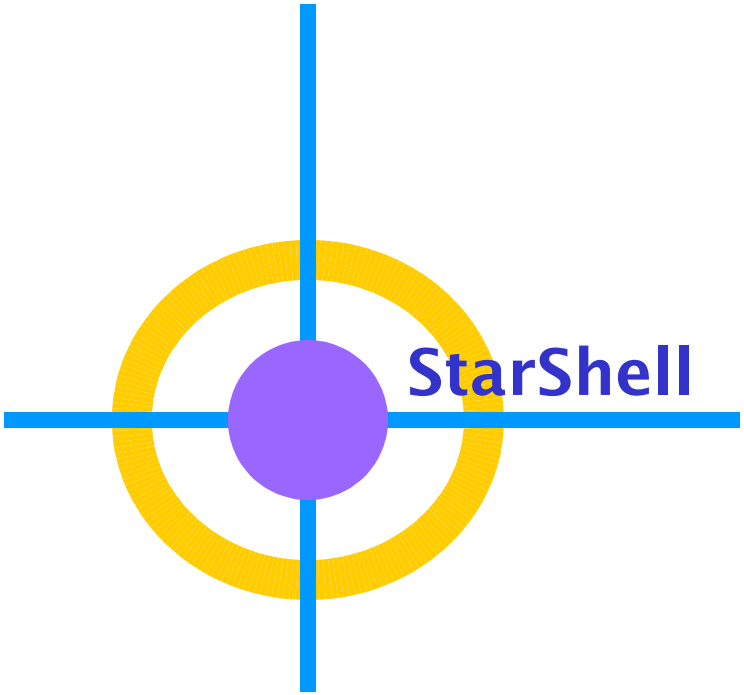


Virtual Private Networks

Definizioni di VPN

- Virtual Private Network

  Rete Privata Virtuale

- Definizione Formale

  Una VPN è un ambiente di comunicazione in cui vi è controllo di accesso per permettere connessioni solo entro una comunità predefinita, e costruito tramite qualche tipo di partizionamento di un mezzo comunicativo sottostante comune, il quale fornisce di suo dei servizi alla rete su base non esclusiva.

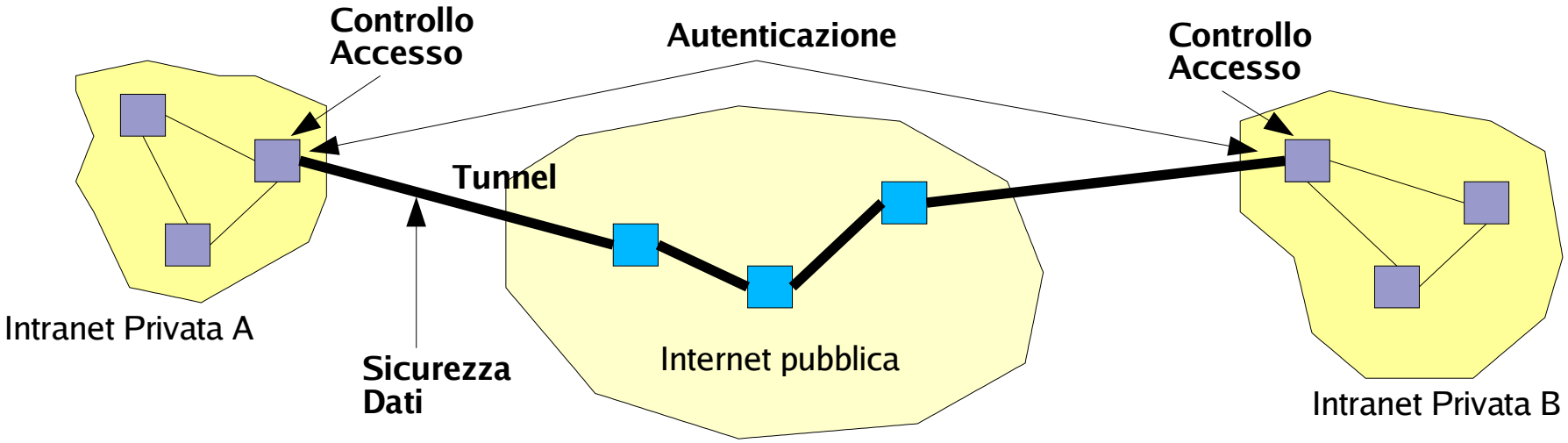
- Definizione più semplice

  Una VPN è una rete privata costruita entro un'infrastruttura di rete pubblica, come l'Internet

Il Mercato VPN

- Prodotti VPN
  - VPN Gateway
  - VPN Client
- Categorie VPN
  - Software based
  - Hardware based
- Servizi VPN
  - Gestito dall'ente possessore
  - In outsourcing a fornitore di servizi
    - **Contratto a ditta di telecomunicazioni**
    - **Problema: chi detiene il controllo della rete**

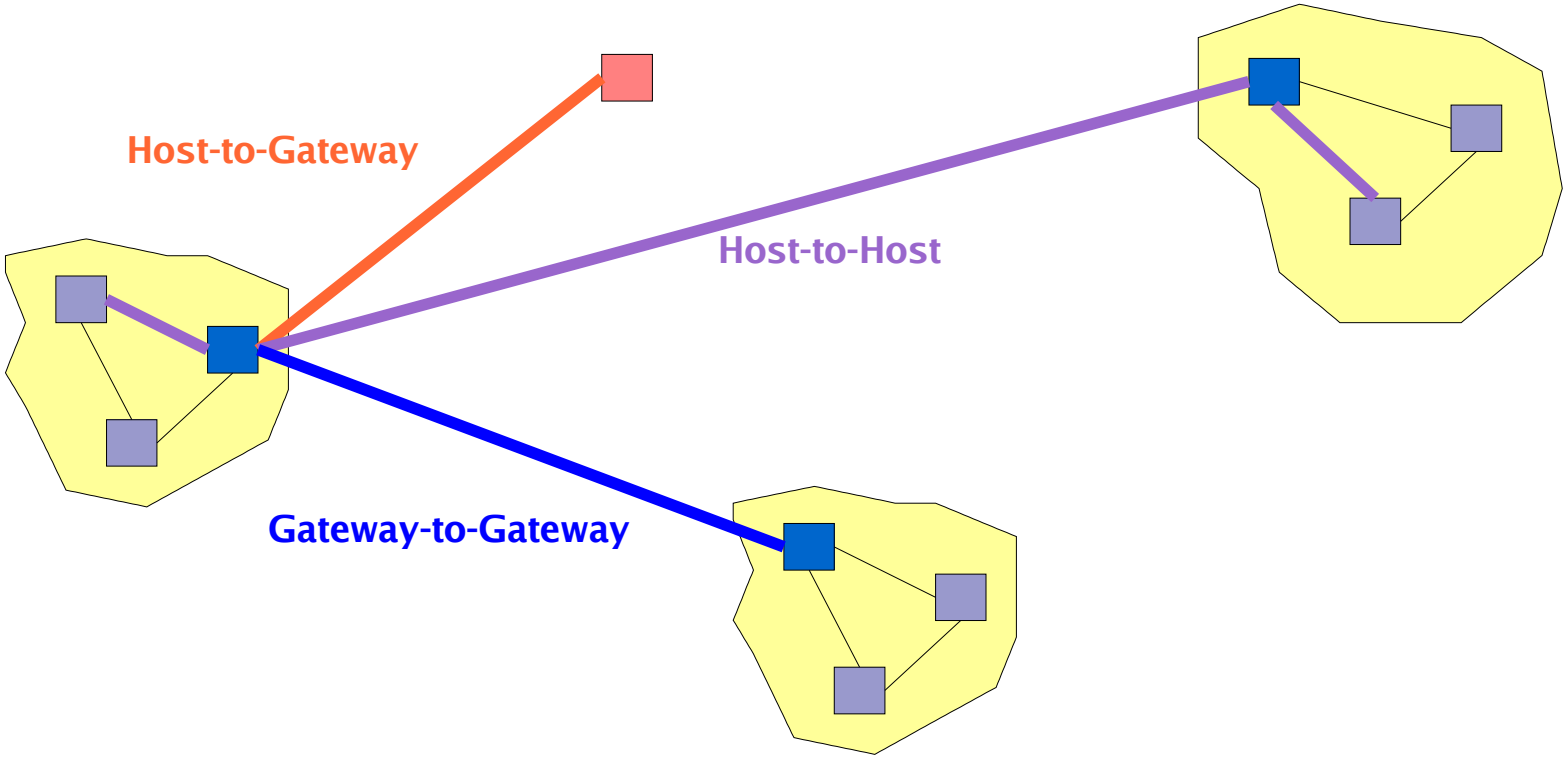
Tecnologie Chiave



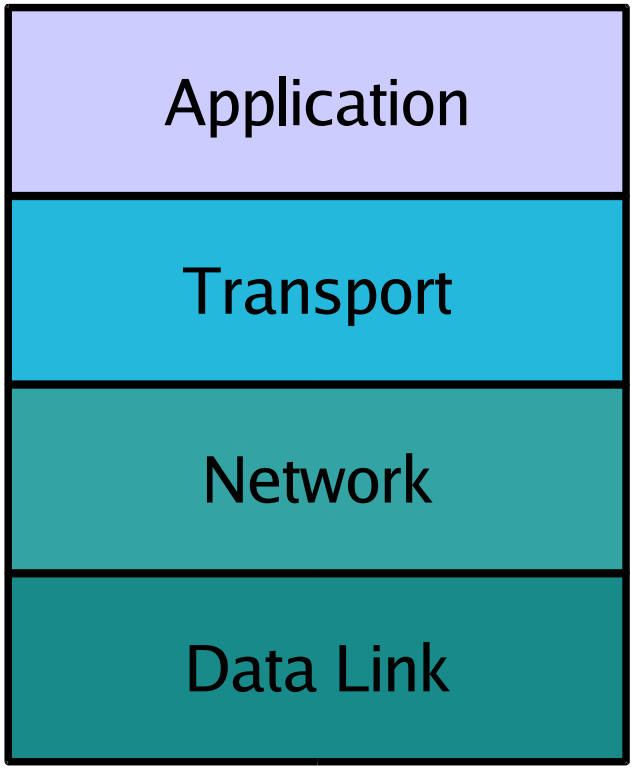
- **Tunnelling**
- **Autenticazione**
- **Controllo Accesso**
- **Sicurezza Dati**

Categorie di VPN

- Host-to-Host
- Host-to-Gateway
- Gateway-to-Gateway

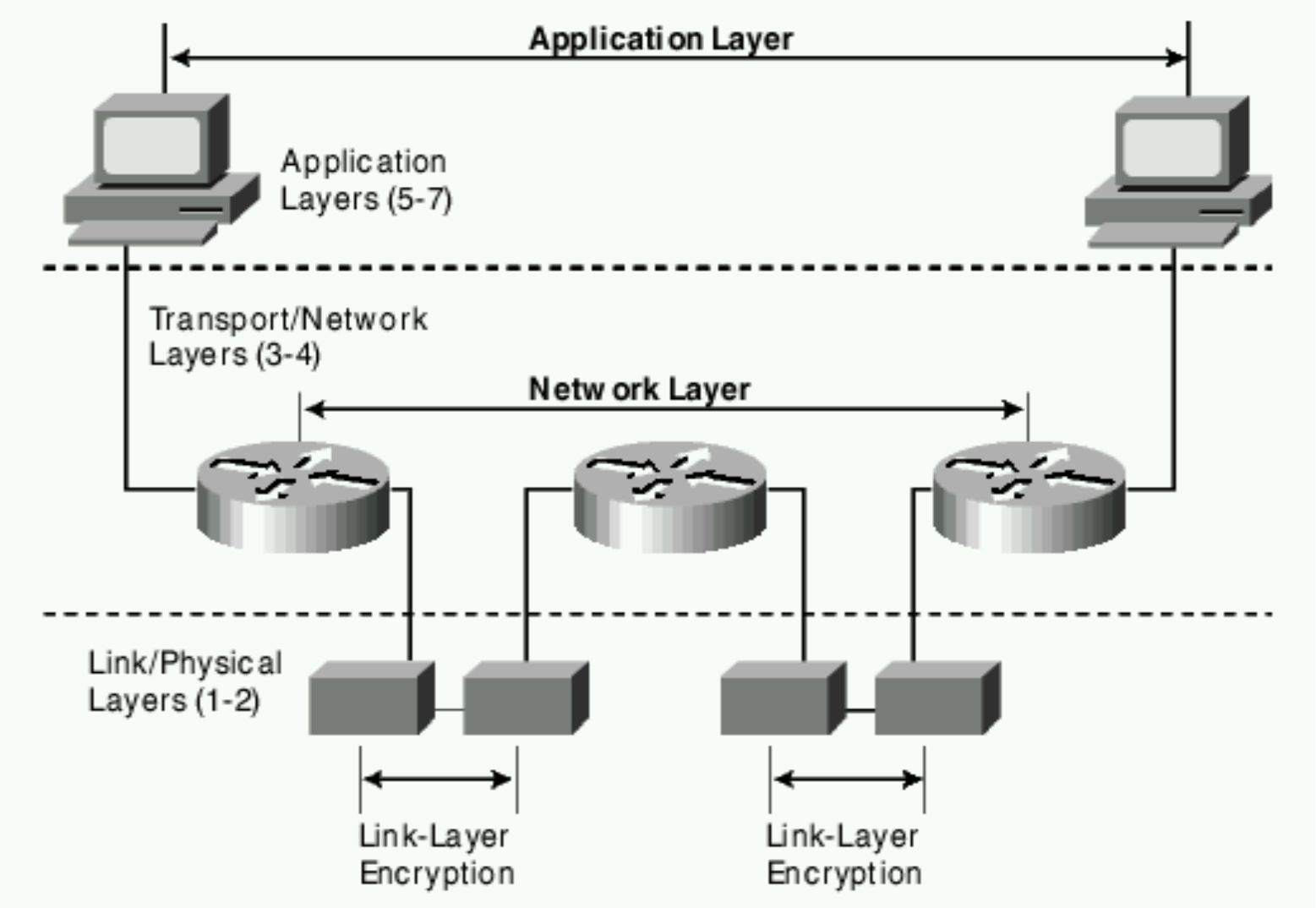


Livelli di VPN



- SSH
- SSL
- IPSec
- PPTP, L2F, L2TP

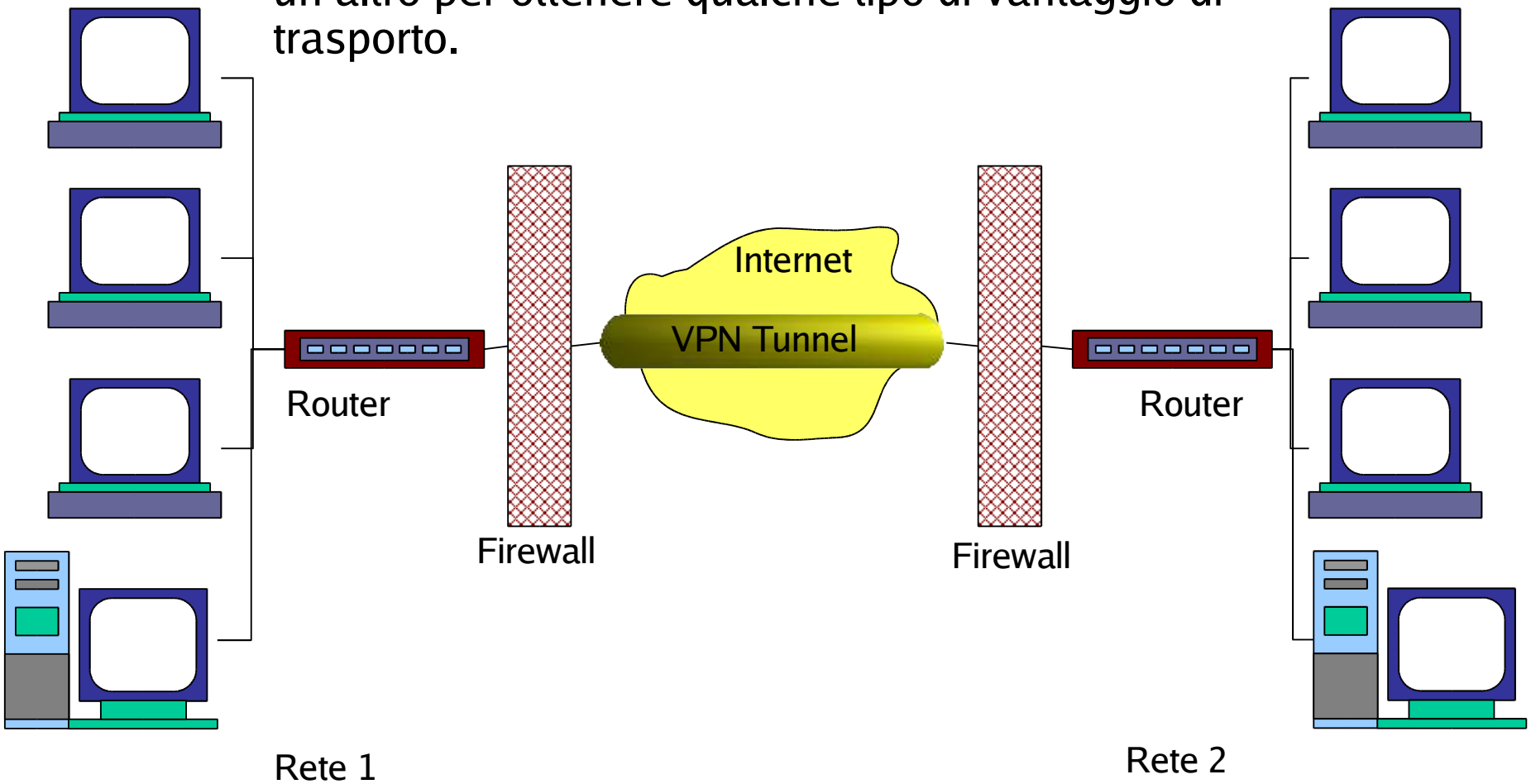
Livelli di VPN



StarShell

Tunnel Virtuale

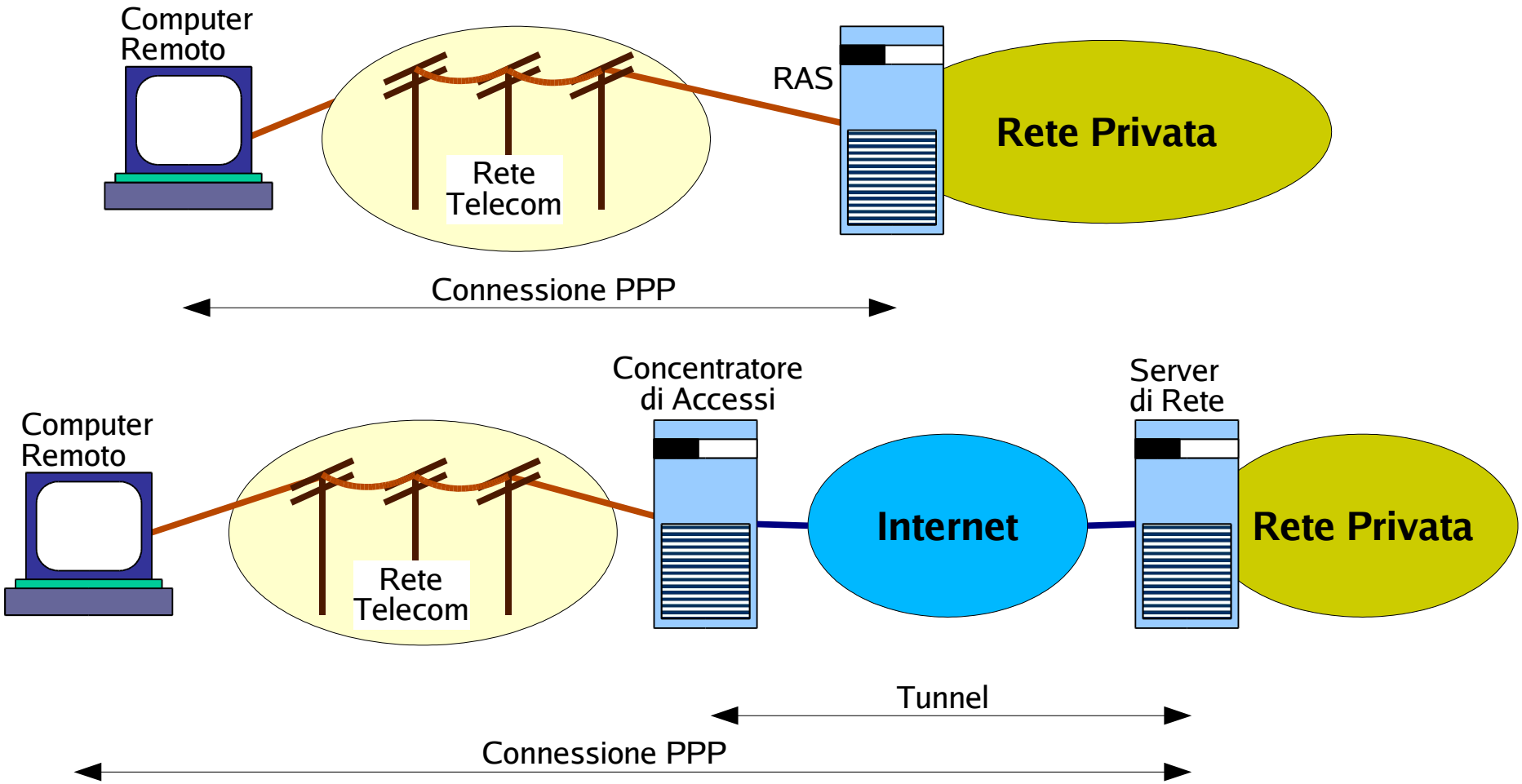
Tunnel: incapsulamento di un tipo di pacchetto entro un altro per ottenere qualche tipo di vantaggio di trasporto.



Protocolli di Tunnelling

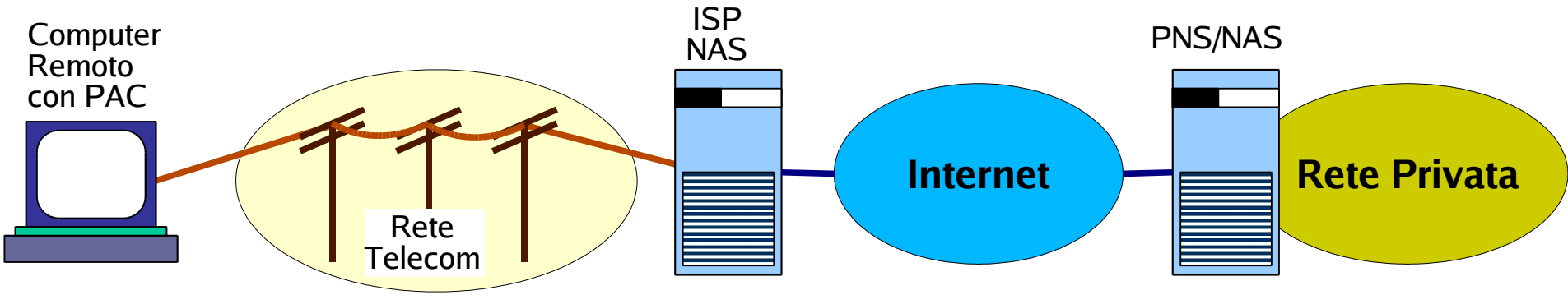
- Scopi:
  - Incapsulamento di un protocollo entro un altro protocollo
    - **Protocolli diversi trasportati nella stessa infrastruttura IP**
  - Routing di pacchetti con indirizzi privati attraverso l'Internet pubblica
  - Fornire confidenzialità ed integrità dati
- Tunnelling a Livello 2
  - Tunnelling di PPP (point to Point Protocol)
  - Utili per telecommuting
    - **Connessioni on-demand attraverso linee telecom**
    - **Accesso tramite Remote Access Server o PPP Server**

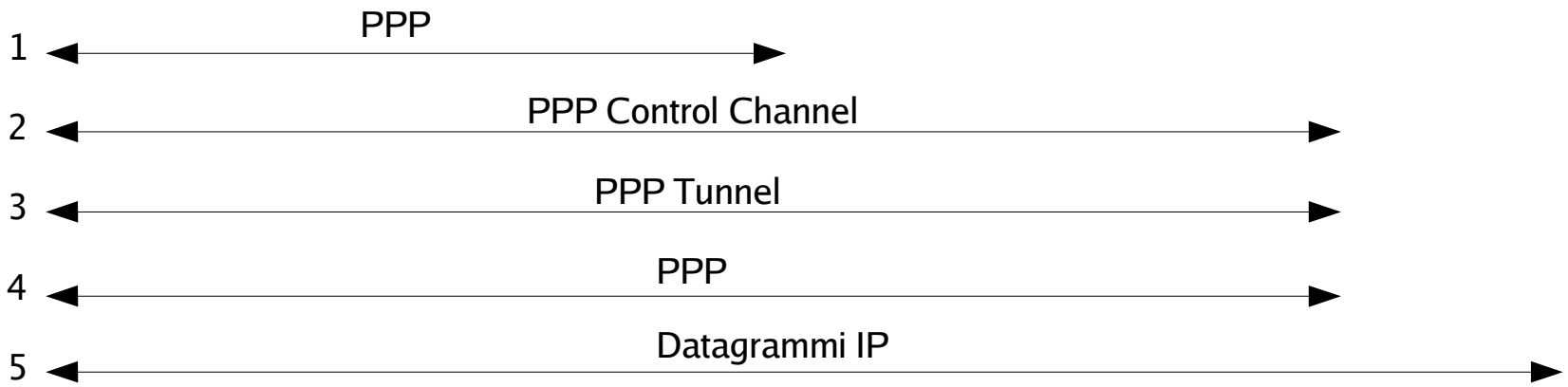
Layer 2 Tunnelling



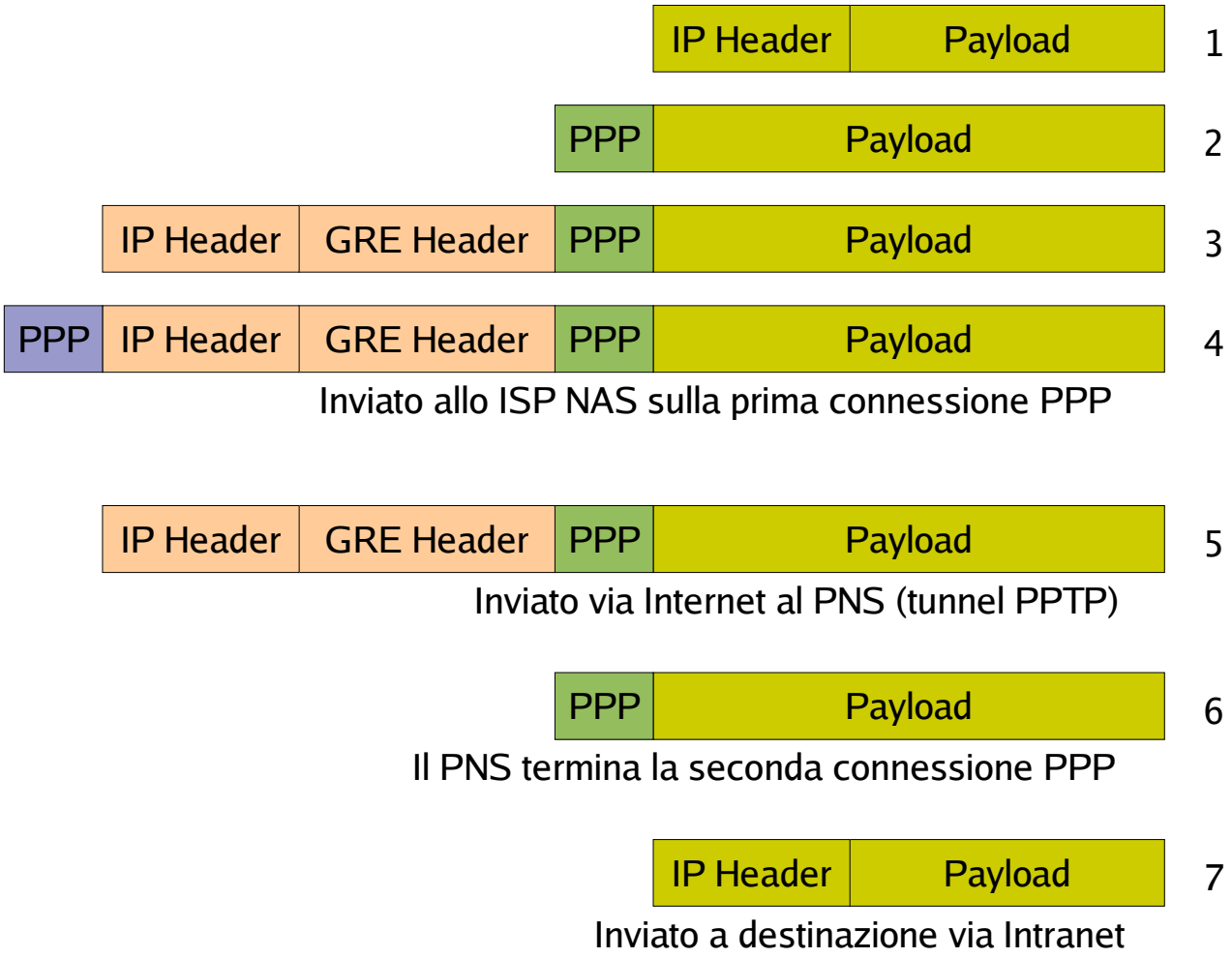
PPTP

- Point to Point Tunnelling Protocol (RFC2637)
  - **PPTP Access Concentrator (PAC)**
  - **PPTP Network Server (PNS)**





Incapsulamento PPTP

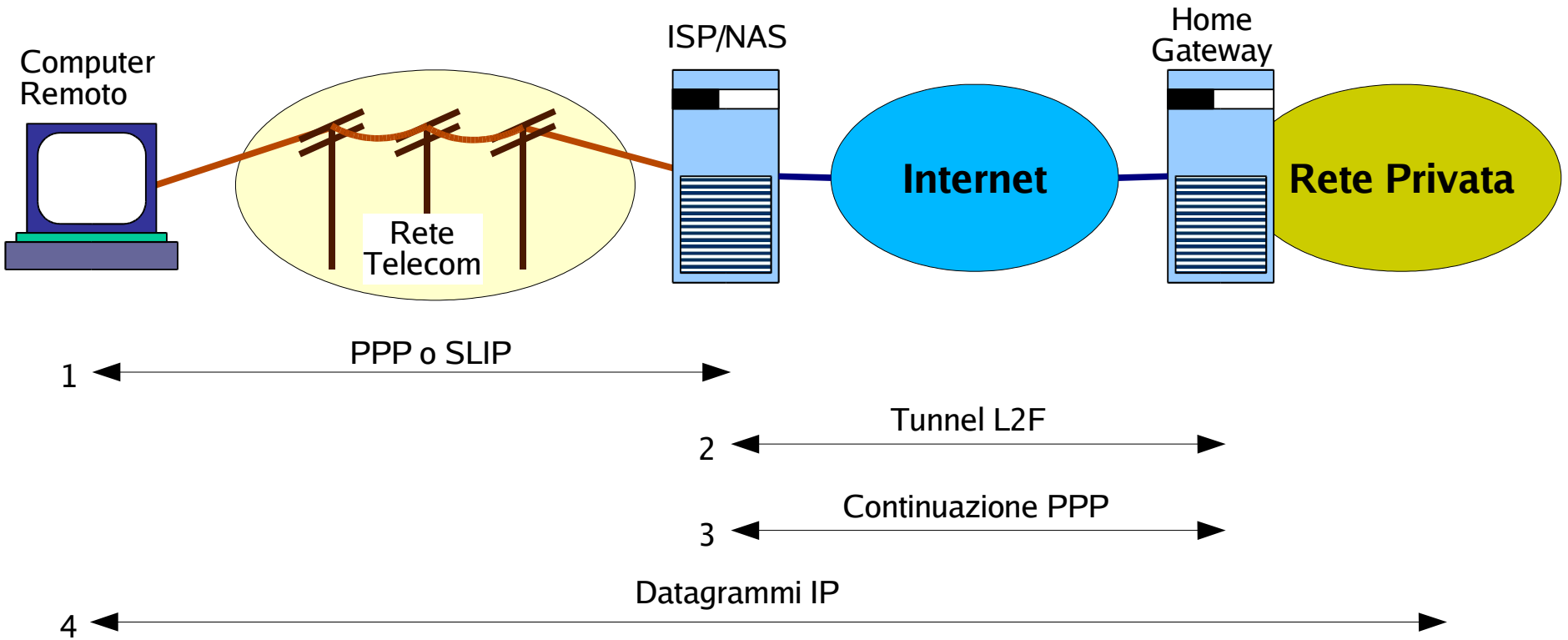


PPTP

- Relazione molti-a-molti tra PACs e PNSs
- Soluzione originata da Microsoft
- Autenticazione con PAP, CHAP ed EAP (Extensible Authentication Protocol – MS)
  - **Debolezze originarie nel MS-CHAP versione 1**
  - **La versione 2 non è molto meglio**
  - **Problemi di interoperabilità con RAS Microsoft se usa CHAP esteso**
- Crittografazione fornita da Microsoft, basata su password utente

L2F

- Layer Two Forwarding protocol
  - **Cisco, Nortel, Shiva corp (Intel)**
  - **Concepito per operazioni outsourcing**



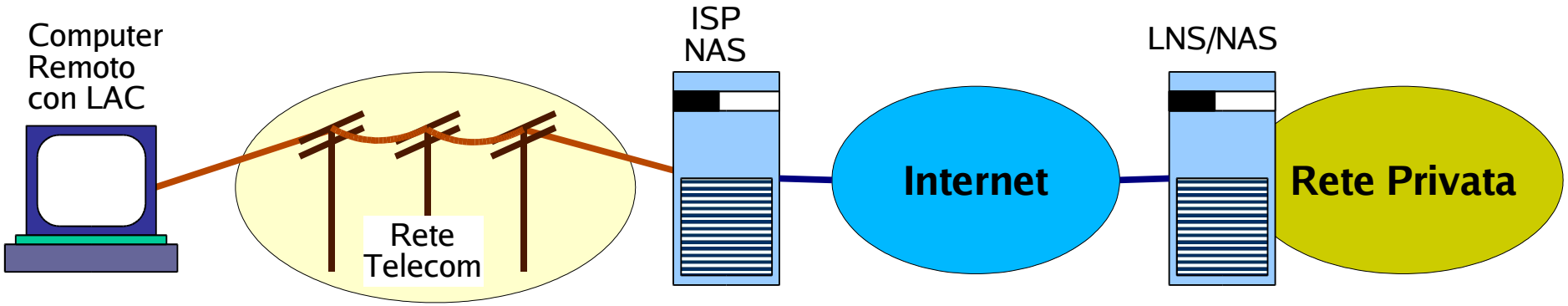
L2F

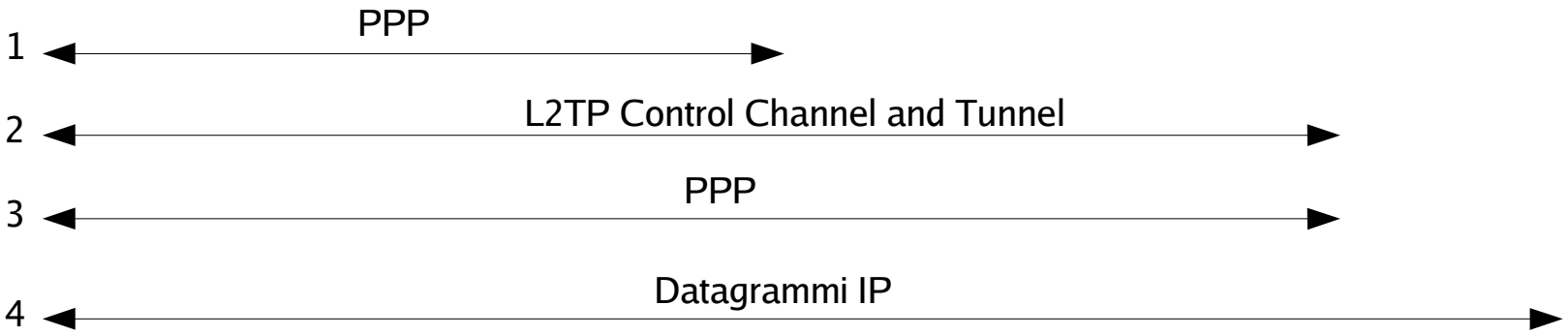
- Computer remoto usa PPP o SLIP
- RAS autentica con PAP o CHAP
  - **Ottiene nome utente e rete di destinazione dall'autenticazione**
- Per il tunnel usa UDP, X.25 o Frame Relay, non GRE
- Assume l'esistenza di un Gateway d'accesso
  - **Soluzione Cisco**
  - **Accetta connessione estes PPP o SLIP**
  - **Crea una Interfaccia Virtuale**
  - **Supporta server di autenticazione ausiliari**
    - **RADIUS, TACACS, TACACS+**
- Non vi è Client L2F su computer remoto
  - **E' la telecom che forma il tunnel – *compulsory mode***
  - **In PPTP è il computer remoto che crea il tunnel – *voluntary mode***

L2TP

- Layer Two Tunnelling Protocol
  - **Molto simile a PPTP**
- Componenti
  - **L2TP Access Concentrator (LAC) – PAC**
  - **L2TP Network Server (LNS) – LNS**
- Per l'incapsulamento usa UDP porta 1701, non GRE
- In futuro sarà possibile usare ATM e Frame Relay
- Non usa connessione separata per il Control Channel
- Supporta *voluntary mode* e *compulsory mode*

L2TP


Computer
Remoto
con LAC
Rete
Telecom
ISP
NAS
Internet
LNS/NAS
Rete Privata


1
PPP
2
L2TP Control Channel and Tunnel
3
PPP
4
Datagrammi IP

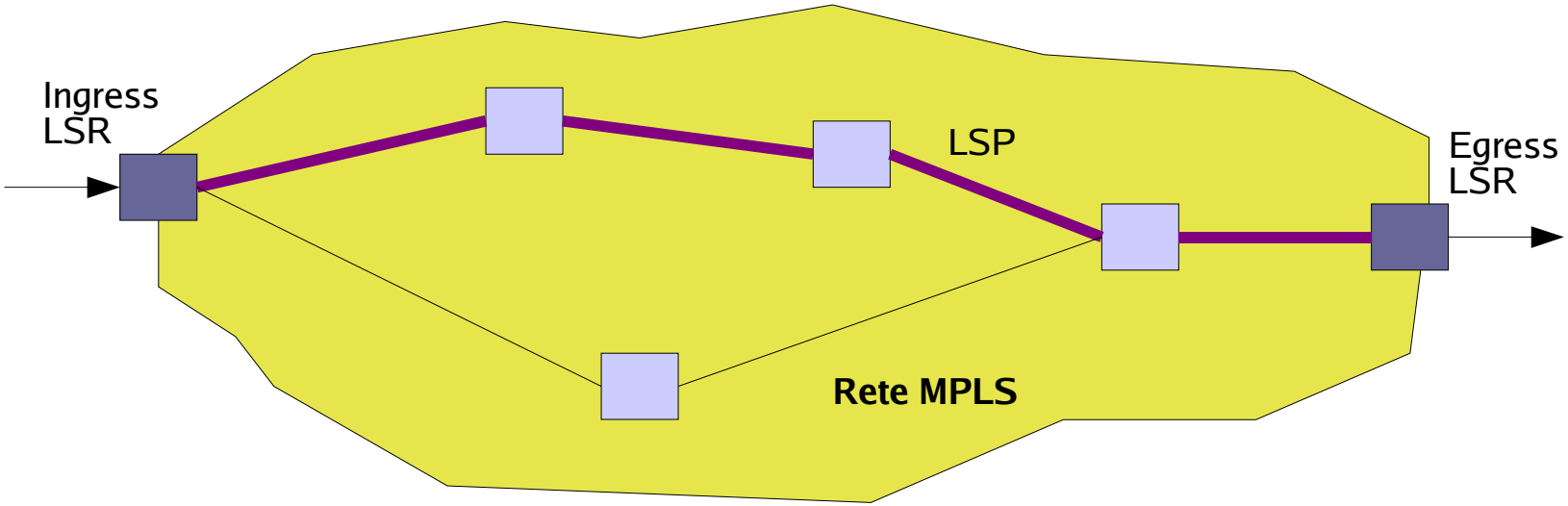
Layer 2 Tunnelling: Svantaggi

- Assenza di meccanismi solidi di protezione
  - Meccanismi di sicurezza ereditati da PPP
  - Non forniscono autenticazione a livello pacchetto
  - Insufficiente controllo e protezione dei pacchetti
  - Non includono Key Management Facility

Multi Protocol Layer Switching (MPLS)

- Scopi
  - Ridurre l'overhead di processamento ai router
  - Routing non basato su informazioni della testata di pacchetto
- Routing
  - Basato su un campo Label tra livelli link e rete
    - **Indice in una tabella di forwarding**
    - **La label è rimpiazzata ad ogni operazione di routing**
    - **Più labels sono possibili – label stacking**
  - Fornito da Label Switch Router (LSR)
    - **Ingress point**
      - **Unico punto di analisi della testata del pacchetto**
    - **Routing LSR**
    - **Egress router**

MPLS



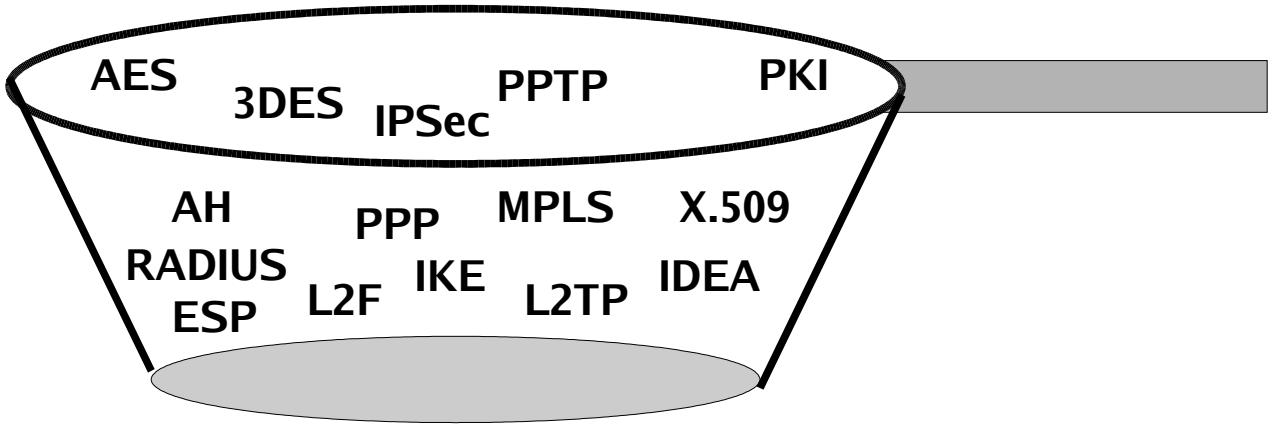
- Etichette hanno significato locale
  - **Label Distribution Protocol per distribuire le etichette**
  - **Etichette di 32 bit: 20 di label, 12 di extra info**
- Applicabile aqualsiasi protocollo di rete, non solo IP
- Supporto a Quality of Service (QoS)

MPLS

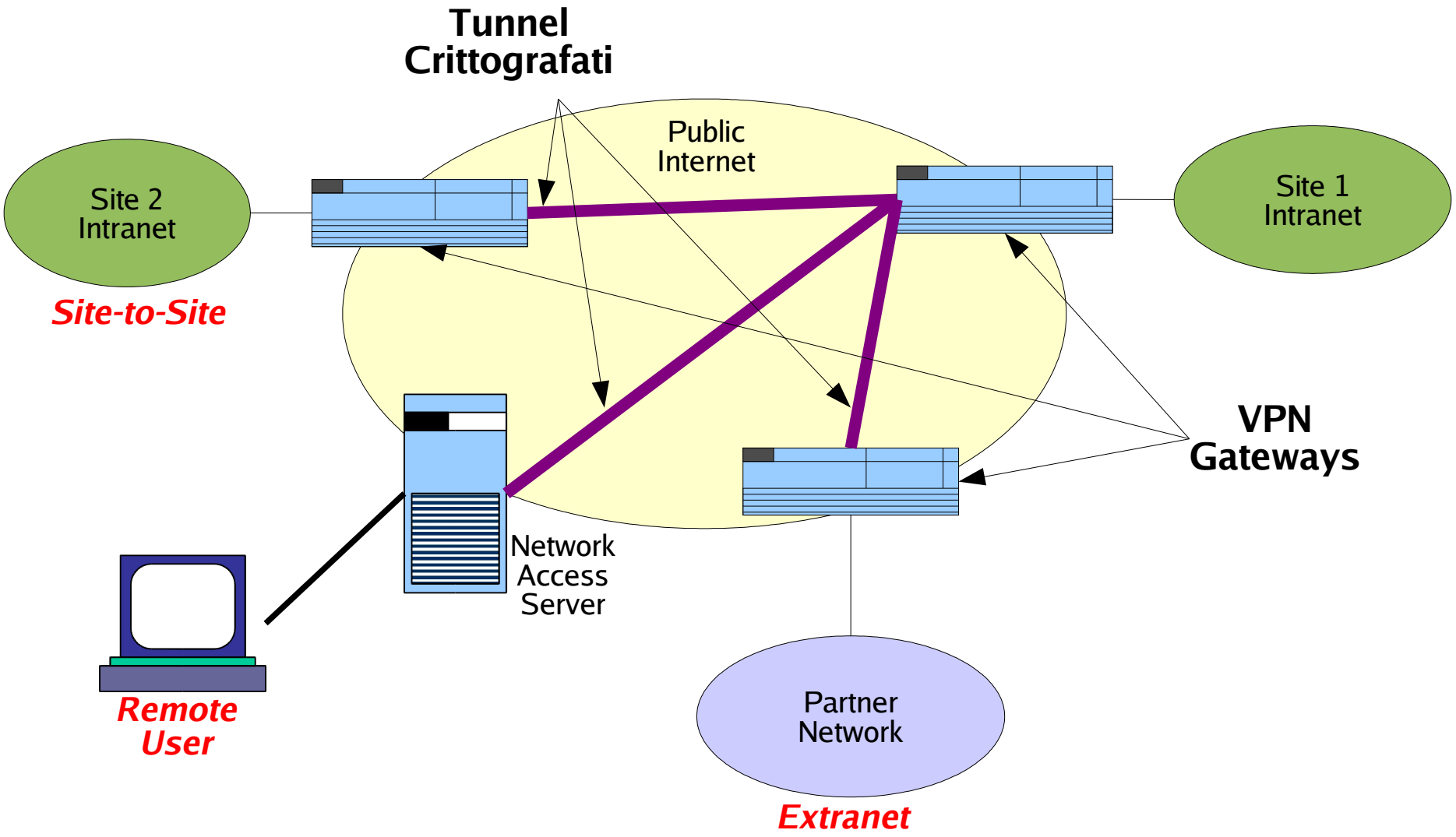
- Vantaggi
  - Domini di routing logicamente indipendenti
  - Supporto a Quality of Service
    - **Prenotazione di risorse ad uso esclusivo**
  - Aggregazione di traffico con simile livello di sicurezza
- Svantaggi
  - Non supporta direttamente Autenticazione e Confidenzialià
  - Fiducia implicita nei LSR intermedi
  - Il Payload non è reso opaco

Funzioni di un Gateway VPN

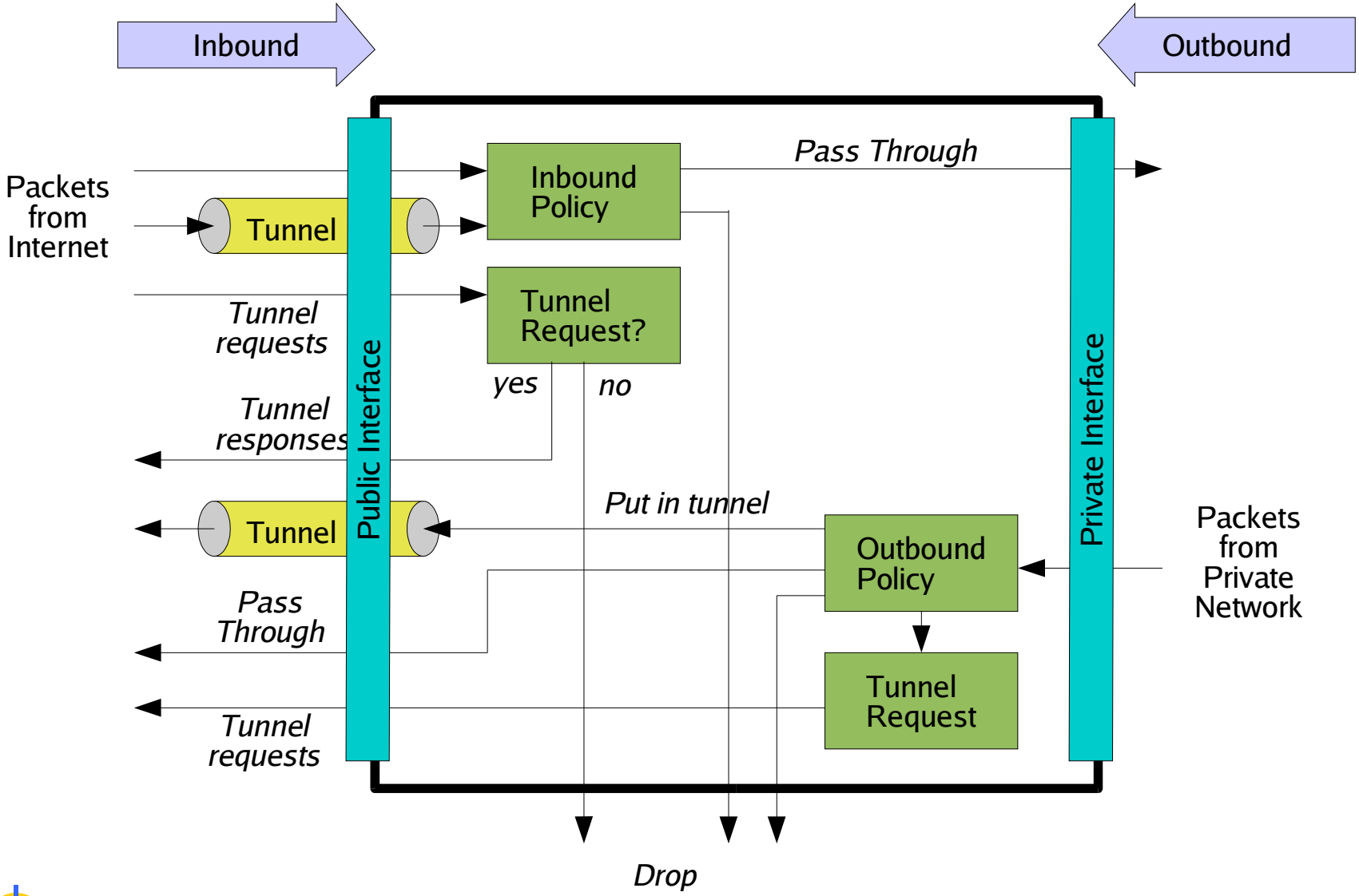
– Scelta di tecnologie appropriate dalla “zuppa” di simboli
  - **Scelte appropriate a tutti i livelli**
  - **Implementazioni in hardware, software o entrambi**
  - **Considerare anche failover e bilanciamento del carico**



Tipi di VPN Gateways



VPN Gateway



StarShell

Gateway Site-to-Site Intranet

- Tutto il traffico crittografato
  - **Algoritmo 3DES**
  - **Chiavi generate dinamicamente**
- Tutte le sottoreti comunicano tra loro tramite le VPN
  - **Incapsulamento per nascondere indirizzi privati**
  - **IPSec in Tunnel Mode**
  - **Aggregazione di traffico**
- Certificati digitali per l'autenticazione reciproca tra ogni coppia di gateway
  - **Algoritmo IKE**
  - **Gestione certificati e revoche**

Gateway Remote Access

- Implementa allocazione dinamica di indirizzi
  - **Tipicamente DHCP**
- Tutto il traffico crittografato
  - **Algoritmo 3DES**
  - **Chiavi generate dinamicamente**
  - **Tunnelling ESP e IKE**
- Accesso differenziato sulla base di identità e policy
- Possibile accesso simultaneo a Internet e Intarnet
  - **Proteggere da condotte involontarie**
  - **Firewall associato al Gateway**
- Meccanismi di autenticazione multipli
  - **RADIUS**
  - **Certificati digitali**

Gateway Extranet

- Tutto il traffico crittografato
  - **Algoritmo 3DES**
  - **Chiavi generate dinamicamente**
  - **Tunnelling ESP e IKE**
- La Extranet può accedere solo a un sottoinsieme limitato di server interni
  - **Filtri di accesso**
  - **Security Policy Database**
  - **Più tunnel con la stessa Extranet**
- Autenticazione forte
  - **Certificati digitali**

Funzioni ausiliarie dei Gateways

- Routing e forwarding
  - **Network Address Translation – eventuali problemi di coesistenza con IPSec**
- Filtraggio pacchetti
  - **Applicabilità a tunnel multipli**
  - **Difficoltà con crittografazione del contenuto – prima e dopo il tunnel**
- Considerazioni Quality of Service
- Failover e Bilanciamento del Carico
- Accelerazione Hardware

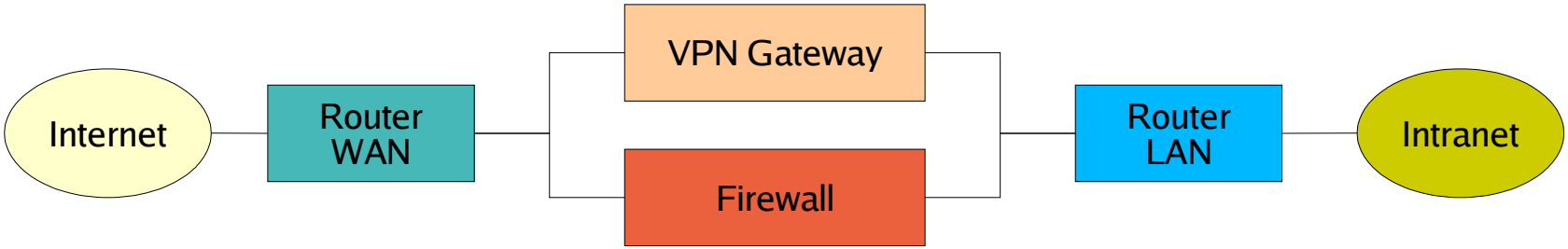
Configurazione dei Gateways

- Informazioni di Identità
  - Identità multiple per funzioni multiple
    - **Nomi, indirizzi interni ed esterni e di management, certificati**
- Informazioni sui Device Esterni
  - Routers, DNS, RADIUS, SNMP, Policy Servers, CA, Server di Directory, DHCP, WINS
- Informazioni di Security Policy
  - A seconda del tipo di funzione
    - **Site-to-Site, Extranet, Remote Access**
  - Tipi di tunnel permessi, accessibilità dei server interni, filtri inbound e outbound, pool di indirizzi per host remoti, metodi di accesso

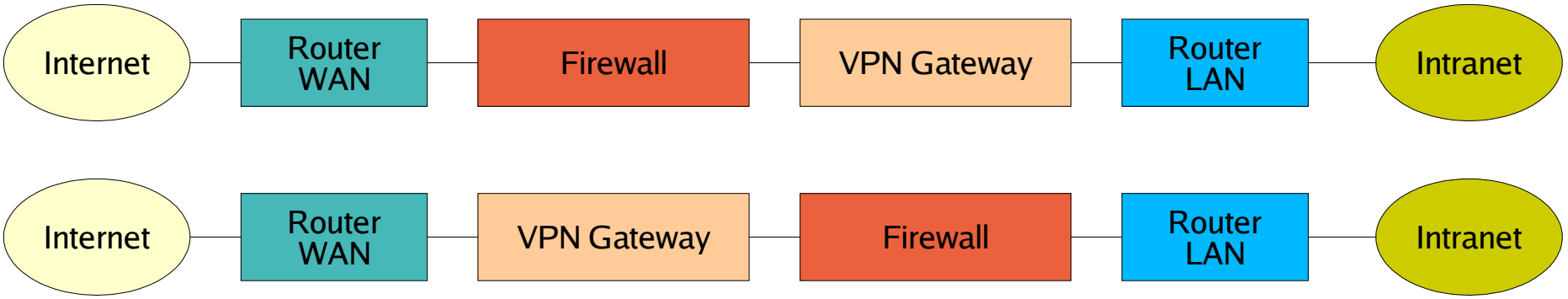
Gestione dei Gateways

- Gestione della Configurazione
  - Interfacce a comando o GUI
  - Programmabilità ed automatizzazione
- Monitoraggio della Rete
  - Network Management – SNMP
  - Monitoraggio: ping, traceroute, scansioni di vulnerabilità
  - Logging e analisi
- Informazioni di Contabilità
  - Efficacia e tuning, ripartizione spese di utilizzo
- Gestione dei Certificati
  - Processo di certificazione e adeguamento agli standard
  - Manutenzione e decadimento dei certificati

Interazioni Gateway VPN - Firewall

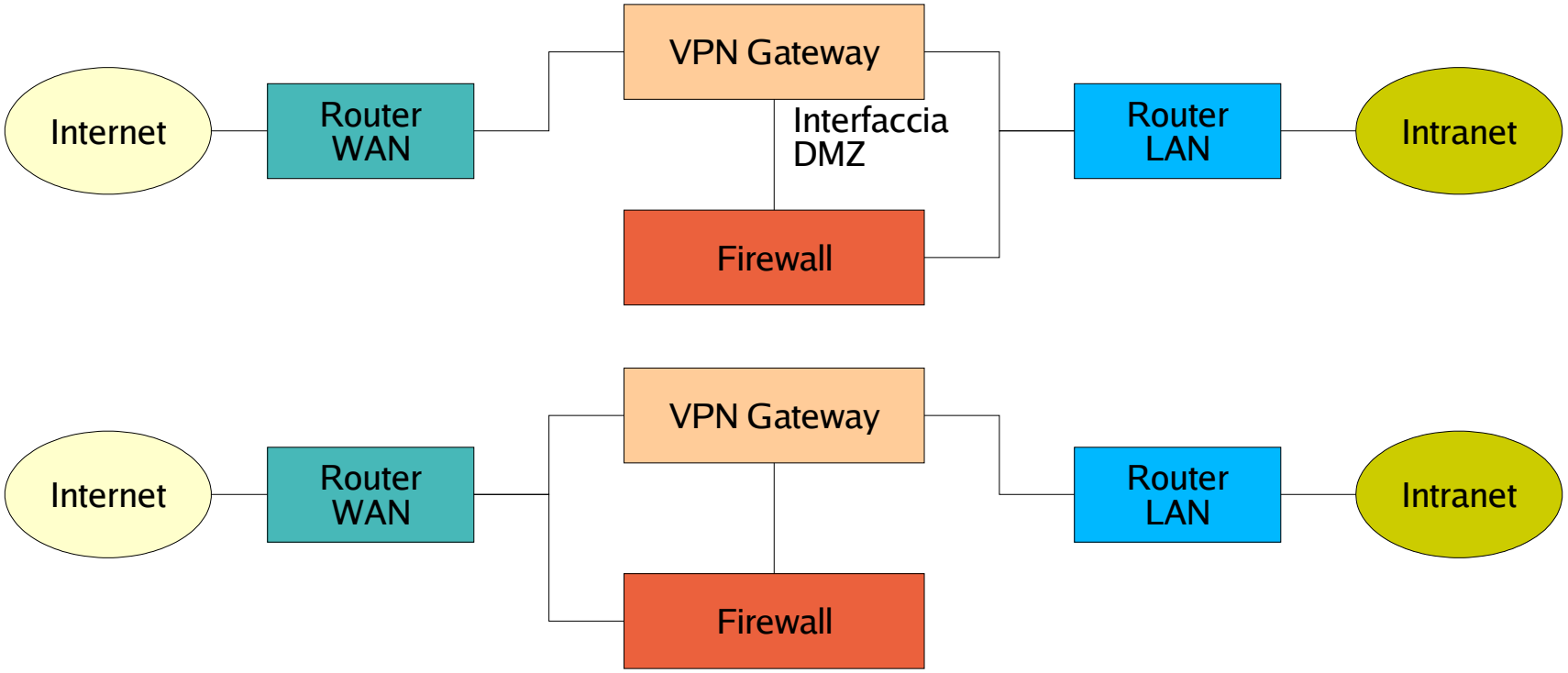


Configurazione in Parallelo



Configurazioni in Serie

Interazioni Gateway VPN - Firewall



Configurazioni Ibride

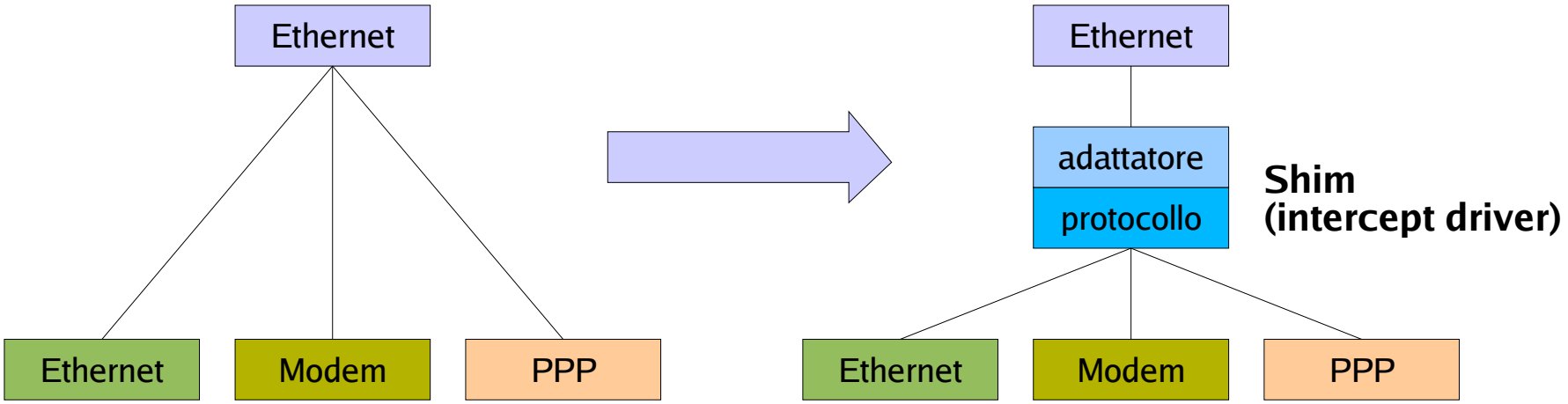
Design dei VPN Gateway

- Topologia di rete
  - Maglie piene, hub, maglie parziali
- Indirizzamento e routing
  - Tabelle di routing statiche
- Quality of Service
  - Combinata con routing e filtraggio: Routing version 2
  - IETF DiffServ
    - **Differentiated Service Code Points (DSCP) in testata IP**
- Scalabilità
    - **Banda usata**
    - **Numero di tunnel**
  - Differenziare Site-to-Site da Remote Access

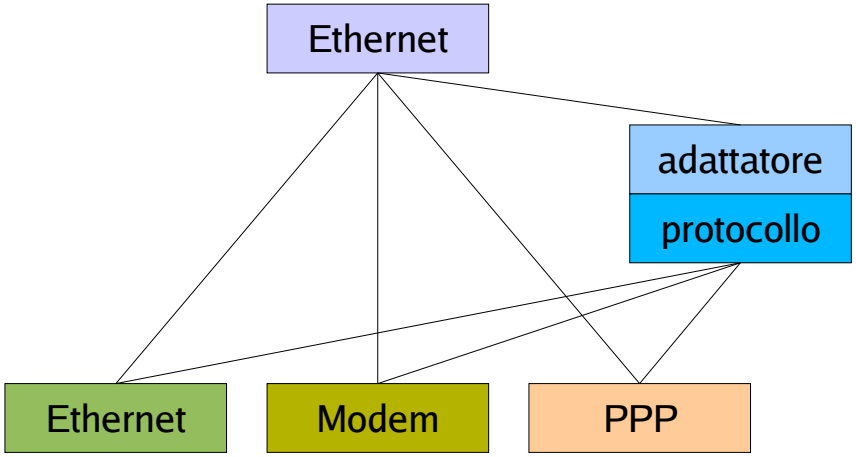
VPN Clients

- Operati da non esperti
  - **Singola selezione di protocollo di tunnelling nell'azienda**
  - **Automatismi di configurazione e attivazione**
- Autenticazione
  - **Semplice scelta: password**
    - **Challenge-Response trasparente o RADIUS**
  - **Più complessa: certificati lato client**
    - **Difficoltà di emissione e manutenzione**
- Controllo accesso delegato al Gateway
- Integrità dati e Confidenzialità
  - **Intrinseche nella scelta del VPN**
- Altre funzioni
  - **Connessione Dial-up o Diretta**
  - **Indirizzamento conforme a regole aziendali**
  - **Timeout di disconnessione per idle**

Architettura di rete Client Windows



Aggiunta di uno Shim tra il TCP/IP e gli adattatori di rete



Aggiunta di un Adattatore Virtuale
tra il TCP/IP e gli adattatori reali

Altri Sistemi Operativi

- UNIX
  - Modifica del Kernel
    - **Aggiunta di IPSec**
  - Aggiunta di un nuovo device driver VPN
    - **Modulo caricabile a run-time**
  - Offre più controllo di Windows
    - **Richiede più attenzione utente**
- MacOS
  - Simile al secondo caso di UNIX
    - **Moduli basati su system V STREAMS**

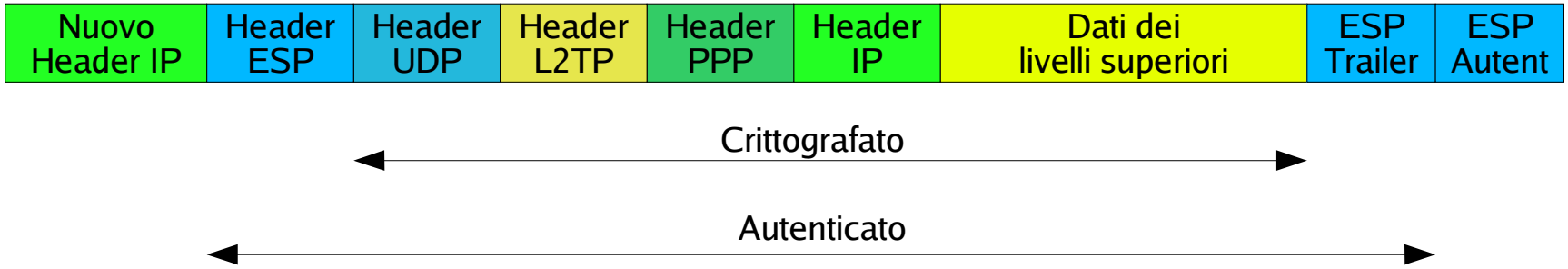
Considerazioni Operative

  - Necessità di facilità d'uso e robustezza (utenti semplici)
  - Diminuzione apprezzabile delle prestazioni
- Lavoro entro il Firewall aziendale
  - Apertura porte per il VPN
- Incompatibilità NAT/PAT con IPSec
- Problemi di MTU e frammentazione pacchetti
  - Notevole lunghezza dei pacchetti IPSec
- Interfacciamento ai server DNS aziendali e pubblici
  - DNS pubblici inaccessibili in regime VPN
- Collegamento ai server WINS

Client IPSec per Windows

- Aspetti di dettagli implementativi
  - **Modi di incapsulamento (tunnel-transport, AH-ESP)**
  - **Opzioni crittografiche (DES, 3DES, AES, RC4, RC5)**
  - **Opzioni di autenticazione (RADIUS, TACACS, PKI)**
  - **Meccanismi per assegnazione indirizzi (DHCP, proprietari)**
  - **Capacità di compressione dati**
  - **Meccanismi di timeout (idle, keepalive)**
- Rivenditori principali prodotti IPSec per Windows
  - **Alcatel/TimeStep**
  - **CheckPoint**
  - **Cisco**
  - **Indus river**
  - **Intel/Shiva**
  - **Nortel**
  - **RedCreek**

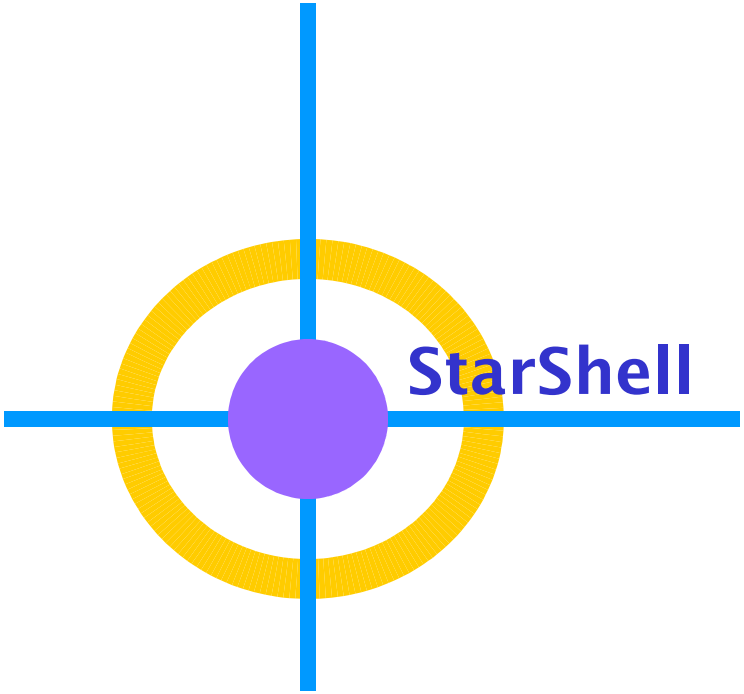
Client combinati L2TP/IPSec



- Disponibile in Windows
- Overhead di incapsulamento notevole
  - **La compressione è desiderabile**
- L2TP fornisce autenticazione utente
  - **PAP, CHAP, MS-CHAP, EAP**
- IPSec fornisce autenticazione host e Security Association

Client per altri sistemi Operativi

- Layer 2
  - PPTP-linux
- IPSec
  - Linux FreeS/WAN
  - KAME – varianti BSD
  - Cerberus – Linux
  - Ipnsec – Linux e OpenBSD


StarShell