Configuring VRF on HP Switches: in a single site deployment

Technical Configuration Guide

Version:2.1

January 2013

Table of Contents

Introduction

This Technical Configuration Guide (TCG) describes how to configure Virtual Routing and Forwarding (VRF) in a single site environment. The intended audience is HP Solution Architects, HP Technical Consultants, HP resellers and HP customers.

Background Information

Customer networks have become a critical component in the daily operation of a company. A network outage can result in lost revenue as well as lost productivity from unavailable resources. While some outages are related to failures, most outages are due to a misconfiguration or a small hardware failure, like a NIC card, that has ultimately failed. While most networks employ VLANs to reduce broadcast traffic, there are certain instances where having a VRF are more beneficial. One such instance is when R&D or test labs are connected to the corporate network. Having separate infrastructures is no longer a viable option due to the rising CAPEX and OPEX costs to maintain these standalone networks. By deploying VRFs, these labs are isolated from the corporate network so any failures or misconfigurations can be contained local and not result in a corporate wide outage. VRFs can also provide a level of network security since these lab environments, if compromised, cannot access corporate resources. While some manufacturers, including HP, have released virtualization features that segment out a single physical switch, sometimes the implementation of a switch that has these features is cost prohibitive and typically is limited in scale. VRFs provide another way to accomplish this network segmentation and isolation.

Requirements

Readers of this document should be familiar with features and configuration of HP switches.

The following hardware is required:

- HP Networking switches that support the VRF feature. In this guide a core switch, HP 12500, is used with 5800s and 5820s as the IDF switches.

The following software is required:

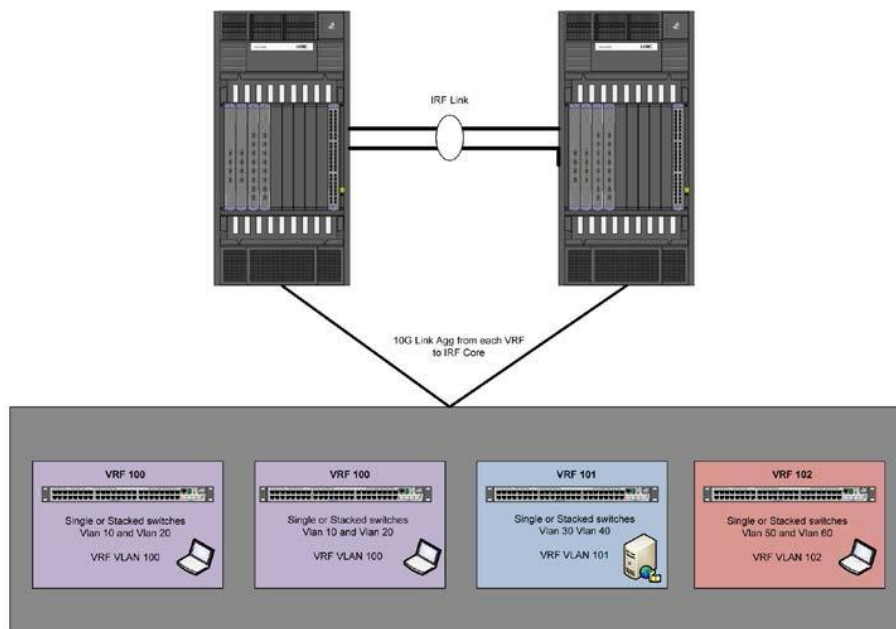- The latest firmware should be used.

The following tools are required:

- If a demonstration of the feature is necessary, having a server and some end points as well as access to a traffic generation tool will help demonstrate failure scenarios.

Network Diagram

Figure 1 illustrates the connectivity for this configuration.

Figure 1 VRF Network Diagram

Configure

First we will configure the core switch since this is really the bulk of the configuration steps. If HP's IRF technology is to be used, the switches should already be configured with IRF before continuing.

Core Device Configuration

- Create an IP-VPN instance and Route-Distinguisher (RD)

```
[VRF-Core]ip vpn-instance idf
[VRF-Core-vpn-instance-idf]route-distinguisher 100:1
[VRF-Core]ip vpn-instance server
[VRF-Core-vpn-instance-idf]route-distinguisher 101:1
[VRF-Core]ip vpn-instance disti
[VRF-Core-vpn-instance-idf]route-distinguisher 102:1
```

The RD is just a distinguishing number used for the routing table and as such can be arbitrary. In this example we will use the transport VLAN for the different VPN-instances.

- Create the VLANs that will be used to transport port information between VRFs. You can also at this point create any VLANs that are going to be associated with each VRF or are to be configured on the core device itself.

```
[VRF-Core]vlan 100 to 102
[VRF-Core-vlan100]vlan 10 to 20
```

- Create and bind the vlan-interface to each vpn-instance. It is recommended that you configure the IP address after binding the interface since this command removes any previously configured information.

```
[VRF-Core] interface vlan-interface 100
[VRF-Core-Vlan-interface100]ip binding vpn-instance idf
[VRF-Core-Vlan-interface100]ip address 172.16.100.254 24
[VRF-Core] interface vlan-interface 101
[VRF-Core-Vlan-interface101]ip binding vpn-instance server
[VRF-Core-Vlan-interface101]ip address 172.16.101.254 24
[VRF-Core] interface vlan-interface 102
[VRF-Core-Vlan-interface102]ip binding vpn-instance disti
[VRF-Core-Vlan-interface102]ip address 172.16.102.254 24
```

- Create the bridge aggregation groups that you will be using to connect the IDF, server farm and distribution switches to the core

```
[VRF-Core] interface Bridge-Aggregation100
[VRF-Core-Bridge-Aggregation100]port link-type trunk
[VRF-Core-Bridge-Aggregation100]port trunk permit vlan 1 10 20
100 [VRF-Core-Bridge-Aggregation100]link-aggregation mode
dynamic
[VRF-Core-Bridge-Aggregation100]mad enable
```

- Create the remaining bridge aggregation groups and add the corresponding ports to the groups (CLI commands omitted)

Configure Core Device Routing

To be able to route between VRFs the following steps must be taken. Once configured, all VLANs in all VRFs will be able to communicate. If certain VLANs are to be restricted, route policies must be configured to prevent routing information from being exchanged.

```
[VRF-Core]bgp 65000
[VRF-Core-bgp]router-id 1.1.1.1
[VRF-Core-bgp]ipv4-family vpn-instance idf
[VRF-Core-bgp-idf]peer 172.16.100.252 as-number 65001
[VRF-Core-bgp-idf]peer 172.16.100.253 as-number 65001
[VRF-Core-bgp-idf]import-route direct
```

```
[VRF-Core-bgp-idf]quit
[VRF-Core-bgp]ipv4-family vpn-instance server
[VRF-Core-bgp-server]peer 172.16.101.253 as-number 65002
[VRF-Core-bgp- server]import-route direct
[VRF-Core-bgp- server]quit
[VRF-Core-bgp]ipv4-family vpn-instance disti
[VRF-Core-bgp-disti]peer 172.16.102.253 as-number 65003
[VRF-Core-bgp- disti]import-route direct
[VRF-Core-bgp- disti]quit
```

• The following commands are what allow the exchange of routing information between VRFs. Note that the RD used is that of the vpn-instance you are trying to reach not of the originating vpn-instance.

```
[VRF-Core-vpn-instance-idf]vpn-target 101:1 both
[VRF-Core-vpn-instance-idf]vpn-target 102:1 both
[VRF-Core-vpn-instance-server]vpn-target 100:1 both
[VRF-Core-vpn-instance-server]vpn-target 102:1 both
[VRF-Core-vpn-instance-disti]vpn-target 100:1 both
[VRF-Core-vpn-instance-disti]vpn-target 101:1 both
```

Edge Device Configuration

For this scenario, the intelligence of VRF is in the core 12500 hardware. Each stackable switch has minimal configuration.

• First configure the VLANs that each device will have locally as well as the transport VLAN for VRF.

```
[vrf-idf01]vlan 10
[vrf-idf01]vlan 20
[vrf-idf01]vlan 100
```

• Next configure the IP address for each VLAN

```
[vrf-idf01-Vlan-interface100]ip address 172.16.100.253 24
[vrf-idf01-Vlan-interface10]ip address 10.1.10.1 24
[vrf-idf01-Vlan-interface20]ip address 10.1.20.1 24
```

• Create the Bridge Aggregation group and add the corresponding ports to the group

```
[VRF-idf01] interface Bridge-Aggregation100
[VRF-idf01-Bridge-Aggregation100]port link-type trunk
[VRF-idf01-Bridge-Aggregation100]port trunk permit vlan 1
10 20 100
[VRF-idf01-Bridge-Aggregation100]link-aggregation mode
dynamic
[VRF-idf01-Ten-GigabitEthernet1/0/1]port link-type trunk
```

```
[VRF-idf01-Ten-GigabitEthernet1/0/1]port trunk permit vlan
1 10 20 100
[VRF-idf01-Ten-GigabitEthernet1/0/1]port link-aggregation
group 100
```

Configure Edge Device Routing

• The final step is to configure BGP on the IDF switch(es). In this example, a static route has been configured to the core.   A dynamic routing protocol could be used as well.

```
[VRF-idf01]bgp 65001
[VRF-idf01-bgp]peer 172.16.100.254 as-number 65000
[VRF-idf01-bgp]quit
[VRF-idf01]ip route-static 0.0.0.0 0.0.0.0 172.16.100.254
```

Demonstration

Here's an example of a demonstration that can be used to verify this configuration:

Introduce a broadcast storm in a VRF to show that it stays localized. Creating a STP Loop is another effective demo as well.

• If you have access to Ixia test gear, this equipment can generate a broadcast storm at line rate 10G.

• To prove that only the local VRF is affected, streaming video and ICMP requests were monitored in the other VRFs. A physical server in the server VRF can share a folder and laptops in the other VRFs (IDF and Disti) can play the same video. When there is no broadcast storm, the videos are in sync and play smoothly and there are no ICMP timeouts. When the Ixia test port was enabled and introduced a broadcast storm into a VRF, video degradation was seen only on the laptop in the same VRF as the Ixia and there were multiple ICMP timeouts. Once the broadcast was eliminated the video resumed playing normally with no ICMP timeouts.

• If test equipment or a traffic generator isn't available you could use hacking tools like Metasploit and launch a DOS attack or ping of death to achieve similar results.

Appendix A – Configurations

Below are the actual configurations from an IRF 12508 core with 5800, 5820 and 5500-EI as edge devices:

Core switch configuration
```
sysname CORE12508
#
irf mac-address persistent always irf auto-update enable
```

```
undo irf link-delay
#
domain default enable system
#
forward-path check enable
hardware-failure-detection chip
warning hardware-failure-detection board
warning hardware-failure-detection forwarding
#
ip vpn-instance edge route-distinguisher 100:1
vpn-target 101:1 102:1 export-extcommunity
vpn-target 101:1 102:1 import-extcommunity
#
ip vpn-instance server route-distinguisher 101:1
vpn-target 102:1 100:1 export-extcommunity
vpn-target 102:1 100:1 import-extcommunity
#
ip vpn-instance disti route-distinguisher 102:1
vpn-target 101:1 100:1 export-extcommunity
vpn-target 101:1 100:1 import-extcommunity
#
vlan 1
#
vlan 10
#
vlan 20
#
vlan 100 to 102
#
domain system access-limit disable state active
idle-cut disable
self-service-url disable
#
user-group system
#
interface Bridge-Aggregation100
description LAG to Edge
port link-type trunk
port trunk permit vlan 1 10 20 100
link-aggregation mode dynamic
mad enable
#
interface Bridge-Aggregation101
description LAG to Server
port link-type trunk
port trunk permit vlan 1 101
link-aggregation mode dynamic
mad enable
#
interface Bridge-Aggregation102
description LAG to Disti
port link-type trunk
```

```
port trunk permit vlan 1 102
link-aggregation mode dynamic
mad enable
#
Interface Bridge-Aggregation110
description LAG to edge_5800_2
port link-type trunk
port trunk permit vlan 1 10 20 100
link-aggregation mode dynamic
mad enable
#
interface NULL0
#
interface LoopBack0
ip address 10.10.10.10 255.255.255.255
#
interface Vlan-interface10
ip address 10.1.10.254 255.255.255.0
#
interface Vlan-interface20
ip address 10.1.20.254 255.255.255.0
#
interface Vlan-interface100
ip binding vpn-instance edge
ip address 172.16.100.254 255.255.255.0
#
interface Vlan-interface101
ip binding vpn-instance server
ip address 172.16.101.254 255.255.255.0
#
interface Vlan-interface102
ip binding vpn-instance disti
ip address 172.16.102.254 255.255.255.0
#
interface Ten-GigabitEthernet1/2/0/1
port link-type trunk
port trunk permit vlan 1 102
port link-aggregation group 102
#
interface Ten-GigabitEthernet1/2/0/2
port link-type trunk
port trunk permit vlan 1 102
port link-aggregation group 102
#
interface Ten-GigabitEthernet1/2/0/3
port link-type trunk
port trunk permit vlan 1 101
port link-aggregation group 101
#
```

Configuration omitted for brevity

9

```
interface Ten-GigabitEthernet1/2/0/4
port link-type trunk
port trunk permit vlan 1 101
port link-aggregation group 101
#
interface Ten-GigabitEthernet1/2/0/5
port link-type trunk
port trunk permit vlan 1 10 20 100
port link-aggregation group 100
#
interface Ten-GigabitEthernet1/2/0/6
port link-type trunk
port trunk permit vlan 1 10 20 100
port link-aggregation group 110
#
interface Ten-GigabitEthernet2/2/0/1
port link-type trunk
port trunk permit vlan 1 102
port link-aggregation group 102
#
interface Ten-GigabitEthernet2/2/0/2
port link-type trunk
port trunk permit vlan 1 102
port link-aggregation group 102
#
interface Ten-GigabitEthernet2/2/0/3
port link-type trunk
port trunk permit vlan 1 101
port link-aggregation group 101
#
interface Ten-GigabitEthernet2/2/0/4
port link-type trunk
port trunk permit vlan 1 101
port link-aggregation group 101
#
interface Ten-GigabitEthernet2/2/0/5
port link-type trunk
port trunk permit vlan 1 10 20 100
port link-aggregation group 100
#
interface Ten-GigabitEthernet2/2/0/6
port link-type trunk
port trunk permit vlan 1 10 20 100
port link-aggregation group 110
#
bgp 65000
router-id 1.1.1.1 undo synchronization
#
ipv4-family vpn-instance edge
peer 172.16.100.252 as-number 65001
```

```
peer 172.16.100.253 as-number 65001 import-route
direct
#
ipv4-family vpn-instance server
peer 172.16.101.253 as-number 65002 import-route
direct
#
ipv4-family vpn-instance disti
peer 172.16.102.253 as-number 65003
preference 20 200 20 import-route direct
#
user-interface con 1/0 2/1
user-interface aux 1/0 2/1
user-interface vty 0 4
#
irf-port 1/1
port group interface Ten-GigabitEthernet1/2/0/7
port group interface Ten-GigabitEthernet1/2/0/8
#
irf-port 2/2
port group interface Ten-GigabitEthernet2/2/0/7
port group interface Ten-GigabitEthernet2/2/0/8
#
return
```

Distribution Switch Configuration

```
version 5.20, Feature 1208
#
sysname VRF-Disti
#
irf mac-address persistent timer irf auto-update
enable
undo irf link-delay
#
domain default enable system
#
telnet server enable
#
vlan 1
#
vlan 50
#
vlan 60
#
vlan 102
#
vlan 300
#
```

Configuration omitted for brevity

```
Bridge-Aggregation12 description LAG to 12500
```

11

```
port link-type trunk
port trunk permit vlan 1 102
link-aggregation mode dynamic
#
interface NULL0
#
interface Vlan-interface50
ip address 10.1.50.1 255.255.255.0
#
interface Vlan-interface60
ip address 10.1.60.1 255.255.255.0
#
interface Vlan-interface102
ip address 172.16.102.253 255.255.255.0
#
interface Vlan-interface300
ip address 10.1.30.1 255.255.255.0
#
interface GigabitEthernet1/0/15
port link-mode bridge
port access vlan 50
#
interface GigabitEthernet1/0/16
port link-mode bridge
port access vlan 50
#
interface GigabitEthernet1/0/17
port link-mode bridge
port access vlan 60
#
interface GigabitEthernet1/0/18
port link-mode bridge
port access vlan 60
#
interface Ten-GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 102
port link-aggregation group 12
#
interface Ten-GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 102
port link-aggregation group 12
#
interface Ten-GigabitEthernet1/0/4
port link-mode bridge
port access vlan 50
#
bgp 65003
```

```
router-id 3.3.3.3 import-route direct undo
synchronization
peer 172.16.102.254 as-number 65000
#
load xml-configuration
#
user-interface aux 0
user-interface vty 0 15
#
return
```

Server switch configuration

```
version 5.20, Feature 1208
#
sysname VRF-Server
#
irf mac-address persistent timer irf auto-update
enable
undo irf link-delay
#
domain default enable system
#
telnet server enable
#
vlan 1
#
vlan 30
#
vlan 40
#
vlan 101
#
radius scheme system server-type extended
primary authentication 127.0.0.1 1645
primary accounting 127.0.0.1 1646 user-name-format
without-domain
#
domain system access-limit disable state active
idle-cut disable
self-service-url disable
#
user-group system
#
interface Bridge-Aggregation101
description Server LAG
port link-type trunk
port trunk permit vlan 1 101
link-aggregation mode dynamic
#
interface NULL0
#
interface Vlan-interface30
```

```
ip address 10.1.30.1 255.255.255.0
#
interface Vlan-interface40
ip address 10.1.40.1 255.255.255.0
#
interface Vlan-interface101
ip address 172.16.101.253 255.255.255.0
#
interface GigabitEthernet2/0/15
port link-mode bridge

port access vlan 30
#
interfaceGigabitEthernet2/0/16
port link-mode bridge
port access vlan 30
#
Interface GigabitEthernet2/0/17
port link-mode bridge
port access vlan 40
#
interface GigabitEthernet2/0/18
port link-mode bridge
port access vlan 40
#
interface Ten-GigabitEthernet2/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 101
port link-aggregation group 101
#
interface Ten-GigabitEthernet2/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 101
port link-aggregation group 101
#
```

Configuration omitted for brevity

```
#
bgp 65002 import-route direct
undo synchronization
peer 172.16.101.254 as-number 65000
#
load xml-configuration
#
user-interface aux 1
user-interface vty 0 15
#
return
```

Edge switch configuration

```
version 5.20, Release 1206
#
sysname VRF-01
#
irf mac-address persistent timer irf auto-update
enable
undo irf link-delay
#
domain default enable system
#
telnet server enable
#
vlan 1
#
vlan 10 to 15
#
vlan 100
description VRF to MCE
#
radius scheme system server-type extended
primary authentication 127.0.0.1 1645
primary accounting 127.0.0.1 1646 user-name-format
without-domain
#
domain system access-limit disable state active
idle-cut disable
self-service-url disable
#
user-group system
#
interface NULL0
#
interface Vlan-interface10
ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface100
ip address 172.16.100.253 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 10
#
interface GigabitEthernet1/0/2
port link-mode bridge

port access vlan 10
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 10
```

```
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 10
#
interface GigabitEthernet1/0/5
port link-mode bridge
port access vlan 10
#
interface GigabitEthernet1/0/6
port link-mode bridge
port access vlan 10
#
interface Ten-GigabitEthernet1/0/25
port link-mode bridge
port access vlan 100
#
```
Configuration omitted for brevity

```
ospf 1
area 0.0.0.0
network 172.16.100.0 0.0.0.255
network 192.168.10.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 172.16.100.254
#
load xml-configuration
#
user-interface aux 0
user-interface vty 0 15
#
return
```

For more information

To read more about HP Networking Products, go to http://www.hp.com/go/networking

Sign up for updates

hp.com/go/getupdated

Share with colleagues

Rate this document