπορούν να μεταφέρουν πακέτα IPv6 στον τελικό προορισμό του host IPv6 / IPv4. Αυτό το tunnel εκτείνεται μόνο στο τελευταίο τμήμα της διαδρομής από άκρο σε άκρο.



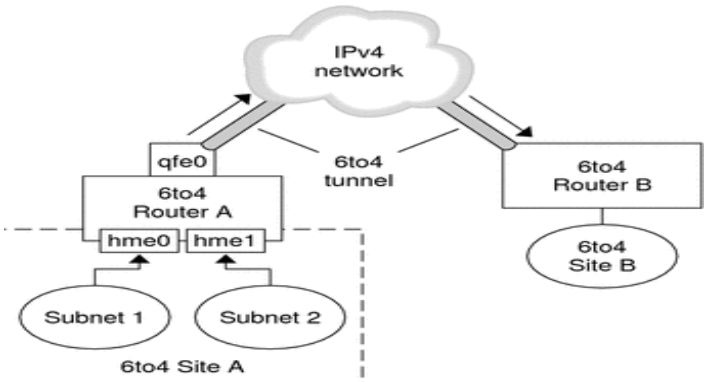
Σχήμα 12: επικοινωνία μεταξύ δύο άκρων (Router-to-Host)

Στην συνέχεια, όπως είπαμε παραπάνω, θα αναφερθούμε επιγραμματικά και στη δεύτερη κατηγορία μηχανισμών tunneling, τους αυτόματους μηχανισμούς tunneling. Οι κυριότεροι μηχανισμοί είναι:

- 6to4 tunnels

Ένας αυτόματος μηχανισμός tunneling 6to4 επιτρέπει σε απομονωμένα IPv6 domains να συνδέονται μέσω ενός δικτύου IPv4 μεταξύ τους. Η βασική διαφορά μεταξύ των αυτόματων tunnels 6to4 και των διαμορφωμένων tunnels είναι ότι το tunnel δεν είναι μόνο μεταξύ σημείου-προς-σημείου άλλα και από σημείο σε πολλαπλά σημεία Στις αυτόματες σήραγγες 6to4, οι δρομολογητές δεν έχουν διαμορφωθεί σε ζεύγη, αλλά αντιμετωπίζουν την υποδομή IPv4 ως σύνδεση virtual multi-access. Η IPv4 διεύθυνση η οποία έχει ενθυλακωθεί στην IPv6 διεύθυνση χρησιμοποιείται για την αυτόματη εύρεση του άλλου άκρου (έξοδος). [14]

Παρακάτω στο σχήμα 13 βλέπουμε και την τοπολογία ενός μηχανισμού 6to4 tunneling.



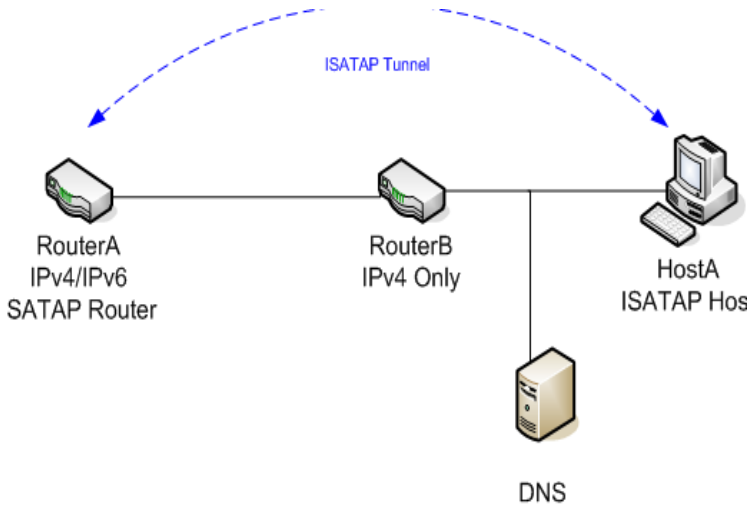
Σχήμα 13: Τοπολογία 6to4 tunnel

- ISATAP

Ο μηχανισμός ISATAP προέρχεται από τις λέξεις intra site automatic tunnel addressing protocol, που σημαίνει πρωτόκολλο διευθυνσιοδότησης αυτόματης σήραγγας υποδικτύου.

Πρόκειται για μία τεχνική τούνελ η οποία χρησιμοποιείται μέσα στο δίκτυο για να συνδέσει με το IPv6 τους απομονωμένους κόμβους διπλής στοίβας. Συνήθως απαιτείται ένας δρομολογητής ISATAP για ένα υποδίκτυο που λειτουργεί και ως εξυπηρετητής για όλους τους κόμβους που εξυπηρετεί.

Από το μηχανισμό αυτό, το δίκτυο IPv4 αντιμετωπίζεται ως ένα επίπεδο διασύνδεσης για το IPv6 θεωρώντας τους κόμβους στο δίκτυο ως δυνητικούς δρομολογητές IPv6. Πρόκειται, όπως είπαμε, για αυτόματο μηχανισμό καθώς απαιτεί μόνο τη διαμόρφωση των κόμβων του εφόσον υπάρχει αντίστοιχος δρομολογητής.



Σχήμα 14: ISATAP tunnel

3. Μοντέλα υπηρεσιών υπολογιστικού νέφους και εικονικοποίηση.

3.1 Υπολογιστικό νέφος.

Το cloud computing θα πρωταγωνιστήσει στην εξέλιξη των επιχειρήσεων και γενικότερα στην ανάπτυξη των οικονομικών μεγεθών των χώρων παγκοσμίως. Οι επιχειρήσεις επενδύουν όλο και περισσότερο στην τεχνολογία με την υιοθέτηση των τεχνολογιών του cloud computing και με αυτό τον τρόπο γίνονται πιο προσαρμόσιμες, πιο ευέλικτες και πιο καινοτόμες στην παγκόσμια οικονομία.

Παρόλα αυτά φαίνεται ότι η χρήση τεχνολογιών cloud στις επιχειρήσεις δεν είναι καθολική (private cloud), ειδικότερα στις μικρό-μεσαίες επιχειρήσεις η υιοθέτηση του cloud computing βρίσκεται ακόμα σε πολύ μικρό βαθμό. Όλο αυτό, όμως, έρχεται σε αντίθεση με εμάς τους καταναλωτές – χρήστες που έχουμε προσαρμοστεί πολύ καλύτερα στην χρήση τέτοιων τεχνολογιών. Αυτό συμβαίνει διότι καθημερινά χρησιμοποιούμε εφαρμογές όπως το Facebook, το tweeter και πολλές άλλες και προβλέπεται ότι λόγω της εξοικείωσης των χρηστών σε cloud τεχνολογίες και λόγω της μελλοντικής ένταξής τους ως εργατικό δυναμικό στις διάφορες επιχειρήσεις, η νοοτροπία τους αυτή είναι φυσικό να μεταφερθεί και να διαδοθεί και στις επιχειρήσεις στις οποίες θα εργαστούν. [2]

Το cloud computing αναφέρεται σε εφαρμογές που παραδίδονται ως υπηρεσίες μέσω του διαδικτύου και στα υπολογιστικά μηχανήματα και στο λογισμικό και τα οποία βρίσκονται σε ένα data center που παρέχει αυτές τις υπηρεσίες. Ως cloud αποκαλούμε το software και το hardware που βρίσκονται σε ένα κέντρο πληροφοριών. Ένα νέφος αποκαλείται public cloud όταν είναι διαθέσιμο με έναν τρόπο χρονικής μίσθωσης και οι υπηρεσίες που παρέχονται ονομάζονται υπολογιστικές δημόσιες υπηρεσίες. Ως ιδιωτικό νέφος αναφερόμαστε σε εσωτερικά κέντρα πληροφοριών ενός οργανισμού ή μιας επιχείρησης. [15]

Τα πληροφοριακά συστήματα των επιχειρήσεων δημιουργήθηκαν με την υπόσχεση να κάνουν τις επιχειρήσεις πιο ευκίνητες και πιο ευπροσάρμοστες. Πολλές επιχειρήσεις προέβησαν σε αναδιάρθρωση των διαδικασιών τους εφαρμόζοντας συστήματα ERP, όμως λόγω του πολύ μεγάλου μεγέθους των εφαρμογών αυτών, οι

επιχειρήσεις έπαψαν να είναι ευπροσάρμοστες σε οποιαδήποτε αλλαγή – αναβάθμιση των εφαρμογών λογισμού που χρησιμοποιούσαν. Πλέον, όπως αναφέρθηκε, οι επιχειρήσεις έχουν την δυνατότητα τέτοιες εφαρμογές όπως τα ERP συστήματα να φιλοξενούνται σε έναν πάροχο cloud, ο οποίος είναι και υπεύθυνος για τις διάφορες αναβαθμίσεις στο λογισμικό καθώς και της ίδιας εφαρμογής που χρησιμοποιεί η επιχείρηση. Έτσι γίνεται βελτιστοποίηση των διάφορων λειτουργιών και διαδικασιών σε μία επιχείρηση και με αυτόν τον τρόπο οι ανάγκες της καλύπτονται με κόστος που είναι εφικτό.

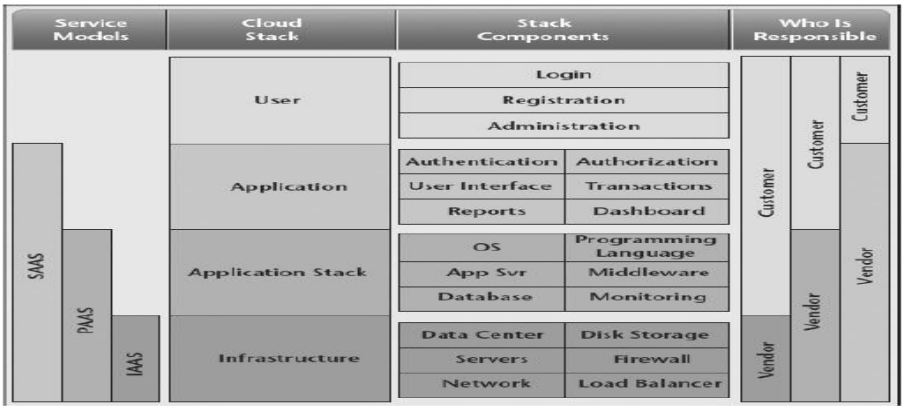
3.1.1 Μοντέλα υπηρεσιών υπολογιστικού νέφους.

Η επιλογή του σωστού μοντέλου εξυπηρέτησης cloud (cloud service model) αποτελεί πολύ κρίσιμο παράγοντα για την επιτυχημένη παροχή λύσεων που θα προταθούν. Για να γίνει η σωστή επιλογή του σωστού μοντέλου πρέπει να έχει κατανοηθεί πλήρως τα μοντέλα και την λειτουργία τους. Παρακάτω θα παρουσιαστούν τα μοντέλα αυτά. Υπάρχουν τρία μοντέλα υπηρεσίας νέφους και τρις θεμελιώδεις κατηγορίες οι οποίες συχνά αναφέρονται ως μοντέλο SPI.

Τα μοντέλα υπηρεσίας είναι:

- Δομή του νέφους ως υπηρεσία (IaaS)
- Πλατφόρμα νέφους ως υπηρεσία (PaaS)
- Λογισμικό νέφους ως υπηρεσία (SaaS)

Θα αναφερθούμε εκτενέστερα σε κάθε ένα από τα μοντέλα υπηρεσίας παρακάτω. Στο σχήμα 15 βλέπουμε αυτό που αποκαλούμε cloud stack το οποίο μας δίνει μια γενική άποψη της λειτουργίας των τριών αυτών μοντέλων. [7]



Σχήμα 15: Cloud stack [7]

3.1.1.1 Δομή του νέφους ως υπηρεσία (IaaS).

Όπως βλέπουμε και στο σχήμα 15 στο μοντέλο Iaas παρέχεται στον χρήστη η δυνατότητα να αναπτύσσει και να χρησιμοποιεί όποιο λογισμικό αυτός θέλει, που μπορεί να περιλαμβάνει λειτουργικά συστήματα και εφαρμογές, χρησιμοποιώντας βασικούς υπολογιστικούς πόρους, όπως επεξεργαστική ισχύ, αποθηκευτικά μέσα και δίκτυα. Ο χρήστης δεν διαχειρίζεται ούτε ελέγχει την υποδομή, αλλά μπορεί να έχει τον έλεγχο σε λειτουργικά συστήματα, μνήμες, εφαρμογές και πιθανόν περιορισμένο έλεγχο σε επιλεγμένα μέρη του εξοπλισμού της δικτύωσης.

Ο οργανισμός CSA (Cloud Security Alliance) ο οποίος αναφέρεται σε πρότυπα ασφάλειας του cloud computing αναφέρει ότι η υπηρεσία IaaS παρέχει υπολογιστική υποδομή συνήθως μέσα σε ένα εικονικό περιβάλλον μαζί με την δυνατότητα αποθήκευσης και δικτύωσης. Ο χρήστης έτσι δεν έχει την υποχρέωση να αγοράσει servers, αποθηκευτικό χώρο και δικτυακό εξοπλισμό και αντί αυτού αγοράζει – ενοικιάζει όλα τα παραπάνω ως υπηρεσίες από διάφορους providers που υπάρχουν. [26] Με την υπηρεσία IaaS η διαχείριση και η συντήρηση του κέντρο δεδομένων και γενικότερα της φυσικής υποδομής, μπορεί να πραγματοποιηθεί από τον χρήστη μέσω εφαρμογών που μας επιτρέπει να χρησιμοποιήσουμε ο διαχειριστής της φυσικής υποδομής – provider όπως για παράδειγμα από web – based κονσόλες.

Επειδή δεν υπάρχει η φυσική υποδομή δεν υπάρχει και η ανάγκη για τη διαχείριση της. Έτσι οι χρήστες – διαχωριστές μιας υπηρεσίας IaaS δεν ανησυχούν για την εγκατάσταση και την ανανέωση του hardware κάθε φορά που είναι αναγκαίο αυτό αφού αποκλειστικά υπεύθυνος είναι ο πάροχος που έχει αγοράσει την υπηρεσία.

Συνοπτικά μπορούμε να πούμε ότι με την υπηρεσία IaaS οι χρήστες έχουν την δυνατότητα να επικεντρωθούν πολύ περισσότερο στην υλοποίηση και διαχείριση των εφαρμογών τους και όχι στο να σπαταλούν χρόνο και χρήμα στην διαχείριση της φυσικής υποδομής. [7]

Παρακάτω θα αναφερθούμε σε μερικούς providers IaaS υπηρεσιών:

- Amazon AWS
- Microsoft Azure
- IBM SmartCloud Enterprise
- Google Compute Engine

3.1.1.2 Πλατφόρμα νέφους ως υπηρεσία (PaaS).

Το επόμενο επίπεδο στο cloud stack, όπως φαίνεται και στο σχήμα 15 δηλαδή, είναι οι υπηρεσίες PaaS, οι οποίες βρίσκονται πάνω από το επίπεδο υπηρεσιών IaaS στις οποίες αναφερθήκαμε παραπάνω. Ο χρήστης στο επίπεδο PaaS έχει την δυνατότητα να λειτουργήσει εφαρμογές που έχουν αναπτυχθεί από τον ίδιο, χρησιμοποιώντας κάποια γλώσσα προγραμματισμού η διάφορα εργαλεία τα οποία όμως παρέχονται από τον ίδιο τον πάροχο αυτών των υπηρεσιών τον cloud provider δηλαδή.

Σύμφωνα με τον CSA (Cloud Security Alliance) η υπηρεσία PaaS προσφέρει και διευκολύνει την ανάπτυξη εφαρμογών χωρίς το κόστος και την πολυπλοκότητα της αγοράς και της διαχείρισης του βασικού υλικού και λογισμικού. Ακόμα αναφέρεται ότι οι υπηρεσίες PaaS είναι διαθέσιμες εξ ολοκλήρου από το διαδίκτυο, οι πάροχοι PaaS υπηρεσιών διαχειρίζονται την πλατφόρμα εφαρμογών και παρέχουν στους προγραμματιστές - χρήστες μια σουίτα τέτοιων εργαλείων που θα βοηθήσουν στην διαδικασίας ανάπτυξης εφαρμογών. Οι προγραμματιστές προσφέρουν έναν βαθμό ευελιξίας με τις PaaS υπηρεσίες και όχι πλήρη ελευθερία διότι περιορίζουν τους χρήστες από τα εργαλεία και το λογισμικό που έχουν προς χρήση. Ακόμα ένας cloud πάροχος μπορεί ανάλογα με τις απαιτήσεις να διαθέσει ανάλογα την υπολογιστική ισχύ της πλατφόρμας έτσι ώστε όλοι οι χρήστες να λειτουργούν σε αποδεκτά επίπεδα. [7]

Ένα πολύ μεγάλο πλεονέκτημα των PaaS υπηρεσιών είναι ότι οι πλατφόρμες που παρέχονται από τους providers ενσωματώνουν μέσα τους πολλά λογισμικά τρίτων κατασκευαστών τα οποία αναφέρονται ως plugins - add-ons. Παρακάτω αναφέρουμε κάποιες βασικές κατηγορίες τέτοιων επεκτάσεων.

- Database
- Logging
- Monitoring
- Security
- Analytics
- Payments

Εν κατακλείδι, οι υπηρεσίες PaaS επιτρέπουν στις εταιρείες – πελάτες να επικεντρωθούν στις εφαρμογές στις οποίες θέλουν να αναπτύξουν και να προωθήσουν στην αγορά, κάνοντας τις εφαρμογές πολύ ανταγωνιστικές αφού τους δίνεται η δυνατότητα από τους providers να χρησιμοποιούν εργαλεία τα οποία είναι κάθε φορά ενημερωμένα στην τελευταία έκδοση τους. Έτσι, με αυτόν τον τρόπο μπορούν να εκμεταλλευτούν όλες τις δυνατότητες που τους διατίθενται.

3.1.1.3 Λογισμικό νέφους ως υπηρεσία (SaaS).

Στην κορυφή του cloud stack όπως βλέπουμε και στο σχήμα 15 βρίσκεται η υπηρεσία SaaS (software as a service) στην οποία παρέχεται η δυνατότητα στον χρήστη – πελάτη να κάνει χρήση των διάφορων εφαρμογών που παρέχονται από τον provider της cloud υπηρεσίας. Ο provider χειρίζεται εξ ολοκλήρου όλη την υποδομή του cloud, όλες τις εφαρμογές και γενικότερα όλο το deployment, οι πιο ευρέως διαδεδομένες εφαρμογές SaaS έχουν να κάνουν με υπηρεσίες customer management, ERP συστήματα και accounting εφαρμογές.

Οι υπηρεσίες SaaS χρησιμοποιούνται ευρέως από επιχειρήσεις και ένας από τους πολλούς λόγους είναι ότι η επιχείρηση δεν χρειάζεται να διαθέσει επιπλέον προσωπικό για την διαχείριση των εφαρμογών που αναφέραμε παραπάνω, αφού αποκλειστικά υπεύθυνος για την σωστή λειτουργία τους είναι ο cloud provider.

Ο NIST (National Institute of Standards and Technology) ορίζει τις υπηρεσίες SaaS ως τη δυνατότητα που παρέχεται στους χρήστες-πελάτες να χρησιμοποιούν εφαρμογές οι οποίες λειτουργούν και φιλοξενούνται στις υποδομές του cloud provider. Οι διάφορες εφαρμογές είναι προσβάσιμες από πολλούς χρήστες μέσω για παράδειγμα ενός web browser ή ενός application. [7]

Ο χρήστης δεν μπορεί να ελέγχει και να διαχειρίζεται την υποδομή του cloud συμπεριλαμβανομένων των δικτύων, των δρομολογητών, των servers και γενικότερα των διαφόρων λειτουργικών συστημάτων. Το μοναδικό το οποίο είναι πιθανά εφικτό να κάνει είναι να μπορεί να προχωρήσει σε αλλαγές στο προφίλ του και στο interface της εφαρμογής και αυτό διότι το έχει επιτρέψει ο διαχωριστής, ο cloud provider.

Παρακάτω θα αναφερθούμε σε μερικούς πολύ γνωστούς providers SaaS υπηρεσιών:

- Microsoft (Office 365)

- Amazon Web Services SaaS
- Oracle (ERP, CRM, SCM, HR)
- Cisco (WebEx)
- SAP (SAP Business ByDesign)
- Adobe

3.2 Εικονικοποίηση και Υπολογιστικό νέφος.

Για να λειτουργήσει ένα υπολογιστικό σύστημα προϋπόθεση είναι η ύπαρξη τριών βασικών και κύριων μονάδων, όπως οι επεξεργαστές, η κύρια και η δευτερεύουσα μνήμη και οι δίαυλοι επικοινωνίας οι οποίοι υπάρχουν για την επικοινωνία των διαφορετικών συστημάτων μεταξύ τους. Το λειτουργικό σύστημα είναι το λογισμικό αυτό το οποίο είναι υπεύθυνο για την διαχείριση των παραπάνω υπολογιστικών πόρων.

Η διαχείριση των υπολογιστικών πόρων για λογαριασμό πολλών και διαφορετικών χρηστών, οι οποίοι με την σειρά τους μπορούν να χρησιμοποιούν πολλές και διαφορετικές εφαρμογές, οι οποίες ενδεχομένως να «τρέχουν» σε διαφορετικά λειτουργικά συστήματα μόνο εύκολη υπόθεση δεν είναι για ένα cloud περιβάλλον ενός provider.

Η λύση για την παραπάνω πρόκληση είναι η εικονικοποίηση πόρων ή αλλιώς virtualization, η οποία είναι και μια βασική αρχή του cloud computing. Το πλεονέκτημα του virtualization είναι ότι απλοποιούνται ορισμένες εργασίες ως προς την διαχείριση πόρων για τους οποίους μιλήσαμε παραπάνω. Η κοινή χρήση πόρων σε ένα virtualized περιβάλλον έχει μεγάλες απαιτήσεις σε hardware και συγκεκριμένα υπάρχει η ανάγκη για μεγάλη επεξεργαστική ισχύ. [4]

3.2.1 Πλεονεκτήματα της Εικονικοποίησης στο Υπολογιστικό νέφος.

Όπως αναφέραμε και παραπάνω το virtualization είναι μια πολύ κρίσιμη πτυχή για το cloud computing και εξίσου σημαντική για τους providers όπως και για τους χρήστες – πελάτες cloud υπηρεσιών και διαδραματίζει πολύ σημαντικό ρόλο στην:

- ασφάλεια των λειτουργικών συστημάτων, και αυτό διότι επιτρέπει την απομόνωση υπηρεσιών που εκτελούνται από το ίδιο υλικό.
- απόδοση και αξιοπιστία των συστημάτων – εφαρμογών, επειδή επιτρέπει στις εφαρμογές να μετακινούνται από μια πλατφόρμα στην άλλη.
- ανάπτυξη και διαχείριση υπηρεσιών που παρέχονται από τον provider.
- απομόνωση της απόδοσης. [16]

3.2.2 Αρχιτεκτονική ενός Εικονικοποιημένου συστήματος.

Σε ένα cloud computing περιβάλλον ο Hypervisor η αλλιώς virtual machine monitor(VMM) λειτουργεί πάνω σε ένα φυσικό hardware ενός συστήματος και αυτό που κάνει είναι να δημιουργεί εικονικές μηχανές(VMs) και να είναι υπεύθυνος για την διαχείριση των φυσικών πόρων του συστήματος στις απαιτήσεις των διάφορων εικονικών μηχανών που θα δημιουργηθούν. Ακόμα επιτρέπει πολλαπλές υπηρεσίες να διαμοιράζονται την ίδια πλατφόρμα, επιτρέπει την μεταφορά ενός server από τη μια πλατφόρμα σε μία άλλη, την διαμόρφωση του συστήματος ενώ διατηρείται η προς τα πίσω συμβατότητα με το αυθεντικό σύστημα. Επίσης εντοπίζει τις προνομιακές οδηγίες που εκτελούνται από ένα φιλοξενούμενο λειτουργικό σύστημα κι επιβάλλει την ορθότητα και την ασφάλεια της λειτουργιάς. Τέλος ελέγχει τη διαχείριση της εικονικής μνήμης.

Παρακάτω όπως φαίνεται και στο σχήμα 17 βλέπουμε τους δύο τύπους Hypervisors. [17]

- Bare-metal hypervisors

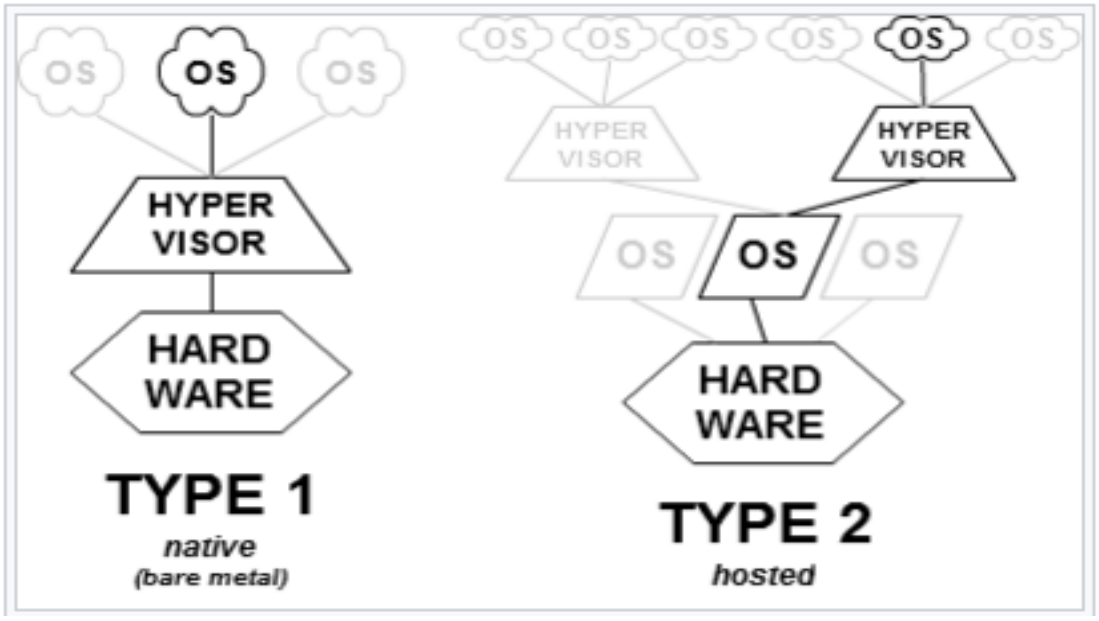
Αυτοί οι hypervisors «τρέχουν» απευθείας στο hardware του κεντρικού υπολογιστή έτσι ώστε να ελέγχουν το υλικό και να διαχειρίζονται το λειτουργικό σύστημα των guest μηχανημάτων (VMs).

VMware ESX- ESXi, Microsoft Hyper-V, Citrix XenServer, Oracle VM είναι παραδείγματα type-1 Hypervisors.

- Hosted hypervisors

Αυτοί οι hypervisors «τρέχουν» σε ένα συμβατικό λειτουργικό σύστημα, όπως δηλαδή ένα οποιοδήποτε πρόγραμμα σε έναν ηλεκτρονικό υπολογιστή. Το λειτουργικό σύστημα ενός μηχανήματος επισκέπτη υπάρχει ως διεργασία στον κεντρικό υπολογιστή.

Τα Virtual Box, VMware Player, VMware Workstation, QEMU είναι παραδείγματα Hypervisors.



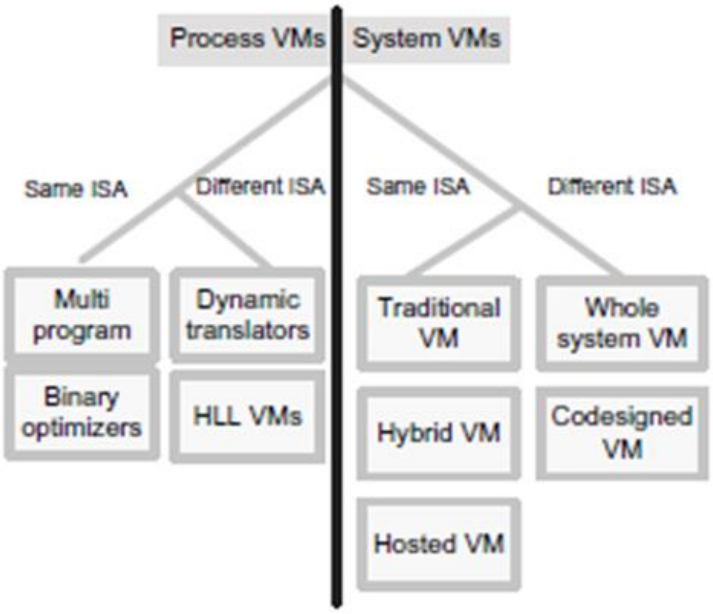
Σχήμα 17: Type-1 και type-2 Hypervisors. [27]

Παρακάτω θα γίνει αναφορά στην έννοια της εικονικής μηχανής – virtual machine (VM) και στα είδη εικονικών μηχανών που υπάρχουν. [4]

Μια εικονική μηχανή είναι ένα απομονωμένο περιβάλλον που παρουσιάζεται ως ένα ολόκληρο υπολογιστικό σύστημα, ενώ στην πραγματικότητα έχει πρόσβαση μονό σε ένα συγκεκριμένο σύνολο πόρων του υπολογιστικού συστήματος που την φιλοξενεί.

Υπάρχουν διαφορετικά είδη εικονικών μηχανών με διαφορετικές λειτουργίες το κάθε ένα.

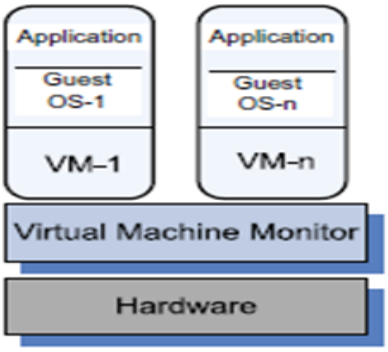
Όπως βλέπουμε στο παρακάτω σχήμα, ξεχωρίζουμε δύο διαφορετικά είδη εικονικών μηχανών την εικονική μηχανή διεργασίας (Process VM) και την εικονική μηχανή συστήματος (System VM). Στην πρώτη περίπτωση μία μηχανή διεργασίας είναι μια εικονική πλατφόρμα που δημιουργείται για μία μοναδική διεργασία και καταστρέφεται μόλις η διεργασία τερματιστεί. Στην δεύτερη περίπτωση μια εικονική μηχανή συστήματος υποστηρίζει ένα λειτουργικό σύστημα μαζί με πολλές διεργασίες χρηστών.



Σχήμα 18: Είδη εικονικών μηχανών

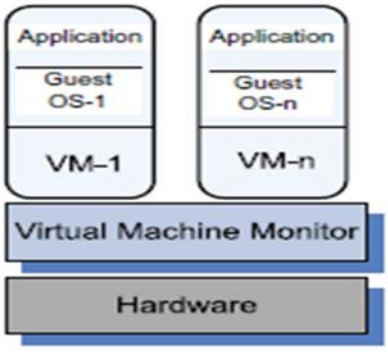
Στα παρακάτω σχήματα βλέπουμε τις βασικές κατηγορίες των εικονικών μηχανών συστήματος (System VMs).

- Παραδοσιακή εικονική μηχανή (Traditional VM), υποστηρίζει πολλές εικονικές μηχανές κι εκτελείται απευθείας πάνω στο υλικό.



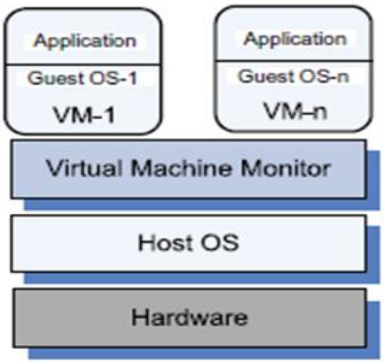
Σχήμα 19: Παραδοσιακή εικονική μηχανή

- Υβριδική εικονική μηχανή (Hybrid VM), μοιράζεται το υλικό το λειτουργικό σύστημα του host και υποστηρίζει πολλές εικονικές μηχανές.



Σχήμα 20: Υβριδική εικονική μηχανή

- Φιλοξενούμενη εικονική μηχανή (Hosted VM), εκτελείται μέσα από το λειτουργικό σύστημα του host.



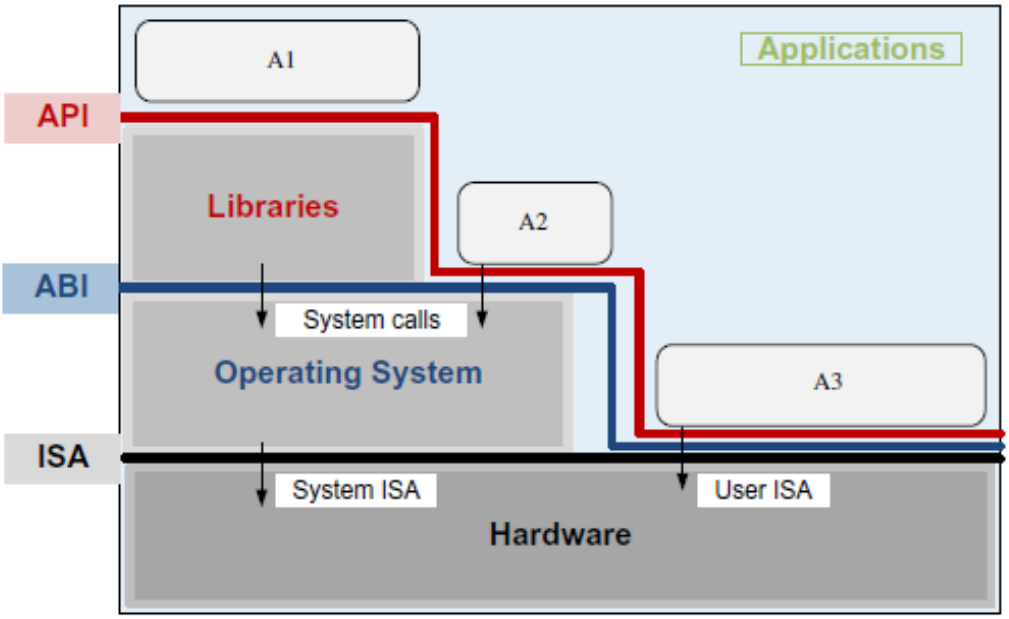
Σχήμα 21: Φιλοξενούμενη εικονική μηχανή

3.2.3 Στρωματοποίηση – Διαχείριση πολυπλοκότητας σε Εικονικοποιημένα συστήματα.

Στρωματοποίηση ή layering είναι μια κοινή προσέγγιση για τη διαχείριση της πολυπλοκότητας ενός virtualized συστήματος. Έτσι με την στρωματοποίηση καταφέρνουμε να μειώσουμε τις αλληλεπιδράσεις μεταξύ των διαφόρων υποσυστημάτων και βέβαια καταφέρνουμε να απλοποιήσουμε και την περιγραφή τους. Μπορούμε ακόμα να σχεδιάσουμε, να υλοποιήσουμε και να τροποποιήσουμε το κάθε υποσύστημα ξεχωριστά.

Στο παρακάτω σχήμα βλέπουμε την στρωματοποίηση σε ένα υπολογιστικό σύστημα και παρατηρούμε ότι αποτελείται ξεκινώντας από κάτω προς τα επάνω από το υλικό και το λογισμικό (λειτουργικό σύστημα, βιβλιοθήκες, εφαρμογές).

Τώρα θα μιλήσουμε για τις διεπαφές – interfaces με τις οποίες το ένα υποσύστημα αλληλεπιδρά με το άλλο. [4]



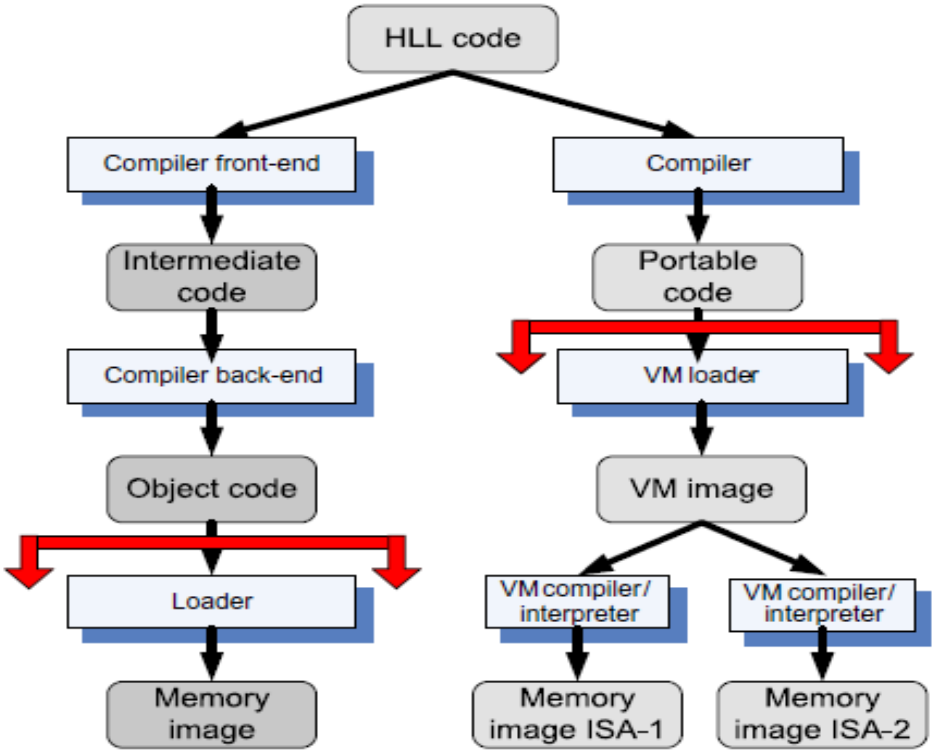
Σχήμα 22: Στρωματοποίηση και οι διεπαφές μεταξύ των layers

Όπως βλέπουμε και στο σχήμα 22 ξεκινώντας πάλι από κάτω προς τα επάνω η πρώτη διεπαφή που βλέπουμε είναι η (ISA) - Instruction Set Architecture, η οποία βρίσκεται μεταξύ υλικού και λογισμικού.

Στην συνέχεια η επόμενη διεπαφή είναι η (ABI) - Application Binary Interface η οποία επιτρέπει στα περιεχόμενα της εφαρμογής και στις ενότητες της βιβλιοθήκης να έχουν πρόσβαση στο υλικό. Δεν περιλαμβάνει προνομιακές οδηγίες συστήματος και επικαλείται κλήσεις συστήματος.

Τελευταία διεπαφή είναι η (API) - Application Program Interface η οποία προσδιορίζει τις οδηγίες που μπορεί να εκτελεί το υλικό και παρέχει στην εφαρμογή πρόσβαση στο ISA. Περιλαμβάνει κλήσεις για τη βιβλιοθήκη HLL που συχνά επικαλείται κλήσεις συστήματος και χρησιμοποιεί τις λειτουργίες της βιβλιοθήκης (A1), κάνει κλήσεις συστήματος (A2) κι εκτελεί τις οδηγίες μηχανής (A3).

Παρακάτω στο σχήμα 23 γίνεται αναφορά στην φορητότητα κώδικα. Ως παραδοχή έχουμε ότι αρχεία που δημιουργούνται από ένα μεταγλωττιστή για συγκεκριμένη ISA και συγκεκριμένα λειτουργικά συστήματα δεν είναι φορητά, είναι όμως εφικτό να μεταγλωττιστεί ένα HLL (High Level Programming) πρόγραμμα για το περιβάλλον μίας εικονικής μηχανής όπου ο φορητός κώδικας παράγεται και διανέμεται και μετά μετατρέπεται από τους δυαδικούς μεταφραστές στην ISA του host. [4]



Σχήμα 23: Διαδικασία μεταγλώττισης ενός HLL προγράμματος

4. Πλεονεκτήματα του πρωτοκόλλου IPv6 στο Υπολογιστικό νέφος.

Σε αυτό το κεφάλαιο, θα αναλυθούν δύο πολύ σημαντικά ζητήματα, τα οποία διαδραματίζουν κομβικό ρόλο προκειμένου η υπολογιστική νέφους να συνεχίσει τον πρωταγωνιστικό της ρόλο και στο μέλλον. Αυτά είναι: το ζήτημα της ασφάλειας στην μετάδοση δεδομένων σε δίκτυα υπολογιστικού νέφους και το ζήτημα της κινητικότητας (mobility) του χρήστη.

4.1 Ασφάλεια.

Στο cloud computing κυρίαρχος και καθοριστικός παράγοντας είναι η ασφάλεια των δεδομένων διότι πιθανοί πελάτες είτε είναι ιδιώτες είτε εταιρείες θα εμπιστευτούν και θα συνεχίζουν να εμπιστεύονται παρόχους - providers οι οποίοι θα μπορούν να καλύψουν αυτή τους την ανάγκη. Η ιδέα ειδικά για τους εταιρικούς πελάτες, ότι τα "ευαίσθητα" δεδομένα τους είναι κάπου αποθηκευμένα στο "σύννεφο" χωρίς κάποιος να τους εγγυηθεί για την ασφαλή αποθήκευση αλλά και διάδοση τους, είναι κομβικής σημασίας. Επομένως η παροχή ασφάλειας στις υπηρεσίες του cloud computing είναι μονόδρομος.

Οι μηχανισμοί που έχουν αναπτυχθεί για την ασφαλή μετάδοση και μεταφορά δεδομένων από το πρωτόκολλο διαδικτύου IPv4 είναι προς την σωστή κατεύθυνση της ασφάλειας αλλά λόγω της ανάγκης για μεγαλύτερη ανάπτυξη του cloud computing, το πρωτόκολλο IPv4 ίσως να μην έχει την δυνατότητα να ανταποκριθεί σε αυτήν την πρόκληση.

Το νέο πρωτόκολλο διαδικτύου IPv6 μπορεί πολύ καλύτερα να επιτύχει σε αυτήν την πρόκληση και αυτό γιατί είναι ένα πρωτόκολλο που τα δομικά του στοιχεία προέβλεψαν εξ αρχής να καλύψουν την ανάγκη για ασφαλή μετάδοση και μεταφορά δεδομένων. Παρακάτω θα τονιστούν αναλυτικά οι μηχανισμοί και η λειτουργία τους ώστε η ασφάλεια στο του cloud computing να έχει το επιθυμητό αποτέλεσμα. [9]

Ο μηχανισμός που χρησιμοποιείται ευρύτατα στο πρωτόκολλο διαδικτύου IPv4 και κατ' επέκταση σε δίκτυα υπολογιστικού νέφους είναι ο NAT (Network Address Translation), ο κύριος λόγος που δημιουργήθηκε είναι λόγω του περιορισμένου αριθμού IP διευθύνσεων που παρέχει το πρωτόκολλο αυτό. Ταυτόχρονα, όμως, ο

μηχανισμός NAT είναι και ο κύριος λόγος που το πρωτόκολλο IPv4 υστερεί σε επίπεδο ασφάλειας σε δίκτυα υπολογιστικού νέφους.

Το πρωτόκολλο IPsec "Internet Protocol Security" είναι αυτό, που όπως λέει και η ονομασία του, παρέχει ασφάλεια στην μεταφορά και την διάδοση των δεδομένων κάνοντας αυθεντικοποίηση και κρυπτογράφηση των διάφορων πακέτων που μεταδίδονται στο δίκτυο. Παρακάτω θα παρουσιαστεί πώς αποφεύγοντας τον μηχανισμό NAT το πρωτόκολλο ασφαλείας IPsec δημιουργεί περισσότερες δυνατότητες και επιλογές σε ένα cloud computing περιβάλλον.

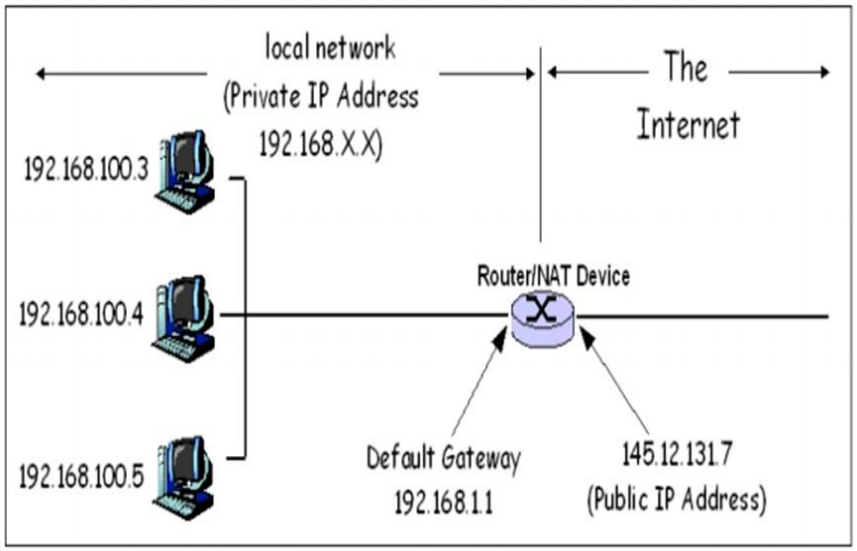
4.1.1 Μη χρησιμοποίηση του μηχανισμού NAT (Network Address Translation).

Το πρωτόκολλο IPv6 όπως αναφέραμε και παραπάνω δημιουργήθηκε ώστε να έχει νέα χαρακτηριστικά, τα οποία όπως θα φανεί σε αυτό το κεφάλαιο θα επιλύσουν προβλήματα του πρωτοκόλλου IPv4.

Το πρώτο και κύριο χαρακτηριστικό είναι το πλήθος των IP διευθύνσεων που τώρα μπορούν να φτάσουν σε αριθμούς 2^{128}. Το πλεονέκτημα αυτό λύνει το πρόβλημα της εξάντλησης των IP διευθύνσεων παγκόσμια. Παράλληλα αυτό μας απαλλάσσει από την ανάγκη για χρήση του μηχανισμού NAT.

4.1.1.1 Λειτουργία NAT μηχανισμού.

Παρακάτω δίνεται με τη βοήθεια του σχήματος 24 ένα παράδειγμα χρήσης του NAT.



Σχήμα 24: Μηχανισμός NAT

Βλέπουμε ότι το NAT router αποτελείται από μία ιδιωτική διεύθυνση, την 192.168.1.1, και από μία δημόσια, την 145.12.131.7. Η κίνηση που φεύγει από το δρομολογητή με προορισμό το διαδίκτυο όπως και η κίνηση που φτάνει στο δρομολογητή από το διαδίκτυο έχει IP πηγής και IP προορισμού τη δημόσια IP διεύθυνση. Όταν ένα πακέτο δεδομένων θα φτάσει στο δρομολογητή από έναν υπολογιστή του δικτύου, τότε αυτός θα αντικαταστήσει την IP πηγής με τη δική του την δημόσια, θα του αναθέσει ένα καινούριο port και αφού δημιουργήσει μία καταχώρηση στον πίνακα NAT (translation table) που διαθέτει, θα στείλει το πακέτο.

Όταν αυτό θα φτάσει στον προορισμό του αγνοώντας ότι το πακέτο έχει τροποποιηθεί από τον NAT router θα στείλει την απάντηση με IP προορισμού που αντιστοιχεί στο δρομολογητή. Φτάνοντας στο δρομολογητή, αυτός ελέγχει τον πίνακα NAT για να αποκτήσει την κατάλληλη IP διεύθυνση για τον υπολογιστή που πρέπει να καταλήξει το πακέτο. Αφού τα βρει, θα κάνει την αντιστοίχηση των IPs και προωθεί το πακέτο κατάλληλα εντός του δικτύου. [18]

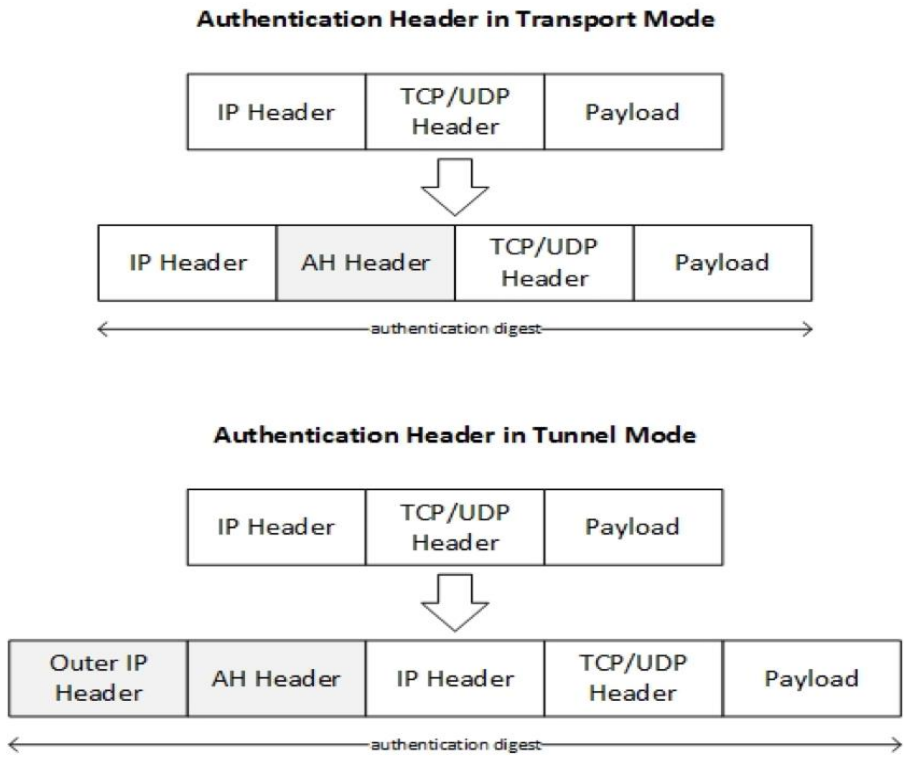
Παραπάνω παρουσιάστηκε η λειτουργία του βασικού μηχανισμού NAT για να μπορέσουμε παρακάτω να δούμε πώς αυτός ο μηχανισμός επηρεάζει το πρωτόκολλο ασφαλείας IPsec.

4.1.1.2 Πρωτόκολλο IPSec.

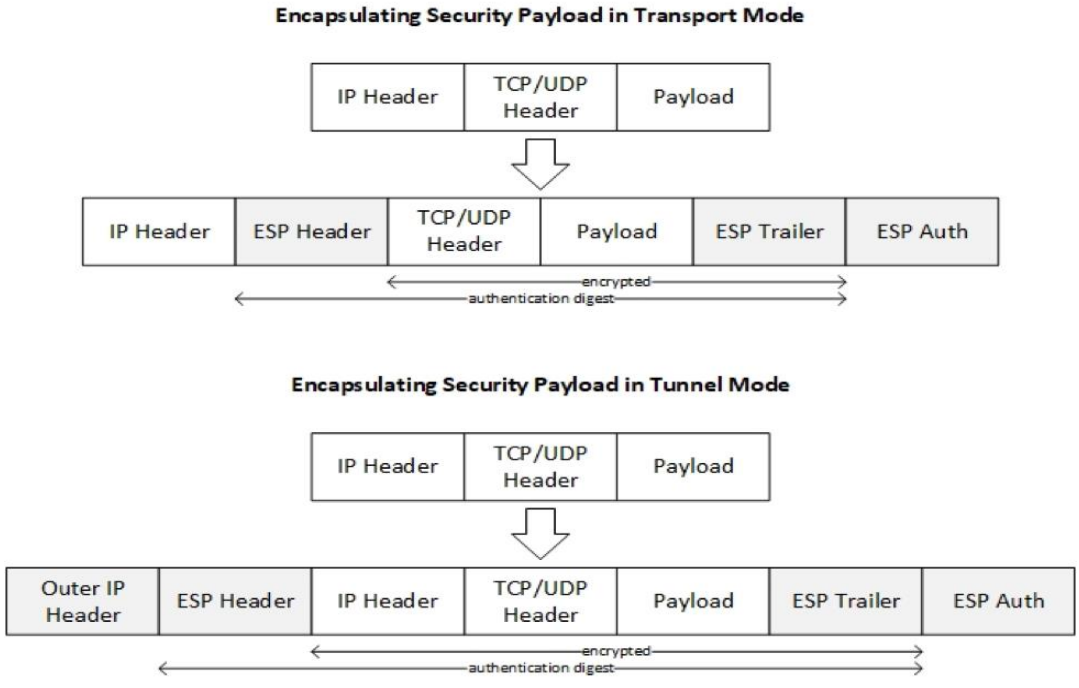
Παρακάτω παρουσιάζεται η βασική λειτουργία του πρωτόκολλου ασφάλειας IPsec έτσι ώστε, σε συνδυασμό με την λειτουργία του μηχανισμού NAT που αναλύθηκε παραπάνω, να μπορέσει να βγει το συμπέρασμα ότι: ένα end to end IPsec είναι αδύνατο σε δίκτυα υπολογιστικού νέφους στα οποία χρησιμοποιείται το πρωτόκολλο IPv4.

Οι αρχές της αυθεντικοποίησης και της κρυπτογράφησης είναι βασικές για την μεταφορά πακέτων - δεδομένων με ασφάλεια, αυτό επιτυγχάνεται μέσω των επικεφαλίδων AH(authentication) και ESP(encryption) του IPsec πρωτοκόλλου, οι οποίες προστίθενται στο αρχικό πακέτο που βρίσκεται προς αποστολή.

Όπως βλέπουμε και στα παρακάτω σχήματα, σχήματα 25 και 26 το πρωτόκολλο IPsec κάνει αυθεντικοποίηση και κρυπτογράφηση σε δύο λειτουργίες, σε tunnel mode (επικοινωνία χρήστη με το gateway) και transport mode (επικοινωνία χρήστη με χρήστη) και σε κάθε μια από τις παρακάτω περιπτώσεις η εισαγωγή της επικεφαλίδας γίνεται με διαφορετικό τρόπο. [20]

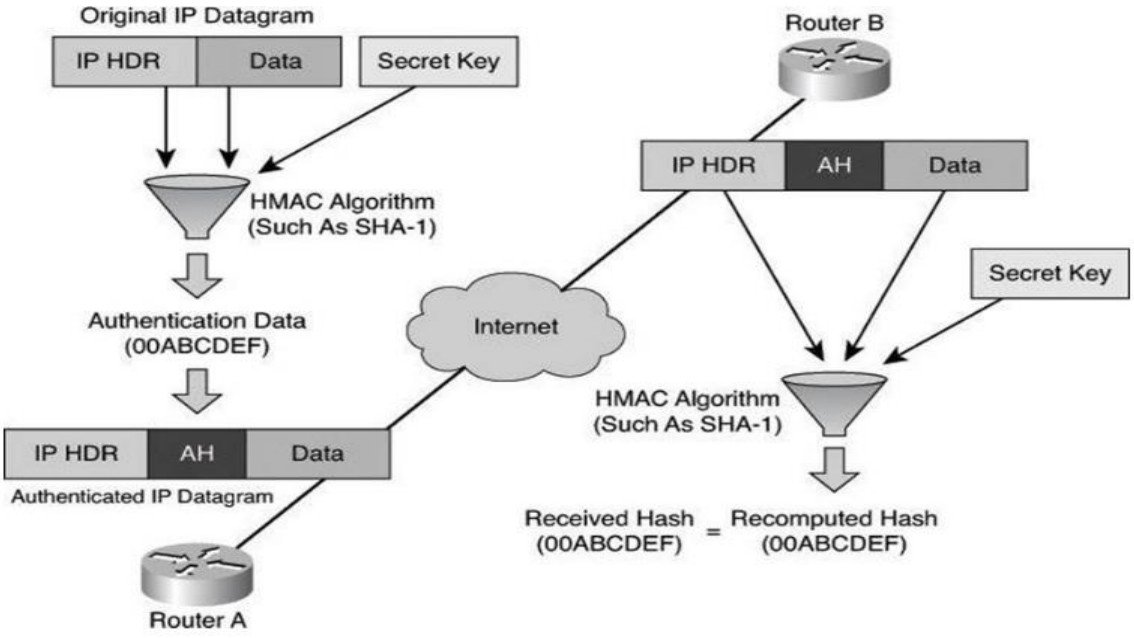


Σχήμα 25: Αυθεντικοποίηση σε transport mode και σε tunnel mode



Σχήμα 26: Encryption σε transport mode και σε tunnel mode

Παρακάτω στο σχήμα 27 θα δούμε πως το πρωτόκολλο IPsec, παράγει την επικεφαλίδα AH (Authentication Header).



Σχήμα 27: Διαδικασία παραγωγής του AH (Authentication Header) [20]

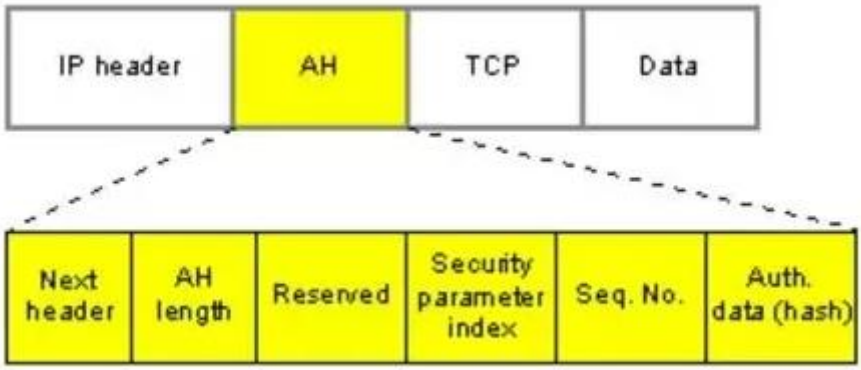
Η παραγωγή της επικεφαλίδας AH και η μετάδοση του πακέτου από τον Router A στον Router B γίνεται σε τέσσερα βήματα.

Βήμα 1. Η επικεφαλίδα IP μαζί με το φορτίο δεδομένων από τα υψηλότερα επίπεδα και με την βοήθεια ενός αλγορίθμου HMAC παράγει έναν μοναδικό αριθμό (Hash).

Βήμα 2. Ο μοναδικός αριθμός Hash δημιουργεί μια νέα επικεφαλίδα την AH σχήμα 28, η οποία προστίθεται και στο αρχικό πακέτο.

Βήμα 3. Το νέο πακέτο μεταδίδεται στον Router B.

Βήμα 4. Ο Router B από το πακέτο που έλαβε υπολογίζει από την αρχή τον Hash αριθμό των επικεφαλίδων IP και δεδομένων και τον συγκρίνει με τον αριθμό Hash που έλαβε από την επικεφαλίδα AH. Έστω και μια μικρή αλλαγή στο πακέτου που μεταφέρθηκε να έχει συμβεί τότε οι αριθμοί Hash δεν πρόκειται να είναι ίσοι, στην περάτωση αυτή το πακέτο απορρίπτεται.



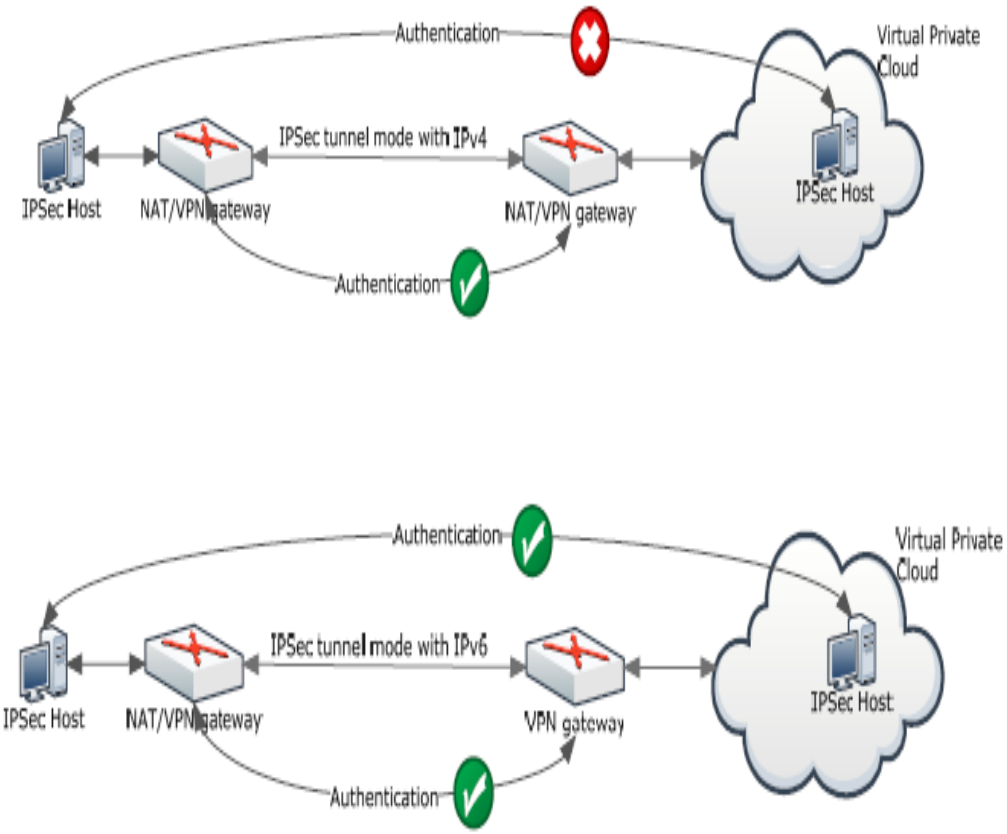
Σχήμα 28: Από τη αποτελείται ο AH (Authentication Header)

4.1.2 Συμπεράσματα.

Τώρα αφού αναλύσαμε την επικεφαλίδα AH του πρωτοκόλλου IPsec και με βάση την λειτουργία του μηχανισμού NAT σε IPv4 δίκτυο που είδαμε παραπάνω ένα συμπέρασμα που ίσως θα μπορούσε να εξαχθεί είναι ότι, εάν ένα πακέτο δεδομένων το οποίο βρίσκεται σε διαδικασία αποστολής τροποποιηθεί για οποιονδήποτε λόγο κατά την διάρκεια της μεταφοράς του από τον ένα κόμβο σε άλλον, η αποστολή θα αποτύχει λόγο της μη αυθεντικότητας των δεδομένων που θα ληφθούν στον τελικό προορισμό.

΄Ετσι βγάζουμε το συμπέρασμα ότι ο μηχανισμός NAT δεν κάνει μία end to end IPsec σύνδεση δυνατή και αυτό σε ένα cloud computing περιβάλλον με τόσες αυξημένες απαιτήσεις δεν είναι τόσο επιθυμητό διότι ενδεχομένως η ασφάλεια και η ταχύτητα στην μεταφορά των δεδομένων να μην είναι σε τόσο υψηλό επίπεδο.

Παρακάτω στο σχήμα 29 απεικονίζονται διαφορετικές τοπολογίες IPv4 και IPv6 δικτύων και τον τρόπο που κάθε φορά γίνεται η αυθεντικοποίηση μεταξύ των δύο Hosts. Στο πρώτο δίκτυο βλέπουμε ότι μέσω του μηχανισμού NAT γίνεται η αυθεντικοποίηση μεταξύ των διάφορων κόμβων (gateways), ενώ σε ένα IPv6 δίκτυο η αυθεντικοποίηση γίνεται και σε επίπεδο Hosts, έχουμε δηλαδή μια end to end IPsec σύνδεση μεταξύ τους.



Σχήμα 29: End to end αυθεντικοποίηση σε δίκτυο IPv6 σε σύγκριση με το IPv4

Εν κατακλείδι μπορούμε να αναφέρουμε ότι η ασφάλεια σε ένα cloud computing περιβάλλον παίζει κυρίαρχο ρόλο και είναι ένας πολύ σημαντικός παράγοντας για πελάτες – εταιρείες και όχι μόνο, ώστε να εμπιστευτούν τέτοιες υπηρεσίες. Το πρωτόκολλο IPsec δημιουργήθηκε από την αρχή για να λειτουργεί με το νέο πρωτόκολλο διαδικτύου IPv6, αλλά λόγο της χαμηλής ακόμα υιοθέτησης του, το IPsec προσαρμόστηκε σε δίκτυα IPv4 που ακόμα κυριαρχούν.

Όπως είναι φυσικό, το IPsec δεν παρέχει όλες τις δυνατότητες του όταν εφαρμόζεται στα δίκτυα που λειτουργούν με το πρωτόκολλο IPv4 και ένας παράγοντας που το επηρεάζει είναι η χρησιμοποίηση του μηχανισμού NAT.

4.2 Κινητικότητα (Mobility).

Στη προηγούμενη ενότητα είδαμε ότι ο τομέας της ασφάλειας δεδομένων σε ένα cloud computing περιβάλλον είναι η πρώτη προτεραιότητα που πρέπει να έχουν οι πάροχοι (providers), έτσι ώστε το cloud computing να συνεχίσει την ολοένα

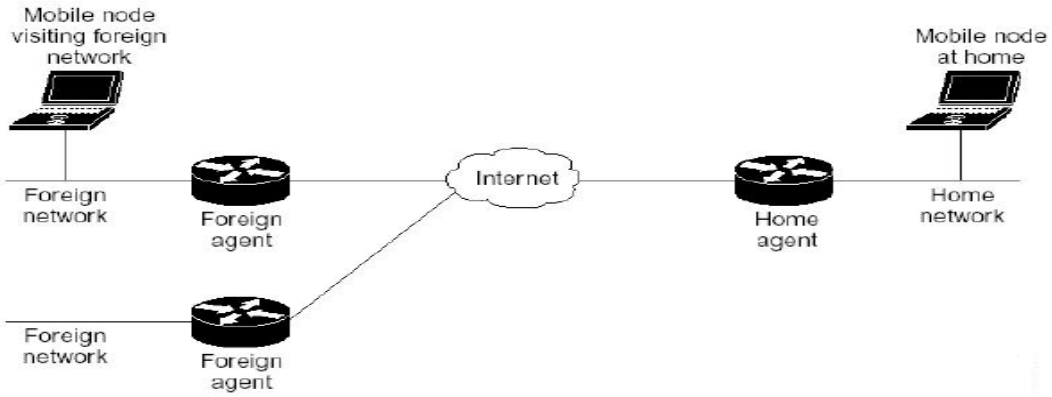
αυξανόμενη χρήση του και αυτό ίσως επιτευχθεί με την χρήση του νέου πρωτοκόλλου διαδικτύου IPv6.

Η χρήση του διαδικτύου όπως φάνηκε και στο πρώτο κεφάλαιο βρίσκεται σε διαρκή αύξηση, παράλληλα όμως αναπτύσεται διαρκώς και η χρήση του διαδικτύου από κινητές συσκευές. Οι κινητές συσκευές χρησιμοποιούν κατά βάση εφαρμογές cloud computing οπότε ένα εύλογο συμπέρασμα θα ήταν ότι όσο αυξάνεται η χρήση έξυπνων κινητών συσκευών έτσι θα αυξάνεται και η χρήση cloud εφαρμογών, βέβαια αυτή η σχέση είναι αμφίδρομη. Παράλληλα όμως θα αυξάνονται και οι απαιτήσεις των χρηστών αυτών των υπηρεσιών, οι οποίες θα πρέπει να είναι αποτελεσματικές σε όλη την διάρκεια της λειτουργίας τους από αυτές τις συσκευές.

Είναι δεδομένο ότι μια συσκευή αλλάζει πολλά διαφορετικά δίκτυα κατά την διάρκεια της λειτουργία της, επομένος προκύπτει η ανάγκη για παροχή cloud υπηρεσιών με μεγάλες απαιτήσεις σε κινητικότητα από τον χρήστη.

4.2.1 Mobile IPV4.

Το πρωτόκολλο το οποίο σχεδιάστηκε για να καλύψει την ανάγκη για κινητικότητα των χρηστών για την οποία έγινε αναφορά παραπάνω είναι το MIPv4 (Mobile Internet Protocol) το οποίο χρησιμοποιείται σε δίκτυα IPv4. Η βασική αρχή είναι η κινητή συσκευή να διατηρήσει την ίδια IP διεύθυνση ανεξάρτητα εάν ο χρήστης αλλάζει από το ένα δίκτυο σε άλλο με σκοπό να μην αλλάξουν την κατάσταση τους οι τρέχουσες εφαρμογές του χρήστη. Στο σχήμα 30 βλέπουμε την βασική αρχιτεκτονική του.



Σχήμα 30: Αρχιτεκτονική του MIPv4 (Mobile Internet Protocol)

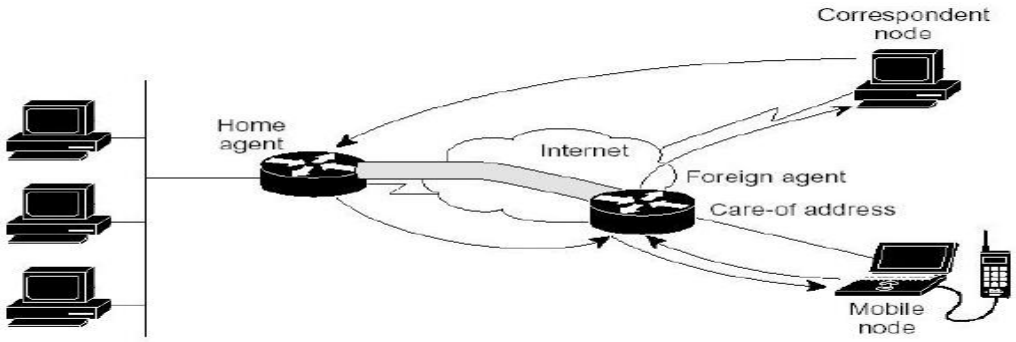
Η βασική αρχιτεκτονική του πρωτοκόλλου MIP αποτελείται από τα βασικά στοιχεία τα όποια και θα αναλυθούν παρακάτω:

- Mobile Node: είναι για παράδειγμα μια κινητή συσκευή η οποία έχει την δυνατότητα να εναλλάσσει δίκτυα.
- Home Agent: είναι ένας δρομολογητής στο home δίκτυο μας και είναι υπεύθυνος για να προωθεί τα πακέτα στην κινητή συσκευή ενώ είναι μέσα στο home δίκτυο. Σε περίπτωση τώρα που η κινητή συσκευή απομακρύνεται από το home δίκτυο τα πακέτα που θα φτάσουν σε αυτό το δίκτυο θα πρέπει να παραδοθούν στην νέα θέση της κινητής συσκευής. Αυτό επιτυγχάνεται με μια διαδικασία (packet tunneling) που προωθεί τα πακέτα στην νέα θέση.
- Foreign Agent: είναι και αυτός ένας δρομολογητής και συνδέεται με την κινητή συσκευή όταν αυτή αλλάζει δίκτυο και είναι υπεύθυνος για να παραδώσει τα πακέτα από τον home agent στην κινητή συσκευή.

Σε αυτό το σημείο προκείμενου να γίνει κατανοητή η λειτουργία του MIP θα πρέπει να εξηγηθεί και η CoA (Care of-address).

CoA: είναι το σημείο λήξης του tunnel προς την κινητή συσκευή όταν βρίσκεται σε ξένο δίκτυο, ο home agent διατηρεί μια ένωση μεταξύ της home IP της κινητής συσκευής και της CoA, η οποία αντιπροσωπεύει την τρέχουσα θέση της συσκευής όταν βρίσκεται σε ξένο δίκτυο.

Παρακάτω παρουσιάζεται ένα σενάριο αποστολής πακέτων σε MIPv4. Η κινητή συσκευή έχει την δυνατότητα να στέλνει τα πακέτα με την χρήση της home IP δείχνοντας έτσι ότι βρίσκεται πάντα συνδεδεμένος με το home δίκτυο του, αυτό ισχύει ακόμα και στην περίπτωση που η κινητή συσκευή βρίσκεται σε ξένο δίκτυο. Αυτό βέβαια είναι και το ζητούμενο για την κινητικότητα χρήστη που αναφέρθηκε και παραπάνω. Τα πακέτα που απευθύνονται προς την κινητή συσκευή οδηγούνται στο home δίκτυο της και ο home agent παρεμποδίζει την αποστολή τους στο home δίκτυο, αλλά τα αποστέλλει μέσω ενός tunnel προς την κινητή συσκευή χρησιμοποιώντας την CoA. Η αντίστροφή διαδικασία όπως φαίνεται και στο σχήμα 31 γίνεται με την βοήθεια του correspondent node, δηλαδή η κινητή συσκευή στέλνει τα πακέτα στον foreign agent ο οποίος τα οδηγεί στον τελικό τους προορισμό μέσω του correspondent node. [21]



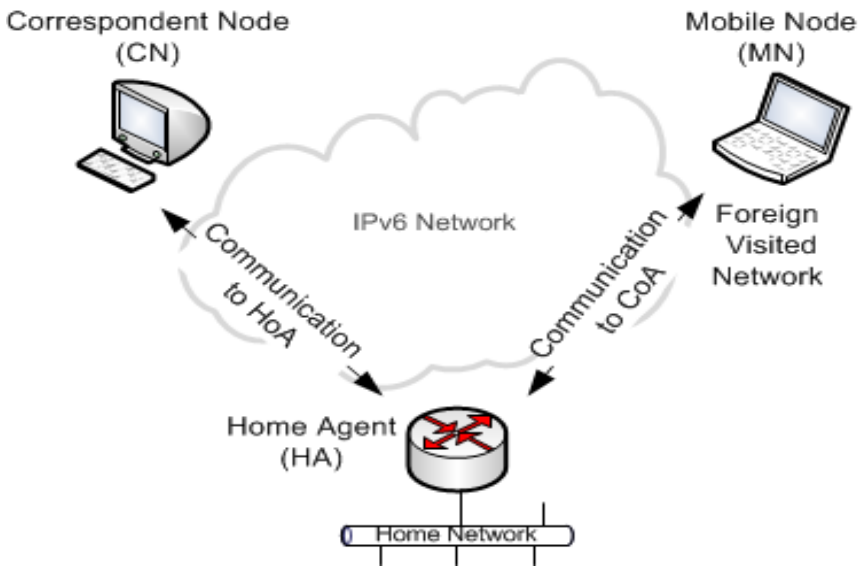
Σχήμα 31: Παραλαβή – αποστολή πακέτων σε MIPv4

4.2.2 Mobile IPV6.

Στην συνέχεια του κεφαλαίου θα γίνει αναφορά στη κινητικότητα του χρήστη με το καινούργιο πρωτόκολλο κινητικότητας MIPv6 το οποίο εφαρμόζεται μέσω του νέου πρωτόκολλου διαδικτύου IPv6 ακόμα θα παρουσιαστεί το νέο αυτό πρωτόκολλο ώστε να γίνει κατανοητή η λειτουργία του και βέβαια να εντοπιστούν οι διαφορές με το προηγούμενο πρωτόκολλο κινητικότητας MIPv4.

Αρχικά σε κάθε κινητή συσκευή της ανατίθενται δύο διευθύνσεις από το αρχικό δίκτυο δηλαδή από τον home agent, μία στατική διεύθυνση home address (HoA) η οποία χρησιμοποιείται για την σύνδεση με το αρχικό της δίκτυο και μια δεύτερη διεύθυνση που είναι δυναμική και ονομάζεται care of address (CoA), η οποία χρησιμοποιείται για την δρομολόγηση πακέτων προς το πιο πρόσφατο σημείο σύνδεσης την κινητής συσκευής. Η home address είναι μια IP, της οποίας το πρόθεμα υποδικτύου αντιστοιχεί στο οικείο - αρχικό δίκτυ., Με αυτό τον τρόπο η δρομολόγηση πακέτων προς την κινητή συσκευή γίνεται σαν να ήταν ένας σταθερός κόμβος. Στην περίπτωση που η κινητή συσκευή βρίσκεται σε ξένο δίκτυο τότε αποκτά μία CoA διεύθυνση η οποία έχει ως πρόθεμα υποδικτύου από το νέο δίκτυο. Η δρομολόγηση των πακέτων σε όλη την διάρκεια παραμονής της κινητής συσκευής στο νέο δίκτυο γίνεται μέσω αυτής της διεύθυνσης (CoA), ο home agent κρατάει πάντα την πληροφορία της CoA διεύθυνσης του ξένου δικτύου που βρίσκεται κάθε φορά η κινητή συσκευή και κάθε φορά που έρχονται πακέτα προς αυτήν ο home agent τα προωθεί στην εκάστοτε CoA διεύθυνση του. [22]

Στο πρωτόκολλο MIPv6 όπως βλέπουμε και στο σχήμα 32 δεν υπάρχει ο foreign agent αλλά μόνο ο home agent και ο correspondent node.



Σχήμα 32: Γενική εικόνα κινητικότητας με χρήση του πρωτοκόλλου MIPv6

4.2.3 Συμπεράσματα.

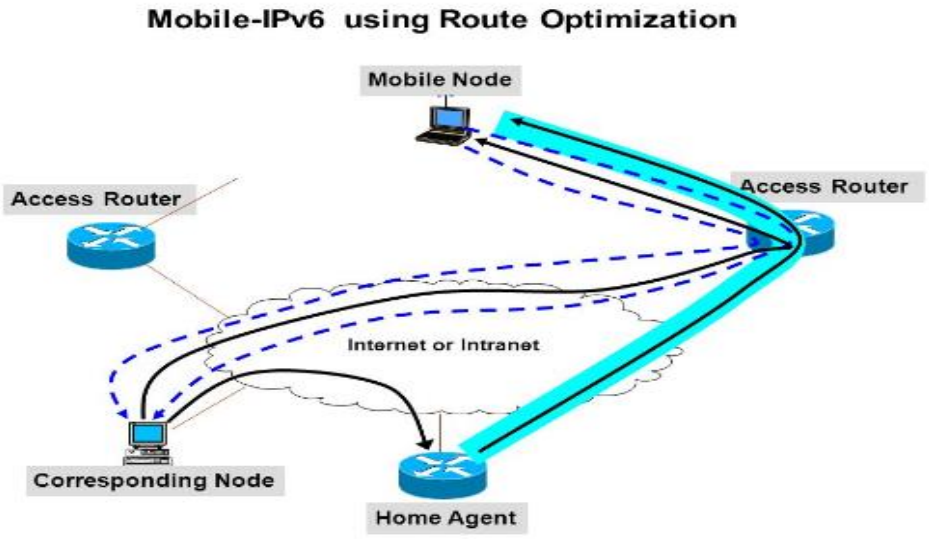
Αφού τονίστηκαν τα χαρακτηριστικά των δύο πρωτοκόλλων κινητικότητας MIPv4 και MIPv6 και παρουσιάστηκε η βασική τους λειτουργία, μπορούν να βγούν κάποια συμπεράσματα για το πιο πρωτόκολλο έχει περισσότερα πλεονεκτήματα. Λαμβάνοντας πάντα υποψίν αυτό που να αναφέρθηκε και στην αρχή του τέταρτου κεφαλαίου, δηλαδή την αύξηση των απαιτήσεων από τους χρήστες.

Αρχικά θα πρέπει να αναφερθεί ότι το πρωτόκολλο MIPv6 δεν είναι μια απλή προσθήκη στο νέο πρωτόκολλο διαδικτύου IPv6, αλλά μια εξ΄ αρχής ολοκληρωμένη λειτουργία του. Επιπλέον θα πρέπει να επισημανθεί ότι στο πρωτόκολλο MIPv6 δεν υπάρχει η ανάγκη παρουσίας των Foreign Agents όπως γίνετε στο MIPv4 , με αυτό τον τρόπο κάθε κινητή συσκευή μπορεί να λειτουργεί σε οποιοδήποτε δίκτυο χωρίς να χρειάζεται ειδική υποστήριξη προς τον τοπικό δρομολογητή. Μπορούμε να πούμε

ότι το νέο πρωτόκολλο MIPv6 προσφέρει μια ποίο “αυθεντική” λύση στο θέμα της κινητικότητας.

Στο πρωτόκολλο MIPv6 όταν μία κινητή συσκευή είναι εκτός του home δικτύου της, τα πακέτα που στέλνονται σε αυτήν την κάνουν χρήση της επικεφαλίδας δρομολόγησης (IPv6 routing header) αντί της ενθυλάκωσης IPs που χρησιμοποιεί το MIPv4 πρωτόκολλο. Όταν για παράδειγμα στο MIPv4 μία κινητή συσκευή εισέλθει σε ένα ξένο δίκτυο, ο χρόνος από εκείνη την στιγμή μέχρι να αρχίσει να λαμβάνει πακέτα μπορεί να είναι πολύ μεγάλος και αυτό εξαιτίας όλων των μηνυμάτων εγκατάστασης της σύνδεσης που πρέπει να ανταλλάξουν οι δύο συσκευές μεταξύ τους. Όπως προκύπτει, αυτή η καθυστέρηση μπορεί να διαδραματίσει αρνητικό ρόλο σε εφαρμογές που απαιτούν real time επικοινωνία όπως συμβαίνει για παράδειγμα στις VoIP(Voice over IP) επικοινωνίες.

Ακόμα θα πρέπει να αναφερθεί ότι στο πρωτόκολλο MIPv6 ο μηχανισμός βέλτιστης διαδρομής (Route optimization) όπως παρουσιάζεται και στο σχήμα 33, υποστηρίζεται εξ’ αρχής και αποτελεί βασικό κομμάτι του MIPv6 αντί για προαιρετικό όπως γίνεται στην περίπτωση που χρησιμοποιείται το MIPv4. Με αυτόν τον τρόπο τα πακέτα από και προς την κινητή συσκευή μεταφέρονται με μικρότερη καθυστέρηση και με περισσότερη αξιοπιστία, αυτοί είναι δύο κρίσιμοι παράγοντες για τις real time εφαρμογές. [23]



Σχήμα 33: Βελτιστοποίηση διαδρομής (Route optimization) στο MIPv6

Συνοψίζοντας θα πρέπει να αναφερθεί ότι όσον αφορά την κινητικότητα σε δίκτυα IP και έχοντας υπόψιν την αύξηση των απαιτήσεων των χρηστών στο cloud computing προκύπτει το συμπέρασμα ότι, τα δίκτυα που χρησιμοποιούν το πρωτόκολλο κινητικότητας MIPv4 λόγω της ανάγκης τους για ύπαρξη του Foreign Agent (FA) φαίνεται να παρουσιάζουν δυσκολία στο να είναι αποτελεσματικά

Ακόμα αξίζει να σημειωθεί ότι λόγω του πολύ μεγάλου αριθμού διευθύνσεων IP που μπορεί να υποστηρίξει το πρωτόκολλο διαδικτύου IPv6, το MIPv4 που χρησιμοποιείται σε δίκτυα IPv4 δεν θα είναι σε θέση να ανταποκριθεί στον πολύ μεγάλο αριθμό των συσκευών που θα θέλουν να είναι συνδεδεμένες συνεχώς στο διαδίκτυο.

Όπως προκύπτει οι cloud εφαρμογές που χρειάζονται συνεχή επικοινωνία με την κινητή συσκευή συνεχώς αυξάνονται οπότε οι providers θα πρέπει να είναι σε θέση να προσφέρουν δίκτυα τέτοιων απαιτήσεων και συγκεκριμένων προδιαγραφών. Το πρωτόκολλο κινητικότητας MIPv6 φαίνεται από κατασκευής του να μπορεί να ανταπεξέλθει σε αυτήν την πρόκληση.

5. Συμπεράσματα.

Οι υπηρεσίες υπολογιστικού νέφους, είτε μιλάμε για απλούς χρήστες είτε για εταιρικούς πελάτες, χρησιμοποιούνται όλο και περισσότερο από τους χρήστες. Επομένως, η έννοια της ασφάλειας και της αξιοπιστίας στην μεταφορά – αποθήκευση δεδομένων διαδραματίζει πρωταγωνιστικό ρόλο. Τα δεδομένα των χρηστών πρέπει να είναι πάντα διαθέσιμα από τους πάροχους υπηρεσιών υπολογιστικού νέφους και διασφαλισμένα όσον αφορά την ασφάλεια τους. Αυτό το ζήτημα είναι κομβικό προκειμένου το cloud computing να συνεχίσει τον πρωταγωνιστικό του ρόλο και στο μέλλον.

Η χρήση cloud computing υπηρεσιών όπως είδαμε και προηγουμένως βρίσκεται σε διαρκή αύξηση, παράλληλα όμως αυξάνεται και η χρήση του διαδικτύου και από κινητές συσκευές. Οι κινητές συσκευές χρησιμοποιούν κατά βάση εφαρμογές cloud computing και συμπερασματικά θα μπορούσε να λεχθεί ότι όσο αυξάνεται η χρήση έξυπνων κινητών συσκευών τόσο θα αυξάνεται και η χρήση cloud εφαρμογών. Όμως αυτό έχει ως αποτέλεσμα να αυξάνονται διαρκώς και οι απαιτήσεις των χρηστών οι οποίοι θέλουν οι εφαρμογές που χρησιμοποιούν να είναι αποτελεσματικές σε όλη την διάρκεια της λειτουργίας τους ανεξάρτητα από την τοπολογία του δικτύου στο οποίο βρίσκονται κάθε φορά. Επομένως, μια κινητή συσκευή μπορεί να αλλάξει πολλά και διαφορετικά δίκτυα κατά την διάρκεια της λειτουργία της με αποτέλεσμα να προκύπτει η ανάγκη για παροχή cloud υπηρεσιών με μεγάλες απαιτήσεις συντονισμένες με την κινητικότητα του χρήστη.

Τα δύο παραπάνω ζητήματα, το θέμα της ασφάλειας και το θέμα της κινητικότητας σε cloud computing περιβάλλοντα, είναι αυτά που αναλύθηκαν και στο τελευταίο κεφάλαιο της εργασίας. Τα συμπεράσματα από την σύγκριση της λειτουργίας των δύο πρωτοκόλλων διαδικτύου IPv4 και IPv6 είναι τα εξής.

Όσον αφορά την ασφάλεια, το πρωτόκολλο IPsec δημιουργήθηκε από την αρχή για να λειτουργεί με το νέο πρωτόκολλο διαδικτύου IPv6, αλλά λόγω της χαμηλής ακόμα υιοθέτησής του, προσαρμόστηκε σε δίκτυα IPv4 που ακόμα κυριαρχούν. Έτσι όπως είναι φυσικό, το IPsec δεν προσφέρει όλες τις δυνατότητες που έχει όταν εφαρμόζεται σε δίκτυα IPv4. Επίσης, ένας ακόμα παράγοντας που επηρεάζει την λειτουργία του είναι η χρησιμοποίηση του μηχανισμού NAT (Network Address Translation). Έτσι

εξάγεται το συμπέρασμα ότι ο μηχανισμός NAT δεν επιτρέπει μία end to end IPsec σύνδεση μεταξύ των δύο hosts.

Σχετικά με την κινητικότητα (mobility) σε δίκτυα IP θα πρέπει να αναφερθεί ότι το πρωτόκολλο κινητικότητας MIPv6 δεν είναι μια απλή προσθήκη στο νέο πρωτόκολλο διαδικτύου IPv6, αλλά μια εξ΄ αρχής ολοκληρωμένη λειτουργία του, ενώ το πρωτόκολλο κινητικότητας MIPv4 προστέθηκε αργότερα στα δίκτυα IPv4. Ακόμα θα πρέπει να τονιστεί ότι τα δίκτυα που χρησιμοποιούν το πρωτόκολλο κινητικότητας MIPv4 έχουν την ανάγκη ύπαρξης του Foreign Agent (FA) προκειμένου να μεταβούν χωρίς διακοπή της υπηρεσίας τους από το ένα δίκτυο στο άλλο.

Επομένως, παρατηρείται ότι σε μεγάλη κλίμακα τέτοιων δικτύων η αποτελεσματικότητά τους δεν είναι σύμφωνη με τις απαιτήσεις των χρηστών.

Επιπρόσθετα, λόγω του πολύ μεγάλου αριθμού διευθύνσεων IPs που μπορεί να υποστηρίξει το πρωτόκολλο διαδικτύου IPv6, το MIPv4 που χρησιμοποιεί το πρωτόκολλο δικτύου IPv4 δεν θα μπορέσει να ανταποκριθεί στον πολύ μεγάλο αριθμό των κινητών και όχι μόνο συσκευών, που μπορεί να είναι συνδεδεμένες συνεχώς στο διαδίκτυο με αποτέλεσμα η διαχείριση τους μέσα από μηχανισμούς NAT στο MIPv4 να μην είναι η κατάλληλη.

Τέλος, στο πρωτόκολλο MIPv6 ο μηχανισμός βέλτιστης διαδρομής (Route optimization) υποστηρίζεται εξ’ αρχής και αποτελεί βασικό κομμάτι του MIPv6 αντί για προαιρετικό στην περίπτωση που χρησιμοποιούμε το MIPv4. Με αυτόν τον τρόπο τα πακέτα από και προς την κινητή συσκευή μεταφέρονται με μικρότερη καθυστέρηση και με περισσότερη αξιοπιστία, το οποίο όπως ειπώθηκε και στην αρχή της εργασίας είναι το ζητούμενο.

6. Βιβλιογραφία.

[1] ekke.gr, "Το διαδίκτυο στην Ελλάδα τελική έκθεση 2017" http://ekke.gr/siemens/WIPreport_%20gr_2017.pdf

[2] economist.com, "Cloud computing The sky's limit" 2015. - https://www.economist.com/leaders/2015/10/17/the-skys-limit

[3] epset.gr, "Υπολογιστικό Νέφος" - http://www.epset.gr/el/content/ypologistiko-nefos-cloud-computing

[4] Marinescu, Dan C, "Cloud Computing Theory and Practice" 2013.

[5] internetworldstats.com, "Internet users in the world by regios" 2017. - https://www.internetworldstats.com/stats.htm

[6] google.com, "IPv6 Adoption from 2008-2018" - https://www.google.com/intl/en/ipv6/statistics.html

[7] Michael J. Kavis, "Architecting the Cloud Design Decisions for Cloud Computing Service Models" 2014.

[8] Adeel Ahmed, Salman Asadullah, "Deploying IPv6 in Broadband Access Networks" 2009.

[9] cisco.com, "Implementing IPsec in IPv6 Security" – https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-15-2s-book/ip6-ipsec.html

[10] ieeexplore.ieee.org, "Simultaneous mobility in MIPv6" - https://ieeexplore.ieee.org/document/1626976

[11] ibm.com, "Comparison of IPv4 and IPv6" - https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.hale001/ipv6d0011006452.htm

[12] ipv6-es.com, "Transition Mechanisms Overview" - http://www.ipv6-es.com/02/docs/david_fernandez_2.pdf

[13] R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", The Internet Society, 2005.

[14] cisco.com, "IPv6 Automatic 6to4 Tunnels" - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-6to4-tunls-xe.pdf

[15] Michael Armbrust, "Above the Clouds: A Berkeley View of Cloud

Computing" ,UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.

[16] wikipedia.org, "Temporal isolation among virtual machines" - https://en.wikipedia.org/wiki/Temporal_isolation_among_virtual_machines

[17] Gerald J. Popek and Robert P. Goldberg, “Formal Requirements for Virtualizable Third Generation Architectures” 2014 - https://pdfs.semanticscholar.org/d800/009a27fbc8da40095f9ab59ef72441c654bb.pdf

[18] wikipedia.org, “Network address translation (NAT)” - https://en.wikipedia.org/wiki/Network_address_translation

[19] Sabrina De Capitani di Vimercati, Ray Indrakshi, Indrajit Ray , “Data and Applications Security”, Kluwer Academic Publishers, 2004.

[20] Catherine Paquet, “Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide”, Cisco Press, 2nd Edition, 2013.

[21] Jie Li; Hsiao-Hwa Chen, "Mobility support for IP-Based networks", IEEE, 2005.

[22] Perkins, C.E. and Johnson, D.B. , ‘‘Mobility support in IPv6’’, The Internet Society 2004.

[23] R. Koodli, “Mobile IPv6 Fast Handovers”, IETF Trust, 2009.

[24] tools.ietf.org, “Framework for IPv4/IPv6 Translation”-https://tools.ietf.org/html/rfc6144

[25] catarina.udlap.mx, SIT("Simple Internet Transition")- http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/aldrette_m_a/capitulo4.pdf

[26] cloudsecurityalliance.org, “New Software Defined Perimeter for Iaas” - https://cloudsecurityalliance.org/articles/cloud-security-alliance-releases-new-software-defined-perimeter-for-infrastructure-as-a-service-research/

[27] en.wikipedia.org, “Hypervisor” - https://en.wikipedia.org/wiki/Hypervisor