Το πρωτόκολλο L2TP στο VPN

Γενικά στοιχεία για το L2TP

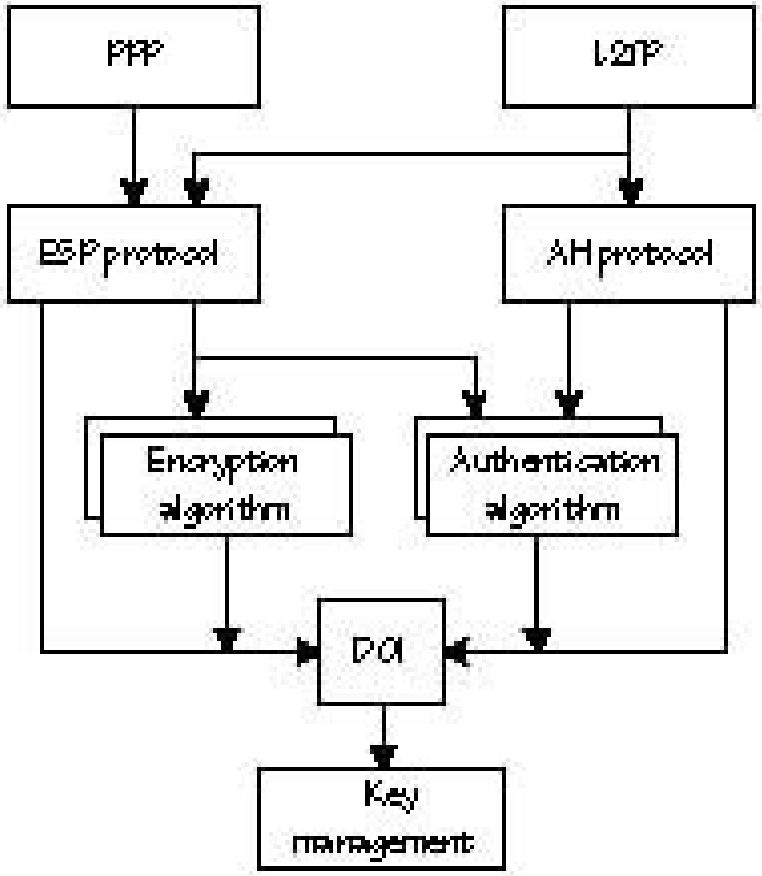
- Αποτελεί εξέλιξη των προϋπαρχόντων PPTP και L2F. Είναι λοιπόν επίσης πρωτόκολλο για ασφαλή μετάδοση σε ένα δημόσιο δίκτυο μέσω εγκαθίδρυσης διόδου.
- Μπορεί να χρησιμοποιηθεί και σε δίκτυα μεταγωγής πακέτων, όπως Frame Relay ή ATM.
- Παρέχει και έλεγχο ροής – δηλαδή δεν αποδέχεται κίνηση περισσότερη από αυτή που μπορεί να διαχειριστεί το δίκτυο (αυτό το στοιχείο υπάρχει και στο L2F).
- Μπορεί να συνεργαστεί με το IPSec πρωτόκολλο – υπ' αυτήν την έννοια, παρέχει υπηρεσίες και δεύτερου αλλά και τρίτου επιπέδου.

Λίγα λόγια για το L2F

- Διαφορά του με το PPTP: δεν κάνει ενθυλάκωση GRE – το ίδιο το πρωτόκολλο έχει δικούς του μηχανισμούς ενθυλάκωσης.
- Όπως και το PPTP, βασίζεται στο PPP για εγκαθίδρυση μιας dial-in ζεύξης. Ωστόσο, για πιστοποίηση ταυτότητας εκτός από το πρωτόκολλο RADIUS υποστηρίζει και το TACACS. Η πιστοποίηση γίνεται σε δύο επίπεδα: μία από τον ISP πριν την εγκατάσταση της διόδου και μία μετέπειτα, από την αντίστοιχη πύλη (το άκρο της διόδου).

Αρχιτεκτονική του L2TP

- Το PPP ενθυλακώνει Apple Talk, IP, IPX και NETBEUI πακέτα σε PPP πλαίσια και τα στέλνει μέσω μιας σημείο-προς-σημείο ζεύξης.
- Το PPP δημιουργεί μία dial-up σύνδεση ενός χρήστη με τον NAS. Το L2TP αναμένει από το PPP να πραγματοποιήσει αυτή τη σύνδεση, να κάνει μια πρώτη αυθεντικοποίηση (με PAP ή CHAP) και να δημιουργήσει τα PPP πλαίσια.
- Το L2TP αναλαμβάνει να ελέγξει αν ο server του δικτύου στο οποίο ο χρήστης ζητάει πρόσβαση επιτρέπει τη δημιουργία διόδου. Αν ναι, τότε ενθυλακώνει PPP πακέτα και τα στέλνει μέσω της διόδου.
- Η δίοδος δημιουργείται μεταξύ του Access Concentrator στον ISP και του Network Server (εξηγούνται παρακάτω). Στην ίδια δίοδο μπορούν να υπάρχουν ταυτόχρονα πολλές σύνοδοι (επικοινωνίες): κάθε σύνοδος έχει ένα δικό της μοναδικό αριθμό Call ID, που υπάρχει στην επικεφαλίδα κάθε L2TP πακέτου.
- Μπορούν επίσης να υπάρχουν ταυτόχρονα πολλές διαφορετικές δίοδοι μεταξύ του ίδιου Access Concentrator και του Access Server. Η κάθε μία τότε μπορεί να ικανοποιεί διαφορετικό QoS.

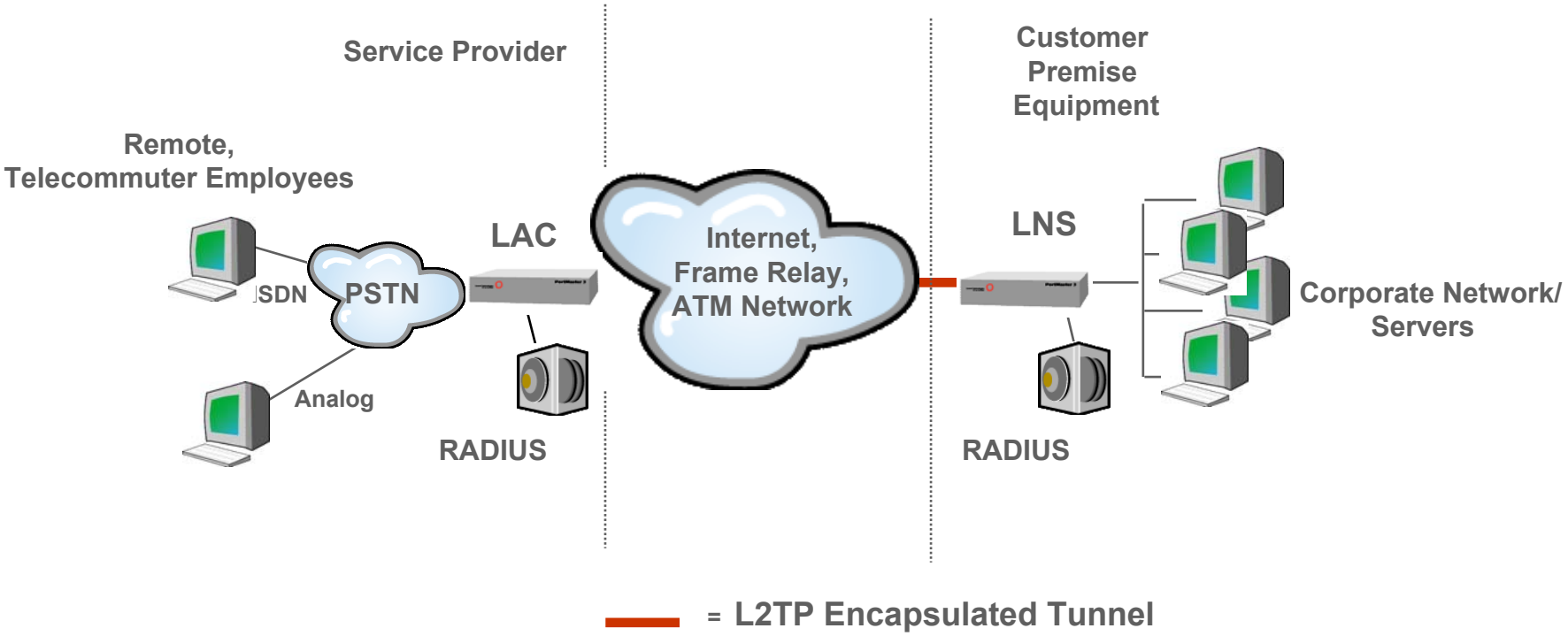


Αρχιτεκτονική του L2TP (συνέχεια)

- Όπως και το PPTP, υπάρχουν δύο είδη μηνυμάτων: μηνύματα ελέγχου (control messages) και μηνύματα δεδομένων (data messages). Τα μηνύματα ελέγχου χρησιμοποιούνται για εγκαθίδρυση και τερματισμού της διόδου. Τα μηνύματα δεδομένων είναι στην ουσία τα ενθυλακωμένα PPP πακέτα, συν μια επικεφαλίδα για το μέσο μετάδοσης (π.χ. Ethernet, Frame Relay, X25, ATM).

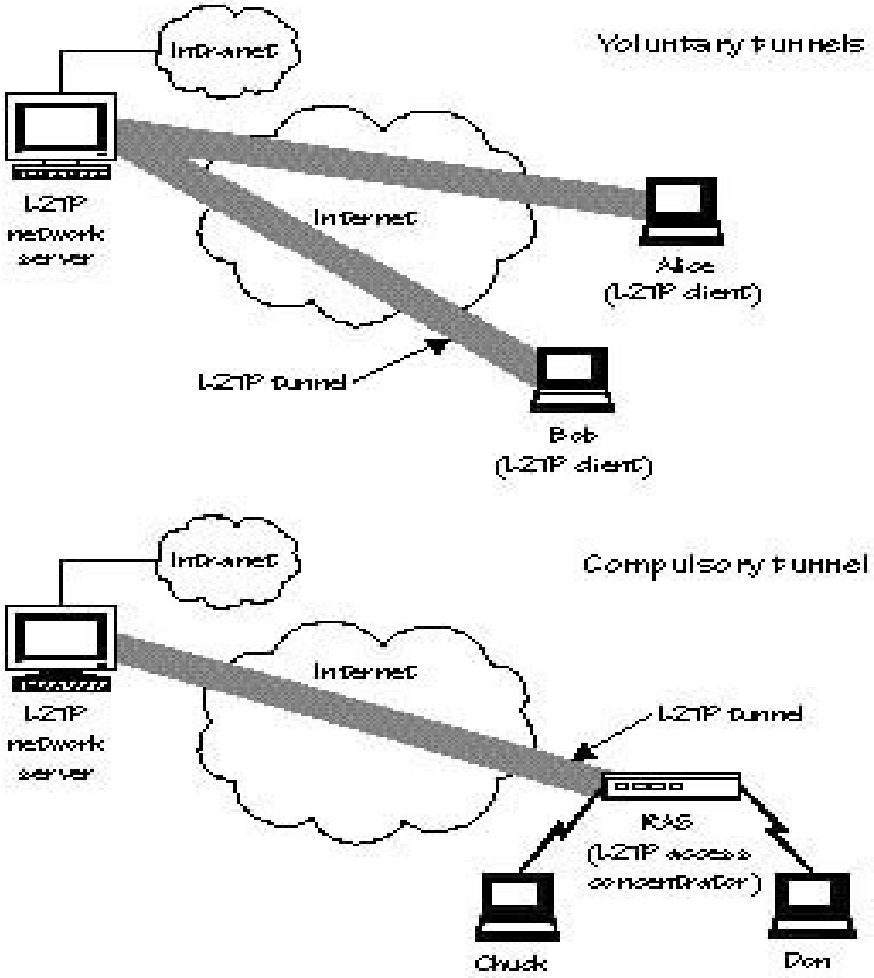
- Γίνεται επίσης έλεγχος ροής δεδομένων μεταξύ των δύο άκρων της διόδου, που στην L2TP ορολογία αποκαλούνται L2TP Access Concentrator (LAC) και L2TP Network Server (LNS). (Ο LAC είναι για το L2TP ό,τι είναι ο RAS για το PPTP).
- Οι ίδιες κατηγορίες διόδων που είδαμε και στο PPTP υποστηρίζονται και εδώ – αυθόρμητες (voluntary) και αναγκαστικές (compulsory).

Σχηματική αναπαράσταση ενός VPN tunnel, βασισμένο σε L2TP



Δίοδοι στο L2TP

- Στις αυθόρμητες διόδους το ένα άκρο είναι στον υπολογιστή του χρήστη, ενώ στις αναγκαστικές το άκρο τους είναι το LAC.



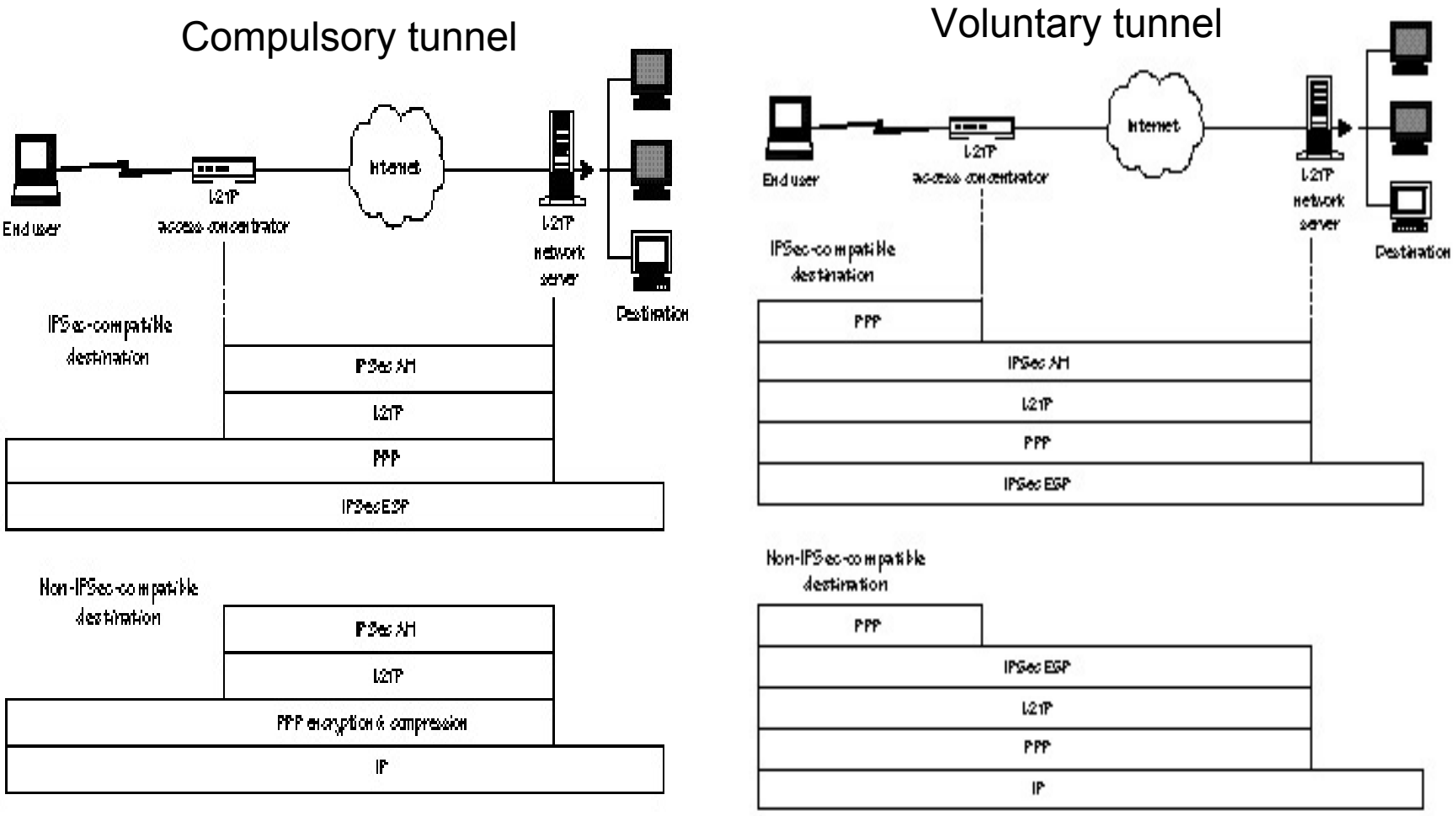
Αυθεντικοποίηση (πιστοποίηση ταυτότητας) στο L2TP

- Στην πρώτη φάση, ο ISP χρησιμοποιεί το user name του χρήστη για να τον αυθεντικοποιήσει – και στη συνέχεια εγκαθιστά μία δίοδο με τον απομακρυσμένο Network Server. Με την εγκατάσταση της διόδου, ο LAC θα αποδώσει ένα Call ID στη ζεύξη και θα προωθήσει την πληροφορία σχετικά με την πιστοποίηση ταυτότητας.
- Ο απομακρυσμένος server κάνει πιστοποίηση σε μία δεύτερη φάση (είτε CHAP είτε PAP, με password πληροφορίες που του στέλνει ο ISP).

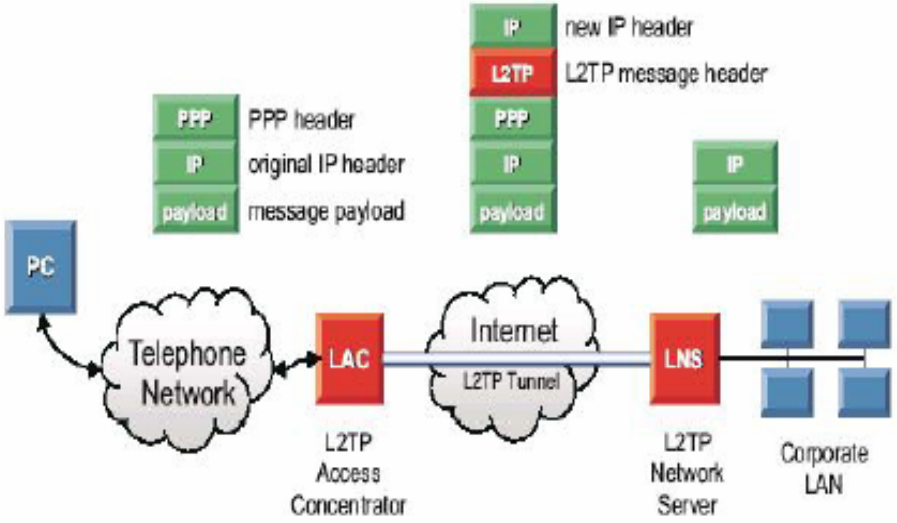
Κρυπτογράφηση στο L2TP

- Η κρυπτογράφηση του PPP δεν θεωρείται αρκετή: χρήση του IPSec για καλύτερη κρυπτογράφηση.
  - Σε αναγκαστική δίοδο, ο χρήστης στέλνει PPP πακέτα στον LAC και η δημιουργία διόδου μεταξύ του LAC και του απομακρυσμένου δικτύου γίνεται ερήμην του – ο ίδιος ο χρήστης δεν κάνει καμία άλλη ενέργεια για τη δημιουργία αυτής της διόδου. Το IPSec λοιπόν είναι η καλύτερη επιλογή για τον χρήστη – στέλνει απευθείας κρυπτογραφημένα (και άρα ασφαλή) τα δεδομένα. Το AH προστίθεται από τον LAC του ISP. Ο ESP προστίθεται μόνο όταν ο προορισμός υποστηρίζει IPSec.
  - Σε αυθόρμητη δίοδο, ο AH εφαρμόζεται στον υπολογιστή του χρήστη απευθείας (μια που είναι άκρο της διόδου). Αν ο LNS στον προορισμό δεν υποστηρίζει IPSec, ο ESP προστατεύει τα δεδομένα μόνο μέχρι να καταφτάσουν στον LNS.
  - Σε IP δίκτυα, τα πακέτα μεταξύ LAC και LNS είναι συνήθως UDP (και όχι TCP).
- Το IKE χρησιμοποιείται για τη διαχείριση του κλειδιού (όταν το L2TP είναι πάνω στο IP).

Σχηματικές αναπαραστάσεις της ενθυλάκωσης των πρωτοκόλλων



L2TP σύνοδος σε IP δίκτυα



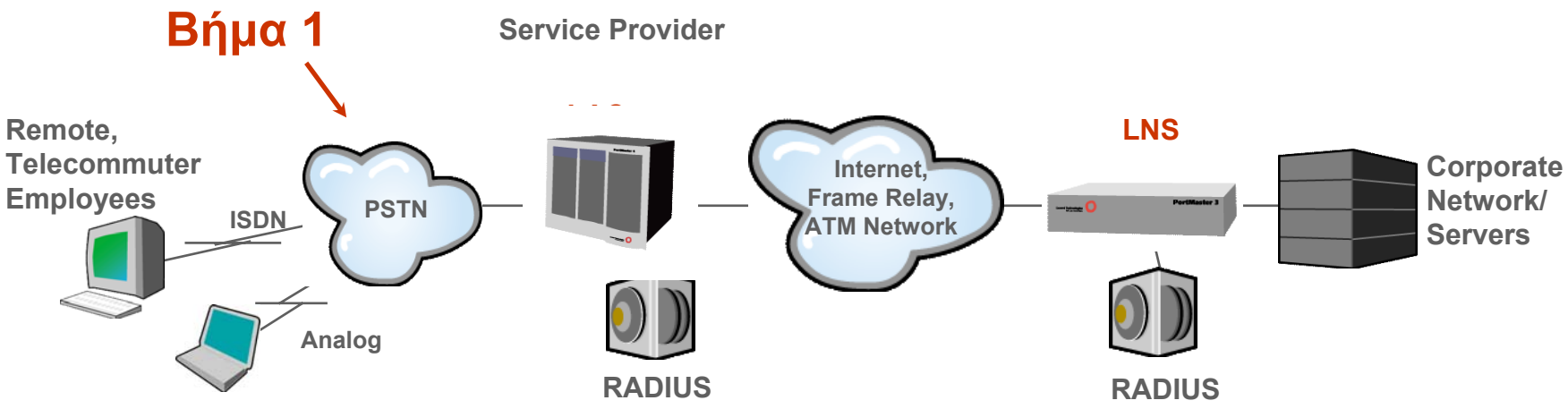
Stage 1. Ο απομακρυσμένος χρήστης συνδέεται με τον ISP's LAC με χρήση PPP protocol. Ο LAC αυθεντικοποιεί. Σύμφωνα με το profile του user, ο LAC προσδιορίζει την IP address του LNS που ανήκει στο LAN για το οποίο ο user αιτείται σύνδεση. Μεταξύ LAC και LNS, η σύνοδος L2TP ξεκινά.

Stage 2. Μετά την εκκίνηση της L2TP συνόδου, ξεκινά η αυθεντικοποίηση του χρήστη στον LNS. Μπορεί να χρησιμοποιηθεί οποιαδήποτε τυποποιημένος authentication algorithm, e.g, CHAP. Όπως στα PPTP και L2F , το L2TP δεν θέτει περιορισμό για authentication algorithm

Stage 3. Μετά από επιτυχές authentication, μπορεί να δημιουργηθεί ένα cryptographically protected tunnel μεταξύ LAC και LNS. Το L2TP δεν προσδιορίζει ρητά μεθόδους για αυτό. Ωστόσο, για tunnels σε IP δίκτυα, μπορεί να χρησιμοποιηθεί IPSec protocol. Τότε το L2TP protocol ενθυλακώνεται σε UDP-packets που μεταφέρονται μεταξύ LAC και LNS μέσω IPSec tunnel. Για αυτό χρησιμοποιείται η UDP-port 1701.

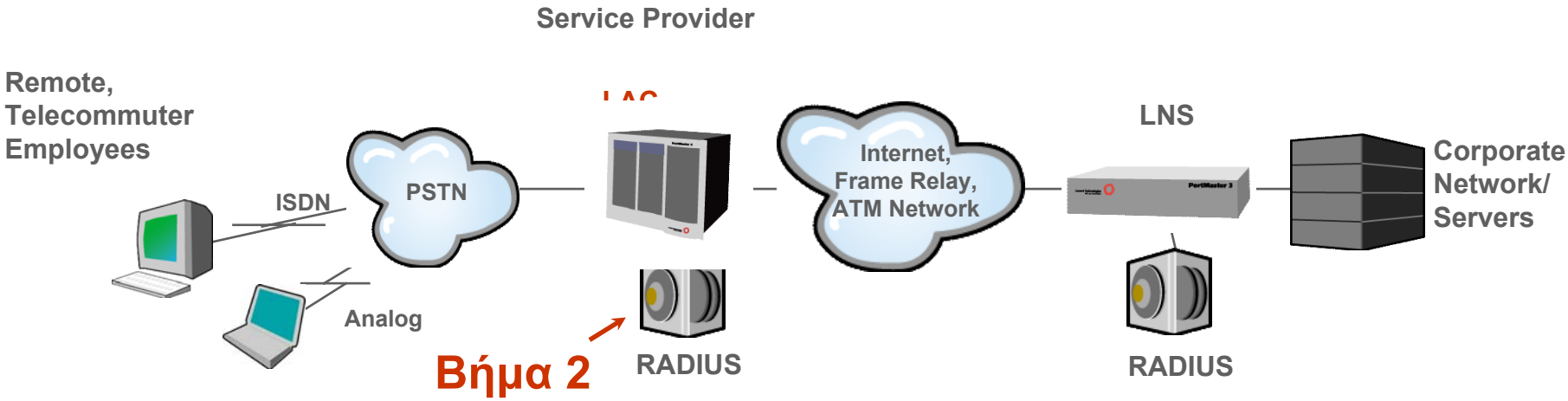
Αναλυτική περιγραφή της λειτουργίας ενός L2TP VPN

- **Βήμα 1**
  - Ο χρήστης ζητά μία σύνδεση μέσω του LAC.



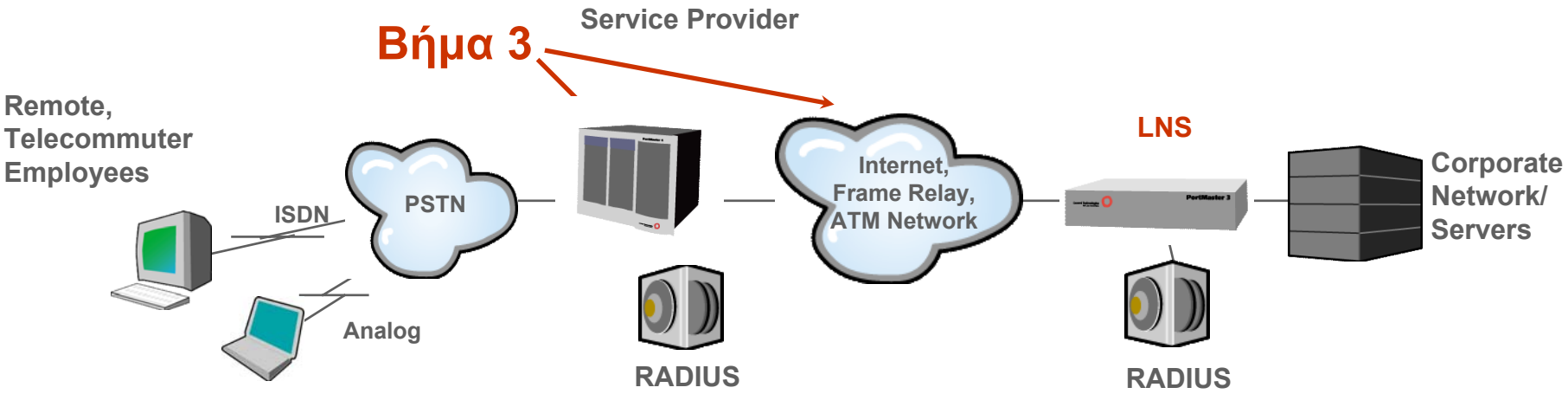
Αναλυτική περιγραφή της λειτουργίας ενός L2TP VPN (2)

- **Βήμα 2**
  - Ο LAC στέλνει μία αίτηση αυθεντικοποίησης στον RADIUS Server, ο οποίος θα πραγματοποιήσει πιστοποίηση ταυτότητας και θα δώσει πληροφορίες για το είδος της διόδου και το άλλο της άκρο



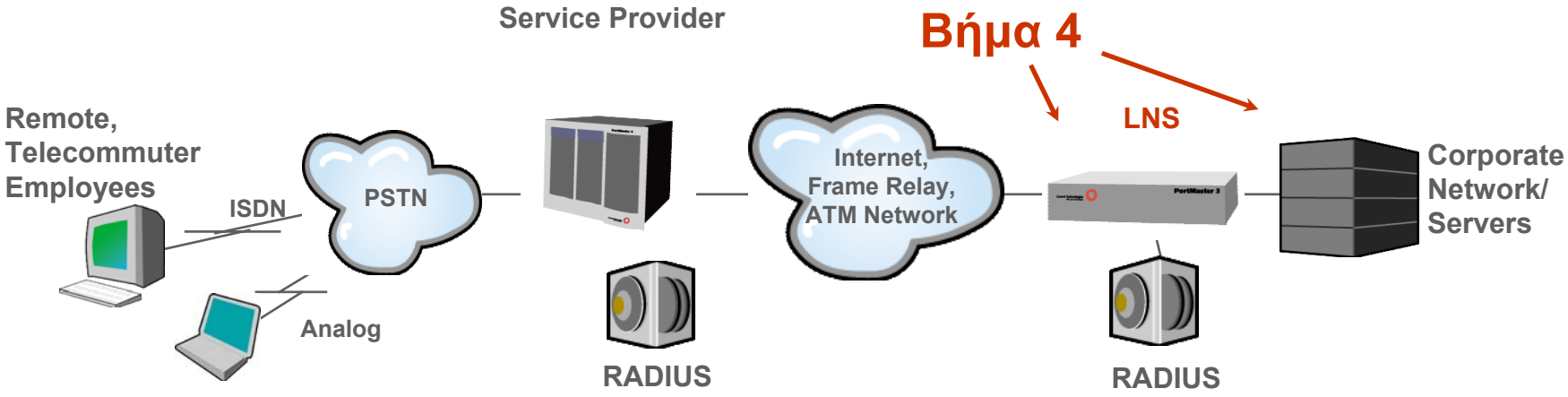
Αναλυτική περιγραφή της λειτουργίας ενός L2TP VPN (3)

- **Βήμα 3**
  - Η δίοδος έχει εγκατασταθεί, τα PPP πακέτα ενθυλακώνονται σε L2TP πακέτα και μεταδίδονται από τον LAC στον LNS.

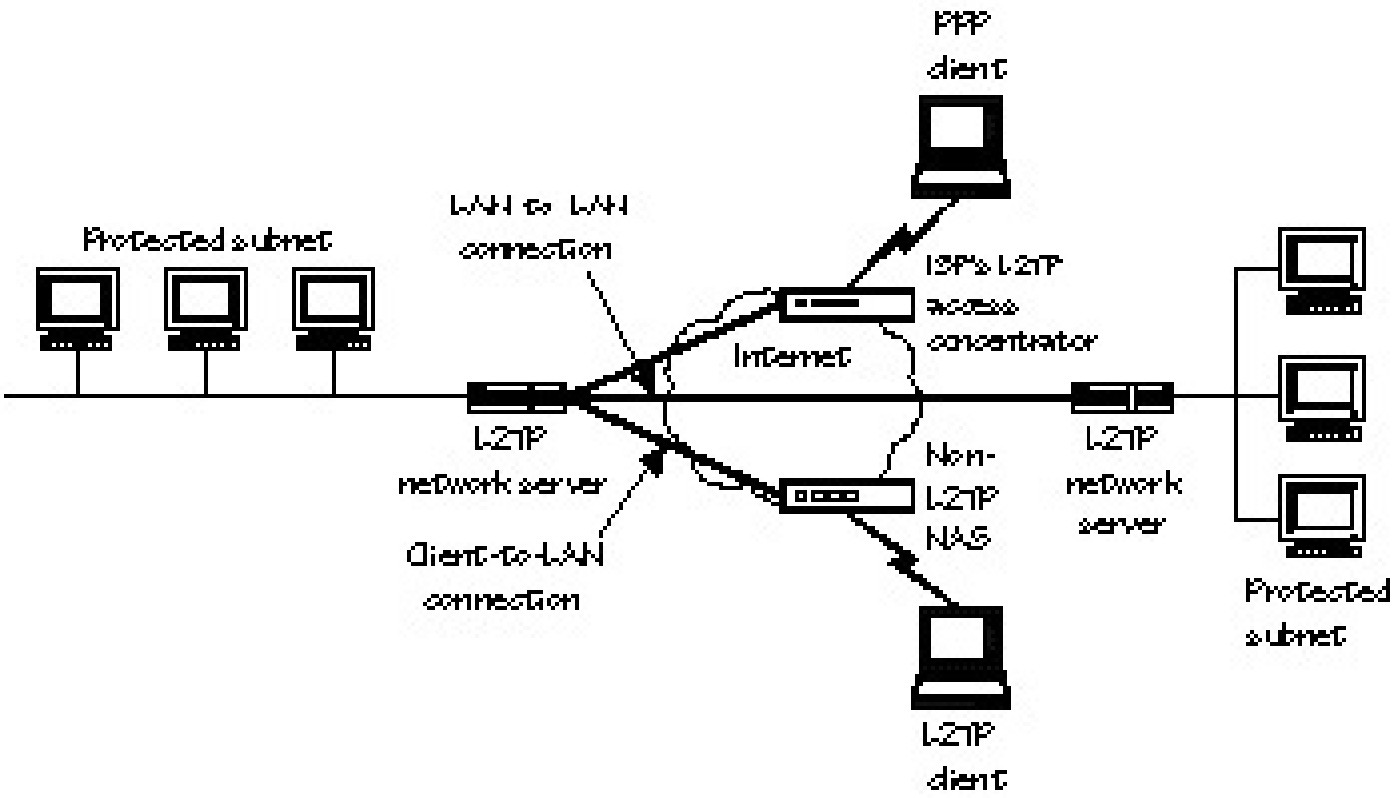


Αναλυτική περιγραφή της λειτουργίας ενός L2TP VPN (4)

- **Βήμα 4**
  - Ο LNS δρα ως τερματικός κόμβος της διόδου, όπου επεξεργάζεται το L2TP πλαίσιο. Επανακτά το αρχικό PPP πλαίσιο, το οποίο προωθείται από τον παραλήπτη στα πρωτόκολλα ανώτερου επιπέδου.



Δομικά στοιχεία του L2TP



L2TP Network Server (LNS)

- Είναι άκρα σε L2TP διόδους. Προωθούν τα λαμβανόμενα L2TP πακέτα στον αντίστοιχο υπολογιστή του δικτύου, με βάση το όνομά του ή τη διεύθυνσή του που ενυπάρχει στα PPP πακέτα.
- Δεν κάνει φιλτράρισμα των πακέτων (κάτι που δεν ισχύει για το PPTP). Το φιλτράρισμα στα L2TP VPNs γίνεται μόνο από τοίχους ασφαλείας (firewalls).
- Για να υποστηρίζουν το IPSec, πρέπει να ικανοποιούν, μεταξύ άλλων, και τα ακόλουθα:
  - Υποστήριξη των κρυπτογραφικών αλγορίθμων που θα χρησιμοποιηθούν
  - Υποστήριξη και AH και ESP

L2TP Access Concentrator – L2TP software

- LAC: Χρησιμοποιείται για την εγκαθίδρυση της διόδου. Όταν ο ISP διαθέτει τέτοιον, ο υπολογιστής του χρήστη δεν χρειάζεται να έχει ειδικό L2TP software.
- L2TP client software: πρέπει να υποστηρίζει IPSec.

Μπορούν να υπάρξουν LAN-to-LAN δίοδοι, πάνω σε L2TP?

- Όπως και στο PPTP, η απάντηση είναι καταφατική: κάθε άκρο της διόδου πρέπει να δρα ταυτόχρονα και σαν LAC αλλά και σαν LNS.

Σύγκριση με το PPTP

- Μια που δεν υπάρχει GRE ενθυλάκωση, το πρόβλημα συμβατότητας L2TP συσκευών με τοίχους ασφαλείας (firewalls) δεν είναι τόσο μεγάλο όσο στα PPTP.
- Μεγαλύτερη ασφάλεια ως προς την ανάλυση κίνησης (traffic analysis) από επιτιθέμενο: σε αντίθεση με το PPTP, η επικοινωνία δεν γίνεται μόνο μέσω μιας συγκεκριμένης UDP θύρας στον LNS (αν και υπάρχει μια προκαθορισμένη θύρα ως βασική, η 1701). Οι διαχειριστές δικτύου μπορούν να αλλάζουν αυτήν τη θύρα, δυσκολεύοντας έτσι το έργο ενός επιτιθέμενου.

Κατηγοριοποίηση των Εικονικών Δικτύων

- Με βάση την προηγούμενη ανάλυση, γίνεται φανερό ότι τα Εικονικά Δίκτυα μπορούν να ταξινομηθούν με πολλούς τρόπους, ανάλογα με την οπτική γωνία που τα εξετάζει κανείς. Συγκεκριμένα, έχουμε τους ακόλουθους τρόπους ταξινόμησης:
  - Με βάση τα επίπεδα OSI στα οποία αντιστοιχούν τα πρωτόκολλα που χρησιμοποιούνται για να δομήσουν ένα VPN. Ήδη είδαμε σε αυτήν την κατηγορία τα IPSec VPN (επίπεδο 3), τα PPTP VPN (επίπεδο 2), τα L2TP VPN (επίπεδο 2, αλλά και 3 όταν υποστηρίζει IPSec), ενώ υπάρχουν και τα VPN επιπέδου 7.
  - Με βάση το είδος της διόδου. Έτσι έχουμε τα VPN με αυθόρμητη δίοδο (voluntary tunnel) και τα VPN με αναγκαστική δίοδο (compulsory tunnel)
  - Με βάση το ποιοι είναι οι τελικοί χρήστες. Έτσι έχουμε είτε τα «πελάτης-προς-δίκτυο» VPNs (client-to-LAN) (που λέγονται επίσης και εικονικά δίκτυα απομακρυσμένης πρόσβασης), είτε τα «δίκτυο-προς-δίκτυο» VPNs (LAN-to-LAN).