Using Policy Based Routing and Access Control Lists in a Virtualized Network

A deployment guide for Dell Networking switches

Victor Teeter
Dell Engineering
December 2013

A Dell Deployment and Configuration Guide

Revisions

Date	Description
January 2014	Initial release

THIS DOCUMENT IS PROVIDED "AS-IS", AND WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED. IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE SPECIFICALLY DISCLAIMED. PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Table of Contents

Executive Summary

Administrators who manage internetworks within an organization can implement packet routing based on the organization's policies using the Policy Based Routing (PBR) feature. PBR provides a flexible mechanism to implement solutions in cases where organizational constraints dictate that traffic be routed through specific network paths.

1 Introduction

Enterprise networks which are typically used by several departments within an organization are often divided into VLANs to increase efficiency. Administrators can join multiple physical switches into one virtual switch to make interdepartmental traffic flow more efficiently. Members of each department who communicate frequently reap the benefits of increased traffic flow despite the constraints of geographical distances. With the use of PBR, another layer of control is introduced allowing administrators to evaluate incoming traffic on a switch and apply rules to each packet. These rules, or SET statements, can change the path a packet takes along the network.

Configuring PBR involves constructing a route-map with match and set commands and then applying the corresponding route-map to the interface. IP routing must be enabled on the interfaces for PBR to operate. PBR can only be applied to inbound traffic on these interfaces.

Enabling PBR on a VLAN interface causes the router to compare all incoming packets on the interface against a route-map to match certain criteria in that route-map. An interface can only have one route-map policy assigned to it, but each policy can have multiple route-maps, each with a sequence number to determine its priority. If a single entry's criterion matches the incoming packet, then the entry is chosen and its SET statements are performed. If two or more entries match the criteria, the one with the lowest sequence number is chosen and its SET statements are performed. If there is no match, packets are routed as usual.

Each route-map statement that is used for PBR is configured as **permit** or **deny**. If the statement is marked as deny, traditional destination-based routing is performed on the packet that meets the match criteria. If the statement is marked as permit, and if the packet meets all the match criteria, then SET commands in the route-map statement are applied. If no match is found in the route-map, the packet is not dropped, but instead is forwarded using the routing decision taken by performing destination-based routing. If the network administrator does not want to revert to normal forwarding but instead wants to drop a packet that does not match the specified criteria, a SET statement needs to be configured to route packets to interface null 0 as the last entry in the route-map.

See Appendix A for a flow chart of the packet process.

1.1 User Scenarios

Using PBR and ACLs (access lists) have a wide assortment of uses for any organization. Network Administrators can use PBR when load sharing needs to be done for the incoming traffic across multiple paths based on packet entities in the incoming traffic. To boost network performance of an organization, bulk traffic may need to use a higher bandwidth and high-cost link while basic connectivity continues over a lower bandwidth and low-cost link. For such applications, PBR is the right fit. This document provides three very diverse examples:

- Example 1 – Traffic Isolation is applied on groups of people.
- Example 2 – Server Priority has emphasis on server traffic.
- Example 3 – VLAN Traffic Redirection focuses around VLANs.

1.2 Dell Networking Switches Supporting PBR

The following Dell Networking N-series switches support PBR and may be used in building the configurations in this guide:

N2024

N2024P

N2048

N2048P

N3024

N3024P

N3024F

N3048

N3048P

N4032

N4032F

N4064

N4064F

Note: In the examples it is assumed that traditional routing is already enabled. At minimum, the “ip routing” global command is configured on the switch with static routes in place.

2 Example 1 – Traffic Isolation

Route one IP address range (or subnet) to ISP A, and a second IP address range (or subnet) to ISP B. In this example, it is assumed that traditional routing is already enabled and configured.

Consider the network of the company below which is comprised of several groups including **Human Resources** (HR) and **Accounting**. Each group has a different IP address range within the same subnet. There is a requirement to route HR internet traffic through ISP A while the Accounting traffic needs to be routed through ISP B as shown in Figure 1. The switch that routes this traffic for the different groups can use PBR.

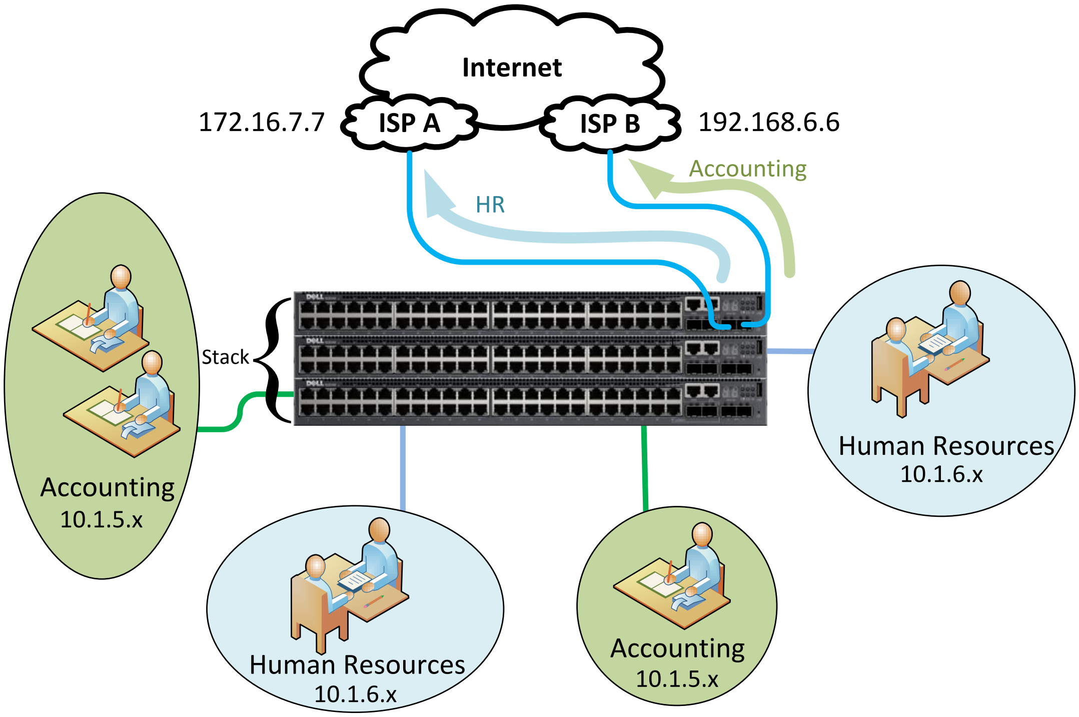


Figure 1. Using Policy Based Routing for Traffic Isolation

Using a route-map, a match statement is configured based on the IP address range of each group. Equal access as well as source IP address-sensitive routing is achieved using this technique.

Two access lists (Accounting and HR) are created to associate each packet to a corresponding work group (Accounting or HR). Packets coming from one range of IP addresses are associated with the Accounting group. Packets from another range of IP addresses are associated with the HR group. A route-map is then used to determine the group each packet belongs to and send them out the desired interface using a “next-hop” statement.

Note: The "next-hop" IP address must be found in the IP routing table to prevent the packet from reverting to traditional routing. This requires that the next hop router be directly connected. Packets are dropped if the next-hop address specified in the route-map is not reachable.

The following commands are used on the switch or switch stack.

```
Enable routing…
console(config)#ip routing

Create three Access-Lists…
console(config)#ip access-list accounting
console(config-ip-acl)#permit ip 10.1.5.0 0.0.0.255 any
console(config-ip-acl)#exit
console(config)#ip access-list hr
console(config-ip-acl)#permit ip 10.1.6.0 0.0.0.255 any
console(config-ip-acl)#exit
console(config)#ip access-list inter-communications
console(config-ip-acl)#permit ip 10.1.5.0 0.0.0.255 10.1.6.0 0.0.0.255
console(config-ip-acl)#permit ip 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
console(config-ip-acl)#exit

Create a Route-Map with three sequences (10, 20, 30)…
console(config)#route-map equal-access deny 10
console(config-route-map)#match ip address inter-communications
console(config-route-map)#exit
console(config)#route-map equal-access permit 20
console(config-route-map)#match ip address accounting
console(config-route-map)#set ip next-hop 192.168.6.6
console(config-route-map)#exit
console(config)#route-map equal-access permit 30
console(config-route-map)#match ip address hr
console(config-route-map)#set ip next-hop 172.16.7.7
console(config-route-map)#exit

Set the ISP-A port configuration…
console(config)#vlan 101
console(config-vlan101)#exit
console(config)#interface vlan 101
console(config-if-vlan101)#ip address 172.16.7.6 255.255.255.0
console(config-if-vlan101)#interface Te1/0/1
console(config-if-Te1/0/1)#switchport trunk allowed vlan all
console(config-if-Te1/0/1)#switchport mode trunk
console(config-if-Te1/0/1)#exit

Set the ISP-B port configuration…
console(config)#vlan 102
console(config-vlan102)#exit
console(config)#interface vlan 102
console(config-if-vlan102)#ip address 192.168.6.5 255.255.255.0
console(config-if-vlan102)#interface Te1/0/2
console(config-if-Te1/0/2)#switchport trunk allowed vlan all
console(config-if-Te1/0/2)#switchport mode trunk
console(config-if-Te1/0/2)#exit

VLAN configuration for HR and Accounting…
console(config)#vlan 111
console(config-vlan111)#exit
console(config)#interface vlan 111
console(config-if-vlan111)#ip address 10.1.5.1 255.255.0.0
console(config-if-vlan111)#ip policy route-map equal-access
console(config-if-vlan111)# exit

Assign interfaces to VLAN…
console(config)#interface range gigabitethernet all
console(config-if)#switchport access vlan 111
console(config-if)#switchport mode access
```

The ip policy route-map "equal-access" is applied to all HR and Accounting interfaces. All packets ingressing these interfaces are policy-routed.

Route map sequence 10 in route map "equal-access" is used to match all packets sourced from any host in the IP address range of 10.1.5.0 /24. If there is a match, it is sent to the next-hop address 192.168.6.6. Route map sequence 20 in route map "equal-access" is used to match all packets sourced from any host in the IP address range of 10.1.6.0 /24. If there is a match, it is sent to the next-hop address 172.16.7.7.

All other packets are forwarded as per normal L3 destination-based routing.

2.1 Validation

Use the commands below to validate or help troubleshoot the configuration in Example 1 – Traffic Isolation.

```
console#show ip access-lists

Current number of ACLs: 2  Maximum number of ACLs: 100

      ACL Name            Rules    Interface(s)       Direction
---------------------------------------------------------------
accounting                  1
hr                          1
inter-communications        1

console#show route-map

route-map “equal-access” deny 10
     Match clauses:
       ip address (access-lists) : inter-communications
     Set clauses:
Policy routing matches: 480 packets, 37440 bytes

route-map "equal-access" permit 20
     Match clauses:
       ip address (access-lists) : accounting
     Set clauses:
       ip default next-hop 192.168.6.6
Policy routing matches: 25 packets, 1950 bytes

route-map "equal-access" permit 30
```

```
     Match clauses:
       ip address (access-lists) : hr
     Set clauses:
       ip default next-hop 172.16.7.7
Policy routing matches: 67 packets, 5226 bytes
```

Note: To see policy routing match counters, issue an ICMP echo request (ping) packet from an HR host to ISP B, or from an Accounting host to ISP A.

```
console#show ip policy

 Interface                     Route-Map
---------   -----------------------------------------------------
Vl111         equal-access


console#show vlan
VLAN   Name               Ports              Type
-----  ---------------   -------------  --------------
1      default            Po1-128,        Default
101    VLAN0101           Te1/0/1         Static
102    VLAN0102           Te1/0/2         Static
111    VLAN0111           Gi1/0/1-48      Static
                          Gi2/0/1-48      Static
                          Gi3/0/1-48      Static
```

3 Example 2 – Server Priority

Ensure server traffic is routed across a higher bandwidth and given the highest priority. Consider the following example where it is assumed traditional routing is already enabled and configured.

It is critical that an organization's primary database server on VLAN 30 is backed up across the network every Thursday morning at 1:00 AM, while using only the larger bandwidth path on the network (Figure 2). The switch that routes this traffic for the server can use PBR.

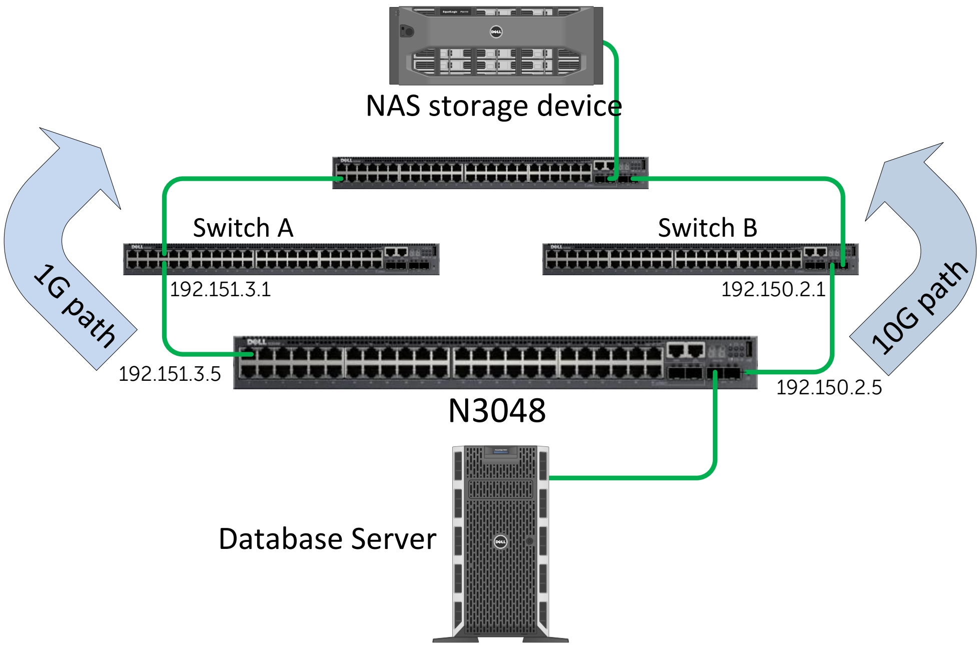


Figure 2. Using Policy Based Routing for Server Priority

An access list is created to determine the IP address to filter, set a priority queue, and set the time and duration for when the PBR will take effect. The route-map then routes all packets from the specified IP address over the larger bandwidth path during the time specified.

The following commands on the Dell Networking N3048 assign the highest COS queue to the server from 1:00 AM to 5:00 AM every Thursday morning, and then routes its traffic across the higher cost, larger bandwidth path (switch B).

Use the following commands in creating Figure 2…

1G Routing interface configuration…

```
console#config
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface vlan 10
console(config-if-vlan10)#ip address 192.151.3.5 255.255.255.0
console(config-if-vlan10)#exit
console(config)#interface gi1/0/1
console(config-if-Gi1/0/1)#switchport trunk allowed vlan 10
console(config-if-Gi1/0/1)#switchport mode trunk
console(config-if-Gi1/0/1)#exit
```

10G Routing interface configuration…

```
console(config)#vlan 20
console(config-vlan20)#exit
console(config)#interface vlan 20
console(config-if-vlan20)#ip address 192.150.2.5 255.255.255.0
console(config-if-vlan20)#exit
console(config)#interface te/1/0/2
console(config-if-Te1/0/2)#switchport trunk allowed vlan 20
console(config-if-Te1/0/2)#switchport mode trunk
console(config-if-Te1/0/2)#exit
```

Server Interface configuration…

```
console(config)#vlan 30
console(config-vlan30)#exit
console(config)#interface vlan 30
console(config-if-vlan30)#ip address 192.149.1.1 255.255.255.0
console(config-if-vlan30)#exit
console(config)#interface te1/0/1
console(config-if-Te1/0/1)#switchport access vlan 30
console(config-if-Te1/0/1)#switchport mode access
console(config-if-Te1/0/1)#exit
```

Add the following commands to implement the Policy Based Route…

Create a time-range…

```
console(config)#time-range db-backup
console(config-time-range)#periodic thursday 1:00 to 5:00
console(config-time-range)#exit
```

Configure an ACL with IP address, time-range and priority…

```
console(Config)#ip access-list db-backup-cos
console(config-ip-acl)#permit ip 192.16.44.2 0.0.0.0 any time-range db-backup
assign-queue 6
console(config-ip-acl)#exit
```

```
Create a Route-Map to set the servers next-hop…
console(config)#route-map database-path permit
console(route-map)#match ip address db-backup-cos
console(route-map)#set ip next-hop 192.150.2.1
console(route-map)#exit
```

```
Assign Route-Map to VLAN…
console(config)#interface vlan 30
console(config-if-vlan30)#ip policy route-map database-path
console(config-if-vlan30)#exit
```

The IP policy route-map "database-path" is applied to the server interface. During the time specified in the range, all packets from the server ingressing this interface are policy-routed to the next-hop address 192.150.2.1. For all other times outside of the range of 1:00 to 5:00 AM Thursday, the access-list is void (therefore the route-map is also void), and traditional routing takes place for server packets.

To recap, the necessary steps to take for this example:

1. Create and embed the time-range in the access list configuration.
2. Embed the values in the route-map.
3. Add the values to the VLAN configuration.
4. Assign the values to the port.

3.1 Validation

Use the commands below to validate or help troubleshoot the configurations in Example 2..

```
console#show ip access-lists

Current number of ACLs: 1  Maximum number of ACLs: 100

      ACL Name            Rules    Interface(s)       Direction
---------------------------------------------------------------
db-backup-cos              1
```

```
console#show route-map

route-map "database-path" permit 10
     Match clauses:
       ip address (access-lists) : db-backup-cos
     Set clauses:
       ip next-hop 192.150.2.1
Policy routing matches: 0 packets, 0 bytes
```

Note: As seen above, the **show route-map** command keeps a counter of matched packets, which is convenient in determining where those packets are sent through the router.

```
console#show vlan

VLAN   Name                     Ports            Type
-----  ---------------       ----------      --------------
1      default                 Po1-128,        Default
                               Gi1/0/2-48,
                               Gi2/0/1-48,
                               Te2/0/1-2,
                               Gi3/0/1-48,
                               Te3/0/1-2
10    VLAN0010                 Gi1/0/1          Static
20    VLAN0020                 Te1/0/2          Static
30    VLAN0030                 Te1/0/1          Static


console#show ip policy
Interface                      Route-Map
---------   -----------------------------------------------------
Vl30          database-path
```

4 Example 3 – VLAN Traffic Redirection

Match packets on one VLAN, then route them to egress another VLAN to get to their destination. Consider the following example where it is assumed traditional routing is already enabled and configured.

Remote servers X, Y, and Z are cached hourly to local servers A, B, and C. Users on VLAN 10 use the local cache servers 99% of the time but periodically need to access the most current data from servers X, Y, and Z located in another city (Figure 3). Traffic on the path between the local and remote servers is oversubscribed and often uses 100% bandwidth. To minimize any delays in traffic between the user workstations on VLAN 10 and the remote servers, a PBR is used to avoid the bottleneck depicted by the red arrow in Figure 3.

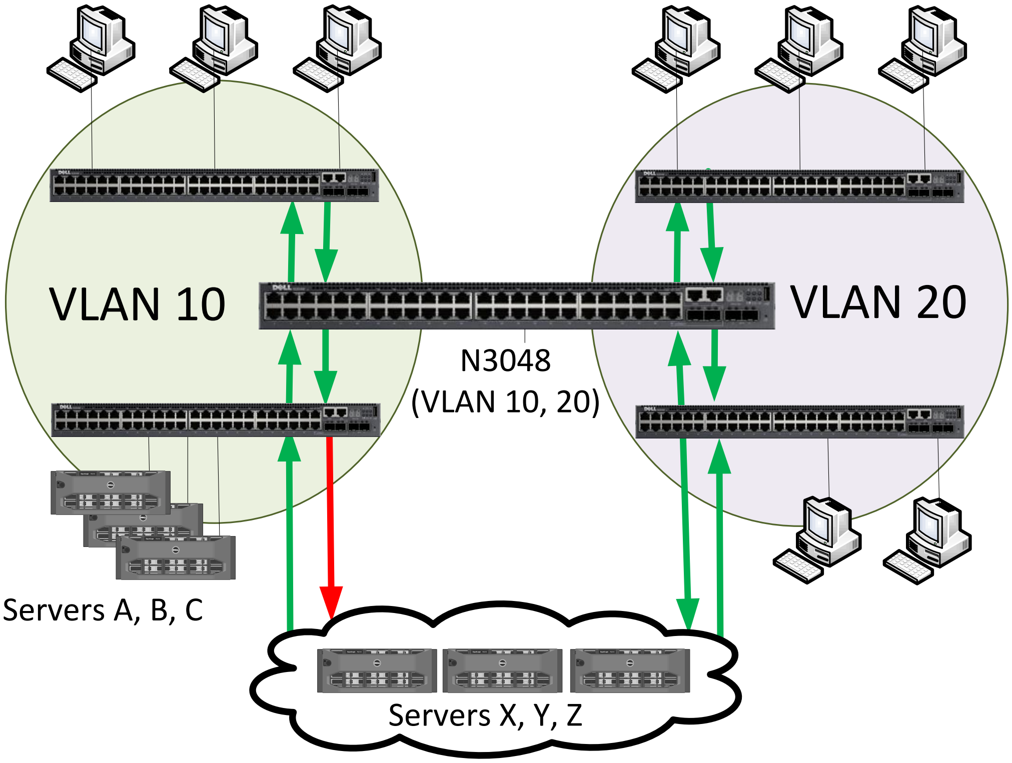


Figure 3. VLAN traffic without PBR

A route-map is created to forward matching packets incoming on VLAN 10 with a destination of Servers X, Y, or Z to egress VLAN 20. Traffic from VLAN 10 workstations to the remote servers is then rerouted over a less utilized path as shown in Figure 4.

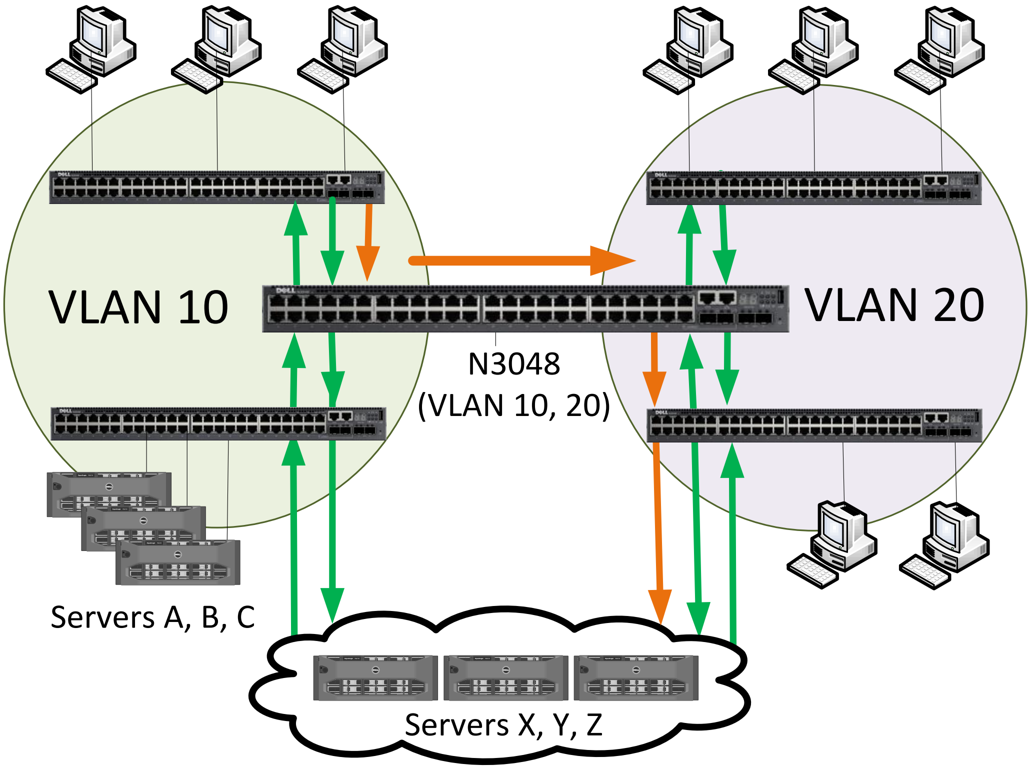


Figure 4. Using Policy Based Routing to redirect VLAN traffic

Two access lists are created. The first access list contains the source IP addresses of servers A, B, and C to filter out these packets, since it is undesirable to reroute any server traffic. This traffic continues to be routed using traditional routing.

The second access list contains destination IP addresses for servers X, Y, and Z so that any packet on VLAN 10 containing one of these IP addresses as a destination will receive a new "next-hop" and rerouted across VLAN 20. When packets from servers A, B, or C have a destination IP address of servers X, Y, or Z, those packets will never see this second access list because the Route-Map sequence "10" takes priority over sequence "20" when both sequences match (note the sequences in the CLI commands below). Client traffic however will never match sequence "10", and only match sequence "20" when they are trying to reach Servers X, Y, or Z.

Note: This example is policy-routing only the VLAN traffic that matches the criteria. It is not policy-routing the entire VLAN (e.g. traffic from servers A, B, and C).

Figure 5 shows IP addresses on the network used for this example.

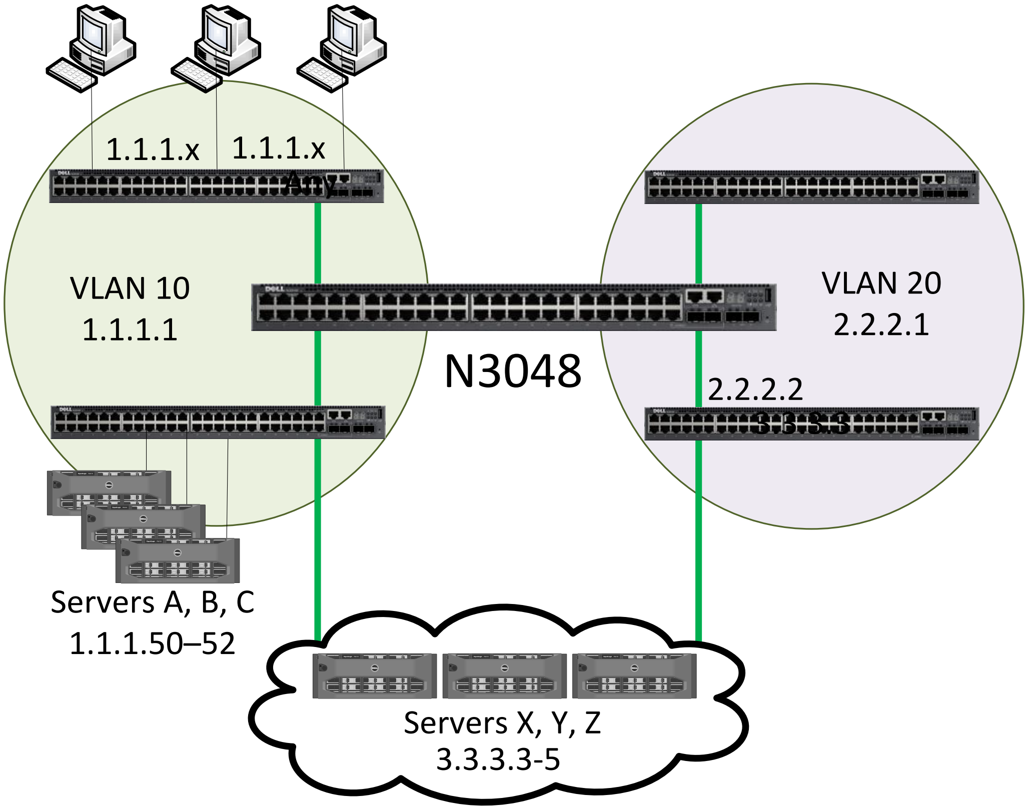


Figure 5. IP addresses on network

The following commands are used to configure the Dell Networking N3048.

```
Create Access-list with source IP addresses of servers ABC…
console(config)#ip access-list servers-ABC
console(config-ip-acl)#permit ip host 1.1.1.50 any
console(config-ip-acl)#permit ip host 1.1.1.51 any
console(config-ip-acl)#permit ip host 1.1.1.52 any
console(config-ip-acl)#exit

Create Access-list with destination IP addresses of servers XYZ…
console(config)#ip access-list allow-1-1-1-clients
console(config-ip-acl)#permit ip any host 3.3.3.3
console(config-ip-acl)#permit ip any host 3.3.3.4
console(config-ip-acl)#permit ip any host 3.3.3.5
console(config-ip-acl)#exit

Create Route-Map using both Access-lists to exempt servers from policy
routing while re-routing clients over VLAN 20…
console(config)#route-map clients-to-XYZ deny 10
console(route-map)#match ip address servers-ABC
console(route-map)#exit
console(config)#route-map clients-to-XYZ permit 20
console(route-map)#match ip address allow-1-1-1-clients
console(route-map)#set ip next-hop 2.2.2.2
console(route-map)#exit
```

Note: Matches on deny route-maps automatically reverts packets to traditional routing and the policy routing is ignored. For this reason there is no SET statement for the first MATCH statement above.

```
Assign Route-Map and IP address to VLAN…
console(config)#vlan 10
console(config-vlan10)#exit
console(config)#interface vlan 10
console(config-if-vlan10)#ip address 1.1.1.1 255.255.255.0
console(config-if-vlan10)#ip policy route-map clients-to-XYZ
console(config-if-vlan10)#exit

Remaining commands to configure traditional routing on the Dell N3048 as
shown in Figure 5 (if not previously configured)…
console(config)#ip routing
console(config)#vlan 20
console(config-vlan20)#exit
console(config)#interface vlan 20
console(config-if-vlan20)#ip address 2.2.2.1 255.255.255.0
console(config-if-vlan20)#exit
console(config)#interface range gi1/0/1-10
console(config-if)#switchport access vlan 10
console(config)#interface range gi1/0/11-20
console(config-if)#switchport access vlan 20
```

The route-map "clients-to-XYZ" is applied to all incoming packets on VLAN 10. Each packet is compared to see if it is from one of the servers A, B, or C, and at the same time compared to see if it is on its way to servers X, Y, or Z.

- If it matches both then it means the packet is from either server A, B, or C, and will not be routed using policy routing, but will still be routed as normal.
- If it matches only the "deny 10" statement it also means it is from server A, B, or C, and again will not be routed using policy routing, but will still be routed as normal.
- If it matches only the "permit 20" statement it means it is not from server A, B, or C, and it also means it is on its way to servers X, Y, or Z. In this case, the packet will be policy routed over VLAN 20.

All other packets are forwarded as per normal L3 destination-based routing.

4.1 Validation

Use the commands below to validate or help troubleshoot the Example 3 configuration.

```
console#show ip access-lists

Current number of ACLs: 2  Maximum number of ACLs: 100

      ACL Name                    Rules       Interface(s)        Direction
------------------------------- ----- ------------------------- ---------
servers-ABC                       3
allow-1-1-1-clients               3


N3048-55#show route-map

route-map "clients-to-XYZ" deny 10
     Match clauses:
       ip address (access-lists) : servers-ABC
     Set clauses:
Policy routing matches: 0 packets, 0 bytes

route-map "clients-to-XYZ" permit 20
     Match clauses:
       ip address (access-lists) : allow-1-1-1-clients
     Set clauses:
       ip next-hop 2.2.2.2
Policy routing matches: 0 packets, 0 bytes


N3048-55#show vlan

VLAN   Name                     Ports              Type
-----  ---------------      ----------        --------------
1      default               Po1-128,          Default
                             Gi1/0/21-48,
                             Te1/0/1-2
10     VLAN0010              Gi1/0/1-10        Static
20     VLAN0020              Gi1/0/11-20       Static


console#show ip policy
Interface                     Route-Map
---------   -----------------------------------------------------
Vl10          clients-to-XYZ
```

5 Dropping Packets

Unlike a “deny” statement in an access list, a Route-Map “deny” statement does not drop a packet when the criteria matches the packet. Instead the Route-Map simply turns all control of the packet back over to traditional routing and ignores all Policy Based Routing rules. In other words, when a “deny” sequence is matched, the packet is treated as if no PBR exists.

PBR does however provide a way to drop a packet if desired. By using the **set interface null0** command, users can drop any packet that matches the criteria on a *permit* statement. Simply add the following set statement to your *permit* sequence:

```
console(config-route-map)#set interface null0
```

All packets matching the *permit* statement will be dropped. They will neither be routed with a PBR nor will they be routed with traditional routing.

Note: Only permit sequences may have set statements. Matching on deny sequences will always turn control back to traditional routing.

6 Rerouting Remaining Packets on an Interface

If there is a need to route any remaining packets on an incoming interface, it can be done with PBR. This is achieved simply by not specifying a match statement in the route-map sequence. If used by itself without other sequences, this can also be used to re-route all incoming traffic.

Note: In a route-map sequence, all packets match by default if no match statement is specified.

This can be useful as a lowest priority sequence to send all remaining traffic through a particular route if no higher priority sequences were matched.

Using Example 1 above, the route-map only matches packets from two groups (hr and accounting) on the network. If there are more groups, they will use traditional routing since there is no route-map matching critera for those packets. However, if it is desired that all other traffic be routed along a third path, then a third sequence (i.e. 30) can be used. The third sequence does not require a match statement since the desire is that all packets not matching sequence 10 or 20 are routed through a third next-hop.

Consider the following commands taken from Example 1. By adding a few more commands, the remaining traffic can also be policy routed.

```
The existing sequences from Example 1 are…
console(config)#route-map equal-access permit 10
console(config-route-map)#match ip address accounting
console(config-route-map)#set ip default next-hop 192.168.6.6
console(config-route-map)#exit
console(config)#route-map equal-access permit 20
console(config-route-map)#match ip address hr
console(config-route-map)#set ip default next-hop 172.16.7.7
console(config-route-map)#exit

Add the following to route all remaining packets along a third path…
console(config)#route-map equal-access permit 30
console(config-route-map)#set ip default next-hop 175.10.8.8
console(config-route-map)#exit
```

All incoming packets that do not match sequence 10 or 20 are now policy routed with a next-hop of 175.10.8.8.

7 Other Resources

This document only provides a few examples of the many ways PBR can be used to route traffic based on organizational policies or contraints.

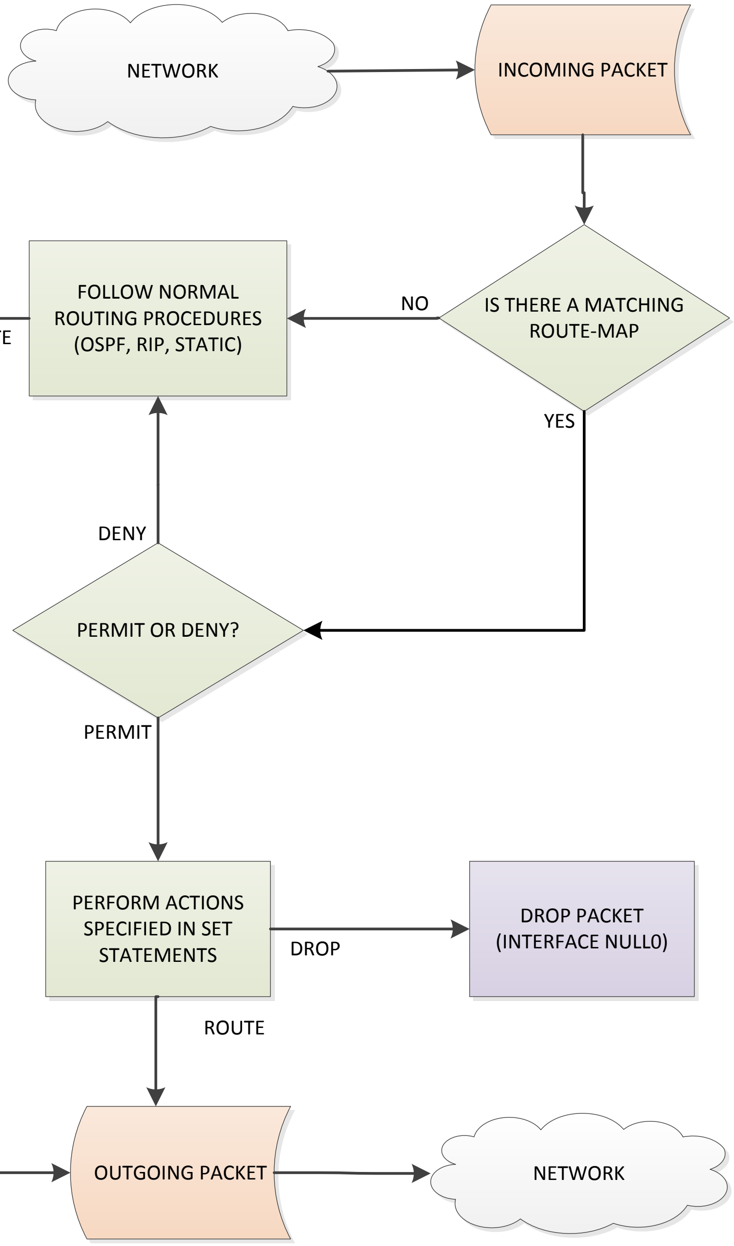
The User Guide for the Dell N-series switches contains additional details on configuring this feature.

The Command Line (CLI) Reference Guide also contains details on each command used in this document.

Download the latest User Guide and CLI Reference Guide at http://www.dell.com/support. This site is focused on meeting your needs with proven services and support.

http://DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Appendix A: Packet Process flow through a Route-map


NETWORK
INCOMING PACKET
IS THERE A MATCHING ROUTE-MAP
NO
FOLLOW NORMAL ROUTING PROCEDURES (OSPF, RIP, STATIC)
ROUTE
YES
DENY
PERMIT OR DENY?
PERMIT
PERFORM ACTIONS SPECIFIED IN SET STATEMENTS
DROP
DROP PACKET (INTERFACE NULL0)
ROUTE
OUTGOING PACKET
NETWORK