ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«IP BONDING ΚΑΙ ΕΦΑΡΜΟΓΕΣ»

ΑΓΓΕΛΟΥΔΗΣ Δ. ΑΓΓΕΛΟΣ-ΑΓΓΕΛΟΥΣΗΣ Θ. ΞΕΝΟΦΩΝΤΑΣ

Επιβλέπων: Παναγιώτης Γ. Κωττής

Καθηγητής Ε.Μ.Π

Αθήνα, Ιανουάριος 2020

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«IP BONDING ΚΑΙ ΕΦΑΡΜΟΓΕΣ»

ΑΓΓΕΛΟΥΣΗΣ Θ. ΞΕΝΟΦΩΝΤΑΣ-ΑΓΓΕΛΟΥΔΗΣ Δ. ΑΓΓΕΛΟΣ

Επιβλέπων: Παναγιώτης Γ. Κωττής

Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29η Ιανουαρίου 2020

.....	.....	.....
Π. Κωττής	**Χ. Καψάλης**	**Γ. Φικιώρης**
Καθηγητής Ε.Μ.Π.	**Καθηγητής Ε.Μ.Π.**	**Καθηγητής Ε.Μ.Π.**

Αθήνα, Ιανουάριος 2020

.....Άγγελος Δ. Αγγελούδης Διπλωματούχος Ηλεκτρολόγος Μηχανικός & Μηχανικός Υπολογιστών Ε.Μ.Π

..... Ξενοφώντας Θ. Αγγελούσης Διπλωματούχος Ηλεκτρολόγος Μηχανικός & Μηχανικός Υπολογιστών Ε.Μ.Π

ΠΕΡΙΛΗΨΗ:

Στα πλαίσια αυτής της εργασίας επικεντρώσαμε το ενδιαφέρον μας σε μία νέα τεχνολογία ταυτόχρονης μετάδοσης πακέτων στα δίκτυα επικοινωνιών: το Internet Bonding.

Στο πρώτο κεφάλαιο ασχοληθήκαμε με τις γενικές έννοιες της ευρυζωνικότητας και της τεχνολογίας του x-DSL καθώς και τις υπηρεσίες εφαρμογές που εξυπηρετούν. Στο δεύτερο κεφάλαιο δώσαμε μεγάλη σημασία στην έννοια του bonding στα δίκτυα και κατά πόσο μπορεί να επιταχύνει τη διεκπεραιωτική ικανότητά τους εξισορροπώντας το φορτίο τους. Το τρίτο κεφάλαιο της παρούσας διπλωματικής εργασίας είναι αφιερωμένο στα πρωτόκολλα ασφαλείας που διέπουν τα δίκτυα υπολογιστών. Γι' αυτό το λόγο γίνεται μία αναδρομή στο IPsec, στο SSH και στο SSL και παρουσιάζονται κάποια παραδείγματα όπως το Cisco NetSonar και το Cisco NetRanger. Τέλος, το κεφάλαιο 4 εστιάζει στις εμπορικές εφαρμογές της ευρυζωνικής τεχνολογίας και ειδικότερα του Internet Bonding.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Internet Bonding, Ευρυζωνικότητα, Ασφάλεια Δικτύου, Τεχνολογίες x-DSL.

ABSTRACT:

In the context of this work, we focused on a new technology of simultaneous transmission of packages in communication communications: Internet Bonding.

In the first chapter we deal with the broad concepts of broadband and x-DSL technology as well as the service applications they serve. In the second chapter, importance was given to the meaning of network interconnection and whether it can accelerate their dispatching capacity by exposing their load.

The third chapter of this diploma thesis is devoted to the security protocols governing computational infrastructures. That's why we take a look at IPsec, SSH, and SSL and showcase examples such as Cisco NetSonar and Cisco NetRanger.

Finally, Chapter 4 focuses on commercial applications of broadband technology, particularly Internet Bonding.

KEY WORDS: Internet Bonding, Broadband, Network Security, x-DSL Technologies.

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα καθηγητή της διπλωματικής μας εργασίας κ. Παναγιώτη Γ. Κωττή για την ευκαιρία που μας έδωσε να ασχοληθούμε με ένα τόσο ενδιαφέρον θέμα. Η καθοδήγησή του, οι επισημάνσεις και οι διορθώσεις του συνέβαλαν καθοριστικά στο τελικό αποτέλεσμα.

ΠΕΡΙΕΧΟΜΕΝΑ:

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή-Ευρυζωνικότητα

1.1 Γενικά

Στη σύγχρονη κοινωνία, το οικονομικό, βιομηχανικό, τεχνολογικό και πολιτιστικό περιβάλλον καθώς και οι συνθήκες ζωής μεταβάλλονται ραγδαία. Η άνθιση της τεχνολογίας και των εφαρμογών της είναι τεράστια ενώ παράλληλα οι απαιτήσεις και οι ανάγκες των πολιτών αλλά και των ίδιων των κρατών για παροχή προηγμένων υπηρεσιών ολοένα αυξάνουν. Στο σημερινό περιβάλλον υψηλής τεχνολογίας, η βάση πάνω στην οποία θα θεμελιωθεί η ανταγωνιστικότητα και η ανάπτυξη ενός κράτους ή και μιας περιφέρειας αποτελείται σε μεγάλο βαθμό από προηγμένες δικτυακές υποδομές υψηλής ποιότητας, ορθολογικά κοστολογημένες. Τα δίκτυα «ευρυζωνικής πρόσβασης» μπορούν να καλύψουν από τεχνολογικής σκοπιάς αυτές τις σύγχρονες απαιτήσεις και η ταχεία ανάπτυξή τους αποτελεί για όλα τα αναπτυγμένα και αρκετά αναπτυσσόμενα κράτη, σημαντικό στρατηγικό στόχο.

Οι τηλεπικοινωνίες επέτρεψαν να αναδυθεί ένας εικονικός κόσμος στον οποίο ο χρόνος και η απόσταση δεν αποτελούν εμπόδιο στην επικοινωνία. Οι μεγάλες συντελούμενες αλλαγές στον τομέα των τηλεπικοινωνιών έχουν επηρεάσει τη καθημερινή ζωή σε όλα τα επίπεδα. Έχουν σημαντικές επιπτώσεις στον τρόπο που εργάζονται οι άνθρωποι, οργανώνονται οι επιχειρήσεις, και γίνονται οι εμπορικές συναλλαγές. Η ταχεία εισδοχή νέων τεχνολογιών και υπηρεσιών και ο μεγάλος ανταγωνισμός στην τηλεπικοινωνιακή αγορά δημιουργούν μεγάλες ευκαιρίες στον επιχειρηματικό και όχι μόνο τομέα να αναβαθμίσει την υποδομή του και να αυξήσει την ανταγωνιστικότητα του με όρους πλέον οικονομικά σύμφορους οδηγώντας έτσι την αντίστοιχη αγορά και ζητώντας όλο και περισσότερο αναβαθμισμένες υπηρεσίες. Το internet είναι απαραίτητο εργαλείο στους περισσότερους τομείς της καθημερινής επιχειρηματικής αλλά και προσωπικής ζωής. Οι προηγμένες δικτυακές υποδομές υψηλής ποιότητας προσφέρουν επαρκείς ρυθμούς μετάδοσης και αδιάλειπτη λειτουργία στους χρήστες καθώς και εύκολη δυνατότητα πρόσβασης για την πλειοψηφία του πληθυσμού. Οι απαιτήσεις αυτές, από τεχνολογική σκοπιά, καλύπτονται από τα δίκτυα ευρυζωνικής πρόσβασης.

Με τον όρο ευρυζωνικότητα ορίζεται η προσιτή, αξιόπιστη, γρήγορη και συνεχής σύνδεση Internet που φέρνει γρήγορη πρόσβαση στο διαδίκτυο, ραδιόφωνο,

τηλεόραση, ταινίες, παιχνίδια, VoIP (Voice over Internet Protocol), τηλεδιάσκεψη, εργασία – μάθηση - ιατρική φροντίδα. Ειδικότερα, η ευρυζωνικότητα :

α) δίνει δυνατότητες αδιάλειπτης παροχής γρήγορων συνδέσεων στο Διαδίκτυο σε όσο το δυνατόν μεγαλύτερο μέρος του πληθυσμού σε ανταγωνιστικές τιμές χωρίς εγγενείς περιορισμούς στα συστήματα μετάδοσης και τον τερματικό εξοπλισμό των επικοινωνούντων άκρων με διαφάνεια και δυνατότητα επιλογής μέσα από ένα ευρύ φάσμα προσφορών σύνδεσης και εφαρμογών ανάλογα με τις ανάγκες που επιθυμεί ο κάθε πολίτης να καλύψει

β) αποτελείται από την κατάλληλη δικτυακή υποδομή που :

- επιτρέπει την κατανεμημένη ανάπτυξη υπαρχόντων και μελλοντικών δικτυακών εφαρμογών και πληροφοριακών υπηρεσιών,

- ικανοποιεί τις εκάστοτε ανάγκες των εφαρμογών σε εύρος ζώνης και διαθεσιμότητα, και

- είναι ικανή να αναβαθμίζεται συνεχώς και με μικρό επιπλέον κόστος ώστε να εξακολουθεί να ικανοποιεί τις ανάγκες όπως αυτές αυξάνουν και μετεξελίσσονται με ρυθμό και κόστος που επιτάσσονται από την πρόοδο της πληροφορικής και της τεχνολογίας επικοινωνιών

γ) δίνει την δυνατότητα στον πολίτη να επιλέγει:

- ανάμεσα σε εναλλακτικές προσφορές σύνδεσης που ταιριάζουν στον εξοπλισμό του,

- μεταξύ διαφόρων δικτυακών εφαρμογών και

- μεταξύ διαφόρων υπηρεσιών πληροφόρησης και ψυχαγωγίας χωρίς να αποκλείεται και η συμμετοχή του ίδιου στην παροχή περιεχομένου, εφαρμογών και υπηρεσιών

δ) αποτελείται από το κατάλληλο ρυθμιστικό πλαίσιο από πολιτικές, μέτρα, πρωτοβουλίες, άμεσες και έμμεσες παρεμβάσεις, αναγκαίες για την ενδυνάμωση των νέων τεχνολογιών, την προστασία του ανταγωνισμού και την εγγύηση σοβαρής και

ισορροπημένης οικονομικής ανάπτυξης, ικανής να προκύψει από τη γενικευμένη συμμετοχή στην Ευρυζωνικότητα και την Κοινωνία της Πληροφορίας.

Η ανάπτυξη των τηλεπικοινωνιών μέχρι σήμερα προσαρμοζόταν στις ανάγκες και στις απαιτήσεις που διαχρονικά υπήρχαν. Οι κύριοι παράγοντες που συνέβαλαν αποφασιστικά στην εξέλιξη των ευρυζωνικών τεχνολογιών είναι :

- Η ανάγκη για υψηλότερους ρυθμούς μετάδοσης για την υποστήριξη σύγχρονων εφαρμογών πολυμέσων που συνδυάζουν κλασικές υπηρεσίες με κινούμενη εικόνα (διαδραστική τηλεόραση, τηλεδιάσκεψη, βίντεο κατ' απαίτηση, κ.α.).

- Η τάση υλοποίησης όλων των μορφών υπηρεσιών μετάδοσης (συμμετρικές, ασύμμετρες, πολύ υψηλών ταχυτήτων κλπ.) πάνω από την υπάρχουσα υποδομή των δισύρματων χάλκινων καλωδίων.

- Η ανάγκη για υποστήριξη μεγαλύτερων αποστάσεων μεταξύ συνδρομητών και τηλεφωνικών κέντρων, ώστε να καταστεί δυνατή η προσφορά της ίδιας υπηρεσίας σε όλους τους συνδρομητές.

1.2 Ιστορική Εξέλιξη

Μέχρι πριν από κάποια χρόνια ο τρόπος μεταφοράς σήματος μέσω των τηλεφωνικών γραμμών ήταν αναλογικός. Κατά την επικοινωνία μας με κάποιον η φωνή μετατρεπόταν από το τηλέφωνο σε ηλεκτρικά σήματα και από την άλλη πλευρά τα ηλεκτρικά αυτά σήματα δονούσαν το ηχείο του ακουστικού του συνομιλητή. Καθώς το σήμα περνούσε μέσα από τα τηλεφωνικά κέντρα, οι συχνότητες που βρίσκονταν εκτός του φάσματος της ανθρώπινης φωνής, "κόβονταν", ώστε να μην υπάρχουν παράσιτα. Αυτός είναι και ο λόγος για τον οποίο τα modems στους υπολογιστές, δεν μπορούσαν να προσφέρουν αρκετά υψηλές ταχύτητες.

Το πρόβλημα αυτό ήρθε αρχικά να διορθώσει η τεχνολογία ISDN (Integrated Services Digital Network), που είχε ως αποτέλεσμα την επίτευξη λίγο υψηλότερων ταχυτήτων. Το ISDN, όμως, προσέφερε μέγιστη ταχύτητα μετάδοσης τα 128Kbps και ως εκ τούτου πλέον δεν ήταν αρκετή για τις ανάγκες μετάδοσης τηλεπικοινωνιακών υπηρεσιών, ακόμα και απλών υπηρεσιών διαδικτύου (Internet Services).

Εδώ και λίγα χρόνια παρατηρείται η συνεχώς αυξανόμενη ζήτηση για όλο και περισσότερη χωρητικότητα μετάδοσης που οδήγησε στην εποχή της ευρυζωνικότητας. Τη ζήτηση αυτή ήρθε, μεταξύ άλλων, να καλύψει η τεχνολογία Ψηφιακής Γραμμής Συνδρομητή (Digital Subscriber Line- DSL) με τις ποικίλες παραλλαγές της.

Το ISDN λοιπόν αποτέλεσε τον πρόδρομο του DSL και αυτό έγινε για δύο βασικούς λόγους:

α) Ήταν η πρώτη τεχνολογία που εκμεταλλεύτηκε μεγαλύτερο τμήμα του διαθέσιμου φάσματος στο χάλκινο καλώδιο του συνδρομητικού βρόχου σε σχέση με την αναλογική τηλεφωνία.

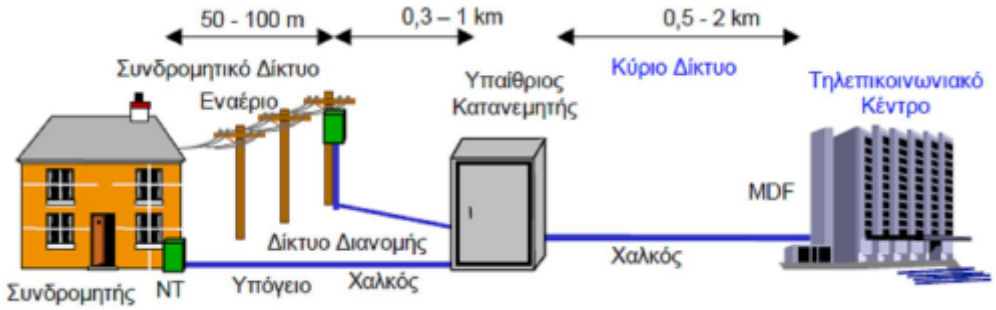
β) Στηρίζεται σε έναν ψηφιακό κώδικα μετάδοσης πληροφορίας (2B1Q) που χρησιμοποιείται και σήμερα σε κάποιες παραλλαγές της τεχνολογίας DSL.

Η ιστορική εξέλιξη της εμφάνισης της ευρυζωνικότητας έχει ως εξής: Το 1985 η Bell Labs ανακαλύπτει ένα νέο τρόπο για να κάνει τα παραδοσιακά χάλκινα καλώδια να υποστηρίξουν νέες ψηφιακές υπηρεσίες. Το 1988 γίνονται οι πρώτες εγκαταστάσεις του DSL στην Αμερική αλλά ήδη έχει αρχίσει να φαίνεται πως σύντομα η τεχνολογία αυτή θα υπερκεράσει το ISDN, το οποίο υστερεί σημαντικά σε ταχύτητα. Το 1990 κάποιες τηλεφωνικές εταιρείες ξεκινούν να υλοποιούν High-Speed DSL (HDSL) για να παρέχουν συμμετρική υπηρεσία (~1,5Mbps) πάνω σε καλώδια χαλκού, αρχικά μεταξύ μικρών τηλεφωνικών κέντρων. Οι τηλεφωνικές εταιρείες ξεκινούν να προωθούν το HDSL σε μικρές εταιρείες και το νεοεμφανιζόμενο ADSL προς οικιακούς χρήστες για διαδικτυακή πρόσβαση. Το 1993 αξιολογούνται και προτυποποιούνται οι τρεις κύριες τεχνοτροπίες του ADSL. Το 1995 οι εταιρείες ανάπτυξης νέων τεχνολογιών αρχίζουν να βλέπουν το ADSL ως το μέσο για να ικανοποιηθεί η ανάγκη για γρήγορο Internet («Fast Internet»), και ξεκινούν να δουλεύουν πάνω στο έργο αυτό. Από το 1999 και μετά πλέον αρχίζουν σιγά σιγά να εμφανίζονται, με πρώτες τις UADSL (ITU-T G.992.2 “G.lite”) και ADSL full (ITU-T G.992.2 “G.full”), οι διάφορες τεχνολογίες DSL στις οποίες θα γίνει αναφορά σε επόμενες ενότητες. Η ανάπτυξη ευρυζωνικών δικτύων έχει υιοθετηθεί σήμερα από την κοινή Ευρωπαϊκή πολιτική για την υλοποίηση της Κοινωνίας της Πληροφορίας και πολλά είναι τα κράτη τα οποία έχουν τοποθετήσει τα έργα υλοποίησης τέτοιων υποδομών ως βασικό στρατηγικό τους στόχο.

Οι ευρυζωνικές τεχνολογίες βασίζονται τόσο στο υπάρχον τηλεπικοινωνιακό δίκτυο, και κυρίως στο δίκτυο πρόσβασης όπως αναλύεται στο παρακάτω κεφάλαιο, όσο και σε νέες υποδομές οι οποίες υποστηρίζουν καλύτερα τις υπηρεσίες και τις ταχύτητες που προσφέρονται από τις DSL συνδέσεις.

1.3 Δομή Παραδοσιακού Δικτύου Πρόσβασης

Όλες οι χώρες διαθέτουν τηλεπικοινωνιακό δίκτυο έτσι ώστε να μπορούν να καλύψουν την ιδιαίτερα αυξημένη ανάγκη για επικοινωνία σε όλους τους τομείς της ζωής. Το δίκτυο κάθε τηλεπικοινωνιακού οργανισμού είναι ιδιαίτερα πολύπλοκο. Στην εν λόγω Διπλωματική εργασία θα γίνει αναφορά μόνο στο μέρος του δικτύου που ονομάζεται δίκτυο πρόσβασης. Σύμφωνα με τον Ευρωπαϊκό Οργανισμό Τηλεπικοινωνιακής Τυποποίησης (ETSI), ως δίκτυο πρόσβασης (access network) ορίζεται το μέρος του δικτύου, που ξεκινά από το αστικό κέντρο (κτίριο Ο.Τ.Ε.) και φθάνει μέχρι το συνδρομητή. Εναλλακτικά χρησιμοποιούνται και οι όροι τοπικός βρόχος (ToB), βρόχος χαλκού και τελευταίο μίλι (Local Loop, Copper Loop, Last Mile). Δίκτυο πρόσβασης είναι δηλαδή, το τελευταίο κομμάτι ενός τηλεπικοινωνιακού δικτύου το οποίο συνδέει το συνδρομητή στο πρώτο σημείο συγκέντρωσης.



Σχήμα 1.1: Το «κλασικό» δίκτυο πρόσβασης

Σε κάθε Τερματικό Κέντρο (Τ/Κ) στους υπόγειους χώρους υπάρχει ο κεντρικός κατανεμητής. Ο κεντρικός κατανεμητής είναι ένα κουτί από το οποίο ξεκινούν τα καλώδια (χάλκινα καλώδια ζευγών ή τετράδων αγωγών, συνεστραμμένα ζεύγη - twisted pairs), τα οποία κατανέμονται σε όλη την περιοχή κάλυψης και καταλήγουν στους υπαίθριους κατανεμητές.

Το κομμάτι του δικτύου πρόσβασης από το Τ/Κ μέχρι τον υπαίθριο κατανεμητή ονομάζεται Κύριο Δίκτυο. Η απόσταση από τον κεντρικό κατανεμητή ως τον υπαίθριο κατανεμητή μπορεί να είναι από 0,5 ως 2 χλμ. και τα καλώδια είναι μεγαλύτερης χωρητικότητας (400 έως 2400 ζευγών κατά μέσο όρο). Ο υπαίθριος κατανεμητής (ΚΚ) είναι ένα κουτί στο οποίο εισέρχονται τα καλώδια του κυρίου δικτύου και εξέρχονται άλλα καλώδια (μικρότερης χωρητικότητας από 10 έως 200 ζεύγη) σε δενδρική διάταξη, που φθάνουν μέχρι το κουτί τερματισμού (τερματική διάταξη) του δικτύου σε εσωτερικό (εισαγωγή) ή εξωτερικό χώρο του κτιρίου του συνδρομητή ή πάνω σε στύλο, κοντά στο κτίριο του συνδρομητή. Το κουτί τερματισμού είναι ένα μικρό κουτί που βρίσκεται έξω από τα σπίτια. Από αυτό το κουτί διανέμονται οι τηλεφωνικές γραμμές σε κάθε κατοικία ξεχωριστά (συνδρομητικό δίκτυο). Το τμήμα του δικτύου από τον υπαίθριο κατανεμητή ως την τερματική διάταξη ονομάζεται δίκτυο διανομής και είναι από 0,3 ως 1 χλμ. ενώ το τμήμα από το κουτί ως το συνδρομητή ονομάζεται συνδρομητικό δίκτυο. Το δίκτυο πρόσβασης έχει σχεδιασθεί για την εξυπηρέτηση της φωνητικής τηλεφωνίας (POTS). Με την ανάπτυξη όμως της ευρυζωνικότητας, χρησιμοποιείται και για τη μετάδοση δεδομένων (data). Η μόνη διαφορά είναι ότι στο χώρο του πελάτη εγκαθίσταται ένας διαχωριστής (splitter) που διαχωρίζει τα δεδομένα από τις τηλεφωνικές κλήσεις. Η τηλεφωνική κλήση δρομολογείται στο τηλέφωνο και τα δεδομένα δρομολογούνται στο modem που αποτελεί έναν ψηφιακό επεξεργαστή σήματος. Ο υπολογιστής συνδέεται με το μόντεμ με σύνδεση υψηλής ταχύτητας που επιτυγχάνεται τοποθετώντας μία κάρτα Ethernet στον υπολογιστή και δημιουργώντας ένα μικρό δίκτυο δύο κόμβων. Στο άλλο άκρο του συστήματος, στο τερματικό κέντρο, εγκαθίσταται επίσης ένας διαχωριστής που διαχωρίζει το φωνητικό σήμα από το σήμα δεδομένων. Το φωνητικό σήμα δρομολογείται στον μεταγωγέα φωνής (PSTN) και το σήμα δεδομένων δρομολογείται στην συσκευή Πολύπλεκτης Προσπέλασης Ψηφιακής Συνδρομητικής Γραμμής (DSLAM), η οποία περιέχει το ίδιο είδος ψηφιακού επεξεργαστή με το modem. Ο πολυπλέκτης DSLAM, ο οποίος ενσωματώνει ένα μεγάλο αριθμό από DSL modems (κάρτες και θύρες), συγκεντρώνει την ροή των δεδομένων πολλών DSL συνδέσεων σε ένα ευρυζωνικό δίκτυο κορμού.

1.4 Υποδομές Ευρυζωνικών Δικτύων

Οι τεχνολογίες που μπορούν να εξασφαλίσουν ευρυζωνική σύνδεση στον καταναλωτή είναι πολλές. Η διαφοροποίηση τους έγκειται γενικά στον τρόπο διασύνδεσης του Η/Υ με το υπόλοιπο δίκτυο. Σε ανώτερο επίπεδο χωρίζονται σε δύο βασικές κατηγορίες :

• Ενσύρματες: Όπου η σύνδεση εξασφαλίζεται μέσω καλωδίου (τηλεφωνικό δίκτυο, δίκτυα καλωδιακής τηλεόρασης, δίκτυα οπτικών ινών, δίκτυα παροχής ηλεκτρικού ρεύματος κ.α.)

• Ασύρματες: Όπου η σύνδεση εξασφαλίζεται μέσω εκπομπής / λήψης σημάτων στον αέρα (δίκτυα κινητής τηλεφωνίας, δορυφορικά δίκτυα, ασύρματα δίκτυα κατά το πρότυπο IEEE802.11, WiMax, Wi-fi, 3G/UMTS).

Το ενσύρματο δίκτυο πρόσβασης, που περιγράφηκε παραπάνω, μπορεί να αποτελείται είτε από καλώδια χαλκού με μετάδοση ηλεκτρικού ρεύματος είτε από ινοοπτικά καλώδια με μετάδοση παλμών φωτός. Τα καλώδια χαλκού μπορεί να είναι καλώδια συνεστραμμένων ζευγών (twisted wires) ή ομοαξονικά καλώδια. Τα καλώδια συνεστραμμένων ζευγών είναι τα γνωστά χάλκινα σύρματα των τηλεφωνικών γραμμών. Αποτελούνται από τέσσερις ή περισσότερους χάλκινους αγωγούς συστρεμμένους σε ζεύγη (ένα για τη γείωση κι ένα για τη μεταφορά του σήματος). Συνήθως, με το ένα ζεύγος γίνεται η αποστολή και με το άλλο η λήψη. Οι ταχύτητες μετάδοσης είναι από 300 bits / sec ως 10 Mbits / sec. Στα ομοαξονικά καλώδια (coaxial cables), οι (δύο) αγωγοί είναι τοποθετημένοι ό ένας μέσα στον άλλο και χωρίζονται μεταξύ τους από ένα μονωτικό υλικό. Με τον τρόπο αυτό επιτυγχάνονται μεγαλύτερες ταχύτητες μετάδοσης (56 kbits /sec - 200 Mbits / sec). Οι οπτικές ίνες χρησιμοποιούνται για την υλοποίηση ευρυζωνικών δικτύων. Αυτό συμβαίνει διότι είναι η μόνη τεχνολογία η οποία έχει τη δυνατότητα να υποστηρίξει τη συγκέντρωση ευρυζωνικών συνδέσεων πρόσβασης και να μεταφέρει με υψηλό ρυθμό μεγάλες ποσότητες δεδομένων από κεντρικά σημεία διανομής προς τους συνδρομητές. Οι οπτικές ίνες παρέχουν μεγάλο εύρος ζώνης, το οποίο σήμερα φθάνει στις ευρέως χρησιμοποιούμενες υλοποιήσεις όπως το Gigabit Ethernet μέχρι και τα 10 Gbps. Η απόσταση κυμαίνεται μεταξύ 70-100 Km ανάλογα με τον τύπο της οπτικής ίνας και το σήμα που μεταφέρεται.

Ακόμη περιορίζεται ο αριθμός των ενδιάμεσων ενισχύσεων που απαιτούνται για να διασχίσει το σήμα μια μεγάλη απόσταση, έχοντας ταυτόχρονα σημαντική ανοχή στον θόρυβο. Οι οπτικές ίνες μπορούν να χρησιμοποιηθούν σε τοπικά δίκτυα αλλά και για μεταδόσεις σε μεγάλες αποστάσεις (δίκτυα ευρείας περιοχής). Έχουν στο κέντρο τους τον πυρήνα μέσω του οποίου μεταδίδεται το οπτικό σήμα. Ο πυρήνας εγκλωβίζει τις ακτίνες φωτός και τις οδηγεί στο τέρμα. Αποτελούνται από εύκαμπτες ίνες (νήματακαλώδια) από πλαστική ύλη ή γυαλί, μέσω των οποίων διέρχονται ακτίνες φωτός ή laser. Αποτελούν το ταχύτερο, ασφαλέστερο αλλά και το πιο δαπανηρό μέσο μετάδοσης.

Ανάλογα με το που τερματίζεται η οπτική ίνα έχουμε τις εξής περιπτώσεις:

⎪ FTTH (Fiber to the Home): Η οπτική ίνα φτάνει μέχρι τον τελικό χρήστη.

⎪ FTTB (Fiber to the Building): Η οπτική ίνα φτάνει μέχρι το κτήριο, ενώ μέσα σ' αυτό η διασύνδεση συνεχίζεται με συνεστραμμένα ζεύγη χαλκού.

⎪ FTTC (Fiber to the Curb): Η οπτική ίνα φτάνει μέχρι τους κατανεμητές και μετά η σύνδεση συνεχίζεται με καλώδια χαλκού.

Τα πλεονεκτήματα των οπτικών ινών είναι ότι έχουν μεγάλη χωρητικότητα (της τάξης των Gbps) ενώ λόγω του υλικού κατασκευής τους, συμπεριφέρονται σαν καθρέπτες χωρίς απώλειες. Η χαμηλή εξασθένιση στις οπτικές ίνες οφείλεται στην υψηλή διαύγεια του υλικού. Λόγω της εξαιρετικά καλής μόνωσης οι οπτικές ίνες είναι απρόσβλητες από περιβαλλοντικές παρεμβολές που προκαλούν εξασθένιση του σήματος και δεν υπάρχει παρεμβολή στο σήμα λόγω περιβαλλοντικών μαγνητικών πεδίων. Επειδή η οπτική ίνα δεν μεταφέρει ηλεκτρικό σήμα, προτιμάται σε περιοχές υψηλού κίνδυνου εκρήξεων από σπινθήρες π.χ. σε χώρους καυσίμων, εύφλεκτων αερίων κλπ. και δεν είναι ευαίσθητες σε υγρό περιβάλλον, όπου τα χάλκινα καλώδια μπορεί να δημιουργήσουν βραχυκυκλώματα. Όμως παράλληλα, παρατηρείται δυσκολία υλοποίησης συνδέσεων, επειδή απαιτείται υψηλή προσαρμογή και ευθυγράμμιση της φωτεινής πηγής, για να μην υπάρχει διασπορά και για να ελαχιστοποιηθούν οι απώλειες. Όσον αφορά στο ασύρματο δίκτυο, πρόκειται για υπηρεσίες broadband που στηρίζονται στη χρήση δορυφόρου (Satellite Internet), δικτύων ασύρματης σταθερής πρόσβασης (LMDS), δικτύων κινητής τηλεφωνίας τρίτης γενιάς ή των νέων ασύρματων τεχνολογιών που έχουν κάνει την εμφάνισή τους

το τελευταίο διάστημα με προεξάρχουσες τις τεχνολογίες Wi-Fi και WiMax. Κάθε μια από τις προαναφερθείσες τεχνολογίες έχει τα δικά της πλεονεκτήματα και μειονεκτήματα, τα οποία σχετίζονται με την απόδοση, την τιμή και την ποιότητα των υπηρεσιών, αλλά κυρίως με την γεωγραφία του χώρου, την ευχρηστία και τη λειτουργικότητα της υπηρεσίας εντός αυτού και άλλους σημαντικούς πολιτισμικούς και πολιτικούς παράγοντες.

1.5 Τεχνολογία x-DSL

Το DSL προέρχεται από τα αρχικά των λέξεων Digital Subscriber Line και αποτελεί μια τεχνολογία που μετατρέπει το απλό τηλεφωνικό καλώδιο σε ένα δίαυλο ψηφιακής επικοινωνίας μεγάλου εύρους ζώνης με τη χρήση ειδικών modems, τα οποία τοποθετούνται στις δυο άκρες της γραμμής. Ο δίαυλος αυτός μεταφέρει τόσο τις χαμηλές όσο και τις υψηλές συχνότητες ταυτόχρονα (τις χαμηλές για τη μεταφορά του σήματος της φωνής και τις υψηλές για τα δεδομένα). Η τεχνολογία DSL χρησιμοποιεί την τηλεφωνική εγκατάσταση των χάλκινων καλωδίων για τη μεταφορά δεδομένων σε σπίτια και επιχειρήσεις. Αξιοποιεί στο έπακρο τις δυνατότητες των καλωδίων αυτών και εγγυάται δικτυακές συνδέσεις υψηλών ταχυτήτων τόσο για οικιακούς χρήστες όσο και για επιχειρήσεις που δεν χρησιμοποιούν την τεχνολογία των καλωδίων οπτικών ινών.

Έτσι, η επικοινωνία γίνεται εξ ολοκλήρου ψηφιακά, επιτρέποντας τη χρήση μεγαλύτερου εύρους ζώνης για τη μεταφορά των δεδομένων, με αποτέλεσμα την επίτευξη πολύ υψηλότερων ταχυτήτων επιτρέποντας ταυτόχρονα τη χρήση ενός μέρους του εύρους για τη μεταφορά αναλογικού σήματος (φωνής). Η ταχύτητα μεταφοράς είναι τεράστια και μπορεί να φτάσει τα 52,8Mbps από το Internet (downstream) προς το χρήστη και τα 2,5Mbps από το χρήστη (upstream) προς το Internet. Η DSL τεχνολογία προσφέρει συνεχή σύνδεση με το Internet, ο χρήστης δηλαδή δεν χρειάζεται να καλεί κάθε φορά κάποιον αριθμό αφού ο υπολογιστής είναι μόνιμα συνδεδεμένος στο δίκτυο, ενώ ταυτόχρονα δίνει ταχύτητες επαρκείς για τη μεταφορά εικόνας, επιπέδου τηλεοπτικής εκπομπής. Η DSL όμως, όπως προαναφέρθηκε, έχει μια μεγάλη δέσμευση: την απόσταση. Σε αντίθεση με την ISDN σύνδεση ή τα αναλογικά modems, έχει σαφή περιορισμό στο επιτρεπόμενο μήκος του

καλωδίου ανάμεσα στον υπολογιστή και στο κοντινότερο κέντρο της τηλεφωνικής εταιρείας (T/K), ή – ακριβέστερα – στον κοντινότερο DSL κόμβο του τηλεπικοινωνιακού παρόχου (DSLAM). Το μήκος του καλωδίου κυμαίνεται από 300 μέτρα για τις πολύ καλές ταχύτητες και μέχρι τα 5,5 χιλιόμετρα για πολύ μικρότερες ταχύτητες. Είναι σαφές, λοιπόν, ότι η τεχνολογία DSL απευθύνεται κατά βάση στους κατοίκους των αστικών κέντρων. Σύμφωνα με την αρχιτεκτονική του DSL, το εύρος ζώνης της γραμμής επικοινωνίας χωρίζεται σε τρία μέρη: Το πρώτο μέρος αφορά τις υπηρεσίες φωνής που είναι γνωστές με τον όρο POTS (Plain Old Telephone Service). Το δεύτερο μέρος χρησιμοποιείται κατά το ανέβασμα (Uploading) δεδομένων από τη συσκευή του συνδρομητή προς τον κεντρικό τηλεπικοινωνιακό κόμβο. Τέλος, το τρίτο μέρος αναλώνεται στο κατέβασμα (Downloading) των δεδομένων από τον κεντρικό τηλεπικοινωνιακό κόμβο προς τη συσκευή του συνδρομητή.

Ανάλογα με τις απαιτήσεις σε εύρος ζώνης προς τις δύο κατευθύνσεις (από και προς τον συνδρομητή), η DSL μπορεί να προσφέρει τόσο συμμετρικές, όσο και ασύμμετρες υπηρεσίες. Οι εφαρμογές που χρησιμοποιούν συμμετρικές υπηρεσίες απαιτούν το ίδιο εύρος ζώνης και προς τις δύο κατευθύνσεις. Για παράδειγμα, η υπηρεσία φωνής που παρέχεται από τις εταιρείες τηλεπικοινωνιών είναι συμμετρική. Αντίθετα, οι ασύμμετρες υπηρεσίες παρέχονται στις εφαρμογές που αξιώνουν μεγαλύτερο εύρος ζώνης προς την μια κατεύθυνση. Επειδή οι ευρυζωνικές τεχνολογίες που παρέχονται σήμερα είναι πολλές και πολύπλοκες, έχουν δημιουργηθεί οργανισμοί τυποποίησης υπεύθυνοι για την έκδοση οδηγιών και προτύπων που θα διαμορφώνουν και θα καθοδηγούν την ανάπτυξη των τεχνολογιών αυτών έτσι ώστε να είναι πιο απλές, κατανοητές και βοηθητικές σε όλους τους πολίτες.

1.6 Φορείς- Διεθνείς Οργανισμοί Τυποποίησης

Ως τα τέλη της δεκαετίας του 1980 ο τομέας των Τηλεπικοινωνιών δεν είχε εκδηλώσει τις ανάγκες της τυποποίησης όπως την εφαρμόζουν οι οργανισμοί τυποποίησης. Οι ανάγκες των διάφορων τηλεπικοινωνιακών οργανισμών και διοικήσεων (PTT) εστιάζονταν κυρίως στην απαίτηση συνεργασίας των εθνικών τηλεπικοινωνιακών δικτύων για τη διεκπεραίωση επιτυχών διεθνών επικοινωνιών.

Η πιο πάνω απαίτηση, λοιπόν, ικανοποιούνταν από τις συστάσεις (Recommendations) της Διεθνούς Συμβουλευτικής Επιτροπής Τηλεγραφίας και Τηλεφωνίας (CCITT) και της Διεθνούς Συμβουλευτικής Επιτροπής Ραδιοεπικοινωνιών (CCIR) που και οι δύο ήταν επιτροπές της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU), ενός οργανισμού υπό τον Οργανισμό Ηνωμένων Εθνών (ΟΗΕ).

Στον Ευρωπαϊκό χώρο τα PTT είκοσι έξι χωρών ιδρύσαν (1959) την Ευρωπαϊκή Διάσκεψη Ταχυδρομείων και Τηλεπικοινωνιών (CEPT) με κύριο στόχο την ανάπτυξη των σχέσεων μεταξύ των οργανισμών-μελών (δηλαδή των PTT) και την εναρμόνιση και πρακτική βελτίωση των τεχνικών και διοικητικών υπηρεσιών τους. Αυτό επιδιώχθηκε με τις Συστάσεις της CEPT. Η ραγδαία ανάπτυξη, όμως, της Τεχνολογίας Πληροφοριών (IT) και η σημαντική και συνεχώς επεκτεινόμενη επικάλυψη την οποία είχε αρχίσει να επιφέρει στις Τηλεπικοινωνίες, έκαναν επιτακτική την ανάγκη συνεργασίας τους με τους οργανισμούς τυποποίησης και τις CEN, CENELEC που είχαν ήδη προωθήσει την τυποποίηση στο «καθαρό» τμήμα του τομέα IT.

Το 1989 ήταν το έτος στο οποίο άρχισε να εφαρμόζεται στην πράξη η πολιτική της «νέας προσέγγισης» της Ευρωπαϊκής Ένωσης (ΕΕ) στο ζωτικό και αλματωδώς αναπτυσσόμενο τομέα των Τηλεπικοινωνιών, δηλαδή η στροφή στην ευρωπαϊκή πολιτική της τεχνικής εναρμόνισης από το αυστηρά κανονιστικό στο τυποποιητικό πλαίσιο. Είχε ήδη εκδοθεί από την ΕΕ η Πράσινη Βίβλος των τηλεπικοινωνιών (Green Paper) που προέβλεπε την έκδοση μιας σειράς Κοινοτικών Οδηγιών πλαισιακού χαρακτήρα οι οποίες θα υποστηρίζονταν τεχνικά, από εναρμονισμένα ευρωπαϊκά πρότυπα που θα παράγονταν από έναν αυτόνομο ευρωπαϊκό φορέα τυποποίησης.

Ο φορέας αυτός – που δεν ήταν άλλος από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) – ιδρύθηκε από τα μέλη της CEPT το 1988, για το σκοπό αυτό, και το 1989 άρχισε, πλέον, την παραγωγή των ευρωπαϊκών τηλεπικοινωνιακών προτύπων. Τα πρότυπα αυτά αποτέλεσαν και αποτελούν τη βάση των κοινών ευρωπαϊκών εναρμονισμένων τεχνικών απαιτήσεων όλων των σύγχρονων λειτουργούντων και αναπτυσσόμενων, αλλά και των μελλοντικών, τηλεπικοινωνιακών συστημάτων. Έτσι σήμερα υπάρχουν τρεις ευρωπαϊκές οργανώσεις τυποποίησης, η CEN, η CENELEC και το ETSI, οι οποίες έχουν ήδη αναπτύξει εκτεταμένη

συνεργασία για την ενιαία αντιμετώπιση της τυποποίησης στην Ευρώπη. Παράλληλα στον παγκόσμιο χώρο, έγινε αναδιοργάνωση της ITU και μετεξέλιξη των CCITT και CCIR, αντίστοιχα, οι οποίες έγιναν:

• Τομέας Τηλεπικοινωνιακής Τυποποίησης (ITU-T) και

• Τομέας Ραδιοεπικοινωνιών (ITU-R),

και παράγουν, ως παγκόσμια πρότυπα πλέον, συστάσεις ITU-T για τις Τηλεπικοινωνίες και συστάσεις ITU-R για τις Ραδιοεπικοινωνίες, αντίστοιχα. Όλα τα Ευρωπαϊκά Πρότυπα (EN, ETS) που εκπονούν οι τρεις ευρωπαϊκές οργανώσεις τυποποίησης (CEN, CENELEC, ETSI) μεταφέρονται αυτούσια στην εθνική τυποποίηση των χωρών μελών της ΕΕ και της EFTA. Σήμερα, το ETSI έχει 493 πλήρη μέλη από 36 χώρες της CEPT, 99 συνδεδεμένα μέλη από άλλες 20 χώρες από όλο τον κόσμο και 37 παρατηρητές. Τα σημερινά ελληνικά μέλη του ETSI είναι πέντε: ΥΠΜΕ, ΟΤΕ, INTRAKOM, VODAFONE και COSMOTE. Οι εκπρόσωποι των μελών αυτών συναποτελούν τη σημερινή Ελληνική Εθνική Αντιπροσωπεία στο ETSI με επικεφαλής τον εκπρόσωπο του ΥΠΜΕ.

Στην απαίτηση της Ευρωπαϊκής Επιτροπής να οριστεί από κάθε χώρα ένας εθνικός οργανισμός τυποποίησης αρμόδιος για τις εθνικές διαδικασίες δημόσιας κρίσης, ψηφοφορίας και εθνικής μεταφοράς των ευρωπαϊκών τηλεπικοινωνιακών προτύπων που θα παρήγε το ETSI, συνεργάστηκαν τα τρία πρώτα ελληνικά μέλη, με συντονιστή το ΥΠΜΕ, και αποφάσισαν να οριστεί ως εθνικός οργανισμός τυποποίησης και για τις τηλεπικοινωνίες ο ήδη δραστηριοποιημένος σε άλλους τομείς Ελληνικός Οργανισμός Τυποποίησης (ΕΛΟΤ). Παρακάτω αναφέρονται οι διεθνείς οργανισμοί τυποποίησης :

ITU International Telecommunication Union

ITU-T ITU - Telecommunication Sector, γνωστή παλαιότερα ως CCITT

ISO International Standards Organization

ANSI American National Standards Institute

IEEE Institute of Electrical and Electronics Engineers

NIST National Institute of Standards and Technology

IETF Internet Engineering Task Force

COS Corporation for Open Systems

ETSI European Telecommunications Standards Institute

ECMA European Computer Manufactures Association

EIA Electronic Industries Association

TIA Telecommunications Industries Association

MPEG Motion Picture Experts Group

1.7 Τύποι xDSL

Τα πρότυπα που έχουν εκδοθεί από τους οργανισμούς τυποποίησης αφορούν τους διάφορους τύπους στους οποίους διακρίνονται οι ευρυζωνικές τεχνολογίες. Όπως αναφέρθηκε σε παραπάνω κεφάλαιο τα μέλη της οικογένειας DSL διακρίνονται σε διάφορες κατηγορίες. Σε ασύμμετρο (ADSL: Asymmetric DSL) και συμμετρικό (SDSL: Symmetrical DSL), υψηλού ρυθμού μετάδοσης (HDSL: High bit rate DSL), προσαρμοζόμενου ρυθμού μετάδοσης (RADSL: Rate Adaptive DSL) και πολύ υψηλού ρυθμού μετάδοσης DSL (VDSL: Very high bit rate DSL). Μπορούν επίσης να κατηγοριοποιηθούν και στις Splitter-based και Splitterless. Η βασική τους διαφορά βρίσκεται στο ότι για την Splitter-based απαιτείται η εγκατάσταση ενός διαχωριστή σήματος από την τηλεφωνική εταιρεία στο χώρο που βρίσκεται ο υπολογιστής, ενώ για τη Splitterless ο διαχωρισμός του σήματος γίνεται κεντρικά στις εγκαταστάσεις της τηλεφωνικής εταιρείας.

Σύμφωνα με την κατηγοριοποίηση των ευρυζωνικών τεχνολογιών σε συμμετρικές και ασύμμετρες οι κυριότερες υποκατηγορίες του DSL και τα βασικότερα χαρακτηριστικά τους είναι τα εξής :

ΣΥΜΜΕΤΡΙΚΕΣ

HDSL. Το HDSL (High-bit-rate Digital Subscriber Line) υπήρξε η πρώτη εμπορικά αξιοποιημένη έκδοση του DSL. Χρησιμοποιεί το ίδιο εύρος και για την αποστολή και για τη λήψη των δεδομένων, με αποτέλεσμα να προσφέρει σχετικά μικρές ταχύτητες 2Mbps). Η τεχνολογία HDSL είναι από τις πρώτες που αναπτύχθηκαν στα τέλη της δεκαετίας του 1980 από την BellCore. Με την τεχνολογία HDSL είναι δυνατό να επιτευχθούν ταχύτητες της τάξεως των 2Mbps για αποστάσεις μεγαλύτερες των 3,6Km.

Τα βασικά πλεονεκτήματα του HDSL ήταν τα ακόλουθα :

• Μεγάλη ανοχή σε οποιαδήποτε τροποποίηση του τοπικού βρόχου από την εταιρεία παροχής τηλεφωνικών υπηρεσιών.

• Δυνατότητα αντιμετώπισης περιπτώσεων αποτυχίας του συστήματος. Αυτό σημαίνει ότι το HDSL μπορεί να ανακάμψει όταν ένα από τα δύο καλώδια αποτύχει. Απλά η χρήση μόνο του ενός καλωδίου περιορίζει τις επιδόσεις του συστήματος στο μισό.

HDSL2. Το πρότυπο HDSL2 σχεδιάστηκε για να αντικαταστήσει το HDSL. Παρέχει τους ίδιους ρυθμούς μετάδοσης με το HDSL απαιτώντας όμως μόνο ένα ζεύγος καλωδίων. Το πλεονέκτημα αυτό είναι πολύ σημαντικό, κυρίως σε περιοχές όπου τα αχρησιμοποίητα ζεύγη καλωδίων είναι σπάνια. Το HDSL2 είναι βασισμένο στο πρότυπο ANSI T1E1.4.

IDSL. Το IDSL (ISDN Digital Subscriber Line) είναι μια υβριδική τεχνολογία των DSL και ISDN. Χρησιμοποιεί την ίδια τεχνική κωδικοποίησης δεδομένων με το ISDN, τις συσκευές ISDN, και επιτυγχάνει ταχύτητες συμμετρικής μεταφοράς δεδομένων 64, 128, και 144Kbps.

SDSL. Το SDSL (Single-line Digital Subscriber Line) πρακτικά είναι το ίδιο με το HDSL, μόνο που χρησιμοποιεί μία μόνο γραμμή σύνδεσης. Η τεχνολογία SDSL είναι γνωστή και ως ψηφιακή γραμμή συνδρομητή απλού καλωδίου. Αποτέλεσε τον «πρόδρομο» του HDSL2.

Το SDSL βρίσκει πολλές εφαρμογές σε επιχειρησιακό επίπεδο. Αποτελεί ακόμα και σήμερα μια από τις καλύτερες λύσεις για τη σύνδεση εξυπηρετητών (servers) στο διαδίκτυο. Αν και το κανάλι της παραδοσιακής τηλεφωνικής υπηρεσίας μπορεί να είναι διαχωρισμένο από αυτά των δεδομένων, συνήθως, η τηλεφωνική

επικοινωνία δεν μπορεί να πραγματοποιείται ταυτόχρονα με τις υπηρεσίες δεδομένων. Κάτι τέτοιο δεν αποτελεί σοβαρό πρόβλημα σε επιχειρησιακό επίπεδο εξαιτίας της ύπαρξης εναλλακτικών λύσεων.

SHDSL ή G.SHDSL. Η SHDSL (Symmetric High-Bit rate Digital Subscriber Line) είναι η νεότερη προτυποποιημένη συμμετρική τεχνολογία και η πρώτη συμμετρική πολλαπλού ρυθμού. Είναι σχεδιασμένη να μεταφέρει συμμετρικούς ρυθμούς από 92Kbps μέχρι 2.3 Mbps σε ένα χάλκινο ζεύγος, ή 384 kbps έως 4,6 Mbps από δύο χάλκινα ζεύγη. Με αυτό τον τρόπο καλύπτει απαιτήσεις παραδοσιακά εξυπηρετούμενες από HDSL, SDSL ή άλλες συμμετρικές υπηρεσίες. Έχει προτυποποιηθεί με βάση τη σύσταση ITU G.991.2. Είναι γνωστό και ως G. SHDSL.

Το πρότυπο SHDSL παρέχει την επιλογή της αύξησης του ρυθμού ή της απόστασης με τη χρήση και δεύτερου χάλκινου ζεύγους. Το φορτίο της κίνησης διαμοιράζεται εξίσου και στα δύο ζεύγη, αλλά όσον αφορά την εφαρμογή και οι δύο συνδέσεις λειτουργούν ταυτόχρονα ως ένας μεγάλος δίαυλος. Σημαντικό μειονέκτημα της τεχνολογίας SHDSL είναι το ότι δεν μπορεί να εφαρμοστεί στο ίδιο ζευγάρι με την κλασική POTS τηλεφωνία, καθώς χρησιμοποιεί και αυτή το χαμηλό τμήμα του φάσματος.

ΑΣΥΜΜΕΤΡΕΣ

ADSL. Το ADSL (Asymmetric Digital Subscriber Line) είναι η πιο γνωστή έκδοση του DSL. Χρησιμοποιεί διαφορετικό εύρος για την αποστολή και διαφορετικό εύρος για τη λήψη των δεδομένων. Οι στατιστικές έχουν δείξει ότι ο μεγάλος όγκος κατά τη μεταφορά δεδομένων είναι προς το χρήστη, ενώ η ποσότητα των δεδομένων που αποστέλλει ο χρήστης προς το Διαδίκτυο, είναι πολύ μικρότερη. Το πρώτο πρότυπο ADSL προέβλεπε ονομαστικές ταχύτητες μέχρι 6,1Mbps downstream και 640kbps upstream ενώ επέτρεπε επίσης και την ταυτόχρονη μεταφορά φωνής από την ίδια γραμμή.

Η τεχνολογία αυτή παρέχεται και από εναλλακτικούς τηλεπικοινωνιακούς παρόχους καθώς η αποδέσμευση του τοπικού βρόγχου (local loop unbundling - LLU) τους δίνει τη δυνατότητα να έχουν πρόσβαση στο τελευταίο μίλι χαλκού.

Η τεχνολογία ADSL δίνει τη δυνατότητα εύκολα και με χαμηλό κόστος να υλοποιηθεί ευρυζωνική πρόσβαση πάνω από υπάρχουσα υποδομή και σε ικανοποιητικούς ρυθμούς μετάδοσης.

ADSL2/ADSL2+. Κατά τη διάρκεια των τελευταίων τριών ετών έχουν αναπτυχθεί πρότυπα για την επόμενη γενιά των τεχνολογιών ADSL. Οι ακόλουθες λοιπόν τεχνολογίες ADSL αποτελούν πλέον πρότυπα της ITU-T κάτω από τις αντίστοιχες συστάσεις: ADSL2 (G.992.3), ADSL2lite (G.992.4)και ADSL2plus (G.992.5 – Annexes A/B/M). Αυτές οι νέες τεχνολογίες έχουν κατά πολύ εξελίξει και εμπλουτίσει τις δυνατότητες αλλά και την ευελιξία που προσέφερε η αρχική ομάδα προτύπων του ADSL (ADSL - G.992.1 και ADSLlite - G.992.

RADSL. Το RADSL (Rate-Adaptive Digital Subscriber Line) αποτελεί μια παραλλαγή του ADSL, κατά την οποία γίνεται συνεχής μέτρηση της δυνατότητας μεταφοράς που έχει η γραμμή, και προσαρμόζεται ανάλογα ο ρυθμός μεταφοράς. Ο πιο συνηθισμένος συνδυασμός ρυθμών είναι 6,1Mbps για κάθοδο δεδομένων και 640Kbps για άνοδο δεδομένων. Ο τηλεπικοινωνιακός πάροχος είναι αυτός που αποφασίζει και μπορεί να μεταβάλει στατικά ή δυναμικά το ρυθμό μετάδοσης των δεδομένων σε μια σύνδεση.

DSL-Lite ή G.Lite ή Splitterless DSL ή Universal ADSL. Το G.Lite αποτελεί μια "περιορισμένη" έκδοση του ADSL, η οποία δεν απαιτεί την ύπαρξη splitter (διαχωριστή) στο άκρο που βρίσκεται ο υπολογιστής. Το G.Lite είναι πλέον πρότυπο του οργανισμού ITU (G- 992.2) και δίνει ταχύτητες downstream από 1,544Mbps μέχρι 6Mbps και upstream από 128Kbps μέχρι 384Kbps. Σε σχέση με το κανονικό ADSL, το πρότυπο G.Lite ADSL παρέχει μικρότερους ρυθμούς μετάδοσης, ενώ δεν απαιτεί διαχωρισμό της γραμμής στην πλευρά του χρήστη για την εξυπηρέτηση της τηλεφωνίας και των εφαρμογών δεδομένων. Ο διαχωρισμός της γραμμής γίνεται στον τηλεπικοινωνιακό φορέα. Αυτό συντελεί στη μείωση του κόστους εξοπλισμού και της ανάπτυξης. Μια σύνδεση G.Lite λειτουργεί καλύτερα με τη χρήση μικροφίλτρων, τα οποία τοποθετούνται στις τηλεφωνικές γραμμές στις εγκαταστάσεις του πελάτη.

VDSL. Το VDSL (Very-high-data-rate Digital Subscriber Line) βρίσκεται ακόμη σε ανάπτυξη και έχοντας πραγματοποιήσει εξωπραγματικές, για τα μέχρι τώρα δεδομένα του χαλκού, ταχύτητες που φτάνουν τα 55Mb το δευτερόλεπτο και υπόσχεται πολλά περισσότερα. Βέβαια μόνο όσοι βρίσκονται σε απόσταση μικρότερη από 300 μέτρα από τον κοντινότερο VDSL κόμβο θα μπορούν να την αξιοποιήσουν. Το VDSL

παρουσιάζοντας μια τεχνική ομοιότητα με το ADSL αναμένεται να συνυπάρξει με αυτό και να το υποκαταστήσει στις περιπτώσεις που οι τεχνικοί περιορισμοί το επιτρέπουν, όπως για παράδειγμα όταν το μήκος του ακραίου χάλκινου τμήματος του δικτύου πρόσβασης μειώνεται λόγω μεσολάβησης Μονάδας Οπτικού δικτύου, ONU.

1.8 Ευρυζωνικές Υπηρεσίες & Εφαρμογές

Με την απόκτηση οποιουδήποτε τύπου DSL σύνδεσης, οι ταχύτητες είναι πολύ μεγαλύτερες από μια απλή dial-up σύνδεση, έτσι, μπορούν να γίνουν και κάποια πράγματα που δεν θα ήταν δυνατά υπό άλλες συνθήκες. Οι υπηρεσίες και οι εφαρμογές που πρόκειται να κατακλύσουν τα δίκτυα νέας γενιάς σχεδιάζονται όλο και με ταχύτερους ρυθμούς και ως ένα βαθμό έχουν αρχίσει να εμφανίζονται. Σε πιο προηγμένα τεχνολογικά κράτη έχουν παρουσιαστεί και μελέτες την χρήσης αυτών και της συμπεριφοράς τους ως προς τους χρήστες. Ειδικότερα το περιεχόμενο των ευρυζωνικών δικτύων αποτελείται από εφαρμογές σαν τις ακόλουθες.

¬ Ηλεκτρονική μάθηση (E-learning) Μία από τις κύριες κατηγορίες εφαρμογών που έχει ήδη εμφανιστεί στα ευρυζωνικά δίκτυα αφορά διαδικασίες και μεθόδους που σχετίζονται με το e-learning. Με τον όρο αυτό περιγράφονται οι διαδικασίες που στοχεύουν στην μάθηση μέσω του διαδικτύου, με τη χρήση διαφόρων τεχνικών. Οι κυριότερες μορφές έκφρασης elearning διαδικασιών που αναμένεται να βρουν εφαρμογή είναι η παροχή Online μαθημάτων σε μεγάλη μερίδα σπουδαστών (multicast of online courses) και η δημιουργία online βιβλιοθηκών. Το τελευταίο έχει ήδη αρχίσει να αναπτύσσεται (υπάρχουν ήδη σημαντικές online libraries) που αποσκοπούν στην εύκολη αναζήτηση και απόκτηση γνώσης.

¬ Ηλεκτρονική εκπαίδευση (E–Training) Η Ηλεκτρονική Επαγγελματική Εκπαίδευση (Technology Based Training - TBT), είναι μέρος του e-learning που αφορά επιχειρήσεις και οργανισμούς σε αντίθεση με το κατεξοχήν e-learning που αφορά μαθησιακή εκπαίδευση σε ΑΕΙ, δευτεροβάθμια εκπαίδευση κτλ.

¬ Ηλεκτρονική υγεία (E-health) Παράλληλα μια κατηγορία εφαρμογών με μεγάλη κοινωνική κυρίως σημασία είναι οι εφαρμογές τηλε-ιατρικής.

Στον τομέα αυτό εντάσσονται εφαρμογές που επιτρέπουν διάγνωση ασθενειών και εξέταση ασθενών από απόσταση όπως και εφαρμογές ρομποτικής για πραγματοποίηση χειρουργικών επεμβάσεων. Οι εφαρμογές αυτές αναμένεται να βρουν σημαντικό πεδίο εφαρμογής τα επόμενα χρόνια και επίσης θεωρείται πιθανό να ζητούν και συγκεκριμένη μεταχείριση από το δίκτυο εξαιτίας του σκοπού που επιτελούν.

¬ Ηλεκτρονικό εμπόριο (E-commerce) Με τον όρο ηλεκτρονικό εμπόριο περιγράφεται η διάθεση και αγοραπωλησία προϊόντων ηλεκτρονικά. Ο τομέας αυτός έχει γνωρίσει μεγάλη άνθηση σε όλο τον κόσμο και εξαπλώνεται διαρκώς και στην Ελλάδα. Ήδη υπάρχουν πολλά ηλεκτρονικά καταστήματα (ελληνικά αλλά και ξένα) και η απήχησή τους στον κόσμο όλο και διευρύνεται. Στην νέα εποχή των ευρυζωνικών δικτύων, που θα έχει πρόσβαση πολύ μεγάλη μερίδα του πληθυσμού, αναμένεται να γνωρίσουν ιδιαίτερη άνθηση, αφού παρέχουν ένα εύχρηστο και γρήγορο τρόπο για πραγματοποίηση αγορών. Σημαντικό τους επίσης πλεονέκτημα είναι η προσφορά οικονομικότερων τιμών, λόγω μειωμένου διαχειριστικού κόστους. ¬ Εφαρμογές κατά απαίτηση (Applications on demand) Επίσης μια σημαντική κατηγορία εφαρμογών που πρόκειται να εμφανιστούν (και ίσως η εμπορικότερη) είναι οι εφαρμογές «On demand». Στην περίπτωση αυτή ανήκουν διάφορες εφαρμογές/υπηρεσίες που παρέχονται στους χρήστες «κατ' απαίτησή» τους, χρεώνονται από τον πάροχο και με κατάλληλη κωδικοποίηση μεταδίδονται. Τέτοιες συνήθεις εφαρμογές είναι ταινίες (movies), μουσικά αρχεία, παιχνίδια ή software για χρήση.

¬ Ηλεκτρονικό παιχνίδι (E-gaming) Τα παιχνίδια στον ηλεκτρονικό υπολογιστή είναι μια πολύ διαδεδομένη ενασχόληση σε όλους τους χρήστες των υπολογιστών, μικρούς και μεγάλους. Μάλιστα μπορούμε να πούμε ότι μεγάλο μέρος των χρηστών υπολογιστών ασχολείται σχεδόν αποκλειστικά, τις ώρες που χρησιμοποιεί τον υπολογιστή, με τα παιχνίδια. Τα τελευταία χρόνια, με την εξάπλωση των δικτύων και του Internet, αναπτύχθηκαν πάρα πολύ τα online παιχνίδια, είτε σε επίπεδο τοπικού δικτύου (LAN), είτε σε επίπεδο Internet.

¬ Peer-to-peer applications Οι εφαρμογές peer-to-peer (P2P) είναι δικτυακές εφαρμογές που δεν ακολουθούν τη λογική Client/Server, αλλά σχηματίζεται ένα δίκτυο από εφαρμογές (και χρήστες), όπου όλοι είναι ισότιμοι ή έστω δεν υπάρχει κάποιος κεντρικός έλεγχος. Το περιεχόμενο που προσφέρεται δεν καθορίζεται συνεπώς από κάποιον content provider, αλλά από τους ίδιους τους χρήστες αυτού του δικτύου. Οι

εφαρμογές αυτές είναι συνήθως εφαρμογές για διαδικτυακή συζήτηση ή εφαρμογές που επιτρέπουν την ανταλλαγή αρχείων. Αυτές οι εφαρμογές, επειδή τα μηνύματα και τα δεδομένα που ανταλλάσσονται δεν μεταφέρονται προς κάποιον κεντρικό υπολογιστή και από εκεί στους υπόλοιπους, μπορούν να προκαλέσουν υψηλή συμφόρηση σε ένα δίκτυο.

¬ Advanced Communications To Internet χρησιμοποιείται εδώ και χρόνια ως ένα φθηνό μέσο επικοινωνίας μεταξύ ανθρώπων. Στα προγράμματα προχωρημένων επικοινωνιών υποστηρίζονται χαρακτηριστικά που επιτρέπουν τη μετάδοση φωνής για την επικοινωνία μεταξύ δύο ή περισσότερων ανθρώπων (Voice over IP) ή τη μετάδοση κινούμενης εικόνας (εικονοδιάσκεψη - videoconferencing) μαζί με τον ήχο. Τα ευρυζωνικά δίκτυα προσφέρουν εικονοδιάσκεψη, ή VoIP τηλεφωνία (και εικονοτηλεφωνία) και γνωρίζουν μεγάλη απήχηση στο ευρύ κοινό καθώς επιτρέπουν μορφές επικοινωνίας, που με χρήση των κλασικών τηλεφωνικών δικτύων είναι πολύ ακριβές, με σχεδόν μηδενικό κόστος.

¬ Interactive TV Η χρήση των δικτύων μεγάλου εύρους ζώνης επεκτείνεται και στην υποστήριξη της αμφίδρομης διαδραστικής τηλεόρασης. Διαδραστική τηλεόραση νοείται η εφαρμογή στην οποία ο τηλεθεατής/χρήστης (μέσω του τηλεχειριστηρίου του) συμμετέχει ενεργά και σε πραγματικό χρόνο στην υπηρεσία που λαμβάνει. Οι πλατφόρμες διαδραστικής τηλεόρασης χρησιμοποιούν συνήθως διαφορετικά μέσα για το κανάλι μετάδοσης των υπηρεσιών και για το κανάλι επιστροφής. Η χρήση ενός ευρυζωνικού δικτύου για τη μετάδοση του video/audio stream θα επέτρεπε την απλοποίηση της αρχιτεκτονικής μιας πλατφόρμας διαδραστικής τηλεόρασης καθώς και τη λήψη διαδραστικών τηλεοπτικών καναλιών μέσω υπολογιστή.

¬ Virtual / Augmented / Mixed Reality Ο όρος Virtual Reality (VR) είναι αρκετά διαδεδομένος στις μέρες μας. Σημαίνει τη σύνθεση ενός κόσμου μέσω υπολογιστή, ο οποίος μιμείται κάποια χαρακτηριστικά του αληθινού κόσμου, στον οποίο όμως δεν υπάρχουν τα όρια και οι περιορισμοί του αληθινού κόσμου. Στους λεγόμενους Virtual Worlds ή Virtual Environments πολλοί χρήστες μπορούν να περιπλανηθούν στους χώρους τους. Το να είναι όλοι οι χρήστες ενημερωμένοι για τη θέση και την κατάστασή τους, καθώς και για τις αντίστοιχες ιδιότητες των άλλων χρηστών, όπως επίσης και η ενημέρωση του συστήματος για τις ενέργειες που επιθυμούν να κάνουν οι χρήστες απαιτεί τη διακίνηση τεράστιων ποσοτήτων δεδομένων. Το μέγεθος της διακινούμενης

πληροφορίας είναι ακόμα μεγαλύτερο όταν μιλάμε για κόσμους augmented reality, augmented virtuality ή γενικότερα mixed reality. Ένας κόσμος augmented reality είναι το αποτέλεσμα του εμπλουτισμού ενός φυσικού κόσμου με στοιχεία και αντικείμενα δημιουργημένα με υπολογιστή. Είναι προφανές ότι ο ερχομός των broadband δικτύων δίνει τη δυνατότητα για την ανάπτυξη πραγματικά εντυπωσιακών online real-time συνθετικών κόσμων, που είναι αδύνατο να δημιουργηθούν σήμερα (όχι λόγω έλλειψης επεξεργαστικής ισχύος ή άλλων τεχνολογικών περιορισμών, αλλά αποκλειστικά εξαιτίας της έλλειψης αρκετού εύρους ζώνης).

¬ Voice-over-DSL Η εξέλιξη στις υπηρεσίες φωνής πάνω στο DSL αποτελεί το μεγάλο πλεονέκτημα της τεχνολογίας και βαρόμετρο στην αγοραστική προοπτική της. Κατά την εφαρμογή τεχνολογίας DSL η μεταφορά φωνητικού σήματος είναι εφικτή με τουλάχιστον τρεις τρόπους:

• Κλασική τηλεφωνία με χρήση διαχωριστών (splitters)

• Φωνή πάνω από ATM (VoATM - Voice over ATM)

• Φωνή πάνω από IP (VoIP - Voice over IP) Λόγω της μεγάλης φασματικής περιοχής που χρησιμοποιείται σε μια σύνδεση DSL είναι δυνατό να μεταφερθούν αρκετές τηλεφωνικές συνδιαλέξεις. Για τη μεταφορά τηλεφωνικών συνδιαλέξεων πάνω από σύνδεση DSL απαιτείται η μετατροπή της φωνής σε ψηφιακά πακέτα δεδομένων. Τα πακέτα αυτά μεταφέρονται μέσω της σύνδεσης δεσμεύοντας δυναμικά το απαραίτητο εύρος ζώνης, μόνο όταν πραγματοποιείται η κλήση. Η τεχνική αυτή είναι δυνατό μακροπρόθεσμα να αντικαταστήσει τις παραδοσιακές τηλεφωνικές συνδέσεις.

¬ Teleworking Η ύπαρξη συνδέσεων υψηλής ταχύτητας, επιτρέπει στους απομονωμένους χρήστες να έχουν με αποτελεσματικό τρόπο πρόσβαση στα εταιρικά τοπικά δίκτυα. Ο θεσμός της τηλε-εργασίας προωθείται από τις μεγάλες εταιρίες παγκοσμίως και η εξέλιξή του θα σταθμίσει την αγορά του DSL, καθώς πρόκειται για την «επέκταση» των τοπικών δικτύων αυτών των εταιρειών στο διαδίκτυο (e-LANs). ¬ Περιβάλλον Ιδιωτικών Δικτύων Το DSL είναι μια τεχνολογία μετάδοσης δεδομένων πάνω από καλώδια χαλκού, η οποία είναι ευρέως διαθέσιμη σήμερα και μπορεί να χρησιμοποιηθεί για να λύσει πολλά από τα προβλήματα που αντιμετωπίζονται σε περιβάλλον ιδιωτικών δικτύων (Private Network Environment, PNE). Ως περιβάλλον ιδιωτικού δικτύου μπορεί να οριστεί μια οργάνωση, ένα ίδρυμα, μια εταιρία ή μια

αντιπροσωπεία που απαιτούν τις μεταδόσεις μεγάλων όγκων δεδομένων. Αυτές οι διαφορετικές οργανώσεις έχουν ένα κοινό χαρακτηριστικό: την υπάρχουσα υποδομή χάλκινων καλωδίων που αποτελεί το δίκτυο φωνής. Ένα κοινώς γνωστό PNE είναι το εσωτερικό δίκτυο ενός πανεπιστημίου.

¬ Επέκταση των LAN δικτύων και συνένωση τους (Lan-to-Lan) Κατά τη διάρκεια του χρόνου, οι άνθρωποι που χρησιμοποιούν διαφορετικά LANs έχουν την ανάγκη να μοιραστούν τις πληροφορίες ο ένας με τον άλλο. Συχνά αυτά τα LANs χωρίζονται από πολύ μεγάλες αποστάσεις και χρειάζεται να επεκτείνουν απλά το τμήμα του τοπικού LAN. Χρησιμοποιώντας την τεχνολογία DSL, η τηλεφωνική καλωδίωση μπορεί να χρησιμοποιηθεί για την εύκολη και ανέξοδη συνδεσιμότητα LAN-to-LAN. Γίνεται η σύνδεση της συσκευής DSL με τα τηλεφωνικά καλώδια σε ένα κτήριο και μετά συνδέεται μια άλλη συσκευή DSL με το άλλο τέλος των καλωδίων στο άλλο κτήριο. Τέλος, οι συσκευές DSL συνδέονται στο αντίστοιχο LAN τους, μέσω κάποιου μεταγωγέα (switch) ή δρομολογητή (router). Το αποτέλεσμα είναι απλός, γρήγορος, και ανέξοδος τρόπος την επέκτασης του μεγάλου τοπικού LAN.

Από την ανάλυση που έγινε είναι φανερές οι πολλαπλές δυνατότητες που προκύπτουν από τις ευρυζωνικές συνδέσεις. Είναι φανερό, πως όλες σχεδόν οι παραλλαγές του DSL αποτελούν αξιόπιστες πλατφόρμες για ανταγωνιστικές υπηρεσίες τόσο σε οικιακά όσο και σε επιχειρησιακά περιβάλλοντα, αποδοτικά και οικονομικά αφού εκμεταλλεύονται την υπάρχουσα φυσική υποδομή – καλωδίωση. Από τα στατιστικά στοιχεία που προκύπτουν από έρευνες τόσο διεθνώς όσο και στη χώρα μας, αποδεικνύεται η σημαντικότητα της ευρυζωνικότητας τόσο στην εξέλιξη όλων των χωρών σε όλους τους τομείς όσο και της διευκόλυνσης των πολιτών στην καθημερινότητα τους.

ΚΕΦΑΛΑΙΟ 2: Γενικά για το Bonding στα Δίκτυα

Το Broadband Bonding είναι η σύνθεση του εύρους ζώνης πολλών broadband συνδέσεων και η δημιουργία μίας ενιαίας σύνδεσης υψηλής ταχύτητας και μέγιστης αξιοπιστίας για την υποστήριξη σύγχρονων διαδικτυακών εφαρμογών.Η νέα

τεχνολογία πρόσβασης στο Internet για το ευρύ κοινό και τις μικρομεσαίες επιχειρήσεις ακούει στο όνομα VDSL (Very high-bitrate/high speed DSL). Το VDSL είναι το πιο γρήγορο ασύμμετρο DSL και αποτελεί τον πρόδρομο της τεχνολογίας FTTH (Fiber-To-The-Home). Καθώς η αντικατάσταση όλων των χαλκινων τηλεπικοινωνιακών καλωδίων με οπτικές ίνες είναι μία χρονοβόρος και ακριβή διαδικασία, είναι πιο εύκολη και προσιτή η επέκταση του δικτύου κορμού των παρόχων και η δημιουργία περισσότερων τηλεπικοινωνιακών κέντρων (DSLAMs) τα οποία εξυπηρετούν μερικές δεκάδες συνδρομητές σε μικρή ακτίνα απο αυτά, παρέχοντας μεγαλύτερες ταχύτητες απο αυτές των ADSL. Το VDSL επιτρέπει την παροχή υπηρεσιών που απαιτούν υψηλό εύρος ζώνης, όπως η τηλεόραση υψηλής ανάλυσης, το ψηφιακό βίντεο, η διασύνδεση απομακρυσμένων εταιρικών καταστημάτων κ.α.

Το μεγαλύτερο πρόβλημα των συνδέσεων VDSL είναι η αξιοπιστία που προσφέρουν η οποία δεν είναι μεγαλύτερη αυτής των ADSL συνδέσεων. Αυτό συμβαίνει γιατί οι πάροχοι προσφέρουν τις συνδέσεις VDSL χωρίς εγγύηση διαθεσιμότητας (best effort) που σημαίνει ότι η κάθε σύνδεση μπορεί να δυσλειτουργεί για κάποιο χρονικό διάστημα ή να έχει χαμηλότερη απόδοση τις ώρες αιχμής. Επομένως μία επιχείρηση για την οποία η πρόσβαση στο Internet είναι κρίσιμης σημασίας, δεν μπορεί να βασιστεί σε μία σύνδεση VDSL παρόλο που η ονομαστική προσφερόμενη ταχύτητα μπορεί να φαίνεται ικανοποιητική για τις ανάγκες της επιχείρησης. Άλλωστε δεν είναι λίγες οι επιχειρήσεις που ενώ βρίσκονται εντός δικτύου VDSL επιλέγουν την χρήση μισθωμένης γραμμής για τις επιχειρησιακές τους ανάγκες.

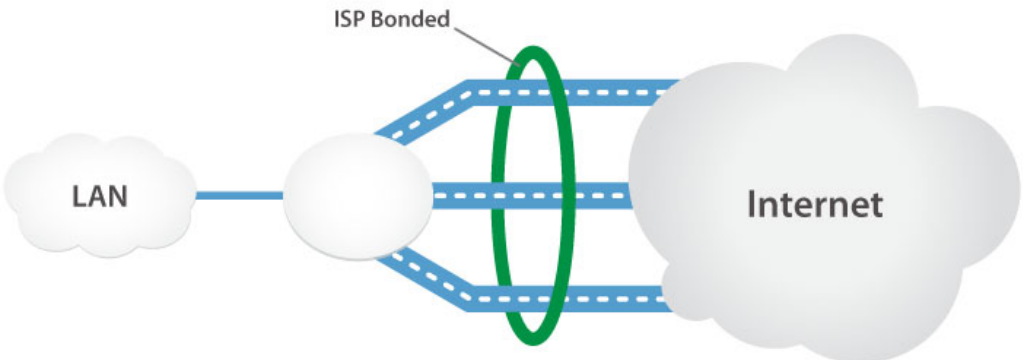
Το πρόβλημα της χαμηλής αξιοπιστίας των συνδέσεων VDSL έρχονται να το καλύψουν οι υπηρεσίες broadband bonding οι οποίες επιτρέπουν τον συνδυασμό πολλαπλών συνδέσεων VDSL για την δημιουργία εικονικών μισθωμένων γραμμών πολλαπλασιάζοντας την αξιοπιστία των επιμέρους συνδέσεων πρόσβασης και αξιοποιώντας ταυτόχρονα τα δίκτυα πολλαπλών παρόχων. Η σύνθεση του bandwidth πολλαπλών συνδέσεων VDSL έχει πολλαπλά ωφέλη καθώς παρέχει ασύμμετρη ταχύτητα πρόσβασης στο Internet, μεγαλύτερη αξιοπιστία απο την παραδοσιακή μισθωμένη γραμμή και πολύ χαμηλότερο κόστος, ακόμα και αν συγκριθεί μόνο βάσει της ταχύτητας upload. Για παράδειγμα, συνδυάζοντας τέσσερις συνδέσεις VDSL με ονομαστική ταχύτητα 50/5Mbps, η υπηρεσία Broadband bonding δημιουργεί μία ενιαία εικονική σύνδεση με συνολική ταχύτητα 200/20Mbps. Το κόστος αυτής της

υλοποίησης ανέρχεται στο 1/4 του κόστους μίας μισθωμένης γραμμής 20/20Mbps, παρέχοντας παράλληλα πολύ μεγαλύτερη ταχύτητα download και υψηλή αξιοπιστία που δεν βασίζεται στη σωστή λειτουργία του δικτύου ενός μόνο παρόχου.

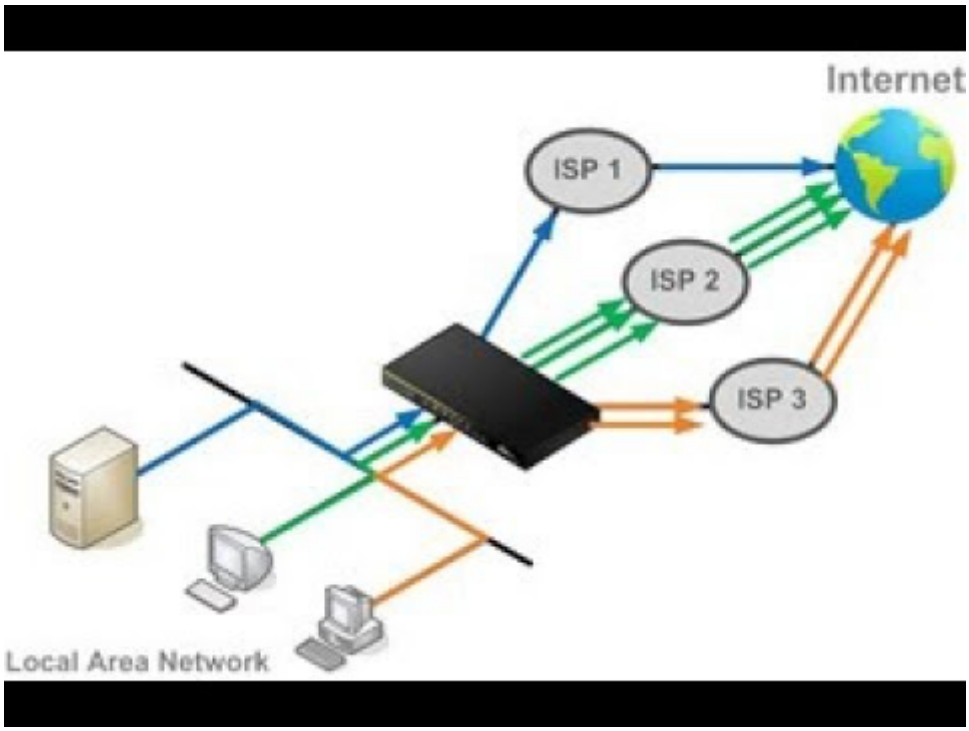
Το bonding σημαίνει πραγματική συσσωμάτωση του εύρους ζώνης όλων των μέσων WAN που πρόκειται να συνδεθούν. Σε αντίθεση με την εξισορρόπηση φορτίου, η οποία μπορεί να διανέμει φορτίο σε αρκετούς συνδέσμους WAN, πραγματοποιείται εδώ πραγματική συγκόλληση όλων των διαθέσιμων συνδέσεων. Το Bonding είναι ιδανικό όταν επιθυμούμε:

- Αξιοπιστία
- Ευαίσθητες εφαρμογές στην καθυστέρηση
- Σύνδεση με το εταιρικό δίκτυο

Το Bonding επιτρέπει τη χρήση μηχανισμών για την παρακολούθηση της απόδοσης κάθε καναλιού όσον αφορά την ταχύτητα, την καθυστέρηση και την απώλεια πακέτων. Αυτό σημαίνει ότι η ποιότητα της υπηρεσίας (QoS) μπορεί να ρυθμιστεί σύμφωνα με αυτά τα δεδομένα, για παράδειγμα, δεν στέλνει φωνή κάτω από ένα κανάλι που έχει ξεπεράσει ένα προκαθορισμένο όριο καθυστέρησης. Στις εικόνες που ακολουθούν έχουμε ένα παράδειγμα για το πώς μπορεί να γίνει το bonding από πολλαπλούς ISP's.



Σχήμα 2.1: Διαγραμματική Απεικόνιση του Bonding



Σχήμα 2.2: Εφαρμογή Internet Bonding από πολλαπλούς παρόχους

2.1 Βελτιστοποίηση και επιτάχυνση Δικτύων WAN

Οι τεχνολογίες και τα προϊόντα που χρησιμοποιούνται στη βελτιστοποίηση WAN εξελίσσονται συνεχώς. Η βελτιστοποίηση του δικτύου WAN επιτρέπει στους οργανισμούς να αξιοποιήσουν περισσότερο τις συνδέσεις WAN με συμφόρηση. Επιπλέον, μπορεί να επιτευχθεί εξοικονόμηση κόστους, καθώς οι αγορές πρόσθετου εύρους ζώνης ενδέχεται να καθυστερήσουν. Εάν το εύρος ζώνης WAN διπλασιάζεται, εξακολουθεί να είναι συνήθως πολύ μικρότερο από την απόδοση που παρέχεται σε ένα τοπικό δίκτυο. Αυτό σημαίνει ότι η βελτιστοποίηση συνδέσεων συνήθως δεν επαρκεί για την επίτευξη της ιδανικής απόδοσης.

Η συμπίεση και το QoS πρέπει να συμπεριλαμβάνονται με άλλες τεχνικές επιτάχυνσης προκειμένου να παρασχεθεί μια εκτεταμένη λύση για την παράδοση των εφαρμογών. Οι πιο εξελιγμένες λύσεις παροχής εφαρμογών, για παράδειγμα, μπορούν να συνδυάσουν όλες τις τεχνικές διαχείρισης εύρους ζώνης και επιτάχυνσης εφαρμογής.

2.2 Μείωση Δεδομένων

"Η μείωση των δεδομένων είναι μια τεχνική όπου οι συσκευές επιτάχυνσης εξετάζουν όλες τις εισερχόμενες και εξερχόμενες κυκλοφορίες WAN και αποθηκεύουν μια τοπική παρουσία πληροφοριών σε ένα ανεξάρτητο κατάστημα δεδομένων εφαρμογής." Πριν από την αποστολή των πακέτων WAN ελέγχονται αν υπάρχει αντιστοιχία στην τοπική παρουσία στο προορισμού. Σε περίπτωση που υπάρχει αντιστοιχία, τότε οι επαναλαμβανόμενες πληροφορίες δεν αποστέλλονται μέσω του WAN και αποστέλλονται οδηγίες για την τοπική διανομή των δεδομένων. Μόνο τα απαραίτητα δεδομένα θα μεταδοθούν μέσω του WAN, εάν έχουν τροποποιηθεί τα δεδομένα.

Η μείωση των δεδομένων βελτιώνει τόσο τη χρήση του WAN όσο και τον χρόνο απόκρισης της εφαρμογής. Με την παροχή πληροφοριών τοπικά, όποτε είναι δυνατόν, μπορεί να μειωθεί ένα αξιοσημείωτο τμήμα του εύρους ζώνης WAN, συμβάλλοντας έτσι στην παροχή επιδόσεων τύπου LAN σε όλο το WAN.

2.3 Συμπίεση Δεδομένων

Η συμπίεση δεδομένων είναι μια τεχνική που επιτρέπει καλύτερη χρήση εύρους ζώνης σε όλο το WAN. Βασίζεται σε μορφές δεδομένων που μπορούν να εκπροσωπούνται πιο αποτελεσματικά. Η συμπίεση δεδομένων μειώνει το μέγεθος των πλαισίων δεδομένων που μεταδίδονται μέσω μιας σύνδεσης δικτύου. Με μειωμένο μέγεθος πλαισίου μειώνεται επίσης ο χρόνος που απαιτείται για τη μετάδοση του πλαισίου στο δίκτυο. Ένα σύστημα κωδικοποίησης παρέχεται σε κάθε άκρο ενός συνδέσμου μετάδοσης που επιτρέπει την απομάκρυνση χαρακτήρων από τα πλαίσια δεδομένων στην πλευρά αποστολής του συνδέσμου. Στη συνέχεια αντικαθίσταται σωστά από την πλευρά λήψης. Επειδή τα συμπυκνωμένα πλαίσια απαιτούν μικρότερο εύρος ζώνης, μεγαλύτεροι όγκοι μπορούν να μεταδοθούν σε ένα συγκεκριμένο χρονικό σημείο.

Τα οφέλη που προκύπτουν από τις τεχνικές συμπίεσης ποικίλλουν ανάλογα με τον τύπο κίνησης που διέρχεται μέσω του WAN, αλλά είναι αρκετά συνεπή στις διάφορες λύσεις των πωλητών. Για παράδειγμα, με κείμενο και υπολογιστικά φύλλα

είναι δυνατή η απόδοση λόγων συμπίεσης 2-5x. Οι οργανισμοί εμφανίζουν συνήθως περίπου 50% βελτίωση στη χρήση του WAN με τεχνολογία συμπίεσης. Αυτό ισοδυναμεί με διπλασιασμό του αποτελεσματικού εύρους ζώνης WAN.

2.4 Μείωση καθυστέρησης

Η καθυστέρηση είναι ένας κοινός όρος για μια καθυστέρηση που εισάγεται από το δίκτυο και μπορεί επίσης να ονομάζεται χρόνος διάδοσης σήματος. Η καθυστέρηση στρογγυλού ταξιδιού υποδεικνύει την ώρα που τα δεδομένα μεταβαίνουν από έναν αποστολέα στον δέκτη και πίσω. Η ελάχιστη λανθάνουσα κατάσταση είναι ευθέως ανάλογη με την απόσταση που διανύεται μεταξύ των δύο τελικών σημείων επικοινωνίας. Όσο μεγαλύτερη είναι η απόσταση, τόσο μεγαλύτερη είναι η ελάχιστη καθυστέρηση. Η καθυστέρηση επηρεάζεται επίσης από την καθυστέρηση ουράς και την καθυστέρηση επεξεργασίας σε δρομολογητές και άλλες συσκευές δικτύου κατά μήκος της διαδρομής.

Η καθυστέρηση έχει συχνά μεγάλη επίδραση στην απόδοση των εφαρμογών σε όλο το WAN. Για τις μεταφορές δεδομένων TCP χύδην, η καθυστέρηση μπορεί να περιορίσει σημαντικά τη διακίνηση δεδομένων. Ο λόγος για αυτό είναι ότι ο έλεγχος συμφόρησης TCP περιορίζει το ποσό των μη αναγνωρισμένων δεδομένων κατά τη μεταφορά. Όταν η ποσότητα των μη αναγνωρισμένων δεδομένων φτάσει στο μέγεθος του παραθύρου συμφόρησης, η μεταβίβαση νέων δεδομένων αναβάλλεται μέχρις ότου αναγνωριστούν τα παλαιότερα δεδομένα. Υπάρχουν τεχνικές επιτάχυνσης που χρησιμοποιούνται για την αντιμετώπιση των προβλημάτων καθυστέρησης που σχετίζονται με την παράδοση εφαρμογών σε ένα WAN, όπως η επιτάχυνση TCP και η επιτάχυνση του Common File System (CIFS).

2.5 Μείωση Απωλειών

Η Διόρθωση Προειδοποίησης (FEC=Forward Error Correction) είναι μια τεχνική που έχει τη δυνατότητα να διορθώνει σφάλματα δυαδικών ψηφίων στο φυσικό επίπεδο. Αυτή η τεχνολογία μπορεί επίσης να προσαρμοστεί ώστε να λειτουργεί σε

πακέτα στο επίπεδο δικτύου για να βελτιώσει την απόδοση εφαρμογών σε δίκτυα WAN που έχουν υψηλά χαρακτηριστικά απώλειας πακέτων.

Με FEC σε επίπεδο πακέτου, είναι δυνατή η ανασυγκρότηση πακέτων χαμένων δεδομένων στο τελικό σημείο ενός συνδέσμου WAN, αποφεύγοντας τις καθυστερήσεις που έρχονται με επαναμεταδόσεις πολλαπλών γύρων. Μέσα από αυτό, τα δίκτυα WAN μπορούν εύκολα να ανακάμψουν από την απώλεια πακέτων εξαιτίας ποικίλων συνθηκών στρώματος δικτύου, όπως υπερχείλιση ουρών και δεσμοί περιορισμένου εύρους ζώνης. Ορισμένες λύσεις επιτάχυνσης είναι σε θέση να ρυθμίζουν δυναμικά τα γενικά έξοδα FEC σε ανταπόκριση στις μεταβαλλόμενες συνθήκες σύνδεσης για μέγιστη απόδοση σε περιβάλλοντα με υψηλή απώλεια πακέτων.

2.6 Συνδυασμός συνδέσεων και εξισορρόπηση φορτίου

Η συνάθροιση συνδέσμων είναι ένας διφορούμενος όρος που χρησιμοποιείται για τον ορισμό διαφόρων εφαρμογών και τεχνολογιών που δεν εμπλέκονται. Σε γενικές γραμμές, η συσσωμάτωση συνδέσεων αναφέρεται στον συνδυασμό παράλληλων πολλαπλών δικτύων για την αύξηση της απόδοσης και της απόλυσης. Η σύνδεση συνδέσεων (a.k.a., σύνδεσμος καναλιών, ομαδοποίηση, ομαδοποίηση) υλοποιείται χρησιμοποιώντας δύο ή περισσότερους δεσμούς μεταξύ φυσικών διεπαφών σε χαμηλότερο επίπεδο, είτε ανά πακέτο (OSI layer 3) είτε σε σύνδεση δεδομένων (OSI layer 2). Εδώ, για παράδειγμα, αρκετοί σύνδεσμοι DSL μπορούν να φορτωθούν ισορροπημένοι. Χρησιμοποιώντας πρότυπα όπως το LACP, οι σύνδεσμοι συνδυάζονται σε έναν λογικό σύνδεσμο, με την κυκλοφορία να κατανέμεται ομοιόμορφα.

Η εξισορρόπηση φορτίου είναι ένας συχνά χρησιμοποιούμενος όρος όταν περιγράφεται η σύνδεση δεσμών. Αυτή η προσέγγιση διαφοροποιεί την ποσότητα εργασίας που πρέπει να κάνει ένας υπολογιστής μεταξύ δύο ή περισσότερων υπολογιστών. Διαχωρίζει την κίνηση μεταξύ των διεπαφών δικτύου σε μια υποδοχή δικτύου (OSI layer 4). Κατά συνέπεια, γίνεται περισσότερη δουλειά στο ίδιο χρονικό διάστημα και, γενικά, όλοι οι χρήστες γίνονται πιο γρήγοροι. Η εξισορρόπηση φορτίου στοχεύει στη βελτιστοποίηση της χρήσης των πόρων, στη μεγιστοποίηση της απόδοσης, στην ελαχιστοποίηση του χρόνου απόκρισης και στην αποφυγή

υπερφόρτωσης οποιουδήποτε μεμονωμένου πόρου. Το λογισμικό εξισορρόπησης φορτίου περιλαμβάνει ειδικό λογισμικό ή υλικό, όπως διακόπτη πολλαπλών στρώσεων ή διαδικασία διακομιστή DNS (Domain Name System).

Η εξισορρόπηση φορτίου διαφέρει από τη σύνδεση καναλιών, έτσι ώστε η εξισορρόπηση φορτίου να μπορεί να υλοποιηθεί με υλικό, λογισμικό ή με συνδυασμό των δύο. Σε ένα σύμπλεγμα που βασίζεται σε υλικό, η συσκευή υλικού ελέγχει όλη την επισκεψιμότητα στους διακομιστές του συμπλέγματος εξισορρόπησης φορτίου. Σε ένα λογισμικό εξισορρόπησης φορτίου, κάθε ένας από τους διακομιστές στο σύμπλεγμα εξισορρόπησης φορτίου περιλαμβάνει λογισμικό που υποστηρίζει το σύμπλεγμα.

Όταν ένας χρήστης συνδέεται σε έναν ιστότοπο, ο εξισορροπιστής φορτίου χρησιμοποιεί έναν αλγόριθμο για να κατευθύνει το χρήστη σε έναν συγκεκριμένο διακομιστή ιστού. Διαφορετικοί χρήστες συνδέονται με διαφορετικούς διακομιστές ιστού και το συνολικό αποτέλεσμα είναι ότι το φορτίο είναι ισορροπημένο μεταξύ κάθε διακομιστή. Η εξισορρόπηση φορτίου είναι συνήθως ο κύριος λόγος για την ομαδοποίηση διακομιστών υπολογιστών.

Οι εταιρείες των οποίων οι τοποθεσίες Web έχουν μεγάλο όγκο επισκεψιμότητας χρησιμοποιούν συνήθως εξισορρόπηση φορτίου. Για την υπηρεσία Web, μια μέθοδος είναι να δρομολογήσει κάθε αίτημα με τη σειρά του σε μια διαφορετική διεύθυνση κεντρικού υπολογιστή διακομιστή σε έναν πίνακα DNS, στρογγυλό-robin μόδα. Σε πολλές περιπτώσεις, εάν δύο διακομιστές αντισταθμίζουν ένα φορτίο εργασίας, απαιτείται ένας τρίτος διακομιστής για να καθορίσει ποιο διακομιστή θα εκχωρήσει το έργο.

Δεδομένου ότι ένα σύστημα εξισορρόπησης φορτίου απαιτεί πολλούς διακομιστές, συνήθως συνδυάζεται με διακομιστές backup και backup. Σε ορισμένες περιπτώσεις, οι διακομιστές διανέμονται σε διαφορετικές γεωγραφικές τοποθεσίες.

Με την εξισορρόπηση φορτίου, είναι δυνατή η εξισορρόπηση της κυκλοφορίας μεταξύ διαφορετικών τεχνολογιών δικτύου. Οι εφαρμογές κατανέμονται σε διάφορους συνδέσμους, χρησιμοποιώντας παράλληλα το εύρος ζώνης των επιμέρους συνδέσμων. Με άλλα λόγια, η εφαρμογή 1 πηγαίνει στη σύνδεση ένα, η εφαρμογή δύο στη σύνδεση δύο, και ούτω καθεξής. Λόγω αυτού του λόγου, οι εφαρμογές μπορούν να έχουν πρόσβαση μόνο στο εύρος ζώνης ενός μεμονωμένου συνδέσμου αλλά όχι στο

άθροισμα όλων των συνδέσμων. Εάν ένας σύνδεσμος πέσει κάτω, επηρεάζονται όλες οι εφαρμογές που μεταδίδουν δεδομένα σε όλη τη σύνδεση. Εάν η ποιότητα της σύνδεσης μειώνεται σταδιακά (π.χ. αύξηση της καθυστέρησης ή της απώλειας πακέτων), είναι αδύνατο να δρομολογηθεί η εφαρμογή (π.χ. τηλεφωνία IP ή θύρα SIP) σε διαφορετικό σύνδεσμο.

2.7 Δρομολόγηση βασισμένη στην απόδοση

Η δρομολόγηση βάσει επιδόσεων επιτρέπει τη μετάδοση εφαρμογών με βάση διαφορετικά κριτήρια σε παράλληλες υποδομές δικτύου. Αυτά τα κριτήρια είναι π.χ. χρόνος απόκρισης, απώλεια πακέτων, jitter, μέσος βαθμός γνώμης (MOS), διαθεσιμότητα, φόρτος κυκλοφορίας και πολιτικές κόστους. Το μοχλό-παίζει κανονικά πρωτόκολλα δρομολόγησης όπως το BGP, το OSPF και το EIGRP. Αυτή η τεχνολογία είναι πιο προηγμένη από την εξισορρόπηση φορτίου αφού λαμβάνει υπόψη τις ειδικές ανάγκες των εφαρμογών. Για το λόγο αυτό, η τεχνολογία είναι πολύ εντατική στο CPU και απαιτεί πλατφόρμες δρομολογητών μεσαίας έως υψηλού επιπέδου.

Υπάρχουν και ορισμένες αδυναμίες στη δρομολόγηση βάσει απόδοσης. Οι εφαρμογές μπορούν να έχουν πρόσβαση στο εύρος ζώνης ενός μεμονωμένου συνδέσμου παρόχου, αλλά όχι το άθροισμα όλων των συνδέσμων. Εάν ένας σύνδεσμος καταρρεύσει, επηρεάζονται όλες οι εφαρμογές που μεταδίδουν δεδομένα μέσω του συνδέσμου. Παίρνει λίγο χρόνο για να ανακτήσει και να ξεκινήσει την εκ νέου διαβίβαση των δεδομένων σε μια διαφορετική σύνδεση. Επιπλέον, εάν η ποιότητα της σύνδεσης μειωθεί σταδιακά (π.χ. αύξηση της καθυστέρησης ή της απώλειας πακέτων), είναι αδύνατο να δρομολογηθεί η εφαρμογή (π.χ. τηλεφωνία IP ή θύρα SIP) σε διαφορετικό σύνδεσμο.

2.8 Broadband Bonding

Οι προηγούμενες μεθοδολογίες σύνδεσης, όπως η σύνδεση καναλιών, πραγματοποιήθηκαν σε χαμηλότερα στρώματα OSI (Επίπεδα 1, 2 και πιθανώς 3). Η δέσμευση καναλιών αναφέρεται στη ρύθμιση δικτύωσης όπου δύο ή περισσότερες διεπαφές δικτύου σε έναν κεντρικό υπολογιστή συνδυάζονται για πλεονασμό ή

αυξημένη απόδοση. Αυτή η προσέγγιση απαιτεί συντονισμό με την telcos για την υλοποίηση. Επιπλέον, οι ευρωπαϊκές και ασιατικές ρυθμιστικές αρχές ραδιοφάσματος έχουν απαγορεύσει τη σύνδεση 802.11 καναλιών από τις χώρες τους.

Η ευρυζωνική σύνδεση (που αναφέρεται και σε σύνδεση WAN σε αυτή τη διπλωματική εργασία) αναφέρεται σε συσσωμάτωση πολλαπλών καναλιών σε OSI Layers στο επίπεδο 4 ή παραπάνω. Τα δεσμευμένα κανάλια μπορούν να περιλαμβάνουν ενσύρματους συνδέσμους όπως μια γραμμή T1 ή DSL. Επιπλέον, είναι δυνατό να συνδεθούν πολλαπλοί κυτταρικοί σύνδεσμοι ή ένα μείγμα ενσύρματων και κυτταρικών γραμμών για μια συσσωρευμένη σύνδεση. Η ευρυζωνική σύνδεση προσδίδει γρήγορα και οικονομικά αποδοτικό εύρος ζώνης στο δίκτυο χωρίς την ανάγκη αλλαγών στην αρχιτεκτονική τοπικού δικτύου (LAN). Δεδομένου ότι η ευρυζωνική σύνδεση εφαρμόζεται σε υψηλότερα επίπεδα OSI, μπορεί να αναπτυχθεί χωρίς συντονισμό με τη telcos.

Οι λύσεις μισθωμένων γραμμών βασίζονται σε αποκλειστικές ίνες ή παρόμοιες συνδέσεις με το γραφείο και τυπικά παρέχουν εύρος ζώνης μεταξύ 1 Mbit/s και 10 Mbit/s. Η διαθεσιμότητα αυτών των συνδέσεων εξαρτάται από την τοποθεσία και συχνά υπόκειται σε ρυθμίσεις και μηνιαία τέλη μίσθωσης με συμβατικές δεσμεύσεις πολλών ετών. Δεν είναι εύκολο να μεταφερθούν μεταξύ τοποθεσιών που επηρεάζουν το κόστος και την ευκολία οποιασδήποτε κίνησης ή αλλαγής στις επιχειρηματικές λειτουργίες. Οι λύσεις ευρυζωνικής σύνδεσης μπορούν να θεωρηθούν αξιοσημείωτη εναλλακτική λύση στις μισθωμένες γραμμές ή ένα υποκατάστατο για συνδέσεις οπτικών ινών.

Σε αντίθεση με την εξισορρόπηση φορτίου, η ευρυζωνική σύνδεση βασίζεται στην ταυτόχρονη χρήση πολλαπλών συνδέσμων. Εδώ, αρκετοί σύνδεσμοι WAN από διάφορους παρόχους υπηρεσιών και μέσω διαφορετικών μέσων μετάδοσης συνδυάζονται σε μία ενιαία σύνδεση που είναι διαθέσιμη για όλες τις εφαρμογές εντός του δικτύου. Αυτή η εικονική υψηλής ταχύτητας σύνδεση βασίζεται σε τουλάχιστον δύο μεμονωμένες ευρυζωνικές συνδέσεις. Ως αποτέλεσμα, όλοι οι διαθέσιμοι σύνδεσμοι WAN συνδυάζονται για να σχηματίσουν μια σύνδεση η οποία παρέχει το άθροισμα όλων των ατομικών εύρους ζώνης είτε μόνο για μία μόνο εφαρμογή ή για πολλές εφαρμογές. Αυτό είναι πολύ επιλεκτικό π.χ. για τηλεδιασκέψεις, αντίγραφα ασφαλείας, μεταφορές αρχείων, λήψεις και για την παράδοση περιεχομένου. Επιπλέον,

το εύρος ζώνης μπορεί να αυξηθεί σταδιακά προς τα πάνω ανεξάρτητα από έναν μεμονωμένο πάροχο Διαδικτύου.

Το κύριο πλεονέκτημα της σύνδεσης WAN είναι ότι ακόμα και αν μια σύνδεση αποτύχει ή μειωθεί η ποιότητα, ο δρομολογητής μπορεί να στείλει δυνητικά χαμένα πακέτα μέσω ενός διαφορετικού συνδέσμου παροχέα. Μόνο το συνολικό εύρος ζώνης του συνδέσμου μειώνεται. Αυτή η αρχιτεκτονική εξασφαλίζει επίσης υψηλό επίπεδο ασφάλειας. Εδώ, τα μοναδικά πακέτα είναι κατακερματισμένα σε διαφορετικά δίκτυα παρόχων. Είναι σχεδόν αδύνατο να παρεμποδίσουμε διάφορα δίκτυα παρόχων και να συσχετίσουμε τα θραύσματα για να αναδημιουργήσουμε το πακέτο IP.

Η ανάμιξη διαφορετικών τεχνολογιών πρόσβασης δημιουργεί χρόνο λειτουργίας μόλις 100%, γεγονός που μειώνει σημαντικά τον κίνδυνο διακοπής λειτουργίας. Δεν υπάρχει απώλεια συνδεσιμότητας για μια εφαρμογή, εάν ένας σύνδεσμος πάει κάτω, εφόσον παραμένει τουλάχιστον ένας σύνδεσμος. Συνεπώς, η απώλεια πακέτων είναι ελάχιστη, ακόμη και σε περιβάλλοντα με τα περισσότερα προβλήματα (π.χ. σε ταχύτατα κινούμενα οχήματα).

Ορισμένα εταιρικά δίκτυα ενδέχεται να εκτείνεται σε διάφορες χώρες ή ακόμα και σε άλλες ηπείρους. Σε πολλές περιπτώσεις, τα δίκτυα αυτά λειτουργούν από έναν μόνο μεγάλο πάροχο Διαδικτύου όπως η T-Systems, η AT & T ή η TeliaSonera. Κατά συνέπεια, τα εταιρικά δίκτυα συχνά διαχειρίζονται εξωτερικά. Αυτοί οι μεγάλοι πάροχοι διαδικτύου προσφέρουν συνήθως δαπανηρές και μακροπρόθεσμες συμβάσεις, οι οποίες είναι επίσης άκαμπτες. Αυτό σημαίνει ότι οι προτιμώμενες τροποποιήσεις ή ενημερώσεις στο δίκτυο ενδέχεται να χρειαστούν πολύ χρόνο για να εκτελεστούν και συνήθως κοστίζουν πολλά χρήματα. Οι πάροχοι μπορούν επίσης να δημιουργήσουν εξαρτήσεις από άποψη διαθεσιμότητας, ποιότητας υπηρεσιών και QoS με τις επιχειρήσεις των οποίων τα δίκτυα λειτουργούν.

Η προσθήκη νέων ή προσωρινών τοποθεσιών σε ένα εταιρικό δίκτυο απαιτεί συνήθως χρόνο με μεγάλους παρόχους υπηρεσιών. Μερικές φορές ένας μεγάλος πάροχος δεν είναι σε θέση να προσφέρει κατάλληλες συνδέσεις (MPLS, T1, SDSL) σε μια νέα θέση ή μπορεί να τους προσφέρει μόνο πολύ υψηλό κόστος ή με μεγάλο χρόνο παράδοσης. Όσον αφορά τις διεθνείς συνδέσεις, ο συγκεκριμένος πάροχος που έχει επιλέξει η επιχείρηση πρέπει να έχει τη δική της υποδομή στις αναφερόμενες χώρες. Εναλλακτικά, πρέπει να είναι έτοιμοι να συνεργαστούν με τους τοπικούς παρόχους.

Εάν μια τέτοια συνεργασία πρέπει να αποτελέσει αντικείμενο διαπραγμάτευσης, η τοπική σύνδεση στο χώρο του site μπορεί να καθυστερήσει δραματικά. Σε τέτοιες περιπτώσεις, η επιχείρηση μπορεί να επιλέξει μια παραδοσιακή λύση VPN χωρίς σύνδεση.

Η ιδέα της σύλληψης είναι ότι δεν βασίζεται σε μια ενιαία σύνδεση, αλλά στη σύνδεση τουλάχιστον δύο συνδέσεων διαφορετικών παρόχων υπηρεσιών και τεχνολογιών πρόσβασης. Είναι δυνατό να ξεκινήσετε με μία μόνο τεχνολογία πρόσβασης και, σε μεταγενέστερο στάδιο, να προσθέσετε επιπλέον μέσα WAN στη ρύθμιση σύνδεσης. Αυτή η εργασία εισάγει τεχνολογία συγκόλλησης ως τεχνολογία αιχμής για την αύξηση της απόδοσης του δικτύου.

2.9 Bonding σε πολλαπλά μέσα

Με την τεχνολογία συγκόλλησης, είναι δυνατόν να επωφεληθείτε από μέσα που είναι φυσικά διαφορετικά για να αποκτήσετε υψηλή αξιοπιστία. Σχετικά φθηνά καταναλωτικά προϊόντα όπως οι ADSL, καλωδιακές και 3G / 4G κινητές συνδέσεις μπορούν να χρησιμοποιηθούν για να σχηματίσουν ένα γρήγορο και αξιόπιστο VPN site-to-site. Αυτό το είδος λύσης μπορεί να είναι πολύ χαμηλότερο σε σχέση με την εκχώρηση μισθωμένης γραμμής ή MPLS. Η λύση υλοποιείται με συνδυασμό υλικού, λογισμικού και μέσω ορισμένων αλγορίθμων. Η διαδικασία συνδυασμού προστατεύεται από διπλώματα ευρεσιτεχνίας που ανήκουν στους πωλητές.

2.10 WAN Bonding σε διάφορα περιβάλλοντα και εφαρμογές

Υπάρχουν πολλοί κλάδοι των βιομηχανιών που μπορούν εύκολα να βελτιστοποιήσουν και να αυξήσουν την απόδοση των λύσεων συνδεσιμότητάς τους χρησιμοποιώντας αυτή τη λύση. Αυτό μπορεί να έχει ως αποτέλεσμα κέρδη σε έναν οργανισμό. Όποτε απαιτείται αξιόπιστη ευρυζωνική σύνδεση, οι συμβατικές προσφορές υπηρεσιών παρέχονται συνήθως πολύ στενά. Για το λόγο αυτό, πολλοί συνάδελφοι συχνά δεν παίρνουν αυτό που χρειάζονται από τις συνδέσεις τους. Αυτή είναι η κατάσταση, ιδίως όταν διαφορετικές εφαρμογές πρέπει να καλύπτονται από μία μόνο λύση συνδεσιμότητας. Στις παρακάτω υποενότητες παρουσιάζονται ορισμένα

πιθανά σενάρια δέσμευσης WAN σε ορισμένους τομείς των βιομηχανιών και της καθημερινότητάς μας.

- Δημόσιος Τομέας

Αν κάθε κυβερνητική υπηρεσία προσπαθήσει να αναπτύξει λύση ειδικά για δικούς της σκοπούς, το συνολικό νομοσχέδιο θα είναι σίγουρα πάνω από τον προϋπολογισμό. Ο δημόσιος τομέας εν γένει με τις διάφορες δραστηριότητές του είναι ένα παράδειγμα όπου μπορεί να εφαρμοστεί τεχνολογία συγκόλλησης WAN και έτσι να επιτευχθεί αξιοσημείωτη εξοικονόμηση κόστους. Δημιουργεί επίσης μια σπονδυλική στήλη για πολλές χρήσιμες εφαρμογές.

Για να αλλάξει η πορεία, οι δημόσιες υπηρεσίες πρέπει να παράγονται με πολύ πιο αποτελεσματικό τρόπο, μειώνοντας δραστικά το κόστος σε κάθε τομέα. Προκειμένου να επιτευχθεί ο στόχος, οι λύσεις συνδεσιμότητας δικτύου πρέπει να σχεδιαστούν εκ νέου για να ικανοποιήσουν τις απαιτήσεις. Οι λύσεις δικτύου πρέπει να παρέχουν την αξιοπιστία, την προσβασιμότητα και το επαρκές εύρος ζώνης ώστε να καλύπτουν τις ανάγκες συνδεσιμότητας των μελλοντικών εφαρμογών.

Ένα άλλο πεδίο στον δημόσιο τομέα όπου μπορεί να εφαρμοστεί η τεχνολογία είναι η υγειονομική περίθαλψη και τα ασθενοφόρα: Αντί να βασιζόμαστε σε έναν πάροχο υπηρεσιών, η συγκέντρωση και η αθροιστική, π.χ. τρεις κυψελοειδείς συνδέσεις από διαφορετικούς παρόχους εξασφαλίζουν μια αξιόπιστη σύνδεση υψηλής ταχύτητας. Μέσα από αυτό, τα ασθενοφόρα μπορούν να μεταδίδουν βίντεο HD για να συμβουλεύονται ειδικούς στα νοσοκομεία τους.

- Τηλεματική και Έξυπνη μέτρηση

Ορισμένοι φορείς εκμετάλλευσης έχουν ήδη προσαρμόσει τις υπηρεσίες τους σε συγκεκριμένες βιομηχανίες, ενώ άλλοι εξακολουθούν να διερευνούν τις δυνατότητες που προσφέρουν διαφορετικές βιομηχανίες. Κάθε τομέας του κλάδου έχει το δικό του προφίλ όσον αφορά τον αριθμό των χρηστών, τις απαιτήσεις για το εύρος ζώνης, την αποδοτικότητα ανά σύνδεση και το προφίλ ανάπτυξης.

Η Τηλεματική διαδραματίζει σημαντικό ρόλο στην ευρύτερη βιομηχανία M2M και περιλαμβάνει πολλές διαφορετικές εφαρμογές τόσο στον καταναλωτικό όσο και στον εμπορικό τομέα, από την ενημέρωση εντός του οχήματος για τους καταναλωτές

έως τις υπηρεσίες διαχείρισης στόλου για τις επιχειρήσεις. Πολλές εφαρμογές τηλεματικής, ειδικά ο τομέας τηλεματικής καταναλωτών, απαιτούν μεγαλύτερο εύρος ζώνης από άλλες εφαρμογές M2M. Η τηλεματική μπορεί να χρησιμεύσει ως πλατφόρμα για υπηρεσίες ανάκτησης και κλεμμένων υπηρεσιών ανάκτησης που βασίζονται στη χρήση. Επιπλέον, η τηλεματική μπορεί να χρησιμοποιηθεί από εμπορικούς αυτοκινητιστές για προϊόντα στόλου, δεδομένα οδηγών και παρακολούθηση οχημάτων.

Για να είναι υλοποιήσιμες αυτές οι εφαρμογές, θα χρειαστεί μια αξιόπιστη και πολύ διαθέσιμη πρόσβαση στο δίκτυο. Η έξυπνη μέτρηση παρέχει μετρήσεις σε πραγματικό χρόνο του ηλεκτρισμού, του νερού, του φυσικού αερίου και άλλων υπηρεσιών κοινής ωφέλειας. Περιλαμβάνει τη χρήση τσιπ, κάρτες SIM και αξιόπιστη πρόσβαση στο δίκτυο για να μοιραστούν αυτές οι πληροφορίες. Η ιδέα της έξυπνης μέτρησης και της ιδέας του «έξυπνου δικτύου» είναι ότι οι μετρητές και άλλες συσκευές συνδέονται μέσω ενός δικτύου. Αυτό επιτρέπει την ευρεία συλλογή και ανταλλαγή πληροφοριών σχετικά με τις πτυχές της χρήσης των πόρων. Μια αξιόπιστη πρόσβαση στο δίκτυο αποτελεί προϋπόθεση για εφαρμογές Smart Metering. Αυτό μπορεί να πραγματοποιηθεί αξιόπιστα εφαρμόζοντας σύνδεση WAN στον τόπο όπου λαμβάνει χώρα η μέτρηση.

- Υγειονομική περίθαλψη και απομακρυσμένη παρακολούθηση ασθενών

Η τηλεϊατρική και η τηλεπαρακολούθηση απαιτούν πρόσβαση στο δίκτυο με υψηλό εύρος ζώνης και την υψηλότερη διαθεσιμότητα. Ένας τύπος εφαρμογής είναι η επικοινωνία μεταξύ ιατρών ή νοσηλευτών στα νοσοκομεία και των ασθενών τους με χρόνιες ασθένειες στο σπίτι. Οι συσκευές παρακολούθησης διαφέρουν ως προς την πολυπλοκότητά τους και είναι κρίσιμες για όλες τις υπηρεσίες ηλεκτρονικής υγείας. Σε μια απλή περίπτωση, μια συσκευή παρακολούθησης μπορεί να χρησιμοποιηθεί για την παρακολούθηση της αρτηριακής πίεσης ή του βάρους του ασθενούς σε ένα σύστημα που συνδέεται με έναν υπολογιστή ή tablet και ένα smartphone μπορεί να χρησιμοποιηθεί ως κόμβος. Σε μια πιο περίπλοκη περίπτωση, οι αρρυθμίες της καρδιάς μπορούν να αντιμετωπιστούν μέσω μιας ειδικής συσκευής παρακολούθησης η οποία συνδέεται μέσω αξιόπιστης σύνδεσης στο Internet με έναν καρδιολόγο.

Πολλαπλοί αισθητήρες θα αποκτήσουν τα δεδομένα που αντιστοιχούν σε διαφορετικές παραμέτρους υγείας για διάφορα μέρη του σώματος του ασθενούς

χρησιμοποιώντας ένα κατάλληλο δίκτυο πρόσβασης με υψηλή διαθεσιμότητα και εύρος ζώνης. Διάφοροι αισθητήρες μπορεί να είναι για βοήθεια σε μια μελέτη συνεργασίας για ένα ενιαίο πρόβλημα υγείας. Αυτό επιτρέπει την απομακρυσμένη παρακολούθηση του ασθενούς ενώ ο ασθενής είναι στατικός (π.χ. στο σπίτι του ασθενούς) ή όταν είναι κινητός (π.χ. σε ασθενοφόρο). Παρέχει επίσης τη δυνατότητα λήψης κατάλληλων άμεσων ενεργειών εάν υπάρχει συναγερμός ή η απομακρυσμένη συμβουλή από γιατρό ή ειδικό. Πιλοτικά έργα τηλεπαρακολούθησης έχουν υλοποιηθεί με τη λύση Wip bonding της Viprinet, καθώς προσφέρει συνεχή συνδεσιμότητα ανεξάρτητα από την τοποθεσία του σπιτιού του ασθενούς. Οι δρομολογητές επέτρεψαν στους ασθενείς να γίνουν δεκτοί από το νοσοκομείο στο σπίτι με ένα κιτ tele-homecare. Ο ασθενής υποβάλλει δεδομένα όπως επίπεδο οξυγόνου στο αίμα, σφυγμό, πίεση αίματος και ΗΚΓ σε κεντρική βάση δεδομένων. Αυτό εφαρμόζεται πολλές φορές την ημέρα. Εάν ορισμένες από τις παραμέτρους είναι εκτός προρυθμισμένων επιπέδων, ενεργοποιείται μια τηλεδιάσκεψη μεταξύ τηλε-νοσοκόμου και ασθενούς στο σπίτι.

- Λιανεμπόριο

Ψηφιοποιημένες εφαρμογές, π.χ. τα προγράμματα πελατών, η τιμολόγηση, η εφοδιαστική ή η λογιστική είναι μερικοί από τους λόγους για τους οποίους οι λιανοπωλητές απαιτούν συνεχώς υψηλότερο εύρος ζώνης και uptime. Προηγουμένως 98% ή 99% διαθεσιμότητα και τα εύρος ζώνης DSL ήταν αρκετά για τους λιανοπωλητές. Σήμερα, απαιτούν 100% χρόνο λειτουργίας και μεγαλύτερο εύρος ζώνης φόρτωσης λόγω της ύπαρξης εφαρμογών ψηφιακής σήμανσης και ηλεκτρονικών πληρωμών στο διαδίκτυο. Κάθε αποτυχία ή συμφόρηση όσον αφορά την πρόσβαση στο δίκτυο θα έχει αρνητικό αντίκτυπο στις συναλλαγές του ταμείου και στην ικανοποίηση του πελάτη.

Η παροχή αξιόπιστης υπηρεσίας Internet είναι ένα κρίσιμο βήμα για την προετοιμασία της επιχείρησης λιανικής για τις αναδυόμενες τεχνολογίες. Οι έμποροι λιανικής πώλησης υιοθετούν γρήγορα νέες τεχνολογίες και προσαρμόζουν τις λειτουργίες τους για να προσφέρουν μια πιο εξατομικευμένη εμπειρία αγορών στους πελάτες τους. Mobile POS, περιβάλλον Wi-Fi ή περίπτερο πελάτη και συσκευές και αισθητήρες Internet of Things χρειάζονται αξιόπιστο Internet.

Οι έμποροι λιανικής αναμένουν ότι οι συσκευές IoT θα μειώσουν το λειτουργικό κόστος και θα βελτιώσουν την επιχειρησιακή απόδοση σε κάθε περιοχή. Οι συσκευές

IoT έχουν τη δυνατότητα να δημιουργήσουν ένα "ανταποκρινόμενο" περιβάλλον λιανικής πώλησης το οποίο θα είναι σε θέση να ενημερώνει τις πιθανές επαναγορές των πελατών για να επηρεάσει τη συμπεριφορά τους.

- Ζωντανές μεταδόσεις

Η ραδιοφωνική δραστηριότητα ζωντανής ραδιοτηλεόρασης απαιτούσε κατά παράδοση περιττές μισθωμένες γραμμές. Με τη σύνδεση δεσμών αρκετών παρόχων 3G και 4G, οι ραδιοτηλεοπτικοί σταθμοί μπορούν να χρησιμοποιήσουν την ευελιξία και τον πλεονασμό της λύσης.

Η έρευνα στο Διαδίκτυο θα μπορούσε να εφαρμοστεί νωρίτερα μόνο όταν το όχημα ήταν σταθμευμένο με εκτεταμένη και ευθυγραμμισμένη κεραία. Η διαδικασία έπρεπε να ξεκινήσει από το μηδέν όποτε το όχημα έπρεπε να μετακινηθεί (π.χ. για παραβίαση στάθμευσης). Το αποτέλεσμα ήταν συχνά μια άκαμπτη και δαπανηρή σύνδεση στο Internet με μεγάλη καθυστέρηση.

- Πλοία και Πλατφόρμες Πετρελαίου

Οι τουρίστες και οι ταξιδιώτες χρειάζονται τις κατάλληλες συνδέσεις στο διαδίκτυο ανεξάρτητα από την τοποθεσία. Ένας τουρίστας που ταξιδεύει σε ποτάμι ή ταξιδεύει για επαγγελματικούς λόγους πρέπει να έχει πρόσβαση στο διαδίκτυο για ταξίδια ή επιχειρηματικές επικοινωνίες. Προηγουμένως, η δυνατότητα σύνδεσης παρέχεται πιθανώς από έναν πάροχο 3G / 4G, ο οποίος οδήγησε σε πολύ κακή απόδοση όσον αφορά το εύρος ζώνης και την καθυστέρηση. Επιπλέον, η κακή κάλυψη του δικτύου, ιδίως στις αγροτικές περιοχές, όπως οι ακτές του ποταμού και της θάλασσας, συχνά οδηγεί σε συχνές αποσυνδέσεις.

Τα δύσκολα σενάρια σύνδεσης μπορούν να επιλυθούν ακόμη και στις θαλάσσιες και στις υπεράκτιες βιομηχανίες. Σε αυτές περιλαμβάνονται οι περιοχές χωρίς κινητή λήψη ή τα πλοία που διασχίζουν συχνά τα σύνορα. Με την τεχνολογία συγκόλλησης, οι πλοιοκτήτες, οι κρουαζιέρες και οι επιχειρήσεις πορθμείων έχουν μια νέα ευκαιρία να προσφέρουν καλύτερη ποιότητα υπηρεσιών και να δημιουργήσουν νέες υπηρεσίες και εφαρμογές για ταξιδιώτες. Ταυτόχρονα, η λύση μειώνει την καθυστέρηση και αποσυνδέει λόγω καλύτερης κάλυψης συνδυάζοντας διαφορετικά δίκτυα παρόχων. Κατά συνέπεια, μπορεί να επιτευχθεί μια αυξημένη ικανοποίηση του πελάτη η οποία, μακροπρόθεσμα, οδηγεί σε αύξηση του αριθμού των πελατών.

Οι ιδιοκτήτες σκαφών συχνά υποφέρουν από την έλλειψη αξιόπιστης και οικονομικά αποδοτικής σύνδεσης στο Internet, ιδίως όταν τα σκάφη είναι μακριά από την ακτή. Δεδομένου ότι με την τεχνολογία σύνδεσης που παρέχεται από τη Viprinet, είναι δυνατό να συνδεθούν 4G και VSAT μαζί με άλλες τεχνολογίες WAN, δραστηριότητες διαχείρισης, τηλεδιάσκεψη και άλλες δραστηριότητες κατανάλωσης εύρους ζώνης μπορούν να γίνουν κοντά και μακριά από την ακτή. Με άλλα λόγια, π.χ. ένα πλωτό απομακρυσμένο γραφείο είναι εύκολο να εγκατασταθεί σε σκάφη ή μεγαλύτερα σκάφη χωρίς να εξαρτάται μόνο από ένα ISP και την τεχνολογία πρόσβασης. Η λύση Viprinet έχει ήδη εφαρμοστεί σε ορισμένα κρουαζιερόπλοια και σκάφη, όπου παρέχει μια απρόσκοπτη σύνδεση στο Internet ακόμη και όταν διασχίζουν τα σύνορα των χωρών. Επιπλέον, αυτή η λύση χρησιμοποιείται ήδη σε ορισμένες πλατφόρμες πετρελαίου προκειμένου να μειωθεί το κόστος των δορυφορικών συνδέσεων κατά τη διάρκεια έκτακτων περιστατικών.

- Νομικές Υπηρεσίες

Οι οργανισμοί επιβολής του νόμου έχουν αναγνωρίσει την ανάγκη γρήγορων και αξιόπιστων εφαρμογών ευρυζωνικών δεδομένων. Οι φορείς επιβολής του νόμου απαιτούν πρόσβαση στο Διαδίκτυο στο σημείο ανάγκης, ανεξάρτητα από την κάλυψη ενός και μοναδικού παρόχου υπηρεσιών. Αυτά εξαρτώνταν προηγουμένως από δορυφορικούς συνδέσμους με την ανάγκη για οπτική επαφή και σταθερή τοποθεσία ή κάλυψη δικτύου κινητής τηλεφωνίας ενός μόνο παροχέα. Αυτές οι προσεγγίσεις δεν λειτουργούσαν καλά για τους πρώτους ανταποκριτές, όπου η κάλυψη και η οπτική επαφή δεν ανταποκρίνονταν στην πραγματική ανάγκη.

- Τα τρένα υψηλής ταχύτητας και τα λεωφορεία

Οι άνθρωποι σήμερα αναμένουν επίσης αξιόπιστες συνδέσεις στο Διαδίκτυο όταν ταξιδεύουν. Υπάρχει έντονη ζήτηση στην αγορά για βελτιωμένη εμπειρία Wi-Fi επιβατών. Ωστόσο, σε μερικά περιβάλλοντα όπως τρένα υψηλής ταχύτητας, αυτό μπορεί να είναι πολύ δύσκολο. Λόγω των συχνών μεταβιβάσεων μεταξύ των κυττάρων, της χαμηλής κάλυψης του δικτύου και της μεγάλης κυκλοφορίας που προκαλούν οι ταξιδιώτες επιχειρηματίες, η ποιότητα της υπηρεσίας μπορεί να είναι πολύ χαμηλή.

Πολλοί επιβάτες επιλέγουν το τρένο για μεγάλες διαδρομές επειδή τους παρέχει την ευκαιρία να δουλέψουν, να στείλουν e-mail ή να παρακολουθήσουν βίντεο και ταινίες online κατά τη διάρκεια του ταξιδιού τους. Ως αποτέλεσμα, οι συνδέσεις WLAN σε τρένα αποτελούν βασικό παράγοντα για τον ανταγωνισμό μεταξύ των φορέων εκμετάλλευσης σιδηροδρόμων στην Ευρώπη. Ωστόσο, οι τεχνικές προκλήσεις που αφορούν την κάλυψη και τη διαθεσιμότητα των υπηρεσιών καθιστούν δύσκολη την προσφορά υψηλής ευρυζωνικής πρόσβασης σε τρένα.

Η κάλυψη του παρόχου ποικίλλει σημαντικά και μπορεί να υπάρχουν «νεκρές ζώνες» για έναν μόνο φορέα εκμετάλλευσης. Δεδομένου ότι οι αμαξοστοιχίες περνούν ραδιοπύργους σε πολύ υψηλές ταχύτητες, υπάρχουν συχνές μεταφορές από κυψέλη σε κυψέλες, γεγονός που μπορεί να σημαίνει αύξηση του ποσοστού απώλειας πακέτων. Τα ποσοστά μεταφοράς μεταξύ της αμαξοστοιχίας και του πύργου ραδιοφώνου διαφέρουν από μερικά έως 200 χιλιοστά του δευτερολέπτου. Οι μεγάλοι χρόνοι μετάδοσης προκαλούν συχνές αποσυνδέσεις. Η μετάβαση μέσω νεκρών ζωνών, η αναμετάδοση των χαμένων πακέτων και η συχνή μεταβίβαση οδηγούν σε κακή εμπειρία χρήστη. Εάν ένας πάροχος δικτύου δεν παρέχει ικανοποιητική κάλυψη, μπορούν να επιτευχθούν βελτιωμένα αποτελέσματα συνδυάζοντας υπηρεσίες από πολλούς παρόχους.

Όταν χρησιμοποιείται μια ιδιαίτερα διαθέσιμη συνδετική σύνδεση, ένας αποτυχημένος σύνδεσμος δεν θα φέρει τη σύνδεση προς τα κάτω. Εάν συμβεί αυτό, οι επιβάτες σε ένα τρένο ή ένα λεωφορείο δεν θα το παρατηρήσουν. Όταν χρησιμοποιείτε WAN bonding σε τρένα ή λεωφορεία, υπάρχουν λιγότερες νεκρές ζώνες, πιο εύχρηστο εύρος ζώνης και λιγότερες αποσυνδέσεις, παρά την υψηλή ταχύτητα ταξιδιού και τις γρήγορες παραδόσεις πακέτων.

ΚΕΦΑΛΑΙΟ 3: Πρωτόκολλα ασφαλείας

3.1 IPSec (IP Security)

3.1.1 Εισαγωγή

Το Internet αποτελεί αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των

δεδομένων, της πλαστοπροσωπίας και της άρνησης παροχής υπηρεσιών. Ο στόχος της IPSec είναι η αντιμετώπιση όλων αυτών των προβλημάτων μέσα στην ίδια την υποδομή του δικτύου χωρίς να είναι αναγκαία η εγκατάσταση και η ρύθμιση ακριβών μηχανών και λογισμικού.

Η IPSec παρέχει κρυπτογράφηση στο επίπεδο του IP και για αυτό το λόγο αποτελεί ένα αξιοσημείωτο κομμάτι της συνολικής ασφάλειας. Οι προδιαγραφές της IPSec ορίζουν δύο νέους τύπους δεδομένων στα πακέτα: την επικεφαλίδα πιστοποίησης (AH-Authentication Header), για την παροχή υπηρεσίας ακεραιότητας δεδομένων και το φορτίο ενθυλάκωσης ασφάλειας (ESP-Encapsulating Security Payload) το οποίο παρέχει πιστοποίηση ταυτότητας και ακεραιότητα δεδομένων. Ορίζονται επίσης οι παράμετροι επικοινωνίας μεταξύ δύο συσκευών που είναι η διαχείριση των κλειδιών και η συσχετισμοί ασφάλειας (security associations).

3.1.2 Γιατί χρειαζόμαστε την IPSec

- Απώλεια του Απορρήτου (Loss of Privacy)

Κάποιος που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνηση των τελευταίων στο Internet. Αυτή η δυνατότητα είναι ίσως ο μεγαλύτερος ανασταλτικός παράγοντας στις επικοινωνίες μεταξύ των επιχειρήσεων σήμερα. Χωρίς τη χρήση κρυπτογραφικών μεθόδων κάθε μήνυμα είναι ανοικτό προς ανάγνωση από όποιον έχει τη δυνατότητα να το αιχμαλωτίσει Το CERT (Computer Emergency Response Team Coordination Center) αναφέρεται στα προγράμματα "packet sniffers" ως την πιο συνηθισμένη περίπτωση επίθεσης από αυτές που συναντώνται, λέγοντας:

"Οι εισβολείς συνηθίζουν να εγκαθιστούν packet sniffers σε συστήματα που έχουν εκτεθεί σε κάθε είδους κίνδυνο μετά την απώλεια της μυστικότητας του root password. Αυτά τα προγράμματα, που συλλέγουν ονόματα και κωδικούς, εγκαθίστανται σαν μέρος ενός kit το οποίο αντικαθιστά επιπλέον κοινά αρχεία του συστήματος με προγράμματα που δείχνουν ότι κάνουν αυτό που θα έπρεπε αλλά στην πραγματικότητα εκτελούν άλλες λειτουργίες (Trojan horse programs). Αυτά τα kit παρέχουν οδηγίες οι

οποίες καθιστούν και τον αρχάριο χρήστη τους επικίνδυνο για την ασφάλεια ενός απροστάτευτου δικτύου".

- Απώλεια της Ακεραιότητας των Δεδομένων (Loss of Data Integrity)

Ακόμα και για δεδομένα που δεν είναι εμπιστευτικά πρέπει να λαμβάνονται μέτρα διασφάλισης της ακεραιότητάς τους. Μπορεί να μην μας ενδιαφέρει εάν κάποιος "δει" τη κίνηση ρουτίνας της δουλείας μας, αλλά σίγουρα θα μας προβλημάτιζε εάν αυτός αλλοίωνε κατά οποιοδήποτε τρόπο τα δεδομένα αυτά. Για παράδειγμα το να μπορεί κάποιος να πιστοποιεί με ασφάλεια τον εαυτό του στη τράπεζα κάνοντας χρήση ψηφιακών πιστοποιητικών δεν είναι αρκετό εάν η κύρια εργασία του στη τράπεζα θα μπορούσε να αλλοιωθεί με κάποιο τρόπο.

- Πλαστοπροσωπία (Identity Spoofing)

Εκτός της προστασίας των ίδιων των δεδομένων, θα πρέπει να παίρνουμε μέτρα ώστε να προστατεύεται και η ταυτότητά μας στο Internet. Πολλά συστήματα ασφάλειας, σήμερα, βασίζονται στην IP διεύθυνση για να αναγνωρίσουν μοναδικά τους χρήστες. Τα συστήματα αυτά είναι πολύ εύκολο να ξεγελαστούν και αυτό το γεγονός έχει οδηγήσει σε αναρίθμητα τρυπήματα διαφόρων συστημάτων. Το CERT έχει αναφερθεί σε αυτού του είδους την επίθεση : "Συνεχίζουμε να λαμβάνουμε αρκετές αναφορές που μιλάνε για επιθέσεις τύπου IP Spoofing. Οι εισβολείς επιτίθενται χρησιμοποιώντας αυτοματοποιημένα εργαλεία που κυκλοφορούν ελευθέρα στο Internet. Κάποια sites πίστευαν, λανθασμένα, ότι σταματούσαν τέτοιου είδους επιθέσεις ενώ άλλα σχεδίαζαν να το κάνουν αλλά δεν είχαν προλάβει να το εφαρμόσουν".

- Άρνηση Παροχής Υπηρεσιών (Denial-of-Service)

Εφόσον κάποιος οργανισμός εκμεταλλεύεται το Internet, πρέπει να λάβει κάποια μέτρα ώστε να διασφαλίσει τη διαθεσιμότητα του συστήματός του σε αυτό. Τα τελευταία χρόνια διάφοροι hackers έχουν βρει αδυναμίες στο πρωτόκολλο TCP/IP που τους δίνει τη δυνατότητα να "ρίχνουν" τις μηχανές. Το CERT έχει μιλήσει για το θέμα : "Ο αριθμός των επιθέσεων εναντίον συστημάτων έχει αυξηθεί σημαντικά αφού υπάρχουν πλέον πακέτα που κυκλοφορούν ελευθέρα και που κάνουν εύκολη την πραγματοποίηση τέτοιου είδους επιθέσεων".

3.1.3 Ορισμός

Η IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών. Είναι βασισμένο στις προδιαγραφές που ανέπτυξε η ομάδα εργασίας του Internet (IETF). Η IPSec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο. Η IPSec παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφάλειας σε ένα δίκτυο.

Πριν την άφιξη της IPSec στο προσκήνιο, εφαρμόζονταν αποσπασματικές λύσεις που αντιμετώπιζαν μέρος μόνο του προβλήματος. Για παράδειγμα, το SSL(Secure Sockets Layer) παρέχει κρυπτογράφηση σε επίπεδο εφαρμογής για Web browsers και άλλες εφαρμογές. Το SSL προστατεύει την πιστότητα των δεδομένων που στέλνονται από κάθε εφαρμογή που το χρησιμοποιεί, αλλά δεν προστατεύει τα δεδομένα που αποστέλλονται από άλλες εφαρμογές. Κάθε σύστημα και εφαρμογή πρέπει να είναι προστατεμένη από το SSL για να του παρέχει το τελευταίο την προστασία.

Οργανισμοί όπως ο στρατός χρησιμοποιούσαν για χρόνια κρυπτογράφηση επιπέδου συνδέσμου. Σε αυτό το σχήμα κάθε σύνδεσμος επικοινωνιών προστατεύεται από ένα ζεύγος συσκευών κρυπτογράφησης - μια στο τέλος κάθε πλευράς του συνδέσμου. Αν και αυτό το σύστημα παρέχει εξαιρετική ασφάλεια δεδομένων είναι πολύ δύσκολο να παρακολουθηθεί και να διαχειριστεί. Επιπλέον απαιτεί η κάθε πλευρά του συνδέσμου στο δίκτυο να είναι ασφαλής διότι τα δεδομένα είναι σε καθαρή μορφή σε αυτά τα σημεία. Φυσικά αυτό το σχήμα δεν μπορεί να δουλέψει καθόλου στο

Internet όπου πιθανότατα κανένας από τους ενδιάμεσους συνδέσμους δεν είναι προσβάσιμος σε κανέναν και δεν εμπιστεύεται κανέναν.

3.1.4 Πιστοποίηση Ταυτότητας

Για την πιστοποίηση της ταυτότητας μεταξύ δύο οντοτήτων στο IPSEC, υλοποιούνται οι παρακάτω μηχανισμοί.

• Προ-Μοιρασμένα Κλειδιά—το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας hash συνάρτησης) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.

• Κρυπτογράφηση Δημοσίων Κλειδιών—κάθε μηχανή "γεννάει" έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το public key (δημόσιο κλειδί) της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια hash συνάρτηση του τυχαίου αριθμού αποκρυπτογραφώντας με τα private keys (ιδιωτικά κλειδιά) ότι λαμβάνουν από το συνομιλητή τους. Το σύστημα παρέχει ακόμα και δυνατότητα άρνησης συμμετοχής σε οποιαδήποτε διαδικασία πιστοποίησης. Προς το παρόν μόνο ο αλγόριθμος δημοσίων κλειδιών της RSA υποστηρίζεται.

• Ψηφιακές Υπογραφές—κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Αυτή η μέθοδος είναι παρόμοια με την προηγούμενη μόνο που δεν παρέχει μηχανισμό άρνησης της εμπλοκής της σε κάποια προσπάθεια πιστοποίησης. Προς το παρόν υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

3.2 Secure Socket Layer (SSL)

3.2.1 Γενικά

Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0) και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή RFC (Request For Comments). Τον Δεκέμβριο του 1994 εκδίδεται μια επαναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0). Η παρούσα έκδοση του SSL, version 3.0, παρουσιάσθηκε στο κοινό στα τέλη του 1995, ενώ από τα μέσα του 1995 είχε αρχίσει να εφαρμόζεται σε προϊόντα της εταιρίας, όπως τον Netscape Navigator.

Επειδή η Netscape επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου γεγονός που ερχόταν σε σύγκρουση με τους νόμους των Ηνωμένων Πολιτειών περί εξαγωγή κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει την χρήση ασθενών αλγορίθμων στις εξαγόμενες εφαρμογές. Πιο συγκεκριμένα, δημιούργησε παραλλαγές των αλγόριθμων RC4-128 και RC2-128 που στην πραγματικότητα χρησιμοποιούν κλειδιά των 40 bits.

3.2.2 Εισαγωγή στο SSL

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος,

εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Όλα τα παραπάνω γίνονται με τρόπο διαφανές και απλό.

Η έκδοση 3 του πρωτοκόλλου κάλυψε πολλές αδυναμίες της δεύτερης. Οι σημαντικότερες αλλαγές έχουν να με την μείωση των απαραίτητων μηνυμάτων κατά το handshake για την εγκαθίδρυση της σύνδεσης, την επιλογή των αλγόριθμων συμπίεσης και κρυπτογράφησης από τον server και την εκ νέου διαπραγμάτευση του master-key και session-id. Ακόμα αυξάνονται οι διαθέσιμοι αλγόριθμοι και προστίθενται νέες τεχνικές για την διαχείριση των κλειδιών.

Συμπερασματικά μπορούμε να πούμε πως η έκδοση 3 του SSL είναι πιο ολοκληρωμένη σχεδιαστικά, με μεγαλύτερο εύρος υποστήριξης εφαρμογών και λιγότερες ατέλειες. Παρ' όλο που είναι συμβατή με την δεύτερη έκδοση, η χρήση της τελευταίας δεν πρέπει να προτιμάται.

Το SSL μπορεί να τοποθετηθεί στην κορυφή οποιουδήποτε πρωτοκόλλου μεταφοράς, δεν εξαρτάται από την ύπαρξη του TCP/IP και τρέχει κάτω από πρωτόκολλα εφαρμογών όπως το HTTP, FTP και TELNET.

3.2.3 Υποστηριζόμενοι Αλγόριθμοι

Οι αλγόριθμοι κρυπτογράφησης χωρίζονται στους stream ciphers και στους block ciphers. Στους stream ciphers ανήκουν οι RC4 με κλειδιά 40 bits και 128 bits. Στους block ciphers ανήκουν οι RC2 με κλειδιά 40 και 128 bits, οι DES, DES40, Triple DES και οι IDEA και Fortezza.

Οι αλγόριθμοι για την παραγωγή των hash και digest values για τα MACs είναι ο MD5 (128-bit hash) και ο SHA (160-bit hash).

Οι τεχνικές διαχείρισης των κλειδιών (key management) διακρίνονται στους: την ασύμμετρη κρυπτογραφία με RSA, την τεχνική Diffie-Hellman. Τα πιστοποιητικά είναι της μορφής X.509. Ο RSA μαζί με τον DSS και τον Fortezza μπορούν να χρησιμοποιηθούν για την ψηφιακή υπογραφή των κλειδιών κρυπτογράφησης.

Προσφέρεται και η δυνατότητα επιλογής ανασφάλιστης επικοινωνίας, αλλά δεν συνιστάται.

3.2.4 SSL Handshake Protocol

Το πρωτόκολλο SSL Handshake διαχωρίζεται σε δύο επιμέρους φάσεις: η πρώτη φάση αφορά την επιλογή των αλγόριθμων, την ανταλλαγή ενός master key και την πιστοποίηση της ταυτότητας του server. Η δεύτερη φάση διαχειρίζεται την πιστοποίηση της ταυτότητας του client (εάν ζητηθεί) και ολοκληρώνει την διαδικασία του handshaking. Όταν το ολοκληρωθούν και οι δύο φάσεις, το στάδιο του handshake τελειώνει και η μεταφορά μεταξύ των δύο άκρων αρχίζει. Όλα τα μηνύματα κατά την διάρκεια του handshaking και μετά στέλνονται σύμφωνα με το SSL Record Protocol.

Το πακέτο των αλγορίθμων κρυπτογράφησης (Cipher Suite) περιλαμβάνει την μέθοδο για την ανταλλαγή των κλειδιών, τον αλγόριθμο κρυπτογράφησης και τον μηχανισμό για την παραγωγή του MAC.

3.2.5 Αντοχή του SSL σε Γνωστές Επιθέσεις

- **Dictionary Attack**

Αυτό το είδος της επίθεσης λειτουργεί όταν ένα μέρος του μη κρυπτογραφημένου κειμένου είναι στην κατοχή του ανέντιμων προσώπων. Το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί.

Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα των 128 bit. Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα,

υποστηρίζουν 128 bit κλειδιά και παρ' όλο που τα 88 bit αυτών μεταδίδονται ανασφάλιστα, ο υπολογισμός 2^{40} διαφορετικών ακολουθιών κάνει την επίθεση αδύνατο να επιτύχει.

- **Brute Force Attack**

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι τελείως ανούσια. Μόνο ο DES56 bit cipher είναι ευαίσθητος σε αυτήν την επίθεση, αλλά η χρήση του δεν συνιστάται.

- **Replay Attack**

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση replay attack. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id και το σύνολο των είδη χρησιμοποιημένων μηνυμάτων δεν γίνονται δεκτά από τον server. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.

- **Man-In-The-Middle-Attack**

Η επίθεση Man-In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα.

Το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατον. Μην ξεχνάμε την δυνατότητα επικοινωνίας των κλειδιών υπογεγραμμένα.

3.2.6 Αδυναμίες του SSL

- **Brute Force Attack Εναντίον Αδύναμων Αλγορίθμων**

Η μεγαλύτερη αδυναμία του πρωτοκόλλου είναι η ευαισθησία των αλγόριθμων που χρησιμοποιούν μικρά κλειδιά. Συγκεκριμένα, οι RC4-40, RC2-40 και DES-56 εισάγουν σοβαρά προβλήματα ασφαλείας και θα πρέπει να αποφεύγονται.

- **Renegotiation of Session Keys (μόνο στην 2 έκδοση)**

Από την στιγμή που μία σύνδεση δημιουργηθεί, το ίδιο master key χρησιμοποιείται καθ' όλη την διάρκεια της. Όταν το SSL χρησιμοποιείται πάνω από μια μακρόχρονη σύνδεση (π.χ. μιας TELNET εφαρμογής), η αδυναμία αλλαγής του master key γίνεται επικίνδυνη. Η καλύτερη μέθοδος επίλυσης αυτού του προβλήματος είναι η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα, μειώνοντας έτσι την πιθανότητα μιας επιτυχής Brute Force Attack.

3.2.7 Χρήσεις του SSL

Η πιο κοινή του εφαρμογή είναι για την διασφάλιση HTTP επικοινωνιών μεταξύ του browser και του web server. Η ασφαλή έκδοση του HTTP χρησιμοποιεί URLs που ξεκινούν με "https" αντί του κανονικού "http" και διαφορετική πόρτα (port) που είναι η προκαθορισμένη στην 443. Ο browser αποθηκεύει τα ιδιωτικά κλειδιά του χρήστη και με κατάλληλο τρόπο υποδεικνύει την διενέργεια ασφαλών συνδέσεων.

Παρ' όλο που μπορεί κανείς να γράψει μια εφαρμογή του SSL ακολουθώντας τα Internet drafts και RFCs, είναι προτιμότερο να χρησιμοποιήσει μία από τις υπάρχοντες βιβλιοθήκες εργαλείων του SSL (SSL toolkit Libraries). Τέτοιες βιβλιοθήκες περιέχούν ρουτίνες για κρυπτογράφηση, digestion, και διαχείριση πιστοποιητικών και διακρίνονται στις ακόλουθες:

- SSLRef
- SSLPlus
- SSLava
- SSLeay

3.3 Secure MIME

3.3.1 Γενικά

Το S/MIME είναι μια εξειδίκευση του πρωτοκόλλου MIME και αναπτύχθηκε για την ασφαλή ανταλλαγή ηλεκτρονικών μηνυμάτων. Σκοπός του είναι η καταπολέμηση της πλαστογραφίας και της υποκλοπής ηλεκτρονικών μηνυμάτων καθώς και η ευκολία στην χρήση. Σχεδιάστηκε ώστε να μπορεί εύκολα να ενοποιηθεί σε προϊόντα ηλεκτρονικού ταχυδρομείου, επεκτείνοντας το πρωτόκολλο MIME σύμφωνα με ένα σύνολο κρυπτογραφικών τυποποιήσεων, το Public Key Cryptography Standards (PKCS).

Η παγκόσμια υιοθέτηση του S/MIME θα επωφελήσει τους χρήστες, αφού έννοιες όπως η ακεραιότητα των δεδομένων, η αυθεντικότητα και η διαφύλαξη του απόρρητου των συναλλαγών (privacy), θα είναι διαθέσιμες σε όλους.

Το S/MIME είναι ένα πρωτόκολλο που χρησιμοποιείται από προγράμματα ηλεκτρονικού ταχυδρομείου για την εφαρμογή κρυπτογραφικών υπηρεσιών σε αποστέλλοντα μηνύματα και για την επεξεργασία προστατευμένων παραληφθέντων. Η δεύτερη έκδοση του S/MIME είναι επί του παρόντος ενσωματωμένη σε πολλά δημοφιλή προϊόντα, όπως τα Lotus Domino, Netscape Communicator, Novell

GroupWise και Microsoft Exchange. Το S/MIME δίνει την δυνατότητα σε εταιρίες που σχεδιάζουν λογισμικό να αναπτύσσουν προγράμματα τέτοια ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί από ένα άλλο.

Η ομάδα Internet Engineering Task Force (IETF) αναπτύσσει την 3η έκδοση του S/MIME που περιλαμβάνει την εξειδίκευση Cryptographic Message Syntax (CMS) που ορίζει μια τυποποιημένη σύνταξη για την επικοινωνία των κρυπτογραφικών πληροφοριών που είναι ανεξάρτητες από την μορφή των ενθυλακωμένων περιεχομένων ή από τον μηχανισμό μεταφοράς. Κάθε τύπος δεδομένων μπορεί να προστατευθεί από το CMS. Εκτός από τις εφαρμογές S/MIME, το CMS μπορεί να χρησιμοποιηθεί με τα πρωτόκολλα HTTP, X.400, FTP, SSL και SET. Η στρατηγική ανάπτυξης της τρίτης έκδοσης είναι τέτοια ώστε να διατηρείται

η συμβατότητα με την προηγούμενη έκδοση (version 2). Αυτό επιτυγχάνεται με την πρόσθεση νέων, προαιρετικών στοιχείων στην νέα έκδοση, των οποίων η απουσία στις επικεφαλίδες επιτρέπει την συνεργασία των δύο εκδόσεων.

Επίσης, η έκδοση 3 του S/MIME απαιτεί την ύπαρξη ενός ελάχιστου συνόλου κρυπτογραφικών αλγορίθμων που διασφαλίζουν την συνεργασίας μεταξύ διαφορετικών εφαρμογών.

3.3.2 Δημιουργία S/MIME μηνυμάτων

Τα μηνύματα S/MIME είναι συνδυασμός MIME μηνυμάτων και CMS αντικειμένων. Τα CMS αντικείμενα περιγράφουν το είδος της ασφάλειας που θέλουμε να εφαρμόσουμε και μπορεί να είναι Ψηφιακός Φάκελος (Enveloped-Data), Υπογεγραμμένα δεδομένα (Signed-Data) και άλλα. Μπορούν να χρησιμοποιηθούν όλοι οι τύποι δεδομένων του MIME, χωρίς κανένα περιορισμό. Το MIME μήνυμα, μαζί με άλλες πληροφορίες (πιστοποιητικά, αναγνωριστικά αλγόριθμων κ.α.), επεξεργάζονται από τις διαδικασίες του CMS και παράγεται το CMS αντικείμενο. Τέλος, το CMS αντικείμενο τυλίγεται σε εξωτερικό MIME μήνυμα με κατάλληλες επικεφαλίδες.

3.4 PGP: Pretty Good Privacy

3.4.1 Εισαγωγή

Το λογισμικό Pretty Good Privacy (PGP), το οποίο σχεδιάστηκε από τον Phill Zimmerman, είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX/VMS και για άλλες πλατφόρμες. Το PGP επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.

- Διασφάλιση του απορρήτου σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το διαβάσει.
- Πιστοποίηση της ταυτότητας σημαίνει ότι μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο.
- Ευκολία σημαίνει ότι η διασφάλιση του απόρρητου και η πιστοποίησης της ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία. Δεν είναι αναγκαία ασφαλή κανάλια για την ανταλλαγή κλειδιών μεταξύ χρηστών κάτι που κάνει το PGP πολύ ευκολότερο στη χρήση από κάθε άλλο αντίστοιχο πακέτο. Αυτό συμβαίνει διότι το PGP είναι βασισμένο σε μια δυναμική νέα τεχνολογία που καλείται κρυπτογράφηση "δημοσίων κλειδιών" (public key).

Το PGP συνδυάζει την ευκολία του RSA κρυπτοσυστήματος δημοσίων κλειδιών με την ταχύτητα της συμβατικής κρυπτογράφησης, περιλήψεις μηνυμάτων για ψηφιακές υπογραφές, συμπίεση δεδομένων πριν την κρυπτογράφηση, καλός εργονομικός σχεδιασμός και υψηλού επιπέδου διαχείριση κλειδιών. Επιπλέον το PGP εκτελεί τις λειτουργίες των δημοσίων κλειδιών γρηγορότερα από τα περισσότερα αντίστοιχα προγράμματα. Το PGP είναι κρυπτογράφηση δημοσίων κλειδιών για τις μάζες.

Σήμερα εάν η κυβέρνηση θελήσει να παραβιάσει το απόρρητο των πολιτών πρέπει να καταβάλλει ένα συγκεκριμένο ποσό χρημάτων και εργασίας για να υποκλέψει και να διαβάσει το συμβατικό ταχυδρομείο και να ακούσει ή να υποκλέψει τηλεφωνικές συνομιλίες. Αυτός ο τρόπος της παρακολούθησης δεν είναι πρακτικός σε μεγάλο επίπεδο. Αυτό συμβαίνει μόνο σε σημαντικές περιπτώσεις όπου φαίνεται ότι αξίζει.

Όλο και μεγαλύτερο ποσοστό από τις ιδιωτικές μας επικοινωνίες δρομολογείται μέσω ηλεκτρονικών καναλιών. Το ηλεκτρονικό ταχυδρομείο σταδιακά αντικαθιστά το συμβατικό ταχυδρομείο. Τα μηνύματα e-mail είναι πολύ εύκολο να υποκλέπτουν και να περάσουν από διαδικασία ανίχνευσης βάσει καθορισμένων λέξεων-κλειδιών (keywords). Αυτό μπορεί να γίνει εύκολα, αυτόματα και χωρίς να πέσει στην αντίληψη κανενός σε μεγάλο επίπεδο. Οι διεθνείς συνδέσεις βρίσκονται ήδη κάτω από μια τέτοια διαδικασία παρακολούθησης από την NSA.

Κινούμαστε προς ένα μέλλον όπου οι υπολογιστές διεθνώς θα ενώνονται με δίκτυα οπτικών ινών υψηλής χωρητικότητας. Το e-mail θα είναι κάτι το αυτονόητο για όλους και όχι η καινοτομία που θεωρείται σήμερα. Οι κυβερνήσεις θα προστατεύουν το e-mail των πολιτών με πρωτόκολλα σχεδιασμένα από τις ίδιες. Πιθανότατα οι περισσότεροι άνθρωποι θα συμβιβαστούν με αυτή τη λύση αλλά ίσως μερικοί προτιμήσουν να πάρουν τα δικά τους μέτρα ασφάλειας.

3.4.2 Λειτουργία Του PGP

Για να κατανοήσουμε τη λειτουργία του PGP θα πρέπει να αναφέρουμε λίγα λόγια πάνω στην ορολογία που χρησιμοποιείται. Ας θεωρήσουμε ότι θέλει κάποιος να στείλει ένα μήνυμα αλλά δεν θέλει να το διαβάσει κανένας άλλος εκτός από τον παραλήπτη. Μπορεί να το κρυπτογραφήσει με τη χρήση ενός κλειδιού το οποίο θα πρέπει να χρησιμοποιηθεί στην αποκρυπτογράφηση του μηνύματος από τον παραλήπτη του—τουλάχιστον έτσι δουλεύει η συμβατική κρυπτογραφία ενός κλειδιού.

Στα συμβατικά κρυπτοσυστήματα, όπως το DES, ένα και μόνο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτό σημαίνει ότι το κλειδί θα πρέπει να μεταδοθεί αρχικά μέσα από ένα ασφαλές

κανάλι έτσι ώστε και τα δυο μέρη να το γνωρίζουν προτού αρχίσει η αποστολή κρυπτογραφημένων μηνυμάτων μέσω ασφαλών καναλιών. Αυτό δεν είναι και τόσο βολικό διότι αν έχεις ένα ασφαλές κανάλι για να ανταλλάζεις κλειδιά τότε τι χρειάζεσαι την κρυπτογραφία;

Στα κρυπτοσυστήματα δημοσίων κλειδιών ο καθένας έχει δυο συμπληρωματικά κλειδιά. Ένα που δίδεται δημόσια (public key) και ένα μυστικό (secret key ή private key). Το κάθε κλειδί ξεκλειδώνει τον κώδικα που το άλλο φτιάχνει. Η γνώση του δημοσίου κλειδιού δεν βοηθάει στην εξαγωγή του αντίστοιχου μυστικού κλειδιού. Το δημόσιο κλειδί μπορεί να διατεθεί σε ένα δίκτυο επικοινωνιών. Αυτό το πρωτόκολλο παρέχει διασφάλιση του απόρρητου χωρίς την ανάγκη ύπαρξης ασφαλών καναλιών, όπως απαιτεί η συμβατική κρυπτογραφία.

Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη ενός μηνύματος για να κρυπτογραφήσει ένα μήνυμα προς αυτό το άτομο ενώ ο παραλήπτης μπορεί να χρησιμοποιήσει με τη σειρά του το αντίστοιχο μυστικό κλειδί για να αποκρυπτογραφήσει το μήνυμα. Κανένας άλλος εκτός από τον παραλήπτη δεν μπορεί να το αποκρυπτογραφήσει διότι κανένας άλλος δεν έχει πρόσβαση στο μυστικό κλειδί - ακόμη και το άτομο που κρυπτογράφησε το μήνυμα.

Επίσης παρέχεται υπηρεσία πιστοποίησης του μηνύματος. Το μυστικό κλειδί του αποστολέα μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος άρα και για την υπογραφή του. Έτσι δημιουργείται μια ψηφιακή υπογραφή του μηνύματος την οποία ο παραλήπτης ή οποιοσδήποτε άλλος μπορεί να ελέγξει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να την αποκρυπτογραφήσει. Αυτό αποδεικνύει ότι ο αποστολέας ήταν ο πραγματικός δημιουργός του μηνύματος και ότι το μήνυμα δεν αλλοιώθηκε από κάποιον άλλον διότι μόνο ο αποστολέας έχει στην κατοχή του το μυστικό κλειδί που έφτιαξε την υπογραφή. Η πλαστογράφηση ενός υπογεγραμμένου μηνύματος δεν είναι εφικτή και ο αποστολέας δεν μπορεί μετά να απαρνηθεί την υπογραφή του.

Αυτές οι δυο διαδικασίες μπορούν να συνδυαστούν για την παροχή τόσο διασφάλισης του απόρρητου όσο και πιστοποίησης της ταυτότητας αφού μπορεί κάποιος πρώτα να υπογράψει ένα μήνυμα με το μυστικό κλειδί του και μετά να το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης αντιστρέφει αυτά τα βήματα αποκρυπτογραφώντας πρώτα το μήνυμα με το μυστικό κλειδί του και

κατόπιν ελέγχοντας την ψηφιακή υπογραφή που περιέχεται σε αυτό με το δημόσιο κλειδί του αποστολέα. Αυτές οι διαδικασίες γίνονται αυτόματα από το λογισμικό του παραλήπτη.

Επειδή ο αλγόριθμος της κρυπτογράφησης δημοσίων κλειδιών είναι πολύ πιο αργός από τη συμβατική κρυπτογράφηση ενός κλειδιού η κρυπτογράφηση επιτυγχάνεται καλύτερα με τη χρήση ενός υψηλής ποιότητας γρήγορου αλγόριθμου συμβατικής κρυπτογράφησης ενός κλειδιού για την κρυπτογράφηση του μηνύματος. Το αρχικό μη κρυπτογραφημένο μήνυμα καλείται "απλό κείμενο". Σε μια διαδικασία αόρατη στο χρήστη ένα προσωρινό τυχαίο κλειδί, το οποίο έχει δημιουργηθεί μόνο για τη συγκεκριμένη φορά, χρησιμοποιείται για να κρυπτογραφηθεί συμβατικά το αρχείο "απλό κείμενο". Μετά το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για να κρυπτογραφηθεί αυτό το προσωρινό κλειδί. Αυτό το συμβατικά δημιουργημένο κλειδί μιας φοράς (session key) το οποίο έχει κρυπτογραφηθεί και με τη διαδικασία του δημόσιου κλειδιού αποστέλλεται μαζί με το κρυπτογραφημένο κείμενο (κρυπτοκείμενο) στον παραλήπτη. Ο παραλήπτης χρησιμοποιεί το δικό του μυστικό κλειδί για να ανακτήσει το session key και μετά χρησιμοποιεί αυτό κλειδί για να τρέξει τον γρήγορο συμβατικό αλγόριθμο ενός κλειδιού έτσι ώστε να αποκρυπτογραφήσει το κρυπτοκείμενο. Τα δημόσια κλειδιά φυλάσσονται σε ξεχωριστά πιστοποιητικά κλειδιών (key certificates) τα οποία περιλαμβάνουν την ταυτότητα του ιδιοκτήτη τους (το όνομα του ιδιοκτήτη), μια σφραγίδα χρόνου που δείχνει πότε το ζεύγος των κλειδιών δημιουργήθηκε και τέλος το ίδιο το υλικό του κλειδιού. Τα πιστοποιητικά δημοσίων κλειδιών περιλαμβάνουν το υλικό των δημοσίων κλειδιών ενώ τα πιστοποιητικά των μυστικών κλειδιών περιλαμβάνουν το υλικό των μυστικών κλειδιών. Κάθε μυστικό κλειδί κρυπτογραφείται επιπλέον με τον κωδικό του σε περίπτωση που κλαπεί. Ένα αρχείο κλειδιών ή ένα μπρελόκ κλειδιών (key ring) περιέχει ένα ή περισσότερα από αυτά τα πιστοποιητικά κλειδιών. Τα δημόσια μπρελόκ περιέχουν τα δημόσια πιστοποιητικά κλειδιών ενώ τα ιδιωτικά μπρελόκ περιέχουν τα ιδιωτικά πιστοποιητικά κλειδιά.

Τα κλειδιά χαρακτηρίζονται από ένα "key id" (ταυτότητα κλειδιού) η οποία είναι μια συντομογραφία του δημόσιου κλειδιού (τα 64 λιγότερο σημαντικά bits του δημοσίου κλειδιού). Όταν αυτή η ταυτότητα παρουσιάζεται μόνο τα 32 λιγότερο σημαντικά bits δίνονται για επιπλέον ελαχιστοποίηση του όγκου της ταυτότητας.

Καθώς πολλά κλειδιά μπορεί να μοιράζονται το ίδιο user id (ταυτότητα χρήστη), για πρακτικούς λόγους κανένα κλειδί δεν μοιράζεται το ίδιο key id με κανένα άλλο.

Το PGP χρησιμοποιεί τις περιλήψεις μηνυμάτων (message digests) για να δημιουργήσει υπογραφές. Μια περίληψη μηνύματος είναι μια κρυπτογραφικά πολλή δυνατή μονόδρομη (hash) συνάρτηση 128 bit του μηνύματος. Είναι κάτι ανάλογο με το "check sum" ή CRC κώδικα ελέγχου στο ότι αντιπροσωπεύουν συμπαγώς το μήνυμα και χρησιμοποιούνται για την ανίχνευση αλλαγών σε αυτό. Αντίθετα βέβαια με το CRC είναι υπολογιστικά αδύνατο για κάποιον επιτιθέμενο να φτιάξει ένα υποκατάστατο μήνυμα το οποίο θα μπορούσε να παράγει την ίδια περίληψη μηνύματος. Η περίληψη μηνύματος κρυπτογραφείται με το μυστικό κλειδί και έτσι σχηματίζει την ψηφιακή υπογραφή.

Τα κείμενα υπογράφονται με την εισαγωγή στην αρχή τους ψηφιακών πιστοποιητικών υπογραφών οι οποίες περιέχουν το key id του κλειδιού που χρησιμοποιήθηκε για την υπογραφή τους, μια υπογεγραμμένη με το μυστικό κλειδί περίληψη του κειμένου και μια χρονική σφραγίδα της δημιουργίας της υπογραφής. Το key id χρησιμοποιείται από τον παραλήπτη για την ανεύρεση του δημόσιου κλειδιού του αποστολέα έτσι ώστε να ελέγξει την ψηφιακή υπογραφή. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το δημόσιο κλειδί του αποστολέα και το user id του στο μπρελόκ δημοσίων κλειδιών που έχει στην κατοχή του ο παραλήπτης.

Τα κρυπτογραφημένα αρχεία περιέχουν στην αρχή τους το key id του δημοσίου κλειδιού που χρησιμοποιήθηκε στην κρυπτογράφησή τους. Ο παραλήπτης χρησιμοποιεί αυτό το key id για την ανεύρεση του μυστικού κλειδιού που απαιτείται για την αποκρυπτογράφηση του μηνύματος. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το απαραίτητο μυστικό κλειδί αποκρυπτογράφησης στο μπρελόκ μυστικών κλειδιών του παραλήπτη.

Αυτοί οι δυο τύποι μπρελόκ κλειδιών είναι η κύρια μέθοδος της αποθήκευσης και διαχείρισης των δημόσιων και ιδιωτικών κλειδιών. Αντί να κρατάμε ξεχωριστά κλειδιά σε ξεχωριστά αρχεία κλειδιών τα μαζεύουμε σε μπρελόκ κλειδιών έτσι ώστε να διευκολύνουμε την αυτόματη ανεύρεσή τους είτε με τη χρήση του key id είτε με τη χρήση του user id. Κάθε χρήστης διατηρεί το δικό του ζεύγος μπρελόκ. Ένα ξεχωριστό δημόσιο κλειδί αποθηκεύεται προσωρινά σε ένα ξεχωριστό αρχείο μόνο για το χρόνο

που χρειάζεται για την αποστολή του σε κάποιο φίλο ο οποίος κατόπιν θα το προσθέσει στο δικό του μπρελόκ κλειδιών.

3.4.3 Προστασία Δημοσίων Κλειδιών

Σε ένα κρυπτοσύστημα δημοσίων κλειδιών δεν υπάρχει ανάγκη προστασίας των δημοσίων κλειδιών, διότι το επιδιωκόμενο είναι η όσο το δυνατόν ευρύτερη διάδοσή τους. Το σημαντικό και αυτό που θα πρέπει να διασφαλίζεται είναι το να είμαστε σίγουροι ότι κάποιο δημόσιο κλειδί που φαίνεται ότι ανήκει σε κάποιον, όντως να ανήκει σε αυτόν. Αυτό μπορεί να είναι και το πιο σημαντικό μειονέκτημα του κρυπτοσυστήματος δημόσιων κλειδιών.

Κάποιο άτομο που τυγχάνει ευρείας εμπιστοσύνης θα μπορούσε να εξειδικευτεί στην παροχή αυτής της υπηρεσίας, δηλαδή της παροχής υπογραφών σε πιστοποιητικά δημοσίων κλειδιών άλλων χρηστών. Αυτό το κοινά αποδεκτό άτομο θα μπορούσε να είναι κάποιος "key server" ή κάποια υπηρεσία πιστοποίησης. Κάθε πιστοποιητικό δημόσιου κλειδιού που φέρει την υπογραφή αυτού του key server θα μπορεί να θεωρείται γνήσιο και έτσι άξιο της εμπιστοσύνης κάποιου. Το μόνο που χρειάζεται να κάνουν όσοι χρήστες θα ήθελαν να συμμετέχουν σε αυτή τη διαδικασία είναι να αποκτήσουν ένα καλό αντίγραφο του δημοσίου κλειδιού του key server έτσι ώστε να είναι σε θέση να επιβεβαιώσουν την υπογραφή αυτού.

Κάποιος κεντρικός key server ή μια υπηρεσία πιστοποίησης, θα ήταν κατάλληλη για κάποια μεγάλη και απρόσωπη επιχείρηση ή κυβερνητική υπηρεσία.

Η αποκεντρωμένη έκδοση του σχήματος αυτού είναι εκείνη που επιτρέπει σε όλους τους χρήστες να δρουν σαν μεσάζοντες, ο ένας για τον άλλο,κάτι που έχει καλύτερα αποτελέσματα από έναν και μοναδικό key server. Το PGP τείνει προς αυτή τη κατεύθυνση διότι αντανακλά καλύτερα το φυσικό τρόπο με τον οποίο αλληλεπιδρούν μεταξύ τους οι άνθρωποι στις σχέσεις τους και ταυτόχρονα επιτρέπει σε αυτούς να διαλέξουν ποιόν εμπιστεύονται για τη διαχείριση των κλειδιών τους.

Αυτή ολόκληρη η διαδικασία της προστασίας των δημοσίων κλειδιών είναι το μοναδικό δύσκολο πρόβλημα στις πρακτικές εφαρμογές της κρυπτογράφησης

δημοσίων κλειδιών. Θα μπορούσαμε να πούμε ότι είναι η Αχίλλειος φτέρνα της κρυπτογράφησης δημοσίων κλειδιών και έχει καταβληθεί μεγάλη προσπάθεια για τη λύση αυτού του προβλήματος.

Η χρήση ενός δημόσιου κλειδιού δεν θα πρέπει να ξεκινάει εάν δεν είμαστε σίγουροι ότι πρόκειται για ένα καλό δημόσιο κλειδί το οποίο ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει. Μπορούμε να είμαστε σίγουροι για την προέλευση του κλειδιού εάν έχουμε κάποιο πιστοποιητικό από τον ιδιοκτήτη του ή κάποιον άλλο που εμπιστευόμαστε,από τον οποίο όμως έχουμε ήδη ένα εγγυημένο δημόσιο κλειδί. Επιπλέον το user id θα πρέπει να έχει ολόκληρο το όνομα του ιδιοκτήτη και όχι απλά το μικρό του ή κάποιο άλλο ψευδώνυμο.

Δεν έχει σημασία πόσο σίγουροι μπορεί να αισθανόμαστε για κάποιο δημόσιο κλειδί που κατεβάσαμε από κάποιον ηλεκτρονικό πίνακα ανακοινωθέντων—ΠΟΤΕ δεν θα πρέπει να εμπιστευόμαστε οτιδήποτε δεν έχει την υπογραφή κάποιου που εμπιστευόμαστε. Ένα δημόσιο κλειδί που απλά κατεβάσαμε δίχως να το ελέγξουμε είναι πιθανόν να έχει αλλοιωθεί από κάποιον τρίτο, ακόμα και από το διαχειριστή του ηλεκτρονικού πίνακα. Εάν ποτέ μας ζητηθεί να υπογράψουμε το δημόσιο κλειδί κάποιου άλλου θα πρέπει να σιγουρευτούμε ότι αυτό πραγματικά του ανήκει. Αυτό πρέπει να γίνει διότι η υπογραφή μας στο δημόσιο κλειδί εγγυάται την αυθεντικότητά του. Εάν έχουμε κάνει λάθος,τότε όσοι μας εμπιστεύονται θα εμπιστευτούν και το κλειδί με αβέβαια αποτελέσματα. Ο κανόνας λέει ότι υπογράφουμε δημόσια κλειδιά για τα οποία έχουμε ιδία γνώση της αυθεντικότητάς τους. Για να αποκτήσουμε αυτή τη γνώση μπορούμε για παράδειγμα να μιλήσουμε στον ιδιοκτήτη του κλειδιού στο τηλέφωνο και να επιβεβαιώσουμε τα στοιχεία που έχουμε στα χέρια μας. Με το να βάλουμε την υπογραφή μας σε ένα δημόσιο κλειδί για το οποίο ήμαστε σίγουροι δεν χάνουμε την αξιοπιστία μας ακόμα και αν αυτό ανήκει σε κάποιον ψυχοπαθή. Αυτό συμβαίνει διότι με την υπογραφή μας δεν λέμε τίποτα παραπάνω από το ότι αυτό το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει—το ότι κάποιος μπορεί να εμπιστευθεί το κλειδί δεν έχει καμία σχέση με το αν μπορεί να εμπιστευθεί ή όχι τον ιδιοκτήτη του.

Θα ήταν καλή ιδέα, οι χρήστες να κρατούσαν το δημόσιο κλειδί τους μαζί με ένα σύνολο από πιστοποιητικά για αυτό από διαφόρους μεσάζοντες με την ελπίδα ότι οι περισσότεροι χρήστες εμπιστεύονται κάποιον από αυτούς. Μπορεί λοιπόν, κάποιος

χρήστης να ανακοινώσει το δημόσιο κλειδί του μαζί με τη συλλογή των πιστοποιητικών που διαθέτει για αυτό. Όταν υπογράφουμε το δημόσιο κλειδί κάποιου πρέπει να του το επιστρέφουμε μαζί με την υπογραφή μας ώστε να την προσθέσουνε στη συλλογή πιστοποιητικών για το δημόσιο κλειδί τους.

Το PGP κρατάει στοιχεία για το ποια από τα δημόσια κλειδιά που έχουμε στην κατοχή μας είναι πιστοποιημένα με υπογραφές που εμπιστευόμαστε. Το μόνο που εμείς πρέπει να κάνουμε είναι να πούμε στο PGP ποιους εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας.

Το PGP αναλαμβάνει από εκεί και πέρα να κρίνει αυτόματα κάποιο δημόσιο κλειδί ως έγκυρο ή όχι.

Πρέπει να διασφαλίσουμε ότι κανένας δεν πρόκειται να αλλοιώσει το μπρελόκ με τα κλειδιά μας. Ο έλεγχος ενός νέου υπογεγραμμένου δημοσίου κλειδιού πρέπει να εξαρτάται ολοκληρωτικά από την ακεραιότητα των κλειδιών τα οποία ήδη έχουμε στο μπρελόκ μας και τα οποία φυσικά εμπιστευόμαστε. Πρέπει να διατηρούμε συνεχή φυσικό έλεγχο των μπρελόκ δημοσίων κλειδιών μας σε κάποιο PC εκτός δικτύου όπως ακριβώς θα κάναμε και με το μυστικό κλειδί μας. Επιπλέον πρέπει να κρατάμε ένα αντίγραφο του δημόσιου και μυστικού κλειδιού μας σε κάποιο προστατευμένο μέσο όπου αποκλείεται ποτέ να τα σβήσουμε κατά λάθος. Από τη στιγμή κατά την οποία το δημόσιο κλειδί μας χρησιμοποιείται ως ο τελικός κριτής για τη πιστοποίηση ή μη όλων των άλλων κλειδιών του μπρελόκ είναι σημαντική για την ασφάλεια όλου του συστήματος η διασφάλισή του. Το PGP μπορεί αυτόματα να συγκρίνει το δημόσιο κλειδί μας με ένα αντίγραφό του σε κάποιο προστατευμένο φυσικό μέσο.

Το PGP γενικά θεωρεί ότι διατηρούμε το σύστημά μας, τα μπρελόκ και το PGP ασφαλές σε φυσικό επίπεδο. Εάν κάποιος έχει πρόσβαση στο σκληρό δίσκο του συστήματός μας τότε θεωρητικά μπορεί να αλλοιώσει το ίδιο το PGP έτσι ώστε αυτό να αδυνατεί να ανιχνεύσει οποιαδήποτε αλλοιώσει σε άλλα κλειδιά.

Ένας ακόμα τρόπος να προστατεύσουμε ολόκληρο το μπρελόκ με τα κλειδιά μας είναι να το υπογράψουμε ολόκληρο με το μυστικό μας κλειδί. Βέβαια θα έπρεπε πάλι να έχουμε κάπου αλλού προστατευμένο ένα αντίγραφο του δημοσίου κλειδιού μας για να είμαστε σε θέση να ελέγξουμε την υπογραφή μας. Όπως είναι φυσικό δεν

μπορούμε να βασιστούμε στο δημόσιο κλειδί μας, που βρίσκεται στο μπρελόκ, για τον έλεγχο της υπογραφής μας διότι αυτό είναι μέρος αυτού που πάμε να προστατέψουμε.

3.4.4 Διαδικασία Αναγνώρισης Έγκυρων Κλειδιών

Το PGP παρακολουθεί ποια από τα κλειδιά που υπάρχουν στο μπρελόκ δημοσίων κλειδιών είναι πιστοποιημένα και ποια όχι με υπογραφές χρηστών που εμπιστευόμαστε. Το μόνο που πρέπει να κάνουμε είναι να "πούμε" στο PGP ποιους χρήστες εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας κλειδί. Το PGP αναλαμβάνει από εκεί να κινήσει αυτόματα διαδικασίες ελέγχου της εγκυρότητας κλειδιών που είναι υπογεγραμμένα από τους μεσάζοντες που εμείς ορίσαμε. Υπάρχει βέβαια πάντα η δυνατότητα να υπογράψουμε κλειδιά και εμείς οι ίδιοι.

Υπάρχουν δύο διαφορετικά κριτήρια βάση των οποίων το PGP κρίνει τη χρησιμότητα των κλειδιών και τα οποία δεν πρέπει να συγχέουμε:

1. Το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει; (έχει πιστοποιηθεί από κάποιον του οποίου την υπογραφή εμπιστευόμαστε;)

2. Ανήκει σε κάποιον που μπορούμε να εμπιστευθούμε για την πιστοποίηση άλλων κλειδιών;

Το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση. Η απάντηση στη δεύτερη πρέπει να δοθεί αποκλειστικά από το χρήστη. Όταν ο χρήστης δώσει την απάντηση στην δεύτερη ερώτηση τότε το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση για άλλα κλειδιά τα οποία υπογράφονται από αυτόν που έχουμε ορίσει σαν έμπιστο. Κλειδιά τα οποία έχουν πιστοποιηθεί από κάποιον που έχουμε ορίσει ως έμπιστο θεωρούνται έγκυρα από το PGP. Τα κλειδιά που ανήκουν σε

έμπιστους μεσάζοντες πρέπει να πιστοποιηθούν από είτε από εμάς τους ίδιους είτε από κάποιον άλλο που έχουμε ορίσει ως έμπιστο.

Το PGP δίνει επιπλέον τη δυνατότητα ορισμού διαφορετικών επιπέδων εμπιστοσύνης για διαφορετικούς μεσάζοντες. Το ότι εμπιστευόμαστε κάποιον να δράσει ως μεσάζοντας δεν σημαίνει μόνο ότι τον εμπιστευόμαστε αλλά επιπλέον ότι τον θεωρούμε αρκετά ικανό να διαχειριστεί κλειδιά επιλέγοντας ποια από αυτά πρέπει και ποια όχι να υπογράψει. Μπορεί να ορίσουμε έναν χρήστη - μεσάζοντα στο PGP σαν άγνωστο, μη έμπιστο, μερικώς έμπιστο και εντελώς έμπιστο για να πιστοποιεί δημόσια κλειδιά. Αυτή η πληροφορία, που αφορά το βαθμό εμπιστοσύνης κάποιου μεσάζοντα, περιέχεται στο μπρελόκ των κλειδιών μαζί με το αντίστοιχο κλειδί (του μεσάζοντα) και δεν αντιγράφεται σε καμία περίπτωση κατά την αντιγραφή κάποιου κλειδιού του μπρελόκ διότι θεωρείται εμπιστευτική πληροφορία μια και αντικατοπτρίζει την άποψη του κατόχου του για τους μεσάζοντες - απόλυτα προσωπικό στοιχείο.

Όταν το PGP ελέγχει την εγκυρότητα ενός κλειδιού αυτό που κάνει είναι να ελέγχει τον βαθμό εμπιστοσύνης όλων των συνημμένων υπογραφών πιστοποίησής του. Κατόπιν υπολογίζει ένα μέσο επίπεδο εμπιστοσύνης - για παράδειγμα δύο μερικώς έμπιστες υπογραφές ισοδυναμούν με μία πλήρως έμπιστη. Το σκεπτικό λειτουργίας του PGP προσαρμόζεται στις απαιτήσεις του χρήστη και ρυθμίζεται αναλόγως (για παράδειγμα μπορούμε να ρυθμίσουμε το PGP να θεωρεί ένα κλειδί έγκυρο μόνο εάν αυτό φέρει δύο πλήρως έμπιστες υπογραφές ή τρεις μερικώς έμπιστες).

Το δικό μας κλειδί θεωρείται έγκυρο από το PGP αξιωματικά και για αυτό το λόγο δεν χρειάζεται την πιστοποίηση από κανέναν. Το PGP γνωρίζει ποια δημόσια κλειδιά είναι δικά μας κοιτάζοντας να βρει τα αντίστοιχα μυστικά κλειδιά στο μπρελόκ τους. Το PGP θεωρεί επιπλέον ότι εμπιστευόμαστε τους εαυτούς μας για να πιστοποιούν άλλα κλειδιά.

Όσο θα περνάει ο καιρός θα λαμβάνουμε όλο και περισσότερα κλειδιά από χρήστες που ίσως να θέλουμε να ορίσουμε ως μεσάζοντες. Κάθε ένας από αυτούς θα έχει τους δικούς του μεσάζοντες των οποίων τα πιστοποιητικά - υπογραφές θα μοιράζει μαζί με το κλειδί του με την ελπίδα ότι όποιος τα λάβει να εμπιστεύεται κάποιο από όλα. Έτσι δημιουργείται ένα αποκεντρωμένο δίκτυο εμπιστοσύνης για όλα τα δημόσια κλειδιά.

Αυτή η μοναδική προσέγγιση έρχεται σε αντίθεση με τα κατεστημένα κυβερνητικά σχήματα διαχείρισης κλειδιών, όπως το PEM (Internet Privacy Enhanced Mail), τα οποία βασίζονται σε συστήματα κεντρικού ελέγχου και υποχρεωτικής εμπιστοσύνης σε αυτά. Τα σχήματα αυτά απαρτίζονται από ιεραρχικές οντότητες που υπαγορεύουν ποιόν πρέπει να εμπιστευόμαστε. Αυτό είναι φανερό ότι έρχεται σε πλήρη αντίθεση με τη σχεδιαστική αρχή του PGP η οποία επιτρέπει στον καθένα και ανεξάρτητα από οποιονδήποτε και οτιδήποτε άλλο να καθορίσει ο ίδιος την πολιτική που θέλει να ακολουθήσει στη διαχείριση των κλαδιών του. Έτσι το PGP βάζει το χρήστη και όχι το σύστημα στην κορυφή της προσωπική του πυραμίδα πιστοποίησης.

3.4.5 Προστασία του Μυστικού Κλειδιού

Η προστασία του μυστικού κλειδιού και της φράσης-κλειδί του, είναι κάτι το αυτονόητο στο οποίο πρέπει να δοθεί μεγάλη προσοχή. Εάν ποτέ το μυστικό κλειδί πέσει σε λάθος χέρια – τα οποία είναι οποιαδήποτε άλλα εκτός των δικών μας—τότε θα πρέπει άμεσα, τόσο για τη δική μας ασφάλεια όσο και των άλλων, να ειδοποιήσουμε τους πάντες για το γεγονός προτού κάποιος αρχίσει να υπογράφει με το "όνομά" μας. Θα μπορούσε, για παράδειγμα, να υπογράψει ένα σύνολο από δημόσια κλειδιά δημιουργώντας έτσι πρόβλημα σε πολλούς χρήστες ειδικά εάν η υπογραφή μας τυγχάνει ευρείας εμπιστοσύνης και αποδοχής. Φυσικά, κίνδυνο διατρέχουμε και από το γεγονός της έκθεσης όλων των μηνυμάτων μας στα μάτια αυτού που έχει το προσωπικό μας κλειδί.

Η προστασία του μυστικού κλειδιού πρέπει να αρχίζει με τη φυσική του διασφάλιση. Μπορούμε να το κρατάμε σε κάποιο PC στο σπίτι ή κάποιο υπολογιστή notebook μια και αυτά τα έχουμε υπό την επίβλεψή μας συνεχώς. Εάν ποτέ υπάρξει ανάγκη χρησιμοποίησης υπολογιστή στο γραφείο ή οπουδήποτε αλλού τότε θα πρέπει να μεταφέρουμε το μυστικό κλειδί μας σε αυτόν μέσο κάποιας δισκέτας ενδεχομένως και για όσο χρειάζεται ενώ όταν τελειώσουμε τη δουλειά μας δεν πρέπει να αφήσουμε πίσω οτιδήποτε μπορεί να οδηγήσει στην αποκάλυψη του. Δεν είναι επίσης σωστό να αφήνουμε το μυστικό κλειδί μας σε κάποιο απομακρυσμένο μηχάνημα (ένας Unix dial-in server) διότι μπορεί κάποιος που παρακολουθεί τις επικοινωνίες μέσω modem να

υποκλέψει τη μυστική φράση (pass phrase) και να αποκτήσει το μυστικό από το απομακρυσμένο σύστημα. Συμπερασματικά λέμε ότι θα πρέπει να γίνεται χρήση του μυστικού κλειδιού μόνο σε συστήματα στα οποία έχουμε φυσικό έλεγχο.

Επιπρόσθετα, πρέπει να προσέξουμε πού αποθηκεύουμε τη μυστική φράση-κλειδί. Δεν πρέπει ποτέ αυτή να βρίσκεται στον ίδιο υπολογιστή με αυτόν που έχει το αρχείο του μυστικού κλειδιού μας. Η αποθήκευση τόσο του μυστικού κλειδιού όσο και της μυστικής φράσης στον ίδιο υπολογιστή είναι το ίδιο επικίνδυνη με την φύλαξη του PIN ενός τραπεζικού ATM λογαριασμού στο ίδιο πορτοφόλι με την κάρτα ATM. Ένα πράγμα είναι σίγουρο - δεν θέλουμε σε καμία περίπτωση αυτός που θα έχει στα χέρια του τον σκληρό δίσκο με το μυστικό μας κλειδί να έχει στη διάθεσή του και τη μυστική φράση. Το ιδανικό θα ήταν να απομνημονεύαμε τη μυστική φράση και να μην την φυλάγαμε σε κανένα άλλο μηχάνημα εκτός του εγκεφάλου μας. Εάν, ωστόσο, νιώθουμε ότι πρέπει να τη γράψουμε κάπου θα πρέπει να την ασφαλίσουμε καλλίτερα ίσως και από το ίδιο το μυστικό μας κλειδί.

Κάτι άλλο επίσης σημαντικό, που πρέπει να κάνουμε, είναι να παίρνουμε backup του μυστικού μπρελόκ μας διότι μόνο εμείς έχουμε το μοναδικό αντίγραφο αυτού και πιθανή απώλειά του θα ισοδυναμούσε με αχρήστευση όλων των δημοσίων κλειδιών που διανείμαμε στον κόσμο.

Το αποκεντρωτικό σχήμα φιλοσοφίας αλλά και λειτουργίας που έχει επιλέξει να χρησιμοποιήσει το PGP εκτός από τα πλεονεκτήματα στη διαχείριση των κλειδιών έχει και τα μειονεκτήματα του. Δεν υπάρχει μία κεντρική λίστα που να περιέχει τα μη έγκυρα κλειδιά κάνοντας πιο δύσκολη την γνώση τους. Έτσι αν κάτι πάει στραβά η διαδικασία γνωστοποίησής του είναι επίπονη. Εάν τελικά το μυστικό κλειδί και η μυστική φράση πέσουν στα χέρια άλλων θα πρέπει να φτιάξουμε και να διανείμουμε ένα "πιστοποιητικό απολεσθέντος κλειδιού" (key compromise certificate). Αυτός ο τύπος πιστοποιητικού χρησιμοποιείται για να προειδοποιεί άλλους χρήστες να σταματήσουν να χρησιμοποιούν το αντίστοιχο δημόσιο κλειδί μας. Μπορούμε να χρησιμοποιήσουμε το PGP στη δημιουργία αυτού του πιστοποιητικού και κατόπιν να το στείλουμε σε όλους τους φίλους και συνεργάτες μας σε όλο τον κόσμο. Η έκδοση του PGP που τρέχει σε αυτούς θα αναλάβει να εγκαταστήσει το πιστοποιητικό του απολεσθέντος κλειδιού στα δημόσια μπρελόκ τους και από εκείνη τη στιγμή θα αποτρέπεται αυτόματα η επαναχρησιμοποίησή τους. Μπορούμε κατόπιν να

δημιουργήσουμε ένα νέο ζεύγος μυστικού/δημοσίου κλειδιού και να αρχίσουμε πλέον να δουλεύουμε με αυτά.

3.5 SSH (Secure Shell)

3.5.1 Εισαγωγή

Τα εργαλεία απομακρυσμένης επικοινωνίας (rsh, rcp, rlogin) είναι γνωστά για την ευκολία χρήσης τους και την παροχή γρήγορης πρόσβασης σε άλλες μηχανές. Το πρόβλημα, όμως, είναι ότι βασίζονται σε IP διευθύνσεις ή host names για την πιστοποίηση της ταυτότητας των μηχανών, γεγονός που τα καθιστά ανασφαλή καθ' ότι οι υπηρεσίες του DNS δεν είναι άξιες εμπιστοσύνης. Επίσης, η μετάδοση των κωδικών χωρίς κανένα είδος προστασίας οξύνει τις τρύπες ασφαλείας. Για να μπορούν, λοιπόν, να χρησιμοποιούνται σε ασφαλή περιβάλλοντα πρέπει να διαθέτουν πιο καλύτερους μηχανισμούς πιστοποίησης ταυτότητας. Η εισαγωγή της έννοιας της κρυπτογράφησης και των ψηφιακών υπογραφών στα εργαλεία rsh, rcp και rlogin, δημιούργησε το Secure Shell (SSH).

Το SSH σχεδιάστηκε για να αντικαταστήσει τα εργαλεία rsh, rcp και rlogin με τα αντίστοιχα ssh, scp και slogin, με επιπλέον χαρακτηριστικά αυτά της ισχυρής από άκρη σε άκρη κρυπτογράφηση, της βελτιωμένης πιστοποίησης ταυτότητας χρήστη και μηχανής και την προώθηση TCP πορτών και X11 συνδέσεων.

3.5.2 Περιγραφή του SSH πρωτοκόλλου

Το SSH είναι ένα πρωτόκολλο που παρέχει ασφαλή απομακρυσμένη σύνδεση σε υπολογιστές πάνω από μη ασφαλές δίκτυο. Αποτελείται από τρία βασικά στοιχεία:

• Το Transport layer protocol παρέχει πιστοποίηση της ταυτότητας του server, ακεραιότητα των δεδομένων και εξασφάλιση του απόρρητου της συναλλαγής.

Προαιρετικά μπορεί να εφαρμόσει και συμπίεση δεδομένων. Τυπικά τρέχει πάνω από μία TCP/IP σύνδεση.

• Το User Authentication protocol πιστοποιεί την ταυτότητα του πελάτη- χρήστη στον server. Τρέχει πάνω από το Transport layer protocol.

• Το Connection protocol πολυπλέκει το κρυπτογραφημένο φυσικό κανάλι σε αρκετά λογικά κανάλια και τρέχει πάνω από το User Authentication protocol.

3.5.3 Δομή του SSH

Ιδιωτικά Και Δημόσια Κλειδιά

Κάθε server και client πρέπει να έχει ένα ζευγάρι ιδιωτικής – δημόσιας κλείδας για να μπορεί να επαλήθευση την ταυτότητα του στο άλλο άκρο. Επιτρέπεται η κατοχή περισσότερων του ενός ζευγάρια κλειδιών, όταν χρησιμοποιούνται με διαφορετικούς αλγόριθμους, ενώ η από κοινού χρήση ενός ζεύγους από πολλούς server δεν απαγορεύεται.

Για να μπορεί ο client με ευκολία να επαληθεύει την ταυτότητα του server είναι απαραίτητο να γνωρίζει την δημόσια κλείδα που αντιστοιχεί στον server που θέλει να συνδεθεί. Υπάρχουν δυο διαφορετικά μοντέλα που εξασφαλίζουν την προηγούμενη προϋπόθεση:

• Πρώτον, ο client έχει αποθηκευμένα σε μια τοπική βάση δεδομένων τα ονόματα των server και τις σχετιζόμενες με αυτά δημόσιες κλείδες. Αυτή η μέθοδος δεν απαιτεί μια κεντρική διαχείριση των κλειδιών από τρίτους. Το μειονέκτημα είναι ότι το μέγεθος μιας τέτοιας βάσης δεδομένων μπορεί να εξελιχθεί σημαντικά και συνεπώς η συντήρηση της να γίνει δύσκολη.

• Στην δεύτερη περίπτωση, σχέση μεταξύ του ονόματος του server και του κλειδιού του πιστοποιείται από μια άξια εμπιστοσύνης Certification Authority. Το πρόγραμμα του πελάτη γνωρίζει μόνο την δημόσια κλείδα της Certification Authority και μπορεί να επιβεβαιώσει την εγκυρότητα των κλείδων που έχουν πιστοποιηθεί από την CA.

Εδώ δεν υπάρχει το πρόβλημα της διατήρησης μεγάλων βάσεων δεδομένων από τα τοπικά συστήματα, αφού μόνο ένα κλειδί χρειάζεται να αποθηκεύει ο client. Από την άλλη μεριά, όμως, δεν είναι δυνατή η απόλυτη εμπιστοσύνη στις διαδικασίες της Certification Authority. Επίσης, πιστοποίηση κάθε κλειδιού μπορεί να είναι μια χρονοβόρα και περίπλοκή διαδικασία.

Οι εφαρμογές του SSH μπορούν να παρέχουν επιπρόσθετες μεθόδους επικύρωσης των δημόσιων κλειδιών, όπως για παράδειγμα την παραγωγή ενός δεκαεξαδικού "αποτυπώματος" της κλείδας και από τα δύο άκρα και την σύγκριση τους μέσω εξωτερικών καναλιών επικοινωνίας (π.χ. τηλέφωνο). Κλείδες που δεν επαληθεύονται, κανονικά δεν πρέπει να γίνονται δεκτές.

Επεκτασιμότητα

Βασικός στόχος της σχεδίασης είναι η διατήρηση του πρωτοκόλλου όσο το δυνατόν απλό γίνεται, με όσο το δυνατόν λιγότερους αλγόριθμους. Όλες οι εφαρμογές πρέπει να υποστηρίζουν ένα ελάχιστο σύνολο αλγόριθμων για να εξασφαλιστεί η δια – λειτουργικότητα. Στο μέλλον αναμένεται η πρόσθεση και άλλων αλγορίθμων.

Θέματα Πολιτικής

Το πρωτόκολλο επιτρέπει την διαπραγμάτευση όλων των χρησιμοποιούμενων αλγορίθμων. Έτσι, οι αλγόριθμοι κρυπτογράφησης, ανταλλαγή κλειδιών και συμπίεσης καθώς επίσης και οι μηχανισμοί ασύμμετρων κλειδιών και παροχής ακεραιότητας, μπορούν να επιλεγούν από λίστες που παρέχουν ο client και ο server ο ένας στον άλλο

και μάλιστα διαφορετικοί για κάθε κατεύθυνση. Η πολιτική ασφαλείας κάθε συστήματος καθορίζει ποιοι προτιμούνται.

Τα παρακάτω θέματα πολιτικής θα πρέπει υπολογίζονται κατά την ρύθμιση SSH εφαρμογών:

• Οι αλγόριθμοι και οι μηχανισμοί που πρόκειται να χρησιμοποιηθούν για κάθε κατεύθυνση. Πρέπει να ορίζεται ποιος προτιμάται.

• Η μέθοδοι πιστοποίησης της ταυτότητας, ξεχωριστοί για κάθε χρήστη που θα εφαρμόζει ο server. Η πολιτική του server μπορεί να ζητά πολλαπλές διαδικασίες πιστοποίησης για μερικού ή όλους τους χρήστες, ενώ οι απαιτούμενοι αλγόριθμοι μπορούν να εξαρτώνται από την τοποθεσία από όπου προσπαθεί να συνδεθεί ο χρήστης.

• Οι ενέργειες που επιτρέπονται σε κάθε χρήστη και στον server. Η πολιτική ασφαλείας δεν θα πρέπει να επιτρέπει στον server να εκτελεί εντολές στην μηχανή του χρήστη ούτε στον χρήστη να συνδέεται στον authentication server.

Ιδιότητες Ασφάλειας

Ο πρωταρχικός στόχος του SSH πρωτοκόλλου είναι η βελτίωση της ασφάλειας στο Internet και ο τρόπος με τον οποίο προσπαθεί να το επιτύχει αυτό βασίζεται στο εξής σκεπτικό:

• Όλοι οι αλγόριθμοι κρυπτογράφησης, παροχής ακεραιότητας και ανταλλαγής κλειδιών έχουν δοκιμαστεί και

• Οι αλγόριθμοι χρησιμοποιούν κλειδιά μεγέθους ικανού να παρέχει προστασία απέναντι στις ισχυρότερες επιθέσεις κρυπτοανάλυσης.

• Στην περίπτωση που κάποιος αλγόριθμος "σπάσει", είναι εύκολη η αντικατάσταση του από κάποιον άλλο χωρίς αλλαγές στις βάσεις του SSH.

Για την ταχεία ανάπτυξη και υιοθέτηση του πρωτοκόλλου, κάποιες έχουν γίνει παραχωρήσεις. Σημαντικότερη από αυτές είναι η καθιέρωση της επαλήθευσης των κλείδων με υποχρεωτική, γεγονός όμως που δεν συνιστάται.

3.6 S/HTTP (Secure Hyper-Text Transfer Protocol)

3.6.1 Εισαγωγή

Το WWW είναι ένα διανεμημένο σύστημα πολυμέσων το οποίο χαίρει μεγάλης αποδοχής από πολλούς χρήστες. Το βασικό και περισσότερο χρησιμοποιούμενο πρωτόκολλο μεταξύ WWW clients και WWW servers είναι το Hyper Text Transfer Protocol. Η ευκολία της χρήσης του WWW έχει προκαλέσει το παγκόσμιο ενδιαφέρον και χρησιμοποιείται σαν η υποδομή client / server για πολλές δικτυακές εφαρμογές. Τέτοιες εφαρμογές απαιτούν την αμοιβαία πιστοποίηση της ταυτότητας των δύο επικοινωνούντων υπολογιστών και την ικανότητα ανταλλαγής ευαίσθητων πληροφοριών. Οι τρέχοντες, όμως, HTTP εφαρμογές έχουν μέτρια έως και μηδαμινή υποστήριξη για τους κρυπτογραφικούς μηχανισμούς που είναι απαραίτητοι για τέτοιες συναλλαγές.

Το πρωτόκολλο Secure HTTP παρέχει ασφαλής μηχανισμούς επικοινωνίας μεταξύ ένα ζευγάρι HTTP server – client με σκοπό να επιτρέψει αυθόρμητες εμπορικές συναλλαγές. Στόχος της σχεδίασης ήταν ένα ευέλικτο πρωτόκολλο που διαθέτει πολλαπλούς μηχανισμούς και αλγόριθμους, και την δυνατότητα διαπραγμάτευσης αυτών. Σχεδιάστηκε από τους E. Rescorla και A. Schiffman του EIT και αποτελεί υπερσύνολο του HTTP.

3.6.2 Χαρακτηριστικά του S/HTTP

1. Το S/HTTP υποστηρίζει μία ποικιλία μηχανισμών ασφαλείας στους HTTP clients και servers. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και server που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών μεταχειρίζονται με τον ίδιο τρόπο, ενώ παράλληλα διατηρούνται το μοντέλο συναλλαγής και τα χαρακτηριστικά επικοινωνίας του HTTP.

2. Αρκετά κρυπτογραφικά στάνταρντς ενσωματώνονται στους S/HTTP clients και servers συμπεριλαμβανομένων των PEM, PGP, Kerberos και PKCS-7 (ο πρόγονος του CMS). Είναι συμβατό με το HTTP.

3. Το S/HTTP δεν απαιτεί πιστοποιητικά δημοσίων κλείδων από την μεριά του client, καθ' ότι υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι σημαντικό γιατί αυθόρμητες ιδιωτικές συναλλαγές μπορούν να λάβουν χώρα, χωρίς την απαίτηση από τους χρήστες να έχουν ένα έγκυρο ζεύγος δημόσιας – ιδιωτικής κλείδας. Βέβαια, είναι σε θέση να εκμεταλλευτεί την υπάρχουσα υποδομή πιστοποιητικών και ασύμμετρων κλειδιών.

4. Το S/HTTP υποστηρίζει απ' άκρη σ' άκρη ασφαλής συναλλαγές, σε αντίθεση με το HTTP που προϋποθέτει μία αποτυχημένη προσπάθεια πρόσβασης του χρήστη πριν την εφαρμογή οποιωνδήποτε μηχανισμών ασφαλείας. Με το S/HTTP, σε καμία περίπτωση ευαίσθητα δεδομένα θα μεταδοθούν στο δίκτυο απροστάτευτα.

5. Επιτρέπει πλήρη ευελιξία όσον αναφορά τους κρυπτογραφικούς αλγόριθμούς και τις παραμέτρους αυτών. Το είδος της παρεχόμενης προστασίας (κρυπτογράφηση, ψηφιακή υπογραφή, και τα δύο), οι αλγόριθμοι και τα πιστοποιητικά μπορούν να διαπραγματευτούν.

6. Οι χρήστες αναμένονται να έχουν (αν και δεν συνιστάται) πολλαπλά πιστοποιητικά.

3.6.3 Είδη Προστασίας

Η προστασία ενός μηνύματος εφαρμόζεται με τρεις διαφορετικούς τρόπους: με υπογραφή, με κρυπτογράφηση και με παραγωγή MACs. Κάθε μήνυμα μπορεί να υπογραφεί, να κρυπτογραφηθεί ή οποιοσδήποτε συνδυασμός αυτών,

συμπεριλαμβανομένων της παραγωγής και της παροχής καμίας προστασίας. Υποστηρίζονται αρκετές τεχνικές διαχείρισης κλειδιών όπως συμμετρικά μυστικά κλειδιά, ασύμμετρη διαχείριση και το σύστημα Key Distribution Center (KDC) του Kerberos. Επιπλέον, ένας μηχανισμός challenge-response παρέχει στους επικοινωνούντες υπολογιστές την δυνατότητα να αναγνωρίζουν τις επιθέσεις επανάληψης (replay attacks).

3.7 RADIUS & TACACS+

3.7.1 Εισαγωγή

Καθώς τα δίκτυα εξαπλώνονται πέρα από το φυσικό χώρο των επιχειρήσεων η έννοια της ασφάλειας γίνεται πιο σημαντική και σύνθετη. Οι εταιρίες πρέπει να προστατέψουν τα δίκτυά και τους δικτυακούς τους πόρους από απομακρυσμένους χρήστες που μπαίνουν παράνομα στο σύστημα αποκτώντας πρόσβαση με κάποιο τρόπο. Τα συστήματα της Cisco χρησιμοποιούν μία στρατηγική που είναι γνωστή σαν Πιστοποίηση, Έγκριση και Παρακολούθηση (authentication, authorization, accounting-AAA) για να εκτελέσει τις λειτουργίες της πιστοποίησης της ταυτότητας του χρήστη, τη παροχή ή όχι πρόσβασης και την παρακολούθηση των κινήσεων των απομακρυσμένων χρηστών αντίστοιχα. Στα σημερινά δίκτυα χρησιμοποιούνται τα πρωτοκολλά0 TACACS+ (Terminal Access Controller Access Control System plus) και RADIUS (Remote Access Dial-In User Service) για τη παροχή AAA λύσεων. Η υποστήριξη των RADIUS και TACACS+ δίνει τη δυνατότητα στη Cisco να προτείνει μία πολύ ευέλικτη και αποδοτική AAA λύση.

3.7.2 Ανάλυση Απαιτήσεων Ασφαλείας

- Authentication – Πιστοποίηση

Η Πιστοποίηση είναι η διαδικασία με την οποία καθορίζεται ποιος έχει πρόσβαση στο LAN. Απλές μέθοδοι έγκρισης χρησιμοποιούν μια βάση δεδομένων που αποτελείται από usernames και passwords στον server πρόσβασης. Πιο εξελιγμένα συστήματα χρησιμοποιούν μεθόδους όπως το TACACS και το Kerberos.

Ωστόσο, το ότι πιστοποιείται η ταυτότητα κάποιου χρήστη δε σημαίνει ότι αυτός έχει αποκτήσει πρόσβαση σε όλες τις υπηρεσίες του δικτύου—είναι πιθανό να του ζητηθεί εκ νέου κάποιος κωδικός από κάποια συγκεκριμένη υπηρεσία UNIX, NetWare ή AppleShare. Ένας καλός NAS server υποστηρίζει μία πλειάδα επιλογών πιστοποίησης.

- Authorization – Έγκριση

Η Έγκριση είναι η ικανότητα του περιορισμού των δικτυακών υπηρεσιών σε διαφορετικούς χρήστες βάση μιας δυναμικά εφαρμοζόμενης λίστας πρόσβασης (access list) που μερικές φορές αναφέρεται και ως "προφίλ χρήστη" και που βασίζεται στο δίδυμο username/password. Αυτό το χαρακτηριστικό είναι σημαντικό για δύο λόγους: βοηθάει στη μείωση της έκθεσης του εσωτερικού δικτύου στον έξω κόσμο και απλοποιεί τη μορφή του δικτύου για τον τελικό χρήστη που αγνοεί τις τεχνικές του λεπτομέρειες.

Το χαρακτηριστικό της έγκρισης επιτρέπει στους χρήστες να κινούνται. Κινούμενοι και προσωρινοί χρήστες (χρήστες με φορητά από ξενοδοχεία και τηλεργαζόμενοι με modems και ISDN συνδέσεις από το σπίτι) θέλουν να συνδεθούν στη πιο κοντινή τοπική σύνδεση διατηρώντας ωστόσο όλα τα προνόμιά των LAN τους.

Ο Διαχειριστής του δικτύου (Network Administrator) πρέπει να είναι σε θέση να περιορίζει τη πρόσβαση στο δίκτυο για όλα τα πρωτόκολλα και τις υπηρεσίες (Telnet, IP, IPX και AppleTalk) όσο οι χρήστες συνδέονται (dial-in) από τη την ίδια "πηγή" modem (pool). Η διαδικασία έγκρισης με τη χρήση access list για κάθε χρήστη δεν περιορίζεται σε συγκεκριμένα interfaces αλλά ανατίθεται δυναμικά στη συγκεκριμένη πόρτα στην οποία συνδέεται ο χρήστης. Για παράδειγμα όταν ο χρήστης Α συνδέεται στη πόρτα 1, μπορεί να δει τα υπο-δίκτυα 1, 2, 3 και τις AppleTalk ζώνες bldg D, bldg E και bldg F. Όταν ο χρήστης 2 συνδέεται στη πόρτα 1, τότε το προφίλ του τον περιορίζει στο υπο-δίκτυο 1 και στη ζώνη bldg D.

Από τη στιγμή που το NAS υποστηρίζει πολύ περισσότερους απομακρυσμένους χρήστες από τις φυσικές γραμμές που έχει στη διάθεσή του κάθε χρήστης ή group, μπορεί να τηλεφωνήσει στο ίδιο περιστροφικό κέντρο και να πάρει πρόσβαση στο δίκτυο. Αυτή η access list βασίζεται στο username και σαν τέτοια κάθε NAS μπορεί να υποστηρίξει χιλιάδες χρήστες στη βάση δεδομένων που έχει για τα usernames και passwords.

- Accounting—Παρακολούθηση

Η παρακολούθηση είναι το τρίτο κύριο συστατικό ενός ασφαλούς συστήματος. Οι διαχειριστές του συστήματος μπορεί από το να θέλουν να χρεώσουν τους πελάτες τους για την ώρα που παρέμειναν συνδεδεμένοι στο δίκτυο μέχρι να παρακολουθήσουν ύποπτες προσπάθειες σύνδεσης στο δίκτυο.

3.7.3 Το Πρωτόκολλο RADIUS

Το πρωτόκολλο RADIUS αναπτύχθηκε από την Livingston Enterprises ως ένας server πρόσβασης, πιστοποίησης και παρακολούθησης. Από τότε έχει υλοποιηθεί από διάφορους άλλους πωλητές και έχει κερδίσει ευρεία υποστήριξη ανάμεσα ακόμα και στους παροχείς υπηρεσιών (ISPs).

Το RADIUS είναι βασισμένο στο client/server μοντέλο. Οι servers πρόσβασης (NAS-Network Access Servers) λειτουργούν σαν clients του RADIUS. Ο client είναι υπεύθυνος για την προώθηση της πληροφορίας του χρήστη στον αρμόδιο RADIUS server και την εκτέλεση των εντολών που θα του σταλούν πίσω από το server.

Ο RADIUS server ή daemon παρέχει υπηρεσίες πιστοποίησης και παρακολούθησης σε έναν ή περισσότερους RADIUS clients δηλαδή συσκευές NAS. Οι RADIUS servers είναι υπεύθυνοι για το να λαμβάνουν τις αιτήσεις σύνδεσης των χρηστών, να τους πιστοποιούν και τέλος να επιστρέφουν όλη τη πληροφορία με τις απαιτούμενες ρυθμίσεις για τους clients ώστε να δοθούν οι αιτούμενες υπηρεσίες στους

χρήστες. Ο RADIUS server πρόσβασης είναι συνήθως ένας αφιερωμένος σταθμός εργασίας συνδεδεμένος με το δίκτυο.

3.7.4 Το πρωτόκολλο TACACS+

Το TACACS+ επιτρέπει σε ένα ξεχωριστό server πρόσβασης (τον TACACS+ server) να παρέχει τις υπηρεσίες πιστοποίησης, έγκρισης και παρακολούθησης με ανεξάρτητο τρόπο. Κάθε υπηρεσία μπορεί να συνδυαστεί με τη δική της βάση δεδομένων ή μπορεί να χρησιμοποιήσει τις άλλες υπηρεσίες που είναι διαθέσιμες στο δίκτυο.

Η φιλοσοφία σχεδίασης του TACACS+ είναι ο καθορισμός μιας μεθόδου για την διαχείριση όχι όμοιων server πρόσβασης (NAS) από ένα και μόνο σύνολο διαχειριστικών υπηρεσιών όπως μια βάση δεδομένων. Ένας NAS παρέχει πρόσβαση σε έναν χρήστη, σε ένα δίκτυο ή υποδίκτυο ή και σε διασυνδεδεμένα δίκτυα.

Το TACACS+ αποτελείται από τρία κύρια μέρη: την υποστήριξη του πρωτοκόλλου από servers πρόσβασης και δρομολογητές, τα χαρακτηριστικά του πρωτοκόλλου και την κεντρική βάση δεδομένων. Παρόμοια με μια εσωτερική βάση δεδομένων, το TACACS+ υποστηρίζει τα παρακάτω τρία απαιτούμενα χαρακτηριστικά ενός ασφαλούς συστήματος.

3.8 Cisco NetSonar

Το Cisco NetSonar είναι ένα προϊόν Ανίχνευσης Αδυναμιών Ασφάλειας και Χαρτογράφησης Δικτύου. Αποτελεί το πρώτο τέτοιο προϊόν που συνδυάζει τεχνολογία αιχμής στην ανίχνευση αδυναμιών ασφάλειας, ευέλικτη ανάλυση δεδομένων και είναι φιλικότατο προς το χρήστη τόσο στη λειτουργία του όσο και στους όρους της άδειάς του. Στοχεύει στην αγορά των Διαχειριστών Συστημάτων (Network Administrators) σε επιχειρησιακά περιβάλλοντα όπως επίσης αποτελεί εργαλείο και για συμβούλους ασφάλειας δικτύων. Αυτό που κάνει είναι να ψάχνει στα βάθη ενός δικτύου για τρύπες στην ασφάλειά του. Χαρτογραφεί γρήγορα όλα τα συστήματα στο δίκτυο, τα λειτουργικά τους συστήματα και τις υπηρεσίες τους και τέλος τις σχετιζόμενες με αυτά αδυναμίες όσον αφορά το βαθμό ασφάλειας που προσφέρουν. Επιπλέον ερευνά ενεργά για να διαπιστώσει τις όποιες τρύπες στο σύστημα συγκεντρώνοντας αναλυτικές

πληροφορίες διασφαλίζοντας την ακρίβεια των δεδομένων. Με την παρουσίαση των αποτελεσμάτων, που γίνεται με ένα πολύ διαμορφώσιμο τρόπο – ανάλογα με τις ανάγκες του ενδιαφερόμενου – το NetSonar δίνει την ευκαιρία στο χρήστη του να αποκτήσει μοναδική αίσθηση για τη λειτουργία και την ασφάλεια του συστήματός του.

3.9 Cisco NetRanger

Το σύστημα NetRanger είναι μια διαδικασία η οποία ανιχνεύει και αντιδρά σε κάθε παραβίαση ή κατάχρηση που γίνεται στην πολιτική ασφάλειας ενός δικτύου. Τοποθετώντας σε κατάλληλα επιλεγμένα σημεία του δικτύου αισθητήρες, παρακολουθείται η κίνηση και συγκρίνεται με γνωστά σχέδια ή υπογραφές που αντιπροσωπεύουν ύποπτη δραστηριότητα, κατάχρηση του συστήματος ή ακόμα και επίθεση σε αυτό. Ο αισθητήρας μπορεί να στείλει σήματα προειδοποίησης – κινδύνου στον υπεύθυνο, σε ένα σύστημα διαχείρισης ασφάλειας, και υπό συγκεκριμένες συνθήκες να πάρει τη πρωτοβουλία να στείλει εντολές αντιμετώπισης της κατάστασης κατευθείαν στον δικτυακό εξοπλισμό, όπως σε routers και firewalls, τροποποιώντας τις ρυθμίσεις τους έτσι ώστε να μην επιτρέψουν την είσοδο του εισβολέα στο σύστημα. Το σύστημα αυτόματα και γρήγορα απαντά, λοιπόν, προειδοποιώντας ή αναλαμβάνοντας δράση σε αληθινό χρόνο βάση οδηγιών που έχει πάρει από το χρήστη του.

ΚΕΦΑΛΑΙΟ 4: Εμπορικές εφαρμογές της ευρυζωνικής σύνδεσης

Υπάρχουν μερικές εμπορικές εφαρμογές ευρυζωνικής σύνδεσης: η τεχνολογία πολλαπλών καναλιών VPN Biping της Viprinet, η υπηρεσία ευρείας ζώνης σύνδεσης των δικτύων Mushroom και η τεχνολογία της Peplink Speedfusion Bonding.

4.1 Mushroom Networks

Το Mushroom Networks, Incorporated, εδρεύει στο Σαν Ντιέγκο της Καλιφόρνια. Τα προϊόντα και οι υπηρεσίες τους επικεντρώνονται σε μια σειρά λύσεων δικτύωσης για επιχειρήσεις και μικρές / μεσαίες επιχειρήσεις σε διάφορες βιομηχανίες. Το Mushroom Networks ιδρύθηκε το 2004 ως ένα spin-off από το Πανεπιστήμιο της Καλιφόρνια στο Σαν Ντιέγκο. Τα προϊόντα των μανιταριών βασίζονται στην τεχνολογία Broadband Bonding® που αναπτύχθηκε από την ομάδα μηχανικών τους.

Τα Mushroom Networks παρέχουν λύσεις σύνδεσης για επιχειρήσεις. Για μια οργάνωση που διαθέτει υποκαταστήματα που συνδέονται με την έδρα, η Virtual Leased Line (VLL) που τροφοδοτείται από συσκευές τροφοδοσίας ευρείας ζώνης Truffle παρέχει μια λύση σύνδεσης WAN. Με τις συσκευές δικτύου Truffle στα υποκαταστήματα και στα κεντρικά γραφεία, τα υποκαταστήματα μπορούν να ενώσουν τις διάφορες γραμμές πρόσβασης στο Διαδίκτυο για να δημιουργήσουν ένα εικονικό ασφαλές IP σωλήνα από και προς την έδρα τους. Το VLL είναι μια οικονομικά αποδοτική εναλλακτική λύση για το MPLS. Μπορεί επίσης να χρησιμοποιηθεί για την εκφόρτωση δημόσιας διαδικτυακής κυκλοφορίας του MPLS όταν αναπτυχθεί ως επέκταση στο MPLS.

Αν η διαδικτυακή κίνηση του υποκαταστήματος μεταδίδεται μέσω της κεντρικής έδρας (π.χ. μέσω ενός VPN), τότε το υποκατάστημα είναι σε θέση να χρησιμοποιήσει τη σύνδεση VPN και το συνολικό εύρος ζώνης όχι μόνο για τη σύνδεση από σημείο σε σημείο στην έδρα, αλλά και για την κίνηση προς / από το

δημόσιο Διαδίκτυο. Προαιρετικά, η απομακρυσμένη διαδικτυακή κίνηση στο διαδίκτυο μπορεί να εκφορτωθεί και να συνδεθεί τοπικά.

Τα Μανιτάρια Δίκτυα έχουν μια ελαφρύτερη λύση για μικρές και μεσαίες επιχειρήσεις. Το Standalone Truffle παρέχει διπλό δρομολογητή WAN για σύνδεση υψηλής ταχύτητας στο Διαδίκτυο για εταιρείες που απαιτούν υψηλές ταχύτητες σύνδεσης στο Διαδίκτυο, αλλά δεν είναι διατεθειμένες να πληρώσουν τα υψηλά μηνιαία τέλη συνδρομής ή δεν διαθέτουν αυτές τις υπηρεσίες υψηλής ταχύτητας. Με το Truffle Lite, διπλό τείχος προστασίας WAN, μπορούν να συνδυαστούν διάφορες ευρυζωνικές συνδέσεις για τη δημιουργία ενός εικονικού σωλήνα για την υπηρεσία Διαδικτύου μικρών επιχειρήσεων.

Εάν υπάρχουν περισσότερα υποκαταστήματα που πρέπει να συνδεθούν μέσω μισθωμένων γραμμών, η λύση Virtual VLL (Mushroom) παρέχει ένα οικονομικά αποδοτικό συνδεδεμένο σωλήνα IP μεταξύ των γραφείων. Το VLL τροφοδοτείται από μονάδες Truffle εγκατεστημένες στις θέσεις γραφείου και επιτρέπει στα γραφεία να συνδέουν τις γραμμές πρόσβασης στο Internet για να δημιουργήσουν μια εικονική σύνδεση από σημείο σε σημείο.

Οποιοσδήποτε τύπος κίνησης μεταξύ των γραφείων (συμπεριλαμβανομένης της κυκλοφορίας VPN) θα συνδεθεί και στις δύο κατευθύνσεις προς τα κάτω και προς τα πάνω. Οι γραμμές ADSL και καλωδίων μπορούν να συνδεθούν μεταξύ τους για να δημιουργήσουν μια μισθωμένη γραμμή ταχύτερη από την T1 ή E1.

Το VLL επιτρέπει την ύπαρξη αξιόπιστου σωλήνα IP μεταξύ του γραφείου και της μετεγκατάστασης του σε ένα κέντρο δεδομένων Internet. Σε περιπτώσεις όπου η ροή του Διαδικτύου μεταδίδεται μέσω του κέντρου δεδομένων, όλη η κίνηση στο Διαδίκτυο προς / από το γραφείο θα είναι σε θέση να αξιοποιήσει τις συνδεδεμένες ταχύτητες IP.

4.2 Viprinet GmbH

Η Viprinet κατασκευάζει καινοτόμα στοιχεία δικτύου από το 2006. Είναι ο εφευρέτης μιας πατενταρισμένης τεχνολογίας που συγκεντρώνει τα εύρος ζώνης διαφορετικών τεχνολογιών δικτύου ευρείας περιοχής. Η εταιρεία βρίσκεται στην πόλη

Bingen am Rhein Valley. Οι 55 υπάλληλοί τους αναπτύσσουν, παράγουν και πωλούν προϊόντα δικτύωσης σε ολόκληρο τον κόσμο. Η Viprinet έχει τοπικές ομάδες στην Ολλανδία, το Ηνωμένο Βασίλειο, τις Σκανδιναβικές χώρες και την Καλιφόρνια.

Η τεχνική σήραγγας VPN της Viprinet παρέχει πιο αξιόπιστες συνδέσεις στο Internet και αυξημένες ταχύτητες μεταφοράς δεδομένων. Επιτρέπει ένα νέο είδος υψηλής σύνδεσης για σταθερές καθώς και για κινητές τοποθεσίες. Με έναν πολυκαναλικό δρομολογητή VPN, πολλές ευρυζωνικές γραμμές μπορούν να συνδυαστούν σε μια ενιαία γραμμή υψηλής ευκρίνειας. Είναι δυνατό να συνδυάσετε έως και έξι φυσικούς συνδέσμους WAN. Η Viprinet ισχυρίζεται ότι η τεχνολογία της είναι πιο προηγμένη από την εξισορρόπηση φορτίου, η οποία μπορεί να διανέμει μόνο την κυκλοφορία σε αρκετούς συνδέσμους WAN.

Η λύση της Viprinet μπορεί να συνδυάσει τεχνολογίες πρόσβασης, όπως ADSL, SDSL, 3G / UMTS / HSPA + ή 4G / LTE. Το LAN θεωρεί αυτές τις συνδέσεις ως έναν σύνδεσμο που παρέχει το συσσωρευμένο προς τα πάνω και προς τα κάτω των διαφόρων συνδέσμων. Ωστόσο, η εταιρεία υποστηρίζει ότι το 10-15% του εύρους ζώνης καταναλώνεται με τη διαδικασία συγκόλλησης. Σύμφωνα με το Viprinet, η αξιοπιστία μιας σύνδεσης αυξάνεται έως και 99,9% όταν, για παράδειγμα, η 4G συνδέεται με ενσύρματη σύνδεση.

Το Viprinet χρησιμοποιεί μια εξαιρετική τεχνική σήραγγας VPN με μια τοπολογία αστέρα για γρήγορη και ασφαλή σύνδεση, εγκατάσταση και συνδεσιμότητα οχημάτων. Αυτή η διαδικασία απαιτεί την ενσωμάτωση δύο διαφορετικών συσκευών. Ένας πολυκαναλικός δρομολογητής VPN δημιουργεί μια κρυπτογραφημένη σήραγγα VPN σε έναν κεντρικό απομακρυσμένο σταθμό, τον πολυκαναλικό κόμβο VPN, μέσω κάθε διαθέσιμης γραμμής Internet. Αυτές οι σήραγγες VPN στη συνέχεια συνοδεύονται σε μία σήραγγα μέσω της οποίας μεταφέρονται τα δεδομένα.

Ο πολυκαναλικός κόμβος VPN εγκαθίσταται συνήθως σε ένα ασφαλές και επαρκώς συνδεδεμένο κέντρο δεδομένων και λειτουργεί ως ανταλλαγή. Τα δεδομένα που στοχεύουν σε άλλη τοποθεσία της εταιρείας θα προωθηθούν μέσω της συνδυασμένης σήραγγας VPN. Τα δεδομένα που στοχεύουν στο δημόσιο διαδίκτυο θα αποκρυπτογραφηθούν και θα μεταφερθούν στον προορισμό τους. Ο διανομέας VPN παρέχει αξιόπιστες και γρήγορες επικοινωνίες μεταξύ διαφόρων δρομολογητών VPN

πολλαπλών καναλιών. Επιπλέον, χρησιμεύει ως σημείο ανταλλαγής μεταξύ του κρυπτογραφημένου VPN και του δημόσιου διαδικτύου.

Το Viprinet μπορεί να ενσωματωθεί με ευελιξία στις υπάρχουσες υποδομές δικτύου. Αυτά μπορούν να επεκταθούν ή να αντικατασταθούν βήμα προς βήμα με οικονομικά αποδοτική λύση που εξασφαλίζει μεγαλύτερη διαθεσιμότητα. Επιπλέον, η λύση της Viprinet προσφέρει μεγαλύτερη ανεξαρτησία από τους ISP των επιχειρήσεων που χρησιμοποιούνται μέχρι σήμερα. Αυτό παρέχει μια καλή διαπραγματευτική θέση για την εταιρεία σε σχέση με τους μεμονωμένους φορείς παροχής Internet και λύσεων.

Το εύρος ζώνης και η καθυστέρηση όλων των συνδέσεων θα μετρηθούν. Από αυτές τις μετρήσεις προκύπτει το ιδανικό εύρος ζώνης για κάθε σύνδεση WAN καθώς και μια επισκόπηση του τρόπου με τον οποίο οι διάφοροι σύνδεσμοι WAN μπορούν να συντονιστούν λογικά με βάση τις λανθάνοντες χρόνο τους. Για αυτές τις μετρήσεις και προσαρμογές, το Viprinet παρέχει αυτόματες διαδικασίες (αυτόματη τάνυση) καθώς και χειροκίνητες προσαρμογές.

Δεδομένου ότι καμία κίνηση δεδομένων δεν είναι πανομοιότυπη με άλλη, η διαδικασία σύνδεσης που παρέχεται από το Viprinet επιτρέπει τη διαφορετική διαχείριση διαφορετικών τύπων κίνησης. Αυτό υλοποιείται μέσω της προκαταρκτικής εκπόνησης και της διανομής πακέτων δεδομένων εντός της συνδεδεμένης σήραγγας. Επιπλέον, η λύση της Viprinet επιτρέπει τη δυναμική διανομή των τύπων κίνησης στο διαθέσιμο εύρος ζώνης χρησιμοποιώντας τάξεις QoS που μπορούν να οριστούν ελεύθερα.

Λόγω ειδικών βελτιστοποιήσεων μεταφοράς, όπως η βελτιστοποίηση του TCP και της ροής, η τεχνολογία Viprinet μπορεί να χρησιμοποιηθεί σε σενάρια χρήσης που χρειάζονται πολύ εύρος ζώνης, όπως οι ενοποιημένες επικοινωνίες ή η ζωντανή μετάδοση βίντεο σε εκδηλώσεις, καθώς και στην κλασική σύνδεση μεταξύ τοποθεσιών. Η λύση της Viprinet μπορεί να εναρμονίσει και να συμπληρώσει ήδη υπάρχουσες υποδομές δικτύου με διάφορους τρόπους. Στις ακόλουθες υποενότητες, περιγράφονται δυο πιθανά επιχειρησιακά σενάρια.

4.3 International Site-to-Site VPN

Τα δίκτυα των εταιρειών είναι συχνά δομές που έχουν αυξηθεί εδώ και αρκετά χρόνια και, ως εκ τούτου, δεν μπορούν να αντικατασταθούν αμέσως. Σε πολλές περιπτώσεις, τα δίκτυα αυτά βασίζονται σε υποδομές MPLS που προσφέρονται ως υπηρεσία από εξωτερικούς παρόχους υπηρεσιών Διαδικτύου. Όταν μια εταιρεία δημιουργεί μια νέα τοποθεσία, πρέπει να συνδεθεί. Οι αλλαγές στην υπάρχουσα λύση MPLS σε σύντομο χρονικό διάστημα μπορεί να κοστίζουν ένα μεγάλο χρηματικό ποσό.

Μια μεγάλη διεθνής επιχείρηση από τη Γερμανία είχε ως στόχο τη σύνδεση αρκετών μεγαλύτερων και μικρότερων τοποθεσιών σε διάφορες χώρες σε όλο τον κόσμο μέσω του MPLS. Πολλές από αυτές τις νέες τοποθεσίες βρίσκονταν σε πολύ απομακρυσμένες περιοχές. Η υλοποίηση της πλήρους σύνδεσης μέσω του MPLS σε αυτά τα μέρη θα ήταν άσκοπη λόγω κόστους και λογικών λόγων.

Ωστόσο, η επιχείρηση συνέχισε να χρησιμοποιεί το MPLS για διηπειρωτικές συνδέσεις μεταξύ των περιφερειακών κεντρικών γραφείων, προκειμένου να διατηρήσει το κόστος για τη σύνδεση ενώ διατηρεί σταθερή ποιότητα. Σε αυτή την περίπτωση, οι συνδέσεις των τοπικών τοποθεσιών με τα σημεία παράδοσης MPLS έπρεπε να συνοψιστούν από χώρες και ηπείρους και να πραγματοποιηθούν μέσω της Viprinet.

Κατά συνέπεια, ένας hub κόμβος VPN Viprinet για κάθε ήπειρο (Ευρώπη, Βόρεια Αμερική, Νότια Αμερική) εγκαταστάθηκε σε ένα επαρκώς συνδεδεμένο κέντρο δεδομένων και οι νέες θέσεις εξοπλίστηκαν με έναν κατάλληλο πολυκαναλικό δρομολογητή VPN. Με αυτόν τον τρόπο, η κυκλοφορία δεδομένων από το Βερολίνο και το Λονδίνο τερματίζεται στο κέντρο της Ευρώπης, η κυκλοφορία από τη Νέα Υόρκη και το Λος Άντζελες καταλήγει σε κόμβο ΗΠΑ και η κυκλοφορία από το Σαντιάγκο της Χιλής καταλήγει στο κέντρο της Νότιας Αμερικής. Οι κόμβοι αυτοί συνδέονται μεταξύ τους μέσω του MPLS.

Υποστηρίζεται ότι σε σύγκριση με τις λύσεις που βασίζονται σε SDSL / IPSec και MPLS, μια λύση που βασίζεται πλήρως στην τεχνολογία του Viprinet μπορεί να οδηγήσει σε εξοικονόμηση περίπου 90%.

4.4 Redundant Site-to-Site VPN

Η τιμή των εταιρικών λύσεων MPLS που προσφέρονται από μεγάλους παρόχους τηλεπικοινωνιών είναι συχνά πολύ υψηλή. Ο λόγος για αυτό είναι ότι σε πολλές περιπτώσεις, η υποδομή MPLS δεν είναι διαθέσιμη στις αντίστοιχες τοποθεσίες και η υλοποίηση του δικτύου πρέπει να ξεκινήσει από την αρχή.

Αυτό έγινε σε μια γερμανική εταιρεία που είχε αναθέσει έναν μεγάλο πάροχο να εγκαταστήσει τις συνδέσεις στις τοποθεσίες της. Δεδομένου ότι η εταιρεία δεν έπρεπε πλέον να φροντίζει τις τοπικές συνδέσεις της, η εταιρεία δεν ήταν πλέον σε θέση να τροποποιήσει την υφιστάμενη υποδομή δικτύου ή να παρέμβει σε περίπτωση αποτυχίας. Επιπλέον, η εταιρεία εξαρτιόταν εξ ολοκλήρου από τον προμηθευτή της. Η σύνδεση μιας νέας θέσης οδήγησε σε διοικητικά έξοδα, καθώς ο πάροχος έπρεπε να ελέγξει εάν η λύση MPLS ήταν διαθέσιμη για αυτή τη θέση. Σε ορισμένες περιπτώσεις, μια νέα ανάπτυξη VPN σε κάθε τοποθεσία καθυστέρησε μερικές εβδομάδες και μήνες, ή το απαραίτητο χρηματικό ποσό για την υλοποίηση αυτού αυξήθηκε δραματικά.

Η εταιρεία επέστρεψε μέρος της ανεξαρτησίας της και αύξησε επίσης τη διαθεσιμότητα των θέσεών της με τη βοήθεια του Viprinet. Μια λύση σύνδεσης WAN εγκαταστάθηκε παράλληλα με την υπάρχουσα υποδομή MPLS. Ένας πολλαπλών καναλιών VPN δρομολογητής εγκαταστάθηκε σε κάθε χώρο δίπλα σε κάθε δρομολογητή MPLS και εξοπλισμένος με θερμές μονάδες βύσματος σύμφωνα με τις συνθήκες επί τόπου. Μέσα από αυτό, τα DSL και LTE μπορούν τώρα να συνδεθούν με μια ευρέως διαθέσιμη ευρυζωνική σύνδεση η οποία μεταδίδει τη ροή κατακερματισμένων δεδομένων σε ένα διανομέα Viprinet πολλαπλών καναλιών VPN. Ο διανομέας εγκαταστάθηκε ξεχωριστά από την υποδομή MPLS της εταιρείας σε ένα ασφαλές κέντρο δεδομένων. Ο κόμβος επανασυναρμολογεί τη ροή δεδομένων, αποκωδικοποιεί και προωθεί τον επιθυμητό στόχο στο δημόσιο διαδίκτυο ή στο intranet.

Μετά από αυτό, η εταιρεία ήταν σε θέση να αποφασίσει ανεξάρτητα εάν η κίνηση δεδομένων μεταφέρθηκε μέσω της υποδομής MPLS ή Viprinet. Αυτό θα μπορούσε να εφαρμοστεί δυναμικά σύμφωνα με τη διαθεσιμότητα και άλλες απαιτήσεις. Το μόνο που χρειαζόταν ήταν μια πύλη με μια ανάντη σύνδεση και στα δύο συστήματα που κατανέμονταν ανάλογα την κυκλοφορία δεδομένων.

Σε περίπτωση αποτυχίας της λύσης MPLS που διαχειρίζεται εξωτερικά, η τοποθεσία θα συνδεθεί ούτως ή άλλως με το Internet και με το intranet της εταιρείας.

Μέσα από αυτό, η εταιρεία έγινε ανεξάρτητη από τη διαθεσιμότητα της διαχειριζόμενης υπηρεσίας. Δεδομένου ότι υπάρχουν τώρα δύο παράλληλες συνδέσεις για να χρησιμοποιήσετε, έχουν επιτύχει περισσότερο εύρος ζώνης συνολικά. Ήταν δυνατή η εγκατάσταση του Viprinet ανεξάρτητα από την υπηρεσία που διαχειρίζεται. Αυτό σημαίνει ότι η εταιρεία βρίσκεται σε καλύτερη διαπραγματευτική θέση σε σχέση με αυτούς τους παρόχους.

4.5 Πολυκαναλικά VPN Hub και Router

Το Viprinet χρησιμοποιεί μια τεχνική σήραγγας VPN με μια τοπολογία αστέρα για ασφαλή και γρήγορη σύνδεση, εγκατάσταση και συνδεσιμότητα οχημάτων. Για αυτές τις υλοποιήσεις πρέπει να ενσωματωθούν δύο διαφορετικές συσκευές. Ο πολυκαναλικός κόμβος VPN χρησιμεύει ως συγκεντρωτής VPN για τις σήραγγες VPN που κατασκευάζονται από τους πολυκαναλικούς δρομολογητές VPN για τη μεταφορά δεδομένων μέσω πολλών ευρυζωνικών γραμμών. Αυτές οι δέσμες στη συνέχεια τερματίζονται στην τοπολογία αστέρα με ένα πολυκαναλικό κόμβο VPN σε ένα κέντρο δεδομένων. Εκεί, τα δεδομένα αποκρυπτογραφούνται και μεταφέρονται στον αρχικό προορισμό τους.

Υπάρχουν τρεις τύποι πολυκαναλικών κόμβων VPN που προσφέρει η Viprinet. Ο διανομέας VPN 1020 παρέχει δυνατότητα σύνδεσης μέχρι 200 MBit / s, γεγονός που καθιστά αυτό το διανομέα κατάλληλο για μικρά ή μεσαία δίκτυα εταιρειών. Ανάλογα με το διαθέσιμο εύρος ζώνης σε κάθε τοποθεσία, μπορούν να καλυφθούν δίκτυα εταιρειών που αποτελούνται από 10 έως 15 τοποθεσίες.

Ο διανομέας VPN 2030 έχει σχεδιαστεί για να παρέχει δυνατότητες συγκόλλησης στον τομέα των επιχειρήσεων. Ιδιαίτερα μεγάλες εταιρείες που χρειάζονται να συνδέσουν ένα μεγάλο αριθμό τοποθεσιών μπορούν να χρησιμοποιήσουν αυτό το μοντέλο αφού η ικανότητα συγκόλλησης είναι έως 500 MBit / s. Είναι δυνατό να τερματίσετε πολυάριθμους πολυκαναλικούς δρομολογητές VPN σε ένα μόνο διανομέα. Εδώ, το λεγόμενο σύστημα Redundancy Hub επιτρέπει υψηλή αξιοπιστία στη συντήρηση του απομακρυσμένου σταθμού. Εκτός από αυτούς τους κόμβους σε παραγωγική χρήση, ένας ή περισσότεροι εφεδρικοί (hot spare) διανομέας μπορούν, σε περίπτωση δυσλειτουργίας του διανομέα, να αναλάβουν όλες τις

λειτουργίες της ελαττωματικής συσκευής με μικρή καθυστέρηση. Ο διανομέας VPN 2030 χρειάζεται να έχει συνδρομή στη συντήρηση Viprinet Lifetime. Χωρίς αυτήν την άδεια χρήσης, οι ενημερώσεις και η υποστήριξη δεν θα είναι διαθέσιμες.

Ο πολλαπλών καναλιών VPN Hub 5010 έχει σχεδιαστεί για χρήση σε μεγάλους ISPs και επιχειρήσεις. Παρέχει ικανότητα σύνδεσης 2 GBit / s, η οποία επιτρέπει τη διαχείριση μεγάλου αριθμού πελατών. Ανάλογα με το σενάριο χρήστη, μπορεί να διαχειριστεί μέχρι 250 ιστότοπους VPN. Αυτό το μοντέλο μπορεί να λειτουργήσει σε δύο ξεχωριστά ηλεκτρικά κυκλώματα, καθώς διαθέτει δύο πλεονασματικές μονάδες τροφοδοσίας με καυτές φιάλες.

Η προαιρετική τμηματοποίηση της σήραγγας διανομέα επιτρέπει τον τερματισμό διαφόρων διαφορετικών πελατών στον ίδιο διανομέα VPN με την κυκλοφορία τους να διαχωρίζεται μεταξύ τους. Αυτή είναι μια επιλογή ειδικά σχεδιασμένη για χρήση από το ISP. Επιτρέπει πολλαπλές ρυθμίσεις, όπου διαφορετικοί πελάτες μπορούν να χρησιμοποιήσουν ακόμη και τον ίδιο χώρο ιδιωτικής διεύθυνσης IP χωρίς να δημιουργούν διενέξεις για την αντιμετώπιση IP. Η κατάτμηση της σήραγγας Hub επιτρέπει τη τοποθέτηση μιας ή περισσοτέρων σηράγγων σε ένα ειδικό τμήμα, παρόμοιο με τον τρόπο λειτουργίας των VLANs στον κόσμο LAN.

Ο πολυκαναλικός κόμβος VPN εγκαθίσταται συνήθως σε ένα εξαιρετικά ασφαλές κέντρο δεδομένων και λειτουργεί ως ανταλλαγή: Τα δεδομένα που απευθύνονται σε άλλο γραφείο της εταιρείας θα διαβιβαστούν μέσω της σχετικής σήραγγας VPN. Τα δεδομένα που στοχεύουν στο δημόσιο διαδίκτυο θα αποκρυπτογραφηθούν και θα μεταφερθούν στον προορισμό. Ο διανομέας VPN παρέχει ένα σημείο ανταλλαγής για ασφαλή και γρήγορη επικοινωνία μεταξύ των πολυκαναλικών δρομολογητών VPN. Επιπλέον, χρησιμεύει ως κεντρικό σημείο ανταλλαγής μεταξύ του κρυπτογραφημένου VPN και του δημόσιου Διαδικτύου.

Ο πολυκαναλικός δρομολογητής VPN Router 200, είναι ένας υβριδικός δρομολογητής ειδικά για χρήση σε οικιακά γραφεία και κατά τη διάρκεια ταξιδιών. Με αυτή τη συσκευή, μια υπάρχουσα σύνδεση στο Internet μπορεί να συνδεθεί με μια άλλη. Η υβριδική τεχνολογία συνδυάζει ένα σταθερό μέσο όπως DSL ή καλώδιο με μια κινητή σύνδεση δεδομένων όπως UMTS / 3G ή LTE / 4G.

Εδώ, οι αχρησιμοποίητες δυνατότητες αποστολής σε δίκτυα κινητής τηλεφωνίας χρησιμεύουν ως "upstream booster" για DSL. Μέσω αυτού, μια αργή σύνδεση DSL με 3 Mbit / s downstream και 300 Kbit / s upstream μετατρέπεται σε συμμετρικό σύνδεσμο που παρέχει αρκετά Megabit στην ανάντη κατεύθυνση, π.χ. για τηλεδιάσκεψη.

Το ενσωματωμένο σημείο πρόσβασης WiFi Router 200 του δρομολογητή με 2,4 ή 5 GHz (Dual Band) διανέμει εύρος ζώνης σε όλα τα διαθέσιμα τερματικά, όπως υπολογιστές και tablet. Ο υβριδικός δρομολογητής μπορεί να αναβαθμιστεί στις μελλοντικές τεχνολογίες, χάρη στην κατάλληλη υποδοχή της μονάδας.

Οι πολυκαναλικοί δρομολογητές VPN 300 και 310 είναι κατάλληλες συσκευές για τη σύνδεση μικρών γραφείων ή κινητών τοποθεσιών στο Διαδίκτυο ή ένα εταιρικό VPN. Συνδέοντας μέχρι τρεις διαφορετικές γραμμές Internet σε έναν ενιαίο εικονικό σύνδεσμο, η σύνδεση γίνεται τόσο αξιόπιστη όσο και γρήγορη. Ο παθητικά σχεδιασμένος επιτραπέζιος υπολογιστής κάνει τις συσκευές κατάλληλες για χρήση σε οικιακά γραφεία.

Οι δρομολογητές VPN 300 και 310 μπορούν να χρησιμοποιηθούν απευθείας σε σταθμούς εργασίας καθώς ψύχονται παθητικά. Η δομή του δικτύου μπορεί εύκολα να μεταβληθεί με τις μεταβαλλόμενες απαιτήσεις προσθέτοντας ή αφαιρώντας τα διαφορετικά μόντεμ καυτών βυσμάτων. Οι μέγιστες δυναμικότητες σύνδεσης είναι 100 MBit / s (Διακομιστής VPN πολλαπλών καναλιών 310) ή 50 MBit / s (Πολυκαναλικός δρομολογητής VPN 300). Σε συνδυασμό με το Multichannel VPN Hub 1020, οι συσκευές είναι ιδιαίτερα κατάλληλες για δίκτυα μικρών και μεσαίων εταιρειών.

Με τον πολυκαναλικό δρομολογητή VPN 2620 είναι δυνατό να συνδέσετε έως και έξι διαφορετικούς συνδέσμους WAN σε έναν ενιαίο εικονικό σύνδεσμο υψηλής απόδοσης. Η μέγιστη ικανότητα συγκόλλησης είναι 400 MBit / s. Με μοντέρνα modem plug, η δομή του δικτύου μπορεί να προσαρμοστεί μεμονωμένα στις μεταβαλλόμενες απαιτήσεις. Αυτό το μοντέλο είναι ιδανικό για μεσαίες και μεγάλες επιχειρήσεις. Ο πολυκαναλικός δρομολογητής VPN 2620 είναι ανθεκτικός και ανθεκτικός. Μπορεί να τοποθετηθεί σε ράφια 19 "με τις παρεχόμενες γωνίες στήριξης. Συνιστάται να συνδυάσετε το δρομολογητή 2620 με τον πολυκαναλικό διανομέα VPN 5010 κατά την εγκατάσταση μεσαίων και μεγάλων δικτύων εταιρειών.

ΒΙΒΛΙΟΓΡΑΦΙΑ-ΑΝΑΦΟΡΕΣ:

1 Microsoft Technet: WAN Technologies https://technet.microsoft.com/en-us/library/bb962087.aspx [ONLINE]

2 ExitingIP.com, Web publication: Rajesh K.: Introduction to WAN Optimization Techniques http://www.excitingip.com/459/introduction-to-wan-optimization-techniques/ [ONLINE]

3 Viprinet GmbH company Website: Implementation and design of Viprinet for largescale networks https://www.viprinet.com/en/solutions/industries/alternative-to-leased-lines-andmpls [ONLINE]

4 Viprinet White paper: Always Online – Wherever and whenever needed https://www.viprinet.com/en/download/2324/viprinet-whitepaper-principle-en.pdf?redirect=node/1050 [ONLINE, premium download]

5 IHS Markit Ltd, Newsroom: HIS Businesses Losing $700 Billion a Year to IT Downtime http://press.ihs.com/press-release/technology/businesses-losing-700-billion-year-itdowntime-says-ihs [ONLINE]

6 Viprinet Product Folder: Never Be Offline Again https://www.viprinet.com/sites/default/files/files/viprinet_product_folder_web_en.pdf [ONLINE]

7 Viprinet White paper: Security of Corporate Networks https://www.viprinet.com/en/download/2834/viprinet-whitepaper-security en.pdf?redirect=node/1369 [ONLINE, Premium Download]

8 Global mobile suppliers Association, GSA: Global LTE Subscriptions Forecast to 2020 http://gsacom.com/paper/global-lte-subscriptions-forecast-to-2020/ [ONLINE]

9 BBC News: Fastest mobile 4G network speed record 'broken' http://www.bbc.com/news/technology-37221565 [ONLINE]

10 Qualitative Research Methods: A Data Collector's Field Guide, page 1 http://www.ccs.neu.edu/course/is4800sp12/resources/qualmethods.pdf [ONLINE]

11 Cisco: Introduction to WAN Technologies http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies [ONLINE]

12 Cisco Networking Academy, Connecting Networks Companion Guide: Connecting to the WAN, Chapter 4 http://www.ciscopress.com/articles/article.asp?p=2202411&seqNum=4 [ONLINE]

13 TechTarget, Search WinDevelopment, post by Margaret Rouse: Definition: ISP (Internet service provider) http://searchwindevelopment.techtarget.com/definition/ISP [ONLINE]

14 Cisco Networking Academy (CCNA 4), Chapter 2: WAN Access Options https://static-course-assets.s3.amazonaws.com/CN503/en/index.html#2.2.1.1 [ONLINE]

15 TechTarget, Search Enterprise WAN, Post by Margaret Rouse: Wide Area Ethernet (WAE) http://searchenterprisewan.techtarget.com/definition/Wide-Area-Ethernet-WAE [ONLINE]

16 Viprinet GmbH, Company Website: Broadband Internet via DSL bonding https://www.viprinet.com/en/technology/combinable-media/dsl [ONLINE]

17 Viprinet GmbH, company Website: Satellite radio, cable and WiMAX bonding - alternatives to DSL & Co. https://www.viprinet.com/en/technology/combinable media/cable-satellite-andethernet [ONLINE]

18 TechTarget, Search Enterprise WAN, post by Margaret Rouse: DOCSIS (Data Over Cable Service Interface Specifications) http://searchnetworking.techtarget.com/definition/DOCSIS [ONLINE]

19 Figure of a Cable System Principle http://vtvnet.net/cong-nghe-cmts-su-dung-tren-internet-vtvnet-la-gi.html [ONLINE]

20 Viprinet GmbH, Company Website: Mobile Internet by Bonding UMTS / 3G and CDMA https://www.viprinet.com/en/technology/combinable-media/umts-cdma-3g [ONLINE]

21 Netradar, An Application Provided by Researchers at Aalto University, the Department of Communications and Networking https://www.netradar.org/en [ONLINE]

22 Ericsson, White paper: 5G Radio Access, pages 2-3 (Uen 284 23-3204 Rev C | April 2016) https://www.ericsson.com/res/docs/whitepapers/wp-5g.pdf [ONLINE]

23 TechTarget, Search Enterprise WAN, post by Margaret Rouse: Multiprotocol Label Switching (MPLS)

http://searchenterprisewan.techtarget.com/definition/Multiprotocol-Label-Switching [ONLINE]

24 Microsoft Technet library: How VPN Works https://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx [ONLINE]