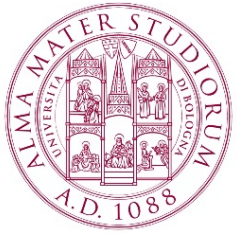


ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

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

- Vantaggi
  - Condivisione di risorse fisiche
  - Disaccoppiamento del progetto software da quello hardware
  - Maggiore flessibilità (mobilità, scalabilità)
- Criticità
  - Isolamento fra sistemi distinti che condividono lo stesso hardware
  - Sicurezza e privacy

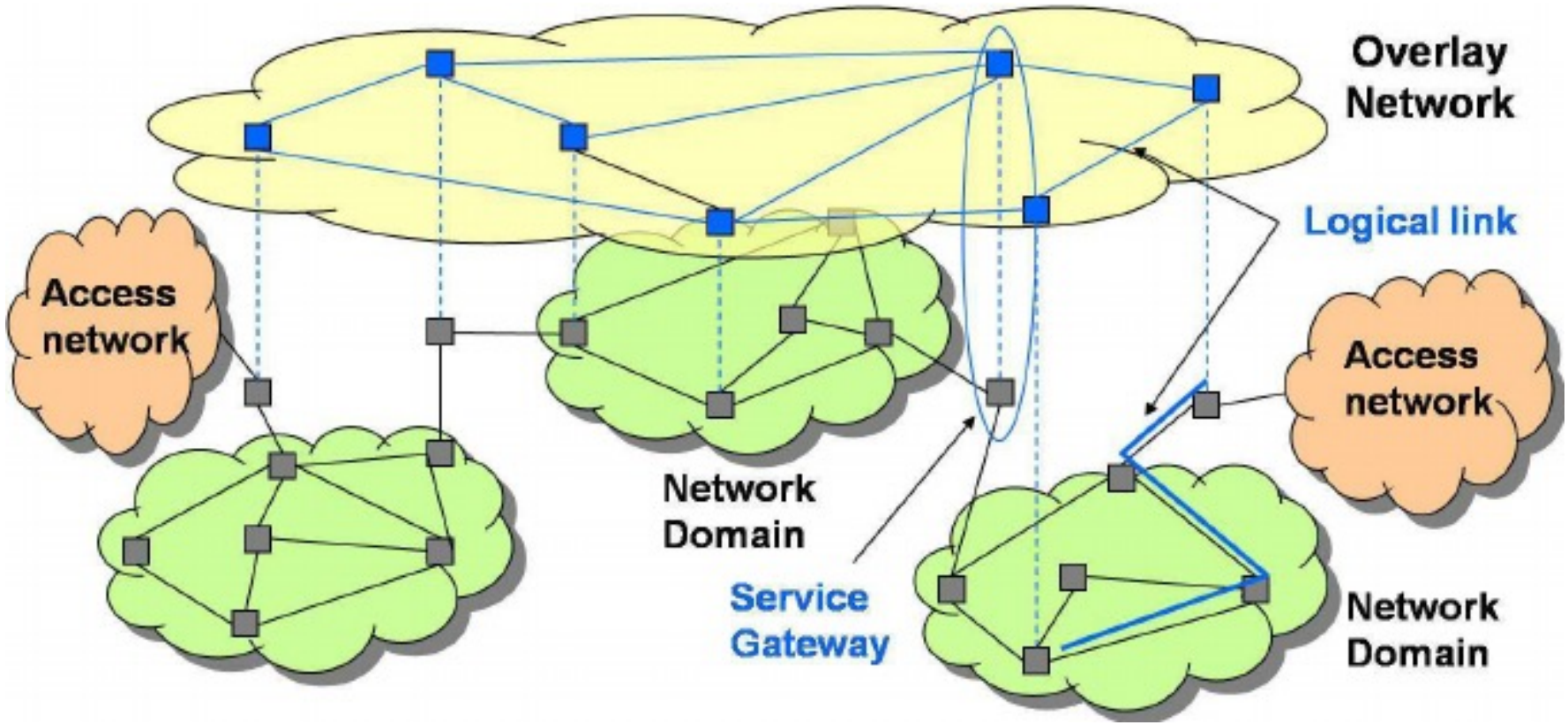
Virtualizzazione di rete

- 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

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

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

Reti “Overlay”



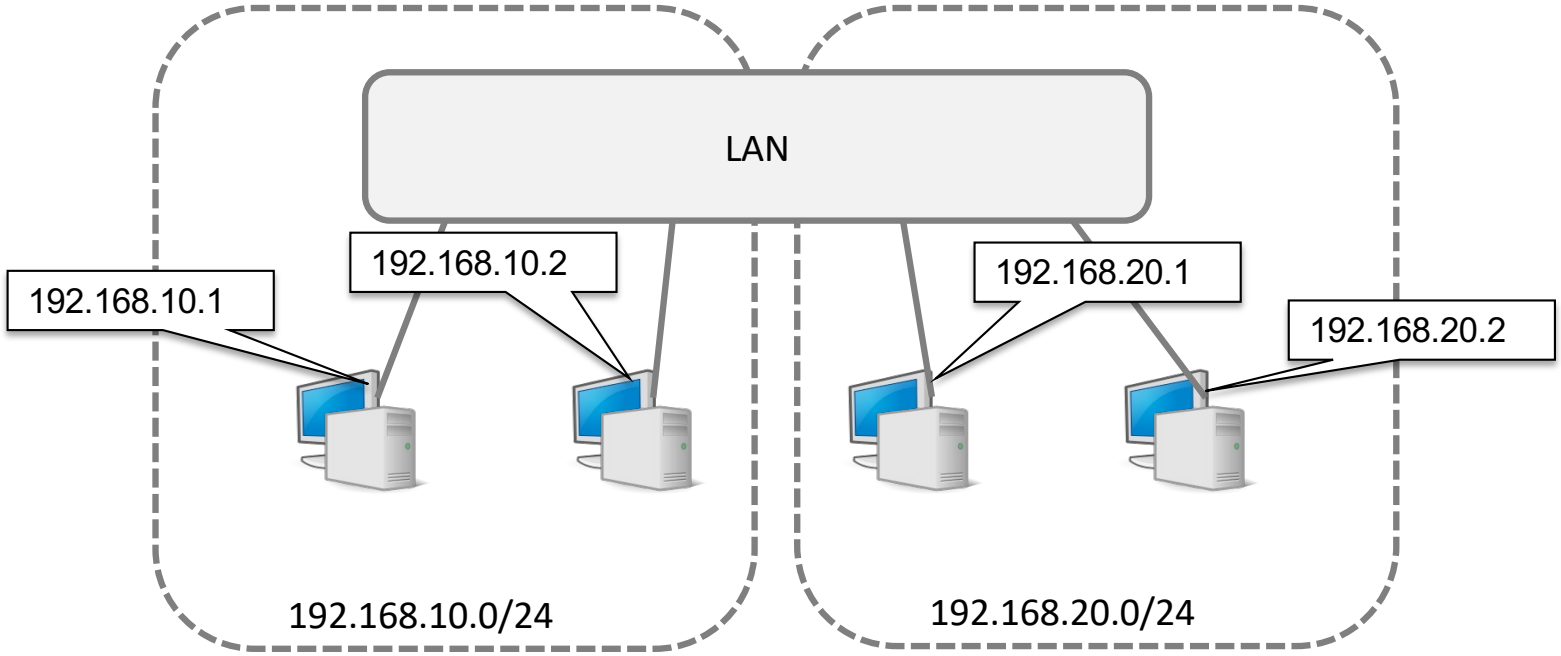
Tecnologie di virtualizzazione

- 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

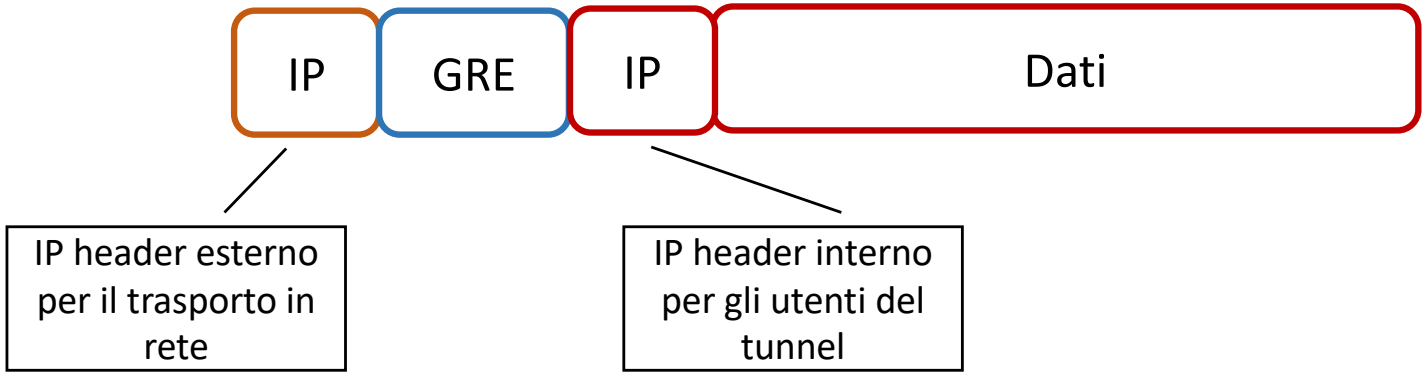
- La network IP è già una forma di network overlay
- Gli switch interconnessi realizzano la LAN
  - Un solo dominio di broadcast
  - La ripartizione degli host in diverse network IP determina differenze nelle politiche di instradamento politica di instradamento
    - Direct forwarding fra Host della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



GRE Tunnel (RFC 1701)

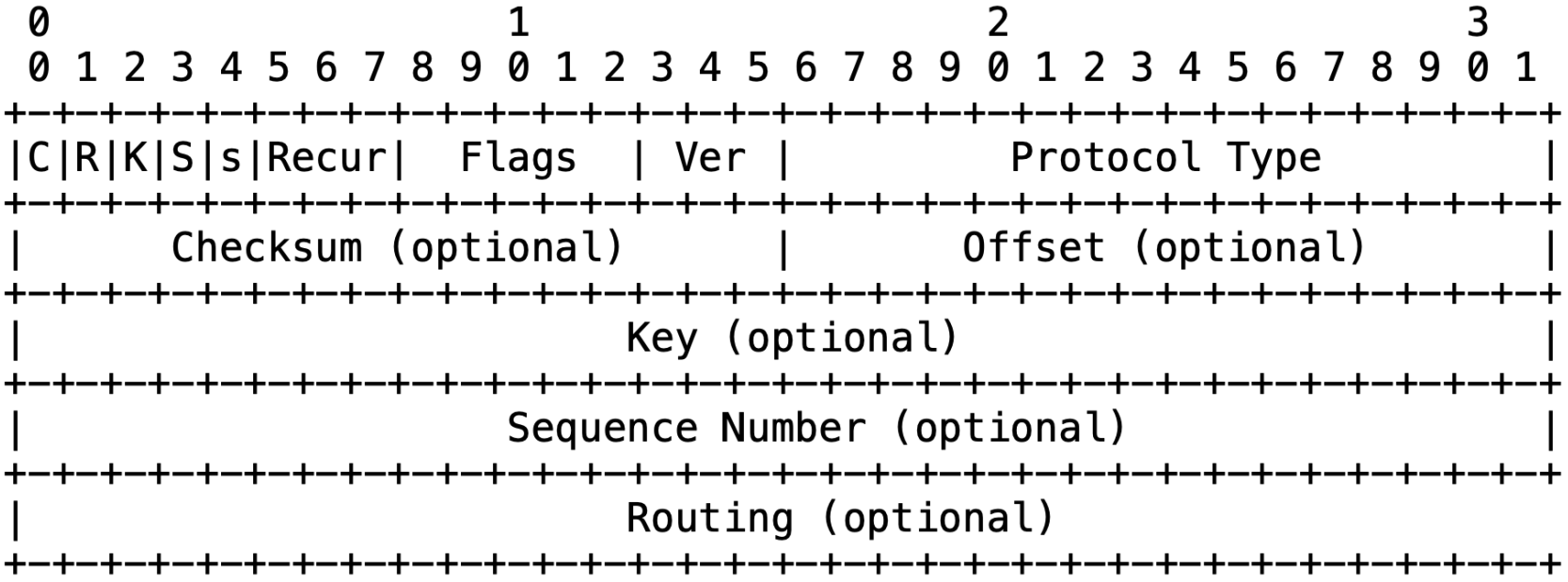
- Protocollo per l'incapsulamento di pacchetti generici su protocollo IP

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



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

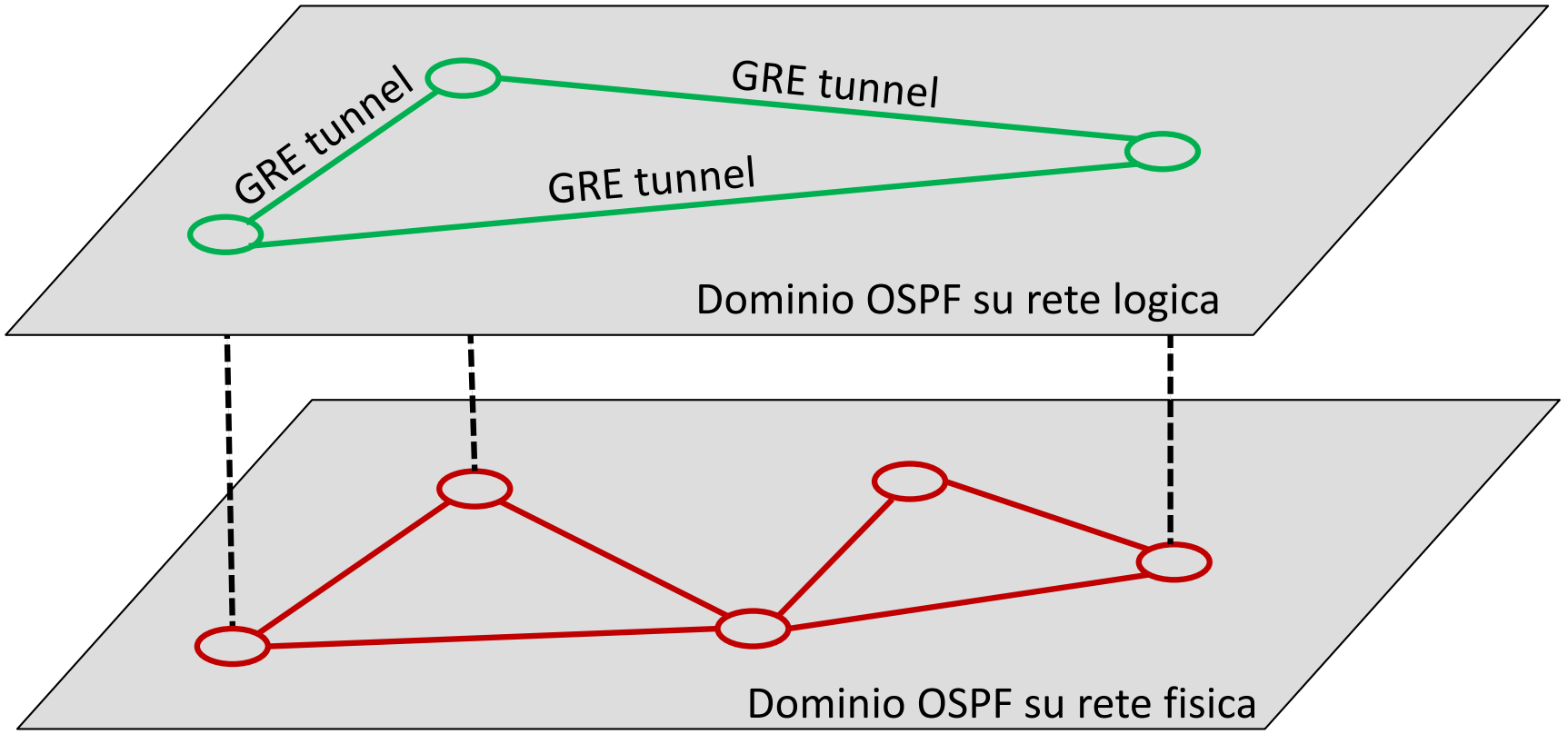


GRE header: campi opzionali

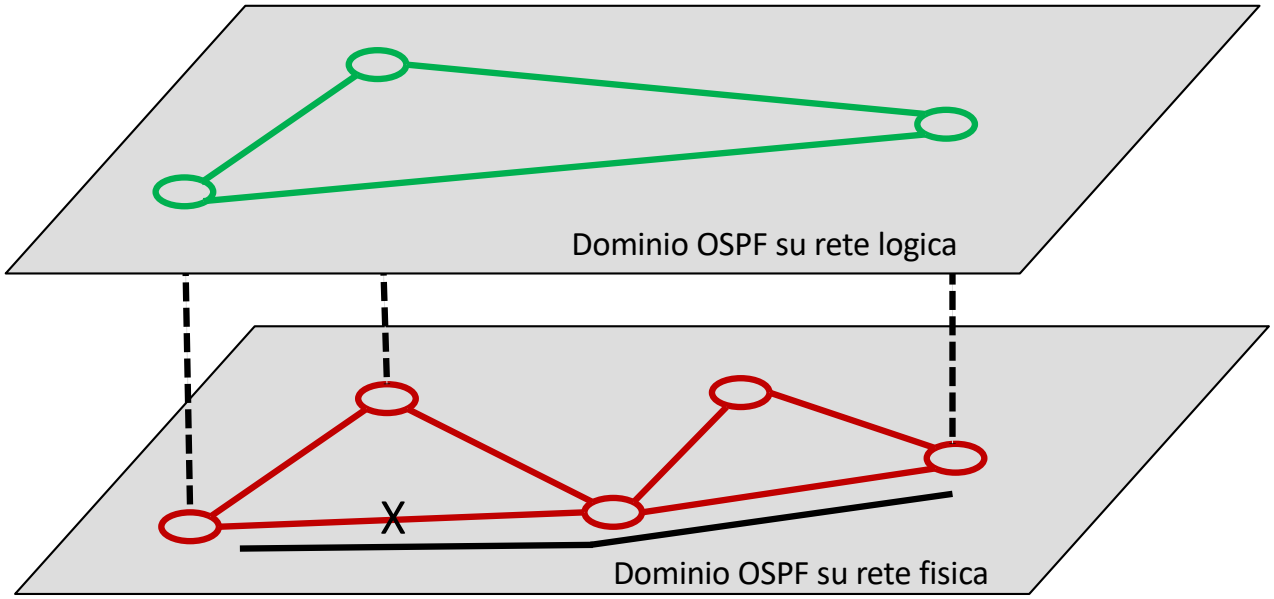
- Checksum
  - Inserito per controllare la correttezza dei dati (Internet checksum)
- Key
  - Può essere inserito per autenticare la sorgente del pacchetto incapsulato nel tunnel con un qualche metodo di autenticazione (password)
- Sequence Number
  - Inserito alla sorgente per stabilire la sequenza di invio dei pacchetti sul tunnel
  - La destinazione dovrebbe instradare i pacchetti ricevuti nel corretto ordine
- Routing
  - È possibile elencare i router che si vuole vengano attraversati dal pacchetto (determina la politica di instradamento del tunnel)

Applicazione del GRE

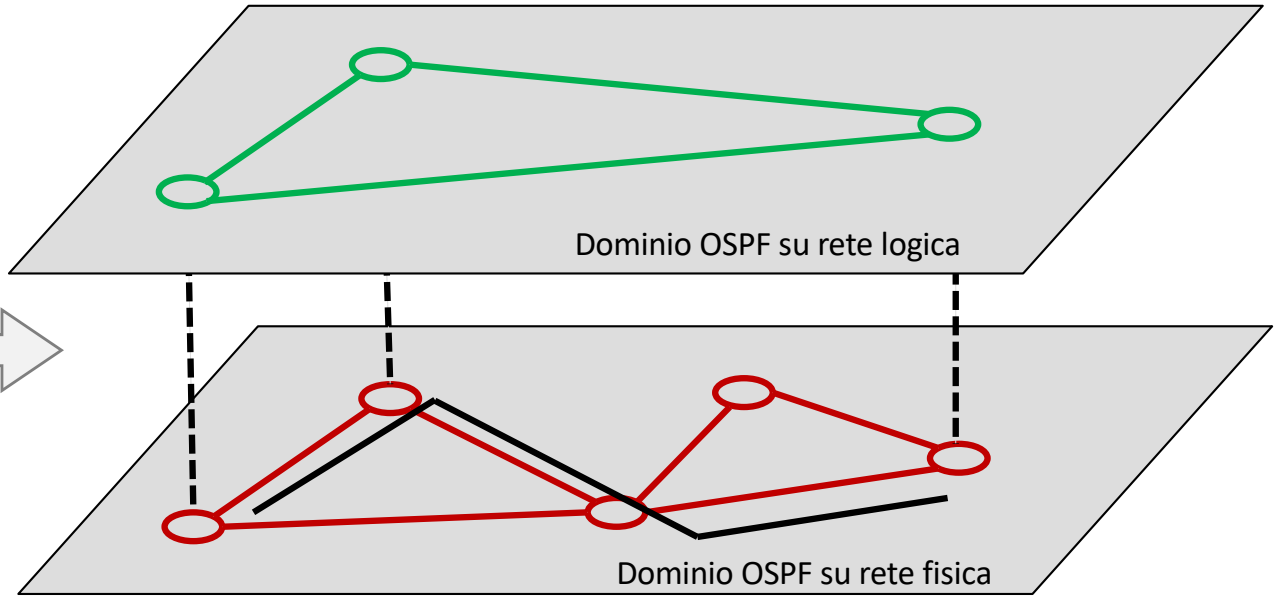
- Incapsulamento di IP su IP
- Permette di creare un overlay a livello di routing



Applicazione del GRE

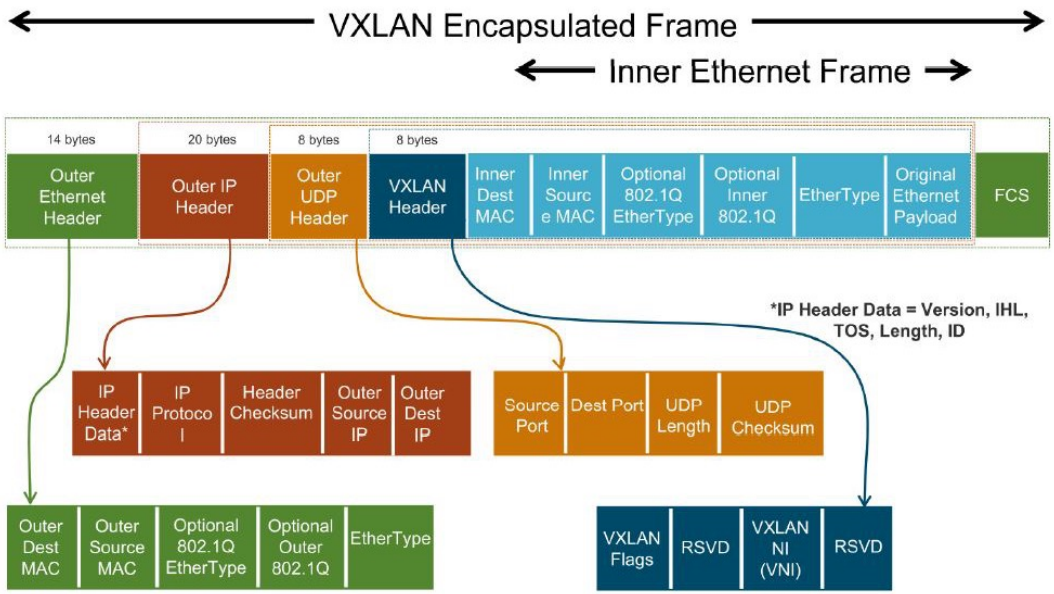


Una modifica del percorso nel dominio su rete fisica non viene percepita nel dominio su rete logica



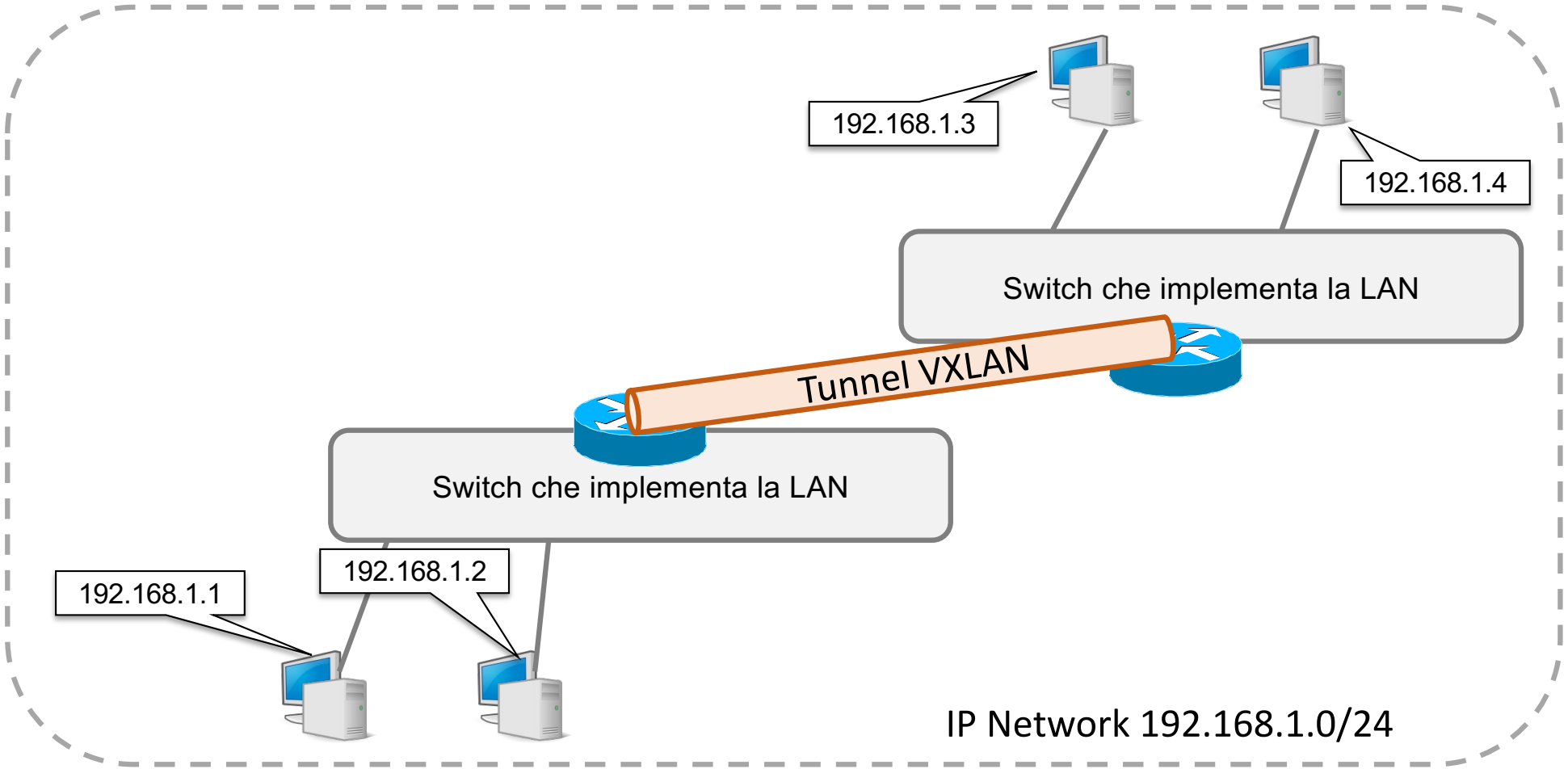
Virtual Extensible LAN (VXLAN)

- 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

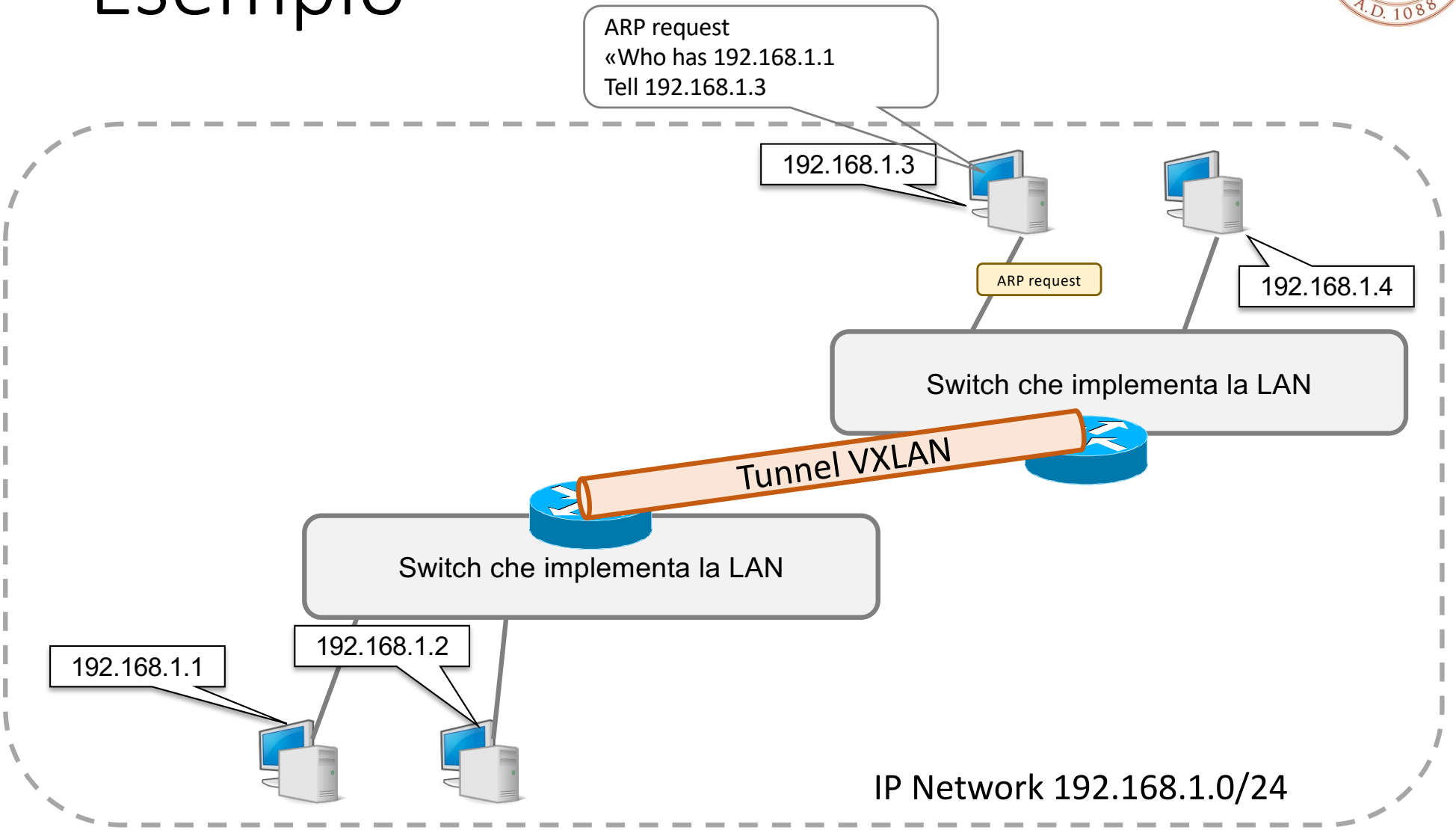


Applicazione di VXLAN

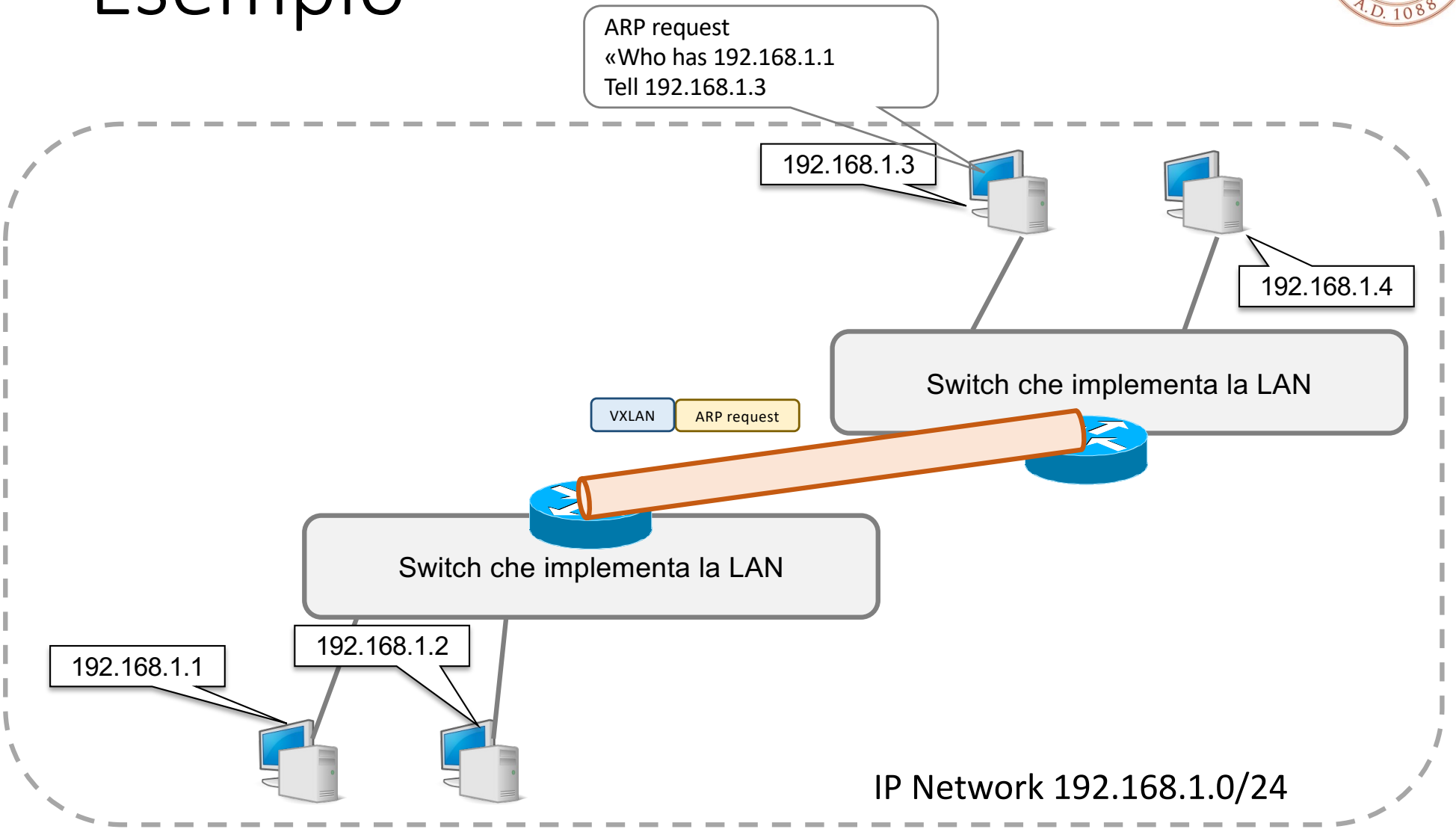
- Una sola network IP estesa sulla rete globale
- VXLAN trasporta i frame Ethernet sulla rete di interconnessione IP



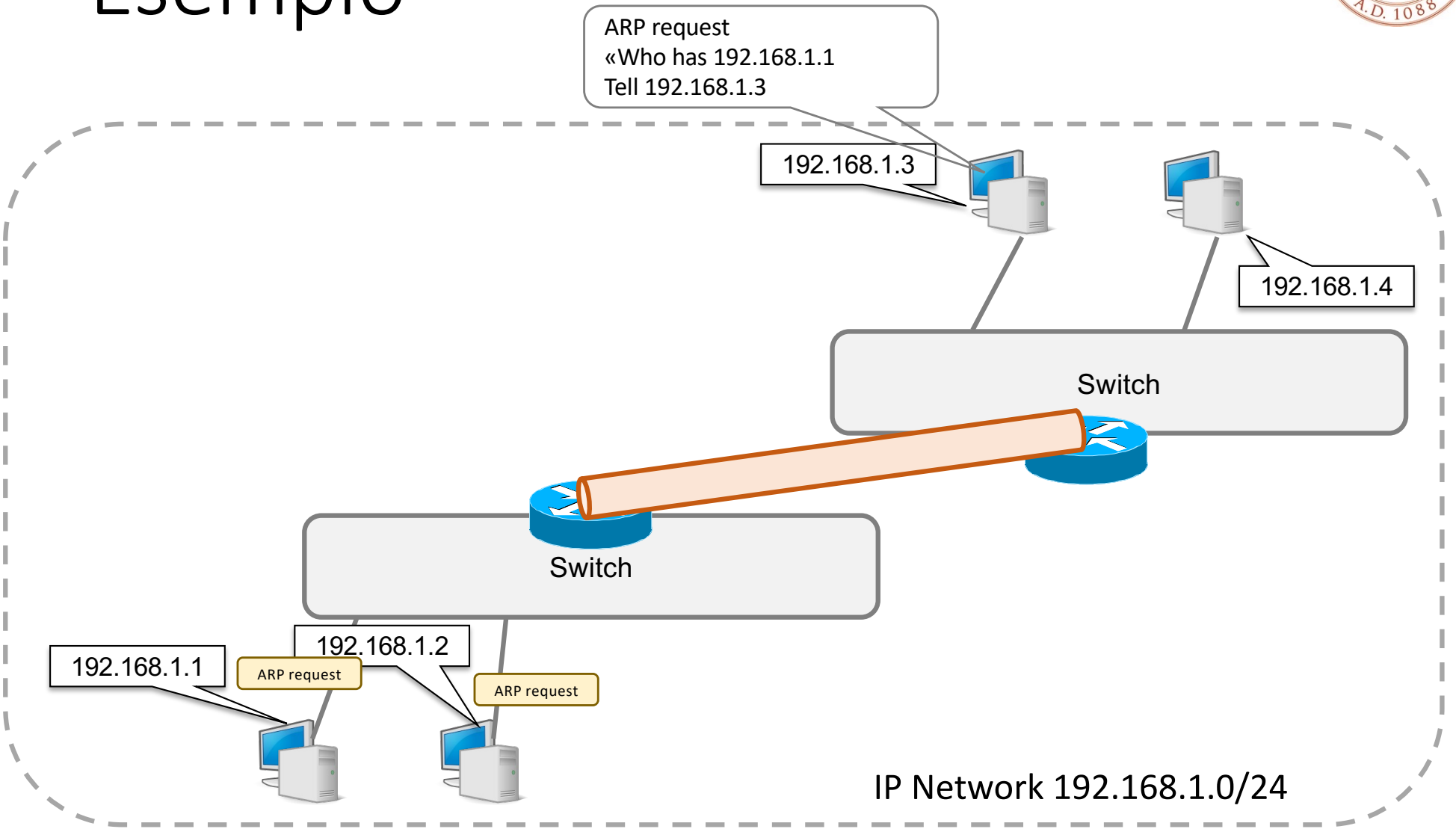
Esempio


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

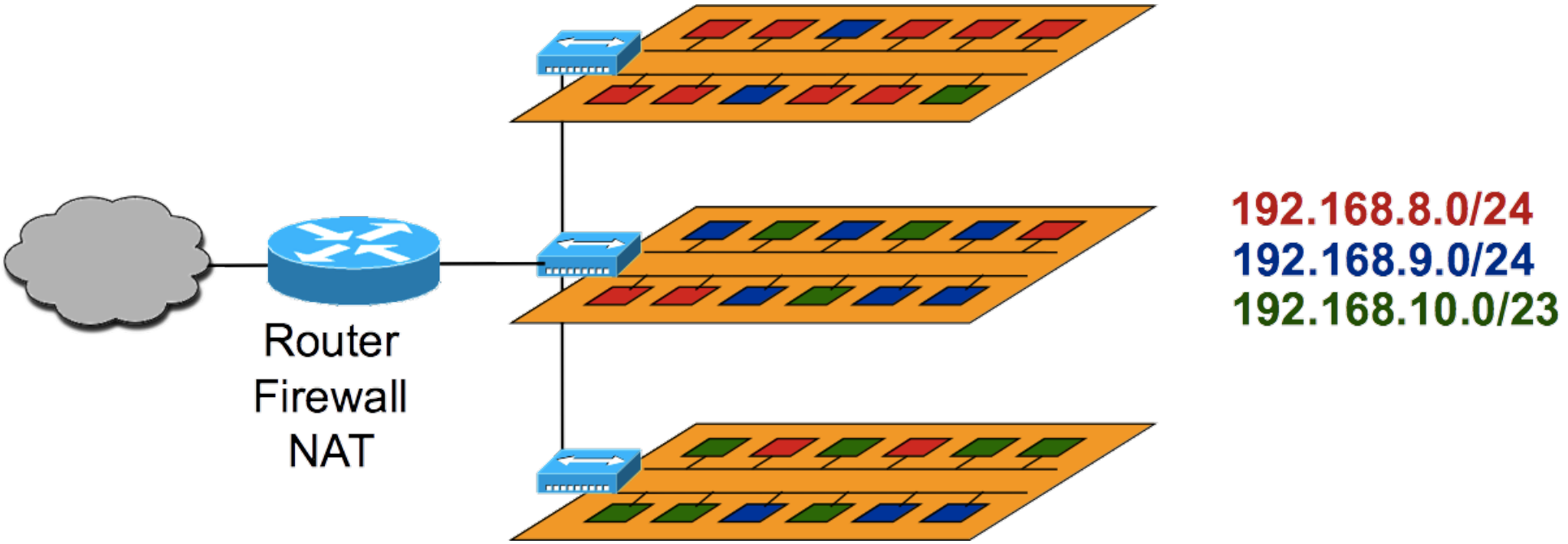

ARP request
«Who has 192.168.1.1
Tell 192.168.1.3
192.168.1.3
192.168.1.4
Switch
Switch
192.168.1.2
192.168.1.1
ARP request
ARP request
IP Network 192.168.1.0/24

Il dominio di broadcast

- Quando il dominio di broadcast è uno solo
  - Un broadcast inviato da un calcolatore 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
  - *Sicurezza*: i pacchetti broadcast possono essere utilizzati per studiare la topologia di rete e/o per tentare attacchi alla sicurezza della rete stessa

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

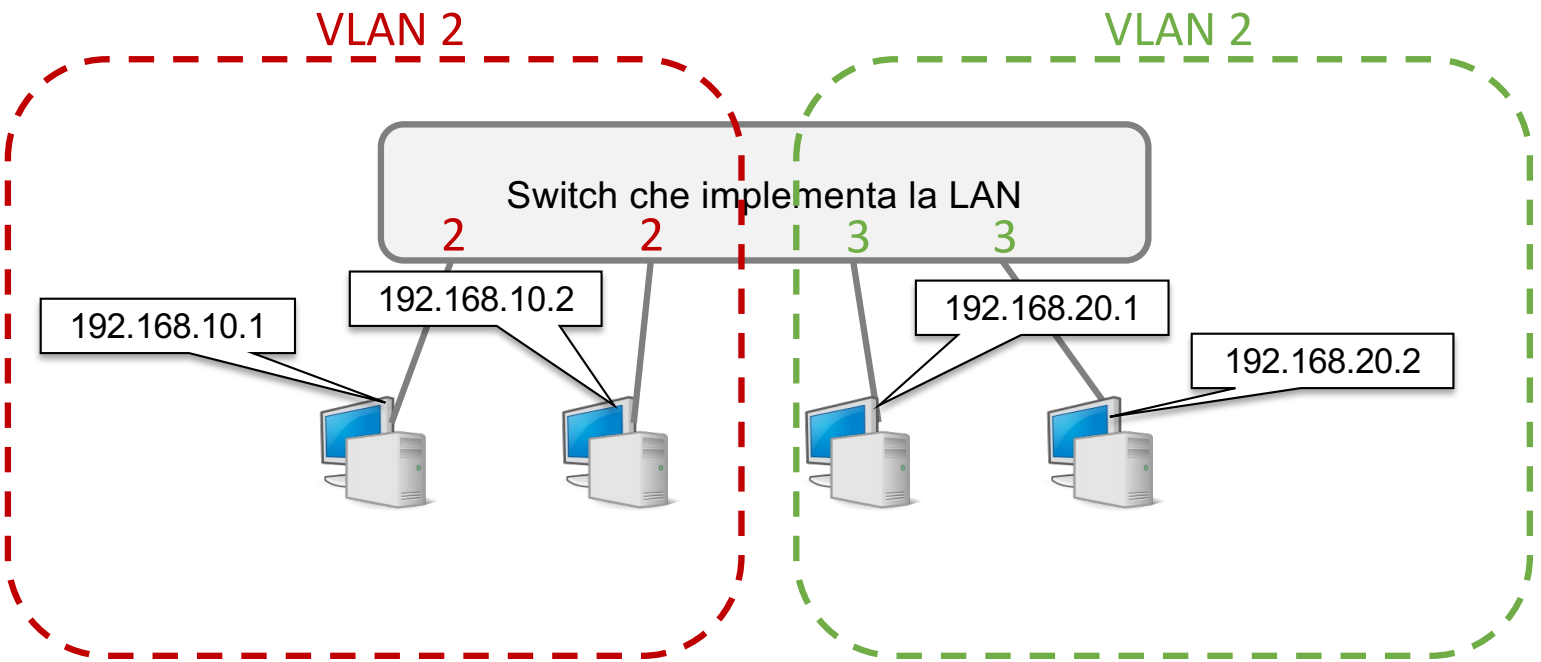


Classificazione delle VLAN

- 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

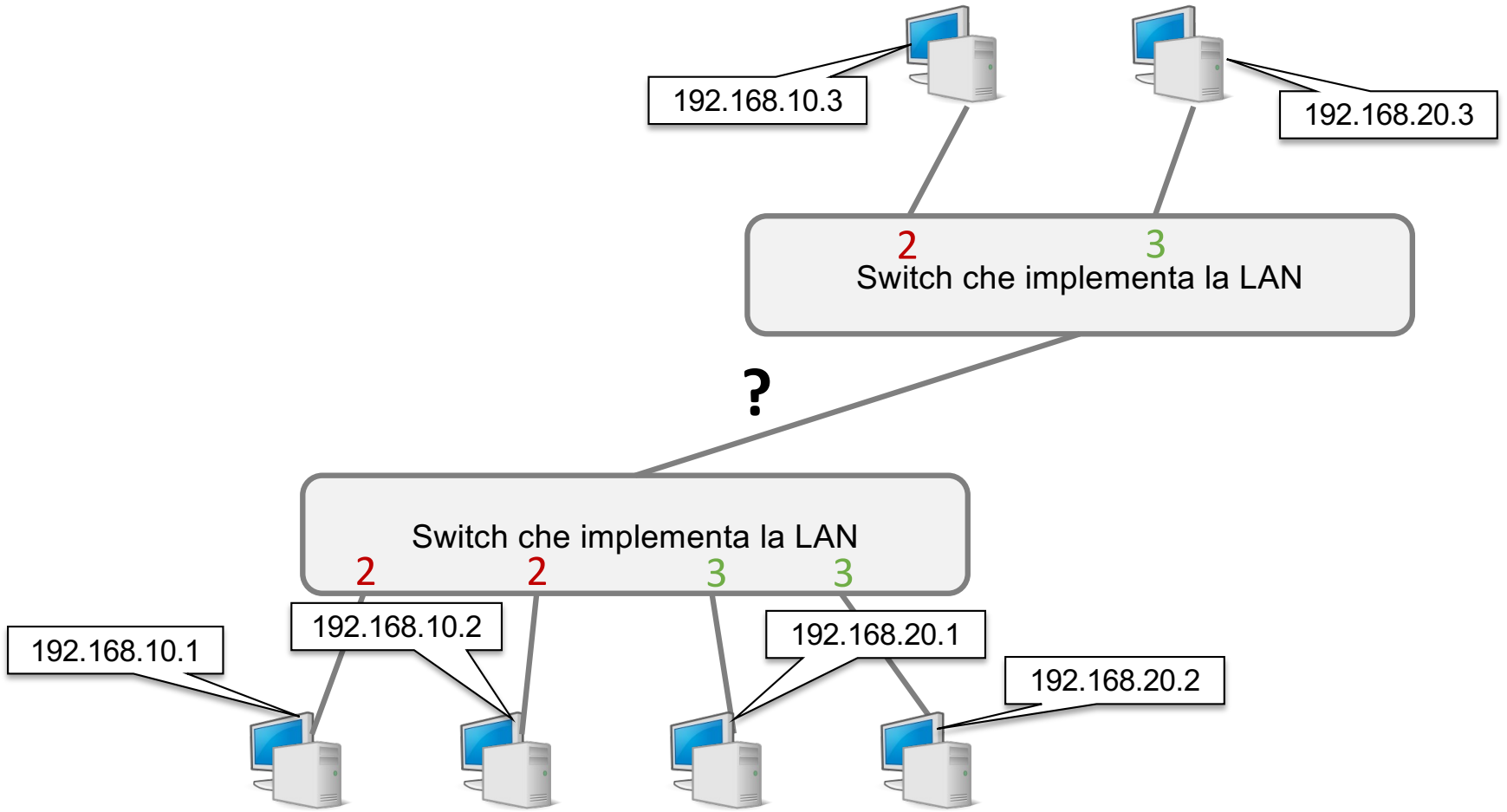
VLAN statica

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



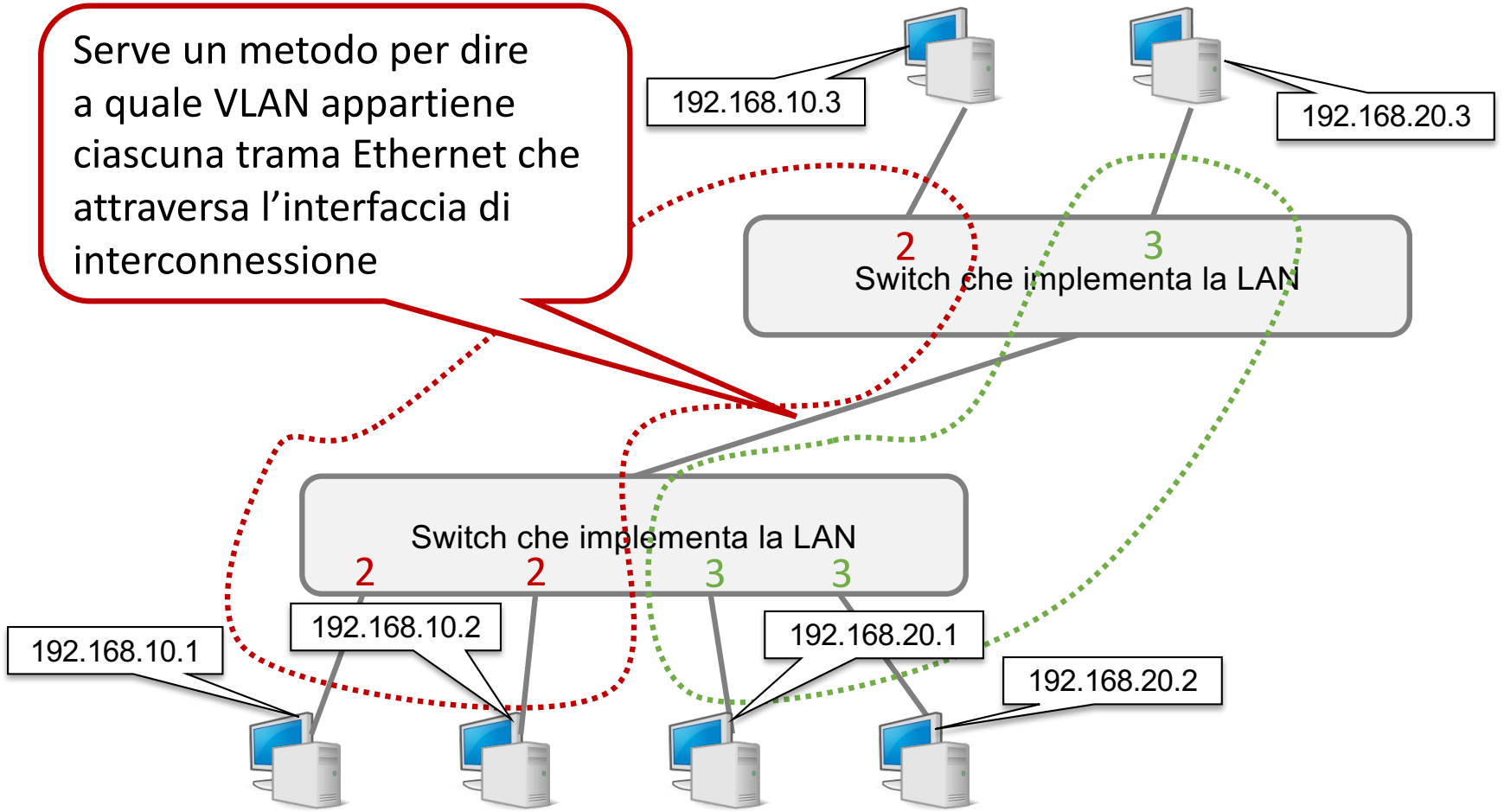
LAN estesa

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



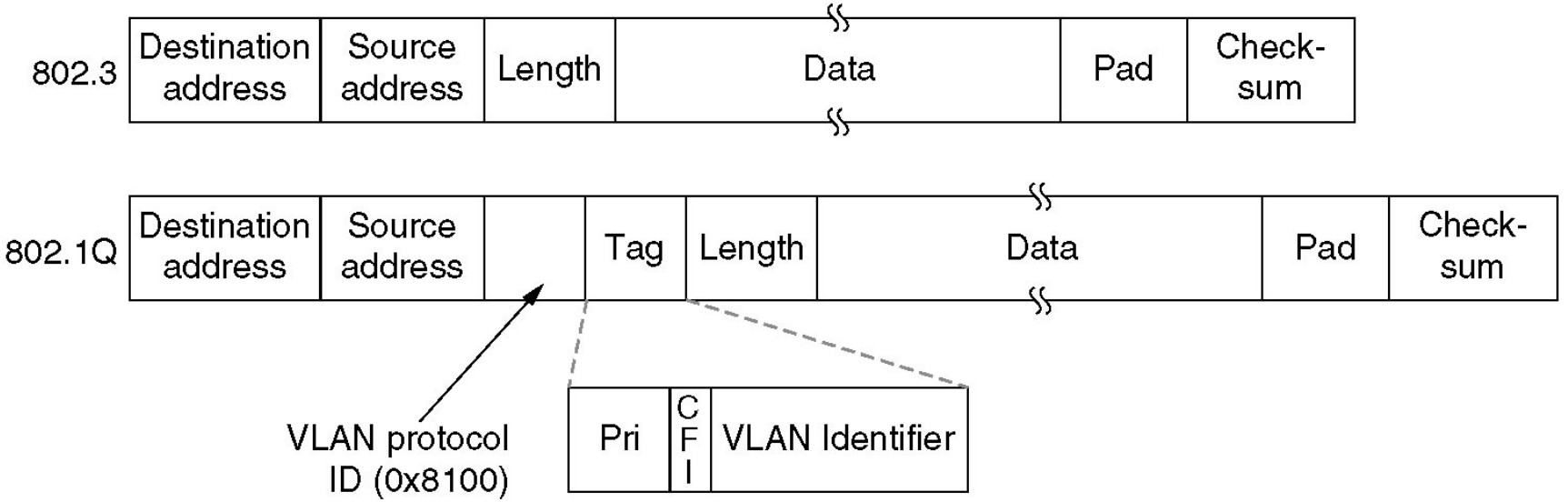
LAN estesa

- 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)

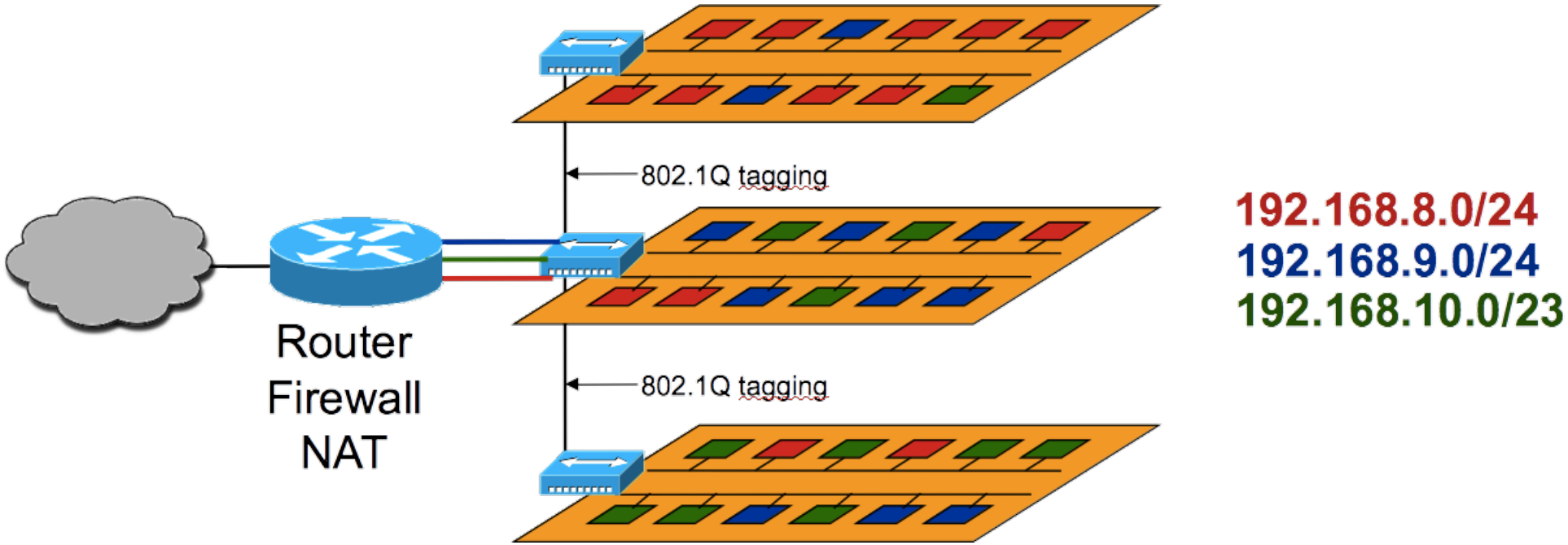
Porte dello switch

- 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

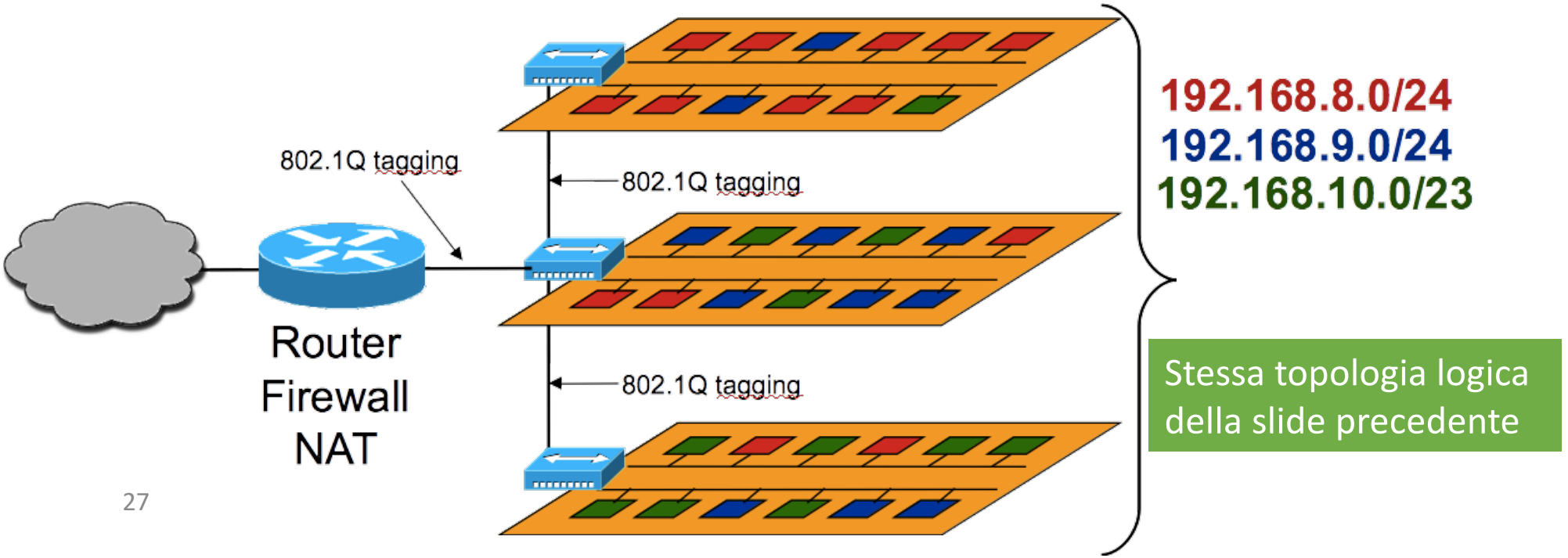
Inter-VLAN routing

- 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

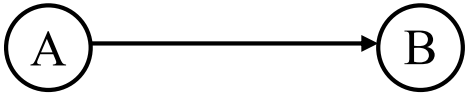
- Più efficiente e scalabile l'utilizzo di interfacce virtuali, o sub-interfacce
  - unica interfaccia fisica compatibile con il tagging 802.1Q
  - n interfacce virtuali sulla stessa interfaccia fisica
  - ogni sub-interfaccia utilizza il VLAN ID corrispondente alla sua VLAN



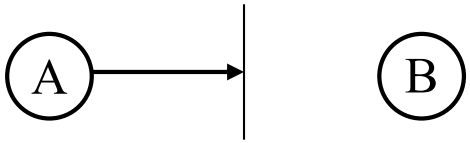
Reti private e reti private virtuali

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

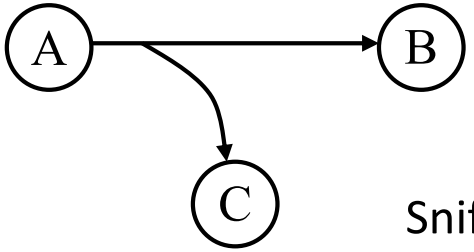
I rischi della comunicazione remota



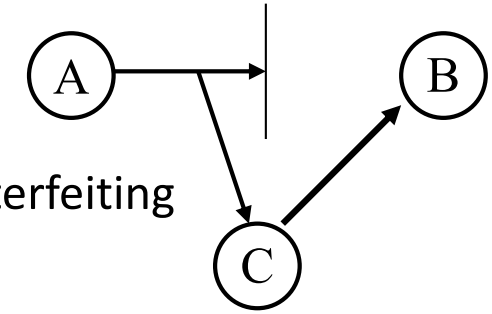
Normal information flow



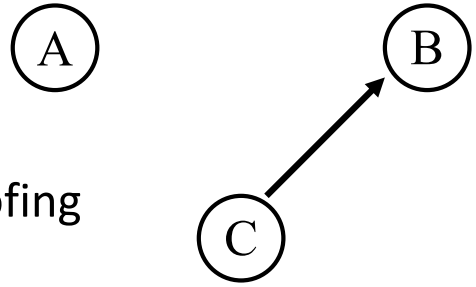
Blocking



Sniffing



Counterfeiting

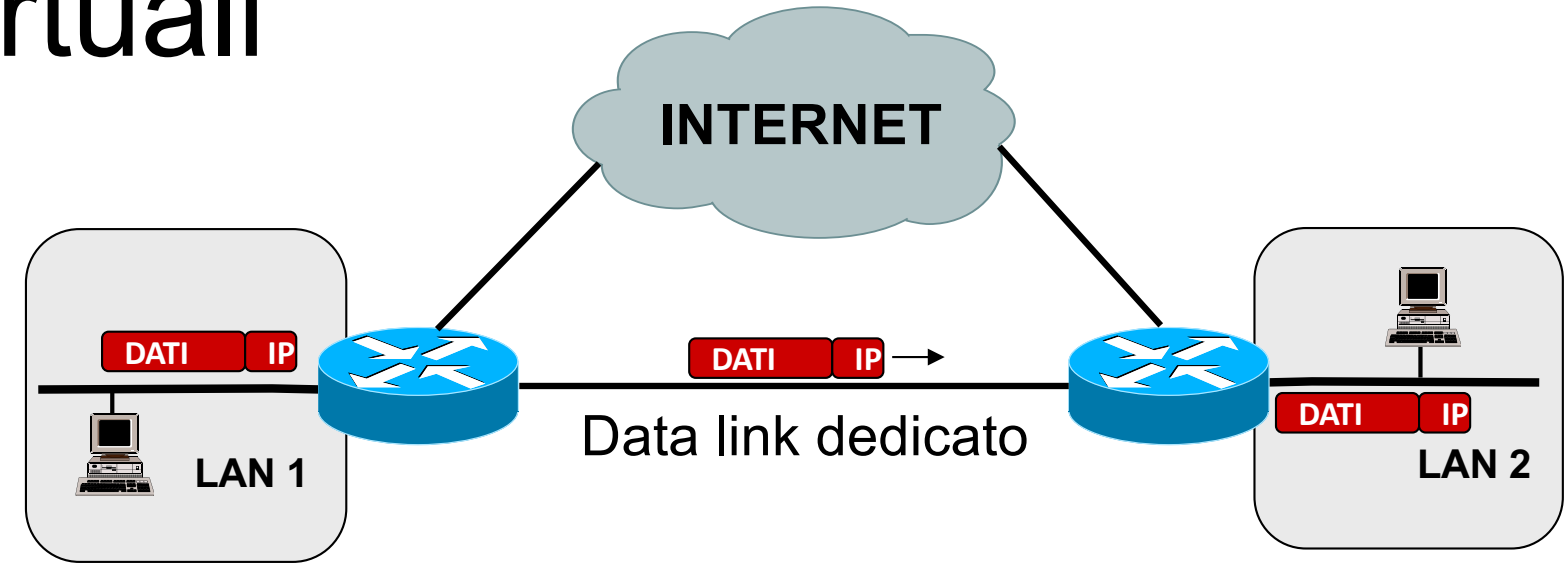


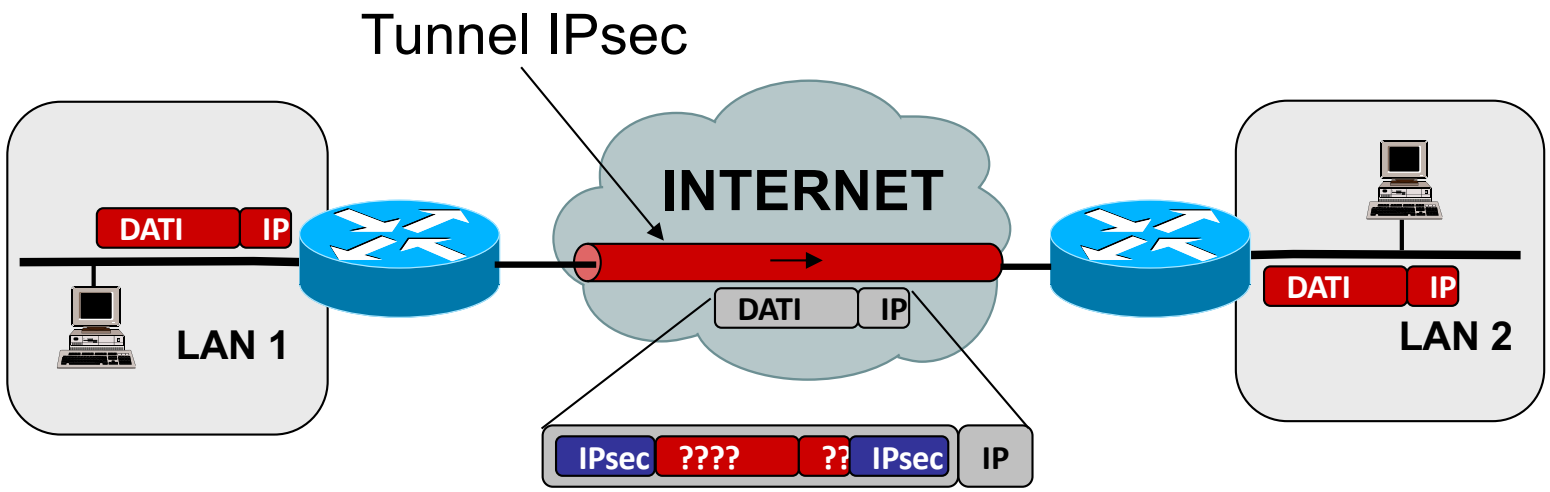
Spoofing

Obiettivi di una rete privata

- Riservatezza
  - Le informazioni non sono leggibili da tutti
- Autorizzazione
  - Definisco il sottoinsieme di coloro che sono in grado di leggere i dati
- Autenticazione
  - Verifico chi sta leggendo i dati
- Paternità
  - Garantisco l'origine dei dati

Reti private reali e reti private virtuali



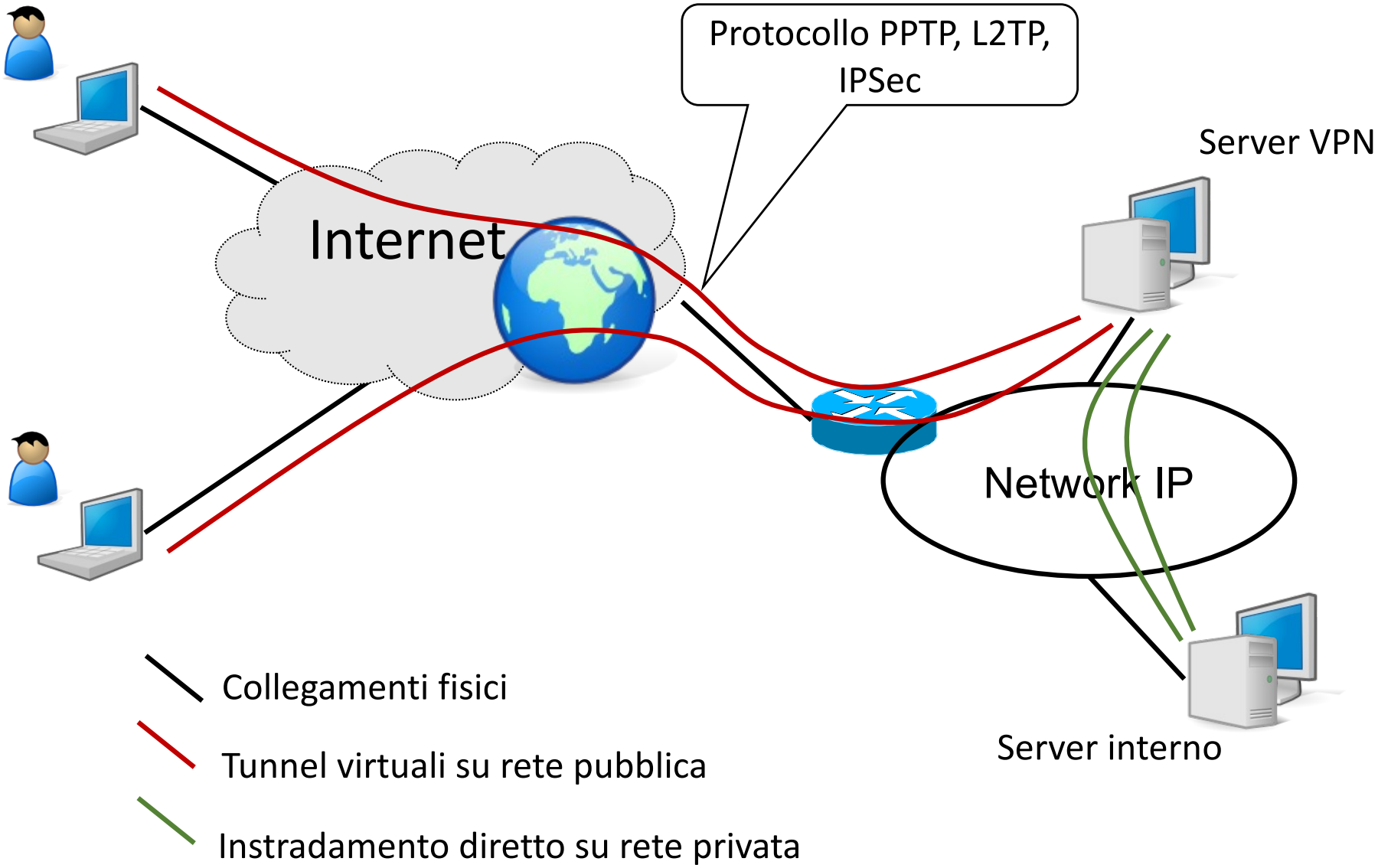


VPN Roadwarrior

- 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

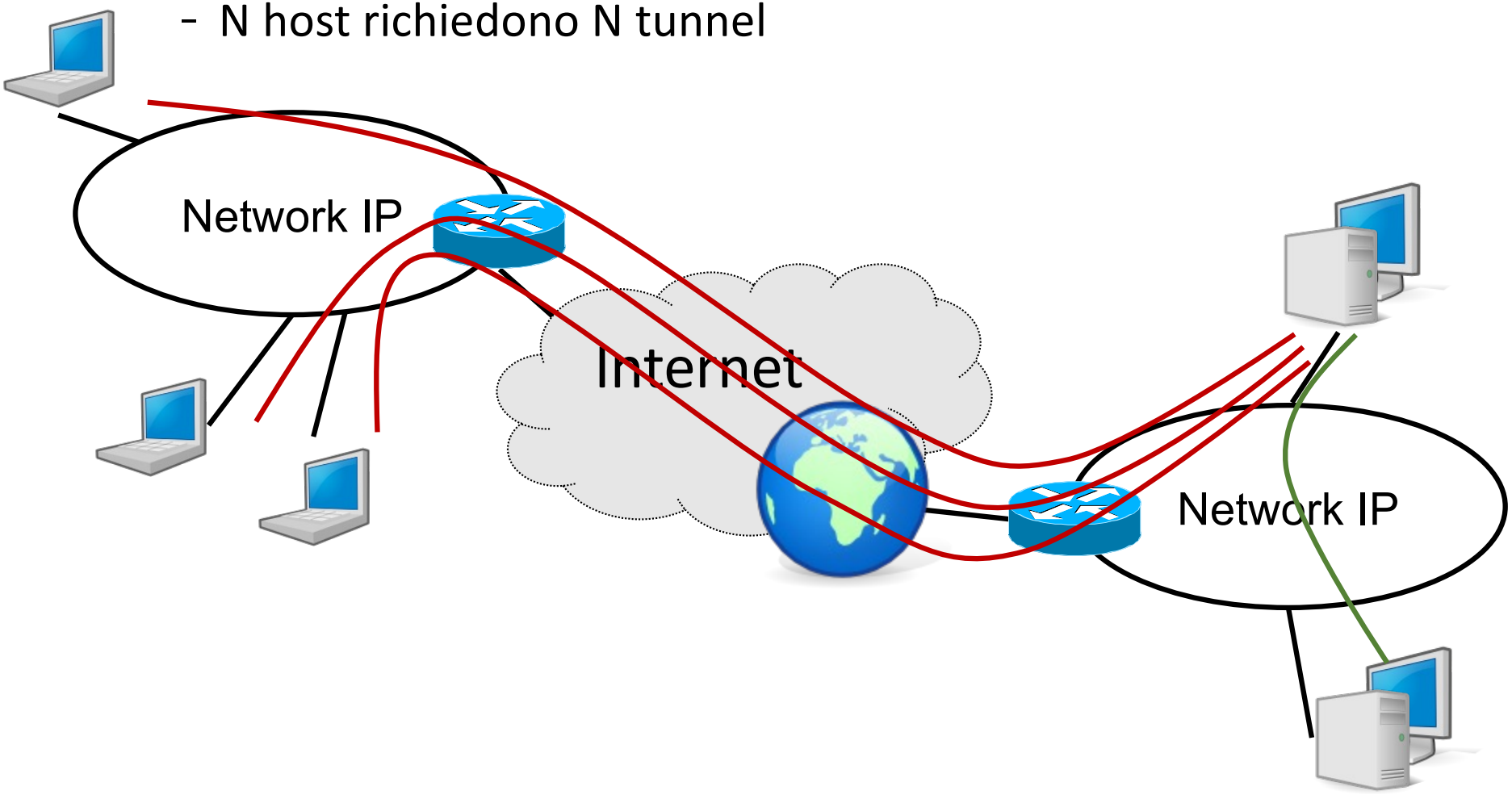
- Si configura come una rete di comunicazioni sicure sul server VPN

Roadwarrior



Problema

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

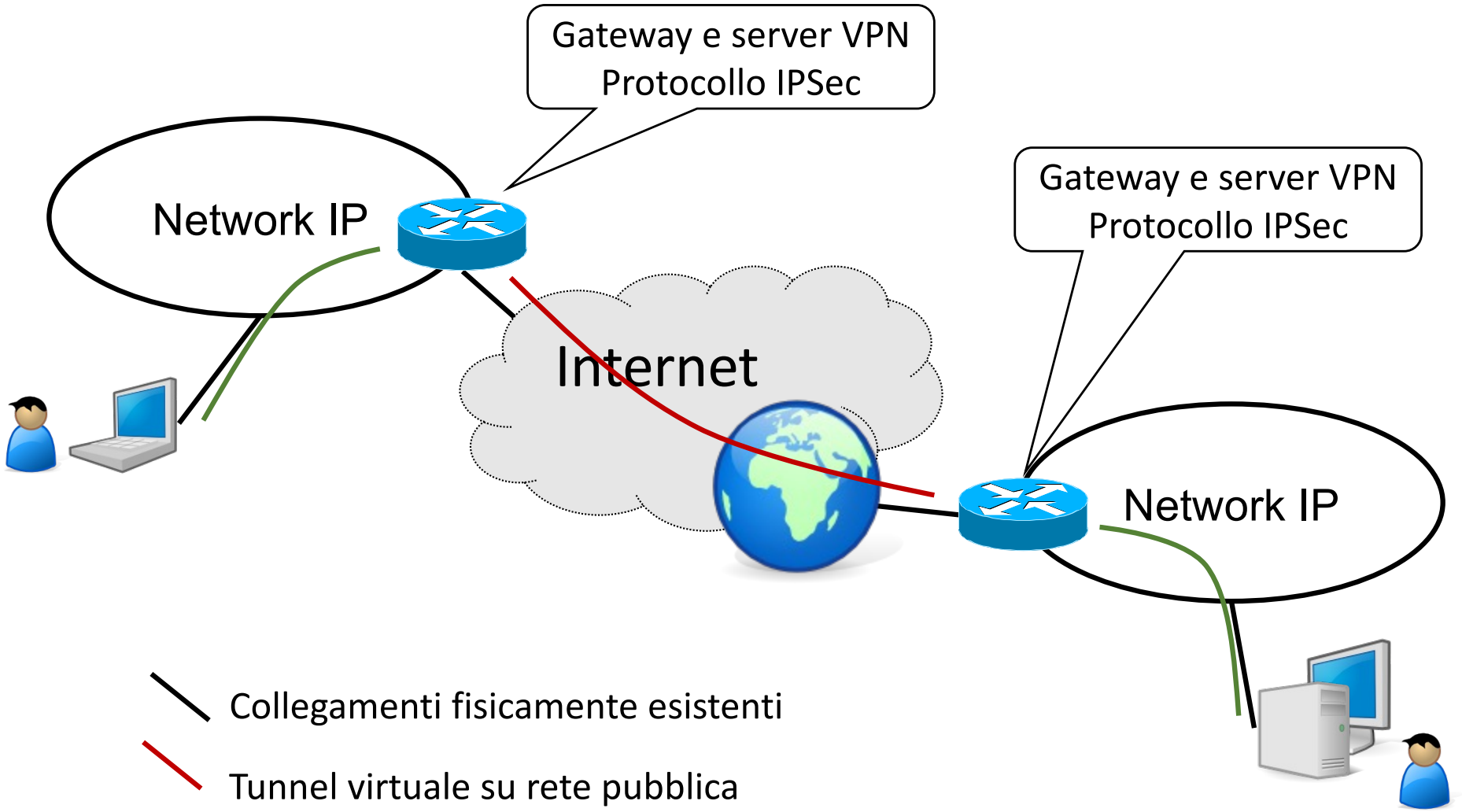


VPN da rete a rete

- 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

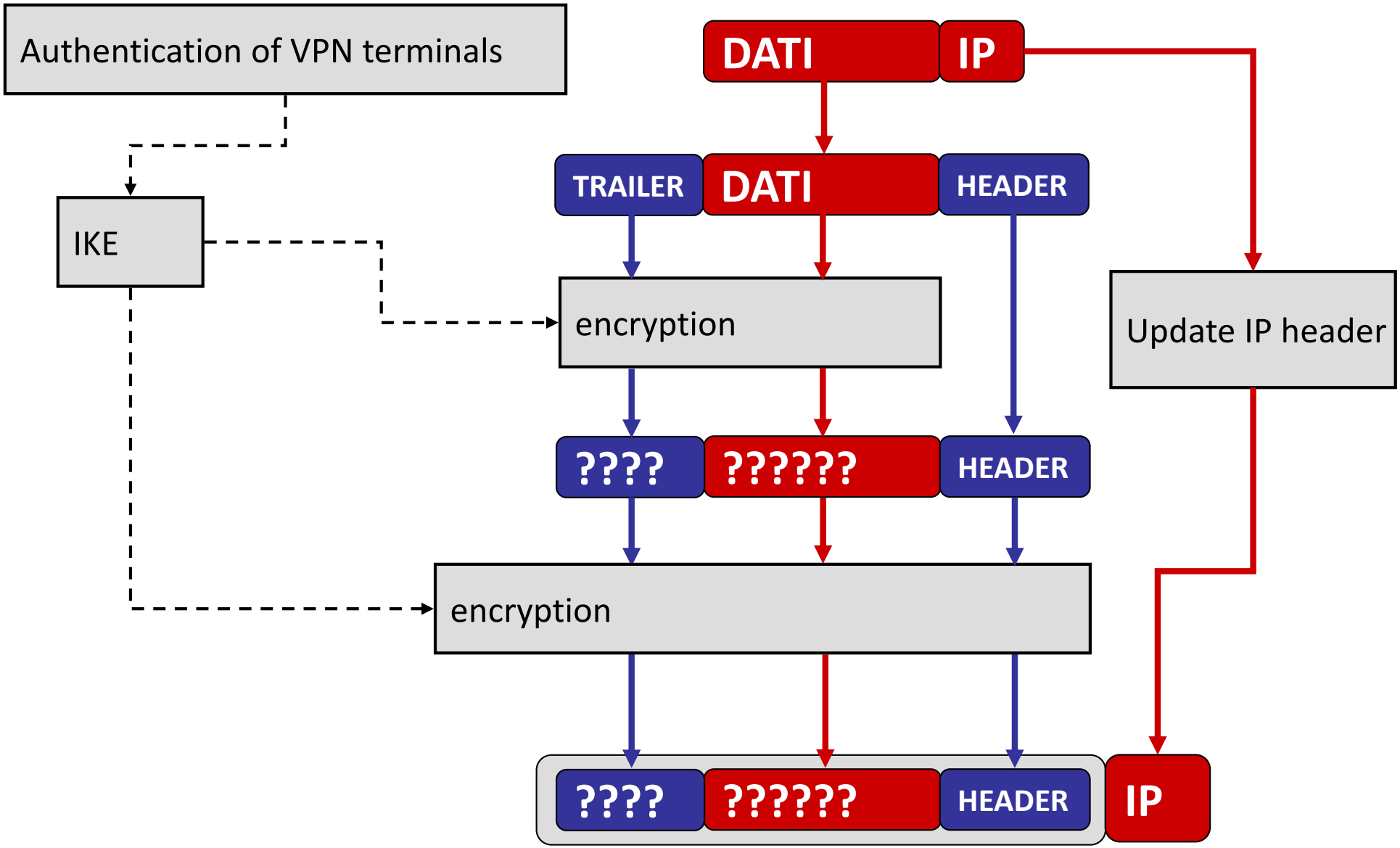
Protocolli

- 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

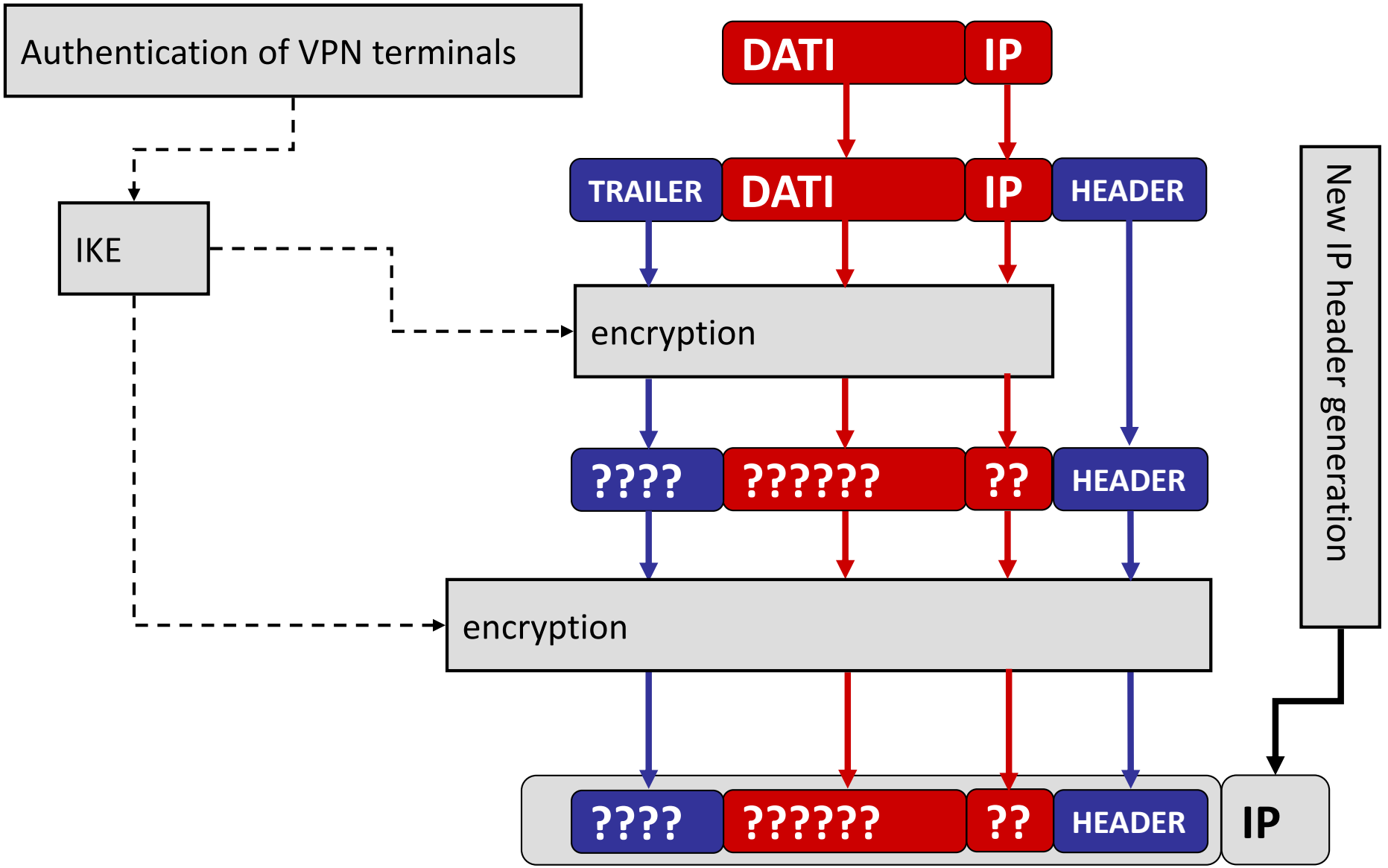
IKE

- 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