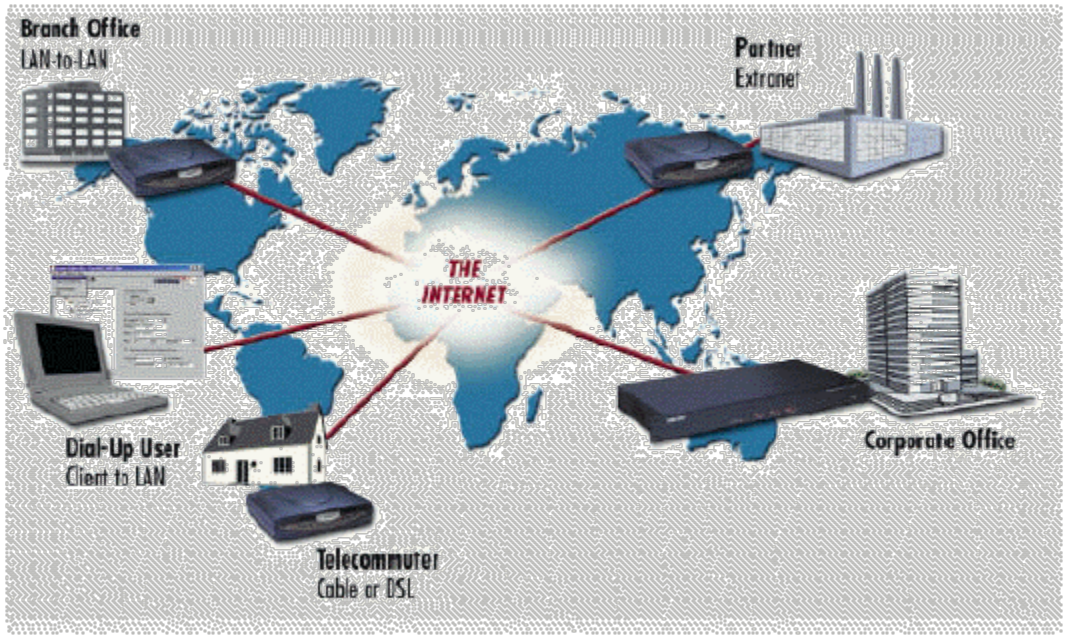
VPN: connessioni sicure di LAN geograficamente distanti

IZ3MEZ
Francesco Canova
www.iz3mez.it
francesco@iz3mez.it

Virtual Private Network, cosa sono?

- Le Virtual Private Networks utilizzano una parte di infrastruttura pubblica (Internet) per veicolare traffico "privato" tra alcune entità (ad esempio sedi aziendali)

- Requisiti importanti per le VPN sono
  - la sicurezza,
  - la privatezza delle informazioni,
  - la possibilità di accesso remoto,
  - la trasparenza alle applicazioni



Tipi di VPN

- Una classificazione comune è la seguente:
  - intranet VPN: collega i diversi uffici periferici o sedi della società
  - remote access VPN: collega la sede centrale della società con gli utenti remoti o mobili
  - extranet VPN: collega la sede centrale con i business partner, i fornitori ed i clienti

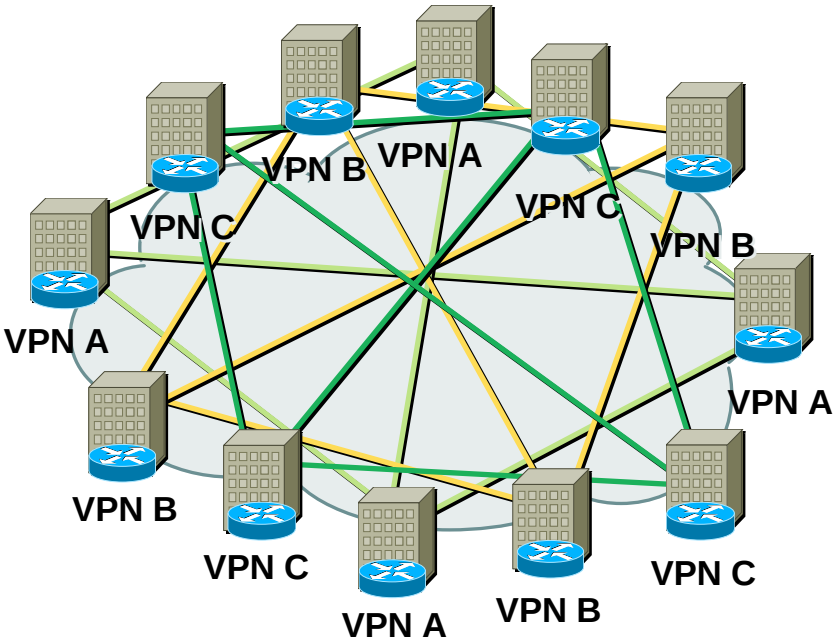
- Ciascuna categoria ha specifici requisiti in termini di tecnologia e sicurezza
- Ad esempio:
  - intranet VPN: protezione delle informazioni, alla performance delle risposte, alla scalabilità
  - remote access VPN: autenticazione “forte” e sistema efficiente di gestione centralizzata degli account
  - extranet VPN: utilizzo di piattaforme standard ed aperte al fine di garantire l’operabilità tra le parti

Esistono due possibili modelli realizzativi

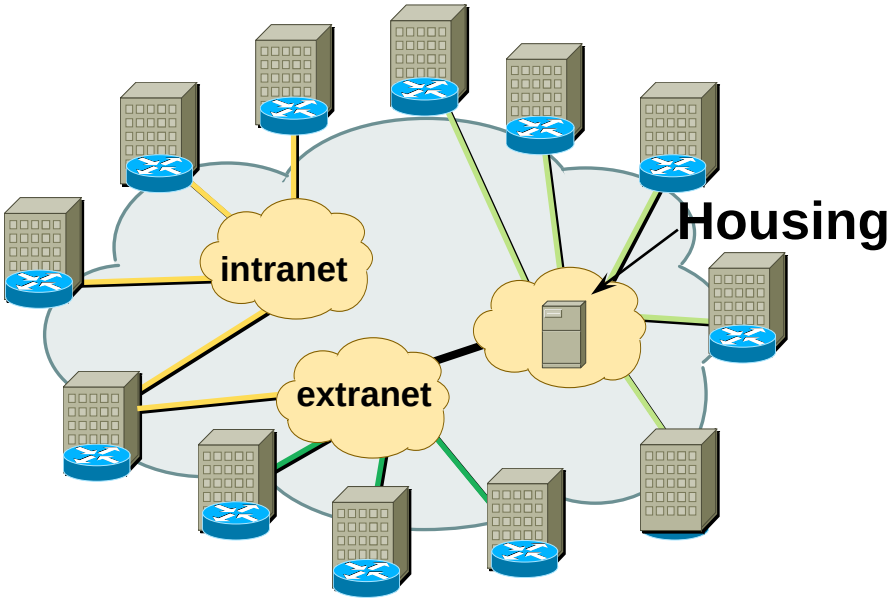
- Overlay
  - trasparenza della VPN all'interno del backbone dell'Internet Service Provider
  - routing: pacchetti scambiati solo tra i edge router
  - flusso punto-punto di pacchetti autenticati (con contenuto informativo cifrato) incapsulati in pacchetti tradizionali
  - tecnica principalmente utilizzata: Tunneling
    - livello 2: PPTP, L2TP
    - livello 3: IPsec

- Peers
  - i router del backbone hanno la conoscenza della topologia della VPN
  - routing: esplicito all'interno del backbone
  - tecnica principalmente utilizzata: Mpls

Overlay vs Peers



Overlay VPN
VPN Topology



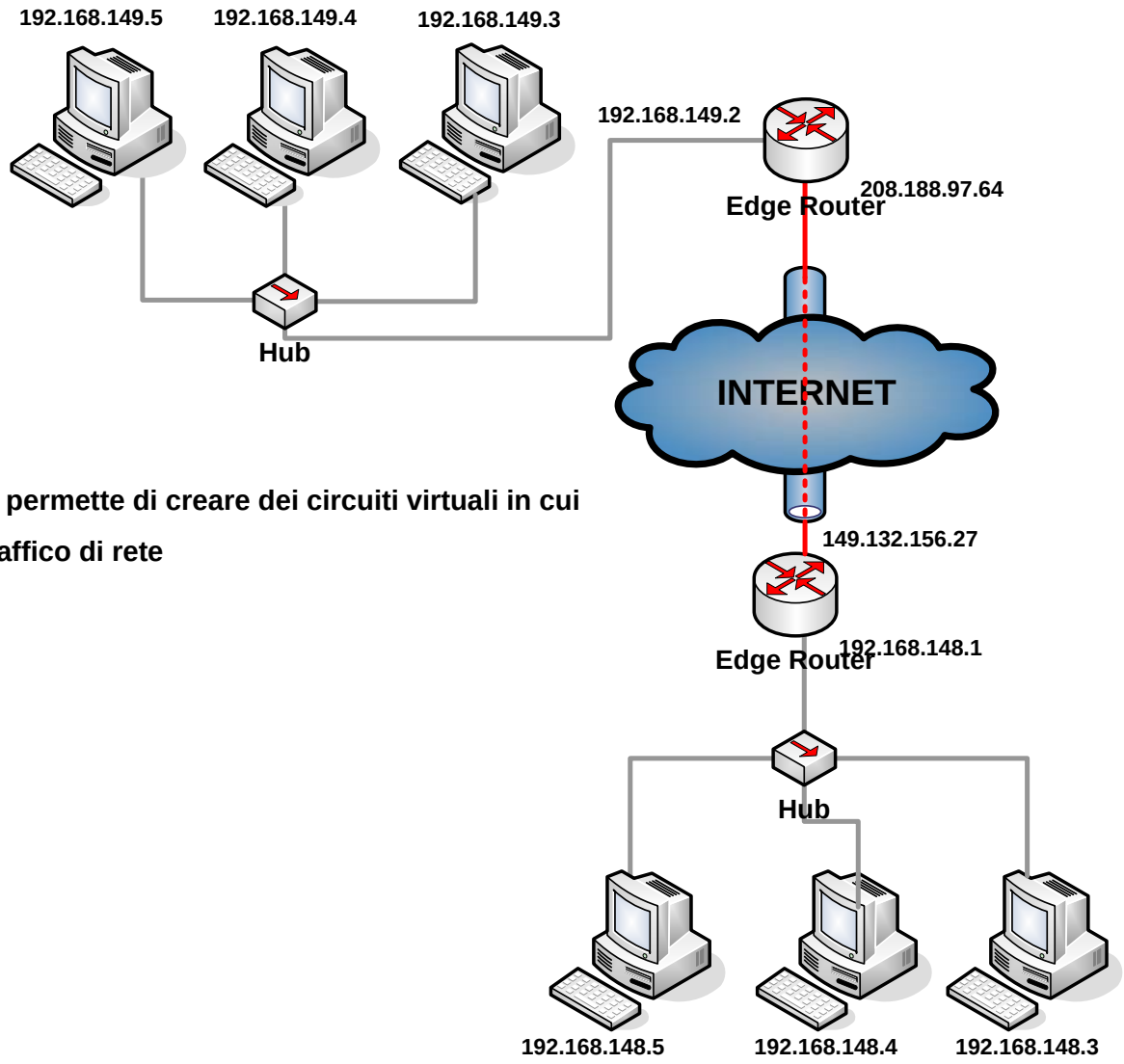
Peers VPNs
VPN Topology

Tunneling

- Funzionamento:
  - un pacchetto raggiunge il edge router il quale determina la locazione del destinatario
  - inserisce il pacchetto originale in un header IP contenete come indirizzo di destinazione quello dell'edge router che ha in carico il servizio della destinazione del pacchetto
  - una volta ricevuto il pacchetto, il router lo "sbusta" e lo invia all'effettivo destinatario

- Vantaggio: è possibile far viaggiare messaggi con protocolli di livello 3 diversi da IP

Tunneling: uno schema



Il tunneling permette di creare dei circuiti virtuali in cui viaggia il traffico di rete

La sicurezza

- Un aspetto fondamentale dell'architettura della VPN riguarda la problematica della sicurezza

- Il protocollo TCP/IP utilizzato da Internet non offre adeguate garanzie rispetto agli elementi fondamentali di una trasmissione sicura che sono:
  - controllo d'accesso: abilitazione al servizio solo alle parti autorizzate
  - autenticazione: identificazione delle parti in comunicazione
  - confidenzialità: protezione delle informazioni riservate
  - integrità: garanzia che i dati non siano manipolati durante la trasmissione
- Attraverso la cifratura è possibile garantire confidenzialità e integrità delle trasmissioni dati
- In generale la sicurezza (matematica) di un algoritmo di cifratura è direttamente proporzionale alla lunghezza della chiave

Cifratura dei messaggi

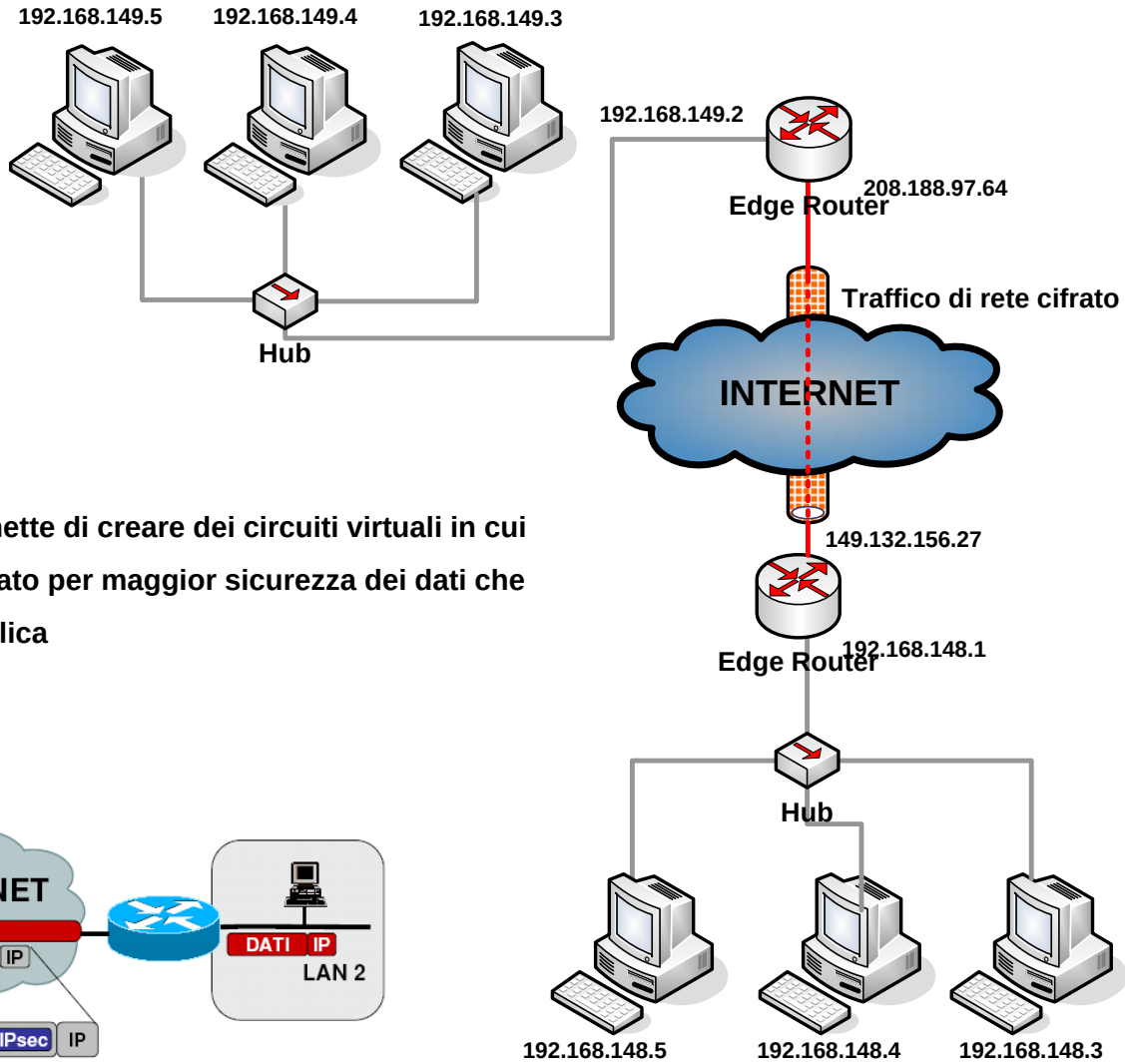
- Sono disponibili diverse alternative per la cifratura dei dati in trasmissione attraverso una VPN
- Alcune soluzioni prevedono di cifrare l'intero messaggio (IP Header e data) mentre altri cifrano solo la parte dati

- In particolare:
  - Place Transmission Mode: solo i dati mantenendo la dimensione del pacchetto invariata;
  - Transport Mode: solo i dati ma la dimensione dei pacchetti viene aumentata per offrire maggiore sicurezza nella trasmissione;
  - Encrypted Tunnel Mode: sia l'IP header che i dati, e le informazioni sono cifrate con un nuovo IP al fine di aumentare la sicurezza complessiva della rete

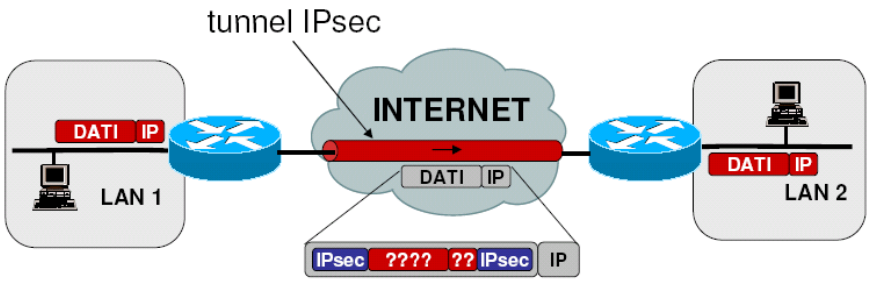
IPSec

- L'Internet Engineering Task Force (IETF) un organismo per la definizione degli standard Internet ha un gruppo di studio chiamato IP Security (IPSec) che lavora alla definizione di un protocollo di trasmissione dati Internet sicuro
- Poiché il protocollo IP non fornisce nessuna sicurezza, IPSec è stato introdotto con lo scopo di fornire servizi di sicurezza quali:
  - Cifratura del traffico: il traffico è letto solo dai destinatari
  - Integrità: assicura che il traffico non è stato alterato
  - Autenticazione dei peer: assicura che il traffico arrivi da un peer fidato
- Standard:
  - Authentication Header (AH): garantisce solo la data integrity;
  - Encapsulating Security Payload (ESP): fornisce sia cifratura che data integrity
- La differenza fra l'integrità dati in AH e ESP è che AH autentica l'intero pacchetto IP mentre ESP autentica solo i dati

Tunneling con IPSec



Il tunneling con IP sec permette di creare dei circuiti virtuali in cui viaggia il traffico di rete cifrato per maggior sicurezza dei dati che Viaggiano su una rete pubblica



Tunneling: altre tecnologie

- Però ci sono anche ...

Point to Point Tunneling Protocol (PPTP)	Sviluppato da Microsoft, è un'estensione del Point to Point Protocol (PPP) che incapsula IP, IPX, NetBEUI all'interno dei pacchetti IP. Prevede un meccanismo (proprietario e opzionale) di cifratura
Layer 2 Forwarding (L2F)	Sviluppato da Cisco viene utilizzato per il "tunnelling" di protocolli di tipo link (HDLC, asynchronous HDLC, SLIP). Non prevede la cifratura dei dati
Layer 2 Tunneling Protocol (L2TP)	Frutto di un accordo fra Microsoft e Cisco, permette il "tunneling" del traffico PPP su diversi network. Serve a fornire un multi-protocol dial-up service per i provider ISP ed i POP. Come L2F, anche L2TP non prevede cifratura
Socksv5	Alternativa di Nec a L2TP

- ... ed altre ancora

Fine