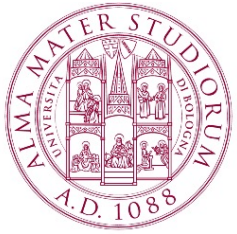


ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Virtualizzazione di rete

Franco CALLEGATI

Dipartimento di Informatica: Scienza e Ingegneria

Virtualizzazione

- Creare versioni “virtuali” di sistemi di computazione, di memorizzazione, di rete
- Versione virtuale di un sistema
  - Il sistema viene eseguito come elemento software logicamente indipendente dall’hardware utilizzato

È facile spostare un sistema virtuale da un server fisico all'altro, scalare le risorse a seconda delle necessità e creare nuovi ambienti di test senza dover aggiungere hardware fisico.

- Vantaggi
  - Condivisione di risorse fisiche
  - Disaccoppiamento del progetto software da quello hardware
  - Maggiore flessibilità (mobilità, scalabilità)

La virtualizzazione permette di utilizzare al meglio le risorse fisiche. Invece di avere risorse hardware dedicate e spesso sottoutilizzate, più sistemi virtuali possono condividere lo stesso hardware, aumentando l'efficienza complessiva.

- Criticità
  - Isolamento fra sistemi distinti che condividono lo stesso hardware

Se l’isolamento tra questi sistemi virtuali non è adeguato, problemi in un sistema potrebbero influire sugli altri.

  - Sicurezza e privacy

Dato che più sistemi virtuali condividono lo stesso hardware, è fondamentale garantire che non vi siano compromissioni nella sicurezza che possano esporre dati o risorse di un sistema virtuale agli altri.

Grazie alla virtualizzazione, il software può essere progettato e distribuito indipendentemente dall’hardware sottostante. Questo rende possibile spostare facilmente sistemi da una macchina fisica all'altra.

La virtualizzazione di rete è un processo che permette di creare reti logiche sovrapposte all'infrastruttura fisica esistente.

Virtualizzazione di rete

- Punto di partenza
  - L'infrastruttura di rete, soprattutto se geografica, non è facilmente modificabile su richiesta
  - Le esigenze di servizio dell'utenza presentano una complessità sempre crescente

Cambiare la configurazione di una rete fisica può richiedere interventi complessi, lunghi e costosi.

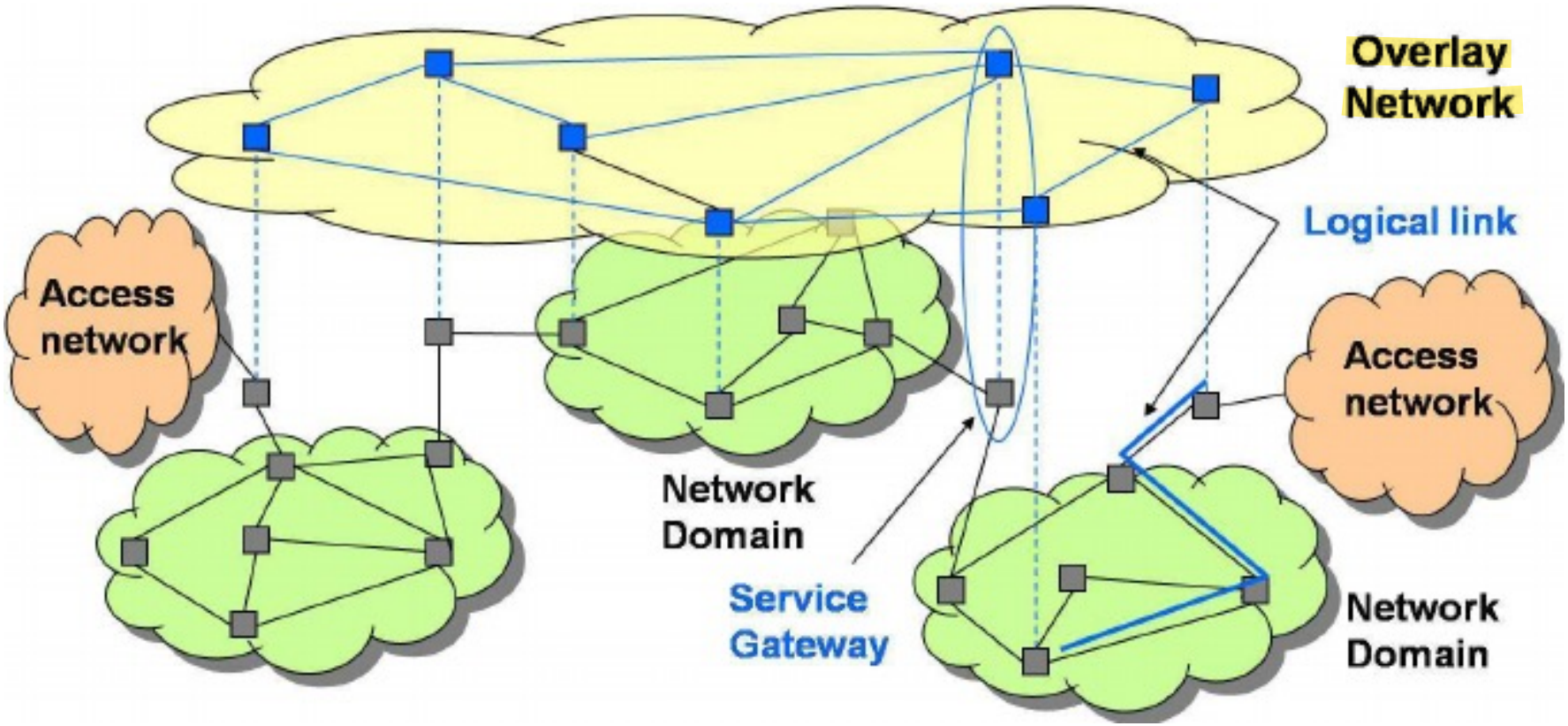
Gli utenti oggi richiedono servizi più complessi e personalizzati, con necessità di risorse di rete che possano adattarsi velocemente.

- Obiettivo della virtualizzazione
  - Realizzare topologie o funzionalità sull'infrastruttura esistente diverse da quelle native

di rete che possano essere implementate

- In generale si parla di reti "overlay"
  - Sovrapposte logicamente all'infrastruttura fisica per realizzare funzionalità diverse da quelle normalmente fornite dalla stessa

Reti “Overlay”



Tecnologie di virtualizzazione

- Virtual Local Area Network (VLAN) IEEE 802.1Q
- Generic Routing Encapsulation (GRE) RFC 1701
- Virtual eXtensible Local Area Network (VXLAN) RFC 7348
- Virtual Private Network (VPN)

- Virtual Private Wire Service (VPWS)
- Virtual Private LAN Service (VPLS) RFC 4761 4762

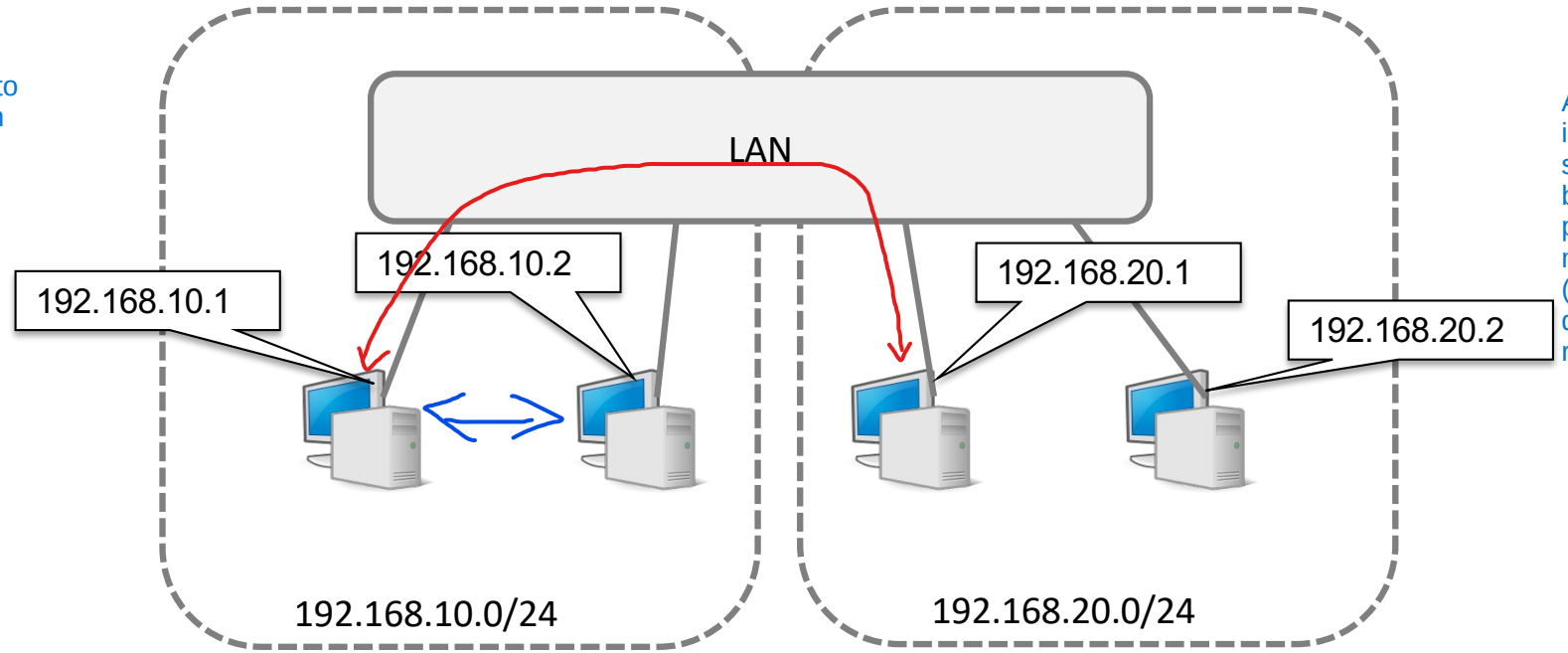
La network IP

Una rete IP non rappresenta l'infrastruttura fisica di una rete, bensì una struttura logica sopra un'infrastruttura fisica che permette ai dispositivi di comunicare tra loro utilizzando indirizzi IP

- La network IP è già una forma di network overlay
- Gli switch interconnessi realizzano la LAN
  - Un solo dominio di broadcast
  - La ripartizione degli host in diverse network IP determina differenze nelle politiche di instradamento ~~politica di instradamento~~
    - Direct forwarding fra Host della stessa network IP
    - Indirect forwarding tramite gateway fra host di network IP diverse

All'interno della LAN, i dispositivi sono suddivisi in diverse network IP. Ogni network IP è rappresentata da un range specifico di indirizzi IP e rappresenta un segmento logico all'interno della rete. Questa suddivisione permette di applicare politiche di instradamento differenziate per ciascun gruppo di dispositivi.

All'interno di una LAN, tutti i dispositivi condividono lo stesso dominio di broadcast, ovvero una porzione di rete dove i messaggi broadcast (indirizzati a tutti i dispositivi) possono essere ricevuti da tutti i dispositivi.



GRE Tunnel (RFC 1701)

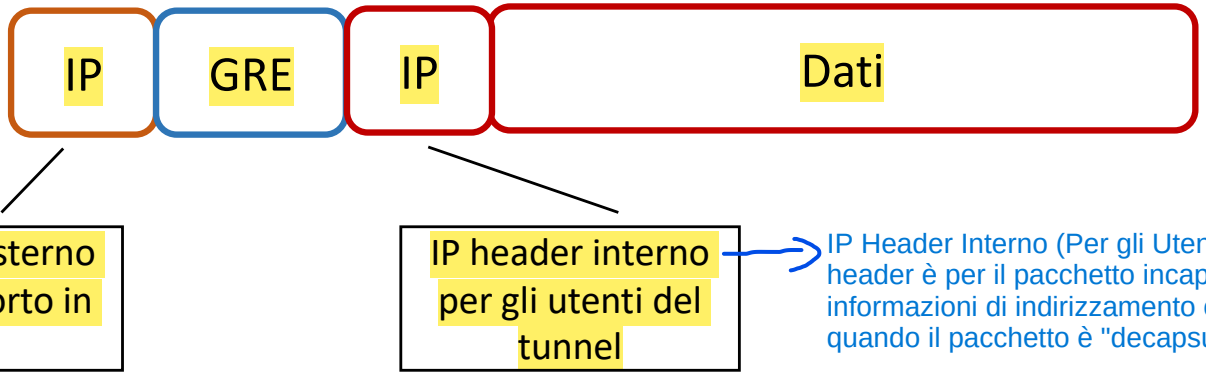
Questo header contiene informazioni di controllo che specificano il tipo di dati incapsulati e altri dettagli di gestione del tunnel.

- Protocollo per l'incapsulamento di pacchetti generici su protocollo IP

Il protocollo GRE permette di prendere un pacchetto di dati generico (può essere un pacchetto di vari protocolli) e inserirlo all'interno di un pacchetto IP. In questo modo, è possibile utilizzare l'IP come mezzo di trasporto per dati che non necessariamente seguono il protocollo IP originale.

- In particolare può permettere l'incapsulamento di IP su IP

Questo permette di creare una connessione privata tra due punti, trasportando pacchetti IP all'interno di un altro pacchetto IP.



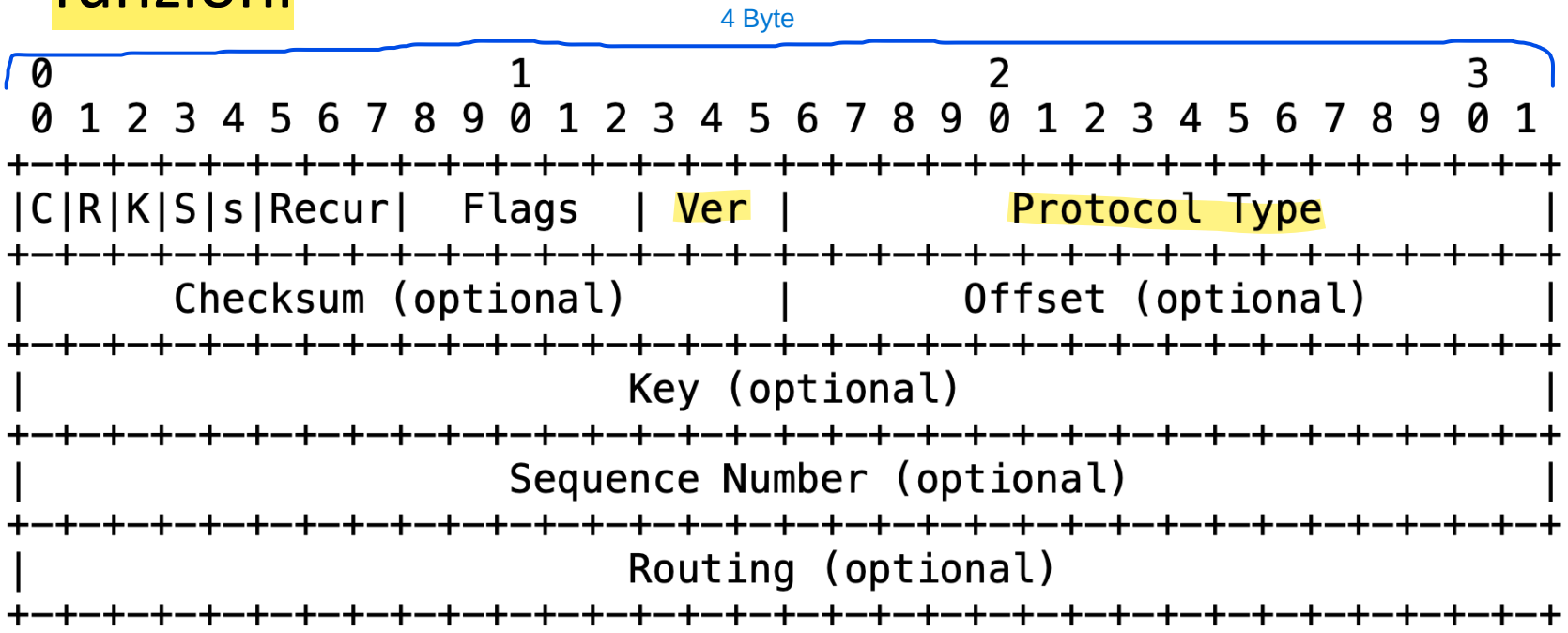
IP Header Interno (Per gli Utenti del Tunnel): Questo header è per il pacchetto incapsulato e contiene le informazioni di indirizzamento originali, visibili solo quando il pacchetto è "decapsulato" alla fine del tunnel.

IP Header Esterno (Per il Trasporto): Questo header contiene gli indirizzi IP del router di origine e del router di destinazione del tunnel GRE. Questi indirizzi identificano i punti terminali del tunnel attraverso il quale il pacchetto viaggia. All'arrivo al router di destinazione, l'intestazione GRE e l'intestazione IP esterna vengono rimosse, permettendo al pacchetto originale di proseguire verso la sua destinazione finale.

GRE header

- Version (0) indica la versione dell'header
- Protocol type: dice che tipo di protocollo viene incapsulato nel tunnel
- Sono poi disponibili campi opzionali per altre funzioni

Indica la versione dell'header. Attualmente, la versione più comune è la versione 0, che si riferisce al GRE standard.



GRE header: campi opzionali

- Checksum
  - Inserito per controllare la correttezza dei dati (Internet checksum)

Utilizzato per verificare l'integrità del pacchetto GRE (Controlla la correttezza dei dati durante il transito.).

- Key

Autenticazione della sorgente del pacchetto: Il campo Key può contenere un valore specifico che consente al destinatario di verificare l'origine del pacchetto incapsulato.

  - Può essere inserito per autenticare la sorgente del pacchetto incapsulato nel tunnel con un qualche metodo di autenticazione (password)
- Sequence Number

Utilizzato per numerare i pacchetti in sequenza (Numerando i pacchetti, permette di mantenere l'ordine di arrivo dei pacchetti alla destinazione, riducendo il rischio che pacchetti arrivino fuori sequenza).

  - Inserito alla sorgente per stabilire la sequenza di invio dei pacchetti sul tunnel
  - La destinazione dovrebbe instradare i pacchetti ricevuti nel corretto ordine

Alla sorgente, i pacchetti vengono numerati in sequenza, mentre la destinazione usa questi numeri per riorganizzare i pacchetti nel corretto ordine.

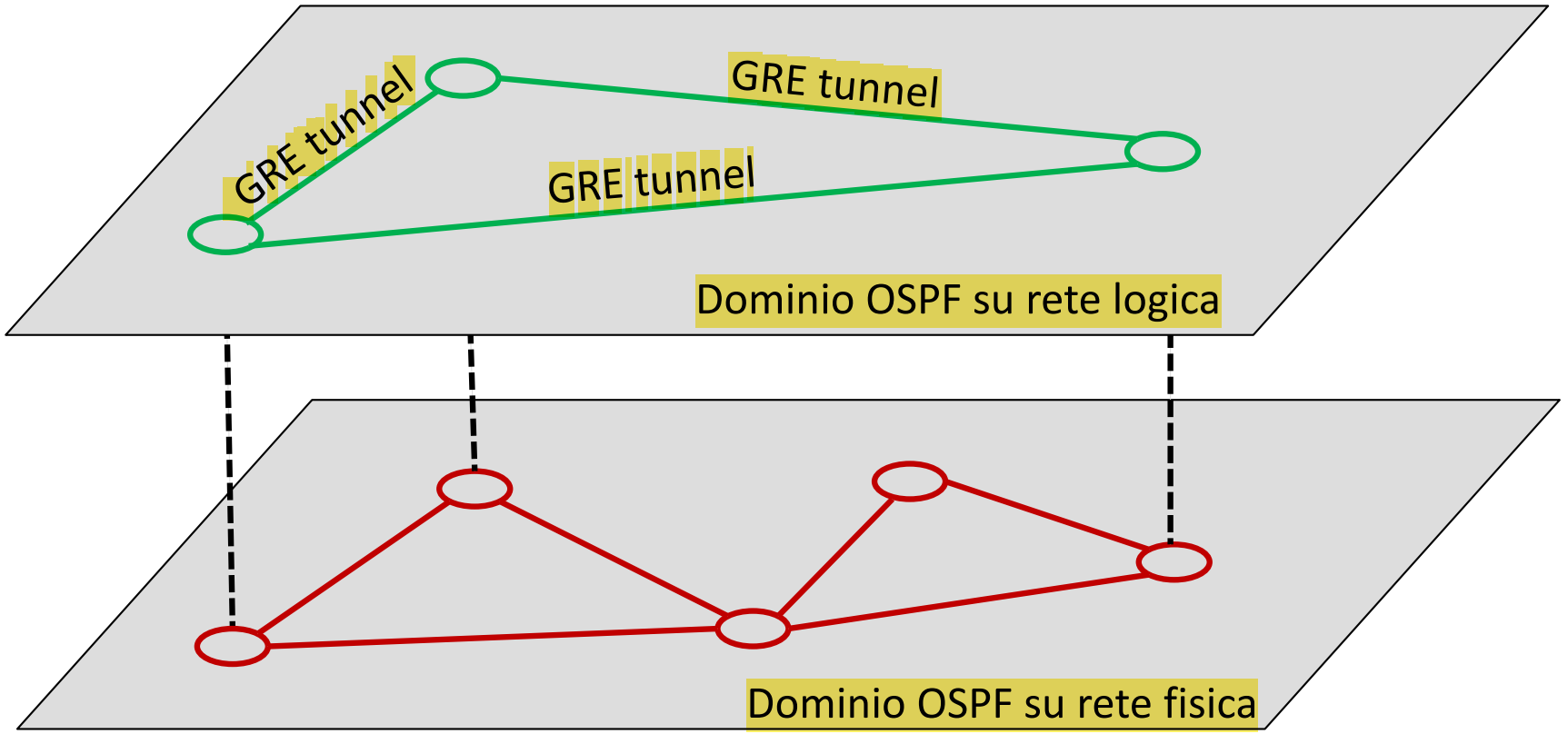
- Routing

Può contenere una lista di router che il pacchetto dovrebbe attraversare, definendo una "politica di instradamento" che controlla il cammino del pacchetto.

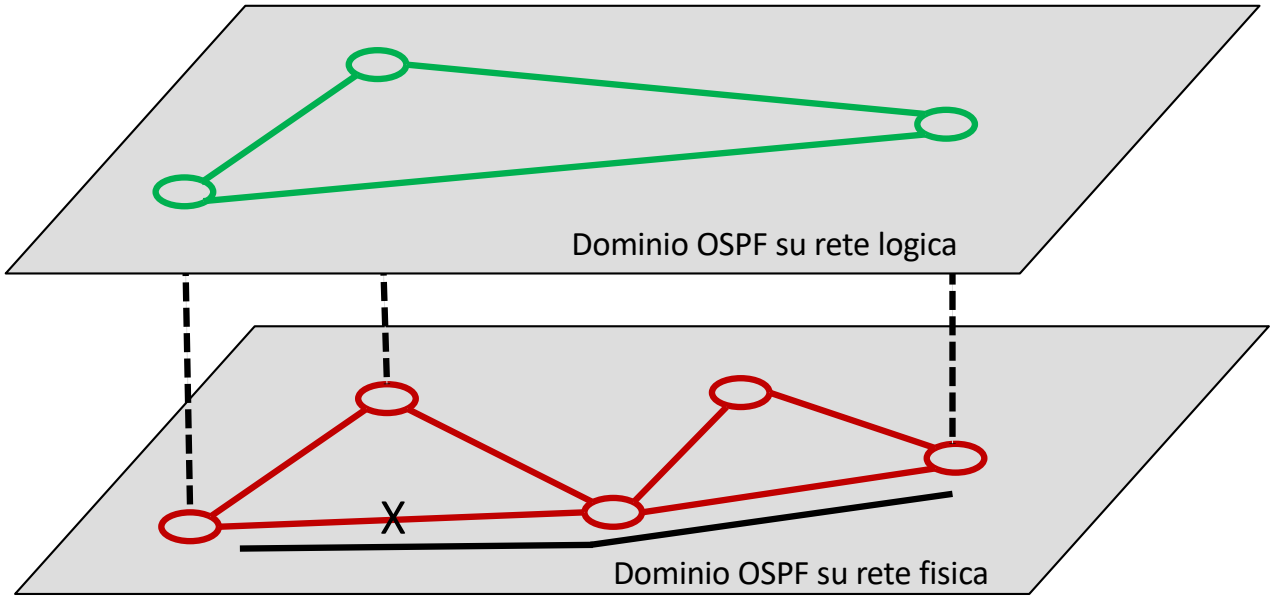
  - È possibile elencare i router che si vuole vengano attraversati dal pacchetto (determina la politica di instradamento del tunnel)

Applicazione del GRE

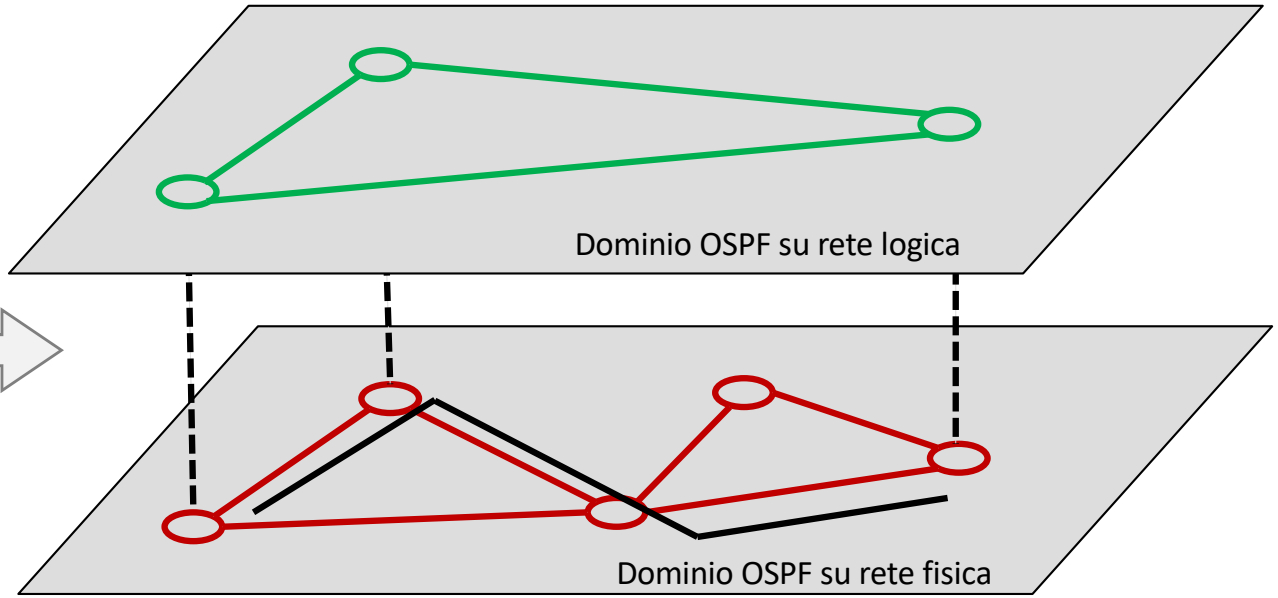
- Incapsulamento di IP su IP
- Permette di creare un overlay a livello di routing



Applicazione del GRE



Una modifica del percorso nel dominio su rete fisica non viene percepita nel dominio su rete logica



In una rete VXLAN, i VTEP incapsulano i frame Ethernet originali in pacchetti VXLAN, aggiungendo un header VXLAN che include il VNI. Questi pacchetti vengono poi trasportati attraverso la rete IP underlay fino al VTEP di destinazione, dove vengono decapsulati e inoltrati al segmento di rete appropriato.

Virtual Extensible LAN (VXLAN)

VXLAN è un protocollo di overlay di livello 2 altamente scalabile, progettato per isolare il traffico di utenti o gruppi di utenti in ambienti di cloud computing e reti distribuite, garantendo l'isolamento del traffico e migliorando la sicurezza.

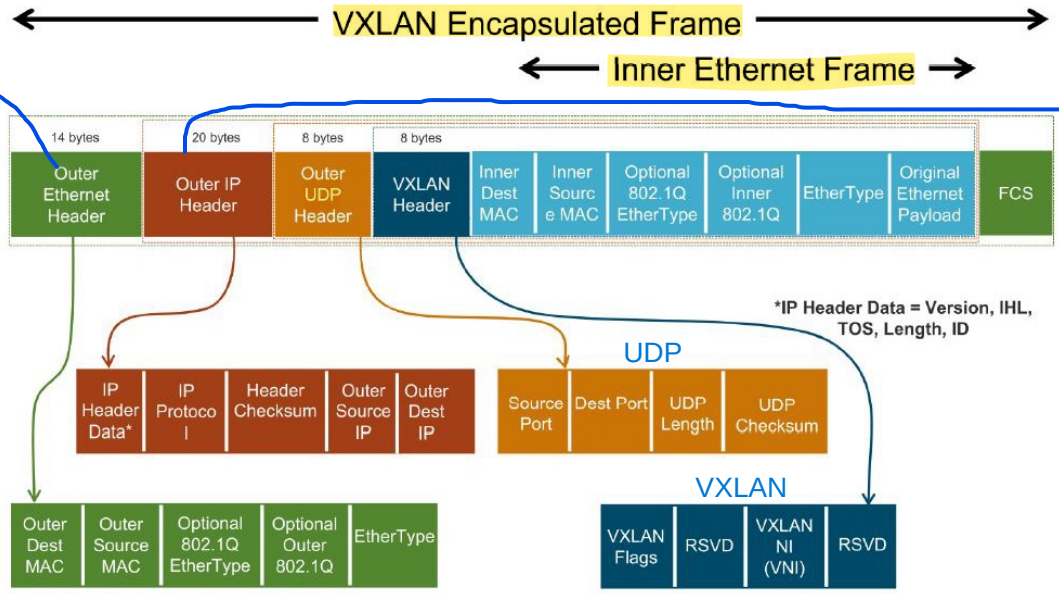
- Highly scalable distributed Layer 2 overlay network for tenant traffic isolation in could computing environments
- Encapsulation of L2 traffic in UDP packets (dest port 4789)
  - stateless tunnels between VXLAN Tunnel End Points (VTEPs)
  - each isolated L2 segment is identified by a 24-bit VXLAN Network Identifier (VNI) → 16M VNIs

VXLAN incapsula i frame Ethernet di livello 2 all'interno di pacchetti UDP di livello 4, consentendo il trasporto del traffico Ethernet su una rete IP. Questo processo è noto come incapsulamento MAC-in-UDP.

VXLAN utilizza un Identificatore di Rete Virtuale (VNI) a 24 bit, permettendo la creazione di circa 16 milioni di segmenti di rete unici.

I VTEP sono dispositivi responsabili dell'incapsulamento e del decapsulamento dei pacchetti VXLAN. Possono essere implementati su switch, router o hypervisor, facilitando la comunicazione tra segmenti di rete virtuali.

Gli indirizzi MAC di origine e destinazione nell'header Ethernet esterno vengono aggiornati a ogni hop.

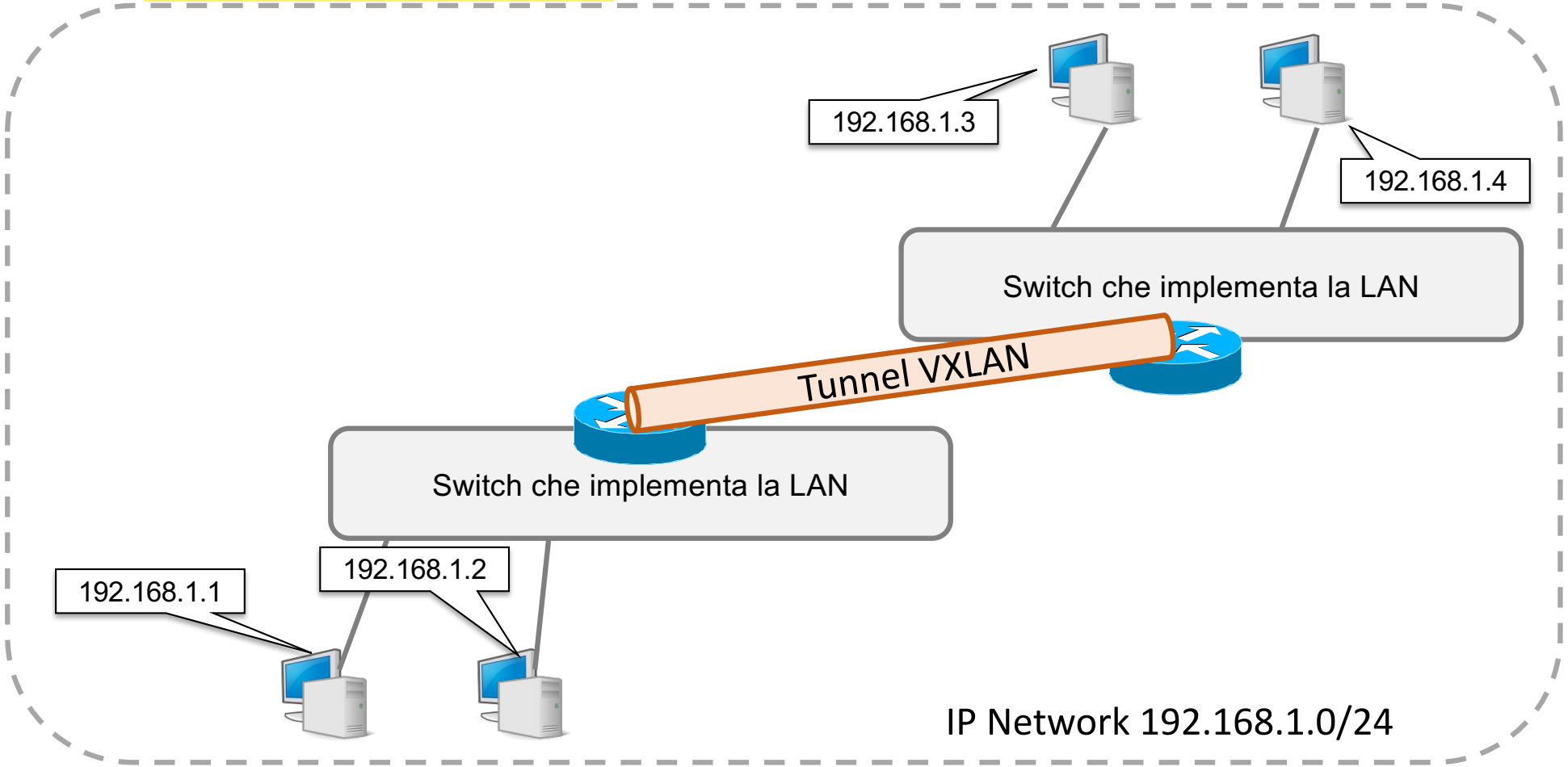


MAC di Destinazione (Outer Dest MAC): Rappresenta l'indirizzo MAC del prossimo dispositivo di rete (come uno switch o un router) nella catena di trasporto del pacchetto. Questo dispositivo può essere il primo hop verso la destinazione finale.
MAC di Origine (Outer Source MAC): Indica l'indirizzo MAC del dispositivo che invia il pacchetto, come il VTEP (VXLAN Tunnel Endpoint) che incapsula il pacchetto.

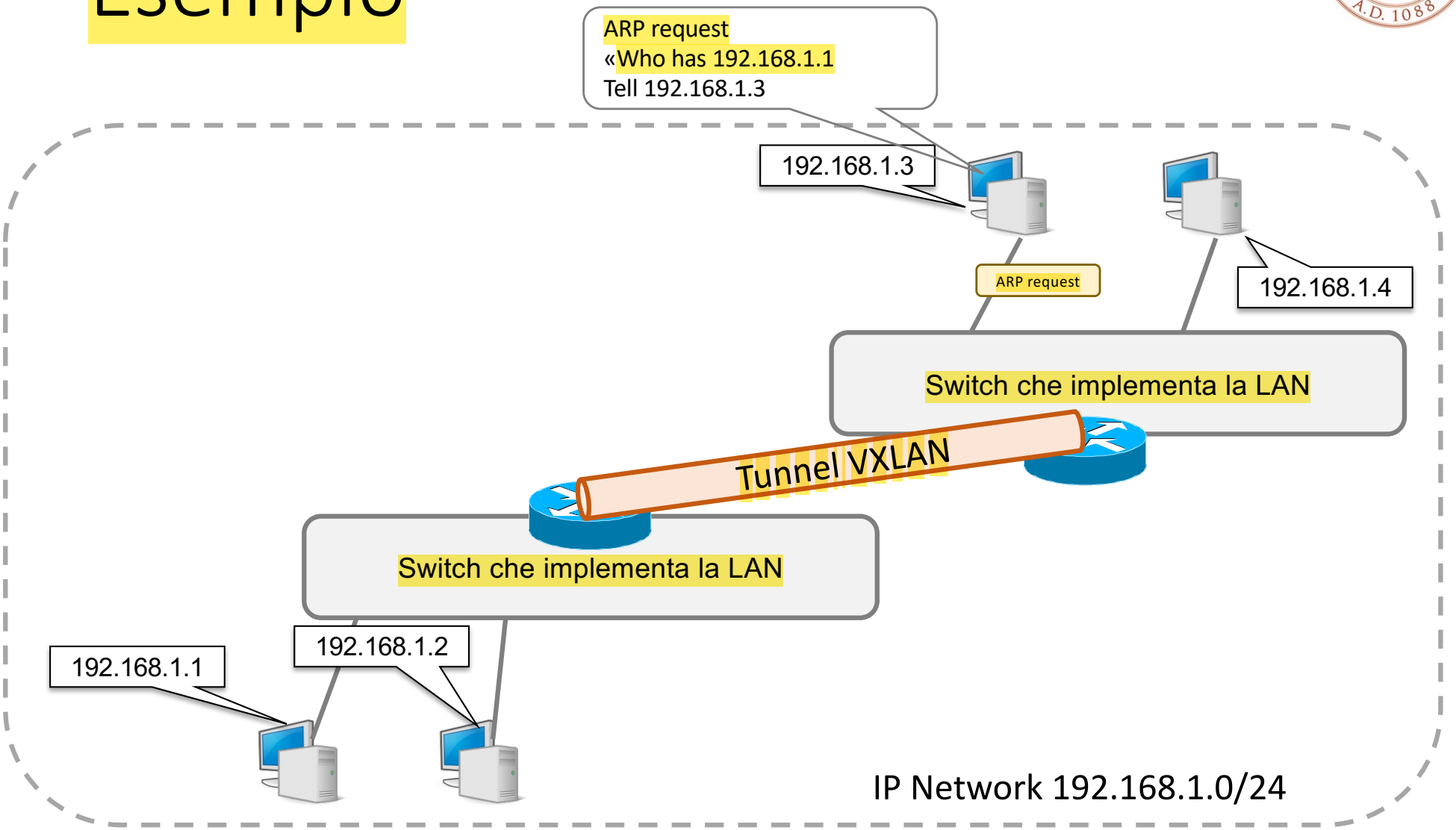
Indirizzo IP di Origine (Outer Source IP): Questo è l'indirizzo IP del dispositivo che sta incapsulando il traffico VXLAN, come un VTEP. L'indirizzo di origine è quello del punto in cui il pacchetto entra nella rete IP.
Indirizzo IP di Destinazione (Outer Dest IP): L'indirizzo IP del dispositivo VTEP di destinazione, dove il pacchetto VXLAN sarà decapsulato e inoltrato alla rete di livello 2 di destinazione. Questo indirizzo rappresenta il punto finale del tunnel VXLAN.
Sia l'indirizzo IP di origine che quello di destinazione nell'Outer IP Header di un pacchetto VXLAN non cambiano durante il transito attraverso la rete sottostante.

Applicazione di VXLAN

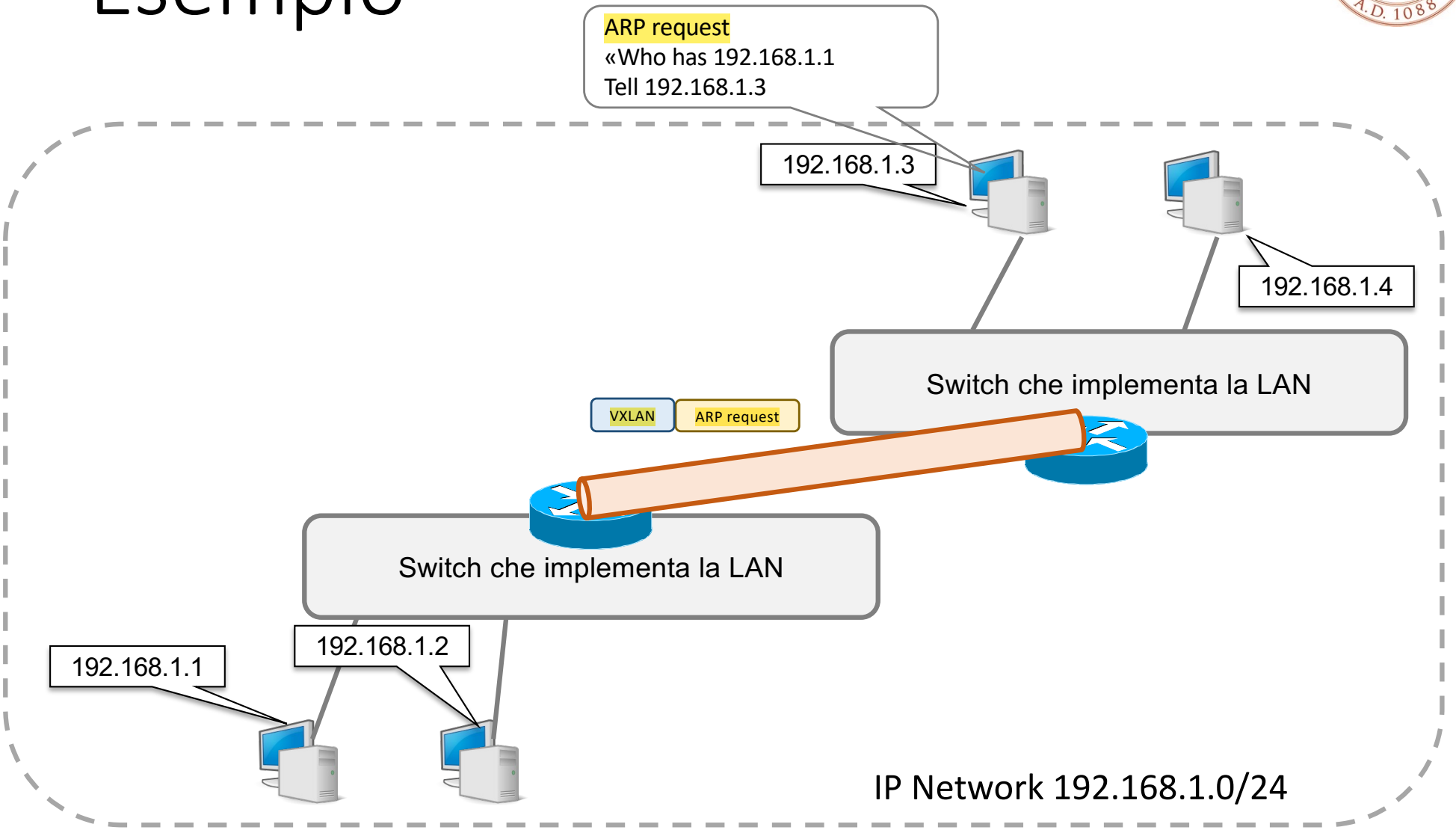
- Una sola network IP estesa sulla rete globale
- VXLAN trasporta i frame Ethernet sulla rete di interconnessione IP



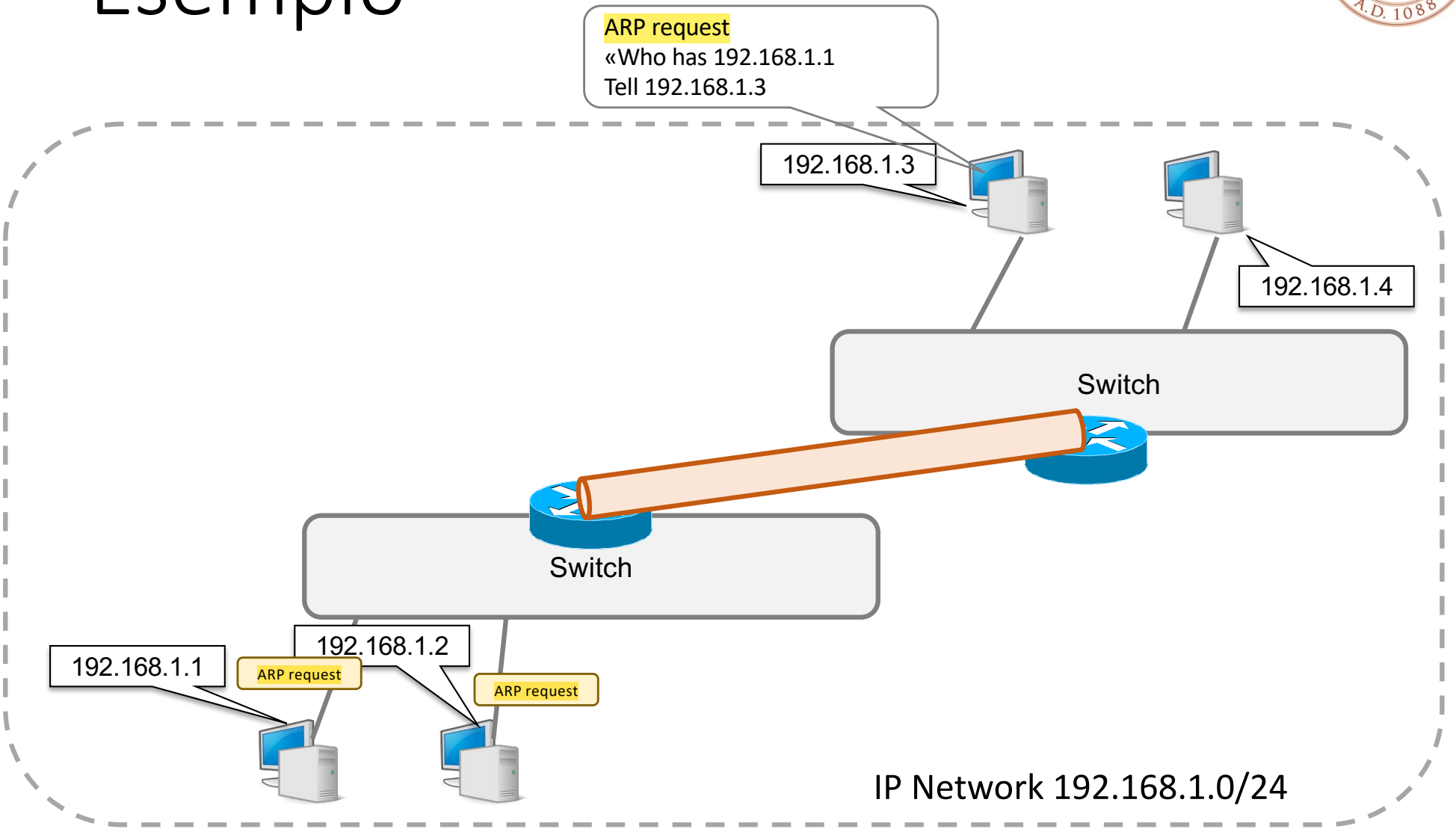
Esempio


ARP request
«Who has 192.168.1.1
Tell 192.168.1.3
192.168.1.3
ARP request
192.168.1.4
Switch che implementa la LAN
Tunnel VXLAN
Switch che implementa la LAN
192.168.1.2
192.168.1.1
IP Network 192.168.1.0/24

Esempio


ARP request
«Who has 192.168.1.1
Tell 192.168.1.3
192.168.1.3
192.168.1.4
Switch che implementa la LAN
VXLAN
ARP request
Switch che implementa la LAN
192.168.1.2
192.168.1.1
IP Network 192.168.1.0/24

Esempio


ARP request
«Who has 192.168.1.1
Tell 192.168.1.3
192.168.1.3
192.168.1.4
Switch
Switch
192.168.1.2
192.168.1.1
ARP request
ARP request
IP Network 192.168.1.0/24

In una rete, il dominio di broadcast è l'insieme di dispositivi che ricevono un pacchetto trasmesso in broadcast. Generalmente, i router separano i domini di broadcast, impedendo la propagazione dei pacchetti broadcast tra reti IP diverse. Tuttavia, esistono situazioni in cui un dominio di broadcast può estendersi su reti IP differenti:
Configurazione di router per l'inoltro di broadcast ; Utilizzo di tecnologie come VLAN e VXLAN ; Reti con indirizzamento IP non convenzionale
IN TUTTI QUESTI CASI, SI HA UN UNICO DOMINIO DI BROADCAST

Il dominio di broadcast

- Quando il dominio di broadcast è uno solo
  - Un broadcast inviato da un calcolatore a tutti gli altri calcolatori della LAN
  - Anche se su reti IP diverse
- Questo rappresenta un doppio problema
  - *Prestazioni*: i pacchetti broadcast utilizzano capacità di rete, più ce ne sono minore è la capacità per il traffico rimanente

    I pacchetti broadcast utilizzano risorse della rete, perché vengono inviati a tutti i dispositivi all'interno del dominio di broadcast.
  - *Sicurezza*: i pacchetti broadcast possono essere utilizzati per studiare la topologia di rete e/o per tentare attacchi alla sicurezza della rete stessa

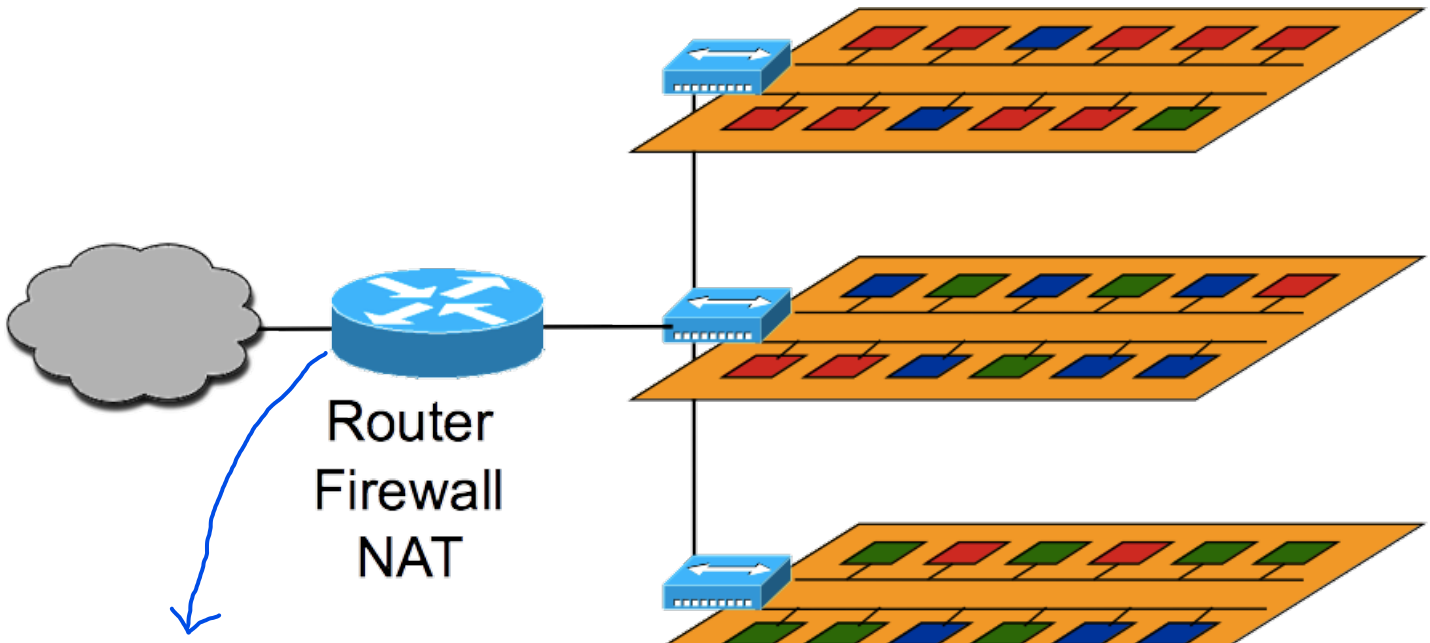
    I pacchetti broadcast possono essere utilizzati da attaccanti per studiare la topologia della rete, ovvero la struttura della rete stessa, inclusi i dispositivi connessi e i loro indirizzi.

È consigliato sempre assegnare subnet IP distinte a VLAN diverse

Virtual LAN (VLAN)

- Un solo switch
- Più LAN separate
  - Ogni VLAN rappresenta un diverso dominio di broadcast
  - Se facciamo coincidere le network IP con le VLAN i broadcast di una network non raggiungono gli host di un'altra

- Senza un indirizzo IP associato, i dispositivi in VLAN diverse non potranno comunicare in alcun modo.
- Se host di VLAN diverse ma stessa rete IP, non possono comunicare direttamente



192.168.8.0/24
192.168.9.0/24
192.168.10.0/23

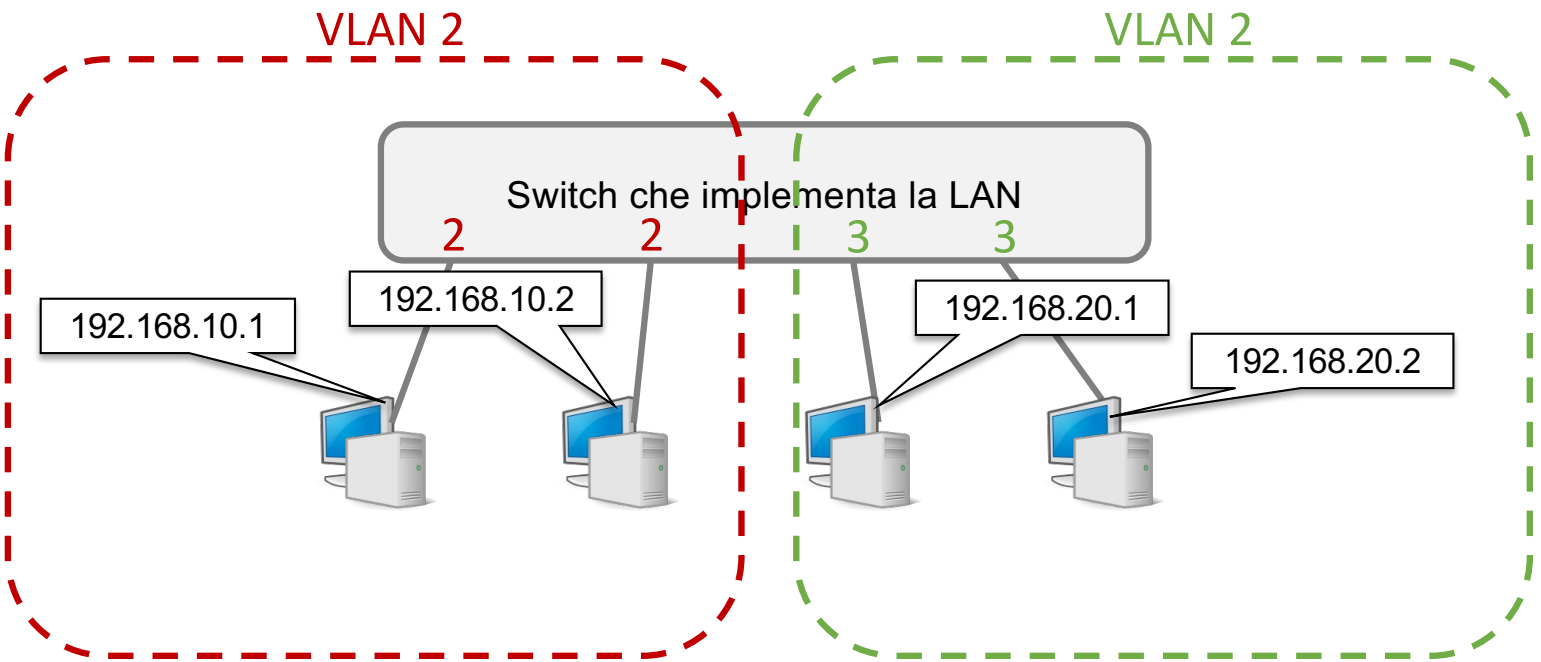
Il router gestisce il traffico tra VLAN differenti e tra VLAN e il resto della rete.

Classificazione delle VLAN

- VLAN statiche o port-based
  - ogni porta dello switch è associata ad una VLAN
  - un host appartiene alla VLAN corrispondente alla porta a cui è connesso
  - per spostare un host su una diversa VLAN occorre intervenire sullo switch e modificare la VLAN a cui è associata la porta a cui l'host è connesso
- VLAN dinamiche
  - l'appartenenza alle VLAN è stabilita in base all'indirizzo dell'host
    - MAC-based
    - IP-based
  - un host appartiene alla corrispondente VLAN indipendentemente dalla porta a cui è connesso
  - per spostare un host su una diversa VLAN occorre intervenire sullo switch e modificare la VLAN associata all'indirizzo dell'host
- Normalmente VLAN statiche

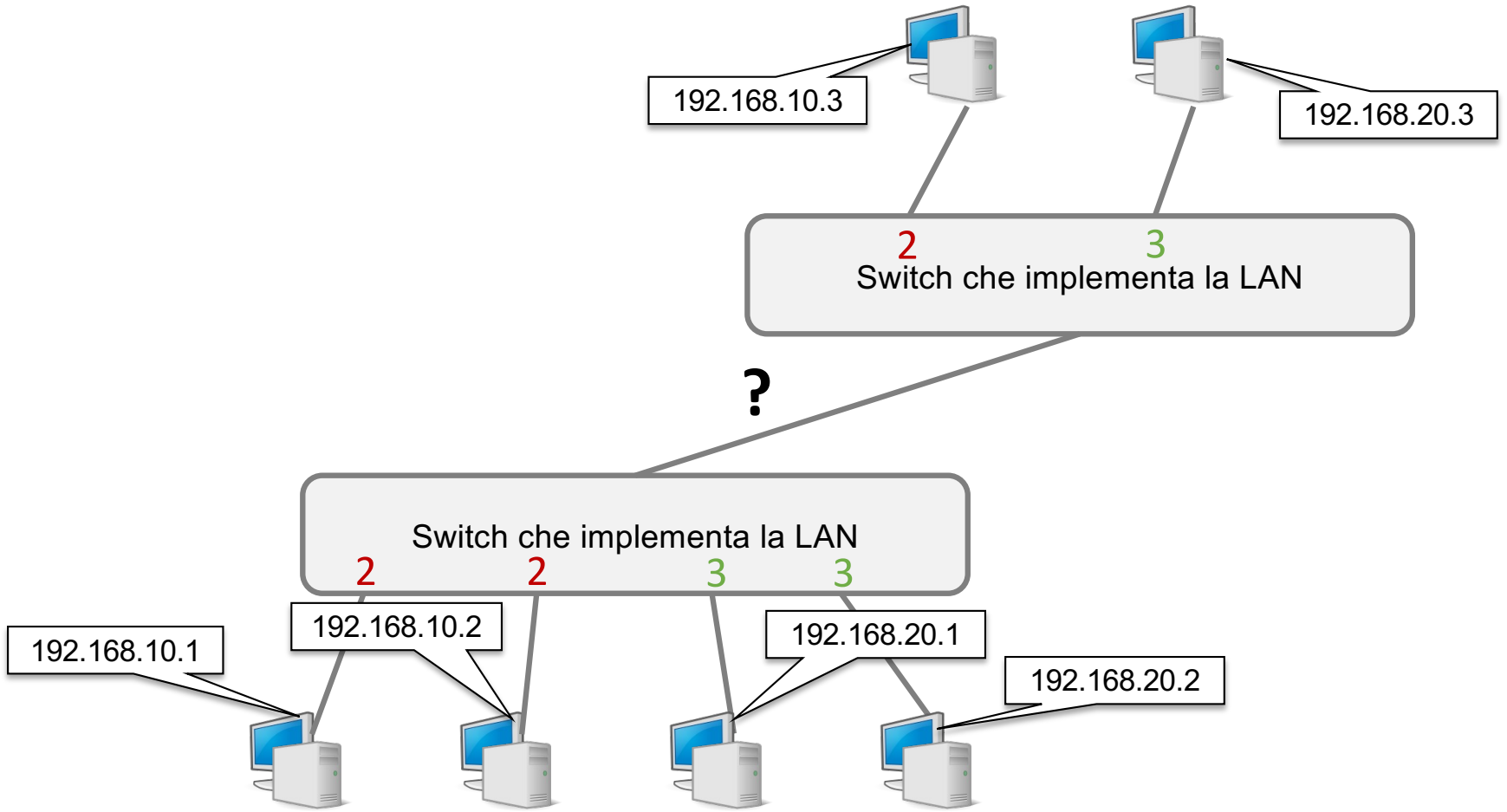
VLAN statica

- Lo switch conosce la VLAN di appartenenza di un host in base alla configurazione della porta a cui è connesso



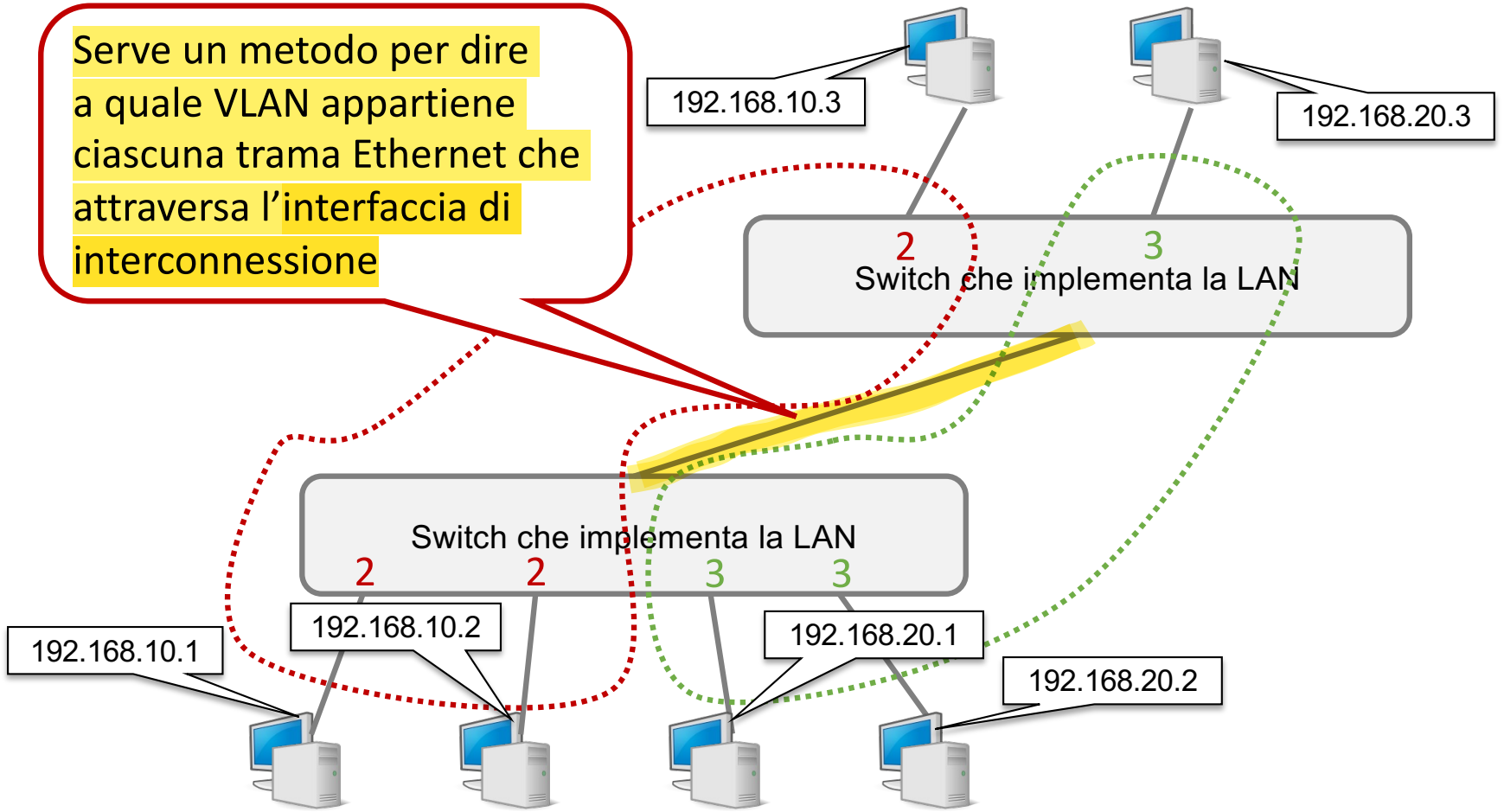
LAN estesa

- Se una LAN è realizzata con più di uno switch come posso gestire le VLAN inter-switch?



LAN estesa

- Se una LAN è realizzata con più di uno switch come posso gestire le VLAN inter-switch?



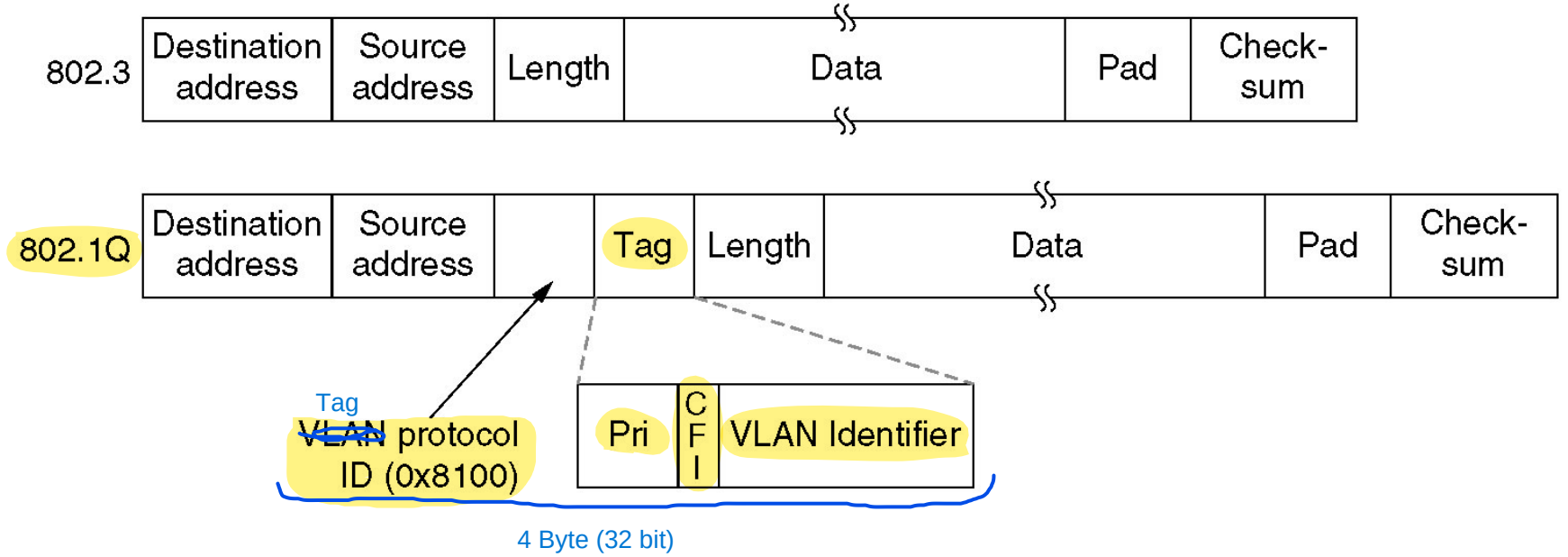
è uno standard IEEE 802.x

IEEE 802.1Q

- Protocollo che permette l'utilizzo delle stesse VLAN su diversi switch interconnessi tra loro

Serve per dire a quale VLAN appartiene ciascuna trama Ethernet che attraversa l'interfaccia di interconnessione

- Occorre specificare a quale VLAN appartiene una trama inviata ad un altro switch
- Etichetta (tag) nell'intestazione Ethernet



Da A.S. Tanenbaum "Reti di Calcolatori, 4 ed."

IEEE 802.1Q header format

- 4 bytes
- Tag Protocol Identifier (TPID) Identifica il frame come appartenente a una VLAN
  - 16 bit
  - Usually 0x8100
- Priority Permette di assegnare una priorità al traffico
  - 3 bit
- CFI
  - 1 bit
  - Identifica il formato del MAC address
- Unique LAN Identifier (VID) Identifica la VLAN specifica a cui appartiene il frame
  - 12 bits
  - Numero della VLAN (da 0 a 4095)

Porte dello switch

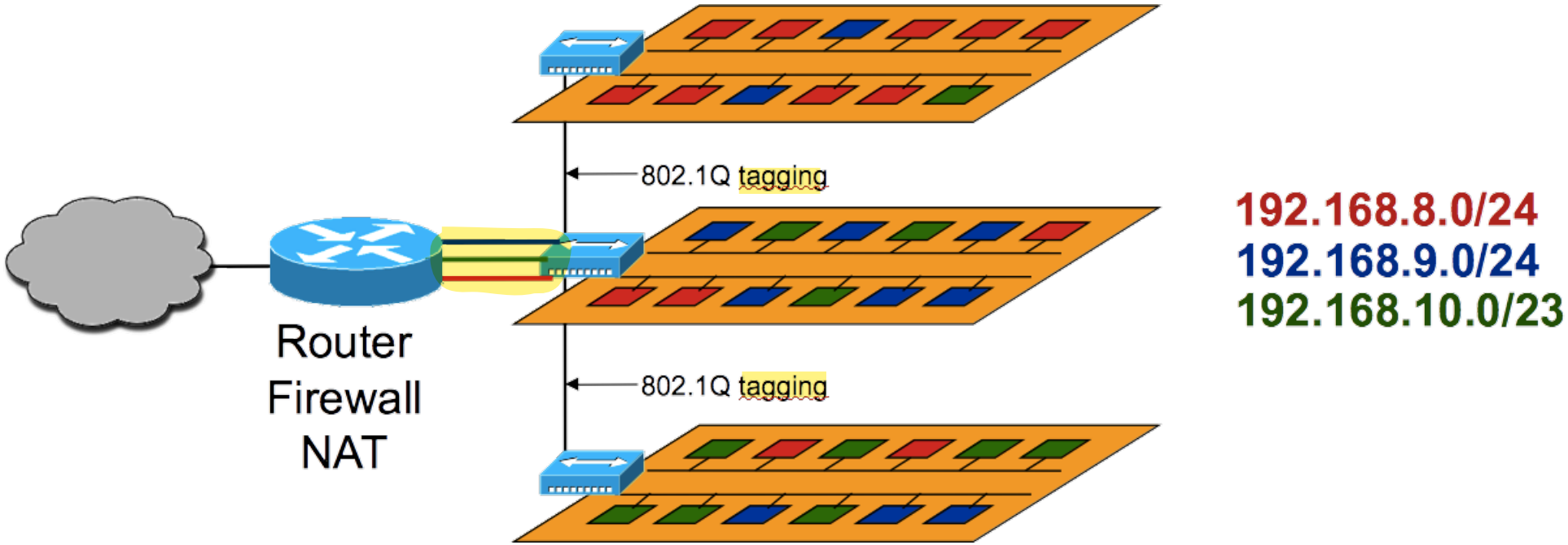
- Access mode
  - porta associata ad una sola VLAN
  - tagging 802.1Q non necessario
  - modalità tipica per porte connesse agli hosts (cioé ad una porta collego un calcolatore)

- Trunk mode
  - porta associata a VLAN multiple
  - tagging 802.1Q necessario per determinare la VLAN a cui appartiene ciascun frame Ethernet
  - una porta trunk può essere associata contemporaneamente a una sola VLAN “untagged” e a più VLAN “tagged”
  - modalità tipica per porte connesse a switch e router

(cioé ad una porta collego piú di un calcolatore tramite switch)

Inter-VLAN routing

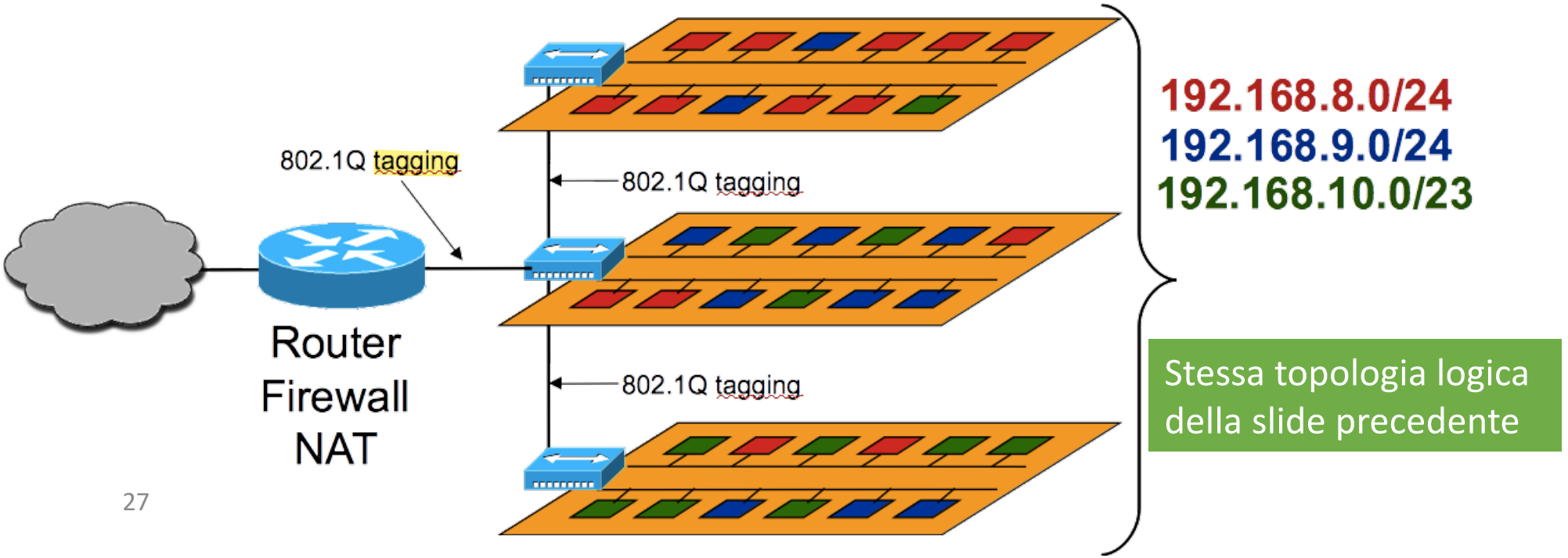
- In teoria un router dovrebbe avere un'interfaccia dedicata a ciascuna VLAN
- Soluzione inefficiente e poco scalabile
  - n VLAN richiedono l'uso di n interfacce sul router e n porte sullo switch



sub-interfaccia e interfaccia virtuale sono sinonimi

Inter-VLAN routing

- Più efficiente e scalabile l'utilizzo di interfacce virtuali, o sub-interfacce
  - unica interfaccia fisica compatibile con il tagging 802.1Q
  - n interfacce virtuali sulla stessa interfaccia fisica
  - ogni sub-interfaccia utilizza il VLAN ID corrispondente alla sua VLAN



Reti private e reti private virtuali

- Aziende e/o enti di dimensioni medio/grandi in genere hanno necessità di interconnettere in maniera sicura sedi sparse sul territorio e distanti tra loro

Reti private fisiche

- Soluzione tradizionale: utilizzo di linee dedicate da affittare direttamente presso gli operatori (**reti private**)
  - Implica costi di acquisto e di gestione dedicati

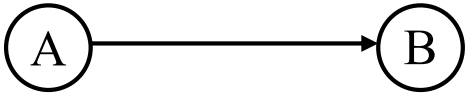
Reti private virtuali

- Alternativa: utilizzo di una rete in "overlay" attraverso reti pubbliche (**reti private virtuali - VPN**)
  - flusso punto-punto di pacchetti autenticati (con contenuto informativo criptato) incapsulati in pacchetti tradizionali
  - diverse tecnologie disponibili
  - Diversi protocolli di tunnelling
    - livello 2: PPTP, L2TP
    - livello 3: IPsec

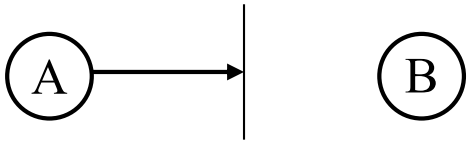
La VPN utilizza diversi protocolli di tunneling per garantire che i dati siano protetti durante il trasferimento

Le reti private fisiche sono più sicure e più stabili ma anche più costose e difficili da gestire.
Le VPN sono più economiche e facili da implementare perché utilizzano reti pubbliche esistenti, ma richiedono l'uso di tecnologie di crittografia e tunneling per garantire la sicurezza e la protezione dei dati.

I rischi della comunicazione remota



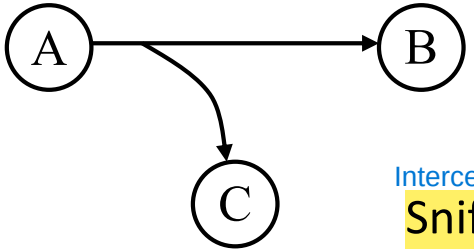
Normal information flow



Interruzione

Blocking

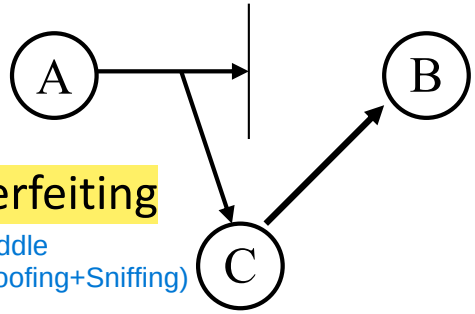
dove l'attaccante sovraccarica un sistema o una rete con traffico eccessivo, rendendo i servizi inaccessibili agli utenti legittimi.



Intercettazione

Sniffing

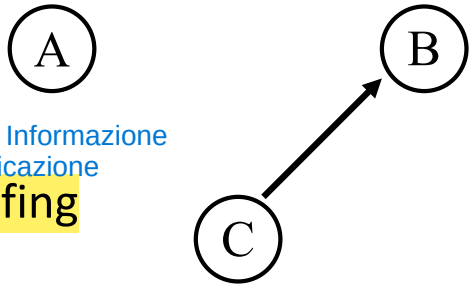
per intercettare e analizzare il traffico di rete.



Counterfeiting

Man in the Middle
(Blocking+Spoofing+Sniffing)

si inserisce furtivamente nella comunicazione tra due parti, intercettando e potenzialmente alterando le informazioni scambiate.



Creazione Informazione
e Personificazione

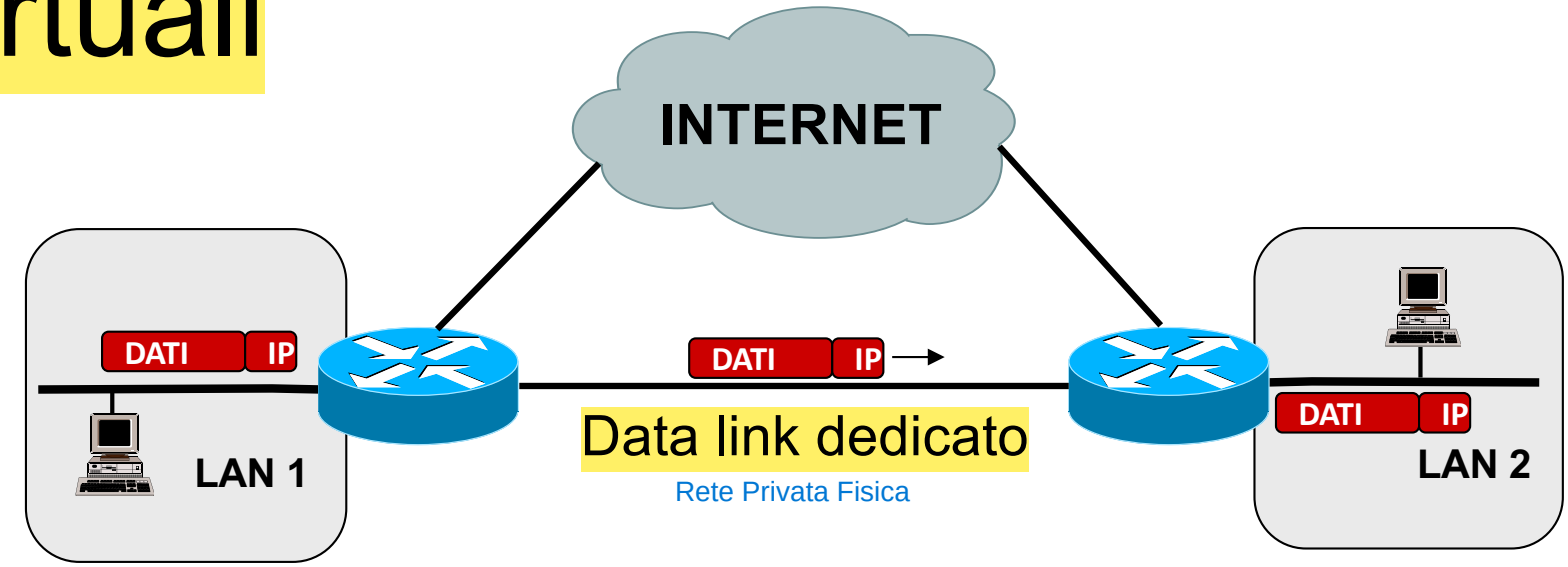
Spoofing

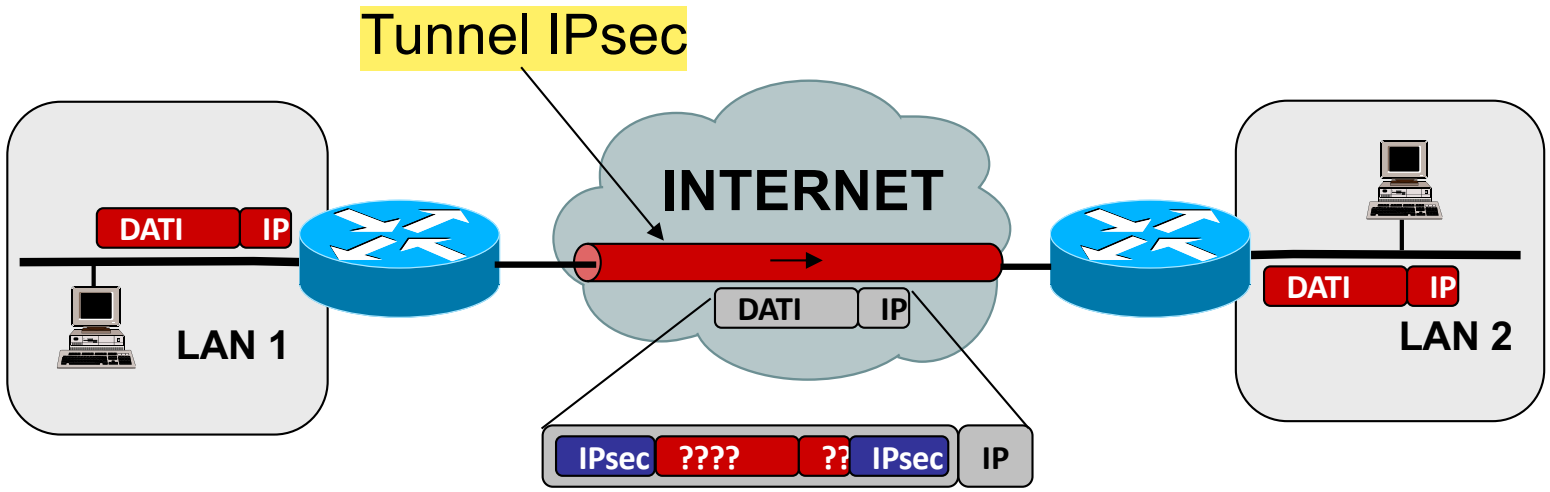
per ingannare le vittime e ottenere accesso non autorizzato a sistemi o informazioni.

Obiettivi di una rete privata

- Riservatezza
  - Le informazioni non sono leggibili da tutti ma solo dagli utenti autorizzati (Questo implica l'uso di tecniche come la crittografia).
- Autorizzazione
  - Definisco il sottoinsieme di coloro che sono in grado di leggere i dati (cioè indico quali dati possono essere letti, modificati o cancellati da un utente).
- Autenticazione
  - Verifico l'identità di chi sta leggendo i dati (cioè assicura che un utente o dispositivo sia effettivamente chi dice di essere).
- Paternità
  - Garantisco l'origine dei dati cioè sapere chi ha creato o inviato una determinata informazione.

Reti private reali e reti private virtuali





Su rete pubblica i pacchetti vengono cifrati
Su rete pubblica l'indirizzamento reale può essere mascherato

1

VPN Roadwarrior

La configurazione Roadwarrior è ideale per utenti remoti (ad esempio dipendenti in smart working) che necessitano di accedere in modo sicuro alle risorse aziendali.

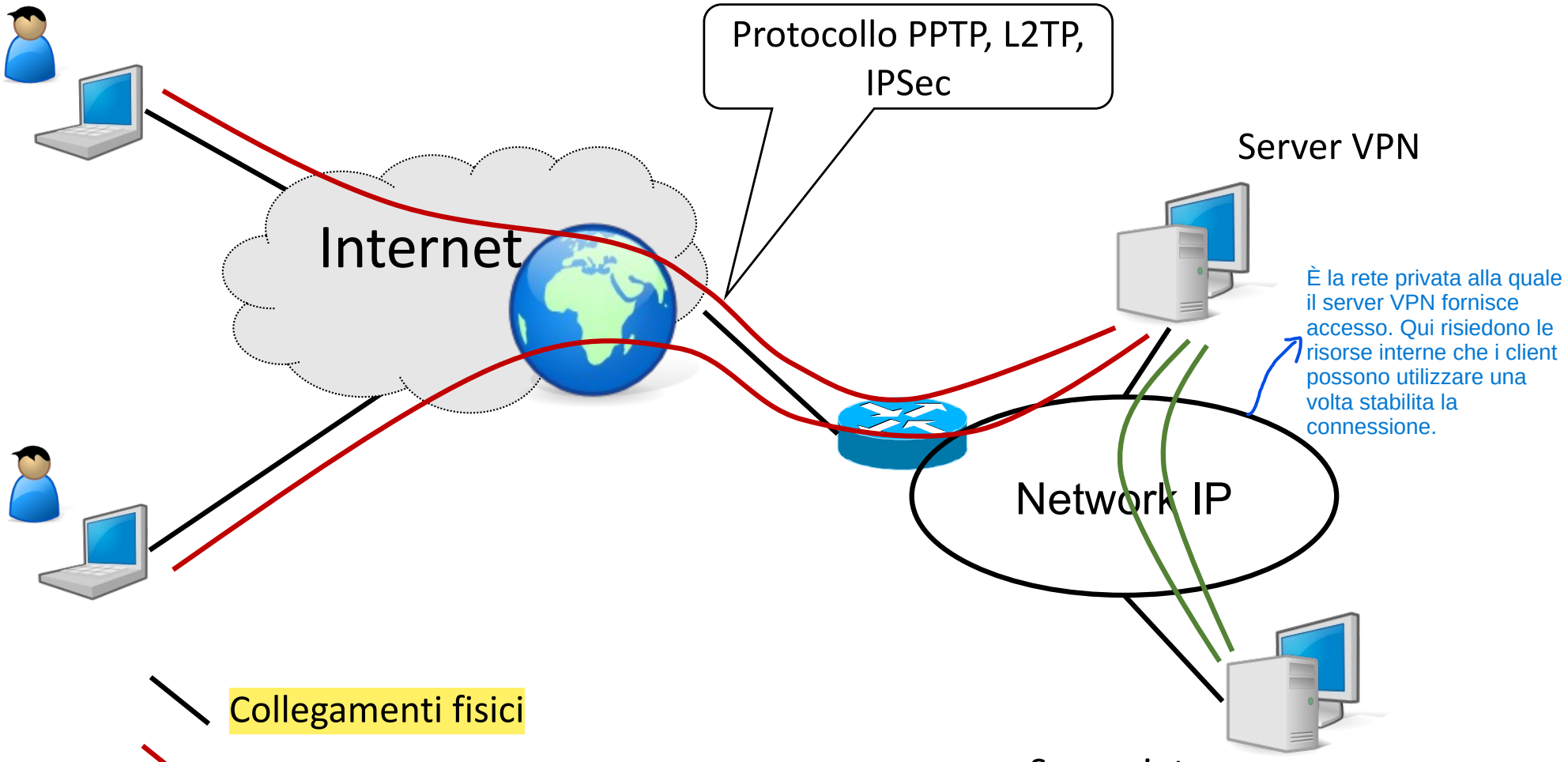
- Su una network viene configurato un server VPN
- Tutti i client si collegano a quel server da un punto qualunque di Internet
  - Tunnel sicuri punto-punto
- Topologia a stella

Il server VPN è al centro, mentre tutti i client che si collegano rappresentano i punti finali della stella.

- Si configura come una rete di comunicazioni sicure sul server VPN

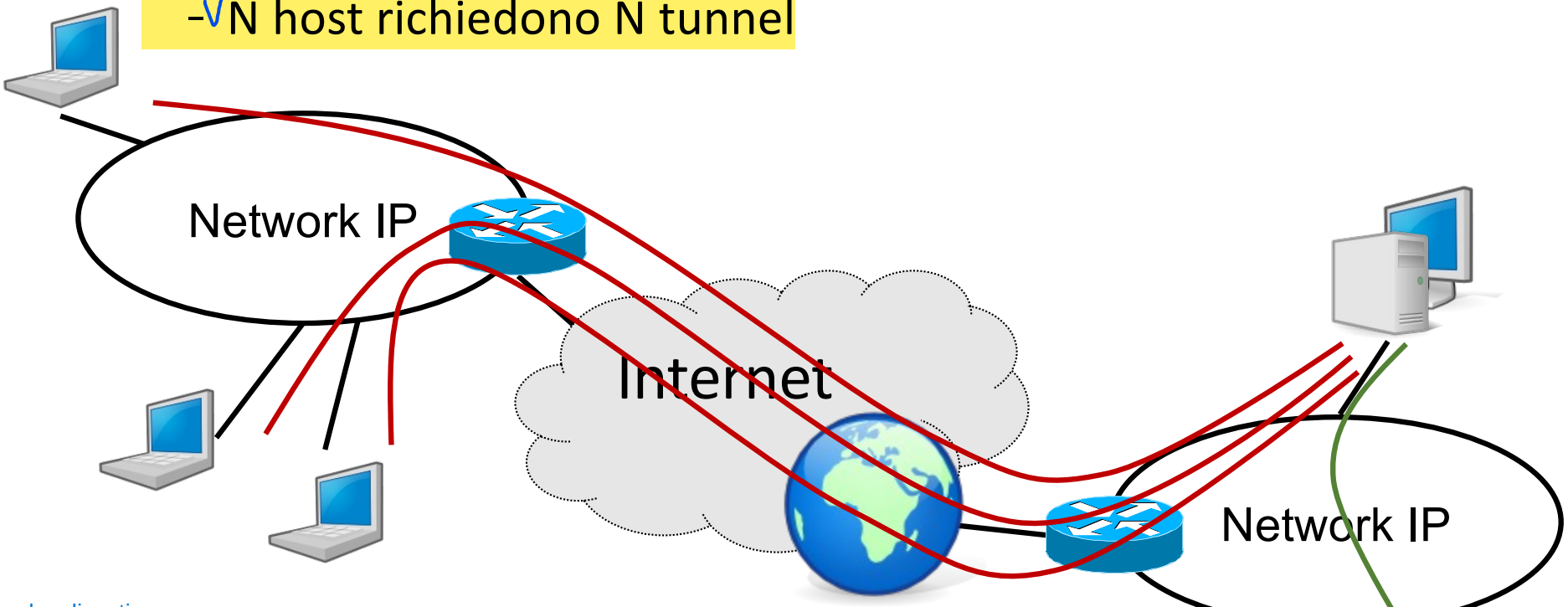
Roadwarrior

Una VPN Roadwarrior è una configurazione di tipo molti a uno. Il server può essere un dispositivo dedicato o un router configurato per gestire anche le funzionalità di server VPN.



Problema

- Se ho molti host co-localizzati il rodawarrior è inefficiente
  - poiché √N host richiedono N tunnel



Molti host co-localizzati:
Gli host si trovano nella stessa rete locale (Network IP) e hanno bisogno di accedere a risorse attraverso un server VPN.

Richiesta inefficiente di tunnel:
Ogni host deve stabilire il proprio tunnel VPN con il server remoto.
Questo comporta che per N host, sono necessari N tunnel VPN.

Impatto sull'efficienza:
Ogni tunnel VPN consuma risorse sia lato client che lato server (es. CPU per crittografia e decrittografia, larghezza di banda, ecc.).
Questa configurazione è inefficiente se molti host co-localizzati devono accedere alla stessa destinazione tramite la VPN.

2 VPN da rete a rete

Differenze rispetto alla VPN Roadwarrior:
Nella VPN da rete a rete, il tunnel viene stabilito tra i dispositivi di rete (come router o gateway), non tra singoli client.
Gli utenti nelle reti collegate non necessitano di software VPN specifico, poiché il tunnel è gestito a livello di rete.

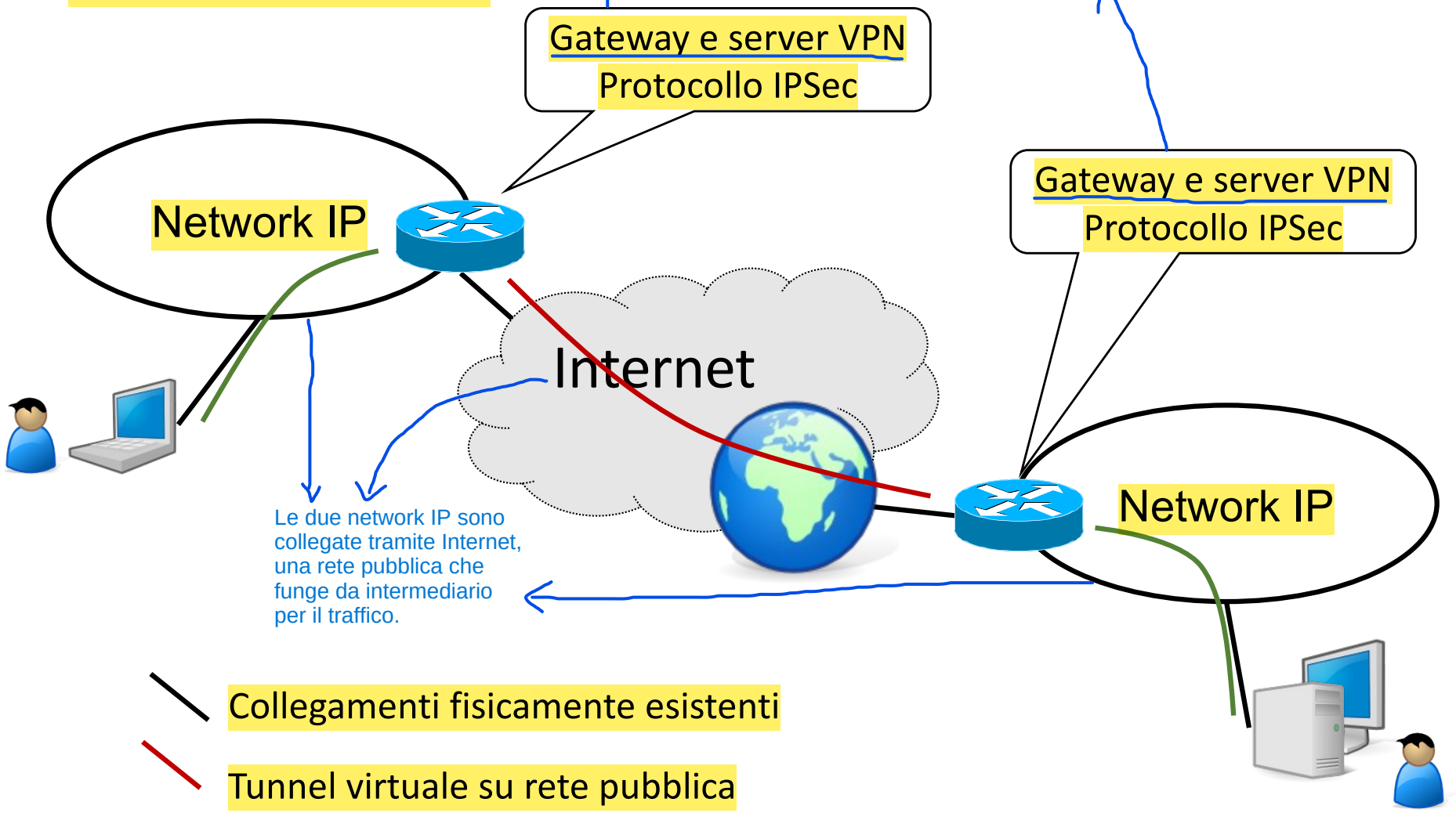
- Si crea un tunnel cifrato su rete pubblica fra due LAN o fra due network IP
  - Su rete pubblica i pacchetti vengono cifrati garantendo la riservatezza e impedendo intercettazioni da parte di terzi.
  - Su rete pubblica l'indirizzamento reale può essere mascherato → proteggendo ulteriormente l'identità e la posizione dei dispositivi collegati.

- Normalmente i server VPN vengono co-localizzati con i gateway delle network

Co-localizzare i server VPN con i gateway di rete significa integrare le funzionalità di entrambi in un unico punto, ottimizzando l'efficienza, la sicurezza e la gestione della rete. Un gateway di rete IP può svolgere contemporaneamente le funzioni di router e server VPN.

2 Net-to-Net

Ogni rete ha un router che agisce sia da Gateway che da Server VPN. Questo dispositivo:
Gestisce l'instradamento del traffico tra la rete locale e Internet.
Stabilisce e mantiene il tunnel VPN con l'altra rete.
Utilizza un protocollo sicuro come IPSec per crittografare il traffico.



Collegamenti fisicamente esistenti

Tunnel virtuale su rete pubblica

Instradamento indiretto su rete privata

IPSec

SA (Security Association):
Una Security Association è una relazione unidirezionale tra un mittente e un destinatario, che definisce come proteggere i dati durante la trasmissione (definisce i parametri di sicurezza utilizzati per proteggere la comunicazione).
Ogni SA è caratterizzata da:
Security Parameter Index (SPI): Un identificatore univoco per la SA.
IP Destination Address: L'indirizzo IP del destinatario a cui i pacchetti devono essere inviati.
Security Protocol Identifier: Specifica quale protocollo di sicurezza viene utilizzato.

- IPSec documents:
  - RFC 2401: An overview of security architecture
  - RFC 2402: Description of a packet encryption extension to IPv4/IPv6
  - RFC 2406: Description of a packet emcryption extension to IPv4/IPv6
  - RFC 2408: Specification of key managament capabilities
- Concetti base
  - SA (Security Association) relazione unidirezionale tra mittente e destinatario, definita da
    - Security Parameter Index (SPI)
    - IP Destination address
    - Security Protocol Identifier
  - Due modalità possibili di SA
    - Transport Mode
    - Tunnel Mode

Modalità possibili di SA:
Esistono due modalità operative per l'uso di una SA in IPSec:

- Transport Mode:
In questa modalità, solo il payload (cioè i dati) del pacchetto IP è crittografato e/o autenticato.
L'intestazione IP originale rimane intatta.
È più adatta per comunicazioni end-to-end (ad esempio, tra due dispositivi) (VPN Roadwarrior).

- Tunnel Mode:
In questa modalità, l'intero pacchetto IP è incapsulato in un nuovo pacchetto e crittografato.
Viene aggiunta una nuova intestazione IP per il trasporto.
È comunemente usata per connessioni tra due reti (VPN site-to-site).

Protocolli utilizzati in IPSec

Utilizzato per creare connessioni VPN sicure negoziando automaticamente i parametri di sicurezza.

- **IKE (Internet Key Exchange):**
  - autenticazione interlocutore → IKE verifica che entrambe le parti coinvolte nella comunicazione siano autentiche e autorizzate.
  - negoziazione algoritmi e chiavi crittografiche → necessarie per la crittografia e l'autenticazione.
    - Utilizza UDP (porta sorgente e destinazione = 500)

Usato in scenari dove l'integrità dei dati è più importante della confidenzialità (non crittografa i dati)

- **AH (Authentication Header) (campo protocol IP = 51):** → AH non fornisce la crittografia del payload, quindi i dati rimangono leggibili durante il transito (non garantisce la confidenzialità).
  - autenticazione dei pacchetti trasmessi in VPN garantendo
    - integrità ed autenticità dei dati (assicurando che non siano stati modificati durante il transito)
    - identità del mittente → (Conferma l'identità del mittente) (L'identità del mittente può essere confermata in IPSec utilizzando certificati digitali con firma digitale)

Usato principalmente nelle VPN per proteggere completamente i dati trasmessi su Internet

- **ESP (Encapsulating Security Payload) (campo protocol IP = 50):**
  - come in AH + riservatezza delle informazioni tramite crittografia

Fornisce le stesse funzionalità di AH (integrità e autenticità dei dati) ed inoltre garantisce la riservatezza delle informazioni tramite crittografia, rendendo i dati illeggibili a chiunque non abbia le chiavi corrette.

Transport Mode: Solo il payload del pacchetto IP viene crittografato.
Tunnel Mode: L'intero pacchetto IP (intestazione + payload) viene incapsulato in un nuovo pacchetto con una nuova intestazione IP.

IKE

Essendo che, con IKE, si fa apertura connessione su UDP su porta 500, il problema nasce se ci sono NAT nel percorso, perché il ricevente aspetta solo su porta 500 ed il nat al passaggio, se ci sono piú comunicazioni IPSEC contemporaneamente, cambia la porta e non funziona piú

Stabilisce un canale sicuro preliminare (SA ISAKMP) tra i due nodi VPN. Questo canale serve per proteggere la negoziazione successiva della connessione vera e propria.

Fase 1 – Negoziazione preliminare

- uno dei due nodi VPN (initiator) tenta di contattare l'altro
- i due nodi si accordano sui parametri di sicurezza da usare in questa fase (cioé nella Fase 2 di IKE)

Una volta completata la Fase 1, viene stabilita una connessione sicura preliminare, che protegge la successiva negoziazione della connessione vera e propria.

preliminari, che servono per creare la connessione iniziale sicura,

(nella fase 1, i parametri di sicurezza sono preliminari e servono solo per proteggere la fase successiva)

Stabilire i dettagli della connessione IPSec vera e propria, incluse le Security Associations e le chiavi crittografiche.

Fase 2 – Negoziazione della connessione

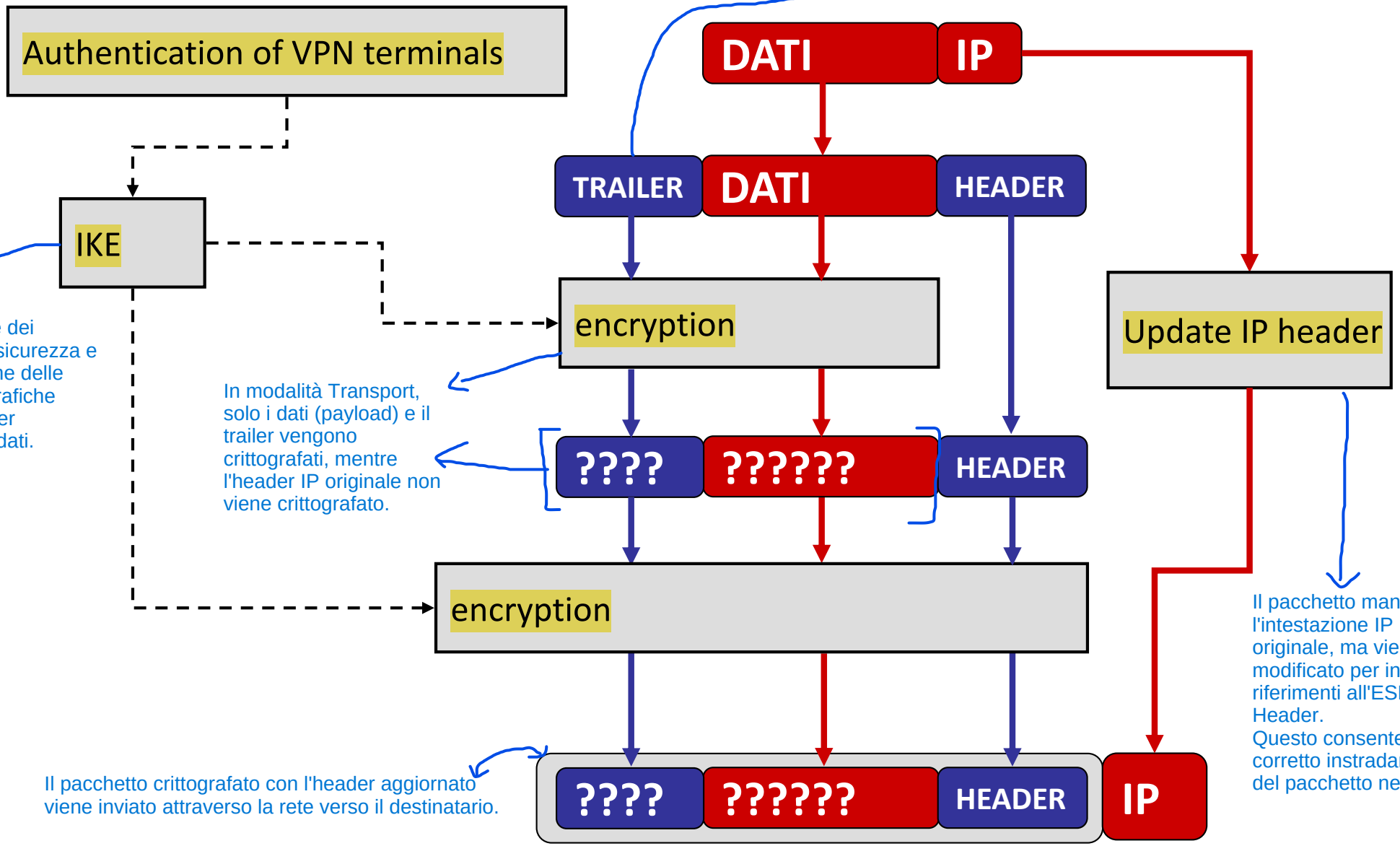
- i due nodi VPN si accordano sui parametri di sicurezza e sulla modalità di comunicazione
- si generano e si rinnovano le chiavi crittografiche

Le chiavi crittografiche vengono generate e aggiornate periodicamente per garantire la sicurezza nel tempo (evitando attacchi di lunga durata).

I due nodi si accordano su:
Quali protocolli utilizzare (ESP o AH).
Algoritmi e chiavi crittografiche per proteggere il traffico.
I tempi di validità delle chiavi e delle SA.

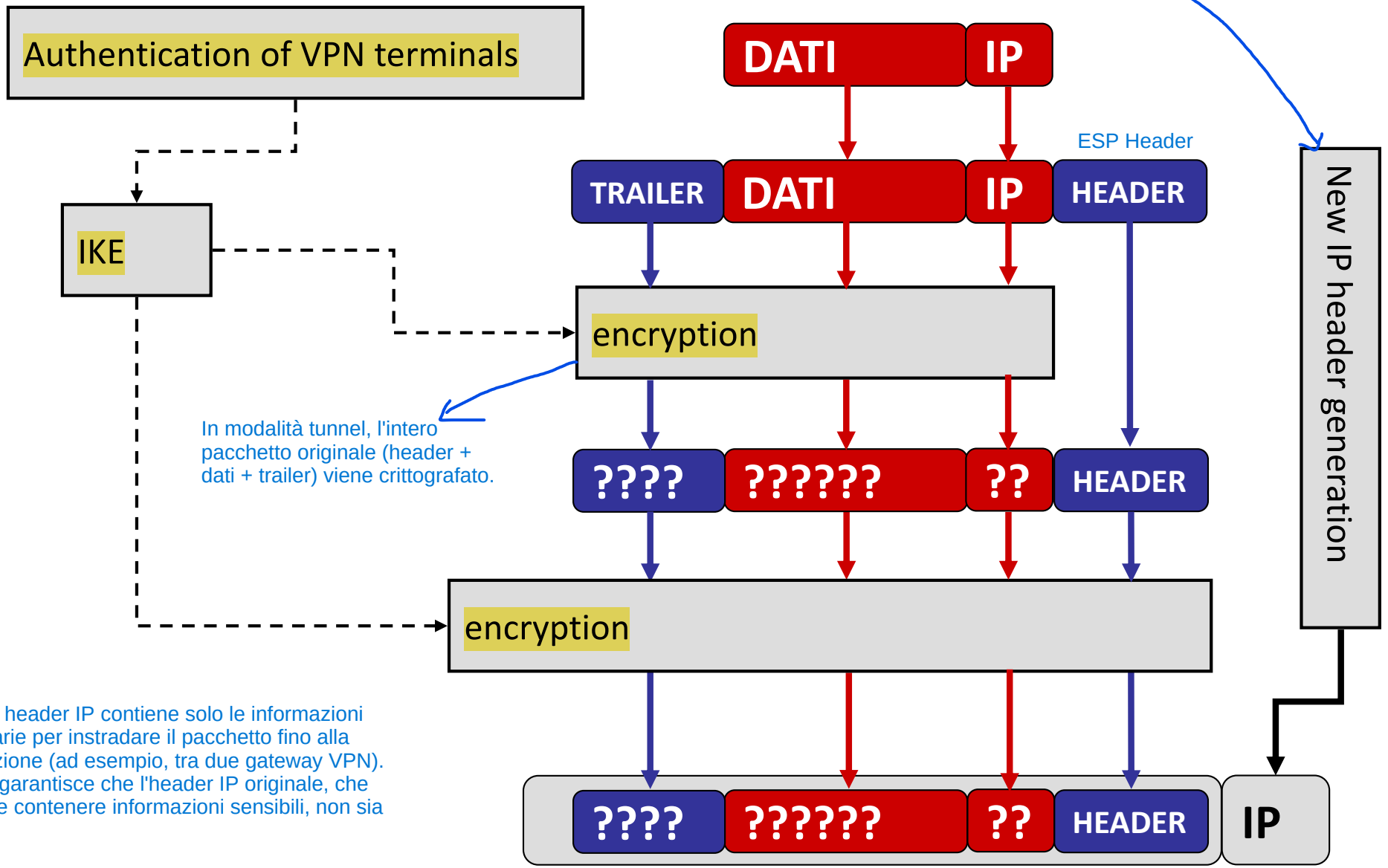
Viene creato un canale sicuro IPSec per il trasferimento dei dati.

IPsec: ESP Transport



IPsec: ESP Tunnel

Una nuova intestazione IP viene creata e posizionata davanti al pacchetto ESP. Questa intestazione consente di instradare il pacchetto crittografato fino alla sua destinazione (ad esempio, il gateway remoto o il dispositivo di destinazione).



In modalità tunnel, l'intero pacchetto originale (header + dati + trailer) viene crittografato.

Il nuovo header IP contiene solo le informazioni necessarie per instradare il pacchetto fino alla destinazione (ad esempio, tra due gateway VPN). Questo garantisce che l'header IP originale, che potrebbe contenere informazioni sensibili, non sia visibile.

ESP: tunnel vs transport