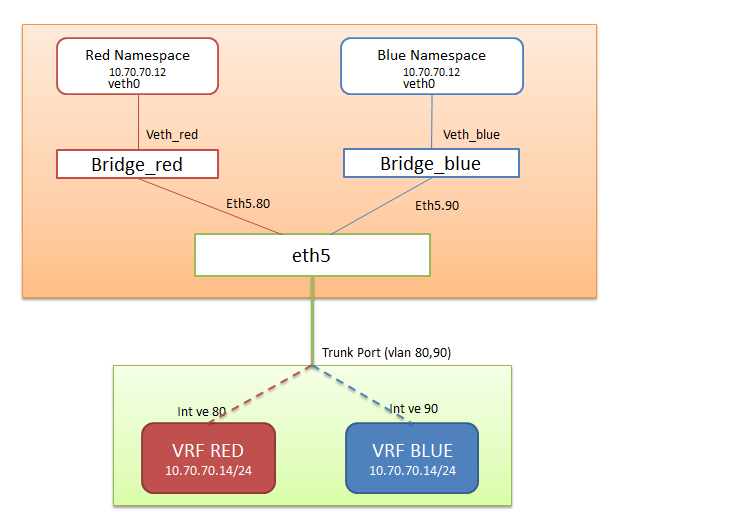
此文章已于 16:24:04 2016/8/10 发布到 MADHEX

VRF & Linux Network Name Space

**Introduction**

As we know, VRF (Virtual Routing and Forwarding on Switch) and [Linux Network Name Space](http://rmadapur.blogspot.in/2014/02/linux-network-namespaces.html) (on Linux hosts) can be used to achieve Network Isolation. Lets see how we can use them together.

**Setup**



Host there are two namespaces, namely **red** and **blue.**  
Each of the namespace is connected to its own Linux Bridge (i.e Red Namespace is connected to Bridge\_red  and Blue Namespace is connected to Bridge\_Blue ). Virtual Interface (veth0) connected to each bridge is assigned the same ip address (10.70.70.12/24). This L3 Network isolation achieved on the same host by using Network Namespaces.  
  
  
Bridge\_red is connected to external interface eth5 via eth5.80(eth5.80 sends tagged packet with vlan value as 80).  
Bridge\_blue is connected to external interface eth5 via eth5.90(eth5.80 sends tagged packet with vlan value as 90).  
  
Linux host is connected to external device (that has VRF capability). 10.70.70.14/24 is the ip address configured on both the blue and red vrf's.

**Commands to Create Red Name Space**

//Create a red namespace

ip netns add red

//Create eth5.80 (80 vlan tagged interface on eth5)

ip link add link eth5 eth5.80 type vlan id 80

//Create a veth pair

ip link add veth0 type veth peer name veth\_red

//Set on end of the veth pair to red namespace

ip link set veth0 netns red

//Bring up the veth pairs

ip netns exec red ip link set dev veth0 up

ip link set dev veth\_red up

//create a red bridge and add interfaces

brctl addbr bridge\_red

brctl addif bridge\_red eth5.80

brctl addif bridge\_red veth\_red

//bring up bridge interfaces

ip link set dev bridge\_red up

ip link set dev eth5.80 up

//Configuer ip address within the namespace

ip netns exec red ifconfig veth0 10.70.70.12 netmask 255.255.255.0 up

ip netns exec red ip route add default via 10.70.70.12

**Commands to Create Blue Name Space**

ip link add link eth5 eth5.90 type vlan id 90

//Create a blue Namespace.

ip netns add blue

//Create veth pair

ip link add veth0 type veth peer name veth\_blue

//assign one end of the veth pair to blue namespace

ip link set veth0 netns blue

//Bring veth pairs

ip netns exec blue ip link set dev veth0 up

ip link set dev veth\_blue up

//Create Linux bridge and add interfaces to it.

brctl addbr bridge\_blue

brctl addif bridge\_blue eth5.90

brctl addif bridge\_blue veth\_blue

//Bring up the bridge interfaces

ip link set dev bridge\_blue up

ip link set dev eth5.90 up

//Assign ip address to veth pair in the blue Namespace

ip netns exec blue ifconfig veth0 10.70.70.12 netmask 255.255.255.0 up

ip netns exec blue ip route add default via 10.70.70.12

**Commands to Create VRF on external device.**

//interface connected to eth5

interface GigabitEthernet 3/0/41

switchport

switchport mode trunk

switchport trunk allowed vlan add 80,90

switchport trunk tag native-vlan

spanning-tree shutdown

no shutdown

!

//Configuration for VRF red

rbridge-id 153

vrf red

rd 1:1

address-family ipv4 max-route 3600

!

!

interface Ve 80

vrf forwarding red

ip proxy-arp

ip address 10.70.70.14/24

no shutdown

!

!

rbridge-id 153

vrf blue

rd 1:2

address-family ipv4 max-route 3600

!

!

!

interface Ve 90

vrf forwarding blue

ip proxy-arp

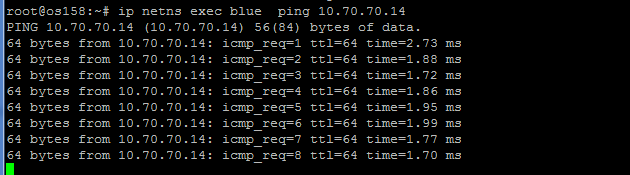
ip address 10.70.70.14/24

no shutdown

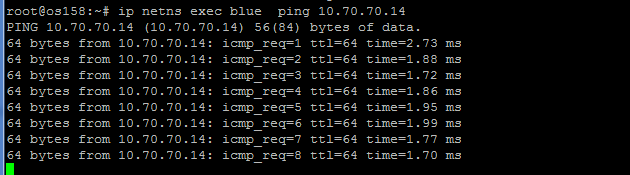
!

### Communication from Linux host to external device (ie Network Namespace to VRF)

Here ping is initiated from the veth0(10.70.70.12) in the blue namespace to 10.70.70.14 (in the blue VRF)



ping is initiated from the veth0(10.70.70.12) in the red namespace to 10.70.70.14 (in the redVRF)



an be used on LinuxBridge interfaces to verify that traffic is indeed flowing to the correct VRF on the external device.  
  
Network Isolation (L3,ip address isolation)  can be achieved by using Linux Network Namespaces and VRFs.Also, we have seen here how they can be interconnected.  
  
Network Isolation is an important concept in multi-tenant cloud environment.