

# GARR-T: Update e DC network

M. Carboni

Stato e modelli DC per le nuove sfide

2022-05-26

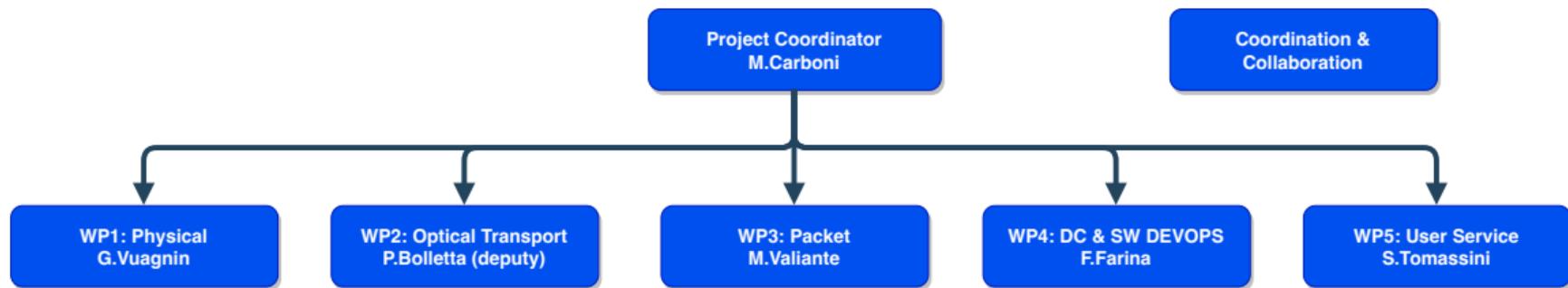


# Outline

---

- 1 GARR-T: Update 22Q1
  - Roadmap complessiva
  - Update Trasmissivo
- 2 Architettura Rete DC
  - Disegno rete locale
  - IP Fabric: DC Net
  - GARR-T Architecture: mDC Net
- 3 Modelli di DC geografici su larga scala
  - LAN vs WAN: differenze e punti contatto
- 4 Datalake: Architettura DRAFT-0.2

# Organizzazione del Progetto GARR-T



**WP1 - Physical** Infrastruttura fisica e POP

**WP2 - Optical Transport** Sistemi di Linea e Trasporto Ottico

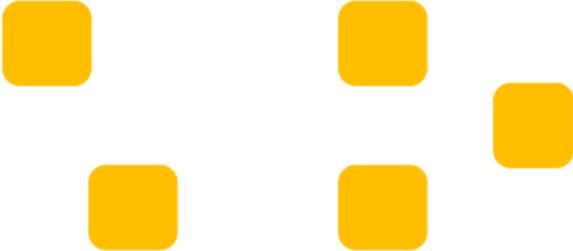
**WP3 - Packet** Sistemi a pacchetto e migrazione dei servizi di dorsale e utente

**WP4 - Automation & SW DevOps** Sviluppo, Gestione e Monitoraggio

**WP5 - Services** Consolidamento e Ampliamento proposta di servizi



# WP2 GARR-T: Trasmissivo Update



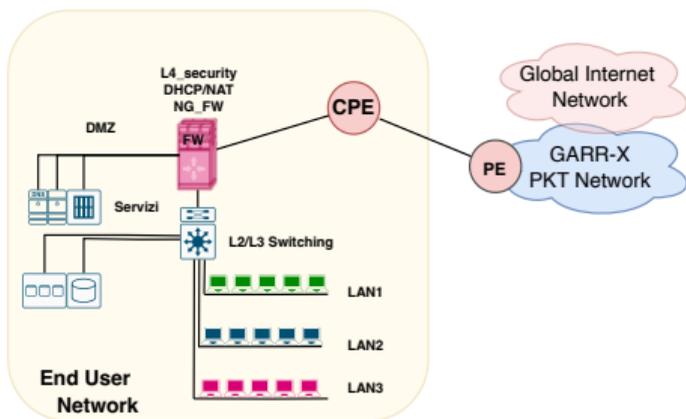
**FT** PKT

# Architetture Rete DC



# Schema di Rete “tradizionale”

Soluzione di rete base, non sono disponibili soluzioni avanzate, vi è una chiara separazione tra interno ed esterno. I servizi vengono gestiti attraverso le funzionalità di sicurezza fornite dal **Firewall** che può svolgere alcune funzioni aggiuntive a supporto delle tematiche di sicurezza connessa con attacchi "slow-and-low"



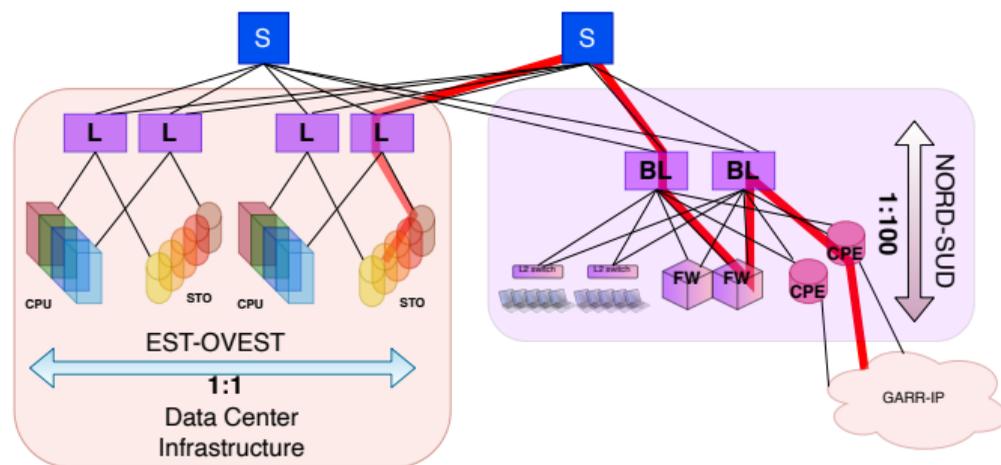
Svolge le tre distinte funzioni:

- CPE: separazione tra il dominio di routing interno e quello esterno
- firewall: svolge il ruolo di filtro (statefull L4) con funzione di NG-Firewall per traffici "noti"
- DMZ: è la LAN dei servizi esposti verso l'esterno
- L2/L3: sistema di rete interno L2/L3 funzionale alle prestazioni. Le funzioni di sicurezza sono svolte altrove
- LANx: rete locale utenti, non presenta servizi verso l'esterno, riceve solo traffico a partire da richieste dei client

# DC Network Architecture: IP Fabric

Elementi di rete:

- **Spine**: funzione di aggregazione. Rappresenta la matrice di switching delle soluzioni collassate
- **Leaf**: erogazione dei servizi lato client, garantisce la comunicazione nella medesima istanza di routing
- **Border Leaf**: funzionalmente equivalente alla **Leaf**, inferiore solo a livello di prestazioni complessive in quanto deve gestire traffico (nord-sud) dalla 10÷100 volte inferiore
- **Firewall**: svolge il ruolo di filtro (statefull L4) con funzione di NG-Firewall per traffici "noti"
- **CPE**: apparato di accesso alla rete IP

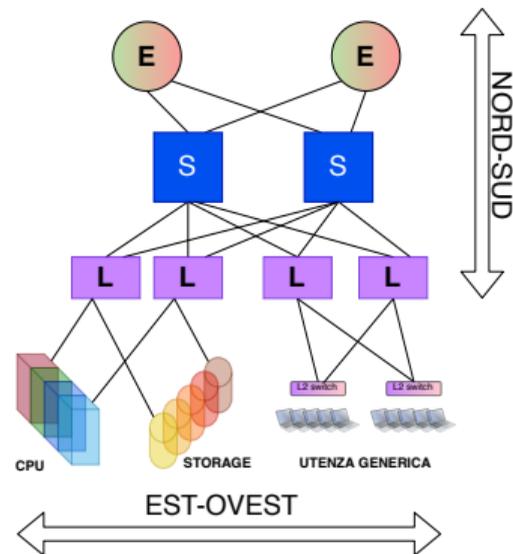


# GARR-T mDC Architecture: IP Fabric

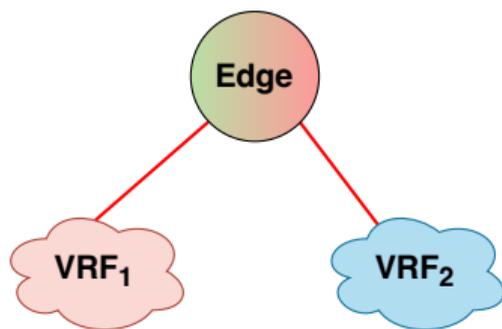
## Modello di Rete (IP Fabric) con funzioni collassate

Elementi di rete:

- **Spine**: funzione di aggregazione. Rappresenta la matrice di switching delle soluzioni monolitiche
- **Leaf**: erogazione dei servizi lato client, garantisce la comunicazione nella medesima istanza di routing
- **Edge**: demarcazione dominio esterno e quello interno. Mette in comunicazione diverse istanze di routing. Raccoglie insieme più funzioni: Leaf, Firewall, CPE



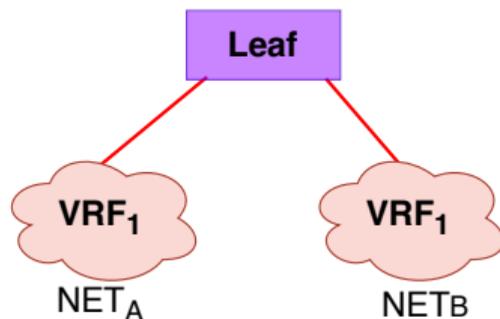
# Funzioni apparato di Edge



Svolge le tre distinte funzioni:

- "router" comunicazione tra istanze di routing separate
- "firewall" gestione del traffico line-rate con policy layer4 IP\_SRC,IP\_DST,P\_SRC,P\_DST
- "leaf" agisce a tutti gli effetti come elemento di erogazione dei servizi mettendo in comunicazione elementi appartenenti ad una determinata istanza di routing

# Funzioni apparato Leaf



Svolge le tre distinte funzioni:

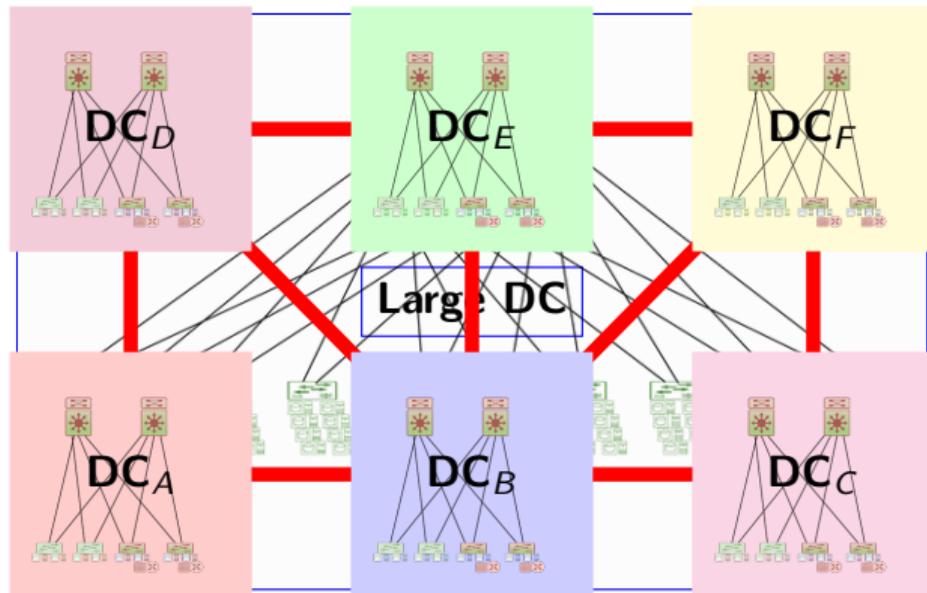
- "leaf" marca il traffico VLAN (VTEP) e determina la comunicazione "VXLAN over UDP/IP"
- "router" comunicazione tra VLAN differenti all'interno della stessa istanza di routing
- "firewall" gestione del traffico line-rate con policy layer4 IP\_SRC,IP\_DST,P\_SRC,P\_DST

## Modelli di DC geografici su larga scala



# LAN vs WAN: differenze e punti contatto

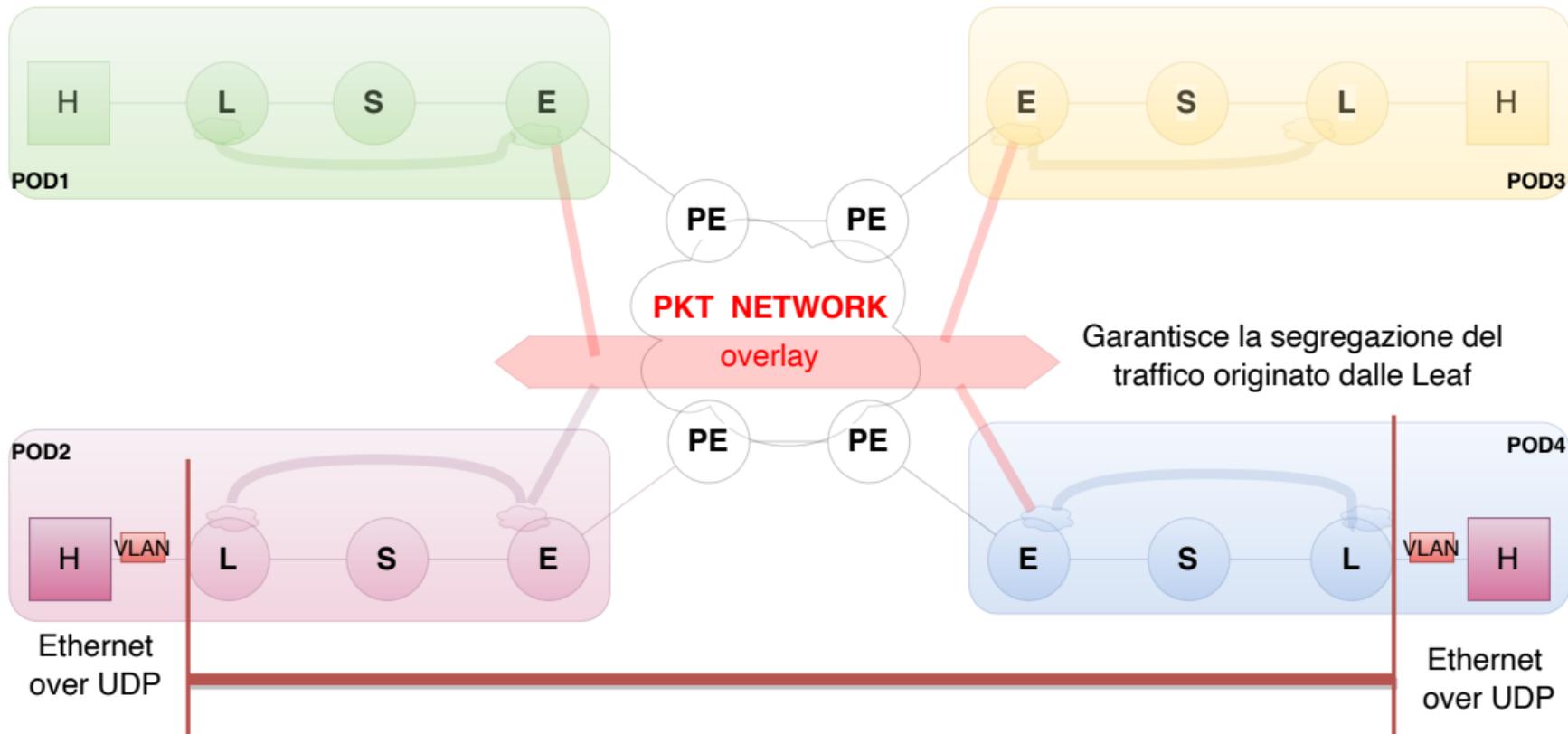
Costruzione di un Large DC a partire da mDC



## Arch e Funzioni DC multi Site

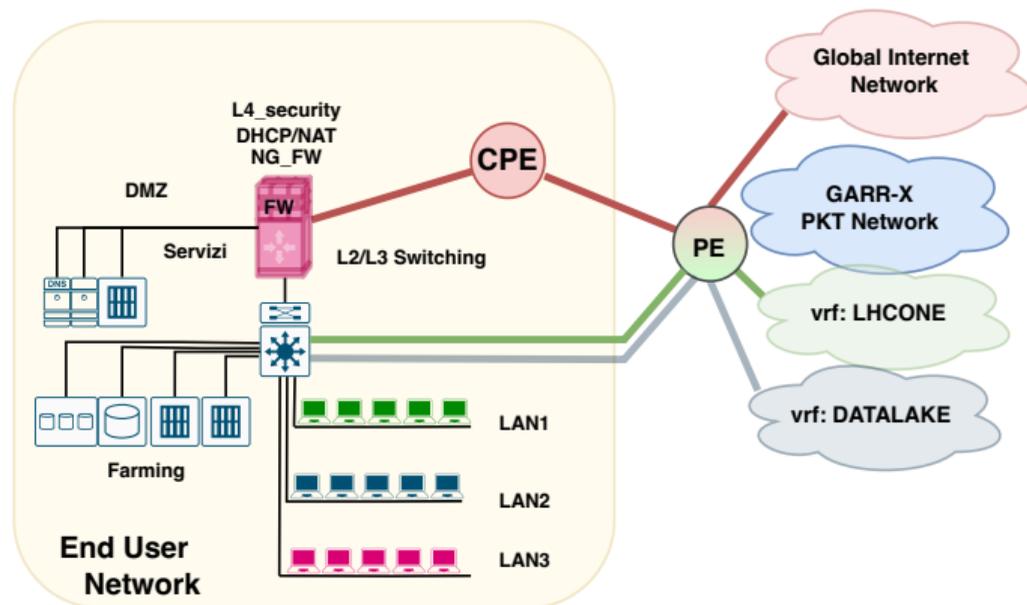


# Architettura e Funzioni di un DC distribuito multi Site



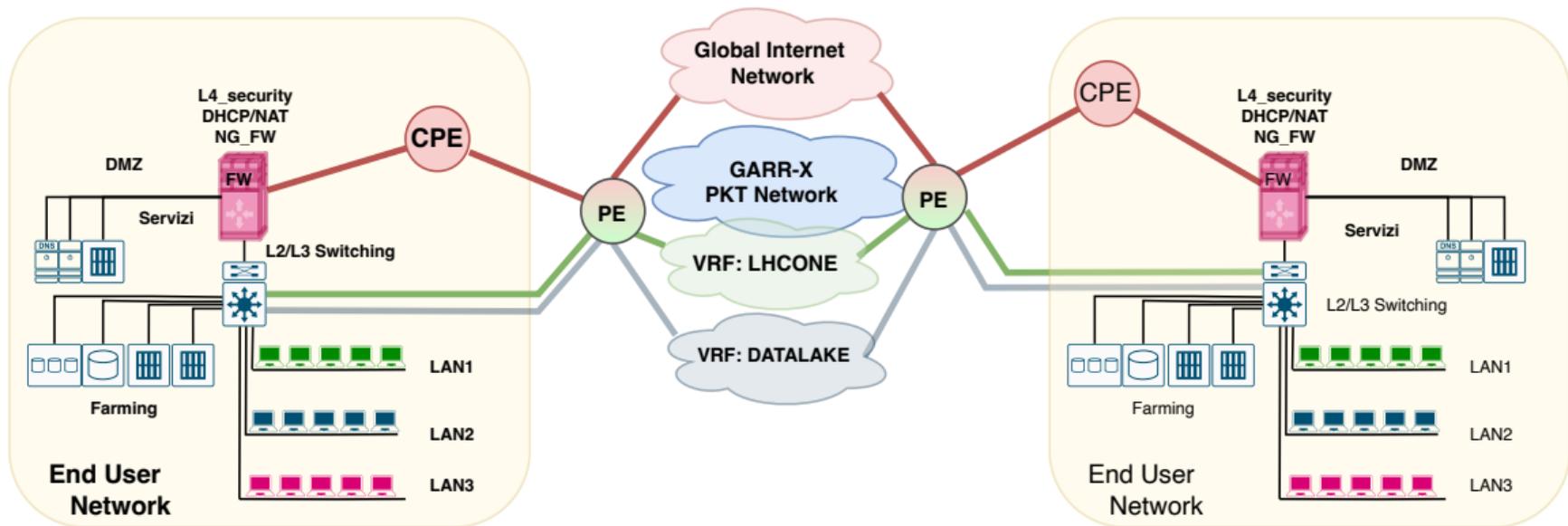
# LAN & DC Network: General Purpose & High Speed Network

- Global Internet: accesso *Global Internet*
- Packet Network: rete di *trasporto nazionale GARR*
- LHCONE: rete HTC dedicata *Science DMZ*
- DATALAKE: istanza di routing segregata su scala nazionale

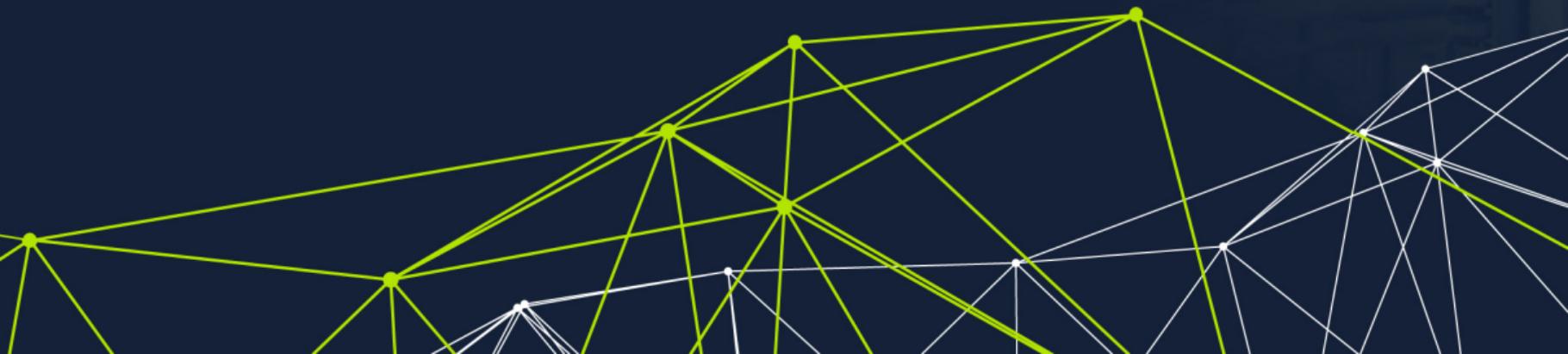


# Multi VRF

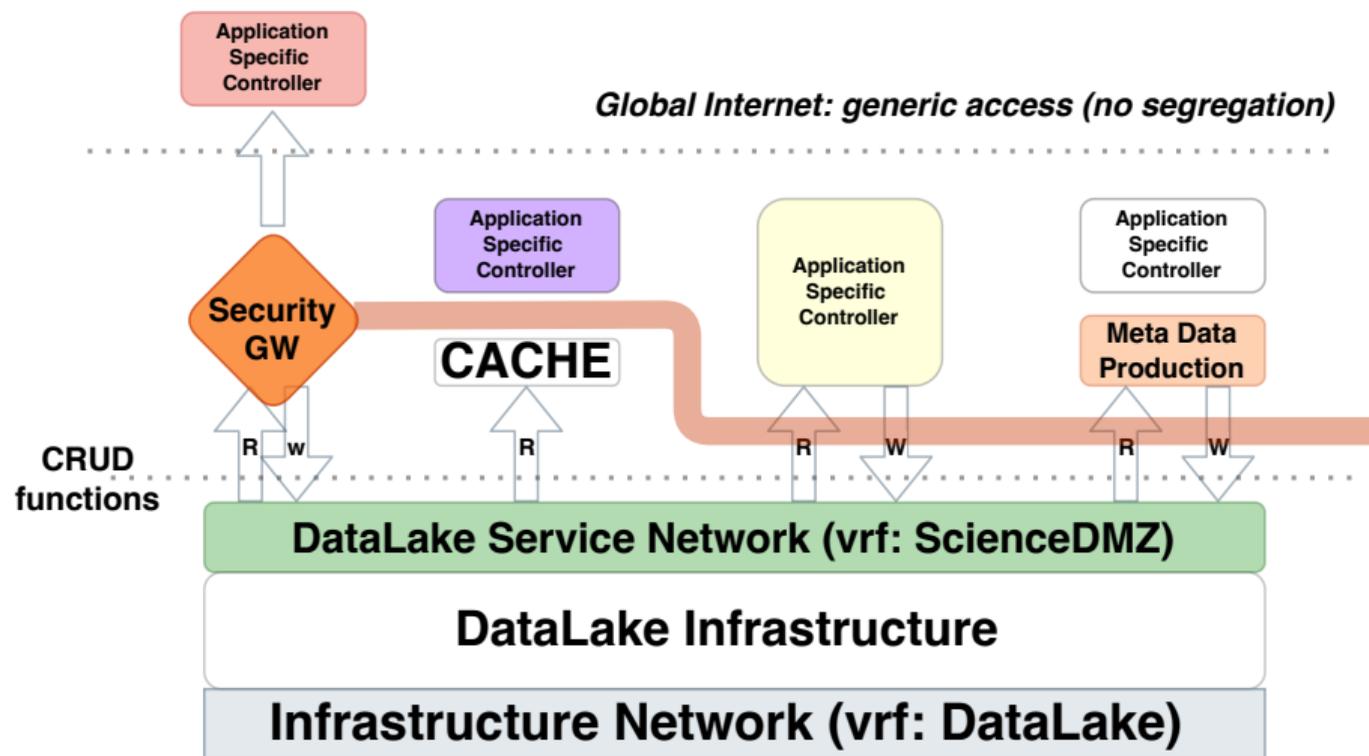
- Global Internet: accesso *Global Internet*
- Packet Network: rete di *trasporto nazionale* GARR
- LHCONE: rete HTC dedicata *Science DMZ*
- DATA LAKE: istanza di routing segregata su scala nazionale



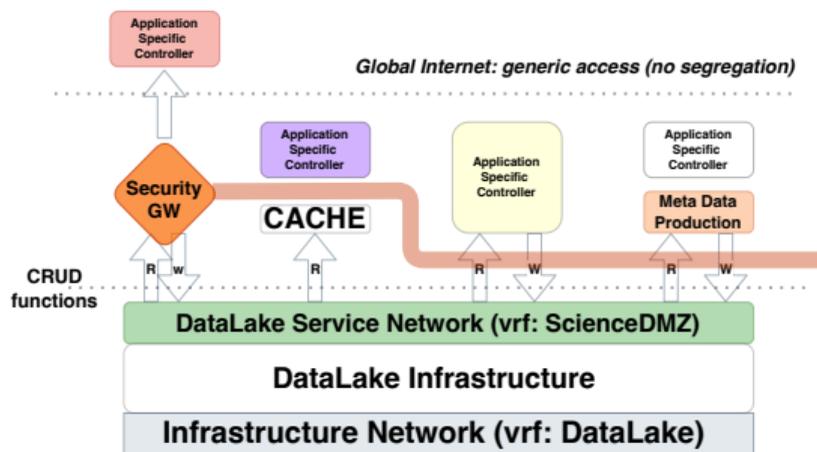
# Datalake: Architettura DRAFT-0.2



# Datalake: possibile architettura di rete e applicativa I



# Datalake: possibile architettura di rete e applicativa II



## Es. Arch DataLake

I modelli di accesso alle risorse basati su API rappresentano la giusta direzione per quello che riguarda le funzioni “controllo” e “gestione” dell’informazione ma non sono idonee a consentire livelli adeguati di prestazioni e sicurezza. Mescolare CTRL-plane con il FORW-plane pone un problema di funzionamento a lungo termine difficilmente risolvibile (esposizione)

# alcune considerazioni I

## Evoluzione di Rete

- L'attività di realizzazione di GARR-T(erabit) prosegue
- Contiamo di completare la dorsale prevista entro 23Q1
- La migrazione dei servizi da GARR-X a GARR-T è prevista per 22Q4. Contiamo di completare il tutto entro 23Q3

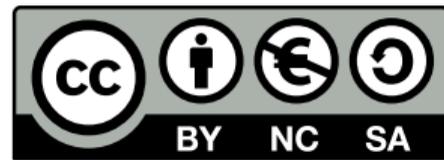
## Evoluzione dei Servizi

- L'accesso ad alte prestazioni va distinto da quello general Internet
- Soluzioni basate su IP\_Fabric favoriscono scenari evolutivi

# Licenza d'uso del materiale presente in queste slide

---

Quest'opera è distribuita con licenza Creative Commons "Attribuzione – Non commerciale – Condividi allo stesso modo 4.0 Internazionale".



Strumenti OpenSource

$\LaTeX$  - Draw.IO - GNU.Makefile