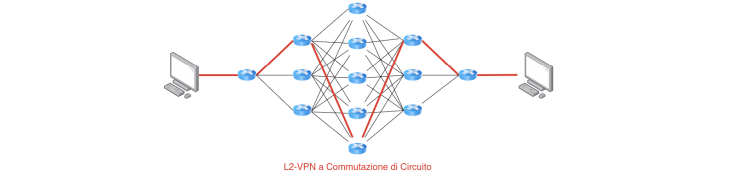
# Sicurezza su scala geografica

#### **L2-VPN**

**Linee dedicate**: realizzando una L2-VPN a tramite linea dedicata (Circuito diretto numerico) permette di definire dei collegamenti fisici punto-punto.



**Linee a commutazione di circuito**: realizzando una L2-VPN a commutazione di circuito vuol dire utilizzare una serie di funzionalità e tecniche legate alla telecomunicazione per creare un collegamento diretto tramite diversi nodi.



A causa degli alti costi implementativi, le L2-VPN sono state ormai soppiantate dalle **IP-VPN**: connessioni punto-punto basate su Internet come canale di comunicazione.

IP-VPN

Fornisce un metodo sicuro e veloce per comunicare con partner attraverso reti pubbliche (Internet).

Le IP-VPN vengono realizzate utilizzando Internet come canale di comunicazione, e creando connessioni sicure tramite meccanismi software.

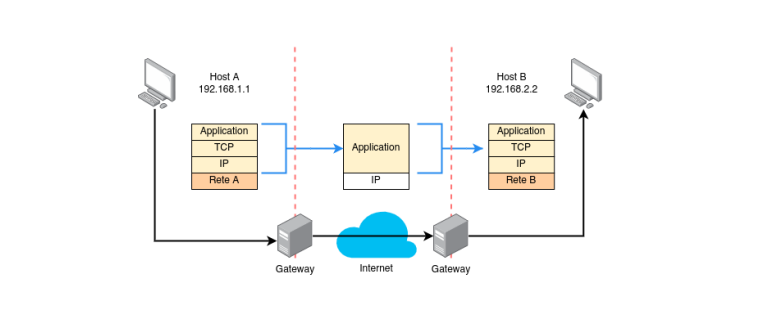
Tecniche per garantire riservatezza, integrità e autenticazione durante la comunicazione:

* Tunneling (incapsulamento)
* Cifratura

Tunneling

I pacchetti sono inseriti all'interno di altri pacchetti.

Esempio: incapsulamento IP. Utile per far comunicare gli host di due LAN che usano indirizzi privati oppure differenti protocolli di comunicazione.



Due tipologie di tunnel:

* Presenza di cifratura della comunicazione
* Presenza di funzionalità per garantire autenticazione e integrità dei pacchetti trasmessi

Possibilità di realizzare VPN a due livelli:

* Sopra il livello 3 dello stack TCP/IP: **IPSec**
* Sopra il livello 4 dello stack TCP/IP: **SSL**

#### IPSec-VPN

IPSec è di gran lunga la tecnologia più conveniente delle L2-VPN per realizzare VPN "stabili".

Allo stesso tempo, è considerata una tecnologia **rigida**, troppo legata ai sistemi operativi e troppo complessa da gestire nei casi di IP-VPN di mobilità tra un dipendente in viaggio e la propria azienda.

SSL-VPN

SSL-VPN è ad oggi la tecnologia considerata vincente per realizzare VPN grazie alla sua semplicità di realizzazione e flessibilità (consente connessioni VPN da qualsiasi dispositivo), indipendenza dal sistema operativo (operando sopra il livello 4 siamo a livello di user space) e più firewall-friendly.

# Architetture locali "sicure"

1. **Screening router**
2. **Dual-homed gateway/firewall**
3. **Screened-host gateway**
4. **Screened-host gateway**
5. **Screened subnet**