Το πρωτόκολλο PPTP στο VPN

Εισαγωγή

- Για VPN μικρής γεωγραφικής εμβέλειας ή για περιπτώσεις όπου η εταιρία ενδιαφέρεται απλά και μόνο στο να δώσει πρόσβαση σε απομακρυσμένους κινητούς πελάτες της, τα πρωτόκολλα PPTP και L2TP προτιμώνται από το IPSec (χωρίς αυτό να σημαίνει ότι το IPSec δεν μπορεί να εφαρμοστεί και σε αυτές τις περιπτώσεις).
- Το PPTP είναι πρωτόκολλο εγκαθίδρυσης διόδου (tunneling) που προτάθηκε από τη Microsoft και την Ascend. Σύντομα έγινε δημοφιλές. Ταυτόχρονα η Cisco είχε προτείνει το L2F. Ως διάδοχος αυτών των δύο εμφανίστηκε το L2TP, που υποστηρίχτηκε από όλες τις εταιρίες για να γίνει πρότυπο.
- Η εξάπλωση του PPTP οδηγεί στην ανάγκη το να αναλυθεί ξέχωρα από το L2TP.

Τι είναι το PPTP?

- Point-to-Point Tunneling Protocol: δημιουργήθηκε από τις εταιρίες 3Com, Ascend Communications, Microsoft, ECI Telematics και US Robotics.
- Στόχος ήταν το να καταστεί δυνατό ένας χρήστης να συνδέεται απλά στον ISP μέσω μίας απλής τηλεφωνικής κλήσης, και στη συνέχεια μέσω αυτού να συνδέεται με ασφάλεια στο ιδιωτικό δίκτυο.

Γενικά χαρακτηριστικά του PPTP

- Βασίζεται στο βασικό πρωτόκολλο τηλεφωνικής πρόσβασης (dial-up access) στο Ίντερνετ, το **PPP (Point-to-Point-Protocol).**
- Ενθυλακώνει PPP πακέτα με τη χρήση μίας τροποποιημένης έκδοσης του **GRE** πρωτοκόλλου (**Generic Routing Encapsulation**), δίνοντας έτσι τη δυνατότητα να μπορούν να χρησιμοποιηθούν και πακέτα που δεν είναι απαραίτητα IP, όπως IPX, NETBEUI (πλεονέκτημά του έναντι του IPSec).
- Έχει τους ίδιους μηχανισμούς πιστοποίησης ταυτότητας με το PPP, δηλαδή PAP και CHAP. Επίσης το PPP χρησιμοποιείται για την κρυπτογράφηση, αν και η Microsoft έχει αναπτύξει μία καλύτερη μέθοδο κρυπτογράφησης, την MPPE (Microsoft Point-to-Point Encryption). Πάντως η κρυπτογράφηση σε καμία από τις δύο περιπτώσεις δεν είναι τόσο καλή όσο αυτή του IPSec.
- Είναι πρωτόκολλο επιπέδου 2 του OSI.
- Ορίζει διαφόρων ειδών διόδων (tunnels), αναλόγως των άκρων της διόδου και των μηχανισμών πιστοποίησης.

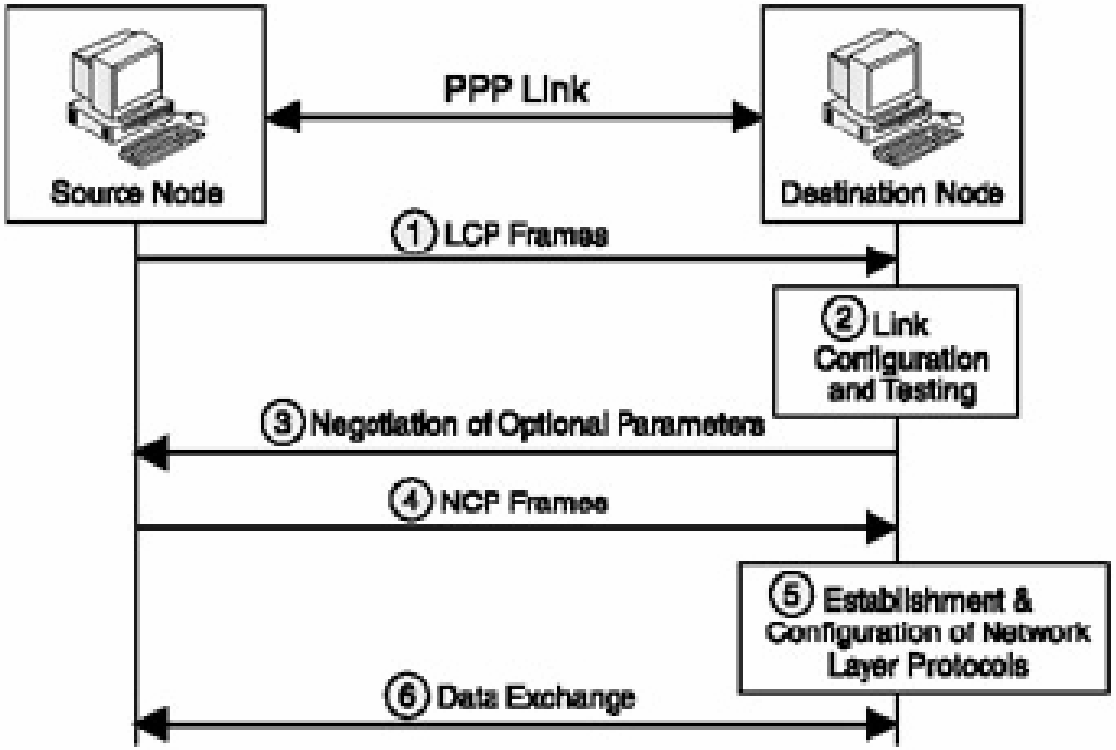
Περιγραφή του PPP

- Πρωτόκολλο επιπέδου 2: Περιλαμβάνει τεχνικές για ενθυλάκωση πακέτων διαφόρων τύπων, προκειμένου να μεταδοθούν σε μία ζεύξη.
- Περιέχει δύο σετ πρωτοκόλλων:
  - Link Control Protocols (LCP) για εγκαθίδρυση και έλεγχο της ζεύξης μετάδοσης
  - Network Control Protocols (NCP) για εγκαθίδρυση και έλεγχο διαφορετικών πρωτοκόλλων επιπέδου δικτύου.

Λειτουργία του PPP

- Ενθυλακώνει πακέτα IP, IPX και NETBEUEI σε PPP πλαίσια, πραγματοποιώντας μία σημείο-προς-σημείο ζεύξη μεταξύ του αποστολέα και του δέκτη. Για τη δημιουργία της σύνδεσης, καθένας από τους συνδιαλεγομένους πρέπει πρώτα να στείλει LCP πακέτα.
- Η πιστοποίηση ταυτότητας γενικά είναι προαιρετική στο PPP: ωστόσο, πρέπει οπωσδήποτε να υπάρχει όταν γίνεται εφαρμογή του σε VPN. Το PPP το πετυχαίνει αυτό είτε με PAP είτε με CHAP (το δεύτερο είναι πιο ασφαλές).
  - Η IETF στο RFC 2284 πρότεινε πιο καλές τεχνικές πιστοποίησης ταυτότητας, το Extensible Authentication Protocol (EAP), το οποίο υποστηρίζει πολλές διαφορετικές τεχνικές πιστοποίησης.
- Μετά την εγκαθίδρυση της ζεύξης, NCP πακέτα ανταλλάσσονται για έλεγχο και προσδιορισμό των πρωτοκόλλων επιπέδου δικτύου. Αφού προσδιοριστούν τα πρωτόκολλα αυτά, τα πλαίσια τους (datagrams) μεταφέρονται πάνω στη ζεύξη.

Σχηματική αναπαράσταση του PPP



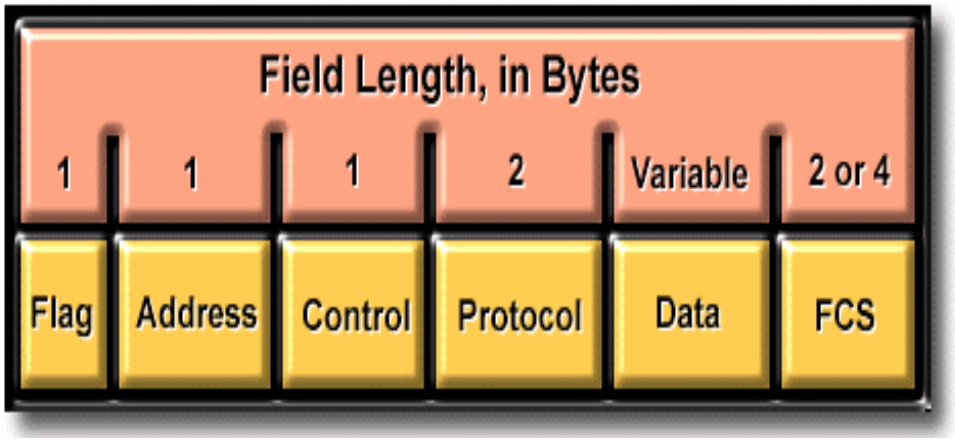
Δομή ενός πλαισίου PPP

•**Flag**: υποδηλώνει την αρχή του πλαισίου – ισούται πάντα με 01111110.

•**Address:** Αποτελείται πάντα από 11111111 (μια που στο PPP η ζεύξη είναι απευθείας, άρα δεν χρειάζεται διεύθυνση παραλήπτη).

•**Control:** Αποτελείται στο PPP πάντα από το byte 00000011.

•**Protocol:** 2 bytes, που προσδιορίζουν το πρωτόκολλο ανώτερου επιπέδου που ενθυλακώνεται στο PPP πλαίσιο



•**Data:** Το ενθυλακωμένο πλαίσιο (datagram) του επιπέδου δικτύου (ή πληροφορίες ελέγχου αν είναι PPP πλαίσιο ελέγχου). Το τέλος του ανιχνεύεται από ένα πεδίο flag.

•**Frame Check Sequence (FCS):** χρησιμοποιείται για ανίχνευση σφαλμάτων στο PPP πλαίσιο

Εξάρτηση PPTP από PPP

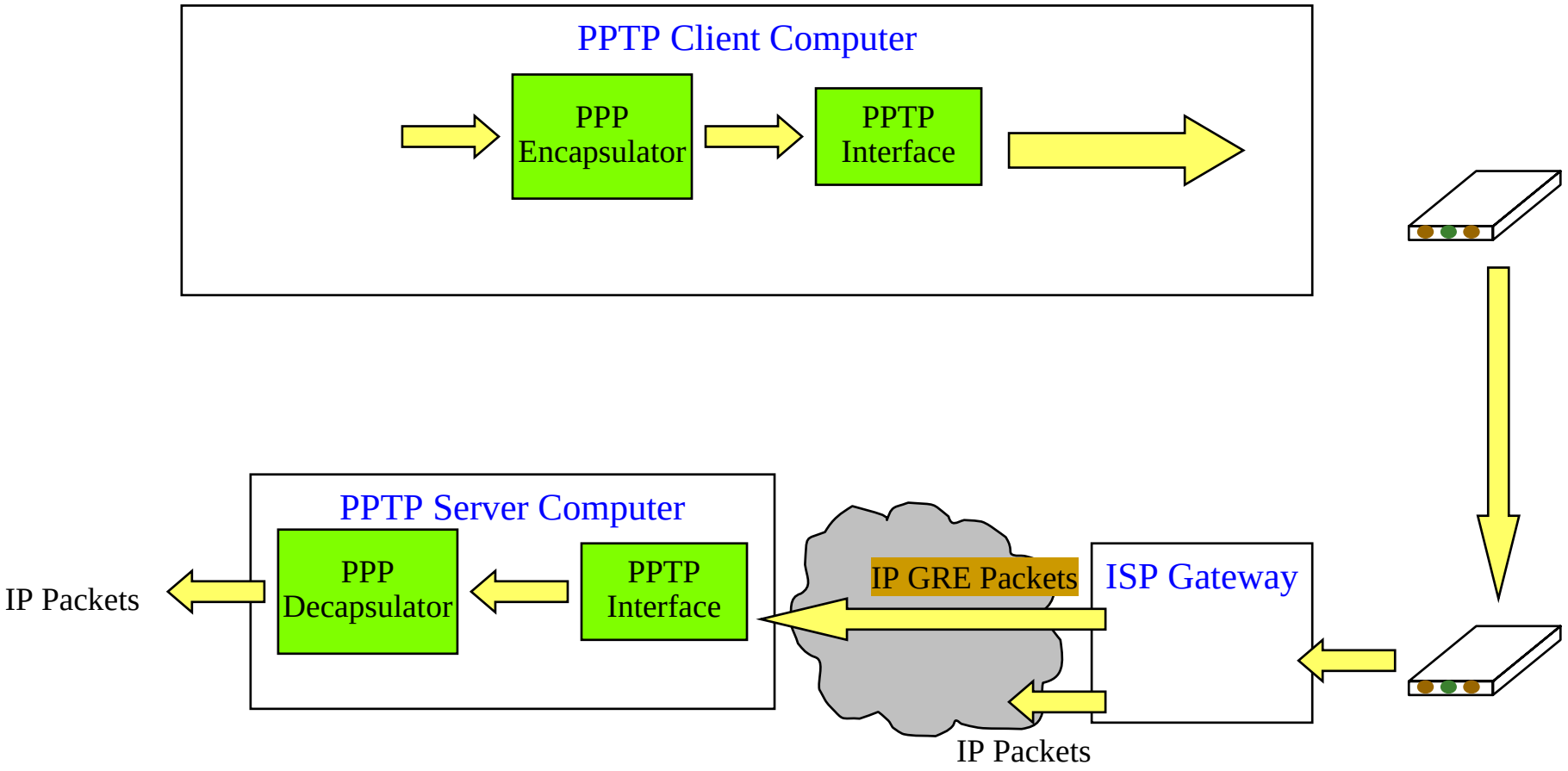
- Το PPTP περιμένει από το PPP τις ακόλουθες λειτουργίες:
  - Εγκαθίδρυση της φυσικής ζεύξης
  - Πιστοποίηση των χρηστών
  - Δημιουργία PPP πλαισίων

- Στη συνέχεια, το PPTP ενθυλακώνει PPP πακέτα, για τη μετάδοση μέσω μίας διόδου (tunnel).

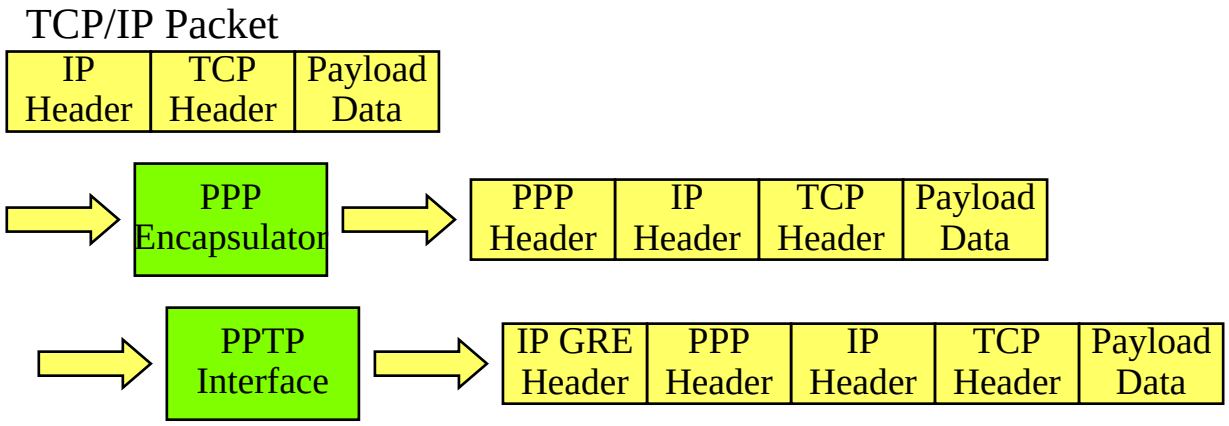
Πακέτα στο PPTP

- Δύο ειδών:
  - Πακέτα ελέγχου
  - Πακέτα δεδομένων
- Μετά την εγκατάσταση της PPTP διόδου, τα δεδομένα μεταφέρονται μεταξύ του «πελάτη» (client) και του PPTP εξυπηρετητή (server). Ο client μπορεί να είναι είτε πρόγραμμα στον υπολογιστή ενός χρήστη είτε πρόγραμμα στον ISP.
- Τα δεδομένα μεταφέρονται σε IP πακέτα, που εμπεριέχουν PPP πλαίσια. **Τα IP πακέτα δημιουργούνται με μια τροποποιημένη έκδοση του GRE.**

Σχηματικό παράδειγμα PPTP διόδου



Ενθυλάκωση PPTP



Περιγραφή των RAS (Remote Access Server) και NAS (Network Access Server)

REMOTE ACCESS SERVER: Συλλογή από modems και κατάλληλο λογισμικό που επιτρέπει dial-in συνδέσεις.
Έχει Interface με έναν telecom operator (PSTN, ISDN).
Λαμβάνει κλήσεις μέσω dial-up.

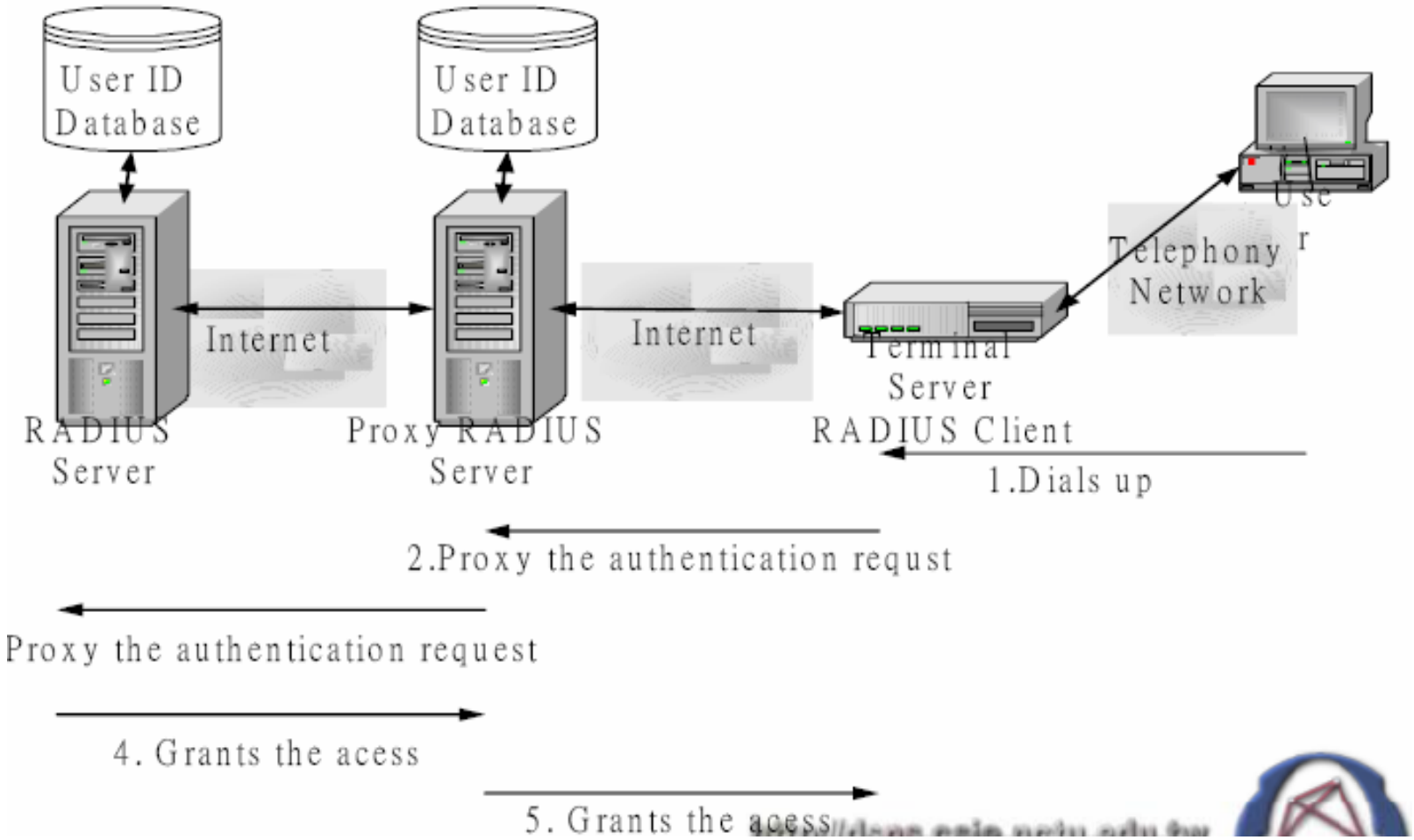
Μηχανισμοί αυθεντικοποίησης:

- TACACS (Terminal Access Controller Access Control System)
- RADIUS (Remote Authentication of Dial-up Users Services)

Χρήση του RADIUS

- Μοντέλο πελάτη-εξυπηρετητή. Χρησιμοποιεί NAS, ο οποίος στο RADIUS δρα σαν πελάτης (client). Ο NAS είναι υπεύθυνος να δέχεται τις αιτήσεις των χρηστών, να παίρνει ID και passwords από αυτούς, και να τα προωθεί στον RADIUS server. Ο RADIUS Server ενημερώνει για το αν εγκρίνει την πρόσβαση ή όχι.
- Ο RADIUS διατηρεί μία κεντρική βάση δεδομένων των χρηστών με τις αντίστοιχες υπηρεσίες.
- Διατηρεί διάφορα στοιχεία της διόδου: το ποιο πρωτόκολλο χρησιμοποιείται (PPTP ή L2TP), τη διεύθυνση του άκρου της διόδου, καθώς και τη διεύθυνση του NAS (για πληροφορίες στατιστικής φύσεως της χρήσης της ζεύξης).
- Συχνά υπάρχουν και RADIUS proxy servers, οι οποίοι είναι εγκατεστημένοι στους ISPs και ενημερώνονται ανά περιοδικά διαστήματα από τον κεντρικό RADIUS server.

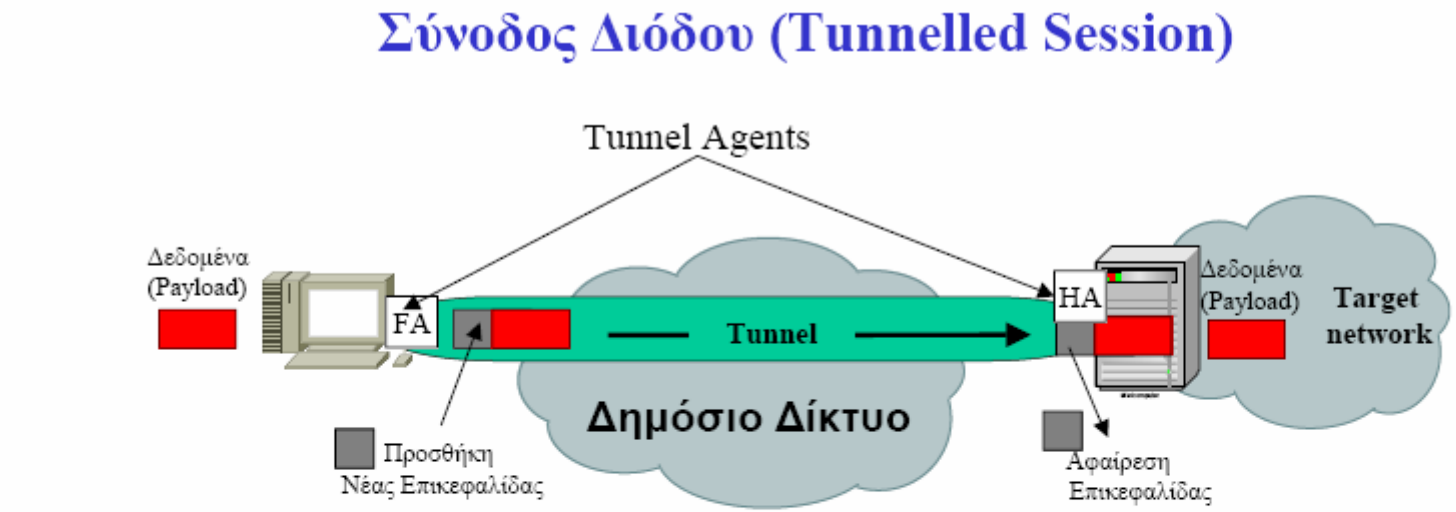
RADIUS με proxy server



Δίοδοι (tunnels)

- Δίοδος (tunnel): τεχνική ενθυλάκωσης ενός πακέτου/πλαισίου σε ένα άλλο πακέτο/πλαίσιο διαφορετικού πρωτοκόλλου. Η δρομολόγησή του γίνεται σε ένα ιδεατό κύκλωμα (tunnel). Ο δέκτης μετατρέπει το λαμβανόμενο πακέτο στην αρχική του μορφή.
- **Στο PPTP, οι ζεύξεις γίνονται πάνω σε διόδους (tunnels)**
- Οι δυνατότητες του υπολογιστή του χρήστη καθορίζουν το άκρο της διόδου: αν ο υπολογιστής έχει PPTP software τότε αυτός είναι το άκρο της διόδου. Διαφορετικά, αν υποστηρίζει μόνο PPP και όχι PPTP, τότε το άκρο της διόδου βρίσκεται στον ISP και συγκεκριμένα στον RAS (Remote Access Server).
- Οι δίοδοι μπορούν να είναι δύο ειδών: **αυθόρμητες δίοδοι (voluntary tunnels)** και **αναγκαστικές δίοδοι (compulsory tunnels).** Οι πρώτες δημιουργούνται μετά από αίτηση του χρήστη, ενώ οι αναγκαστικές δημιουργούνται αυτόματα, χωρίς καμία παρεμβολή από τον χρήστη.

Σχηματική αναπαράσταση διόδου



- Υποστηρίζεται από δύο end-points:

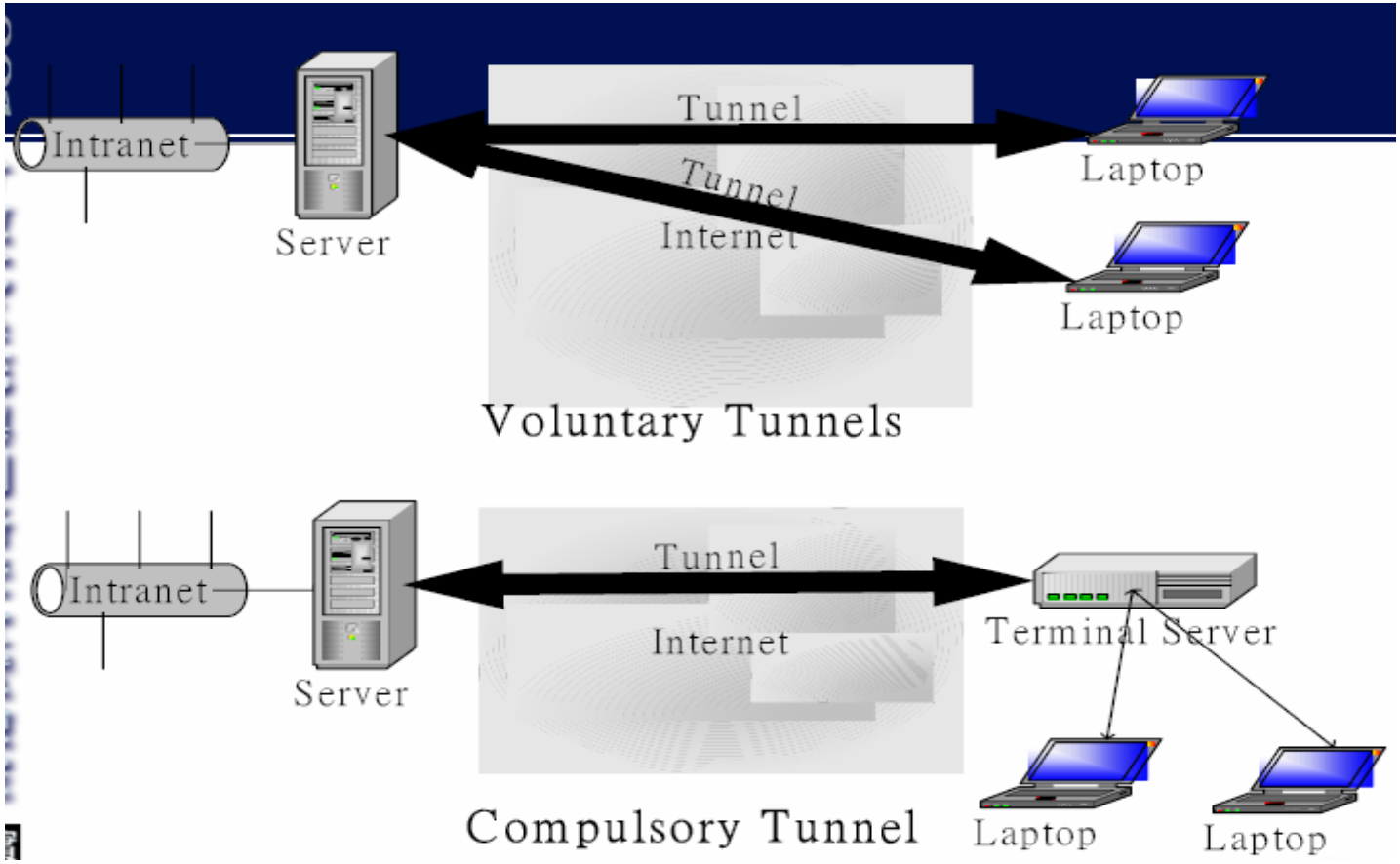
  tunnel client (initiator node) και target network

- Και δύο Agents:

  Home και Foreign Agents (AH και FA) ⟶ Software interfaces

- Για τη δημιουργία μιας διόδου και οι δύο agents πρέπει να υποστηρίζουν το ίδιο πρωτόκολλο διόδου

Είδη διόδων (σχηματική αναπαράσταση)



Γενικά χαρακτηριστικά των διόδων

- Μία αναγκαστική δίοδος έχει προκαθορισμένα ακραία σημεία, άρα ο έλεγχος πρόσβασης είναι πιο εύκολος. Δίνει επίσης τη δυνατότητα, αν η πολιτική της εταιρίας είναι τέτοια, να μην έχουν πρόσβαση στο Internet οι εργαζόμενοι αλλά να χρησιμοποιούν τις Internet ζεύξεις για το VPN.
- Επίσης στις αναγκαστικές διόδους μπορούν πολλαπλές συνδέσεις να υπάρχουν πάνω σε μία δίοδο. Ένα μειονέκτημα είναι ότι η σύνδεση του υπολογιστή του χρήστη με τον RAS είναι έξω από τη δίοδο και, συνεπώς, μη ασφαλής. Γενικά, οι αυθόρμητες δίοδοι προσφέρουν μεγαλύτερη ασφάλεια.

Υποκατηγορίες αναγκαστικών διόδων

- Στατικές δίοδοι (static compulsory tunnels):
  - Realm-based: ο RAS ελέγχει ένα τμήμα του ονόματος του χρήστη, τον *τομέα (realm)* και με βάση αυτό αποφασίζει τη δρομολόγηση της διόδου αυτού του χρήστη
  - *Automatic:* Υπάρχει προεγκατεστημένος εξοπλισμός – ο χρήστης καλεί ένα συγκεκριμένο τηλεφωνικό αριθμό για να έχει πρόσβαση στο VPN (να ξεκινήσει μία δίοδος)

- Δυναμικές δίοδοι (dynamic compulsory tunnels):
  - Με βάση την αίτηση κάθε χρήστη, γίνεται σύνδεσή του με τον RAS. Χρειάζεται ένας RADIUS server για την εξουσιοδότηση του χρήστη.

Περιγραφή των κλάσεων των διόδων

- Οι στατικές δίοδοι χρειάζονται έναν NAS (Network Access Server) για κάθε δίοδο. Αυτό «κοστίζει» στον ISP. Συνεπώς, για συστήματα με πολλούς ταυτόχρονους χρήστες δεν συνιστάται αυτή η λύση.
- Οι realm-based δίοδοι χειρίζονται όλους τους χρήστες του ίδιου τομέα με τον ίδιο τρόπο – αυτό μειώνει την «ευλυγισία» του συστήματος.

Γενικός τρόπος λειτουργίας PPTP

- Παρέχει νέο τρόπο για μεταφορά PPP πακέτων πάνω σε μη ασφαλή μέσο (Internet)

• Υπάρχουν Servers ειδικού σκοπού που λειτουργούν ως ενδιάμεσοι (NAS) ή τελικοί (RAS) για την εγκαθίδρυση του tunnel (Stage 1).

• Υπάρχουν τρεις περιπτώσεις:

  • Άμεση πρόσβαση στο corporate LAN's RAS (PPTP Server)

  • Πρόσβαση μέσω ISP που δεν υποστηρίζει PPTP στο corporate LAN's RAS (PPTP Server)

  • Πρόσβαση μέσω ISP που υποστηρίζει PPTP στο corporate LAN's RAS (PPTP Server)

• Εδώ εξετάζεται διεξοδικά η 3η περίπτωση. Βήματα:

Ένας dial-up χρήστης καλεί έναν Net. Access Switch (μέσω PPP) στον ISP provider

Ο χρήστης έχει δηλώσει στο profile του τον upstream RAS Server

Η PPP σύνοδος «οδεύεται» (tunneled) στον RAS Server του Corporate LAN

Εγκαθιδρύεται η PPTP σύνοδος μεταξύ του client και του upstream PPTP Server που επιθυμεί ο client υπό την προϋπόθεση ότι μπορεί να εντοπιστεί μέσω routing ο upstream RAS Server

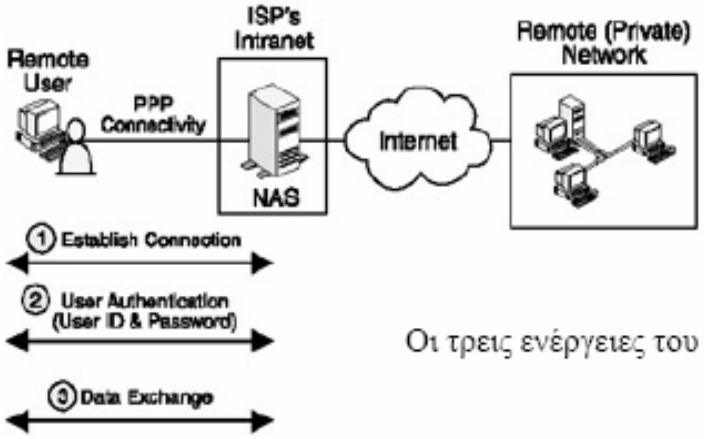
Φάσεις λειτουργίας PPTP – Φάση 1 (χρήση του PPP)

- Το PPP συνδράμει με το να

  - Εγκαθιδρύει – τερματίζει τις physical συνδέσεις μεταξύ των άκρων της επικοινωνίας

  - Αυθεντικοποιεί PPTP clients

  - Κρυπτογραφεί IPX, NetBEUI, ή TCP/IP datagrams για να παράγει PPP datagrams και να διασφαλίσει την ανταλλαγή δεδομένων μεταξύ άκρων της επικοινωνίας

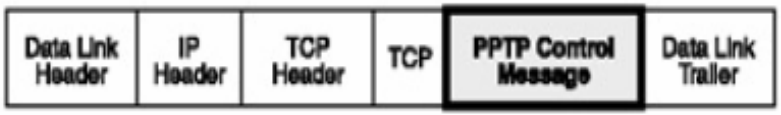


Οι τρεις ενέργειες του PPP σε ένα PPTP transaction.

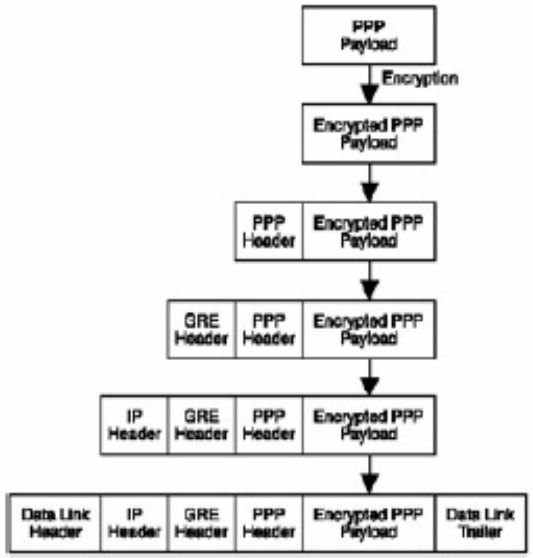
Φάσεις λειτουργίας PPTP – Φάση 2 (λογική εγκαθίδρυση του PPTP)

Ανταλλάσσονται μηνύματα ελέγχου μεταξύ PPTP client και PPTP Server (RAS) για τη διατήρηση αλλά και τον τερματισμό (στο τέλος) της διόδου. Τα μηνύματα αυτά ανταλλάσσονται με βάση τις IP διευθύνσεις τους, στην 1723 TCP θύρα του RAS.

Τα PPTP μηνύματα ελέγχου ενθυλακώνονται σε TCP/IP πακέτα



Φάσεις λειτουργίας PPTP – Φάση 3 (PPTP tunelling – μεταφορά δεδομένων)



Encapsulation of data. Το PPP payload κρυπτογραφείται και ενθυλακώνεται σε ένα PPP frame. Ο PPP header προστίθεται στο frame.

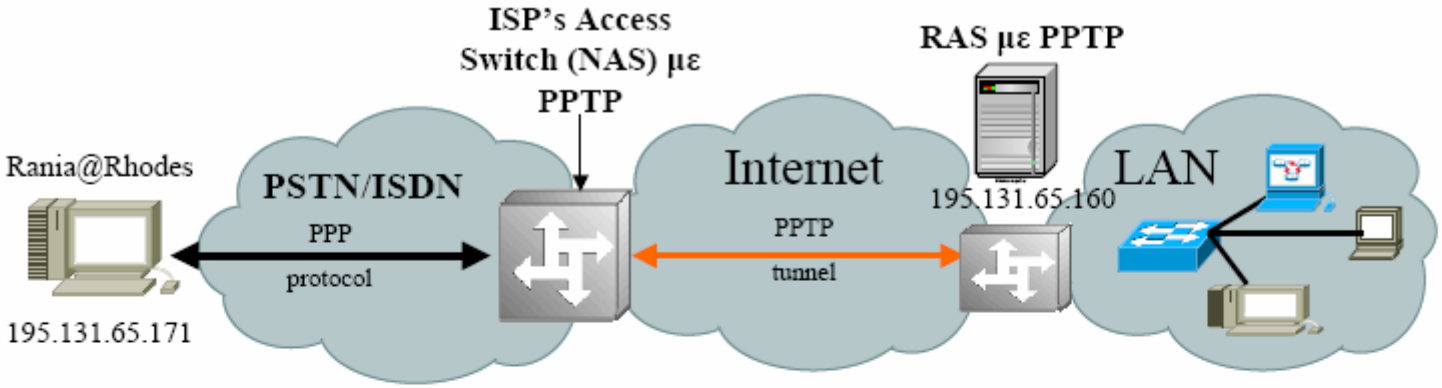
Encapsulation of PPP frames. Το PPP frame ενθυλακώνεται στο Generic Routing Encapsulation (GRE).

Encapsulation of GRE packets. Έπειτα, ένας IP header προστίθεται στο PPP frame, που είναι ήδη ενθυλακωμένο στο GRE packet. Ο header περιέχει την IP addresses του PPTP client και του destination server.

Data Link layer encapsulation. Το PPTP είναι Layer 2 tunneling protocol. Αν το datagram πρέπει να περάσει μέσα από ένα WAN PPTP tunnel, τότε το datagram ενθυλακώνεται με header και trailer του PPP.

Το GRE είναι ένα απλό γενικής χρήσεως πρωτόκολλο για IP μετάδοση. Χρησιμοποιείται από τους ISPs για να προωθούν πληροφορίες δρομολόγησης.

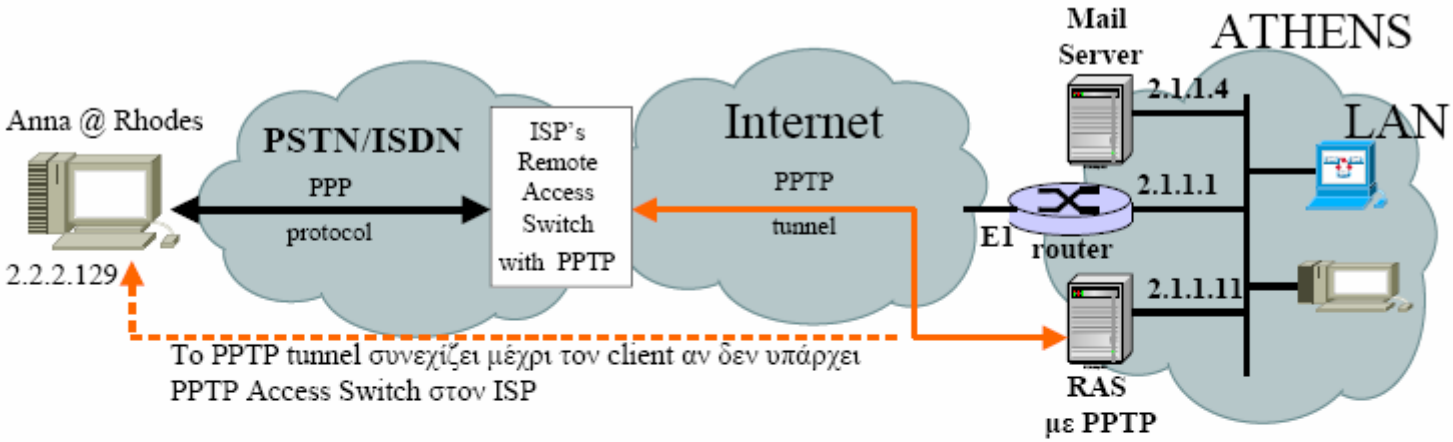
PPTP δίοδος, όταν ο ISP διαθέτει NAS



1. Η Rania ξεκινά με Dial-up στον ISP's με χρήση PPP, και login με όνομα "Rania"
2. Ο ISP διατηρεί στο "profile" της Rania την upstream corporate RAS Server IP Address : 195.131.65.160
3. Αυτό ξεκινά μία PPTP σύνδεση μεταξύ του ISP Access Switch και του RAS στο LAN
4. Η σύνοδος PPP της Rania οδεύει (tunneled) μέσω του PPTP upstream
5. Ο RAS server authenticates το username και το password και ενεργοποιεί την PPP σύνοδο με την Rania .
6. Η σύνοδος PPTP είναι έτοιμη να μεταφέρει (tunnel) τα πρωτοκόλλα που επιτρέπεται να χρησιμοποιεί η dial-up χρήστης Rania.
7. Π.χ. Για το TCP/IP ο RAS server θέτει στην μηχανή της Rania μία "εσωτερική" IP address π.χ. 195.131.65.171

Πηγή: Oreilly - Virtual Private Networks, Second Edition

PPTP δίοδος, με ISP που διαθέτει RAS με PPTP δυνατότητα



Η Rania θέλει να δει τα mails της

Dialup με ISP που διαθέτει PPTP-enabled remote access switch.

Αφού αυθεντικοποιηθεί από το switch, ξεκινά ένα PPTP call προς το RAS server, όπως ορίζεται από το profile της.

Στο router, η TCP/IP PPTP πόρτα - socket (1723) πρέπει να είναι ανοικτή.

Πηγή: Oreilly - Virtual Private Networks, Second Edition

Πιστοποίηση ταυτότητας και κρυπτογράφηση στο PPTP

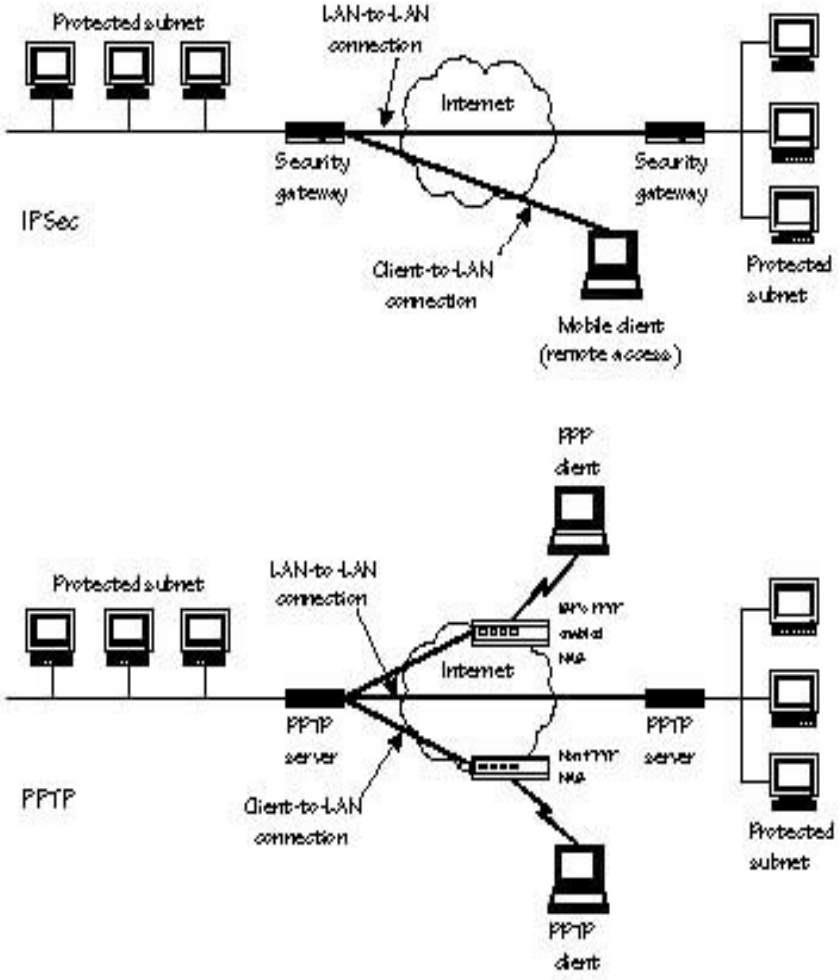
- Τεχνικές ίδιες με αυτές του PPP: CHAP, PAP (Βλέπε διαφάνειες κεφαλαίου 4). Δεν είναι όμως πολύ ασφαλείς, αφού τα passwords βρίσκονται σε κάποιον υπολογιστή.
- Πρόταση της Microsoft: Microsoft Point-to-Point Encryption (MPPE): κάνει ταυτόχρονα κρυπτογράφηση των δεδομένων (με τα πρωτόκολλο RSA RC4) και πιστοποίηση ταυτότητας με το MS-CHAP. Το κλειδί κρυπτογράφησης προκύπτει από εφαρμογή μίας συνάρτησης κατακερματισμού στο password, το οποίο βρίσκεται αποθηκευμένο και στον υπολογιστή του χρήστη αλλά και στον server. Το κλειδί είναι μήκους 40bit, αλλά υπάρχει η δυνατότητα με πρόσθετο software να γίνει 128 bit. Η κρυπτογράφηση γίνεται στον υπολογιστή του χρήστη, προτού τα δεδομένα φτάσουν στον PPTP server – το οποίο προσδίδει πρόσθετη ασφάλεια.

Μπορούν να υπάρξουν LAN-to-LAN tunnels με PPTP?

- Την αρχή την έκανε η Microsoft: Routing and Remote Access Server (RRAS) στα Windows NT (ακολούθησαν και άλλες εταιρίες).
- RRAS: LAN-to-LAN δίοδοι μεταξύ δύο PPTP servers, κατά πλήρη αναλογία με τα tunnels του IPSec μεταξύ πυλών ασφαλείας (gateways). Όμως το PPTP δεν υποστηρίζει διαχείριση κλειδιού (κάτι ανάλογο του IKE): το CHAP ή το MS-CHAP παίζουν τον ρόλο αυτό. Στην ουσία, κάθε ένας PPTP server συμπεριφέρεται σαν client ως προς τον άλλον (ζητάει πρόσβαση με βάση το password κ.ο.κ.)

Σύγκριση IPSec και PPTP

- Ο PPTP server είναι το ανάλογο της πύλης ασφαλείας (security gateway)
- Το πρόγραμμα (software) του PPTP client έχει πολλά κοινά με το software του IPSec client, αν και δεν κάνει ανταλλαγές κλειδιών.



Δομικά στοιχεία για το PPTP

- NAS (Network Access Server) (υπευθυνότητα του ISP).
- PPTP Server
- PPTP Client

Περιγραφή των PPTP servers

- Έχουν δύο κύριους ρόλους:
  - Είναι ακραία (τελικά) σημεία σε μία δίοδο
  - Προωθούν πακέτα από και προς το αντίστοιχο LAN
- Επίσης «φιλτράρουν» τα πακέτα (PPTP filtering). Με αυτόν τον τρόπο θέτει περιορισμούς στο ποιος θα έχει πρόσβαση στο τοπικό δίκτυο.
- Μόνο από την TCP/IP πόρτα 1723 περνούν τα δεδομένα – αυτό καθιστά τα PPTP συστήματα ευαίσθητα σε επιθέσεις.
- Επέκταση των PPTP servers είναι τα λεγόμενα tunnel switches (εισήχθηκαν στην αγορά από την 3Com)

Περιγραφή των PPTP clients

- Αν ο ISP διαθέτει PPTP δυνατότητα, δεν χρειάζεται πρόσθετο PPTP software στον client. Αν δεν υπάρχει η δυνατότητα, τότε ένας client δημιουργεί ένα tunnel, πρώτα εγκαθιστώντας μία PPP σύνδεση με τον ISP.
- Χρειάζεται συμβατότητα του PPTP software του client με αυτό του server. Για παράδειγμα, δεν υποστηρίζουν όλα MS-CHAP κι έτσι δεν μπορούν να εκμεταλλευθούν το RRAS.

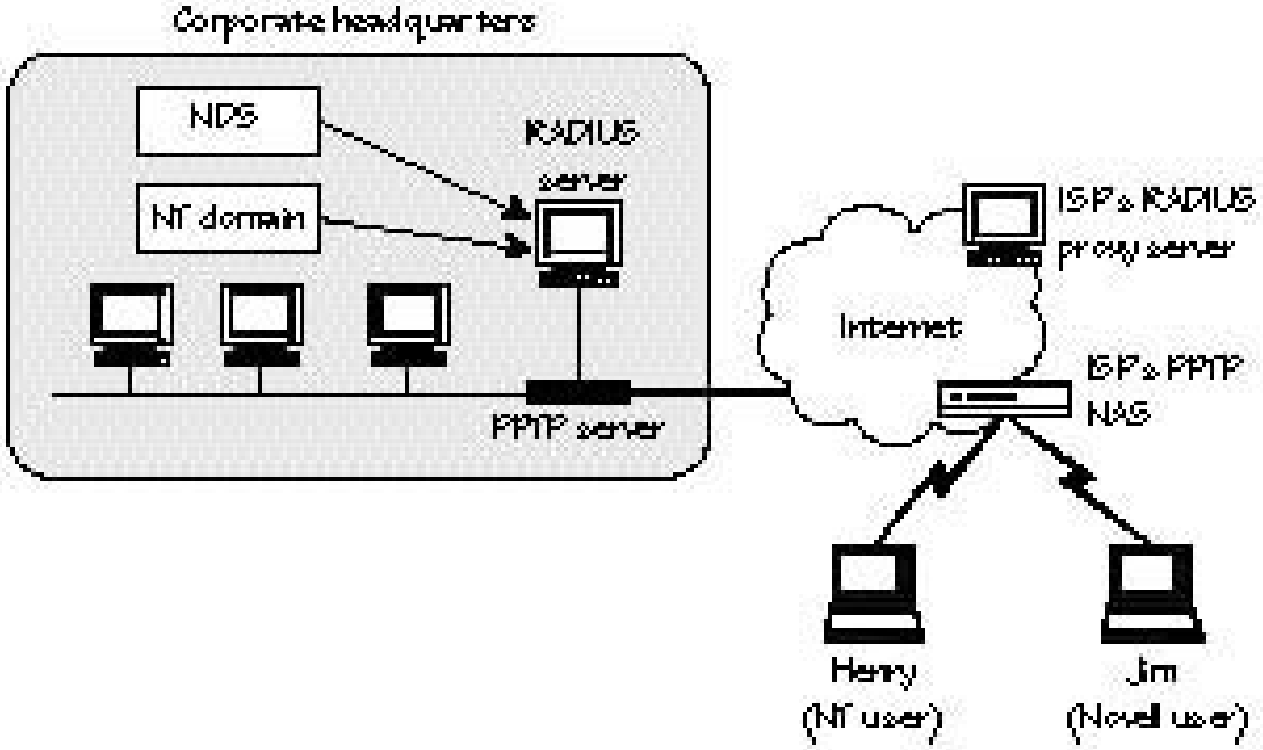
Περιγραφή των NAS

- Σχεδιάζονται με σκοπό να εξυπηρετούν πολλές dial-in συνδέσεις και να παρέχουν PPTP υπηρεσίες σε πολλές πλατφόρμες (windows, unix, Macintosh).

Παράδειγμα: PPTP dial-in VPN

- Μία εταιρία θέλει να χρησιμοποιήσει τον ISP για VPN δυνατότητες. Συνεπώς, ο ISP πρέπει να διαθέτει RADIUS Proxy Server και NAS με PPTP δυνατότητες. Από την άλλη μεριά, και η ίδια η εταιρία πρέπει να διαθέτει έναν κεντρικό (master) RADIUS server και έναν PPTP server.
- Δεν χρειάζεται PPTP software στους υπολογιστές των χρηστών (αφού διαθέτει τέτοιες δυνατότητες ο ISP).

Παράδειγμα: PPTP dial-in VPN (σχήμα)

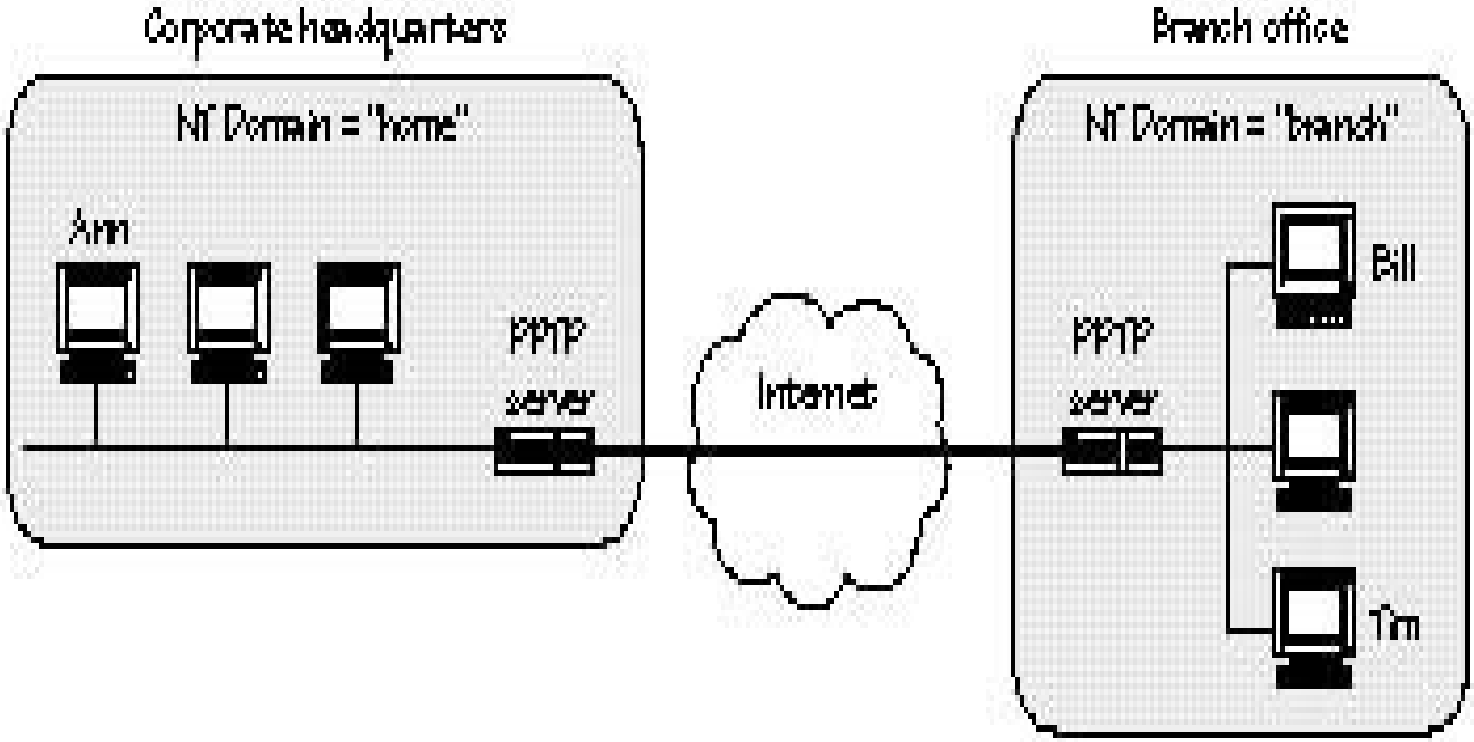


- Ο RADIUS server παρέχει κεντρικοποιημένο έλεγχο πρόσβασης, ανεξαρτήτως πρωτοκόλλου (είτε για Windows NT χρήστες, είτε για Novell Directory Services (NDS)).

Παράδειγμα: PPTP LAN-to-LAN VPN

- Ένας Windows Server εγκαθίσταται σε κάθε πλευρά, παίζοντας το ρόλο και δρομολογητή και PPTP server. Επίσης, ο κάθε PPTP server πρέπει να σεταριστεί ώστε να παίζει το ρόλο client για τον άλλον (αν η εγκαθίδρυση της ζεύξης γίνεται μετά από αίτηση του χρήστη και δεν είναι μόνιμη, η IP διεύθυνση του NAS πρέπει να ληφθεί υπόψιν στο παραπάνω σετάρισμα.
- Για να καθορίζεται το ποιος έχει πρόσβαση, μπορεί να υπάρχει είτε ένα κεντρικό domain είτε κάθε χρήστης να έχει το δικό του.

Παράδειγμα: PPTP LAN-to-LAN VPN (σχήμα)



Σχόλια πάνω στο PPTP

- Το IP GRE δεν είναι εύκολα διαχειρίσιμο από όλους τους «τοίχους ασφαλείας» (firewalls).
- Τα VPN που στηρίζονται στο PPTP εξαρτώνται πολύ από τα πρωτόκολλα που διαθέτει ο ISP (σε αντίθεση με το IPSec).