

LHCONE proposal: routed VPN over P2P service

Amsterdam, 1st December 2012
edoardo.martelli@cern.ch

Service: Dynamic P2P circuits



The Dynamic P2P services provides point-to-point links between any pair of devices connected to the LHCONE infrastructure.

A Device can be a router at the Tier1/2/3 premises, an Aggregator router, a router of the Routed VPN service.

The LHCONE infrastructure is a set of long distance links and L1/2 network devices belonging to different domains and interconnected at Open Exchange Points.

Links can be provisioned by manual configuration or by means of a common provisioning system.

Operations

This service is managed by the Carriers (Research and Education Networks providers) and the Open Exchange points which provide resources to the service; it is operated by the NOCs of the resource providers.

Service: Routed VPN



This service provides the Tier1/2/3s with a private routed backbone where they can exchange LHC data traffic.

The Routed VPN is made of a small set of routers located in key locations and interconnected by links provided by the P2P Circuits Service.

Tier1/2/3s can connect to the the closest router of the Routed VPN service with p2p links provided by the P2P Circuits Service.

Tier1/2/3s can peer with the Routed VPN and announce their own LHCONE prefixes so to reach all the other LHCONE prefixes announced to the VPN.

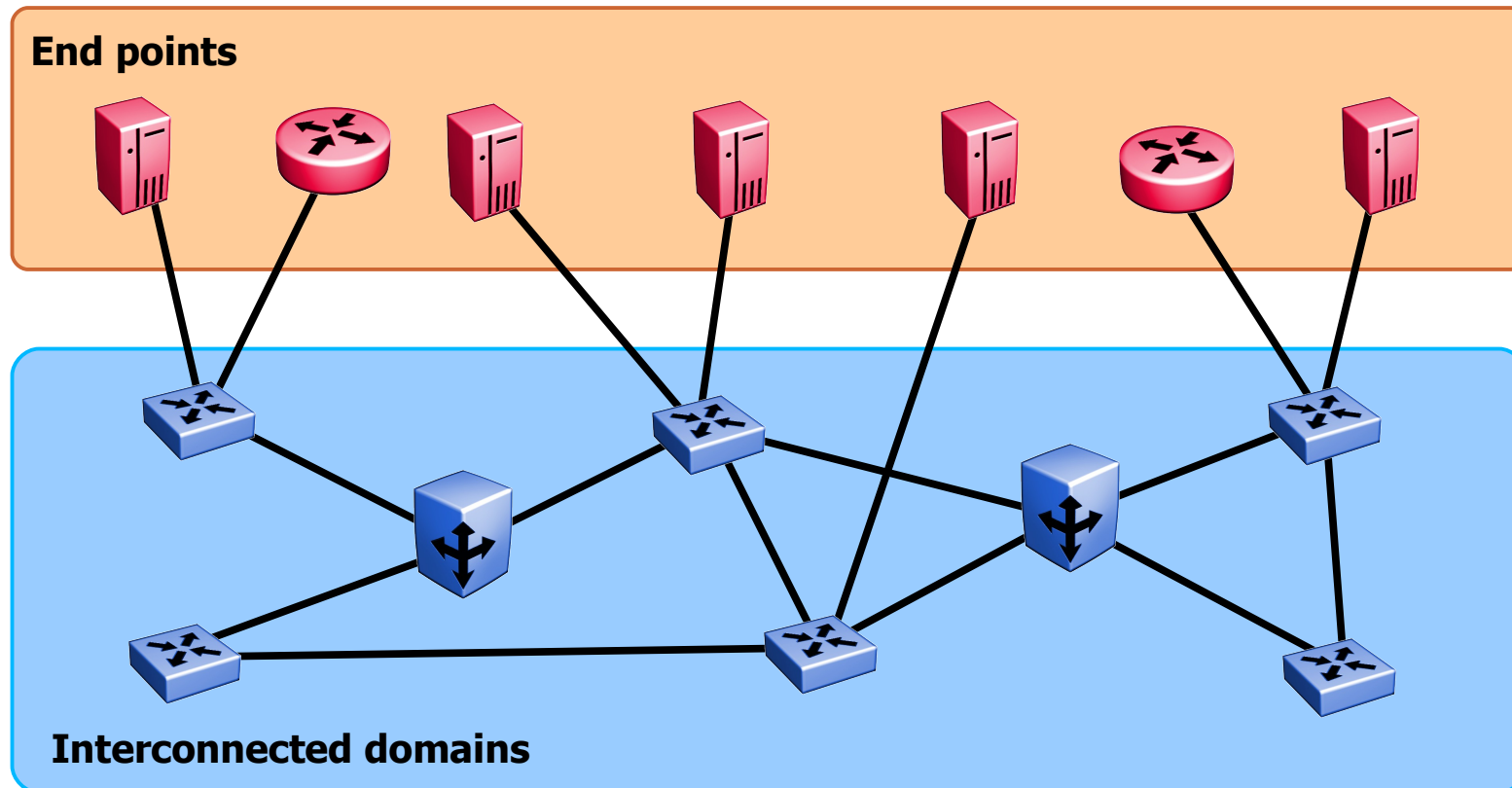
Tier2/3s without the right capabilities to connect to the VPN (BGP capable router, public Autonomous System number) can connect via Aggregators.

Thanks to the controlled kind of servers connected to the LHCONE VPN service , Tier1/2/3s can safely connect to the service without the need send their traffic through their statefull inspection firewalls. On the other hand, Tier1/2/3s will have to assure their traffic follows a symmetric path.

Operations

This service is supervised by the Tier1/2/3s connected to the the service; it is operated by the LHCONE NOC.

Physical infrastructure



Tier1/2/3



VPN/Aggregator router

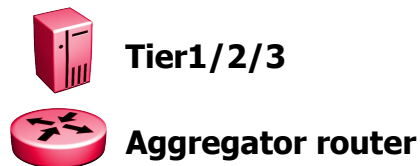
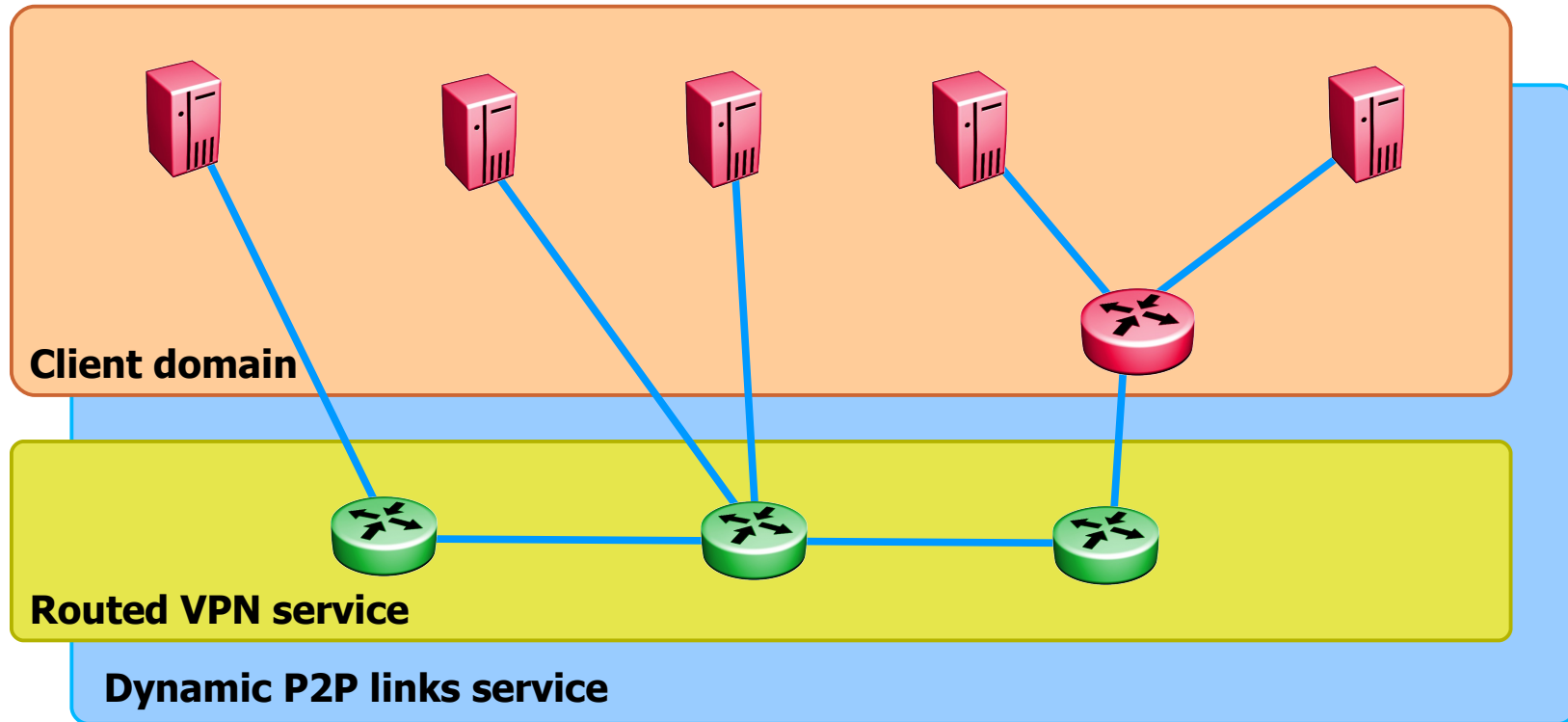


Network domain



Open Exchange point

Service Overview



Implementation plan, timeline



The current Shared VLAN implementation can be transformed into the Routed VPN service.

The VPN Service routers can be obtained from existing L2/L3 switch/routers by using Virtual Routing instances or dedicating their L3 engine to the Service (it can be the case of the CERNlight switch/router).

The P2P service can be provided by the infrastructure already put in place for the LHCONE Shared VLAN.

The first version of the VPN Service may be without redundancy and with a limited number of routers, indicatively one per continent. The VPN Service may grow in capacity and redundancy over time, reaching full maturity in time for the LHC restart in 2014.

The first stage of the Dynamic P2P service will not be Dynamic and will relay on static configuration implemented by the operators. Operators will have time to develop a common Network Provisioning System during the time till the LHC restart.

Funding



Network Operators will directly charge Tier1/2/3 for their access links to the LHCONE.

Expensive resources for the interconnections of the VPN routers (namely transoceanic links) will have to be funded by LHC funding agencies or by surcharges of the access links.

Questions?