Transparent Networking e tecnologie di virtualizzazione della rete

M. Caberletti (INFN-CNAF)
A. Brunengo (INFN Genova)

Sommario

- Networking nel Cloud Computing
- Virtualizzazione della rete
- Soluzioni di virtualizzazione
- WNoDeS Dynamic Virtual Networks

Introduzione

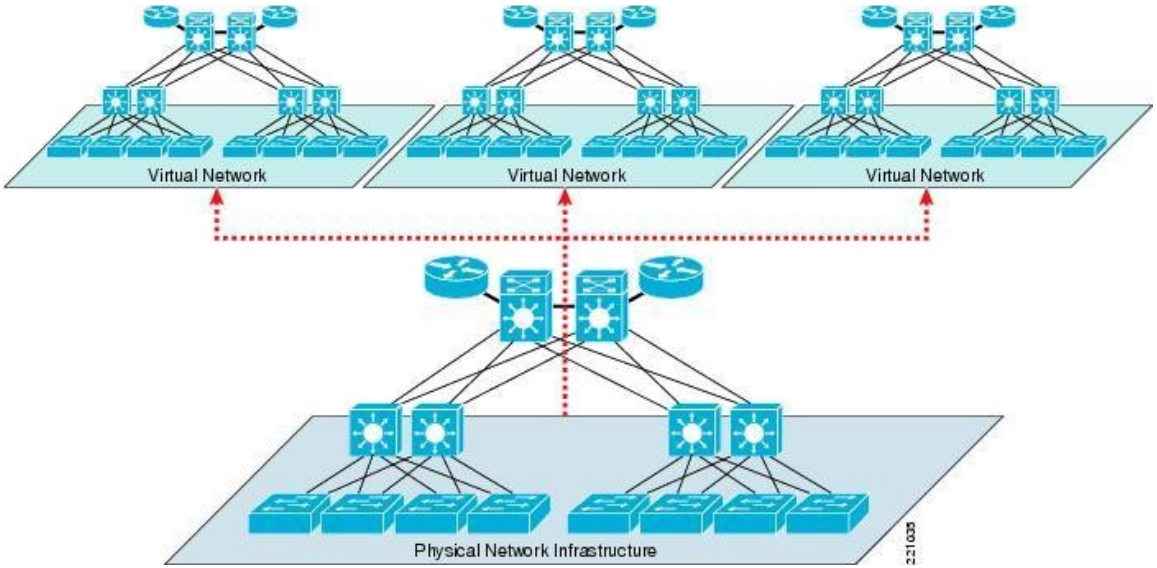
- Costante crescita di servizi on-line e di applicazioni on-demand.
- Nuove sfide per le reti di nuova generazione in termini di **capacità**, **configurabilità**, e **resilienza**.
- Occorre costruire reti con architetture e tecnologie scalabili, in termini di costo, dimensioni e consumo energetico;
- Devono essere in grado di gestire elevati volumi di traffico e poter cambiare dinamicamente la propria configurazione.

Cloud Computing

- Utilizza la virtualizzazione per costruire un'infrastruttura dinamicamente scalabile e soddisfare i requisiti di applicazioni eterogenee
- Un ambiente che fa largo uso della virtualizzazione è caratterizzato da alta **mobilità** delle entità (VM)
- In un Cloud IaaS, gli utenti richiedono di accedere alle proprie risorse con privilegi di amministratore: problemi di **sicurezza**

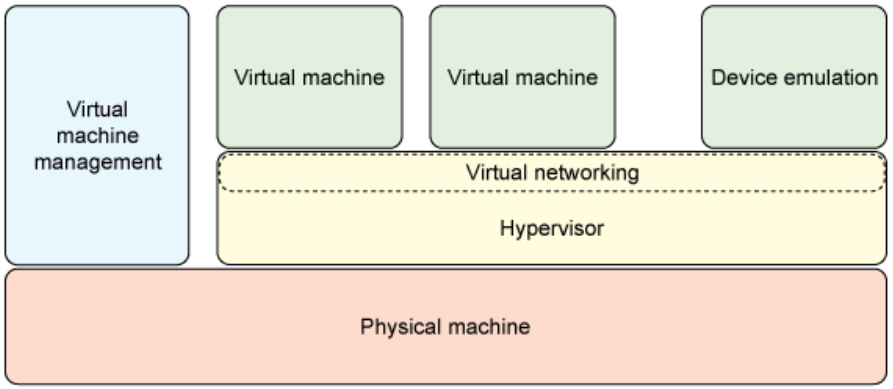
Virtualizzazione di rete

- Processo di combinazione di hardware, software e funzionalità di rete in una singola entità software-based, detta rete virtuale (*virtual network*).
- Proprietà:
  - scalabilità
  - resilienza
  - sicurezza
  - disponibilità



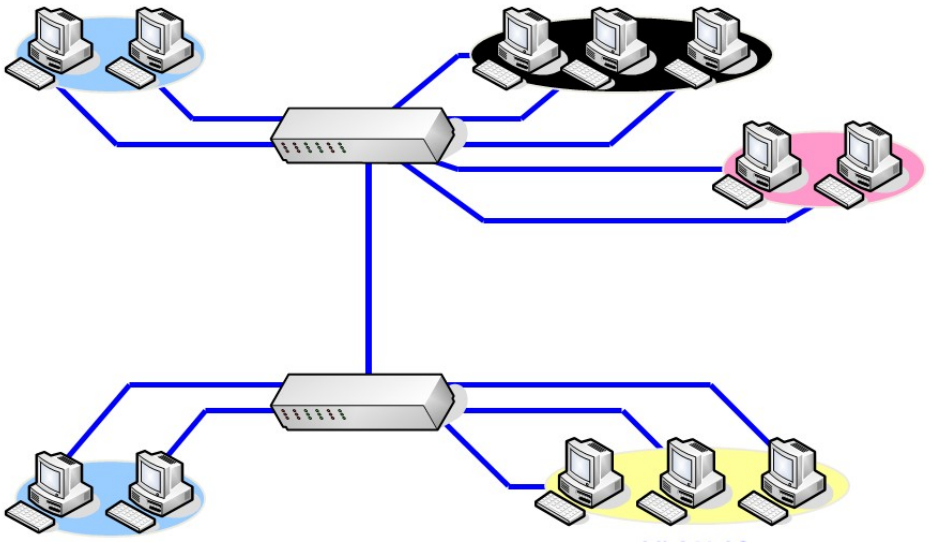
Virtualizzazione interna

- Mira a fornire funzionalità di rete all'interno di un singolo host fisico ("*network in a box*").
- Migliora l'efficienza complessiva permettendo l'isolamento delle applicazioni
- Con l'uso della virtualizzazione si possono combinare l'uso di bridge, switch e router virtuali per realizzare reti fra le VM.



Virtualizzazione esterna

- Mira all'unione (o suddivisione) di più reti o parti di reti in un'unica (o più) entità virtuale.
- Lo scopo è di migliorare l'efficienza d'uso di una rete di grandi dimensioni.
- Esempio tipico è l'uso delle VLAN per "separare" host connessi ad uno stesso switch fisico e "unire" host connessi a device diversi.

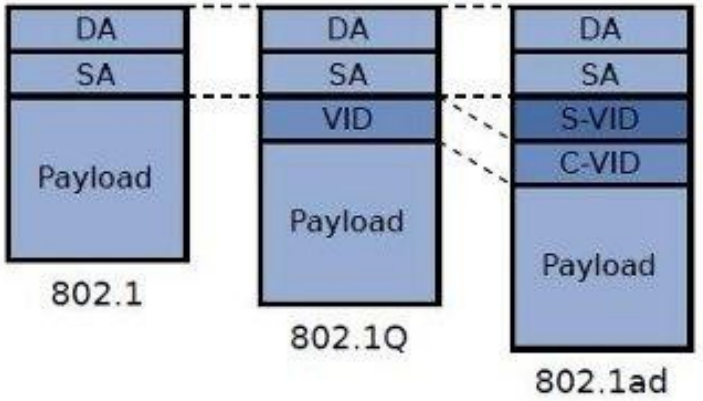


Soluzioni di virtualizzazione

- VLAN tagging
- Labeling
- Tunneling
- OpenFlow

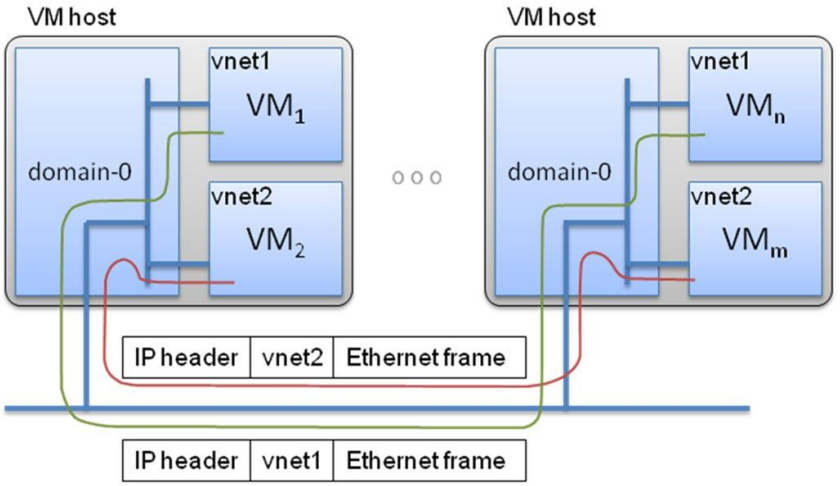
VLAN tagging

- Alterazione dell'intestazione Ethernet per aggiungere un campo (*tag*) che identifica un flusso di pacchetti
- Esempi: 802.1Q e 802.1ad
- Come soddisfa i requisiti?
  - Scalabilità : limite di 4096 tag (in 802.1q)
  - Resilienza : dipende dagli switch fisici/virtuali
  - Disponibilità : dipende sempre dagli switch
  - Sicurezza : gestione dei tag è compito degli switch
  - Trasparenza : le applicazioni ignorano i tag
  - Mobilità : configurazione poco dinamica



Labeling

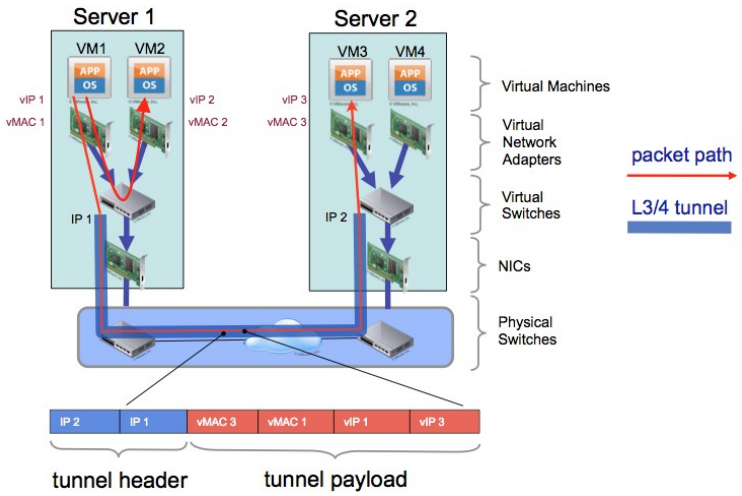
- Aggiunta di un header fra intestazione IP e Ethernet.
- Concetto analogo al tagging, con qualche sostanziale differenza
- Esempio: MPLS, ViNE, SoftUDC



- Come soddisfa i requisiti?
  - Scalabilità : nessun limite fisso al numero di reti virtuali
  - Resilienza : dipende dagli switch fisici/virtuali usati
  - Disponibilità : dipende sempre dagli switch
  - Sicurezza : gestione label è compito degli switch
  - Trasparenza : le applicazioni ignorano le label
  - Mobilità : configurazione poco dinamica

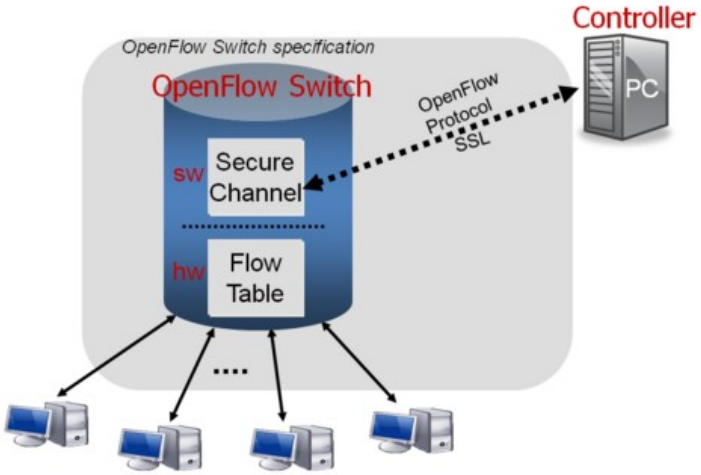
Tunneling

- Incapsulamento di datagram come payload del protocollo di tunneling.
- Esempi: IP-over-IP (IPIP, SIT), Ethernet-over-IP (GRE, VPN)
- Come soddisfa i requisiti?
  - Scalabilità : dipende dal protocollo
  - Resilienza : dipende dalla rete IP
  - Disponibilità : dipende dalla rete IP
  - Sicurezza : dipende dal protocollo e dal tipo di deployment
  - Trasparenza : le applicazioni ignorano l'incapsulamento e la rete fisica non vede le reti virtuali
  - Mobilità : riconfigurazione dei tunnel



OpenFlow

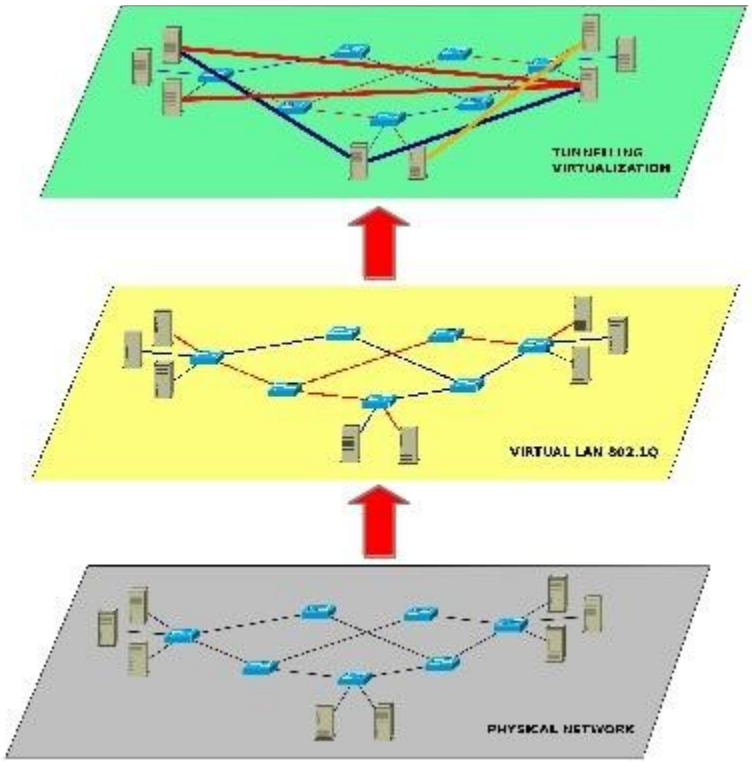
- Protocollo standard, permette di controllare i device di rete attraverso software che risiede su di un controller esterno.
- Realizza reti in grado di modificare il proprio comportamento in base alle condizioni al contorno (*Software Defined Networks*).



- Come soddisfa i requisiti?
  - Scalabilità : ???
  - Resilienza : dipende dal controller
  - Disponibilità : dipende dal controller
  - Sicurezza : ???
  - Trasparenza : completamente trasparente all'utente, non per la rete fisica
  - Mobilità : intrinseca in OpenFlow

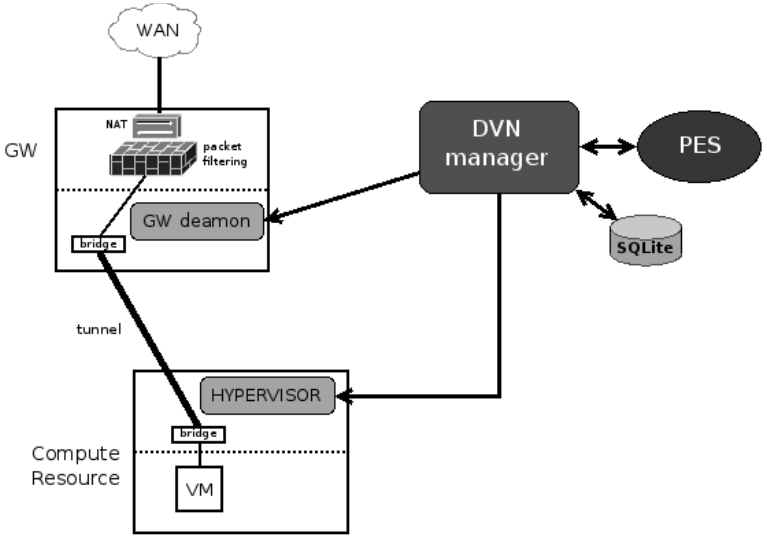
WNoDeS Dynamic Virtual Networks

- Nei centri di calcolo di dimensioni significative la definizione dinamica di reti virtuali risulta problematica
- L'approccio a tunneling permette di creare reti virtuali senza modificare il setup di rete
- WNoDeS DVN propone una soluzione di virtualizzazione basata su GRE



Architettura di DVN

- Tutto il traffico dell VM circola nei tunnel
- Topologia "Hub and Spoke"
- Ogni rete virtuale usa tunnel separati per garantire l'isolamento
- Implementato interamente con tool Linux (iproute, iptables, bridge)
- Ogni rete virtuale usa una subnet privata



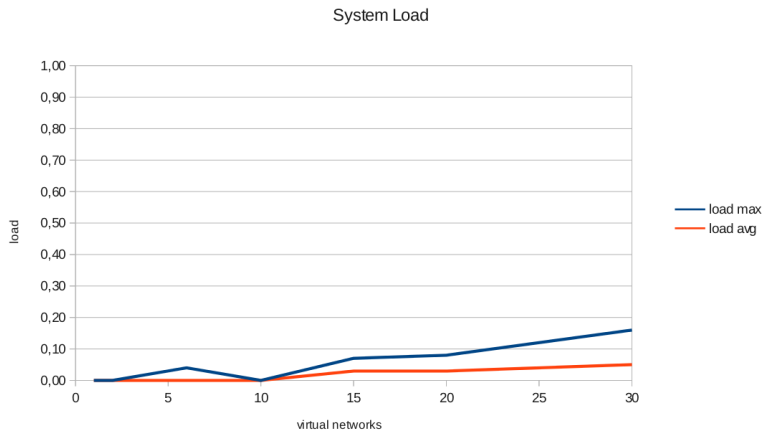
- Componenti:
  - DVN Manager gestisce il deployment delle reti virtuali utilizzando un database (SQLite)
  - Policy Enforcement Service gestisce le regole di controllo del traffico
  - Il nodo GW fa da GRE Gateway verso altri segmenti di rete
  - Il nodo GW può essere ridondato mediante Heartbeat

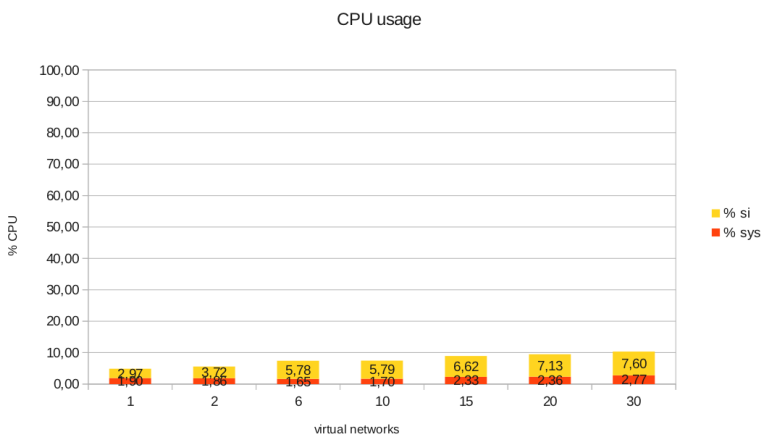
Caratteristiche di DVN

- Scalabilità
  - limite imposto dal pool di sottoreti
- Resilienza
  - legata al funzionamento del nodo GW
- Disponibilità
  - legata al GW
- Mobilità
  - l'inclusione/esclusione di nodi fisici e/o virtuali richiede operazioni semplici: l'aggiunta/rimozione di tunnel, modifica regole iptables
- Trasparenza
  - valgono le considerazioni fatte per il tunneling

Performance tests

- Test di carico per valutare il comportamento del nodo GW al crescere del numero di reti virtuali attive (traffico generato mediante *iperf*)





- Delay nel RTT:
  - 0,020 ms dovuti al processo d'incapsulamento del SO dell'hypervisor
  - 0,150 ms dovuti alla presenza del nodo GW (hop aggiuntivo)

Evoluzione di DVN

- Multicast address come remote IP
- Interconnessione multi-sito
- Utilizzo di IPSEC
- Job Transparent Proxy
- Cluster-on-Demand
- VPN connection