Contrail Networking:  
  
Contrail Networking provides dynamic end-to-end networking policy and control for any cloud, any workload, and any deployment, from a single user interface by translating abstract workflows into specific policies.  
although our focus in this book would be building a secure container network orchestrated by Kubernetes but contrail can build Virtual networks that integrate container, VM and BMS  
but what is virtual network ?  
Virtual Networks (VNs) are a key concept in the Contrail System. Virtual networks are logical constructs implemented on top of the physical networks. Virtual networks are used to replace VLAN-based isolation and provide multi-tenancy in a virtualized data center. Each tenant or an application can have one or more virtual networks. Each virtual network is isolated from all the other virtual networks unless explicitly allowed by security policy.

Virtual networks can be extended to physical networks using a gateway. Finally, Virtual networks are used to implement Network Function Virtualization (NFV) and service chaining.

as explained in the diagram where Network operate only deal with the logical abstraction of the network then contrail do the heavy lifting of building polices, exchanging routes, building tunnels on the physical topology.

Firewall

policy



BMS



PNF



*VM1*

BMS

*Red Virtual Network*

*Blue Virtual Network*

policy



C1

C4

*VM2*

VNF



C

C

LOGICAL



Orchestrator

Contrail

Controller

**KVM Hypervisor**

**ESXi Hypervisor**



C

C

C

C



*VM2*

*VM1*

VNF

vRouter



PHYSICAL

Contrail Networking Architecture:

Contrail run in Logically centralized, physically distributed model as it has two main components, Contrail controller and Contrail vrouter

the Controller is the Control and management plane that Collects/presents analytics   
and Manages/configures the vrouter  
Contrail vrouter is the Forwarding plane that Provides Layer 2/3 services , Distributed firewall capabilities and Implements policies between virtual networks   
  
Contrail integrates with many orchestrator such as OpenStack , VMware , Kubernetes , OpenShift and Mesos and use multiple protocols to provide SDN to these orchestrators as shown in the diagram where   
  
XMPP : Extensible Messaging and Presence Protocol (XMPP) is an open XML technology for real-time communication defined in RFC 6120, in Contrail it offers two main functionality, distributing routing information and pushing configuration, which are similar to what IBGP do in MPLS VPNs model plus NETCONF in device management. XMPP is also used to exchange operational state, statistics, logs and events

MPLSoGRE/UDP or VXLAN: are three different kind of overlay tunnels to carry traffic over IP network. They are all IP-UDP packet but in VXLAN we use the VNI values in VXLAN header for segmentation where in MPLSoGRE and MPLSoUDP we use the MPLS label value for segmentation

BGP: is used to exchange router with physical router and in same case Contrail device manager can use Netconf to configure this Gateway  
  
EVPN: Ethernet VPN is a standards-based technology RFC 7432 that provides virtual multipoint bridged connectivity between different Layer 2 domains over an IP network.

Contrail controller exchange EVPN routes with TOR switches (acting as L2 VXLAN GW) to offer faster recovery with active-active VXLAN forwarding

OVSDB: Open vSwitch Database is a standards-based control protocol used to configure ToR switch and to import dynamically-learned addresses with VXLAN in the data plane.

To simplify the relation between contrail vrouter, contrail controller and the IP Fabric from the prospective of the Architecture prospective, let’s compare it to MPLS VPN model in any services provider   
vrouter is like PE router and the VM/container is like CE but vrouter is just a slave of contrail controller. and when it comes to BMS the TOR would be the PE

Physical IP Fabric  
*(no changes)*

CONTRAIL CONTROLLER

ORCHESTRATOR

*Host O/S*



vRouter

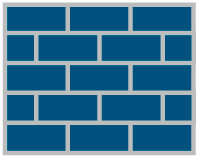
*Network / Storage orchestration*



Gateway



…



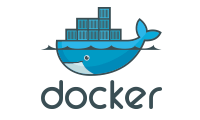
Internet / WAN or Legacy Env.

(Config, Control, Analytics)



*(Windows, Linux ….) on BMS*

TOR



*Compute orchestration*

Centralized

Policy Definition

Distributed

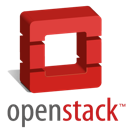
Policy Enforcement

*BGP*

*BGP*

*XMPP*

*EVPN   
Netconf  
or OVSDB*



MPLSoGRE/UDP or VXLAN Virtual Overlay Networks