How to connect to LHCONE

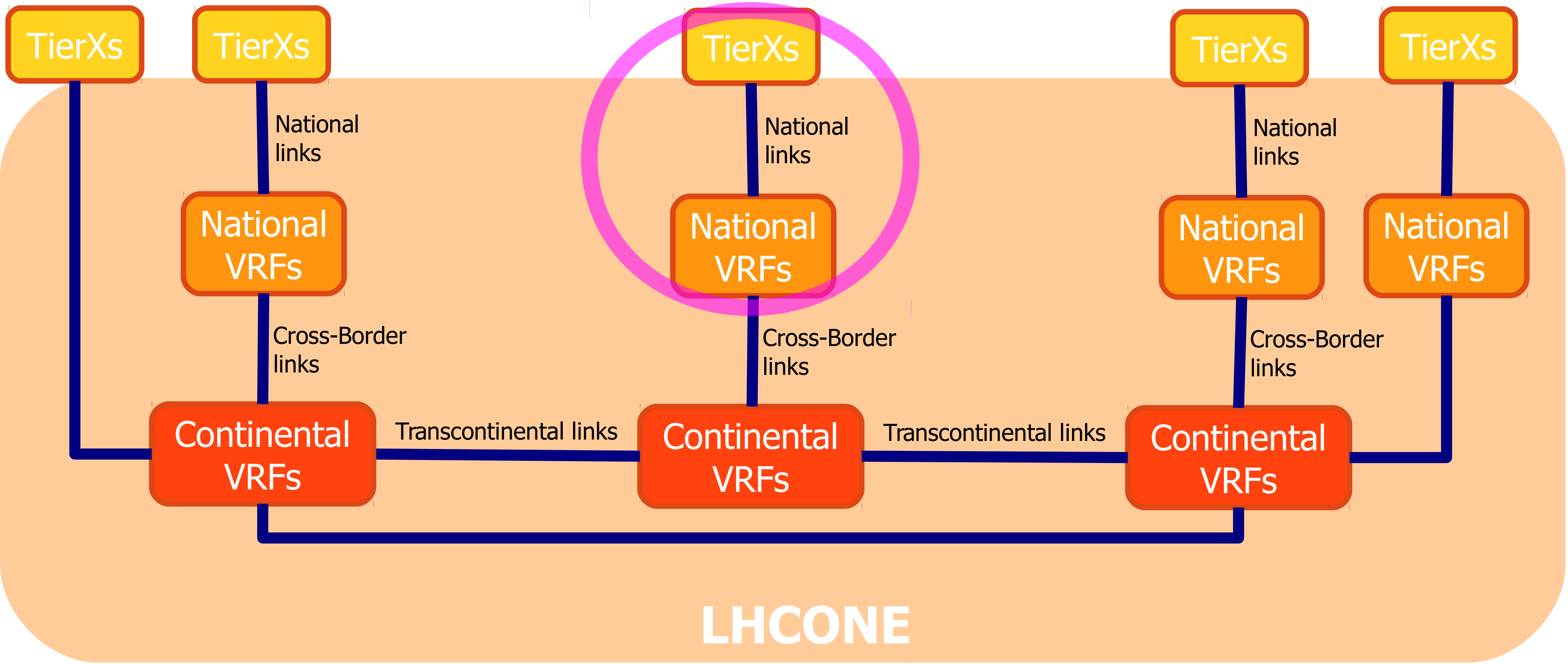
APAN workshop
Nantou, 13th August 2014
Edoardo.Martelli@cern.ch

Summary

- Howto connect to LHCONE

LHCONE L3VPN architecture

- TierX sites connected to National-VRFs or Continental-VRFs



Pre-requisites

The TierX site needs to have:

- Public IP addresses

- A public Autonomous System (AS) number

- A BGP capable router

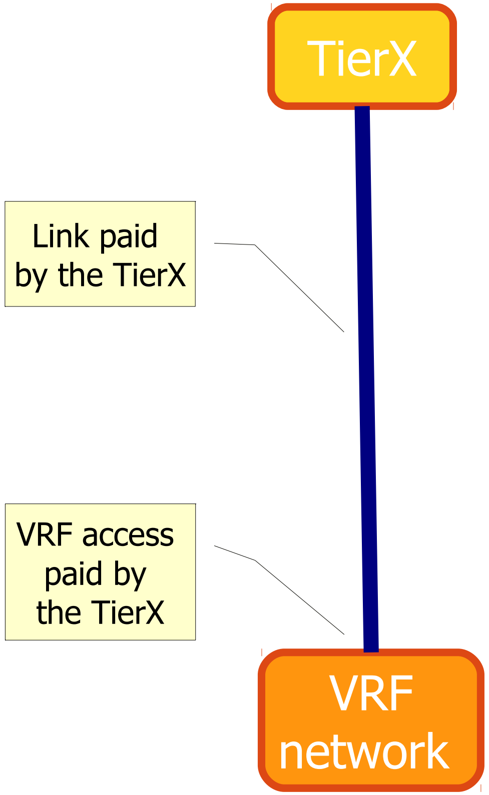
Physical connection

The TierX has to:

- Contact the Network Provider that runs the closest LHCONE VRF

- Agree on the cost of the access

- Lease a link from the TierX premises to the closest LHCONE VRF PoP (Point of Presence)



LHCONE AUP

LHCONE Acceptable Use Policy (AUP):

Use of LHCONE should be restricted to WLCG related traffic

IP addresses announced to LHCONE:
- should be assigned only to WLCG servers
- cannot be assigned to generic campus devices (desktop and portable computers, wireless devices, printers, VOIP phones....)

https://twiki.cern.ch/twiki/bin/view/LHCONE/LhcOneAup (draft)

Routing setup

- A BGP peering is established between the TierX and the VRF border routers

- The **TierX announce** only the IP subnets used for WLCG servers

- The **TierX accepts** all the prefixes announced by the LHCONE VRF router

Routing setup (2)

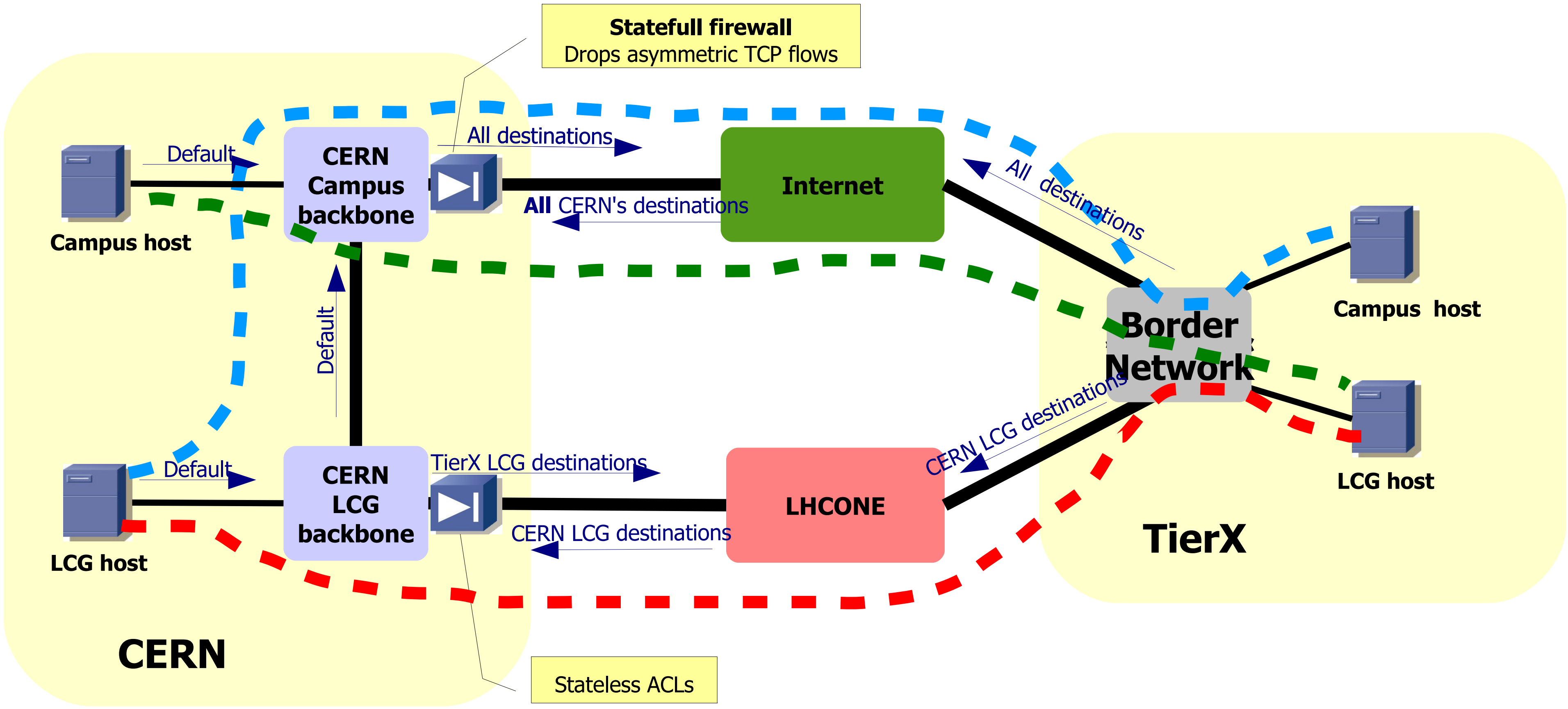
- The TierX **must** ensure traffic symmetry: injects only packets sourced by the announced subnets

- That's because LHCONE traffic may be allowed to bypass the TierX's central firewall (decision up to the TierX)

Symmetric paths must be ensured

Beware: statefull firewalls discard unidirectional TCP connections!

CERN example:



🟥 Flow: LHCONE host to LHCONE host

🟦 Flow: CERN's LHCONE host to TierX not LHCONE host

🟩 Flow: CERN's not LHCONE host to TierX's LHCONE host

Symmetry setup

To achieve symmetry, use one of the following techniques:

- Policy Base Routing (source-destination routing)

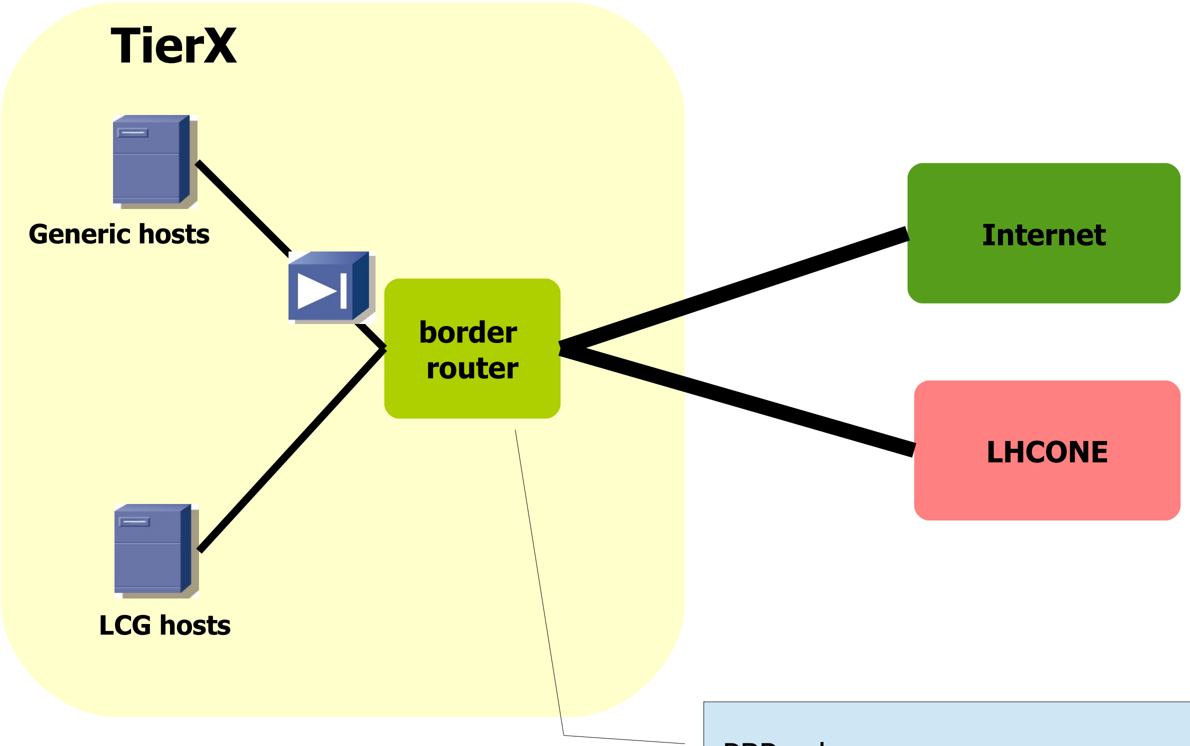
- Physically Separated networks

- Virtually separated networks (VRF)

- Scienze DMZ

Policy Based Routing

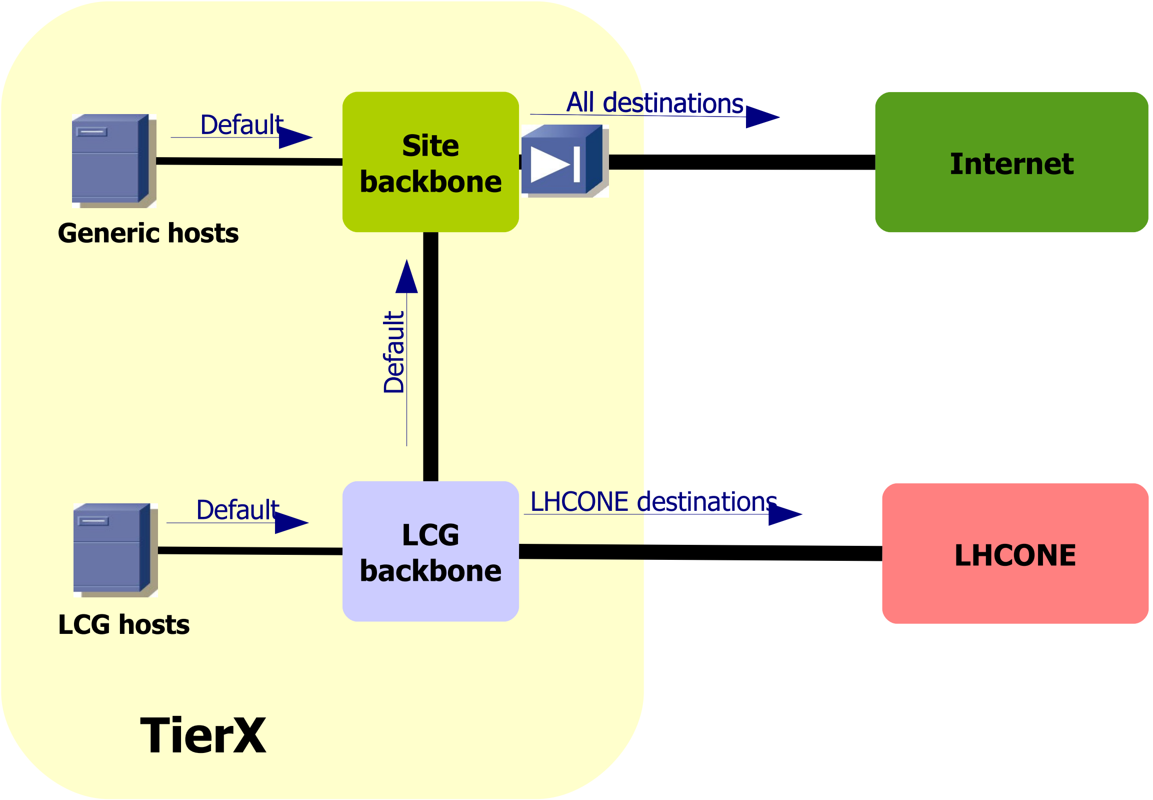
If a single border router is used to connect to the Internet and LHCONE, source-destination routing must be used



PBR rules:
From LCG host to LHCONE host: next-hop LHCONE
From Generic host to Any host: next-hop Internet

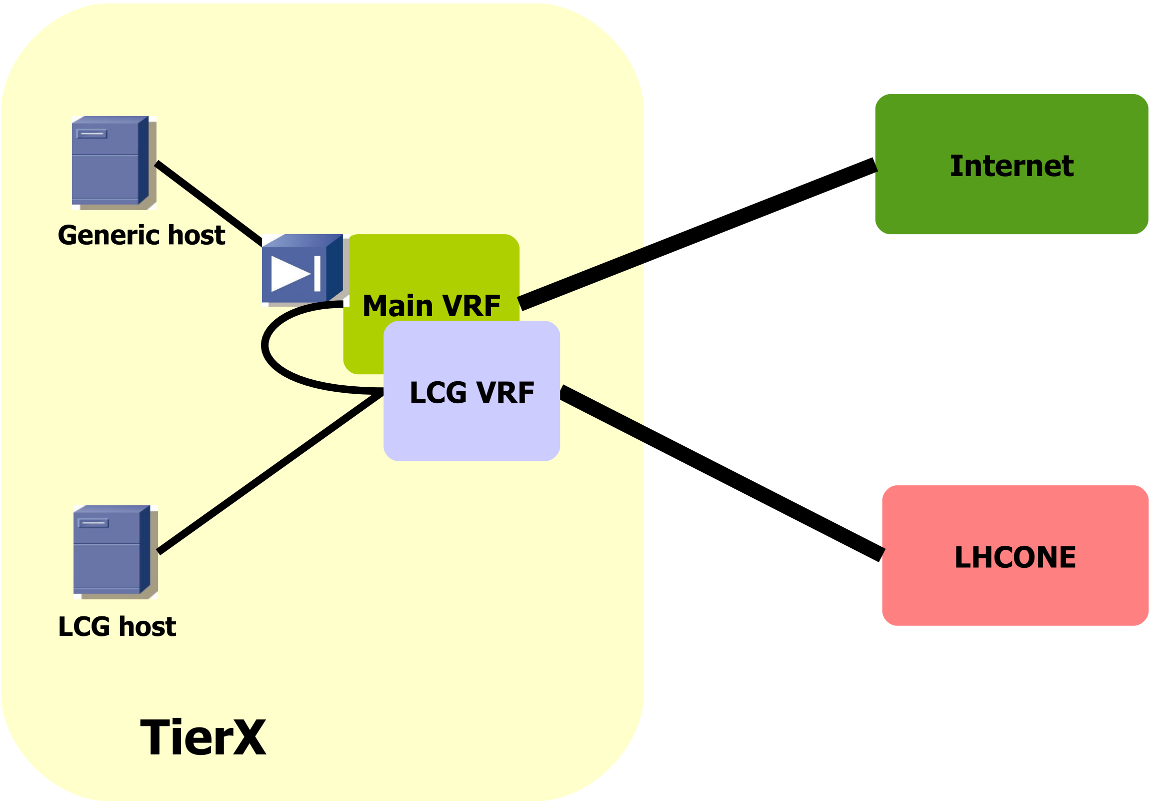
Physically separated networks

Different routers can be used for Generic and LCG Hosts



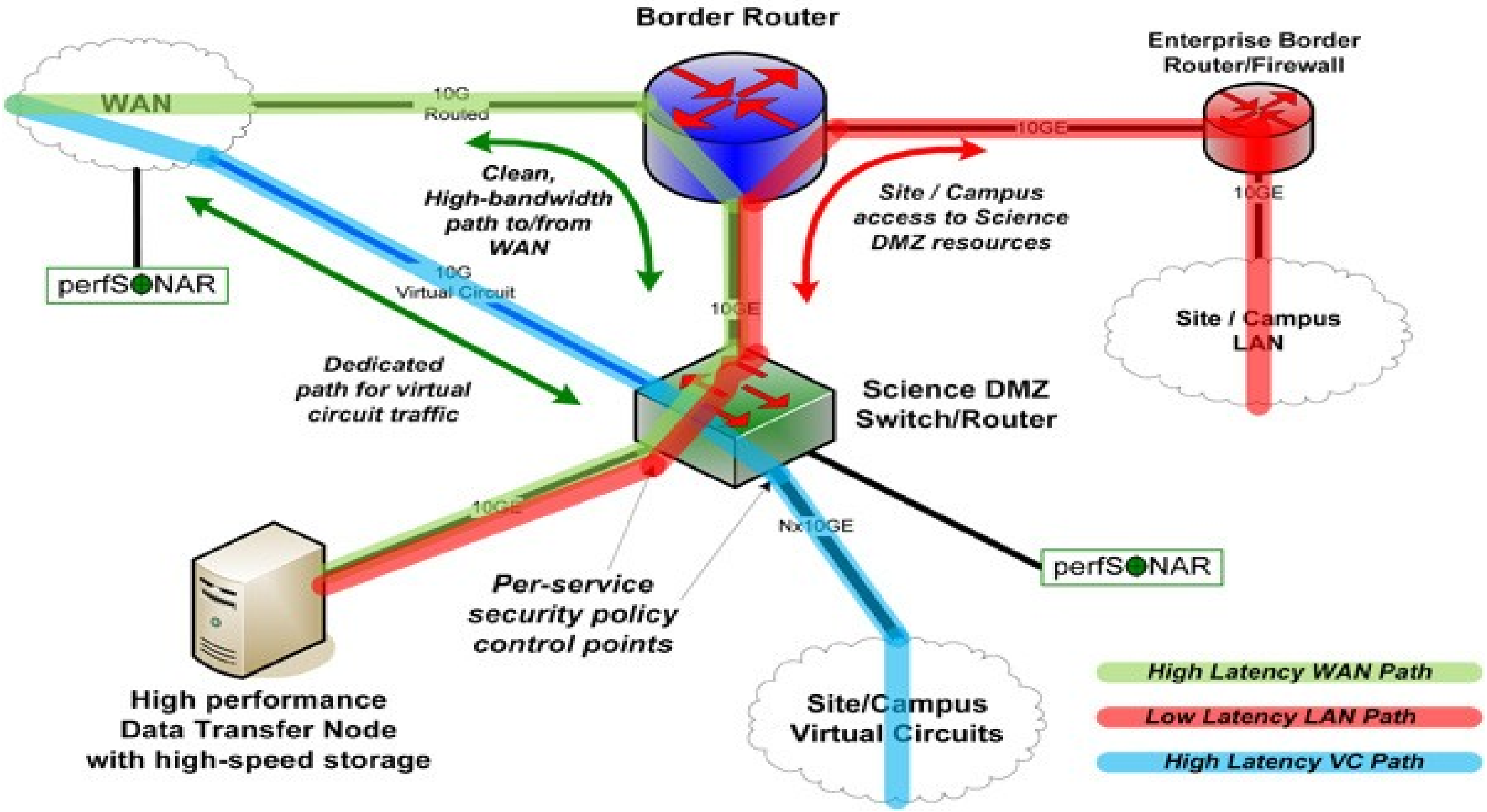
Virtually separated networks (VRF)

Traffic separation is achieved with Virtual Routing instances on the same physical box



Scienze DMZ

Few High Perfromence data transfer nodes conencted to a High Bandwidth DMZ


Border Router
Enterprise Border Router/Firewall
WAN
10G Routed
10GE
Clean, High-bandwidth path to/from WAN
Site / Campus access to Science DMZ resources
10GE
perfSONAR
10G Virtual Circuit
10GE
Site / Campus LAN
Dedicated path for virtual circuit traffic
Science DMZ Switch/Router
10GE
Nx10GE
perfSONAR
Per-service security policy control points
High performance Data Transfer Node with high-speed storage
Site/Campus Virtual Circuits
High Latency WAN Path
Low Latency LAN Path
High Latency VC Path

http://fasterdata.es.net/science-dmz/science-dmz-architecture/

Summary

- provision **Physical Connectivity** to the closest LHCONE router

- configure **BGP peering** with the connected LHCONE router

- set up **Symmetric routing**

Questions?