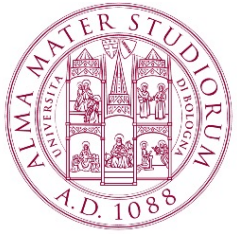


ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Virtualizzazione di rete

Franco CALLEGATI

Dipartimento di Informatica: Scienza e Ingegneria

Virtualizzazione

La virtualizzazione è un processo che permette di creare versioni "virtuali" di risorse fisiche come sistemi di calcolo, sistemi di memorizzazione e reti. Attraverso la virtualizzazione, è possibile simulare l'esistenza di queste risorse all'interno di un ambiente software, permettendo loro di operare in maniera indipendente rispetto all'hardware su cui sono installate.

- 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

In pratica, anche se il sistema sembra operare come un'unità autonoma, non ha bisogno di essere legato strettamente a una specifica risorsa fisica: questo aumenta la flessibilità e l'efficienza nella gestione delle risorse.

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
  - Sicurezza e privacy

Sistemi distinti condividono lo stesso hardware fisico. Se l'isolamento tra questi sistemi virtuali non è adeguato, problemi in un sistema potrebbero influire sugli altri.

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 virtualizzati da una macchina fisica all'altra, favorendo il miglioramento e la continuità operativa.

Virtualizzazione di rete

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

- 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

Le reti fisiche, soprattutto quelle su vasta scala o distribuite geograficamente, non sono facilmente modificabili o adattabili alle richieste dinamiche. Cambiare la configurazione di una rete fisica può richiedere interventi complessi, lunghi e costosi.

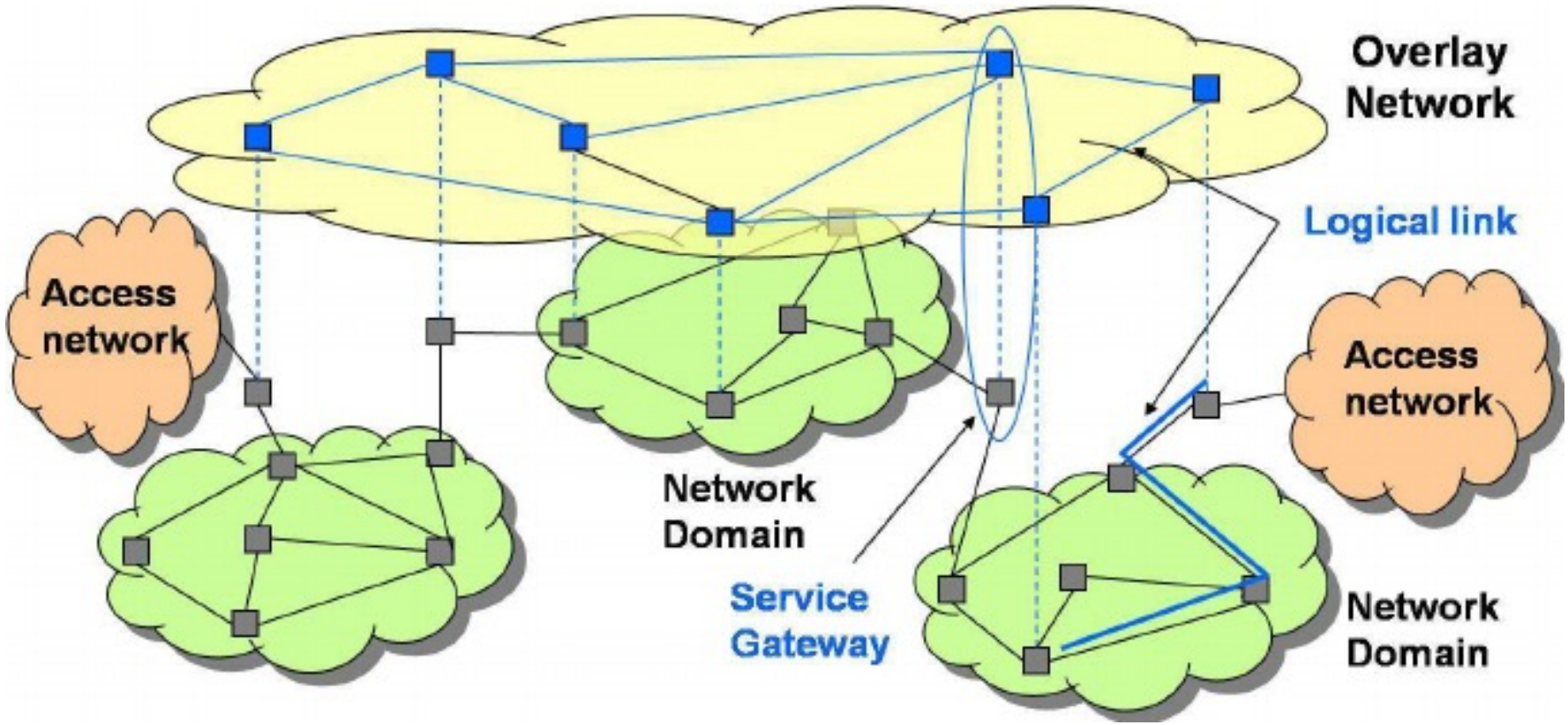
Gli utenti oggi richiedono servizi più complessi e personalizzati, con necessità di risorse di rete che possano adattarsi velocemente. Questo porta a un aumento della complessità nella gestione e configurazione delle reti.

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

L'obiettivo principale della virtualizzazione di rete è quello di realizzare topologie o funzionalità di rete virtuali che possano essere implementate sull'infrastruttura fisica esistente, senza bisogno di modifiche hardware. Questo consente di avere reti che operano in maniera distinta rispetto alla rete fisica sottostante, offrendo funzionalità aggiuntive o migliorate.

- 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

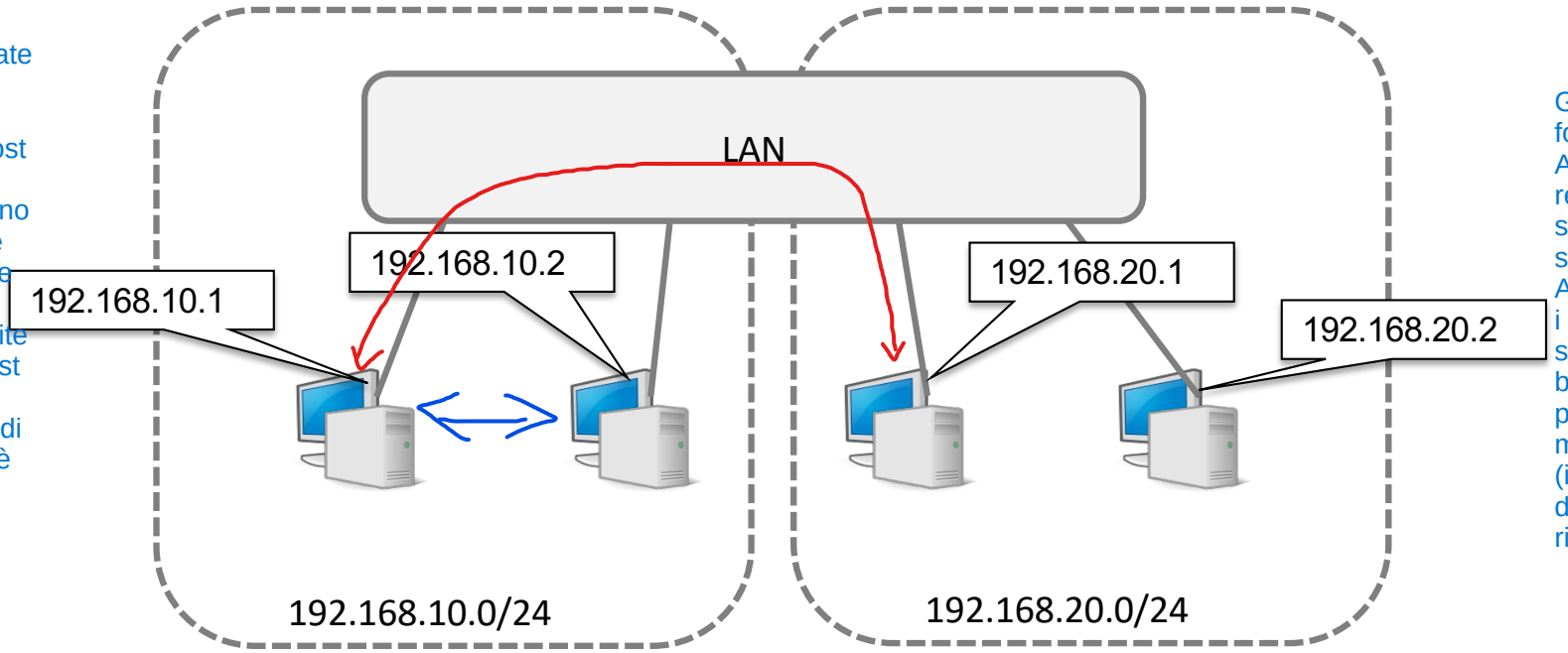
La network IP è una delle forme più comuni di rete overlay, dove viene costruita una rete logica sopra un'infrastruttura fisica utilizzando indirizzi IP per identificare e instradare i dispositivi (host) all'interno della rete.

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

La network 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.
Direct Forwarding: Gli host che appartengono alla stessa network IP possono comunicare direttamente senza bisogno di passare per un gateway.
Indirect Forwarding tramite Gateway: Quando un host di una network IP vuole comunicare con un host di una network IP diversa, è necessario l'uso di un gateway.



Gli switch interconnessi formano la LAN (Local Area Network), un'area di rete delimitata che solitamente copre un singolo edificio o campus. 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 per il trasporto attraverso una rete IP. In questo modo, è possibile utilizzare la rete IP come mezzo di trasporto per dati che non necessariamente seguono il protocollo IP originale.

Il pacchetto esterno ha un header IP che indica gli indirizzi IP di origine e destinazione per il trasporto sulla rete.

- 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 esterno per il trasporto in rete

IP header interno per gli utenti del tunnel

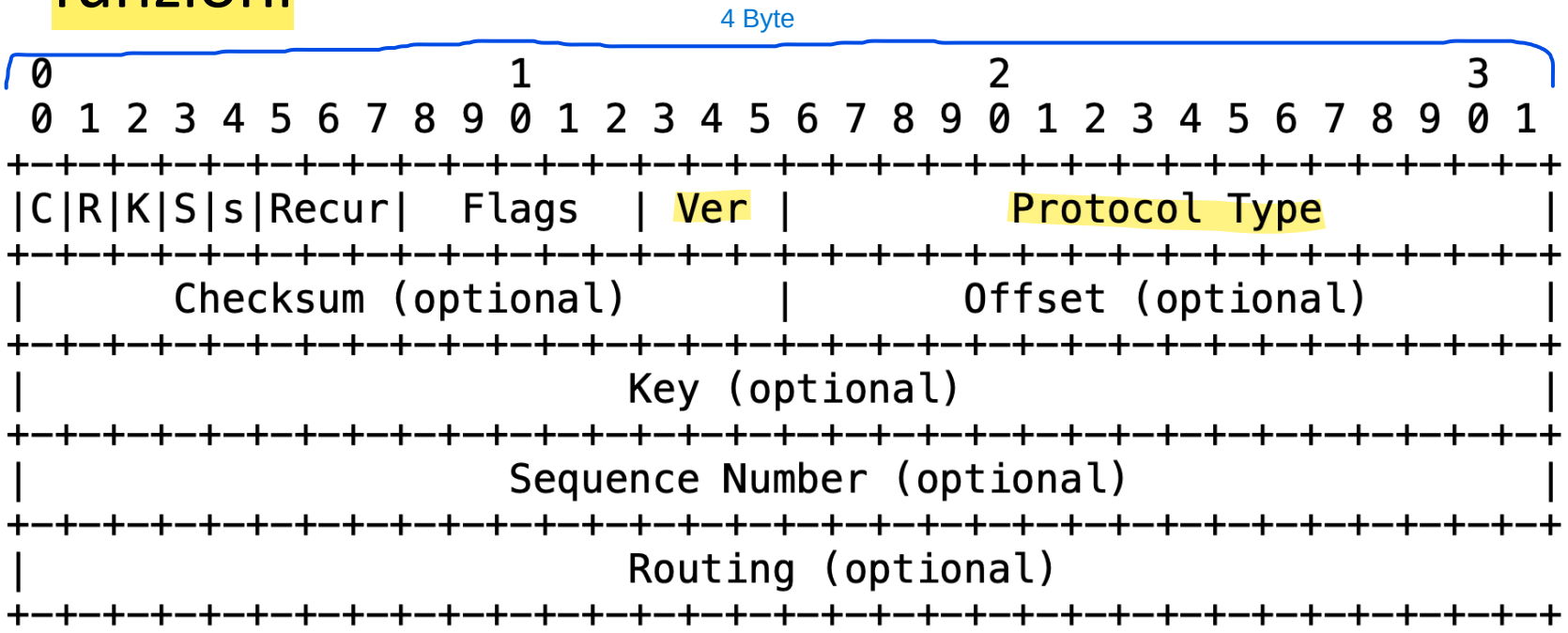
IP Header Interno (Per gli Utenti del Tunnel): Questo header è per il pacchetto incapsulato e contiene le informazioni di indirizzamento originali, visibili solo quando il pacchetto è "decapsulato" alla fine del tunnel.

IP Header Esterno (Per il Trasporto): Questo header è utilizzato per instradare il pacchetto nella rete principale, consentendo di inviare il pacchetto incapsulato attraverso una rete IP pubblica o privata.

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

spesso utilizzato per identificare un tunnel specifico o per applicazioni che richiedono autenticazione tra i due endpoint del tunnel.

- 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.

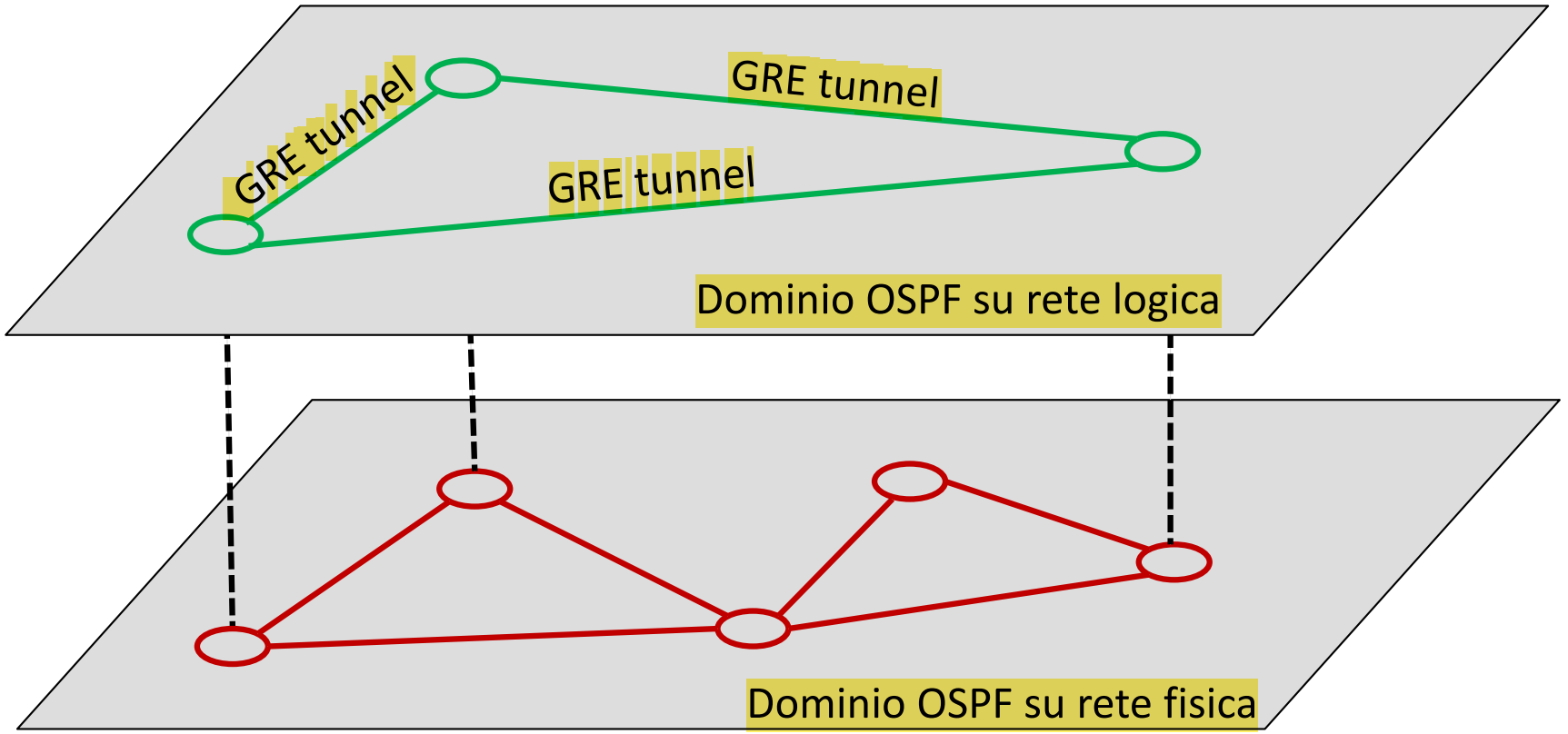
- Routing

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

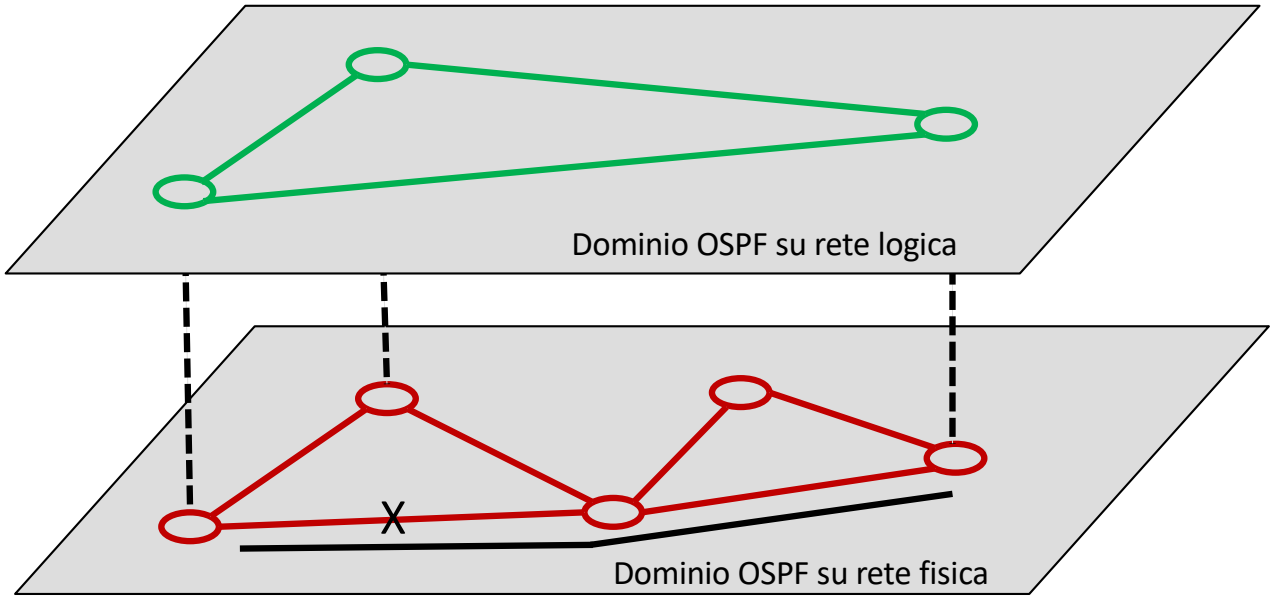
  - È possibile elencare i router che si vuole vengano attraversati dal pacchetto (determina la politica di instradamento del tunnel)

Applicazione del GRE

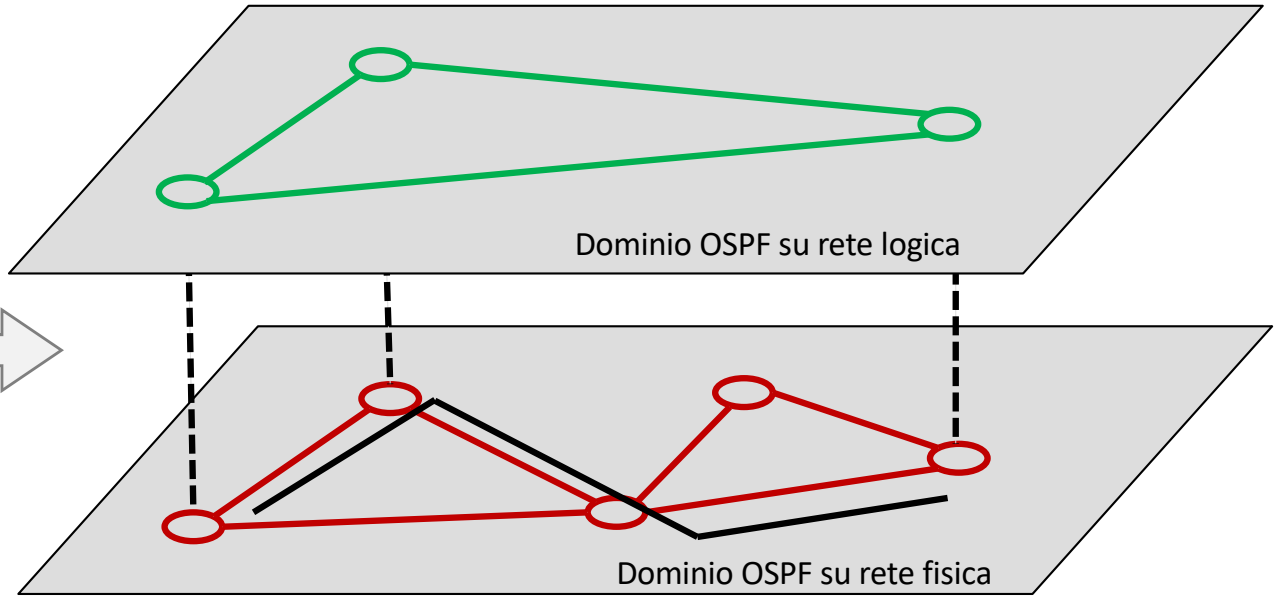
- Incapsulamento di IP su IP
- Permette di creare un overlay a livello di routing



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.

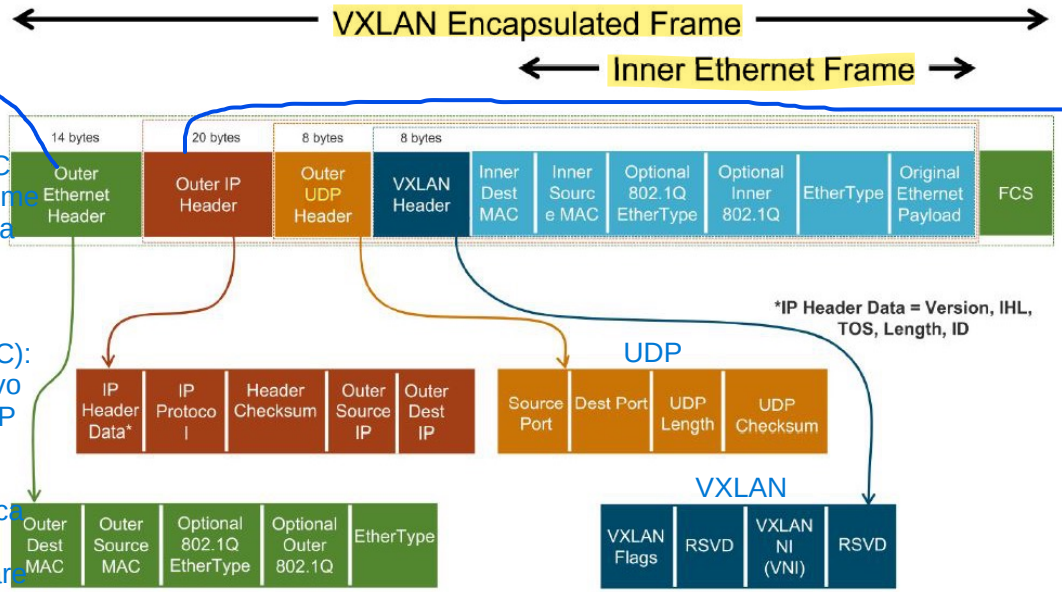
- Highly scalable distributed Layer 2 overlay network for tenant traffic isolation in could computing environments
- Encapsulation of L2 traffic in UDP packets (dest port 4789)
  - stateless tunnels between VXLAN Tunnel End Points (VTEPs)
  - each isolated L2 segment is identified by a 24-bit VXLAN Network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

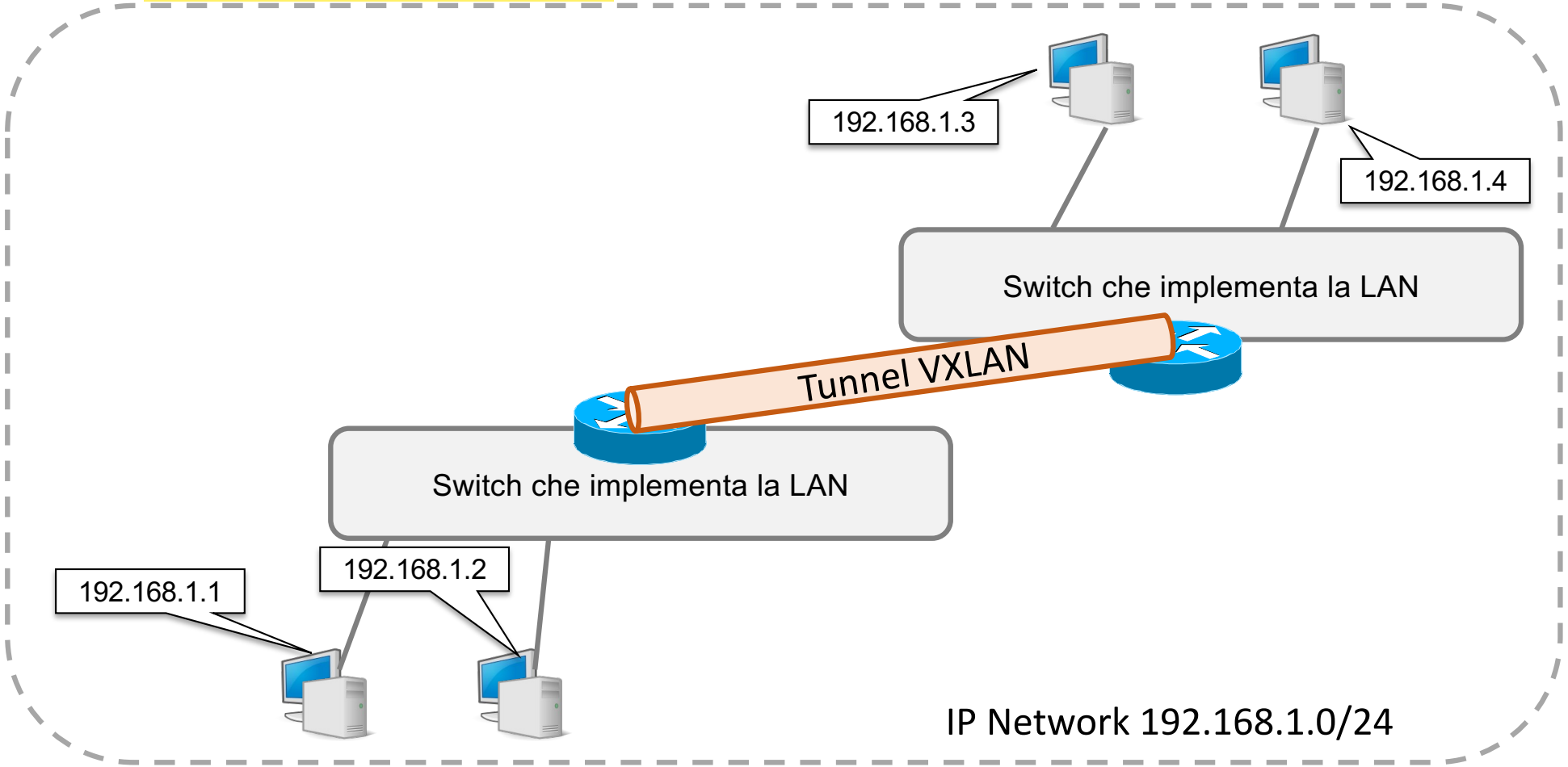


MAC di Destinazione (Outer Dest MAC): Rappresenta l'indirizzo MAC del prossimo dispositivo di rete (come uno switch o un router) nella catena di trasporto del pacchetto. Questo dispositivo può essere il primo hop verso la destinazione finale.
MAC di Origine (Outer Source MAC): Indica l'indirizzo MAC del dispositivo che invia il pacchetto, come il VTEP (VXLAN Tunnel Endpoint) che incapsula il pacchetto.
Tipo Ethernet (EtherType): Specifica il tipo di protocollo del payload Ethernet, solitamente per identificare il protocollo IP (Internet Protocol) quando si usa VXLAN.

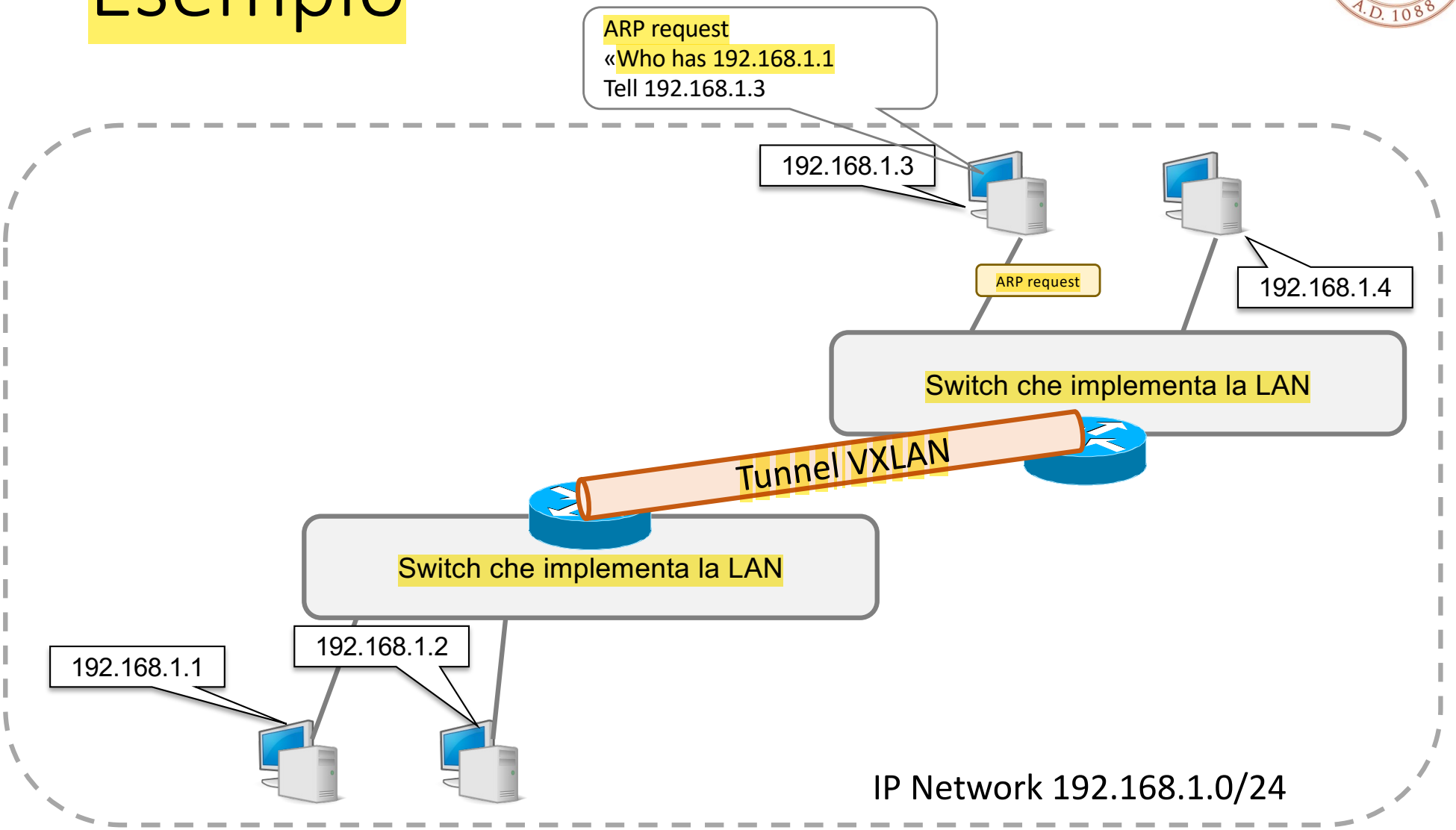
Indirizzo IP di Origine (Outer Source IP): Questo è l'indirizzo IP del dispositivo che sta incapsulando il traffico VXLAN, come un VTEP. L'indirizzo di origine è quello del punto in cui il pacchetto entra nella rete IP.
Indirizzo IP di Destinazione (Outer Dest IP): L'indirizzo IP del dispositivo VTEP 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

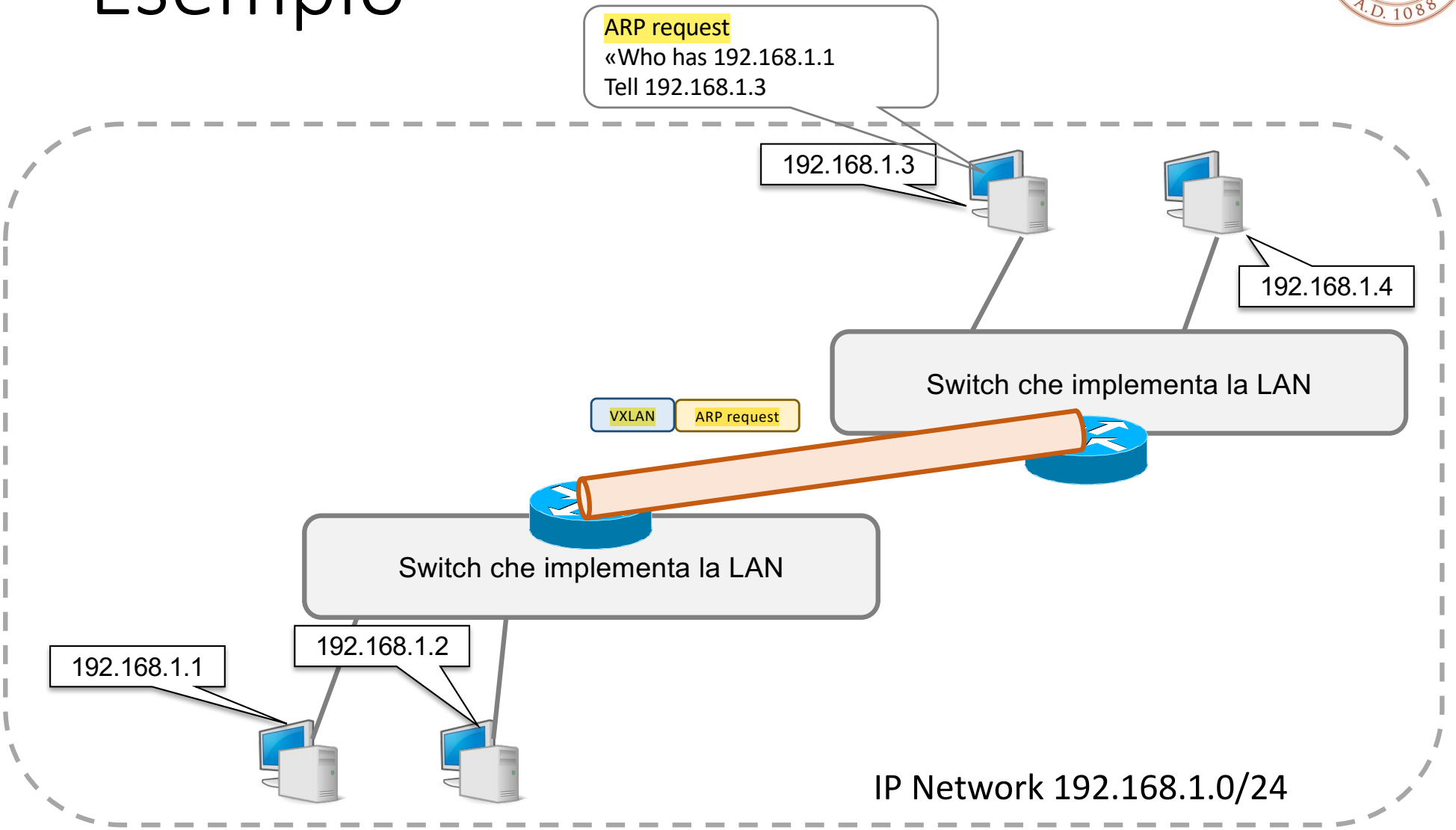
- Una sola network IP estesa sulla rete globale
- VXLAN trasporta i frame Ethernet sulla rete di interconnessione IP



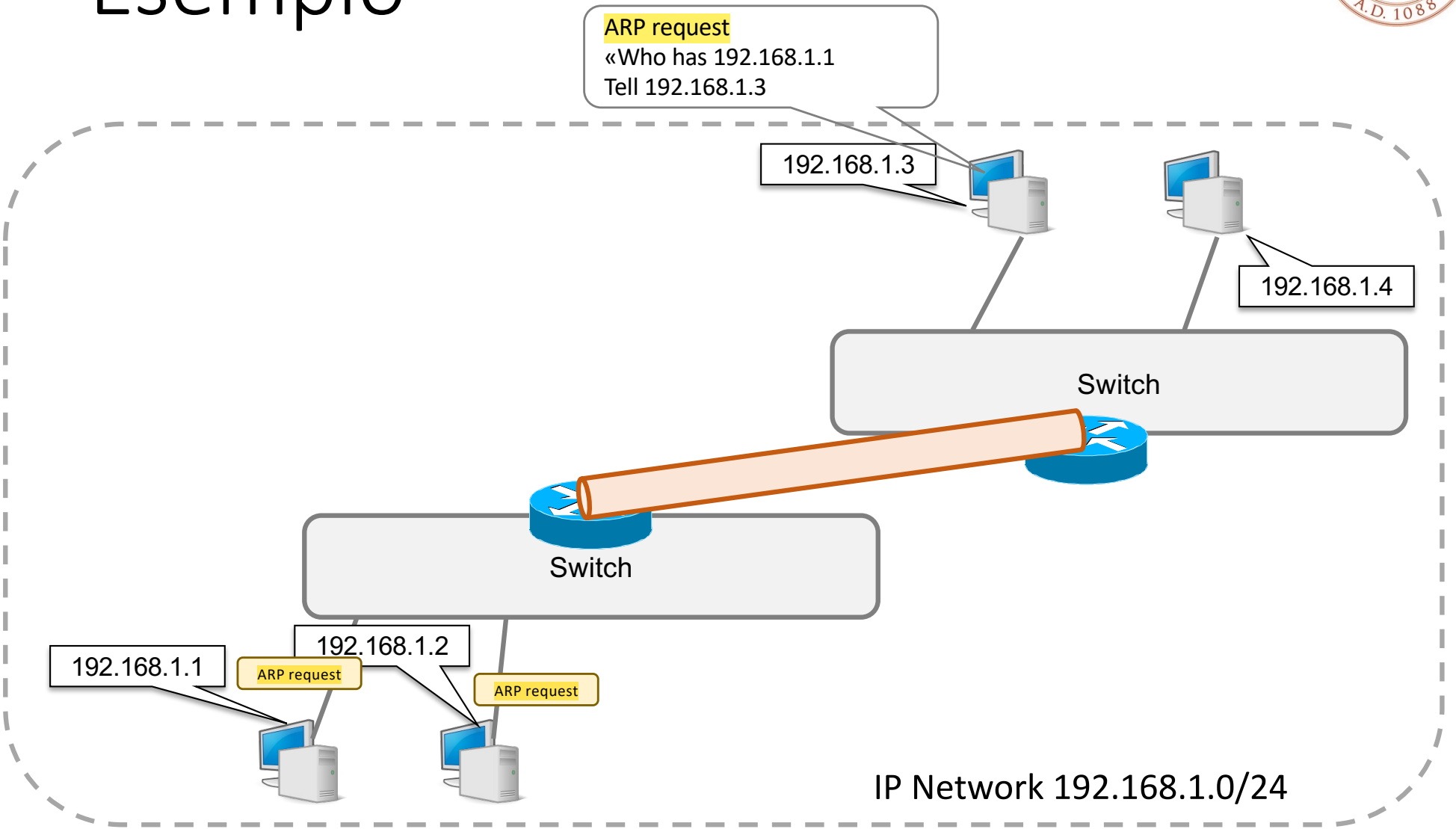
Esempio


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

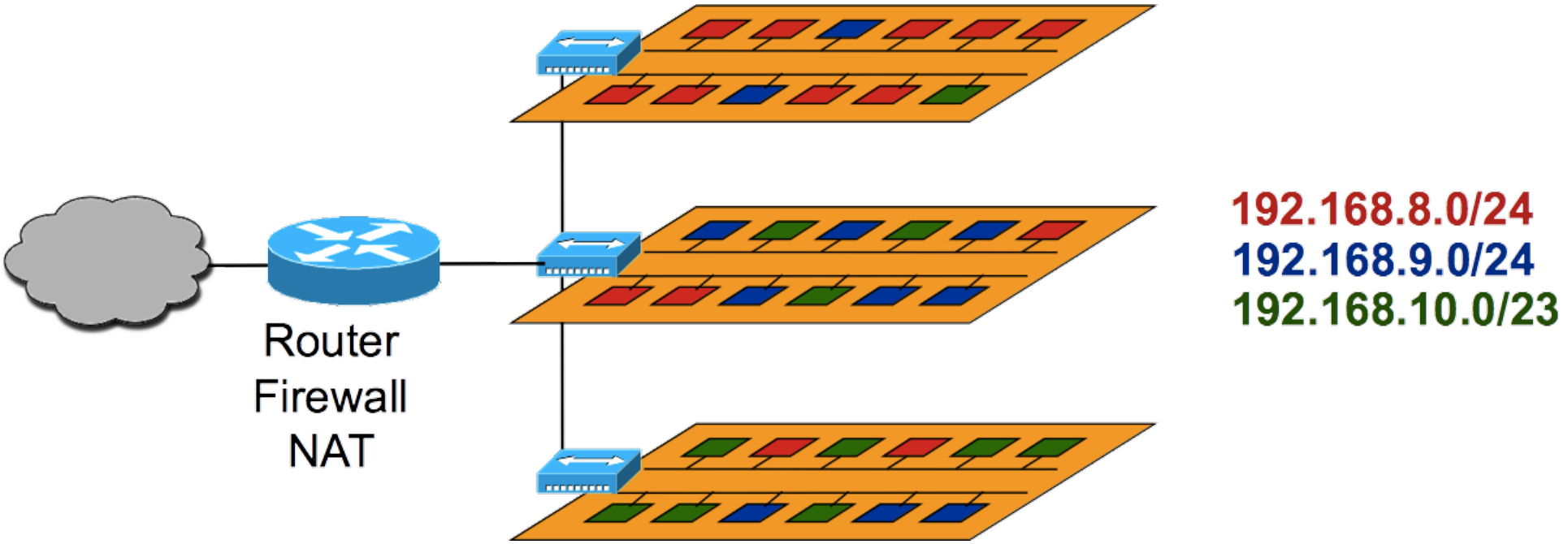
- Quando il dominio di broadcast è uno solo
  - Un broadcast inviato da un calcolatore a tutti gli altri calcolatori della LAN
  - Anche se su reti IP diverse
- Questo rappresenta un doppio problema
  - *Prestazioni*: i pacchetti broadcast utilizzano capacità di rete, più ce ne sono minore è la capacità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

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

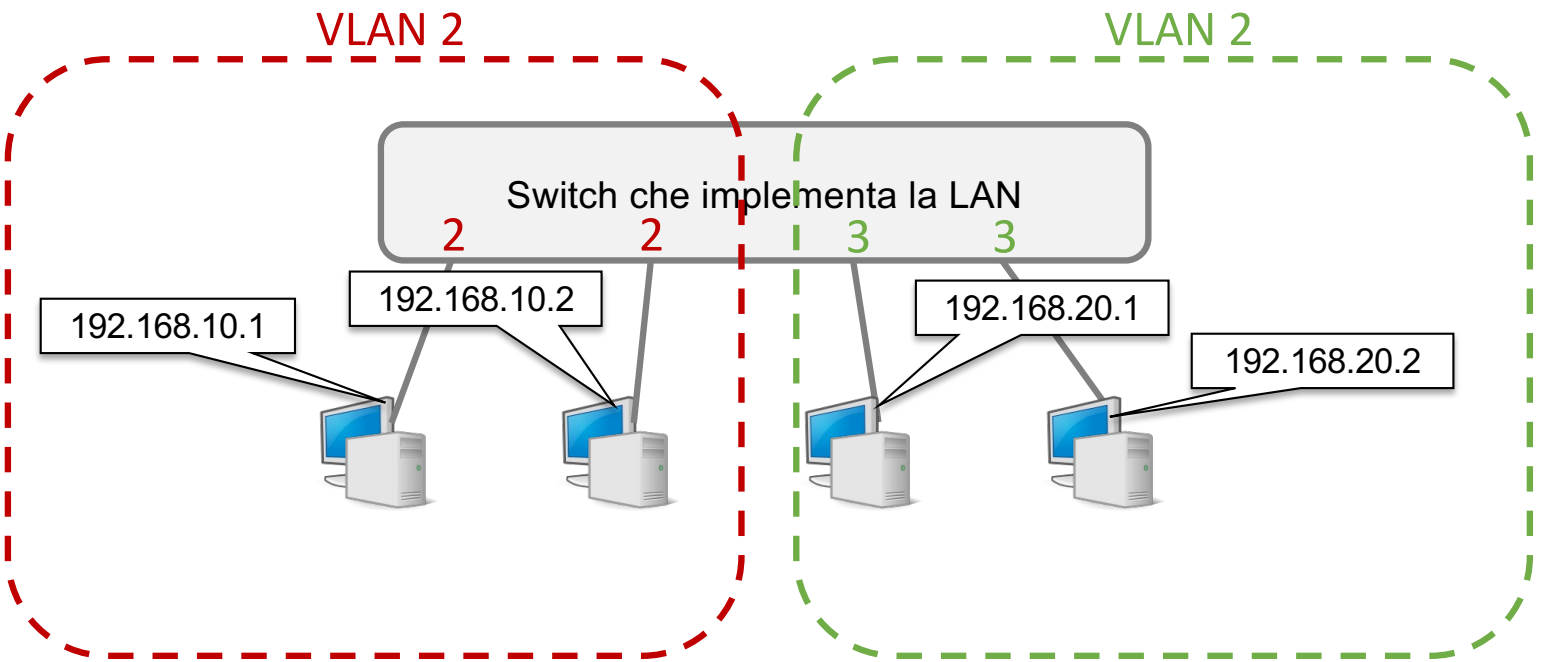


Classificazione delle VLAN

- 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

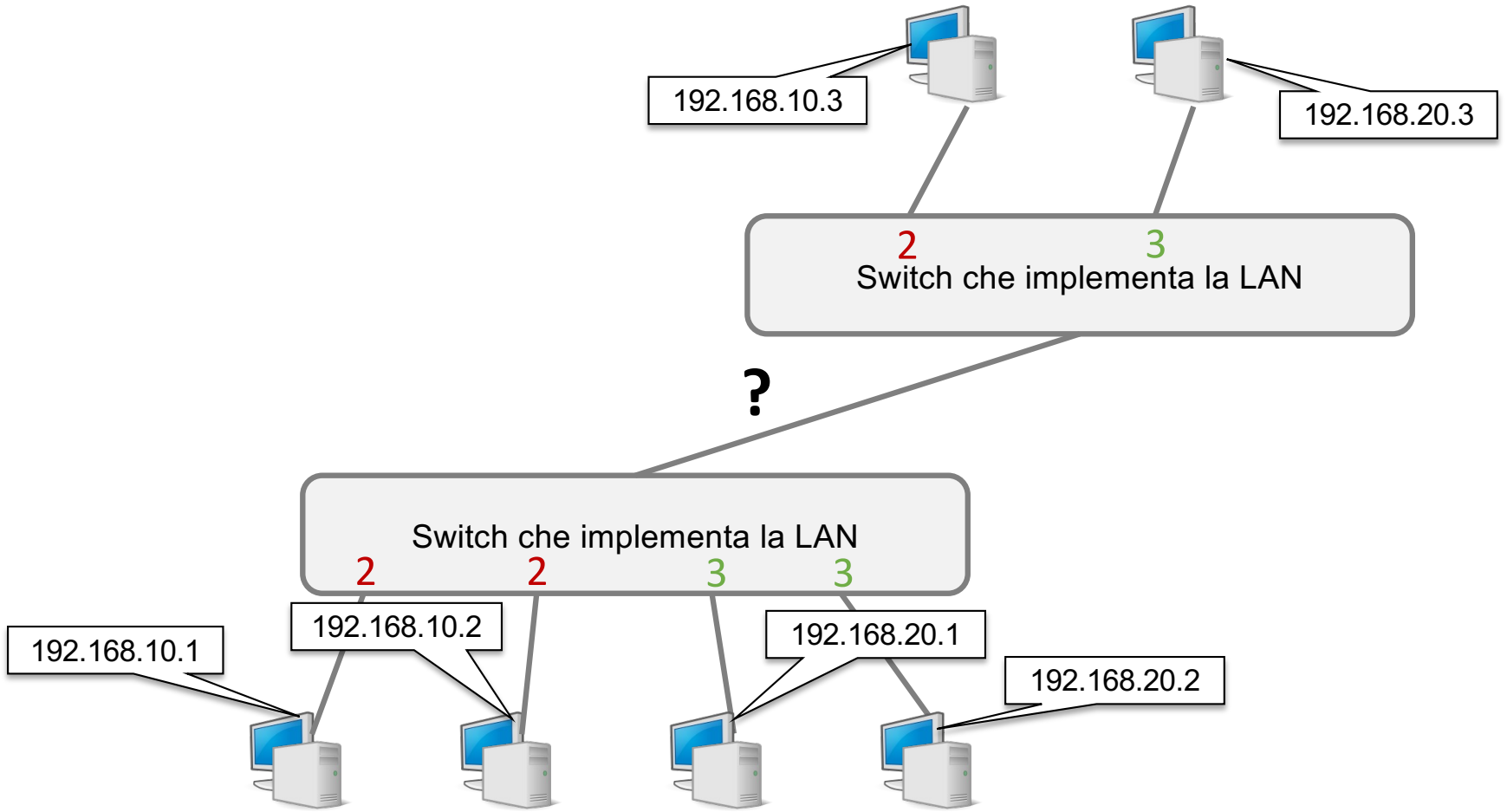
VLAN statica

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



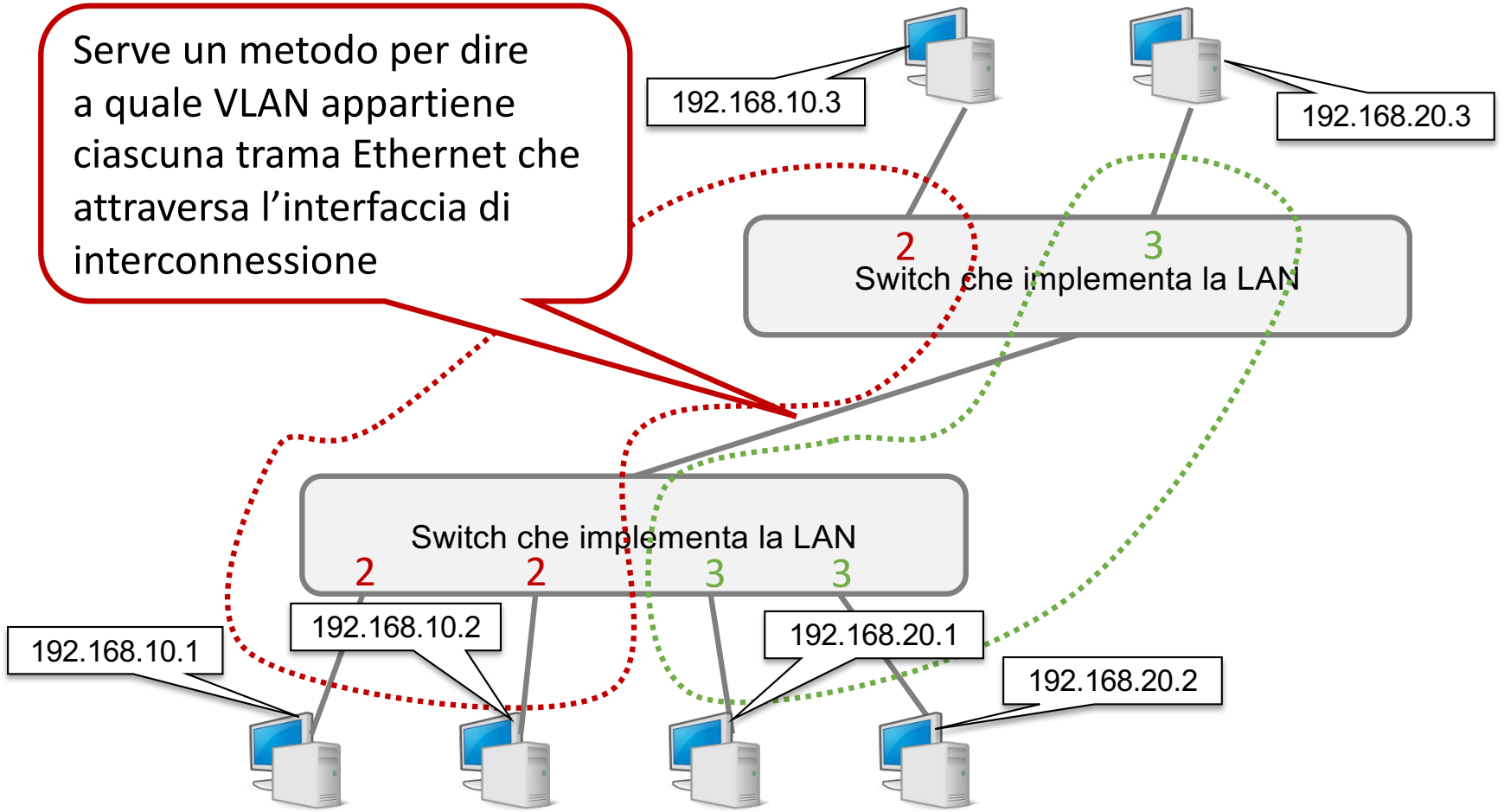
LAN estesa

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



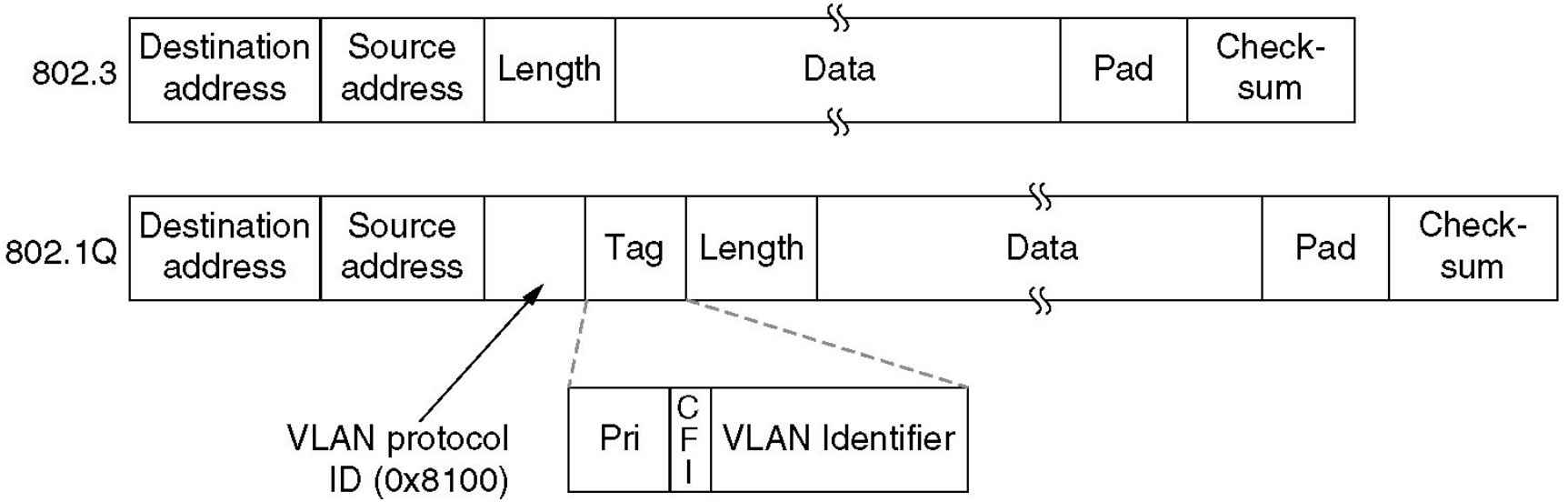
LAN estesa

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



IEEE 802.1Q

- Protocollo che permette l'utilizzo delle stesse VLAN su diversi switch interconnessi tra loro
- 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)
  - 16 bit
  - Usually 0x8100
- Priority
  - 3 bit
- CFI
  - 1 bit
  - Identifica il formato del MAC address
- Unique LAN Identifier (VID)
  - 12 bits
  - Numero della VLAN (da 0 a 4095)

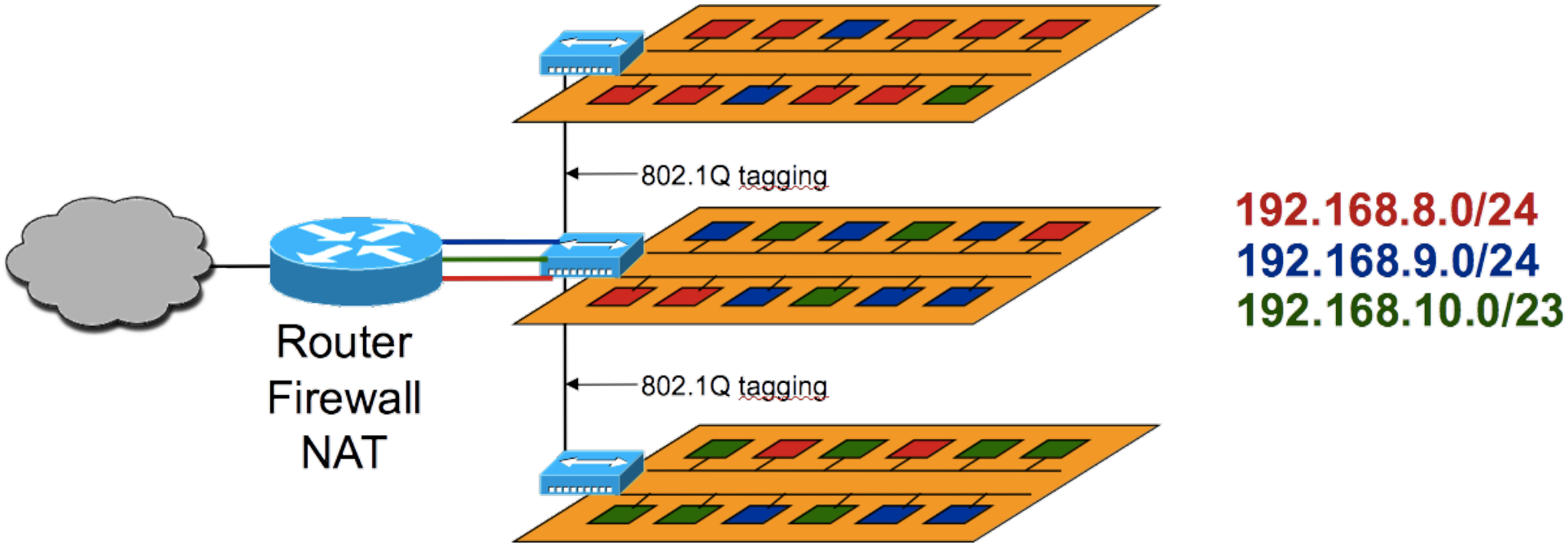
Porte dello switch

- Access mode
  - porta associata ad una sola VLAN
  - tagging 802.1Q non necessario
  - modalità tipica per porte connesse agli hosts

- 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

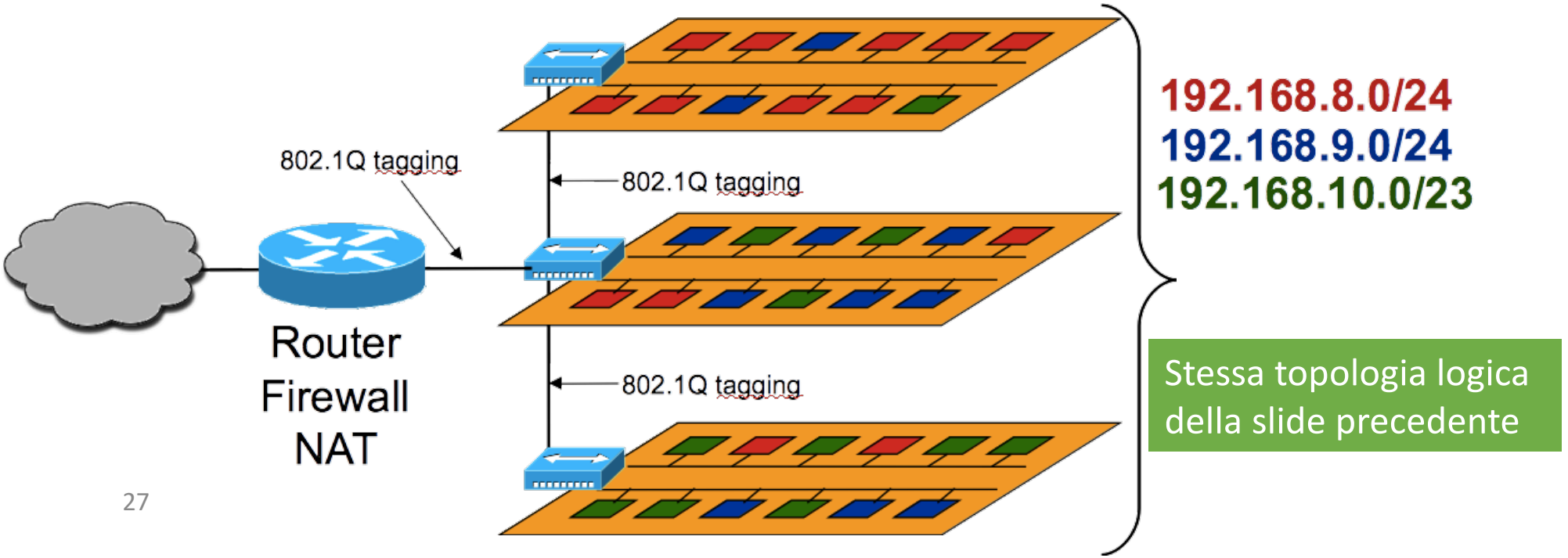
Inter-VLAN routing

- 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



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

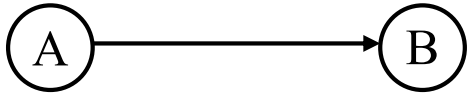
Reti private virtuali

- 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

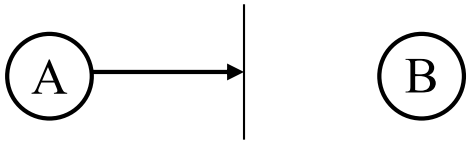
La VPN utilizza diversi protocolli di tunneling per garantire che i dati siano protetti durante il trasferimento

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

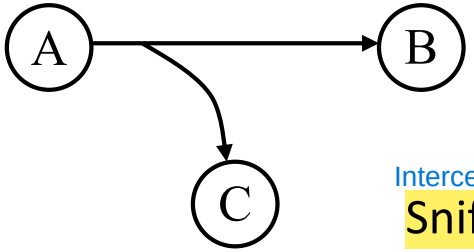


Normal information flow



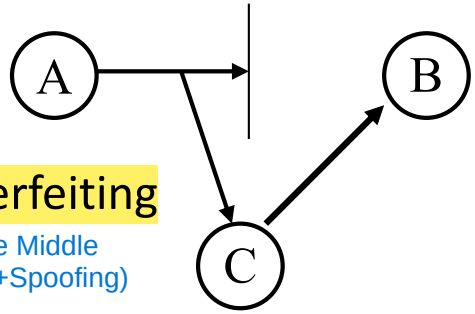
Interruzione

Blocking



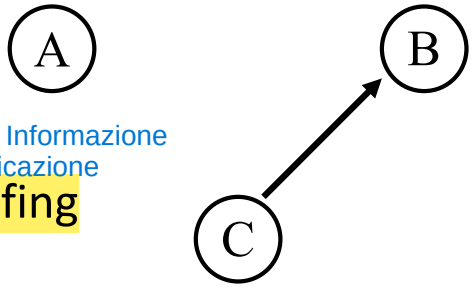
Intercettazione

Sniffing



Counterfeiting

Man in the Middle
(Blocking+Spoofing)



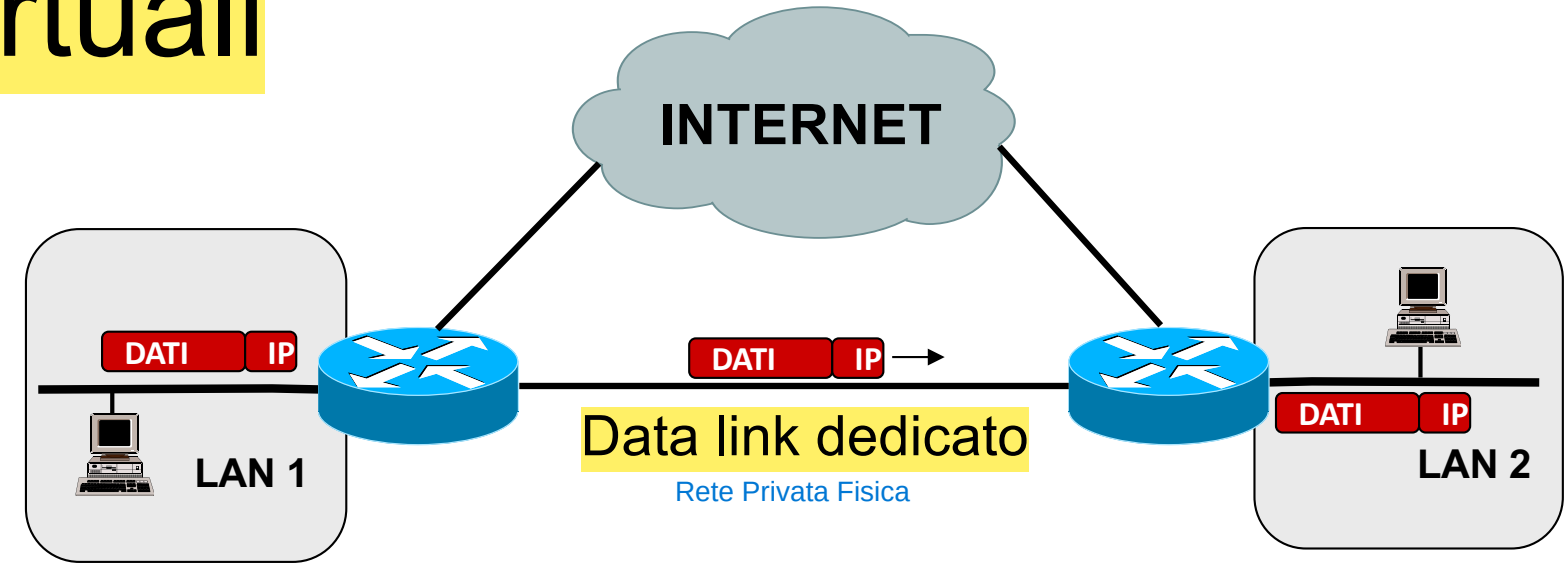
Creazione Informazione
e Personificazione

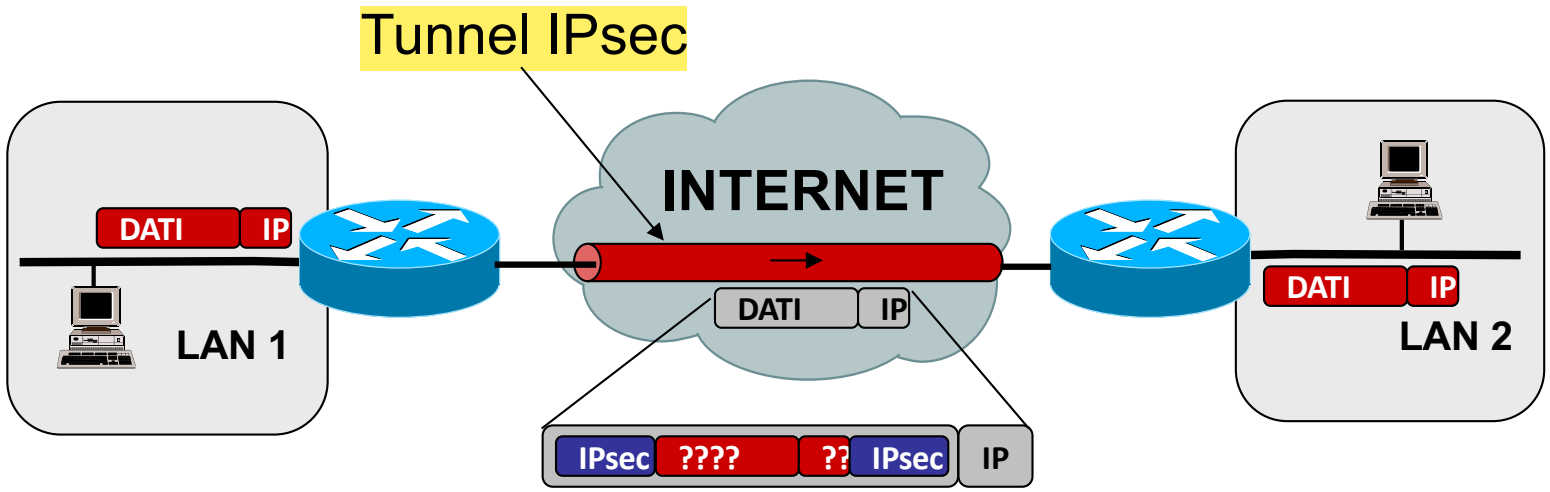
Spoofing

Obiettivi di una rete privata

- Riservatezza — Garantire che solo gli utenti autorizzati possano leggere le informazioni trasmesse o memorizzate nella rete (Questo implica l'uso di tecniche come la crittografia).
  - Le informazioni non sono leggibili da tutti
- Autorizzazione — Stabilire chi ha il permesso di accedere o interagire con i dati (L'autorizzazione definisce i privilegi di ogni utente o dispositivo nella rete, indicando quali dati possono essere letti, modificati o cancellati.).
  - Definisco il sottoinsieme di coloro che sono in grado di leggere i dati
- Autenticazione — Verificare l'identità di chi sta accedendo o leggendo i dati (L'autenticazione è il processo che assicura che un utente o dispositivo sia effettivamente chi dice di essere.).
  - Verifico chi sta leggendo i dati
- Paternità — Garantire l'origine dei dati, cioè sapere chi ha creato o inviato una determinata informazione (Questo obiettivo è cruciale per la tracciabilità e per verificare che i dati non siano stati manipolati durante il loro percorso nella rete.).
  - Garantisco l’origine dei dati

Reti private reali e reti private virtuali



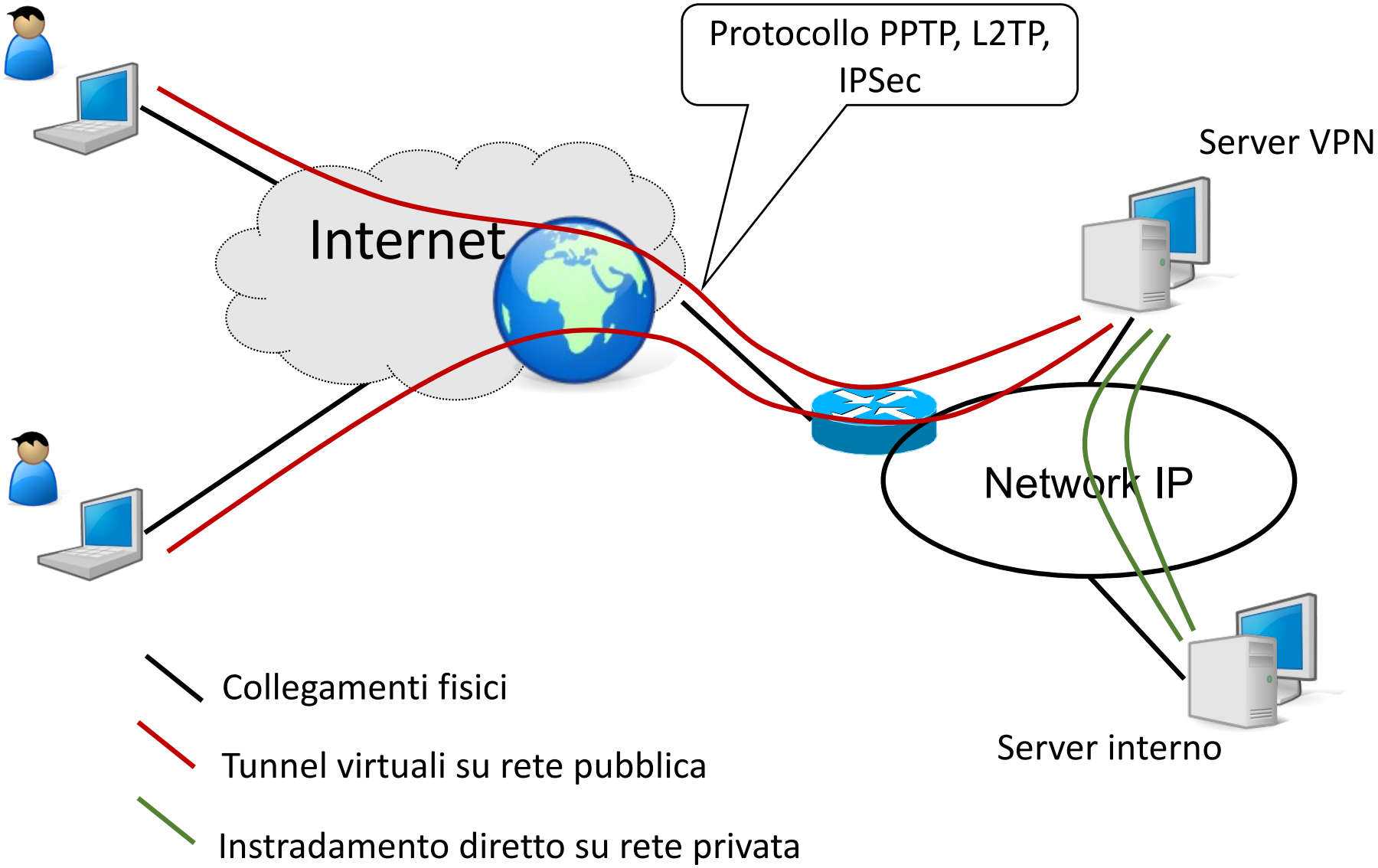


VPN Roadwarrior

- 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

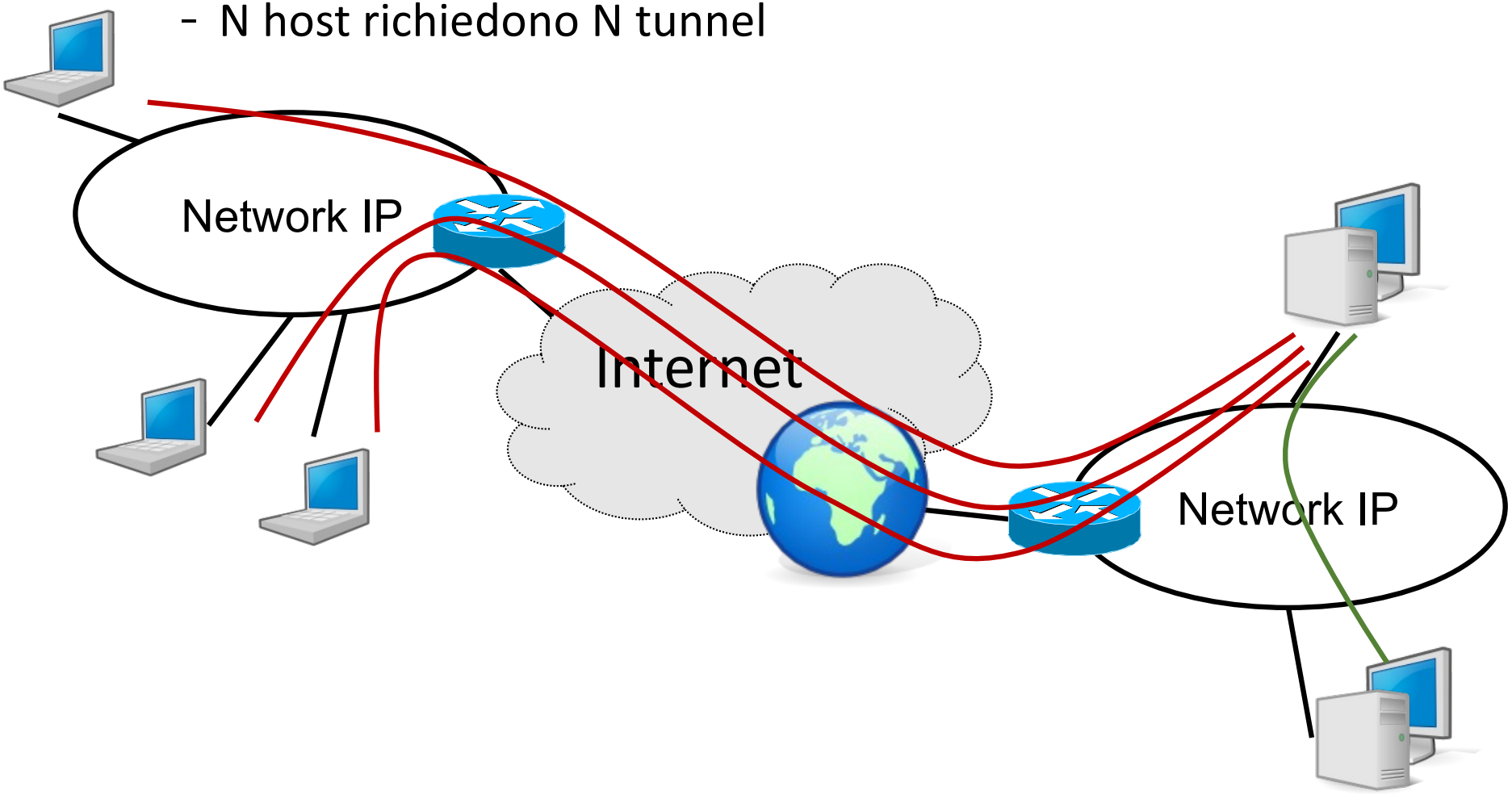
- Si configura come una rete di comunicazioni sicure sul server VPN

Roadwarrior



Problema

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

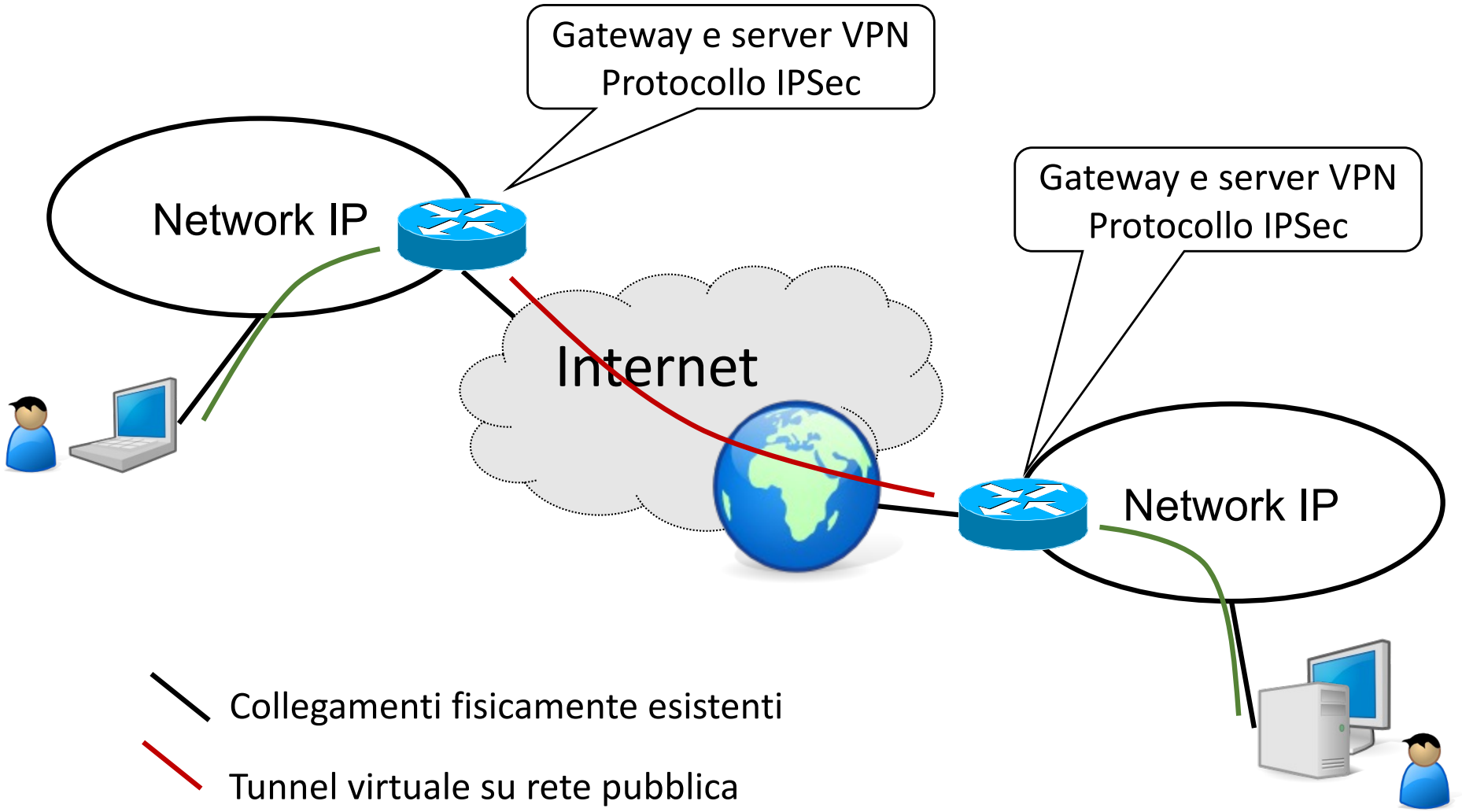


VPN da rete a rete

- Si crea un tunnel cifrato su rete pubblica fra due LAN o fra due network IP
  - Su rete pubblica i pacchetti vengono cifrati
  - Su rete pubblica l'indirizzamento reale può essere mascherato

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

Net-to-Net


Gateway e server VPN
Protocollo IPSec
Network IP
Internet
Gateway e server VPN
Protocollo IPSec
Network IP
Collegamenti fisicamente esistenti
Tunnel virtuale su rete pubblica
Instradamento indiretto su rete privata

IPSec

- 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

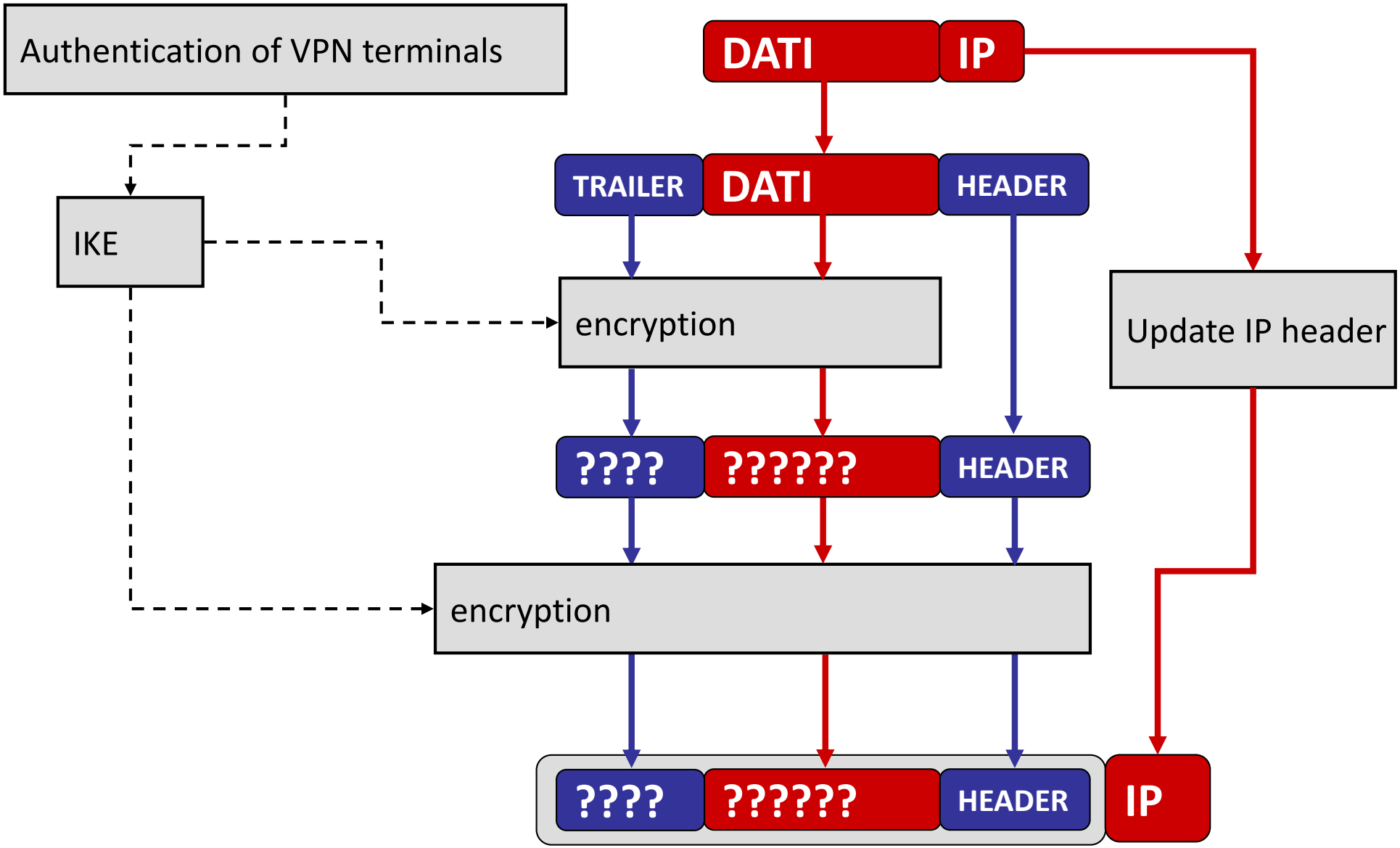
Protocolli

- IKE (Internet Key Exchange):
  - autenticazione interlocutore
  - negoziazione algoritmi e chiavi crittografiche
    - Utilizza UDP (porta sorgente e destinazione = 500)
- AH (Authentication Header) (campo protocol IP = 51):
  - autenticazione dei pacchetti trasmessi in VPN garantendo
    - integrità ed autenticità dei dati
    - identità del mittente
- ESP (Encapsulating Security Payload) (campo protocol IP = 50):
  - come in AH + riservatezza delle informazioni tramite crittografia

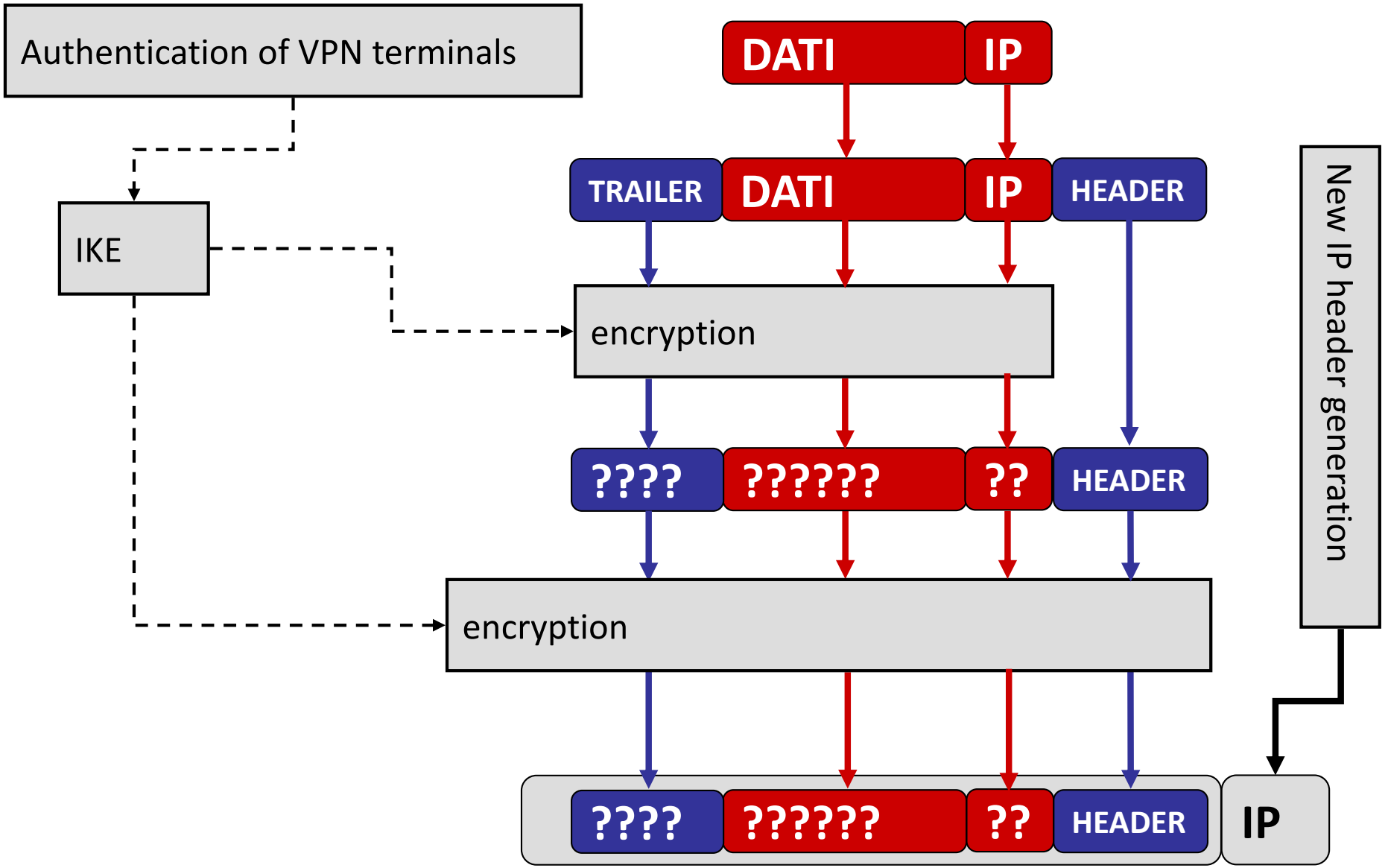
IKE

- 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
- 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

IPsec: ESP Transport



IPsec: ESP Tunnel



ESP: tunnel vs transport